SIEMENS

SIMATIC NET

Industrial Ethernet Security SCALANCE SC-600 Web Based Management (WBM) V3.0

Configuration Manual

11/2022
C79000-G8976-C475-06

Legal information

Warning notice system

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

⚠ DANGER

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

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

⚠ WARNING

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

Trademarks

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

Disclaimer of Liability

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

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000-G8976-C475-06
Ⓟ 12/2022 Subject to change

Introduction

Validity of the configuration manual

This Configuration Manual covers the following products:

- SCALANCE SC622-2C
- SCALANCE SC626-2C
- SCALANCE SC632-2C
- SCALANCE SC636-2C
- SCALANCE SC642-2C
- SCALANCE SC646-2C

This Configuration Manual applies to the following software version:

- Firmware as of version V3.0

Purpose of the Configuration Manual

This Configuration Manual is intended to provide you with the information you require to commission and operate the SCALANCE SC-600 Security Appliances as information modules for network communication. It provides you with the information you require to configure the SCALANCE SC-600 Security Appliances.

Designations used

Classification	Description	Term
Product line	If information applies to all product groups within the product line, the term SCALANCE SC-600 is used.	• SCALANCE SC-600
Product group	If information applies to all devices of a product group, a suitable term is used. • SCALANCE SC622-2C and SC626-2C • SCALANCE SC622-2C, SC632-2C and SCALANCE SC642-2C • SCALANCE SC626-2C, SCALANCE SC636-2C and SCALANCE SC646-2C • SCALANCE SC632-2C and SCALANCE SC636-2C • SCALANCE SC642-2C and SCALANCE SC646-2C	• SC62x-2C • SC6x2-2C • SC6x6-2C • SC63x-2C • SC64x-2C
Device	If information relates to a specific device, the device name is used.	• SCALANCE SC622-2C • SCALANCE SC626-2C • SCALANCE SC632-2C • SCALANCE SC636-2C • SCALANCE SC642-2C • SCALANCE SC646-2C

New in this edition

- Export von Firewall- und NAT-Tabellen
- Importing SINEMA configuration data
- Configuration backup
- Port Mirroring
- Activation of a unique VLAN MAC address
- Quality of Service (QoS) technology
- OSPFv2
- IPv6 support
- Scheduled restart: Apply configurations from the selected backup prior to restart
- Advanced SNMP configuration
- Configurable password policies
- Deactivation of ring ports and standby ports
- Dynamic firewall: Time triggered and login to RADIUS server
- "Enhanced Passive Listening Compatibility" function
- Extended firewall logging

- Brute Force Prevention
- Policy-based routing
- Connection check
- Deactivation of firewall rules
- Configuration backup
- Creating remote clients
- Appendix C "Ciphers used"

Replaced edition

Edition 09/20201

Orientation in the documentation

Apart from this configuration manual, the products also have the following documentation:

- Configuration Manual:
  - SCALANCE SC-600 Command Line Interface (CLI)
    This document contains the CLI commands that are supported by the Security Appliances SCALANCE SC-600 .
- Operating instructions:
  - SCALANCE SC-600
  - Pluggable transceiver SFP/SFP+/SCP/STP

  These documents contain information on installing and connecting up and approvals for the products.
- Getting Started SCALANCE S615
  Based on examples, these documents explain the configuration of the SCALANCE S615 and can also be used for the Security Appliances SCALANCE SC-600.

You will find the documentation here:

- On the data medium that ships with some products:
  - Product CD / product DVD
  - SIMATIC NET Manual Collection
- On the Internet pages of Siemens Industry Online Support:
  Link: (https://support.industry.siemens.com/cs/ww/en/ps/15327/man)

Further documentation

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

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

You will find the system manuals here:

- On the data medium that ships with some products:
  - Product CD / product DVD
  - SIMATIC NET Manual Collection
- On the Internet pages of Siemens Industry Online Support:
  - Industrial Ethernet / PROFINET Industrial Ethernet System Manual
    Link: (https://support.industry.siemens.com/cs/ww/en/view/27069465)
  - Industrial Ethernet / PROFINET - Passive Network Components System Manual
    Link: (https://support.industry.siemens.com/cs/ww/en/view/84922825)

SIMATIC NET manuals

You will find the SIMATIC NET manuals here:

- On the data medium that ships with some products:
  - Product CD / product DVD
  - SIMATIC NET Manual Collection
- On the Internet pages of Siemens Industry Online Support:
  Link: (https://support.industry.siemens.com/cs/ww/en/ps/15247)

License conditions

Note

Open source software

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

You will find the license conditions as a loadable file on the WBM pages of the device.
You will find the description of opening and loading license conditions in section File list (Page 155) of the configuration manuals.

You can find the file with the license conditions for open source software under the following name:

- OSS_Readme.zip

Security information

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

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

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

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

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

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

Note on firmware/software support

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

Firmware

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

Device defective

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

Decommissioning

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

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

Also restore the factory settings on the storage medium.

Recycling and disposal

The product is low in pollutants, can be recycled and meets the requirements of the WEEE directive 2012/19/EU "Waste Electrical and Electronic Equipment".

Do not dispose of the product 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.

Keep to the local regulations.

You will find information on returning the product on the Internet pages of Siemens Industry Online Support:
Link: (https://support.industry.siemens.com/cs/ww/en/view/109479891)

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 on the Internet at the following address:

Link: (https://support.industry.siemens.com/cs/ww/en/view/50305045)

Table of contents

Security recommendations

1

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

General

- Check the device regularly to ensure that these recommendations and/or other internal security policies are complied with.
- Evaluate the security of your location and use a cell protection concept with suitable products. For more information, refer to:
  Link: (https://www.siemens.com/industrialsecurity)
- When the internal and external network are disconnected, an attacker cannot access internal data from the outside. If possible, operate the device only within a protected network area.
- Use VPN to encrypt and authenticate communication from and to the devices.
- For data transmission via a non-secure network, use an encrypted VPN tunnel (IPsec, OpenVPN).
- 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.

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 pre-installed Web server certificate (RSA, 2048 bit key length) and an SSH Private Key in the device. Replace this certificate with a user-generated, high-quality certificate with key. Use a certificate signed by a reliable external or internal certification authority. You can install the certificate in the WBM via "System > Load and Save".
- Use the certification authority including key revocation and management to sign the certificates.
- Use password-protected certificates in the format "PKCS #12".
- Use certificates with a key length of 4096 bits.
- 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.
- SSH and SSL keys are available for admin users. Make sure that you take appropriate security measures when shipping the device outside of the trusted environment:
  - Replace the SSH and SSL keys with disposable keys prior to shipping.
  - Decommission the existing SSH and SSL keys. Create and program new keys when the device is returned.
- Verify certificates based on the fingerprint on the server and client side to prevent "man in the middle" attacks. Use a second, secure transmission path for this.
- Before sending the device to Siemens for repair, replace the current certificates and keys with temporary disposable certificates and keys, which can be destroyed when the device is returned.

Physical/remote access

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

Hardware / Software

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

- Use the authentication and encryption mechanisms of SNMPv3 if possible. Use strong passwords.
- Configuration files can be downloaded from the device. Ensure that configuration files are adequately protected.
  Configuration files can be password protected during download. You enter passwords on the WBM page "System > Load & Save > Passwords".
- When using SNMP (Simple Network Management Protocol):
  - Configure SNMP to generate a notification when authentication errors occur.
    For more information, see WBM "System > SNMP > Notifications".
  - Ensure that the default community strings are changed to unique values.
  - Use SNMPv3 whenever possible. SNMPv1 and SNMPv2c are considered non-secure and should only be used when absolutely necessary.
  - If possible, prevent write access.

Secure/ non-secure protocols

- Use secure protocols if access to the device is not prevented by physical protection measures.
- Restrict the use of non-secure protocols. While some protocols are secure (e.g. HTTPS, SSH, 802.1X, etc.), others were not designed for the purpose of securing applications (e.g. SNMPv1/v2c, RSTP, etc.).
  Therefore, take appropriate security measures against non-secure protocols to prevent unauthorized access to the device/network. Use non-secure protocols on the device using a secure connection (e.g. SINEMA RC).
- If non-secure protocols and services are required, ensure that the device is operated in a protected network area.
- Check whether use of the following protocols is necessary:
  - HTTP
  - Broadcast pings
  - Non authenticated and unencrypted interfaces
  - ICMP (redirect)
  - LLDP
  - DHCP Options 66/67
  - SNTP
  - NTP
  - TFTP
  - VRRPv3
  - DNS
  - SNMPv1/V2c

- If a secure alternative is available for a protocol, use it.
  The following protocols provide secure alternatives:
  - SNMPv1/v2 → SNMPv3
    Check whether use of SNMPv1 is necessary. SNMPv1 is classified as non-secure. Use the option of preventing write access. The product provides you with suitable setting options. If SNMP is enabled, change the community names. If no unrestricted access is necessary, restrict access with SNMP.
  - HTTP → HTTPS
  - NTP → Secure NTP
  - TFTP → SFTP
- Using a firewall, 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.
- For the DCP function, leave the "Read-Only" mode after commissioning.

Interfaces security

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

1.1 Ports

Notes on the ports

VLAN1 and VLAN2 on different ports

Depending on the device type, VLAN1 and VLAN2 are on different physical ports:

- SC632-2C, SC642-2C: VLAN1 = port 1, VLAN2 = port 2
- SC636-2C, SC646-2C: VLAN1 = port 1-4, VLAN2 = port 5-6

With SC62x-2C, only access via VLAN1 is possible:

- SC622: Port 1
- SC626: Port 1-5

No Layer2 bridge functionality

The following ports do not support Layer 2 bridge functionality and thus form a natural network boundary for PROFINET:

- SC622-2C: Port 2
- SC626-2C: Port 6

The SC622-2C and SC626-2C devices fulfil the properties of a 2-port router according to IEC 61784-3-3 (PROFIsafe), section 8.1.2.
They are therefore suitable for use as cell protection device in safety environments in which it cannot be guaranteed that PROFIsafe addresses are unique.

List of available services

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

The table includes the following columns:

- **Service/Protocol**
  The services/protocols that the device supports.
- **Protocol / Port number**
  Port number assigned to the protocol.
- **Default port status**
  The port status on delivery (factory setting) distinguishes between local and external access.
  - Local access: The port is accessed via a local connection (VLAN1).
  - External access: The port is accessed via an external connection (VLAN2).
    For SC622-2C: Port 2
    For SC626-2C: Port 6
- **Configurable port/service**
  Indicates whether the port number or the service can be configured via WBM / CLI.
- **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	Protocol/ Port number	Default status		Configurable		Authentication	Encryption [4]
		Local	External	Port	Service		
DHCPv4 Client	UDP/68	Closed	Open	--	✓	--	--
DHCPv4-Server	UDP/67	Closed	Closed	--	✓	--	--
DNS-Client	TCP/53 UDP/53	Outgoing only	Outgoing only	--	✓	--	--
DNS-Server	TCP/53 UDP/53	Closed	Closed	--	✓	--	--
DDNS	TCP/80 UDP/80 TCP/443 UDP/443	Outgoing only	Outgoing only	--	✓	✓	--
Firewall State Sync	UDP/3780	Closed	Closed	✓	✓	--	--
HTTP [1]	TCP/80	Open	Closed	✓	✓	✓	--
HTTP Proxy	TCP/3128 TCP/8080	Outgoing only	Outgoing only	✓	✓	Optional	--

Service/Protocol	Protocol/ Port number	Default status		Configurable		Authentication	Encryption [4]
		Local	External	Port	Service		
HTTPS	TCP/443	Open	Closed	✓	✓	✓	✓
IPsec/IKE	UDP/500 UDP/4500	Closed	Closed	--	✓	✓	✓
IPv6 router-advertisement, neighbor-solicitation, neighbor-advertisement	ICMPv6	Open	Open	--	✓	--	--
NTP-Client	UDP/123	Outgoing only	Outgoing only	✓	✓	--	--
NTP-Server	UDP/123	Closed	Closed	✓	✓	--	--
NTP-Server (secure)	UDP/123	Closed	Closed	✓	✓	✓	--
OpenVPN-Client	UDP/1194 TCP/1194	Outgoing only	Outgoing only	✓	✓	✓	✓
OpenVPN-Server	UDP/1194 TCP/1194	Closed	Closed	✓	✓	✓	✓
OSPF	IP/89	Closed	Closed	--	✓	--	--
Ping	ICMP/ICMPv6	Open	Closed	--	✓	--	--
RADIUS	UDP/1812 UDP/1813	Outgoing only	Outgoing only	✓	✓	✓	--
SFTP	TCP/22	Outgoing only	Outgoing only	✓	✓	✓	✓
Siemens Remote Service (cRSP/SRS)	TCP/443	Outgoing only	Outgoing only	--	✓	Optional	✓
SINEMA RC	HTTPS/443 and TCP/UDP depending on the server configuration	Outgoing only	Outgoing only	✓	✓	✓	✓
SMTP Client	TCP/25	Outgoing only	Outgoing only	✓	✓	Optional	--
SMTP (secure)	TCP/465 TCP/587	Outgoing only	Outgoing only	✓	✓	Optional	✓
SNMPv1/v2c [2]	UDP/161	Open	Closed	✓	✓	--	--
SNMPv3	UDP/161	Open	Closed	✓	✓	Optional	Optional
SNMP Traps	UDP/162	Outgoing only	Outgoing only	✓	✓	--	--
SNTP Client	UDP/123	Closed	Closed	✓	✓	--	--
SSH	TCP/22	Open	Closed	✓	✓	✓	✓
Syslog Client	UDP/514	Outgoing only	Outgoing only	✓	✓	--	--
Syslog Client TLS	TCP/6514	Outgoing only	Outgoing only	✓	✓	--	✓
TFTP	UDP/69	Outgoing only	Outgoing only	✓	✓	--	--
VRRP	IP/112	Closed	Closed	--	✓	--	--
VXLAN [3]	UDP/4789	Closed	Closed	✓	✓	--	--

[1] Is rerouted to HTTPS

[2] Read-only access

[3] Only SC63x-2C/SC64x-2C

[4] You can find additional information on the encryption methods used in the WBM appendix "Ciphers used".

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

The table includes the following columns:

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

Layer 2 service	Default status	Configurable
DCP	Open (when configured)	✓
LLDP	Open (when configured)	✓
SIMATIC NET TIME	Open (when configured)	✓
VLAN	Open (when configured)	✓

Description

2

2.1 Function

Configuration

Configuration of all parameters using the

- Web Based Management (WBM) via HTTPS.
- Command Line Interface (CLI) via SSH and serial interface.

Security functions

- Router with NAT function
  - IP masquerading
  - NAPT
  - Source NAT
  - NETMAP
- Password protection
- Firewall function
  - Port forwarding
  - MAC firewall (layer 2)
  - IP firewall with stateful packet inspection (layer 3 and 4)
  - Global and dynamic firewall rules
- VPN functions
  To establish a VPN (Virtual Private Network), the following functions are available:
  - IPsec VPN (SC64x-2C)
  - OpenVPN (SC64x-2C)
- SINEMA RC client
- Use of proxy servers
- Siemens Remote Service cRSP/SRS (SC64x-2C)
- Brute Force Prevention

Monitoring / diagnostics / maintenance

- LEDs
  Display of operating statuses via an LED display. You will find further information on this in the Operating Instructions of the device.
- Logging
  For monitoring have the events logged.
- SNMP
  For monitoring from a central network management station.

Other functions

- Time-of-day synchronization
  - NTP client and NTP server
  - Secure NTP server
  - SIMATIC Time Client
  - SNTP
- DHCP
  - DHCP Server
  - DHCP Client
- Virtual networks (VLAN)
  To structure Industrial Ethernet networks with a fast growing number of nodes, a physical network can be divided into several virtual subnets.
- Digital input/digital output via signaling contact
- DDNS client
- DNS client / DNS proxy
- SMTP client

Combo ports

Combo port is the name for two communication ports. A combo port has the two following plug-in options:

- a fixed RJ-45 port
- a pluggable transceiver slot that can be equipped individually

Of these two ports, only one can ever be active.

You can set the active port on the WBM page "System > Ports > Configuration" or with the CLI command `media-type`.

2.2 Requirements for operation

Requirements for installation and operation

A PG/PC with a network connection must be available in order to configure the devices. If no DHCP server is available, a PG/PC on which SINEC PNI is installed is necessary for the initial assignment of an IP address to the device. For the other configuration settings, a PG/PC with a serial interface or an Internet browser is necessary.

Serial interface

The device has a serial interface. An IP address is unnecessary to be able to access the device via the serial interface. A serial cable ships with the products.

Set the following parameters for the connection:

- Bits per second: 115200
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

Power supply

A power supply with a voltage between 12 VDC and 24 VDC that can provide sufficient current.

You will find further information on this in the device-specific operating instructions.

Configuration

In the factory settings, the SCALANCE SC-600 can be reached as follows for initial configuration:

	Default values set in the factory		
Ethernet interface for the configuration (internal)	**SC622-2C** **SC632-2C** **SC642-2C**	**SC636-2C** **SC646-2C**	**SC626-2C**
	P01	P01 ... P04 (VLAN 1)	P01 ... P05 (VLAN 1)
IP address	Must be assigned manually. See section "Initial assignment of an IPv4 address (Page 40)".		
WBM	Access using HTTP: Port 80 with forwarding to HTTPS Access using HTTPS: TCP port 443		
CLI	Access using SSH: TCP port 22 Access via the serial interface: It is then no longer possible to assign the IP address via SINEC PNI. The IP address can then only be assigned using CLI.		

	Default values set in the factory
User name	admin The user name can be changed after the first login or after a "Restore Factory Defaults and Restart". Afterwards, renaming "admin" is no longer possible.
Password	admin The password needs to be changed after the first login or after a "Restore Factory Defaults and Restart".

You will find more information in "Web Based Management (Page 75)" and in "Starting and logging in (Page 76)".

2.2.1 Use in a PROFINET environment

Configuration information

When using the device in a PROFINET environment, follow the following configuration instructions:

- Set the "Aging Time [s]" to 45 seconds under "Layer 2 > Dynamic MAC Aging".
- Disable the function "Spanning Tree" under "Layer 2" and enable the function "Passive Listening" under "Layer 2 > Configuration".

2.3 System functions

Availability of the system functions

The following table shows the availability of the system functions. Note that all functions are described in this configuration manual and in the online help.

We reserve the right to make technical changes.

Information	ARP Table
	Log Tables
	Faults
	DHCP Server
	LLDP
	Fiber Monitoring
	IPv4 routing
	IPv6 routing
	Redundancy
	Ethernet-Statistik
	Unicast/Multicast
	Richtlinien-basiertes Routing
	SNMP
	Security
	IPsec VPN (SC64x-2C)
	SINEMA RC
	OpenVPN (SC64x-2C)
	VXLAN (SC63x/SC64x)
	Firewall Monitoring

System	Configuration
	General
	DNS
	Restart
	Load&Save
	Events
	SMTP client
	DHCP
	SNMP
	System time
	Auto logout
	Button
	Syslog client
	Ports
	Fault Monitoring
	PLUG
	Ping
	DCP Discovery
	Port diagnostics
	cRSP/SRS (SC64x-2C)
	Proxy server
	SINEMA RC
	Connection Check
	Backup der Konfiguration
Layer 2	Configuration
	Quality of Service
	Port Based VLAN
	VXLAN (SC63x/SC64x)
	Mirroring
	Dynamic MAC Aging
	Ring redundancy
	Spanning Tree
	DCP-Weiterleitung
	LLDP
	Fiber Monitoring Protocol
	Unicast/Multicast
	Broadcast
	RMON
	Inter-VLAN Bridge (SC63x/SC64x)

Layer 3 (IPv4)	Subnets
	PBR
	OSPFv2
	NAT
	Static routes
	VRRPv3
Layer 3 (IPv6)	Subnets
	Static routes
Security	Users
	Passwords
	AAA
	Certificates
	Firewall
	IPsec VPN (SC64x-2C)
	OpenVPN (SC64x-2C)
	Brute Force Prevention

2.4 Configuration limits for WBM and CLI

Configuration limits of the device

The following table lists the configuration limits for Web Based Management and the Command Line Interface of the device.

	Configurable function		Maximum number
System	DNS Server		2
	DNS Records		128 Domain name: Maximum of 256 characters
	Syslog server		3
	SNMPv1 trap receiver		10
	SNTP server		1
	NTP server		4
	NTP (secure) server		4
	DHCP pools		8
	IPv4 addresses managed by the DHCP server (dynamic + static)		100
	Static assignments per DHCP pool		128
	DHCP options (3, 6, 12, 15, 66, 67)		5
	SINEMA RC		1
	Proxy server		5
	Configuration backup		Without PLUG: • 2 without firmware • 0 with firmware
			With PLUG: • 5 without firmware • 2 with firmware (firmware on PLUG)
Layer 2	VLAN	Virtual LANs (port-based; including VLAN 1)	257
		Maximum frame size	2048 bytes
	VXLAN	NVE interface / VNI	1 NVE / 1 VNI
Layer 3	IP interfaces		32
	Static routes		100
	Possible routes to the same destination		8
	NAPT		1000
	Source NAT		1000
	NETMAP rules		1000
	NETMAP rules in conjunction with VRRPv3		1000
	Alias IP addresses		1024
	VRRPv3		VRRPv3 instances (VRID): 16 Assigned IP addresses: 1 per VRID

	Configurable function	Maximum number
Security	Users	30 (incl. user preset in the factory "admin")
	Groups	32
	Roles	32 (incl. the predefined roles)
	RADIUS Server	4
	NAT rules	1000
	Firewall rules	IP protocols: 16 IP services: 128 ICMP services: 16 IP rules: 1000 MAC rules: 1000 Dynamic firewall: • Maximum number: 8 rule sets • Parallel user access: 4 • Maximum of 128 IP rules per firewall rule set
	IPsec VPN	200 tunnels [1)]
	OpenVPN	Server: 3 Clients: 5 Maximum of 128 client connections per server Maximum of 128 client connections to a device

[1)] Applies only to SCALANCE SC642-2C and SCALANCE SC646-2C; restriction: You can create a maximum of 20 phase 2 connections per phase 1 (Remote End).

2.5 PLUG

The PLUG is a removable medium and is used to transfer the configuration of the old device to the new device when a device is replaced. The PLUG is available in the following variants:

- C-PLUG: The removable data storage medium only saves the configuration data of the device.

How it works

NOTICE
Do not remove or insert a C-PLUG during operation! A PLUG may only be removed or inserted when the device is turned off. The device checks whether a PLUG is present at one second intervals. If it is detected that the PLUG was removed, there is a restart. If a valid PLUG was inserted in the device, the device changes to a defined error state following the restart.

The device supports the following modes of operation:

- Without C-PLUG/KEY-PLUG
  The device stores the configuration in internal memory.
  This mode is active if no C-PLUG/KEY-PLUG is inserted.
- With unwritten C-PLUG/KEY-PLUG
  If an unwritten C-PLUG/KEY-PLUG (factory status or deleted with Clean function) is used, the local configuration already existing on the device is automatically stored on the inserted C-PLUG/KEY-PLUG during startup.
  This mode is active as soon as an unwritten C-PLUG/KEY-PLUG is inserted.
- With written C-PLUG/KEY-PLUG
  A device with a written and accepted C-PLUG/KEY-PLUG ("ACCEPTED" status) uses the configuration data of the PLUG automatically when it starts up. The requirement for acceptance is that the data was written by a compatible device type.
  If there is configuration data in the internal memory of the device, this is overwritten.
  This mode is active as soon as a written C-PLUG/KEY-PLUG is inserted.

Response to errors

Inserting a C-PLUG/KEY-PLUG that does not contain the configuration of a compatible device type, accidentally removing the C-PLUG/KEY-PLUG or general malfunctions of the C-PLUG/KEY-PLUG are signaled by the diagnostics mechanisms of the device:

- Fault LED
- Web Based Management (WBM)
- SNMP
- Command Line Interface (CLI)

The user then has the choice of either removing the C-PLUG/KEY-PLUG again or selecting the option to reformat the C-PLUG/KEY-PLUG.

Type	Description	Article number
C-PLUG	Removable data storage medium (256 MB) for the configuration data and saving the firmware.	6GK1900-0AB10

2.5.1 PRESET PLUG

PLUG with preset function (PRESET-PLUG)

With PRESET-PLUG it is possible to install the same configuration and the firmware belonging to it on several devices.

Note

Using configurations with DHCP

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

You assign fixed IP addresses extra following the basic installation.

In a PLUG that was configured as a PRESET-PLUG, the device configuration, user accounts, certificates and the firmware are stored.

Note

Restore factory defaults and restart with a PRESET PLUG inserted

If you reset a device to the factory defaults, when the device restarts an inserted PRESET PLUG is formatted and the PRESET PLUG functionality is lost. You then need to create a new PRESET PLUG.

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

For more detailed information on creating and using a PRESET PLUG refer to the section Device configuration with PRESET-PLUG (Page 421).

Technical basics

3

3.1 IP address

3.1.1 IPv4 / IPv6

What are the essential differences?

	IPv4	IPv6
IP configuration	• DHCP server • Manual	• Stateless Address Autoconfiguration (SLAAC): Stateless autoconfiguration using NDP (Neighbor Discovery Protocol) – Creates a link local address for every interface that does not require a router on the link. – Checks the uniqueness of the address on the link that requires no router on the link. – Specifies whether the global addresses are obtained via a stateless mechanism, a stateful mechanism or via both mechanisms. (Requires a router on the link.) • Manual • DHCPv6 (stateful)
Available IP addresses	32-bit: 4, 29 * 10^9 addresses	128-bit: 3, 4 * 10^{38} addresses
Address format	Decimal: 192.168.1.1 with port: 192.168.1.1:20	Hexadecimal: 2a00:ad80::0123 with port: [2a00:ad80::0123]:20
Loopback	127.0.0.1	::1
IP addresses of the interface	4 IP addresses	Multiple IP addresses • LLA: A link local address (formed automatically) fe80::/128 per interface • ULA: Several unique local unicast addresses per interface • GUA: Several global unicast addresses per interface
Header	• Checksum • Variable length • Fragmentation in the header • No security	• Checking at a higher layer • Fixed size • Fragmentation in the extension header
Fragmentation	Host and router	Only endpoint of the communication
Quality of service	Type of Service (ToS) for prioritization	The prioritization is specified in the header field "Traffic Class".
Types of frame	Broadcast, multicast, unicast	Multicast, unicast, anycast

	IPv4	IPv6
Identification of DHCP clients/ server	Client ID: • MAC address • DHCP client ID • System name • PROFINET station name • IAID and DUID	DUID + IAID(s) = exactly one interface of the host DUID = DHCP unique identifier Unique identifier of server and clients IAID = Identity Association Identifier At least one per interface is generated by the client and remains unchanged when the DHCP client restarts Three methods of obtaining the DUID • DUID-LLT • DUID-EN • DUID-LL
Resolution of IP addresses in hardware addresses	ARP (Address Resolution Protocol)	NDP (Neighbor Discovery Protocol)

3.1.2 IPv4

	IPv4
IP configuration	• DHCP Server • Manual
Available IP addresses	32-bit: 4, 29 * 10^9 addresses
Address format	Decimal: 192.168.1.1 with port: 192.168.1.1:20
Loopback	127.0.0.1
IP addresses of the interface	4 IP addresses
Header	• Checksum • Variable length • Fragmentation in the header • No security
Fragmentation	Host and router
Quality of service	Type of Service (ToS) for prioritization
Types of frame	Broadcast, multicast, unicast
Identification of DHCP clients/server	Client ID: • MAC address • DHCP client ID • System name • PROFINET station name • IAID and DUID
DHCP	via UDP with broadcast
Resolution of IP addresses in hardware addresses	ARP (Address Resolution Protocol)

3.1.3 IPv4 address

3.1.3.1 Structure of an IPv4 address

The IPv4 address consists of 4 decimal numbers separated by a dot. Each decimal number can have a value from 0 to 255.

Example: 192.168.16.2

The IPv4 address is composed of:

- Address of the (sub)network
- The address of the node (generally also called end node, host or network node)

Subnet mask

The subnet mask consists of four decimal numbers with the range from 0 to 255, each number separated by a period; example: 255.255.0.0

The binary representation of the 4 subnet mask decimal numbers must contain a series of consecutive 1s from the left and a series of consecutive 0s from the right.

The "1" values determine the network address within the IPv4 address. The "0" values determine the device address within the IPv4 address.

Example:

Correct values

255.255.0.0 D = 1111 1111.1111 1111.0000 0000.0000 0000 B

255.255.128.0 D = 1111 1111.1111 1111.1000 0000.0000 0000 B

255.254.0.0 D = 1111 1111.1111 1110.0000 0000.0000.0000 B

Incorrect value:

255.255.1.0 D = 1111 1111.1111 1111.0000 0001.0000 0000 B

In the example for the IP address mentioned above, the subnet mask shown here has the following meaning:

The first 2 bytes of the IP address determine the subnet - i.e. 192.168. The last two bytes address the device, i.e. 16.2.

The following applies in general:

- The network address results from the AND combination of IPv4 address and subnet mask.
- The device address results from the AND-NOT combination of IPv4 address and subnet mask.

Classless Inter-Domain Routing (CIDR)

CIDR is a method that groups several IPv4 addresses into an address range by representing an IPv4 address combined with its subnet mask. To do this, a suffix is appended to the IPv4 address that specifies the number of bits of the network mask set to 1. Using the CIDR notation, routing tables can be reduced in size and the available address ranges put to better use.

Example:

IPv4 address 192.168.0.0 with subnet mask 255.255.255.0

The network part of the address covers 3 x 8 bits in binary representation; in other words 24 bits.

This results in the CIDR notation 192.168.0.0/24.
The host part covers 1 x 8 bits in binary notation. This results in an address range of 2 to the power 8, in other words 256 possible addresses.

Masking additional subnets

Using the subnet mask, you can further structure a subnet assigned to one of the address classes A, B or C and form "private" subnets by setting further lower-level digits of the subnet mask to "1". For each bit set to "1", the number of "private" networks doubles and the number of nodes contained in them is halved. Externally, the network still looks like a single network.

Example:

You change the default subnet mask for a subnet of address class B (e.g. IP address 129.80.xxx.xxx) as follows:

Masks	Decimal	Binary
Default subnet mask	255.255.0.0	11111111.11111111.00000000 .00000000
Subnet mask	255.255.128.0	11111111.11111111.10000000 .00000000

Result:

All devices with addresses from 129.80.1.xxx to 129.80.127.xxx are on one IP subnet, all devices with addresses from 129.80.128.xxx to 129.80.255.xxx are on another IP subnet.

Network gateway (router)

The task of the network gateways (routers) is to connect the IP subnets. If an IP datagram is to be sent to another network, it must first be sent to a router. For make this possible, you need to enter the router address for each member of the IP subnet.

The IP address of a device in the subnet and the IP address of the network gateway (router) may only be different at the points where the subnet mask is set to "0".

3.1.3.2 Initial assignment of an IPv4 address

Configuration options

An initial IP address for the device cannot be assigned using Web Based Management (WBM) because this configuration tool can only be used if an IP address already exists.

The following options are available to assign an IP address to an unconfigured device:

- **DHCP** (default)

  Note

  When the product ships and following "Restore Factory Defaults and Restart", DHCP is enabled. If a DHCP server is available in the local area network, and this responds to the DHCP request of a device, the IP address, subnet mask and gateway are assigned automatically when the device first starts up.

  Note

  DHCP on VLAN 2 must not be used for initial configuration.

  You will find the VLAN assignment set on the device in the factory in the section VLAN (Page 47).

- **SINEC PNI**
  - To be able to assign an IP address to the device with SINEC PNI, it must be possible to reach the device via Ethernet.
  - You can find SINEC PNI on the Internet pages of Siemens Industry Online Support: Link: (https://support.industry.siemens.com/cs/ww/en/ps/26672/dl)
  - For additional information about assigning the IP address with SINEC PNI, refer to the online help or the "SINEC PNI network management" operating instructions.
- **CLI** via the serial interface
  For further information on assigning the IP address using the CLI, refer to the configuration manual "SCALANCE SC-600 Command Line Interface (CLI)".

3.1.3.3 Address assignment with DHCP

Properties of DHCP

DHCP (Dynamic Host Configuration Protocol) is a method for automatic assignment of IP addresses. It has the following characteristics:

- DHCP can be used both when starting up a device and during ongoing operation.
- The assigned IP address remains valid only for a limited time known as the lease time. When half the period of validity has elapsed. the DHCP client can extend the period of the assigned IPv4 address. When the entire time has elapsed, the DHCP client needs to request a new IPv4 address.

- There is normally no fixed address assignment; in other words, when a client requests an IP address again, it normally receives a different address from the previous address. It is possible to configure the DHCP server so that the DHCP client always receives the same fixed address in response to its request. The parameter with which the DHCP client is identified for the fixed address assignment is set on the DHCP client. The address can be assigned via the MAC address, the DHCP client ID or the device name. You configure the parameter in "System > DHCP Client (Page 182)".
- The following DHCP options are supported:
  - DHCP option 1: Assignment of a subnet mask
  - DHCP option 3: Assignment of a router address
  - DHCP option 6: Assignment of a DNS server address
  - DHCP option 15: DNS domain name
  - DHCP option 12: Assignment of a host name
  - DHCP option 66: Assignment of a dynamic TFTP server name
  - DHCP option 67: Assignment of a dynamic boot file name

Note

DHCP uses a mechanism with which the IP address is assigned for only a short time (lease time). If the device does not reach the DHCP server with a new request on expiry of the lease time, the assigned IP address, the subnet mask and the gateway continue to be used.

The device therefore remains accessible under the last assigned IP address even without a DHCP server. This is not the standard behavior of office devices but is necessary for problem-free operation of the plant.

3.1.4 IPv6 address

3.1.4.1 IPv6 terms

Network node

A network node is a device that is connected to one or more networks via one or more interfaces.

Router

A network node that forwards IPv6 packets.

Host

A network node that represents an end point for IPv6 communication relations.

Link

A link is, according to IPv6 terminology, a direct layer 3 connection within an IPv6 network.

Neighbor

Two network nodes are called neighbors when they are located on the same link.

IPv6 interface

Physical or logical interface on which IPv6 is activated.

Path MTU

Maximum permitted packet size on a path from a sender to a recipient.

Path MTU discovery

Mechanism for determining the maximum permitted packet size along the entire path from a sender to a recipient.

LLA

Link local address FE80::/10

As soon as IPv6 is activated on the interface, a link local address is formed automatically. Can only be reached by nodes located on the same link.

ULA

Unique Local Address

Defined in RFC 4193. The IPv6 interface can be reached via this address in the LAN.

GUA

Global unicast address

The IPv6 interface can be reached through this address, for example, via the Internet.

Interface ID

The interface ID is formed with the EUI-64 method or manually.

EUI-64

Extended Unique Identifier (RFC 4291); process for forming the interface ID. In Ethernet, the interface ID is formed from the MAC address of the interface. Divides the MAC address into the manufacturer-specific part (OUI) and the network-specific part (NIC) and inserts FFFE between the two parts.

Example:

MAC address = AA:BB:CC:DD:EE:FF

OUI = AA:BB:CC

NIC = DD:EE:FF

EUI-64 = OUI + **FFFE** + NIC = AA:BB:CC:**FF:FE**:DD:EE:FF

Scope

Defines the range of the IPv6 address.

3.1.4.2 Structure of an IPv6 address

IPv6 address format - notation

IPv6 addresses consist of 8 fields each with four-character hexadecimal numbers (128 bits in total). The fields are separated by a colon.

Example:

fd00:0000:0000:ffff:02d1:7d01:0000:8f21

Rules / simplifications:

- If one or more fields have the value 0, a shortened notation is possible.
  The address fd00:**0000:0000**:ffff:02d1:7d01:0000:8f21 can also be shortened and written as follows:
  fd00**::**ffff:02d1:7d01:0000:8f21
  To ensure uniqueness, this shortened form can only be used once within the entire address.
- Leading zeros within a field can be omitted.
  The address fd00:0000:0000:ffff:**02d1**:7d01:0000:8f21 can also be shortened and written as follows:
  fd00**::**ffff:**2d1**:7d01:0000:8f21
- Decimal notation with periods
  The last 2 fields or 4 bytes can be written in the normal decimal notation with periods.
  Example: The IPv6 address fd00::ffff.125.1.0.1 is equivalent to fd00::ffff:7d01:1

Structure of the IPv6 address

The IPv6 protocol distinguishes between three types of address: Unicast, Anycast and Multicast. The following section describes the structure of the global unicast addresses.

IPv6 prefix		**Suffix**
Global prefix: n bits	Subnet ID m bits	Interface ID 128 - n - m bits
Assigned address range	Description of the location, also subnet prefix or subnet	Unique assignment of the host in the network. The ID is generated from the MAC address.

The prefix for the link local address is always fe80:0000:0000:0000. The prefix is shortened and noted as follows: fe80::

IPv6 prefix

Specified in: RFC 4291

The IPv6 prefix represents the subnet identifier.

Prefixes and IPv6 addresses are specified in the same way as with the CIDR notation (Classless Inter-Domain Routing) for IPv4.

Design

IPv6 address / prefix length

Example

IPv6 address: 2001:0db8:1234::1111/48

Prefix: 2001:0db8:1234::/48

Interface ID: ::1111

Entry and appearance

The entry of IPv6 addresses is possible in the notations described above. IPv6 addresses are always shown in the hexadecimal notation.

3.2 MAC address

Note on the structure of the MAC address:

MAC addresses are hardware addresses for identifying network nodes. A MAC address consists of six byes separated by hyphens in hexadecimal notation.

The MAC address consists of a fixed and a variable part. The fixed part ("basic MAC address") identifies the manufacturer (Siemens, 3COM, ...). The variable part of the MAC address distinguishes the various Ethernet nodes.

3.3 ICMP

The acronym ICMP stands for Internet Control Message Protocol (RFC792) and is used to exchange error and information messages.

- Error message
  Informs the sender of the IP frame that when forwarding the frame an error or a parameter problem occurred.
- Information message
  Can contain information about the time measurement, the address mask, the reachability of the destination or for finding the router.

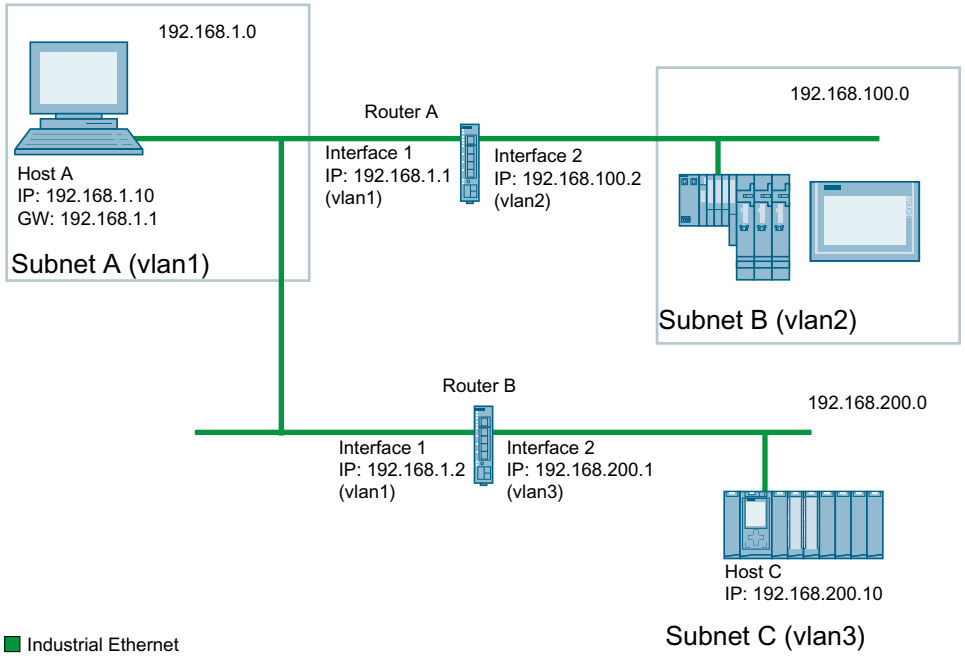
Structure of the ICMP data packet

0	4	8	12	16	20	24	28	31
ICMP packet type Type of message		Code Further details of the message		Checksum				
Data (optional)								

- **ICMP packet type**
  The most important ICMP packet types are as follows:
  - Redirect
    The router informs the host in one of its subnets that there is a better route to the destination. This ICMP packet type is dealt with in more detail in the following description.
  - Destination Unreachable
    IP frame cannot be delivered.
  - Time Exceeded
    Time limit exceeded
  - Echo-Request
    Echo request, better known as ping.
- **Code**
  The code describes the ICMP packet type in greater detail. The selection depends on the selected ICMP packet type. With "Destination Unreachable,", for example "Code 1" host cannot be reached.

You will find a full list of the ICMP packet types and codes on the website of IANA (http://www.iana.org/assignments/icmp-parameters).

ICMP packet type 5 - Redirect



Host A wants to send an IP frame to host C. Host C is not located in the same subnet as host A. For this reason host A sends the IP frame to its default gateway. The default gateway of host A is interface 1 of router A. Via its routing table, however, router A knows that subnet C is reachable via router B. Router B connects subnet A with subnet C. Router A sends a redirect message to host A. In this, router A instructs host A in future to send IP frames to host C via router B whose IP address is contained in the redirect message. The initial IP frame is sent by router A directly to router B that forwards it to Host C.

Conditions for sending redirect messages

- The IP frame is received and sent via the same interface of router A.
- The source IP address (host A) is from the same subnet as the next hop address (router B) in the routing table.
- The IP frame is not affected by a source NAT rule (masquerading, source NAT or NETMAP).
- So that router A forwards the initial IP frame to router B, a firewall rule vlanX → vlanX is required.

3.4 VLAN

Network definition regardless of the spatial location of the nodes

VLAN (Virtual Local Area Network) divides a physical network into several logical networks that are shielded from each other. Here, devices are grouped together to form logical groups. Only nodes of the same VLAN can address each other. Since multicast and broadcast frames are only forwarded within the particular VLAN, they are also known as broadcast domains.

The particular advantage of VLANs is the reduced network load for the nodes and network segments of other VLANs.

To identify which packet belongs to which VLAN, the frame is expanded by 4 bytes, refer to VLAN tagging (Page 48). This expansion includes not only the VLAN ID but also priority information.

Options for the VLAN assignment

There are various options for the assignment to VLANs:

- Port-based VLAN
  Each port of a device is assigned a VLAN ID. You configure port-based VLAN in "Layer 2 > VLAN > Port-based VLAN (Page 265)".

VLAN assignment on the device

In the factory settings, the following assignments are made:

SCALANCE SC6x2-2C

P0.1	VLAN1 For access from the local network (LAN) to the device
P0.2	VLAN2 For access from the external network (WAN) to the device

SCALANCE SC6x6-2C

P0.1 - P0.4	VLAN1 For access from the local network (LAN) to the device
P0.5 - P0.6	VLAN2 For access from the external network (WAN) to the device

You can change the assignment in "Layer 2 > VLAN > General".

The VLANs are in different IP subnets. To allow these to communicate with each other, the route and firewall rule must be configured on the device.

3.4.1 VLAN tagging

Expansion of the Ethernet frames by four bytes

For CoS (Class of Service, frame priority) and VLAN (virtual network), the IEEE 802.1Q standard defined the expansion of Ethernet frames by adding the VLAN tag.

Note

The VLAN tag increases the permitted total length of the frame from 1518 to 1522 bytes. The end nodes on the networks must be checked to find out whether they can process this length / this frame type. If this is not the case, only frames of the standard length may be sent to these nodes.

The additional 4 bytes are located in the header of the Ethernet frame between the source address and the Ethernet type / length field:

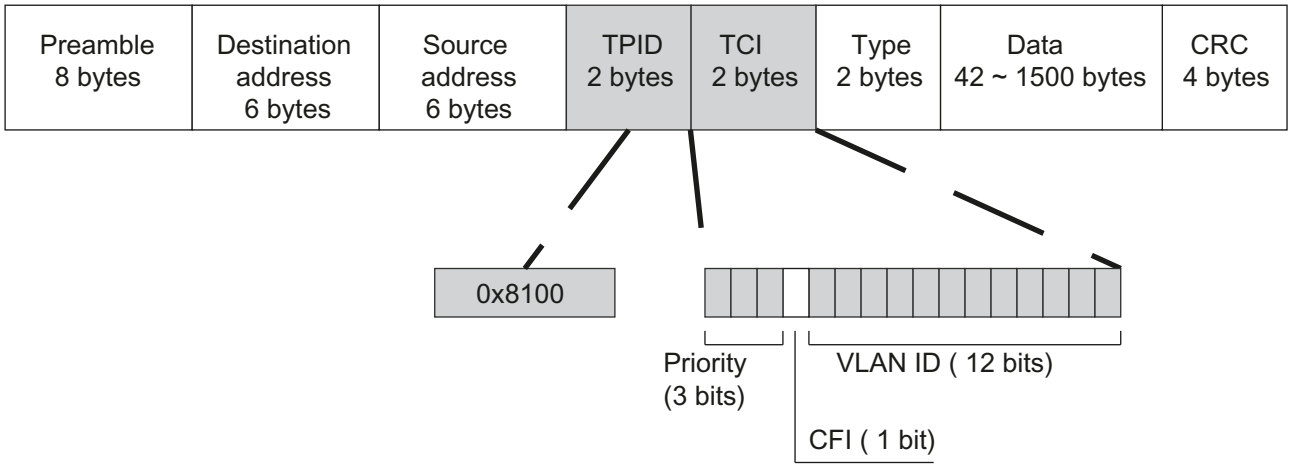


Figure 3-1 Structure of the expanded Ethernet frame

The additional bytes contain the tag protocol identifier (TPID) and the tag control information (TCI).

Tag protocol identifier (TPID)

The first 2 bytes form the Tag Protocol Identifier (TPID) and always have the value 0x8100. This value specifies that the data packet contains VLAN information or priority information.

Tag Control Information (TCI)

The 2 bytes of the Tag Control Information (TCI) contain the following information:

QoS Trust

The tagged frame has 3 bits for the priority that is also known as Class of Service (CoS), see also IEEE 802.1Q.

CoS bits	Priority	Type of the data traffic
000	0 (lowest)	Background
001	1	Best Effort
010	2	Excellent Effort
011	3	Critical Applications
100	4	Video, < 100 ms delay (latency and jitter)
101	5	Voice (language), < 10 ms delay (latency and jitter)
110	6	Internetwork Control
111	7 (highest)	Network Control

The prioritization of the data packets is possible only if there is a queue in the components in which they can buffer data packets with lower priority.

The device has multiple parallel queues in which the frames with different priorities can be processed. As default, first, the frames with the highest priority are processed. This method ensures that the frames with the highest priority are sent even if there is heavy data traffic.

Canonical Format Identifier (CFI)

The CFI is required for compatibility between Ethernet and the token Ring.
The values have the following meaning:

Value	Meaning
0	The format of the MAC address is canonical. In the canonical representation of the MAC address, the least significant bit is transferred first. Standard-setting for Ethernet switches.
1	The format of the MAC address is not canonical.

VLAN ID

In the 12-bit data field, up to 4096 VLAN IDs can be formed. The following conventions apply:

VLAN ID	Meaning
0	The frame contains only priority information (priority tagged frames) and no valid VLAN identifier.
1- 4094	Valid VLAN identifier, the frame is assigned to a VLAN and can also include priority information.
4095	Reserved

3.5 VXLAN

VXLAN (Virtual eXtensible LAN), like VLAN, divides a network into multiple logical networks. VXLAN forwards the Ethernet frame (Layer 2) through a tunnel via an IP network (Layer 3). The Ethernet frame is extended with a VXLAN header and then embedded in UDP.

VNI

The VNI (VXLAN Network Identifier) determines the VLAN to which a data packet belongs. The nodes with the same VXLAN identifier are in a virtual network.

3.6 Mirroring

The device provides the option of simultaneously channeling incoming or outgoing data streams via other interfaces for analysis or monitoring. This has no effect on the monitored data streams. This procedure is known as mirroring. In this menu section, you enable or disable mirroring and set the parameters.

Mirroring ports

Mirroring a port means that the data traffic at a port (mirrored port) of the IE switch is copied to another port (monitor port). You can mirror one or more ports to a monitor port.

If a protocol analyzer is connected to the monitor port, the data traffic at the mirrored port can be recorded without interrupting the connection. This means that the data traffic can be investigated without being affected. This is possible only if a free port is available on the device as the monitor port.

Note

Forwarding RSPAN stream

If the device is to forward RSPAN streams, two requirements must be met:

- Input port and output port must belong to the same port group.
- The "Learning" function must be disabled for the input port.
  In WBM: System > Ports > Configuration > Unicast MAC Learning
  In CLI: no unicast mac learning

3.7 SNMP

Introduction

With the aid of the Simple Network Management Protocol (SNMP), you monitor and control network components from a central station, for example routers or switches. SNMP controls the communication between the monitored devices and the monitoring station.

Tasks of SNMP:

- Monitoring of network components
- Remote control and remote parameter assignment of network components
- Error detection and error notification

In versions v1 and v2c, SNMP has no security mechanisms. Each user in the network can access data and also change parameter assignments using suitable software.

For the simple control of access rights without security aspects, community strings are used.

The community string is transferred along with the query. If the community string is correct, the SNMP agent responds and sends the requested data. If the community string is not correct, the SNMP agent discards the query. Define different community strings for read and write permissions. The community strings are transferred in plain text.

Standard values of the community strings:

- public
  has only read permissions
- private
  has read and write permissions

Note

Because the SNMP community strings are used for access protection, do not use the standard values "public" or "private". Change these values following the initial commissioning.

Further simple protection mechanisms at the device level:

- Allowed Host
  The IP addresses of the monitoring systems are known to the monitored system.
- Read Only
  If you assign "Read Only" to a monitored device, monitoring stations can only read out data but cannot modify it.

SNMP data packets in versions v1 and v2c are not encrypted and can easily be read by others.

The central station is also known as the management station. An SNMP agent is installed on the devices to be monitored with which the management station exchanges data.

The management station sends data packets of the following type:

- GET
  Request for a data record from the SNMP agent
- GETNEXT
  Calls up the next data record.

- GETBULK (available as of SNMPv2c)
  Requests multiple data records at one time, for example several rows of a table.
- SET
  Contains parameter assignment data for the relevant device.

The SNMP agent sends data packets of the following type:

- RESPONSE
  The SNMP agent returns the data requested by the manager.
- TRAP
  If a certain event occurs, the SNMP agent itself sends traps.

SNMPv1/v2c/v3 use UDP (User Datagram Protocol) and use the UDP ports 161 and 162. The data is described in a Management Information Base (MIB).

SNMPv3

Compared with the previous versions SNMPv1 and SNMPv2c, SNMPv3 introduces an extensive security concept.

SNMPv3 supports:

- Fully encrypted user authentication
- Encryption of the entire data traffic
- Access control of the MIB objects at the user/group level

With the introduction of SNMPv3 you can no longer transfer user configurations to other devices without taking special action, e.g. by loading a configuration file or replacing the C-PLUG.

According to the standard, the SNMPv3 protocol uses a unique SNMP engine ID as an internal identifier for an SNMP agent. This ID must be unique in the network. It is used to authenticate access data of SNMPv3 users and to encrypt it.

Depending on whether you have enabled or disabled the “SNMPv3 User Migration” function, the SNMP engine ID is generated differently.

Restriction when using the function

Use the "SNMPv3 User Migration" function only to transfer configured SNMPv3 users to a substitute device when replacing a device.
Do not use the function to transfer configured SNMPv3 users to multiple devices. If you load a configuration with created SNMPv3 users on several devices, these devices use the same SNMP engine ID. If you use these devices in the same network, your configuration contradicts the SNMP standard.

Compatibility with predecessor products

You can only transfer SNMPv3 users to a different device if you have created the users as migratable users. To create a migratable user the "SNMPv3 User Migration" function must be activated when you create the user.

3.8 Redundancy

3.8.1 HRP

HRP - High Speed Redundancy Protocol

HRP is the name of a redundancy method for networks with a ring topology. The devices are interconnected via ring ports. One of the devices is configured as the redundancy manager (RM). The other devices are redundancy clients. Using test frames, the redundancy manager checks the ring to make sure it is not interrupted. The redundancy manager sends test frames via the ring ports and checks that they are received at the other ring port. The redundancy clients forward the test frames.

If the test frames of the RM no longer arrive at the other ring port due to an interruption, the RM switches through its two ring ports and informs the redundancy clients of the change immediately. The reconfiguration time after an interruption of the ring is a maximum of 300 ms.

Requirements

HRP

- HRP is supported in ring topologies with up to 50 devices.
  Exceeding this number of devices can lead to a loss of data traffic.
- For HRP, only devices that support this function can be used in the ring.
- Devices that do not support HRP must be linked to the ring using special devices with HRP capability. Up to the ring, this connection is not redundant.
- All devices must be interconnected via their ring ports. Multimode connections up to 3 km and single mode connections up to 26 km between two IE switches are possible. At greater distances, the specified reconfiguration time may be longer.
- A device in the ring must be configured as redundancy manager by selecting the "HRP manager" setting. On all other devices in the ring, the "HRP Client" mode must be activated.
- The standby ports must be disabled in spanning tree.
- You configure HRP in Web Based Management, Command Line Interface or using SNMP.
- With standby coupling partners HRP must be set permanently.
- The ports of the standby coupling partners must be disabled in spanning tree.
- You configure standby redundancy in Web Based Management, Command Line Interface or using SNMP.

Example for configuration

You can find an example for configuration of HRP rings with standby coupling on the Internet pages of Siemens Industry Online Support.

Link: (https://support.industry.siemens.com/cs/ww/en/view/109739600)

3.8.2 MRP

The "MRP" method conforms to the Media Redundancy Protocol (MRP) specified in the following standard:

IEC 62439-2 Release 1.0 (2010-02) Industrial communication networks - High availability automation networks Part 2: Media Redundancy Protocol (MRP)

The reconfiguration time after an interruption of the ring is a maximum of 200 ms.

Topology

The following figure shows a possible topology for devices in a ring with MRP.

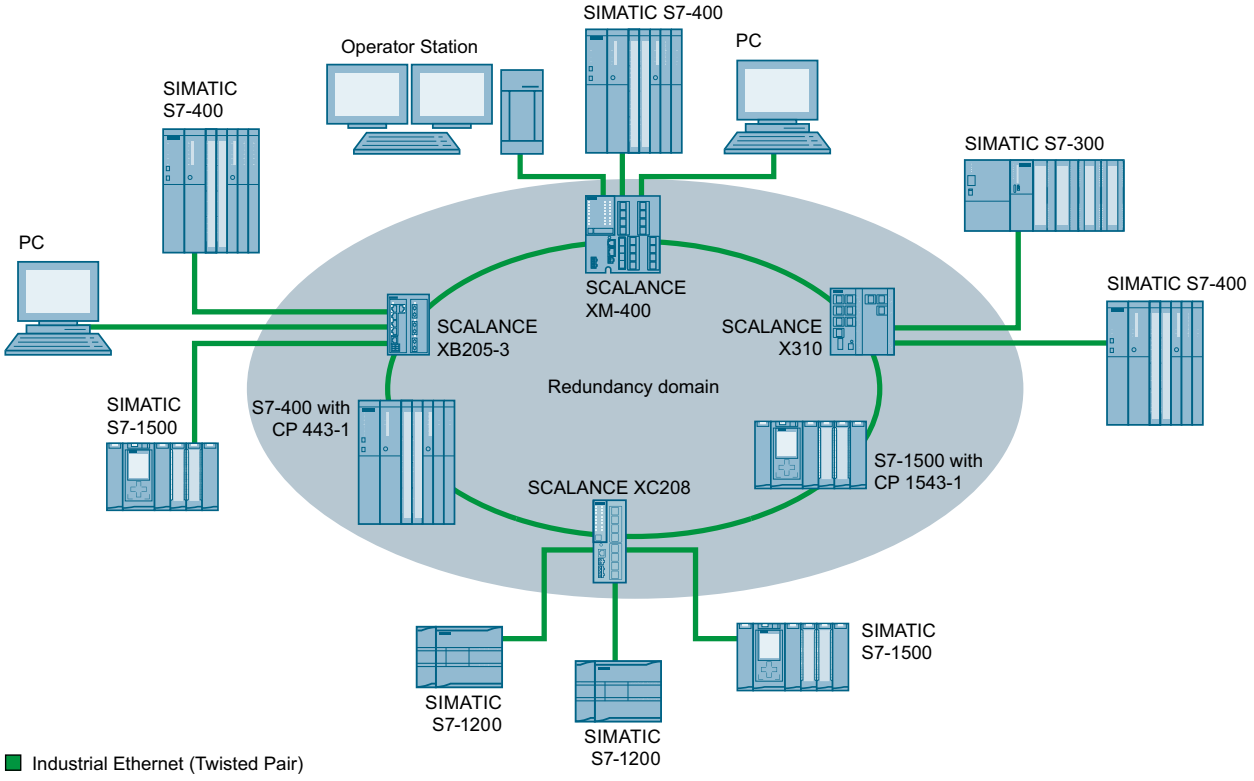


Figure 3-2 Example of a ring topology with the MRP media redundancy protocol

The following rules apply to a ring topology with media redundancy using MRP:

- All the devices connected within the ring topology are members of the same redundancy domain.
- One device in the ring is acting as redundancy manager.
- All other devices in the ring are redundancy clients.

Non MRP-compliant devices can be connected to the ring via a SCALANCE X switch or via a PC with a CP capable of MRP.

Requirements

The requirements for problem-free operation with the MRP media redundancy protocol are as follows:

- MRP is supported in ring topologies with up to 50 devices.
  Exceeding this number of devices can lead to a loss of data traffic.
- The ring in which you want to use MRP may only consist of devices that support this function. These include, for example, some of the Industrial Ethernet SCALANCE X switches, some of the communications processors (CPs) for SIMATIC S7 and PG/PC, and non-Siemens devices that support this function.
- All devices must be interconnected via their ring ports.
  Multimode connections up to 3 km and single mode connections up to 26 km between two SCALANCE X IE switches are possible. At greater distances, the specified reconfiguration time may be longer.
- "MRP" must be enabled for all devices in the ring.
- The connection settings (transmission medium / duplex) must be set to full duplex and at least 100 Mbps for all ring ports. Otherwise there may be a loss of data traffic.
  - STEP 7: Set all the ports involved in the ring to "Automatic settings" in the "Options" tab of the properties dialog.
  - WBM: If you configure with Web Based Management, the ring ports are set automatically to autonegotiation.

Example for configuration

You can find an example for configuration of a ring topology based on "MRP" on the Internet pages of Siemens Industry Online Support.

Link: (https://support.industry.siemens.com/cs/ww/en/view/109739614)

3.8.3 Spanning Tree

Avoiding loops on redundant connections

The spanning tree algorithm allows network structures to be created in which there are several connections between two IE switches / bridges. Spanning tree prevents loops being formed in the network by allowing only one path and disabling the other (redundant) ports for data traffic. If there is an interruption, the data can be sent over an alternative path. The functionality of the spanning tree algorithm is based on the exchange of configuration and topology change frames.

Definition of the network topology using the configuration frames

The devices exchange configuration frames known as BPDUs (Bridge Protocol Data Units) with each other to calculate the topology. The root bridge is selected and the network topology created using these frames. BPDUs also bring about the status change of the root ports.

The root bridge is the bridge that controls the spanning tree algorithm for all involved components.

Once the root bridge has been specified, each device sets a root port. The root port is the port with the lowest path costs to the root bridge.

Response to changes in the network topology

If nodes are added to a network or drop out of the network, this can affect the optimum path selection for data packets. To be able to respond to such changes, the root bridge sends configuration messages at regular intervals. The interval between two configuration messages can be set with the "Hello Time" parameter.

Keeping configuration information up to date

With the "Max Age" parameter, you set the maximum age of configuration information. If a bridge has information that is older than the time set in "Max Age", it discards the message and initiates recalculation of the paths.

New configuration data is not used immediately by a bridge but only after the period specified in the "Forward Delay" parameter. This ensures that operation is only started with the new topology after all the bridges have the required information.

3.8.4 RSTP

Rapid Spanning Tree Protocol (RSTP)

One disadvantage of STP is that if there is a disruption or a device fails, the network needs to reconfigure itself: The devices start to negotiate new paths only when the interruption occurs. This can take up to 30 seconds. Fur this reason, STP was expanded to create the "Rapid Spanning Tree Protocol" (RSTP, IEEE 802.1w). This differs from STP essentially in that the devices are already collecting information about alternative routes during normal operation and do not need to gather this information after a disruption has occurred. This means that the reconfiguration time for an RSTP controlled network can be reduced to a few seconds.
This is achieved by using the following functions:

- Edge ports (end node port)
  Edge ports are ports connected to an end device.
  A port that is defined as an edge port is activated immediately after connection establishment. If a spanning tree BPDU is received at an edge port, the port loses its role as edge port and it takes part in (R)STP again. If no further BPDU is received after a certain time has elapsed (3 x hello time), the port returns to the edge port status.
- Point-to-point (direct communication between two neighboring devices)

  By directly linking the devices, a status change (reconfiguration of the ports) can be made without any delays.

- Alternate port (substitute for the root port)

  A substitute for the root port is configured. If the connection to the root bridge is lost, the device can establish a connection over the alternate port without any delay due to reconfiguration.

- Reaction to events

  Rapid spanning tree reacts to events, for example an aborted connection, without delay. There is no waiting for timers as in spanning tree.

- Counter for the maximum bridge hops
  The number of bridge hops a package is allowed to make before it automatically becomes invalid.
  In principle, therefore with rapid spanning tree, alternatives for many parameters are preconfigured and certain properties of the network structure taken into account to reduce the reconfiguration time.

Example for configuration

You can find an example for configuration of a mesh network based on "RSTP" on the Internet pages of Siemens Industry Online Support.

Link: (https://support.industry.siemens.com/cs/ww/en/view/109742120)

3.9 Routing function

3.9.1 Routing

Introduction

The term routing describes the specification of routes for communication between different networks; in other words, how does a data packet from subnet A get to subnet B.

SCALANCE SC-600 supports the following routing functions:

- Static routing
  With static routing, the routes are entered manually in the routing table.
- Router redundancy
  With standardized VRRP (Virtual Router Redundancy Protocol), the availability of important gateways is increased by redundant routers.
  - VRRPv2
  - VRRPv3

3.9.2 VRRPv3

Router redundancy with VRRPv3

With the Virtual Router Redundancy Protocol v3 (VRRPv3), the failure of a router in a network can be countered. Version 3 of VRRP (RFC 5798) is based on version 2 (RFC 5798).

VRRP can only be used with virtual IP interfaces (VLAN interfaces).

Several VRRP routers in a network segment are put together as a logical group representing a virtual router (VR). The group is defined using the virtual ID (VRID). Within the group, the VRID must be the same. The VRID can no longer be used for other groups in the same L2/Ethernet segment.

The virtual router is assigned a virtual IP address and a virtual MAC address. One of the VRRP routers within the group is specified as the master router. The other VRRP routers are backup routers. The master router assigns the virtual IP address and the virtual MAC address to its network interface. The master router sends VRRP packets (advertisements) to the backup routers at specific intervals. With the VRRP packets, the master router signals that it is still functioning. The master router also replies to the ARP queries to the virtual address.

If the virtual master router fails, a backup router takes over the role of the master router. The backup router with the highest priority becomes the master router. If the priority of the backup routers is the same, the higher MAC address decides. The backup router becomes the new virtual master router.

The new virtual master router adopts the virtual MAC and IP address. This means that no routing tables or ARP tables need to be updated. The consequences of a device failure are therefore minimized.

You configure VRRP in "Layer 3 > VRRPv3".

3.9.3 Static routing

The route is entered manually in the routing table. Enter the route in the routing table on the following page.

- Layer 3 > Static Routes

3.10 Security functions

3.10.1 Adapting the MTU for IPsec VPN and SINEMA RC

Adapting the MTU (Maximum Transmission Unit)

The MTU specifies the permitted size of a data packet for transmission in the network. When these data packets are then transferred from the device via the IPsec tunnel or SINEMA RC, the original data packet becomes larger as a result of the additional header information and may need to be segmented for further transfer. This depends on the MTU specifications in the connected network. However, a necessary segmentation may lead to noticeable losses in performance or cancelation of the data transfer.

Avoid this by adapting the MTU format on the terminal device, which means reducing it in such a way that the data packets received by the device can be supplemented by the required additional information without the need for subsequent segmentation. A reasonable size is in the range of between 1000 and 1400 bytes.

3.10.2 User management

Overview of user management

Access to the device is managed by configurable user settings. Set up users with a password for authentication. Assign a role with suitable rights to the users.

The authentication of users can either be performed locally by the device or by an external RADIUS server. You configure how the authentication is handled on the "Security > AAA > General" page.

Local logon

The local logging on of users by the device runs as follows:

1. The user logs on with user name and password on the device.
2. The device checks whether an entry exists for the user.
   → If an entry exists, the user is logged in with the rights of the associated role.
   → If no corresponding entry exists, the user is denied access.

Login via an external RADIUS server

RADIUS (Remote Authentication Dial-In User Service) is a protocol for authenticating and authorizing users by servers on which user data can be stored centrally.

Depending on the RADIUS authorization mode you have selected on the "Security > AAA > RADIUS Client" page, the device evaluates different information of the RADIUS server.

RADIUS authorization mode "Standard"

If you have set the authorization mode "conventional", the authentication of users via a RADIUS server runs as follows:

1. The user logs on with user name and password on the device.
2. The device sends an authentication request with the login data to the RADIUS server.
3. The RADIUS server runs a check and signals the result back to the device.
   - The RADIUS server reports a successful authentication and returns the value "Administrative User" to the device for the attribute "Service Type".
     → The user is logged in with administrator rights.
   - The RADIUS server reports a successful authentication and returns a different or even no value to the device for the attribute "Service Type".
     → The user is logged in with read rights.
   - The RADIUS server reports a failed authentication to the device:
     → The user is denied access.

RADIUS authorization mode "SiemensVSA"

Requirement

For the RADIUS authorization mode "Siemens VSA" the following needs to be set on the RADIUS server:

- Manufacturer code: 4196
- Attribute number: 1
- Attribute format: Character string (group name)

Procedure

If you have set the authorization mode "SiemensVSA", the authentication of users via a RADIUS server runs as follows:

1. The user logs on with user name and password on the device.
2. The device sends an authentication request with the login data to the RADIUS server.
3. The RADIUS server runs a check and signals the result back to the device.
   Case A: The RADIUS server reports a successful authentication and returns the group assigned to the user to the device.
   - The group is known on the device and the user is not entered in the table "External User Accounts"
     → The user is logged in with the rights of the assigned group.
   - The group is known on the device and the user is entered in the table "External User Accounts"
     → The user is assigned the role with the higher rights and logged in with these rights.
   - The group is not known on the device and the user is entered in the table "External User Accounts"
     → The user is logged in with the rights of the role linked to the user account.
   - The group is not known on the device and the user is not entered in the table "External User Accounts"
     → The user is logged in with the rights of the role "Default".

   Case B: The RADIUS server reports a successful authentication but does not return a group to the device.
   - The user is entered in the table "External User Accounts":
     → The user is logged in with the rights of the linked role "".
   - The user is not entered in the table "External User Accounts":
     → The user is logged in with the rights of the role "Default".

   Case C: The RADIUS server reports a failed authentication to the device:
   - The user is denied access.

3.10.3 Firewall

3.10.3.1 Firewall rules SC600

Firewall rules are automatically created, predefined or specially configured IP rules for data traffic.

Automatic firewall rules

The "Auto firewall rules" setting is available for the following functions:

- System > SINEMA RC
- Security > IPsec VPN> Phase 2
- Security > OpenVPN Client > Connections

The automatically created firewall rules allow packets in the following direction:

From	To	SINEMA RC	IPsec VPN	OpenVPN
Internal	External	✓	✓	✓
External	Internal	✓	✓	✓
Device	External	--	--	✓
External	Device	Predefined IPv4 rules When the connection is created, the following IPv4 services are enabled:		
		HTTP HTTPS SSH Ping	Ping	Ping

Predefined firewall rules

The firewall contains predefined IPv4 rules that enable specific IPv4 services on the device.

Specify the interface via which access takes place under "Security > Firewall > Predefined IPv4".

The following options are available:

- VLANx: VLANs with configured subnet
- VPN connection: SINEMA RC, IPsec and OpenVPN

Factory setting

The firewall is enabled by default. In the delivery state (factory setting), the configuration of the predefined IPv4 rules is as follows:

Service	Access	
	Local access (vlan1) to the device [1)]	External access (vlan2) to the device
DHCP	✓	✓ For the DHCP client function
DNS	✓	--
HTTP	✓ Is rerouted to HTTPS	--
HTTPS	✓	--
IPsec VPN	--	✓
Ping	✓	--
SNMP	✓	--
SSH	✓	--
System time	--	--
Telnet	✓	--
VRRP	--	--

The security functions of the device include a stateful inspection firewall. This is a method of packet filtering or packet checking.

The IP packets are checked based on firewall rules in which the following is specified:

- The permitted protocols
- IP addresses and ports of the permitted sources
- IP addresses and ports of the permitted destinations

If an IP packet fits the specified parameters, it is allowed to pass through the firewall. The rules also specify what is done with IP packets that are not allowed to pass through the firewall.

Simple packet filter techniques require two firewall rules per connection.

- One rule for the query direction from the source to the destination.
- A second rule for the response direction from the destination to the source

Stateful Inspection Firewall

You only need to specify one firewall rule for the query direction from the source to the destination. The second rule is added implicitly. The packet filter recognizes when, for example, computer "A" is communicating with computer "B" and only then does it allow replies. A query by computer "B" is therefore not possible without a prior request by computer "A".

You configure the firewall in "Security > Firewall".

Note

IP packets via layer 2 (within the same VLAN)

If the IP packets from the device are sent via a switch port (layer 2), these IP packets are not checked based on firewall rules. The firewall has no effect on packets forwarded at the layer 2 level.

Communication directions

from	to	Meaning
vlan x	vlan x	Access from IP subnet vlan x to IP subnet vlan x. Example: vlan1 (INT) → vlan2 (EXT) Access from the local IP subnet to the external IP subnet.
	Device	Access from the IP subnet to the device.
	SINEMA RC	Access from the IP subnet to the SINEMA RC connection.
	IPsec (all) IPsec <Connection Name>	Access from the IP subnet to the VPN tunnel partners that can be reached via all VPN connections (all) or via a certain VPN connection <Connection Name>.
Device	vlan x	Access from the device to the IP subnet.
	SINEMA RC	Access from the device to the SINEMA RC connection.
	IPsec (all) IPsec <Connection Name>	Access from the device to the VPN tunnel partners that can be reached via all VPN connections(all) or via a certain VPN connection (<Connection Name>).

from	to	Meaning
SINEMA RC	vlan x	Access from SINEMA RC connections to the IP subnet.
	Device	Access from SINEMA RC connections to the device.
	IPsec (all) IPsec <Connection Name>	Access from the SINEMA RC server to the tunnel partners that can be reached via all VPN connections (all) or via a certain VPN connection <Connection Name>.
IPsec (all) IPsec <Connection Name>	vlan x	Access via VPN tunnel partners to the IP subnet.
	Device	Access via VPN tunnel partners to the device.
	SINEMA RC	Access via VPN tunnel partners to the SINEMA RC connection.

Firewall factory setting

Service	Access	
	from internal (vlan1) to the device	from external (vlan2) to the device
HTTP	yes, is rerouted to HTTPS	No
HTTPS	yes	No
DNS	yes	No
SNMP	yes	No
IPsec VPN	No	yes
SSH	yes	No
DHCP	yes	yes (for the DHCP client function)
Ping	yes	No
System time	yes	No
VRRP	No	No

3.10.4 NAT

NAT (Network Address Translation) is a method of translating IP addresses in data packets. With this, two different networks (internal and external) can be connected together.

A distinction is made between source NAT in which the source IP address is translated and destination NAT in which the destination IP address is translated.

You will find information on NAT scenarios that are implemented with the device at the following address: (https://support.industry.siemens.com/cs/en/view/109744660)

IP masquerading

IP masquerading is a simplified source NAT. With each outgoing data packet sent via this interface, the source IP address is replaced by the IP address of the interface. The adapted data packet is sent to the destination IP address. For the destination host it appears as if the queries always came from the same sender. The internal nodes cannot be reached directly from the external network. By using NAPT, the services of the internal nodes can be made reachable via the external IP address of the device.

IP masquerading can be used if the internal IP addresses cannot or should not be forwarded externally, for example because the internal network structure should remain hidden.

You configure masquerading in "Layer 3" > "NAT" > "IP Masquerading (Page 334)".

NAPT

NAPT (Network Address and Port Translation) is a form of destination NAT and is often called port forwarding. This allows the services of the internal nodes to be reached from external that are hidden by IP masquerading or source NAT.

Incoming data packets are translated that come from the external network and are intended for an external IP address of the device (destination IP address). The destination IP address is replaced by the IP address of the internal node. In addition to address translation, port translation is also possible.

The options are available for port translation:

from	to	Response
a single port	the same port	If the ports are the same, the frames will be forwarded without port translation.
a single port	a single port	The frames are translated to the port.
a port range	a single port	The frames from the port range are translated to the same port (n:1).
a port range	the same port range	If the port ranges are the same, the frames will be forwarded without port translation.

Port forwarding can be used to allow external nodes access to certain services of the internal network e.g. FTP, HTTP.

You configure NAPT in "Layer 3" > "NAT" > "NAPT (Page 335)".

Source NAT

As with masquerading, in source NAT the source address is translated. In addition to this, the outgoing data packets can be restricted. These include limitation to certain IP addresses or IP address ranges and limitation to certain interfaces.

Source NAT can be used if the internal IP addresses cannot or should not be forwarded externally, for example because a private address range such as 192.168.x.x is used.

You configure source NAT in "Layer 3" > "NAT" > "Source NAT (Page 336)".

NETMAP

With NETMAP it is possible to translate complex subnets to a different subnet. In this translation, the subnet part of the IP address is changed and the host part remains. For translation with NETMAP only one rule is required. NETMAP can translate both the source IP address and the destination IP address. To perform the translation with destination NAT and source NAT, numerous rules would be necessary. NETMAP can also be applied to VPN connections.

You configure NETMAP in "Layer 3" > "NAT" > "NETMAP (Page 338)".

3.10.5 NAT and firewall

The firewall and NAT router support the "Stateful Inspection" mechanism. If the IP data traffic from internal to external is enabled, internal notes can initiate a communications connection into the external network.

The reply frames from the external network can pass through the NAT router and firewall without it being necessary for their addresses to be included extra in the firewall rule and the NAT address translation. Frames that are not a reply to a query from the internal network are discarded without a matching firewall rule.

NAT translation and firewall rules

You will find an example of NAT translations on the Internet pages of Siemens Industry Online Support.

Link: (https://support.industry.siemens.com/cs/ww/en/view/109744660)

3.10.6 Certificates

Certificate types

The device uses different certificates to authenticate the various nodes.

Certificate		Is used in...
CA certificate	The CA certificate is a certificate issued by a Certificate Authority from which the server, device and partner certificates are derived. To allow a certificate to be derived, the CA certificate has a private key signed by the certificate authority. The key exchange between the device and the VPN gateway of the partner takes place automatically when establishing the connection. No manual exchange of key files is necessary.	IPsec VPN (Page 403)
Server certificate	Server certificates are required to establish secure communication (e.g. HTTPS, VPN...) between the device and another network participant. The server certificate is an encrypted SSL certificate. The server certificate is derived from the oldest valid CA, even if this is "out of service". The crucial thing is the validity date of the CA.	SINEMA RC
Device certificate	Certificates with the private key (key file) with which the device identifies itself.	IPsec VPN (Page 403)
Partner certificate	Certificates with which the VPN gateway of the partner identifies itself with the device.	IPsec VPN (Page 403)

File types

File type	Description
*.crt	File that contains the certificate.
*.p12	In the PKCS12 certificate file, the private key is stored with the corresponding certificate and is password protected. The CA creates a certificate file (PKCS12) for both ends of a VPN connection with the file extension ".p12". This certificate file contains the public and private key of the local station, the signed certificate of the CA and the public key of the CA.
*.pem	Certificate and key as Base64-coded ASCII text.

3.10.7 VPN

The device supports the following VPN systems:

- IPsec VPN (SC64x-2C)
- OpenVPN

3.10.7.1 IPsec VPN

You configure the IPsec connections in "Security" > " IPsec VPN".

With IPsec VPN, the frames are transferred in tunnel mode. To allow the device to establish a VPN tunnel, the remote network must have a VPN gateway as the partner.

For the VPN connections, the device distinguishes two modes:

- **Roadwarrior mode**
  In this mode, the address of the partner is either entered manually or "any" is selected. If you select "any" a connection establishment from every address is accepted. The device learns the reachable remote subnets from the partner.
- **Standard mode**
  In this mode the address of the partner and the remote subnet is entered permanently. The device can either establish the connection actively as a VPN client or wait passively for connection establishment by the partner.

The IPsec method

The device uses the IPsec method in the tunnel mode for the VPN tunnel. Here, the frames to be transferred are completely encrypted and provided with a new header before they are sent to the VPN gateway of the partner. The frames received by the partner are decrypted and forwarded to the receiver.

To provide security, the IPsec protocol suite uses various protocols:

- The Encapsulation Security Payload (**ESP**) encrypts the data.
- The Security Association (**SA**) contains the specifications negotiated between the partners, e.g. about the lifetime of the key, the encryption algorithm, the period for new authentication etc.
- Internet Key Exchange (**IKE**) is a key exchange method. The key exchange takes place in two phases:
  - Phase 1
    In this phase, no security services such as encryption, authentication and integrity checks are available yet since the required keys and the IPsec SA still need to be created. Phase 1 serves to establish a secure VPN tunnel for phase 2. To achieve this, the communications partners negotiate an ISAKMP Security Association (ISAKMP SA) that defines the required security services (algorithms, authentication methods used). The subsequent messages and phase 2 are therefore secure.
  - Phase 2
    Phase 2 serves to negotiate the required IPsec SA. Similar to phase 1, exchanging offers achieves agreement about the authentication methods, the algorithms and the encryption method to protect the IP packets with IPsec AH and IPsec ESP.
    The exchange of messages is protected by the ISAKMP SA negotiated in phase 1. Due to the ISAKMP SA negotiated in phase 1, the identity of the nodes is known and the method for the integrity check already exists.

Authentication method

- CA certificate, device and partner certificate (digital signatures)
  The use of certificates is an asymmetrical cryptographic system in which every node (device) has a pair of keys. Each node has a secret, private key and a public key of the partner. The private key allows the device to authenticate itself and to generate digital signatures.
- Pre-shared key
  The use of a pre-shared key is a symmetrical cryptographic system. Each node has only one secret key for decryption and encryption of data packets. The authentication is via a common password.

Local ID and remote ID

The local ID and the remote ID are used by IPsec to uniquely identify the partners (VPN end point) during establishment of a VPN connection.

Encryption methods

The following encryption methods are supported. The selection depends on the phase und the key exchange method (IKE)

	Phase 1		Phase 2	
	IKEv1	**IKEv2**	**IKEv1**	**IKEv2**
3DES	x	x	x	x
AES128 CBC	x	x	x	x

	Phase 1		Phase 2	
	IKEv1	**IKEv2**	**IKEv1**	**IKEv2**
AES192 CBC	x	x	x	x
AES256 CBC	x	x	x	x
AES128 CTR	-	x	x	x
AES192 CTR	-	x	x	x
AES256 CTR	-	x	x	x
AES128 CCM 16	-	x	x	x
AES192 CCM 16	-	x	x	x
AES256 CCM 16	-	x	x	x
AES128 GCM 16	-	x	x	x
AES192 GCM 16	-	x	x	x
AES256 GCM 16	-	x	x	x

x: is supported

-: is not supported

Default Ciphers

During connection establishment a preset list can be transferred to the VPN connection partners. The list contains combinations of the three algorithms (Encryption, Authentication, Key Derivation). To establish a VPN connection, the VPN connection partner must support at least one of these combinations. The combinations depend on the phase und the key exchange method (IKE).

Combination			Phase 1		Phase 2	
Encryption	**Authentica-tion**	**Key derivation**	**IKEv1**	**IKEv2**	**IKEv1**	**IKEv2**
AES128	SHA1	DH Group 14	x	x	x	x
AES256	SHA512	DH Group 16	x	x	x	x
AES128 CCM 16	SHA256	DH Group 14	-	x	x	x
AES256 CCM 16	SHA512	DH Group 16	-	x	x	x
AES128	SHA1	none	-	-	x	x
AES256	SHA512	none	-	-	x	x
AES128 CCM 16	SHA256	none	-	-	x	x
AES256 CCM 16	SHA512	none	-	-	x	x

x: Combination is part of the default cipher

-: Combination is not part of the default cipher

none: For phase 2, no separate keys are exchanged. This means that Perfect Forward Secrecy (PFS) is disabled.

Requirements of the VPN partner

The VPN partner must support IPsec with the following configuration to be able to establish an IPsec connection successfully:

- Authentication with partner certificate, CA certificates or pre-shared key
- IKEv1 or IKEv2
- Support of at least one of the following DH groups: Diffie-Hellman group 1, 2, 5 and 14 - 18
- 3DES or AES encryption
- MD5, SHA1, SHA256, SHA384 or SHA512
- Tunnel mode

If the VPN partner is downstream from a NAT router, the partner must support NAT-T. Or, the NAT router must know the IPsec protocol (IPsec/VPN passthrough).

NAT traversal (NAT-T)

There may be a NAT router between the device and the VPN gateway of the remote network. Not all NAT routers allow IPsec frames to pass through. This means that it may be necessary to encapsulate the IPsec frames in UDP packets to be able to pass through the NAT router.

Dead peer detection

This is only possible when the VPN partner supports DPD. DPD checks whether the connection is still operating problem free or whether there has been an interruption on the line. Without DPD and depending on the configuration, it may be necessary to wait until the SA lifetime has expired or the connection must be reinitiated manually. To check whether the IPsec connection is still problem-free, the device itself sends DPD queries to the VPN partner station. If the VPN partner station does not reply after a certain time has elapsed, the connection to the VPN partner station will be declared invalid. You configure the settings for DPD in phase 1.

3.10.7.2 OpenVPN

With OpenVPN, virtual private networks (VPN) can be established. As an OpenVPN client, the device can establish a VPN connection to a remote network.

You configure the OpenVPN client under "Security" > "OpenVPN (Page 410)".

The VPN connection is established via virtual device drivers, the TAP and TUN device. During this, virtual network interfaces are created that act like a physical interface of the device and represent the endpoint of the VPN tunnel.

The device supports the following:

- TUN device: Routing mode
  The LAN Interface and the virtual network interface are located in different IP subnets. The virtual tunnel interface is assigned a virtual IP address from a devised subnet by the OpenVPN server. The IP packets (layer 3) are routed between the virtual tunnel interface and the LAN interface.
- TAP device: Bridge Mode
  For operation in flat networks. External and internal interface are in the same IP subnet.

Authentication method

- Certificates: CA certificate and device certificate
  The use of certificates is an asymmetrical cryptographic system. Each node (device) has a secret, private key and a public key of the partner. The private key allows the device to authenticate itself and to generate digital signatures.
- User name / Password
  Access is restricted by a user name and a password.

Encryption methods

The device also supports the following methods:

- BF CBC
- AES128 CBC
- AES192 CBC
- AES256 CBC
- DES EDE3

3.10.7.3 VPN connection establishment

The device supports the following options for establishing a VPN connection.

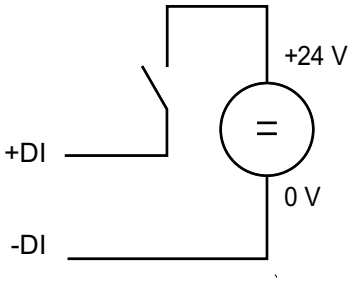
- IPsec VPN: Security > IPsec VPN > Connections (Page 401)
- OpenVPN: Security > OpenVPN > Connections
- SINEMA RC: System > SINEMA RC (Page 249)

Options	Use			Description
	IPsec VPN	OpenVPN	SINEMA RC	
start	x	x	-	The device is "active", in other words, it attempts to establish a connection to a partner. The partner is addressed using its configured WAN IP address or the configured FQDN.
wait	x	-	-	The device is "passive", in other words, it waits for the partner to initiate the connection.
on demand	x	-	-	The device attempts to establish a connection to a partner when necessary. The receipt of requests for VPN connection establishment is also possible. For the configured local and remote subnets, an entry is created in the routing table. If a node attempts to send data packets via the VPN tunnel from one of the networks, the VPN connection is established. The settable timeout has the effect that after this time without any further data packets the VPN tunnel is terminated again.
start on DI	x	X	x	Connection establishment is controlled via the digital input (DI).
wait on DI	x	-	-	
Digital In	-		x	

Options	Use			Description
	IPsec VPN	OpenVPN	SINEMA RC	
Auto	-	-	x	The device adopts the settings of the SINEMA RC server. You configure the settings on the SINEMA RC Server in "Remote Connections > Devices". You can find additional information on this topic in the operating instructions "SINEMA RC Server".
Permanent	-	-	x	The device establishes a VPN connection to the SINEMA RC Server. The VPN tunnel is established permanently

Digital input (DI)

The establishment of the VPN tunnel can also be controlled via the digital input, e.g. using a button. When the button is closed, voltage is applied to the digital input and the LED of the digital input lights up. The lit LED indicates that signal 1 (TRUE / HIGH) is applied. Signal 1 triggers an event on the device with which the establishment of the VPN tunnel is controlled. You will find information on connecting and the maximum current load in the operating instructions of the devices.



Requirement

- In "System > Events > Configuration" for the "Digital Input" event "VPN Tunnel" is activated. If this setting is not activated, the event is not passed on to the VPN connection.

Options

The device supports the following options for controlling the VPN tunnel via the digital input:

- start on DI
  If the event "Digital Input" occurs, the device becomes "active". The device attempts to establish a VPN connection (IPsec) to a partner.
- wait on DI
  If the event "Digital Input" occurs, the device becomes "passive". The device waits for the partner to initiate the connection establishment.
- Digital In
  The settings of the SINEMA RC server are ignored. If the event "Digital In" occurs, the device becomes "active". The device attempts to establish a VPN connection to the SINEMA RC server.

Notification options

If the status of the digital input or a VPN tunnel (IPsec, SINEMA RC) changes, the device provides several options for notification on the "Events" page.

Type of notification	Digital In	VPN tunnel	Behavior if there is a status change
E-mail	x	x	The device sends an e-mail. The e-mail contains the identification of the sending device, a description of the cause of the alarm in plain language, and a time stamp. Requirement: • An SMTP server is set up. • In "System > SMTP Client" the function is activated, a receiver and the IP address of the SMTP server are configured.
Trap	x	x	The device sends an SNMP trap. Requirement: • "SNMPv1 traps" is enabled in "System > Configuration". • In "System > Configuration > Traps", a receiver is configured to which the device sends the SNMP traps.
Log Table	x	x	The device writes an entry in the event log table. The content of the event log table is displayed in "Information > Log Tables".
Syslog	x	x	The device writes an entry to the Syslog server. Requirement: • A Syslog server has been set up. • In "System > Syslog Client" the function is activated and the IP address of the Syslog server is configured.
Fault LED	x	-	The fault LED lights up on the device.
Read out the status of the MIB variable	x	-	Using the private MIB variable snMspsDigitalInputLevel, you can read out the status of the digital input. • OID of the private MIB variable snMspsDigitalInputLevel: `iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).siemens(4329).industrialComProducts(20).iComPlatforms(1).simaticNet(1).snMsps(1).snMspsCommon(1).snMspsDigitalIO(39).snMspsDigitalIOObjects(1).snMspsDigitalInputTable(2).snMspsDigitalInputEntry(1).snMspsDigitalInputLevel(6)` • values of the MIB variable – 1: Signal 0 at the digital input (DI) – 2: Signal 1 at the digital input (DI)

Configuring with Web Based Management 4

4.1 Web Based Management

How it works

The device has an integrated HTTP server for Web Based Management (WBM). If a device is addressed with a Web browser, it returns HTML pages to the Admin PC depending on the user input.

The user enters the configuration data in the HTML pages sent by the device. The device evaluates this information and generates reply pages dynamically.

Access via HTTPS is enabled in the factory setting. With access via HTTP, the address is automatically redirected to HTTPS.

If you wish to access the WBM via an HTTP connection, you need to select "HTTP & HTTPS" for "HTTP Services" in "System > Configuration"

Requirements

WBM display

- The device has an IP address.
- There is a connection between the device and the Admin PC.
  With the Windows ping command, you can check whether or not a connection exists.
  If the device has the factory settings, refer to "Requirements for operation (Page 27)".
- Access via HTTPS is enabled.
- JavaScript is activated in the Web browser.
- The Web browser must not be set so that it reloads the page from the server each time the page is accessed. The updating of the dynamic content of the page is ensured by other mechanisms.
- If a firewall is used, the relevant ports must be opened.
  - For access using HTTPS: TCP port 443
- The display of the WBM was tested with the following desktop Web browsers:
  - Microsoft Edge
  - Firefox Quantum
  - Google Chrome

  Recommendation: Use the latest available version of the Web browser, if possible.

4.2 Starting and logging in

Establishing a connection to a device

Follow the steps below to establish a connection to a device using an Internet browser:

1. There is a connection between the device and the Admin PC. With the ping command, you can check whether or not a device can be reached.
2. In the address box of the Internet browser, enter the IP address or the URL of the device. Access via HTTPS is enabled as default. If you access the device via HTTP, the address is automatically diverted to HTTPS.

   Note

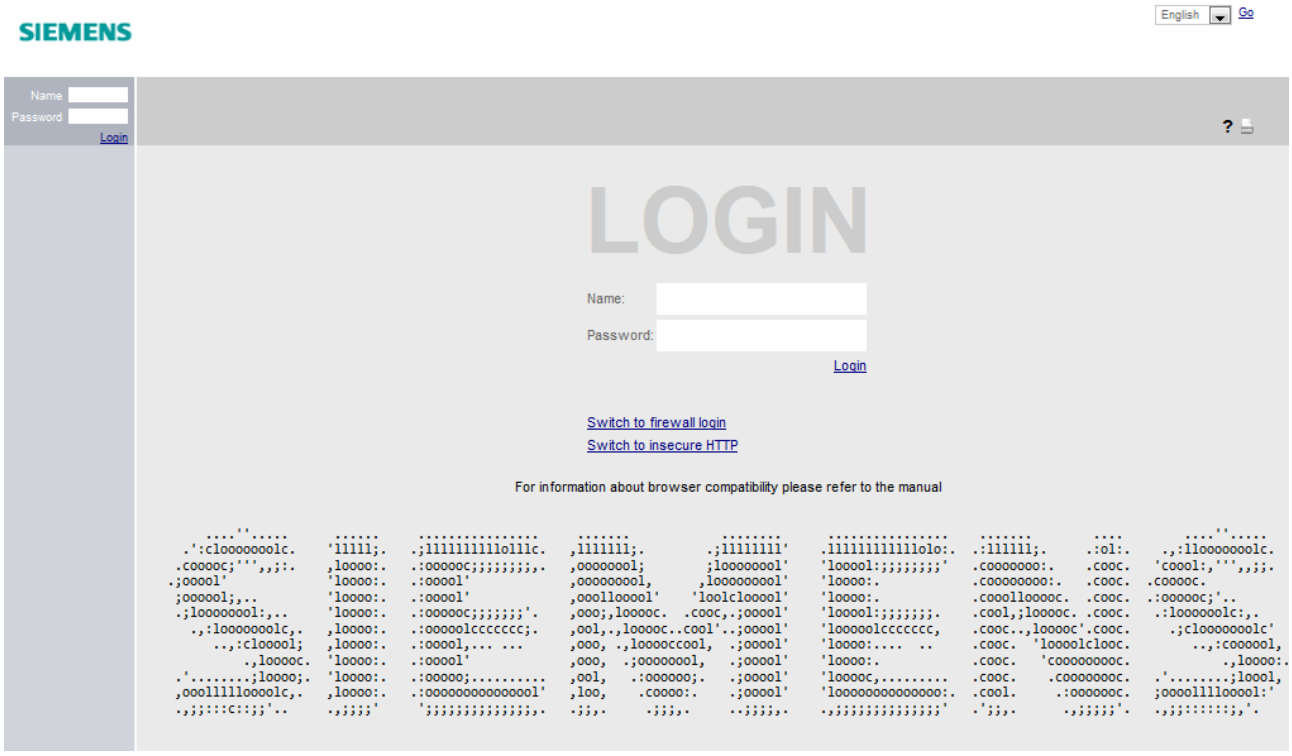
   Information on the security certificate

   Because the device can only be administered using encrypted access, it is delivered with a self-signed certificate. If certificates with signatures that the operating system does not know are used, a security message is displayed. You can display the certificate.

   A message relating to the security certificate appears. Acknowledge this message and continue loading the page.
   If you use a port other than the standard port, enter a colon ":" as separator between the IP address and the port number.
   Example: https://192.168.16.178:49152
   You change the port in "System > Configuration".
3. If there is a connection to the device, the login page of Web Based Management (WBM) is displayed.
   If you wish to access the WBM via an HTTP connection, you need to select "Redirect HTTP to HTTPS" for "HTTP Services" in "System > Configuration".

Changing language

1. From the drop-down list at the top right, select the language version of the WBM pages.
2. Click the "Go" button to change to the selected language.



Default Login Page

Under "System > Configuration > Default Login Page", you can define which login page is opened by default.

You can change the type of login via the "Switch to..." links.

To log in, you have the following options:

- Login option in the center of the browser window.
- Login option in the upper left area of the browser window.

Personalizing the login page

You can show an additional text on the login page.

1. Create a txt file that contains the desired text or the ASCII type. With ASCII type, pictograms, e.g. the Siemens company logo, are displayed based on the available characters.

   Note

   The use of the following special characters is not supported:
   - Backslash (\)
   - Question mark (?)
   - Tabs: Use spaces instead of tabs

2. Load the text file into the device using "System > Load&Save".
3. Log out. The configured text is shown below the credentials on the login page.

Restrictions

The following characters are generally not permitted:

- | ; : ? "
- The characters coded with the ASCII value as of 128 (extended ASCII code)
- The characters for Space and Delete

Logging in to WBM

To log in via HTTPS/HTTP, you have the following options:

- Login option in the center of the browser window
- Login option in the upper left area of the browser window.

Procedure:

1. "Name" input box:
   - When you log in for the first time or following a "Restore Factory Defaults and Restart", enter the user preset in the factory "admin".
     With this user account, you can change the settings of the device (read and write access to the configuration data).
   - Enter the user name of the created user account. You configure local user accounts and roles in "Security > Users".
2. "Password" input box:
   - When you log in for the first time or following a "Restore Factory Defaults and Restart", enter the password of the default user preset in the factory "admin": "admin".
   - Enter the password of the relevant user account.

