SIEMENS

SIMATIC NET

Industrial Wireless LAN SCALANCE W780/W740 to IEEE 802.11n Web Based Management

Configuration Manual

11/2014

C79000-G8976-C267-07

Legal information

Warning notice system

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

⚠ DANGER

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

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

⚠ WARNING

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

Trademarks

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

Disclaimer of Liability

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

Siemens AG
Division Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000-G8976-C267-07
Ⓟ 12/2014 Subject to change

Table of contents

Introduction 1

1.1 Information on the Configuration Manual

Validity of the configuration manual

This Configuration Manual covers the following products:

- SCALANCE W748-1 M12
- SCALANCE W748-1 RJ-45
- SCALANCE W788-1 M12
- SCALANCE W788-2 M12
- SCALANCE W788-2 M12 EEC
- SCALANCE W788-1 RJ-45
- SCALANCE W788-2 RJ-45
- SCALANCE W786-1 RJ-45
- SCALANCE W786-2 RJ-45
- SCALANCE W786-2IA RJ-45
- SCALANCE W786-2 SFP

This Configuration Manual applies to the following software version:

- SCALANCE W700 firmware as of Version V 5.00

Note

This configuration manual does not apply to the SCALANCE W7xC-2.

Purpose of the Configuration Manual

This Configuration Manual is intended to provide you with the information you require to install, commission and operate devices correctly. It explains how to configure the devices and how to integrate them in a WLAN network.

How you install and connect up the device correctly is described in the operating instructions of the device.

Orientation in the documentation

Apart from the Configuration Manual you are currently reading, the following documentation is also available from SIMATIC NET on the topic of Industrial Wireless LANs:

- Configuration Manual: SCALANCE W780/W740 Command Line Interface

  This document contains the CLI commands that are supported by SCALANCE W700 devices.

- Performance data 802.11abgn PCIe Minicard MPCIE-R1-ABGN-U3

  This document contains information about the frequency, modulation, transmit power and receiver sensitivity of the wireless card.

- SCALANCE W788-x / W748-1 Operating Instructions

  This document contains information on installing and connecting up the following products and their approvals:

  - SCALANCE W788-1 RJ-45
  - SCALANCE W788-1 M12
  - SCALANCE W788-2 RJ-45
  - SCALANCE W788-2 M12
  - SCALANCE W788-2 M12 EEC
  - SCALANCE W748-1 RJ-45
  - SCALANCE W748-1 M12

- SCALANCE W786 Operating Instructions

  This document contains information on installing and connecting up the following products and their approvals:

  - SCALANCE W786-1 RJ-45
  - SCALANCE W786-2 RJ-45
  - SCALANCE W786-2IA RJ-45
  - SCALANCE W786-2 SFP

- System Manual Structure of an Industrial Wireless LAN

  Apart from the description of the physical basics and a presentation of the main IEEE standards, this also contains information on data security and a description of the industrial applications of wireless LAN.
  You should read this manual if you want to set up WLAN networks with a more complex structure (not simply a connection between two devices).

- System manual RCoax

  This system manual contains both an explanation of the fundamental technical aspects as well as a description of the individual RCoax components and their functionality. Installation/commissioning and connection of RCoax components and their operating principle are explained. The possible applications of the various SIMATIC NET components are described.

- System manual - Passive Network Components IWLAN

  This system manual explains the entire IWLAN cabling that you require for your IWLAN application. For a flexible combination and installation of the individual IWLAN components both indoors and outdoors, a wide ranging selection of compatible coaxial accessories are available. The system manual also covers connecting cables as well as a variety of plug-in connectors, lightning protectors, a power splitter and an attenuator.

SIMATIC NET manuals

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

- Using the search function:

  support.automation.siemens.com (http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo2&aktprim=99&lang=en)

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

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

  Industrial communication (http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&lang=de&siteid=csius&aktprim=0&extranet=standard&viewreg=WW&objid=10805878&treeLang=en)

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

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

- Product CD / product DVD
- SIMATIC NET Manual Collection
- SIMATIC NET IWLAN CD

Further documentation

The "SIMATIC NET Industrial Ethernet Network Manual" contains information on other SIMATIC NET products that you can operate along with the devices of this product line in an Industrial Ethernet network. There, you will find among other things optical performance data of the communication partners that you require for the installation.

The "SIMATIC NET Industrial Ethernet Network Manual" can be found on the Internet pages of Siemens Industry Online Support under the following entry ID:
27069465 (http://support.automation.siemens.com/WW/view/en/27069465)

SIMATIC NET manuals

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

- Using the search function:

  support.automation.siemens.com (http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo2&aktprim=99&lang=en)

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

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

  Industrial communication (http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&lang=de&siteid=csius&aktprim=0&extranet=standard&viewreg=WW&objid=10805878&treeLang=en)

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

Further documentation

The "SIMATIC NET Industrial Ethernet Network Manual" contains information on other SIMATIC NET products that you can operate along with the devices of this product line in an Industrial Ethernet network. There, you will find among other things optical performance data of the communications partners that you require for the installation.

The "SIMATIC NET Industrial Ethernet Network Manual" can be found on the Internet pages of Siemens Industry Online Support under the following entry ID:
27069465 (http://support.automation.siemens.com/WW/view/en/27069465)

Security messages

Note

Siemens offers IT security mechanisms for its automation and drive product portfolio in order to support the safe operation of the plant/machine. Our products are also continuously developed further with regard to IT security. We therefore recommend that you regularly check for updates of our products and that you only use the latest versions. You will find information in:

(http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo2&aktprim=99&lang=en)

Here, you can register for a product-specific newsletter.

For the safe operation of a plant/machine, however, it is also necessary to integrate the automation components into an overall IT security concept for the entire plant/machine, which corresponds to the state-of-the-art IT technology. You will find information on this in: (http://www.siemens.com/industrialsecurity)

Products from other manufacturers that are being used must also be taken into account.

1.2 Type designations

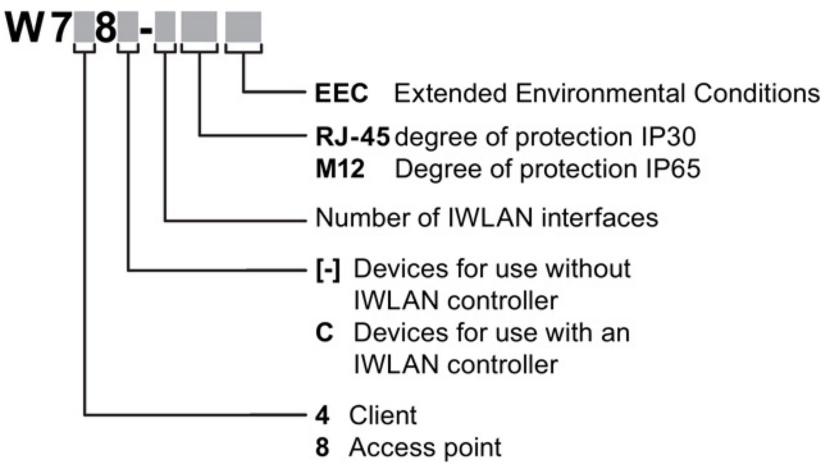
Abbreviations used

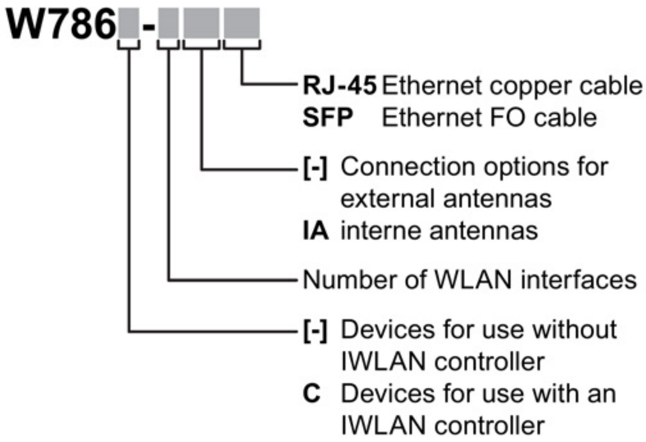
The information in the manuals for the SCALANCE W700 product family often applies to more than one product variant. In such situations, the designations of the products are shortened to avoid having to list all the type designations. The following table shows how the abbreviations relate to the product variants.

Product group	The designation . . . stands for . . .	Product name
Clients (IP30 and IP65)	W748-1	SCALANCE W748-1 RJ-45 SCALANCE W748-1 M12
Access points (IP30 and IP65)	W788-x	SCALANCE W788-1 M12 SCALANCE W788-2 M12 SCALANCE W788-2 M12 EEC SCALANCE W788-1 RJ-45 SCALANCE W788-2 RJ-45
Access points (IP65)	W786-x	SCALANCE W786-1 RJ-45 SCALANCE W786-2 RJ-45 SCALANCE W786-2IA RJ-45 SCALANCE W786-2 SFP
All SCALANCE W access points	W78x	SCALANCE W788-1 M12 SCALANCE W788-2 M12 SCALANCE W788-2 M12 EEC SCALANCE W788-1 RJ-45 SCALANCE W788-2 RJ-45 SCALANCE W786-1 RJ-45 SCALANCE W786-2 RJ-45 SCALANCE W786-2IA RJ-45 SCALANCE W786-2 SFP
SCALANCE W without W786-x	W7x8	SCALANCE W788-1 RJ-45 SCALANCE W788-1 M12 SCALANCE W788-2 RJ-45 SCALANCE W788-2 M12 SCALANCE W748-1 RJ-45 SCALANCE W748-1 M12
All SCALANCE W devices	W700	SCALANCE W748-1 M12 SCALANCE W748-1 M12 SCALANCE W788-1 M12 SCALANCE W788-2 M12 SCALANCE W788-2 M12 EEC SCALANCE W788-1 RJ-45 SCALANCE W788-2 RJ-45 SCALANCE W786-1 RJ-45 SCALANCE W786-2 RJ-45 SCALANCE W786-2IA RJ-45 SCALANCE W786-2 SFP

1.3 Structure of the type designation

The type designation of a SCALANCE W700 is made up of several parts that have the following meaning:


W7 8 -
EEC Extended Environmental Conditions
RJ-45 degree of protection IP30
M12 Degree of protection IP65
Number of IWLAN interfaces
[-] Devices for use without IWLAN controller
C Devices for use with an IWLAN controller
4 Client
8 Access point


W786 -
RJ-45 Ethernet copper cable
SFP Ethernet FO cable
[-] Connection options for external antennas
IA interne antennas
Number of WLAN interfaces
[-] Devices for use without IWLAN controller
C Devices for use with an IWLAN controller

SIMATIC NET glossary

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

You will find the SIMATIC NET glossary here:

- SIMATIC NET Manual Collection or product DVD

  The DVD ships with certain SIMATIC NET products.

- On the Internet under the following entry ID:

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

Description 2

2.1 Network structures

The following article deals with the setting up of various network structures using access points and clients. A client is also an access point in client mode.

Standalone configuration with access point

This configuration does not require a server and the access point does not have a connection to a wired Ethernet. Within its transmission range, the access point forwards data from one WLAN node to another.

The wireless network has a unique name. All the devices exchanging data within this network must be configured with this name.

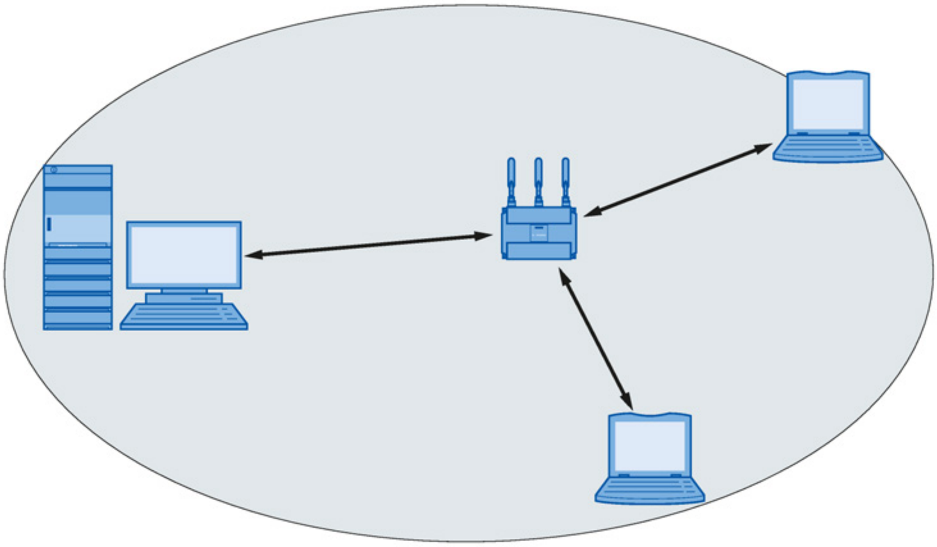


Figure 2-1 Standalone configuration of an access point. The gray area symbolizes the wireless range of the access point.

Wireless access to a wired Ethernet network

If one (or more) access points have access to wired Ethernet, the following applications are possible:

- A single device as gateway:

  A wireless network can be connected to a wired network via an access point.

- Span of wireless coverage for the wireless network with several access points:

  The access points are all configured with the same unique SSID (network name). All nodes that want to communicate over this network must also be configured with this SSID.

  If a mobile station moves from the area covered by one access point to the area covered by another access point, the wireless link is maintained (roaming).

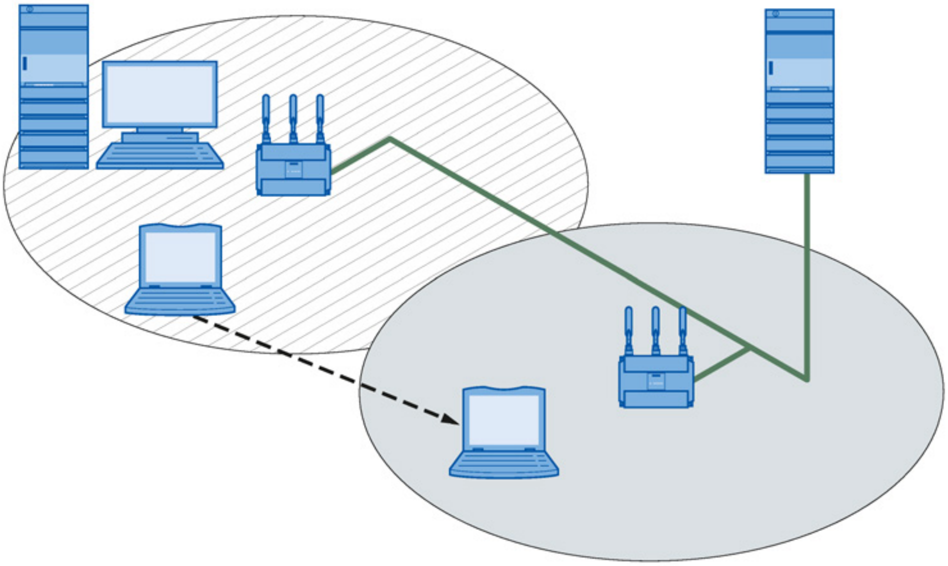


Figure 2-2 Wireless connection of a mobile station over two cells (roaming)

Multichannel configuration

If neighboring access points use the same frequency channel, this can lead to longer response times due to any collisions that may occur. If the configuration shown in the figure is implemented as a single-channel system, computers A and B cannot communicate at the same time with the access points in their wireless cells.

If neighboring access points are set up for different frequencies, this leads to a considerable improvement in performance. As a result, neighboring wireless cells each have their own medium available and the delays resulting from time-offset transmission no longer occur.

The channel spacing should be as large as possible; a practical value is 25 MHz. Even in a multichannel configuration, all access points can be configured with the same network name.

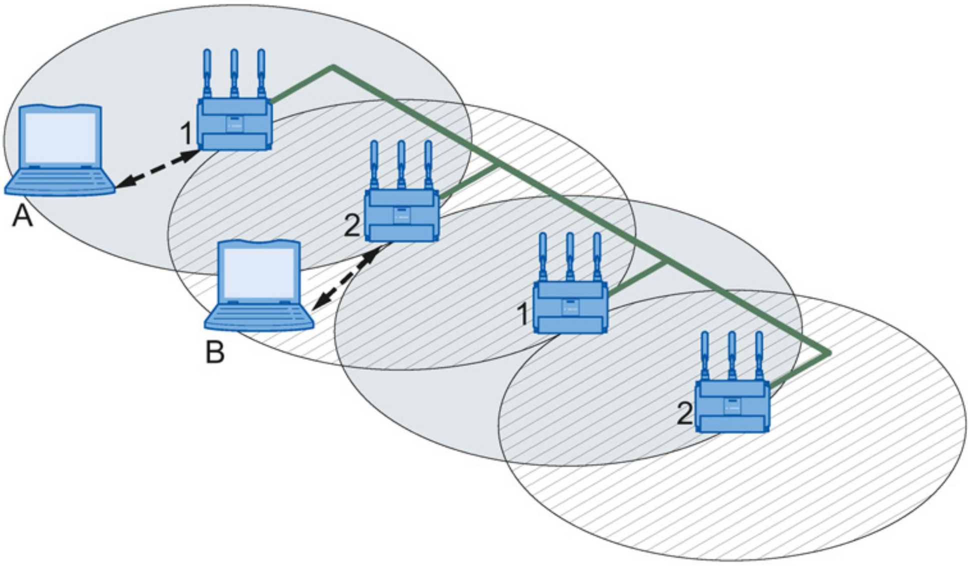


Figure 2-3 Multichannel configuration on channels 1 and 2 with four access points

Wireless Distribution System (WDS)

WDS allows direct links between access points and or between access points and other WDS-compliant devices. These are used to create a wireless backbone or to connect an individual access point to a network that cannot be connected directly to the cable infrastructure due to its location.

Two alternative configurations are possible. The WDS partner can be configured using the WDS ID or using its MAC address.

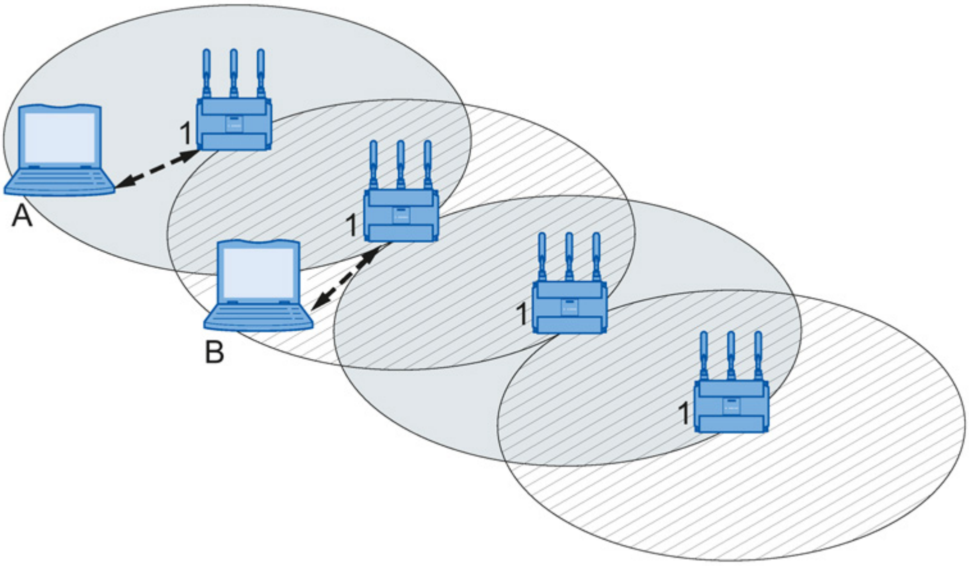


Figure 2-4 Implementation of WDS with four access points

Network access with a client or an access point in client mode

The device can be used to integrate wired Ethernet devices (for example SIMATIC S7 PLC) in a wireless network.

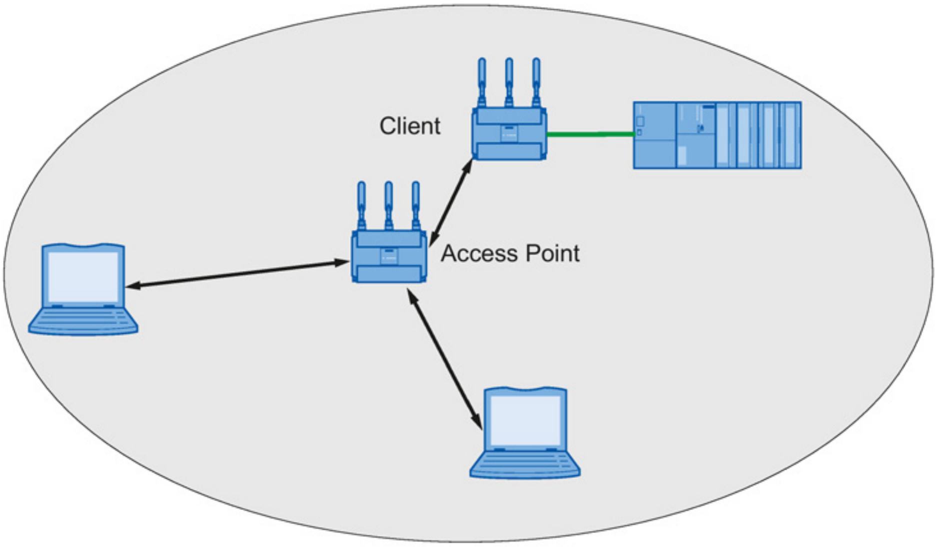


Figure 2-5 Connecting a SIMATIC S7 PLC to a wireless LAN.

2.2 Possible applications of SCALANCE W700 devices

Note

The SIMATIC NET WLAN products use OpenSSL.

This is open source code with license conditions (BSD).

Please refer to the current license conditions.

Since the driver includes encryption software, you should also adhere to the appropriate regulations for your specific country.

Possible applications of the SCALANCE W788

The SCALANCE W788 is equipped with an Ethernet interface and one or two WLAN interfaces. This makes the device suitable for the following applications:

- The SCALANCE W788 forwards data within its transmission range from one node to another without a connection to wired Ethernet being necessary.
- The SCALANCE W788 can be used as a gateway from a wired to a wireless network.
- The SCALANCE W788 can be used as a wireless bridge between two networks.
- The SCALANCE W788 can be used as a bridge between two different frequencies.
- The SCALANCE W788 supports the protection class IP65 and the protection class IP30. The access points are available in two versions:
  - M12 for degree of protection IP65
  - RJ-45 for the degree of protection IP30

With a SCALANCE W788 with two WLAN interfaces, you can also implement a redundant wireless connection to a SCALANCE W78x with two WLAN interfaces.

Possible applications of the SCALANCE W786

The SCALANCE W786 is equipped with up to two Ethernet interfaces and up to two WLAN interfaces. This makes the device suitable for the following applications:

- Due to its extended temperature range, the SCALANCE W786 can be recommended in particular for outdoor applications.
- The SCALANCE W786 forwards data within its transmission range from one node to another without a connection to wired Ethernet being necessary.
- The SCALANCE W786 can be used as a gateway from a wired to a wireless network.
- The SCALANCE W786 can be used as a wireless bridge between two networks.
- The SCALANCE W786 can be used as a bridge between two cells operating at different frequencies.

With a SCALANCE W786 with more than one WLAN interface, you can also implement a redundant wireless connection to a SCALANCE W78x with a maximum of two WLAN interfaces.

Possible applications of the SCALANCE W748

The SCALANCE W748 is equipped with an Ethernet interface and a WLAN interface. This makes the device suitable for the following applications:

- The SCALANCE W748 forwards data within its transmission range from one node to another without a connection to wired Ethernet being necessary.
- The SCALANCE W748 can be used as a gateway from a wired to a wireless network.
- The SCALANCE W748 can be used as a wireless bridge between two networks.

The device can also connect up to 8 stations with IP communication on the Ethernet port to a wireless cell.

2.3 Product characteristics

Properties of the SCALANCE W700 devices

- The Ethernet interface supports the following:
  - 10 Mbps and 100 Mbps both in full and half duplex
  - 1000 Mbps full duplex
  - Autocrossing
  - Autopolarity
- Operating the WLAN interface in the frequency bands 2.4 GHz and 5 GHz.
- The WLAN interface is compatible with the standards IEEE 802.11a , IEEE 802.11b , and IEEE 802.11g. In the 802.11a and 802.11g mode, the gross transmission rate is up to 54 Mbps.
- IEEE 802.11n
  High-speed WLAN standard (wireless LAN) up to 450 Mbps and can operate in the 2.4 GHz and in the 5 GHz range.
- IEEE 802.11h - Supplement to IEEE 802.11a
  In the 802.11h mode, the methods "Transmit Power Control (TPC)" as well as "Dynamic Frequency Selection (DFS)" are used in the range 5.25 - 5.35 and 5.47 - 5.75 GHz. In some countries, this allows the frequency subband of 5.47 - 5.725 GHz to be used in the outdoor area even with higher transmit powers.
  TPC is a method of adapting the transmit power.
  With DFS, the access point searches for primary users for 60 seconds before starting communication on the selected channel. During this time the access point does not send beacons. If signals are found on the channel, the channel is blocked for 30 minutes, the access point changes channel and repeats the check. Primary users are also searched for during operation.
- Support of the authentication standards WPA, WPA-PSK, WPA2, WPA2-PSK and IEEE 802.1x and the encryption methods WEP, AES and TKIP.

Note

The transmission standard IEEE 802.11 n with the setting "802.11n" or "802.11 n only" only supports WPA2/ WPA2-PSK with AES in the security settings.

- For better transmission via WLAN, the function WMM (wireless multimedia) is enabled. The frames are evaluated according to their priority and sent prioritized via the WLAN interface.
- Suitable for inclusion of a RADIUS server for authentication.
- Device-related and application-related monitoring of the wireless connection.
- The interoperability of the devices with Wi-Fi devices of other vendors was tested thoroughly.

- Before commissioning the SCALANCE W700, check the wireless conditions on site. If you intend to use Industrial Wireless LAN systems and WirelessHART systems in the 2.4 GHz band, you will need to plan the use of the channels. At all costs, avoid parallel use of overlapping frequency ranges. The following overlaps exist with Industrial Wireless LAN and WirelessHART:

IWLAN channel **IEEE 802.11 b/g/n**	**WHART channel** **IEEE 802.15.4**
1	11 - 16
6	15 - 20
7	16 - 21
11	20 - 25
13	21 - 25

Note

All SCALANCE W700 access points can be reconfigured for client mode.

Features of the SCALANCE W700

Type	Number of WLAN ports	Antennas	Number and type of Ethernet interface	Degree of protection	Order no.
SCALANCE W748-1 M12	1	external	1 x gigabit Ethernet (copper)	IP65	6GK5748-1GD00-0AA0 6GK5748-1GD00-0AB0 (1)
SCALANCE W748-1 RJ-45	1	external	1 x gigabit Ethernet (copper)	IP30	6GK5748-1FC00-0AA0 6GK5748-1FC00-0AB0 (1)
SCALANCE W786-1 RJ-45	1	external	1 x gigabit Ethernet (copper)	IP65	6GK5786-1FC00-0AA0 6GK5786-1FC00-0AB0 (1)
SCALANCE W786-2 RJ-45	2	external	1 x gigabit Ethernet (copper)	IP65	6GK5786-2FC00-0AA0 6GK5786-2FC00-0AA0 (1)
SCALANCE W786-2IA RJ-45	2	Internal	1 x gigabit Ethernet (copper)	IP65	6GK5786-2HC00-0AA0 6GK5786-2HC00-0AB0 (1)
SCALANCE W786-2 SFP	2	external	2 x SFP slots	IP65	6GK5786-2FE00-0AA0 6GK5 786-2FE00-0AB0 (1)
SCALANCE W788-1 M12	1	external	1 x gigabit Ethernet (copper)	IP65	6GK5788-1GD00-0AA0 6GK5788-1GD00-0AB0 (1)
SCALANCE W788-2 M12	2	external	1 x gigabit Ethernet (copper)	IP65	6GK5788-2GD00-0AA0 6GK5788-2GD00-0AB0 (1)
SCALANCE W788-2 M12 EEC	2	external	1 x gigabit Ethernet (copper)	IP65	6GK5788-2GD00-0TA0 6GK5788-2GD00-0TB0 (1)
SCALANCE W788-1 RJ-45	1	external	1 x gigabit Ethernet (copper)	IP30	6GK5788-1FC00-0AA0 6GK5788-1FC00-0AB0 (1)
SCALANCE W788-2 RJ-45	2	external	1 x gigabit Ethernet (copper)	IP30	6GK5788-2FC00-0AA0 6GK5788-2FC00-0AB0 (1)

(1) US variant

2.4 IEEE 802.11n

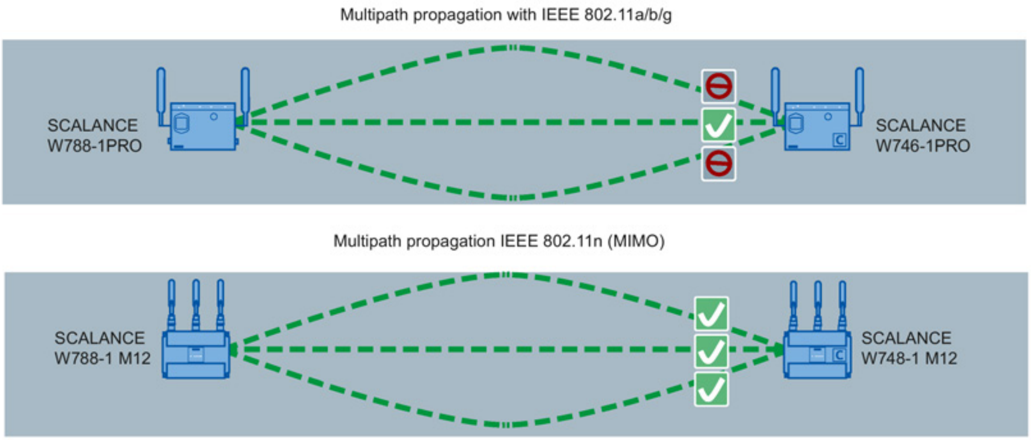
Overview

The standard IEEE 802.11n is an expansion of the 802.11 standard and was approved in 2009.
Previous standards worked either in the 2.4 GHz frequency band (IEEE 802.11g /b) or in the 5 GHz frequency band (IEEE 802.11a). IEEE 802.11n can operate in both frequency band.
In the IEEE 802.11n standard, there are mechanisms implemented in PHY and MAC layers that increase the data throughput and improve the wireless coverage.

- MIMO antenna technology
- Maximum ratio combining (MRC)
- Spatial multiplexing
- Channel bonding
- Frame aggregation
- Accelerated guard interval
- Modulation and coding scheme
- Data throughput rates up to 450 Mbps (gross)
  This is not possible on all devices.

MIMO antenna technology

MIMO (Multiple Input - Multiple Output) is based on an intelligent multiple antenna system. The transmitter and the receiver have several spatially separate antennas. The spatially separate antennas transmit the data streams at the same time. Up to four data streams are possible. The data streams are transmitted over spatially separate paths and return over different paths due to diffraction, refraction, fading and reflection (multipath propagation). The multipath propagation means that at the point of reception a complex, space- and time-dependent pattern results as a total signal made up of the individual signals sent. MIMO uses this unique pattern by detecting the spatial position of characteristic signals. Here, each spatial position is different from the neighboring position. By characterizing the individual senders, the recipient is capable of separating several signals from each other.



Multipath propagation with IEEE 802.11a/b/g

Multipath propagation IEEE 802.11n (MIMO)

Maximum ratio combining (MRC)

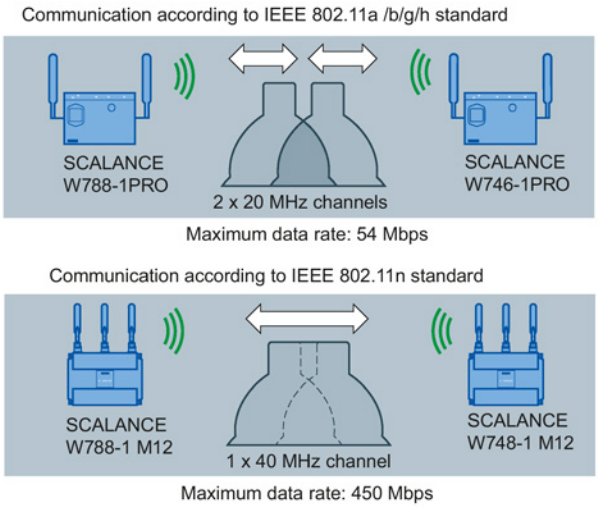
In a multiple antenna system, the wireless signals are received by the individual antennas and combined to form one signal. The MRC method is used to combine the wireless signals. The MRC method weights the wireless signals according to their signal-to-noise ratio and combines the wireless signals to form one signal. The signal-to-noise ratio is improved and the error rate is reduced.

Spatial mutliplexing

With spatial multiplexing, different information is sent using the same frequency. The data stream is distributed over n transmitting antennas; in other words, each antenna sends only 1/n of the data stream. The division of the data stream is restricted by the number of antennas. At the receiver end, the signal is reconstructed.
Due to the spatial multiplexing, there is a higher signal-to-noise ratio and a higher data throughput.

Channel bonding

With IEEE 802.11n, data can be transferred via two directly neighboring channels. The two 20 MHz channels are put together to form one channel with 40 MHz. This allows the channel bandwidth to be doubled and the data throughput to be increased.
To be able to use channel bonding, the recipient must support 40 MHz transmissions. If the recipient does not support 40 MHz transmissions, the band is automatically reduced to 20 MHz. This means that IEEE 802.11n can also communicate with IEEE 802.11a/b/g devices.
The channel bonding is set on the "AP" WBM page with the "HT Channel Width [MHz]" parameter.


Communication according to IEEE 802.11a /b/g/h standard
SCALANCE W788-1PRO
2 x 20 MHz channels
SCALANCE W746-1PRO
Maximum data rate: 54 Mbps
Communication according to IEEE 802.11n standard
SCALANCE W788-1 M12
1 x 40 MHz channel
SCALANCE W748-1 M12
Maximum data rate: 450 Mbps

Frame aggregation

With IEEE 802.11n, it is possible to group together individual data packets to form a single larger packet; this is known as frame aggregation. There are two types of frame aggregation: Aggregated MAC Protocol Data Unit (A-MPDU) and Aggregated MAC Service Data Unit (A-MSDU).
The frame aggregation reduces the packet overheads. Frame aggregation can only be used if the individual data packets are intended for the same receiving station (client).
The W700 devices support both types of frame aggregation. You specify the settings for the A-MPDU data packet on the "AP 802.11n" WBM page.

Accelerated guard interval

The guard interval prevents different transmissions being mixed together. In telecommunications, this mixing is also known as intersymbol interference (ISI).
When the send time has elapsed, a send pause (guard interval) must be kept to before the next transmission begins.

The guard interval of IEEE 802.11a /b/g is 800 ns. IEEE 802.11n can use the reduced guard interval of 400 ns. You specify the guard interval on the "AP 802.11n" WBM page.

Modulation and coding schemes

The IEEE 802.11n standard supports different data rates. The data rates are based on the number of spatial streams, the modulation method and the channel coding. The various combinations are described in modulation and coding schemes.

2.5 Requirements for installation and operation of SCALANCE W700 devices

Requirements for installation and operation of SCALANCE W700 devices

A PG/PC with a network connection must be available in order to configure SCALANCE W700 devices. If no DHCP server is available, a PC on which the Primary Setup Tool (PST) is installed is necessary for the initial assignment of an IP address to the SCALANCE W700 devices. For the other configuration settings, a computer with Telnet or a Web browser is necessary.

2.6 C-PLUG and KEY-PLUG

Configuration information on the C-PLUG / KEY-PLUG

The C-PLUG or KEY-PLUG stores the configuration of a device and can therefore transfer the configuration of the old device to the new device.

NOTICE
Do not remove or insert a C-PLUG / KEY-PLUG during operation!
A PLUG may only be removed or inserted when the device is turned off. The device checks whether or not a PLUG is present at one second intervals. If it is detected that the PLUG was removed, there is a restart. If a valid KEY-PLUG was inserted in the device, the device changes to a defined error state following the restart. With SCALANCE W, the available wireless interfaces are deactivated in this case.
If the device was configured at some time with a PLUG, the device can no longer be used without this PLUG. To be able to use the device again, reset the device to the factory settings.

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

A reconfiguration is necessary if you use functions based on MAC addresses.

Note

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

- **Without PLUG**
  The device stores the configuration in internal memory. This mode is active when no PLUG is inserted.
- **With PLUG**
  The configuration stored on the PLUG is displayed over the user interfaces. If changes are made to the configuration, the device stores the configuration directly on the PLUG and in the internal memory. This mode is active as soon as a PLUG is inserted. As soon as the device is started with a PLUG inserted, the SCALANCE W700 starts up with the configuration data on the PLUG.

Note

Incompatibility with previous versions with PLUG inserted

During the installation of a previous version of the firmware, the configuration data can be lost. In this case, the device starts up with the factory settings after the firmware has been installed. In this situation, if a PLUG is inserted in the device, following the restart, this has the status "NOT ACCEPTED" since the PLUG still has the configuration data of the previous more up-to-date firmware. This allows you to return to the previous, more up-to-date firmware without any loss of configuration data. If the original configuration on the PLUG is no longer required, the PLUG can be deleted or rewritten manually using "System > PLUG".

License information on the KEY-PLUG

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

2.7 Digital input / output

Introduction

The SCALANCE W788-x/W748-x devices in the RJ-45 variant have a digital input/output.

The connection is made using a 4-pin terminal block. You will find information about the pin assignment in the compact operating instructions of the devices.

Application example

- Digital input to signal one item of information, for example "door open", "door closed".
- Digital output, for example for "go to sleep" for devices on an automated guided transport system.

Control of the digital output

Using CLI and using the private MIB variable snMspsDigitalOutputLevel, you can control the digital output (DO/1L).

Note

You cannot configure the digital output with Web Based Management (WBM).

If the digital input changes the status, an entry is made in the event protocol table.

- OID of the private MIB variable snMspsDigitalOutputLevel:

  ```
  iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).siemens(4329).industrialComProducts(20).iComPlatforms(1).simaticNet(1).snMsps(1).snMspsCommon(1).snMspsDigitalIO(39).snMspsDigitalIOObjects(1).snMspsDigitalOutputTable(3).snMspsDigitalOutputEntry(1).snMspsDigitalOutputLevel(6)
  ```

- values of the MIB variable
  - 1: Digital output is open (DO and 1L are interrupted).
  - 2: Digital output is closed (DO and 1L are jumpered).

Digital input

Using the private MIB variable snMspsDigitalInputLevel, you can read out the status of the digital input.

Note

If the digital output changes status, an entry is made in the event protocol table.

- OID of the private MIB variable snMspsDigitalInputLevel:

  ```
  iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).siemens(4329).industria
  lComProducts(20).iComPlatforms(1).simaticNet(1).snMsps(1).snMspsCommon(1).snMspsDi
  gitalIO(39).snMspsDigitalIOObjects(1).snMspsDigitalInputTable(2).snMspsDigitalInpu
  tEntry(1).snMspsDigitalInputLevel(6)
  ```

- values of the MIB variable
  - 1: Signal 0 at the digital input (DI)
  - 2: Signal 1 at the digital input (DI)

MIB file

The MIB variables can be found in the file "SN-MSPS-DIGITAL-IO-MIB" that is part of the private MIB file "snMspsWlan.mib". You will find more detailed information in "Private MIB variables of the SCALANCE W700 (Page 299)".

2.8 Power over Ethernet (PoE)

General

"Power over Ethernet" (PoE) is a power supply technique for network components according to IEEE 802.3af or IEEE 802.3at. The power is supplied over the Ethernet cables that connect the individual network components together. This makes an additional power cable unnecessary. PoE can be used with all PoE-compliant network components that require little power (max. 12.95 W).

Which Ethernet connectors of a device are capable of PoE can be found in the operating instructions of the relevant device.

Cable used for the power supply

- **Variant 1 (redundant wires)**
  In Fast Ethernet, the wire pairs 1, 2 and 3, 6 are used to transfer data. Pairs 4, 5 and 7, 8 are then used to supply power. If there are only four wires, the voltage is modulated onto wires 1, 2 and 3, 6 (see variant 2). This alternative is suitable for a data transmission rate of 10/100 Mbps. This type of power supply is not suitable for 1 Gbps because with gigabit Ethernet, all 8 wires are used for the data transmission.
- **Variant 2 (phantom power)**
  With phantom power, the power is supplied over the pairs that are used for data transfer, in other words, all eight (1 Gbps) or four (10/100 Mbps) wires are used both for the data transfer and the power supply.

Whether a device supports variant 1 and variant 2 or only variant 2 can be found in the operating instructions of the relevant device.

A PoE-compliant switch can supply the end device either using:

- Variant 1 or
- Variant 2 or
- Variant 1 and variant 2.

Endspan

With endspan, the power is supplied via a switch that can reach a device over an Ethernet cable. The switch must be capable of PoE, for example a SCALANCE X108PoE, SCALANCE X308-2M POE, SCALANCE XR552-12M.

Midspan

Midspan is used when the switch is not PoE-compliant. The power is supplied by an additional device between the switch and end device. In this case, only data rates of 10/100 Mbps can be achieved because the power is supplied on redundant wires.

A Siemens power insert can also be used as the interface for the power input. Since a power insert supports a power supply of 24 VDC, it does not conform with 802.3af or IEEE 802.3at. The following restrictions relating to the use of power inserts should be noted:

⚠ WARNING

Operate the power insert only when the following conditions apply:

- with extra low voltages SELV, PELV complying with IEC 60364-4-41
- in USA/CAN with power supplies complying with NEC class 2
- in USA/CAN, the cabling must meet the requirements of NEC/CEC
- Power load maximum 0.5 A.

Cable lengths

Table 2- 1 Permitted cable lengths (copper cable - Fast Ethernet)

Cable type	Accessory (plug, outlet, TP cord)	Permitted cable length
IE TP torsion cable	with IE FC Outlet RJ-45 + 10 m TP cord	0 to 45 m + 10 m TP cord
	with IE FC RJ-45 Plug 180	0 to 55 m
IE FC TP Marine Cable IE FC TP Trailing Cable IE FC TP Flexible Cable	with IE FC Outlet RJ-45 + 10 m TP cord	0 to 75 m + 10 m TP cord
	with IE FC RJ-45 Plug 180	0 to 85 m
IE FC TP standard cable	with IE FC Outlet RJ-45 + 10 m TP cord	0 to 90 m + 10 m TP cord
	with IE FC RJ-45 Plug 180	0 to 100 m

Table 2- 2 Permitted cable lengths (copper cable - gigabit Ethernet)

Cable type	Accessory (plug, outlet, TP cord)	Permitted cable length
IE FC standard cable, 4×2, 24 AWG	with IE FC RJ-45 Plug 180, 4x2	0 to 90 m
IE FC flexible cable, 4×2, 24 AWG	with IE FC RJ-45 Plug 180, 4x2	0 to 60 m
IE FC standard cable, 4×2, 22 AWG	with IE FC Outlet RJ-45 + 10 m TP cord	0 to 100 m + 10 m TP cord

Table 2- 3 Fitting connectors

PIN	Color of the wire CAT5	Color of the wire CAT6a	Use	
			Power over unused wires (10/100 Mbps only)	Phantom power
1	Yellow	Green/white	Data	Data/power
2	Orange	Green	Data	Data/power
3	White	Orange/white	Data	Data/power
6	Blue	Orange	Data	Data/power
4		Blue	Power	unused at 10/100 Mbps
5		Blue/white	Power	unused at 10/100 Mbps
7		Brown/white	Power	unused at 10/100 Mbps
8		Brown	Power	unused at 10/100 Mbps

LEDs for PoE on the SCALANCE W700 device

When the device is supplied by PoE, the green "PoE" LED is lit on the SCALANCE W700 device.

Technical basics 3

3.1 VLAN

Network definition regardless of the spatial location of the nodes

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

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

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

Options for the VLAN assignment

There are various options for the assignment to VLANs:

- Port-based VLAN

  Each port of a device is assigned a VLAN ID. You configure port-based VLAN in "Layer 2 > VLAN (Page 242)".

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

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

3.2 MAC-based communication

Adopt MAC automatically / Adopt MAC manually

Frames in the direction from the client to the access point always have the MAC address of the WLAN interface as the source MAC address. As a result, the learning table at the access point end always has only the MAC address of the WLAN interface of the client. If the MAC address of a device connected to the client is adopted, both the MAC-based and the IP-based frames find their destination in precisely this device.

Communication at the MAC address level (ISO/OSI layer 2) can only be to a subscriber downstream from the client. With IP Mapping, several subscribers downstream from a client can be addressed based on the IP protocol.

The access point checks whether the destination MAC address matches the MAC addresses of the connected clients. Since a client can only adopt one MAC address, the access point does not find a match and discards the packets of several nodes.

Maximum possible number of MAC nodes downstream from the client: 1

Notes on the "Automatic" setting:

- As long as there is no link on the Ethernet interface, the device uses the MAC address of the Ethernet interface so that it can be reached in this status. In this status, the device can be found using the Primary Setup Tool and configured with WBM or CLI.
- As soon as there is a link on the Ethernet interface, the device adopts the source MAC address of the first received frame.

Note

From the moment that the device adopts another MAC address (whether manually or automatically), the device no longer responds to queries of the Primary Setup Tool when the query is received over the WLAN interface. Queries of the PST over the Ethernet interface continue to be replied to.

Adopt Own MAC

If IP-based frames need to be sent to a device connected downstream from the client, the default setting "Own" can be retained. The client registers with the MAC address of its Ethernet adapter. The IP packets are broken down according to an internal table and forwarded to the connected devices (IP mapping).

Maximum possible number of MAC nodes downstream from the client: 8

Layer 2 Tunnel

With a "Layer 2 Tunnel", the client provides information about the devices downstream from it when it registers with an access point. This makes it possible to enter the MAC addresses of these devices in the learning table of the access point. The access point can forward MAC-based frames for the devices downstream from the client to the appropriate client.

In much the same way as with WDS, a separate port is created for the L2T client over which the Ethernet frames are sent without changing the destination MAC address.

Maximum possible number of MAC nodes downstream from the client: 8

3.3 iPCF / iPCF-MC

The wireless range of an IWLAN system can be expanded by using multiple access points. If a client moves from the area covered by one access point to the area covered by another access point, the wireless link is maintained after a short interruption (roaming).

In an industrial environment, there are applications that require a deterministic response when there are large numbers of nodes and when roaming to another cell require handover times of less than 100 milliseconds.

- **iPCF** (industrial Point Coordination Function)

  iPCF ensures that the entire data traffic of a cell is ordered, controlled by the access point. Even with large numbers of nodes, collisions can also be avoided. iPCF also allows fast cell changes.

  You configure iPCF in "iFeatures > iPCF (Page 281)".

- **iPCF-MC** (industrial Point Coordination Function - Management Channel)

  iPCF-MC was developed to make the advantages of iPCF available to fully mobile nodes that communicate without being dependent on RCoax cable or directional antennas. With iPCF-MC, the client also searches for potentially suitable access points when it receives iPCF queries from the access point and the existing connection to an access point is working problem-free. This means that if a change to a different access point is necessary, this is achieved extremely quickly. In contrast to iPCF, the handover times for iPCF-MC are not dependent on the number of wireless channels being used.

  You configure iPCF-MC in "iFeatures > iPCF-MC (Page 284)".

iPCF / iPCF-MC - how it works

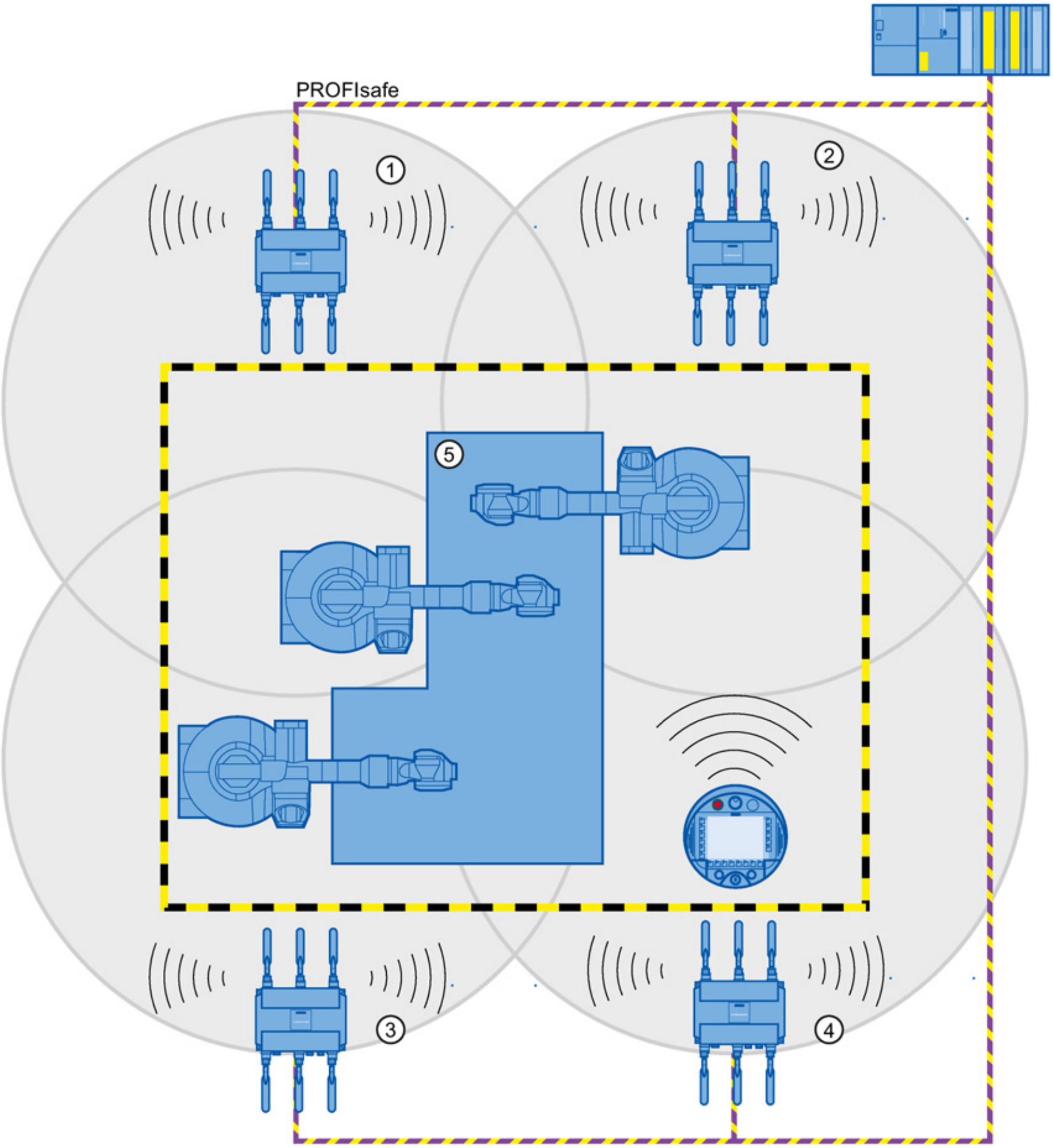
The access point checks all nodes in the wireless cell cyclically. At the same time, the scan includes the downlink traffic for this node. In the reply, the node sends the uplink data. The access point scans a new node at least every 5 ms.

The scan of a node is seen by all other nodes in the cell. This allows a client to detect the quality of the wireless link to the access point even when it is not communicating with the access point itself. If the client does not receive any frames from the access point for a certain time, it starts to search for a new access point.

In iPCF mode, both the search for a new access point and the registration with this access point have been optimized in terms of time. Handover times significantly below 50 ms are achieved.

Stable PNIO communication is only possible when a WLAN client is in a cell with more than 60 % (-65 dBm) signal strength at all times. This can be checked by activating and deactivating the various wireless cells.

This does not mean that the client needs to change when there is a signal strength < 60 % (< -65 dBm). Make sure that access points are available with adequate signal strength.



①	Wireless cell of access point 1
②	Wireless cell of access point 2
③	Wireless cell of access point 3
④	Wireless cell of access point 4
⑤	Plant

Figure 3-1	Configuration example of iPCF-MC

Restrictions

- iPCF and iPCF-MC are developments of Siemens AG and function only with nodes on which iPCF / iPCF-MC is implemented.
- With an access point with several WLAN interfaces, it is possible to use both iPCF as well as standard WLAN at the same time.
- Access points with a WLAN interface cannot take part in the iPCF-MC procedures, iPCF is, however, possible.

Requirements for iPCF-MC

iPCF-MC uses the two wireless interface of the access point in different ways: One interface works as the management interface and sends a beacon every five milliseconds. The other interface transfers the user data.

The following requirements must be met before you can use iPCF-MC:

- Only devices with two WLAN interfaces can be used as access points
- The data interface (WLAN1) and management interface (WLAN2) must be operated in the same frequency band and must match in terms of their wireless coverage. iPCF-MC will not work if the two wireless interfaces are equipped with directional antennas that cover different areas.
- The management interfaces of all access points to which a client can change must use the same channel. A client scans only this one channel to find accessible access points.
- Transmission based on IEEE 802.11h (DFS) cannot be used for the management interface. 802.11h (DFS) is possible for the data interface.
- A client must support this feature on its WLAN interface.

3.4 iREF

How it works

If an access point has several activated antennas, the transmit power is distributed equally on these antennas. The transmit power is subject to country-specific legal restrictions. The maximum permitted power depends on the gain of the connected antennas. If the connected antennas have different gains, the maximum antenna gain effectively restricts the permitted transmit power.

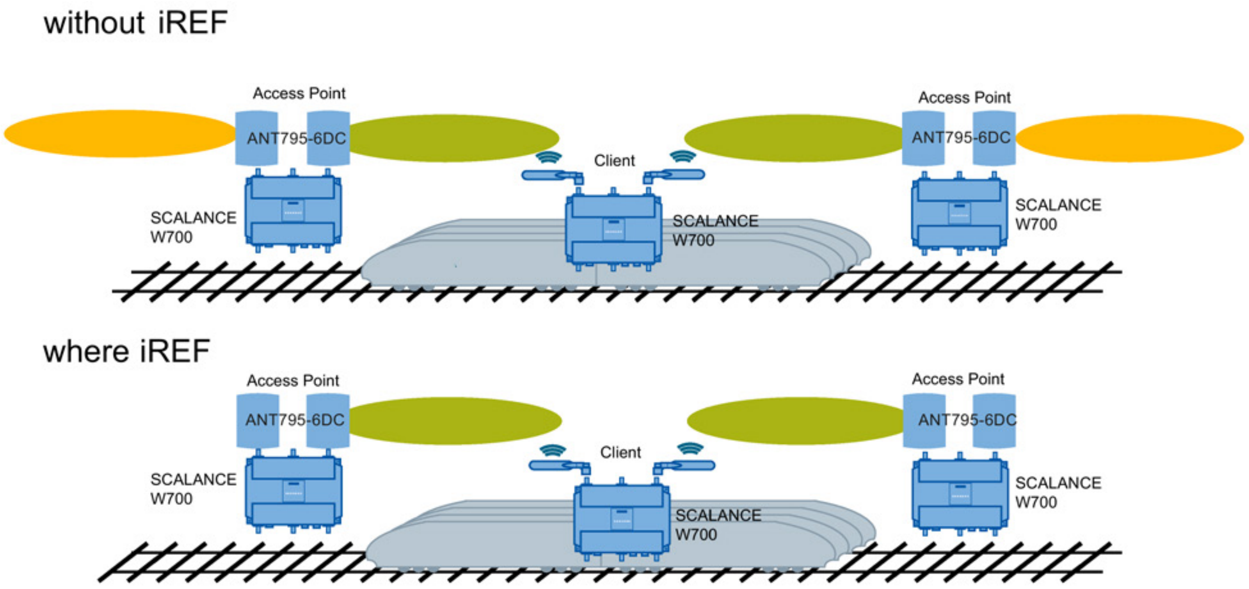
iREF (industrial Range Extension Function) ensures that the data traffic from the access point to each individual client is handled via the most suitable antenna. Which antenna is most suitable is determined by the access point based on the RSSI values of received packets.

Taking into account antenna gain and possible cable losses, packets are only sent via the antennas with which the maximum signal strength at the client end can be expected.

During this time the other antennas are inactive and the legally permitted transmit power is available for the selected antenna. The inactive antennas do not restrict the permitted transmit power.

In particular in applications in which MIMO cannot be used or brings no advantage, this allows data to be transmitted at the highest possible data transmission rate.

You configure iREF in "iFeatures > iREF (Page 286)"


without iREF

where iREF

Requirement

- To be able to use iREF, the device must have at least 2 activated antennas.

Restrictions

- A maximum data rate of only up to 150 Mbps (MCS 0 - 7 or 1 x spatial stream) is possible
- iREF cannot be used along with other iFeatures (for example iPCF or iPCF-MC)

Advantages

- Due to the directional data transmission and dynamic deactivation of antennas that do not radiate in the direction of the particular client, interference can be reduced.
- The signal strength is improved because the active antenna always has the maximum permitted transmit power available.

3.5 AeroScout

AeroScout tags

SCALANCE W devices support tags of the AeroScout company. Tags are battery-operated RFID sensors that send their data cyclically as multicast frames.

Among other things, AeroScout tags have the following features:

- **Ambient temperature**

  If a tag is fitted to a device or material, it is possible to monitor whether a selected ambient temperature is being maintained.

- **Motion**

  Here, a tag can also supply information indicating whether it is in motion or stationary. The areas of material flow and material handling engineering represent possible applications for this function.

- **Button**

  Regardless of the frames sent cyclically, a user can also send a message by pressing a button.

- **LED**

  This provides information on the operating status of the tag.

Note

For more detailed information, please refer to the AeroScout documentation (www.aeroscout.com).

How it works

The tag sends its data as AeroScout frames. The tags and the access points communicate in the 2.4 GHz band.

If the WLAN interface of the access point receives the AeroScout frame, this is converted into a UDP datagram. The device forwards the UDP datagram along with the information about the signal strength (RSSI) to a PC. The AeroScout Engine runs on the PC and evaluates the received information.

Note

It is **not** advisable to use PNIO communication and AeroScout together on one wireless interface.

Accuracy of localization

To achieve optimum precision in the localization of AeroScout Tags,

- we recommend the use of antennas with omnidirectional characteristics
- if the signals should be received by at least three access points.

3.6 NAT/NAPT

What is NAT?

With Network Address Translation (NAT), the IP address in a data packet is replaced by another. NAT is normally used on a gateway between a private LAN and an external network with globally valid IP addresses. A local IP address of the internal LAN is changed to an external global IP address by a NAT device at the gateway.

To translate the internal into the global IP address, the NAT device maintains a translation list. The address assignment is automatic. You configure the address assignment in "Layer 3 > NAT > Basic (Page 260)".

What is NAPT?

In "Network Address Port Translation" (NAPT) or "Port Address Translation" (PAT), several internal source IP addresses are translated into the same external source IP address. To identify the individual source nodes, the port of the source device is also stored in the translation list of the NAT gateway and translated for the external address.

If several local clients send a query to the same external destination IP address over the NAT gateway, the gateway enters its own external source IP address in the header of these forwarded frames. Since the forwarded frames have the same global source IP address, the NAT gateway assigns the frames to the clients using different port number.

Note

NAT/NAPT is possible only on layer 3 of the ISO/OSI reference model. To use the NAT function, the networks must use the IP protocol.

When using the ISO protocol that operates at layer 2, it is not possible to use NAT.

If a client from the global network wants to use a service in the internal network, the translation list for the static address assignment needs to be configured. You configure the translation list for NAPT in "Layer 3 > NAT > NAPT (Page 261)".

3.7 SNMP

Introduction

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

Tasks of SNMP:

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

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

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

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

Standard values of the community strings:

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

Note

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

Further simple protection mechanisms at the device level:

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

SNMP data packets are not encrypted and can easily be read by others.

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

The management station sends data packets of the following type:

- GET
  Request for a data record from the agent
- GETNEXT
  Calls up the next data record.
- GETBULK (available as of SNMPv2)
  Requests multiple data records at one time, for example several rows of a table.
- SET
  Contains parameter assignment data for the relevant device.

The SNMP agent sends data packets of the following type:

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

SNMPv1 and SNMPv2 and SNMPv3 use UDP (User Datagram Protocol). The data is described in a Management Information Base (MIB).

SNMPv3

Compared with the previous versions SNMPv1 and SNMPv2. SNMPv3 introduces an extensive security concept.

SNMPv3 supports:

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

3.8 Spanning Tree

Avoiding loops

The Spanning Tree algorithm detects redundant physical network structures and prevents the formation of loops by disabling redundant paths. It evaluates the distance and performance of a connection or bases the decisions on settings made by the user. Data is then exchanged only over the remaining connection paths.

If the preferred data path fails, the Spanning Tree algorithm then searches for the most efficient path possible with the remaining nodes.

Root bridge and bridge priority

The identification of the most efficient connection is always related to the root bridge, a network component that can be considered as a root element of a tree-like network structure. With the "Bridge Priority" parameter, you can influence the selection of the root bridge. The computer with the lowest value set for this parameter automatically becomes the root bridge. If two computers have the same priority value, the computer with the lower MAC address becomes the root bridge.

Response to changes in the network topology

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

Keeping configuration information up to date

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

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

3.8.1 RSTP, MSTP, CIST

Rapid Spanning Tree Protocol (RSTP)

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

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

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

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 or VLAN groups and, for example, making paths available within the individual VLANs that the single Rapid Spanning Tree Protocol would globally block.

Note

Default setting

HTTP is enabled as default on the device.

Common and internal Spanning Tree (CIST)

CIST identifies the internal instance used by the switch that is comparable in principle with an internal RSTP instance.

Assignment of an IP address 4

4.1 Structure of an IP address

Address classes

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

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

XXX.XXX.XXX.XXX

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

Subnet mask

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

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

Example of a class B network:

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

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

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

Note

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

4.2 Initial assignment of an IP address

Configuration options

An initial IP address for a SCALANCE W700 cannot be assigned using Web Based Management (WBM) or the Command Line Interface (CLI) over Telnet because these configuration tools require that an IP address already exists.

The following options are available to assign an IP address to an unconfigured device currently without an IP address:

- DHCP (default)
- Primary Setup Tool
- STEP 7
- NCM PC

Note

When the product ships and following "Restore Factory Defaults and Restart", DHCP is enabled. If a DHCP server is available in the local area network, and this responds to the DHCP request of a SCALANCE W700, the IP address, subnet mask and gateway are assigned automatically when the device first starts up. " Restore Memory Defaults and Restart" does not delete an IP address assigned either by DHCP or by the user.

4.3 Address assignment with DHCP

Properties of DHCP

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

- DHCP can be used both when starting up a device and during ongoing operation.
- The assigned IP address remains valid only for a limited time known as the lease time. Once this period has elapsed, the client must either request a new IP address or extend the lease time of the existing IP address.
- There is normally no fixed address assignment; in other words, when a client requests an IP address again, it normally receives a different address from the previous address. It is possible to configure the DHCP server so that the DHCP client always receives the same fixed address in response to its request. The parameter with which the DHCP client is identified for the fixed address assignment is set on the DHCP client. The address can be assigned via the MAC address, the DHCP client ID or the system name. You configure the parameter in "System > DHCP Client (Page 162)".
- The following DHCP options are supported:
  - DHCP option 66: Assignment of a dynamic TFTP server name
  - DHCP option 67: Assignment of a dynamic boot file name
  - DHCP option 82: Assignment of IP addresses depending on the switch port or the VLAN ID

Note

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

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

4.4 Address assignment with the Primary Setup Tool

Introduction

The PST (Primary Setup Tool) is capable of assigning such an address to unconfigured devices that do not yet have an IP address.

Requirement

The devices can be reached via Ethernet.

Note

For more detailed information, refer to the Primary Setup Tool configuration manual.

You will find the PST at Siemens Industry Automation and Drives Service & Support on the Internet under entry ID 19440762. The URL for this entry is:

http://support.automation.siemens.com/WW/view/en/19440762
(http://support.automation.siemens.com/WW/view/en/19440762)

4.5 Address assignment with STEP 7

In STEP 7, you can configure the topology, the device name and the IP address; in other words, an IP address is specified for the MAC address of the IWLAN device. If you connect the unconfigured IWLAN device to the controller, the controller assigns the configured device name and the IP address to the IWLAN device automatically.

STEP 7 V5.x and earlier

For further information on the assignment of the IP address using STEP 7 V5.x and earlier, refer to the documentation "Configuring Hardware and Communication Connections STEP 7", in the section "Steps for Configuring a PROFINET IO System".

STEP 7 as of V13

For further information on assigning the IP address using STEP 7 as of V13, refer to the online help "Information system", section "Addressing PROFINET devices".

Configuring with Web Based Management 5

5.1 Web Based Management

How it works

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

Note

Secure connection

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

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

Requirements

WBM display

- The device has an IP address
- There is a connection between the device and the client device. With the Windows ping command, you can check whether or not a connection exists.
- Access via HTTPS is enabled.
- JavaScript is activated in the Web browser.
- The Web browser must not be set so that it reloads the page from the server each time the page is accessed. The updating of the dynamic content of the page is ensured by other mechanisms. In the Internet Explorer, you can make the appropriate setting in the "Options > Internet Options > General" menu in the section "Browsing history" with the "Settings" button. Under "Check for newer versions of stored pages:", select "Automatically".

- If a firewall is used, the relevant ports must be opened.
  - For access using HTTP: Port 80
  - For access using HTTPS: Port 443
- The display of the WBM was tested with the following desktop Web browsers:
  - MS IE 10

    Note

    Compatibility view

    In Microsoft Internet Explorer, disable the compatibility view to ensure correct display and to allow problem-free configuration using WBM.

  - Mozilla Firefox ESR31

Display of the WBM on mobile devices

- The display of the WBM was tested with the following Web browsers for mobile devices:
  - Safari as of V7 on iOS as of V7.1.1 (iPad mini Model A1432)
  - Chrome as of V32 on Android as of version 4.4.3 (Nexus 7C Asus),
- Minimum resolution: 960 x 640 pixels

Note

Display of the WBM and working with it on mobile devices

The display on the WBM pages and how you work with them on mobile devices may differ compared with the same pages on desktop devices. Some pages also have an optimized display for mobile devices.

