SIEMENS

SCALANCE X-500 Web Based Management

Configuration Manual

09/2011

C79000-G8976-C248-01

Legal information

Warning notice system

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

⚠DANGER

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

⚠WARNING

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

⚠CAUTION

with a safety alert symbol, indicates that minor personal injury can result if proper precautions are not taken.

CAUTION

without a safety alert symbol, indicates that property damage can result if proper precautions are not taken.

NOTICE

indicates that an unintended result or situation can occur if the relevant information is not taken into account.

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
Industry Sector
Postfach 48 48
90026 NÜRNBERG
GERMANY

Order number: C79000-G8976-C248-01
℗ 09/2011

Table of contents

General information 1

1.1 Web Based Management

How it works

The device has an integrated HTTP server for Web Based Management (WBM). If a device is addressed over an Internet browser, it returns HTML pages to the client 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.

The advantage of this method is that only an Internet browser is required on the client.

Requirements

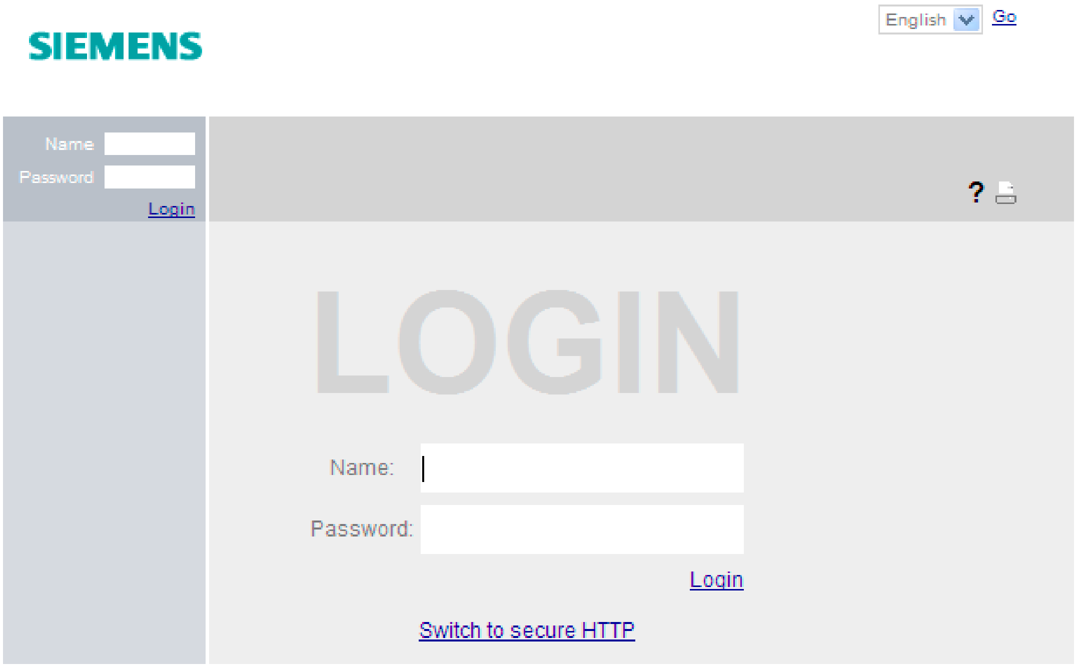
- The device has an IP address
- There is a connection between the device and the client PC. With the ping command, you can check whether or not a connection exists.
- The integrated HTTP server is activated.
- Recommended Internet browser:
  - Microsoft Internet Explorer version 8.0
  - Mozilla Firefox version 4.0
- JavaScript is activated in the Internet browser.
- The Internet browser must not be set so that it reloads the page from the server each time the page is accessed. The updating of the dynamic content of the page is ensured by other mechanisms. In the Internet Explorer, you can make the appropriate setting in the "Options > Internet Options > General" menu in the section "Browsing history" with the "Settings" button. Under "Check for newer versions of stored pages:", select "Automatically".
- If a firewall is used, the relevant ports must be opened.
  - For access using HTTP: Port 80
  - For access using HTTPS: Port 443

1.2 Login

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. Note that in this version, only English is available.
2. Click the "Go" button to change to the selected language.



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 client PC. With the ping command, you can check whether or not a connection exists.
2. In the address box of the Internet browser, enter the IP address or the URL of the device. If there is a problem-free connection to the device, the login page of Web Based Management (WBM)is displayed.

Login with HTTP

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

The following steps apply when logging in whichever of the above options you choose:

1. Enter the following in the "Name" input box:
   - "admin": With this user type, you can change the settings of the device (read and write access to the configuration data).
   - "user": With this user type, you cannot change any of the settings of the device (read access to the configuration data).
2. Enter your password in the "Password" input box. If you have not yet set a password, the default passwords as shipped are valid:
   - Enter "admin" to log in with the "Administrator" user type.
   - Enter "user" to log with the "User" user type.
3. Click the "Login" button or confirm your input with "Enter" to start the login procedure.
   Once you have logged in successfully, the start page appears.

Note

Password change

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.

Login 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 login page or enter "https://" and the IP address of the device in the address box of the Internet browser.

   The "Certification Error Warning" is displayed and asks you whether you want to continue the action.
2. Click the "Yes" button if you want to continue.
   The Login page of Web-Based Management appears.
3. Enter the following in the "Name" input box:
   - "admin": With this user type, you can change the settings of the device (read and write access to the configuration data).
   - "user": With this user type, you cannot change any of the settings of the device (read access to the configuration data).
4. Enter your password. If you have not yet set a password, the default passwords as shipped are valid:
   - Enter "admin" to log in with the "Administrator" user type.
   - Enter "user" to log with the "User" user type.
5. Click the "Login" button or confirm your input with "Enter" to log in.

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

The "Information" menu 2

2.1 Start page

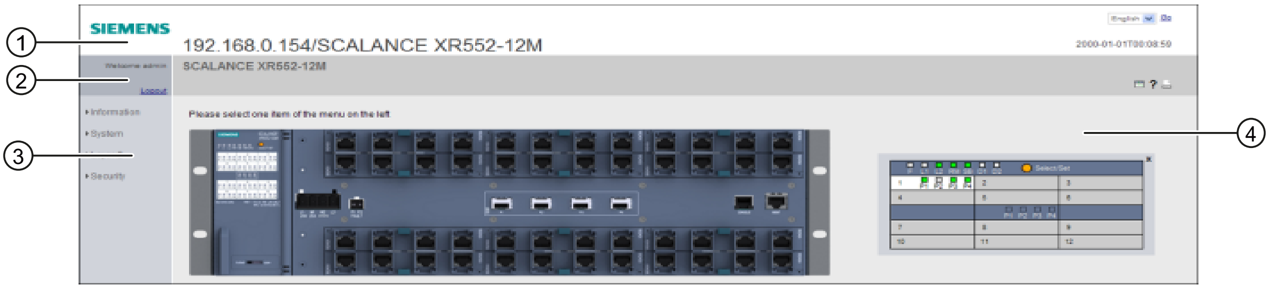
View of the Start page

When you enter the IP address of the device, the start page is displayed after a successful login. You cannot configure anything on this page.

General layout of the WBM pages

The following areas are generally 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



192.168.0.154/SCALANCE XR552-12M

2000-01-01T00:08:59

SCALANCE XR552-12M

Please select one item of the menu on the left

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 SCALANCE X devices, the in-band port IP address of the device is displayed as default.
    With SCALANCE W devices, the IP address of the Ethernet interface is displayed as default.
  - "System Name" is the device name. With the settings when the device ships, the device type is displayed.

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

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

  You can change the content of this display with "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.

In the right-hand part of the display area, you will see the following buttons (from right to left):

- 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.

  The help page contains a description of the content area. Under certain circumstances, options are described that are not available on the device. To allow a distinction, the following icon has been introduced.

X These are additional options available with SCALANCE X devices.

W These are additional options available with SCALANCE W devices.

- LED simulation ▦
  Each component of a 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. Unoccupied slots or unused connectors are displayed as a grayed-out LED. The meaning of the LED displays is described in the operating instructions (compact).

  With SCALANCE X devices, if you click the simulated "Select/Set" button, you can change the display mode (LEDs DM or D1/D2).

  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.

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.

Buttons you require often

The pages of the WBM contain the following standard buttons:

- Refresh the display with "Refresh"
  Web Based Management 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"
  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.

- Create entries with "Create"
  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"
  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 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.

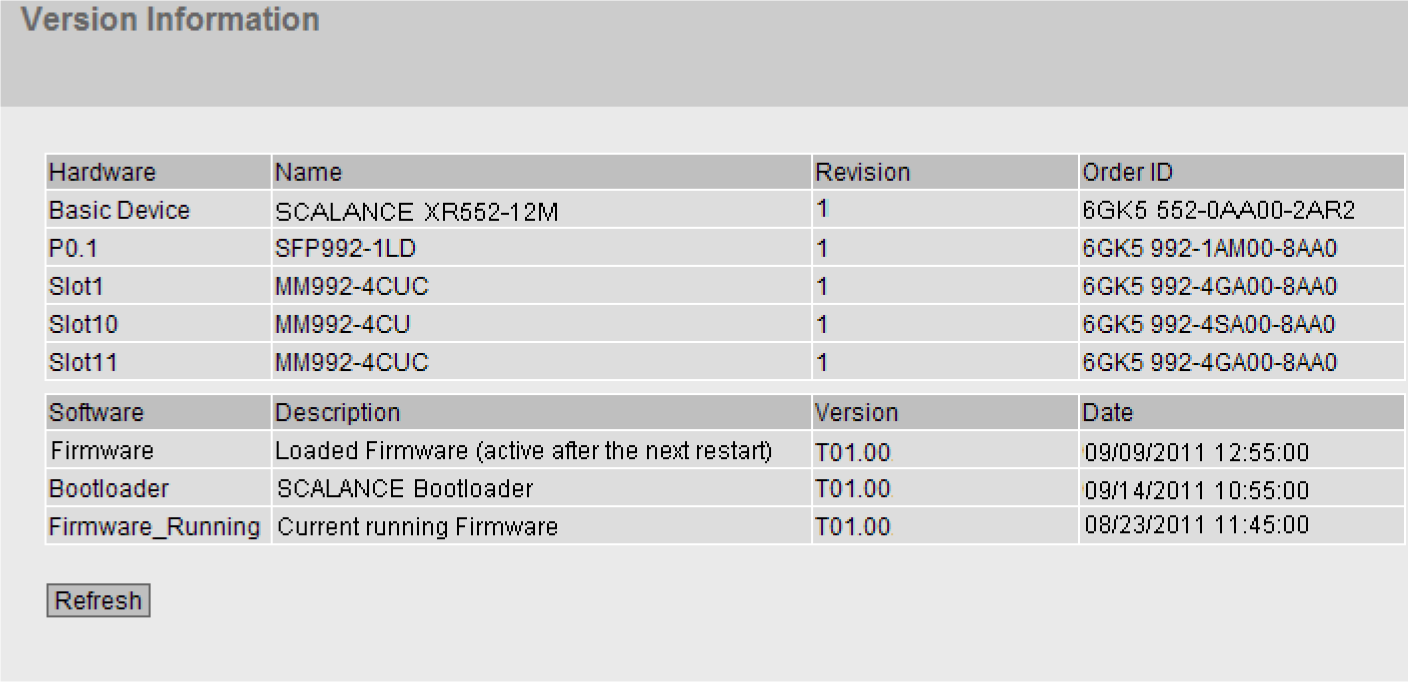
Logout

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

2.2 Versions

Versions of hardware and software

This page shows the versions of the hardware and software of the device. You cannot configure anything on this page.



Version Information

Hardware	Name	Revision	Order ID
Basic Device	SCALANCE XR552-12M	1	6GK5 552-0AA00-2AR2
P0.1	SFP992-1LD	1	6GK5 992-1AM00-8AA0
Slot1	MM992-4CUC	1	6GK5 992-4GA00-8AA0
Slot10	MM992-4CU	1	6GK5 992-4SA00-8AA0
Slot11	MM992-4CUC	1	6GK5 992-4GA00-8AA0

Software	Description	Version	Date
Firmware	Loaded Firmware (active after the next restart)	T01.00	09/09/2011 12:55:00
Bootloader	SCALANCE Bootloader	T01.00	09/14/2011 10:55:00
Firmware_Running	Current running Firmware	T01.00	08/23/2011 11:45:00

Description of the displayed values

Table 1 has the following columns:

- Hardware
  - Basic Device
    The basic device.
  - Slot X (SCALANCE X only)
    "X" = slot number: Module plugged into this slot.
- Name
  Name of the device or module.
- Revision
  The hardware version of the device.
- Order ID
  The order number of the device or module.

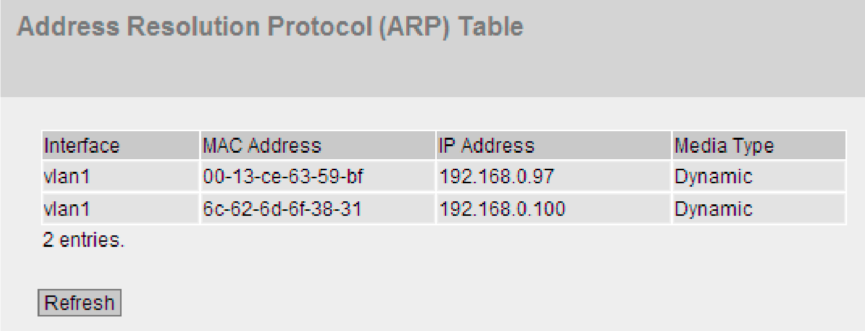
Table 2 has the following columns:

- Software
  - Firmware
    The current version of the current firmware is shown here. If a new firmware file was downloaded and the device has not yet restarted, the firmware version of the downloaded firmware file is displayed here. After the next restart, the downloaded firmware is activated and used.
  - Bootloader
    The version of the boot software stored on the device is displayed here.
  - FirmwareRunning
    This entry is only displayed when a new firmware file has been downloaded to the device and the device has not yet restarted. In this case, the firmware version currently being used is displayed.
- Description
  Brief description of the software.
- Version
  Version number of the software version.
- Date
  Date on which the software version was created.

2.3 ARP table

Assignment of MAC address and IP address

The ARP table (Address Resolution Protocol) obtains the corresponding MAC address of a known IP address. The page of this submenu also indicates the interface over which an address can be reached. The last column indicates how the information was obtained. You cannot configure anything on this page.



Address Resolution Protocol (ARP) Table

Interface	MAC Address	IP Address	Media Type
vlan1	00-13-ce-63-59-bf	192.168.0.97	Dynamic
vlan1	6c-62-6d-6f-38-31	192.168.0.100	Dynamic

2 entries.

Description of the displayed values

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 target device found using the ARP table.
- IP Address
  Shows the IP address of the target device.
- Media Type
  Shows the type of connection. The options here are as follows:
  – Dynamic
    The device recognized the address data automatically.
  – Static
    The user entered the address data using the Command Line Interface (CLI).

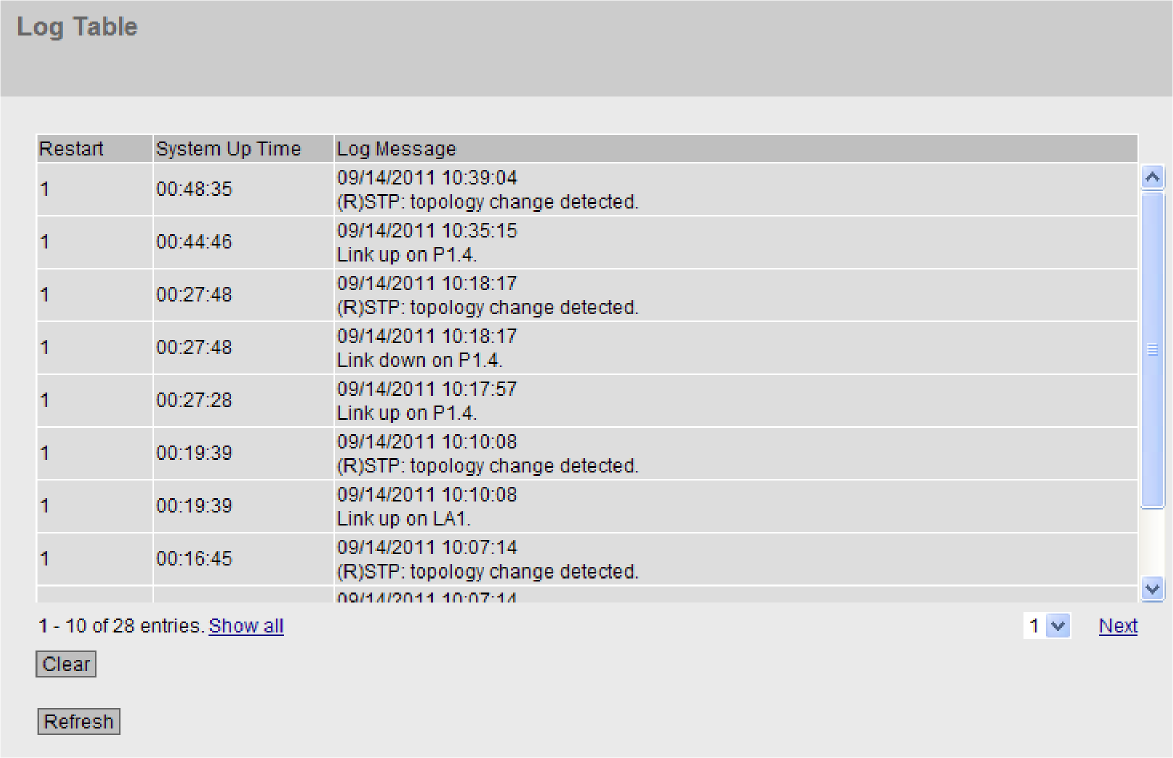
2.4 Log table

Logging events

The device allows you to log occurring events, some of which you can specify on the page of the System > Events menu. This, for example, allows you to record when an SNMP authentication attempt failed or when the connection status of a port has changed.

The content of the events log table is retained even when the device is turned off.

You cannot configure anything on this page.



Log Table

Restart	System Up Time	Log Message
1	00:48:35	09/14/2011 10:39:04 (R)STP: topology change detected.
1	00:44:46	09/14/2011 10:35:15 Link up on P1.4.
1	00:27:48	09/14/2011 10:18:17 (R)STP: topology change detected.
1	00:27:48	09/14/2011 10:18:17 Link down on P1.4.
1	00:27:28	09/14/2011 10:17:57 Link up on P1.4.
1	00:19:39	09/14/2011 10:10:08 (R)STP: topology change detected.
1	00:19:39	09/14/2011 10:10:08 Link up on LA1.
1	00:16:45	09/14/2011 10:07:14 (R)STP: topology change detected.
		09/14/2011 10:07:14

1 - 10 of 28 entries.

Description of the displayed values

The table has the following columns:

- System > Events
  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 running time of the device since the last restart in the format "DD HH:MM:SS".
- 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. 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. When this number is reached, the oldest entries are overwritten. The table remains permanently in memory.

Button "Show all"

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

Button "Next"

Click this button to go to the next page.

Button "Prev"

Click this button to go to the previous page.

Drop-down list for page change

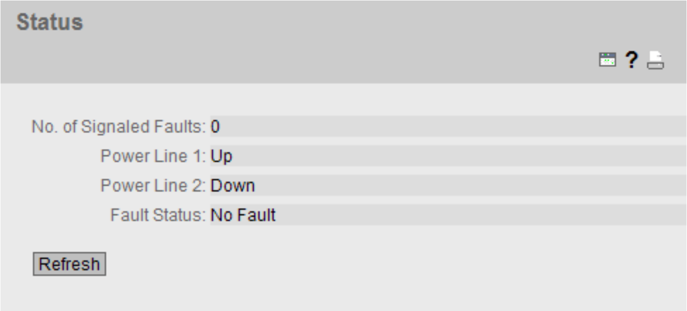
From the drop-down list, select the page you want to go to.

2.5 Status

Information on the operating status

The page shows information about the power supply and the error status. The text boxes on this page are read-only and cannot be modified.

You cannot configure anything on this page.



No. of Signaled Faults: 0
Power Line 1: Up
Power Line 2: Down
Fault Status: No Fault

Description of the displayed values

The table has the following rows:

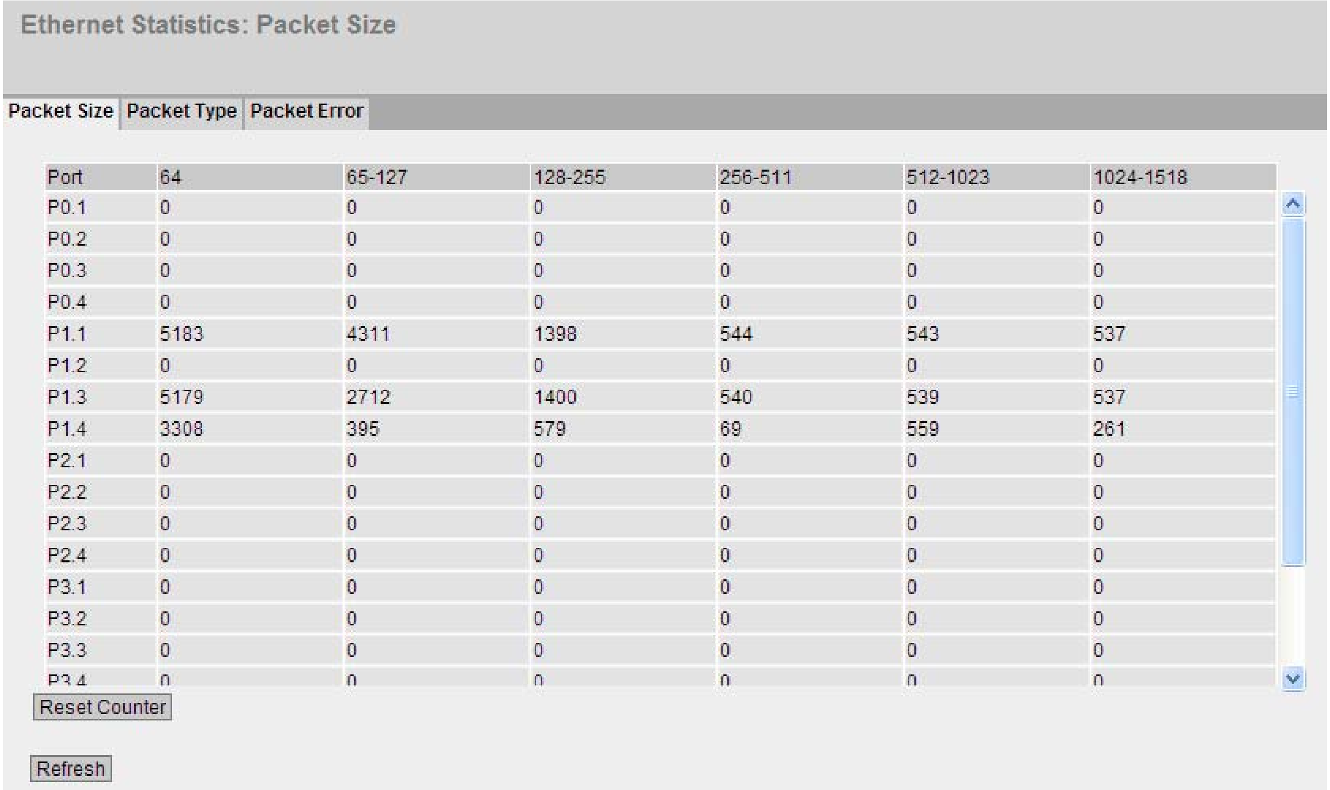
- No. of Signaled Faults
  Indicates how often the signaling contact of the device responded. The counter is reset each time the system is restarted.
- Power Line 1 and Power Line 2
  - UP
    Power supply is applied.
  - Down
    Power supply is not applied or is below the permitted voltage.
- Fault Status
  The fault status of the device is shown here. If problems have occurred, they are listed in the text box one above the other.

2.6 Ethernet statistics

2.6.1 Ethernet statistics: Packet size

Frames sorted by length

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



Ethernet Statistics: Packet Size

Port	64	65-127	128-255	256-511	512-1023	1024-1518
P0.1	0	0	0	0	0	0
P0.2	0	0	0	0	0	0
P0.3	0	0	0	0	0	0
P0.4	0	0	0	0	0	0
P1.1	5183	4311	1398	544	543	537
P1.2	0	0	0	0	0	0
P1.3	5179	2712	1400	540	539	537
P1.4	3308	395	579	69	559	261
P2.1	0	0	0	0	0	0
P2.2	0	0	0	0	0	0
P2.3	0	0	0	0	0	0
P2.4	0	0	0	0	0	0
P3.1	0	0	0	0	0	0
P3.2	0	0	0	0	0	0
P3.3	0	0	0	0	0	0
P3.4	0	0	0	0	0	0

Description of the displayed values

The table has the following columns:

- Port
  All available ports are listed in this column. Unavailable ports are not displayed. The other columns after the entry contain the absolute numbers of the incoming frames according to their frame length.

X With SCALANCE X devices, this column lists all available ports as well as the link aggregations.
The port is made up of the port number and slot number. , for example port 0.1 is slot 0, port 1.

W With SCALANCE W devices, the port number is displayed, for example, P1 is port number 1.

Note

Display of frame statistics

In the statistics relating to frame size, note that frames are counted both at the input port and the output port.

- Frame lengths
  In the columns of the table, a distinction is made according to the following frame lengths:
  - 64 bytes
  - 65 - 127 bytes
  - 128 - 255 bytes
  - 256 - 511 bytes
  - 512 - 1023 bytes
  - 1024 - 1518 bytes

Description of the button

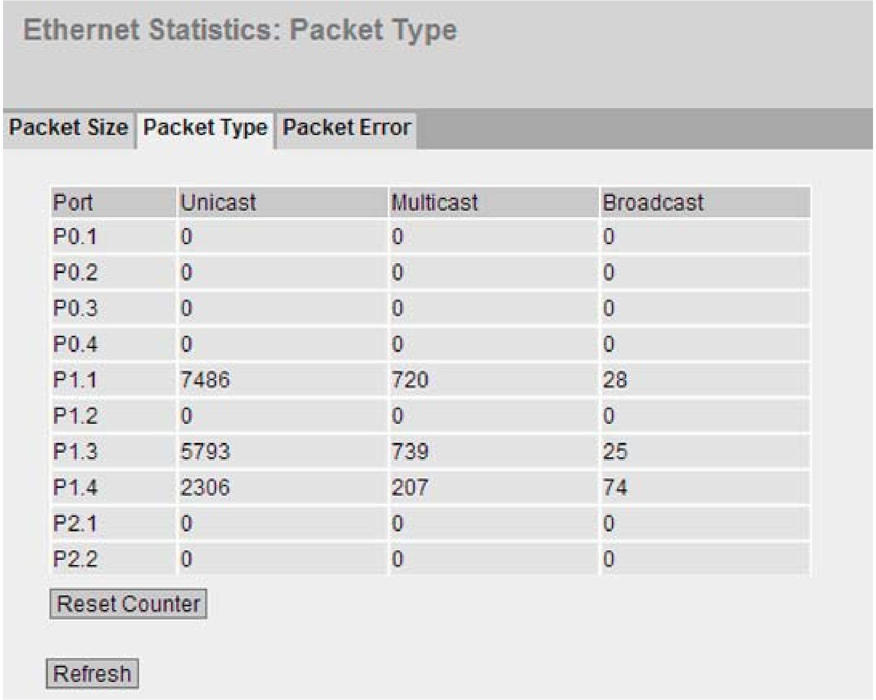
"Reset Counters" button

Click this button to reset the counters for all ports. The counters are reset by a restart.

