SIEMENS

SIMATIC NET

Industrial Ethernet Security SCALANCE S615 Web Based Management

Configuration Manual

08/2016

C79000-G8976-C388-04

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

Document order number: C79000-G8976-C388
Ⓟ 09/2016 Subject to change

Preface

Validity of the manual

This Configuration Manual covers the following product:

- SCALANCE S615

This Configuration Manual applies to the following software version:

- SCALANCE S615 firmware as of version V 4.2

Purpose of the Configuration Manual

This Configuration Manual is intended to provide you with the information you require to install, commission and operate the device. It provides you with the information you require to configure the devices.

Orientation in the documentation

Apart from the Configuration Manual you are currently reading, the following documentation is also available from on the topic of Remote Network:

- Getting Started SCALANCE S615

  Based on examples, this document explains the configuration of the SCALANCE S615.

- Operating Instructions SCALANCE S615

  You will find this document on the Internet pages of Siemens Industry Online Support. It contains information on installation, connecting up and approvals of the SCALANCE S615.

- Operating Instructions SINEMA RC Server

  You will find this document on the Internet pages of Siemens Industry Online Support. It contains information on the installation, configuration and operation of the application SINEMA Remote Connect Server.

SIMATIC NET manuals

You will find SIMATIC NET manuals on the Internet pages of Siemens Industry Online Support:

- Using the search function:

  Link to Siemens Industry Online Support (http://support.automation.siemens.com/WW/view/en)

  Enter the entry ID of the relevant manual as the search item.

- In the navigation panel on the left-hand side in the area "Industrial Communication":

  Link to the area "Industrial Communication" (http://support.automation.siemens.com/WW/view/en/10805878/130000)

  Go to the required product group and make the following settings:
  tab "Entry list", Entry type "Manuals"

You will find the documentation for the SIMATIC NET products relevant here on the data storage medium that ships with some products:

- Product CD / product DVD
- SIMATIC NET Manual Collection

SIMATIC NET glossary

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

You will find the SIMATIC NET glossary here:

- SIMATIC NET Manual Collection or product DVD

  The DVD ships with certain SIMATIC NET products.

- On the Internet under the following address:

  50305045 (http://support.automation.siemens.com/WW/view/en/50305045)

Firmware

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

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 only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit
Link: (http://www.siemens.com/industrialsecurity)

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

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

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_ScalanceM-800_S615_86.htm

Trademarks

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

SCALANCE, SINEMA, KEY-PLUG, C-PLUG

Table of contents

Description 1

1.1 Function

Configuration

Configuration of all parameters using the

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

Security functions

- Router with NAT function
  - IP masquerading
  - NAPT
  - SourceNAT
  - NETMAP
- Password protection
- Firewall function
  - Port forwarding
  - 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
  - OpenVPN client
- SINEMA RC client
- Proxy server
- Siemens Remote Service (SRS)

Monitoring / diagnostics / maintenance

- LEDs

  Display of operating statuses via the 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 and controlling network components such as routers or switches from a central station.

Other functions

- Time-of-day synchronization
  - NTP
  - SIMATIC Time Client
  - SNTP
- DHCP
  - DHCP server (local network)
  - DHCP client
- Virtual networks (VLAN)

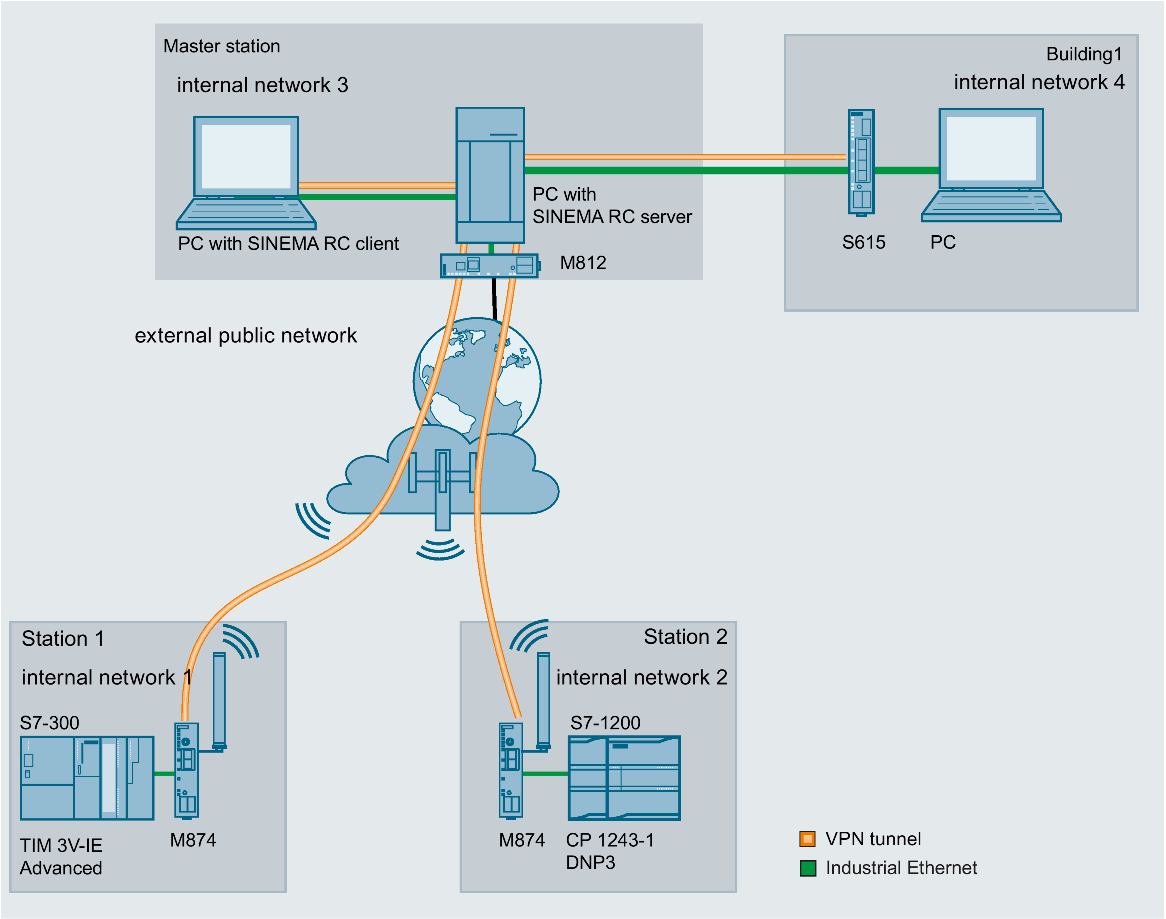
  To structure Industrial Ethernet networks with a fast growing number of nodes, a physical network can be divided into several virtual subnets
- Digital input/digital output
- Dynamic DNS client
- DNS client / DNS proxy
- SMTP client

1.2 Configuration examples

1.2.1 TeleControl with SINEMA RC

In this configuration, the remote maintenance master station is a connected to the Internet/intranet via the SINEMA Remote Connect Server. The stations communicate via SCALANCE M874 or SCALANCE S615 that establish a VPN tunnel to the SINEMA RC server server. In the master station, the SINEMA SINEMA RC client establishes a VPN tunnel to the SINEMA RC Server.

The devices must log on to the SINEMA RC server. The VPN tunnel between the device and the SINEMA RC Server is established only after successful authentication. Depending on the configured communications relations and the security settings, the SINEMA RC server connects the individual VPN tunnels.



Procedure

To be able to access a plant via a remote maintenance master station, follow the steps below:

1. Establish the Ethernet connection between the S615 and the connected Admin PC.
2. Create the devices and node groups on the SINEMA RC Server.
3. Configure the connection to the SINEMA RC server on the device, refer to the section SINEMA RC (Page 150).
4. Set up the connected applications of the plant for data communication.

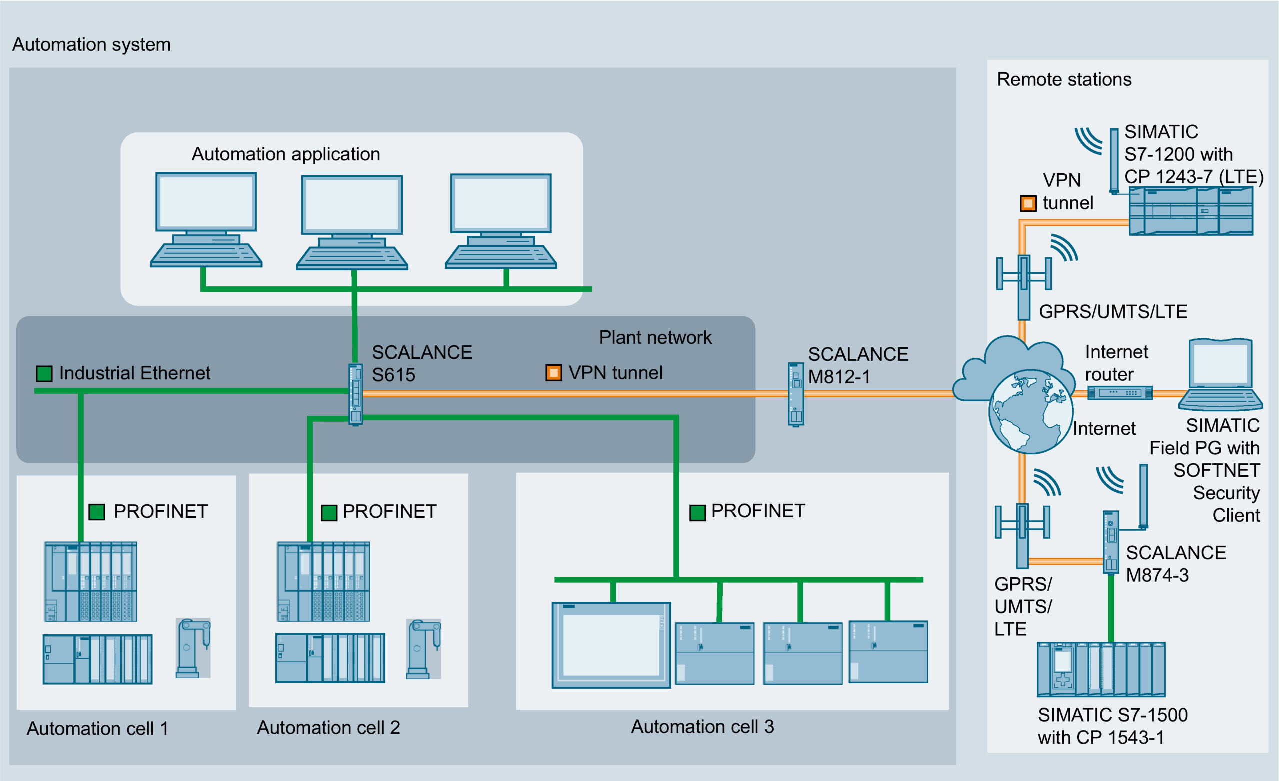
1.2.2 Secure access with S615

Secure remote access and network segmentation with SCALANCE S615

A secure connection for data exchange between an automation plant and remote stations will be established via the Internet and mobile wireless network. At the same time, a secure connection will be established when necessary for service purposes. This connection is, however, restricted to a specific plant section or a specific machine.

In the automation plant, a SCALANCE S615 is connected to the Internet via the ADSL+ router M812-1. The remote stations will be connected to the Internet via the LTE-CP 1243-7 or the HSPA+ router SCALANCE M874-3. The devices establish a VPN connection to the SCALANCE S615 via which data can be exchanged securely.

When necessary, the service technician connects to the Internet. With the SOFTNET Security Client, he or she establishes a secure VPN connection to the S615. Various IP subnets are connected to the S615 between which the integrated firewall checks communication. This allows the communication of the service technician to be restricted to a specific IP subnet.



1.3 Requirements for operation

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 S615 can be reached as follows for initial configuration:

	Default values set in the factory
Ethernet interface for the configuration (internal)	P1 ... P4 (vlan 1)
Ethernet interface for the connection to WAN (external)	P5 (vlan 2)
IP address	192.168.1.1
Subnet mask	255.255.255.0
User name	admin (cannot be changed)
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 55)" and in "Starting and logging in (Page 57)".

1.4 System functions

Availability of the system functions

The following table shows the availability of the system functions on the devices. Note that all functions are described in this configuration manual and in the online help. Depending on the KEY-PLUG, some functions are not available.

We reserve the right to make technical changes.

		SCALANCE S615
Basic Wizard	IP Settings	✓
	Device Settings	✓
	SIM	✓
	Operator	✓
	Time	✓
	SINEMA RC	✓ (KEY-PLUG SINEMA RC 6GK5908-0PA00)
	DDNS	✓
Informationen	ARP Table	✓
	Log Tables	✓
	SINEMA RC	✓ (KEY-PLUG SINEMA RC 6GK5908-0PA00)
System	SMTP-Client	✓
	SNMP	✓
	Manual Setting	✓
	SNTP	✓
	NTP	✓
	SIMATIC Time Client	✓
	Auto Logout	✓
	Syslog Client	✓
	Fault Monitoring	✓
	PLUG	✓
	SMS	✓
	DNS	✓
	DHCP	✓
	SRS	✓
	Proxy Server	✓
	SINEMA RC	✓ (KEY-PLUG SINEMA RC 6GK5908-0PA00)

		SCALANCE S615
Interfaces	Ethernet	✓
	PPP	✓
Layer 2	Port-basiertes VLAN	✓
	Dynamic MAC Aging	✓
	LLDP	✓
Layer 3	Static Routes	✓
	Subnets	✓
	NAT	✓
Security	Password	✓
	User Accounts	✓
	Certificates	✓
	Firewall	✓
	IPsec VPN	✓
	OpenVPN	✓

1.5 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.

Depending on your IE switch, some functions are not available.

	Configurable function	Maximum number
System	Syslog server	3
	E-mail server	3
	SNMPv1 trap recipient	10
	SNTP server	1
	NTP server	1
	DHCP pools	5
	IPv4 addresses managed by the DHCP server (dynamic + static)	100
	DHCP static assignments per DHCP pool	20
	DHCP options	20
	SINEMA RC	1
Layer 2	Virtual LANs (port-based; including VLAN 1)	16
	Maximum frame size	2048 bytes
Security	Users	16
	Firewall rules	64
	IPsec VPN	20
	OpenVPN	Connections: 5 Remote end. 25

1.6 C-PLUG and KEY-PLUG

How it works

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

NOTICE
Do not remove or insert a C-PLUG / KEY-PLUG during operation!
A PLUG may only be removed or inserted when the device is turned off. The device checks whether 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 KEY-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 WBM in "Information > 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.

License information on the KEY-PLUG

In addition to the configuration, the KEY-PLUG also contains a license that allows the use of Siemens Remote Services.

Type	Properties	Article number
C-PLUG	Exchangeable storage medium (32 MB) for the configuration data	6GK1900-0AB00
	Exchangeable storage medium (256 MB) for the configuration data	6GK1900-0AB10
KEY-PLUG SINEMA RC	Exchangeable storage medium (256 MB) to enable the connection functionality to SINEMA Remote Connect and for accepting configuration data.	6GK5908-0PB00

Technical basics 2

2.1 IPv4 address, subnet mask and address of the gateway

Range of values for IPv4 address

The IPv4 address consists of four decimal numbers with the range from 0 to 255, each number separated by a period; example: 141.80.0.16

IPv4 address format - notation

An IPv4 address consists of 4 bytes. Each byte is represented in decimal, with a dot separating it from the previous one.

XXX.XXX.XXX.XXX

XXX stands for a number between 0 and 255

The IPv4 address consists of two parts:

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

Range of values for subnet mask

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

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

The 1s specify the network number within the IPv4 address. The 0s specify the host address within the IPv4 address.

Example:

Correct values:

255.255.0.0 D =   1111 1111.1111 1111.0000 0000.0000 0000 B

255.255.128.0 D = 1111 1111.1111 1111.1000 0000.0000 0000 B

255.254.0.0 D =   1111 1111.1111 1110.0000 0000.0000.0000 B

Incorrect value:

255.255.1.0 D =   1111 1111.1111 1111.0000 0001.0000 0000 B

Relationship between the IPv4 address and subnet mask

The first decimal number of the IPv4 address (from the left) determines the structure of the subnet mask with regard to the number of "1" values (binary) as follows (where "x" is the host address):

First decimal number of the IPv4 address	Subnet mask
0 to 127	255.x.x.x
128 to 191	255.255.x.x
192 to 223	255.255.255.x

Classless Inter-Domain Routing (CIDR)

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

Example:

IPv4 address 192.168.0.0 with subnet mask 255.255.255.0

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

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

Value range for gateway address

The address consists of four decimal numbers taken from the range 0 to 255, each number being separated by a period; example: 141.80.0.1

Relationship between IPv4 address and gateway address

The only positions of the IPv4 address and gateway address that may differ are those in which "0" appears in the subnet mask.

Example:

You have entered the following: 255.255.255.0 for the subnet mask; 141.30.0.5 for the IPv4 address and 141.30.128.0 for the gateway address. The Ipv4 address and gateway address may only be different in the 4th decimal number. In the example, however, the 3rd position is different.

You must, therefore, change one of the following in the example:

The subnet mask to: 255.255.0.0 or

the IPv4 address to: 141.30.128.1 or

the gateway address to: 141.30.0.1

2.2 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

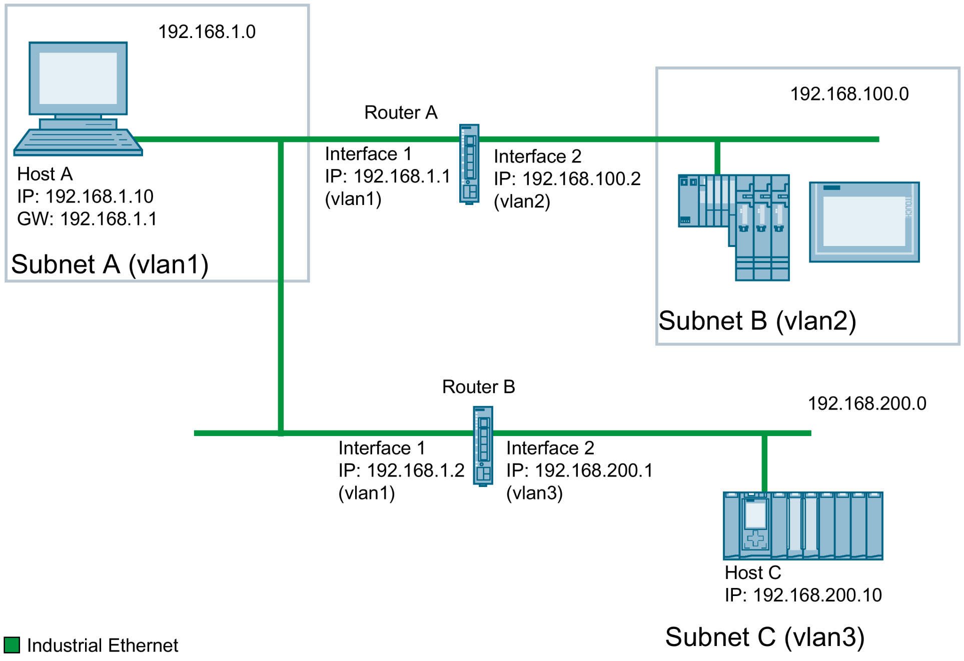
    Echo request, better known as ping.

- **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. Router A cannot forward the IP frame because it does not know the destination network. 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.

2.3 VLAN

2.3.1 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 28). 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 164)".

- Protocol-based VLAN
  Each port of a device is assigned a protocol group.

- Subnet-based VLAN
  The IP address of the device is assigned a VLAN ID.

VLAN assignment on the device

In the factory settings, the following assignments are made on the SCALANCE S615:

P1 to P4	vlan1 For access from the local network (LAN) to the device
P5	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.

2.3.2 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:

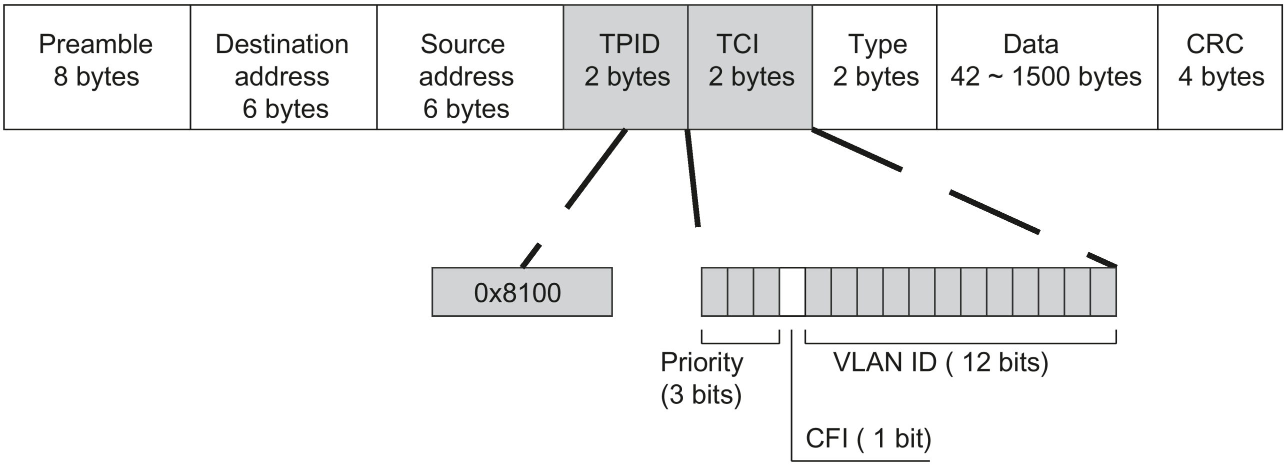


Figure 2-1 Structure of the expanded Ethernet frame

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

2.4 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 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

2.5 Security functions

2.5.1 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.

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 174)".

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.

from	to	Response
a port range	another port range	The frames are translated to any free port from the target range. With individual connection, they are normally translated to the first port in the target range. If there are connections at the same time, the round robin method is used to translate to a free port in the target range.
a single port	a port range	The frames are translated to any free port from the target range. With individual connection, they are normally translated to the first port in the target range. If there are connections at the same time, the round robin method is used to translate to a free port in the target range.

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 175)".

Source NAT

As in 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 177)".

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 179)".

See also

Connections (Page 208)

2.5.2 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

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.
	ppp2	Access from the IP subnet to the WAN interface of the device.
	Device	Access from the IP subnet to the device.
	SINEMA RC	Access from the IP subnet and the device to the SINEMA RC server.
	IPsec (all) IPsec <Connection Name> OpenVPN (all) OpenVPN <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>.

from	to	Meaning
Device	vlan x	Access from the device to the IP subnet.
	ppp2	Access from the device to the WAN interface of the device.
	SINEMA RC	Access from the device to the SINEMA RC server.
	IPsec (all) IPsec <Connection Name> OpenVPN (all) OpenVPN <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 the SINEMA RC server to the IP subnet.
	ppp2	Access from the IP subnet to the WAN interface of the device.
	Device	Access from the SINEMA RC server to the device.
	IPsec (all) IPsec <Connection Name> OpenVPN (all) OpenVPN <Connection Name>	Access from the SINEMA RC server to the VPN tunnel partners that can be reached via all VPN connections (all) or via a certain VPN connection <Connection Name>.
IPsec (all) IPsec <Connection Name> OpenVPN (all) OpenVPN <Connection Name>	vlan x	Access via VPN tunnel partners to the IP subnet.
	ppp2	Access from the IP subnet to the WAN interface of the device.
	Device	Access via VPN tunnel partners to the device.
	SINEMA RC	Access via VPN tunnel partners to the SINEMA RC server.
ppp0/usb	vlan x	Access from the mobile wireless interface to the IP subnet.
	Device	Access from the mobile wireless interface to the device.
	SINEMA RC	Access from the mobile wireless interface to the SINEMA RC server.
	IPsec (all) IPsec <Connection Name> OpenVPN (all) OpenVPN <Connection Name>	Access from the mobile wireless interface to the VPN tunnel partners that can be reached via all VPN connections (all) or via a certain VPN connection <Connection Name>.

2.5.3 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

Example of NAT translations

<table>
<tr><th colspan="8">NAT rule</th></tr>
<tr><th></th><th>Type</th><th>Source Interface</th><th>Destination Interface</th><th>Source IP Subnet</th><th>Translated Source IP Subnet</th><th>Destination IP Subnet</th><th>Translated Destination IP Subnet</th></tr>
<tr><td rowspan="2">①</td><td>Source</td><td>vlan1
(internal)</td><td>vlan2
(external)</td><td>192.168.1.0/24</td><td>10.100.1.0/24</td><td>10.10.10.0/24</td><td>-</td></tr>
<tr><td colspan="7">The rule applies to packets sent from vlan1 (internal) to vlan2 (external). With the packets that arrive at vlan1 there is a check to establish whether the rule applies.
If the source IP address in the subnet of the sender (Source IP Subnet) and the destination IP address in the subnet of the recipient (Destination IP Subnet), the source IP address is replaced by the suitable IP address from the "Translated Source IP Subnet". The subnet part of the source IP address is changed and the host part remains unchanged.
A packet, for example with the source IP address 192.168.1.102 is changed to 10.100.1.102. For the devices connected to vlan2 it appears as if the packets were sent from the IP subnet 10.100.1.0/24. This allows for example overlaps of IP subnets to be resolved. The rule is only specified for the send direction. The retranslation is performed implicitly. If the rule does not apply, the packets are forwarded without translation.</td></tr>
<tr><td rowspan="2">②</td><td>Destination</td><td>vlan2
(external)</td><td>vlan1
(internal)</td><td>10.10.10.0/24</td><td>-</td><td>10.100.1.0/24</td><td>192.168.1.0/24</td></tr>
<tr><td colspan="7">The rule applies to packets sent from vlan2 (external) to vlan1 (internal). With the packets that arrive at vlan2 there is a check to establish whether the rule applies.
If the source IP address in the subnet of the sender (Source IP Subnet) and the destination IP address are in the subnet of the recipient (Destination IP Subnet), the source IP address is replaced by the suitable IP address from the "Translated Destination IP Subnet".
A packet, for example with the source IP address 10.10.10.102 is changed to 192.168.1.102. The devices connected to vlan1 can communicate with the devices connected to vlan2. This assumes that the corresponding firewall rule is set.
The devices connected to vlan2 must address the devices connected to vlan1 with the virtual IP address from the subnet 10.100.1.0.</td></tr>
</table>

Firewall rules for the NAT rules ① and ②

Example 1:

These IP packet filter rules allow the IP data traffic for all devices for the specified direction.

NAT rule	IP packet filter rules						Description
	Action	From	To	Source (Range)	Destination (Range)	Service	
①	Accept	vlan1 (internal)	vlan2 (external)	192.168.1.0/24 (Source IP subnet)	10.10.10.0/24 (Destination IP subnet)	all	All packets sent from vlan1 (internal) to vlan2 (external) are allowed to pass. This IP packet filter rule applies to the devices connected to vlan1.
②	Accept	vlan2 (external)	vlan1 (internal)	192.168.1.0/24 (Translated destination IP subnet)	10.100.1.0/24 (Destination IP subnet)	all	All packets sent from vlan2 (external) to vlan1 (internal) are allowed to pass.

Example 2:

These IP packet filter rules restrict the IP data traffic to a specific device.

NAT rule	IP packet filter rules						Description
	Action	From	To	Source (Range)	Destination (Range)	Service	
①	Accept	vlan1 (internal)	vlan2 (external)	192.168.1.20/32 (Source IP subnet)	10.10.10.0/24 (Destination IP subnet)	all	Only packets sent to vlan2 (external) from the IP address 192.168.1.20 are allowed to pass.
②	Accept	vlan2 (external)	vlan1 (internal)	192.168.1.20/32 (Translated destination IP subnet)	10.100.1.0/24 (Destination IP subnet)	all	Only packets sent from vlan2 (external) to the IP address 192.168.1.20 are allowed to pass.

2.5.4 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 202)
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 202)
Partner certificate	Certificates with which the VPN gateway of the partner identifies itself with the device.	IPsec VPN (Page 202)

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.

2.5.5 VPN

The device supports the following VPN systems

- IPsec VPN
- OpenVPN

2.5.5.1 IPsec VPN

You configure the IPsec connections in "Security" > " IPsec VPN (Page 197)".

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 device can only operate as a VPN server. The device can only wait for VPN connections but cannot establish a VPN tunnel as the active partner. The address of the partner does not need to be known in this mode. This means that it is also possible to use dynamic IP addresses.

- **Standard mode**

  In standard mode, the address of the VPN gateway of the partner must be known so that the VPN connection can be established. 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 IP Authentication Header (**AH**) handles the authentication and identification of the source.
- 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	Authentication	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

Combination			Phase 1		Phase 2	
Encryption	**Authentication**	**Key Derivation**	**IKEv1**	**IKEv2**	**IKEv1**	**IKEv2**
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.

2.5.5.2 OpenVPN

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

You configure the OpenVPN client in "Security" > " OpenVPN Client (Page 208)".

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

The device supports the following:

- TUN device: Routing mode

  The LAN Interface and the virtual network interface are located in different IP subnets. The virtual tunnel interface is assigned a virtual IP address from a devised subnet by the OpenVPN server. The IP packets (layer 3) are routed between the virtual tunnel interface and the LAN interface.

Authentication method

- Certificates: CA certificate and device certificate

  The use of certificates is an asymmetrical cryptographic system. Each node (device) has a secret, private key and a public key of the partner. The private key allows the device to authenticate itself and to generate digital signatures.

- User name / password

  Access is restricted by a user name and a password.

Encryption methods

The device also supports the following methods:

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

2.5.5.3 VPN connection establishment

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

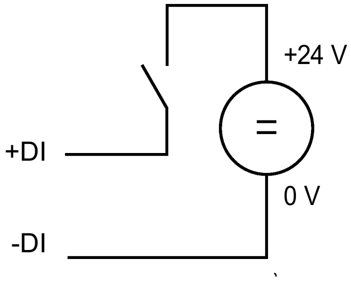
- OpenVPN: Security > OpenVPN > Connections (Page 208)
- IPsec VPN: Security > IPsec VPN > Connections (Page 200)
- SINEMA RC: System > SINEMA RC (Page 150)

Options	Use			Description
	OpenVPN	IPsec VPN	SINEMA RC [1)]	
start	x	x	-	The device is "active", in other words, it attempts to establish a connection to a partner. The partner is addressed using its configured WAN IP address or the configured FQDN.
wait	-	x	-	The device is "passive", in other words, it waits for the partner to initiate the connection.
on demand	-	x	-	The device attempts to establish a connection to a partner when necessary. The receipt of requests for VPN connection establishment is also possible. For the configured local and remote subnets, an entry is created in the routing table. If a node attempts to send data packets via the VPN tunnel from one of the networks, the VPN connection is established. The settable timeout has the effect that after this time without any further data packets the VPN tunnel is terminated again.
start on DI	x	x	-	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".
Permanet	-	-	x	The device establishes a VPN connection to the SINEMA RC Server. The VPN tunnel is established permanently

[1)] KEY-PLUG SINEMA REMOTE CONNECT required

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 In" 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 In" occurs, the device becomes "active". The device attempts to establish a VPN connection (OpenVPN, IPsec) to a partner.

- wait on DI

  If the event "Digital In" occurs, the device becomes "passive". The device waits for the partner to initiate the connection.

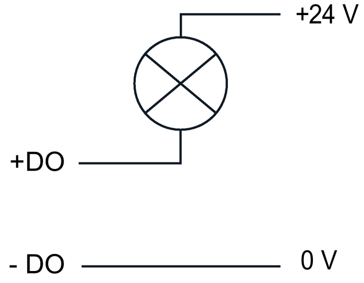
- Digital In

  The settings of the SINEMA RC server are ignored. If the event "Digital In" occurs, the device becomes "active". The device attempts to establish a VPN connection to the SINEMA RC server.

Notification options

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

Type of notification	Digital In	VPN tunnel	Behavior if there is a status change
E-mail	x	x	The device sends an e-mail. The e-mail contains the identification of the sending device, a description of the cause of the alarm in plain language, and a time stamp. Requirement: • An SMTP server is set up. • In "System > SMTP-Client" the function is activated, a recipient and the IP address of the SMTP server are configured.
Trap	x	x	The device sends an SNMP trap. Requirement: • In "System > Configuration", "SNMPv1 Traps" is activated. • 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 Table".
Syslog	x	x	The device writes an entry to the Syslog server. Requirement: • A Syslog server has been set up. • In "System > Syslogclient" the function is activated and the IP address of the Syslog server is configured.
Fault	x	-	The error LED lights up on the device.

Type of notification	Digital In	VPN tunnel	Behavior if there is a status change
Digital Out	x	x	Controls the digital output or signals the status change with the "DO" LED. A consumer can be connected to the digital output. You will find information on connecting in the operating instructions of the devices. The bulb signals a status change.  **Note** You can control the digital output directly via CLI or SNMP. In WBM and CLI, you can configure the use of the digital output in "Events". Do not control the digital output directly when you use this in the WBM and CLI.
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)

3 Security recommendation

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:

  Web page: (http://www.industry.siemens.com/topics/global/en/industrial-security/network-security/Pages/Default.aspx)
- When the internal and external network are disconnected, an attacker cannot access internal data from the outside. Therefore operate the device only within a protected network area.
- Operate the device only within a protected network area.
- Use VPN to encrypt and authenticate communication from and to the devices.
- For data transmission via a non-secure network use an encrypted VPN tunnel (IPsec, Open VPN).
- Separate connections correctly (WBM. Telnet, SSH etc.).

Physical access

- Limit physical access to the device to qualified personnel.
  The memory card or the PLUG (C-PLUG, KEY-PLUG) contains sensitive data such as certificates, keys etc. that can be read out and modified.
- Lock unused physical ports on the device. Unused ports can be used to gain forbidden access to the plant.

Software (security functions)

- Keep the software up to date. Check regularly for security updates of the product.
  You will find information on this on the Internet pages "Industrial Security (http://www.siemens.com/industrialsecurity)".
- Inform yourself regularly about security advisories and bulletins published by Siemens ProductCERT.
- Only activate protocols that you really require to use the device.
- The option of VLAN structuring provides good protection against DoS attacks and unauthorized access. Check whether this is practical or useful in your environment.
- Restrict access to the device by firewall, VPN (IPsec, OSINEMA RC) and NAT.
- 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.

See also

http://www.siemens.com/cert/de/cert-security-advisories.htm
(http://www.siemens.com/cert/en/cert-security-advisories.htm)

Passwords

- Define rules for the use of devices and assignment of passwords.
- Regularly update passwords and keys to increase security.
- Change all default passwords for users before you operate the device.
- Only use passwords with a high password strength. Avoid weak passwords for example password1, 123456789, abcdefgh.
- Make sure that all passwords are protected and inaccessible to unauthorized personnel.
- Do not use the same password for different users and systems or after it has expired.

Keys and certificates

This section deals with the security keys and certificates you require to set up SSL, VPN (IPsec, OpenVPN) and SINEMA RC.