5.2 Login

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.

Logging on using the Internet browser

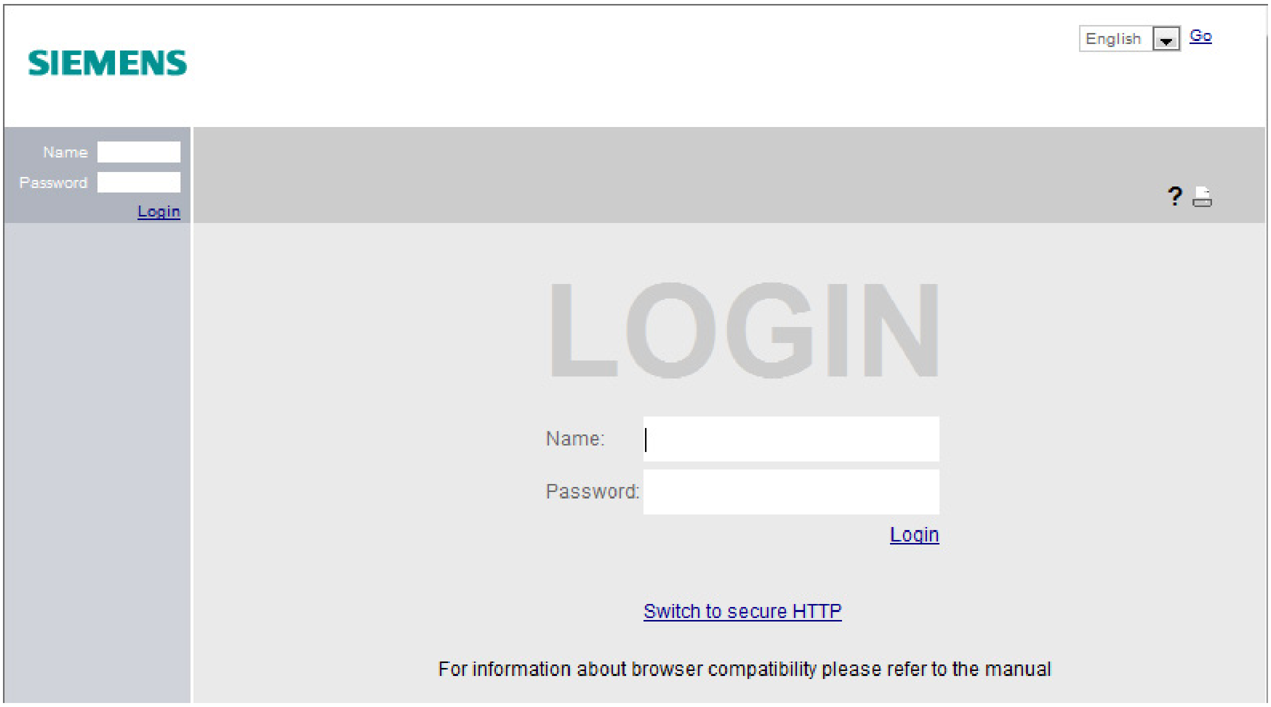
Selecting the language of the WBM

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

Note

Available languages

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



For information about browser compatibility please refer to the manual

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.
   When you log in for the first time or following a "Restore Factory Defaults und Restart", enter the standard password in the "Password" input box.
   - "admin": standard password "admin"
   - "user": standard password "user"
3. Click the "Login" button or confirm your entry with "Enter".
   When you log in for the first time or following a "Restore Factory Defaults and Restart", you will be prompted to change the password. The new password must be at least 6 characters long. You need to repeat the password as confirmation. The password entries must match. Click the "Set Values" to complete the action and activate the new password.

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

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.
2. Confirm the displayed certificate warning.
   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 in the "Password" input box.
   When you log in for the first time or following a "Restore Factory Defaults und Restart", enter the standard password in the "Password" input box.
   - "admin": standard password "admin"
   - "user": standard password "user"
5. Click the "Login" button or confirm your entry with "Enter".
   When you log in for the first time or following a "Restore Factory Defaults and Restart", you will be prompted to change the password. The new password must be at least 6 characters long. You need to repeat the password as confirmation. The password entries must match. Click the "Set Values" to complete the action and activate the new password.

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

5.3 "Wizard" menu

5.3.1 Basic Wizard

Introduction

With the Basic Wizard, menus guide you through the configuration of the most important parameters.

On the Basic Wizard pages, you can only configure the parameters important for the basic functionality. You make further settings when you have finished with the Basic Wizard.

Requirement

- The device is in the status it was when it was shipped and can be reached via the Ethernet interface.
- You have assigned an IP address to the device. For more detailed information, refer to the section "Assignment of an IP address (Page 53)".
- You are logged on in WBM as the "admin" user. For more detailed information, refer to the section "Login (Page 61)".

Starting the Basic Wizard

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

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

Buttons you require often

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

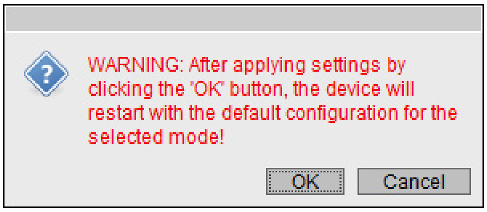
Button	Description
Next	Goes to the next page
Previous	Goes back to the previous page
Abort	The Basic Wizard is closed without adopting the settings.
Set Values	Saves the configuration and exits the Wizard.

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

5.3.1.1 System Settings

Introduction

On this Basic Wizard page, you specify the mode of the device. After changing the mode, a message is displayed.

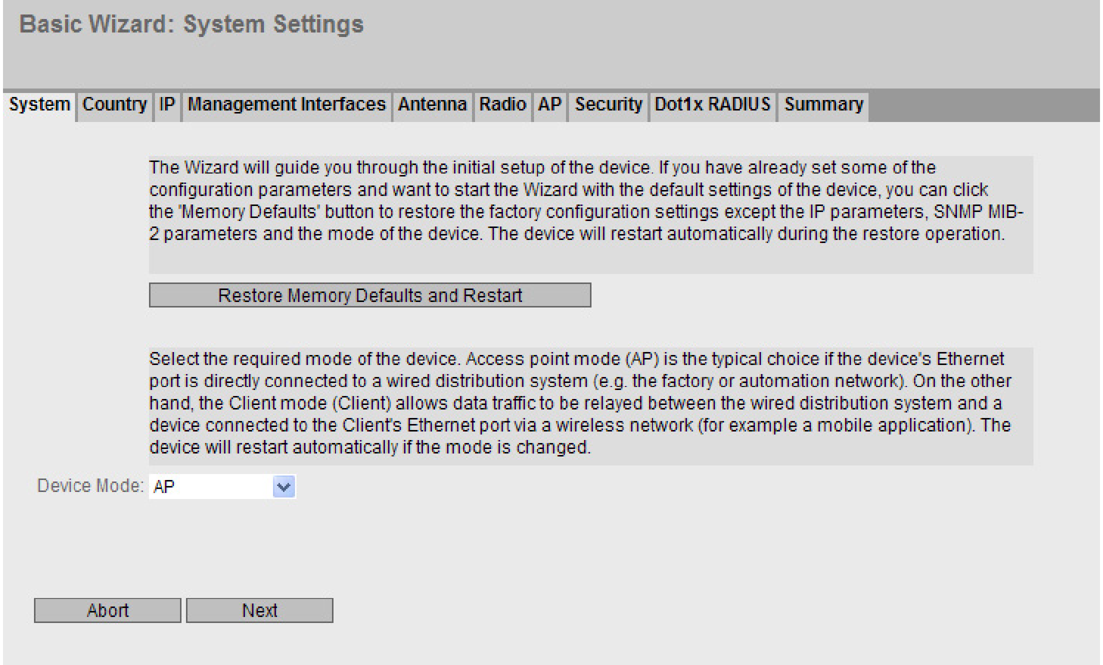


WARNING: After applying settings by clicking the 'OK' button, the device will restart with the default configuration for the selected mode!

If you confirm the message with "OK", the device restarts with the factory-set configuration settings. Log on again and start the Basic Wizard to continue the configuration of the device for the selected mode.

Note

Because only access points can work in client mode as well, the mode can only be selected for these devices.



Basic Wizard: System Settings

The Wizard will guide you through the initial setup of the device. If you have already set some of the configuration parameters and want to start the Wizard with the default settings of the device, you can click the 'Memory Defaults' button to restore the factory configuration settings except the IP parameters, SNMP MIB-2 parameters and the mode of the device. The device will restart automatically during the restore operation.

Select the required mode of the device. Access point mode (AP) is the typical choice if the device's Ethernet port is directly connected to a wired distribution system (e.g. the factory or automation network). On the other hand, the Client mode (Client) allows data traffic to be relayed between the wired distribution system and a device connected to the Client's Ethernet port via a wireless network (for example a mobile application). The device will restart automatically if the mode is changed.

Device Mode: AP

Description

The Basic Wizard page contains the following boxes:

- **"Restore Memory Defaults and Restart" button**
  If you click this button, the factory configuration settings are restored with the exception of the parameters below followed by a restart.
  - IP address
  - Subnet mask
  - IP address of the default gateway
  - DHCP client ID
  - DHCP
  - System name
  - System location
  - System contact
  - User names and passwords
  - Mode of the device

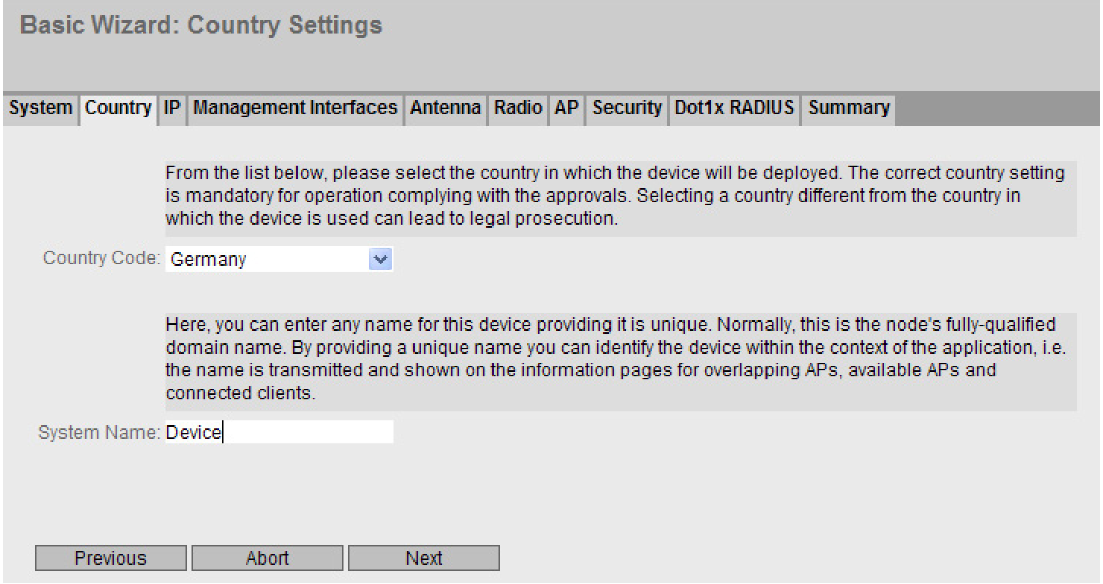
After restarting the device, you will need to log on again and start the Basic wizard again to configure the device.

- **"Device Mode" drop-down list**
  Select the mode of the device. This selection is available only for access points.
  The following operating modes are possible:
  - AP: Access point mode
  - Client: Client mode

5.3.1.2 Country Settings

Introduction

On this Basic Wizard page, you configure the country and the system name.



Basic Wizard: Country Settings

From the list below, please select the country in which the device will be deployed. The correct country setting is mandatory for operation complying with the approvals. Selecting a country different from the country in which the device is used can lead to legal prosecution.

Country Code: Germany

Here, you can enter any name for this device providing it is unique. Normally, this is the node's fully-qualified domain name. By providing a unique name you can identify the device within the context of the application, i.e. the name is transmitted and shown on the information pages for overlapping APs, available APs and connected clients.

System Name: Device

Description

The Basic Wizard page contains the following boxes

- **"Country Code" drop-down list**
  From this drop-down list, you select the country in which the device will be deployed. You do not need to know the data for the specific country, the channel division and output power are set by the device according to the country you select.

  Note

  Locale setting

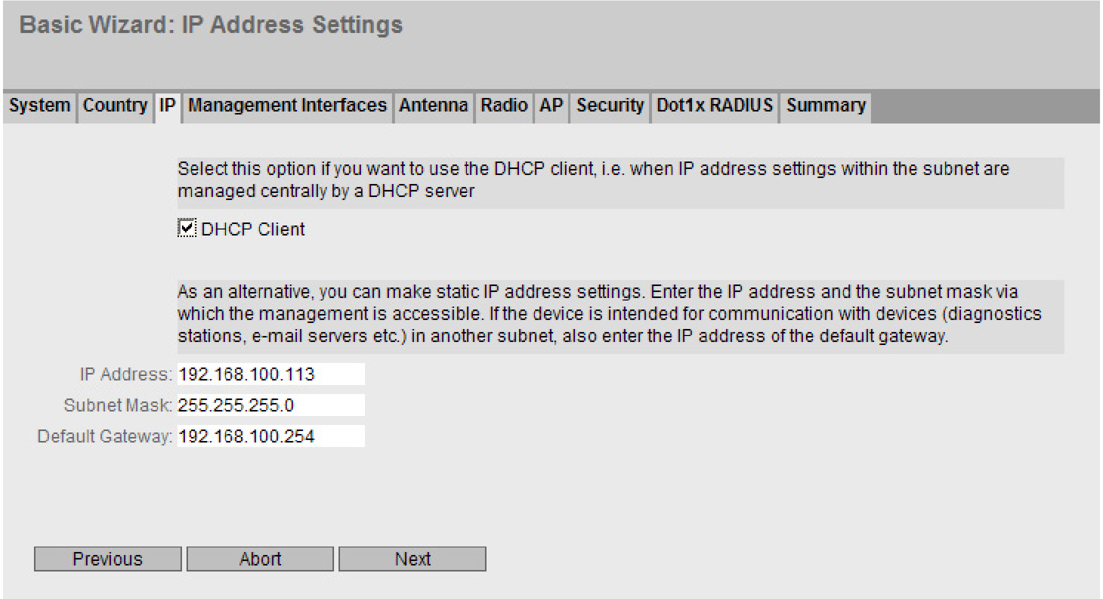
  The correct country setting is mandatory for operation complying with the approvals. Selecting a country different from the country of use can lead to legal prosecution.

- **"System Name" input box**
  You can enter the name of the device. If you configure this box, this configuration is adopted and displayed in the selection area. A maximum of 255 characters are possible. The system name is also displayed in the CLI input prompt. The number of characters in the CLI input prompt is limited. The system name is truncated after 16 characters.

5.3.1.3 IP Address Settings

Introduction

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



Basic Wizard: IP Address Settings

Select this option if you want to use the DHCP client, i.e. when IP address settings within the subnet are managed centrally by a DHCP server

☑ DHCP Client

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

IP Address: 192.168.100.113
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.100.254

Description

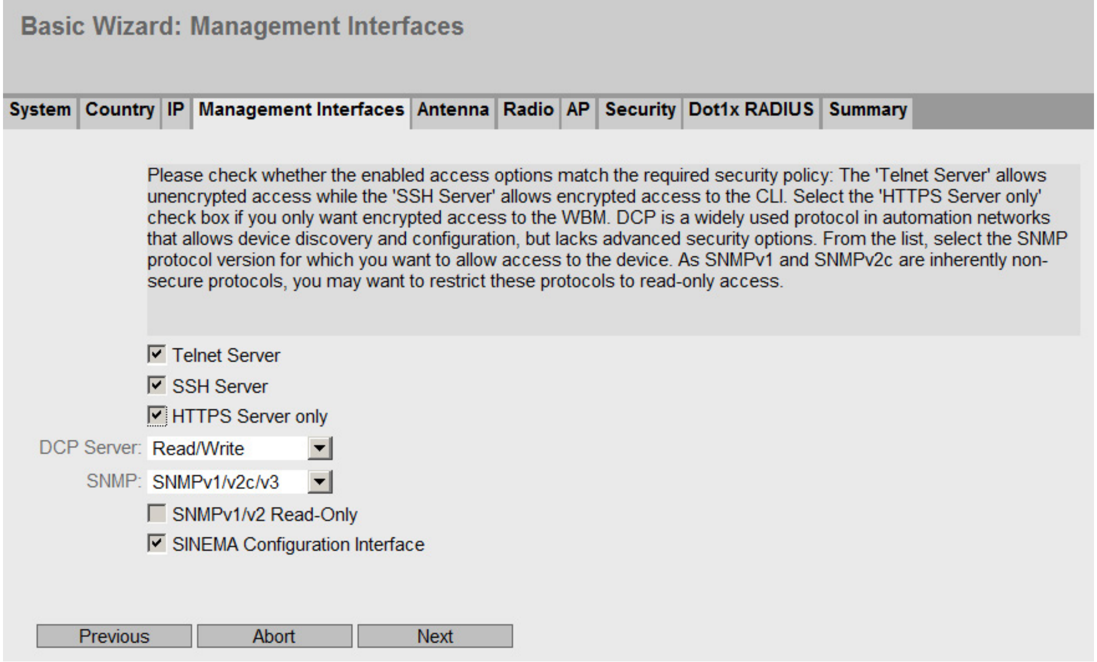
The Basic Wizard page contains the following boxes

- **"DHCP Client" check box**
  Specify how the IP address will be assigned. There are two methods of assigning IP addresses.
  – Enabled
    The device obtains a dynamic IP address from a DHCP Server.
  – Disabled
    You enter the IP settings in the "IP Address" and "Subnet Mask" input boxes.
- **"IP Address" input box**
  Enter an IP address that is unique within your network.
- **"Subnet Mask" input box**
  Enter the subnet mask of the device.
- **"Default Gateway" input box**
  Enter the IP address of the default gateway so that the device can communicate with devices in other subnets, for example diagnostics stations, e-mail server.

5.3.1.4 Management Interfaces

System configuration

On this Basic Wizard page, you specify the services with which the device can be accessed. With some services, there are further configuration pages on which more detailed settings can be made. Configure these services after completing the Basic Wizard.



Basic Wizard: Management Interfaces

Please check whether the enabled access options match the required security policy: The 'Telnet Server' allows unencrypted access while the 'SSH Server' allows encrypted access to the CLI. Select the 'HTTPS Server only' check box if you only want encrypted access to the WBM. DCP is a widely used protocol in automation networks that allows device discovery and configuration, but lacks advanced security options. From the list, select the SNMP protocol version for which you want to allow access to the device. As SNMPv1 and SNMPv2c are inherently non-secure protocols, you may want to restrict these protocols to read-only access.

☑ Telnet Server
☑ SSH Server
☑ HTTPS Server only
DCP Server: Read/Write
SNMP: SNMPv1/v2c/v3
☐ SNMPv1/v2 Read-Only
☑ SINEMA Configuration Interface

Description

The page contains the following boxes:

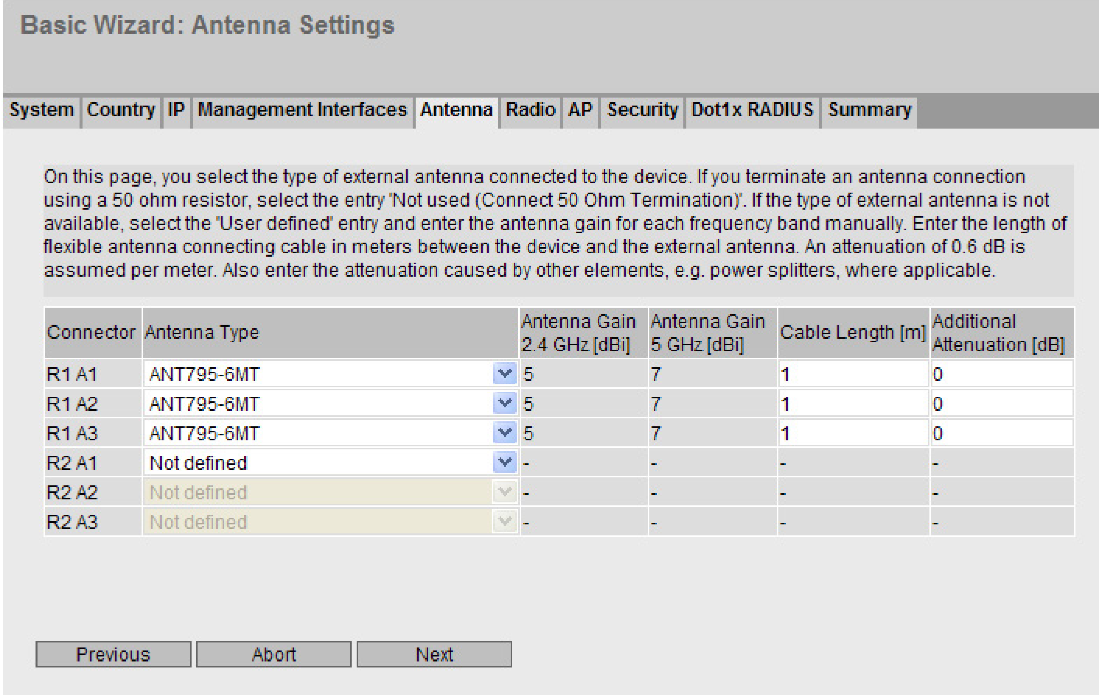
- **"Telnet Server" check box**
  Enable or disable the "Telnet Server" service for unencrypted access to the CLI.
- **"SSH Server" check box**
  Enable or disable the "SSH Server" service for encrypted access to the CLI.
- **"HTTPS Server only" check box**
  Enable or disable access using HTTPS.
- **"DCP Server"** drop-down list
  Specify whether or not the device can be accessed with DCP (Discovery and Configuration Protocol):
  - "-" (disabled)
    DCP is disabled. Device parameters can neither be read nor modified.
  - Read/Write
    With DCP, device parameters can be both read and modified.
  - Read-Only
    With DCP, device parameters can be read but cannot be modified.

- **"SNMP" drop-down list:**
  Select the protocol from the drop-down list. The following settings are possible:
  - "-" (SNMP disabled)
    Access to device parameters via SNMP is not possible.
  - SNMPv1/v2c/v3
    Access to device parameters is possible with SNMP versions 1, 2c or 3. You can configure other settings in "System > SNMP > General".
  - SNMPv3
    Access to device parameters is possible with SNMP version 3. You can configure other settings in "System > SNMP > General".
- **"SNMPv1/v2 Read-Only"** check box
  Enable or disable write access to SNMP variables with SNMPv1/v2c.
- "**SINEMA Configuration Interface**" check box
  If the SINEMA configuration interface is enabled, you can download configurations to the device via the TIA Portal.

5.3.1.5 Antenna Settings

Introduction

On this Basic Wizard page, you configure the settings for the external antenna.



Basic Wizard: Antenna Settings

On this page, you select the type of external antenna connected to the device. If you terminate an antenna connection using a 50 ohm resistor, select the entry 'Not used (Connect 50 Ohm Termination)'. If the type of external antenna is not available, select the 'User defined' entry and enter the antenna gain for each frequency band manually. Enter the length of flexible antenna connecting cable in meters between the device and the external antenna. An attenuation of 0.6 dB is assumed per meter. Also enter the attenuation caused by other elements, e.g. power splitters, where applicable.

Connector	Antenna Type	Antenna Gain 2.4 GHz [dBi]	Antenna Gain 5 GHz [dBi]	Cable Length [m]	Additional Attenuation [dB]
R1 A1	ANT795-6MT	5	7	1	0
R1 A2	ANT795-6MT	5	7	1	0
R1 A3	ANT795-6MT	5	7	1	0
R2 A1	Not defined	-	-	-	-
R2 A2	Not defined	-	-	-	-
R2 A3	Not defined	-	-	-	-

Description

This table contains the following columns:

- **Connector**
  Shows the name of the relevant antenna connection.
- **Antenna Type**
  Select the type of external antenna connected to the device. If the type of your antenna is not available, select the entry "User defined".

  Connectors that are not used must have a 50 Ω terminating resistor fitted. Select the entry "Not used (connect 50 Ohms Termination)".

  Note

  50 Ω terminating resistor

  Each WLAN interface has three antenna connectors. The antennas R1A1 and R2A1 must be always be connected as soon as the associated WLAN Interface is turned on. If no antenna is connected, the relevant interface must also be disabled for RX and TX. Otherwise, there may be transmission disruptions.

- **Antenna Gain**
  If you select the "User-defined" entry for the "Antenna Type", enter the antenna gain manually in the "dB" unit.
  - Antenna Gain 2.4 GHz [dBi]
    Here, enter the antenna gain the antenna has in the 2.4 GHz frequency band.
  - Antenna Gain 5 GHz [dBi]
    Here, enter the antenna gain the antenna has in the 5 GHz frequency band.
- **Cable length [m]**
  Enter the length of the flexible antenna connecting cable in meters between the device and the external antenna.
- **Additional Attenuation [dB]**
  Here, specify the additional attenuation caused, for example, by an additional splitter.

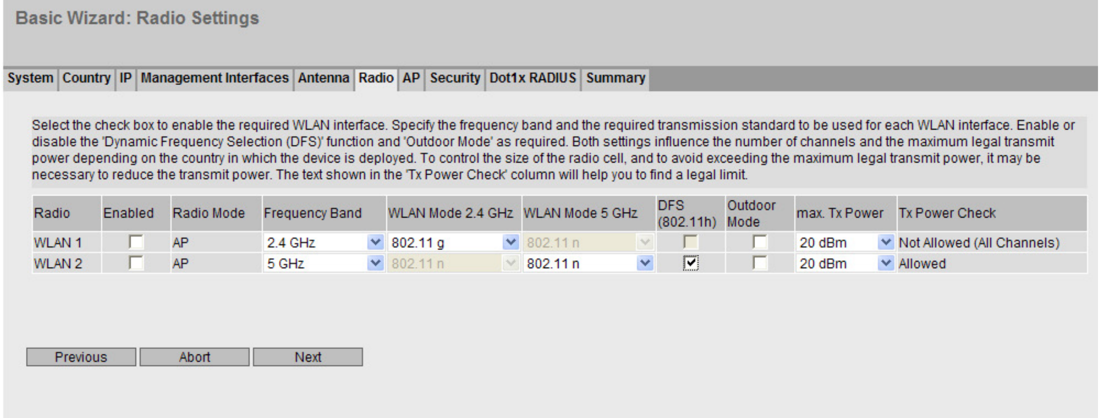
  Note

  If you use other WLAN interfaces, make sure that you have adequate channel spacing.

5.3.1.6 Radio Settings

Introduction

On this Basic Wizard page, you specify the configuration for the WLAN interfaces.



Select the check box to enable the required WLAN interface. Specify the frequency band and the required transmission standard to be used for each WLAN interface. Enable or disable the 'Dynamic Frequency Selection (DFS)' function and 'Outdoor Mode' as required. Both settings influence the number of channels and the maximum legal transmit power depending on the country in which the device is deployed. To control the size of the radio cell, and to avoid exceeding the maximum legal transmit power, it may be necessary to reduce the transmit power. The text shown in the 'Tx Power Check' column will help you to find a legal limit.

Radio	Enabled	Radio Mode	Frequency Band	WLAN Mode 2.4 GHz	WLAN Mode 5 GHz	DFS (802.11h)	Outdoor Mode	max. Tx Power	Tx Power Check
WLAN 1	□	AP	2.4 GHz	802.11 g	802.11 n	□	□	20 dBm	Not Allowed (All Channels)
WLAN 2	□	AP	5 GHz	802.11 n	802.11 n	☑	□	20 dBm	Allowed

Description

This table contains the following columns:

- **Radio**
  Shows the available WLAN interfaces.
- **Enabled**
  Enable or disable the WLAN interface. The WLAN interfaces are disabled when the device is supplied.
- **Radio Mode**
  Shows the mode of the WLAN interface.
- **Frequency Band**
  Specify the frequency band. In client mode, dual-frequency operation is also possible.

  Note

  Configuring WLAN interfaces of the W786-2IA RJ-45 for different frequency bands

  If both WLAN interfaces are configured for the same frequency band on this device, there may be mutual influence or interference. This applies in particular when there is a high data throughput.

- **WLAN Mode**
  Select the required transmission standard for the configured frequency band.
  - WLAN Mode 2.4 GHz
    Specify the transmission standard for the 2.4 GHz frequency band. The selection depends on the country setting.
  - WLAN Mode 5 GHz
    Specify the transmission standard for the 5 GHz frequency band. The selection depends on the country setting.

- **DFS (802.11h)**
  - Enabled
    If the access point discovers a disruption on the current channel, for example due to a primary user, it automatically switches to an alternative channel. You specify the alternative channel on the "AP Settings" Basic Wizard page. DFS is also the requirement for the use of certain wireless channels. This can only be enabled in the 5 GHz band.
  - Disabled
    The DFS function is not used.
- **Outdoor Mode**
  - Enabled
    In outdoor mode, the selection of country-dependent channels and the transmit power for operation are extended for outdoor use.
  - Disabled
    The device is being operated in indoor mode. In indoor mode, the selection of country-dependent channels and the transmit power for operation in a building are restricted.
- **max. Tx Power**
  Specify the transmit power of the device. It may be necessary to reduce the transmit power when using antennas to avoid exceeding the maximum legal transmit power. Reducing the transmit power effectively reduces cell size

Note

The maximum possible transmit power varies depending on the channel and data rate. For more detailed information on transmit power, refer to the documentation "Characteristics radio interface".

Note

If both interfaces of access points with two WLAN interfaces are operated in the same frequency range, this may cause wireless interference on one or both interfaces at a transmit power higher than 15 dBm.

- **Tx Power Check**
  Indicates whether the settings that have been made will violate the permitted transmit power restrictions of the selected country. The following parameters influence this calculation:
  max. Tx Power, Antenna Gain, Additional Attenuation.
  The following displays can appear:
  - Allowed
    The channels can be used with the current settings.
  - Not Allowed (Some Channels)
    Among the channels, there are some on which the current transmit power exceeds the maximum permitted transmit power.
  - Not Allowed (All Channels)
    No permitted operation is possible. The transmit power is too high.
  - Controlled automatically by iREF
    The transmit power is set by the "iREF" function.

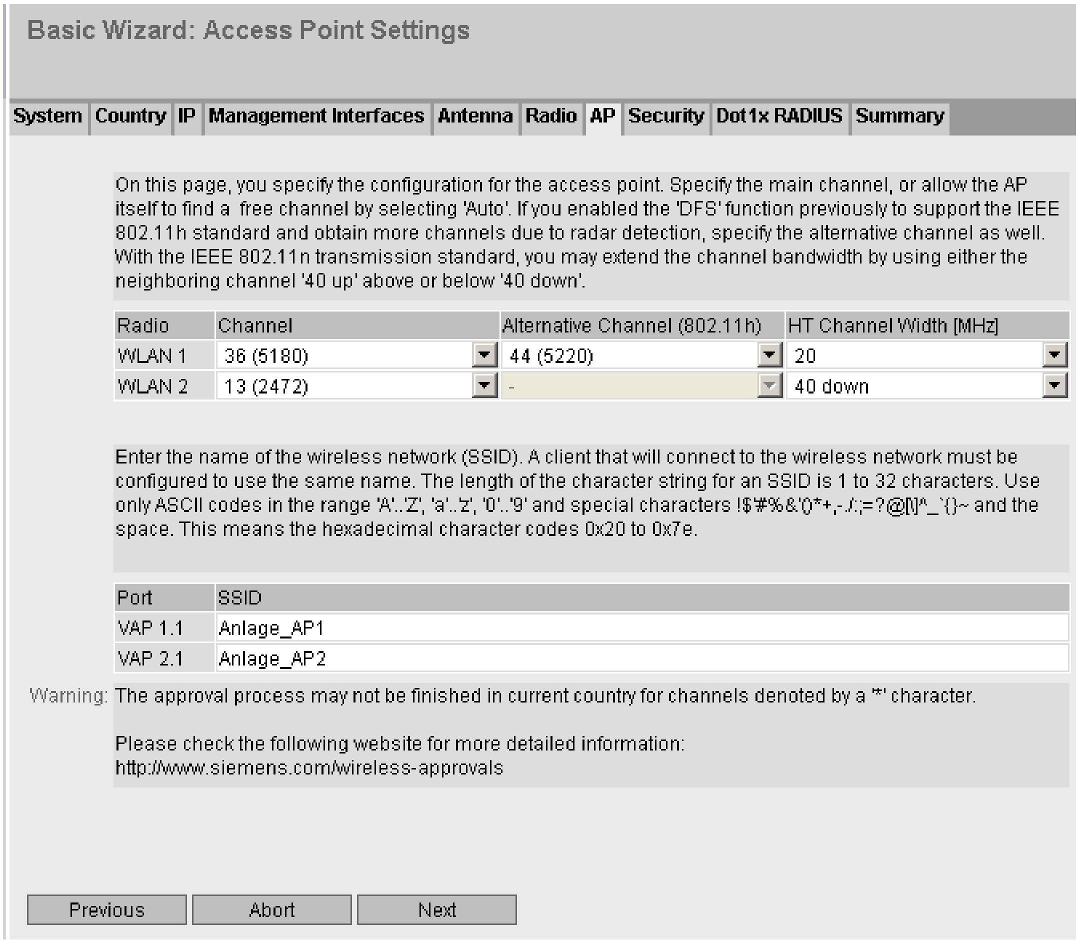
5.3.1.7 Access Point Settings

Introduction

On this Basic Wizard page, you specify the configuration for the Access Point .

Note

This page is available only in access point mode.



Basic Wizard: Access Point Settings

On this page, you specify the configuration for the access point. Specify the main channel, or allow the AP itself to find a free channel by selecting 'Auto'. If you enabled the 'DFS' function previously to support the IEEE 802.11h standard and obtain more channels due to radar detection, specify the alternative channel as well. With the IEEE 802.11n transmission standard, you may extend the channel bandwidth by using either the neighboring channel '40 up' above or below '40 down'.

Radio	Channel	Alternative Channel (802.11h)	HT Channel Width [MHz]
WLAN 1	36 (5180)	44 (5220)	20
WLAN 2	13 (2472)	-	40 down

Enter the name of the wireless network (SSID). A client that will connect to the wireless network must be configured to use the same name. The length of the character string for an SSID is 1 to 32 characters. Use only ASCII codes in the range 'A'..'Z', 'a'..'z', '0'..'9' and special characters !$'#%&'()*+,-./:;=?@[\]^_`{}~ and the space. This means the hexadecimal character codes 0x20 to 0x7e.

Port	SSID
VAP 1.1	Anlage_AP1
VAP 2.1	Anlage_AP2

Warning: The approval process may not be finished in current country for channels denoted by a '*' character.

Please check the following website for more detailed information:
http://www.siemens.com/wireless-approvals

Description

Table 1 contains the following columns:

- **Radio**
  Shows the available WLAN interfaces.
- **Channel**
  Specify the main channel. If you want the access point to search for a free channel itself, use "Auto". If you want to use a fixed channel, select the required channel from the drop-down list.

- **Alternative Channel (802.h)**
  If you have enabled the "DFS" function on the Basic Wizard page "Radio Settings", specify the alternative channel here. If you want the access point to search for a free channel itself, use "Auto". If you want to use a fixed channel, select the required channel from the drop-down list.
- **HT Channel Width [MHz]**
  You can specify the channel bandwidth with the IEEE 802.11n transmission standard. The following settings are possible.
  - 20
    Channel bandwidth 20 MHz
  - 40 up
    Channel bandwidth 40 MHz. The configured channel and the neighboring channel above it are used.
  - 40 down
    Channel bandwidth 40 MHz. The configured channel and the neighboring channel below it are used.

Table 2 contains the following columns:

- **Port**
  Shows the first VAP interface per WLAN interface.
- **SSID**
  Enter the SSID. The length of the character string for SSID it is 1 to 32 characters.
  The ASCII code 0x20 to 0x7e is used for the SSID.
  After completing the Basic Wizard, you can define further SSIDs with "Interfaces > WLAN > AP".

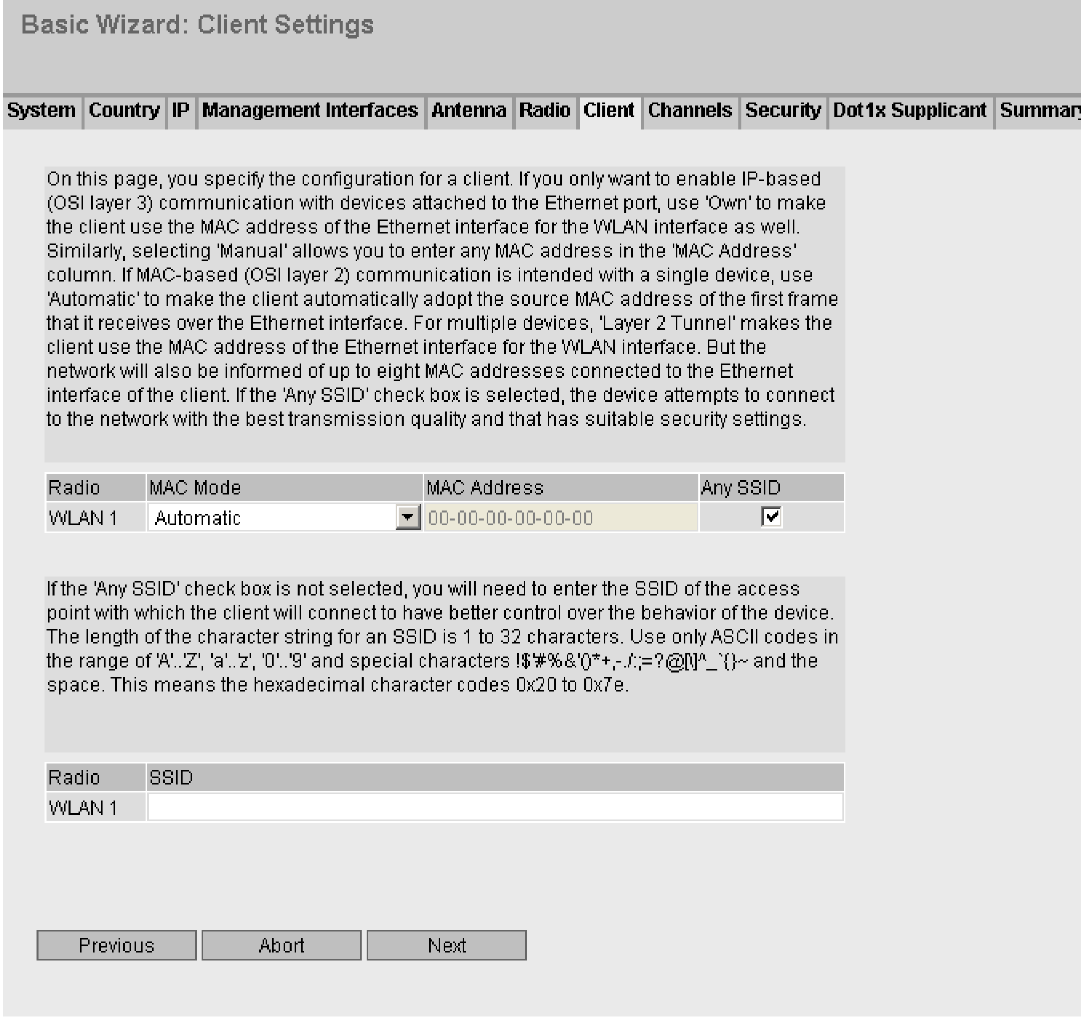
5.3.1.8 Client Settings

Introduction

On this Basic Wizard page, you specify the configuration for clients, for example the assignment of the MAC address.

Note

This page is only available in client mode.



Basic Wizard: Client Settings

On this page, you specify the configuration for a client. If you only want to enable IP-based (OSI layer 3) communication with devices attached to the Ethernet port, use 'Own' to make the client use the MAC address of the Ethernet interface for the WLAN interface as well. Similarly, selecting 'Manual' allows you to enter any MAC address in the 'MAC Address' column. If MAC-based (OSI layer 2) communication is intended with a single device, use 'Automatic' to make the client automatically adopt the source MAC address of the first frame that it receives over the Ethernet interface. For multiple devices, 'Layer 2 Tunnel' makes the client use the MAC address of the Ethernet interface for the WLAN interface. But the network will also be informed of up to eight MAC addresses connected to the Ethernet interface of the client. If the 'Any SSID' check box is selected, the device attempts to connect to the network with the best transmission quality and that has suitable security settings.

Radio	MAC Mode	MAC Address	Any SSID
WLAN 1	Automatic	00-00-00-00-00-00	☑

If the 'Any SSID' check box is not selected, you will need to enter the SSID of the access point with which the client will connect to have better control over the behavior of the device. The length of the character string for an SSID is 1 to 32 characters. Use only ASCII codes in the range of 'A'..'Z', 'a'..'z', '0'..'9' and special characters !$'#%&'()*+,-./:;=?@[\]^_`{}~ and the space. This means the hexadecimal character codes 0x20 to 0x7e.

Radio	SSID
WLAN 1	

Description

Table 1 contains the following columns:

- **Radio**
  Shows the available WLAN interfaces.
- **MAC Mode**
  Specify how the MAC address is assigned to the client. The following are possible:
  - Automatic
    The client automatically adopts the source MAC address of the first frame that it receives over the Ethernet interface.
  - Manual
    If you select "Manual", enter the MAC address in the "MAC Address" column.
  - Own
    The client uses the MAC address of the Ethernet interface for the WLAN interface.
  - Layer 2 Tunnel
    The client uses the MAC address of the Ethernet interface for the WLAN interface. The network is also informed of the MAC addresses connected to the Ethernet interface of the client. Up to eight MAC addresses can be used.
- **MAC Address**
  Enter the MAC address of the client. The input box can only be edited if you have set "Manual" for the "MAC Mode".
- **Any SSID**
  - Enabled
    In client mode, the device attempts to connect to the network with the best transmission quality and that has suitable security settings.
  - Disabled
    The client attempts to connect to the network from the SSID list that has the best transmission quality.

Table 2 contains the following columns:

- **Radio**
  Shows the available WLAN interfaces.
- **SSID**
  Enter the SSID of the access point with which the client connects. In the Basic Wizard, you can only specify one SSID. After completing the Basic Wizard, you can define further SSIDs with "Interfaces > WLAN > Client".

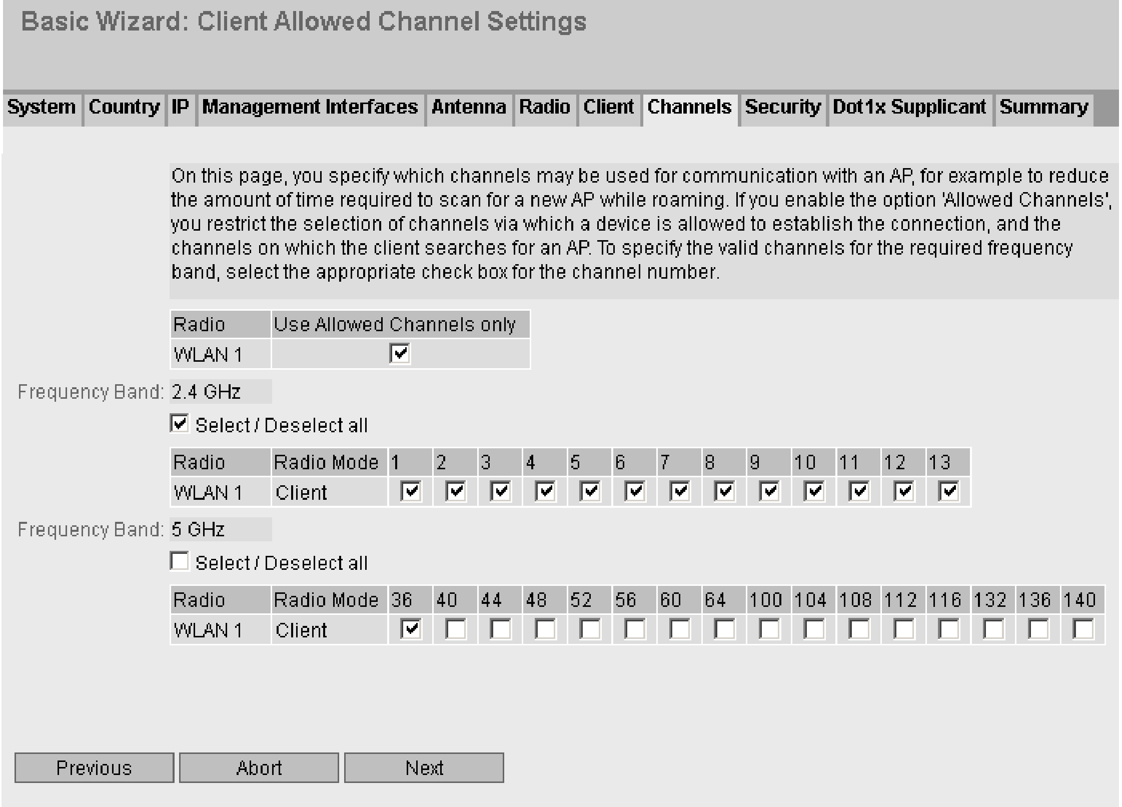
5.3.1.9 Client Allowed Channel Settings

Introduction

For communication, a specific channel within a frequency band is used. On this page, you can either set this channel specifically or configure so that the channel is selected automatically.

Note

This page is only available in client mode.



On this page, you specify which channels may be used for communication with an AP, for example to reduce the amount of time required to scan for a new AP while roaming. If you enable the option 'Allowed Channels', you restrict the selection of channels via which a device is allowed to establish the connection, and the channels on which the client searches for an AP. To specify the valid channels for the required frequency band, select the appropriate check box for the channel number.

Radio	Use Allowed Channels only
WLAN 1	☑

Frequency Band: 2.4 GHz

☑ Select / Deselect all

Radio	Radio Mode	1	2	3	4	5	6	7	8	9	10	11	12	13
WLAN 1	Client	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Frequency Band: 5 GHz

□ Select / Deselect all

Radio	Radio Mode	36	40	44	48	52	56	60	64	100	104	108	112	116	132	136	140
WLAN 1	Client	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Description

Table 1 contains the following columns:

- **Radio**
  Shows the available WLAN interfaces.
- **Use Allowed Channels only**
  If you enable the option, you restrict the selection of channels via which the client is allowed to establish the connection.
  In the following tables, you define the channels on which the client searches for an AP. The tables are divided up according to frequency bands.

If the option is disabled, the channels available based on the settings (country code, antennas, transmit power etc.) are used.

Above the tables for the frequency bands, you will find the following check box:

- **Select / Deselect all**
  - Enabled
    If you enable the check box, all channels are selected.
  - Disabled
    If you deselect the check box, only the first valid channel of the frequency band remains enabled.

The tables of the frequency bands have the following columns:

- **Radio**
  Shows the available WLAN interfaces in this column.
- **Radio Mode**
  Shows the mode of the device.
- **Channel number**
  To specify the valid channels for the required frequency band, select the appropriate check box for the channel number.
  The table displays the permitted channels of the country. Only the valid channels can be enabled. Invalid channels are grayed out and cannot be enabled.

Note

To specify the channels, the setting "Use Allowed Channels only" must be enabled.

5.3.1.10 Security Settings

Introduction

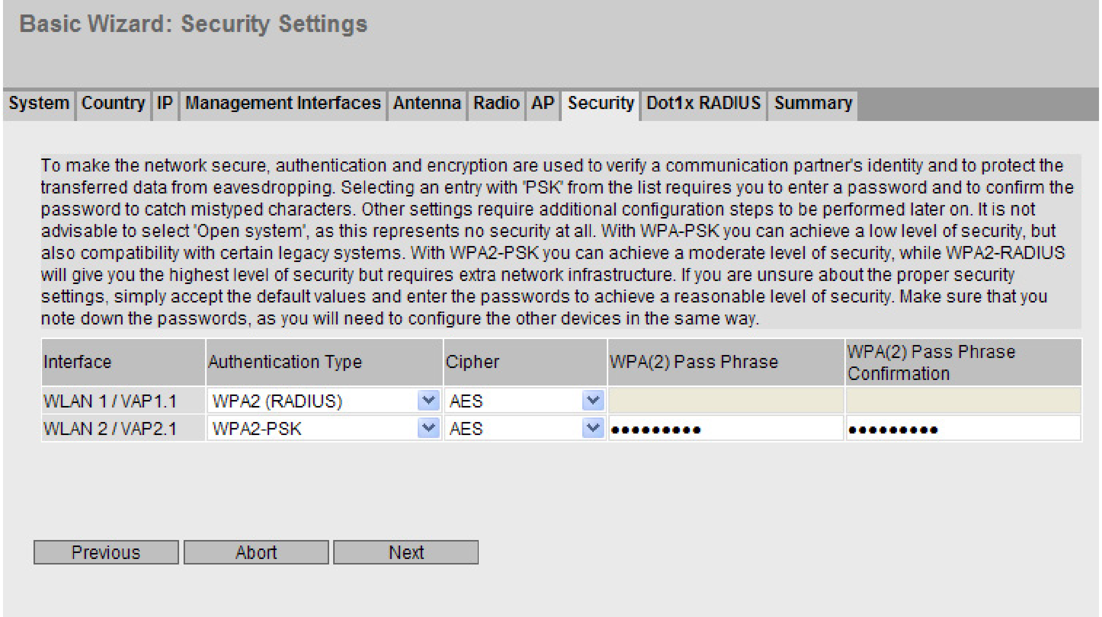
To make the network secure, authentication and encryption are used. You specify the security levels with the type of authentication and the encryption procedure.

Note

If "AUTO" or "802.11n" or "802.11 n only is set for WLAN Mode "AUTO", only the authentication types Open System, WPA2 (RADIUS), WPA2-PSK can be set.

Use WPA2/AES, to prevent misuse of a password WPA2 (RADIUS) / WPA2-PSK with AES provides the greatest security. You will find further information on security in the configuration manual under "Instructions for secure network design".

The security settings on both devices must match to allow a client to communicate with an access point.



To make the network secure, authentication and encryption are used to verify a communication partner's identity and to protect the transferred data from eavesdropping. Selecting an entry with 'PSK' from the list requires you to enter a password and to confirm the password to catch mistyped characters. Other settings require additional configuration steps to be performed later on. It is not advisable to select 'Open system', as this represents no security at all. With WPA-PSK you can achieve a low level of security, but also compatibility with certain legacy systems. With WPA2-PSK you can achieve a moderate level of security, while WPA2-RADIUS will give you the highest level of security but requires extra network infrastructure. If you are unsure about the proper security settings, simply accept the default values and enter the passwords to achieve a reasonable level of security. Make sure that you note down the passwords, as you will need to configure the other devices in the same way.

Interface	Authentication Type	Cipher	WPA(2) Pass Phrase	WPA(2) Pass Phrase Confirmation
WLAN 1 / VAP1.1	WPA2 (RADIUS)	AES		
WLAN 2 / VAP2.1	WPA2-PSK	AES	●●●●●●●●●	●●●●●●●●●

Description

This table contains the following columns:

- **Interface**
  Shows the interface to which the settings relate.
- **Authentication Type**
  Select the type of authentication.

Note

IEEE 802.11n devices

With devices according to the IEEE 802.11n standard, only WPA2 encryption is possible.

- Open System
  Without authentication
- WPA-PSK
  WPA authentication with WPA key. Enter the WPA key in "WPA(2) Pass phrase".
- WPA (RADIUS)
  WPA authentication with RADIUS server. You configure the access data on the next Basic Wizard page.
- WPA2-PSK
  WPA2 authentication with WPA2 key. Enter the WPA2 key in "WPA(2) Pass phrase".
- WPA2 (RADIUS)
  WPA2 authentication with RADIUS server. You configure the access data on the next Basic Wizard page.

- **Cipher**
  Select the encryption method.
  - AUTO
    AES or TKIP is used depending on the capability of the other station.
  - TKIP (Temporal Key Integrity Protocol)
    A symmetrical encryption method with the RC4 algorithm (Ron's Code 4). In contrast to the weak WEP encryption, TKIP uses changing keys derived from a main key. TKIP can also recognize corrupted data frames.
  - AES (Advanced Encryption Standard)
    Strong symmetrical block encryption method based on the Rijndael algorithm that further improves the functions of TKIP.
- **WPA(2) Pass Phrase**
  Enter a WPA(2) key. The key can be 8 to 63 ASCII characters or exactly 64 hexadecimal characters long. This WPA(2) key must be known on both the client and the access point and is entered by the user at both ends.

Note

The WPA(2) key can be 8 to 63 ASCII characters or exactly 64 hexadecimal characters long. It should be selected so that is complex for example consisting of random numbers, letters (upper-/lowercase), have few repetitions and special characters. Do not use known names, words or terms that could be guessed. If a device is lost or if the key becomes known, change the key on all devices to maintain security.

- **WPA(2) Pass Phrase Confirmation**
  Confirm the entered WPA(2) key.

5.3.1.11 Dot1x Supplicant Settings

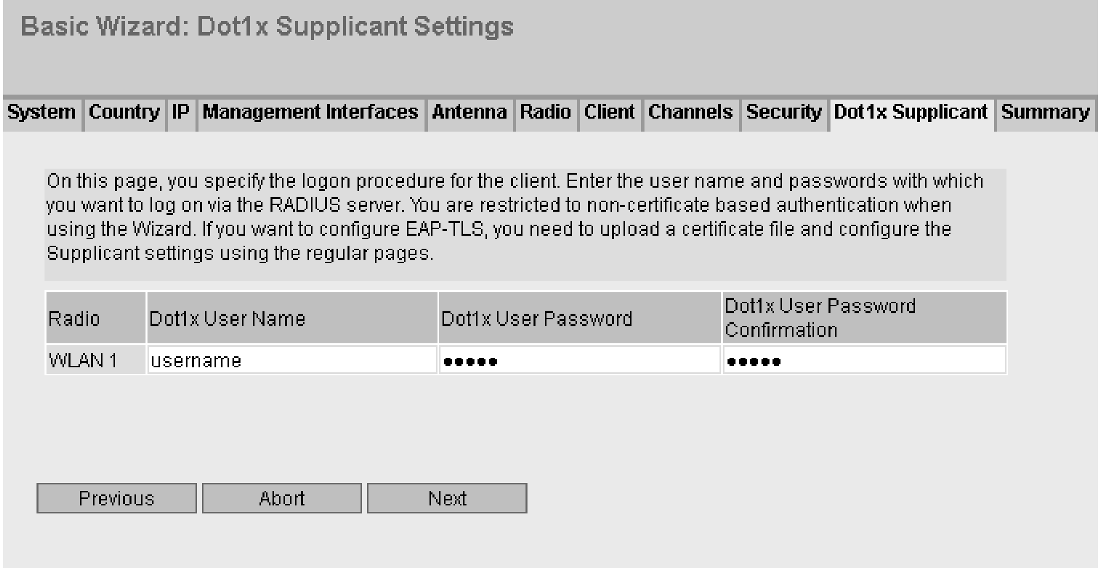
Introduction

On this Basic Wizard page, you configure the user name and the password with which the client will be logged on with the RADIUS server.

If you require additional authentication methods, you can configure them after completing the Basic Wizard with "Security > WLAN > Client Radius Supplicant".

Note

This page is only available in client mode.



On this page, you specify the logon procedure for the client. Enter the user name and passwords with which you want to log on via the RADIUS server. You are restricted to non-certificate based authentication when using the Wizard. If you want to configure EAP-TLS, you need to upload a certificate file and configure the Supplicant settings using the regular pages.

Radio	Dot1x User Name	Dot1x User Password	Dot1x User Password Confirmation
WLAN 1	username	●●●●●	●●●●●

Description

Table 1 contains the following columns:

- **Radio**
  Shows the available WLAN interfaces.
- **Dot1x User Name**
  Enter the user name with which the client will log on with the RADIUS server.
- **Dot1x User Password**
  Enter the password for the user name selected above. The client is logged on with the RADIUS server using this combination.
  For password assignment, ASCII code 0x20 to 0x7e is used.
- **Dot1x User Password Confirmation**
  Enter the password again in this input box.

5.3.1.12 Dot1x RADIUS Server Settings

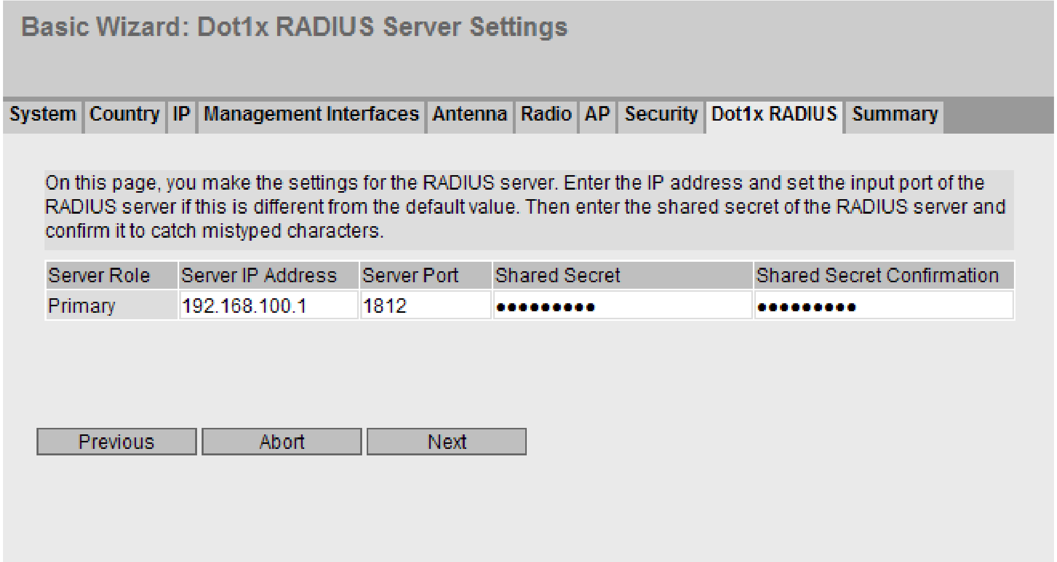
Introduction

On this Basic Wizard page, you configure the settings for the primary RADIUS Server.

After completing the Basic Wizard, you can configure a backup server and other settings, for example the number of logon attempts with "Security > WLAN > AP Radius Authenticator".

Note

This page is available only in access point mode.



Basic Wizard: Dot1x RADIUS Server Settings

On this page, you make the settings for the RADIUS server. Enter the IP address and set the input port of the RADIUS server if this is different from the default value. Then enter the shared secret of the RADIUS server and confirm it to catch mistyped characters.

Server Role	Server IP Address	Server Port	Shared Secret	Shared Secret Confirmation
Primary	192.168.100.1	1812	●●●●●●●●●	●●●●●●●●●

Description

This table contains the following columns:

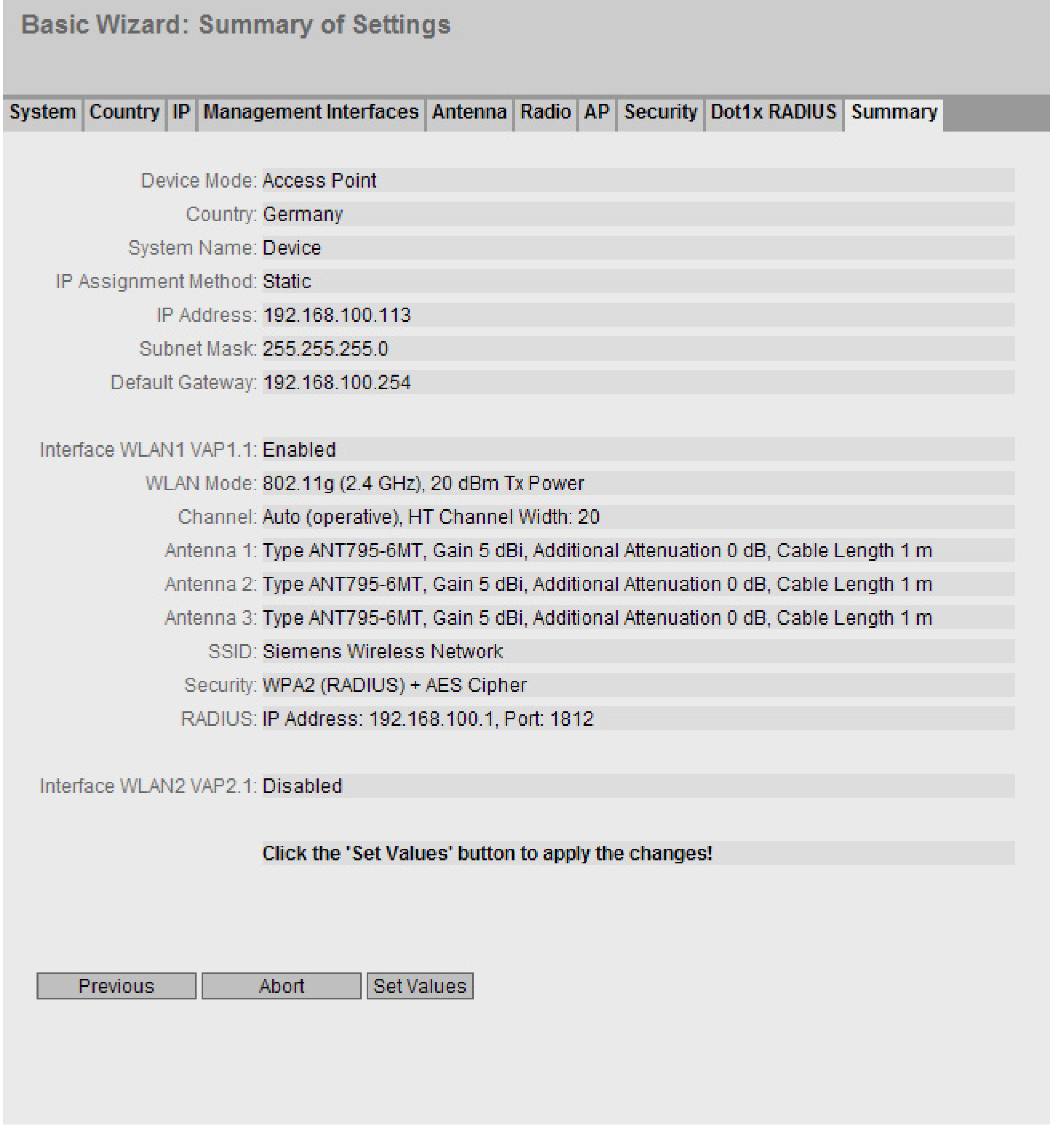
- **Server Role**
  Shows the role of the server.
- **Server IP Address**
  Enter the IP address of the RADIUS server. The use of the computer name (name resolution using DNS) instead of the IP address is not supported.
- **Server Port**
  Enter the port of the RADIUS server.
- **Shared Secret**
  Enter the password of the RADIUS server.
- **Shared Secret Confirmation**
  Enter the password again in this input box.

5.3.1.13 Summary of Settings

Introduction

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

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



Basic Wizard: Summary of Settings

Device Mode: Access Point

Country: Germany

System Name: Device

IP Assignment Method: Static

IP Address: 192.168.100.113

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.100.254

Interface WLAN1 VAP1.1: Enabled

WLAN Mode: 802.11g (2.4 GHz), 20 dBm Tx Power

Channel: Auto (operative), HT Channel Width: 20

Antenna 1: Type ANT795-6MT, Gain 5 dBi, Additional Attenuation 0 dB, Cable Length 1 m

Antenna 2: Type ANT795-6MT, Gain 5 dBi, Additional Attenuation 0 dB, Cable Length 1 m

Antenna 3: Type ANT795-6MT, Gain 5 dBi, Additional Attenuation 0 dB, Cable Length 1 m

SSID: Siemens Wireless Network

Security: WPA2 (RADIUS) + AES Cipher

RADIUS: IP Address: 192.168.100.1, Port: 1812

Interface WLAN2 VAP2.1: Disabled

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

Set Values

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

5.4 "Information" menu

5.4.1 Start Page

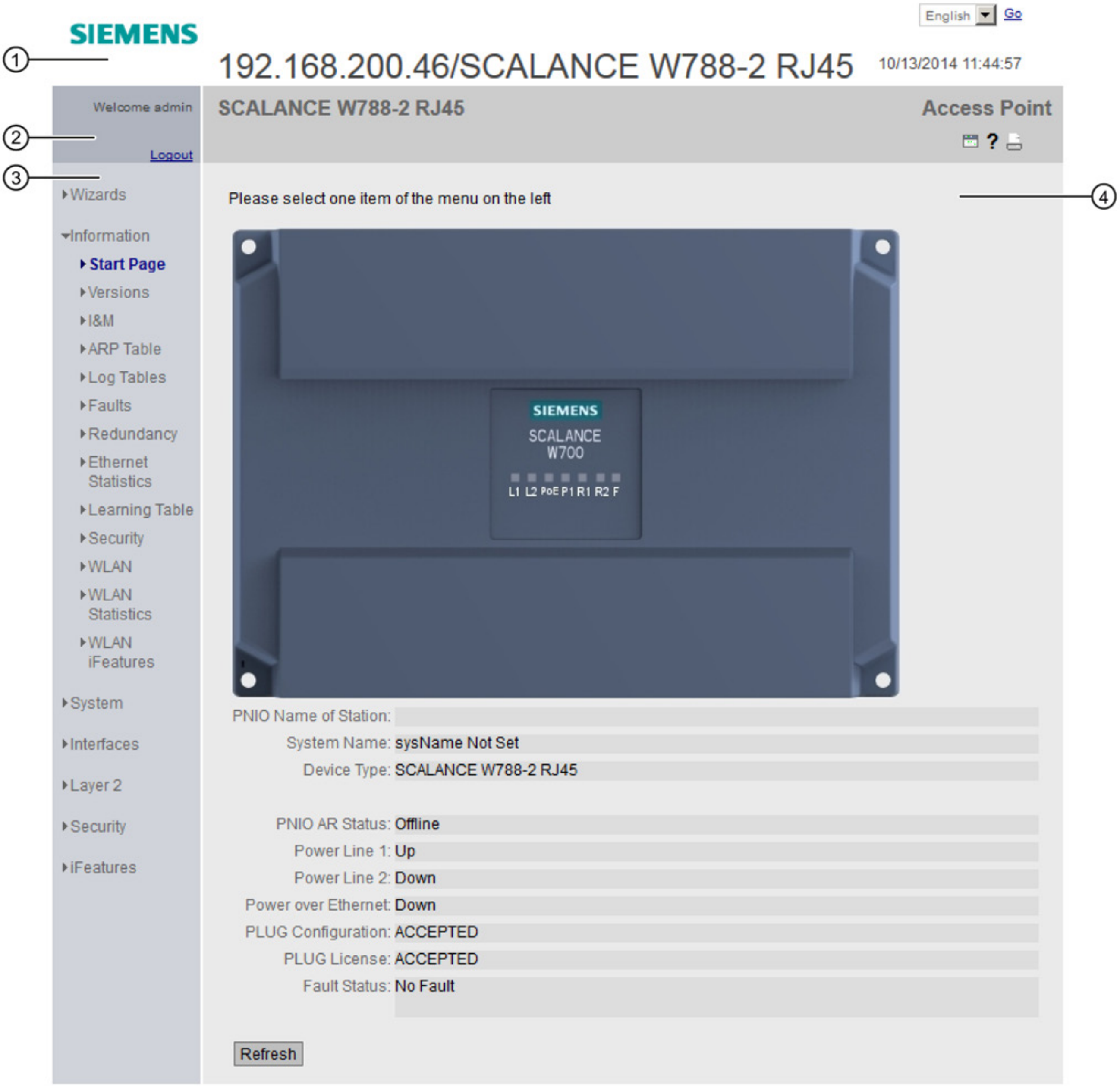
View of the Start page

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



Please select one item of the menu on the left

PNIO Name of Station:
System Name: sysName Not Set
Device Type: SCALANCE W788-2 RJ45

PNIO AR Status: Offline
Power Line 1: Up
Power Line 2: Down
Power over Ethernet: Down
PLUG Configuration: ACCEPTED
PLUG License: ACCEPTED
Fault Status: No Fault

Selection area (1)

The following is available in the selection area:

- Logo of Siemens AG

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

- **Mode**
  Shows whether the device is an access point or a client.
- **Printer** 🖶

  When you click this button, a pop-up window opens with a view of the page content optimized for the printer.
- **Help** ?