3. Click the "Login" button or confirm your input with "Enter".

   Note

   When you log in for the first time or following a "Restore Factory Defaults and Restart", you can rename the "admin" user preset in the factory once. Afterwards, renaming "admin" is no longer possible. Enter the new name in the corresponding text box.

   When you log in for the first time or following a "Restore Factory Defaults and Restart", you are prompted to change the password.
   The new password must meet the following password policies:

   – Password length: at least 8 characters, maximum 128 characters
   – At least 1 uppercase letter
   – At least 1 special character (special characters § and ß are not permitted)
   – At least 1 number

   You need to repeat the password as confirmation. The password entries must match.

4. Click the "Set Values" button to complete the action.
   The changes take immediate effect. Access via DCP is write-protected after the admin password is changed. The network parameters can be read with the Primary Setup Tool or with "DCP Discovery", but can no longer be changed.

Once you have logged in successfully, the start page appears.

Logging into the dynamic firewall

Requirement

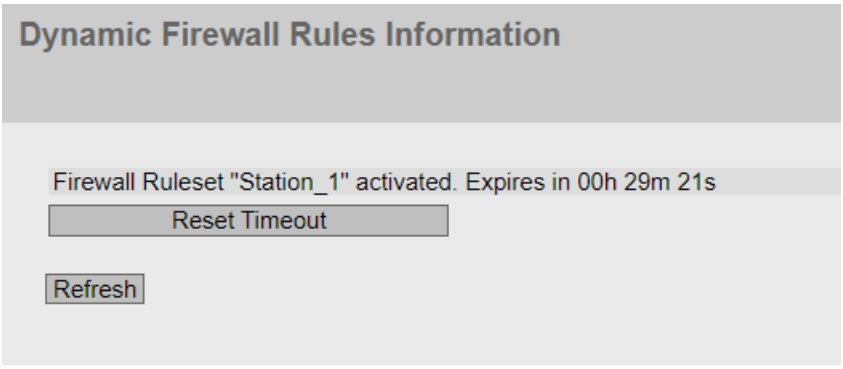
- The user has the right to remote access. You configure the setting "Security > Users > Local users".
- A rule set is assigned to the user.
  You can find more information on this in the "Dynamic Firewall" Getting Started.

Procedure

1. If the login page is not set by default for the user-specific firewall, click the link "Switch to firewall login".
2. Enter the user name of the created user account. You configure local user accounts and roles in "Security > Users".
3. Enter the password of the relevant user account.
4. Click the "Login" button or confirm your input with "Enter".
   If you combine the user account with an event, this condition must also be fulfilled.

After successful login, the WBM page "Dynamic Firewall Rules Information" opens.

The current rule set and the remaining time are displayed. If needed, the user can extend the access time via the "Reset Timeout" button.



After successful login, the WBM page "Information on dynamic firewall rules" opens.

The current ruleset and the remaining time are displayed. If needed, the user can extend the access time via the "Reset Timeout" button.

4.3 "Information" menu

4.3.1 Start page

View of the Start page

When you enter the IP address of the device, the start page is displayed after a successful login.

General layout of the WBM page

The following areas are available on every WBM page:

- Selection area (1): Top area
- Display area (2): Top area

- Navigation area (3): Left-hand area
- Content area (4): Middle area

Selection area (1)

The following is available in the selection area:

- Logo of Siemens AG
  When you click on the logo, you arrive at the Internet page of the corresponding basic device in Siemens Industry Online Support.
- Display of: "System Location / System Name"
  - "System Location" contains the location of the device.
    In the delivery state, the IP address of the device is displayed.
  - "System Name" is the device name.
    In the delivery state, the device type is displayed.

  You can change the content of this display with "System > General > Devices".
- Drop-down list for language selection
- System time and date
  You can change the content of this display with "System > System Time".
  If the system time is not set, the status is . If the system time is configured, but the system time cannot be synchronized, a yellow warning triangle can be seen. Check whether the time server can be reached. If necessary adapt your configuration. If the system time is set and/or can be synchronized, the status is .

Display area (2)

In the left-hand part of the display area, the full title of the currently selected menu item is always displayed.

- **LED simulation**
  Each device has one or more LEDs that provide information on the operating state of the device. Depending on its location, direct access to the device may not always be possible. Web Based Management therefore displays simulated LEDs. The meaning of the LED displays is described in the operating instructions.
  If you click this button, you open the window for the LED simulation. You can show this window during a change of menu and move it as necessary. To close the LED simulation, click the close button in the LED simulation window.
- **Help**
  When you click this button, the help page of the currently selected menu item is opened in a new browser window.
- **Printer**
  When you click this button, a pop-up window opens with a view of the page content optimized for the printer.

- **Favorites**
  When the product ships, the button is disabled on all pages .
  If you click this button, the symbol changes and the currently open page or currently open tab is marked as favorite. Once you have enabled the button once, the navigation area is divided into two tabs. The first tab "Menu" contains all the available menus as previously. The second tab "Favorites" contains all the pages/tabs that you selected as favorites. On the "Favorites" tab the pages/tabs are arranged according to the structure in the "Menu" tab.
  To do this, click the button on the relevant pages/tabs.
  If you disable all the favorites you have created, the "Favorites" tab is removed again.
  You can save, upload and delete the favorites configuration of a device on the "System > Load&Save" page using HTTP, TFTP or SFTP.
- **Update on On / Update off Off**
  WBM pages with overview lists can also have the "Update" button.
  With this button, you can enable or disable updating of the content area. If updating is turned on, the display is updated every 2 seconds. To disable the update, click "On". Instead of "On", "Off" is displayed. As default, updating is always enabled on the WBM page.

Navigation area (3)

In the navigation area, you have various menus available. Click the individual menus to display the submenus. The submenus contain pages on which information is available or with which you can create configurations. These pages are always displayed in the content area.

Content area (4)

In the navigation area, click a menu to display the pages of the WBM in the content area.

Below the device image, the following entries are possible:

- **PROFINET Name of Station** Shows the PROFINET device name.
- **System Name**: System name of the device.
- **Device Type**: Shows the type designation of the device.
- **Power Supply 1 / Power Supply 2**
  - Up
    Power supply 1 or 2 is applied.
  - Down
    Power supply 1 or 2 is not applied or is below the permitted voltage.
- **PLUG Configuration** Shows the status of the configuration data on the PLUG, refer to the section "System > PLUG > Configuration".
- **PLUG License** Shows the status of the license on the PLUG, refer to the section "System > PLUG > License".

- **DDNS Status**
  If a dynamic DNS service is used, the host name of the device is displayed, e.g. example.no-ip.com. The status of the update is also displayed.
  - update successful
    Update successful
  - update failed
    Update unsuccessful
  - status unkown
    Status unknown
- **Fault Status:** Displays the error status of the device.

Buttons you require often

The WBM pages contain the following standard buttons:

Refresh the display with "Refresh"
WBM pages that display current parameters have a "Refresh" button at the lower edge of the page. Click this button to request up-to-date information from the device for the current page.

Note

If you click the "Refresh" button, before you have transferred your configuration changes to the device using the "Set Values" button, your changes will be deleted and the previous configuration will be loaded from the device and displayed here.

Save entries with "Set Values"
WBM pages in which you can make configuration settings have a "Set Values" button at the lower edge. The button only becomes active if you change at least one value on the page. Click this button to save the configuration data you have entered on the device. Once you have saved, the button becomes inactive again.

Note

Changing configuration data is possible only with the "admin" role.

Note

The changes take immediate effect. But it takes some time for the changes in the configuration to be stored.

Create entries with "Create"
WBM pages in which you can make new entries have a "Create" button at the lower edge. Click this button to create a new entry.

Delete entries with "Delete"
WBM pages in which you can delete entries have a "Delete" button at the lower edge. Click this button to delete the previously selected entries from the device memory. Deleting also results in an update of the page in the WBM.

Page down with "Next"
On WBM pages with a lot of data records the number of data records that can be displayed on a page is limited. Click the "Next" button to page down through the data records.

Page back with "Prev"
On WBM pages with a lot of data records, the number of data records that can be displayed on a page is limited. Click the "Prev" button to page back through the data records.

Delete the display with "Clear"
In pages with sequence logs, you can delete all table entries at the same time regardless of whether filters are selected. The display is cleared in this process. The restart counter is only reset after you have restored the device to the factory settings and restarted the device.

Click the "Clear" button to completely delete the data record.

Button "Show all"
You can show all entries in pages with a large number of data records. Click "Show all" to display all entries on the page.

Note that displaying all messages can take some time.

Drop-down list to change page
In pages with a large number of data records, you can navigate to the desired page. From the drop-down list, select the relevant page to display it.

"Reset Counters" button
Click "Reset Counters" to reset all counters. The counters are reset by a restart**.**

Logout

You can log out from any WBM page by clicking the "Logout" link.

Messages

If you have enabled the "Automatic Save" mode and you change a parameter the following message appears in the display area "Changes will be saved automatically in x seconds. Click 'Write Startup Config' to save the changes immediately."

Note

Interrupting the save

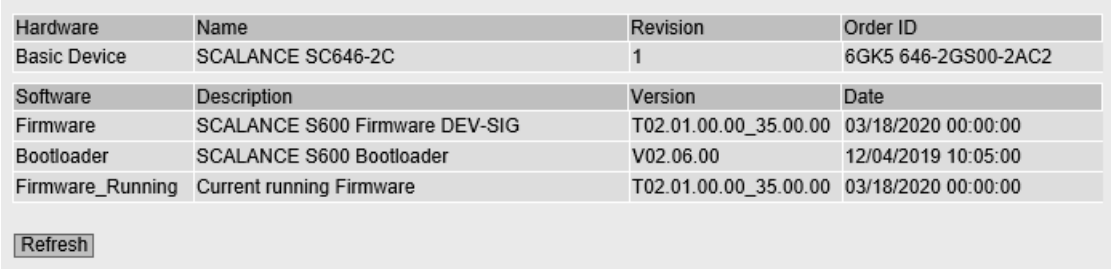
Saving starts only after the timer in the message has elapsed. How long saving takes depends on the device.

During the save, the message "Saving configuration data in progress. Please do not switch off the device." is displayed.

- Do not switch off the device immediately after the timer has elapsed.

4.3.2 Versions

This WBM page shows the versions of the hardware and software of the device.



Hardware	Name	Revision	Order ID
Basic Device	SCALANCE SC646-2C	1	6GK5 646-2GS00-2AC2

Software	Description	Version	Date
Firmware	SCALANCE S600 Firmware DEV-SIG	T02.01.00.00_35.00.00	03/18/2020 00:00:00
Bootloader	SCALANCE S600 Bootloader	V02.06.00	12/04/2019 10:05:00
Firmware_Running	Current running Firmware	T02.01.00.00_35.00.00	03/18/2020 00:00:00

Refresh

Description

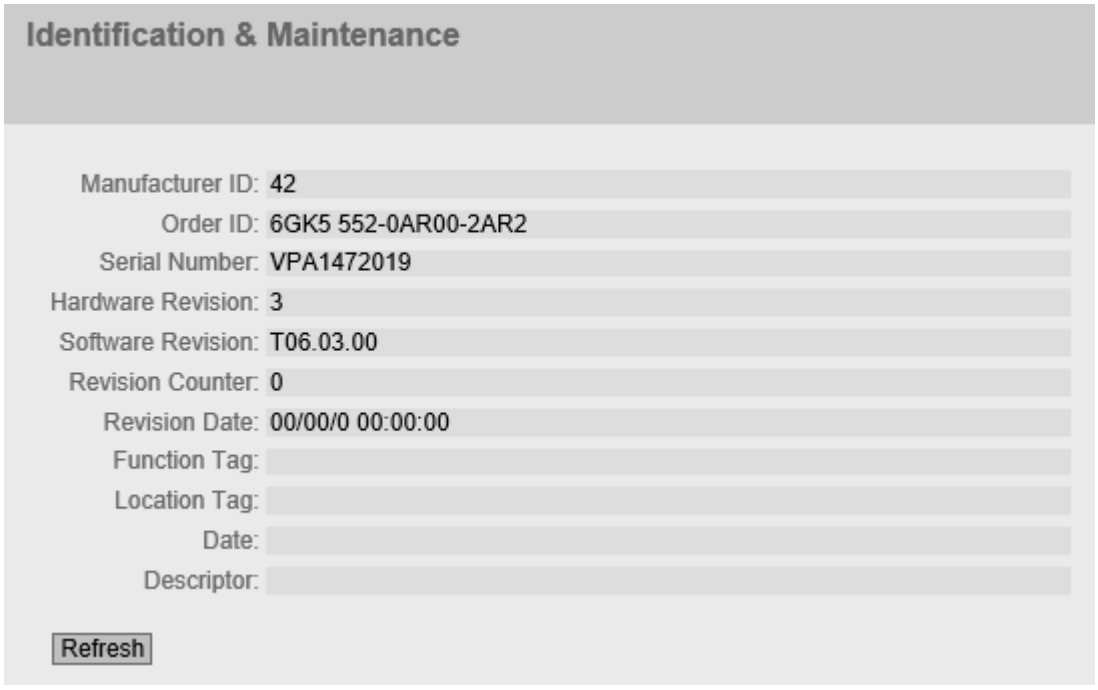
Table 1 has the following columns:

- **Hardware**
  - Basic Device
    Shows the basic device
  - PX.X
    X.X = port in which the SFP module is inserted.
  - SlotX
    "X" = slot number: Module plugged into this slot.
- **Name**
  Shows the name of the device or module.
- **Revision**
  Shows the hardware version of the device.
- **Order ID**
  Shows the article number of the device or described module.
- **Software**
  - Firmware
    Shows the current firmware version. If a new firmware file was downloaded and the device has not yet restarted, the firmware version of the downloaded firmware file is displayed here. After the next restart, the loaded firmware is activated and used.
  - Bootloader
    Shows the version of the boot software stored on the device.
  - Firmware_Running
    Shows the firmware version currently being used on the device.
- **Description**
  Shows the short description of the software.
- **Version**
  Shows the version number of the software version.
- **Date**
  Shows the date on which the software version was created.

4.3.3 Identification & Maintenance

Identification and Maintenance data

This page contains information about device-specific vendor and maintenance data such as the order number, serial number, version number etc. You cannot configure anything on this page.



Description of the displayed values

The table has the following rows:

- **Manufacturer ID**
  Shows the manufacturer ID.
- **Order ID**
  Shows the order ID.
- **Serial Number**
  Shows the serial number.
- **Hardware Revision**
  Shows the hardware version.
- **Software Revision**
  Shows the software version.
- **Revision Counter**
  Regardless of a version change, this box always displays the value "0".
- **Revision Date**
  Date and time of the last revision

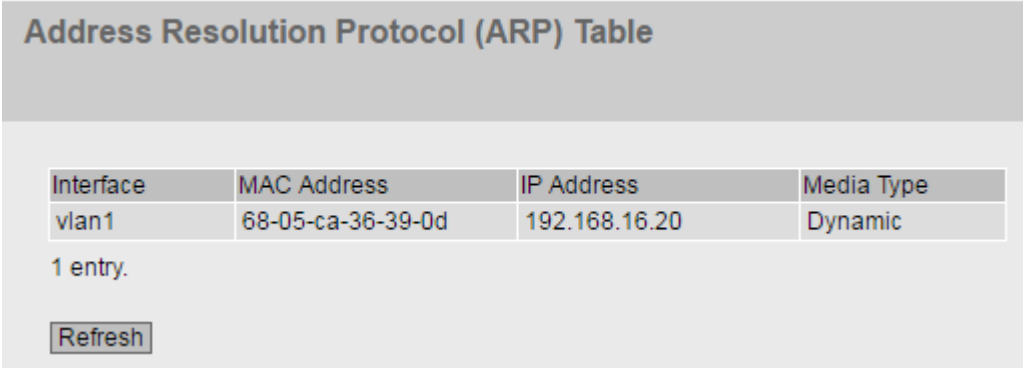
- **Function designation**
  is not supported.
- **Location designation**
  is not supported.
- **Date**
  is not supported.
- **Descriptor**
  is not supported.

4.3.4 ARP / Neighbors

4.3.4.1 ARP Table

Assignment of MAC address and IP address

With the Address Resolution Protocol (ARP), there is a unique assignment of MAC address to IP address. This assignment is kept by each network node in its own separate ARP table. The WBM page shows the ARP table of the device.



Description

The table has the following columns:

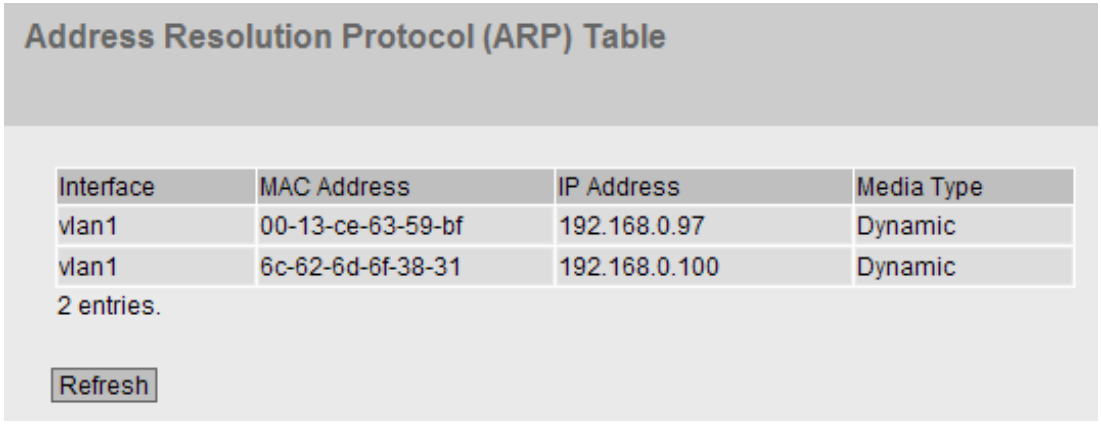
- **Interface**
  Shows the interface via which the row entry was learnt.
- **MAC Address**
  Shows the MAC address of the destination or source device.

- **IP Address**
  Shows the IPv4 address of the destination device.
- **Media Type**
  Shows the type of connection.
  - Dynamic
    The device recognized the address data automatically.
  - Static
    The addresses were entered as static addresses.

4.3.4.2 IPv6 Neighbor Table

Assignment of MAC address and IPv6 address

Via the IPv6 neighbor table, there is a unique assignment of MAC address to IPv6 address. This assignment is kept by each network node in its own separate neighbor table.



Description of the displayed values

The table has the following columns:

- **Interface**
  Displays the interface via which the row entry was learnt.
- **MAC Address**
  Shows the MAC address of the destination or source device.
- **IP Address**
  Shows the IPv6 address of the destination device.
- **Media Type**
  Shows the type of connection.
  - Dynamic
    The device recognized the address data automatically.
  - Static
    The addresses were entered as static addresses.

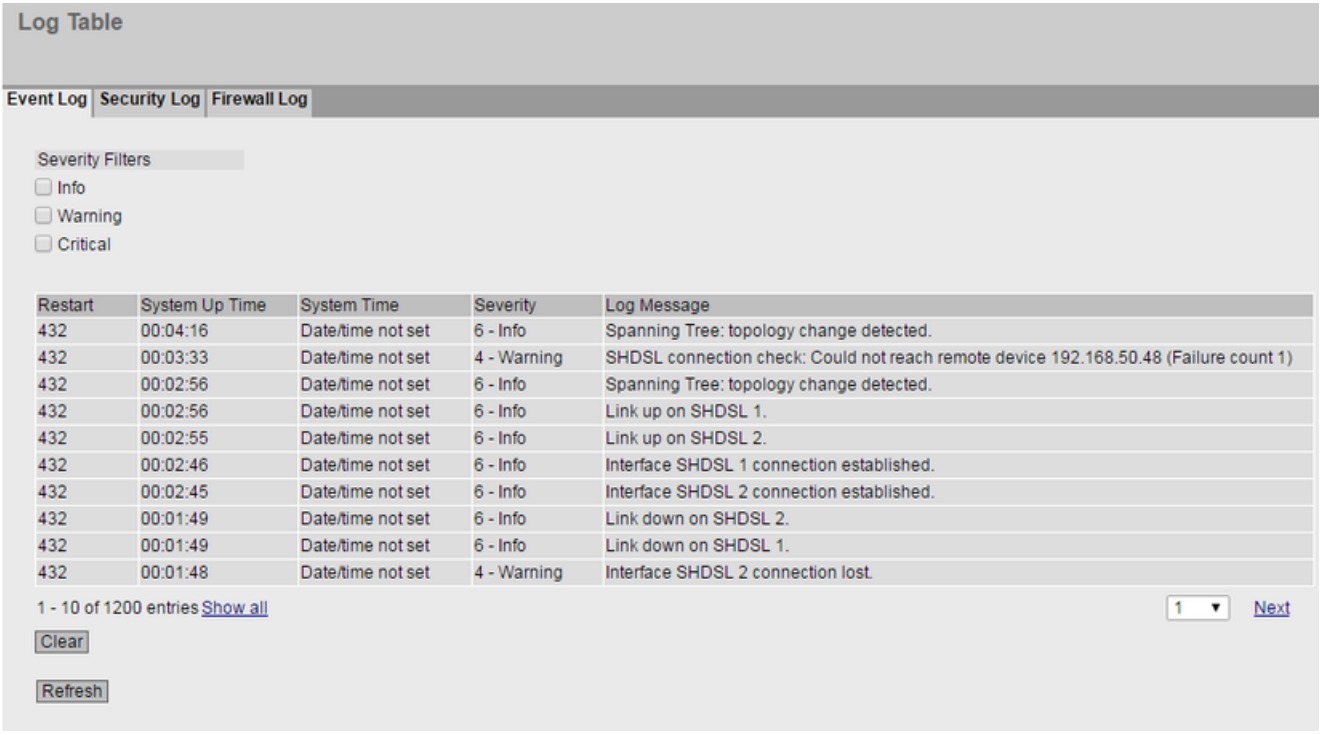
4.3.5 Log Tables

4.3.5.1 Event Log

Logging events

The WBM page shows the system events that have occurred in the form of a table. Some of the system events can be configured in "System > Events", for example if the connection status of a port has changed.

The content of the table is retained even when the device is turned off. The event log file can be loaded using HTTP, TFTP or SFTP.



Description

- **Severity Filters**
  You can filter the entries in the table according to severity. To display all the entries, enable or disable all parameters.

  Note

  A maximum of 800 entries in the table are possible for each severity. If the maximum number of entries is reached for a severity, the oldest entries of this severity are overwritten in the table. The table remains permanently in the memory.

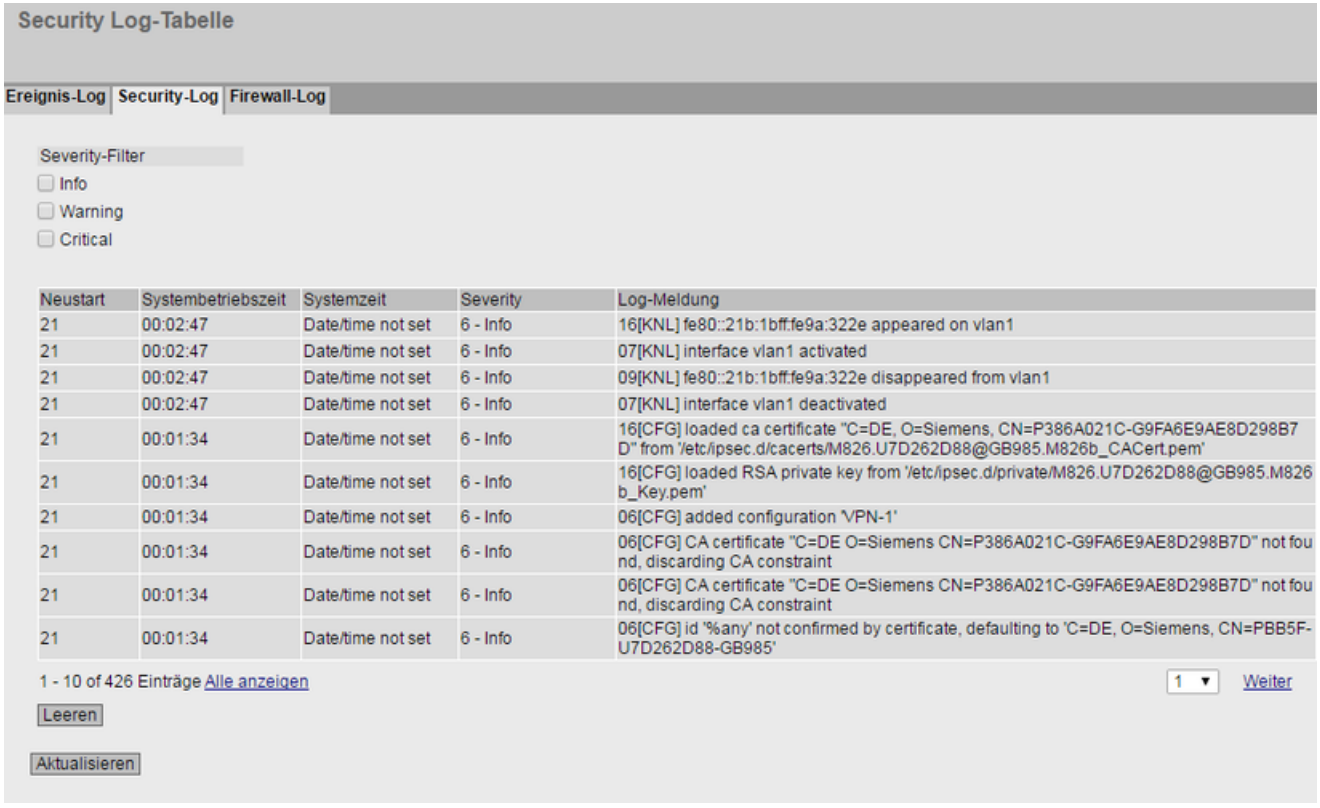
  – Critical
    Critical
    When this parameter is enabled, all entries of the category "Critical" are displayed.
  – Warning
    warning
    When this parameter is enabled, all entries of the category "Warning" are displayed.
  – Info
    Informative
    When this parameter is enabled, all entries of the category "Info" are displayed.

The table has the following columns:

- **Restart**
  Counts the number of restarts since you last reset to factory settings and shows the device restart after which the corresponding event occurred.
- **System Up Time**
  Shows the time the device has been running since the last restart when the described event occurred.
- **System Time**
  Shows the date and time when the described event occurred. If no system time is set, the box displays "Date/time not set".
- **Severity**
  Sorts the entry into the categories above.
- **Log Message**
  Displays a brief description of the event that has occurred.

4.3.5.2 Security Log

The WBM page shows the events that occurred during communication via a secure VPN tunnel in the form of the table.



Description

- **Severity Filters**
  You can filter the entries in the table according to severity. To display all the entries, enable or disable all parameters.

  Note

  A maximum of 800 entries in the table are possible for each severity. If the maximum number of entries is reached for a severity, the oldest entries of this severity are overwritten in the table. The table remains permanently in the memory.

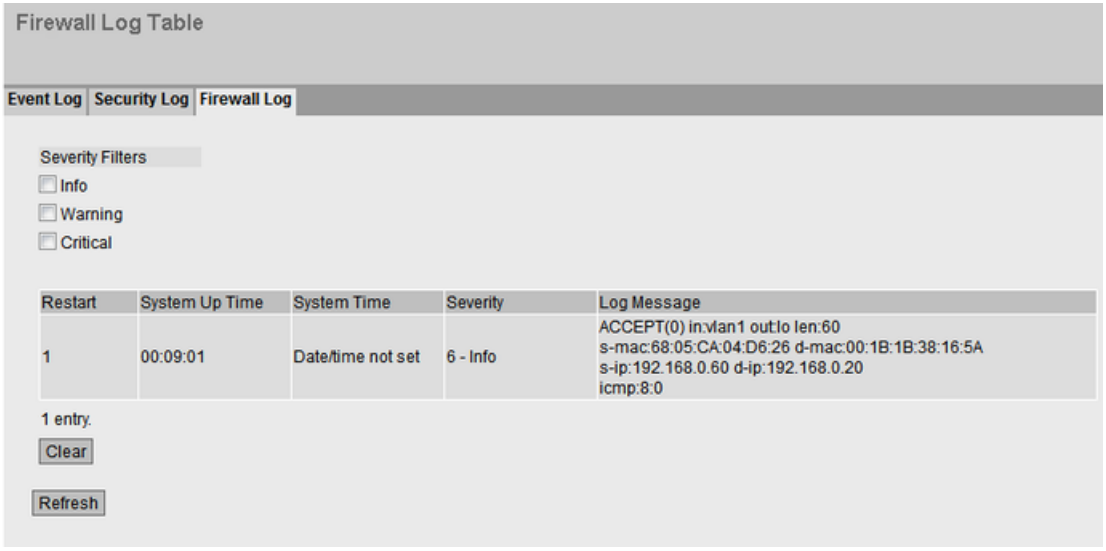
  – Critical
    Critical
    When this parameter is enabled, all entries of the category "Critical" are displayed.
  – Warning
    warning
    When this parameter is enabled, all entries of the category "Warning" are displayed.
  – Info
    Informative
    When this parameter is enabled, all entries of the category "Info" are displayed.

The table has the following columns:

- **Restart**
  Counts the number of restarts since you last reset to factory settings and shows the device restart after which the corresponding event occurred.
- **System Up Time**
  Shows the time the device has been running since the last restart when the described event occurred.
- **System Time**
  Shows the date and time when the described event occurred. If no system time is set, the box displays "Date/time not set".
- **Severity**
  Sorts the entry into the categories above.
- **Log Message**
  Displays a brief description of the event that has occurred.

4.3.5.3 Firewall Log

The firewall log logs the events that occurred on the firewall. When you create firewall rules, you can specify the event severity with which they are logged.



Description

- **Severity Filters**
  You can filter the entries in the table according to severity. To display all the entries, enable or disable all parameters.

  Note

  A maximum of 800 entries in the table are possible for each severity. If the maximum number of entries is reached for a severity, the oldest entries of this severity are overwritten in the table. The table remains permanently in the memory.

  – Critical
    Critical
    When this parameter is enabled, all entries of the category "Critical" are displayed.
  – Warning
    warning
    When this parameter is enabled, all entries of the category "Warning" are displayed.
  – Info
    Informative
    When this parameter is enabled, all entries of the category "Info" are displayed.

The table has the following columns:

- **Restart**
  Counts the number of restarts since you last reset to factory settings and shows the device restart after which the corresponding event occurred.
- **System Up Time**
  Shows the time the device has been running since the last restart when the described event occurred.
- **System Time**
  Shows the date and time when the described event occurred. If no system time is set, the box displays "Date/time not set".
- **Severity**
  Sorts the entry into the categories above.
- **Log Message**
  Displays a brief description of the event that has occurred.

4.3.6 Faults

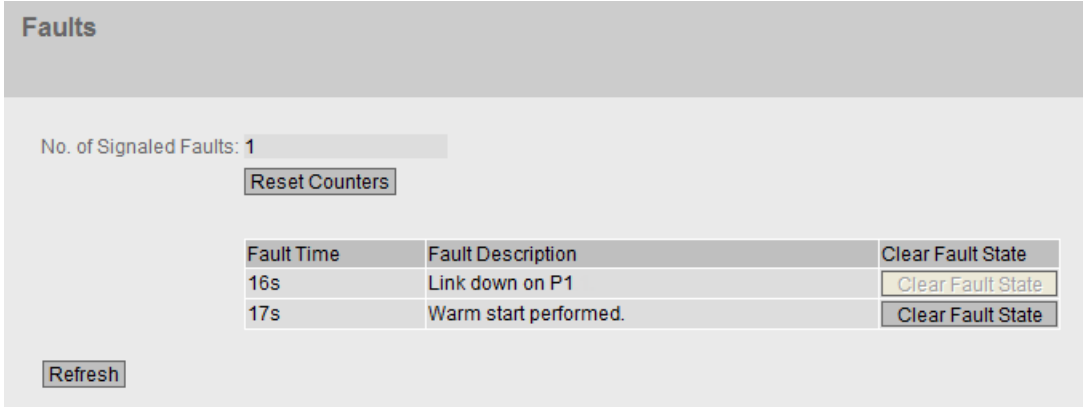
Fault status

If a fault occurs, it is shown on this page. On the device, faults are indicated by the red fault LED lighting up.

Internal faults of the device and faults that you configure on the following pages are indicated:

- "System > Events"
- "System > Fault Monitoring"

The calculation of the time of a fault always begins after the last system start. If there are no faults present, the fault LED switches off.



Description

The page contains the following boxes:

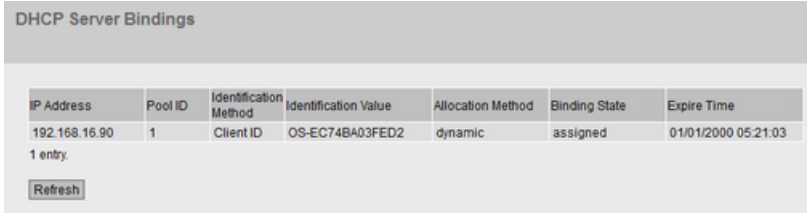
- **No. of Signaled Faults**
  Number of faults displayed since the last startup.
- **Reset Counters**
  The number is reset with this button. The counter is reset when there is a restart.

The table contains the following columns:

- **Fault Time**
  Shows the time the device has been running since the last system restart when the described fault occurred.
- **Fault Description**
  Displays a brief description of the error that has occurred.
- **Clear Fault State**
  Some faults can be acknowledged and thus removed from the fault list, e.g. a fault of the event "Cold/Warm Start". If the "Clear Fault State" button is enabled, you can delete the error.

4.3.7 DHCP Server

This page shows which IPv4 addresses were assigned to the devices by the DHCP server.



Description of the displayed values

- **IP Address**
  Shows the IPv4 address assigned to the DHCP client.
- **Pool ID**
  Shows the number of the IPv4-DHCP-Pool.
- **Identification Method**
  Shows the method with which the DHCP client is identified.
  - Remote ID
    Shows the remote ID of the DHCP client.
  - Circuit ID
    Shows the circuit ID of the DHCP client.
- **Identification Value**
  Shows the value that is assigned to the identification method.

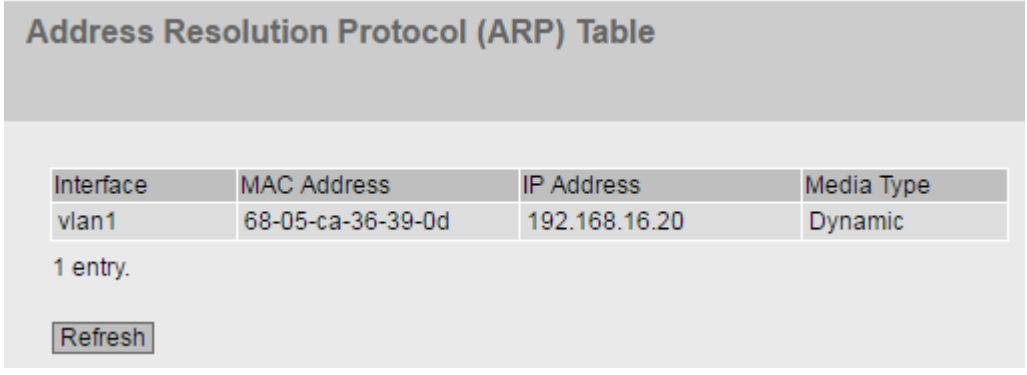
- **Allocation Method**
  Shows whether the IPv4 address was assigned statically or dynamically. You configure the static entries in "System > DHCP > Static Leases".
- **Binding State**
  Shows the status of the assignment.
  - Associated
    The assignment is used.
  - not used
    The assignment is not used.
  - probing
    The assignment is being checked.
  - unknown
    The status of the assignment is unknown.
- **Expire Time**
  Shows how long the assigned IPv4 address is still valid. When half the period of validity has elapsed. the DHCP client can extend the period of the assigned IPv4 address. When the entire time has elapsed, the DHCP client needs to request a new IPv4 address.

4.3.8 LLDP

Status of the neighborhood table

This page shows the current content of the neighborhood table. This table stores the information that the LLDP agent has received from connected devices.

You set the interfaces via which the LLDP agent receives or sends information in the following section: "Layer 2 > LLDP".



Description of the displayed values

The table contains the following columns:

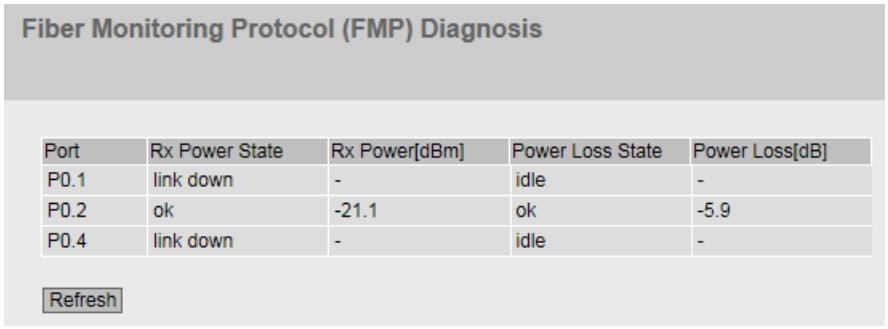
- **System Name**
  System name of the connected device.
- **Device ID**
  Device ID of the connected device. The device ID corresponds to the device name assigned via SINEC PNI (STEP 7). If no device name is assigned, the MAC address of the device is displayed.
- **Local Interface**
  Port at which the device received the information
- **Hold Time**
  An entry remains stored on the device for the time specified here. If the device does not receive any new information from the connected device during this time, the entry is deleted.
- **Capability**
  Shows the properties of the connected device:
  - Router
  - Bridge
  - Telephone
  - DOCSIS Cable Device
  - WLAN Access Point
  - Repeater
  - Station
  - Other
- **Port ID**
  Port of the device with which the device is connected.

4.3.9 Fiber Monitoring Protocol

Monitoring optical links

With Fiber Monitoring, you can monitor optical links. The table shows the current status of the ports.

You set the values to be monitored on the following page: "Layer 2 > FMP".



Description of the displayed values

- **Port**
  Shows the optical ports that support Fiber Monitoring. This depends on the transceivers.
- **Rx Power State**
  - **disabled**
    Fiber monitoring is disabled.
  - **ok**
    The value for the received power of the optical link is within the set limits.
  - **maint. req.**
    Check the link.
    A warning is signaled.
  - **maint. dem.**
    The link needs to be checked.
    An alarm is signaled and the fault LED is lit.
  - **link down**
    The connection to the communications partner is down. No link is detected.
- **Rx Power [dBm]**
  Shows the current value of the received power. The value can have a tolerance of +/- 3 dB. If there is no connection (link down) or fiber monitoring is disabled, "-" is displayed. If fiber monitoring is not enabled on the partner port, the value 0.0 is displayed.

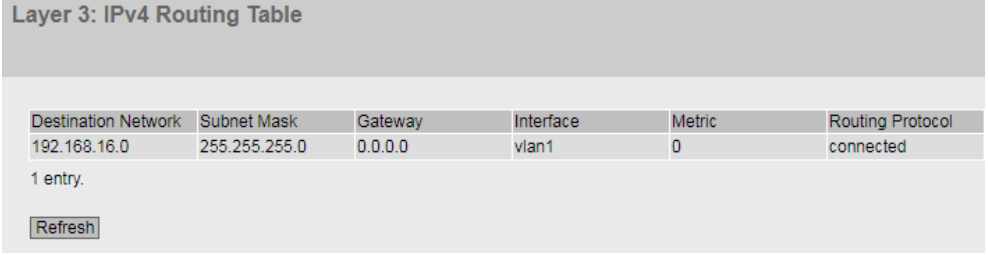
- **Power Loss State**
  To be able to monitor the power loss of the connection the function fiber monitoring must be enabled for the optical port of the connection partner.
  - **disabled**
    Fiber monitoring is disabled.
  - **ok**
    The value for the power loss of the optical link is within the defined limits.
  - **maint. req.**
    Check the link.
    A warning is signaled.
  - **maint. dem.**
    The link needs to be checked.
    An alarm is signaled and the fault LED is lit.
  - **idle**
    The port has no connection to another port with fiber monitoring enabled.
    If no diagnostics information is received from the optical port of the connection partner for 5 cycles, the fiber monitoring connection is assumed to be interrupted. A cycle lasts 5 seconds.
- **Power Loss [dB]**
  Shows the current value of the power loss. The value can have a tolerance of +/- 3 dB.
  If there is no connection (link down), Fiber Monitoring is disabled or the partner port does not support Fiber Monitoring, "-" is displayed.

4.3.10 IPv4 Routing

4.3.10.1 Routing Table

Introduction

This page shows the routes currently being used.



Description

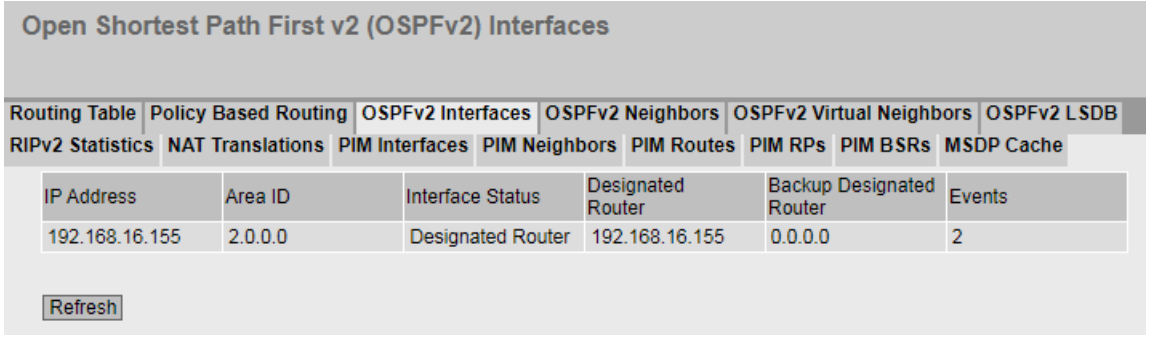
The table has the following columns:

- **Destination Network**
  Shows the destination address of this route.
- **Subnet Mask**
  Shows the subnet mask of this route.
- **Gateway**
  Shows the gateway for this route.
- **Interface**
  Shows the interface for this route.
- **Metric**
  Shows the metric of the route. The higher value, the longer packets require to their destination.
- **Routing Protocol**
  Shows the routing protocol from which the entry in the routing table originates. The following entries are possible:
  - Connected: Connected routes
  - Static: Static routes
  - DHCP: Routes via DHCP

4.3.10.2 OSPFv2 Interfaces

Overview

This page shows the configuration of the OSPF interface.



Description of the displayed values

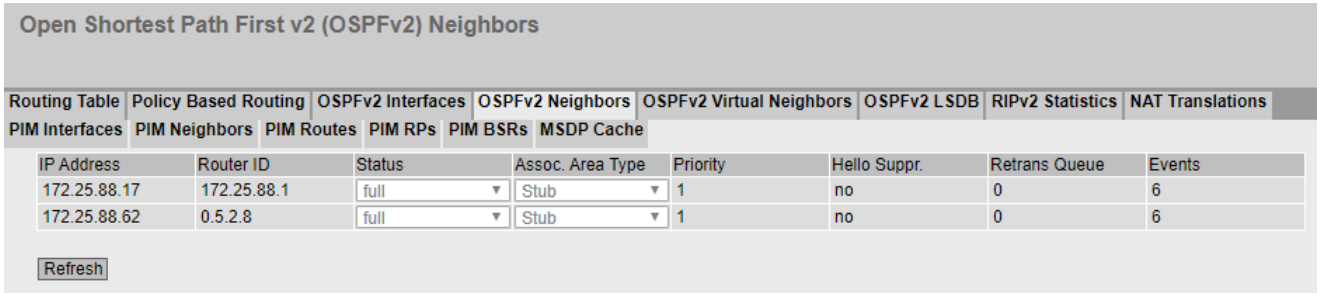
The table has the following columns:

- **IP address**
  Shows the IPv4 address of the OSPF interface
- **Area ID**
  Shows the area ID to which the OSPF interface belongs.
- **Interface Status**
  Shows the status of the WLAN interface:
  - Down
    The interface is not available.
  - Loop back
    Loop back interface
  - Waiting
    Starting up and negotiating the interface.
  - Point to Point
    Point-to-point link
  - Designated Router
    The router is a designated router and generates network LSAs.
  - Backup D. Router
    The router is the backup router for the designated router.
  - Other D. Router
    The Interface has started up. The router is neither a designated nor a designated backup router.
- **Designated Router**
  Shows the IPv4 address of the designated router for this OSPF interface.
- **Backup Designated Router**
  Shows the IPv4 address of the designated backup router for this OSPF interface.
- **Events**
  Shows the number of status changes of OSPF.

4.3.10.3 OSPFv2 Neighbors

Overview

This page shows the dynamically detected neighbor routers in the relevant networks.



Description of the displayed values

The table has the following columns:

- **IP Address**
  Shows the IPv4 address of the neighbor router in this network.
- **Router ID**
  Shows the ID of the neighbor router. The two addresses can match.
- **Status**
  Shows the status of the neighbor router. The status can adopt the following values:
  - unknown
    Status of the neighbor router is unknown.
  - down
    The neighbor router cannot be reached.
  - attempt and init
    Status during the initialization
  - two-way
    Two-way receipt of Hello packets. Specification of the designated router and the designated backup router.
  - exchangestart, exchange and loading
    Status during exchange of the LSAs
  - full
    The database is complete and synchronized within the area. The routes can now be detected.

  Note

  Normal status

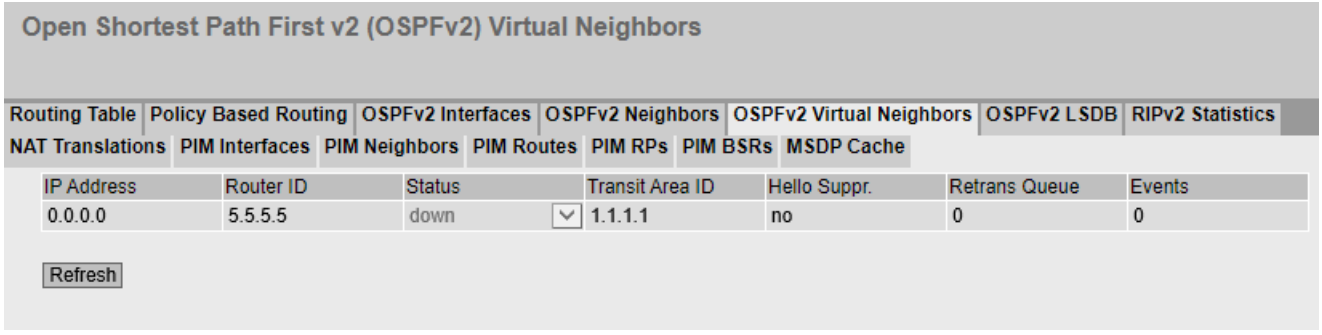
  If the partner router is a designated router or a designated backup router, the status is "full". Otherwise, the status is "two-way".

- **Assoc. Area Type**
  Shows the area type via which the neighbor-neighbor relation is maintained. The following area types exist:
  - Normal
  - Stub
  - NSSA
  - Backbone
- **Priority**
  Shows the priority of the neighbor router. This is only significant when selecting the designated router on a network. For virtual neighbor routers, this information is irrelevant.
- **Hello Suppr.**
  Shows the suppressed Hello packets to the neighbor router. This field normally displays "no".
- **Retrans. Queue**
  Shows the length of the queue with Hello packets still to be transmitted.
- **Events**
  Shows the number of status changes.

4.3.10.4 OSPFv2 Virtual Neighbors

Overview

This page shows the configured virtual neighbors.



Description of the displayed values

The table has the following columns:

- **IP Address**
  Shows the IPv4 address of the virtual neighbor router in this network.
- **Router ID**
  Shows the router ID of the virtual neighbor router.

- **Status**
  Shows the status of the neighbor router. The status can adopt the following values:
  - unknown
    Status of the neighbor router is unknown.
  - down
    The neighbor router cannot be reached.
  - attempt and init
    Brief status during initialization
  - two-way
    Two-way receipt of Hello packets. Specification of the designated router and the designated backup router.
  - exchangestart, exchange and loading
    Status during exchange of the LSAs
  - full
    The database is complete and synchronized within the area. The routes can now be detected.

  Note

  Normal status

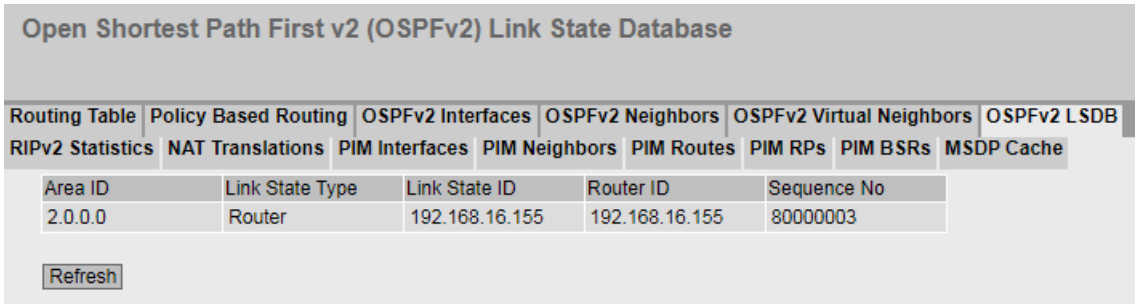
  If the partner router is a designated router or a designated backup router, the status is "full". Otherwise, the status is "two-way".

- **Trans. Area ID**
  Shows the ID of the area via which the virtual neighborhood relation exists.
- **Hello Suppr.**
  Shows whether there are suppressed Hello packets to the virtual neighbor router.
  - No: There are no suppressed Hello packets (default)
  - Yes: There are suppressed Hello packets.
- **Retrans. Queue**
  Shows the length of the queue with Hello packets still to be transmitted.
- **Events**
  Shows the number of status changes.

4.3.10.5 OSPFv2 LSDB

Overview

The link state database is the central database for managing all links within an area. It consists of the link state advertisements (LSAs). The most important data of these LSAs is shown on the this WBM page.



Description of the displayed boxes

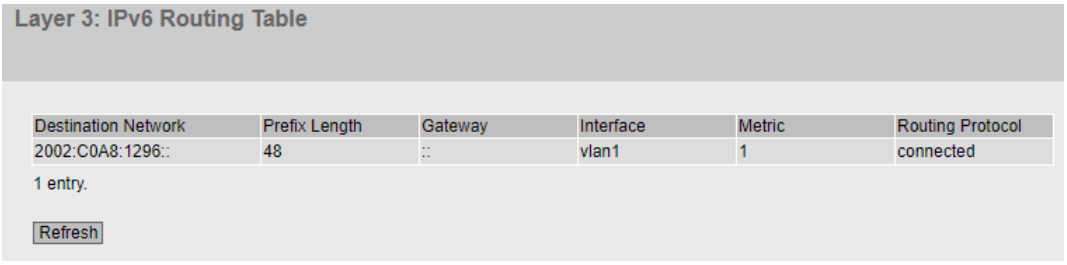
The table has the following columns:

- **Area ID**
  Shows the ID of the area to which the LSA belongs. If the LSA is an external connection, '-' is displayed.
- **Link State Type**
  Shows the LSA type. The following values are possible:
  - Unknown
    LSA type is unknown.
  - Router
    The router LSA (Type 1) is sent by the OSPF router within an area. The LSA contains information about the status of all router interfaces.
  - Network
    The network LSA (Type 2) is sent by the designated router within an area. The LSA contains a list of routers connected to the network.
  - NSSA External
    The NSSA external LSA (Type 7) is sent by the NSSA-ASBR within an NSSA. The NSSA-ASBR receives LSAs of Type 5 and converts the information to LSAs of Type 7. The NSSA router can forward these LSAs within an NSSA.
  - Summary
    The summary LSA (Type 3) is sent by the ABR within an area. The LSA contains information about routes to other networks.
  - AS Summary
    The AS summary LSA (Type 4) is sent by the area border router within an area. The LSA contains information about routes to other autonomous systems.
  - AS External
    The AS external LSA (Type 5) is sent by the AS border router within an autonomous system. The LSA contains information about routes from one network to another.
- **Link State ID**
  Shows the ID of the LSA.
- **Router ID**
  Shows the ID of the router that sent this LSA.
- **Sequence Number**
  Shows the sequence number of the LSA. Each time an LSA is renewed, this sequence number is incremented by one.

4.3.11 IPv6 Routing

Introduction

This page shows the IPv6 routes currently being used.



Description

The table has the following columns:

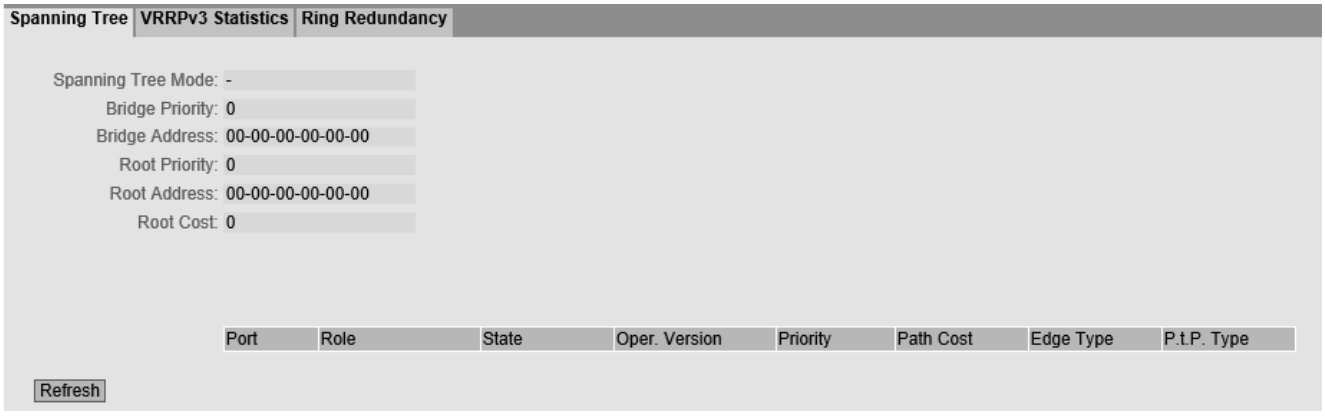
- **Destination Network**
  Shows the destination address of this route.
- **Prefix Length**
  Shows the prefix length of this route.
- **Gateway**
  Shows the gateway for this route.
- **Interface**
  Shows the interface for this route.
- **Metric**
  Shows the metric of the route. The higher value, the longer packets require to their destination.
- **Routing Protocol**
  Shows the routing protocol from which the entry in the routing table originates. The following entries are possible:
  - Connected: Connected routes
  - Static: Static routes
  - RIPng: Routes via RIPng
  - OSPFv3: Routes via OSPFv3
  - Other: Other routes

4.3.12 Redundancy

4.3.12.1 Spanning Tree

Introduction

The page shows the current information about the spanning tree and the settings of the root bridge.



Description of the displayed values

The following fields are displayed:

- **Spanning Tree Mode**
  Shows the set mode. You specify the mode in "Layer 2 > Configuration" and in "Layer 2 > Spanning Tree > General".
  The following values are possible:
  - '-'
  - RSTP
- **Bridge Priority / Root Priority**
  Which device becomes the root bridge is decided by the bridge priority. The bridge with the highest priority (in other words, with the lowest value for this parameter) becomes the root bridge. If several devices in a network have the same priority, the device whose MAC address has the lowest numeric value will become the root bridge. Both parameters, bridge priority and MAC address together form the bridge identifier. Since the root bridge manages all path changes, it should be located as centrally as possible due to the delay of the frames. The value for the bridge priority is a whole multiple of 4096 with a range of values from 0 to 32768.
- **Bridge Address / Root Address**
  The bridge address shows the MAC address of the device and the root address shows the MAC address of the root switch.

- Root Cost
  Shows the path costs from the device to the root bridge.
- Bridge Status
  Shows the status of the bridge, e.g. whether or not the device is the root bridge.

The table has the following columns:

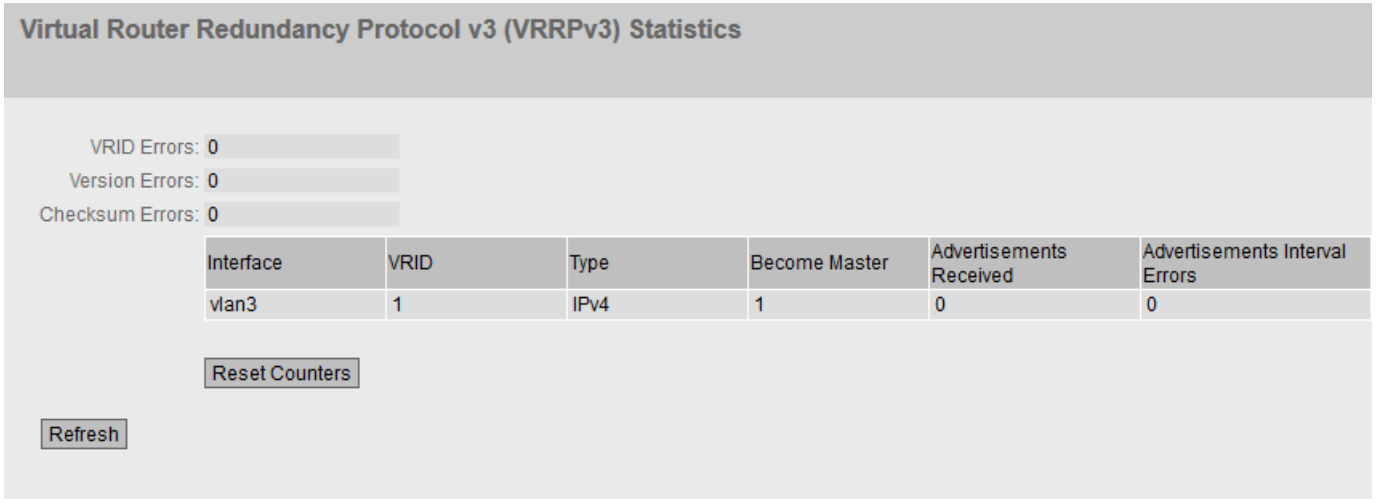
- **Port**
  Shows the interfaces via which the device communicates.
- **Role**
  Shows the status of the port. The following values are possible:
  - Disabled
    The port was removed manually from the spanning tree and will no longer be taken into account by the spanning tree.
  - Designated
    The ports leading away from the root bridge.
  - Alternate
    The port with an alternative route to a network segment
  - Backup
    If a switch has several ports to the same network segment, the "poorer" Port becomes the backup port.
  - Root
    The port that provides the best route to the root bridge.
  - Master
    This port points to a root bridge located outside the MST region.
- **Status**
  Shows the current status of the interface. The values are only displayed. The parameter depends on the configured protocol.
  - Discarding
    The port receives BPDU frames. Other incoming or outgoing frames are discarded.
  - Listening
    The port receives and sends BPDU frames. The port is involved in the spanning tree algorithm. Other outgoing and incoming frames are discarded.
  - Learning
    The port actively learns the topology; in other words, the node addresses. Other outgoing and incoming frames are discarded.
  - Forwarding
    Following the reconfiguration time, the port is active in the network. The port receives and sends data frames.
- **Oper. Version**
  Shows the compatibility mode of Spanning Tree used by the port.
- **Priority**
  If the path calculated by the spanning tree is possible over several ports of a device, the port with the highest priority (in other words the lowest value for this parameter) is selected. A value between 0 and 240 can be entered for the priority in steps of 16. If you enter a value that cannot be divided by 16, the value is automatically adapted. The default is 128.

- **Path Cost**
  This parameter is used to calculate the path that will be selected. The path with the lowest value is selected. If several ports of a device have the same value, the port with the lowest port number is selected.
  If the value in the "Cost Calc" field is "0", the automatically calculated value is displayed. Otherwise, the value of the "Cost Calc" field is displayed.
  The calculation of the path costs is largely based on the transmission speed. The higher the achievable transmission speed is, the lower the value of the path costs.
  Typical values for path costs with rapid spanning tree:
  - 10,000 Mbps = 2,000
  - 1000 Mbps = 20,000
  - 100 Mbps = 200,000
  - 10 Mbps = 2,000,000
- **Edge Type**
  Shows the type of the connection. The following values are possible:
  - Edge Port
    There is an end device at this port.
  - No Edge Port
    There is a spanning tree or rapid spanning tree device at this port.
- **P.t.P. Type**
  Shows the type of point-to-point link. The following values are possible:
  - P.t.P.
    With half duplex, a point-to-point link is assumed.
  -
    Shared Media
    With a full duplex connection, a point-to-point link is not assumed.

4.3.12.2 VRRPv3 Statistics

Introduction

This page shows the statistics of the VRRPv3 protocol and all configured virtual routers.



Description

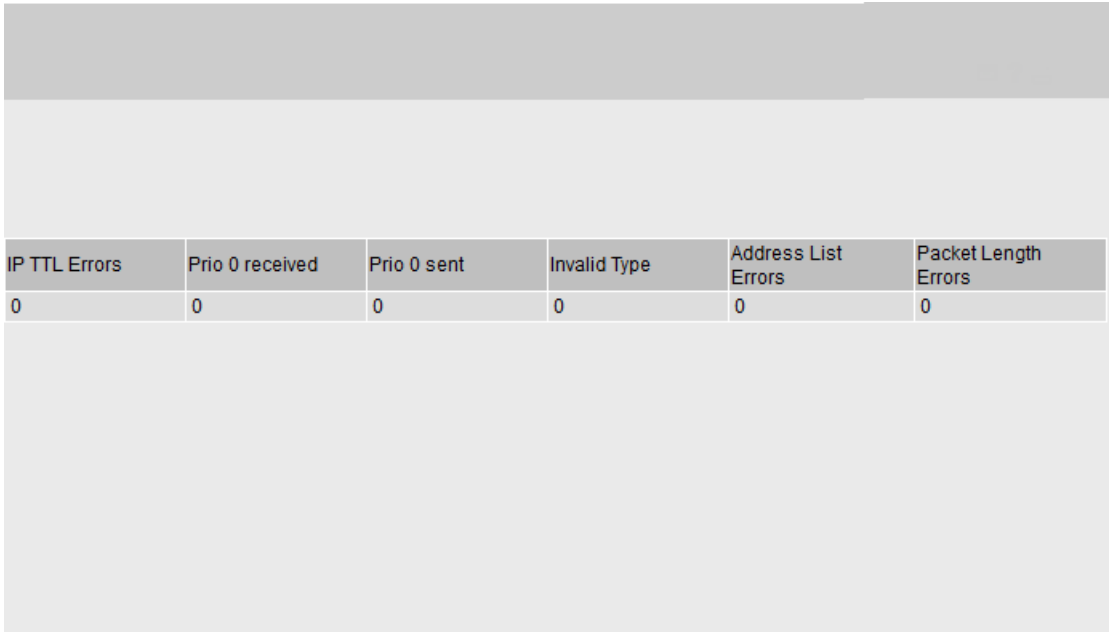
The following fields are displayed:

- **VRID Errors**
  Shows how many VRRPv3 packets containing an unsupported VRID were received.
- **Version Errors**
  Shows how many VRRPv3 packets containing an invalid version number were received.
- **Checksum Errors**
  Shows how many VRRPv3 packets containing an invalid checksum were received.

The table has the following columns:

- **Interfaces**
  Interface to which the settings relate.
- **VRID**
  Shows the ID of the virtual router. Valid values are 1 ... 255.
- **Address Type**
  Shows the version of the IP protocol.
- **Become Master**
  Shows how often this virtual router changed to the "Master" status.
- **Advertisements Received**
  Shows how many VRRPv3 packets were received.

- **Advertisement Interval Errors**
  Shows how many bad VRRPv3 packets were received whose interval does not match the value set locally.



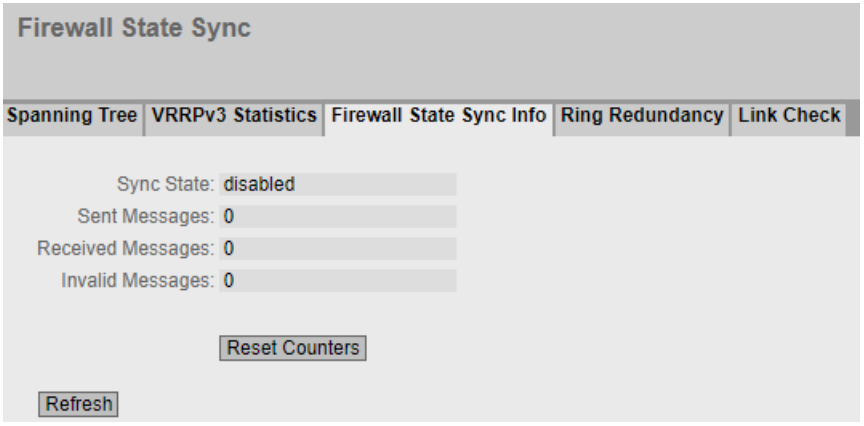
IP TTL Errors	Prio 0 received	Prio 0 sent	Invalid Type	Address List Errors	Packet Length Errors
0	0	0	0	0	0

- **IP TTL Errors**
  Shows how many bad VRRPv3 packets were received whose TTL (Time to live) value in the IP header is incorrect.
- **Prio 0 received**
  Shows how many VRRPv3 packets with priority 0 were received. VRRPv3 packets with priority 0 are sent when a master router is shut down. These packets allow a fast handover to the relevant backup router.
- **Prio 0 sent**
  Shows how many VRRPv3 packets with priority 0 were sent. Packets with priority 0 are sent when a master router is shut down. These packets allow a fast handover to the relevant backup router.
- **Invalid Type**
  Shows how many bad VRRPv3 packets were received whose value in the "Type" field of the IP header is invalid.
- **Address List Errors**
  Shows how many bad VRRPv3 packets were received whose address list does not match the locally configured list.
- **Packet Length Errors**
  Shows how many bad VRRPv3 packets were received whose length is not correct.

4.3.12.3 Firewall State Sync

Information on the Firewall State Sync

On this page, you obtain the following information about the Firewall State Sync.



Description of the displayed values

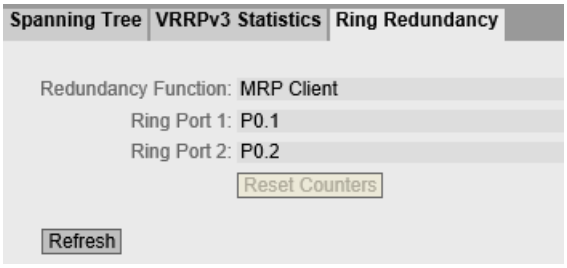
The table has the following columns:

- **Sync State**
  Shows the status of the Firewall State Sync:
  - running: Valid messages from the synchronization partner are being received.
  - no receive: No messages were received from the synchronization partner during the valid period (5 seconds).
  - error: The message could not be sent due to an internal error.
  - disabled: The function is disabled.
- **Sent Messages**
  Number of sent synchronization messages.
- **Received Messages**
  Number of valid messages that were transferred by the synchronization partner.
- **Invalid Messages**
  Number of invalid messages that were transferred by the synchronization partner.
- **Reset Counters**
  Click this button to reset the counters on this page.
  Refresh
  Refreshes the display of the values. The result is shown in the table.

4.3.12.4 Ring redundancy

Information on ring redundancy

On this page, you obtain information about the status of the device in terms of ring redundancy. The text boxes on this page are read-only.



Description of the displayed values

The table has the following columns:

- **Redundancy Function**
  The "Redundancy Function" column shows the role of the device within the ring:
  - No Ring Redundancy
    The device is operating without redundancy function.
  - HRP Client
    The device is operating as HRP Client.
  - MRP Client
    The device is operating as MRP Client.
- **Ring Port 1/Ring Port 2**
  The "Ring Port 1"and "Ring Port 2" columns show the ports being used as ring ports. If media redundancy in ring topologies is completely disabled, ring ports configured last are displayed.

4.3.12.5 Link check

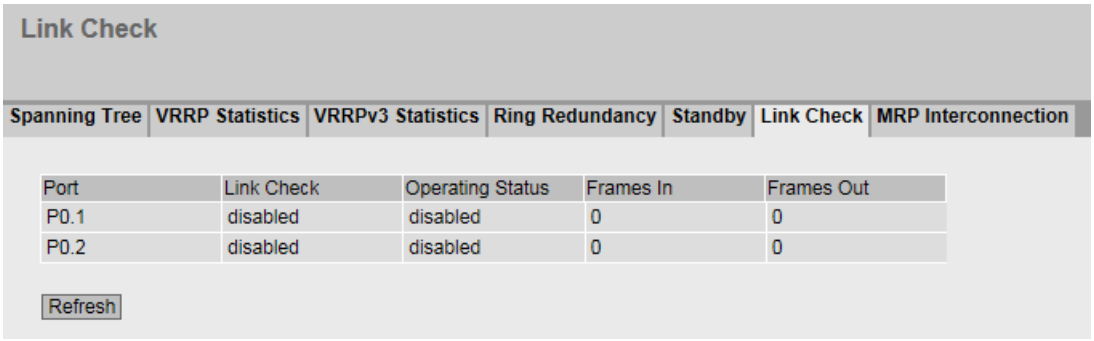
Monitoring optical connections in the ring

The page shows the following information on Link Check:

- The ring ports
- The current status (activated or not activated)
- The statistics of sent and received Link Check frames of the monitored connections

Note

If you use Link Check together with a redundancy protocol (e.g. HRP), the values for the sent and received Link Check frames can be different.



Description of the displayed values

The following boxes are displayed:

- **Port**
  Shows the port to which the following information relates. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.
- **Link Check**
  Shows whether the Link Check function is enabled or disabled.
- **OperState**
  Shows the status of the Link Check function. The following statuses are possible:
  - Disabled
    The function is disabled.
  - Enabled
    The function is enabled. The connection partner has not yet confirmed the monitoring.
  - Running
    The function is enabled. The connection monitoring is enabled. The outgoing and incoming test frames are counted and matched up.
  - Faults
    The function is enabled. Link Check has detected a fault on the monitored section and turned off the port.
- **Frames in**
  Shows how many Link Check test frames were received.
- **Frames out**
  Shows how many Link Check test frames were sent.

4.3.13 Ethernet Statistics

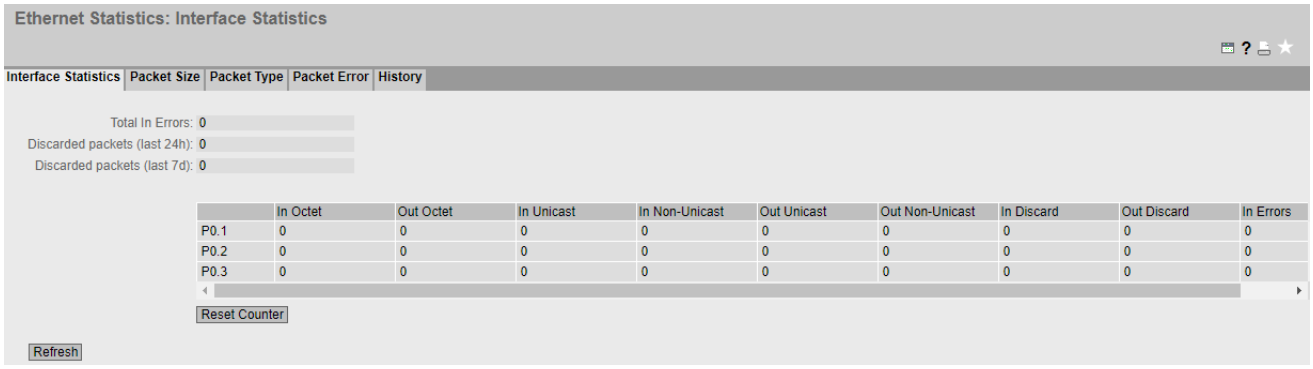
4.3.13.1 Interface Statistics

Interface statistics

The page shows the statistics from the interface table of the Management Information Base (MIB).

Note

The interface statistics specify the total number of received or sent bytes for each port. In contrast, the information for VLAN interfaces only relates to the Layer 3 data traffic of the corresponding interface.



Description of the displayed values

The page contains the following boxes:

- **In Errors (total)**
  Shows the sum of all received errors.
- **Discarded packets (last 24 hrs)**
  Shows the sum of all discarded packets within the last 24 hours.
- **Discarded packets (last 7 days)**
  Shows the sum of all discarded packets within the last 7 days.

The table has the following columns:

- **In Octet**
  Shows the number of received bytes.
- **Out Octet**
  Shows the number of sent bytes.
- **In Unicast**
  Shows the number of received unicast frames.

- **In Non Unicast**
  Shows the number of received frames that are not of the type unicast.
- **Out Unicast**
  Shows the number of sent unicast frames.
- **Out Non Unicast**
  Shows the number of sent frames that are not of the type unicast.
- **In Discard**
  Shows the number of incoming frames that were discarded.
- **Out Discard**
  Shows the number of outgoing frames that were discarded.
- **In Errors**
  Shows the number of all possible RX errors, refer to the tab "Packet Error".

Description of the button

"Reset Counters" button

Click "Reset Counters" to reset all counters. The counters are reset by a restart.

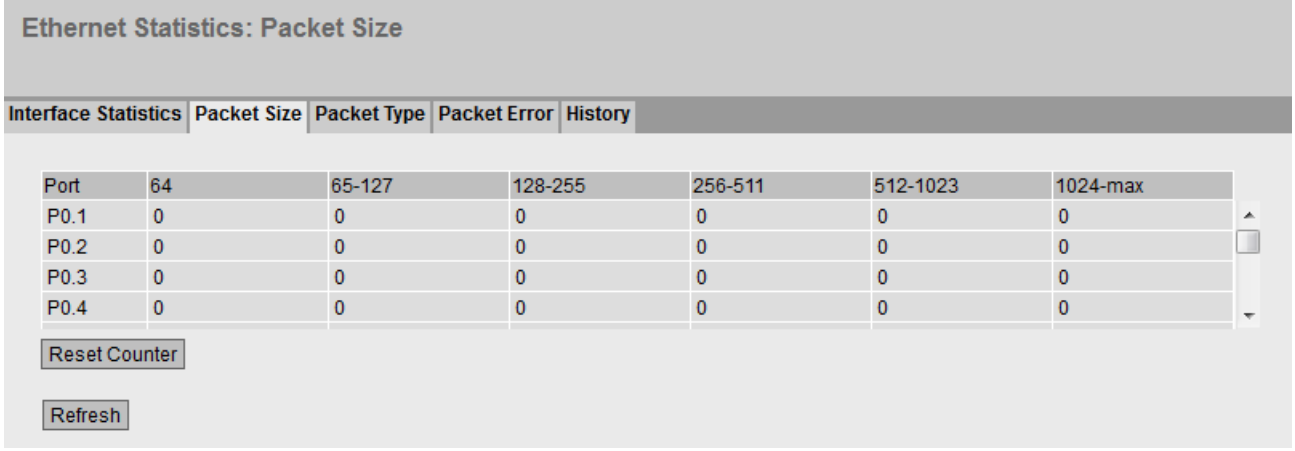
4.3.13.2 Packet Size

Frames sorted by length

This page displays how many frames of which length were sent and received at each port. You cannot configure anything on this page.

The displayed values are transferred by RMON.

On the page "Layer 2 > RMON > Statistics", you can set the ports for which values will be displayed.



Description of the displayed values

The table has the following columns:

- **Port**
  Shows the available ports and link aggregations. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.

  Note

  Display of frame statistics

  In the statistics relating to frame lengths, note that both incoming and outgoing frames are counted.

- **Frame lengths**
  The other columns after the port number contain the absolute numbers of frames according to their frame length.
  The following frame lengths are distinguished:
  - 64 bytes
  - 65 - 127 bytes
  - 128 - 255 bytes
  - 256 - 511 bytes
  - 512 - 1023 bytes
  - 1024 - Max.

Note

Data traffic on blocked ports

For technical reasons, data packets can be indicated on blocked ports.

Description of the button

"Reset Counters" button

Click "Reset Counters" to reset all counters. The counters are reset by a restart.

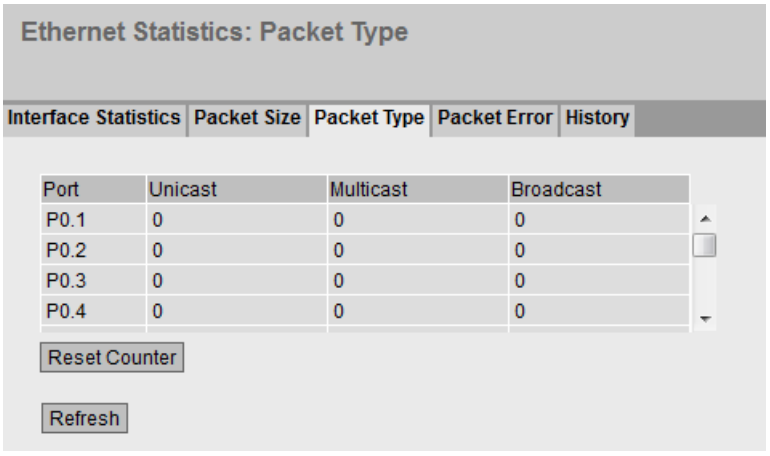
4.3.13.3 Packet Type

Received frames sorted by Packet Type

This page displays how many frames of the types "Unicast", "Multicast", and "Broadcast" were received at each port. You cannot configure anything on this page.

The displayed values are transferred by RMON.

On the page "Layer 2 > RMON > Statistics", you can set the ports for which values will be displayed.



Description of the displayed values

The table has the following columns:

- **Port**
  Shows the available ports and link aggregations. The port is made up of the module number and the port number, for example, port 0.1 is module 0, port 1.
- **Unicast / Multicast / Broadcast**
  The other columns after the port number contain the absolute numbers of the incoming frames according to their Packet Type "Unicast", "Multicast" and "Broadcast".

Description of the button

"Reset Counters" button

Click "Reset Counter" to reset all counters. The counters are reset by a restart.

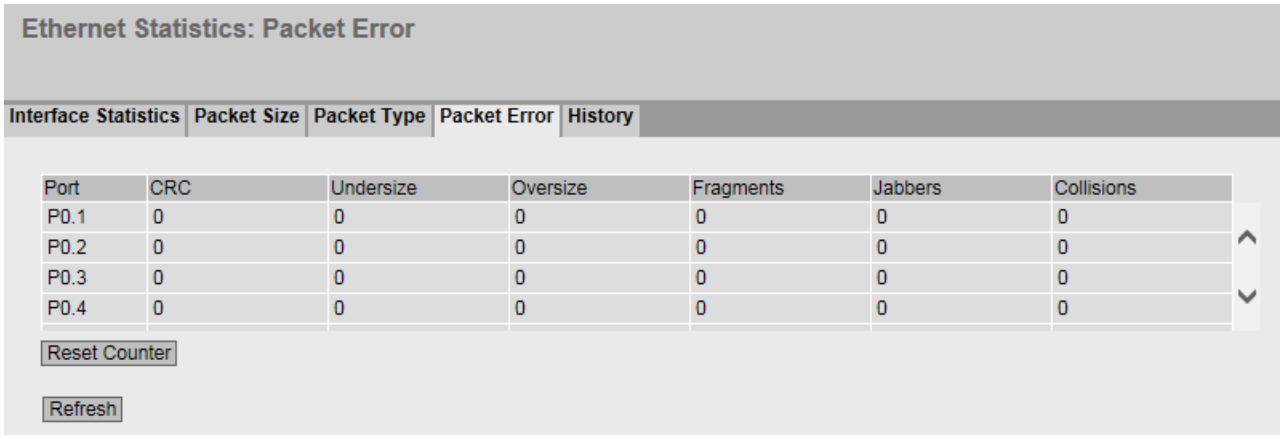
4.3.13.4 Packet Error

Received bad frames

This page shows how many bad frames were received per port. You cannot configure anything on this page.

The displayed values are transferred by RMON.

On the page "Layer 2 > RMON > Statistics", you can set the ports for which values will be displayed.



Description of the displayed values

The table has the following columns:

- **Port**
  Shows the available ports and link aggregations. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.
- **Error types**
  The other columns after the port number contain the absolute numbers of the incoming frames according to their error type.
  In the columns of the table, a distinction is made according to the following error types:
  - CRC
    Packets whose content does not match the CRC checksum.
  - Undersize
    Packets with a length less than 64 bytes.
  - Oversize
    Packets discarded because they were too long.
  - Fragments
    Packets with a length less than 64 bytes and a bad CRC checksum.
  - Jabbers
    VLAN-tagged packets with an incorrect CRC checksum that were discarded because they were too long.
  - Collisions
    Collisions that were detected.

Description of the button

"Reset Counters" button

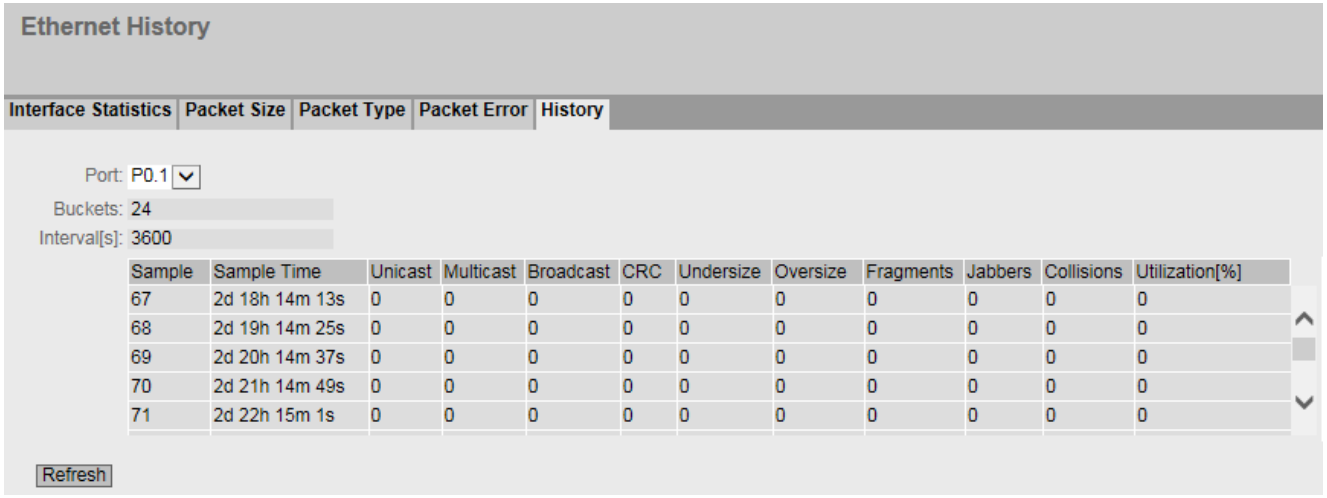
Click "Reset Counters" to reset all counters. The counters are reset by a restart.

4.3.13.5 History

Samples of the statistics

The page shows samples from each port with information from the RMON statistics.

On the page "Layer 2 > RMON > History", you can set the ports for which samples will be taken.



Sample	Sample Time	Unicast	Multicast	Broadcast	CRC	Undersize	Oversize	Fragments	Jabbers	Collisions	Utilization[%]
67	2d 18h 14m 13s	0	0	0	0	0	0	0	0	0	0
68	2d 19h 14m 25s	0	0	0	0	0	0	0	0	0	0
69	2d 20h 14m 37s	0	0	0	0	0	0	0	0	0	0
70	2d 21h 14m 49s	0	0	0	0	0	0	0	0	0	0
71	2d 22h 15m 1s	0	0	0	0	0	0	0	0	0	0

Settings

- **Port**
  Select the port for which the History will be displayed.

Description of the displayed values

- **Buckets**
  Maximum number of samples that can be saved at the same time.
- **Interval [s]**
  Interval after which the current status of the statistics is saved as a sample.

The table has the following columns:

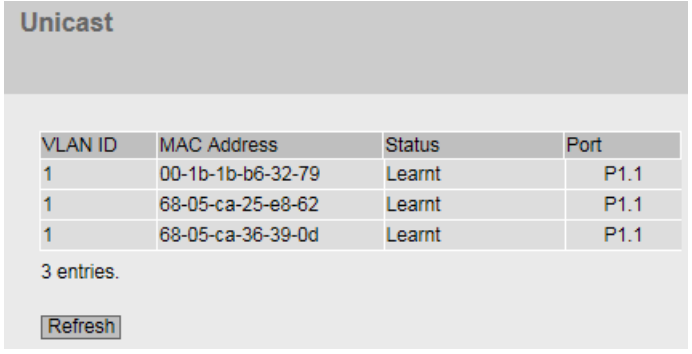
- **Sample**
  Number of the sample
- **Sample Time**
  System up time at which the sample was taken.
- **Unicast**
  Number of received unicast frames.
- **Multicast**
  Number of received multicast frames.
- **Broadcast**
  Number of received broadcast frames.

- **CRC**
  Number of frames with a bad CRC checksum.
- **Undersize**
  Number of frames that are shorter than 64 bytes.
- **Oversize**
  Number of frames discarded because they are too long.
- **Fragments**
  Number of frames that are shorter than 64 bytes and have a bad CRC checksum.
- **Jabbers**
  Number of frames with a VLAN tag that have a bad CRC checksum and are discarded because they are too long.
- **Collisions**
  Number of collisions of received frames.
- **Utilization [%]**
  Utilization of the port during a sample.

4.3.14 Unicast

Status of the unicast filter table

This page shows the current content of the unicast filter table. This table lists the source addresses of unicast address frames. The entries are made statically through parameter assignment by the user.



Description of the displayed values

The table contains the following columns:

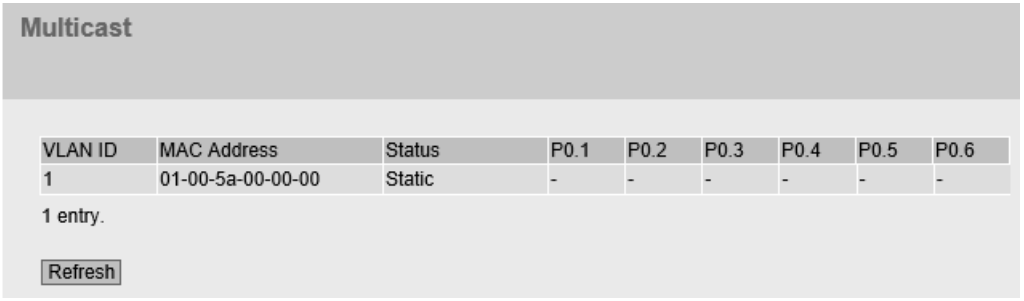
- **VLAN ID**
  Shows the VLAN-ID assigned to this MAC address.
- **MAC Address**
  Shows the MAC address of the node that the device has learned or the user has configured.

- **Status**
  Shows the status of each address entry:
  - Static
    Configured by the user. Static addresses are stored permanently; in other words, they are not deleted when the aging time expires or on a restart.
  - Invalid
    These values are not evaluated.
- **Port**
  Shows the port via which the node with the specified address can be reached. Frames received by the device whose destination address matches this address will be forwarded to this port.

4.3.15 Multicast

Status of the multicast filter table

This table shows the multicast frames currently entered in the multicast filter table and their destination ports. The entries are configured statically by the user.



Description of the displayed values

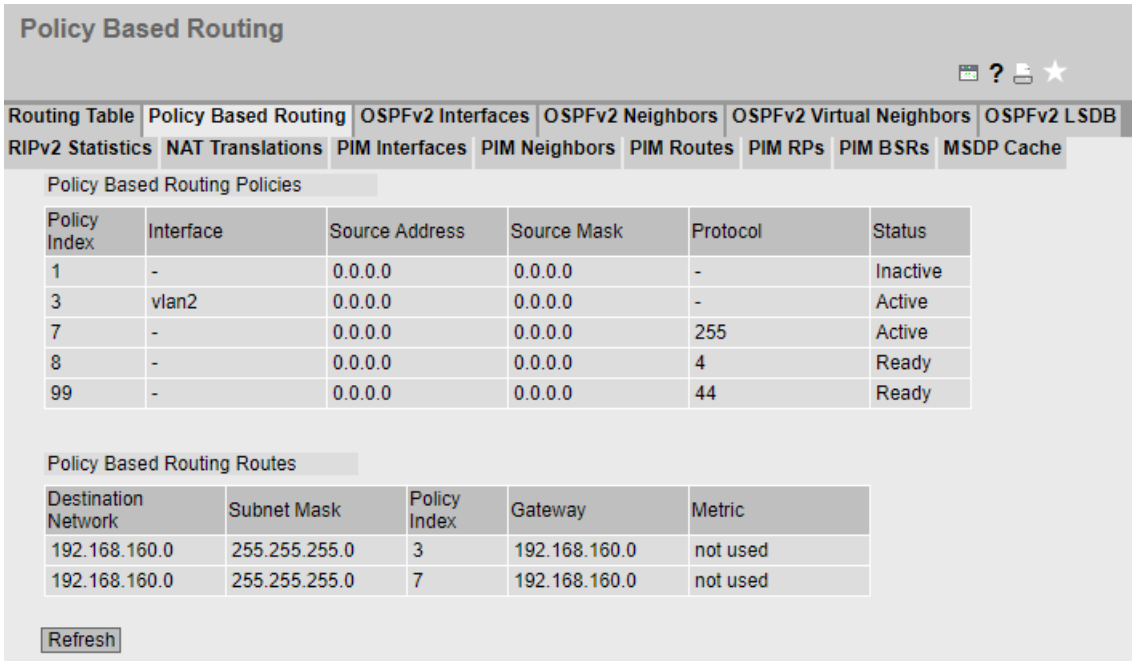
The table contains the following columns:

- **VLAN ID**
  Shows VLAN ID of the VLAN to which the MAC multicast address is assigned.
- **MAC Address**
  Shows the MAC multicast address that the device has learned or the user has configured.
- **Status**
  Shows the status of each address entry. The following information is possible:
  - Static
    The address was entered statically by the user. Static addresses are stored permanently; in other words, they are not deleted when the aging time expires or when the device is restarted. These must be deleted by the user.

4.3.16 Policy Based Routing

Overview

This page shows which policies and which routes were configured for Policy Based Routing.



Description of the displayed boxes

The "Policy Based Routing Policies" table has the following columns:

- **Policy Index**
  Shows the number of the PBR policy.
- **Interface**
  Shows the interface to which the PBR policy applies.
- **Source Address**
  Shows the source address of the network or device to which the PRB policy applies.
- **Source Subnet Mask**
  Shows the source subnet mask of the network or device to which the PBR policy applies.

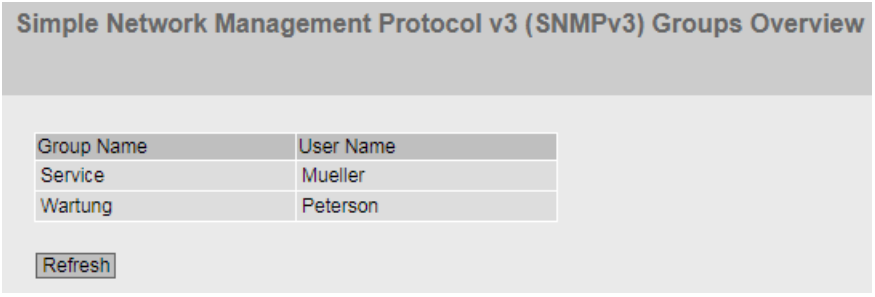
- **Protocol**
  Shows the number of the Layer 4 protocol to which the PBR policy applies.
- **Status**
  Shows the status of the PBR policy.
  - Inactive
    The PBR policy has been created but not completely configured. In this status, the PBR policy cannot be linked to a PBR route.
  - Ready
    The PBR policy is completely configured and can be linked to a PBR route.
  - Active
    The PBR policy is linked to a PBR route.

The "Policy Based Routing Routes" table has the following columns:

- **Destination Network**
  Shows the IP address of the destination network.
- **Subnet Mask**
  Shows the subnet mask of the destination network.
- **Policy Index**
  Shows the number of the PBR policy.
- **Gateway**
  Shows the gateway for this route.
- **Metric**
  Shows the routing metric to the destination network.

4.3.17 SNMP

This page displays the created SNMPv3 groups. You configure the SNMPv3 groups in "System > SNMP".



Description

The table has the following columns:

- **Group Name**
  Shows the group name.
- **User Name**
  Shows the user that is assigned to the group.

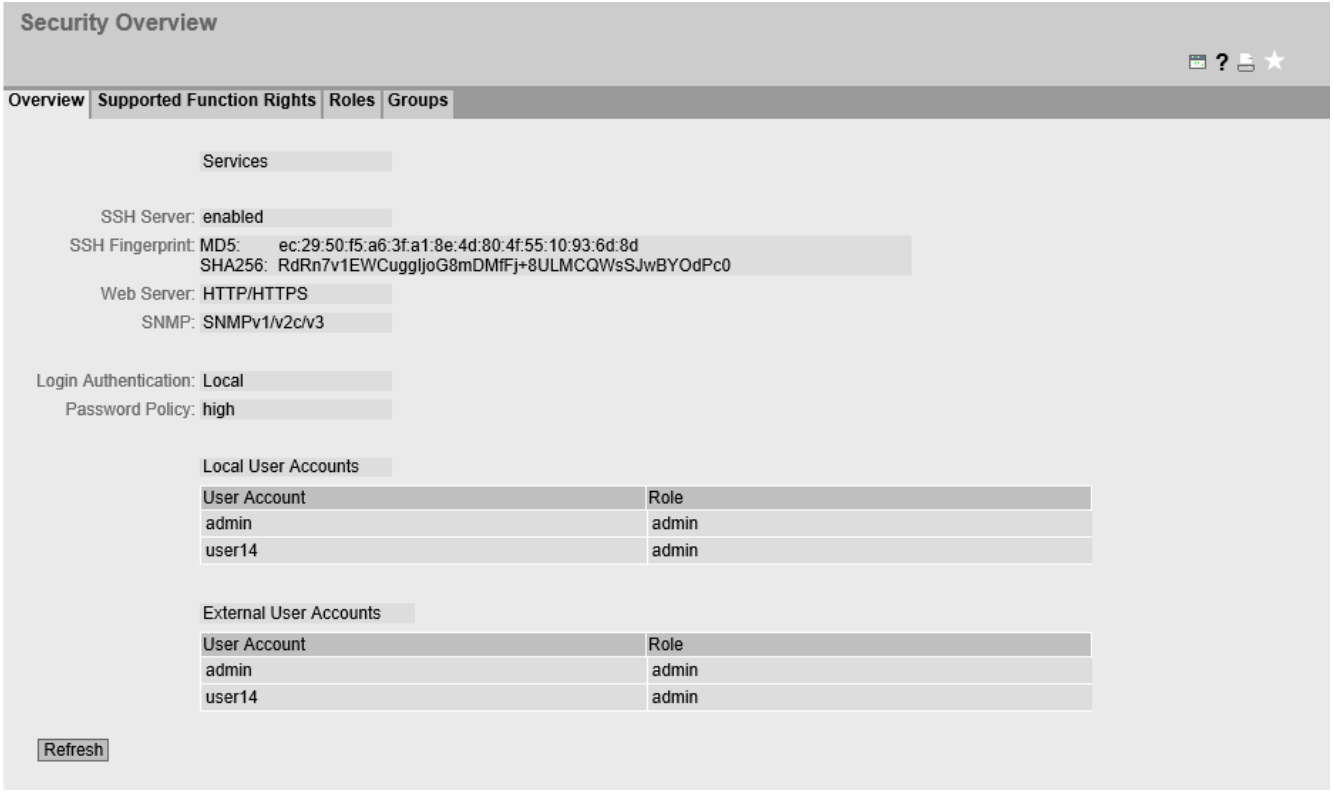
4.3.18 Security

4.3.18.1 Overview

Note

The values displayed depend on the rights of the logged-in user.