- The device contains a pre-installed SSL 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 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:
  - Broadcast pings
  - Non authenticated and unencrypted interfaces
  - ICMP (redirect)
  - LLDP
  - Syslog
  - DHCP Options 66/67
  - TFTP
- The following protocols provide secure alternatives:
  - SNMPv1/v2 → SNMPv3

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

    If SNMP is enabled, change the community names. If no unrestricted access is necessary, restrict access with SNMP.
  - HTTP → HTTPS
  - Telnet → SSH

- Use secure protocols when access to the device is not prevented by physical protection measures.
- To prevent unauthorized access to the device or network, take suitable protective measures against non-secure protocols.
- If you require non-secure protocols and services, activate these at interfaces that are located within a protected network area.
- Using a firewall, restrict the services and protocols available to the outside to a minimum.
- For the DCP function, enable the "DCP read-only" mode after commissioning.

Available protocols per port

The following list provides you with an overview of the open ports on this device. Keep this in mind when configuring a firewall.

The table includes the following columns:

- **Protocol**

  All protocols that the device supports
- **Port number**

  Port number assigned to the protocol
- **Port status**
  - Open

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

    The port is open if it has been configured.
- **Factory setting**
  - Open

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

    The factory setting of the port is "Closed".
- **Authentication**

  Specifies whether or not the protocol is authenticated during access.

With some protocols the port can be open but access is prevented by a predefined IP package filter rule. You will find further information on the predefined IP package rules in "Security > Firewall > Predefined IPv4"

Protocol	Port number	Port status	Factory setting		Authentication
			Internal interface	External interface	
SSH	TCP/22	Open (when configured)	Open	Closed	Yes
HTTP	TCP/80	Open (when configured)	Open	Closed	Yes
HTTPS	TCP/443	Open	Open	Closed	Yes
SNTP	UDP/123	Open (only outgoing)	Closed	Closed	No
SNMP	UDP/161	Open (when configured)	Open	Closed	Yes
DNS	TCP/53	Open (when configured)	Open	Closed	No
	UDP/53	Open (when configured)	Open	Closed	No
Syslog	UDP/514	Open (only outgoing)	Closed	Closed	No
IPsec	UDP/500 UDP/4500	Open (when configured)	Closed	Open	Yes
DHCP	UDP/67 UDP/68	Open (when configured)	Open	Closed	No
NTP	UDP/123	Open (only outgoing)	Closed	Closed	Yes
Siemens Remote Service (cRSP/SRS)	TCP/443	Open (only outgoing)	Closed	Closed	Yes
PROFINET	UDP/34964	Open (when configured)	Closed	Closed	No
OpenVPN to SINEMA RC	TCP, any	Open (only outgoing)	Closed	Closed	Yes
TFTP	UDP/69	Open (only outgoing)	Closed	Closed	No
DynDNS	TCP/80	Open (only outgoing)	Closed	Closed	No
Telnet	TCP/23	Open (when configured)	Open	Closed	Yes
Ping	ICMP	Open	Open	Closed	No

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.

Note

Secure connection

WBM also allows you to establish a secure connection via HTTPS.

Use HTTPS for protected data transmission. If you want to access WBM only via a secure connection, under "System > Configuration" enable the option "HTTPS Server only".

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 16)".
- Access using HTTP or 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. Check whether "Automatically" is enabled for "Check for newer versions of stored pages".

- If a firewall is used, the relevant ports must be opened.
  - For access using HTTP: TCP port 80
  - 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 45 ESR
  - Google Chrome V50

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. If there is a connection to the device, the login page of Web Based Management (WBM) is displayed.

Logging in using the Internet browser

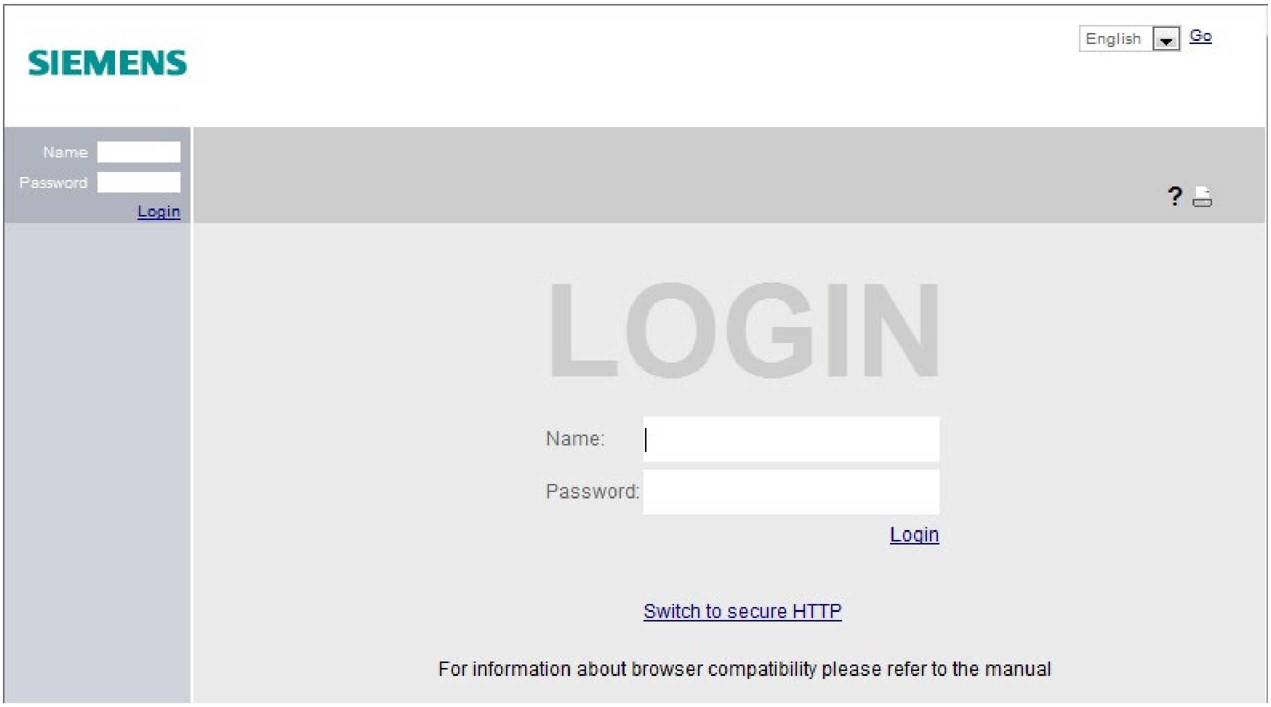
Selecting the language of the WBM

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.

Note

Available languages

in this version, only English is available. Other languages will follow in a later version.



For information about browser compatibility please refer to the manual

Logon with HTTP

There are two ways in which you can log on via HTTP. You either use the logon option in the center of the browser window or the logon option in the upper left area of the browser window.

1. Enter the user name "admin".
2. Enter the corresponding password.

   When you log on the first time or following a "Restore Factory Defaults and Restart", enter the default password "admin".
3. Click the "Login" button.
   When you log on for the first time or following a "Restore Factory Defaults and Restart", you will be prompted to change the password. The new password must meet the following password policies:
   - Password length: at least 8 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. Click the "Set Values" to complete the action and activate the new password.

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

Logon with HTTPS

Web Based Management also allows you to connect to the device over the secure connection of the HTTPS protocol. Follow these steps:

1. Click on the link "Switch to secure HTTP" on the logon page or enter "https://" and the IP address of the device in the address box of the Internet browser.
2. Confirm the displayed certificate warning.
   The logon page of Web Based Management appears.
3. Enter the user name "admin". Enter the corresponding password. When you log on the first time or following a "Restore Factory Defaults and Restart", enter the default password "admin".
4. Click the "Login" button or confirm your entry with "Enter".
   When you log on for the first time or following a "Restore Factory Defaults and Restart", you will be prompted to change the password. The new password must meet the following password policies:
   - Password length: at least 8 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. Click the "Set Values" to complete the action and activate the new password.

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

4.3 "Wizard" menu

4.3.1 Basic Wizard

Introduction

With the Basic Wizard, menus guide you through the configuration of the most important parameters. On the Basic Wizard pages, you can only configure the parameters important for the basic functionality. You make further settings when you have finished with the Basic Wizard.

Requirement

- The device has an IP address and can be reached via the Ethernet interface.
- You are logged on in the WBM as a user with administrator rights.
- When shipped or following a "Restore Factory Defaults and Restart" the device can be reached with the values preset in the factory. For more detailed information, refer to the section "Requirements for operation (Page 16)".

Starting the Basic Wizard

Click on "Wizard > Basic Wizard" in the navigation area to start the Basic Wizard.

If you log on the first time or log on after a "Restore Factory Defaults and Restart", the Basic wizard is always started automatically after you have changed the default password.

Buttons you require often

The WBM pages of the Basic Wizard contain the following buttons:

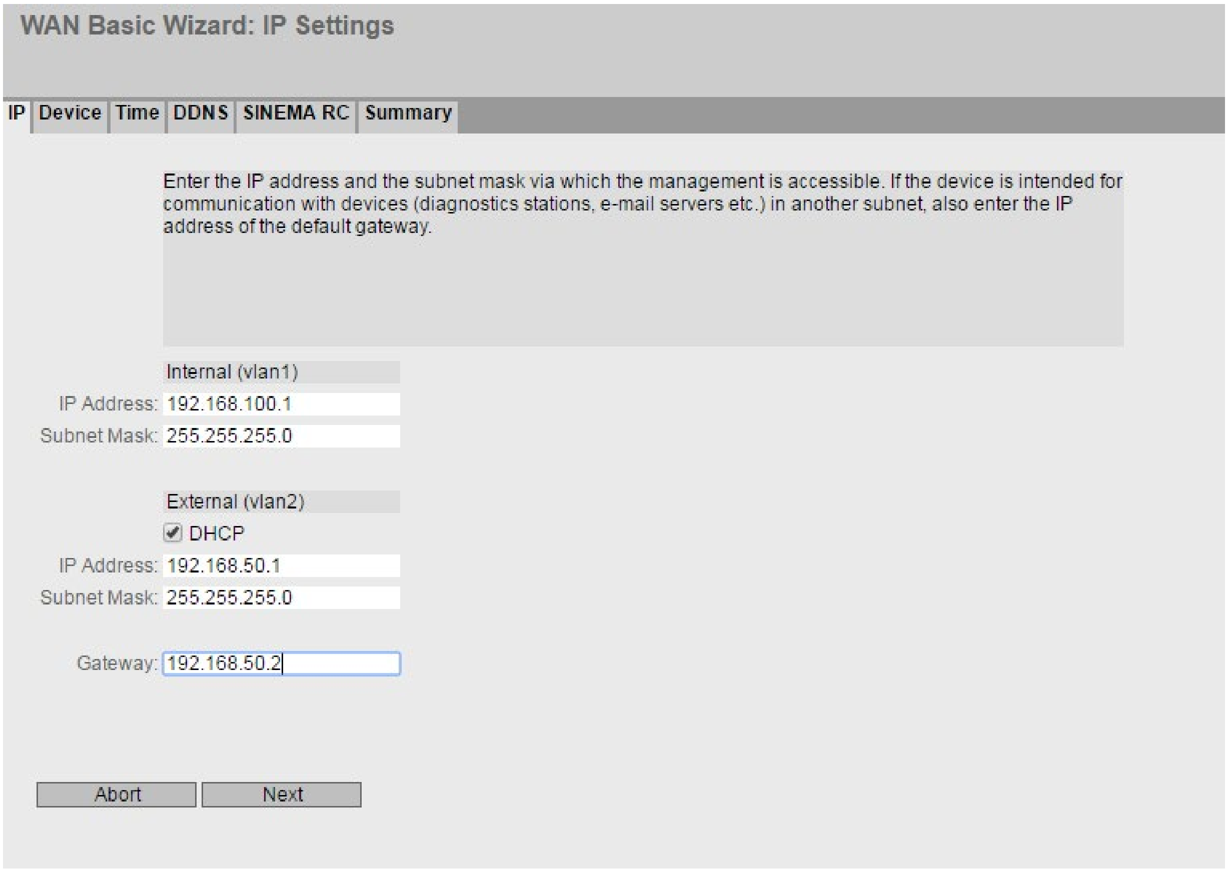
Button	Description
Next	Goes to the next page
Previous	Goes back to the previous page
Abort	The Basic Wizard is closed without adopting the settings.
Set Values	Saves the configuration and exits the Basic Wizard.

Navigation within the pages of the Basic Wizard is possible only with the "Previous" and "Next" buttons.

4.3.2 IP Settings

Introduction

One of the basic steps in configuration of a device is setting the IPv4 address. The IP address identifies a device in the network uniquely.



Enter the IP address and the subnet mask via which the management is accessible. If the device is intended for communication with devices (diagnostics stations, e-mail servers etc.) in another subnet, also enter the IP address of the default gateway.

Internal (vlan1)

IP Address: 192.168.100.1

Subnet Mask: 255.255.255.0

External (vlan2)

☑ DHCP

IP Address: 192.168.50.1

Subnet Mask: 255.255.255.0

Gateway: 192.168.50.2

Description

The Basic Wizard page contains the following boxes:

- **Internal (vlan 1)**

  In this area make the settings for connection to the LAN.

  – **IP Address**

    Enter the IPv4 address of the interface that is unique within your network.

  – **Subnet Mask**

    Enter the subnet mask of the subnet you are creating.

- **External (vlan 2)**

  In this area make the settings for connection to the WAN.

  – **DHCP**

    When enabled the interface receives the IPv4 address from a DHCP server.

  – **IP Address**

    Enter the IPv4 address of the interface.

  – **Subnet Mask**

    Enter the subnet mask of the subnet you are creating. Subnets on different interfaces must not overlap.

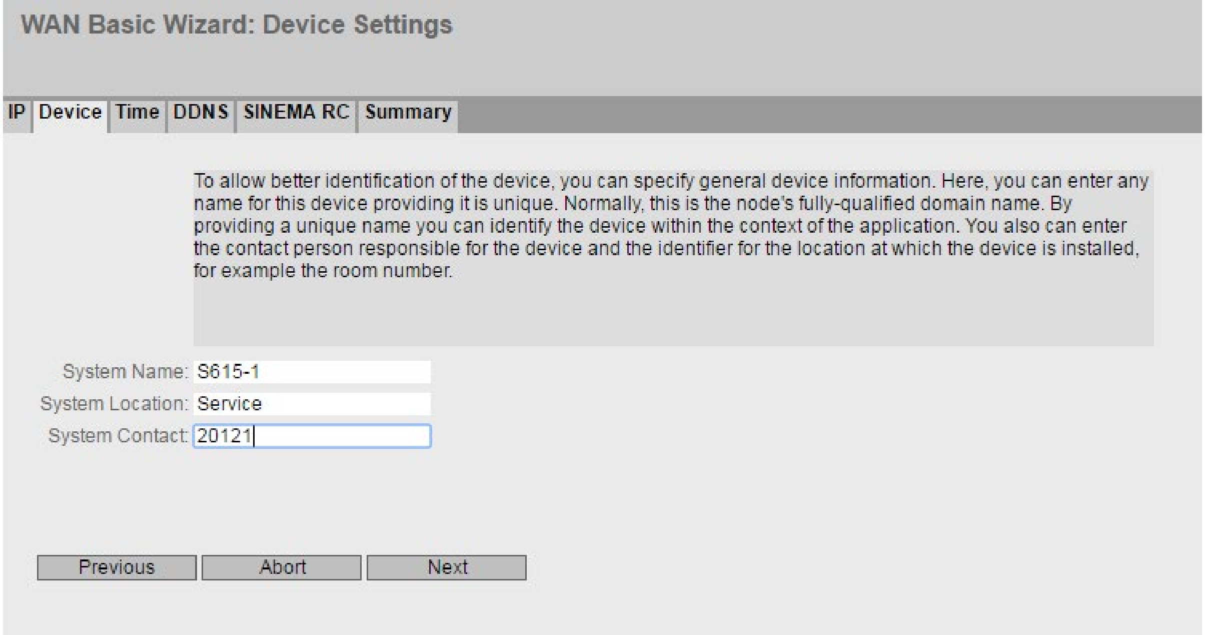
  – **Gateway**

    Enter the IP address of the default gateway to be able to communicate with devices in another subnet.

4.3.3 Device Settings

Introduction

On this Basic Wizard page, you configure the general device information.



WAN Basic Wizard: Device Settings

To allow better identification of the device, you can specify general device information. Here, you can enter any name for this device providing it is unique. Normally, this is the node's fully-qualified domain name. By providing a unique name you can identify the device within the context of the application. You also can enter the contact person responsible for the device and the identifier for the location at which the device is installed, for example the room number.

System Name: S615-1
System Location: Service
System Contact: 20121

Description

The Basic Wizard page contains the following boxes:

- **System Name**
  You can enter the name of the device. If you configure this box, this configuration is adopted and 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 Location**
  You can enter the location where the device is installed. The location is displayed in the selection area. A maximum of 255 characters are possible.

  Note

  Permitted characters

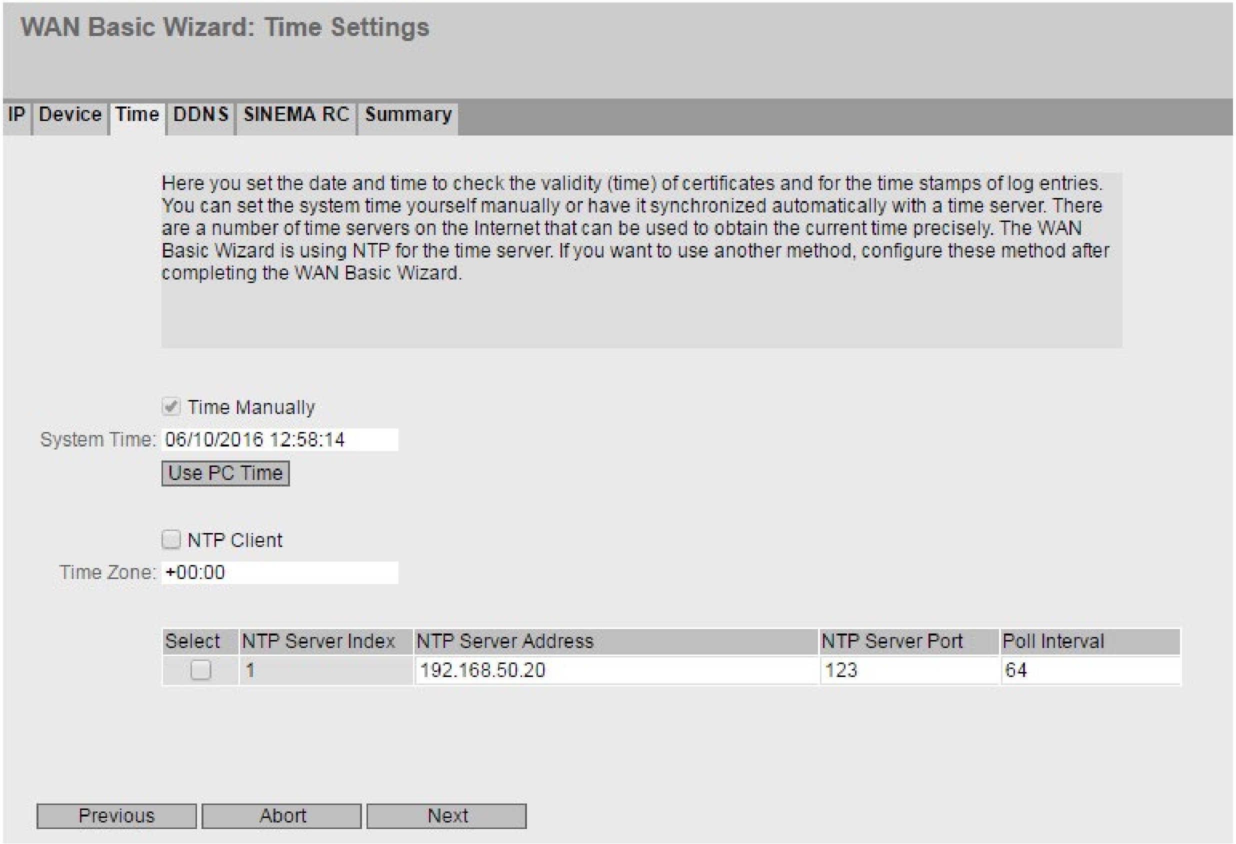
  The following printable ASCII characters (0x20 to 0x7) are permitted in the input fields:

  - 0123456789
  - A...Z a...z
  - !"#$%&'()*+,-./:;<=>?@ [\]_{|}~¦^`
- **System Contact**
  You can enter a contact person responsible for managing the device. A maximum of 255 characters are possible.

4.3.4 Time

Time setting

On this Basic Wizard page, you set the date and time of the system.



WAN Basic Wizard: Time Settings

Here you set the date and time to check the validity (time) of certificates and for the time stamps of log entries. You can set the system time yourself manually or have it synchronized automatically with a time server. There are a number of time servers on the Internet that can be used to obtain the current time precisely. The WAN Basic Wizard is using NTP for the time server. If you want to use another method, configure these method after completing the WAN Basic Wizard.

☑ Time Manually

System Time: 06/10/2016 12:58:14

□ NTP Client

Time Zone: +00:00

Select	NTP Server Index	NTP Server Address	NTP Server Port	Poll Interval
□	1	192.168.50.20	123	64

Description

Manual time setting:

- **Time Manually**

  Enable or disable manual setting of the time. If you enable the option, the "System Time" input box can be edited.

- **System Time**

  Enter the date and time in the format "MM/DD/YYYY HH:MM:SS".

  After a restart, the time of day begins at 01/01/2000 00:00:00

- **Use PC Time**

  Click the button to use the time setting of the PC.

Automatic time-of-day setting with NTP

- **NTP Client**

  Enable or disable time synchronization using NTP.

- **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. Settings for daylight-saving and standard time are taken into account in this box by specifying the time offset.

In the table, configure the NTP server

- **NTP Server Index**

  Number corresponding to a specific NTP server entry.

- **NTP Server Address**

  Enter the address of the NTP server.

- **NTP Server Port**

  Enter the port of the NTP server.
  The following ports are possible:

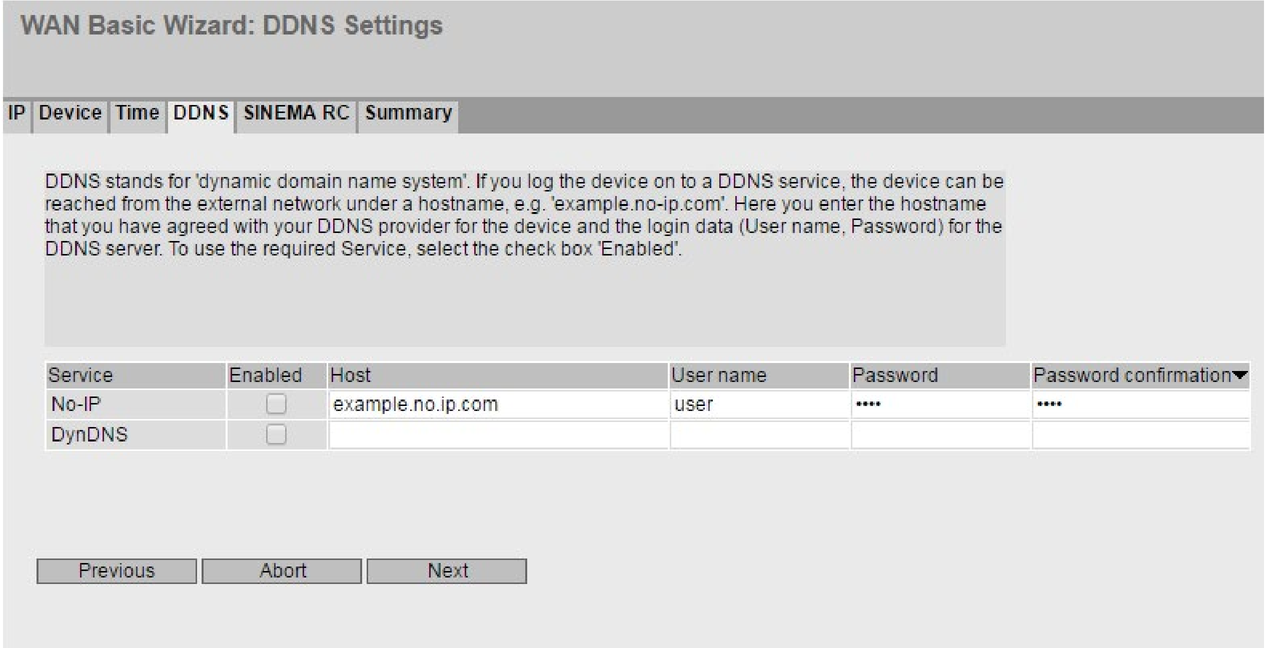
  - 123 (standard port)
  - 1025 to 36564

- **Poll Interval**

  Here, enter the interval between two-time queries. In this box, you enter the query interval in seconds. Possible values are 64 to 1024 seconds

4.3.5 DDNS

On this Basic Wizard page, you configure the dynamic DNS client (DDNS client). 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.



WAN Basic Wizard: DDNS Settings

DDNS stands for 'dynamic domain name system'. If you log the device on to a DDNS service, the device can be reached from the external network under a hostname, e.g. 'example.no-ip.com'. Here you enter the hostname that you have agreed with your DDNS provider for the device and the login data (User name, Password) for the DDNS server. To use the required Service, select the check box 'Enabled'.

Service	Enabled	Host	User name	Password	Password confirmation
No-IP	□	example.no.ip.com	user	••••	••••
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 hostname 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**

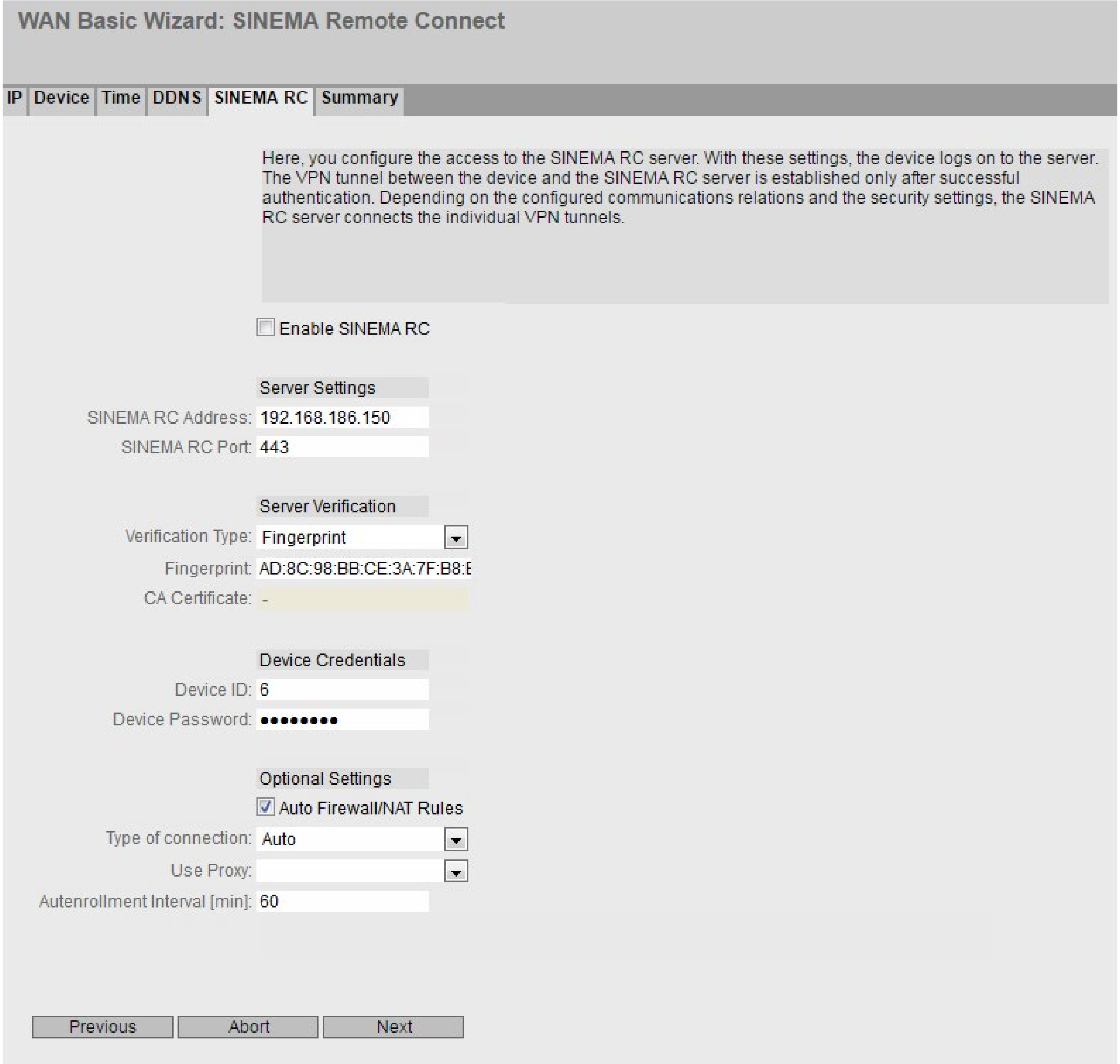
  Confirm the password.

4.3.6 SINEMA RC

On this Basic Wizard page, you configure the access to the SINEMA RC server.

Note

This function can only be used with a KEY PLUG (Page 20).



WAN Basic Wizard: SINEMA Remote Connect

Here, you configure the access to the SINEMA RC server. With these settings, the device logs on to the server. The VPN tunnel between the device and the SINEMA RC server is established only after successful authentication. Depending on the configured communications relations and the security settings, the SINEMA RC server connects the individual VPN tunnels.

□ Enable SINEMA RC

Server Settings

SINEMA RC Address: 192.168.186.150
SINEMA RC Port: 443

Server Verification

Verification Type: Fingerprint
Fingerprint: AD:8C:98:BB:CE:3A:7F:B8:E
CA Certificate: -

Device Credentials

Device ID: 6
Device Password: ●●●●●●●●●

Optional Settings

☑ Auto Firewall/NAT Rules
Type of connection: Auto
Use Proxy:
Autenrollment Interval [min]: 60

Description

The Basic Wizard page contains the following boxes:

- **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.

Range "Server Settings"

- **SINEMA RC Address**

  Enter the IPv4 address or the DNS host name of the SINEMA RC Server.
- **SINEMA RC Port**

  Enter the port via which the SINEMA RC Server can be reached.

Range "Server Verification"

- **Verifcation 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 "Fingerprint" setting. 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 “CA Certificate" setting. Select the CA certificate of the server used to sign the server certificate. Only loaded CA certificates can be selected.

Range "Device Credentials"

- **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.

Range "Optional Settings"

- **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 In

    The settings of the SINEMA RC server are ignored. If the "Digital In" event occurs, the device attempts to establish a VPN connection to the SINEMA RC Server. This is on condition that the event "Digital In" is passed onto the VPN connection. To do this, in "System > Events > Configuration" for the event "Digital In" activate "VPN Tunnel".
- **Use Proxy**

  Specify whether a 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".
- **Autenrollment Intervall [min]**

  Specify the period of time in minutes after which queries are sent to the SINEMA RC server.. With these queries, the device checks whether there is a newer firmware file on the SINEMA RC server.

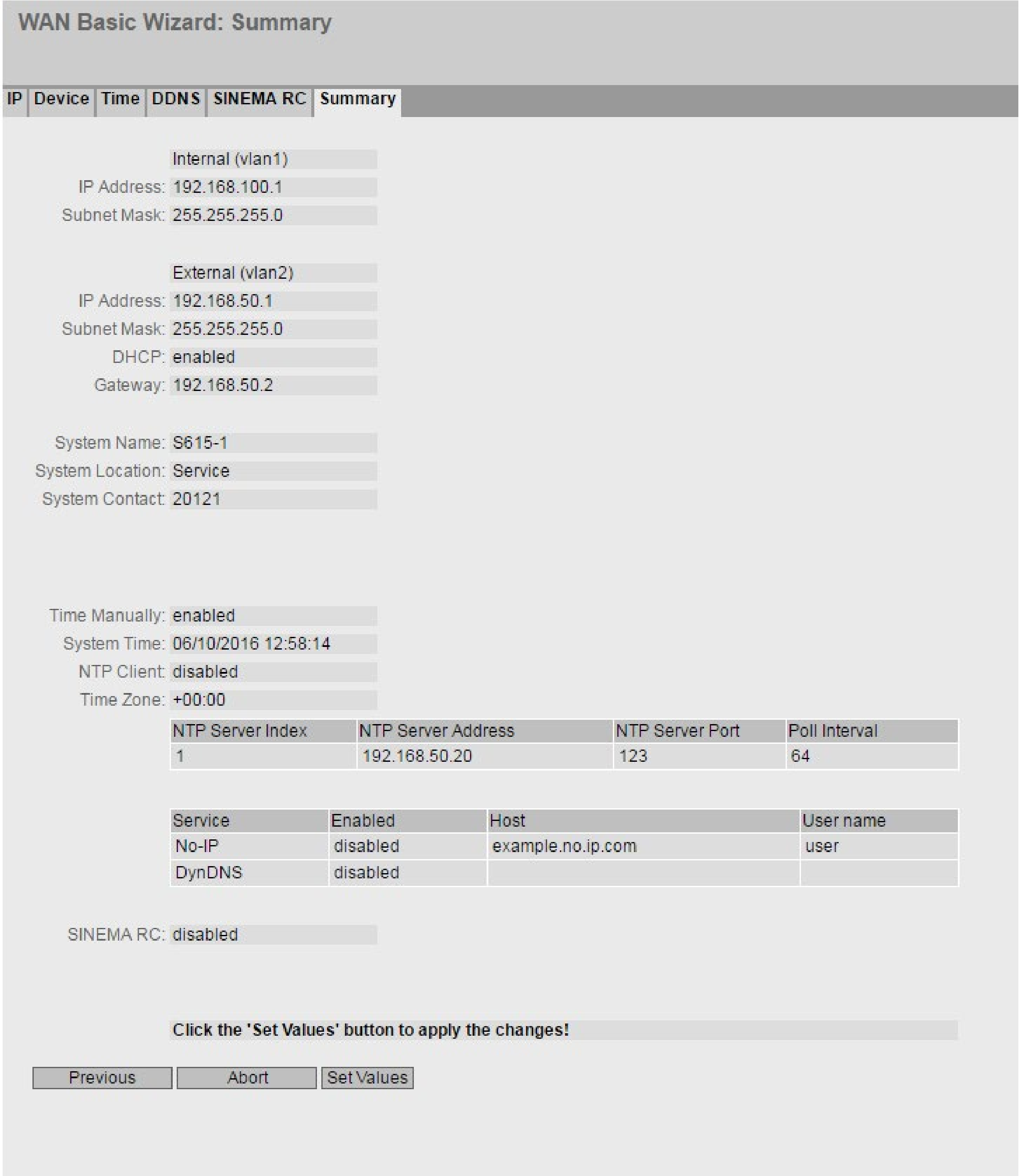
  If you enter the value 0, this function is disabled.

4.3.7 Summary

Introduction

The settings are summarized on this page. The content of the page depends on the set parameters and the device.

Check the settings before you exit the Basic Wizard with the "Set Values" button. If settings are incorrect, go back using the "Previous" button and change the settings to the required ones.



