SIEMENS

SIMATIC NET

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

Configuration Manual

02/2019

C79000-G8976-C475-02

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
Division Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000-G8976-C475-02
Ⓟ 02/2019 Subject to change

Introduction

Validity of the configuration manual

This Configuration Manual covers the following products:

- 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 V2.0

Purpose of the Configuration Manual

This Configuration Manual is intended to provide you with the information you require to install, commission and operate the security appliances SCALANCE SC-600. It provides you with the information you require to configure the Security Appliances SCALANCE SC-600.

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 SC632-2C and SCALANCE SC642-2C • SCALANCE SC636-2C and SCALANCE SC646-2C • SCALANCE SC632-2C and SCALANCE SC636-2C • SCALANCE SC642-2C and SCALANCE SC646-2C	• SC6x2-2C • SC6x6-2C • SC63x-2C • SC64x-2C
Device	If information relates to a specific device, the device name is used.	• SCALANCE SC632-2C • SCALANCE SC636-2C • SCALANCE SC642-2C • SCALANCE SC646-2C

New in this edition

- Bridge firewall
- User-specific firewall rules

- RADIUS client
- Global Passive Listening
- Signaling contact can be configured as digital output
- Upload of the configuration from TIA
- RSTP/STP support
- DCP Discovery
- Configuration limit for IP services extended to 128
- Configuration limit for NAT/NAPT rules extended to 1000
- Downloading and saving using SFTP
- C-PLUG support 6GK1900-0AB10
- Downloading firmware via C-PLUG
- Use of SC6x6-2C as MRP client or HRP client with ring redundancy
- VRRP
- Factory default "admin" user can be renamed
- Uniqueness of firewall precedence
- Pre-defined IPv4 rules for system time
- Editable NAT/NETMAP rules
- NAT: Bidirectional rules; AutoFirewall rules; NATv2MIB
- Expansion of events (e.g. for successful authentication)

Replaced edition

Edition 10/2017

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 license conditions in the following documents on the supplied data medium:

- OSS_SCALANCE-SC-600_99.pdf

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
Link: (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 customers' exposure to cyber threats.

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

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)

Training, Service & Support

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

Trademarks

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

SIMATIC NET, SCALANCE, SINEMA, C-PLUG

Table of contents

Security recommendations 1

To prevent unauthorized access, note the following security recommendations.

General

- You should make regular checks to make sure that the device meets these recommendations and/or other security guidelines.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products.
  Link: (https://www.industry.siemens.com/topics/global/en/industrial-security/pages/default.aspx)
- Separate connections correctly (WBM. Telnet, SSH etc.).

Physical access

- Restrict physical access to the device to qualified personnel because the plug-in data medium can contain sensitive data.
- Lock unused physical interfaces on the device. Unused interfaces can be used to gain access to the plant without permission.

Software (security functions)

- Keep the firmware up to date. Check regularly for security updates for the device. You can find information on this at the Industrial Security (https://www.siemens.com/industrialsecurity) website.
- Inform yourself regularly about security recommendations published by Siemens ProductCERT (https://www.siemens.com/cert/en/cert-security-advisories.htm).
- Only activate protocols that you require to use the device.
- Restrict access to the management of the device with rules in an access control list (ACL).
- The option of VLAN structuring provides protection against DoS attacks and unauthorized access. Check whether this is practical or useful in your environment.
- Use a central logging server to log changes and accesses. Operate your logging server within the protected network area and check the logging information regularly.

Passwords

- Define rules for the assignment of passwords.
- Regularly change your passwords to increase security.
- Use passwords with a high password strength.

- Make sure that all passwords are protected and inaccessible to unauthorized persons.
- Do not use the same password for different users and systems.

Keys and certificates

- The device contains a pre-installed X.509 certificate with key. Replace this certificate with a self-made certificate with key. We recommend that you use a certificate signed by a reliable external or internal certification authority.
- Use the certification authority including key revocation and management to sign the certificates.
- Make sure that user-defined private keys are protected and inaccessible to unauthorized persons.
- Verify certificates and fingerprints on the server and client to prevent "man in the middle" attacks.
- It is recommended that you use password-protected certificates in the PKCS #12 format
- It is recommended that you use certificates with a key length of at least 2048 bits.
- Change keys and certificates immediately, if there is a suspicion of compromise.

Secure/non-secure protocols

- Avoid or disable non-secure protocols, for example HTTP, Telnet and TFTP. For historical reasons, these protocols are still available, however not intended for secure applications. Use non-secure protocols on the device with caution.
- Avoid or disable non-secure protocols. Check whether use of the following protocols is necessary:
  - Non authenticated and unencrypted ports
  - MRP, HRP
  - IGMP snooping
  - LLDP
  - Syslog
  - RADIUS
  - DHCP Options 66/67
  - TFTP
  - GMRP and GVRP

- The following protocols provide secure alternatives:
  - HTTP → HTTPS
  - Telnet → SSH
  - FTP → SFTP
  - SNMPv1/v2c → SNMPv3

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

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

    Use the authentication and encryption mechanisms of SNMPv3.
- Use secure protocols when access to the device is not prevented by physical protection measures.
- If you require non-secure protocols and services, operate the device only within a protected network area.
- Restrict the services and protocols available to the outside to a minimum.
- For the DCP function, enable the "Read Only" mode after commissioning.
- If you use RADIUS for management access to the device, activate secure protocols and services.
- For secure storage of your configuration, use the option of assigning a password with "Load and Save".

Interfaces security

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

Available protocols

The following list provides you with an overview of the open protocol ports.

The table includes the following columns:

- **Protocol**
- **Port**

- **Factory setting**
  - Open

    The factory setting of the port is "Open".
  - Closed

    The factory setting of the port is "Closed".
- **Port status**
  - Open

    The port is always open and cannot be closed.
  - Open (when configured)

    The port is open if it has been configured.
- **Authentication**

  Specifies whether or not the protocol is authenticated.
- **Encryption**

  Specifies whether or not the transfer is encrypted.

Protocol	Port	Factory setting		Port status	Authentication	Encryption
		VLAN1*)	VLAN2*)			
SSH SFTP	TCP/22	Open	Closed	Open (when configured with login)	Yes	Yes
HTTP	TCP/80	Open	Open	Open (when configured with login)	No	No
HTTPS	TCP/443	Open	Closed	Open (when configured with login)	Yes	Yes
SNMPv1/v3	UDP/161	Open	Closed	Open (when configured)	Yes	Yes
DNS	TCP/53 UDP/53	Open	Closed	Open (when configured)	No	No
Syslog	UDP/514	Closed	Closed	Open (only outgoing)	No	No
IPsec	UDP/500 UDP/4500	Closed	Closed	Open (when configured)	Yes	Yes
DHCP	UDP/67 UDP/68	Open	Open	Open (when configured)	No	No

Protocol	Port	Factory setting		Port status	Authentication	Encryption
		VLAN1*)	VLAN2*)			
NTP client	UDP/123	Closed	Closed	Open (only outgoing, when configured)	Yes	Yes (when configured)
NTP server	UDP/123	Closed	Closed	Open (when configured)	No	No
Siemens Remote Service (cRSP/SRS)	TCP/443	Closed	Closed	Open (only outgoing, when configured)	Yes	Yes
OpenVPN	TCP/UDP, depending on the configuration in SINEMA RC	Closed	Closed	Open (only outgoing, when configured)	Yes	Yes
TFTP	UDP/69	Closed	Closed	Open (only outgoing)	No	No
DDNS	TCP/80	Closed	Closed	Open (only outgoing, when configured)	Yes	No
ICMP	-	Open	Closed	Open	No	No
RADIUS client	UDP/1812 UDP/1813	Closed	Closed	Open (only outgoing, when configured)	Yes	No
VRRP	Multicast	Closed	Closed	Open (when configured)	No	No

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

SC6x2-2C: VLAN1 = port 1, VLAN2 = port 2

SC6x6-2C: VLAN1 = port 1-4, VLAN2 = port 5-6

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
  - MAC firewall (layer 2)
  - IP firewall with stateful packet inspection (layer 3 and 4)
  - Global and user-defined firewall rules
- VPN functions

  To establish a VPN (Virtual Private Network), the following functions are available:
  - IPsec VPN (SC64x-2C)
- SINEMA RC client
- Use of proxy servers
- Siemens Remote Service cRSP/SRS (SC64x-2C)

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

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 the Primary Setup Tool (PST) 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)	**SC632-2C** **SC642-2C**	**SC636-2C** **SC646-2C**
	P01	P01 ... P04 (VLAN 1)
IP address	Must be assigned manually. See section "Initial assignment of an IP address (Page 30)".	
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 PST. 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 logon or after a "Restore Factory Defaults and Restart"

You will find more information in "Web Based Management (Page 61)" and in "Starting and logging in (Page 62)".

2.2.1 C-PLUG

How it works

The C-PLUG is used to transfer the configuration of the old device to the new device when a device is replaced.

The following types are supported:

Type	Description	Article number
C-PLUG	Removable data storage medium (32 MB) for the configuration data and saving the firmware	6GK1900-0AB00
	Removable data storage medium (32 MB) for the configuration data and saving the firmware	6GK1900-0AB10

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 or not 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.

When the new device starts up with the PLUG, it then continues automatically with exactly the same configuration as the old device. One exception to this can be the IP configuration if it is set over DHCP and the DHCP server has not been reconfigured accordingly.

A reconfiguration is necessary if you use functions based on MAC addresses.
If an incorrect PLUG, for example from another product or a damaged PLUG is inserted, the device signals an error with the "F" LED.

You can either remove the PLUG again or select the option to reformat the PLUG.

In terms of the PLUG, devices work in two modes:

- Without PLUG

  The device stores the configuration in internal memory. This mode is active when no PLUG is inserted.
- With PLUG

  The configuration stored on the PLUG is displayed in the WBM in "System > PLUG". If changes are made to the configuration, the device stores the configuration directly on the PLUG and in the internal memory. This mode is active as soon as a PLUG is inserted. As soon as the device is started with a PLUG inserted, the device starts up with the configuration data on the PLUG.

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
	Routing
	Redundancy
	SNMP
	Security
	IPsec VPN (SC64x-2C)
	SINEMA RC
System	Configuration
	General
	DNS
	Restart
	Load&Save
	Events
	DHCP client
	DHCP server
	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
Layer 2	Configuration
	Port Based VLAN
	Dynamic MAC aging
	Ring redundancy
	Spanning Tree
	LLDP
Layer 3	Subnets
	NAT
	Static routes
	VRRPv3
Security	Users
	Passwords
	AAA
	Certificates
	Firewall
	IPsec VPN (SC64x-2C)

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
	Syslog server	3
	SNMPv1 trap recipient	10
	SNTP server	1
	NTP server/NTP (secure)	4
	DHCP pools	5
	IPv4 addresses managed by the DHCP server (dynamic + static)	100
	DHCP static assignments per DHCP pool	128
	DHCP options (3, 6, 12, 15, 66, 67)	5
	SINEMA RC	1
	Proxy server	5
Layer 2	Virtual LANs (port-based; including VLAN 1)	257
Layer 3	IP interfaces	12 (4 sub-interfaces are possible per IP interface)
	Static routes	100
	Possible routes to the same destination	8
	NAPT	1000
	Source NAT	1000
	NETMAP	1000
	VRRPv3	VRRPv3 instances (VRID): 6 Assigned IP addresses: 1 per VRID
Security	Users	30
	Groups	32
	Roles	32
	RADIUS Server	4
	NAT rules	1000
	Firewall rules	IP protocols: 16 IP services: 128 ICMP services: 16 IP rules: 1000 User-specific firewall: • Maximum number: 8 rule sets • Parallel user access: 4 • Maximum of 128 IP rules per firewall rule set

	Configurable function	Maximum number
	IPsec VPN	200 tunnels [1]

[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).

Technical basics 3

3.1 IP address

3.1.1 Structure of an IP address

Address classes

IP address range	Max. number of networks	Max. number of hosts/network	Class	CIDR
1.x.x.x through 126.x.x.x	126	16777214	A	/8
128.0.x.x through 191.255.x.x	16383	65534	B	/16
192.0.0.x through 223.255.255.x	2097151	254	C	/24
224.0.0.0 - 239.255.255.255	Multicast applications		D	
240.0.0.0 - 255.255.255.255	Reserved for future applications		E	

An IP address consists of 4 bytes. Each byte is represented in decimal, with a dot separating it from the previous one. This results in the following structure, where XXX stands for a number between 0 and 255:

XXX.XXX.XXX.XXX

The IP address is made up of two parts, the network ID and the host ID. This allows different subnets to be created. Depending on the bytes of the IP address used as the network ID and those used for the host ID, the IP address can be assigned to a specific address class.

Subnet mask

The bits of the host ID can be used to create subnets. The leading bits represent the address of the subnet and the remaining bits the address of the host in the subnet.

A subnet is defined by the subnet mask. The structure of the subnet mask corresponds to that of an IP address. If a "1" is used at a bit position in the subnet mask, the bit belongs to the corresponding position in the IP address of the subnet address, otherwise to the address of the computer.

Example of a class B network:

The standard subnet address for class B networks is 255.255.0.0; in other words, the last two bytes are available for defining a subnet. If 16 subnets must be defined, the third byte of the subnet address must be set to 11110000 (binary notation). In this case, this results in the subnet mask 255.255.240.0.

To find out whether two IP addresses belong to the same subnet, the two IP addresses and the subnet mask are ANDed bit by bit. If both logic operations have the save result, both IP addresses belong to the same subnet, for example, 141.120.246.210 and 141.120.252.108.

Outside the local area network, the distinction between network ID and host ID is of no significance, in this case packets are delivered based on the entire IP address.

Note

In the bit representation of the subnet mask, the "ones" must be set left-justified; in other words, there must be no "zeros" between the "ones".

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	via UDP with broadcast
Resolution of IP addresses in hardware addresses	ARP (Address Resolution Protocol)

3.1.3 Initial assignment of an IP 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 35).

- **Primary Setup Tool** (PST)
  - To be able to assign an IP address to the device with the PST, it must be possible to reach the device via Ethernet.
  - You will find the PST on the Internet pages of Siemens Industry Online Support:
    Link: (https://support.industry.siemens.com/cs/ww/en/view/19440762)
  - For further information about assigning the IP address with the PST, refer to the documentation "Primary Setup Tool (PST)".
- **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)".

3.1.4 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 126)".
- 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.

3.2 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

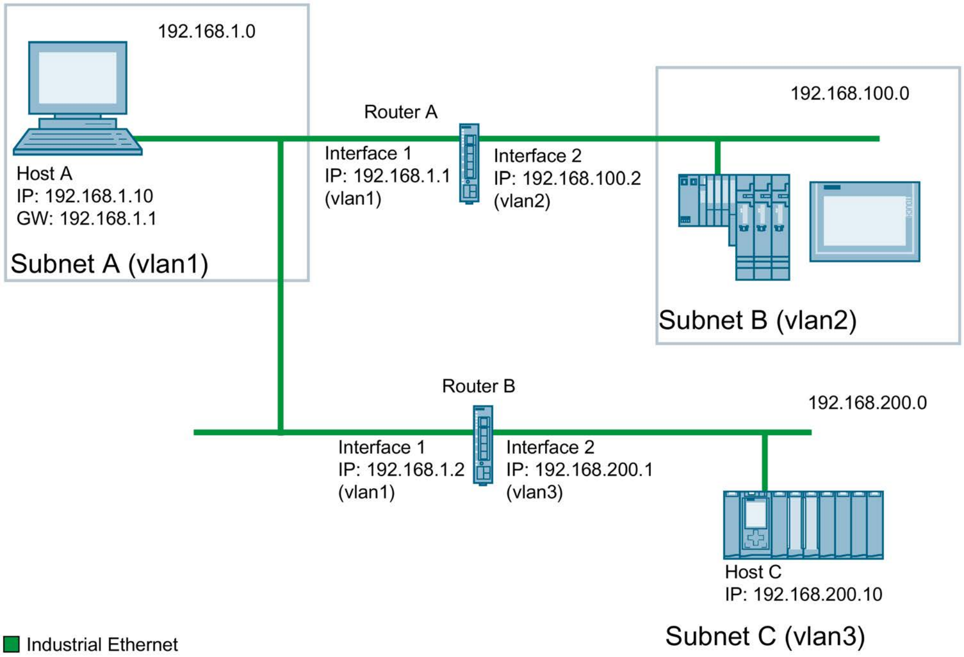
    Echo request, better known as ping.

- **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 36). 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 189)".

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:

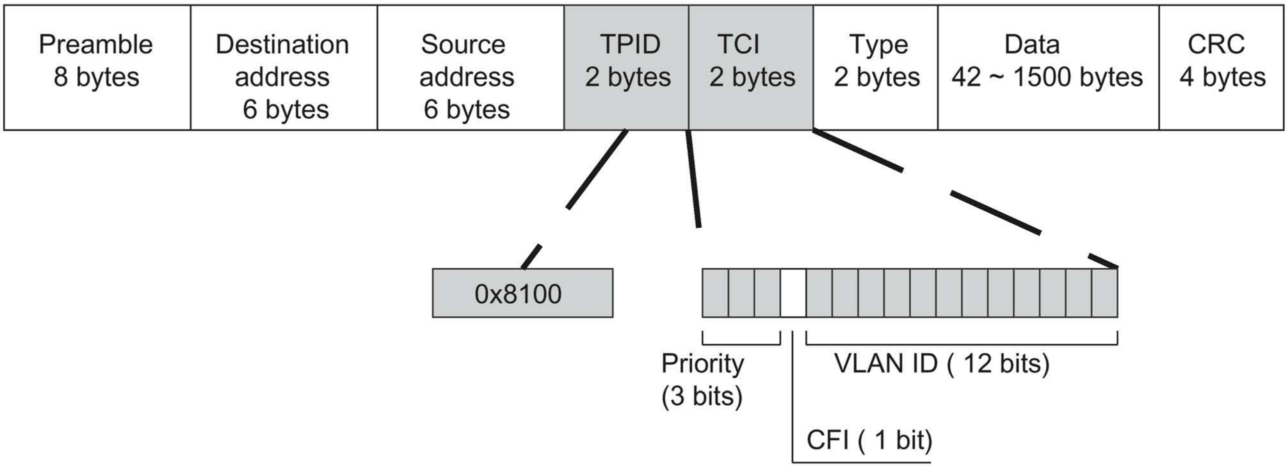


Figure 3-1 Structure of the expanded Ethernet frame

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 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.

3.6 Redundancy

3.6.1 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)

3.6.2 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.

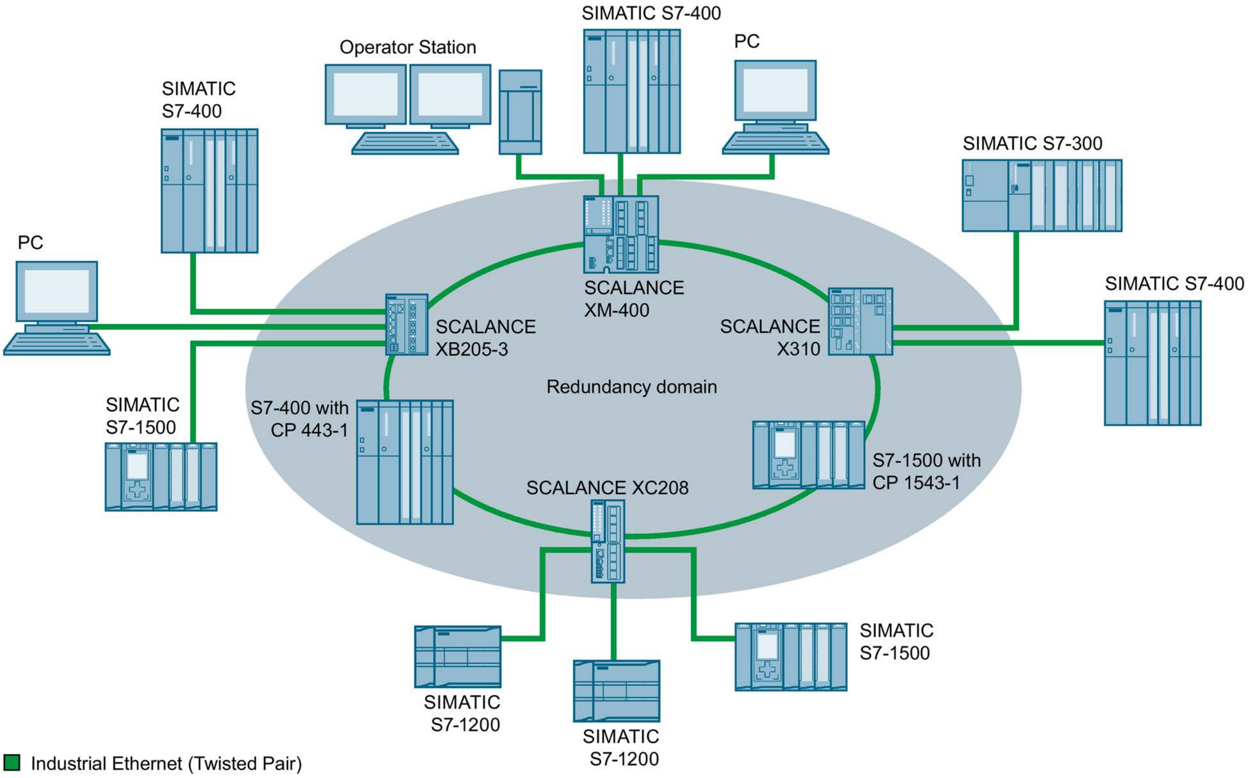


Figure 3-2 Example of a ring topology with the MRP media redundancy protocol

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 or 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)

3.6.3 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.

3.6.4 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)

3.7 Routing function

3.7.1 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

3.7.2 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.

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 master router has priority 255. 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.

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 (Page 217)".

3.7.3 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".

3.7.4 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

3.8 Security functions

3.8.1 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.

3.8.2 User administration

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.

3.8.3 Firewall

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>).
SINEMA RC	vlan x	Access from SINEMA RC connections to the IP subnet.
	Device	Access from SINEMA RC connections to the device.

from	to	Meaning
	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

3.8.4 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 207)".

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 207)".

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 210)".

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 212)".

3.8.5 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)

3.8.6 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 262)
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 262)
Partner certificate	Certificates with which the VPN gateway of the partner identifies itself with the device.	IPsec VPN (Page 262)

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.

3.8.7 VPN

The device supports the following VPN systems:

- IPsec VPN (SC64x-2C)

3.8.7.1 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 recipient.

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
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.

3.8.7.2 VPN connection establishment

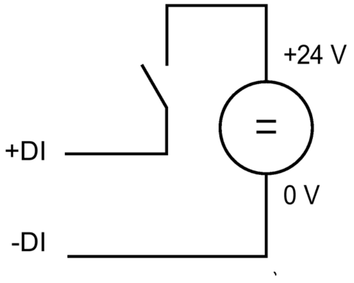
The device supports the following options for establishing a VPN connection.

- IPsec VPN: Security > IPsec VPN > Connections (Page 260)
- SINEMA RC: System > SINEMA RC (Page 183)

Options	Use		Description
	IPsec VPN	SINEMA RC	
start	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	Connection establishment is controlled via the digital input (DI).
wait on DI	x	-	
Digital input	-	x	
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 will find further 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.

- Digital input

  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
Trap	x	x	The device sends an SNMP trap. Requirement: • "SNMPv1 traps" is enabled in "System > Configuration". • In "System > Configuration > Traps" a recipient 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.

Type of notification	Digital In	VPN tunnel	Behavior if there is a status change
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 23)".
- 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.

  In the Internet Explorer, you can make the appropriate setting in the "Options > Internet Options > General" menu in the section "Browsing history" with the "Settings" button. Under "Check for newer versions of stored pages:", select "Automatically".

- 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 Internet Explorer 11

    Note

    Compatibility view

    In Microsoft Internet Explorer, disable the compatibility view to ensure correct display and to allow problem-free configuration using WBM.
  - Mozilla Firefox 55
  - Google Chrome V60

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.

   A message relating to the security certificate appears. Acknowledge this message and continue loading the page.

   Note

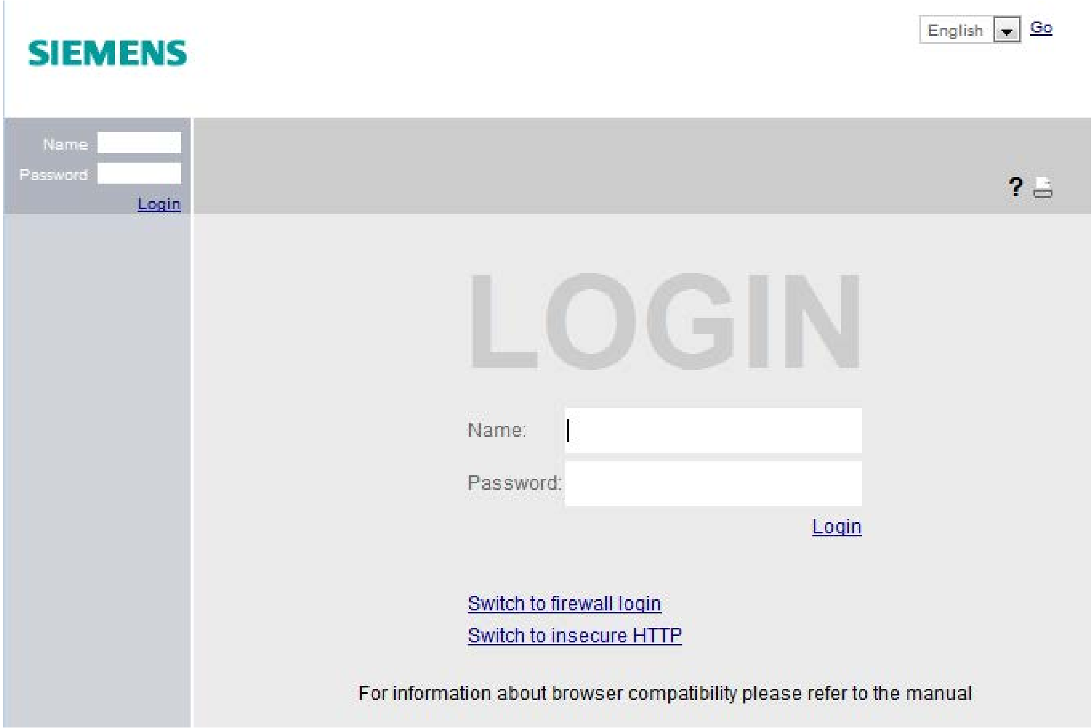
   Information on the security certificate

   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.
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.



For information about browser compatibility please refer to the manual

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

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
   - 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 WBM page for user-specific 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 "User-defined 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".

   After successful login, the WBM page "User-defined firewall 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.

4.3 "Information" menu

4.3.1 Start Page

View of the Start page

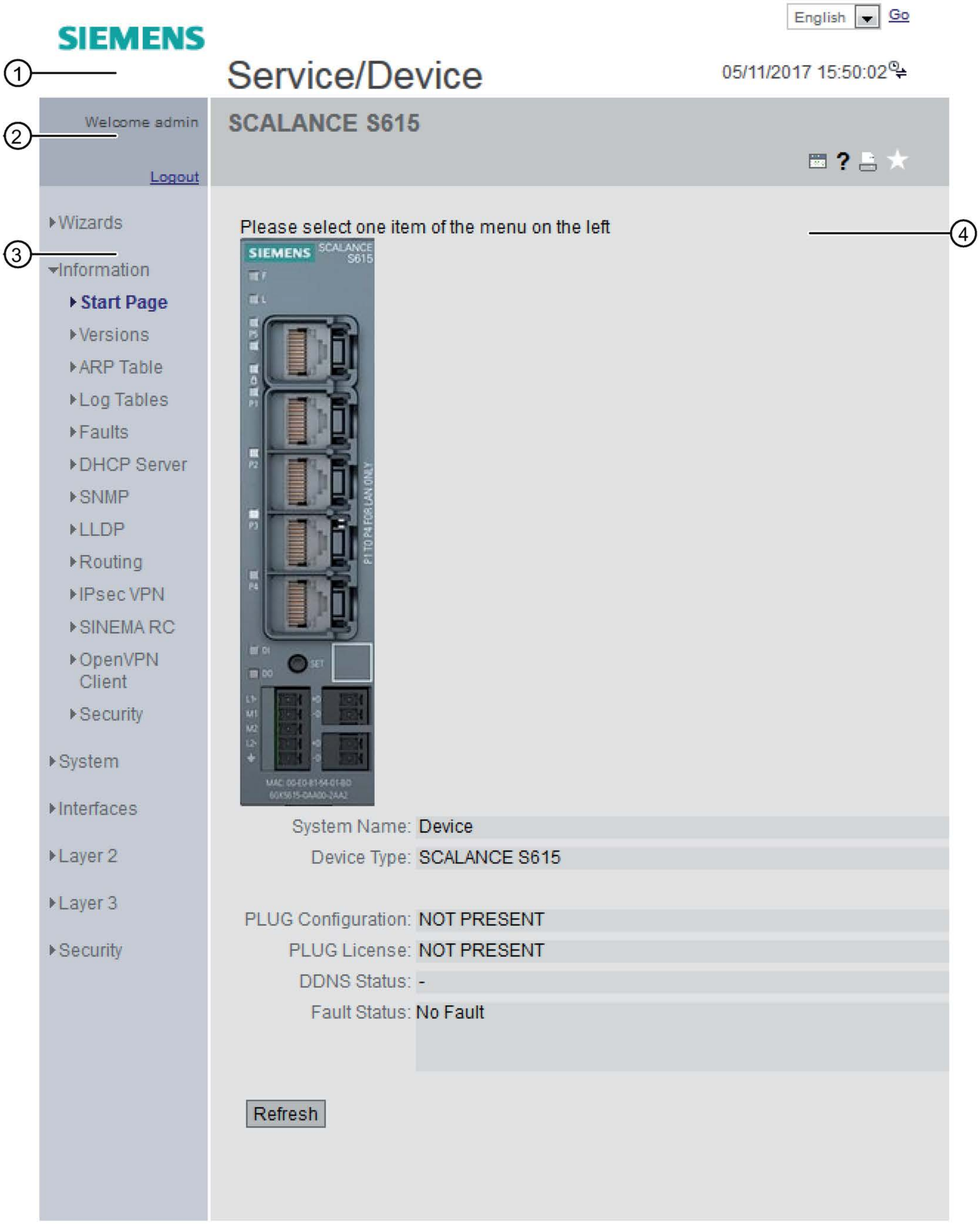
When you enter the IP address of the device, the start page is displayed after a successful login.

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



Please select one item of the menu on the left

System Name: Device

Device Type: SCALANCE S615

PLUG Configuration: NOT PRESENT

PLUG License: NOT PRESENT

DDNS Status: -

Fault Status: No Fault

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 Name"

  – "System Name" is the device name.
  With the settings when the device ships, 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.

If you disable all the favorites you have created, the "Favorites" tab is removed again.

- **Update on** On **/ Update off** Off
  WBM pages with overview lists can also have the additional "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**: Shows the 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.

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

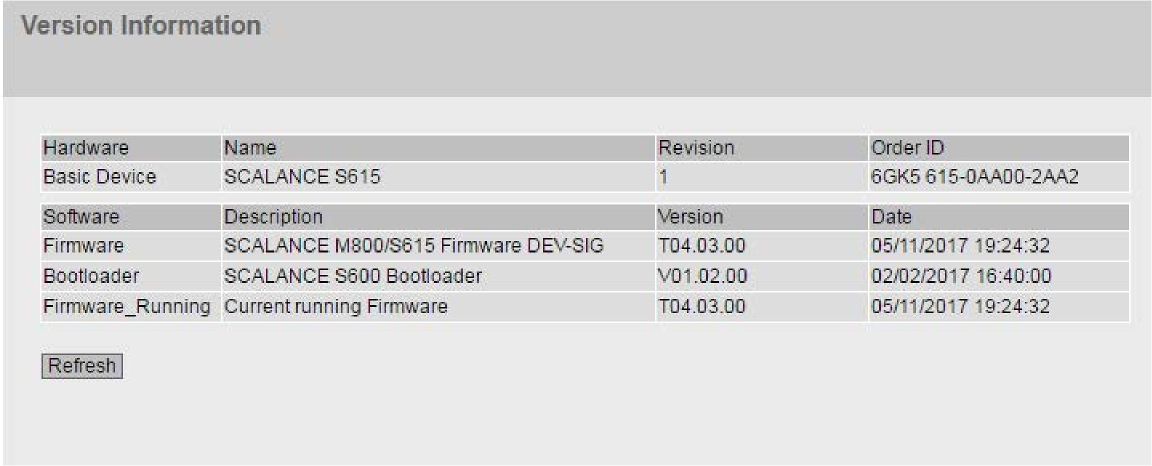
Interrupting the save

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

- 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.



Version Information

Hardware	Name	Revision	Order ID
Basic Device	SCALANCE S615	1	6GK5 615-0AA00-2AA2

Software	Description	Version	Date
Firmware	SCALANCE M800/S615 Firmware DEV-SIG	T04.03.00	05/11/2017 19:24:32
Bootloader	SCALANCE S600 Bootloader	V01.02.00	02/02/2017 16:40:00
Firmware_Running	Current running Firmware	T04.03.00	05/11/2017 19:24:32

Description

Table 1 has the following columns:

- **Hardware**
  - Basic Device
    Shows the basic device
  - PX.X

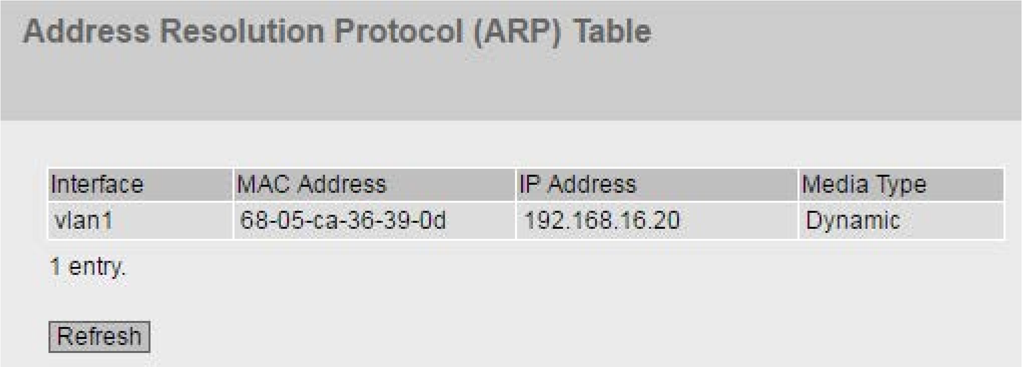
    X.X = port in which the SFP module is inserted.
  - SlotX

    "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 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.



Address Resolution Protocol (ARP) Table

Interface	MAC Address	IP Address	Media Type
vlan1	68-05-ca-36-39-0d	192.168.16.20	Dynamic

1 entry.

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.

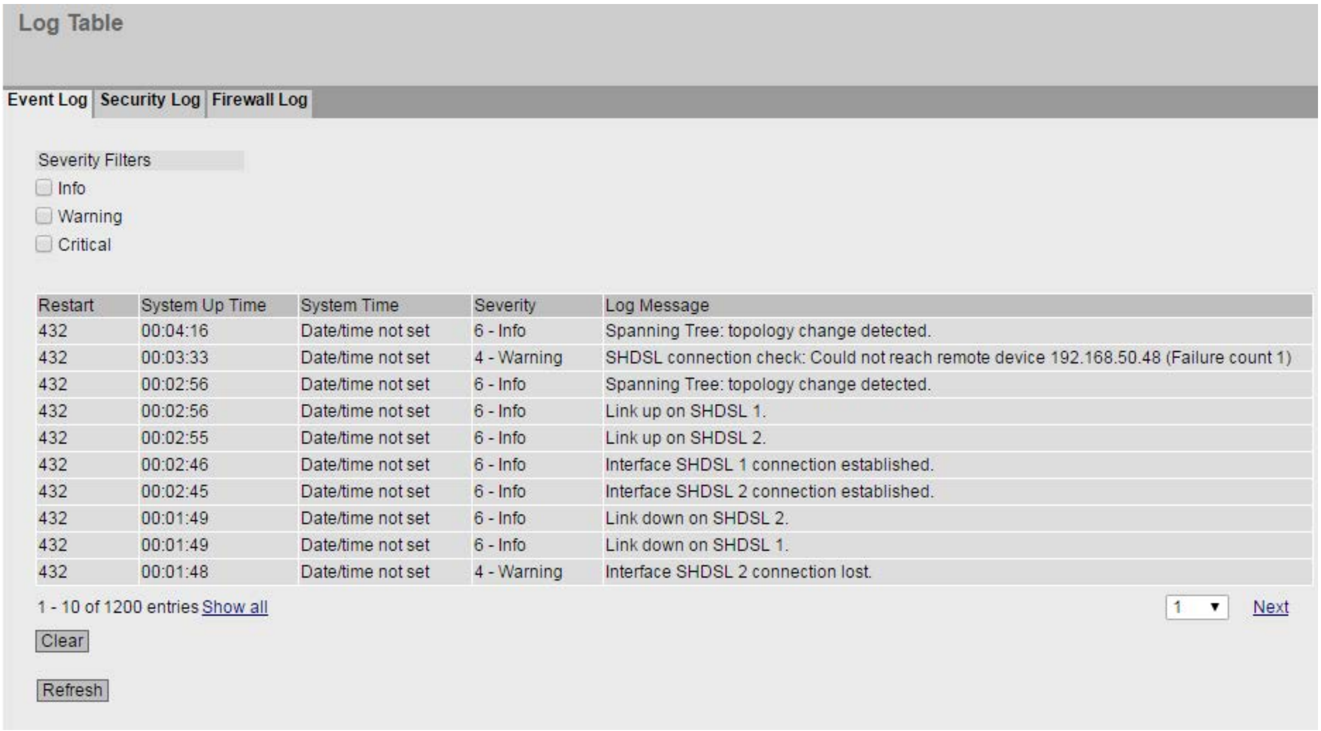
4.3.4 Log Tables

4.3.4.1 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.



