SIEMENS

SIMATIC NET

Industrial Wireless LAN SCALANCE W700 according to IEEE 802.11ax Web Based Management V2.2

Configuration Manual

08/2023
C79000-G8976-C618-06

Legal information

Warning notice system

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

⚠ DANGER

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

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

⚠ WARNING

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

Trademarks

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

Disclaimer of Liability

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

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

Document order number: C79000-G8900-C618
Ⓟ 08/2023 Subject to change

Table of contents

Introduction 1

1.1 Purpose of the configuration manual

This Configuration Manual is intended to provide you with the information you require to commission and operate the device. It is aimed primarily at planning, commissioning and maintenance personnel and at security officers. It provides you with the information you require to configure the devices.

The operating instructions of the device describe how you install and connect up the device correctly.

1.2 Scope of validity

This Configuration Manual covers the following products:

Product	Article number	Certification ID
Access points		
SCALANCE WAM766-1	6GK5766-1GE00-7DA0 6GK5766-1GE00-7DB0 (US) 6GK5766-1GE00-7DC0 (ME)	MSAX65-W1-M12-E2
SCALANCE WAM766-1 EEC	6GK5766-1GE00-7TA0 6GK5766-1GE00-7TB0 (US) 6GK5766-1GE00-7TC0 (ME)	MSAX65-W1-M12-E2
SCALANCE WAM763-1	6GK5763-1AL00-7DA0 (DI/DO) 6GK5763-1AL00-7DB0 (US) (DI/DO) 6GK5763-1AL00-7DC0 (ME) (DI/DO)	MSAX-W1-RJ-E2
SCALANCE WAB762-1	6GK5762-1AJ00-6AA0	ELAX-W1-RJ-E2
Client		
SCALANCE WUM766-1	6GK5766-1GE00-3DA0 6GK5766-1GE00-3DB0 (US) 6GK5766-1GE00-3DC0 (ME)	MSAX65-W1-M12-E2
SCALANCE WUM763-1	6GK5763-1AL00-3AA0 6GK5763-1AL00-3AB0 (US)	MSAX-W1-RJ-E2-NO
	6GK5763-1AL00-3DA0 (DI/DO) 6GK5763-1AL00-3DB0 (US) (DI/DO)	MSAX-W1-RJ-E2
SCALANCE WUB762-1	6GK5762-1AJ00-1AA0	ELAX-W1-RJ-E2
SCALANCE WUB762-1 iFeatures	6GK5762-1AJ00-2AA0	ELAX-W1-RJ-E2

The configuration manual applies to the following firmware version:

- SCALANCE W700 IEEE 802.11ax firmware as of version V2.2

1.3 Supplementary documentation

Documentation on the Internet

You can find the current version of the document on the Internet at (https://support.industry.siemens.com/cs/de/en/ps/28575/man)

Enter the name or article number of the product in the search filter.

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 W700 according to IEEE 802.11ax Command Line Interface
  This document contains the CLI commands supported by SCALANCE W700ax devices.
- Operating Instructions SCALANCE WxM766-1
  This document contains information on installing, connecting, maintaining and servicing the following products:
  - SCALANCE WAM766-1
  - SCALANCE WAM766-1 EEC
  - SCALANCE WUM766-1
- Operating Instructions SCALANCE WxM763-1
  This document contains information on installing, connecting, maintaining and servicing the following products:
  - SCALANCE WAM763-1
  - SCALANCE WUM763-1
- Operating Instructions SCALANCE WxM763-1
  This document contains information on installing, connecting, maintaining and servicing the following products:
  - SCALANCE WAB762-1
  - SCALANCE WUB762-1
  - SCALANCE WUB762-1 iFeatures
- SCALANCE W700 802.11ax approvals
  This document contains information on currently available country approvals.
- Performance data SCALANCE W700 802.11ax
  This document contains information about the frequency, modulation, transmit power and receiver sensitivity of the wireless card.

1.4 Further documentation

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

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

You will find the system manuals here:

- On the Internet pages of Siemens Industry Online Support under the following entry IDs:
  - 27069465 (https://support.industry.siemens.com/cs/de/en/view/27069465)
    Industrial Ethernet / PROFINET Industrial Ethernet System Manual
  - 84922825 (https://support.industry.siemens.com/cs/de/en/view/84922825)
    Industrial Ethernet / PROFINET - Passive network components System Manual

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

You can find the RCoax system manual on the Internet pages of Siemens Industry Online Support under the following entry ID:

- 109480869 (https://support.industry.siemens.com/cs/de/en/view/109480869)
  SIMATIC NET: Industrial Wireless LAN RCoax

1.5 Terms used

The designation . . .	stands for . . .
IPv4 address	IPv4 address
IPv6 address	IPv6 address
IP address	IPv4/IPv6 address
IPv4 interface	Interface that supports IPv4.
IPv6 interface	Interface that supports IPv6. The interface can have more than one IPv6 address The IPv6 addresses have different ranges (scope), e.g. link local
IP interface	Interface that supports both IPv4 and IPv6. As default the IPv4 support is already activated. The IPv6 support needs to be activated extra.

1.6 SIMATIC NET glossary

The SIMATIC NET glossary describes terms that may be used in this document.

You will find the SIMATIC NET glossary in the Siemens Industry Online Support at the following address:

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

1.7 Cybersecurity information

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

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

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

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html).

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

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/global/en/products/services/cert.html (https://new.siemens.com/global/en/products/services/cert.html).

1.8 Firmware

The firmware is available on the Internet pages of the Siemens Industry Online Support: (https://support.industry.siemens.com/cs/ww/en/ps/28575/dl)

Firmware

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

Note on firmware/software support

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

1.9 Open source license conditions

Note

Open source software

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

The license terms and copyright information can be downloaded from the WBM or CLI as a zip file.

- WBM: System > Load&Save > HTTP / TFTP / SFTP > LicenseCondition
- CLI: `sftp save filetype LicenseConditions / tftp save filetype LicenseConditions`

1.10 Error/fault

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

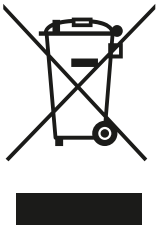
1.11 Decommissioning

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

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

Also restore the factory settings on the storage medium.

1.12 Recycling and disposal



The products are low in pollutants, can be recycled and meet the requirements of the WEEE directive 2012/19/EU for the disposal of electrical and electronic equipment.

Do not dispose of the products at public disposal sites.

For environmentally friendly recycling and the disposal of your old device contact a certified disposal company for electronic scrap or your Siemens contact (Product return (https://support.industry.siemens.com/cs/ww/en/view/109479891)).

Note the different national regulations.

1.13 Marken

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

SCALANCE, RCoax

Security recommendations

2

2.1 Security recommendations

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

General

- Check the device regularly to ensure that these recommendations and/or other internal security policies are complied with.
- Evaluate the security of your location and use a cell protection concept with suitable products (https://www.siemens.com/industrialsecurity).
- When the internal and external network are disconnected, an attacker cannot access internal data from the outside. Therefore operate the device only within a protected network area.
- No product liability will be accepted for operation in a non-secure infrastructure.
- Use VPN to encrypt and authenticate communication from and to the devices.
- For data transmission via a non-secure network, use an encrypted VPN tunnel (IPsec, OpenVPN).
- Separate connections correctly (WBM, SSH etc.).
- Check the user documentation of other Siemens products that are used together with the device for additional security recommendations.
- Using remote logging, ensure that the system protocols are forwarded to a central logging server. Make sure that the server is within the protected network and check the protocols regularly for potential security violations or vulnerabilities.

WLAN

- We recommend that you ensure redundant coverage for WLAN clients.
- More information on data security and data encryption for SCALANCE W is available in SCALANCE W: Setup of a Wireless LAN in the Industrial Environment (https://support.industry.siemens.com/cs/ww/en/view/22681042)

Authentication

Note

Accessibility risk - Risk of data loss

Do not lose the passwords for the device. Access to the device can only be restored by resetting the device to factory settings which completely removes all configuration data.

- Replace the default passwords for all user accounts, access modes and applications (if applicable) before you use the device.
- Define rules for the assignment of passwords.
- Use passwords with a high password strength. Avoid weak passwords, (e.g. password1, 123456789, abcdefgh) or recurring characters (e.g. abcabc).
  This recommendation also applies to symmetrical passwords/keys configured on the device.
- Make sure that passwords are protected and only disclosed to authorized personnel.
- Do not use the same passwords for multiple user names and systems.
- Store the passwords in a safe location (not online) to have them available if they are lost.
- Regularly change your passwords to increase security.
- A password must be changed if it is known or suspected to be known by unauthorized persons.
- When user authentication is performed via RADIUS, make sure that all communication takes place within the security environment or is protected by a secure channel.
- Watch out for link layer protocols that do not offer their own authentication between endpoints, such as ARP or IPv4. An attacker could use vulnerabilities in these protocols to attack hosts, switches and routers connected to your layer 2 network, for example, through manipulation (poisoning) of the ARP caches of systems in the subnet and subsequent interception of the data traffic. Appropriate security measures must be taken for non-secure layer 2 protocols to prevent unauthorized access to the network. Physical access to the local network can be secured or secure, higher layer protocols can be used, among other things.

Certificates and keys

- There is a preset SSL/TLS (RSA) certificate with 4096 bit key length in the device. Replace this certificate with a user-generated, high-quality certificate with key. Use a certificate signed by a reliable external or internal certification authority. You can install the certificate via the WBM ("System > Load and Save").
- Use certificates with a key length of 4096 bits.
- Use the certification authority including key revocation and management to sign the certificates.
- Make sure that user-defined private keys are protected and inaccessible to unauthorized persons.
- If there is a suspected security violation, change all certificates and keys immediately.
- Use password-protected certificates in the format "PKCS #12".
- Verify certificates based on the fingerprint on the server and client side to prevent "man in the middle" attacks. Use a second, secure transmission path for this.
- Before sending the device to Siemens for repair, replace the current certificates and keys with temporary disposable certificates and keys, which can be destroyed when the device is returned.

Physical/remote access

- Operate the devices only within a protected network area. Attackers cannot access internal data from the outside when the internal and the external network are separate from each other.
- Limit physical access to the device exclusively to trusted personnel.
  The memory card or the PLUG (C-PLUG, KEY-PLUG, CLP) contains sensitive data such as certificates and keys that can be read out and modified. An attacker with control of the device's removable media could extract critical information such as certificates, keys, etc. or reprogram the media.
- Lock unused physical ports on the device. Unused ports can be used to gain forbidden access to the plant.
- We highly recommend that you keep the protection from brute force attacks (BFA) activated to prevent third parties from gaining access to the device. For more information, see the configuration manuals, section "Brute Force Prevention (Page 288)".
- For communication via non-secure networks, use additional devices with VPN functionality to encrypt and authenticate communication.
- When you establish a secure connection to a server (e.g. for an upgrade), make sure that strong encryption methods and protocols are configured for the server.
- Terminate the management connections (e.g. HTTP, HTTPS, SSH) properly.
- Make sure that the device has been powered down completely before you decommission it. For more information, refer to "Decommissioning (Page 13)".
- We recommend formatting a PLUG that is not being used.

Hardware / Software

- Use VLANs whenever possible as protection against denial-of-service (DoS) attacks and unauthorized access.
- Restrict access to the device by setting firewall rules or rules in an access control list (ACL).
- Selected services are enabled by default in the firmware. It is recommended to enable only the services that are absolutely necessary for your installation.
  For more information on available services, see "List of available services (Page 19)".
- To ensure you are using the most secure encryption methods available, use the latest web browser version compatible with the product. Also, the latest web browser versions of Mozilla Firefox, Google Chrome, and Microsoft Edge have 1/n-1 record splitting enabled, which reduces the risk of attacks such as SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (for example, BEAST).
- Ensure that the latest firmware version is installed, including all security-related patches. You can find the latest information on security patches for Siemens products at the Industrial Security (https://www.siemens.com/industrialsecurity) or ProductCERT Security Advisories (https://www.siemens.com/cert) website.
  For updates on Siemens product security advisories, subscribe to the RSS feed on the ProductCERT Security Advisories website or follow @ProductCert on Twitter.
- Enable only those services that are used on the device, including physical ports. Free physical ports can potentially be used to gain access to the network behind the device.

- Use the authentication and encryption mechanisms of SNMPv3 if possible. Use strong passwords.
- Configuration files can be downloaded from the device. Ensure that configuration files are adequately protected.
  Configuration files can be password protected during download. You enter passwords on the WBM page "System > Load & Save > Passwords (Page 146)".
- When using SNMP (Simple Network Management Protocol):
  - Configure SNMP to generate a notification when authentication errors occur.
    For more information, see WBM "System > SNMP > Notifications (Page 168)".
  - Ensure that the default community strings are changed to unique values.
  - Use SNMPv3 whenever possible. SNMPv1 and SNMPv2c are considered non-secure and should only be used when absolutely necessary.
  - If possible, prevent write access.
- Use the security functions such as address translation with NAT (Network Address Translation) or NAPT (Network Address Port Translation) to protect receiving ports from access by third parties.
- Use WPA2/ WPA2-PSK / WPA3-SAE with AES to protect the WLAN. You can find additional information in the configuration manual Web Based Management "Security menu (Page 290)".
- Use PMF (Protected Management Frames) to cryptographically protect the management telegrams. You can find additional information in the configuration manual Web Based Management "Security menu (Page 290)".

Secure/ non-secure protocols

- Use secure protocols if access to the device is not prevented by physical protection measures.
- Disable or restrict the use of non-secure protocols. While some protocols are secure (e.g. HTTPS, SSH, 802.1X, etc.), others were not designed for the purpose of securing applications (e.g. SNMPv1/v2c, etc.).
  Therefore, take appropriate security measures against non-secure protocols to prevent unauthorized access to the device/network. Use non-secure protocols on the device using a secure connection (e.g. SINEMA RC).
- If non-secure protocols and services are required, ensure that the device is operated in a protected network area.

- Check whether use of the following protocols and services is necessary:
  - Non-authenticated and unencrypted ports
  - LLDP
  - Syslog
  - DHCP options 66/67
  - TFTP
  - Telnet
  - HTTP
  - SNMP v1/2c
  - SNTP
- The following protocols provide secure alternatives:
  - SNMPv1/v2c → SNMPv3
    Check whether use of SNMPv1/v2c is necessary. SNMPv1/v2c is classified as non-secure. Use the option of preventing write access. The product provides you with suitable setting options.
    If SNMP is enabled, change the community names. If no unrestricted access is necessary, restrict access with SNMP.
    Use SNMPv3 in conjunction with passwords.
  - HTTP → HTTPS
  - Telnet → SSH
  - TFTP → SFTP
  - Syslog Client → Syslog Client TLS
- Using a firewall, restrict the services and protocols available to the outside to a minimum.
- For the DCP function, enable the "Read Only" mode after commissioning.

2.2 Available services

List of available services

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

The table includes the following columns:

- **Service**
  The services that the device supports.
- **Protocol/port number**
  Port number assigned to the protocol.
- **Default status**
  The default status of the ports/service (e.g. open, closed, outgoing only).

- **Configurable port/service**
  Indicates whether the port number or the service can be configured via WBM / CLI.
- **Authentication**
  Specifies whether the communication partner is authenticated.
  If "optional", the authentication can be configured as required.
- **Encryption**
  Specifies whether the transfer is encrypted.
  If "optional", the encryption can be configured as required.

Service	Protocol / Port number	Default port status	Configurable		Authentication	Encryption [1]
			Port	Service		
DHCP Client IPv4	UDP/68	Outgoing only	--	✓	--	--
DHCP Client IPv6	UDP/546	Outgoing only	--	✓	--	--
DNS Client	TCP/53 UDP/53	Outgoing only	--	✓	--	--
HTTP	TCP/80	Open	✓	✓	✓	--
HTTPS	TCP/443	Open	✓	✓	✓	✓
NTP- Client	UDP/123	Outgoing only	✓	✓	--	--
Packet Capture	TCP/2002 TCP/2003 [2]	Closed	--	✓	--	--
PROFINET	UDP/34964 UDP/49154 UDP/49155	Open	--	✓	--	--
RADIUS	UDP/1812	Outgoing only	✓	✓	✓	--
SFTP Server	TCP/22	Closed	✓	✓	✓	✓
SMTP Client	TCP/25	Closed	✓	✓	--	--
SMTP (secure)	TCP/465	Closed	✓	✓	Optional	✓
SNMPv1/v2c	UDP/161	Open	✓	✓	--	--
SNMPv3	UDP/161	Open	✓	✓	Optional	Optional
SNMP Traps	UDP/162	Outgoing only	--	✓	--	--
SNTP Client	UDP/123	Outgoing only	✓	✓	--	--
SSH	TCP/22	Open	✓	✓	✓	✓
Syslog Client	UDP/514	Closed	✓	✓	--	--
Syslog Client TLS	TCP/6514	Closed	✓	✓	--	✓
Telnet	TCP/23	Closed	✓	✓	✓	--
TFTP Server	UDP/69	Closed	✓	✓	--	--
TCP Event	TCP/26864	Closed	✓	✓	✓	--

[1] You can find additional information on the encryption methods used in the WBM appendix "Ciphers used (Page 345)".

[2] The basic port of Packet Capture for the communication to Wireshark is TCP/2002. For each enabled interface, another port is enabled. Each additional port is an increment of TCP/2002, i.e. TCP/2003, TCP/2004, TCP/2005 etc.

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

The table includes the following columns:

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

Layer 2 service	**Default status**	**Service configurable**
DCP	Open	✓
LLDP	Open	✓
RSTP	Closed	✓
iPRP	Closed	✓
MSTP	Closed	✓
SIMATIC NET TIME	Closed	✓
802.1x	Closed	✓

Description

3

Note

Interruption of the WLAN communication

The WLAN communication can be influenced by high frequency interference signals and can be totally interrupted.

Remember this and take suitable action.

3.1 Product properties and hardware equipment

Properties of the SCALANCE W700 devices according to IEEE 802.11ax

- 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.
- Dual mode of the WLAN interface in access point mode with 2.4 GHz and 5 GHz with a CLP 2GB W700 AP iFeatures plugged in (not with SCALANCE WxB762).
- IEEE 802.11ax
  The WLAN standard IEEE 802.11ax (Wi-Fi 6) for efficient use of the frequencies with a gross transmission speed
  - SCALANCE WxM76x: 1201 Mbps per radio interface
  - SCALANCE WxB762: 601 Mbps per radio interface
- The WLAN interface is compatible with the standards IEEE 802.11n.
- IEEE 802.11r
  Optimization of roaming (Fast BSS Transition)

- 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 outdoors even with a higher transmit power.
  TPC is a technique for adapting the transmit power.
  With the DFS function, it is possible to also use the higher 5 Ghz channels. Before the access point transmits over one of these channels, it checks for competing radar signals for 60 seconds according to the CAC (Channel Availability Check). The access point also does not send any beacons for the duration of the search. With weather radar channels (5.6 - 5.65 GHz), the duration of the search is 10 minutes.
  If no radar signals are detected after the search period has elapsed, the access point transmits on the channel. Otherwise, the access point changes channel and repeats the check.
  The access point also searches for radar signals continuously during operation. If the access point discovers a radar signal on the current channel, it notifies the clients of the channel change. It then automatically switches to an alternative DFS channel and the current channel is blocked for 30 minutes.
- Support of the authentication standards WPA (RADIUS), WPA-PSK, WPA2 (RADIUS), WPA2-PSK, WPA3-SAE and IEEE 802.1X as well as the encryption method AES.

  Note

  With devices operated in WLAN mode IEEE 802.11n/ac, only WPA2 authentication (WPA2-PSK and WPA2 (RADIUS)) encryption is possible.

  Devices in WLAN mode IEEE 802.11ax support authentication methods WPA2 and WPA3-SAE (Simultaneous Authentication of Equals).

- Suitable for inclusion of a RADIUS server for authentication.
- Device-related and application-related monitoring of the wireless connection.
- Thoroughly tested for interoperability with Wi-Fi devices of other vendors.
- Before commissioning the SCALANCE W700ax, check the wireless conditions on site. Overlaps can lead to performance impairments, especially with simultaneous operation of multiple applications. We recommend thorough spectrum management or channel planning enforced by processes.

Hardware equipment

The following table shows the hardware equipment of the SCALANCE W devices.

We reserve the right to make technical changes.

Device	**Access point** **WAM766-1** **WAM 766-1 EEC**	**Client** **WUM766-1**	**Access point** **WAM763-1**	**Client** **WUM763-1**	**Access point** **WAB762-1**	**Client** **WUB762-1** **WUB762-1 iFeatures**
Number of WLAN interfaces	2	1	2	1	1	1
Connections for external antennas	2 x N-Connector		2 x R-SMA female		1 x R-SMA female	

Device	Access point WAM766-1 WAM 766-1 EEC	Client WUM766-1	Access point WAM763-1	Client WUM763-1	Access point WAB762-1	Client WUB762-1 WUB762-1 iFeatures
Ethernet interface	M12 Ethernet interface P1 LAN PoE, X-coded, 8-pin		4 x RJ45 socket		1 x RJ45 socket	
Power supply (direct)	M12 interface, direct infeed, L-coded, 4-pin		Terminal block, 5-pin		Terminal block, 3-pin	
Digital input/output	M12 interface, A-coded, 5-pin		Terminal block, 2-pin		Not available	
Degree of protection	IP65		IP30		IP20	
CLP interface	Available		Available		Not available	
PoE interface	Available		Not available		Not available	

3.2 Availability of the interfaces

The following table shows the availability of the physical and logical interfaces. Note that in this table all interfaces are listed. Depending on the system function, some interfaces are not available. On the WBM pages you can only select the available interfaces.

We reserve the right to make technical changes.

Device	Access point WAM766-1 WAM766-1 EEC	Client WUM766-1	Access point WAM763-1	Client WUM763-1	Access point WAB762-1	Client WUB762-1 WUB762-1 iFeatures
Wireless interface (WLAN)	WLAN 1 WLAN 2	WLAN 1	WLAN 1 WLAN 2	WLAN 1	WLAN 1 WLAN 2	WLAN 1
LAN interface	P1 LAN PoE	P1 LAN PoE	P1 - P4	P1 - P4	P1	P1
VAP interface	VAP X.Y X = 1 ... 2 Y = 1 ... 8	-	VAP X.Y X = 1 ... 2 Y = 1 ... 8	-	VAP X.Y X = 1 ... 2 Y = 1	-
VLAN	24	24	24	24	5	5

3.3 Availability of the system functions

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

We reserve the right to make technical changes.

Menu item in the WBM	**System functions**		**SCALANCE WxM76x**		**SCALANCE WxB762**	
			Access point mode	**Clients Access points in client mode**	**Access point mode**	**Clients Access points in client mode**
Information	ARP table		✓		✓	
	Log table		✓		✓	
	Error		✓		✓	
	Redundancy protocol		✓		✓	
	Ethernet statistics		✓		✓	
	Unicast MAC table		✓		✓	
	LLDP neighbors		✓		✓	
	IPv4 Routing		✓		✓	
	IPv6 Routing		✓		✓	
	SNMPv3 Groups		✓		✓	
	Security		✓		✓	
	WLAN	Overview AP	✓	-	✓	-
		Client List	✓	-	✓	-
		Overlap AP	✓	-	✓	-
		Overview Client	-	✓	-	✓
		Available APs	-	✓	-	✓
		IP Mapping	-	✓	-	✓
	WLAN statistics		✓		✓	
	WLAN iFeatures		✓		-	✓[1)]

Menu item in the WBM	System functions		SCALANCE WxM76x		SCALANCE WxB762	
			Access point mode	Clients Access points in client mode	Access point mode	Clients Access points in client mode
System	DNS client		✓		✓	
	SMTP client		✓		✓	
	DHCP client		✓		✓	
	SNMP		✓		✓	
	Sleep Mode		✓		-	
	Manual time setting		✓		✓	
	DST		✓		✓	
	SNTP Client		✓		✓	
	NTP Client		✓		✓	
	NTP server		✓		✓	
	SIMATIC Time Client		✓		✓	
	Auto logout		✓		✓	
	Syslog client		✓		✓	
	Fault monitoring		✓		✓	
	PROFINET		✓		✓	
	PLUG		✓		-	
	Ping		✓		✓	
	DCP Discovery		✓		✓	
	Configuration backup		✓		✓	
	TCP Event		✓		✓ [1)]	
Interfaces	Ethernet		✓		✓	
	WLAN	Basic	✓		✓	
		Extensions	✓		✓	
		Antennas&Power	✓		✓	
		Allowed Channels	✓		✓	
		Access point	✓	-	✓	-
		Client	-	✓	-	✓
	Packet Capture		✓	-	✓	-
Layer 2	Port Based VLAN		✓		✓	
	Dynamic MAC aging		✓		✓	
	Ring with RSTP		✓		✓	
	Spanning Tree		✓		✓	
	RSTP		✓		✓	
	MSTP		✓		✓	
	DCP forwarding		✓		✓	
	LLDP		✓		✓	
Layer 3	Agent IPv4/IPv6		✓		✓	
	NAT/NAPT		-	✓	-	✓
	Static routes		✓		✓	

Menu item in the WBM	System functions		SCALANCE WxM76x		SCALANCE WxB762	
			Access point mode	Clients Access points in client mode	Access point mode	Clients Access points in client mode
Security	Users		✓		✓	
	Passwords		✓		✓	
	RADIUS authentication		✓		✓	
	Brute Force Prevention		✓		✓	
	WLAN	Basic	✓	✓	✓	✓
		AP RADIUS Authenticator	✓	-	✓	-
		Client RADIUS Supplicant	-	✓	-	✓
		802.11r	✓	-	✓	-
iFeature	iPRP		✓[2)]	✓[2) 3)]	-	✓[1)]
	iPCF-2		✓[2)]	✓[2) 3)]	-	✓[1)]

1) Only for SCALANCE WUB762-1 iFeatures

2) CLP 2GB W700 AP iFeatures 6GK5907-8UA00-0AA0

3) CLP 2GB W700 Client iFeatures 6GK5907-4UA00-0AA0

3.4 Configuration limits

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

Depending on your device, some functions are not available.

Menu item in the WBM	Configurable function		Maximum number	
			SCALANCE WxM76x	SCALANCE WxB762
System	Syslog server		3	3
	DNS server	manual (IPv4)	3	3
		learned (IPv4)	2	2
		in total	7	7
	SMTP server		3	3
	SNMPv1/v2c and v3 Trap receiver		10	10
	SNMP queries		50	50
	SNTP server		2	2
	NTP server		1	1
Interfaces	Connected clients per WLAN interface		128	10
Layer 2	Virtual LANs (port-based, including VLAN 1)		24	5
	Multiple Spanning Tree instances		16	3
Layer 3	IP interface		2 1 subnet per IP interface	
	DHCP client		1	

Menu item in the WBM	Configurable function	Maximum number	
		SCALANCE WxM76x	SCALANCE WxB762
Security	IP addresses from RADIUS servers	• AAA:6 • WLAN: 2	• AAA:6 • WLAN: 2
	User roles	32 (incl. the predefined roles)	32 (incl. the predefined roles)
	User groups	32	32
	Users	30 (incl. the predefined users)	30 (incl. the predefined users)
	Firewall • NAPT rules (only with clients)	 32	 12

3.5 Planned operating environment

This section describes the recommended conditions for the most secure operation possible of the SCALANCE W700 components. These recommendations are not exhaustive and do not replace your own Threat and Risk Assessment with derivation of relevant measures.

- For secure operation, observe the security recommendations (Page 15).
- Make sure that only authorized persons have physical access to the component.
- Make sure that only authorized persons have permission to access the component via the network (user or access management).
- Introduce effective security incident handling processes.

3.6 Requirements for installation and operation

A PG/PC with network connection must be available in order to configure the SCALANCE W devices. If no DHCP server is available, a PC on which the SINEC PNI is installed is necessary for the initial assignment of an IP address to the SCALANCE W devices. The other configuration settings require a client PC with a Web browser (HTTPS) or a terminal software (SSH client).

3.7 Configuration License PLUG (CLP)

Note

Availability of the CLP interface

Not all device variants have a CLP interface. For more detailed information, refer to the section "Product properties and hardware equipment (Page 23)".

The PLUG is available in the following variants:

- PLUG Configuration: The exchangeable storage medium only saves the configuration data of the device.
- PLUG License: In addition to the configuration data, the exchangeable storage medium contains a license with which special functions are enabled, e.g. iFeatures.

How it works

NOTICE
Do not remove or insert the PLUG during operation. A PLUG may only be removed or inserted when the device is turned off. The device checks whether a PLUG is inserted at one second intervals. If it is detected that the PLUG has been removed, the device restarts. If a valid PLUG license 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 license, 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.

Devices with CLP slot support the following operating modes:

- **Without PLUG**
  The device saves the configuration data in the internal memory. This mode is active when no PLUG is inserted.
- **With PLUG**
  If an empty PLUG (as supplied) is inserted in the device, the device automatically backs up the configuration data on the PLUG during startup. If the PLUG contains a license, additional functions are also enabled. Changes to the configuration are stored directly on the PLUG and in the internal memory.
  The configuration stored on the PLUG is displayed over the user interfaces.
  When a device starts up, it automatically adopts the configuration data of the inserted, written PLUG. The prerequisite for this is that the configuration data was written by a compatible device type.
  One exception to this can be the IP configuration if it is set using DHCP and the DHCP server has not been reconfigured accordingly. Reconfiguration is necessary if you use functions based on MAC addresses.

Component	Description	Article number
CLP Configuration License PLUG	Exchangeable storage medium for saving configuration data	
	SCALANCE CLP 2GB	6GK1900-0UB00-0AA0
	SCALANCE CLP EEC 2GB	6GK1900-0UQ00-0AA0
	SCALANCE CLP 32GB	6GK1900-0UB40-0AA0

Component	Description	Article number
CLP iFeatures	Exchangeable storage medium for saving configuration data and enabling iFeatures	
	SCALANCE CLP 2GB W700 AP iFeatures	6GK5907-8UA00-0AA0
	SCALANCE CLP 2GB W700 Client iFeatures	6GK5907-4UA00-0AA0

3.8 PRESET PLUG

CLP with preset function (PRESET-PLUG)

Note

Availability of the CLP interface

Not all device variants have a CLP interface. For more detailed information, refer to the section "Product properties and hardware equipment (Page 23)".

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

Note

Using configurations with DHCP

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

You assign fixed IP addresses extra following the basic installation.

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

Note

Restore factory defaults and restart with a PRESET PLUG inserted

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

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

For more detailed information on creating and using a PRESET PLUG refer to the section Device configuration with PRESET-PLUG (Page 313).

3.9 Power over Ethernet (PoE)

General

"Power over Ethernet" (PoE) is a power supply strategy for network components according to IEEE with 802.3af or 802.3at.

With PoE, power and data transmission takes place over the used Ethernet cables that connect the individual network components. This makes an additional power cable unnecessary and reduces investment and maintenance costs. PoE can be used with all 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 device.

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.

LEDs for PoE on the SCALANCE W device

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

3.10 Digital input / output

Introduction

Some device variants have a digital input and output. You can find information on the availability of a digital input and output in the section "Product properties and hardware equipment (Page 23)". You can find information on connection and pin assignment in the operating instructions for the relevant device.

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 the private MIB variable snMspsDigitalOutputLevel, you can control the digital output (DO/1L). The digital output acts as NO contact and conducts current in the closed state.

Note

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

You can note the current state of the digital output and restore it after a restart. You can find more information on the WBM page "System > Configuration".

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 (DO) is open.
  - 2: Digital output (DO) is closed.

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).industrialComProducts(20).iComPlatforms(1).simaticNet(1).snMsps(1).snMspsCommon(1).snMspsDigitalIO(39).snMspsDigitalIOObjects(1).snMspsDigitalInputTable(2).snMspsDigitalInputEntry(1).snMspsDigitalInputLevel(6)`
- Values of the MIB variable
  - 1: Signal 0 at the digital input (DI)
  - 2: Signal 1 at the digital input (DI)

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". For more detailed information, refer to Appendix B "Private MIBs" (Page 323).

Technical basics

4

4.1 PROFINET

PROFINET

PROFINET is an open standard (IEC 61158/61784) for industrial automation based on Industrial Ethernet. PROFINET uses existing IT standards and allows end-to-end communication from the field level to the management level as well as plant-wide engineering. PROFINET also has the following features:

- Use of TCP/IP
- Automation of applications with real-time requirements
  - Real-Time (RT) communication
  - Isochronous Real-Time (IRT) communication
- Seamless integration of fieldbus systems

You configure PROFINET in "System > PROFINET (Page 188)".

PROFINET IO

Within the framework of PROFINET, PROFINET IO is a communications concept for implementing modular, distributed applications. PROFINET IO is implemented by the PROFINET standard for programmable controllers (IEC 61158-x-10).

4.2 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.

For the identifier which frame is assigned to which VLAN, the frame is expanded by 4 bytes (VLAN tagging). Apart from the VLAN-ID this expansion also includes priority information.

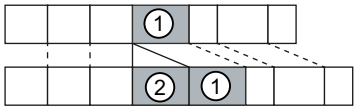
Options for the VLAN assignment

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 239)".
- 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.

Doubly tagged frame (Q-in-Q)

There are devices e.g. SCALANCE XR500 that support the Q-in-Q function. With the Q-in-Q function the incoming data traffic is treated as if it were untagged. With frames that are already tagged ①, this means they are expanded by a second VLAN tag, the outer VLAN tag ②.



When a SCALANCE W device receives a doubly tagged frame, it uses the VLAN ID from the outer VLAN tag ② and the priority information from the inner VLAN tag ①. The frame is then forwarded to the relevant VLAN.

4.3 MAC-based communication

Frames sent by the client to the access point always have the MAC address of the WLAN client as the source MAC address. In the "learning table" of the access point there is therefore only the MAC address of the WLAN client.

MAC mode "Own"

If the MAC address of the Ethernet interface of the WLAN client is used (Own), the MAC-based and IP-based frames only reach the WLAN client.

The access point checks whether the destination MAC address matches the MAC addresses of the connected clients. Since a WLAN client can only use a MAC address, communication at the MAC address level (ISO/OSI layer 2) can be to a maximum of one node downstream from the client or the client itself.

With IP Mapping, several nodes downstream from a client can be addressed based on the IP protocol. The IP packets are broken down according to an internal table and forwarded to the connected devices.

Maximum possible number of Ethernet nodes with layer 2 communication downstream from the client: 1

MAC mode "Layer 2 Tunnel"

The WLAN client uses the MAC address of the Ethernet interface for the WLAN interface.

The access point is also informed of the MAC addresses connected to the Ethernet interface of the WLAN client. 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 or MESH, a separate port is created for the L2T client over which the Ethernet frames are sent without changing the destination MAC address.

Performance statements from Siemens relating to real-time communication are calculated with a maximum number of 8 Ethernet subscribers downstream from the client.

4.4 iFeatures

4.4.1 iPCF-2

The wireless range of an IWLAN system can be expanded by using multiple access points. If a client is moved 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). If very fast update times and low latencies are required, for example for PROFINET communication, access points and client modules need to be used that meet the requirements through proprietary improvements, such as iPCF-2.

iPCF-2 and other iFeatures can only be operated alone. A combination with each other is not possible.

How it works

iPCF

With iPCF 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.

The "Legacy Free (iPCF-LF)" setting is available to prevent the performance from being slowed down by the IEEE 802.11 a/b/g device generation. When enabled, only the devices that communicate with the IEEE 802.11n standard and have the "Legacy Free (iPCF-LF)" setting enabled are accepted. WLAN mode IEEE 802.11n need not be enabled for this, however.

Stable PROFINET communication is only possible when a WLAN client is in a wireless cell with more than 60 % or -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.

iPCF-HT and iPCF-MC are expansions of iPCF for the WLAN mode IEEE 802.11n. You can find more information in the document "IWLAN: Configuring an Industrial Wireless LAN" under the following entry ID:
90880063 (https://support.industry.siemens.com/cs/de/en/view/90880063)

iPCF-2

iPCF-2 is introduced according to IEEE 802.11ax for the first time with the firmware version V2.0 of the SCALANCE W700 devices. The functionality will be expanded and improved during the subsequent stages.

iPCF-2 in FW V2.0 consists of various proprietary mechanisms that enable real-time communication along defined paths, such as absolute prioritization of PROFINET traffic, Fast Transition and more.