WAN Basic Wizard: Summary

	Internal (vlan1)
IP Address:	192.168.100.1
Subnet Mask:	255.255.255.0
	External (vlan2)
IP Address:	192.168.50.1
Subnet Mask:	255.255.255.0
DHCP:	enabled
Gateway:	192.168.50.2
System Name:	S615-1
System Location:	Service
System Contact:	20121
Time Manually:	enabled
System Time:	06/10/2016 12:58:14
NTP Client:	disabled
Time Zone:	+00:00

NTP Server Index	NTP Server Address	NTP Server Port	Poll Interval
1	192.168.50.20	123	64

Service	Enabled	Host	User name
No-IP	disabled	example.no.ip.com	user
DynDNS	disabled		

SINEMA RC: disabled

Click the 'Set Values' button to apply the changes!

Set Values

Click the "Set Values" button to exit the Basic Wizard. The settings are adopted.

4.4 "Information" menu

4.4.1 Start page

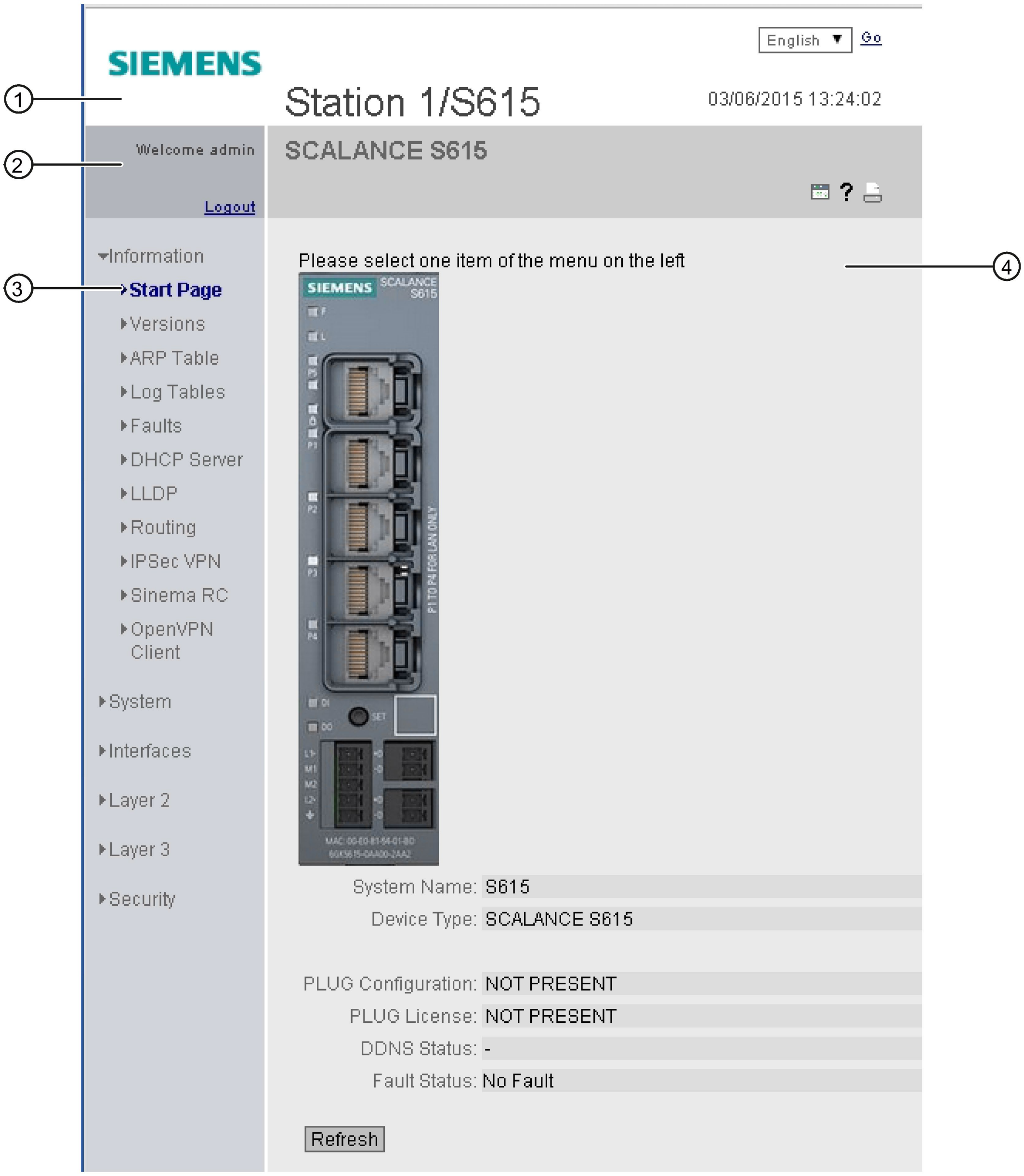
View of the Start page

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:	S615
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
- Display of: "System Location/System Name".
  - "System Location" contains the location of the device.
    With the settings when the device ships, the IP address of the Ethernet interface is displayed.
  - "System Name" is the device name.

You can change the content of this display with "System" > "General" > "Device".

- Drop-down list for language selection
- System time and date

  You can change the content of this display in "System" > "System Time".

Display area (2)

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

- **Printer** 🖨
  When you click this button, a pop-up window opens with a view of the page content optimized for the printer.
- **Help** ?
  When you click this button, the help page of the currently selected menu item is opened in a new browser window.
- **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.
- **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:

- System Name: System name of the device
- Device Type: The type of the device

- 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 hostname 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" login.

  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"**
  The number of data records that can be displayed on a WBM page is limited. Click the "Next" button to page down through the data records.
- **Page up with "Prev"**
  The number of data records that can be displayed on a page is limited. Click the "Prev" button to page up through the data records.

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 %u seconds.Press 'Write Startup Config' to save immediately'."

Note

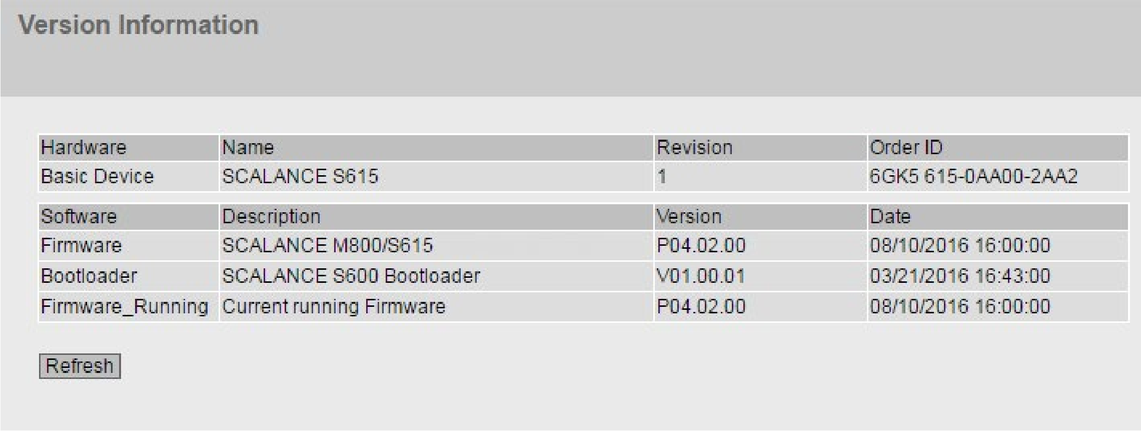
Interrupting the save

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.

4.4.2 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	P04.02.00	08/10/2016 16:00:00
Bootloader	SCALANCE S600 Bootloader	V01.00.01	03/21/2016 16:43:00
Firmware_Running	Current running Firmware	P04.02.00	08/10/2016 16:00:00

Description

Table 1 has the following columns:

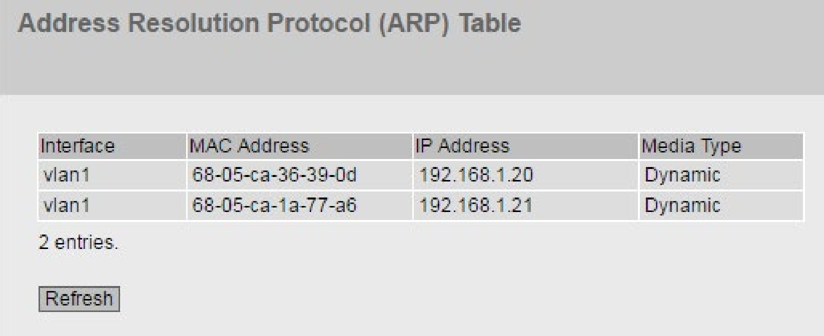
- **Hardware**
  - Basic Device
    Shows the basic device
- **Name**
  Shows the name of the device.
- **Revision**
  Shows the hardware version of the device.
- **Order ID**
  Shows the order number of the device.
- **Software**
  - Firmware
    Shows the current firmware version. If a new firmware file was loaded and the device has not yet restarted, the firmware version of the loaded firmware file is displayed. 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.
- **Date**
  Shows the date the software was created.

4.4.3 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	192.168.1.20	Dynamic
vlan1	68-05-ca-1a-77-a6	192.168.1.21	Dynamic

2 entries.

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 known device.
- **IP address**
  Shows the IP address of the known device.
- **Media Type**
  Shows the type of connection.
  - Dynamic
    The device recognized the address data automatically.
  - Static

    The addresses were entered as static addresses.

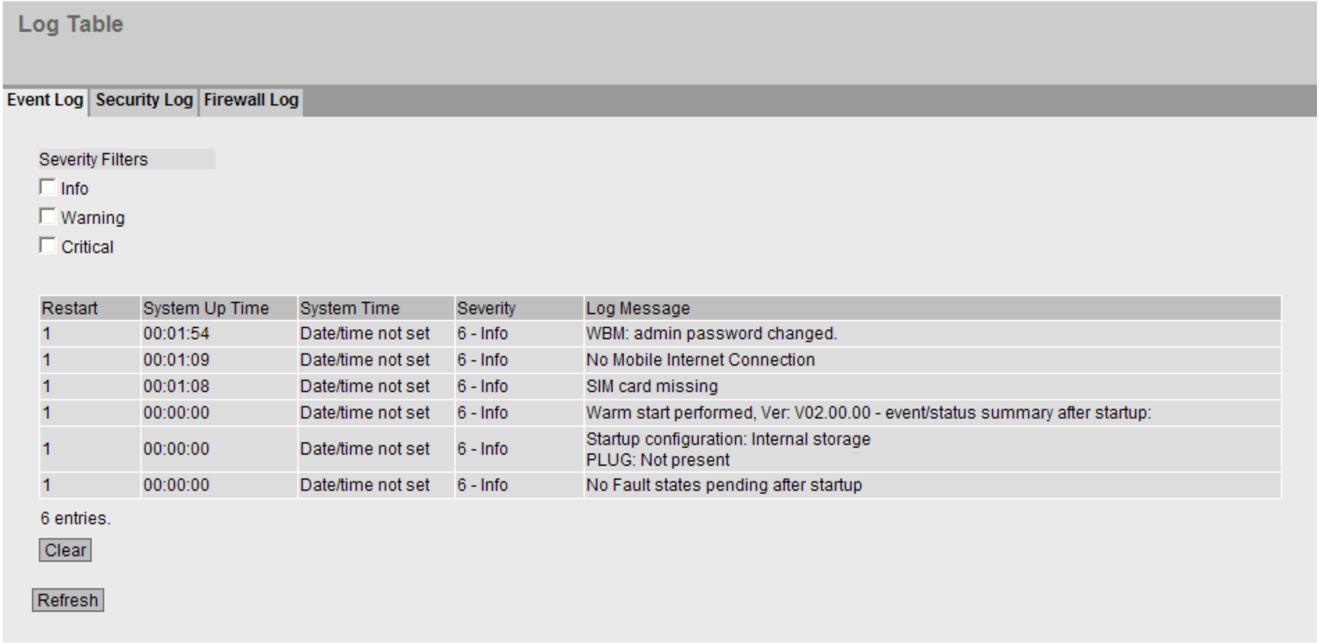
4.4.4 Log tables

4.4.4.1 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 on TFTP.



Severity Filters

□ Info

□ Warning

□ Critical

Restart	System Up Time	System Time	Severity	Log Message
1	00:01:54	Date/time not set	6 - Info	WBM: admin password changed.
1	00:01:09	Date/time not set	6 - Info	No Mobile Internet Connection
1	00:01:08	Date/time not set	6 - Info	SIM card missing
1	00:00:00	Date/time not set	6 - Info	Warm start performed, Ver: V02.00.00 - event/status summary after startup:
1	00:00:00	Date/time not set	6 - Info	Startup configuration: Internal storage PLUG: Not present
1	00:00:00	Date/time not set	6 - Info	No Fault states pending after startup

6 entries.

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**
  Shows the system time of the device. If no system time is set, the box displays "Date/time not set".
- **Severity**
  Shows the severity of the event.
- **Log Message**
  Displays a brief description of the event that has occurred.

Description of the button

"Clear" button

Click this button to delete the content of the log file. All entries are deleted regardless of what you have selected under "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 400 per degree of severity. When this number is reached, the oldest entries are overwritten. 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

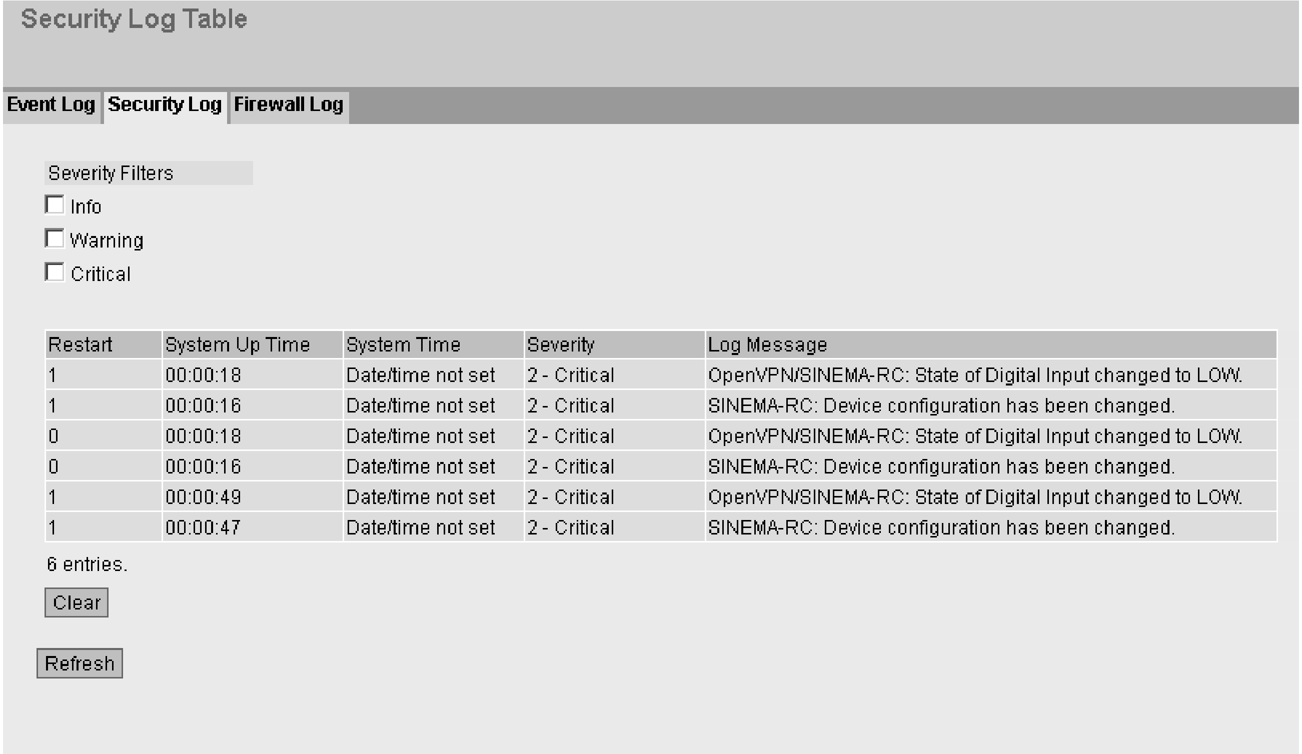
From the drop-down list, select the page you want to go to.

"Refresh" button

Refreshes the display of the values in the table.

4.4.4.2 Security log

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



Security Log Table

Severity Filters

□ Info
□ Warning
□ Critical

Restart	System Up Time	System Time	Severity	Log Message
1	00:00:18	Date/time not set	2 - Critical	OpenVPN/SINEMA-RC: State of Digital Input changed to LOW.
1	00:00:16	Date/time not set	2 - Critical	SINEMA-RC: Device configuration has been changed.
0	00:00:18	Date/time not set	2 - Critical	OpenVPN/SINEMA-RC: State of Digital Input changed to LOW.
0	00:00:16	Date/time not set	2 - Critical	SINEMA-RC: Device configuration has been changed.
1	00:00:49	Date/time not set	2 - Critical	OpenVPN/SINEMA-RC: State of Digital Input changed to LOW.
1	00:00:47	Date/time not set	2 - Critical	SINEMA-RC: Device configuration has been changed.

6 entries.

Description

- **Severity Filters**
  You can filter the entries in the table according to severity. To display all messages, 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 message occurred.
- **System Up Time**
  Shows the time the device has been running since the last restart when the event occurred.
- **System time**
  Shows the system time of the device. If no system time is set, the box displays "Date/time not set".
- **Severity**
  Shows the severity of the event.
- **Log Message**
  Displays a brief description of the event that has occurred.
  If the system time is set, the time is also displayed at which the event occurred.

Description of the button

"Clear" button

Click this button to delete the content of the log file. All entries are deleted regardless of what you have selected under "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 400 per degree of severity. When this number is reached, the oldest entries are overwritten. 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

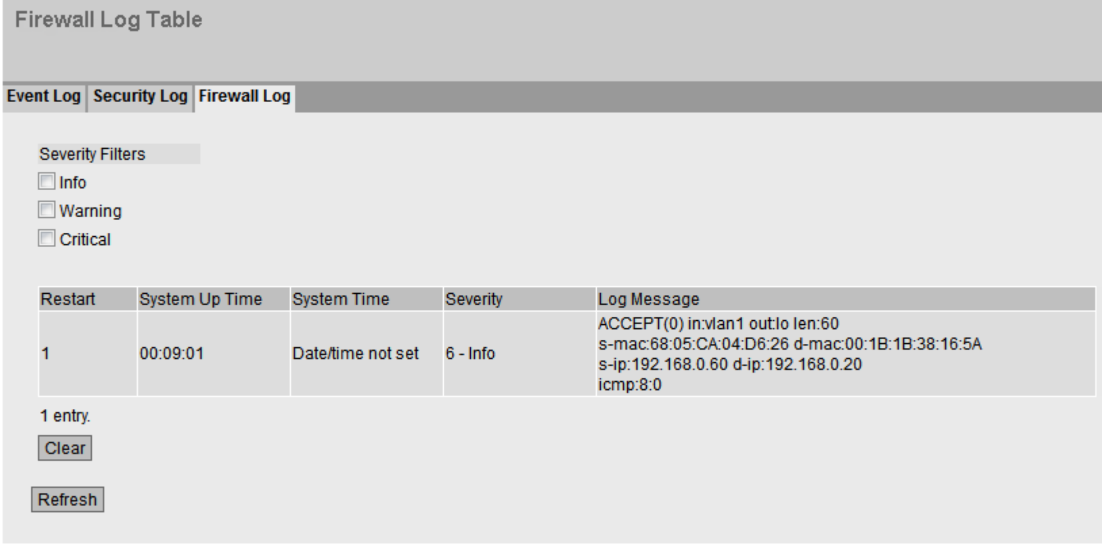
From the drop-down list, select the page you want to go to.

"Refresh" button

Refreshes the display of the values in the table.

4.4.4.3 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**
  Shows the system time of the device. If no system time is set, the box displays "Date/time not set".
- **Severity**
  Shows the severity of the event.
- **Log Message**
  Displays a brief description of the event that has occurred.

Description of the button

"Clear" button

Click this button to delete the content of the log file. All entries are deleted regardless of what you have selected under "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 400 per degree of severity. When this number is reached, the oldest entries are overwritten. 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.

"Refresh" button

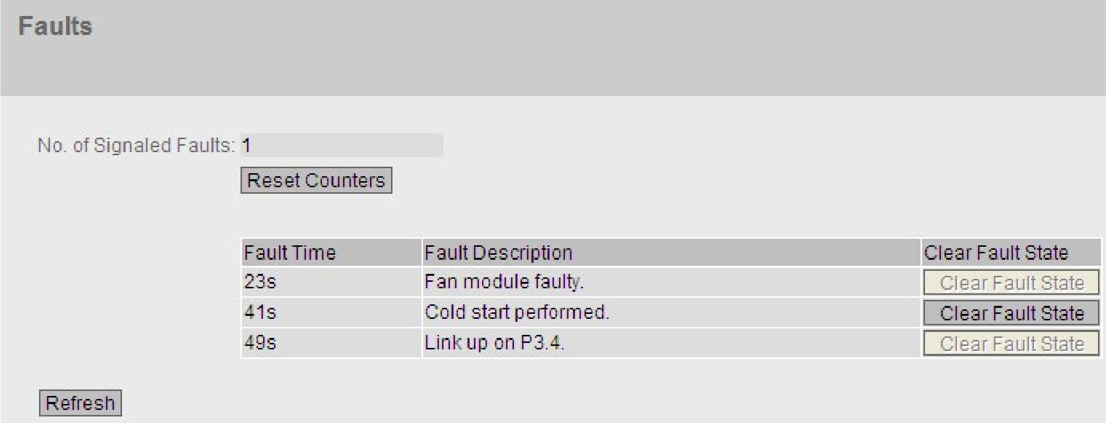
Refreshes the display of the values in the table.

4.4.5 Faults

Error status

This page shows errors that occur that are configured in "Events" and "Fault Monitoring". Errors of the "Cold/Warm Start" event can be deleted following confirmation.
If there are no more unanswered error/fault messages, the fault LED goes off.

The time calculation always begins after the last system start. When the system is restarted, a new entry with the type of restart is created in the fault memory.



Faults

No. of Signaled Faults: 1

Fault Time	Fault Description	Clear Fault State
23s	Fan module faulty.	Clear Fault State
41s	Cold start performed.	Clear Fault State
49s	Link up on P3.4.	Clear Fault State

Description

The page contains the following boxes:

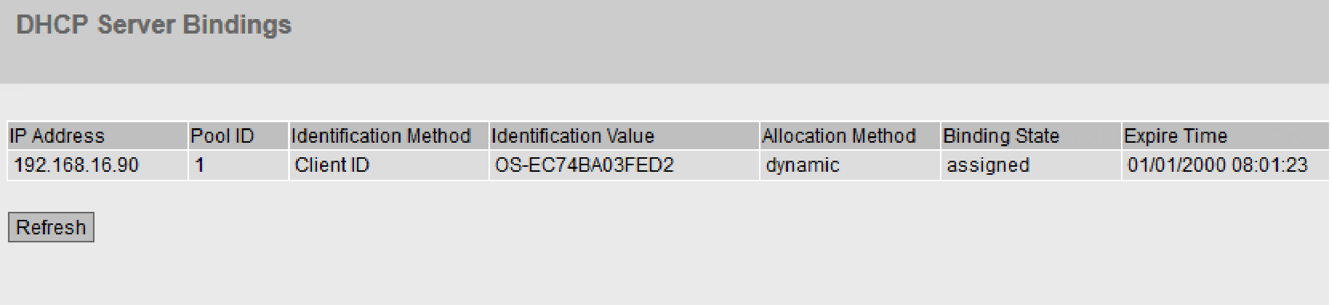
- **No. of Signaled Faults**
  Indicates how often the fault LED lit up and not how many faults occurred.
- **Reset Counters**
  The number is reset with this button.

The table contains the following columns:

- **Fault Time**
  Shows the time the device has been running since the last restart when the described fault occurred.
- **Fault Description**
  Displays a brief description of the error/fault that has occurred.
- **Clear Fault State**
  To delete errors of the "Cold/Warm Start" event, click the "Clear Fault State" button.

4.4.6 DHCP Server

This page shows whether 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 08:01:23

Description

- **IP Address**
  Shows the IPv4 address assigned to the device.
- **Pool ID**
  Shows the number of the IPv4 address band.
- **Identification Method**
  Select the method according to which a client is identified.
- **Identification Value**

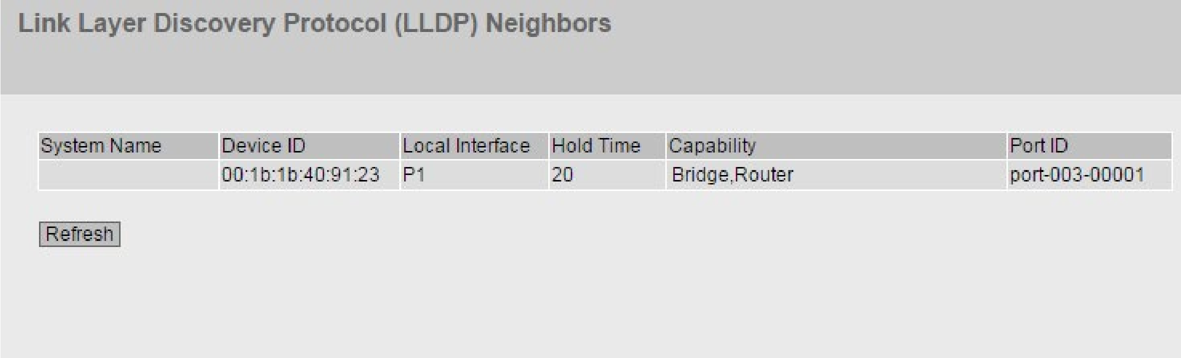
  Shows the MAC address or he client ID of the DHCP client.
- **Allocation Method**
  Show whether the IPv4 address was assigned statically or dynamically. You configure the static entries in "System > DHCP > Static Leases".
- **Binding State**
  Shows the status of the assignment.
  - assigned
    The assignment is used.
  - not assigned
    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.

4.4.7 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".



Link Layer Discovery Protocol (LLDP) Neighbors

System Name	Device ID	Local Interface	Hold Time	Capability	Port ID
	00:1b:1b:40:91:23	P1	20	Bridge,Router	port-003-00001

Figure 4-1 Information LLDP

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 in the MIB for the time specified here. If the IE switch 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

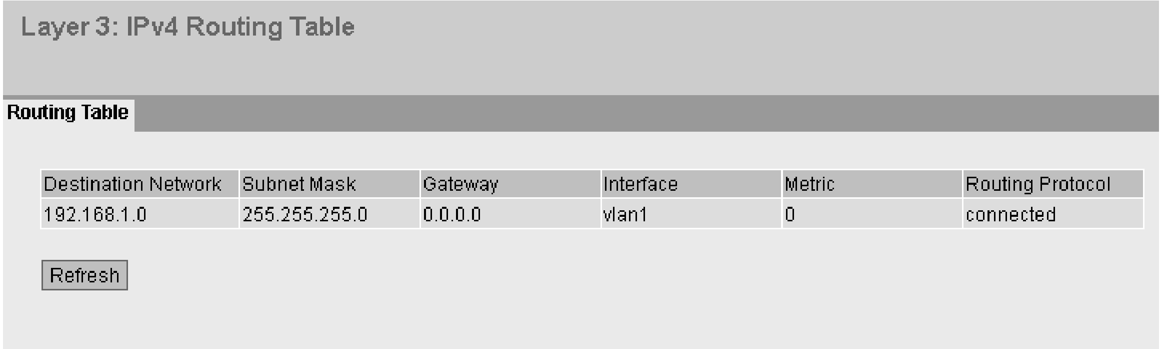
- **Port ID**

  Port of the device with which the IE switch is connected.

4.4.8 Routing table

Introduction

This page shows the routing table of the device.



Layer 3: IPv4 Routing Table

Routing Table

Destination Network	Subnet Mask	Gateway	Interface	Metric	Routing Protocol
192.168.1.0	255.255.255.0	0.0.0.0	vlan1	0	connected

Description

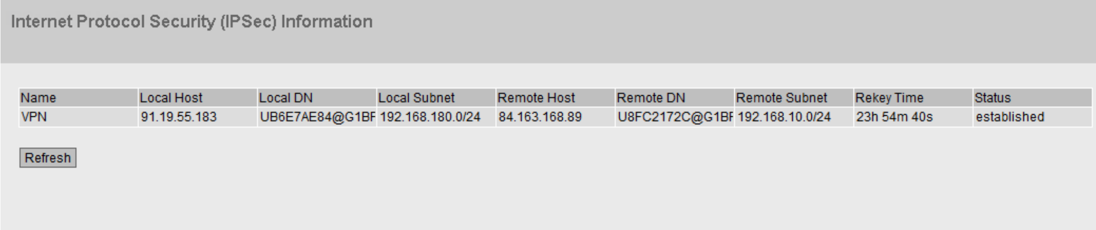
The table has the following columns:

- **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 the 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

4.4.9 IPsec VPN

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



Internet Protocol Security (IPSec) Information

Name	Local Host	Local DN	Local Subnet	Remote Host	Remote DN	Remote Subnet	Rekey Time	Status
VPN	91.19.55.183	UB6E7AE84@G1BF	192.168.180.0/24	84.163.168.89	U8FC2172C@G1BF	192.168.10.0/24	23h 54m 40s	established

Description

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 hostname of the remote device.

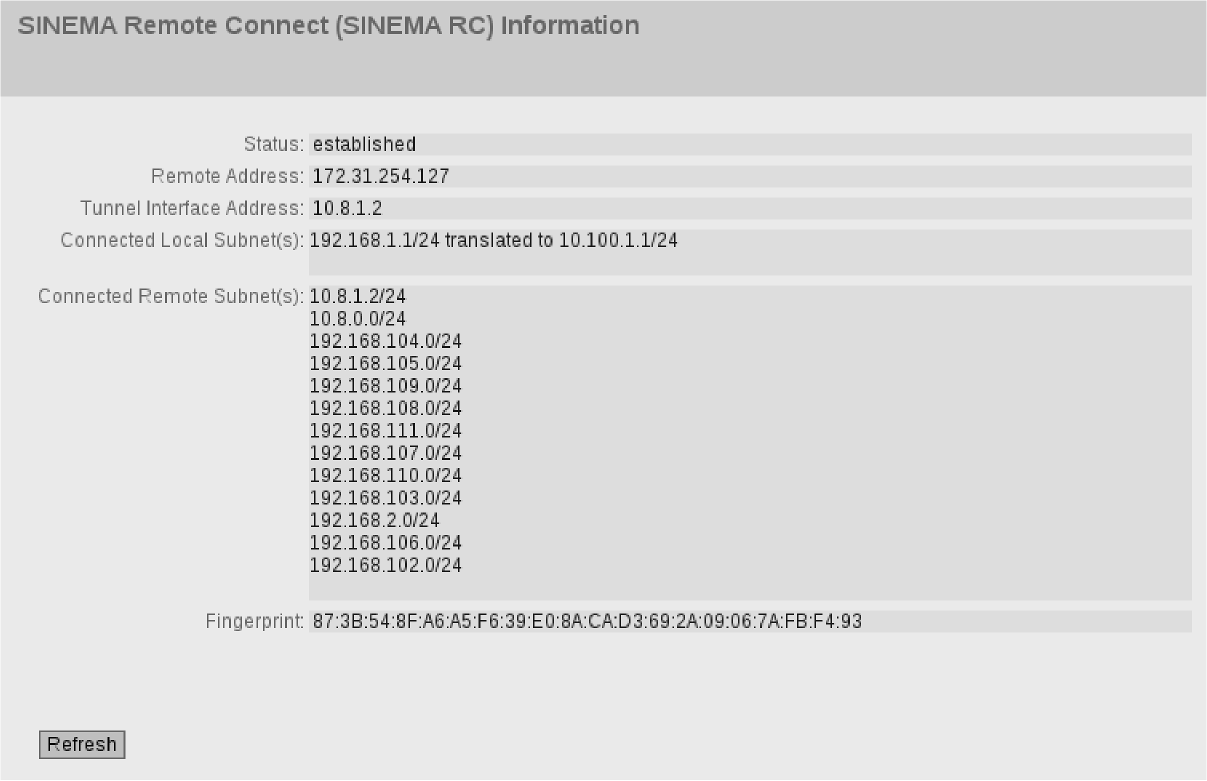
- **Remote DN**
  Shows the Distinguished Name (DN) signaled by the remote device during connection establishment.
- **Remote Subnet**
  Shows the remote subnet.
- **Rekey Time**
  Shows when the validity of the key elapses.
- **Status**
  Shows the status of the VPN connection.

4.4.10 SINEMA RC

Shows information on SINEMA RC Server.

Note

This function can only be used with a KEY PLUG.



SINEMA Remote Connect (SINEMA RC) Information

Status: established
Remote Address: 172.31.254.127
Tunnel Interface Address: 10.8.1.2
Connected Local Subnet(s): 192.168.1.1/24 translated to 10.100.1.1/24
Connected Remote Subnet(s): 10.8.1.2/24
10.8.0.0/24
192.168.104.0/24
192.168.105.0/24
192.168.109.0/24
192.168.108.0/24
192.168.111.0/24
192.168.107.0/24
192.168.110.0/24
192.168.103.0/24
192.168.2.0/24
192.168.106.0/24
192.168.102.0/24
Fingerprint: 87:3B:54:8F:A6:A5:F6:39:E0:8A:CA:D3:69:2A:09:06:7A:FB:F4:93

Description

- **Status**

  Shows the status of the SINEMA RC Server connection.
- **Remote Address**

  Shows the IP address of the SINEMA RC Server.
- **Tunnel Interface Address**

  Shows the IP address of the virtual tunnel interface.
- **Connected Local Subnet(s)**

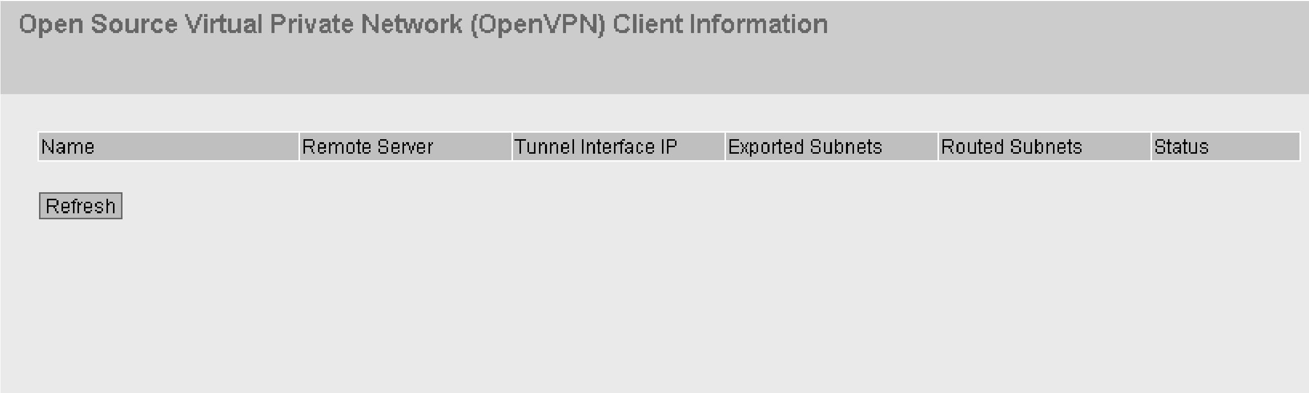
  Shows the IP addresses of the local subnets. Is only displayed when the option "Connected local subnets" is enabled on the SINEMA RC Server. You will find further information on this in the Operating Instructions of the SINEMA RC Server.
- **Connected Remote Subnet(s)**

  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.
- **Fingerprint**

  Displays the fingerprint of the server certificate. Is only displayed when the fingerprint is used for verification.