Restart	System Up Time	System Time	Severity	Log Message
432	00:04:16	Date/time not set	6 - Info	Spanning Tree: topology change detected.
432	00:03:33	Date/time not set	4 - Warning	SHDSL connection check: Could not reach remote device 192.168.50.48 (Failure count 1)
432	00:02:56	Date/time not set	6 - Info	Spanning Tree: topology change detected.
432	00:02:56	Date/time not set	6 - Info	Link up on SHDSL 1.
432	00:02:55	Date/time not set	6 - Info	Link up on SHDSL 2.
432	00:02:46	Date/time not set	6 - Info	Interface SHDSL 1 connection established.
432	00:02:45	Date/time not set	6 - Info	Interface SHDSL 2 connection established.
432	00:01:49	Date/time not set	6 - Info	Link down on SHDSL 2.
432	00:01:49	Date/time not set	6 - Info	Link down on SHDSL 1.
432	00:01:48	Date/time not set	4 - Warning	Interface SHDSL 2 connection lost.

1 - 10 of 1200 entries Show all

Description

- **Severity Filters**

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

  – 2 - Critical

    Critical

    When this parameter is enabled, all entries of the category "Critical" are displayed.

  – 4 - Warning

    warning

    When this parameter is enabled, all entries of the category "Warning" are displayed.

  – 6 - 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**

  If the system time is set, the date and time are also displayed at which the 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.

Description of the buttons and input boxes

"Clear" button

Click this button to delete the content of the event log file. All entries are deleted regardless of what you have selected in "Severity Filters".

The display is also cleared. The restart counter is only reset after you have restored the device to the factory settings and restarted the device.

Note

The number of entries in this table is restricted to 1200. The table can contain 400 entries for each severity. When this number is reached, the oldest entries of the relevant severity are discarded. The table remains permanently in memory.

"Show all" button

Click this button to display all the entries on the WBM page. Note that displaying all messages can take some time.

"Next" button

Click this button to go to the next page.

"Prev" button

Click this button to go to the previous page.

Drop-down list for page change

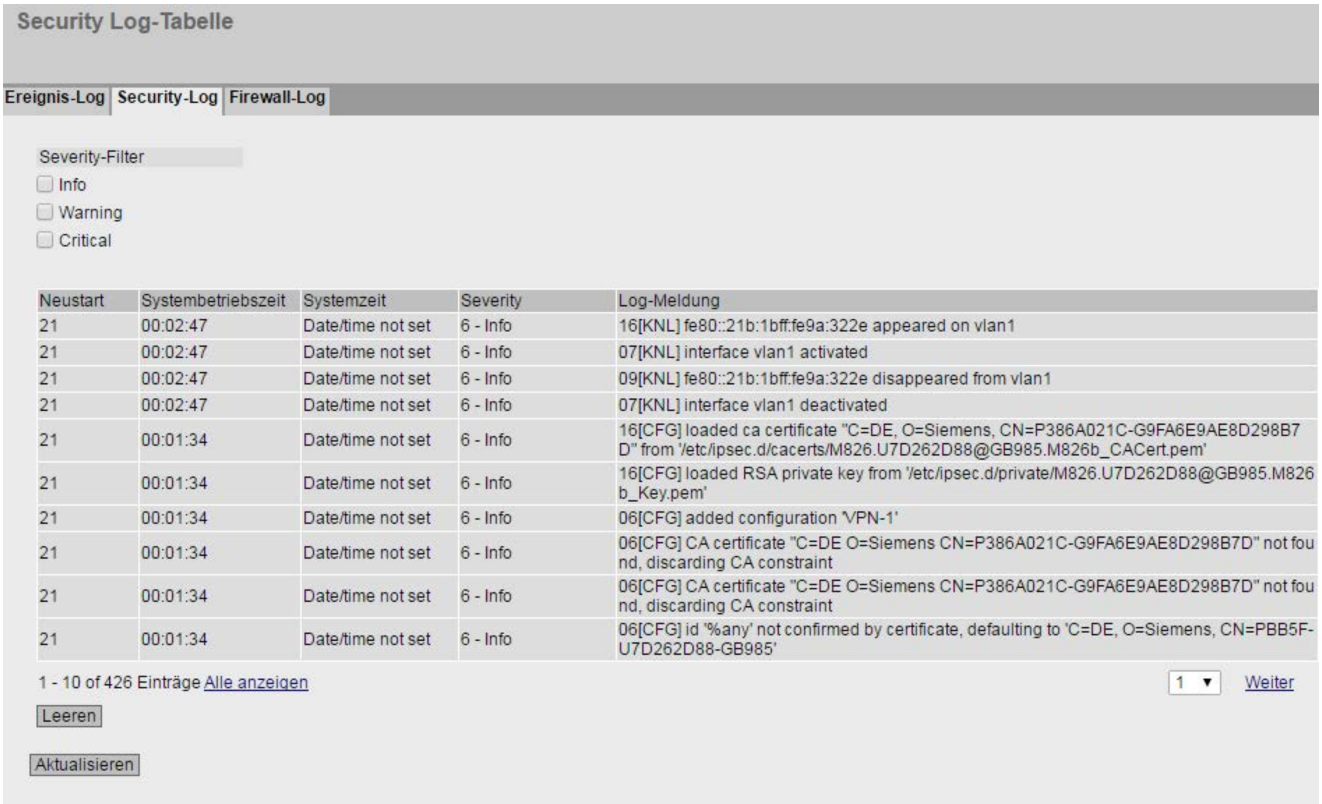
From the drop-down list, select the page you want to go to.

"Update" button

Refreshes the display of the values in the table.

4.3.4.2 Security Log

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



Neustart	Systembetriebszeit	Systemzeit	Severity	Log-Meldung
21	00:02:47	Date/time not set	6 - Info	16[KNL] fe80::21b:1bff:fe9a:322e appeared on vlan1
21	00:02:47	Date/time not set	6 - Info	07[KNL] interface vlan1 activated
21	00:02:47	Date/time not set	6 - Info	09[KNL] fe80::21b:1bff:fe9a:322e disappeared from vlan1
21	00:02:47	Date/time not set	6 - Info	07[KNL] interface vlan1 deactivated
21	00:01:34	Date/time not set	6 - Info	16[CFG] loaded ca certificate "C=DE, O=Siemens, CN=P386A021C-G9FA6E9AE8D298B7D" from '/etc/ipsec.d/cacerts/M826.U7D262D88@GB985.M826b_CACert.pem'
21	00:01:34	Date/time not set	6 - Info	16[CFG] loaded RSA private key from '/etc/ipsec.d/private/M826.U7D262D88@GB985.M826b_Key.pem'
21	00:01:34	Date/time not set	6 - Info	06[CFG] added configuration 'VPN-1'
21	00:01:34	Date/time not set	6 - Info	06[CFG] CA certificate "C=DE O=Siemens CN=P386A021C-G9FA6E9AE8D298B7D" not found, discarding CA constraint
21	00:01:34	Date/time not set	6 - Info	06[CFG] CA certificate "C=DE O=Siemens CN=P386A021C-G9FA6E9AE8D298B7D" not found, discarding CA constraint
21	00:01:34	Date/time not set	6 - Info	06[CFG] id '%any' not confirmed by certificate, defaulting to 'C=DE, O=Siemens, CN=PBB5F-U7D262D88-GB985'

Description

- **Severity Filters**

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

  - 2 - Critical

    Critical

    When this parameter is enabled, all entries of the category "Critical" are displayed.
  - 4 - Warning

    warning

    When this parameter is enabled, all entries of the category "Warning" are displayed.
  - 6 - 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**

  If the system time is set, the date and time are also displayed at which the 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.

Description of the buttons and input boxes

"Clear" button

Click this button to delete the content of the event log file. All entries are deleted regardless of what you have selected in "Severity Filters".

The display is also cleared. The restart counter is only reset after you have restored the device to the factory settings and restarted the device.

Note

The number of entries in this table is restricted to 1200. The table can contain 400 entries for each severity. When this number is reached, the oldest entries of the relevant severity are discarded. The table remains permanently in memory.

"Show all" button

Click this button to display all the entries on the WBM page. Note that displaying all messages can take some time.

"Next" button

Click this button to go to the next page.

"Prev" button

Click this button to go to the previous page.

Drop-down list for page change

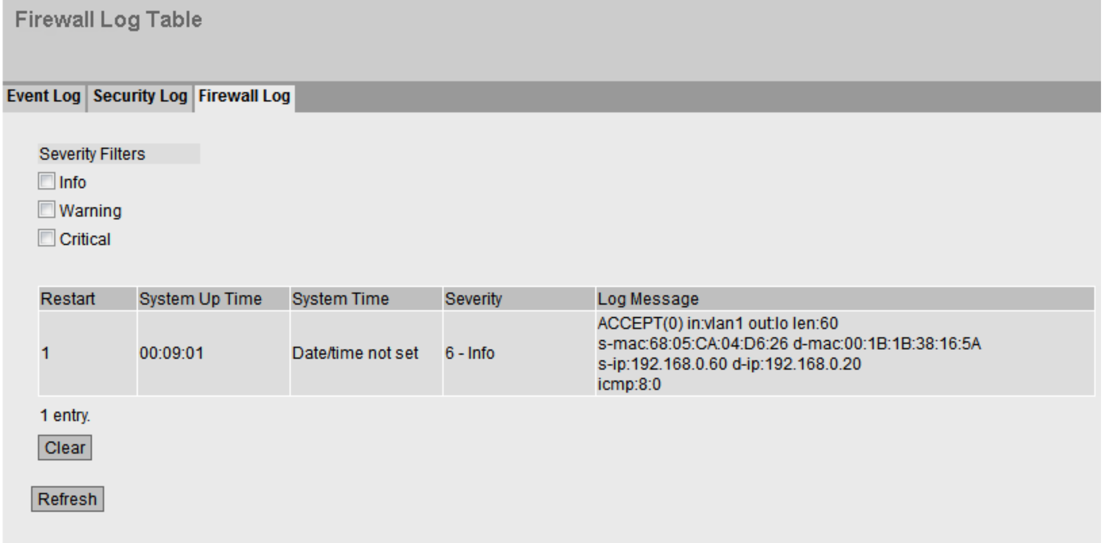
From the drop-down list, select the page you want to go to.

"Update" button

Refreshes the display of the values in the table.

4.3.4.3 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.



Severity Filters

☐ Info

☐ Warning

☐ Critical

Restart	System Up Time	System Time	Severity	Log Message
1	00:09:01	Date/time not set	6 - Info	ACCEPT(0) in:vlan1 out:lo len:60 s-mac:68:05:CA:04:D6:26 d-mac:00:1B:1B:38:16:5A s-ip:192.168.0.60 d-ip:192.168.0.20 icmp:8:0

1 entry.

Description

- **Severity Filters**

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

  - 2 - Critical

    Critical

    When this parameter is enabled, all entries of the category "Critical" are displayed.

  - 4 - Warning

    warning

    When this parameter is enabled, all entries of the category "Warning" are displayed.

  - 6 - 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**

  If the system time is set, the date and time are also displayed at which the 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.

Description of the buttons and input boxes

"Clear" button

Click this button to delete the content of the event log file. All entries are deleted regardless of what you have selected in "Severity Filters".

The display is also cleared. The restart counter is only reset after you have restored the device to the factory settings and restarted the device.

Note

The number of entries in this table is restricted to 1200. The table can contain 400 entries for each severity. When this number is reached, the oldest entries of the relevant severity are discarded. The table remains permanently in memory.

"Show all" button

Click this button to display all the entries on the WBM page. Note that displaying all messages can take some time.

"Next" button

Click this button to go to the next page.

"Prev" button

Click this button to go to the previous page.

Drop-down list for page change

From the drop-down list, select the page you want to go to.

"Update" button

Refreshes the display of the values in the table.

4.3.5 Faults

Fault status

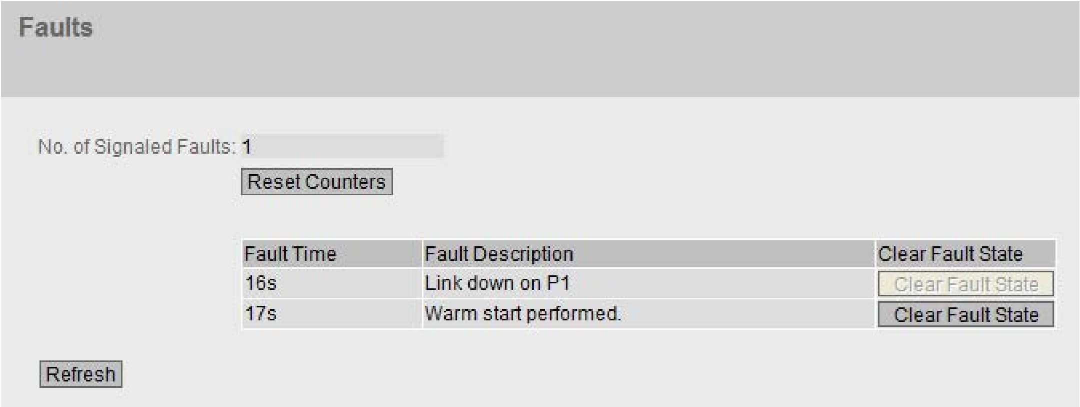
If a fault occurs, it is shown on this page. On the device, faults are indicated by the red fault LED lighting up.

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

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

Faults of the "Cold/Warm Start" event can be deleted by a confirmation. 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.



Faults

No. of Signaled Faults: 1

Fault Time	Fault Description	Clear Fault State
16s	Link down on P1	Clear Fault State
17s	Warm start performed.	Clear Fault State

Description

The page contains the following boxes:

- **No. of Signaled Faults**

  Number of faults displayed since the last startup.

- **Reset Counters**

  Click "Reset Counter" to reset the counter. The counter is reset when there is a restart.

The table contains the following columns:

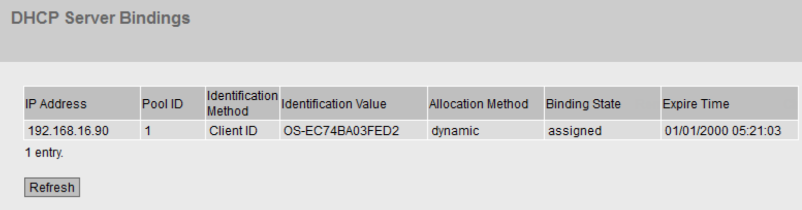
- **Fault Time**
  Shows the time the device has been running since the last system restart when the described fault occurred.

- **Fault Description**
  Displays a brief description of the fault that has occurred.

- **Clear Fault State**
  If the "Clear Fault State" button is enabled, you can delete the fault.

4.3.6 DHCP Server

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



DHCP Server Bindings

IP Address	Pool ID	Identification Method	Identification Value	Allocation Method	Binding State	Expire Time
192.168.16.90	1	Client ID	OS-EC74BA03FED2	dynamic	assigned	01/01/2000 05:21:03

1 entry.

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.

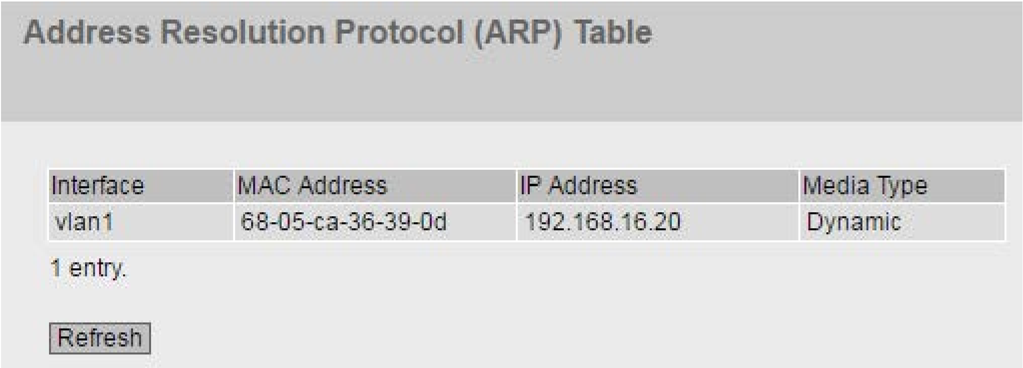
- **Expire Time**
  Shows how long the assigned IPv4 address is still valid. When half the period of validity has elapsed. the DHCP client can extend the period of the assigned IPv4 address. When the entire time has elapsed, the DHCP client needs to request a new IPv4 address.

4.3.7 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".



Address Resolution Protocol (ARP) Table

Interface	MAC Address	IP Address	Media Type
vlan1	68-05-ca-36-39-0d	192.168.16.20	Dynamic

1 entry.

Description of the displayed values

This 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 PST (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

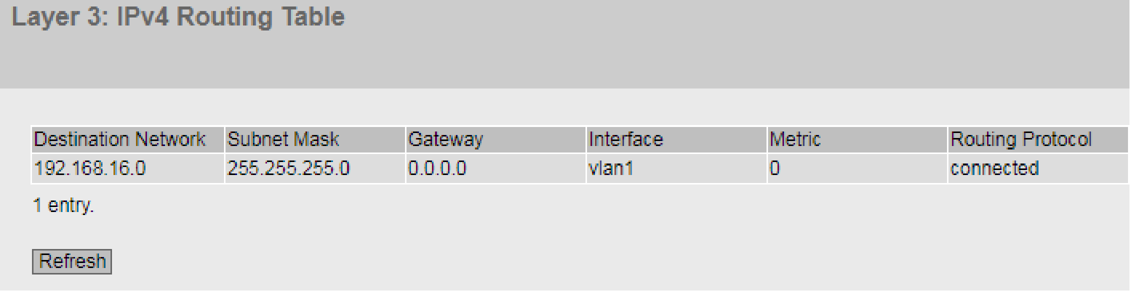
- **Port ID**

  Port of the device with which the device is connected.

4.3.8 Routing

Introduction

This page shows the routes currently being used.



Layer 3: IPv4 Routing Table

Destination Network	Subnet Mask	Gateway	Interface	Metric	Routing Protocol
192.168.16.0	255.255.255.0	0.0.0.0	vlan1	0	connected

1 entry.

Description

The table has the following columns:

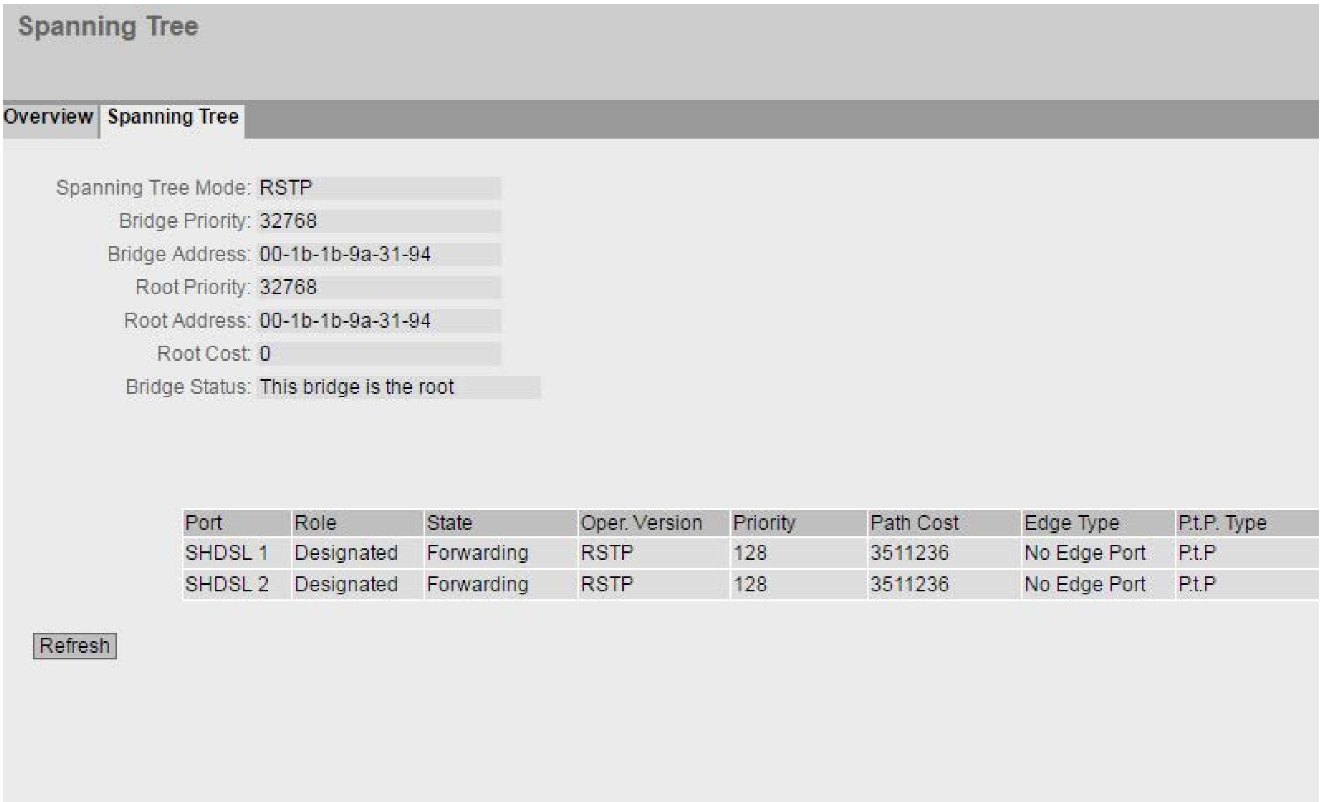
- **Destination Network**
  Shows the destination address of this route.
- **Subnet Mask**
  Shows the subnet mask of this route.
- **Gateway**
  Shows the gateway for this route.
- **Interface**
  Shows the interface for this route.
- **Metric**
  Shows the metric of the route. The higher value, the 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

4.3.9 Redundancy

4.3.9.1 Spanning Tree

Introduction

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



Spanning Tree

Spanning Tree Mode: RSTP
Bridge Priority: 32768
Bridge Address: 00-1b-1b-9a-31-94
Root Priority: 32768
Root Address: 00-1b-1b-9a-31-94
Root Cost: 0
Bridge Status: This bridge is the root

Port	Role	State	Oper. Version	Priority	Path Cost	Edge Type	P.t.P. Type
SHDSL 1	Designated	Forwarding	RSTP	128	3511236	No Edge Port	P.t.P
SHDSL 2	Designated	Forwarding	RSTP	128	3511236	No Edge Port	P.t.P

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

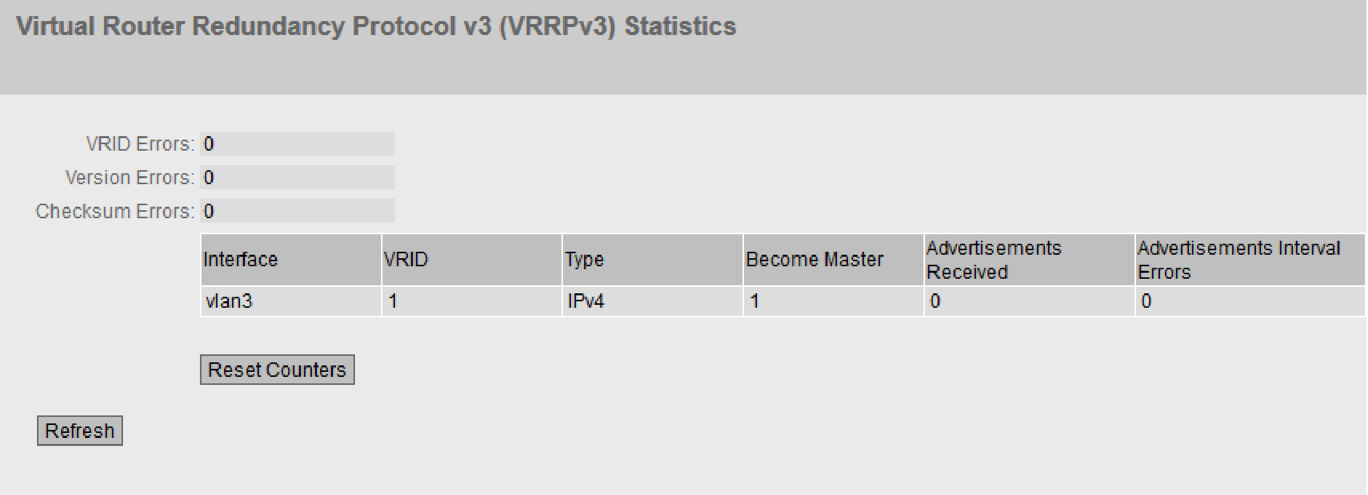
  – 10 Mbps = 2,000,000

- **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.

4.3.9.2 VRRPv3 Statistics

Introduction

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



Virtual Router Redundancy Protocol v3 (VRRPv3) Statistics

VRID Errors: 0
Version Errors: 0
Checksum Errors: 0

Interface	VRID	Type	Become Master	Advertisements Received	Advertisements Interval Errors
vlan3	1	IPv4	1	0	0

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**

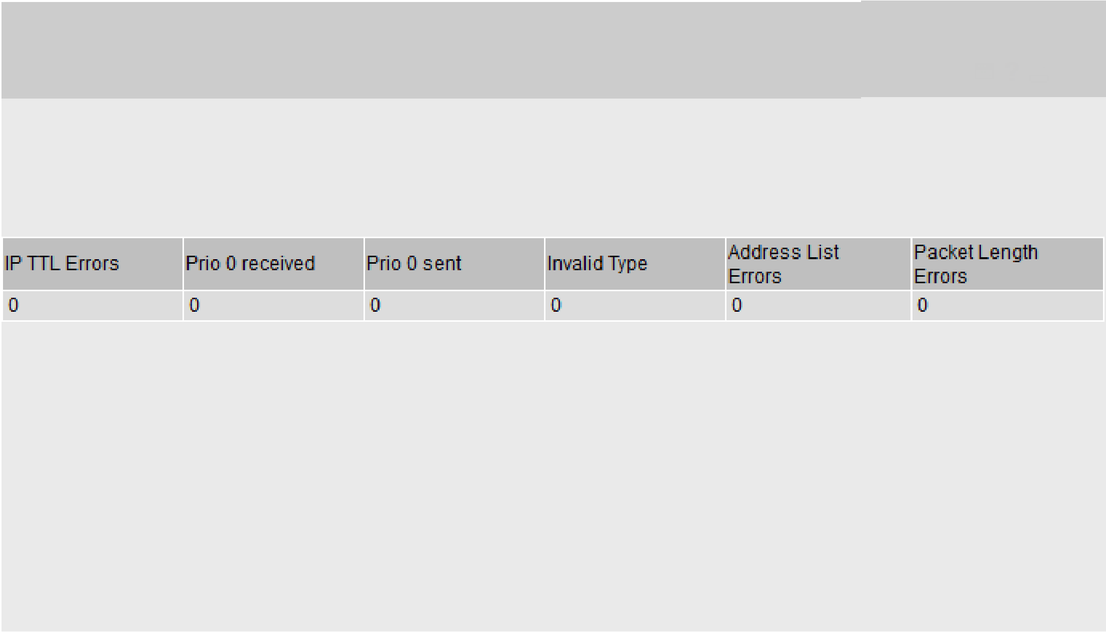
  Shows the ID of the virtual router. Valid values are 1 ... 255.
- **Address Type**

  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**

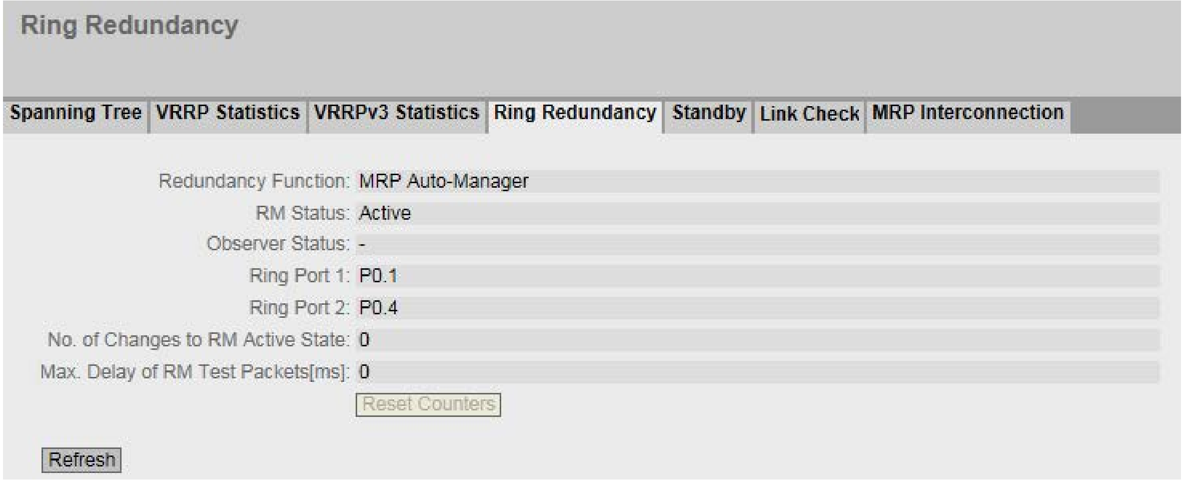
  Shows how many bad VRRPv3 packets were received whose address list does not match the locally configured list.
- **Packet Length Errors**

  Shows how many bad VRRPv3 packets were received whose length is not correct.

4.3.9.3 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.



Redundancy Function: MRP Auto-Manager
RM Status: Active
Observer Status: -
Ring Port 1: P0.1
Ring Port 2: P0.4
No. of Changes to RM Active State: 0
Max. Delay of RM Test Packets[ms]: 0

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.

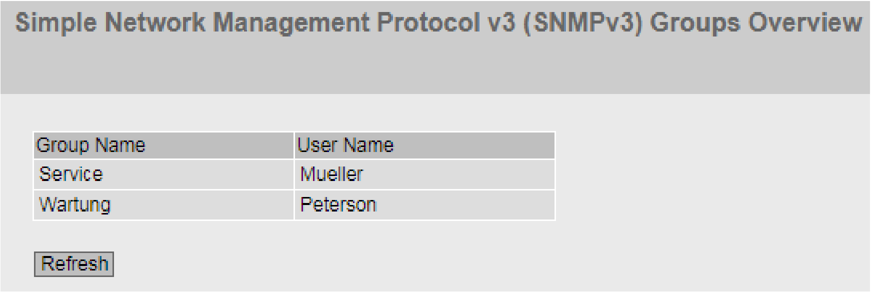
Description of the button

"Reset Counters" button

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

4.3.10 SNMP

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



Simple Network Management Protocol v3 (SNMPv3) Groups Overview

Group Name	User Name
Service	Mueller
Wartung	Peterson

Description

The table has the following columns:

- **Group Name**

  Shows the group name.

- **User Name**

  Shows the user that is assigned to the group.

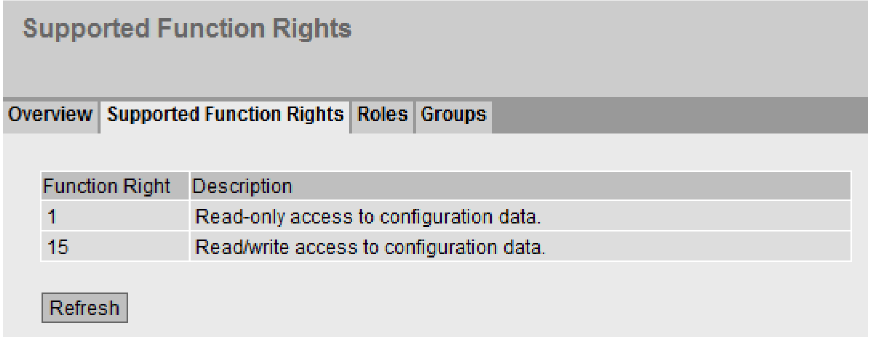
4.3.11 Security

4.3.11.1 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.



Function Right	Description
1	Read-only access to configuration data.
15	Read/write access to configuration data.

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**

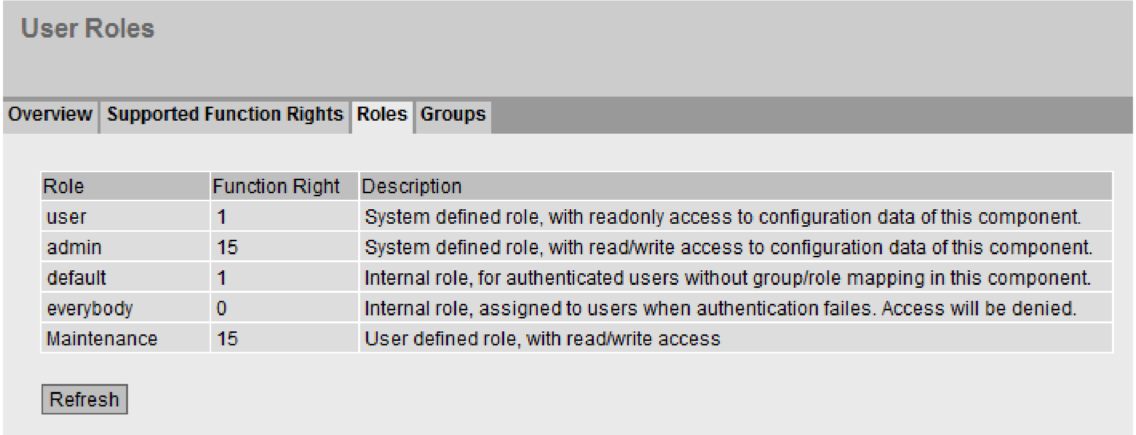
  Shows the description of the function right.

4.3.11.2 Roles

Note

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

The page shows the roles valid locally on the device.



Role	Function Right	Description
user	1	System defined role, with readonly access to configuration data of this component.
admin	15	System defined role, with read/write access to configuration data of this component.
default	1	Internal role, for authenticated users without group/role mapping in this component.
everybody	0	Internal role, assigned to users when authentication failes. Access will be denied.
Maintenance	15	User defined role, with read/write access

Description of the displayed values

This 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**

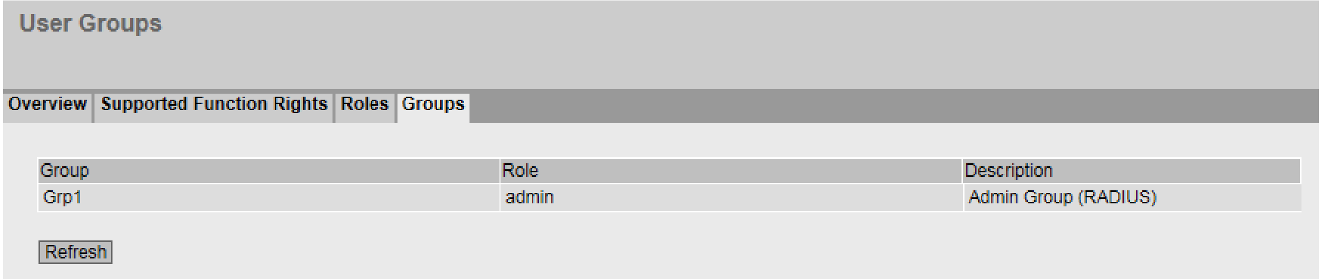
  Shows a description of the role.

4.3.11.3 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 roll is defined locally on the device.



Group	Role	Description
Grp1	admin	Admin Group (RADIUS)

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**

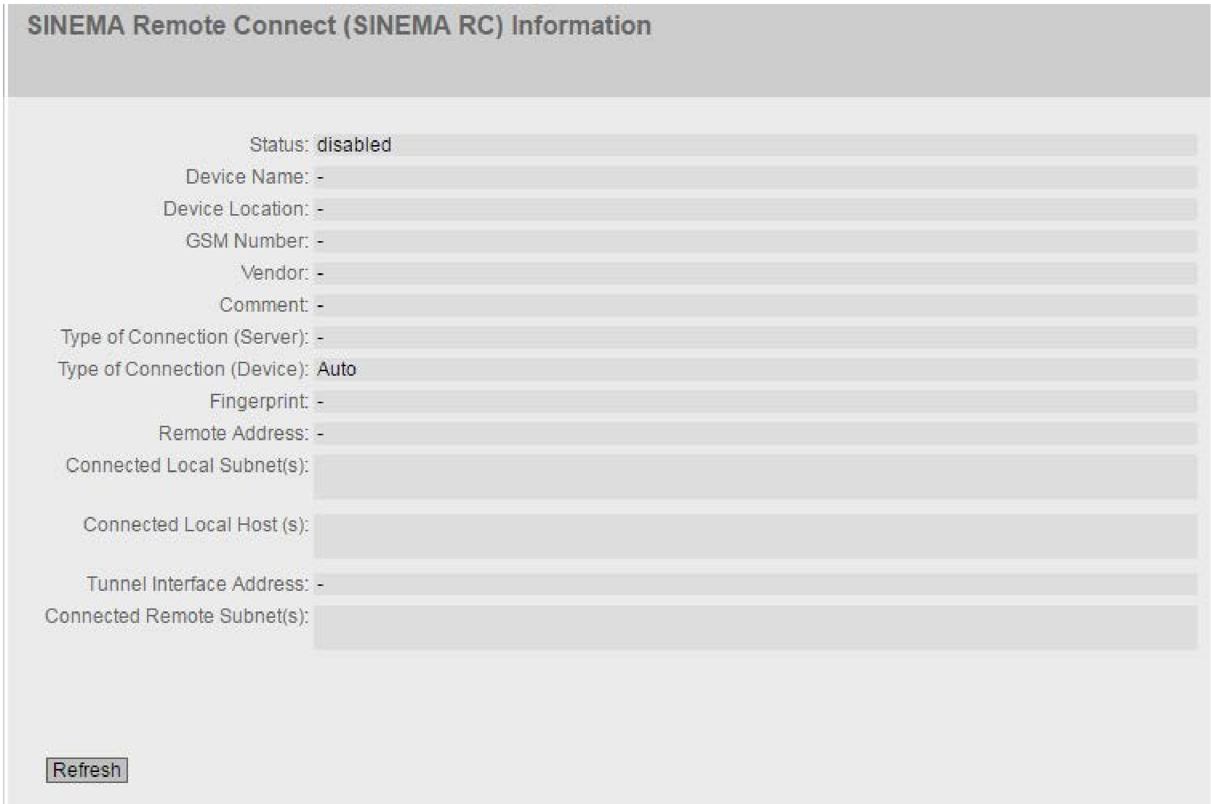
  Shows the name of the role. Users who are authenticated with the linked group on the RADIUS server receive the rights of this role locally on the device.