2.6.2 Ethernet statistics: Packet type

Received frames sorted by type

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



Port	Unicast	Multicast	Broadcast
P0.1	0	0	0
P0.2	0	0	0
P0.3	0	0	0
P0.4	0	0	0
P1.1	7486	720	28
P1.2	0	0	0
P1.3	5793	739	25
P1.4	2306	207	74
P2.1	0	0	0
P2.2	0	0	0

Description of the displayed values

The table has the following columns:

- Port
  All available ports are listed in this column. Unavailable ports are not displayed.

X With SCALANCE X devices, this column lists all available ports and the link aggregations.
The port is made up of the port number and slot number, for example port 0.1 is slot 0, port 1.

W With SCALANCE W devices, the port number is displayed, for example, P1 is port number 1.

- Unicast / Multicast / Broadcast
  The other columns after the port number contain the absolute numbers of the incoming frames according to their frame type "Unicast", "Multicast" and "Broadcast".

Description of the button

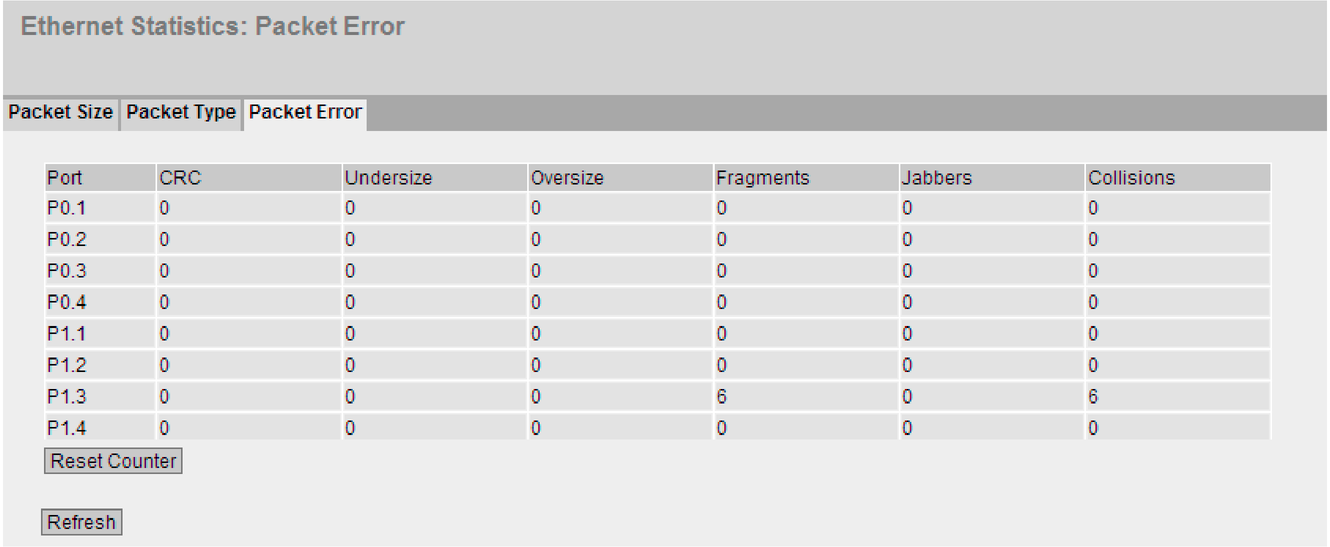
"Reset Counters" button

Click this button to reset the counters for all ports.
The counters are reset by a restart.

2.6.3 Ethernet statistics: Packet Error

Bad received frames

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



Ethernet Statistics: Packet Error

Port	CRC	Undersize	Oversize	Fragments	Jabbers	Collisions
P0.1	0	0	0	0	0	0
P0.2	0	0	0	0	0	0
P0.3	0	0	0	0	0	0
P0.4	0	0	0	0	0	0
P1.1	0	0	0	0	0	0
P1.2	0	0	0	0	0	0
P1.3	0	0	0	6	0	6
P1.4	0	0	0	0	0	0

Description of the displayed values

The table has the following columns:

- Port
  All available ports are listed in this column. Unavailable ports are not displayed.

X With SCALANCE X devices, this column lists all available ports and the link aggregations.
The port is made up of the port number and slot number, for example port 0.1 is slot 0, port 1.

W With SCALANCE W devices, the port number is displayed, for example, P1 is port number 1.

- **Error types**
  The other columns after the port number contain the absolute numbers of the incoming frames according to their error type.

  In the columns of the table, a distinction is made according to the following error types:

  – CRC
  Packets whose content does not match the CRC checksum.

  – Undersize
  Packets with a length less than 64 bytes.

  – Oversize
  Packets discarded because they were too long.

  – Fragments
  Packets with a length less than 64 bytes and a bad CRC checksum.

  – Jabbers
  VLAN-tagged packets with an incorrect CRC checksum that were discarded because they were too long.

  – Collisions
  Detected collisions.

Description of the button

"Reset Counters" button

Click this button to reset the counters for all ports. The counters are reset by a restart.

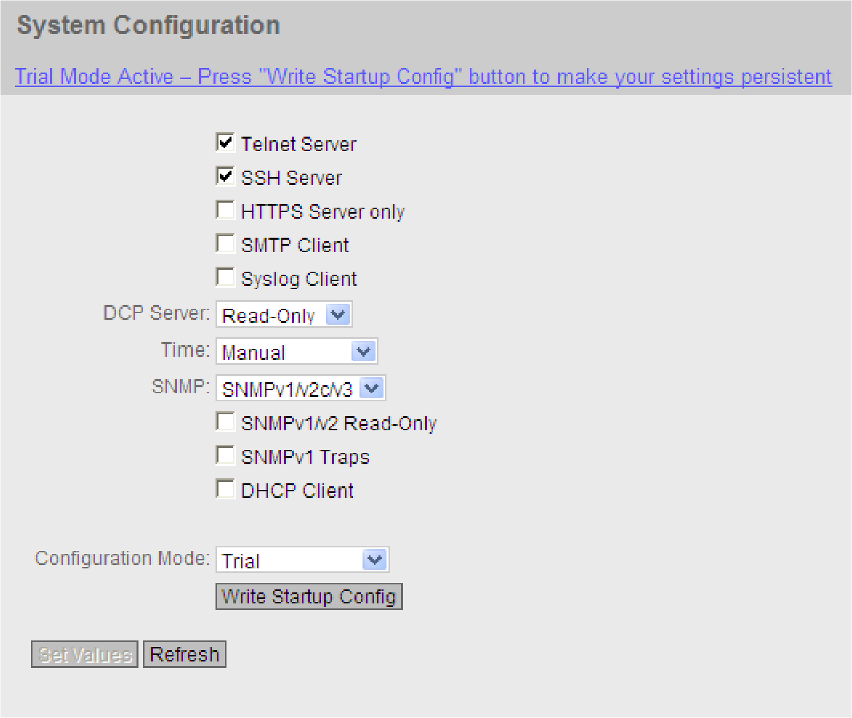
The "System" menu 3

3.1 Configuration

System configuration

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

Here, you can specify the services to be used when accessing the device. With some services, there are further configuration pages on which more detailed settings can be made.



System Configuration

Trial Mode Active – Press "Write Startup Config" button to make your settings persistent

☑ Telnet Server
☑ SSH Server
☐ HTTPS Server only
☐ SMTP Client
☐ Syslog Client
DCP Server: Read-Only
Time: Manual
SNMP: SNMPv1/v2c/v3
☐ SNMPv1/v2 Read-Only
☐ SNMPv1 Traps
☐ DHCP Client

Configuration Mode: Trial

Description of the displayed boxes

The page contains the following boxes:

- Check box "Telnet Server"
  Enables / disables the "Telnet Server" service for unencrypted access to CLI.
- Check box "SSH Server"
  Enables / disables the "SSH Server" service for encrypted access to CLI.
- Check box "HTTPS Server only"
  Enables / disables access via HTTP.

- **Check box "SMTP Client"**
  Enables / disables the SMTP client. You can configure other settings in "System > SMTP Client".
- **Check box "Syslog Client"**
  Enables / disables the system event client. You can configure other settings in "System > Syslog Client".
- **Drop-down list "DCP Server"**
  Here, you decide 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
    Device parameters can be read with DCP but cannot be modified.
- **Drop-down list "Time"**
  Select one of the following options from the drop-down list:
  - Manual
    The system time is set manually. You can configure other settings in "System > Time > Manual Setting".
  - SNTP Client
    The system time is set via an SNTP server. You can configure other settings in "System > Time > SNTP Client".
  - NTP Client
    The system time is set via an NTP server. You can configure other settings in "System > Time > NTP Client".
  - SIMATIC Time
    The system time is set using a SIMATIC time transmitter. You can configure other settings in "System > Time > SIMATIC Time Client".
- **Drop-down list "SNMP":**
  Select one of the following options from the drop-down list:
  - "-" (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".
  - SNMPv3
    Access to device parameters is possible with SNMP version 3. You can configure other settings in "System > SNMP".
- **Check box "SNMPv1/v2 Read-Only"**
  Enables / disables write access to SNMP variables with SNMPv1/v2.
- **Check box "SNMPv1 Traps"**
  Enables / disables the sending of traps (alarm frames). You can configure other settings in "System > SNMP > Traps".

- **Check box "DHCP Client"**
  Enables / disables the DHCP client. You can configure other settings in "System > DHCP Client".
- **Drop-down list "Configuration Mode":**

  Select one of the following modes from the drop-down list:

  – Automatic
    Automatic save 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, use the "Write Startup Config" button. The "Write Startup Config" button is displayed when you set trial mode. In the display area, the message "Trial Mode Active - Press "Write Startup Config" button to make your settings persistent." is displayed 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.

Steps in configuration

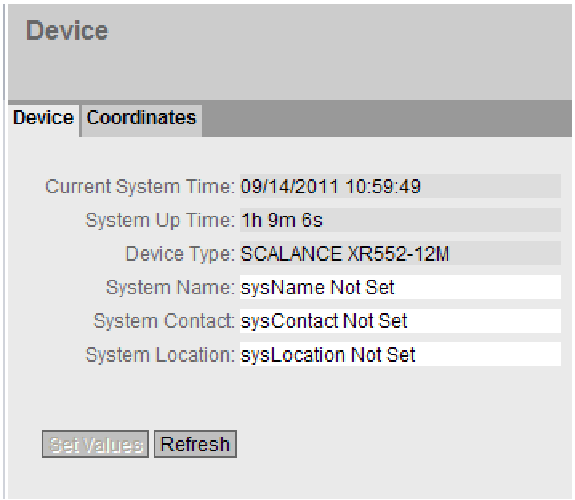
1. Click the check box in front of the functions you want to enable.
2. Select the options you require from the drop-down lists.
3. Click the "Set Values" button.

3.2 General

3.2.1 Device

General device information

This page contains the general device information.



Current System Time: 09/14/2011 10:59:49
System Up Time: 1h 9m 6s
Device Type: SCALANCE XR552-12M
System Name: sysName Not Set
System Contact: sysContact Not Set
System Location: sysLocation Not Set

The boxes "Current System Time", "System Up Time" and "Device Type" cannot be changed.

Description of the displayed boxes

The page contains the following boxes:

- Current System Time
  The current 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. (readonly)
- System Up Time
  The time since the last restart. (readonly)
- Device Type
  The type of the device. (readonly)
- Input box "System Name"
  Here, 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.

- **Input box "System Contact"**
  Here you can enter the name of a contact person responsible for managing the device. A maximum of 255 characters are possible.
- **Input box "System Location"**
  Here, you can enter the Location 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.

Steps in configuration

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.

3.2.2 Coordinates

Information on geographic coordinates

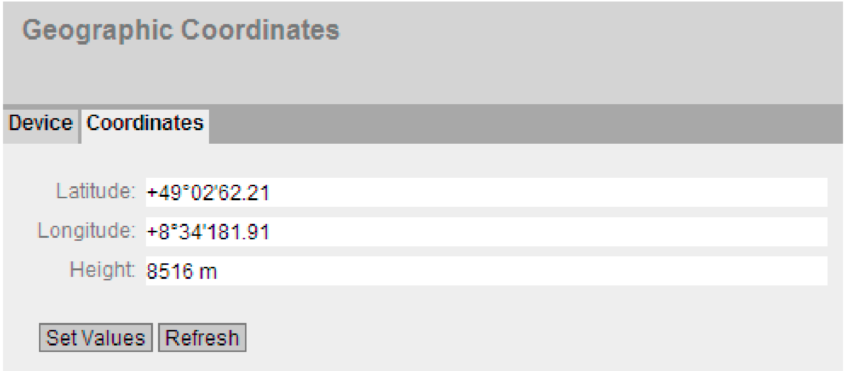
In the "Geographic Coordinates" window, you can enter or read out information on the geographic coordinates. To be able to read out the geographic coordinates, the geographic location of the device must be entered correctly once. The parameters of the geographic coordinates (latitude, longitude and the 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.

Following configuration, the device provides you with this geographic data for management purposes using SNMP private MIBs, Telnet or WEB.



Latitude: +49°02'62.21

Longitude: +8°34'181.91

Height: 8516 m

Description of the displayed boxes

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

- Input box "Latitude"
  Geographical latitude: Here, enter the value for the northerly or southerly latitude of the location of the device.

  For example, +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).
- Input box "Longitude"
  Geographical longitude: Here, you enter the value of the eastern or western longitude of the location of the device.
  For example, +8° 20´ 58.73" means that the device is located at 8 degrees, 20 minutes and 58.73 seconds east.
  A western longitude is indicated by a preceding minus sign.
  You can also add the letter E (easterly longitude) or W (westerly longitude) to the numeric information (8° 20´ 58.73" E).
- Input box: "Height"
  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.

Steps in configuration

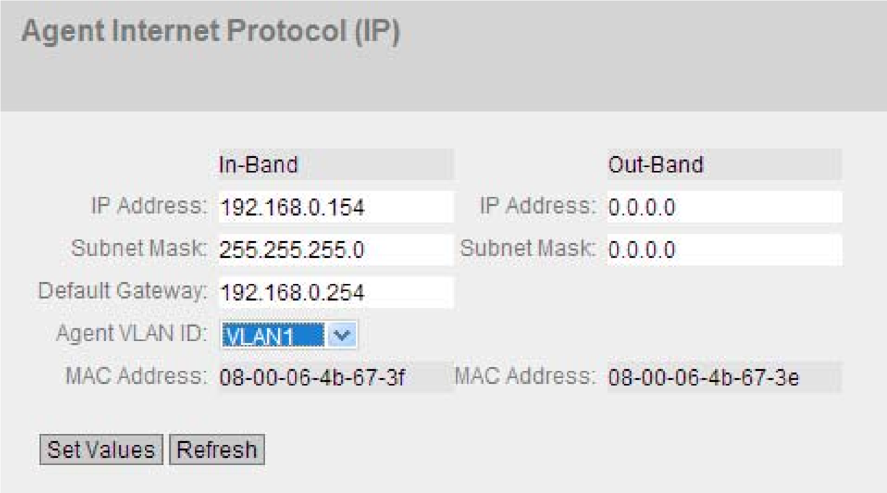
1. Enter the latitude in the "Latitude" input box.
2. Enter the longitude in the "Longitude" input box.
3. Enter the height in the "Height" input box.
4. Click the "Set Values" button to transfer the values you have set to the device.

3.3 Agent IP

Configuration of the IP addresses

Here, you specify the IP configuration for the device.

With SCALANCE X devices, a distinction is made between the switch ports ("In-Band" column) and the Ethernet port of the switch CPU ("Out-Band" column).



Agent Internet Protocol (IP)

	In-Band		Out-Band
IP Address:	192.168.0.154	IP Address:	0.0.0.0
Subnet Mask:	255.255.255.0	Subnet Mask:	0.0.0.0
Default Gateway:	192.168.0.254		
Agent VLAN ID:	VLAN1		
MAC Address:	08-00-06-4b-67-3f	MAC Address:	08-00-06-4b-67-3e

Note

The IP addresses of the in-band interface and the out-band interface must belong to different subnets.

Description of the displayed boxes

The page contains the following boxes:

- Input box "IP Address"
  Here, in "In-Band", you enter the IP address via which the management will be accessible via the switch ports. In "Out-Band", enter the IP address at which the management will be accessible via the out-band port.

  If you change the IP address, you should be automatically guided to the new address. If this does not happen, enter the new address in the Web browser manually.
- Text box "Subnet Mask"
  Here, in "In-Band", you enter the subnet mask of the CPU module and in "Out-Band" the subnet mask of the out-band port.
- Text box "Default Gateway"
  If the device is required to communicate with devices (diagnostics stations, e-mail servers etc.) in another subnet, enter the IP address of the default gateway here. The out-band port it is not accessible from a different subnet.

- Drop-down list "Agent VLAN ID"

  From the drop-down list, select the VLAN ID for the in-band management. You can only select VLANs that have already been configured.

  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.

  To be able to reach the device again via Ethernet, adapt the settings for "Layer 2 > VLAN > General" and "Layer 2 > VLAN > Port Based VLAN".

- Text box "MAC Address"

  The MAC address of the device depends on the hardware and cannot be modified.

Configuration procedure for SCALANCE X500 devices

Follow the steps below to configure the in-band:

1. In the input boxes under "In Band", enter the IP address, subnet mask and the default gateway.
2. Select the assigned VLAN ID from the "Agent VLAN ID" drop-down list.
3. Click the "Set Values" button.

Follow the steps below to configure the out-band:

1. In the input boxes under "Out Band", enter the IP address and subnet mask.
2. Click the "Set Values" button.

Configuration procedure for SCALANCE W700 devices

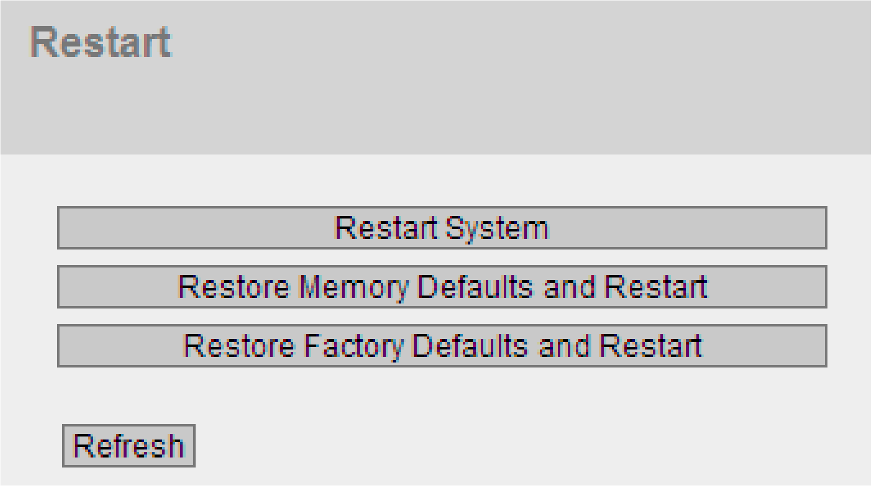
Follow these steps during configuration:

1. In the input boxes, enter the IP address, subnet mask and the default gateway.
2. Select the assigned VLAN ID from the "Agent VLAN ID" drop-down list.
3. Click the "Set Values" button.

3.4 Restart

Resetting to the defaults

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



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

Note

Note the following points about restarting a device:

- You can only restart the device with administrator privileges.
- A device should only be restarted with the buttons of this menu or with the appropriate CLI commands 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", any configuration modifications must be saved manually before a restart. In "Autosave mode", the last changes are saved automatically before a restart.

Description of the displayed boxes

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 learned entries in the address table are deleted. You can leave the browser window open while the device restarts. You then 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
  - (R)STP

W

With SCALANCE W700 devices, the following parameters are also not reset.

- Mode of the device
- Locale setting

- Restore Factory Defaults and Restart
  Click this button to restore the factory defaults for the configuration. The protected defaults are also reset.
  An automatic restart is triggered.

Note

By resetting all the defaults to the factory settings, the IP address is also lost. Following this, the device can only be accessed using the Primary Setup Tool or using DHCP.

With the appropriate attachment, a previously correctly configured device can cause circulating frames and therefore the failure of the data traffic.

3.5 Load & Save

3.5.1 HTTP

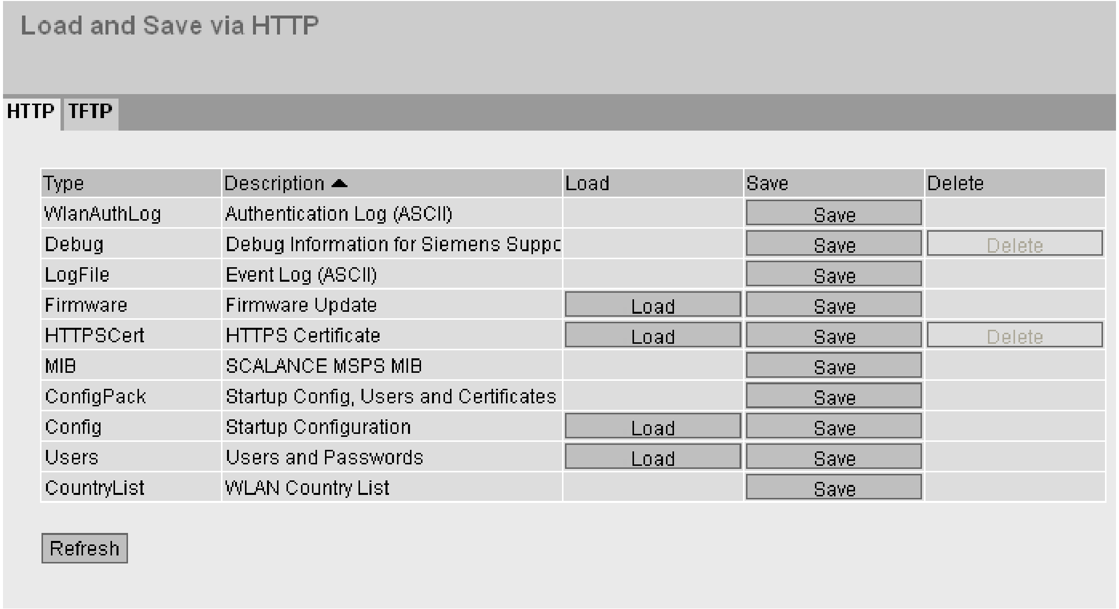
Loading and saving data via HTTP

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

Note

Configuration files and trial mode

In Trial mode, although the changes are adopted, they are not saved in the configuration files (ConfigPack and Config). To save changes in the configuration file, use the "Write Startup Config" button. You will find more detailed information on the WBM page "System > Configuration".



Load and Save via HTTP

Type	Description ▲	Load	Save	Delete
WlanAuthLog	Authentication Log (ASCII)		Save	
Debug	Debug Information for Siemens Suppc		Save	Delete
LogFile	Event Log (ASCII)		Save	
Firmware	Firmware Update	Load	Save	
HTTPSCert	HTTPS Certificate	Load	Save	Delete
MIB	SCALANCE MSPS MIB		Save	
ConfigPack	Startup Config, Users and Certificates		Save	
Config	Startup Configuration	Load	Save	
Users	Users and Passwords	Load	Save	
CountryList	WLAN Country List		Save	

Description of the displayed boxes

The table has the following columns:

- **Type**
  The file type is specified here.

W With SCALANCE W devices, you can also load or store the following document types.

- WlanAuthLog
- Country List
- In client mode:
  - Server certificate
  - User certificate

    For the user certificate, a password can be created on the WBM page "Security > WLAN > Client RADIUS supplicant" in "Dot1x user Certificate Password".

- Description
  The description of the document is shown here.
- Load
  With this button, you can upload files to the device. The button can be enabled, if this function is supported by the file type.
- Save
  With this button, you can 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, delete the cache of the Web browser.

Steps in configuration

Loading files using HTTP

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

   The dialog for uploading a file opens.
2. Go to the file you want to upload.
3. Click the "Open" button in the dialog.

   The file is now uploaded.
4. After loading, restart the device. The changes only take effect a restart.

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 was 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. Download this configuration file to 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.

3.5.2 TFTP

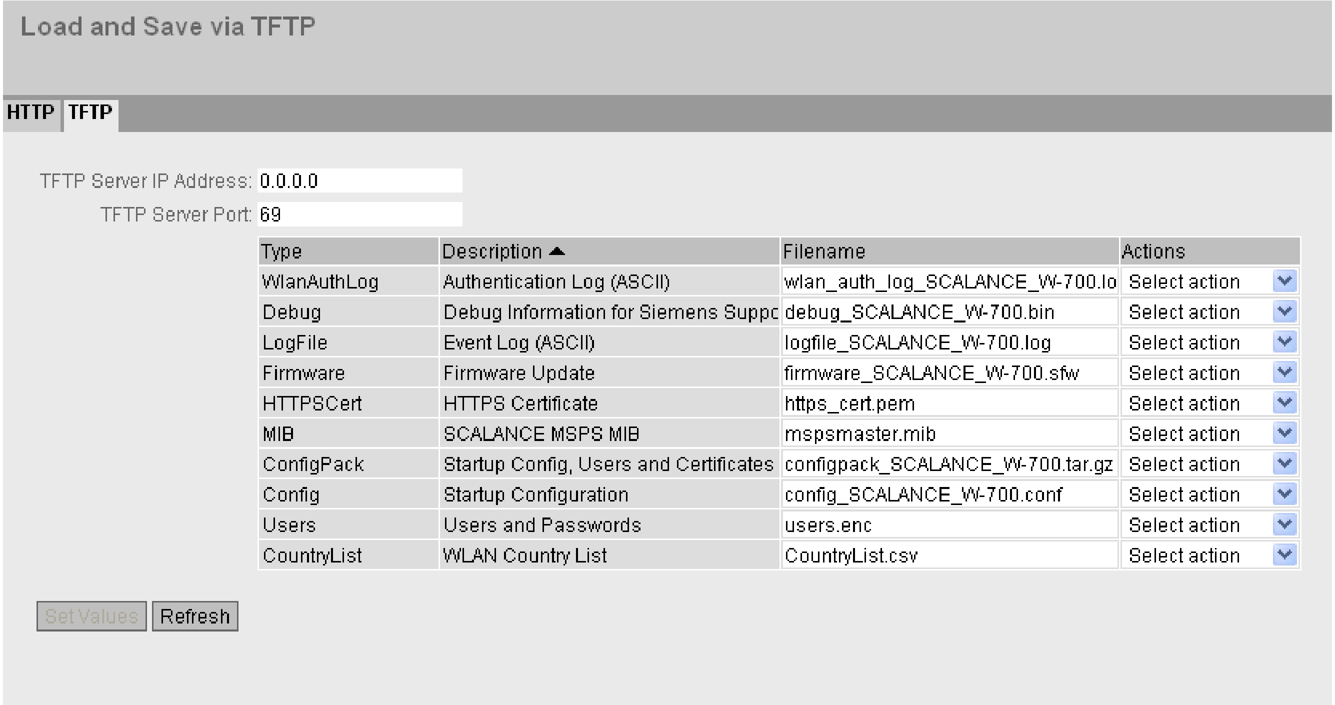
Loading and saving data via a TFTP server

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

Note

Configuration files and trial mode

In Trial mode, although the changes are adopted, they are not saved in the configuration files (ConfigPack and Config). To save changes in the configuration file, use the "Write Startup Config" button. You will find more detailed information on the WBM page "System > Configuration".