This page shows the security settings and the local and external user accounts.



Description

Services

The "Services" list shows the security settings.

- **SSH Server**
  You configure the setting in "System > Configuration".
  - Enabled: Encrypted access to the CLI.
  - Disabled: No encrypted access to the CLI.
- **SSH Fingerprint x**
  The following SSH fingerprints are displayed:
  - MD5
  - SH256

  You can uniquely identify the device with the fingerprint shown.
- **Web Server**
  You configure the setting in "System > Configuration".
  - HTTP/HTTPS: Access to the WBM is possible with HTTP and HTTPS.
  - HTTPS: Access to the WBM is now only possible with HTTPS.
- **SNMP**
  You can configure setting in "System > SNMP > General".
  - "-" (SNMP disabled)
    Access to device parameters via SNMP is not possible.
  - SNMPv1/v2c/v3
    Access to device parameters is possible with SNMP versions 1, 2c or 3.
  - SNMPv3
    Access to device parameters is possible only with SNMP version 3.
- **Login Authentication**
  You configure the setting in "Security > AAA > General".
  - Local
    The authentication must be made locally on the device.
  - RADIUS
    The authentication must be handled via a RADIUS server.
  - Local and RADIUS
    The authentication is possible both with the users that exist on the device (user name and password) and via a RADIUS server.
    The user is first searched for in the local database. If the user does not exist there, a RADIUS query is sent.
  - RADIUS and fallback local
    The authentication must be handled via a RADIUS server.
    A local authentication is performed only when the RADIUS server cannot be reached in the network.
- **Password Policy**
  Shows which password policy is currently being used.

Local and external user accounts

You configure local user accounts and roles in "Security > Users".

When you create a local user account an external user account is generated automatically.

Local user accounts involve users each with a password for logging in on the device.

In the table "External User Accounts" a user is linked to a role. In this example the user "Observer" is linked to the "user" role. The user is defined on a RADIUS server. The role is defined locally on the device. When a RADIUS server authenticates a user, the corresponding group however is unknown or does not exist, the device checks whether or not there is an entry for the user in the table "External User Accounts". If an entry exists, the user is logged in with the rights of the associated role. If the corresponding group is known on the device, both tables are evaluated. The user is assigned the role with the higher rights.

Note

The table "External User Accounts" is only evaluated if you have set "SiemensVSA" in the RADIUS Authorization Mode.

With CLI you can access external user accounts.

The "Local User Accounts" and "External User Accounts" tables have the following columns:

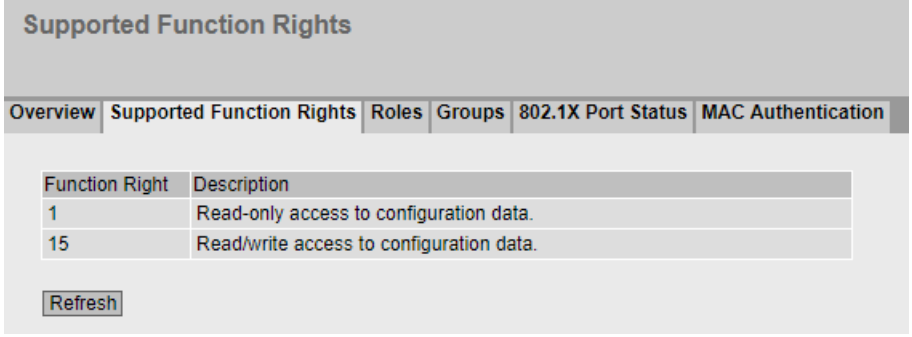
- **Account**
  Shows the name of the local user.
- **Role**
  Shows the role of the user. You can obtain more information on the function rights of the role in "Information > Security > Roles".

4.3.18.2 Supported Function Rights

Note

The values displayed depend on the role of the logged-on user.

The page shows the function rights available locally on the device.



Description of the displayed values

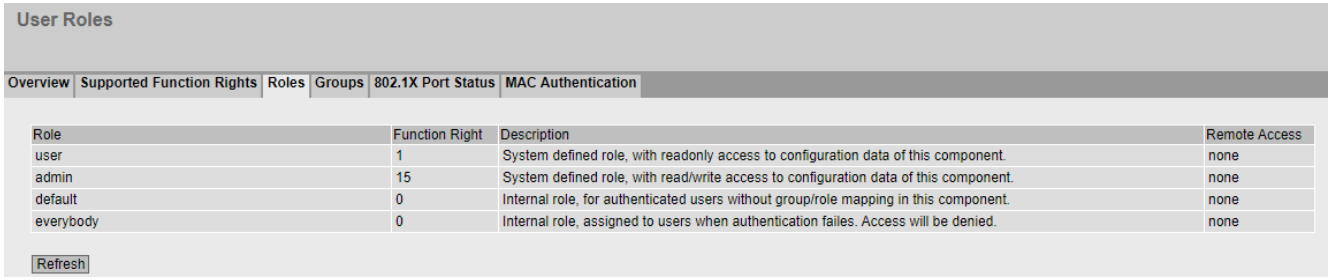
- **Function Right**
  Shows the number of the function right. Different rights relating to the device parameters are assigned to the numbers.
- **Description**
  Shows the description of the function right.

4.3.18.3 Roles

Note

The values displayed depend on the role of the logged-on user.

The page shows the roles valid locally on the device.



Description

The table contains the following columns:

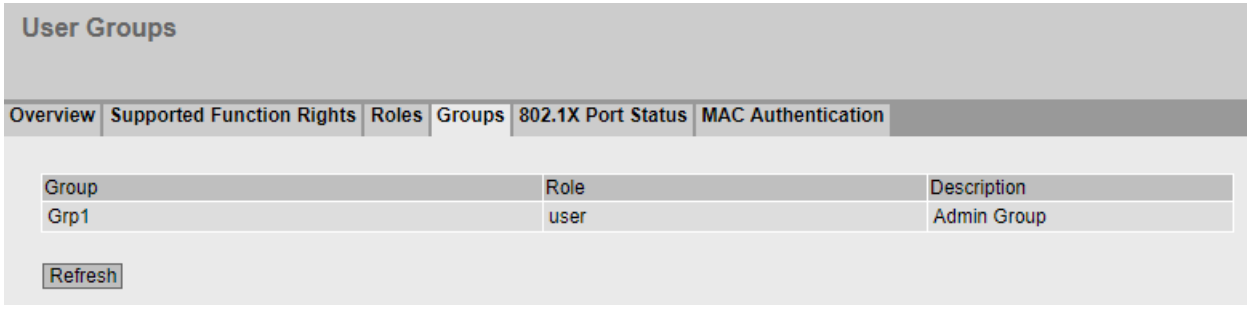
- **Role**
  Shows the name of the role.
- **Function Right**
  Shows the function right of the role:
  - 1
    Users with this role can read device parameters but cannot change them.
  - 15
    Users with this role can both read and change device parameters.
  - 0
    This is a role that the device assigns internally when a user could not be authenticated. The user is denied access to the device.
- **Description**
  Shows a description of the role.
- **Remote Access**
  Shows which remote access is currently being used.

4.3.18.4 Groups

Note

The values displayed depend on the role of the logged-on user.

This page shows which group is linked to which role. The group is defined on a RADIUS server. The role is defined locally on the device.



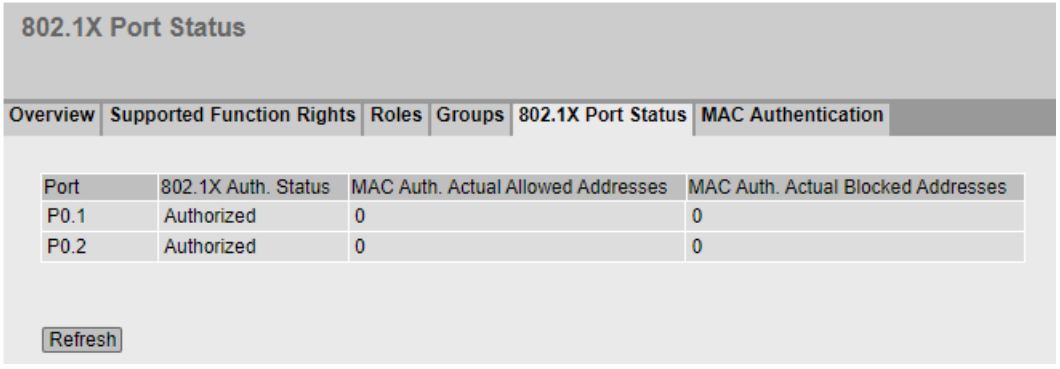
Description of the displayed values

The table has the following columns:

- **Group**
  Shows the name of the group. The name matches the group on the RADIUS server.
- **Role**
  Shows the name of the role. Users who are authenticated with the linked group on the RADIUS server receive the rights of this role locally on the device.
- **Description**
  Shows a description for the link.

4.3.18.5 802.1X Port Status

This page shows the status of 802.1X authentication as well as the MAC authentication for the individual ports.



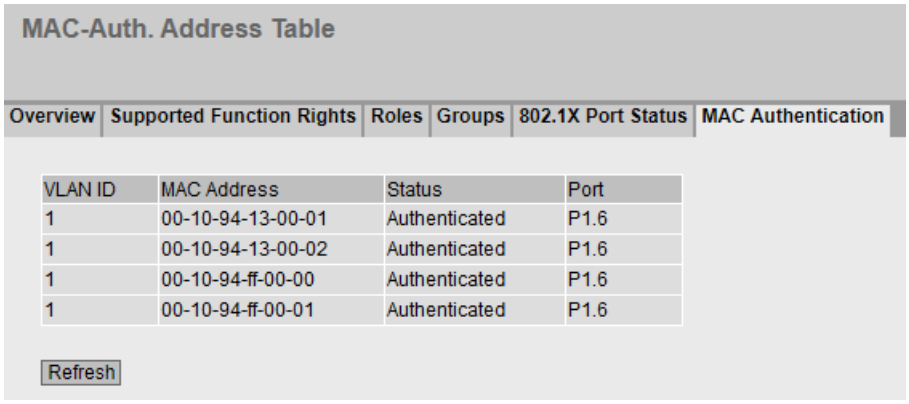
Description

The table has the following columns:

- **Port**
  All ports of the device are displayed in this column.
- **802.1X Auth. Status**
  The authentication status of the node. The following options are possible:
  - Authorized
    Data traffic via the port is possible after successful authentication with the "802.1X" method.
  - Unauthorized
    Data traffic via the port is not possible because no authentication has taken place with the "802.1X" method yet or the authentication method was not successful.
- **MAC Auth. Port Status**
  Shows the status of the MAC authentication for the port. The following options are possible:
  - -
    MAC authentication was disabled for the port.
  - Individual
    MAC authentication is configured for the port. Clients can be authenticated individually with their MAC address.
  - Blocked
    MAC authentication is configured for the port. Clients are not authenticated individually. The first client that is authenticated opens the port for all clients. No client is authenticated yet.
  - Open
    MAC authentication is configured for the port. Clients are not authenticated individually. The first client that is authenticated opens the port for all clients. The port was opened after successful authentication of a client.
- **MAC Auth. Actual Allowed Addresses**
  Shows the number of nodes that are allowed access after successful MAC authentication.
- **MAC Auth. Actual Blocked Addresses**
  Shows the number of nodes that are allowed access after failed MAC authentication.

4.3.18.6 MAC Authentication

This page shows the MAC addresses for which MAC authentication was performed.



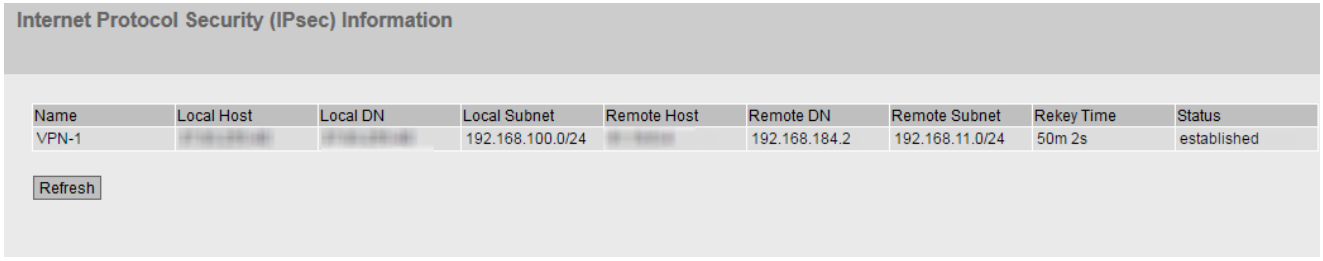
Description

The table has the following columns:

- **VLAN ID**
  Shows the VLAN ID assigned to this MAC address.
- **MAC Address**
  Shows the MAC address of the node for which the authentication status is displayed.
- **Status**
  The authentication status of the node. The following options are possible:
  - **Authorized**
    Data traffic via the port is possible after successful authentication with the "MAC Authentication" method.
  - **Unauthorized**
    Data traffic via the port is not possible because no authentication has taken place with the "MAC Authentication" method yet or the authentication method was not successful.
- **Port**
  Shows the port via which the node with the specified address can be reached.

4.3.19 IPSec VPN (SC64x-2C)

The WBM page shows the status of the activated VPN connections.



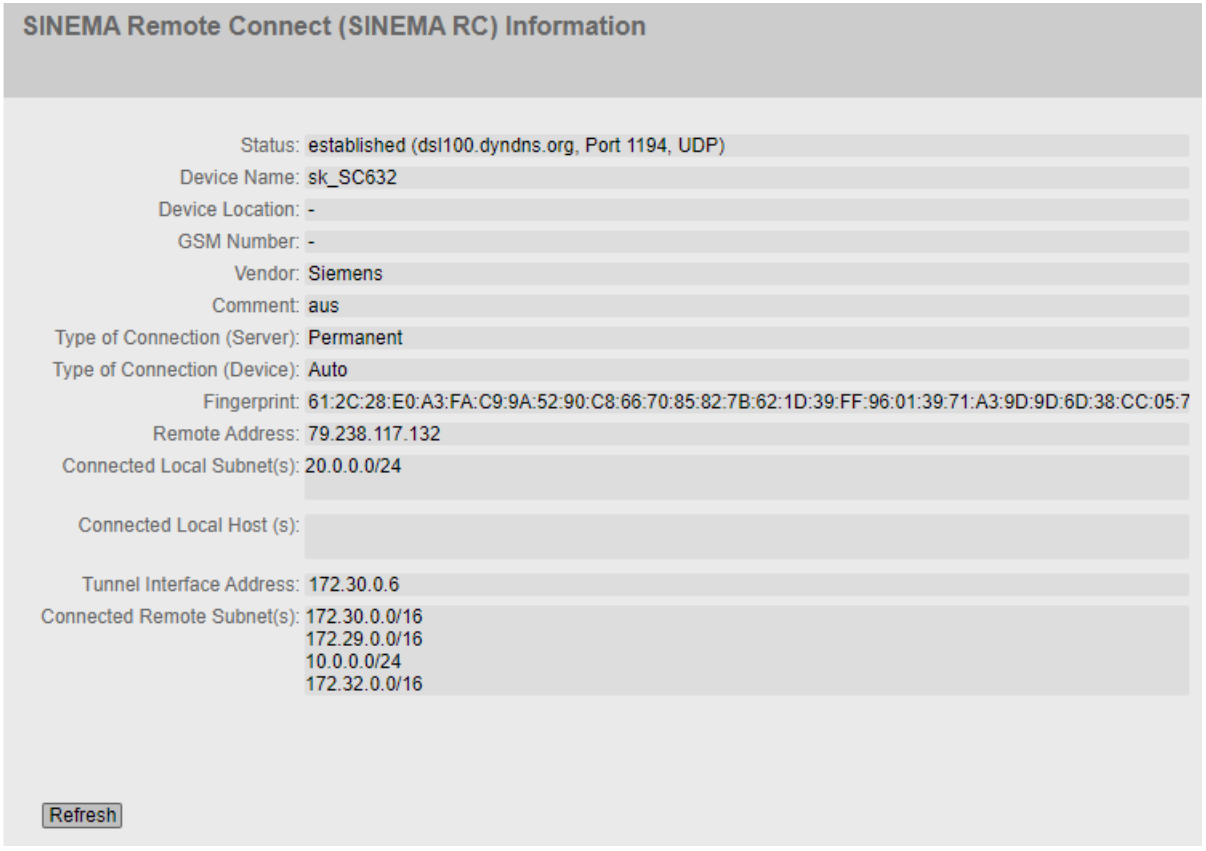
Description of the displayed values

The table contains the following columns:

- **Name**
  Shows the name of the VPN connection.
- **Local Host**
  Shows the IP address of the device.
- **Local DN**
  Shows the Distinguished Name (DN) of the device that was signaled to the remote station during connection establishment. The entry is adopted from the "Local ID" box, the device certificate or the IP address of the device.
- **Local Subnet**
  Shows the local subnet.
- **Remote Host**
  Shows the IP address or the host name of the remote device.
- **Remote DN**
  Shows the Distinguished Name (DN) signaled by the remote device during connection establishment.
- **Remote Subnet**
  Shows the remote subnet.
- **Rekey Time**
  Shows when the validity of the key expires.
- **Status**
  Shows the status of the VPN connection.

4.3.20 SINEMA RC

Shows information on SINEMA RC Server



Description of the displayed values

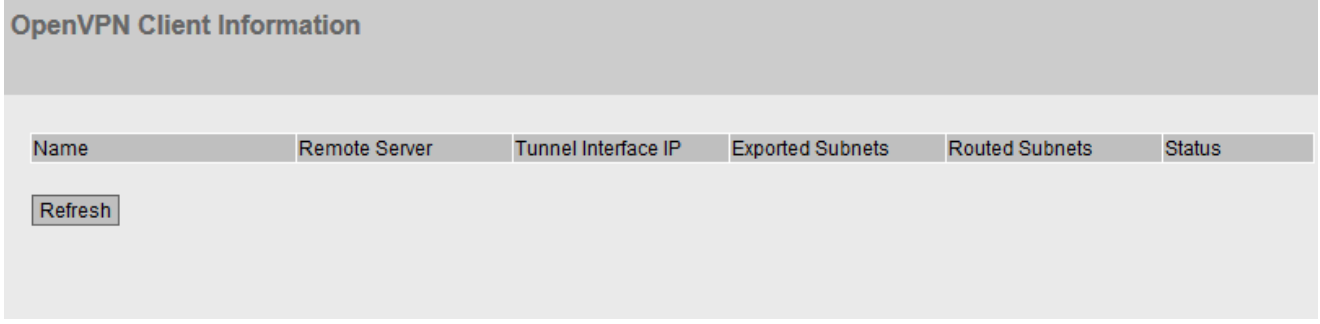
- **Status**
  Shows the status of the connection to SINEMA RC Server.
- **Device Name**
  If configured, the name of the device is displayed.
- **Device Location**
  If configured, the location of the device is displayed.
- **GSM Number**
  If configured, the phone number of the device is displayed.
- **Vendor**
  If configured, the entry is displayed.
- **Comment**
  If configured, the comment is displayed.
- **Type of Connection (Server)**
  Shows which type of connection is set on the SINEMA RC Server.

- **Type of Connection (Device)**
  Shows which type of connection is set on the device.
- **Fingerprint**
  Shows the fingerprint of the server certificate. Is only displayed when the fingerprint is used for verification.
- **Remote Address**
  Shows the IP address of the SINEMA RC Server.
- **Connected Local Subnet(s)**
  Shows the IP addresses of the local subnets. Is only displayed when the option "Connected local subnets" is enabled on the SINEMA RC Server. You will find further information on this in the Operating Instructions of the SINEMA RC Server.
- **Connected Local Host (s)**
  Shows the destination IP address of the hosts that can be reached.
- **Tunnel Interface Address**
  Shows the IP address of the virtual tunnel interface.
- **Connected Remote Subnet(s)**
  Shows the subnets of the SINEMA RC Server that are reachable for the device. Which subnets are reachable for the device depends on the communications relations on the SINEMA RC Server. You will find further information on this in the Operating Instructions of the SINEMA RC Server.

4.3.21 OpenVPN (SC64x-2C)

4.3.21.1 Client

The WBM page shows the status of the activated OpenVPN connections.



Description of the displayed values

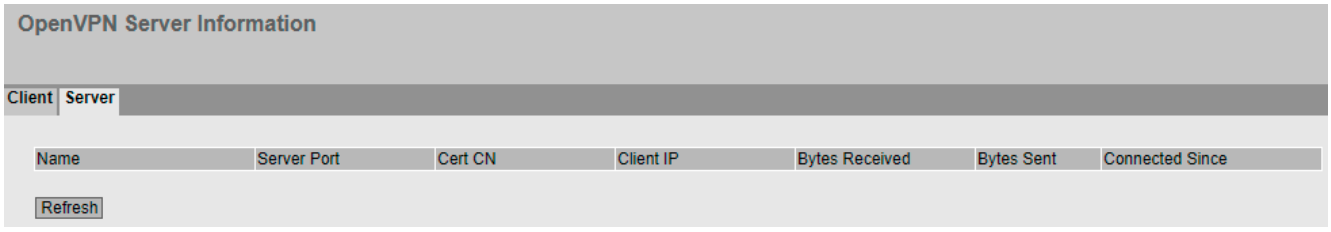
The table contains the following columns:

- **Name**
  Shows the name of the OpenVPN connection.
- **Remote Server**
  Shows the IP address or the hostname of the OpenVPN server.

- **Tunnel Interface IP**
  Shows the IP address of the virtual tunnel interface.
- **Exported Subnets**
  Shows the IP address of the local subnets.
- **Routed Subnets**
  Shows the subnets of the OpenVPN server.
- **Status**
  Shows the status of the OpenVPN connection.

4.3.21.2 Server

The WBM page shows the status of the activated OpenVPN server.



Description of the displayed values

The table contains the following columns:

- **Name**
  Shows the name of the OpenVPN server.
- **Server Port**
  Shows the port via which the OpenVPN server sends data.
- **Certificate CN**
  Shows the "Common Name" of the certificate used. The Common Name designates the domain for which the certificate is issued.
- **Client IP address**
  Shows the IP address of the OpenVPN server.
- **Received bytes**
  Shows how many bytes were received.
- **Sent bytes**
  Shows how many bytes were sent.
- **Connected since**
  Shows how long a connection has been present.

4.3.22 VXLAN (SC63x/SC64x)

Note

The page is only available if there is an online connection to the device.

This page shows the current content of the VXLAN NVE Peer table.

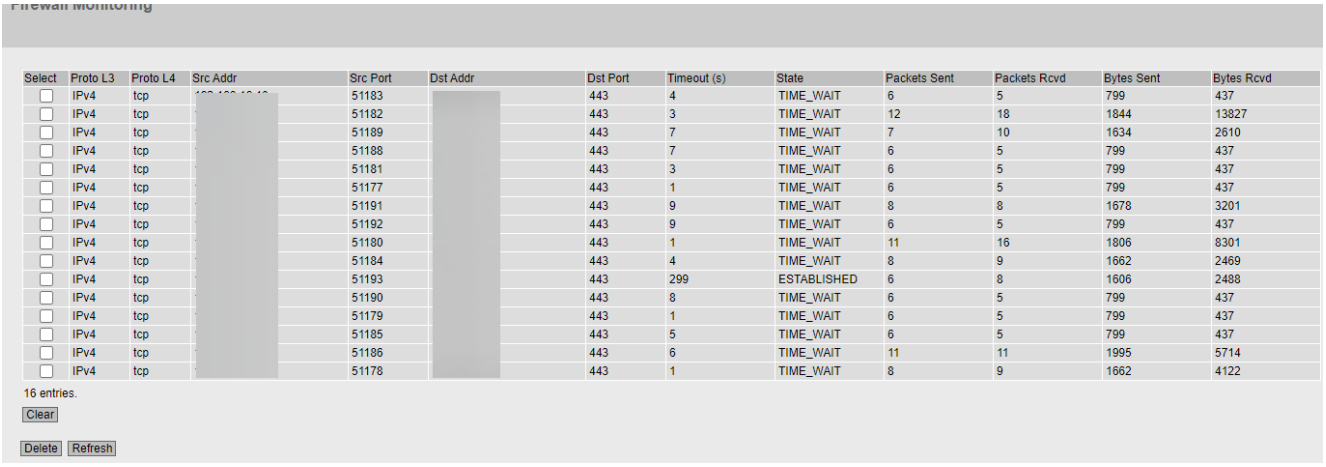
Description of the displayed values

The table contains the following columns:

- **Interface**
  Displays the NVE interface via which the row entry was learned.
- **Remote VTEP IP Address**
  Shows the IPv4 address of the remote VTEP.
- **VNI ID**
  Shows the VNI segment of which the remote VTEP is a member.
- **Remote MAC Address**
  Shows the MAC address of the remote VTEP that the device learned or that was configured.
- **MAC Type**
  Shows how the MAC address of the remote VTEP is obtained.
  - Static:
    The MAC and IP addresses were configured under "Layer 2 > VXLAN > Static MAC Addresses". The static addresses are stored permanently; in other words, they are not deleted when the aging time expires or when the device is restarted.
  - Dynamic:
    The VTEP of the device obtains the MAC address from the received frame.
- **ARP Suppression**
  This function is not supported.

4.3.23 Firewall monitoring

This page shows all connections currently running over the firewall (Firewall-State).



Select	Proto L3	Proto L4	Src Addr	Src Port	Dst Addr	Dst Port	Timeout (s)	State	Packets Sent	Packets Rcvd	Bytes Sent	Bytes Rcvd
☐	IPv4	tcp		51183		443	4	TIME_WAIT	6	5	799	437
☐	IPv4	tcp		51182		443	3	TIME_WAIT	12	18	1844	13827
☐	IPv4	tcp		51189		443	7	TIME_WAIT	7	10	1634	2610
☐	IPv4	tcp		51188		443	7	TIME_WAIT	6	5	799	437
☐	IPv4	tcp		51181		443	3	TIME_WAIT	6	5	799	437
☐	IPv4	tcp		51177		443	1	TIME_WAIT	6	5	799	437
☐	IPv4	tcp		51191		443	9	TIME_WAIT	8	8	1678	3201
☐	IPv4	tcp		51192		443	9	TIME_WAIT	6	5	799	437
☐	IPv4	tcp		51180		443	1	TIME_WAIT	11	16	1806	8301
☐	IPv4	tcp		51184		443	4	TIME_WAIT	8	9	1662	2469
☐	IPv4	tcp		51193		443	299	ESTABLISHED	6	8	1606	2488
☐	IPv4	tcp		51190		443	8	TIME_WAIT	6	5	799	437
☐	IPv4	tcp		51179		443	1	TIME_WAIT	6	5	799	437
☐	IPv4	tcp		51185		443	5	TIME_WAIT	6	5	799	437
☐	IPv4	tcp		51186		443	6	TIME_WAIT	11	11	1995	5714
☐	IPv4	tcp		51178		443	1	TIME_WAIT	8	9	1662	4122

16 entries.

Clear

Delete Refresh

Description

The table contains the following columns:

- **Select**
  Select the row you want to delete.
- **L3 protocol**
  Shows the Layer 3 protocol (e.g. IPv4 or IPv6) of the connection.
- **L4 protocol**
  Shows the Layer 4 protocol (e.g. TCP, UDP, ICMP) of the connection.
- **Source IP address**
  The IP address of the device that initiates the connection.
- **Source port**
  Source port from which the connection was initiated. With ICMP, the value is "0".
- **Destination IP address**
  IP address of the device to which the connection was established.
- **Destination port**
  Destination port to which the connection was established. With ICMP, the value is "0".
- **Timeout [s]**
  Time in seconds after which the connection is automatically terminated if no communication takes place.
- **Status**
  Status of the connection. Only relevant with TCP and SCTP.
- **Packets sent**
  Number of packets sent from this initiator via the connection.
- **Packets received**
  Number of packets sent from the destination device via this connection or received from the initiator.

- **Bytes sent**
  Number of packets sent from the initiator via this connection.
- **Bytes received**
  Number of bytes sent from the destination device via this connection or received from the initiator.

Description of the button

- **Clear**
  All active connections will be terminated and need to be established again.
- **Create**
  No function stored.
- **Delete**
  Deletes all selected connections.
- **Refresh**
  Updates the values of the table.

4.4 "System" menu

4.4.1 Configuration

System configuration

The WBM page contains the configuration overview of the access options of the device.

Specify the services that access the device. With some services, there are further configuration pages on which more detailed settings can be made.

The standard port can also be changed for some services.

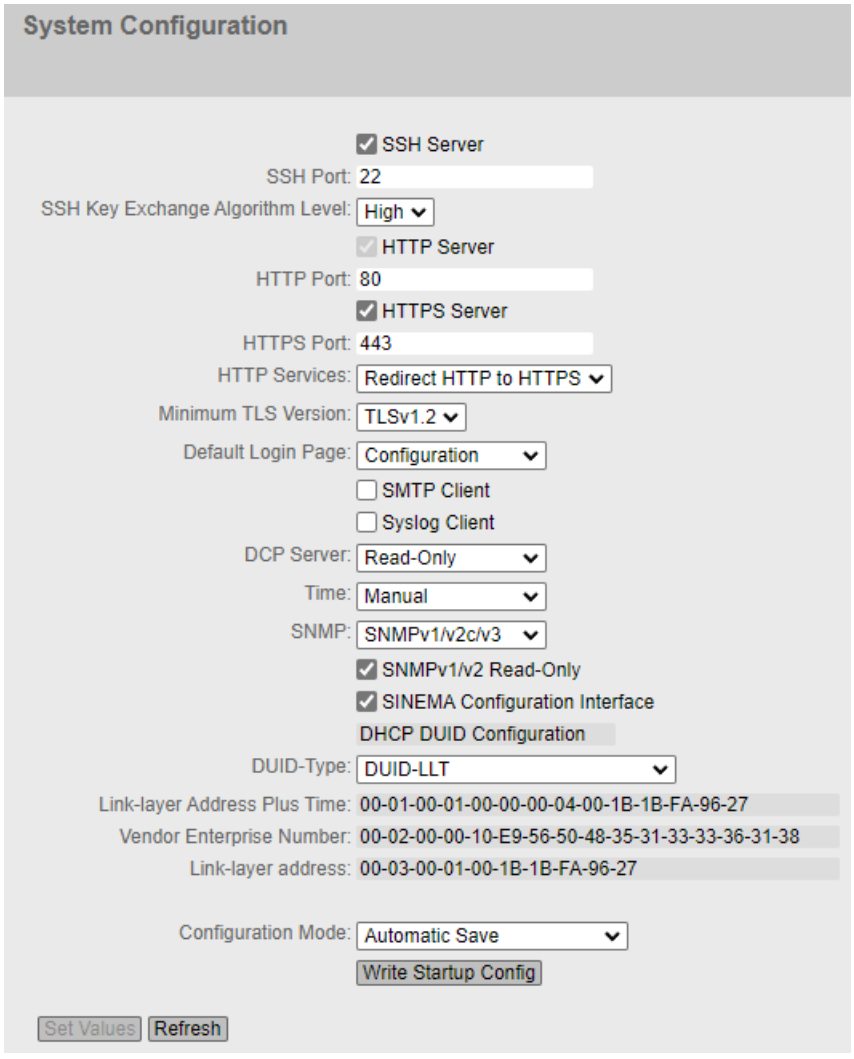
Note

Changing the standard port

Some programs can only access the service over the standard port, e.g. TIA Portal accesses HTTPS over standard port 443. Before you change the port, check which port the program uses. When you change the standard port, you must access the service over the changed port.

Firewall

The firewall is reinitialized after the ports are changed. This means that the changed ports are applied in the firewall rules. Existing connections, for example, via the dynamic firewall, can be used with restrictions during this time.



Description of the displayed boxes

The page contains the following boxes:

- **SSH Server**
  Enable or disable the "SSH Server" service for encrypted access to the CLI.
- **SSH Port**
  Specify the port for SSH access to the CLI.

- **SSH key exchange algorithm level**
  Configure the level of SSH key exchange algorithm for SSH access to the CLI.
  High (default)
  - Curve25519-sha256
  - Curve25519-sha256@libssh.org
  - Ecdh-sha2-nistp256
  - Ecdh-sha2-nistp384
  - Ecdh-sha2-nistp521
  - Diffie-hellman-group16-sha512
  - Diffie-hellman-group18-sha512

  Low
  - Curve25519-sha256
  - Curve25519-sha256@libssh.org
  - Ecdh-sha2-nistp256
  - Ecdh-sha2-nistp384
  - Ecdh-sha2-nistp521
  - Diffie-hellman-group16-sha512
  - Diffie-hellman-group18-sha512
  - Diffie-hellman-group14-sha256
  - Diffie-hellman-group14-sha1
- **HTTP Server**
  Enable or disable HTTP access to the WBM.
- **HTTP Port**
  Specify the port for HTTP access to the WBM.
- **HTTPS Server**
  Enable or disable HTTP access to the WBM.
- **HTTPS Port**
  Specify the port for HTTPS access to the WBM.
- **HTTP Services**
  Specify how the WBM is accessed:
  - HTTPS
    Access to the WBM is only possible with HTTPS.
  - Redirect HTTP to HTTPS
    Access via HTTP is automatically diverted to HTTPS.
- **Min. TLS version**
  Specify the minimum TLS version to be used.

- **Default Login Page**
  Specify the login page with which the WBM starts by default.
  - Firewall
    Logging into the WBM page for dynamic firewall.
  - Configuration
    Logging into the WBM.
- **SMTP Client**
  Enable or disable the SMTP client. You can configure other settings in "System > SMTP Client".
- **Syslog Client**
  Enable or disable the Syslog client. You can configure other settings in "System > Syslog Client".
- **DCP Server**
  Specify whether the device can be accessed with DCP (Discovery and Configuration Protocol):
  - "-" (disabled)
    DCP is disabled. Device parameters can neither be read nor modified.
  - Read/Write
    With DCP, device parameters can be both read and modified.
  - Read Only
    With DCP, device parameters can be read but cannot be modified.
- **Time**
  Select the setting from the drop-down list. The following settings are possible:
  - Manual
    The system time is set manually. You can configure other settings in "System > System Time > Manual Setting".
  - SIMATIC Time
    The system time is set via a SIMATIC time source. You can configure other settings in "System > System Time > SIMATIC Time Client".
  - SNTP Client
    The system time is set via an SNTP server. You can configure other settings in "System > System Time > SNTP Client".
  - NTP Client
    The system time is set via an NTP server. You can configure other settings in "System > System Time > NTP Client".
- **SNMP**
  Select the protocol from the drop-down list. The following settings are possible:
  - "-" (SNMP disabled)
    Access to device parameters via SNMP is not possible.
  - SNMPv1/v2c/v3
    Access to device parameters is possible with SNMP versions 1, 2c or 3. You can configure other settings in "System > SNMP > General".
  - SNMPv3
    Access to device parameters is possible only with SNMP version 3. You can configure other settings in "System > SNMP > General".

- **SNMPv1/v2 Read Only**
  Enable or disable write access to SNMP variables with SNMPv1/v2c.
- **SNMPv1 Traps**
  Enable or disable the sending of SNMPv1 traps (alarm frames). You can configure other settings in "System > SNMP > Traps".
- **SINEMA Configuration Interface**
  If the SINEMA configuration interface is enabled, you can download configurations to the device using STEP 7 Basic / Professional.
- **DUID-Type**
  Specify which DUID type will be used. The DUID types are defined in RFC 3315.
  - DUID-LLT
    DUID is based on the link-layer address of the interface and a time stamp.
  - DUID-EN
    DUID is assigned by the vendor (EN = enterprise number).
  - DUID-LL
    DUID is based on the link-layer address of the interface.
- **Link-layer Address Plus Time (LLT)**
  The value is based on the link-layer address of the interface and a time stamp. The value is regenerated each time the factory settings are restored.
- **Vendor Enterprise Number (EN)**
  The value is based on the enterprise number specific to the vendor. The value is regenerated each time the factory settings are restored.

- **Link-layer address (LL)**
  The link-layer address is based on the MAC address. The value is regenerated each time the factory settings are restored.
- **Configuration mode**
  Select the mode from the drop-down list. The following modes are possible:
  - Automatic Save
    Automatic backup mode. Approximately 1 minute after the last parameter change or before you restart the device, the configuration is automatically saved.
    In addition to this, the following message appears in the display area "Changes will be saved automatically in x seconds. Click 'Write Startup Config' to save the changes immediately."

    Note

    Interrupting the save

    Saving starts only after the timer in the message has elapsed. How long saving takes depends on the device.

    During the save, the message "Saving configuration data in progress. Please do not switch off the device." is displayed.

    - Do not switch off the device immediately after the timer has elapsed.
  - Trial
    Trial mode. In Trial mode, although changes are adopted, they are not saved in the configuration file (startup configuration).
    To save changes in the configuration file, use the "Write startup config" button. The display area also shows the message "Trial Mode Active – Press the "Write Startup Config" button to make your settings persistent" as soon as there are unsaved modifications. This message can be seen on every WBM page until the changes made have either been saved or the device has been restarted.

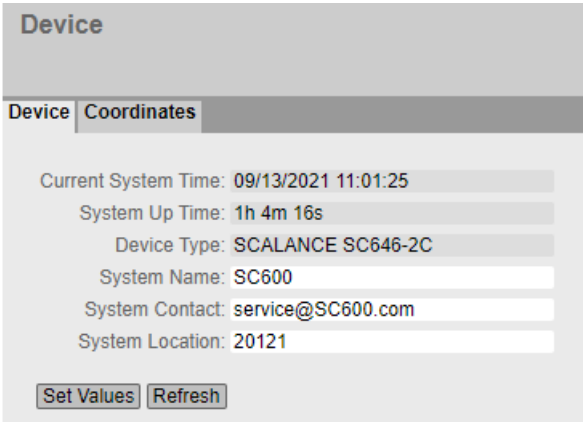
Procedure

1. To use the required function, select the corresponding check box.
2. Select the options you require from the drop-down lists.
3. Click the "Set Values" button.

4.4.2 General

4.4.2.1 Devices

This WBM page contains the general device information.



Description

The WBM page contains the following boxes:

- **Current System Time**
  Shows the current system time. The system time is either set by the user or by a time-of-day frame: either SIMATIC time-of-day frame, NTP or SNTP.
- **System Up Time**
  Shows the operating time of the device since the last restart.
- **Device Type**
  Shows the type designation of the device.
- **System Name**
  You can enter the name of the device. The entered name is displayed in the selection area. A maximum of 255 characters are possible.
  The system name is also displayed in the CLI input prompt. The number of characters in the CLI input prompt is limited. The system name is truncated after 16 characters.

- **System Contact**
  You can enter the name of a contact person responsible for managing the device. A maximum of 255 characters are possible.
- **System Location**
  You can enter the location where the device is installed. The entered installation location is displayed in the selection area. A maximum of 255 characters are possible.

Note

Permitted characters

The following printable ASCII characters (0x20 to 0x7e) are permitted in the input fields **"System Name"**, **"System Contact"** and **"System Location"**:

- 0123456789
- A...Z a...z
- !"#$%&'()*+,-./:;<=>?@ [\]_{|}~^`

Procedure

1. Enter the contact person responsible for the device in the "System Contact" input box.
2. Enter the identifier for the location at which the device is installed in the "System Location" input box.
3. Enter the name of the device in the "System Name" input box.
4. Click the "Set Values" button.

Note: Steps 1 to 3 can also be performed with the SNMP Management Tool.

4.4.2.2 Coordinates

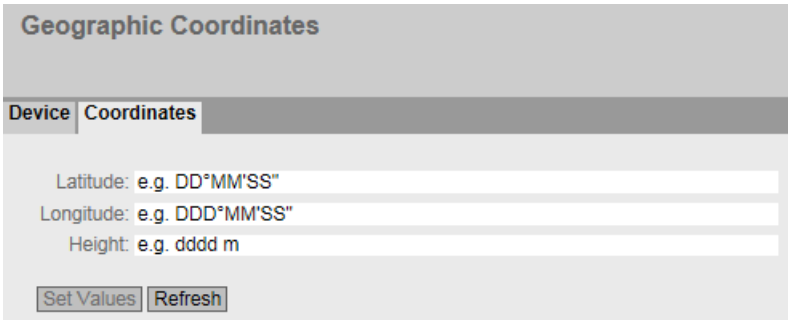
Information on geographic coordinates

In the "Geographic Coordinates" window, you can enter information on the geographic coordinates. The parameters of the geographic coordinates (latitude, longitude and the height above the ellipsoid according to WGS84) are entered directly in the input boxes of the "Geographic Coordinates" window.

Getting the coordinates

Use suitable maps for obtaining the geographic coordinates of the device.

The geographic coordinates can also be obtained using a GPS receiver. The geographic coordinates of these devices are normally displayed directly and only need to be entered in the input boxes of this page.



Description

The page contains the following boxes. These are purely information boxes with a maximum length of 32 characters.

- **"Latitude" input box**
  Geographical latitude: Here, enter the value for the northerly or southerly latitude of the location of the device.
  For example, the value +49° 1´31.67" means that the device is located at 49 degrees, 1 arc minute and 31.67 arc seconds northerly latitude.
  A southerly latitude is shown by a preceding minus character.
  You can also append the letters N (northerly latitude) or S (southerly latitude) to the numeric information (49° 1´31.67" N).
- **"Longitude" input box**
  Geographic longitude: Here, you enter the value of the eastern or western longitude of the location of the device.
  The value +8° 20´58.73" means that the device is located at 8 degrees, 20 minutes and 58.73 seconds east.
  A western longitude is indicated by a preceding minus sign.
  You can also add the letter E (easterly longitude) or W (westerly longitude) to the numeric information (8° 20´58.73" E).
- **Input box: "Height"**
  Height Here, you enter the value of the geographic height above sea level in meters.
  For example, 158 m means that the device is located at a height of 158 m above sea level.
  Heights below sea level (for example the Dead Sea) are indicated by a preceding minus sign.

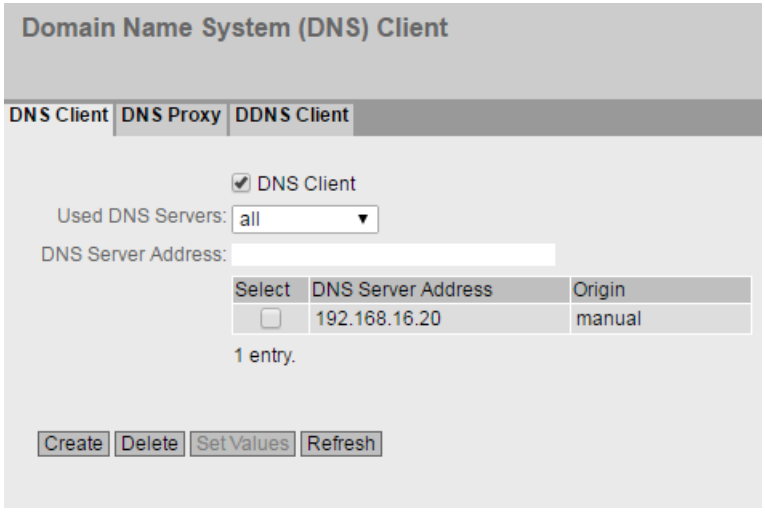
Procedure

1. Enter the calculated latitude in the "Latitude" input box.
2. Enter the calculated longitude in the "Longitude" input box.
3. Enter the height above sea level in the "Height" input box.
4. Click the "Set Values" button.

4.4.3 DNS

4.4.3.1 DNS client

On the WBM page you specify whether or not the device uses the DNS server of the network provider or another DNS server.



Description

The page contains the following boxes:

- **DNS client**
  Enable or disable depending on whether the device should operate as a DNS client.
- **Used DNS Servers**
  Specify which DNS server the device uses:
  - learned only
    The device uses only the DNS servers assigned by DHCP.
  - manual only
    The device uses only the manually configured DNS servers. The DNS servers must be connected to the Internet. A maximum of two DNS servers can be configured.
  - all
    The device uses all available DNS servers.
- **DNS Server Address**
  Enter the IP address of the DNS server.

The table has the following columns:

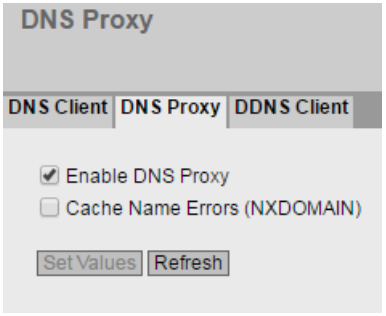
- **Select**
  Activate the check box in the row to be deleted

- **DNS Server Address**
  Shows the IP address of the DNS server.
- **Origin**
  Shows whether the DNS server was configured manually or was assigned by DHCP.

4.4.3.2 DNS proxy

The device provides a DNS server for the local network. If you enter the IP address of the device in the local application as a DNS server, then the device answers the DNS requests from its cache.

If the device does not know the IP address for a domain address, it forwards the query to an external DNS server. How long the device keeps a domain address in the cache depends on the host being addressed. In addition to the IP address, a DNS request to an external DNS server also supplies the life span of this information.



Description

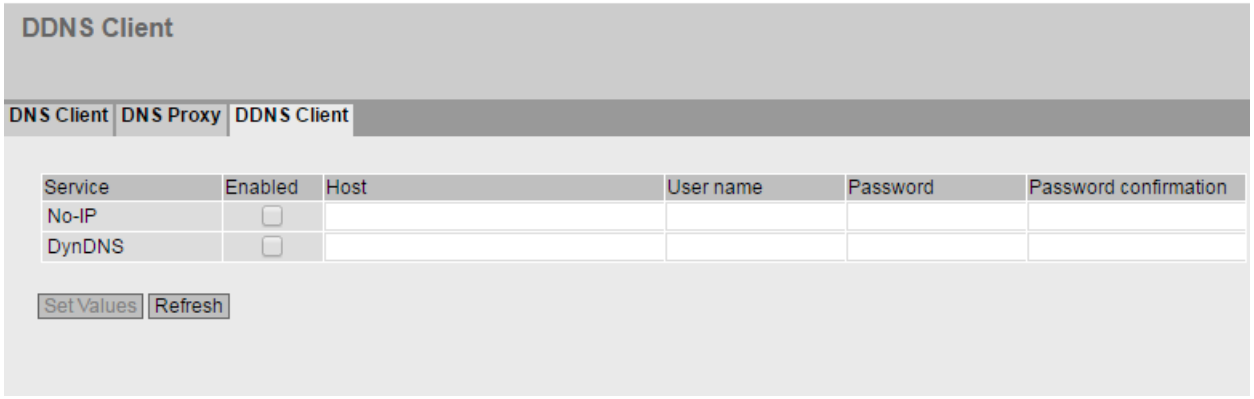
The page contains the following boxes:

- **Enable DNS Proxy**
  Enable or disable the proxy of the DNS server.
- **Cache Name Errors (NXDOMAIN)**
  Enable or disable the caching of NXDOMAIN replies. If you enable the option, the domain names that were unknown to the DNS server remain in the cache.

4.4.3.3 DDNS client

The DDNS (Dynamic Domain Name System) is an Internet service that allows a fixed hostname to be set up as a pseudonym for a dynamically changing IP address.

The DDNS client synchronizes the assigned IP address with the hostname registered at the DDNS provider. This means that the device can always be reached using the same hostname.



Description

The table has the following columns:

- **Service**
  Shows which providers are supported.
- **Enabled**
  When enabled, the device logs on to the DDNS server.
- **Host**
  Enter the host name that you have agreed with your DDNS provider for the device, e.g. example.no-ip-com.
- **User Name**
  Enter the user name with which the device logs on to the DDNS server.
- **Password**
  Enter the password assigned to the user.
- **Password Confirmation**
  Confirm the password**.**

Procedure

Requirement:

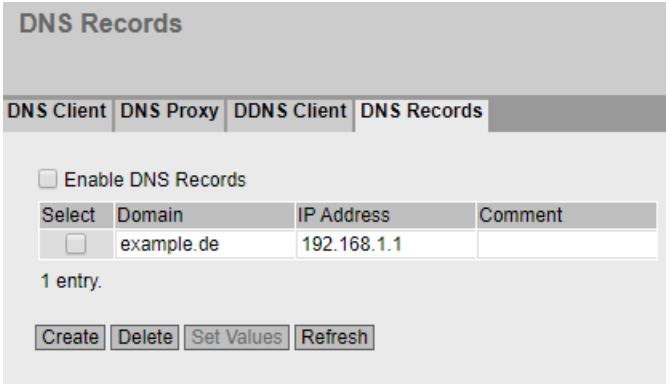
- User name and password that gives you the right to use the DDNS service.
- Registered hostname, e.g. example.no-ip.com
- UDP port 53 for DNS is enabled and is not used for NAPT.

1. In "Host", enter the hostname that you have agreed with your DDNS provider for the device, e.g. example.no-ip-com.
2. Enter the login data (user name, password) for the DDNS server.
3. Select "Enabled". This hostname is used for the device.
4. Click on "Set Values".

4.4.3.4 DNS Records

You configure a DNS address directory on this WBM page. To do this, enter the IPv4 address associated with an FQDN.

The device checks if there is an entry for DNS requests and converts the URL into the corresponding IPv4 address.



Description

The page contains the following boxes:

- **Enable DNS Records**
  When this is enabled, the address directory is used.

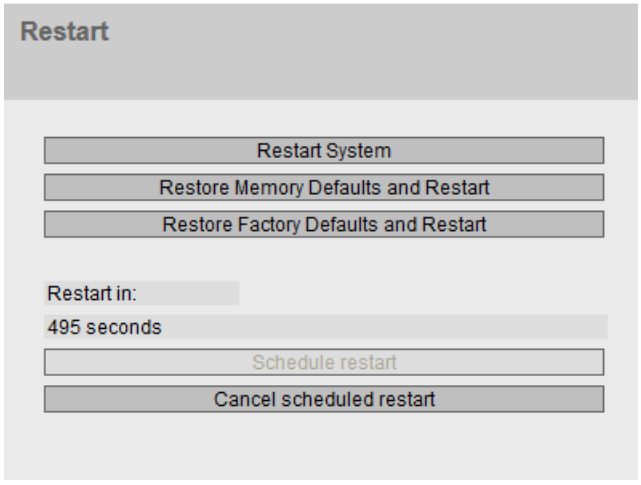
The table has the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **Domain**
  Enter the FQDN (Fully Qualified Domain Name).
- **IP Address**
  Enter the corresponding IPv4 address.
- **Comment**
  If needed, enter a comment.

4.4.4 Restart

Resetting to the defaults

Using the WBM page, you can restart the device manually or as scheduled. In addition, there are various options for resetting to the device defaults.



Note

Note the following points about restarting a device:

- You can only restart the device with administrator privileges.
- A device should only be restarted with the buttons of this menu and not by a power cycle on the device.
- If the device is in "Trial" mode, configuration modifications must be saved manually before a restart. Any modifications you have made only become active on the device after clicking the "Set values" button on the relevant WBM page.
- If the device is in "Automatic Save" mode, the last changes are saved automatically before a restart.

Description

To restart the device, the buttons on this page provide you with the following options:

- **Restart**
  Click this button to restart the system. You must confirm the restart in a dialog box. During a restart, the device is reinitialized, the internal firmware is reloaded, and the device runs a self-test. The settings of the start configuration are retained, e.g. the IP address of the device. The learned entries in the address table are deleted. You can leave the browser window open while the device restarts. After the restart you will need to log in again.
- **Restore Memory Defaults and Restart**
  Click this button to restore the factory defaults of the device with the exception of the following parameters and to restart the device:
  - IP addresses
  - Subnet mask
  - IP address of the default gateway
  - DHCP client ID
  - DHCP
  - System name
  - System location
  - System contact
  - Mode of the device
  - Login text
- **Restore Factory Defaults and Restart**
  Click this button to restore the factory defaults for the configuration. The protected defaults are also reset.
  An automatic restart is triggered.

  Note

  By resetting to the factory configuration settings, the device loses the IP address. This must then be reassigned.

- **Restart in**
  Specify the time after which the device restarts.

- **Schedule restart**
  When you click this button, a timer starts and runs backwards with the defined time. When the timer has expired, the device restarts.
  The following message is also displayed in the display area: "The automatic restart starts in [..] minutes. Click 'Cancel scheduled restart' to cancel the restart". This message can be seen on every WBM page until you cancel the restart or the SCALANCE device is restarted.

  Note

  Unsaved configuration is lost after restart

  The scheduled restart is performed after the time has elapsed without any further message. Unsaved configuration changes are lost.

- **Cancel scheduled restart**
  With this button you disable the timer for the scheduled restart.

See also

Requirements for operation (Page 27)

4.4.5 Load&Save

4.4.5.1 File list

Overview of the file types

Note

Extracting password-protected 7-Zip files

You extract password-protected files of the type ".7z" with the program "7-Zip". Extracting with "WinZip" is not possible.

Area	File type	Description	Down-load	Save	De-lete[1)]
Update	Firmware	The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be downloaded to the device.	X	X	--

Area	File type	Description	Download	Save	Delete[1)]
Configuration	Config	This file contains the start configuration. Among other things, this file contains the definitions of the users, roles, groups and function rights. The passwords are stored in the file "Users". The file can be supplied with a password before download. To load the file into the device successfully, use the specified password. You enter the password on the WBM page "Passwords". If the file is password-protected, you cannot load the file via DHCP with options 66 and 67.	X	X	--
	ConfigPack	Detailed configuration information, for example, startup configuration, users, certificates, favorites, firmware of the device (if saved as well). The file can be supplied with a password before download. To load the file into the device successfully, use the specified password. You enter the password on the WBM page "Passwords". For more detailed information on creating and using the ConfigPack incl. firmware, refer to the section "Maintenance". If the file is password-protected, you cannot load the file via DHCP with options 66 and 67.	X	X	--
	ConfigPack-Backup	This ZIP file stores all the configuration backups you have created.	X	X	X
	Firewall-NATConfig	Creates a .zip file with the firewall and NAT settings. The individual files are in *.csv format and can be opened with Excel.	--	X	--
	IPV4ACD_PRMS				
	LoginWelcomeMessage	File in *.txt format with a text for the login page. The content of the file can consist only of a maximum of 50 lines with a maximum of 255 ASCII characters.	X	X	X
	RunningCLI	Text file with CLI commands This file contains an overview of the current configuration in the form of CLI commands. Passwords are masked in this file as follows: [PASSWORD] You can download the text file. The file is not intended to be uploaded again unchanged.	--	X	--
	RunningSINEMAConfig	You save the current device configuration in this file type for transfer to STEP 7 Basic/ Professional. The file can be imported in STEP 7 Basic/Professional and installed on a device with the same article number and firmware version.	--	X	--

Area	File type	Description	Down-load	Save	De-lete[1)]
		Before you can save a file, you must assign a password for the "RunningSINEMAConfig" in the WBM under "System > Load&Save > Passwords". You also need this password to import the file into STEP 7 Basic/Professional. See also "SINEMAConfig"			
	Script	Text file with CLI commands You can upload a script file in a device. The CLI commands it contains are executed accordingly. CLI commands for saving and loading files cannot be executed with the CLI script file.	X	--	--
	SINEMA-Config	You load configuration data that was exported via STEP 7 Basic/Professional for transfer to the WBM with this file type. To load a file, you must assign a password for the "SINEMAConfig" under "System > Load&Save > Passwords". You also need this password to export the file from STEP 7 Basic/Professional. See also "RunningSINEMAConfig"	X	--	--
	TraceConfig				
	Users	This file contains the assignment of the user names to the corresponding passwords.	X	X	--
	WBMFav	WBM favorites This file contains the favorites that you created in the WBM. You can download this file and upload it in other devices.	X	X	X

Area	File type	Description	Down-load	Save	De-lete[1)]
Certificate & Key	HTTPSCert	Default HTTPS certificates including key The preset and automatically created HTTPS certificates are self-signed. We strongly recommend that you create your own HTTPS certificates and make them available. We recommend that you use HTTPS certificates signed either by a reliable external or by an internal certification authority. The HTTPS certificate checks the identity of the device and controls the encrypted data exchange. The following file types can be loaded into the device. • .pem To successfully load an HTTPS certificate with this data type into the device, the certificate must include the unencrypted private key. • .p12 For HTTPS certificates with this file type, the private key is encrypted and secured with a password. To load the certificate successfully into the device, enter the password specified for the file on the WBM page "Passwords". **We recommend using password-protected certificates in PKCS#12 format with a key length of at least 4096 bits.** Maximum key length: 8192 bits	X	X	X
	SSHPrivate-KeyECDSA	SSH private key (ECDSA) The SSH key ecdsa-sha2-nistp521 is supported. There are files to which access is password-protected. To successfully load the file into the device, enter the password specified for the file on the WBM page "Passwords".	X	X	X
	SSHPrivate-KeyRSA	SSH private key (RSA) with and without password The following SSH keys are supported: • rsa-sha2-512 • rsa-sha2-256 There are files to which access is password-protected. To successfully load the file into the device, enter the password specified for the file on the WBM page "Passwords".	X	X	X
	X509Cert	Various nodes are certified with certificates. The following file types can be loaded into the device:	X	X	--

Area	File type	Description	Down-load	Save	De-lete[1)]
		• .crt, pem, zip: Maximum file name length 255 characters • .p12: Maximum file name length 248 characters There are files to which access is password-protected. To successfully load the file into the device, enter the password specified for the file on the WBM page "Passwords". The loaded files are listed in "Security > Certificates > Overview". For more information on certificates, refer to section "Certificates".			
Services & log	Debug	This file contains information for Siemens Support. It is encrypted and can be sent by e-mail to Siemens Support without any security risk.	--	X	X
	LogFile	File with entries from the event log table	--	X	--
	StartupInfo	Startup log file This file contains the messages that were entered in the log file during the last startup.	--	X	--
Information	MIB	Private MSPS MIB file "Scalance_s600_msps.mib"	--	X	--
Licenses	LicenseConditions	ZIP file with the open source software license conditions.	--	X	--

1) Deletion is only possible via HTTP/HTTPS.

See also

Overview (Page 375)

Passwords (Page 172)

Certificates (Page 66)

4.4.5.2 HTTP

Loading and saving data via HTTP

The WBM allows you to store device data in an external file on your client PC or to load such data from an external file from the PC to the devices. This means, for example, that you can also load new firmware from a file located on your Admin PC. On this page, the certificates required to establish a secure VPN connection can also be loaded.

Firmware

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

Configuration files

Note

Configuration files and Trial mode/Automatic Save

In "Automatic Save" mode, the data is saved automatically before the configuration files (ConfigPack and Config) are transferred.
In "Trial" mode, although the changes are adopted, they are not saved in the configuration files (ConfigPack and Config). Use the "Write Startup Config" button on the "System > Configuration" WBM page to save changes in the configuration files.

CLI script file

You can download existing CLI configurations (RunningCLI).

Note

The downloadable CLI script is not intended to be uploaded again unchanged.

CLI commands for saving and loading files cannot be executed with the CLI script file (Script).

Exchange of configuration data with STEP 7 Basic/Professional using a file

You use the two file types "RunningSINEMAConfig" and "SINEMAConfig" to exchange configuration data between a device (WBM) and STEP 7 Basic/Professional via a file.

Requirements:

- Same article number
- Same firmware version
- Password
  You assign the password in the WBM under "System > Load&Save > Passwords".

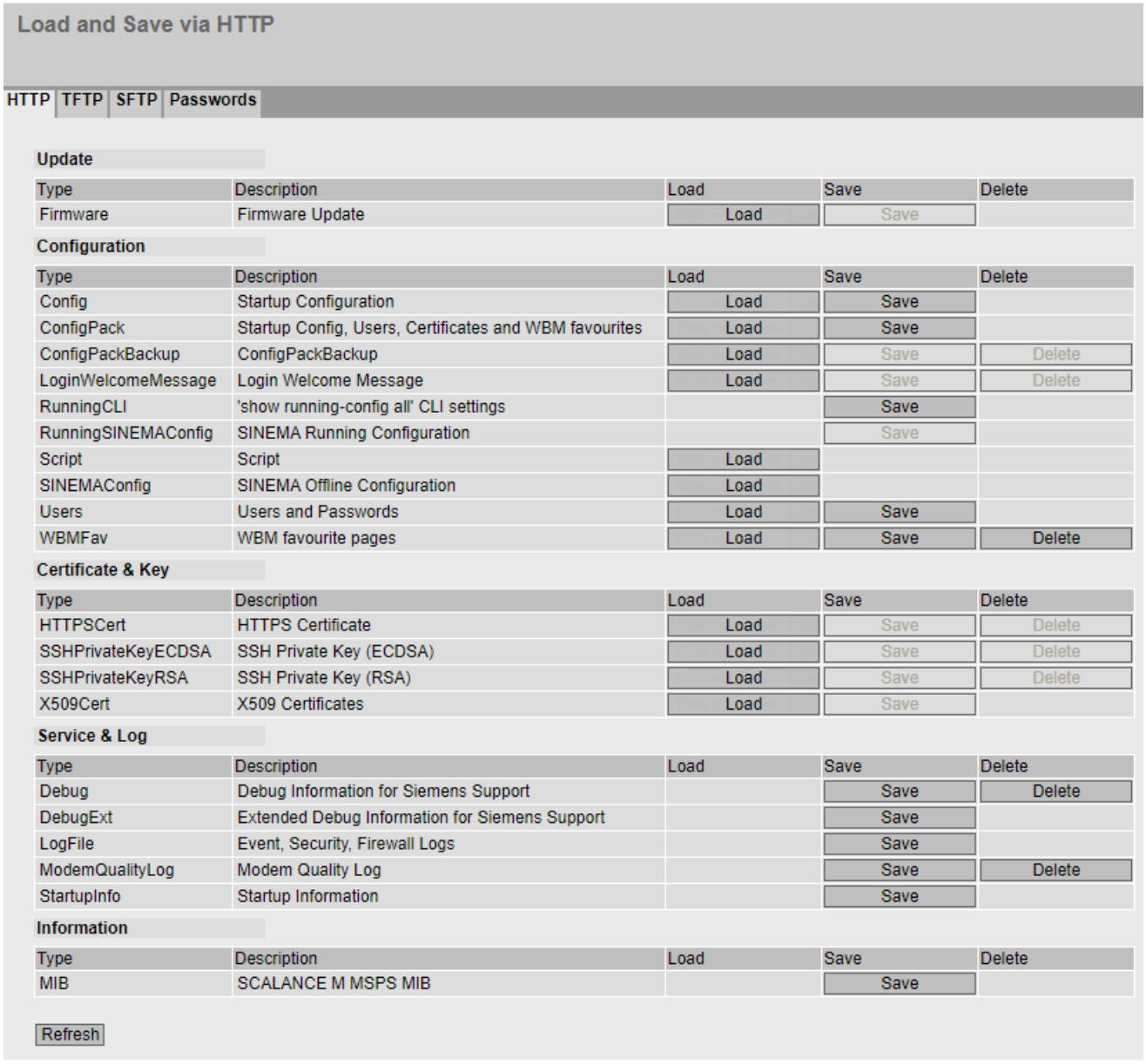
You can use the file types as follows:

- For offline diagnostics
  You can save the faulty configuration of a device as "RunningSINEMAConfig" via the WBM and import it in STEP 7 Basic/Professional. No connection to a real device is required for the diagnostics in STEP 7 Basic/Professional. You can export a corrected configuration and load it as "SINEMAConfig" again using the WBM.
- For configuration
  No connection to a real device is required to configure a device in STEP 7 Basic/Professional. You can export the configuration and load it as "SINEMAConfig" to the real device using the WBM.

X509 certificates

The following file types can be loaded into the device:

- .crt, pem, zip: Maximum file name length 255 characters
- .p12: Maximum file name length 248 characters



Description

The table has the following columns:

- **Type**
  Shows the file type.
- **Description**
  Shows the short description of the file type.
- **Load**
  With this button, you can upload files to the device. The button can be enabled, if this function is supported by the file type.

- **Save**
  With this button, you can download files from the device. The button can only be enabled if this function is supported by the file type and the file exists on the device.
- **Delete**
  With this button, you can delete files from the device. The button can only be enabled if this function is supported by the file type and the file exists on the device.

Note

Following a firmware update, delete the cache of your Internet browser.

Procedure

Uploading data using HTTP

1. Start the upload function by clicking one of the "Load" buttons.

   Note

   Files whose access is password protected

   To be able to load these files on the device successfully, you need to enter the password specified for the file in "System" > "Load&Save" > "Passwords".

   A dialog for uploading a file opens.
2. Select the required file and confirm the upload.
   The file is uploaded.
3. If a restart is necessary, a message to this effect will be output. Click the "OK" button and run the restart. If you click the "Abort" button, there is no device restart. The changes only take effect after a restart.

Downloading data using HTTP

1. Start the download by clicking the one of the "Save" buttons.
2. Select a storage location and a name for the file.
3. Save the file.
   The file is downloaded and saved.

Deleting files using HTTP

1. Start the delete function by clicking the one of the "Delete" buttons.
   The file is deleted.

Reusing configuration data

If several devices are to receive the same configuration and the IP addresses are assigned using DHCP, the effort for configuration can be reduced by saving and reading in the configuration data.

Follow the steps below to reuse configuration data:

1. Save the configuration data of a configured device on your PC.
2. Load these configuration files on all other devices you want to configure in this way.
3. If individual settings are necessary for specific devices, these must be made online on the relevant device.

Note

Configuration data has a checksum. If you edit the files, you can no longer upload them to the IE switch.

4.4.5.3 TFTP

Loading and saving data via a TFTP server

On this page, you can configure the TFTP server and the file names. The WBM also allows you to store device data in an external file on your client PC or to load such data from an external file from the PC to the devices. This means, for example, that you can also load new firmware from a file located on your Admin PC.

On this page, the certificates required to establish a secure VPN connection can also be loaded.

Firmware

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

Configuration files

Note

Configuration files and Trial mode/Automatic Save

In "Automatic Save" mode, the data is saved automatically before the configuration files (ConfigPack and Config) are transferred.
In "Trial" mode, although the changes are adopted, they are not saved in the configuration files (ConfigPack and Config). Use the "Write Startup Config" button on the "System > Configuration" WBM page to save changes in the configuration files.

CLI script file

You can download existing CLI configurations (RunningCLI) and upload your own CLI scripts (Script).

Note

The downloadable CLI script is not intended to be uploaded again unchanged.

CLI commands for saving and loading files cannot be executed with the CLI script file (Script).

Exchange of configuration data with STEP 7 Basic/Professional using a file

You use the two file types "RunningSINEMAConfig" and "SINEMAConfig" to exchange configuration data between a device (WBM) and STEP 7 Basic/Professional via a file.

Requirements:

- Same article number
- Same firmware version
- Password
  You assign the password in the WBM under "System > Load&Save > Passwords".

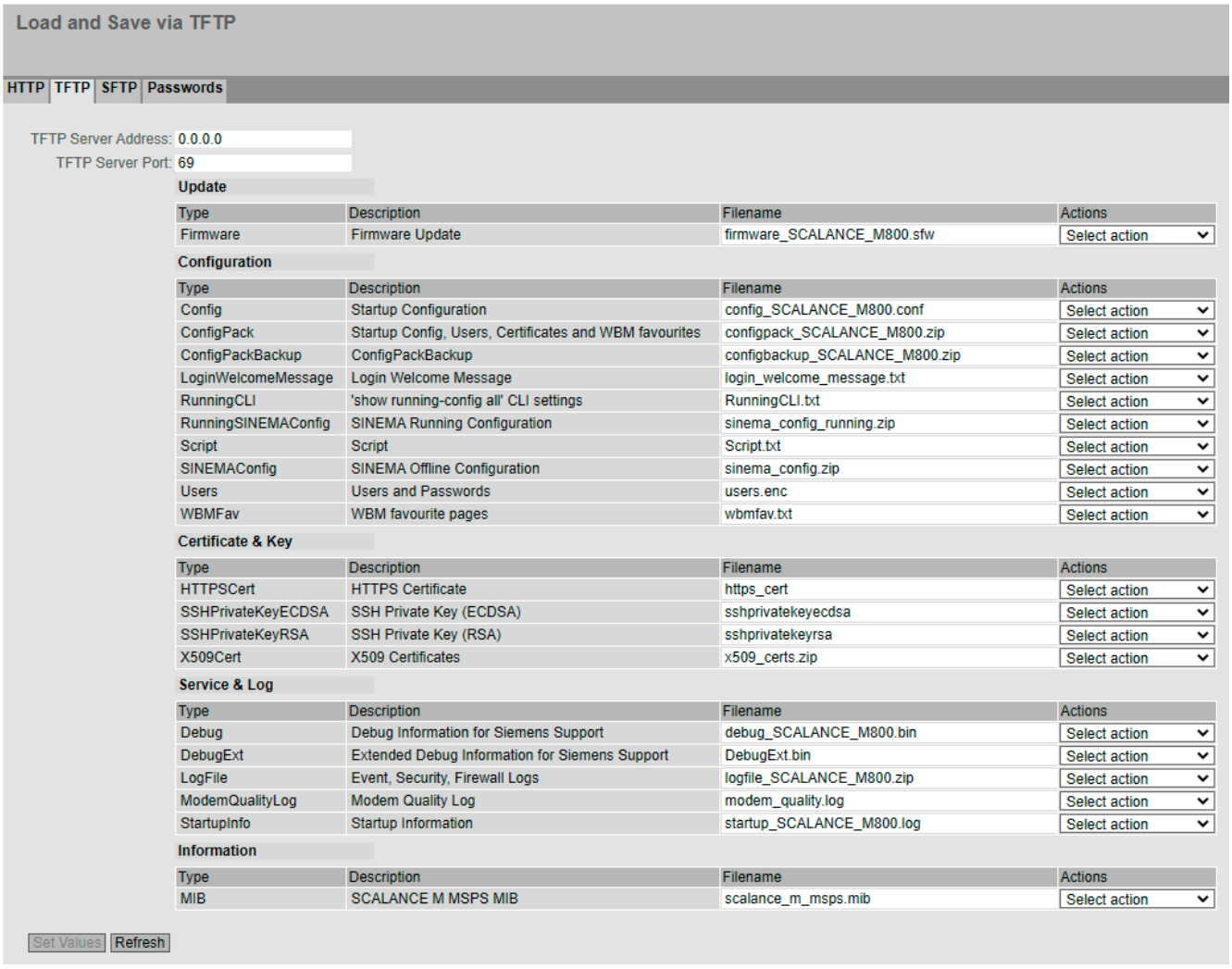
You can use the file types as follows:

- For offline diagnostics
  You can save the faulty configuration of a device as "RunningSINEMAConfig" via the WBM and import it in STEP 7 Basic/Professional. No connection to a real device is required for the diagnostics in STEP 7 Basic/Professional. You can export a corrected configuration and load it as "SINEMAConfig" again using the WBM.
- For configuration
  No connection to a real device is required to configure a device in STEP 7 Basic/Professional. You can export the configuration and load it as "SINEMAConfig" to the real device using the WBM.

X509 certificates

The following file types can be loaded into the device:

- .crt, pem, zip: Maximum file name length 255 characters
- .p12: Maximum file name length 248 characters



Description

The page contains the following boxes:

- **TFTP Server Address**
  Enter the IP address or the FQDN (Fully Qualified Domain Name) of the TFTP server with which you exchange data.
- **TFTP Server Port**
  Enter the port of the TFTP server via which data exchange will be handled. If necessary, you can change the default value 69 to your own requirements.

The table has the following columns:

- **Type**
  Shows the file type.
- **Description**
  Shows the short description of the file type.

- **Filename**
  A file name is preset here for every file type.

  Note

  Changing the file name

  You can change the file name preset in this column. After loading on the device, the changed file name can also be used with the Command Line Interface.

- **Actions**
  Select the action from the drop-down list. The selection depends on the selected file type, for example, the log file can only be saved.
  The following actions are possible:
  - **Save file**
    With this selection, you save a file on the TFTP server.
  - **Load file**
    With this selection, you load a file from the TFTP server.

Procedure

Loading or saving data using TFTP

1. Enter the address of the TFTP server in "TFTP server address".
2. Enter the port of the TFTP server to be used in "TFTP Server Port".
3. If applicable, enter the name of a file in which you want to save the data or take the data from in "Filename".

   Note

   Files whose access is password protected

   To be able to load these files on the device successfully, you need to enter the password specified for the file in "System" > "Load&Save" > "Passwords".

4. Select the action you want to execute from the "Actions" drop-down list.
5. Click "Set Values" to start the selected action.
6. If a restart is necessary, a message to this effect will be output. Click the "OK" button to run the restart. If you click the "Abort" button, there is no device restart. The changes only take effect after a restart.

Reusing configuration data

If several identical devices are to receive the same configuration and the IP addresses are assigned using DHCP, the effort for reconfiguration can be reduced by saving and reading in the configuration data.

Follow the steps below to reuse configuration data:

1. Save the configuration data of a configured device on your PC.
2. Load these configuration files on all other devices you want to configure in this way.
3. If individual settings are necessary for specific devices, these must be made online on the relevant device.

Note

Configuration data has a checksum. If you change the data, you can no longer upload it to the device.

4.4.5.4 SFTP

Loading and saving data via a SFTP server

SFTP (SSH File Transfer Protocol) transfers the files encrypted. On this page, you configure the access data for the SFTP server.

You can also store device data in an external file on your client PC or load such data from an external file from the PC to the devices. This means, for example, that you can also load new firmware from a file located on your Admin PC.

On this page, the certificates required to establish a secure VPN connection can also be loaded.

Firmware

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

Configuration files

Note

Configuration files and Trial mode/Automatic Save

In "Automatic Save" mode, the data is saved automatically before the configuration files (ConfigPack and Config) are transferred.
In "Trial" mode, although the changes are adopted, they are not saved in the configuration files (ConfigPack and Config). Use the "Write Startup Config" button on the "System > Configuration" WBM page to save changes in the configuration files.

CLI script file

You can download existing CLI configurations (RunningCLI) and upload your own CLI scripts (Script).

Note

The downloadable CLI script is not intended to be uploaded again unchanged.

CLI commands for saving and loading files cannot be executed with the CLI script file (Script).

Exchange of configuration data with STEP 7 Basic/Professional using a file

You use the two file types "RunningSINEMAConfig" and "SINEMAConfig" to exchange configuration data between a device (WBM) and STEP 7 Basic/Professional via a file.

Requirements:

- Same article number
- Same firmware version
- Password
  You assign the password in the WBM under "System > Load&Save > Passwords".

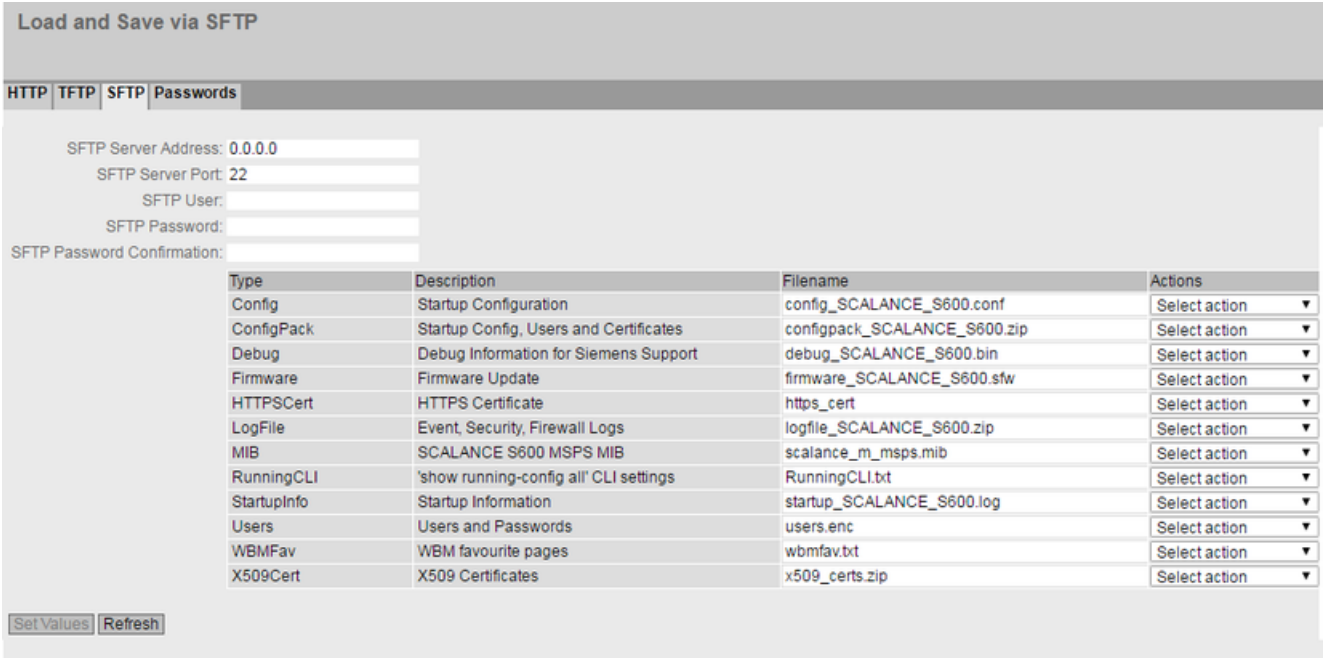
You can use the file types as follows:

- For offline diagnostics
  You can save the faulty configuration of a device as "RunningSINEMAConfig" via the WBM and import it in STEP 7 Basic/Professional. No connection to a real device is required for the diagnostics in STEP 7 Basic/Professional. You can export a corrected configuration and load it as "SINEMAConfig" again using the WBM.
- For configuration
  No connection to a real device is required to configure a device in STEP 7 Basic/Professional. You can export the configuration and load it as "SINEMAConfig" to the real device using the WBM.

X509 certificates

The following file types can be loaded into the device:

- .crt, pem, zip: Maximum file name length 255 characters
- .p12: Maximum file name length 248 characters



Description

The page contains the following boxes:

- **SFTP Server Address**
  Enter the IP address or the FQDN of the SFTP server with which you exchange data.
- **SFTP Server Port**
  Enter the port of the SFTP server via which data exchange will be handled. If necessary, you can change the default value 22 to your own requirements.
- **SFTP User**
  Enter the user for access to the SFTP server. This assumes that a user with the corresponding rights has been created on the SFTP server.
- **SFTP Password**
  Enter the password for the user
- **SFTP Password Confirmation**
  Confirm the password.

The table has the following columns:

- **Type**
  Shows the file type.
- **Description**
  Shows the short description of the file type.
- **Filename**
  A file name is preset here for every file type.

  Note

  Changing the file name

  You can change the file name preset in this column. After loading on the device, the changed file name can also be used with the Command Line Interface.

- **Actions**
  Select the action from the drop-down list. The selection depends on the selected file type, for example you can only save the log file.
  The following actions are possible:
  - **Save file**
    With this selection, you save a file on the SFTP server.
  - **Load file**
    With this selection, you load a file from the SFTP server.

Procedure

Loading or saving data using SFTP

1. Enter the address of the SFTP server in "SFTP Server Address".
2. Enter the port of the SFTP server to be used in "SFTP Server Port".
3. Enter the user data (user name and password) required for access to the SFTP server.

4. If applicable, enter the name of a file in which you want to save the data or take the data from in "Filename".

   Note

   Files whose access is password protected

   To be able to load these files on the device successfully, you need to enter the password specified for the file in "System" > "Load&Save" > "Passwords".

5. Select the action you want to execute from the "Actions" drop-down list.
6. Click "Set Values" to start the selected action.
7. If a restart is necessary, a message to this effect will be output. Click the "OK" button to run the restart. If you click the "Abort" button, there is no device restart. The changes only take effect after a restart.

Reusing configuration data

If several identical devices are to receive the same configuration and the IP addresses are assigned using DHCP, the effort for reconfiguration can be reduced by saving and reading in the configuration data.

Follow the steps below to reuse configuration data:

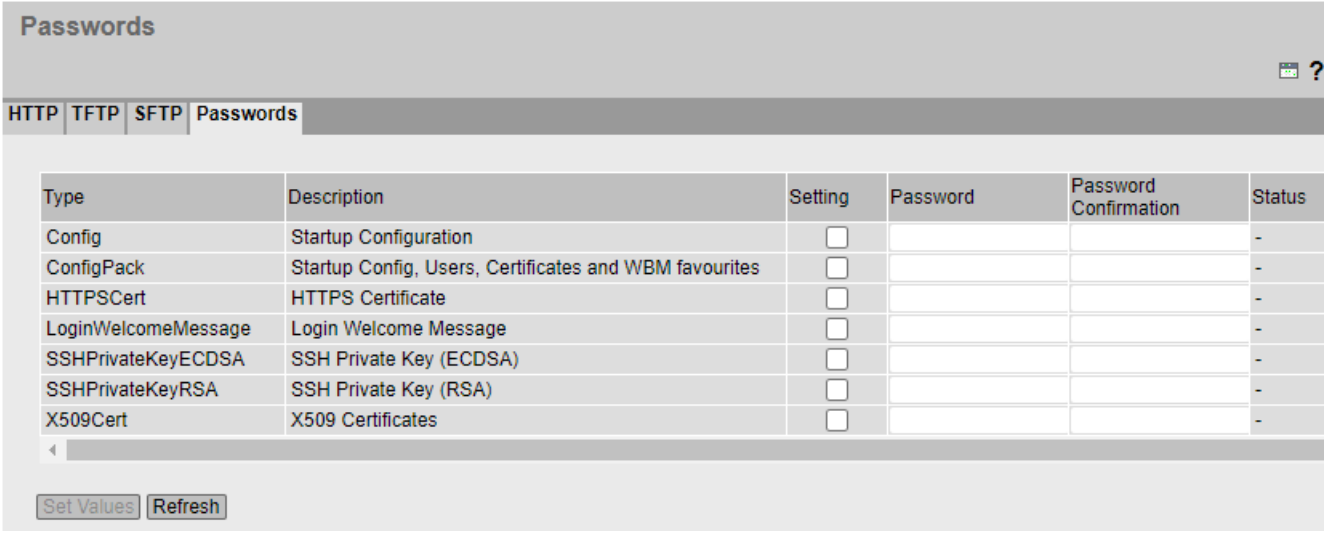
1. Save the configuration data of a configured device on your PC.
2. Load these configuration files on all other devices you want to configure in this way.
3. If individual settings are necessary for specific devices, these must be made online on the relevant device.

Note

Configuration data has a checksum. If you change the data, you can no longer upload it to the device.

4.4.5.5 Passwords

There are files to which access is password protected. To load the file on the device, enter the password specified for the file on the WBM page.



Description

The table has the following columns:

- **Type**
  Shows the file type.
- **Description**
  Shows the short description of the file type.
- **Setting**
  When selected, the password is used. Can only be enabled if the password is configured.
- **Password**
  Enter the password for the file.
- **Password Confirmation**
  Confirm the new password.
- **Status**
  Shows whether the current settings for the file match the device.
  - Valid
    The settings are valid.
  - Invalid
    the settings are invalid.
  - '-'
    Status cannot be evaluated.

Procedure

1. Enter the password in "Password".
2. To confirm the password, enter the password again in "Password Confirmation".
3. Select the "Enabled" option.
4. Click the "Set Values" button.

4.4.6 Events

4.4.6.1 Configuration

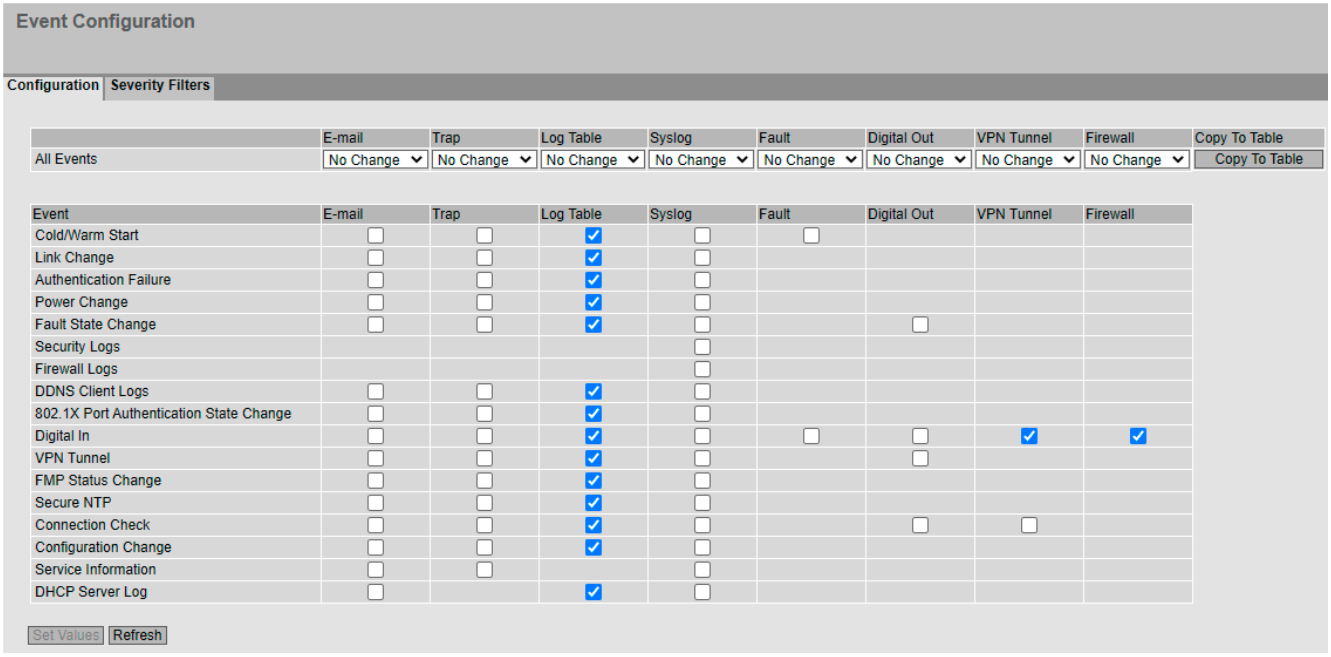
Selecting system events

On the WBM page, you define which system events are reported and how, or execute a follow-up reaction.

The following messages are always entered in the event log table and cannot be deselected:

- Changing the admin password
- Starting the device
- Operational status of the device, e.g. whether or not a PLUG is inserted
- Status of errors not yet dealt with

To send these messages to a Syslog server as well, enable the "Syslog" button for the event "System General Logs".



Description

With Table 1, you can enable or disable all check boxes of a column of Table 2 at once.

Table 1 has the following columns:

- **All Events**
  Shows that the settings are valid for all events of table 2.
- **E-mail / Trap / Log Table / Syslog / Fault / Digital Out / VPN Tunnel / Firewall**
  Enable or disable the required type of notification for all events. If "No Change" is selected, the entries of the corresponding column in table 2 remain unchanged.
- **Copy To Table**
  If you click the button, the setting is adopted for all events of table 2.

Table 2 has the following columns:

- **Event**
  The "Event" column contains the following:
  - Cold/Warm Start
    The device was turned on or restarted by the user. In the error memory of the device a new entry is generated with the type of restart performed.
  - Link Change
    This event occurs only when the port status is monitored and has changed, see "System > Fault Monitoring > Link Change".
  - Authentication Failure
    This event occurs when access is attempted with an incorrect password.
  - Power Change
    This event occurs only when power supply lines 1 and 2 are monitored. It indicates that there was a change to line 1 or line 2. See "System > Fault Monitoring > Power Supply".
  - Fault State Change
    The fault status has changed. The fault status can relate to the activated port monitoring, the response of the signaling contact or digital output or the power supply monitoring.
    Fault at signaling contact
    When a fault occurs at the signaling contact, the signaling contact opens and the error LED "F" lights up. When the error/fault status is no longer pending, the fault LED goes out and the signaling contact is closed.
    Fault at digital output
    If you have configured the signaling contact as digital output:
    For an error to also be signaled by the fault LED "F", you must enable "Fault State Change" for the "Digital Out". In this case, the fault LED "F" lights up when an internal error occurs and the signaling contact is closed.
  - Security Logs
    An entry is made in the security log if the IPsec method is used for VPN or a SINEMA RC connection is enabled.
  - Firewall Logs
    Each time individual firewall rules are applied, this is recorded in the firewall log. To do this, the LOG function must be enabled for the various firewall functions.
  - DDNS Client Logs
    The event occurs when the DDNS client synchronizes the assigned IP address with the hostname registered at the DDNS provider.
  - 802.1X Port Authentication State Change
    This event occurs with 802.1X authentications.
  - Digital In
    The event occurs when the status of the digital input has changed.
  - VPN Tunnel
    The event occurs when the status of VPN (IPsec, SINEMA RC) has changed.

  - FMP Status Change
    The value of the received power or the power loss has exceeded or fallen below a certain limit.

    Note

    You can only configure this event in devices that support FMP.

  - NTP (secure)
    This event occurs when the device receives the system time from a secure NTP server.
  - Connection Check
    This event occurs when connections are being monitored, see "System > Connection Check".
  - Configuration Change
    This event occurs when the configuration of the device has changed.
  - Service Information
    For certain events, entries are made in the log table even without configuration. For these events, you can configure additional subsequent actions here (e-mail, Trap, Syslog).
  - DHCP Server Log
    DHCP events are saved in the logbook.

- **E-mail**
  The device sends an e-mail. This is only possible if the SMTP server is set up and the "SMTP Client" function is enabled.
- **Trap**
  The device sends an SNMP trap. This is only possible if "SNMPv1 Traps" is enabled in "System > Configuration".
- **Log Table**
  The device writes an entry in the event log table, see "Information > Log Table".
- **Syslog**
  The device writes an entry to the system log server. This is only possible if the system log server is set up and the "Syslog client" function is enabled.
- **Fault**
  Select for which events the device is to trigger a fault. The fault is signaled by the fault LED lighting up.
- **Digital Out**
  Controls the digital output.
  By default, the digital output is closed, which means the signaling contact is open. The digital output is opened as soon as you enable at least one event for the digital output under "Events > Configuration". It also is no longer automatically connected to the fault LED. You connect the digital output with the fault LED under "Fault State Change".
- **VPN Tunnel**
  Controls the forwarding of an event to a VPN connection (IPsec, SINEMA RC). As long as the event is present, the VPN connection is switched to active.
- **Firewall**
  Controls application of the user-defined rule set. This requires a rule set to be assigned to the digital input under "Security > Firewall > User Specific".

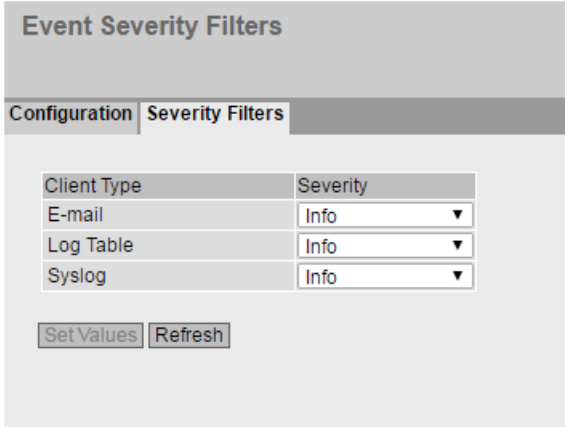
Procedure

Establishing/terminating a VPN tunnel via the digital input

1. For the "Digital In" event, activate the "VPN Tunnel" entry.
2. Configure the VPN connection
   - IPsec:
     In "Operation" set "wait on DI" or "start on DI". You can find more information on this in "IPsec VPN > Connections" and in "VPN connection establishment".
   - SINEMA RC:
     For "Type of connection", set "Auto" or "Digital In". For "Auto" type of connection, you must set the "Digital In" type of connection on the SINEMA RC Server under "Remote connections > Devices". You can find additional information on this topic in the operating instructions "SINEMA RC Server".
3. Click on "Set Values".

4.4.6.2 Severity Filters

On this page, you configure the severity for the sending of system event notifications.



Description

The table has the following columns:

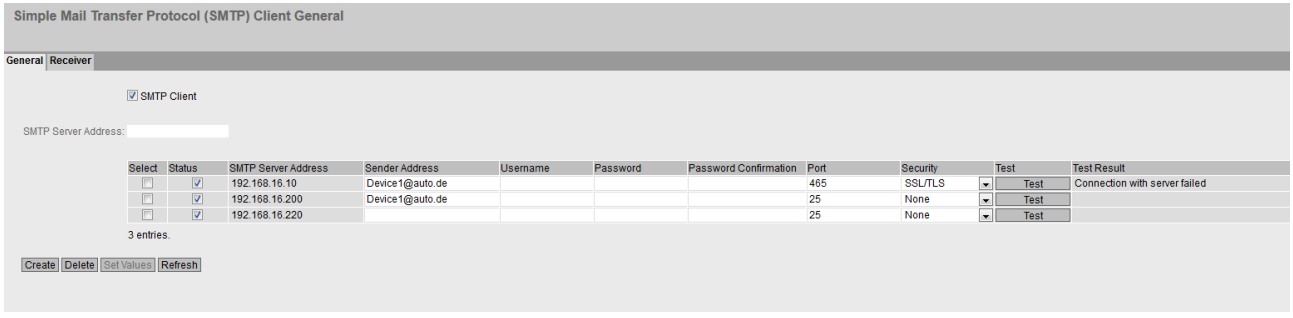
- **Client Type**
  Select the client type for which you want to make settings:
  - **E-mail**
    Sending system event messages by e-mail.
  - **Log Table**
    Entry of system events in the log table.
  - **Syslog**
    Entry of system events in the Syslog file.
- **Severity**
  Select the required severity. The following settings are possible:
  - **Info**
    The messages of all severities are sent or logged.
  - **Warning**
    The messages of this severity and the "critical" severity are sent or logged.
  - **Critical**
    Only the messages of this severity are sent or logged.

4.4.7 SMTP client

4.4.7.1 General

Network monitoring with e-mails

If events occur, the device can automatically send an e-mail, e.g. to the service technician. The e-mail contains the identification of the sending device, a description of the cause in plain text, and a time stamp. This allows centralized network monitoring to be set up for networks with few nodes based on an e-mail system.



Requirements for sending e-mails

- "E-mail" is activated for the relevant event in "System > Events > Configuration".
- The desired severity is configured under "System > Events > Severity level".
- At least one entry exists under "System > SMTP Client > Receiver" and the setting "Send" is activated.

Description

The page contains the following boxes:

- **SMTP Client**
  Enable or disable the SMTP client.
- **SMTP Server Address**
  Enter the IP address or the FQDN (Fully Qualified Domain Name) of the SMTP server.