  When you click this button, the help page of the currently selected menu item is opened in a new browser window.
- **LED simulation**

  Each 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 compact operating instructions.

  If you click this button, you open the window for the LED simulation. You can show this window during a change of menu and move it as necessary. To close the LED simulation, click the close button in the LED simulation window.
- **Update on** On / **Update off** Off
  WBM pages with overview lists can also have the additional "Update" button

  With this button, you can enable or disable updating of the content area

  . If updating is turned on, the display is updated every 2 seconds

  To disable the update, click "On". Instead of "On", "Off" is displayed. As default, updating is always enabled on the WBM page.

Navigation area (3)

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

Content area (4)

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

The following is displayed below the picture of the device:

- PNIO Name of Station: PROFINET IO device name
- System Name: System name of the device
- Device Type: The type of the device
- PNIO AR Status: PROFINET IO application relation status
- Power Line1, Power Line2, Power over Ethernet: Status of the power supplies line 1 and line 2 or power over Ethernet. The power line 2 and power over Ethernet are only displayed if they are supported by the hardware. You will find further information on this in the compact operating instructions.
- PLUG configuration: Status of the configuration data on the PLUG
- PLUG license: Status of license on the PLUG
- Fault Status: Error status

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.

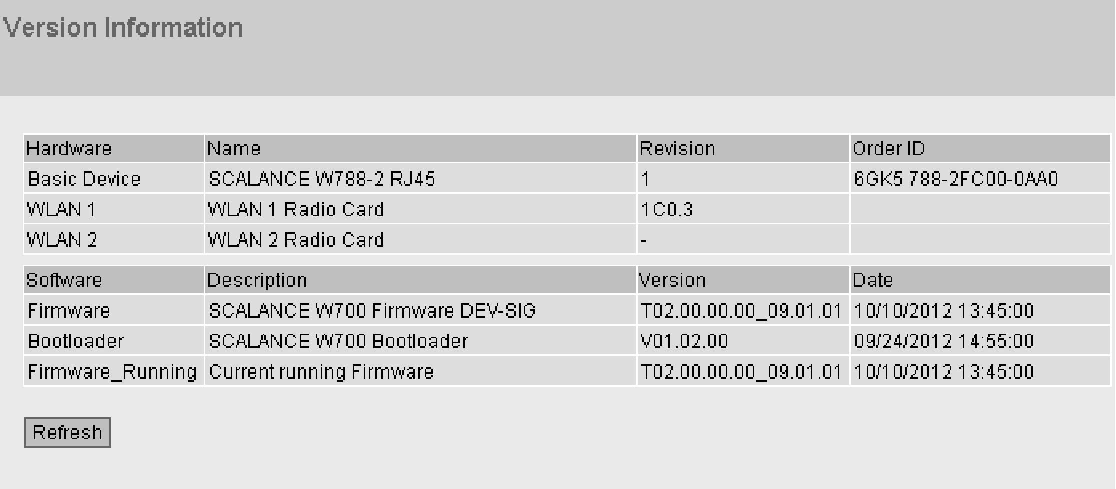
Logout

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

5.4.2 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 W788-2 RJ45	1	6GK5 788-2FC00-0AA0
WLAN 1	WLAN 1 Radio Card	1C0.3	
WLAN 2	WLAN 2 Radio Card	-	

Software	Description	Version	Date
Firmware	SCALANCE W700 Firmware DEV-SIG	T02.00.00.00_09.01.01	10/10/2012 13:45:00
Bootloader	SCALANCE W700 Bootloader	V01.02.00	09/24/2012 14:55:00
Firmware_Running	Current running Firmware	T02.00.00.00_09.01.01	10/10/2012 13:45:00

Description

Table 1 has the following columns:

- **Hardware**
  - Basic Device
    Shows the basic device
- **Name**
  Shows the name of the device or module.
- **Revision**
  Displays the hardware version of the device. For the wireless card, only one version is then displayed if the WLAN interface is enabled.
- **Order ID**
  Shows the order number of the device or module.

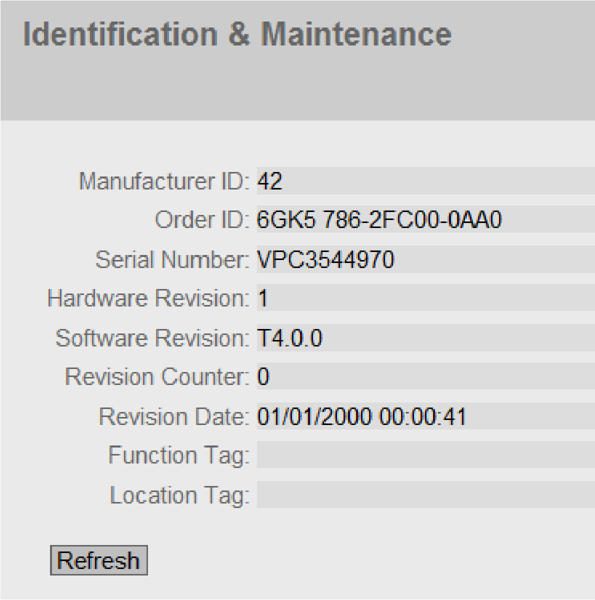
Table 2 has the following columns:

- **Software**
  - Firmware
    Shows the current firmware version. If a new firmware file was downloaded and the device has not yet restarted, the firmware version of the downloaded firmware file is displayed here. After the next restart, the downloaded firmware is activated and used.
  - Bootloader
    Shows the version of the boot software stored on the device.
  - Firmware_Running
    Shows the firmware version currently being used on the device.
- **Description**
  Shows the short description of the software.
- **Version**
  Shows the version number of the software version.
- **Date**
  Shows the date on which the software version was created.

5.4.3 I&M

Identification and maintenance data

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



Identification & Maintenance

Manufacturer ID: 42
Order ID: 6GK5 786-2FC00-0AA0
Serial Number: VPC3544970
Hardware Revision: 1
Software Revision: T4.0.0
Revision Counter: 0
Revision Date: 01/01/2000 00:00:41
Function Tag:
Location Tag:

Description of the displayed values

The table has the following rows:

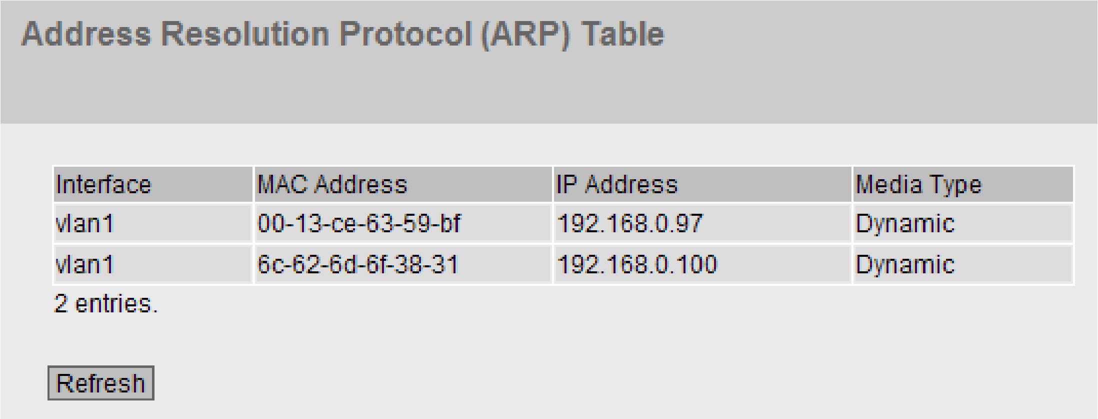
- **Manufacturer ID**
  Shows the manufacturer ID.
- **Order ID**
  Shows the order number.
- **Serial Number**
  Shows the serial number.
- **Hardware Revision**
  Shows the hardware version.
- **Software Revision**
  Shows the software version.
- **Revision Counter**
  As of firmware version 4.0, the value "0" is always shown here regardless of the version change.
- **Revision Date**
  Revision date: Date and time of the last revision

- **Function Tag**
  Shows the function tag (plant designation) of the device. The plant designation (HID) is created during configuration of the device with HW Config of STEP 7.
- **Location Tag**
  Shows the location tag (location identifier) of the device. The location identifier (LID) is created during configuration of the device with HW Config of STEP 7.

5.4.4 ARP Table

Assignment of MAC address and IP address

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



Address Resolution Protocol (ARP) Table

Interface	MAC Address	IP Address	Media Type
vlan1	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

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

    The addresses were entered as static addresses.

5.4.5 Log Tables

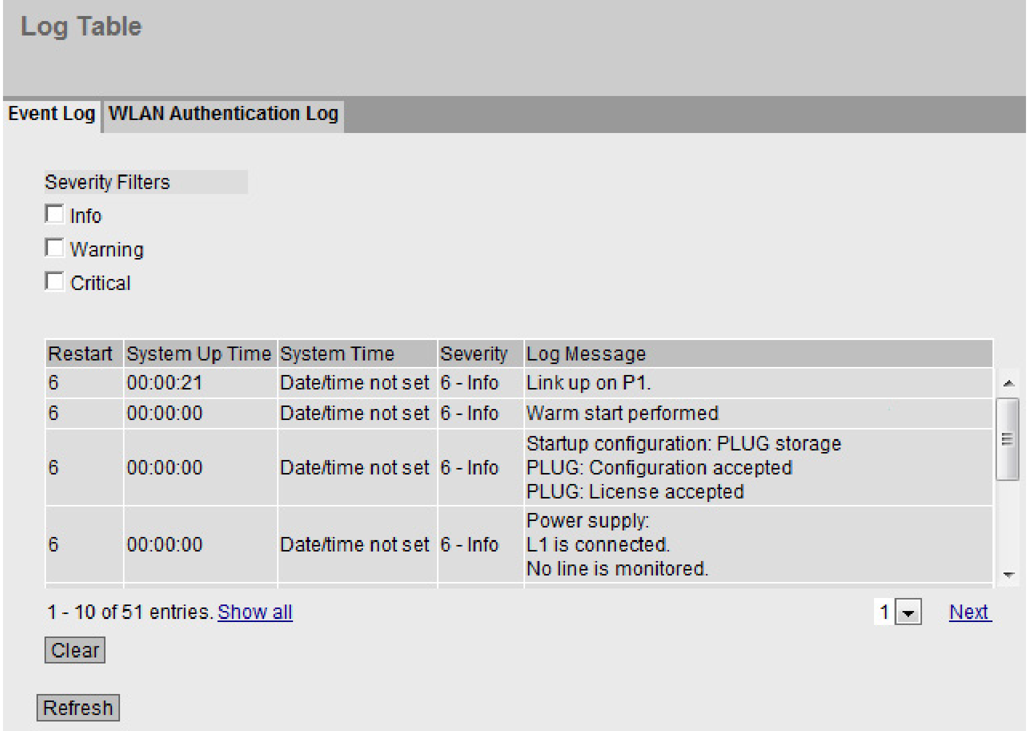
5.4.5.1 Events

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 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.



Restart	System Up Time	System Time	Severity	Log Message
6	00:00:21	Date/time not set	6 - Info	Link up on P1.
6	00:00:00	Date/time not set	6 - Info	Warm start performed
6	00:00:00	Date/time not set	6 - Info	Startup configuration: PLUG storage PLUG: Configuration accepted PLUG: License accepted
6	00:00:00	Date/time not set	6 - Info	Power supply: L1 is connected. No line is monitored.

1 - 10 of 51 entries.

Description

- **Severity Filters**
  You can filter the entries in the table according to severity. To display all the entries, enable or disable all parameters.
  - 6 - Info
    Informative
  - 4 - Warning
    Warnings
  - 2 - Critical
    Critical

The table has the following columns:

- **Restart**
  Counts the number of restarts since you last reset to factory settings and shows the device restart after which the corresponding event occurred.
- **System Up Time**
  Shows the time the device has been running since the last restart when the described event occurred.
- **System Time**
  Shows the date and time when the described event occurred.
- **Severity**
  Shows the severity of the message.
- **Log Message**
  Displays a brief description of the event that has occurred. You will find the list of possible messages in Appendix D of the configuration manual.

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 event 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.

"Show all" button

Click this button to display all the entries on the WBM page. Note that displaying all messages can take some time. The button only becomes active if there is more than one page.

"Next" button

Click this button to go to the next page. The button only becomes active if there is more than one page.

"Prev" button

Click this button to go to the previous page. The button only becomes active if there is more than one page.

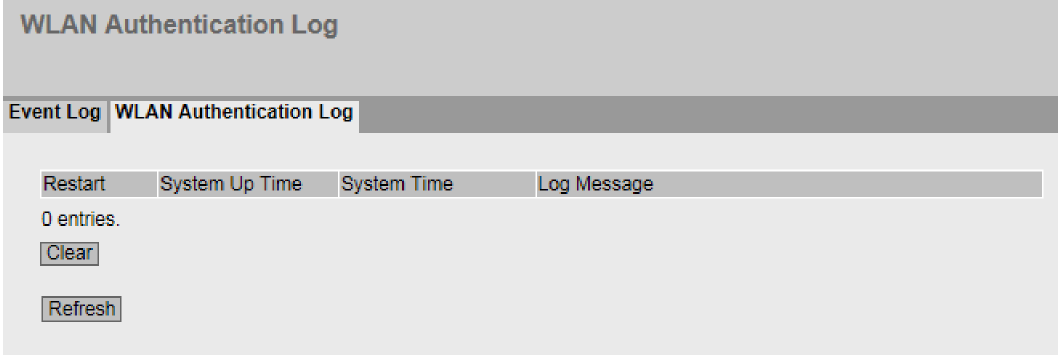
Drop-down list for page change

From the drop-down list, select the page you want to go to. This list only becomes active if there is more than one page.

5.4.5.2 WLAN Authentication Log

Logging authentication attempts

This page shows a table with information on successful or failed authentication attempts.



Restart	System Up Time	System Time	Log Message

0 entries.

You cannot configure anything on this page.

Description

The table has the following columns:

- **Restart**
  Counts the number of restarts since you last reset to factory settings and shows the device restart after which the corresponding event occurred.
- **System Up Time**
  Shows the time the device has been running since the last restart when the described fault occurred.
- **System Time**
  Shows the time at which the described error occurred.
- **Log Message**
  Displays a brief description of the event that has occurred. You will find the list of possible messages in Appendix D of the configuration manual.

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.

"Show all" button

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

"Next" button

Click this button to go to the next page.

"Prev" button

Click this button to go to the previous page.

Drop-down list for page change

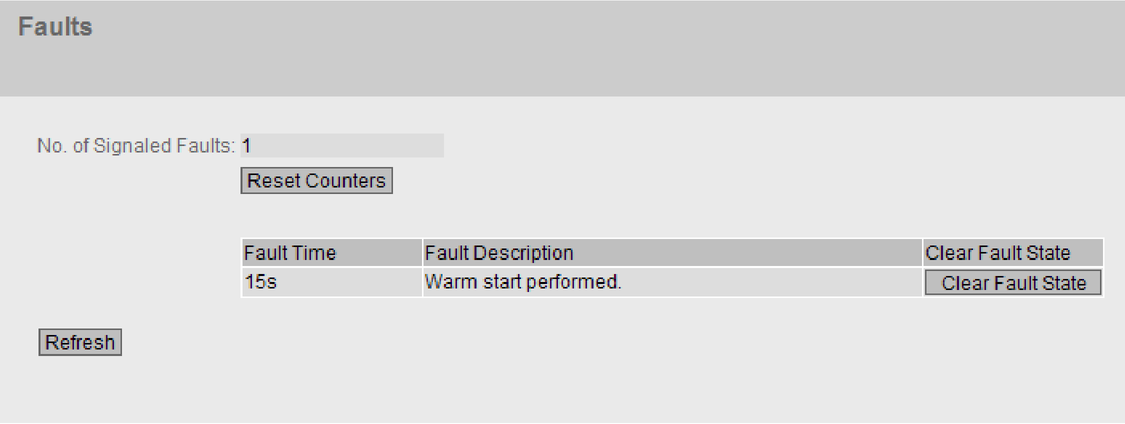
From the drop-down list, select the page you want to go to.

5.4.6 Faults

Error status

This page displays any errors that occur. Errors of the "Cold/Warm Start" event can be deleted following confirmation.
If there are no more unanswered error/fault messages, the fault LED goes off.

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



Faults

No. of Signaled Faults: 1

Fault Time	Fault Description	Clear Fault State
15s	Warm start performed.	Clear Fault State

Description

The page contains the following boxes:

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

The table contains the following columns:

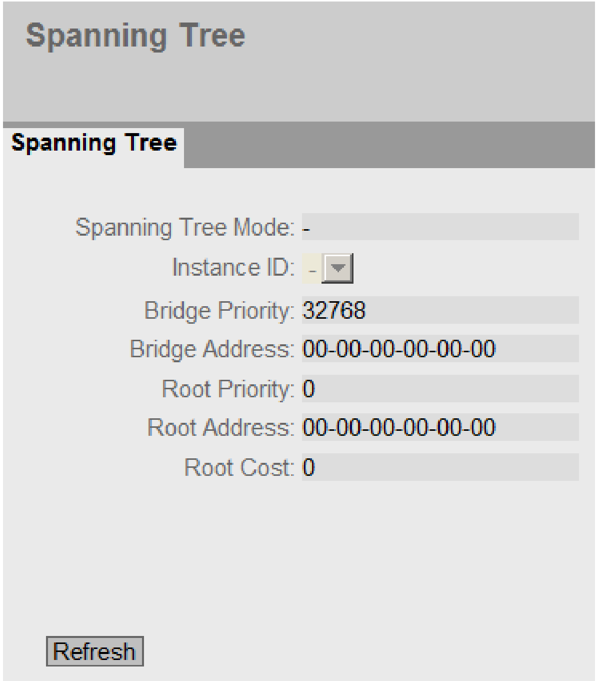
- **Fault Time**
  Shows the time the device has been running since the last restart when the described fault occurred.
- **Fault Description**
  Display of the fault status for the device.
- **Clear Fault State**
  To delete errors of the "Cold/Warm Start" event, click the Clear Fault State" button.

5.4.7 Redundancy

Introduction

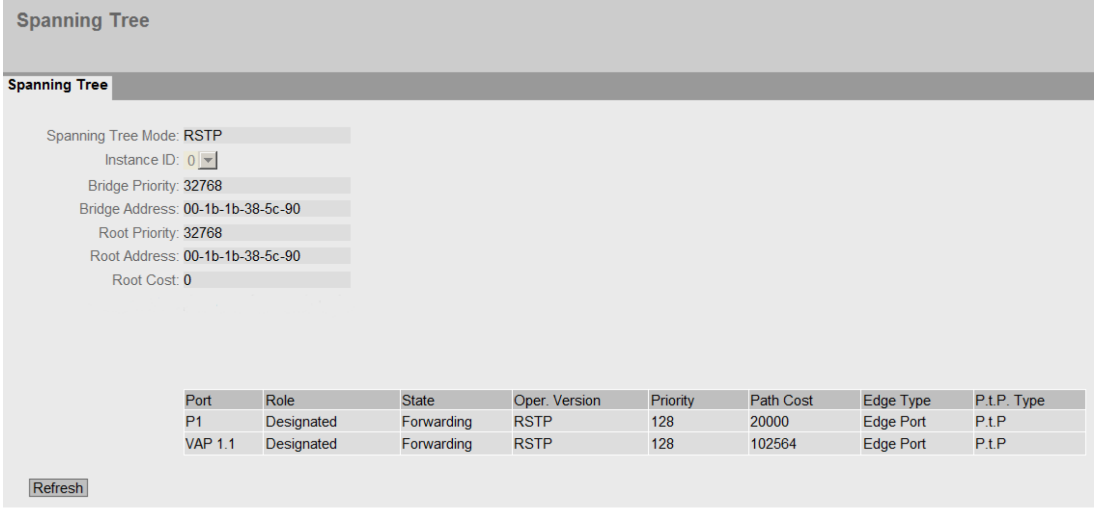
The page shows the current information about the Spanning Tree and the settings of the root bridge.

If Spanning Tree is turned off, only the basic information about this device is displayed.



Spanning Tree Mode: -
Instance ID: -
Bridge Priority: 32768
Bridge Address: 00-00-00-00-00-00
Root Priority: 0
Root Address: 00-00-00-00-00-00
Root Cost: 0

If Spanning Tree is turned on, the information about the status of the instance selected in the "Instance ID" drop-down list is displayed and the information about the configured ports is shown in the table. The information shown depends on the Spanning Tree mode.



Spanning Tree Mode: RSTP
Instance ID: 0
Bridge Priority: 32768
Bridge Address: 00-1b-1b-38-5c-90
Root Priority: 32768
Root Address: 00-1b-1b-38-5c-90
Root Cost: 0

Port	Role	State	Oper. Version	Priority	Path Cost	Edge Type	P.t.P. Type
P1	Designated	Forwarding	RSTP	128	20000	Edge Port	P.t.P
VAP 1.1	Designated	Forwarding	RSTP	128	102564	Edge Port	P.t.P

Description

The page contains the following boxes:

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

- **Root Cost**
  The path costs from this device to the root bridge.
- **Bridge Status**

  Shows the status of the bridge, e.g. whether or not the device is the root bridge.
- **Regional Root Priority** (only available with MSTP)
  For a description, see Bridge Priority / Root Priority
- **Regional Root Address** (only available with MSTP)
  Shows the MAC address of the device.
- **Regional Root Cost** (only available with MSTP)

  Shows the path costs from the regional root bridge to the root bridge.

The table contains the following boxes:

- **Port**
  Shows the port via which the device communicates.
- **Role**
  shows the status of the port. The following values are possible:
  - Disabled
    The port was removed manually from the spanning tree and will no longer be taken into account by the spanning tree.
  - Designated
    The ports leading away from the root bridge.
  - Alternate
    The port with an alternative route to a network segment
  - Backup
    If a switch has several ports to the same network segment, the "poorer" Port becomes the backup port.
  - Root
    The port that provides the best route to the root bridge.
  - Master
    This port points to a root bridge located outside the MST region.

- **State**
  Displays the current status of the port. The values are only displayed. The parameter depends on the configured protocol. The following statuses are possible:
  - Discarding
    The port receives BPDU frames. Other incoming or outgoing frames are discarded.
  - Listening
    The port receives and sends BPDU frames. The port is involved in the spanning tree algorithm. Other outgoing and incoming frames are discarded.
  - Learning
    The port actively learns the topology; in other words, the node addresses. Other outgoing and incoming frames are discarded.
  - Forwarding
    Following the reconfiguration time, the port is active in the network. The port receives and sends data frames.
- **Oper. Version**
  Describes the type of spanning tree in which the port operates
- **Priority**
  If the path calculated by the spanning tree is possible over several ports of a device, the port with the highest priority (in other words the lowest value for this parameter) is selected. A value between 0 and 240 can be entered for the priority in steps of 16. If you enter a value that cannot be divided by 16, the value is automatically adapted. The default is 128.
- **Path Cost**
  This parameter is used to calculate the path that will be selected. The path with the lowest value is selected as the route. If several ports of a device have the same value, the port with the lowest port number is selected.
  If the value in the "Cost Calc" box is "0", the automatically calculated value is displayed. Otherwise, the value of the "Cost Calc" box is displayed.
  The calculation of the path costs is largely based on the transmission speed. The higher the achievable transmission speed is, the lower the value of the path costs.

  Typical values for path costs with rapid spanning tree:
  - 10,000 Mbps = 2,000
  - 1000 Mbps = 20,000
  - 100 Mbps = 200,000
  - 10 Mbps = 2,000,000.

- **Edge Type**
  Shows the type of the connection. The following values are possible:
  - Edge Port
    An edge port is connected to this port.
  - No Edge Port
    There is a spanning tree or rapid spanning tree device at this port.
- **P.t.P. Type**
  shows the type of the point-to-point link. The following values are possible:
  - P.t.P.
    With half duplex, a point-to-point link is assumed.
  - Shared Media
    With a full duplex connection, a point-to-point link is not assumed.

Note

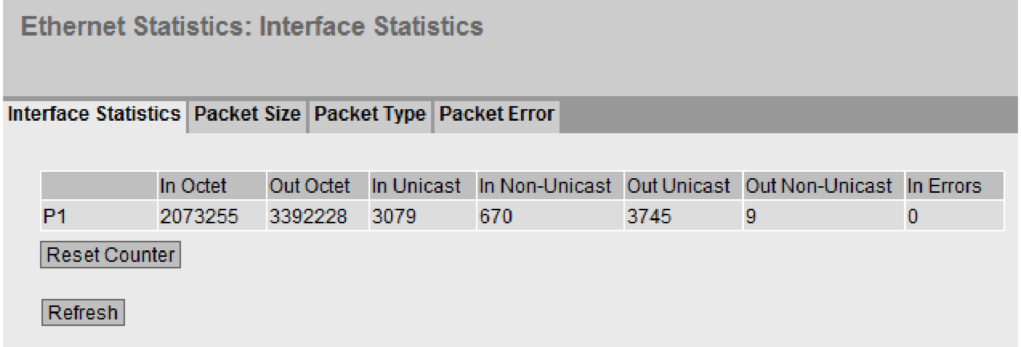
Point-to-point link means a direct connection between two devices. A shared media connection is, for example, a connection to a hub.

5.4.8 Ethernet Statistics

5.4.8.1 Interface statistics

Interface statistics

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


Ethernet Statistics: Interface Statistics

	In Octet	Out Octet	In Unicast	In Non-Unicast	Out Unicast	Out Non-Unicast	In Errors
P1	2073255	3392228	3079	670	3745	9	0

Figure 5-1 Interface statistics

Displayed values

The table has the following columns:

- **In Octet**

  Shows the number of received bytes.
- **Out Octet**

  Shows the number of sent bytes.
- **In Unicast**

  Shows the number of received unicast frames.
- **In Non-Unicast**

  Shows the number of received frames that are not of the type unicast.
- **Out Unicast**

  Shows the number of sent unicast frames.
- **Out Non-Unicast**

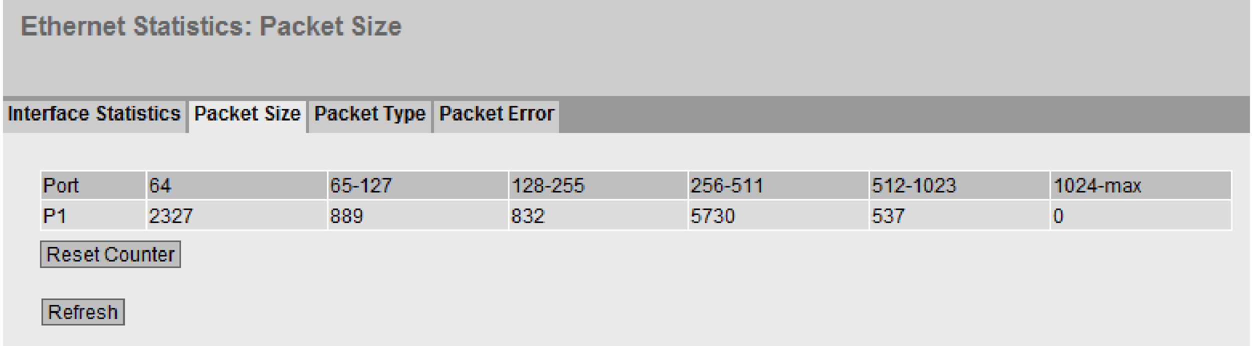
  Shows the number of sent frames that are not of the type unicast.
- **In Errors**

  Shows the number of all possible RX errors, refer to the "Packet Error" tab.

5.4.8.2 Packet Size

Frames sorted by length

This page displays how many frames of which size were 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-max
P1	2327	889	832	5730	537	0

Description

The table has the following columns:

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

Description of the button

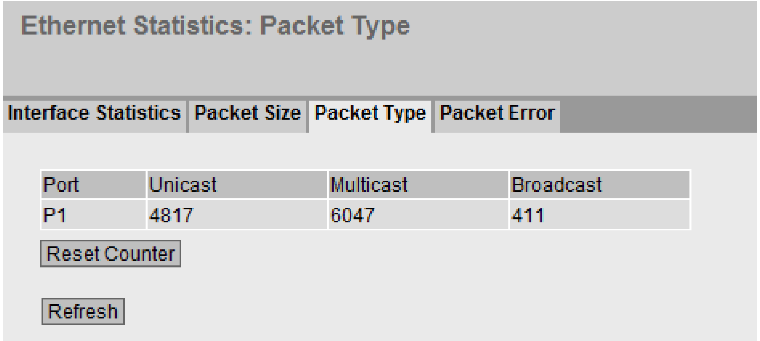
"Reset Counter" button

Click "Reset Counter" to reset all counters. The counters are also reset by a restart on the device.

5.4.8.3 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.



Ethernet Statistics: Packet Type

Port	Unicast	Multicast	Broadcast
P1	4817	6047	411

Description

The table has the following columns:

- **Port**
  Shows the available ports.
- **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

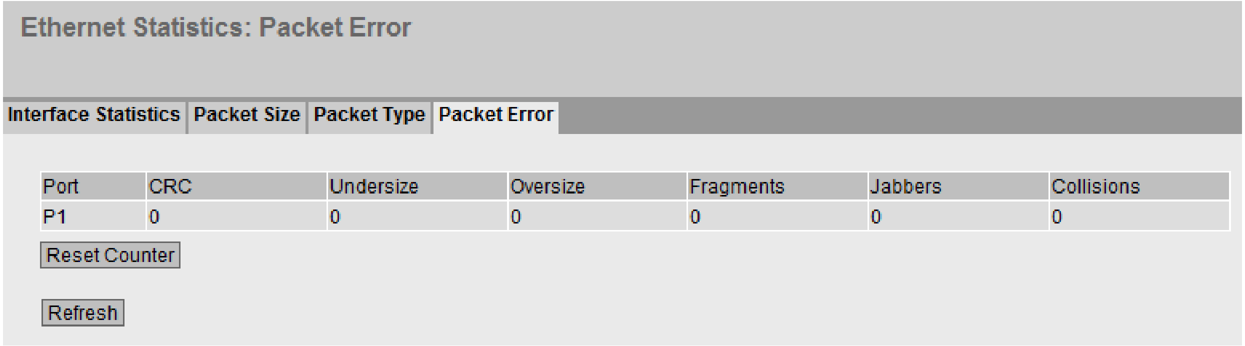
"Reset Counter" button

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

5.4.8.4 Packet Error

Bad received frames

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



Port	CRC	Undersize	Oversize	Fragments	Jabbers	Collisions
P1	0	0	0	0	0	0

Description

The table has the following columns:

- **Port**
  Shows the available ports.
- **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

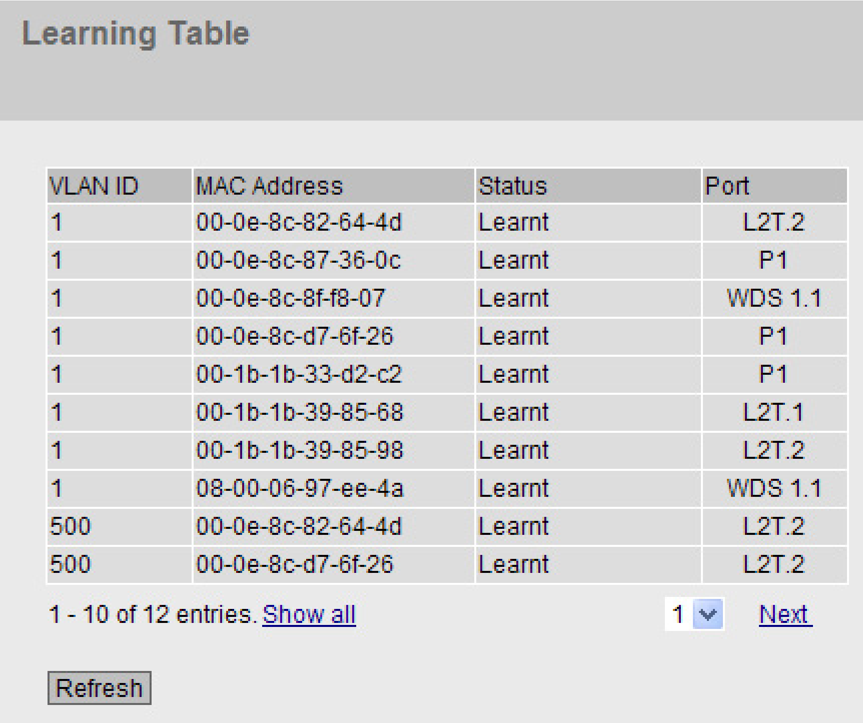
"Reset Counter" button

Click "Reset Counter" to reset all counters. The counters are also reset by a restart on the device.

5.4.9 Learning Table

Address filtering

This WBM page shows the current content of the learning table. This table lists the source addresses of unicast address frames.



Learning Table

VLAN ID	MAC Address	Status	Port
1	00-0e-8c-82-64-4d	Learnt	L2T.2
1	00-0e-8c-87-36-0c	Learnt	P1
1	00-0e-8c-8f-f8-07	Learnt	WDS 1.1
1	00-0e-8c-d7-6f-26	Learnt	P1
1	00-1b-1b-33-d2-c2	Learnt	P1
1	00-1b-1b-39-85-68	Learnt	L2T.1
1	00-1b-1b-39-85-98	Learnt	L2T.2
1	08-00-06-97-ee-4a	Learnt	WDS 1.1
500	00-0e-8c-82-64-4d	Learnt	L2T.2
500	00-0e-8c-d7-6f-26	Learnt	L2T.2

1 - 10 of 12 entries. Show all

Description

This table contains the following columns:

- **VLAN ID**
  Shows the VLAN ID of the node.

  Note

  This column appears in the table only if a VLAN is configured.

- **MAC Address**
  Shows the MAC address of the node.

- **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.
  - Invalid
    These values are not evaluated.
- **Port**
  Shows 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.

Button "Show all"

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

"Next" button

Click this button to go to the next page.

"Prev" button

Click this button to go to the previous page.

Drop-down list for page change

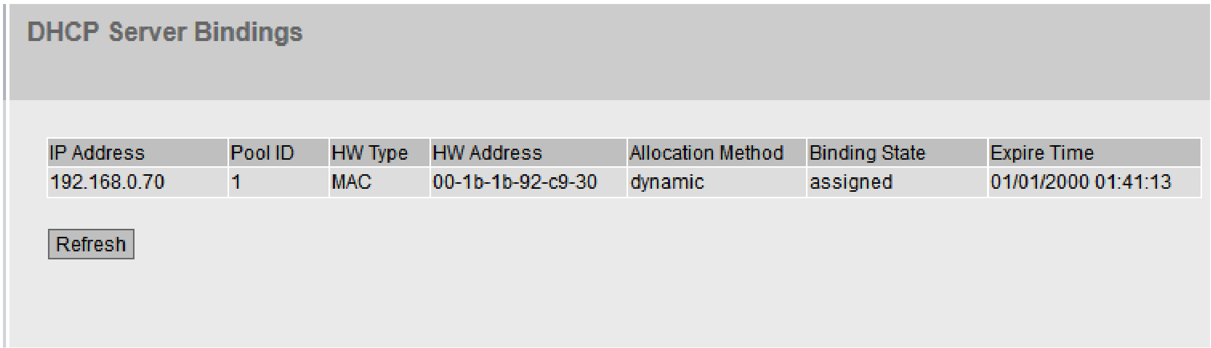
From the drop-down list, select the page you want to go to.

5.4.10 DHCP Server

Note

This tab is only available in the client mode.

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



DHCP Server Bindings

IP Address	Pool ID	HW Type	HW Address	Allocation Method	Binding State	Expire Time
192.168.0.70	1	MAC	00-1b-1b-92-c9-30	dynamic	assigned	01/01/2000 01:41:13

Description

- **IP Address**
  Shows the IPv4 address assigned to the device.
- **Pool ID**
  Shows the number of the IPv4 address band.
- **HW Type**
  Shows that the DHCP server identifies the devices in the network based on the MAC address.
- **HW Address**

  Shows the MAC address of the DHCP client.
- **Allocation Method**
  Show whether the IPv4 address was assigned statically or dynamically. You configure the static entries in "System > DHCP > Static Leases".
- **Binding State**
  Shows the status of the assignment.
  - assigned
    The assignment is used.
  - not assigned
    The assignment is not used.
  - probing
    The assignment is being checked.
  - unknown
    The status of the assignment is unknown.
- **Expire Time**
  Shows how long the assigned IPv4 address is still valid. Once this period has elapsed, the device must either request a new IPv4 address or extend the lease time of the existing IPv4 address.

5.4.11 WLAN

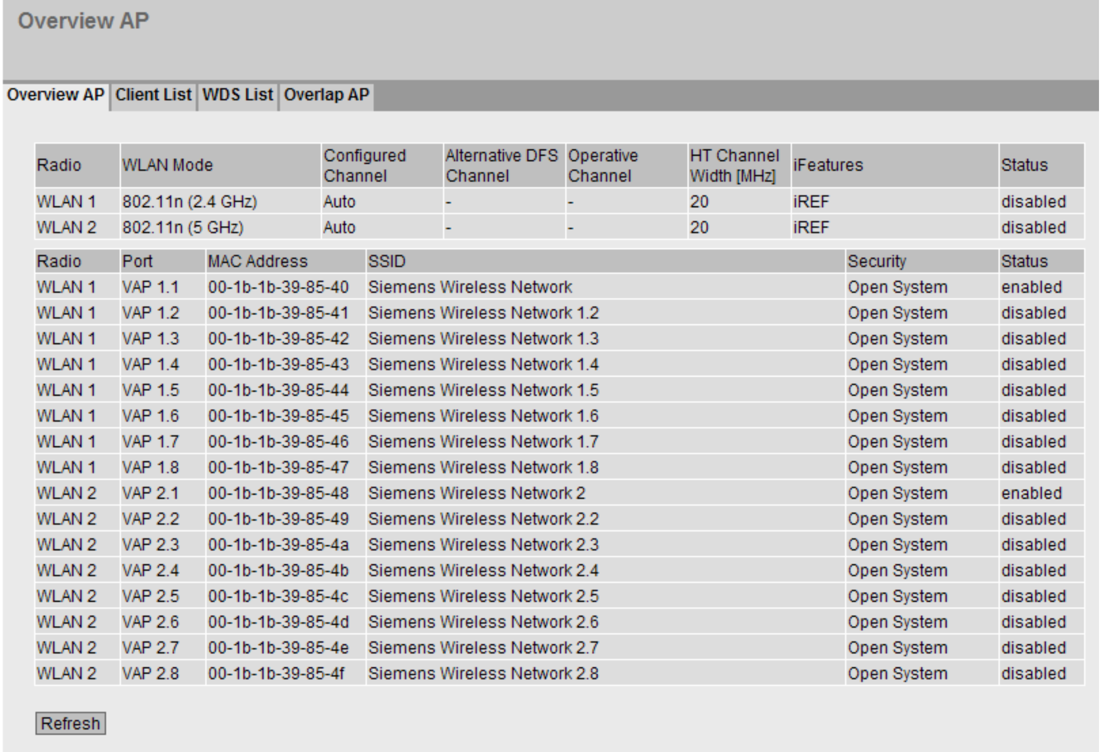
5.4.11.1 Overview AP

Overview of the configuration

This page shows these settings/properties of the WLAN or the WLAN interface.

Note

This tab is available only in access point mode.



Radio	WLAN Mode	Configured Channel	Alternative DFS Channel	Operative Channel	HT Channel Width [MHz]	iFeatures	Status
WLAN 1	802.11n (2.4 GHz)	Auto	-	-	20	iREF	disabled
WLAN 2	802.11n (5 GHz)	Auto	-	-	20	iREF	disabled

Radio	Port	MAC Address	SSID	Security	Status
WLAN 1	VAP 1.1	00-1b-1b-39-85-40	Siemens Wireless Network	Open System	enabled
WLAN 1	VAP 1.2	00-1b-1b-39-85-41	Siemens Wireless Network 1.2	Open System	disabled
WLAN 1	VAP 1.3	00-1b-1b-39-85-42	Siemens Wireless Network 1.3	Open System	disabled
WLAN 1	VAP 1.4	00-1b-1b-39-85-43	Siemens Wireless Network 1.4	Open System	disabled
WLAN 1	VAP 1.5	00-1b-1b-39-85-44	Siemens Wireless Network 1.5	Open System	disabled
WLAN 1	VAP 1.6	00-1b-1b-39-85-45	Siemens Wireless Network 1.6	Open System	disabled
WLAN 1	VAP 1.7	00-1b-1b-39-85-46	Siemens Wireless Network 1.7	Open System	disabled
WLAN 1	VAP 1.8	00-1b-1b-39-85-47	Siemens Wireless Network 1.8	Open System	disabled
WLAN 2	VAP 2.1	00-1b-1b-39-85-48	Siemens Wireless Network 2	Open System	enabled
WLAN 2	VAP 2.2	00-1b-1b-39-85-49	Siemens Wireless Network 2.2	Open System	disabled
WLAN 2	VAP 2.3	00-1b-1b-39-85-4a	Siemens Wireless Network 2.3	Open System	disabled
WLAN 2	VAP 2.4	00-1b-1b-39-85-4b	Siemens Wireless Network 2.4	Open System	disabled
WLAN 2	VAP 2.5	00-1b-1b-39-85-4c	Siemens Wireless Network 2.5	Open System	disabled
WLAN 2	VAP 2.6	00-1b-1b-39-85-4d	Siemens Wireless Network 2.6	Open System	disabled
WLAN 2	VAP 2.7	00-1b-1b-39-85-4e	Siemens Wireless Network 2.7	Open System	disabled
WLAN 2	VAP 2.8	00-1b-1b-39-85-4f	Siemens Wireless Network 2.8	Open System	disabled

Description

Table 1 has the following columns:

- **Radio**
  Shows the available WLAN interfaces.
- **WLAN mode**
  Shows the transmission standard. If DFS is activated, the transmission standard "802.11h" is not shown additionally but only the configured transmission standard "802.11a".
- **Configured Channel**
  Shows the configured channel. If "Auto" is displayed, the access point searches for a free channel itself.
- **Alternative DFS Channel**
  If the DFS function is enabled, the configured alternative channel of the access point is displayed.
  If "Auto" is displayed, the access point searches for an alternative channel itself.
  If the DFS function is activated and the access point browses for primary users for 60 seconds before starting communication with the selected channel, the text "scanning ..." is displayed instead of the channel.
- **Operative Channel**
  Shows the channel of the access point via which the access point communicates.

- **HT Channel Width [MHz]**
  Shows the channel bandwidth.
  - 20
    Channel bandwidth 20 MHz
  - 40 up
    Channel bandwidth 40 MHz. The configured channel and the neighboring channel above it are used.
  - 40 down
    Channel bandwidth 40 MHz. The configured channel and the neighboring channel below it are used.

  Note

  Channel bandwidth 40 MHz and frequency band 2.4 GHz

  If the access point detects another access point on the configured channel or on neighboring channels, the access point changes the channel bandwidth from 40 MHz to 20 MHz. If you set a "free" channel on the access point, the access point uses the channel bandwidth 40 MHz.

- **iFeatures**
  Shows which iFeatures are used.
  - -
    iFeatures are not used.
  - iPCF
  - iPCF-MC
  - iREF
- **Status**
  Shows the status of the WLAN interface.
  - enabled
    The WLAN interface is enabled.
  - disabled
    The WLAN interface is disabled.

Table 2 has the following columns:

- **Radio**
  Shows the available WLAN interfaces in this column.
- **Port**
  Shows the port of the virtual access point.
- **MAC Address**
  Shows the MAC address of the virtual access point.
- **SSID**
  Shows the SSID.
- **Security**
  Shows which authentication method is used.

If the authentication method "Open System + Encryption" or "Shared Key" is used, "Encrypted (WEP/AES)" is displayed for both authentication methods.

- **Status**
  Shows the status of the WLAN interface.
  - enabled
    The WLAN interface is enabled.
  - disabled
    The WLAN interface is disabled.

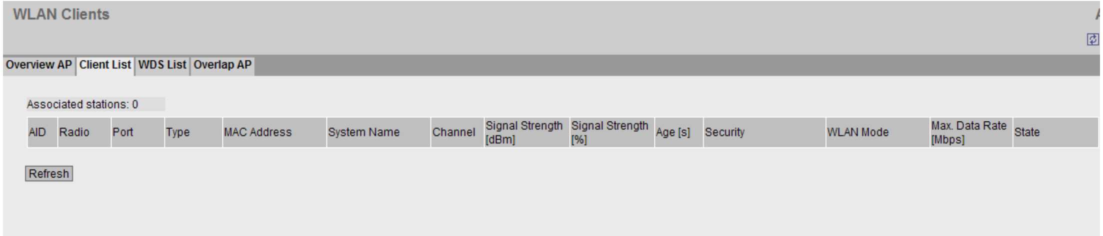
5.4.11.2 Client List

Logged-on clients

The page the clients logged on with the access point as well as additional information, for example status, signal strength, MAC address.

Note

This tab is available only in access point mode.



WLAN Clients

Associated stations: 0

AID	Radio	Port	Type	MAC Address	System Name	Channel	Signal Strength [dBm]	Signal Strength [%]	Age [s]	Security	WLAN Mode	Max. Data Rate [Mbps]	State

Description

- **Associated stations**
  Shows the number of clients logged on to the access point.

The table has the following columns:

- **AID** (Associated ID)
  Shows the connection ID of the client. If the client connects to the access point via the VAP interface, the client is assigned a connection ID. The connection ID is unique within a VAP interface. If two clients log on at different VAP interfaces, both clients can receive the same ID.
- **Radio**
  Shows the available WLAN interfaces.
- **Port**
  Shows the VAP interface.
- **Type**
  Shows the client type, for example "Sta" stands for IEEE 802.11 standard client.

- **MAC Address**
  Shows the MAC address of the client.
- **System Name**
  Shows the system name of the client if the client communicates this to the access point. Not all clients support this parameter.
- **Channel**
  Shows the channel over which the client communicates with the access point.
- **Signal Strength [dBm]**
  Shows the signal strength of the connected client in bBm.
- **Signal Strength [%]**
  Shows the signal strength of the connected client as a percentage.
- **Age [s]**
  Shows the time that has elapsed since the last client activity.
- **Security**
  Shows which authentication method is used.
  If the authentication method "Open System + Encryption" or "Shared Key" is used, "Encrypted (WEP/AES)" is displayed for both authentication methods.
- **WLAN Mode**
  Shows the transmission standard. If DFS is activated, the transmission standard "802.11h" is not shown additionally but only the configured transmission standard "802.11a".
- **Max. Data Rate [Mbps]**
  Shows the maximum data transmission speed in megabits per second.
- **State**
  Shows the current status of the connection, for example Connected means that the client is connected to the AP and is ready to communicate with the AP.

5.4.11.3 WDS List

Communication between access points

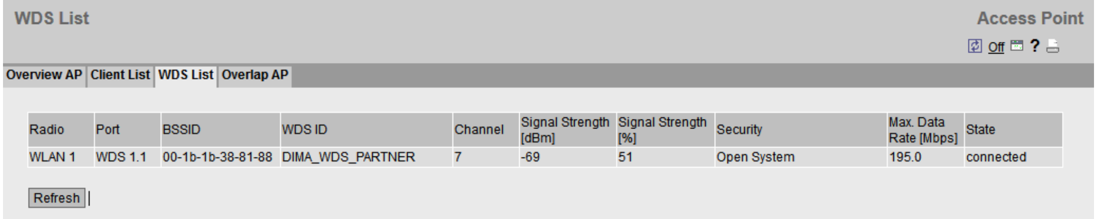
In normal operation, the access point is used as an interface to a network and communicates with clients. There are, however, situations in which several access points need to communicate with each other, for example to extend wireless coverage or to set up a wireless backbone. This mode is possible with WDS (Wireless Distributed System).

As default, the list is updated every 2 seconds. To disable the update, click "On". Instead of "On", "Off" is displayed. As default, updating is always enabled on the WBM page.

Note

This tab is available only in access point mode.

This page shows information about the WDS connections of the access point.



Radio	Port	BSSID	WDS ID	Channel	Signal Strength [dBm]	Signal Strength [%]	Security	Max. Data Rate [Mbps]	State
WLAN 1	WDS 1.1	00-1b-1b-38-81-88	DIMA_WDS_PARTNER	7	-69	51	Open System	195.0	connected

Description

The table has the following columns:

- **Radio**
  Shows the available WLAN interfaces.
- **Port**
  Shows the port.
- **BSSID**
  Shows the MAC address of the WDS partner.
- **WDS ID**
  Shows the name of the WDS partner.
- **Channel**
  Shows the channel over which the access point communicates with the WDS partner.
- **Signal Strength [dBm]**
  Shows the signal strength of the connected access point in bBm.
- **Signal Strength [%]**
  Shows the signal strength of the connected access point as a percentage.
- **Security**
  Shows which authentication method is used.
  If the authentication method "Open System + Encryption" or "Shared Key" is used, "Encrypted (WEP/AES)" is displayed for both authentication methods.
- **Max. Data Rate [Mbps]**
  Shows the maximum data transmission speed for the relevant WDS partner.
- **State**
  Shows the current status of the WDS connection.

5.4.11.4 Overlap AP

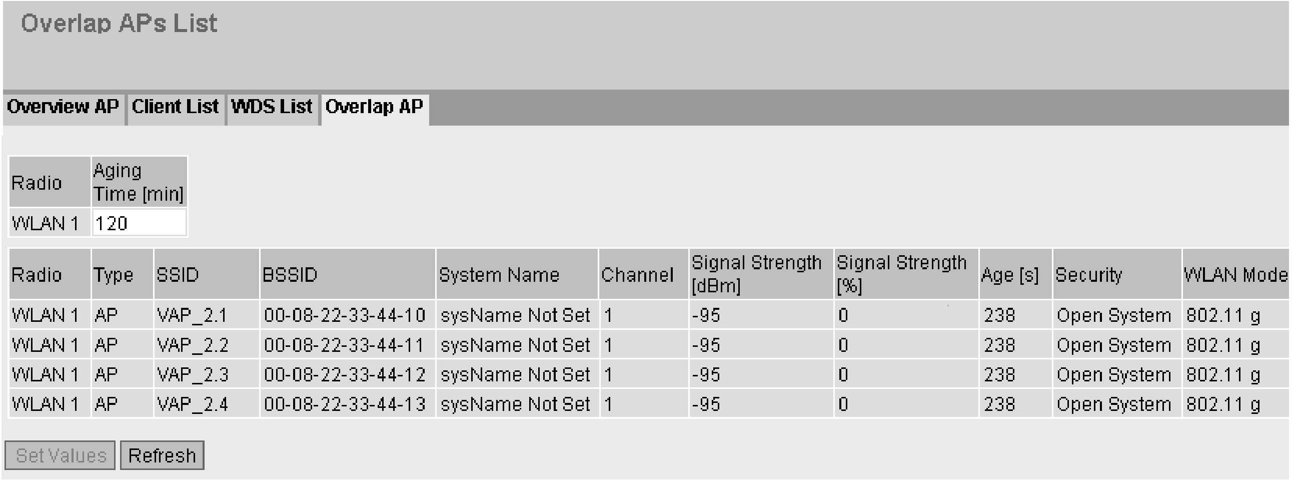
Overlapping channels

Note

This tab is available only in access point mode.

For optimum data throughput, it is important that the set wireless channel is not used by other access points. In the 2.4 GHz band (802.11b or 802.11g), there is overlapping of the channels so that an access point occupies not only the set channel but also the two or three adjacent channels. You should therefore make sure that there is adequate channel spacing to neighboring access points.

This page shows all access points that are visible on the set or adjacent channels (at 2.4 GHz). If entries exist here, the maximum data throughput of the access point and the availability of the communication link to the access point is potentially impaired.



Radio	Aging Time [min]
WLAN 1	120

Radio	Type	SSID	BSSID	System Name	Channel	Signal Strength [dBm]	Signal Strength [%]	Age [s]	Security	WLAN Mode
WLAN 1	AP	VAP_2.1	00-08-22-33-44-10	sysName Not Set	1	-95	0	238	Open System	802.11 g
WLAN 1	AP	VAP_2.2	00-08-22-33-44-11	sysName Not Set	1	-95	0	238	Open System	802.11 g
WLAN 1	AP	VAP_2.3	00-08-22-33-44-12	sysName Not Set	1	-95	0	238	Open System	802.11 g
WLAN 1	AP	VAP_2.4	00-08-22-33-44-13	sysName Not Set	1	-95	0	238	Open System	802.11 g

Description

Table 1 has the following columns:

- **Radio**
  Shows the available WLAN interfaces.
- **Aging Time [min]**
  Specify the life time of the entries in the list. If an access point is inactive for longer than the set time, it is removed from the list.

Note

Changing the aging time

The aging time is a WLAN setting. For this reason, if a change is made, the WLAN connection is briefly interrupted to accept the new value.

The table has the following columns:

- **Radio**
  Shows the available WLAN interfaces in this column.
- **Type**
  Shows the mode of the WLAN interface.
- **SSID**
  Shows the SSID of the access point.
- **BSSID**
  Shows the MAC address of the access point.

- **System Name**
  displays the system name of the device. The entry depends on the access point. Not all access points support this parameter.
- **Channel**
  Shows the channel over which the client communicates with the access point.
- **Signal Strength [dBm]**
  Shows the signal strength of the client in dBm.
- **Signal Strength [%]**
  Shows the signal strength of the client as a percentage.
- **Age [s]**
  Shows the time that has elapsed since the last access point activity.
- **Security**
  Shows which authentication method is used.
  If the authentication method "Open System + Encryption" or "Shared Key" is used, "Encrypted (WEP/AES)" is displayed for both authentication methods.
- **WLAN Mode**
  Shows the transmission standard. If DFS is activated, the transmission standard "802.11h" is not shown additionally but only the configured transmission standard "802.11a" or "802.11n".

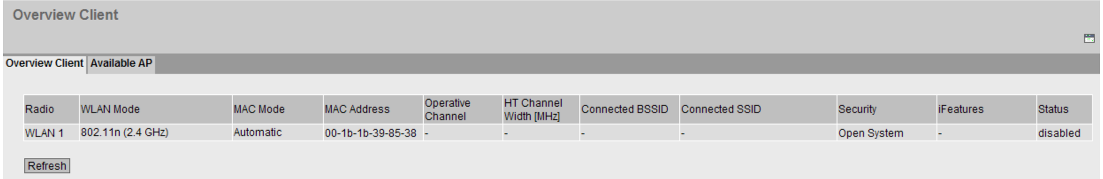
5.4.11.5 Overview Client

Overview of the configuration

Note

This page is only available for clients or access points in client mode.

The page shows an overview of the existing clients and their configuration.



Overview Client

Radio	WLAN Mode	MAC Mode	MAC Address	Operative Channel	HT Channel Width [MHz]	Connected BSSID	Connected SSID	Security	iFeatures	Status
WLAN 1	802.11n (2.4 GHz)	Automatic	00-1b-1b-39-85-38	-	-	-	-	Open System	-	disabled

Description

- **Radio**
  Shows the available WLAN interfaces in this column.
- **WLAN mode**
  Shows the transmission standard.

- **MAC Mode**
  Shows how the MAC address is assigned to the interface.
  - Automatic
    The client automatically adopts the source MAC address of the first frame that it receives over the Ethernet interface.
  - Manual
    The address was entered manually.
  - Own
    The client uses the MAC address of the Ethernet interface for the WLAN interface.
  - Layer 2 Tunnel
    The client uses the MAC address of the Ethernet interface for the WLAN interface. The network is also informed of the MAC addresses connected to the Ethernet interface of the client. Up to eight MAC addresses can be used.
- **MAC Address**
  Displays the MAC address of the WLAN interface.
- **Operative Channel**
  Shows the channel of the access point with which the client is connected.
- **HT Channel Width [MHz]**
  Shows the channel bandwidth.
  - 20
    Channel bandwidth 20 MHz.
  - 40 up
    Channel bandwidth 40 MHz. The configured channel and the neighboring channel above it are used.
  - 40 down
    Channel bandwidth 40 MHz. The configured channel and the neighboring channel below it are used.

  Note

  Channel bandwidth 40 MHz and frequency band 2.4 GHz

  If the access point detects another access point on the configured channel or on neighboring channels, the access point changes the channel bandwidth from 40 MHz to 20 MHz. If you set a "free" channel on the access point, the access point uses the channel bandwidth 40 MHz.

- **Connected BSSID**
  Shows the MAC address of the access point with which the client is connected.
- **Connected SSID**
  Shows the SSID of the access point with which the client is connected.
- **Security**
  Shows which authentication method is used.
  If the authentication method "Open System + Encryption" or "Shared Key" is used, "Encrypted (WEP/AES)" is displayed for both authentication methods.

- **iFeatures**
  Shows which iFeatures are used.
  - -
    iFeatures are not used.
  - iPCF
  - iPCF-MC
- **Status**
  Shows the status of the WLAN interface.
  - enabled
    The WLAN interface is enabled.
  - disabled
    The WLAN interface is disabled.

5.4.11.6 Available AP

Available access points

Note

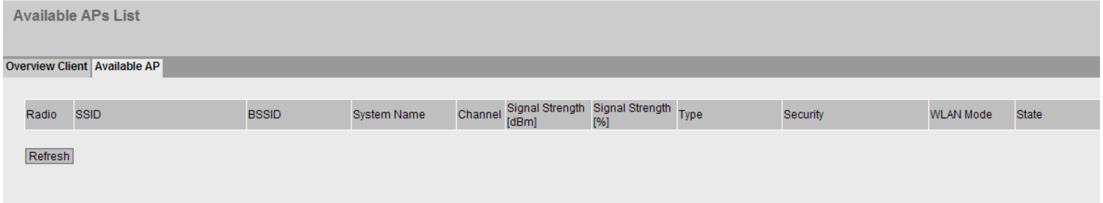
This page is only available for clients or access points in client mode.

This page shows all the access points visible to the client. The list also includes the access points to which the client cannot connect due to its configuration.

Note

Display when iPCF mode is activated

If the iPCF mode is active with a SCALANCE W700, the display is different. Since the client does not run a background scan in this case, only the access point with which the client is currently connected is displayed.



Available APs List

Radio	SSID	BSSID	System Name	Channel	Signal Strength [dBm]	Signal Strength [%]	Type	Security	WLAN Mode	State

Description

The table has the following columns:

- **Radio**
  Shows the WLAN interface visible to the access point.
- **SSID**
  Shows the SSID of the access point.
- **BSSID**
  Shows the MAC address of the access point.
- **System Name**
  displays the system name of access point. The entry depends on the access point. Not all access points support this parameter.
- **Channel**
  Shows the channel on which the access point transmits or communicates.
- **Signal Strength [dBm]**
  Shows the signal strength of the access point in dBm.
- **Signal Strength [%]**
  Shows the signal strength of the access point as a percentage.
- **Type**
  Shows the mode of the WLAN interface.
- **Security**
  Shows which authentication method is used.
  If the authentication method "Open System + Encryption" or "Shared Key" is used, "Encrypted (WEP/AES)" is displayed for both authentication methods.
- **WLAN Mode**
  Shows the transmission standard. If DFS is activated, the transmission standard "802.11h" is not shown additionally but only the configured transmission standard "802.11a" or "802.11n".
- **State**
  Shows the status of the access point, for example whether or not the access point is available.

5.4.11.7 IP Mapping Table

WLAN access for several devices via a client

Note

This page is only available for clients or access points in client mode.

You can make WLAN access available for several devices with one client if you use IP mapping. This means that you do not need to equip every device with its own WLAN client. This is possible only if the connected devices are addressed only by IP frames. Communication at MAC address level (ISO/OSI layer 2) can

- be established with one component whose MAC address is configured on the client,
- be established with a maximum of eight components if the "Layer 2 Tunnel" function is selected.

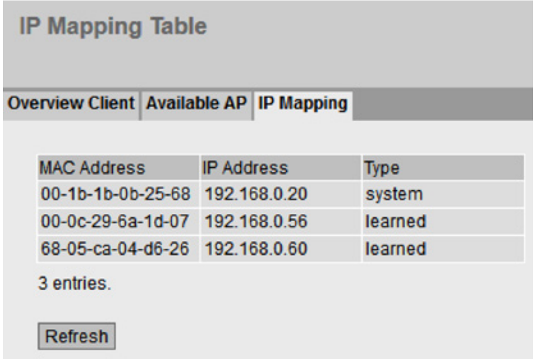
The "Layer 2 Tunnel" setting meets the requirements of industrial applications in which MAC address-based communication takes place with several devices downstream from the client. Clients with this setting cannot connect to standard Wi-Fi devices and access points with firmware V3.0 or older.

The client maintains a table with the assignment of MAC address and IP address to be able to send incoming IP frames to the correct MAC address. The "IP Mapping Table" menu command displays this table.

Note

IP mapping table

If "Layer 2 Tunnel" is configured for a client, the IP mapping table is not displayed.



MAC Address	IP Address	Type
00-1b-1b-0b-25-68	192.168.0.20	system
00-0c-29-6a-1d-07	192.168.0.56	learned
68-05-ca-04-d6-26	192.168.0.60	learned

3 entries.

Description

- MAC Address
  The MAC address of the device located downstream from the WLAN client from the perspective of the access point.
- IP Address
  The IP address managed for this device by the WLAN client.
- Type
  There are two options for the type:
  - system
    The information relates to the WLAN client itself.
  - learned
    The information relates to a device downstream from the WLAN client.

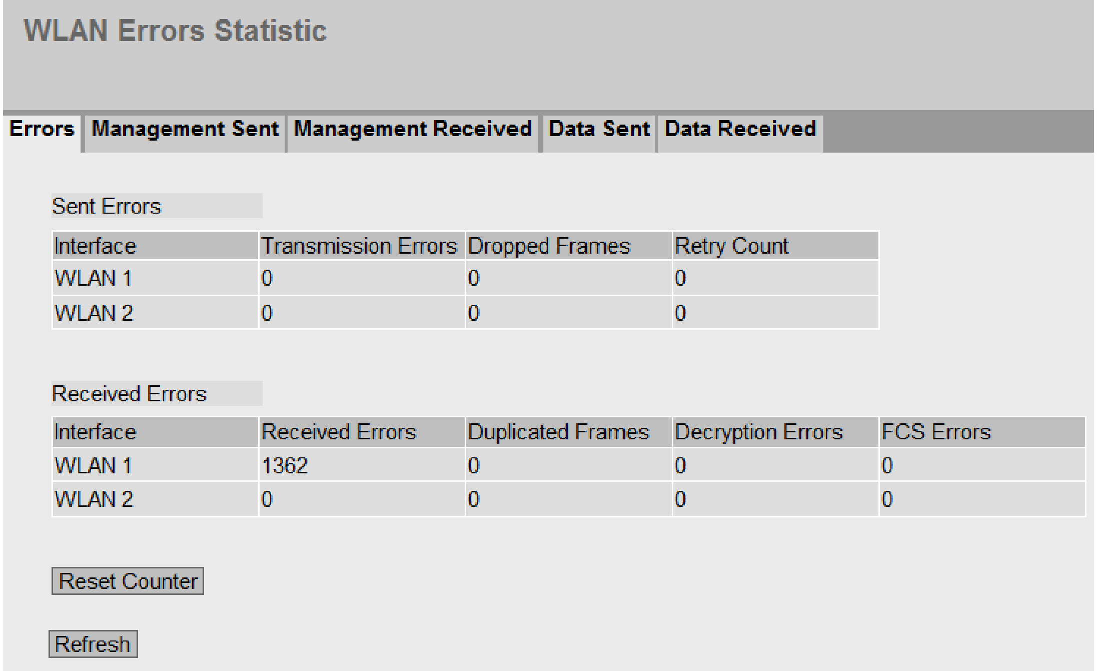
MAC Mode

IP frames in the direction from the client to the access point always have the MAC address of the WLAN interface as the source MAC address. As a result, the ARP tables at the access point end always contain only the MAC address of the WLAN interface of the clients. If there are several devices downstream from the client, the "Auto find Adopt MAC" function should not be enabled. In this case, the MAC address would be assigned indiscriminately to the first device that signals over Ethernet. If there is only IP communication between the access point and the client, the default setting "Adopt own MAC" can be retained. If you also want MAC address-based frames to be sent by devices downstream from the client, select the settings "Adopt MAC manually", "Auto find 'Adopt MAC'" or "Layer 2 Tunnel".