Load and Save via TFTP

TFTP Server IP Address: 0.0.0.0

TFTP Server Port: 69

Type	Description ▲	Filename	Actions
WlanAuthLog	Authentication Log (ASCII)	wlan_auth_log_SCALANCE_W-700.lo	Select action
Debug	Debug Information for Siemens Suppc	debug_SCALANCE_W-700.bin	Select action
LogFile	Event Log (ASCII)	logfile_SCALANCE_W-700.log	Select action
Firmware	Firmware Update	firmware_SCALANCE_W-700.sfw	Select action
HTTPSCert	HTTPS Certificate	https_cert.pem	Select action
MIB	SCALANCE MSPS MIB	mspsmaster.mib	Select action
ConfigPack	Startup Config, Users and Certificates	configpack_SCALANCE_W-700.tar.gz	Select action
Config	Startup Configuration	config_SCALANCE_W-700.conf	Select action
Users	Users and Passwords	users.enc	Select action
CountryList	WLAN Country List	CountryList.csv	Select action

Description of the displayed boxes

The page contains the following input boxes:

- TFTP Server IP Address
  Here, enter the IP address of the TFTP server with which you want to exchange data.
- TFTP Server Port
  Here, 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
  The file type is specified here.

W

With SCALANCE W devices, you can also load or store the following document types.

- WlanAuthLog
- Country List
- In client mode:
  - Server certificate
  - User certificate

    For the user certificate, a password can be created on the WBM page "Security > WLAN > Client RADIUS supplicant" in "Dot1x user Certificate Password".

- Description
  A brief description of the document is shown here.
- Filename
  The name of the file on the TFTP server is specified here.
- Actions
  The selection depends on the selected file type, for example the log file can only be saved.
  The options are as follows:
  - 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.

Steps in configuration

Loading or saving data 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 a name for the file in which you want to save the data or take the data from in the "Filename" input box.
4. Select the action you want to execute from the "Actions" drop-down list.
5. Click the "Set Values" button to start the selected actions.
6. After loading the configuration and the SSL certificate, restart the device. The changes only take effect a restart.

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:

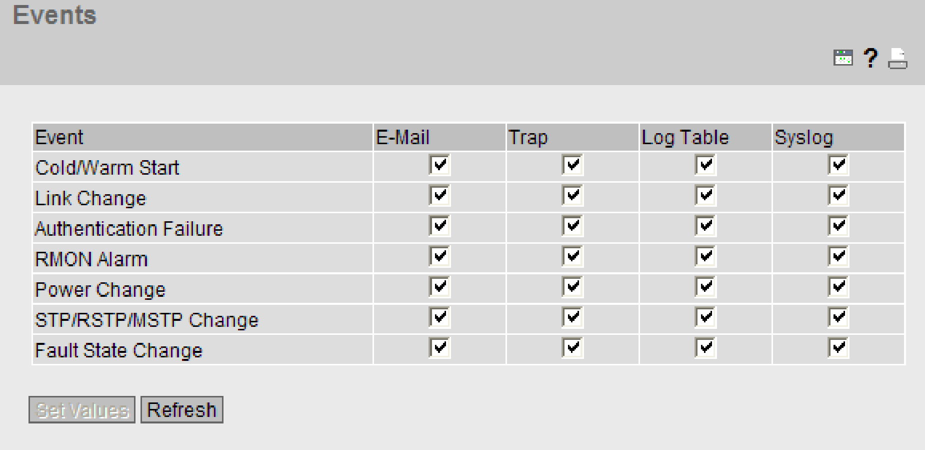
1. Save the configuration data of a configured device on your PC. As an alternative, you can save the data on your computer.
2. Download this configuration file to all other devices you want to configure.
3. If individual settings are necessary for specific devices, these must be made online on the relevant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

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

3.6 Events

Selecting system events

On this page, you specify how a device reacts to system events. By enabling the appropriate check boxes, you specify which events trigger which reactions on the device. To enable or disable the options, click the relevant check boxes of the columns.



Event	E-Mail	Trap	Log Table	Syslog
Cold/Warm Start	☑	☑	☑	☑
Link Change	☑	☑	☑	☑
Authentication Failure	☑	☑	☑	☑
RMON Alarm	☑	☑	☑	☑
Power Change	☑	☑	☑	☑
STP/RSTP/MSTP Change	☑	☑	☑	☑
Fault State Change	☑	☑	☑	☑

Description of the displayed boxes

The table has the following columns:

- E-Mail
  The device sends an e-mail. This is only possible if the SMTP server is set up and the "SMTP client" function is enabled.
- Trap
  The device sends an SNMP trap. This is only possible if "SNMPv1 Traps" is enabled in "System > Configuration".
- Log Table
  The device writes an entry in the event log table.
- 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.

W With SCALANCE W devices, there is also the following column:

- Fault
  The device triggers a fault. The error LED lights up.

The "Event" column contains the following values:

- Cold/Warm Start
  The device was turned on or restarted by the user.
- Link Change
  A port has failed or data traffic is being handled again over a port that had previously failed.
- Authentication Failure
  There was an SNMP access with a bad password or inadequate access rights.
- Power Change
  This event occurs only when power supply lines 1 and 2 are monitored. It indicates that there was a change to line 1 or line 2.
- STP/RSTP/MSTP Change
  The STP or RSTP or MSTP topology has changed.

X With SCALANCE X devices, there are also the following events:

- RMON Alarm
  An alarm or event has occurred relating to the remote monitoring of the system.
- 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.

W With SCALANCE W devices, there are also the following events:

- WLAN Authentication Log
  When entries are made in the log file.
- WLAN De/Authentication (Only in client mode)
  With successful or failed authentication attempts.
- Overlap Detection (Only in access point mode)
  There is overlapping of the wireless channels so that an access point occupies not only the set channel but also the two or three adjacent channels.
- WDS (Only in access point mode)
  The connection status of WDS has changed.
- Radar Interferences (Only in access point mode)
  There is transmission interference, for example caused by radar or weather stations.

Steps in configuration

Changing entries

1. Click the check box in the row of the event you want to configure. Select the event in the column under the following actions:

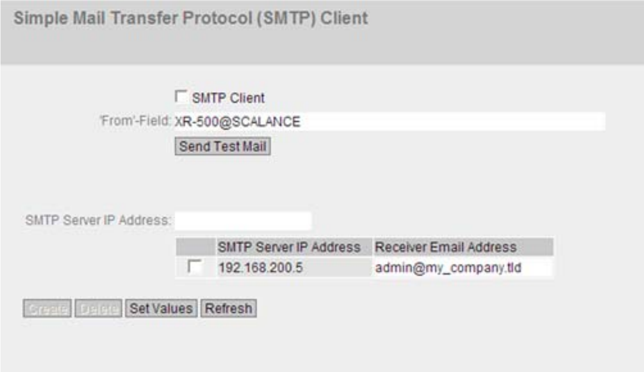
- E-mail
- SNMP trap
- Log file
- Syslog

2. Click the "Set Values" button.

3.7 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 event message is received, the WBM can be started by the browser using the identification of the sender to read out further diagnostics information.



Simple Mail Transfer Protocol (SMTP) Client

□ SMTP Client

'From'-Field: XR-500@SCALANCE

SMTP Server IP Address:

	SMTP Server IP Address	Receiver Email Address
□	192.168.200.5	admin@my_company.tld

Description of the displayed boxes

The page contains the following boxes:

- **Check box "SMTP Client"**
  Select this check box to enable the SMTP client.
- **Input box "'From'-Field"**
  Here, enter the e-mail address of the sender.
- **Input box "SMTP Server IP Address"**
  Here, enter the IP address of the SMTP server.
- **Button "Send TestMail"**
  Sends an e-mail for testing.

This table contains the following columns:

- **Check box for deleting**
  Select this check box to enable the delete status.
- **SMTP Server IP Address**
  The IP address of the SMTP server is adopted here.
- **Receiver Email Address**
  Here, you enter the E-mail address to which the device sends an e-mail if a fault occurs.

Steps in configuration

Follow the steps below to configure the SMTP client:

1. Click the "SMTP Client" check box to enable the function.
2. Enter the data in the appropriate input boxes.
3. Click the "Set Values" button.

Note

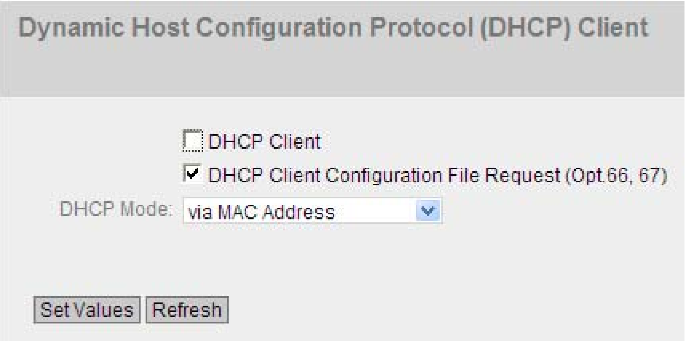
Depending on the properties and configuration of the SMTP server, it may be necessary to adapt the "'From'-Field” input box for the e-mails. Check with the administrator of the SMTP server. You can set the "'From'-Field" using WBM, CLI, or direct SNMP access.

3.8 DHCP client

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.

On this page, you can enable the client functionality of the device.



Dynamic Host Configuration Protocol (DHCP) Client

☐ DHCP Client

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

DHCP Mode: via MAC Address

Description of the displayed boxes

The page contains the following boxes:

- **Check box "DHCP Client"**
  Select this option if the DHCP client is to be used.
- **Check box "DHCP Client Config File Request (Op. 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.
- **Drop-down list "DHCP Mode"**
  Here, you set the DHCP mode.

  The following modes can be selected:

  – 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.

Steps in configuration

There are several configuration options for identifying the device in the configuration of the DHCP server:

1. Select the suitable configuration options from the "DHCP Mode" drop-down list.
2. If you have selected the DHCP mode "via DHCP Client ID", enter a string to identify the device in the activated "DHCP Client ID" input box. This is then evaluated by the DHCP server. Letters and numbers are permitted.
3. 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.
4. Click the "Set Values" button.

NOTICE
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.

3.9 SNMP

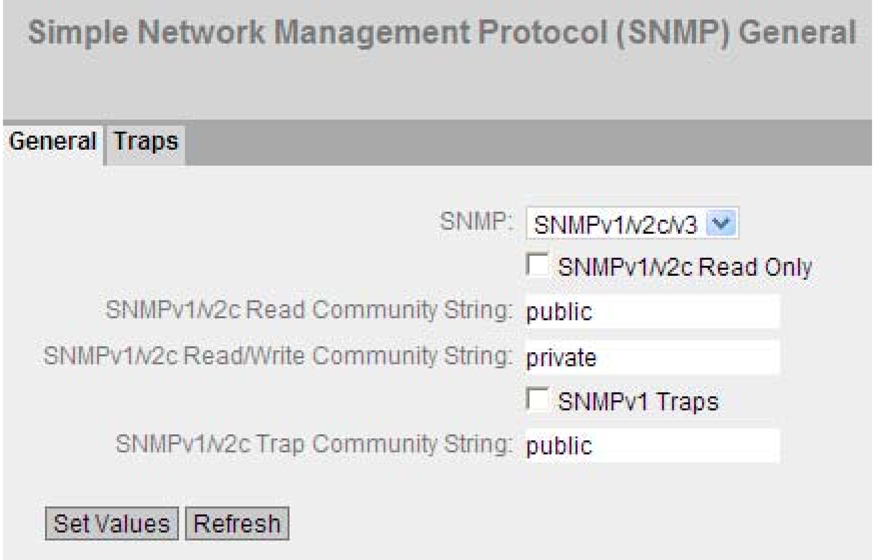
3.9.1 General

Description of the SNMP agent

How SNMP works

Using SNMP (**S**imple **N**etwork **M**anagement **P**rotocol), a management station can configure and monitor SNMP-compliant nodes such as an IE switch. To allow this, a management agent is installed on the device with which the management station exchanges data. The options for this are as follows:

- Read
  The management station reads values from a device.
- Write
  The management station writes values to a device.
- Send events to registered nodes (traps).
  The agent sends messages to the registered management stations.



Simple Network Management Protocol (SNMP) General

SNMP: SNMPv1/v2c/v3

□ SNMPv1/v2c Read Only

SNMPv1/v2c Read Community String: public

SNMPv1/v2c Read/Write Community String: private

□ SNMPv1 Traps

SNMPv1/v2c Trap Community String: public

SNMPv3 (and SNMPv2c) enhancements compared with SNMPv1

SNMPv3 (and SNMPv2c) has the following enhancements compared with the original SNMPv1:

- Management stations can communicate with each other.
- User-defined security settings
- SNMPv2c/v3 has a GetBulk

Access permissions with SNMP

When using the SNMPv1 and v2c protocol, you specify access permissions by means of the community string. A community string contains information about the user name and password in a string. Different community strings are defined for read and write permissions. In the simplest case, the community string is transferred in plain language. More complex and more secure authentication methods are only possible in SNMPv3.

Note

For security reasons, you should not use the standard values "public" or "private". Change the values following the initial installation.

Configuration of SNMP

On this page, you make the basic settings for SNMP. Enable the check boxes according to the SNMP functionality you want to use. For detailed settings (traps, groups, users), there are separate menu items in WBM.

Steps in configuration

1. Select one of the following options from the "SNMP" drop-down list:
   - "-" (disabled)
   - SNMPv1/v2c/v3
   - SNMPv3
2. Click 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 a maximum of 63 characters for the SNMP protocol.
4. In the "SNMPv1/v2c Read/Write Community String" input box, enter a maximum of 63 characters for the SNMP protocol.
5. In the "SNMPv1/v2c Trap Community String" input box, enter a maximum of 63 characters for the SNMP protocol.
6. Click the "SNMPv1 Traps" check box and enable / disable the sending of SNMPv1 messages.
7. Click the "Set Values" button.

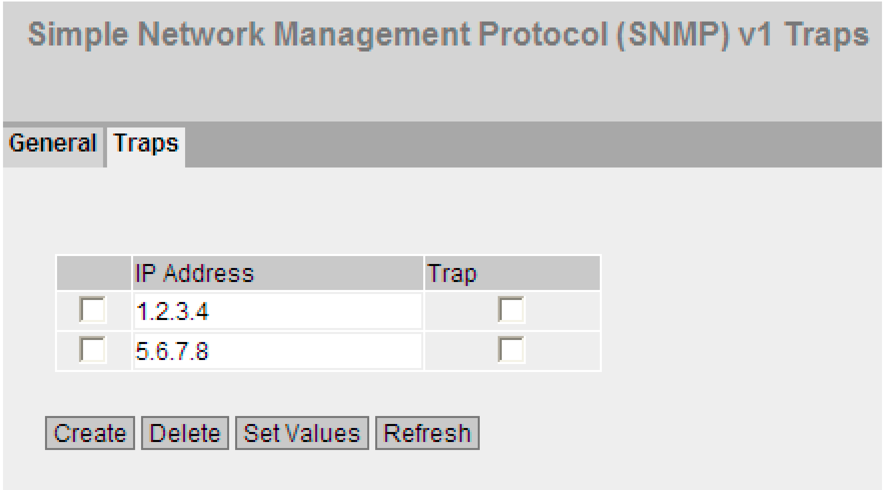
3.9.2 Traps

SNMP traps for alarm events

If an alarm event occurs, a device can send 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 sent only when the "SNMPv1 Traps" option was selected in the "General" menu.



Simple Network Management Protocol (SNMP) v1 Traps

	IP Address	Trap
□	1.2.3.4	□
□	5.6.7.8	□

Steps in configuration

Creating a trap entry

1. Click the "Create" button to create a new trap entry.
2. In the input boxes of the "IP Address" column, enter the addresses of the stations to which the device will send traps. You can specify up to ten different IP addresses for various recipients.
3. Click the check box next to the IP addresses to enable the sending of traps to these stations. Stations that are entered but not selected do not receive any alarm frames.
4. Click the "Set Values" button.

Deleting a trap entry

1. Select the check box next to the IP address whose trap entry you want to delete.
2. Click the "Delete" button to delete a trap entry.

3.10 System time

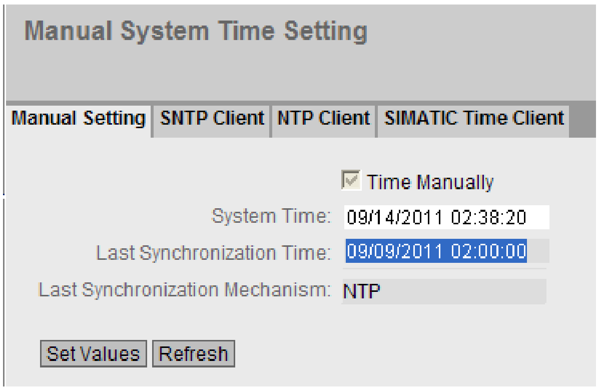
There are four different methods that can be used to set the system time of the device. Only one method can be active at any one time.

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

3.10.1 Manual setting

Manual setting of the system time

On this page, you set the date and time of the system yourself. For this setting to be used, enable "Time Manually".



Manual System Time Setting

☑ Time Manually

System Time: 09/14/2011 02:38:20

Last Synchronization Time: 09/09/2011 02:00:00

Last Synchronization Mechanism: NTP

Description of the displayed boxes

The page contains the following boxes:

- Check box "Time Manually"
  Select this check box to enable the manual time setting. The "System Time" box becomes active.
- System Time
  This box displays the current system 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

- 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. The following methods are possible:
  - Not set
    The system time was not set manually.
  - Manual
    Manual time setting
  - SNTP
    Automatic time-of-day synchronization via SNTP
  - NTP
    Automatic time-of-day synchronization with NTP
  - SIMATIC
    Automatic time-of-day synchronization using SIMATIC time-of-day frames, synchronized with the time transmitter.

Steps in configuration

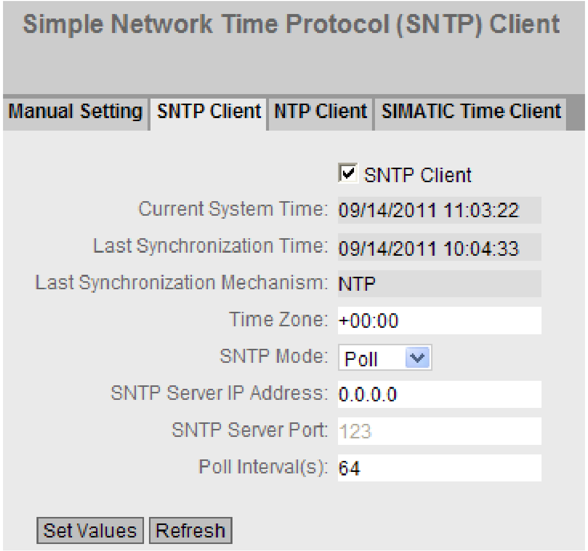
Setting the time and date

1. Click the "Time Manually" check box to enable manual setting of the date and time of the system.
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.

3.10.2 SNTP client

Time-of-day synchronization in the network

The SNTP (**S**imple **N**etwork **M**anagement **P**rotocol) is used for time-of-day synchronization in the network. The appropriate frames are sent by an SNTP server in the network.



☑ SNTP Client

Current System Time: 09/14/2011 11:03:22

Last Synchronization Time: 09/14/2011 10:04:33

Last Synchronization Mechanism: NTP

Time Zone: +00:00

SNTP Mode: Poll

SNTP Server IP Address: 0.0.0.0

SNTP Server Port: 123

Poll Interval(s): 64

Description of the displayed boxes

The page contains the following boxes:

- Check box "SNTP Client"
  Select this check box to enable automatic time-of-day synchronization with SNTP. If you enable this check box, the "Time Zone" input box and the "SNTP Mode" drop-down list become active.
- Display box "Current System Time"
  Display of the values currently set in the system for date and time.
- Display box "Last Synchronization Time"
  This box is read-only and shows when the last time-of-day synchronization took place.

- Display box "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 manually.
  - Manual
    Manual time setting
  - SNTP
    Automatic time-of-day synchronization via SNTP
  - SIMATIC
    Automatic time-of-day synchronization using SIMATIC time-of-day frames, synchronized with the time transmitter.
  - NTP
    Automatic time-of-day synchronization with NTP
- Input box "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.
- Drop-down list "SNTP Mode"
  Select the synchronization mode from the drop-down list. Here, you have the following options:
  - 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.
- Input box "SNTP Server IP Address"
  Here, enter the IP address of the SNTP server.
- Input box "SNTP Server Port"
  Here, enter the port of the SNTP server.
  The following ports are possible:
  - 123 (standard port)
  - 1025 through 36564
- Input box "Poll Interval(s)"
  Here, enter the interval between two-time queries. In this box, you enter the query interval in seconds. Possible values are 16 to 16284 seconds.

Steps in configuration

Configure the automatic time setting of the SNTP client as follows:

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.

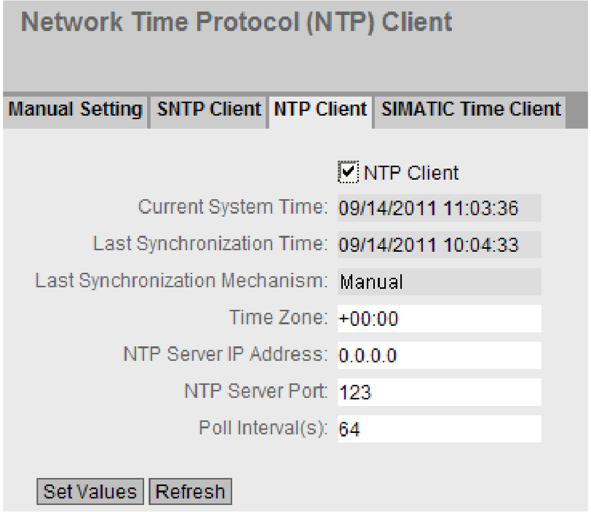
6. In the "Poll Interval(s)" input box, enter the time in seconds after which a new time query is sent to the time server.

7. Click the "Set Values" button to transfer your changes to the device.

3.10.3 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: 09/14/2011 11:03:36

Last Synchronization Time: 09/14/2011 10:04:33

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 of the displayed boxes

The page contains the following boxes:

- Check box "NTP Client"
  Select this check box to enable automatic time-of-day synchronization with NTP. If you select this check box, the "Time Zone", "NTP Server IP Address", "NTP Server Port" and "Poll Interval(s)" input boxes are enabled.
- Display box "System Time"
  This box displays the current system time.
- Display box "Last Synchronization Time"
  This box is read-only and shows when the last time-of-day synchronization took place.

- **Display box "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 manually.
  - Manual
    Manual time setting
  - SNTP
    Automatic time-of-day synchronization via SNTP
  - NTP
    Automatic time-of-day synchronization with NTP
  - SIMATIC
    Automatic time-of-day synchronization using SIMATIC time-of-day frames, synchronized with the time transmitter.
- **Input box "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.
- **Input box "NTP Server IP Address"**
  Here, enter the IP address of the NTP server.
- **Input box "NTP Server Port"**
  Enter the port of the NTP server.
  The following ports are possible:
  - 123 (standard port)
  - 1025 through 36564
- **Input box "Poll Interval(s)"**
  Here, enter the interval between two-time queries. In this box, you enter the query interval in seconds. Possible values are 16 to 16284 seconds.

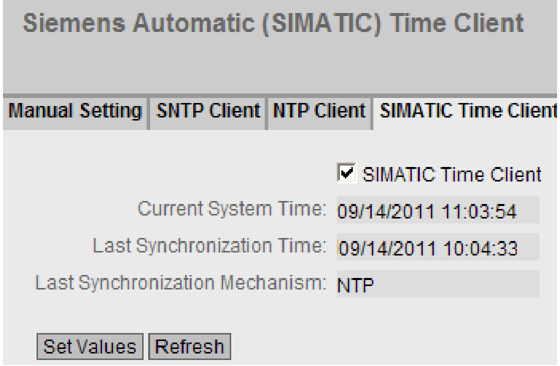
Steps in configuration

Configure the NTP client as follows:

1. Click the "NTP Client" check box to enable the automatic time setting via 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.

3.10.4 SIMATIC time client

Time setting via SIMATIC time client



☑ SIMATIC Time Client

Current System Time: 09/14/2011 11:03:54

Last Synchronization Time: 09/14/2011 10:04:33

Last Synchronization Mechanism: NTP

Description of the displayed boxes

The page contains the following boxes:

- Check box "SIMATIC Time Client"
  Select this check box to enable the device as a SIMATIC time client.
- Display box "System Time"
  This box displays the current system time.
- Display box "Last Synchronization Time"
  This box is read-only and shows when the last time-of-day synchronization took place.
- Display box "Last Synchronization Mechanism"
  This box displays how the last time-of-day synchronization was performed. The following methods are possible:
  - Not setThe system time was not set manually.
  - ManualManual time setting
  - SNTP
    Automatic time-of-day synchronization via SNTP
  - NTP
    Automatic time-of-day synchronization with NTP
  - SIMATIC
    Automatic time-of-day synchronization using SIMATIC time-of-day frames, synchronized with the time transmitter.