The table contains the following columns:

- **Select**
  Select the check box in a row to be deleted.
- **Status**
  Specify whether this SMTP server will be used.
- **SMTP Server Address**
  Shows the IP address or the FQDN (Fully Qualified Domain Name) of the SMTP server.
- **Sender Email Address**
  Enter the e-mail address of the sender that is specified in the e-mail.
- **User Name**
  If necessary, enter the user name used for authentication on the SMTP server.
- **Password**
  If necessary, enter the password used for authentication on the SMTP server.
- **Password Confirmation**
  Repeat the password.
- **Port**
  Enter the port via which your SMTP server can be reached.
  Factory settings:
  - 25 (None)
  - 465 (SSL/TLS and StartTLS)

- **Security**
  Specify whether transfer of the e-mail from the device to the SMTP server is encrypted. This is only possible when the SMTP server supports the selected setting.

  Note

  2-factor authentication (2FA)

  2-factor authentication is not supported.

  – SSL/TLS
  – StartTLS
  – None: The e-mail is transferred unencrypted.
- **Test**
  Sends a test e-mail to the configured receivers.
- **Test Result**
  Shows whether the e-mail was sent successfully or not. If sending was not successful, the message contains possible causes.

Procedure

Configuring the SMTP server

1. Enable the "SMTP Client" function.
2. Enter the IP address or the FQDN of the SMTP server for "SMTP Server Address".
3. Click the "Create" button. A new entry is generated in the table.
4. Enter the name of the sender that will be included in the e-mail for "Sender Email Address".
5. Enter the user name and password if the SMTP server prompts you to log in.
6. Under "Security", specify whether transfer to the SMTP server is encrypted.
7. Enable the SMTP server entry.
8. Click the "Set Values" button.

   Note

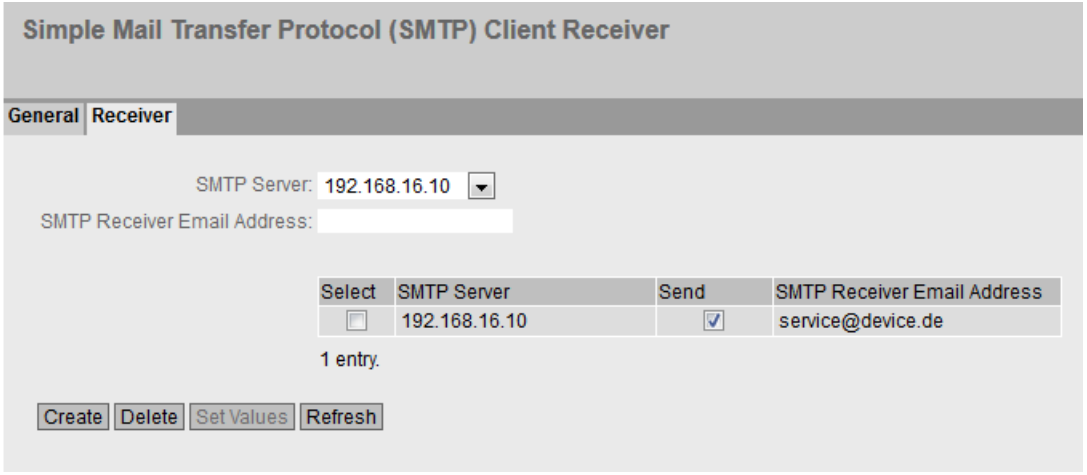
   Depending on the properties and configuration of the SMTP server, it may be necessary to adapt the "Sender E-Mail Address" input for the e-mails. Check with the administrator of the SMTP server.

Testing the configuration of the SMTP server

1. Configure receivers
   - Click the "Receiver" tab.
   - Select the desired SMTP server under "SMTP server".
   - Enter the desired address under "SMTP Receiver Email Address".
   - Click the "Create" button. A new entry is generated in the table. The setting "Send" is activated by default.
2. Send test e-mail
   - Click the "General" tab.
   - Click the "Test" button next to the SMTP server entry. The device sends to every configured receiver
   - Check the test result. If sending was not successful, the message contains possible causes.

4.4.7.2 Receiver

On this page, you specify who receives an e-mail when an event occurs.



Description

The page contains the following boxes:

- **SMTP Server**
  Specify the SMTP server via which the e-mail is sent.
- **SMTP Receiver Email Address**
  Enter the e-mail address to which the device sends an e-mail.

The table contains the following columns:

- **Select**
  Select the check box in a row to be deleted.
- **SMTP Server**
  Shows the IP address or the FQDN (Fully Qualified Domain Name) of the SMTP server to which the entry relates.
- **Send**
  When enabled, the device sends an e-mail to this receiver.
- **SMTP Receiver Email Address**
  Shows the e-mail address to which the device sends an e-mail if a fault occurs.

Procedure

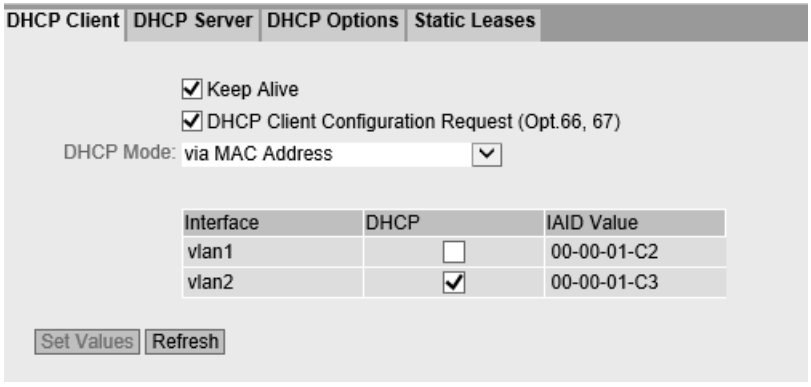
Configuring an SMTP receiver

1. Select the required "SMTP Server".
2. Enter the SMTP receiver email address.
3. Click the "Create" button. A new entry is generated in the table.
4. Activate the "Send" option for the entry.
5. Click the "Set Values" button.

4.4.8 DHCPv4

4.4.8.1 DHCP Client

If the device is configured as a DHCP client, it starts a DHCP request. As the reply to the query the device receives an IPv4 address from the DHCP server. The server manages an address range from which it assigns IPv4 addresses. It is also possible to configure the server so that the client always receives the same IPv4 address in response to its request.



Description

The page contains the following boxes:

- **Keep Alive**
  When this is enabled, the IP address is retained in the event of a connection breakdown and is not reset to 0.0.0.0. Keep Alive is enabled by default. When Keep Alive is disabled, the IP address is reset to 0.0.0.0 in the event of a communication breakdown.
- **DHCP Client Configuration Request (Opt. 66, 67)**
  When enabled, the DHCP client uses the options to download the configuration file (option 67) from the TFTP server (option 66). After the restart, the device uses the data from the configuration file.
- **DHCP Mode**
  Specify the type of identifier with which the DHCP client logs on with its DHCP server.
  - via MAC Address
    Identification is based on the MAC address.
  - via DHCP Client ID
    Identification is based on a freely defined DHCP client ID.
  - via System Name
    Identification is based on the Device Name. If the device name is 255 characters long, the last character is not used for identification.
  - via IAID and DUID
    With this, the DHCP client can log on with DHCP servers that support parallel operation of IPv4 and IPv6.
    The identification is via the IAID and the DUID and identifies precisely one IP interface of the device.
    IAID (Interface Association Identifier): At least one IAID is generated for each IP interface. The IAID remains unchanged when the DHCP client restarts.
    DUID (DHCP Unique Identifier): Uniquely identifies server and clients and applies to all IP interfaces of the device. The DUID remains unchanged when there is a restart.

The table has the following columns:

- **Interface**
  Interface to which the setting relates.
- **DHCP**
  Enable or disable the DHCP client for the relevant interface.
- **IAID Value**
  Value with which the interface (DHCP client) identifies itself with the DHCP server.

Procedure

Follow the steps below to configure the IP address using the DHCP client ID:

1. Select the identification method in the "DHCP Mode" drop-down list.
   If you select the DHCP mode "via DHCP Client ID" an input box appears.
   In the enabled input box "DHCP client ID" enter a string to identify the device. This is then evaluated by the DHCP server.
2. Select the "DHCP Client Configuration Request (Opt. 66, 67)", if you want the DHCP client to use options 66 and 67 to download and then enable a configuration file.

3. Enable the "DHCP" option in the table.
4. Click the "Set Values" button.

Note

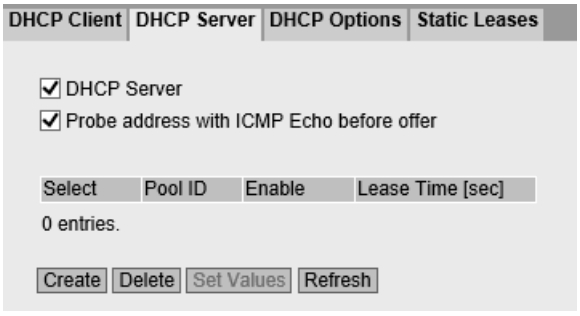
If a configuration file is downloaded, this can trigger a system restart. If the currently running configuration and the configuration in the downloaded configuration file differ, the system restarts.

Make sure that the option "DHCP Client Configuration Request (Opt. 66, 67)" is no longer set.

4.4.8.2 DHCP Server

You can operate the device as a DHCP server. This allows IP addresses to be assigned automatically to the connected devices. The IP addresses are either distributed dynamically from an address band (pool) you have specified or a specific IP address is assigned to a particular device.

On this page, specify the address band from which the device receives any IP address. You configure the static assignment of the IP addresses in "Static Leases".



Requirement

- The connected devices are configured so that they obtain the IP address from a DHCP server.

Description

The page contains the following boxes:

- **DHCP Server**
  Enable or disable the DHCP server on the device.

  Note

  To avoid conflicts with IPv4 addresses, only one device may be configured as a DHCP server in the network.

- **Probe address with ICMP echo before offer**
  When selected, the DHCP server checks whether or not the IP address has already been assigned. To do this the DHCP server sends ICMP echo messages (ping) to the IPv4 address. If no reply is received, the DHCP server can assign the IPv4 address.

  Note

  If there are devices in your network on which the echo service is disabled as default, there may be conflicts with the IPv4 addresses. To avoid this, assign these devices an IPv4 address outside the IPv4 address band.

The table has the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **Pool ID**
  Shows the number of the IPv4 address band. If you click the "Create" button, a new row with a unique number is created (pool ID).
- **Interface**
  Select a VLAN IP interface. The IPv4 addresses are assigned dynamically via this interface. The requirement for the assignment is that the IPv4 address of the interface is located in the subnet of the IPv4 address band. If this is not the case, the interface does not assign any IPv4 addresses.
- **Enable**
  Specify whether or not this IPv4 address band will be used.

  Note

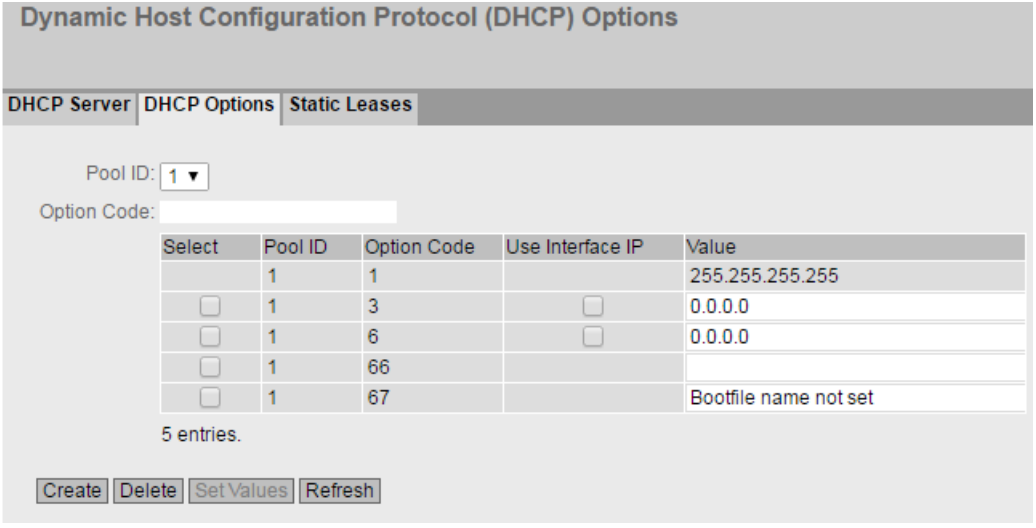
  If you enable the IPv4 address band, its settings in this and the other DHCP tabs are grayed out and can no longer be edited.

- **Subnet**
  Enter the network address range that will be assigned to the devices. Use the CIDR notation.
- **Lower IP Address**
  Enter the IPv4 address that specifies the start of the dynamic IPv4 address band. The IPv4 address must be within the network address range you configured for "Subnet".

- **Upper IP address**
  Enter the IPv4 address that specifies the end of the dynamic IPv4 address band. The IPv4 address must be within the network address range you configured for "Subnet".
- **Lease Time (sec)**
  Specify for how many seconds the assigned IPv4 address remains valid. When half the period of validity has elapsed. the DHCP client can extend the period of the assigned IPv4 address. When the entire time has elapsed, the DHCP client needs to request a new IPv4 address.

4.4.8.3 DHCP options

On this page you specify which DHCP options the DHCP server supports. The various DHCP options are defined in RFC 2132.



Description

The page contains the following boxes:

- **Pool ID**
  Select the required address band.
- **Option Value**
  Enter the number of the required DHCP option.

Note

DHCP options supported

The DHCP options 1, 3, 6, 12, 15, 66, 67 are supported.

The DHCP options are created automatically when the IPv4 address band is created. With the exception of option 1, the options can be deleted.

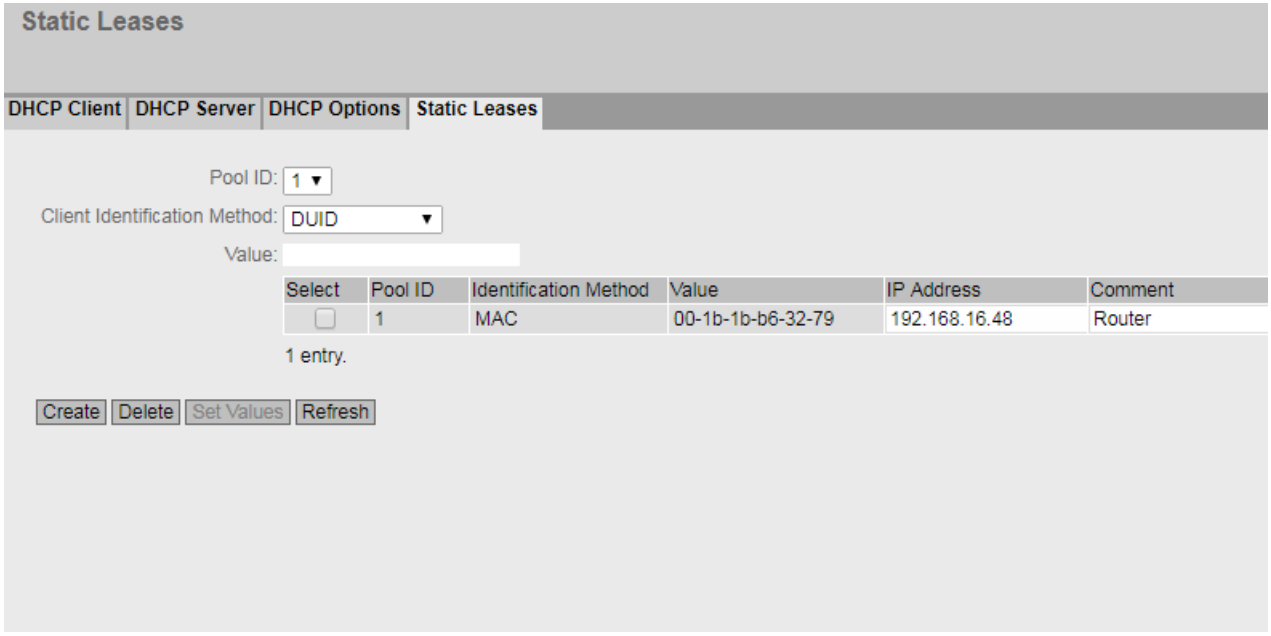
The table has the following columns:

- **Select**
  Select the check box in the row to be deleted
- **Pool ID**
  Shows the number of the address band.
- **Option Value**
  Shows the number of the DHCP option.
- **Description**
  Text describing the option value.
- **Use Interface IP**
  Specify whether or not the internal IP address of the device will be used.
- **Value**
  Enter the DHCP parameter that is transferred to the DHCP client. The content depends on the DHCP option.

Option value	Option name		
1	Subnet mask	The subnet mask is entered automatically.	Option cannot be deleted.
3	Router	The IPv4 address for router in the subnet of the DHCP client. If the device itself is the router, the IPv4 address of the interface is used.	You can specify several IPv4 addresses separated by commas.
6	DNS Server	The IPv4 address of the DNS server available to the DHCP client. If the device itself is the DNS server, the IPv4 address of the interface is used.	
12	Host name	Enter the host name in the string format.	
15	DNS domain name	Assign the DNS domain name.	
66	TFTP server	The IPv4 address or the hostname of the TFTP server available to the DHCP client.	Enter the address of the TFTP server.
67	Name of the boot file	The name of the boot file that the client downloads from the TFTP server.	Enter the name of the boot file in the string format.

4.4.8.4 Static Leases

On this page you specify that certain devices will be assigned a certain IP address. The address assignment is made based on the MAC address, the client ID or the DUID.



Description

The page contains the following boxes:

- **Pool ID**
  Select the required address band.
- **Client Identification Method**
  Select the method according to which a client is identified.
  - Ethernet MAC
    Identification is based on the MAC address. Enter the MAC address in "Value". A MAC address consists of six byes separated by hyphens in hexadecimal notation, e.g. 00-ab-1d-df-b4-1d.
  - Client ID
    Identification is based on a freely defined DHCP client ID. Enter the required designation in "Value".
  - DUID
    Identification is based on the DUID and IAID. Enter the required designation in "Value" e.g. 00-00-01-C2-00-01-00-01-00-00-00-72-00-1B-1B-B6-32-9D.
- **Value**
  Enter the required value. The entry depends on the selected identification method of the client.

  Note

  The maximum is 128 entries.

The table has the following columns:

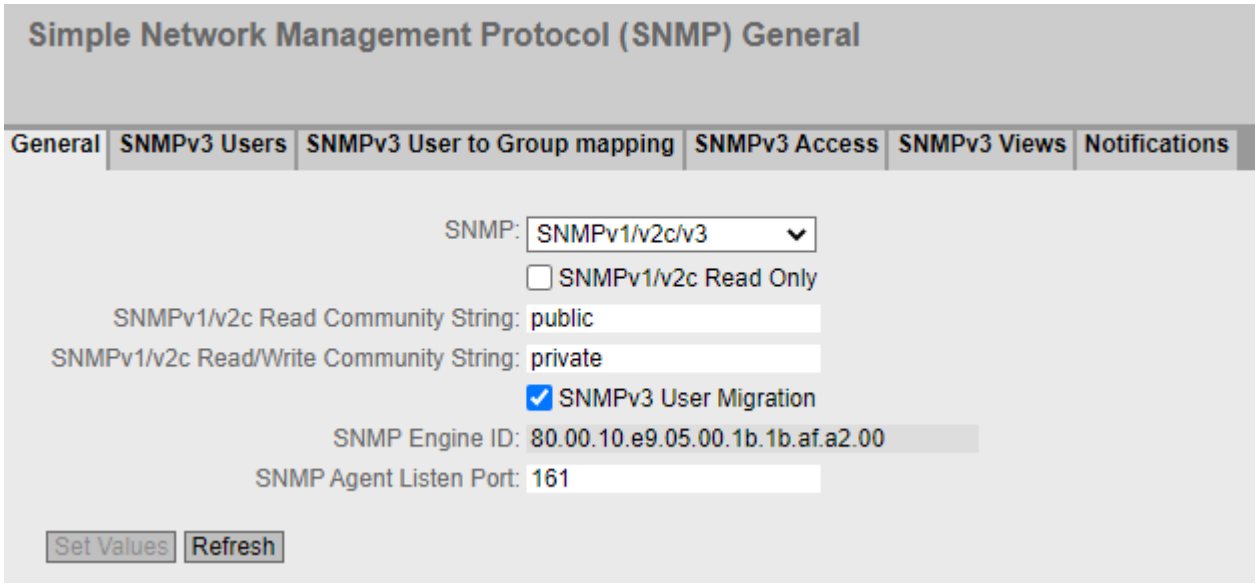
- **Select**
  Select the check box in the row to be deleted.
- **Pool ID**
  Shows the number of the address band.
- **Identification Method**
  Shows the method with which the client identifies itself with the DHCP server.
- **Value**
  Shows the MAC address or client ID or DUID of the client.
- **IP Address**
  Specify the IPv4 address that will be assigned to the client. The IPv4 address must be within the address band.
- **Comment**
  Enter a description for the address assignment.
  The maximum is 32 characters.

4.4.9 SNMP

4.4.9.1 General

Configuration of SNMP

On this page, you make the basic settings for SNMP. Enable the check boxes according to the function you want to use.



Description

The page contains the following boxes:

- **SNMP**
  Select the SNMP protocol from the drop-down list. The following settings are possible:
  - "-" (Disabled)
    SNMP is disabled.
  - SNMPv1/v2c/v3
    SNMPv1/v2c/v3 is supported.

    Note

    Note that SNMP in versions 1 and 2c does not have any security mechanisms.

  - SNMPv3
    Only SNMPv3 is supported.
- **SNMPv1/v2c Read-Only**
  If you enable this option, SNMPv1/v2c can only read the SNMP variables.

  Note

  Community String

  For security reasons, do not use the standard values "public" or "private". Change the community strings following the initial installation.

  The recommended minimum length for community strings is 6 characters.

  For security reasons, only limited access to objects of the SNMPCommunityMIB is possible with the SNMPv1/v2c Read Community String. With the SNMPv1/v2c Read/Write Community String, you have full access to the SNMPCommunityMIB.
- **SNMPv1/v2c Read Community String**
  Enter the community string for read access of the SNMP protocol.
- **SNMPv1/v2c Read/Write Community String**
  Enter the community string for read and write access of the SNMP protocol.
- **SNMPv3 User Migration**
  - **Enabled**
    If the function is enabled, an SNMP engine ID is generated that can be migrated. You can transfer configured SNMPv3 users to a different device.
    If you enable this function and load the configuration of the device on another device, configured SNMPv3 users are retained.
  - **Disabled**
    If the function is disabled, a device-specific SNMP Engine ID is generated. To generate the ID, the agent MAC address of the device is used. You cannot transfer this SNMP user configuration to other devices.
    If you load the configuration of the device on another device, all configured SNMPv3 users are deleted.

- **SNMP Engine ID**
  Shows the SNMP engine ID.
- **SNMP Agent Listen Port**
  Specify the port at which the SNMP agent waits for the SNMP queries. Standard port 161 is the default. You can optionally enter the standard port 162 or a port number in the range 1024 ... 49151 or 49500 ... 65535.

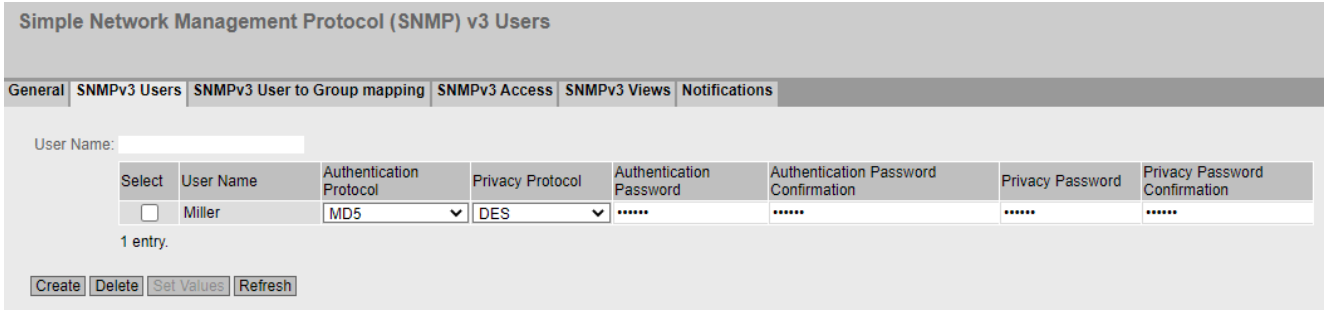
Procedure

1. Select the required option from the "SNMP" drop-down list:
   – "-" (disabled)
   – SNMPv1/v2c/v3
   – SNMPv3
2. Enable the "SNMPv1/v2c Read Only" check box if you only want read access to SNMP variables with SNMPv1/v2c.
3. Enter the required character string in the "SNMPv1/v2c Read Community String" input box.
4. Enter the required character string in the "SNMPv1/v2c Read/Write Community String" input box.
5. If necessary, enable the SNMPv3 User Migration.
6. Click the "Set Values" button.

4.4.9.2 SNMPv3 Users

User-specific security settings

On the WBM page, you can create new SNMPv3 users and modify or delete existing users. The user-based security model works with the concept of the user name; in other words, a user ID is added to every frame. This user name and the applicable security settings are checked by both the sender and recipient.



Description

The page contains the following boxes:

- **User Name**
  Enter a freely selectable user name. After you have entered the data, you can no longer modify the name.

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **User Name**
  Shows the created users.
- **Authentication Protocol**
  Specify the authentication protocol for which a password will be stored.
  The following settings are available:
  - None
  - MD5
  - SHA
- **Privacy Protocol**
  Specify the encryption protocol for which a password will be stored. This drop-down list is only enabled when an authentication protocol has been selected.
  The following settings are available:
  - None
  - DES
  - AES
- **Authentication Password**
  Enter the authentication password in the first input box. This password must have at least 1 character, the maximum length is 32 characters.

  Note

  Length of the password

  As an important measure to maximize security, we recommend that the password has a minimum length of 6 characters and that it contains special characters, uppercase/lowercase letters, numbers.
- **Authentication Password Confirmation**
  Confirm the password by repeating the entry.

- **Privacy Password**
  Enter your encryption password. This password must have at least 1 character, the maximum length is 32 characters.

  Note

  Length of the password

  As an important measure to maximize security, we recommend that the password has a minimum length of 6 characters and that it contains special characters, uppercase/lowercase letters, numbers.

- **Privacy Password Confirmation**
  Confirm the encryption password by repeating the entry.

Procedure

Create a new user

1. Enter the name of the new user in the "User Name" input box.
2. Click the "Create" button. A new entry is generated in the table.
3. Select the authentication algorithm for "Authentication Protocol". In the relevant input boxes, enter the authentication password and the confirmation.
4. Select the algorithm in "Privacy Protocol". In the relevant input boxes, enter the encryption password and the confirmation.
5. Click the "Set Values" button.

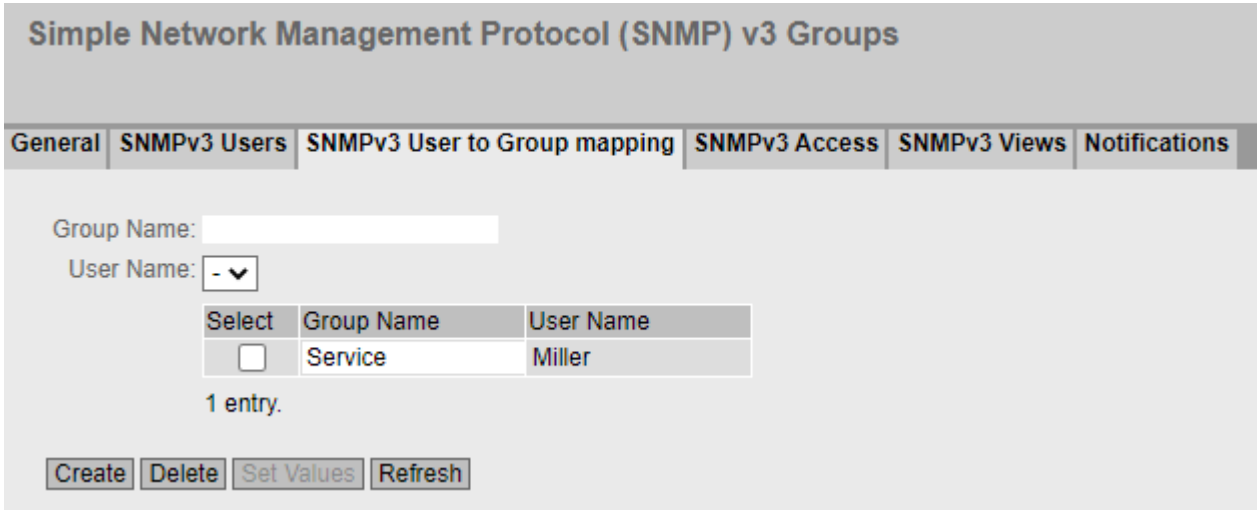
Delete user

1. Enable "Select" in the row to be deleted.
   Repeat this for all users you want to delete.
2. Click the "Delete" button. The entry is deleted.

4.4.9.3 SNMPv3 User to Group mapping

Configuration of group members

You assign users to SNMPv3 groups on this WBM page. Each user can only be a member of one group.



Description

The page contains the following boxes:

- **Group Name**
  Enter the group that will be assigned to the user.
- **User Name**
  Select the user to be a member of the specified group. The drop-down list only contains users that are not yet assigned to a group.

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **Group Name**
  Displays the SNMPv3 group. A group name can only be changed later if no access rights have been defined for the group yet.
- **User Name**
  Shows the user that is a member of this group.

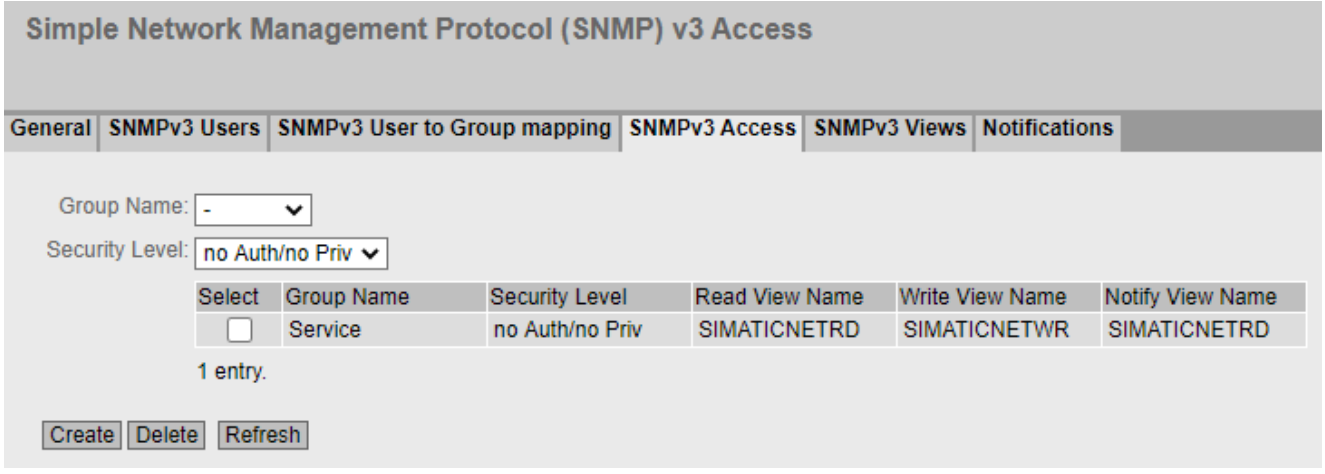
4.4.9.4 SNMPv3 Access

Security settings and assigning permissions

SNMP version 3 allows permissions to be assigned, authentication, and encryption at protocol level. The security level and read/write permissions are assigned according to groups. The settings automatically apply to every member of a group.

Note

Different access permissions for different security levels can be assigned to a group. If no access permission is defined for a security level, no access to the device is possible for members of the group using this security level.



Description

The page contains the following boxes:

- **Group Name**
  Select the name of the group.
- **Security Level**
  Select the security level (authentication, encryption) for which you want to define the access permissions of the group:
  - **No Auth/no Priv**
    No authentication enabled/no encryption enabled.
  - **Auth/no Priv**
    Authentication enabled/no encryption enabled.
  - **Auth/Priv**
    Authentication enabled/encryption enabled.

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **Group Name**
  Shows the name of the SNMPv3 group.
- **Security Level**
  Shows the security level to which this access permission applies.
- **Read View Name**
  Enter an SNMPv3 view that grants read access to members of the group with the specified Security Level.
- **Write View Name**
  Enter an SNMPv3 view that grants write access to members of the group with the specified Security Level.

  Note

  For write access to work, you also need to enable read access.

- **Notification View Name**
  Enter an SNMPv3 view for which SNMP notification to members of the group with the defined security level should be used.

Procedure

Creating a new group

1. Select the name of the group for which you are configuring SNMP access.
2. Select the required security level from the "Security Level" drop-down list.
3. Click the "Create" button to create a new entry.
4. In the "Read View Name" field, enter the SNMPv3 view for read access.
5. In the "Write View Name" field, enter the SNMPv3 view for write access.
6. In the "Notification View Name" field, enter the SNMPv3 view for notifications.
7. Click the "Set Values" button.

Modifying a group

Once a group name and the security level have been specified, they can no longer be modified after the group is created. If you want to change the group name or the security level, you will need to delete the group and create it and configure it with the new name.

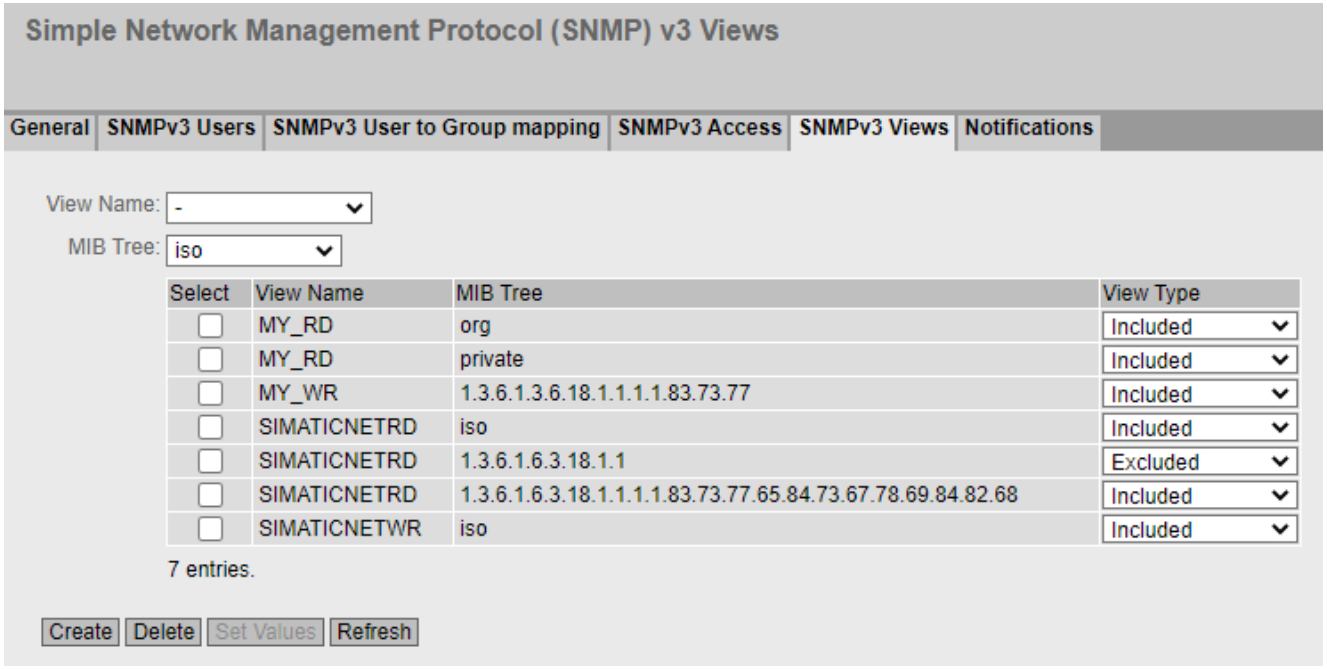
Deleting a group

1. Enable "Select" in the row to be deleted.
   Repeat this for all groups you want to delete.
2. Click the "Delete" button. The entries are deleted.

4.4.9.5 SNMPv3 Views

Configuration of SNMPv3 views

You configure the parameters of SNMP views on this WBM page.



Note

Controlling the SNMPv1 and SNMPv2c access

The preconfigured **SIMATICNETRD** and **SIMATICNETWR** views are used internally to control the SNMPv1 and SNMPv2c access. If you delete or change these views, this directly affects the SNMPv1 and SNMPv2c access.

Description

The page contains the following boxes:

- **View Name**
  Select the name of the view that you want to configure. An SNMPv3 view always needs to be assigned to an SNMPv3 access. For this reason, you need to enter a new SNMPv3 view in the table in the "SNMP Access" tab.
- **MIB Tree**
  Select the Object Identifier (OID) of the MIB area that is to be used for the SNMPv3 view. The following options are possible:
  - **iso**
  - **std**
  - **member-body**
  - **org**
  - **mgmt**
  - **private**
  - **snmpV2**

  The drop-down list only contains the OIDs that are usually used. If the configuration of a specific OID that is not listed is necessary, you can configure this via the CLI with the `snmp view` command. This OID is then also displayed in the WBM in the overview table.

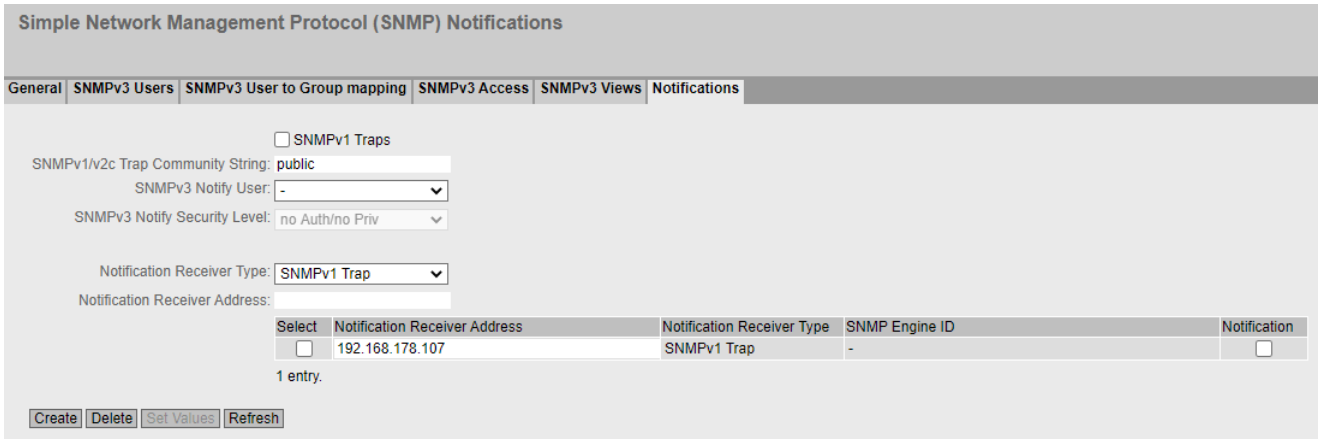
The table has the following columns:

- **Select**
  Select the row you want to delete.
- **View Name**
  The name of the SNMPv3 view.
- **MIB Tree**
  The OID of the MIB area for the SNMPv3 view.
- **View Type**
  The available options are as follows:
  - **Included**
    The MIB OID and its lower-level nodes are part of the SNMPv3 view. Access to the corresponding MIB objects is possible.
  - **Excluded**
    The MIB OID and its lower-level nodes are not part of the SNMPv3 view. Access to the corresponding MIB objects is not possible.

4.4.9.6 Notifications

SNMP traps and SNMPv3 notifications

If an alarm event occurs, a device can send SNMP notifications (traps and inform notifications) to up to ten different management stations at the same time. Notifications are only sent for events that were specified in the "Events" menu.



Description

The page contains the following boxes:

- **SNMPv1 Traps**
  Enable or disable sending of SNMPv1 traps. This setting affects all receivers of SNMPv1 traps and has no effects on receivers of SNMPv2c or SNMPv3 notifications.
- **SNMPv1/v2c Trap Community String**
  Enter the community string for sending SNMPv1/v2c notifications.
- **SNMPv3 Notify User**
  Select the user to which SNMPv3 notifications are to be sent.
- **SNMPv3 Notify Security Level**
  Select the security level (authentication, encryption) to be used for SNMPv3 notification. The following options are possible:
  - no Auth/no Priv
    No authentication enabled / no encryption enabled.
  - Auth/no Priv
    Authentication enabled / no encryption enabled.
  - Auth/Priv
    Authentication enabled / encryption enabled.

- **Notification Receiver Type**
  The receiver type defines the SNMP version and the type of notification. SNMP inform notifications must be acknowledged by the receiver, SNMP traps do not. The following options are possible:
  - SNMPv1 Trap
  - SNMPv2c Trap
  - SNMPv2c Inform
  - SNMPv3 Trap
  - SNMPv3 Inform
- **Notification Receiver Address**
  Enter the IP address of the receiver station to which the device sends SNMP notifications. You can specify up to ten different receivers servers.

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **Notification Receiver Address**
  If necessary, change the IP address of the stations.
- **Notification Receiver Type**
  Shows the defined receiver type.
- **SNMP Engine ID**
  The ID of the SNMP engine to which SNMPv3 inform notifications are sent. You can only configure this parameter for the "SNMPv3-Inform" receiver type.
- **Notification**
  Enable or disable the sending of SNMP notifications. Stations that are entered but not selected do not receive any SNMP notifications.

Note

If a table row is grayed out, the corresponding notification was configured via the CLI and can only be deleted via the CLI.

Procedure

Configuring a notification

1. Select the receiver for SNMPv3 notifications in the "SNMPv3 Notify User" drop-down list.
2. Select the security level for SNMPv3 notifications in the "SNMPv3 Notify Security Level" drop-down list.
3. Select the receiver type in the "Notification Receiver Type" drop-down list.
4. In "Notification Receiver Address", enter the IP address of the station to which the device should send traps or notifications.
5. Click the "Create" button to create a new trap entry.

6. Activate "Notification" in the required row.
7. Click the "Set Values" button.

Deleting a trap entry

1. Enable "Select" in the row to be deleted.
2. Click the "Delete" button. The entry is deleted.

4.4.10 System time

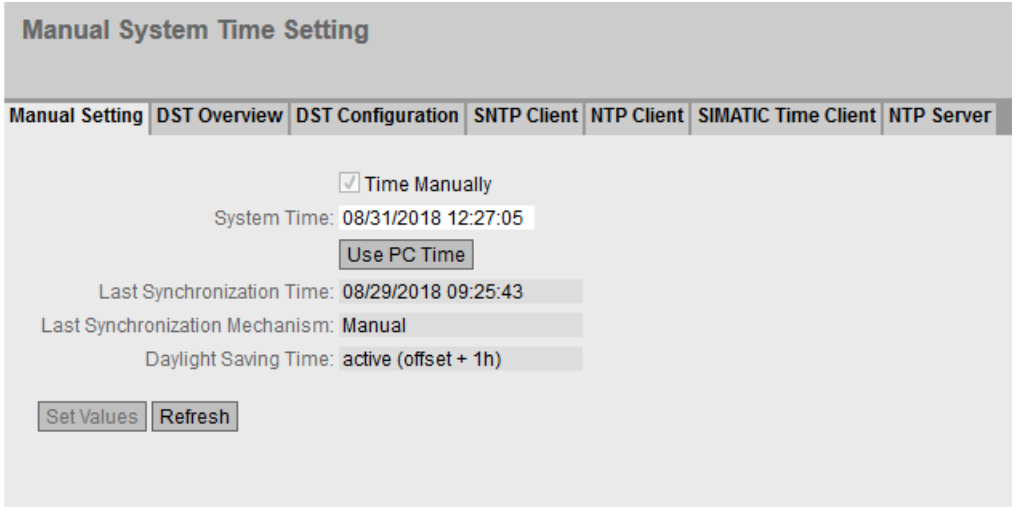
There are different methods that can be used to set the system time of the device. Only one method can be active at any one time.

If one method is activated, the previously activated method is automatically deactivated.

4.4.10.1 Manual Setting

Manual setting of the system time

On this page, you set the date and time of the system yourself. For this setting to be used, enable "Time Manually".



Description

The page contains the following boxes:

- **Time Manually**
  Enable or disable the manual time setting. If you enable the option, the "System Time" input box can be edited.
- **System Time**
  Enter the date and time in the format "MM/DD/YYYY HH:MM:SS".
  After a restart, the time of day begins at 01/01/2000 00:00:00
- **Use PC Time**
  Click the button to use the time setting of the PC.
- **Last Synchronization Time**
  Shows when the last time-of-day synchronization took place. If no time-of-day synchronization was possible, the box displays "Date/time not set".
- **Last Synchronization Mechanism**
  Shows how the last time synchronization was performed.
  - Not set
    The time was not set.
  - Manual
    Manual time setting
  - SNTP
    Automatic time-of-day synchronization with SNTP
  - NTP
    Automatic time-of-day synchronization with NTP
  - SIMATIC
    Automatic time-of-day synchronization using the SIMATIC time frame
- **Daylight Saving Time**
  Shows whether the daylight saving time changeover is active.
  - active (offset +1 h)
    The system time was changed to daylight saving time; in other words, an hour was added. You can see the current system time at the top right in the selection area of the WBM. The set time continues to be displayed in the "System Time" box.
  - inactive (offset +0 h)
    The current system time is not changed.

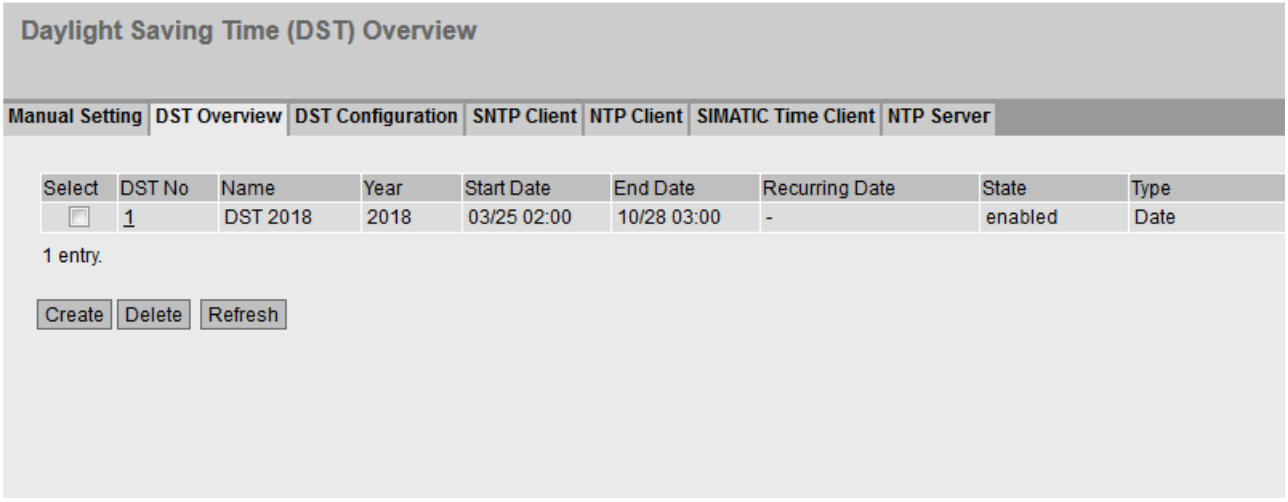
Procedure

1. Enable the "Time Manually" option.
2. Click in the "System Time" input box.
3. In the "System Time" input box, enter the date and time in the format "MM/DD/YYYY HH:MM:SS".
4. Click the "Set Values" button.
   The date and time are adopted and "Manual" is entered in "Last Synchronization Mechanism" box.

4.4.10.2 DST Overview

Daylight saving time switchover

On this page, you can create new entries for the daylight saving time changeover. The table provides an overview of the existing entries.



Settings

The page contains the following boxes:

- **Select**
  Select the row you want to delete.
- **DST No.**
  Shows the number of the entry.
  If you create a new entry, a new line with a unique number is created.
- **Name**
  Shows the name of the entry.
- **Year**
  Shows the year for which the entry was created.
- **Start Date**
  Shows the month, day and time for the start of daylight saving time.
- **End Date**
  Shows the month, day and time for the end of daylight saving time.
- **Recurring Date**
  With an entry of the type "Recurring", the period in which daylight saving time is active is displayed consisting of week, day, month and time of day.
  With an entry of the type "Date" a "-" is displayed.

- **Status**
  Shows the status of the entry:
  - Enabled
    The entry was created correctly.
  - Invalid
    The entry was created new and the start and end date are identical.
- **Type**
  Shows how the daylight saving time changeover is made:
  - Date
    A fixed date is entered for the daylight saving time changeover.
  - Recurring
    A rule was defined for the daylight saving time changeover.

Procedure

Creating an entry

1. Click the "Create" button.
   A new entry is created in the table.
2. Click on the required entry in the "DST No" column.
   You change to the "DST Configuration" page.
3. Select the required type in the "Type" drop-down list.
   Depending on the selected type, various settings are available.
4. Enter a name in the "Name" box.
5. If you have selected the type "Date", fill in the following boxes.
   - Year
   - Day (for start and end date)
   - Hour (for start and end date)
   - Month (for start and end date)
6. If you have selected the type "Recurring", fill in the following boxes.
   - Hour (for start and end date)
   - Month (for start and end date)
   - Week (for start and end date)
   - Day (for start and end date)
7. Click the "Set Values" button.

Deleting an entry

1. Enable "Select" in the row to be deleted.
2. Click the "Delete" button. The entry is deleted.

4.4.10.3 DST Configuration

Configuring the daylight saving time switchover

On this page, you can configure the entries for the daylight saving time changeover. As result of the changeover to daylight saving or standard time, the system time for the local time zone is correctly set.

You can define a rule for the daylight saving time changeover or specify a fixed date.

Settings

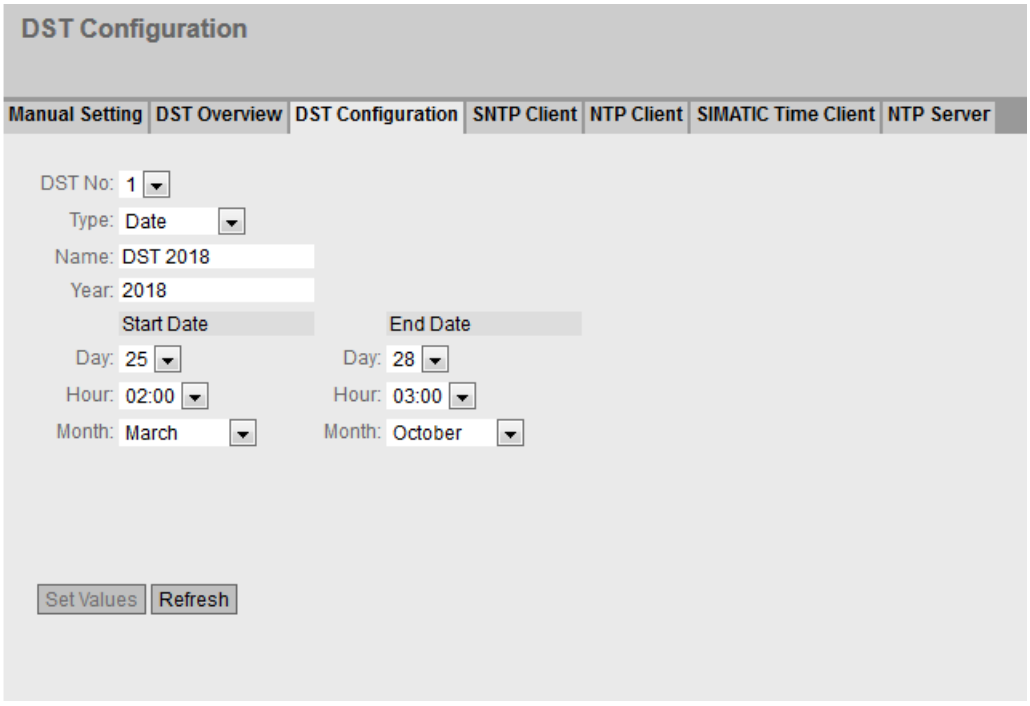
Note

The content of this page depends on the selection in the "Type" box.

The boxes "DST No.", "Type" and "Name" are always shown.

- **DST No.**
  Select the type of the entry.
- **Type**
  Select how the daylight saving time changeover is made:
  - Date
    You can enter a fixed date for the daylight saving time changeover.
    This setting is suitable for regions in which the daylight saving time changeover is not governed by rules.
  - Recurring
    You can define a rule for the daylight saving time changeover.
    This setting is suitable for regions in which the daylight saving time always begins or ends on a certain weekday.
- **Name**
  Enter a name for the entry.
  The name can be a maximum of 16 characters long.

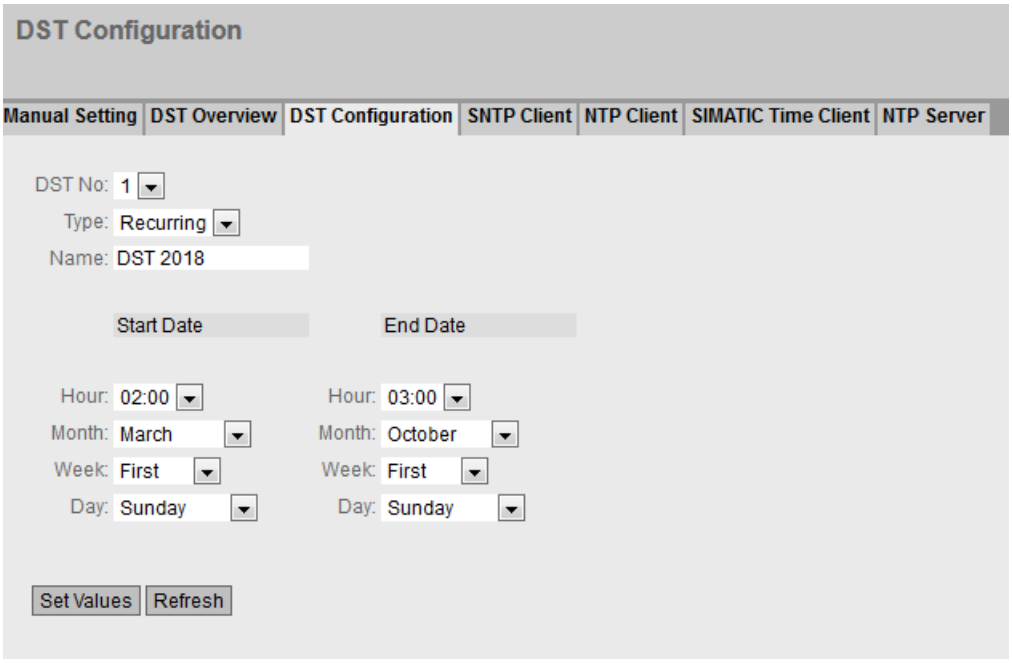
Settings with "Date" selected



You can set a fixed date for the start and end of daylight saving time.

- **Year**
  Enter the year for the daylight saving time changeover.
- **Start Date**
  Enter the following values for the start of daylight saving time:
  - Day
    Enter the day.
  - Hour
    Enter the hour.
  - Month
    Enter the month.
- **End Date**
  Enter the following values for the end of daylight saving time:
  - Day
    Enter the day.
  - Hour
    Enter the hour.
  - Month
    Enter the month.

Settings with "Recurring" selected



You can create a rule for the daylight saving time changeover.

- **Year**
  Enter the year for the daylight saving time changeover.
- **Start Date**
  Enter the following values for the start of daylight saving time:
  - Hour
    Enter the hour.
  - Month
    Enter the month.
  - Week
    Enter the week.
    You can select the first to fourth or the last week of the month.
  - Day
    Enter the weekday.
- **End Date**
  Enter the following values for the end of daylight saving time:
  - Hour
    Enter the hour.
  - Month
    Enter the month.
  - Week
    Enter the week.
    You can select the first to fourth or the last week of the month.
  - Day
    Enter the weekday.

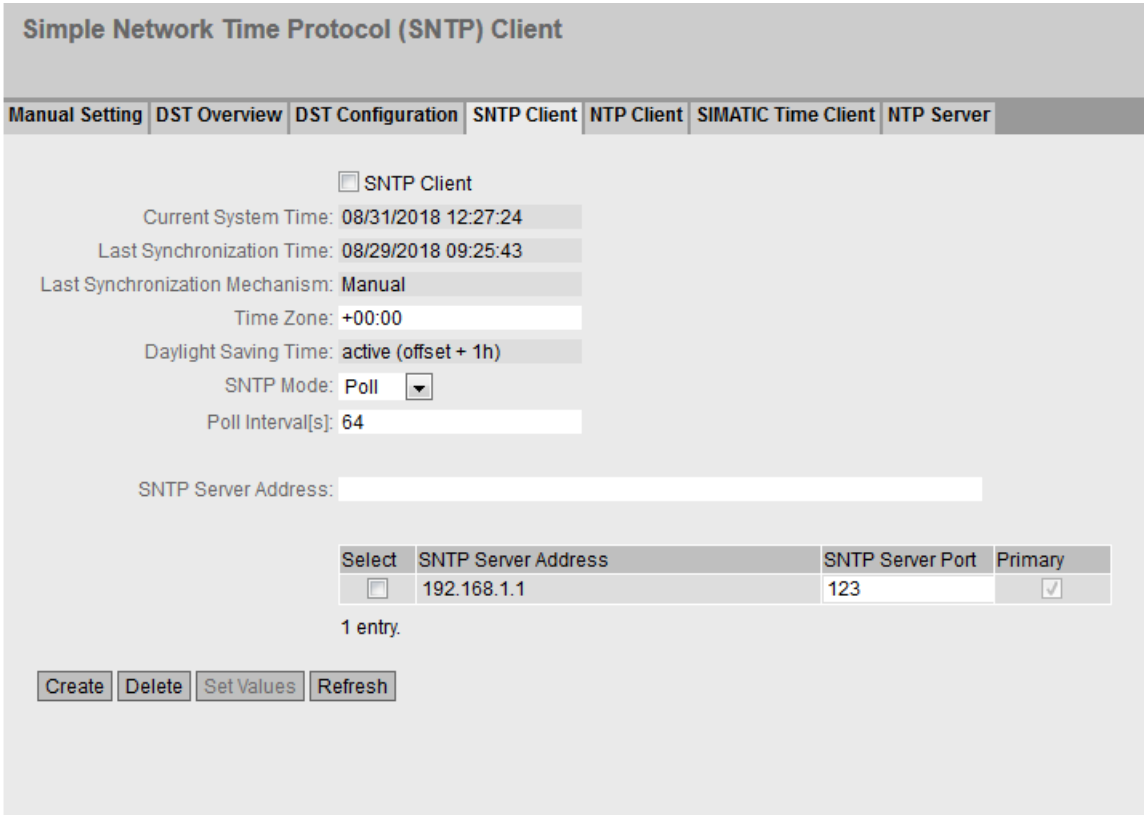
4.4.10.4 SNTP Client

Time-of-day synchronization in the network

SNTP (**Simple Network Time Protocol**) is used for synchronizing the time in the network. The appropriate frames are sent by an SNTP server in the network.

Note

To avoid time jumps, make sure that there is only one time server in the network.



Requirement

To receive the SNTP frames, enable the entry "System Time" under "Security > Firewall > Predefined IPv4 rules".

Description

The page contains the following boxes:

- **SNTP Client**
  When enabled, the device receives the system time from an SNTP server.
- **Current System Time**
  Shows the current date and current normal time received by the IE switch. If you specify a time zone, the time information is adapted accordingly.
- **Last Synchronization Time**
  Shows when the last time-of-day synchronization took place.
- **Last Synchronization Mechanism**
  Shows how the last time synchronization was performed. The following types are possible:
  - Not set
    The time was not set.
  - Manual
    Manual time setting
  - SNTP
    Automatic time-of-day synchronization with SNTP
  - NTP
    Automatic time-of-day synchronization with NTP
  - SIMATIC
    Automatic time-of-day synchronization using the SIMATIC time frame
- **Time Zone**
  In this box, enter the time zone you are using in the format "+/- HH:MM". The time zone relates to UTC standard world time.
  The time in the "Current System Time" box is adapted accordingly.
- **Daylight Saving Time**
  Shows whether the daylight saving time changeover is active.
  - active (offset +1 h)
    The system time was changed to daylight saving time; in other words, an hour was added. You can see the current system time at the top right in the selection area of the WBM. The set time continues to be displayed in the "System Time" box.
  - inactive (offset +0 h)
    The current system time is not changed.

- **SNTP Mode**
  Select the synchronization mode from the drop-down list. The following types are possible:
  - Poll
    If you select this mode, the text boxes "SNTP Server Address", "SNTP Server Port" and "Poll Interval[s]" are displayed to allow further configuration. With this type of synchronization, the device is active and sends a time query to the SNTP server.
    In this mode, IPv4 and IPv6 addresses are supported.
  - Listen
    With this type of synchronization, the device is passive and receives SNTP frames that deliver the time of day. The settings in the text boxes "SNTP Server Address" and "SNTP Server Port" have no effect in this mode.
    In this mode, IPv4 and IPv6 addresses are supported.

    Note

    SNTP Client in Listen mode and NTP Server cannot be enabled at the same time.

- **Poll Interval[s]**
  Enter the interval between two time queries. In this box, you enter the polling interval in seconds. Possible values are 16 to 16284 seconds.
- **SNTP Server Address**
  Enter the IP address, the FQDN (Fully Qualified Domain Name) or the host name of the SNTP server.

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **SMTP Server Address**
  Shows the IP address, the FQDN (Fully Qualified Domain Name) or the host name of the SMTP server.
- **SNTP Server Port**
  Enter the port of the SNTP server.
  The following ports are possible:
  - 123 (standard port)
  - 1025 to 36564
- **Primary**
  The check mark is set for the SNTP server that you create first. If several SNTP servers have been created, the primary server is queried first.

Procedure

1. Click the "SNTP Client" check box to enable the automatic time setting.
2. In "Time Zone", enter the local time difference to world time (UTC).
   The input format is "+/-HH:MM" because the NTP server always sends UTC time, for example +02:00 for CEST, the Central European Summer Time. This time is recalculated and displayed as the local time based on the specified time zone.

3. Select one of the following options from the "SNTP Mode" drop-down list:
   – Poll
     For this mode, you need to configure the following:
     - time zone difference (step 2)
     - query interval (step 4)
     -time server (step 5)
     - Port (step 7)
     - complete the configuration with step 8.
   – Listen
     For this mode, you need to configure the following:
     - time difference to the time sent by the server (step 2)
     - time server (step 5)
     - port (step 7)
     - complete the configuration with step 8.
4. In "SNTP Server Address", enter the address of the SNTP server whose frames will be used to synchronize the time of day.
5. In "SNTP Server Port", enter the port via which the SNTP server is available. The port can only be modified if the IP address of the SNTP server is entered.
6. In "Poll Interval[s]", enter the time in seconds after which a new time query is sent to the time server.
7. Click the "Set Values" button.

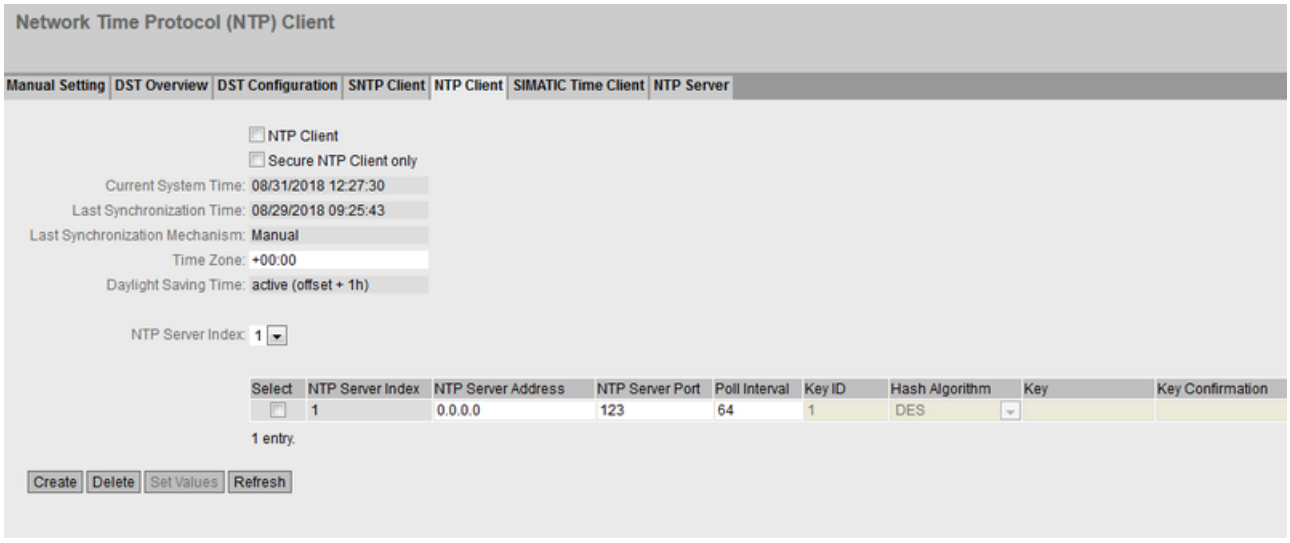
4.4.10.5 NTP Client

Automatic time-of-day setting with NTP

If time synchronization is to take place via NTP, define the time server that is used to synchronize the time.

Note

To avoid time jumps, make sure that there is only one time server in the network.



Requirement

To receive the NTP frames, enable the entry "System Time" under "Security > Firewall > Predefined IPv4 rules".

Description

The page contains the following boxes:

- **NTP client**
  When enabled, the device receives the system time from an NTP server.
- **Secure NTP Client only**
  When enabled, the device receives the system time from a secure NTP server. The setting applies to all server entries.
  To use the secure NTP client, you configure the parameters for authentication (key ID, hash algorithm, key).
- **Current System Time**
  Shows the current date and current normal time received by the device. If you specify a time zone, the time information is adapted accordingly.
- **Last Synchronization Time**
  Shows when the last time-of-day synchronization took place.

- **Last Synchronization Mechanism**
  Shows how the last time synchronization was performed. The following methods are possible:
  - Not set
    The time was not set.
  - Manual
    Manual time setting
  - SNTP
    Automatic time-of-day synchronization with SNTP
  - NTP
    Automatic time-of-day synchronization with NTP
  - SIMATIC
    Automatic time-of-day synchronization using the SIMATIC time frame
  - PTP
    Automatic time-of-day synchronization with PTP
- **Time Zone**
  Enter the time zone you are using in the format "+/- HH:MM". The time zone relates to UTC standard world time.
  The time in the "Current System Time" box is adapted accordingly.
- **Daylight Saving Time**
  Shows whether the daylight saving time changeover is active.
  - active (offset +1 h)
    The system time was changed to daylight saving time; in other words, an hour was added. You can see the current system time at the top right in the selection area of the WBM. The set time continues to be displayed in the "System Time" box.
  - inactive (offset +0 h)
    The current system time is not changed.
- **NTP Server Index**
  Select the index of the NTP server. The NTP servers are queried in the order of the NTP Server Index. The time of the server that is found first is applied. If time frames of an NTP server with a smaller stratum value are received, this time is applied. The switchover to the time with the smaller stratum takes about 30 minutes

In the table, configure the NTP server

- **Select**
  Select the row you want to delete.
- **NTP Server Index**
  Number corresponding to a specific NTP server entry.
- **NTP Server Address**
  Enter the IP address, the FQDN (Fully Qualified Domain Name) or the host name of the NTP server.

- **NTP Server Port**
  Enter the port of the NTP server.
  The following ports are possible:
  - 123 (standard port)
  - 1025 to 36564
- **Poll Interval**
  Specify the interval between two-time queries. The greater the interval, the less accurate the time of the device.
  Possible values are 64 to 2592000 seconds (30 days).

The following columns are only relevant for a secure NTP client. If the check box "Secure NTP Client only" is not selected, these boxes are grayed out:

- **Key ID**
  Enter the ID of the authentication key.
- **Hash Algorithm**
  Specify the format for the authentication key.
- **Key**
  Enter the authentication key. The length depends on the hash algorithm.
  - DES: ASCII 8 characters
  - MD5: ASCII 16 – 128 characters
  - SHA1: ASCII 20 – 128 characters
- **Key confirmation**
  Repeat the authentication key.

Procedure

Time-of-day synchronization with NTP server

1. Click in the "NTP Client" check box to enable the automatic time setting using NTP.
2. In "Time Zone", enter the local time difference to world time (UTC).
   The input format is "+/-HH:MM" because the NTP server always sends UTC time, for example +02:00 for CEST, the Central European Summer Time. This time is recalculated and displayed as the local time based on the specified time zone.
3. Select the "NTP Server Index".
4. Click the "Create" button.
   A new row is inserted in the table for the NTP server.
5. In "NTP Server Address", enter the address of the NTP server whose frames are used to synchronize the time of day.
6. In "NTP Server Port", enter the port via which the NTP server is available. The port can only be modified if the address of the NTP server is entered.
7. In the "Poll Interval" column, enter the interval in seconds after which a new time-of-day query is sent to the time server.
8. Click the "Set Values" button.

Time-of-day synchronization via a secure NTP server

To synchronize the time of day via a secure NTP server, the following additional steps are necessary:

1. Click the "Secure NTP Client only" check box to enable the automatic time setting using Secure NTP.
2. Configure the authentication.
   - In "Key ID" enter the ID of the authentication key.
   - In "Hash Algorithm" select the required format.
   - In "Key" enter the authentication key.

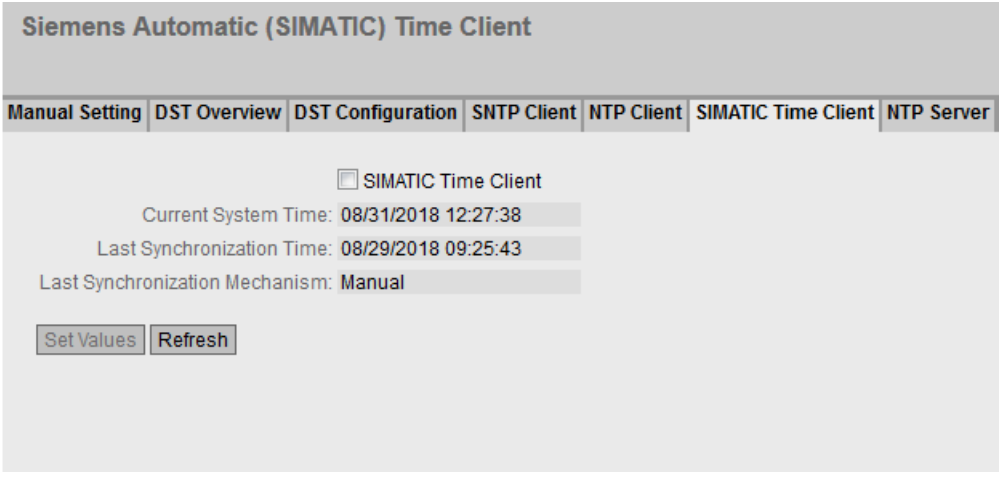
   With these entries, the NTP client authenticates itself with the secure NTP server. These entries must be present on the secure NTP server.
3. Click the "Set Values" button.

4.4.10.6 SIMATIC Time Client

Time setting via SIMATIC time client

Note

To avoid time jumps, make sure that there is only one time server in the network.



Description

The page contains the following boxes:

- **SIMATIC Time Client**
  Select this check box to enable the device as a SIMATIC time client.
- **Current System Time**
  Shows the current system time.

- **Last Synchronization Time**
  Shows when the last time-of-day synchronization took place.
- **Last Synchronization Mechanism**
  Shows how the last time synchronization was performed. The following methods are possible:
  - Not set
    The time was not set.
  - Manual
    Manual time setting
  - SNTP
    Automatic time-of-day synchronization with SNTP
  - NTP
    Automatic time-of-day synchronization with NTP
  - SIMATIC
    Automatic time-of-day synchronization using the SIMATIC time frame

Procedure

1. Click the "SIMATIC Time Client" check box to enable the SIMATIC Time Client.
2. Click the "Set Values" button.

4.4.10.7 NTP server

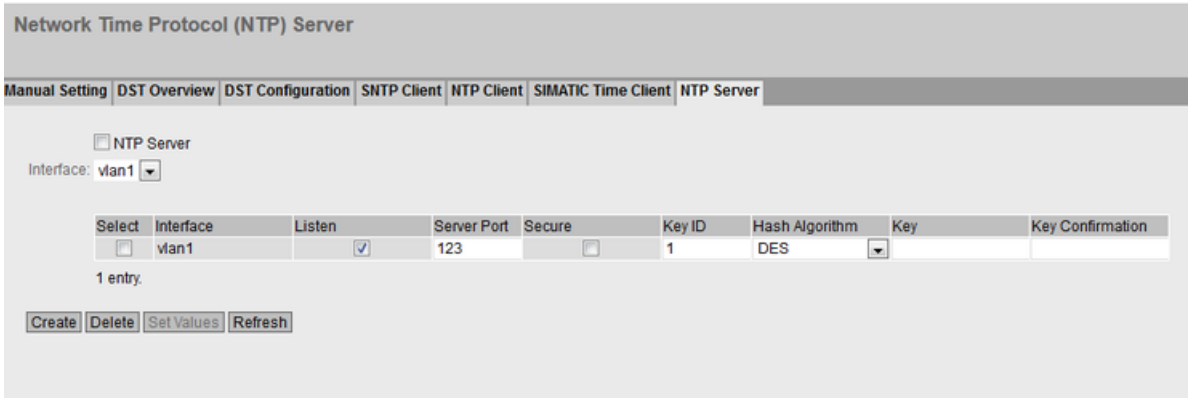
On this WBM page, you configure the device as an NTP server or as an NTP server of the type "NTP (secure)". The other devices can call up the time made available by the device via this NTP server. This means that the supplied devices are not dependent on a connection to an external time server.

Note

Time synchronization

Also configure the device as NTP client so that it synchronizes the connected devices to a correct time. As NTP client, the device gets the precise time from an external time server and as NTP server distributes it to its NTP clients.

The NTP server does not send cyclic messages with time information on its own, but only responds to corresponding requests. Settings in the function as a client (time zone and daylight saving time) do not influence the time information that the device sends as a server.



Requirement

- To receive the NTP frames, enable the entry "System Time" under "Security > Firewall > Predefined IPv4 rules".

Description

The page contains the following boxes:

- **NTP Server**
  Enable or disable the service of the NTP server.

  Note

  SNTP Client in Listen mode and NTP Server cannot be enabled at the same time.

- **Interface**
  Specify the interface via which the time is transferred using NTP.

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **Interface**
  Via this interface the time is transferred using NTP.
- **Listen**
  When enabled, the other devices can call up the time via this interface.
- **Server Port**
  Enter the port of the NTP server.
  The following ports are possible:
  - 123 (standard port)
  - 1025 to 36564
- **Secure**
  When this is enabled, the NTP server becomes an NTP server of the type "NTP (secure)".

The following columns are only relevant for "NTP (secure)". Otherwise, these boxes cannot be edited:

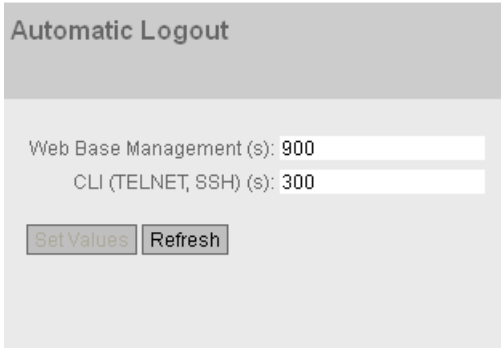
- **Key ID**
  Enter the ID of the authentication key.
- **Hash Algorithm**
  Specify the format for the authentication key.
- **Key**
  Enter the authentication key. The length depends on the hash algorithm.
  The following minimum lengths are recommended for the hash algorithm:
  - DES: ASCII 8 characters
  - MD5: ASCII 16 characters
  - SHA1: ASCII 20 characters
- **Key Confirmation**
  Enter the authentication key for confirmation.

4.4.11 Auto logout

Setting the automatic logout

On this page, set the times after which there is an automatic logout from WBM or the CLI following user in activity.

If you have been logged out automatically, you will need to log in again.



Procedure

1. Enter a value of 60-3600 seconds in the "Web Base Management (s)" input box. If you enter the value 0, the automatic logout is disabled.
2. Enter a value of 60-600 seconds in the "CLI (SSH, Serial) (s)" input box. If you enter the value 0, the automatic logout is disabled.
3. Click the "Set Values" button.

4.4.12 Button

Functionality

The SET button is used for:

- Resetting to factory settings.
- Defining the fault mask and the LED display.

You will find a detailed description of the functions in the operating instructions for the device.

On this page, the functionality of the button can be restricted.

Description

The following functionality is possible:

- **Restore Factory Defaults**
  When disabled, the SET button cannot be used to restore factory defaults.

  CAUTION

  Button function "Restore Factory Defaults" active during startup

  If you have disabled this function in your configuration, disabling is only valid during operation. When restarting, for example after power down, the function is active until the configuration is loaded so that the device can inadvertently be reset to the factory settings. This may cause unwanted disruption in network operation since the device then needs to be reconfigured. An inserted PLUG is also deleted and returned to the status as shipped.

- **Set Fault Mask**
  Enable or disable the function "Define fault mask via the LED display" with the SELECT/SET button.

Configuration procedure

1. To use the functionality, select the corresponding check box.
2. Click the "Set Values" button.

See also

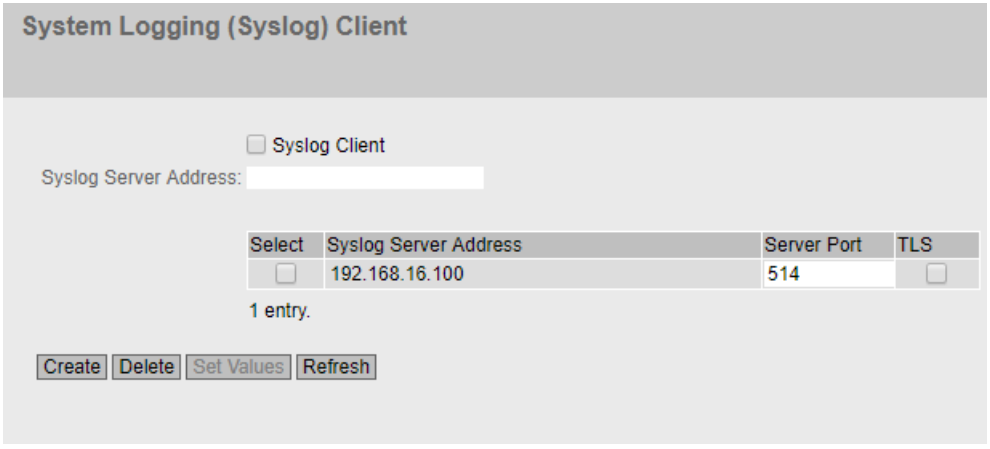
Upkeep and maintenance (Page 421)

4.4.13 Syslog client

On this page, you configure the Syslog client. The Syslog messages can be sent to the Syslog server unencrypted or encrypted.

Requirements for sending Syslog messages

- The Syslog client is enabled.
- In "System > Events > Configuration", "Syslog" is activated for the relevant event.
- There is a Syslog server in your network that receives the Syslog messages.
- The IP address or the FQDN (Fully Qualified Domain Name) of the Syslog server is entered in the device.



Description

The page contains the following boxes:

- **Syslog Client**
  Enable or disable the Syslog client on the device.
- **Syslog Server Address**
  Enter the IP address, the FQDN (Fully Qualified Domain Name) or the host name of the Syslog server.

This table contains the following columns

- **Select**
  Select the row you want to delete.
- **Syslog Server Address**
  Shows the IP address, the FQDN (Fully Qualified Domain Name) or the host name of the Syslog server.

- **Server Port**
  Enter the port of the Syslog server being used.
- **TLS**
  - Enabled
    The syslog messages are sent using TLS encryption over TCP.
  - Disabled
    Syslog messages are sent unencrypted over UDP.

Procedure

Enabling function

1. Select the "Syslog Client" check box.
2. Click the "Set Values" button.

Creating a new entry

1. In the "Syslog Server Address" input box, enter the address of the Syslog server to which the Syslog messages are sent.
2. Click the "Create" button. A new row is inserted in the table.
3. In the "Server Port" input box, enter the number of the server port.
4. Click the "Set Values" button.

Note

The default setting of the server port is 514.

Changing the entry

1. Delete the entry.
2. Create a new entry.

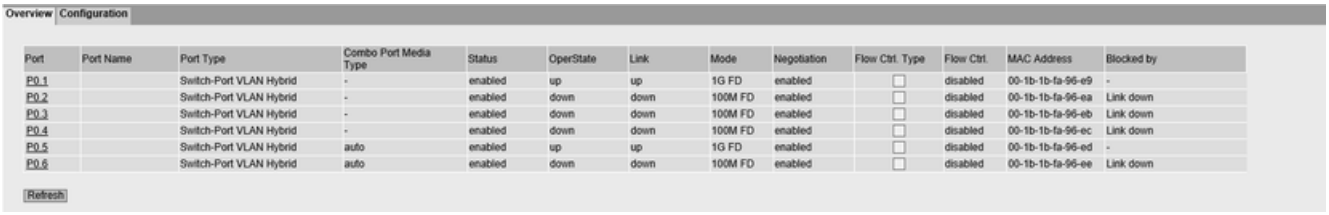
Deleting an entry

1. Select the check box in the row to be deleted.
2. Click the "Delete" button. All selected entries are deleted and the display is refreshed.

4.4.14 Ports

4.4.14.1 Overview

The page shows the configuration for the data transfer for all ports of the device. You cannot configure anything on this page.



Description

The table has the following columns:

- **Port**
  Shows the configurable ports. The entry is a link. If you click on the link, the corresponding configuration page is opened. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.
- **Port Name**
  Shows the name of the port.
- **Port Type** (only with routing)
  Shows the type of the port. The following types are possible:
  - Switch Port VLAN Hybrid
  - Switch Port VLAN Trunk
- **Combo Port Media Type**
  This column contains a value only with combo ports.
  Shows the mode of the combo port:
  - auto
  - rj45
  - sfp
- **Status**
  Shows whether the port is on or off. Data traffic is possible only over an enabled port.
- **OperState**
  Displays the current operational status. The operational status depends on the configured "Status" and the "Link". The following options are possible:
  - Up
    You have configured the status "enabled" for the port and the port has a valid connection to the network.
  - Down
    You have configured the status "disabled" or "Link down" for the port or the port has no connection.

- **Link**
  Shows the connection status to the network. With the connection status, the following is possible:
  - Up
    The port has a valid link to the network, a "link integrity signal" is being received.
  - Down
    The link is down, for example because the connected device is turned off.
- **Mode**
  Shows the transfer parameters of the port.
- **Negotiation**
  Shows whether the automatic configuration is enabled or disabled.
- **Flow Ctrl. Type**
  Shows whether flow control is enabled or disabled for the port.
- **Flow Ctrl.**
  Shows whether or not flow control is working on this port.
- **MAC Address**
  Shows the MAC address of the port.
- **Blocked by**
  Shows why the port is in the "blocked" status:
  - -
    The port is not blocked.
  - Admin down
    The status "disabled" is configured for the port, see "System > Ports > Configuration".
  - Link down
    The status "enabled" is configured for the port but there is no connection, see "System > Ports > Configuration".
  - Power down
    The status "Link down" is configured for the port, see "System > Ports > Configuration".

Deviating display of the transmission parameters with combo ports

In the connection status "down", the displayed transmission parameters do not match the actual values of the combo port. In the connection status "up", the correct values are displayed.

Initial situation

A pluggable transceiver is plugged into the combo port with the following settings:

- Combo Port Media Type: auto
- Status: enabled
- Link: down

Display of the transmission parameters

With 100 Mbps pluggable transceivers

- Actual response: Mode: 100M HD
- Expected response: Mode: 100M FD

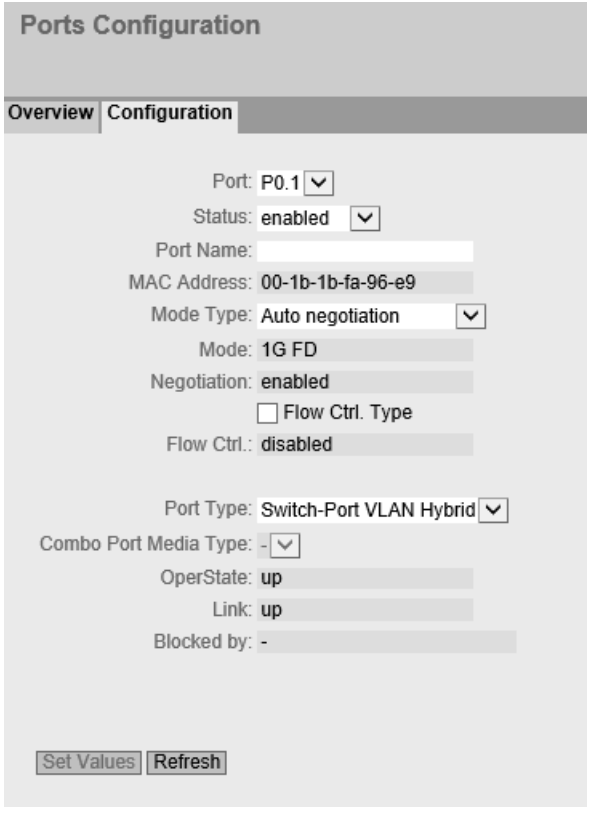
With 1 Gbps pluggable transceivers

- Actual response: Mode: 1G HD
- Expected response: Mode: 1G FD

4.4.14.2 Configuration

Configuring ports

With this page, you can configure all the ports of the device.



Description

- **Port**
  Select the port to be configured from the drop-down list.
- **Status**
  Specify whether the port is enabled or disabled.
  - enabled
    The port is enabled. Data traffic is possible only over an enabled port.
  - disabled
    The port is disabled but the connection remains.

    Note

    Turn off unused ports.

  - Link down
    The port is disabled and the connection to the partner device is terminated.
  - Power down
    The port is disabled. This option can be selected independently of the connection status. To enable the port again, select the entry "enabled" from the drop-down list.
- **Port Name**
  Here, enter a name for the port.
- **MAC Address**
  Shows the MAC address of the port.
- **Mode Type**
  From this drop-down list, select the transmission speed and the transfer mode of the port. If you set the mode to "Autonegotiation", these parameters are automatically negotiated with the connected device or network component. This must also be in the "Autonegotiation" mode for this purpose.

  Note

  Before the port and partner port can communicate with each other, the settings must match at both ends.

  Note

  "Mode Type" with combo ports

  To be able to set the "Mode Type" of a combo port, change the "Combo Port Media Type" to "rj45". If "auto" is set for the "Combo Port Media Type" and the RJ-45 port is used, you cannot set the "Mode Type".

- **Mode**
  Shows the transmission speed and the transmission mode of the port. The following settings are possible:
  - 10 Mbps full duplex (FD) or half duplex (HD)
  - 100 Mbps full duplex (FD) or half duplex (HD)
  - 1000 Mbps (full duplex)

- **Negotiation**
  Shows whether the automatic configuration of the connection to the partner port is enabled or disabled.

Note

Turning flow control on/off with autonegotiation

Flow control can only be enabled or disabled if the "Autonegotiation" function is turned off. The function cannot be enabled again afterwards.

- **Flow Ctrl. Type**
  Enable or disable flow control for the port.
- **Flow Ctrl.**
  Shows whether flow control is working on this port.
- **Port Type**
  Select the type of port from the drop-down list.
  - Switch-Port VLAN Hybrid
    The port sends tagged and untagged frames. It is not automatically a member of a VLAN.
  - Switch-Port VLAN Trunk
    The port only sends tagged frames and is automatically a member of all VLANs.

Note

Private VLAN functionality and RADIUS authentication

When VLAN assignment is enabled via RADIUS authentication for one or more ports of a VLAN, you should not configure this VLAN additionally as private VLAN.

The private VLAN functionality in connection with VLAN assignment via RADIUS authentication can result in an inconsistent system state.

- **Combo Port Media Type**
  Specify the mode of the combo port:
  - auto
    If you select this mode, the pluggable transceiver port has priority.
    As soon as a pluggable transceiver is plugged in, an existing connection at the fixed RJ-45 port is terminated. If no pluggable transceiver is plugged in, a connection can be established via the fixed RJ-45 port.
  - rj45
    If you select this mode, the fixed RJ-45 port is used regardless of the pluggable transceiver port.
    If a pluggable transceiver is plugged in, it is disabled and the power turned off.
    To run a cable test at the combo port, the media type "rj45" must be set. The cable test is run under "System > Port Diagnostics > Cable Tester".
  - sfp
    If you select this mode, the pluggable transceiver port is used regardless of the fixed RJ-45 port.
    If an RJ-45 connection is established, it is terminated because the power of the RJ-45 port is turned off.

  The factory setting for the combo ports is the "auto" mode.

  Note

  Automatic adaptation due to PROFINET configuration

  When establishing a PROFINET connection, the setting of the combo port media type is adapted automatically:
  - If a pluggable transceiver is configured, the combo port media type will be set to "sfp".
  - If the built-in RJ-45 port is configured, the combo port media type will be set to "rj45".

  So that the automatic adaptation can be made, the combo port media type must be set to "auto".

  Configure the combo port media type accordingly using the WBM or CLI.

- **OperState**
  Displays the current operational status. The operational status depends on the configured "Status" and the "Link". The following options are possible:
  - Up
    You have configured the "enabled" status for the port and the port has a valid connection to the network.
  - Down
    You have configured the "disabled status " or "Link down" for the port or the port has no connection.
  - not present
    With modular devices, this status is displayed when, for example, no media module is inserted.

- **Link**
  Shows the physical connection status to the network. The following options are possible:
  - Up
    The port has a valid link to the network, a "link integrity signal" is being received.
  - Down
    The link is down, for example because the connected device is turned off.
- **Blocked by**
  Shows why the port is in the "blocked" status:
  - -
    The port is not blocked.
  - Admin down
    The status "disabled" is configured for the port, see "System > Ports > Configuration".
  - Link down
    The status "enabled" is configured for the port but there is no connection, see "System > Ports > Configuration".
  - Power down
    The status "Link down" or "Power down" is configured for the port; see "System > Ports > Configuration".

Changing the port configuration

Click the appropriate box to change the configuration.

Note

Optical ports only work with the full duplex mode and at maximum transmission rate. As a result, the following settings cannot be made for optical ports:

- Automatic configuration
- Transmission speed
- Transmission mode

Note

With various automatic functions, the device prevents or reduces the effect on other ports and priority classes (Class of Service) if a port is overloaded. This can mean that frames are discarded even when flow control is enabled.

Port overload occurs when the device receives more frames than it can send, for example as the result of different transmission speeds.

Configuration procedure

1. Change the settings according to your configuration.
2. Click the "Set Values" button.

4.4.15 Fault monitoring

4.4.15.1 Power supply

Settings for monitoring the power supply

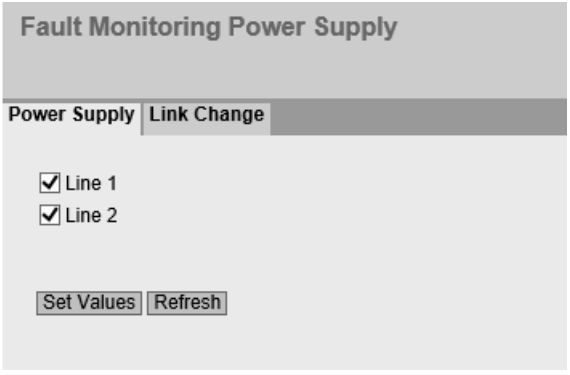
Configure whether or not the power supply should be monitored by the messaging system. With a redundant power supply, configure the monitoring separately for each individual feed-in line.

A fault is then signaled by the message system when there is no power on one of the monitored lines (line 1 or line 2) or when the voltage is too low.

Note

You will find the permitted operating voltage limits in the compact operating instructions of the device.

A fault causes the signaling contact to trigger and the fault LED on the device to light up and, depending on the configuration, can trigger a trap or an entry in the event log table.



Procedure

1. Click the check box in front of the line name you want to monitor to enable or disable the monitoring function.
2. Click the "Set Values" button.

4.4.15.2 Link Change

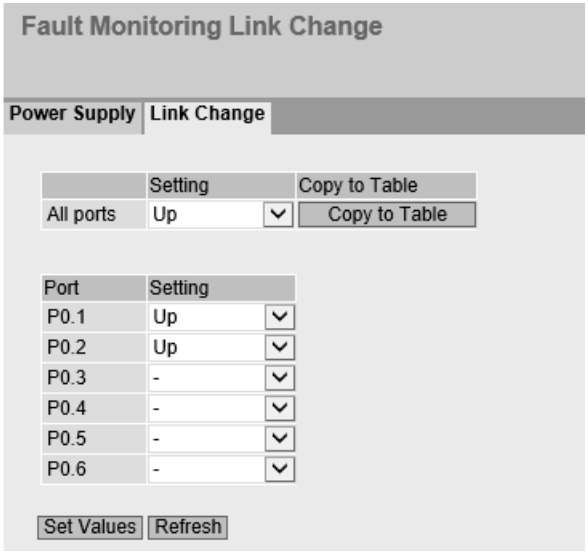
Configuration of fault monitoring of status changes on connections

On this page, you configure whether or not an error message is triggered if there is a status change on a network connection.

If connection monitoring is enabled, an error is signaled

- when there should be a link on a port and this is missing.
- or when there should not be a link on a port and a link is detected.

A fault causes the fault LED on the device to light up and, depending on the configuration, can trigger a trap or an entry in the event log table.



Description

Table 1 has the following columns:

- **1st column**
  Shows that the settings are valid for all ports.
- **Setting**
  Select the setting from the drop-down list. You have the following setting options:
  - "-" (disabled)
  - Up
  - Down
  - No Change: The setting in table 2 remains unchanged.
- **Copy to Table**
  If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
  Shows the available ports. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.
- **Setting**
  Select the setting from the drop-down list. You have the following options:
  - Up
    Error handling is triggered when the port changes to the active status.
    (From "Link down" to "Link up")
  - Down
    Error handling is triggered when the port changes to the inactive status.
    (From "Link up" to "Link down")
  - "-" (disabled)
    The error handling is not triggered.

Procedure

Configure error monitoring for a port

1. From the relevant drop-down list, select the options of the slots / ports whose connection status you want to monitor.
2. Click the "Set Values" button.

Configure error monitoring for all ports

1. Select the required setting from the drop-down list of the "Setting" column.
2. Click the "Copy to Table" button. The setting is adopted for all ports of table 2.
3. Click the "Set Values" button.