The function "TCP Event > WLAN Roaming" enables rapid roaming through transfer of parameters of the access point to which the client will establish a connection next after the application.

You configure iPCF-2 under "iFeatures > iPCF-2 (Page 305)".

4.4.2 iPRP

The "Parallel Redundancy Protocol" (PRP) is a redundancy protocol for cabled networks. It is defined in Part 3 of the IEC 62439 standard.

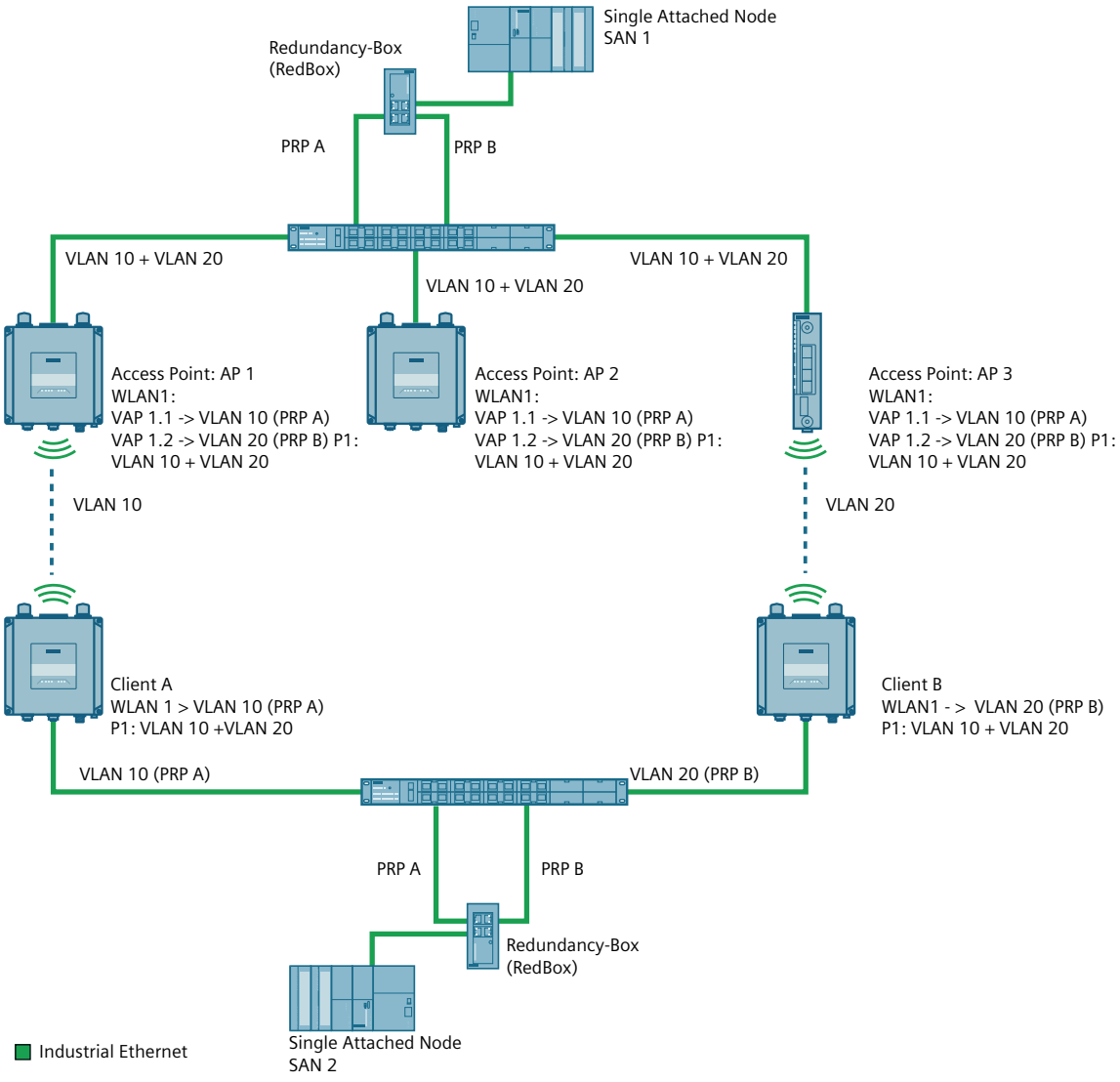
With the "industrial Parallel Redundancy Protocol" (iPRP) the PRP technology can be used in wireless networks. This improves the availability of wireless communication.

How it works

A PRP network consists of two completely independent networks. If one network is disrupted, the frames are sent without interruption/reconfiguration via the parallel redundant network. To achieve this the Ethernet frames are sent to the recipient in duplicate via both networks. Devices capable of PRP have at least two separate Ethernet interfaces that are connected to independent networks.

With devices not capable of PRP a redundancy box (RedBox) is connected upstream. This allows access for so-called Single Attached Nodes (SAN) to PRP networks. The RedBox duplicates every Ethernet frame to be sent and adds a PRP trailer to the frame that among other things contains a sequence number. The RedBox simultaneously sends a copy of the frame to the PRP A and PRP B network. At the receiving end the duplicate frame is discarded by the RedBox. For this the RedBox requires certain transfer times designed for Ethernet networks. For this reason using PRP in WLAN networks results in duplicate and delayed frames.

With iPRP, this problem is solved and the use of PRP in WLAN with SCALANCE W devices becomes possible



The access points (AP 1, AP 2 and AP 3) and the RedBox at the AP end are connected to each other via a switch. PRP network A und B are separated from each other via VLANs.

If SAN1 sends a frame to SAN2, the frame is duplicated by the RedBox at the AP end and the two redundant frames are transferred via the switch to the access points. Via the two different wireless paths the redundant PRP frames are transferred to the RedBox at the client end. The clients are also connected to their RedBox via a switch. This forwards the first PRP frame to arrive to SAN2 and discards the second one.

With transfer paths that are not the same, iPRP reduces the number of duplicated and out-of-order packets. The application/protocol used must be able to handle the remaining duplicates and out-of-order packets.

Note

On the interfaces of the switches to the SCALANCE W devices, only the VLANs that are also set on the VAP or WLAN interfaces of the SCALANCE W devices may be configured.

With iPRP the redundant partners (here: AP1 and AP3 or client A and client B) communicate with each other via a switch to prevent the two redundant PRP frames from arriving at the RedBox with too great a time difference.

If for example the communication between AP1 and client A is very slow, the slower frame is discarded at the receiving end.

You configure iPRP in "iFeatures > iPRP (Page 307)".

Requirement

- iPRP can only be used with the CLP iFeatures (Page 29).
- The base bridge mode "802.1Q VLAN Bridge" is set.
- The VLANs have been created.
- Access point mode: The VAP interface is enabled.
- Client mode: In MAC mode "Layer 2 Tunnel" is set.
- Depending on the configuration the clients can communicate with every access point.
- The Spanning Tree Protocol is disabled.

4.5 SNMP

Introduction

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

Tasks of SNMP:

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

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

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

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

Standard values of the community strings:

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

Note

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

Further simple protection mechanisms at the device level:

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

SNMP data packets 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 a data record from the SNMP agent
- GETNEXT
  Calls up the next data record.
- GETBULK (available as of SNMPv2c)
  Requests multiple data records at once, for example several rows of a table.
- SET
  Contains parameter assignment data for the relevant device.

The SNMP agent sends data packets of the following type:

- RESPONSE
  The SNMP agent returns the data requested by the manager.
- TRAP
  If a certain event occurs, the SNMP agent itself sends traps.
- INFORM
  Like a trap except that it is acknowledged by the receiver.

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

SNMPv3

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

SNMPv3 supports:

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

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

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

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

Restriction when using the function

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

Compatibility with predecessor products

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

4.6 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.

4.6.1 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.

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.

4.7 User management

Overview of user management

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

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

Local logon

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

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

Login via an external RADIUS server

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

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

RADIUS authorization mode "Standard"

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

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

RADIUS authorization mode "Manufacturer-specific"

Requirement

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

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

Procedure

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

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

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

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

4.8 NAT

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

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

IP masquerading

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

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

You configure masquerading in "Layer 3" > "NAT" > "IP Masquerading (Page 265)".

NAPT

NAPT (Network Address and Port Translation) is a form of destination NAT and is often called port forwarding.

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

The options are available for port translation:

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

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

Configure NAPT under "Layer 3 (IPv4)" > "NAPT (Page 266)".

4.9 Network structures

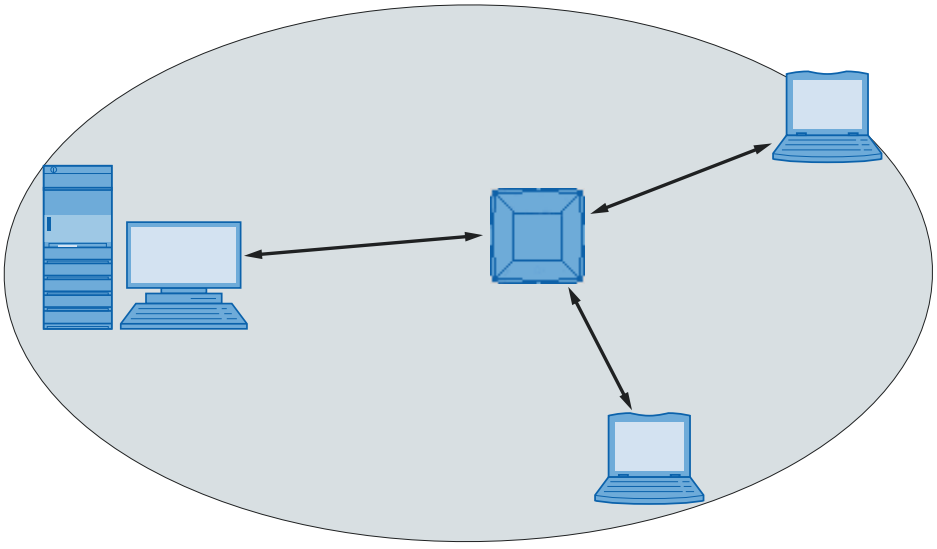
The following article deals with the setup of various network structures using access points.

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 SCALANCE W devices exchanging data within this network must be configured with this name.

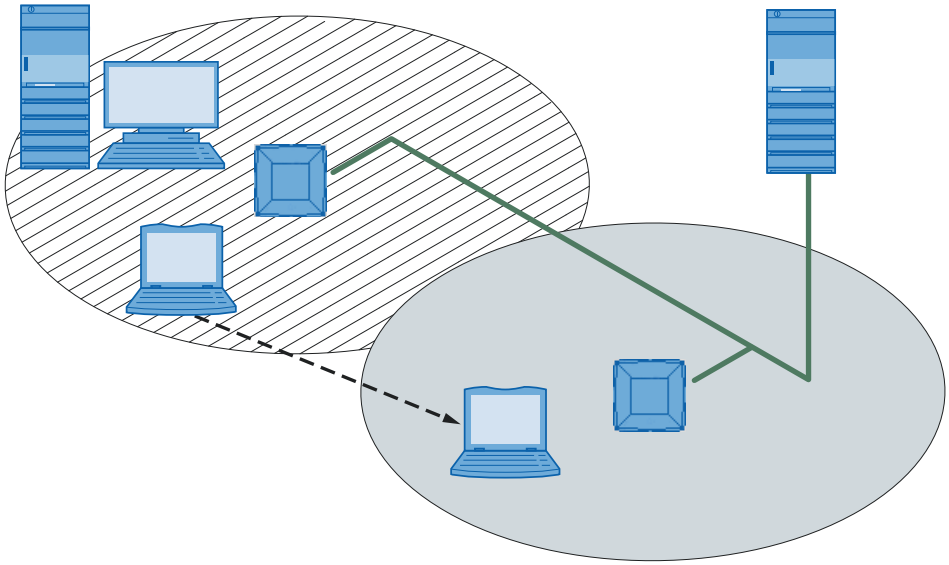
The gray area in the graphic symbolizes the wireless range of the access point.



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).
  The following graphic shows the wireless connection of a mobile station over two wireless cells (roaming).



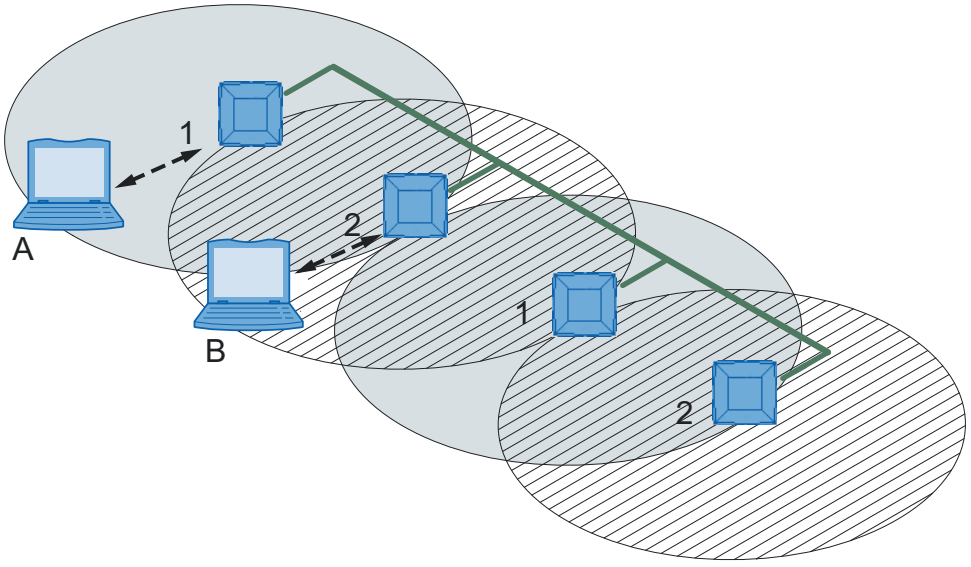
Multichannel configuration

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.

The following graphic shows a multichannel configuration on channels 1 and 2 with four access points.



4.10 Possible applications

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.

4.11 IEEE 802.11r

During roaming, the WLAN client roams from one access point to the next. A delay time of several 100 ms can come about at the connection transition.

The following steps can be executed during this time:

- Client searches for a new access point (scanning)
- Logon at a new access point (authentication and association)
- Allow a data connection via the new access point

Shorter delay times are required for time-critical applications, for example, Voice over IP. The standard IEEE 802.11r contains amendments which optimize roaming and therefore is also referred to as Fast BSS Transition (FT).

With FT, the WLAN client must not authenticate every time the access point changes. For this purpose, the access points are grouped into a mobility domain. The WLAN client receives the mobility domain ID from the first access point to which it logs on. The log-on information is buffered within the mobility domain. This logon is valid for all members of the mobility domain.

Based on the ID, the WLAN client recognizes whether the access point is a member of the same mobility domain and can therefore log on without delay. Only WLAN clients with IEEE 802.11r support can use the improved roaming or handover functions.

Requirement

- The access points are members of the same mobility domain
- Only possible with the following encryptions:
  - WPA2-PSK
  - WPA2 RADIUS
  - WPA3-SAE

IP addresses

5

5.1 IPv4 / IPv6

What are the essential differences?

	IPv4	IPv6
IP configuration	• DHCP server • Manual	• Stateless Address Autoconfiguration (SLAAC): Stateless autoconfiguration using NDP (Neighbor Discovery Protocol) – Creates a link local address for every interface that does not require a router on the link. – Checks the uniqueness of the address on the link that requires no router on the link. – Specifies whether the global addresses are obtained via a stateless mechanism, a stateful mechanism or via both mechanisms. (Requires a router on the link.) • Manual • DHCPv6 (stateful)
Available IP addresses	32-bit: 4, 29 * 10^9 addresses	128-bit: 3, 4 * 10^{38} addresses
Address format	Decimal: 192.168.1.1 with port: 192.168.1.1:20	Hexadecimal: 2a00:ad80::0123 with port: [2a00:ad80::0123]:20
Loopback	127.0.0.1	::1
IP addresses of the interface	5 IP addresses	Multiple IP addresses • LLA: A link local address (formed automatically) fe80::/128 per interface • ULA: Several unique local unicast addresses per interface • GUA: Several global unicast addresses per interface
Header	• Checksum • Variable length • Fragmentation in the header • No security	• Checking at a higher layer • Fixed size • Fragmentation in the extension header
Fragmentation	Host and router	Only endpoint of the communication
Quality of service	Type of Service (ToS) for prioritization	The prioritization is specified in the header field "Traffic Class".
Types of frame	Broadcast, multicast, unicast	Multicast, unicast, anycast

	IPv4	**IPv6**
Identification of DHCP clients/ server	Client ID: • MAC address • DHCP client ID • System name • PROFINET station name • IAID and DUID	DUID + IAID(s) = exactly one interface of the host DUID = DHCP unique identifier Unique identifier of server and clients IAID = Identity Association Identifier At least one per interface is generated by the client and remains unchanged when the DHCP client restarts Three methods of obtaining the DUID • DUID-LLT • DUID-EN • DUID-LL
DHCP	via UDP with broadcast	via UDP with unicast RFC 3315, RFC 3363 **Stateful DHCPv6** Stateful configuration in which the IPv6 address and the configuration settings are transferred. Four DHVPv6 messages are exchanged between client and server: 1. SOLICIT: Sent by the DHCPv6 client to localize DHCPv6 servers. 2. ADVERTISE The available DHCPv6 servers reply to this. 3. REQUEST The DHCPv6 client requests an IPv6 address and the configuration settings from the DHCPv6 server. 4. REPLY The DHCPv6 server sends the IPv6 address and the configuration settings. If the client and server support the function "Rapid commit" the procedure is shortened to two DHCPv6 messages SOLICIT and REPLY . **Stateless DHCPv6** In stateless DHCPv6, only the configuration settings are transferred. **Prefix delegation** The DHCPv6 server delegates the distribution of IPv6 prefixes to the DHCPv6 client. The DHCPv6 client is also known as PD router.
Resolution of IP addresses in hardware addresses	ARP (Address Resolution Protocol)	NDP (Neighbor Discovery Protocol)

5.2 IPv4 address

5.2.1 Structure of an IPv4 address

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

Example: 192.168.16.2

The IPv4 address is composed of:

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

Subnet mask

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

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

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

Example:

Correct values

255.255.0.0 D = 1111 1111.1111 1111.0000 0000.0000 0000 B

255.255.128.0 D = 1111 1111.1111 1111.1000 0000.0000 0000 B

255.254.0.0 D = 1111 1111.1111 1110.0000 0000.0000.0000 B

Incorrect value:

255.255.1.0 D = 1111 1111.1111 1111.0000 0001.0000 0000 B

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

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

The following applies in general:

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

Classless Inter-Domain Routing (CIDR)

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

Example:

IPv4 address 192.168.0.0 with subnet mask 255.255.255.0

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

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

Masking additional subnets

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

Example:

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

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

Result:

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

Network gateway (router)

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

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

5.2.2 Initial assignment of an IPv4 address

Configuration options

An initial IP address for a SCALANCE W device 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)
- SINEC PNI
- STEP 7
- SINEC NMS

Note

When the product ships and following "Restore Memory 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 W device, the IP address, subnet mask and gateway are assigned automatically when the device first starts up. "Restore Factory Defaults and Restart" does not delete an IP address assigned either by DHCP or by the user.

SINEC INS can be used as in-house DHCP server and assign IP addresses to devices in the network.

5.2.3 Address assignment via DHCPv4

Properties of DHCP

DHCP (Dynamic Host Configuration Protocol) is a method for automatic assignment of IPv4 addresses. It has the following characteristics:

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

- There is normally no fixed address assignment; in other words, when a client requests an IP address again, it normally receives a different address from the previous address. It is possible to configure the DHCP server so that the DHCP client always receives the same fixed address in response to its request. The parameter with which the DHCP client is identified for the fixed address assignment is set on the DHCP client. The address can be assigned via the MAC address, the DHCP client ID, PROFINET device name or the device name. You configure the parameter in "System > DHCP Client (Page 156)".
- 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

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.

5.2.4 Address assignment with SINEC PNI

Introduction

The SINEC PNI is capable of assigning such an address to unconfigured devices that do not yet have an IP address.

SINEC PNI

- To be able to assign an IP address to the device with SINEC PNI, it must be possible to reach the device via Ethernet.
- You can find SINEC PNI on the Internet pages of Siemens Industry Online Support at the following Link: (https://support.industry.siemens.com/cs/de/en/ps/26672/dl)
- For additional information about assigning the IP address with SINEC PNI, refer to the online help or the "SINEC PNI network management" operating instructions.

5.2.5 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 device. If you connect the unconfigured device to the controller, the controller assigns the configured device name and the IP address to the 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 additional information on assigning the IP address using STEP 7 as of V13, refer to the online help "Information system", section "Addressing PROFINET devices".

5.2.6 Address assignment with SINEC NMS

With SINEC NMS, you can detect and configure devices in the network.

- The device must be reachable via Ethernet.
- You can find SINEC NMS on the Internet pages of Siemens Industry Online Support at the following link: (https://support.industry.siemens.com/cs/ww/en/ps/25518)

5.3 IPv6 address

5.3.1 IPv6 terms

Network node

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

Router

A network node that forwards IPv6 packets.

Host

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

Link

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

Neighbor

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

IPv6 interface

Physical or logical interface on which IPv6 is activated.

Path MTU

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

Path MTU discovery

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

LLA

Link local address FE80::/10

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

ULA

Unique Local Address

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

GUA

Global unicast address

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

Interface ID

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

EUI-64

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

Example:

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

OUI = AA:BB:CC

NIC = DD:EE:FF

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

Scope

Defines the range of the IPv6 address.

5.3.2 Structure of an IPv6 address

IPv6 address format - notation

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

Example:

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

Rules / simplifications:

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

Structure of the IPv6 address

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

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

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

IPv6 prefix

Specified in: RFC 4291

The IPv6 prefix represents the subnet identifier.

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

Design

IPv6 address / prefix length

Example

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

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

Interface ID: ::1111

Entry and appearance

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

Configuring with Web Based Management 6

6.1 Web Based Management

To access Web Based Management (WBM) of the device, make a remote connection between a client PC and a device via the network. The device has an integrated HTTPS server for the WBM. When you address a device using an Internet browser, it returns HTML pages to the client PC depending on the user input.

Requirements

- The device has an IP address.

  Note

  Assign an IP address to the device using DHCP or SINEC PNI.

- There is a network connection between the device and the client PC.
- The network settings of the device and of the client PC match.

  Note

  You can use a ping to check whether a connection exists and communication is possible.

- Access via HTTP(S) is activated on the device.
- An Internet browser is available on the client PC.
- JavaScript is activated in the Internet browser.
- The Internet browser must not be configured in such a way that it reloads the page from the server each time the page is accessed. The updating of the dynamic content of the page is ensured by other mechanisms.
- If you are using a firewall, enable the corresponding ports.
  - For access using HTTPS: TCP port 443
  - For access using HTTP: TCP port 80

WBM display

The display of the WBM was tested with the following desktop Internet browsers:

- Mozilla Firefox
- Google Chrome
- Microsoft Edge

The WBM is tested with the current version of the Internet browser available at the time of firmware release.

Display of the WBM on mobile devices

For mobile devices, the following minimum requirements must be met:

Resolution	Operating system	Internet browser
960 x 640 pixels	Android as of version 4.2.1 iOS as of version 6.0.2	Chrome as of version 18 on Android Safari as of version 6 on iOS

- Tested with the following Internet browsers for mobile devices:
  - Safari as of version 8 on iOS as of V8.1.3 (iPad Mini Model A1432)
  - Chrome as of version 46 on Android as of version 5.0.2 (Nexus 7C Asus)
  - Firefox as of version 35 on Android as of version 5.0.2

Note

Display of the WBM and working with it on mobile devices

The display and operation of the WBM pages on mobile devices may differ compared with the same pages on desktop devices. Some pages also have an optimized display for mobile devices.

6.2 Login

Establishing a connection to a device

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

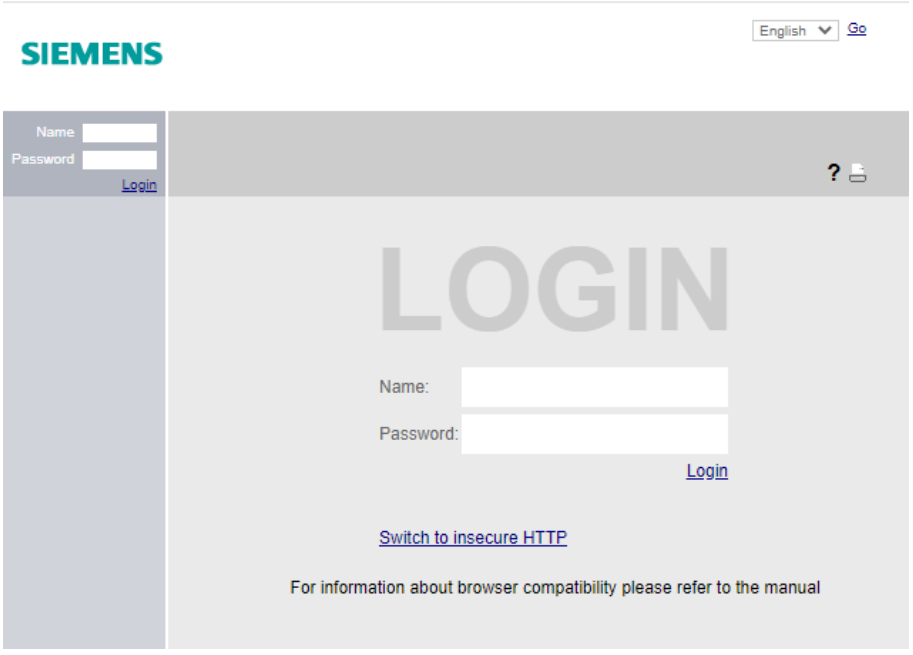
1. There is a connection between the device and the Admin PC. With the ping command, you can check whether or not a device can be reached.
2. In the address field of the web browser, enter "https://" followed by the IP address of the device to be configured or its URL, e.g. https://192.168.16.178.
   Access via HTTPS is enabled as default.

   Note

   Information on the security certificate

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

   A message relating to the security certificate appears. Acknowledge this message and continue loading the page.
   If you use a port other than the standard port, enter a colon ":" as separator between the IP address and the port number.
   Example: https://192.168.16.178:49152
   You change the port in "System > Configuration".
3. If there is a connection to the device, the login page of Web Based Management (WBM) is displayed.
   If you wish to access the WBM via a non-secure HTTP connection, activate the HTTP server under "System > Configuration". On the next login, click on the link "Switch to insecure HTTP" on the login page or enter "http://" and the IP address of the device in the address box of the web browser.



Changing language

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

Note
Available languages

English and German are available as languages.

Logging in to WBM

You have the following options for logging in via HTTPS. 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, whichever of the above options you choose.

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

     Note

     The password for the "admin" user has been changed for devices with the US version. Specialist personnel for professional WLAN installations can obtain the password from Siemens support.

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

   Note

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

   When you log in for the first time or following a "Restore Factory Defaults and Restart", you are prompted to change the password.
   The new password must meet the password policy "High":
   - Password length: At least 8 characters, maximum 128 characters
   - At least 1 uppercase letter
   - At least 1 special character (special characters | § ? " ; : ß \ ² ³ ° € µ ä ö ü Ä Ö Ü are not permitted)
   - At least 1 number
   - The characters for Space and Delete also cannot be contained.
4. Repeat the password to confirm. The password entries must match.
5. Click the "Set Values" button to complete the action.
   The changes take immediate effect. Access via DCP is write-protected after the admin password is changed. The network parameters can be read with SINEC PNI or with "DCP Discovery" but cannot be changed.

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

Protection from brute force attacks

To protect against brute force attacks, login to the device is denied for a user or for the IP address of a user after multiple failed login attempts. By default, the number of login attempts is preset to 12 per user and 10 per IP address. The wait time for which the page is locked for new login attempts increases after each invalid login attempt. You can change these settings on the page "Security > Brute Force Prevention".

Service technician login

The device has a service technician login for servicing purposes. This is only available after activation by an administrator and may only be used by Siemens Support.

6.3 "Information" menu

6.3.1 Start page

View of the Start page

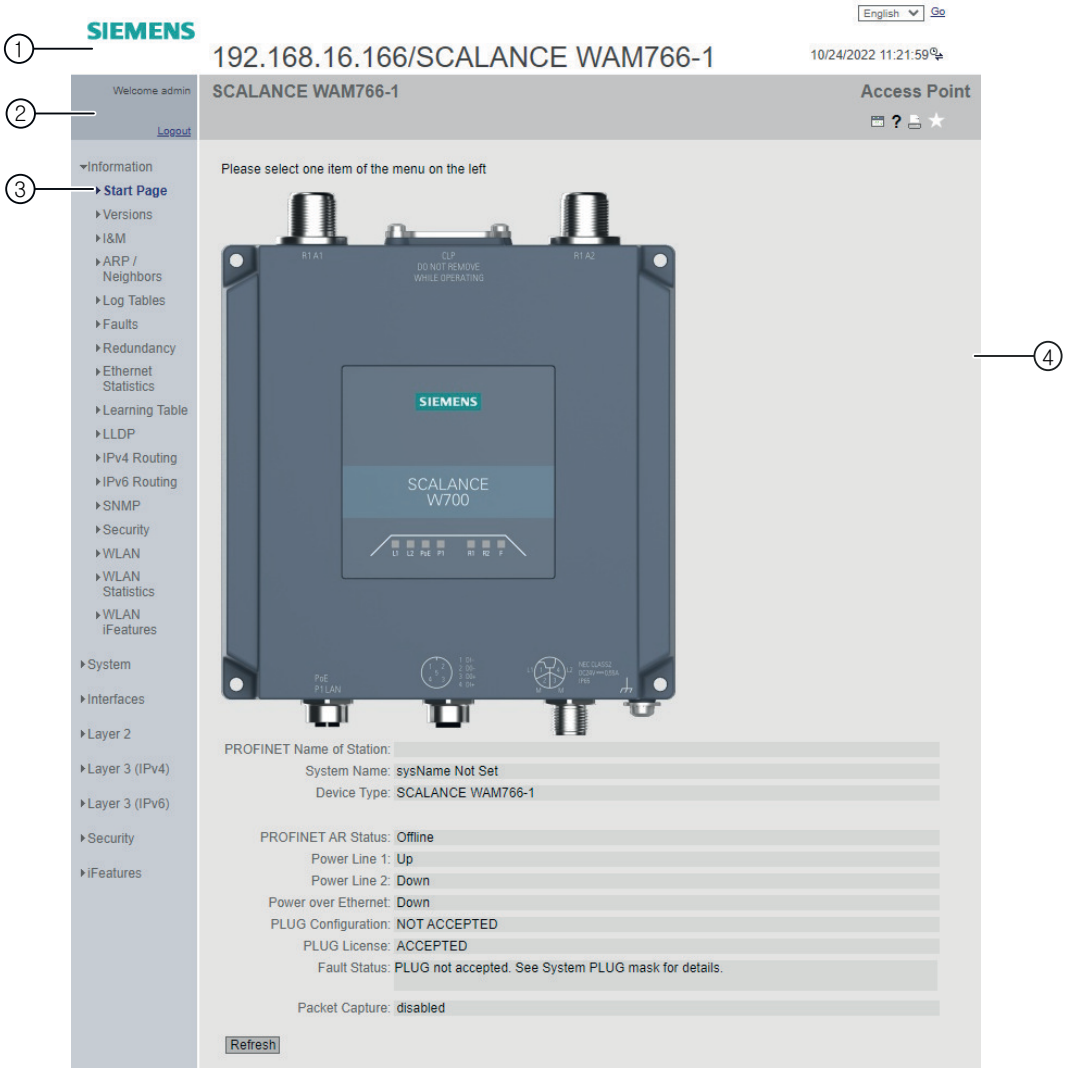
When you enter the IP address of the device, the start page is displayed after a successful login. You cannot configure anything on this page.

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



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.
    In delivery state, the IP address of the Ethernet interface is displayed.
  - "System Name" is the device name. In delivery state, the device type is displayed.

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

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

Display area (2)

In the upper part of the display area, you can see name of the currently logged in user and the full title of the currently selected menu item.

In the lower part of the display area, you will find:

- **Logout**
  You can log out from any WBM page by clicking the "Logout" link.
- **Device name**
  Shows the name of the device.
- **Mode**
  Shows the mode.
- **LED simulation**
  Each device has one or more LEDs that provide information on the operating state of the device. Depending on its location, direct access to the device may not always be possible. Web Based Management therefore displays simulated LEDs. Unused connectors are displayed as gray LEDs. The meaning of the LED displays is described in the operating instructions.
  If you click this button, you open the window for the LED simulation. This window is displayed for every menu item/submenu after opening and can be moved as desired. To close the LED simulation, click the close button in the LED simulation window.
- **Help**
  When you click this button, the help page of the currently selected menu item is opened in a new browser window.
  On every help page, there is an input box for the search function at the top edge. In this input box, enter a term for which you need additional information and start the search by pressing Enter. A dialog box displays a list of WBM pages that contain the term searched for. The corresponding WBM page is opened in a new tab of the browser after a list element is clicked
- **Printer**
  If you click this button, a popup window opens. The popup window contains a view of the page content optimized for printers.

Note

Printing larger tables

If you want to print large tables, please use the "Print preview" function of your Internet browser.

- **Favorites**
  When the product ships, the button is disabled on all pages .
  If you click this button, the symbol changes and the currently open page or currently open tab is marked as favorite. Once you have enabled the button once, the navigation area is divided into two tabs. The first tab "Menu" contains all the available menus as previously. The second tab "Favorites" contains all the pages/tabs that you selected as favorites. On the "Favorites" tab the pages/tabs are arranged according to the structure in the "Menu" tab.
  If you disable all the favorites you have created, the "Favorites" tab is removed again. To do this, click the button on the relevant pages/tabs.
  You can save, upload and delete the favorites configuration of a device on the "System > Load&Save" page using HTTP or TFTP.
- **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 disabled on the WBM page.

Navigation area (3)

In the navigation area, you have various menus with submenus available.

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.

You can expand or collapse menu entries in the navigation using the arrows. To expand the menu entries, click on the right arrow. If you click on the left arrow, the menu entries are collapsed again.

Content area (4)

The content area shows a graphic of the device. The graphic always shows the device whose WBM you have called up.

The following is displayed below the picture of the device:

- **PROFINET Name of Station**
  Shows the PROFINET device name.
- **System Name**
  Shows the name of the device.
- **Device Type**
  Shows the type designation of the device.

- **PROFINET AR Status**
  Shows the PROFINET application relation status.
  - Online
    There is a connection to a PROFINET controller. The PROFINET controller has downloaded its configuration data to the device. The device can send status data to the PROFINET controller.
    In this status, the parameters set by the PROFINET controller cannot be configured on the device.
  - Offline
    There is no connection to a PROFINET controller.
- **Power Line 1 / Power Line 2 / Power over Ethernet**
  Status of the power supplies 1 and 2 or power over Ethernet. The power line 2 and Power over Ethernet are only displayed if they are supported by the hardware. You can find additional information on this in the operating instructions.
- **PLUG configuration** (not with WxB762-1**)**
  Shows the status of the configuration data on the PLUG, refer to the section "System > PLUG > PLUG Configuration".
- **PLUG license** (not with WxB762-1**)**
  Shows the status of the license on the PLUG, refer to the section "System > PLUG > PLUG License".
- **Fault Status**
  Shows the fault status of the device.
- **Packet Capture**
  Shows the status of the "Packet Capture" function at the interface (Ethernet, WLAN).