Steps in configuration

Setting the time and date

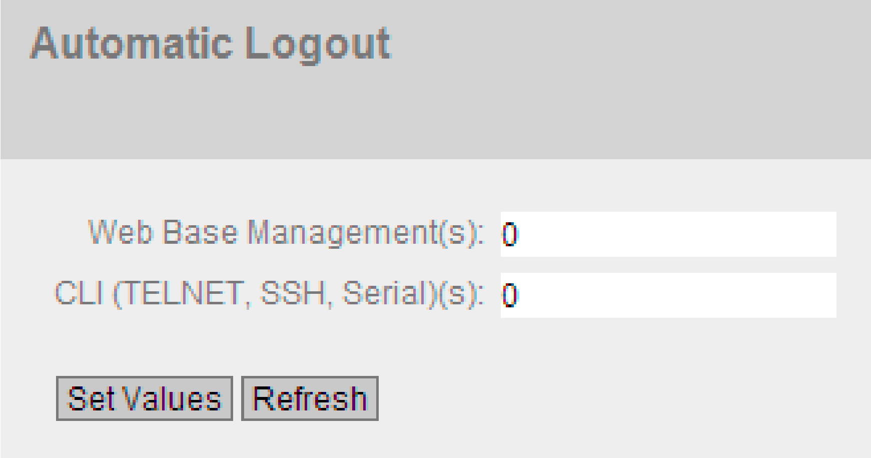
1. Click the "SIMATIC Time Client" check box to enable the SIMATIC Time Client.
2. Click the "Set Values" button.

3.11 Auto logout

Setting the automatic logout

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

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


Automatic Logout

Web Base Management(s): 0

CLI (TELNET, SSH, Serial)(s): 0

Configuration

Enter the values in the input boxes as follows:

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, Serial)(s)" input box. If you enter the value 0, the automatic logoff is disabled.
   With SCALANCE W devices, there is no serial interface available.
3. Click the "Set Values" button.

3.12 Select/Set button configuration

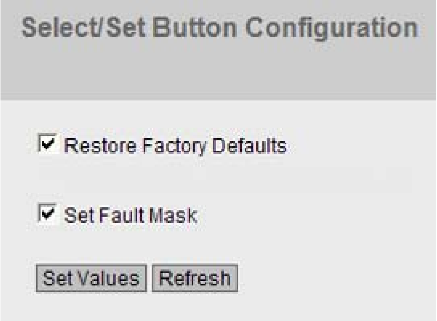
Description of the Select/Set button

The "Select/Set" button is used for the following:

- Changing the display mode,
- Resetting to factory defaults,
- Defining the fault mask and the LED display,

You will find a detailed description of the individual functions available with the buttons in the device operating instructions.

On this page, the functionality of the Select/Set button can be restricted or fully disabled.



Select/Set Button Configuration

☑ Restore Factory Defaults

☑ Set Fault Mask

Description of the displayed boxes

The following functions are possible:

- Restore Factory Defaults
  Enables/disables the "reset to factory defaults" function for the Select/Set button.
- Set Fault Mask
  Enables/disables the "Define fault mask and the LED display" for the Select/Set button.

Steps in configuration

1. Click the check box of the required function to enable or disable it.
2. Click the "Set Values" button.

3.13 Syslog client

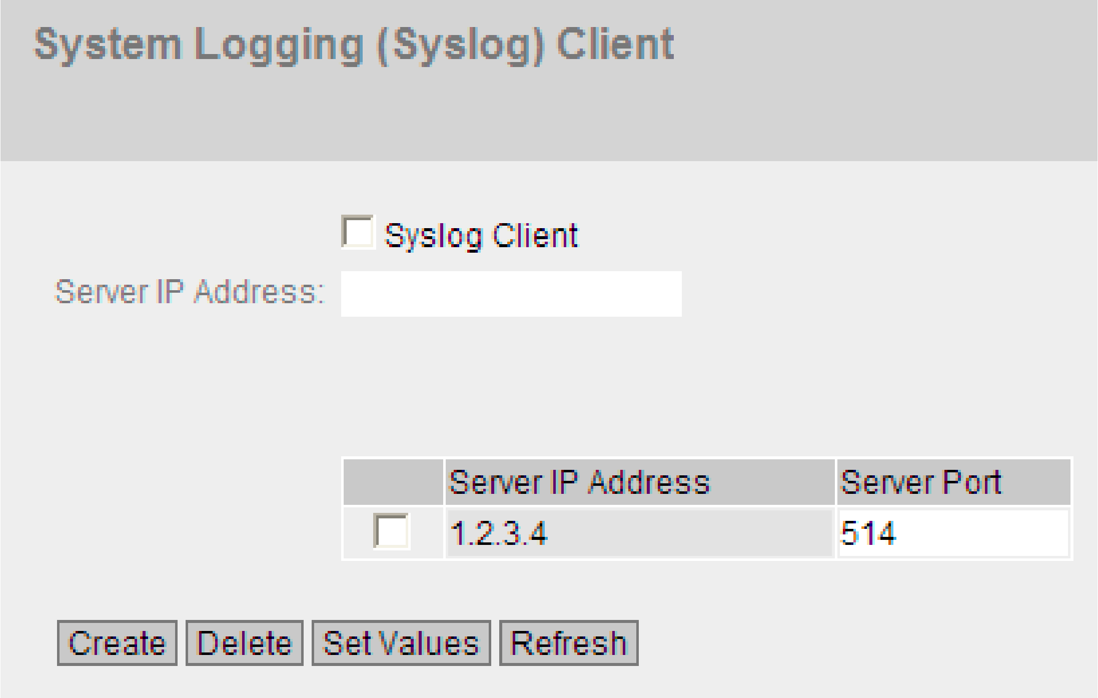
System event agent

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

Server IP Address:

	Server IP Address	Server Port
□	1.2.3.4	514

Description of the displayed boxes

The page contains the following boxes:

- Check box "Syslog Client"
  Click the check box to enable the Syslog function.
- Input box "Server IP Address"
  Here, enter the IP address of the Syslog server.
- Column entry "Server IP Address"
  In this box, you will see the IP address of the Syslog server.
- Column entry "Server Port"
  Enter the port being used on the Syslog server.

Steps in configuration

Follow the steps below to configure on this page:

Enabling function

1. Click the "Syslog client" check box to enable the function.
2. Click the "Set Values" button.

Creating new entry

1. In the "Server IP Address" input box, enter the IP address of the Syslog server on which the log entries will be saved.
2. Click the "Create" button to create a new empty entry.
3. In the "Server Port" input box, enter the number of the UDP port of this server.
4. Click the "Set Values" button.

Note

The default setting of the server port is 514.

A maximum of one Syslog server can be created.

Changing the entry

Change the IP address of the Syslog server as follows.

1. Delete the entry.
2. Create a new entry.

Deleting an entry

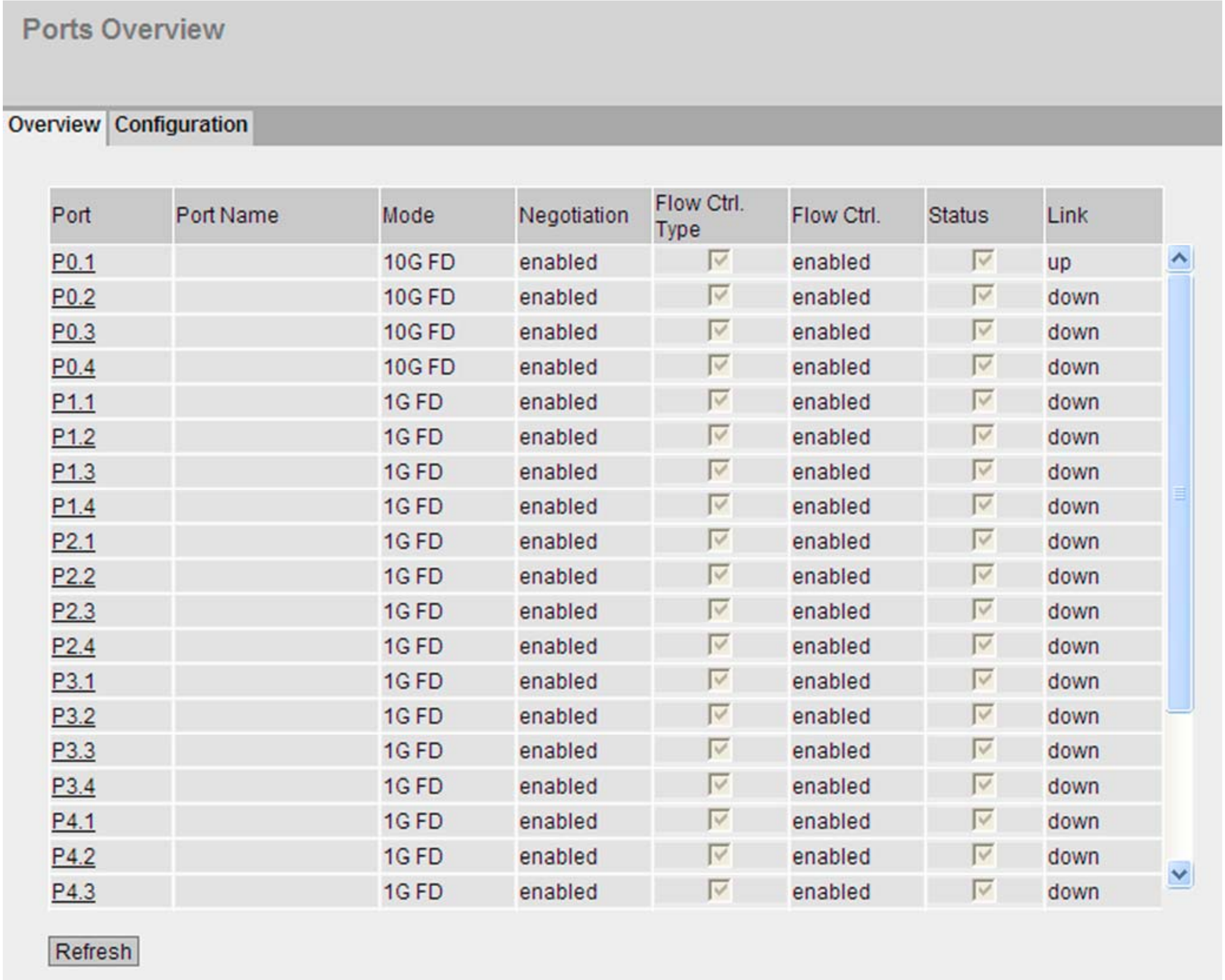
1. Click the check box in front of each entry in the table you want to delete.
2. Click the "Delete" button. All selected entries are deleted and the display is refreshed.

3.14 Ports

3.14.1 Overview

Overview of the port configuration

The page shows the configuration for data transfer for all ports of the device (and, if appropriate, for the ports of the expansions). You cannot configure anything on this page.



Ports Overview

Port	Port Name	Mode	Negotiation	Flow Ctrl. Type	Flow Ctrl.	Status	Link
P0.1		10G FD	enabled	☑	enabled	☑	up
P0.2		10G FD	enabled	☑	enabled	☑	down
P0.3		10G FD	enabled	☑	enabled	☑	down
P0.4		10G FD	enabled	☑	enabled	☑	down
P1.1		1G FD	enabled	☑	enabled	☑	down
P1.2		1G FD	enabled	☑	enabled	☑	down
P1.3		1G FD	enabled	☑	enabled	☑	down
P1.4		1G FD	enabled	☑	enabled	☑	down
P2.1		1G FD	enabled	☑	enabled	☑	down
P2.2		1G FD	enabled	☑	enabled	☑	down
P2.3		1G FD	enabled	☑	enabled	☑	down
P2.4		1G FD	enabled	☑	enabled	☑	down
P3.1		1G FD	enabled	☑	enabled	☑	down
P3.2		1G FD	enabled	☑	enabled	☑	down
P3.3		1G FD	enabled	☑	enabled	☑	down
P3.4		1G FD	enabled	☑	enabled	☑	down
P4.1		1G FD	enabled	☑	enabled	☑	down
P4.2		1G FD	enabled	☑	enabled	☑	down
P4.3		1G FD	enabled	☑	enabled	☑	down

Description of the displayed boxes

The table has the following columns:

- Port
  This shows the port to which the information in the columns of the row relates. All the configurable ports on this device are displayed here.

X With SCALANCE X devices, the port is made up of the port number and the slot number, for example port 0.1 is slot 0, port 1.

W With SCALANCE W devices, the port is made up of the port number, for example P 1 is port 1.

- Port Name
  The name of port is displayed here.
- Mode
  The transmission parameter of the port is shown here.
- Negotiation
  Shows whether the automatic configuration is enabled or disabled.

X With SCALANCE X devices, there are also the following options:

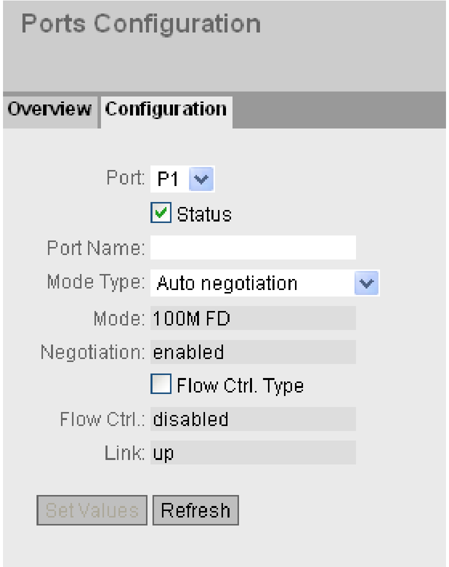
- Flow Ctrl. Type
  Shows whether flow control is enabled or disabled for the port.
- Flow Ctrl.
  Shows whether flow control is working on this port.

- Status
  Shows whether the port is on or off. Data traffic is possible only over an enabled port.
- link
  This box indicates the 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.

3.14.2 Configuration

Configuring ports

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



Ports Configuration

Port: P1

☑ Status

Port Name:

Mode Type: Auto negotiation

Mode: 100M FD

Negotiation: enabled

□ Flow Ctrl. Type

Flow Ctrl.: disabled

Link: up

Description of the displayed boxes

The table has the following rows:

- Drop-down list "Port"
  Here, you select the port to which the following information relates. All the configurable ports on this device are displayed here. The entries in this drop-down list cannot be changed.

X With SCALANCE X devices, the port is made up of the port number and the slot number, for example port 0.1 is slot 0, port 1.

W With SCALANCE W devices, the port is made up of the port number, for example P 1 is port 1.

- Check box "Status"
  Turns the port on or off. Data traffic is possible only over an enabled port.
- Input box ""Port Name"
  Here, enter a name for the port.
- Drop-down list "Mode Type"
  From this drop-down list, select the transmission speed and the duplicity of the port. If you set the mode to "Auto negotiation", these parameters are automatically negotiated with the connected end device. This must also be in the "Autonegotiation" mode.

Note

Set the mode to "Autonegotiation" if you want to use the automatic configuration of the connection to the partner port.

- Display box "Mode"
  Shows the transmission speed and the duplicity of the port. The transmission speed can be 10 Mbps, 100 Mbps, 1000 Mbps or 10 Gbps. As the transmission mode, you can configure full duplex (FD) or half duplex (HD).
- Display box "Negotiation"
  Shows whether the automatic configuration of the connection to the partner port is enabled or disabled.

With SCALANCE X devices, there are also the following options:

- Flow Ctrl. Type
  Shows whether flow control is enabled or disabled for the port.
- Flow Ctrl.
  Shows whether flow control is working on this port.

- Display box "Link"
  This box indicates the 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.

Changing the port configuration

Click the appropriate box to change the configuration.

Note

Optical ports only work with the full duplex mode and at maximum transmission rate. As a result, the following settings cannot be made for optical ports:

- Automatic configuration
- Transmission speed
- Transmission technique

Note

With various automatic functions, the device prevents or reduces the effect on other ports and priority classes (Class of Service) if a port is overloaded. This can mean that frames are discarded even when flow control is enabled.

Port overload occurs when the device receives more frames than it can send, for example as the result of different transmission speeds.

Steps in configuration

Follow the steps below to change the settings:

1. Change the settings according to your configuration.

2. Click the "Set Values" button.

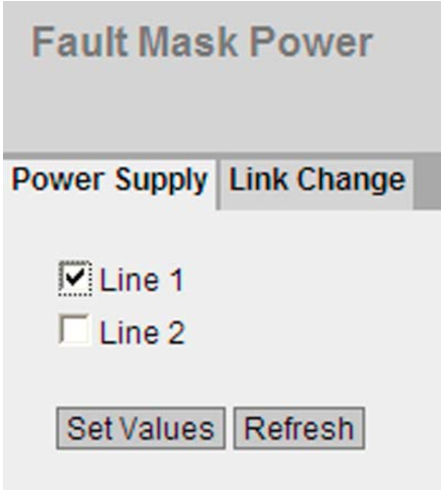
3.15 Fault monitoring

3.15.1 Power Supply

Settings for monitoring the power supply

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

A fault is then signaled by the message system when there is no power on one of the monitored lines (line 1 or line 2) or when the voltage is too low (less than 14 V). A fault causes the signaling contact to trigger and the fault LED on the device to light up and, depending on the configuration of the event table, can trigger a trap, an e-mail, or an entry in the event log table.



Fault Mask Power

☑ Line 1
□ Line 2

Steps in configuration

Set the monitoring of the power supply as follows:

1. Click the check box in front of the line name you want to monitor to enable or disable the monitoring function.
2. Click the "Set Values" button.

3.15.2 Link Change

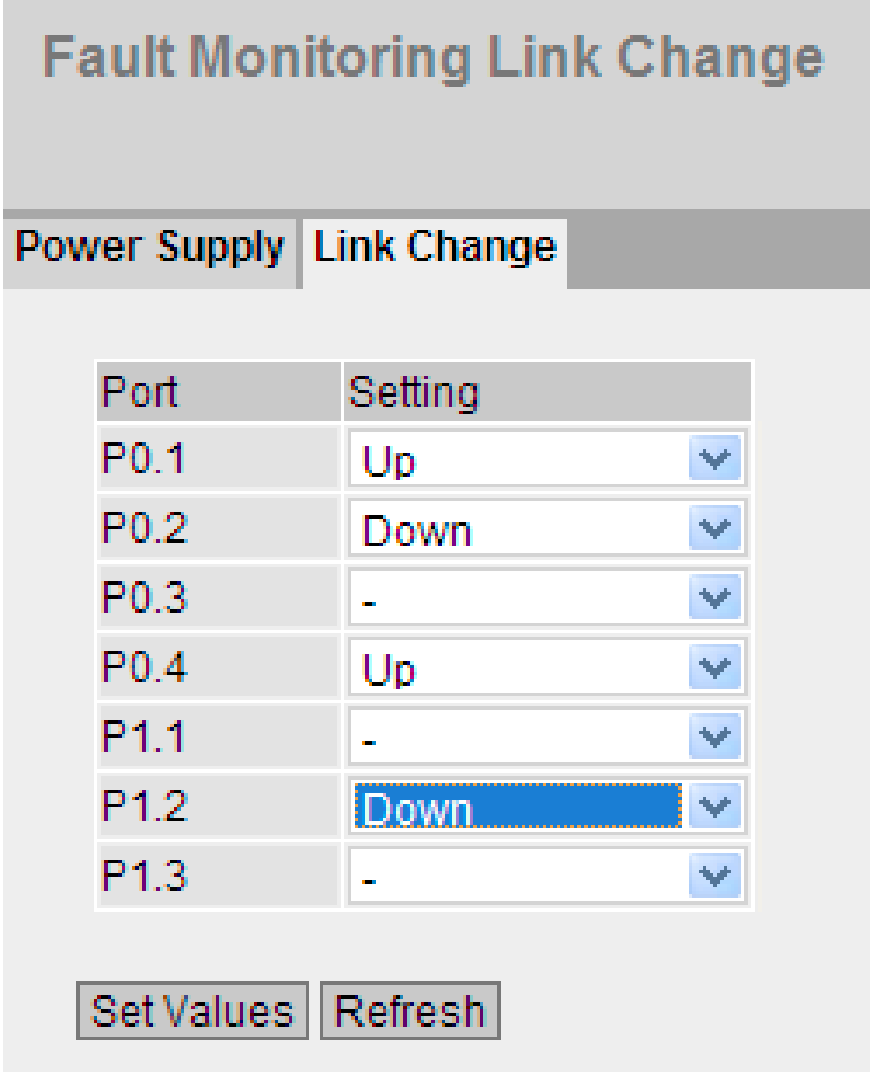
Configuration of fault monitoring of status changes on connections

On this page, you configure whether or not an error message is triggered if there is a status change on a network connection.

If connection monitoring is enabled, an error is signaled

- when there should be a link on a port and this is missing.
- or when there should not be a link on a port and a link is detected.

The error message is then output on the configured path (signaling contact, fault LED, SNMP trap, e-mail, entry in the log table, Syslog).



Fault Monitoring Link Change

Port	Setting
P0.1	Up
P0.2	Down
P0.3	-
P0.4	Up
P1.1	-
P1.2	Down
P1.3	-

Description of the displayed boxes

The table has the following columns:

- Port
  All available ports are listed in this column. Unavailable ports are not displayed.

X With SCALANCE X devices, this column lists all available ports and the link aggregations.
The port is made up of the port number and slot number, for example port 0.1 is slot number 0, port number 1.

W With SCALANCE W devices, the port number is displayed, for example, P1 is port number 1.

- Setting
  You have the options for following settings:
  – 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.

Steps in configuration

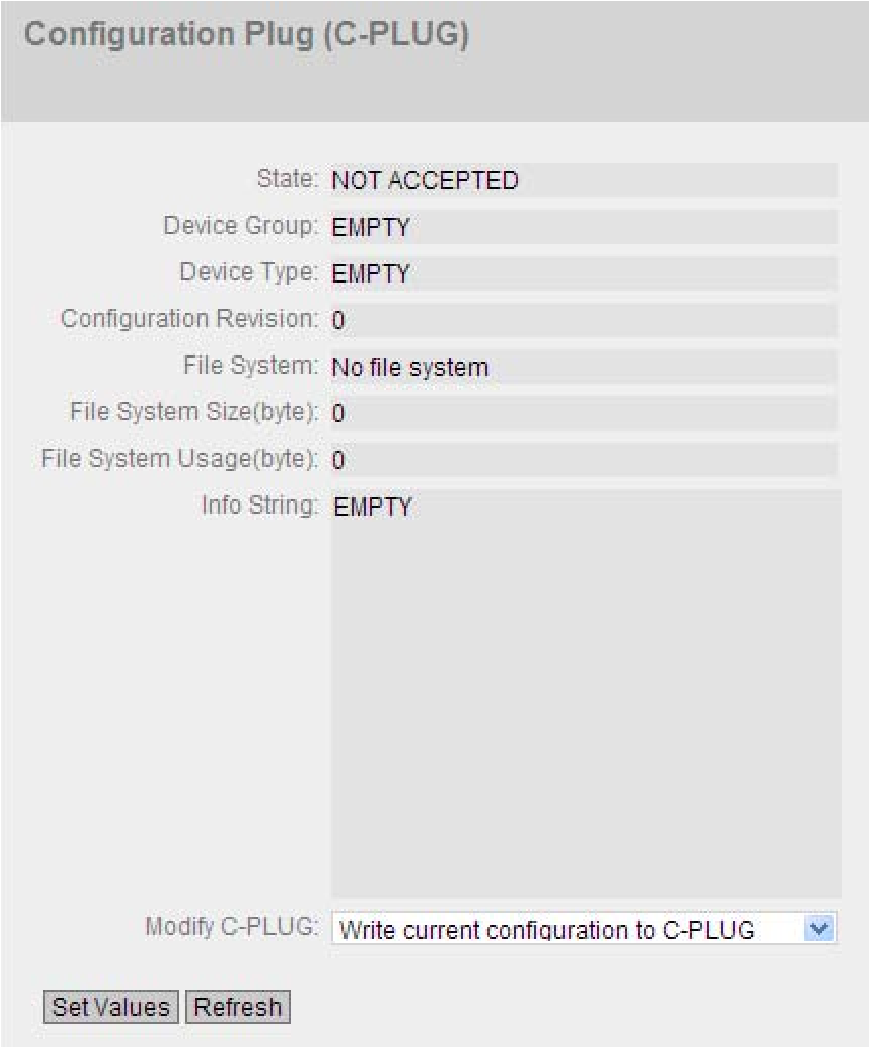
Configure the error monitoring as follows:

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.

3.16 C-PLUG

Information on the content of the C-PLUG

This page provides you with detailed information on the C-PLUG. You can also format the C-PLUG or provide it with new content.



Configuration Plug (C-PLUG)

State: NOT ACCEPTED

Device Group: EMPTY

Device Type: EMPTY

Configuration Revision: 0

File System: No file system

File System Size(byte): 0

File System Usage(byte): 0

Info String: EMPTY

Modify C-PLUG: Write current configuration to C-PLUG

Description of the displayed boxes

The table has the following rows:

- State
  This displays the status of the C-PLUG. The following are possible:
  - ACCEPTED
    A C-PLUG with a valid and suitable content is inserted in the device.
  - NOT ACCEPTED
    Invalid or incompatible content of an inserted C-PLUG. This status is also displayed when the C-PLUG was formatted during operation.
  - NOT PRESENT
    No C-PLUG is inserted in the device.
- Device Group
  Indicates the SIMATIC NET product line that used the C-PLUG previously.
- Device Type
  Indicates 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 C-PLUG.
- File System Size(byte)
  Displays the maximum storage space of the file system on the C-PLUG.
- File System Usage(byte)
  Shows the storage space being utilized in the C-PLUG file system.
- Info String
  Here, additional information is displayed about the device that had used the C-PLUG previously, for example order number, type designation and version of hardware and software.
  With the status "NOT ACCEPTED", further information on the cause of the problem is displayed. If the C-PLUG configuration does not match the device configuration, the Info string of the C-PLUG is displayed instead.
- Drop-down list "Modify C-PLUG"
  Here, you can select the following options from the drop-down list to modify the C-PLUG:
  - Write current configuration to C-PLUG
    The configuration in the flash memory of the device is copied to the C-PLUG and this is followed by a restart.
  - Erase C-PLUG to factory default
    Deletes all data from the C-PLUG and triggers low-level formatting. This is not followed by an automatic restart and the device displays an error. You can clear this error status by restarting or removing the C-PLUG.

Steps in configuration

Follow the steps below to modify the C-PLUG:

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 C-PLUG.
2. Select the required option from the "Modify C-PLUG" drop-down list.
3. Click the "Set Values" button.

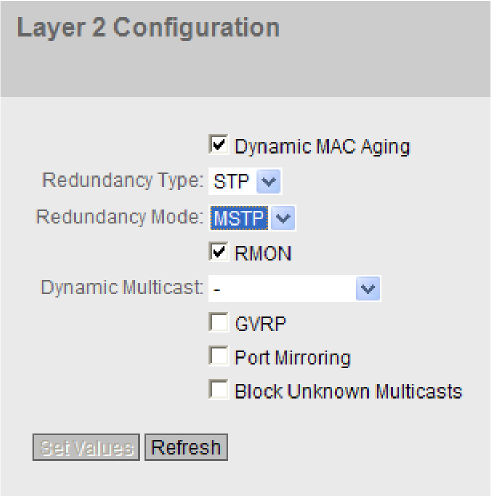
NOTICE
The action is only executed after you click the "Set Values" button. The action cannot be undone. If you decide against executing the function after making your selection, click the "Refresh" button. As a result the data of this page is read from the device again and the selection is canceled.