- **Description**

  Shows a a description for the link.

4.3.12 IPSec VPN (SC64x-2C)

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



SINEMA Remote Connect (SINEMA RC) Information

Status:	disabled
Device Name:	-
Device Location:	-
GSM Number:	-
Vendor:	-
Comment:	-
Type of Connection (Server):	-
Type of Connection (Device):	Auto
Fingerprint:	-
Remote Address:	-
Connected Local Subnet(s):	
Connected Local Host (s):	
Tunnel Interface Address:	-
Connected Remote Subnet(s):	

Description of the displayed values

This 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**

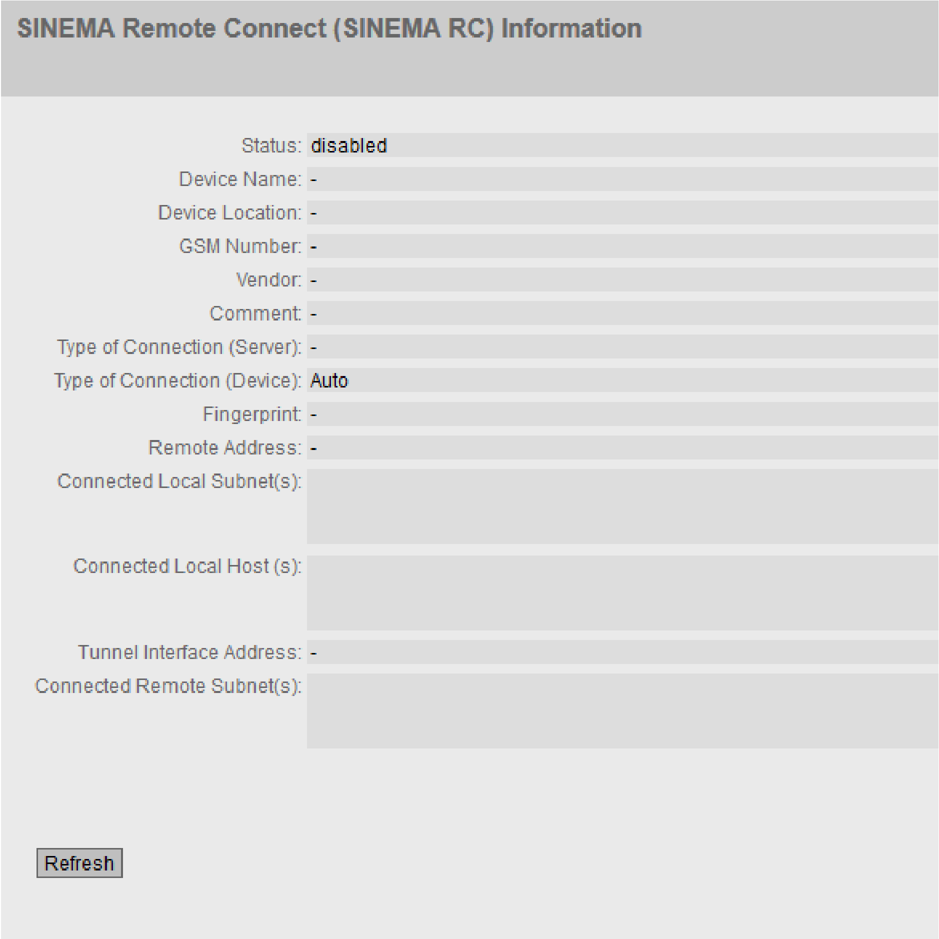
  Shows the remote subnet.
- **Rekey Time**

  Shows when the validity of the key expires.
- **Status**

  Shows the status of the VPN connection.

4.3.13 SINEMA RC

Shows information on SINEMA RC Server



SINEMA Remote Connect (SINEMA RC) Information

Status:	disabled
Device Name:	-
Device Location:	-
GSM Number:	-
Vendor:	-
Comment:	-
Type of Connection (Server):	-
Type of Connection (Device):	Auto
Fingerprint:	-
Remote Address:	-
Connected Local Subnet(s):	
Connected Local Host (s):	
Tunnel Interface Address:	-
Connected Remote Subnet(s):	

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.

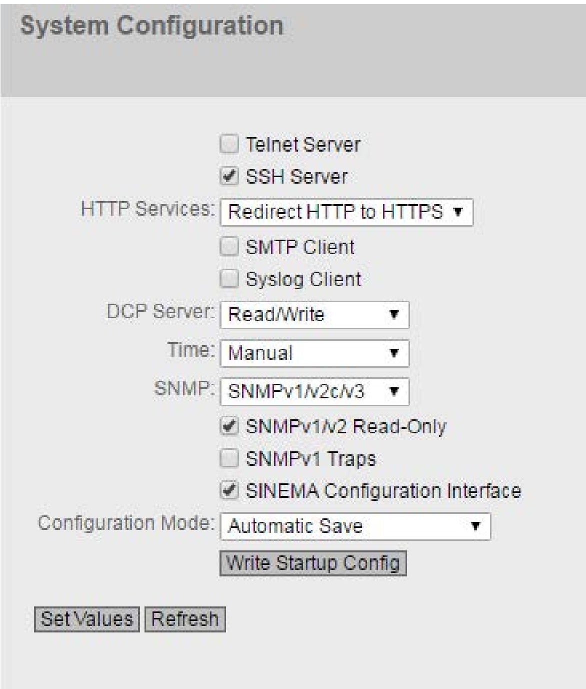
4.4 "System" menu

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.



System Configuration

□ Telnet Server
☑ SSH Server
HTTP Services: Redirect HTTP to HTTPS ▼
□ SMTP Client
□ Syslog Client
DCP Server: Read/Write ▼
Time: Manual ▼
SNMP: SNMPv1/v2c/v3 ▼
☑ SNMPv1/v2 Read-Only
□ SNMPv1 Traps
☑ SINEMA Configuration Interface
Configuration Mode: Automatic Save ▼

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.
- **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.

- **Default Login Page**

  Specify the login page with which the WBM starts by default.

  – Firewall

    Logging into the WBM page for user-specific firewall.

  – Configuration

    Logging into the WBM.

- **Syslog Client**
  Enable or disable the Syslog client. You can configure other settings in "System > Syslog Client".

- **DCP Server**
  Specify whether or not 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 using a SIMATIC time transmitter. 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 as of V15.
- **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.

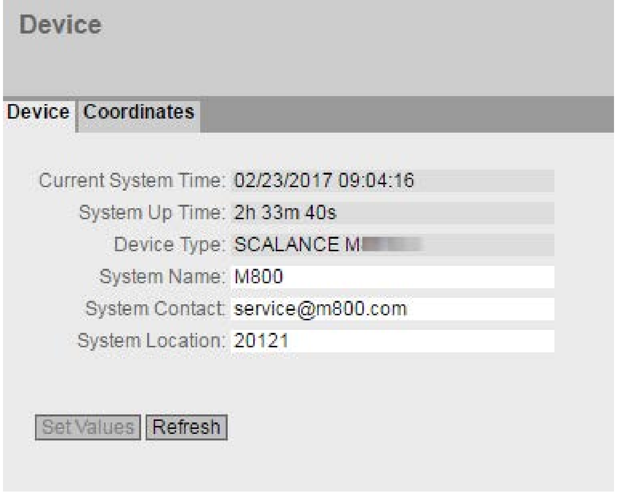
Procedure

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.



Device

Current System Time: 02/23/2017 09:04:16
System Up Time: 2h 33m 40s
Device Type: SCALANCE M[redacted]
System Name: M800
System Contact: service@m800.com
System Location: 20121

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 boxes **"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

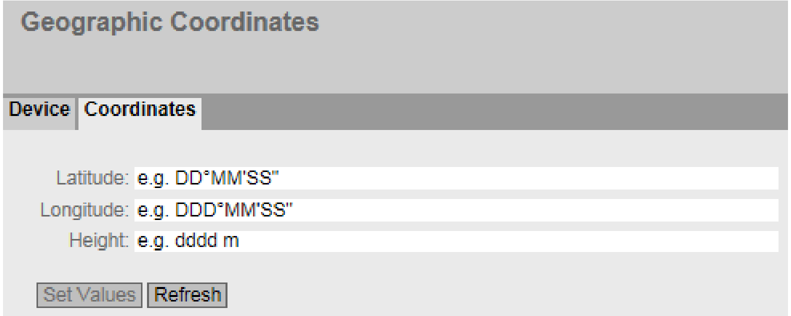
Information on geographic coordinates

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.



Latitude: e.g. DD°MM'SS"
Longitude: e.g. DDD°MM'SS"
Height: e.g. dddd m

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.

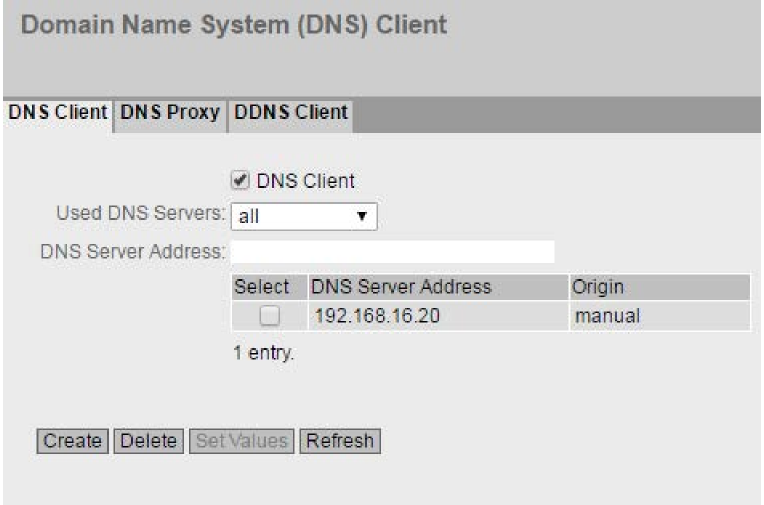
Procedure

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.



Domain Name System (DNS) Client

☑ DNS Client

Used DNS Servers: all ▼

DNS Server Address:

Select	DNS Server Address	Origin
□	192.168.16.20	manual

1 entry.

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**

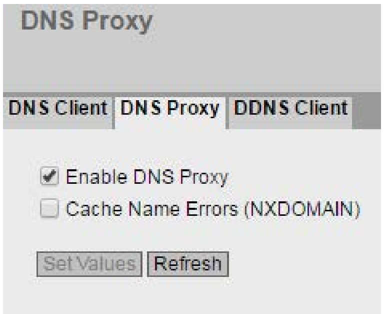
  Shows the IP address of the DNS server.
- **Origin**

  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.



☑ Enable DNS Proxy

□ Cache Name Errors (NXDOMAIN)

Description

The page contains the following boxes:

- **Enable DNS Proxy**

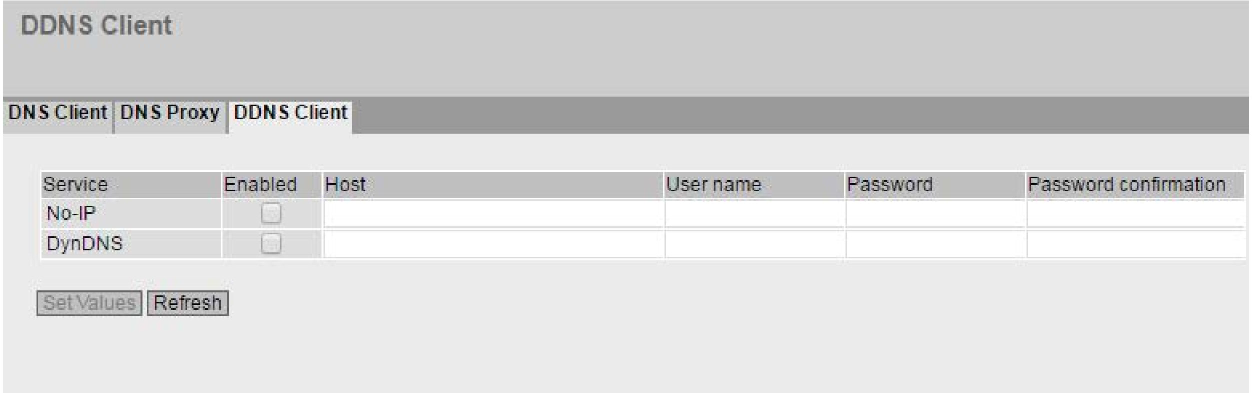
  Enable or disable the proxy of the DNS server.
- **Cache Name Errors (NXDOMAIN)**

  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.



DDNS Client

Service	Enabled	Host	User name	Password	Password confirmation
No-IP	□				
DynDNS	□				

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:

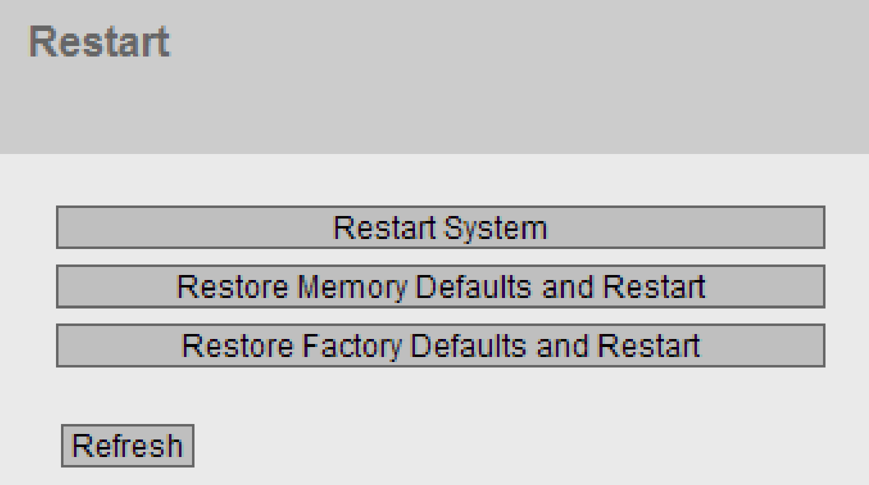
- User name and password that gives you the right to use the DDNS service.
- Registered hostname, e.g. example.no-ip.com
- UDP port 53 for DNS is enabled and is not used for NAPT.

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".

4.4.4 Restart

Resetting to the defaults

In this menu, there is a button with which you can restart the device and various options for resetting to the device defaults.


Restart
Restart System
Restore Memory Defaults and Restart
Restore Factory Defaults and Restart
Refresh

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.
- 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 "Trial Mode", configuration modifications must be saved manually before a restart. 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 configuration settings with the exception of the following parameters and to restart:
  - IP addresses
  - Subnet mask
  - IP address of the default gateway
  - DHCP client ID
  - DHCP
  - System name
  - System location
  - System contact
  - User names and passwords
- **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, refer to the section "Requirements for operation (Page 23)".

4.4.5 Load&Save

4.4.5.1 File list

Overview of the file types

File type	Description
Config	This file contains the start configuration. Among other things, this file contains the settings for users, roles, groups and function rights. The passwords are stored the file "Users".
ConfigPack	ZIP file consisting of the Config, Users and LSYS file, which means the entire configuration. Recommended for a backup of the configuration.
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.
Firmware	The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be downloaded to the device.
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. 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 "Passwords (Page 120)".
LogFile	File with entries from the event log table
MIB	Private MSPS MIB file
RunningCLI	Text file with CLI commands This file contains an overview of the current configuration in the form of CLI commands. You can download the text file. The file is not intended to be uploaded again unchanged.
StartupInfo	Startup log file This file contains the messages that were entered in the log during the last startup.
Users	This file contains the assignment of the user names to the corresponding passwords.

File type	Description
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.
X509Cert	Various nodes are certified with certificates. The following device types can be loaded on the device: .crt, .p12, .pem 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 "Passwords (Page 120)". The loaded files are listed on "Security > Certificates > Overview (Page 238)". For more information on certificates, refer to section "Certificates (Page 53)".

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

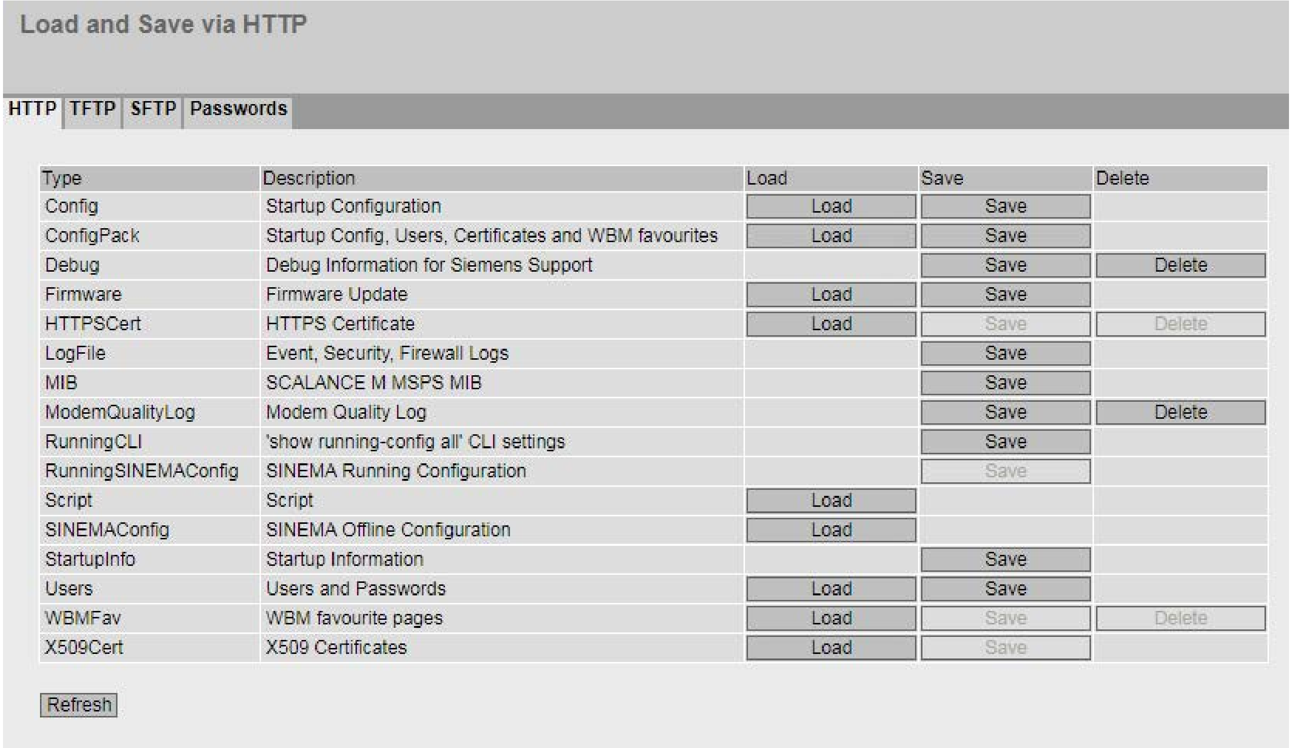
  You can save the faulty configuration of a device as "RunningSINEMAConfig" via the WBM and import it in STEP 7 Basic/Professional. No connection to a real device is required for the diagnostics in STEP 7 Basic/Professional. You can export a corrected configuration and load it as "SINEMAConfig" again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



Load and Save via HTTP

Type	Description	Load	Save	Delete
Config	Startup Configuration	Load	Save	
ConfigPack	Startup Config, Users, Certificates and WBM favourites	Load	Save	
Debug	Debug Information for Siemens Support		Save	Delete
Firmware	Firmware Update	Load	Save	
HTTPSCert	HTTPS Certificate	Load	Save	Delete
LogFile	Event, Security, Firewall Logs		Save	
MIB	SCALANCE M MSPS MIB		Save	
ModemQualityLog	Modem Quality Log		Save	Delete
RunningCLI	'show running-config all' CLI settings		Save	
RunningSINEMAConfig	SINEMA Running Configuration		Save	
Script	Script	Load		
SINEMAConfig	SINEMA Offline Configuration	Load		
StartupInfo	Startup Information		Save	
Users	Users and Passwords	Load	Save	
WBMFav	WBM favourite pages	Load	Save	Delete
X509Cert	X509 Certificates	Load	Save	

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

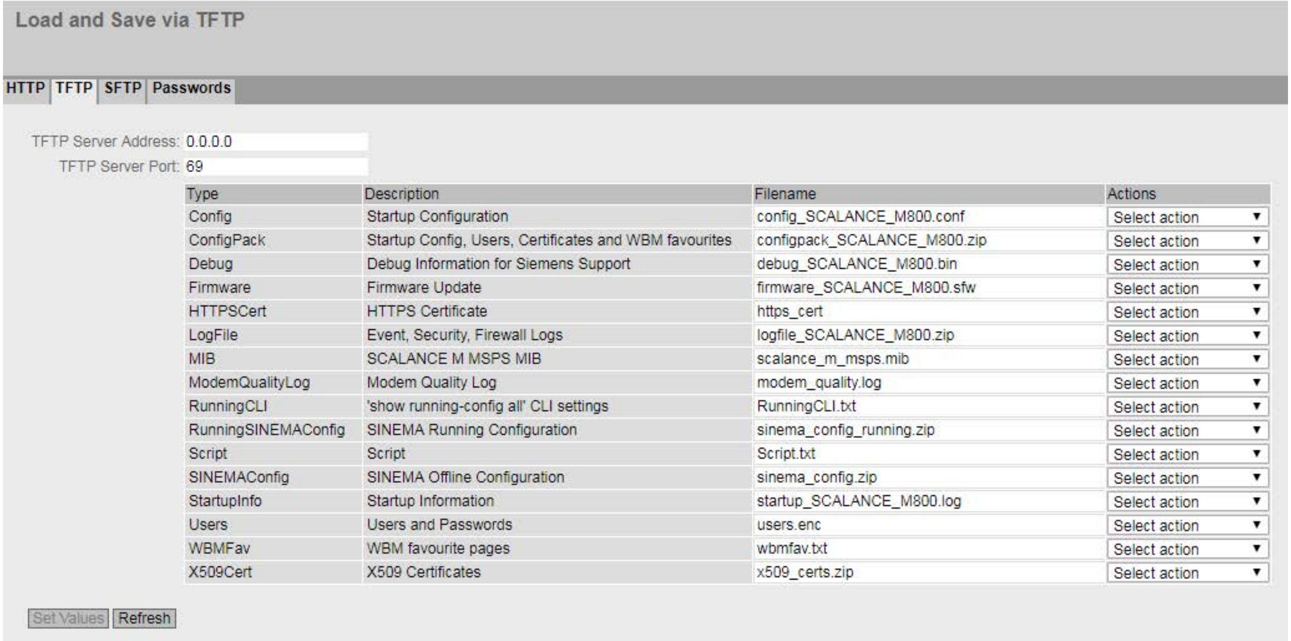
  You can save the faulty configuration of a device as "RunningSINEMAConfig" via the WBM and import it in STEP 7 Basic/Professional. No connection to a real device is required for the diagnostics in STEP 7 Basic/Professional. You can export a corrected configuration and load it as "SINEMAConfig" again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



TFTP Server Address: 0.0.0.0
TFTP Server Port: 69

Type	Description	Filename	Actions
Config	Startup Configuration	config_SCALANCE_M800.conf	Select action ▼
ConfigPack	Startup Config, Users, Certificates and WBM favourites	configpack_SCALANCE_M800.zip	Select action ▼
Debug	Debug Information for Siemens Support	debug_SCALANCE_M800.bin	Select action ▼
Firmware	Firmware Update	firmware_SCALANCE_M800.sfw	Select action ▼
HTTPSCert	HTTPS Certificate	https_cert	Select action ▼
LogFile	Event, Security, Firewall Logs	logfile_SCALANCE_M800.zip	Select action ▼
MIB	SCALANCE M MSPS MIB	scalance_m_msps.mib	Select action ▼
ModemQualityLog	Modem Quality Log	modem_quality.log	Select action ▼
RunningCLI	'show running-config all' CLI settings	RunningCLI.txt	Select action ▼
RunningSINEMAConfig	SINEMA Running Configuration	sinema_config_running.zip	Select action ▼
Script	Script	Script.txt	Select action ▼
SINEMAConfig	SINEMA Offline Configuration	sinema_config.zip	Select action ▼
StartupInfo	Startup Information	startup_SCALANCE_M800.log	Select action ▼
Users	Users and Passwords	users.enc	Select action ▼
WBMFav	WBM favourite pages	wbmfav.txt	Select action ▼
X509Cert	X509 Certificates	x509_certs.zip	Select action ▼

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

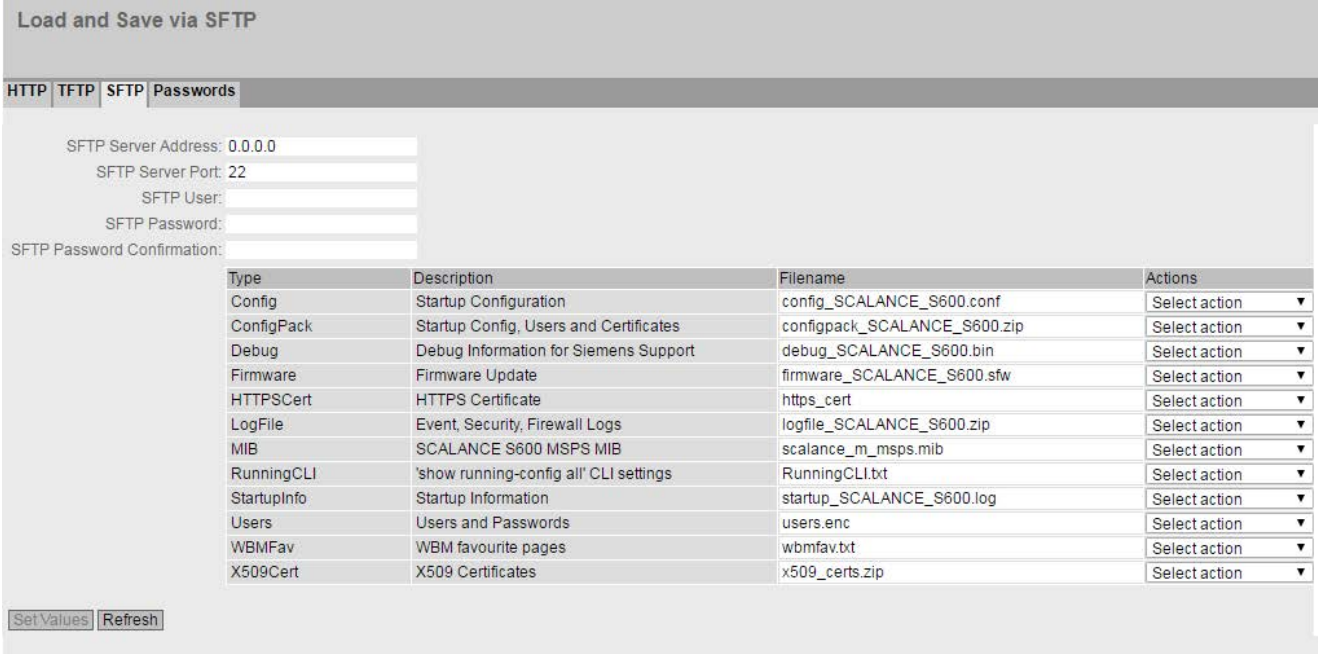
  You can save the faulty configuration of a device as "RunningSINEMAConfig" via the WBM and import it in STEP 7 Basic/Professional. No connection to a real device is required for the diagnostics in STEP 7 Basic/Professional. You can export a corrected configuration and load it as "SINEMAConfig" again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



Load and Save via SFTP

SFTP Server Address: 0.0.0.0
SFTP Server Port: 22
SFTP User:
SFTP Password:
SFTP Password Confirmation:

Type	Description	Filename	Actions
Config	Startup Configuration	config_SCALANCE_S600.conf	Select action
ConfigPack	Startup Config, Users and Certificates	configpack_SCALANCE_S600.zip	Select action
Debug	Debug Information for Siemens Support	debug_SCALANCE_S600.bin	Select action
Firmware	Firmware Update	firmware_SCALANCE_S600.sfw	Select action
HTTPSCert	HTTPS Certificate	https_cert	Select action
LogFile	Event, Security, Firewall Logs	logfile_SCALANCE_S600.zip	Select action
MIB	SCALANCE S600 MSPS MIB	scalance_m_msps.mib	Select action
RunningCLI	'show running-config all' CLI settings	RunningCLI.txt	Select action
StartupInfo	Startup Information	startup_SCALANCE_S600.log	Select action
Users	Users and Passwords	users.enc	Select action
WBMFav	WBM favourite pages	wbmfav.txt	Select action
X509Cert	X509 Certificates	x509_certs.zip	Select action

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:

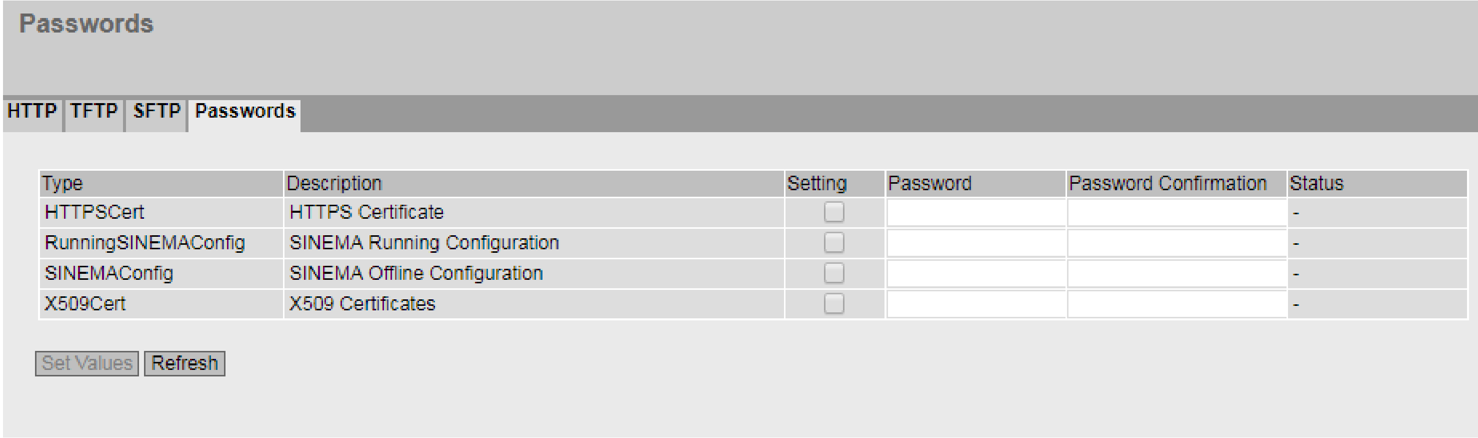
1. Save the configuration data of a configured device on your PC.
2. Load these configuration files on all other devices you want to configure in this way.
3. If individual settings are necessary for specific devices, these must be made online on the relevant device.

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.



Type	Description	Setting	Password	Password Confirmation	Status
HTTPSCert	HTTPS Certificate	□			-
RunningSINEMAConfig	SINEMA Running Configuration	□			-
SINEMAConfig	SINEMA Offline Configuration	□			-
X509Cert	X509 Certificates	□			-

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

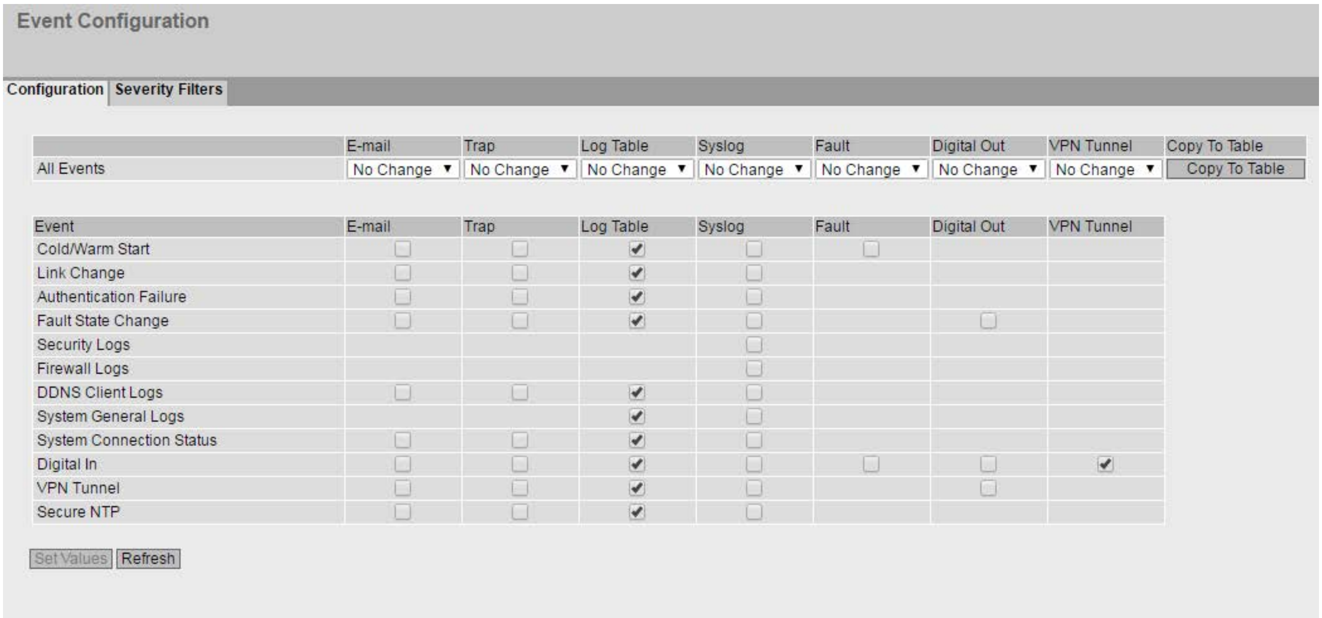
Selecting system events

On this WBM page, you specify which system events are logged and how.

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, select the "Syslog" check box for the event "System General Logs".



	E-mail	Trap	Log Table	Syslog	Fault	Digital Out	VPN Tunnel	Copy To Table
All Events	No Change ▼	No Change ▼	No Change ▼	No Change ▼	No Change ▼	No Change ▼	No Change ▼	Copy To Table

Event	E-mail	Trap	Log Table	Syslog	Fault	Digital Out	VPN Tunnel
Cold/Warm Start	□	□	☑	□	□		
Link Change	□	□	☑	□			
Authentication Failure	□	□	☑	□			
Fault State Change	□	□	☑	□		□	
Security Logs				□			
Firewall Logs				□			
DDNS Client Logs	□	□	☑	□			
System General Logs			☑	□			
System Connection Status	□	□	☑	□			
Digital In	□	□	☑	□	□	□	☑
VPN Tunnel	□	□	☑	□		□	
Secure NTP	□	□	☑	□			

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.
- **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.
  - 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.

  - Secure NTP
    An error occurred when using Secure NTP, e.g. a key with the wrong length was specified.
  - 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).

- **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:

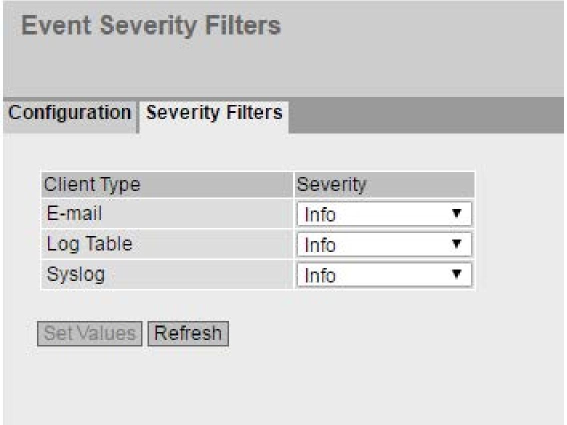
     In "Operation" set "wait on DI" or "start on DI". You can find more information on this in "IPsec VPN > Connections" and in "VPN connection establishment".
   - SINEMA RC:

     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 further 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.



Client Type	Severity
E-mail	Info
Log Table	Info
Syslog	Info

Description

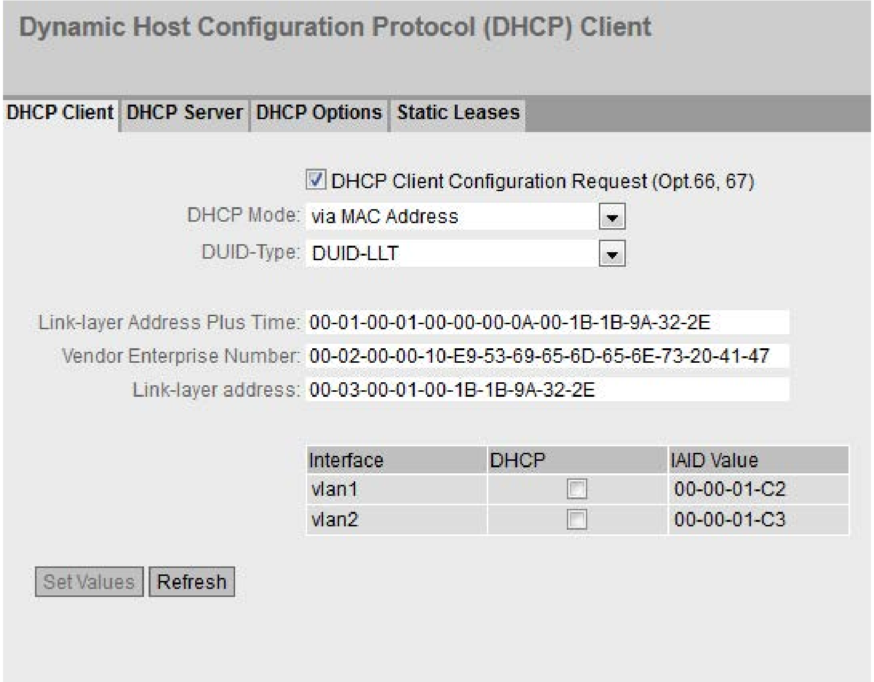
The table has the following columns:

- **Client Type**
  Select the client type for which you want to make settings:
  - **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 Severity are sent or logged.
  - **Warning**
    The message of this Severity and the "Critical" level are sent or logged.
  - **Critical**
    Only the messages of this Severity are sent or logged.