4.4.16 PLUG

4.4.16.1 Configuration

NOTICE
Do not remove or insert a C-PLUG / KEY-PLUG during operation! A PLUG may only be removed or inserted when the device is turned off. The device checks whether a PLUG is present at one second intervals. If it is detected that the PLUG was removed, there is a restart. If a valid KEY-PLUG was inserted in the device, the device changes to a defined error state following the restart. With SCALANCE M, the available wireless interfaces are deactivated in this case. If the device was configured at some time with a PLUG, the device can no longer be used without this PLUG. To be able to use the device again, reset the device to the factory settings.

Information about the configuration of the KEY-PLUG

This page provides detailed information about the configuration stored on the C-PLUG. It is also possible to reset the PLUG to "factory defaults" or to load it with new contents.

Note

Incompatibility with older firmware versions with PLUG inserted

During the installation of an older firmware version, the configuration data can be lost. In this case, reset the device to the factory settings after the firmware has been installed.
In this situation, when a PLUG is inserted in the device, following the restart, this has the status "NOT ACCEPTED" because the PLUG still has the configuration data of the previous more up-to-date firmware. This allows you to return to the previous, more up-to-date firmware without any loss of configuration data.

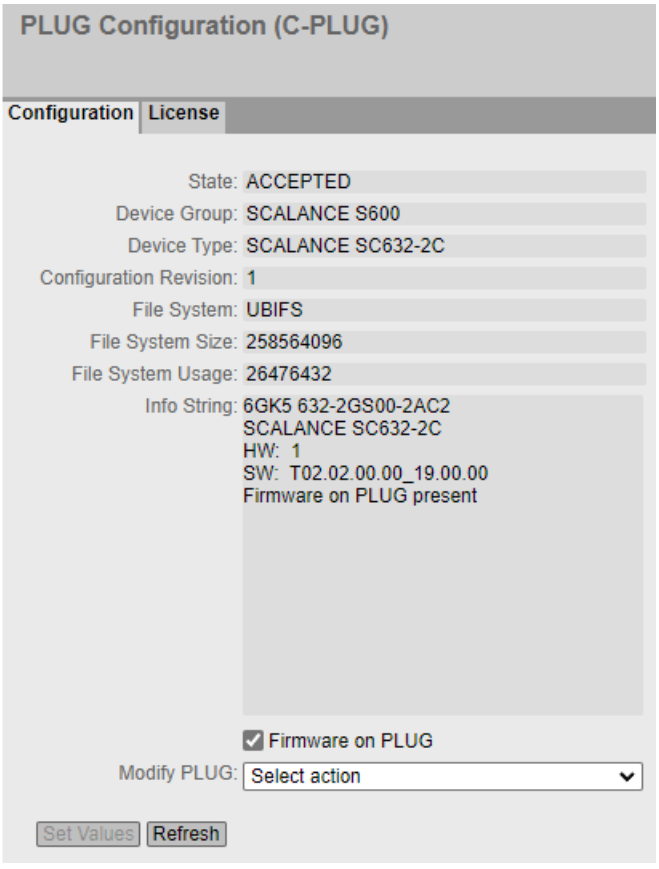
If the original configuration on the PLUG is no longer required, the PLUG can be deleted or rewritten manually using "System > PLUG".

Note

The action is only executed after you click the "Set Values" button.

The action cannot be undone.

If you decide against executing the function after making your selection, click the "Refresh" button. As a result the data of this page is read from the device again and the selection is canceled.



Description

The table has the following rows:

- **Status**
  Shows the status of the PLUG. The following are possible:
  - ACCEPTED
    There is a PLUG with a valid and suitable configuration in the device.
  - NOT ACCEPTED
    Invalid or incompatible configuration on the inserted PLUG.
  - NOT PRESENT
    There is no C-PLUG or KEY-PLUG inserted in the device.
  - FACTORY
    PLUG is inserted and does not contain a configuration. This status is also displayed when the PLUG was formatted during operation.
  - MISSING
    There is no PLUG inserted. Functions are configured on the device for which a license is required.
- **Device Group**
  Shows the SIMATIC NET product line that used the C-PLUG or KEY-PLUG previously.

- **Device Type**
  Shows the device type within the product line that used the C-PLUG or KEY-PLUG previously.
- **Configuration Revision**
  The version of the configuration structure. This information relates to the configuration options supported by the device and has nothing to do with the concrete hardware configuration. This revision information does not therefore change if you add or remove additional components (modules or extenders), it can, however, change if you update the firmware.
- **File System**
  Displays the type of file system on the PLUG.
- **File System Size**
  Displays the maximum storage capacity of the file system on the PLUG.
- **File System Usage**
  Displays the memory utilization of the file system of the PLUG.
- **Firmware on PLUG**
  When the function is enabled (default), the firmware will be stored on the PLUG. This means that automatic firmware updates/downgrades can be made with the PLUG. The "Info" box shows whether or not the firmware is stored on the PLUG.

  Note

  C-PLUG 256 MB V2.2 and higher

  As of firmware version 2.2, you can only save the firmware on a C-PLUG with 256 MB.

- **Info String**
  Shows additional information about the device that used the PLUG previously, for example, article number, type designation, and the versions of the hardware and software. The displayed software version corresponds to the version in which the configuration was last changed. With the "NOT ACCEPTED" status, further information on the cause of the problem is displayed.
  If a PLUG was configured as a PRESET PLUG this is shown here as additional information in the first row. For more detailed information on creating and using a PRESET PLUG refer to the section "Maintenance (Page 421)".
- **Modify PLUG**
  Select the setting from the drop-down list. You have the following options for changing the configuration on the C-PLUG or KEY-PLUG:
  - Write Current Configuration to the PLUG
    This option is available only if the status of the PLUG is "NOT ACCEPTED" or "FACTORY". The configuration in the internal flash memory of the device is copied to the PLUG.
  - Erase PLUG to factory default
    Deletes all data from the PLUG and triggers low-level formatting.

Procedure

1. You can only make settings in this box if you are logged on as "Administrator". Here, you decide how you want to change the content of the PLUG.
2. Select the required option from the "Modify PLUG" drop-down list.
3. Click the "Set Values" button.

4.4.16.2 License

NOTICE
Do not remove or insert a C-PLUG / KEY-PLUG during operation! A PLUG may only be removed or inserted when the device is turned off. The device checks whether a PLUG is present at one second intervals. If it is detected that the PLUG was removed, there is a restart. If a valid KEY-PLUG was inserted in the device, the device changes to a defined error state following the restart. With SCALANCE M, the available wireless interfaces are deactivated in this case. If the device was configured at some time with a PLUG, the device can no longer be used without this PLUG. To be able to use the device again, reset the device to the factory settings.

Note

Incompatibility with previous versions with PLUG inserted

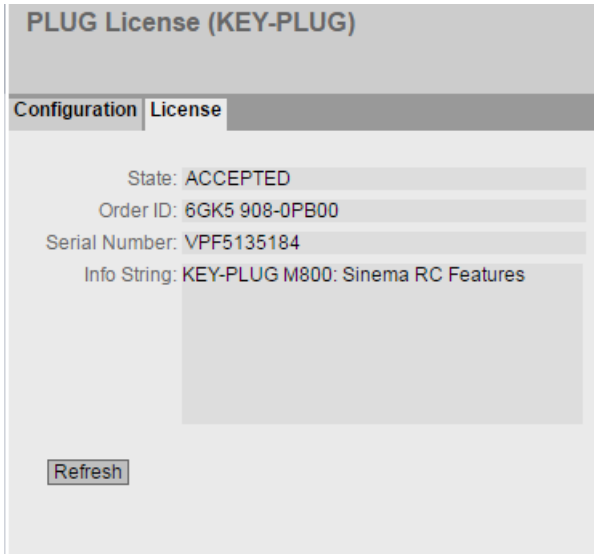
During the installation of a previous version, the configuration data can be lost. In this case, the device starts up with the factory settings after the firmware has been installed. In this situation, if a PLUG is inserted in the device, following the restart, this has the status "NOT ACCEPTED" since the PLUG still has the configuration data of the previous more up-to-date firmware. This allows you to return to the previous, more up-to-date firmware without any loss of configuration data.

If the original configuration on the PLUG is no longer required, the PLUG can be deleted or rewritten manually using "System > PLUG".

Information about the license of the KEY-PLUG

A C-PLUG can only store the configuration of a device. In addition to the configuration, a KEY-PLUG also contains a license that enables certain functions of your SIMATIC NET device.

This page provides detailed information about the license on the KEY-PLUG.



Description

- **Status**
  Shows the status of the KEY-PLUG. The following are possible:
  - ACCEPTED
    There is a KEY-PLUG with a valid and matching license in the device.
  - NOT ACCEPTED
    The license of the inserted KEY-PLUG is not valid.
  - NOT PRESENT
    No KEY-PLUG is inserted in the device.
  - MISSING
    There is no KEY-PLUG inserted with the "FACTORY" status. Functions are configured on the device for which a license is required.
  - WRONG
    The inserted KEY-PLUG is not suitable for the device.
  - UNKNOWN
    Unknown content of the KEY-PLUG.
  - DEFECTIVE
    The content of the KEY-PLUG contains errors.
- **Order ID**
  Shows the order ID of the KEY-PLUG. The KEY-PLUG is available for various functional enhancements and for various target systems.

- **Serial Number**
  Shows the serial number of the KEY-PLUG.
- **Info String**
  Shows additional information about the device that used the KEY-PLUG previously, for example, article number, type designation, and the versions of the hardware and software. The displayed software version corresponds to the version in which the configuration was last changed. With the "NOT ACCEPTED" status, further information on the cause of the problem is displayed.

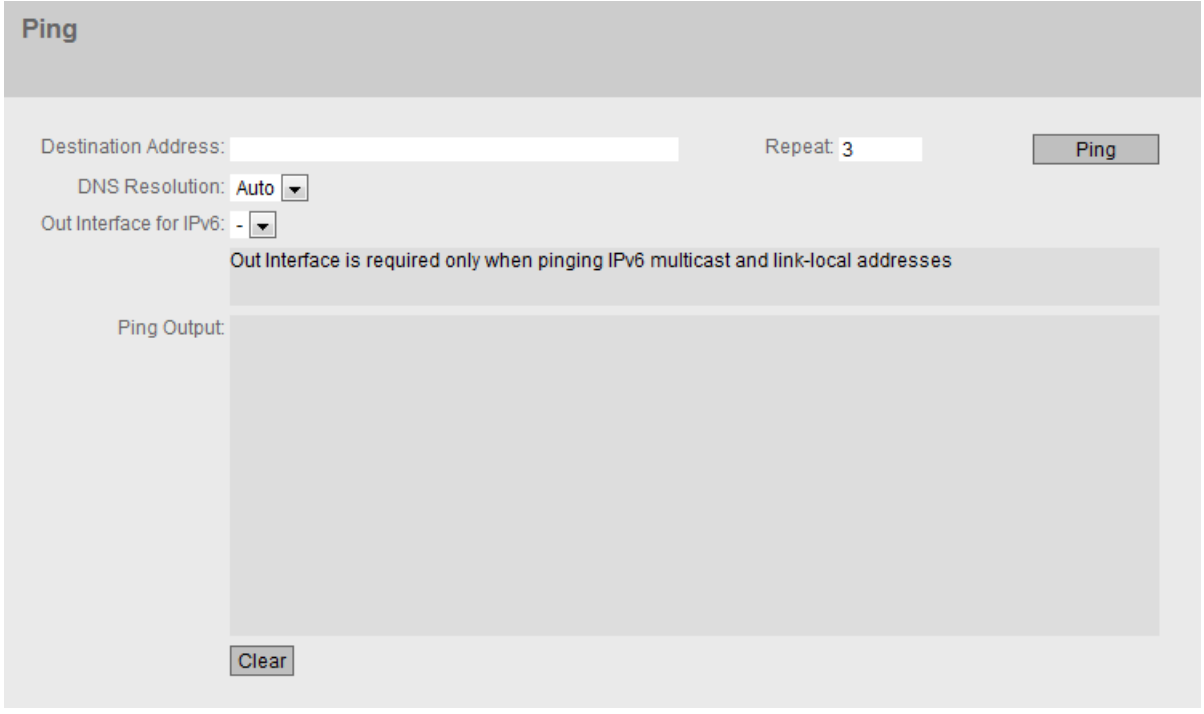
Note

When you save the configuration, the information about whether or not a KEY-PLUG was inserted in the device at the time is also saved. This configuration can then only work if a KEY-PLUG with the same order number / license is inserted.

4.4.17 Ping

Reachability of an address in an IP network

With the Ping function, you can check whether a certain IP address is reachable in the network.



Description

The page contains the following boxes:

- **Destination Address**
  Enter the IPv4, IPv6 address or the FQDN (Fully Qualified Domain Name) of the device.
- **Repeat**
  Enter the number of Ping requests.
- **DNS Resolution**
  Select the IP address type in which an entered FQDN will be resolved.
  - Auto
    In this mode, the IP address type is selected automatically.
  - IPv4
    The entered FQDN will be resolved in an IPv4 address.
  - IPv6
    The entered FQDN will be resolved in an IPv6 address.
- **Out Interface for IPv6**
  This selection is only required when the destination address is a multicast or a link local address.
  - "-" (factory setting)
  - Select the relevant IPv6 interface.
- **Ping**
  Click this button to start the Ping function.
- **Ping Output**
  This box shows the output of the Ping function.
- **Clear**
  Click this button to delete the ping output.

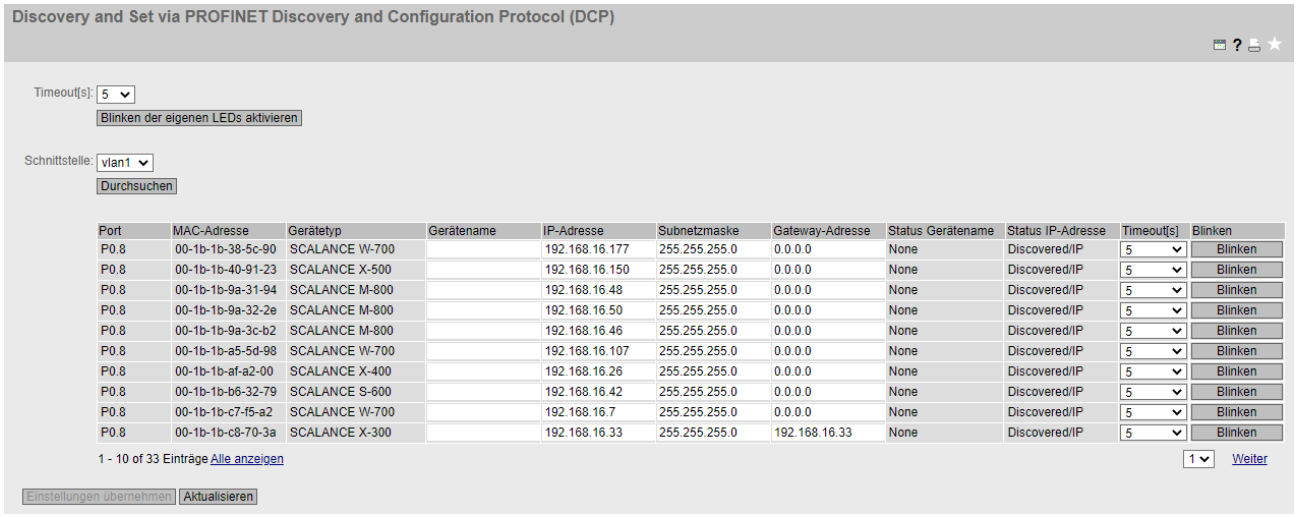
4.4.18 DCP Discovery

On this page, you can select an interface and search for devices that are reachable via the interface and support DCP. DCP Discovery only searches for devices located in the same subnet as the interface. The reachable devices are listed in a table. In the table you can check and adapt the network parameters of the devices. To identify and configure the devices the Discovery Configuration Protocol (DCP) is used.

Note

DCP Discovery

The function is only available with the VLAN associated with the TIA interface. You can configure the TIA interface with "Layer 3 > Subnets > Configuration".



Requirement:

To adapt network parameters, DCP requires write access to the device. If access is write-protected, the network parameters cannot be configured.

On SCALANCE devices, you configure access under "System > Configuration".

Description

The page contains the following boxes:

- **Timeout[s]**
  Specify the time for flashing. When the time elapses, flashing stops.
- **Blink Own LEDs**
  Makes the LEDs of your own device flash.
- **Interface**
  Select the required interface.
- **Discover**
  Starts the search for devices reachable via the selected interface.
  On completion of the search the reachable devices are listed in the table. The table is limited to 100 entries.

The table has the following columns:

- **Port**
  Shows the port via which the device can be reached.
- **MAC Address**
  Shows the MAC address of the device.
- **Device Type**
  Shows the product line or product group to which the device belongs.
- **Device Name**
  Adapt the PROFINET device name if necessary.
  The device name must be DNS-compliant. If the device name is not used, the box is empty.

- **IP Address**
  If necessary, adapt the IPv4 address of the device.
  The IPv4 address should be unique within your network and should match the network. The IPv4 address 0.0.0.0 means that no IPv4 address has yet been set.
- **Subnet mask**
  If necessary, adapt the subnet mask of the device.
- **Gateway Address**
  Adapt the IPv4 address of the gateway if necessary.
- **Status Device Name**
  - None: The device name is not used.
  - Discovered: The set device name is used.
  - Configured: The device was assigned a new device name.
- **IP Status**
  - Discovered/IP: The device uses a static IPv4 address.
  - Discovered/DHCP: The device has obtained the IPv4 address from a DHCP server.
  - Configured: The device was assigned a new IPv4 address.
- **Timeout[s]**
  Specify the time for flashing. When the time elapses, flashing stops.
- **Flash**
  Makes the LEDs of the selected device flash.

Procedure

1. Select the TIA interface.
2. To show all devices that can be reached via the TIA interface, click the "Browse" button.
3. Adapt the desired properties.
4. Click the "Set Values" button.
   The status of the modified properties changes to "Configured".
5. To ensure that the properties were applied correctly, click the "Browse" button again.
   The status of the modified properties changes to "Discovered".

4.4.19 Port diagnostics

4.4.19.1 Cable tester

With this page, each individual Ethernet port can run independent fault diagnostics on the cable. This test is performed without needing to remove the cable, connect a cable tester and install a loopback module at the other end. Short-circuits and cable breaks can be localized to within a few meters.

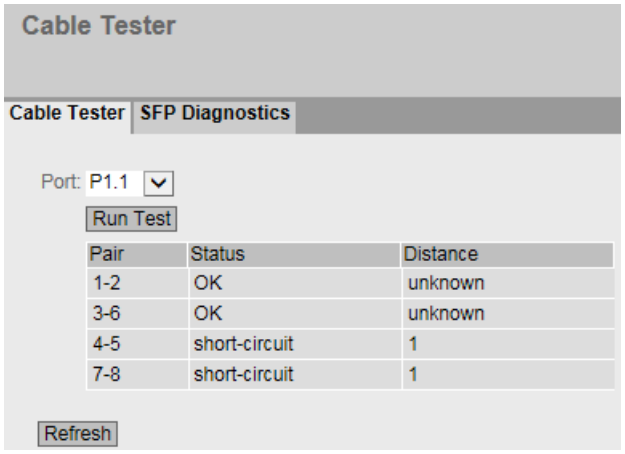
Note

Please note that this test is permitted only when no data connection is established on the port to be tested.

If, however, there is a data connection to the port to be tested, this is briefly interrupted.

Automatic re-establishment of the connection can fail; in this case, the connection needs to be re-established manually.

To run a cable test at the combo port, the "Combo Port Media Type" "RJ45" must be set under "System > Ports > Configuration".



Description

The page contains the following boxes:

- **Port**
  Select the required port from the drop-down list.
- **Run Test**
  Activates error diagnostics. The result is shown in the table.

The table contains the following columns:

- **Pair**
  Shows the wire pair in the cable.

  Note

  Wire pairs

  Wire pairs 4-5 and 7-8 of 10/100 Mbps network cables are not used.

  1000 Mbps or gigabit Ethernet uses all 4 wire pairs.

  The wire pair assignment - pin assignment is as follows (DIN 50173):

  Pair 1 = pin 4-5

  Pair 2 = pin 1-2

  Pair 3 = pin 3-6

  Pair 4 = pin 7-8

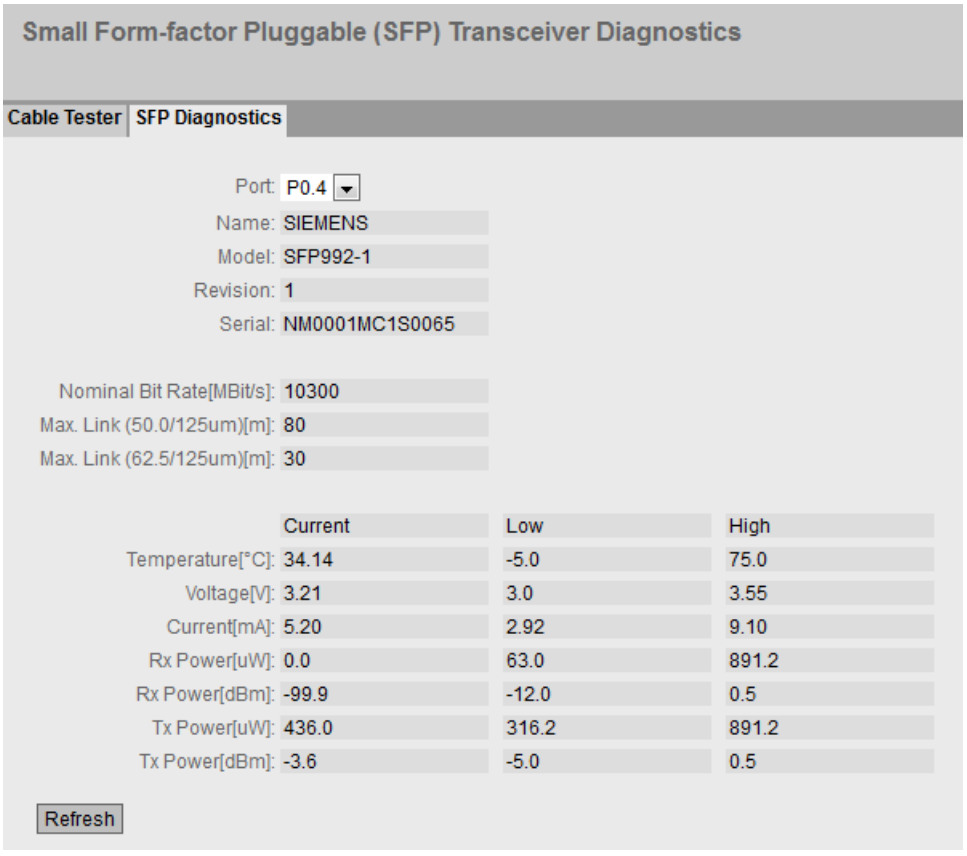
- **Status**
  Displays the status of the cable.
- **Distance**
  Displays the distance to the open cable end, cable break, or short-circuit in meters. The value for the distance has a tolerance of +/- 1 m.
  If the status is "OK", the length is specified with "unknown".

4.4.19.2 SFP diagnostics

On this page, you run independent error diagnostics for each individual SFP port. This test is performed without needing to remove the cable, connect a cable tester or install a loopback module at the other end.

Note

Please note that this test is permitted only when no data connection is established on the port to be tested. If, however, there is a data connection to the port to be tested, this is briefly interrupted. Automatic re-establishment of the connection can fail; in this case, the connection needs to be re-established manually.



Description

The page contains the following boxes:

- **Port**
  Select the required port from the drop-down list.
- **Refresh**
  Refreshes the display of the values of the set port. The result is shown in the table.

The values are shown in the following boxes:

- **Name**
  Shows the name of the interface.
- **Model**
  Shows the type of interface.
- **Revision**
  Shows the hardware version of the SFP.
- **Serial**
  Shows the serial number of the SFP.
- **Nominal Bit Rate [Mbps]**
  Shows the nominal bit rate of the interface.

- **Max. Link (50.0/125um) [m]**
  Shows the maximum distance in meters that is possible with this medium.
- **Max. Link (62.5/125um) [m]**
  Shows the maximum distance in meters that is possible with this medium.

The following table shows the values of the SFP transceiver used in this port:

- **Temperature [°C]**
  Shows the temperature of the interface module.
- **Voltage [V]**
  Shows the voltage applied to the interface in volts.
- **Current [mA]**
  Shows the current consumption of the interface in milliamperes.
- **Rx Power [µW]/Rx Power [dBm]**
  Shows the receive power of the interface in microwatts/decibel milliwatts.
- **Tx Power [µW]/Tx Power [dBm]**
  Shows the transmit power of the interface in microwatts/decibel milliwatts.
- **Current** column
  Shows the current value.
- **Low** column
  Shows the lowest value.
- **High** column
  Shows the highest value.

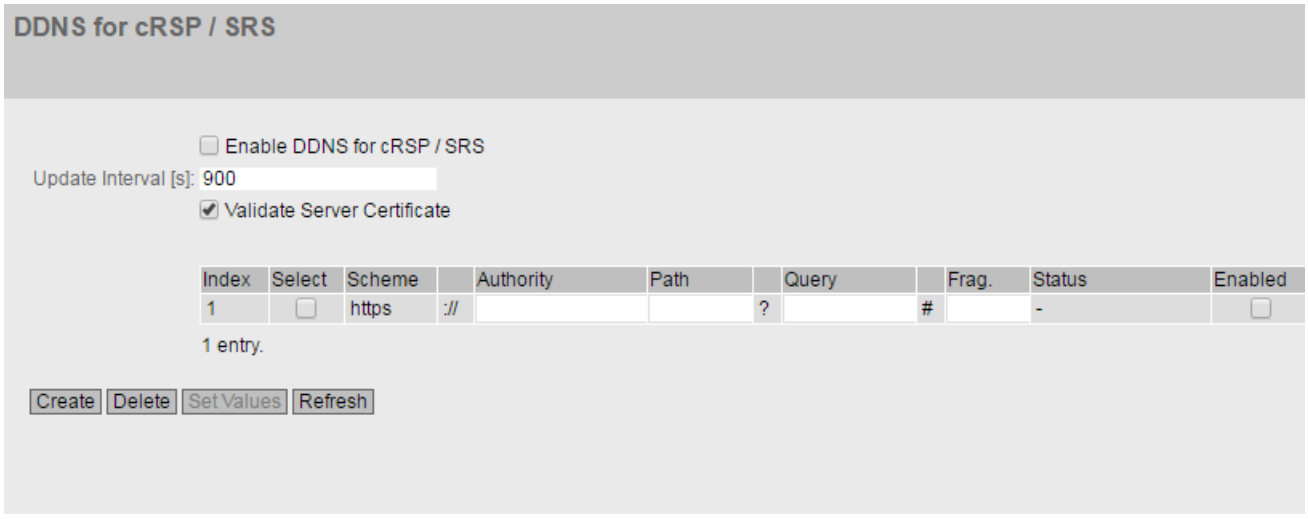
4.4.20 cRSP / SRS

Note

Common Remote Service Platform (cRSP) / Siemens Remote Service (SRS) is a remote maintenance platform via which remote maintenance access is possible.

To use the platform, additional service contracts are necessary and certain constraints must be kept to. If you are interested in cRSP / SRS, call your local Siemens contact or visit Web page (https://support.industry.siemens.com/cs/de/en/sc/2281).

On this page, you configure the access data for the SRS / cRSP acc. to URI syntax. The Uniform Resource Identifier (URI) is defined in RFC 3986.



Description

The page contains the following boxes:

- **Enable DDNS for cRSP / SRS**
  Enable or disable the use of cRSP / SRS.
- **Update Interval [s]**
  Enter the time interval.
- **Validate Server Certificate**
  When enabled, the device checks the validity of the received server certificate.

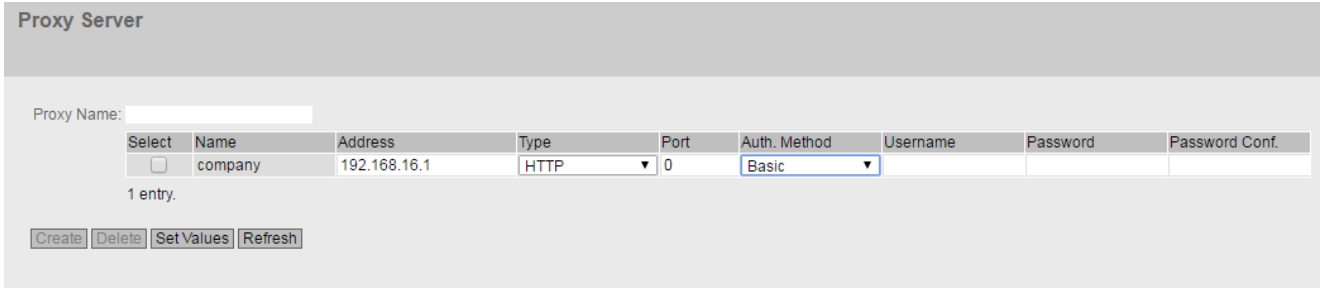
The table has the following columns:

- **Index**
  The number of the entry.
- **Select**
  Select the check box in the row to be deleted. Click "Delete" to delete the entry.
- **Scheme**
  Identifies the access method and the resource type.
  https: Secure access to a Web page.
- **Authority**
  Contains the address of the destination server
- **Path**
  Contains the target path to the resource. The target path can correspond to a directory name or file name.
- **Query**
  A query can contain parameter values for an application.
  - WAN_IP (keyword): Replaces WAN_IP with current external IP address of the device to the destination server.
- **Frag**.
  Addresses local parts of the resource, e.g. the anchor attribute of a Web page.

- **Status**
  Shows the status of the last cRSP / SRS access of the entry.
- **Enabled**
  When enabled, this entry is used.

4.4.21 Proxy server

On this WBM page, you configure the proxy server that is used by various components, for example SINEMA RC.



Description

- **Proxy Name**
  Enter a name for the proxy server.

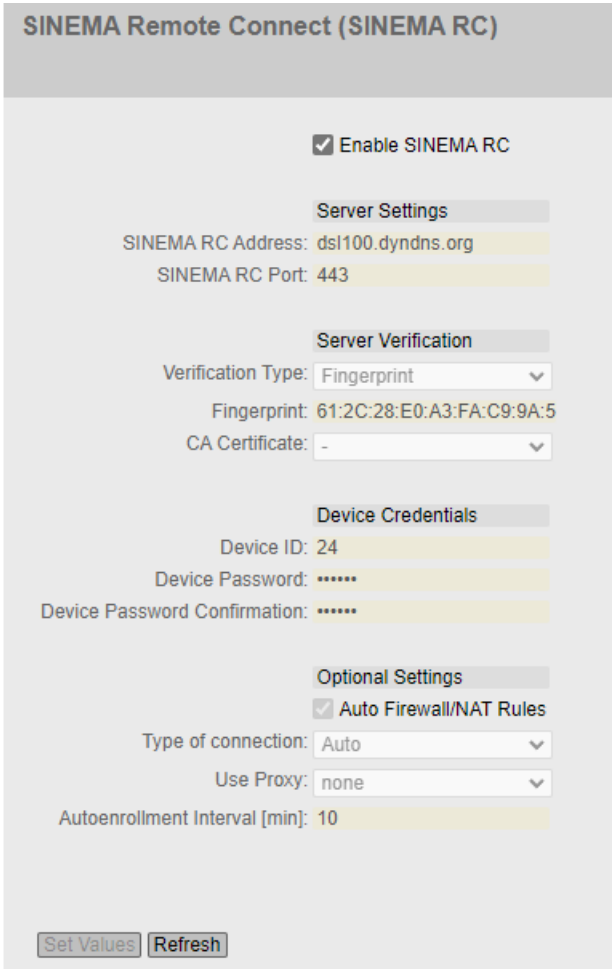
The table has the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **Name**
  Shows the name of the proxy server.
- **Address**
  Enter the IPv4 address of the proxy server.
- **Type**
  Specify the type of the proxy server.
  - HTTP: Proxy server only for access using HTTP.
  - SOCKS: Universal proxy server
- **Port**
  Enter the port on which the proxy service runs.

- **Auth. Method**
  Specify the authentication method.
  - None
    No authentication
  - Basic
    Standard authentication. User name and password are sent unencrypted.
  - NTML (NT LAN Manager)
    Authentication according to the NTML standard (Windows user logon)
- **User Name**
  Enter the user name for access to the proxy server.
- **Password**
  Enter the password for access to the proxy server.
- **Password Confirmation**
  Enter the password again to confirm it.

4.4.22 SINEMA RC

On the WBM page, you configure the access to the SINEMA RC server.



Description

The page contains the following:

- **Enable SINEMA RC**
  - Enabled
    A connection to the configured SINEMA RC Server is established. These boxes cannot be edited.
  - Disabled
    The boxes can be edited. Any existing connection is terminated.

"Server settings" area

- **SINEMA RC Address**
  Enter the IP address or the FQDN (Fully Qualified Domain Name) of the SINEMA RC Server.
- **SINEMA RC Port**
  Enter the port via which the SINEMA RC Server can be reached.

"Server Verification" area

- **Verification Type**
  - Fingerprint: The identity of the server is verified based on the fingerprint.
  - CA Certificate: The identity of the server is verified based on the CA certificate.
- **Fingerprint**
  Only necessary with the setting "Fingerprint". Enter the fingerprint of the device. The fingerprint is assigned during commissioning of the SINEMA RC Server. Based on the fingerprint, the device checks whether the correct SINEMA RC Server is involved. You will find further information on this in the Operating Instructions of the SINEMA RC Server.
- **CA Certificate**
  Only necessary with the setting "CA Certificate". Select the CA certificate of the server used to sign the server certificate. Only loaded CA certificates can be selected.

"Device Credentials" area

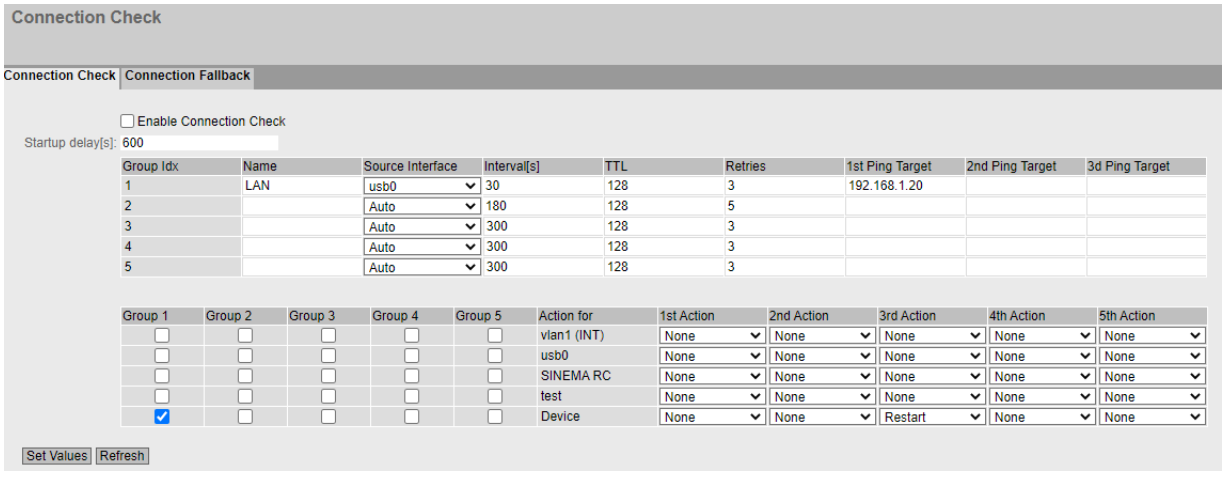
- **Device ID**
  Enter the device ID. The device ID is assigned when configuring the device on the SINEMA RC Server. You will find further information on this in the Operating Instructions of the SINEMA RC Server.
- **Device Password**
  Enter the password with which the device logs on to the SINEMA RC Server. The password is assigned when configuring the device on the SINEMA RC Server. You will find further information on this in the Operating Instructions of the SINEMA RC Server.
- **Device Password Confirmation**
  Repeat the password.

"Optional Settings" area

- **Auto Firewall/NAT Rules**
  - Enabled
    The firewall and NAT rules are created automatically for the VPN connection. The connections between the configured exported subnets and the subnets that can be reached via the SINEMA RC Server are allowed. The NAT settings are implemented as configured in the SINEMA RC Server.
  - Disabled
    You will need to create the firewall and NAT rules yourself.
- **Type of connection**
  Specify the type of VPN connection. For more detailed information, refer to the section "VPN connection establishment".
  - Auto
    The device adopts the settings of the SINEMA RC server. You configure the settings on the SINEMA RC server in "Remote connections > Devices". You will find further information on this topic in the "SINEMA RC Server" operating instructions.
  - Permanent
    The settings of the SINEMA RC server are ignored. The device establishes a VPN connection to the SINEMA RC Server. The VPN tunnel is established permanently
  - Digital In
    The settings of the SINEMA RC server are ignored. If the "Digital In" event occurs, the device attempts to establish a VPN connection to the SINEMA RC Server. This is on condition that the event "Digital Input" is forwarded to the VPN connection. To do this in "System > Events> Configuration" activate "VPN Tunnel" for the "Digital In" event.
- **Use Proxy**
  Specify whether the connection to the defined SINEMA RC Server is established via a proxy server. Only the proxy servers can be selected that you configured in "System > Proxy Server".
- **Autoenrollment Interval [min]**
  Specify the period of time in minutes after which queries are sent to the SINEMA RC server. With this query, the device checks whether the configuration data has changed on the SINEMA RC server.
  If you enter the value 0, this function is disabled.

4.4.23 Connection Check

On this page, you activate a ping test that monitors connections. During the ping test, the device sends ICMP echo request packets (pings) to the configured destination address at regular intervals. If this destination address does not respond, the device tries to reach the destination address again. If all ping attempts (retries) are unsuccessful, the ping test is considered to have failed or the group is considered unreachable. If the group is not reachable, the device initiates the configured action on the selected interface. If all 5 actions have been executed or after a restart, the device starts again with the first action.



Description

- **Enable Connection Check**
  Enable or disable the ping test for connection monitoring.
- **Start delay[s]**
  Define the wait time after restart of the device after which the device sends a ping to the first destination address.
  Range of values: 0 to 3600 seconds, default value 600 seconds. If you enter "0", the start delay is disabled.

The first table contains the following columns:

- **Group Identifier**
  Index of the group
- **Name**
  Specify a name for the group. The entry is displayed in the "Action" table as column name.
- **Source Interface**
  Specify the interface via which reachability of the destination addresses is monitored.
- **Interval**
  Specify the interval at which the ping tests take place.
- **TTL (Time to live)**
  Specify the TTL value.

- **Retries**
  Specify how often the ping attempt is repeated.
  The time interval between the ping attempts is 100 ms. With a large number of ping attempts, this can result in a time delay.
  If none of the configured addresses responds, the ping test is considered to have failed (error). In the "Action" table, you define whether a specific action is executed.
- **1. - 3. Ping destination**
  Specify the destination address that is used as reference for the reachability.

The second table contains the following columns:

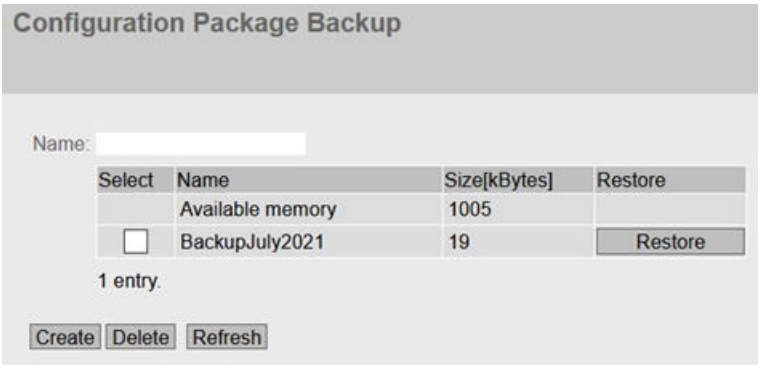
- **Group 1 - 5**
  If a name if configured, it is used as column name. Assign the groups to the desired interface. The interface is considered reachable when all assigned groups are reachable. If only one of the groups is not reachable, the configured action is executed on the selected interface.
- **Action for**
  Indicates the interface on which the action is executed.
- **1st action - 5th action**
  The following actions are possible:
  - None (default)
  - Restart
    Restart the device. After the restart, the device waits until the time specified in the "Start delay[s]" input box has expired and then sends a ping to the first destination address.
  - Digital Out
  - VPN Reset

4.4.24 Configuration Backup

Backup

On this page, you can create backups of the configuration. The maximum number depends on the size of the backup and the available memory space.

The created backups are saved under the "ConfigPackBackup" file type. On the "System > Load&Save > HTTP/TFTP/SFTP" page, you can save configuration backups in ZIP format on your client PC or load them from there.



Description

The page contains the following boxes:

- **Name**
  Enter a name for the backup.

The table contains the following columns:

- **Select**
  Select the row you want to delete.
- **Name**
  Shows the name of the backup.
- **Size [KB]**
  The first row "Available memory" shows how much memory is available for backups on the device. When you create a backup, the available memory space is reduced accordingly.
  The other rows show the size of each backup.
- **Restore**
  Click the "Restore" button to load the relevant backup on the device.

Procedure

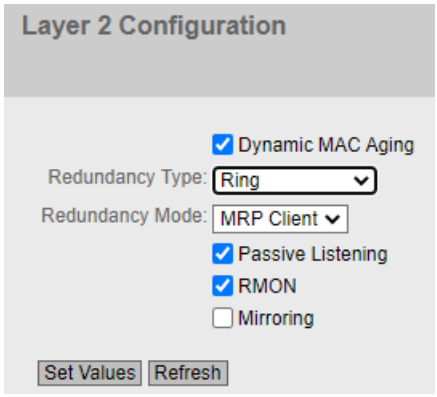
1. Enter the required name.
2. Click the "Create" button.
   The current configuration is saved as a configuration backup.
   Saving the backup may take some time. A new row is created for the backup. The size of the backup is displayed and subtracted from the available memory space.

4.5 "Layer 2" menu

4.5.1 Configuration

Configuring layer 2

On this page, you create a basic configuration for the functions of layer 2.



Description

- **Dynamic MAC Aging**
  Enable or disable the "Aging" mechanism. You can configure other settings under "Layer 2 > Dynamic MAC Aging".
- **Redundancy Type**
  The following settings are available:
  - **"-" (disabled)**
    The redundancy function is disabled.
  - **Ring**
    If you select this option, you specify the required redundancy mode in the "Redundancy Mode" drop-down list.
  - **Spanning Tree**
    If you select this option, you specify the required redundancy mode in the "Redundancy Mode" drop-down list.

- **Redundancy Mode**
  If you select "Ring" in the "Redundancy Type" drop-down list, the following options are then available:
  - **MRP-Client**
    The device adopts the role of MRP client.
  - **HRP-Client**
    The device adopts the role of HRP client.

  If you select "Spanning Tree" in the "Redundancy Type" drop-down list, the following options are then available:
  - **STP**
    Enabled Spanning Tree Protocol. Typical reconfiguration times with spanning tree are between 20 and 30 seconds. You can configure other settings in "Layer 2 > Spanning Tree".
  - **RSTP**
    Enabled Rapid Spanning Tree Protocol (RSTP). If a spanning tree frame is detected at a port, this port reverts from RSTP to spanning tree. You can configure other settings in "Layer 2 > Spanning Tree".

  Note

  When using RSTP (Rapid Spanning Tree Protocol), loops involving duplication of frames or frames being overtaken may occur briefly. If this is not acceptable in your particular application, use the slower standard spanning tree mechanism.

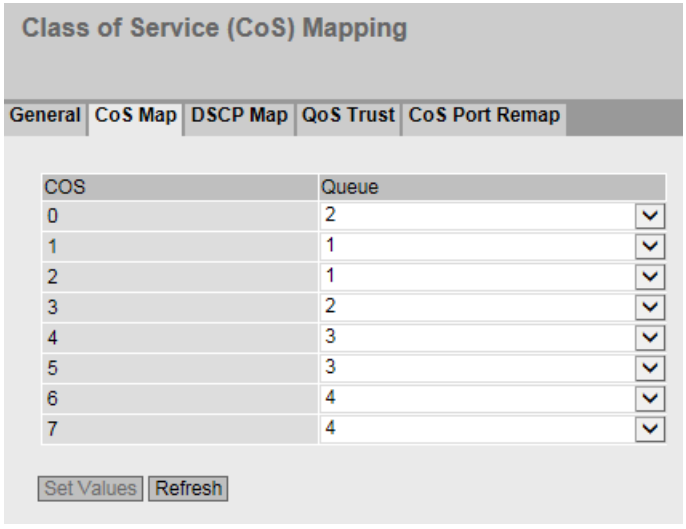
- **Passive Listening**
  Enable or disable the Passive Listening function.
- **RMON**
  If you select this check box, Remote Monitoring (RMON) allows diagnostics data to be collected on the device, prepared and read out using SNMP by a network management station that also supports RMON. This diagnostic data, for example port-related load trends, allows problems in the network to be detected early and eliminated. Some of the "Ethernet Statistics Counters" are part of the RMON function. If you disable RMON, the "Ethernet Statistics Counter" in "Information > Ethernet Statistics" is no longer updated.
- **Mirroring**
  Enable or disable port mirroring. You can configure other settings in "Layer 2 > Mirroring".

4.5.2 Quality of Service (QoS)

4.5.2.1 CoS Map

CoS Map

On this page, you can assign CoS priorities to different queues.



Description of the displayed boxes

The table has the following columns:

- **CoS**
  Shows the CoS priority of the incoming frames.
- **Queue**
  From the drop-down list, select the queue that is assigned to the CoS priority.
  The higher the number of the Queue, the higher the processing priority.

The service classes (CoS) are assigned to the queues as default as follows:

COS	Devices with 4 queues	Devices with 8 queues
0	Queue 2	Queue 2
1	Queue 1	Queue 1
2	Queue 1	Queue 3
3	Queue 2	Queue 4
4	Queue 3	Queue 5
5	Queue 3	Queue 6
6	Queue 4	Queue 7
7	Queue 4	Queue 8

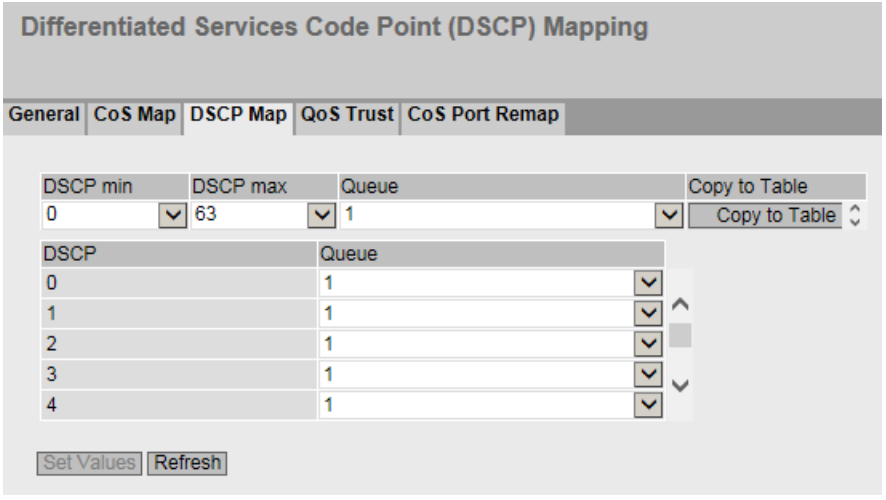
Steps in configuration

1. For each value in the "CoS" column, select the queue from the "Queue" drop-down list.
2. Click the "Set Values" button.

4.5.2.2 DSCP Mapping

DSCP queue

On this page, you can assign DSCP priorities to different Queues.



Description of the displayed values

Table 1 has the following columns:

- **DSCP min**
  From the drop-down list, select the minimum value for a range of DSCP codes to which you wish to assign a queue.
- **DSCP max**
  From the drop-down list, select the maximum value for a range of DSCP codes to which you wish to assign a queue.
- **Queue**
  From the drop-down list, select the forwarding queue (send priority) that is assigned to the range of DSCP codes.
- **Copy to Table**
  When you click the button, the selected forwarding queue (send priority) is assigned to the DSCP codes in the specified range.

Table 2 has the following columns:

- **DSCP**
  Shows the DSCP priority of the incoming frames.
- **Queue**
  From the drop-down list, select the queue that is assigned to the DSCP priority.
  The higher the queue number the higher the processing priority

The DSCP priorities are assigned to the queues as default as follows:

DSCP codes	Devices with 4 queues
0 - 15	Queue 1
16 - 31	Queue 2
32 - 47	Queue 3
48 - 63	Queue 4

DSCP codes	Devices with 8 queues
0 - 7	Queue 2
8 - 15	Queue 1
16 - 23	Queue 3
24 - 31	Queue 4
32 - 39	Queue 5
40 - 47	Queue 6
48 - 55	Queue 7
56 - 63	Queue 8

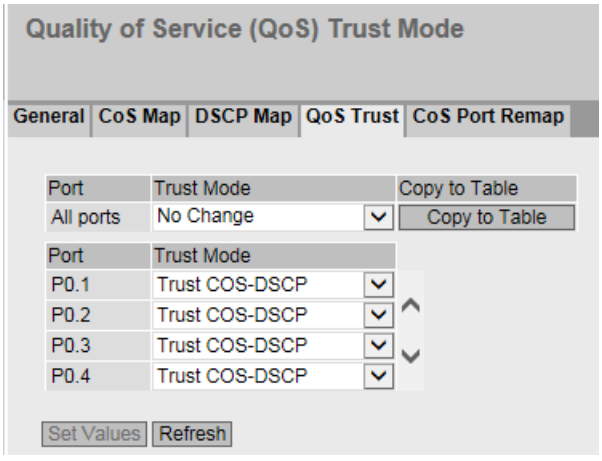
Steps in configuration

1. For each value in the "DSCP" column, select the queue from the "Queue" drop-down list.
2. Click the "Set Values" button.

4.5.2.3 QoS Trust

Specifying the subnet priority

On this page you can set the method according to which frames to be forwarded are prioritized port by port.



Description of the displayed values

Table 1 has the following columns:

- **Port**
  Shows that the setting is valid for all ports of table 2.
- **Trust Mode**
  Select the setting from the drop-down list. You have the following setting options:
  - No Trust
  - Trust COS
  - Trust DSCP
  - Trust COS-DSCP
  - No Change
    Table 2 remains unchanged.
- **Copy to Table**
  If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
  Shows the configurable ports.
  The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.
- **Trust Mode**
  Select the required mode from the drop-down list:

  Note

  You configure the prioritization of the receiving port on the page "Layer 2 > VLAN > Port Based VLAN".

  You configure the assignment of the following priorities to a queue on the page ""Layer 2 > QoS > CoS Map".

  - Receiving port
  - VLAN tag
  - Broadcast and agent frame

  You configure the assignment of the DSCP prioritization to a queue on the page ""Layer 2 > QoS > DSCP Mapping".

  – No Trust
  The switch sorts the incoming frames into a queue according to the prioritization of the receiving port.
  If there is a DSCP value in the IP header, this is ignored. If a VLAN tag exists, its priority value is replaced by the priority value of the receiving port.

  – Trust COS
  If an incoming frame contains a VLAN tag, the switch sorts it into a queue according to this prioritization.
  If the frame does not contain a VLAN tag, the switch sorts the frame into a queue according to the prioritization of the receiving port.
  If there is a DSCP value in the IP header, this is ignored.

  – Trust DSCP
  If an incoming frame contains a DSCP prioritization, the switch sorts it into a queue according to this prioritization.
  If the frame does not contain a DSCP prioritization, the switch sorts the frame into a queue according to the prioritization of the receiving port.
  If the frame contains a VLAN tag, this is ignored.

  – Trust COS-DSCP
  With an incoming frame, there is a sequential check of which prioritization it contains.
  If it contains a DSCP prioritization, it is handled as in the "Trust DSCP" mode.
  If it contains no DSCP prioritization, the switch checks whether it contains a VLAN tag. If it contains a VLAN tag, the switch sorts it into a queue according to this prioritization.
  If the frame contains neither a DSCP prioritization nor a VLAN tag, the switch sorts the frame into a queue according to the prioritization of the receiving port.

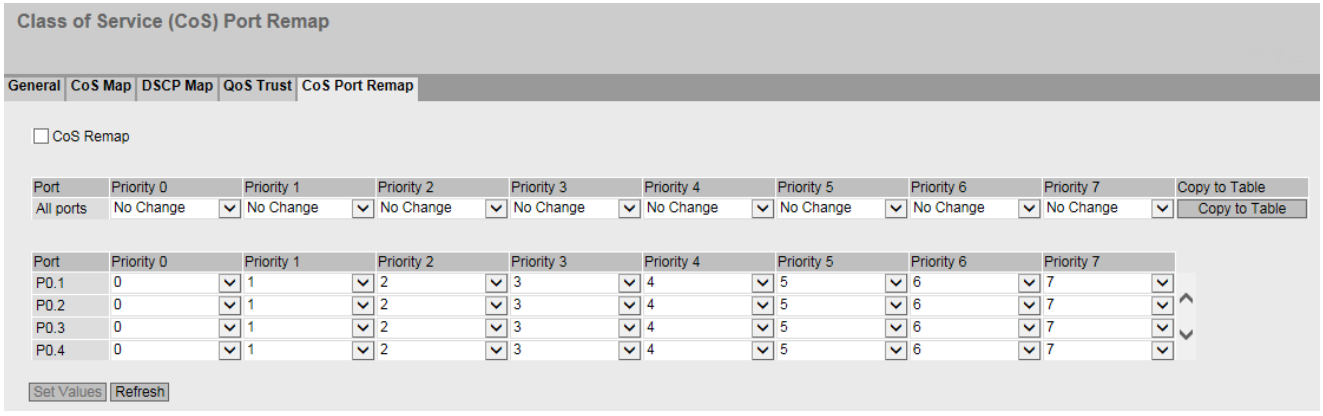
Steps in configuration

1. Select the required Trust Mode from the drop-down list.
2. Click the "Set Values" button.

4.5.2.4 CoS Port Remap

Changing priority when sending

On this page depending on the priority when receiving, you can change the priority of a frame with which it is sent. The new priority effects only the following devices that receive the frame.



Description of the displayed boxes

The page contains the following boxes:

- **CoS Remap**
  Enable or disable frames being sent with changed priorities according to Table 2.

Table 1 has the following columns:

- **Port**
  Shows that the settings are valid for all ports of table 2.
- **Priority 0 - 7**
  The priority in the column stands for the priority with which a frame is received.
  - 0 - 7
    Select the priority with which a frame will be sent.
  - No Change
    No change in table 2.
- **Copy to Table**
  If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
  Shows all available ports. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.
- **Priority 0 - 7**
  The priority in the column stands for the priority with which a frame is received.
  In the drop-down list select the priority with which a frame will be sent.

Steps in configuration

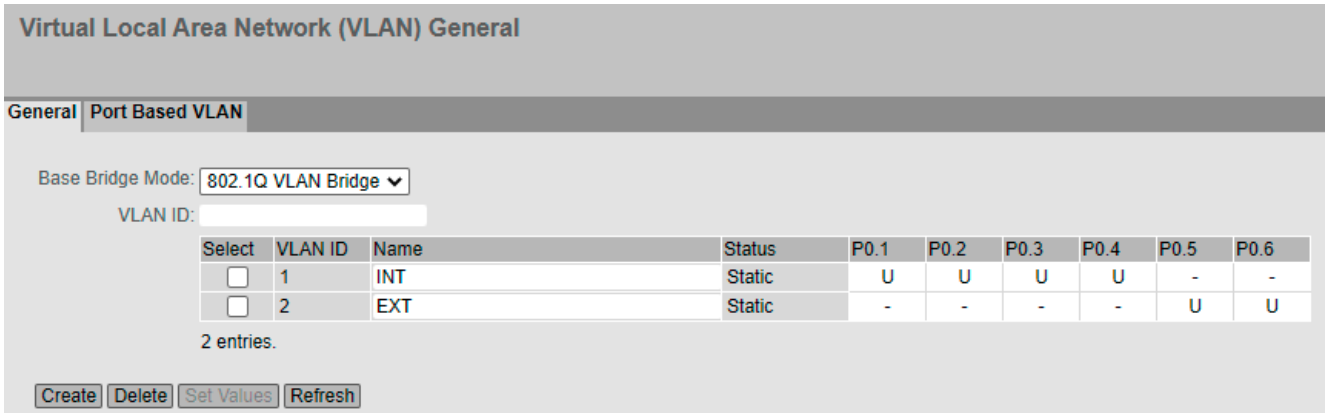
1. Select the "CoS Remap" check box.
2. Using the drop down lists select the priority for sending for each receive priority per port.
3. Click the "Set Values" button.

4.5.3 VLAN

4.5.3.1 General

VLAN configuration page

On this page you can define VLANs and specify the use of the ports. The device takes VLAN information into account (IEEE 802.1Q/VLAN-aware mode). If the device is in the "802.1Q VLAN Bridge" mode, you can define VLANs and specify the use of the ports.



Description

The page contains the following boxes:

- **Base Bridge Mode**
  - 802.1Q VLAN Bridge
    Sets the mode "VLAN-aware" for the device. In this mode, VLAN information is taken into account.
- **VLAN ID**
  Enter the VLAN ID in the "VLAN ID" input box.
  Range of values: 1 ... 4094

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **VLAN ID**
  Shows the VLAN ID. The VLAN ID (a number between 1 and 4094) can only be assigned once when creating a new data record and can then no longer be changed. To make a change, the entire data record must be deleted and created again.
- **Name**
  Enter a name for the VLAN. The name only provides information and has no effect on the configuration. The length is a maximum of 32 characters.
- **Status**
  Shows the status type of the entry in the internal port filter table. Here, "Static" means that the VLAN was entered statically by the user.
- **List of ports**
  Specify the use of the port. The following options are available:
  - "-"
    The port is not a member of the specified VLAN.
    With a new definition, all ports have the identifier "-".
  - M
    The port is a member of the VLAN. Frames sent in this VLAN are forwarded with the corresponding VLAN tag.
  - U (uppercase)
    The port is an untagged member of the VLAN. Frames sent in this VLAN are forwarded without the VLAN tag. Frames without a VLAN tag are sent from this port.
  - u (lowercase)
    The port is an untagged member of the VLAN, but the VLAN is not configured as a port VLAN. Frames sent in this VLAN are forwarded without the VLAN tag.
  - F
    The port is not a member of the specified VLAN and cannot become a member of this VLAN even if it is configured as a trunk port.
  - T
    This option is only displayed and cannot be selected in the WBM.
    This port is a trunk port making it a member in all VLANs.

Procedure

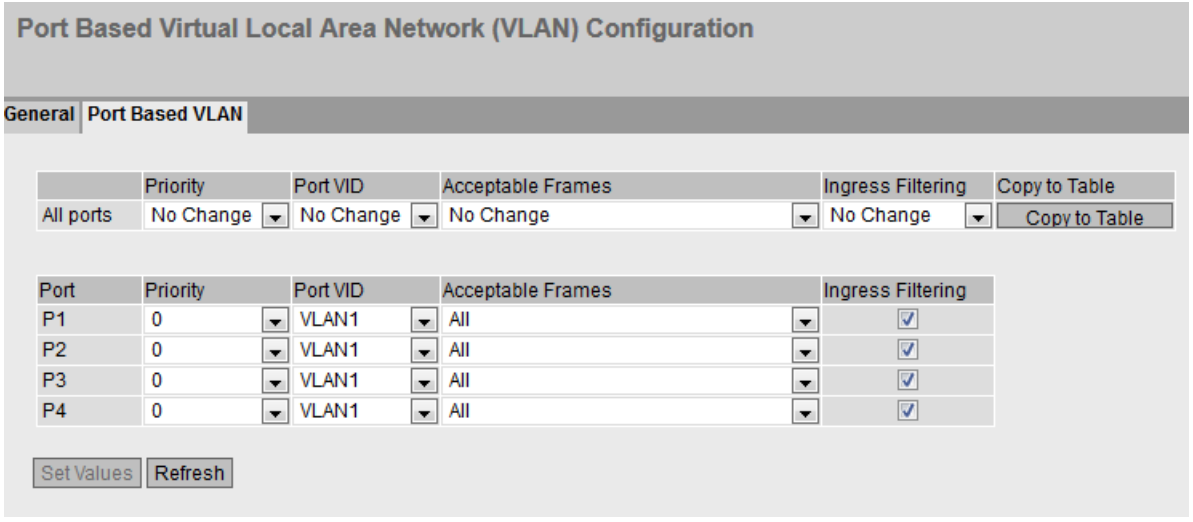
Creating a new VLAN

1. Enter an ID in the "VLAN ID" input box.
2. Click the "Create" button. A new entry is generated in the table. As default, the boxes have "-" entered.
3. Enter a name for the VLAN under "Name".
4. Specify the use of the port in the VLAN. If, for example, you select "M", the port is a member of the VLAN. The frame sent in this VLAN is forwarded with the corresponding VLAN tag.
5. Specify the mode of the device.
6. Click the "Set Values" button.

4.5.3.2 Port Based VLAN

Processing received frames

On this WBM page, you specify the configuration of the port properties for receiving frames.



Description

Table 1 has the following columns:

- **All ports**
  Shows that the settings are valid for all ports of table 2.
- **Priority / Port VID / Acceptable Frames / Ingress Filtering**
  In the drop-down list, select the setting for all ports. If "No Change" is selected, the entries of the corresponding column in table 2 remain unchanged.
- **Copy to Table**
  If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
  Shows the available ports.
- **Priority**
  Select the required priority assigned to untagged frames.
  The CoS priority (Class of Service) used in the VLAN tag. If a frame is received without a tag, it will be assigned this priority. This priority specifies how the frame is further processed compared with other frames.
  There are a total of eight priorities with values 0 to 7, where 7 represents the highest priority (IEEE 802.1p Port Priority).
- **Port VID**
  Select the required VLAN ID. Only VLAN IDs defined in "VLAN > General" can be selected.
  If a received frame does not have a VLAN tag, it has a tag with the VLAN ID specified here added to it and is sent according to the rules at the port.
- **Acceptable Frames**
  Specify which types of frames will be accepted. The following alternatives are possible:
  - Tagged Frames Only
    The device discards all untagged frames. Otherwise, the forwarding rules apply according to the configuration.
  - All
    The device forwards all frames.
  - Untagged and Priority Tagged Only
    The device discards all tagged frames. The device forwards all untagged frames and frames with a priority (Priority Tagged Frames). Otherwise, the forwarding rules apply according to the configuration. If you have configured the Bridge mode "Provider", this means that the device treats all incoming frames like untagged frames.
- **Ingress Filtering**
  Specify whether the VID of received frames is evaluated.
  You have the following options:
  - Enabled
    The VLAN ID of received frames decides whether they are forwarded: To forward a VLAN tagged frame, the receiving port must be a member in the same VLAN. Frames from unknown VLANs are discarded at the receiving port.
  - Disabled
    All frames are forwarded.

Configuration procedure

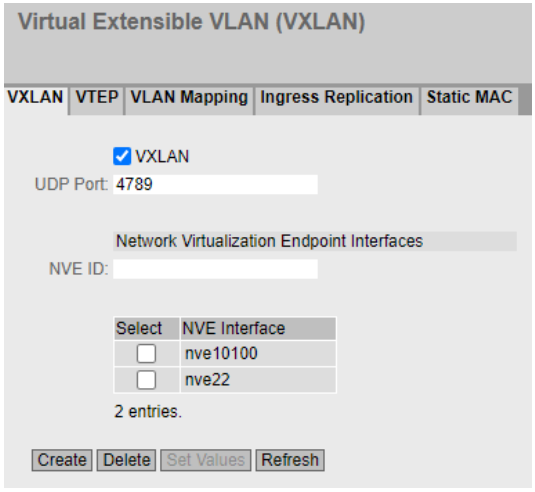
1. In the row of the port to be configured, click on the relevant cell in the table to configure it.
2. Enter the values to be set in the input boxes as follows.
3. Select the values to be set from the drop-down lists.
4. Click the "Set Values" button.

4.5.4 VXLAN (SC63x/SC64x)

4.5.4.1 VXLAN

On this page, you define VXLANs (Virtual eXtensible LAN). VXLAN is a virtual network technology for extending VLAN and allows the transmission of Layer 2 packets via Layer 3 networks.

The maximum size of a packet (MTU) for VXLAN is 1500 bytes. Larger packets are fragmented.



Description

The page contains the following boxes:

- **VXLAN**
  Enables the VXLAN function.
- **UDP port**
  Enter the destination port of the VXLAN.
  Range of values: 1000 ... 65535
  UDP port 4789 is assigned by default.
- **Network Virtual Endpoint Interface (NVE)**
  In this area, you configure the virtual interface via which the VXLAN tunnel is established.
  - **NVE ID**
    Enter a number for the NVE interface.
    Range of values: 1 ... 65535
- The table contains the following columns.
  - **Select**
    Select the row you want to delete.
  - **NVE Interface**
    Shows the NVE interface. The label is automatically composed of "nve" and the entered number.

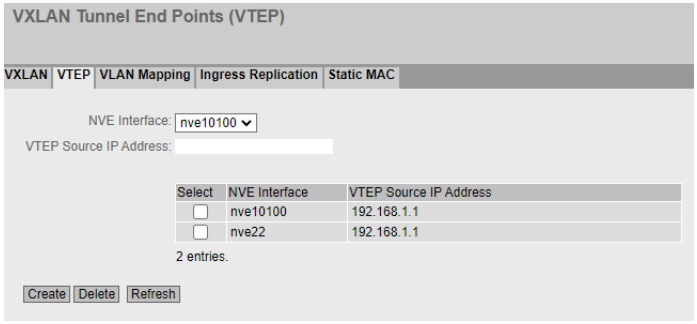
Procedure

Creating a new VXLAN

1. Select the "VXLAN" check box.
2. Enter the "UDP Port" and the "NVE ID".
3. Click the "Create" button.

4.5.4.2 VTEP

On this page, you make settings relating to the VTEPs (VXLAN Tunnel End Points). The VTEPS form the endpoints in the VXLAN over which the connection runs. In the "Static MAC" tab, you set end devices that are to be reachable via a VTEP in the destination network.



Description

The page contains the following boxes:

- **NVE Interface**
  Select the required NVE interface. Only the interfaces that you created in the "VXLAN" tab can be selected.
- **VTEP Source IP Address**
  Enter the IPv4 address of the source VTEP. The requirement is that the IPv4 address is created on the device. You configure the IPv4 address under "Layer 3 > Subnets".

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **NVE Interface**
  Shows the NVE interface. The ID of the NVE interface can only be assigned once when you create a new data record and can then no longer be changed. To make a change, the entire data record must be deleted and created again.
- **VTEP Source IP Address**
  Shows the IPv4 address of the source VTEP.

Procedure

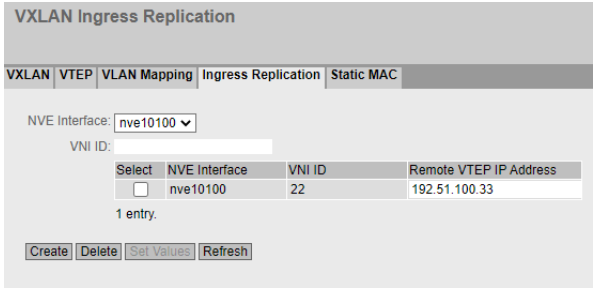
Creating the source IP address

1. Select the NVE interface.
2. Enter the corresponding VTEP source IP address.
3. Click the "Create" button.

4.5.4.3 Ingress Replication

If there are multiple VTEPs in a VNI segment, the source VTEP does not know which remote VTEP the receiver of the Ethernet frame is behind.

On this page, you enter the remote VTEP IP addresses to which Ethernet frames are sent. The source VTEP replicates the received Ethernet frame and sends the encapsulated Ethernet frame to the remote VTEPs.



Description

The page contains the following boxes:

- **NVE Interface**
  Select the required NVE interface.
- **VNI ID**
  Enter the required VNI. Only VXLAN networks with the same VNI ID can communicate with one another.
  Range of values: 1 ... 16777215

The table has the following columns:

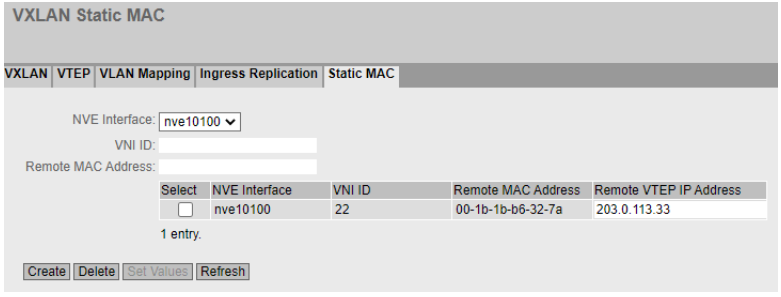
- **Select**
  Select the row you want to delete.
- **NVE Interface**
  Shows the selected NVE interface.
- **VNI ID**
  Shows the VNI ID.
- **Remote VTEP IP Address**
  Enter the IPv4 address of the remote VTEP.
  The replicated Ethernet frame is encapsulated and sent to this remote VTEP. The prerequisite is that the remote VTEP is a member of the VNI segment.

Procedure

1. Select the NVE interface.
2. Enter an ID in the "VNI ID" input box.
3. Click the "Create" button.
   A new entry is generated in the table.
4. Enter the remote VTEP IP address.
5. Click the "Set Values" button.

4.5.4.4 Static MAC

On this page, you can enter the MAC addresses of devices in the destination network that should be reached over a remote VTEP. The entry is displayed under "Information > VXLAN".



Description

The page contains the following boxes:

- **NVE Interface**
  Select the NVE interface via which the remote VTRP can be reached. Only the interfaces that you created in the "VXLAN" tab can be selected.
- **VNI ID**
  Enter the VNI ID (VXLAN Network Identifier). Only VTEPs that are members of the same VXLAN segment can communicate with one another.
- **Remote MAC Address**
  Enter the MAC address of the end device in the destination network to be reached via the VTEP entered in the table.

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **NVE Interface**
  Shows the NVE interface.
- **VNI**
  Shows the VNI. The VNI can only be assigned once when you create a new data record and can then no longer be changed. To make a change, the entire data record must be deleted and created again.

- **Remote MAC Address**
  Shows the MAC address of the end device in the destination network.
- **Remote VTEP IP Address**
  Enter the IPv4 address of the VTEP via which the end device with the entered remote MAC address can be reached in the destination network.

Procedure

1. Select the NVE interface.
2. Enter an ID in the "VNI ID" input box.
3. Enter the remote MAC address.
4. Click the "Create" button.
   A new entry is generated in the table.
5. Enter the remote VTEP IP address.
6. Click the "Set Values" button.

4.5.5 Mirroring

4.5.5.1 General

On this page, you can enable or disable the mirroring function and make the basic settings.

Note

It cannot be guaranteed when mirroring the data traffic that all packets are mirrored. This depends primarily on the load on the mirrored ports and on the number of sessions. To achieve maximum precision, a limit of one session is recommended.

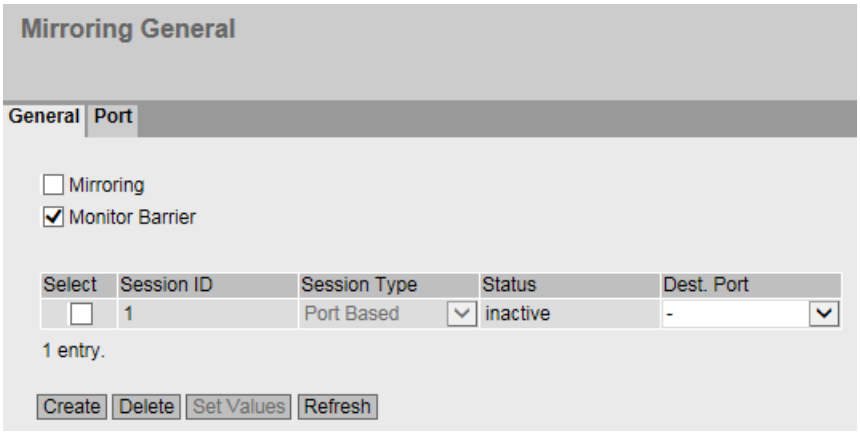
Note the data rate

If the maximum data rate of the mirrored port is higher than that of the monitor port, data may be lost and the monitor port no longer reflects the data traffic at the mirrored port. Several ports can be mirrored to one monitor port at the same time.

Several source ports from the same VLAN

If in a VLAN you select more than one source port for the port-based egress mirroring, unknown unicast and multicast frames as well as broadcast frames are forwarded only once to the destination port.

Settings



The page contains the following boxes:

- **Mirroring**
  Click this check box to enable or disable mirroring.

  Note

  You need to disable port mirroring if you want to connect a normal end device to the monitor port.

- **Monitor Barrier**
  Click this check box to enable or disable Monitor Barrier.

  Note

  Effects of Monitor Barrier

  If you enable this option, management of the switch via the monitor port is no longer reachable. The following port-specific functions are changed:

  - The DCP Forwarding is turned off.
  - LLDP is turned off.
  - Unicast, multicast and broadcast blocking are turned on.

  The previous statuses of these functions are no longer restored after disabling monitor barrier again. They are reset to the default values and may need to be reconfigured.

  You can configure these functions manually even if monitor barrier is turned on. The data traffic on the monitor port is also allowed again. If you do not require this, make sure that only the data traffic you want to monitor is forwarded to the interface.

  If mirroring is disabled, the listed port-specific functions are reset to the default values. This reset takes place regardless of whether the functions were configured manually or automatically by enabling Monitor Barrier.

The table for the basic settings contains the following boxes:

- **Select**
  Select the row you want to delete.
- **Session ID**
  The Session ID is assigned automatically when a new entry is created. You can create precisely one session.
- **Session Type**
  Shows the type of mirroring session.
- **Status**
  Shows whether or not mirroring is enabled.
- **Dest. Port**
  From the drop-down list, select the output port to which data will be mirrored in this session.

Procedure

Creating a mirroring session

1. Activate mirroring.
2. Click the "Create" button to create an entry in the table.
   The session ID is assigned automatically.
3. Select a destination port.
4. Click the "Set Values" button to save and activate the selected settings.
5. Change to the following tab to make further detailed settings for the session ID.

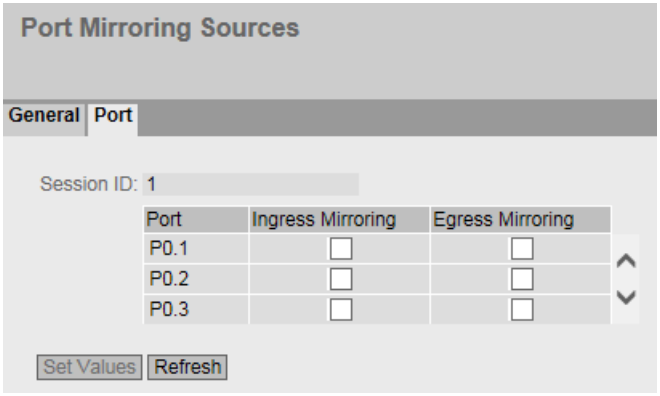
Deleting a mirroring session

1. Click the check box in the first column to select the row.
2. Click the "Delete" button to delete the selected rows.

4.5.5.2 Port

Mirroring ports

You can only configure the settings on this page if you have already generated a session ID with the session type "Port-based" on the "General" tab.



Description of the displayed boxes

The page contains the following boxes:

- **Session ID**
  Shows the session.
- **Port**
  Shows all available ports. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.
- **Ingress Mirroring**
  Enable or disable listening in on incoming packets at the required port.
- **Egress Mirroring**
  Enable or disable listening in on outgoing packets at the required port.

Note

Mirroring with ring ports

If you enable the mirroring function for a ring port, the ring port sends test frames even in the "link down" status.

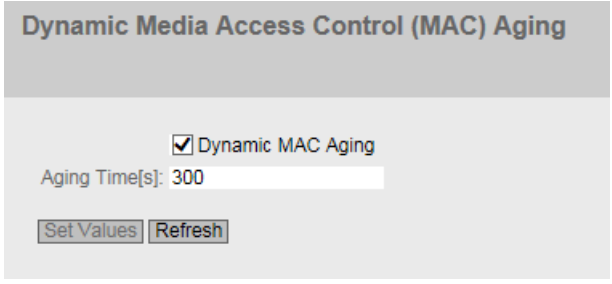
Steps in configuration

1. In the table, click the check box of the row after the port to be mirrored.
   Select whether you want to monitor incoming or outgoing packets.
   To monitor the entire data traffic of the port, select both check boxes.
2. Click the "Set Values" button.

4.5.6 Dynamic MAC Aging

Protocol settings and switch functionality

The device automatically learns the source addresses of the connected nodes. This information is used to forward frames to the nodes specifically involved. This reduces the network load for the other nodes.
If a device does not receive a frame whose source address matches a learnt address within a certain time, it deletes the learnt address. This mechanism is known as "Aging". Aging prevents frames being forwarded incorrectly, for example when an end device (for example a programming device) is connected to a different port.
If the check box is not enabled, a device does not delete learnt addresses automatically.



Description

The page contains the following boxes:

- **Dynamic MAC-Aging**
  Enable or disable the function for automatic aging of learned MAC addresses.
- **Aging Time[s]**
  Enter the time in seconds in steps of 15. After this time, a learned address is deleted if the device does not receive any further frames from this sender address.
  Range of values: 15 - 630 seconds

Note

Rounding of the values, deviation from desired value

When you input the Aging Time, note that it is rounded to correct values. If you enter a value that cannot be divided by 15, the value is automatically rounded down.

Procedure

1. Select the "Dynamic MAC Aging" check box.
2. Enter the time in seconds in the "Aging Time[s]" text box.
3. Click the "Set Values" button.

4.5.7 Ring redundancy (SC6x6-2C)

4.5.7.1 Ring

Rules for ring redundancy

Factory settings

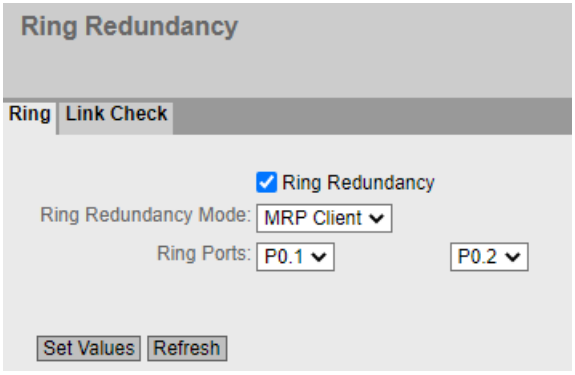
- The factory setting defines ports P0.1 and P0.2 as ring ports.

Enabling redundancy

You can enable ring redundancy as follows:

- using the WBM
- using the CLI

Configuration of ring redundancy



- **Ring Redundancy**
  If you enable the "Ring Redundancy" check box, you turn ring redundancy on. The Ring Ports set on this page are used.
- **Ring redundancy mode**
  Here, you set the mode of the ring redundancy.
  The following modes are available:
  - MRP Client
    The device adopts the role of MRP client.
  - HRP Client
    The device adopts the role of HRP client.
- **Ring ports**
  Here, you set the ports to be used as ring ports in ring redundancy.

Restoring factory settings

If you have restored the factory defaults, ring redundancy is disabled and the default ports are used as the ring ports. This can lead to circulating frames and failure of the data traffic if other settings were used in a previous configuration.

4.5.7.2 Link Check

Requirements

Note

Replacing: media modules: Optical → electrical

If you run Link Check on an optical port of a media module, not the following:

- Link Check is activated on the optical port of a media module.
- You want to replace the media module with a module without optical ports:
  1. Disable Link Check on the ports of the inserted module.
  2. Replace the media module.

Note

Changing the media type with a combo port: Optical → electrical

If Link Check is active for a combo port with the media type "SFP" and you want to enable the "RJ45" media type, disable Link Check first.

- You cannot enable Link Check on ports with 10 Gbps.
- You can only enable the Link Check function with optical ring ports of an HRP or MRP ring.
- Link Check must be enabled on two neighboring devices (connection partners) within an HRP or MRP ring.
- The ring ports on which you enable Link Check must be connected.

Monitoring optical connections in the ring

With the Link Check function, you can monitor the transmission quality of optical sections within an HRP or MRP ring, identify disturbed connections and under certain conditions turn them off. When the disturbed section is turned off, the redundancy manager can close the ring and restore communication.

NOTICE
Make sure that the frames used by Link Check for monitoring the optical connections are not supplanted by an overload of high priority frames in the network. An overload of high priority frames can, for example, be caused by the following: • Network loops that can cause duplication of the high priority frames • Changing the priorities for forwarding frames

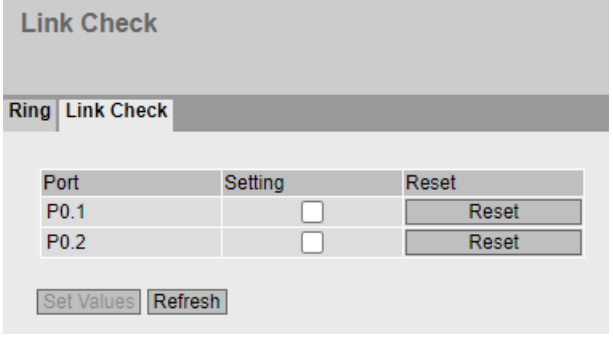
Note

Enable Link Check on only one of two connection partners This can lead to incorrect behavior.

Note

If Link Check is enabled on all devices of a ring at the same time, and several connections within the ring have problems, this leads to fragmentation of the ring.

1. During commissioning enable the Link Check function for one connection section after the other by enabling Link Check for the two connection partners connected to a line.
2. To ensure an error-free connection, wait 1 min. before you enable Link Check for the next connection.



Description of the displayed boxes

The table contains the following columns:

- **Port**
  Shows the available ports. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.
- **Setting**
  With this check box, you enable or disable the Link Check function for a port.
  When connection monitoring is enabled, you can see the number of sent and received Link Check test frames on the "Information > Redundancy > Link Check" page.
- **Reset**
  After resetting Link Check, the function is restarted on the port and the statistics are reset. If you use the "Reset" button, the reset must be performed on both connection partners within 30 s.

Note

When you use the "Reset" button, loops can form temporarily resulting in a loss of data traffic. The loop is automatically cleared again.

If this is not acceptable for your application, reset Link Check by pulling the cable and plugging it in again.

Configuration procedure

Enabling Link Check

Follow the steps below to activate the monitoring of a ring port:

1. Select the appropriate check box in the "Setting" column.
2. Click the "Set Values" button.

Disabling Link Check

Follow the steps below to deactivate the monitoring of a ring port:

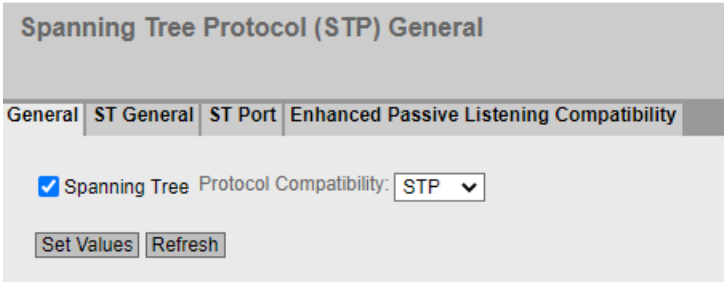
1. Deactivate the appropriate check box in the "Setting" column.
2. Click the "Set Values" button.

4.5.8 Spanning Tree

4.5.8.1 General

General settings of the Spanning Tree protocol

On this page, you can enable Spanning Tree and select the protocol compatibility. By default, the "Spanning Tree Protocol" (STP) is enabled.



Description of the displayed boxes

The page contains the following boxes:

- **Spanning Tree**
  Enable or disable Spanning Tree.

  Note

  No operation of Spanning Tree with enabled ring redundancy

  If ring redundancy is enabled under "Layer 2", Spanning Tree cannot be used.

- **Protocol Compatibility**
  Select the protocol compatibility. The following settings are available:
  - STP
  - RSTP

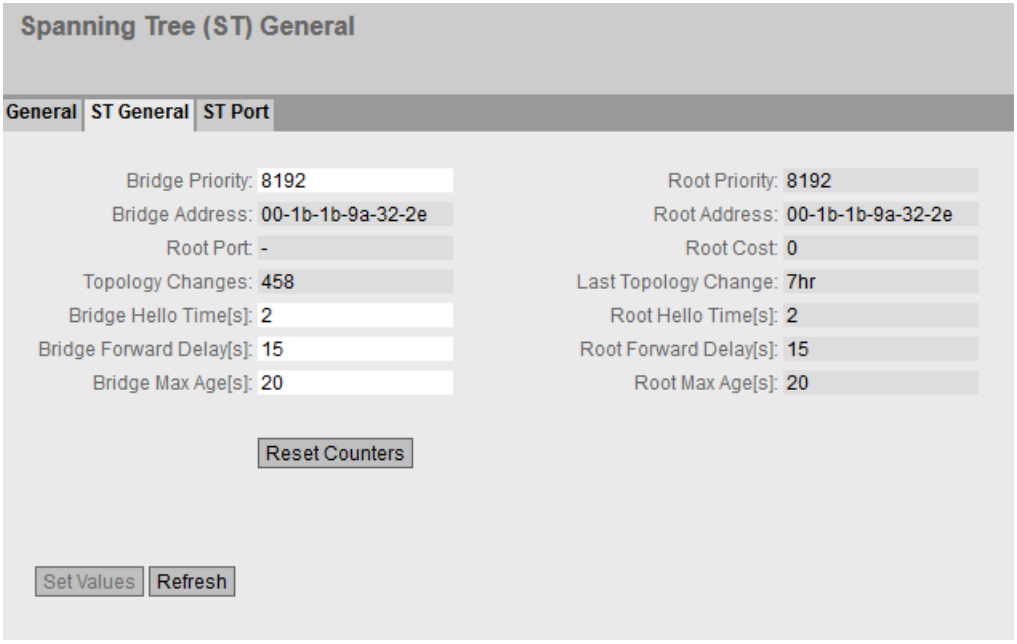
Configuration procedure

1. Select the "Spanning Tree" check box.
2. From the "Protocol Compatibility" drop-down list, select the type of compatibility.
3. Click the "Set Values" button.

4.5.8.2 ST general

The page consists of the following parts.

- The left-hand side of the page shows the configuration of the device.
- The right-hand part shows the configuration of the root bridge that can be derived from the spanning tree frames received by a device.



Description

The page contains the following boxes:

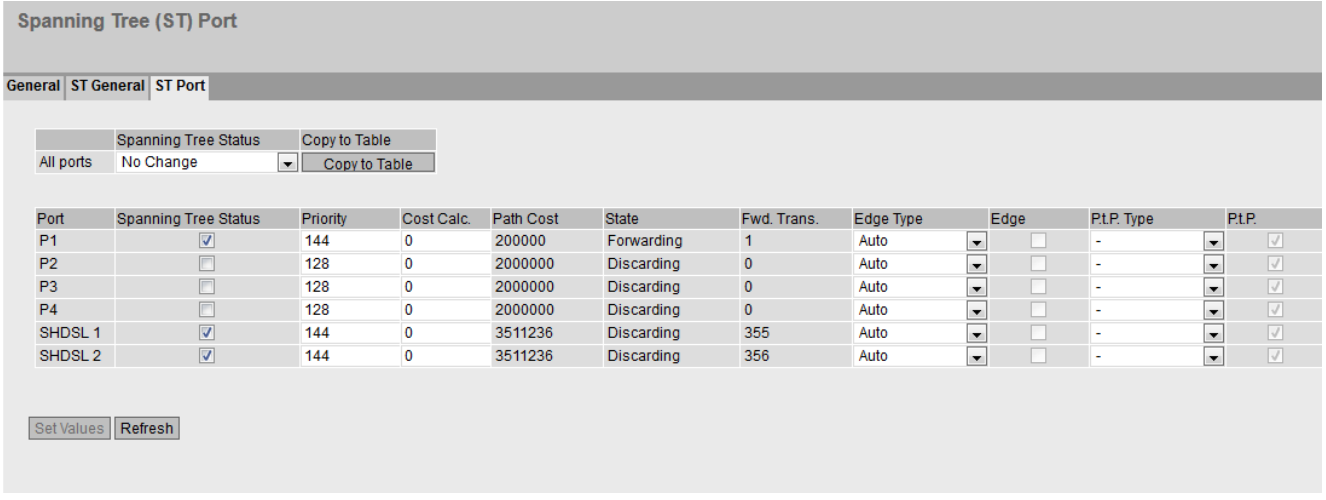
- **Bridge Priority / Root Priority**
  Which device becomes the root bridge is decided by the bridge priority. The bridge with the highest priority (in other words, with the lowest value for this parameter) becomes the root bridge. If several devices in a network have the same priority, the device whose MAC address has the lowest numeric value will become the root bridge. Both parameters, bridge priority and MAC address together form the bridge identifier. Since the root bridge manages all path changes, it should be located as centrally as possible due to the delay of the frames.
  The value for the bridge priority is a whole multiple of 4096. Range of values: 0 - 61440
- **Bridge Address / Root Address**
  The bridge address shows the MAC address of the device and the root address shows the MAC address of the root bridge.
- **Root port**
  Shows the port via which the switch communicates with the root bridge.
- **Root Cost**
  The path costs from this device to the root bridge.

- **Topology Changes / Last Topology Change**
  The entry for the device shows the number of reconfiguration actions due to the spanning tree mechanism since the last startup. For the root bridge, the time since the last reconfiguration is displayed as follows:
  - Seconds: Unit "sec" after the number
  - Minutes: Unit min after the number
  - Hours: Unit hr after the number
- **Bridge hello time [s] / Root hello time [s]**
  Each bridge sends configuration frames (BPDUs) regularly. The interval between two configuration frames is the "Hello Time".
  Factory setting: 2 seconds
- **Bridge Forward Delay[s] / Root Forward Delay[s]**
  New configuration data is not used immediately by a bridge but only after the period specified in the Forward Delay parameter. This ensures that operation is only started with the new topology after all the bridges have the required information.
  Factory setting: 15 seconds
- **Bridge Max Age[s] / Root Max Age[s]**
  If the BPDU is older than the specified "Max Age" it is discarded.
  Factory setting: 20 seconds
- **Reset Counters**
  Click this button to reset the counters on this page.

4.5.8.3 ST Port

When the page is called, the table displays the current status of the configuration of the port parameters.

To configure them, click the relevant cells in the port table.



Description

Table 1 has the following columns:

- **All ports**
  Shows that the settings are valid for all ports of table 2.
- **Spanning Tree Status**
  In the drop-down list, select the setting for all ports. If "No Change" is selected, the entries of the corresponding column in table 2 remain unchanged.
- **Copy to Table**
  If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
  Shows the available ports.
- **Spanning Tree Status**
  Specify whether the port is integrated in the spanning tree or not.

  Note

  If you disable the "Spanning Tree Status" option for a port, this may cause the formation of loops. The topology must be kept in mind.

- **Priority**
  Enter the priority of the port. The priority is only evaluated when the path costs are the same. The value must be divisible by 16. If the value that cannot be divided by 16, the value is automatically adapted.
  Range of values: 0 - 240.
  The default is 128.
- **Cost Calc.**
  Enter the path cost calculation. If you enter the value "0" here, the automatically calculated value is displayed in the "Path costs" box.
- **Path Cost**
  This parameter is used to calculate the path that will be selected. The path with the lowest value is selected as the path. If several ports of a device have the same value for the path costs, the port with the lowest port number is selected.
  If the value in the "Cost Calc." is "0", the automatically calculated value is shown. If a value other than "0" is entered, the value of the "Cost Calc." box is displayed.
  The calculation of the path costs is largely based on the transmission speed. The higher the achievable transmission speed is, the lower the value of the path costs.
  Typical values for path costs with RSTP:
  - 10,000 Mbps = 2,000
  - 1000 Mbps = 20,000
  - 100 Mbps = 200,000
  - 10 Mbps = 2,000,000

  The values can, however, also be set individually.

- **Status**
  Displays the current status of the port. The values are only displayed and cannot be configured. The "Status" parameter depends on the configured protocol. The following values are possible:
  - Disabled
    The port only receives and is not involved in STP and RSTP.
  - Discarding
    In the "Discarding" mode, BPDU frames are received. Other incoming or outgoing frames are discarded.
  - Listening

    In this status, BPDUs are both received and sent. The port is involved in the spanning tree algorithm.
  - Learning
    Stage prior to the "Forwarding" status, the port is actively learning the topology (in other words, the node addresses).
  - Forwarding
    Following the reconfiguration time, the port is active in the network; it receives and forwards data frames.
- **Fwd. Trans**
  Specifies the number of changes from the "Discarding" status to the "Forwarding" status.
- **Edge Type**
  Specify the type of the "Edge Port". You have the following options:
  - "-"
    Edge port is disabled. The port is treated as a "no Edge Port".
  - Admin
    Select this option when there is always an end device on this port. Otherwise a reconfiguration of the network will be triggered each time a connection is changed.
  - Auto
    Select this option if you want a connected end device to be detected automatically at this port. When the connection is established the first time, the port is treated as a "no Edge Port".
  - Admin/Auto
    Select these options if you operate a combination of both on this port. When the connection is established the first time, the port is treated as an "Edge Port".

- **Edge**
  Shows the status of the port.
  - Enabled

    An end device is connected to this port.
  - Disabled
    There is a Spanning Tree or Rapid Spanning Tree device at this port.

  With an end device, a switch can change over the port faster without taking into account spanning tree frames. If a Spanning Tree frame is received despite this setting, the port automatically changes to the "Disabled" setting.
- **P.t.P. Type**
  Select the required option from the drop-down list. The selection depends on the port that is set.
  - "-"
    Point to point is calculated automatically. If the port is set to half duplex, a point-to-point link is not assumed.
  - P.t.P.
    Also with half duplex, a point-to-point link is assumed.
  - Shared Media
    Even with a full duplex connection, a point-to-point link is not assumed.

    Note

    Point-to-point connection means a direct connection between two devices. A shared media connection is, for example, a connection to a hub.
- **Restr. Role**
  If this check box is selected, the corresponding port is not selected as root port, regardless of the priority value. If the check box is selected, the port with the lowest priority also does not become the root port. Only activate this option if you wish to restrict the impact of bridges outside of the administered range to the Spanning Tree topology.
- **Restr. TCN**
  If this check box is selected, the corresponding port does not forward either received or detected topology changes (Topology Change Notifications) to other ports. Only activate this option if you wish to restrict the impact of bridges outside of the administered range to the Spanning Tree topology.

4.5.8.4 Enhanced Passive Listening Compatibility

Spanning Tree and ring redundancy

If you enable Enhanced Passive Listening Compatibility, topology change notifications will be sent via RSTP edge ports. In conjunction with the "Edge Type" function (see "Layer 2 > Spanning Tree > CIST Port"), this parameter is necessary to link spanning tree networks with HRP rings. Otherwise no TCN frames will be sent via edge ports; this is, however, necessary for the passive listening function on ring nodes.