4 The "Layer 2" menu

4.1 Configuration

Configuring layer 2

On this page, you create a basic configuration for the functions of layer 2. On the configuration pages of these functions, you can make detailed settings. You can also check the settings on the configuration pages.



Layer 2 Configuration

☑ Dynamic MAC Aging

Redundancy Type: STP

Redundancy Mode: MSTP

☑ RMON

Dynamic Multicast: -

□ GVRP

□ Port Mirroring

□ Block Unknown Multicasts

Description of the displayed boxes

"Dynamic MAC Aging" check box

The automatically learned source addresses of the connected nodes are deleted again after a certain period "Aging Time" if no frame with the learned address is received. If the check box is not enabled, a device does not delete learned addresses automatically.

Options of the "Redundancy Type" drop-down list:

- "-" (disabled)
  The redundancy function is disabled. If you select this option, you cannot select anything in the following drop-down list "Redundancy Mode".
- STP
  If you select this option, you can select the following in the "Redundancy Mode" drop-down list:
  - STP (Spanning Tree Protocol)
  - RSTP (Rapid Spanning Tree Protocol)
  - MSTP (Multiple Spanning Tree Protocol)

Options of the "Redundancy Mode" drop-down list

If you select "STP" in the "Redundancy Type" drop-down list, the following options are then available:

- STP
  The Spanning Tree Protocol (STP) is a method with which loops are prevented in redundant network structures. You can enable or disable spanning tree functionality with the check box. Typical reconfiguration times with spanning tree are between 20 and 30 seconds.
- RSTP
  The Rapid Spanning Tree Protocol (RSTP) is a further development of the Spanning Tree Protocol. The aim of RSTP is to achieve a faster reconfiguration within a few seconds. If you select the check box, RSTP is enabled. If a spanning tree frame is detected at a port, this port reverts from RSTP to spanning tree.

  Note

  When using RSTP (Rapid Spanning Tree Protocol), loops involving duplication of frames or frames being overtaken may occur briefly. If this is not acceptable in your particular application, use the slower standard spanning tree mechanism.
- MSTP
  The Multiple Spanning Tree Protocol (MSTP) is a further development of the Rapid Spanning Tree Protocol. Among other things, it provides the option of operating several RSTP instances within different VLANs and, for example, making paths available within the individual VLANs that the single Rapid Spanning Tree Protocol would globally block.

"RMON" check box

If you select this check box, Remote Monitoring (RMON) allows diagnostics data to be collected on the device, prepared and read out using SNMP by a network management station that also supports RMON. This diagnostic data, for example port-related load trends, allow problems in the network to be detected early and eliminated. Some of the "Ethernet statistics counters" are part of the RMON function. If you disable RMON, the "Ethernet statistics counters" are no longer updated.

Options of the "Dynamic Multicast" drop-down list

- "-" (disabled)
- IGMP Snooping
  IGMP (Internet Group Management Protocol) allows the assignment of IP addresses to multicast groups. If IGMP snooping is enabled, IGMP frames are evaluated and the multicast filter table is updated with this information.
- GMRP
  If the GMRP option (GARP Multicast Registration Protocol) is selected, GMRP registrations are entered in the multicast filter table for all ports and generated automatically. If the check box is not selected
  - an IE switch does not evaluate received GMRP frames
  - an IE switch does not send its own GMRP frames.

  Note

  GMRP and IGMP cannot operate at the same time.

"GVRP" check box

If you enable the "GVRP" option (GARP VLAN Registration Protocol), the VLAN to which the port belongs is set dynamically by GVRP.

"Port Mirroring" check box

In port mirroring, the data traffic at one or more ports (mirrored ports) of the device is copied to a free port (monitor port). If a protocol analyzer is connected to the monitor port, the data traffic can be recorded without interrupting the connection at the mirrored port.

Note

You can mirror all ports of a device.

If the maximum data rate of the mirrored port is higher than that of the monitor port, data may be lost and the monitor port no longer reflects the data traffic at the mirrored port.

Disable the function if you want to connect a normal end device to the monitor port.

"Block Unknown Multicasts" check box

If the "Block Unknown Multicasts" setting is enabled, the device does not forward any multicast packets of unknown origin. To be forwarded, the multicast addresses must be make known.

Steps in configuration

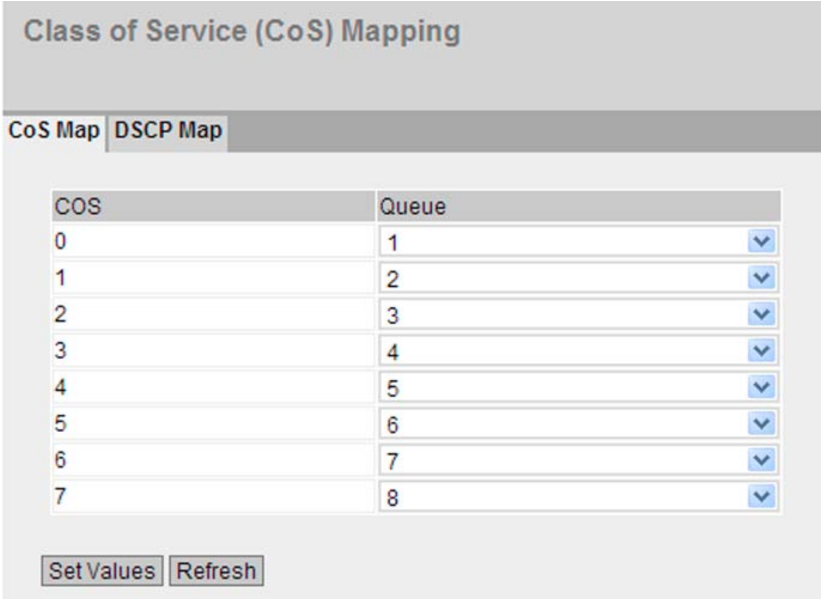
1. Click the check box to enable or disable the corresponding functions.
2. Select the options you require from the drop-down lists.
3. Click the "Set Values" button.

4.2 Qos

4.2.1 CoS queue mapping

COS Queue Mapping

Here, CoS priorities are assigned to certain queues (Traffic Queues).



Class of Service (CoS) Mapping

COS	Queue
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

Description of the displayed boxes

The table has the following columns:

- COS
  The CoS order of priority of the incoming packets.
- Queue
  The traffic-forwarding queue (send priority) that is assigned the CoS priority.

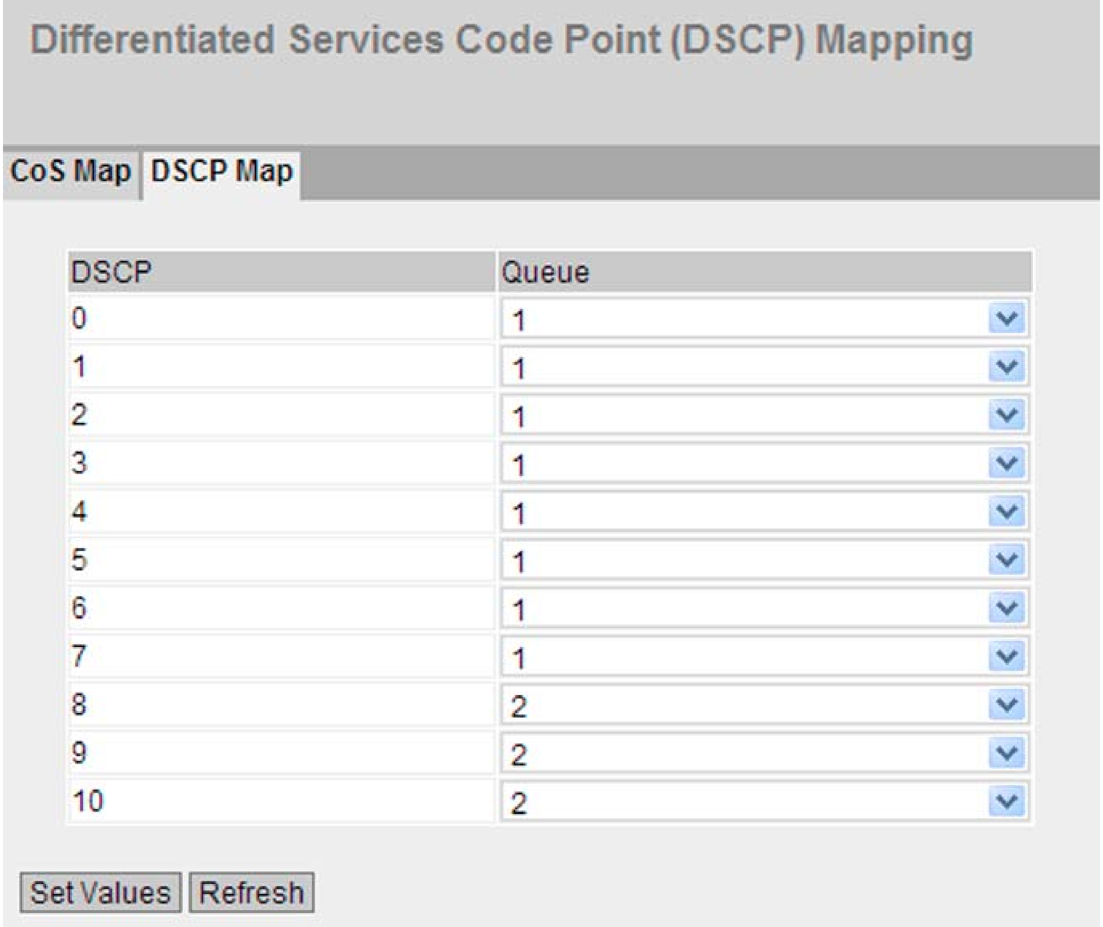
Steps in configuration

1. For each value in the "COS" column, select the forwarding queue from the "Queue" drop-down list.
2. Once you have set all COS values, click the "Set Values" button.

4.2.2 DSCP mapping

DSCP queue

Here, DSCP settings are assigned to various queues (Traffic Queues).



Differentiated Services Code Point (DSCP) Mapping

DSCP	Queue
0	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	2
9	2
10	2

Description of the displayed values

The table has the following columns:

- DSCP
  The DSCP order of priority of the incoming packets.
- Queue
  The traffic-forwarding queue (send priority) that is assigned the DSCP value.

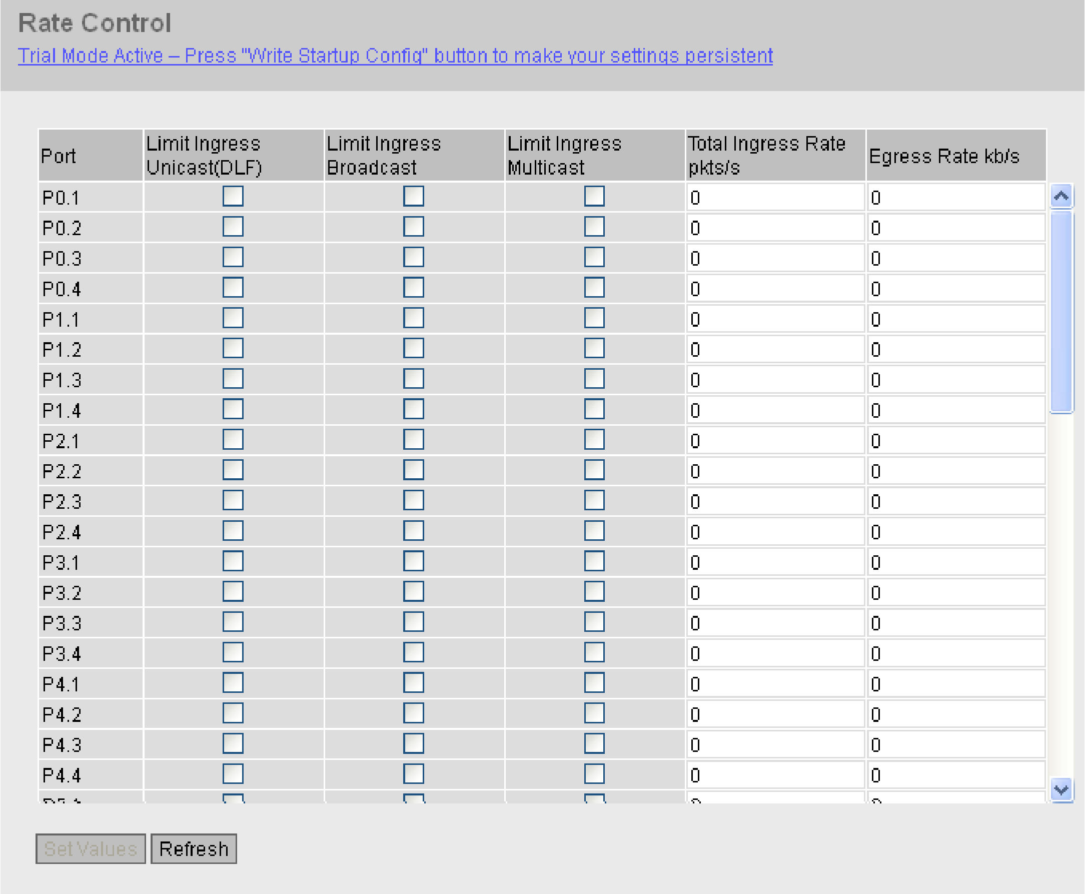
Steps in configuration

1. For each value in the "DSCP" column, select the forwarding queue from the "Queue" drop-down list.
2. Once you have set all DSCP values, click the "Set Values" button.

4.3 Rate control

Limiting the transfer rate of incoming and outgoing data

On this page, you configure the load limitation (maximum number of data packets per second) for the individual ports. You can specify the category of frame for which these limit values will apply.



Rate Control

Trial Mode Active – Press "Write Startup Config" button to make your settings persistent

Port	Limit Ingress Unicast(DLF)	Limit Ingress Broadcast	Limit Ingress Multicast	Total Ingress Rate pkts/s	Egress Rate kb/s
P0.1	□	□	□	0	0
P0.2	□	□	□	0	0
P0.3	□	□	□	0	0
P0.4	□	□	□	0	0
P1.1	□	□	□	0	0
P1.2	□	□	□	0	0
P1.3	□	□	□	0	0
P1.4	□	□	□	0	0
P2.1	□	□	□	0	0
P2.2	□	□	□	0	0
P2.3	□	□	□	0	0
P2.4	□	□	□	0	0
P3.1	□	□	□	0	0
P3.2	□	□	□	0	0
P3.3	□	□	□	0	0
P3.4	□	□	□	0	0
P4.1	□	□	□	0	0
P4.2	□	□	□	0	0
P4.3	□	□	□	0	0
P4.4	□	□	□	0	0

Description of the displayed values

The table has the following columns:

- **Port**
  Displays the slot and the port to which the information relates. This field cannot be configured.
- **Limit Ingress Unicast (DLF)**
  Enables / disables the data rate for limiting incoming unicast frames with an unresolvable address (Destination Lookup Failure).
- **Limit Ingress Broadcast**
  Enables / disables the data rate for limiting incoming broadcast frames.

- Limit Ingress Multicast
  Enables / disables the data rate for limiting incoming multicast frames.
- Total Ingress Rate pkts/s
  Specifies the maximum number of incoming packets processed by the device.
- Egress Rate kb/s
  Specifies the data rate for all outgoing frames.

Note

Rounding of the values, deviation from desired value

When you input the rate values, note that the WBM rounds to correct values.

If values are configured for Total Ingress Rate and Egress Rate, the actual values in operation can exceed or fall below the set values by 10%.

Steps in configuration

1. Enter the relevant values in the columns "Total Ingress Rate" and "Egress Rate" in the row of the port being configured.
2. To use the ingress limitation, enable the check boxes in the required columns of the row. For egress limitation, the value in the "Egress Rate" column is used.
3. Click the "Set Values" button.

4.4 VLAN

4.4.1 General

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 can be 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.

Options for the VLAN assignment

There are various options for the assignment to VLANs:

- Port-based VLAN (layer 2)
- MAC address-based VLAN (layer 2)
- IP address–based VLAN (layer 3) (SCALANCE X only)

A device supports port-based VLAN. This makes it possible to set parameters for the device or to configure it using GVRP frames.

Important rules for VLANs

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

Frames with VLAN-ID "0" (for example only frames with a priority tag) are treated like untagged frames in terms of the VLAN ID, but nevertheless 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. This basic setting is necessary since it is not always certain that all nodes can interpret tagged frames.

As default, a device of the SCALANCE XR-500 series that supports VLAN is set at all ports with VLAN ID 1 (default VLAN).

Note

The VLAN-ID 500 is reserved for future use and is already configured

---

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).

VLAN configuration page

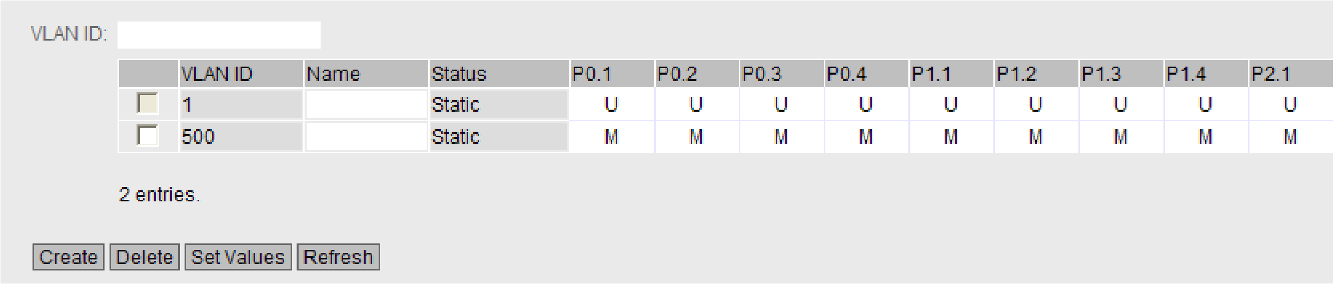
The "Virtual Local Area Network (VLAN) General" page shows the current assignment of the ports in terms of VLAN configuration.

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.

To be able to reach the device again via Ethernet, adapt the settings for "Layer 2 > VLAN > General" and "Layer 2 > VLAN > Port Based VLAN".



VLAN ID:

	VLAN ID	Name	Status	P0.1	P0.2	P0.3	P0.4	P1.1	P1.2	P1.3	P1.4	P2.1
□	1		Static	U	U	U	U	U	U	U	U	U
□	500		Static	M	M	M	M	M	M	M	M	M

2 entries.

Description of the displayed boxes

Use the scroll bar to bring the display to the required position.

"VLAN ID" input box

Make your entries in the "VLAN ID" input box.

The table has the following columns:

W

With SCALANCE W devices, there is also the following option:

Base Bridge Mode
Specifies whether or not the device is configured as a bridge according to IEEE 802.1D for the Spanning Tree protocol or according to IEEE 802.1Q for a virtual bridged LAN:

- 802.1 D Transparent Bridge
  Sets the mode of the device to "transparent" for the Spanning Tree protocol.
- 802.1 Q VLAN Bridge
  Sets the mode of the device to "VLAN-aware" for a virtual bridged LAN. Configure the port-based VLAN.

- Check box
  Click the relevant check box to select the row to be deleted.
- 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 257 VLANs can be defined.
- Name
  This name is assigned when a VLAN is defined. It only provides information and has no effect on the configuration. The length is a maximum of 32 characters.
- Status
  Shows the status type of entry in the port filter table. Here, static means that the address was entered as a static address by the user. The entry GVRP means that the configuration was registered by a GVRP frame. This is, however, only possible if GVRP was enabled for the device.

- **List of ports**
  Shows the VLAN IDs set for the slots or ports. Link aggregations are also displayed. The meaning of the entries in the drop-down lists is as follows:
  - "-"
    The port is not a member of the 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.
  - R
    The port is a member of the VLAN. A GVRP frame is used for the registration.
  - U (uppercase)
    The port is an untagged member of the VLAN. Frames sent in this VLAN are forwarded without the VLAN tag.
  - u (lowercase)
    The port is an untagged member of the VLAN, but the VLAN is not configured as a port VLAN. Frames sent in this VLAN are forwarded without the VLAN tag.
  - F
    The port is not a member of the specified VLAN and it is not possible for the VLAN to be registered dynamically at this port using GVRP.

If a new data record is created, the boxes have the content "-" as default. If you click in the box, a drop-down list opens. In the box you want to configure, select values from the drop-down lists that you want to set.

Steps in configuration

Follow the steps outlined below to configure port-based VLANs:

Step 1: Preparation

Prior to the actual configuration, follow the steps below to configure your VLANs:

1. Specify the nodes for the individual VLANs.
2. Assign the VLAN ID for each node and each device.
3. Specify the device and port to which a connection will exist.

Step 2: Procedure

Set the following configuration on the device:

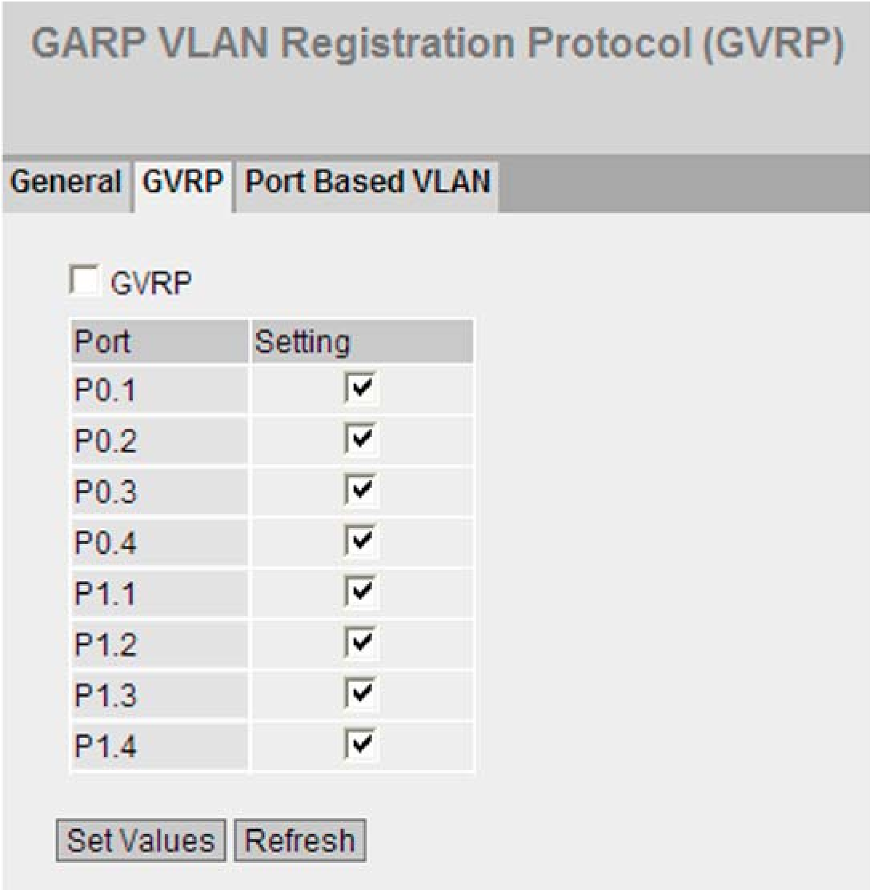
1. Define all VLANs used on this device.
2. Specify which VLAN will be supported on which port.
3. Specify how the frames will be processed entering and leaving the ports.
4. Specify whether frames are sent via the port with or without a VLAN tag.
5. Click the "Set Values" button.

4.4.2 GVRP

Configuration of GVRP functionality

With a GVRP frame, an end node or other device (for example a switch) can register for a specific VID at a port of the device. The device can also send GVRP frames via this port.

On this page, you can enable each port for GVRP functionality.



GARP VLAN Registration Protocol (GVRP)

□ GVRP

Port	Setting
P0.1	☑
P0.2	☑
P0.3	☑
P0.4	☑
P1.1	☑
P1.2	☑
P1.3	☑
P1.4	☑

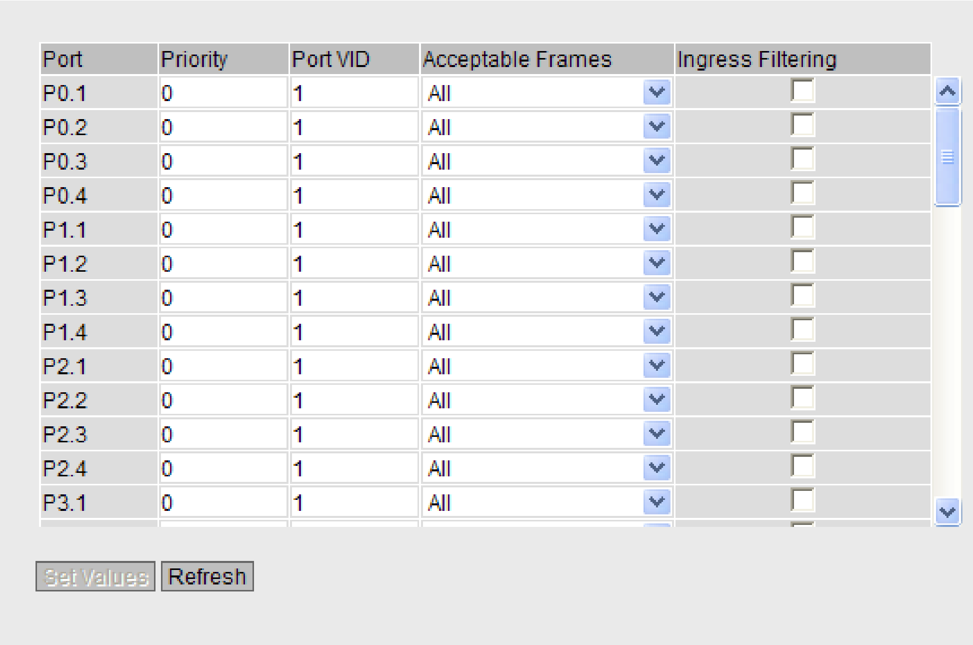
Steps in configuration

1. Click "GVRP" check box.
2. Click the check box after the port in the "Setting" column to enable or disable GVRP for this port.
   Repeat this for every port for which you want to enable or disable the function.
3. Click the "Set Values" button.

4.4.3 Port-based VLAN

Processing received frames

This page shows the rules according to which a device handles received frames.



Port	Priority	Port VID	Acceptable Frames	Ingress Filtering
P0.1	0	1	All	□
P0.2	0	1	All	□
P0.3	0	1	All	□
P0.4	0	1	All	□
P1.1	0	1	All	□
P1.2	0	1	All	□
P1.3	0	1	All	□
P1.4	0	1	All	□
P2.1	0	1	All	□
P2.2	0	1	All	□
P2.3	0	1	All	□
P2.4	0	1	All	□
P3.1	0	1	All	□

Description of the displayed boxes

The table has the following columns:

- Port
  All available ports are listed in this column. Unavailable ports are not displayed.

X With SCALANCE X devices, this column lists all available ports and the link aggregations.
The port is made up of the port number and slot number. , for example port 0.1 is slot 0, port 1.