4.4.11 OpenVPN client

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



Open Source Virtual Private Network (OpenVPN) Client Information

Name	Remote Server	Tunnel Interface IP	Exported Subnets	Routed Subnets	Status

Description

This table contains the following columns:

- **Name**

  Shows the name of the OpenVPN connection.
- **Remote Server**

  Shows the IP address or the hostname of the OpenVPN server.
- **Tunnel Interface IP**

  Shows the IP address of the virtual tunnel interface.
- **Exported Subnets**

  Shows the IP address of the local subnets.
- **Routed Subnets**

  Shows the subnets of the OpenVPN server.
- **Status**

  Shows the status of the OpenVPN connection.

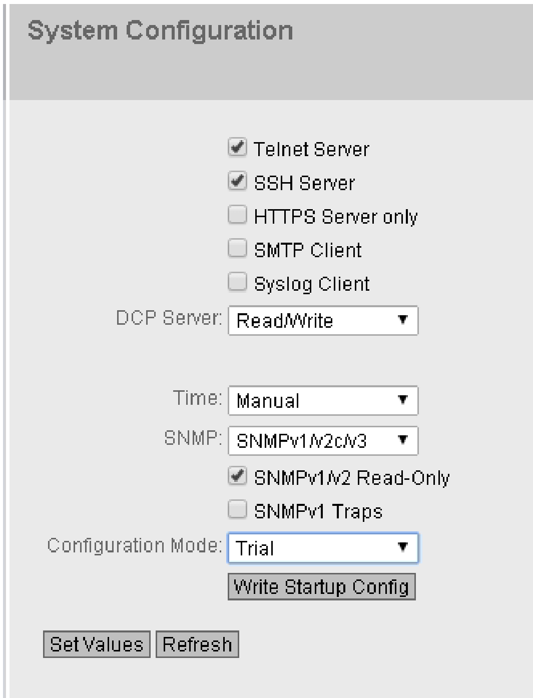
4.5 "System" menu

4.5.1 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
□ HTTPS Server only
□ SMTP Client
□ Syslog Client
DCP Server: Read/Write

Time: Manual
SNMP: SNMPv1/v2c/v3
☑ SNMPv1/v2 Read-Only
□ SNMPv1 Traps
Configuration Mode: Trial

Description

The page contains the following boxes:

- **Telnet Server**
  Enable or disable the "Telnet Server" service for unencrypted access to the CLI.
- **SSH Server**
  Enable or disable the "SSH Server" service for encrypted access to the CLI.
- **HTTPS Server only**

  When enabled, you can only access the device using HTTPS.
- **SMTP Client**

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

- **Syslog Client**

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

- **DCP Server**
  Specify whether 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".

  – 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".

  – SIMATIC Time
  The system time is set using a SIMATIC time transmitter. You can configure other settings in "System > System Time > SIMATIC Time 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 SNMP traps (alarm frames). You can configure other settings in "System > SNMP > Traps".

- **DHCP Client** (M816 only)
  Enable or disable the DHCP client. You can configure other settings in "System > DHCP Client".

- **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 when you restart the device, the configuration is automatically saved.

  – 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, us the "Write Startup Config" button. The "Write Startup Config" button is displayed when you set trial mode. The message "Trial Mode Active – Press "Write Startup Config" button to make your settings persistent" is also displayed in the display area as soon as there are unsaved changes. This message can be seen on every WBM page until the changes made have either been saved or the device has been restarted.

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 %u seconds.Press 'Write Startup Config' to save 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.

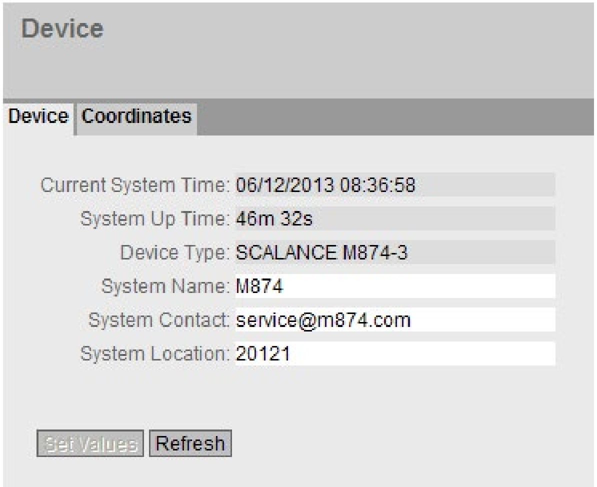
Procedure

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.

4.5.2 General

4.5.2.1 Device

This WBM page contains the general device information.



Current System Time: 06/12/2013 08:36:58
System Up Time: 46m 32s
Device Type: SCALANCE M874-3
System Name: M874
System Contact: service@m874.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 SINEC H1 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 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 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 location is displayed in the selection area. A maximum of 255 characters are possible.

Note

Permitted characters

The following printable ASCII characters (0x20 to 0x7) are permitted in the input fields "System Name", "System Contact" and "System Location":

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

Procedure

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

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

4.5.2.2 Coordinates

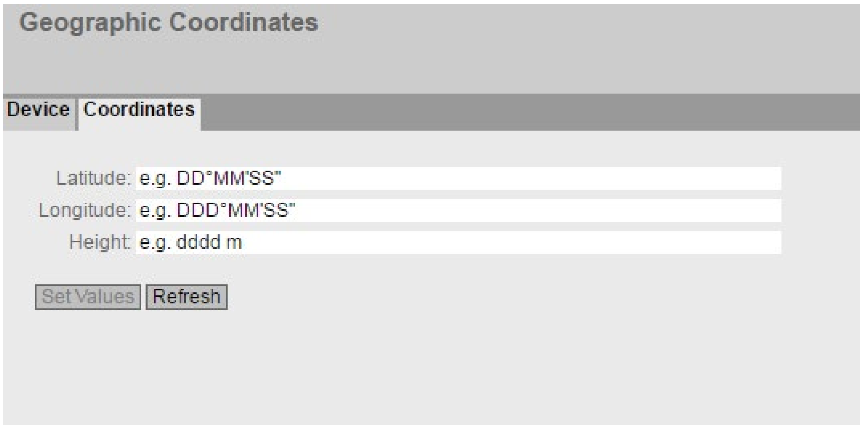
Information on geographic coordinates

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.


Geographic Coordinates

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

Description

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

- **Latitude**
  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**
  Geographical 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).
- **Height**
  Geographical 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.

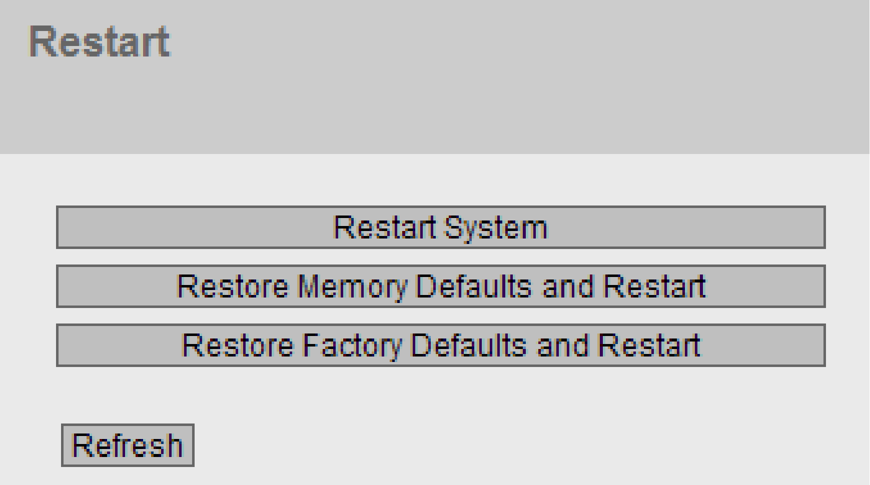
Procedure

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

4.5.3 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 "Autosave 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 System**
  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 on 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 configuration settings. The protected defaults are also reset.
  An automatic restart is triggered.

Note

By resetting to the factory configuration settings, the device loses its configured IP address and is
reachable again with the IP address 192.168.1.1 set in the factory.

4.5.4 Load and Save

4.5.4.1 File list

Overview of the file types

File type	Description
Config	This file contains the start configuration. Among other things, this device contains the definitions of the users, roles, groups and function rights. The passwords are stored the file "Users".
ConfigPack	Detailed configuration information. for example, start configuration, users, certificates ZIP file consisting of the Config, Users and LSYS fle.
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.

File type	Description
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 "Passwords (Page 106)" WBM page.
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.
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 "Passwords (Page 106)" WBM page. The loaded files are listed on "Security > Certificates > Overview (Page 185)". For more information on certificates, refer to section "Certificates (Page 38)".

4.5.4.2 HTTP

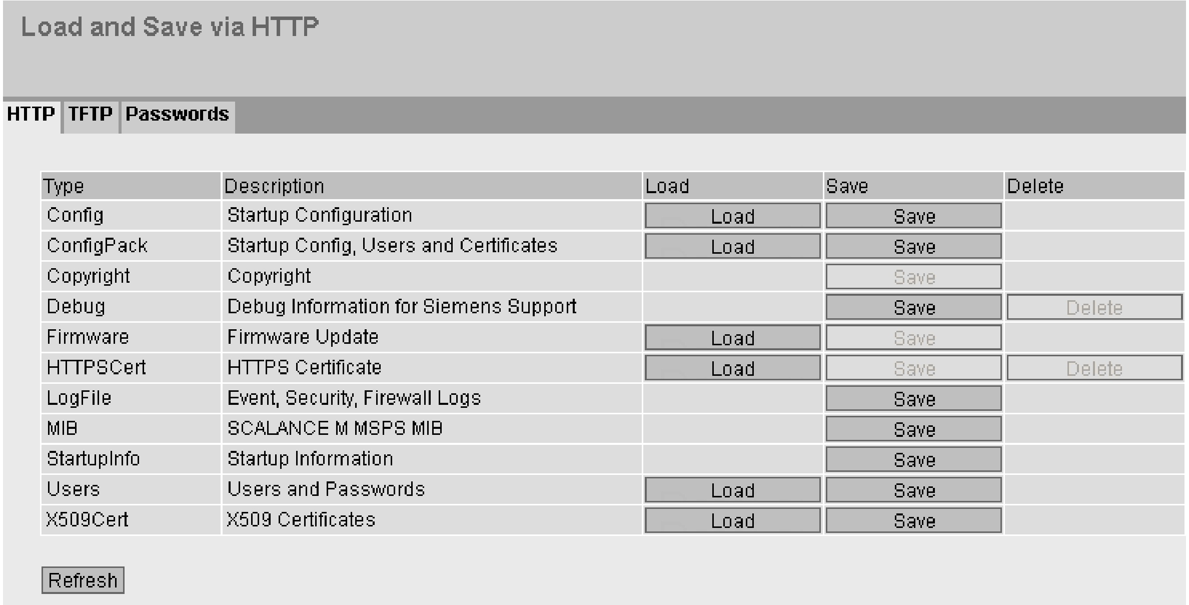
Loading and saving data using HTTP

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.

Note

Configuration files and trial mode/Automatic Save mode

In Automatic Save mode, the data is saved automatically before the configuration files (ConfigPack and Config) are transferred.
In Trial, 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.



Load and Save via HTTP

Type	Description	Load	Save	Delete
Config	Startup Configuration	Load	Save	
ConfigPack	Startup Config, Users and Certificates	Load	Save	
Copyright	Copyright		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	
StartupInfo	Startup Information		Save	
Users	Users and Passwords	Load	Save	
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 load files on the device. The button can be enabled, if this function is supported by the file type.
- **Save**
  With this button, you can save 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, empty the cache of the Web browser.

Procedure

Loading files using HTTP

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

   The dialog for loading a file is opened.

   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" > "Password".

   ---

2. Go to the required file
3. Click the "Open" button in the dialog.

   The file is now loaded.
4. If a restart is necessary, a message to this effect will be output.

Saving files using HTTP

1. Start the save function by clicking the one of the "Save" buttons.
2. You will be prompted to select a storage location and a name for the file. Or you accept the proposed file name. To make the selection, use the dialog in your browser. After making your selection, click the "Save" button.

Deleting files using HTTP

1. Start the delete function by clicking the one of the "Delete" buttons.

   The file will be 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 this configuration file on all other devices you want to configure.
3. If individual settings are necessary for specific devices, these must be made online on the relevant device.

Note that the configuration data is coded when it is saved. This means that you cannot edit the files with a text editor.

4.5.4.3 TFTP

Loading and saving data using a TFTP server

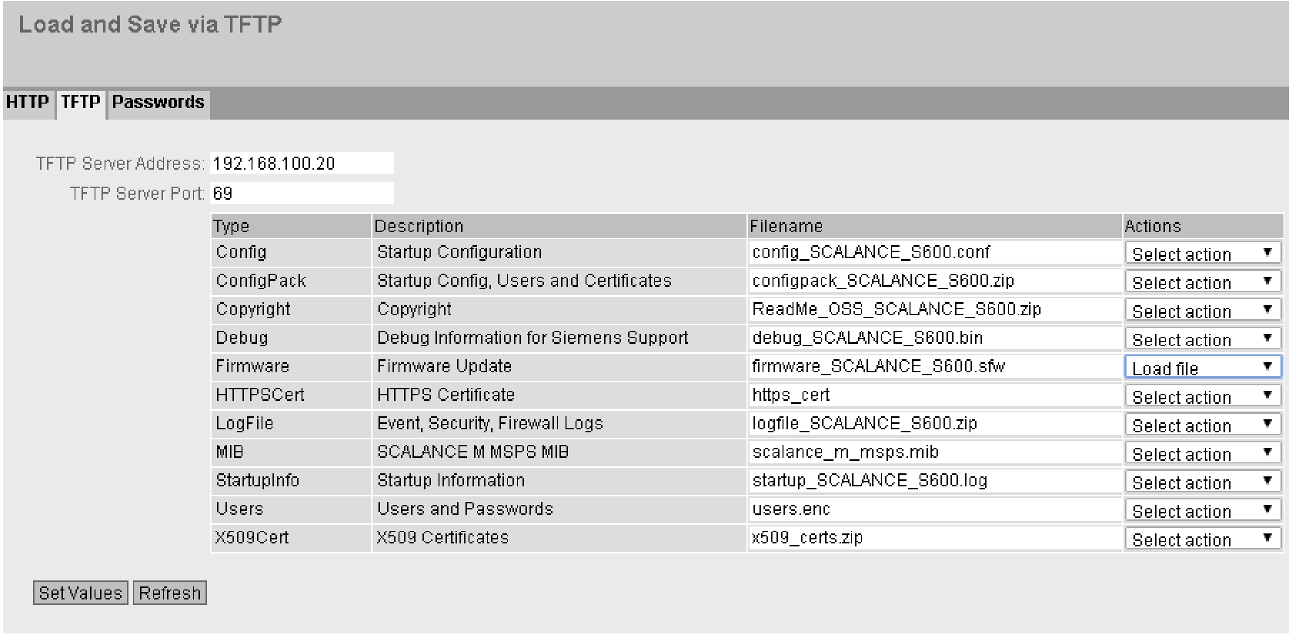
On this page, you can configure the TFTP server and the file names. The WBM also allows you to store device data in an external file on your client PC or to load such data from an external file from the PC to the devices. This means, for example, that you can also load new firmware from a file located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

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

Note

Configuration files and trial mode/Automatic Save mode

In Automatic Save mode, the data is saved automatically before the configuration files (ConfigPack and Config) are transferred.
In Trial, 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.



TFTP Server Address: 192.168.100.20
TFTP Server Port: 69

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
Copyright	Copyright	ReadMe_OSS_SCALANCE_S600.zip	Select action
Debug	Debug Information for Siemens Support	debug_SCALANCE_S600.bin	Select action
Firmware	Firmware Update	firmware_SCALANCE_S600.sfw	Load file
HTTPSCert	HTTPS Certificate	https_cert	Select action
LogFile	Event, Security, Firewall Logs	logfile_SCALANCE_S600.zip	Select action
MIB	SCALANCE M MSPS MIB	scalance_m_msps.mib	Select action
StartupInfo	Startup Information	startup_SCALANCE_S600.log	Select action
Users	Users and Passwords	users.enc	Select action
X509Cert	X509 Certificates	x509_certs.zip	Select action

Description

The page contains the following boxes:

- **"TFTP Server IP Address" input box**
  Enter the IP address of the TFTP server with which you exchange data.
- **"TFTP Server IP Port" input box**
  Enter the port of the TFTP server over 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" input box**
  Enter a file name.
- **"Actions" drop-down list**
  Select the required action. 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 files using TFTP

1. Enter the IP address of the TFTP server in the "TFTP Server IP Address" input box.
2. Enter the server port to be used in the in the "TFTP Server Port" input box.
3. Enter the file name in the "Filename" input box.

> **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" > "Password".

4. Select the Load file action from the "Actions"drop-down list.
5. Click the "Set Values" button to start loading.
6. If a restart is necessary, a message to this effect will be output.

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.

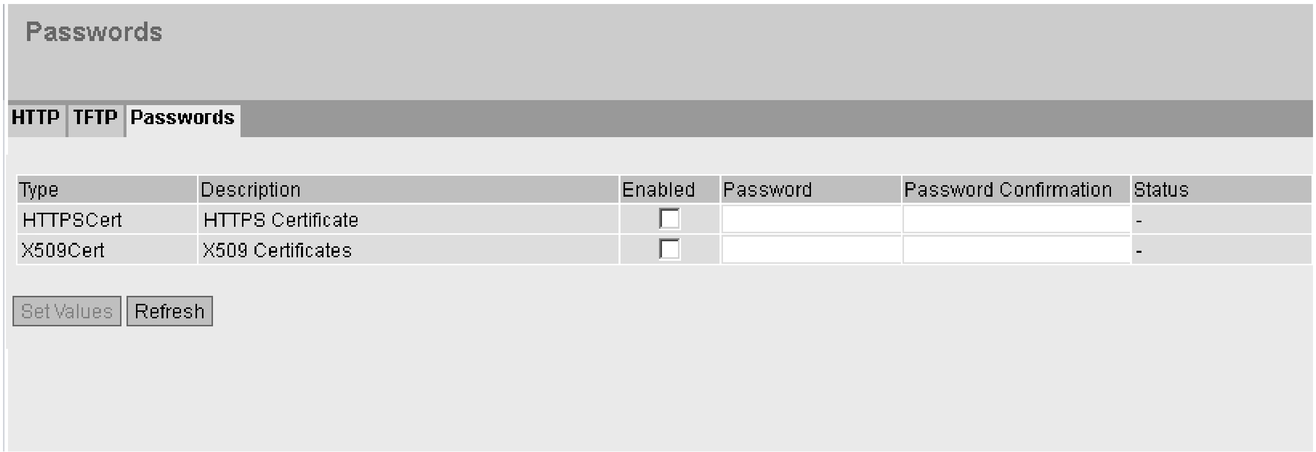
Follow the steps below to reuse configuration data:

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

Note that the configuration data is coded when it is saved. This means that you cannot edit the files with a text editor.

4.5.4.4 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.



Passwords

Type	Description	Enabled	Password	Password Confirmation	Status
HTTPSCert	HTTPS Certificate	□			-
X509Cert	X509 Certificates	□			-

Description

The table has the following columns:

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

4.5.5 Events

4.5.5.1 Configuration

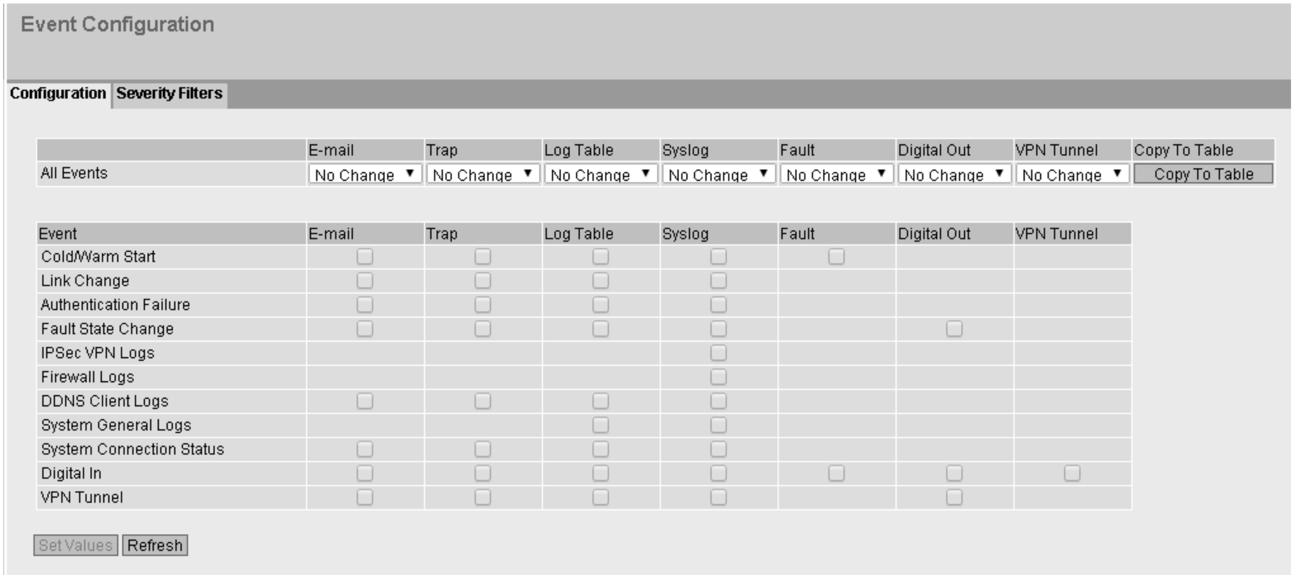
Selecting system events

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 messages additionally to a syslog server, enable the "Syslog" setting.



Event Configuration

	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	□	□	□	□		□	
IPSec VPN Logs				□			
Firewall Logs				□			
DDNS Client Logs	□	□	□	□			
System General Logs			□	□			
System Connection Status	□	□	□	□			
Digital In	□	□	□	□	□	□	□
VPN Tunnel	□	□	□	□		□	

Description

Table 1 has the following columns:

- **Event**
  Shows that the settings are valid for all events of table 2.
- **E-Mail / Trap / Log Table / Syslog / Fault / Digital Out / VPN Tunnel**
  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.
  - 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 attempting access with a bad password.

  - 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 the power supply monitoring.
  - IPsec VPN Logs
    An entry is made in the security log if the IPsec method for VPN was used.
  - 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.
  - System Connection Status
    The connection status has changed.
  - System General Logs
    Connection establishment, change to the configuration.
  - 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, OpenVPN, SRC) has changed.

  E-Mail
  The device sends an e-mail. This is only possible if the SMTP server is set up and the "SMTP client" function is enabled.

- **Trap**
  The device sends an SNMP trap. This is only possible if "System > Configuration" SNMPv1 Traps" is enabled.
- **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**
  The fault LED lights up on the device.
- **Digital Output**

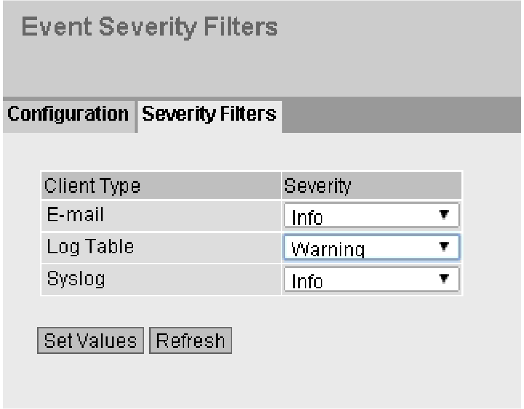
  Controls the digital output or signals the status change with the "DO" LED.
- **VPN Tunnel**
  Controls the VPN connection (establishment/termination).

Steps in configuration

1. Select the check box in the row of the required event. Select the event in the column under the following actions:
   - E-Mail
   - Trap
   - Log Table
   - Syslog
   - Fault
   - Digital Output
   - VPN Tunnel
2. Click the "Set Values" button.

4.5.5.2 Severity filter

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



Event Severity Filters

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

Description

The table has the following columns:

- **Client Type**
  Select the client type for which you want to make settings:
  - **E-Mail**
    Sending system event messages by e-mail.
  - **Log Table**
    Entry of system events in the log table.
  - **Syslog**
    Entry of system events in the Syslog file

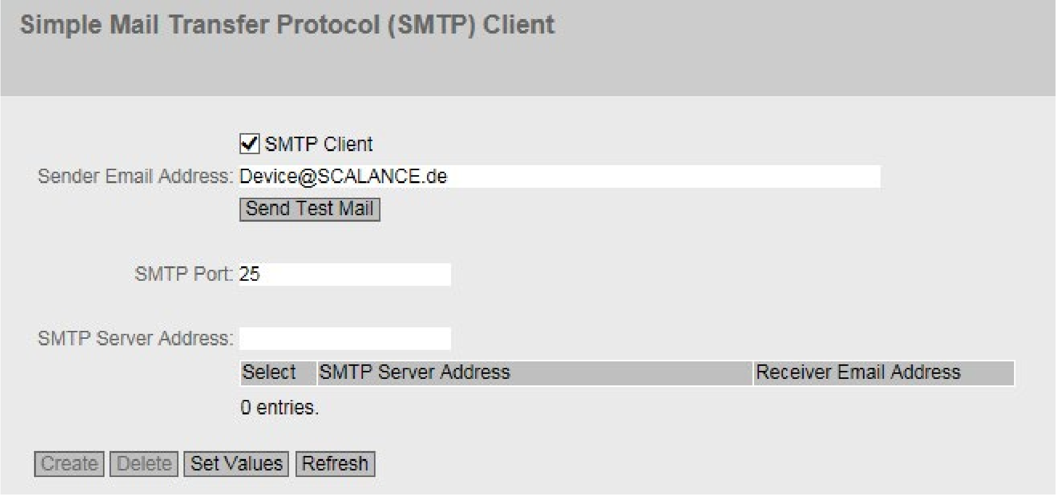
- **Severity**
  Select the required level. The following settings are possible:
  – **Info**
    The messages of all levels are sent or logged.
  – **Warning**
    The message of this level and the "critical" level are sent or logged.
  – **Critical**
    Only the messages of this level are sent or logged.

4.5.6 SMTP client

Network monitoring with e-mails

The device provides the option of automatically sending an e-mail if an alarm event occurs (for example to the network administrator). The e-mail contains the identification of the sending device, a description of the cause of the alarm in plain language, and a time stamp. This allows centralized network monitoring to be set up for networks with few nodes based on an e-mail system. When an e-mail error message is received, the WBM can be started by the Internet browser using the identification of the sender to read out further diagnostics information.

On this page, you can configure up to three SMTP servers and the corresponding e-mail addresses.



Simple Mail Transfer Protocol (SMTP) Client

☑ SMTP Client

Sender Email Address: Device@SCALANCE.de

SMTP Port: 25

SMTP Server Address:

Select	SMTP Server Address	Receiver Email Address

0 entries.

Description

The page contains the following boxes:

- **SMTP Client**
  Enable or disable the SMTP client.
- **Sender Email Address**
  Enter the name of the sender to be included in the e-mail, for example the device name.

  This setting applies to all configured SMTP servers.
- **Send Test Mail**

  Send a test e-mail to check your configuration.
- **SMTP Port**

  Enter the port via which your SMTP server can be reached.

  Factory settings: 25

  This setting applies to all configured SMTP servers.
- **SMTP Server Address**
  Enter the IP address or the FQDN name of the SMTP server.

This table contains the following columns:

- **Select**
  Enable the check box in a row to be deleted.
- **SMTP Server Address**
  Shows the IP address or the FQDN name of the SMTP server.
- **Receiver Email Address**
  Enter the e-mail address to which the device sends an e-mail if a fault occurs.

Procedure

1. Enable the "SMTP Client" option.
2. Enter the IP address of the SMTP server or the FQDN name in the "SMTP Server Address" input box.
3. Click the "Create" button. A new entry is generated in the table.
4. In the "Receiver Email Address" input box, enter the e-mail address to which the device is to send an e-mail if a fault occurs.
5. Click the "Set Values" button.

Note

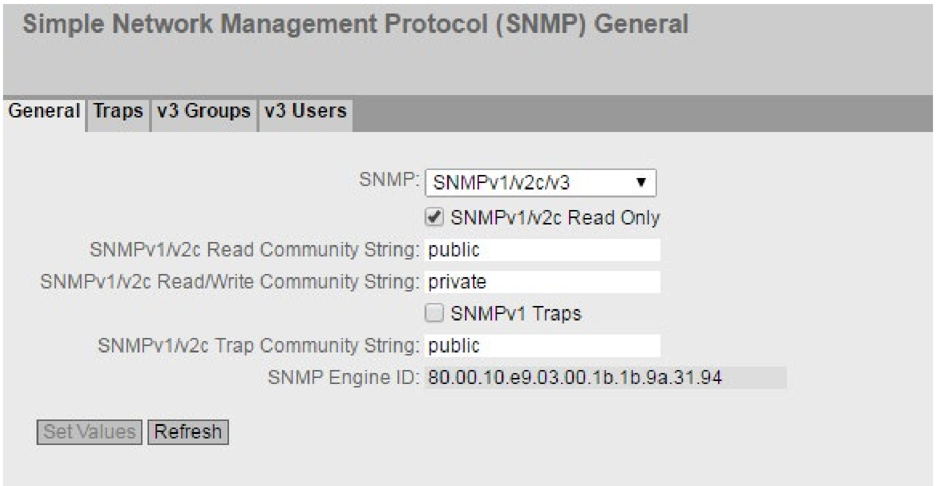
Depending on the properties and configuration of the SMTP server, it may be necessary to adapt the "Sender Email Address” box for the e-mails. Check with the administrator of the SMTP server.

4.5.7 SNMP

4.5.7.1 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".



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.
  – 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.

- **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 SNMP traps (alarm frames). On the "Trap" tab, specify the IP addresses of the devices to which SNMP traps will be sent.
- **SNMPv1/v2c Trap Community String**
  Enter the community string for sending SNMPv1/v2 messages.
- **SNM 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. Select the "SNMPv1/v2c Read only" check box if you only want read access to SNMP variables with SNMPv1/v2c.
3. In the "SNMPv1/v2c Read Community String" input box, enter the required character string.
4. In the "SNMPv1/v2c Read/Write Community String" input box, enter the required character string.
5. Click the "Set Values" button.

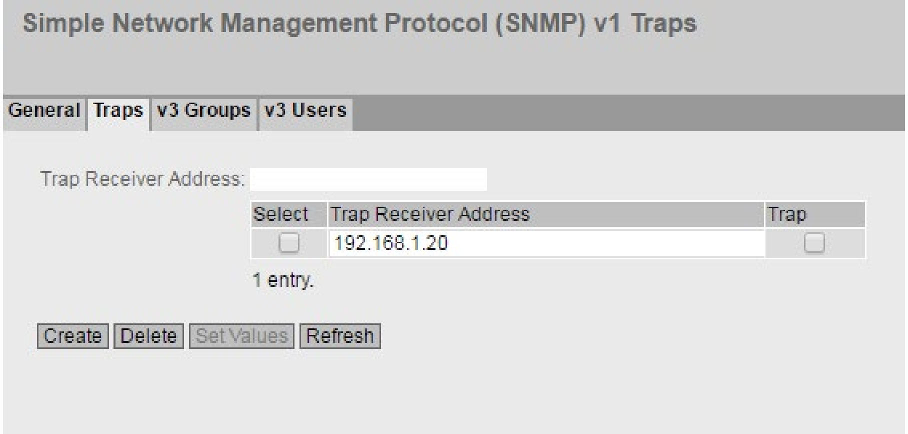
4.5.7.2 Traps

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".



Simple Network Management Protocol (SNMP) v1 Traps

Trap Receiver Address:

Select	Trap Receiver Address	Trap
□	192.168.1.20	□

1 entry.

Description

- **Trap Receiver Address**
  Enter the IP address or the FQDN 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 addresses or the FQDN 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 sends SNMP 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.

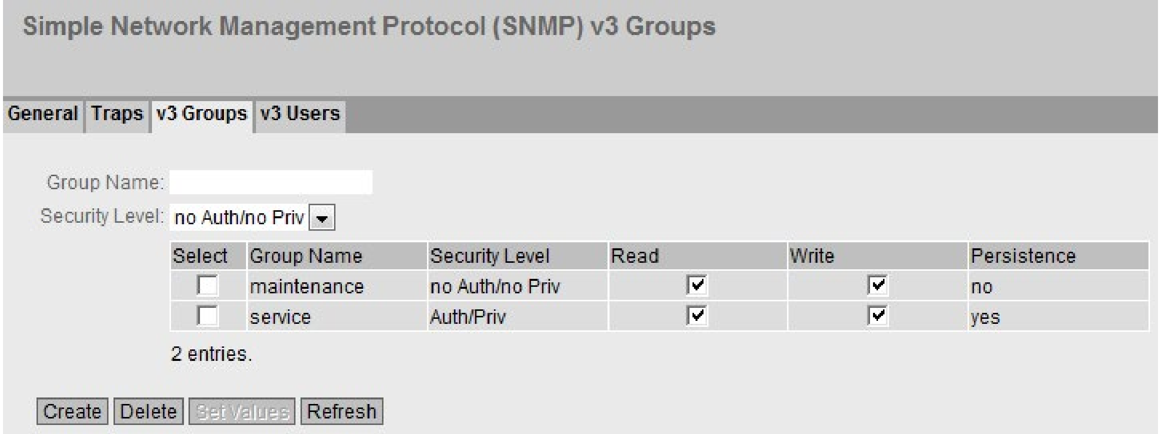
Deleting a trap entry

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

4.5.7.3 Groups

Security settings and assigning permissions

SNMP version 3 allows permissions to be assigned, authentication, and encryption at protocol level. The security levels 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/Priv	☑	☑	yes

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. In the security levels, the following options:
  - 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 wite 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 disappears again 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.

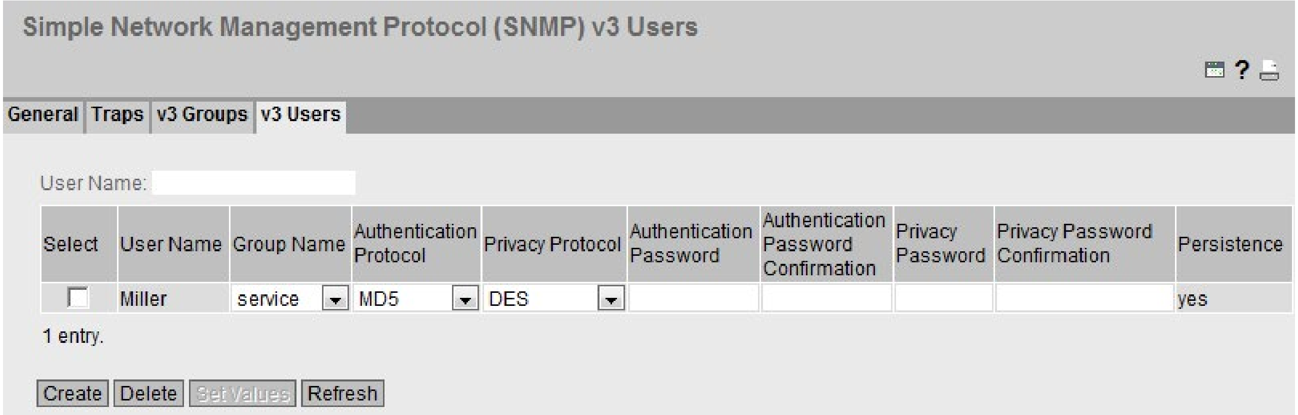
Deleting a group

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.