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 bottom 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. When you create an entry, the page is refreshed
- **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. When you delete an entry, the page is refreshed.
- **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 back with "Prev"**
  The number of data records that can be displayed on a page is limited. Click the "Prev" button to page back through the data records.
- **Delete the display with "Clear"**
  In pages with sequence logs, you can delete all table entries at the same time regardless of whether filters are selected. The display is cleared in this process. The restart counter is only reset after you have restored the device to the factory settings and restarted the device. Click the "Clear" button to completely delete the data set.
- **Button "Show all"**
  You can show all entries in pages with a large number of data sets. Click "Show all" to display all entries on the page. Note that displaying all messages can take some time.
- **Drop-down list for page change**
  In pages with a large number of data records, you can navigate to the desired page. From the drop-down list, select the affected page to display it.
- **"Reset Counters" button**
  Click "Reset Counters" to reset all counters. The counters are also reset by a restart.

Messages

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

Note

Interrupting the save

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

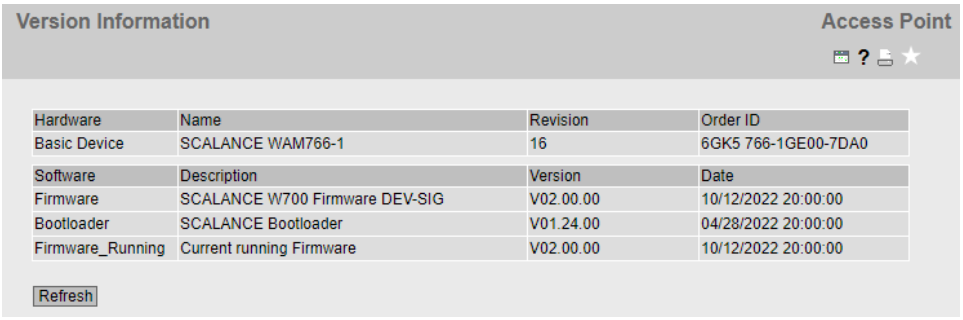
During the save, the message "Saving configuration data in progress. Please do not switch off the device" is displayed.

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

6.3.2 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.



Description

Table 1 has the following columns:

- **Hardware**
  - Basic Device
    Shows the basic device.
- **Name**
  Shows the name of the device or module.
- **Revision**
  Shows the hardware version of the device.
- **Article number**
  Shows the article number of the device or described module.

Table 2 has the following columns:

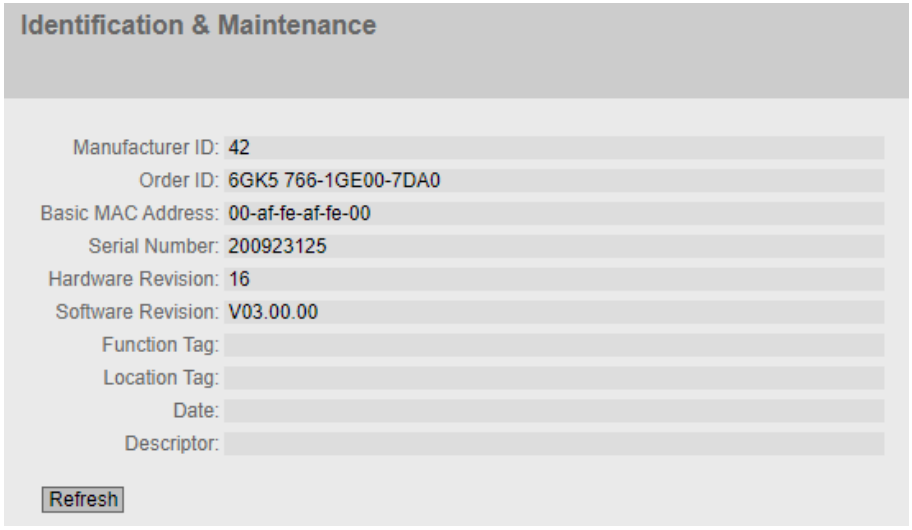
- **Software**
  - Firmware
    Shows the current firmware version. If a new firmware file was downloaded and the device has not yet restarted, the firmware version of the downloaded firmware file is displayed here. After the next restart, the downloaded firmware is activated and used.
  - Bootloader
    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.

6.3.3 I&M

Identification and maintenance data

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



Description

The table has the following rows:

- **Manufacturer ID**
  Shows the manufacturer ID.
- **Article number**
  Shows the article number.
- **Basic MAC Address**
  Shows the MAC address of the IPv4 interface.
- **Serial Number**
  Shows the serial number.
- **Hardware Revision**
  Shows the hardware version.
- **Software Revision**
  Shows the software version.

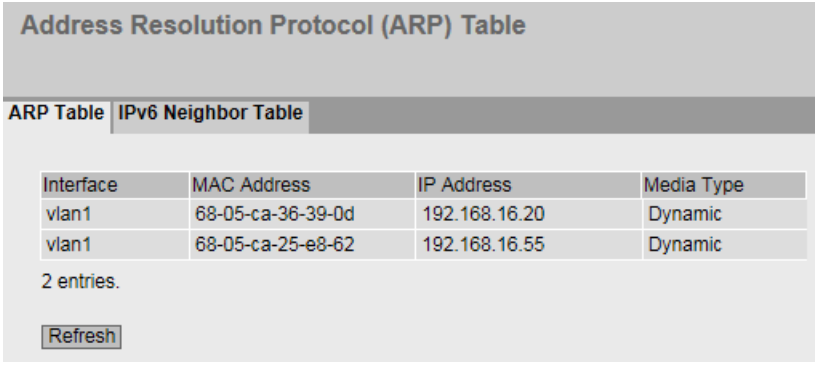
- **Function tag**
  Shows the function tag (plant designation) of the device. The plant designation (HID) is created during configuration of the device with HW Config of STEP 7.
- **Location tag**
  Shows the location tag of the device. The location identifier (LID) is created during configuration of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

6.3.4 ARP / neighbors

6.3.4.1 ARP-Tabelle

Assignment of MAC address and IPv4 address

With the Address Resolution Protocol (ARP), there is a unique assignment of MAC address to IPv4 address. This assignment is kept by each network node in its own separate ARP table. The WBM page shows the ARP table of the device.



Description of the displayed values

The table has the following columns:

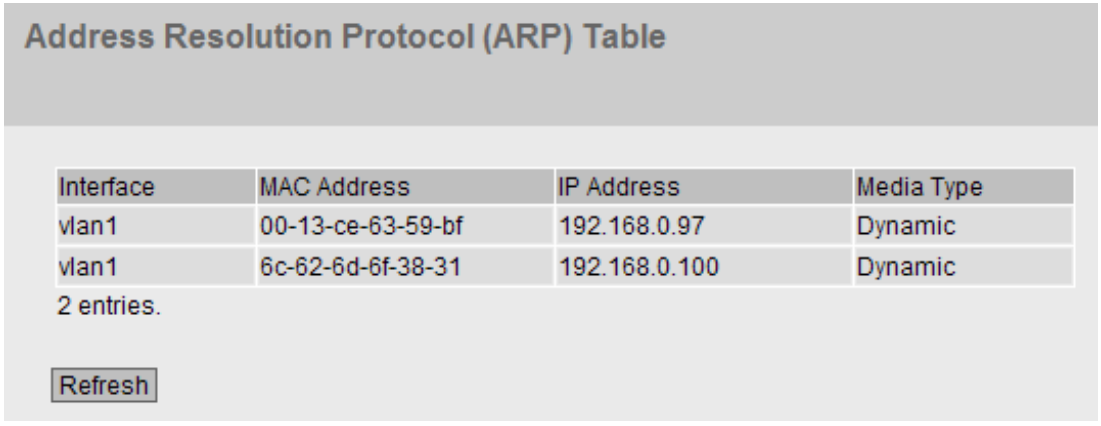
- **Interface**
  Shows the interface via which the row entry was learnt.
- **MAC Address**
  Shows the MAC address of the destination or source device.

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

6.3.4.2 IPv6 Neighbor Table

Assignment of MAC address and IPv6 address

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



Description of the displayed values

The table has the following columns:

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

6.3.5 Log Tables

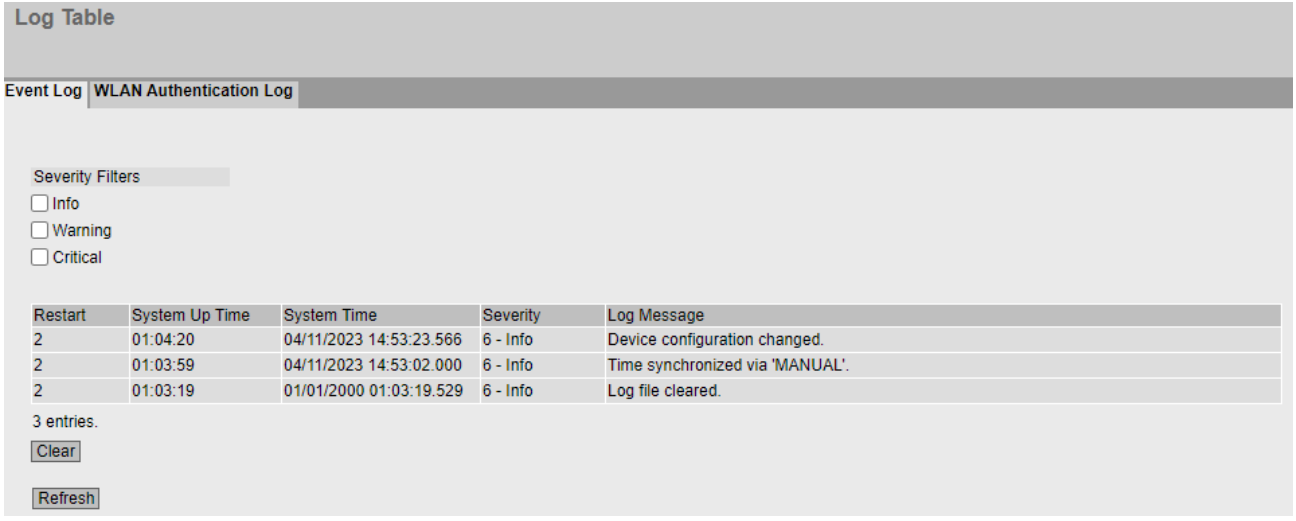
6.3.5.1 Event Log

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.



Description

The page contains the following boxes:

Severity filter

You can filter the entries in the table according to severity. Select the required entries in the check boxes above the table.

Note

A maximum of 2000 entries in the table are possible for each severity. If the maximum number of entries is reached for a severity, the oldest entries of this severity are overwritten in the table. The table remains permanently in the memory.

Under "System > Event > Configuration", you can specify a limit for the entries for each severity with "Log Table Alarm Threshold". If the specified limit will be reached with the next entry, an alarm message is output.

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

To display all entries, either select all of them or leave the check boxes empty.

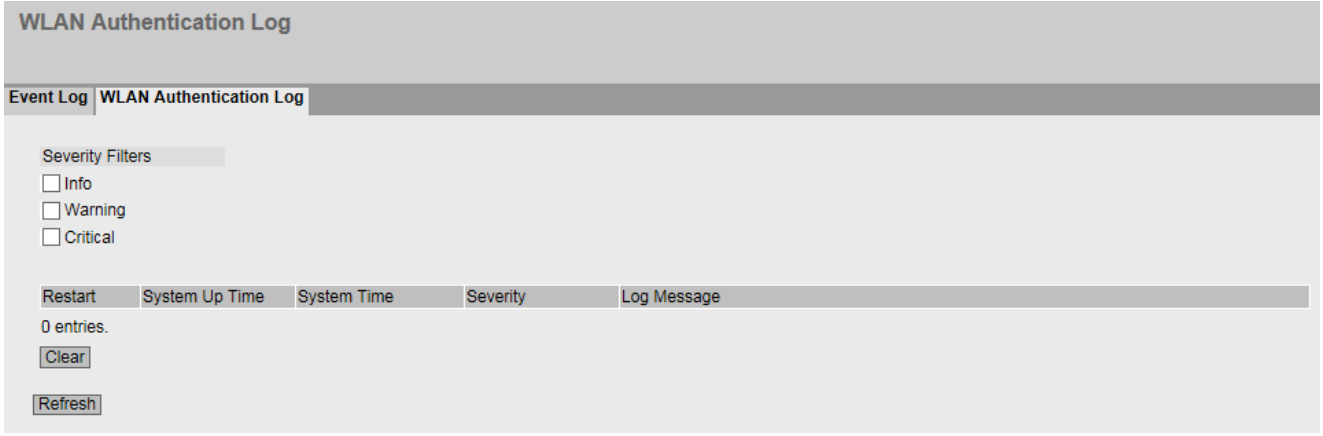
The table has the following columns:

- **Restart**
  Counts the number of restarts since you last reset to factory settings and shows the device restart after which the corresponding event occurred.
- **System Up Time**
  Shows the time the device has been running since the last restart when the described event occurred.
- **System Time**
  Shows the system time in the format MM/DD/YYYY hh:mm:ss.
  If the system time is set, the date and time of the described occurring event is displayed.
  If no system time is set or time synchronization has not yet taken place, the system time that has elapsed since the last restart is shown. After a restart, the time of day begins at 01/01/2000 00:00:00.
- **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 (Page 327) of the configuration manual.

6.3.5.2 WLAN authentication log

Logging authentication attempts

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



You cannot configure anything on this page.

Description

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

  Note

  A maximum of 2000 entries in the table are possible for each severity. If the maximum number of entries is reached for a severity, the oldest entries of this severity are overwritten in the table. The table remains permanently in the memory.

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

The table has the following columns:

- **Restart**
  Counts the number of restarts since you last reset to factory settings and shows the device restart after which the corresponding event occurred.
- **System Up Time**
  Shows the time the device has been running since the last restart when the described event occurred.
- **System Time**
  Shows the system time in the format MM/DD/YYYY hh:mm:ss.
  If the system time is set, the date and time of the described occurring event is displayed. If no system time is set or time synchronization has not yet taken place, the system time that has elapsed since the last restart is shown. After a restart, the time of day begins at 01/01/2000 00:00:00.
- **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 (Page 327) of the configuration manual.

6.3.6 Faults

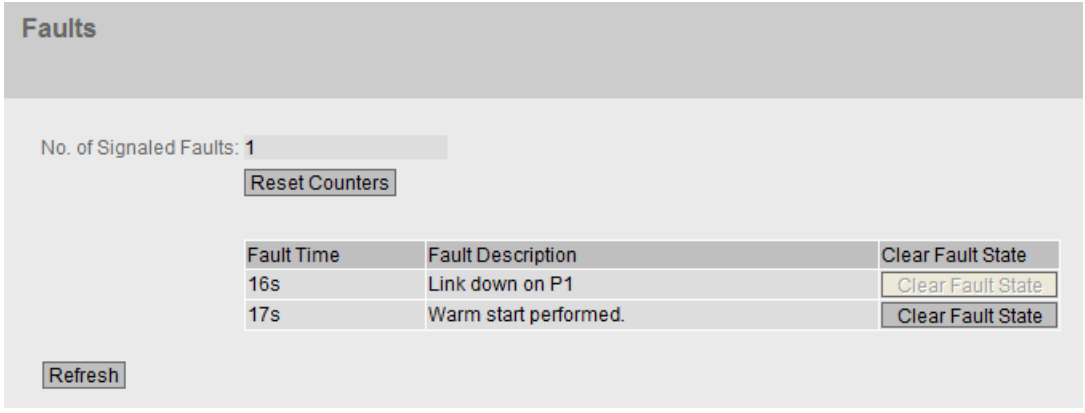
Error status

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

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

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

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



Description

The page contains the following boxes:

- **No. of Signaled Faults**
  Indicates how often the fault LED lit up and not how many faults occurred.

The table contains the following columns:

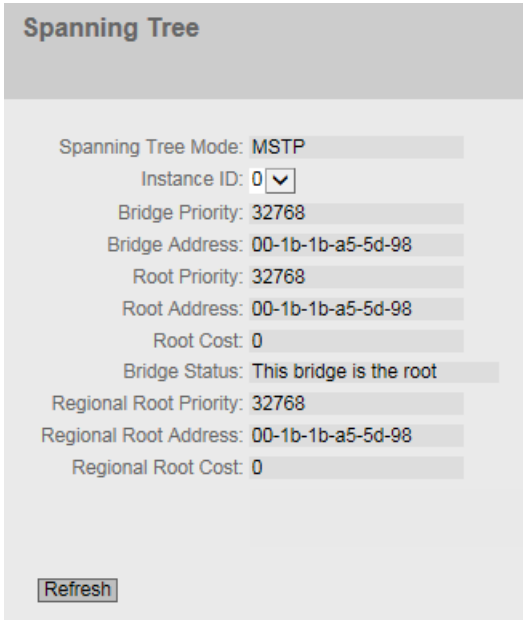
- **Fault Time**
  Shows the time the device has been running since the last restart when the described fault occurred.
- **Fault Description**
  Displays a brief description of the error/fault that has occurred.
- **Clear Fault State**
  Some faults can be acknowledged and thus removed from the fault list, e.g. a fault of the event "Cold/Warm Start". You can acknowledge these faults or remove them from the fault list with the "Clear Fault State" button.

6.3.7 Redundancy

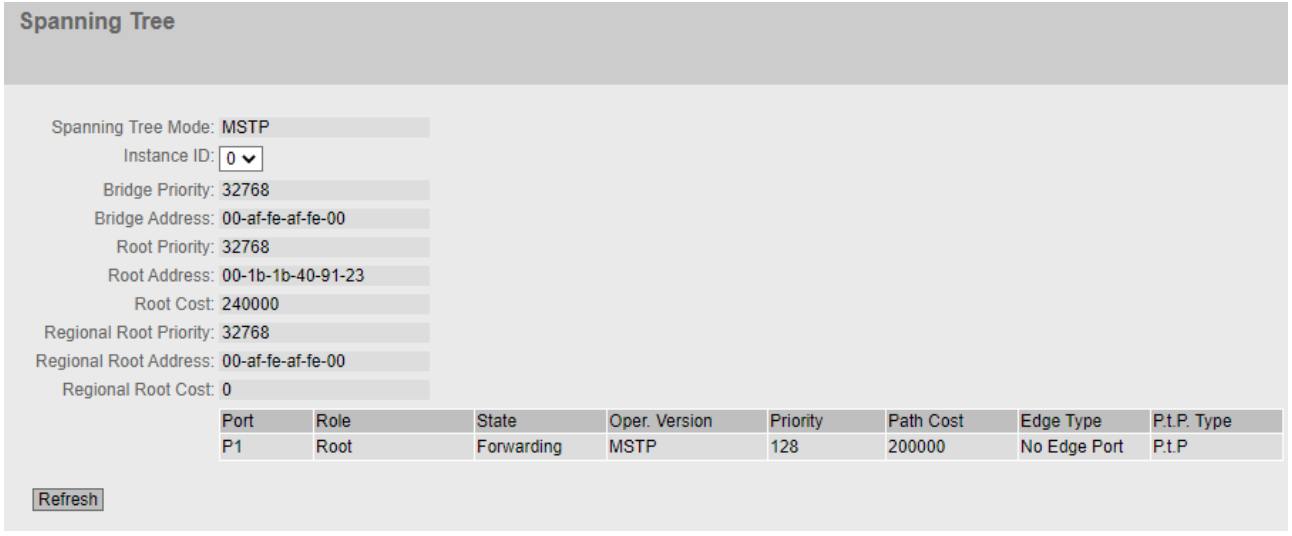
Introduction

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.



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.



Description

The page contains the following boxes:

- **Spanning Tree Mode**
  Shows the set mode. You specify the mode in "Layer 2 > Spanning Tree".
  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 Address / Root Address**
  The bridge address shows the MAC address of the device and the root address shows the MAC address of the root bridge.
- **Root Cost**
  The path costs from this device to the root bridge.
- **Regional root priority** (available only with MSTP)
  For a description, see Bridge priority / Root priority
- **Regional root address** (available only with MSTP)
  Shows the MAC address of the regional root bridge.
- **Regional Root Cost** (available only with MSTP)
  Shows the path costs from this device to the regional 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 port with the most favorable connection to a lower-level LAN segment. When RSTP starts, switches evaluate connections based on BPDUs. The most favorable connections are then used. Generally, all root bridge RSTP ports are Designated Ports because they are set to forwarding. The path costs and the port ID of the respective port determine which ports of the remaining nodes are selected as Designated Ports.
  - Alternate
    The port with an alternative route to a network segment.
  - Backup
    The port on which BPDUs from a port of the same switch that has a better connection to the root are received.
  - 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 state of the port. The values are only displayed. The parameter depends on the configured protocol. The following states 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.
  The calculation of the path costs is based largely 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.

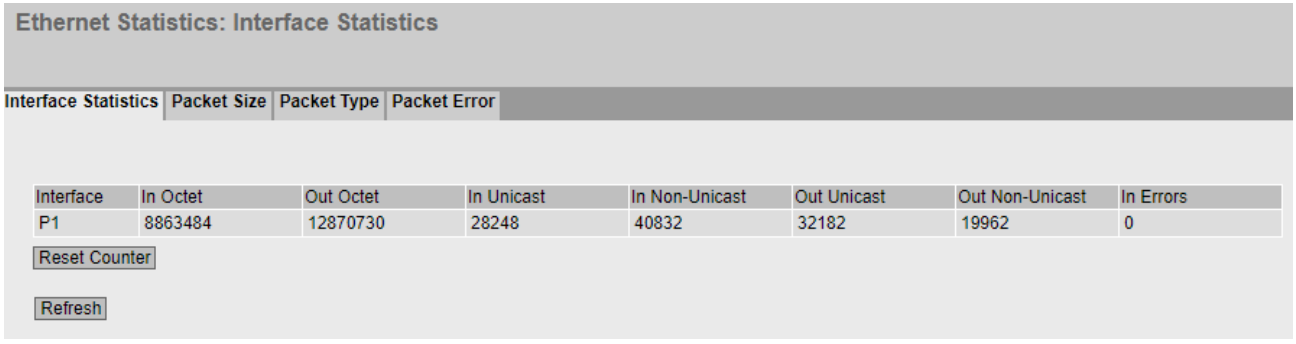
    Note

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

6.3.8 Ethernet Statistics

6.3.8.1 Interface Statistics

The page shows the statistics from the interface table of the Management Information Base (MIB). You cannot configure anything on this page.



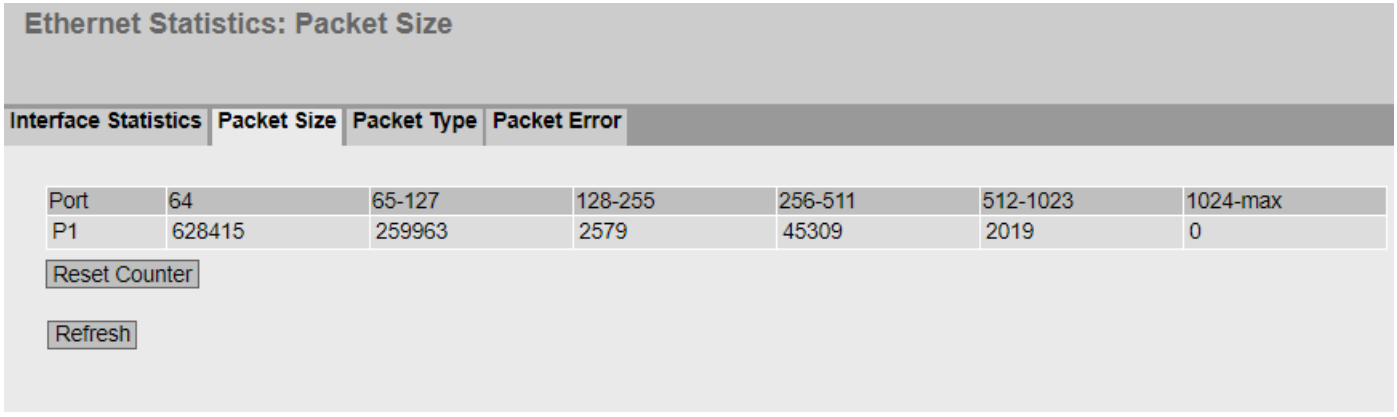
Description

- **Interface**
  Shows the available interfaces.
- **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.

6.3.8.2 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.



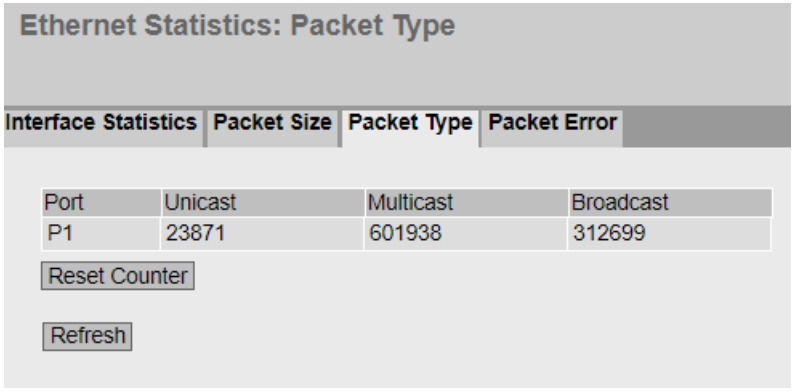
Description

- **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.

6.3.8.3 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.



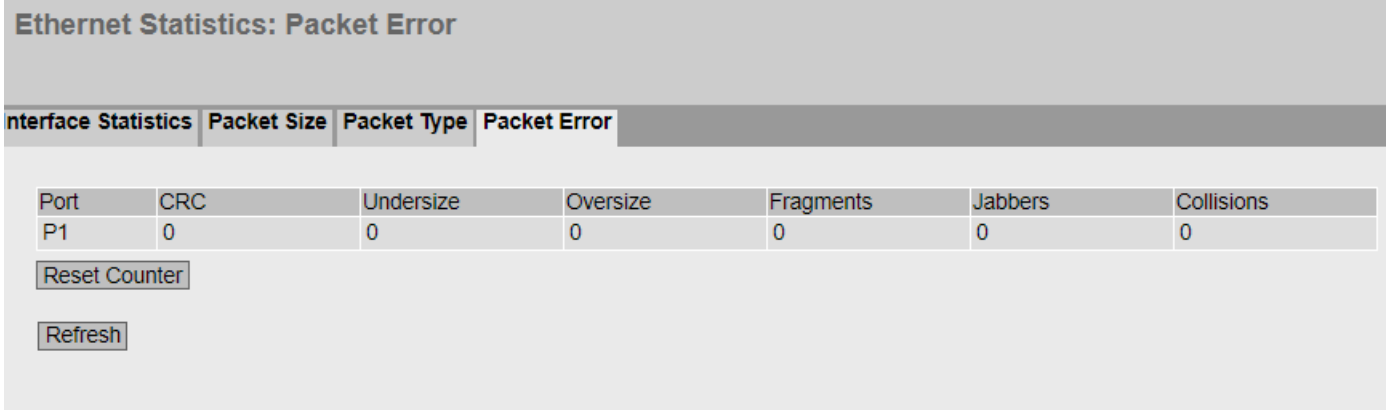
Description

- **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"

6.3.8.4 Packet Error

Received bad frames

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



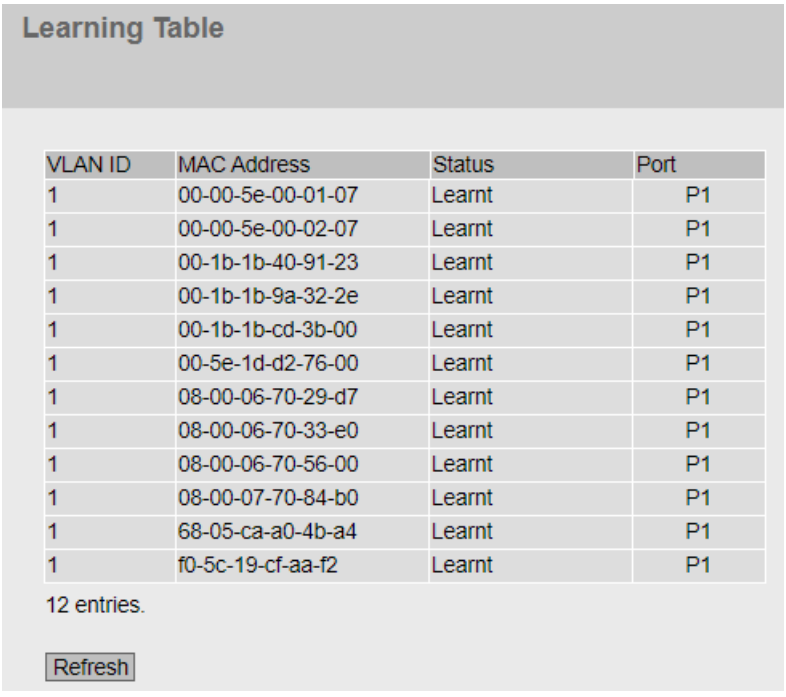
Description

- **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.
  In the columns of the table, a distinction is made according to the following errors:
  - CRC (Cyclic Redundancy Code)
    The packet length is between 64 and 2048 bytes. The CRC of the packet is invalid.
  - Undersize
    The packet length is less than 64 bytes. The CRC of the packet is valid.
  - Oversize
    The packet size is more than 2048 bytes. The CRC of the packet is valid.
  - Fragments
    The packet length is less than 64 bytes. The CRC of the packet is invalid.
  - Jabbers
    The frame length is more than 2048 bytes. The CRC of the packet is invalid.
  - Collisions
    Frames in which a collision event was detected.

6.3.9 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.



Description

The 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.

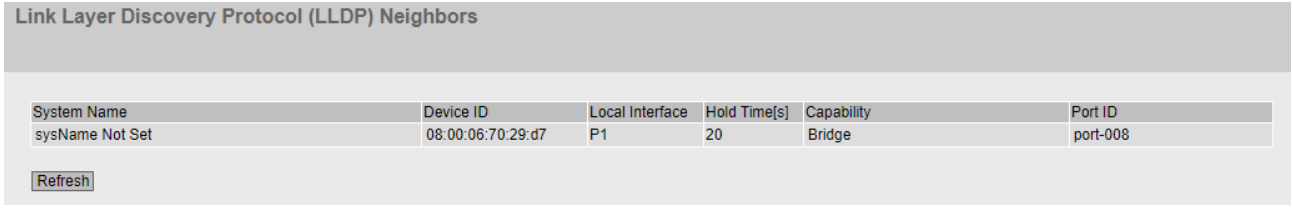
- **State**
  Shows the status of each address entry:
  - Learnt
    The specified address was learned by receiving a frame from this node and will be deleted when the aging time expires if no further packets are received from this node.
  - Invalid
    These values are not evaluated.
- **Port**
  Shows the port via which the node with the specified address can be reached. Frames received by the device whose destination address matches this address will be forwarded to this port.

6.3.10 LLDP

Status of the neighborhood table

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

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



Description

The table contains the following columns:

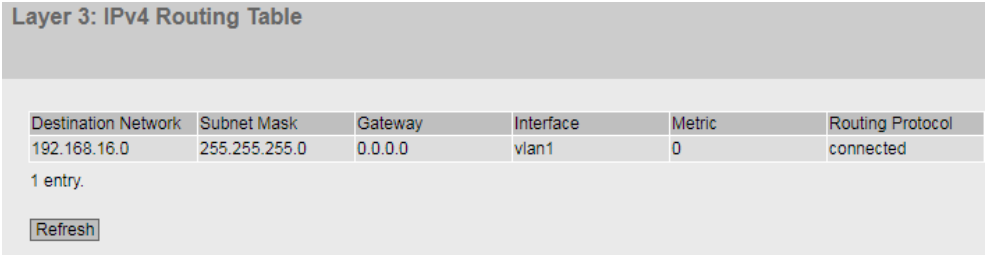
- **System Name**
  System name of the connected device.
- **Device ID**
  Device ID of the connected device. The device ID corresponds to the device name assigned via SINEC PNI (STEP 7). If no device name is assigned, the MAC address of the device is displayed.
- **Local Interface**
  Port at which the device received the information.
- **Hold Time[s]**
  Hold time in seconds
  An entry remains stored on the device for the time specified here. If the device does not receive any new information from the connected device during this time, the entry is deleted.

- **Capability**
  Shows the properties of the connected device:
  - Router
  - Bridge
  - Telephone
  - DOCSIS Cable Device
  - WLAN Access Point
  - Repeater
  - Station
  - Other
- **Port ID**
  Port of the device with which the device is connected. If no port ID is assigned, the MAC address of the connected device is shown.

6.3.11 IPv4 Routing

Introduction

This page shows the routes currently being used.



Description

The table has the following columns:

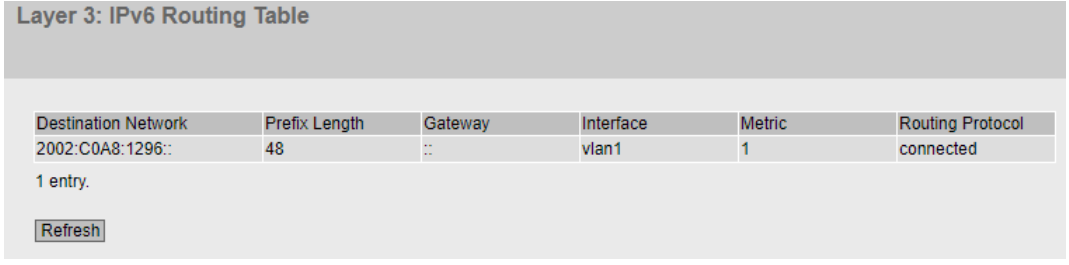
- **Destination Network**
  Shows the destination address of this route.
- **Subnet Mask**
  Shows the subnet mask of this route.
- **Gateway**
  Shows the gateway for this route.
- **Interface**
  Shows the interface for this route.

- **Metric**
  Shows the metric of the route. The higher value, the longer packets require to their destination.
- **Routing Protocol**
  Shows the routing protocol from which the entry in the routing table originates. The following entries are possible:
  - Connected: Connected routes
  - Static: Static routes
  - DHCP: Routes via DHCP

6.3.12 IPv6-Routing

Introduction

This page shows the IPv6 routes currently being used.



Description

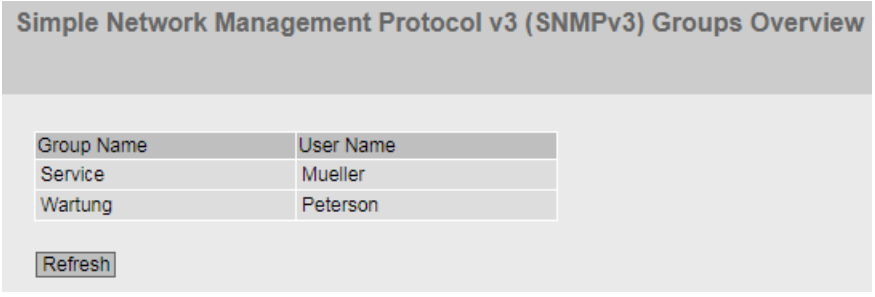
The table has the following columns:

- **Destination Network**
  Shows the destination address of this route.
- **Prefix Length**
  Shows the prefix length of this route.
- **Gateway**
  Shows the gateway for this route.
- **Interface**
  Shows the interface for this route.