5.4.12 WLAN Statistics

5.4.12.1 Errors

The WBM page show how many bad frames were received or sent per WLAN interface. If an increased number of errors occurs, you should check the settings for the WLAN interface(s), the setup of the devices and the connection quality.


WLAN Errors Statistic

Sent Errors

Interface	Transmission Errors	Dropped Frames	Retry Count
WLAN 1	0	0	0
WLAN 2	0	0	0

Received Errors

Interface	Received Errors	Duplicated Frames	Decryption Errors	FCS Errors
WLAN 1	1362	0	0	0
WLAN 2	0	0	0	0

Description

The Tx Errors table has the following columns:

- **Interface**
  Shows the WLAN interface to which the entries apply.
- **Error types**
  The other columns after the WLAN interface contain the absolute numbers of the frames sent according to their error type.
  The columns of the table distinguish the following error types:
  - Transmission Errors
    Shows the number of bad frames that were sent.
  - Dropped Frames
    Shows the number of frames that were discarded.

    Despite all the retries, the frame could not be successfully sent.

    The frame has not yet been sent and the recipient has logged off in the meantime.
  - Retry Count
    Shows the number of frames sent successfully that required one or more retries.

The Rx Errors table has the following columns:

- **Interface**
  Shows the WLAN interface to which the entries apply.
- **Error types**
  The other columns after the WLAN interface contain the absolute numbers of the frames received according to their error type.
  The columns of the table distinguish the following error types:
  - Received Errors
    Shows the number of bad frames that were received.
  - Duplicate Frames
    Shows the number of frames that were received twice.
  - Decryption Errors
    Shows the number of bad encrypted frames.
  - FCS Errors
    Shows the number of frames in which the checksum was incorrect.

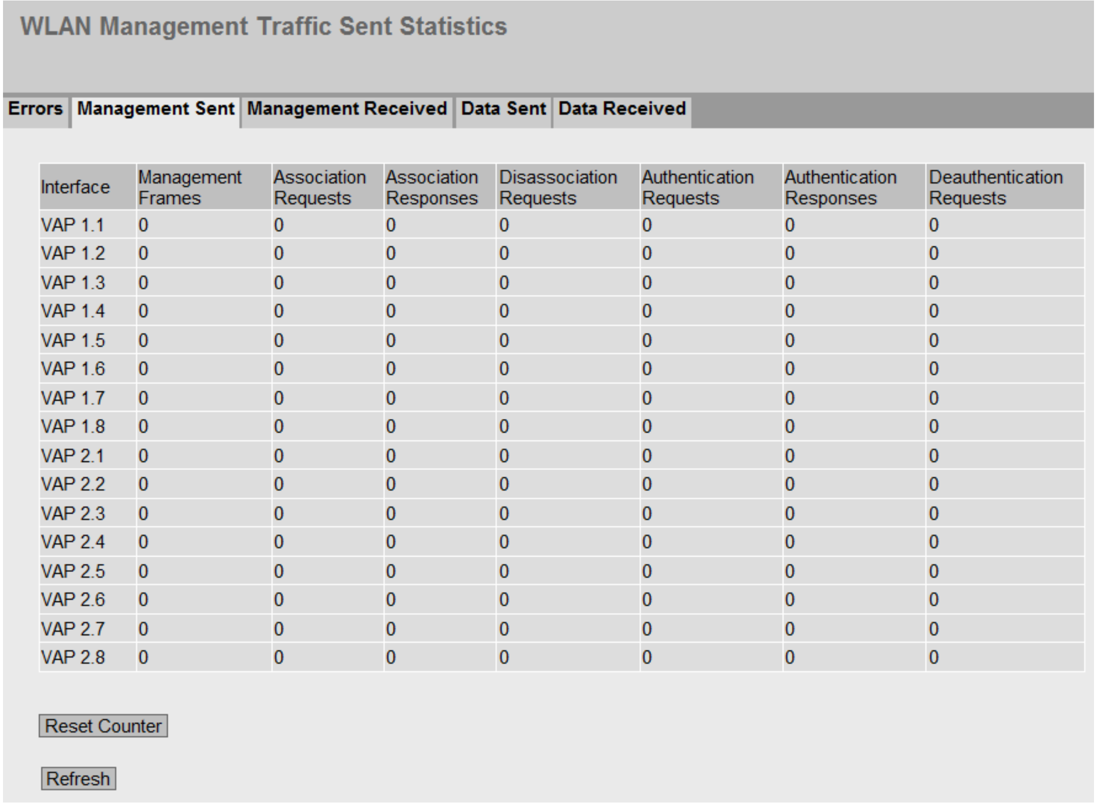
"Reset Counter" button
Click this button to reset the counters.

5.4.12.2 Management Sent

The WBM page shows how many frames in response to logging on or logging off were counted per VAP interface.

Note

This tab is available only in access point mode.



WLAN Management Traffic Sent Statistics

Interface	Management Frames	Association Requests	Association Responses	Disassociation Requests	Authentication Requests	Authentication Responses	Deauthentication Requests
VAP 1.1	0	0	0	0	0	0	0
VAP 1.2	0	0	0	0	0	0	0
VAP 1.3	0	0	0	0	0	0	0
VAP 1.4	0	0	0	0	0	0	0
VAP 1.5	0	0	0	0	0	0	0
VAP 1.6	0	0	0	0	0	0	0
VAP 1.7	0	0	0	0	0	0	0
VAP 1.8	0	0	0	0	0	0	0
VAP 2.1	0	0	0	0	0	0	0
VAP 2.2	0	0	0	0	0	0	0
VAP 2.3	0	0	0	0	0	0	0
VAP 2.4	0	0	0	0	0	0	0
VAP 2.5	0	0	0	0	0	0	0
VAP 2.6	0	0	0	0	0	0	0
VAP 2.7	0	0	0	0	0	0	0
VAP 2.8	0	0	0	0	0	0	0

Description

The table has the following columns:

- **Interface**
  Shows the VAP interface to which the entries apply.
- **Frame**
  - Management Frames
    Shows the number of management frames
  - Association Request
    Shows the number of requesting association frames relevant for a logon.

– Association Responses
  Shows the number of responding association frames relevant for a logon.

– Disassociation Request
  Shows the number of requesting disassociation frames relevant for a logoff.

– Authentication Request
  Shows the number of requesting authentication frames relevant for a logon.

– Authentication Responses
  Shows the number of responding authentication frames relevant for a logon.

– Deauthentication Request
  Shows the number of deauthentication frames relevant for a logoff.

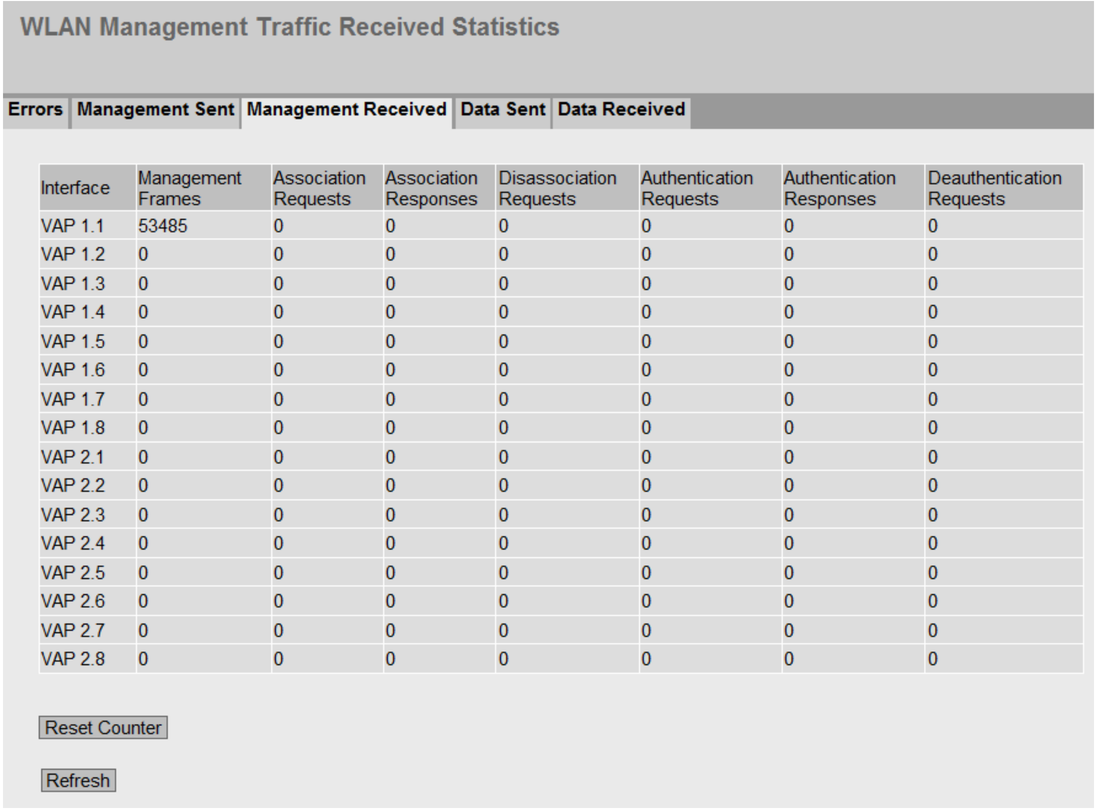
"Reset Counter" button
Click this button to reset the counters.

5.4.12.3 Management Received

The WBM page shows how many frames in response to logging on or logging off were counted per VAP interface.

Note

This tab is available only in access point mode.



WLAN Management Traffic Received Statistics

Interface	Management Frames	Association Requests	Association Responses	Disassociation Requests	Authentication Requests	Authentication Responses	Deauthentication Requests
VAP 1.1	53485	0	0	0	0	0	0
VAP 1.2	0	0	0	0	0	0	0
VAP 1.3	0	0	0	0	0	0	0
VAP 1.4	0	0	0	0	0	0	0
VAP 1.5	0	0	0	0	0	0	0
VAP 1.6	0	0	0	0	0	0	0
VAP 1.7	0	0	0	0	0	0	0
VAP 1.8	0	0	0	0	0	0	0
VAP 2.1	0	0	0	0	0	0	0
VAP 2.2	0	0	0	0	0	0	0
VAP 2.3	0	0	0	0	0	0	0
VAP 2.4	0	0	0	0	0	0	0
VAP 2.5	0	0	0	0	0	0	0
VAP 2.6	0	0	0	0	0	0	0
VAP 2.7	0	0	0	0	0	0	0
VAP 2.8	0	0	0	0	0	0	0

Description

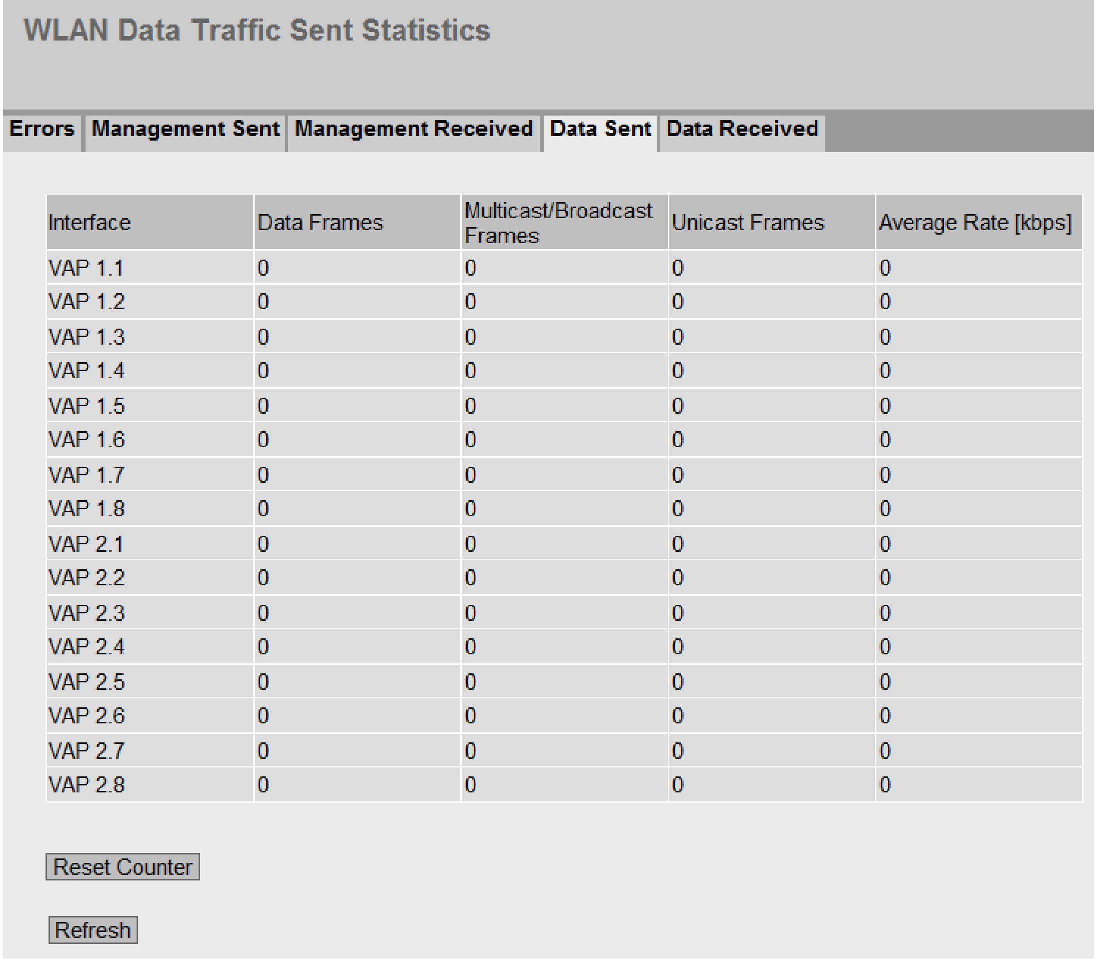
The table has the following columns:

- **Interface**
  Shows the VAP interface to which the entries apply.
- **Frame**
  - Management Frames
    Shows the number of management frames
  - Association Request
    Shows the number of requesting association frames relevant for a logon.
  - Association Responses
    Shows the number of responding association frames relevant for a logon.
  - Disassociation Request
    Shows the number of requesting disassociation frames relevant for a logoff.
  - Authentication Request
    Shows the number of requesting authentication frames relevant for a logon.
  - Authentication Responses
    Shows the number of responding authentication frames relevant for a logon.
  - Deauthentication Request
    Shows the number of deauthentication frames relevant for a logoff.

"Reset Counter" button
Click this button to reset the counters.

5.4.12.4 Data Sent

The WBM page shows how many frames were sent per VAP interface.



WLAN Data Traffic Sent Statistics

Interface	Data Frames	Multicast/Broadcast Frames	Unicast Frames	Average Rate [kbps]
VAP 1.1	0	0	0	0
VAP 1.2	0	0	0	0
VAP 1.3	0	0	0	0
VAP 1.4	0	0	0	0
VAP 1.5	0	0	0	0
VAP 1.6	0	0	0	0
VAP 1.7	0	0	0	0
VAP 1.8	0	0	0	0
VAP 2.1	0	0	0	0
VAP 2.2	0	0	0	0
VAP 2.3	0	0	0	0
VAP 2.4	0	0	0	0
VAP 2.5	0	0	0	0
VAP 2.6	0	0	0	0
VAP 2.7	0	0	0	0
VAP 2.8	0	0	0	0

Description

The table has the following columns:

- **Interface**
  Shows the VAP interface to which the entries apply.
- **Frame types**

  The other columns after the VAP interface contain the absolute numbers of the sent frames according to the frame types.

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

  – Data Frames
    Shows the number of sent data frames.

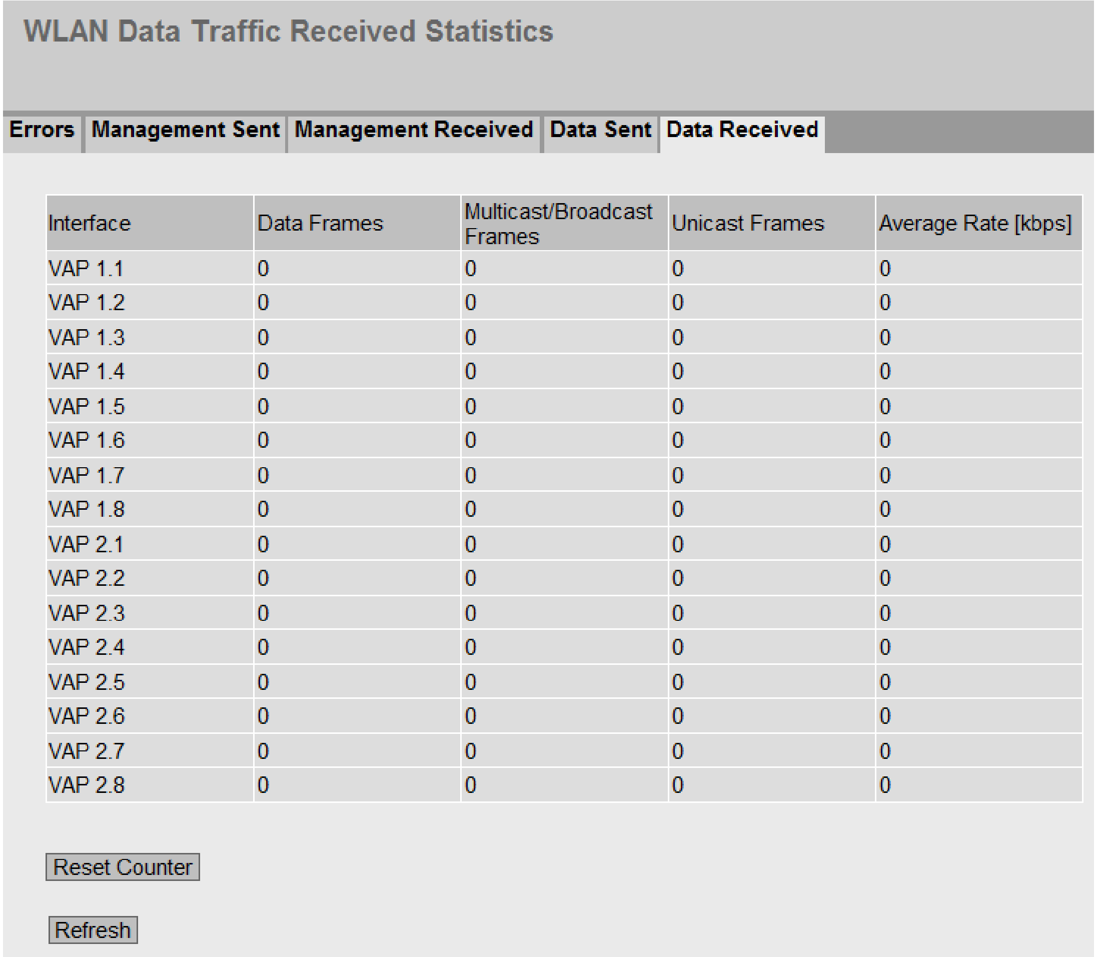
  – Multicast/Broadcast Frames
    Shows the number of sent multicast and broadcast frames.

- Unicast Frames
  Shows the number of sent unicast frames.
- Average Rate
  Shows average data rate of the last data frames sent.

"Reset Counter" button
Click this button to reset the counters.

5.4.12.5 Data Received

The WBM page shows how many frames were received per VAP interface.



WLAN Data Traffic Received Statistics

Interface	Data Frames	Multicast/Broadcast Frames	Unicast Frames	Average Rate [kbps]
VAP 1.1	0	0	0	0
VAP 1.2	0	0	0	0
VAP 1.3	0	0	0	0
VAP 1.4	0	0	0	0
VAP 1.5	0	0	0	0
VAP 1.6	0	0	0	0
VAP 1.7	0	0	0	0
VAP 1.8	0	0	0	0
VAP 2.1	0	0	0	0
VAP 2.2	0	0	0	0
VAP 2.3	0	0	0	0
VAP 2.4	0	0	0	0
VAP 2.5	0	0	0	0
VAP 2.6	0	0	0	0
VAP 2.7	0	0	0	0
VAP 2.8	0	0	0	0

Description

The table has the following columns:

- **Interface**
  Shows the VAP interface to which the entries apply.

- **Frame types**
  The other columns after the VAP interface contain the absolute numbers of the received frames according to the frame types.

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

  – Data Frames
    Number of received data frames.

  – Multicast/Broadcast Frames
    Shows the number of received multicast and broadcast frames.

  – Unicast Frames
    Shows the number of received unicast frames.

  – Average Rate
    Shows average data rate of the last data frames received.

"Reset Counter" button
Click this button to reset the counters.

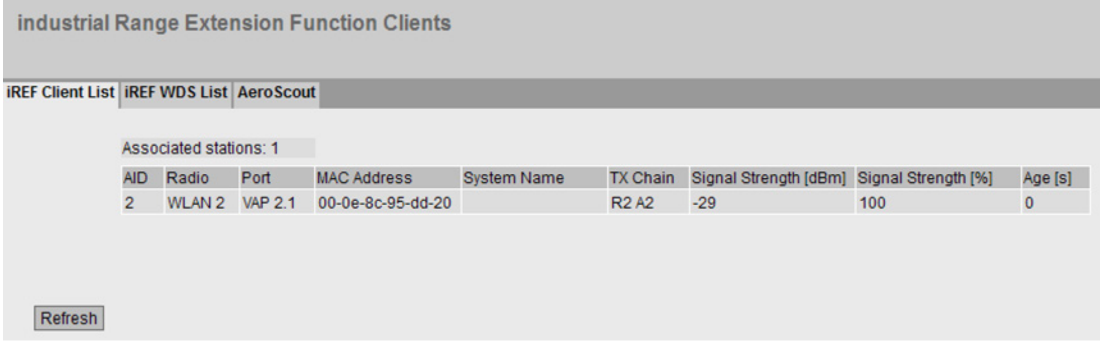
5.4.13 WLAN iFeatures

5.4.13.1 iREF Client List

The WBM page shows the antenna connector via which the clients logged on to the access point communicate. Other information such as the signal strength and the MAC address of the WLAN interface is also shown.

Note

- This tab is available only in access point mode.
- This WBM page can only be configured with the following KEY-PLUG:
  – Access point: W780 iFeatures (MLFB 6GK5 907-8PA00)



industrial Range Extension Function Clients

Associated stations: 1

AID	Radio	Port	MAC Address	System Name	TX Chain	Signal Strength [dBm]	Signal Strength [%]	Age [s]
2	WLAN 2	VAP 2.1	00-0e-8c-95-dd-20		R2 A2	-29	100	0

Description

The page contains the following box:

- **Associated stations**
  Shows the number of clients logged on to the access point

The table has the following columns:

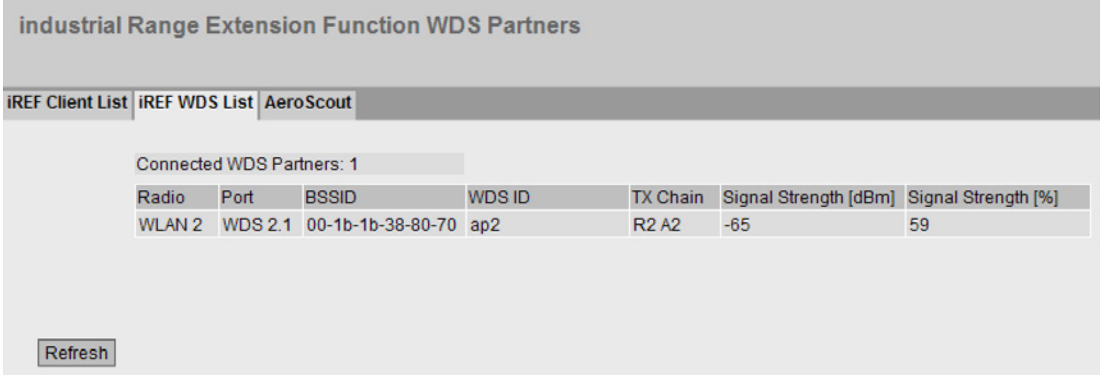
- **AID** (Associated ID)
  Shows the connection ID of the client. If the client connects to the access point via the VAP interface, the client is assigned a connection ID. The connection ID is unique within a VAP interface. If two clients log on at different VAP interfaces, both clients can receive the same ID.
- **Radio**
  Shows the available WLAN interfaces.
- **Port**
  Shows the VAP interface.
- **MAC Address**
  Shows the MAC address of the client.
- **System Name**
  Shows the system name of the client if the client communicates this to the access point. Not all clients support this parameter.
- **Tx Chain**
  Shows the antenna connector over which the client communicates with the access point.
- **Signal Strength [dBm]**
  Shows the signal strength of the connected client in bBm.
- **Signal Strength [%]**
  Shows the signal strength of the connected client as a percentage.
- **Age [s]**
  Shows the age of the listed client.

5.4.13.2 iREF WDS List

The WBM page shows the access points logged on to the access point via a WDS link. This page shows information such as the antenna used and the signal strength of the WLAN interface.

Note

- This tab is available only in access point mode.
- This WBM page can only be configured with the following KEY-PLUG:
  – Access point: W780 iFeatures (MLFB 6GK5 907-8PA00)



Connected WDS Partners: 1

Radio	Port	BSSID	WDS ID	TX Chain	Signal Strength [dBm]	Signal Strength [%]
WLAN 2	WDS 2.1	00-1b-1b-38-80-70	ap2	R2 A2	-65	59

Description

The page contains the following box:

- **Connected WDS Partners**
  Shows the number of access points logged on to the access point

The table has the following columns:

- **Radio**
  Shows the available WLAN interfaces.
- **Port**
  Shows the WDS interface.
- **BSSID**
  Shows the MAC address of the WDS partner.
- **WDS ID**
  Shows the name of the WDS partner.
- **Tx Chain**
  Shows the antenna connector over which the two access points communicate with each other.
- **Signal Strength [dBm]**
  Shows the signal strength of the connected access point in bBm.
- **Signal Strength [%]**
  Shows the signal strength of the connected access point as a percentage.

5.4.13.3 AeroScout

This page shows information on forwarding AeroScout frames.

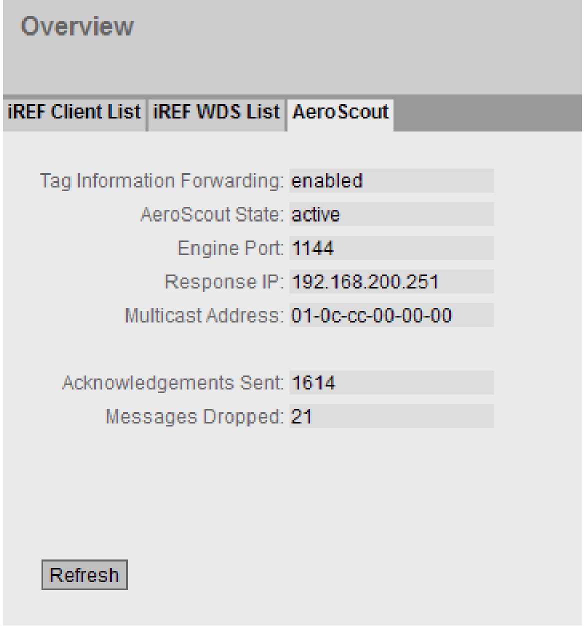
Note

- This tab is available only in access point mode.
- This WBM page can only be configured with the following KEY-PLUG:
  Access point: W780 iFeatures (MLFB 6GK5 907-8PA00)

Note

The AeroScout function cannot be combined with other iFeatures (iPCF, iPCF-MC,, iREF). AeroScout can only be used in the 2.4 GHz band according to IEEE 802.11g, IEEE 802.11n and IEEE 802.11n-only.

For more detailed information, please refer to the documentation of the AeroScout company (www.aeroscout.com).



Tag Information Forwarding: enabled
AeroScout State: active
Engine Port: 1144
Response IP: 192.168.200.251
Multicast Address: 01-0c-cc-00-00-00

Acknowledgements Sent: 1614
Messages Dropped: 21

Description

- **Tag Information forwarding**
  In the management program that evaluates the AeroScout frames, you can specify whether or not an IWLAN device will forward frames. Here, you can see which setting was made in the management program.

  Note

  With a suitable configuration, the SCALANCE W700 forwards AeroScout frames but does not process or evaluate them itself. This is done only in the "AeroScout System Manager" program.

- **AeroScout State**
  This indicates whether AeroScout is enabled or disabled.
- **Engine port**
  The IWLAN device expects UDP packets from the management program at port 1144.
- **Response IP**
  The IP address of the computer on which the management program for evaluation of the AeroScout frames is running.
- **Multicast address**
  The tag sends frames as multicast. This multicast address is configured in the management program and displayed here.
- **Acknowledgements sent**
  The number of acknowledgments sent by the IWLAN device to the management program as a result of cyclic queries or manual configuration changes in the management program (UDP packets).
- **Messages dropped**
  The number of frames not forwarded. If, for example, an AeroScout tag is configured so that it sends on channel 1, the IWLAN device does not forward a frame received on channel 6.

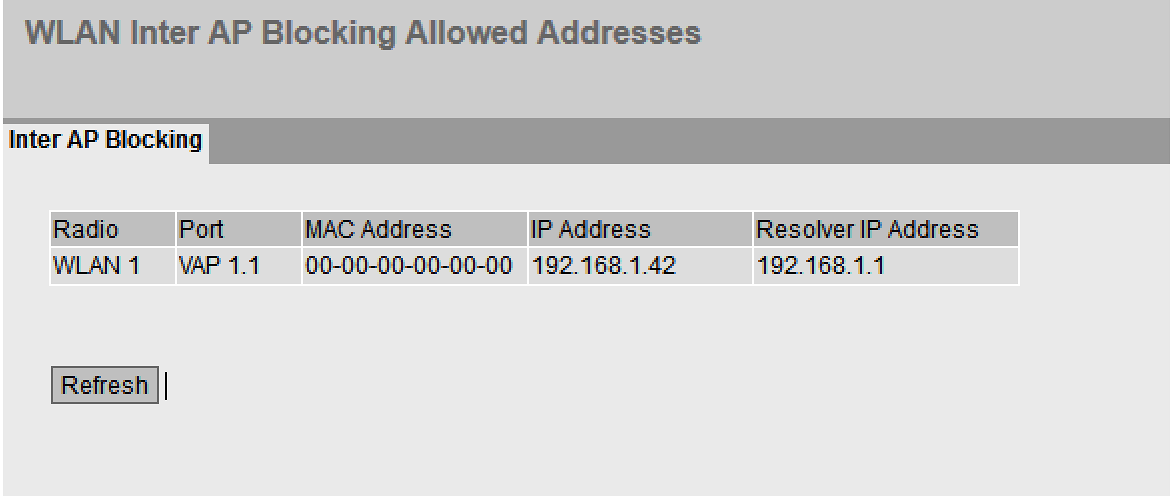
5.4.14 Security

5.4.14.1 Inter AP blocking

Note

- This tab is available only in access point mode.
- This WBM page is enabled with the following KEY-PLUGs:
  - W780 iFeatures (MLFB 6GK5 907-8PA00)
  - W700 Security (MLFB 6GK5907-0PA00)

The WBM page shows a list of the devices with which the clients are allowed to communicate.



WLAN Inter AP Blocking Allowed Addresses

Radio	Port	MAC Address	IP Address	Resolver IP Address
WLAN 1	VAP 1.1	00-00-00-00-00-00	192.168.1.42	192.168.1.1

Description

The table has the following columns:

- **Radio**
  Shows the available WLAN interfaces to which the settings relate.
- **Port**
  Shows the VAP interface to which the settings relate.
- **MAC Address**
  Shows the MAC address of the device with which the client may communicate.
- **IP Address**
  Shows the IP address of the device with which the client may communicate.
- **Resolver IP Address**
  Shows the IP address with which the permitted IP address is resolved.

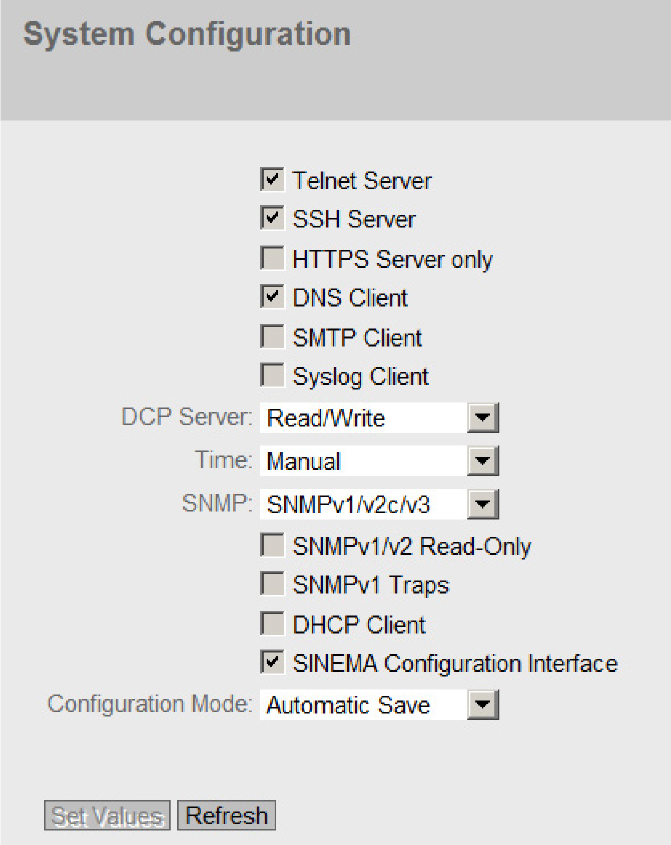
5.5 "System" menu

5.5.1 System Configuration

System configuration

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

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



System Configuration

☑ Telnet Server
☑ SSH Server
☐ HTTPS Server only
☑ DNS Client
☐ SMTP Client
☐ Syslog Client
DCP Server: Read/Write
Time: Manual
SNMP: SNMPv1/v2c/v3
☐ SNMPv1/v2 Read-Only
☐ SNMPv1 Traps
☐ DHCP Client
☑ SINEMA Configuration Interface
Configuration Mode: Automatic Save

Description

The page contains the following boxes:

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

- **"DNS Client" check box**
  Enable or disable the DNS client. You can configure other settings in "System > DNS Client".
- **"SMTP Client" check box**
  Enable or disable the SMTP client. You can configure other settings in "System > SMTP Client".
- **"Syslog Client"** check box
  Enable or disable the Syslog client. You can configure other settings in "System > Syslog Client".
- **"DCP Server"** drop-down list
  Specify whether or not the device can be accessed with DCP (Discovery and Configuration Protocol):
  - "-" (disabled)
    DCP is disabled. Device parameters can neither be read nor modified.
  - Read/Write
    With DCP, device parameters can be both read and modified.
  - Read-Only
    With DCP, device parameters can be read but cannot be modified.
- **"Time"**drop-down list
  Select the setting from the drop-down list. The following settings are possible:
  - Manual
    The system time is set manually. You can configure other settings in "System > Time > Manual Setting".
  - SIMATIC Time
    The system time is set using a SIMATIC time transmitter. You can configure other settings in "System > System Time > SIMATIC Time Client".
  - SNTP Client
    The system time is set via an SNTP server. You can configure other settings in "System > System Time > SNTP Client".
  - NTP Client
    The system time is set via an NTP server. You can configure other settings in "System > System Time > NTP Client".
- **"SNMP" drop-down list:**
  Select the protocol from the drop-down list. The following settings are possible:
  - "-" (SNMP disabled)
    Access to device parameters via SNMP is not possible.
  - SNMPv1/v2c/v3
    Access to device parameters is possible with SNMP versions 1, 2c or 3. You can configure other settings in "System > SNMP > General".
  - SNMPv3
    Access to device parameters is possible only with SNMP version 3. You can configure other settings in "System > SNMP > General".
- **"SNMPv1/v2 Read-Only"** check box
  Enable or disable write access to SNMP variables with SNMPv1/v2c.

- **"SNMPv1 Traps"** check box
  Enable or disable the sending of traps (alarm frames). You can configure other settings in "System > SNMP > Traps".
- **"DHCP Client" check box**
  Enable or disable the DHCP client. You can configure other settings in "System > DHCP Client".
- **"SINEMA Configuration Interface" check box**
  If the SINEMA configuration interface is enabled, you can download configurations to the device via the TIA Portal.
- **"Configuration Mode" drop-down list:**

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

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

Procedure

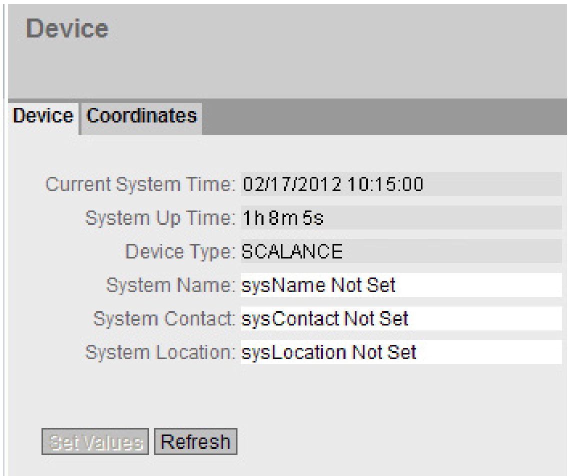
1. To use the required function, select the corresponding check box.
2. Select the options you require from the drop-down lists.
3. Click the "Set Values" button.

5.5.2 General

5.5.2.1 Device

General device information

This page contains the general device information.



Current System Time: 02/17/2012 10:15:00
System Up Time: 1h 8m 5s
Device Type: SCALANCE
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

The page contains the following boxes:

- **Current System Time**
  Shows the current system time. The system time is either set by the user or by a time-of-day frame: either SINEC H1 time-of-day frame, NTP or SNTP. (readonly)
- **System Up Time**
  Shows the running time of the device since the last restart. (readonly)
- **Device Type**
  Shows the type of the device. (readonly)
- **"System Name" input box**
  You can enter the name of the device. The entered name is displayed in the selection area. A maximum of 255 characters are possible.
  The system name is also displayed in the CLI input prompt. The number of characters in the CLI input prompt is limited. The system name is truncated after 16 characters.

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

Note

The ASCII code 0x20 to 0x7e is used in the input boxes.

At the start and end of the boxes **"System Name"**, **"System Contact"** and **"System Location"**, the characters "<", ">" and "space" are not permitted.

Procedure

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

5.5.2.2 Coordinates

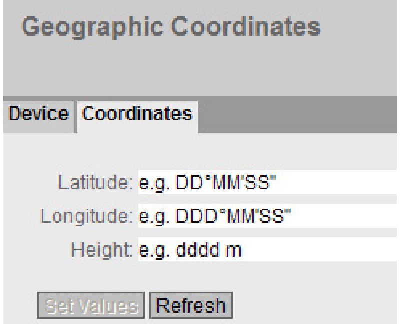
Information on geographic coordinates

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

Getting the coordinates

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

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



Geographic Coordinates

Latitude: e.g. DD°MM'SS"

Longitude: e.g. DDD°MM'SS"

Height: e.g. dddd m

Description

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

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

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

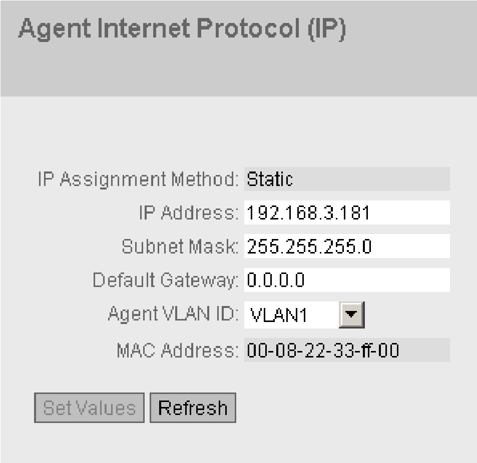
Procedure

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

5.5.3 Agent IP

Configuration of the IP addresses

On this WBM page, you configure the IP address for the device.



Agent Internet Protocol (IP)

IP Assignment Method: Static

IP Address: 192.168.3.181

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

Agent VLAN ID: VLAN1

MAC Address: 00-08-22-33-ff-00

Description

The page contains the following boxes:

- **IP Assignment Method**
  Shows how the IP address is assigned.
  - Static
    The IP address is static. You enter the IP settings in the "IP Address" and "Subnet Mask" input boxes.
  - Dynamic (DHCP)
    The device obtains a dynamic IP address from a DHCP server.
- **"IP Address" input box**
  Enter the IP address of the device.
  After clicking the "Set Values" button, this IP address is also displayed in the address bar of the Web browser. If this does not take place automatically, you will need to enter the IP address in the address bar of the Web browser manually.
- **"Subnet Mask" input box**
  Enter the subnet mask of the device.
- **"Default Gateway" input box**
  Enter the IP address of the default gateway to be able to communicate with devices in another subnet, for example diagnostics stations, e-mail server.

- **"Agent VLAN ID" drop-down list**

  Select the VLAN ID from the drop-down list. The drop-down list is available only if the "Base Bridge Mode" parameter is set to "802.1 Q VLAN Bridge". You can configure the parameter in "Layer 2 > VLAN > General". 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.

- **MAC Address**

  Shows the MAC address of the device. The MAC address is linked to the hardware and cannot be modified.

Procedure

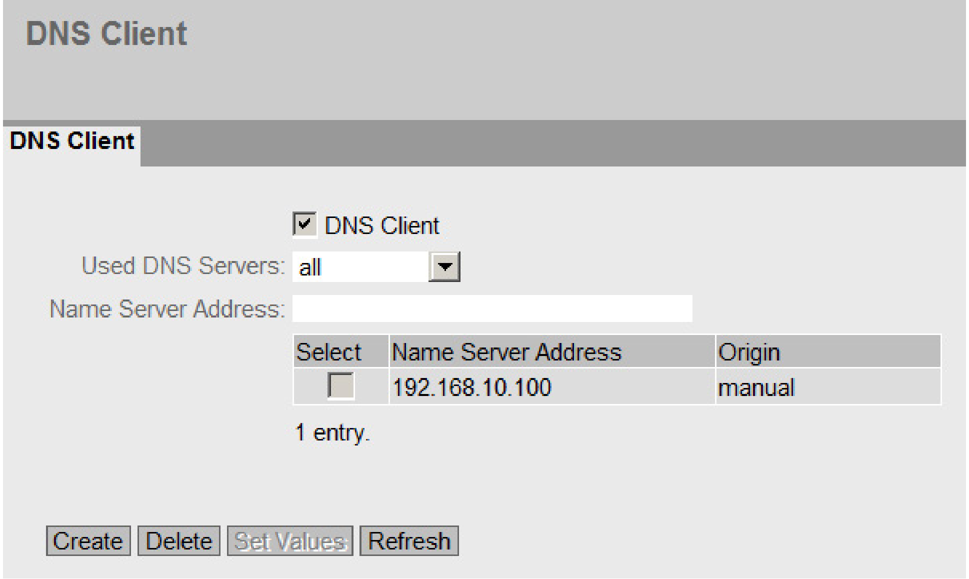
1. In the input boxes, enter the IP address, subnet mask and the default gateway.
2. Select the assigned VLAN ID from the "Agent VLAN ID" drop-down list. If the drop-down list cannot be enabled, check whether the "Base Bridge Mode" parameter is set to "802.1 Q VLAN Bridge". You can configure the parameter in "Layer 2 > VLAN > General".
3. Click the "Set Values" button.

5.5.4 DNS Client

On this page, you configure the DNS server for the device.

Note

Only resource records of type A (IPv4 address of a host) are supported.



DNS Client

DNS Client

☑ DNS Client

Used DNS Servers: all

Name Server Address:

Select	Name Server Address	Origin
□	192.168.10.100	manual

1 entry.

Description

The page contains the following boxes:

- **"DNS Client" check box**
  If the check box is enabled, the "DNS client" function is enabled.
- **"Used DNS Server" drop-down list**

  Here you specify which DNS server the device uses:

  – public only
  The device uses only the DNS servers assigned by DHCP.

  – manual only
  The device uses only the manually configured DNS servers. The DNS servers must be connected to the Internet. A maximum of three DNS servers can be configured.

  – all
  The device uses all available DNS servers.
- **"Name Server Address" input box**

  When configuring manually, you enter the IP address of a DNS server here. After clicking the "Create" button, an entry is generated in the table of DNS servers.
- The table for the DNS servers with the following columns:

  – **Select**
  Select a check box in this column and click the "Delete" button to delete an entry in the list.

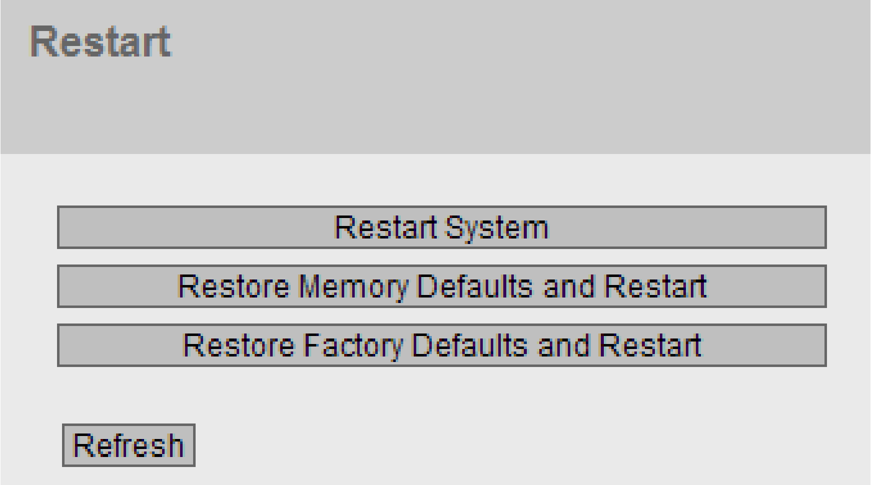
  – **Name Server Address**
  The IP address of the DNS server.

  – **Origin**
  This shows whether the DNS server was configured manually or was assigned by DHCP.

5.5.5 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", configuration modifications must be saved manually before a restart. In "Autosave mode", the last changes are saved automatically before a restart.

Description

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

- **"Restart System" button**
  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" button**
  Click this button to restore the factory configuration settings with the exception of the following parameters and to restart:
  - IP addresses
  - Subnet mask
  - IP address of the default gateway
  - DHCP client ID
  - DHCP
  - System name
  - System location
  - System contact
  - User names and passwords
  - Mode of the device
- **"Restore Factory Defaults and Restart" button**
  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 configuration 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.

5.5.6 Commit Control

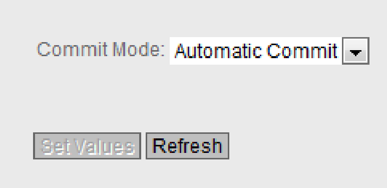
Change management

On this page, you specify when the WLAN settings become effective on the device.
If you change a WLAN setting and confirm the change with "Set Values", this change is adopted and takes effect immediately. To do this, the WLAN connection is briefly interrupted. This means that you can lose the WLAN connection to your device before it is fully configured.

With the "Manual Commit" setting, you have the opportunity of first fully configuring the device. The changes are accepted, but are not active immediately. The changes only take effect when you confirm the changes with the "Commit Changes" button.

Note

If you configure the device via the WLAN interface, we recommend that you use the "Manual Commit" setting. Check the parameters again before you confirm the changes with the "Commit Changes" button.



Commit Mode: Automatic Commit

Description

The page contains the following boxes:

- **Drop-down list "Commit Mode"**
  Select the required setting from the drop-down list:
  - Automatic Commit
    Each change in the WLAN settings is adopted and is immediately effective when you click the "Set Values" button. With its default setting, the device is set to Automatic Commit.
  - Manual Commit
    Die changes are accepted, but are not immediately effective. The changes only take effect when you click the "Commit Changes" button. The "Commit Changes" button is displayed if you set "Manual Commit". The message "Manual Commit Mode Active - Press "Commit Changes" button to provide current configuration to driver" is also displayed in the display area as soon as there are WLAN changes. This message can be seen on every WBM page until the changes made have either taken effect or the device has been restarted.

    Note

    When the changes take effect, the WLAN connections to all WLAN interfaces will be interrupted for a short time. The WLAN driver is started with the new settings.

5.5.7 Load&Save

Overview of the file types

Table 5- 1 HTTP

File type		Down-load	Save	Delete
Config	Start configuration	X	X	--
ConfigPack	Detailed configuration information. for example, start configuration, users, certificates	X	X	--
CountryList	The zip file contains the country list as a csv and as a pdf file.	--	X	--
Debug	This file contains information for Siemens Support.	--	X	X
Firmware	Firmware	X	--	--
GSDML	Information on the device properties	--	X	--
HTTPS Cert	HTTPS certificate	X	--	X
LogFile	File with entries from the event log table	--	X	--
MIB	Private MSPS MIB file "Scalance_w_msps.mib"	--	X	--
Script	CLI script file	X	--	--
StartupInfo	Startup log file	--	X	--
Users	File with user names and passwords	X	X	--
WLANAuthlog	File with entries from the WLAN Authentication Log (information on successful or failed authentication attempts)	--	X	--
WLANCert (in client mode only)	User certificate. You can specify a password for the user certificate on the WBM page "Load&Save > Password".	X	X	X
WLANServCert (in client mode only)	Server certificate.	X	--	X
WLANSigRec (in client mode only)	The zip file contains the following: • csv file with the measured values of the signal recorder • pdf file with the measured values and an additional graphic representation of the measured values. You will find information about the measured values and their graphic representation in the section "Signal Recorder (Page 234)".	--	X	X

Table 5- 2 TFTP

File type		Save	Down-load
Config	Start configuration	X	X
ConfigPack	Detailed configuration information. for example, start configuration, users, certificates	X	X
CountryList	The zip file contains the country list as a csv and as a pdf file.	X	--
Debug	This file contains information for Siemens Support.	X	--
Firmware	Firmware	X	X
GSDML	Information on the device properties	X	--
HTTPS Cert	HTTPS certificate	X	X
LogFile	File with entries from the event log table	X	--
MIB	Private MSPS MIB file "Scalance_w_msps.mib"	X	--
Script	CLI script file	--	X
StartupInfo	Startup log file	X	--
Users	File with user names and passwords	X	X
WLANAuthlog	File with entries from the WLAN Authentication Log (information on successful or failed authentication attempts)	X	--
WLANCert (in client mode only)	User certificate. You can specify a password for the user certificate on the WBM page "Load&Save > Password".	X	X
WLANServerCert (in client mode only)	Server certificate	X	X
WLANSigRec (in client mode only)	The zip file contains the following: • csv file with the measured values of the signal recorder • pdf file with the measured values and an additional graphic representation of the measured values. You will find information about the measured values and their graphic representation in the section "Signal Recorder (Page 234)".	X	--

5.5.7.1 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

Incompatibility with predecessor versions

During the installation of a previous version, the configuration data and log files can be lost. In this case, the device starts up with the factory settings after the firmware has been installed.

Incompatibility with previous versions with PLUG inserted

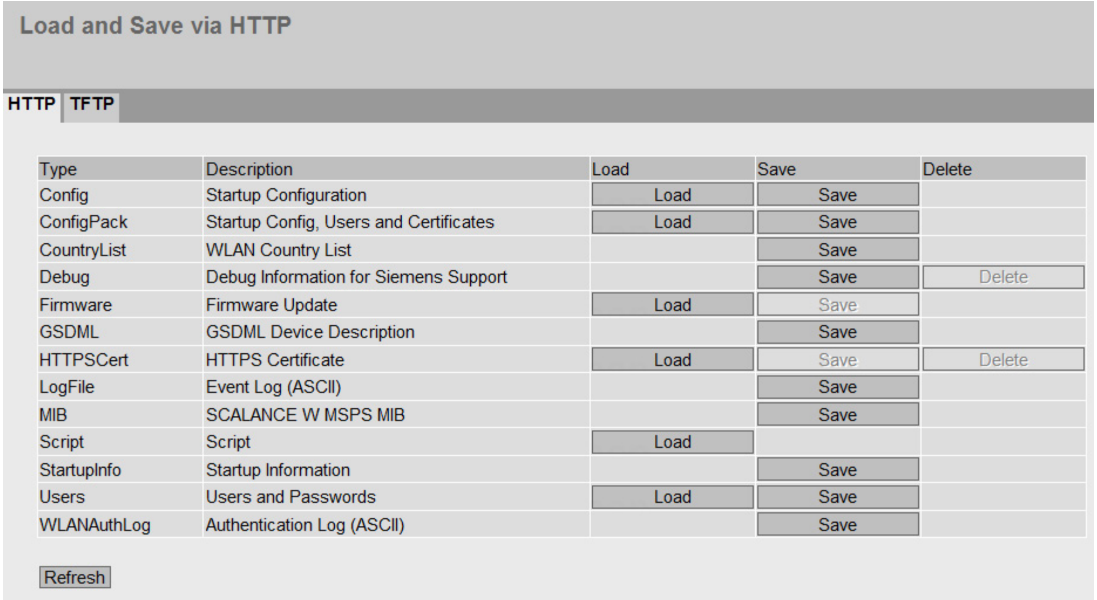
During the installation of a previous version, the configuration data and log files can be lost. In this case, the device starts up with the factory settings after the firmware has been installed. In this situation, if a PLUG is inserted in the device, following the restart, this has the status "Not Accepted" since the PLUG still has the configuration data of the previous more up-to-date firmware. This allows you to return to the previous, more up-to-date firmware without any loss of configuration data.

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

Note

Configuration files and trial mode/Automatic Save mode

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



Load and Save via HTTP

Type	Description	Load	Save	Delete
Config	Startup Configuration	Load	Save	
ConfigPack	Startup Config, Users and Certificates	Load	Save	
CountryList	WLAN Country List		Save	
Debug	Debug Information for Siemens Support		Save	Delete
Firmware	Firmware Update	Load	Save	
GSDML	GSDML Device Description		Save	
HTTPSCert	HTTPS Certificate	Load	Save	Delete
LogFile	Event Log (ASCII)		Save	
MIB	SCALANCE W MSPS MIB		Save	
Script	Script	Load		
StartupInfo	Startup Information		Save	
Users	Users and Passwords	Load	Save	
WLANAuthLog	Authentication Log (ASCII)		Save	

Description

The table has the following columns:

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

Procedure

Loading files using HTTP

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

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

   The file is now loaded.

Whether or not a restart is necessary, depends on the loaded file. If a restart is necessary, a message to this effect will be output. Other files are executed immediately, for example the CLI script file and new settings are applied without 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 will be deleted.

Reusing configuration data

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

Follow the steps below to reuse configuration data:

1. Save the configuration data of a configured device on your PC.
2. 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.

5.5.7.2 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

Incompatibility with predecessor versions

During the installation of a previous version, the configuration data and log files can be lost. In this case, the device starts up with the factory settings after the firmware has been installed.

Incompatibility with previous versions with PLUG inserted

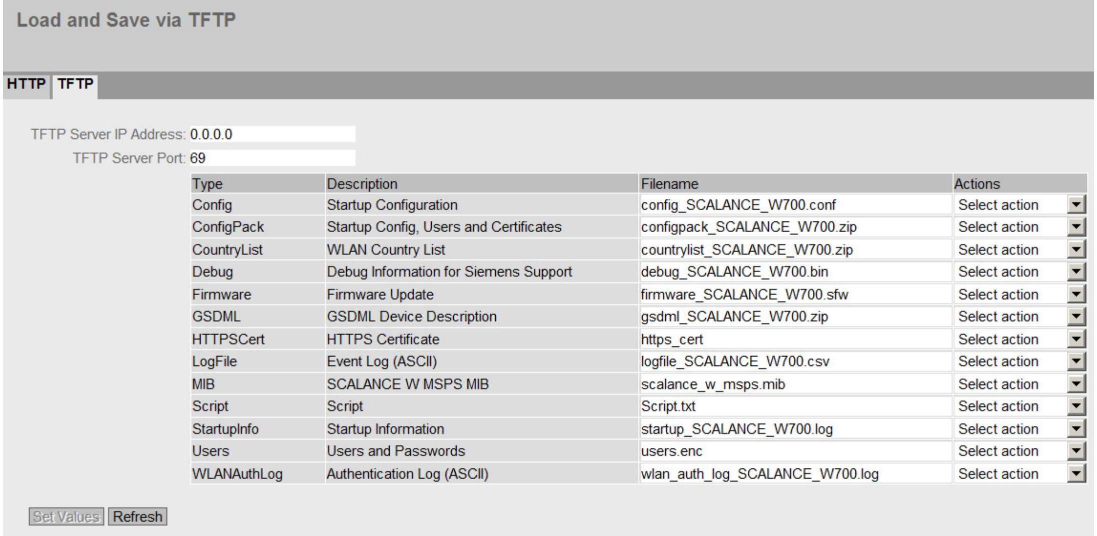
During the installation of a previous version, the configuration data and log files can be lost. In this case, the device starts up with the factory settings after the firmware has been installed. In this situation, if a PLUG is inserted in the device, following the restart, this has the status "Not Accepted" since the PLUG still has the configuration data of the previous more up-to-date firmware. This allows you to return to the previous, more up-to-date firmware without any loss of configuration data.

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

Note

Configuration files and trial mode/Automatic Save mode

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



Load and Save via TFTP

TFTP Server IP Address: 0.0.0.0

TFTP Server Port: 69

Type	Description	Filename	Actions
Config	Startup Configuration	config_SCALANCE_W700.conf	Select action
ConfigPack	Startup Config, Users and Certificates	configpack_SCALANCE_W700.zip	Select action
CountryList	WLAN Country List	countrylist_SCALANCE_W700.zip	Select action
Debug	Debug Information for Siemens Support	debug_SCALANCE_W700.bin	Select action
Firmware	Firmware Update	firmware_SCALANCE_W700.sfw	Select action
GSDML	GSDML Device Description	gsdml_SCALANCE_W700.zip	Select action
HTTPSCert	HTTPS Certificate	https_cert	Select action
LogFile	Event Log (ASCII)	logfile_SCALANCE_W700.csv	Select action
MIB	SCALANCE W MSPS MIB	scalance_w_msps.mib	Select action
Script	Script	Script.txt	Select action
StartupInfo	Startup Information	startup_SCALANCE_W700.log	Select action
Users	Users and Passwords	users.enc	Select action
WLANAuthLog	Authentication Log (ASCII)	wlan_auth_log_SCALANCE_W700.log	Select action

Description

The page contains the following boxes:

- **Input box "TFTP Server IP Address"**
  Here, enter the IP address of the TFTP server with which you 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**
  Shows the file type.
- **Description**
  Shows the short description of the file type.
- **Input box "Filename"**
  Enter a file name.
- **Drop-down list "Actions"**
  Select the action from the drop-down list. The selection depends on the selected file type, for example the log file can only be saved.
  The following actions are possible:
  - **Save file**
    With this selection, you save a file on the TFTP server.
  - **Load file**
    With this selection, you load a file from the TFTP server.

Procedure

Loading or saving data using TFTP

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

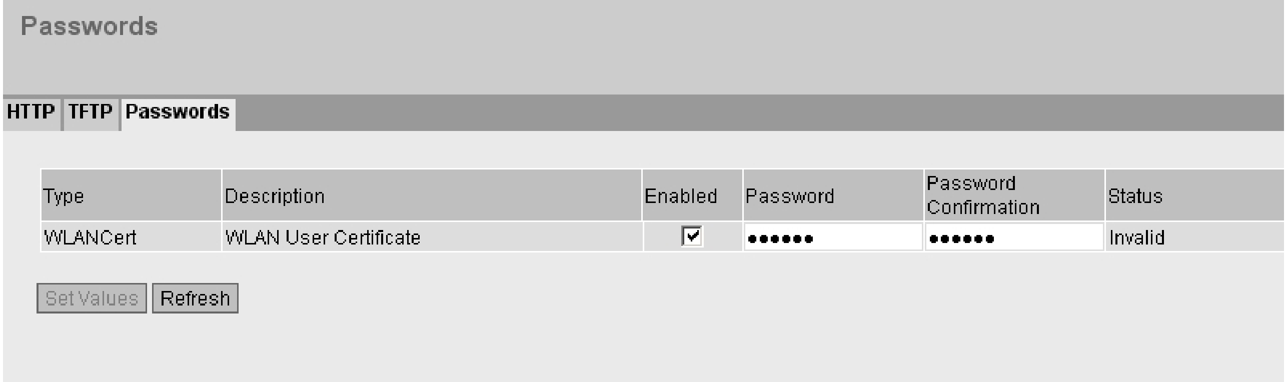
5.5.7.3 Passwords

Password for user certificate

With this menu item, you specify whether the user certificate needs a password.

Note

This tab is only available in the client mode.



Type	Description	Enabled	Password	Password Confirmation	Status
WLANCert	WLAN User Certificate	☑	••••••	••••••	Invalid

Description

The table has the following columns:

- **Type**
  Shows the user certificate
- **Description**
  Shows the short description of the user certificate.
- **Enabled**
  Specifies whether the user certificate needs a password. If you enable the settings, specify the password in "Password".
- **Password**
  Enter the password for the user certificate.

  Note

  When assigning the password, ASCII code 0x20 to 0x7e is used.
- **Password Confirmation**
  Confirm the password.
- **Status**
  Shows whether the current settings for the certificate match the device.
  - **Valid**
    The settings are valid.
  - **Invalid**
    The settings are invalid.

Procedure

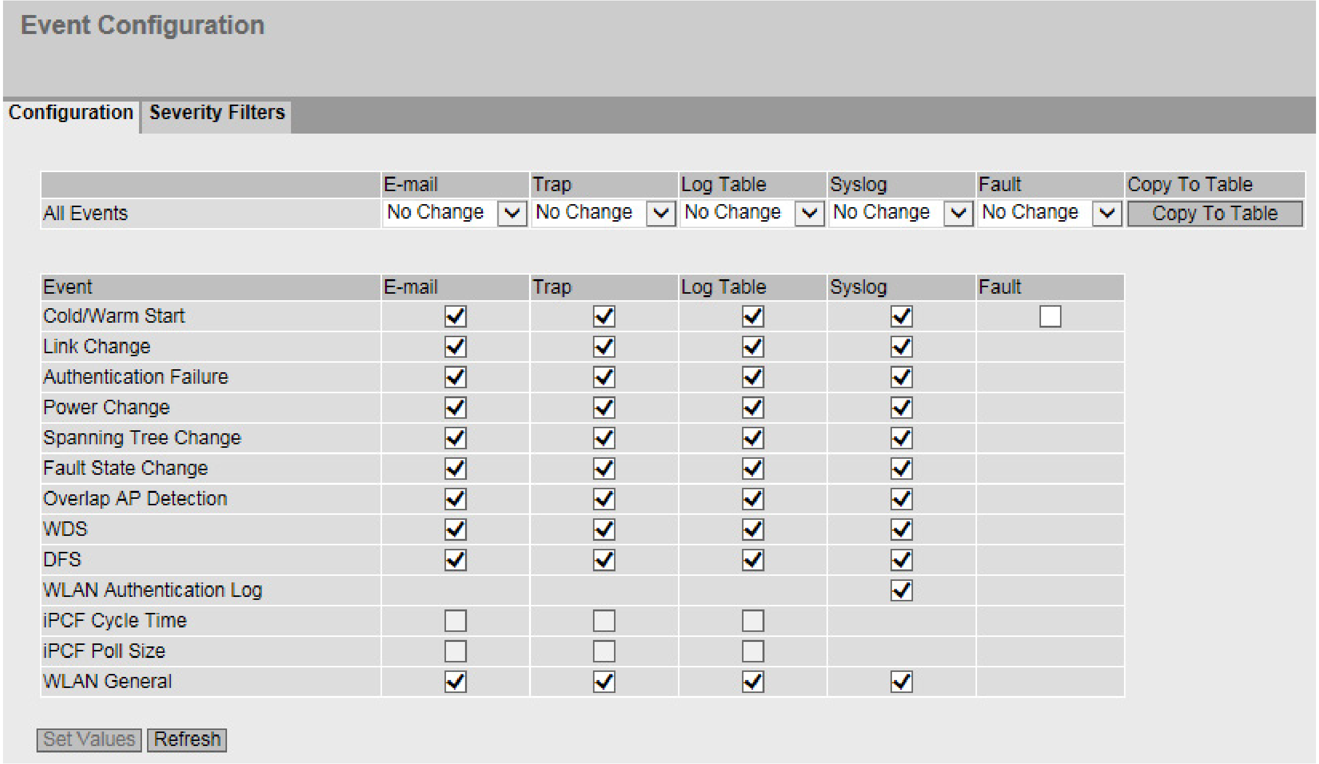
1. Select the "Enabled" option.
2. Enter the password in "Password".
3. To confirm the password, enter the password again in "Password Confirmation".
4. Click the "Set Values" button.

5.5.8 Events

5.5.8.1 Configuration

Selecting system events

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



	E-mail	Trap	Log Table	Syslog	Fault	Copy To Table
All Events	No Change	No Change	No Change	No Change	No Change	Copy To Table

Event	E-mail	Trap	Log Table	Syslog	Fault
Cold/Warm Start	☑	☑	☑	☑	□
Link Change	☑	☑	☑	☑	
Authentication Failure	☑	☑	☑	☑	
Power Change	☑	☑	☑	☑	
Spanning Tree Change	☑	☑	☑	☑	
Fault State Change	☑	☑	☑	☑	
Overlap AP Detection	☑	☑	☑	☑	
WDS	☑	☑	☑	☑	
DFS	☑	☑	☑	☑	
WLAN Authentication Log				☑	
iPCF Cycle Time	□	□	□		
iPCF Poll Size	□	□	□		
WLAN General	☑	☑	☑	☑	

Description

With Table 1, you can enable or disable all check boxes of a column of Table 2 at once. Table 1 has the following columns:

- **Event**
  Shows that the settings are valid for all events of table 2.
- **E-Mail / Trap / Log Table / Syslog / Fault**
  Enable or disable the required type of notification for all events. If "No Change" is selected, the entries of the corresponding column in Table 2 remain unchanged.
- **Copy to Table**
  If you click the button, the setting is adopted for all events of table 2.