4.5.7.4 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.



Simple Network Management Protocol (SNMP) v3 Users

User Name:

Select	User Name	Group Name	Authentication Protocol	Privacy Protocol	Authentication Password	Authentication Password Confirmation	Privacy Password	Privacy Password Confirmation	Persistence
□	Miller	service	MD5	DES					yes

1 entry.

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 to which the user will be assigned.
- **Authentication Protocol**
  Specify the authentication protocol. Can only be enabled, if this group supports the function.

  The following settings are available:

  – none

  – MD5

  – SHA

- **Privacy Protocol**
  Specify whether or not the user uses the DES algorithm. Can only be enabled, if the group supports this function.
- **Authentication Password**
  Enter the authentication password in the first input box. This password must have at least 6 characters, the maximum length is 32 characters.
- **Authentication Password Confirmation**
  Confirm the password by repeating the entry.
- **Privacy Password**
  Enter your encryption password. This password must have at least 6 characters, the maximum length is 32 characters.
- **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 disappears again 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 "Groups", 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 "Authentification Protocol".
   In the relevant input boxes, enter the authentication password and its confirmation.
5. If encryption was specified for the group, select the algorithm from the "Privacy Protocol" drop-down list. 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.

Note

If you click a different button prior to this step (for example the "Refresh" button), the delete action is canceled. The data of the selected rows is retained. The selections are removed. If you want to repeat the action, you will need to reselect the data records to be deleted.

4.5.8 System Time

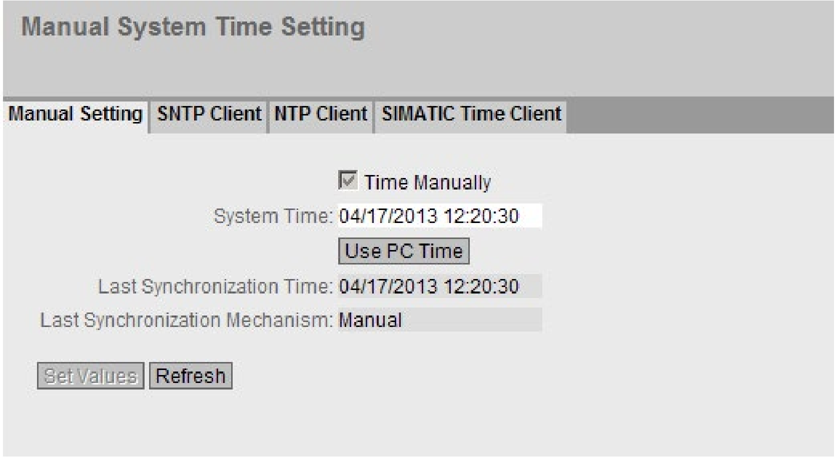
There are different methods that can be used to set the system time of the device. Only one method can be active at any one time.

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

4.5.8.1 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: 04/17/2013 12:20:30

Last Synchronization Time: 04/17/2013 12:20:30

Last Synchronization Mechanism: Manual

Description

The page contains the following boxes:

- **Time Manually**
  Enable or disable manual setting of the time. If you enable the option, the "System Time" input box can be edited.
- **System Time**
  Enter the date and time in the format "MM/DD/YYYY HH:MM:SS".

  After a restart, the time of day begins at 01/01/2000 00:00:00
- **Use PC Time**
  Click the button to use the time setting of the PC.
- **Last Synchronization Time**
  This box is read-only and 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**
  This box displays how the last time-of-day synchronization was performed.
  - Not set
    The system 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

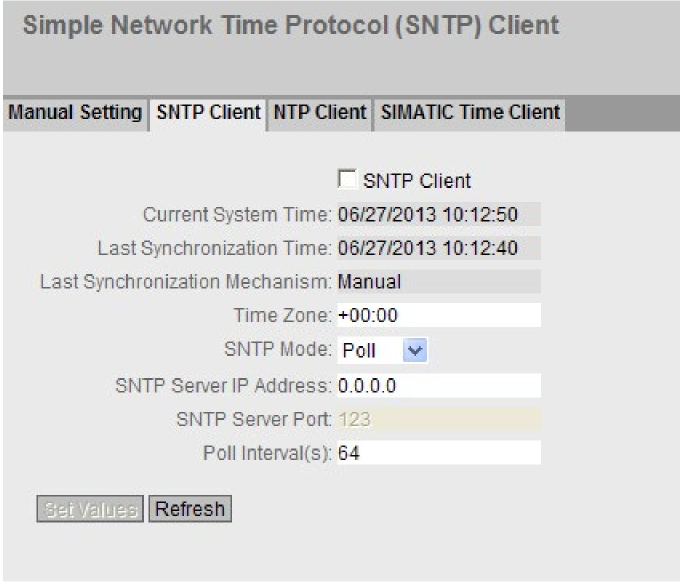
Procedure

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 the "Last Synchronization Mechanism" box.

4.5.8.2 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: 06/27/2013 10:12:50

Last Synchronization Time: 06/27/2013 10:12:40

Last Synchronization Mechanism: Manual

Time Zone: +00:00

SNTP Mode: Poll

SNTP Server IP Address: 0.0.0.0

SNTP Server Port: 123

Poll Interval(s): 64

Description

The page contains the following boxes:

- **SNTP Client**
  Enable or disable automatic time-of-day synchronization using SNTP.
- **Current System Time**
  Shows the values currently set in the system for date and time.
- **Last Synchronization Time**
  This box is read-only and shows when the last time-of-day synchronization took place.

- **Last Synchronization Mechanism**
  This box displays how the last time-of-day synchronization was performed. The following methods are possible:
  - Not set
    The system 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**
  Enter the time zone you are using in the format "+/- HH:MM". The time zone relates to UTC standard world time. Settings for daylight-saving and standard time are taken into account in this box by specifying the time offset.
- **SNTP Mode**
  Select the synchronization mode from the drop-down list. The following types of synchronization are possible:
  - Poll
    If you select this protocol type, the input boxes "SNTP Server IP Address", "SNTP Server Port" and "Poll Interval(s)" are displayed for 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 "listens" for SNTP frames that deliver the time of day.
- **SNTP Server IP Address**
  Enter the IP address 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)**
  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 the "Time Zone" input box, enter the local time difference to world time (UTC). The input format is "+/-HH:MM" (for example +02:00 for CEST), because the SNTP server always sends the UTC time. This time is then recalculated and displayed as the local time

based on the specified time zone. On the device itself, there is no changeover from the daylight saving to standard time. You also need to take this into account when completing the "Time Zone" input box.

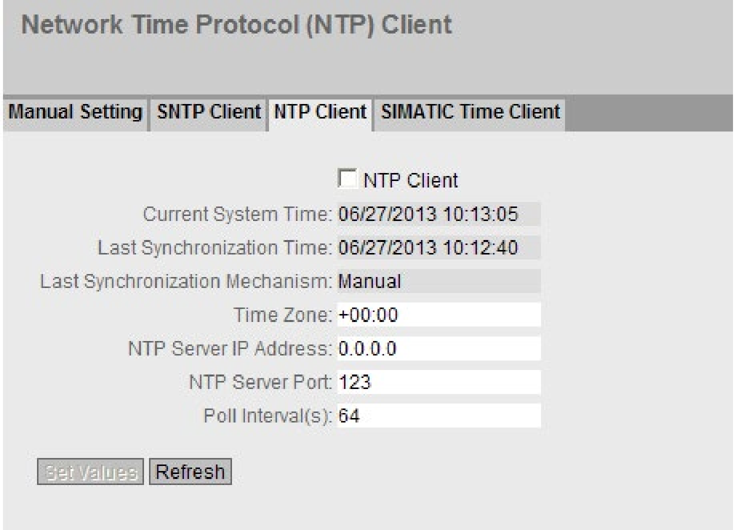
3. Select one of the following options from the "SNTP Mode" drop-down list:
   – Poll
   For this mode, you need to configure the following:
   - time zone difference (step 2)
   - time server (step 4)
   - Port (step 5)
   - query interval (step 6)
   - complete the configuration with step 7.

   – 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 7.
4. In the "SNTP Server IP Address" input box, enter the IP address of the SNTP server whose frames will be used to synchronize the time of day.
5. In the "SNTP Server Port" input box, enter the port via which the SNTP server is available. The port can only be modified if the IP address of the SNTP server is entered.
6. In the "Poll Interval(s)" input box, enter the time in seconds after which a new time query is sent to the time server.
7. Click the "Set Values" button to transfer your changes to the device.

4.5.8.3 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

Current System Time: 06/27/2013 10:13:05
Last Synchronization Time: 06/27/2013 10:12:40
Last Synchronization Mechanism: Manual
Time Zone: +00:00
NTP Server IP Address: 0.0.0.0
NTP Server Port: 123
Poll Interval(s): 64

Description

The page contains the following boxes:

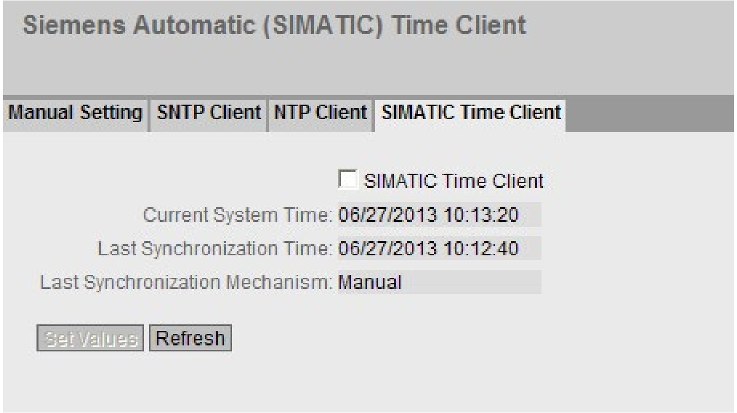
- **NTP Client**
  Select this check box to enable automatic time-of-day synchronization with NTP.
- **Current System Time**
  This box displays the current system time.
- **Last Synchronization Time**
  This box is read-only and shows when the last time-of-day synchronization took place.
- **Last Synchronization Mechanism**
  This box displays how the last time-of-day synchronization was performed. The following methods are possible:
  - Not set
    The system 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. Settings for daylight-saving and standard time are taken into account in this box by specifying the time offset.
- **NTP Server Address**
  Enter the address 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(s)**
  Here, enter the interval between two time queries. In this box, you enter the query interval in seconds. Possible values are 64 to 1024 seconds.

Procedure

1. Click the "NTP Client" check box to enable the automatic time setting using NTP.
2. Enter the necessary values in the following boxes:
   – Time zone
   – NTP server IP address
   – NTP server port
   – Query interval
3. Click the "Set Values" button.

4.5.8.4 SIMATIC Time Client

Time setting via SIMATIC time client



Siemens Automatic (SIMATIC) Time Client

□ SIMATIC Time Client

Current System Time: 06/27/2013 10:13:20

Last Synchronization Time: 06/27/2013 10:12:40

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**
  This box displays the current system time.

- **Last Synchronization Time**
  This box is read-only and shows when the last time-of-day synchronization took place.
- **Last Synchronization Mechanism**
  This box displays how the last time-of-day synchronization was performed. The following methods are possible:
  - Not set
    The system 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.

4.5.9 Auto logout

Setting the automatic logout

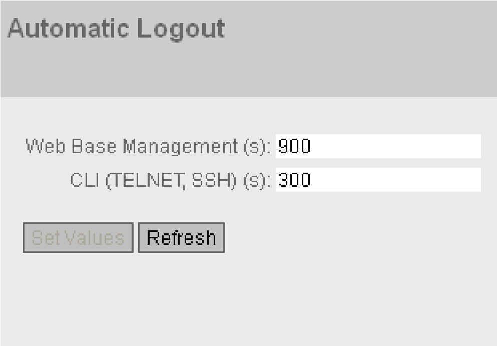
On this page, set the times after which there is an automatic logout from WBM or the CLI following user in activity.

If you have been logged out automatically, you will need to log in again.

Note

No automatic logout from the CLI

If the connection is not terminated after the set time, check the setting of the "keepalive" function on the Telnet client. If the set time interval is less than the configured time, the lower value applies. For example, you have set 300 seconds for the automatic logout and 120 seconds is set for the "keepalive" function. In this case, a packet is sent every 120 seconds that keeps the connection up.



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 (TELNET, SSH) (s)" input box. If you enter the value 0, the automatic logout is disabled.
3. Click the "Set Values" button.

4.5.10 Syslog Client

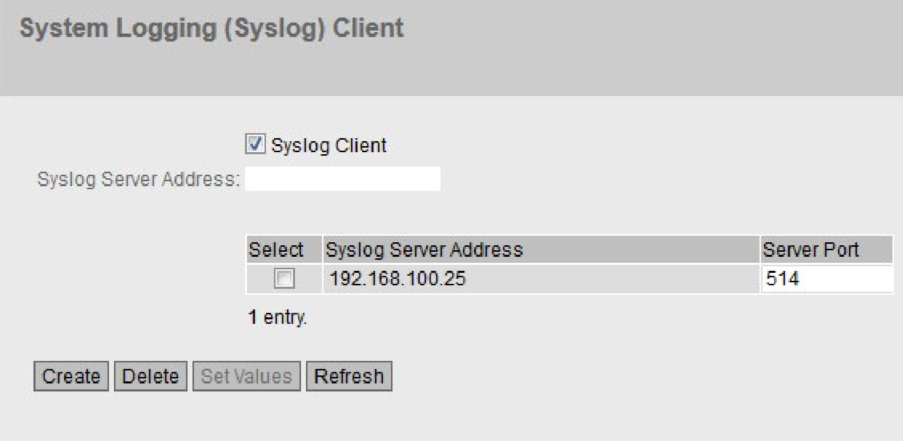
System event agent

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.



System Logging (Syslog) Client

☑ Syslog Client

Syslog Server Address:

Select	Syslog Server Address	Server Port
□	192.168.100.25	514

1 entry.

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.

4.5.11 Fault monitoring

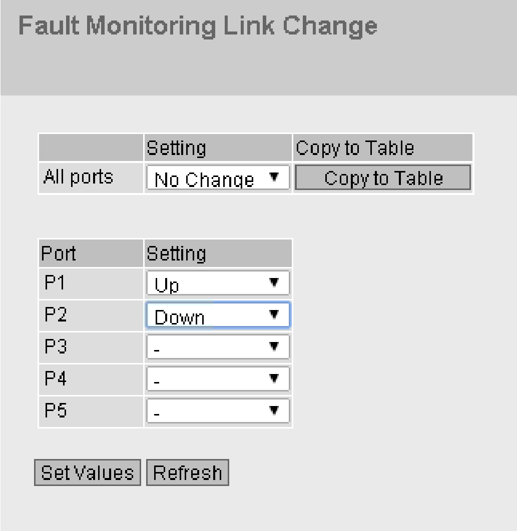
Configuration of fault monitoring of status changes on connections

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, an e-mail, 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.

4.5.12 PLUG

4.5.12.1 Configuration

NOTICE

Do not remove or insert a C-PLUG / KEY-PLUG during operation!

A PLUG may only be removed or inserted when the device is turned off.
The device checks whether 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 KEY-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.

Information about the configuration of the KEY-PLUG

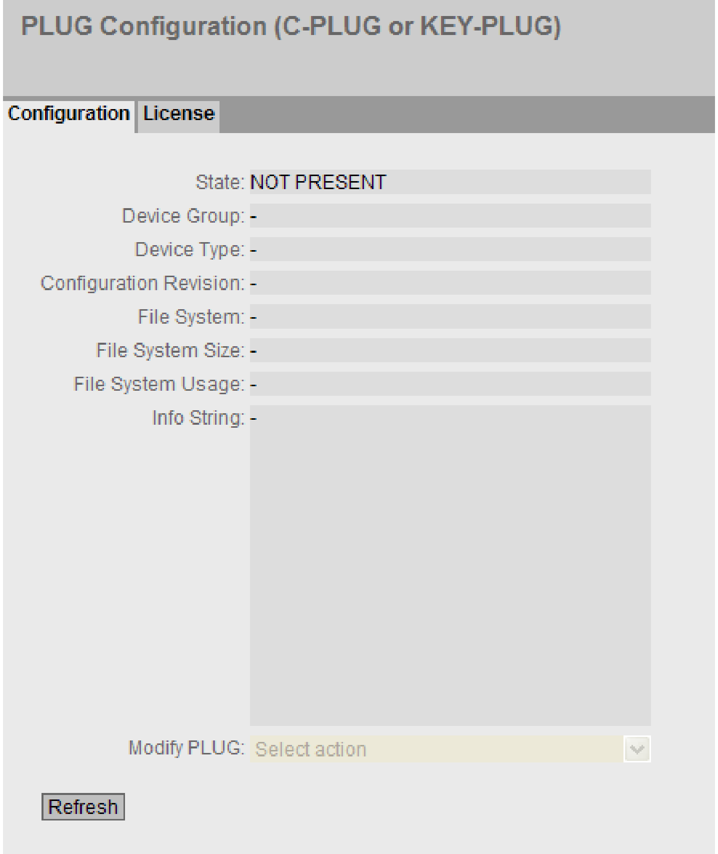
This page provides detailed information about the configuration stored on the C-PLUG. It is also possible to reset the PLUG to "factory defaults" or to load it with new contents.

Note

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 (C-PLUG or KEY-PLUG)

State: NOT PRESENT
Device Group: -
Device Type: -
Configuration Revision: -
File System: -
File System Size: -
File System Usage: -
Info String: -

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 C-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 C-PLUG previously.

- **Device Type**
  Shows the device type within the product line that used the C-PLUG previously.
- **Configuration Revision**
  The version of the configuration structure. This information relates to the configuration options supported by the device and has nothing to do with the concrete hardware configuration. This revision information does not therefore change if you add or remove additional components (modules or extenders), it can, however, change if you update the firmware.
- **File System**
  Displays the type of file system on the PLUG.
- **File System Size [Byte]**
  Displays the maximum storage capacity of the file system on the PLUG.
- **File System Usage [Byte]**
  Displays the memory utilization of the file system of the PLUG.
- **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.
- **"Modify PLUG" drop-down list**
  Select the setting from the drop-down list. You have the following options for changing the configuration on the C-PLUG:
  - Write current configuration to 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 the data from the PLUG and runs a low-level formatting function.

Procedure

1. You can only make settings in this box if you are logged on as "Administrator". Here, you decide how you want to change the content of the PLUG.
2. Select the required option from the "Modify PLUG" drop-down list.
3. Click the "Set Values" button.

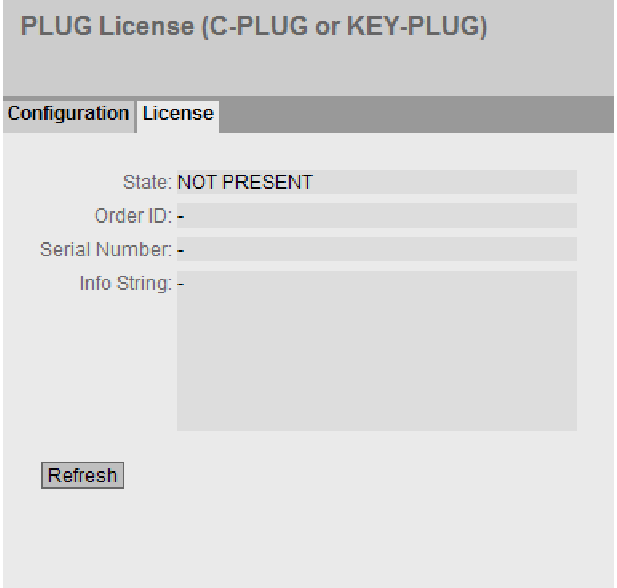
4.5.12.2 License

NOTICE
Do not remove or insert a C-PLUG / KEY-PLUG during operation!
A PLUG may only be removed or inserted when the device is turned off. The device checks whether 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 KEY-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.

Information about the license of the KEY-PLUG

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

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



PLUG License (C-PLUG or KEY-PLUG)

State: NOT PRESENT
Order ID: -
Serial Number: -
Info String: -

Description

- **State**
  Shows the status of the KEY-PLUG. The following are possible:
  - ACCEPTED
    The KEY-PLUG in the device contains a suitable and valid license.
  - NOTACCEPTED
    The license of the inserted KEY-PLUG is not valid.
  - NOTPRESENT
    No KEY-PLUG is inserted in the device.
  - MISSING
    There is no KEY-PLUG inserted with the "FACTORY" status. Functions are configured on the device for which a license is required.
  - WRONG
    The inserted KEY-PLUG is not suitable for the device.
  - UNKNOWN
    Unknown content of the KEY-PLUG.
  - DEFECTIVE
    The content of the KEY-PLUG contains errors.
- **Order ID**
  Shows the order number of the KEY-PLUG. The KEY-PLUG is available for various functional enhancements and for various target systems.
- **Serial Number**
  Shows the serial number of the KEY-PLUG.
- **Info String**
  Shows additional information about the device that used the KEY-PLUG previously, for example, 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.

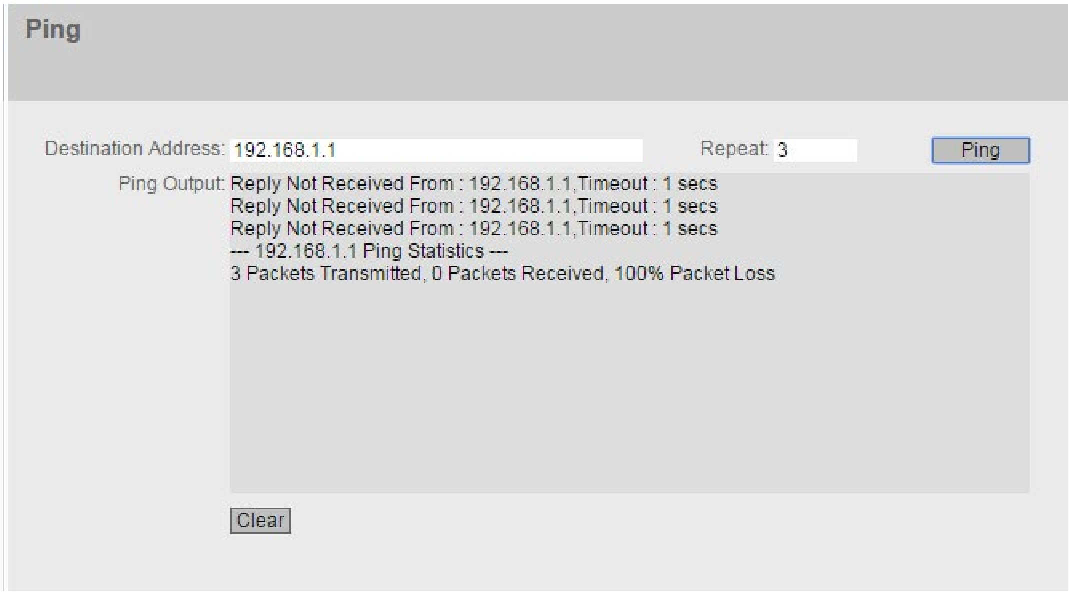
Note

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

4.5.13 Ping

Reachability of an address in an IPv4 network

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



```
Reply Not Received From : 192.168.1.1,Timeout : 1 secs
Reply Not Received From : 192.168.1.1,Timeout : 1 secs
Reply Not Received From : 192.168.1.1,Timeout : 1 secs
--- 192.168.1.1 Ping Statistics ---
3 Packets Transmitted, 0 Packets Received, 100% Packet Loss
```

Description

The page contains the following:

- **Destination Adress**

  Enter the IPV4 address or the FQDN (Fully Qualified Domain Name) 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.

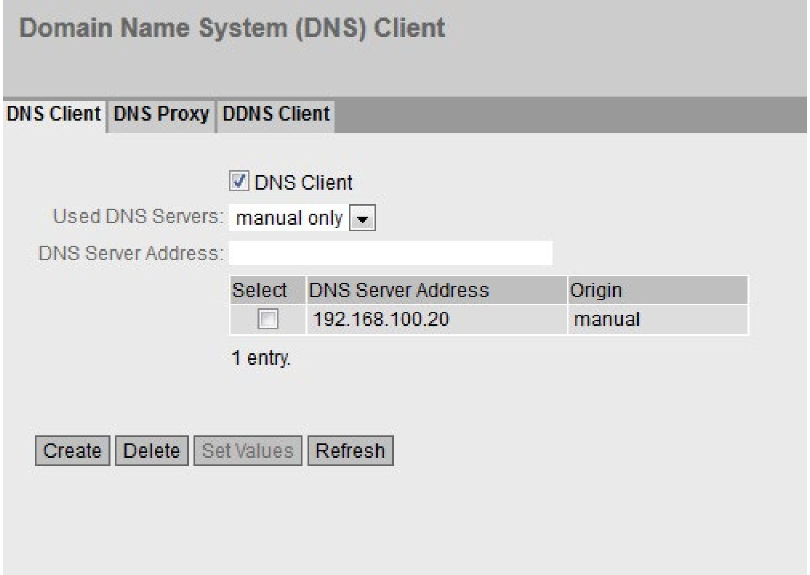
- **Clear**

  Click this button to empty the "Ping Output" box.

4.5.14 DNS

4.5.14.1 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: manual only

DNS Server Address:

Select	DNS Server Address	Origin
□	192.168.100.20	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 Server**

  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:

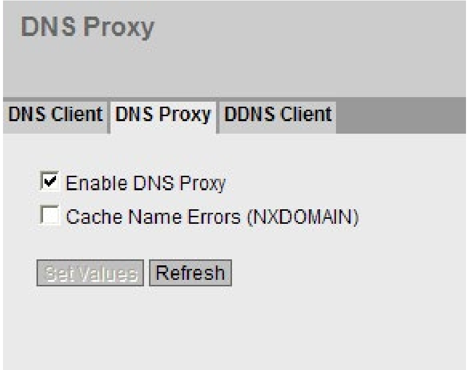
- **Select**
  Select the check box in the row to be deleted

- **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.

4.5.14.2 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.



DNS Proxy

☑ Enable DNS Proxy
□ Cache Name Errors (NXDOMAIN)

Description

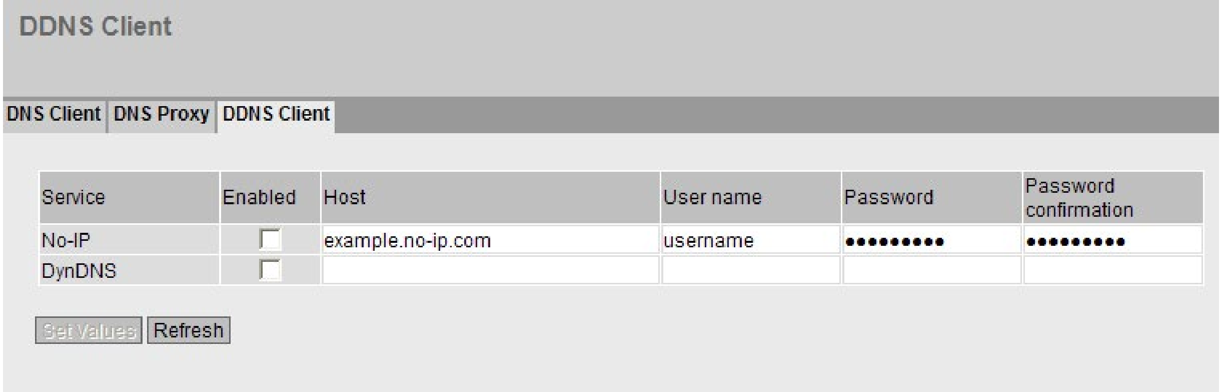
The page contains the following boxes:

- **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.

4.5.14.3 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	□	example.no-ip.com	username	●●●●●●●●●	●●●●●●●●●
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 hostname 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 NAT.

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 (Username, Password) for the DDNS server.
3. Select Enable". This hostname is used for the device.
4. Click "Set Values".

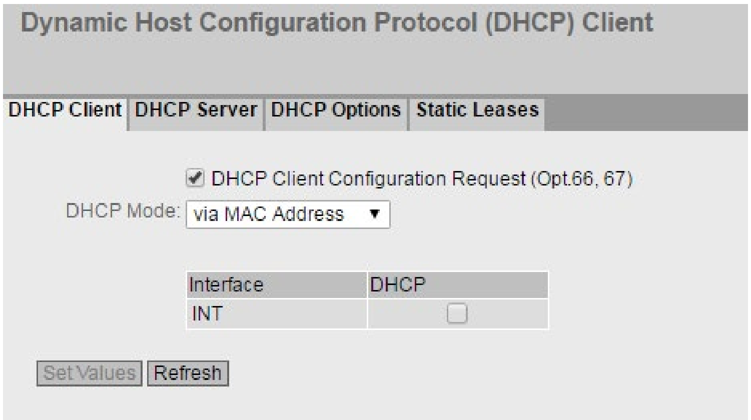
4.5.15 DHCP

4.5.15.1 DHCP client

M826

Setting the DHCP mode

If the DHCP mode is activated, the DHCP client starts a DHCP request to a configured DHCP server and is assigned an IP address as the response. The server manages an address range from which it assigns IP addresses. It is also possible to configure the server so that the client always receives the same IP address in response to its request.



Dynamic Host Configuration Protocol (DHCP) Client

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

DHCP Mode: via MAC Address

Interface	DHCP
INT	□

Description

The page contains the following boxes:

- **DHCP Client Config File Request (Opt.66, 67)**
  Select this option if you want the DHCP client to use options 66 and 67 to download and then enable a configuration file.
- **DHCP Mode**
  Select the DHCP mode from the drop-down list. The following modes are possible:
  - 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 system name. If the system 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. Enable the "DHCP Client" option.
2. Select the DHCP mode "via DHCP Client ID" from the "DHCP Mode" drop-down list.
3. Enter a character string to identify the device in the enabled "DHCP Client ID" input box. This is then evaluated by the DHCP server.
4. Select the "Client Config File Request (Opt.66, 67)" option, if you want the DHCP client to use options 66 and 67 to download and then enable a configuration file.
5. Click the "Set Values" button.

Note

If a configuration file is downloaded, this triggers a system restart. Make sure that the option "Client Config File Request (Opt.66, 67)" is no longer set in this configuration file.

4.5.15.2 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 range you have specified or you can a specific IP address is assigned to a particular device.

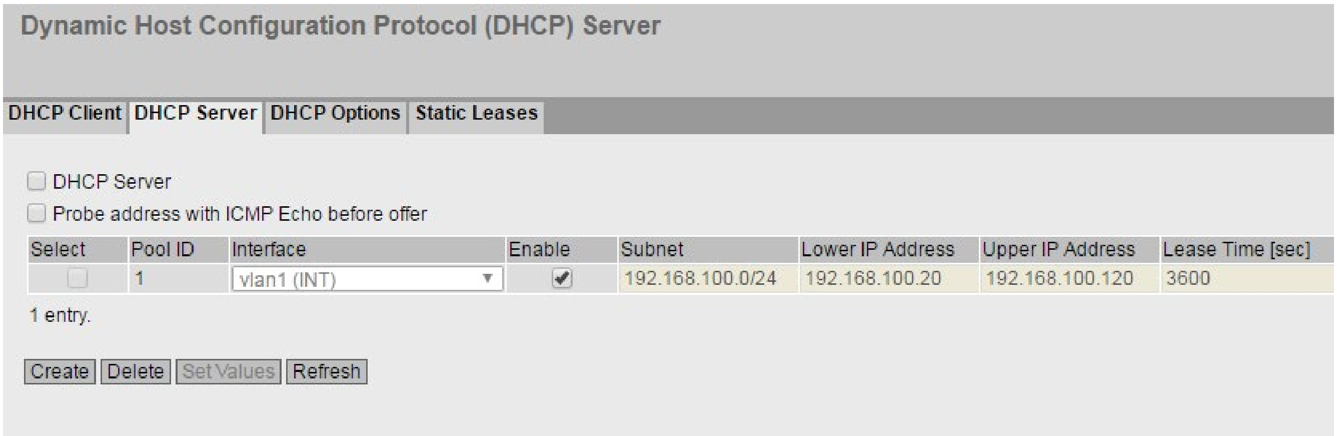
On this page, specify the address band from which the device receives any IP address. You configure the static assignment of the IP addresses in "Static Leases".

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).

Maximum of 20 static entries.



Dynamic Host Configuration Protocol (DHCP) Server

□ 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)	☑	192.168.100.0/24	192.168.100.20	192.168.100.120	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 IPv4 address has already been assigned. To do this the DHCP server sends ICMP echo messages (ping) to the IP 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 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 (Pool ID) is created.

- **Interface**
  Select a VLAN 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 address band will be used.

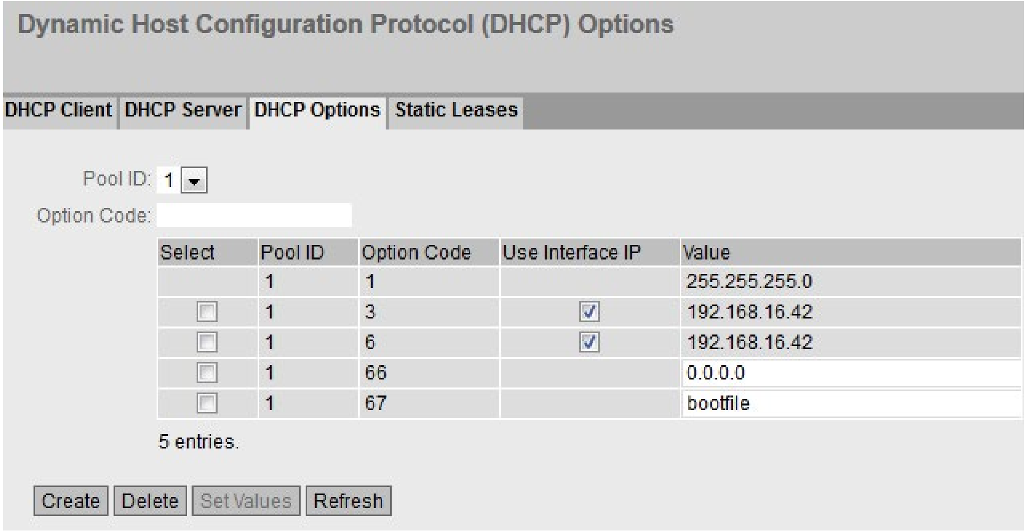
Note

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 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 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.

4.5.15.3 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		255.255.255.0
□	1	3	☑	192.168.16.42
□	1	6	☑	192.168.16.42
□	1	66		0.0.0.0
□	1	67		bootfile

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. A maximum of 20 DHCP options are possible.

  The various DHCP options are defined in RFC 2132.

  The DHCP options 1, 3, 6, 66 and 67 are created automatically when the IPv4 address band is created. With the exception of option 1, the options can be deleted.