- **Metric**
  Shows the metric of the route. The higher value, the longer packets require to their destination.
- **Routing Protocol**
  Shows the routing protocol from which the entry in the routing table originates. The following entries are possible:
  - Connected: Connected routes
  - Static: Static routes
  - RIPng: Routes via RIPng
  - OSPFv3: Routes via OSPFv3
  - Other: Other routes

6.3.13 SNMP

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



Description

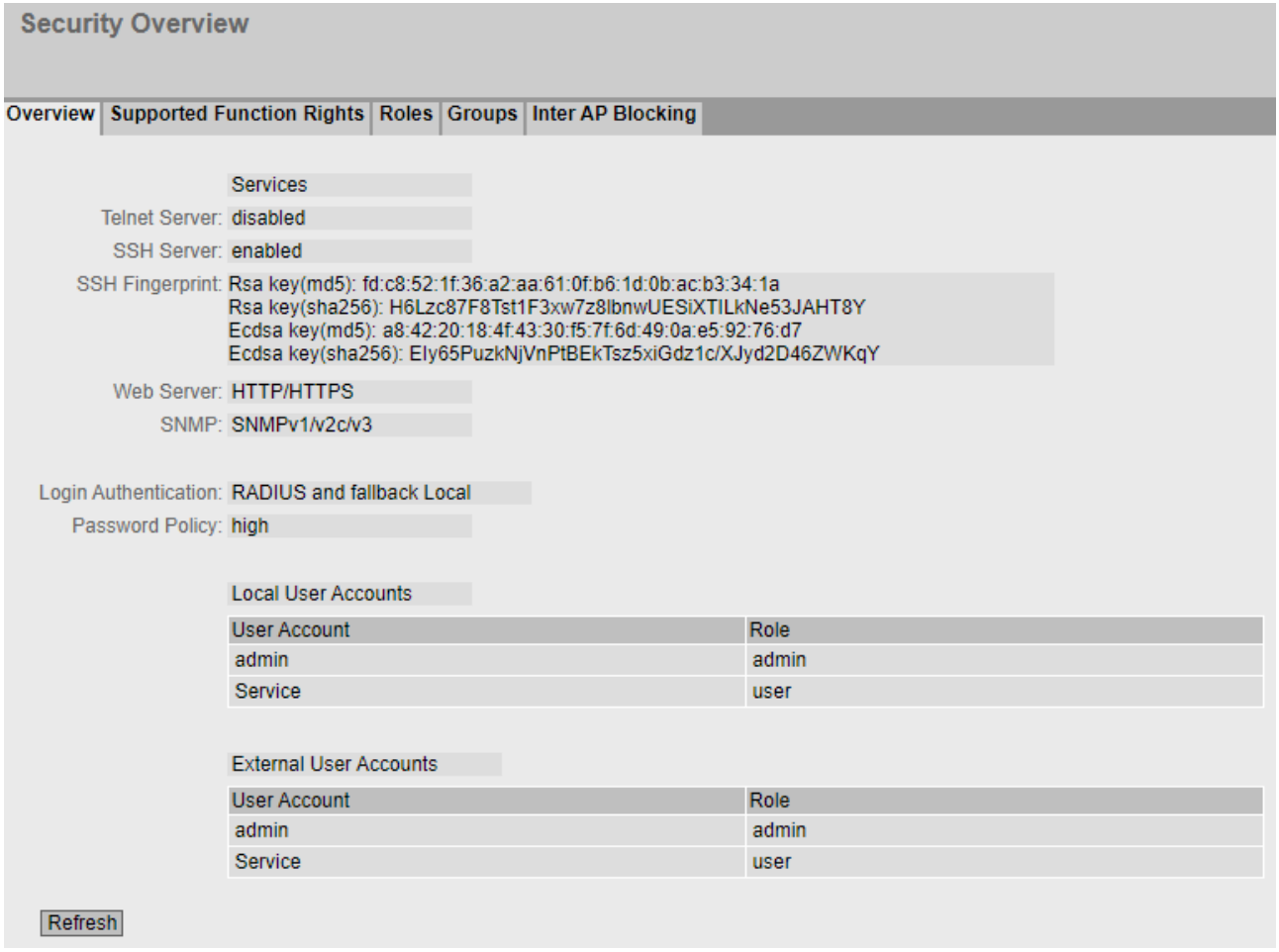
The table has the following columns:

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

6.3.14 Security

6.3.14.1 Overview

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



Description

Services

The "**Services**" list shows the security settings.

- **Telnet Server**
  You configure the setting in "System > Configuration".
  - Enabled: Unencrypted access to the CLI.
  - Disabled: No unencrypted access to the CLI.
- **SSH Server**
  You configure the setting in "System > Configuration".
  - Enabled: Encrypted access to the CLI.
  - Disabled: No encrypted access to the CLI.
- **SSH fingerprint**
  Shows the SSH fingerprint. You can uniquely identify the device with the fingerprints shown.
- **Webserver**
  You configure the setting in "System > Configuration".
  - HTTPS
    Access to the WBM is only possible with HTTPS.
  - HTTP/HTTPS
    Access to the WBM is possible with HTTP and HTTPS.
  - Redirect HTTP to HTTPS
    Access via HTTP is automatically diverted to HTTPS.
- **SNMP**
  You can configure the setting in "System > SNMP > General".
  - "-" (SNMP disabled)
    Access to device parameters via SNMP is not possible.
  - SNMPv1/v2c/v3
    Access to device parameters is possible with SNMP versions 1, 2c or 3.
  - SNMPv3
    Access to device parameters is possible only with SNMP version 3.

- **Login Authentication**
  Configure the setting under "Security > AAA > General".
  - Local
    The authentication must be made locally on the device.
  - RADIUS
    The authentication must be handled via a RADIUS server.
  - Local and RADIUS
    The authentication is possible both with the users that exist on the device (user name and password) and via a RADIUS server.
    The user is first searched for in the local database. If the user does not exist there, a RADIUS request is sent.
  - RADIUS and fallback Local
    The authentication must be handled via a RADIUS server.
    A local authentication is performed only when the RADIUS server cannot be reached in the network.
- **Password Policy**
  Shows which password policy is currently being used.

Local and external user accounts

Configure local user accounts and roles under "Security > Users".

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

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

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

Note

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

With CLI you can access external user accounts.

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

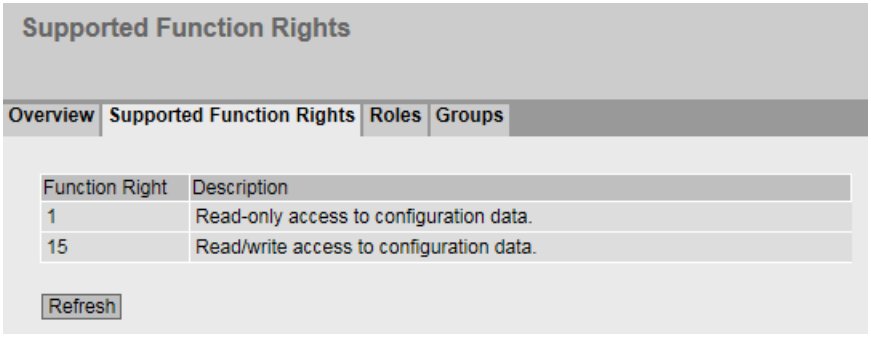
- **User Account**
  Shows the name of the local user.
- **Role**
  Shows the role of the user. You can obtain more information on the function rights of the role in "Information > Security > Roles".

6.3.14.2 Supported Function Rights

Note

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

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



Description of the displayed values

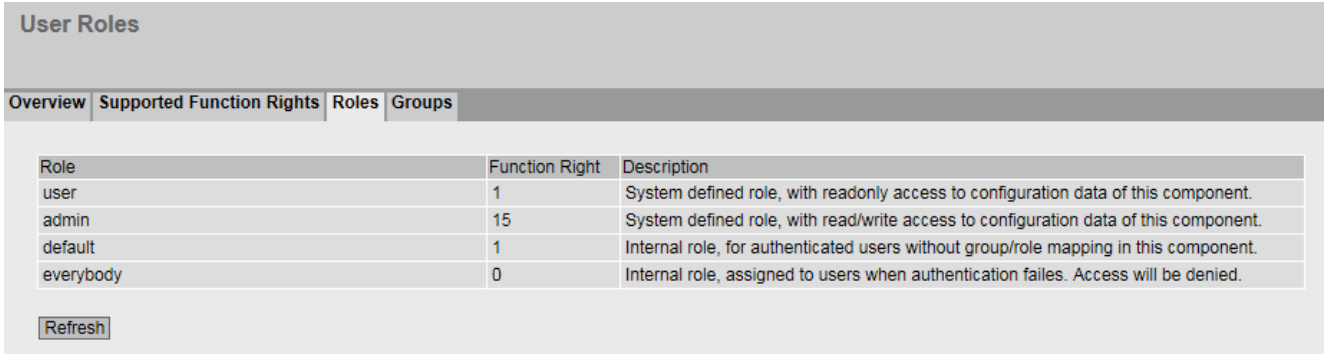
- **Function Right**
  Shows the number of the function right. Different rights relating to the device parameters are assigned to the numbers.
- **Description**
  Shows the description of the function right.

6.3.14.3 Roles

Note

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

The page shows the roles valid locally on the device.



Description

The table contains the following columns:

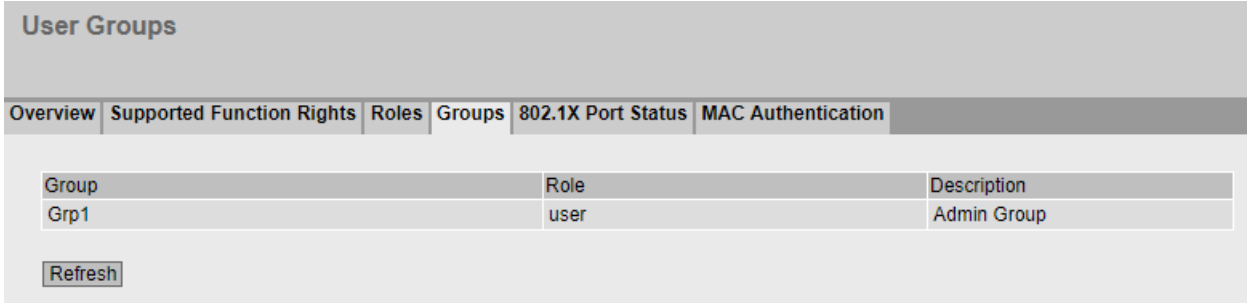
- **Role**
  Shows the name of the role.
- **Function Right**
  Shows the function right of the role:
  - 1
    Users with this role can read device parameters but cannot change them.
  - 15
    Users with this role can both read and change device parameters.
  - 0
    This is a role that the device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

6.3.14.4 Groups

Note

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

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



Description of the displayed values

The table has the following columns:

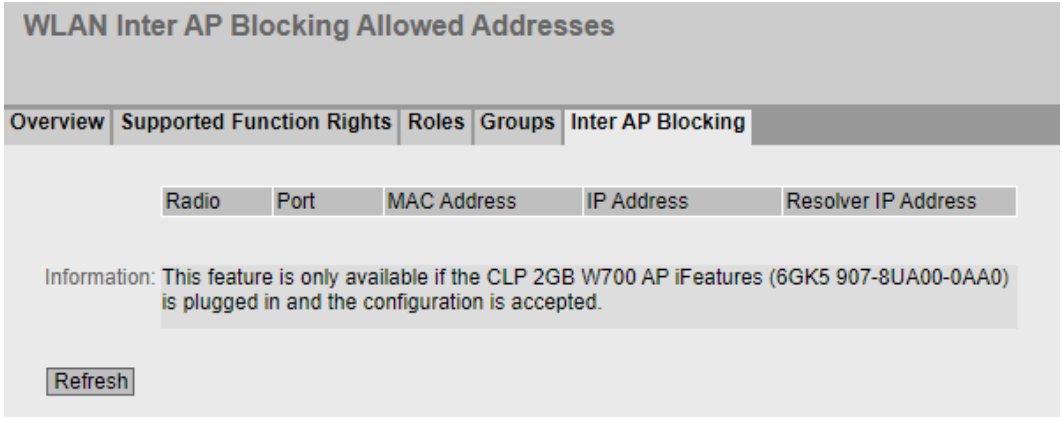
- **Group**
  Shows the name of the group. The name matches the group on the RADIUS server.
- **Role**
  Shows the name of the role. Users who are authenticated with the linked group on the RADIUS server receive the rights of this role locally on the device.
- **Description**
  Shows a description for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

6.3.14.5 Inter AP blocking

Note

This WBM page is only available in access point mode.

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



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 IPv4 address of the device with which the client may communicate.
- **Resolver IP Address**
  Shows the IPv4 address with which the access point resolves the permitted IPv4 address.

6.3.15 WLAN

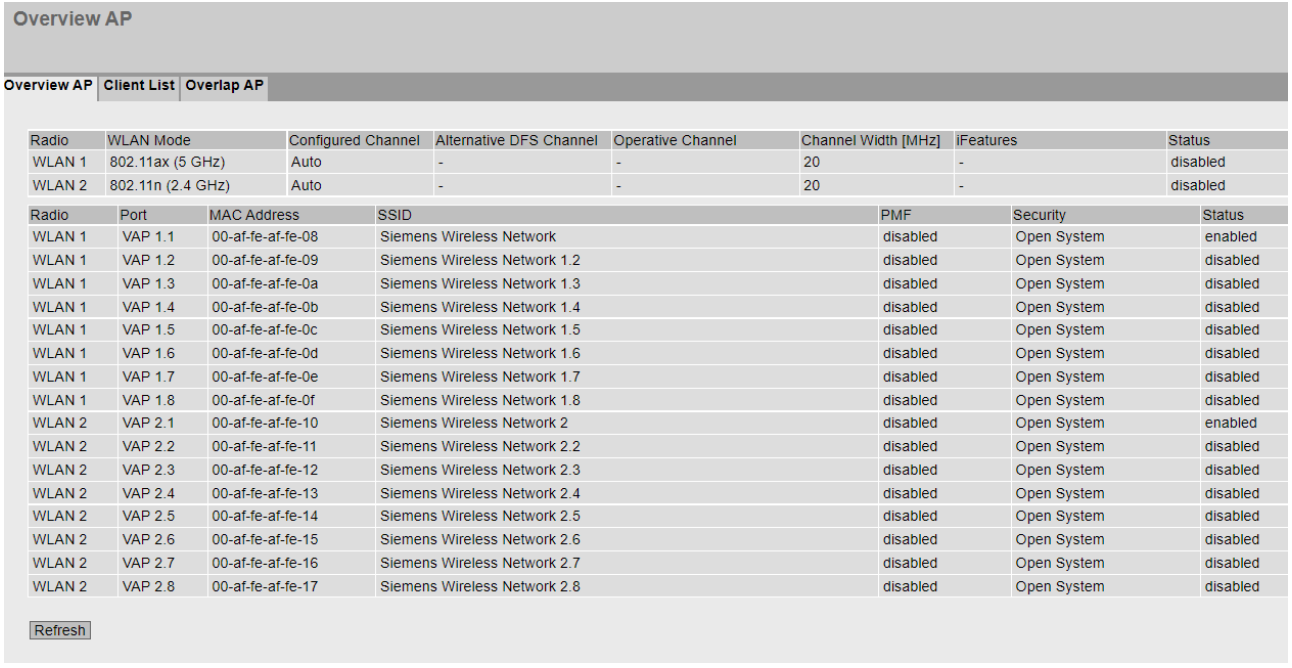
6.3.15.1 Overview AP

Note

This page is available only in access point mode.

Overview of the configuration

This page shows the settings/properties of the access point.



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

Radio	Port	MAC Address	SSID	PMF	Security	Status
WLAN 1	VAP 1.1	00-af-fe-af-fe-08	Siemens Wireless Network	disabled	Open System	enabled
WLAN 1	VAP 1.2	00-af-fe-af-fe-09	Siemens Wireless Network 1.2	disabled	Open System	disabled
WLAN 1	VAP 1.3	00-af-fe-af-fe-0a	Siemens Wireless Network 1.3	disabled	Open System	disabled
WLAN 1	VAP 1.4	00-af-fe-af-fe-0b	Siemens Wireless Network 1.4	disabled	Open System	disabled
WLAN 1	VAP 1.5	00-af-fe-af-fe-0c	Siemens Wireless Network 1.5	disabled	Open System	disabled
WLAN 1	VAP 1.6	00-af-fe-af-fe-0d	Siemens Wireless Network 1.6	disabled	Open System	disabled
WLAN 1	VAP 1.7	00-af-fe-af-fe-0e	Siemens Wireless Network 1.7	disabled	Open System	disabled
WLAN 1	VAP 1.8	00-af-fe-af-fe-0f	Siemens Wireless Network 1.8	disabled	Open System	disabled
WLAN 2	VAP 2.1	00-af-fe-af-fe-10	Siemens Wireless Network 2	disabled	Open System	enabled
WLAN 2	VAP 2.2	00-af-fe-af-fe-11	Siemens Wireless Network 2.2	disabled	Open System	disabled
WLAN 2	VAP 2.3	00-af-fe-af-fe-12	Siemens Wireless Network 2.3	disabled	Open System	disabled
WLAN 2	VAP 2.4	00-af-fe-af-fe-13	Siemens Wireless Network 2.4	disabled	Open System	disabled
WLAN 2	VAP 2.5	00-af-fe-af-fe-14	Siemens Wireless Network 2.5	disabled	Open System	disabled
WLAN 2	VAP 2.6	00-af-fe-af-fe-15	Siemens Wireless Network 2.6	disabled	Open System	disabled
WLAN 2	VAP 2.7	00-af-fe-af-fe-16	Siemens Wireless Network 2.7	disabled	Open System	disabled
WLAN 2	VAP 2.8	00-af-fe-af-fe-17	Siemens Wireless Network 2.8	disabled	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 with the suffix "DFS".
- **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 searches for competing radar signals for 60 seconds before starting communication with the selected channel, the text "scanning ..." is displayed instead of the channel.
- **Operational channel**
  Shows the channel including the frequency via which the access point communicates.
  At 80 MHz the channel range is displayed additionally.
- **Channel Width [MHz]**
  Shows the set channel bandwidth.
  - 20 MHz
  - 40 MHz (only with IEEE 802.11n/ac/ax)
  - 80 MHz (only with IEEE 802.11ac/ax)
- **iFeatures**
  Shows which iFeatures are used.
  - "-"
    iFeatures are not used.
  - iPRP
  - iPCF-2
- **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 (VAP).
- **MAC Address**
  Shows the MAC address of the virtual access point.
- **SSID**
  Shows the SSID.

- **PMF**
  Shows whether the management frames are cryptographically protected.
  - disabled
    The management frames are not encrypted.
  - required
    The management frames are always encrypted. A connection of the WLAN clients to the access point is only possible when these also support PMF.
  - optional
    The management frames are encrypted or unencrypted depending on support of the WLAN client.
- **Security**
  Shows which authentication method is used.
  If the authentication method "Open System + Encryption" or "Shared Key" is used, the "Encrypted (WEP/AES)" authentication method is displayed for both.
  If the access point is connected to a client that supports Fast BSS Transition, "FT" is displayed in addition to the authentication method.
- **Status**
  Shows the status of the WLAN interface.
  - enabled
    The WLAN interface is enabled.
  - disabled
    The WLAN interface is disabled.

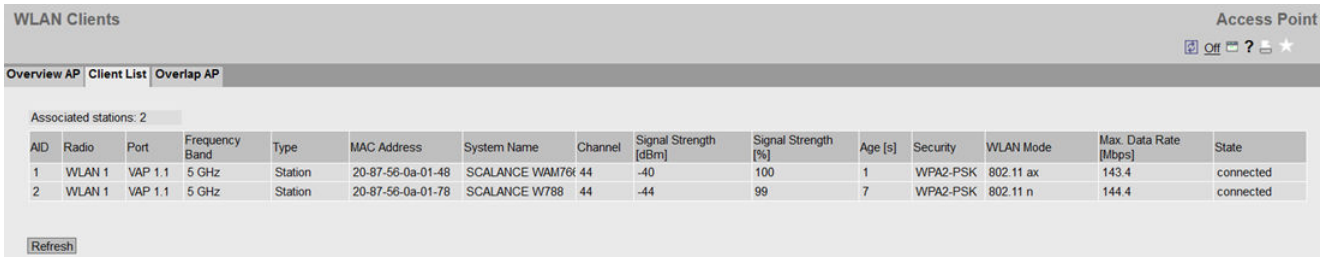
6.3.15.2 Client List

Note

This WBM page is only available in access point mode.

Associated stations

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



Description

- **Associated stations**
  Shows the number of clients logged in 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 in at different VAP interfaces, both clients can receive the same ID.
- **Radio**
  Shows the available WLAN interfaces.
- **Port**
  Shows the VAP interface.
- **Frequency Band**
  Shows the frequency band.
  - 2.4 GHz
  - 5 GHz
- **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 decibel milliwatts.
- **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.
- **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. e.g. "802.11a".
- **Max. Data Rate (Mbps)**
  Shows the maximum data transmission speed in megabits per second.
- **State**
  Shows the current state of the connection, for example "connected" that means the client is connected to the access point and is ready to communicate with the AP.

6.3.15.3 Overlap AP

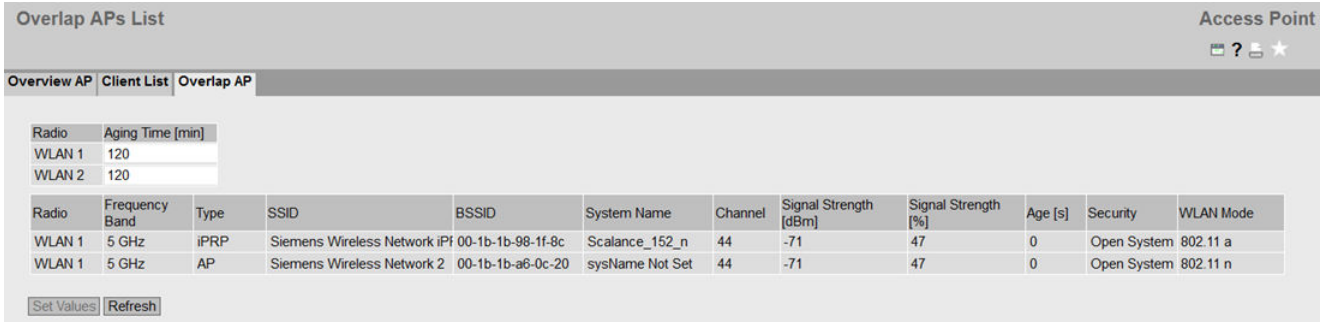
Note

This page is available only in access point mode.

Overlapping channels

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, 802.11g or 802.11n), the channels overlap, so that an access point not only occupies the configured channel, but also the neighboring 2-3 channels. You should therefore make sure that there is adequate channel spacing to neighboring access points.

The WBM page shows all access points that are visible on the set channel at 2.4 GHz or at 5 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.



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.

Table 2 has the following columns:

- **Radio**
  Shows the available WLAN interfaces in this column.
- **Frequency Band**
  Shows the frequency band.
  - 2.4 GHz
  - 5 GHz
- **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**
  Shows the system name of the SCALANCE W device. The entry depends on the access point. Not all access points support this parameter.
- **Channel**
  Indicates the channel over which the access point is communicating.
- **Signal Strength [dBm]**
  Shows the signal strength of the access point in decibel milliwatts.
- **Signal strength [%]**
  Shows the signal strength of the access point as a percentage.
- **Age [s]**
  Shows the time that has elapsed since the last access point activity.
- **Security**
  Shows which authentication method is used.
- **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 with the suffix "DFS".

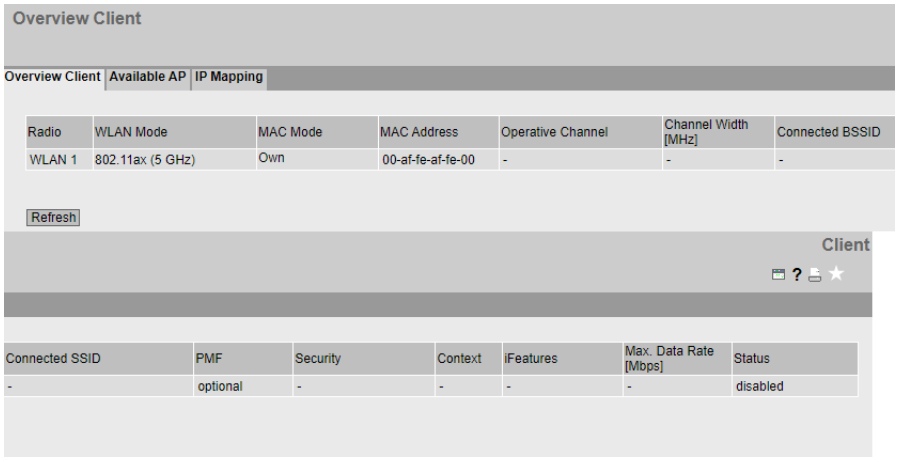
6.3.15.4 Overview Client

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.



Description

- **Radio**
  Shows the available WLAN interfaces.
- **WLAN Mode**
  Shows the transmission standard.
- **MAC Mode**
  Shows how the MAC address is assigned to the interface.
  - 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**
  Shows the MAC address of the WLAN interface.
- **Operational channel**
  Shows the channel including frequency of the access point to which the client is connected.
- **Channel Width [MHz]**
  Shows the set channel bandwidth.
  - 20 MHz
  - 40 MHz (only with IEEE 802.11n/ac/ax)
  - 80 MHz (only with IEEE 802.11ac/ax)
- **Connected BSSID**
  Shows the MAC address of the access point to which the client is connected.
- **Connected SSID**
  Shows the SSID of the access point to which the client is connected.

- **PMF**
  Shows whether the management frames are cryptographically protected.
  - disabled
    The management frames are not encrypted.
  - required
    The management frames are always encrypted. A connection of the WLAN clients to the access point is only possible when these also support PMF.
  - optional
    The management frames are encrypted or unencrypted depending on support of the access point.
- **Security**
  Shows which authentication method is used.
  If the client is connected to an access point that supports Fast BSS Transition, "FT" is displayed in addition to the authentication method.
- **Context**
  Shows which security context is used.
- **iFeatures**
  Shows which iFeatures are used.
  - "-"
    iFeatures are not used.
  - iPRP
- **Max. Data Rate [Mbps]**
  Shows the maximum data transmission speed in megabits per second.
- **Status**
  Shows the status of the WLAN interface.
  - enabled
    The WLAN interface is enabled.
  - disabled
    The WLAN interface is disabled.

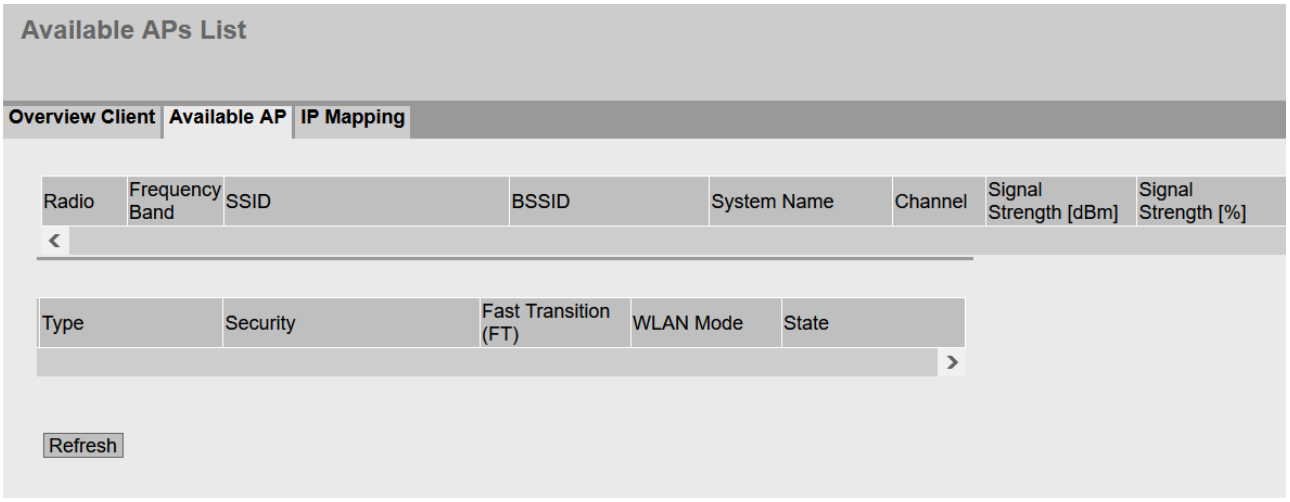
6.3.15.5 Available APs

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.



Description

The table has the following columns:

- **Radio**
  Shows the WLAN interface visible to the access point.
- **Frequency Band**
  Shows the frequency band.
  - 2.4 GHz
  - 5 GHz
- **SSID**
  Shows the SSID of the access point.
- **BSSID**
  Shows the MAC address of the access point.
- **System Name**
  Shows the system name of the 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.

- **Fast transition (FT)**
  Shows whether the access point supports Fast BSS Transition:
  - "-"
    FT is not supported or is not available.
  - Over the Air
    FT available wirelessly in access point. The client communicates with the destination access point directly and wirelessly.
- **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, for example "802.11n".
- **State**
  Shows the status of the access point, for example whether or not the access point is available.

6.3.15.6 IP Mapping

WLAN access for several SCALANCE W devices via one client

Note

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

You can make WLAN access available for several SCALANCE W devices with one client if you use IP mapping. This means that you do not need to equip every SCALANCE W device with its own WLAN client. The prerequisite for this is that the connected SCALANCE W devices are addressed only with 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.

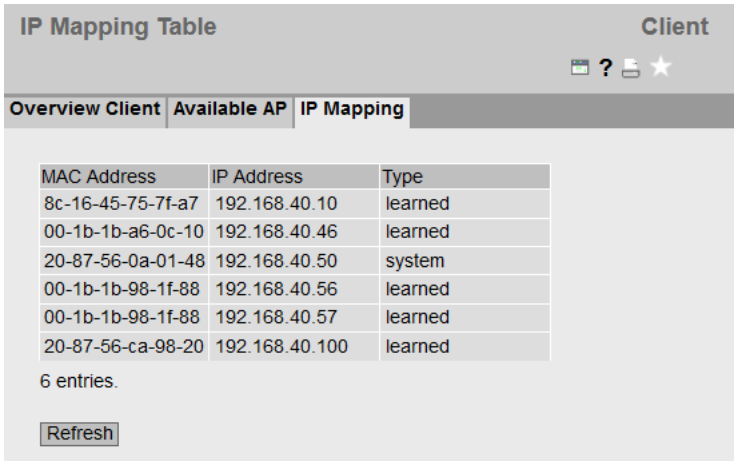
The "Layer 2 Tunnel" setting meets the requirements of industrial applications in which MAC address-based communication takes place with several SCALANCE W devices downstream from the client. Clients with this setting cannot connect on standard Wifi access points.

The client maintains a table with the assignment of MAC address and IP address to send incoming IP frames to the correct MAC address. This WBM page shows this table.

Note

IP mapping table

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



Description

The table has the following columns

- **MAC Address**
  The MAC address of a 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

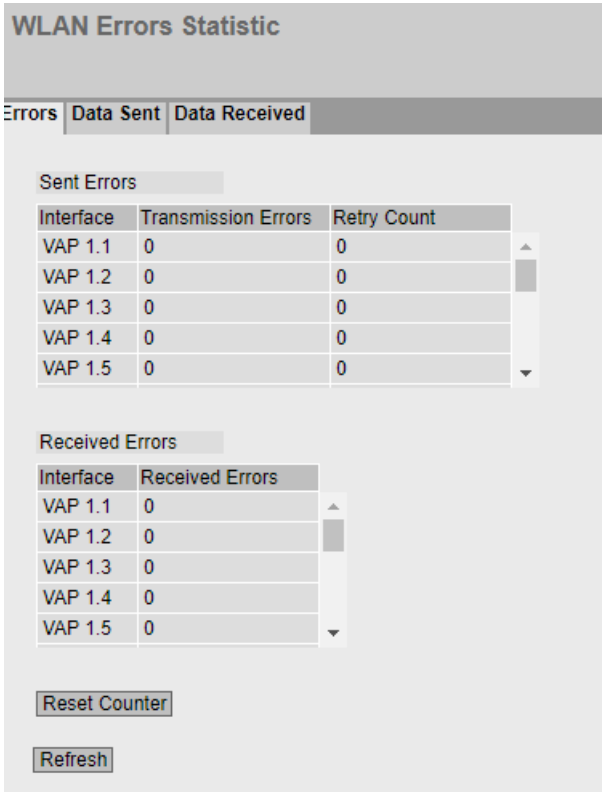
Frames sent by the client to the access point always have the MAC address of the WLAN client as the source MAC address. In the "learning table" of the access point there is therefore only the MAC address of the WLAN client.

If there is only IP communication between the access point and the client, the default setting "Own" can be retained. If MAC address-based frames are also to be sent by SCALANCE W700 devices downstream from the client, you need to select the "Layer 2 Tunnel" setting.

6.3.16 WLAN Statistics

6.3.16.1 Errors

The page shows how many bad data frames were received or sent per WLAN interface in the client or per VAP in the access point. If an increased number of errors occurs, you should check the settings for the WLAN interface(s), the setup of the SCALANCE W devices and the connection quality.



Description

The Sent Errors table has the following columns:

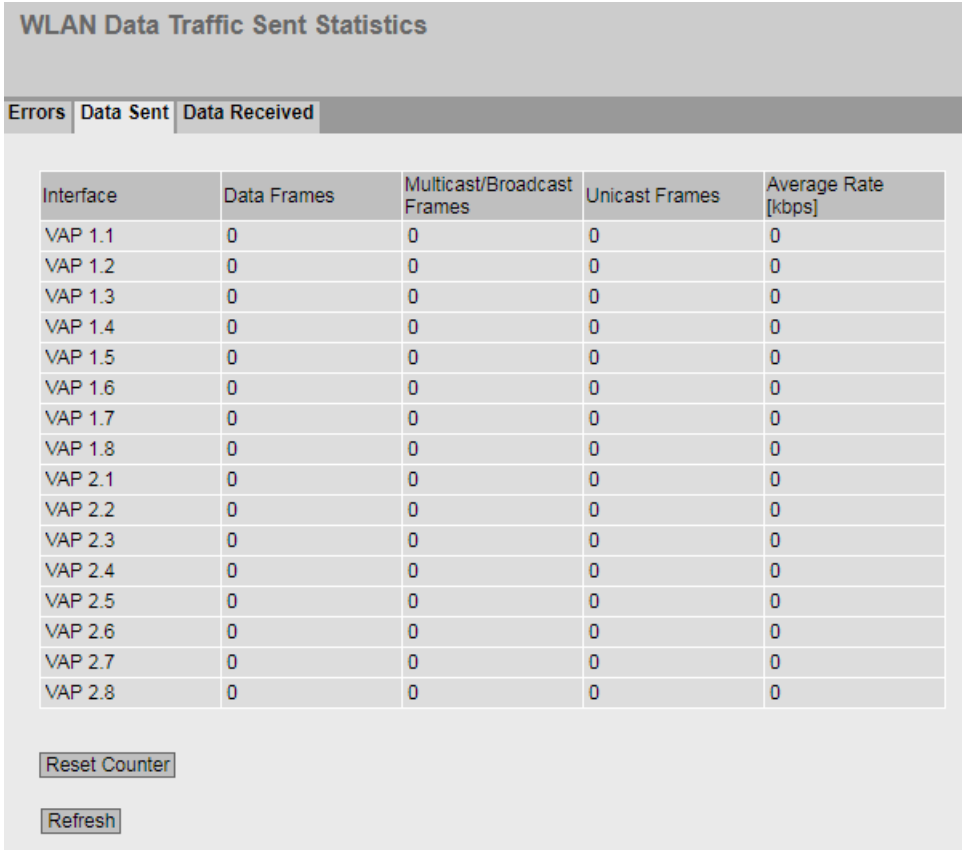
- **Interface**
  Shows the interface to which the entries apply.
- **Error types**
  The other columns after the WLAN interface contain the absolute numbers of the data frames sent according to their error type.
  The columns of the table distinguish between the following error types:
  - Transmission Errors
    Shows the number and percentage of bad data frames that were sent.
  - Retry Count
    Shows the number and percentage of data frames sent successfully that required one or more retries.

The Received Errors table has the following columns:

- **Interface**
  Shows the WLAN interface to which the entries apply.
- **Received Errors**
  Shows the number and percentage of bad data frames that were received.

6.3.16.2 Data Sent

The page shows how many frames were sent per interface.