Table 2 has the following columns:

- **Event**
  The column contains the following values:
  - **Cold/Warm Start**
    The device was turned on or restarted by the user.
  - **Link Change**
    This event occurs only when the port status is monitored and has changed, see "System > Fault Monitoring > Link Change".
  - **Authentication Failure**
    This event occurs when attempting access with a bad password.
  - **Power Change**
    This event occurs when power supply lines 1 and 2 are monitored. It indicates that there was a change to line 1 or line 2. The event occurs when the PoE power supply has failed, see "System > Fault Monitoring > Power Supply".
  - **Spanning Tree Change**
    The STP or RSTP or MSTP topology has changed.
  - **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.
  - **Overlap AP Detection** (Only in access point mode)
    This event is triggered when there is an entry in the overlap AP list.
  - **WDS** (Only in access point mode)
    The connection status of a WDS link has changed.
  - **DFS** (Only in access point mode)
    This event occurs if a radar signal was received or the DFS scan was started or stopped.
  - **WLAN General** (Only in access point mode)
    This event occurs if a the channel bandwidth has changed.
  - **WLAN Authentication Log**
    Forwarding of the entries from the WLAN Authentication Log to the system protocol server.
  - **WLAN De/Authentication** (Only in client mode)
    With successful or failed WLAN authentication attempts.
  - **iPCF Cycle Time** (Only in access point mode)
    Only available when the KEY-PLUG is inserted.
    This event occurs if too many clients are logged on for the set iPCF cycle time or if some clients were not reached in one cycle.
  - **iPCF Poll Size**
    Only available when the KEY-PLUG is inserted.
    This event occurs if the PNIO data size is too large for transfer.
- **E-Mail**
  The device sends an e-mail. This is only possible if the SMTP server is set up and the "SMTP client" function is enabled.

- **Trap**
  The device sends an SNMP trap. This is only possible if "System > Configuration" SNMPv1 Traps" is enabled.
- **Log Table**
  The device writes an entry in the event log table.
- **Syslog**
  The device writes an entry to the system log server. This is only possible if the system log server is set up and the "Syslog client" function is enabled.
- **Fault**
  The device triggers a fault. The error LED lights up.

Procedure

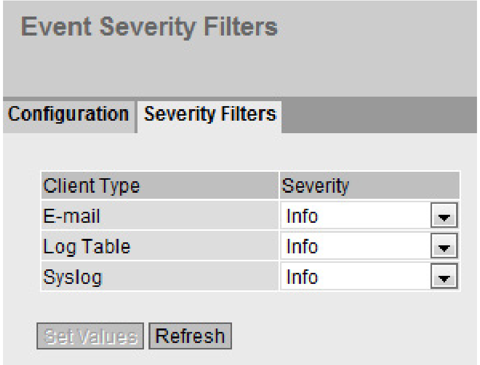
Follow the steps below to change entries:

1. Select the check box in the row of the required event. Select the event in the column under the following actions:
   - E-mail
   - Trap
   - Log table
   - Syslog
   - Fault
2. Click the "Set Values" button.

5.5.8.2 Severity Filter

Setting the severity filter

On this page, set the threshold levels for sending system event notifications.



Event Severity Filters

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

The first table column shows the client type for which you are making the settings:

- **E-Mail**

  Sending system event messages by e-mail
- **Log Table**

  Entry of system events in the log table
- **Syslog**

  Entry of system events in the Syslog file

Select the required level from the drop-down lists of the second table column.

You can select from the following values:

- **Critical**
  System events are processed as of the severity level "Critical".
- **Warning**

  System events are processed as of the severity level "Warning".
- **Info**
  System events are processed as of the severity level "Info".

Procedure

Follow the steps below to configure the required level:

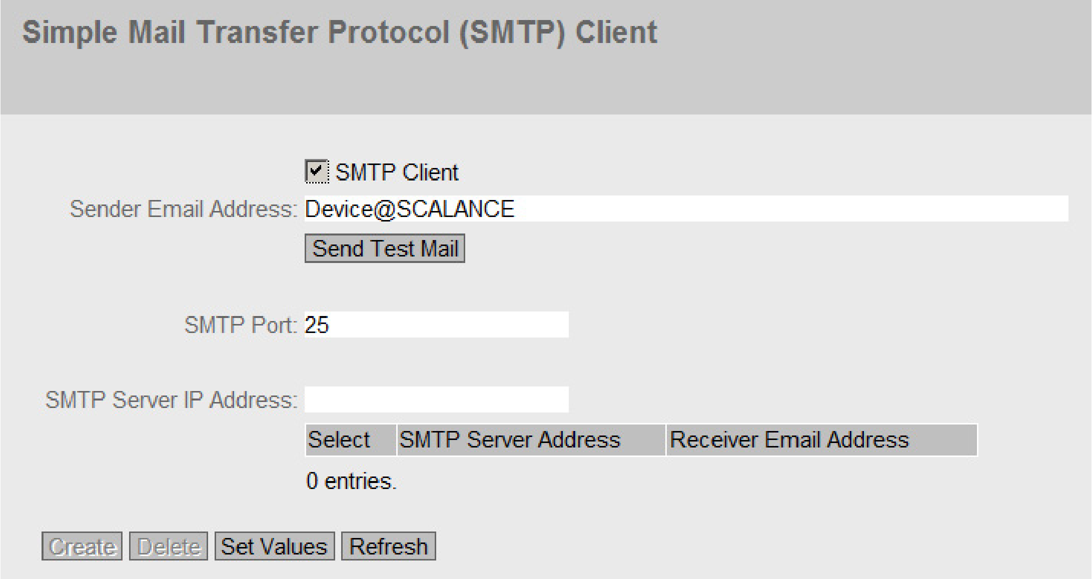
1. Select the required values from the drop-down lists of the second table column after the client types.
2. Click the "Set Values" button.

5.5.9 SMTP Client

Network monitoring with e-mails

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

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



Simple Mail Transfer Protocol (SMTP) Client

☑ SMTP Client

Sender Email Address: Device@SCALANCE

SMTP Port: 25

SMTP Server IP Address:

Select	SMTP Server Address	Receiver Email Address

0 entries.

Description

The page contains the following boxes:

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

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

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

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

  Factory settings: 25

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

This table contains the following columns:

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

Procedure

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

Note

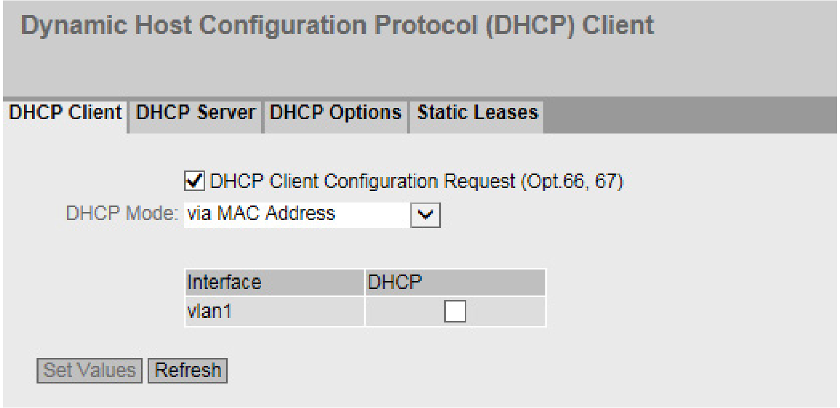
Depending on the properties and configuration of the SMTP server, it may be necessary to adapt the "Sender Email Address” box for the e-mails. Check with the administrator of the SMTP server.

5.5.10 DHCP

5.5.10.1 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 IPv4 address as the response. The server manages an address range from which it assigns IPv4 addresses. It is also possible to configure the server so that the client always receives the same IPv4 address in response to its request.



Dynamic Host Configuration Protocol (DHCP) Client

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

DHCP Mode: via MAC Address

Interface	DHCP
vlan1	□

Description

The page contains the following boxes:

- **"DHCP Client Configuration Request (Opt.66, 67)" check box**
  Select this option if you want the DHCP client to use options 66 and 67 to download and then enable a configuration file.
- **"DHCP Mode" drop-down list**
  Select the DHCP mode from the drop-down list. The following modes are possible:
  - via MAC Address
    Identification is based on the MAC address.
  - via DHCP Client ID
    Identification is based on a freely defined DHCP client ID.
  - via System Name
    Identification is based on the system name. If the system name is 255 characters long, the last character is not used for identification.
  - via PNIO Name of Station
    Identification is based on the PNIO name of the station.

The table has the following columns:

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

Procedure

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

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

Note

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

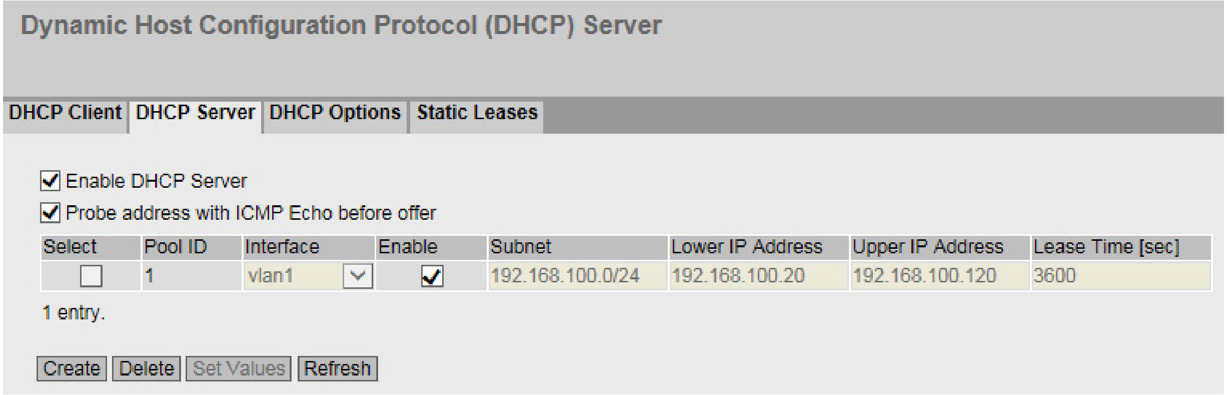
5.5.10.2 DHCP Server

Note

This tab is only available in the client mode.

You can operate the device as a DHCP server. This allows IPv4 addresses to be assigned automatically to the connected devices. The IPv4 addresses are either distributed dynamically from an address band you have specified or a specific IPv4 address (static) can be assigned to a particular device.

On this page, specify the IPv4 address band from which the DHCP client receives any IPv4 address. You configure the static assignment of the IPv4 addresses in "Static Leases".



Dynamic Host Configuration Protocol (DHCP) Server

☑ Enable DHCP Server

☑ Probe address with ICMP Echo before offer

Select	Pool ID	Interface	Enable	Subnet	Lower IP Address	Upper IP Address	Lease Time [sec]
□	1	vlan1	☑	192.168.100.0/24	192.168.100.20	192.168.100.120	3600

1 entry.

Requirements for the DHCP server

- NAT is enabled. You enable NAT in "Layer 3 > NAT".
- The connected devices are configured so that they obtain the IPv4 address from a DHCP server.

Description

The page contains the following boxes:

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

  Note

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

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

  Note

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

The table has the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **Pool ID**
  Shows the number of the IPv4 address band. If you click the "Create" button, a new row with a unique number (Pool ID) is created.

  Note

  Only one Pool ID (ID = 1) can be created.

- **Interface**
  Specify the interface via which the IPv4 addresses are dynamically assigned.
- **Enable**
  Specify whether or not this IPv4 address band will be used.

  Note

  If you enable the IPv4 address band, the tabs "DHCP Options" and "Static Leases" are grayed out and cannot be configured.

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

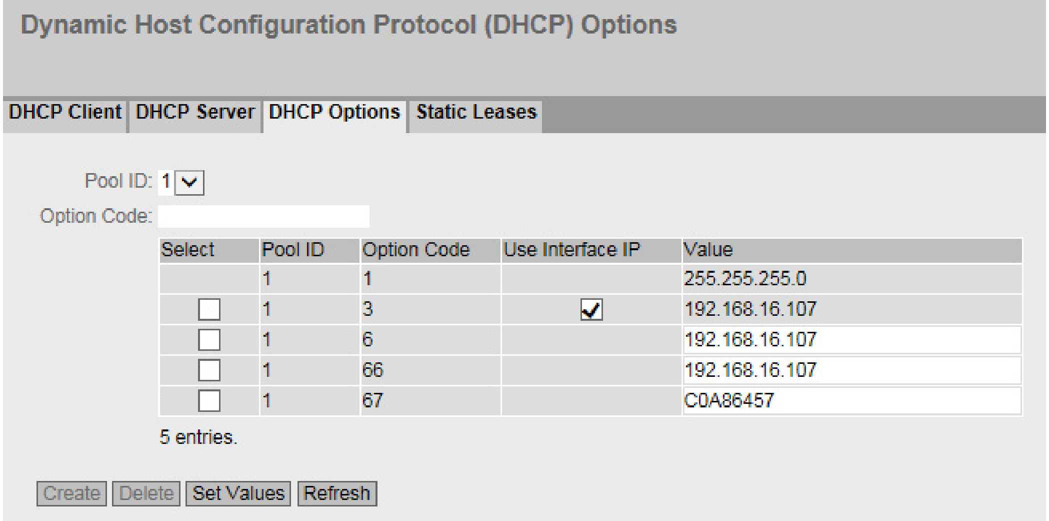
- **Upper IP Address**
  Enter the IPv4 address that specifies the end of the dynamic IPv4 address band. The IPv4 address must be within the network address range you configured for "Subnet".
- **Lease Time [sec]**
  Specify for how many seconds the assigned IPv4 address remains valid. Once this period has elapsed, the device must either request a new IPv4 address or extend the lease time of the existing IPv4 address.

5.5.10.3 DHCP Options

Note

This tab is only available in the client mode.

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



Dynamic Host Configuration Protocol (DHCP) Options

Pool ID: 1

Option Code:

Select	Pool ID	Option Code	Use Interface IP	Value
	1	1		255.255.255.0
□	1	3	☑	192.168.16.107
□	1	6		192.168.16.107
□	1	66		192.168.16.107
□	1	67		C0A86457

5 entries.

Description

The page contains the following boxes:

- **"Pool ID" drop-down list**
  Select the required IPv4 address band.
- **"Option Code" input box**
  Enter the number of the required DHCP option. The various DHCP options are defined in RFC 2132. The DHCP options 1, 3, 6, 66 and 67 are created automatically when the IPv4 address band is created. With the exception of option 1, the options can be deleted.

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

  Note

  DHCP options not supported

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

The table has the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **Pool ID**
  Shows the number of the IPv4 address band.
- **Option Code**
  Shows the number of the DHCP option.
- **Use Interface IP**
  Specify whether or not the internal IPv4 address of the device will be used.
- **Value**
  Enter the DHCP parameter that is transferred to the DHCP client. The content depends on the DHCP option.
  - DHCP option 67 (boot file name)

    Enter the name of the boot file in the string format.
  - DHCP options 3 (router), 6 (DNS) and 66 (TFTP server):

    Enter the DHCP parameter as an IPv4 address, e.g. 192.168.100.2. With the exception of DHCP option 3, you can specify several IPv4 addresses separated by commas.
  - All other DHCP options

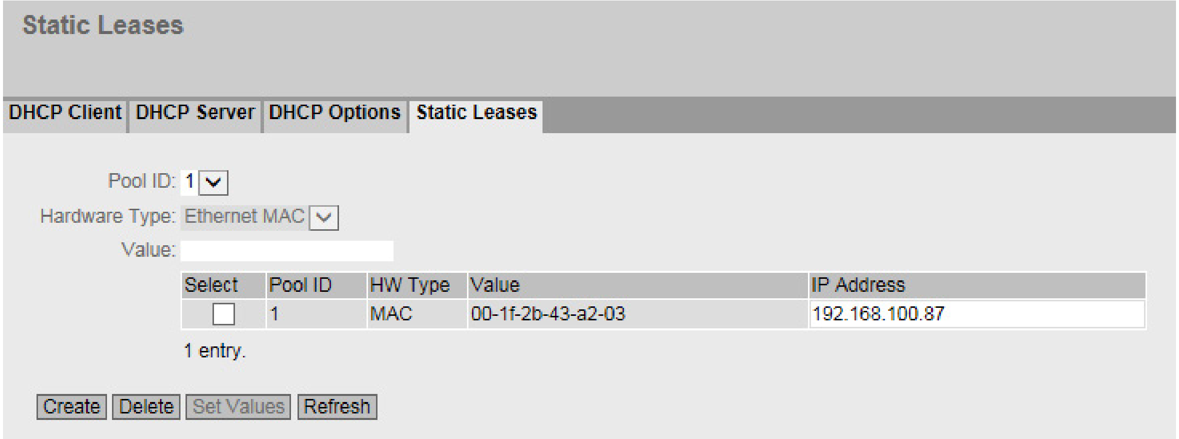
    Enter the DHCP parameter in hexadecimal, e.g. the IPv4 address 192.168.100.2 corresponds to "C0A86402".

5.5.10.4 Static Leases

Note

This tab is only available in the client mode.

On this page you specify that devices with a certain MAC address are assigned to the selected IPv4 address.



Pool ID: 1
Hardware Type: Ethernet MAC
Value:

Select	Pool ID	HW Type	Value	IP Address
□	1	MAC	00-1f-2b-43-a2-03	192.168.100.87

1 entry.

Description

The page contains the following boxes:

- **"Pool ID" drop-down list**
  Select the required IPv4 address band.
- **"Hardware Type" drop-down list**
  Ethernet MAC
  Identification is based on the MAC address. Enter the MAC address in "Value". A MAC address consists of six byes separated by hyphens in hexadecimal notation, e.g. 00-ab-1d-df-b4-1d.
- **"Value" input box**
  Enter the MAC address and click the "Create" button to create the entry. A maximum of 20 entries are possible.

The table has the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **Pool ID**
  Shows the number of the IPv4 address band.

Note

Only Pool ID = 1 is supported.

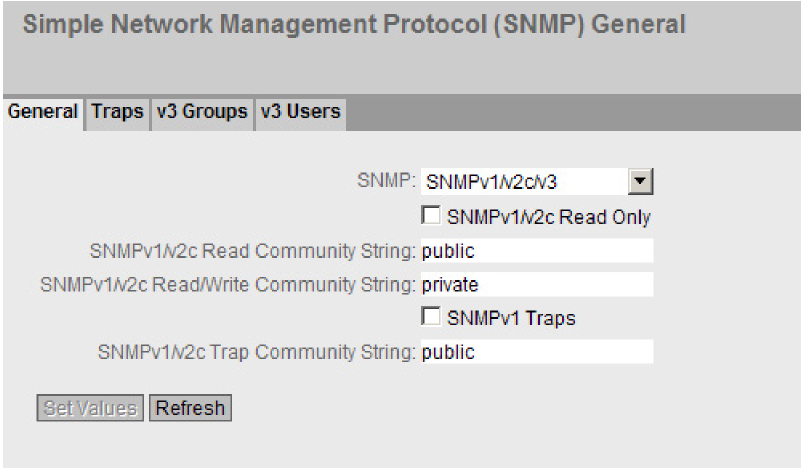
- **HW Type**
  Shows that the IPv4 address depends on the MAC address.
- **Value**
  Shows the MAC address to which the IPv4 address is assigned.
- **IP Address**
  Specify the IPv4 address. The IPv4 address must match the subnet of the IPv4 address band.

5.5.11 SNMP

5.5.11.1 General

Configuration of SNMP

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



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

Description

The page contains the following boxes:

- **"SNMPv1/v2c/v3" drop-down list**
  Select the SNMP protocol from the drop-down list. The following settings are possible:
  - "-" (disabled)
    SNMP is disabled.
  - SNMPv1/v2c/v3
    SNMPv1/v2c/v3 is supported.
  - SNMPv3
    Only SNMPv3 is supported.
- **"SNMPv1/v2c Read Only" check box**
  If you enable this option, SNMPv1/v2c can only read the SNMP variables.

Note

Community String

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

- **"SNMPv1/v2c Read/Write Community String" input box**
  Enter the community string for read and write access of the SNMP protocol.
- **"SNMPv1/v2c Read Community String" input box**
  Enter the community string for access of the SNMP protocol.
- **"SNMPv1 Traps"** check box
  Enable or disable the sending of traps (alarm frames). On the "Trap" tab, specify the IP addresses of the devices to which SNMP traps will be sent.
- **"SNMPv1/v2c Trap Community String" input box**
  Enter the community string for sending SNMPv1/v2 messages.

Procedure

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

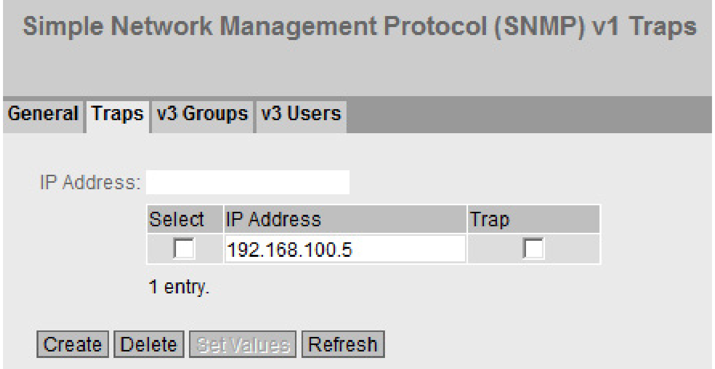
5.5.11.2 Traps

SNMP traps for alarm events

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

Note

Traps are sent only when the "SNMPv1 Traps" option was selected in the "General" or "System > Confguration" tab.



Simple Network Management Protocol (SNMP) v1 Traps

IP Address:

Select	IP Address	Trap
□	192.168.100.5	□

1 entry.

Description

- **IP Address**
  Enter the IP address or the FQDN name of the station to which the device sends SNMP traps. You can specify up to ten different recipients servers.

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **IP Address**
  If necessary, change the IP addresses or the FQDN names of the stations.
- **Trap**
  Enable or disable the sending of traps. Stations that are entered but not selected do not receive SNMP traps.

Procedure

Creating a trap entry

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

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

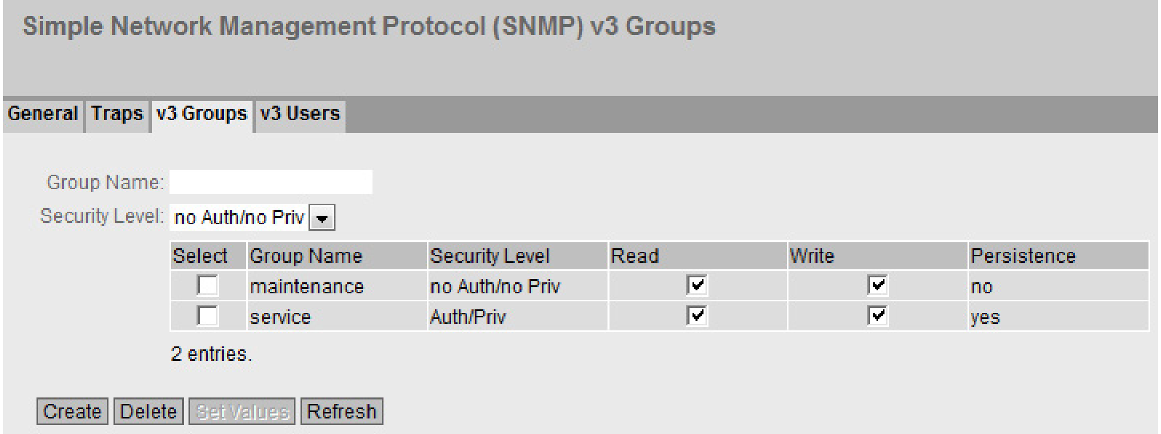
Deleting a trap entry

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

5.5.11.3 v3 Groups

Security settings and assigning permissions

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



Simple Network Management Protocol (SNMP) v3 Groups

Group Name:

Security Level: no Auth/no Priv

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

2 entries.

Description

The page contains the following boxes:

- **Group Name**
  Enter the name of the group. The maximum length is 32 characters.
- **Security Level**
  Select the security level (authentication, encryption) valid for

  the selected group. In the security levels, the following options:
  - No Auth/no Priv
    No authentication enabled, no encryption enabled.
  - Auth/no Priv
    Authentication enabled / no encryption enabled.
  - Auth/Priv
    Authentication enabled / encryption enabled.

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **Group Name**
  Shows the defined group names.
- **Security Level**
  Shows the configured security level.
- **Read**
  Enable or disable read access for the required group.
- **Write**
  Enable or disable wite access for the required group.

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

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

    The group is assigned to an SNMPV3 user.
  - No

    The group is not assigned to an SNMPV3 user.

Procedure

Creating a new group

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

Modifying a group

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

Note

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

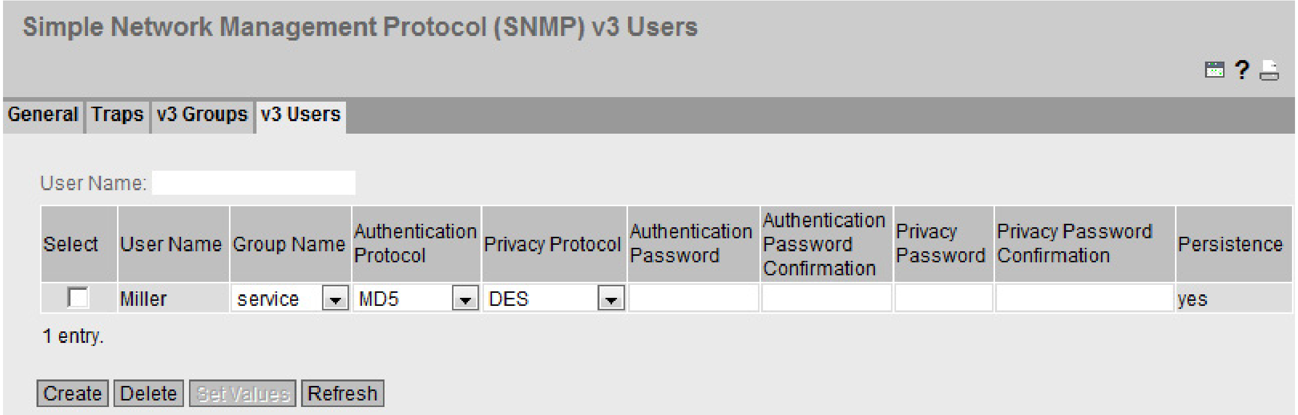
Deleting a group

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

5.5.11.4 v3 Users

User-specific security settings

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



User Name:

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

1 entry.

Description

The page contains the following boxes:

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

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **User Name**
  Shows the created users.
- **Group Name**
  Select the group to which the user will be assigned.
- **Authentication Protocol**
  Specify the authentication protocol. Can only be enabled, if this group supports the function.

  The following settings are available:

  – none

  – MD5

  – SHA
- **Privacy Protocol**
  Specify whether or not the user uses the DES algorithm. Can only be enabled, if the group supports this function.
- **Authentication Password**
  Enter the authentication password in the first input box. This password must have at least 6 characters, the maximum length is 32 characters.
- **Authentication Password Confirmation**
  Confirm the password by repeating the entry.
- **Privacy Password**
  Enter your encryption password. This password must have at least 6 characters, the maximum length is 32 characters.
- **Privacy Password Confirmation**
  Confirm the encryption password by repeating the entry.
- **Persistence**
  Shows whether or not the user is assigned to an SNMPv3 group. If the user is not assigned to an SNMPv3 group, no automatic saving is triggered and the configured user disappears again after restarting the device.

  – Yes

    The user is assigned to an SNMPv3 group.

  – No

    The user is not assigned to an SNMPv3 group.

Procedure

Create a new user

1. Enter the name of the new user in the "User Name" input box.
2. Click the "Create" button. A new entry is generated in the table.
3. In "Groups", select the group to which the new user will belong.

   If the group has not yet been created, change to the "v3 Groups" page and make the settings for this group.
4. If an authentication is necessary for the selected group, select the authentication algorithm in "Authentification Protocol".
   In the relevant input boxes, enter the authentication password and its confirmation.
5. If encryption was specified for the group, select the algorithm from the "Privacy Protocol" drop-down list. In the relevant input boxes, enter the encryption password and the confirmation.
6. Click the "Set Values" button.

Delete user

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

Note

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

5.5.12 System Time

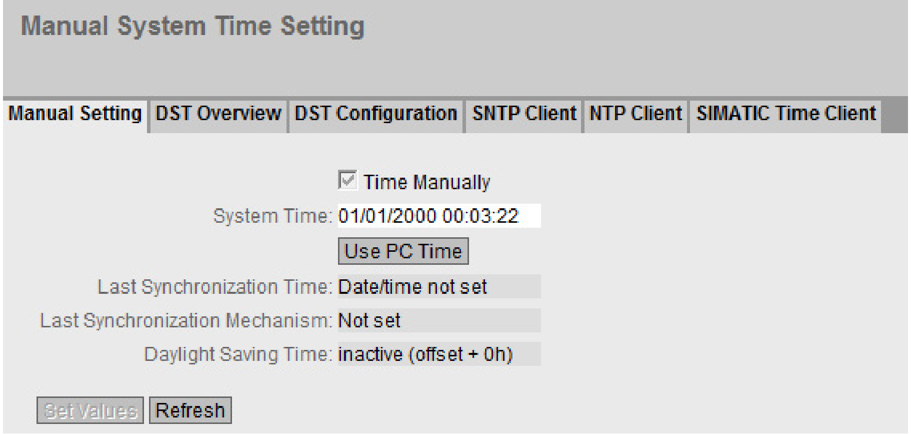
There are different methods that can be used to set the system time of the device. Only one method can be active at any one time.

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

5.5.12.1 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: 01/01/2000 00:03:22

Last Synchronization Time: Date/time not set

Last Synchronization Mechanism: Not set

Daylight Saving Time: inactive (offset + 0h)

Description

The page contains the following boxes:

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

  With the manual time setting, the time of day is stored once a day in the internal memory of the device. This value is set as the system time following a device restart and therefore differs by less than 24 hours from the actual time of day. If the device is reset to the factory settings, the time is set to the value 01/01/2000 00:00:00.
- **Use PC Time**
  Click the button to use the time setting of the PC.
- **Last Synchronization Time**
  This box is read-only and shows when the last time-of-day synchronization took place. If no time-of-day synchronization was possible, the box displays "Date/time not set".

- **Last Synchronization Mechanism**
  This box displays how the last time-of-day synchronization was performed.
  - Not set
    The system time was not set.
  - Manual
    Manual time setting
  - SNTP
    Automatic time-of-day synchronization with SNTP
  - NTP
    Automatic time-of-day synchronization with NTP
  - SIMATIC
    Automatic time-of-day synchronization using the SIMATIC time frame
- **Daylight Saving Time**
  Shows whether the daylight saving time changeover is active:
  - active (+1 hour)
    The time in "Current System Time" is daylight saving time.
  - inactive (+0 hours)
    The time in "Current System Time" is not daylight saving time.

Procedure

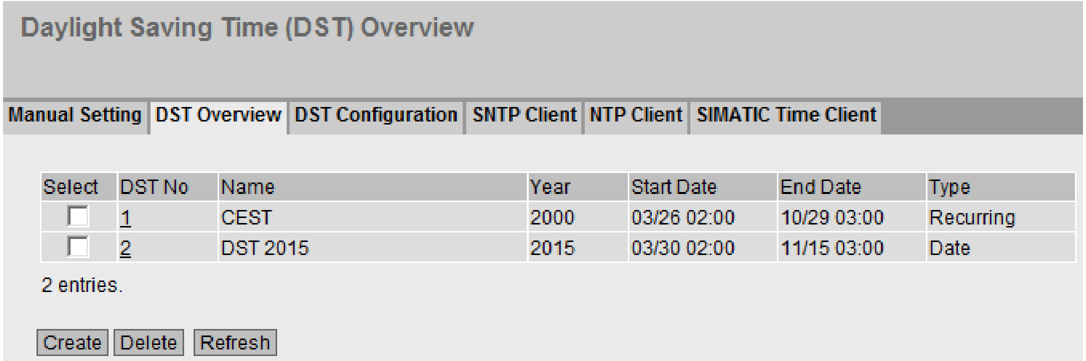
1. Enable the "Time Manually" option.
2. Click in the "System Time" input box.
3. In the "System Time" input box, enter the date and time in the format "MM/DD/YYYY HH:MM:SS".
4. Click the "Set Values" button.
   The date and time are adopted and "Manual" is entered in the "Last Synchronization Mechanism" box.

5.5.12.2 DST Overview

On this page, you can create new entries for the daylight saving time changeover.

The table provides an overview of the existing entries.

Settings



Select	DST No	Name	Year	Start Date	End Date	Type
□	1	CEST	2000	03/26 02:00	10/29 03:00	Recurring
□	2	DST 2015	2015	03/30 02:00	11/15 03:00	Date

2 entries.

Figure 5-2 DST Overview

- **Select**

  Select the row you want to delete.
- **DST No.**

  Shows the number of the entry.

  If you create a new entry, a new line with a unique number is created.
- **Name**

  Shows the name of the entry.
- **Year**

  Shows the year for which the entry was created.
- **Start Date**

  Shows the month, day and time for the start of daylight saving time.
- **End Date**

  Shows the month, day and time for the end of daylight saving time.
- **Type**

  Shows how the daylight saving time changeover is made:

  – Date

    A fixed date is entered for the daylight saving time changeover.

  – Recurring

    A rule was defined for the daylight saving time changeover.

5.5.12.3 DST Configuration

On this page, you can configure the entries for the daylight saving time changeover. As result of the changeover to daylight saving or standard time, the system time for the local time zone is correctly set.

You can define a rule for the daylight saving time changeover or specify a fixed date.

Settings

Note

The content of this page depends on the selection in the "Type" box.

The boxes "DST No.", "Type" and "Name" are always displayed.

- **DST No.**

  Select the type of the entry.
- **Type**
  Select how the daylight saving time changeover is made:
  - Date

    You can set a fixed date for the daylight saving time changeover.

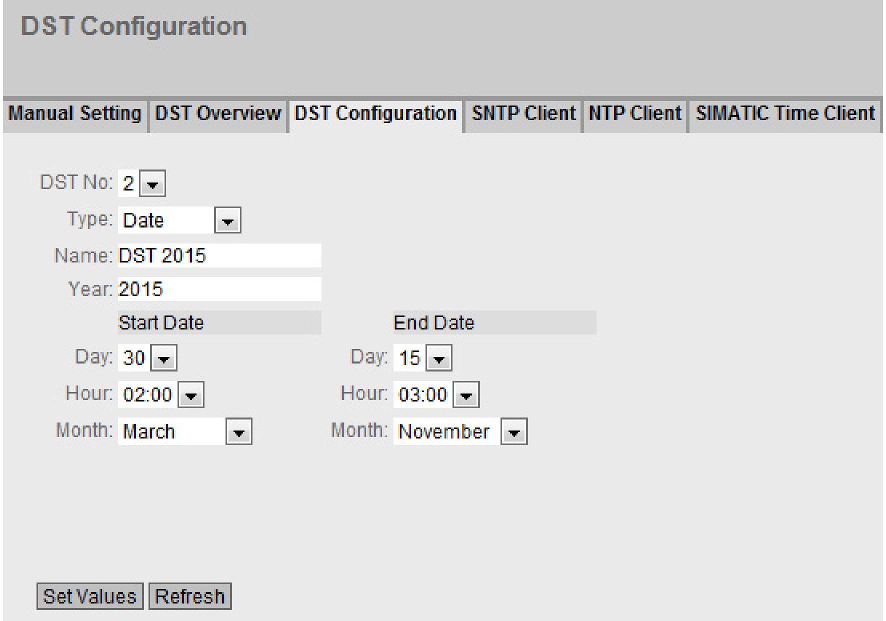
    This setting is suitable for regions in which the daylight saving time changeover is not governed by rules.
  - Recurring

    You can define a rule for the daylight saving time changeover.

    This setting is suitable for regions in which the daylight saving time always begins or ends on a certain weekday.
- **Name**

  Enter a name for the entry.

Settings with "Date" selected



DST Configuration

DST No: 2

Type: Date

Name: DST 2015

Year: 2015

	Start Date		End Date
Day:	30	Day:	15
Hour:	02:00	Hour:	03:00
Month:	March	Month:	November

Figure 5-3 DST Configuration Date

You can set a fixed date for the start and end of daylight saving time.

- **Year**

  Enter the year for the daylight saving time changeover.

- **Start Date**

  Enter the following values for the start of daylight saving time:

  – Day

    Specify the day.

  – Hour

    Specify the hour.

  – Month

    Specify the month.

- **End Date**

  Enter the following values for the end of daylight saving time:

  – Day

    Specify the day.

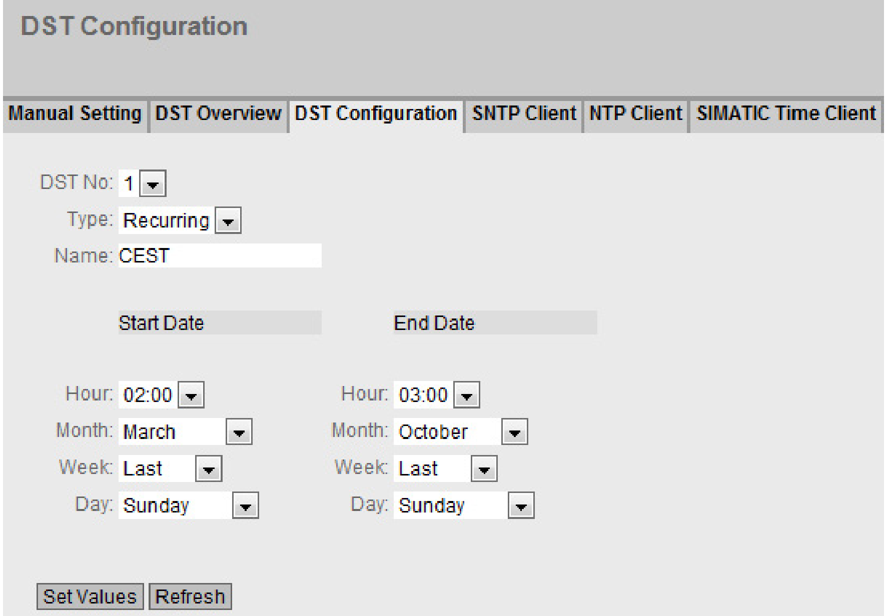
  – Hour

    Specify the hour.

  – Month

    Specify the month.

Settings with "Recurring" selected



DST Configuration

DST No: 1
Type: Recurring
Name: CEST

Start Date
Hour: 02:00
Month: March
Week: Last
Day: Sunday

End Date
Hour: 03:00
Month: October
Week: Last
Day: Sunday

Figure 5-4 DST Configuration Recurring

You can create a rule for the daylight saving time changeover.

- **Start Date**

  Enter the following values for the start of daylight saving time:

  – Hour

    Specify the hour.

  – Month

    Specify the month.

  – Week

    Specify the week.

    You can select the 1st to 5th or the last week of the month.

  – Weekday

    Specify the weekday.

- **End Date**

  Enter the following values for the end of daylight saving time:

  – Hour

    Specify the hour.

  – Month

    Specify the month.

  – Week

    Specify the week.

    You can select the 1st to 5th or the last week of the month.

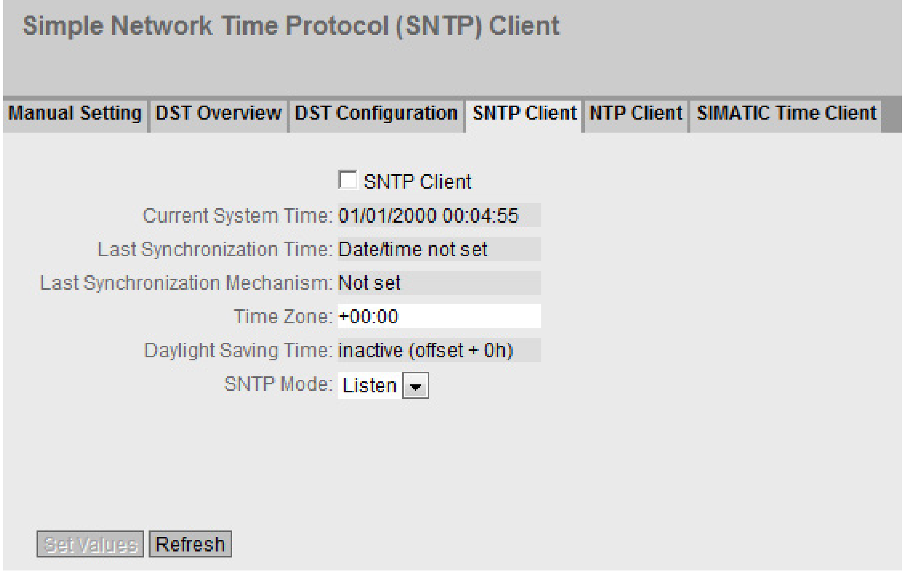
  – Weekday

    Specify the weekday.

5.5.12.4 SNTP Client

Time-of-day synchronization in the network

SNTP (**Simple Network Time Protocol**) is used for synchronizing the time in the network. The appropriate frames are sent by an SNTP server in the network.



□ SNTP Client

Current System Time: 01/01/2000 00:04:55

Last Synchronization Time: Date/time not set

Last Synchronization Mechanism: Not set

Time Zone: +00:00

Daylight Saving Time: inactive (offset + 0h)

SNTP Mode: Listen

Description

The page contains the following boxes:

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

- **Last Synchronization Mechanism**
  This box displays how the last time-of-day synchronization was performed. The following methods are possible:
  - Not set
    The system time was not set.
  - Manual
    Manual time setting
  - SNTP
    Automatic time-of-day synchronization with SNTP
  - NTP
    Automatic time-of-day synchronization with NTP
  - SIMATIC
    Automatic time-of-day synchronization using the SIMATIC time frame
- **Daylight Saving Time**
  Shows whether the daylight saving time changeover is active:
  - active (+1 hour)
    The time in "Current System Time" is daylight saving time.
  - inactive (+0 hours)
    The time in "Current System Time" is not daylight saving time.
- **Time Zone**
  Enter the time zone you are using in the format "+/- HH:MM". The time zone relates to UTC standard world time. Settings for daylight-saving and standard time are taken into account in this box by specifying the time offset.
- **SNTP Mode**
  Select the synchronization mode from the drop-down list. The following types of synchronization are possible:
  - Poll
    If you select this protocol type, the input boxes "SNTP Server IP Address", "SNTP Server Port" and "Poll Interval(s)" are displayed for further configuration. With this type of synchronization, the device is active and sends a time query to the SNTP server.
  - Listen
    With this type of synchronization, the device is passive and "listens" for SNTP frames that deliver the time of day.
- **SNTP Server IP Address**
  Enter the IP address or the FQDN name of the SNTP server.
- **SNTP Server Port**
  Enter the port of the SNTP server.
  The following ports are possible:
  - 123 (standard port)
  - 1025 to 36564
- **Poll Interval(s)**
  Here, enter the interval between two-time queries. In this box, you enter the query interval in seconds. Possible values are 16 to 16284 seconds.

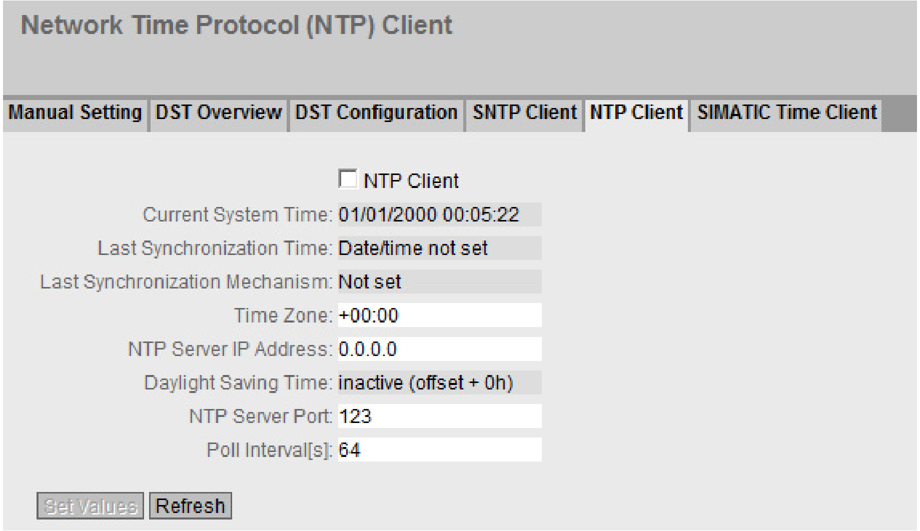
Procedure

1. Click the "SNTP Client" check box to enable the automatic time setting.
2. In 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 or the FQDN name 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 or the FQDN name 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.

5.5.12.5 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.



☐ NTP Client

Current System Time: 01/01/2000 00:05:22
Last Synchronization Time: Date/time not set
Last Synchronization Mechanism: Not set
Time Zone: +00:00
NTP Server IP Address: 0.0.0.0
Daylight Saving Time: inactive (offset + 0h)
NTP Server Port: 123
Poll Interval[s]: 64

Description

The page contains the following boxes:

- **NTP Client**
  Select this check box to enable automatic time-of-day synchronization with NTP.
- **Current System Time**
  This box displays the current system time.
- **Last Synchronization Time**
  This box is read-only and shows when the last time-of-day synchronization took place.
- **Last Synchronization Mechanism**
  This box displays how the last time-of-day synchronization was performed. The following methods are possible:
  - Not set
    The system time was not set.
  - Manual
    Manual time setting
  - SNTP
    Automatic time-of-day synchronization with SNTP
  - NTP
    Automatic time-of-day synchronization with NTP
  - SIMATIC
    Automatic time-of-day synchronization using the SIMATIC time frame

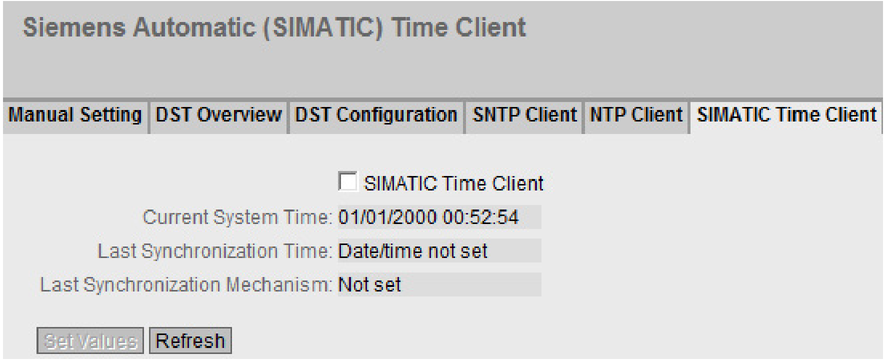
- **Daylight Saving Time**
  Shows whether the daylight saving time changeover is active:
  - active (+1 hour)
    The time in "Current System Time" is daylight saving time.
  - inactive (+0 hours)
    The time in "Current System Time" is not daylight saving time.
- **Time Zone**
  In this box, enter the time zone you are using in the format "+/- HH:MM". The time zone relates to UTC standard world time. Settings for daylight-saving and standard time are taken into account in this box by specifying the time offset.
- **NTP Server IP Address**
  Enter the IP address or the FQDN name of the NTP server.
- **NTP Server Port**
  Enter the port of the NTP server.
  The following ports are possible:
  - 123 (standard port)
  - 1025 to 36564
- **Poll Interval(s)**
  Here, enter the interval between two-time queries. In this box, you enter the query interval in seconds. Possible values are 64 to 1024 seconds.

Procedure

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

5.5.12.6 SIMATIC Time Client

Time setting via SIMATIC time client


Siemens Automatic (SIMATIC) Time Client

□ SIMATIC Time Client

Current System Time: 01/01/2000 00:52:54

Last Synchronization Time: Date/time not set

Last Synchronization Mechanism: Not set

Description

The page contains the following boxes:

- **SIMATIC Time Client**
  Select this check box to enable the device as a SIMATIC time client.
- **Current System Time**
  This box displays the current system time.
- **Last Synchronization Time**
  This box is read-only and shows when the last time-of-day synchronization took place.
- **Last Synchronization Mechanism**
  This box displays how the last time-of-day synchronization was performed. The following methods are possible:
  - Not set
    The system time was not set.
  - Manual
    Manual time setting
  - SNTP
    Automatic time-of-day synchronization with SNTP
  - NTP
    Automatic time-of-day synchronization with NTP
  - SIMATIC
    Automatic time-of-day synchronization using the SIMATIC time frame

Procedure

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

5.5.13 Auto Logout

Setting the automatic logout

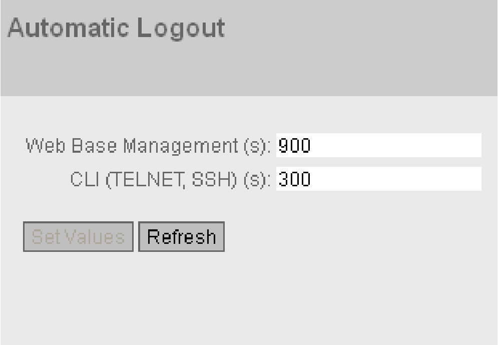
On this page, set the times after which there is an automatic logout from WBM or the CLI following user in activity.

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

Note

No automatic logout from the CLI

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



Automatic Logout

Web Base Management (s): 900

CLI (TELNET, SSH) (s): 300

Procedure

1. Enter a value of 60-3600 seconds in the "Web Base Management (s)" input box. If you enter the value 0, the automatic logout is disabled.
2. Enter a value of 60-600 seconds in the "CLI (TELNET, SSH) (s)" input box. If you enter the value 0, the automatic logout is disabled.
3. Click the "Set Values" button.

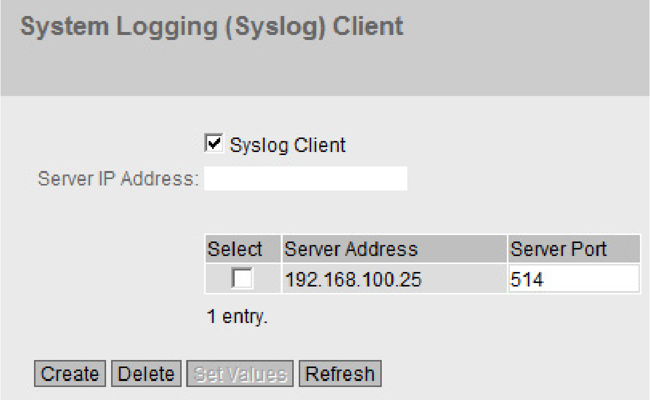
5.5.14 Syslog Client

System event agent

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

Requirements for sending log entries:

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



System Logging (Syslog) Client

☑ Syslog Client

Server IP Address:

Select	Server Address	Server Port
□	192.168.100.25	514

1 entry.

Description

The page contains the following boxes:

- **Syslog Client**
  Enable or disable the Syslog function.
- **Server IP Address**
  Enter the IP address or the FQDN name of the Syslog server.

This table contains the following columns

- **Select**
  Select the row you want to delete.
- **Server Address**
  Shows the IP address or the FQDN name of the Syslog server.
- **Server Port**
  Enter the port of the Syslog server being used.

Procedure

Enabling function

1. Select the "Syslog Client" check box.
2. Click the "Set Values" button.

Creating a new entry

1. In the "Server IP Address" input box, enter the IP address or the FQDN name of the Syslog server on which the log entries will be saved.
2. Click the "Create" button. A new row is inserted in the table.
3. In the "Server Port" input box, enter the number of the UDP port of the server.
4. Click the "Set Values" button.

Note

The default setting of the server port is 514.

Changing the entry

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

Deleting an entry

1. Select the check box in the row to be deleted.
2. Click the "Delete" button. All selected entries are deleted and the display is refreshed.

5.5.15 Fault Monitoring

5.5.15.1 Power Supply

Settings for monitoring the power supply

Configure whether or not the power supply should be monitored by the messaging system. Depending on the hardware variant there are one or two power connectors (Line 1 / Line 2) and a PoE power supply. 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 a monitored line (Line 1, Line 2 or PoE) or when the applied voltage is too low.

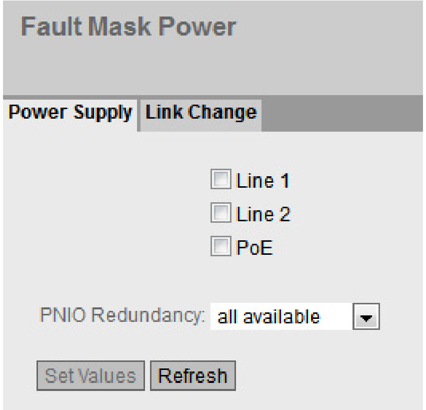
Note

You will find the permitted operating voltage limits in the operating instructions of the device.

A fault causes the signaling contact to trigger and the fault LED on the device to light up and, depending on the configuration, can trigger a trap, an e-mail, or an entry in the event log table.

Note

This WBM page is not available on the SCALANCE W786-2 SFP.



□ Line 1
□ Line 2
□ PoE

PNIO Redundancy: all available

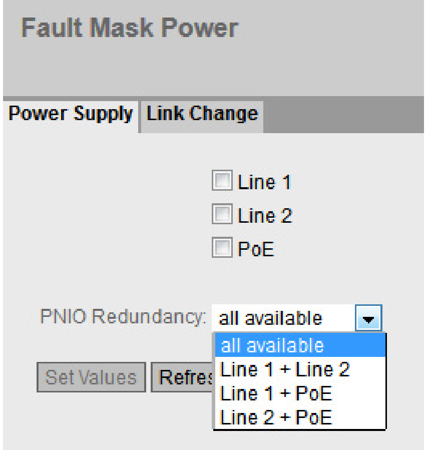
Procedure

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

Monitoring of the redundant power supply by PNIO

With the following devices, you can also configure which power supply will be monitored by PNIO:

- SCALANCE W788-x (RJ-45 variants)
- SCALANCE W748-1 RJ-45
- SCALANCE W774-1 (RJ-45 and M12 variant)
- SCALANCE W734-1 RJ-45


Fault Mask Power

Power Supply | Link Change

□ Line 1
□ Line 2
□ PoE

PNIO Redundancy: all available

Procedure

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

5.5.15.2 Link Change

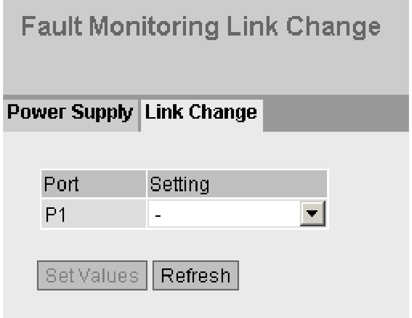
Configuration of fault monitoring of status changes on connections

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

If connection monitoring is enabled, an error is signaled

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

A fault causes the signaling contact to trigger and the fault LED on the device to light up and, depending on the configuration, can trigger a trap, an e-mail, or an entry in the event log table.



Fault Monitoring Link Change

Port	Setting
P1	-

Description

The table has the following columns:

- **Port**
  Shows the available ports.
- **Setting**
  Select the setting from the drop-down list. You have the following options:
  - Up
    Error handling is triggered when the port changes to the active status.

    (From "Link down" to "Link up")
  - Down
    Error handling is triggered when the port changes to the inactive status.

    (From "Link up" to "Link down")
  - "-" (disabled)
    The error handling is not triggered.

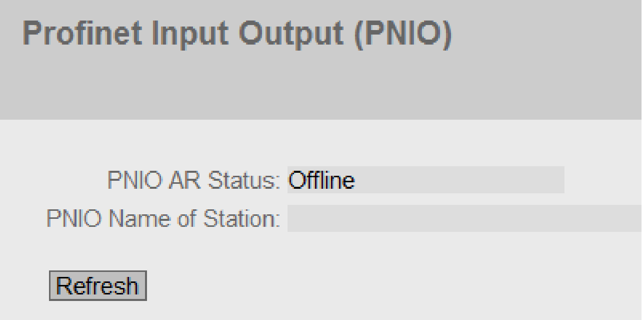
Procedure

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.

5.5.16 PNIO

Settings for PROFINET IO

This page shows the PROFINET IO AR status and the device name.



Profinet Input Output (PNIO)

PNIO AR Status: Offline

PNIO Name of Station:

Description of the displayed boxes

The page contains the following boxes:

- **PNIO AR Status**
  This box shows the status of the PROFINET IO connection; in other words whether the device is connected to a PROFINET IO controller "Online " or "Offline".
  Here, online means that a connection to a PROFINET IO controller exists, that this has downloaded its configuration data to the device and that the device can send status data to the PROFINET IO controller. In this status known as "in data exchange", the parameters set with the PROFINET IO controller cannot be configured.
- **PNIO Name of Station**
  This box displays the PROFINET IO device name according to the configuration in HW Config of STEP 7.

Note

Devices with two Ethernet ports

With devices that have two Ethernet ports, only port P1 should be used for the PNIO configuration because LLPD frames can only be sent and received via port 1. They are blocked at port 2 and are also not forwarded between the ports. This applies to the following devices:

- SCALANCE W786-2 SFP
- SCALANCE W774-1 RJ-45
- SCALANCE W774-1 M12 EEC
- SCALANCE W734-1 RJ-45

SCALANCE W700 and STEP 7

The Ethernet interface can be configured in STEP 7 if the following requirements are met:

- STEP 7 V13 Update 3 with HSP0107 or
- STEP7 version 5.5.4 with GSDML version 2.31

The diagnostics functions can also be used. The WLAN interface cannot be configured with STEP 7.

PNIO for client devices

If a client is to be used as a PNIO device, the MAC address of the client must be specified as follows (MAC Mode):

- **Own**
  In the network beyond the device, only IP communication and no PNIO is possible.
- **Layer 2 Tunnel**
  The client and the devices downstream from it can be used as PNIO devices.

Note

If "Automatic" or "Manual" is configured as the MAC mode for a client, this device cannot be used as a PNIO device.

5.5.17 PLUG

5.5.17.1 Configuration

NOTICE

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

A PLUG may only be removed or inserted when the device is turned off.

The device checks whether or not a PLUG is inserted at one second intervals. If it is detected that the PLUG was removed, there is a restart. If a valid KEY-PLUG was inserted in the device, the device changes to a defined error state following the restart. With SCALANCE W, the available wireless interfaces are deactivated in this case.

If the device was configured at some time with a PLUG, the device can no longer be used without this PLUG. To be able to use the device again, reset the device to the factory settings.

Information about the configuration of the C-PLUG / KEY-PLUG

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

Note

The action is only executed after you click the "Set Values" button.

The action cannot be undone.

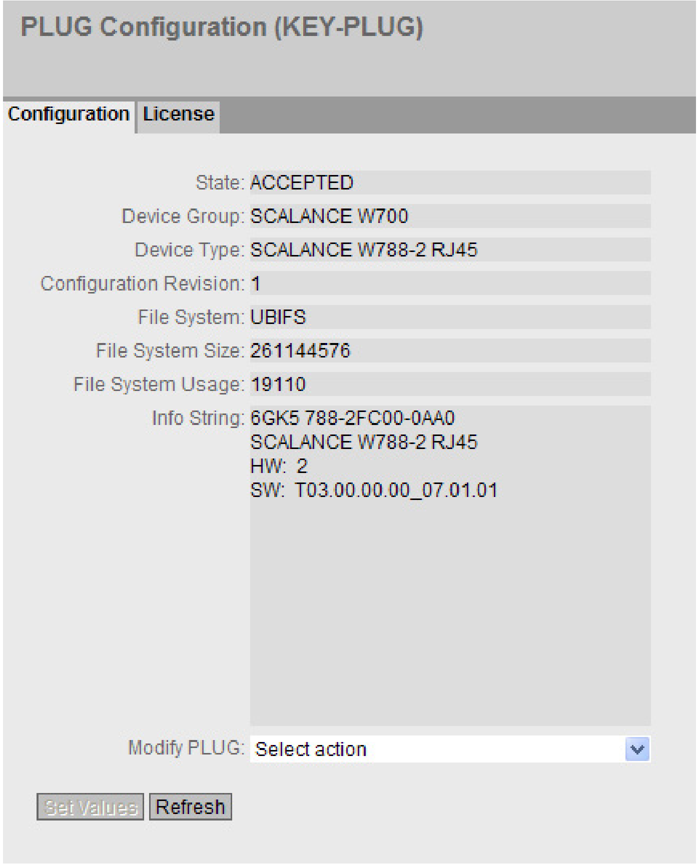
If you decide against executing the function after making your selection, click the "Refresh" button. As a result the data of this page is read from the device again and the selection is canceled.

Note

Incompatibility with previous versions with PLUG inserted

During the installation of a previous version, the configuration data can be lost. In this case, the device starts up with the factory settings after the firmware has been installed. In this situation, if a PLUG is inserted in the device, following the restart, this has the status "Not Accepted" since the PLUG still has the configuration data of the previous more up-to-date firmware. This allows you to return to the previous, more up-to-date firmware without any loss of configuration data.

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



PLUG Configuration (KEY-PLUG)

State: ACCEPTED

Device Group: SCALANCE W700

Device Type: SCALANCE W788-2 RJ45

Configuration Revision: 1

File System: UBIFS

File System Size: 261144576

File System Usage: 19110

Info String: 6GK5 788-2FC00-0AA0
SCALANCE W788-2 RJ45
HW: 2
SW: T03.00.00.00_07.01.01

Modify PLUG: Select action

Description

The table has the following rows:

- **State**
  Shows the status of the PLUG. The following are possible:
  - ACCEPTED
    There is a PLUG with a valid and suitable configuration in the device.
  - NOT ACCEPTED
    Invalid or incompatible configuration on the inserted PLUG.
  - NOT PRESENT
    There is no C-PLUG or KEY-PLUG inserted in the device.
  - FACTORY
    PLUG is inserted and does not contain a configuration. This status is also displayed when the PLUG was formatted during operation.
  - MISSING
    There is no PLUG inserted. Functions are configured on the device for which a license is required.
- **Device Group**
  Shows the SIMATIC NET product line that used the C-PLUG or KEY-PLUG previously.

- **Device Type**
  Shows the device type within the product line that used the C-PLUG or KEY-PLUG previously.
- **Configuration Revision**
  The version of the configuration structure. This information relates to the configuration options supported by the device and has nothing to do with the concrete hardware configuration. This revision information does not therefore change if you add or remove additional components (modules or extenders), it can, however, change if you update the firmware.
- **File System**
  Displays the type of file system on the PLUG.

NOTICE
New file system UBI
As of SCALANCE W firmware version 2.0, UBI is the standard file system for the C-PLUG or KEY-PLUG. If a C-PLUG with the previous file system IECP is detected in such a device, this C-PLUG will be formatted for the UBI file system and the data will be rewritten to the C-PLUG. The file system is also changed following a firmware update to V2.0 with SCALANCE W. A downgrade to the previous version of the corresponding software is then a problem. The firmware can neither read nor write the C-PLUG or KEY-PLUG and it is not even possible to "Erase PLUG to Factory Default".

- **File System Size [Byte]**
  Displays the maximum storage capacity of the file system on the PLUG.
- **File System Usage [Byte]**
  Displays the memory utilization of the file system of the PLUG.
- **Info String**
  Shows additional information about the device that used the PLUG previously, for example, order number, type designation, and the versions of the hardware and software. The displayed software version corresponds to the version in which the configuration was last changed. With the "NOT ACCEPTED" status, further information on the cause of the problem is displayed.
- **"Modify PLUG" drop-down list**
  Select the setting from the drop-down list. You have the following options for changing the configuration on the C-PLUG or KEY-PLUG:
  - Write current configuration to PLUG
    This option is available only if the status of the PLUG is "NOT ACCEPTED" or "FACTORY".
    The configuration in the internal flash memory of the device is copied to the PLUG.
  - Erase PLUG to factory default
    Deletes all the data from the PLUG and runs a low-level formatting function.

Procedure

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

5.5.17.2 License

NOTICE

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

A PLUG may only be removed or inserted when the device is turned off.
The device checks whether or not a PLUG is present at one second intervals. If it is detected that the PLUG was removed, there is a restart. If a valid KEY-PLUG was inserted in the device, the device changes to a defined error state following the restart. With SCALANCE W, the available wireless interfaces are deactivated in this case.

If the device was configured at some time with a PLUG, the device can no longer be used without this PLUG. To be able to use the device again, reset the device to the factory settings.

Note

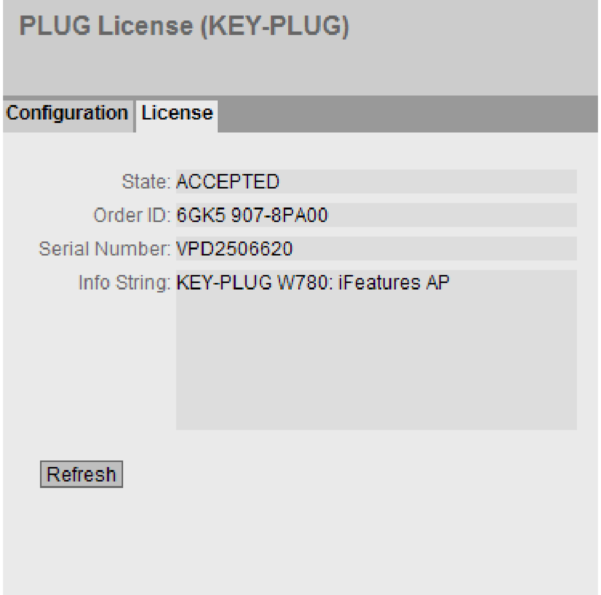
Incompatibility with previous versions with PLUG inserted

During the installation of a previous version, the configuration data can be lost. In this case, the device starts up with the factory settings after the firmware has been installed. In this situation, if a PLUG is inserted in the device, following the restart, this has the status "Not Accepted" since the PLUG still has the configuration data of the previous more up-to-date firmware. This allows you to return to the previous, more up-to-date firmware without any loss of configuration data.