  With the DHCP option 3, the internal IPv4 address of the device is automatically set as a DHCP parameter

  Note

  DHCP options not supported

  The DHCP options 50 - 60 and 255 are not supported.

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.
- **Options Code**
  Shows the number of the DHCP option.
- **Use Interface IP**
  Specify whether or not the internal IP address of the device will be used.
- **Value**
  Enter the value that is transferred to the DHCP client. The content depends on the DHCP option.

  Some examples of this are as follows:

  – DHCP option 1 (subnet mask)

    The subnet mask is entered automatically.

  – DHCP options 3 (Router) and 6 (DNS):

    Enter the DHCP parameter as an IPv4 address, e.g. 192.168.100.2. With DHCP option 6, you can specify several IPv4 addresses separated by commas.

  – DHCP option 66 (TFTP Server):

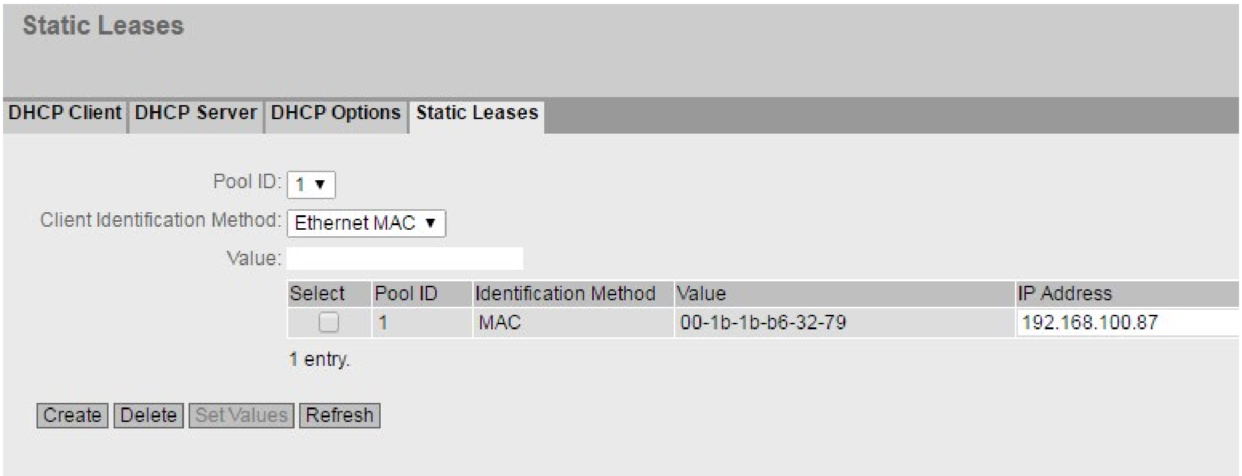
    Enter the DHCP parameter as an IPv4 address, e.g. 192.168.100.2 or the FQDN name. You can specify several IPv4 addresses separated by commas.

  – DHCP option 67 (boot file name)

    Enter the name of the boot file in the string format.

4.5.15.4 Static Leases

On this page you define that DHCP clients are assigned a preset IPv4 address depending on their client ID or MAC address.



Pool ID: 1 ▼

Client Identification Method: Ethernet MAC ▼

Value:

Select	Pool ID	Identification Method	Value	IP Address
□	1	MAC	00-1b-1b-b6-32-79	192.168.100.87

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 MAC address (Ethernet MAC) or the client ID 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.

- **HW Type**
  Shows whether the client is identified by its MAC address or the client ID.
- **Value**
  Shows the MAC address or 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.

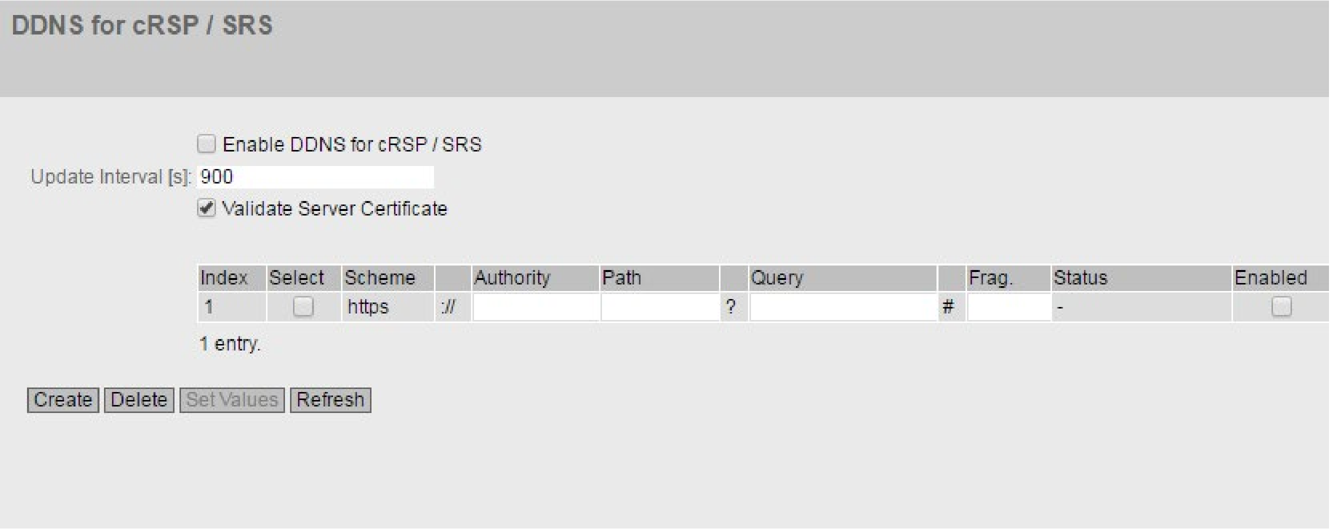
4.5.16 cRSP / SRS

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 (http://www.industry.siemens.com/topics/global/en/service/remote-service/seiten/home.aspx).

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**.

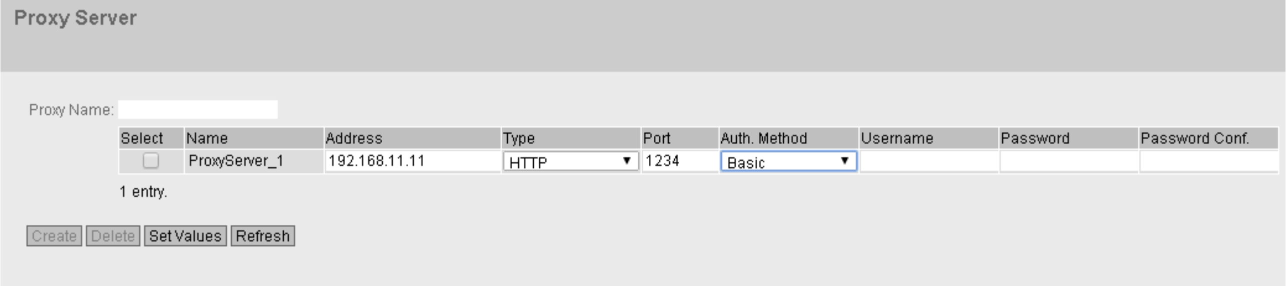
  Addresses local parts of the resource, e.g. the anchor attribute of a Web page.
- **Status**

  Shows the status of the last cRSP / SRS access of the entry.
- **Enabled**

  When enabled, this entry is used.

4.5.17 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.
□	ProxyServer_1	192.168.11.11	HTTP	1234	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 Conf.**

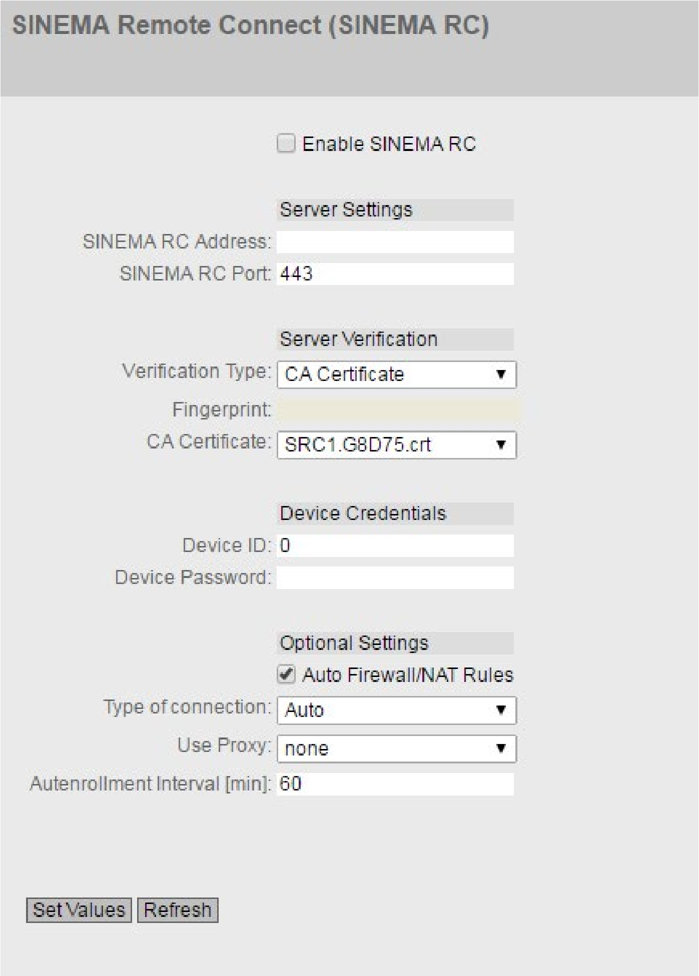
  Enter the password again to confirm it.

4.5.18 SINEMA RC

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

Note

This function can only be used with a KEY PLUG (Page 20).



SINEMA Remote Connect (SINEMA RC)

☐ Enable SINEMA RC

Server Settings

SINEMA RC Address:
SINEMA RC Port: 443

Server Verification

Verification Type: CA Certificate ▼
Fingerprint:
CA Certificate: SRC1.G8D75.crt ▼

Device Credentials

Device ID: 0
Device Password:

Optional Settings

☑ Auto Firewall/NAT Rules
Type of connection: Auto ▼
Use Proxy: none ▼
Autenrollment 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.

Range "Server Settings"

- **SINEMA RC Address**

  Enter the IPv4 address or the DNS host name of the SINEMA RC Server.
- **SINEMA RC Port**

  Enter the port via which the SINEMA RC Server can be reached.

Range "Server Verification"

- **Verifcation 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 "Fingerprint" setting. 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 “CA Certificate" setting. Select the CA certificate of the server used to sign the server certificate. Only loaded CA certificates can be selected.

Range "Device Credentials"

- **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.

Range "Optional Settings"

- **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 In

    The settings of the SINEMA RC server are ignored. If the "Digital In" event occurs, the device attempts to establish a VPN connection to the SINEMA RC Server. This is on condition that the event "Digital In" is passed onto the VPN connection. To do this, in "System > Events > Configuration" for the event "Digital In" activate "VPN Tunnel".
- **Use Proxy**

  Specify whether a 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".
- **Autenrollment Intervall [min]**

  Specify the period of time in minutes after which queries are sent to the SINEMA RC server. With these queries, the device checks whether there is a newer firmware file on the SINEMA RC server.

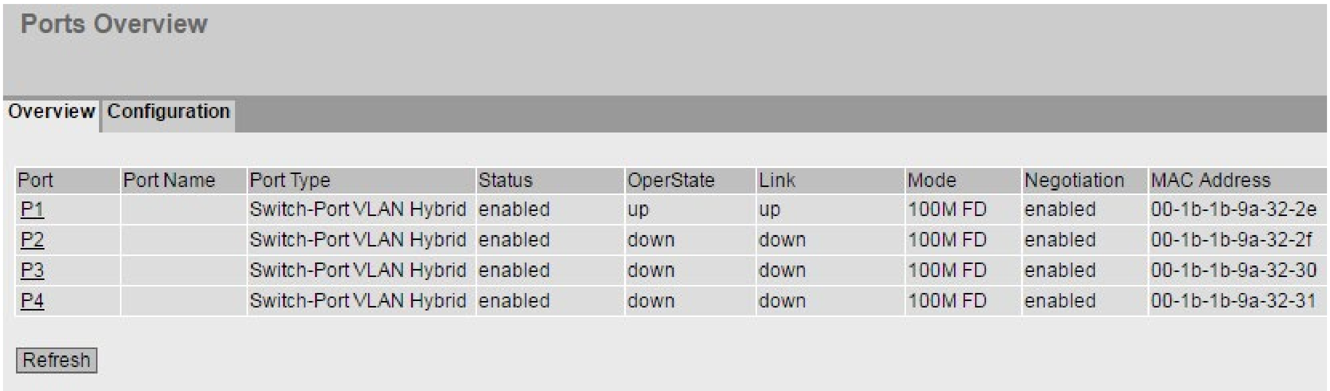
  If you enter the value 0, this function is disabled.

4.6 "Interfaces" menu

4.6.1 Ethernet

4.6.1.1 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	Negotiation	MAC Address
P1		Switch-Port VLAN Hybrid	enabled	up	up	100M FD	enabled	00-1b-1b-9a-32-2e
P2		Switch-Port VLAN Hybrid	enabled	down	down	100M FD	enabled	00-1b-1b-9a-32-2f
P3		Switch-Port VLAN Hybrid	enabled	down	down	100M FD	enabled	00-1b-1b-9a-32-30
P4		Switch-Port VLAN Hybrid	enabled	down	down	100M FD	enabled	00-1b-1b-9a-32-31

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.
- **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
- **Status**
  Shows whether the port is on or off. Data traffic is possible only over an enabled port.

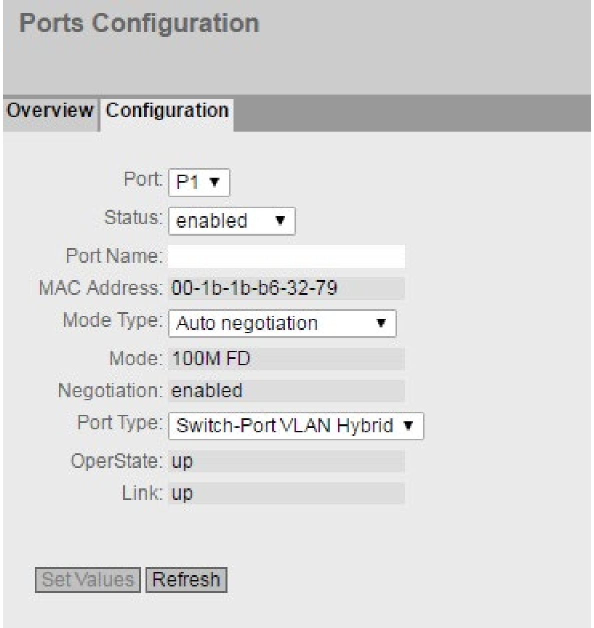
- **OperState**
  Displays the current operational status. The operational status depends on the configured "Status" and the "Link". The available options are as follows:
  - Up
    You have configured the status "enabled" for the port and the port has a valid connection to the network.
  - Down
    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.
- **MAC Address**

  Shows the MAC address of the port.

4.6.1.2 Configuration

Configuring ports

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



Ports Configuration

Port: P1 ▼
Status: enabled ▼
Port Name:
MAC Address: 00-1b-1b-b6-32-79
Mode Type: Auto negotiation ▼
Mode: 100M FD
Negotiation: enabled
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.

  The following settings are possible:

  – 10 Mbps full duplex (FD) or half duplex (HD)

  – 100 Mbps full duplex (FD) or half duplex (HD)

  – Auto negotiation

  If you set the mode to "Auto negotiation", these parameters are automatically negotiated with the connected end device or network component. This must also be in the "Autonegotiation" mode.

  Note

  Before the port and partner port can communicate with each other, the settings must match at both ends.

- **Mode**

  Shows the transmission speed and the transmission mode of the port. The display depends on the set "Mode Type".

- **Negotiation**

  Shows whether the automatic configuration of the connection to the partner port is enabled or disabled.

- **MTU**

  MTU (Maximum Transmission Unit) specifies the maximum size of the packet. If packets are longer than the set MTU they are fragmented.

  The range of values is from 64 to 1500 bytes.

- **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.

- **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 physical connection status to the network. The available options are as follows:

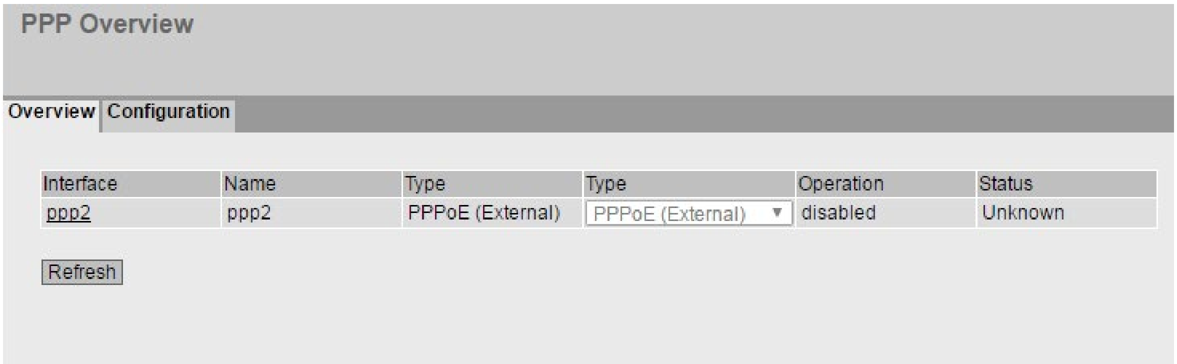
  – Up
    The port has a valid link to the network, a link integrity signal is being received.

  – Down
    The link is down, for example because the connected device is turned off.

4.6.2 PPP

4.6.2.1 Overview

The page shows the status of the PPP connection.



PPP Overview

Interface	Name	Type	Type	Operation	Status
ppp2	ppp2	PPPoE (External)	PPPoE (External)	disabled	Unknown

Description of the displayed values

This table contains the following columns:

- **Interface**

  Shows the PPP interface. The entry is a link. If you click on the link, the corresponding configuration page is opened.

- **Name**

  Shows the name of the PPP interface.

- **Type**

  Shows the protocol of the PPP connection.
- **Operation**

  Shows whether the PPP connection is activated or deactivated.
- **Status**

  Shows the status of the PPP connection.
  - Ready

    The PPP connection can be configured and enabled.
  - Connecting

    The PPP connection is configured, enabled and the connection is being established.
  - Connected

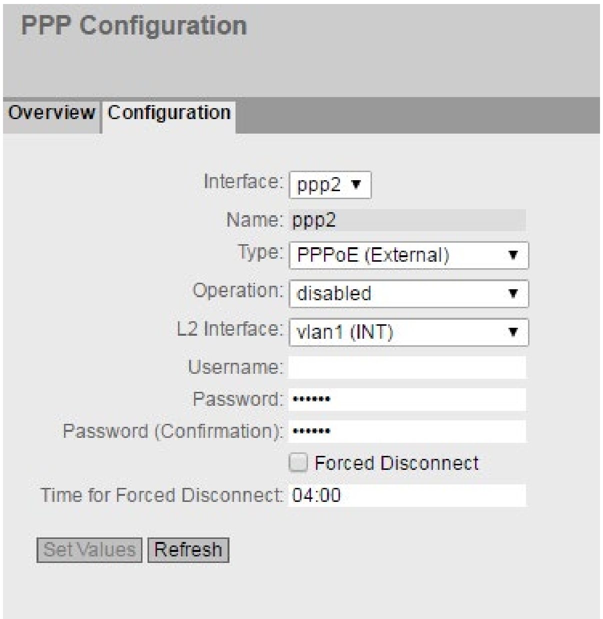
    The PPP connection is established.
  - Error

    Error status in which operator intervention is required, e.g. wrong password.

4.6.2.2 Configuration

On this page, you configure the PPP connection. The point-to-point protocol (PPP) allows the connection of an external ADSL modem to an Ethernet interface and via this then a connection to the Internet. The interface is also called PPP interface.

The device acts as a router and logs in with the user name and password. All connected devices can use the PPP connection.



PPP Configuration

Interface: ppp2 ▼
Name: ppp2
Type: PPPoE (External) ▼
Operation: disabled ▼
L2 Interface: vlan1 (INT) ▼
Username:
Password: ••••••
Password (Confirmation): ••••••
□ Forced Disconnect
Time for Forced Disconnect: 04:00

Description

The page contains the following:

- **Interface**

  Select the PPP interface to be configured.

- **Name**

  Shows the name of the PPP interface. You can change the name in "Layer 3 > Subnets".

- **Type**

  Specify the protocol for the PPP connection.

  – PPPoE (Point-to-Point over Ethernet)

    The PPP data is encapsulated in an Ethernet frame.

- **Operation**

  Specify whether the PPP connection is activated or deactivated.

- **L2 Interface**

  Specify the interface via which the PPP connection is established. Only VLANs with a configured subnet can be selected.

- **User Name**

  Enter the user name. You will receive the user name from the DSL provider.

- **Password**

  Enter the password. You will receive the password from the DSL provider.

- **Password (Confirmation**)

  Repeat the password.

- **Forced Disconnect**

  After a certain time, the DSL provider terminates the connection. Enable this option if you want to shift the forced disconnect of your provider to a specific time of day, for example at night outside normal office hours.

- **Time for Forced Disconnect**

  Specify the time of day to which you want to shift the forced disconnect of the DSL provider. This is only possible if the correct system time is set on the device.

  Input format: HH:MM

Procedure

1. Specify how the PPP interface obtains the IP address. The following options are available:

   – Dynamic

     Activate the Dynamic function on the PPP interface. You can configure this setting in "Layer 3 > Subnets > Configuration".

     Note

     - With the subnets, a maximum of one interface can have a dynamic IP configuration.

   – Static IP address

     Deactivate the Dynamic function on the PPP interface. Enter the IP address and the subnet mask.

2. Configure the PPP interface.
3. Select the "Enabled" operation to activate the PPP interface.
4. Click "Set Values" to adopt the settings.

4.7 "Layer 2" menu

4.7.1 VLAN

4.7.1.1 General

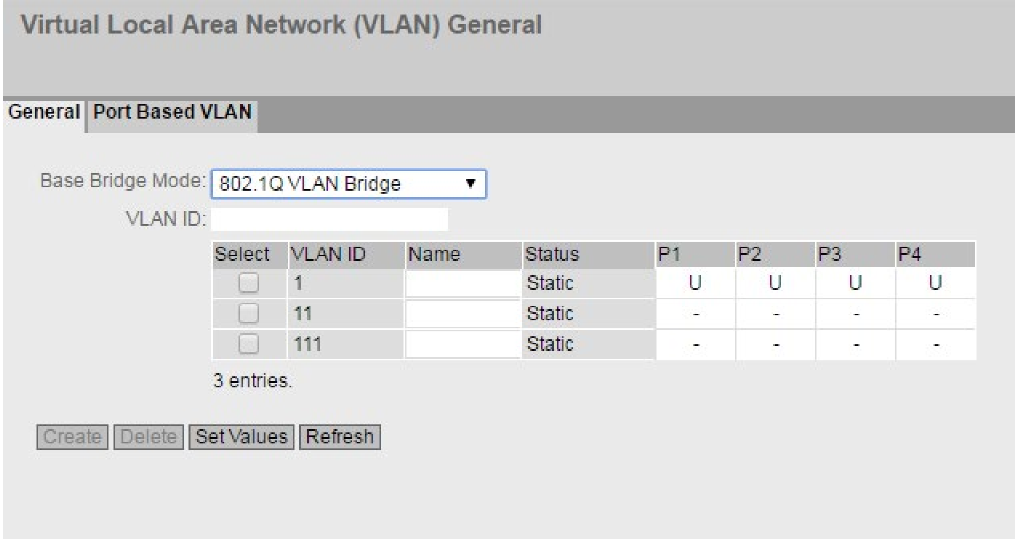
VLAN configuration page

On this page you specify whether or not the device forwards frames with VLAN tags transparently (IEEE 802.1D/VLAN-unaware mode) or 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 .

Note

Changing the agent VLAN ID

If the configuration PC is connected directly to the device via Ethernet and you change the agent VLAN ID, the device is no longer reachable via Ethernet following the change.



Base Bridge Mode: 802.1Q VLAN Bridge ▼
VLAN ID:

Select	VLAN ID	Name	Status	P1	P2	P3	P4
☐	1		Static	U	U	U	U
☐	11		Static	-	-	-	-
☐	111		Static	-	-	-	-

3 entries.

Description

The page contains the following boxes:

- **Base Bridge Mode**

  Select the required mode from the drop-down list. The following modes are possible:

  Note

  Changing Base Bridge mode

  Note the section "Changing Base Bridge mode". This section describes how a change affects the existing configuration.

  – 802.1D Transparent Bridge
    Sets the mode "VLAN-unaware" for the device. In this mode, VLAN tags are not taken into account or changed but are forwarded transparently. In this mode, you cannot create any VLANs.

  – 802.1Q VLAN Bridge
    Sets the mode "VLAN-unaware" for the device. In this mode, VLAN tags are not taken into account or changed but are forwarded transparently. In this mode, you cannot create any VLANs. Only a management VLAN is available: VLAN 1.

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

- **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. Up to 24 VLANs can be defined.

- **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 address was entered as a static address 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. You can configure other settings in "Layer 2 > VLAN > Port-based VLAN".

Changing Base Bridge mode

VLAN-unaware (802.1D transparent bridge) → VLAN-aware (802.1Q VLAN bridge)

If you change the Base Bridge mode from VLAN-unaware to VLAN aware, this has the following effects

- All static and dynamic unicast entries are deleted.

VLAN-aware (802.1Q VLAN bridge) → VLAN-unaware (802.1D transparent bridge)

If you change the Base Bridge mode from VLAN-aware to VLAN-unaware, this has the following effects:

- All VLAN configurations are deleted.
- A management VLAN is created: VLAN 1.
- All static and dynamic unicast entries are deleted.

802.1Q VLAN Bridge: Important rules for VLANs

Make sure you keep to the following rules when configuring and operating your VLANs:

- Frames with the VLAN ID "0" are handled as untagged frames but retain their priority value.
- As default, all ports on the device send frames without a VLAN tag to ensure that the end node can receive these frames.
- In the factory, the VLAN ID "1" is the default on all ports.

- 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.
- If an end node is connected to a port, outgoing frames should be sent without a tag (static access port). If, however, there is a further switch at this port, the frame should have a tag added (trunk port).

Procedure

Requirement:

In Base Bridge mode "802.1Q VLAN Bridge" is set.

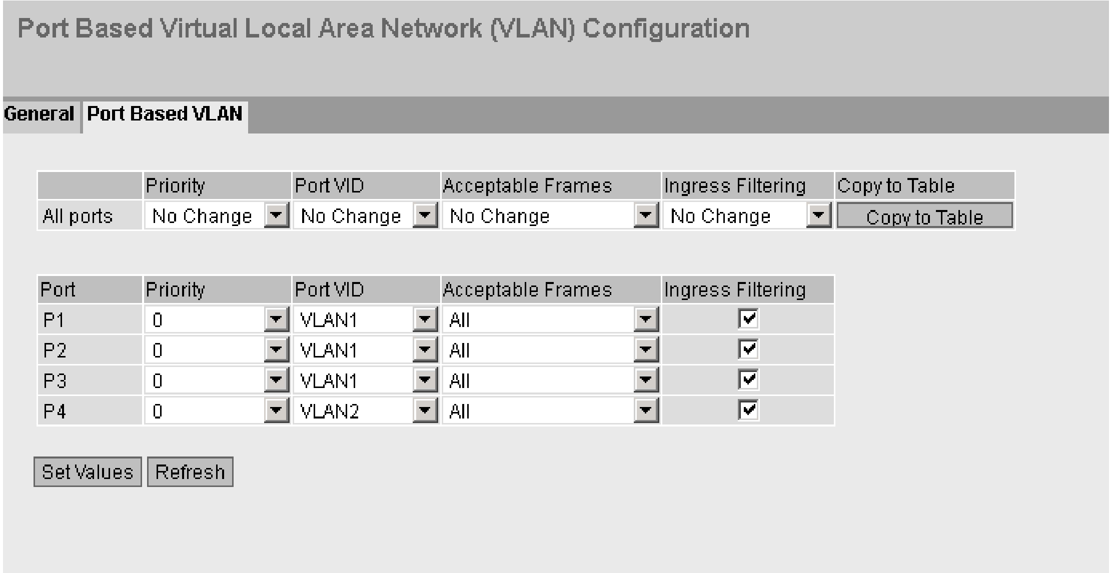
Creating a new VLAN

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.

4.7.1.2 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	VLAN2	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.

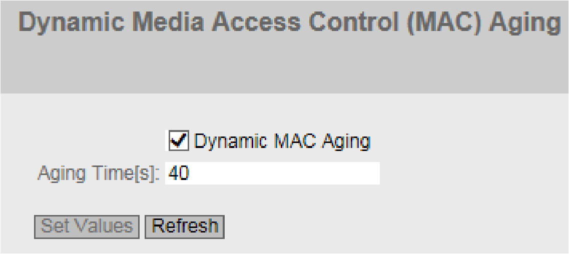
Steps in configuration

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.

4.7.2 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]: 40

Description

The page contains the following boxes:

- **"Dynamic MAC Aging" check box**
  Enable or disable the function for automatic aging of learned MAC addresses:
- **"Aging Time [s]" input box**
  Enter the time in seconds. After this time, a learned address is deleted if the device does not receive any further frames from this sender address. The range of values is from 10 seconds to 1000000 seconds

Procedure

1. Select the "Dynamic MAC Aging" check box.
2. Enter the time in seconds in the "Aging Time [s]" input box.
3. Click the "Set Values" button.

4.7.3 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.

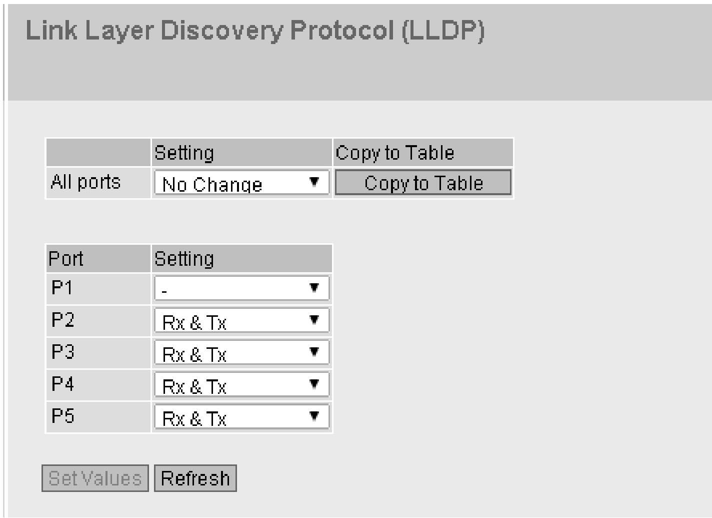
Network components that support LLDP have an LLDP agent. The LLDP agent sends information about itself and receives information from connected devices at periodic intervals. The received information is stored in the MIB.

Applications

PROFINET uses LLDP for topology diagnostics. In the default setting, LLDP is enabled for ports p1 - P4; in other words, LLDP frames are sent and received 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	- ▼
P2	Rx & Tx ▼
P3	Rx & Tx ▼
P4	Rx & Tx ▼
P5	Rx & Tx ▼

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. 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 port.
- **Setting**
  Specify the LLDP functionality. The following options are available:
  - Tx
    This port can only send LLDP frames.
  - Rx
    This port can only receive LLDP frames.
  - Rx & Tx
    This port can receive and send LLDP frames.
  - "-" (Disabled)
    This port can neither receive nor send LLDP frames.

Procedure

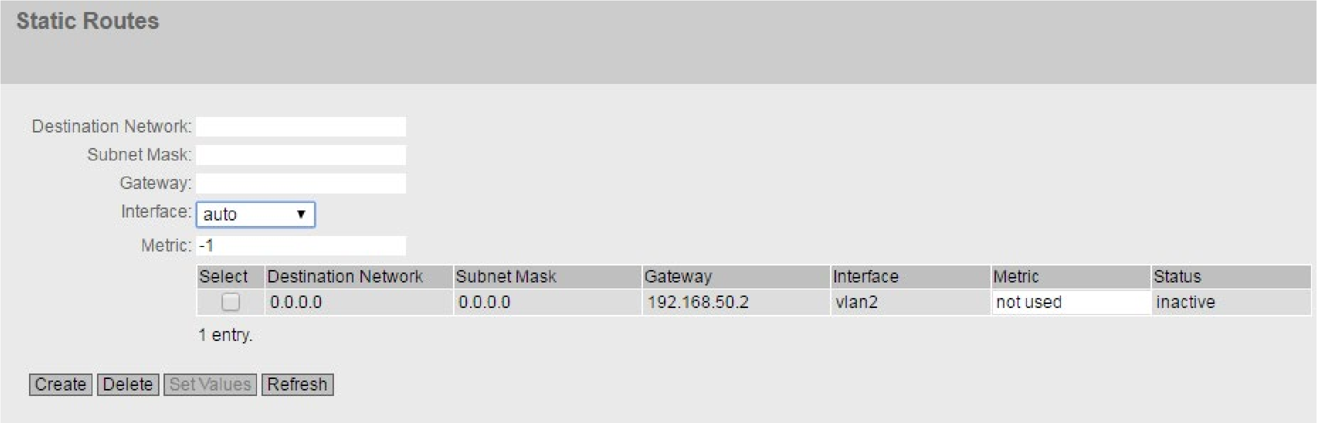
1. Select the required LLDP functionality from the drop-down list.
2. Click the "Set Values" button.

4.8 "Layer 3" menu

4.8.1 Static routes

Static route

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



Static Routes

Destination Network:
Subnet Mask:
Gateway:
Interface: auto
Metric: -1

Select	Destination Network	Subnet Mask	Gateway	Interface	Metric	Status
□	0.0.0.0	0.0.0.0	192.168.50.2	vlan2	not used	inactive

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 IP address of the gateway via which this network address can be reached.
- **Metric**
  Enter the metric for the route. The metric 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 used automatically. The metric can be changed later.

  Range of values: 1 - 254 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 IP address of the next gateway.
- **Interface**
  Shows the Interface of the route.
- **Metric**
  When creating the route, "not used" is entered automatically. The metric 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.
  Range of values: 1 - 254 or -1 for "not used". 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.

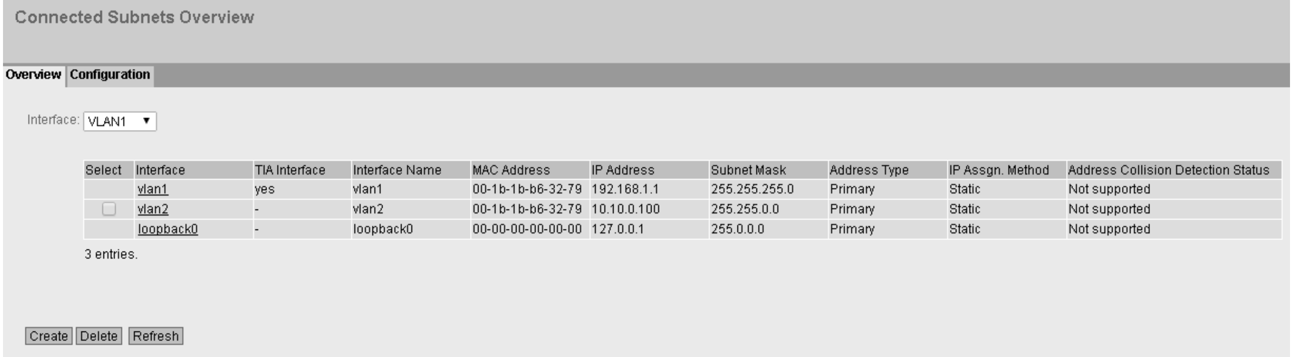
Procedure

1. Enter the network address of the destination in "Destination Network".
2. Enter the corresponding subnet mask in "Subnet Mask".
3. For "Interface" select the entry "auto".
4. Enter the gateway in "Gateway".
5. Enter the weighting of the route in "Metric".
6. Click the "Create" button. A new entry is generated in the table.