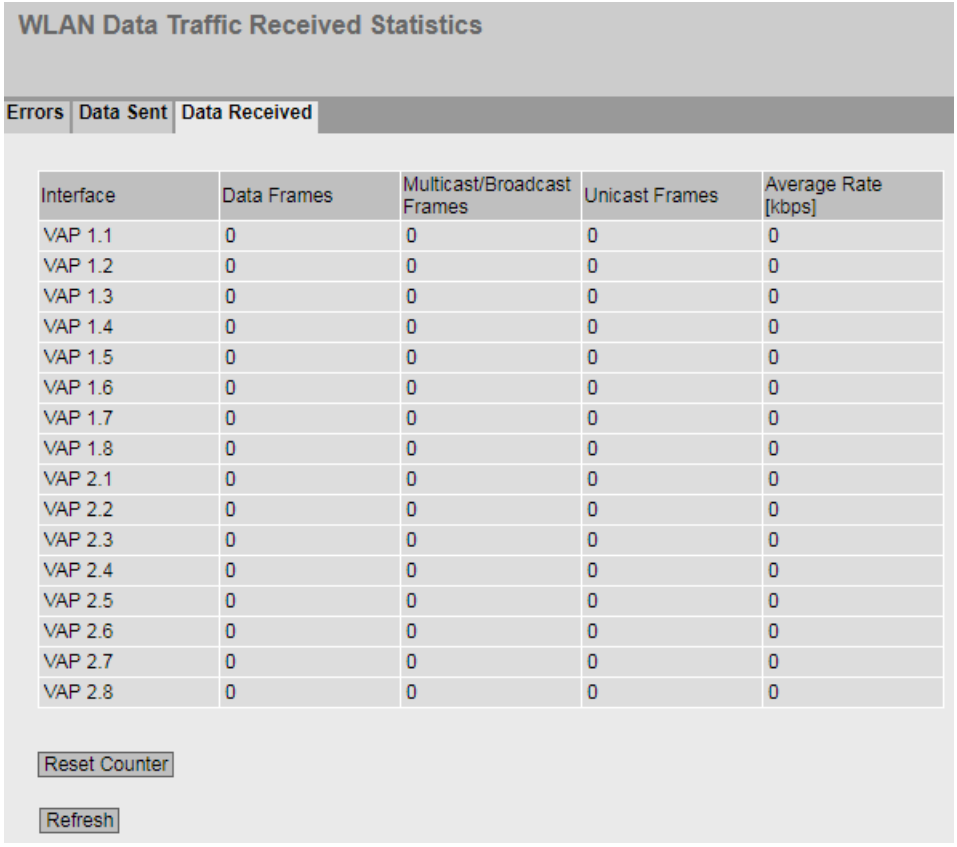
Description

The table has the following columns:

- **Interface**
  Shows the interface to which the entries apply.
- **Frame types**
  The other columns after the 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 [kbps]
    Shows the average data rate of the last data frames sent.

6.3.16.3 Data Received

The page shows how many frames were received per interface.



Description

The table has the following columns:

- **Interface**
  Shows the interface to which the entries apply.
- **Frame types**
  The other columns after the 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
    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 [kbps]
    Shows the average data rate of the last data frames sent.

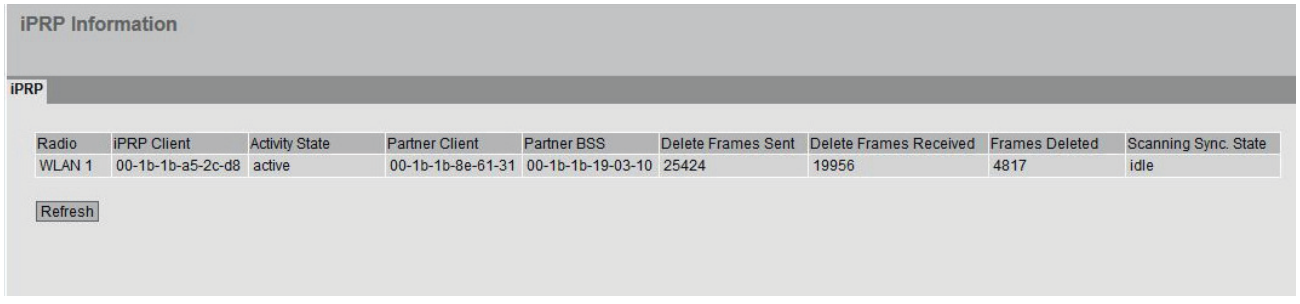
6.3.17 WLAN iFeatures

6.3.17.1 iPRP

On this WBM page you can check whether the settings for iPRP are correct. For example, you can see which device is the partner client.

Display in access point mode

Display in client mode



Description

The table has the following columns:

- **Radio**
  Shows the WLAN interfaces via which the client is connected to the access point.
- **Port** (only in access point mode)
  Shows the VAP interface on which the iPRP clients are logged in. The column is hidden when the table is empty.
- **iPRP Client**
  Shows the MAC address of the iPRP client.
- **Activity State**
  Shows whether or not iPRP is enabled.
- **Partner Client**
  Shows the MAC address of the partner client.
- **Partner BSS**
  Shows the MAC address of the access point to which the partner client is connected.
- **Delete Frames Sent**
  Shows the number of sent iPRP delete frames that the device has sent to its partner device.
- **Delete Frames Received**
  Shows the number of iPRP delete frames that the device has received from its partner device.
- **Frames Deleted**
  Shows the number of frames not yet sent that were deleted from the queue due to the iPRP delete frame.
- **Scanning Sync State** (in client mode only)
  So that both clients do not search for an access point and change to the scan mode at the same time, they synchronize with each other.
  Synchronization can have the following statuses:
  - idle: Idle. No scanning.
  - requested: Query to the partner client whether scanning is possible.
  - pending: Scanning is possible. Waits until scanning starts and then changes to the status "foreground" or "background".
  - background: Background scan is performed.
  - foreground: The client has, for example, just started up and is running a foreground scan.

Note

The display has no function. SCALANCE W700 IEEE 802.11ax firmware does not support scanning sync.

6.4 "System" menu

6.4.1 Configuration

System configuration

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

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

The standard port can also be changed for your own services.

Note

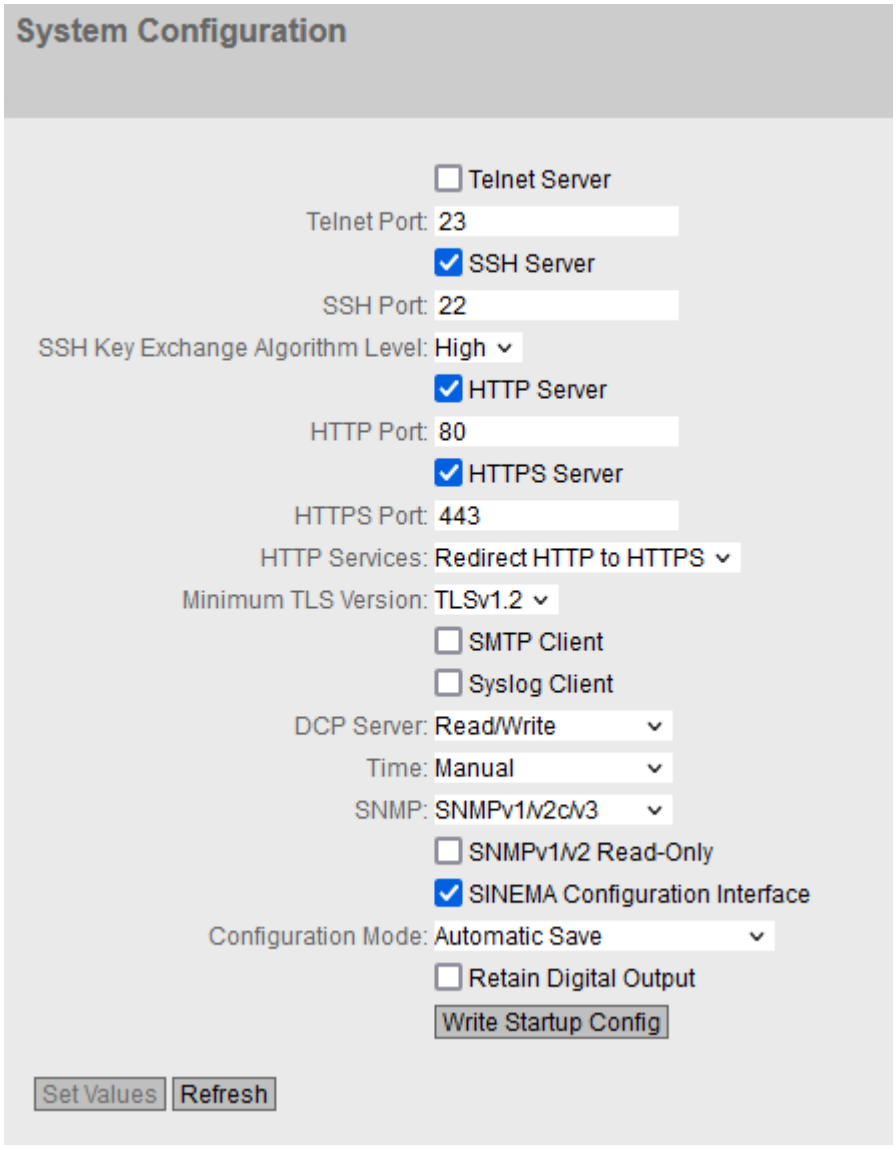
Change standard port

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

When you change the standard port, you must access the service using the changed port.

Reserved ports

Some ports are permanently reserved. Make sure that the specified port is not already in use. You can find the ports used in the "List of available services".



Description

The page contains the following boxes:

- **Telnet Server**
  Enable or disable the "Telnet Server" service for unencrypted access to the CLI.
- **Telnet port**
  Standard port 23 is the default. You can optionally enter a port number in the range 1024 ... 49151 or 49500 ... 65535.
- **SSH Server**
  Enable or disable the "SSH Server" service for encrypted access to the CLI.
- **SSH port**
  Standard port 22 is the default. You can optionally enter a port number in the range 1024 ... 49151 or 49500 ... 65535.

- **SSH key exchange algorithm level**
  From the drop-down list, select the level of the SSH key exchange algorithm for SSH access to the CLI. The settings options are "Low" and "High". The two levels contain the following encryption algorithms:

  – High
  Curve25519-sha256
  Curve25519-sha256@libssh.org
  Ecdh-sha2-nistp256
  Ecdh-sha2-nistp384
  Ecdh-sha2-nistp521

  Note

  If you experience problems connecting to SSH clients (TeraTerm, PuTTY, STS) when the level is set to "High", a possible cause is that the SSH clients do not support the exchange algorithms of the "High" setting.

  Make sure that you are using the latest versions of the SSH clients.

  – Low
  Curve25519-sha256
  Curve25519-sha256@libssh.org
  Ecdh-sha2-nistp256
  Ecdh-sha2-nistp384
  Ecdh-sha2-nistp521
  Diffie-hellman-group16-sha512
  Diffie-hellman-group18-sha512
  Diffie-hellman-group14-sha256
  Diffie-hellman-group14-sha1

  With the "Low" setting, you cannot set up a connection to the following SSH clients because these programs do not support the respective algorigthms:

  – TeraTerm
  – PuTTY
  – STS

- **HTTP server**
  Enable or disable the "HTTP Server" service for unencrypted access to the WBM.
- **HTTP port**
  Standard port 80 is the default. You can optionally enter a port number in the range 1024 ... 49151 or 49500 ... 65535.
- **HTTPS server**
  Enable or disable the HTTPS server service for encrypted access to the WBM.
- **HTTPS port**
  Standard port 443 is the default. You can optionally enter a port number in the range 1024 ... 49151 or 49500 ... 65535.

- **HTTP Services**
  Specify how the WBM is accessed:
  - HTTPS
    Access to the WBM is only possible with HTTPS.
  - HTTP/HTTPS
    Access to the WBM is possible with HTTP and HTTPS.
  - Redirect HTTP to HTTPS
    Access via HTTP is automatically diverted to HTTPS.
- **Minimum TLS Version**
  Select the minimum TLS version to be used for the encryption from the drop-down list. Communication is not possible with devices that do not support the required TLS version.
- **SMTP Client**
  Enable or disable the SMTP client. You can configure other settings in "System > SMTP Client".
- **Syslog Client**
  Enable or disable the Syslog client. You can configure other settings in "System > Syslog Client".
- **DCP Server**
  Specify whether or not the device can be accessed with DCP (Discovery and Configuration Protocol):
  - "-" (disabled)
    DCP is disabled. Device parameters can neither be read nor modified.
  - Read/Write
    With DCP, device parameters can be both read and modified.
  - Read Only
    With DCP, device parameters can be read but cannot be modified.

- **Time**
  Select the setting from the drop-down list. The following settings are possible:
  - Manual
    The system time is set manually. You can configure other settings in "System > System Time > Manual Setting".
  - SIMATIC Time
    The system time is set using a SIMATIC time transmitter. You can configure other settings in "System > System Time > SIMATIC Time Client".
  - SNTP Client
    The system time is set via an SNTP server. You can configure other settings in "System > System Time > SNTP Client".
  - NTP Client
    The system time is set via an NTP server. You can configure other settings in "System > System Time > NTP Client".
- **SNMP**
  Select the protocol from the drop-down list. The following settings are possible:
  - "-" (SNMP disabled)
    Access to device parameters via SNMP is not possible.
  - SNMPv1/v2c/v3
    Access to device parameters is possible with SNMP versions 1, 2c or 3. You can configure other settings in "System > SNMP > General".
  - SNMPv3
    Access to device parameters is possible only with SNMP version 3. You can configure other settings in "System > SNMP > General".
- **SNMPv1/v2 Read-Only**
  Enable or disable write access to SNMP variables with SNMPv1/v2c.
- **SINEMA Configuration Interface**
  If the SINEMA configuration interface is enabled, you can download configurations to the device via the TIA Portal.

- **Configuration Mode**
  Select the mode from the drop-down list. The following modes are possible:
  - Automatic Save
    Automatic backup mode. Approximately 1 minute after the last parameter change or when you restart the device, the configuration is automatically saved. In addition to this, the following message appears in the display area "Changes will be saved automatically in x seconds. Press 'Write Startup Config' to save the changes immediately."

    Note

    Interrupting the save

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

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

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

  - Trial
    Trial mode. In Trial mode, although changes are adopted, they are not saved in the configuration file (startup configuration).
    To save changes in the configuration file, use the "Write startup config" button. The display area also shows the message "Trial Mode Active – Press "Write Startup Config" button to make your settings persistent" as soon as there are unsaved modifications. This message can be seen on every WBM page until the changes made have either been saved or the device has been restarted.
- **Retain Digital Output** (only for device variants with DI/DO)
  When the option is enabled, the current state of the digital output is saved in the configuration and restored after a restart.
  Default value: Disabled.

Procedure

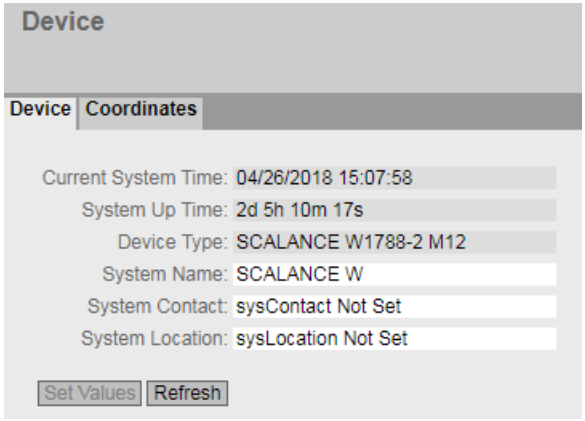
1. To use the required function, select the respective check box.
2. Select the options you require from the drop-down lists.
3. Click the "Set Values" button.

6.4.2 General

6.4.2.1 Device

General device information

This page contains the general device information.



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 operating time of the device since the last restart. (readonly)
- **Device Type**
  Shows the type designation of the device. (readonly)
- **System Name**
  You can enter the name of the device. The entered name is displayed in the selection area. A maximum of 255 characters are possible.
  The system name is also displayed in the CLI input prompt. The number of characters in the CLI input prompt is limited. The system name is truncated after 16 characters.
- **System Contact**
  You can enter the name of a contact person responsible for managing the device. A maximum of 255 characters are possible.
- **System Location**
  You can enter the location where the device is installed. The entered installation location is displayed in the selection area. A maximum of 255 characters are possible.

Note

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

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.

6.4.2.2 Coordinates

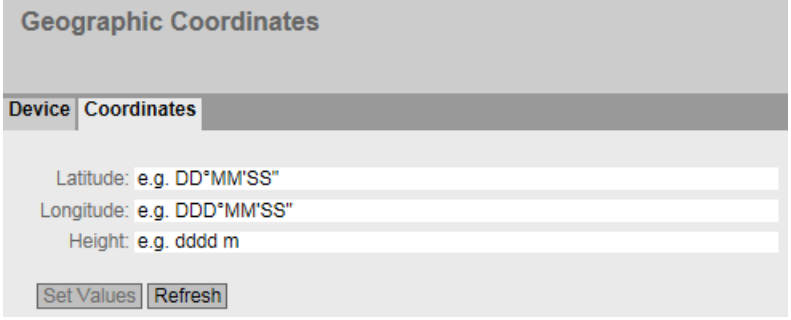
Information on geographic coordinates

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

Getting the coordinates

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

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



Description

The page contains the following input boxes with a maximum length of 32 characters.

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

Procedure

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

6.4.3 Agent IPv4 / IPv6

The calls refer to the following menu items:

- Agent IPv4: Layer 3 (IPv4) > Subnets
- Agent IPv6: Layer 3 (IPv6) > Subnets

6.4.4 DNS

6.4.4.1 DNS Client

The DNS (Domain Name System) server assigns a unique IP address to a domain name so that a device can be uniquely identified.

You can manually configure up to three DNS servers with IPv4 addresses on this page. Using DHCP, the device can learn two DNS servers with IP addresses.

If there is more than one DNS server, the order in the table specifies the order in which the servers are queried. The top server is queried first. A total of two DNS servers can be configured on the device. Manually configured DNS servers are given preference.

If this function is enabled, the device can communicate with a DNS server as a DNS client. You have the option of entering names in IP address boxes.

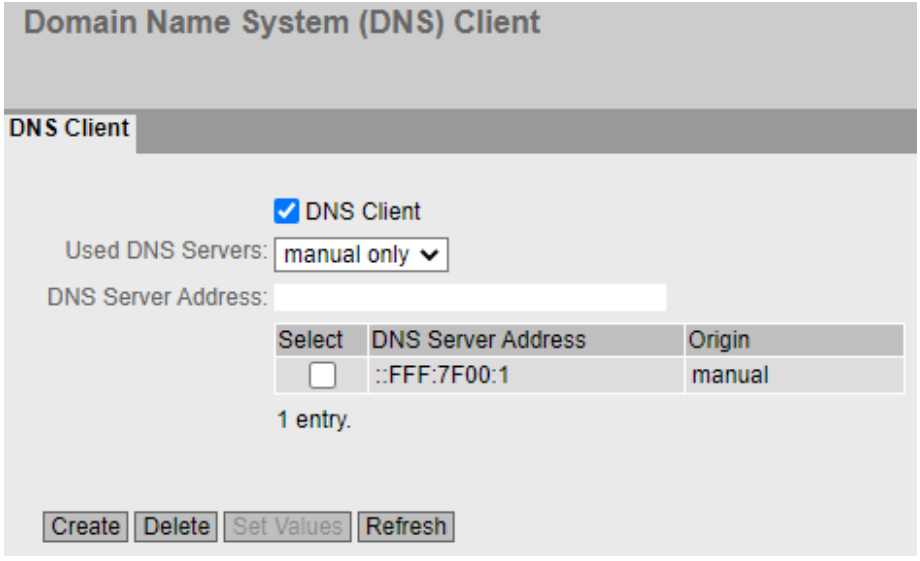
Note

Update from V1.0 to V1.1

The configuration of the DNS client is not transfered with an update from V1.0 to V1.1.

Note

The DNS client function can only be used if there is a DNS server in the network.



Description

The page contains the following boxes:

- **DNS Client**
  Select or clear the check box indicating that the device operates as a DNS client.
- **Used DNS Servers**
  Here you specify which DNS server the device uses:
  - learned only
    The device uses only the DNS servers assigned by DHCP.
  - manual only
    The device uses only the manually configured DNS servers. The DNS servers must be connected to the Internet. A maximum of two DNS servers can be configured.
  - all
    The device uses all available DNS servers.
- **DNS Server Address**
  Enter the IP address of the DNS server.

The table contains the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **DNS Server Address**
  Shows the IP address of the DNS server.
- **Origin**
  This shows whether the DNS server was configured manually or was assigned by DHCP.

Procedure

Activating DNS

1. Enable the "DNS-Client" check box.
2. Click the "Set Values" button.

Creating a DNS server

1. In the "DNS Server Address" box, enter the IP address of the DNS server.
2. Click the "Create" button.

Filtering DNS servers

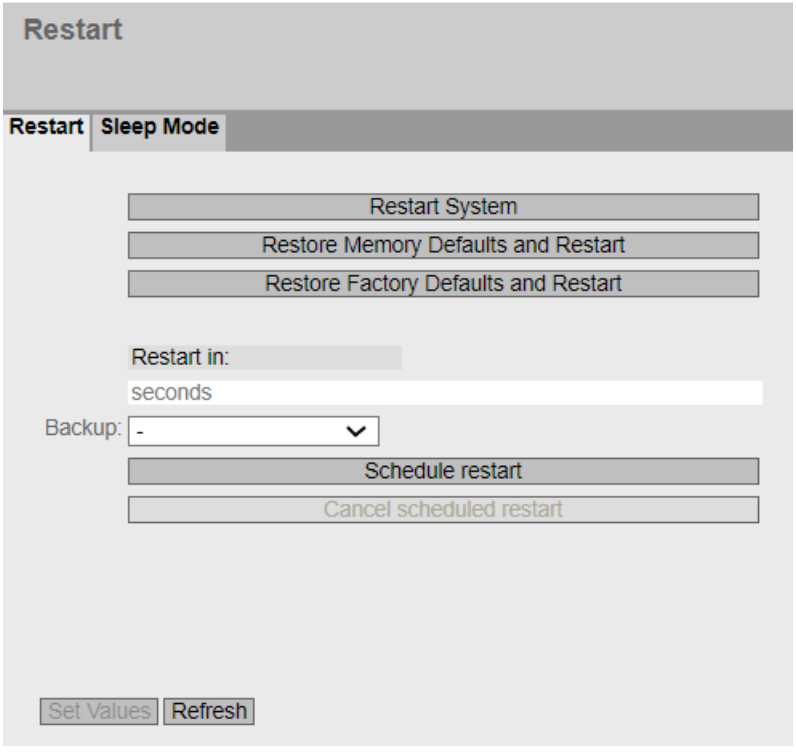
1. In the "Used DNS Servers" drop-down list, select which DNS servers are to be used.
2. Click the "Set Values" button.

6.4.5 Restart

6.4.5.1 Restart

Resetting to the defaults

Using the WBM page, you can restart the device based on a schedule or manually. In addition, there are various options for resetting to the device defaults.



Restart

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.
- If the device is in "Trial" mode, configuration modifications must be saved manually before a restart. Any modifications you have made only become active on the device after clicking the "Set values" button on the relevant WBM page.
- If the device is in "Automatic Save" mode, the last changes are saved automatically before a restart.

Description

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

- **Restart**
  Click this button to restart the system. You must confirm the restart in a dialog box. During a restart, the device is reinitialized, the internal firmware is reloaded, and the device runs a self-test. The settings of the start configuration are retained, e.g. the IP address of the device. The learned entries in the address table are deleted. You can leave the browser window open while the device restarts. After the restart you will need to log in again.
- **Restore Memory Defaults and Restart**
  Click this button to restore the factory settings of the device, with the exception of protected default settings, and to restart the device.
  The protected presets include the following parameters:
  - 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
  - DHCPv6 Rapid Commit
  - PROFINET Name of Station
- **Restore Factory Defaults and Restart**
  Click this button to restore the factory configuration settings and to restart the device. The protected defaults are also reset. You must confirm the restart in a dialog box.

  Note

  By resetting all the defaults to the factory configuration settings, the IP address is also lost. Assign an IP address to the device using DHCP or SINEC PNI.

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

- **Restart in: seconds**
  This field is used to set the timer. The field can no longer be edited when the timer is running. Specify the amount of time in seconds after which the device restarts.
  Value range 300 ... 86400 seconds
- **Backup**
  The configuration backups under "System > Configuration Backup" are available for selection. Before the scheduled restart, the device applies the configurations of the selected backup and continues working with them after the restart.
  All configurations made up to this point that have not been saved in a backup are lost.

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

  Note

  Unsaved configuration is lost after reboot

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

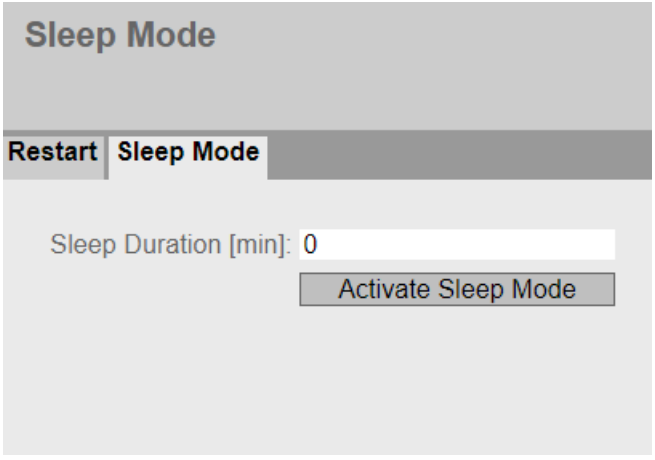
  Save the current configuration via "System > Backup of configuration" before setting the timer for the restart.

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

6.4.5.2 Sleep Mode

To reduce the power consumption of the device, you can use the "Sleep Mode" energy saving mode. This mode puts the device to sleep and changes to the previous state after the configured time has elapsed. When sleep mode is activated, all processes are aborted, even a firmware update for example.

On this page, you specify after the time after which the device in sleep mode wakes up again.



Description

- **Sleep Duration [min.]**
  Specify how long the device should remain in power saving mode.
  Value range 1 ... 44639. Default value 0: Power saving mode off
- **Activate Sleep Mode**
  Use this button to activate the sleep timer.

Procedure

1. Enter a value of 1 ... 44639 minutes in the "Sleep Duration [min.]" text box.
2. Click on the "Activate Sleep Mode" button.

Result

The device applies the setting for the duration and immediately switches to sleep mode. Once the time has elapsed, the device returns to the active state. The digital output is deactivated after the restart.

Note

Retaining the state of the digital output

The device can note the current state of the digital output and restore it after a restart. You can find more information on the WBM page "System > Configuration".

6.4.6 Commit Control

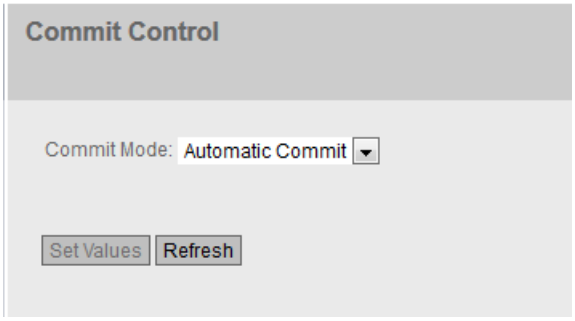
Change management

On this page, you specify when the WLAN settings become effective on the SCALANCE W 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 SCALANCE W device before it is fully configured.

With the "Manual Commit" setting, you have the opportunity of first fully configuring the SCALANCE W 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 SCALANCE W 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.



Description

The page contains the following boxes:

- **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. In the default setting, the SCALANCE W device is set to "Automatic Commit".
  - Manual Commit
    The changes are accepted, but are not effective immediately. The changes only take effect when you click the "Commit Changes" button. The "Commit Changes" button is displayed when you set "Manual Commit".
    The following message is also displayed in the display area when there are WLAN changes: "Manual Commit Mode active - Press 'Commit Changes' button to provide current configuration to driver". This message can be seen on every WBM page until either the changes made have taken effect or the SCALANCE W 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.

6.4.7 Load & Save

6.4.7.1 File list

Overview of the file types

For a clearer overview, the file list is divided into different areas.

Area	Type	Description	Down-load	Save	Delete[1)]
Update	Firmware	The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be down-loaded to the device.	X	X	--

Area	Type	Description	Down-load	Save	Delete[1)]
Configuration	Config	This file contains the start configuration. Among other things, this file contains the definitions of the users, roles, groups and function rights. The passwords are stored in the file "Users". The file can be supplied with a password before down-load. To load the file into the device successfully, use the specified password. You enter the password on the WBM page "Passwords (Page 146)". If the file is password-protected, you cannot load the file via DHCP with options 66 and 67.	X	X	--
	ConfigPack	Detailed configuration information. for example, start configuration, users, certificates, favorites, firmware of the device (if saved as well). The file can be supplied with a password before down-load. To load the file into the device successfully, use the specified password. You enter the password on the WBM page "Passwords (Page 146)". For more detailed information on creating and using the ConfigPack incl. firmware, refer to the section "Maintenance (Page 311)". If the file is password-protected, you cannot load the file via DHCP with options 66 and 67.	X	X	--
	ConfigPack-Backup	This ZIP file stores all the configuration backups you have created.	X	X	X
	RunningCLI	Text file with CLI commands This file contains an overview of the current configu-ration in the form of CLI commands. Passwords are masked in this file as follows: [PASSWORD] You can download the text file. The file is not intended to be uploaded again unchanged.	--	X	--
	RunningSINE-MAConfig	You save the current device configuration in this file type for transfer to STEP 7 Basic/Professional. The file can be imported in STEP 7 Basic/Professional and in-stalled on a device with the same article number and firmware version. Before you can save a file, you must assign a password for the "RunningSINEMAConfig" in the WBM under "System > Load&Save > Passwords". You also need this password to import the file into STEP 7 Basic/Profes-sional. See also "SINEMAConfig"	--	X	--
	Script	Text file with CLI commands	X	--	--
	SINEMAConfig	You load configuration data that was exported via STEP 7 Basic/Professional for transfer to the WBM with this file type. To load a file, you must assign a password for the "SI-NEMAConfig" under "System > Load&Save > Pass-words". You also need this password to export the file from STEP 7 Basic/Professional.	X	--	--

Area	Type	Description	Down-load	Save	Delete[1)]
		See also "RunningSINEMAConfig"			
	Users	File with user names and passwords	X	X	--
	WBMFav	WBM favorites This file contains the favorites that you created in the WBM. You can download this file and upload it to other devices.	X	X	X

Area	Type	Description	Down-load	Save	Delete[1)]
Certificates & keys	HTTPSCert	Default HTTPS certificates including key The preset and automatically created HTTPS certificates are self-signed. We strongly recommend that you create your own HTTPS certificates and make them available. We recommend that you use HTTPS certificates signed either by a reliable external or by an internal certification authority. The HTTPS certificate checks the identity of the device and controls the encrypted data exchange. The following file types can be loaded into the device. • .pem To successfully load an HTTPS certificate with this data type into the device, the certificate must include the unencrypted private key. • .p12 For HTTPS certificates with this file type, the private key is encrypted and secured with a password. To load the certificate successfully into the device, enter the password specified for the file on the WBM page "Passwords (Page 146)". After the upload, the existing HTTPS certificate is overwritten. It is recommended that you use password-protected certificates in the PKCS#12 format. The following certificates are supported: • ECDSA certificates that were generated with secp521r1 (NIST P-521) • RSA certificates with a maximum key length of 4096 bits	X	X	X
	SSHPrivate-KeyECDSA	SSH private key (ECDSA) The SSH key ecdsa-sha2-nistp521 is supported. There are files to which access is password-protected. To successfully load the file into the device, enter the password specified for the file on the WBM page "Passwords (Page 146)".	X	X	X
	SSHPrivate-KeyRSA	SSH private key (RSA) with and without password The following SSH keys are supported: • rsa-sha2-512 • rsa-sha2-256 There are files to which access is password-protected. To successfully load the file into the device, enter the password specified for the file on the WBM page "Passwords (Page 146)".	X	X	X
	WLANCert (only in client mode)	User certificate. You can specify a password for the user certificate on the WBM page "Load&Save > Password". Maximum key length: 8192 bits	X	X	X

Area	Type	Description	Down-load	Save	Delete[1)]
	WLANServer-Cert (only in client mode)	Server certificate. You can specify a password for the server certificate on the WBM page "Load&Save > Password". Maximum key length: 8192 bits	X	X	X
Services & log	Debug	This file contains information for Siemens Support. It is encrypted and can be sent by e-mail to Siemens Support without any security risk.	--	X	X
	LogFile	File with entries from the event log table	--	X	--
	StartupInfo	Startup log file This file contains the messages that were entered in the log file during the last startup.	--	X	--
	WLANAuthlog	File with entries from the WLAN Authentication Log (information on successful or failed authentication attempts)	--	X	--
	WLANSigRec (only in client mode)	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 227)".	--	X	X
Information	CountryList	The ZIP file contains the country list as a csv file.	--	X	--
	GSDML	Information on the device properties (PROFINET)	--	X	--
	MIB	Private MSPS MIB file "Scalance_w_msps.mib"	--	X	--
License	LicenseConditions	The ZIP file contains the licensing conditions and copyright information	--	X	--

[1)] Deletion is only possible via HTTP/HTTPS.