W With SCALANCE W devices, the port number is displayed, for example, P1 is port number 1.

- Priority
  The 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
  If a received frame has no VLAN tag, it has a tag added with the VLAN-ID specified here and is sent according to the port rules.

  The VLAN ID that is assigned to untagged frames can have the following values:

  - 1 - 4094: Valid VLAN identifier, the frame is assigned to a VLAN and can also include priority information.
- Drop-down list "Acceptable Frames"
  From the drop-down list, select the types of frames that 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.
- Check box "Ingress Filtering"
  This specifies whether the VID of received frames is evaluated
  You have the following options:

  - Enabled
    The VLAN ID of received frames decides whether they are forwarded: To forward a VLAN tagged frame, the receiving port must be a member in the same VLAN. Frames from unknown VLANs are discarded at the receiving port.
  - Disabled
    All frames are forwarded.

Steps in configuration

1. In the row of the port to be configured, click on the relevant cell in the table to configure it.
2. Enter the values to be set in the input boxes as follows.
3. Select the values to be set from the drop-down lists.
4. Click the "Set Values" button.

4.5 Port Mirroring

Mirroring ports

Mirroring a port means that the data traffic at a port (mirrored port) of the IE switch is copied to another port (monitor port).

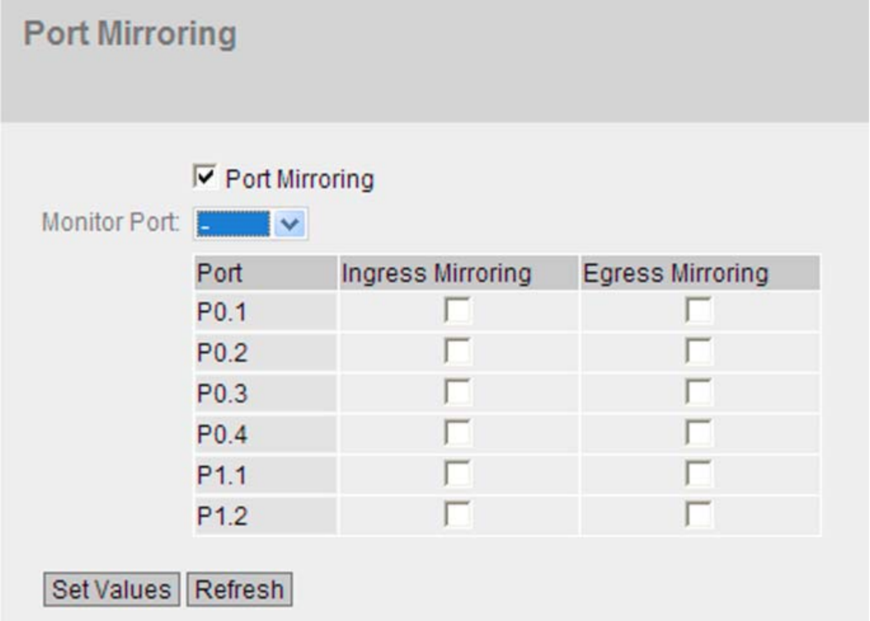
If a protocol analyzer is connected to the monitor port, the data traffic at the mirrored port can be recorded without interrupting the connection. This means that the data traffic can be investigated without being affected. This is possible only if a free port is available on the device as the monitor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

Note

If the maximum data rate of the mirrored port is higher than that of the monitor port, data may be lost and the monitor port no longer reflects the data traffic at the mirrored port.

Mirroring a port does not work beyond switch core boundaries.

Disable port mirroring if you want to connect a normal end device to the monitor port.



Port Mirroring

☑ Port Mirroring

Monitor Port: -

Port	Ingress Mirroring	Egress Mirroring
P0.1	□	□
P0.2	□	□
P0.3	□	□
P0.4	□	□
P1.1	□	□
P1.2	□	□

Description of the displayed boxes

- Check box "Port Mirroring"
  Enables / disables port mirroring.
- Drop-down list "Monitor Port"
  Select the port with which you want to monitor.

- Ingress Mirroring
  Enables/disables listening in on incoming packets at the required port.
- Egress Mirroring
  Enables/disables listening in on outgoing packets at the required port.

Steps in configuration

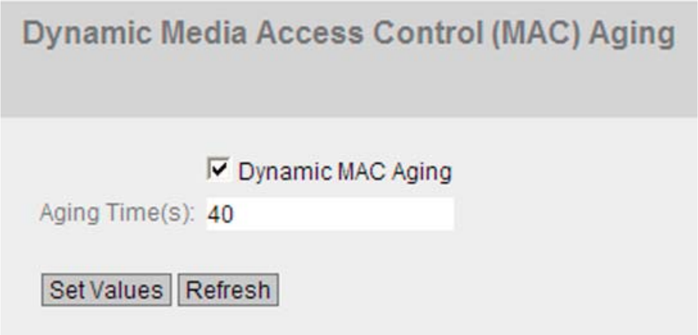
Follow these steps:

1. Click the "Port Mirroring" check box to enable or disable port mirroring.
2. In the "Monitor Port" drop-down list, select the port that will monitor the mirrored port. The monitor port must be a different port form the mirrored port.
3. In the table, click the check box of the row after the port to be mirrored.
   Select whether you want to monitor incoming or outgoing packets.
   To monitor the entire data traffic of the port, select both check boxes.
4. Click the "Set Values" button.

4.6 Dynamic MAC aging

Protocol settings and switch functionality

The device automatically learns the source addresses of the connected nodes. This information is used to forward data 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 switch 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

Steps in configuration

Follow these steps:

1. Click the "Dynamic MAC Aging" check box if you want to enable or disable the function for automatic aging of learned MAC addresses.

2. In the "Aging Time(s)" input box, select the time (in seconds) after which a learned address is deleted again if the device does not receive any further frames from this sender address. The range of values is from 10 seconds to 630 seconds.
3. Click the "Set Values" button.

4.7 MSTP

4.7.1 General

Spanning Tree Protocol (STP)

Avoiding loops on redundant connections

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

Definition of the network topology using the configuration frames

The devices exchange configuration frames known as BPDUs (Bridge Protocol Data Unit) with each other to calculate the topology. The root bridge is selected and the network topology created using these frames. The root bridge is the bridge that controls the spanning tree algorithm for all involved components. BPDUs also bring about the status change of the bridge ports.

Rapid Spanning Tree Protocol (RSTP)

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

- Edge Ports
  A port defined as an edge port is switched active directly following connection establishment. If a spanning tree PDU is received at an edge port, the port loses its role as edge port and it takes part in (R)STP again. If no further BPDU is received after a certain time has elapsed (3 x hello time), the port returns to the edge port status.
- Point-to-point (direct communication between two neighboring devices)
  By directly linking the devices, a status change (reconfiguration of the ports) can be made without any delays.
- Alternate port (substitute for the root port)
  A substitute for the root port is configured. If the connection to the root bridge is lost, the device can establish a connection over the alternate port without any delay due to reconfiguration.
- Reaction to events
  Rapid spanning tree reacts to events, for example an aborted connection, without delay. There is no waiting for timers as in spanning tree.
- Counter for the maximum bridge hops
  In this input box, enter the number of bridge hops a package is allowed to make before it automatically becomes invalid.

  In principle, therefore with rapid spanning tree, alternatives for many parameters are preconfigured and certain properties of the network structure taken into account to reduce the reconfiguration time.

Multiple Spanning Tree Protocol (MSTP)

The Multiple Spanning Tree Protocol (MSTP) is a further development of the Rapid Spanning Tree Protocol. Among other things, it provides the option of operating several RSTP instances within different VLANs and, for example, making paths available within the individual VLANs that the single Rapid Spanning Tree Protocol would globally block.

Common and internal Spanning Tree (CIST)

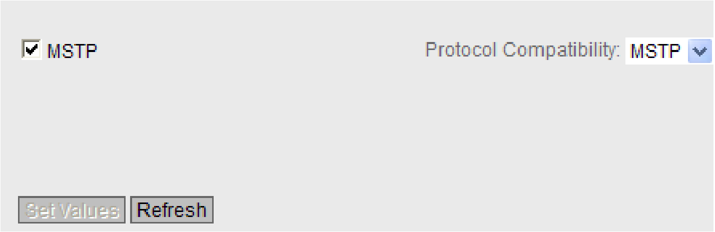
CIST is a term from the multiple spanning tree. CIST identifies the internal instance used by the switch that is comparable in principle with an internal RSTP instance.

General settings of MSTP

On this page, you configure the settings for MSTP. As default, Multiple Spanning Tree is enabled that can be set to the MST, RST or STP compatible mode with a switch.

On the configuration pages of these functions, you can make detailed settings.

Depending on the compatibility mode, you can configure the corresponding function on the relevant configuration page.



☑ MSTP

Protocol Compatibility: MSTP

Description of the displayed boxes

The page contains the following boxes:

- Check box "MSTP"
  Click the check box to enable MSTP.
- Drop-down list "Protocol Compatibility"
  Here, you specify the compatibility mode of MSTP, for example if you select RSTP, MSTP behaves like RSTP.

  The following settings are available:

  – STP

  – RSTP

  – MSTP (SCALANCE W only)

Steps in configuration

Follow the steps below to configure on this page:

1. Click the "MSTP" check box to enable or disable the Spanning Tree Protocol.
2. If you have enabled the Spanning Tree Protocol, select the type of compatibility from the "Protocol Compatibility" drop-down list.
3. Click the "Set Values" button.

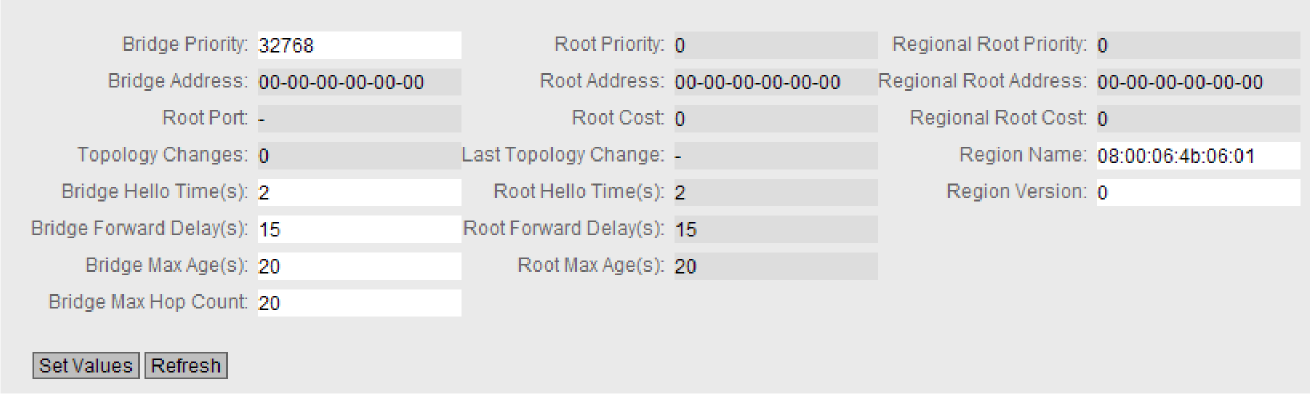
4.7.2 CIST general

MSTP-CIST configuration

The page consists of the following parts.

- The left-hand side of the page shows the configuration of the device.
- The central part shows the configuration of the root bridge that can be derived from the spanning tree frames received by an device.

With SCALANCE X devices, there is also a part on the right. The right-hand side shows the configuration of the regional root bridge that can be derived from the MSTP frames received by an device. The displayed data is only visible if you have enabled "MSTP" on the "General" page and when "MSTP" is set for "Protocol Compatibility". This also applies to the "Bridge Max Hop Count" parameter. If the device is a root bridge, the information on the left and right matches.



Bridge Priority:	32768	Root Priority:	0	Regional Root Priority:	0
Bridge Address:	00-00-00-00-00-00	Root Address:	00-00-00-00-00-00	Regional Root Address:	00-00-00-00-00-00
Root Port:	-	Root Cost:	0	Regional Root Cost:	0
Topology Changes:	0	Last Topology Change:	-	Region Name:	08:00:06:4b:06:01
Bridge Hello Time(s):	2	Root Hello Time(s):	2	Region Version:	0
Bridge Forward Delay(s):	15	Root Forward Delay(s):	15		
Bridge Max Age(s):	20	Root Max Age(s):	20		
Bridge Max Hop Count:	20				

Description of the displayed boxes

The table has the following rows:

- Bridge Priority / Root Priority
  The Bridge priority decides which device becomes the root bridge. The bridge with the highest priority (in other words, with the lowest value for this parameter) becomes the root bridge. If several devices in a network have the same priority, the device whose MAC address has the lowest numeric value will become the root bridge. Both parameters, bridge priority and MAC address together form the Bridge identifier. Since the root bridge manages all path changes, it should be located as centrally as possible due to the delay of the frames. The value for the bridge priority is a whole multiple of 4096 with a range of values from 0 to 32768.
- Bridge Address / Root Address
  The MAC address of the device
- Root Port
  The port over which the device communicates with the root bridge.
- Root Cost The path costs from this device to the root bridge.
- Topology Changes / Last Topology Change
  The entry for the device shows the number of reconfiguration actions due to the spanning tree mechanism since the last startup. For the root bridge, the time since the last reconfiguration is displayed as follows:
  - Seconds: sec unit after the number
  - Minutes: min unit after the number
  - Hour: hr unit after the number

- Bridge Hello Time(s) / Root Hello Time(s)
  Each bridge sends configuration frames (BPDUs) regularly. The interval between two such frames is the Hello time. The default for this parameter is 2 seconds.
- Bridge Forward Delay(s) / Root Forward Delay(s)
  New configuration data is not used immediately by a bridge but only after the period specified in the Forward Delay parameter. This ensures that operation is only started with the new topology after all the bridges have the required information. The default for this parameter is 15 seconds.
- Bridge Max Age / Root Max Age
  Bridge Max Age defines the maximum "age" of a received BPDU for it to be accepted as valid by the switch. The default for this parameter is 20.

X

With SCALANCE X devices, there are also the following options:

- Regional Root Priority
  For a description, see Bridge Priority / Root Priority
- Regional Root Address
  The MAC address of the device.
- Regional Root Cost
  The path costs from this device to the root bridge.
- Bridge Max Hop Count
  This parameter specifies how many MSTP nodes a BPDU may pass through. If an MSTP BPDU is received and has a hop count that exceeds the value configured here, it is discarded. The default for this parameter is 20.
- Region Name
  The name of the MSTP region to which this device belongs. As default, the MAC address of the device is entered here. This value must be the same on all devices that belong to the same MSTP region.
- Region Version
  Version number of the MSTP region in which the device is located. This value must be the same on all devices that belong to the same MSTP region.

W

With SCALANCE W devices, there are also the following options in access point mode:

- Layer-2 Tunnel Admin Edge Port
  Select this check box if there can be an end device on a layer 2 tunnel port. Otherwise a reconfiguration of the network will be triggered whenever a link to this port is modified. The L2T clients should be interconnected.
- Layer-2 Tunnel Auto Edge Port
  Select this check box if you want to detect automatically at all layer 2 tunnel ports whether or not an end device is connected.

Steps in configuration

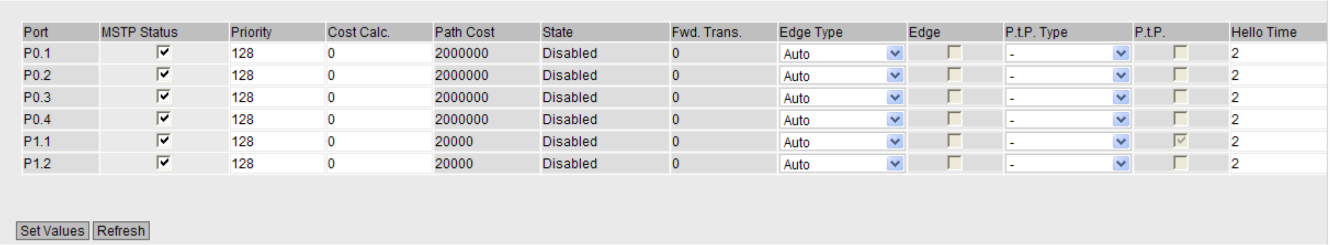
1. Enter the data required for the configuration in the input boxes.
2. Click the "Set Values" button.

4.7.3 CIST port

MSTP-CIST port configuration

When the page is called, the table displays the current status of the configuration of the port parameters.

To configure them, click the relevant cells in the port table.



Port	MSTP Status	Priority	Cost Calc.	Path Cost	State	Fwd. Trans.	Edge Type	Edge	P.t.P. Type	P.t.P.	Hello Time
P0.1	☑	128	0	2000000	Disabled	0	Auto	□	-	□	2
P0.2	☑	128	0	2000000	Disabled	0	Auto	□	-	□	2
P0.3	☑	128	0	2000000	Disabled	0	Auto	□	-	□	2
P0.4	☑	128	0	2000000	Disabled	0	Auto	□	-	□	2
P1.1	☑	128	0	20000	Disabled	0	Auto	□	-	☑	2
P1.2	☑	128	0	20000	Disabled	0	Auto	□	-	□	2

Description of the displayed boxes

The table has the following columns:

- Port
  All available ports are listed in this column. Unavailable ports are not displayed.

X With SCALANCE X devices, the port is made up of the port number and slot number. , for example port 0.1 is slot 0, port 1.

W With SCALANCE W devices, the port number is displayed, for example, P1 is port number 1.

- .MSTP Status
  With MSTP status, you specify whether or not the port is integrated in the spanning tree. As default, this option is enabled.

  Note

  If you disable the "MSTP Status" option for a port, this may cause the formation of loops. (The topology must be kept in mind)

- Priority
  If the path calculated by spanning tree is possible over several ports of a device, the port with the highest priority (in other words the lowest value for this parameter) is selected. A value between 0 and 240 can be entered for the priority in steps of 16. If you enter a value that cannot be divided by 16, the value is automatically adapted. The default is 128.
- Cost Calc
  Enter the path cost calculation in the input box. If you enter the value "0" here, the automatically calculated value is displayed in the "Path Cost" box.

- **Path Cost**
  This parameter is used to calculate the path that will be selected. The path with the lowest value is selected. If several ports of a device have the same value, the port with the lowest port number is selected.
  If the value in the path cost calculation box is "0", the automatically calculated value is displayed. Otherwise, the value of the path cost calculation box is displayed.
  The calculation of the path costs is largely based on the transmission speed. The higher the achievable transmission speed is, the lower the value of the path costs.

  Typical values for path costs with rapid spanning tree:

  – 10,000 Mbps = 2,000

  – 1000 Mbps = 20,000

  – 100 Mbps = 200,000

  – 10 Mbps = 2,000,000

  The values can, however, also be set individually.

- **Status**
  Displays the current status of the port. The values are only displayed and cannot be configured. The "Status" parameter depends on the configured protocol. The following statuses are possible:

  – Disabled
    The port only receives and is not involved in STP, MSTP and RSTP.

  – Discarding
    In the "Discarding" mode, BPDU frames are received. Other incoming or outgoing frames are discarded.

  – Listening
    In this status, BPDUs are both received and sent. The port is involved in the spanning tree algorithm.

  – Learning
    Stage prior to the forwarding status, the port is actively learning the topology (in other words, the node addresses).

  – Forward
    Following the reconfiguration time, the port is active in the network; it receives and forwards data frames.

- **Fwd. Trans**
  Specifies the number of changes from the "Discarding" status to the "Forward" status.

- **Edge Type**
  Select the type of connection from the drop-down list. You have the following options:
  - "-"
    Edge port is disabled.
  - Admin
    Select this option when there is an end device on this port. Otherwise a reconfiguration of the network will be triggered whenever a link to this port is modified.
  - Auto
    Select this option if you want a connected end device to be detected automatically at this port.
  - Admin/Auto
    Select these options if you operate a combination of both on this port.
- **P.t.P. Type**
  Select one of the following options from the drop-down list:
  - "-"
    Point to point is calculated automatically. If the port is set to half duplex, a point-to-point link is not assumed.
  - P.t.P.
    Even with half duplex, a point-to-point link is assumed.
  - Shared Media
    Even with a full duplex connection, a point-to-point link is not assumed.

  Note

  Point-to-point connection means a direct connection between two devices. A shared media connection is, for example, a connection to a hub.

With SCALANCE X devices, there is also the following option:

- **Hello Time** Here, you enter the Hello time for frames in seconds. As default, 2 seconds is set here. The range of values is 1 to 2 seconds.

Note

The port-specific setting of the Hello time is only possible in MSTP compatible mode.

Steps in configuration

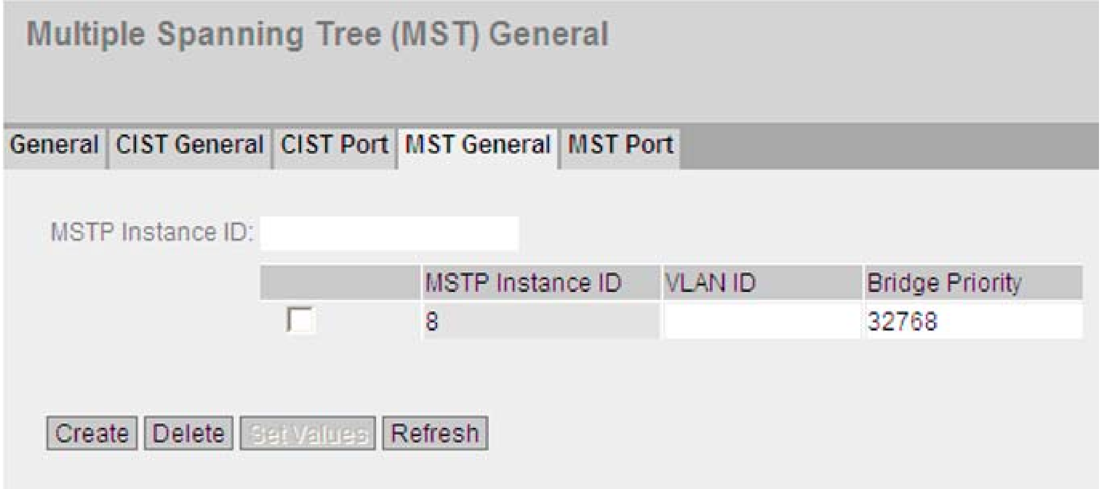
Follow the steps outlined below to configure a port for multiple spanning tree:

1. In the input cells of the table row, enter the values of the port you are configuring.
2. From the drop-down lists of the cells of the table row, select the values of the port you are configuring.
3. Click the "Set Values" button.

4.7.4 MST general

Multiple Spanning Tree configuration

With MSTP, in addition to RSTP, several VLANs can be managed in a LAN with separate RSTP trees.



MSTP Instance ID:

	MSTP Instance ID	VLAN ID	Bridge Priority
□	8		32768

Description of the boxes

The table has the following columns:

- Check box for deleting
  Select the entry by clicking this check box for the delete function.
- MSTP Instance ID
  Enter a value in the range 0 - 64 for the instance ID.
- VLAN ID
  Identifier of the VLAN. Here, you can also specify ranges with Start ID, "-", End ID. Several ranges or IDs are separated by ",". Permitted values are 1 to 4094.
- Bridge Priority
  Enter the bridge priority in this box.

Steps in configuration

Follow the steps below to configure the entries:

Changing the region configuration

1. In the "Region Name" box, enter the name of the MSTP region to which the device will belong.
2. In the "Region Version" box, enter the version number of the MSTP region to which the device will belong.
3. Enter the ID of the virtual LAN in the "VLAN ID" input box.

4. Enter the priority of the bridge in the "Bridge Priority" input box.
5. Click the "Set Values" button.

Creating a new entry

1. Enter the identifier for this MSTP instance in the "MSTP Instance ID" input box.
2. Click the "Create" button.
3. Enter the identifier of the virtual LAN in the "VLAN ID" input box.
4. Enter the priority of the bridge in the "Bridge Priority" input box.
5. Click the ""Set Values" button.

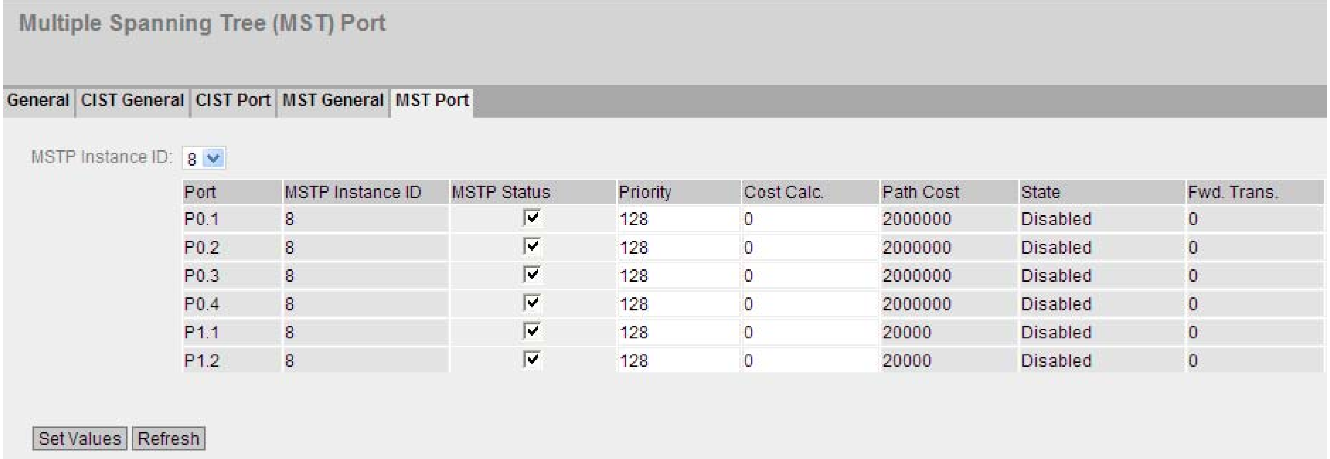
Deleting entries

1. Use the check box at the beginning of the relevant row to select the entries to be deleted.
2. Click the "Delete" button to delete the selected entries from memory. The entries are deleted from the memory of the device and the display on this page is updated.

4.7.5 MST port

Configuration of the Multiple Spanning Tree port parameters

On this page, you set the parameters for the ports of the configured multiple spanning tree instances.