4.4.7 DHCP

4.4.7.1 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.



Dynamic Host Configuration Protocol (DHCP) Client

☑ DHCP Client Configuration Request (Opt.66, 67)

DHCP Mode: via MAC Address

DUID-Type: DUID-LLT

Link-layer Address Plus Time: 00-01-00-01-00-00-00-0A-00-1B-1B-9A-32-2E

Vendor Enterprise Number: 00-02-00-00-10-E9-53-69-65-6D-65-6E-73-20-41-47

Link-layer address: 00-03-00-01-00-1B-1B-9A-32-2E

Interface	DHCP	IAID Value
vlan1	□	00-00-01-C2
vlan2	□	00-00-01-C3

Description

The page contains the following boxes:

- **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.

The table has the following columns:

- **Interface**
  Interface to which the setting relates.
- **DHCP**
  Enable or disable the DHCP client for the relevant interface.

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.

4.4.7.2 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.

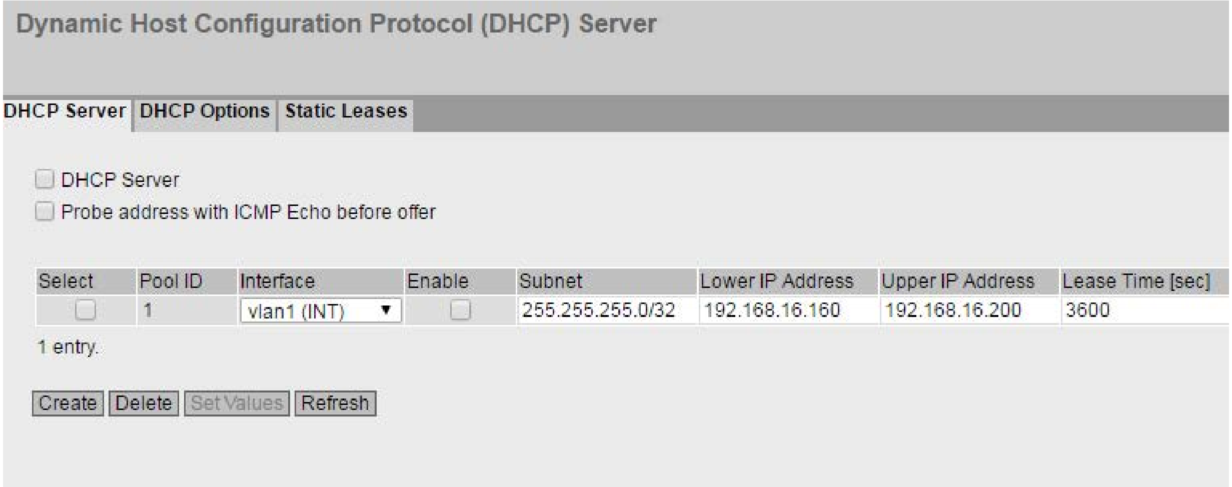
On this page, specify the address band from which the device receives any IP address. You configure the static assignment of the IP addresses in "Static Leases".

Note

Maximum number of IP addresses

The maximum number of IPv4 addresses that the DHCP server supports is 100. In other words, a total of 100 IPv4 addresses (dynamic + static).

With the static assignments, you can create a maximum of 20 entries.



□ DHCP Server
□ Probe address with ICMP Echo before offer

Select	Pool ID	Interface	Enable	Subnet	Lower IP Address	Upper IP Address	Lease Time [sec]
□	1	vlan1 (INT) ▼	□	255.255.255.0/32	192.168.16.160	192.168.16.200	3600

1 entry.

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".

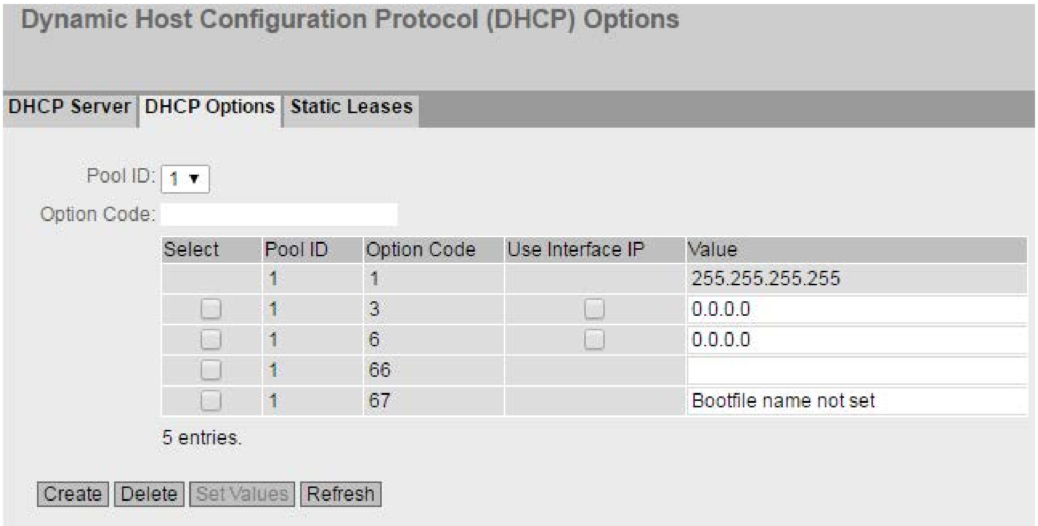
- **Upper IP address**

  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.

4.4.7.3 DHCP options

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



Dynamic Host Configuration Protocol (DHCP) Options

Pool ID: 1 ▾

Option Code:

Select	Pool ID	Option Code	Use Interface IP	Value
	1	1		255.255.255.255
□	1	3	□	0.0.0.0
□	1	6	□	0.0.0.0
□	1	66		
□	1	67		Bootfile name not set

5 entries.

Description

The page contains the following boxes:

- **Pool ID**

  Select the required address band.

- **Option Code**

  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 Code**

  Shows the number of the DHCP option.

- **Description**
  Text describing the option value.

- **Use Interface IP**

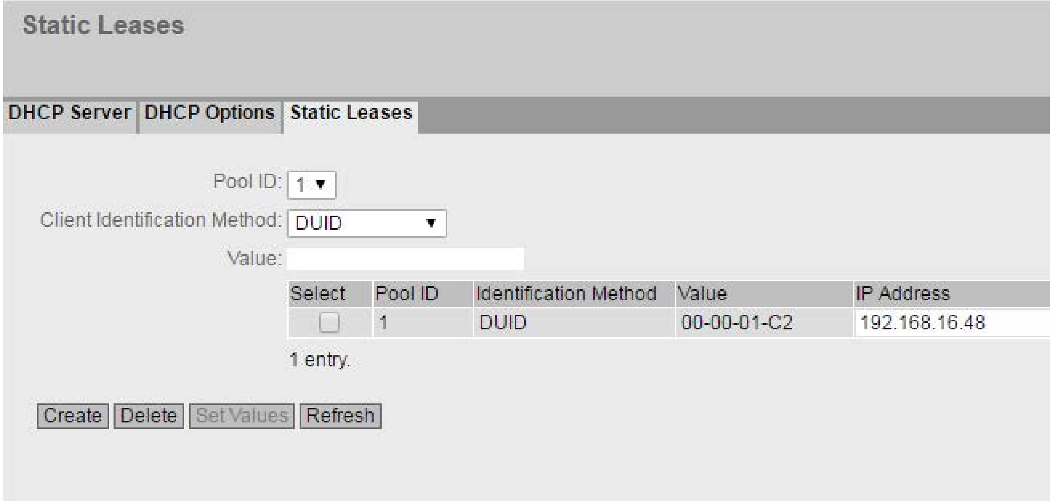
  Specify whether or not the internal IP address of the device will be used.

- **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.

4.4.7.4 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, based on the client ID.



Pool ID: 1

Client Identification Method: DUID

Value:

Select	Pool ID	Identification Method	Value	IP Address
□	1	DUID	00-00-01-C2	192.168.16.48

1 entry.

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".

- **Value**

  Enter the required value. The entry depends on the selected identification method of the client.

Note

A maximum of 20 entries are possible.

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, the client ID of the client.
- **IP Address**

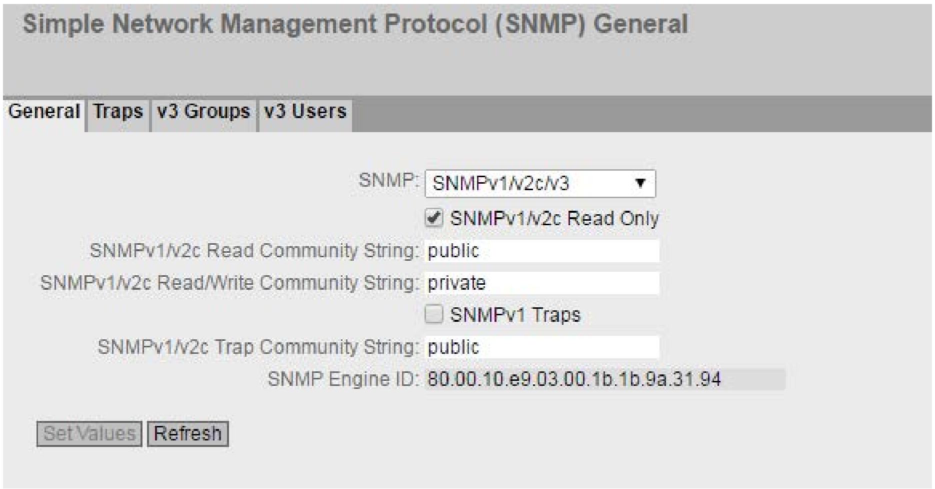
  Specify the IPv4 address that will be assigned to the client. The IPv4 address must be within the address band.

4.4.8 SNMP

4.4.8.1 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. Note the information in the section "Technical basics (Page 29)".



Simple Network Management Protocol (SNMP) General

SNMP: SNMPv1/v2c/v3 ▼

☑ SNMPv1/v2c Read Only

SNMPv1/v2c Read Community String: public

SNMPv1/v2c Read/Write Community String: private

☐ SNMPv1 Traps

SNMPv1/v2c Trap Community String: public

SNMP Engine ID: 80.00.10.e9.03.00.1b.1b.9a.31.94

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.
- **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.
- **SNMPv1 Traps**
  Enable or disable the sending of SNMPv1 traps (alarm frames). On the "Trap" tab, specify the IP addresses of the devices to which SNMPv1 traps will be sent.
- **SNMPv1/v2c Trap Community String**
  Enter the community string for sending SNMPv1/v2c messages.

- **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.

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.

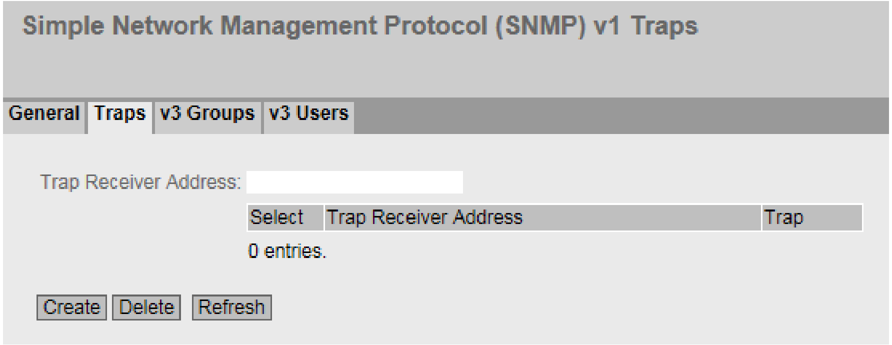
4.4.8.2 Traps

SNMP traps for alarm events

If an alarm event occurs, a device can send SNMP traps (alarm frames) to up to ten different management stations at the same time. Traps are only sent if the events specified in the "Events" menu occur.

Note

Traps are only sent if you have enabled the option "SNMPv1 Traps" in the "General" tab or in "System > Configuration".



Trap Receiver Address:

Select	Trap Receiver Address	Trap

0 entries.

Description

- **Trap Receiver Address**
  Enter the IP address or the FQDN (Fully Qualified Domain Name) of the station to which the device sends SNMP traps. You can specify up to ten different recipients servers.

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **Trap Receiver Address**
  If necessary, change the IP address or the FQDN (Fully Qualified Domain Name) of the stations.
- **Trap**
  Enable or disable the sending of traps. Stations that are entered but not selected do not receive SNMP traps.

Procedure

Creating a trap entry

1. In "Trap Receiver Address", enter the IP address or the FQDN of the station to which the device will send traps.
2. Click the "Create" button to create a new trap entry.

3. Select the check box in the required row "Trap".
4. Click the "Set Values" button.

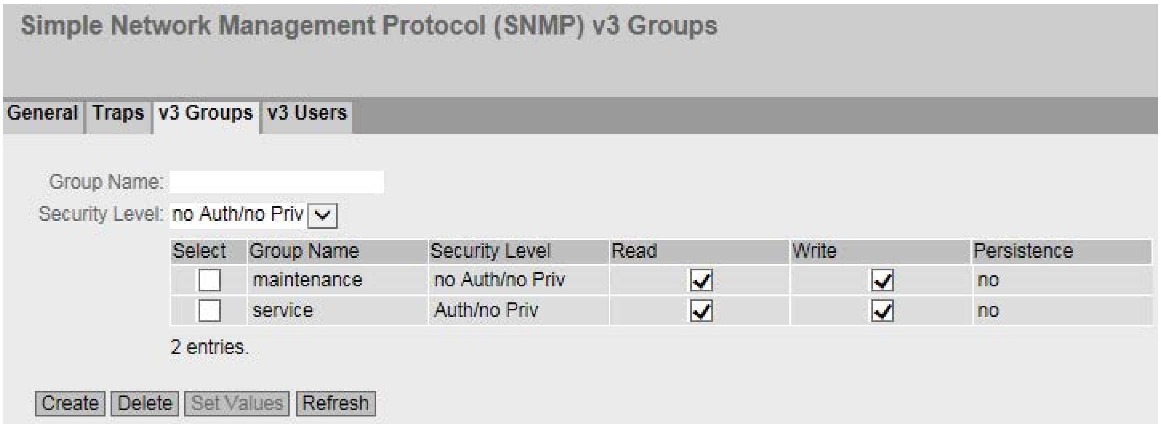
Deleting a trap entry

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

4.4.8.3 v3 Groups

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.



Simple Network Management Protocol (SNMP) v3 Groups

Group Name:
Security Level: no Auth/no Priv

Select	Group Name	Security Level	Read	Write	Persistence
□	maintenance	no Auth/no Priv	☑	☑	no
□	service	Auth/no Priv	☑	☑	no

2 entries.

Description

The page contains the following boxes:

- **Group Name**
  Enter the name of the group. The maximum length is 32 characters.
- **Security Level**
  Select the security level (authentication, encryption) valid for the selected group. The available options are as follows:
  - 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 defined group names.
- **Security Level**
  Shows the configured security level.
- **Read**
  Enable or disable read access for the required group.
- **Write**
  Enable or disable write access for the required group.

  Note

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

- **Persistence**
  Shows whether or not the group is assigned to an SNMPv3 user. If the group is not assigned to an SNMPv3 user, no automatic saving is triggered and the configured group is deleted after restarting the device.
  – Yes

    The group is assigned to an SNMPv3 user.
  – No

    The group is not assigned to an SNMPv3 user.

Procedure

Creating a new group

1. Enter the required group name in "Group Name".
2. Select the required security level from the "Security Level" drop-down list.
3. Click the "Create" button to create a new entry.
4. Specify the required read rights for the group in "Read".
5. Specify the required write rights for the group in "Write".
6. Click the "Set Values" button.

Modifying a group

1. Specify the required read rights for the group in "Read".
2. Specify the required write rights for the group in "Write".
3. Click the "Set Values" button.

Note

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 recreate it and reconfigure it with the new name.

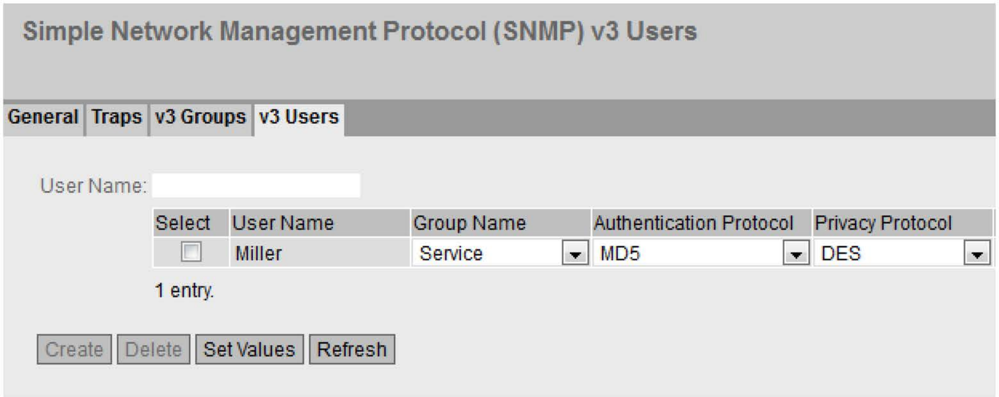
Deleting a group

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.

4.4.8.4 v3 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.

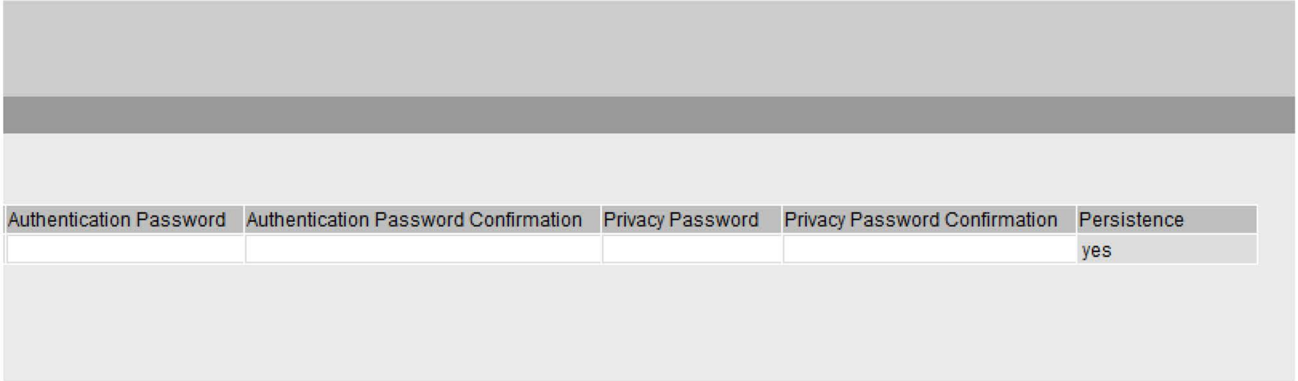


User Name:

Select	User Name	Group Name	Authentication Protocol	Privacy Protocol
□	Miller	Service	MD5	DES

1 entry.

SNMPv3 Users - first part of the table



Authentication Password	Authentication Password Confirmation	Privacy Password	Privacy Password Confirmation	Persistence
				yes

SNMPv3 Users - second part of the table

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.

- **Group Name**
  Select the group which will be assigned to the user.
- **Authentication Protocol**

  Specify the authentication protocol for which a password will be stored.

  The following settings are available:

  – None

  – MD5

  – SHA

- **Privacy Protocol**

  Specify whether or not a password should be stored for encryption with the 128-bit DES algorithm or AES algorithm. Can only be enabled when an authentication protocol has been selected.
- **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.
- **Persistence**
  Shows whether or not the user is assigned to an SNMPv3 group. If the user is not assigned to an SNMPv3 group, no automatic saving is triggered and the configured user is deleted after restarting the device.
  – Yes

    The user is assigned to an SNMPv3 group.
  – No

    The user is not assigned to an SNMPv3 group.

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. In "Group Name", select the group to which the new user will belong.

   If the group has not yet been created, change to the "v3 Groups" page and make the settings for this group.
4. If an authentication is necessary for the selected group, select the authentication algorithm in "Authentication Protocol".
   In the relevant input boxes, enter the authentication password and its confirmation.
5. If encryption was specified for the group, select the algorithm in "Privacy Protocol". In the relevant input boxes, enter the encryption password and the confirmation.
6. 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 System Time

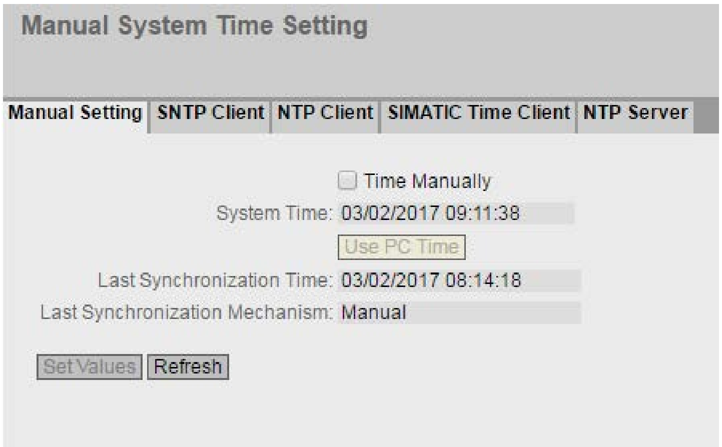
There are different methods that can be used to set the system time of the device. Only one method can be active at any one time.

If one method is activated, the previously activated method is automatically deactivated.

4.4.9.1 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".



Manual System Time Setting

□ Time Manually

System Time: 03/02/2017 09:11:38

Last Synchronization Time: 03/02/2017 08:14:18

Last Synchronization Mechanism: Manual

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".
- **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

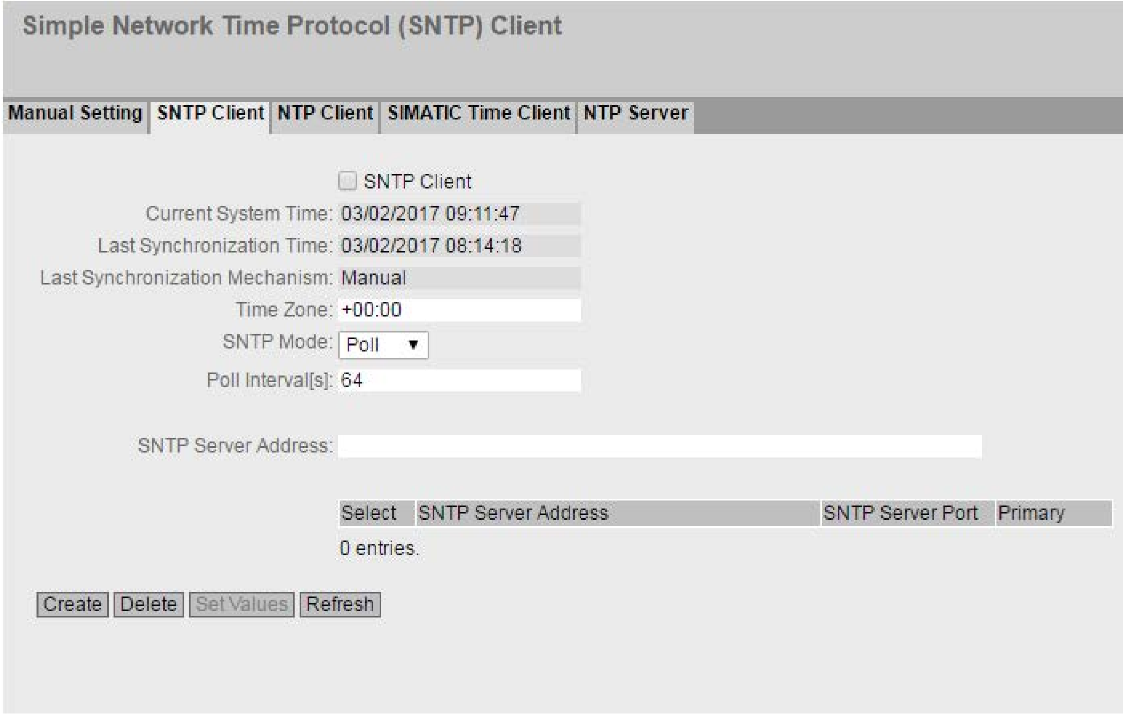
Procedure

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.

4.4.9.2 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.


Simple Network Time Protocol (SNTP) Client

□ SNTP Client

Current System Time: 03/02/2017 09:11:47

Last Synchronization Time: 03/02/2017 08:14:18

Last Synchronization Mechanism: Manual

Time Zone: +00:00

SNTP Mode: Poll

Poll Interval[s]: 64

SNTP Server Address:

Select	SNTP Server Address	SNTP Server Port	Primary

0 entries.

Requirement

To receive the SNTP frames, enable the entry "System Time" under "Security > Firewall > Pre-defined IPv4 rules".

Description

The page contains the following boxes:

- **SNTP Client**
  Enable or disable automatic time-of-day synchronization using SNTP.
- **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
- **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.
- **SNTP Mode**
  Select the synchronization mode from the drop-down list. The following types of synchronization 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.
  - Listen
    With this type of synchronization, the device is passive and receives SNTP frames that deliver the time of day. Settings in the text boxes "SNTP Server Address" and "SNTP Server Port" have no effect in this mode.

  Note

  "Listen" SNTP mode of the SNTP Client and NTP Server cannot be enabled at the same time.
- **SNTP Server Address**
  Enter the IP address or the FQDN (Fully Qualified Domain Name) of the SNTP server.
- **SNTP Server Port**
  Enter the port of the SNTP server.
  The following ports are possible:
  - 123 (standard port)
  - 1025 to 36564
- **Poll Interval[s]**
  Here, enter the interval between two-time queries. In this box, you enter the query interval in seconds. Possible values are 16 to 16284 seconds.

Procedure

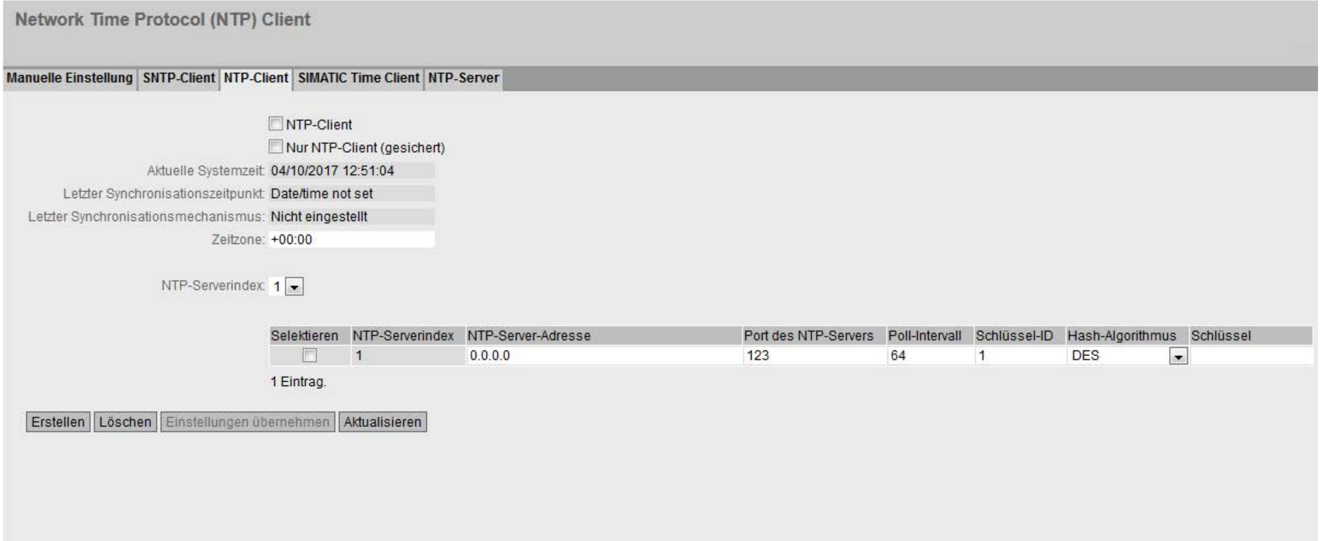
1. Click the "SNTP Client" check box to enable the automatic time setting.
2. In "Time Zone", enter the local time difference to world time (UTC).

   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)
     - 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.
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.

4.4.9.3 NTP Client

Automatic time-of-day setting with NTP

If you require time-of-day synchronization using NTP, you can make the relevant settings here.



Network Time Protocol (NTP) Client

□ NTP-Client
□ Nur NTP-Client (gesichert)

Aktuelle Systemzeit: 04/10/2017 12:51:04
Letzter Synchronisationszeitpunkt: Date/time not set
Letzter Synchronisationsmechanismus: Nicht eingestellt
Zeitzone: +00:00

NTP-Serverindex: 1

Selektieren	NTP-Serverindex	NTP-Server-Adresse	Port des NTP-Servers	Poll-Intervall	Schlüssel-ID	Hash-Algorithmus	Schlüssel
□	1	0.0.0.0	123	64	1	DES	

1 Eintrag.

Requirement

To receive the NTP frames, enable the entry "System Time" under "Security > Firewall > Pre-defined 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 enable the secure NTP client, the parameters for authentication (key ID, hash algorithm, key) must be configured.
- **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
- **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.
- **NTP Server Index**
  Select the index of the NTP server. The server with the lowest index is queried first.

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 or the FQDN (Fully Qualified Domain 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).
- **Key ID**
  Enter the ID of the authentication key.
- **Hash Algorithm**
  Specify the format for the authentication key.

- **Key**
  Enter the authentication key.
- **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 will be 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 NTP server (secure)

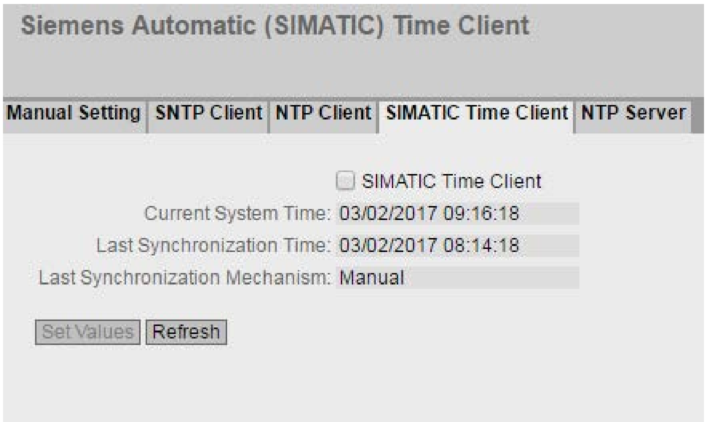
To synchronize the time of day via a secure NTP server, the following additional steps are necessary:

1. 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.
2. Click in the "Secure NTP Client only" check box to enable the automatic time setting using Secure NTP.
3. Click the "Set Values" button.

4.4.9.4 SIMATIC Time Client

Time setting via SIMATIC time client


Siemens Automatic (SIMATIC) Time Client

□ SIMATIC Time Client

Current System Time: 03/02/2017 09:16:18

Last Synchronization Time: 03/02/2017 08:14:18

Last Synchronization Mechanism: Manual

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.

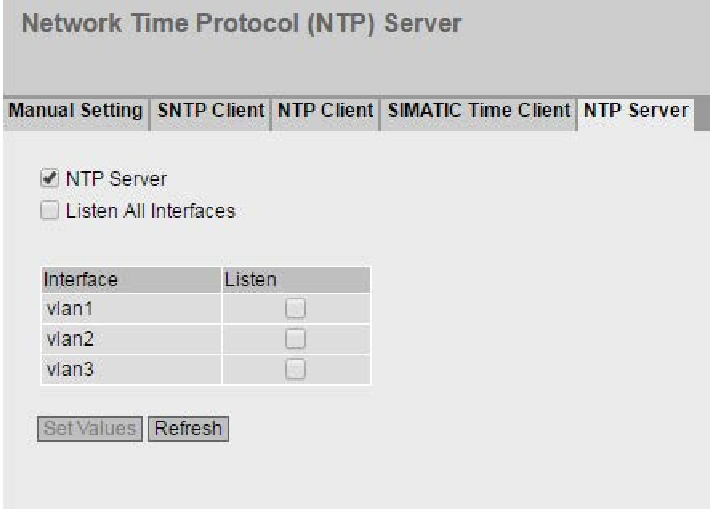
4.4.9.5 NTP Server

On this WBM page, you configure the device as an NTP server. The other devices can call up the current time 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.



☑ NTP Server

□ Listen All Interfaces

Interface	Listen
vlan1	□
vlan2	□
vlan3	□

Requirement

- To receive the NTP frames, enable the entry "System Time" under "Security > Firewall > Pre-defined IPv4 rules".

Description

The page contains the following boxes:

- **NTP Server**

  Enable or disable the NTP server service.

  Note

  "Listen" SNTP mode of the SNTP Client and NTP Server cannot be enabled at the same time.

- **Interface**

  Selection over which interface the time is to be 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.
- **Set Values**

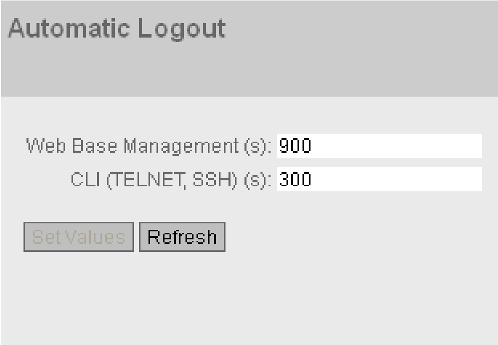
  If you click the button, the setting is adopted for all interfaces.

4.4.10 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.



Automatic Logout

Web Base Management (s): 900
CLI (TELNET, SSH) (s): 300

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.

4.4.11 Button

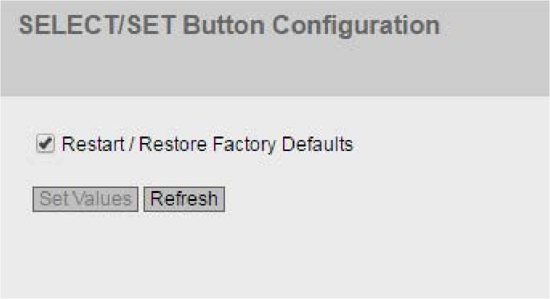
Functionality

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 device operating instructions.

On this page, the functionality of the button can be restricted.



SELECT/SET Button Configuration

☑ Restart / Restore Factory Defaults

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.

  You will find more information on how to restore the device to the factory defaults despite disabled functions in the section "Upkeep and maintenance (Page 269)".

- **Set Fault Mask**

  Enable or disable the function "Define fault mask via the LED display" with the SELECT/SET button.

Steps in configuration

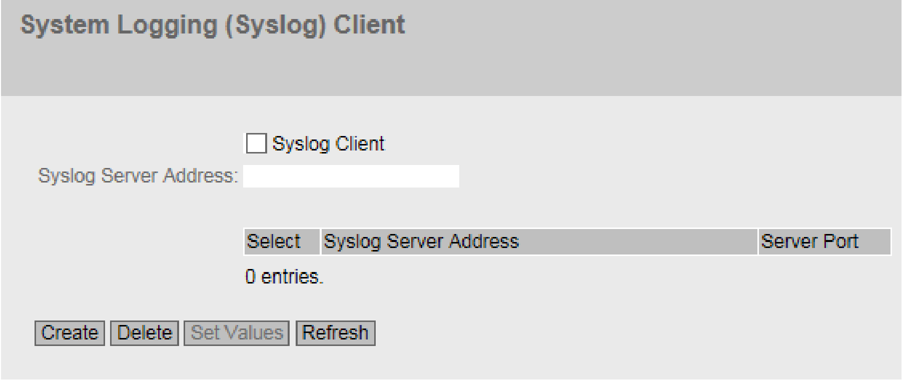
1. To use the functionality, select the corresponding check box.
2. Click the "Set Values" button.

4.4.12 Syslog client

Syslog according to RFC 3164 is used for transferring short, unencrypted text messages over UDP in the IP network. This requires a Syslog server.

Requirements for sending log entries

- The Syslog function is enabled on the device.
- The Syslog function is enabled for the relevant event.
- There is a Syslog server in your network that receives the log entries. Since this is a UDP connection, there is no acknowledgment to the sender.
- The IP address of the Syslog server is entered on the device.



Description

The page contains the following boxes:

- **Syslog Client**

  Enable or disable the Syslog function.
- **Syslog Server Address**

  Enter the IP address 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 of the Syslog server.
- **Server Port**

  Enter the port of the Syslog server being used.

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 IP address of the Syslog server on which the log entries will be saved.
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 UDP port of the server.
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.

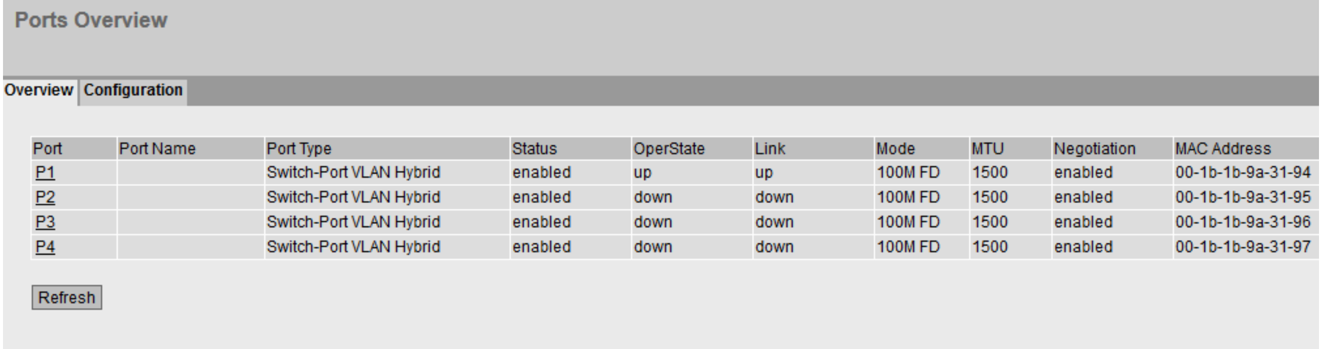
Deleting an entry

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.