Using configuration files

Note

Configuration files and Trial mode/Automatic Save

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

CLI script file

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

Note

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

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

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

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

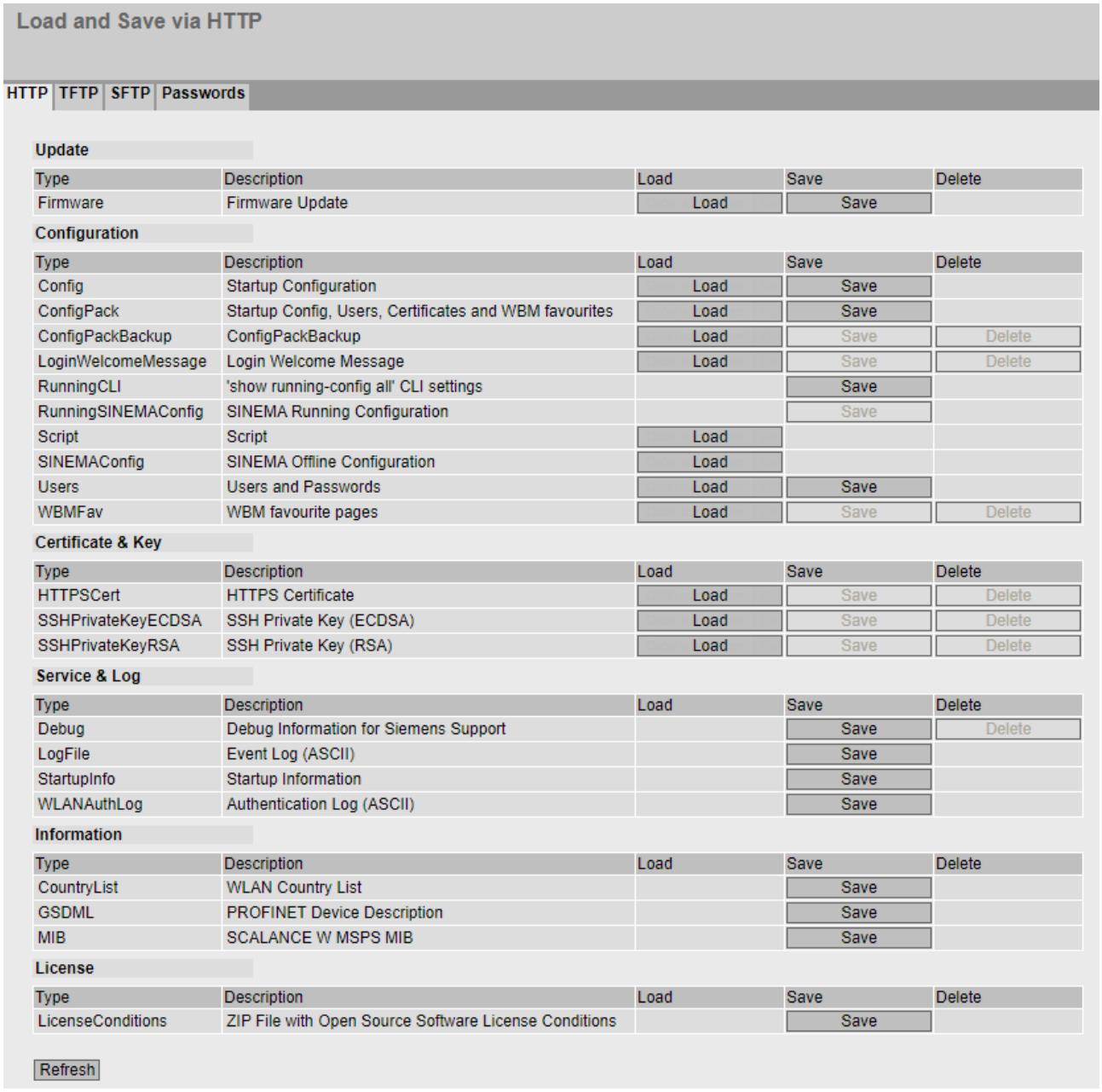
Requirements:

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

You can use the file types as follows:

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

6.4.7.2 HTTP


Load and Save via HTTP
HTTP
TFTP
SFTP
Passwords
Update
Type
Description
Load
Save
Delete
Firmware
Firmware Update
Load
Save
Configuration
Type
Description
Load
Save
Delete
Config
Startup Configuration
Load
Save
ConfigPack
Startup Config, Users, Certificates and WBM favourites
Load
Save
ConfigPackBackup
ConfigPackBackup
Load
Save
Delete
LoginWelcomeMessage
Login Welcome Message
Load
Save
Delete
RunningCLI
'show running-config all' CLI settings
Save
RunningSINEMAConfig
SINEMA Running Configuration
Save
Script
Script
Load
SINEMAConfig
SINEMA Offline Configuration
Load
Users
Users and Passwords
Load
Save
WBMFav
WBM favourite pages
Load
Save
Delete
Certificate & Key
Type
Description
Load
Save
Delete
HTTPSCert
HTTPS Certificate
Load
Save
Delete
SSHPrivateKeyECDSA
SSH Private Key (ECDSA)
Load
Save
Delete
SSHPrivateKeyRSA
SSH Private Key (RSA)
Load
Save
Delete
Service & Log
Type
Description
Load
Save
Delete
Debug
Debug Information for Siemens Support
Save
Delete
LogFile
Event Log (ASCII)
Save
StartupInfo
Startup Information
Save
WLANAuthLog
Authentication Log (ASCII)
Save
Information
Type
Description
Load
Save
Delete
CountryList
WLAN Country List
Save
GSDML
PROFINET Device Description
Save
MIB
SCALANCE W MSPS MIB
Save
License
Type
Description
Load
Save
Delete
LicenseConditions
ZIP File with Open Source Software License Conditions
Save
Refresh

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

This WBM page is available both for connections using HTTP and for connections using HTTPS.

Description

For a clearer overview, the tables are divided into different areas. Each table has the following columns:

- **Type**
  Shows the name of the file.

  Note

  Size of certificate files

  With certificate files only certificates with a maximum of 8192 bits are supported.

- **Description**
  Shows the short description of the file type.
- **Load**
  With this button, you can load files on the device. The button can be enabled, if this function is supported by the file type.
- **Save**
  With this button, you can save files from the device. The button can only be enabled if this function is supported by the file type and the file exists on the device.
- **Delete**
  With this button, you can delete files from the device. The button can only be enabled if this function is supported by the file type and the file exists on the device.

  Note

  Following a firmware update, delete the cache of the Web browser.

Procedure

Loading data using HTTP(S)

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 data using HTTP(S)

1. Start the save function by clicking the one of the "Save" buttons. Depending on the size of the file this may take some time.
2. Depending on your browser configuration 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 data using HTTP(S)

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.

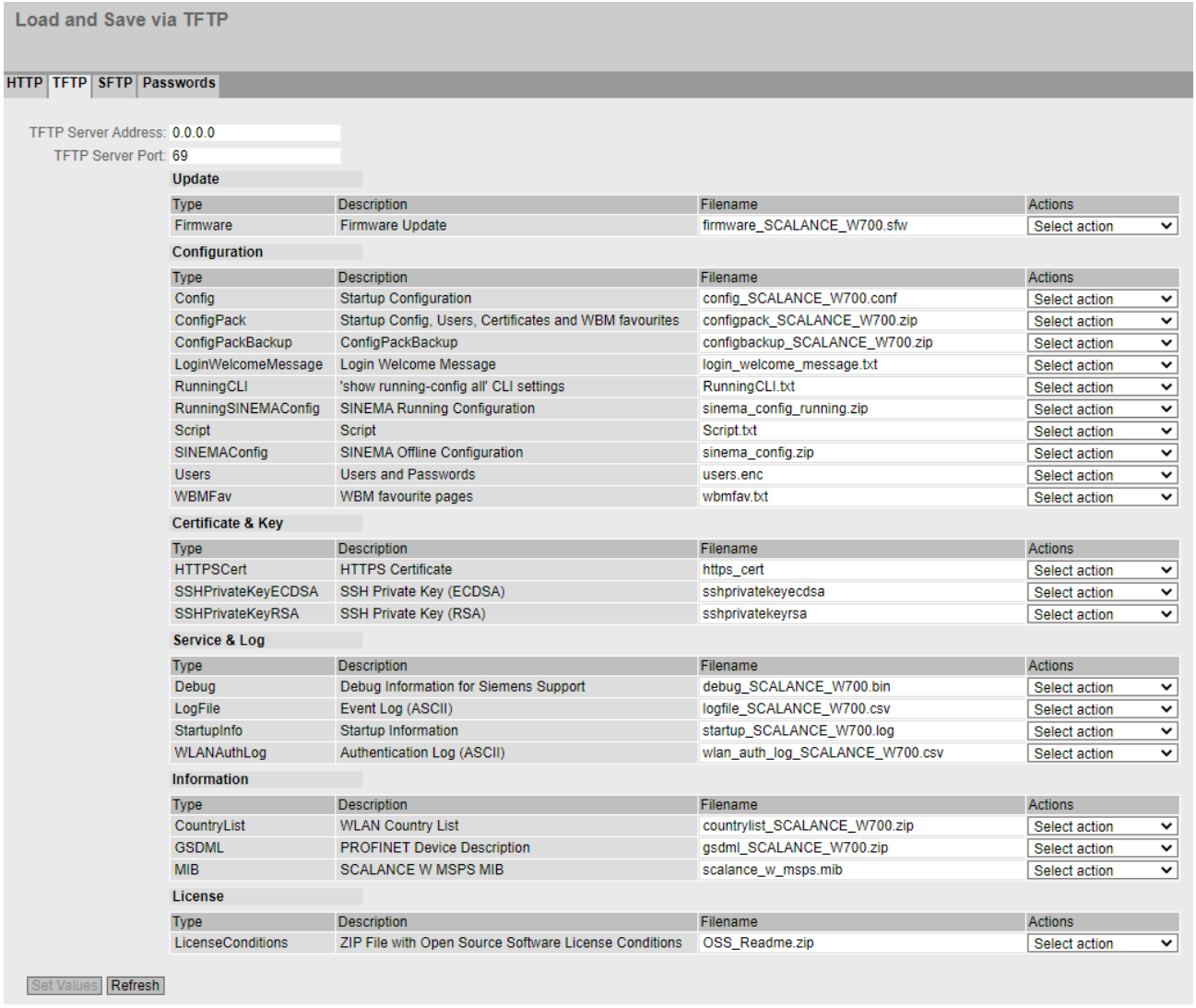
Note

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

Password-protected config file

If the file is password-protected, you cannot load the file via DHCP with options 66 and 67.

6.4.7.3 TFTP



Loading and saving data via a TFTP server

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

Description

The page contains the following boxes:

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

For a clearer overview, the tables are divided into different areas. Each table has the following columns:

- **Type**
  Shows the name of the file.

  Note

  Size of certificate files

  With certificate files only certificates with a maximum of 8192 bits are supported.

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

  Note

  Changing the file name

  You can change the file name preset in this column. After clicking the "Set Values" button, the changed name is saved on the device and can also be used with the Command Line Interface.

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

Procedure

Loading or saving data using TFTP

1. Enter the IP address or the FQDN of the TFTP server in the "TFTP Server 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 "File name" 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. Depending on the size of the file this may take some time.
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.

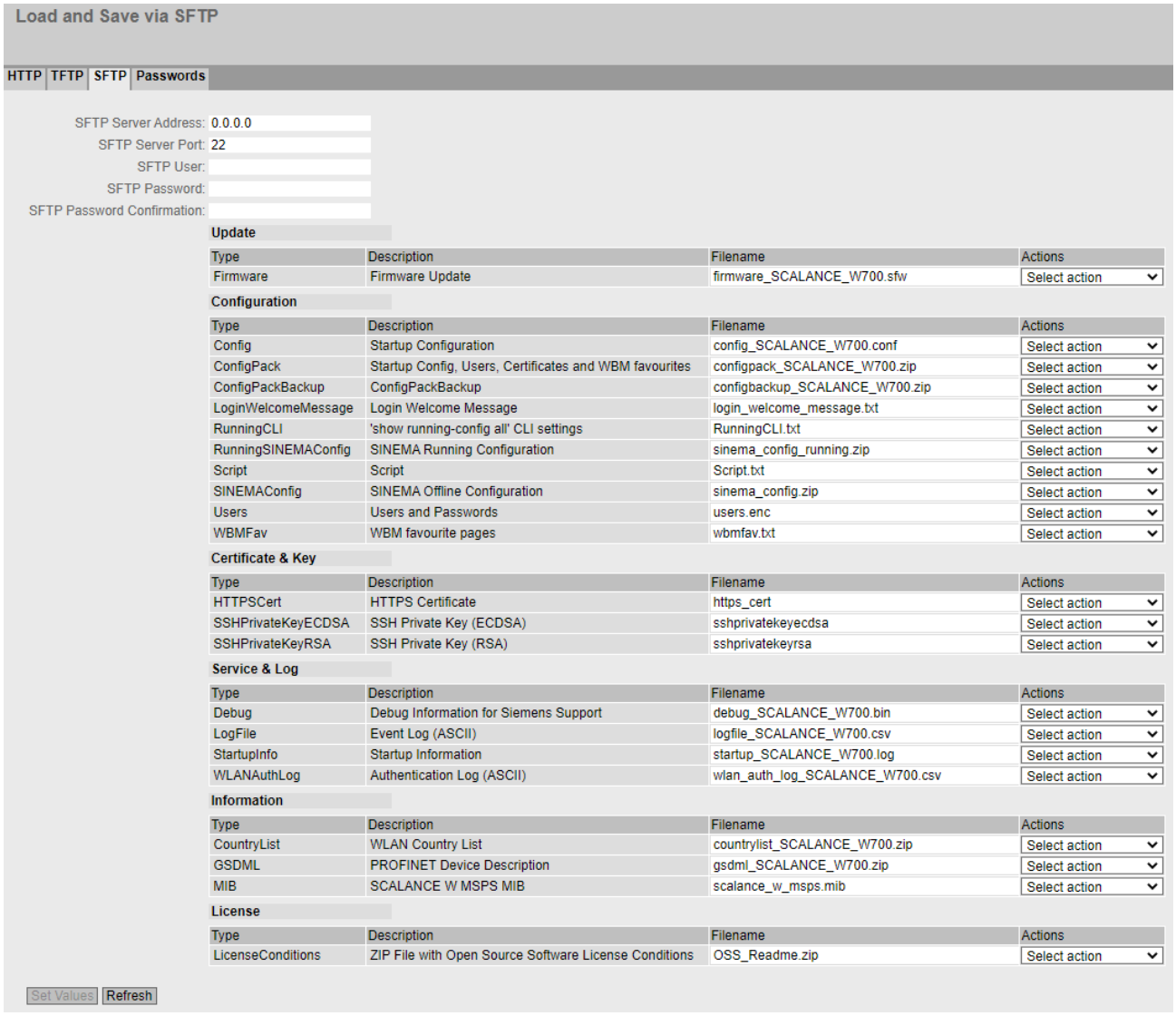
Note

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

Password-protected config file

If the file is password-protected, you cannot load the file via DHCP with options 66 and 67.

6.4.7.4 SFTP



Loading and saving data via an SFTP server

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

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

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

Description

The page contains the following boxes:

- **SFTP Server Address**
  Enter the IP address or the FQDN of the SFTP server with which you exchange data.
- **SFTP Server Port**
  Enter the port of the SFTP server via which data exchange will be handled. If necessary, you can change the default value 22 to your own requirements.
- **SFTP User**
  Enter the user for access to the SFTP server. This assumes that a user with the corresponding rights has been created on the SFTP server.
  The name must meet the following conditions:
  - It must be unique.
  - It must be between 1 and 250 characters long.
  - The following characters must not be included: § ? " ; :
    The characters for Space and Delete also cannot be included.
- **SFTP Password**
  Enter the password for the user
- **SFTP Password Confirmation**
  Confirm the password.

For a clearer overview, the tables are divided into different areas. Each table has the following columns:

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

  Note

  Changing the file name

  You can change the file name preset in this column. After clicking the "Set Values" button, the changed name is saved on the device and can also be used with the Command Line Interface.

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

Procedure

Loading or saving data using SFTP

1. Enter the address of the SFTP server in "SFTP Server Address".
2. Enter the port of the SFTP server to be used in "SFTP Server Port".
3. Enter the user data (user name and password) required for access to the SFTP server.
4. If applicable, enter the name of a file in which you want to save the data or take the data from in "Filename".

   Note

   Files whose access is password protected

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

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

Reusing configuration data

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

Follow the steps below to reuse configuration data:

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

Note

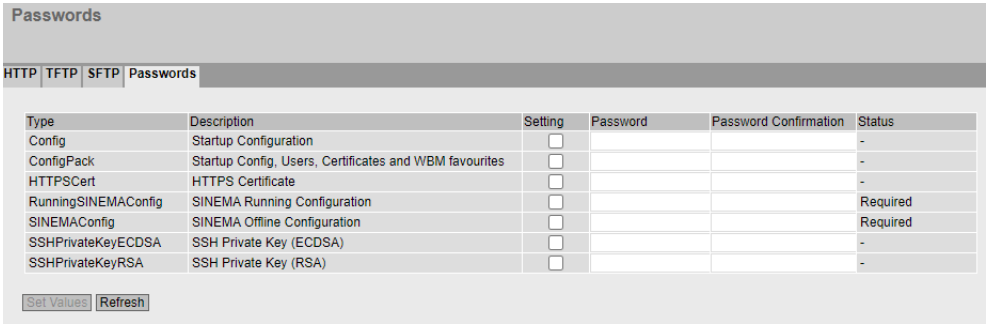
Configuration data has a checksum. If you edit the files, you can no longer upload them to the device.

Password-protected config file

If the file is password-protected, you cannot load the file via DHCP with options 66 and 67.

6.4.7.5 Passwords

There are files to which access is password-protected. For example to be able to use the HTTPS certificate, you need to specify the corresponding password on this WBM page.



Description

The table has the following columns:

- **Type**
  Shows the file type.
- **Description**
  Shows the short description of the file type.
- **Setting**
- When enabled, the file is used. Can only be enabled if the password is configured.
- **Password**
  Enter the password for the file.
- **Password Confirmation**
  Confirm the password.
- **Status**
  Shows whether the password corresponds to the file on the device.
  - Valid
    The "Enabled" check box is selected and the password matches the file.
  - Invalid
    The "Enabled" check box is selected but the password does not match the file or no file has been loaded yet.
  - '-'
    The password cannot be evaluated or is not yet being used. The "Enabled" check box is not selected.
  - Required
    A password is required for loading or saving.

Procedure

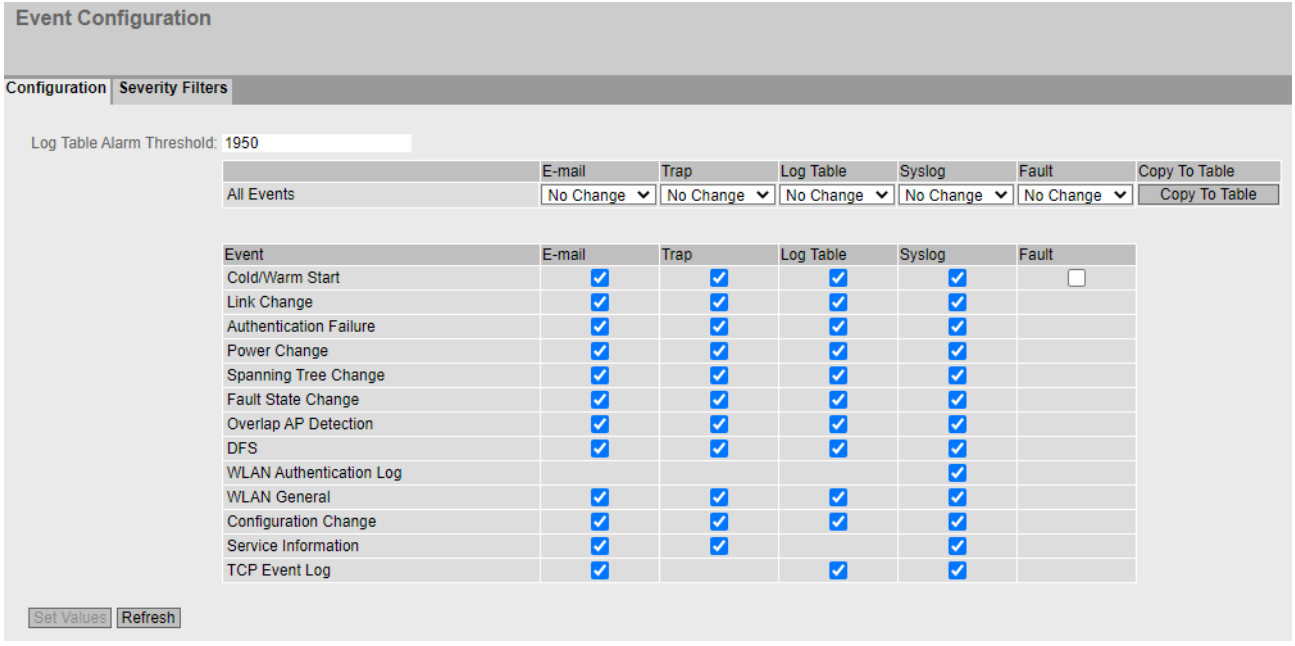
1. Enter the password in "Password".
2. To confirm the password, enter the password again in "Password Confirmation".
3. Select the "Enabled" option.
4. Click the "Set Values" button.

6.4.8 Events

6.4.8.1 Configuration

Selecting system events

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



Description

- **Log Table Alarm Threshold**
  Set the limit for the entries for each severity. A maximum of 2000 entries are possible for each severity.
  If the specified limit will be reached with the next entry, an alarm message is output, e.g. if 1950 is specified, the message that limit 1950 has been reached is output after entry 1949.

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

- **All Events**
  Shows that the settings are valid for all events of table 2.
- **E-mail / Trap / Log Table / Syslog / Faults**
  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 restart
    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 only 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.
    For an error to also be signaled by the fault LED "F", you must enable "Fault State Change" for the "Digital Out". In this case, the fault LED "F" lights up when an internal error occurs and the digital input is closed.
  - Overlap AP Detection (only in access point mode)
    This event is triggered when there is an entry in the "Overlap AP" list.
  - DFS (Only in access point mode)
    This event occurs if a radar signal was received or the DFS scan was started or stopped.
  - 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.
  - WLAN General (only in access point mode)
    Enabling the "WLAN General" event has no function.
  - Configuration Change
    This event occurs when the configuration of the device has changed.
  - Service Information
    Some system events that occurred are entered in the event log table without configuration. For these events, you can configure additional types of notification.
  - TCP Event Log
    The device has received a TCP packet. The prerequisite is that the "TCP Event" function is enabled.
- **Type of notification**

- E-mail
  The device sends an e-mail. This is only possible if the SMTP server is set up and the "SMTP Client" function is enabled.
- Trap
  The device sends an SNMP trap. This is only possible if "SNMPv1 Traps" is enabled in "System > Configuration".
- Log Table
  The device writes an entry to the event log table. The content of the event log table is displayed in "Information > Log Tables > Event Log".
- 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.
- Error
  The device triggers an error. The error LED lights up and the currently pending error is displayed under "Information > Faults".

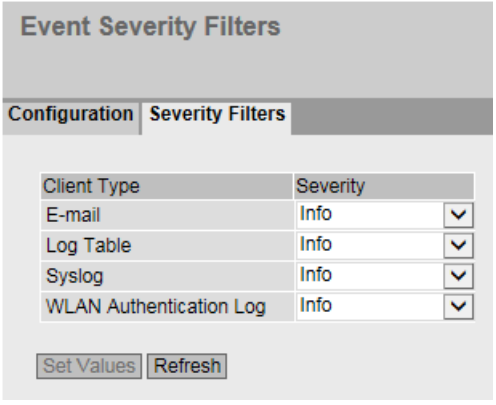
Procedure

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
   - Error
2. Click the "Set Values" button.

6.4.8.2 Severity Filters

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



Description

The table has the following columns:

- **Client Type**
  Select the client type for which you want to make settings:
  - **E-mail**
    Sending system event messages by e-mail
  - **Log Table**
    Entry of system events in the log table
  - **Syslog**
    Entry of system events in the Syslog file
  - **WLAN Authentication Log**
    Entry of system events in the WLAN authentication log
- **Severity**
  Select the desired severity. The following settings are possible:
  - **Critical**
    System events with the severity Critical are processed.
  - **Warning**
    System events with the Warning severity or higher are processed: This means events of the categories "Warning" and "Critical".
  - **Info**
    System events with the Info severity or higher are processed: This means events of the categories "Info", "Warning" and "Critical".

Procedure

Follow the steps below to configure the required level:

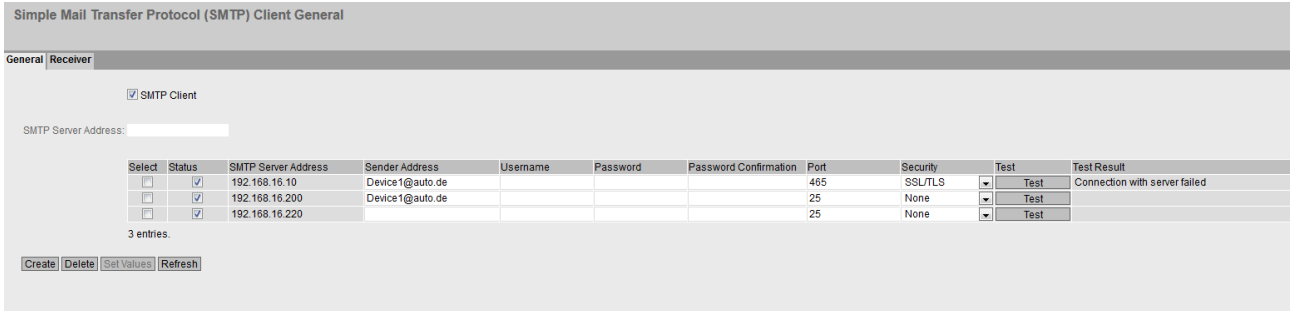
1. Select the required values from the drop-down lists of the second table column after the client types.
2. Click the "Set Values" button.

6.4.9 SMTP client

6.4.9.1 General

Network monitoring with e-mails

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



Requirements for sending e-mails

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

Description

The page contains the following boxes:

- **SMTP Client**
  Enable or disable the SMTP client.
- **SMTP Server Address**
  Enter the IP address or the FQDN of the SMTP server.

The table contains the following columns:

- **Select**
  Select the check box in a row to be deleted.
- **Status**
  Specify whether this SMTP server will be used.
- **SMTP Server Address**
  Shows the SMTP server IP address.
- **Sender Email Address**
  Enter the e-mail address of the sender that is specified in the e-mail.

- **User Name**
  If necessary, enter the user name used for authentication on the SMTP server.
- **Password**
  If necessary, enter the password used for authentication on the SMTP server.
- **Password Confirmation**
  Repeat the password.
- **Port**
  Enter the port via which your SMTP server can be reached.
  Factory settings:
  - 25 (None)
  - 465 (SSL/TLS and StartTLS)
- **Security**
  Specify whether transfer of the e-mail from the device to the SMTP server is encrypted. This is only possible when the SMTP server supports the selected setting.

  Note

  2-factor authentication (2FA)

  2-factor authentication is not supported.

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

Procedure

Configuring the SMTP server

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

7. Enable the SMTP server entry.
8. Click the "Set Values" button.

Note

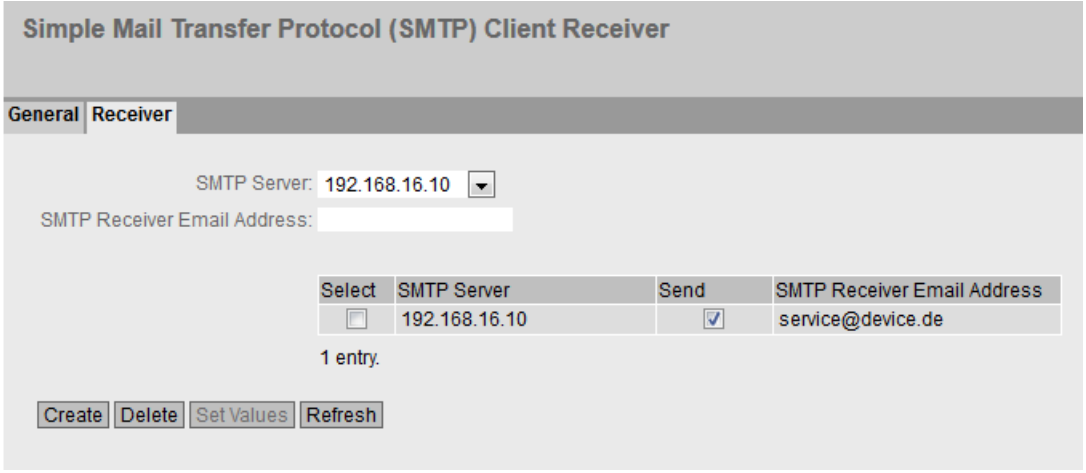
Depending on the properties and configuration of the SMTP server, it may be necessary to adapt the "Sender E-Mail Address" input for the e-mails. Check with the administrator of the SMTP server.

Testing the configuration of the SMTP server

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

6.4.9.2 Recipient

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



Description

The page contains the following boxes:

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

The table contains the following columns:

- **Select**
  Select the check box in a row to be deleted.
- **SMTP Server**
  Shows the IP address of the SMTP server to which the entry relates.
- **Send**
  When enabled, the device sends an email to this receiver.
- **Email address of the SMTP receiver**
  Shows the e-mail address to which the device sends an e-mail if a fault occurs.

Procedure

Configuring an SMTP receiver

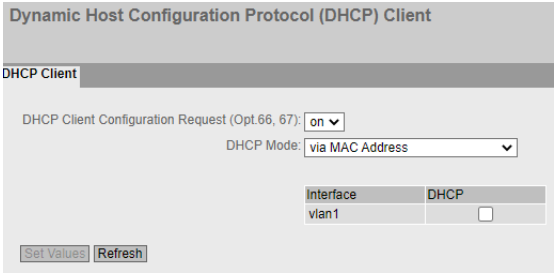
1. Select the required "SMTP server".
2. Enter the email address of the SMTP receiver.
3. Click the "Create" button. A new entry is generated in the table.
4. Activate the "Send" option for the entry.
5. Click the "Set Values" button.

6.4.10 DHCPv4

6.4.10.1 DHCP Client

Setting of the DHCP mode

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



Description

The page contains the following boxes:

- **DHCP client configuration file request (opt. 66, 67)**
  From the drop-down list, select whether you want the DHCP client to use options 66 and 67 to download a configuration file.
  - On
    Options 66 and 67 are enabled
  - Off
    Options 66 and 67 are disabled
- **DHCP Mode**
  Select the DHCP mode from the drop-down list. The following modes are possible:
  - via MAC Address
    Identification is based on the MAC address.
  - via DHCP Client ID
    Identification is based on a freely defined DHCP client ID.
  - via System Name
    Identification is based on the system name. If the system name is 255 characters long, the last character is not used for identification.
  - via PROFINET Name of Station
    Identification is based on the PROFINET station name.

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

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

Note

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

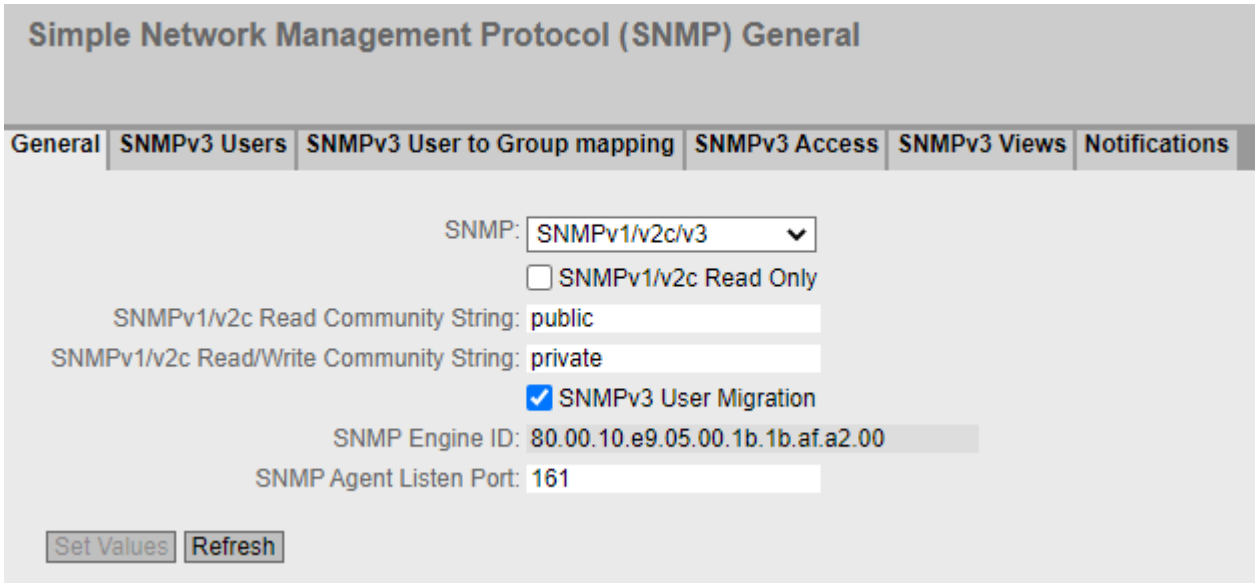
Make sure that the option "DHCP Client Configuration Request (Opt. 66, 67)" is no longer set.

6.4.11 SNMP

6.4.11.1 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.



Description

The page contains the following boxes:

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

    Note

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

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

  Note

  Community String

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

  The recommended minimum length for community strings is 6 characters.