Enabling the function

On this page, you can enable the "Enhanced Passive Listening Compatibility" function.

Description of the displayed boxes

The page contains the following box:

- **Enhanced Passive Listening Compatibility**
  Enable or disable this function for the entire device.

Steps in configuration

1. Enable or disable "Enhanced Passive Listening Compatibility"
2. Click the "Set Values" button.

4.5.9 DCP Forwarding

Applications

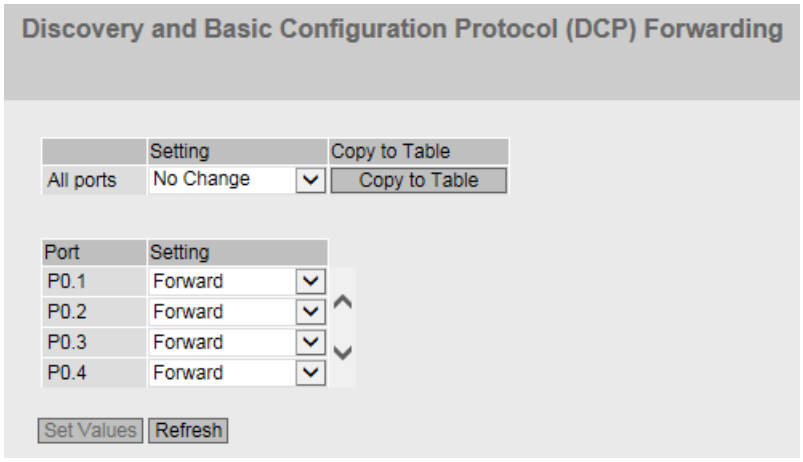
The DCP protocol is used by STEP 7 and SINEC PNI for configuration and diagnostics. When shipped, DCP is enabled on all ports; in other words, DCP frames are forwarded at all ports. With this option, you can disable the forwarding of the frames for individual ports, for example to exclude individual parts of the network from configuration with SINEC PNI or to divide the full network into smaller subnetworks for configuration and diagnostics.

Note

PROFINET configuration

Since DCP is a PROFINET protocol, the configuration created here is only effective in the VLAN associated with the TIA interface.

All the ports of the device are displayed on this page. After each displayed port, there is a drop-down list for function selection.



Description of the displayed values

Table 1 has the following columns:

- **1st column**
  Shows that the settings are valid for all ports of table 2.
- **Setting**
  Select the setting from the drop-down list. If "No Change" is selected, the entry in table 2 remains unchanged.
- **Copy to Table**
  If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
  Shows the available ports. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.
- **Setting**
  From the drop-down list, select whether the port should block or forward outgoing DCP frames. You have the following options available:
  - Forward
    DCP frames are forwarded via this port.
  - Block
    No outgoing DCP frames are forwarded via this port. It is nevertheless still possible to receive via this port.

Configuration procedure

1. From the options in the drop-down list in the row, select which ports should support sending DCP frames.
2. Click the "Set Values" button.

4.5.10 LLDP

Identifying the network topology

LLDP (Link Layer Discovery Protocol) is defined in the IEEE 802.AB standard.

LLDP is a method used to discover the network topology. Network components exchange information with their neighbor devices using LLDP.

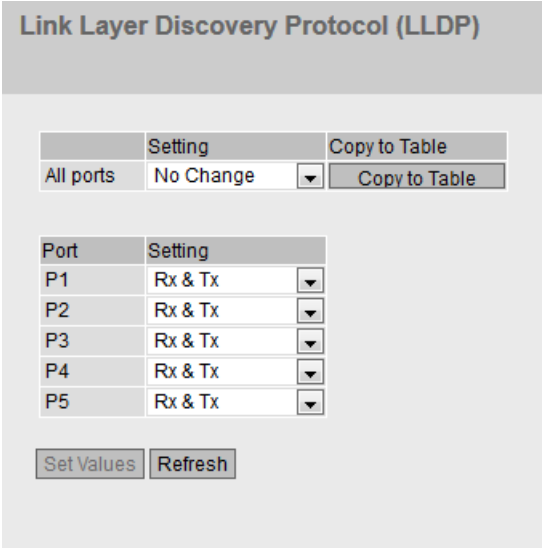
Network components that support LLDP have an LLDP agent. The LLDP agent sends information about itself and receives information from connected devices at periodic intervals. The received information is stored in the MIB.

Applications

PROFINET uses LLDP for topology diagnostics. In the factory setting, LLDP is enabled for all available ports; in other words, LLDP frames are sent on the ports.

The information sent is stored on every device with LLDP capability in an LLDP MIB file. Network management systems can access these LLDP MIB files using SNMP and therefore recreate the existing network topology. In this way, an administrator can find out which network components are connected to each other and can localize disruptions.

On this page, you have the option of enabling or disabling sending and/or receiving per port.



Description

Table 1 has the following columns:

- **All Ports**
  Shows that the settings are valid for all ports.
- **Setting**
  Select the setting from the drop-down list. If "No Change" is selected, the entry in table 2 remains unchanged.
- **Copy to Table**
  If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
  Shows the available ports.
- **Setting**
  Specify the LLDP functionality. The following options are available:
  - Rx
    This port can only receive LLDP frames.
  - Tx
    This port can only send LLDP frames.
  - Rx & Tx
    This port can receive and send LLDP frames.
  - "-" (disabled)
    This port can neither receive nor send LLDP frames.

Procedure

1. Select the LLDP functionality of the port from the "Setting" drop-down list.
2. Click the "Set Values" button.

4.5.11 Fiber Monitoring Protocol

Requirements

- You can only use Fiber Monitoring with transceivers capable of diagnostics. Note the documentation of the devices.
- To be able to use the Fiber Monitoring function, enable LLDP. The Fiber Monitoring information is appended to the LLDP packets.

Monitoring optical links

With Fiber Monitoring, you can monitor the received power and the loss of power on optical links between two devices.

If you enable Fiber Monitoring on an optical port, the device sends the current transmit power of the port to its connection partner using LLDP packets. In addition to sending, the device also checks whether corresponding information is received from the connection partner.

Regardless of whether the device receives diagnostics information from its connection partner, it monitors the received power measured at the optical port for the set limit values.

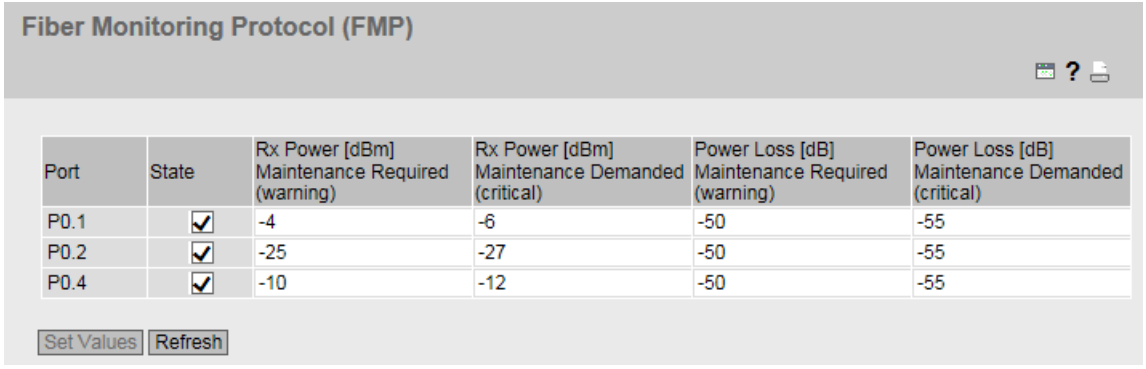
If Fiber Monitoring is enabled on the connection partner, the connection partner transfers the current value for the transmit power of the port to the device. The device compares the value it has received for the transmit power with the actually received power. The difference between the received power and the transmit power represents the power loss on the link. The calculated power loss is also monitored for the set limit values.

If the value of the received power or the power loss falls below or exceeds the set limit values, an event is triggered. You can set limit values in two stages for messages with the severity levels "Warning" and "Critical".

In "System > Events > Configuration", you can specify how the device indicates the event.

Note

If you have enabled Fiber Monitoring and a pluggable transceiver with diagnostics capability is pulled, Fiber Monitoring is automatically disabled for this port and the set limit values and a possibly pending error status are deleted.



Description of the displayed boxes

In the table you can specify the limit values for the measured received power too be monitored and the calculated power loss.

- **Port**
  Shows the optical ports that support Fiber Monitoring. This depends on the transceivers.
- **Status**
  Enable or disable Fiber Monitoring.
  As default, the function is disabled.

- **Rx Power [dBm] Maintenance Required (Warning)**
  Specify the value at which you are informed of the deterioration of the received power by a message of the severity level "Warning".
  If you enter the value "0", the received power is not monitored.
  The default value depends on the relevant transceiver.
- **Rx Power [dBm] Maintenance Demanded (Critical)**
  Specify the value at which you are informed of the deterioration of the received power by a message of the severity level "Critical".
  If you enter the value "0", the received power is not monitored.
  The default value depends on the relevant transceiver.
- **Power Loss [dB] Maintenance Required (Warning)**
  Specify the value at which you are informed of the power loss of the connection by a message of the severity level "Warning".
  If you enter the value "0", the power loss is not monitored.
  Default: -50 dB
- **Power Loss [dB] Maintenance Demanded (Critical)**
  Specify the value at which you are informed of the power loss of the connection by a message of the severity level "Critical".
  If you enter the value "0", the power loss is not monitored.
  Default: -55 dB

Configuration procedure

Activating fiber monitoring

Follow the steps below to activate the monitoring of a port:

1. Select the appropriate check box in the "Status" column.
2. For your setup, enter practical values value at which you want to be informed of deterioration of the received power and the power loss of the connection.
3. Click the "Set Values" button.

Deactivating fiber monitoring

Follow the steps below to deactivate the monitoring of a port:

1. Deselect the appropriate check box in the "Status" column.
2. Click the "Set Values" button.

Follow the steps below to deactivate the monitoring of the Rx power or power loss:

1. Enter the value "0" in the appropriate box.
2. Click the "Set Values" button.

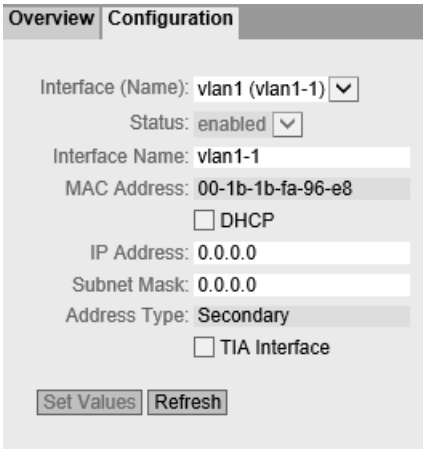
4.5.12 Unicast

4.5.12.1 Filtering

Address filtering

This table shows the unicast addresses entered statically by the user during parameter assignment.

On this page, you also define the static unicast filters.



Description of the displayed boxes

The page contains the following boxes:

- **VLAN ID**
  Select the VLAN ID in which you configure a new static MAC address. If nothing is set, "VLAN1" is set as the basic setting.
- **MAC Address**
  Enter the MAC address here.

The table contains the following columns:

- **Select**
  Select the row you want to delete.
- **VLAN ID**
  Shows the VLAN-ID assigned to this MAC address.
- **MAC Address**
  Shows the MAC address of the node that the device has learned or the user has configured.

- **Status**
  Shows the status of each address entry:
  - Static
    Configured by the user. Static addresses are stored permanently; in other words, they are not deleted when the Aging Time expires or when the switch is restarted.
  - Invalid
    These values are not evaluated.
- **Port**
  Shows the port via which the node with the specified address can be reached. Frames received by the device whose destination address matches this address will be forwarded to this port.

Note

You can only specify **one** port for unicast addresses.

Configuration procedure

To edit the entries, follow the steps below.

Creating a new entry

1. Select the relevant VLAN ID.
2. Enter the MAC address in the "MAC address" input box.
3. Click the "Create" button to create a new entry in the table.
4. Select the relevant port from the drop-down list.
5. Click the "Set Values" button.

Changing the entry

1. Select the relevant port.
2. Click the "Set Values" button.

Deleting an entry

1. Select the check box in the row to be deleted.
   Repeat this for all entries you want to delete.
2. Click the "Delete" button to delete the selected entries from the filter table.
3. Click the "Refresh" button.

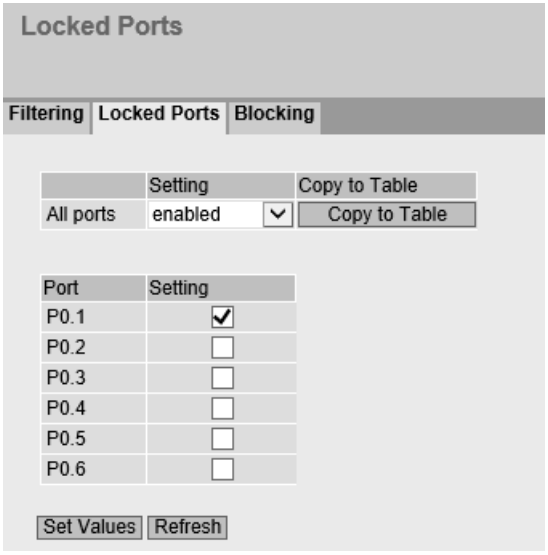
4.5.12.2 Locked Ports

Activating the access control

On this page, you can block individual ports for unknown nodes.

If the Port Lock function is enabled, packets arriving at this port from unknown MAC addresses are discarded immediately. Packets from known nodes are accepted by the port. Since ports with the Port Lock function enabled cannot learn any MAC addresses, learned

addresses on these ports are automatically deleted after the Port Lock function is enabled. The port accepts only static MAC addresses that were created previously either manually or with the "Start learning" function and the "Stop learning" function.



Description of the displayed boxes

Table 1 has the following columns:

- **1st column**
  Shows that the settings are valid for all ports of table 2.
- **Setting**
  Select the setting from the drop-down list. You have the following setting options:
  - Enabled
    Enables the port lock function.
  - Disabled
    Disables the port lock function.
  - No change
    Table 2 remains unchanged.
- **Copy to Table**
  If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
  This column lists all the ports available on this device.
- **Setting**
  Enable or disable access control for the port.

Configuration procedure

Enabling access control for an individual port

1. Select the check box in the relevant row in table 2.
2. To apply the changes, click the "Set Values" button.

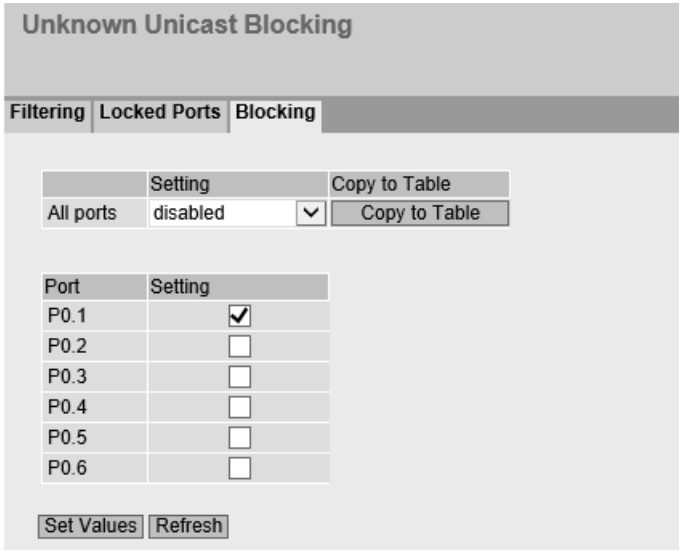
Enabling access control for all ports

1. In the "Setting" drop-down list in Table 1, select the "Enabled" entry.
2. Click the "Copy to Table" button. The check box is enabled for all ports in table 2.
3. To apply the changes, click the "Set Values" button.

4.5.12.3 Blocking

Blocking forwarding of unknown unicast frames

On this page, you can block the forwarding of unknown unicast frames for individual ports.



Description of the displayed values

Table 1 has the following columns:

- **1st column**
  Shows that the settings are valid for all ports of table 2.
- **Setting**
  Select the setting from the drop-down list. You have the following setting options:
  - Enabled
    Blocking of unicast frames is enabled.
  - Disabled
    Blocking of unicast frames is disabled.
  - No change
    Table 2 remains unchanged.
- **Copy to Table**
  If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
  All available ports are listed in this column. Unavailable ports are not displayed.
- **Setting**
  Enable or disable the blocking of unicast frames.

Steps in configuration

Enabling blocking for an individual port

1. Select the check box in the relevant row in table 2.
2. To apply the changes, click the "Set Values" button.

Enabling blocking for all ports

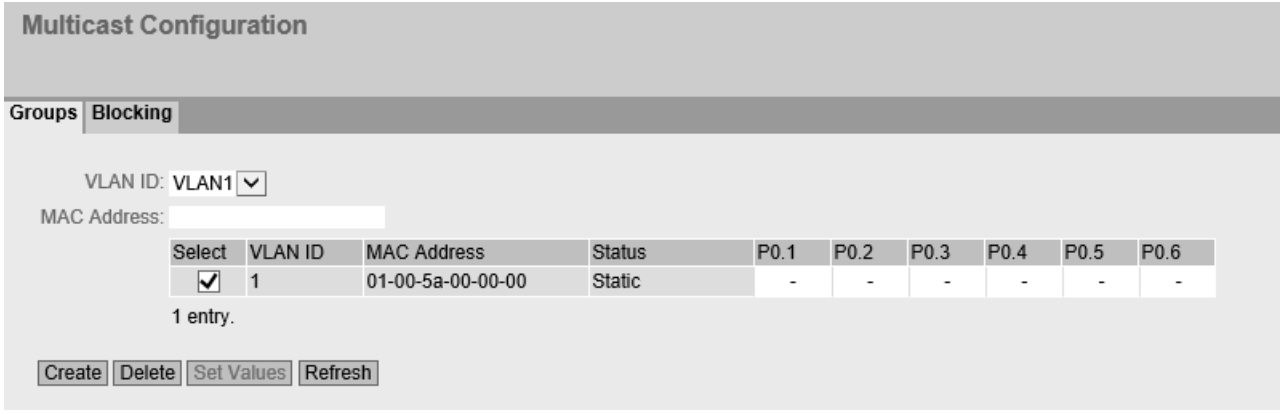
1. In the "Setting" drop-down list, select the "Enabled" entry.
2. Click the "Copy to Table" button. The check box is enabled for all ports in table 2.
3. To apply the changes, click the "Set Values" button.

4.5.13 Multicast

4.5.13.1 Groups

Multicast applications

In the majority of cases, a frame is sent with a unicast address to a particular receiver. If an application sends the same data to several receivers, the amount of data can be reduced by sending the data using one multicast address. For some applications (e.g. NTP), there are fixed multicast addresses.



Description of the displayed boxes

The page contains the following boxes:

- **VLAN ID**
  If you click on this text box, a drop-down list is displayed. Here you can select the VLAN ID of a new MAC address you want to configure.
- **MAC address**
  Here you enter a new MAC multicast address you want to configure.

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **MAC address**
  Here, the multicast address is displayed that the device has learned or the user has configured.
- **Status -** Static
  Shows the status of each address entry. The address was entered statically by the user. Static addresses are stored permanently; in other words, they are not deleted when the Aging-Time expires or when the device is restarted. These must be deleted by the user.

Configuration procedure

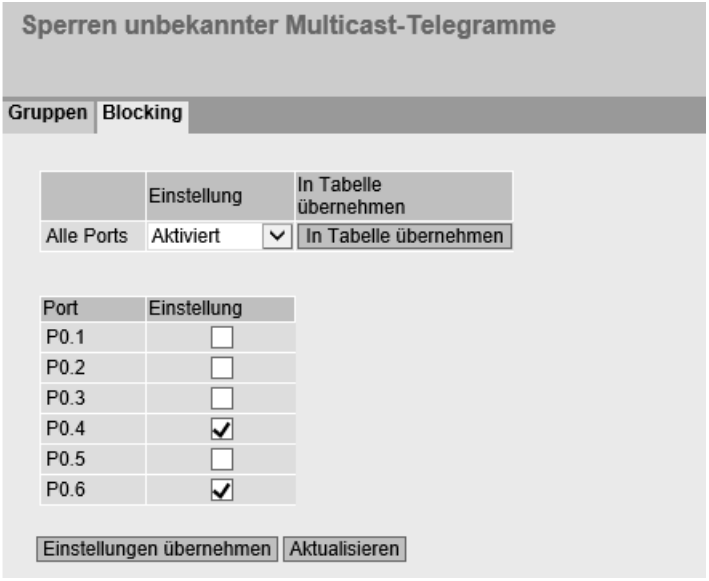
Creating a new entry

1. Select the required VLAN ID from the ""drop-down list.
2. Enter the MAC address in the "MAC address" input box.
3. Click the "Create" button. A new entry is generated in the table.
4. Assign the relevant ports to the MAC address.
5. Click the "Set Values" button.

4.5.13.2 Blocking

Disabling the forwarding of unknown multicast frames

On this page, you can block the forwarding of unknown multicast frames for individual ports.



Description of the displayed values

Table 1 has the following columns:

- **1st column**
  Shows that the settings are valid for all ports of table 2.
- **Setting**
  Select the setting from the drop-down list. You have the following setting options:
  - Enabled
    Blocking of multicast frames is enabled.
  - Disabled
    Blocking of unknown multicast frames is disabled.
  - No change
    Table 2 remains unchanged.
- **Copy to Table**
  If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
  All available ports are listed in this column. Unavailable ports are not displayed.
- **Setting**
  Enable or disable the blocking of multicast frames.

Steps in configuration

Enabling blocking for an individual port

1. Select the check box in the relevant row in table 2.
2. To apply the changes, click the "Set Values" button.

Enabling blocking for all ports

1. In the "Setting" drop-down list, select the "Enabled" entry.
2. Click the "Copy to Table" button. The check box is enabled for all ports in table 2.
3. To apply the changes, click the "Set Values" button.

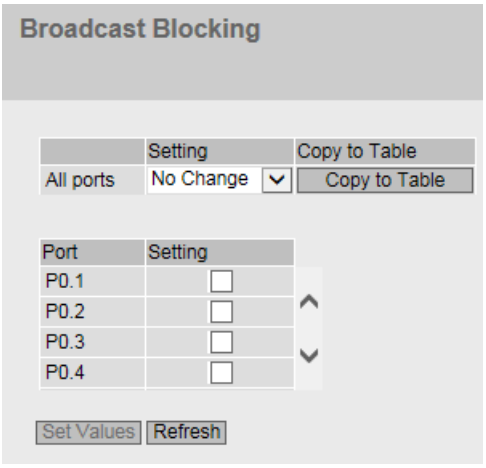
4.5.14 Broadcast

Blocking the forwarding of broadcast frames

On this page, you can block the forwarding of broadcast frames for individual ports.

Note

Some communication protocols work only with the support of broadcast. In these cases, blocking can lead to loss of data communication. Block broadcast only when you are sure that you do not need it on the selected ports.



Description of the displayed boxes

Table 1 has the following columns:

- **1st column**
  Shows that the settings are valid for all ports of table 2.
- **Setting**
  Select the setting from the drop-down list. You have the following setting options:
  - Enabled
    The blocking of broadcast frames is enabled.
  - Disabled
    The blocking of broadcast frames is disabled.
  - No change
    Table 2 remains unchanged.
- **Copy to Table**
  If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
  All available ports are displayed.
- **Setting**
  Enable or disable the blocking of broadcast frames.

Steps in configuration

Enabling the blocking of broadcast frames for an individual port

1. Select the check box in the relevant row in table 2.
2. To apply the changes, click the "Set Values" button.

Enabling the blocking of broadcast frames for all ports

1. In the "Setting" drop-down list in table 1, select the "Enabled" entry.
2. Click the "Copy to Table" button. The check box is enabled for all ports in table 2.
3. To apply the changes, click the "Set Values" button.

4.5.15 RMON

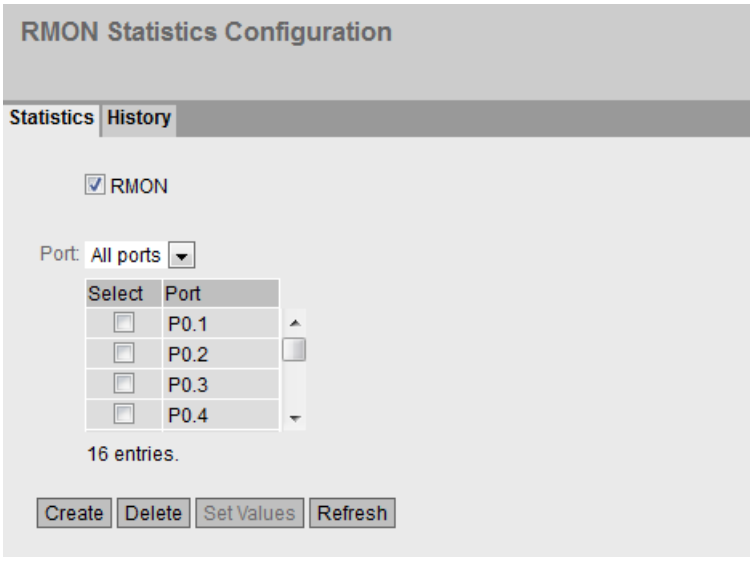
4.5.15.1 Statistics

Statistics

On this page you can specify the ports for which RMON statistics are displayed.

The RMON statistics are shown on the page “Information > Ethernet Statistics” in “Packet Size”, “Frame Type” and “Packet Error” tabs.

Settings



- **RMON**
  If you select this check box, Remote Monitoring (RMON) allows diagnostics data to be collected on the device, prepared and read out using SNMP by a network management station that also supports RMON. This diagnostic data, for example port-related load trends, allow problems in the network to be detected early and eliminated.

  Note

  If you disable RMON, these statistics are not deleted but retain their last status.

- **Port**
  Select the ports for which statistics will be displayed.

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **Port**
  Shows the ports for which statistics will be displayed.

Steps in configuration

Enabling the function

1. Select the "RMON" check box.
2. Click the "Set Values" button.
   The "RMON" function is enabled.

Enabling RMON statistics for ports

Note

Requirement

To allow RMON statistics to be displayed for a port, the "RMON" function must be enabled.

1. Select the required port from the "Port" drop-down list or the entry "All Ports".
2. Click the "Create" button.
   RMON statistics can be displayed for the selected port or for all ports.

Disabling RMON statistics for ports

1. Select the row you want to delete in the "Select" column.
2. Click the "Delete" button.
   No RMON statistics are displayed for the selected port.

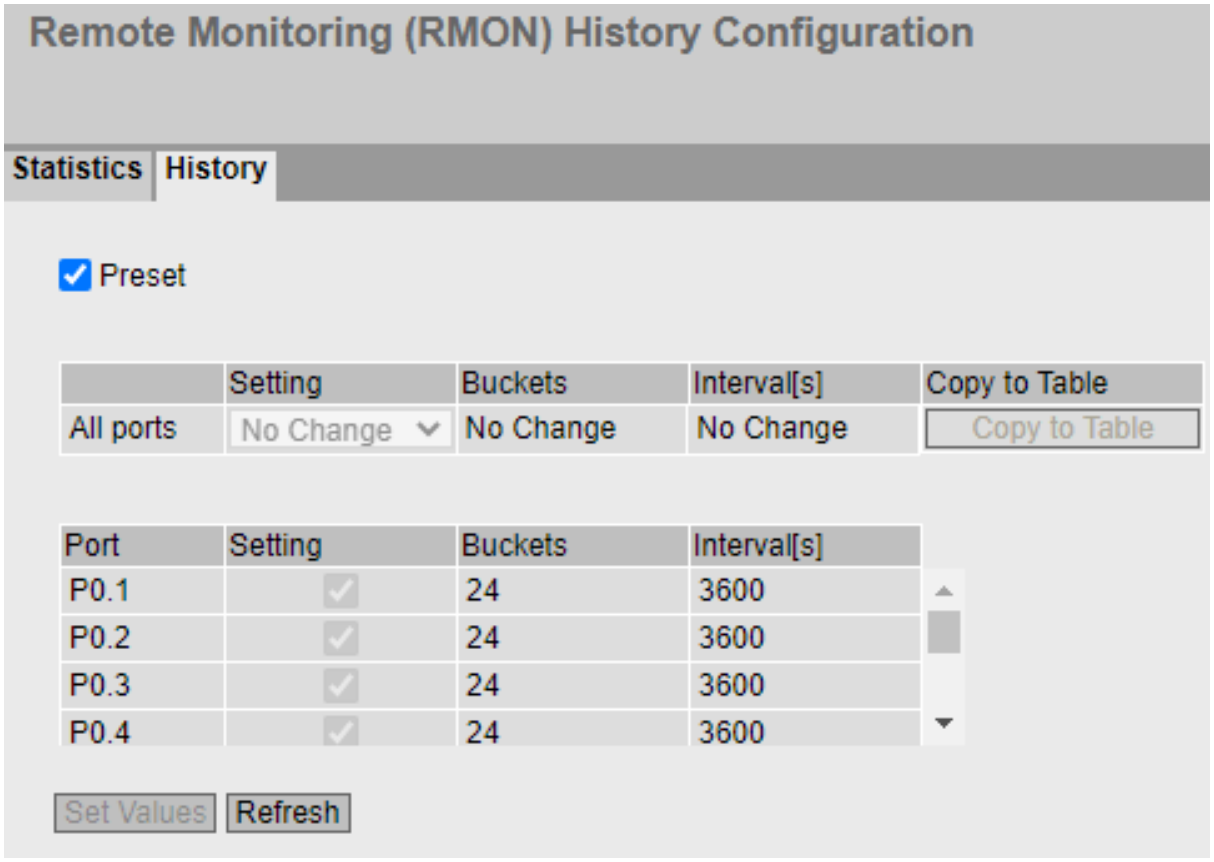
4.5.15.2 History

Samples of the statistics

On this page, you can specify whether or not samples of the statistics are saved for a port. You can specify how many entries should be saved and at which intervals samples should be taken.

Enabled RMON statistics are displayed on the WBM page "Information > Ethernet statistics > History".

Settings



The page contains the following boxes:

- **Default**
  If you enable the option, all custom RMON history settings are deleted and overwritten with the following settings for all ports:
  - Setting: Enabled
  - Entries: 24
  - Interval[s]: 3600

  The values for an individual configuration are locked as long as the default for the RMON history is enabled.
  If you disable the option, the settings are retained, but are individually configurable again.

Table 1 has the following columns:

- **1st column**
  Shows that the settings are valid for all ports.
- **Setting**
  Select the required setting. If "No Change" is selected, the entry in table 2 remains unchanged.

- **Buckets**
  Enter the maximum number of samples to be stored at the same time. If "No Change" is entered, the entry in table 2 remains unchanged
- **Interval [s]**
  Enter the interval after which the current version of the statistics should be saved as sample. If "No Change" is entered, the entry in table 2 remains unchanged
- **Copy to Table**
  If you click the button, the settings are adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
  Shows the port to which the settings relate.
- **Setting**
  Enable or disable the recording of the history on the relevant port.
- **Buckets**
  Enter the maximum number of samples to be stored at the same time.
  The maximum number of entries can be restricted by the capacity of the device.
  Range of values: 1 - 65535
  Factory setting: 24
- **Interval [s]**
  Enter the interval after which the current version of the statistics should be saved as sample.
  Range of values: 1 - 3600
  Factory setting: 3600

Configuration procedure

Enabling RMON statistics for individual ports

1. Select the check box "Setting" in the relevant row in table 2.
   The "Buckets" and "Interval[s]" boxes become active with the factory settings.
2. Enter the required values in the "Buckets" and "Interval[s]" boxes.
3. Click the "Set Values" button.

Enabling RMON statistics for all ports

1. In the "Setting" drop-down list, select the "Enabled" entry in table 1.
2. Enter the required values in the "Buckets" and "Interval[s]" boxes. If you do not change the entries in both boxes, the factory defaults will be used for all ports.
3. Click the "Copy to Table" button.
   The settings are adopted for all ports of table 2.
4. Click the "Set Values" button.

Activate **RMONdefault**

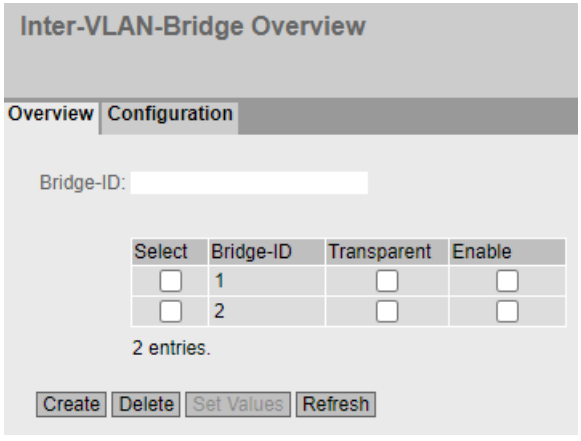
1. Select the "Default" check box.
2. Click the "Set Values" button.

4.5.16 Inter-VLAN Bridge (SC63x/SC64x)

4.5.16.1 Overview

Overview

You can create one bridge per device and add a maximum of six VLANs to the bridge.



Description

The page contains the following boxes:

- **Bridge-ID**
  Enter the bridge ID in the "Bridge-ID" text box. The Bridge-ID (a number between 1 and 255) can only be assigned once when creating a new data record and can then no longer be changed. To make a change, the entire data record must be deleted and created again.

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **Bridge-ID**
  Shows the bridge ID.

- **Transparent**
  When you enable this option, the Inter-VLAN Bridge and the associated VLANs are switched to transparent mode when the bridge is activated. Ports belonging to the bridge become transparent ports. This means the following:
  - Tagged frames that are received at these ports are not evaluated and are forwarded to all other ports of the Inter-VLAN bridge with unchanged tag. No frames are forwarded from ports that do not belong to the Inter-VLAN Bridge to ports that belong to the Inter-VLAN bridge.
  - Untagged frames that are received at these ports are also forwarded to all other ports of the Inter-VLAN bridge without tag.
  - As long as the transparent bridge is enabled, you cannot change the port associations of the affected VLANs.

  The prerequisite for this is that the port VLAN ID of all ports belonging to the VLAN is set to the VLAN ID.
  If you disable this option, the VLAN tags are evaluated.
- **Enable**
  Enables the bridge between the VLANs specified in the "Configuration" tab. After it has been enabled, the bridge adopts the IP address configuration of the VLANs for which the Type "Master" was selected in the "Configuration" tab. The devices of the VLANs can no longer be reached at their own IP addresses after the bridge has been enabled but only over the IP address of the bridge.

Procedure

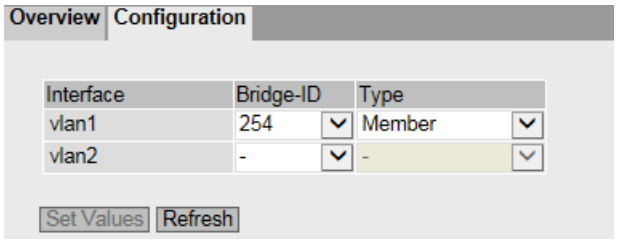
Create new Bridge-ID

1. Enter an ID in the "Bridge-ID" text box.
2. Click the "Create" button. A new entry is generated in the table.
3. Click the "Set Values" button.

4.5.16.2 Configuration

Configuration

On this page you specify the VLANs between which a bridge is to be set up and which VLAN is to be used as master VLAN. You select the bridge you want to use by using its Bridge-ID that was created in the "Overview" tab.



Description

The page contains the following boxes:

- **Interface**
  VLAN or NVE interface to which the setting relates. The list of interfaces is dynamic and is based on the settings from "Layer 3 > Subnets" and "Layer 2 > VXLAN".
- **Bridge-ID**
  Select the ID of the bridge that is to be used for the selected interface.
- **Type**
  Select the type of the interface.
  - Member: The IP address configuration of the interface is not used for the bridge.
  - Master: The IP address configuration of the interface is used for the bridge. Use this setting for the VLAN / interface that is used by the TIA Portal for access to the devices of the VLANs.

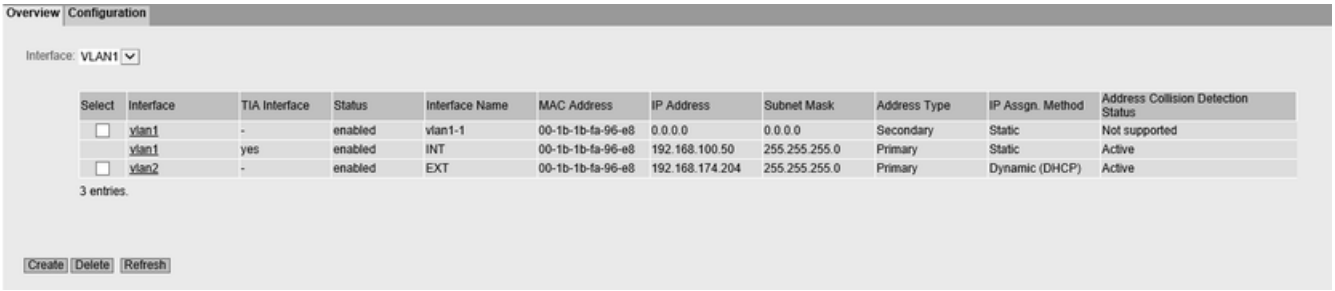
  Special features of the TIA interface
  If one of the interfaces is configured as TIA interface, you must set the type "Master" for it. Otherwise, the bridge cannot be enabled.

4.6 Menu "Layer 3 (IPv4)"

4.6.1 Subnets

4.6.1.1 Overview

The page shows the subnets for the selected interface. A subnet always relates to an interface and is created in the "Configuration" tab.



Description

The page contains the following box:

- **Interface**
  Select the interface on which you want to configure another subnet.
- **Unique VLAN MAC Address**
  When enabled, a separate MAC address is assigned to each VLAN interface. A restart or "Link down" and "Link up" is required to enable this.
  When disabled, all VLAN interfaces have the MAC address of the first VLAN that is inserted.

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **Interface**
  Shows the interface.
- **TIA Interface**
  Shows the selected TIA interface.
- **Status**
  Shows whether or not the interface is enabled.
- **Interface Name**
  Shows the name of the interface.
- **MAC Address**
  Shows the MAC address.
- **IP Address**
  Shows the IPv4 address of the subnet.
- **Subnet Mask**
  Shows the subnet mask.
- **Address Type**
  Shows the address type. The following values are possible:
  - Primary
    The first IPv4 address that was configured on an IPv4 interface.
  - Secondary
    All other IPv4 addresses that were configured on the IPv4 interface.

- **IP Assignment Method**
  Shows how the IPv4 address is assigned. The following values are possible:
  - Static
    The IPv4 address is static. You enter the settings in "IP Address" and "Subnet Mask".
  - Dynamic (DHCP)
    The device obtains a dynamic IPv4 address from a DHCPv4 server.
- **Address Collision Detection Status**
  If new IPv4 addresses become active in the network, the "Address Collision Detection" function checks whether this can result in address collisions. The allows IPv4 addresses that would be assigned twice to be detected.

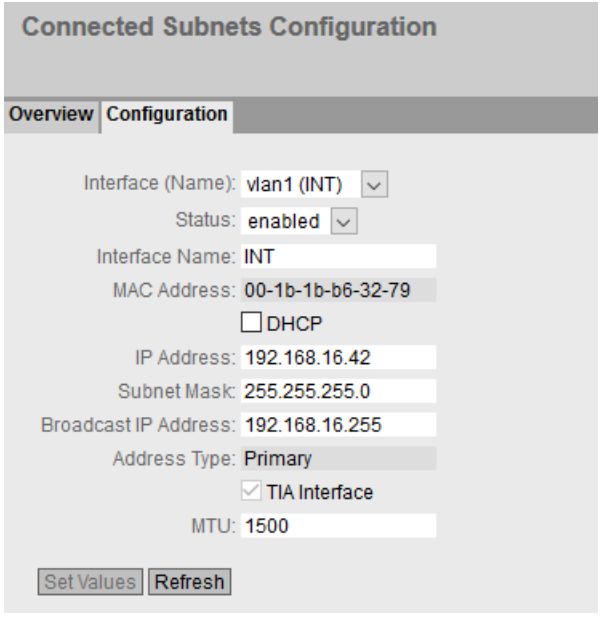
  Note

  The function does not run a cyclic check.

  This column shows the current status of the function. The following values are possible:
  - Idle
    The interface is not enabled and does not have an IPv4 address.
  - Starting
    This status indicates the start-up phase. In this phase, the device initially sends a query as to whether the planned IPv4 address already exists. If the address is not yet been assigned, the device sends the message that it is using this IP address as of now.
  - Conflict
    The interface is not enabled. The interface is attempting to use an IPv4 address that has already been assigned.
  - Defending
    The interface uses a unique IPv4 address. Another interface is attempting to use the same IPv4 address.
  - Active
    The interface uses a unique IPv4 address. There are no collisions.
  - Not supported
    The function for detection of address collisions is not supported.
  - Disabled
    The function for detection of address collisions is disabled.

4.6.1.2 Configuration

On this page, you configure the subnet for the interface.



Description

The page contains the following:

- **Interface (Name)**
  Select the interface from the drop-down list.
- **Status**
  Enable or disable the interface.
- **Interface Name**
  Enter the name of the interface.
- **MAC Address**
  Displays the MAC address of the selected interface.
- **DHCP**
  When enabled, the interface obtains the IPv4 address from a DHCP server.
- **IP Address**
  Enter the IPv4 address of the interface. The IPv4 addresses must not be used more than once.
- **Subnet Mask**
  Enter the subnet mask of the subnet you are creating. Subnets on different interfaces must not overlap.
- **Broadcast IP Address**
  If a specific IP address is to be used as the broadcast IP address of the subnet, enter this. Otherwise the last IP address of the subnet will be used.

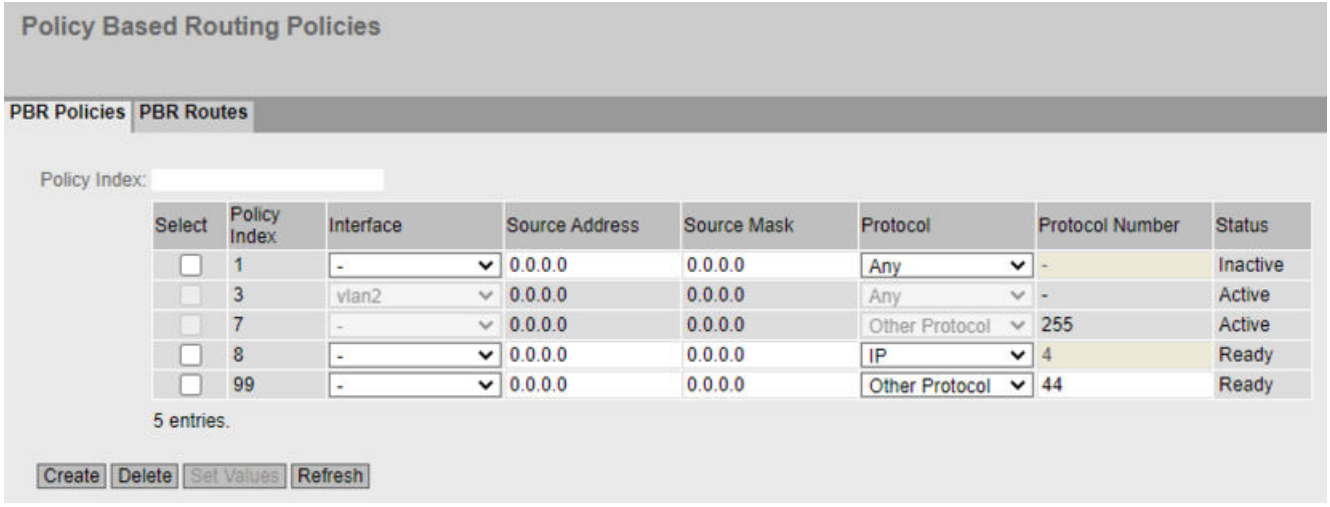
- **Address Type**
  Shows the address type. The following values are possible:
  - Primary
    The first subnet of the interface.
  - Secondary
    All further subnets of the interface.
- **TIA Interface**
  Select whether this interface should become the TIA interface. The TIA interface defines on which VLAN the PROFINET functionalities are available. This mainly affects the device search with or via DCP.
- **MTU**
  MTU (Maximum Transmission Unit) specifies the maximum size of the packet. If packets are longer than the set MTU, they are fragmented. The MTU covers the IP header and the headers of the higher layers.
  The range of values is from 90 to 1500 bytes.

4.6.2 PBR

4.6.2.1 PBR Policies

Configuration of PBR policies

On this page, you configure the policies for the Policy Based Routing.



Description of the displayed boxes

The page contains the following boxes:

- **Policy Index**
  Enter a number to uniquely identify the PBR policy.

The table contains the following columns:

- **Select**
  Select the row you want to delete.
  If a PBR policy is linked to a PBR route, you cannot delete the PBR policy. Delete the associated PBR route first.
- **Policy Index**
  Shows the number of the PBR policy.
- **Interface**
  Select the VLAN IP interface to which the PBR policy applies.
- **Source Address**
  Enter the source address of the network or device to which the PBR policy applies.
- **Source Subnet Mask**
  Enter the source subnet mask of the network or device to which the PBR policy applies.
- **Protocol**
  Select the desired layer 4 protocol for the PBR policy. The corresponding protocol number is displayed in the next column.
  If you select the "Other Protocol" entry, protocol number 254 is set in the next column by default. You can change this setting.
- **Protocol Number**
  Shows the protocol number of the layer 4 protocol.
- **Status**
  Shows the status of the PBR policy.
  - Inactive
    The PBR policy has been created but not completely configured. In this status, the PBR policy cannot be linked to a PBR route.
  - Ready
    The PBR policy is completely configured and can be linked to a PBR route.
  - Active
    The PBR policy is linked to a PBR route.

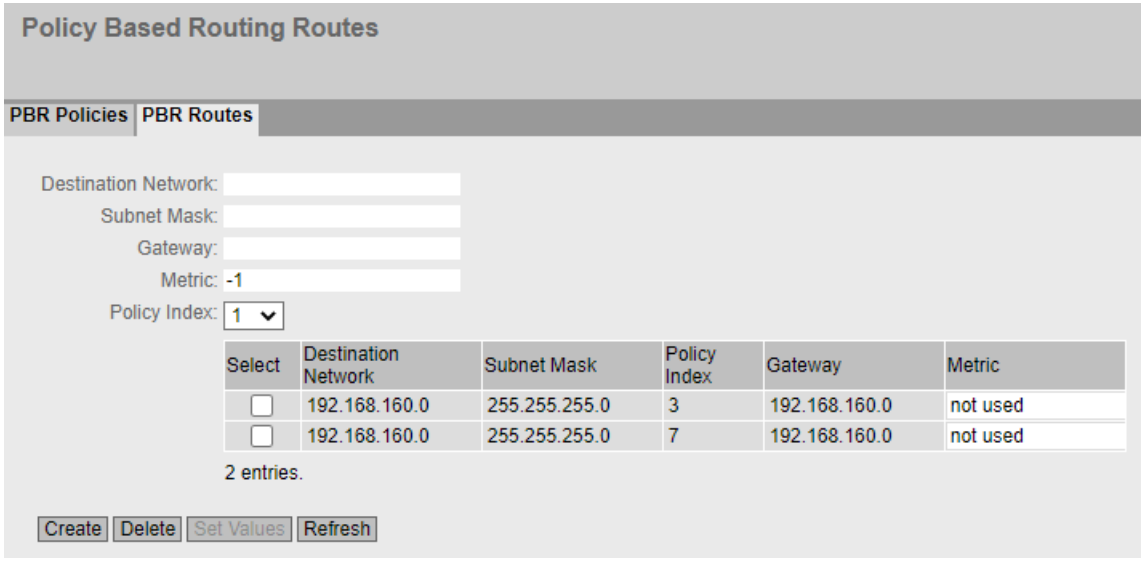
Configuration procedure

1. In the "Policy Index" text box, enter a unique number for the PBR policy.
2. Click the "Create" button. A new entry is generated in the table.
3. Configure the PBR policy.
4. Click the "Set Values" button.

4.6.2.2 PBR Routes

Configuration of PBR routes

On this page, you configure the routes for Policy Based Routing. To be able to create a PBR route, at least one PBR policy must be configured.



Description of the displayed boxes

The page contains the following boxes:

- **Destination Network**
  Enter the IP address of the destination network.
- **Subnet Mask**
  Enter the subnet mask of the destination network.
- **Gateway**
  Enter the IP address of the gateway router.
- **Metric**
  Enter the metric of the PBR route.
- **Policy Index**
  Select the PBR policy number that applies to the PBR route. You can only select PBR policies with "Ready" status.

The table contains the following columns:

- **Select**
  Select the row you want to delete.
- **Destination Network**
  The IP address of the destination network.
- **Subnet Mask**
  The subnet mask of the destination network.

- **Policy Index**
  The number of the PBR policy that applies to the PBR route.
- **Gateway**
  The IP address of the gateway router.
- **Metric**
  The routing metric of the destination network.

Configuration procedure

1. Make sure at least one PBR policy is configured and in the "Ready" status.
2. Configure the PBR route.
3. Click the "Create" button. A new entry is generated in the table.

4.6.3 OSPFv2

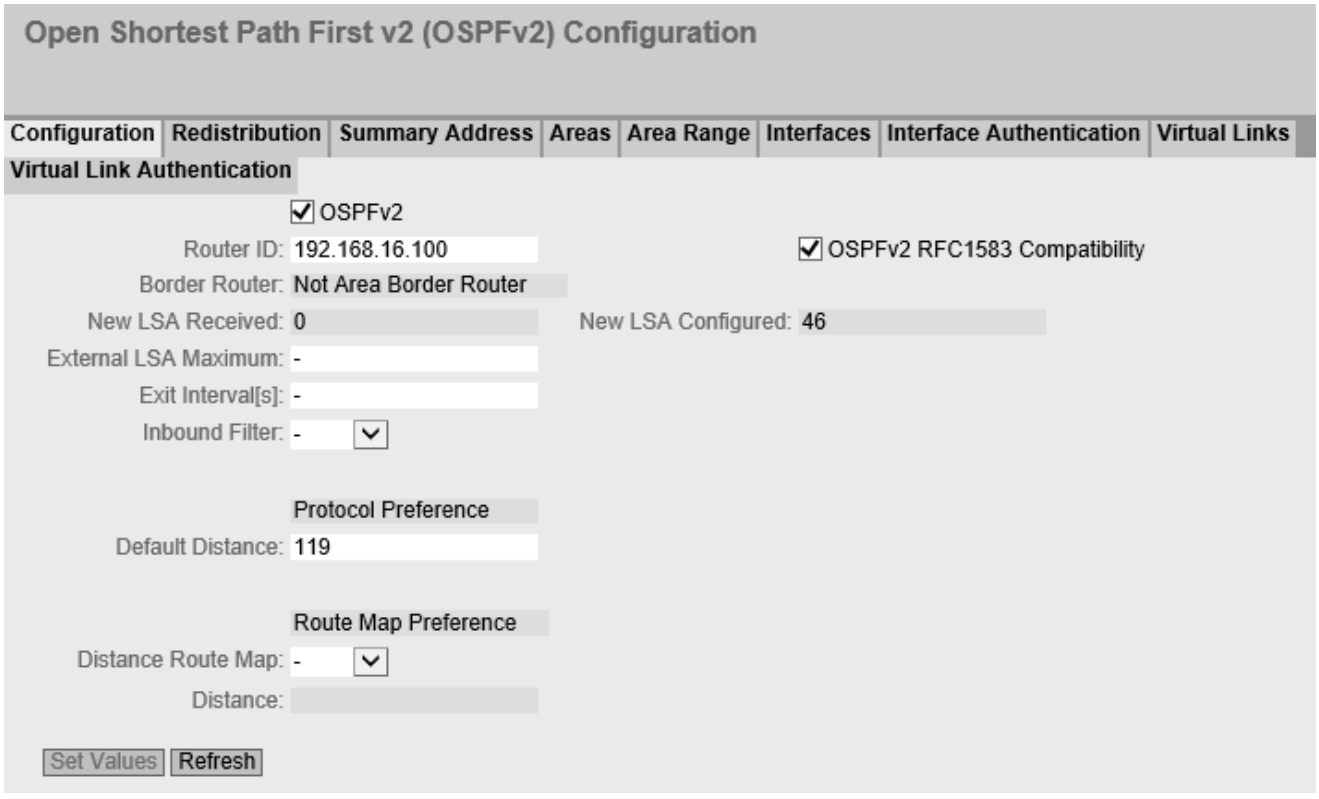
4.6.3.1 Configuration

Introduction

On this page, you configure the routing using OSPFv2.

Note

This function is available only with layer 3.



Description of the displayed values

The page contains the following boxes:

- **OSPFv2**
  Enable or disable routing using OSPFv2.
- **Router ID**
  Enter the name of one of the OSPFv2 interfaces. The name is entered in the IP address format and does not need to match the local IP address. The router ID must be unique in the network.
- **OSPFv2 RFC1583 Compatibility**
  In newer RFCs, the calculation of the shortest route to the destination is defined differently. If the option is enabled, the shortest path is also calculated via the backbone with the lowest path costs (metric). This ensures compatibility with older systems.
  If the option is disabled, paths within an area are preferred, even if the metric is higher. The paths do not necessarily lead via the backbone.
- **Border Router**
  Displays the status of the OSPFv2 router. If the local system is an active member in at least 2 areas, this is an area border router.
- **New LSA Received**
  Shows the number of received LSAs.
  Updates and its own LSAs are not counted.
- **New LSA Configured**
  Shows the number of different LSAs sent by this local system.

- **External LSA Maximum**
  To limit the number of entries of external LSAs in the database, enter the maximum number of external LSAs.
- **Exit Interval [s]**
  Enter the interval after which the OSPFv2 router once again attempts to leave the overflow status. A 0 means that the OSPF router attempts to exit the overflow status only following a restart.
- **Inbound Filter**
  Select a route map that filters inbound routes.
- **Protocol Preferences**
  - **Default Distance**
    Set the administrative distance for the OSPFv2 protocol.
- **Route Map Preferences**
  - **Distance Route Map**
    Select a route map from the drop-down list for which you want to specify the administrative distance.
  - **Distance**
    Configure the administrative distance for the previously selected route map.

Configuration procedure

1. Select the "OSPFv2" check box.
2. Enter the ID of the router in the "Router ID" input box.
3. Select the "AS Border Router" check box.
4. Click the "Set Values" button.

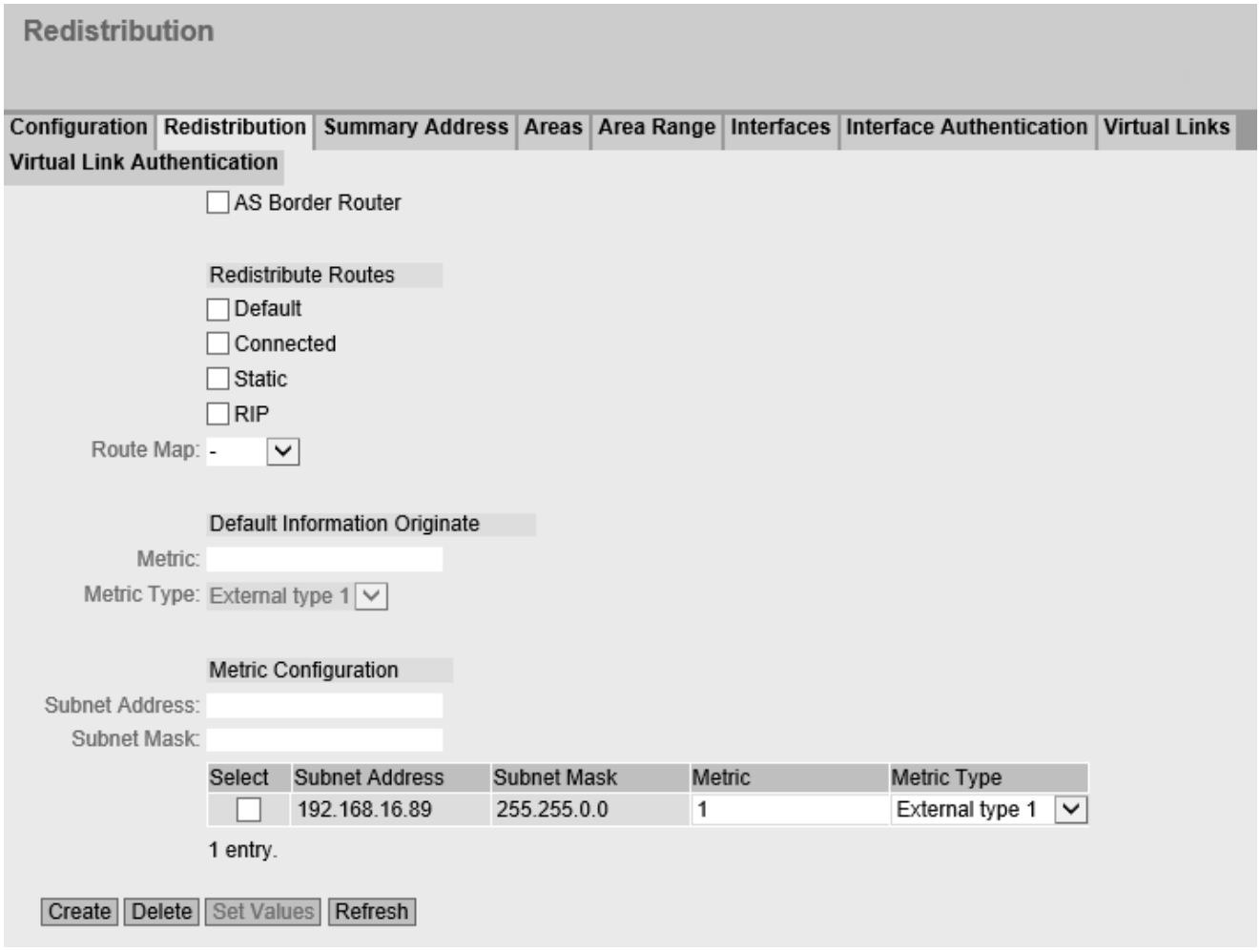
4.6.3.2 Redistribution

Redistribute Routes

On this page, you configure the redistribution of routing information.

Note

This function is available only with layer 3.


Redistribution
Configuration
Redistribution
Summary Address
Areas
Area Range
Interfaces
Interface Authentication
Virtual Links
Virtual Link Authentication
AS Border Router
Redistribute Routes
Default
Connected
Static
RIP
Route Map:
-
Default Information Originate
Metric:
Metric Type:
External type 1
Metric Configuration
Subnet Address:
Subnet Mask:
Select
Subnet Address
Subnet Mask
Metric
Metric Type
192.168.16.89
255.255.0.0
1
External type 1
1 entry.
Create
Delete
Set Values
Refresh

Description of the displayed boxes

The page contains the following boxes:

- **AS Border Router**
  Specify whether the router is an AS border router. An AS border router intercedes between multiple autonomous systems, for example if you have an additional RIP network. An AS border router is also necessary to add and to distribute static routes.
- **Redistribute Routes**
  Specify which known routes are distributed using OSPFv2. The following settings are possible:
  - Default
  - Connected
  - Static
  - RIP

  Note

  The options can only be enabled on an AS border router. Enabling the Default and Static options, in particular, can cause problems if they are enabled at too many points in the network, for example, forwarding loops.

- **Route Map**
  Select a route map that filters which routes are forwarded using OSPFv2.
- **Default Information Originate**
  A standard route is generated for external routes into the OSPF routing domain.
  - **Metric**
    If you enter metric information in this text box, the device becomes the default gateway for external routes in the OSPF routing domain.
    Range of values: 0 ... 16777215
  - **Metric Type**
    This drop-down list is only active when a value is entered in the "Metric" text box. Select how the metric is calculated. You have the following options:
    External type 1
    The sum of internal and external path costs.
    External type 2
    Only external costs; the internal path costs are ignored.
- **Metric Configuration**
  Configure the metric for forwarding routes of a subnet.
  - **Subnet Address**
    The IPv4 address of the network whose routing information is to be forwarded.
  - **Subnet Mask**
    The subnet mask of the network whose routing information is to be forwarded.

The table contains the following columns:

- **Select**
  Select the row you want to delete.
- **Subnet Address**
  Shows the IP address of the network whose routing information will be forwarded.
- **Subnet Mask**
  Shows the subnet mask of the network whose routing information will be forwarded.
- **Metric**
  The Metric for the subnet.
- **Metric Type**
  Select how the metric is calculated. You have the following options:
  - **External type 1**
    The sum of internal and external path costs.
  - **External type 2**
    Only external costs; the internal path costs are ignored.

Configuration procedure

1. Enter the IP address of the network whose routing information will be forwarded.
2. Enter the subnet mask of the network whose routing information will be forwarded.
3. Click the "Create" button. A new entry is generated in the table.
4. In the "Metric" column, enter the Metric for the subnet.
5. Select the suitable entry in the "Metric Type" column.
6. Click the "Set Values" button.

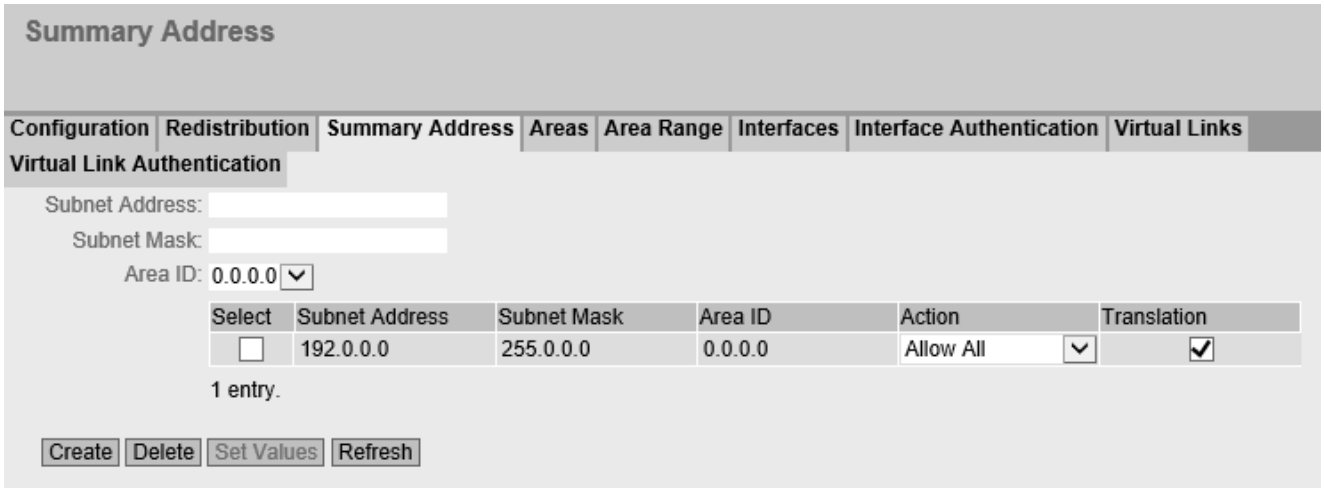
4.6.3.3 Summary Address

Subnets for routing information

On this page, you configure subnets for grouping routing information.

Note

This function is available only with layer 3.



Description of the displayed boxes

- **Subnet Address**
  The IPv4 address of the network whose routing information is to be forwarded.
- **Subnet Mask**
  The subnet mask of the network whose routing information is to be forwarded.
- **Area ID**
  The ID of the area to which the subnet is assigned.

The table contains the following columns:

- **Select**
  Select the row you want to delete.
- **Subnet Address**
  Shows the IP address of the network whose routing information will be forwarded.
- **Subnet Mask**
  Shows the subnet mask of the network whose routing information will be forwarded.
- **Area ID**
  The ID of the area to which the subnet is assigned.

- **Action**
  The following settings are possible:
  - **allowAll**
    This setting is only possible for the area ID 0.0.0.0. The backbone area generates an LSA message of type 5 for the address range and LSA messages of type 7 in the connected NSSAs.
  - **denyAll**
    This setting is only possible for the area ID 0.0.0.0. No LSAs of type 5 or type 7 are generated for the address range.
  - **advertise**
    The address range is advertised outside the areas. If the area ID is 0.0.0.0, the router generates LSA messages of Type 5. If the area ID is not 0.0.0.0, the router generates LSA messages of Type 7.
  - **not-advertise**
    If the area ID is 0.0.0.0, no LSA messages of type 5 will be generated. The NSSAs connected to the backbone area generate LSA messages of Type 7. If the area ID is not 0.0.0.0, no LSA messages of type 7 will be generated.
- **Translation**
  If the check box is selected, LSAs (Link State Advertisement) at the NSSA border router will be translated.

4.6.3.4 Areas

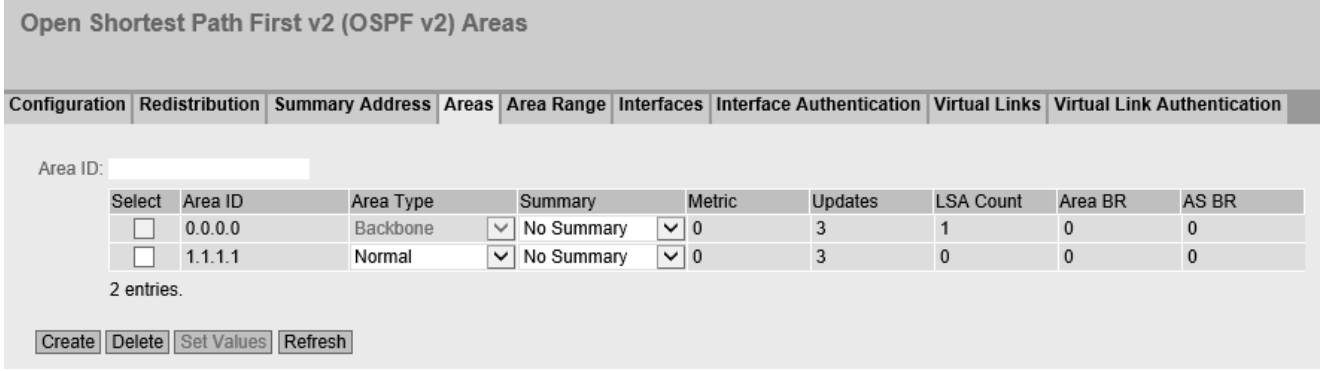
Overview

An Autonomous System can be divided into smaller areas.

On this page, you can view, create, modify or delete the areas of the router.

Note

This function is available only with layer 3.



Description of the displayed values

The page contains the following boxes:

- **Area ID**
  Enter the identifier of the area. The database is synchronized for all routers of an area. The area identifier must be unique in the network.
  The area identifier is a 32-bit number with the following format: x.x.x.x where x = 0 ... 255
  The area identifier 0.0.0.0 is reserved for the backbone area and cannot be deleted.

This table contains the following columns:

- **Select**
  Select the row you want to delete.
- **Area ID**
  Shows the identifier of the area.
- **Area Type**
  Select the area type in the drop-down list.
  - Standard
  - Stub
  - NSSA
- **Summary**
  Specify whether summary LSAs are generated for this area.
  - Summary: Summary LSAs are generated and sent to the area.
  - No Summary: Summary LSAs are not generated and sent to the area.
- **Metric**
  Displays the costs for the OSPFv2 interface.
- **Updates**
  Shows the number of recalculations of the routing tables.
- **LSA Count**
  Shows the number of LSAs in the database.
- **Area BR**
  Shows the number of reachable area border routers (ABR) within this area.
- **AS BR**
  Shows the number of reachable autonomous system border routers (ASBR) in this area.

Steps in configuration

1. Enter the ID for the area in the "Area ID" input box.
2. Click the "Create" button. A new entry is generated in the table.
3. Select the type of area, for example Stub in the "Area Type" drop-down list.
4. Select the "Summary LSA" entry in the "Summary" drop-down list.
5. Click the "Set Values" button.

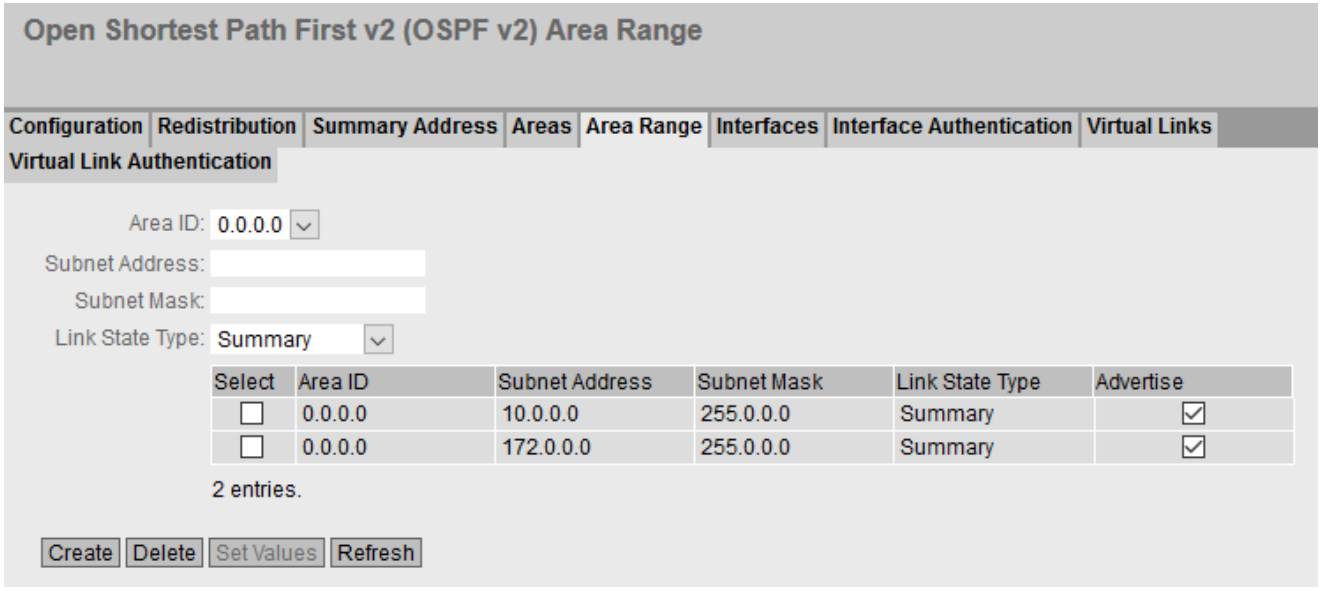
4.6.3.5 Area Range

Creating a new OSPFv2 area range

Using the "Create" button in the "OSPFv2 Area Range" menu, up to four networks can be grouped together under one area ID. The method is used only with area border routers. This means that an area border router only advertises one route for grouped areas to the outside.

Note

This function is available only with layer 3.



Description of the displayed boxes

The page contains the following boxes:

- **Area ID**
  Select the ID of the area from the drop-down list. You specify the ID on the "Areas" tab.
- **Subnet Address**
  Enter the IPv4 address of the network that will be grouped.
- **Subnet mask**
  Enter the subnet mask of the network that will be grouped.
- **Link State Type**
  - **Summary**
    Summary of routes within the areas in which OSPF is enabled.
  - **NSSA external**
    Inclusion of routes from a **N**ot **S**o **S**tubby **A**rea (LSA type 7) and conversion into LSA type 5.

The table contains the following columns:

- **Select**
  Select the row you want to delete.
- **Area ID**
  Shows the ID of the area.
- **Subnet Address**
  Shows the IP address of the network that will be grouped.
- **Subnet Mask**
  Shows the subnet mask of the network that will be grouped.
- **Link State Type**
  Shows which types of routes are summarized.
- **Advertise**
  Enable this option to advertise the grouped network.

Configuration procedure

1. Select the ID of the area from the drop-down list.
2. Enter the IP address of the network that will be grouped.
3. Enter the subnet mask of the network that will be grouped.
4. From the drop-down list, select which types of routes should be summarized.
5. Click the "Create" button. A new entry is generated in the table.
6. Enable the "Advertise" option to advertise the grouped network.
7. Click the "Set Values" button.

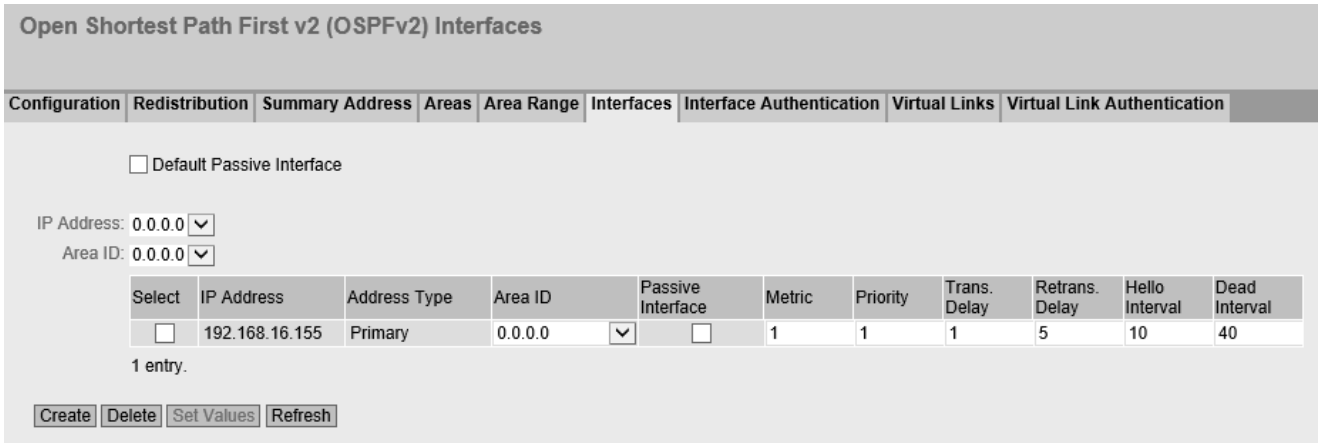
4.6.3.6 Interfaces

Overview

On this page, you can configure OSPFv2 interfaces.

Note

This function is available only with layer 3.



Description of the displayed boxes

The page contains the following boxes:

- **Default: Passive Interface**
  If this check box is selected, all newly created interfaces are created as passive interfaces.
- **IP Address**
  Select the IPv4 address of the OSPFv2 interface from the drop-down list.
- **Area ID**
  Select the ID of the area that is connected to the OSPFv2 interface from the drop-down list.

  Note

  For the secondary interface select the same Area ID as for the corresponding primary interface.
  The information whether an address type is primary or secondary can be found in the "Address Type" column on the "Layer 3 (IPv4) > Subnets > Overview" page.

Select the ID of the area that is connected to the OSPFv2 interface from the drop-down list.
The table has the following columns:

- **Select**
  Select the row you want to delete.
- **IP Address**
  Shows the IPv4 address of the OSPFv2 interface.
- **Address Type**
  There are two address types:
  - Primary
  - Secondary

  Cells for secondary addresses are grayed out and show the values of the associated primary address.
- **Area ID**
  Select the ID of the area that is connected to the OSPFv2 interface from the drop-down list.

- **Passive Interface**
  Specify the behavior of the interface:
  - Enabled
    No OSPFv2 information (e.g. Hello frames and LSDB updates) is sent via this interface and learned.
    All information that an interface learned before the option was enabled are retained in the LSDB. The information is deleted when the option is disabled or the interface is removed from the OSPF configuration.
  - Disabled
    OSPFv2 information is sent via this interface and learned.
- **Metric**
  Enter the costs for the OSPFv2 interface.
- **Priority**
  Enter the router priority. The priority is only relevant for selecting the designated router or designated border router. This parameter can be selected differently on routers within the same subnet.
  Range of values: 0 to 255
  Default setting: 1
- **Trans. Delay**
  Enter the required delay when sending a connection update.
  Range of values: 1 s to 3600 s
  Default setting: 1 s
- **Retrans. Delay**
  Enter the time after which an OSPFv2 packet is transferred again if no confirmation was received.
  Range of values: 1 s to 3600 s
  Default setting: 5 s
- **Hello Interval**
  Enter the interval between two Hello packets.
  Range of values: 1 s to 65,535 s
  Default setting: 10 s
- **Dead Interval**
  Enter the interval after which the neighbor router is marked as "failed" if no more Hello packets are received from it during this time.
  Default setting: 40 s

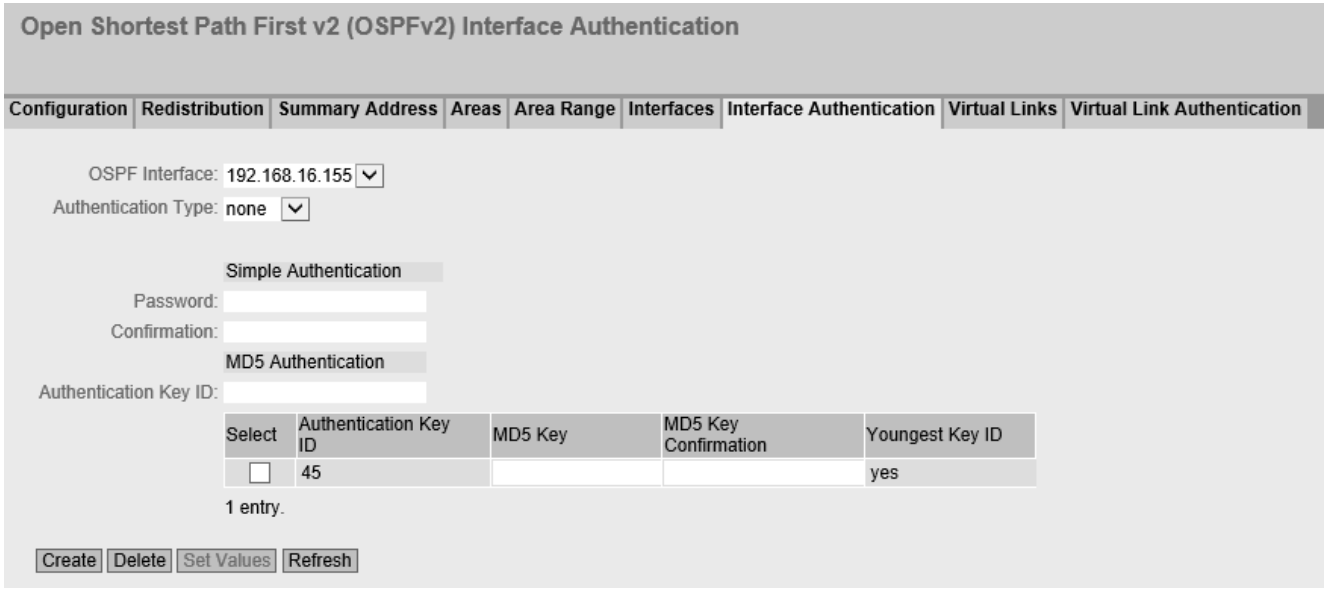
Configuration procedure

1. Select the IPv4 address of the OSPFv2 interface from the "IP Address" drop-down list.
2. Select the ID of the area with which the OSPFv2 interface is connected from the "Area ID" drop-down list.
3. Click the "Create" button. A new entry is generated in the table.
4. Make the required settings or use the factory defaults.
5. Click the "Set Values" button.

4.6.3.7 Interface Authentication

Configuring the interface authentication

On this page, you define the authentication of the interface.



Description of the displayed boxes

The page contains the following boxes:

- **OSPF interface**
  Select the OSPFv2 interface for which you want to configure authentication.
- **Authentication Type**
  Select the authentication method. You have the following options:
  - None
    No authentication
  - Simple
    Authentication using an unencrypted password
  - MD5
    Authentication using MD5

Section "Simple Authentication"

- **Password**
  Enter a password.
- **Confirmation**
  Confirm the entered password.

Section "MD5 Authentication"

- **Authentication Key ID**
  Enter the identifier of the MD5 authentication key.
  Enter the ID for MD5 authentication with which the password will be used as a key.
  Since the key ID is transferred with the protocol, the same key must be stored under the same key ID on all neighboring routers.

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **Authentication Key ID**
  Can only be edited if you set the MD5 authentication method. It is only possible to use several keys there.
- **MD5 Key**
  Enter the MD5 key.
- **MD5 Key Confirmation**
  Confirm the entered key.
- **Youngest Key ID**
  Shows whether or not the MD5 key is the latest key ID.

Configuration procedure

1. Select the OSPFv2 interface and the authentication method from the drop-down lists.
2. Enter the following data in the relevant input box:
   – Password and confirmation for simple authentication.
   – Authentication key ID for MD5 authentication
3. Click the "Create" button.
4. Enter the MD5 key and the confirmation of the MD5 key.
5. Click the "Set Values" button.

4.6.3.8 Virtual Links

Overview

Due to the protocol, each area border router must have access to the backbone area for protocol reasons. If a router is not connected directly to the backbone area, a virtual link to it is created.

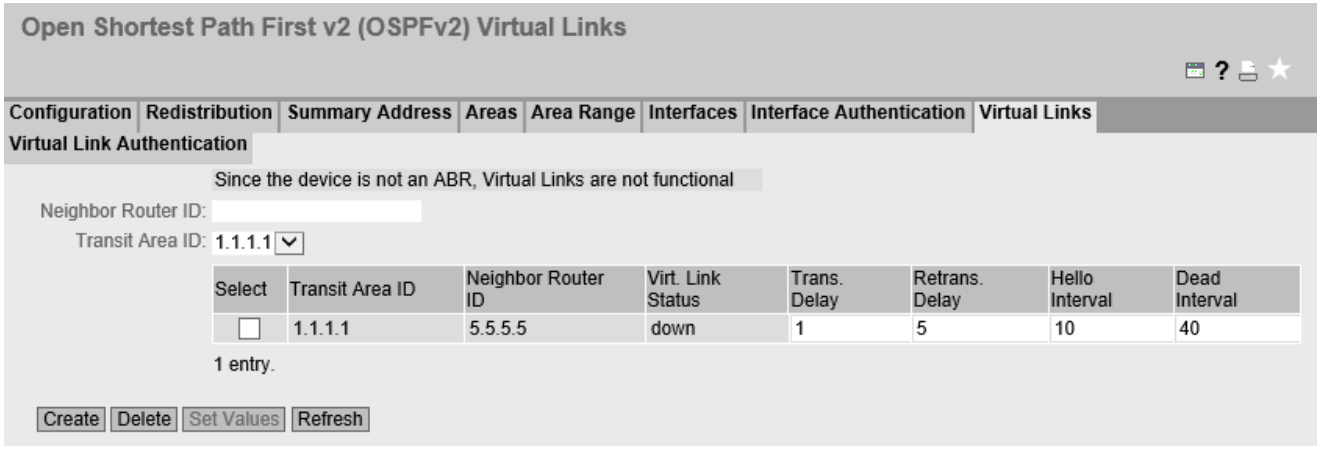
Note

This function is available only with layer 3.

Note

Note that when creating a virtual link both the transit area and the backbone area must already be configured.

A virtual link must be configured identically at both ends.



Description of the displayed boxes

The page contains the following note:

- **Since the device is not an ABR, Virtual Links are not functional**
  This note is displayed when at least one virtual link is configured and the device is not an area border router.

The page contains the following boxes:

- **Neighbor Router ID**
  Enter the ID of the neighbor router at the other end of the virtual connection.
- **Transit Area ID**
  Select the ID of the area that connects both routers from the drop-down list.

The table contains the following columns:

- **Select**
  Select the row you want to delete.
- **Transit Area ID**
  Shows the ID via which the two routers are connected.
- **Neighbor Router ID**
  Shows the ID of the neighbor router at the other end of the virtual connection.
- **Virt. Link Status**
  Specify the status of the virtual link. The following states are possible:
  - down: The virtual link is inactive.
  - point-to-point: The virtual link is active.

- **Trans. Delay**
  Enter the expected delay when sending a link update packet.
  Range of values: 1 s to 3600 s
  Default: 1 s
- **Retrans. Delay**
  Enter the time after which a packet is transferred again if no confirmation was received.
  Range of values: 1 s to 3600 s
  Default: 5 s
- **Hello Interval**
  Enter the interval between two Hello packets.
  Range of values: 1 s to 65,535 s
  Default: 10 s
- **Dead Interval**
  Enter the interval after which the neighbor router counts as "failed" if no more Hello packets are received from it during this time.
  Default setting: 40 s

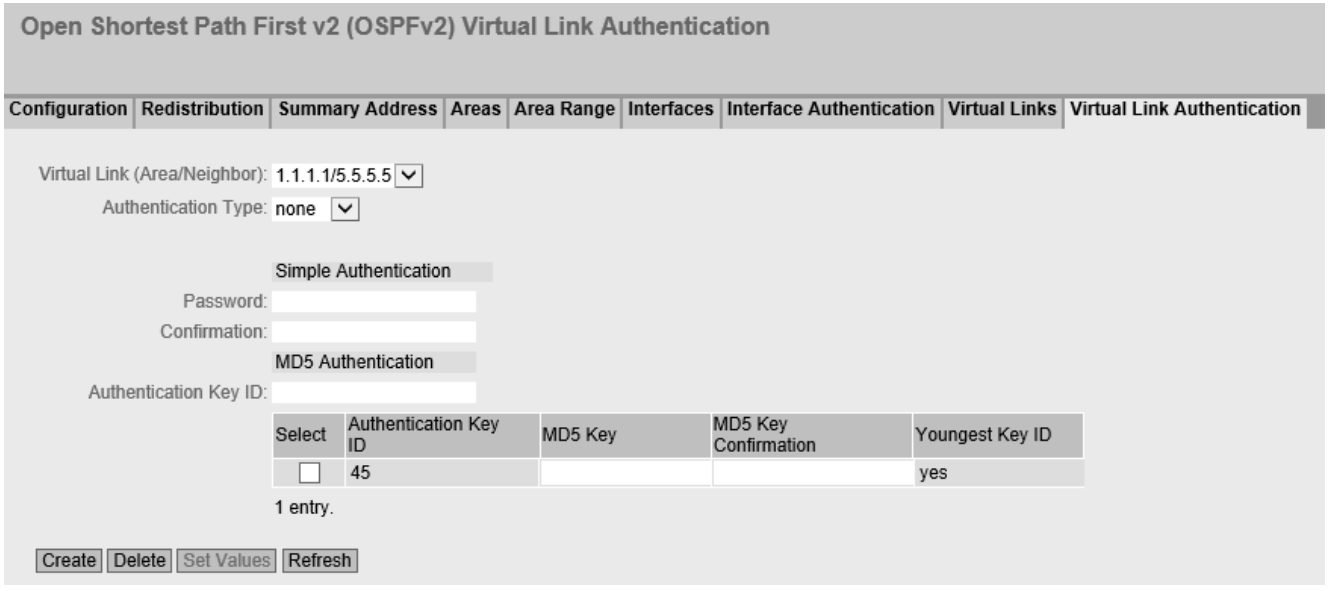
Configuration procedure

1. Enter the ID of the neighbor router at the other end of the virtual link in "Neighbor Router ID".
2. Select the area ID that connects the two routers from the "Transit Area ID" drop-down list.
3. Click the "Create" button. A new entry is generated in the table.
4. Enter the suitable values in "Transit Delay", "Retrans. Delay" and "Dead-Interval".
5. Click the "Set Values" button.

4.6.3.9 Virtual Link Authentication

Configuring the interface login

On this page, you define the authentication of the interface.



Description of the displayed boxes

The page contains the following boxes:

- **Virtual Link (Area/Neighbor)**
  Select the virtual link for which you want to configure authentication.
- **Authentication Type**
  Select the authentication method. You have the following options:
  - None
    No authentication
  - Simple
    Authentication using an unencrypted password
  - MD5
    Authentication using MD5

Section "Simple Authentication"

- **Password**
  Enter a password.
- **Confirmation**
  Confirm the entered password.

Section "MD5 Authentication"

- **Authentication Key ID**
  Enter the identifier of the MD5 authentication key.
  Enter the ID for MD5 authentication with which the password will be used as a key.
  Since the key ID is transferred with the protocol, the same key must be stored under the same key ID on all neighboring routers.

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **Authentication Key ID**
  Can only be edited if you set the MD5 authentication method. It is only possible to use several keys there.
- **MD5 Key**
  Enter the MD5 key.
- **MD5 Key Confirmation**
  Confirm the entered key.
- **Youngest Key ID**
  Shows whether or not the MD5 key is the latest key ID.

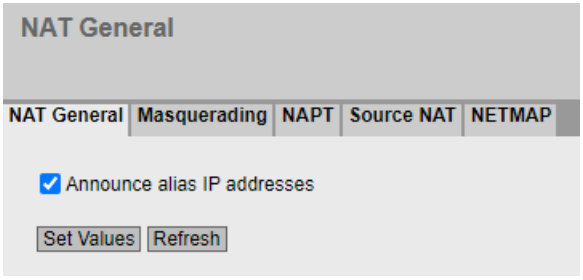
Configuration procedure

1. Select the virtual connection and the authentication method from the drop-down lists.
2. Enter the following data in the relevant input box:
   – Password and confirmation for simple authentication.
   – Authentication key ID for MD5 authentication
3. Click the "Create" button.
4. Enter the MD5 key and the confirmation of the MD5 key.
5. Click the "Set Values" button.

4.6.4 NAT

4.6.4.1 NAT General

On this WBM page, you enable Gratuitous ARP for alias IP addresses.



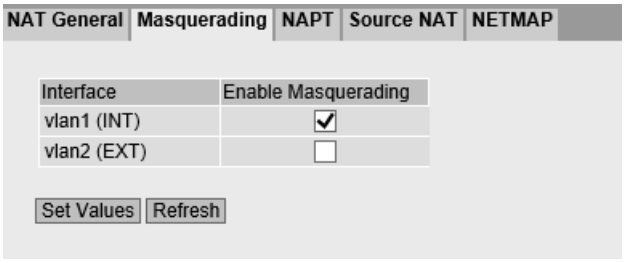
Description

On this page, you can enable the following option:

- **Announce alias IP addresses**
  When the option is enabled, a Gratuitous ARP is sent for each alias IP address. This announces the IP address in the network, and the other devices can update their ARP cache. The Gratuitous ARP is only sent at the time of configuration, that is, during device startup or when an NAT rule (NETMAP) is being configured.

4.6.4.2 Masquerading

On this WBM page, you enable the rules for IP masquerading.



Description

The table has the following columns:

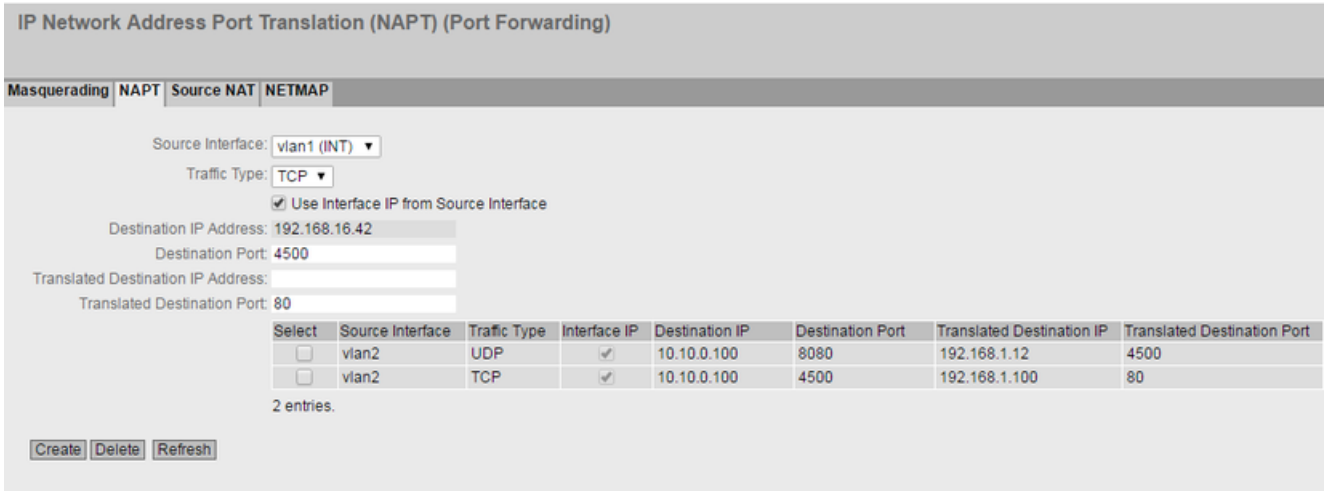
- **Interface**
  Interface to which the setting relates. Only interfaces with configured subnets are available.
- **Enable Masquerading**
  When enabled, with each outgoing data packet sent via this interface, the source IP address is replaced by the IP address of the interface.

4.6.4.3 NAPT

On this WBM page, you can configure a port translation in addition to the address translation.

The following port translations are possible:

- From a single port to the same port:
  If the ports are the same, the frames will be forwarded without port translation.
- From a single port to a single port
  The frames are translated to the port.
- From a port range to a single port
  The frames from the port range are translated to the same port (n:1).
- From a port range to the same port range
  If the port ranges are the same, the frames will be forwarded without port translation.



Description

The page contains the following boxes:

- **Source Interface**
  Select the interface at which the queries will arrive.
- **Traffic Type**
  Specify the protocol for which the address assignment is valid.
- **Use Interface IP from Source Interface**
  When enabled, the IP address of the selected interface is used for "Dest. IP Address".
- **Destination IP Address**
  Enter the destination IP address. The frames are received at this IP address. Can only be edited if "Use Interface IP from Source Interface" is disabled.
- **Destination Port**
  Enter the destination port. Incoming frames with this port as the destination port are forwarded. If the setting is intended to apply to a port range, enter the range with start port "-" end port, for example 30 - 40.

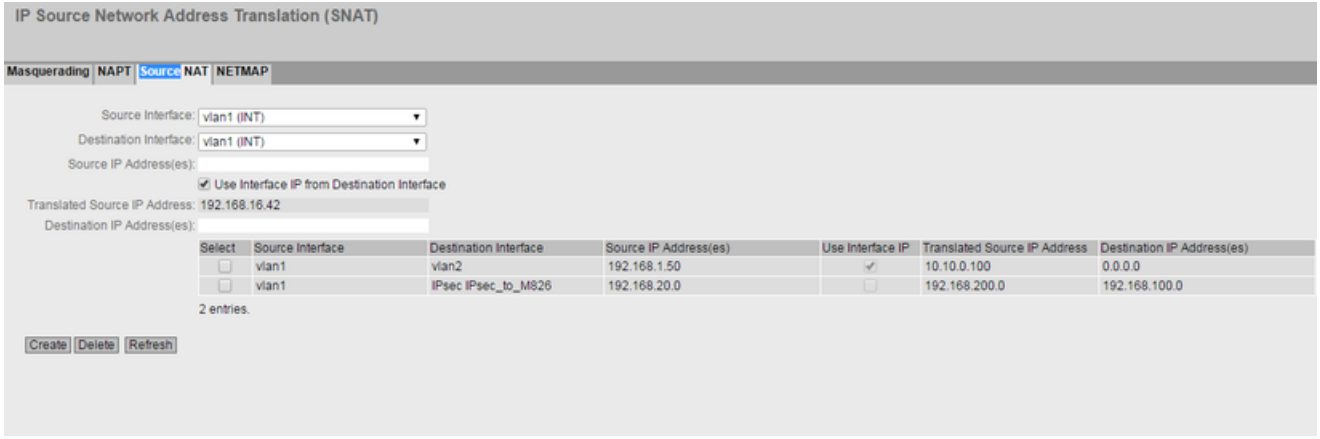
- **Translated Destination IP**
  Enter the IP address of the node to which this frame will be forwarded.
- **Translated Destination Port**
  Enter the number of the port. This is the new destination port to which the incoming frame will be forwarded. If the setting is intended to apply to a port range, enter the range with start port "-" end port, for example 30 - 40.