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

Information about the license of the KEY-PLUG

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



PLUG License (KEY-PLUG)

State: ACCEPTED
Order ID: 6GK5 907-8PA00
Serial Number: VPD2506620
Info String: KEY-PLUG W780: iFeatures AP

Description of the displayed boxes

- **State**
  Shows the status of the KEY-PLUG. The following are possible:
  - ACCEPTED
    The KEY-PLUG in the device contains a suitable and valid license.
  - NOT ACCEPTED
    The license of the inserted KEY-PLUG is not valid.
  - NOT PRESENT
    No KEY-PLUG is inserted in the device.
  - MISSING
    There is no KEY-PLUG or a C-PLUG with the status "FACTORY" inserted in the device. Functions are configured on the device for which a license is required.
  - WRONG
    The inserted KEY-PLUG is not suitable for the device.
  - UNKNOWN
    Unknown content of the KEY-PLUG.
  - DEFECTIVE
    The content of the KEY-PLUG contains errors.
- **Order ID**
  Shows the order number of the KEY-PLUG. The KEY-PLUG is available for various functional enhancements and for various target systems.

- **Serial Number**
  Shows the serial number of the KEY-PLUG.
- **Info String**
  Shows additional information about the device that used the KEY-PLUG previously, for example, order number, type designation, and the versions of the hardware and software. The displayed software version corresponds to the version in which the configuration was last changed. With the "NOT ACCEPTED" status, further information on the cause of the problem is displayed.

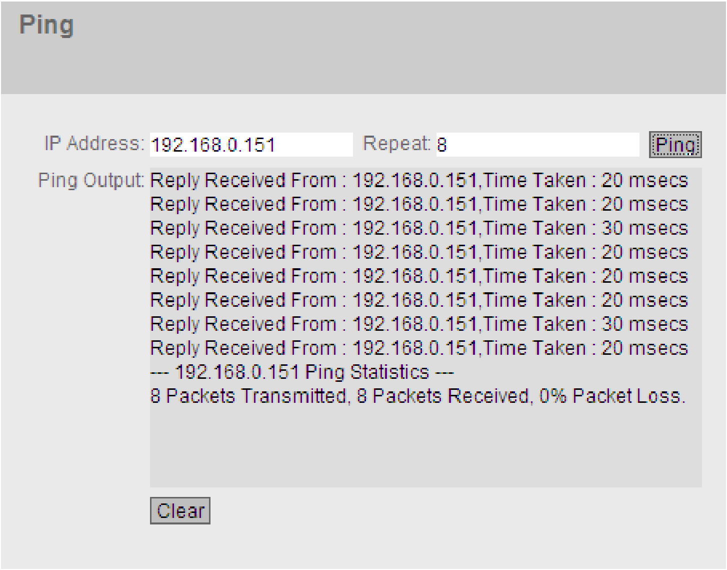
Note

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

5.5.18 Ping

Reachability of an address in an IP network

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



IP Address: 192.168.0.151 Repeat: 8

Ping Output:

```
Reply Received From : 192.168.0.151,Time Taken : 20 msecs
Reply Received From : 192.168.0.151,Time Taken : 20 msecs
Reply Received From : 192.168.0.151,Time Taken : 30 msecs
Reply Received From : 192.168.0.151,Time Taken : 20 msecs
Reply Received From : 192.168.0.151,Time Taken : 20 msecs
Reply Received From : 192.168.0.151,Time Taken : 20 msecs
Reply Received From : 192.168.0.151,Time Taken : 30 msecs
Reply Received From : 192.168.0.151,Time Taken : 20 msecs
--- 192.168.0.151 Ping Statistics ---
8 Packets Transmitted, 8 Packets Received, 0% Packet Loss.
```

Description

The table has the following columns:

- **"IP Address" input box**
  Enter the IP address of the device.
- **"Repeat" input box**
  Enter the number of ping requests.
- **"Ping" button**
  Click this button to start the ping function.
- **Ping Output**
  This box shows the output of the ping function.
- **"Clear" button**
  Click this button to empty the "Ping Output" box.

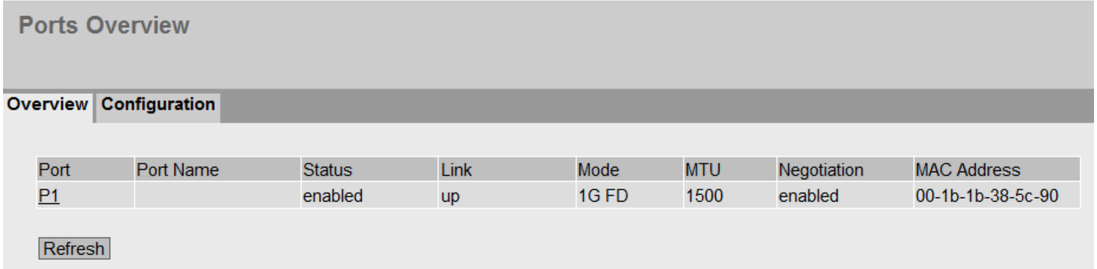
5.6 "Interfaces" menu

5.6.1 Ethernet

5.6.1.1 Overview

Overview of the port configuration

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



Port	Port Name	Status	Link	Mode	MTU	Negotiation	MAC Address
P1		enabled	up	1G FD	1500	enabled	00-1b-1b-38-5c-90

Description

The table has the following columns:

- **Port**
  Shows the configurable ports. If you click on the link, the corresponding configuration page is opened.
- **Port Name**
  Shows the name of the port.
- **Status**
  Shows whether the port is on or off. Data traffic is possible only over an enabled port.
- **Link**
  Shows the connection status to the network. With the connection status, the following is possible:
  - Up
    The port has a valid link to the network, a link integrity signal is being received.
  - Down
    The link is down, for example because the connected device is turned off.
- **Mode**
  Shows the transfer parameters of the port.
- **MTU (Maximum Transmission Unit)**
  Shows the packet size.

- **Negotiation**
  Shows whether the automatic configuration is enabled or disabled.
- **MAC Address**
  Shows the MAC address of the port.

5.6.1.2 Configuration

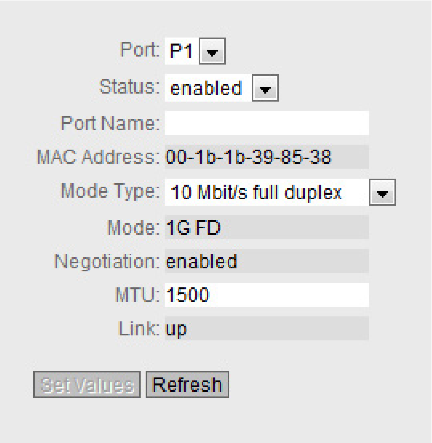
Configuring ports

With this page, you configure the Ethernet ports of the device.

Note

SCALANCE W786-2 SFP

The two SFP ports of the SCALANCE W786-2 SFP cannot be assigned parameters or diagnosed individually.



Port: P1

Status: enabled

Port Name:

MAC Address: 00-1b-1b-39-85-38

Mode Type: 10 Mbit/s full duplex

Mode: 1G FD

Negotiation: enabled

MTU: 1500

Link: up

Description

The table has the following rows:

- **"Port" drop-down list**
  Select the port to be configured from the drop-down list.
- **"Status" drop-down list**
  Specify whether the port is enabled or disabled.
  - enabled
    The port is enabled. Data traffic is possible only over an enabled port.
  - disabled
    The port is disabled.
- **Input box "Port Name"**
  Here, enter a name for the port.

- **MAC Address**
  Shows the MAC address of the port.
- **"Mode Type" drop-down list**

  Note

  The parameter cannot be configured on the SCALANCE W786-2 SFP.

  Select the transmission speed and the transmission method of the port from this drop-down list. The transmission speed can be 10 Mbps, 100 Mbps or 1000 Mbps. As the transmission mode, you can configure full duplex (FD) or half duplex (HD). 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

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

  Note

  If 10 Mbps is configured as the transmission speed or half duplex (HD) as the transmission mode, this can lead to restrictions in PNIO communication. Always select at least 100 Mbps and full duplex (FD) or "Autonegotiation" if you want the device to handle PNIO communication.
- **Mode**
  Shows the transmission speed and the transmission method of the port.
- **Negotiation**
  Shows whether the automatic configuration of the connection to the partner port is enabled or disabled.
- **"MTU" input box**
  Enter the packet size above which packets are fragmented.
- **Link**
  Shows 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

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.

Procedure

Follow the steps below to change the settings:

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

5.6.2 WLAN

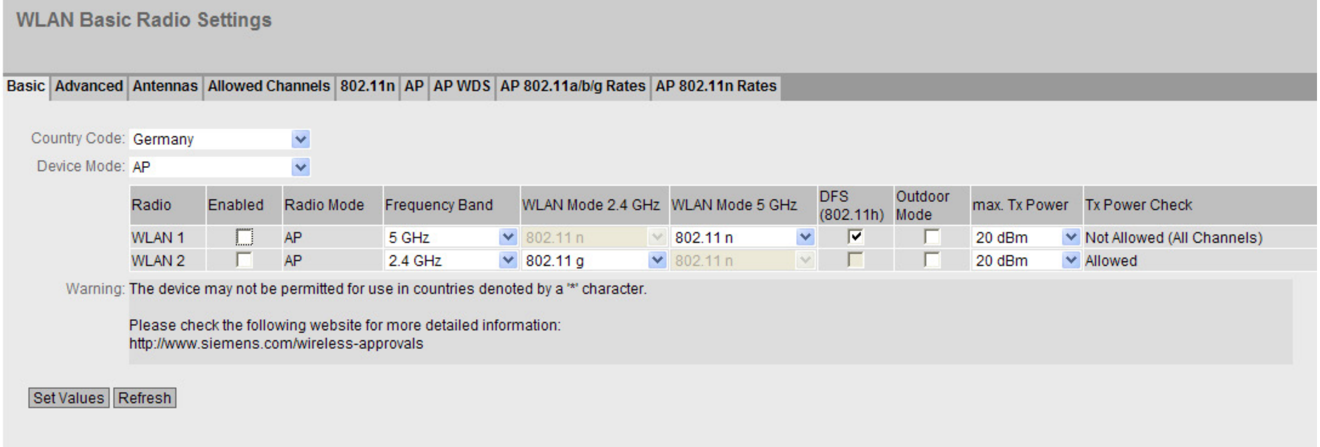
5.6.2.1 Basic

Basic settings

On this page, you make several basic settings for the device, for example the country setting and mode.

Note

To configure the WLAN interface you must always specify the Country Code first. Some parameters are dependent on the country setting, for example the transmission standard.



Country Code: Germany
Device Mode: AP

Radio	Enabled	Radio Mode	Frequency Band	WLAN Mode 2.4 GHz	WLAN Mode 5 GHz	DFS (802.11h)	Outdoor Mode	max. Tx Power	Tx Power Check
WLAN 1	□	AP	5 GHz	802.11 n	802.11 n	☑	□	20 dBm	Not Allowed (All Channels)
WLAN 2	□	AP	2.4 GHz	802.11 g	802.11 n	□	□	20 dBm	Allowed

Warning: The device may not be permitted for use in countries denoted by a "*" character.

Please check the following website for more detailed information:
http://www.siemens.com/wireless-approvals

Description

- **"Country Code" drop-down list**
  From this list, you select the country in which the device will be operated.
  You do not need to know the data for the specific country, the channel division and output power are set by the device according to the country you select.

  Note

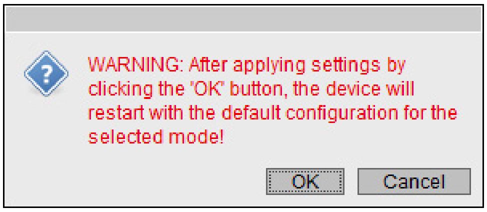
  Locale setting

  The correct country setting is mandatory for operation complying with the approvals. Selecting a country different from the country of use can lead to legal prosecution.

- **"Device Mode" drop-down list**
  Select the mode of the device. This selection is available only for W78x devices. following operating modes are possible:
  - AP: Access point mode
  - Client: Client mode

  Note

  After changing the mode, a message is displayed. If you confirm the message with "OK", the device restarts in the changed mode with the factory-set configuration settings.



WARNING: After applying settings by clicking the 'OK' button, the device will restart with the default configuration for the selected mode!

If you have restarted the device after changing the mode, you will need to log on again to be able to continue the configuration.

The table has the following columns:

- **Radio**
  Shows the available WLAN interfaces in this column.
- **Enabled**
  Status of the WLAN interface. To enable the WLAN interface, select the check box.

  Note

  Enabling the WLAN interface

  The WLAN interfaces are disabled when the device is supplied. The WLAN interfaces are can be enabled once the country and the antenna settings are configured.
- **Radio Mode**
  Shows the mode of the WLAN interface.
- **Frequency Band**
  Specify the frequency band. In client mode, dual-frequency operation is also possible.

  Note

  Configuring WLAN interfaces of the W786-2IA RJ-45 for different frequency bands

  If both WLAN interfaces are configured for the same frequency band on this device, there may be mutual influence or interference. This applies in particular when there is a high data throughput.
- **WLAN Mode**
  Select the required transmission standard for the configured frequency band.
  - WLAN Mode 2.4 GHz
    Specify the transmission standard for the 2.4 GHz frequency band. The selection depends on the country setting.
  - WLAN Mode 5 GHz
    Specify the transmission standard for the 5 GHz frequency band. The selection depends on the country setting.
- **DFS (802.11h)**
  Enables or disables the "Dynamic Frequency Selection (DFS)" function.
  - enabled
    If the access point discovers a disruption on the current channel, for example due to a primary user, it automatically switches to an alternative channel. DFS is also necessary for using certain wireless channels in the 5 GHz band.
  - disabled
    The DFS function is not used.

- **Outdoor Mode**
  - enabled
    In outdoor mode, the selection of country-dependent channels and the transmit power for operation are extended for outdoor use.
  - disabled
    The device is being operated in indoor mode. In indoor mode, the selection of country-dependent channels and the transmit power for operation in a building are restricted.
- **max. Tx Power**
  Specify the maximum possible transmit power of the device. It may be necessary to reduce the transmit power when using antennas to avoid exceeding the maximum legal transmit power. Reducing the transmit power effectively reduces cell size.

Note

The maximum possible transmit power varies depending on the channel and data rate. For more detailed information on transmit power, refer to the documentation "Characteristics radio interface".

Note

If both interfaces of access points with two WLAN interfaces are operated in the same frequency range, this may cause wireless interference on one or both interfaces at a transmit power higher than 15 dBm.

- **Tx Power Check**
  Indicates whether the settings that have been made will violate the permitted transmit power restrictions of the selected country. The following parameters influence this calculation:
  max. Tx Power, Antenna Gain, Additional Attenuation.
  The following displays can appear:
  - Allowed
    The channels can be used with the current settings.
  - Not allowed (Some Channels)
    Among the channels, there are some on which the current transmit power exceeds the maximum permitted transmit power.
  - Not allowed (All Channels)
    No permitted operation is possible. The transmit power is too high.
  - Controlled automatically by iREF.

Procedure

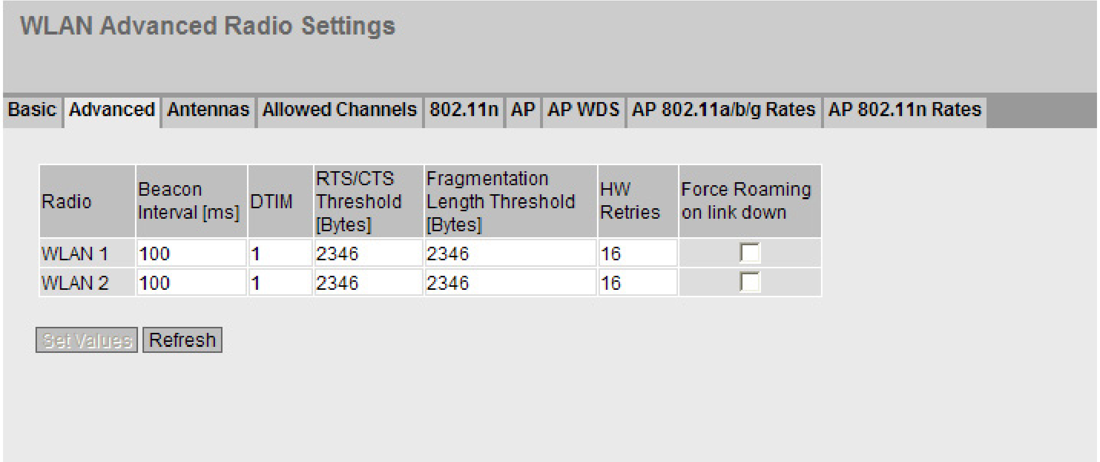
1. To configure the WLAN interface, you must always specify the country first. Select the country in which the device will be operated from the "Country Code" drop-down list.
2. Select the required frequency band from the "Frequency Band" drop-down list.

3. Select the required transmission standard for the configured frequency band from the "WLAN Mode" drop-down list.
4. Click the "Set Values" button.

5.6.2.2 Advanced

Further possible settings

On this page, you can specify details of the transmission characteristics. You only need to adapt the parameters on this page if the device cannot be used as it is intended with the default settings.



WLAN Advanced Radio Settings

Radio	Beacon Interval [ms]	DTIM	RTS/CTS Threshold [Bytes]	Fragmentation Length Threshold [Bytes]	HW Retries	Force Roaming on link down
WLAN 1	100	1	2346	2346	16	□
WLAN 2	100	1	2346	2346	16	□

Description

The table has the following columns:

- **Radio**
  Shows the available WLAN interfaces in this column.
- **Beacon Interval [ms] (Only in access point mode)**
  Specify the interval (40 - 1000 ms) at which the access point sends beacons. Beacons are packets that are sent cyclically by an access point to inform clients of its existence.
- **DTIM (Only in access point mode)**
  The DTIM interval (1-15) specifies the number of beacons to be sent before the access point sends the collected packets (broadcast, unicast, multicast) to the client.
  - If you enter a "1" in this box, the access point transmits broadcast, unicast and multicast packets directly after each beacon (recommended setting for normal network environments).
  - If you entered a "5" in this field, this would mean that the access point collects the packets and sends them after every fifth beacon.

  Increasing this value allows a longer sleep mode for the clients but means a greater delay for packets.

- **RTS/CTS Threshold [Bytes]**
  RTS/CTS (Request To Send/Clear To Send) is a method for avoiding collisions. The method is based on the exchange of status information prior to sending the actual data (hidden node problem). To minimize the network load due to additional protocol traffic, this method is used only as of a specified packet size. You specify the packet size with the "RTS/CTS Threshold" parameter.
- **Fragmentation Length Threshold [Bytes]**
  Specify the maximum packet size transferred on the wireless link. Large packets are divided up into small packets prior to transmission and then reassembled into the original size after they have been received. This can be beneficial if the transmission quality is poor because larger packets are more difficult to transmit. However fragmentation into smaller packets means a poorer throughput.
- **HW Retries**
  Specify the number of hardware retries. The hardware repetition is performed by the WLAN chip itself when it tries to repeat an unacknowledged packet immediately.

  If all hardware repetitions were unsuccessful, the packet is deleted.
- **Force roaming on link down (Only in access point mode)**
  If the wired Ethernet interface is no longer available (cable break, connector removed), a client connected over the wireless network is not aware of this. The access point can force the logged-on clients to roam by deactivating its WLAN interface. The client then attempts to log on at a different access point. You enable this feature by selecting the "Force Roaming on link down" check box.

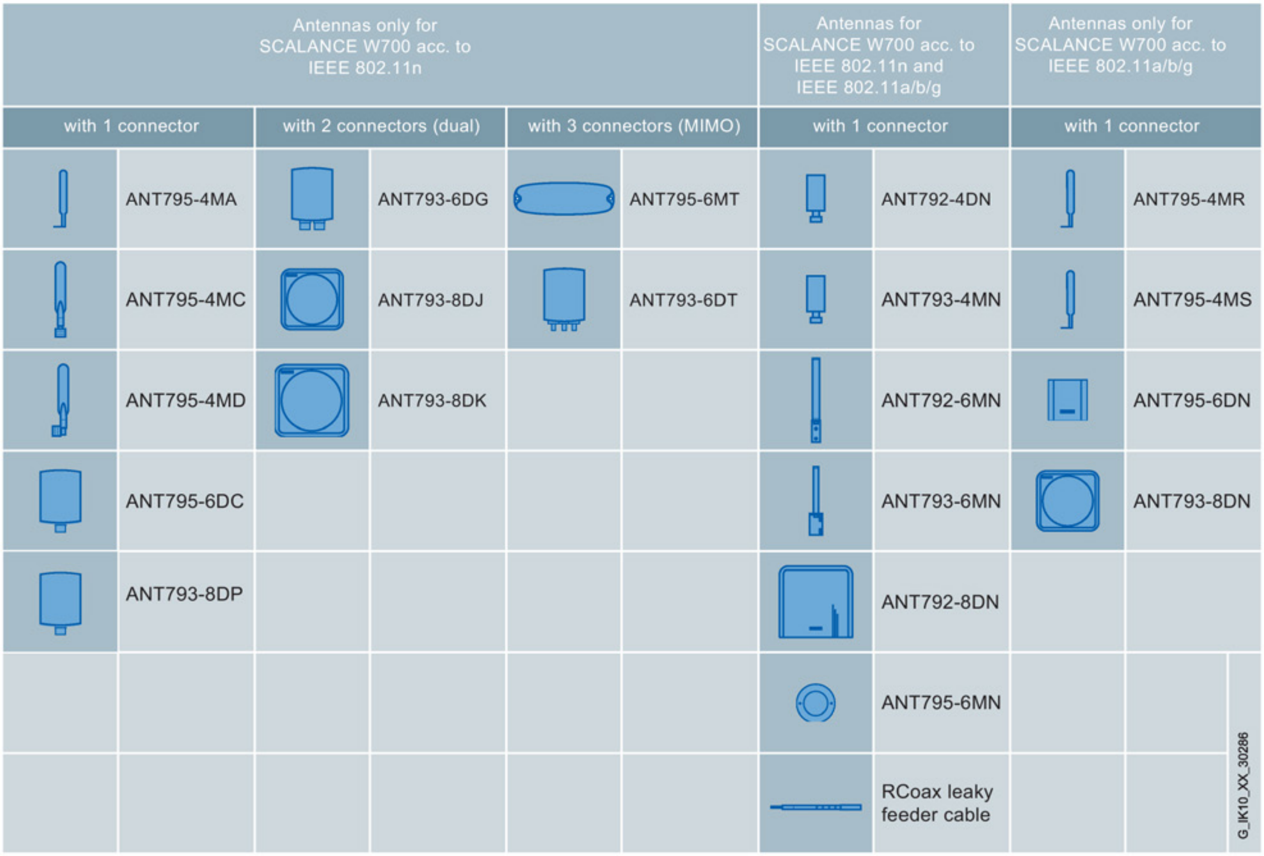
Procedure

1. Enter the values to be set in the input boxes as follows.
2. Click the "Set Values" button.

5.6.2.3 Antennas

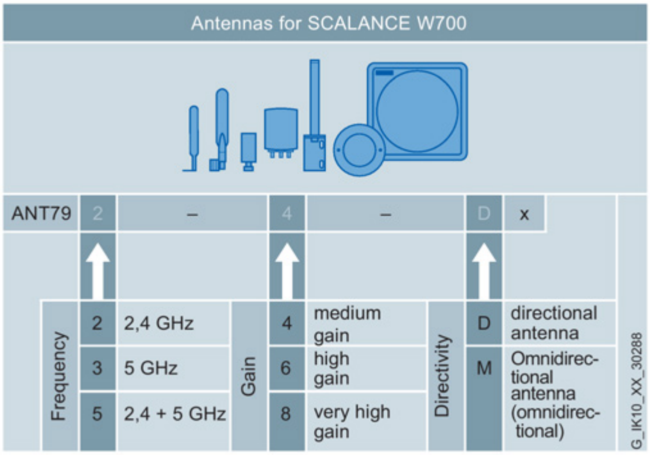
Overview

Overview of IWLAN antennas:



Antennas only for SCALANCE W700 acc. to IEEE 802.11n			Antennas for SCALANCE W700 acc. to IEEE 802.11n and IEEE 802.11a/b/g	Antennas only for SCALANCE W700 acc. to IEEE 802.11a/b/g
with 1 connector	with 2 connectors (dual)	with 3 connectors (MIMO)	with 1 connector	with 1 connector
ANT795-4MA	ANT793-6DG	ANT795-6MT	ANT792-4DN	ANT795-4MR
ANT795-4MC	ANT793-8DJ	ANT793-6DT	ANT793-4MN	ANT795-4MS
ANT795-4MD	ANT793-8DK		ANT792-6MN	ANT795-6DN
ANT795-6DC			ANT793-6MN	ANT793-8DN
ANT793-8DP			ANT792-8DN	
			ANT795-6MN	
			RCoax leaky feeder cable	

The antenna name provides information about the properties of the antennas listed in the IWLAN antenna overview:



Antennas

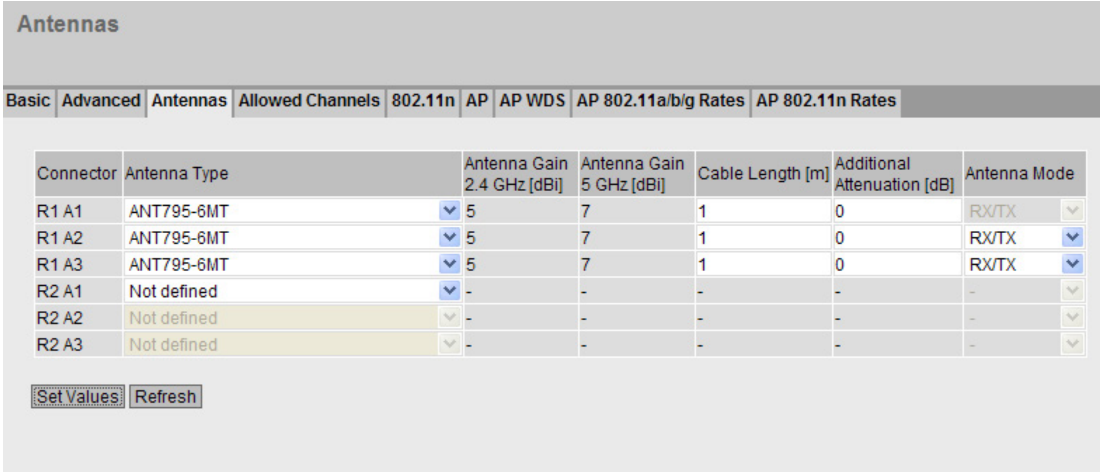
Configuration of external antennas

On this page, you configure the settings for the connected external antennas.

Note

50 Ω terminating resistor

Each WLAN interface has three antenna connectors. Connectors that are not used must have a 50 Ω terminating resistor fitted.
The antennas R1A1 and R2A1 must be always be connected as soon as the associated WLAN interface is turned on. If no antenna is connected, the relevant interface must also be disabled for Rx and Tx. Otherwise, there may be transmission disruptions.



Connector	Antenna Type	Antenna Gain 2.4 GHz [dBi]	Antenna Gain 5 GHz [dBi]	Cable Length [m]	Additional Attenuation [dB]	Antenna Mode
R1 A1	ANT795-6MT	5	7	1	0	RX/TX
R1 A2	ANT795-6MT	5	7	1	0	RX/TX
R1 A3	ANT795-6MT	5	7	1	0	RX/TX
R2 A1	Not defined	-	-	-	-	-
R2 A2	Not defined	-	-	-	-	-
R2 A3	Not defined	-	-	-	-	-

Description

The table has the following columns:

- **Connector**
  Shows the name of the relevant antenna connection.
- **Antenna Type**
  Select the type of external antenna connected to the device. If the type of your external antenna is not available, select the entry "User defined"
  .If you terminate an antenna connection using a 50 Ω terminating resistor, select the entry "Not used (connect 50 Ohms Termination)".
- **Antenna Gain**
  If you select the "User-defined" entry for the "Antenna Type", enter the antenna gain manually in the "dBi" unit.
  – **Antenna Gain 2.4 GHz [dBi]**
    Here, enter the antenna gain the antenna has in the 2.4 GHz frequency band.
  – **Antenna Gain 5 GHz [dBi]**
    Here, enter the antenna gain the antenna has in the 5 GHz frequency band.

- **Cable length [m]**
  Enter the length of the flexible antenna connecting cable in meters between the device and the external antenna.
- **Additional Attenuation [dB]**
  Here, specify the additional attenuation caused, for example, by an additional splitter.
- **Antenna Mode**
  Specify the use of the antenna. For antenna connector 1 (R1 A1 and R2 A1), the entry cannot be changed.
  - Tx
    For sending only
  - Rx
    For receiving only
  - Rx\Tx
    For receiving and sending

  The following table shows which combinations are possible:

R1 A1 **R2 A1**	**R1 A2** **R2 A2**	**R1 A3** **R2 A3**
Rx\Tx	Rx\Tx	Rx\Tx
Rx\Tx	Rx\Tx	Rx
Rx\Tx	Rx	Rx
Rx\Tx	Rx\Tx	Tx
Rx\Tx	Tx	Tx
Rx\Tx	Rx\Tx	-- [1]
Rx\Tx	Tx	-- [1]
Rx\Tx	Rx	-- [1]
Rx\Tx	-- [1]	-- [1]

1) Antenna type "50 Ohms Termination Impedance"

Procedure

To configure two antennas, follow the steps below:

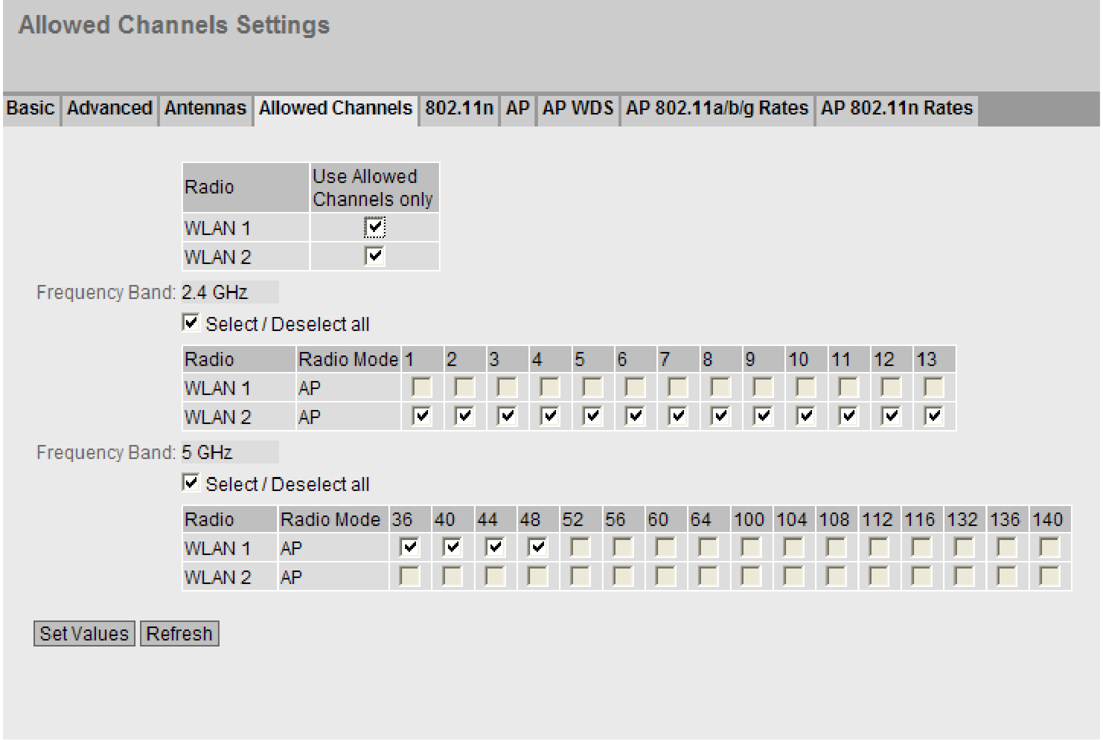
1. For the first antenna connector (R1 A1) in the "Antenna Type" drop-down list, select the type of antenna.
2. In the "Cable Length" input box, enter the length of the connecting cable you are using in meters. For antenna connector 1 (R1 A1 and R2 A1), the "Antenna Mode" cannot be changed.
3. For the second antenna connector (R1 A2) in the "Antenna Type" drop-down list, select the type of antenna.
4. In the "Cable Length" input box, enter the length of the connecting cable you are using in meters.
5. Select the use of the antenna from the "Antenna Mode" drop-down list.
6. Click the "Set Values" button.

5.6.2.4 Allowed Channels

Channel settings

For communication, a specific channel within a frequency band is used. You can either set this channel specifically or configure so that the channel is selected automatically.

On this page, you specify which channels may be used for communication.



Allowed Channels Settings

Radio	Use Allowed Channels only
WLAN 1	☑
WLAN 2	☑

Frequency Band: 2.4 GHz

☑ Select / Deselect all

Radio	Radio Mode	1	2	3	4	5	6	7	8	9	10	11	12	13
WLAN 1	AP	□	□	□	□	□	□	□	□	□	□	□	□	□
WLAN 2	AP	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Frequency Band: 5 GHz

☑ Select / Deselect all

Radio	Radio Mode	36	40	44	48	52	56	60	64	100	104	108	112	116	132	136	140
WLAN 1	AP	☑	☑	☑	☑	□	□	□	□	□	□	□	□	□	□	□	□
WLAN 2	AP	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Description

Table 1 contains the following columns:

- **Radio**
  Shows the available WLAN interfaces in this column.
- **Use Allowed Channels only**
  If you enable the option, you restrict the selection of channels via which the AP or the client is allowed to establish the connection.
  In the following tables, you define the
  - channels that the AP can use to establish a wireless cell when the "Auto" channel setting is enabled.
  - the channels on which the client searches for an AP.

  The tables are divided up according to frequency bands.
  If the option is disabled, the channels available based on the settings (country code, antennas, transmit power etc.) are used.

Above the tables for the frequency bands, you will find the following check box:

- **Select / Deselect all**
  - Enabled
    If you enable the check box, all channels are selected.
  - Disabled
    If you deselect the check box, the first valid channel of the frequency band remains enabled. Enable the required channel.

The tables of the frequency bands have the following columns:

- **Radio**
  Shows the available WLAN interfaces in this column.
- **Radio Mode**
  Shows the mode.
- **Channel number**
  To specify the valid channels for the required frequency band, select the appropriate check box for the channel number.
  The table displays the permitted channels of the country. Only the valid channels can be enabled. Invalid channels are grayed out and cannot be enabled.

Note

To specify the channels, the setting "Use Allowed Channels only" must be enabled.

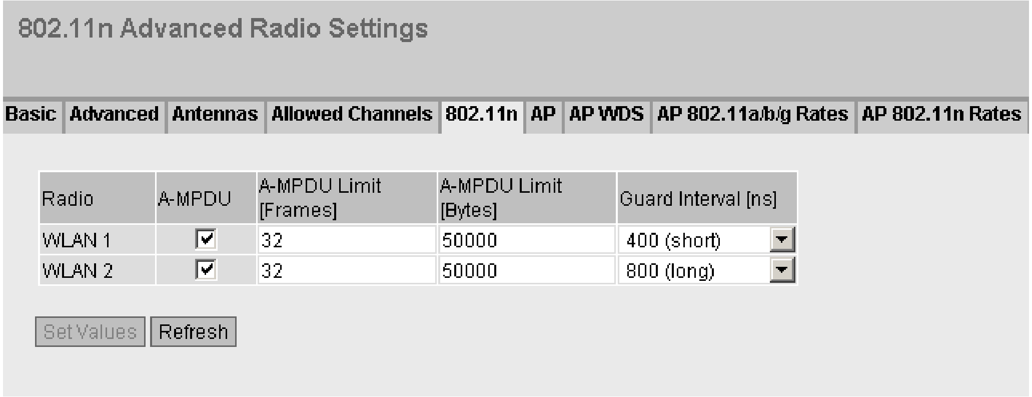
Procedure

1. Enable the "Used Allowed Channels only" option for the required WLAN interface.
2. Deselect the "Select / Deselect all" check box.
3. Select the relevant check box for the required channel number.
4. Click the "Set Values" button.

5.6.2.5 802.11n

Properties of 802.11n

With the IEEE 802.11n standard, it is possible to put together individual data packets in one larger data packet, the A-MPDU data packet. This achieves a higher data throughput.
On this page, you make the settings for the A-MPDU data packets. Some of the settings depend on the set transmission standard and the selected channel width.



802.11n Advanced Radio Settings

Radio	A-MPDU	A-MPDU Limit [Frames]	A-MPDU Limit [Bytes]	Guard Interval [ns]
WLAN 1	☑	32	50000	400 (short)
WLAN 2	☑	32	50000	800 (long)

Description

The table has the following columns:

- **Radio**
  Shows the available WLAN interfaces in this column.
- **A-MPDU**
  Enables or disables the sending of A-MPDU data packets. If this check box is disabled, only A-MPDU data packets are received.
- **A-MPDU Limit [Frames]**
  Specify the number of individual data packets grouped together in one AMPDU data packet.
  Range of values: 2 - 64 frames
- **A-MPDU Limit [Bytes]**
  Specify the maximum size of the AMPDU data packet. Range of values: 1024 - 65535 bytes
- **Guard Interval [ns](Only in access point mode)**
  Select the send pause that must be kept to between two transmitted OFDM symbols. The following settings are possible. The selection depends on the selected transmission standard.
  - 400 (short): The send pause is 400 ns
  - 800 (long): The send pause is 800 ns.

Procedure

Configure 802.11n settings on the access point

1. Enable the "A-MPDU" option.
2. Enter the required values in the "A-MPDU Limit [Frames]" and "A-MPDU Limit [Bytes]" input boxes.
3. Select the required value from the "Guard Interval [ns]" drop-down list.
4. Click the "Set Values" button.

Configure 802.11n settings on the client

1. Enable the "A-MPDU" option.
2. Enter the required values in the "A-MPDU Limit [Frames]" and "A-MPDU Limit [Bytes]" input boxes.
3. Click the "Set Values" button.

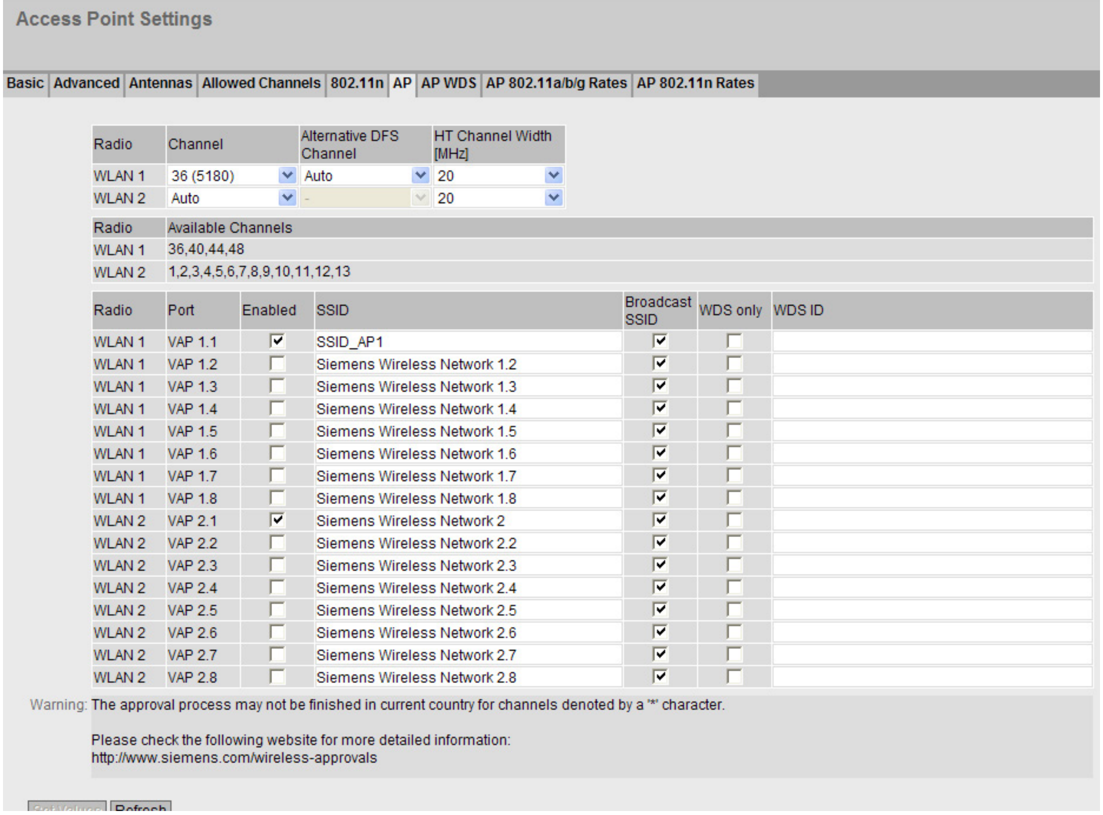
5.6.2.6 AP

Configuration

On this page, you specify the configuration for the access point.

Note

This tab is available only in access point mode.



Access Point Settings
Basic | Advanced | Antennas | Allowed Channels | 802.11n | AP | AP WDS | AP 802.11a/b/g Rates | AP 802.11n Rates

Radio	Channel	Alternative DFS Channel	HT Channel Width [MHz]
WLAN 1	36 (5180)	Auto	20
WLAN 2	Auto	-	20

Radio	Available Channels
WLAN 1	36,40,44,48
WLAN 2	1,2,3,4,5,6,7,8,9,10,11,12,13

Radio	Port	Enabled	SSID	Broadcast SSID	WDS only	WDS ID
WLAN 1	VAP 1.1	☑	SSID_AP1	☑	□	
WLAN 1	VAP 1.2	□	Siemens Wireless Network 1.2	☑	□	
WLAN 1	VAP 1.3	□	Siemens Wireless Network 1.3	☑	□	
WLAN 1	VAP 1.4	□	Siemens Wireless Network 1.4	☑	□	
WLAN 1	VAP 1.5	□	Siemens Wireless Network 1.5	☑	□	
WLAN 1	VAP 1.6	□	Siemens Wireless Network 1.6	☑	□	
WLAN 1	VAP 1.7	□	Siemens Wireless Network 1.7	☑	□	
WLAN 1	VAP 1.8	□	Siemens Wireless Network 1.8	☑	□	
WLAN 2	VAP 2.1	☑	Siemens Wireless Network 2	☑	□	
WLAN 2	VAP 2.2	□	Siemens Wireless Network 2.2	☑	□	
WLAN 2	VAP 2.3	□	Siemens Wireless Network 2.3	☑	□	
WLAN 2	VAP 2.4	□	Siemens Wireless Network 2.4	☑	□	
WLAN 2	VAP 2.5	□	Siemens Wireless Network 2.5	☑	□	
WLAN 2	VAP 2.6	□	Siemens Wireless Network 2.6	☑	□	
WLAN 2	VAP 2.7	□	Siemens Wireless Network 2.7	☑	□	
WLAN 2	VAP 2.8	□	Siemens Wireless Network 2.8	☑	□	

Warning: The approval process may not be finished in current country for channels denoted by a '*' character.

Please check the following website for more detailed information:
http://www.siemens.com/wireless-approvals

Description

Table 1 has the following columns:

- **Radio**
  Shows the available WLAN interfaces in this column.

- **Channel**
  Specify the main channel.
  If you want the access point to search for a free channel itself, use "Auto". The selection of channels used by an access point when establishing a wireless cell can be restricted. To do this, select the "Use Allowed Channels only" check box on the "Allowed Channels" tab.
  ".If you want to use a fixed channel, select the required channel from the drop-down list.

  Note

  Channel spacing with WLAN interfaces

  If you use a second WLAN interface, make sure that you have adequate channel spacing.

- **Alternative Channel (802.11h)**
  If you have enabled the "DFS" function on the "Basic" page, specify the alternative channel here. If you want the access point to search for a free channel itself, use "Auto". If a primary user was detected both on the main and alternative channel, the access point automatically searches for a free channel.
  If you want to use a fixed channel, select the required channel from the drop-down list.
- **HT Channel Width [MHz]**
  You can only specify the channel bandwidth with the IEEE 802.11n transmission standard.
  The following settings are possible.
  - 20
    Channel bandwidth 20 MHz
  - 40 up
    Channel bandwidth 40 MHz. The configured channel and the neighboring channel above it are used.
  - 40 down
    Channel bandwidth 40 MHz. The configured channel and the neighboring channel below it are used.

    Note

    Channel bandwidth 40 MHz and frequency band 2.4 GHz

    If the access point detects another access point on the configured channel or on neighboring channels, the access point changes the channel bandwidth from 40 MHz to 20 MHz. If you set a "free" channel on the access point, the access point uses the channel bandwidth 40 MHz.

Table 2 has the following columns:

- **Radio**
  Shows the available WLAN interfaces in this column.
- **Allowed Channel**
  This box displays the allowed channels. The display depends on the wireless approvals of the currently selected country and the settings for "Allowed Channels".

Table 3 has the following columns:

- **Radio**
  Shows the WLAN interface.
- **Port**
  Shows the VAP interface.
- **Enabled**
  To use the required VAP interface, select this check box.
- **SSID**
  Enter the SSID of the WLAN. The length of the character string for SSID it is 1 to 32 characters.
  The ASCII code 0x20 to 0x7e is used for the SSID.
- **Broadcast SSID**
  - deactived
    The SSID is no longer sent in the beacon frame of the access point. This means that the SSID is not visible for other devices. Only clients that know the SSID of the access point and that are configured with it can connect to the access point. The "Any SSID" option must be disabled on these clients.
  - activated
    The SSID is sent in the Beacon frame of the access point and is visible for other devices. This means that clients on which the "Any SSID" option is enabled can also connect to the access point.

Note

Since no encryption is used for the SSID transfer, this function can only provide basic protection against unauthorized access. The use of an authentication method (for example WPA2 (RADIUS) or WPA2-PSK if this is not possible) provides higher security. You must also expect that certain end devices may have problems with access to a hidden SSID.

- **WDS only**
  If you enable this option, the access point only supports communication via WDS. In WDS mode, all access points must use the same channel.
- **WDS ID**
  Enter the WDS ID. The WDS ID can be a maximum of 32 characters long.
  To establish a WDS connection, enter this WDS ID on the WDS Partner.
  ASCII code 0x20 to 0x7e is used for the WDS ID.

Procedure

1. Select the required channel from the "Channel" drop-down list.
2. Enter network name in the "SSID" input box for the corresponding WLAN interface and port.
3. Select the "Enabled" check box for the relevant WLAN interface and the port.
4. Click the "Set Values" button.

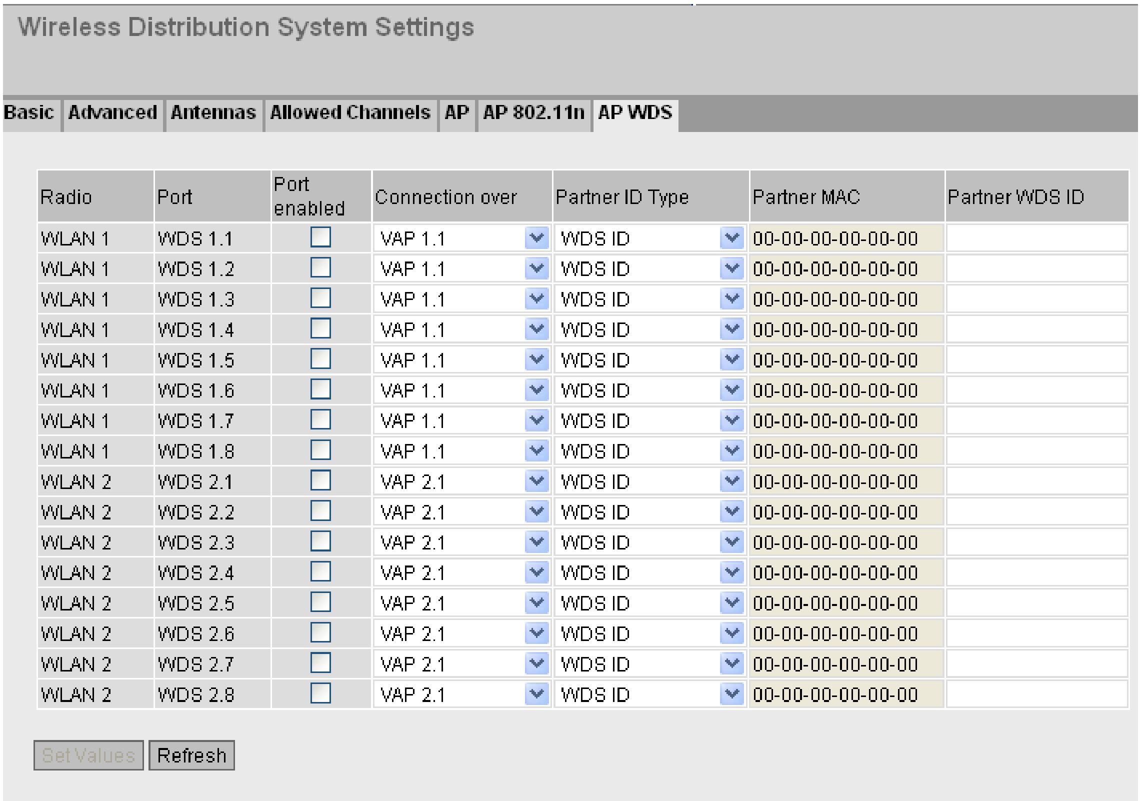
5.6.2.7 AP WDS

Communication

In normal operation, the access point is used as an interface to a network and communicates with clients. There are, however, situations in which several access points need to communicate with each other, for example to extend wireless coverage or to set up a wireless backbone. This mode is possible with WDS (Wireless Distributed System).

Note

This tab is available only in access point mode.



Wireless Distribution System Settings

Radio	Port	Port enabled	Connection over	Partner ID Type	Partner MAC	Partner WDS ID
WLAN 1	WDS 1.1	□	VAP 1.1	WDS ID	00-00-00-00-00-00	
WLAN 1	WDS 1.2	□	VAP 1.1	WDS ID	00-00-00-00-00-00	
WLAN 1	WDS 1.3	□	VAP 1.1	WDS ID	00-00-00-00-00-00	
WLAN 1	WDS 1.4	□	VAP 1.1	WDS ID	00-00-00-00-00-00	
WLAN 1	WDS 1.5	□	VAP 1.1	WDS ID	00-00-00-00-00-00	
WLAN 1	WDS 1.6	□	VAP 1.1	WDS ID	00-00-00-00-00-00	
WLAN 1	WDS 1.7	□	VAP 1.1	WDS ID	00-00-00-00-00-00	
WLAN 1	WDS 1.8	□	VAP 1.1	WDS ID	00-00-00-00-00-00	
WLAN 2	WDS 2.1	□	VAP 2.1	WDS ID	00-00-00-00-00-00	
WLAN 2	WDS 2.2	□	VAP 2.1	WDS ID	00-00-00-00-00-00	
WLAN 2	WDS 2.3	□	VAP 2.1	WDS ID	00-00-00-00-00-00	
WLAN 2	WDS 2.4	□	VAP 2.1	WDS ID	00-00-00-00-00-00	
WLAN 2	WDS 2.5	□	VAP 2.1	WDS ID	00-00-00-00-00-00	
WLAN 2	WDS 2.6	□	VAP 2.1	WDS ID	00-00-00-00-00-00	
WLAN 2	WDS 2.7	□	VAP 2.1	WDS ID	00-00-00-00-00-00	
WLAN 2	WDS 2.8	□	VAP 2.1	WDS ID	00-00-00-00-00-00	

Description

The table has the following columns:

- **Radio**
  Shows the available WLAN interfaces in this column.
- **Port**
  Shows the port.
- **Port enabeld**
  Enables the WDS interface.

- **Connection over**
  Specify the VAP interface via which the WDS connection is established. Both the MAC address of the VAP as well as security settings (for example WPA2) are used.
- **Partner ID Type**
  Specify the type of WDS communication.
  - MAC Address
    The MAC address is used. The "Partner WDS ID" input box is grayed out. In "Partner MAC", enter the MAC address of the WDS partner.
  - WDS ID
    The WDS ID is used. The "Partner MAC" input box is grayed out. In "Partner WDS ID", enter the WDS ID of the WDS partner. Use this option if you want to replace the access point later using the C-PLUG or KEY-PLUG.
- **Partner MAC**
  Enter the MAC address of the WDS partner.
- **Partner WDS ID**
  Enter the WDS ID of the WDS partner. For the WDS ID, the ASCII characters 0x20 to 0x7e are permitted.

Note

Matching security settings in WDS mode

In WDS mode, make sure that the security settings match up for all devices involved. If settings are incorrect or not compatible on the individual devices, no data exchange is possible due to incorrect authentication. Avoid the "Auto" setting in the "Security Settings" tab of the Basic Wizard, because with this setting, synchronization of the security settings between the access points is not possible.

Note

In WDS operation, the following restrictions apply to all access points involved:

- All access points that will communicate with each other must use the same channel, the same transmission procedure and the same data rate.
- You can select either WEP or WPA(2)-PSK as the encryption method.
  You configure the security settings in the assigned VAP interface: "Security > WLAN > Basic"
  You cannot use authentication with a RADIUS server for a WDS connection.
- In the IEEE 802.11h transmission mode, it is not practical to select the WDS mode. In WDS mode, all access points must use the same channel. If a signal from a primary user is detected by an access point, the channel is changed automatically and the existing connection is then terminated.

Procedure

1. Select the required VAP interface from the "Connection over"drop-down list.
2. Select the entry "WDS ID" from the "Partner ID Type"drop-down list.
3. In the "WDS ID" input box, enter the WDS ID of the WDS partner. The "MAC Address" input box is grayed out.
4. Click the "Set Values" button.

5.6.2.8 AP 802.11a/b/g Rates

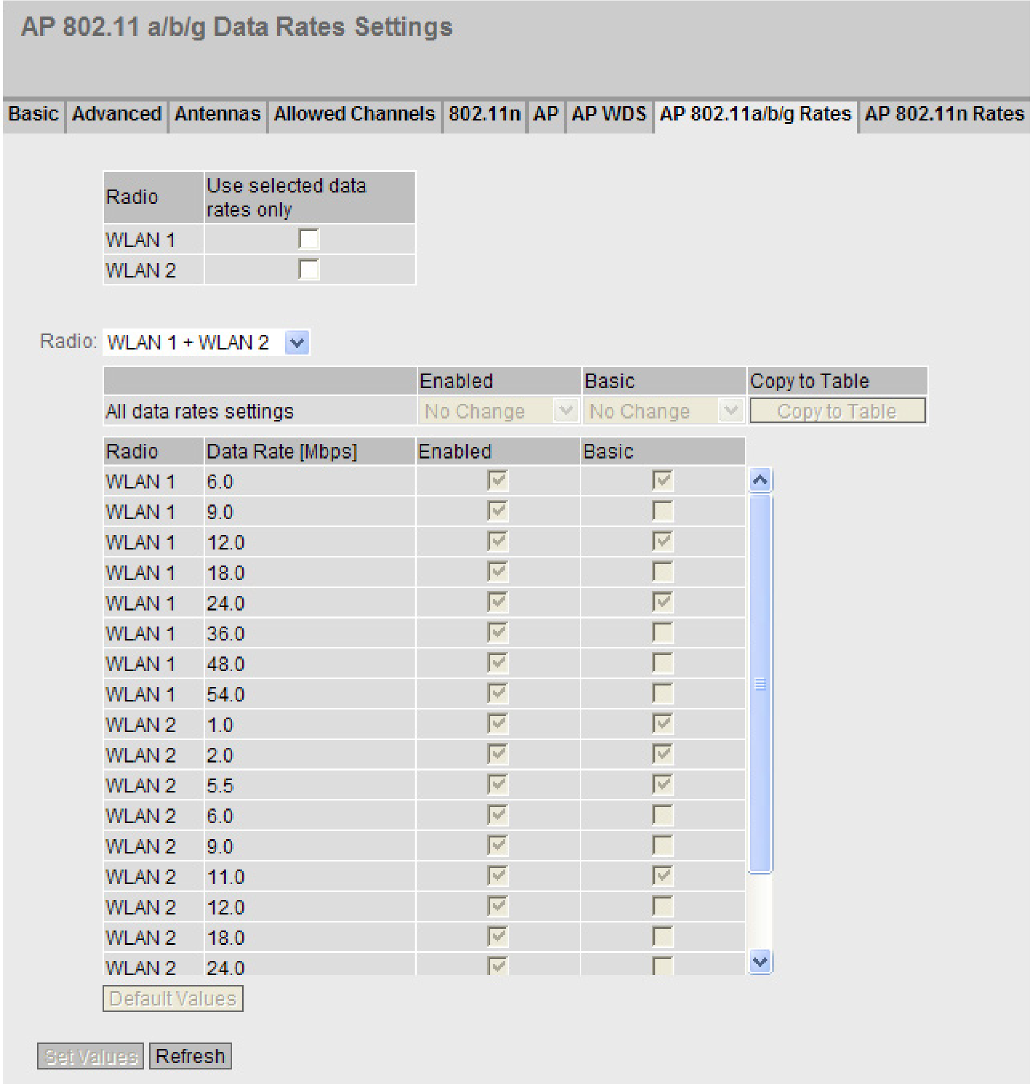
Data transmission speeds with IEEE 802.11a/b/g

Note

The tab is available only in access point mode.

The WBM page can only be configured if "802.11a", "802.11g" or "802.11n" is set for WLAN mode.

The WBM page shows the available data transmission speeds for the WLAN mode 802.11a/b/g. If necessary, you can change the data transmission speeds. Otherwise, we recommend that you retain the default setting for data transmission speeds. The access point will then use only the selected data transmission speeds for communication with the clients.



AP 802.11 a/b/g Data Rates Settings

Radio	Use selected data rates only
WLAN 1	□
WLAN 2	□

Radio: WLAN 1 + WLAN 2

	Enabled	Basic	Copy to Table
All data rates settings	No Change	No Change	Copy to Table

Radio	Data Rate [Mbps]	Enabled	Basic
WLAN 1	6.0	☑	☑
WLAN 1	9.0	☑	□
WLAN 1	12.0	☑	☑
WLAN 1	18.0	☑	□
WLAN 1	24.0	☑	☑
WLAN 1	36.0	☑	□
WLAN 1	48.0	☑	□
WLAN 1	54.0	☑	□
WLAN 2	1.0	☑	☑
WLAN 2	2.0	☑	☑
WLAN 2	5.5	☑	☑
WLAN 2	6.0	☑	□
WLAN 2	9.0	☑	□
WLAN 2	11.0	☑	☑
WLAN 2	12.0	☑	□
WLAN 2	18.0	☑	□
WLAN 2	24.0	☑	□

Description

Table 1 has the following columns:

- **Radio**
  Specifies the WLAN interface to which the information relates.
- **Use selected data rates only**
  If you select this option, you can specify the data transmission speeds for the required WLAN interface.
  If this option is disabled, the default values are used. As default, this option is disabled.

Drop-down list "Radio"
In this drop-down list, select the WLAN interfaces displayed in Table 3 (Data Rate).

With Table 2, you can enable or disable all check boxes of a column of Table 3 (Data Rate) at once. Table 2 has the following columns:

- **All data rates settings**
  Shows that the setting is valid for all entries in Table 3.
- **Enabled / Basic**
  In the drop-down list, select the setting for all entries. If "No Change" is selected, the entry in table 3 remains unchanged.
- **Copy to Table**
  If you click the button, the setting is adopted for all entries of table 3.

Table 3 (Data Rate) consists of the following columns:

- **Radio**
  Specifies the WLAN interface to which the information relates.
- **Data Rate [Mbps]**
  Shows the supported data transmission speeds in megabits per second.
- **Enabled**
  Enable the option to assign the required data transmission speed to the WLAN interface.

  Note

  You need to enable at least one data transmission speed.

- **Basic**
  Enable the option to declare the required data transmission speed as "Basic". The "Basic" parameter specifies that a client must be capable of this speed to be able to connect to the access point. The "Basic" option can only be enabled if an available data transmission speed has been selected.

  Note

  At least one data transmission speed needs to be specified as "Basic".

Button "Default Values"
The "Default Values" button sets the selection of the values in compliance with the standard.

Procedure

To configure a certain data transmission speed on WLAN 1:

1. For "WLAN 1", select the option "Use selected data rates only".
2. From the "Radio" drop-down list, select the entry "WLAN 1".
3. Select the check box in the "Enabled" and in the "Basic" column for the required data transmission speed.
4. Click the "Set Values" button.

To reset the selection:

1. Click the "Default Values" button. The selection is reset to the default setting.

5.6.2.9 AP 802.11n Rates

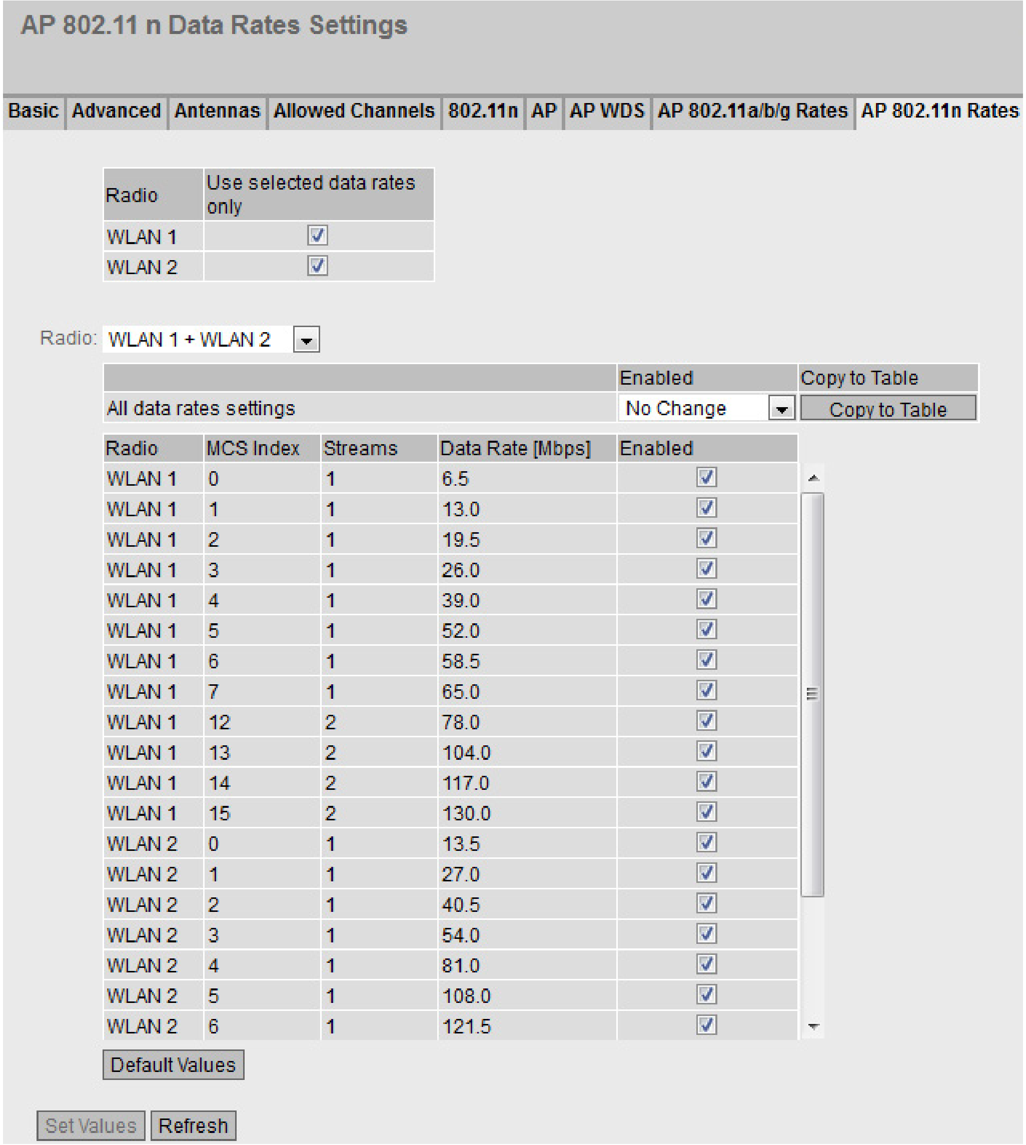
Data transmission speeds in IEEE 802.11n

Note

The tab is available only in access point mode.

The WBM page can only be configured if "802.11n only" or "802.11n" is set for the WLAN mode.

The WBM page shows the available data transmission speeds (MCS = Modulation and Coding Schemes) for the WLAN mode 802.11n. You can select any combination of these data transmission speeds. The access point will then use only the selected data transmission speeds for communication with the clients.



AP 802.11 n Data Rates Settings

Radio	Use selected data rates only
WLAN 1	☑
WLAN 2	☑

Radio: WLAN 1 + WLAN 2

	Enabled	Copy to Table
All data rates settings	No Change	Copy to Table

Radio	MCS Index	Streams	Data Rate [Mbps]	Enabled
WLAN 1	0	1	6.5	☑
WLAN 1	1	1	13.0	☑
WLAN 1	2	1	19.5	☑
WLAN 1	3	1	26.0	☑
WLAN 1	4	1	39.0	☑
WLAN 1	5	1	52.0	☑
WLAN 1	6	1	58.5	☑
WLAN 1	7	1	65.0	☑
WLAN 1	12	2	78.0	☑
WLAN 1	13	2	104.0	☑
WLAN 1	14	2	117.0	☑
WLAN 1	15	2	130.0	☑
WLAN 2	0	1	13.5	☑
WLAN 2	1	1	27.0	☑
WLAN 2	2	1	40.5	☑
WLAN 2	3	1	54.0	☑
WLAN 2	4	1	81.0	☑
WLAN 2	5	1	108.0	☑
WLAN 2	6	1	121.5	☑

Description

Table 1 has the following columns:

- **Radio**
  Specifies the WLAN interface to which the information relates.
- **Use selected data rates only**
  If you select this option, you can specify the data transmission speeds for the required WLAN interface.
  If this option is disabled, the default values are used. As default, this option is disabled.

Drop-down list "Radio"
In this drop-down list, select the WLAN interfaces displayed in Table 3 (MCS Index).

With Table 2, you can enable or disable all check boxes of a column of Table 3 (MCS Index) at once. Table 2 has the following columns:

- **All data rates settings**
  Shows that the setting is valid for all entries in Table 3.
- **Enabled**
  In the drop-down list, select the setting for all entries. If "No Change" is selected, the entry in table 3 remains unchanged.
- **Copy to Table**
  If you click the button, the setting is adopted for all entries of table 3.