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

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

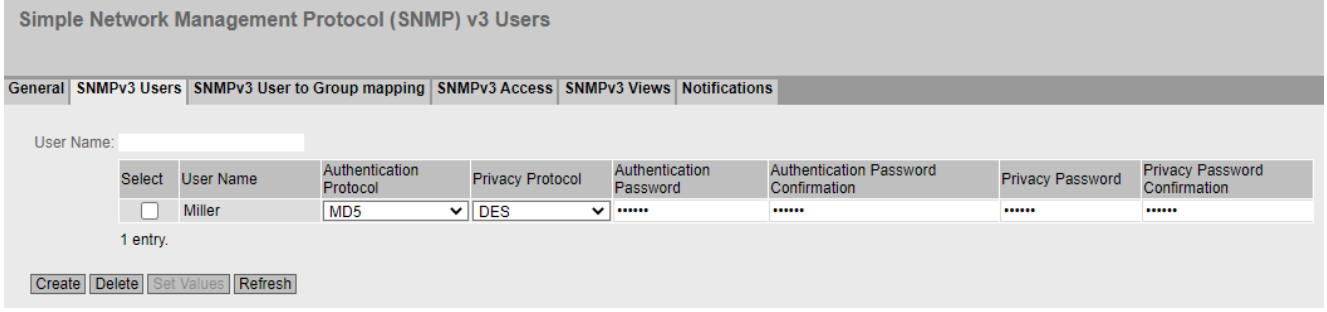
Procedure

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

6.4.11.2 SNMPv3 Users

User-specific security settings

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



Description

The page contains the following boxes:

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

The table has the following columns:

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

  Note

  Length of the password

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

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

  Note

  Length of the password

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

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

Procedure

Create a new user

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

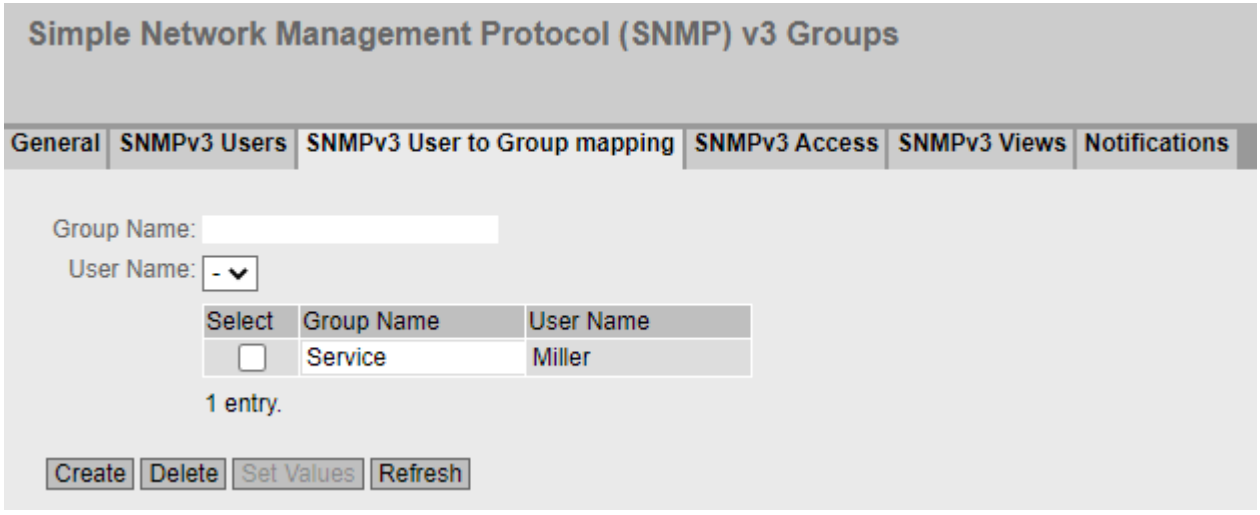
Delete user

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

6.4.11.3 SNMPv3 User to Group mapping

Configuration of group members

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



Description

The page contains the following boxes:

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

The table has the following columns:

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

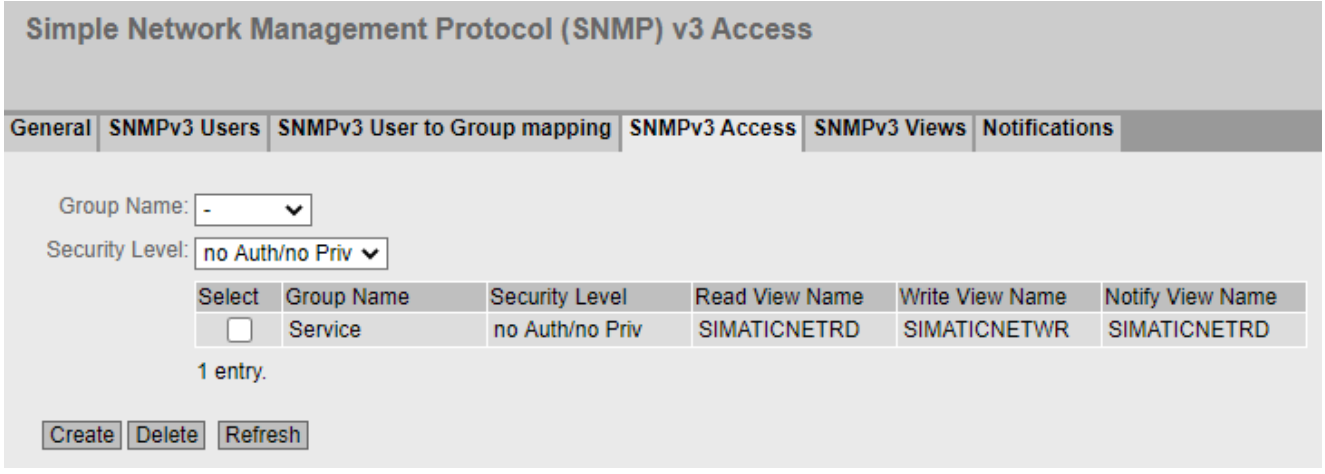
6.4.11.4 SNMPv3 Access

Security settings and assigning permissions

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

Note

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



Description

The page contains the following boxes:

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

The table has the following columns:

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

  Note

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

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

Procedure

Creating a new group

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

Modifying a group

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

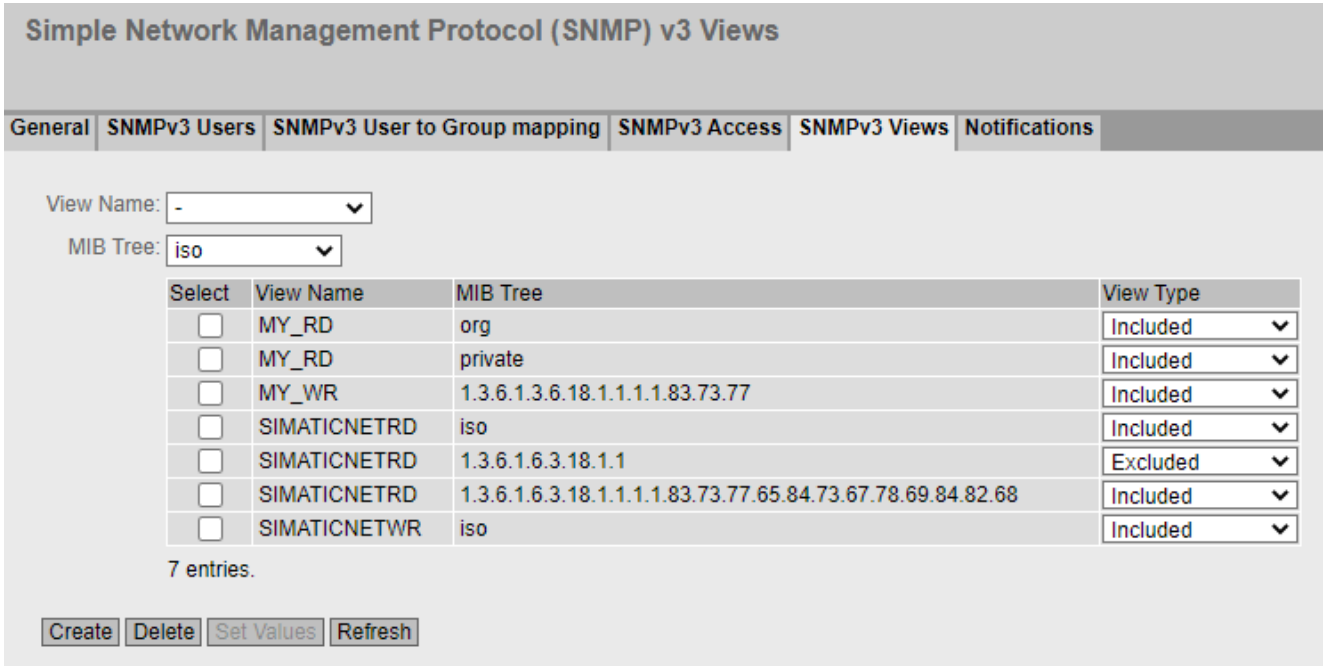
Deleting a group

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

6.4.11.5 SNMPv3 Views

Configuration of SNMPv3 views

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



Note

Controlling the SNMPv1 and SNMPv2c access

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

Description

The page contains the following boxes:

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

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

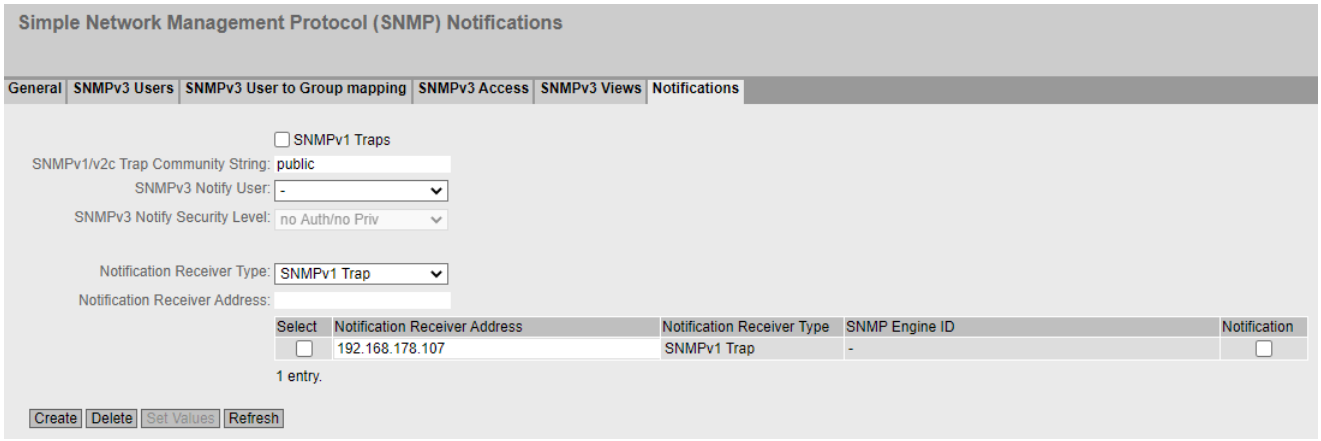
The table has the following columns:

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

6.4.11.6 Notifications

SNMP traps and SNMPv3 notifications

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



Description

The page contains the following boxes:

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

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

The table has the following columns:

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

Note

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

Procedure

Configuring a notification

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

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

Deleting a trap entry

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

6.4.12 System Time

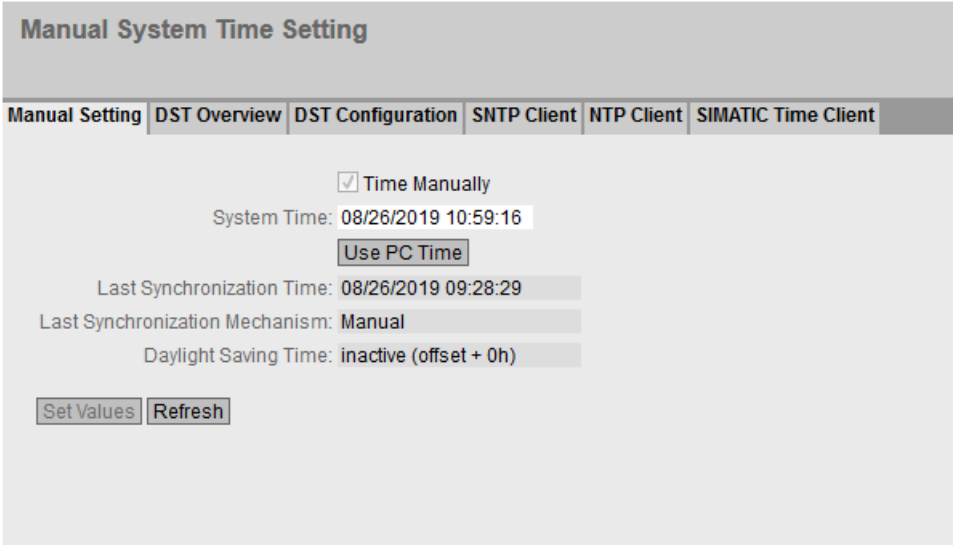
There are different methods that can be used to set the system time of the device. Only one method can be active at any one time.

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

6.4.12.1 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".



Description

The page contains the following boxes:

- **Time Manually**
  Enable the manual time setting. If you enable the option, the "System Time" input box can be edited.
- **System Time**
  Enter the date and time in the format MM/DD/YYYY hh:mm:ss.
  After a restart, the time of day begins at 01/01/2000 00:00:00.
- **Use PC Time**
  Click the button to use the time setting of the PC.
- **Last Synchronization Time**
  Shows when the last time-of-day synchronization took place. If no time-of-day synchronization was possible, the box displays "Date/time not set".
- **Last Synchronization Mechanism**
  Shows how the last time synchronization was performed.
  - Not set
    The time was not set.
  - Manual
    Manual time setting
  - SNTP
    Automatic time-of-day synchronization with SNTP
  - NTP
    Automatic time-of-day synchronization with NTP
  - SIMATIC
    Automatic time-of-day synchronization using the SIMATIC time frame
- **Daylight Saving Time (DST)**
  Shows whether the daylight saving time changeover is active.
  - active (offset +1 h)
    The system time was changed to daylight saving time; in other words an hour was added.
    You can see the current system time at the top right in the selection area of the WBM.
    The current time including daylight saving time is displayed in the "System Time" box.
  - inactive (offset +0 h)
    The current system time is not changed.

Procedure

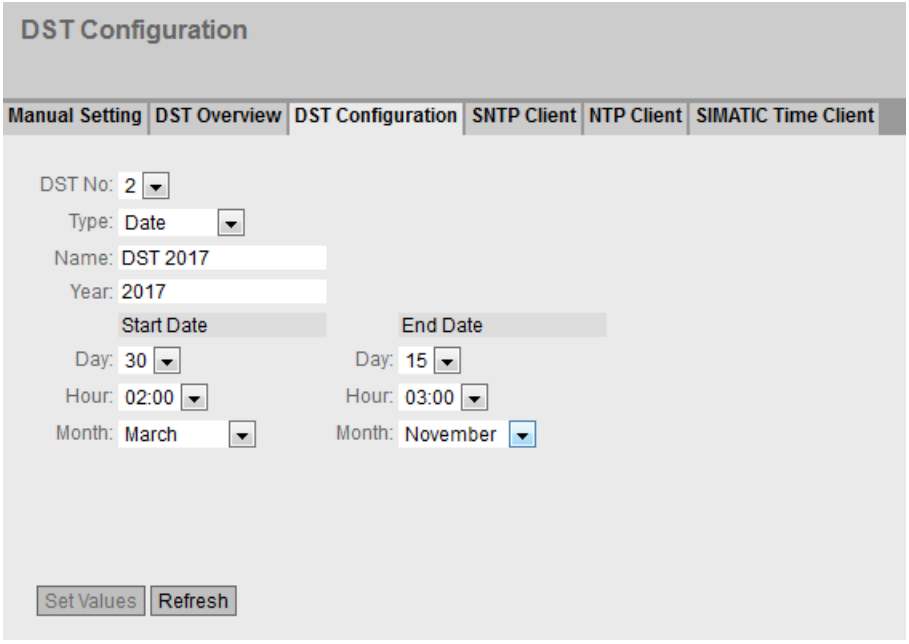
1. Enable the "Time Manually" option.
2. In the "System Time" input box, enter the date and time in the format MM/DD/YYYY hh:mm:ss.
3. Click the "Set Values" button.
   The date and time are adopted and "Manual" is entered in "Last Synchronization Mechanism" box.

6.4.12.2 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**
  Select the row you want to delete.
- **DST No.**
  Shows the number of the entry.
  If you create a new entry, a new line with a unique number is created.
- **Name**
  Shows the name of the entry.
- **Year**
  Shows the year for which the entry was created.
- **Start Date**
  Shows the month, day and time for the start of daylight saving time.
- **End Date**
  Shows the month, day and time for the end of daylight saving time.
- **Recurring Date**
  With an entry of the type "Rule", the period in which daylight saving time is active is displayed consisting of week, day, month and time of day.
  With an entry of the type "Date" a "-" is displayed.

- **State**
  Shows the status of the entry:
  - Enabled
    The entry was created correctly.
  - Invalid
    The entry was created new and the start and end date are identical.
- **Type**
  Shows how the daylight saving time changeover is made:
  - Date
    A fixed date is entered for the daylight saving time changeover.
  - Rule
    A rule was defined for the daylight saving time changeover.

Procedure

Creating an entry

1. Click the "Create" button.
   A new entry is created in the table.
2. Click on the required entry in the "DST No." column.
   You change to the "DST Configuration" page.
3. Select the required type in the "Type" drop-down list.
   Depending on the selected type, various settings are available.
4. Enter a name in the "Name" box.
5. If you have selected the type "Date", fill in the following boxes.
   - Year
   - Day (for start and end date)
   - Hour (for start and end date)
   - Month (for start and end date)
6. If you have selected the type "Rule", fill in the following boxes.
   - Hour (for start and end date)
   - Month (for start and end date)
   - Week (for start and end date)
   - Day (for start and end date)
7. Click the "Set Values" button.

Deleting an entry

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

6.4.12.3 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

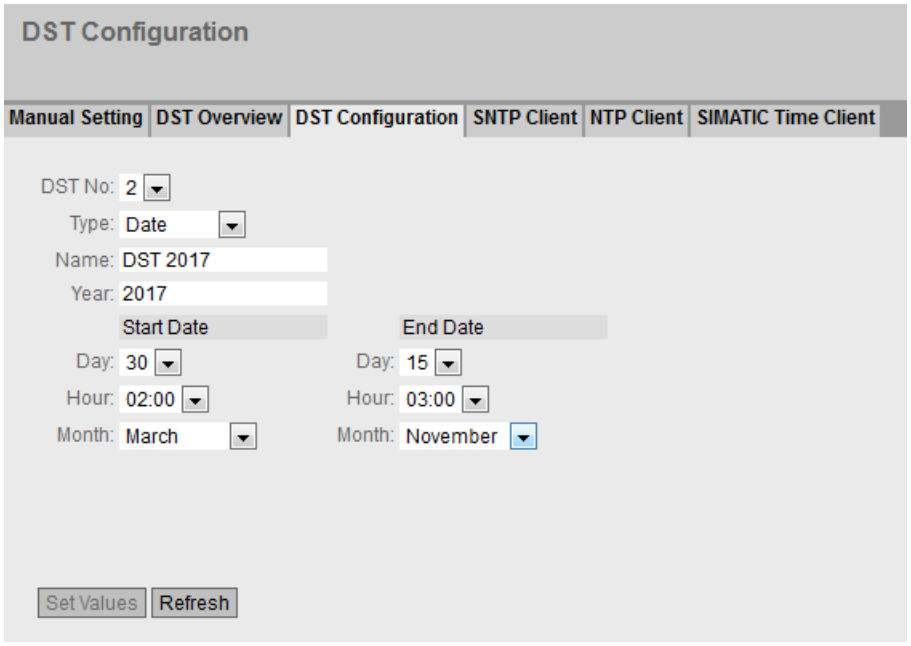
Note

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

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

- **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.
  - Rule
    You can define a rule for the daylight saving time changeover.
    This setting is suitable for regions in which the daylight saving time always begins or ends on a certain weekday.
- **Name**
  Enter a name for the entry.
  The name can be a maximum of 16 characters long.

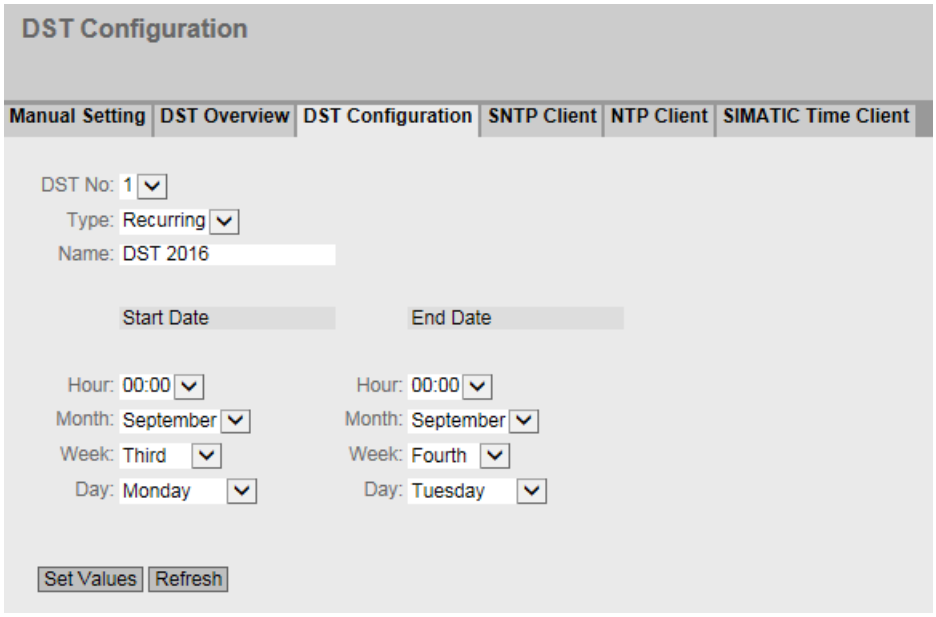
Settings with "Date" selected



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

- **Year**
  Enter the year for the daylight saving time changeover.
- **Start Date**
  Enter the following values for the start of daylight saving time:
  - Day
    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 "Rule" selected



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 first to fifth or the last week of the month.
  - Day
    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 first to fifth or the last week of the month.
  - Day
    Specify the weekday.

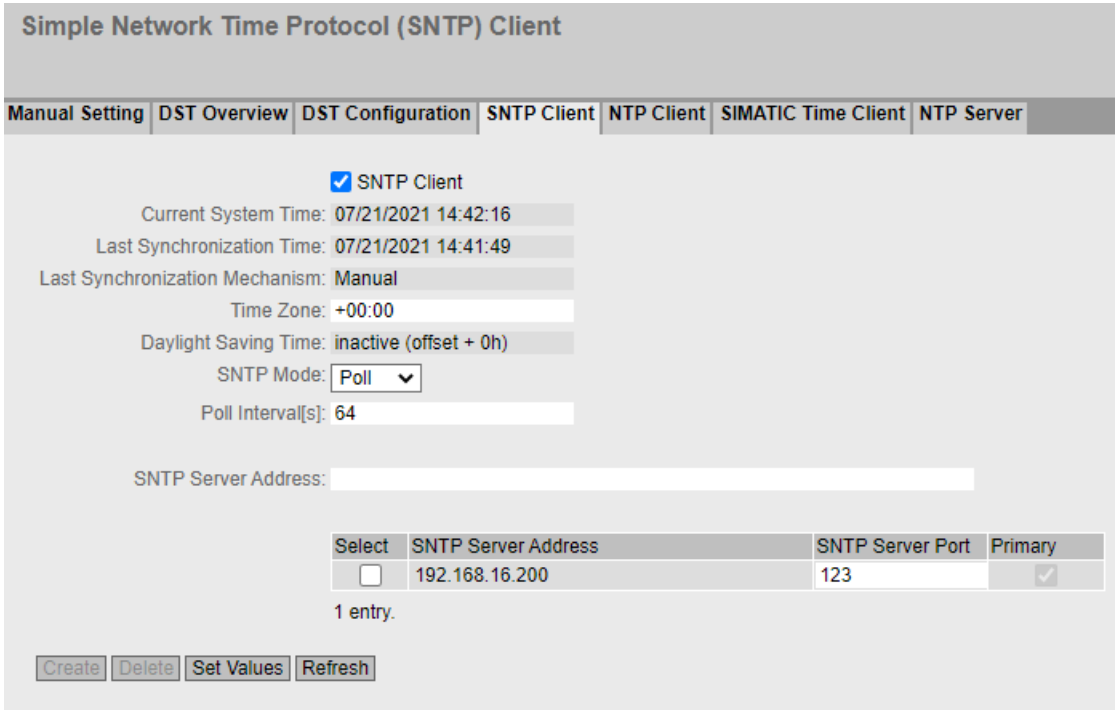
6.4.12.4 SNTP Client

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.

Note

To avoid time jumps, make sure that there is only one time server in the network.



Description

The page contains the following boxes:

- **SNTP Client**
  Enable or disable automatic time-of-day synchronization using SNTP.
- **Current System Time**
  Shows the current date and current normal time received by the device. If you specify a time zone, the time information is adapted accordingly.
- **Last Synchronization Time**
  Shows when the last time-of-day synchronization took place.

- **Last Synchronization Mechanism**
  Shows how the last time synchronization was performed. The following methods are possible:
  - Not set
    The time was not set.
  - Manual
    Manual time setting
  - SNTP
    Automatic time-of-day synchronization with SNTP
  - NTP
    Automatic time-of-day synchronization with NTP
  - SIMATIC
    Automatic time-of-day synchronization using the SIMATIC time frame
- **Time Zone**
  In this box, enter the time zone you are using in the format +/- hh:mm. The time zone relates to UTC standard world time.
  The time in the "Current System Time" box is adapted accordingly.
- **Daylight Saving Time (DST)**
  Shows whether the daylight saving time changeover is active.
  - active (offset +1 h)
    The system time was changed to daylight saving time; in other words an hour was added. You can see the current system time at the top right in the selection area of the WBM. The current time including daylight saving time is displayed in the "System Time" box.
  - inactive (offset +0 h)
    The current system time is not changed.
- **SNTP Mode**
  Select the synchronization mode from the drop-down list. The following types of synchronization are possible:
  - Listen
    With this mode, the device is passive and receives SNTP frames that deliver the time of day. Settings in the input boxes "SNTP Server Address" and "SNTP Server Port" have no effect in this mode.
    In this mode, only IPv4 addresses are supported.
  - Poll
    If you select this mode, the input box "Poll Interval[s]" is displayed to allow further configuration. In this mode, the settings in the input boxes "SNTP Server Address" and "SNTP Server Port" are taken into account. With this type of synchronization, the device is active and sends a time query to the SNTP server.
    In this mode, IPv4 and IPv6 addresses are supported.
- **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.
- **SNTP Server Address**
  Enter the IP address or the FQDN (Fully Qualified Domain Name) of the SNTP server.

- **SNTP Server Port**
  Enter the port of the SNTP server.
  The following ports are possible:
  - 123 (standard port)
  - 1025 to 36564
- **Primary**
  The check mark is set for the SNTP server that you create first. If several SNTP servers have been created, the primary server is queried first.

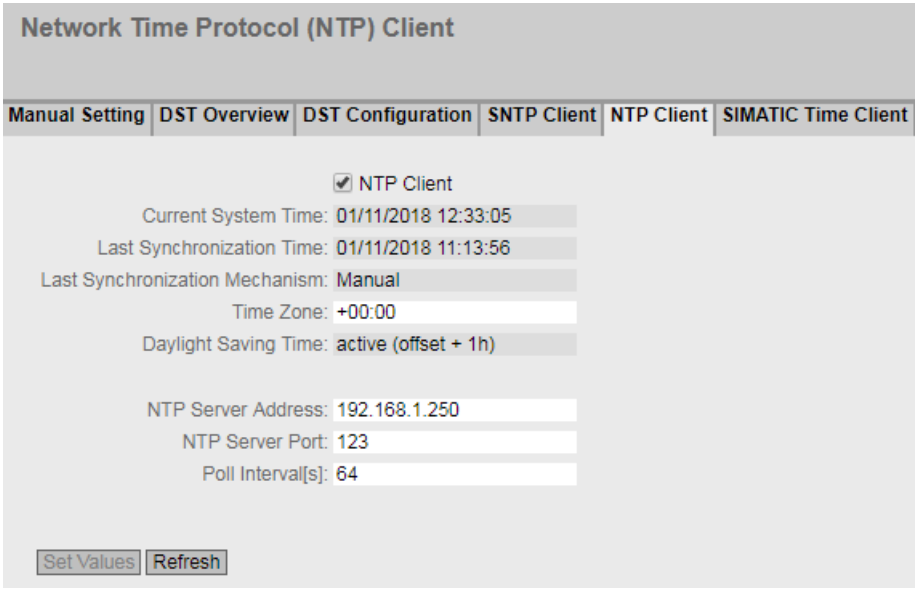
Procedure

1. Click the "SNTP Client" check box to enable the automatic time setting.
2. In 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, Central European Summer Time), 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. You configure the daylight saving time switchover on the pages "System > System Time > DST Overview" and "System > System Time > DST Configuration". 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)
     - Query interval (step 4)
     - Time server (step 5)
     - Port (step 7)
     - Complete the configuration with step 8.
   - Listen
     For this mode, you need to configure the following:
     - Time difference to the time sent by the server (step 2)
     - Complete the configuration with step 8.
4. In the "Poll Interval[s]" input box, enter the time in seconds after which a new time query is sent to the time server.
5. In the "SNTP Server Address" input box, enter the IP address or the FQDN of the SNTP server whose frames will be used to synchronize the time of day.
6. Click the "Create" button.
   A new row is inserted in the table for the SNTP server.
7. In the "SNTP Server Port" column, enter the port via which the SNTP server is available. The port can only be modified if the IPv4 address or the FQDN name of the SNTP server is entered.
8. Click the "Set Values" button to transfer your changes to the device.

6.4.12.5 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.



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**
  Shows the current date and current normal time received by the device. If you specify a time zone, the time information is adapted accordingly.
- **Last Synchronization Time**
  Shows when the last time-of-day synchronization took place.

- **Last Synchronization Mechanism**
  Shows how the last time synchronization was performed. The following methods are possible:
  - Not set
    The time was not set.
  - Manual
    Manual time setting
  - SNTP
    Automatic time-of-day synchronization with SNTP
  - NTP
    Automatic time-of-day synchronization with NTP
  - SIMATIC
    Automatic time-of-day synchronization using the SIMATIC time frame
- **Time Zone**
  In this box, enter the time zone you are using in the format "+/- hh:mm". The time zone relates to UTC standard world time.
  The time in the "Current System Time" box is adapted accordingly.
- **Daylight Saving Time (DST)**
  Shows whether the daylight saving time changeover is active.
  - active (offset +1 h)
    The system time was changed to daylight saving time; in other words an hour was added. You can see the current system time at the top right in the selection area of the WBM. The current time including daylight saving time is displayed in the "System Time" box.
  - inactive (offset +0 h)
    The current system time is not changed.
- **NTP Server Address**
  Enter the IP address or the FQDN (Fully Qualified Domain Name) of the NTP server.
- **NTP Server Port**
  Enter the port of the NTP server.
  The following ports are possible:
  - 123 (standard port)
  - 1025 to 36564
- **Poll Interval[s]**
  In this field, enter the interval between two time queries (query interval) in seconds. Possible values are 64 to 1024 seconds.

Procedure

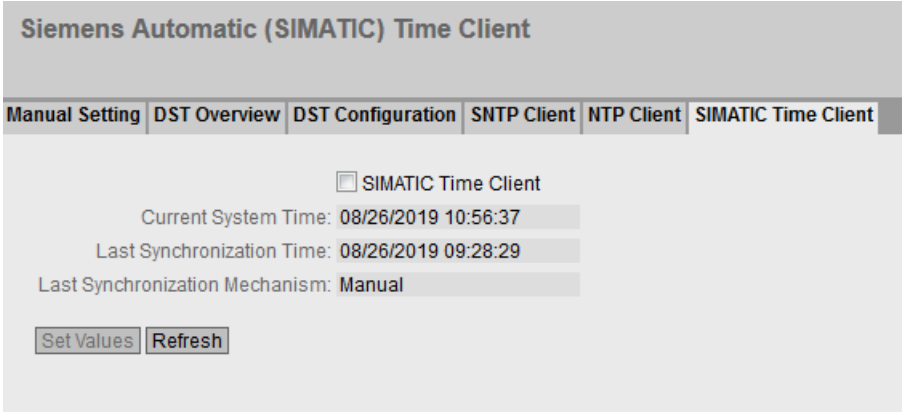
1. Click the "NTP Client" check box to enable the automatic time setting using NTP.
2. Enter the necessary values in the following boxes:
   - Time zone
   - IP address or FQDN of the NTP server
   - NTP Server Port
   - Query interval
3. Click the "Set Values" button.

6.4.12.6 SIMATIC Time Client

Time setting via SIMATIC time client

Note

To avoid time jumps, make sure that there is only one time server in the network.



Description

The page contains the following boxes:

- **SIMATIC Time Client**
  Select this check box to enable the device as a SIMATIC time client.
- **Current System Time**
  Shows the current system time.

- **Last Synchronization Time**
  Shows when the last time-of-day synchronization took place.
- **Last Synchronization Mechanism**
  Shows how the last time synchronization was performed. The following methods are possible:
  - Not set
    The time was not set.
  - Manual
    Manual time setting
  - SNTP
    Automatic time-of-day synchronization with SNTP
  - NTP
    Automatic time-of-day synchronization with NTP
  - SIMATIC
    Automatic time-of-day synchronization using the SIMATIC time frame

Procedure

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

6.4.13 Auto Logout

Setting the automatic logout

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

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

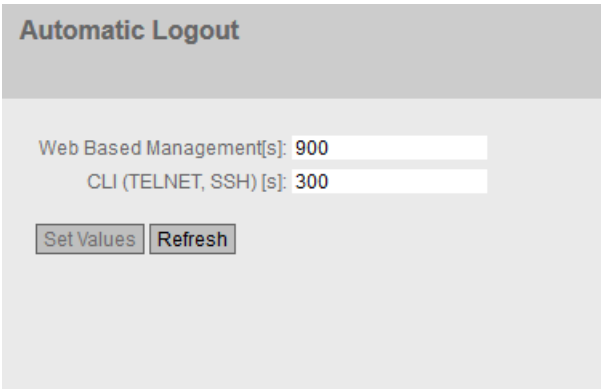
Note

No automatic logout from the CLI

If the connection is not terminated after the set time, check the "Keep alive" setting on the Telnet client.

If the interval for "Keep alive" is shorter than the configured time, the connection is maintained although no user data is transferred. You have set, for example, 300 seconds for the automatic logoff and the "Keep alive" function is set to 120 seconds. In this case, a packet is sent every 120 seconds that keeps the connection uninterrupted.

- Turn off the "Keep alive" (interval time=0)
  or
- Set the interval high enough so that the underlying connection is terminated when there is inactivity.



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.

6.4.14 Syslog Client

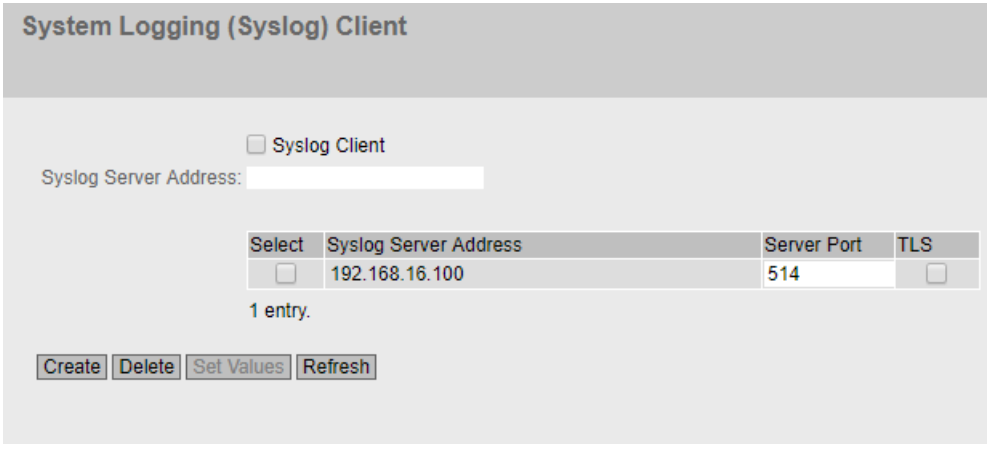
System event agent

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 (Fully Qualified Domain Name) of the Syslog server is entered on the device.



Description

The page contains the following boxes:

- **Syslog Client**
  Enable or disable the Syslog function.
- **Syslog Server Address**
  Enter the IP address, the FQDN (Fully Qualified Domain Name) or the host name of the Syslog server.

This table contains the following columns

- **Select**
  Select the row you want to delete.
- **Syslog Server Address**
  Shows the IP address, the FQDN (Fully Qualified Domain Name) or the host name of the Syslog server.
- **Server Port**
  Enter the port of the Syslog server being used.
- **TLS**
  When this check box is selected, communication with the Syslog server is encrypted.

Procedure

Enabling function

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

Creating a new entry

1. In the "Syslog Server Address" text box, enter the IP address, the FQDN or the host 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.

6.4.15 Fault Monitoring

6.4.15.1 Power Supply

Settings for monitoring the power supply

Configure whether or not the power supply should be monitored by the messaging system. Depending on the hardware variant, there are one or two power connectors (Supply 1 / Supply 2) and a PoE power supply. With a redundant power supply, configure the monitoring separately for each individual feed-in line.

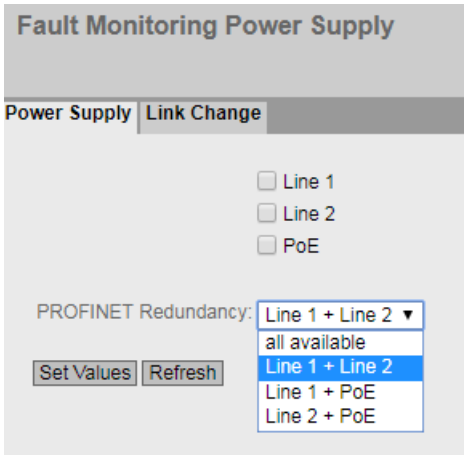
A fault is then signaled by the message system when there is no power on a monitored connection (Power Line 1, Power Line 2 or PoE) or when the applied voltage is too low.

Note

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

If a fault occurs, the error LED lights up on the device. The currently pending fault is displayed under "Information > Faults".

In addition, the corresponding error message is entered in the result log table. The content of the event log table is displayed in "Information > Log Tables > Event Log".



Procedure

1. Click the check box in front of the line name you want to monitor to enable or disable the monitoring function.
2. From the "PROFINET Redundancy" drop-down list, select the desired entry for redundant power supply to be monitored by PROFINET.
3. Click the "Set Values" button.

6.4.15.2 Link Change

Configuration of fault monitoring of status changes on connections

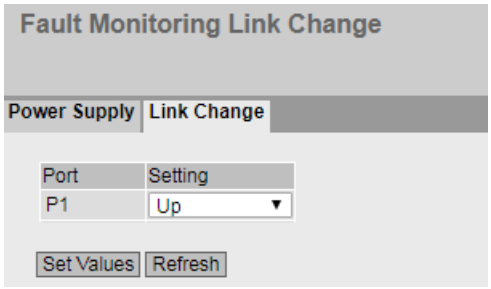
On this page, you configure whether or not an error message is triggered if there is a status change on a network connection.

If connection monitoring is enabled, an error is signaled

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

If a fault occurs, the error LED lights up on the device. The currently pending fault is displayed under "Information > Faults".

In addition, the corresponding error message is entered in the result log table. The content of the event log table is displayed in "Information > Log Tables > Event Log".



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

Configure error monitoring for a port

1. From the relevant drop-down list, select the options of the slots / ports whose connection status you want to monitor.
2. Click the "Set Values" button.

Configure error monitoring for all ports

1. Select the required setting from the drop-down list of the "Setting" column.
2. Click the "Copy to Table" button. The setting is adopted for all ports of table 2.
3. Click the "Set Values" button.