The table has the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **Source Interface**
  Shows the interface from which the packets need to come. Only these packets are considered for port forwarding.
- **Traffic Type**
  Shows the protocol for which the address assignment applies.
- **Interface IP**
  Shows whether the IP address of the interface is used.
- **Destination IP**
  Shows the destination IP address. The frames are received at this IP address.
- **Destination Port**
  Shows the destination port. Incoming frames with this port as the destination port are forwarded.
- **Translated Destination IP**
  Shows the IP address of the node to which the packets will be forwarded.
- **Translated Destination Port**
  Shows the destination port to which the packets are translated.

4.6.4.4 Source NAT

On this WBM page, you configure the rules for source NAT.



Note

Firewall rule with source NAT

Address translation with source NAT is only performed after the firewall; the non-translated addresses are therefore used.

Security > Firewall > IP rules

- Source (Range): Input from "Source IP Addresses"
- Destination (Range): Input from "Destination IP Addresses"

Description

- **Source Interface / Destination Interface**
  Specify the direction of the connection establishment. Only connections established in this specified direction are taken into account.
  The virtual interfaces of VPN connections can also be selected:
  - VLANx: VLANs with configured subnet
  - SINEMA RC: Connection to SINEMA RC Server
  - IPsec: Either all IPsec VPN connections (all) or a specific IPsec VPN connection

  Note

  When you configure a NAT address translation to or from the direction of the VPN tunnel, only the IP addresses involved in the NAT address translation rules can be reached via the VPN tunnel.

- **Source IP Address(es)**
  Specify the source IP addresses for which this source NAT rule is valid. Only the packets that correspond to the addresses entered are taken into account.
  The following entries are possible:
  - IP address: Applies precisely to the specified IP address.
  - IP address range: Applies to a certain IP address range: Start IP address "-" End IP address, e.g. 192.168.100.10 - 192.168.100.20
  - IP subnet: Applies to several IPv4 addresses grouped together to form an IP address range: IP address/number of bits of the network part (CIDR notation)
- **Use Interface IP from Destination Interface**
  When enabled, the IP address of the selected destination interface is used with "Translated Source IP Address".

- **Translated Source IP Address**
  Enter the IP address with which the IP address of the sender is replaced. Can only be edited if "Use Interface IP from Destination Interface" is disabled.
- **Destination IP Address(es)**
  Specify the destination IP addresses for which this source NAT rule is valid. Only the packets whose destination IP address is in the range of entered addresses are taken into account.
  - IP address: Applies precisely to the specified IP address.
  - IP address range: Applies to a certain IP address range: Start IP address "-" End IP address, e.g. 192.168.100.10 - 192.168.100.20
  - IP subnet: Applies to several IPv4 addresses grouped together to form an IP address range: IP address/number of bits of the network part (CIDR notation)

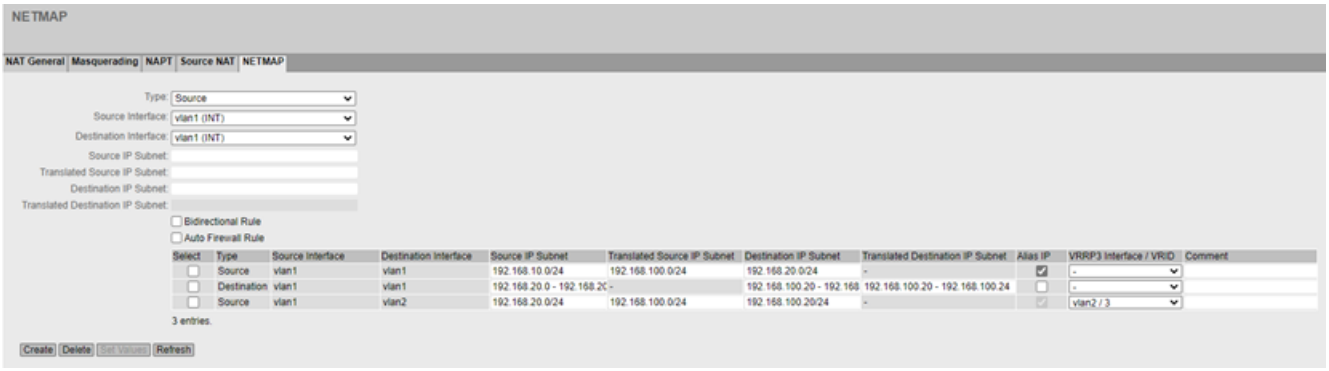
The table has the following columns:

- Select
  Activate the check box in the row to be deleted.
- Source Interface
  Shows the source interface.
- Destination Interface
  Shows the destination interface.
- Source IP Address(es)
  Shows the IP addresses of the senders for which address translation is required.
- Use Interface IP
  Shows whether the IP address of the selected destination interface is used in "Translated Source IP Address".
- Translation Source IP Address
  Shows the IP address with which the IP address of the sender is replaced.
- Destination IP Address(es)
  Shows the IP addresses of the receivers for which address translation is required.

4.6.4.5 NETMAP

On this WBM page, you specify the rules for NETMAP. NETMAP is static 1:1 mapping of network addresses.

For more detailed information, refer to the section "NAT and firewall (Page 66)".



Note

Firewall rule with source NAT

Address translation with source NAT is only performed after the firewall; the non-translated addresses are therefore used.

Security > Firewall > IP rules

- Source (Range): Input from "Source IP Subnet"
- Destination (Range): Input from "Destination IP Subnet"

Firewall rule with destination NAT

Address translation with NAT was already performed before the firewall; the translated addresses are therefore used in the firewall.

Security > Firewall > IP rules

- Source (Range): Input from "Source IP Subnet"
- Destination (Range): Input from "Translated Destination IP Subnet"

Description

- **Type**
  Specify the type of address translation.
  - Source: Replacement of the source IP address
  - Destination: Replacement of the destination IP address
- **Source Interface**
  Specify the source interface.
  - VLANx: VLANs with configured subnet
  - SINEMA RC: Connection to SINEMA RC Server
  - IPsec: Either all IPsec VPN connections (all) or a specific IPsec VPN connection

- **Destination Interface**
  Specify the destination interface.
  - VLANx: VLANs with configured subnet
  - SINEMA RC: Connection to SINEMA RC Server
  - IPsec: Either all IPsec VPN connections (all) or a specific IPsec VPN connection
- **Source IP Subnet**
  Enter the subnet of the sender.
  The subnet can also be a single PC or another subset of the subnet. Use the CIDR notation, for example, 192.168.10.10/32.
  You can also specify the IP range with the start address "-" end address, e.g., 192.168.100.10 - 192.168.100.20.
  For the entire IP range, enter "*".
- **Translated Source IP Subnet**
  Enter the subnet with which the subnet of the sender will be replaced. Can only be edited in the "Source" settings.
  The subnet can also be a single PC or another subset of the subnet. Use the CIDR notation, for example, 192.168.10.10/32.
  You can also specify the IP range with the start address "-" end address, e.g., 192.168.100.10 - 192.168.100.20.
  For the entire IP range, enter "*".
- **Destination IP Subnet**
  Enter the subnet of the receiver.
  The subnet can also be a single PC or another subset of the subnet. Use the CIDR notation, for example, 192.168.10.10/32.
  You can also specify the IP range with the start address "-" end address, e.g., 192.168.100.10 - 192.168.100.20.
  For the entire IP range, enter "*".
- **Translated Destination IP Subnet**
  Enter the subnet with which the subnet of the receiver will be replaced. Can only be edited with the setting "Destination".
  The subnet can also be a single PC or another subset of the subnet. Use the CIDR notation, for example, 192.168.10.10/32.
  You can also specify the IP range with the start address "-" end address, e.g., 192.168.100.10 - 192.168.100.20.
  For the entire IP range, enter "*".
- **Bidirectional rule**
  When this is enabled, the NETMAP rule for the opposite direction is automatically created when the NETMAP rule is created.
  The NETMAP rules are not connected to one another after creation. This means no synchronization of the NETMAP rules when they are changed or deleted.
- **Auto Firewall Rule**
  When this is enabled, the corresponding firewall rule is automatically created when the NETMAP rule is created. These firewall rules are displayed under "Security > Firewall > IP rules". If you change or delete the NETMAP rules, the corresponding firewall rules are adjusted or deleted.

The table has the following columns:

- Select
  Select the check box in the row to be deleted.
- Type
  Shows the direction of the address translation.
- Source Interface
  Shows the source interface.
- Destination Interface
  Shows the destination interface.
- Source IP Subnet
  Shows the subnet of the sender.
- Translated Source IP Subnet
  Shows the subnet of the sender with which the subnet of the sender is replaced.
- Destination IP Subnet
  Shows the subnet of the receiver.
- Translated Destination IP Subnet
  Shows the subnet of the receiver with which the subnet of the receiver is replaced.
- Alias IP
  When enabled, Alias IP addresses are created for the implemented address range. Enabled automatically when a /32 address is entered.
  - Source: For all IP addresses entered in the "Translated Source IP Subnet" field, Alias IP addresses are created at the "Destination Interface".
  - Destination: For all IP addresses entered in the "Destination IP Subnet" field, Alias IP addresses are created at the "Source Interface".

  Note

  Enabling in combination with network or address range

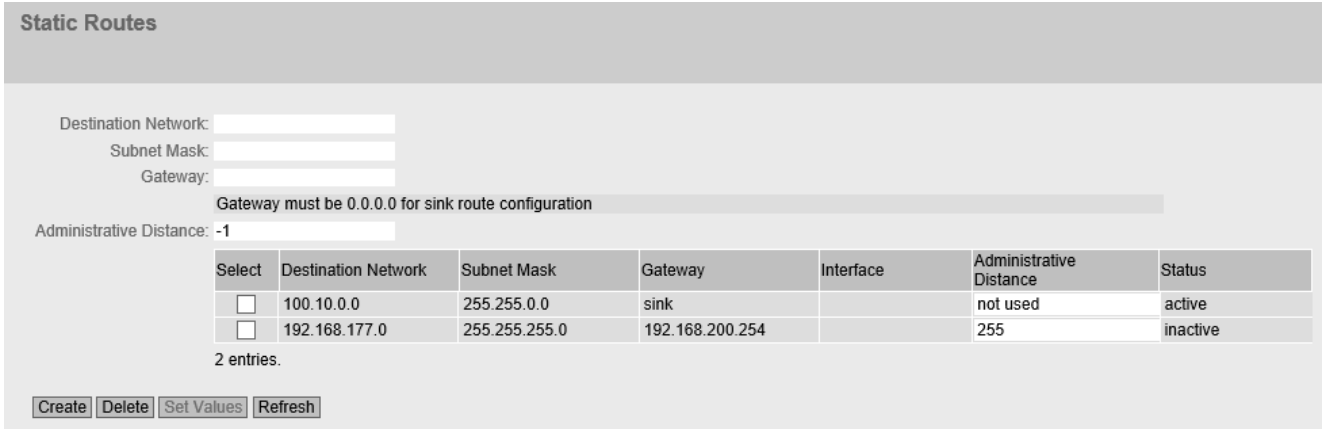
  When you enable the option in combination with a network or address range, the Alias IP addresses are reserved for the entire network or address range. This can lead to network problems.

- VRRP Interface / VRID
  Selection is only possible when the "Alias IP" option is enabled.
  Shows all configured routers of the type "VRRPv3" that are created in the "Layer 3 > VRRPv3 > Router" menu.
  When you select a VRRP3 router, the Alias IP address associated with this NETMAP rule is only active when the VRRP3 router has the router status "Master".
- Comment
  If needed, enter a comment.

4.6.5 Static Routes

Static route

On this page, you create the static IPv4 routes.



Description

The page contains the following boxes:

- **Destination Network**
  Enter the network address of the destination that can be reached via this route.
- **Subnet Mask**
  Enter the corresponding subnet mask.
- **Gateway**
  Enter the IPv4 address of the gateway via which this network address is reachable.
- **Administrative Distance**
  Enter the administrative distance for the route. The administrative distance corresponds to the quality of a connection, based for example on speed or costs. If there are several equal routes, the route with the lowest value is used.
  As default -1 is set. This setting means that the metric is not set.
  Range of values: 1 - 255

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **Destination Network**
  Shows the network address of the destination.
- **Subnet Mask**
  Shows the corresponding subnet mask.
- **Gateway**
  Shows the IPv4 address of the next gateway.

- **Interface**
  Shows the interface of the route.
- **Administrative Distance**
  Enter the administrative distance for the route. When creating the route, "not used" is entered automatically (value -1). The administrative distance corresponds to the quality of a connection, based for example on speed or costs. If there are several equal routes, the route with the lowest value is used.
  Range of values: 1 - 255
- **Status**
  Shows whether or not the route is active.

Configuration procedure

1. Enter the network address of the destination in the "Destination Network" input box.
2. Enter the corresponding subnet mask in the "Subnet Mask" input box.
3. Enter the gateway in the "Gateway" input box.
4. Enter the weighting of the route in "Administrative Distance".
5. Click the "Create" button. A new entry is generated in the table.
6. Click the "Set Values" button.

4.6.6 VRRPv3

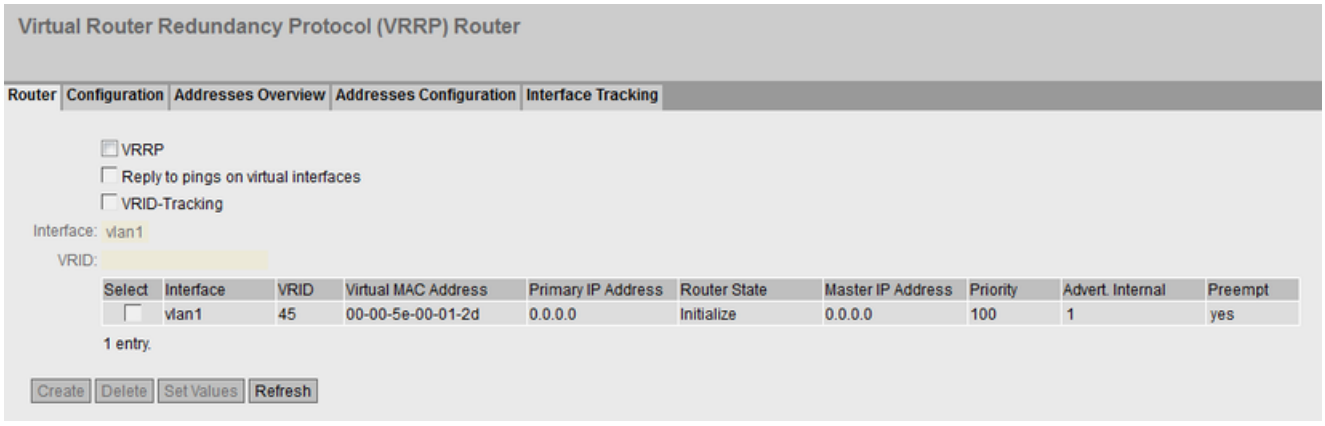
4.6.6.1 Router

Introduction

Using the "Create" button, you can create new virtual routers. A maximum of 16 virtual routers can be configured. You can configure other parameters on the "Configuration" tab.

Note

- You can use VRRPv3 on VLAN interfaces.



Requirement

For the incoming packets to be forwarded to the device, enable the predefined IPv4 rule "VRRP".

Description of the displayed values

The page contains the following boxes:

- **VRRPv3**
  Enable or disable routing using VRRPv3.
- **Reply to pings on virtual interfaces**
  When enabled, the virtual IPv addresses also reply to the ping.
- **VRID-Tracking**
  Enable or disable VRID tracking.
  When enabled, all VRRP instances are monitored. If the status of a VRRP instance changes to "Initialize", the priority of all VRRP instances is reduced to the value "1".
  If the status of the VRRP instance changes, the original priority of all VRRP instances is restored.
- **Interface**
  Select the VLAN Interface that functions as the virtual router from the drop-down list.
- **VRID**
  Enter the ID of the virtual router in the input box. This ID defines the group of routers that form a virtual router (VR). In the group, this is the same. It can no longer be used for other groups.
  Valid values are 1.. 255.

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **Interface**
  Shows the interface that functions as the virtual router.
- **VRID**
  Shows the ID of the virtual router.

- **Virtual MAC Address**
  Shows the virtual MAC address of the virtual router.
- **Primary IP Address**
  Shows the numerically lowest IPv4 address in this VLAN. The entry 0.0.0.0 means that the "Primary" address on this VLAN is used. Otherwise, all IPv4 addresses configured on this VLAN in the "Layer 3 > Subnets" menu are valid values.
- **Router State**
  Shows the current status of the virtual router. Possible values are:
  - Master
    The router is the Master router and handles the routing functionality for all assigned IP addresses.
  - Backup
    The router is the backup router. If the master router fails, the backup router takes over the tasks of the master router.
  - Initialize
    The virtual router has just been turned on. It will soon change to the "Master" or "Backup" state.
- **Master IP Address**
  Shows the IPv4 address of the master router.
- **Priority**
  Shows the priority of the virtual router.
  Valid values are 1-254.
  If an IPv4 address is assigned to the VRRP router that is also actually configured on the local IPv4 interface, the value 255 is entered automatically. All other priorities can be distributed freely among the VRRP routers. The higher the priority, the earlier the VRRP router becomes "Master".
- **Advert. Interval**
  Shows the interval at which the master router sends VRRP packets.
- **Preempt**
  Shows the precedence of a router when changing roles between backup and master.
  - yes
    This router has precedence when changing roles.
  - no
    This router does not have precedence when changing roles.

VRRP and DHCP server

If you want to operate a DHCP server on the devices of a VRRP group, the DHCP server must be configured on the master router. Backup routers do not react to DHCP queries. Make sure that the master router is statically configured and that after a failure, becomes the master of the VRRP group again.

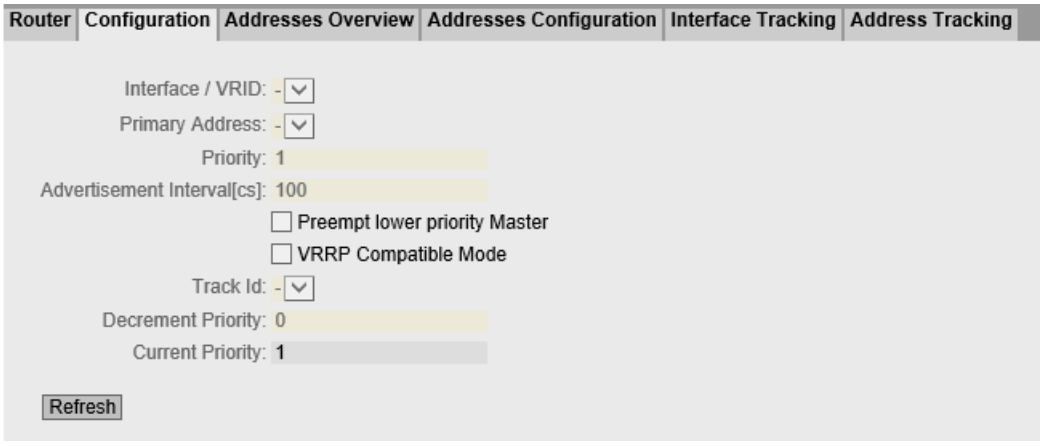
Steps in configuration

1. Select the "VRRPv3" check box.
2. Select the required interface.
3. Enter the ID of the virtual router in the "VRID" input box.
4. Click the "Create" button. A new row is inserted in the table.
5. Select the "Reply to pings on virtual interfaces" check box so that virtual addresses reply to pings as well.
6. Select the "VRID Tracking" check box to monitor the VRID.
7. Click the "Set Values" button. To configure the virtual router, click on the "Configuration" tab.

4.6.6.2 Configuration

Introduction

On this page, you configure the virtual router.



Description of the displayed values

The page contains the following boxes:

- **Interface / VRID**
  Select the ID of the virtual router you are configuring from the drop-down list.
- **Primary address**
  Select the primary IPv4 address. If the router becomes master router, the router uses this IPv4 address.

  Note

  If you only configure one subnet on this VLAN, no entry is necessary. The entry is then 0.0.0.0.
  If you configure more than one subnet on the VLAN and you want a specific IPv4 address to be used as the source address for VRRP packets, select the IPv4 address from the drop-down list. Otherwise, the numerically lowest IPv4 address will be used.

- **Priority**
  Enter the priority of this virtual router. Valid values are 1-254.
  If an IPv4 address is assigned to the VRRP router that is also actually configured on the local IPv4 interface, the value 255 is entered automatically. All other priorities can be distributed freely among the VRRP routers. The higher the priority, the earlier the VRRP router becomes "Master".
- **Advertisement Interval**
  Enter the interval in seconds after which a master router sends a VRRP packet again.
- **Preempt lower priority Master**
  Allow the precedence when changing roles between backup and master based on the selection process.
- **VRRP Compatible Mode**
  When enabled, the VRRPv3 router sends and receives VRRPv2 frames in addition to VRRPv3 frames for configured IPv4 addresses. Only necessary when not all VRRP routers support VRRPv3.
- **Track ID**
  Select a track ID.
- **Decrement Priority**
  Enter the value by which the priority of the VRRP interface will be reduced.
- **Current Priority**
  Shows the priority of the VRRP interface after the monitored interface has changed to the "down" status.

Steps in configuration

To configure a virtual router as the master router, follow the steps below:

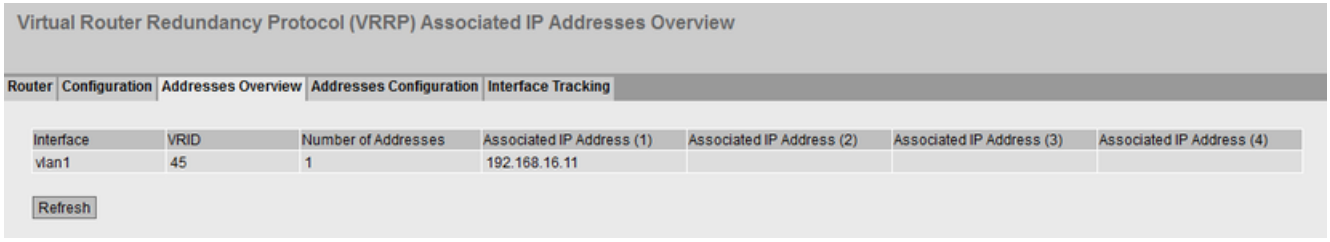
1. Select the ID of the virtual router you want to configure from the "Interface / VRID" drop-down list.
2. Select the source address from the "Primary IP Address" drop-down list.
3. Select the "Master" check box.

4. From the "Priority" drop-down list, enter the priority of this virtual router.
5. Enter the interval in "Advertisement Interval".
6. Select the "Preempt lower priority Master" check box.
7. Select a track ID.
8. Value by which the priority of the VRRP interface will be reduced
9. Click the "Set Values" button.

4.6.6.3 Addresses Overview

Overview

This page shows which IPv4 addresses are monitored by the virtual router. Each virtual router can monitor one IPv4 address.



Description of the displayed boxes:

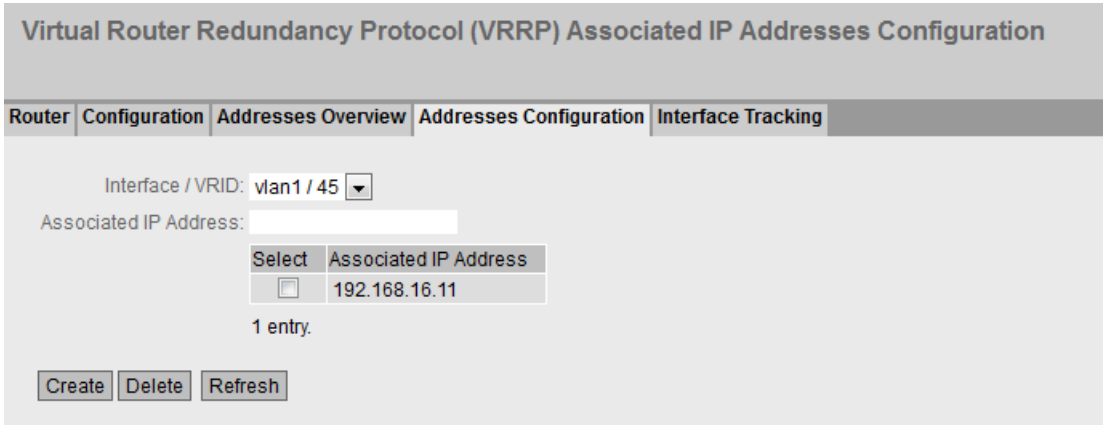
The table has the following columns:

- **Interface**
  Shows the interface that functions as the virtual router.
- **VRID**
  Shows the ID of this virtual router.
- **Number of addresses**
  Shows the number of IPv4 addresses.
- **Assigned IP address (1) ... Assigned IP address (4)**
  Shows the router IPv4 addresses monitored by this virtual router. If a router takes over the role of master, the routing function is taken over by this router for all these IPv4 addresses.

4.6.6.4 Address Configuration

Creating or changing the assigned IPv4 addresses

On this page, you can create, modify or delete the IPv4 addresses to be monitored. Each virtual router can monitor one IPv4 address.



Description of the displayed values

The page contains the following boxes:

- **Interface / VRID**
  Select the virtual router from the drop-down list.
- **Associated IP address**
  Enter the IPv4 address that the virtual router will monitor.

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **Associated IP Address**
  Shows the IPv4 addresses that the virtual router monitors.

Configuration procedure

1. Select the ID of the virtual router from the "Interface / VRID" drop-down list.
2. Enter the IPv4 address that the virtual router will monitor.
3. Click the "Create" button. A new entry is generated in the table.

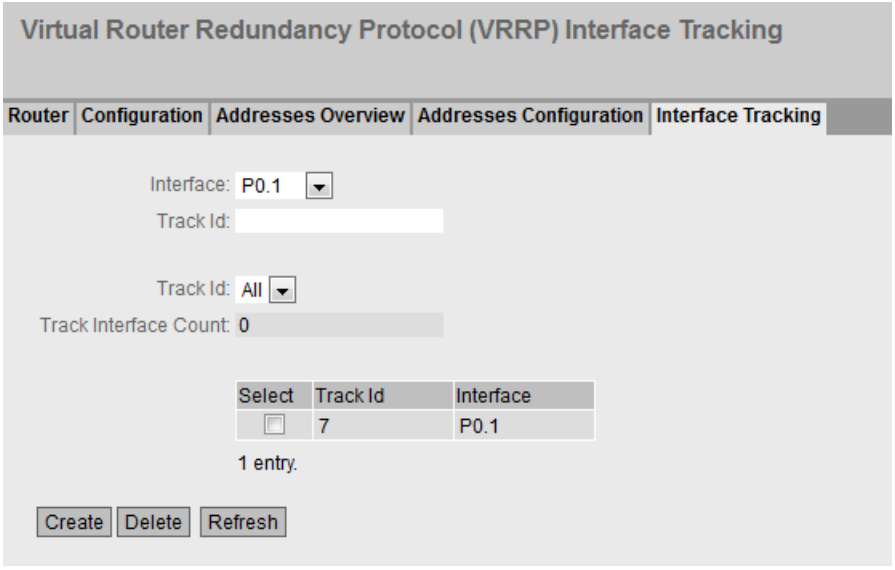
4.6.6.5 Interface Tracking

Introduction

On this page, you configure the monitoring of interfaces.

When the link of a monitored interface changes from "up" to "down", the priority of the assigned VRRP interface is reduced. You configure the value by which the priority is reduced on the page "Layer 3 > VRRPv3 > Configuration".

When the link of the interface changes back from "down" to "up", the original priority of the VRRP interface is restored.



Description of the displayed values

The page contains the following boxes:

- **Interface**
  From the drop-down list, select the interface to be monitored.
- **Track ID**
  Enter a track ID.
- **Track ID**
  Select a track ID.
- **Track Interface Count**
  Enter how many monitored interfaces need to change to the "down" status, before the priority is changed.

The table has the following columns:

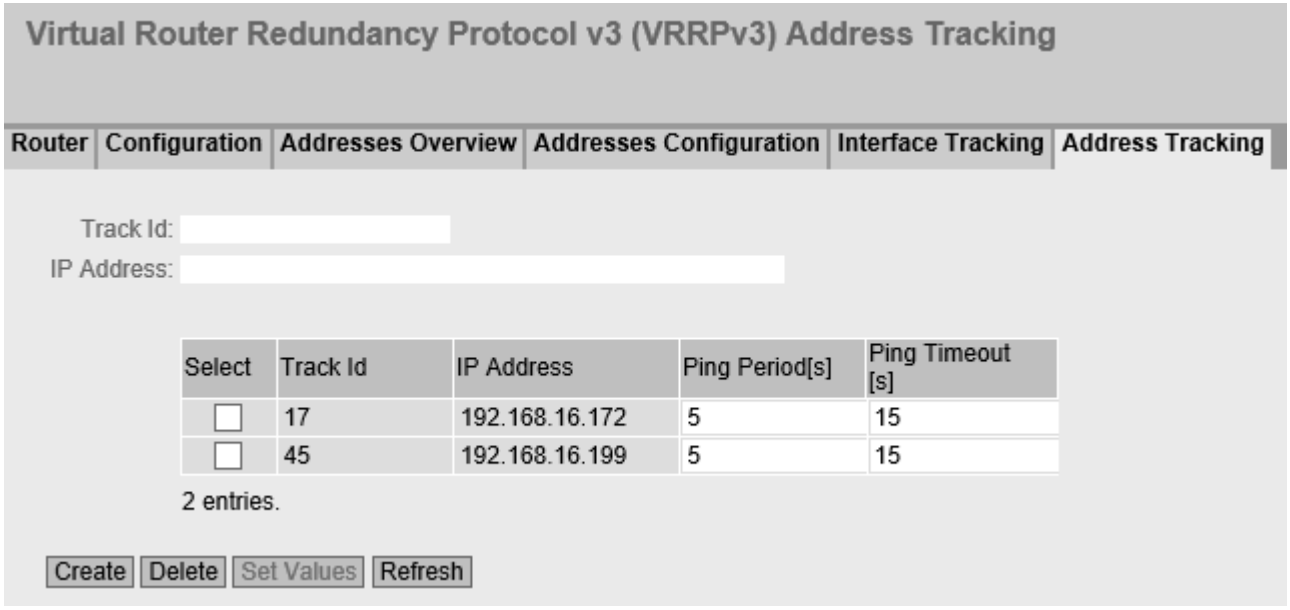
- **Select**
  Select the check box in the row to be deleted.
- **Track ID**
  Shows the track ID.
- **Interface**
  Shows the interface that is being monitored.

Steps in configuration

1. Select the required interface from the "Interface" drop-down list.
2. In the "Track ID" box, enter the required ID.
3. Click the "Create" button.
4. Select an ID from the "Track-ID" drop-down list:
5. In the "Track Interface Count" enter the number of interfaces.
6. Click the "Set Values" button.
7. Link the monitoring to a VRRP interface in the "Configuration" tab.

4.6.6.6 Address tracking

You configure the monitoring of IPv4 addresses on this page. The router sends a ping request to each of the configured IPv4 addresses within the specified time period. If no response is received within a specified time period, the VRRP priority of the corresponding interface is reduced.



Description

The page contains the following boxes:

- **Track ID**
  Enter the track ID.
- **IP Address**
  Enter the IPv4 address to be monitored. You can enter a maximum of five IPv4 addresses.

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **Track ID**
  Shows the track ID.
- **IP Address**
  Show the IPv4 address to be monitored.
- **Ping Period**
  Shows the cycle time in seconds between two ping requests.
- **Ping Timeout**
  Shows the time in seconds that the router waits for a ping response. The minimum duration is three times the ping period.

Procedure

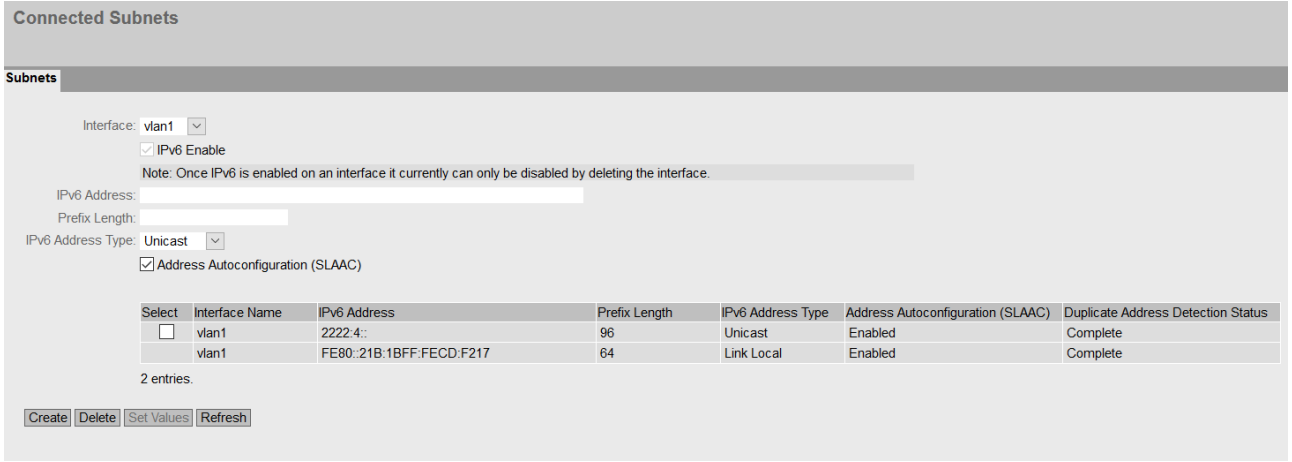
1. In the "Track ID" box, enter the required ID.
2. In the "IPv4 Address" field, enter the IPv4 address that the virtual router is to monitor.
3. Click the "Create" button. A new entry is generated in the table.

4.7 Menu "Layer 3 (IPv6)"

4.7.1 Subnets

Connected Subnets

On this page, you can enable IPv6 on the interface. The interface is also called an IPv6 interface. An IPv6 interface can have several IPv6 addresses.



Description

The page contains the following:

- **Interface**
  Select the IP interface on which IPv6 will be enabled.
- **IPv6 Enable**
  Enable or disable IPv6 on the interface.

  Note

  Disabling IPv6

  If IPv6 is enabled on an interface, you can only disable IPv6 by deleting interface.

- **IPv6 Address**
  Enter the IPv6 address. The entry depends on the selected address type.
- **Prefix Length**
  Enter the number of left-hand bits belonging to the prefix.
- **IPv6 Address Type**
  Select the address type.
  - Unicast
  - Anycast
  - Link Local: IPv6 address is only valid on the link
- **Address Autoconfiguration (SLAAC)**
  Enable or disable the SLAAC (Stateless Address Auto Configuration) mechanism for the address configuration.
  If SLAAC is enabled, there will be stateless auto configuration via NDP (Neighbor Discovery Protocol).

The table has the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **Interface Name**
  Shows the name of the interface.
- **IPv6 Address**
  Shows the IP address of the subnet.
- **Prefix Length**
  Shows the prefix length.

- **IPv6 Address Type**
  Displays the address type. The following values are possible:
  - Unicast
  - Anycast
  - Link Local
- **Duplicate Address Detection Status**
  In Address Autoconfiguration (SLAAC), the "Duplicate Address Detection Status" function prevents IPv6 addresses from being assigned twice. The device can only use free IPv6 addresses during autoconfiguration.
  When the function is enabled, the check via NDP takes place automatically.

  Note

  The function does not run a cyclic check.

  This column shows the current status of the function. The following values are possible:
  - **Tentative**
    This status indicates that the selected IPv6 address is being checked. The device sends a neighbor solicitation message to the selected IPv6 address.
  - **Conflict**
    This status indicates that the IPv6 address is already being used. In this case, a neighbor advertisement message with the selected IPv6 address is returned to the device.
  - **Complete**
    This status indicates that the selected IPv6 address can be used. In this case, the device did not receive feedback within a period of time and assumes that the IPv6 address is not yet assigned.
  - **Down**
    This status indicates that the interface is not active. No check is carried out.

Procedure

Automatically form link local address

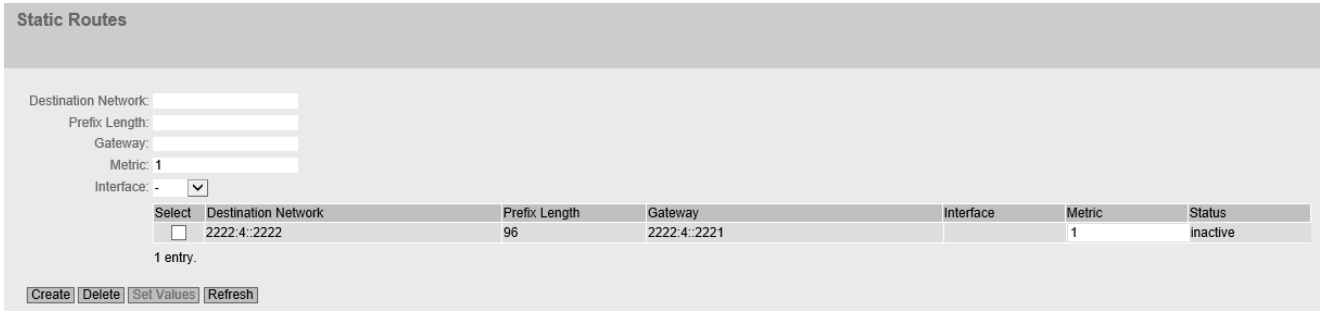
1. Select the required interface.
2. Enable IPv6.
3. Click the "Create" button. In the table an entry with the interface is created and the automatically formed IPv6 address is displayed.

Assign link-local address

1. Select the required interface.
2. Enable IPv6.
3. In "IPv6 Address" enter the link local address, e.g. FE80::21B:1BFF:FE40:9155
4. Enter "64" in "Prefix Length".
5. For "IPv6 Address Type" select the entry "Link Local".
6. Click the "Create" button. In the table an entry with the interface is created and the IPv6 address is displayed.

4.7.2 Static Routes

On this page, you configure static IPv6 routes.



Description

The page contains the following:

- **Destination Network**
  Enter the network address of the destination that can be reached via this route.
- **Prefix Length**
  Enter the number of left-hand bits belonging to the prefix.
- **Gateway**
  Enter the IPv6 address of the gateway via which this network address is reachable.
- **Metric**
  Enter the metric for the route. The metric corresponds to the costs of a connection. If there are several equal routes, the route with the lowest value is used.
  Range of values: 1 - 254
- **Interface**
  Specify the interface via which the network address of the destination is reached.

The table contains the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **Destination Network**
  Shows the network address of the destination.
- **Prefix Length**
  Shows the prefix length.
- **Gateway**
  Shows the IPv6 address of the next gateway.
- **Interface**
  Shows the Interface of the route.

- **Metric**
  Enter the metric for the route. When creating the route, "not used" is entered automatically. The metric corresponds to the quality of a connection, based for example on speed or costs. If there are several equal routes, the route with the lowest value is used.
  Range of values: 1 - 254
- **Status**
  Shows whether or not the route is active.

Configuration procedure

1. Enter the network address of the destination.
2. Enter the prefix length.
3. Enter the IPv6 address of the gateway.
4. Select the required interface.
5. Enter the administrative distance of the route.
6. Click the "Create" button. A new entry is generated in the table.
7. Click the "Set Values" button.

4.8 "Security" menu

4.8.1 Users

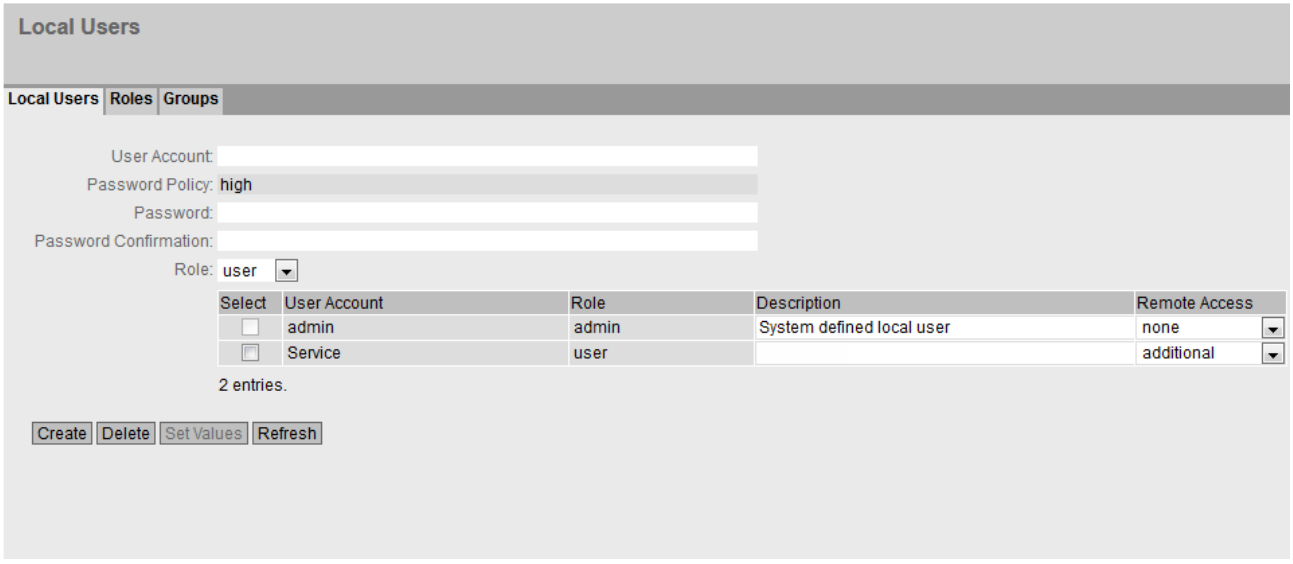
4.8.1.1 Local Users

User accounts

On this page, you create local user accounts with the corresponding rights. To be able to create a user account, the logged in user must have the "admin" role.

Note

You can create up to 30 additional user accounts.



Restrictions

The following characters are generally not permitted:

- | ; : ? "
- The characters coded with the ASCII value as of 128 (extended ASCII code)
- The characters for Space and Delete

Description

The page contains the following:

- **Account**
  Enter the name for the user. The name must meet the following conditions:
  - It must be unique.
  - It must be between 1 and 250 characters long.

  Note

  User name cannot be changed

  After creating a user, the user name can no longer be modified.

  If a user name needs to be changed, the user must be deleted and a new user created.

  Note

  User names: admin

  You can configure the device with this user name.

  When you log in for the first time or log in after a "Restore Factory Defaults and Restart", you are prompted to change the pre-defined password "admin". You can also rename the "admin" user preset in the factory once. Afterwards, renaming "admin" is no longer possible.

- **Password Policy**
  Shows which password policy is being used.
  - High
    Password length: at least 8 characters, maximum 128 characters
    At least 1 uppercase letter
    At least 1 special character
    At least 1 number
  - Low
    Password length: at least 6 characters, maximum 128 characters

  You configure the password policy on the page "Security > Passwords".
- **Password**
  Specify the password. The strength of the password depends on the set password policy.
  It must not contain the following characters: § and ß
- **Password Confirmation**
  Enter the password again to confirm it.
- **Role**
  Select a role.
  You can choose between system-defined and self-defined roles, refer to the page "Security > Users > Roles".

The table contains the following columns:

- **Select**
  Select the check box in the row to be deleted.

  Note

  The preset users as well as logged in users cannot be deleted or changed.

- **Account**
  Shows the user name.
- **Role**
  Shows the role of the user.
- **Description**
  Displays a description of the user account. The description text can be up to 100 characters long.
- **Remote access**
  - Only
    Only remote access, which means no rights other than logging into the WBM page for user-specific firewall.
  - None
    No remote access. The user cannot log in to the user-specific firewall, but only to the WBM of the device.
  - Additional
    The user can log in to both the WBM of the device and the user-specific firewall.

Procedure

Note

Changes in "Trial" mode

Even if the device is in "Trial" mode, changes that you carry out on this page are saved immediately.

Creating users

1. Enter the name for the user.
2. Enter the password for the user.
3. Enter the password again to confirm it.
4. Select the role of the user.
5. Click the "Create" button.
6. Enter a description of the user.
7. Click the "Set Values" button.

Deleting users

1. Select the check box in the row to be deleted.
2. Click the "Delete" button. The entries are deleted and the page is updated.

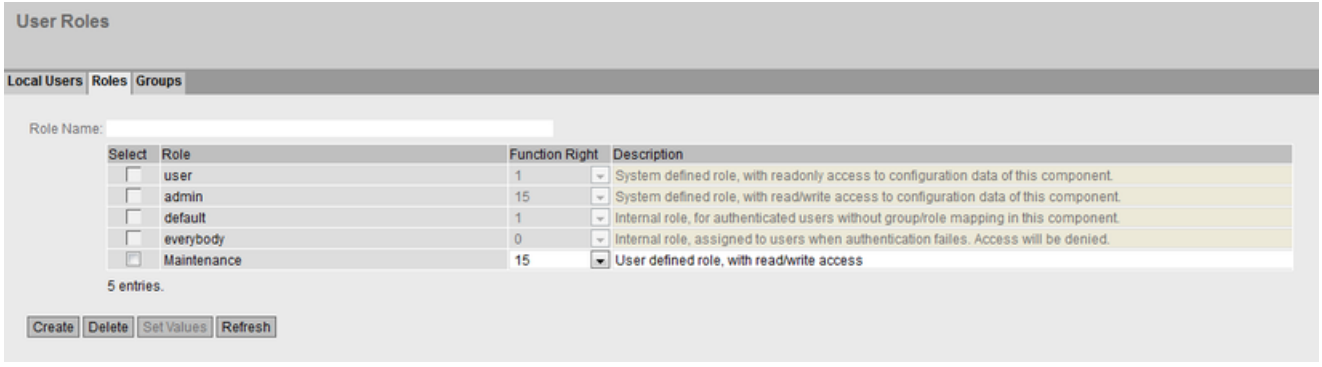
4.8.1.2 Roles

Roles

On this page, you create roles that are valid locally on the device.

Note

The values displayed depend on the rights of the logged-in user.



Restrictions

The following characters are generally not permitted:

- | ; : ? "
- The characters coded with the ASCII value as of 128 (extended ASCII code)
- The characters for Space and Delete

Description

The page contains the following:

- **Role Name**
  Enter the name for the role. The name must meet the following conditions:
  - It must be unique.
  - It must be between 1 and 64 characters long.

  Note

  Role name cannot be changed

  After creating a role, the name of the role can no longer be changed.

  If a name of a role needs to be changed, the role must be deleted and a new role created.

The table contains the following columns:

- **Select**
  Select the check box in the row to be deleted.

  Note

  Predefined roles and assigned roles cannot be deleted or modified.

- **Role**
  Shows the name of the role.
- **Function Right**
  Select the function rights of the role:
  - 1
    Users with this role can read device parameters but cannot change them. Users with this role can change their own password.
  - 15
    Users with this role can both read and change device parameters.
  - 0
    This is a role that the device assigns internally when a user could not be authenticated. The user is denied access to the device.

  Note

  Function right cannot be changed

  If you have assigned a role, you can no longer change the function right of the role.

  If you want to change the function right of a role, follow the steps outlined below:

  1. Delete all assigned users.
  2. Change the function right of the role:
  3. Assign the role again.

- **Description**
  Enter a description for the role. With predefined roles a description is displayed. The description text can be up to 100 characters long.

Procedure

Creating a role

1. Enter the name for the role.
2. Click the "Create" button.
3. Select the function rights of the role.
4. Enter a description of the role.
5. Click the "Set Values" button.

Deleting a role

1. Select the check box in the row to be deleted.
2. Click the "Delete" button. The entries are deleted and the page is updated.

4.8.1.3 Groups

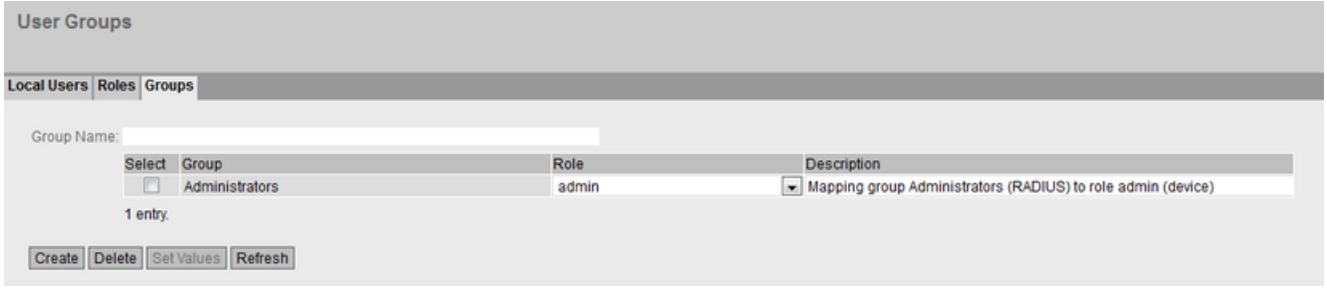
User groups

On this page you link a group with a role.

In this example the group "Administrators" is linked to the "admin" role: The group is defined on a RADIUS server. The role is defined locally on the device. When a RADIUS server authenticates a user and assigns the user to the "Administrators" group, this user is given rights of the "admin" role.

Note

The values displayed depend on the rights of the logged-in user.



Restrictions

The following characters are generally not permitted:

- | ; : ? "
- The characters coded with the ASCII value as of 128 (extended ASCII code)
- The characters for Space and Delete

Description

The page contains the following:

- **Group Name**
  Enter the name of the group. The name must match the group on the RADIUS server.
  The name must meet the following conditions:
  - It must be unique.
  - It must be between 1 and 64 characters long.

The table contains the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **Group**
  Shows the name of the group.
- **Role**
  Select a role. Users who are authenticated with the linked group on the RADIUS server receive the rights of this role locally on the device.
  You can choose between system-defined and self-defined roles, refer to the page "Security > Users > Roles".
- **Description**
  Enter a description for the link of the group.to a role. The description text can be up to 100 characters long.

Procedure

Linking a group to a role.

1. Enter the name of a group.
2. Click the "Create" button.
3. Select a role.
4. Enter a description for the link of a group.to a role.
5. Click the "Set Values" button.

Deleting the link between a group and a role

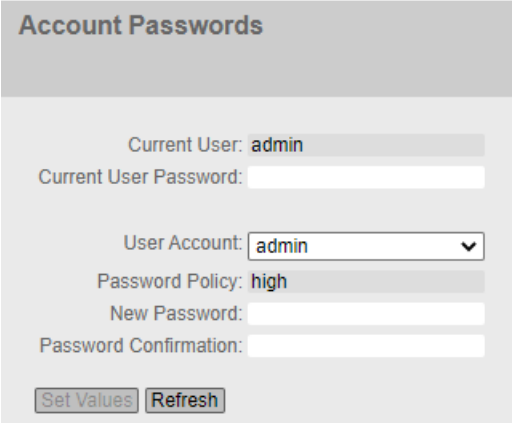
1. Select the check box in the row to be deleted.
2. Click the "Delete" button. The entries are deleted and the page is updated.

4.8.2 Passwords

4.8.2.1 Passwords

Configuration of the passwords

A user with the "admin" role can change the password of already created users. With the "user" role, users can only change their own password.



Description

The page contains the following:

- **Current User**
  Shows the user that is currently logged in.
- **Current User Password**
  Enter the password for the currently logged in user.
- **Account**
  Select the user whose password you want to change.
- **Password Policy**
  Shows which password policy is being used when assigning new passwords.
  - High
    Password length: at least 8 characters, maximum 128 characters
    At least 1 uppercase letter
    At least 1 special character
    At least 1 number
  - User-defined
    The password must meet the configured requirements. You configure the requirements under "Security > Passwords > Options"

- **New Password**
  Enter the new password for the selected user.
  It must not contain any of the following characters: | § ? " ; : ß \

Note

When you log in for the first time or log in after a "Restore Factory Defaults and Restart", you are prompted to change the pre-defined password "admin". You can also rename the "admin" user preset in the factory once. Afterwards, renaming "admin" is no longer possible.

The factory setting for the password when the devices ship is as follows:

- admin: admin

Note

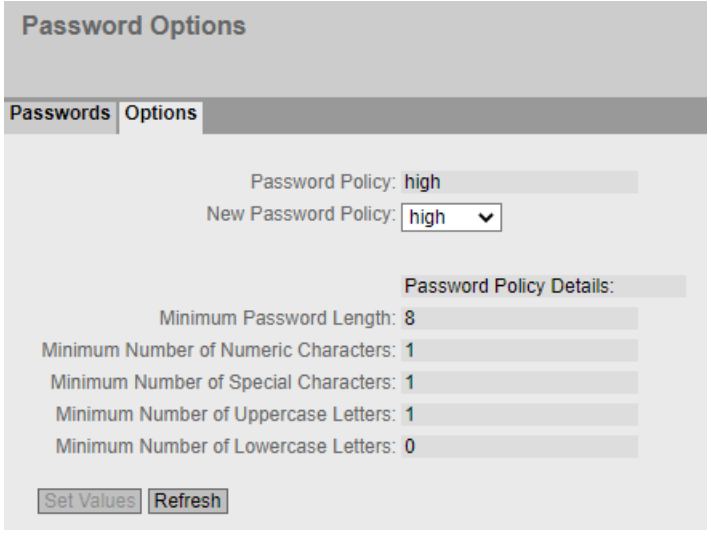
Changing the password in Trial mode

Even if you change the password in Trial mode, this change is saved immediately.

- **Password Confirmation**
  Enter the new password again to confirm it.

4.8.2.2 Options

On this page, you specify which password policy will be used when assigning new passwords.



Description

- **Password Policy**
  Shows which password policy is currently being used.
- **New Password Policy**
  Select the required setting from the drop-down list.
  - High
    Password length: at least 8 characters, maximum 128 characters
    At least 1 number
    At least 1 special character
    At least 1 uppercase letter
  - User-defined
    Configure the desired password requirements under "Password Policy Details".
- **Password Policy Details**
  When you have selected the "High" password policy, the relevant password requirements are displayed.
  When you have selected the "User-defined" password policy, you can configure the relevant password requirements.
  - Minimum Password Length
    Specifies the minimum length of a password.
  - Minimum Number of Numeric Characters
    Specifies the minimum number of numeric characters in a password.
  - Minimum Number of Special Characters
    Specifies the minimum number of special characters in a password.
  - Minimum Number of Uppercase Letters
    Specifies the minimum number of uppercase characters in a password.
  - Minimum Number of Lowercase Letters
    Specifies the minimum number of lowercase characters in a password.

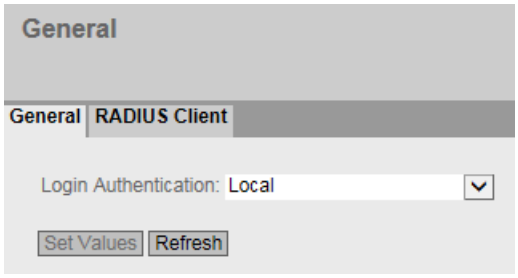
4.8.3 AAA

4.8.3.1 General

Login of network nodes

The designation "AAA" stands for "Authentication, Authorization, Accounting". This feature is used to identify and allow network nodes, to make the corresponding services available to them and to specify the range of use.

On this page, you configure the login.



Description

The page contains the following boxes:

Note

To be able to use the login authentication "RADIUS", "Local and RADIUS" or "RADIUS and fallback Local", a RADIUS server must be stored and configured for user authentication.

- **Login Authentication**
  Specify how the login is made:
  - Local
    The authentication must be made locally on the device.
  - RADIUS
    The authentication must be handled via a RADIUS server.
  - Local and RADIUS
    The authentication is possible both with the users that exist on the device (user name and password) and via a RADIUS server.
    The user is first searched for in the local database. If the user does not exist there, a RADIUS request is sent.
  - RADIUS and fallback Local
    The authentication must be handled via a RADIUS server.
    A local authentication is performed only when the RADIUS server cannot be reached in the network.

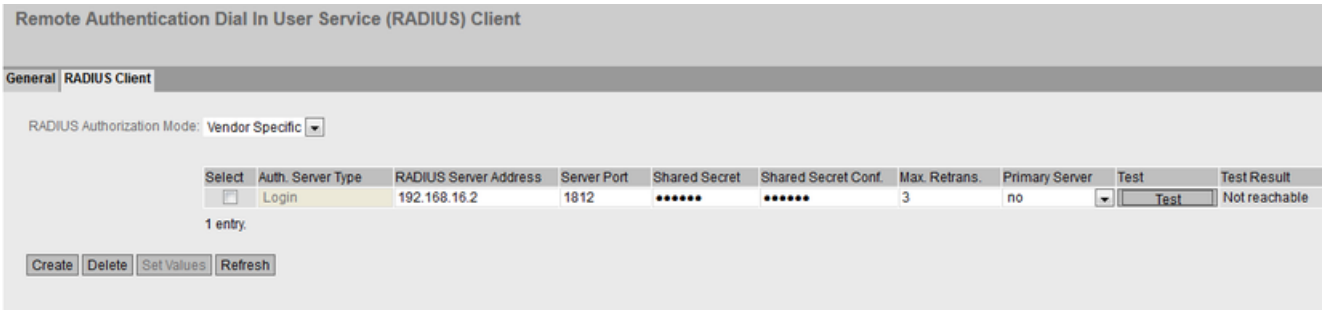
4.8.3.2 RADIUS client

Authentication over an external server

The concept of RADIUS is based on an external authentication server.

Each row of the table contains access data for one server. In the search order, the primary server is queried first. If the primary server cannot be reached, secondary servers are queried in the order in which they are entered.

If no server responds, there is no authentication.



Description

The page contains the following boxes:

- **RADIUS Authorization Mode**
  For the login authentication, the RADIUS authorization mode specifies how the rights are assigned to the user with a successful authentication.
  - Conventional
    In this mode the user is logged in with administrator rights if the server returns the value "Administrative User" to the device for the attribute "Service Type". In all other cases the user is logged in with read rights.
  - SiemensVSA
    In this mode, the assignment of rights depends on whether and which group the server returns for the user and whether or not there is an entry for the user in the table "External User Accounts".

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **RADIUS Server Address**
  Enter the IP address or the FQDN (Fully Qualified Domain Name) of the RADIUS server.
- **Server Port**
  Here, enter the input port on the RADIUS server. As default, input port 1812 is set. The range of values is 1 to 65535.
- **Shared Secret**
  Enter your access ID here. The range of values is 1...128 characters
- **Shared Secret Conf.**
  Enter your access ID again as confirmation.
- **Max. Retrans.**
  Here, enter the maximum number of retries for an attempted request.
  The initial connection attempt is repeated the number of times specified here before another configured RADIUS server is queried or the login counts as having failed. As default 3 retries are set, this means 4 connection attempts. The range of values is 1 to 5.
- **Primary Server**
  Using the options in the drop-down list, specify whether or not this server is the primary server. You can select one of the options "yes" or "no".

- **Test**
  With this button, you can test whether or not the specified RADIUS server is available. The test is performed once and not repeated cyclically.
- **Test Result**
  Shows whether or not the RADIUS server is available:
  - Not reachable
    The IP address is not reachable.
    The IP address is reachable, the RADIUS server is, however, not running.
  - Reachable, key not accepted
    The IP address is reachable, the RADIUS server does not, however accept the shared secret.
  - Reachable, key accepted
    The IP address is reachable, the RADIUS server accepts the specified shared secret.

Procedure

Entering a new server

1. Click the "Create" button. A new entry is generated in the table.
   The following default values are entered in the table:
   - RADIUS Server Address: 0.0.0.0
   - Server Port: 1812
   - Max. Retrans.: 3
   - Primary server: No
2. In the relevant row, enter the following data in the input boxes:
   - RADIUS Server Address
   - Server Port
   - Shared Secret
   - Shared Secret Conf
   - Max. Retrans.: 3
   - Primary server: No
3. If necessary check the reachability of the RADIUS server.
4. Click the "Set Values" button.

Repeat this procedure for every server you want to enter.

Modifying servers

1. In the relevant row, enter the following data in the input boxes:
   - RADIUS Server Address
   - Server Port
   - Shared Secret
   - Shared Secret Conf
   - Max. Retrans.
   - Primary Server
2. If necessary check the reachability of the RADIUS server.
3. Click the "Set Values" button.

Repeat this procedure for every server whose entry you want to modify.

Deleting servers

1. Click the check box in the first column before the row you want to delete to select the entry for deletion.
   Repeat this for all entries you want to delete.
2. Click the "Delete" button. The data is deleted from the memory of the device and the page is updated.

4.8.3.3 802.1X Authenticator

Setting up network access

An end device can only access the network after the device has verified the login data of the device with the authentication server. The authentication can be via 802.1X or the MAC address.

When authenticating using 802.1X both the end device and the authentication server must support the EAP protocol (Extensive Authentication Protocol).

Enabling authentication for individual ports

By enabling the relevant options, you specify for each port whether or not network access protection according to IEEE 802.1X is enabled on this port.

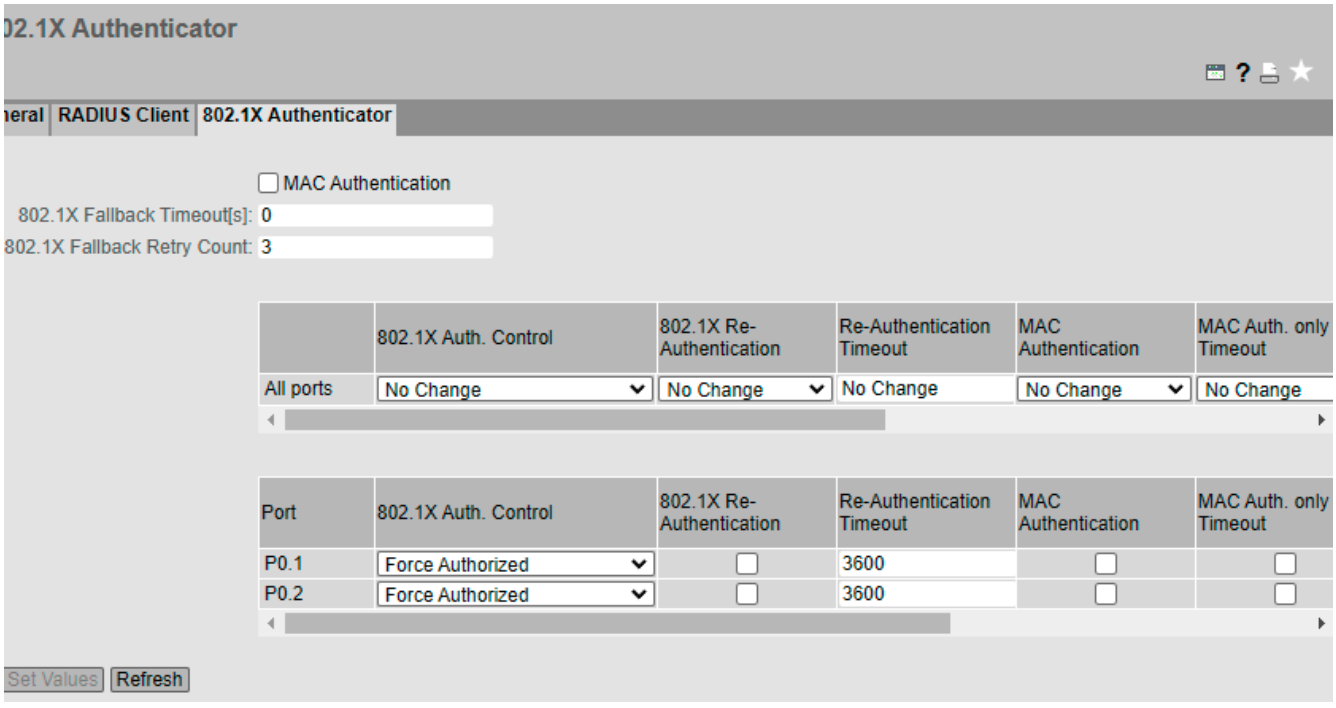


Figure 4-1 802.1x Authenticator - first part of the table

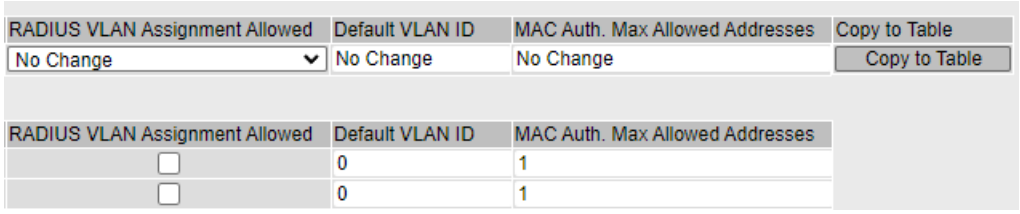


Figure 4-2 802.1X Authenticator - second part of the table

Description of the displayed boxes

The page contains the following boxes:

- **MAC Authentication**
  Enable or disable MAC Authentication for the device.
- **802.1X Fallback Timeout [s]**
  Specify the time interval in seconds after which the device is reinitialized for 802.1X authentication at the relevant port after MAC authentication fails. The default value is 0 seconds, i.e. there is no fallback timeout and no reinitialization for the 802.1X authentication.
- **802.1X Fallback Retry Count**
  Specify how often the port is reinitialized for 802.1X authentication after MAC authentication fails.

Table 1 has the following columns:

- **1st column**
  Shows that the settings are valid for all ports of table 2.
- **802.1X Auth. Control**
  Select the required setting. If "No Change" is selected, the entry in table 2 remains unchanged.
- **802.1X Re-Authentication**
  Select the required setting. If "No Change" is selected, the entry in table 2 remains unchanged.
- **Re-Authentication Timeout**
  Specify the time interval in seconds after which the device is reauthenticated at the relevant port. The default value is 3600 seconds. If "No Change" is selected, the entry in table 2 remains unchanged.
- **Tx Timeout**
  The value specifies the period of time in seconds after which an EAP request packet is sent if no client responds. If MAC authentication is enabled, a switch is made from 802.1X authentication to MAC authentication after the third EAP request packet. The default value is 5 seconds. If "No Change" is selected, the entry in table 2 remains unchanged.
- **MAC Authentication**
  Select the required setting. If "No Change" is selected, the entry in table 2 remains unchanged.
- **MAC Auth only on Timeout**
  Select the required setting. If "No Change" is selected, the entry in table 2 remains unchanged.
- **RADIUS VLAN Assignment Allowed**
  Select the required setting. If "No Change" is selected, the entry in table 2 remains unchanged.

  Note

  The VLAN assignment of RADIUS is only applied if the port has not already been configured for this VLAN. If the port VLAN ID matches the VLAN ID assigned by RADIUS, the type of membership in this VLAN must be preconfigured.

- **MAC Auth. Max Allowed Addresses**
  Specify how many MAC addresses can communicate on the port at the same time.
  If "No Change" is selected, the entry in table 2 remains unchanged.
- **Copy to Table**
  When you click the button, the settings are adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
  This column lists all the ports available on this device.
- **802.1X Auth. Control**
  Specify the authentication of the port:
  - Force Unauthorized
    Data traffic via the port is blocked.
  - Force Authorized
    Data traffic via the port is allowed without any restrictions.
    Default setting
  - Auto
    End devices are authenticated on the port with the "802.1X" method.
    The data traffic via the port is permitted or blocked depending on the authentication result.
- **802.1X Re-Authentication**
  Enable this option if you want reauthentication of an already authenticated end device to be repeated cyclically.
- **Re-Authentication Timeout**
  Specify the time interval in seconds after which the device is reauthenticated at the relevant port. The default value is 3600 seconds.
- **Tx Timeout**
  The value specifies the period of time in seconds after which an EAP request packet is sent if no client responds. If MAC authentication is enabled, a switch is made from 802.1X authentication to MAC authentication after the third EAP request packet. The default value is 5 seconds.
- **MAC Authentication**
  Enable this option if you want end devices to be authenticated with the "MAC Authentication" method.
  If "Auto" is configured for "802.1x Auth. Control" and the "MAC Authentication" is enabled, the timeout for the "802.1X" procedure is 5 seconds. If manual input is necessary at a port for the authentication with the "802.1X" procedure, the 5 seconds may not be adequate. To be able to run authentication using "802.1X", disable the MAC authentication on this port.
- **MAC Auth only on Timeout**
  If this check box is selected, MAC authentication is only possible after a 802.1X timeout, but not after a failed 802.1X authentication. When the check box is not selected, MAC authentication is possible both after an 802.1X timeout and after a failed 802.1X authentication.

- **Adopt RADIUS VLAN Assignment**
  The RADIUS server informs the IE switch of the VLAN to which the port will belong. Enable this option if you want the information of the server to be taken into account.
  The port can only be assigned to the VLAN, if the VLAN has been created on the device. Otherwise Authentication is rejected.
  If during authentication a port is assigned to a VLAN dynamically using this function, assignment using the VLAN-ID or the VLAN name is possible. Configure the following values on the RADIUS server:
  - Tunnel-Type = VLAN
  - Tunnel-Medium-Type = IEEE-802
  - Tunnel-Private-Group-Id = VLAN-ID or VLAN-Name

  The IE switch distinguishes as follows:
  - VLAN ID: The RADIUS server transfers a numeric string for the parameter "Tunnel-Private-Group-Id".
  - VLAN-Name: The RADIUS server transfers an alphanumeric string for the parameter "Tunnel-Private-Group-Id".
- **Default VLAN ID**
  If a VLAN ID is transmitted to the RADIUS server during a successful authentication and the "RADIUS VLAN Assignment Allowed" check box is selected, the current PVID of the port is changed to the value transmitted by the RADIUS server. Otherwise, an "Untagged membership" of the port may be set up in the relevant VLAN to enable communication in the respective VLAN.
  The Default VLAN ID determines the assignment of the VLAN ID when the "RADIUS VLAN Assignment Allowed" check box is selected, but the RADIUS server does not send a VLAN ID after successful authentication. You have two options:
  - **The value "0" is configured for the default VLAN ID**
    The PVID currently configured for the port continues to be used.
  - **A value in the range from "1 ... 4094" is configured for the Default VLAN ID**
    The PVID of the port is changed to the "Default VLAN ID" configured in this column as if it had been transmitted by the RADIUS server.

  In all cases, a changed PVID is reset to the originally configured value after the device logs out. Any "Port membership" that has been set up is deleted again. This applies to both 802.1X authentication and MAC authentication.
- **MAC Auth. Max Allowed Addresses**
  - 1 - 200
    Specify how many MAC addresses can communicate on the port at the same time.

    Note

    If a device uses several MAC addresses, all MAC addresses must be authenticated. Store all the MAC addresses to be authenticated on the RADIUS server. Enter the number in the "MAC Auth. Max Permitted Addresses" box.
  - 0
    You can set the value "0". This setting has the effect that after the first successful authentication of a MAC address, the port is released for all MAC addresses.

Configuration procedure

Enable authentication for an individual port

1. Select the required options in the relevant row in table 2.
2. To apply the changes, click the "Set Values" button.

Enable authentication for all ports

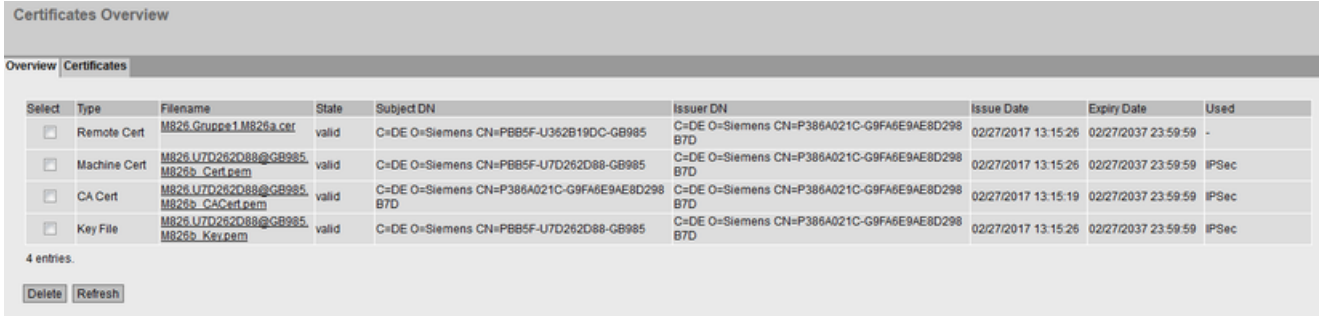
1. Select the required options in table 1.
2. Click the "Copy to Table" button. The relevant settings are adopted for all ports in table 2.
3. To apply the changes, click the "Set Values" button.

4.8.4 Certificates

4.8.4.1 Overview

All loaded files (certificates and keys) are shown on this WBM page. You have the following options for loading files on the device:

- System > Load&Save > HTTP
- System > Load&Save > TFTP
- System > Load&Save > SFTP



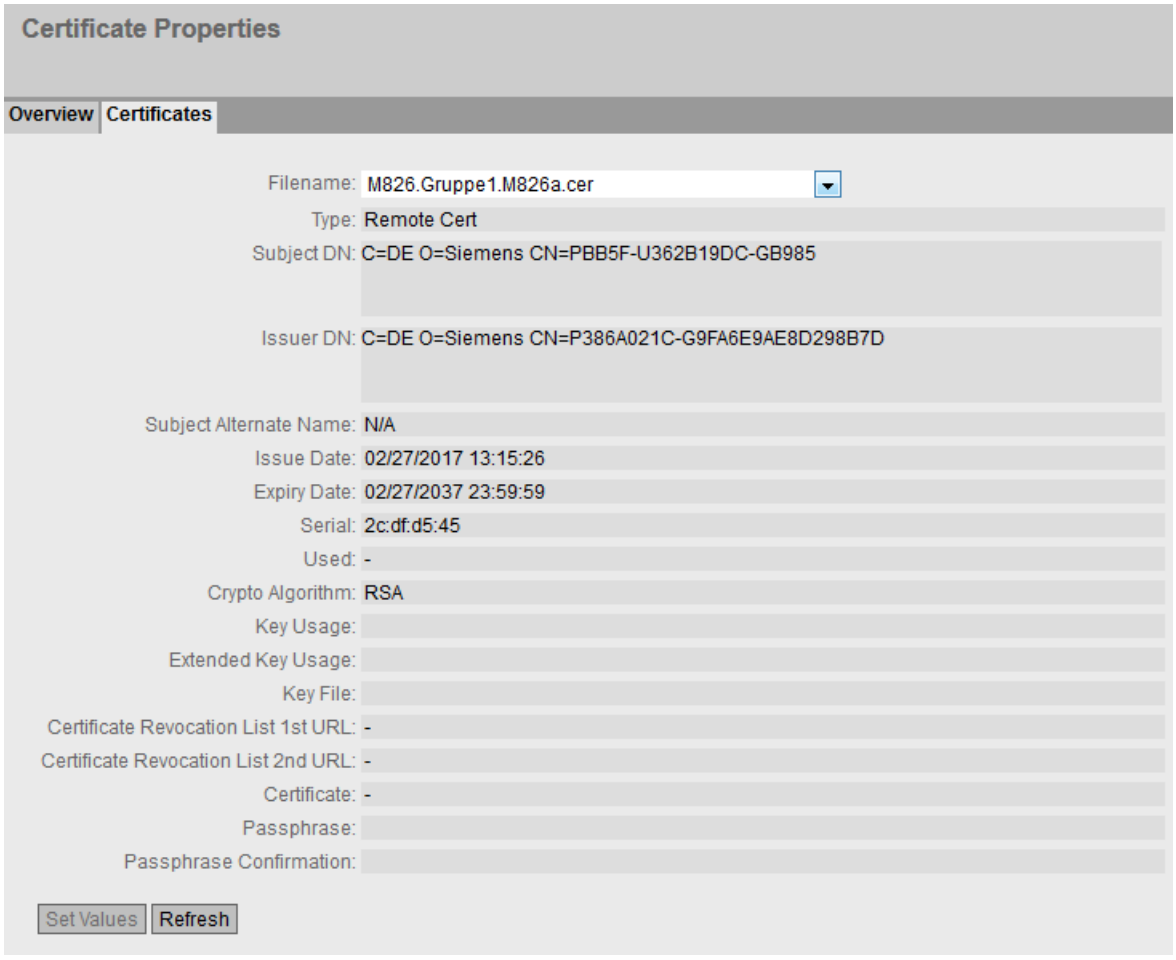
Description

- **Select**
  Select the check box in the row to be deleted. Only unused certificates can be deleted.
- **Type**
  Shows the type of the loaded file.
  - CA Cert
    The CA certificate is signed by a CA (Certification Authority).
  - Machine certificate
  - Key File
  - Remote Cert
    Partner certificate
- **Filename**
  Shows the file name.
- **Status**
  Shows whether the certificate is valid or has already expired.
- **Subject DN**
  Shows the name of the applicant.
- **Issuer DN**
  Shows the name of the certificate issuer.
- **Issue Date**
  Shows the start of the period of validity of the certificate.
- **Expiry Date**
  Shows the end of the period of validity of the certificate.
- **Used**
  Shows which function uses the certificate.

4.8.4.2 Certificates

The format of the certificate is based on X.509, a standard of the ITU-T for creating digital certificates. This standard describes the schematic structure of X.509 certificates. You will find further information on this on the Internet at "http://www.itu.int".

On this WBM page, the content of the following structure elements can be displayed. If the structure element does not exist or is not completed in the selected certificate, nothing is shown in the box on the right. Certain entries can only be edited if they are supported.



Description

- **Information**
  Shows whether a certificate is loaded; if this is the case, the information on the respective certificate is displayed.
- **Filename**
  Select the required certificate.
- **Type**
  Shows the type of the loaded file.
  - CA Cert
    The CA certificate is signed by a CA (Certification Authority).
  - Machine certificate
  - Key File
  - Remote Cert
    Partner certificate
- **Subject DN**
  Shows the name of the applicant.

- **Issuer DN**
  Shows the name of the certificate issuer.
- **Subject Alternate Name**
  If it exists, an alternative name of the applicant is displayed.
- **Issue Date**
  Shows the start of the period of validity of the certificate
- **Expiry Date**
  Shows the end of the period of validity of the certificate.
- **Serial Number**
  Shows the serial number of the certificate.
- **Used**
  Shows which function uses the certificate.
- **Crypto Algorithm**
  Shows which cryptographic method is used.
- **Key Usage**
  Shows the purpose that the key belonging to the certificate is used for, e.g. to verify digital signatures.
- **Extended Key Usage**
  Shows whether the purpose is additionally restricted, e.g. only to verify signatures of the CA certificate.
- **Key File**
  Shows the key file.
- **Certificate Revocation List 1st URL**
  Enter the URL with which the revocation list can be called up. Can only be edited if supported by the certificate.
- **Certificate Revocation List 2nd URL**
  Enter an alternative URL. If the revocation list cannot be called up using the 1st URL, the alternative URL is used. Can only be edited if supported by the certificate.
- **Certificate**
  Shows the name of the certificate.
- **Passphrase**
  Enter the password for the certificate. Can only be edited if the encrypted file is password protected.
- **Passphrase Confirmation**
  Enter the password again. Can only be edited if the encrypted file is password protected.

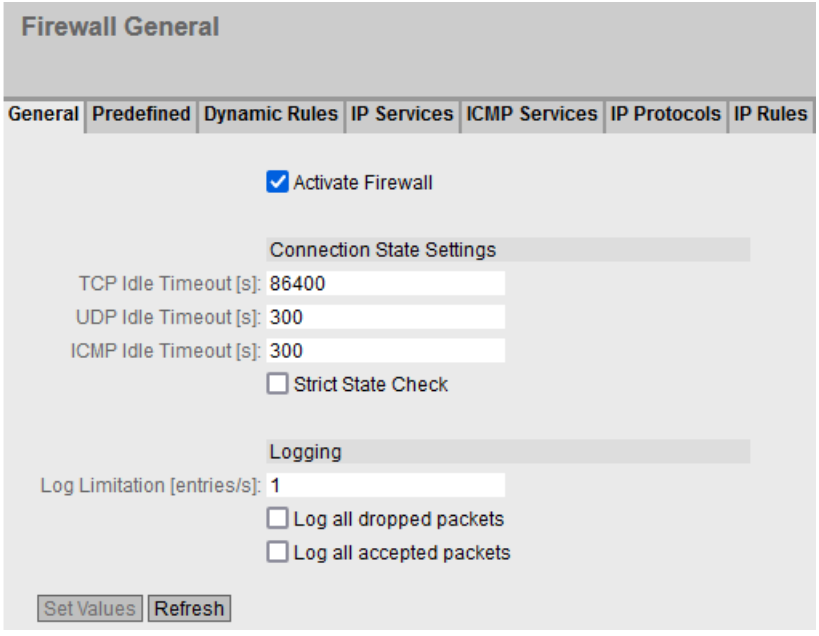
4.8.5 Firewall

4.8.5.1 General

On this WBM page, you enable the firewall.

Note

Please remember that if you disable the firewall, your internal network is unprotected.



Description

The page contains the following:

- **Activate Firewall**
  When enabled, the firewall is active.

Connection status settings

- **TCP Idle Timeout [s]**
  Enter the required time in seconds. If no data exchange takes place, the TCP connection is terminated automatically when this time has elapsed.
  The range of values is 1 to 2147483.
  Default setting: 86400 seconds
- **UDP Idle Timeout [s]**
  Enter the required time in seconds. If no data exchange takes place, the UDP connection is terminated automatically when this time has elapsed.
  The range of values is 1 to 2147483.
  Default setting: 300 seconds

- **ICMP Idle Timeout [s]**
  Enter the required time in seconds. If no data exchange takes place, the ICMP connection is terminated automatically when this time has elapsed.
  The range of values is 1 to 2147483.
  Default setting: 300 seconds
- **Strict State Check**
  When enabled, the firewall only forwards packets to the communication partner that can be assigned to a connection. Packets that cannot be assigned to a connection are discarded. To this end, the firewall checks the status of the connection, for example, whether a three-way handshake has been performed.
  When disabled, the firewall also forwards packets that cannot be assigned to a connection if the corresponding firewall rule has been created. This can be used, for example, in "Asymmetric routing" when the firewall does not recognize all packets of a connection.

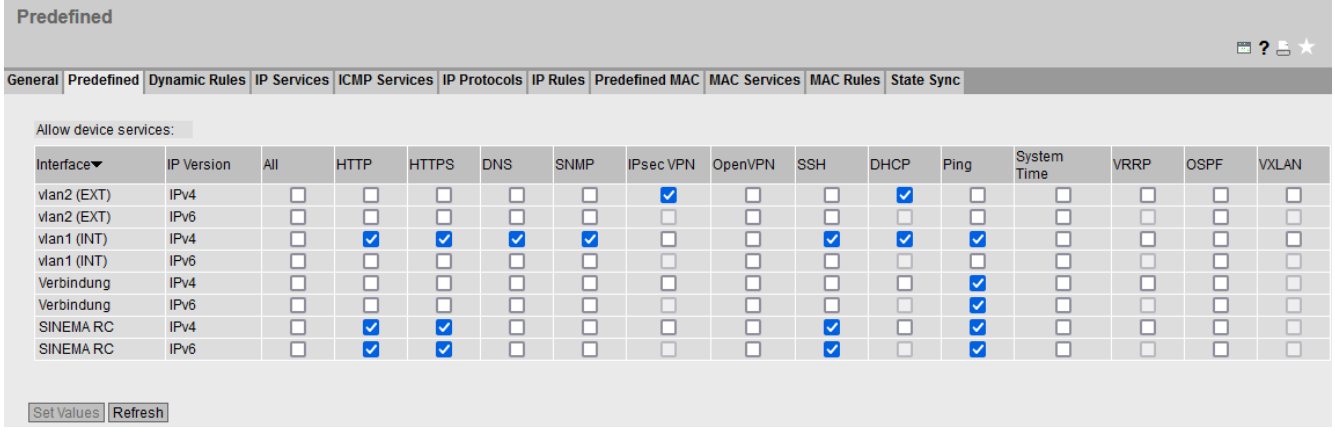
Logging

- **Limitation [entries/s]**
  Maximum number of entries in the firewall log per second. A firewall rule with enabled logging can create max. the entered number of entries per second.
  Note: Intensive logging can have a negative effect on the firewall bandwidth.
- **All discarded packets**
  When enabled, all packets discarded by the firewall are logged, regardless of whether logging is enabled for the firewall rule or not.
- **All accepted packets**
  When enabled, all packets accepted by the firewall are logged, regardless of whether logging is enabled for the firewall rule or not.

4.8.5.2 Predefined

The WBM page contains predefined IP packet filter rules. If you create your own IP packet filter rules, these have a higher priority than the predefined IP packet filter rules.

You set here which services of the device should be reachable from which interface/subnet.



Description

- **Interface**
  Interface to which the setting relates. The list of interfaces/subnets is dynamic and is based on the settings from "Layer 3 > Subnets".
  - VLANx: Allows access from the IP subnet to the device. VLANs with configured IP subnet are available.
  - SINEMARC: Allows access from the SINEMA RC server to the device.
  - IPsec: Allows IKE (Internet Key Exchange) data traffic from the external network to the device.
  - IP Version
    Shows the IP version to which the firewall rules apply.
    IPv4
    IPv6
- Access over the firewall is permitted to the following IPv4 services of the device:
  - All
    All predefined IPv4 services.
  - HTTP
    For access to Web Based Management.
  - HTTPS
    For secure access to Web Based Management.

    Note

    HTTPS disabled

    If you disable HTTPS, the WBM of the device can no longer be reached.
  - DNS
    DNS queries to the device. Only necessary if the "Enable DNS Proxy" function is enabled on the device.
  - SNMP
    Incoming SNMP connections. Required, for example, to access the SNMP information of the device using a MIB browser.
  - IPsec VPN
    Allows IKE (Internet Key Exchange) data transfer from the external network to the device. Necessary if an IPsec VPN remote station needs to establish a connection to this device.
  - OpenVPN
    Allows OpenVPN data traffic from the external network to the device. Necessary if an OpenVPN client is to establish a connection to this device (as OpenVPN server).
  - SSH
    For encrypted access to the CLI.
  - DHCP
    Access to the DHCP server or the DHCP client.
  - Ping
    Access to the ping function.

- System time
  Access to NTP and SNTP.
- VRRP
  Activates "VRRP" in the firewall and thus incoming VRRP frames. Enable the function if "VRRP" is also active on the device, because otherwise no operation of router redundancy VRRPv3 is possible.
- OSPF
  Activates "OSPF" in the firewall and thus incoming OSPF frames. Enable the function if "OSPF" is also active on the device; otherwise, no dynamic routing is possible.
- VXLAN
  To establish the VXLAN tunnel and receive the frames. Necessary if the tunnel endpoint establishes a connection to this device.

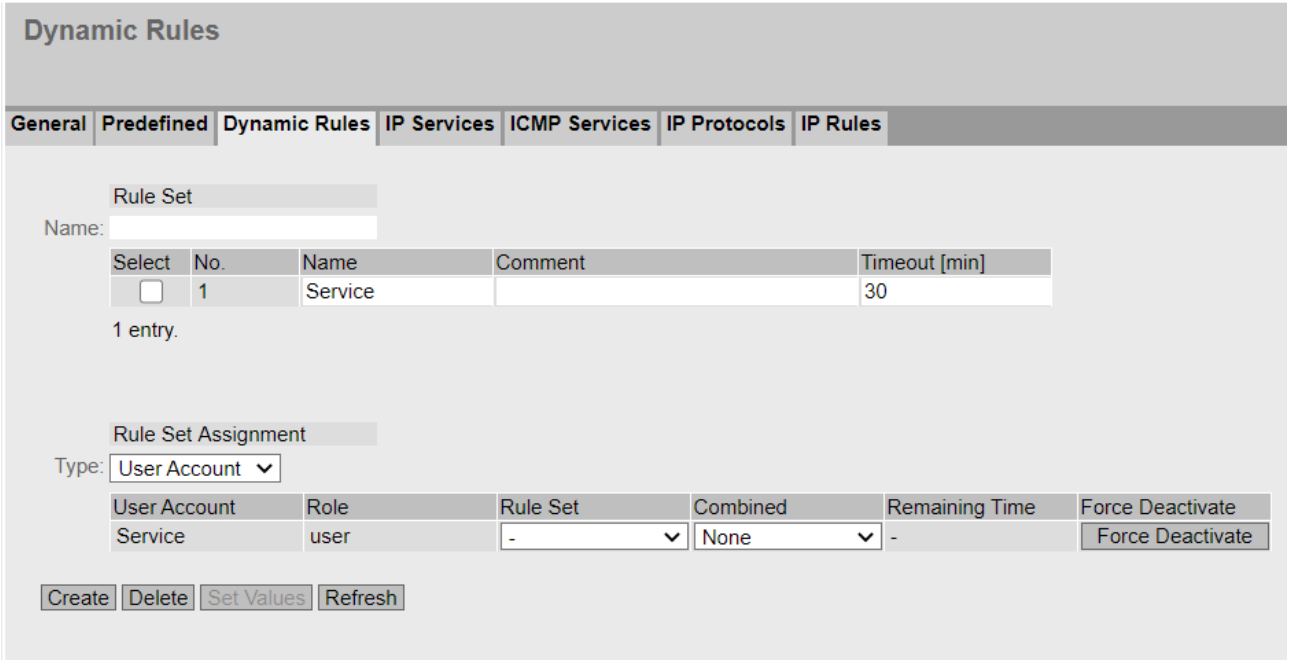
4.8.5.3 Dynamic Rules

On this page, you define dynamic rule sets. Firewall rules that are required for remote access, for example, can be summarized with a rule set.

You can assign a rule set to one or more users. If login of this user was successful, the firewall rule set intended for this user is enabled.

A timer is started after login. When the time expires, the user is automatically logged out from the device.

You can also control the rule sets over time. A start time and an end time are configured. Between these times, the firewall rules assigned to the rule set are enabled.



Description

"Rule set" area

- **Name**
  Define a unique name for the rule set. If you click the "Create" button, a new row with a unique number is created.

The table contains the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **No.**
  Shows the unique number of the entry.
- **Name**
  Name of the rule set. The name can be changed if required.
- **Comment**
  Comment that describes the rule set in more detail.
- **Timeout [min]**
  Access is time-limited. Specify the duration of the access. If needed, the user can extend the access time via the "Reset Timeout" button on the "Dynamic Firewall Rules Information" page.

"Rule Set Assignment" area

- **Type**
  Specify which rule set will be assigned to whom. The display of the following table depends on the selection for "Type".
  - User Account
    The rule set is activated through a local user account.
  - Digital Input
    The rule set is executed by controlling the digital input. The prerequisite for this is that the entry "Digital Input" is activated for the "Firewall" event under "System > Events > Configuration".
  - Radius Role
    The rule set is activated through a RADIUS role.
  - RADIUS User
    The rule set is activated through a RADIUS user.
  - Time triggered
    Enforcement of the rule set is time-triggered.

The "User Account" table contains the following columns:

- User Account
  Only users with the remote access "only" or "additional" are displayed.
- Role
  Shows the role of the user.
- Rule set
  Define the rule set that is valid for this user.

- Combined with
  Combines the user login with an event, e.g. the "Digital Input" event. To log in to the WBM page for the dynamic firewall, voltage must be present at the digital input and user login must be successful.
- Remaining Time
  When this user is logged on, the remaining time for access is displayed.
- Force Deactivate
  A user with administrator rights can log off the active user with this button.

The "**Digital Input**" table contains the following columns:

- Digital Input
  The available digital inputs.
- Rule set
  Define the rule set that is controlled via the digital input.
- Dynamic Source (Range)
  Enter the IP address or an IP range that is allowed to send IP packets.
- Status
  Shows the remaining time for access.

The "**RADIUS Role**" table contains the following columns:

- Role
  Shows the role name. Only roles with the remote access "additional" are displayed. The prerequisite is that the role was created on the RADIUS server and RADIUS users were assigned to the role.
- Rule set
  Define the rule set that is valid for this RADIUS role.
- Combined with
  Combines the logon with an event, e.g. the "Digital Input" event. To log in to the WBM page for the dynamic firewall, voltage must be present at the digital input and login must be successful.
- Number
  After successful login, the number of users active via RADIUS that are assigned to the RADIUS role is displayed.
- Force Deactivate
  A user with administrator rights can log out the RADIUS role with this button.

The "**RADIUS User**" table contains the following columns:

- User
  Shows the users assigned to the role.
  A role with the remote access "additional" is created on the device and assigned to a group. The names of the group must match exactly the names of the user groups on the RADIUS server.
- Role
  The role assigned to the RADIUS user.

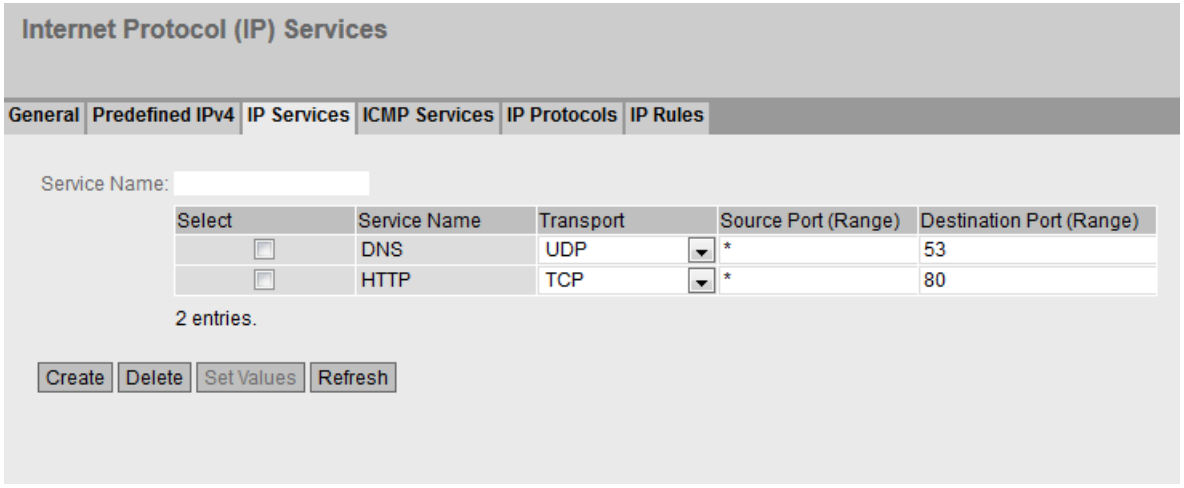
- Remaining Time
  When this user is logged on, the remaining time for access is displayed.
- Force Deactivate
  A user with administrator rights can log out the RADIUS role with this button.