MSTP Instance ID: 8

Port	MSTP Instance ID	MSTP Status	Priority	Cost Calc.	Path Cost	State	Fwd. Trans.
P0.1	8	☑	128	0	2000000	Disabled	0
P0.2	8	☑	128	0	2000000	Disabled	0
P0.3	8	☑	128	0	2000000	Disabled	0
P0.4	8	☑	128	0	2000000	Disabled	0
P1.1	8	☑	128	0	20000	Disabled	0
P1.2	8	☑	128	0	20000	Disabled	0

Description of the displayed boxes

The table has the following columns:

- Port
  This column lists all the ports available on the device with slot and port number. This field cannot be edited.
- MSTP Instance ID
  ID of the MSTP instance.
- MSTP Status
  Click the check box to enable or disable this option.
- Priority
  If the path calculated by spanning tree is possible over several ports of a device, the port with the highest priority (in other words the lowest value for this parameter) is selected. A value between 0 and 240 can be entered for the priority in steps of 16. If you enter a value that cannot be divided by 16, the value is automatically adapted. The default is 128.
- Cost Calc
  Enter the path cost calculation in the input box. If you enter the value "0" here, the automatically calculated value is displayed in the next box "Path Cost".
- Path Cost
  This parameter is used to calculate the path that will be selected. The path with the lowest value is always selected. If several ports of a device have the same value, the port with the lowest port number is selected.
  If the value in the path cost calculation box is "0", the automatically calculated value is displayed. Otherwise, the value of the path cost calculation box is displayed.
  The calculation of the path costs is largely based on the transmission speed. The higher the achievable transmission rate, the lower the value for the path costs will be.
  Typical values for rapid spanning tree are as follows:
  - 1000 Mbps = 20,000
  - 100 Mbps = 200,000
  - 10 Mbps = 2,000,000

  The values can, however, also be set individually.
- State
  Displays the current status of the port. The values are only displayed and cannot be configured. The following statuses are possible:
  - Deactivated
    The port only receives and is not involved in the MSTP configuration.
  - Blocked
    In the blocking mode, BPDU frames are received.
  - Forwarding
    Following the reconfiguration time, the port is active again in the network. It receives and sends data frames.

Steps in configuration

Follow the steps outlined below to configure a port for multiple spanning tree:

1. In the input cells of the table row, enter the values of the port you are configuring.
2. From the drop-down lists of the cells of the table row, select the values of the port you are configuring.
3. Click the "Set Values" button.

4.8 Link aggregation

4.8.1 Link aggregation

Bundling network connections for redundancy and higher bandwidth

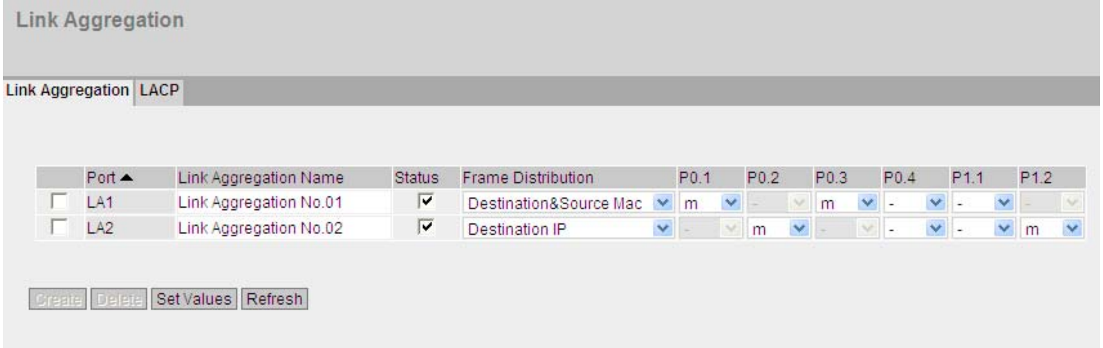
Link aggregations according to IEEE 802.3ad allow several connections between neighboring devices to be bundled to achieve higher bandwidths and protection against failure.

Ports on both partner devices are included in link aggregations and the devices are then connected via these ports. To assign ports (in other words links) correctly to a partner device, the Link Aggregation Control Protocol (LACP) from the IEEE 802.3ad standard is used.

Up to 8 link aggregations can be defined. Any number of ports can be assigned to each link aggregation. However a maximum of 8 ports will become active, the additional ports are standby ports and become active if an active port fails.

Display of the configured aggregation

The menu displays all the configured link aggregations.


Link Aggregation

	Port ▲	Link Aggregation Name	Status	Frame Distribution	P0.1	P0.2	P0.3	P0.4	P1.1	P1.2
□	LA1	Link Aggregation No.01	☑	Destination&Source Mac	m	-	m	-	-	-
□	LA2	Link Aggregation No.02	☑	Destination IP	-	m	-	-	-	m

Description of the displayed boxes

The table has the following columns:

- Port
  Shows the virtual port number of this link aggregation. This is assigned internally by the firmware.
- Link Aggregation Name
  Shows the name of the link aggregation. This name can be specified by the user during configuration. The name is not absolutely necessary but can be useful to distinguish between the various link aggregations.
- Status
  Enable this check box to activate link aggregation.
- Frame Distribution
  Set the type of distribution of packets on the individual links of an aggregation.
  - Source MAC
    The distribution is based on the source MAC address.
  - Destination MAC
    The distribution is based on the destination MAC address.
  - Destination&Source MAC
    The distribution is based on a combination of the destination and source MAC address.
  - Source IP
    The distribution is based on the source IP address
  - Destination IP
    The distribution is based on the destination IP address.
  - Destination&Source IP
    The distribution is based on a combination of the destination and source IP address.
- Port
  Shows the ports that belong to this link aggregation. The following values can be selected from the drop-down list:
  - "-" (disabled)
    Link aggregation is disabled.
  - m
    The port is a member of the link aggregation.

  Note

  Within a "link aggregation", only ports with the same configuration can be activated.

Steps in configuration

Basics prior to configuration

1. First, identify the ports you want to put together to form a link aggregation between the devices.

2. Configure the link aggregation on the devices.
3. Adopt the configuration for all devices.
4. Perform the last step, the cabling.

NOTICE
If you cable aggregated links prior to configuration, it is possible that you will create loops in the network! The network involved may deteriorate badly due to this or complete disruption may occur.

Creating a new link aggregation

1. Click the "Create" button to create a new link aggregation.

   This creates a new row.
2. Select the ports that will belong to this link aggregation.
3. Click the "Set Values" button.

Deleting an aggregation

1. Using the check box at the beginning of a row, select the link aggregation you want to delete.
2. Click the "Delete" button.

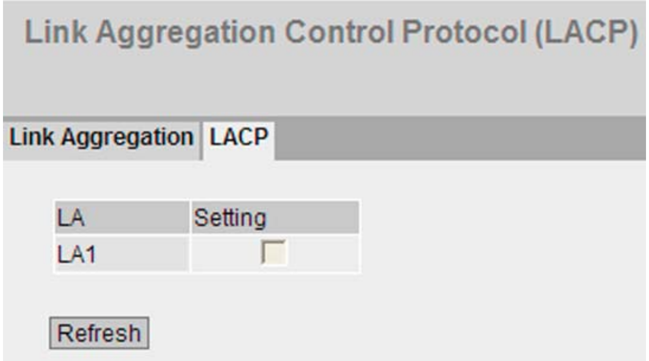
Changing an aggregation

1. In the overview, click on the relevant table entry to change the configuration of a created link aggregation.
2. Make all the changes.
3. Click the "Set Values" button.

4.8.2 LACP

Enabling LACP functionality

The Link Aggregation Control Protocol (LACP) adopts the selection of the active ports of a link aggregation. You can activate LACP for every aggregation.



Link Aggregation Control Protocol (LACP)

LA	Setting
LA1	□

Description of the displayed boxes

The table has the following columns:

- **LA (Link Aggregation)**
  This column in the table shows all the link aggregations configured on the device. It cannot be configured.
- **Setting**
  If the check box is enabled, LACP frames are sent. The hardware ports of inactive aggregations act as normal ports.

Steps in configuration

1. Click the check box of the relevant link aggregation to enable or disable the LACP function. When the LACP function is activated, a check mark appears in the box.
2. Click the "Set Values" button.

Note

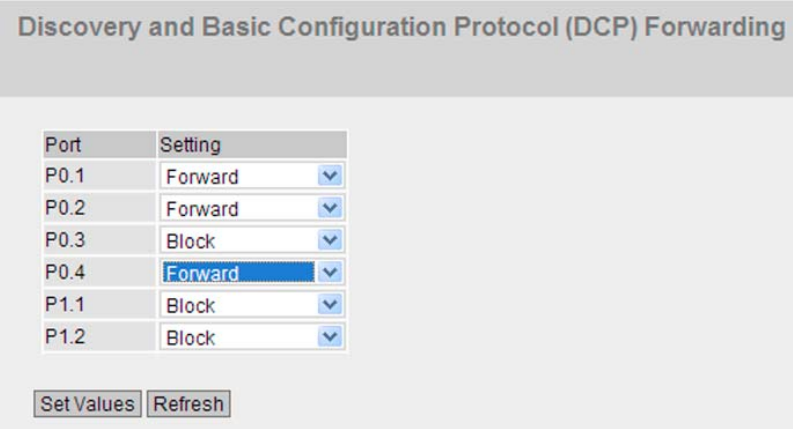
A connection to the attached system is only established when the LACP is enabled or disabled at both ends.

4.9 DCP forwarding

Applications

The DCP protocol is used by STEP 7 and the PST Tool for configuration and diagnostics. When shipped, DCP is enabled on all ports; in other words, DCP frames are forwarded at all ports. With this option, you can disable the sending of these frames for individual ports, for example to prevent individual parts of the network from being configured with the PST Tool or to divide the full network into smaller parts for configuration and diagnostics.

All the ports of the device are displayed on this page. After each displayed port, there is a drop-down list for function selection.



Discovery and Basic Configuration Protocol (DCP) Forwarding

Port	Setting
P0.1	Forward
P0.2	Forward
P0.3	Block
P0.4	Forward
P1.1	Block
P1.2	Block

Description of the displayed values

The table has the following columns:

- Port
  All available ports are listed in this column. Unavailable ports are not displayed.

X With SCALANCE X devices, the port is made up of the port number and slot number. , for example port 0.1 is slot 0, port 1.

W With SCALANCE W devices, the port number is displayed, for example, P1 is port number 1.

- Setting
  From the drop-down list, select whether the port should block or forward outgoing DCP frames. You have the following options available:
  - Forward
    DCP frames are forwarded via this port.
  - Block
    No outgoing DCP frames are forwarded via this port. It is nevertheless still possible to receive via this port.

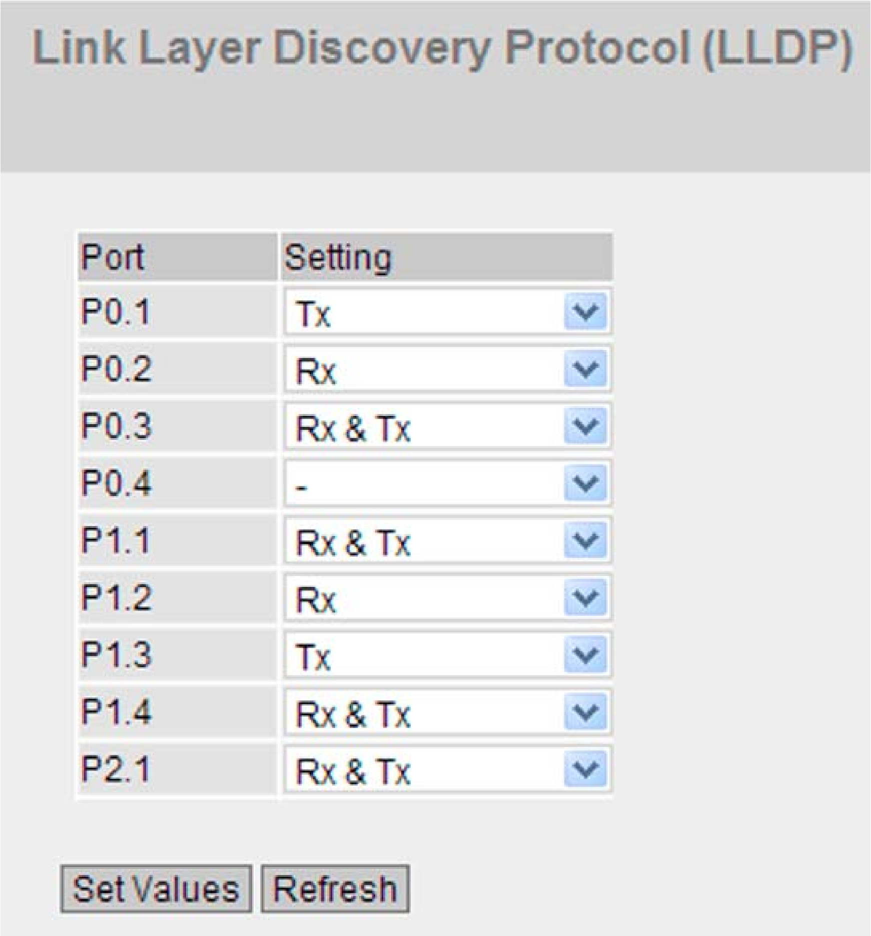
Steps in configuration

1. From the options in the drop-down list in the row, select which ports should support sending DCP frames.
2. Click the "Set Values" button.

4.10 LLDP

Applications

PROFINET uses the LLDP protocol for topology diagnostics. In the default setting, LLDP is enabled for all ports; in other words, LLDP frames are sent and received on all ports. With this function, you have the option of enabling or disabling sending and/or receiving per port.



Link Layer Discovery Protocol (LLDP)

Port	Setting
P0.1	Tx
P0.2	Rx
P0.3	Rx & Tx
P0.4	-
P1.1	Rx & Tx
P1.2	Rx
P1.3	Tx
P1.4	Rx & Tx
P2.1	Rx & Tx

Description of the displayed boxes

The table has the following columns:

- **Port**
  The slot and port names are displayed here.
- **Setting**
  From the drop-down list, select whether or not the port will send or receive LLDP frames. You have the following options available:
  - Rx
    This port can only receive LLDP frames.
  - Tx
    This port can only send LLDP frames.
  - Rx & Tx
    This port can receive and send LLDP frames.
  - "-" (disabled)
    This port can neither receive nor send LLDP frames. In this case, the device does not appear in the STEP 7 topology browser.

Steps in configuration

1. From the drop-down list in the row of the port you want to configure, select the LLDP functionality.
2. Click the "Set Values" button.

4.11 Unicast

Address filtering

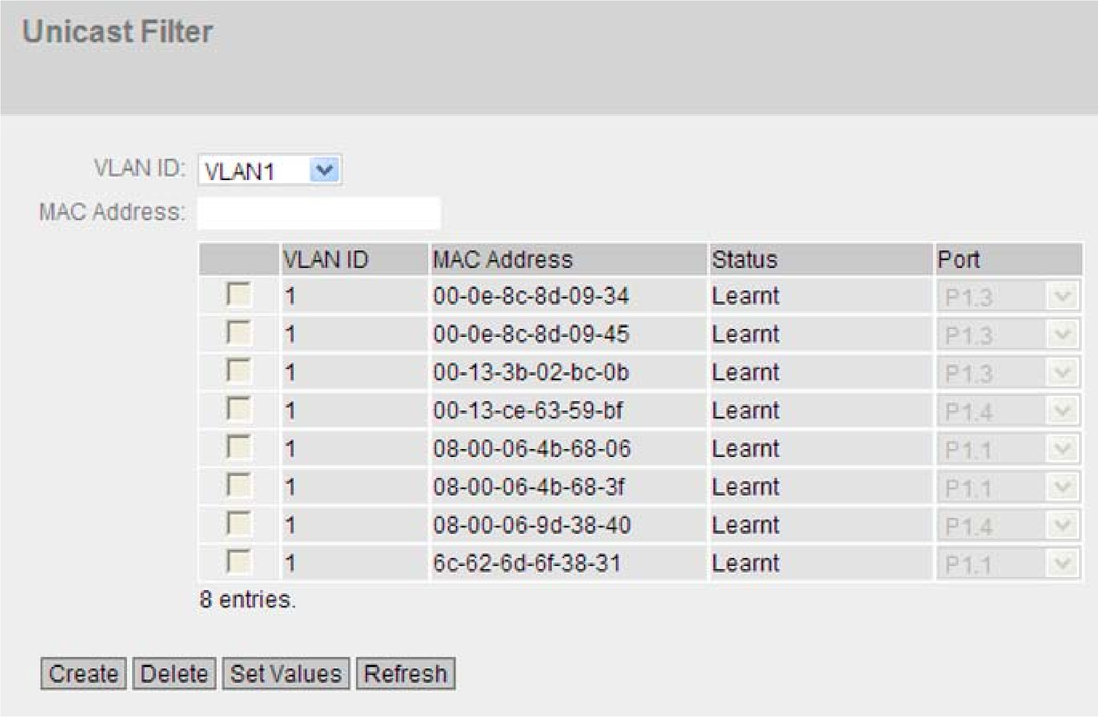
This menu displays the current content of the filter table. This table lists the source addresses of unicast address frames. Entries can be made either dynamically when a node sends a frame to a port or statically by the user setting parameters.

Port Lock with SCALANCE X devices

Unicast filters can be used for access control. Using the Port Lock function (see "Security > Locked Ports > Ports"), individual ports can be blocked for unknown nodes. If the Port Lock function is enabled on a port, packets arriving at this port from unknown MAC addresses are discarded immediately.

Since ports with Port Lock function cannot learn any MAC addresses, learned addresses on these ports are automatically deleted after the Port Lock function is enabled. To include a device in the list of known nodes, a unicast entry must be created (on the relevant port) for its MAC address.

To enter all connected nodes automatically, there is a function for automatic learning (see "Security > Locked Ports > Learning").



Unicast Filter

VLAN ID: VLAN1

MAC Address:

	VLAN ID	MAC Address	Status	Port
□	1	00-0e-8c-8d-09-34	Learnt	P1.3
□	1	00-0e-8c-8d-09-45	Learnt	P1.3
□	1	00-13-3b-02-bc-0b	Learnt	P1.3
□	1	00-13-ce-63-59-bf	Learnt	P1.4
□	1	08-00-06-4b-68-06	Learnt	P1.1
□	1	08-00-06-4b-68-3f	Learnt	P1.1
□	1	08-00-06-9d-38-40	Learnt	P1.4
□	1	6c-62-6d-6f-38-31	Learnt	P1.1

8 entries.

Description of the displayed boxes

With SCALANCE X devices, there are also the following boxes:

- Drop-down list "VLAN ID"
  Select the VLAN ID in which you want to configure a new static MAC address. If nothing is set, "VLAN1" is set as the basic setting.
- Input box "MAC Address"
  Enter the MAC address you want to configure statically.
- Check box
  Here, select the rows of the table you want to delete.

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

- **Status**
  Shows the status of each address entry:
  - Learnt
    The specified address was learned by receiving a frame from this node and will be deleted when the aging time expires if no further packets are received from this node.
  - Static
    Configured by the user. Static addresses are stored permanently; in other words, they are not deleted when the aging time expires or when the switch is restarted.
  - Invalid
    These values are not evaluated.
- **"Port"**
  Specifies the port over which the node with the specified address can be reached. Frames received by the device whose destination address matches this address will be forwarded to this port.

X With SCALANCE X devices, the port is made up of the port number and slot number. , for example port 0.1 is slot 0, port 1.

W With SCALANCE W devices, the port number is displayed, for example, P1 is port number 1.

Note

You can only specify **one** port for unicast addresses.

Configuration procedure for SCALANCE X devices

To edit the entries, follow the steps below. Note that automatically learned entries (status = "Learnt") cannot be modified.

Creating a new entry

1. Select the relevant VLAN ID.
2. Enter the MAC address in the "MAC Address" input box.
3. Click the "Create" button to create a new entry in the table.
4. Select the relevant port.
5. Click the "Set Values" button.

Changing the entry

1. Select the relevant port.
2. Click the "Set Values" button.

Deleting an entry

1. In the first column, click the check box in front of the entry you want to delete.
   Repeat this for all entries you want to delete.
2. Click the "Delete" button to delete the selected entries from the filter table.

4.12 Multicast

4.12.1 Groups

Multicast applications

In the majority of cases, a frame is sent with a unicast address to a particular recipient. If an application sends the same data to several recipients, the amount of data can be reduced by sending the data using one multicast address. For some applications, there are fixed multicast addresses (NTP, IETF1 Audio, IETF1 Video etc.).

Reducing network load

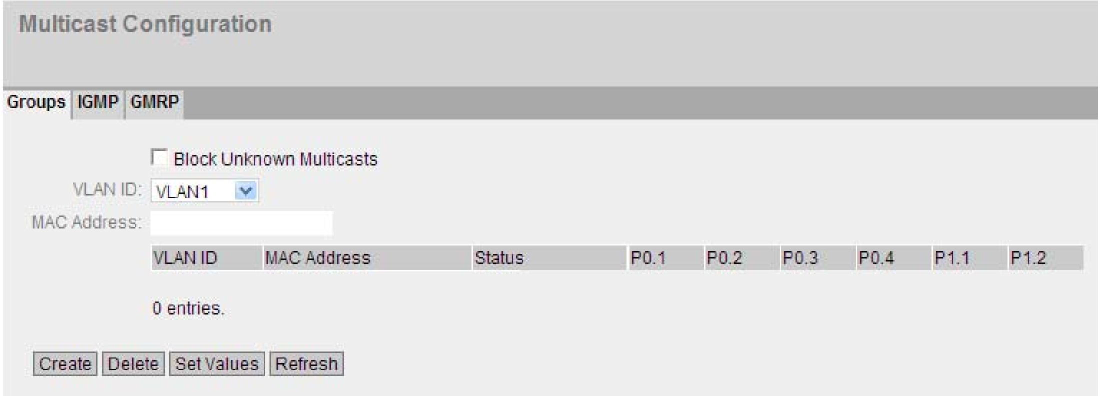
In contrast to unicast frames, multicast frames represent a higher load for the device. Generally, multicast frames are sent to all ports. There are three ways of reducing the load caused by multicast frames:

- Static entry of the addresses in the multicast filter table.
- Dynamic entry of the addresses by listening in on IGMP parameter assignment frames (IGMP Configuration).
- Active dynamic assignment of addresses by GMRP frames.

The result of all these methods is that multicast frames are sent only to ports for which an appropriate address is entered.

The "Multicast" menu item, shows the multicast frames currently entered in the filter table and their destination ports. The entries can be dynamic (the device has learned them) or static (the user has set them).

Configuring multicast addresses



□ Block Unknown Multicasts

VLAN ID: VLAN1

MAC Address:

VLAN ID	MAC Address	Status	P0.1	P0.2	P0.3	P0.4	P1.1	P1.2

0 entries.

Description of the displayed boxes

The page contains the following boxes:

- Check box "Block Unknown Multicasts"
  If this check box is enabled, the IE switch does not forward any multicast packets to an unknown destination address. To be forwarded, the multicast addresses must be make known.
- Drop-down list "VLAN ID"
  If you click on this text box, a drop-down list is displayed. Here you can select the VLAN ID of a new MAC address you want to configure.
- Text box "MAC Address""
  Here you enter a new MAC multicast address you want to configure.

The table has the following columns:

- Check box
  Select the table rows to be deleted.
- VLAN ID
  Here, the VLAN ID of the VLAN is displayed to which the MAC multicast address of this row is assigned.
- MAC Address
  Here, the multicast address is displayed that the device has learned or the user has configured.

- **Status**
  Shows the status of each address entry. The following information is possible:
  - Static
    The address was entered statically by the user. Static addresses are stored permanently; in other words, they are not deleted when the aging time expires or when the device is restarted. These must be deleted by the user.
  - IGMP
    The destination port for this address was obtained by IGMP configuration.
  - GMRP
    The destination port for this address was registered by a received GMRP frame.
- **Port List**
  There is a column for each slot. Within a column, the multicast group to which the port belongs is shown. The drop-down list provides the following options:
  - M
    (Member) Multicast frames are sent via this port.
  - R
  - (Registered) Member of the multicast group, registration was by a GMRP frame.
  - I
    (IGMP) Member of the multicast group, registration was by an IGMP frame.
  - –
    Not a member of the multicast group. No multicast frames with the defined multicast MAC address are sent via this port.
  - F
    (Forbidden) Not a member of the multicast group. This address must also not be an address learned dynamically with GMRP or IGMP.

Steps in configuration

Creating a new entry

Follow the steps below to create a new entry:

1. Specify the required ID in the "VLAN ID" text box.
2. Fill in the "MAC Address" input box.
3. Click the "MAC Address" button.
4. Assign the relevant ports to the multicast MAC address.
5. Click the "Set Values" button.

Deleting an entry

You can only delete entries with the "Static" status. Follow the steps below to delete an entry:

1. Select the check box in the first table column in front of the entry you want to delete.
2. Click the "Delete" button.
   The row is deleted from the display and from the memory of the device.

Note

If you have not made any changes on this page, the "Set Values" button remains inactive.

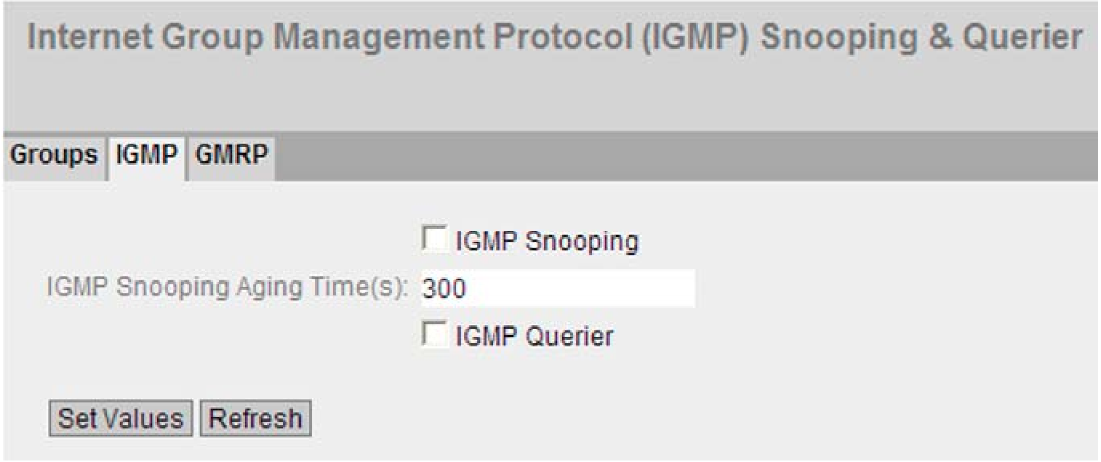
4.12.2 IGMP

Specifying the IGMP snooping aging time

In this menu, you can configure the aging time for IGMP Configuration. When the time elapses, entries created by IGMP are deleted from the address table if they are not updated by a new IGMP frame.

This applies to all ports; a port-specific configuration is not possible.

IE switches support not only "IGMP snooping" but also the IGMP querier function. If "IGMP snooping" is enabled, IGMP frames are evaluated and the multicast filter table is updated with this information. If IGMP Query is also enabled, IE switches also send IGMP queries that trigger responses from IGMP-compliant nodes.