Table 3 (MCS Index) consists of the following columns:

- **Radio**
  Specifies the WLAN interface to which the information relates.
- **MCS Index**
  Shows the supported MCS indexes. The displayed MCS indexes depend on the settings "Antenna Type" and "Antenna Mode". You will find the settings in "Interfaces > WLAN > Antennas". If, for example, you only use one antenna, only the MCS 0 to 7 are displayed.
- **Streams**
  Shows the maximum possible number of parallel data streams that can be transmitted with the selected MCS index.
- **Data Rate [Mbps]**
  Shows the supported data transmission speeds in megabits per second. The displayed data transmission speeds depend on the settings "Guard Interval" and "HT Channel Width". The "HT Channel Width" setting can be found in "Interfaces > WLAN > AP". The "Guard Interval" setting can be found in "Interfaces > WLAN > 802.11n"
- **Enabled**
  Enable the option to assign the required data transmission speed to the WLAN interface.

Note

You need to enable at least one MCS index.

Button "Default Values"
The "Default Values" button sets the selection of the values in compliance with the standard.

Procedure

To configure a certain data transmission speed on WLAN 1:

1. For "WLAN 1", select the option "Use selected data rates only".
2. From the "Radio" drop-down list, select the entry "WLAN 1".
3. Select the corresponding check box in the "Enabled" column for the selected MCS index.
4. Click the "Set Values" button.

To reset the selection:

1. Click the "Default Values" button. The selection is reset to the default setting.

Or

1. Disable the "Use selected data rates only" option in Table 1.
2. Click the "Set Values" button.

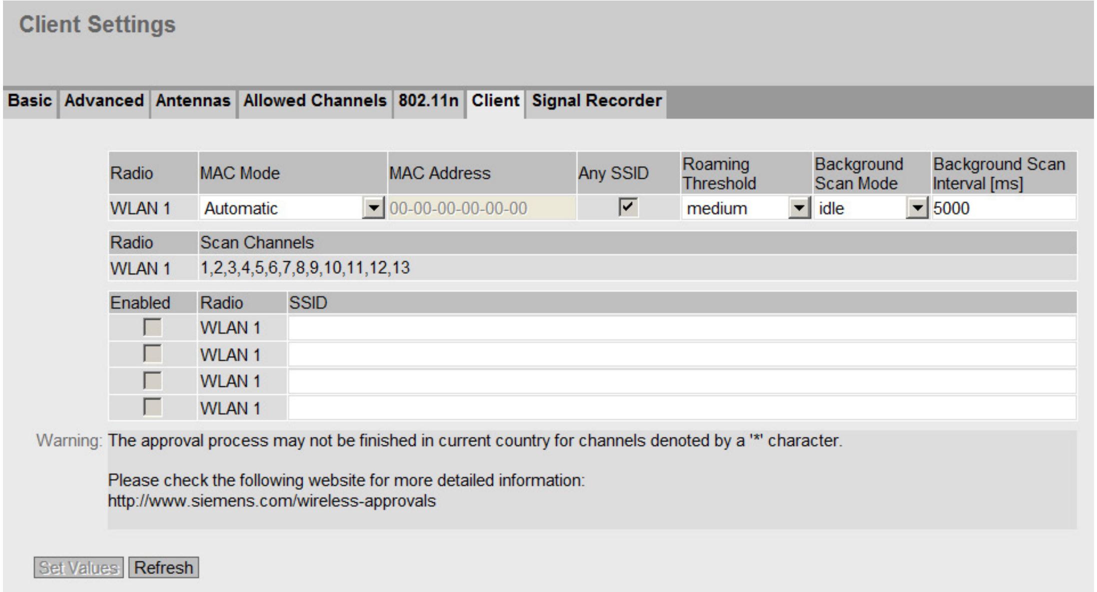
5.6.2.10 Client

Connecting to a network

With this menu command, you can specify how the device connects to a network as client.

Note

This tab is only available in the client mode.



Client Settings

Radio	MAC Mode	MAC Address	Any SSID	Roaming Threshold	Background Scan Mode	Background Scan Interval [ms]
WLAN 1	Automatic	00-00-00-00-00-00	☑	medium	idle	5000

Radio	Scan Channels
WLAN 1	1,2,3,4,5,6,7,8,9,10,11,12,13

Enabled	Radio	SSID
☐	WLAN 1	
☐	WLAN 1	
☐	WLAN 1	
☐	WLAN 1	

Warning: The approval process may not be finished in current country for channels denoted by a '*' character.

Please check the following website for more detailed information:
http://www.siemens.com/wireless-approvals

Description

Table 1 has the following columns:

- **Radio**
  Shows the available WLAN interfaces in this column.
- **MAC Mode**
  Specify how a MAC address is assigned to the client. The following are possible:
  - Automatic
    The client automatically adopts the source MAC address of the first frame that it receives over the Ethernet interface.
  - Manual
    If you select Manual, enter the MAC address in the "MAC Address" column.
  - Own
    The client uses the MAC address of the Ethernet interface for the WLAN interface.
  - Layer 2 Tunnel
    The client uses the MAC address of the Ethernet interface for the WLAN interface. The network is also informed of the MAC addresses connected to the Ethernet interface of the client. Up to eight MAC addresses can be used.
- **MAC Address**
  If you have selected "Manual" for "MAC Mode", enter the MAC address of the client.
- **Any SSID**
  - Enabled

    In client mode, the access point attempts to connect to the network with the best transmission quality and that has suitable security settings. The clients can only connect to the access point on which the "Broadcast SSID" option is enabled.
  - Disabled

    The client attempts to connect to the access point from the SSID list that provides the best transmission quality and on which the "Broadcast SSID" option is disabled.
- **Roaming Threshold**
  Specify the threshold after which the client roams to the new access point.
  - High
    Changes only at a significantly higher field strength to the AP with the stronger signal.
  - Medium
    Changes at a moderately higher field strength to the AP with the stronger signal.
  - Low
    Changes at a slightly higher field strength to the AP with the stronger signal.

- Background Scan Mode
  While the client is connected to an access point, it scans for other access points in the background with which it can connect when necessary. Specify the mode for the scan.

  The following options are available:

  – always
    The client scans continuously for access points.

  – idle
    If there is no data traffic for a certain time, a scan is started for further access points.

  – disabled
    As long as the client is connected, there is no scan for further access points.

- Background Scan Interval [ms]
  Specify the interval at which further access points are scanned.

Table 2 has the following columns:

- Radio
  Shows the WLAN interface.
- Scan channels
  Shows the channels on which the client searches for an access point. The display depends on the wireless approvals of the selected country and the settings for "Allowed Channels".

Table 3 has the following columns:

- Enabled
  Enables or disables the relevant SSID.
- Radio
  Shows the WLAN interface.
- SSID
  Enter the SSID of the access point with which the client will connect.
  For the SSID, ASCII code 0x20 to 0x7e is used.

Procedure

1. From the "MAC Mode" drop-down list, select the required assignment of the MAC address.
2. In table 2, enter an SSID for "SSID" and enable the required SSID.
3. Disable the "Any SSID" function.
4. Click the "Set Values" button.

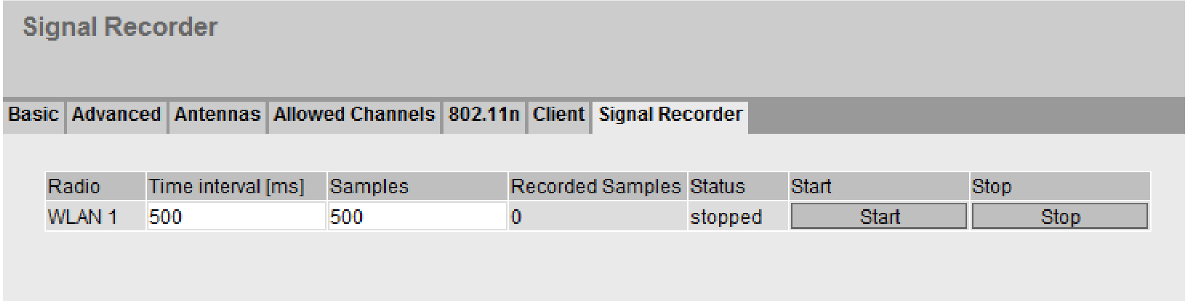
5.6.2.11 Signal Recorder

Recording the signal strength

The signal recorder displays or records the received signal strength of the connected access point. Using this data, you can locate areas with an inadequate signal strength. The signal recorder can be particularly useful when the client moves along a fixed path.

Note

This tab is only available in the client mode. The WLAN interface of the device must be enabled, otherwise no recording is possible.


Signal Recorder

Radio	Time interval [ms]	Samples	Recorded Samples	Status	Start	Stop
WLAN 1	500	500	0	stopped	Start	Stop

Description

This table contains the following columns:

- Radio
  Shows the WLAN interface to which the information applies. Since a client has a WLAN interface, there is only ever one row for "WLAN 1" in this table.
- Time interval [ms]
  The time interval between acquiring two measured values in milliseconds.
- Samples
  The number of measurements.
- Recorded Samples
  Number of currently taken measurements or the number of measurements taken during the last recording
- Status
  The status of the recording
  - stopped
    There is currently no recording of the signal strength.
  - started
    The signal strength is being recorded.

- Start
  Click the button in this column to start recording the signal strength.

  Note
  - If you start a new recording, the previous recording will be overwritten.
  - When the device restarts, the measured values are deleted.

- Stop
  Click the button in this column to stop recording the signal strength prematurely. If the specified number of measurements has been made, recording of the signal strength stops automatically.

Notes on usage

Note the following tips that will help you to obtain useful measurements with the signal recorder:

- Set a fixed data rate on the access point.
- If you have activated iPCF, set as low a cycle time on the access point as possible for the measurements.
- Make sure that there is enough data communication during the measurement because the statistics functions evaluate incoming data frames.
- The measurement path should be traveled 2 to 3 times with the same parameters to find out whether losses of signal strength always occur at the same position.
- Selective measurements at a fixed position should be made over a longer period of time.

Note

- If you start a new recording, the previous recording will be overwritten.
- When the device restarts, the measured values are deleted.

Procedure

1. Enter the values required for the interval between two measurements and the number of measurements.
2. Click the "Start" button, the display "started" appears in the "Status" column.
3. When "stopped" is displayed again in the "Status" column, recording of the signal strength has been completed.
4. Change to one of the following menu items to call up the result of the recording:
   – System > Load&Save > HTTP
   Click the "Save" button in the "WLANSigRec" table row to save the file "signal_recorder_SCALANCE_W700.zip" in the file system of the connected PC.
   – System > Load&Save > TFTP
   If necessary, change the file name "signal_recorder_SCALANCE_W700.zip" in the

"WLANSigRec" table row. In the table row "WLANSigRec", select the "Save file" entry from the drop-down list and click the "Set Values" button.

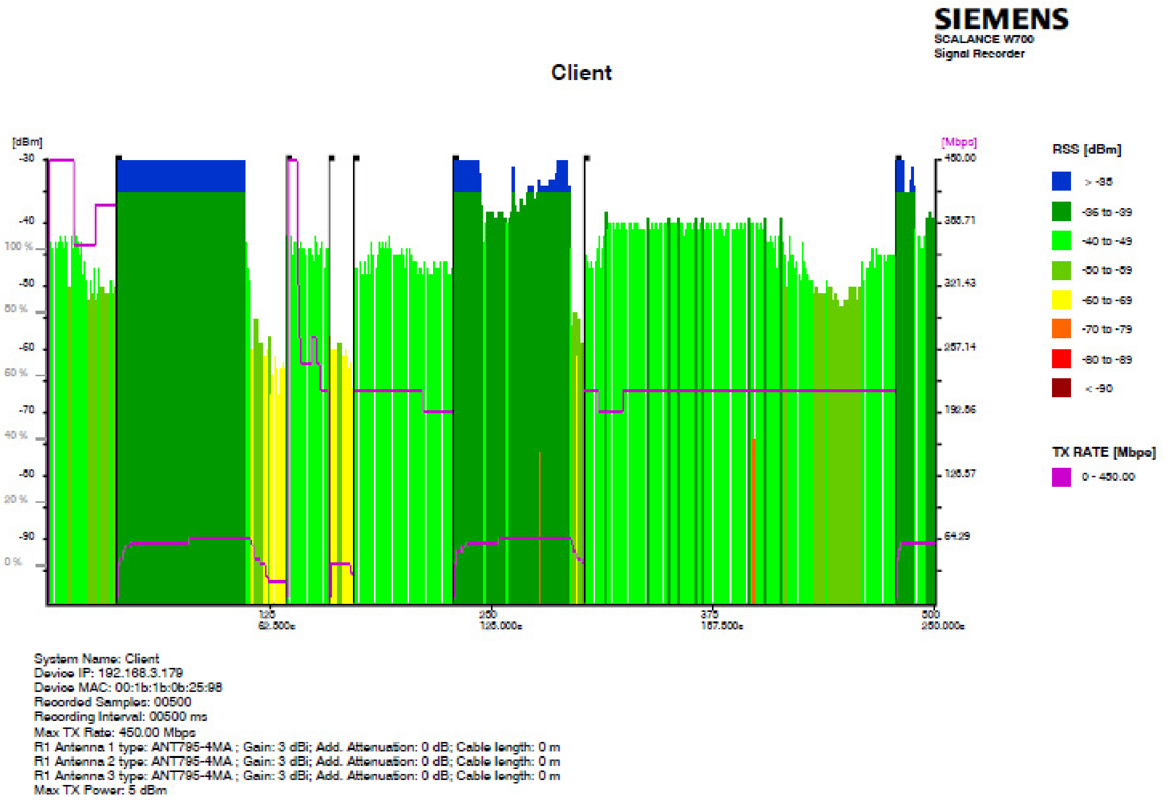
5. The ZIP file contains two files with the results of the recording:
   - A PDF file
   - A CSV file

Measurement results

PDF file

The PDF file contains information on the configuration of the device and detailed information about all individual measurements. There is also a graphic representation of the curve of the RSSI values in dBm and the data rate.

If the client changes the access point (roaming) during the measurement, this is indicated by vertical black bars with a black square at the tip. The range > -35 dBm (blue) is the overmodulation range, in other words the WLAN card overmodulates.



System Name: Client
Device IP: 192.168.3.179
Device MAC: 00:1b:1b:0b:25:98
Recorded Samples: 00500
Recording Interval: 00500 ms
Max TX Rate: 450.00 Mbps
R1 Antenna 1 type: ANT795-4MA ; Gain: 3 dBi; Add. Attenuation: 0 dB; Cable length: 0 m
R1 Antenna 2 type: ANT795-4MA ; Gain: 3 dBi; Add. Attenuation: 0 dB; Cable length: 0 m
R1 Antenna 3 type: ANT795-4MA ; Gain: 3 dBi; Add. Attenuation: 0 dB; Cable length: 0 m
Max TX Power: 5 dBm

CSV file

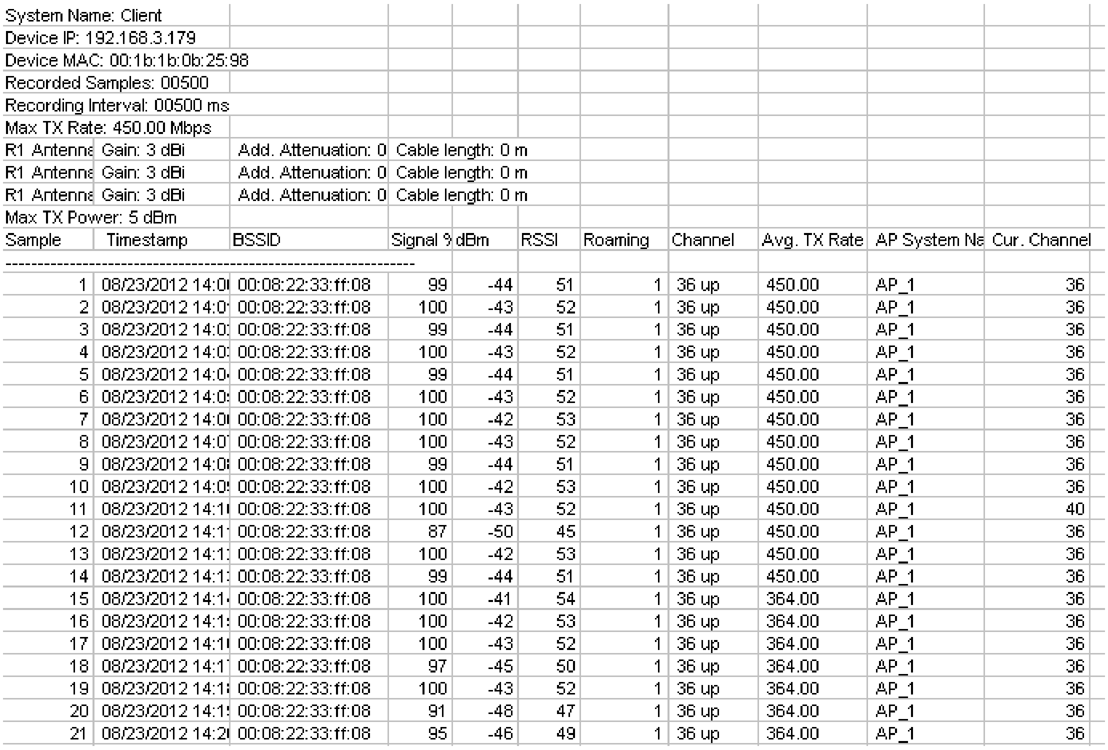
The CSV file contains information on the configuration of the device and detailed information on all individual measurements and is divided into two areas: The first area contains the configured settings:

- The system name of the client
- The IP address of the device
- The MAC address of the device
- The total number of measured values
- The interval between acquisition of two measured values
- The maximum data rate
- The setting of the external antennas
- The maximum possible transmit power

The second area is a table. The table contains the following for each measured value:

- The consecutive number of the measurement
- The time stamp
- The BSSID
- The received signal strength in % and in dBm
- The raw value of the RSSI (Received Signal Strength Indication)
- The roaming indicator. The indicator changes between 0 and 1 with each roam
- The channel on which the client is connected to the access point

- The average data rate (if there is no data exchange between the access point and client, the data rate is "0")
- The name of the access point
- The current channel (this can also be the channel that the client is currently scanning)



System Name: Client										
Device IP: 192.168.3.179										
Device MAC: 00:1b:1b:0b:25:98										
Recorded Samples: 00500										
Recording Interval: 00500 ms										
Max TX Rate: 450.00 Mbps										
R1 Antenna	Gain: 3 dBi	Add. Attenuation: 0	Cable length: 0 m							
R1 Antenna	Gain: 3 dBi	Add. Attenuation: 0	Cable length: 0 m							
R1 Antenna	Gain: 3 dBi	Add. Attenuation: 0	Cable length: 0 m							
Max TX Power: 5 dBm										
Sample	Timestamp	BSSID	Signal %	dBm	RSSI	Roaming	Channel	Avg. TX Rate	AP System Na	Cur. Channel
--										
1	08/23/2012 14:00	00:08:22:33:ff:08	99	-44	51	1	36 up	450.00	AP_1	36
2	08/23/2012 14:01	00:08:22:33:ff:08	100	-43	52	1	36 up	450.00	AP_1	36
3	08/23/2012 14:02	00:08:22:33:ff:08	99	-44	51	1	36 up	450.00	AP_1	36
4	08/23/2012 14:03	00:08:22:33:ff:08	100	-43	52	1	36 up	450.00	AP_1	36
5	08/23/2012 14:04	00:08:22:33:ff:08	99	-44	51	1	36 up	450.00	AP_1	36
6	08/23/2012 14:05	00:08:22:33:ff:08	100	-43	52	1	36 up	450.00	AP_1	36
7	08/23/2012 14:06	00:08:22:33:ff:08	100	-42	53	1	36 up	450.00	AP_1	36
8	08/23/2012 14:07	00:08:22:33:ff:08	100	-43	52	1	36 up	450.00	AP_1	36
9	08/23/2012 14:08	00:08:22:33:ff:08	99	-44	51	1	36 up	450.00	AP_1	36
10	08/23/2012 14:09	00:08:22:33:ff:08	100	-42	53	1	36 up	450.00	AP_1	36
11	08/23/2012 14:10	00:08:22:33:ff:08	100	-43	52	1	36 up	450.00	AP_1	40
12	08/23/2012 14:11	00:08:22:33:ff:08	87	-50	45	1	36 up	450.00	AP_1	36
13	08/23/2012 14:12	00:08:22:33:ff:08	100	-42	53	1	36 up	450.00	AP_1	36
14	08/23/2012 14:13	00:08:22:33:ff:08	99	-44	51	1	36 up	450.00	AP_1	36
15	08/23/2012 14:14	00:08:22:33:ff:08	100	-41	54	1	36 up	364.00	AP_1	36
16	08/23/2012 14:15	00:08:22:33:ff:08	100	-42	53	1	36 up	364.00	AP_1	36
17	08/23/2012 14:16	00:08:22:33:ff:08	100	-43	52	1	36 up	364.00	AP_1	36
18	08/23/2012 14:17	00:08:22:33:ff:08	97	-45	50	1	36 up	364.00	AP_1	36
19	08/23/2012 14:18	00:08:22:33:ff:08	100	-43	52	1	36 up	364.00	AP_1	36
20	08/23/2012 14:19	00:08:22:33:ff:08	91	-48	47	1	36 up	364.00	AP_1	36
21	08/23/2012 14:20	00:08:22:33:ff:08	95	-46	49	1	36 up	364.00	AP_1	36

5.7 "Layer 2" menu

5.7.1 VLAN

5.7.1.1 General

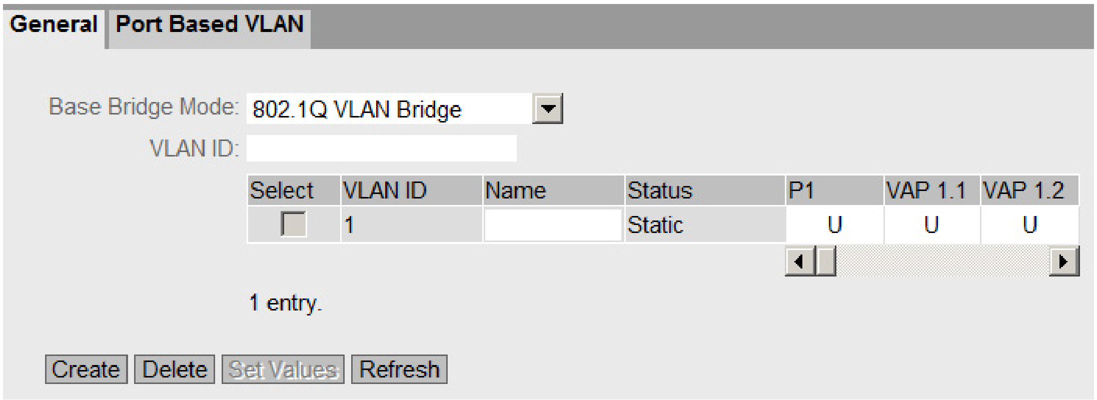
VLAN configuration page

On this page, you define the VLAN and specify the use of the ports.

Note

Changing the Agent VLAN ID

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



Base Bridge Mode: 802.1Q VLAN Bridge

VLAN ID:

Select	VLAN ID	Name	Status	P1	VAP 1.1	VAP 1.2
□	1		Static	U	U	U

1 entry.

Important rules for VLANs

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

Frames with the VLAN ID "0" are handled as untagged frames but retain their priority value.

As default, all ports on the device send frames without a VLAN tag to ensure that the end node can receive these frames.
With SCALANCE W devices, the VLAN ID 1 is the default on all ports.

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).

Description

The page contains the following boxes:

- **"Base Bridge Mode" drop-down list**
  Specify 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
- **Input box "VLAN ID"**
  Enter the VLAN ID in the "VLAN ID" input box.
  Range of values: 1 ... 4094

The table has the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **VLAN ID**
  Shows the VLAN ID. The VLAN ID (a number between 1 and 4094) can only be assigned once when creating a new data record and can then no longer be changed. To make a change, the entire data record must be deleted and created again. Up to 24 VLANs can be defined.
- **Name**
  Enter a name for the VLAN. The name only provides information and has no effect on the configuration. The length is a maximum of 32 characters.
- **Status**
  Shows the status type of the entry in the internal port filter table. Here, static means that the address was entered as a static address by the user.
- **List of ports**
  Specify the use of the port. The following options are available:
  - "-"
    The port is not a member of the VLAN.
    With a new definition, all ports have the identifier "-".
  - M
    The port is a member of the VLAN. Frames sent in this VLAN are forwarded with the corresponding VLAN tag.
  - U (uppercase)
    The port is an untagged member of the VLAN. Frames sent in this VLAN are forwarded without the VLAN tag. Frames without a VLAN tag are sent from this port.
  - u (lowercase)
    The port is an untagged member of the VLAN, but the VLAN is not configured as a port VLAN. Frames sent in this VLAN are forwarded without the VLAN tag.
  - F
    The port is not a member of the specified VLAN. You can configure other settings in "Layer 2 > VLAN > Port-based VLAN".

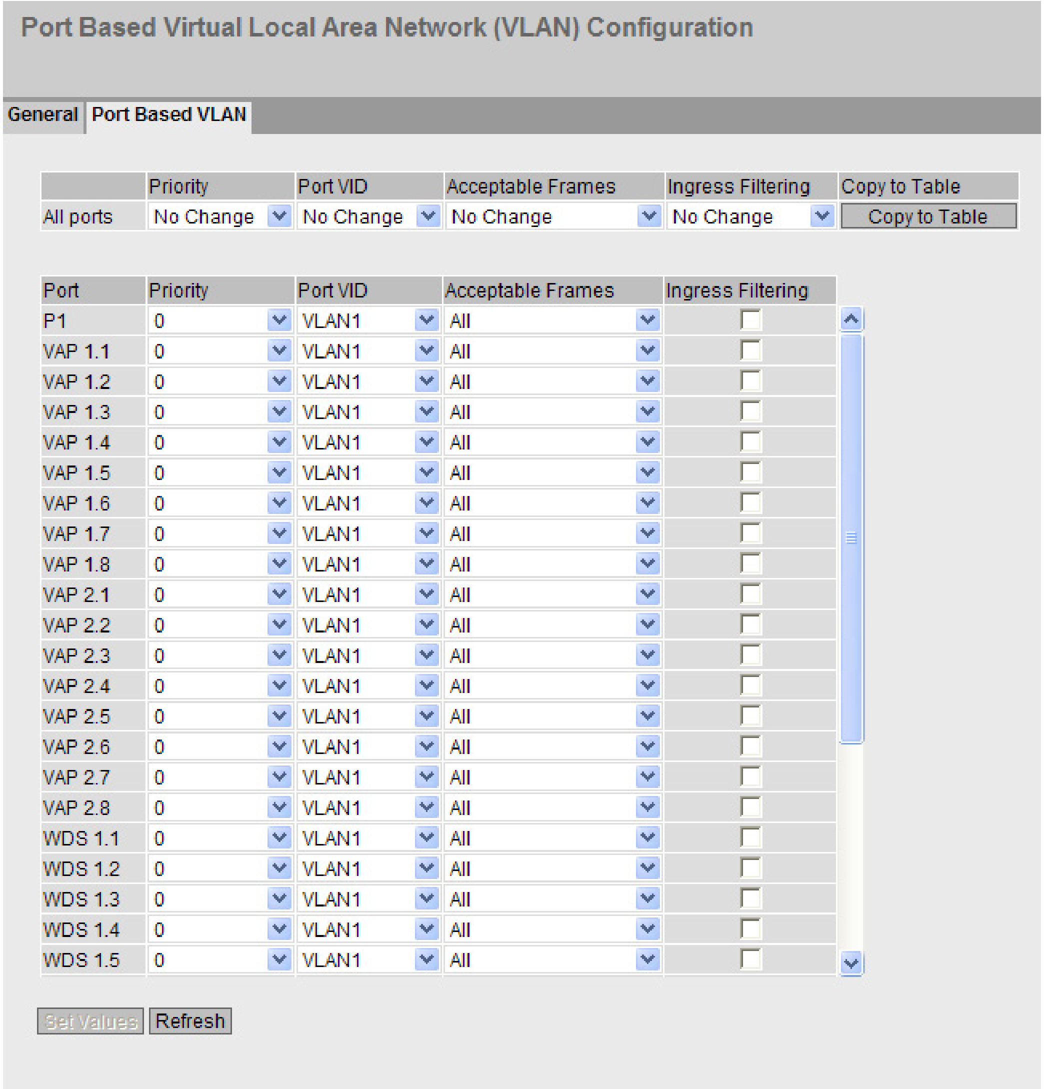
Procedure

1. Enter an ID in the "VLAN ID" input box.
2. Click the "Create" button. A new entry is generated in the table. As default, the boxes have "-" entered.
3. Enter a name for the VLAN under Name.
4. Specify the use of the port in the VLAN. If, for example you select M, the port is a member of the VLAN. The frame sent in this VLAN is forwarded with the corresponding VLAN tag.
5. Specify the mode of the device.
6. Click the "Set Values" button.

5.7.1.2 Port-based VLAN

Processing received frames

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



Port Based Virtual Local Area Network (VLAN) Configuration

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

Port	Priority	Port VID	Acceptable Frames	Ingress Filtering
P1	0	VLAN1	All	□
VAP 1.1	0	VLAN1	All	□
VAP 1.2	0	VLAN1	All	□
VAP 1.3	0	VLAN1	All	□
VAP 1.4	0	VLAN1	All	□
VAP 1.5	0	VLAN1	All	□
VAP 1.6	0	VLAN1	All	□
VAP 1.7	0	VLAN1	All	□
VAP 1.8	0	VLAN1	All	□
VAP 2.1	0	VLAN1	All	□
VAP 2.2	0	VLAN1	All	□
VAP 2.3	0	VLAN1	All	□
VAP 2.4	0	VLAN1	All	□
VAP 2.5	0	VLAN1	All	□
VAP 2.6	0	VLAN1	All	□
VAP 2.7	0	VLAN1	All	□
VAP 2.8	0	VLAN1	All	□
WDS 1.1	0	VLAN1	All	□
WDS 1.2	0	VLAN1	All	□
WDS 1.3	0	VLAN1	All	□
WDS 1.4	0	VLAN1	All	□
WDS 1.5	0	VLAN1	All	□

Description

Table 1 has the following columns:

- **Port**
  Shows that the settings are valid for all ports of table 2.
- **Priority / Port VID / Acceptable Frames / Ingress Filtering**
  In the drop-down list, select the setting for all ports. If "No Change" is selected, the entries of the corresponding column in Table 2 remain unchanged.
- **Copy to Table**
  If you click the button, the setting is adopted for all ports of table 2.

Note

Table 1 is only available if at least one VLAN is configured.

Table 2 has the following columns:

- **Port**
  Shows the available ports and interfaces.
- **Priority**
  From the drop-down list, select the priority given to untagged frames.

  The CoS priority (Class of Service) used in the VLAN tag. If a frame is received without a tag, it will be assigned this priority. This priority specifies how the frame is further processed compared with other frames.
  There are a total of eight priorities with values 0 to 7, where 7 represents the highest priority (IEEE 802.1p Port Priority).
- **Port VID**
  Select the VLAN ID from the drop-down list. Only VLAN IDs defined on the "VLAN > General" page can be selected.
  If a received frame does not have a VLAN tag, it has a tag with the VLAN ID specified here added to it and is sent according to the rules at the port.

- **Acceptable Frames**
  Specify which types of frames will be accepted. The following alternatives are possible:
  - Tagged Frames Only
    The device discards all untagged frames. Otherwise, the forwarding rules apply according to the configuration.
  - All
    The device forwards all frames.
- **Ingress Filtering**
  Specify whether the VID of received frames is evaluated
  You have the following options:
  - Enabled
    The VLAN ID of received frames decides whether they are forwarded: To forward a VLAN tagged frame, the receiving port must be a member in the same VLAN. Frames from unknown VLANs are discarded at the receiving port.
  - Disabled
    All frames are forwarded.

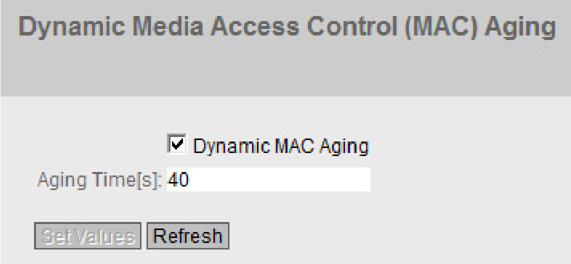
Procedure

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

5.7.2 Dynamic MAC Aging

Protocol settings and switch functionality

The device automatically learns the source addresses of the connected nodes. This information is used to forward frames to the nodes specifically involved. This reduces the network load for the other nodes.
If a device does not receive a frame whose source address matches a learnt address within a certain time, it deletes the learnt address. This mechanism is known as "Aging". Aging prevents frames being forwarded incorrectly, for example when an end device (for example a programming device) is connected to a different port.
If the check box is not enabled, a device does not delete learnt addresses automatically.



Dynamic Media Access Control (MAC) Aging

☑ Dynamic MAC Aging

Aging Time[s]: 40

Description

The page contains the following boxes:

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

Procedure

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

5.7.3 Spanning Tree

5.7.3.1 General

General settings of spanning tree

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

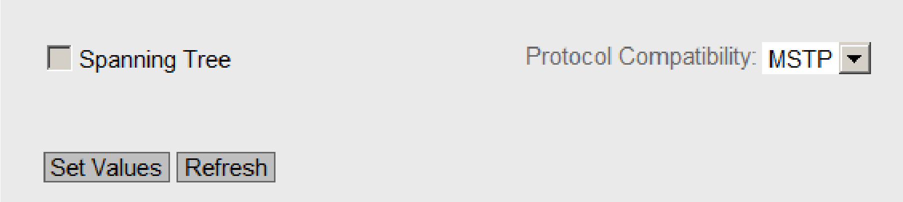
On the configuration pages of these functions, you can make detailed settings.

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

Note

Client device not as root

Using the configuration of priorities and path costs, make sure that a client device can never become the root node. If a client device becomes the root node the Rapid Spanning Tree function no longer works.



☐ Spanning Tree

Protocol Compatibility: MSTP

Description

The page contains the following boxes:

- **Check box "Spanning Tree"**
  Enable or disable MSTP.
- **Drop-down list "Protocol Compatibility"**
  Select the compatibility mode of MSTP, for example if you select RSTP, MSTP behaves like RSTP.

  The following settings are available:

  – STP

  – RSTP

  – MSTP

  Note

  If iPCF mode is enabled, only the compatibility modes STP and RSTP are supported.

Procedure

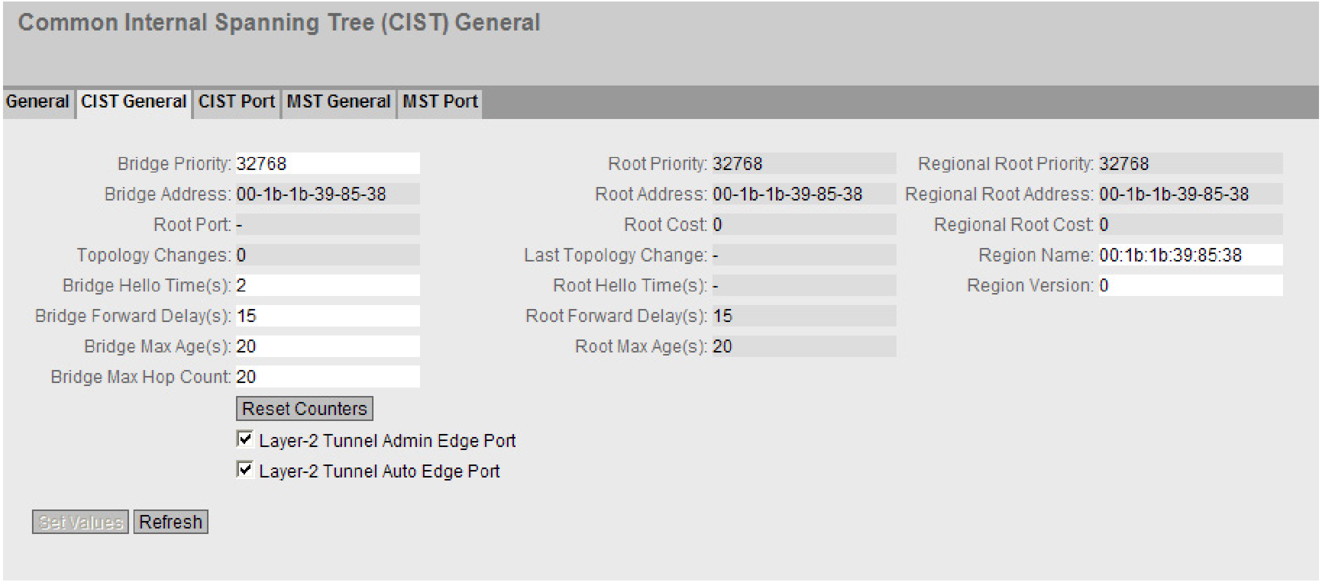
1. Select the "MSTP" check box.
2. From the "Protocol Compatibility" drop-down list, select the type of compatibility.
3. Click the "Set Values" button.

5.7.3.2 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.
- 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 "Protocol Compatiblity" is set to "Spanning Tree". 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
Bridge Address: 00-1b-1b-39-85-38
Root Port: -
Topology Changes: 0
Bridge Hello Time(s): 2
Bridge Forward Delay(s): 15
Bridge Max Age(s): 20
Bridge Max Hop Count: 20

☑ Layer-2 Tunnel Admin Edge Port
☑ Layer-2 Tunnel Auto Edge Port

Root Priority: 32768
Root Address: 00-1b-1b-39-85-38
Root Cost: 0
Last Topology Change: -
Root Hello Time(s): -
Root Forward Delay(s): 15
Root Max Age(s): 20

Regional Root Priority: 32768
Regional Root Address: 00-1b-1b-39-85-38
Regional Root Cost: 0
Region Name: 00:1b:1b:39:85:38
Region Version: 0

Description

The page contains the following boxes:

- **"Bridge Priority" / "Root Priority" input box**
  The Bridge priority decides which device becomes the root bridge. The bridge with the highest priority becomes the root bridge. The lower the value, the higher the priority. 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 61440.

- **Bridge Adresse / Root Adresse**
  The bridge address shows the MAC address of the device and the root address shows the MAC address of the root bridge.
- **Root Port**
  Shows the port via which the switch communicates with the root bridge.
- **Root Cost**
  The path costs from this device to the root bridge.
- **Topologie 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]" input box**
  Each bridge regularly sends configuration frames (BPDUs). 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]" input box**
  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 started with the new topology only after all the bridges have the required information. The default for this parameter is 15 seconds.
- **"Bridge Max Age" / "Root Max Age" input box**
  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.
- **"Bridge Max Hop Count" input box**
  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.
- **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.
- **"Region Name" input box**
  Enter 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" input box**
  Enter the 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.
- **"Reset Counters" button**
  The values are reset with this button.
- **"Layer-2 Tunnel Admin Edge Port" check box (available only in access point mode)**
  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" check box (available only in access point mode)**
  Select this check box if you want to detect automatically whether or not an end device is connected at all layer 2 tunnel ports.

Procedure

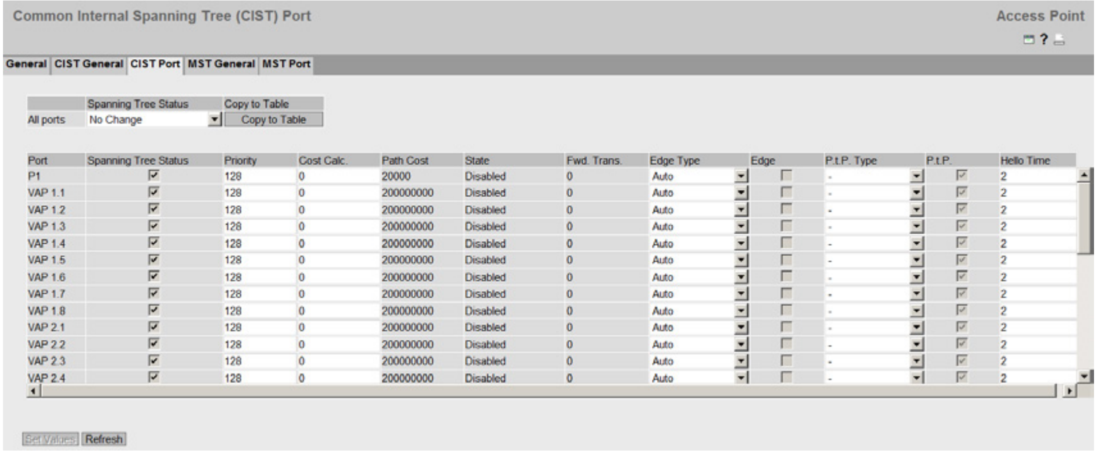
1. Enter the data required for the configuration in the input boxes.
2. Click the "Set Values" button.

5.7.3.3 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.



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

Port	Spanning Tree Status	Priority	Cost Calc.	Path Cost	State	Fwd. Trans.	Edge Type	Edge	P.t.P. Type	P.t.P.	Hello Time
P1	☑	128	0	20000	Disabled	0	Auto	□	-	☑	2
VAP 1.1	☑	128	0	200000000	Disabled	0	Auto	□	-	☑	2
VAP 1.2	☑	128	0	200000000	Disabled	0	Auto	□	-	☑	2
VAP 1.3	☑	128	0	200000000	Disabled	0	Auto	□	-	☑	2
VAP 1.4	☑	128	0	200000000	Disabled	0	Auto	□	-	☑	2
VAP 1.5	☑	128	0	200000000	Disabled	0	Auto	□	-	☑	2
VAP 1.6	☑	128	0	200000000	Disabled	0	Auto	□	-	☑	2
VAP 1.7	☑	128	0	200000000	Disabled	0	Auto	□	-	☑	2
VAP 1.8	☑	128	0	200000000	Disabled	0	Auto	□	-	☑	2
VAP 2.1	☑	128	0	200000000	Disabled	0	Auto	□	-	☑	2
VAP 2.2	☑	128	0	200000000	Disabled	0	Auto	□	-	☑	2
VAP 2.3	☑	128	0	200000000	Disabled	0	Auto	□	-	☑	2
VAP 2.4	☑	128	0	200000000	Disabled	0	Auto	□	-	☑	2

Description

Table 1 has the following columns:

- **Column 1**
  Shows that the settings made in this table will be adopted for all ports of table 2 after clicking the "Copy to Table" button.
- **Spanning Tree Status**
  In the drop-down list, select the setting for all ports. If "No Change" is selected, the entries of the corresponding column in table 2 remain unchanged.
- **Copy to Table**
  If you click the button, the settings are adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
  Shows all available ports and the following interfaces.
  - Port X
  - WLAN X
  - VAP X.Y
  - WDS X.Y
- **Spanning Tree Status**
  Specify whether the port is integrated in the spanning tree or not.

  Note

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

- **Priority**
  Enter the priority of the port. The priority is only evaluated when the path costs are the same.
  The value must be divisible by 16. If the value that cannot be divided by 16, the value is automatically adapted.
  Range of values: 0 - 240.
  The default is 128.
- **Cost Calc**
  Enter the path cost calculation. If you enter the value "0" here, the automatically calculated value is displayed in the "Path Cost" box.

- **Path Cost**
  The path costs from this port to the root bridge. The path with the lowest value is selected as the path. If several ports of a device have the same value, the port with the lowest port number is selected.
  If the value in the "Cost Calc" field is "0", the automatically calculated value is displayed. Otherwise, the value of the "Cost Calc" 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:

  – 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 "State" parameter depends on the configured protocol. The following is possible for status:

  – 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).

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

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

- **Edge Type**
  Specify the type of the edge port. You have the following options:
  - "-"
    Edge port is disabled. The port is treated as a "no EdgePort".
  - Admin
    Select this option when there is always an end device on this port. Otherwise a reconfiguration of the network will be triggered each time a connection is changed.
  - Auto
    Select this option if you want a connected end device to be detected automatically at this port. When the connection is established the first time, the port is treated as a "no Edge Port".
  - Admin/Auto
    Select these options if you operate a combination of both on this port. When the connection is established the first time, the port is treated as an Edge Port.
- **Edge**
  Shows the status of the port.
  - Enabled
    An end device is connected to this port.
  - Disabled
    There is a spanning tree or rapid spanning tree device at this port.

  With an end device, a switch can change over the port faster without taking into account spanning tree frames. If a spanning tree frame is received despite this setting, the port automatically changes to the "Disabled" setting for switches.
- **P.t.P. Type**
  Select the required option from the drop-down list. The selection depends on the port that is set.
  - 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 link means a direct connection between two devices. A shared media connection is, for example, a connection to a hub.
  - "-"
    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.
  - Enabled
    Shows that a point-to-point link exists.
  - Disabled
    Shows that no point-to-point link exists
- Hello Time
  Enter the interval after which the bridge sends configuration BPDUs. As default, 2 seconds is set.
  Range of values: 1-2 seconds

  Note

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

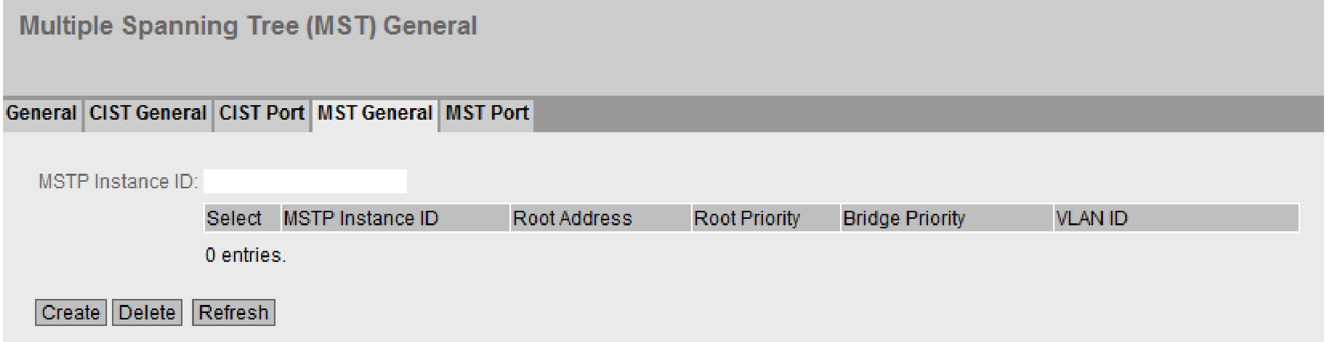
Procedure

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.

5.7.3.4 MST general

Multiple Spanning Tree configuration

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



Multiple Spanning Tree (MST) General

MSTP Instance ID:

Select	MSTP Instance ID	Root Address	Root Priority	Bridge Priority	VLAN ID

0 entries.

Description

The page contains the following box:

- **MSTP Instance ID**
  Enter the number of the MSTP instance.

Permitted values: 1 - 64
You can define up to 16 MSTP instances.

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **MSTP Instance ID**
  Shows the number of the MSTP instance.
- **Root Address**
  Shows the MAC address of the root bridge
- **Root Priority**
  Shows the priority of the root bridge.
- **Bridge Priority**
  Enter the bridge priority in this box. The value for the bridge priority is a whole multiple of 4096 with a range of values from 0 to 61440.
- **VLAN ID**
  Enter the VLAN ID. Here, you can also specify ranges with Start ID, "-", End ID. Several ranges or IDs are separated by ",".
  Permitted values: 1- 4094

Procedure

Creating a new entry

1. Enter the number of the MSTP instance in the "MSTP Instance ID" 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.

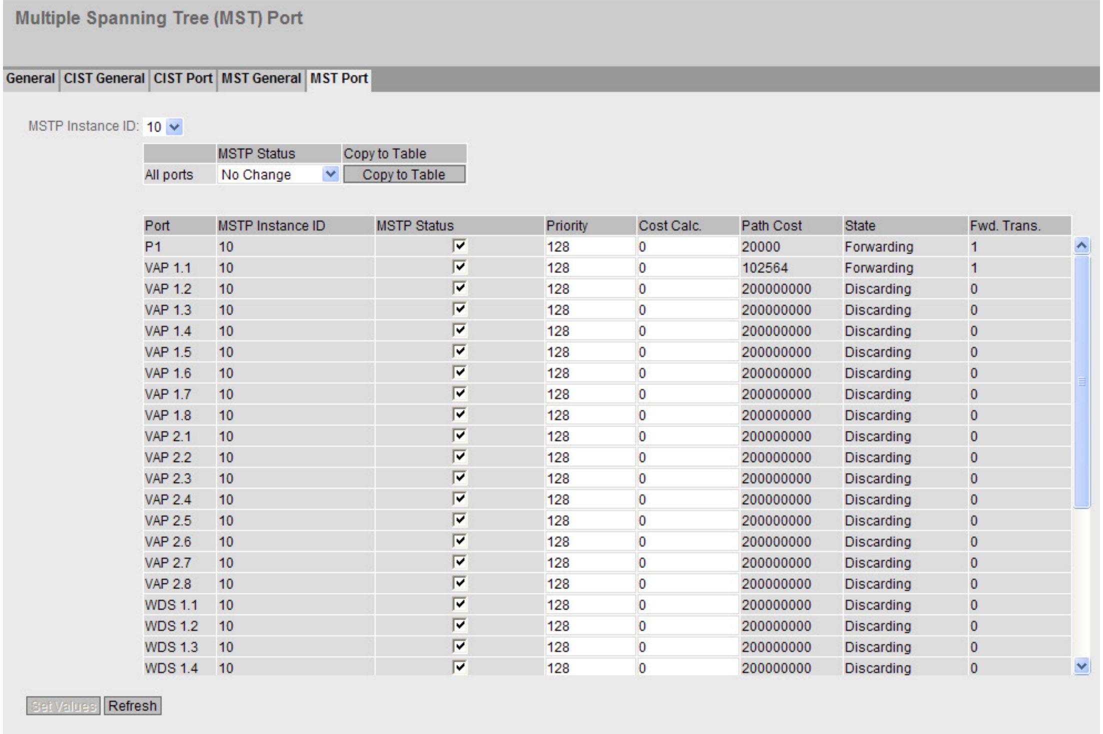
Deleting entries

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.

5.7.3.5 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.



Multiple Spanning Tree (MST) Port

MSTP Instance ID: 10

	MSTP Status	Copy to Table
All ports	No Change	Copy to Table

Port	MSTP Instance ID	MSTP Status	Priority	Cost Calc.	Path Cost	State	Fwd. Trans.
P1	10	☑	128	0	20000	Forwarding	1
VAP 1.1	10	☑	128	0	102564	Forwarding	1
VAP 1.2	10	☑	128	0	200000000	Discarding	0
VAP 1.3	10	☑	128	0	200000000	Discarding	0
VAP 1.4	10	☑	128	0	200000000	Discarding	0
VAP 1.5	10	☑	128	0	200000000	Discarding	0
VAP 1.6	10	☑	128	0	200000000	Discarding	0
VAP 1.7	10	☑	128	0	200000000	Discarding	0
VAP 1.8	10	☑	128	0	200000000	Discarding	0
VAP 2.1	10	☑	128	0	200000000	Discarding	0
VAP 2.2	10	☑	128	0	200000000	Discarding	0
VAP 2.3	10	☑	128	0	200000000	Discarding	0
VAP 2.4	10	☑	128	0	200000000	Discarding	0
VAP 2.5	10	☑	128	0	200000000	Discarding	0
VAP 2.6	10	☑	128	0	200000000	Discarding	0
VAP 2.7	10	☑	128	0	200000000	Discarding	0
VAP 2.8	10	☑	128	0	200000000	Discarding	0
WDS 1.1	10	☑	128	0	200000000	Discarding	0
WDS 1.2	10	☑	128	0	200000000	Discarding	0
WDS 1.3	10	☑	128	0	200000000	Discarding	0
WDS 1.4	10	☑	128	0	200000000	Discarding	0

Description

Table 1 has the following columns:

- **Column 1**
  Shows that the settings are valid for all ports of table 2.
- **MSTP Status**
  Select the setting for all ports from the drop-down list. If "No Change" is selected, the entries of the corresponding column in Table 2 remain unchanged.
- **Copy to Table**
  If you click the button, the setting is adopted for all ports of table 2.

The page contains the following box:

- **"MSTP Instance ID" drop-down list**
  In the drop-down list, select the ID of the MSTP instance.

Table 2 has the following columns:

- **Port**
  Shows all available ports and interfaces.
- **MSTP Instance ID**
  ID of the MSTP instance.
- **MSTP Status**
  Click the check box to enable or disable this option.
- **Priority**
  Enter the priority of the port. The priority is only evaluated when the path costs are the same.
  The value must be divisible by 16. If the value that cannot be divided by 16, the value is automatically adapted.
  Range of values: 0 - 240.
  The default is 128.
- **Cost Calc**
  Enter the path cost calculation 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**
  The path costs from this port to the root bridge. The path with the lowest value is selected as the path. If several ports of a device have the same value, the port with the lowest port number is selected.
  If the value in the "Cost Calc" field is "0", the automatically calculated value is displayed. Otherwise, the value of the "Cost Calc" field is displayed.
  The calculation of the path costs is largely based on the transmission speed. The higher the achievable transmission 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 is possible for status:
  - Discarding
    The port exchanges MSTP information but is not involved in the data traffic.
  - Blocked
    In the blocking mode, BPDU frames are received.
  - Forwarding
    The port receives and sends data frames.
- **Fwd. Trans.**
  Specifies the number of status changes Discarding - Forwarding or Forwarding - Discarding.

Procedure

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.

5.7.4 DCP Forwarding

Applications

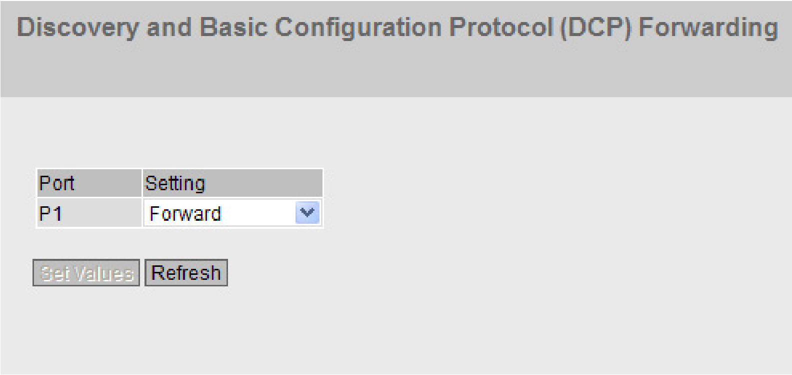
The DCP protocol is used by STEP 7 and the PST Tool for configuration and diagnostics. When shipped, DCP is enabled on all ports; in other words, DCP frames are forwarded at all ports. With this option, you can disable the sending of these frames for individual ports, for example to prevent individual 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 WBM page.

Note

Empty table

If you have enabled NAT on the device, the table is empty or will be emptied.



Discovery and Basic Configuration Protocol (DCP) Forwarding

Port	Setting
P1	Forward

Description

The table has the following columns:

- **Port**
  Shows the available ports.
- **Setting**
  Specify whether the port should block or forward outgoing DCP frames. You have the following options available:
  – Block
    No outgoing DCP frames are forwarded via this port. It is nevertheless still possible to receive via this port.
  – Forward
    The DCP frames are forwarded via this port.

Procedure

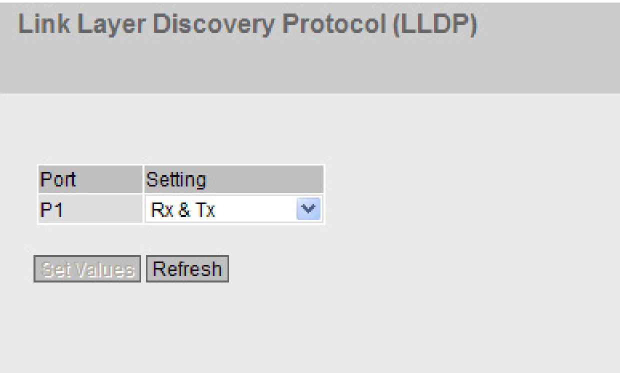
1. Specify whether the port blocks or forwards the DCP frames.
2. Click the "Set Values" button.

5.7.5 LLDP

Link Layer Discovery Protocol (LLDP)

PROFINET uses the LLDP protocol for topology diagnostics.
In the factory settings, LLDP is activated on the interface, in other words LLDP frames are sent and received. LLDP is supported only by the Ethernet interface and by the SFP interface P1.

On this WBM page, you activate or deactivate the sending or receiving of LLDP frames on the interface.



Link Layer Discovery Protocol (LLDP)

Port	Setting
P1	Rx & Tx

Description

The table has the following columns:

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

Procedure

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

5.8 "Layer 3" menu

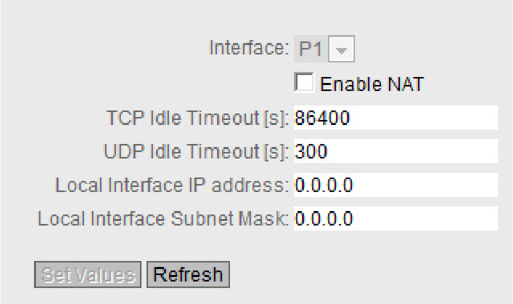
5.8.1 NAT

5.8.1.1 Basic

Note

This tab is only available in the client mode.

On this page, you specify the basic settings for NAT.



Interface: P1

□ Enable NAT

TCP Idle Timeout [s]: 86400

UDP Idle Timeout [s]: 300

Local Interface IP address: 0.0.0.0

Local Interface Subnet Mask: 0.0.0.0

Description

The page contains the following boxes:

- **Drop-down list "Interface"**
  From the drop-down list, select the required Ethernet interface.
- **Check box "Enable NAT"**
  Enable or disable NAT for the Ethernet interface. Can only be enabled if "Own" is set on the client for "MAC Mode".
- **Input box "TCP Idle Timeout [s]"**
  Enter the required time in seconds. If no data exchange takes place, the TCP connection is deleted from the translation table when this time has elapsed.
  The range of values is 1 to 4294967295.
  Default setting: 86400 seconds
- **Input box "UDP Idle Timeout [s]"**
  Enter the required time in seconds. If no data exchange takes place, the UDP connection is deleted from the translation table when this time has elapsed.
  The range of values is 1 to 4294967295.
  Default setting: 300 seconds

- **Input box "Local Interface IP address"**
  Enter the local IP address of the Ethernet interface. This IP address is the gateway address of the local device.
- **Input box "Local Interface Subnet Mask"**
  Enter the subnet mask for the local Ethernet.

Procedure

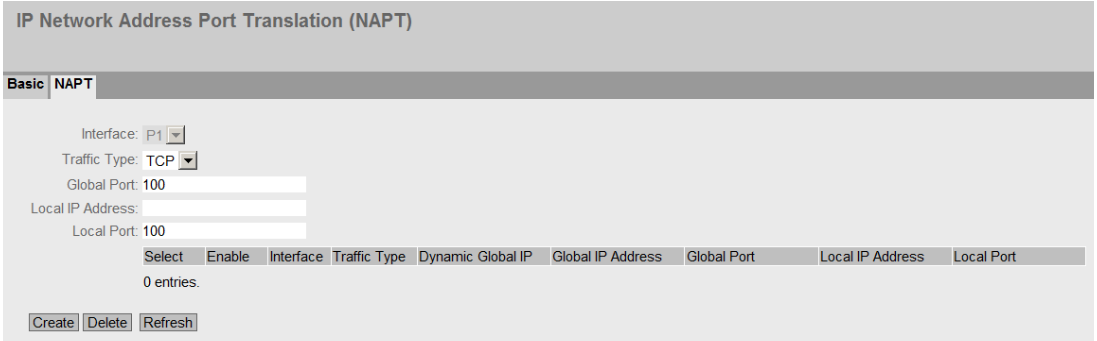
1. In the "Local Interface IP addresses" input box, enter the local IP address of the Ethernet interface.
2. In the "Local Interface Subnet Mask" input box, enter the subnet mask for the local Ethernet
3. Enable NAT for the Ethernet interface.
4. Click the "Set Values" button.

5.8.1.2 NAPT

Note

This tab is only available in the client mode.

On this WBM page, you define the translation list for communication from the global to the local network. Per WLAN client (NAT gateway), 60 entries are possible.



IP Network Address Port Translation (NAPT)

Interface: P1
Traffic Type: TCP
Global Port: 100
Local IP Address:
Local Port: 100

Select	Enable	Interface	Traffic Type	Dynamic Global IP	Global IP Address	Global Port	Local IP Address	Local Port

0 entries.

Description

The page contains the following boxes:

- **"Interface" drop-down list**
  Interface to which the settings relate. Can only be selected if the device has several interfaces.
- **"Traffic Type" drop-down list**
  Specify the protocol for which the address assignment is valid. TCP and UDP frames must have parameters set separately.

- **"Global Port" input box**
  Enter the global port. Incoming frames with this port as the destination port are forwarded. If the setting is intended to apply to a port range, enter the range with start port "-" end port, for example 30 - 40.

  Note

  If the port is already occupied by a local service, for example Telnet, a warning is displayed. In this case, avoid using TCP port 23 (Telnet), port 22 (SSH), ports 80/443 (http/https: reachability of the client with the WBM) and UDP port 161 (SNMP) as global port.

- **"Local IP Address" input box**
  Enter the IP address of the node in the local network.
- **"Local Port" input box**
  Enter the number of the port. This is the new destination port to which the incoming frame will be forwarded. If the setting is intended to apply to a port range, enter the range with start port "-" end port, for example 30 - 40.

  If the local port and global port are the same, the frames will be forwarded without port translation.

The table has the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **Enable**
  Select the check box in the required row. The entry is used for the address assignment
- **Interface**
  Shows the interface to which the settings relate.
- **Traffic Type**
  Shows whether UDP or TCP frames are assigned to the global port.
- **Dynamic Global IP**
  Shows whether or not dynamic address conversion is used.
- **Global IP Address**
  Shows the global IP address to which the local IP address will be translated.
- **Global Port**
  Shows the global port.
- **Local IP Address**
  Shows the IP address of the node in the local network.
- **Local Port**
  Shows the number of the local port.

Procedure

1. From the "Traffic Type" drop-down list, select the protocol for which the address assignment is valid.
2. Enter the number of the global port or a port range in "Global Port".

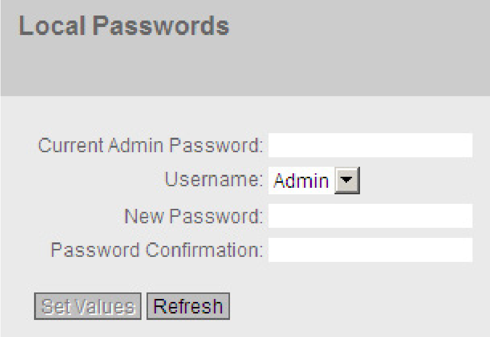
3. Enter the IP address of the node in the local network in "Local IP Address".
4. Enter the number of the local port or a port range in "Local Port".
5. Click the "Create" button. A new entry is generated in the table.
6. Click the "Set Values" button. The device is restarted.

5.9 "Security" menu

5.9.1 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: Admin

New Password:

Password Confirmation:

Procedure

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.
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:

- admin: admin
- user: user

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

Note

Changing the password in Trial mode

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

5.9.2 WLAN

5.9.2.1 Basic

Safety levels

To make the network secure, authentication and encryption are used. On this page, you specify the security settings.

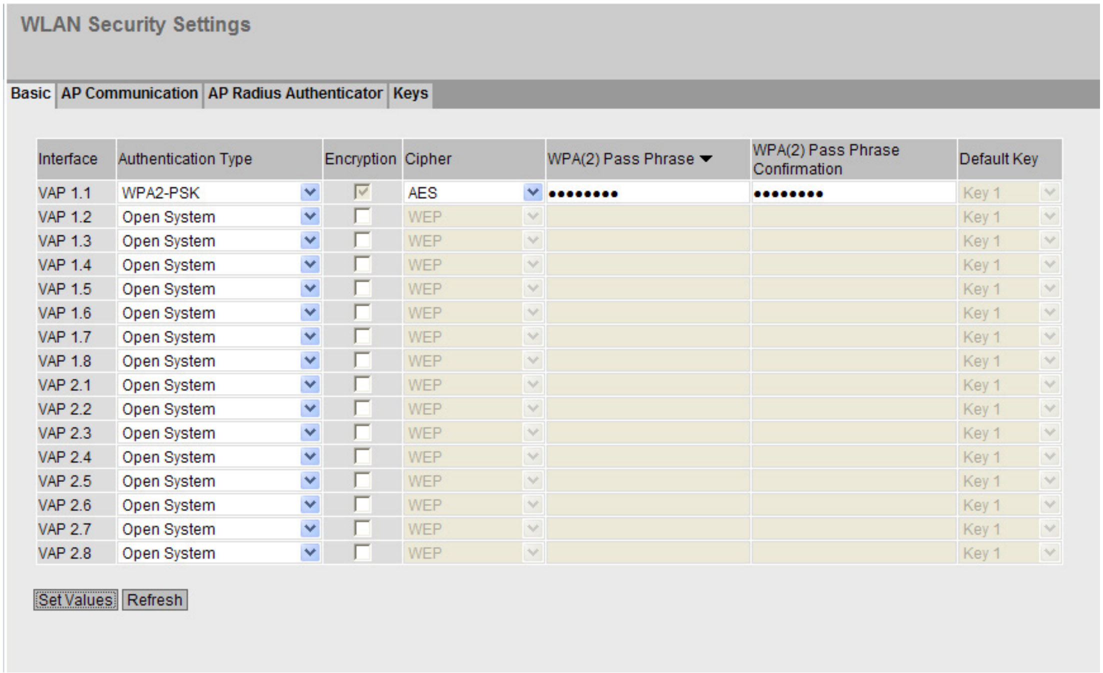
Note

Transmission standard IEEE 802.11 n

The transmission standard IEEE 802.11 n with the setting "802.11n" or "802.11 n only" supports only WPA2/ WPA2-PSK with AES in the security settings.

iPCF or iPCF-MC mode activated

If iPCF or iPCF-MC mode is enabled, only "Open System" with the encryption method AES is supported in the security settings.