The "**Time triggered**" table contains the following columns:

- Time triggered
  Index of the entry.
- Rule set
  Define the rule set that is time triggered.
- Combined with
  Combines the time triggering with an event, for example, the "Digital Input" event. To log in to the WBM page for the dynamic firewall, voltage must be present at the digital input and login must be successful.
- Cycle
  Specify the enforcement cycle for the time triggering.
  - Daily
  - Weekly
  - Monthly
- Days
  If "Weekly" or "Monthly" is set for the cycle, specify the days.
  Enter the days separated by commas, e.g. 1,3,4
  - Weekly: 1 - 7
  - Monthly: 1 - 31
- Dynamic Source (Range)
  - Individual IP address: Specify the IP address
  - IP range: Specify the range with start address "-" end address, e.g.
    IPv4:192.168.100.10 - 192.168.100.20
    IPv6: fe80:: - febf::
  - All IP addresses:
    IPv4: " 0.0.0.0/0"
    IPv6: "::"
  - If the rule set is activated by a user, the placeholder DYNAMIC is replaced by the IP address of the end device used.
- Start time
  Enter the start time in the format HH:MM.
- End time
  Enter the end time in the format HH:MM.
- Enable
  When enabled, the rule set is time-triggered. The connection is briefly interrupted when the time-triggered firewall rules are initiated.

4.8.5.4 IP services

On this WBM page, you define IP services. Using the IP service definitions, you can define firewall rules for specific services. You select a name and assign the service parameters to it. When you configure the IP rules, you simply use this name.



Description

The page contains the following:

- **Service Name**
  Enter the name of the IP service. The name must be unique.

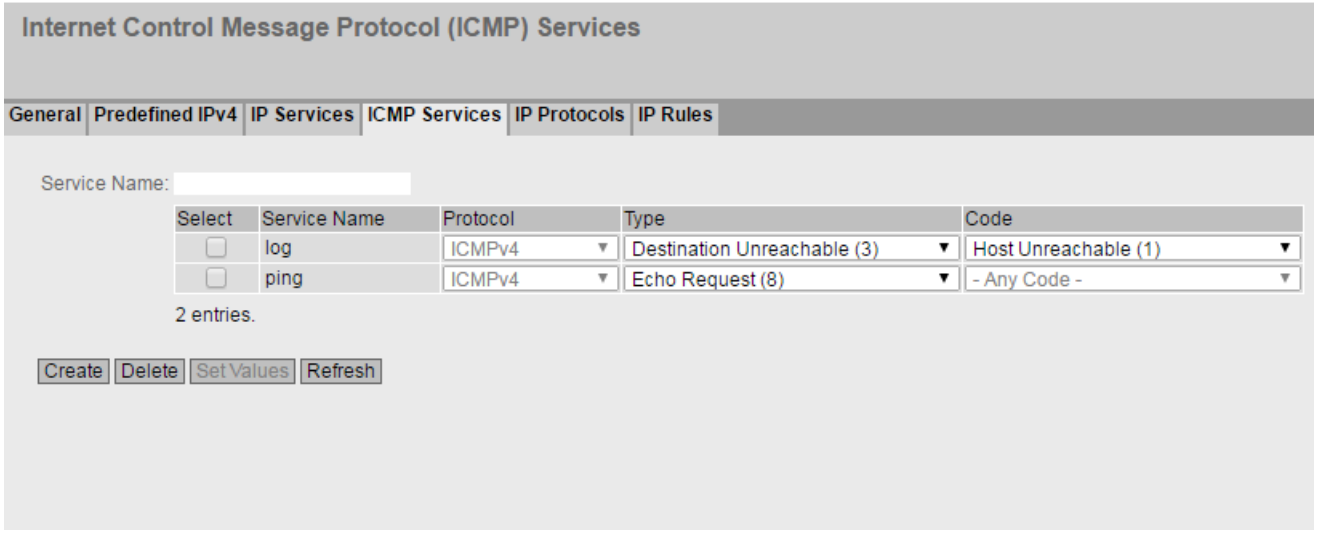
This table contains the following columns:

- **Select**
  Activate the check box in the row to be deleted.
- **Service Name**
  Shows the name of the IP service.
- **Transport**
  Specify the protocol type.
  - UDP
    The rule applies only to UDP frames.
  - TCP
    The rule applies only to TCP frames.

- **Source Port (Range)**
  Enter the source port. The rule applies specifically to the specified port.
  - If the rule is intended to apply to a port range, enter the range with start port "-" end port, for example 30 - 40.
  - If the rule is intended to apply to all ports, enter "*".
- **Destination Port (Range)**
  Enter the destination port. The rule applies specifically to the specified port.
  - If the rule is intended to apply to a port range, enter the range with start port "-" end port, for example 30 - 40.
  - If the rule is intended to apply to all ports, enter "*".

4.8.5.5 ICMP services

On this WBM page, you define ICMP services. Using the ICMP service definitions, you can define firewall rules for specific services. You select a name and assign the service parameters to it. When you configure the IP rules, you simply use this name.



Description

The page contains the following:

- **Service Name**
  Enter a name for the ICMP service. The name must be unique.

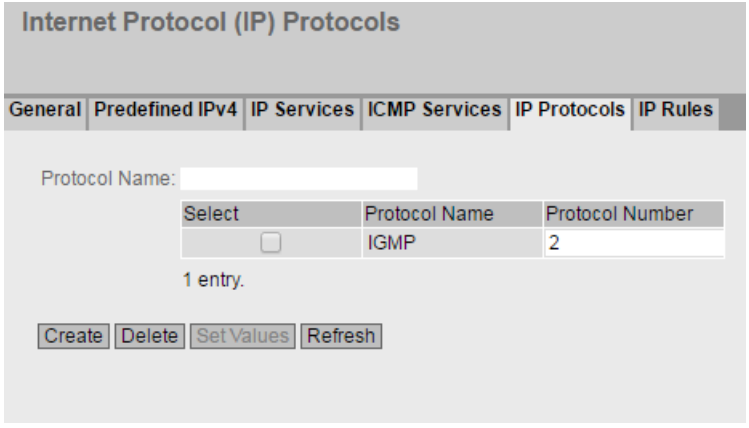
The table contains the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **Service Name**
  Shows the name of the ICMP service.

- **Protocol**
  Shows the version of the ICMP protocol.
- **Type**
  Specify the ICMP packet type. A few examples are shown below:
  - Destination Unreachable
    IP frame cannot be delivered.
  - Time Exeeded
    Time limit exceeded
  - Echo-Request
    Echo request, better known as ping.
- **Code**
  The code describes the ICMP packet type in greater detail. The selection depends on the selected ICMP packet type.
  With "Destination Unreachable", for example "Code 1" host cannot be reached.

4.8.5.6 IP protocols

On this WBM page, you can configure user-defined protocols, e.g. IGMP for multicast groups. You select a protocol name and assign the service parameters to it. When you configure the IP rules, you simply use this protocol name.



Description

The page contains the following:

- **Protocol Name**
  Enter a name for the protocol.

The page contains the following check boxes:

- **Select**
  Select the check box in the row to be deleted.
- **Protocol Name**
  Shows the protocol name.
- **Protocol Number**
  Enter the protocol number, for example "2". You will find list of the protocol numbers on the Internet pages of iana.org

Procedure

Create IGMP protocol

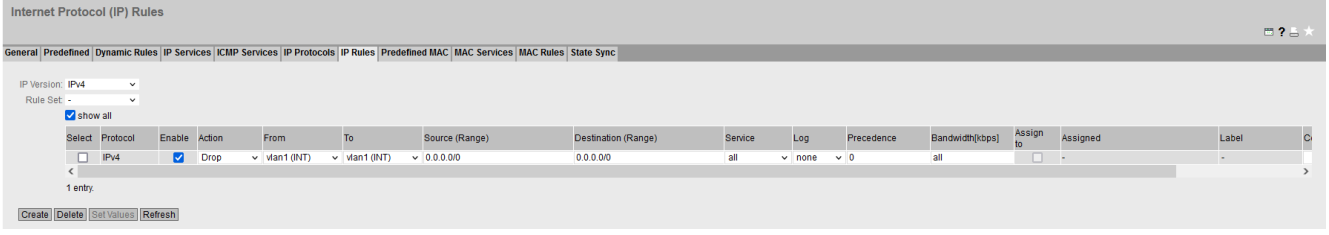
1. Enter IGMP for "Protocol Name".
2. Click the "Set Values" button. A new entry is generated in the table.
3. Enter 2 for "Protocol Number".

4.8.5.7 IP rules

On this WBM page you specify your own IP packet filter rules for the firewall.

The IP rules set here have priority:

- Over the predefined IP rules and
- Over the IP rules created automatically due to a connection configuration (SINEMA RC).



Description

- **IP Version**
  Specify the IP version to which the firewall rule applies.
  When "Any" is selected:
  - The IP version is determined automatically based on the entered source or destination IP address
  - The rule for IPv4 and IPv6 applies if no source and destination address was entered
- **Rule set**
  Select the required rule set. Only the IP rules that are assigned to this rule set will then be displayed in the table.
  Requirement: "Show all" is disabled.
  When "Any" is selected, all IPv4 and IPv6 rules are displayed.
- **Show all**
  When enabled, all available IP rules are displayed. With the "Assign" setting, you assign an IP rule to the selected rule set.

The table contains the following columns:

- **Select**
  Activate the check box in the row to be deleted.
- **Protocol**
  Shows the version of the IP protocol.
- **Enable**
  Enable or disable the firewall rules.
- **Action**
  Select how incoming IP packets are handled:
  - "Accept" – The data packets can pass through.
  - "Reject" – The data packets are rejected, and the sender receives a corresponding message.
  - "Drop" – The data packets are discarded without any notification to the sender.
- **From / To**
  Specify the communications direction of the IP rule.
  - VLANx: VLANs with configured subnet
  - NVEx: Virtual interface via which the VXLAN tunnel is established.
  - Device: Connection to the device
  - SINEMA RC: Connection to SINEMA RC Server
  - IPsec: Either all IPsec connections or a specific IPsec connection
  - OpenVPN: Either all OpenVPN connections or a specific OpenVPN connection
  - Any: All communication directions, except device.

- **Source (Range)**
  Enter the IP address or an IP range that is allowed to receive IP packets.
  - Individual IP address: Specify the IP address
  - IP range: Specify the range with start address "-" end address, e.g.
    IPv4:192.168.100.10 - 192.168.100.20
    IPv6: fe80:: - febf::
  - All IP addresses:
    IPv4: " 0.0.0.0/0"
    IPv6: "::"
    Any (IPv4 and IPv6): Empty
  - DYNAMIC
    If the rule set is activated by a user, the placeholder DYNAMIC is replaced by the IP address of the terminal device used.

    Note

    Digital input and DYNAMIC placeholder

    If the rule set is executed by controlling the digital input, the placeholder DYNAMIC is replaced by the setting for "Dynamic Source (Range)". You configure the setting in "Security > Firewall > User Specific".

- **Destination (Range)**
  Enter the IP address or an IP range that is allowed to receive IP packets.
  - Individual IP address: Specify the IP address
  - IP range: Specify the range with start address "-" end address, e.g.
    IPv4:192.168.100.10 - 192.168.100.20
    IPv6: fe80:: - febf::
  - All IP addresses:
    IPv4: " 0.0.0.0/0"
    IPv6: "::"
    Any (IPv4 and IPv6): Empty
  - If the rule set is enabled by a user, the placeholder DYNAMIC is replaced by the IP address of the end device used.
- **Service**
  Select the service or the protocol name for which this rule is valid.
- **Log**
  Specify whether or not there should be a log entry every time the rule comes into effect and specify the severity of the event.
  The following settings are available:
  - none
    The rule coming into effect is not logged.
  - info / warning / critical
    The rule coming into effect is logged with the selected event severity. The log file is displayed in "Information" > "Log Tables" > "Firewall Log".

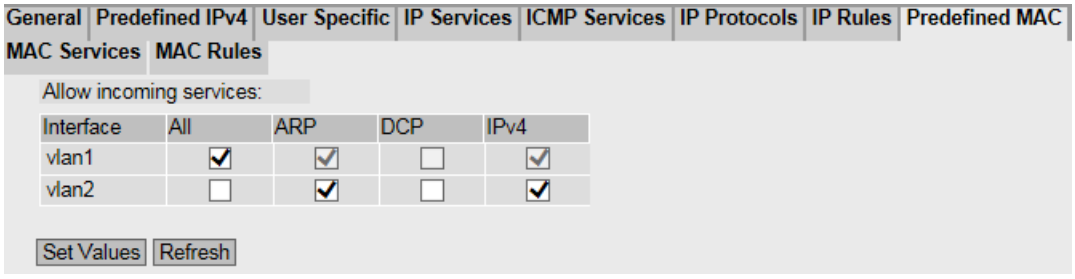
- **Precedence**
  Define the sequence in which the IP rules of the firewall are processed (ascending from 0 ... 999).
- **Bandwidth (kbps)**
  Option for setting a bandwidth limitation. Can only be set if "Accept" is selected as action. A packet passes through the firewall if the
  Accept rule applies and the permitted bandwidth for this rule has not yet been exceeded.
- **Assign**
  To assign the IP rules to the selected rule set, activate the setting for the desired IP rules and click the "Set Values" button.
- **Assigned**
  Shows the rule set to which this IP rule is assigned. The IP rules can also be assigned to multiple rule sets. If the IP rule is assigned to all rule sets, "all" is displayed.
- **Name**
  Shows who created the IP rule.
  – NETMAP - automatically created firewall rule
- **Comment**
  If needed, enter a comment.

4.8.5.8 Pre-defined MAC rules

The WBM page contains pre-defined MAC packet filter rules.

Select which incoming services the interface accepts and also forwards.

If you create your own MAC packet filter rules, these have a higher priority than the pre-defined MAC packet filter rules.

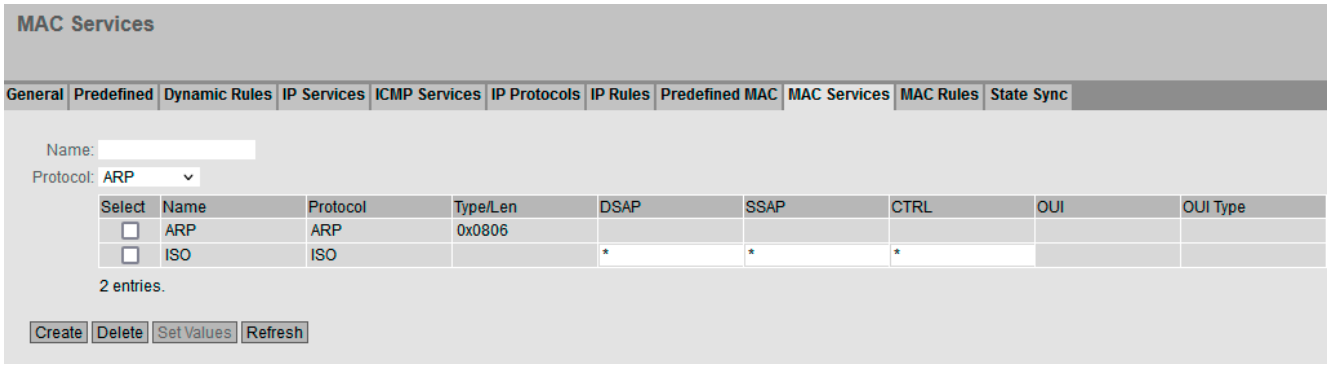


Description

- **Interface**
  Interface to which the settings relate. The list of interfaces/subnets is dynamic and is based on the settings from "Layer 3 > Subnet".
- Access to the following MAC services is permitted:
  - All
    All predefined MAC services, no filtering.
  - ARP
    Access via ARP to the device or bridged subnets is permitted.
    Changes to this setting can have the result that the device is no longer reachable.
  - DCP
    Access via DCP to the device or bridged subnets is permitted.
  - IPv4
    Access via IPv4 to the device, bridged or routed subnets is permitted.

4.8.5.9 MAC services

You define MAC services on this WBM page. Using the MAC service definitions, you can define firewall rules for specific services. You select a name and assign the service parameters to it. Simply use this name when you configure the MAC rules.



Description

The page contains the following:

- **Name**
  Enter a name for the MAC service. The name must be unique.
- **Protocol**
  Selection of the protocol type:

Protocol	Description
ARP	Frames with the following property: Ethertype=0x0806
DCP	The DCP protocol is used by SINEC PNI to set the IP parameters (node initialization) of SIMATIC NET network components.
PNIO	Frames with the following property: Ethertype = 0x8892
ISO	Frames with the following properties: Lengthfield <= 05DC (hex), DSAP=userdefined, SSAP=userdefined, CTRL=userdefined
SNAP	Frames with the following properties: Lengthfield <= 05DC (hex), DSAP=0xAA (hex), SSAP=0xAA (hex), CTRL=0x03 (hex), OUI=userdefined, OUI-Type=userdefined
Users	User-specific rules with the following inputs: Type: >=0x0600 Length: <= 0x05DC
SiClock	For filtering SiCLOCK time-of-day frames.
IPv4	Frames with the following property: Ethertype=0x0800

The table contains the following columns:

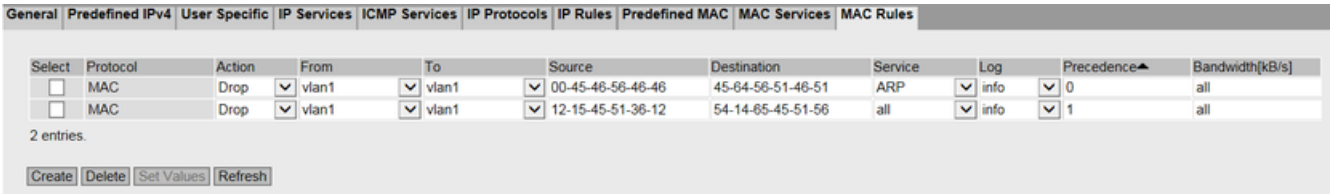
- **Select**
  Select the check box in the row to be deleted.
- **Name**
  Shows the name of the MAC service.
- **Protocol**
  Shows the name of the MAC protocol.

Depending on the protocol, the following inputs are necessary:

- For Ethernet protocols:
  - Type/length
- For ISO-LLC protocols:
  - DSAP: Destination Service Access Point: LLC receiver address
  - SSAP: Source Service Access Point: LLC sender address
  - CTRL: LLC Control Field
- For SNAP:
  - OUI: Organizationally Unique Identifier: the first three bytes of the MAC address = Manufacturer identification
  - OUI Type: Protocol type/identification

4.8.5.10 MAC rules

By default, MAC packet filter rules exist on the device that permit the exchange of ARP frames between device and vlan1 or vlan2. You can define your own ARP rules by selecting the entry "ARP" as protocol in a MAC packet filter rule. Your own ARP rules should also take into account the PC with which the device is configured.



Meaning

MAC packet filter rules are processed based on the following evaluations:

- Parameters entered in the rule
- Sequence of the rule within the rule set

Description of the displayed boxes

The table contains the following columns:

- **Select**
  Activate the check box in the row to be deleted.
- **Protocol**
  Shows the version of the MAC protocol.
- **Action**
  Select how incoming MAC packets are handled:
  - "Accept" – The data packets can pass through.
  - "Drop" – The data packets are discarded without any notification to the sender.
- **From / To**
  Specify the communications direction of the MAC rule.
  - VLANx: VLANs with configured subnets
- **Source**
  Enter the source address of the MAC packets.
- **Destination**
  Enter the destination address of the MAC packets.
- **Service**
  Select the service or the protocol name for which this rule is valid.

- **Log**
  Specify whether or not there should be a log entry every time the rule comes into effect and specify the severity of the event.
  The following settings are available:
  - none
    The rule coming into effect is not logged.
  - info / warning / critical
    The rule coming into effect is logged with the selected event severity. The log file is displayed in "Information > Log Tables > Firewall Log".
- **Precedence**
  In ascending order starting with 0, you define the sequence in which the MAC rules of the firewall are processed.
- **Bandwidth (kB/s)**
  Option for setting a bandwidth limitation. Can only be entered if "Accept" is selected for the action. A packet passes through the firewall if the Accept rule matches and the permitted bandwidth for this rule has not yet been exceeded.
- **Comment**
  If needed, enter a comment.

4.8.5.11 Firewall State Sync

On this WBM page, you set the firewall states of two SC600 that are synchronized with each other via the network.

When the firewall permits passage of a network packet, a firewall state is created for this event. This firewall state is required so that the reply to a packet can pass through the firewall without having to create an additional rule for it. Synchronization of the firewall state transfers this information to another device. In connection with VRRP, this ensures that an established connection must not be set up again but that the existing firewall state is being used.

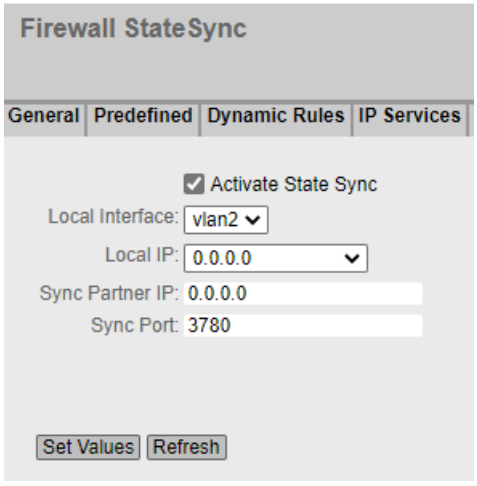
The outgoing queries are logged by the firewall in dynamic state tables. Direct queries from the external network without previous query, that is, without corresponding entry in the state table, are automatically blocked.

Note

Protect connections to the Firewall State Sync

The Firewall State Sync does not use any encryption or authentication. The connection to the synchronization between the two firewalls therefore needs to be specifically protected.

If possible, connect the two firewalls directly via dedicated VLAN interfaces. If this connection cannot be protected from external access, create an IPsec VPN connection for synchronization.



Description of the displayed boxes

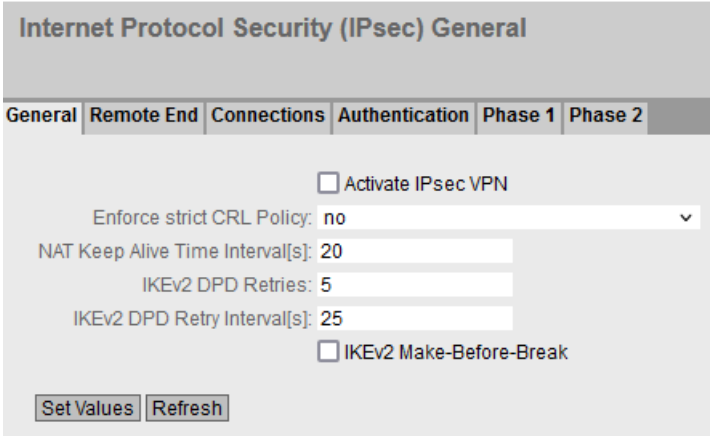
The table contains the following columns:

- **Activate State Sync**
  Activates the Firewall State Sync. When you enable this option, a firewall rule is automatically created.
- **Local Interface**
  Select the interface via which the firewall state is being sent in case of a change.
- **Local IP Address**
  Enter the IP address of the node in the local network.
- **Sync Partner IP**
  Enter the IP address of the synchronization partner.
- **Port Number Sync Partner**
  Enter the port of the synchronization partner.
  Port 3780 is assigned as default.

4.8.6 IPsec VPN (SC64x-2C)

4.8.6.1 General

On the WBM page, you configure the basic settings for VPN.



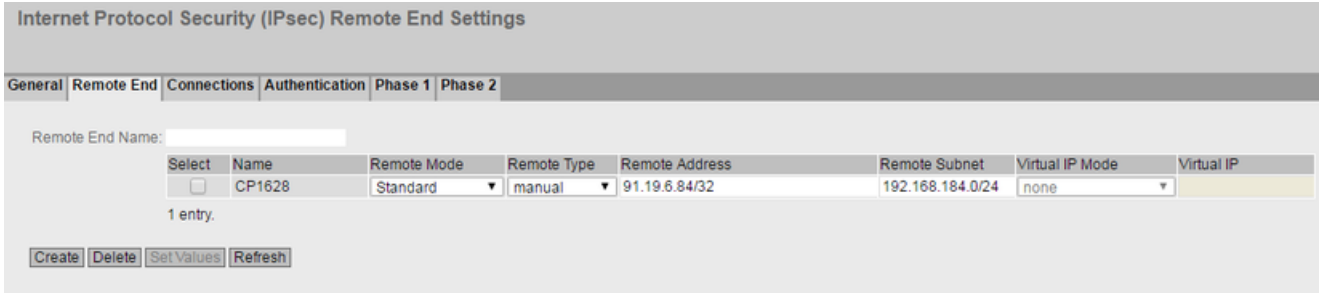
Description

The page contains the following:

- **Activate IPsec VPN**
  Enable or disable the IPsec protocol for VPN.
- **Enforce strict CRL Policy**
  When enabled, the validity of the certificates is checked based on the CRL (Certificate Revocation List). The certificate revocation list lists the certificates issued by the certification authority that have lost their validity before the set expiry date. You configure the certificate revocation list to be used on the WBM page "Certificates (Page 375)".
- **NAT Keep Alive Time Interval**
  Specify the time interval at which keep alive telegrams are sent. If there is a NAT device between two VPN endpoints, when there is inactivity, the connection is deleted from its dynamic NAT table. To prevent this, keepalives are sent.
- **IKEv2 DPD retries**
  Specify the number of allowed failed attempts after which the IKEv2 connection is considered disrupted. The setting applies to all IKEv2 connections.
- **IKEv2 DPD Retry Interval[s]**
  Specify the interval at which the failed attempts are sent.
- **IKEv2 Make-Before-Break**
  When enabled, a duplicate of the IKE and all IPSec security assignments is created and the old ones are deleted. This prevents interruptions in VPN communication from occurring during reauthentication. This setting requires that both VPN endpoints can process overlapping SAs

4.8.6.2 Remote End

On this WBM page, you configure the partner (VPN end point).



Description

The page contains the following:

- **Remote End Name**
  Enter the name of the remote station and click "Create" to create a new remote station.

The table contains the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **Name**
  Shows the name of the partner.
- **Remote Mode**
  Specify the role the remote stations will adopt.
  - Roadwarrior
    The reachable remote addresses are entered. The reachable remote subnets are learned from the partner.
  - Standard
    The reachable remote address and the reachable remote subnets are entered permanently.
- **Remote Type**
  Specify the type of remote station address.
  - Manual
    The address of the partner is known. The device can establish the VPN connection at this remote end either actively as a VPN client or wait passively for connection establishment by the partner.
  - Any
    Accepts the connection from remote stations with any IP address. The device can only wait for VPN connections at this remote end but cannot establish a VPN tunnel as the active partner.

- **Remote Address**
  Can only be edited with the remote type "Manual".
  - In standard mode, enter the WAN IP address or the DDNS host name of the partner. The network mask is always /32
  - In Roadwarrior mode, you can specify either the address of the partner or enter an IP range from which connections will be accepted.
- **Remote Subnet**
  - In standard mode, enter the remote subnet of the remote station. Use the CIDR notation. Multiple subnets can be used only with IKEv2. In this case, enter the subnets separated by a comma.
  - In Roadwarrior mode, the remote station informs the device of its accessible subnets and the device learns them.
- **Virtual IP Mode**
  Specify whether or not the remote station is offered a virtual IP address.
  The following options are available:
  - User defined IPv4
    The virtual IP address is from the band specified in "Virtual IP".
  - None
    No virtual IP address. The VPN tunnel is established dynamically to the internal IP address of the remote station.
- **Virtual IP**
  Specify the subnet (CIDR) from which the remote station is offered a virtual IP address.
  Can only be edited if "user defined IPv4" is selected in "Virtual IP Mode".

Procedure

Configure VPN standard mode

1. Enter the name of the remote station in "Remote End Name".
2. Click the "Create" button. A new entry is generated in the table.
3. For "Remote Mode", select "Standard".
4. For "Remote Type", select "manual".
5. In "Remote Address", enter the WAN IP address and in "Remote Subnet" the subnet of the remote station.
6. Click the "Set Values" button.

Configure VPN Roadwarrior mode

1. Enter the name of the remote station in "Remote End Name".
2. Click the "Create" button. A new entry is generated in the table.
3. For "Remote Mode", select "Roadwarrior".
4. For "Remote Type", select "Any".
5. In "Remote Address", enter the IP address of the remote network.

6. In "Virtual IP Mode", specify how the IP address of the VPN gateway is obtained.
7. Click the "Set Values" button.

4.8.6.3 Connections

On the WBM page, you configure the basic settings for the VPN connection. With these settings, the device (local endpoint) can establish a secure VPN tunnel to the partner. You specify the security settings on the WBM page "Authentication".

Note

Several IPsec VPN connections via the same VPN endpoint

If you have created IPsec VPN connections to different remote subnets via the same VPN endpoint, the first configured VPN connection (lowest index) is the main connection (parent).

Via the main connection all other IPsec VPN connections (children) are created and established. If all VPN tunnels are now established and the main (parent) connection is terminated all child connections are interrupted. After the DPD timeout has expired, all IPsec VPN connections are reestablished via the main connection.

If only one child connection is terminated, the parent connection and the other child connections are retained.

Note

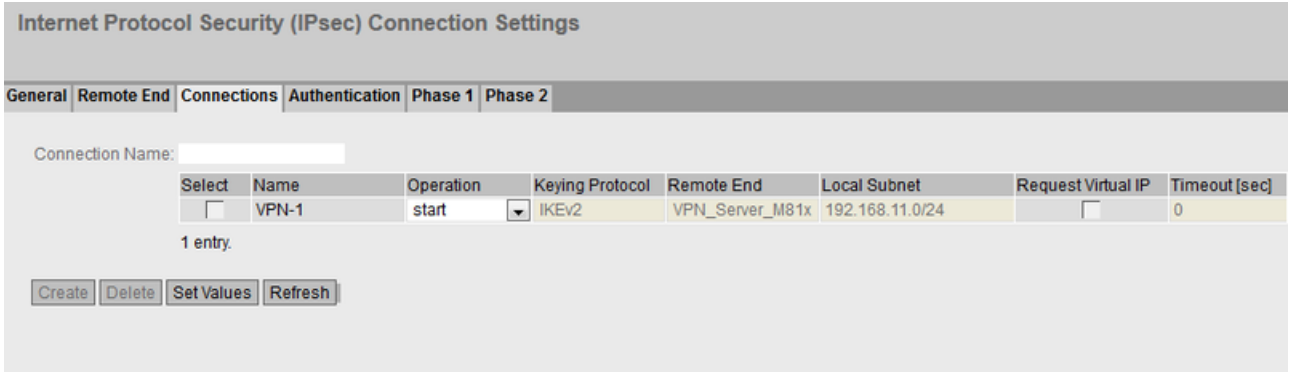
IPsec: Restrictions for phase 2 connections

Create a maximum of 20 phase 2 connections per phase 1 (Remote End).

Note

If you use "NETMAP"

- only "Auto Firewall Rules" are supported.
- For "Operation" the setting "on demand" cannot be selected.



Description

The page contains the following boxes:

- **Connection name**
  Enter a name for the VPN connection and click "Create" to create a new connection.

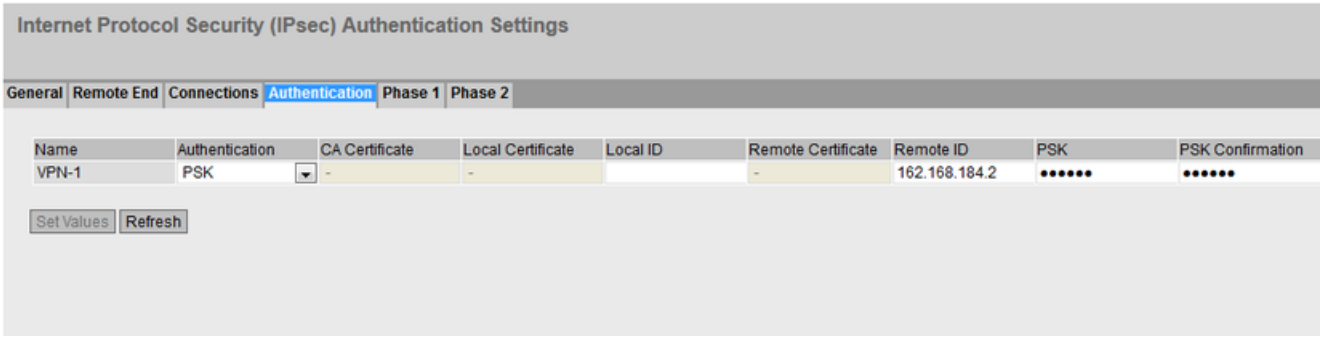
The table contains the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **Name**
  Shows the name of the VPN connection.
- **Operation**
  Specify who establishes the VPN connection. You will find more detailed information in "Technical basics > VPN connection establishment (Page 71)".
  - Disabled
    The VPN connection is disabled.
  - start
    The device attempts to establish a VPN connection to the partner.
  - wait
    The device waits for the partner to initiate the connection establishment.
  - on demand
    The VPN connection is established when necessary.
  - start on DI
    If the event "Digital In" occurs, the device attempts to establish a VPN connection to the partner.
    This is on condition that the event "Digital In" is forwarded to the VPN connection. For this purpose, enable "VPN tunnel" for the "Digital In" event under "System" > "Events" > "Configuration".
  - wait on DI
    If the event "Digital In" occurs, the device waits for the partner to initiate connection establishment.
    This is on condition that the event "Digital In" is forwarded to the VPN connection. This is on condition that the event "Digital In" is forwarded to the VPN connection. For this purpose, enable "VPN tunnel" for the "Digital In" event under "System" > "Events" > "Configuration".
- **Keying Protocol**
  Specify whether IKEv2 or IKEv1 will be used.
- **Tunnel Interface**
  Select the interface via which the VPN tunnel is established. With the default value "auto", the interface is automatically determined via the routing.
- **Remote End**
  Select the required remote station. Only partners that have been configured on the "Remote End" WBM page can be configured.

- **Local Subnet**
  Enter the local subnet. Use the CIDR notation. The local network can also be a single PC or another subset of the local network. Multiple subnets can be used only with IKEv2. In this case, enter the subnets separated by a comma.
- **Request Virtual IP**
  When enabled, a virtual IP address is requested from the remote station during connection establishment.
- **Timeout [s]**
  Only necessary with the "on demand" setting. Enter the interval after which the VPN connection will be terminated. If no packets are sent during this time, the VPN connection is automatically terminated.

4.8.6.4 Authentication

On this WBM page, you specify how the VPN connection partners authenticate themselves with each other.



Description

The table contains the following columns:

- **Name**
  Shows the name of the VPN connection to which the settings relate.
- **TLS Auth. Key**
  Select the key file used to sign the TLS packets. If the incoming TLS packets are not signed with this key, they are discarded.
- **Direction**
  Specify the direction. If you select 0, 1 must be set on the partner and vice versa. With this setting, you restrict the clients that can authenticate themselves.
  Select "none" if nothing is set on the OpenVPN server. With "none", this setting is disabled.

- **Method**
  Select the authentication method. For the VPN connection, it is essential that the partner uses the same authentication method.
  - Disabled
    No authentication method is selected. Connection establishment is not possible.
  - Certificates
    Certificates are used for the authentication.
  - User name / Password
    The user name / password are used for the authentication.
  - Cert/User Name/Password
    For authentication, a user name and password are required in addition to the certificate. The VPN connection is established only if both operations are successful.

  Note

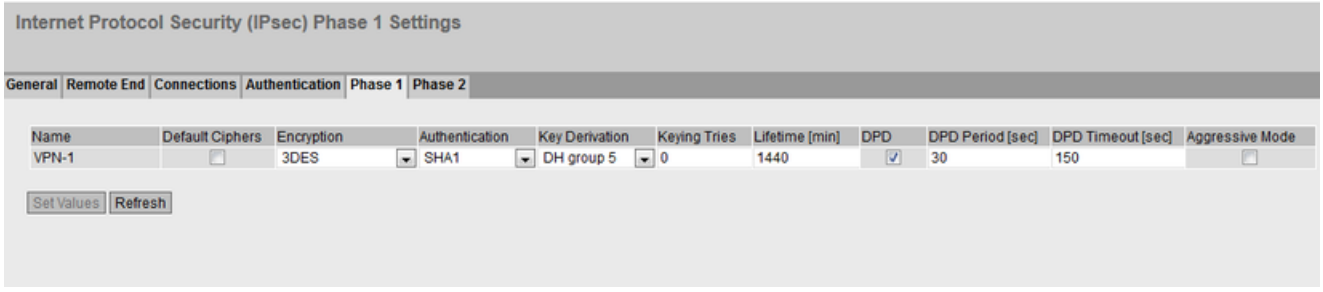
  For the "PSK" authentication method, specify the "Local ID" and "Remote ID". If the entries remain empty, IPsec uses the IP address of the interface as the ID and prevents the VPN tunnel from being set up.

- **CA Certificate**
  Select the certificate. Only loaded certificates can be selected.
  You load the certificates into the device with "System > Load&Save". The loaded certificates and key files are shown on the WBM page "Security > Certificates".
- **Machine Certificate**
  Select the machine certificate. Only loaded certificates can be selected.
  You load the certificates into the device with "System > Load&Save". The loaded certificates and key files are shown on the WBM page "Security > Certificates".
- **User Name**
  Specify the user name.
- **Password**
  Specify the password.
- **Password Confirmation**
  Repeat the password.

4.8.6.5 Phase 1

Phase 1: Encryption agreement and authentication (IKE = Internet Key Exchange)

On this WBM page, you set the parameters for the protocol of the IPsec key management. The key exchange uses the standardized IKE method for which you can set the following protocol parameters.



Description

The table contains the following columns:

- **Name**
  Shows the name of the VPN connection to which the settings relate.
- **Default Ciphers**
  When enabled, a preset list is transferred to the VPN connection partner during connection establishment. The list contains combinations of the three algorithms (Encryption, Authentication, Key Derivation). To establish a VPN connection, the VPN connection partner must support at least one of these combinations. The selection depends on the key exchange method. Additional information can be found in the section "IPsec VPN (Page 67)".
- **Encryption**
  For phase 1, select the required encryption algorithm. Can only be selected if "Default Ciphers" is disabled.
  The selection depends on the key exchange method. Additional information can be found in the section "IPsec VPN (Page 67)".

  Note

  The AES modes CCM and GCM contain separate mechanisms for authenticating data. If you use a mode AES x CCM for "Encryption", this is also used for authentication. Then only the pseudo random function will be derived from the "Authentication" parameter. So that a VPN connection can be established, all devices need to use the same settings.

- **Authentication**
  Specify the method for calculating the checksum. Can only be selected if "Default Ciphers" is disabled.
  The following methods are supported:
  - MD5
  - SHA1
  - SHA512
  - SHA256
  - SHA384
- **Key derivation**
  Select the required Diffie-Hellmann group (DH) from which a key will be generated. Can only be selected if "Default Ciphers" is disabled.
  The following DH groups are supported:
  - DH group 1
  - DH group 2
  - DH group 5
  - DH group 14
  - DH group 15
  - DH group 16
  - DH group 17
  - DH group 18
- **Keying Tries**
  Enter the number of repetitions for a failed connection establishment. If you enter the value 0, the connection establishment will be attempted endlessly.
- **Lifetime [min]**:
  Enter a period in minutes to specify the lifetime of the authentication. When the time has elapsed, the VPN endpoints involved must authenticate themselves with each other again and generate a new key
- **DPD**
  When enabled, DPD (Dead Peer Detection) is used. Using DPD, it is possible to find out whether the VPN connection still exists or whether it has aborted.

  Note

  Sending DPD queries increases the amount of data sent and received. This can lead to increased costs

- **DPD Period [sec]**
  Enter the period after which DPD requests are sent. These queries test whether or not the remote station is still available

- **DPD Timeout [sec]**
  Enter a period. If there is no response to the DPD queries, the connection to the remote station is declared to be invalid after this time has elapsed.

  Note

  To avoid unwanted connection breakdowns, set the DPD timeout significantly higher than the DPD period. We recommend setting it at least 2 minutes longer than the DPD period.

- **Aggressive Mode**
  - disabled:
    Main Mode is used.
  - enabled
    Aggressive Mode is used

  The difference between main and aggressive mode is the "identity protection" used in main mode. The identity is transferred encrypted in main mode but not in aggressive mode.

4.8.6.6 Phase 2

Phase 2: Data exchange (ESP = Encapsulating Security Payload)

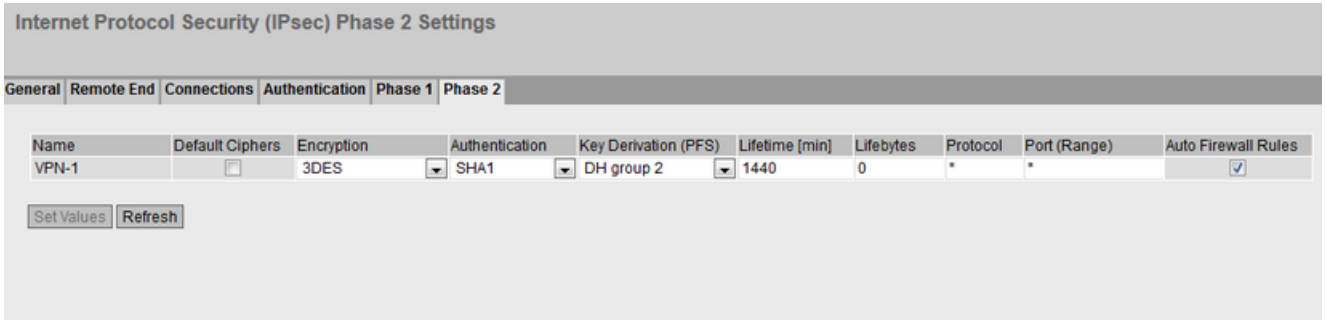
On this WBM page, you set the parameters for the protocol of the IPsec data exchange.

Note

Number of phase 2 SA

You can create 20 phase 2 SAs per phase 1 SA.

The entire communication during this phase is encrypted using the standardized security protocol ESP for which you can set the following protocol parameters.



Description

The table contains the following columns:

- **Name**
  Shows the name of the VPN connection to which the settings relate.
- **Default Ciphers**
  When enabled, a preset list is transferred to the VPN connection partner during connection establishment. The list contains combinations of the three algorithms (Encryption, Authentication, Key Derivation). To establish a VPN connection, the VPN connection partner must support at least one of these combinations. Additional information can be found in the section "IPsec VPN (Page 67)".
- **Encryption**
  For phase 2, select the required encryption algorithm. Can only be selected if "Default Ciphers" is disabled.
  Additional information can be found in the section "IPsec VPN (Page 67)".

  Note

  The AES modes CCM and GCM contain separate mechanisms for authenticating data. If you use a mode AES x CCM or AES x GCM for "Encryption", this will also be used for authentication. Then only the pseudo random function will be derived from the "Authentication" parameter.

- **Authentication**
  Specify the method for calculating the checksum. Can only be selected if "Default Ciphers" is disabled.
  The following methods are supported:
  - MD5
  - SHA1
  - SHA512
  - SHA256
  - SHA384

- **Key Derivation (PFS)**
  Select the required Diffie-Hellmann group (DH) from which a key will be generated. Can only be selected if "Default Ciphers" is disabled.
  The following DH groups are supported:
  - None: For phase 2, no separate keys are exchanged. This means that Perfect Forward Secrecy (PFS) is disabled.
  - DH group 1
  - DH group 2
  - DH group 5
  - DH group 14
  - DH group 15
  - DH group 16
  - DH group 17
  - DH group 18

  Note

  So that a VPN connection can be established, all devices need to use the same settings or provide compatible key procedures.

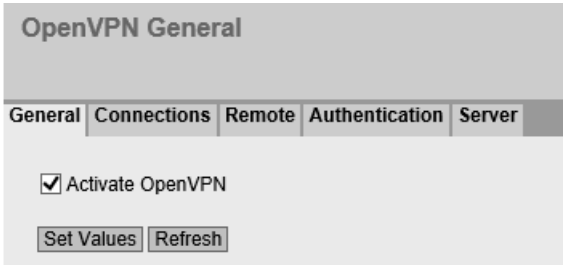
- **Lifetime [min]**:
  Enter a period in minutes to specify the lifetime of the agreed keys. When the time expires, the key is renegotiated.
- **Lifebytes**
  Enter the data limit in bytes that specifies the lifetime of the agreed key. When the data limit is reached, the key is renegotiated.
- **Protocol**
  Specify the protocol for which the VPN connection is valid e.g. UDP, TCP, ICMP. If the setting is intended to apply to all protocols, enter "*".
- **Port (Range)**
  Specify the port via which the VPN tunnel can communicate. The setting applies specifically to the specified port
  - If the setting is intended to apply to a port range, enter the range with start port "-" end port, for example 30 - 40.
  - If the setting is intended to apply to all ports, enter "*".

  The setting is only effective for port-based protocols.
- **Auto Firewall Rules**
  - enabled
    For the VPN connection, the firewall rules for access from "External" to "Internal" and vice versa are created automatically. You can enable access to specific services of the device under "Security" > "Firewall" > "Predefined IPv4". Ping is enabled by default.
  - disabled
    You will need to create the firewall rules yourself.

4.8.7 OpenVPN

4.8.7.1 General

On this WBM page, you enable the OpenVPN functionality.



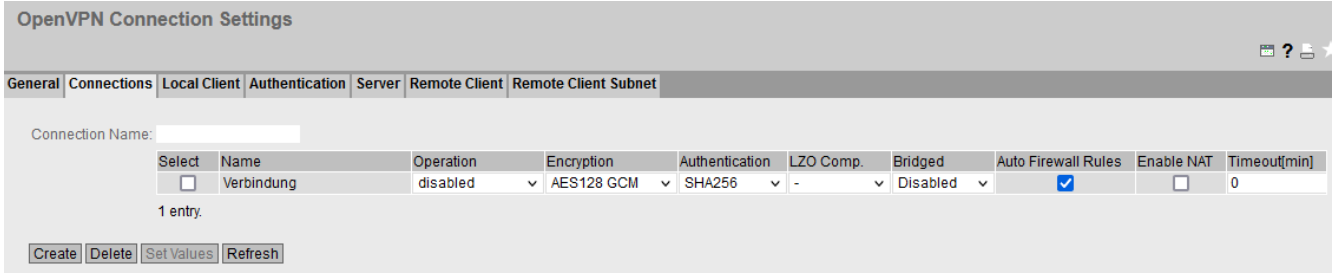
Description

The page contains the following:

- **Activate OpenVPN**
  Enable or disable OpenVPN.

4.8.7.2 Connections

On this WBM page, you configure the basic settings for the OpenVPN connection. You specify the security settings on the WBM page "Authentication".



Description

- **Connection name**
  Enter a unique name for the OpenVPN connection and click "Create" to create a new connection.

The table contains the following columns:

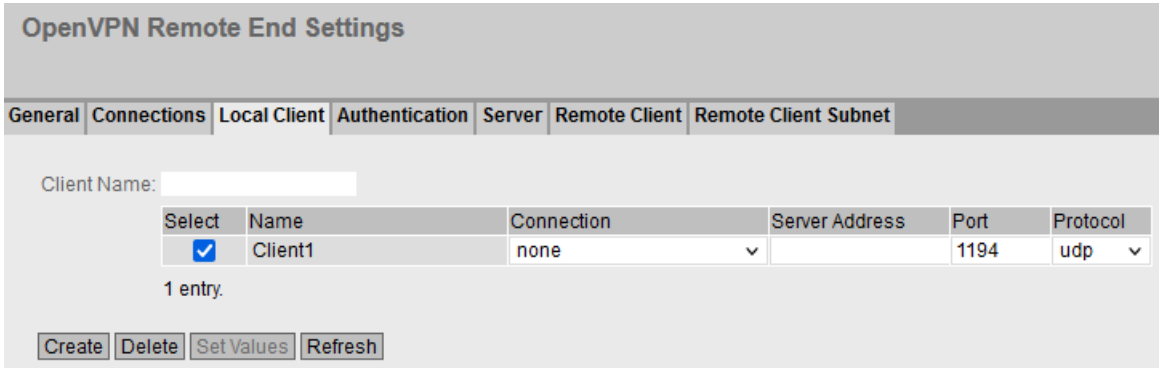
- **Select**
  Select the check box in the row to be deleted.
- **Name**
  Shows the name of the OpenVPN connection.

- **Operation**
  Specify how the connection is established.
  - start
    The device attempts to establish a VPN connection to the partner.
  - start on DI
    If the event "Digital In" occurs, the device attempts to establish a VPN connection to the partner.
    This is on condition that the event "Digital In" is forwarded to the VPN connection. To do this in "System > Events> Configuration" activate "VPN Tunnel" for the "Digital In" event.
  - Disabled
    The VPN connection is disabled.
- **Encryption**
  Select the required encryption algorithm.
  - AES-128-CBC (Default)
  - AES-192-CBC
  - AES-256-CBC
  - AES-128-GCM
  - AES-256-GCM
  - DES-EDE3
  - BF-CBC
- **Authentication**
  Specify the method for calculating the checksum.
  - SHA256 (default)
  - SHA384
  - SHA512
  - SHA224
  - SHA1
  - MD5
- **LZO Comp.**
  - Disabled (-)
    The compression is disabled. The server cannot enable compression again.
  - No
    The compression is disabled as default. The server can enable compression.
  - Yes
    The compression is enabled as default. The server can disable the compression.
  - Self-adjusting
    As default compression is activated adaptively. Compression is only used when the data is good to compress; otherwise, compression is deactivated for a certain time.

- **Bridged**
  Select the bridge ID via which the Layer2 OpenVPN connection should run. One bridge ID can be used for multiple connections. For Layer 3 OpenVPN connections, select "disabled".
- **Auto Firewall Rules**
  - Enabled
    For the VPN connection, the firewall rules for access from "External" to "Internal" and vice versa are created automatically. In addition to this, access from the device to the outside is allowed. You can enable access to specific services of the device under "Security > Firewall > Predefined". Ping is enabled by default.
  - Disabled
    You will need to create the suitable firewall rules yourself.
- **Enable NAT**
  With this setting, you enable automatic IP masquerading for this interface. The local devices are not directly reachable from the outside, but only via the IP address of the interface. The local devices can, however, connect to the devices downstream from the OpenVPN server.
- **Timeout [min]**
  Specify the period of time in minutes. If no data exchange takes place, when this time has elapsed the VPN tunnel is automatically terminated.

4.8.7.3 Client

On this WBM page, you can create multiple OpenVPN clients per connection. The device attempts to establish a connection to the individual clients.



Description

The page contains the following:

- **Client Name**
  Enter a name for the OpenVPN client and click "Create".

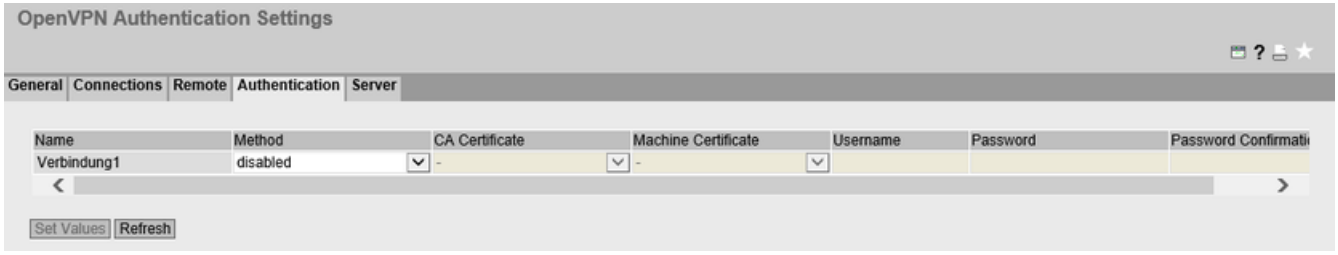
The table contains the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **Name**
  Shows the name of the Open VPN partner.

- **Connection**
  Select the corresponding connection. Only connections can be configured that have been configured on the "Connections" WBM page.
- **Server Address**
  Enter the WAN IP address or the DNS host name of the OpenVPN partner.
- **Port**
  Specify the port via which the OpenVPN tunnel can communicate. The setting applies specifically to the specified port.
- **Protocol**
  Specify the protocol for which the OpenVPN connection will be used.

4.8.7.4 Authentication

On this WBM page, you specify how the VPN connection partners authenticate themselves with each other.



Description

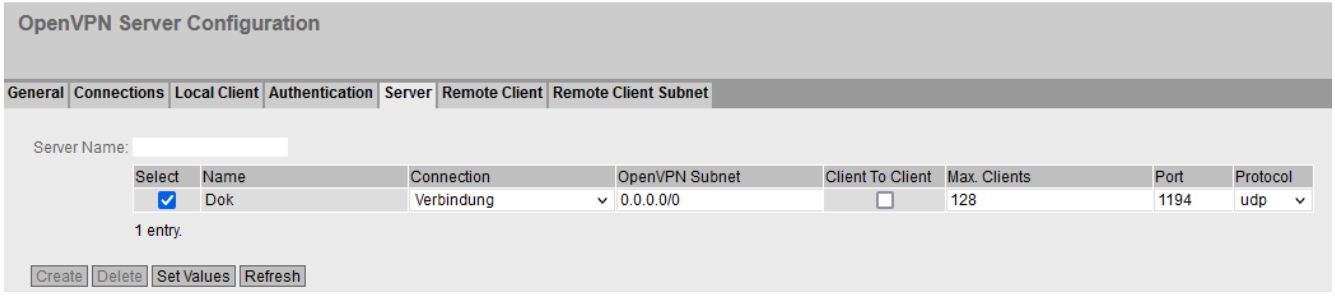
The table contains the following columns:

- **Name**
  Shows the name of the VPN connection to which the settings relate.
- **TLS Auth. Key**
  Select the key file used to sign the TLS packets. If the incoming TLS packets are not signed with this key, they are discarded.
- **Direction**
  Specify the direction. If you select 0, 1 must be set on the partner and vice versa. With this setting, you restrict the clients that can authenticate themselves.
  Select "none" if nothing is set on the OpenVPN server. With "none", this setting is disabled.

- **Method**
  Select the authentication method. For the VPN connection, it is essential that the partner uses the same authentication method.
  - Disabled
    No authentication method is selected. Connection establishment is not possible.
  - Certificates
    Certificates are used for the authentication.
  - User name / Password
    The user name / password are used for the authentication.
  - Cert/User Name/Password
    For authentication, a user name and password are required in addition to the certificate. The VPN connection is established only if both operations are successful.
- **CA Certificate**
  Select the certificate. Only loaded certificates can be selected.
  You load the certificates into the device with "System > Load&Save". The loaded certificates and key files are shown on the WBM page "Security > Certificates".
- **Machine certificate**
  Select the machine certificate. Only loaded certificates can be selected.
  You load the certificates into the device with "System > Load&Save". The loaded certificates and key files are shown on the WBM page "Security > Certificates".
- **User Name**
  Specify the user name.
- **Password**
  Specify the password.
- **Password Confirmation**
  Confirm the password.

4.8.7.5 Server

On this WBM page, you can create multiple OpenVPN servers per connection.



Description

The page contains the following:

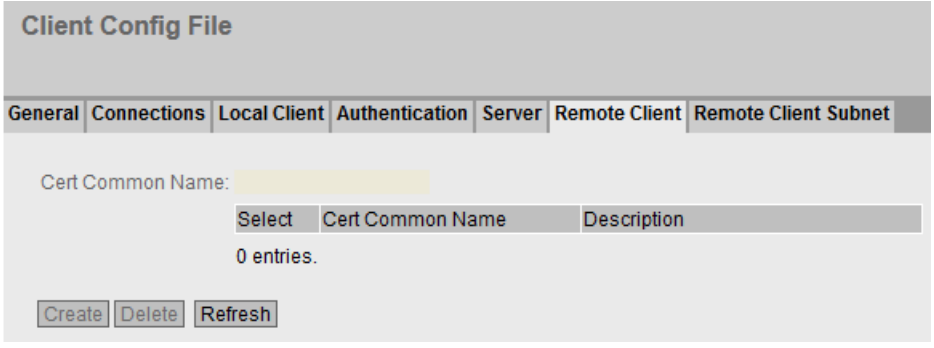
- **Name**
  Enter a name for the OpenVPN server and click "Create".

The table contains the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **Name**
  Shows the name of the OpenVPN server.
- **Connection**
  Select the corresponding connection. Only connections can be configured that have been configured on the "Connections" WBM page.
- **OpenVPN subnet**
  IP address range from which the OpenVPN clients connected to the server obtain their tunnel IP address. The first IP address of this range is assigned to the OpenVPN server.
- **Client to Client**
  Can only be set for Layer 2 OpenVPN server.
  When enabled, communication between L2 OpenVPN clients is possible.
- **Max. Clients**
  Select the maximum number of clients to which the server can establish a connection at the same time.
- **Port**
  Specify the port via which the OpenVPN tunnel can communicate. The setting applies specifically to the specified port.
- **Protocol**
  Specify the protocol for which the OpenVPN connection will be used.

4.8.7.6 Remote client

On this WBM page, you define which OpenVPN clients are permitted to connect to the server.



Description

The page contains the following:

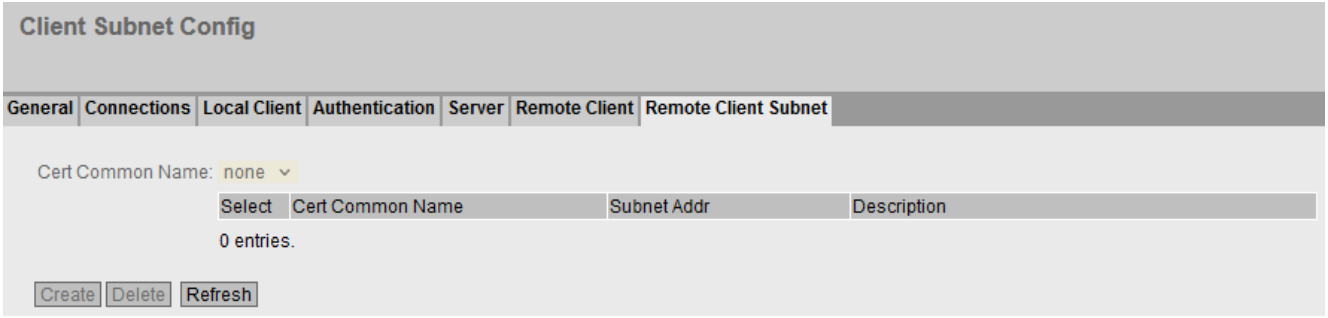
- **Cert CN**
  Enter the "Common Name" from the certificate of the OpenVPN client which is to connect to the server. Then click "Create".

The table contains the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **Cert CN**
  Shows the "Common Name" from the client certificate.
- **Description**
  Enter a description for the "Common Name".

4.8.7.7 Remote client subnet

On this WBM page, you specify the remote subnets in which the server is permitted to communicate.



Description

The page contains the following:

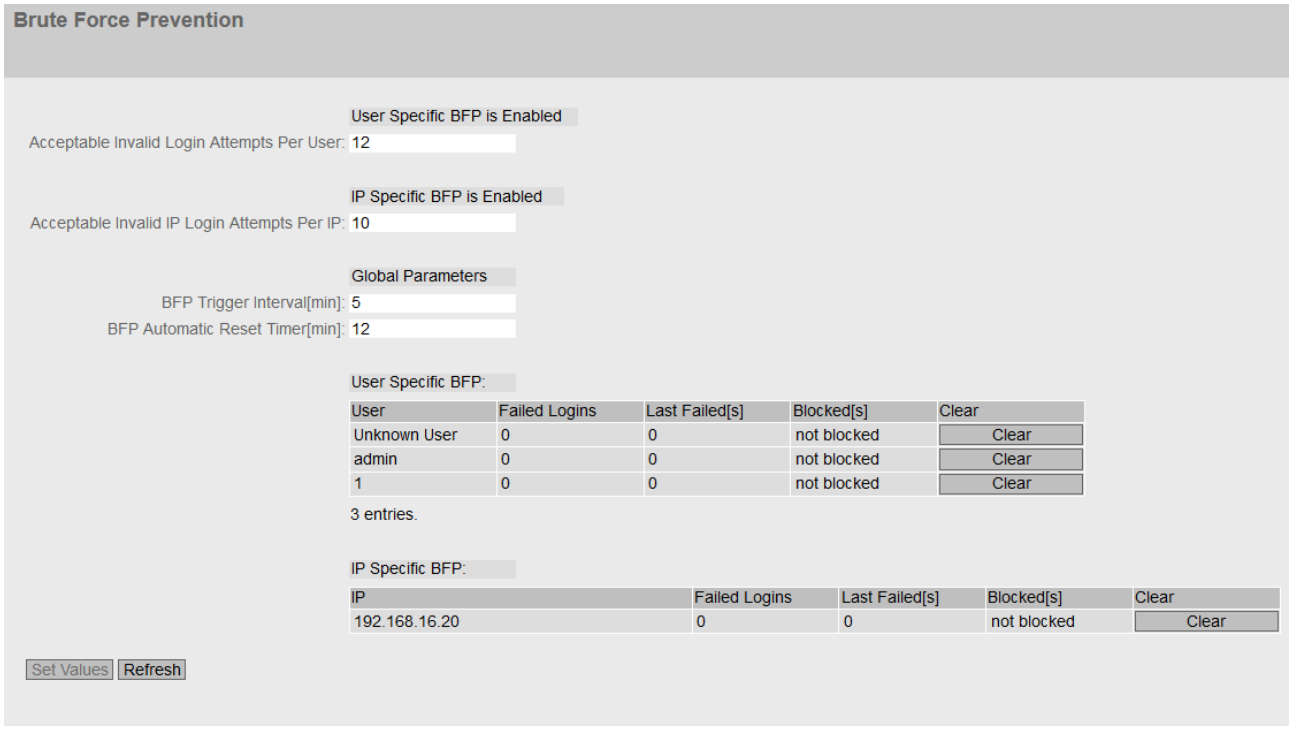
- **Cert CN**
  Select the "Common Name" of the client for which you want to define the subnet to be reached.

The table contains the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **Cert CN**
  Shows the selected "Common Name".
- **Subnet Address**
  Enter the address of the subnet to be connected to the server.
- **Description**
  Shows the description for the "Common Name".

4.8.8 Brute Force Prevention

Brute Force Prevention (BFP) refers to the protection of the device from unauthorized access by trying a sufficiently large number of passwords. The number of incorrect login attempts within a specific time period is limited for this purpose.



Description

The page contains the following boxes:

- **User Specific BFP is Enabled. / User Specific BFP is Disabled.**
  - Enabled:
    With login authentication, the "Local" or "Local and RADIUS" mode is set and the maximum number of invalid login attempts is greater than 0.
  - Disabled:
    With login authentication, the "RADIUS" or "RADIUS and fallback Local" mode is set or the maximum number of invalid login attempts is 0.

  You configure the login authentication under "Security > AAA > General > Login Authentication".
- **Acceptable Invalid Login Attempts Per User**
  The maximum number of invalid login attempts for a user accepted by the device. Further login attempts for this user are blocked for a specific time.
  The users that are not configured as local users for the device are summarized under the user name "UnknownUser".
  0: User Specific BFP is Disabled.

- **IP Specific BFP is Enabled. / IP Specific BFP is Disabled.**
  Shows whether the IP-specific Brute Force Prevention is enabled.
- **Acceptable Invalid Login Attempts Per IP**
  The maximum number of invalid login attempts for an IP address accepted by the device. Further login attempts for this IP address are blocked for a specific time.
  0: IP Specific BFP is Disabled.
- **Trigger Interval BFP [min]**
  The time in minutes that is relevant for counting invalid login attempts.
  If the maximum number of invalid login attempts is exceeded during this time, the device blocks login for a specific period of time.
  Invalid login attempts per user and per IP address are handled independently of one another.
- **BFP Automatic Reset Timer [min]**
  Time in minutes for which the device blocks login because the maximum number of invalid login attempts was exceeded.
  0: The timer is disabled.

The **User Specific BFP** table has the following columns:

- **User**
  The users configured locally on the device. The users that are not locally configured on the device are summarized under the user name "UnknownUser".
- **Failed Logins**
  The number of failed login attempts.
- **Last Failed [s]**
  Time in seconds (s) since the last failed login attempt. To display the current value, click the "Refresh" button.
- **Blocked [s]**
  The time in seconds (s) until the blocking will be removed. To display the current value, click the "Refresh" button.
  When a blocked user attempts to log in before the timer expires, the timer restarts.
- **Delete**
  Ends blocking for the user and resets the displays in the "Last Failed [s]" and "Blocked [s]" boxes.

The **IP Specific BFP** table has the following columns:

- **IP**
  The IP address of the device for the login attempt.
- **Failed Logins**
  The current number of failed login attempts.
- **Last Failed [s]**
  Time in seconds (s) since the last failed login attempt. To display the current value, click the "Refresh" button.

- **Blocked [s]**
  The time in seconds (s) until the blocking will be removed. To display the current value, click the "Refresh" button.
  When a blocked IP address attempts to log in before the timer expires, the timer restarts.
- **Delete**
  Ends blocking for the IP address and resets the displays in the "Last Failed [s]" and "Blocked [s]" boxes.

Upkeep and maintenance 5

5.1 Device configuration with PRESET-PLUG

Please not the additional information and security notes in the operating instructions of your device.

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

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

The PRESET PLUG is write-protected.

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

Creating a PRESET-PLUG

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

Note

Using configurations with DHCP

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

You assign fixed IP addresses extra following the basic installation.

Requirement

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

Procedure

1. Start the remote configuration using CLI and log on as a user with the "admin" role.
   The CLI connection works either with Telnet (port 23) or SSH (port 22).
2. Switch to the global configuration mode with the command "configure terminal".
3. You change to the PLUG configuration mode with the "plug" command.
4. Create the PRESET-PLUG with the "presetplug" command.
   The firmware version of the device and the current device configuration incl. user accounts and certificates are stored on the PLUG and the PLUG is then write protected.
5. Turn off the power to the device.

6. Remove the PRESET-PLUG.
7. Start the device either with a new PLUG inserted or with the internal configuration.

Procedure for installation with the aid of the PRESET-PLUG

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

Note

KEY-PLUG

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

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

Note

Restore factory defaults and restart with a PRESET PLUG inserted

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

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

Formatting a PRESET-PLUG (resetting the preset function)

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

1. Start the remote configuration using Telnet (CLI) and log on with a user with the "admin" role.
2. Switch to the global configuration mode with the command "configure terminal".

3. You change to the PLUG configuration mode with the "plug" command.
4. Enter the command "factoryclean".
   The PRESET-PLUG is formatted and the preset function is reset.
5. Write the current configuration of the device with the "write" command.

Firmware

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

5.2 Firmware update using WBM not possible

Cause

If there is a power failure during the firmware update, it can occur that the device is no longer accessible using WBM and CLI.

Requirement

- The PC is connected to the device via the interfaces (P0.1 - P0.6).
- A TFTP client is installed on the PC and the firmware file is available.

Solution

You can then also transfer firmware to the device using TFTP.
Follow the steps below to load new firmware using TFTP:

1. When starting up press the SET button.
2. Hold down the button until the red fault LED (F) starts to flash after approximately 3 seconds.

   Note

   If you hold down the SET button for approximately 10 seconds, the device is reset to its factory settings.

3. Now release the button. The bootloader waits in this state for a new firmware file that you can download by TFTP.

   Note

   If you want to exit the bootloader without making changes, press the SET button briefly. The device restarts with the loaded configuration.

4. Connect a PC to the device over the Ethernet interface (P0.1 - P0.6).
5. Open a DOS box, change to the directory where the new firmware file is located and then execute the command "tftp -i <ip address> PUT <firmware>". As an alternative, you can use a different TFTP client.
   If you are not sure that the IP address is correct, you can check this, for example with SINEC PNI.

Note

Using TFTP

If you want to access TFTP in Windows 7, make sure that the corresponding Windows function is enabled in the operating system.

Result

The firmware is transferred to the device.

Note

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

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

Requirement

- The device has an IP address.
- The user is logged in with administrator rights.

Firmware update via HTTP

1. Click "System > Load&Save" in the navigation area. Click the "HTTP" tab.
2. Click the "Upload" button next to "Firmware".
3. Go to the storage location of the firmware file.
4. Click the "Open" button in the dialog. The file is uploaded.

Firmware update via TFTP

1. Click "System > Load&Save" in the navigation area. Click the "TFTP" tab.
2. Enter the IP address of the TFTP server in the "TFTP Server Address" input box.
3. Enter the server port in the "TFTP Server Port" input box.
4. Select the action "Load file" in the "Firmware" table row. Make sure that the file name is correct.
5. Click the "Set Values" button. The file is uploaded.

Firmware update via SFTP

1. Click "System > Load&Save" in the navigation area. Click the "SFTP" tab.
2. Enter the IP address of the SFTP server in the "SFTP Server Address" input box.
3. Enter the server port in the "SFTP Server Port" input box.
4. Select the action "Load file" in the "Firmware" table row. Make sure that the file name is correct.
5. Click the "Set Values" button. The file is uploaded.

Result

When the firmware is successfully loaded, a dialog is displayed. Confirm the dialog with "OK". The device is restarted.

In "Information > Versions" there is the additional entry "Firmware_Running". Firmware_Running shows the version of the current firmware. For "Firmware", the firmware version stored after loading the firmware is displayed.

Hardware	Name	Revision	Order ID
Basic Device	SCALANCE SC646-2C	1	6GK5 646-2GS00-2AC2

Software	Description	Version	Date
Firmware	SCALANCE S600 Firmware DEV-SIG	T02.01.00.00_35.00.00	03/18/2020 00:00:00
Bootloader	SCALANCE S600 Bootloader	V02.06.00	12/04/2019 10:05:00
Firmware_Running	Current running Firmware	T02.01.00.00_35.00.00	03/18/2020 00:00:00

Refresh

5.3 Restoring the factory settings

NOTICE
Previous settings If you reset, all the settings you have made will be overwritten by factory defaults.

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

With the reset button

When pressing the button, remember the information in the section "Reset button" in the operating instructions.

Follow the steps below to reset the device parameters to the factory settings:

1. Turn off the power to the device.
2. Now press the Reset button and reconnect the power to the device while holding down the button.
3. Hold down the button until the red fault LED (F) stops flashing after approximately 10 seconds and is permanently lit.
4. Now release the button and wait until the fault LED (F) goes off again.
5. The device then starts automatically with the factory settings.

Via the configuration

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

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

Exchange of configuration data with STEP7 6

6.1 Exchange of configuration data with STEP 7 Basic/Professional using a file

You use the two file types "RunningSINEMAConfig" and "SINEMAConfig" ("System > Load&Save > HTTP/TFTP/SFTP") to exchange configuration data between a device (WBM) and STEP7 Basic/Professional using a file. The export/import of a file via STEP 7 Basic/Professional is described below.

Exporting configuration data via STEP 7 Basic/Professional

To export configuration data via STEP 7 Basic/Professional, follow these steps:

1. Open the relevant STEP 7 project in STEP 7 Basic/Professional.
2. Open the project view.
3. Open the network view or the topology view.
4. Open the Hardware catalog.
5. In the hardware catalog, navigate to the device with the relevant article number.
6. Select the desired device with a mouse click.
7. Set the matching firmware version via the drop-down list of the hardware catalog.
8. Drag-and-drop the device to the network view or to the topology view.
9. Select the device in the network view on in the topology view.
10. Configure the device in the Inspector window under "Properties > General".
11. In the Inspector window, navigate to the "Management" parameter under "Properties > General".
12. In the parameter group "Load / save file", click the "Save to file" button.
13. Select a storage location for the file.
14. Assign a name for the file.
15. Click the "Save" button.
    The "Save configuration file" dialog opens.
16. Assign a password for the encryption of the file.

    Note

    You need this password when you load the file to a device via the WBM.

17. Click the "OK" button.

Importing configuration data via STEP 7 Basic/Professional

To import configuration data via STEP 7 Basic/Professional, follow these steps:

1. Open the relevant STEP 7 project in STEP 7 Basic/Professional.
2. Open the project view.
3. Open the network view or the topology view.
4. Open the Hardware catalog.
5. In the hardware catalog, navigate to the device with the relevant article number.
6. Select the desired device with a mouse click.
7. Set the matching firmware version via the drop-down list of the hardware catalog.
8. Drag-and-drop the device to the network view or to the topology view.
9. Select the device in the network view on in the topology view.
10. In the Inspector window, navigate to the "Management" parameter under "Properties > General".
11. In the parameter group "Load / save file", click the "Load from file" button.
12. Select the desired file.
13. Click the "Open" button.
    The "Load configuration file" dialog opens.
14. Enter the password for the decryption of the file.

    Note

    You assign this password in the WBM under "System > Load&Save > Passwords".

15. Click the "OK" button.

6.2 Message: SINEMA configuration not yet accepted

When the following message is displayed in the display area an error has occurred transferring the configuration from STEP 7 Basic / Professional as of V13 to the device:

"SINEMA Configuration not accepted yet. With restart of device, all configuration changes will be lost."

One possible cause is, for example, that during transfer the device was not reachable.

If you now change a parameter directly on the device (WBM/CLI/SNMP) these changes are lost when the device restarts.

Solution

1. Open the relevant STEP 7 project in STEP 7 Basic / Professional
2. Open the project view.

3. Select the device in the project tree.
4. Select the "Go to network view" command in the shortcut menu.
5. Select the device in the network view.
6. In the shortcut menu of the selected device select the command "SCALANCE configuration > Save as start configuration".

Result

The configuration is saved on the device. The message is no longer visible in the display area. A configuration change directly on the device is no longer lost due to a restart of the device.

Appendix A "Syslog messages"

A

A.1 Structure of the Syslog messages

The Syslog server collects log information of the devices about specific events. The Syslog messages are received by the Syslog server via the set UDP port (standard: 514) and output according to RFC 5424 or RFC 5426. The Syslog protocol prescribes a fixed sequence and structure of the possible parameters.

Syslog messages are structured as follows according to RFC 5424:

Part / Parameter	Explanation
HEADER	
PRI	PRI contains the coded priority of the Syslog message, broken down into Severity (severity of the message) and Facility (origin of the message).
VERSION	Version number of the Syslog specification.
TIMESTAMP	The device sends the time stamp in the format "2010-01-01T02:03:15.0003+02:00" as the local time including the time zone and correction for daylight saving / standard time if needed.
HOSTNAME	References the source computer with its name or the IP address. IPv4 address according to RFC1035: Bytes in decimal representation: XXX.XXX.XXX.XXX IPv6 address according to RFC4291 Section 2.2 "-" is output if information is missing. Example in the product: The station name configured in the "System" tab for the RTU.
APP-NAME	Device or application from which the message originates. "-" is output if information is missing.
PROCID	The process ID serves to clearly identify the individual processes, for example during analysis and troubleshooting. "-" is output if information is missing.
MSGID	ID to identify the message. "-" is output if information is missing.
STRUCTURED-DATA	
timeQuality	The structured data element "timeQuality" provides information on system time. Example: [timeQuality tzKnown="0" isSynced="0"] The "tzKnown" parameter indicates whether the sender knows its time zone (value "1" = known; value "0" = unknown). The "isSynced" parameter indicates whether the sender is synchronized with a reliable external time source, e.g. via NTP (value "1" = synchronized; value "0" = not synchronized).
sysUpTime	The "sysUpTime" parameter is metainformation about the message. It specifies the time (in hundredths of seconds) since the last re-initialization of the network management part of the system.
MSG	
MESSAGE	Message as ASCII string (English)

Note

Additional information

You can read more detailed information on the structure of the Syslog messages and on the meaning of the parameters in the RFCs:

https://tools.ietf.org/html/rfc5424

https://tools.ietf.org/html/rfc5426

A.2 Tags in Syslog messages

The tags are displayed in the section "Syslog messages" in the field "Message text" within curly brackets {variable}.

The output messages can contain the following tags:

Tag	Description	Format	Possible values or example
{Ip address}	IPv4 address according to RFC1035 IPv6 address according to RFC4291 Section 2.2	%d.%d.%d.%d XXX.XXX.XXX.XXX	192.168.1.105 2001:DB8::8:800:200C:417A
{Src port} {Dest port}	Port number (decimal)	%d	0 ... 65535
{Dest mac} {Src mac}	MAC address	%02x:%02x:%02x;%02x:%02x:%02x	00:0C:29:2F:09:B3
{Protocol}	Layer 4 protocol or service used that generated the event.	%s	UDP | TCP | WBM | Telnet | SSH | Console | TFTP | SFTP
{Group}	Name for identification of the group (string)	%s	it-service
{User name}	String (without spaces) that identifies the authenticated user by his or her name.	%s	<name>
{Action user name}	Identifies the user based on his/her name This is not the authenticated user.	%s	<First name>.<Surname>
{Role}	Symbolic name of the group role	%s	Administrator
{Time minute} {Timeout}	Number of minutes	%d	44
{Time second}	Number of seconds	%d	44
{Failed login count}	Number of failed login attempts	%d	10
{Max sessions}	Maximum number of sessions	%d	10
{Firewall rule}	String (with space) for the firewall rule set	%s	Rule1
{Subject}	String (with space) for the subject in the certificate. Used as part of the certificate-based authentication and must include Unicode characters.	%s With UTF8 code: %S	(Peter Maier)

Tag	Description	Format	Possible values or example
{Config detail}	String (with space) for the configuration	%s	OpenVPN
{Connection name}	Name of the VPN connection		to_Baugruppe1
{Firewall accept}	Firewall action executed (accepted package)		ACCEPT
{Firewall action reject}	Firewall action executed (rejected package)		REJECT DROP
{Length}	Length of the network packet (in bytes)	%d	52
{Network interface}	Symbolic name of a network interface	%s	vlan 1

A.3 Syslog messages

This section describes the Syslog messages. The structure of the messages is based on IEC 62443-3-3.

Identification and authentication of human users

Message text	{protocol}: User {User name} has logged in from {ip address}.
Example	WBM: User "Admin" has logged in from 192.168.0.1.
Explanation	Valid login information that is specified during remote login.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{protocol}: User {User name} failed to log in from {ip address}.
Example	WBM: User "Admin" has failed to log in from 192.168.0.1.
Explanation	Incorrect user name or incorrect password (login information) specified during remote login.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{protocol}: User {User name} has logged out from {ip address}.
Example	SSH: User "Admin" has logged out from 192.168.0.1.
Explanation	User session completed - logged out.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{Protocol}: Default user {User name} logged in from {Ip address}.
Example	WBM: Default user <admin> logged in from 192.168.0.1.

Explanation	Default user has logged in via the IP address.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 007-R5)

Identification and authentication of devices (access via firewall)

Message text	{firewall action accept}(1) in:{network interface} out:{network interface} len: {length} s-mac:{src mac} d-mac:{dest mac} s-ip:{ip address} d-ip:{ip address} {protocol}:{src port}->{dest port}
Example	ACCEPT(1) in:vlan1 out:ppp0 len:52 s-mac:58:EF:68:B3:FA:CE d-mac:00:1B:1B:A7:5B:D8 s-ip:172.23.1.6 d-ip:158.85.11.68 tcp:53788->443
Explanation	A known device requested a connection.
Severity	Info or Warning (configurable)
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.2

Message text	{firewall action reject}(1) in:{network interface} out:{network interface} len: {length} s-mac:{src mac} d-mac:{dest mac} s-ip:{ip address} d-ip:{ip address} {protocol}:{src port}->{dest port}
Example	REJECT(1) in:vlan1 out:ppp0 len:52 s-mac:58:EF:68:B3:FA:CE d-mac:00:1B:1B:A7:5B:D8 s-ip:172.23.1.6 d-ip:217.194.40.109 tcp:53773->443
Explanation	An unknown device requested a connection. The request was denied.
Severity	Info or Warning (configurable)
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.2

User account management

Message text	{protocol}: User {user name} changed own password.
Example	WBM: User admin changed own password.
Explanation	User has changed own password.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR1.3

Message text	{protocol}: User {user name} changed password of user {action user name}.
Example	Telnet: User admin changed password of user test.
Explanation	User has changed the password of another user.
Severity	Notice

Facility	local0
Standard	IEC 62443-3-3 Reference: SR1.3

Message text	{protocol}: User {user name} created user-account {action user name}.
Example	WBM: User admin created user-account service.
Explanation	The user has created an account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR1.3

Message text	{protocol}: User {user name} deleted user-account {action user name}.
Example	WBM: User admin deleted user-account service.
Explanation	The administrator deleted an existing account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR1.3

Management of the identifiers

Message text	{Protocol}: User {User name} created group {Group} and assigned to role {Role}.
Example	WBM: User admin created group it-service and assigned to role service.
Explanation	The administrator has created a group and assigned it to a role.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.4

Message text	{Protocol}: User {User name} deleted group {Group} and the role {Role} assignment.
Example	WBM: User maier deleted group it-service and the role service assignment.
Explanation	The administrator has deleted an existing group and the role assignment.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.4

Unsuccessful logon attempts

Message text	{User name} account is locked for {Time minute} minutes after {Failed login count} unsuccessful login attempts.
Example	User service account is locked for 44 minutes after 10 unsuccessful login attempts.
Explanation	If there are too many failed logins, the corresponding user account was locked for a specific period of time.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.11

Access via untrusted networks (IPsec)

Message text	[IKE] <{connection name}|{config detail}> IKE_SA {connection name}[{config detail}] established between {ip address}[{config detail}]...{ip address}[{config detail}]
Example	[IKE] <c1|3> IKE_SA c1[1] established between 192.168.55.210[lokal].. 192.168.55.211[remote]
Explanation	VPN connection is established (IPsec).
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1)

Message text	[IKE] <{connection name}|{config detail}> deleting IKE_SA {connection name} [{config detail}] between {ip address}[{config detail}]...{ip address}[{config detail}]
Example	[IKE] <c1|3> deleting IKE_SA c2[1] between 192.168.55.211[lokal].. 192.168.55.210[remote]
Explanation	VPN tunnel is closed (IPsec).
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1)

Message text	[IKE] <{connection name}|{config detail}> received AUTHENTICATION_FAILED notify error
Example	[IKE] <c1|1> received AUTHENTICATION_FAILED notify error
Explanation	Authentication of VPN connection failed (IPsec).
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R3)

Access via untrusted networks (OpenVPN)

Message text	OVPN_{connection name}[{config detail}]: Initialization Sequence Completed
Example	OVPN_Conn_1[2427]: Initialization Sequence Completed
Explanation	VPN connection is established (OpenVPN).
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1)

Message text	OpenVPN connection {connection name} has been deactivated.
Example	OpenVPN connection c1 has been deactivated.
Explanation	VPN connection was closed (OpenVPN).
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1)

Access via untrusted networks (SINEMA Remote Connect)

Message text	SINEMA RC - State of Digital Input changed to HIGH. SINEMA RC - OpenVPN connection established.
Example	SINEMA RC - State of Digital Input changed to HIGH. SINEMA RC - OpenVPN connection established.
Explanation	Remote access is permitted. (SINEMA RC, Digital Input)
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.13

Message text	[JOB] <{connection name}|{config detail}> deleting CHILD_SA after {time second} seconds of inactivity
Example	[JOB] <to_Baugruppe1|21> deleting CHILD_SA after 20 seconds of inactivity
Explanation	The remote session was ended after a period of inactivity (IPsec).
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.6

Message text	OVPN_{connection name}[{config detail}]: [{config detail}] Inactivity timeout (--ping-restart), restarting
Example	OVPN_c1[26296]: [router] Inactivity timeout (--ping-restart), restarting
Explanation	The remote session was ended after a period of inactivity (OpenVPN).
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.6

Message text	SINEMA RC - State of Digital Input changed to LOW. SINEMA RC - OpenVPN terminated.
Example	SINEMA RC - State of Digital Input changed to LOW. SINEMA RC - OpenVPN terminated.
Explanation	Remote access denied (SINEMA RC, Digital Input)
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.13

Authorization enforcement (access via custom firewall)

Message text	User specific firewall user "{user name}" activated rule set "{firewall rule}" with ip address "{ip address}". Timeout: {timeout} minutes.
Example	User specific firewall user "usf" activated rule set "rs1" with ip address "172.23.1.14". Timeout 5 minutes.
Explanation	The user has logged onto the user-specific firewall. (USF Digital User Login)
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R2)

Message text	User specific firewall digital input {trigger pin} activated rule set "{firewall rule}" with ip "{ip address}".
Example	User specific firewall digital input 1 activated rule set "cpu2" with ip "192.168.16.1".
Explanation	The user has logged onto the user-specific firewall. (USF Digital Input Login)
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R2)4820486

Message text	User specific firewall user "{user name}" ruleset "{firewall rule}" time expired.
Example	User specific firewall user "usf" ruleset "rs1" time expired.
Explanation	The access to the user-specific firewall was denied. The access time is expired. (USF User Logout)
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.1

Message text	User specific firewall user "{user name}" logged out by administrator configuration.
Example	User specific firewall user "usf" logged out by administrator configuration.
Explanation	The access to the user-specific firewall was denied. The device administrator deactivates the user using the "Force Deactivate" button. (USF user force log out by admin)
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.1

Message text	User specific firewall user "{user name}" deactivated by administrator configuration.
Example	User specific firewall user "usf" deactivated by administrator configuration.
Explanation	The access to the user-specific firewall was denied. The device administrator has deactivated the user. (USF user deactivated by admin)
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.1

Message text	User specific firewall digital input {trigger pin} deactivated rule set "{firewall rule}".
Example	User specific firewall digital input 1 deactivated rule set "rs1".
Explanation	The access to the user-specific firewall was denied. The corresponding set of rules has been deactivated. (USF Digital Input Logout)
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.1

Session lock

Message text	{Protocol}: The session of user {User name} was closed after {Time second} seconds of inactivity.
Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: The session of user admin was closed after 60 seconds of inactivity.
Explanation	The current session was ended due to inactivity.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.5

Closing a remote access session

Message text	{Protocol}: Remote session {Config detail} was closed after {Time second} seconds of inactivity.
Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Remote session OpenVPN was closed after 44 seconds of inactivity.
Explanation	The remote session was ended after a period of inactivity.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.6

Limiting the number of simultaneous sessions

Message text	{Protocol}: The maximum number of {Max sessions} concurrent login session exceeded.
Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: The maximum number of 10 concurrent login sessions exceeded.
Explanation	The maximum number of parallel sessions has been exceeded.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.7

Nonrepudiation

Message text	Device configuration changed.
Example	Device configuration changed.
Explanation	The device configuration has been changed permanently.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR2.12

Communication integrity

Message text	[IKE] {connection name} {config detail} received invalid DPD sequence number {config detail} (expected {config detail}), ignored.
Example	[IKE] "c1" "1" received invalid DPD sequence number 10 (expected 12), ignored.
Explanation	Integrity check failed (IPsec)
Severity	Warning

Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.1

Message text	OVPN_{connection name}{config detail}: Authenticate/Decrypt packet error: packet HMAC authentication failed.
Example	OVPN_c1[25409]: Authenticate/Decrypt packet error: packet HMAC authentication failed.
Explanation	Integrity check failed (OpenVPN).
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.1

Restoration of the automation system

Message text	{protocol}: Loaded file type Firmware {version} (restart required).
Example	TFTP: Loaded file type Firmware V02.00.00 (restart required).
Explanation	The firmware was successfully loaded.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.4

Message text	{protocol}: User {user name} loaded file type Firmware {version} (restart required).
Example	WBM: User admin loaded file type Firmware V02.00.00 (restart required).
Explanation	The user has successfully loaded the firmware.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.4

Message text	{protocol}: Failed to load file type Firmware.
Example	WBM: Failed to load file type Firmware.
Explanation	Firmware upload has failed.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.4

Message text	{protocol}: Loaded file type Config (restart required).
Example	TFTP: Loaded file type Config (restart required).
Explanation	The configuration is applied.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.4

Message text	{protocol}: Loaded file type ConfigPack (restart required).
Example	TFTP: Loaded file type ConfigPack (restart required).
Explanation	The configuration is applied.
Severity	Notice

Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.4

Message text	{protocol}: User {user name} loaded file type Config (restart required).
Example	WBM: User admin loaded file type Config (restart required).
Explanation	The configuration is applied.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.4

Message text	{protocol}: User {user name} loaded file type ConfigPack (restart required).
Example	WBM: User admin loaded file type ConfigPack (restart required).
Explanation	The configuration is applied.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.4

Appendix B "Ciphers used"

B

The following tables list the encryption methods (ciphers) used by SCALANCE SC-600.

B.1 SSL

HTTPS WBM Server

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_AES_128_GCM_SHA256	1301	✓
Encryption suite	TLS_CHACHA20_POLY1305_SHA256	1303	✓
Encryption suite	TLS_AES_256_GCM_SHA384	1302	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	c02f	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	c030	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	0xC02B	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0xC02C	✓
Encryption suite	TLS_RSA_WITH_AES_256_CBC_SHA	0035	--
Protocol version	TLSv1	--	--
Protocol version	TLSv11	--	--
Protocol version	TLSv1.2	--	--
Protocol version	TLSv1.3	--	--

OpenVPN Server

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_AES_256_GCM_SHA384	0x1302	✓
Encryption suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xC030	✓
Encryption suite	TLS_AES_128_GCM_SHA256	0x1301	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xC02F	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0xC02C	✓

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_128_GCM_SHA256	0xC02B	✓
Encryption suite	TLS_RSA_WITH_AES_256_CBC_SHA	0x0035	--
Encryption suite	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	0x009F	--
Encryption suite	TLS_ECDHE_ECDSA_WITH_CHA-CHA20_POLY1305_SHA256	0xCCA9	--
Encryption suite	TLS_ECDHE_RSA_WITH_CHA-CHA20_POLY1305_SHA256	0xCCA8	--
Encryption suite	TLS_DHE_RSA_WITH_CHA-CHA20_POLY1305_SHA256	0xCCAA	--
Encryption suite	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	0x009E	--
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_256_CBC_SHA384	0xC024	--
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	0xC028	--
Encryption suite	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	0x006B	--
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_128_CBC_SHA256	0xC023	--
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	0xC027	--
Encryption suite	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	0x0067	--
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_256_CBC_SHA	0xC00A	--
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	0xC014	--
Encryption suite	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	0x0039	--
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_128_CBC_SHA	0xC009	--
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	0xC013	--
Encryption suite	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	0x0033	--
Encryption suite	TLS_RSA_WITH_AES_256_GCM_SHA384	0x009D	--
Encryption suite	TLS_RSA_WITH_AES_128_GCM_SHA256	0x009C	--
Encryption suite	TLS_RSA_WITH_AES_256_CBC_SHA256	0x003D	--
Encryption suite	TLS_RSA_WITH_AES_128_CBC_SHA256	0x003C	--
Encryption suite	TLS_RSA_WITH_AES_128_CBC_SHA	0x002F	--
Encryption suite	TLS_EMPTY_RENEGOTIATION_INFO_SCSV	0x00FF	--
Protocol version	TLSv1	-	--
Protocol version	TLSv1.1	-	--
Protocol version	TLSv1.2	-	✓
Protocol version	TLSv1.3	-	✓

SMTP Client (secure)

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_AES_128_GCM_SHA256	1301	✓
Encryption suite	TLS_CHACHA20_POLY1305_SHA256	1303	✓
Encryption suite	TLS_AES_256_GCM_SHA384	1302	✓
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_256_GCM_SHA384	c02c	✓
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_128_GCM_SHA256	c02b	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	c02f	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	c030	✓
Protocol version	TLSv1.2	--	✓
Protocol version	TLSv1.3	--	✓

Syslog Client TLS

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_AES_128_GCM_SHA256	1301	✓
Encryption suite	TLS_CHACHA20_POLY1305_SHA256	1303	✓
Encryption suite	TLS_AES_256_GCM_SHA384	1302	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	c02f	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	c030	✓
Protocol version	TLSv1.2	--	✓
Protocol version	TLSv1.3	--	✓

SRC Client

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_AES_128_GCM_SHA256	0x1301	✓
Encryption suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	✓
Encryption suite	TLS_AES_256_GCM_SHA384	0x1302	✓
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_256_GCM_SHA384	0xc02c	✓
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_128_GCM_SHA256	0xc02b	✓
Encryption suite	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	0x009e	✓

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	0x009f	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xc02f	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xc030	✓
Protocol version	TLSv1.2	--	✓

B.2 SSH

SSH CLI Server

Category	Process	Hexadecimal value	Enabled by default
Encryption method (enc)	aes256-ctr	--	✓
Host key	ecdsa-sha2-nistp521	--	✓
Host key	rsa-sha2-256	--	✓
Host key	rsa-sha2-512	--	✓
Host key	ssh-rsa	--	--
Key exchange (kex)	curve25519-sha256	--	✓
Key exchange (kex)	curve25519-sha256@libssh.org	--	✓
Key exchange (kex)	ecdh-sha2-nistp256	--	✓
Key exchange (kex)	ecdh-sha2-nistp384	--	✓
Key exchange (kex)	ecdh-sha2-nistp521	--	✓
Key exchange (kex)	diffie-hellman-group16-sha512	--	--
Key exchange (kex)	diffie-hellman-group18-sha512	--	--
Key exchange (kex)	diffie-hellman-group14-sha256	--	--
Key exchange (kex)	diffie-hellman-group14-sha1	--	--
MAC	hmac-sha2-256	--	✓
Protocol version	SSHv2.0	--	✓

SFTP Client

Category	Process	Hexadecimal value	Enabled by default
Encryption method (enc)	aes256-ctr	--	✓
Host key	ecdsa-sha2-nistp521	--	✓
Host key	rsa-sha2-256	--	✓
Host key	rsa-sha2-512	--	✓

Category	Process	Hexadecimal value	Enabled by default
Host key	ssh-rsa	--	--
Key exchange (kex)	curve25519-sha256	--	✓
Key exchange (kex)	curve25519-sha256@libssh.org	--	✓
Key exchange (kex)	ecdh-sha2-nistp256	--	✓
Key exchange (kex)	ecdh-sha2-nistp384	--	✓
Key exchange (kex)	ecdh-sha2-nistp521	--	✓
Key exchange (kex)	diffie-hellman-group16-sha512	--	--
Key exchange (kex)	diffie-hellman-group18-sha512	--	--
Key exchange (kex)	diffie-hellman-group14-sha256	--	--
Key exchange (kex)	diffie-hellman-group14-sha1	--	--
MAC	hmac-sha2-256	--	✓
Protocol version	SSHv2.0	--	✓

B.3 SNMP

SNMP Server

Category	Process	Hexadecimal value	Enabled by default
Authentication	HMAC-MD5-96	--	--
Authentication	HMAC-SHA-96	--	--
Encryption	des-cbc	--	--
Encryption	aes128-cbc	--	--

B.4 RADIUS

RADIUS Client

Category	Process	Hexadecimal value	Enabled by default
Integrity algorithm	MD5	--	--
Integrity algorithm	HMAC-SHA1	--	--
Integrity algorithm	HMAC-MD5	--	--

Index

I

K

L

M

N

O

P

Q

R

S

T

U

V

W