4.4.13 Ports

4.4.13.1 Overview

The page shows the configuration for the data transfer for all ports of the device. You cannot configure anything on this page.



Port	Port Name	Port Type	Status	OperState	Link	Mode	MTU	Negotiation	MAC Address
P1		Switch-Port VLAN Hybrid	enabled	up	up	100M FD	1500	enabled	00-1b-1b-9a-31-94
P2		Switch-Port VLAN Hybrid	enabled	down	down	100M FD	1500	enabled	00-1b-1b-9a-31-95
P3		Switch-Port VLAN Hybrid	enabled	down	down	100M FD	1500	enabled	00-1b-1b-9a-31-96
P4		Switch-Port VLAN Hybrid	enabled	down	down	100M FD	1500	enabled	00-1b-1b-9a-31-97

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 available options are as follows:

  – 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

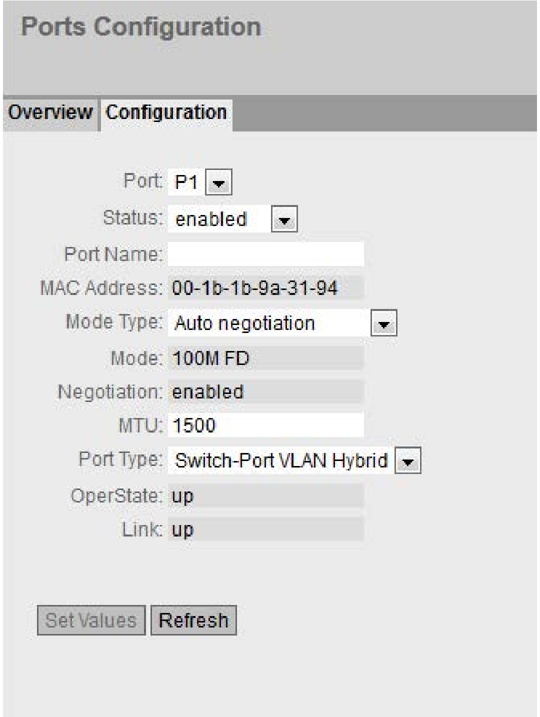
With 1 Gbps pluggable transceivers

- Actual response: Mode: 1G HD
- Expected response: Mode: 1G FD

4.4.13.2 Configuration

Configuring ports

With this page, you can configure all the ports of the device.



Port: P1
Status: enabled
Port Name:
MAC Address: 00-1b-1b-9a-31-94
Mode Type: Auto negotiation
Mode: 100M FD
Negotiation: enabled
MTU: 1500
Port Type: Switch-Port VLAN Hybrid
OperState: up
Link: up

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.

- **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 "Auto negotiation", these parameters are automatically negotiated with the connected device or network component. This must also be in the "Auto negotiation" 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 auto negotiation

  Flow control can only be enabled or disabled if the "auto negotiation" function is turned off. The function cannot 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 available options are as follows:

  – 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 available options are as follows:

  – 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" 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.

Steps in configuration

1. Change the settings according to your configuration.
2. Click the "Set Values" button.

4.4.14 Fault monitoring

4.4.14.1 Power supply

Settings for monitoring the power supply

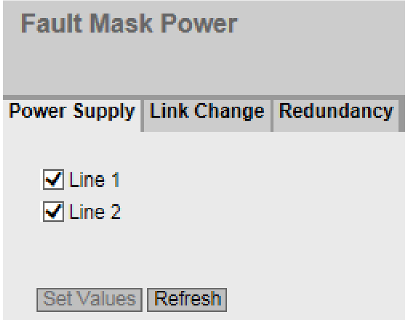
Configure whether or not the power supply should be monitored by the messaging system. With a redundant power supply, configure the monitoring separately for each individual feed-in line.

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.


Fault Mask Power

☑ Line 1
☑ Line 2

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.

4.4.14.2 Link Change

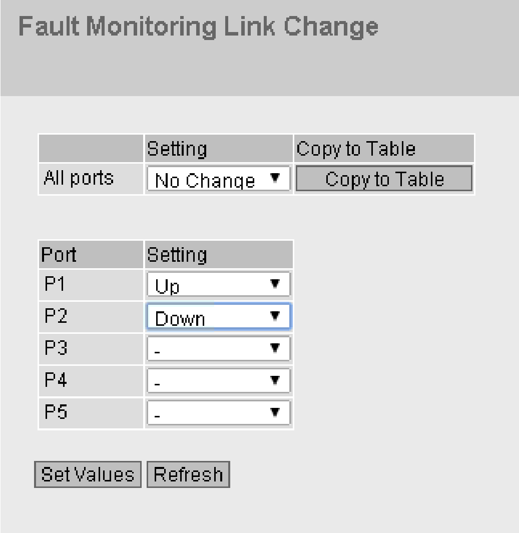
Configuration of fault monitoring of status changes on connections

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.



Fault Monitoring Link Change

	Setting	Copy to Table
All ports	No Change ▼	Copy to Table

Port	Setting
P1	Up ▼
P2	Down ▼
P3	- ▼
P4	- ▼
P5	- ▼

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.

4.4.15 PLUG

4.4.15.1 Configuration

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 or not 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.

Information about the configuration of the C-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 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.

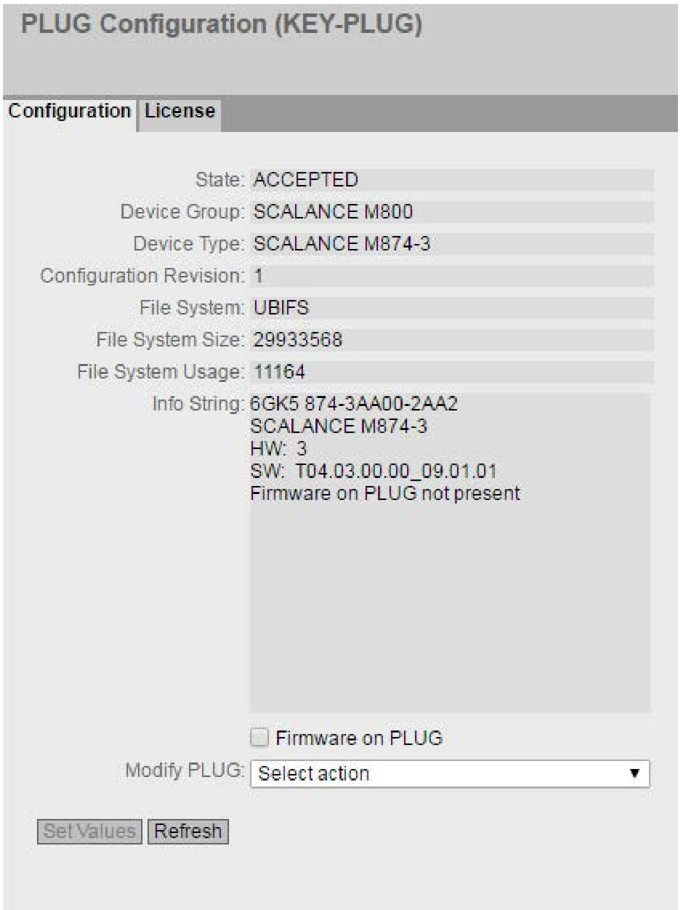
If the original configuration on the PLUG is no longer required, the PLUG can be deleted or rewritten manually via "System > PLUG".

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.


PLUG Configuration (KEY-PLUG)

State: ACCEPTED
Device Group: SCALANCE M800
Device Type: SCALANCE M874-3
Configuration Revision: 1
File System: UBIFS
File System Size: 29933568
File System Usage: 11164
Info String: 6GK5 874-3AA00-2AA2
SCALANCE M874-3
HW: 3
SW: T04.03.00.00_09.01.01
Firmware on PLUG not present

□ Firmware on PLUG

Modify PLUG: Select action ▼

Description

The table has the following rows:

- **State**
  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
    No PLUG is 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 PLUG previously.

- **Device Type**
  Shows the device type within the product line that used the 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 (e.g. modules), 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 in bytes.
- **File System Usage**
  Displays the storage space in use in the file system of the PLUG in bytes.
- **Info String**
  Shows additional information about the device that used the PLUG previously, for example, order 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.
- **Firmware on PLUG**

  When enabled, the firmware will be stored on the PLUG. This means that automatic firmware updates/downgrades can be made with the PLUG. The box "Info String" shows whether or not the firmware is stored on the PLUG.
- **Modify PLUG**
  Select the setting from the drop-down list. You have the following options for changing the configuration on the 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 with administrator rights. Here, you decide how you want to change the content of the PLUG.
2. If you want to save the firmware on the PLUG select the check box "Firmware on PLUG".
3. Select the required option from the "Modify PLUG" drop-down list.
4. Click the "Set Values" button.

4.4.15.2 License

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 or not 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.

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

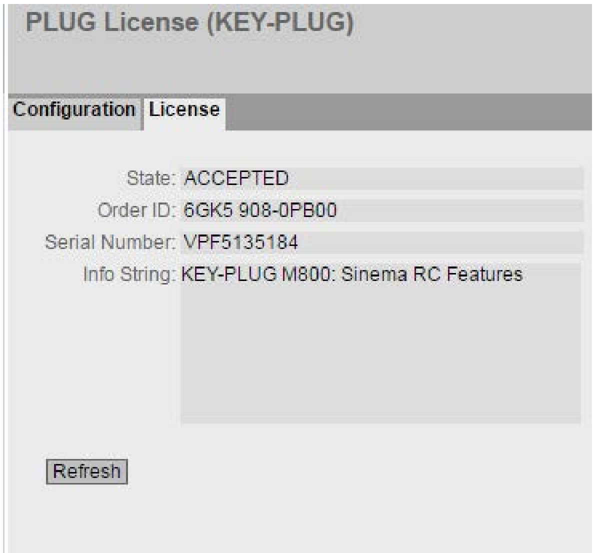
During the installation of a previous version, the configuration data can be lost. In this case, the device starts up with the factory settings after the firmware has been installed. In this situation, if a PLUG is inserted in the device, following the restart, this has the status "NOT ACCEPTED" since 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 via "System > PLUG".

Information about the license of the PLUG

A PLUG can only store the configuration of a device. In addition to the configuration, a PLUG also contains a license that enables certain functions of your SIMATIC NET device.

This page provides detailed information about the license on the PLUG.



PLUG License (KEY-PLUG)

State: ACCEPTED
Order ID: 6GK5 908-0PB00
Serial Number: VPF5135184
Info String: KEY-PLUG M800: Sinema RC Features

Description

- **State**

  Shows the status of the PLUG. The following are possible:

  – ACCEPTED
  The PLUG in the device contains a suitable and valid license.

  – NOT ACCEPTED
  The license of the inserted PLUG is not valid.

  – NOT PRESENT
  No PLUG is inserted in the device.

  – MISSING
  There is no PLUG inserted with the "FACTORY" status. Functions are configured on the device for which a license is required.

  – WRONG
  The inserted PLUG is not suitable for the device.

  – UNKNOWN
  Unknown content of the PLUG.

  – DEFECTIVE
  The content of the PLUG contains errors.

- **Order ID**

  Shows the order ID of the PLUG. The PLUG is available for various functional enhancements and for various target systems.

- **Serial Number**

  Shows the serial number of the PLUG.

- **Info String**

  Shows additional information about the device that used the PLUG previously, for example, order ID, 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.

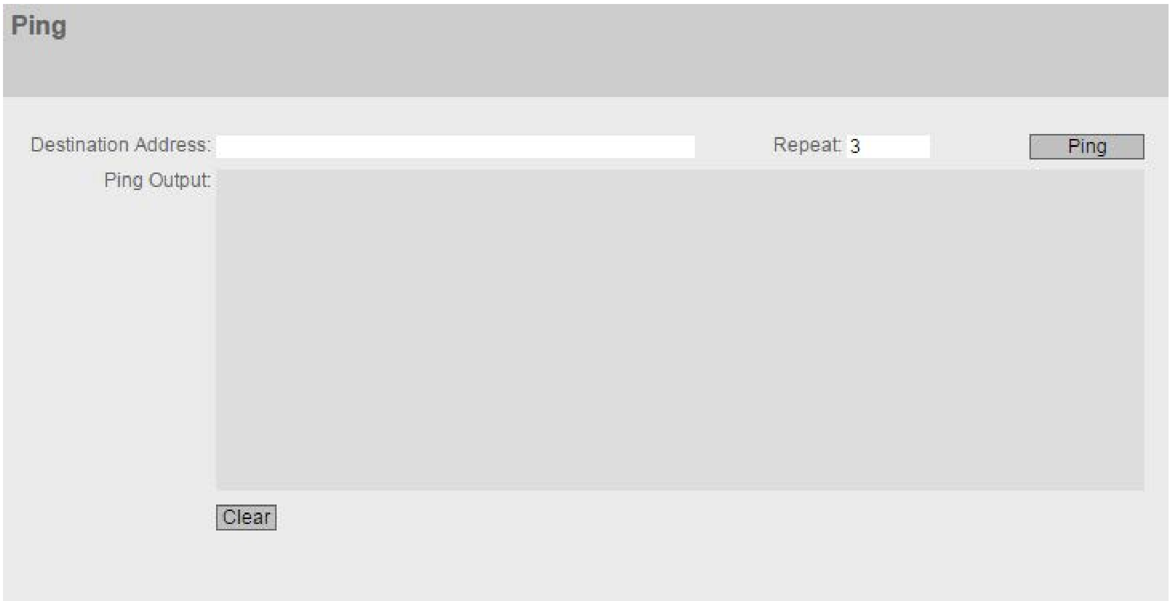
Note

When you save the configuration, the information about whether or not a PLUG was inserted in the device at the time is also saved. This configuration can then only work if a PLUG with the same order number / license is inserted.

4.4.16 Ping

Reachability of an address in an IPv4 network

With the ping function, you can check whether a certain IPv4 address is reachable in the network.



Description

The table has the following columns:

- **Destination Address**
  Enter the IPv4 address or FQDN of the device.
- **Repeat**
  Enter the number of ping requests.
- **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 empty the "Ping Output" box.

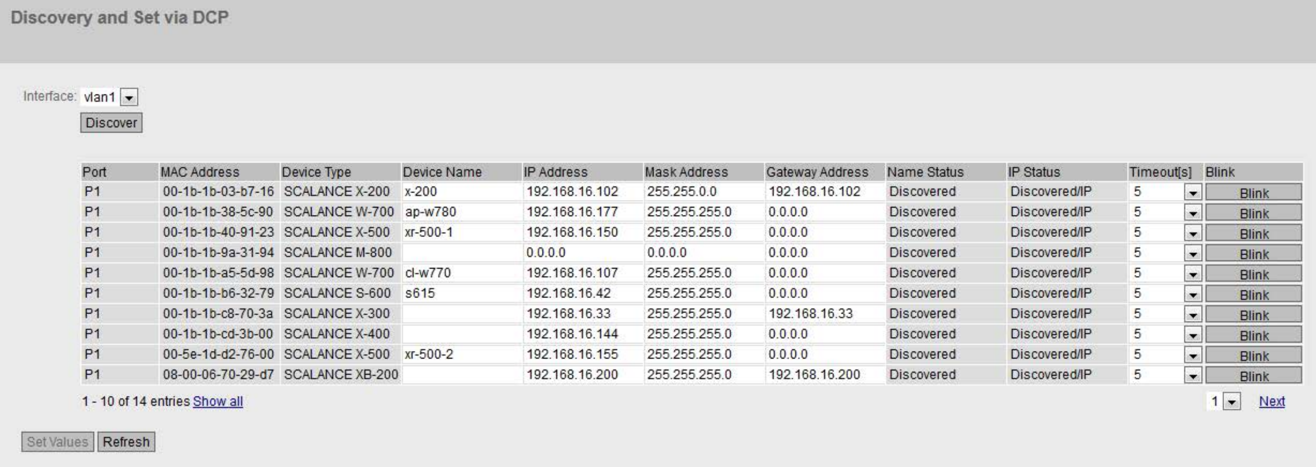
4.4.17 DCP Discovery

On this page, you can select an interface and search for devices that are reachable via the interface. The reachable devices are listed in a table. In the table you can check and adapt the network parameterrs 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".



Port	MAC Address	Device Type	Device Name	IP Address	Mask Address	Gateway Address	Name Status	IP Status	Timeout[s]	Blink
P1	00-1b-1b-03-b7-16	SCALANCE X-200	x-200	192.168.16.102	255.255.0.0	192.168.16.102	Discovered	Discovered/IP	5	Blink
P1	00-1b-1b-38-5c-90	SCALANCE W-700	ap-w780	192.168.16.177	255.255.255.0	0.0.0.0	Discovered	Discovered/IP	5	Blink
P1	00-1b-1b-40-91-23	SCALANCE X-500	xr-500-1	192.168.16.150	255.255.255.0	0.0.0.0	Discovered	Discovered/IP	5	Blink
P1	00-1b-1b-9a-31-94	SCALANCE M-800		0.0.0.0	0.0.0.0	0.0.0.0	Discovered	Discovered/IP	5	Blink
P1	00-1b-1b-a5-5d-98	SCALANCE W-700	cl-w770	192.168.16.107	255.255.255.0	0.0.0.0	Discovered	Discovered/IP	5	Blink
P1	00-1b-1b-b6-32-79	SCALANCE S-600	s615	192.168.16.42	255.255.255.0	0.0.0.0	Discovered	Discovered/IP	5	Blink
P1	00-1b-1b-c8-70-3a	SCALANCE X-300		192.168.16.33	255.255.255.0	192.168.16.33	Discovered	Discovered/IP	5	Blink
P1	00-1b-1b-cd-3b-00	SCALANCE X-400		192.168.16.144	255.255.255.0	0.0.0.0	Discovered	Discovered/IP	5	Blink
P1	00-5e-1d-d2-76-00	SCALANCE X-500	xr-500-2	192.168.16.155	255.255.255.0	0.0.0.0	Discovered	Discovered/IP	5	Blink
P1	08-00-06-70-29-d7	SCALANCE XB-200		192.168.16.200	255.255.255.0	192.168.16.200	Discovered	Discovered/IP	5	Blink

1 - 10 of 14 entries Show all

1 Next

Requirement:

To adapt network parameters, DCP requires write access to the device. If access is write-protected, the network parameters cannot be configutred.

On the SCALANCE devices you configure the access in "System > Configuration".

Description

The page contains the following boxes:

- **Interface**

  Select the required interface.

- **Browse**

  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**

  - Discoverd: The set device name is used.
  - Configured: The device was assigned a new device name.

- **Status IP Address**

  - 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 port LEDs of the selected device flash.

Configuration 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".

4.4.18 Port diagnostics

4.4.18.1 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.

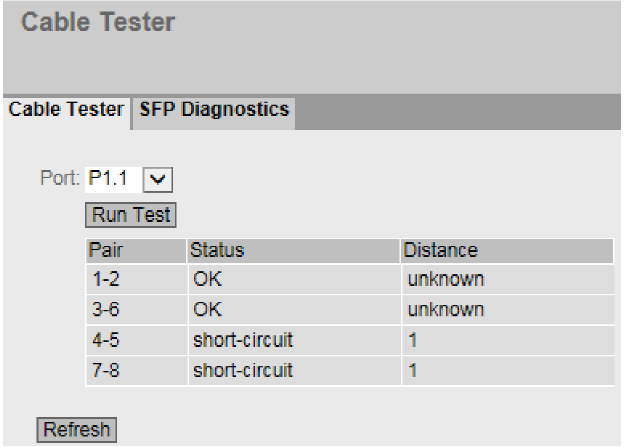
Note

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 and then needs to be done manually.

To run a cable test at the combo port, the "Combo Port Media Type" "RJ45" must be set under "System > Ports > Configuration".



Port: P1.1

Pair	Status	Distance
1-2	OK	unknown
3-6	OK	unknown
4-5	short-circuit	1
7-8	short-circuit	1

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.

This 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.

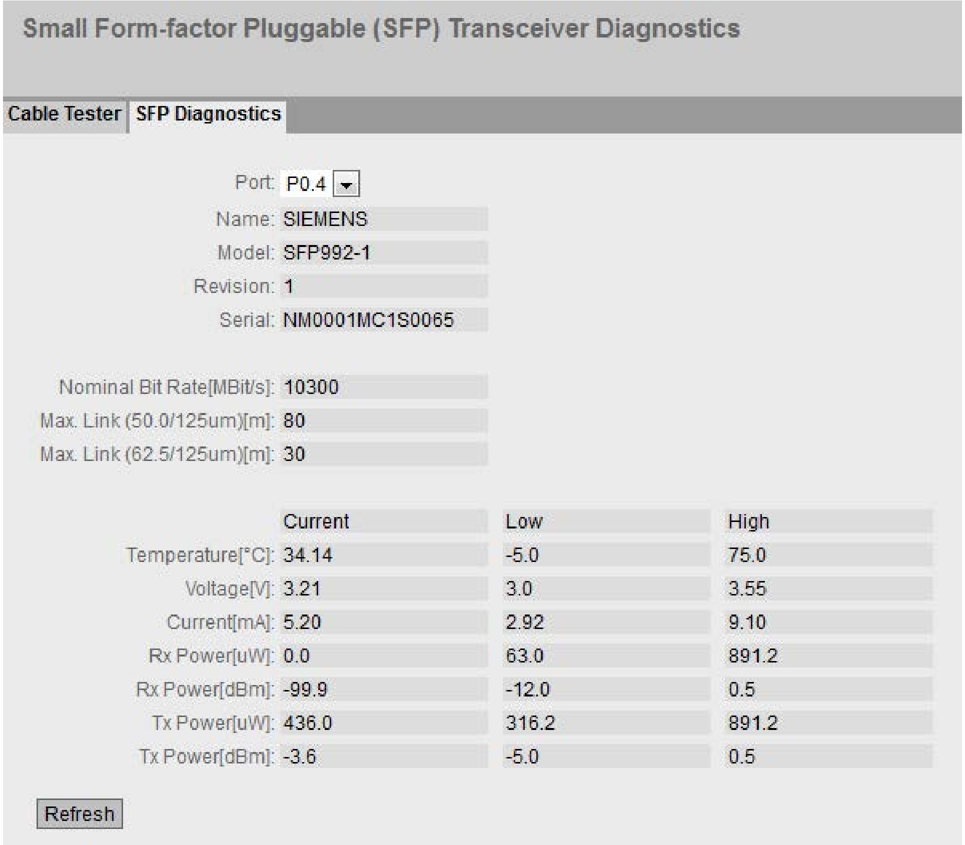
  If the status is "OK", the length is specified with "unknown".

4.4.18.2 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.



Small Form-factor Pluggable (SFP) Transceiver Diagnostics

Port:	P0.4
Name:	SIEMENS
Model:	SFP992-1
Revision:	1
Serial:	NM0001MC1S0065
Nominal Bit Rate[MBit/s]:	10300
Max. Link (50.0/125um)[m]:	80
Max. Link (62.5/125um)[m]:	30

	Current	Low	High
Temperature[°C]:	34.14	-5.0	75.0
Voltage[V]:	3.21	3.0	3.55
Current[mA]:	5.20	2.92	9.10
Rx Power[uW]:	0.0	63.0	891.2
Rx Power[dBm]:	-99.9	-12.0	0.5
Tx Power[uW]:	436.0	316.2	891.2
Tx Power[dBm]:	-3.6	-5.0	0.5

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.
- **Voltage [V]**

  Shows the voltage applied to the interface in volts [V].
- **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.

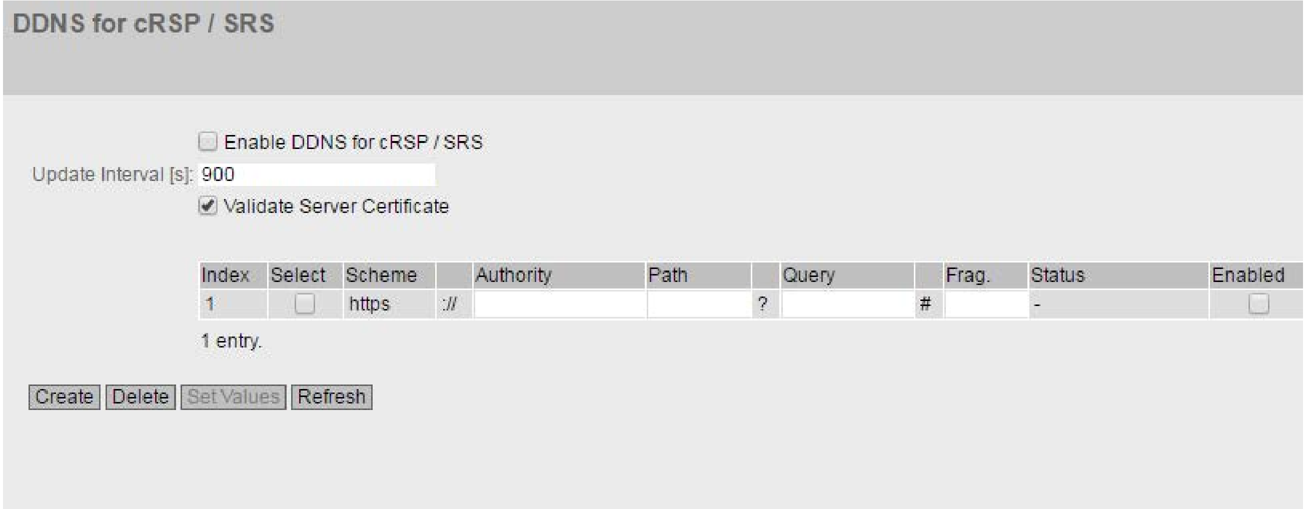
4.4.19 cRSP / SRS

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.



DDNS for cRSP / SRS

□ Enable DDNS for cRSP / SRS

Update Interval [s]: 900

☑ Validate Server Certificate

Index	Select	Scheme		Authority	Path		Query		Frag.	Status	Enabled
1	□	https	://			?		#		-	□

1 entry.

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**

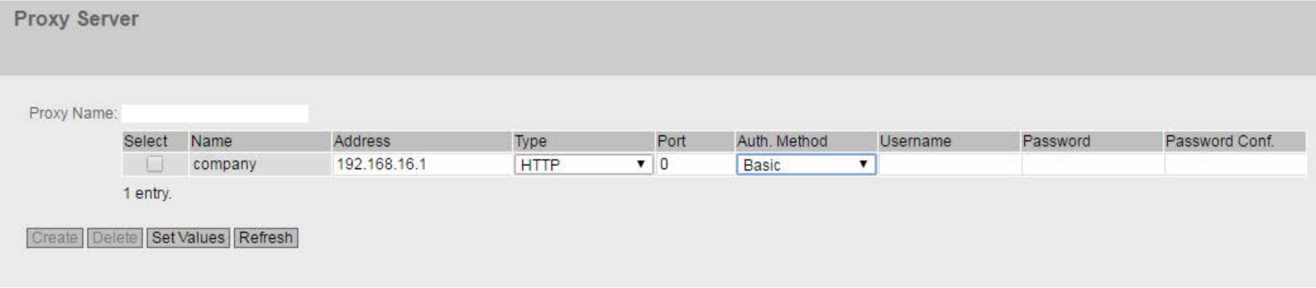
  Shows the status of the last cRSP / SRS access of the entry.

- **Enabled**

  When enabled, this entry is used.

4.4.20 Proxy Server

On this WBM page, you configure the proxy server that is used by various components, for example SINEMA RC.



Proxy Server

Proxy Name:

Select	Name	Address	Type	Port	Auth. Method	Username	Password	Password Conf.
□	company	192.168.16.1	HTTP	0	Basic			

1 entry.

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. Click "Delete" to delete the entry.

- **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
  Without 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**

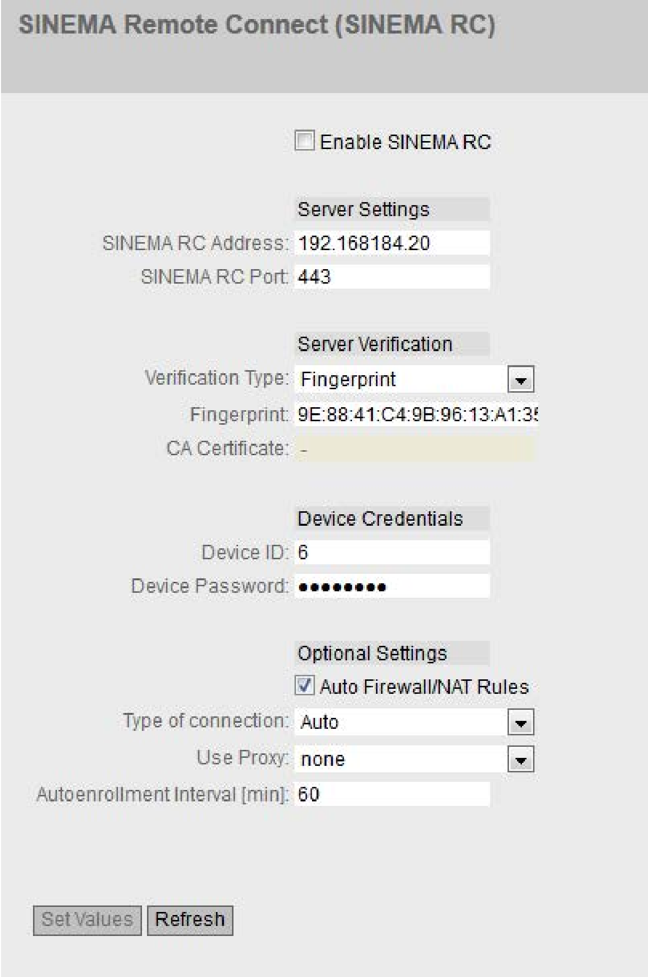
  Enter the password for access to the proxy server.

- **Password Confirmation**

  Enter the password again to confirm it.

4.4.21 SINEMA RC

On the WBM page, you configure the access to the SINEMA RC server.



SINEMA Remote Connect (SINEMA RC)

□ Enable SINEMA RC

Server Settings

SINEMA RC Address: 192.168184.20

SINEMA RC Port: 443

Server Verification

Verification Type: Fingerprint

Fingerprint: 9E:88:41:C4:9B:96:13:A1:3

CA Certificate: -

Device Credentials

Device ID: 6

Device Password: ●●●●●●●●

Optional Settings

☑ Auto Firewall/NAT Rules

Type of connection: Auto

Use Proxy: none

Autoenrollment Interval [min]: 60

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 operating instructions "SINEMA RC Server".
  - 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 Input

    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.

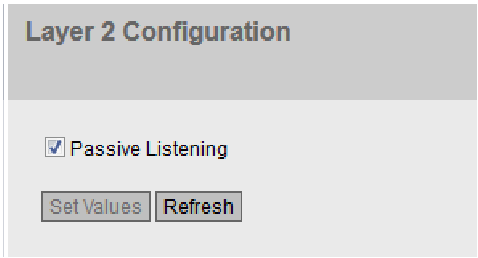
  If you enter the value 0, this function is disabled.

4.5 "Layer 2" menu

4.5.1 Configuration

Configuring layer 2

On this page, you create a basic configuration for the functions of layer 2.



Layer 2 Configuration

☑ Passive Listening

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.
- **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 "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

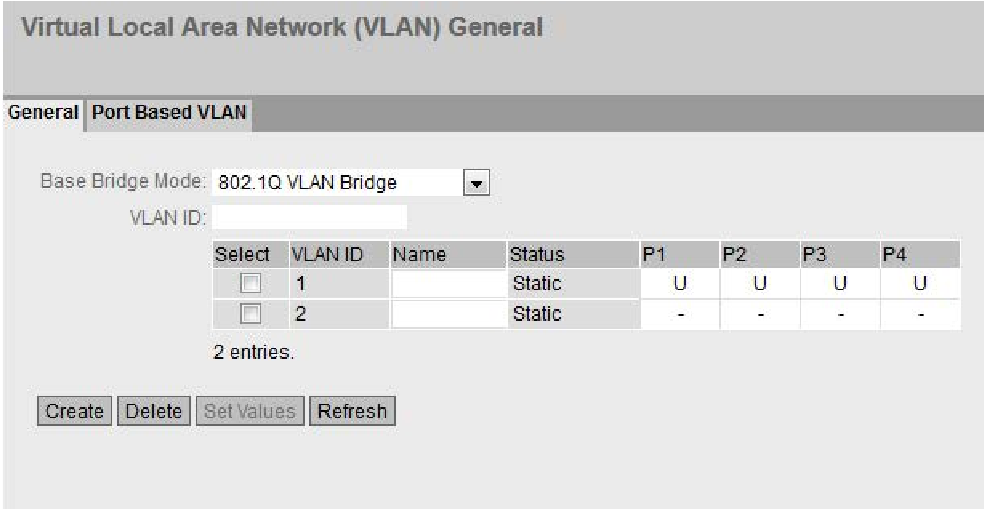
Enable or disable the Passive Listening function.

4.5.2 VLAN

4.5.2.1 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.



Virtual Local Area Network (VLAN) General

Base Bridge Mode: 802.1Q VLAN Bridge

VLAN ID:

Select	VLAN ID	Name	Status	P1	P2	P3	P4
□	1		Static	U	U	U	U
□	2		Static	-	-	-	-

2 entries.

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

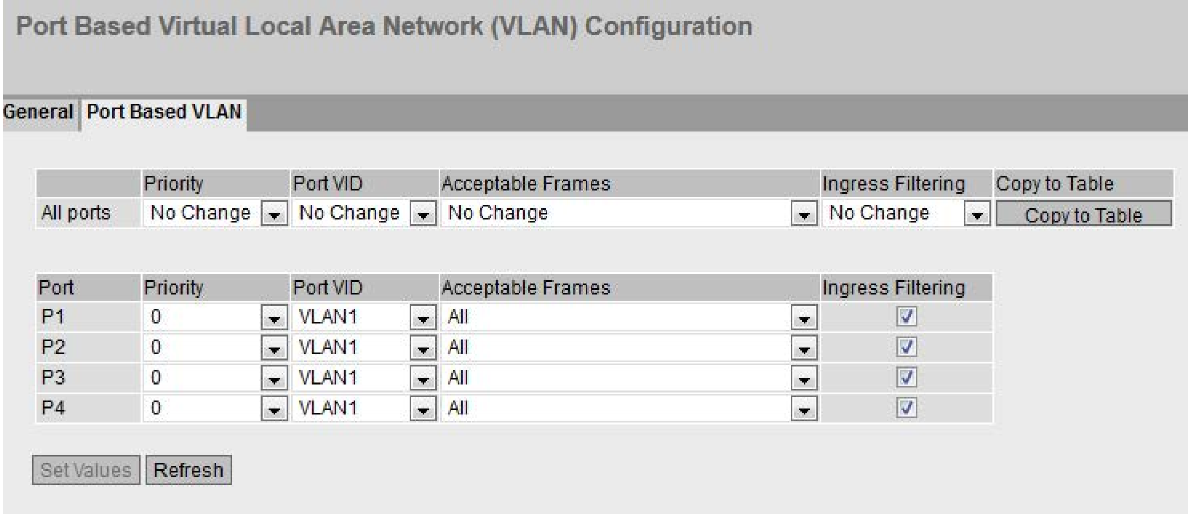
Creating a new VLAN

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.

4.5.2.2 Port Based VLAN

Processing received frames

On this WBM page, you specify the configuration of the port properties for receiving frames.



Port Based Virtual Local Area Network (VLAN) Configuration

	Priority	Port VID	Acceptable Frames	Ingress Filtering	Copy to Table
All ports	No Change	No Change	No Change	No Change	Copy to Table

Port	Priority	Port VID	Acceptable Frames	Ingress Filtering
P1	0	VLAN1	All	☑
P2	0	VLAN1	All	☑
P3	0	VLAN1	All	☑
P4	0	VLAN1	All	☑

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.

- **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.

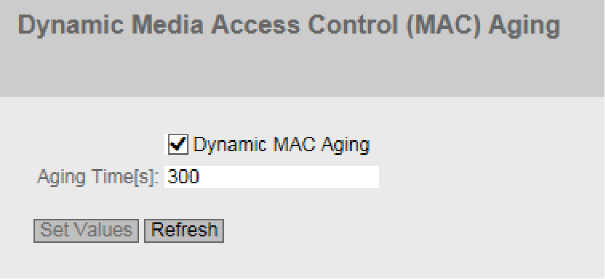
Steps in configuration

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.

4.5.3 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.



Dynamic Media Access Control (MAC) Aging

☑ Dynamic MAC Aging

Aging Time[s]: 300

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 enter 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.

4.5.4 Ring redundancy (SC6x6-2C)

4.5.4.1 Ring

Rules for ring redundancy

Factory settings

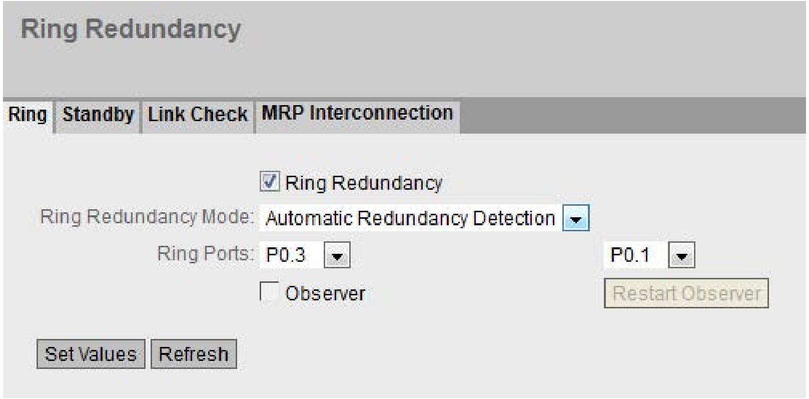
- The factory setting defines ports P0.1 and P0.2 as ring ports.