4.8.2 Subnets

4.8.2.1 Overview

The page shows the subnets for the selected interface. A subnet always relates to an interface and is created in the "Configuration" tab.



Interface: VLAN1

Select	Interface	TIA Interface	Interface Name	MAC Address	IP Address	Subnet Mask	Address Type	IP Assgn. Method	Address Collision Detection Status
	vlan1	yes	vlan1	00-1b-1b-b6-32-79	192.168.1.1	255.255.255.0	Primary	Static	Not supported
☐	vlan2	-	vlan2	00-1b-1b-b6-32-79	10.10.0.100	255.255.0.0	Primary	Static	Not supported
	loopback0	-	loopback0	00-00-00-00-00-00	127.0.0.1	255.0.0.0	Primary	Static	Not supported

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 to which the settings relate.
- **TIA Interface**
  Shows the selected TIA interface.
- **Interface Name**
  Shows the name of the interface.
- **MAC Address**
  Shows the MAC address of the interface.
- **IP Address**
  Shows the IP address of the subnet.
- **Subnet Mask**
  Shows the subnet mask.
- **Address Type**
  Displays the address type. The following values are possible:
  - Primary
    The first IPv4 address that was configured on an IP interface.
  - Secondary
    All other IP addresses that were configured on an interface.

- **IP Assign. Method**
  Shows how the IP address is assigned. The following values are possible:
  - Static
    The IP address is static. Enter the IP settings in "IP Address" and "Subnet Mask".
  - Dynamic (DHCP)
    The device obtains a dynamic IP address from a DHCP server.
- **Address Collision Detection Status**

  Shows the current status of the function. If new IP addresses become active in the network, the "Address Collision Detection" function checks whether this can result in address collisions. The allows IP addresses that would be assigned twice to be detected.

  Note

  The function does not run a cyclic check.

  The following values are possible:
  - Idle

    The interface is not enabled and does not have an IP address.
  - Starting

    This status indicates the start-up phase. In this phase, the device initially sends a query as to whether the planned IP 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 IP address that has already been assigned.
  - Defending

    The interface uses a unique IP address. Another interface is attempting to use the same IP address.
  - Active

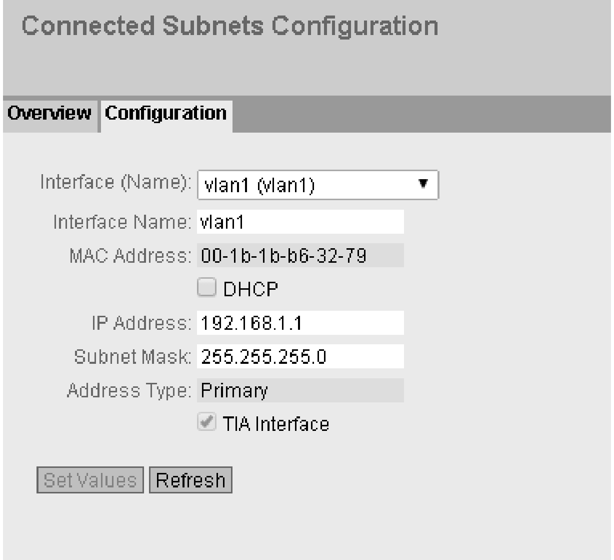
    The interface uses a unique IP address. There are no collisions.
  - Not supported

    The function for detection of address collisions is not supported.
  - Disabled

    The function for detection of address collisions is disabled.

4.8.2.2 Configuration

On this page, you configure the subnet for the interface.



Connected Subnets Configuration

Interface (Name): vlan1 (vlan1) ▼

Interface Name: vlan1

MAC Address: 00-1b-1b-b6-32-79

☐ DHCP

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Address Type: Primary

☑ TIA Interface

Description

The page contains the following:

- **Interface (Name)**
  Select the required interface.
- **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 the interface.

  Note

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

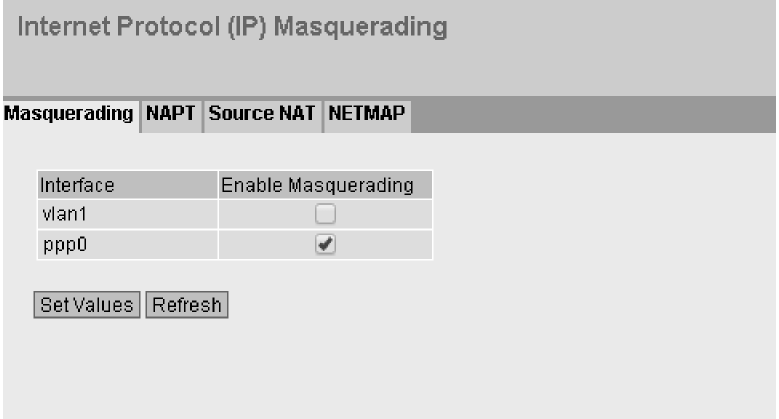
- **IP Address**
  Enter the IP address of the interface. IP addresses must not be used more than once.
- **Subnet Mask**
  Enter the subnet mask of the subnet you are creating. Subnets on different interfaces must not overlap.

- **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**
  Specify whether or not this interface will become the TIA Interface.

4.8.3 NAT

4.8.3.1 Masquerading

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



Internet Protocol (IP) Masquerading

Interface	Enable Masquerading
vlan1	☐
ppp0	☑

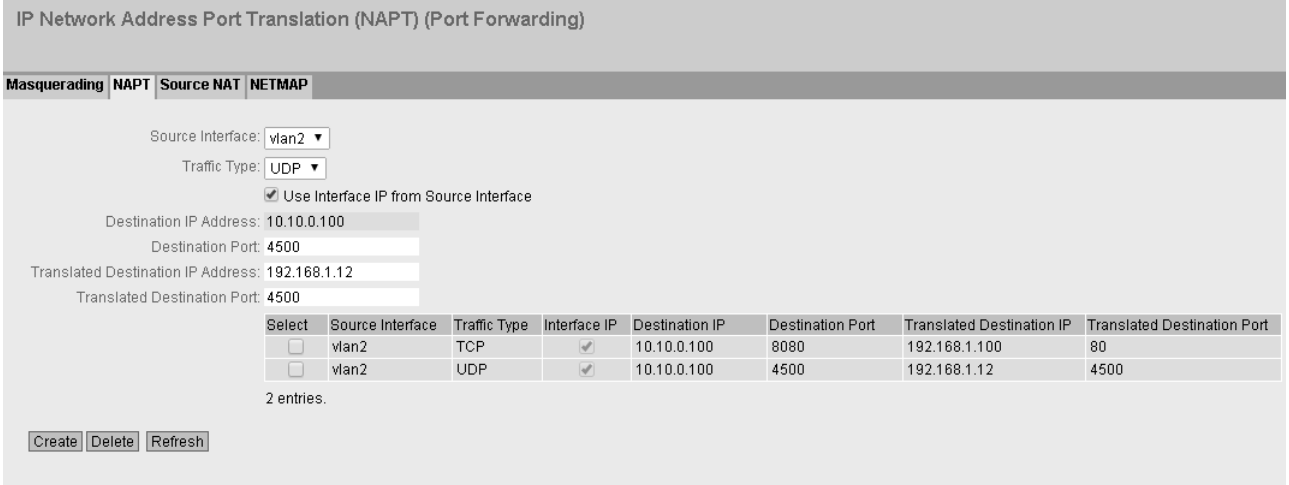
Description

The table has the following columns:

- **Interface**
  Interface to which the setting relates. Only interfaces with a configured subnet 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.

4.8.3.2 NAPT

On this WBM page, you configure port forwarding.



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

Source Interface: vlan2 ▼

Traffic Type: UDP ▼

☑ Use Interface IP from Source Interface

Destination IP Address: 10.10.0.100

Destination Port: 4500

Translated Destination IP Address: 192.168.1.12

Translated Destination Port: 4500

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

2 entries.

Description

The page contains the following boxes:

- **Source Interface**

  Select the the interface for which you want to create further NAT configurations. Can only be selected if the device has several interfaces.

- **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 "Destination 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 Address**

  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.

  If the Destination Port and the Translated Destination Port are the same, the frames will be forwarded without port translation.

  Note

  If the port is already occupied by a local service, for example Telnet, a warning is displayed.
  Make sure that you avoid using the following ports: TCP port 23 (Telnet), port 22 (SSH), the ports 80/443 (http/https: reachability of the client with the WBM), UDP port 161 (SNMP), port 500 (ISAKMP), port 4500 (IPsec Nat-T).

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**

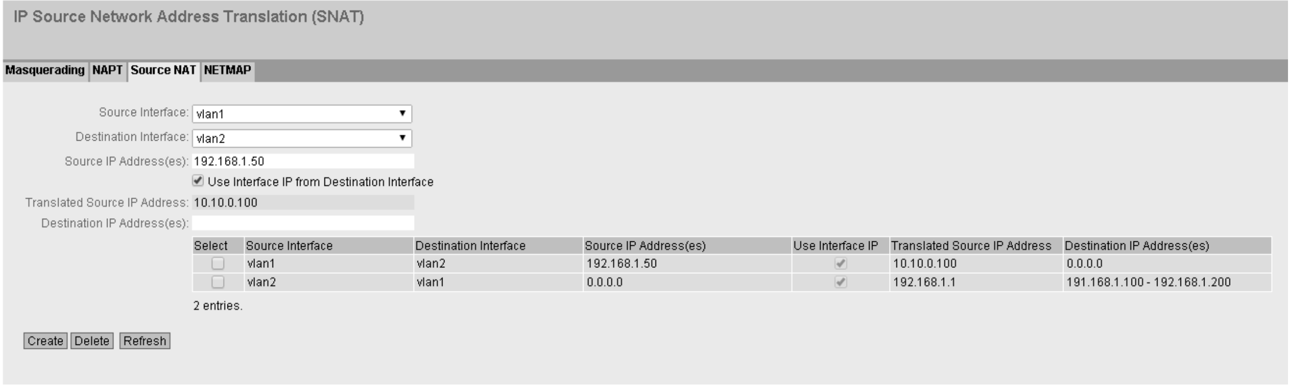
  Shows the IP address of the node to which the packets will be forwarded.

- **Translated Destination Port**

  Shows the destination port to which the packets are translated.

4.8.3.3 Source NAT

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



IP Source Network Address Translation (SNAT)

Source Interface: vlan1

Destination Interface: vlan2

Source IP Address(es): 192.168.1.50

☑ Use Interface IP from Destination Interface

Translated Source IP Address: 10.10.0.100

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
□	vlan2	vlan1	0.0.0.0	☑	192.168.1.1	191.168.1.100 - 192.168.1.200

2 entries.

Note

Firewall rules with source NAT

If you create a firewall rule for a source NAT rule use the entry "Source IP Subnet" for "IP Rules" for the "Source (Range)" And for "Destination (Range)" use the entry from "Destination IP Subnet".

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

  – ppp0 or usb0 (only with M876-4): WAN interface

  – 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)" input box**

  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.

  – 0.0.0.0/0: Applies to all IP addresses

  – IP address range: Applies to the specified IP address range: Start IP address "-" End IP address, e.g. 192.168.100.10 - 192.168.100.20

  – IP address band: Applies to the IP addresses covered in the IP address band: 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 destination 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.

  – 0.0.0.0/0: Applies to all IP addresses

  – IP address range: Applies to the specified IP address range: Start IP address "-" End IP address, e.g. 192.168.100.10 - 192.168.100.20

  – IP address band: Applies to the IP addresses covered in the IP address band: IP address/number of bits of the network part (CIDR notation)

The table has the following columns:

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

- Source Interface
  Shows the source interface.

- Destination Interface
  Shows the destination interface.

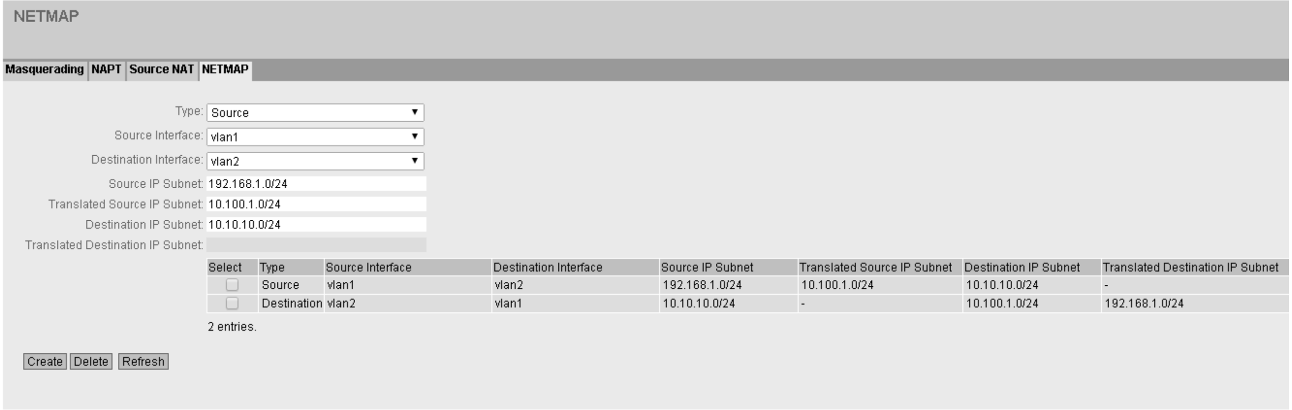
- Source IP Address(es)
  Shows the IP addresses of the senders for which address translation is required.

- Translated 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.

4.8.3.4 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. For more information, refer to the section "NAT and firewall".



Type:	Source ▼
Source Interface:	vlan1 ▼
Destination Interface:	vlan2 ▼
Source IP Subnet:	192.168.1.0/24
Translated Source IP Subnet:	10.100.1.0/24
Destination IP Subnet:	10.10.10.0/24
Translated Destination IP Subnet:	

Select	Type	Source Interface	Destination Interface	Source IP Subnet	Translated Source IP Subnet	Destination IP Subnet	Translated Destination IP Subnet
□	Source	vlan1	vlan2	192.168.1.0/24	10.100.1.0/24	10.10.10.0/24	-
□	Destination	vlan2	vlan1	10.10.10.0/24	-	10.100.1.0/24	192.168.1.0/24

2 entries.

Note

Firewall rules with source NAT

If you create a firewall rule for a source NAT rule use the entry "Source IP Subnet" for "IP Rules" for the "Source (Range)" And for "Destination (Range)" use the entry from "Destination IP Subnet".

Firewall rules with destination NAT

If you create a firewall rule for a destination NAT rule use the entry "Translated Destination IP Subnet" for "IP Rules" for the "Source (Range)" And for "Destination (Range)" use the entry from "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

  – ppp0 or usb0 (only with M876-4): WAN interface

  – 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 "SourceNAT" 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 "DestinationNAT" settings.
  The subnet can also be a single PC or another subset of the subnet. Use the CIDR notation.

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.

4.9 "Security" menu

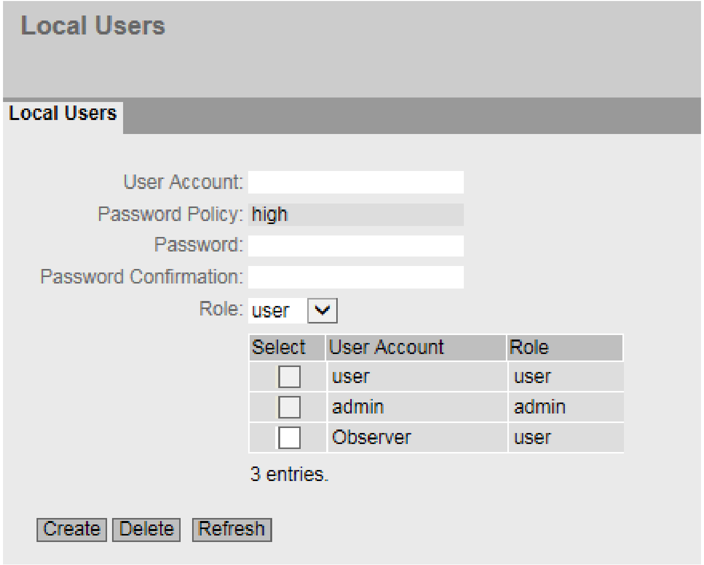
4.9.1 User Accounts

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 16 additional user accounts.



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

Select	User Account	Role
□	user	user
□	admin	admin
□	Observer	user

3 entries.

Description

The page contains the following:

- **User Account**

  Enter the name for the user. The name must meet the following conditions:

  – It must be unique.

  – It must be between 1 and 32 characters.

  – The following characters must not be included: § ? " ; : < =

  – The following user names are not allowed: admin, user, service, debug

  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, user, service, debug

  When shipped the following user names are predefined in the factory. user, admin, service, debug.

  - admin: You can configure the device with this user name. If you log on the first time or log on after a "Restore Factory Defaults and Restart", you will be prompted to change the predefined password "admin".
  - user, service, debug: These user names are reserved for service purposes.

- **Password Policy**

  Shows which password policy is being used.

  Note

  Password policy: high

  Note the following password policies:

  - Password length: at least 8 characters
  - At least 1 uppercase letter
  - At least 1 special character
  - At least 1 number

- **Password**

  Enter the password for the user.

- **Password Confirmation**

  Enter the password again to confirm it.

- **Role**

  Specify the role of the user.

  - admin
    The user can create, edit or delete entries.
  - user
    The user only has read rights.

The table contains the following columns:

- **Select**
  Select the check box in the row to be deleted. Default users "admin" and "user" as well as logged in users cannot be deleted.
- **User Account**
  Shows the user name.
- **Role**
  Shows the role of the user.

Procedure

Creating a user account

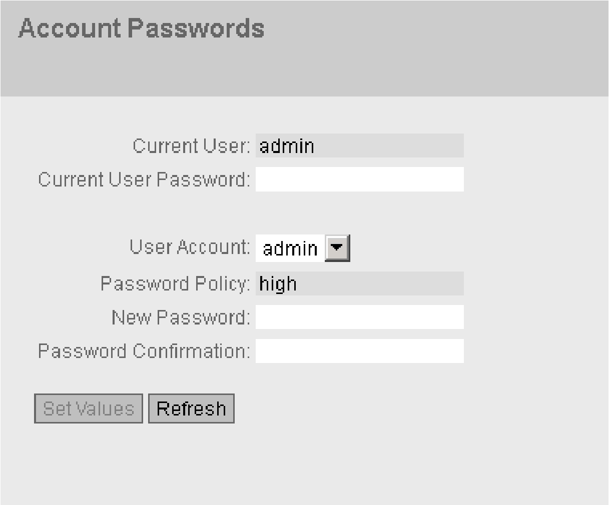
1. Enter the name for the user.
2. Enter the password for the user.
3. Enter the password again to confirm it.
4. Select the role of the user.
5. Click the "Set Values" button.

Deleting a user account

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.

4.9.2 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 currently logged in user.

- **"Current User Password"** input box

  Enter the currently valid password.

- **"User Account"** drop-down list

  – If the current user has the "admin" role, he or she can select a user for whom the password will be changed.

  – If the current user has the "user" role, his or her user name is set automatically.

- **Password Policy**

  Shows the password policy that the password must fulfill.

- **"New Password"** input box

  Enter the new password for the selected user.

  Note

  Password policy: high

  Note the following password policies:

  - Password length: at least 8 characters
  - At least 1 uppercase letter
  - At least 1 special character
  - At least 1 number

- **"Password Confirmation"** input box

  Repeat the new password and click the "Set Values" button.

  Note

  The factory setting for the user "admin" is the password "admin" when the device ships.

  If you log on the first time or log on after a "Restore Factory Defaults and Restart", you will be prompted to change the password.

  Note

  Changing the password in Trial mode

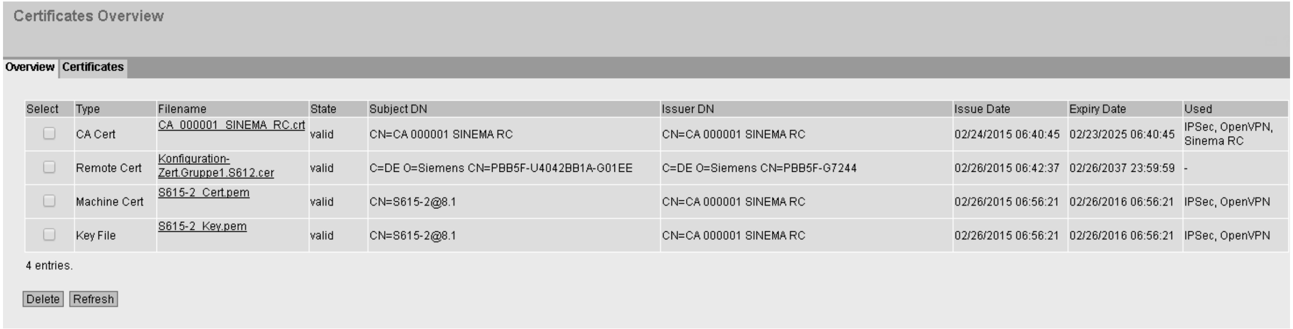
  Even if you change the password in Trial mode, this change is saved immediately.

4.9.3 Certificates

4.9.3.1 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



Select	Type	Filename	State	Subject DN	Issuer DN	Issue Date	Expiry Date	Used
□	CA Cert	CA_000001_SINEMA_RC.crt	valid	CN=CA 000001 SINEMA RC	CN=CA 000001 SINEMA RC	02/24/2015 06:40:45	02/23/2025 06:40:45	IPSec, OpenVPN, Sinema RC
□	Remote Cert	Konfiguration-Zert.Gruppe1.S612.cer	valid	C=DE O=Siemens CN=PBB5F-U4042BB1A-G01EE	C=DE O=Siemens CN=PBB5F-G7244	02/26/2015 06:42:37	02/26/2037 23:59:59	-
□	Machine Cert	S615-2_Cert.pem	valid	CN=S615-2@8.1	CN=CA 000001 SINEMA RC	02/26/2015 06:56:21	02/26/2016 06:56:21	IPSec, OpenVPN
□	Key File	S615-2_Key.pem	valid	CN=S615-2@8.1	CN=CA 000001 SINEMA RC	02/26/2015 06:56:21	02/26/2016 06:56:21	IPSec, OpenVPN

4 entries.

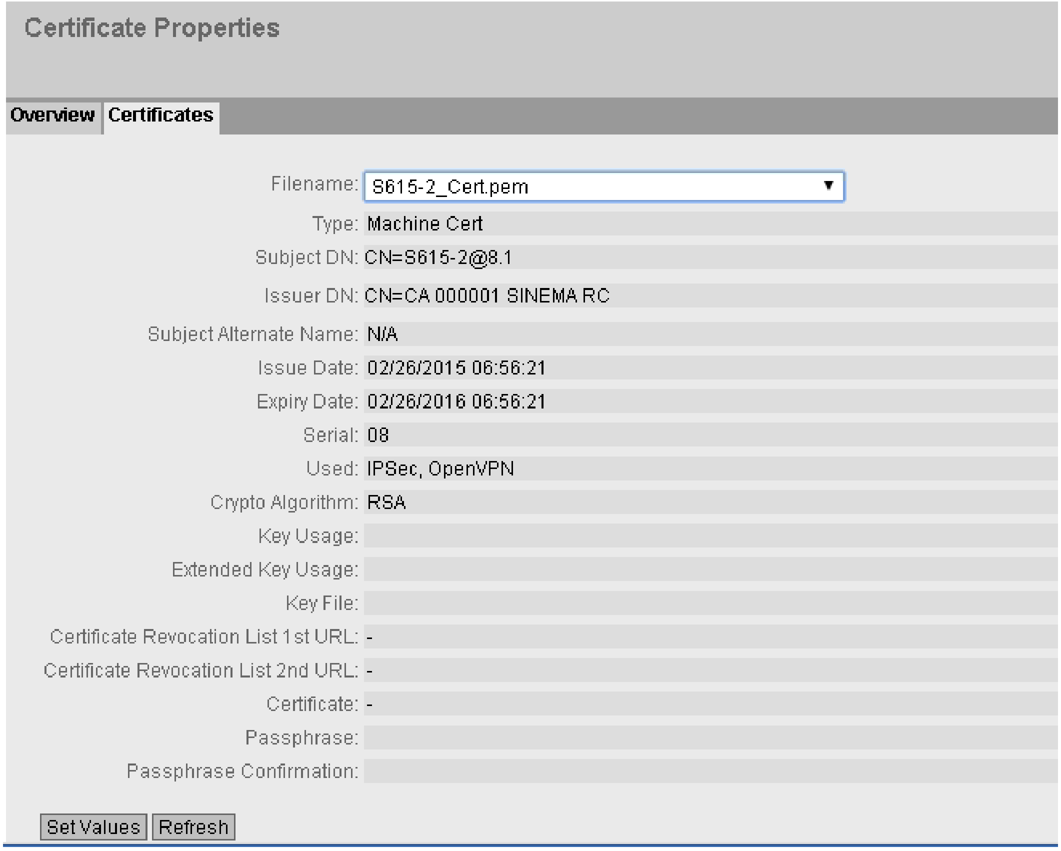
Description

- **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 Cert
    Machine certificate
  - Key File
    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 certificate owner.
- **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 the certificate uses.

4.9.3.2 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 X509 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: S615-2_Cert.pem
Type: Machine Cert
Subject DN: CN=S615-2@8.1
Issuer DN: CN=CA 000001 SINEMA RC
Subject Alternate Name: N/A
Issue Date: 02/26/2015 06:56:21
Expiry Date: 02/26/2016 06:56:21
Serial: 08
Used: IPSec, OpenVPN
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

- **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 Cert
    Machine certificate
  - Key File
    Key file
  - Remote Cert
    Partner certificate
- **Subject DN**
  Shows the name of the certificate owner.
- **Issuer DN**
  Shows the name of the certificate issuer.
- **Subject Alternate Name**
  If it exists, an alternative name of the certificate issuer 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**
  Shows the serial number of the certificate.
- **Used**
  Shows which function the certificate uses.
- **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.

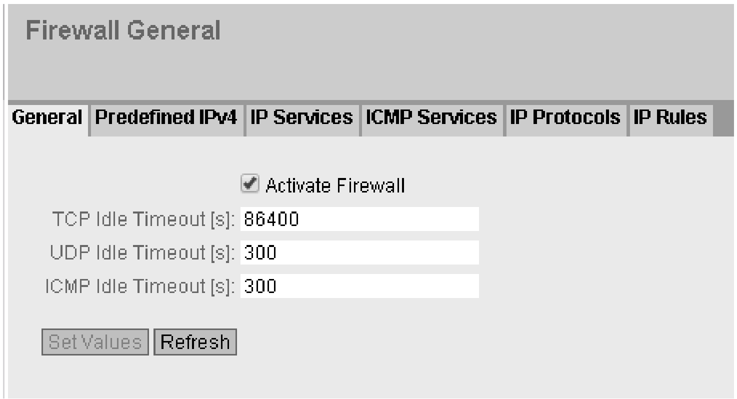
4.9.4 Firewall

4.9.4.1 General

On this WBM page, you enable the firewall.

Note

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



Firewall General

☑ 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" check box**

  When enabled, the firewall is active.

- **"TCP Idle Timeout [s]" input box**

  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 4294967295.

  Default setting: 86400 seconds

- **"UDP Idle Timeout [s]" input box**
  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 4294967295.

  Default setting: 300 seconds

- **"ICMP Idle Timeout [s]" input box**
  Enter the required time in seconds. If no data exchange takes place, the ICMP connection is terminated automatically when this time has elapsed.

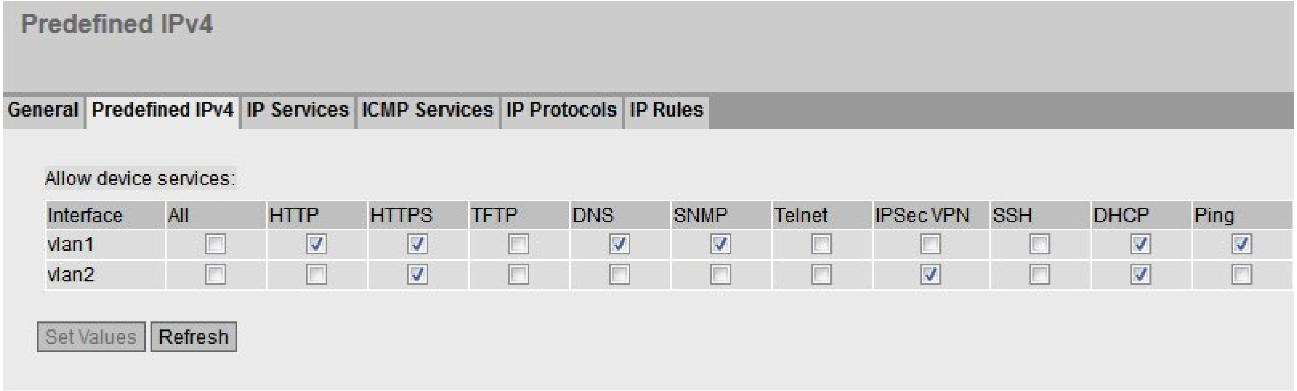
  The range of values is 1 to 4294967295.

  Default setting: 300 seconds

4.9.4.2 Predefined IPv4

The WBM page contains predefined IPv4 rules. If you create user-defined IPv4 rules, these have a higher priority than the predefined IPv4 rules.

Here, you can set which services of the device should be reachable from which VLAN interface/subnet. The list of VLAN interfaces/subnets is dynamic and is based on the settings from "Layer 3 >Subnetz.



Allow device services:

Interface	All	HTTP	HTTPS	TFTP	DNS	SNMP	Telnet	IPSec VPN	SSH	DHCP	Ping
vlan1	□	☑	☑	□	☑	☑	□	□	□	☑	☑
vlan2	□	□	☑	□	□	□	□	☑	□	☑	□

Description

- **Interface**
  VLAN interface to which the setting relates. Only VLANs with a configured subnet are available.
- 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

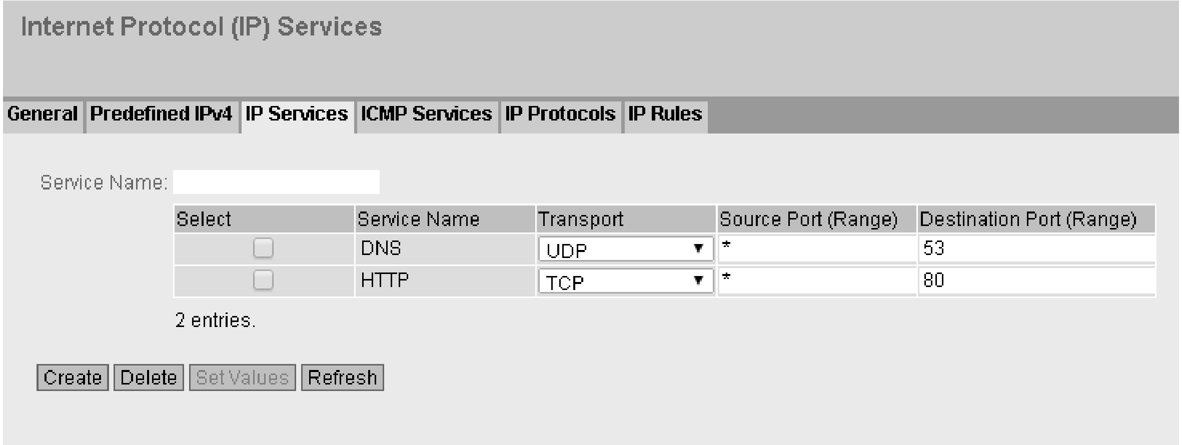
    Access using HTTP / HTTPS

    If you disable both firewall rules, the WBM of the device can no longer be reached.
  - TFTP
    For communication using TFTP. Necessary only, for example to access the device using a TFTP client.

- DNS
  DNS queries to the device. Necessary only if the "DNS-Relay" 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.
- Telnet
  For unencrypted access to the CLI.
- SMS Relay (M874 only)
  For sending SMS messages from the local network.
- 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

4.9.4.3 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.


Internet Protocol (IP) Services

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" input box**
  Enter the name of the IP service. The name must be unique.

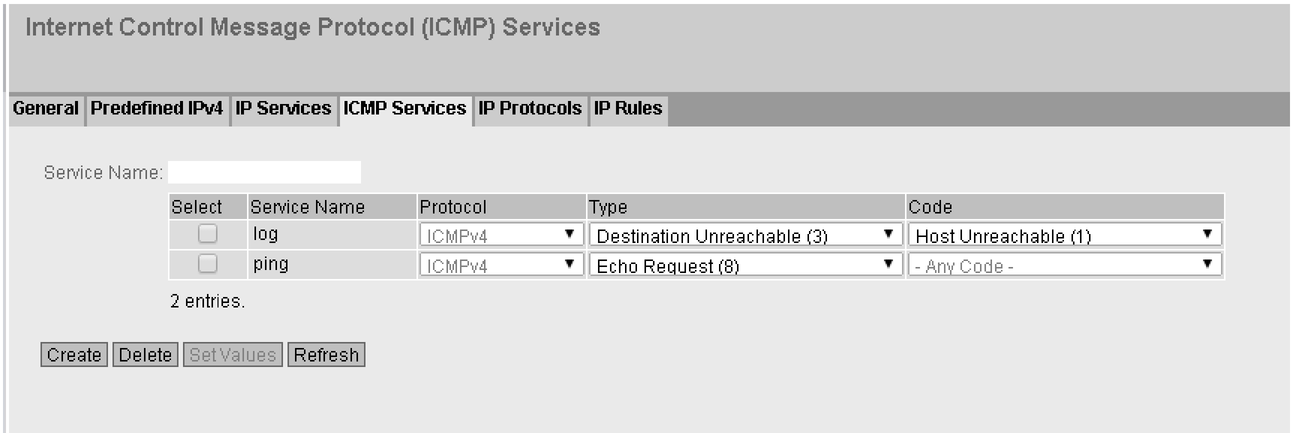
This table contains the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **Service Name**
  Shows the name of the 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 "*".

4.9.4.4 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" input box**
  Enter a name for the ICMP service. The name must be unique.