Internet Group Management Protocol (IGMP) Snooping & Querier

☐ IGMP Snooping

IGMP Snooping Aging Time(s): 300

☐ IGMP Querier

Description of the displayed boxes

The page contains the following boxes:

- Check box "IGMP Snooping"
  IGMP (Internet Group Management Protocol) allows the assignment of IP addresses to multicast groups. If the option is enabled, IGMP entries are included in the table

  and IGMP frames are forwarded.
- Input box "IGMP Snooping Aging Time"
  In this box, enter the value for the aging time in seconds.
- Check box "IGMP Querier"
  Here, you can enable/disable the "IGMP Querier" option.

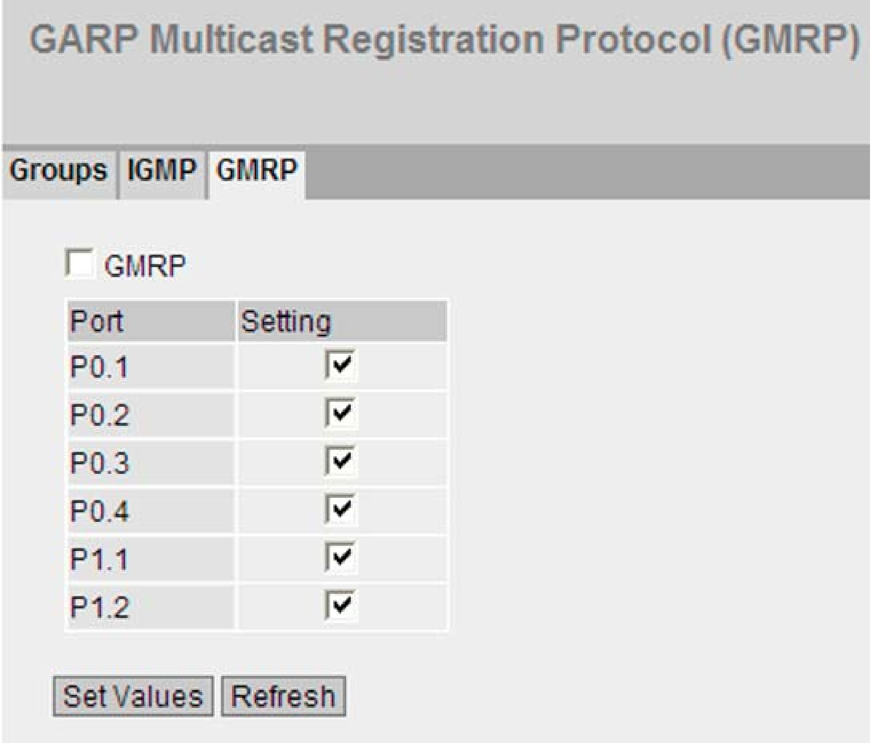
Steps in configuration

1. Enable the "IGMP Snooping" check box if you want to use this function.
2. Enter the value for the aging time in seconds in the "IGMP Snooping Aging Time" box. As default, 300 seconds is set here. You can set values between 130 and 1225 seconds.
3. Select the "IGMP Querier" check box if you also want the device to send IGMP queries.
4. Click the "Set Values" button.

4.12.3 GMRP

Activating GMRP

By selecting the check box, you specify whether or not GMRP is used for each individual port. If "GMRP" is disabled for a port, no registrations are made for it and it cannot send GMRP frames.



GARP Multicast Registration Protocol (GMRP)

□ GMRP

Port	Setting
P0.1	☑
P0.2	☑
P0.3	☑
P0.4	☑
P1.1	☑
P1.2	☑

Description of the displayed boxes

The page contains the following boxes:

- Check box "GMRP"
  With this check box, you enable or disable the function globally.
- Column "Port"
  This column lists all the ports available on the device including link aggregations.
- Column "Setting"
  With this check box, you enable or disable GMRP for each individual port or link aggregation.

Steps in configuration

1. To enable/disable the GMRP function for the required ports:

- – Click of the empty check box following the port for which you want to enable the function.
  Repeat this procedure for every port on which you want to enable the function.

  or

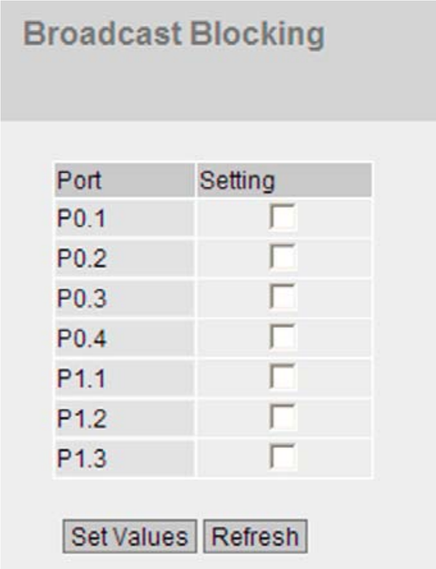
  – Click on the check mark in the check box if you want to disable the function.
  Repeat this for each port for which you want to disable the function.

2. After you have enabled or disabled the function for all required ports, click the "Set Values" button.

4.13 Broadcast

Blocking the forwarding of broadcast frames

On this page, you can block the forwarding of broadcast frames for individual ports.



Broadcast Blocking

Port	Setting
P0.1	□
P0.2	□
P0.3	□
P0.4	□
P1.1	□
P1.2	□
P1.3	□

Description of the displayed boxes

The table has the following columns:

- Column "Port"
  This column lists all the ports available on the device including link aggregations.
- Column "Setting"
  With this check box, you enable or disable the "Broadcast Blocking" function for each individual port or link aggregation.

Steps in configuration

1. To enable/disable the broadcast blocking function for the required ports:

- Click of the empty check box following the port whose function you want to enable. Repeat this procedure for every port on which you want to enable the function.

or

- Click on the check mark in the check box if you want to disable the function. Repeat this for each port whose function you want to disable.

2. After you have enabled or disabled the function for all required ports, click the "Set Values" button.

Note

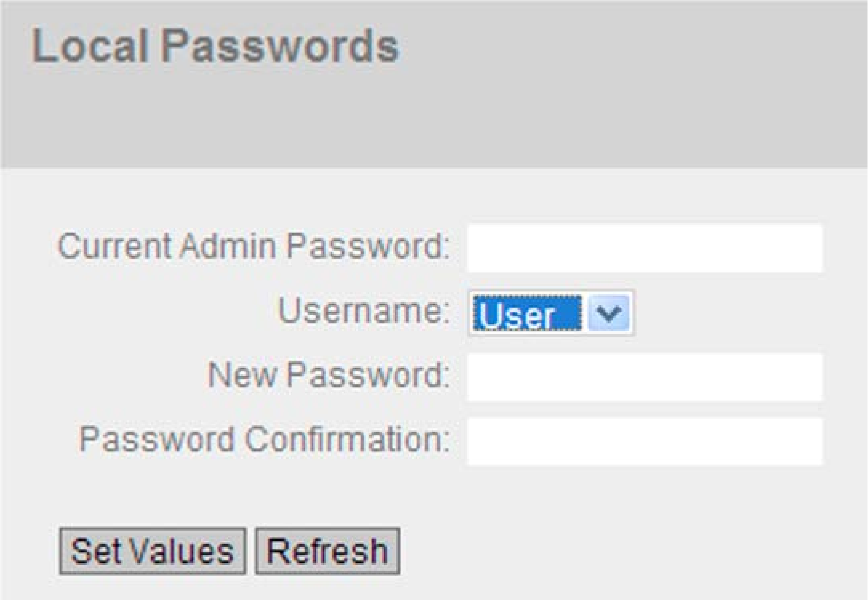
Some communication protocols work only with the support of broadcast. In these cases, blocking can lead to loss of data communication. Block broadcast only when you are sure that you do not need it.

The "Security" menu 5

5.1 Passwords

Configuration of the device passwords

Changes to the device passwords for administrator and users can only be made locally by the administrator.



Local Passwords

Current Admin Password:

Username: User

New Password:

Password Confirmation:

Steps in configuration

To change the passwords, follow the steps below:

1. From the "Username" drop-down list, select the user whose password you want to change.
   Select between "admin" and "user".
2. Enter the valid administrator password in the "Current Admin Password" input box.
3. Enter the new password for the selected user in the "New Password" input box. The new password must be at least 6 characters long.

   The following characters are not currently supported: "<", ">" and space if it comes at the start or end.

4. Repeat the new password in the "Password Confirmation" input box.
5. Click the "Set Values" button.

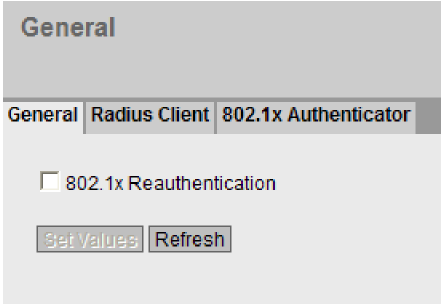
Note

The factory settings for the passwords when the devices ship are as follows:

- Administrator: admin
- User: user

5.2 AAA

5.2.1 General



Description of the displayed boxes

The page contains the following box:

- **Check box "802.1x Reauthentication"**
  If you select this check box, an authenticated 802.1X supplicant is forced to reauthenticate cyclically. As default, one hour (3,600 s) is set.

Steps in configuration

1. Select the "802.1x Reauthentication" check box if you want to enable the forced reauthentication.
2. Click the "Set Values" button.

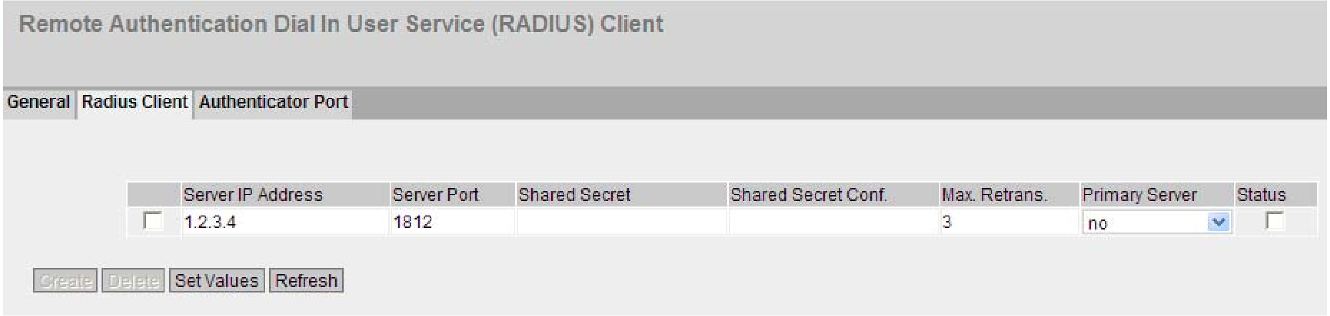
5.2.2 RADIUS client

Authentication over an external server

The concept of RADIUS is based on an external authentication server. An end device can only access the network after the device has verified the logon data of the device with the authentication server. Both the end device and the authentication server must support the EAP protocol (Extensive Authentication Protocol).

Each column of the table contains access data for one server. In the search order, the primary server is queried first. If the primary server cannot be reached, secondary servers are queried in the order in which they are entered.

If no server responds, there is no authentication. The client has no access to the network although a link is indicated at the port.


Remote Authentication Dial In User Service (RADIUS) Client

	Server IP Address	Server Port	Shared Secret	Shared Secret Conf.	Max. Retrans.	Primary Server	Status
□	1.2.3.4	1812			3	no	□

Description of the displayed boxes

The table has the following columns:

- Check box of the relevant row
  Click this check box to select the entry in this row for the delete function.
- Input box "Server IP Address"
  Enter the IP address of the server.
- Input box "Server Port"
  Here, enter the input port on the RADIUS server. As default, input port 1812 is set. The range of values is 1 to 65535.
- Input box "Shared Secret"
  Enter your access ID here.
- Input box "Shared Secret Conf."
  Enter your access ID again as confirmation.
- Input box "Max. Retrans."

  Here, enter the maximum number of query attempts before another configured RADIUS server is queried or the logon counts as having failed. As default, 3 is set. The range of values is 1 to 254.

- **Drop-down list "Primary Server"**
  Using the options in the drop-down list, specify whether or not this server is the primary server. You can select one of the options "yes" or "no".
- **Check box "Status"**
  With this check box, you can enable or disable the RADIUS server.

Note

You can configure a maximum of two servers on this page.

Steps in configuration

Entering a new server

For each new server, make the entries as follows:

1. Click the "Create" button to create a new empty data record. The following default values are entered in the table:
   - Server IP address: 0.0.0.0
   - Port number: 1812
   - Maximum number of transmission retries: 3
   - Primary server: No
2. In the relevant row, enter the following data in the input boxes:
   - Server IP address
   - Port number of the destination
   - Secret access ID
   - Repetition of the secret access ID
   - Maximum number of transmission retries
   - Primary server
3. Click the "Set Values" button.

Repeat this procedure for every server you want to enter.

Modifying servers

1. In the relevant row, enter the following data in the input boxes:
   - IP address
   - Port number of the destination
   - Secret access ID
   - Repetition of the secret access ID
   - Maximum number of transmission retries
   - Primary server
2. Click the "Set Values" button.

Repeat this procedure for every server whose entry you want to modify

Deleting servers

Follow the steps below to delete a server from the table:

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

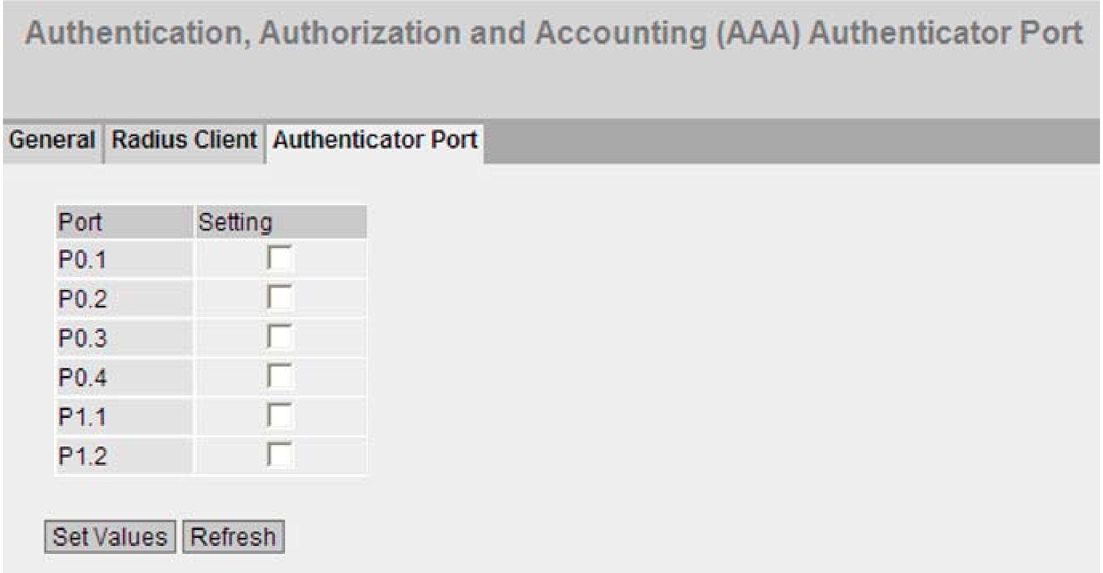
Note

If you click the "Refresh" button before you have transferred your configuration changes with the "Set Values" or "Delete" button, your changes will be canceled and the previous configuration is loaded from the memory of the device and displayed.

5.2.3 Authenticator port

Enabling authentication for individual ports

By selecting the check box, you specify whether or not network access protection according to IEEE 802.1x is enabled on this port.



Authentication, Authorization and Accounting (AAA) Authenticator Port

Port	Setting
P0.1	□
P0.2	□
P0.3	□
P0.4	□
P1.1	□
P1.2	□

Description of the displayed boxes

The table has the following columns:

- Port
  This column lists all the ports available on this device.
- Check box "Setting"
  In this column, select the check boxes for the authentication enabled for this port. An empty check box means that the authentication is not enabled for the port in question. If this configuration is not possible for a port, it is displayed grayed out and you cannot modify the settings.

Steps in configuration

To enable or disable the authentication for the individual ports, follow the steps below:

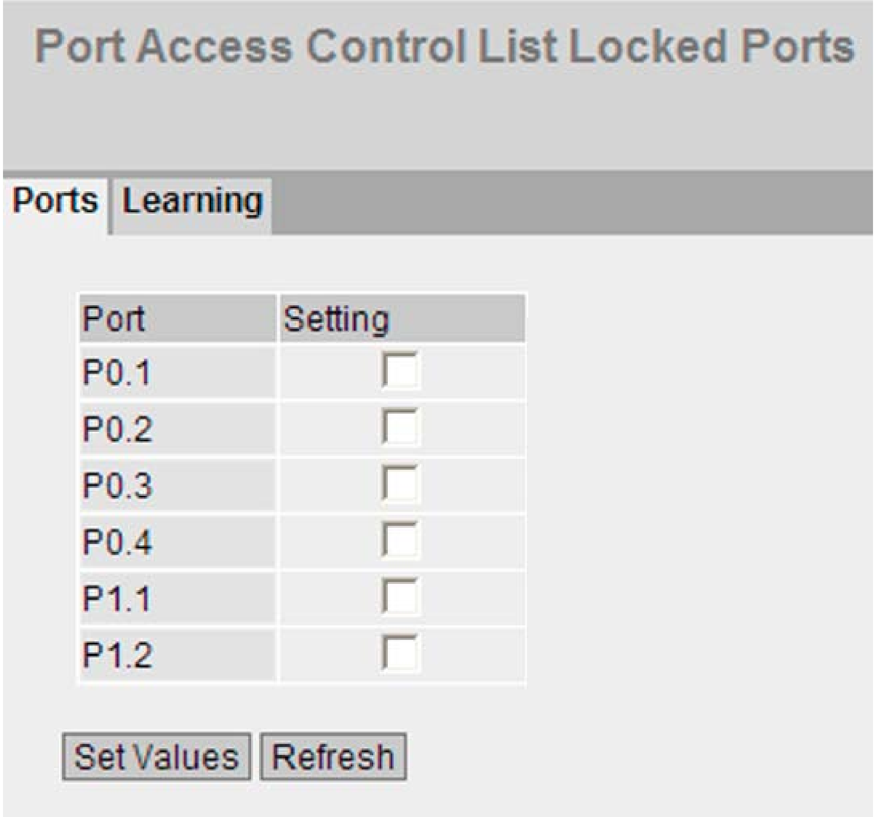
1. Click the empty check box in the row following the port information if you want to enable the authentication function of the port. Repeat this for all ports for which you want to enable the function.
   Or
   Click the selected check box if you want to disable this function for the port. Repeat this until you have disabled the function for the required ports.
2. When you have enabled or disabled all ports, click the "Set Values" button.

5.3 Locked ports

5.3.1 Ports

Activating the access control

By enabling the options, you specify whether or not the Port Lock function is enabled for the individual ports. If the function is enabled for a port, packets at this port from unknown MAC addresses are discarded immediately. Only packets from known nodes are accepted. The port does not learn any more MAC addresses. The port accepts only static MAC addresses that were created previously either manually or with the "Start Learning" function and the "Stop Learning" function.



Port Access Control List Locked Ports

Port	Setting
P0.1	□
P0.2	□
P0.3	□
P0.4	□
P1.1	□
P1.2	□

Description of the displayed boxes

The table has the following columns:

- Port
  This column lists all the ports available on this device.
- Check box "Setting"
  In this column, you select the various check boxes that have a check mark.

Steps in configuration

To enable or disable the access control for the individual ports, follow the steps below:

1. Click the check box in the row following the port information if you want to enable the access control function of the port. Repeat this for all ports for which you want to enable the function.
   Or
   Click the selected check box if you want to disable this function for the port. Repeat this procedure for all ports for which you want to disable the function.
2. When you have made all the changes, click the "Set Values" button.

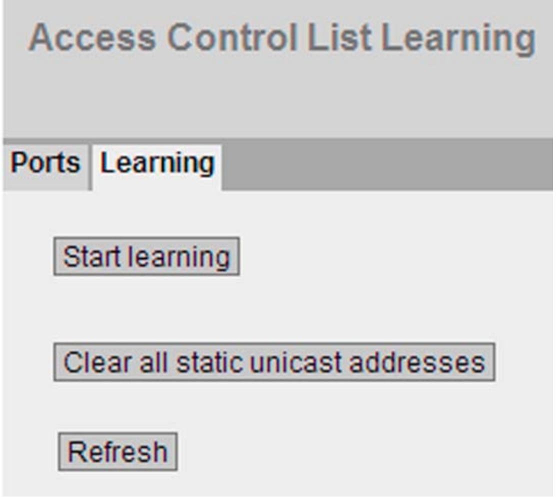
5.3.2 Learning

Starting/stopping learning

With the automatic learning function, all connected devices are automatically entered in the unicast filter table. As long as the "Start learning" function is enabled, all learned unicast addresses are created immediately as static unicast entries.
The learning process is ended only after clicking the "Stop learning" button. With this method, learning can take a few minutes or several hours in larger networks before all nodes have really been learned. Only nodes that send packets during the learning phase are found. By subsequently enabling the Port Lock function, only packets from the nodes known after the end of the learning phase (static unicast entries) will be accepted at the relevant ports.

Note

If the Port Lock function was already active on individual ports prior to the automatic learning phase, no addresses will be learned on these ports. This makes it possible to restrict learning to certain ports. To do this, first enable the Port Lock function of the ports that are not intended to learn addresses.


Access Control List Learning
Ports
Learning
Start learning
Clear all static unicast addresses
Refresh

Steps in configuration

Learning addresses

1. Click the "Start learning" button to start the learning phase.
   After starting the learning phase, the "Start learning" button is replaced by the "Stop learning" button.
   The device now enters the addresses of connected devices until you stop the function.
2. Click the "Stop learning" button to stop the learning function.
   The button is once again replaced by the "Start Learning" button. The learned entries are stored.

Deleting all static unicast addresses

1. Click the "Clear all static unicast addresses" button to delete all static entries.
   In large networks with numerous nodes, automatic learning may lead to a lot of undesired static entries. To avoid having to delete these individually, this button can be used to delete all static entries. This function is disabled during automatic learning.

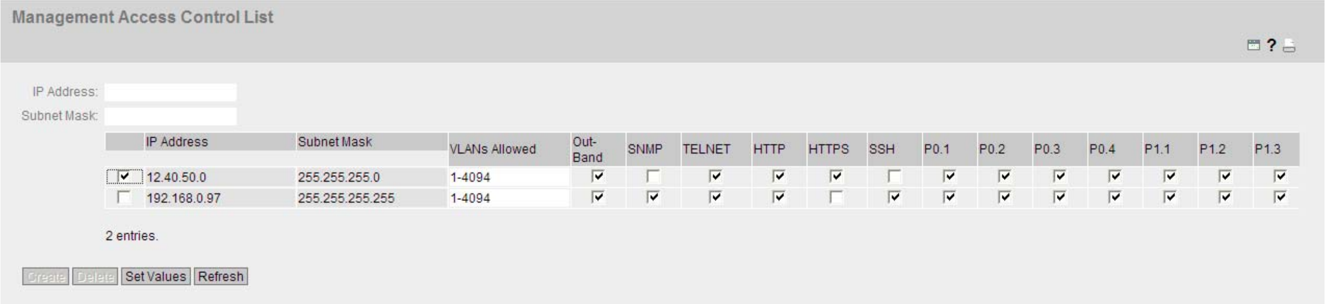
> **Note**
>
> Depending on the number of entries involved, deleting may take some time.

5.4 Management ACL

Description of configuration

On this page, you can increase the security of your device. To specify which station with which IP address is allowed to access your device, configure the IP address or an entire address range.

You can select the protocols and the ports of the station with which it is allowed to access the device. You define the VLAN in which the station may be located. This ensures that only certain stations within a VLAN have access to the switch.



Management Access Control List

IP Address:

Subnet Mask:

	IP Address	Subnet Mask	VLANs Allowed	Out-Band	SNMP	TELNET	HTTP	HTTPS	SSH	P0.1	P0.2	P0.3	P0.4	P1.1	P1.2	P1.3
☑	12.40.50.0	255.255.255.0	1-4094	☑	□	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑
□	192.168.0.97	255.255.255.255	1-4094	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	☑

2 entries.

Description of the displayed boxes

The page contains the following input boxes:

- IP Address
  In this input box, you enter the IP address or the network address to which the rule will apply. If you use the IP address 0.0.0.0, the settings apply to all IP addresses.
- Subnet Mask
  Enter the subnet mask here. The subnet mask 255,255,255,255 is for a specific IP address. If you want to allow a subnet, for example a C subnet, enter 255.255.255.0. The subnet mask 0.0.0.0 applies to all subnets.

The table has the following columns:

- Check box for deleting
  Click this check box if you want to select the entry for deletion.
- Display box "IP Address"
  Here, the IP address you entered earlier is entered automatically.
- Display box "Subnet Mask"
  Here, the subnet mask you entered earlier is entered automatically.
- Input box "VLANs Allowed"
  Here, enter the number of the VLAN in which the device will be located. This gives you the certainty that that the station can only access the device if it is located in this configured VLAN. If this input box remains empty, there is no restriction relating to the VLANs.

Description of the check boxes

X With SCALANCE X devices, there is also the following check box:

- Out-Band
  Click this check box so that the IP address can access the switch via the out-band port.

W With SCALANCE W devices, there is also the following check box:

- WLAN 1(client mode)
- VAP X.Y (access point mode)
- WDS X.Y (access point mode)

- SNMP
  Click this check box so that the station (or IP address) is allowed to access the device using the SNMP protocol.
- TELNET
  Click this check box so that the station (or IP address) is allowed to access the device using the TELNET protocol.
- HTTP
  Click this check box so that the station (or IP address) is allowed to access the device using the HTTP protocol.
- HTTPS
  Click this check box so that the station (or IP address) is allowed to access the switch using the HTTPS protocol.

- SSH
  Click this check box so that the station (or IP address) is allowed to access the switch using the SSH protocol.
- Px.x
  Click this check box so that the station (or IP address) is allowed to access the switch via this port. All available ports are displayed.

X With SCALANCE X devices, the port is made up of the port number and the slot number, for example P 0.1 is slot 0, port 1.

W With SCALANCE W devices, the port number is displayed, for example, P1 is port number 1.

Steps in configuration

Changing the entry

1. Configure the data of the entry you want to modify.
2. Click the "Set Values" button to transfer the changes to the device.

Creating new entry

1. In the "IP Address" input box, enter the IP address of the device and in the "Subnet Mask" input box the corresponding subnet mask.
2. Click the "Create" button to create a new row in the table.
3. Configure the entries of the new row.
4. Click the "Set Values" button to transfer the new entry to the device.

Deleting entries

1. Select the check box in front of the entry you want to select for deletion.
2. Repeat this procedure for every entry you want to delete.
3. Click the "Delete" button to remove the selected entries.
   The entries are deleted and the page is refreshed.

Note

Note that a bad configuration may mean that you can no longer access the device.

Index