Enabling redundancy

You can enable ring redundancy as follows:

- using the WBM
- using the CLI

Configuration of ring redundancy



Ring Redundancy

☑ Ring Redundancy

Ring Redundancy Mode: Automatic Redundancy Detection

Ring Ports: P0.3 P0.1

☐ Observer

- **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

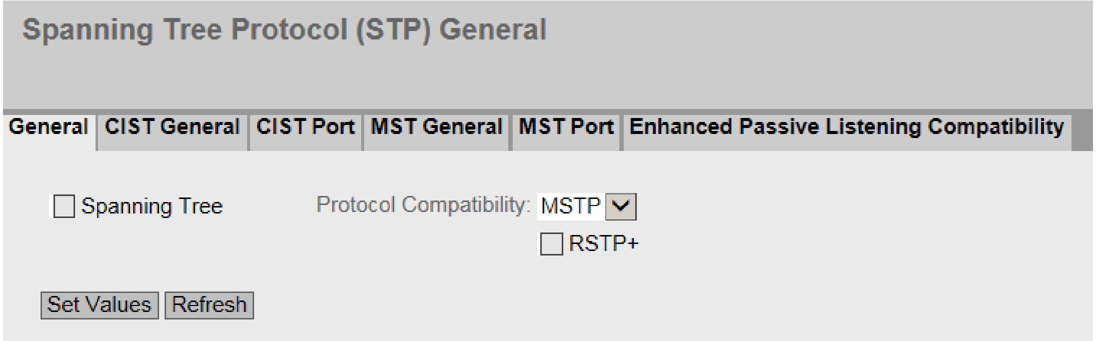
If you have restored the factory defaults, ring redundancy is disabled and the default ports are used as the ring ports. This can lead to circulating frames and failure of the data traffic if other settings were used in a previous configuration.

4.5.5 Spanning Tree

4.5.5.1 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.



Spanning Tree Protocol (STP) General

General | CIST General | CIST Port | MST General | MST Port | Enhanced Passive Listening Compatibility

□ Spanning Tree

Protocol Compatibility: MSTP

□ RSTP+

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

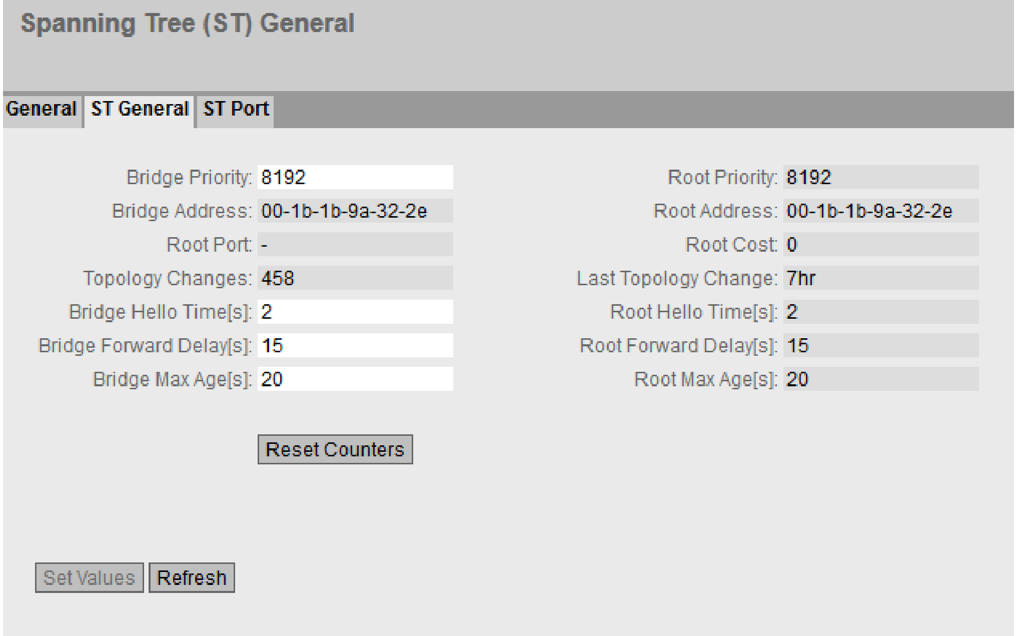
Steps in configuration

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.

4.5.5.2 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.



Spanning Tree (ST) General

Bridge Priority: 8192
Bridge Address: 00-1b-1b-9a-32-2e
Root Port: -
Topology Changes: 458
Bridge Hello Time[s]: 2
Bridge Forward Delay[s]: 15
Bridge Max Age[s]: 20

Root Priority: 8192
Root Address: 00-1b-1b-9a-32-2e
Root Cost: 0
Last Topology Change: 7hr
Root Hello Time[s]: 2
Root Forward Delay[s]: 15
Root Max Age[s]: 20

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.

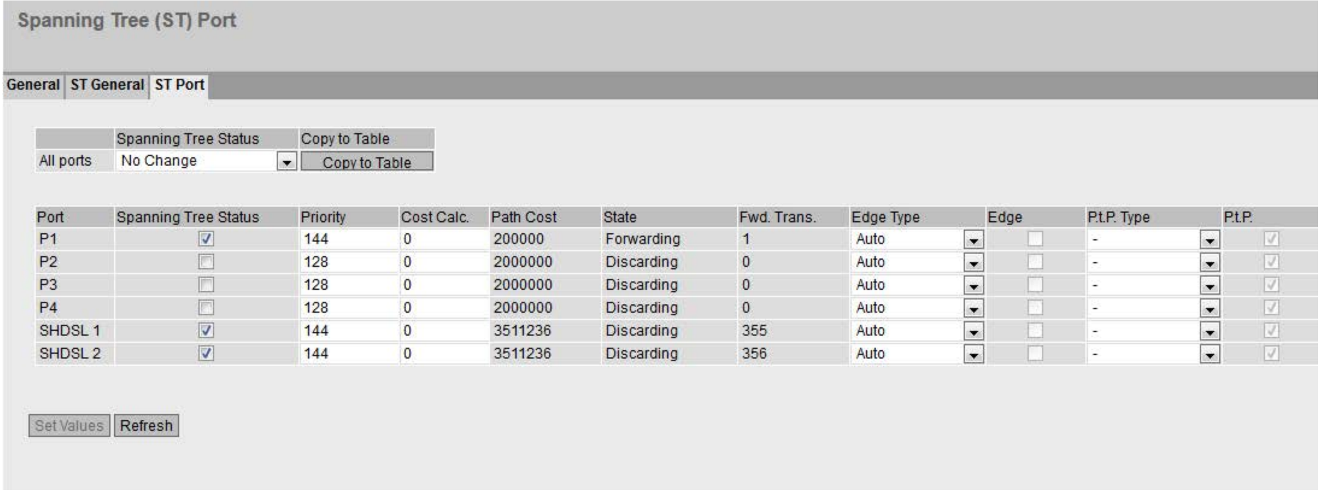
  Factory setting: 20 seconds
- **Reset Counters**

  Click this button to reset the counters on this page.

4.5.5.3 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.



	Spanning Tree Status	Copy to Table
All ports	No Change	Copy to Table

Port	Spanning Tree Status	Priority	Cost Calc.	Path Cost	State	Fwd. Trans.	Edge Type	Edge	P.t.P. Type	P.t.P.
P1	☑	144	0	200000	Forwarding	1	Auto	□	-	☑
P2	□	128	0	2000000	Discarding	0	Auto	□	-	☑
P3	□	128	0	2000000	Discarding	0	Auto	□	-	☑
P4	□	128	0	2000000	Discarding	0	Auto	□	-	☑
SHDSL 1	☑	144	0	3511236	Discarding	355	Auto	□	-	☑
SHDSL 2	☑	144	0	3511236	Discarding	356	Auto	□	-	☑

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. Otherwise, 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.

4.5.6 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.

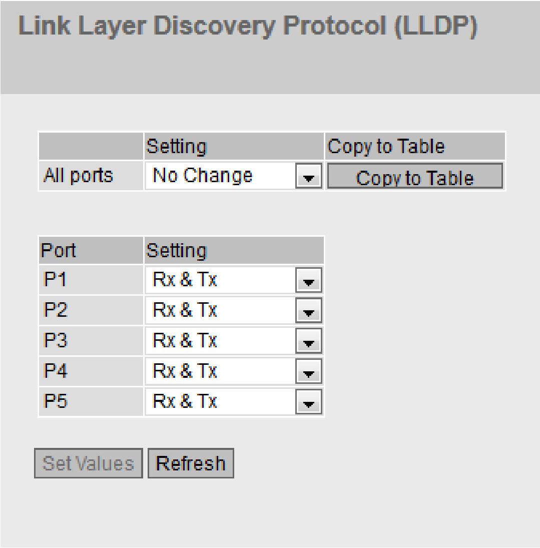
Network components that support LLDP have an LLDP agent. The LLDP agent sends information about itself and receives information from connected devices at periodic intervals. The received information is stored in the MIB.

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.



Link Layer Discovery Protocol (LLDP)

	Setting	Copy to Table
All ports	No Change	Copy to Table

Port	Setting
P1	Rx & Tx
P2	Rx & Tx
P3	Rx & Tx
P4	Rx & Tx
P5	Rx & Tx

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

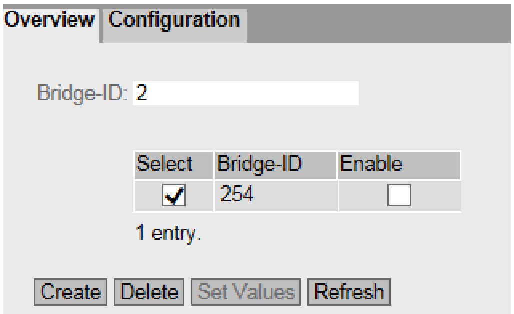
1. Select the LLDP functionality of the port from the "Setting" drop-down list.
2. Click the "Set Values" button.

4.5.7 Inter-VLAN Bridge

4.5.7.1 Overview

Overview

You can create one bridge per device and add a maximum of six VLANs to the bridge.



Bridge-ID: 2

Select	Bridge-ID	Enable
☑	254	☐

1 entry.

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.

- **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

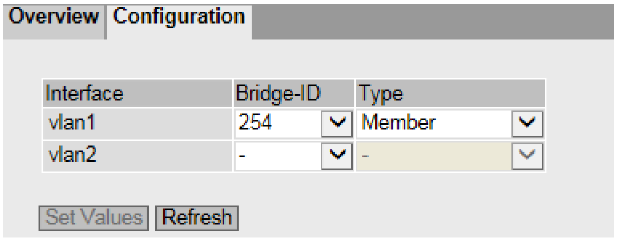
Create new Bridge-ID

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.

4.5.7.2 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.



Interface	Bridge-ID	Type
vlan1	254	Member
vlan2	-	-

Description

The page contains the following boxes:

- **Interface**

  VLAN to which the setting relates. The list of VLANs is dynamic and is based on the settings from "Layer 3 > Subnets".

- **Bridge-ID**

  Select the ID of the bridge that is to be used for the selected VLAN.

- **Type**

  Select the type of the interface.

  – Member: The IP address configuration of the VLAN is not used for the bridge.

  – Master: The IP address configuration of the VLAN 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

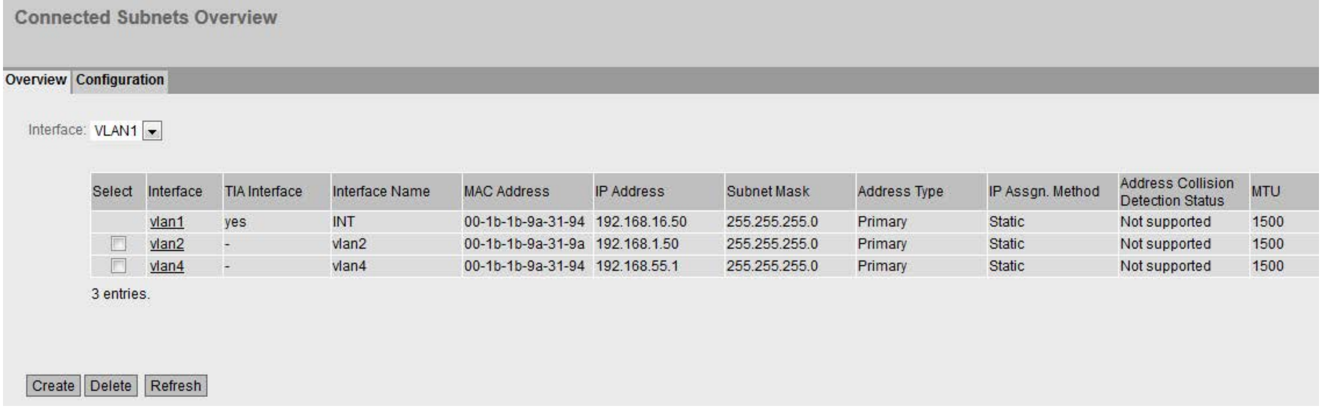
  If one of the interfaces is configured as TIA interface, you must set the type "Master" for it. Otherwise, the bridge cannot be enabled.

4.6 "Layer 3" menu

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.



Connected Subnets Overview

Interface: VLAN1

Select	Interface	TIA Interface	Interface Name	MAC Address	IP Address	Subnet Mask	Address Type	IP Assgn. Method	Address Collision Detection Status	MTU
	vlan1	yes	INT	00-1b-1b-9a-31-94	192.168.16.50	255.255.255.0	Primary	Static	Not supported	1500
□	vlan2	-	vlan2	00-1b-1b-9a-31-9a	192.168.1.50	255.255.255.0	Primary	Static	Not supported	1500
□	vlan4	-	vlan4	00-1b-1b-9a-31-94	192.168.55.1	255.255.255.0	Primary	Static	Not supported	1500

3 entries.

Description

The page contains the following box:

- **Interface**

  Select the interface on which you want to configure another subnet.

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.
- **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.
- **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 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

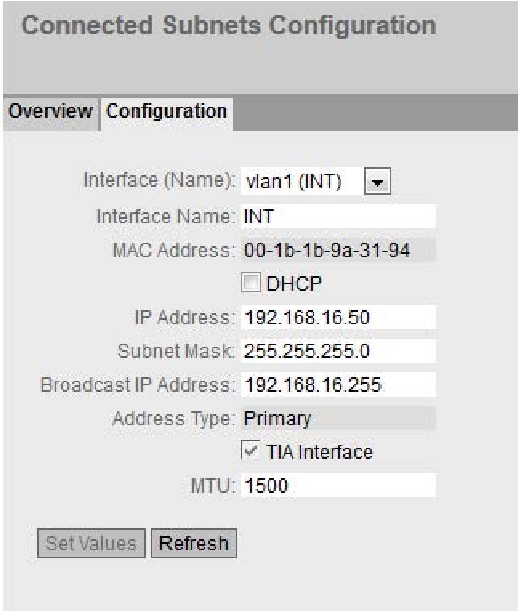
    The interface uses a unique IPv4 address. There are no collisions.
  - Not supported

    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.



Connected Subnets Configuration

Interface (Name): vlan1 (INT)
Interface Name: INT
MAC Address: 00-1b-1b-9a-31-94
□ DHCP
IP Address: 192.168.16.50
Subnet Mask: 255.255.255.0
Broadcast IP Address: 192.168.16.255
Address Type: Primary
☑ TIA Interface
MTU: 1500

Description

The page contains the following:

- **Interface (Name)**
  Select the interface from the drop-down list.
- **Interface Name**
  Enter the name of the interface.
- **MAC Address**

  Displays the MAC address of the selected interface.
- **DHCP**

  Enable or disable the DHCP client for this IPv4 interface.

  Note

  If you want to operate the device as a router with several interfaces, disable DHCP on all interfaces.

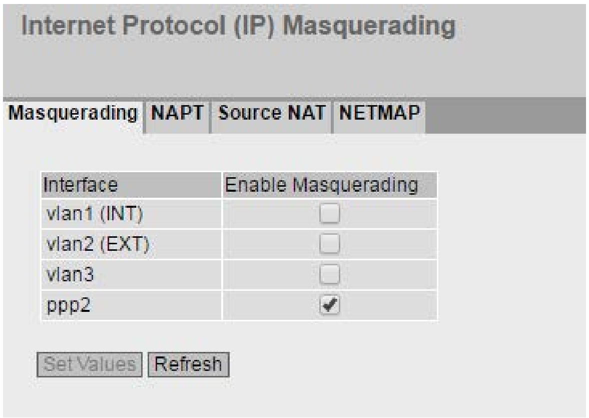
- **IP Address**
  Enter the IPv4 address of the interface. The IPv4 addresses must not be used more than once.
- **Subnet Mask**
  Enter the subnet mask of the subnet you are creating. Subnets on different interfaces must not overlap.

- **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 or not this interface should become the TIA Interface. The TIA interface defines the VLAN on which the PROFINET functionalities are available. This mainly affects the device search with or via DCP.

4.6.2 NAT

4.6.2.1 Masquerading

On this WBM page, you enable the rules for IP masquerading.



Internet Protocol (IP) Masquerading

Interface	Enable Masquerading
vlan1 (INT)	☐
vlan2 (EXT)	☐
vlan3	☐
ppp2	☑

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.

4.6.2.2 NAPT

On this WBM page, you can configure a port translation in addition to the address translation.

The following port translations are possible:

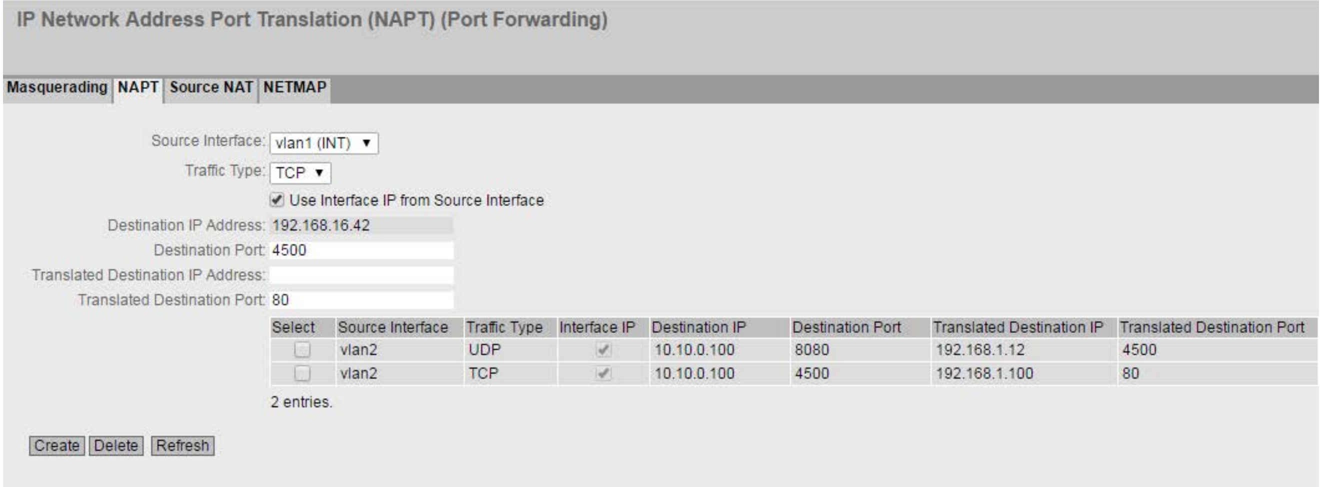
- From a single port to the same port:

  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.



IP Network Address Port Translation (NAPT) (Port Forwarding)

Source Interface:	vlan1 (INT) ▼
Traffic Type:	TCP ▼
	☑ Use Interface IP from Source Interface
Destination IP Address:	192.168.16.42
Destination Port:	4500
Translated Destination IP Address:	
Translated Destination Port:	80

Select	Source Interface	Traffic Type	Interface IP	Destination IP	Destination Port	Translated Destination IP	Translated Destination Port
□	vlan2	UDP	☑	10.10.0.100	8080	192.168.1.12	4500
□	vlan2	TCP	☑	10.10.0.100	4500	192.168.1.100	80

2 entries.

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**

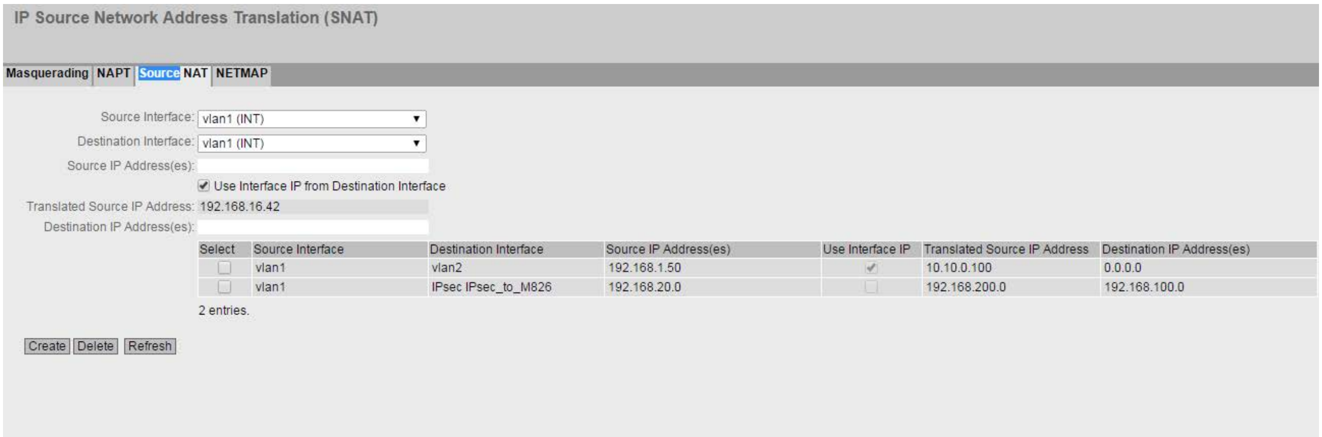
  Shows the IP address of the node to which the packets will be forwarded.

- **Translated Destination Port**

  Shows the destination port to which the packets are translated.

4.6.2.3 Source NAT

On this WBM page, you configure the rules for source NAT.



IP Source Network Address Translation (SNAT)

Source Interface: vlan1 (INT)

Destination Interface: vlan1 (INT)

Source IP Address(es):

☑ Use Interface IP from Destination Interface

Translated Source IP Address: 192.168.16.42

Destination IP Address(es):

Select	Source Interface	Destination Interface	Source IP Address(es)	Use Interface IP	Translated Source IP Address	Destination IP Address(es)
□	vlan1	vlan2	192.168.1.50	☑	10.10.0.100	0.0.0.0
□	vlan1	IPsec IPsec_to_M826	192.168.20.0	□	192.168.200.0	192.168.100.0

2 entries.

Note

Firewall rule with source NAT

Address translation with source NAT was 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

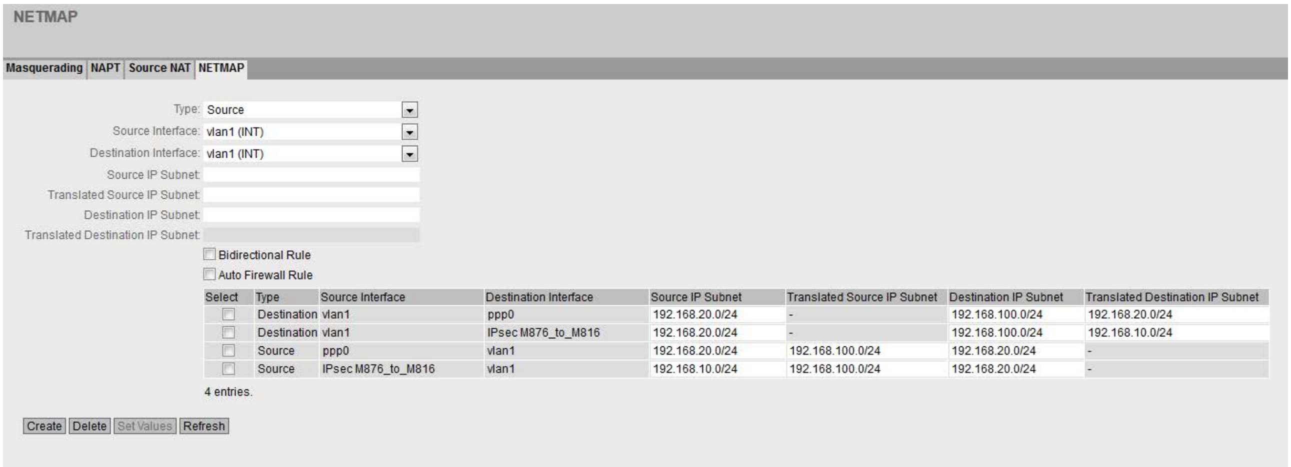
  Shows the source interface.
- Destination Interface

  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 recipients for which address translation is required.

4.6.2.4 NETMAP

On this WBM page, you specify the rules for NETMAP. NETMAP is static 1:1 mapping of network addresses in which the host part is retained.



NETMAP

Type:	Source
Source Interface:	vlan1 (INT)
Destination Interface:	vlan1 (INT)
Source IP Subnet:	
Translated Source IP Subnet:	
Destination IP Subnet:	
Translated Destination IP Subnet:	

□ Bidirectional Rule

□ Auto Firewall Rule

Select	Type	Source Interface	Destination Interface	Source IP Subnet	Translated Source IP Subnet	Destination IP Subnet	Translated Destination IP Subnet
□	Destination	vlan1	ppp0	192.168.20.0/24	-	192.168.100.0/24	192.168.20.0/24
□	Destination	vlan1	IPsec M876_to_M816	192.168.20.0/24	-	192.168.100.0/24	192.168.10.0/24
□	Source	ppp0	vlan1	192.168.20.0/24	192.168.100.0/24	192.168.20.0/24	-
□	Source	IPsec M876_to_M816	vlan1	192.168.10.0/24	192.168.100.0/24	192.168.20.0/24	-

4 entries.

Note

Firewall rule with source NAT

Address translation with source NAT was 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.

- **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.

- **Destination IP Subnet**

  Enter the subnet of the recipient.
  The subnet can also be a single PC or another subset of the subnet. Use the CIDR notation.

- **Translated Destination IP Subnet**

  Enter the subnet with which the subnet of the recipient will be replaced. Can only be edited in the "Destination" settings.
  The subnet can also be a single PC or another subset of the subnet. Use the CIDR notation.

- **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 recipient.

- Translated Destination IP Subnet

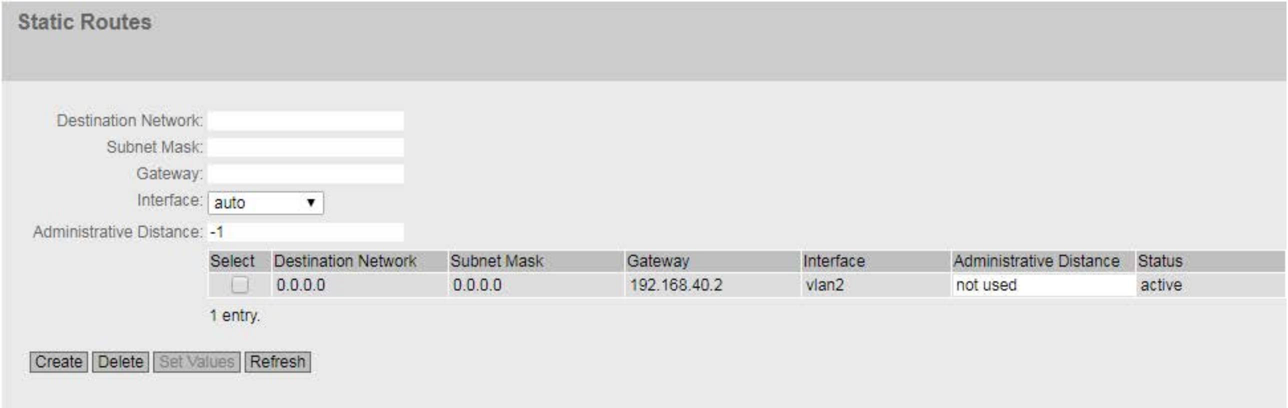
  Shows the subnet of the recipient with which the subnet of the recipient is replaced.

See also

NAT and firewall (Page 53)

4.6.3 Static routes

On this page, you specify the routes via which data exchange can take place between the various subnets. Dynamic routing protocols are not supported, for example RIP, OSPF.



Destination Network:
Subnet Mask:
Gateway:
Interface: auto ▼
Administrative Distance: -1

Select	Destination Network	Subnet Mask	Gateway	Interface	Administrative Distance	Status
□	0.0.0.0	0.0.0.0	192.168.40.2	vlan2	not used	active

1 entry.

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.
- **Interface**
  Specify whether the network address can be reached via a certain interface or via the gateway (auto).
- **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, for example speed, costs. If there are several equal routes, the route with the lowest metric value is used.

  If you do not enter anything, "not used" is entered automatically. The metric can be changed later.

  Range of values: 1 - 255 or -1 for "not used".

  Here, 1 is the value for the best possible route. The higher value, the longer packets require to their destination.

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. 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

  Here, 1 is the value for the best possible route. The higher value, the longer the packets require to their destination.
- **Status**
  Shows whether or not the route is active.

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. For "Interface", select the entry "auto".
4. Enter the gateway in the "Gateway" input box.
5. Enter the weighting of the route in "Administrative Distance".
6. Click the "Create" button. A new entry is generated in the table.
7. Click the "Set Values" button.

4.6.4 VRRPv3

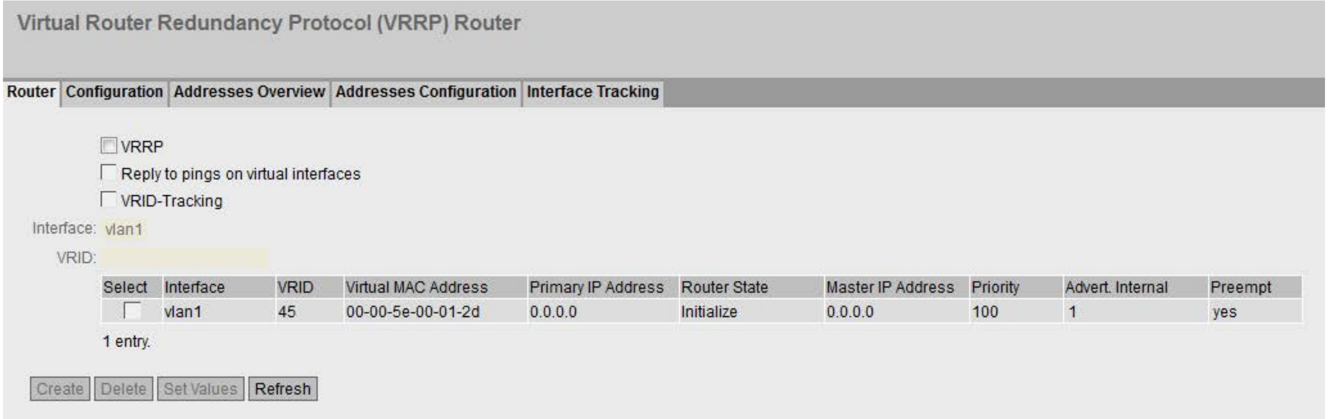
4.6.4.1 Router

Introduction

Using the "Create" button, you can create new virtual routers. A maximum of 6 virtual routers can be configured. You can configure other parameters on the "Configuration" tab.

Note

- You can use VRRPv3 on VLAN interfaces.



□ VRRP
□ Reply to pings on virtual interfaces
□ VRID-Tracking
Interface: vlan1
VRID:

Select	Interface	VRID	Virtual MAC Address	Primary IP Address	Router State	Master IP Address	Priority	Advert. Internal	Preempt
□	vlan1	45	00-00-5e-00-01-2d	0.0.0.0	Initialize	0.0.0.0	100	1	yes

1 entry.

Requirement

For the incoming VRRP packets to be forwarded to the device, you must configure the following firewall rule:

Security > Firewall > IP protocol:

- Protocol Name: "VRRP"
- Protocol Number: 112

Security > Firewall > IP rules:

- Protocol: IPv4
- Action: Accept
- From: <Interface>
- To: Device
- Source (Range): 0.0.0.0/0
- Destination (Range): 224.0.0.18/32
- Services: 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 a 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

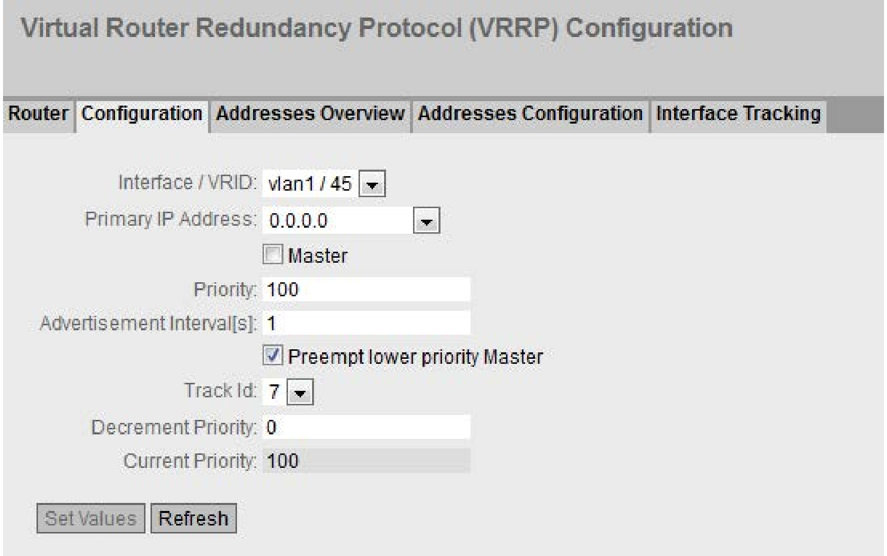
1. Select the "VRRPv3" check box.
2. Select the required interface.
3. Enter the ID of the virtual router in the "VRID" input box.
4. Click the "Create" button. A new row is inserted in the table.
5. Select the "Reply to pings on virtual interfaces" check box so that virtual addresses reply to pings 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.

4.6.4.2 Configuration

Introduction

On this page, you configure the virtual router.



Virtual Router Redundancy Protocol (VRRP) Configuration

Interface / VRID: vlan1 / 45

Primary IP Address: 0.0.0.0

□ Master

Priority: 100

Advertisement Interval[s]: 1

☑ Preempt lower priority Master

Track Id: 7

Decrement Priority: 0

Current Priority: 100

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.

- **Master**
  If this option is enabled, the numerically lowest IPv4 address is entered for "Associated IP Address". This means that the highest priority IPv4 address of the VRRP router is used

as the virtual IPv4 address of the virtual master router. The option must be disabled for the backup routers in this group and the IP address of the router in "Associated IP address" must 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

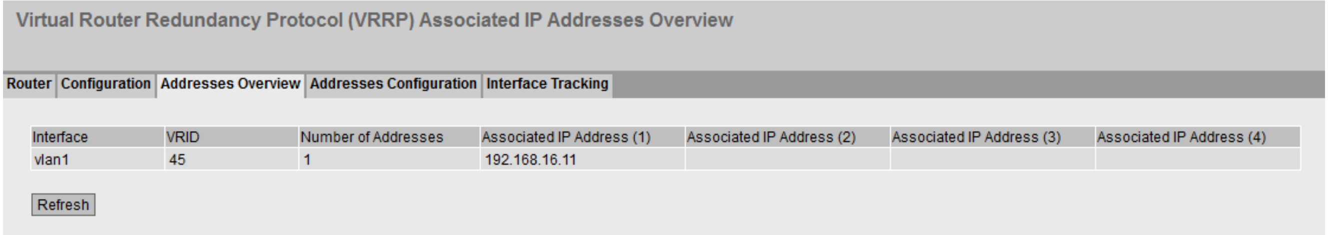
To configure a virtual router as the master router, follow the steps below:

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.

4.6.4.3 Addresses Overview

Overview

This page shows which IPv4 addresses are monitored by the virtual router. Each virtual router can monitor one IPv4 address.



Virtual Router Redundancy Protocol (VRRP) Associated IP Addresses Overview

Interface	VRID	Number of Addresses	Associated IP Address (1)	Associated IP Address (2)	Associated IP Address (3)	Associated IP Address (4)
vlan1	45	1	192.168.16.11			

Description of the displayed boxes:

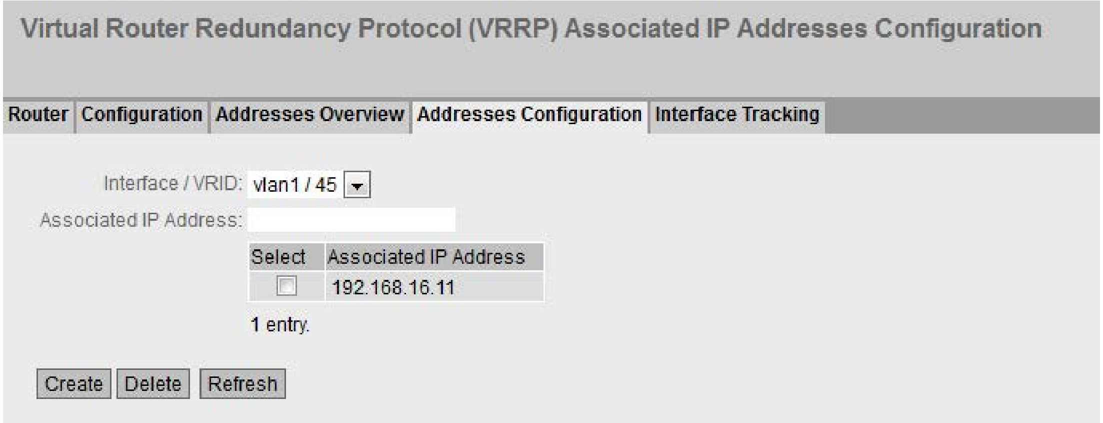
The table has the following columns:

- **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.