Interface	Authentication Type	Encryption	Cipher	WPA(2) Pass Phrase ▼	WPA(2) Pass Phrase Confirmation	Default Key
VAP 1.1	WPA2-PSK	☑	AES	••••••••	••••••••	Key 1
VAP 1.2	Open System	□	WEP			Key 1
VAP 1.3	Open System	□	WEP			Key 1
VAP 1.4	Open System	□	WEP			Key 1
VAP 1.5	Open System	□	WEP			Key 1
VAP 1.6	Open System	□	WEP			Key 1
VAP 1.7	Open System	□	WEP			Key 1
VAP 1.8	Open System	□	WEP			Key 1
VAP 2.1	Open System	□	WEP			Key 1
VAP 2.2	Open System	□	WEP			Key 1
VAP 2.3	Open System	□	WEP			Key 1
VAP 2.4	Open System	□	WEP			Key 1
VAP 2.5	Open System	□	WEP			Key 1
VAP 2.6	Open System	□	WEP			Key 1
VAP 2.7	Open System	□	WEP			Key 1
VAP 2.8	Open System	□	WEP			Key 1

Description

The table has the following columns:

- **Interface**
  Shows the available interfaces.
- **Authentication Type**
  Select the type of authentication. The selection depends on the operating mode and the transmission standard.
  - **Open System**
    There is no authentication. Encryption with a fixed (unchanging) WEP key can be selected as an option. To use the key, enable "Encryption". You define the WEP key on the "Keys" page.
    If iPCF or iPCF-MC mode is enabled, only the encryption method AES with 128 bit key length is supported.
  - **Shared Key**
    In Shared Key authentication, a fixed key is stored on the client and access point. This WEP key is then used for authentication and encryption. You define the WEP key on the "Keys" page.

  Note

  If you use "Open System" with "Encryption" or "Shared Key", Key 1 must always be set on the "Keys" page.

  - **WPA (RADIUS)**
    Wi-Fi Protected Access is a method specified by the Wi-Fi Alliance to close security gaps in WEP. Authentication using a server is stipulated (802.1x). The dynamic exchange of keys at each data frame introduces further security.
  - **WPA-PSK**
    WPA Pre Shared Key (WPA-PSK) is a weakened form of WPA. In this method, authentication is not established by a server but is based on a password. This password is configured manually on the client and server.
  - **WPA2 (RADIUS)**
    WPA2 (Wi-Fi Protected Access 2) is a further development of WPA and implements the functions of the IEEE 802.11i security standard. WPA authentication works, however, without the RADIUS server.
  - **WPA2-PSK**
    WPA2-PSK is based on the 802.11i standard. WPA authentication works, however, without a RADIUS server. Instead of this, a WPA(2) key (WPA(2) pass phrase) is stored on each client and access point. The WPA(2) pass phrase is used for authentication and further encryption.
  - **WPA/WPA2-Auto-PSK**
    Setting with which an access point can process both the "WPA-PSK" as well as the "WPA2-PSK" type of authentication. This is necessary when the access point communicates with different clients, some using "WPA-PSK" and others "WPA2-PSK". The same encryption method is set on the clients.
  - **WPA/WPA2-Auto**
    Setting with which an access point can process both the "WPA" as well as the "WPA2"

type of authentication. This is necessary when the access point communicates with different clients, some using "WPA" and others "WPA2". The same encryption method is set on the clients

- **Encryption**
  Encryption protects the transferred data from eavesdropping and corruption. You can only disable encryption if you have selected "Open System" for authentication. All other security methods include both authentication and encryption.
- **Cipher**
  Select the encryption method. The selection depends on the transmission standard.
  - **AUTO**
    AES or TKIP is used depending on the capability of the other station.
  - **WEP**
    WEP (Wired Equivalent Privacy)
    A symmetrical stream encryption method with only 40- or 104-bit long keys based on the RC4 algorithm (Ron’s Code 4).
  - **TKIP (Temporal Key Integrity Protocol)**
    A symmetrical encryption method with the RC4 algorithm (Ron’s Code 4). In contrast to the weak WEP encryption, TKIP uses changing keys derived from a main key. TKIP can also recognize corrupted data frames.
  - **AES (Advanced Encryption Standard)**
    Strong symmetrical block encryption method based on the Rijndael algorithm that further improves the functions of TKIP.

  Note

  To provide better protection of your data against attacks, use WPA2/ WPA2-PSK with AES.

- **WPA(2) Pass Phrase**
  Enter a WPA(2) key here. This WPA(2) key must be known both at the client end and on the access point and is entered by the user at both ends.
  ASCII code 0x20 to 0x7e is used for the WPA(2) key.
- **WPA(2) Pass phrase confirmation**
  Confirm the entered WPA(2) key.
- **Default key**
  Specify the WEP key used to encrypt the data. You define the WEP key on the "Keys" page.

Procedure

1. Select the required security settings. Which settings are possible depends on the "Authentication Type" you have selected.

Authentication Type	Encryption	Cipher	Encryption key source
Open System	disabled	--	--
Open System	Enabled	WEP	Default key
Open System	Enabled	AES[1)]	Default key (128-bit)
Shared Key	Enabled	WEP	Default key
WPA (RADIUS)	Enabled	Auto/TKIP/AES	RADIUS Server
WPA-PSK	Enabled	Auto/TKIP/AES	WPA(2) pass phrase
WPA2 (RADIUS)	Enabled	Auto/TKIP/AES	RADIUS Server
WPA2-PSK	Enabled	Auto/TKIP/AES	WPA(2) pass phrase
WPA/WPA2-AutoPSK	Enabled	Auto/TKIP/AES	WPA(2) pass phrase
WPA/WPA2-Auto (RADIUS)	Enabled	Auto/TKIP/AES	RADIUS Server

[1)] available only with iPCF or iPCF-MC

2. Click the "Set Values" button.

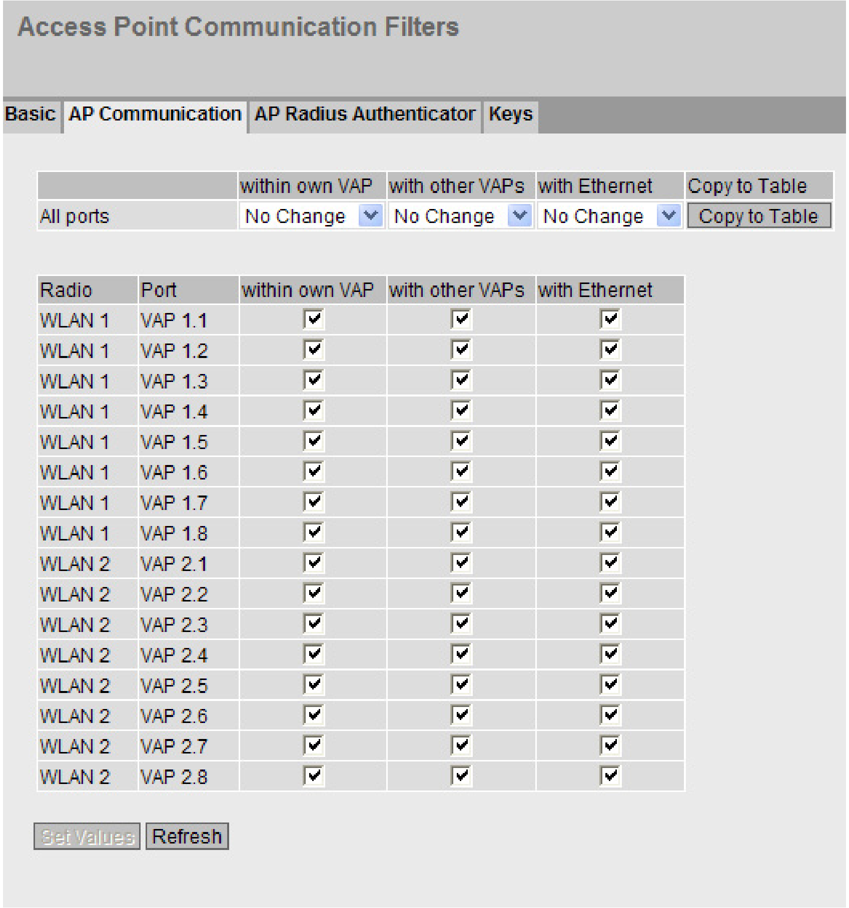
5.9.2.2 AP Communication

Communications options

On this page, you specify the type of communication allowed by the access point.

Note

This tab is available only in access point mode.



Access Point Communication Filters

	within own VAP	with other VAPs	with Ethernet	Copy to Table
All ports	No Change	No Change	No Change	Copy to Table

Radio	Port	within own VAP	with other VAPs	with Ethernet
WLAN 1	VAP 1.1	☑	☑	☑
WLAN 1	VAP 1.2	☑	☑	☑
WLAN 1	VAP 1.3	☑	☑	☑
WLAN 1	VAP 1.4	☑	☑	☑
WLAN 1	VAP 1.5	☑	☑	☑
WLAN 1	VAP 1.6	☑	☑	☑
WLAN 1	VAP 1.7	☑	☑	☑
WLAN 1	VAP 1.8	☑	☑	☑
WLAN 2	VAP 2.1	☑	☑	☑
WLAN 2	VAP 2.2	☑	☑	☑
WLAN 2	VAP 2.3	☑	☑	☑
WLAN 2	VAP 2.4	☑	☑	☑
WLAN 2	VAP 2.5	☑	☑	☑
WLAN 2	VAP 2.6	☑	☑	☑
WLAN 2	VAP 2.7	☑	☑	☑
WLAN 2	VAP 2.8	☑	☑	☑

Description

Table 1 has the following columns:

- **Column 1**
  Shows that the settings are valid for all ports of table 2.
- **within own VAP / with other VAPs / with Ethernet**
  In the drop-down list, select the setting for all ports. If "No Change" is selected, the entry in table 2 remains unchanged.
- **Copy to Table**
  If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Radio**
  Shows the available WLAN interfaces.
- **Port**
  Shows the VAP interface.
- **Within own VAP**
  - Enabled
    Clients logged on to the same VAP interface of an access point can communicate with each other.
  - Disabled

    Option is disabled.
- **With other VAPs**
  - Enabled
    Clients logged on to different VAP interfaces of an access point can communicate with each other.
  - Disabled
    Option is disabled.

  Note

  For an access point, "With other VAP" must be enabled on all WLAN interfaces or on all VAPs to allow communication between clients logged on at different VAP interfaces of the access point.
- **With ethernet**
  - Enabled
    Clients can communicate via the Ethernet interface of the access point.
  - Disabled
    Option is disabled.

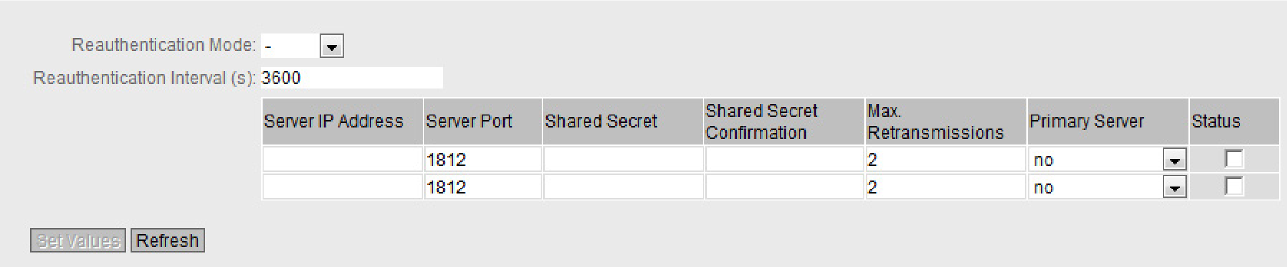
5.9.2.3 AP Radius Authenticator

Configuration of the RADIUS server

On this page, you define the RADIUS servers and the RADIUS authentication of the access point. You can enter data for two RADIUS servers.

Note

This tab is available only in access point mode.



Reauthentication Mode: -

Reauthentication Interval (s): 3600

Server IP Address	Server Port	Shared Secret	Shared Secret Confirmation	Max. Retransmissions	Primary Server	Status
	1812			2	no	□
	1812			2	no	□

Description

The page contains the following boxes:

- **Reauthentication Mode**
  Specify who sets the time after which the clients are forced to reauthenticate.
  – Disabled
    Reauthentication mode is disabled.
  – Server
    Enables time management on the server.
  – Local
    Enables local time management. In "Reauthentication Interval", specify the time of validity.
- **Reauthentication Interval [s]**
  If time management is local, enter the period of validity of the authentication in seconds. The minimum time is 1 minute (enter 60), the maximum time is 12 hours (enter 43200). The default is one hour (3,600 seconds).

The table has the following columns:

- **Server IP Address**
  Here, enter the IP address or the FQDN name of the RADIUS server.
- **Server Port**
  Enter the input port on the RADIUS server.
- **Shared Secret**
  Enter the password of the RADIUS server.
  For the password, ASCII code 0x20 to 0x7e is used.

- **Shared Secret Confirmation**
  Confirm the password.
- **Max. Retransmissions**
  Enter the maximum number of connection attempts.
- **Primary Server**
  Specify whether or not this server is the primary server.
  – yes: Primary server
  – no: Backup server.
- **Status**
  With this check box, you can enable or disable the RADIUS server

Procedure

Entering a new server

To display a new server, follow the steps below:

1. In the relevant row, enter the following data in the input boxes:
   – IP address or FQDN name of the RADIUS server.
   – Port number of the input port
   – Password
   – Confirmation of the password
   – Maximum number of transmission retries
   – Primary server
2. Click the "Set Values" button.

Modifying servers

1. In the relevant row, enter the following data in the input boxes:
   – Server IP address
   – Port number of the input port
   – Password
   – Confirmation of the password
   – 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.

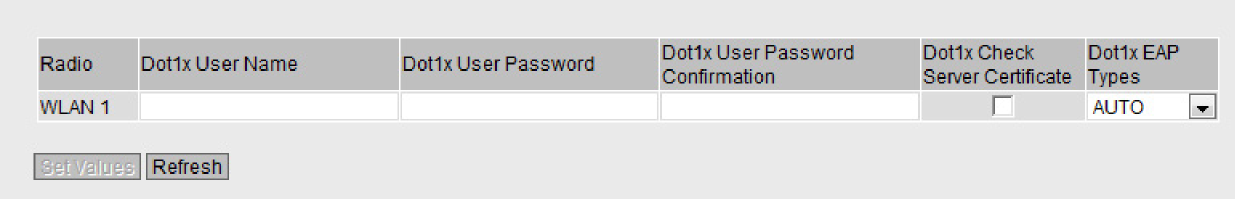
5.9.2.4 Client Radius Supplicant

Client Supplicant

On this page, you configure the settings for the RADIUS authorization of the client.

Note

This tab is only available in the client mode.



Radio	Dot1x User Name	Dot1x User Password	Dot1x User Password Confirmation	Dot1x Check Server Certificate	Dot1x EAP Types
WLAN 1				□	AUTO

Description

The table has the following columns:

- **Radio**
  Shows the WLAN interface.
- **Dot1x Username**
  Enter the user name with which you want to log on to the RADIUS server.
- **Dot1x User Password**
  Here, enter the password for the user name selected above. The client logs on with the RADIUS server using this combination.
  For password assignment, ASCII code 0x20 to 0x7e is used.
- **Dot1x User Password Confirmation**
  Confirm the password.
- **Dot1x Check Server Certificate**
  Specify whether or not the RADIUS server identifies itself to the client using a certificate.
- **Dot1x EAP Types**
  Specify the authentication method. The following methods are available:
  - Auto
    EAP-TLS, EAP-TTLS or PEAP is used depending on the capability of the other station.
  - EAP-TLS
    Client logs on using a certificate.
  - EAP-TTLS
    The client logs on with the RADIUS server using the user name and password
  - PEAP
    The client logs on with the RADIUS server using the user name and password.

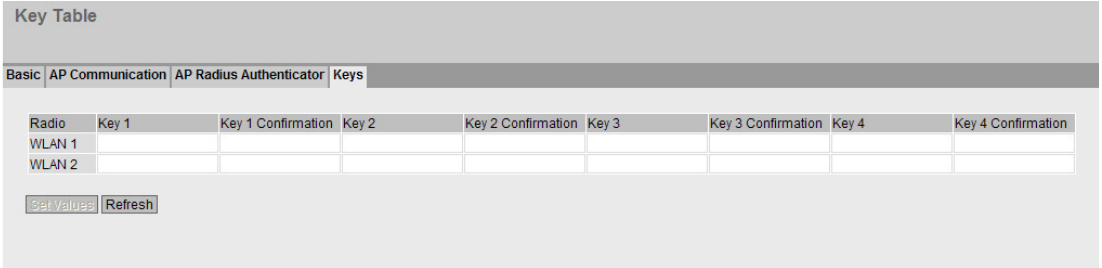
Procedure

1. Enter the necessary values in the input boxes.
2. Select the required entry in the "Dot1x EAP Types" drop-down list.
3. Click the "Set Values" button.

5.9.2.5 Keys

Specifying the WEP key

To allow you to enable the encryption for the "Open System" and "Shared Key" authentication methods, you must first enter at least one key in the key table.



Radio	Key 1	Key 1 Confirmation	Key 2	Key 2 Confirmation	Key 3	Key 3 Confirmation	Key 4	Key 4 Confirmation
WLAN 1								
WLAN 2								

Description

The table has the following columns:

- **Radio**
  Shows the available WLAN interfaces.
- **Key 1 - 4**
  Enter the WEP key or the AES key.
  For the WEP key, characters of the ASCII code from 0x20 to 0x7E or hexadecimal characters from 0x00 to 0xFF are permitted.

  If iPCF or iPCF-MC mode is enabled, only the encryption method AES with 1 28-bit key length is supported.

  You can choose between the following key lengths:

  – 5 or 13 ASCII or 10 or 26 hexadecimal characters (40/104 bits)

  – 16 ASCII or 32 hexadecimal characters (128 bits)

  Note

  The hexadecimal characters are entered without being preceded by "0x". One hexadecimal character codes four bits. The entries "ABCDE" (ASCII characters) and "4142434445" (hexadecimal characters) are therefore the same because the ASCII character "A" has hexadecimal code "0x41".

- **Key 1 - 4 Confirmation**
  Confirm the WEP key.

Procedure

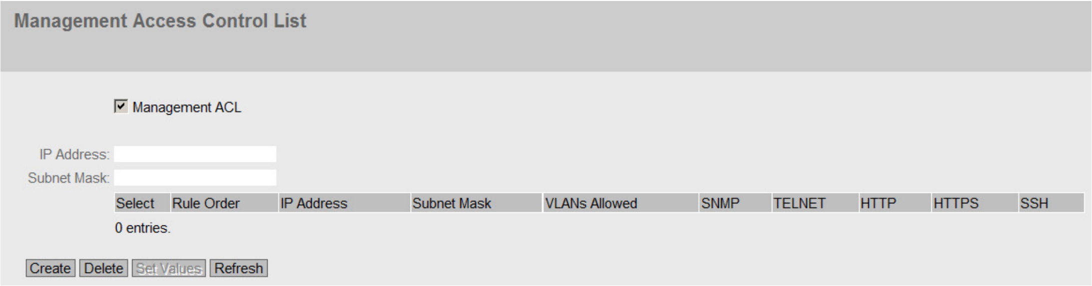
1. Enter at least one WEP key.
2. Click the "Set Values" button.

5.9.3 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

☑ Management ACL

IP Address:

Subnet Mask:

Select	Rule Order	IP Address	Subnet Mask	VLANs Allowed	SNMP	TELNET	HTTP	HTTPS	SSH

0 entries.

Description

The page contains the following boxes:

- **"Management ACL" check box**
  Enable or disable the function.
- **"IP Address" input box**
  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" input box**
  Enter the subnet mask. 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:

- **Select**
  Select the check box in the row to be deleted.
- **Rule Order**
  Shows the number of the rule. If you click the "Create" button, a new row with a unique number is created

- **IP Address**
  Shows the IP address.
- **Subnet Mask**
  Shows the subnet mask.
- **VLANs Allowed**
  Only available if 802.1Q VLAN Bridge is set for "Layer 2 > VLAN > General".
  Enter the number of the VLAN in which the device is located. 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.
- **SNMP**
  Specify whether the station (or the IP address) accesses the device using the SNMP protocol.
- **TELNET**
  Specify whether the station (or the IP address) accesses the device using the TELNET protocol.
- **HTTP**
  Specify whether the station (or the IP address) accesses the device using the HTTP protocol.
- **HTTPS**
  Specify whether the station (or the IP address) accesses the device using the HTTPS protocol.
- **SSH**
  Specify whether the station (or the IP address) accesses the device using the SSH protocol.
- **Px**
  Specify whether the station (or the IP address) accesses the device via this port.
- **WLAN 1** (client mode only)
  Specify whether or not the station or the IP address accesses the device via the WLAN interface.
- **VAP X.Y** (access point mode only)
  Specify whether or not the station or the IP address accesses the device via the VAP interface.
- **WDS X.Y** (access point mode only)
  Specify whether or not the station or the IP address accesses the device via the WDS interface.

Procedure

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 the row to be deleted.
2. Repeat this procedure for every entry you want to delete.
3. Click the "Delete" button. The entries are deleted and the page is updated.

Note

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

You can then only remedy this by resetting the device to the factory defaults and then reconfiguring.

5.9.4 Inter AP blocking

5.9.4.1 Basic

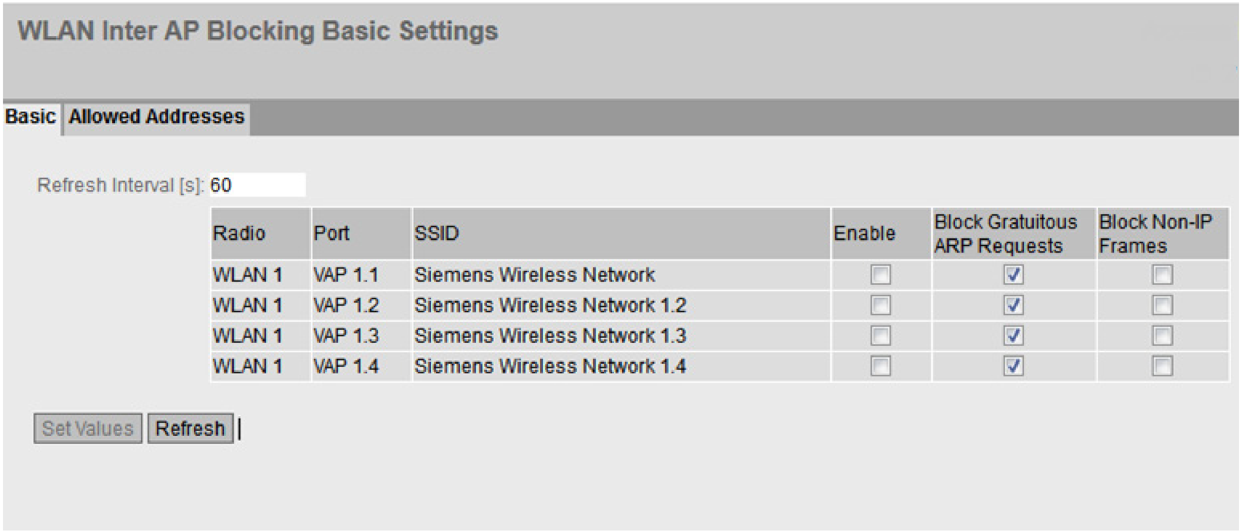
Note

- This tab is available only in access point mode.
- This WBM page can only be configured with the following KEY-PLUGs:
  - W780 iFeatures (MLFB 6GK5 907-8PA00)
  - W700 Security (MLFB 6GK5907-0PA00)

When should Inter AP blocking be used?

The clients connected to an access point can normally communicate with all devices of the layer 2 network.

With inter AP blocking, the communication of the clients connected to the access point can be restricted. Only the devices whose IP addresses are configured in "Allowed Addresses" on the access point are accessible to the clients. Communication with other nodes in the network is therefore prevented.



Refresh Interval [s]: 60

Radio	Port	SSID	Enable	Block Gratuitous ARP Requests	Block Non-IP Frames
WLAN 1	VAP 1.1	Siemens Wireless Network	☐	☑	☐
WLAN 1	VAP 1.2	Siemens Wireless Network 1.2	☐	☑	☐
WLAN 1	VAP 1.3	Siemens Wireless Network 1.3	☐	☑	☐
WLAN 1	VAP 1.4	Siemens Wireless Network 1.4	☐	☑	☐

Description

The page contains the following box:

- **"Refresh interval [s]" input box**
  Enter the refresh interval for the ARP table.

The table has the following columns:

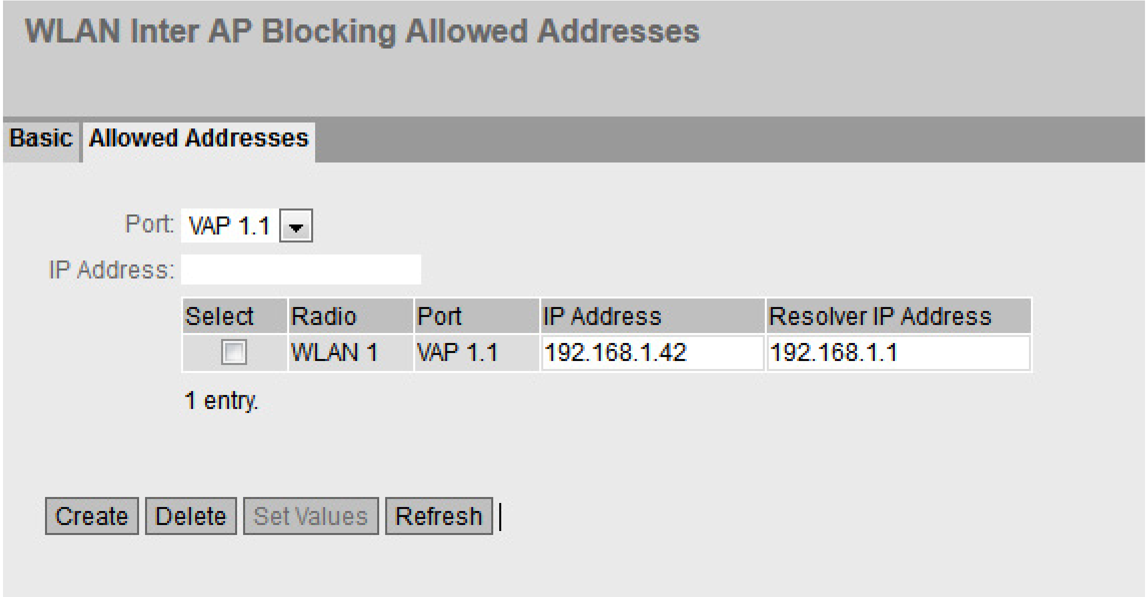
- **Radio**
  Specifies the WLAN interface to which the settings relate.
- **Port**
  Specifies the VAP interface to which the settings relate.
- **SSID**
  Specifies the SSID to which the settings relate.
- **Enable**
  When enabled, the access restriction is used. You configure which devices are accessible to the clients in "Security > Inter AP Blocking > Allowed Adresses".
- **Block Gratuitous ARP Request**
  When enabled, gratuitous ARP packets are not forwarded.
- **Block Non-IP Frames**
  When enabled, there is no exchange of non-IP packets, for example layer 2 packets between the client and the devices configured on the access point as permitted communications partners.

5.9.4.2 Allowed addresses

Note

- This tab is available only in access point mode.
- This WBM page can only be configured with the following KEY-PLUGs:
  - W780 iFeatures (MLFB 6GK5 907-8PA00)
  - W700 Security (MLFB 6GK5907-0PA00)

On this page you specify which devices are accessible to the clients.



WLAN Inter AP Blocking Allowed Addresses

Port: VAP 1.1

IP Address:

Select	Radio	Port	IP Address	Resolver IP Address
□	WLAN 1	VAP 1.1	192.168.1.42	192.168.1.1

1 entry.

Description

The page contains the following boxes:

- **"Port" drop-down list**
  Select the required port from the drop-down list.
- **IP Address" input box**
  Enter the IP address of the devices accessible to the client.

The table has the following columns:

- **Select**
  Select the check box in the row to be deleted
- **Radio**
  Specifies the WLAN interface to which the settings relate
- **Port**
  Specifies the VAP interface to which the settings relate

- **IP Address**
  The IP address of the devices accessible to the client. If necessary, you can change the IP address.
- **Resolver IP Address**
  The IP address with which the permitted IP address is resolved. The entry is necessary when the management IP address is located in a different subnet.
  If the IP address "0.0.0.0" is configured for "Resolve IP Address", the management IP address is used for resolution.

5.10 "iFeatures" menu

5.10.1 iPCF

Note

This WBM page can only be configured with the following KEY-PLUGs:

- Access point: W780 iFeatures (MLFB 6GK5 907-8PA00)
- Client: W740 iFeatures (MLFB 6GK5 907-4PA00)

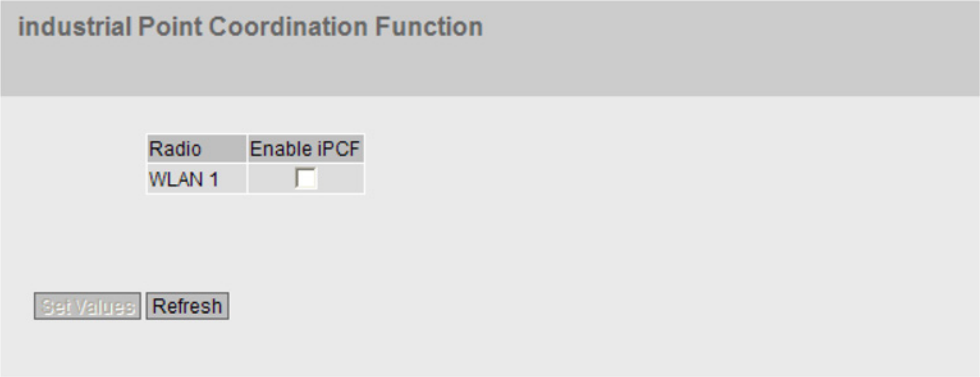
When should iPCF be used?

The use of iPCF is advisable particularly if you have a large number of nodes and want to implement highly deterministic operation. This is necessary, for example with PNIO or other cyclic protocols. You will find a more detailed description of iPCF in the section "Technical basics" in the section "iPCF / iPCF-MC (Page 40)".

Note

- iPCF and iPCF-MC are not compatible with each other and cannot be used at the same time on a device.

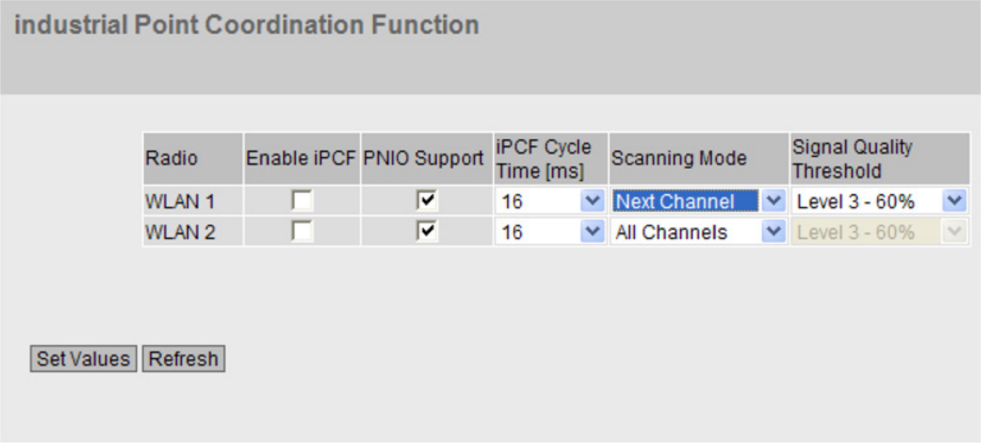
The possible settings differ for access point and client. Below, both will be described.



industrial Point Coordination Function

Radio	Enable iPCF
WLAN 1	□

Darstellung im Client-Modus



industrial Point Coordination Function

Radio	Enable iPCF	PNIO Support	iPCF Cycle Time [ms]	Scanning Mode	Signal Quality Threshold
WLAN 1	□	☑	16	Next Channel	Level 3 - 60%
WLAN 2	□	☑	16	All Channels	Level 3 - 60%

Darstellung im Access Point-Modus

Description

In both modes, the table has the following columns:

- **Radio**
  Specifies the WLAN interface to which the settings relate.
- **Enable iPCF**
  Enable or disable iPCF mode. For PNIO communication, we recommend that you enable the iPCF mode. By enabling iPCF, the data rates provided by the access point are adapted. We strongly recommend that you retain the default setting for the data rates (802.11 a/b/g = 12 Mbps and 802.11n = MCS 2).

In access point mode, the table has the following additional columns:

- PNIO Support
  Enable or disable optimized support of PNIO.
- iPCF Cycle Time [ms]
  Select the required cycle time from the drop-down list.
  The following points need to be taken into account when setting the cycle time. Otherwise it may not be possible to establish stable communication.
  - There is only one access point in the system; in other words, the clients move only in one wireless cell. In this case, update times >= 16 ms are supported.
  - There are several access points in the system that communicate over different channels. The clients roam between the access points. In this case, select update times >= 32 ms.

  In addition to the guide values shown above, remember that the shortest cycle time to be set is calculated according to the formula "2 ms * max. number of nodes".
- Scanning Mode
  The selected setting affects the scanning behavior of the logged-on clients.
  The following settings are available:
  - All Channels
    The client scans all permitted channels and selects the access point with the best signal strength and connects to it.
  - Next Channel
    The client scans the next channel from its permitted channel list. If an access point is there, it connects to it. If it does not find an access point on this channel, it scans the next channel.
- Signal Quality Threshold
  Can only be configured if "Scanning Mode" "Next Channel" is enabled. The client is given a minimum signal strength with which the access point must be seen during the scan so that a connection can be established to it.
  The following threshold values exist for the signal strength:

Level	Signal quality in RSSI	Signal quality in %
1	20	40
2	25	50
3	30	60
4	35	70
5	40	80

Procedure

In access point mode

1. Select the "Enable iPCF" option for the required WLAN interface.
2. Select the required cycle time for the access point from the "iPCF Cylce Time [ms]" drop-down list.
3. Select for example "All Channels" from the "Scanning Mode"drop-down list.

In client mode

1. Select the "Enable iPCF" option for the required WLAN interface.
2. Click the "Set Values" button.

You configure the security settings in "Security > WLAN > Basic".

5.10.2 iPCF-MC

Requirements to be able to use iPCF-MC:

- The access point has at least two WLAN interfaces (dual AP).
- Access point mode: Only dual APs with KEY-PLUG W780 iFeatures (MLFB 6GK5 907-8PA00)
- Client mode: Client with KEY-PLUG W740 iFeatures (MLFB 6GK5 907-4PA00)
- The management interface and data interface must be operated in the same frequency band and mode and must match in terms of their wireless coverage. iPCF-MC will not work if both wireless interfaces are equipped with directional antennas that cover different areas.
- The management interfaces of all access points to which a client can change must use the same channel. A client scans only this one channel to find accessible access points.
- Transmission based on IEEE801.11h (DFS) cannot be used for the management interface. 801.11h (DFS) is possible for the data interface.
- The client cannot be operated with "Use Allowed Channel only".
- "Force roaming on Ethernet down" is automatically mirrored on the second interface.

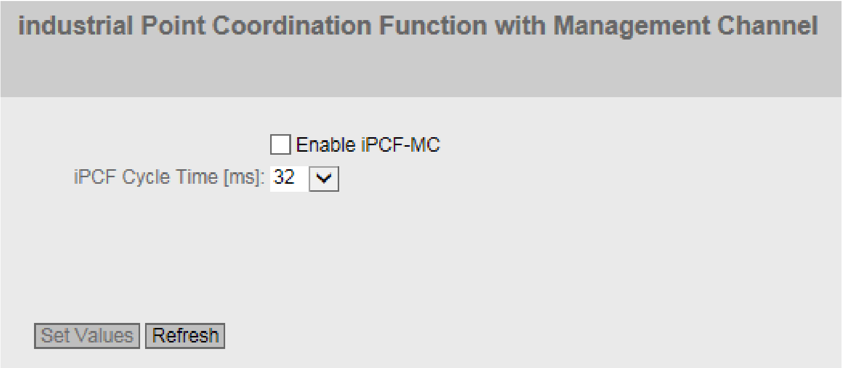
When should iPCF-MC be used?

iPCF was developed to achieve short handover times when roaming between cells. The iPCF-MC technique allows short handover times even for freely mobile clients and when a lot of cells are involved or a large number of channels is being used.

Note

- iPCF and iPCF-MC are not compatible with each other and cannot be used at the same time on a device.
- With 11n devices, remember that the assignment of the WLAN interfaces is fixed for iPCF-MC.
  - WLAN1: Data interface
  - WLAN2: Management interface

In access point mode

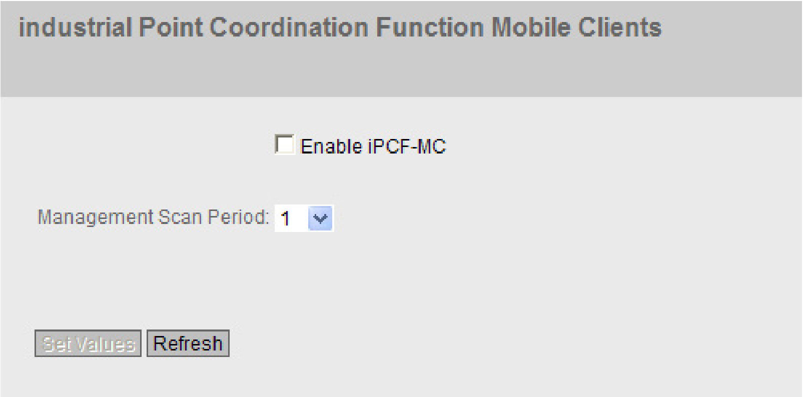


industrial Point Coordination Function with Management Channel

□ Enable iPCF-MC

iPCF Cycle Time [ms]: 32

In client mode



industrial Point Coordination Function Mobile Clients

□ Enable iPCF-MC

Management Scan Period: 1

Description

The page contains the following boxes:

- **"Enable iPCF-MC" check box**
  Enable or disable the iPCF-MC mode of the device.
  For PNIO communication, we recommend enabling the iPCF-MC mode. By enabling iPCF-MC, the data rates provided by the access point are adapted.
  We strongly recommend that you retain the default setting for the data rates (802.11 a/b/g = 6, 9 and 12 Mbps and 802.11n = MCS 2).
- **"iPCF Cycle Time" drop-down list** (only in access point mode)
  Select the PNIO update time configured for the network to which the access point is connected. The lowest value for the update time is 32 ms.
- **"Management Scan Period" drop-down list** (only in client mode)
  This parameter specifies the time between two client management channel scans (specified in iPCF cycles). If, for example, you select two, the client runs a management channel scan only in every second iPCF cycle.
  A lower value for the scan interval provides the basis for fast roaming, however this means that no high data throughput can be achieved. A higher value should be selected for a high data throughput.

5.10.3 iREF

Note

- This tab is available only in access point mode.
- This WBM page can only be configured with the following KEY-PLUG:
  - Access point: W780 iFeatures (MLFB 6GK5 907-8PA00)

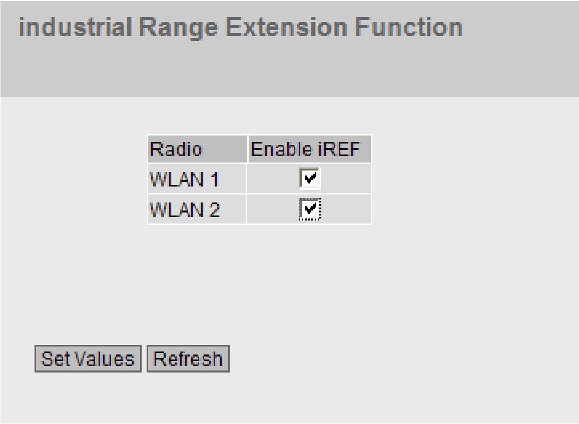
When should iREF be used?

With iREF, the data can be sent with the highest possible transmit power. This applies in particular to use cases in which MIMO cannot be used, is of no advantage or when using sector antennas.

Note

Use of iREF with other iFeatures

iREF and other iFeatures (e.g. iPCF, iPCF-MC) are not compatible with each other and cannot be used at the same time on a device.



industrial Range Extension Function

Radio	Enable iREF
WLAN 1	☑
WLAN 2	☑

Description

The table has the following columns:

- **Radio**
  Specifies the WLAN interface to which the settings relate.
- **Enable iREF**
  Enable or disable iREF for the required WLAN interface. The result is shown in "Information > WLAN >iFeatures".

Note

To be able to use iREF, there must be at least two antennas.

The antennas are automatically switched to Mode RX/TX as soon as iREF is enabled.

5.10.4 AeroScout

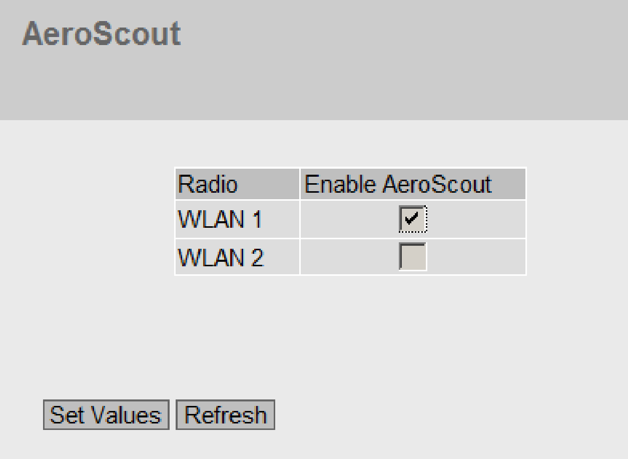
Note

- This tab is available only in access point mode.
- This WBM page can only be configured with the following KEY-PLUG:
  Access point: W780 iFeatures (MLFB 6GK5 907-8PA00)

Note

The AeroScout function cannot be combined with other iFeatures (iPCF, iPCF-MC, iREF). AeroScout can only be used in the 2.4 GHz band according to IEEE 802.11g, IEEE 802.11n and IEEE 802.11n-only.

For more detailed information, please refer to the documentation of the AeroScout company (www.aeroscout.com).



AeroScout

Radio	Enable AeroScout
WLAN 1	☑
WLAN 2	☐

Description

The table has the following columns:

- **Radio**
  Specifies the WLAN interface to which the settings relate.
- **Enable AeroScout**

  Enable or disable AeroScout for the required WLAN interface. The result is shown in "Information > WLAN iFeatures" AeroScout.

Upkeep and maintenance 6

6.1 Firmware update - via WBM

Requirement

- The device has an IP address.
- The "admin" user is logged on.

Firmware update via HTTP

1. Click "System > Load&Save" in the navigation area. Click the "HTTP" tab.
2. Click the "Load" button in the "Firmware" table row.
3. Go to the storage location of the firmware file.
4. Click the "Open" button in the dialog. The file is uploaded.

Firmware update - via TFTP

1. Click "System > Load&Save" in the navigation area. Click the "TFTP" tab.
2. Enter the IP address of the TFTP server in the "TFTP Server IP Address" input box.
3. Enter the port of the TFTP server in the "TFTP Server Port" input box
4. Click the "Load file" button in the "Firmware" table row.
5. Go to the storage location of the firmware file.
6. Click the "Open" button in the dialog. The file is uploaded.

Result

The firmware is has been transferred completely to the device and under ""Information > Versions" there is also the entry "FirmwareRunning". FirmwareRunningshows the version of the current firmware. Firmware shows the firmware version stored after loading the firmware. To activate this firmware, restart the device with "System > Restart".

6.2 Restoring the default parameter settings

Procedure

Follow the steps below to reset the device parameters to the factory settings:

Note

When you reset the device parameters, all previously changed settings are lost!

1. Turn off the power to the device.
2. Now press the Reset button and reconnect the power to the device while holding down the button.
3. Hold down the button until the red fault LED (F) stops flashing after approximately 10 seconds and is permanently lit.
4. Now release the button and wait until the fault LED (F) goes off again.
5. The device then starts automatically with the default parameters.

Troubleshooting/FAQ 7

7.1 Firmware update via WBM or CLI not possible

Cause

If there is a power failure during the firmware update, it is possible that the device is no longer accessible using Web Based Management or the CLI.

Solution

You can then also assign firmware to a SCALANCE W700 using TFTP.
Follow the steps below to load new firmware using TFTP:

1. Turn off the power to the device.
2. Now press the Reset button and reconnect the power to the device while holding down the button.
3. Hold down the button until the red fault LED (F) starts to flash after approximately 2 seconds.
4. Now release the button. The bootloader waits in this state for a new firmware file that you can download by TFTP.
5. Connect a PC to the SCALANCE W700 over the Ethernet interface.
6. Assign an IP address to the SCALANCE W700 with the Primary Setup Tool.
7. Open a DOS box and change to the directory where the file with the new firmware is located and then execute the command "tftp -i <ip address> PUT <firmware>". As an alternative, you can use a different TFTP client.

Note

Use of CLI and TFTP in Windows 7

If you want to access the CLI or TFTP in Windows 7, make sure that the relevant functions are enabled in Windows 7.

Result

The firmware is transferred to the device.

Note

Please note that the transfer of the firmware can take several minutes. During the transmission, the red error LED (F) flashes.

Once the firmware has been transferred completely to the device, the device is restarted automatically.

7.2 Disrupted data transmission due to the received power being too high

Causes and effects of excessive received power

If the received power at the input of a WLAN is too high, this overdrives the amplifier circuit. Overdrive can occur on clients and access points. If the receive power on the device is greater than -40 dBm, this can result in disrupted communication.
Information about the signal strength [in dBm] is displayed in WBM on the following tabs:
Information > WLAN > Client List
Client mode: Information > WLAN > Client List > Available AP list
The power of the input signal on the IWLAN device is influenced by the following factors:

- Distance between the WLAN partners
- Reflections of the electromagnetic waves by parts of the building
- Setting for the "Max. TX Power" (Interfaces > WLAN > Basic) and the antenna settings used (Interfaces > WLAN > Antennas).

Solution

If communication is disrupted by an excessive signal strength (greater than -40 dBm), you can eliminate the problem in the following ways:

- Increase the distance between the transmitter and receiver.
- Reduce the transmit power of the IWLAN partner with suitable settings in WBM or CLI.

7.3 Compatibility with predecessor products

Mixed mode

Mixed operation with predecessor products (6GK57xx-xAA60-xAx0) is possible.

Further information about predecessor products can be found on the Internet at Siemens Industry Automation and Drives Service & Support, entry ID: 42784493 (http://support.automation.siemens.com/WW/view/en/42784493)

Note the following points if you want to make mixed operation possible:

- Transmission standard IEEE 802.11a/b/g/n
  The transmission standards IEEE 802.11a/b/g/n are compatible with the predecessor products. The setting "802.11n only" is not compatible with the predecessor products. The transmission standards IEEE 802.11a/g/h Turbo of the predecessor products are not supported.
- Security settings
  The transmission standards IEEE 802.11a/b/g support the same security settings as the predecessor products.
  The transmission standard IEEE 802.11n with the setting "802.11n" or "802.11n only" only supports WPA2/ WPA2-PSK with AES in the security settings.
- SSID
  For SSID, use only the characters that were supported by the previous products.
- Management only over wired Ethernet interface
  In the previous products, there was a function "Management only over wired Ethernet interface". In the new devices this function is covered by the "Management ACL (Page 275)" function.
- iPCF
  The SCALANCE W700-xRR devices support data rates up to 11 Mbps in the IEEE 802.11b mode. For this reason, they cannot receive beacons sent by an access point at 12 Mbps (default setting for IEEE 802.11a/b/g). If you use the listed devices as clients, you will need to set the data rate of the access point to 11 Mbps.
- WDS ID
  With WDS ID, do not use the ASCII character 0x22 (").
- Key for WEP or AES
  With devices with firmware up to version 3.2, the keys for WEP or AES may only contain ASCII characters or hexadecimal characters from 0x20 to 0x7E.

7.4 Instructions for secure network design

Note the following information about protecting your network from attacks:

- **Use a secure connection with HTTPS**

  In contrast to HTTP, HTTPS allows you secure access for configuring the WLAN clients and the access points using Web Based Management. For more detailed information, refer to the section "Load&Save (Page 148)".

- **Use WPA2/ WPA2-PSK with A**ES

  Use only WPA2/AES to prevent password misuse. WPA2/ WPA2-PSK with AES provides the greatest security. For more detailed information, refer to the section "Basic (Page 265)".

- **Protect your network from man-in-the-middle attacks**

  To protect your network from man-in-the-middle attacks, a network setup is recommended that makes it more difficult for the attacker to access the communications path between two end devices.

  – You can, for example, protect WLAN devices by arranging so that the Agent IP is only accessible via a single management VLAN. For more detailed information, refer to the section "Agent IP (Page 142)".

  – A further option is to install a separate HTTPS certificate on the WLAN client / access point. The HTTPS certificate checks the identity of the device and controls the encrypted data exchange. You can install the HTTPS certificate, for example using HTTP. For more detailed information, refer to the section "HTTP (Page 150)".

- **Use SNMPv3**

  SNMPv3 provides you with highest possible security when accessing the WLAN devices via SNMP. For more detailed information, refer to the section "SNMP (Page 169)".

NOTICE
Changing the default password after configuring with STEP 7
If a device in the default status is configured only with STEP 7, it is not possible to change the default password. This change must be made directly on the device using WBM or CLI. Otherwise the default password is retained and any user could log in using the default password.

Appendix A

A

A.1 MIB files supported by SCALANCE W700

MIB files available for the SCALANCE W700

The following table shows the MIB files available for a SCALANCE W700:

MIB	Root OID	Reference
AUTOMATION SNTP (Siemens) 1) 2)	.1.3.6.1.4.1.4329.6.3.11	Vendor specific
AUTOMATION SYSTEM MIB (Siemens) 1) 2)	.1.3.6.1.4.1.4329.6.3.2	Vendor specific
AUTOMATION TELNET (Siemens) 1) 2)	.1.3.6.1.4.1.4329.6.3.8	Vendor specific
AUTOMATION TIME MIB (Siemens) 1) 2)	.1.3.6.1.4.1.4329.6.3.3	Vendor specific
BRIDGE MIB	.1.3.6.1.2.1.17	RFC1493
ENTITY-MIB	.1.3.6.1.2.1.47	
EtherLike-MIB	.1.3.6.1.2.1.10.7.2	
IANA-MAU-MIB	.1.3.6.1.2.1.26.1.1	
IEEE8021-PAE-MIB	.1.0.8802.1.1.1	IEEE 802.1X
IEEE802dot11-MIB	.1.2.840.10036	IEEE 802.11
IF-MIB:	.1.3.6.1.2.1.2	RFC2233
P-BRIDGE-MIB	.1.3.6.1.2.1.17.4.5	
Q-BRIDGE-MIB	.1.3.6.1.2.1.17.7	
RADIUS-ACC-CLIENT-MIB	.1.3.6.1.2.1.67.2.2	
RADIUS-AUTH-CLIENT-MIB	.1.3.6.1.2.1.67.1.2	
RFC1213-MIB	.1.3.6.1.2.1.4	
RMON-MIB	.1.3.6.1.2.1.16	
SNMP-COMMUNITY-MIB	.1.3.6.1.6.3.18	
SNMP-FRAMEWORK-MIB	.1.3.6.1.6.3.10.2.1	RFC2571
SNMP NOTIFICATION MIB	.1.3.6.1.6.3.13	RFC2573
SNMP PROXY MIB	.1.3.6.1.6.3.14	
SNMP-TARGET-MIB	.1.3.6.1.6.3.12	RFC2573
SNMP USER-BASED SM MIB	.1.3.6.1.6.3.15	RFC2574
SNMPv2-MIB	.1.3.6.1.2.1.1	RFC1907
SNMP VIEW-BASED ACM MIB	.1.3.6.1.6.3.16	RFC2575
SN-MSPS-ACL-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.30	Vendor specific
SN-MSPS-CONFIG-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.1	Vendor specific
SN-MSPS-CPLUG-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.23	Vendor specific
SN-MSPS-DHCP-CLIENT-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.17.1	Vendor specific
SN-MSPS-DIGITAL-IO-MIB (Siemens) 2)3)	.1.3.6.1.4.1.4329.20.1.1.1.1.39	Vendor specific
SN-MSPS-GENERAL-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.2	Vendor specific

MIB	Root OID	Reference
SN-MSPS-HTTP-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.20	Vendor specific
SN-MSPS-IF-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.34	Vendor specific
SN-MSPS-IP-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.13	Vendor specific
SN-MSPS-KEY-PLUG-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.35	Vendor specific
SN-MSPS-LOAD-SAVE-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.26	Vendor specific
SN-MSPS-LOG-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.31	Vendor specific
SN-MSPS-MSTP-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.6	Vendor specific
SN-MSPS-NTP-MIB (Siemens)	.1.3.6.1.4.1.4329.20.1.1.1.1.33	Vendor specific
SN-MSPS-PNAC-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.10	Vendor specific
SN-MSPS-PORT-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.29	Vendor specific
SN-MSPS-RADIUS-SERVER-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.11.2	Vendor specific
SN-MSPS-REPORT-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.28	Vendor specific
SN-MSPS-RMON-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.12	Vendor specific
SN-MSPS-SINEMA-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.25	Vendor specific
SN-MSPS-SNMP-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.4	Vendor specific
SN-MSPS-SNTP-CLIENT-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.19.1	Vendor specific
SN-MSPS-STP-L2T-MIB (Siemens)	.1.3.6.1.4.1.4329.20.1.1.1.1.40	Vendor specific
SN-MSPS-SYSLOG-CLIENT-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.21.1	Vendor specific
SN-MSPS-VLAN-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.3	Vendor specific
SN-MSPS-WLAN-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.27	Vendor specific
SN-MSPS-NAT-MIB	1.3.6.1.4.1.4329.20.1.1.1.1.45	Vendor specific
TCP-MIB	.1.3.6.1.2.1.6	
UDP-MIB	.1.3.6.1.2.1.7	

1) Part of the AUTOMATION.MIB

You can download the AUTOMATION.MIB for SCALANCE W700 from Siemens Industry Automation and Drives Service & Support under the following entry ID 67637278 (http://support.automation.siemens.com/WW/view/en/67637278?Datakey=37421371)

2) Part of the private MIB file "Scalance_w_msps.mib". The file can be downloaded in WBM using "System > Load&Save > HTTP > MIB" and the "Save" button.

3) This MIB is not supported on devices without a digital input/output.

Appendix B

B

B.1 Private MIB variables of the SCALANCE W700

Downloading the MIB of the SCALANCE W700 via WBM

The MIB of the SCALANCE W700 can be downloaded in WBM using "System > Load&Save > HTTP > MIB" and the "Save" button.

OID

The private MIB variables of the SCALANCE W700 have the following object identifiers:

```
iso(1).org(3).dod(6).internet(1).private(4). enterprises(1)
siemens(4329) industrialComProducts(20) iComPlatforms(1)
simaticNet(1) snMsps(1) snMspsCommon(1)
```

WLAN-specific MIB variables

The WLAN-specific MIB variables can be found in "snMspsWlan". You will find further information about the settings and values in the MIB file.

Appendix C

C.1 Underlying standards

Standards met by SCALANCE W700 devices completely or partly

The following table lists some of the standards for SCALANCE W700 devices.

Name of the standard	Topic
IEEE 802.1AB	Link Layer Discovery Protocol (LLDP)
IEEE 802.1D-1998	Media Access Control (MAC), bridges
IEEE 802.1Q	Virtual Bridged LANs (VLAN Tagging, Port Based VLANs)
IEEE 802.1W-2004	Rapid Spanning Tree Protocol (RSTP)
IEEE 802.1X	Port Based Network Access Control
IEEE 802.3-2002	Ethernet
IEEE 802.3af	Power over Ethernet (PoE)
IEEE 802.11	Wireless Local Area Network
IEEE 802.11a	Wireless standard for use of the 5 GHz frequency band
IEEE 802.11at	PoE +
IEEE 802.11b/g	Wireless standard for use of the 2.4 GHz frequency band
IEEE 802.11e	Quality of Service (QoS)
IEEE 802.11 h	Expansion of the spectrum and transmit power for use of the 5 GHz frequency range in Europe.
IEEE 802.11i	Encryption of WLANS
IEEE 802.11n	Standard for high transmission rates

Appendix D

D

D.1 Messages in the event log

Messages during system startup (general)

Alarm	Description
Warm start performed, Ver: V02.00.00 - event/status summary after startup	Type of startup and the loaded firmware version.
Power supply: • L1 is connected • L2 is not connected	Status of the power supplies line 1 and line 2.
No line is monitored	Information about monitoring the power supply from the signaling system.
MSTP disabled MSTP enabled	Information on the status of the Spanning Tree protocol.
No Fault states pending after startup	Fault state following system start.

Status of the power supply

Alarm	Description
	You enable or disable the "Power Change" event in "System > Events".
Power up on line 1 / 2 / PoE.	Power supply exists on line 1, line 2 or PoE..
Power down on line 1 / 2 / PoE.	Power supply interrupted on line 1, line 2 or PoE.

Status of the Ethernet interface

Alarm	Description
	You enable or disable the "Link Change" event in "System > Events".
Link up on P1.	A connection exists on the Ethernet interface.
Link down on P1.	No connection exists on the Ethernet interface.

Status of the WLAN interface (in access point mode only)

Messages	
Link down up VAP X.Y.	The VAP interface Y on the WLAN interface X is enabled.
Link down on VAP X.Y.	The VAP interface Y on the WLAN interface X is disabled.
WDS Y at WLAN X is up.	A link exists on the WDS interface Y of WLAN interface X.

Messages	
WDS Y at WLAN X is down.	No link exists on the WDS interface Y of WLAN interface X.
Overlap-AP found on WLAN X: AP <system name> <MAC> found on channel <channel number.> <RSSI value>	A further access point was detected on the channel set for the WLAN interface X or on a neighboring channel.
Overlap-AP aged out on WLAN X: AP <system name> <MAC> on channel <channel number.> <RSSI value>	The overlapping access point could not be detected during the configured aging time and was removed from the "Overlap AP" list.
DFS: Radar interference detected on WLAN X at channel <channel number> (frequency <frequency> MHz). Changing to channel <channel number> (frequency <frequency> MHz)	A primary user (e.g. radar or weather station) was detected on the channel set for WLAN interface X or on a neighboring channel. The channel will be blocked for 30 min. The access point changes to the configured alternative channel or to the next free channel on which there is no primary user.
DFS: channel <channel number> (frequency <frequency> MHz) aged out from NOL at WLAN X and can be used again.	No primary user detected on the channel any longer. The channel was removed from the list of blocked channels and can be used again
DFS: Radar interference detected on WLAN X at channel <channel number> (frequency <frequency> MHz). No more free channels to use!!	A primary user was found on all available channels. There is no free channel available, the WLAN interface X will be deactivated until one of the channels becomes available.

Status of the WLAN interface (in client mode only)

Messages	Description
Link up on WLAN X.	The WLAN interface X is enabled.
Link down on WLAN X.	The WLAN interface X is disabled.

Messages on configuration

Messages	Description
WBM: Authentication failure.	When logging in with Web Based Management (WBM), the wrong password was entered. The event can be enabled or disabled in "System -> Events" (authentication failure).
Telnet: Authentication failure.	When logging in via Telnet, the wrong password was entered. The event can be enabled or disabled in "System -> Events" (authentication failure).
Restart requested	Restart due to a user request. The event can be enabled or disabled in "System -> Events" (cold/warm start).

Messages about file upload or download

Messages	Description
File upload via HTTP(S): load of FileType <file type> OK -> restart required	Loading the file via HTTP(S) was successful. A restart is required.
File upload via HTTP(S): load of FileType<file type> OK	Loading the file via HTTP(S) was successful.
File upload via HTTP(S): validation of FileType <file type> IDENTICAL	Loading the file via HTTP(S) was successful. The file is identical to the existing file.
File upload via HTTP(S): validation of FileType <file type> FAILED	Loading the file via HTTP(S) failed. The file contains errors or is invalid.

Messages	Description
File upload via TFTP: load of FileType <file type> OK -> restart required	Loading the file using TFTP was successful. A restart is required.
File upload via TFTP: load of FileType <file type> OK	Loading the file using TFTP was successful.
File upload via TFTP: validation of FileType <file type> IDENTICAL	Loading the file using TFTP was successful. The file is identical to the existing file.
File upload via TFTP: validation of FileType <file type> FAILED	Loading the file using TFTP failed. The file contains errors or is invalid.
File upload via TFTP: file transfer of FileType <file type> FAILED	Loading the file using TFTP failed. The file name is incorrect or the file does not exist on the server.
File upload via TFTP: file transfer of FileType <file type> failed. Cannot connect to given IP address	Loading the file using TFTP failed. The TFTP server cannot be reached or the settings are incorrect.
File download via TFTP: file transfer of FileType <file type> failed. Cannot connect to given IP address	Saving the file using TFTP failed. The TFTP server cannot be reached or the settings are incorrect.

Messages error status

Messages	Description
	You configure the events in "System > Events". You configure the monitoring of the power supply and the link on the Ethernet port in "System > Fault Monitoring".
New fault state: <fault description> <fault description>:"Warm start performed." "Cold start performed." "Link down on P1." "Link up on P1." "Power down on line L1 (L2)" "DFS: No channels are available at WLAN2"	Incoming fault. Not all events automatically lead to a fault. On the "Events" WBM page, you specify which events will be logged, for example device restart, changed link on the Ethernet port.
Fault state gone: <fault description> <fault description>:"Warm start performed." "Cold start performed." "Link down on P1." "Link up on P1." "Power down on line L1 (L2)" "DFS: No channels are available at WLAN2" "C-PLUG not accepted. See System C-PLUG mask for details."	Outgoing fault
New Fault state (reconfiguration): <fault description> <fault description>:"Link down on P1." "Link up on P1." "Power down on line L1 (L2)"	Incoming fault. The event was triggered due to a change in the configuration.
Fault state gone (reconfiguration): <fault description> <fault description>:"Link down on P1." "Link up on P1." "Power down on line L1 (L2)".	Outgoing fault. The event was triggered due to a change in the configuration.
Fault state: <fault description> cleared. <fault description>:"Warm start performed" "Cold start performed".	Fault was acknowledged by the user.

Messages about MSTP

Messages	Description
	You enable or disable the "Spanning Tree" event in "System > Events"
Spanning Tree: topology change detected.	The topology of the network has changed; the network will be reorganized.
Spanning Tree: new root bridge xx:xx:xx:xx:xx:xx detected.	The topology of the network has changed; there is a new root bridge with MAC address xx:xx:xx:xx:xx:xx in the network.

Messages about security

Messages	Description
RADIUS: Access accepted / rejected for client <MAC>.	The authentication of the client was successful or not successful.

Messages about message system

Messages	Description
Syslog-Server not reachable!	The configured Syslog server is not accessible.
Unable to send messages to syslog server. Please check syslog socket configuration.	The syslog server configuration is incomplete.
Unable to send e-mail(s) because of IP connection failure.	Sending of e-mail(s) failed. SMTP server cannot be reached (e.g. network connection interrupted).
Unable to send e-mail(s) because of SMTP authentication failure.	Sending of e-mail(s) failed. Authentication of the client on the SMTP server incorrect.
Unable to send e-mail(s) because SMTP message transfer failed.	Sending of e-mail(s) failed. SMTP server can be reached, configuration incomplete or contains errors (e.g. receiver e-mail address wrong / does not exist).
SNMP: Authentification failure.	Authentication of an SNMP client failed; access not possible (e.g. SNMPv1/v2 read-only configured or Read Community String incorrectly configured).
IP communication is possible. Remote logging activated.	IP communication is possible. Remote logging is activated.
IP communication is not possible. Remote logging deactivated. Please check IP configuration and network connectivity.	IP communication is not possible. Remote logging is deactivated. Check whether or not the device has an IP address.

Messages during system startup (PLUG)

Alarm	Description
Startup configuration: Internal storage PLUG: Not present	There is no PLUG inserted.
Startup configuration: Internal storage PLUG: Missing PLUG: License missing	There is no PLUG inserted. There are functions configured on the device for which a license (KEY-PLUG) is required.

Alarm	Description
Startup configuration: Internal storage PLUG: Configuration not accepted PLUG: License missing	Invalid or incompatible configuration on the inserted PLUG. There are functions configured on the device for which a license (KEY-PLUG) is required.
Startup configuration: Internal storage PLUG: Factory clean -> filled with internal configuration PLUG: Configuration accepted PLUG: License accepted	The internal configuration was written successfully to an empty KEY-PLUG.
Startup configuration: Internal storage PLUG: Factory clean -> filled with internal configuration PLUG: Configuration accepted	The internal configuration was written successfully to an empty C-PLUG.
Startup configuration: PLUG storage PLUG: Configuration accepted PLUG: License accepted	The configuration was loaded successfully from the KEY-PLUG.
Startup configuration: PLUG storage PLUG: Configuration accepted	The configuration was loaded successfully from the C-PLUG.

Messages about PLUG

Messages	Description
An empty PLUG was found.	There is an empty or formatted PLUG in the device.
PLUG: Filled PLUG was found. PLUG: Configuration Accepted	There is a valid PLUG with a valid configuration in the device.
PLUG: Removed at runtime.	The C-PLUG / KEY-PLUG was removed during operation.
PLUG accepted.	PLUG was accepted.

Messages about digital input/output

Messages	Description
Digital output is open / closed.	The digital output is open or closed (device dependent).
Value of digital input is 0 / 1.	A low or a high signal is applied to the digital input.

D.2 Messages in the WLAN authentication log

Messages in access point mode

Alarm	Description
Client <MAC address> <system name> associated successfully.	The client has logged in successfully on the access point.
Client <MAC address> <system name> disassociated with reason <reason description>	The client was logged off from the access point.

Messages in client mode

Alarm	Description
Associated successfully to AP <MAC address> <system name> at channel <channel number> (frequency <frequency> MHz)	The client has logged in successfully on the access point.
Disassociated from AP <MAC address> <'sys name'> with reason (Disassociated because sending STA is leaving (or has left) BSS)	The client was logged off from the access point.

Index