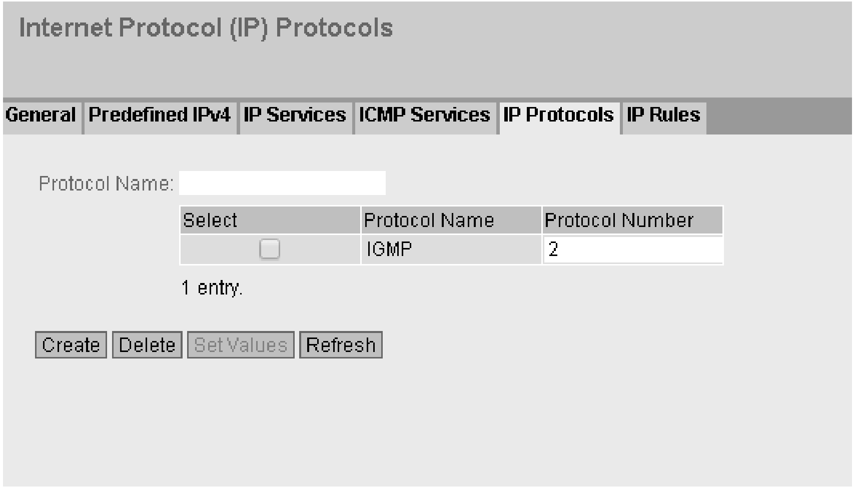
This table contains the following columns:

- **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.

4.9.4.5 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.



Protocol Name:

Select	Protocol Name	Protocol Number
□	IGMP	2

1 entry.

Description

The page contains the following:

- **"Protocol Name" input box**
  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, e.g. 2. You will find a list of protocol numbers on the Internet pages of iana.org

Procedure

Create IGMP protocol

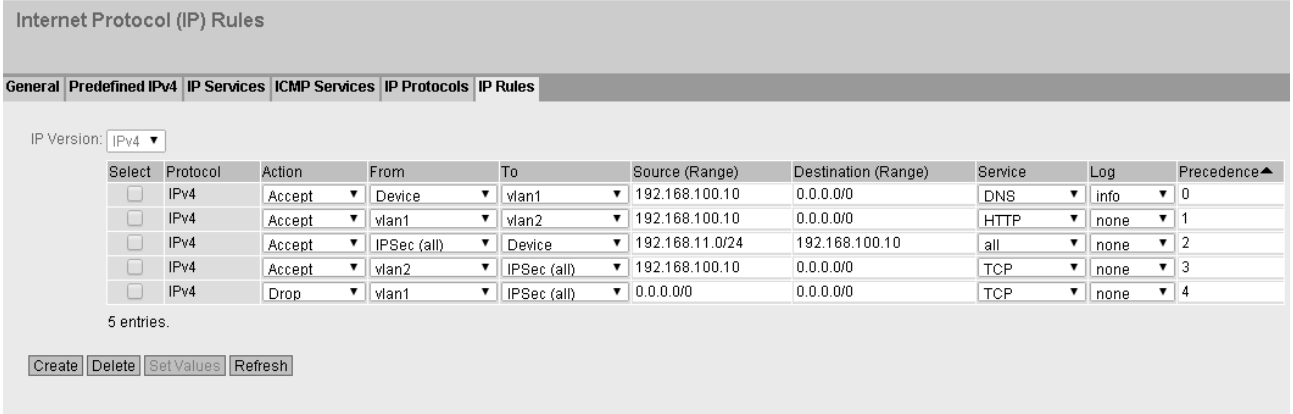
1. Enter IGMP in "Protocol Name".
2. Click the "Set Values" button. A new entry is generated in the table.
3. Enter 2 in "Protocol Number".

4.9.4.6 IP Rules

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

The IP packet filer rules set here have priority:

- over the predefined IP packet filter rules (predefined 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 ▼	Device ▼	vlan1 ▼	192.168.100.10	0.0.0.0/0	DNS ▼	info ▼	0
□	IPv4	Accept ▼	vlan1 ▼	vlan2 ▼	192.168.100.10	0.0.0.0/0	HTTP ▼	none ▼	1
□	IPv4	Accept ▼	IPSec (all) ▼	Device ▼	192.168.11.0/24	192.168.100.10	all ▼	none ▼	2
□	IPv4	Accept ▼	vlan2 ▼	IPSec (all) ▼	192.168.100.10	0.0.0.0/0	TCP ▼	none ▼	3
□	IPv4	Drop ▼	vlan1 ▼	IPSec (all) ▼	0.0.0.0/0	0.0.0.0/0	TCP ▼	none ▼	4

5 entries.

Description of the displayed boxes

This table contains the following columns:

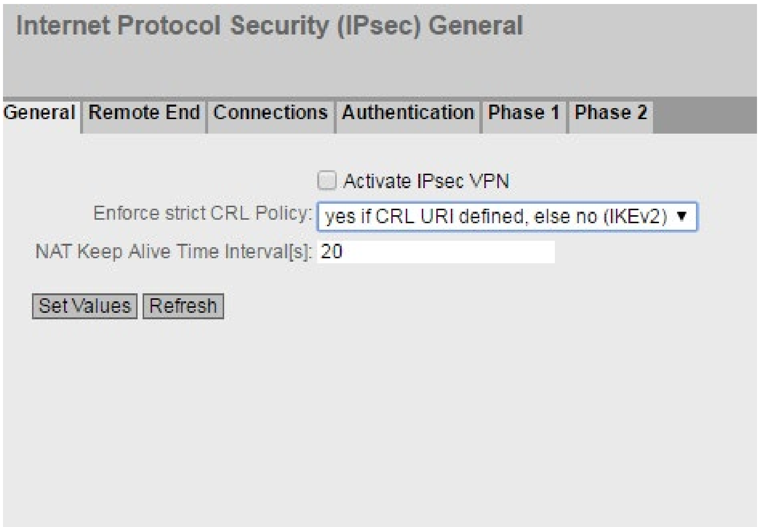
- **Select**
  Select the check box in the row to be deleted.
- **Protocol**
  Shows the version of the IP protocol.
- **Action**
  Select how incoming IP packets are handled:
  - "Accept" – The data packets can pass through.
  - "Reject" – The data packets are rejected, and the sender receives a corresponding 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: Device
  - ppp0 or usb0 (only with M876-4): WAN interface
  - SINEMA RC: Connection to SINEMA RC Server
  - IPsec: Either all IPsec VPN connections (all) or a specific IPsec VPN connection
- **Source (Range)**
  Enter the IP address or an IP range that is allowed to send IP packets.
  - If the rule is intended to apply to an IP range, enter the range with start address "-" end address , for example 192.168.100.10 - 192.168.100.20.
  - If the rule is intended to apply to all IP addresses , enter " 0.0.0.0/0".
- **Destination (Range)**
  Enter the IP address or an IP range that is allowed to receive IP packets.
  - If the rule is intended to apply to an IP range, enter the range with start address "-" end address , for example 192.168.100.10 - 192.168.100.20.
  - If the rule is intended to apply to all IP addresses , enter " 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.

4.9.5 IPsec VPN

4.9.5.1 General

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



Internet Protocol Security (IPsec) General

□ Activate IPsec VPN

Enforce strict CRL Policy: yes if CRL URI defined, else no (IKEv2) ▼

NAT Keep Alive Time Interval[s]: 20

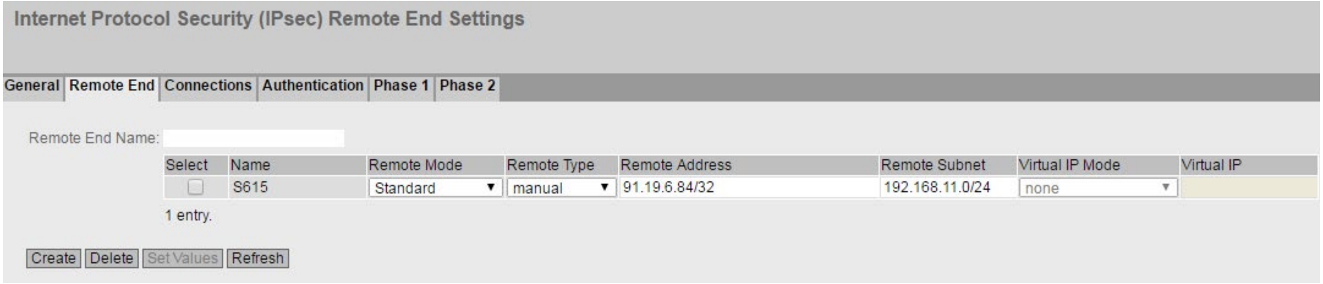
Description

The page contains the following:

- **"Activate IPsec VPN"** check box
  Enable or disable the IPsec method for VPN.
- **"Enforce strict CRL Policy" drop-down list**
  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 186)".
- **"NAT Keep Alive Time Interval (s)" input box**
  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.

4.9.5.2 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
□	S615	Standard ▼	manual ▼	91.19.6.84/32	192.168.11.0/24	none ▼	

1 entry.

Description

The page contains the following:

- **"Remote End Name" input box**
  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
    In Roadwarrior mode, the device accepts VPN connections from partners with an unknown address.
  - Standard
    In standard mode, the device establishes a connection to or from a known remote station. The remote station is identified by the IP address or the DDNS hostname.

- **Remote Type**
  Specify the type of remote station address.
  - any (only with Roadwarrior)
    Accepts the connection from remote stations with any IP address.
  - manual (With Roadwarrior)
    Only accepts connections from remote stations with a fixed IP address (/32), fixed IP subnet (CIDR notation), or (D)DNS hostname.
  - manual (With Standard)
    Only establishes a connection to a specific remote station with a fixed IP address or with (D)DNS hostname.
    Or only accepts a connection from a specific remote station with a fixed IP address or with (D)DNS hostname.
- **Remote Address**
  - In standard mode, enter the WAN IP address or the DDNS hostname.
  - In Roadwarrior mode, you can enter an IP range from which connections will be accepted. 0.0.0.0/0 means all IP addresses are accepted.
- **Remote Subnet**
  Enter the remote subnet of the remote station. Use the CIDR notation. Can only be edited if "Remote Type" "manual" is enabled.
- **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 "Virtual IP Mode" "user defined IPv4" is enabled.

Procedure

Configure VPN standard mode

1. Enter the name of the partner 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 partner.
6. Click the "Set Values" button.

Configure VPN Roadwarrior mode

1. Enter the name of the partner 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.

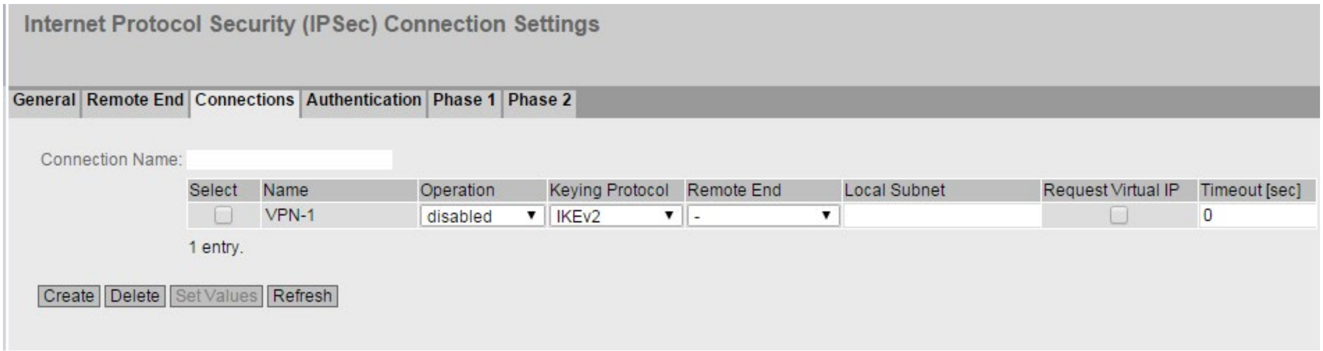
4.9.5.3 Connections

On the WBM page, you configure the basic settings for the VPN connection. With these settings, the device (local endpoint) can establish a non-secure VPN tunnel to the partner. You specify the security settings on the WBM page "Authentication".

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	disabled ▼	IKEv2 ▼	- ▼		□	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.

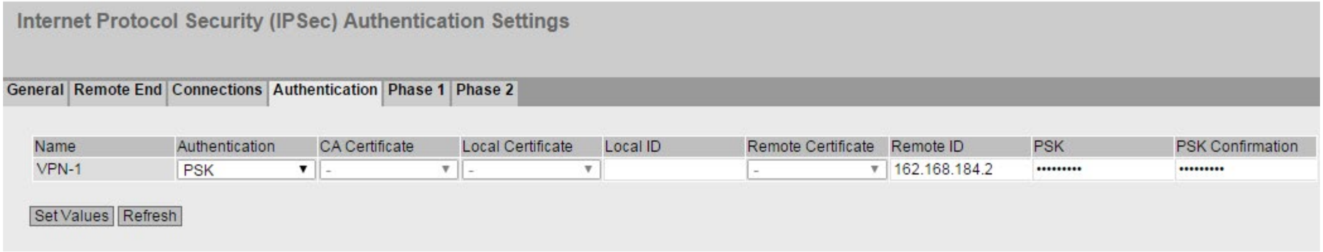
- **Operation**
  Specify who establishes the VPN connection. You will find more detailed information in "Technical basics > VPN connection establishment (Page 44)".
  - disabled
    The VPN connection is disabled.
  - start
    The device attempts to establish a VPN connection to the partner.
  - wait
    The device waits for the partner to initiate the connection.
  - on demand
    The VPN connection is established when necessary.
  - start on DI
    If the event "Digital In" occurs the device attempts to establish a VPN connection to the partner.

    This is on condition that the event "Digital In" is passed onto the VPN connection. To do this, in "System > Events > Configuration" for the event "Digital In" activate "VPN Tunnel".
  - wait on DI
    If the event "Digital In" occurs, the device waits for the partner to initiate a connection establishment.

    This is on condition that the event "Digital In" is passed onto the VPN connection. To do this, in "System > Events > Configuration" for the event "Digital In" activate "VPN Tunnel".
- **Keying Protocol**
  Specify whether IKEv2 or IKEv1 will be used.
- **Remote End**
  Select the required partner. 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.

4.9.5.4 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.
  – CA Cert
    The certificate of the certification authority is used for authentication. You specify the certificate in "CA Certificate".
  – Remote Cert
    The remote certificate is used for authentication. You specify the certificate in "Remote Certificate"
  – PSK
    A key is used for authentication. You configure the key in "PSK".
- **CA Certificate**
  Select the certificate. Only loaded certificates can be selected.
- **Local Certificate**
  Select the device certificate.

  You load the certificate 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 certificate. Only loaded remote certificates can be selected.

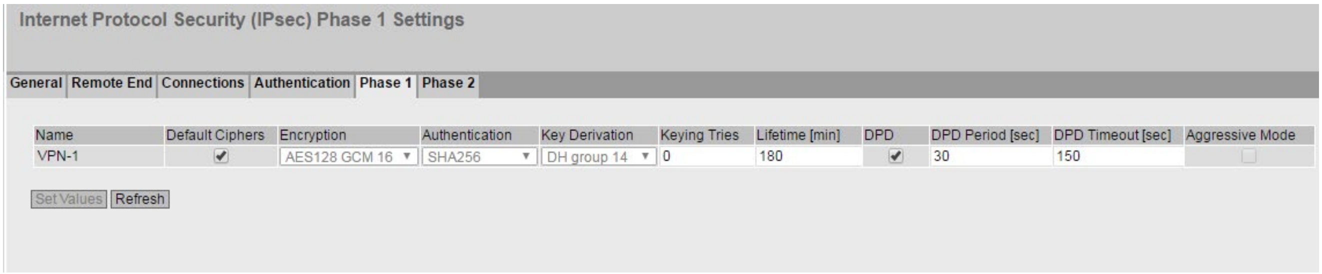
  You load the certificate on the device with "System > Load&Save". The loaded certificates and key files are shown on the WBM page "Security > Certificates".

- **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 key.
- **PSK confirmation**
  Repeat the key.

4.9.5.5 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	☑	AES128 GCM 16 ▼	SHA256 ▼	DH group 14 ▼	0	180	☑	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"

- **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".

  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

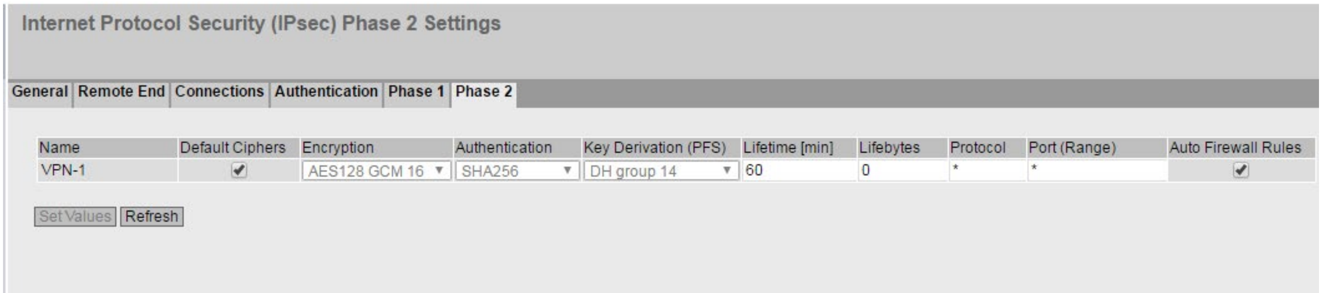
- **DPD Period [sec]**
  Enter the period after which DPD queries are sent. These queries test whether or not the remote station is still available
- **DPD Timeout [sec]**
  Enter the period. If there is no response to the DPD queries, the connection to the remote station is declared to be invalid after this time has elapsed.
- **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.

4.9.5.6 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. The entire communication during this phase is encrypted using the standardized security protocol ESP for which you can set the following protocol parameters.



Name	Default Ciphers	Encryption	Authentication	Key Derivation (PFS)	Lifetime [min]	Lifebytes	Protocol	Port (Range)	Auto Firewall Rules
VPN-1	☑	AES128 GCM 16	SHA256	DH group 14	60	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".
- **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".

  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**
  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**

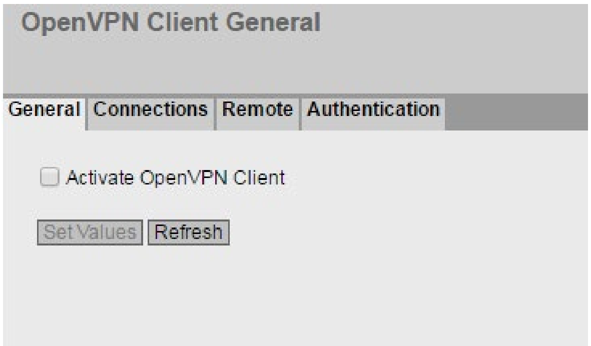
  – enabled
    The firewall rules are created automatically for the VPN connection.

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

4.9.6 OpenVPN client

4.9.6.1 General

On this WBM page, you enable the OpenVPN client.



OpenVPN Client General

□ Activate OpenVPN Client

Description

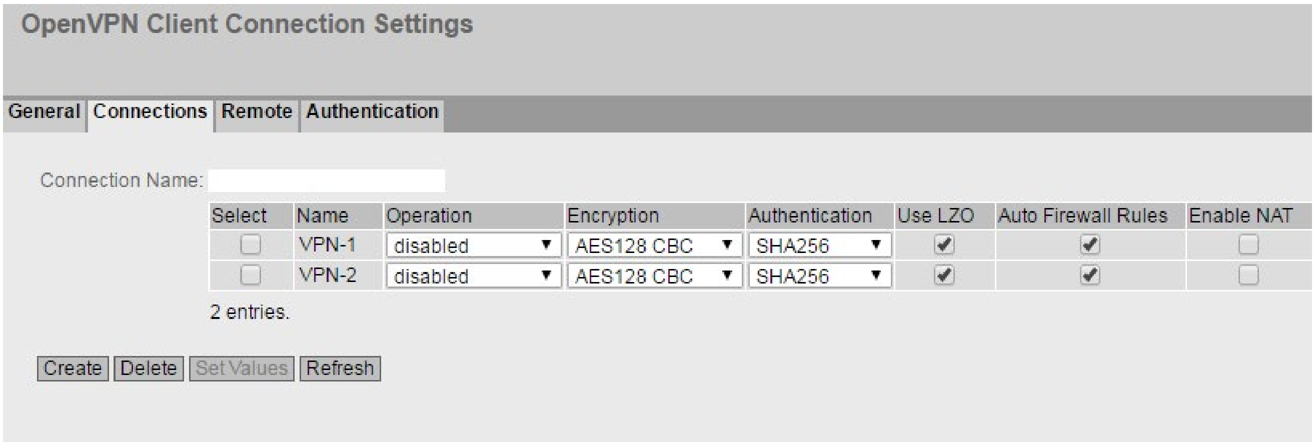
The page contains the following:

- **"Activate OpenVPN Client" check box**

  Enable or disable the OpenVPN client.

4.9.6.2 Connections

On this WBM page, you configure the basic settings for the OpenVPN connection. You specify the security settings on the WBM page "Authentication".



OpenVPN Client Connection Settings

Connection Name:

Select	Name	Operation	Encryption	Authentication	Use LZO	Auto Firewall Rules	Enable NAT
□	VPN-1	disabled	AES128 CBC	SHA256	☑	☑	□
□	VPN-2	disabled	AES128 CBC	SHA256	☑	☑	□

2 entries.

Description

- **"Connection Name" input box**

  Enter a unique name for the OpenVPN 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 OpenVPN connection.
- **Operation**

  Specify how the connection is established. You will find more detailed information in "Technical basics > VPN connection establishment (Page 44)".
  - start

    The device attempts to establish a VPN connection to the partner.
  - start on DI

    If the event "Digital In" occurs the device attempts to establish a VPN connection to the partner.

    This is on condition that the event "Digital In" is passed onto the VPN connection. To do this, in "System > Events > Configuration" for the event "Digital In" activate "VPN Tunnel".
  - disable

    The VPN connection is disabled.
- **Encryption**

  Select the required encryption algorithm.
  - AES-128-CBC (Default)
  - AES-192-CBC
  - AES-256-CBC
  - DES-EDE3-CBC
  - BF-CBC
- **Authentication**

  Specify the method for calculating the checksum.
  - SHA256 (default)
  - SHA384
  - SHA512
  - SHA224
  - SHA1
  - MD5
- **Use LZO**

  When enabled, the data is compressed with the LZO algorithm.

- **Auto Firewall Rules**
  - Enabled

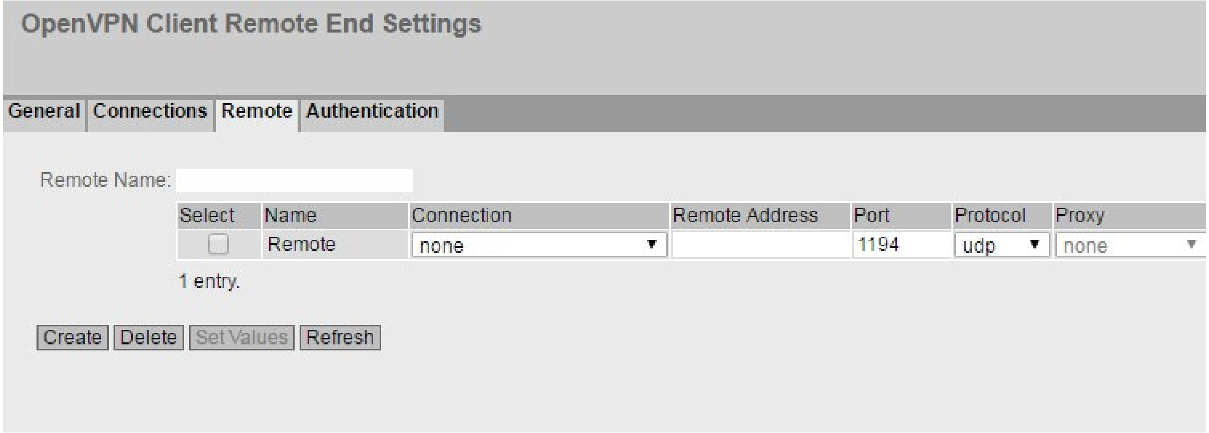
    The firewall rules are created automatically for the VPN connection.
  - Disabled

    You will need to create the suitable firewall rules yourself.
- **Enable NAT**

  With this setting, you enable automatic IP masquerading for this interface. The local devices are not directly reachable from the outside, but only via the IP address of the interface. The local devices can, however, connect to the devices downstream from the OpenVPN server. You will find more information on NAT in "Technical basics > NAT" (Page 32)"

4.9.6.3 Remote

On this WBM page, you configure the partner (OpenVPN end point). Per connection, you can specify several OpenVPN partners. The device tries all configured OpenVPN partners one after the other until a connection is successfully established.



OpenVPN Client Remote End Settings

Remote Name:

Select	Name	Connection	Remote Address	Port	Protocol	Proxy
☐	Remote	none ▼		1194	udp ▼	none ▼

1 entry.

Description

The page contains the following:

- **"Remote Name" input box**

  Enter a name for the OpenVPN partner and click "Create" to create a new partner.

This table contains the following columns:

- **Select**

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

  Shows the name of the Open VPN partner.

- **Connection**

  Select the corresponding connection. Only connections can be configured that have been configured on the "Connections" WBM page.

- **Remote Address**

  Enter the WAN IP address or the DNS host name of the OpenVPN partner.

- **Port**

  Specify the port via which the OpenVPN tunnel can communicate. The setting applies specifically to the specified port.

- **Protocol**

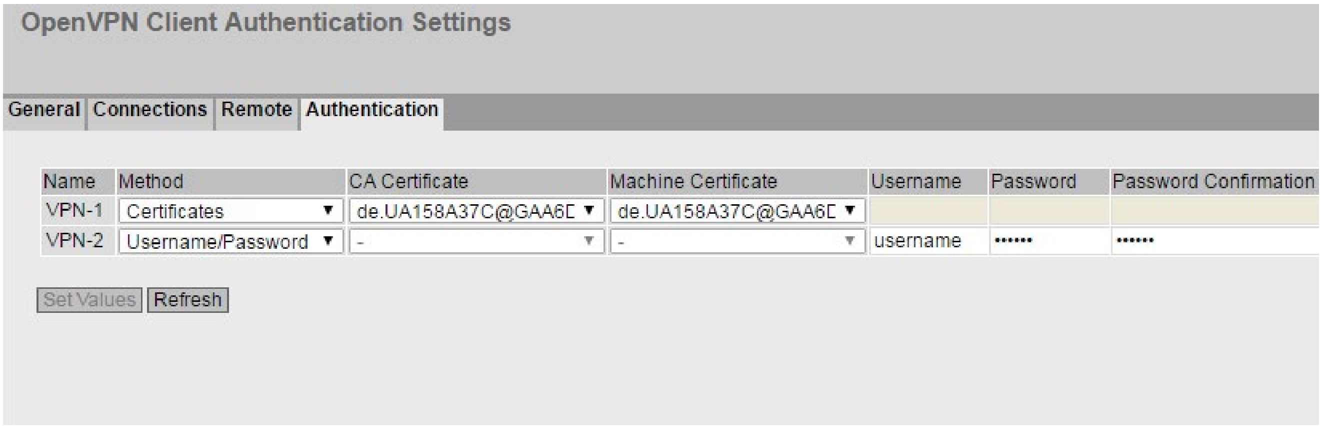
  Specify the protocol for which the OpenVPN connection will be used.

- **Proxy**

  Specify whether the OpenVPN tunnel to the defined OpenVPN partner is established via a proxy server. Only the proxy servers can be selected that you configured in "System > Proxy Server".

4.9.6.4 Authentication

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



OpenVPN Client Authentication Settings

Name	Method	CA Certificate	Machine Certificate	Username	Password	Password Confirmation
VPN-1	Certificates ▼	de.UA158A37C@GAA6D ▼	de.UA158A37C@GAA6D ▼			
VPN-2	Username/Password ▼	- ▼	- ▼	username	••••••	••••••

Description

This table contains the following columns:

- **Name**

  Shows the name of the VPN connection to which the settings relate.

- **Method**

  Select the authentication method. For the VPN connection, it is essential that the partner uses the same authentication method.

  – disabled

    No authentication method is selected. Connection establishment is not possible.

  – Certificates
    Certificates are used for the authentication.

  – Username/Password
    The user name/password are used for the authentication.

- **CA Certificate**

  Select the certificate. Only loaded certificates can be selected.

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

- **Machine Cerificate**

  Select the device certificate. Only loaded certificates can be selected.

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

- **Username**

  Specify the user name.

- **Password**

  Enter the password.

- **Password Confirmation**

  Confirm the password.

Service and maintenance 5

5.1 Firmware update using HTTP

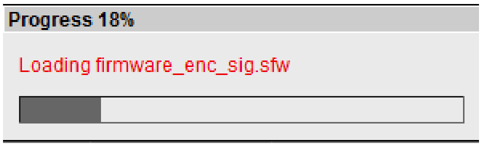
5.1.1 Firmware update using HTTP

Requirement

- The device has an IP address and is reachable.
- WBM has been started and the "admin" user is logged in.

Firmware update using HTTP

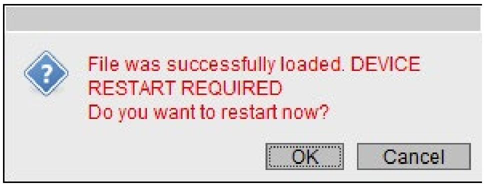
1. Click "System" > "Load&Save" in the navigation area. Click the "HTTP" tab.
2. Click the "Load" button next to "Firmware".
3. Go to the storage location of the firmware file.
4. Click the "Open" button in the dialog. The firmware file is downloaded. The firmware itself is signed and encrypted. This ensures that only authentic firmware is downloaded to the device.



Progress 18%

Loading firmware_enc_sig.sfw

5. If the file is loaded successfully, the following dialog is displayed.

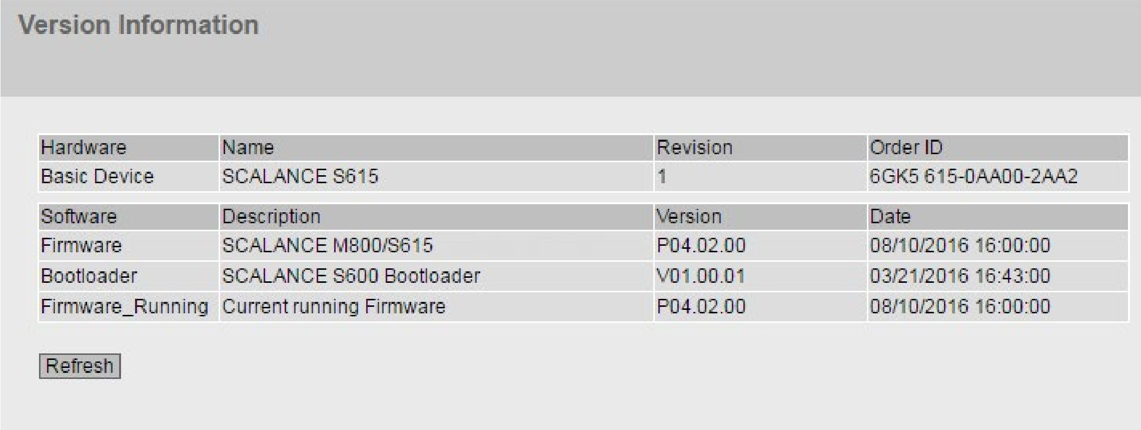


File was successfully loaded. DEVICE RESTART REQUIRED
Do you want to restart now?

6. Click "OK" to restart the device. If you click "Cancel", you will need to restart the device later with "System" > "Restart".

Result

The firmware is has been transferred completely to the device and under "Information" > "Versions" there is also the entry "Firmware_Running". Firmware_Running shows the version of the current firmware. Firmware shows the firmware version stored after loading the firmware.



Version Information

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

Software	Description	Version	Date
Firmware	SCALANCE M800/S615	P04.02.00	08/10/2016 16:00:00
Bootloader	SCALANCE S600 Bootloader	V01.00.01	03/21/2016 16:43:00
Firmware_Running	Current running Firmware	P04.02.00	08/10/2016 16:00:00

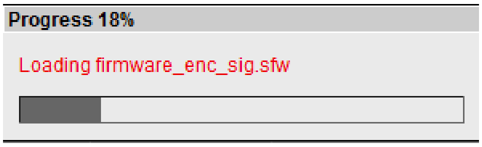
5.2 Firmware update - using TFTP

Requirement

- The device has an IP address and is reachable.
- WBM has been started and the "admin" user is logged in.
- There is a TFTP server in the network.
- The firmware file is on the TFTP server.

Procedure

1. Click "System" > "Load&Save" in the navigation area. Click the "TFTP" tab.
2. In "TFTP Server IP Address", enter the IP address of the TFTP server.
3. In "TFTP Server Port", enter the port of the TFTP server
4. If necessary, change the file name in the "Firmware" table row.
5. Select the table row "Firmware" for the "Load file" action. The firmware itself is signed and encrypted. This ensures that only authentic firmware is downloaded to the device.
6. Click "Set Values". The firmware file is downloaded. The firmware itself is signed and encrypted. This ensures that only authentic firmware is downloaded to the device.



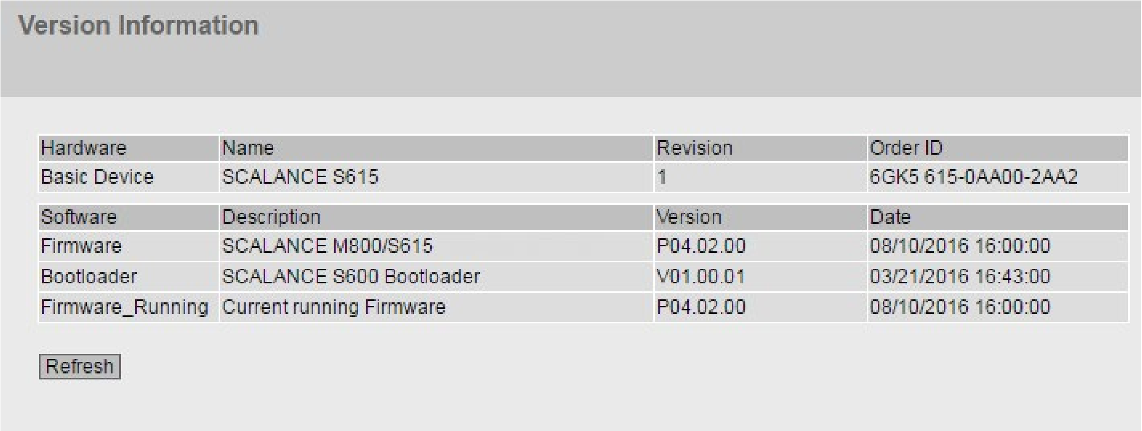
Progress 18%

Loading firmware_enc_sig.sfw

7. If the file is loaded successfully, the following dialog is displayed
8. Confirm the dialog with "OK". The device is restarted.

Result

The firmware is has been transferred completely to the device and under "Information" > "Versions" there is also the entry "Firmware_Running". Firmware_Running shows the version of the current firmware. Firmware shows the firmware version stored after loading the firmware.



Version Information

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

Software	Description	Version	Date
Firmware	SCALANCE M800/S615	P04.02.00	08/10/2016 16:00:00
Bootloader	SCALANCE S600 Bootloader	V01.00.01	03/21/2016 16:43:00
Firmware_Running	Current running Firmware	P04.02.00	08/10/2016 16:00:00

5.3 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 (P1 - P4).
- 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. Now 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 and can be reached with the IP address 192.168.1.1.

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 (P1 - P4).
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.

Index