4.6.4.4 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.



Interface / VRID: vlan1 / 45

Associated IP Address:

Select	Associated IP Address
□	192.168.16.11

1 entry.

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.

Steps in configuration

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.

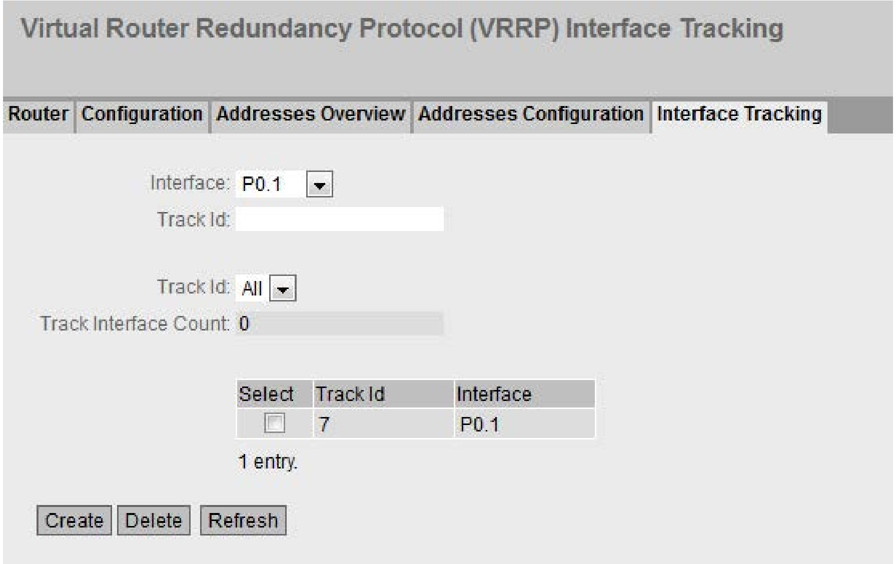
4.6.4.5 Interface Tracking

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.



Virtual Router Redundancy Protocol (VRRP) Interface Tracking

Interface: P0.1
Track Id:

Track Id: All
Track Interface Count: 0

Select	Track Id	Interface
□	7	P0.1

1 entry.

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.

4.7 "Security" menu

4.7.1 Users

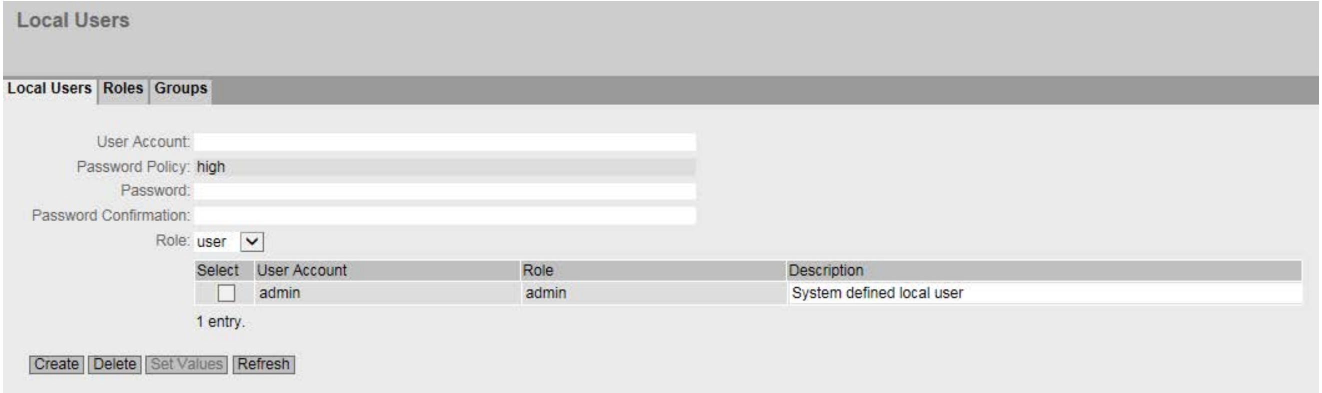
4.7.1.1 Local Users

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.



User Account:
Password Policy: high
Password:
Password Confirmation:
Role: user

Select	User Account	Role	Description
□	admin	admin	System defined local user

1 entry.

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**

  Enter the password. The strength of the password depends on the set password policy.

- **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 is logged in with the rights of the associated role.

  - Additional

    Remote access and rights assigned to the user.

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.

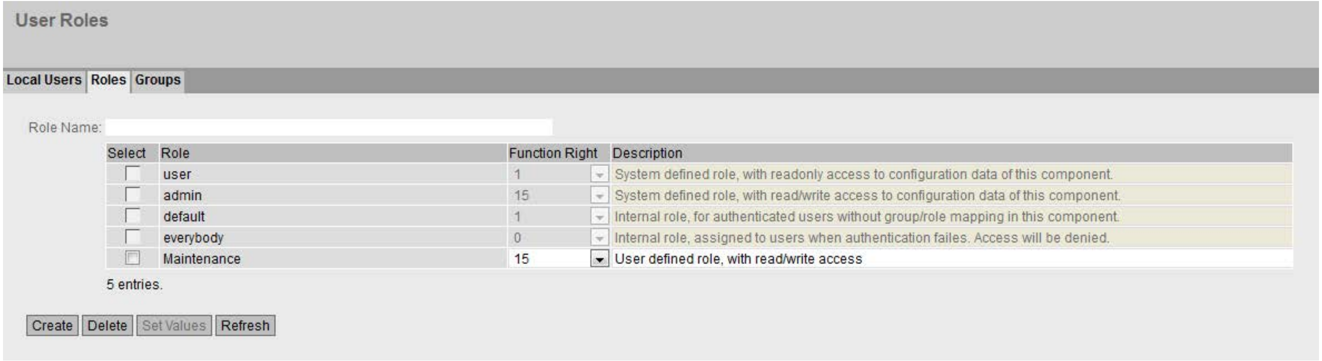
4.7.1.2 Roles

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.



Role Name:

Select	Role	Function Right	Description
□	user	1	System defined role, with readonly access to configuration data of this component.
□	admin	15	System defined role, with read/write access to configuration data of this component.
□	default	1	Internal role, for authenticated users without group/role mapping in this component.
□	everybody	0	Internal role, assigned to users when authentication failes. Access will be denied.
□	Maintenance	15	User defined role, with read/write access

5 entries.

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.

This 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.

4.7.1.3 Groups

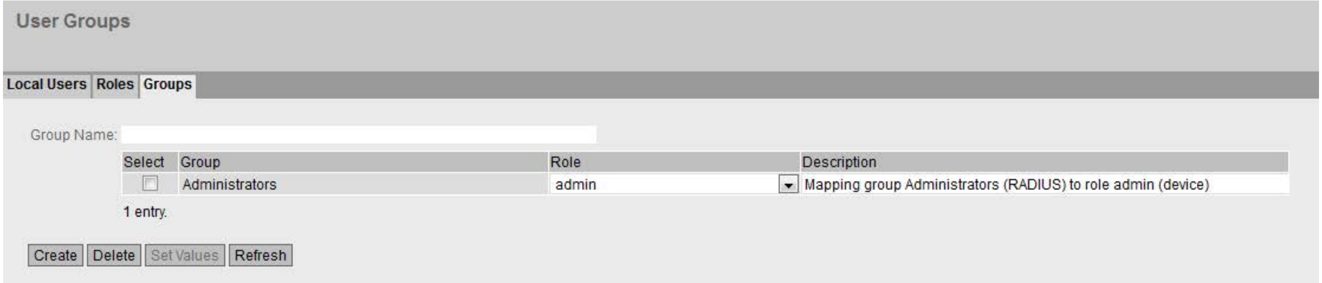
User groups

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.



User Groups

Group Name:

Select	Group	Role	Description
□	Administrators	admin	Mapping group Administrators (RADIUS) to role admin (device)

1 entry.

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.

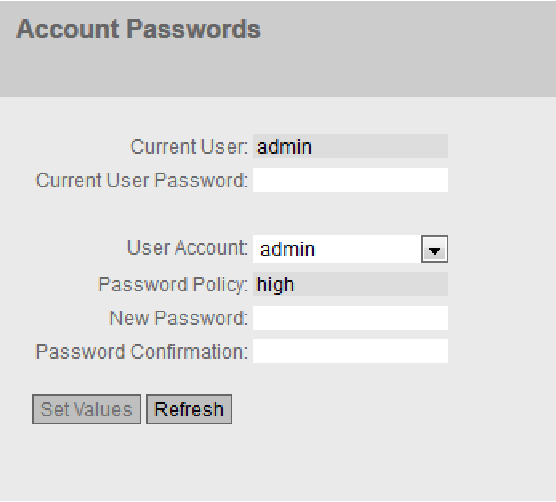
1. Enter the name of a group.
2. Click the "Create" button.
3. Select a role.
4. Enter a description for the link of a group.to a role.
5. Click the "Set Values" button.

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.

4.7.2 Passwords

Configuration of the passwords



Account Passwords

Current User: admin
Current User Password:
User Account: admin
Password Policy: high
New Password:
Password Confirmation:

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
  - Low

    Password length: at least 6 characters, maximum 128 characters
- **New Password**

  Enter the new password for the selected user.

  The following character must not be included: §

  Note

  When you log in for the first time or following a "Restore Factory Defaults and Restart", with the preset user "admin" you will be prompted to change the password.

  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.

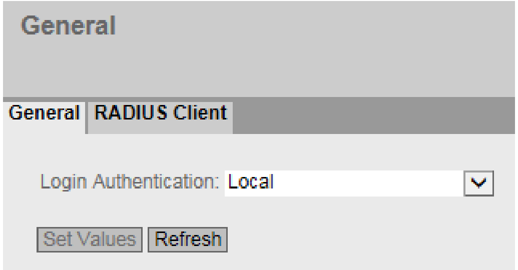
4.7.3 AAA

4.7.3.1 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.



Login Authentication: Local

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.

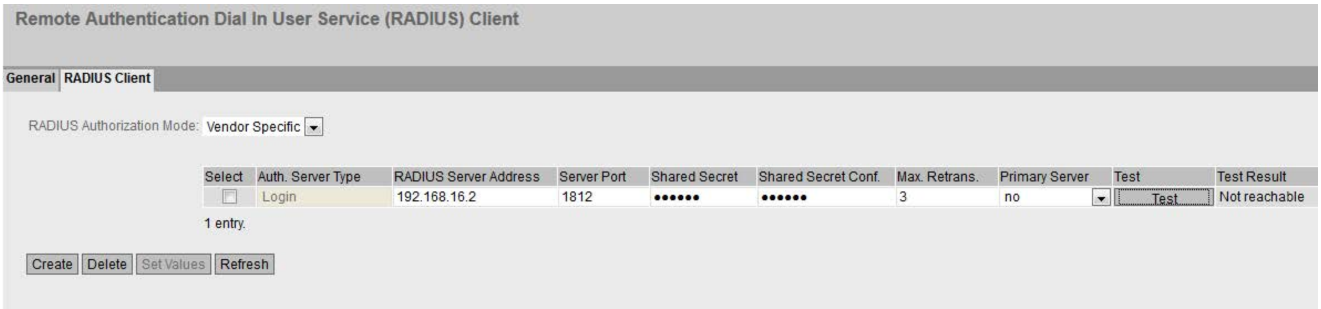
4.7.3.2 RADIUS client

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.



Remote Authentication Dial In User Service (RADIUS) Client

RADIUS Authorization Mode: Vendor Specific

Select	Auth. Server Type	RADIUS Server Address	Server Port	Shared Secret	Shared Secret Conf.	Max. Retrans.	Primary Server	Test	Test Result
□	Login	192.168.16.2	1812	••••••	••••••	3	no	Test	Not reachable

1 entry.

Description of the displayed boxes

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 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 IPv4 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

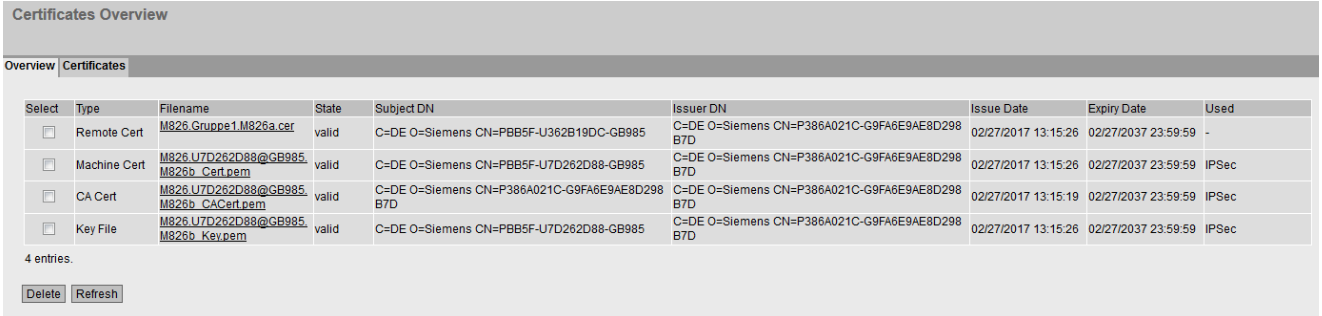
1. Click the check box in the first column before the row you want to delete to select the entry for deletion.
   Repeat this for all entries you want to delete.
2. Click the "Delete" button. The data is deleted from the memory of the device and the page is updated.

4.7.4 Certificates

4.7.4.1 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



Select	Type	Filename	State	Subject DN	Issuer DN	Issue Date	Expiry Date	Used
□	Remote Cert	M826.Gruppe1.M826a.cer	valid	C=DE O=Siemens CN=PBB5F-U362B19DC-GB985	C=DE O=Siemens CN=P386A021C-G9FA6E9AE8D298 B7D	02/27/2017 13:15:26	02/27/2037 23:59:59	-
□	Machine Cert	M826.U7D262D88@GB985.M826b_Cert.pem	valid	C=DE O=Siemens CN=PBB5F-U7D262D88-GB985	C=DE O=Siemens CN=P386A021C-G9FA6E9AE8D298 B7D	02/27/2017 13:15:26	02/27/2037 23:59:59	IPSec
□	CA Cert	M826.U7D262D88@GB985.M826b_CACert.pem	valid	C=DE O=Siemens CN=P386A021C-G9FA6E9AE8D298 B7D	C=DE O=Siemens CN=P386A021C-G9FA6E9AE8D298 B7D	02/27/2017 13:15:19	02/27/2037 23:59:59	IPSec
□	Key File	M826.U7D262D88@GB985.M826b_Key.pem	valid	C=DE O=Siemens CN=PBB5F-U7D262D88-GB985	C=DE O=Siemens CN=P386A021C-G9FA6E9AE8D298 B7D	02/27/2017 13:15:26	02/27/2037 23:59:59	IPSec

4 entries.

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.
- **State**

  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**

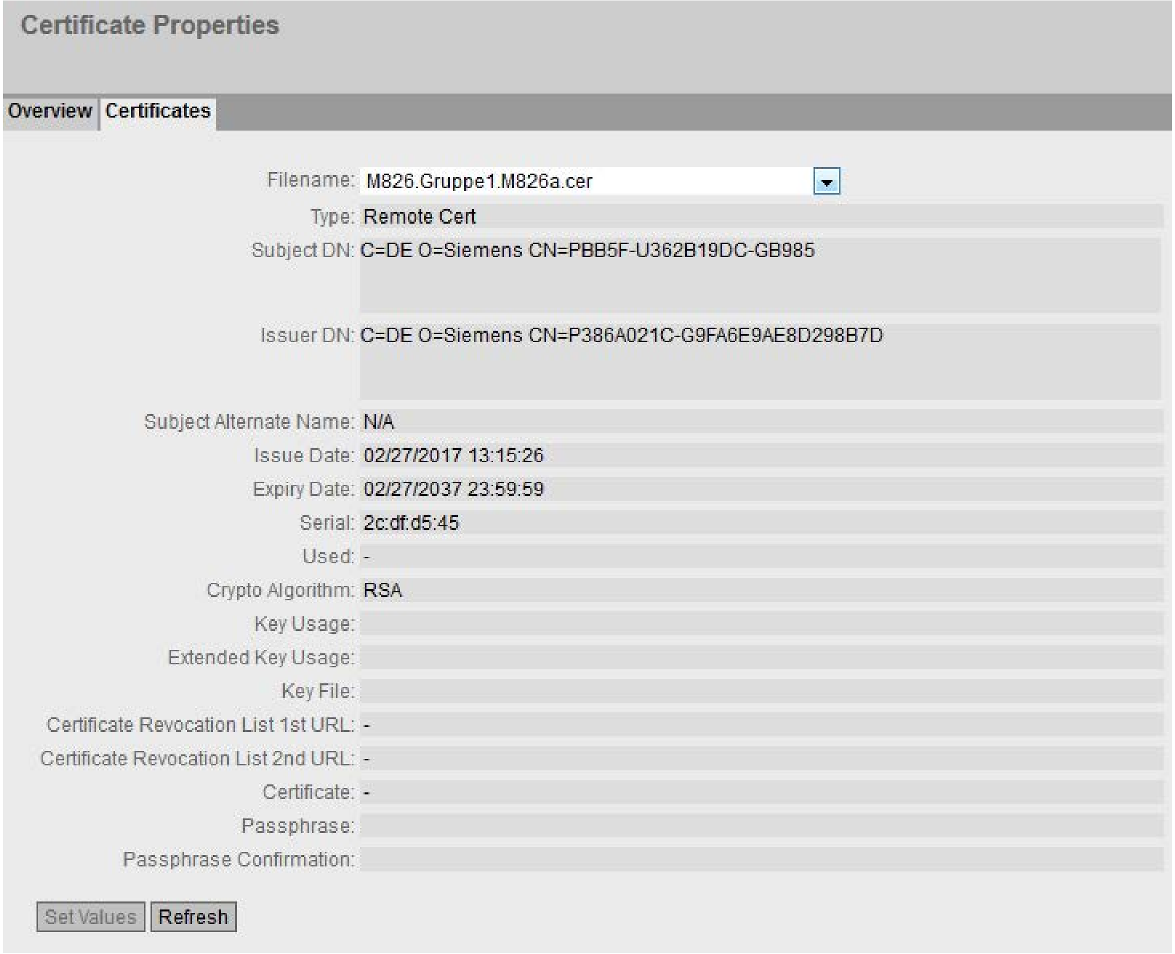
  Shows the end of the period of validity of the certificate.
- **Used**

  Shows which function uses the certificate.

4.7.4.2 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.



Certificate Properties

Filename:	M826.Gruppe1.M826a.cer
Type:	Remote Cert
Subject DN:	C=DE O=Siemens CN=PBB5F-U362B19DC-GB985
Issuer DN:	C=DE O=Siemens CN=P386A021C-G9FA6E9AE8D298B7D
Subject Alternate Name:	N/A
Issue Date:	02/27/2017 13:15:26
Expiry Date:	02/27/2037 23:59:59
Serial:	2c:df:d5:45
Used:	-
Crypto Algorithm:	RSA
Key Usage:	
Extended Key Usage:	
Key File:	
Certificate Revocation List 1st URL:	-
Certificate Revocation List 2nd URL:	-
Certificate:	-
Passphrase:	
Passphrase Confirmation:	

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.

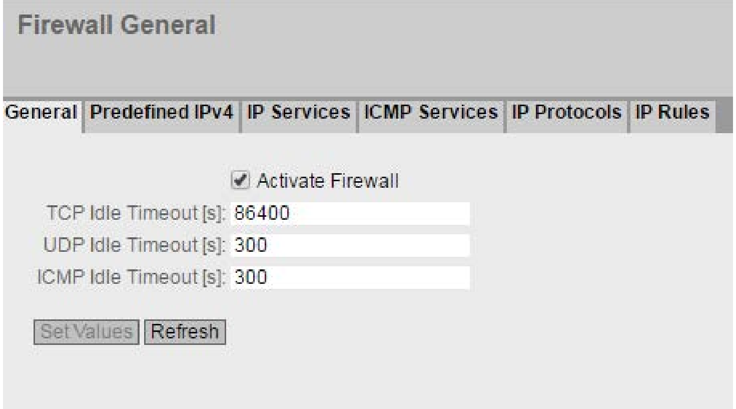
4.7.5 Firewall

4.7.5.1 General

On this WBM page, you enable the firewall.

Note

Please remember that if you disable the firewall, your internal network is unprotected.



☑ Activate Firewall
TCP Idle Timeout [s]: 86400
UDP Idle Timeout [s]: 300
ICMP Idle Timeout [s]: 300

Description

The page contains the following:

- **Activate Firewall**

  When enabled, the firewall is active.

- **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 21474836.

  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 21474836.

  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.

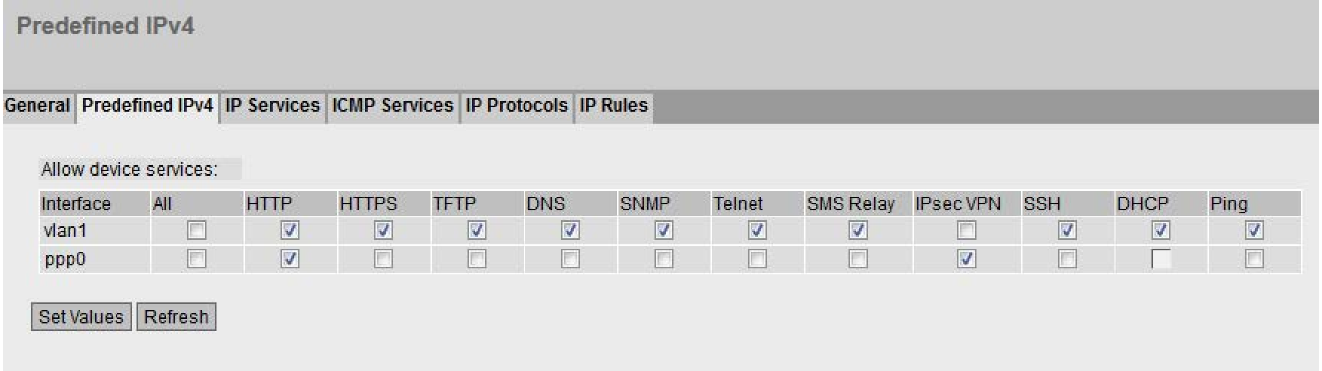
  The range of values is 1 to 21474836.

  Default setting: 300 seconds

4.7.5.2 Predefined IPv4 rules

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.

Here, you can set which services of the device should be reachable from which interface/subnet.



Allow device services:

Interface	All	HTTP	HTTPS	TFTP	DNS	SNMP	Telnet	SMS Relay	IPsec VPN	SSH	DHCP	Ping
vlan1	□	☑	☑	☑	☑	☑	☑	☑	□	☑	☑	☑
ppp0	□	☑	□	□	□	□	□	□	☑	□	□	□

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.

- Access to the following IPv4 services is permitted:

  – All
  All IPv4 services

  – HTTP
  For access to Web Based Management.

  – HTTPS
  For secure access to Web Based Management.

  Note

  HTTP and HTTPS deactivated

  If you disable HTTP and HTTPS, the WBM of the device can no longer be reached.

  HTTPS disabled

  When you disable HTTPS, you can only access the WBM using HTTP. This assumes that "HTTP & HTTPS" is set in "System > Configuration > HTTP Services". If for example "Redirect HTTP to HTTPS" is set, access via HTTP cannot be redirected to HTTPS. This means that 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.

  – SSH
  For encrypted access to the CLI.

  – DHCP
  Access to the DHCP server or the DHCP client

  – Ping
  Access to the ping function

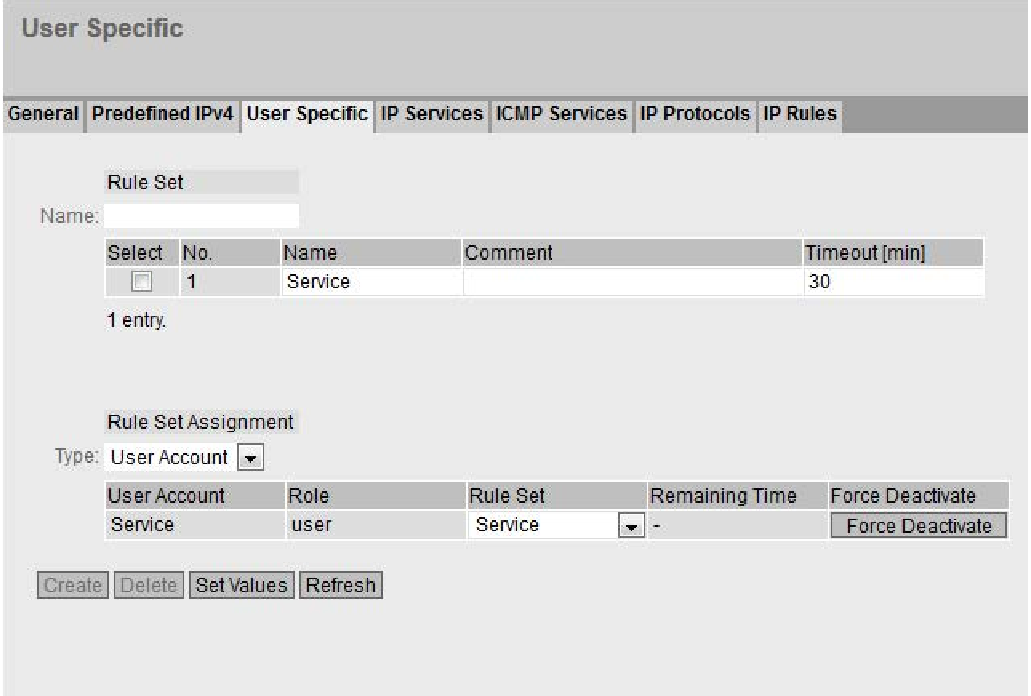
  – System time
  Access to NTP and SNTP.

4.7.5.3 Benutzerspezifisch

On this page, you define user-specific 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.



Rule Set

Name:

Select	No.	Name	Comment	Timeout [min]
□	1	Service		30

1 entry.

Rule Set Assignment

Type: User Account

User Account	Role	Rule Set	Remaining Time	Force Deactivate
Service	user	Service	-	Force Deactivate

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**

  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 "User Specific Firewall" 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 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 > Event > Configuration".

The "User Account" table contains the following columns:

- User Account

  Only the users with 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.

- 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)

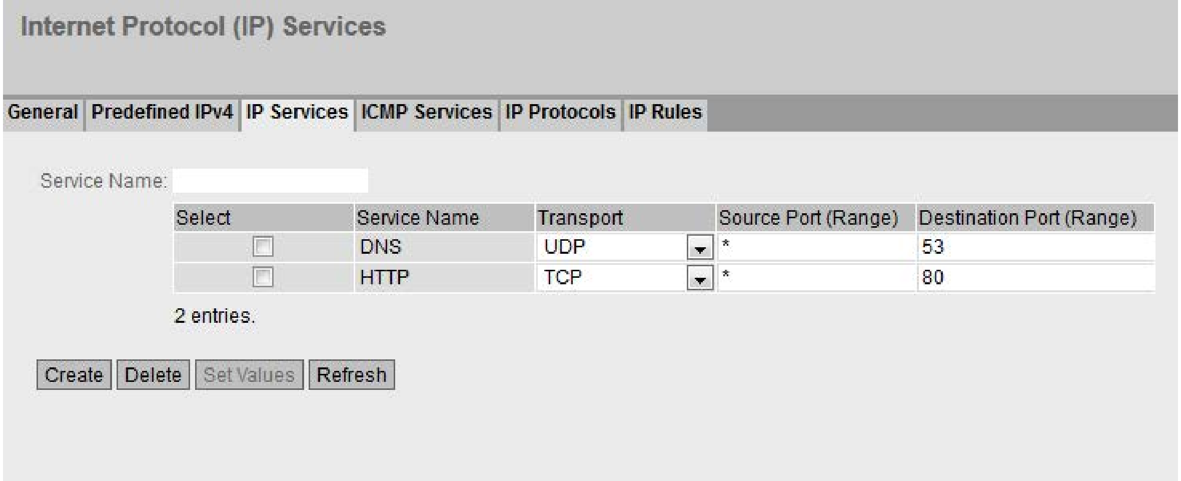
  Enter the IP address or an IP range that is allowed to send IP packets.

- Status

  Shows the remaining time for access.

4.7.5.4 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.



Service Name:

Select	Service Name	Transport	Source Port (Range)	Destination Port (Range)
□	DNS	UDP	*	53
□	HTTP	TCP	*	80

2 entries.

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:

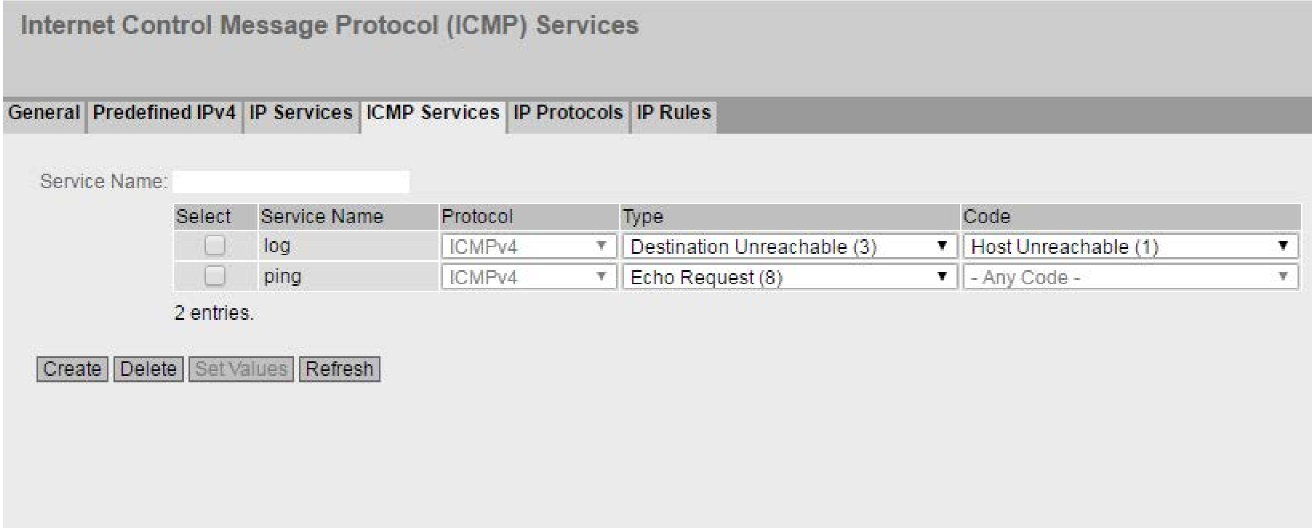
- **Select**
  Activate the check box in the row to be deleted.
- **Service Name**

  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 "*".

4.7.5.5 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.



Internet Control Message Protocol (ICMP) Services

Service Name:

Select	Service Name	Protocol	Type	Code
□	log	ICMPv4	Destination Unreachable (3)	Host Unreachable (1)
□	ping	ICMPv4	Echo Request (8)	- Any Code -

2 entries.

Description

The page contains the following:

- **Service Name**

  Enter a name for the ICMP service. The name must be unique.

This 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.

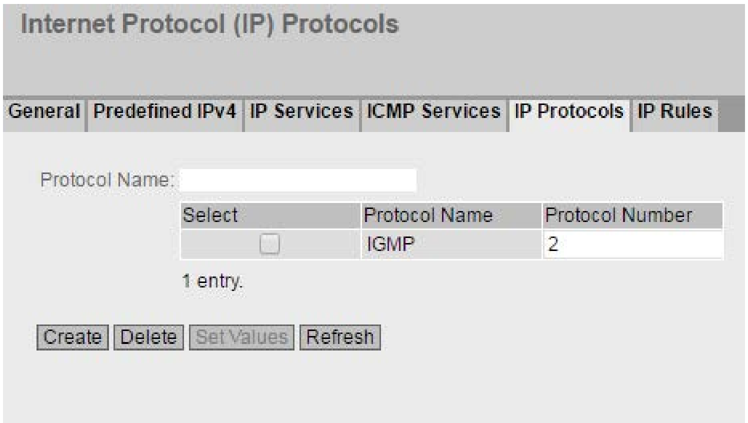
- **Type**
  Specify the ICMP packet type. A few examples are shown below:

  - 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.

4.7.5.6 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.



Internet Protocol (IP) Protocols

Protocol Name:

Select	Protocol Name	Protocol Number
□	IGMP	2

1 entry.

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 in "Protocol Name".
2. Click the "Set Values" button. A new entry is generated in the table.
3. Enter "2" in "Protocol Number".

4.7.5.7 IP rules

On this WBM page you specify your own IP packet filter rules for the firewall.

Note

Opening the WBM via a VPN tunnel

To open the WBM via a VPN tunnel, create the following IP rule:

Action: Accept

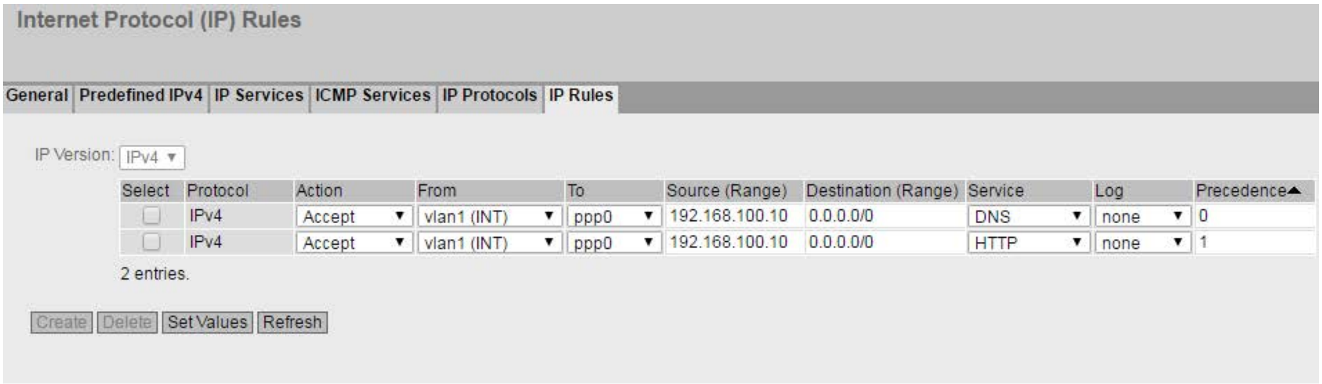
From:IPsec

To: Device

Service: HTTPS

The IP packet filer rules set here have priority:

- over the pre-defined IP packet filter rules (pre-defined IPv4) and
- over the IP packet filter rules created automatically due to a connection configuration (SINEMA RC).


Internet Protocol (IP) Rules

IP Version: IPv4

Select	Protocol	Action	From	To	Source (Range)	Destination (Range)	Service	Log	Precedence▲
□	IPv4	Accept	vlan1 (INT)	ppp0	192.168.100.10	0.0.0.0/0	DNS	none	0
□	IPv4	Accept	vlan1 (INT)	ppp0	192.168.100.10	0.0.0.0/0	HTTP	none	1

2 entries.

Description of the displayed boxes

Description

- **IP Version**

  The version of the IP protocol.

- **Rule set**

  Select the required rule set.

- **Show all**

  – Enabled: All IP rules are displayed.

  – Disabled: Only the IP rules that are assigned to the selected rule set are displayed.

This table contains the following columns:

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

- **Protocol**
  Shows the version of the IP protocol.

- **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

  – Device: Connection to the device

  – SINEMA RC: Connection to SINEMA RC Server

  – IPsec: Either all IPsec connections (all) or a specific IPsec connection

- **Source (Range)**

  Enter the IP address or an IP range that is allowed to receive IP packets.

  – Individual IP address

    Enter the IPv4 address.

  – IP range

    Specify the range with the start address "-" end address, e.g. 192.168.100.10 - 192.168.100.20.

  – All IP addresses

    Specify "0.0.0.0/0".

  – 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

    Enter the IPv4 address.

  – IP range

    Specify the range with the start address "-" end address, e.g. 192.168.100.10 - 192.168.100.20.

  – All IP addresses

    Specify "0.0.0.0/0".

- **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**
  Specify the precedence of the rule.

- **Assign**

  To assign the IP rules to the selected rule set, activate the setting for the desired rule set 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**

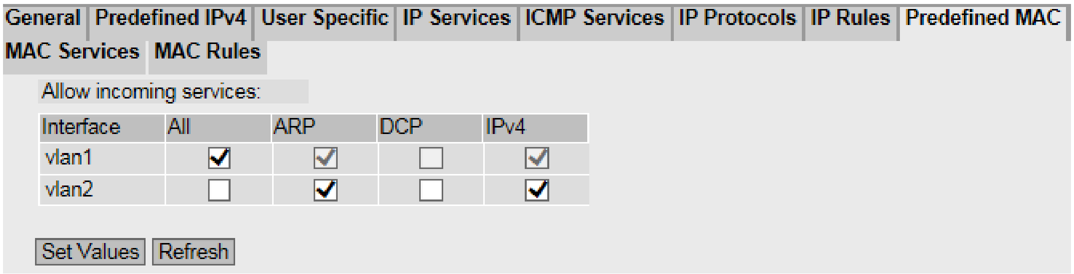
  Shows who created the IP rule.

  – NETMAP - automatically created firewall rule

4.7.5.8 Pre-defined MAC rules

The WBM page contains pre-defined MAC packet filter rules. If you create your own MAC packet filter rules, these have a higher priority than the pre-defined MAC packet filter rules.

Here, you can set which MAC services of the device should be reachable from which interface.



Allow incoming services:

Interface	All	ARP	DCP	IPv4
vlan1	☑	☑	□	☑
vlan2	□	☑	□	☑

Description

- **Interface**

  Interface to which the setting relates. The list of interfaces/subnets is dynamic and is based on the settings from "Layer 3 > Subnet".

  – VLANx: Allows access from the subnet to the device.

- Access to the following MAC services is permitted:

  – All
  All MAC services

  – ARP

  Access via ARP to the device is enabled as default.

  If you make any changes to these settings, the device may no longer be reachable.

  – DCP

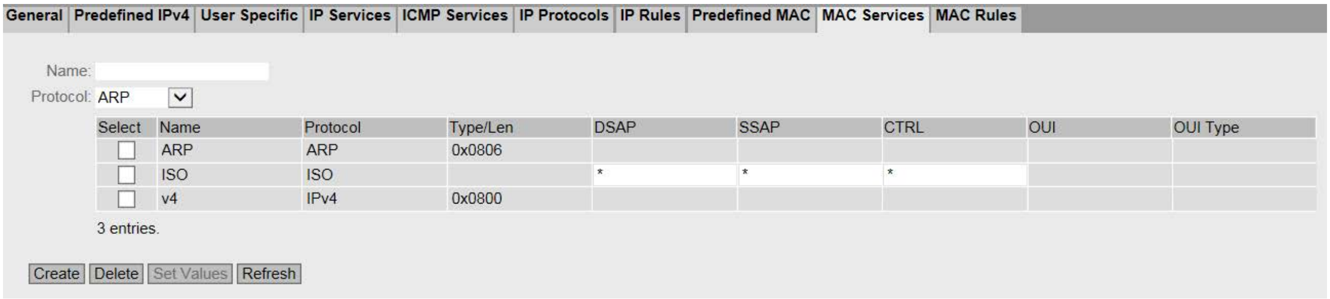
  Access to the device via DCP is permitted.

  – IPv4

  Access to the device via IPv4 is permitted.

4.7.5.9 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.



Name:
Protocol: ARP

Select	Name	Protocol	Type/Len	DSAP	SSAP	CTRL	OUI	OUI Type
□	ARP	ARP	0x0806					
□	ISO	ISO		*	*	*		
□	v4	IPv4	0x0800					

3 entries.

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 the PST tool 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

This 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**

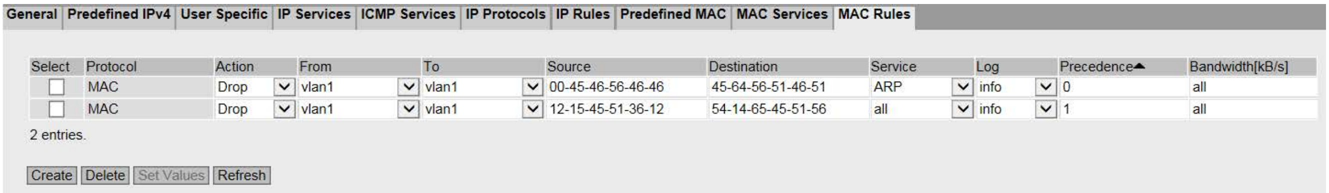
  Shows the name of the MAC protocol.

Depending on the protocol, the following inputs are necessary:

- For Ethernet protocols:
  - Type/length
- For ISO-LLC protocols:
  - DSAP: Destination Service Access Point: LLC recipient 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

4.7.5.10 MAC rules

By default, MAC packet 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.



Select	Protocol	Action	From	To	Source	Destination	Service	Log	Precedence▲	Bandwidth[kB/s]
□	MAC	Drop	vlan1	vlan1	00-45-46-56-46-46	45-64-56-51-46-51	ARP	info	0	all
□	MAC	Drop	vlan1	vlan1	12-15-45-51-36-12	54-14-65-45-51-56	all	info	1	all

2 entries.

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

This 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 subnet
- **Source**

  Enter the source address of the MAC packets.
- **Destination**

  Enter the destination address of the MAC packets.
- **Service**
  Select the service 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.

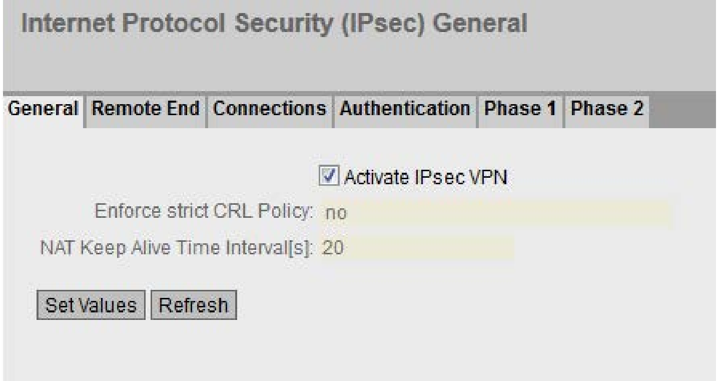
  – info / warning / critical
    The rule coming into effect is logged with the selected event severity. The log file is displayed in "Information > Log Tables > Firewall Log".
- **Precedence**
  Specify the precedence of the rule.
- **Bandwidth (kbps)**

  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.

4.7.6 IPsec VPN (SC64x-2C)

4.7.6.1 General

On the WBM page, you configure the basic settings for VPN.



Internet Protocol Security (IPsec) General

☑ Activate IPsec VPN

Enforce strict CRL Policy: no

NAT Keep Alive Time Interval[s]: 20

Description

The page contains the following:

- **Activate IPsec VPN**

  Enable or disable the IPsec protocol for VPN.

- **Enforce strict CRL Policy**

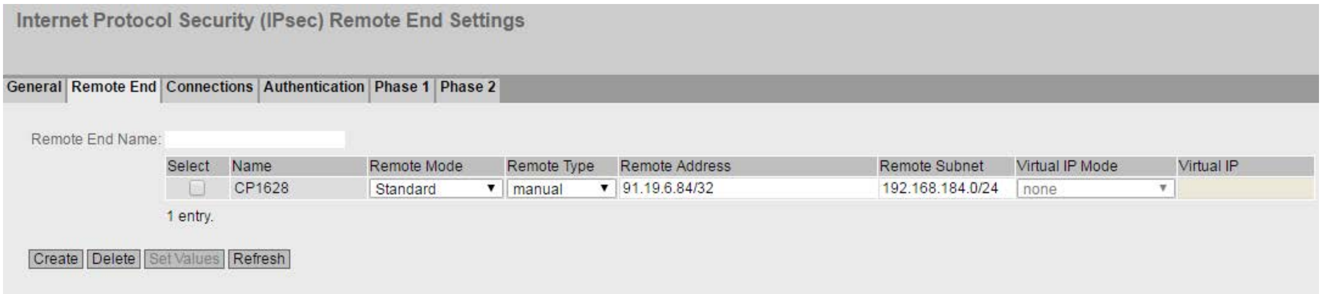
  When enabled, the validity of the certificates is checked based on the CRL (Certificate Revocation List). The certificate revocation list lists the certificates issued by the certification authority that have lost their validity before the set expiry date. You configure the certificate revocation list to be used on the WBM page "Certificates (Page 239)".

- **NAT Keep Alive Time Interval**

  Specify the interval at which sign of life frames (keepalives) 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.

4.7.6.2 Remote End

On this WBM page, you configure the partner (VPN end point).



Internet Protocol Security (IPsec) Remote End Settings

Remote End Name:

Select	Name	Remote Mode	Remote Type	Remote Address	Remote Subnet	Virtual IP Mode	Virtual IP
□	CP1628	Standard ▼	manual ▼	91.19.6.84/32	192.168.184.0/24	none ▼	

1 entry.

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.

This 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 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.

  – In Roadwarrior mode, the remote address informs the device of its reachable 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.

4.7.6.3 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

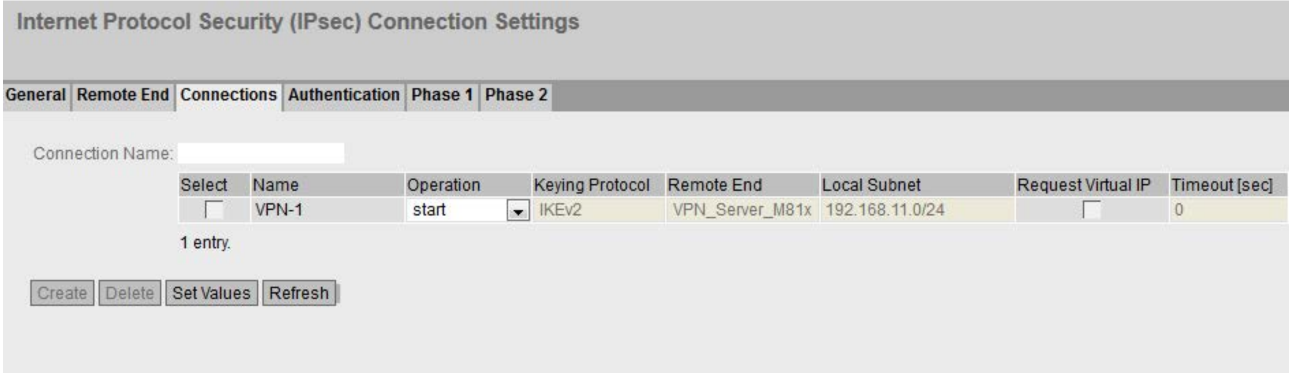
IPsec: Restrictions for phase 2 connections

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.


Internet Protocol Security (IPsec) Connection Settings

Connection Name:

Select	Name	Operation	Keying Protocol	Remote End	Local Subnet	Request Virtual IP	Timeout [sec]
□	VPN-1	start	IKEv2	VPN_Server_M81x	192.168.11.0/24	□	0

1 entry.

Description

The page contains the following boxes:

- **Connection name**

  Enter a name for the VPN connection and click "Create" to create a new connection.

This 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 57)".
  - Disabled

    The VPN connection is disabled.
  - start
    The device attempts to establish a VPN connection to the partner.
  - wait

    The device waits for the remote station 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 remote station.

    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.
  - wait on DI

    If the event "Digital In" occurs, the device waits for the remote station to initiate connection establishment.

    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.
- **Keying Protocol**

  Specify whether IKEv2 or IKEv1 will be used.
- **Remote End**

  Select the required remote station. Only partners can be configured that have been configured on the "Remote End" WBM page.
- **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.

- **Request Virtual IP**

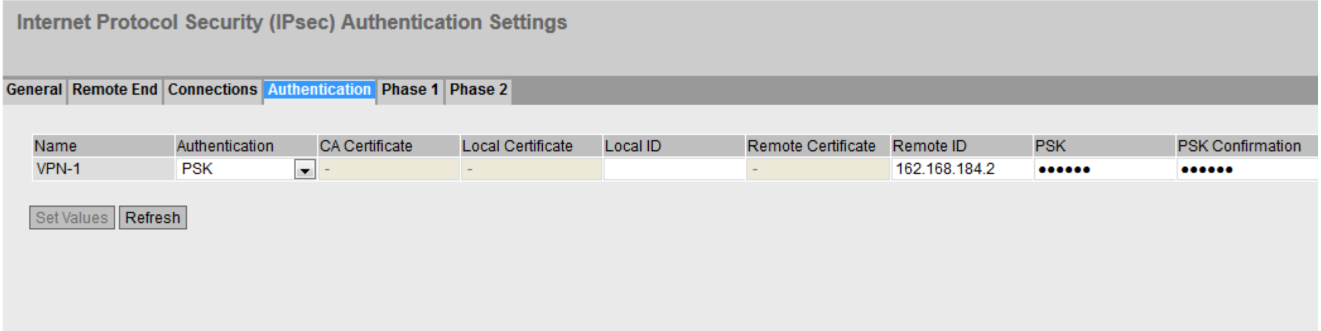
  When enabled, a virtual IP address is requested from the remote station during connection establishment.

- **Timeout [sec]**

  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.

4.7.6.4 Authentication

On this WBM page, you specify how the VPN connection partners authenticate themselves with each other.



Internet Protocol Security (IPsec) Authentication Settings

Name	Authentication	CA Certificate	Local Certificate	Local ID	Remote Certificate	Remote ID	PSK	PSK Confirmation
VPN-1	PSK	-	-		-	162.168.184.2	••••••	••••••

Description

This table contains the following columns:

- **Name**
  Shows the name of the VPN connection to which the settings relate.
- **Authentication**
  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.
  - Remote Cert
    The remote certificate is used for authentication. You specify the certificate in "Remote Certificate"
  - CA Cert
    The certificate of the certification authority is used for authentication. You specify the certificate in "CA Certificate".
  - PSK
    A pre-shared key is used for authentication. You configure the pre-shared key in "PSK".
- **CA Certificate**
  Select the certificate. Only loaded certificates can be selected.

- **Local Certificate**
  Select the machine certificate.

  You load the certificates on the device with "System > Load&Save". The loaded certificates and key files are shown on the WBM page "Security > Certificates".

- **Local ID**
  Enter the local ID from the partner certificate. Only when you use the partner certificate can you leave the box empty. The box is automatically filled with the value from the partner certificate.

- **Remote Certificate**
  Select the remote station certificate. Only loaded remote certificates can be selected.

  You load the certificates on the device with "System > Load&Save". The loaded certificates and key files are shown on the WBM page "Security > Certificates".

- **Remote ID**
  Enter the "Distinguished Name" or "Alternate Name" from the partner certificate. Only when you use the partner certificate can you leave the box empty. The box is automatically filled with the value from the partner certificate.

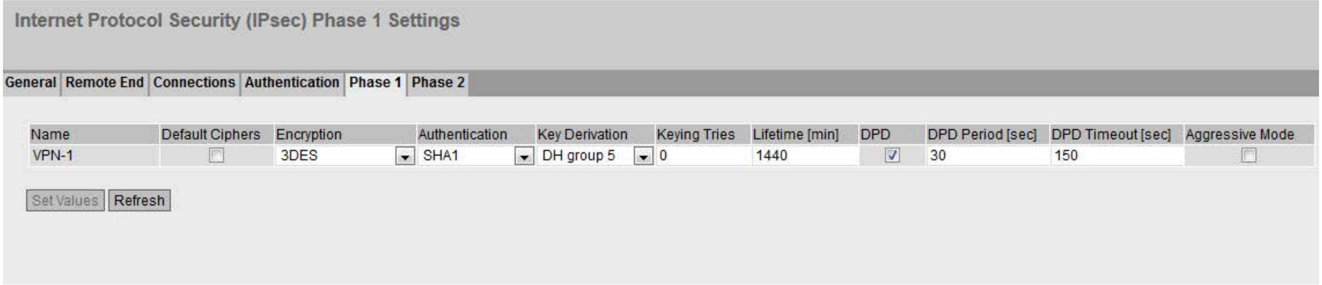
- **PSK**
  Enter the pre-shared key.

- **PSK Confirmation**
  Repeat the pre-shared key.

4.7.6.5 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.



Internet Protocol Security (IPsec) Phase 1 Settings

Name	Default Ciphers	Encryption	Authentication	Key Derivation	Keying Tries	Lifetime [min]	DPD	DPD Period [sec]	DPD Timeout [sec]	Aggressive Mode
VPN-1	□	3DES	SHA1	DH group 5	0	1440	☑	30	150	□

Description

This 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 a combination of the three algorithms (Encryption, Authentication, Key Derivation). To establish a VPN connection, the VPN connection partner must support at least one of the combinations. The selection depends on the key exchange method. Further information can be found in the section "IPsec VPN (Page 54)"

- **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. Further information can be found in the section "IPsec VPN (Page 54)".

  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 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.

4.7.6.6 Phase 2

Phase 2: Data exchange (ESP = Encapsulating Security Payload)

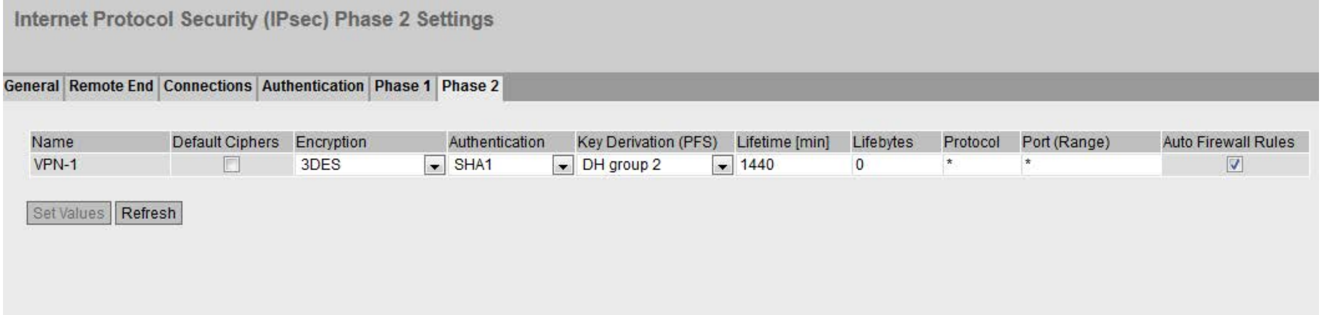
On this WBM page, you set the parameters for the protocol of the IPsec data exchange.

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.



Internet Protocol Security (IPsec) Phase 2 Settings

Name	Default Ciphers	Encryption	Authentication	Key Derivation (PFS)	Lifetime [min]	Lifebytes	Protocol	Port (Range)	Auto Firewall Rules
VPN-1	□	3DES	SHA1	DH group 2	1440	0	*	*	☑

Description

This 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 a combination of the three algorithms (Encryption, Authentication, Key Derivation). To establish a VPN connection, the VPN connection partner must support at least one of the combinations. Further information can be found in the section "IPsec VPN (Page 54)".

- **Encryption**

  For phase 2, select the required encryption algorithm. Can only be selected if "Default Ciphers" is disabled.
  Further information can be found in the section "IPsec VPN (Page 54)".

  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
    The firewall rules are created automatically for the VPN connection.

  – disabled
    You will need to create the firewall rules yourself.

Upkeep and maintenance 5

Firmware

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

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.

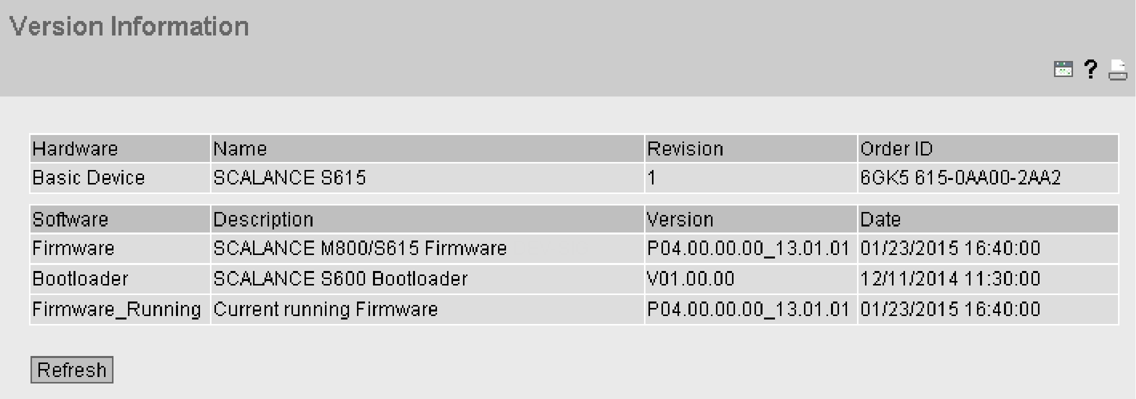
Firmware update via SFTP

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.



Version Information

Hardware	Name	Revision	Order ID
Basic Device	SCALANCE S615	1	6GK5 615-0AA00-2AA2

Software	Description	Version	Date
Firmware	SCALANCE M800/S615 Firmware	P04.00.00.00_13.01.01	01/23/2015 16:40:00
Bootloader	SCALANCE S600 Bootloader	V01.00.00	12/11/2014 11:30:00
Firmware_Running	Current running Firmware	P04.00.00.00_13.01.01	01/23/2015 16:40:00

5.1 Firmware update using WBM not possible

Cause

If there is a power failure during the firmware update, it is possible 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 exists.

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 new firmware file that you can download by TFTP.

   Note

   If you want to exit the boot loader 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 and 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 the Primary Setup Tool.

   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.

5.2 Restoring the factory settings

NOTICE

Previous settings

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

NOTICE

Inadvertent reset

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

With the reset button

When pressing the button, 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"

Appendix A

A

A.1 Format of the syslog messages

The devices generate Syslog messages (UDP default port 514) according to RFC 5424 that contain the following boxes.

PRIORITY

PRIORITY contains the coded priority of the Syslog message broken down into a Severity and Facility box.

- Facility
- Severity

VERSION

- Set to 1.

HEADER

- TIMESTAMP according to RFC 3339
- Host name
- APPNAME, PROGID and MSGID: If no information is known, the "-" character is output.

STRUCTURED DATA

- timeQuality block

MESSAGE:

- ASCII string in English

HOSTNAME_CONTENT:

- IPv4 address according to RFC1035: Each byte is represented in decimal, with a dot separating it from the previous one. XXX.XXX.XXX.XXX
- IPv6 address according to RFC4291 Section 2.2

Note

Additional information about the meaning of the boxes is available in RFC 5424.

https://tools.ietf.org/html/rfc5424

A.2 Parameters in Syslog messages

The Syslog messages can contain the following parameters:

Parameter	Description	Possible values or example
ip address	IPv4 or IPv6 address	IP address according to RFC1035 or RFC4291 Section 2.2
src port dest port	Port that is shown as decimal number. Format: %d	0 ... 65535
client mac dest mac src mac	MAC address Format: %02x:%02x:%02x;%02x:%02x:%02x	00:0C:29:2F:09:B3
protocol	Name of the service that has generated this event or of the Layer 4 protocol used. Format: %s	Possible entries of: UDP | TCP | WBM | Telnet | SSH | Console | TFTP | SFTP
group	String that identifies the group based on its name Format: %s	it-service
user name	String that identifies the authenticated user based on his/her name without spaces Format: %s	maier
local interface	Symbolic name for the local interface Format: %s	Console
action user name	Identifies the user based on his/her name This is not the authenticated user. Format: %s	Peter.Maier
role	Symbolic name for the group role Format: %s	Administrator
time minute timeout	Number of minutes Format: %d	44
time second	Number of seconds Format: %d	44
failed login count	Number of failed logins Format: %d	10
max sessions	Number of sessions Format: %d	10
vap	Symbolic name of the virtual access point interface Format: (%s) or (%s %s)	VAP1.1
status reason	Additional status information as legible string. It can contain multiple words. The string must start with " and end with " so that it can be analyzed.	(Invalid group cipher) (Unknown peer)
wlan interface	Symbolic name of the WLAN interface Format: %s	WLAN1

Parameter	Description	Possible values or example
ssid	SSID in ASCII representation any number of spaces Format: %s	MyWLAN
channel	Name of the channel Format: %s	12
signal strength	Signal strength Format: %d	12
version	Name of the version without spaces Format: %s	V1.0.3SP1
resource	Resource name without spaces protected by the protection level concept Format: %s	FullReadAccess
trigger condition	String for a trigger condition that enables the respective function without spaces Format: %s	I/O pin FB 88
trigger pin	String for an IO pin that triggers the event without spaces Format: %s	DI1
firewall rule	String for a firewall rule with spaces Format: %s	Rule1
subject	String for the subject in the certificate. Used as part of the certificate-based authentication with spaces and must also include Unicode characters Format: (% S) or (% S% S) for UTF8 code.	(Peter Maier)
config detail	String for the configuration with spaces Format: %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) Format: %d	52
network interface	Symbolic name of a network interface Format: %s	vlan 1

A.3 Syslog messages

This section describes selected Syslog messages. The selection is based on IEC 62443-3-3. This means you can integrate these events into a central monitoring system (SIEM).

Identification and authentication of human users

Log Message	Console: User {user name} logged in.
Standard	IEC 62443-3-3 Reference: SR1.1
Description	Valid login information that is specified during local login.
Example	Console: User admin logged in.
Severity	Info
Facility	local0

Log text	Console: Default user {user name} logged in.
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 007-R5)
Description	User is logged in with default user name and password.
Example	Console: Default user admin logged in.
Severity	Info
Facility	local0

Log text	{protocol}: User {user name} logged in from {ip address}.
Standard	IEC 62443-3-3 Reference: SR1.1
Description	Valid login information that is specified during remote login.
Example	WBM: User admin logged in from 192.168.0.1.
Severity	Info
Facility	local0

Log text	{protocol}: Default user {user name} logged in from {ip address}.
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 007-R5)
Description	User logged in with default user name and password.
Example	SSH: Default user admin logged in from 192.168.0.1.
Severity	Info
Facility	local0

Log text	Console: User {user name} logged out.
Standard	IEC 62443-3-3 Reference: SR1.1
Description	User session completed - logged out.
Example	Console: User admin logged out.
Severity	Info
Facility	local0

Log text	{protocol}: User {user name} logged out from {ip address}.
Standard	IEC 62443-3-3 Reference: SR1.1
Description	User session completed - logged out.

Example	SSH: User admin logged out from 192.168.0.1.
Severity	Info
Facility	local0

Log text	Console: User {user name} failed to log in.
Standard	IEC 62443-3-3 Reference: SR1.1
Description	Incorrect user name or incorrect password (login information) specified during local login.
Example	Console: User testuser failed to log in.
Severity	Warning
Facility	local0

Log text	{protocol}: User {user name} failed to log in from {ip address}.
Standard	IEC 62443-3-3 Reference: SR1.1
Description	Incorrect user name or incorrect password (login information) specified during remote login.
Example	SSH: User testuser failed to log in from 192.168.0.1.
Severity	Warning
Facility	local0

Identification and authentication of devices (access via firewall)

Log 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}

Standard	IEC 62443-3-3 Reference: SR 1.2
Description	A known device requested a connection.
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
Severity	Info or Warning or Error (configurable)
Facility	local0

Log 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}

Standard	IEC 62443-3-3 Reference: SR 1.2
Description	An unknown device requested a connection. Request was denied.

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
Severity	Info or Warning or Error (configurable)
Facility	local0

Identification and authentication of device (connection via TIA Portal Cloud Connector)

Log text	Cloud Connector:Connection number {config detail} from {ip address} established.
Standard	IEC 62443-3-3 Reference: SR 1.2
Description	A known device requested a connection. (Connection via TIA Portal Cloud Connector)
Example	Cloud Connector: Connection number 10 from 192.168.55.111 established.
Severity	Info
Facility	local0

Log text	Cloud Connector: Connection number {config detail} from {ip address} closed.
Standard	IEC 62443-3-3 Reference: SR 1.2
Description	An unknown device requested a connection. Request was denied. (Connection via TIA Portal Cloud Connector)
Example	Cloud Connector: Connection number 6 from 192.168.55.111 closed.
Severity	Info
Facility	local0

User account management

Log text	{protocol}: User {user name} changed own password.
Standard	IEC 62443-3-3 Reference: SR1.3
Description	User has changed own password.
Example	WBM: User admin changed own password.
Severity	Info
Facility	local0

Log text	{protocol}: User {user name} changed password of user {action user name}.
Standard	IEC 62443-3-3 Reference: SR1.3
Description	User has changed other password.
Example	Console: User admin changed password of user test.
Severity	Info
Facility	local0

Log text	{protocol}: User {user name} created user-account {action user name}.
Standard	IEC 62443-3-3 Reference: SR1.3
Description	The administrator created a new account.
Example	WBM: User admin created user-account joachim.
Severity	Info
Facility	local0

Log text	{protocol}: User {user name} deleted user-account {action user name}.
Standard	IEC 62443-3-3 Reference: SR1.3
Description	The administrator deleted an existing account.
Example	WBM: User admin deleted user-account joachim.
Severity	Info
Facility	local0

Management of the identifiers

Log text	{protocol}: User {user name} created group {group}.
Standard	IEC 62443-3-3 Reference: SR1.4
Description	The administrator has created a group.
Example	WBM: User admin created group it-service.
Severity	Info
Facility	local0

Log text	{protocol}: User {user name} deleted group {group}.
Standard	IEC 62443-3-3 Reference: SR1.4
Description	The administrator deleted an existing group.
Example	WBM: User admin deleted group it-service.
Severity	Info
Facility	local0

Failed login attempts

Log text	User {user name} account is locked for {time} minutes after {failed login count} unsuccessful login attempts.
Standard	IEC 62443-3-3 Reference: SR1.11
Description	If there are too many failed logins, the corresponding user account was locked for a specific period of time.
Example	User admin account is locked for 10 minutes after 30 unsuccessful login attempts.
Severity	Warning
Facility	local0

Access via untrusted networks (IPsec)

Log text	[IKE] <{connection name}|{config detail}> IKE_SA {connection name}[{config detail}] established between {ip address}[{config detail}]...{ip address}[{config detail}]
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1)
Description	VPN connection established. (IPsec)
Example	[IKE] <c1|3> IKE_SA c1[1] established between 192.168.55.210[lokal].. 192.168.55.211[remote]
Severity	Info
Facility	local0

Log text	[IKE] <{connection name}|{config detail}> deleting IKE_SA {connection name}[{config detail}] between {ip address}[{config detail}]...{ip address}[{config detail}]
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1)
Description	VPN tunnel is closed. (IPsec)
Example	[IKE] <c1|3> deleting IKE_SA c2[1] between 192.168.55.211[lokal].. 192.168.55.210[remote]
Severity	Info
Facility	local0

Log text	[IKE] <{connection name}|{config detail}> received AUTHENTICATION_FAILED notify error
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R3)
Description	Authentication of VPN connection failed (IPsec).
Example	[IKE] <c1|1> received AUTHENTICATION_FAILED notify error
Severity	Warning
Facility	local0

Access via untrusted networks (OpenVPN)

Log text	OVPN_{connection name}[{config detail}]: Initialization Sequence Completed
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1)
Description	VPN connection established. (OpenVPN)
Example	OVPN_Conn_1[2427]: Initialization Sequence Completed
Severity	Info
Facility	local0

Log text	OpenVPN connection {connection name} has been deactivated.
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1)
Description	VPN connection was closed (OpenVPN).

Example	OpenVPN connection c1 has been deactivated.
Severity	Critical
Facility	local0

Access via untrusted networks (SINEMA Remote Connect)

Log text	SINEMA RC - State of Digital Input changed to HIGH. SINEMA RC - OpenVPN connection established.
Standard	IEC 62443-3-3 Reference: SR 1.13
Description	Remote access is permitted. (SINEMA RC, Digital Input)
Example	SINEMA RC - State of Digital Input changed to HIGH. SINEMA RC - OpenVPN connection established.
Severity	Info
Facility	local0

Log text	SINEMA RC - Received Wakeup SMS. SINEMA RC - OpenVPN connection established.
Standard	IEC 62443-3-3 Reference: SR 1.13
Description	Remote access is permitted. (SINEMA RC, Wakeup SMS)
Example	SINEMA RC - Received Wakeup SMS. SINEMA RC - OpenVPN connection established.
Severity	Info
Facility	local0

Log text	SINEMA RC - State of Digital Input changed to LOW. SINEMA RC - OpenVPN terminated.
Standard	IEC 62443-3-3 Reference: SR 1.13
Description	Remote access denied (SINEMA RC, Digital Input)
Example	SINEMA RC - State of Digital Input changed to LOW. SINEMA RC - OpenVPN terminated.
Severity	Info
Facility	local0

Log text	SINEMA RC - Received Shutdown SMS. SINEMA RC - OpenVPN terminated.
Standard	IEC 62443-3-3 Reference: SR 1.13
Description	Remote access denied (SINEMA RC, Wakeup SMS)
Example	SINEMA RC - Received Shutdown SMS. SINEMA RC - OpenVPN terminated.
Severity	Info
Facility	local0

Authorization enforcement (access via custom firewall)

Log text	User specific firewall user "{user name}" activated rule set "{firewall rule}" with ip address "{ip address}". Timeout is set to {timeout} minutes.
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R2)
Description	User has logged onto the user-specific firewall. (USF Digital User Login)
Example	User specific firewall user "usf" activated rule set "rs1" with ip address "172.23.1.14". Timeout is set to 5 minutes.
Severity	Info
Facility	local0

Log text	User specific firewall user "{user name}" activated rule set "{firewall rule}" with ip address "{ip address}". Timeout is set to {timeout} minutes.
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R2)
Description	User has logged onto the user-specific firewall. (USF Digital Input Login)
Example	User specific firewall digital input {trigger pin} activated rule set "{firewall rule}" with ip address "{ip address}".
Severity	Info
Facility	local0

Log text	User specific firewall user "{user name}" ruleset "{firewall rule}" time expired.
Standard	IEC 62443-3-3 Reference: SR 2.1
Description	Access to the user-specific firewall denied. Access time expired. (USF User Logout)
Example	User specific firewall user "usf" ruleset "rs1" time expired.
Severity	Warning
Facility	local0

Log text	User specific firewall user "{user name}" logged out by administrator configuration.
Standard	IEC 62443-3-3 Reference: SR 2.1
Description	Access to the user-specific firewall denied. The device administrator deactivates the user using the "Force Deactivate" button. (USF user force log out by admin)
Example	User specific firewall user "usf" logged out by administrator configuration.
Severity	Warning
Facility	local0

Log text	User specific firewall user "{user name}" deactivated by administrator configuration.
Standard	IEC 62443-3-3 Reference: SR 2.1
Description	Access to the user-specific firewall denied. The device administrator has deactivated the user. (USF user deactivated by admin)
Example	User specific firewall user "usf" deactivated by administrator configuration.

Severity	Warning
Facility	local0

Log text	User specific firewall digital input {trigger pin} deactivated rule set "{firewall rule}".
Standard	IEC 62443-3-3 Reference: SR 2.1
Description	Access to the user-specific firewall denied; corresponding rule set was deactivated. (USF Digital Input Logout)
Example	User specific firewall digital input 1 deactivated rule set "rs1".
Severity	Warning
Facility	local0

Session lock

Log text	The session of user {user name} was closed after {time} seconds of inactivity.
Standard	IEC 62443-3-3 Reference: SR2.5
Description	The current session was locked due to inactivity.
Example	The session of user admin was closed after 60 seconds of inactivity.
Severity	Warning
Facility	local0

Closing a remote access session

Log text	[JOB] <{connection name}|{config detail}> deleting CHILD_SA after {time second} seconds of inactivity
Standard	IEC 62443-3-3 Reference: SR 2.6
Description	The remote session was ended after a period of inactivity. (IPsec)
Example	[JOB] <to_Baugruppe1|21> deleting CHILD_SA after 20 seconds of inactivity
Severity	Info
Facility	local0

Log text	OVPN_{connection name}[{config detail}]: [{config detail}] Inactivity timeout (--ping- restart), restarting
Standard	IEC 62443-3-3 Reference: SR 2.6
Description	The remote session was ended after a period of inactivity. (OpenVPN)
Example	OVPN_c1[26296]: [router] Inactivity timeout (--ping-restart), restarting
Severity	Info
Facility	local0

Limiting the number of simultaneous sessions

Log text	{protocol}: The maximum number of {max sessions} concurrent login session exceeded.
Standard	IEC 62443-3-3 Reference: SR2.7
Description	The maximum number of parallel connections is exceeded.
Example	WBM: The maximum number of 8 concurrent login session exceeded.
Severity	Warning
Facility	local0

This section describes selected Syslog messages. The selection is based on IEC 62443-3-3. This means you can integrate these events into a central monitoring system (SIEM).

Non-deniability (change configuration)

Log text	Device configuration changed.
Standard	IEC 62443-3-3 Reference: SR2.12
Description	The configuration has been changed permanently.
Example	Device configuration changed.
Severity	Info
Facility	local0

Communication integrity

Log text	[IKE] <{connection name}|{config detail}> received invalid DPD sequence number {config detail} (expected {config detail}), ignored
Standard	IEC 62443-3-3 Reference: SR 3.1
Description	Integrity check failed. (IPsec)
Example	[IKE] <c1|1> received invalid DPD sequence number 10 (expected 12), ignored
Severity	Info
Facility	local0

Log text	OVPN_{connection name}[{config detail}]: Authenticate/Decrypt packet error: packet HMAC authentication failed
Standard	IEC 62443-3-3 Reference: SR 3.1
Description	Integrity check failed (OpenVPN).
Example	OVPN_c1[25409]: Authenticate/Decrypt packet error: packet HMAC authentication failed
Severity	Warning
Facility	local0

Restoration of the automation system

Log text	{protocol}: Loaded file type Firmware {version} (restart required).
Standard	IEC 62443-3-3 Reference: SR7.4
Description	Firmware update was successfully uploaded.
Example	TFTP: Loaded file type Firmware V02.00.00 (restart required).
Severity	Info
Facility	local0

Log text	{protocol}: User {user name} loaded file type Firmware {version} (restart required).
Standard	IEC 62443-3-3 Reference: SR7.4
Description	Firmware update was successfully uploaded.
Example	WBM: User admin loaded file type Firmware V02.00.00 (restart required).
Severity	Info
Facility	local0

Log text	{protocol}: Failed to load file type Firmware.
Standard	IEC 62443-3-3 Reference: SR7.4
Description	Error loading the firmware update.
Example	WBM: Failed to load file type Firmware.
Severity	Warning
Facility	local0

Log text	{protocol}: Loaded file type Config (restart required).
Standard	IEC 62443-3-3 Reference: SR7.4
Description	The configuration is applied.
Example	TFTP: Loaded file type Config (restart required).
Severity	Info
Facility	local0

Log text	{protocol}: Loaded file type ConfigPack (restart required).
Standard	IEC 62443-3-3 Reference: SR7.4
Description	The configuration is applied.
Example	TFTP: Loaded file type ConfigPack (restart required).
Severity	Info
Facility	local0

Log text	{protocol}: User {user name} loaded file type Config (restart required).
Standard	IEC 62443-3-3 Reference: SR7.4

Description	The configuration is applied.
Example	WBM: User admin loaded file type Config (restart required).
Severity	Info
Facility	local0

Log text	{protocol}: User {user name} loaded file type ConfigPack (restart required).
Standard	IEC 62443-3-3 Reference: SR7.4
Description	The configuration is applied.
Example	WBM: User admin loaded file type ConfigPack (restart required).
Severity	Info
Facility	local0

Index