6.4.16 PROFINET

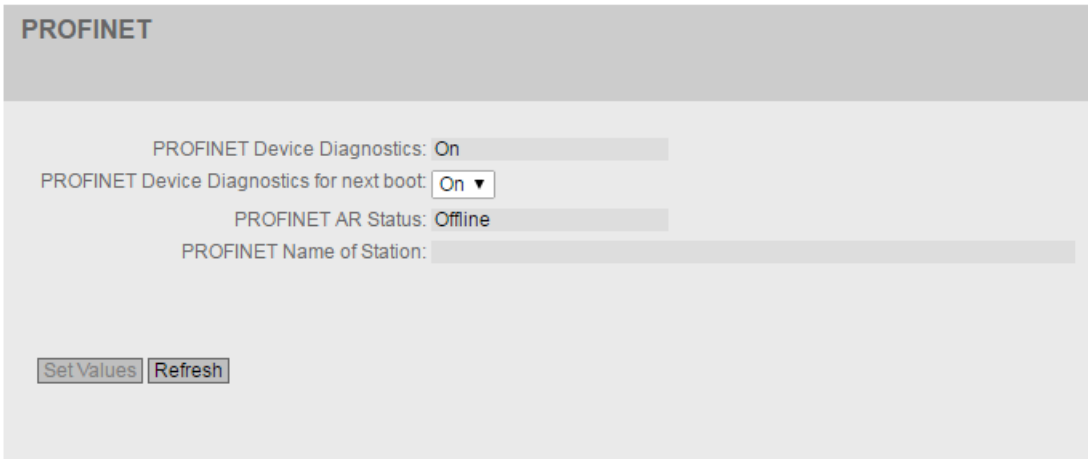
Settings for PROFINET

This page shows the PROFINET AR status and the device name.

Note

GSDML-configuration file: Mode Type

The GSDML configuration file can be used to configure the transfer mode for the Ethernet port. The SCALANCE WxM76x supports only the "Autonegotiation" setting.



Description

The page contains the following boxes:

- **PROFINET Device Diagnostics**
  Shows whether PROFINET is enabled ("On") or disabled ("Off").
- **PROFINET runtime mode for next boot**
  Set whether PROFINET will be enabled ("On") or disabled ("Off") after the next device restart.

  Note

  PROFINET AR Status

  If a PROFINET connection is established; in other words the PROFINET AR status is "Online", you cannot disable PROFINET.

- **PROFINET AR Status**
  This box shows the status of the PROFINET connection; in other words whether the device is connected to a PROFINET 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 via the PROFINET controller cannot be configured.
- **PROFINET Name of Station**
  This box displays the PROFINET device name according to the configuration in HW Config of STEP 7 or via the CLI with the `pnio station-name` command.

6.4.17 PLUG

6.4.17.1 Configuration

NOTICE
Do not remove or insert the PLUG during operation. A PLUG may only be removed or inserted when the device is turned off. The device checks whether a PLUG is inserted at one second intervals. If it is detected that the PLUG has been removed, the device restarts. If a valid PLUG license 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 license, 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 PLUG configuration

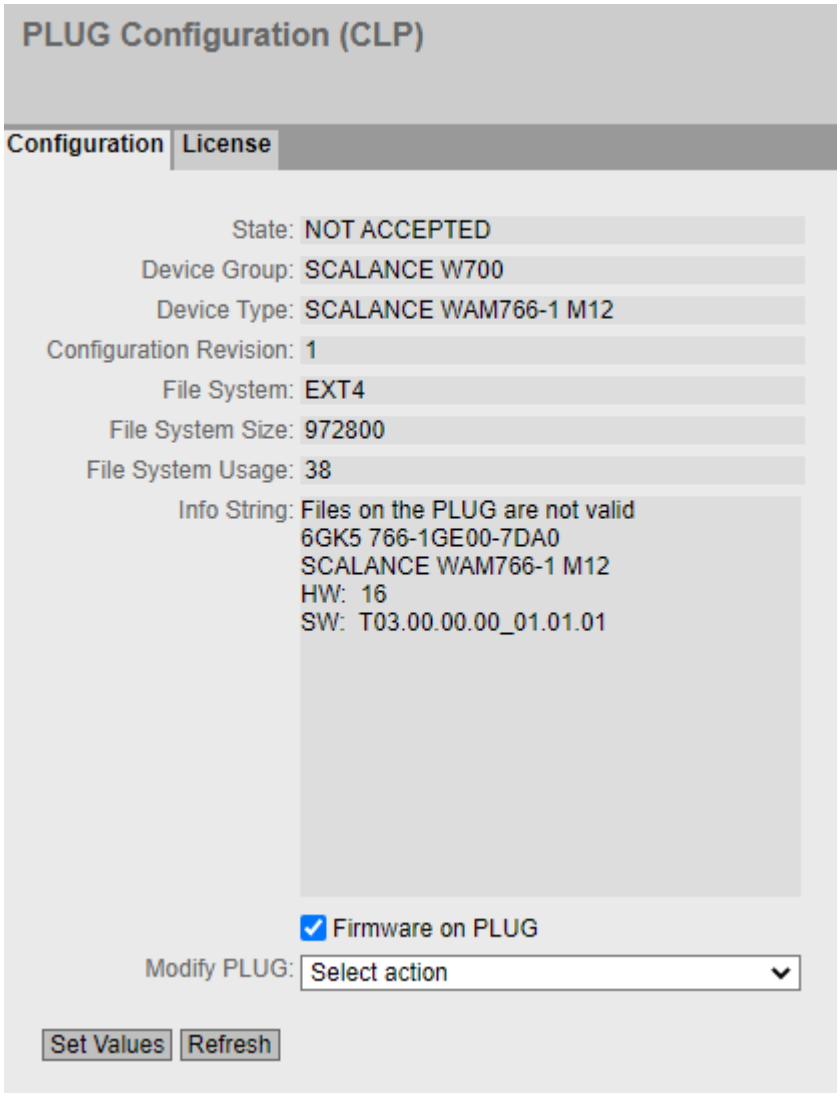
This page provides detailed information about the configuration stored on the PLUG. It is also possible to reset the PLUG to "factory defaults" or to load it with new contents.

Note

The action is only executed after you click the "Set Values" button.

The action cannot be undone.

If you decide against executing the function after making your selection, click the "Refresh" button. As a result the data of this page is read from the device again and the selection is canceled.


PLUG Configuration (CLP)
Configuration
License
State: NOT ACCEPTED
Device Group: SCALANCE W700
Device Type: SCALANCE WAM766-1 M12
Configuration Revision: 1
File System: EXT4
File System Size: 972800
File System Usage: 38
Info String: Files on the PLUG are not valid
6GK5 766-1GE00-7DA0
SCALANCE WAM766-1 M12
HW: 16
SW: T03.00.00.00_01.01.01
Firmware on PLUG
Modify PLUG: Select action
Set Values
Refresh

Description

The table has the following rows:

- **State**
  Shows the status of the PLUG. The following are possible:
  - ACCEPTED
    There is a PLUG with a valid and suitable configuration in the device.
  - NOT ACCEPTED
    Invalid or incompatible configuration on the inserted PLUG.
  - NOT PRESENT
    No PLUG is inserted in the device.
  - FACTORY
    PLUG is inserted and does not contain a configuration. This status is also displayed when the PLUG was formatted during operation.
- **Device Group**
  Shows the SIMATIC NET product line that used the PLUG previously.
- **Device Type**
  Shows the device type within the product line that used the PLUG previously.
- **Configuration Revision**
  The version of the configuration structure. This information relates to the configuration options supported by the device and has nothing to do with the concrete hardware configuration. This revision information does not therefore change if you add or remove additional components (modules or extenders), it can, however, change if you update the firmware.
- **File System**
  Displays the type of file system on the PLUG.
- **File System Size [Kilobytes]**
  Displays the maximum storage capacity of the file system on the PLUG.
- **File System Usage [Kilobytes]**
  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, article number, type designation, and the versions of the hardware and software. The displayed software version corresponds to the version in which the configuration was last changed. With the "NOT ACCEPTED" status, further information on the cause of the problem is displayed.
  If a PLUG was configured as a PRESET PLUG this is shown here as additional information in the first row. For more detailed information on creating and using a PRESET PLUG refer to the section "Maintenance (Page 313)".

- **Firmware on PLUG**
  The setting is enabled by default.
  When enabled, the firmware will be stored on the PLUG. This means that automatic firmware updates/downgrades can be made with the PLUG. The "Info String" box shows whether or not the firmware is stored on the PLUG. You can find more information on this in the section "Configuration License PLUG (CLP) (Page 29)".
- **Modify PLUG**
  Select the required setting from the drop-down list. You have the following options for changing the configuration on the 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 data from the PLUG and performs low-level formatting.

Procedure

Requirement:

- User with administrator rights

Modifying the PLUG configuration

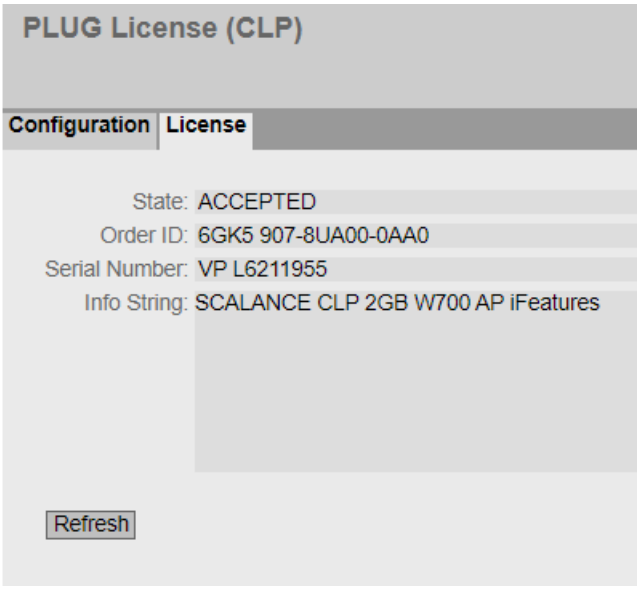
1. Select the required option from the "Modify PLUG" drop-down list.
2. Click the "Set Values" button.

6.4.17.2 License

NOTICE
Do not remove or insert the PLUG during operation. A PLUG may only be removed or inserted when the device is turned off. The device checks whether a PLUG is inserted at one second intervals. If it is detected that the PLUG has been removed, the device restarts. If a valid PLUG license 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 license, the device can no longer be used without this PLUG. To be able to use the device again, reset the device to the factory settings.

Information about the license of the PLUG

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



Description of the displayed boxes

- **State**
  Shows the status of the PLUG license. The following are possible:
  - ACCEPTED
    The PLUG in the device contains a suitable and valid license.
  - NOT ACCEPTED
    The license of the inserted PLUG is not valid
  - NOT PRESENT
    No PLUG is inserted in the device.
  - MISSING
    There is no PLUG inserted. Functions are configured on the device for which a license is required.
  - WRONG
    The inserted PLUG is not suitable for the device.
  - UNKNOWN
    Unknown content of the PLUG license.
  - DEFECTIVE
    The content of the PLUG license contains errors.
- **Article number**
  Shows the article number of the PLUG. The PLUG is available for various functional enhancements and for various target systems.

- **Serial number**
  Shows the serial number of the PLUG.
- **Info String**
  Displays additional information about the PLUG.

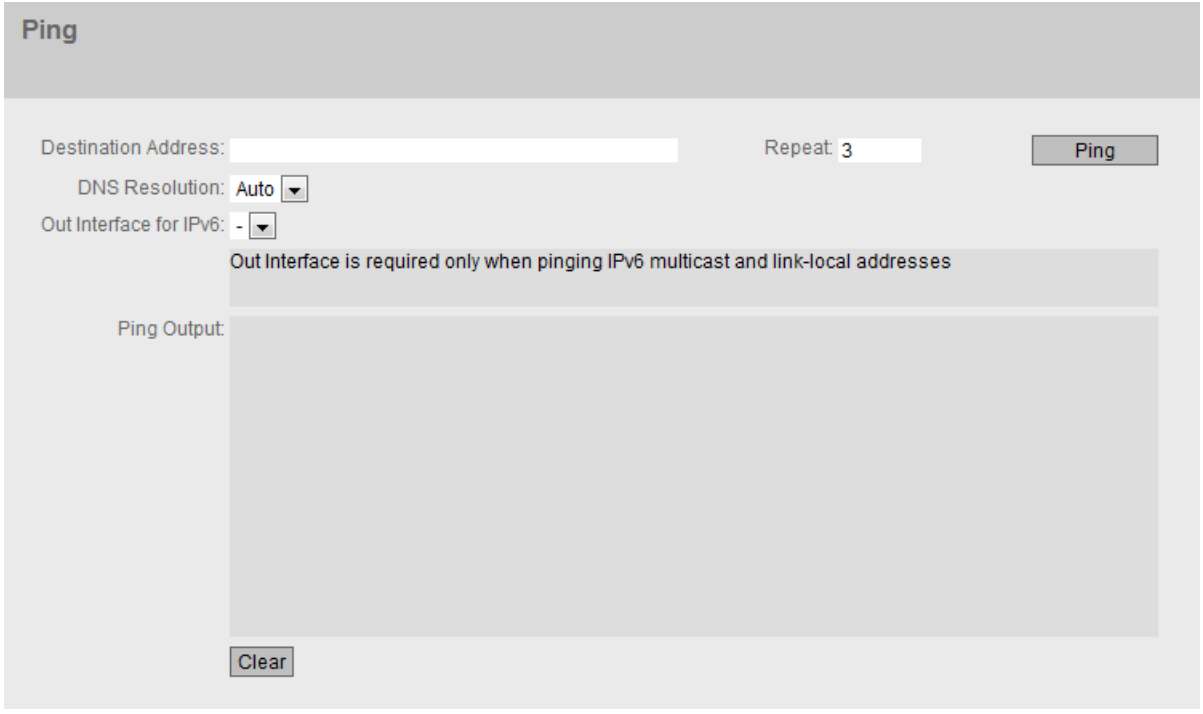
Note

When you save the configuration, the information about whether or not a PLUG was inserted in the device at the time is also saved. This configuration is then only executable, if a PLUG with the same article number / license is plugged in. This applies regardless of whether or not iFeatures are configured.

6.4.18 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.



Description

The page contains the following boxes:

- **Destination Address**
  Enter the IPv4, IPv6 address or the FQDN (Fully Qualified Domain Name) of the device.
- **Repeat**
  Enter the number of Ping requests.
- **DNS Resolution**
  Select the IP address type in which an entered FQDN will be resolved.
  - Auto
    In this mode, the IP address type is selected automatically.
  - IPv4
    The entered FQDN will be resolved in an IPv4 address.
  - IPv6
    The entered FQDN will be resolved in an IPv6 address.
- **Out Interface for IPv6**
  This selection is only required when the destination address is a multicast or a link local address.
  - "-" (factory setting)
  - Select the relevant IPv6 interface.
- **Ping**
  Click this button to start the Ping function.
- **Ping Output**
  This box shows the output of the Ping function.
- **Clear**
  Click this button to delete the ping output.

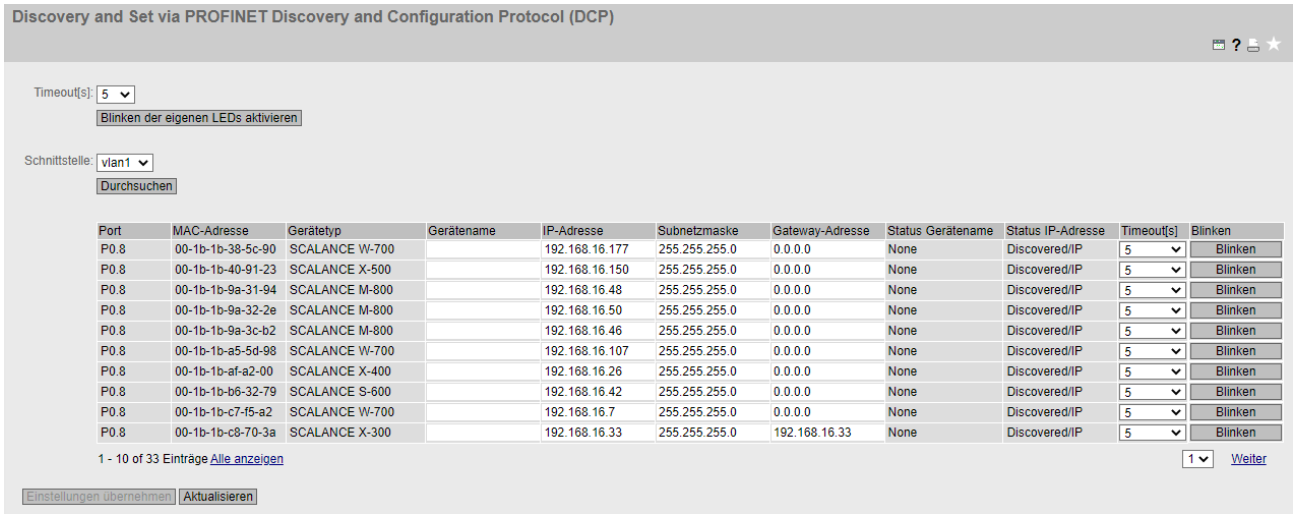
6.4.19 DCP Discovery

On this page, you can select an interface and search for devices that are reachable via the interface and support DCP. DCP Discovery only searches for devices located in the same subnet as the interface. The reachable devices are listed in a table. In the table you can check and adapt the network parameters of the devices. To identify and configure the devices the Discovery Configuration Protocol (DCP) is used.

Note

DCP Discovery

The function is only available with the VLAN associated with the TIA interface. You can configure the TIA interface with "Layer 3 > Subnets > Configuration".



Requirement:

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

On SCALANCE devices, you configure access under "System > Configuration".

Description

The page contains the following boxes:

- **Timeout[s]**
  Specify the time for flashing. When the time elapses, flashing stops.
- **Blink Own LEDs**
  Makes the LEDs of your own device flash.
- **Interface**
  Select the required interface.
- **Discover**
  Starts the search for devices reachable via the selected interface.
  On completion of the search the reachable devices are listed in the table. The table is limited to 100 entries.

The table has the following columns:

- **Port**
  Shows the port via which the device can be reached.
- **MAC Address**
  Shows the MAC address of the device.
- **Device Type**
  Shows the product line or product group to which the device belongs.
- **Device Name**
  Adapt the PROFINET device name if necessary.
  The device name must be DNS-compliant. If the device name is not used, the box is empty.

- **IP Address**
  If necessary, adapt the IPv4 address of the device.
  The IPv4 address should be unique within your network and should match the network. The IPv4 address 0.0.0.0 means that no IPv4 address has yet been set.
- **Subnet mask**
  If necessary, adapt the subnet mask of the device.
- **Gateway Address**
  Adapt the IPv4 address of the gateway if necessary.
- **Status Device Name**
  - None: The device name is not used.
  - Discovered: The set device name is used.
  - Configured: The device was assigned a new device name.
- **IP Status**
  - Discovered/IP: The device uses a static IPv4 address.
  - Discovered/DHCP: The device has obtained the IPv4 address from a DHCP server.
  - Configured: The device was assigned a new IPv4 address.
- **Timeout[s]**
  Specify the time for flashing. When the time elapses, flashing stops.
- **Flash**
  Makes the LEDs of the selected device flash.

Procedure

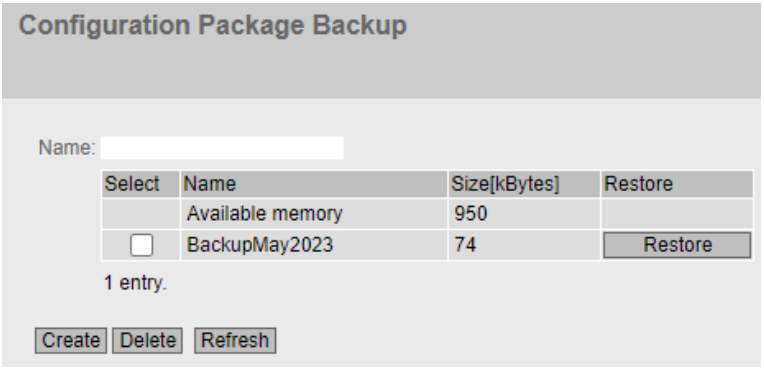
1. Select the TIA interface.
2. To show all devices that can be reached via the TIA interface, click the "Browse" button.
3. Adapt the desired properties.
4. Click the "Set Values" button.
   The status of the modified properties changes to "Configured".
5. To ensure that the properties were applied correctly, click the "Browse" button again.
   The status of the modified properties changes to "Discovered".

6.4.20 Configuration Backup

Backup

On this page, you can create backups of the configuration and save them on the device. The backups are created in "ConfigPack" format and include users with passwords, certificates and favorites in addition to the configuration. You can restore these backups directly from the device. After the restore, the device restarts. The maximum number depends on the size of the backup and the available memory space.

On the "System > Load&Save > HTTP/TFTP/SFTP" page, you can save the created backups in ZIP format under "ConfigPackBackup" on your client PC to be able to load them from there later. You can find more detailed information in the section "Load & Save (Page 131)".



Description

The page contains the following boxes:

- **Name**
  Enter a name for the backup.

The table contains the following columns:

- **Select**
  Select the row you want to delete.
- **Name**
  Shows the name of the backup.
- **Size [KB]**
  The first row "Available memory" shows how much memory is available for backups on the device. When you create a backup, the available memory space is reduced accordingly. The other rows show the size of each backup.
- **Restore**
  Click the "Restore" button to load the relevant backup on the device.

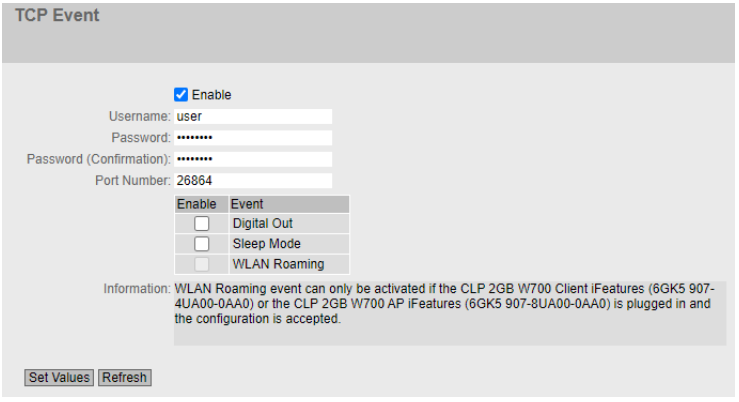
Procedure

1. Enter the required name.
2. Click the "Create" button.
   The current configuration is saved as a configuration backup.
   Saving the backup may take some time. A new row is created for the backup. The size of the backup is displayed and subtracted from the available memory space.

6.4.21 TCP event

On this page, you can enable the "TCP Event" function. After enabling, the device waits for incoming TCP packets on the configured port. These TCP packets can be used to trigger the "Sleep Mode" function or to initiate a roaming operation on the client. You can also switch the digital output on or off. Authorization is performed by comparing the user data.

If the incoming TCP packet contains comformant data, the command contained in it is executed.



Format of the TCP packet

The command is sent in a TCP packet that conforms to the following format:

`<User name>#<Password>#<command code>#<command string>:`

The `<command code>` parameter specifies the TCP event. The following values are possible:

- 106 Digital Out
- 107 Sleep Mode
- 109 WLAN Roaming (client only)

You specify the parameters of the TCP event in the command string `<command string>`. The parameters are separated by semicolons and ended with a colon.

Note

Permitted characters for user name and password

The following characters are permitted:

- 0123456789
- A...Z a...z
- . -_

Additionally allowed in the password:

- Space
- ! " % & / ( ) = ? * + < > ' ,

Requirements for using the TCP event "WLAN Roaming"

- The TCP event "WLAN Roaming" is only available with an inserted CLP iFeatures. You will find further information on this in the configuration manual, section "Description > CLP (Page 29)".
- The TCP event "WLAN Roaming" is configurable in client mode.

Description

The page contains the following:

- **Enable**
  Enable or disable reception of the TCP packets. To log this, activate the "TCP Event Log" event under "System > Event".
- **Username**
  Enter the user name to check the reception of the TCP packet. The user name and password are entered in the TCP packet.
- **Password**
  Enter the password belonging to the user name.
- **Password (Confirmation)**
  Repeat the password to confirm it.
- **Port number**
  Define the port at which the device waits for the TCP packets. The standard port 26864 is preset, or you can enter a port number in the range 1 ... 65535.

Note

Reserved ports

Some ports are permanently reserved. Make sure that the specified port is not already in use. You can find the ports used in the "List of available services (Page 19)".

The table contains the following columns:

- **Enable**
  Enable or disable the event.
- **Event**
  - Digital Out
    Switch the digital output on or off. The digital output is reset on restart (switched off).
    `<User name>#<Password>#106#<(1,2)>:`
    The last parameter specifies the sequence number: 1 (switch on) or 2 (switch off).
    Power on:
    `<User name>#<Password>#106#1:`
    Power off:
    `<User name>#<Password>#106#2:`

    Note

    Retaining the state of the digital output

    The device can note the current state of the digital output and restore it after a restart. You can find more information on the WBM page "System > Configuration".

  - Sleep Mode
    Trigger the "Sleep Mode" function:
    `<User name>#<Password>#107#1;<Time>:`
    The last parameter specifies the sleep time in minutes.
    In the following example, sleep mode is triggered for 10 minutes:
    `<User name>#<Password>#107#1;10:`

– WLAN Roaming (client only)
Control the roaming operation on the client via the TCP connection to enable faster roaming operations of the client:
`<User name>#<Password>#109#<command string>:`
The WLAN roaming behavior of the client is configured in the command string `<command string>`. The parameters are separated by semicolons and ended with a colon. They have the following order:
`<Frequency band>;<Channel (Channel number)>;<Execution Time>;<BSSID>;<Threshold>:`

Parameter	Description	Range of values/note
`Frequency band`	Frequency band	2 = 2.4 GHz 5 = 5 GHz
`Channel (Channel number)`	Channel number	Enter the channel number e.g. 36 Range of values 1 to 233
`Execution Time`	Execution time	0 = Decision by client when it uses the channel/BSSID 1 = Immediate roaming
`BSSID`	MAC address of an AP to which the client has to roam	Enter the MAC address of the associated VAP of the access point, e.g. d4-f5-27-b9-d4-88. You can find the MAC address in the list of available access points on the page "Information > WLAN > Available AP (Page 106)". When 00-00-00-00-00-00 is entered, no AP is defined and the client starts the search for available APs
`Threshold`	Optional parameter (dBm) No function in V2.0	0 = Not used

Example of a command string:
`myusername#mypassword#109#5;36;1;d4-f5-27-b9-d4-88;0:`

Conditions for WLAN roaming via TCP event

WLAN roaming can be initiated when the following conditions are met:

- The frequency band in the command string matches the frequency band currently configured on the device.
- The channel number is in the frequency band configured on the device and this channel is available in the configuration.
- The client is connected to an access point when the TCP event command is received.
- The client is not currently connected to the access point that has the specified BSSID.

If WLAN roaming fails, this event is logged.

Note

Identical WLAN configuration of the access points for WLAN roaming via TCP event required

For problem-free WLAN roaming via TCP, all access points must have identical configuration of the WLAN interface or the VAP (frequency band, SSID, WLAN mode, channel bandwidth, security, DFS).

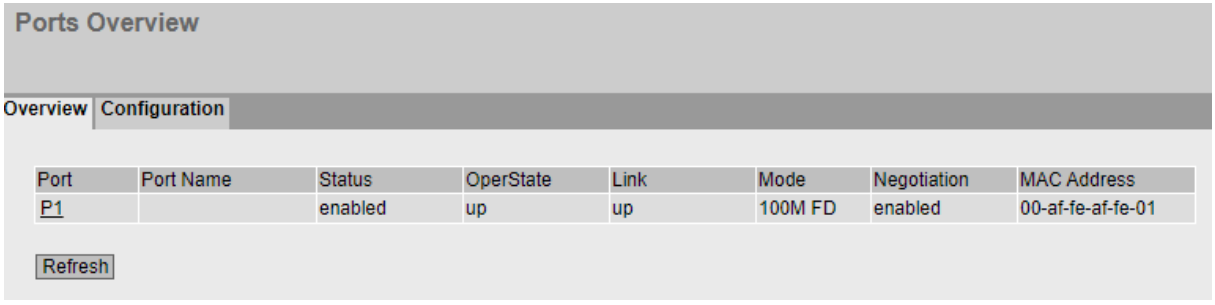
6.5 "Interfaces" menu

6.5.1 Ethernet

6.5.1.1 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.



Description

The table has the following columns:

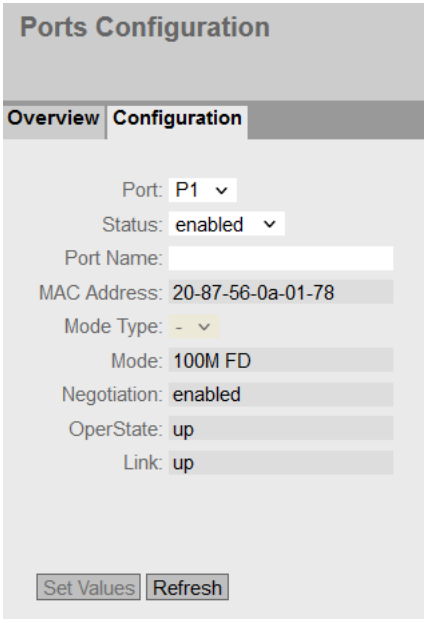
- **Port**
  Shows the configurable ports. If you click on the link, the corresponding configuration page is opened.
- **Port name**
  Shows the name of the port.
- **State**
  Shows whether the port is on or off. Data traffic is possible only over an enabled port.

- **OperState**
  Displays the current operational status. The operational status depends on the configured "Status" and the "Link".
  The available options are as follows:
  - up
    You have configured the status "enabled" for the port and the port has a valid connection to the network.
  - down
    You have configured the status "disabled" or "Link down" for the port or the port has no connection.
- **Link**
  Shows the connection status to the network. With the connection status, the following is possible:
  - up
    The port has a valid link to the network, a link integrity signal is being received.
  - down
    The link is down, for example because the connected device is turned off.
- **Mode**
  Shows the transfer parameters of the port.
- **Negotiation**
  Shows whether the automatic configuration is enabled or disabled.
- **MAC Address**
  Shows the MAC address of the port.

6.5.1.2 Configuration

Configuring ports

With this page, you configure the Ethernet ports of the device.



Description

The table has the following rows:

- **Port**
  Select the port to be configured from the drop-down list.
- **State**
  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.
- **Port name**
  Enter a name for the port.
- **MAC Address**
  Shows the MAC address of the port.

- **Mode Type**
  The operating mode is set to "Auto negotiation". In this case, the parameters are negotiated automatically with the connected terminal device. This must also be in the "Auto negotiation" mode for this purpose.

  Note

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

- **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.
- **OperState**
  Displays the current operational status. The operational status depends on the configured "Status" and the "Link". The available options are as follows:
  - up
    You have configured the status "enabled" for the port and the port has a valid connection to the network.
  - down
    You have configured the status "disabled" or "Link down" for the port or the port has no connection.
- **Link**
  Shows the connection status to the network. 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.

Procedure

Note

Changing the port configuration

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.

To change the configuration of a port, follow these steps:

1. Click the appropriate box to change the configuration.
2. Click the "Set Values" button.

6.5.2 WLAN

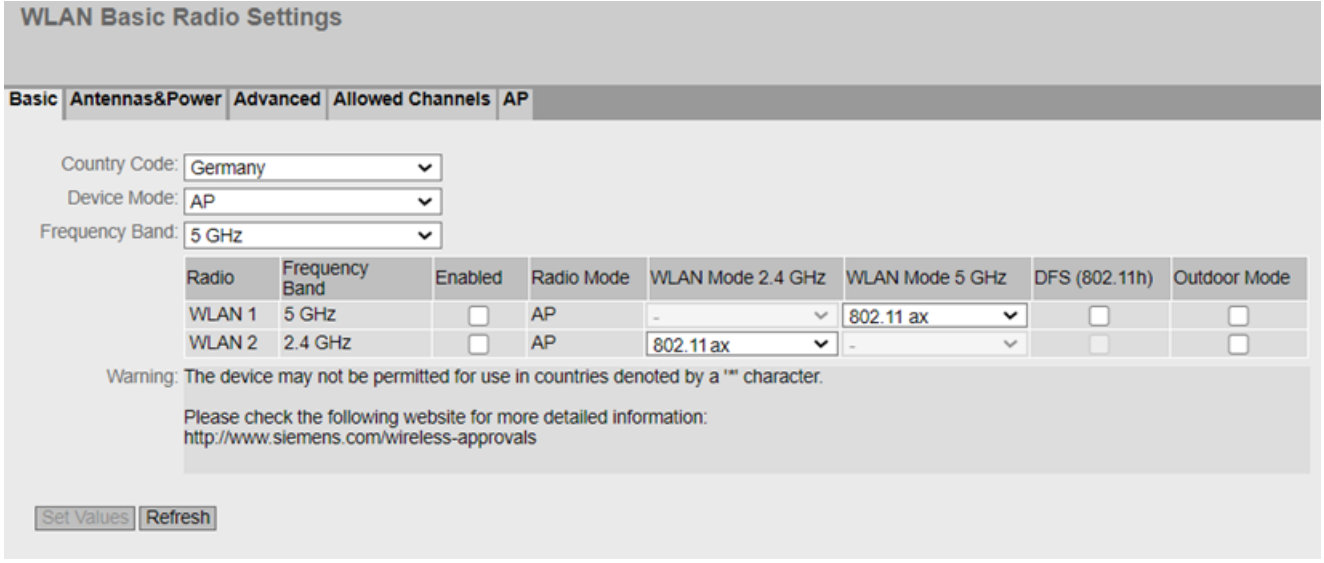
6.5.2.1 Basic

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.



Description

- **Country Code**
  Select the country in which the device will be operated from the drop-down list.
  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.
  You can find more information on currently available country approvals in the "Approvals SCALANCE W700 802.11ax (https://support.industry.siemens.com/cs/ww/en/view/109802595)" documentation.

  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**
  Select the mode of the device. This selection is available only for access points.
  The following modes are possible:

  – AP - Access point mode

  – Client - Client mode

  Note

  After the mode is changed, a message is displayed. If you confirm the message with "OK", the device is reset to the memory defaults (protected settings) and restarted in the selected mode.

  If the device has restarted, you will need to log in again to be able to continue the configuration.

- **Frequency Band**
  Set frequency band with which the device operates.

  – 2.4 GHz

  – 5 GHz

  – 2.4 GHz + 5 GHz
    Dual operation in access point mode. The prerequisite is that CLP 2GB W700 AP iFeatures is plugged in and accepted. Simultaneous configuration, for example via the CLI or SNMP, can lead to inconsistencies in the web-based management.
    If you switch to the "2.4 GHz + 5 GHz" setting (dual mode), all settings for antennas on the "Antennas&Cable" tab are set to "Not defined".

    Note

    iFeatures in dual mode

    When using iFeatures iPCF-2 or iPRP on a WLAN interface, the other WLAN interface must be operated as standard WLAN.

The table has the following columns:

- **Radio**
  Shows the available WLAN interfaces.
- **Frequency Band** (Only in access point mode)
  Shows the frequency band.
  - 2.4 GHz
  - 5 GHz
- **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 in delivery state. The WLAN interfaces are can be enabled once the country and the antenna settings are configured. In the client or in client mode, at least one SSID must be configured and enabled in addition.

  In Access Point mode only:

  Dual mode of the WLAN interface with 2.4 GHz and 5 GHz is only possible if the following prerequisites are met:
  - a CLP 2GB W700 AP iFeatures is plugged in.
  - the frequency band "2.4 GHz + 5 GHz" is set and
  - the antennas are configured under "Antennas&Cable".
- **Radio Mode**
  Shows the mode of the WLAN interface.

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

  Note

  iPCF-2 after WLAN mode change

  If the transmission standard is changed from 802.11ax to another transmission standard, the enabled iPCF-2 mode is disabled. A message to this effect is displayed.

  – Auto (in client mode only)
    The transmission standard is determined automatically (2.4 GHz and 5 GHz).
  – 802.11g
    The transmission standard IEEE 802.11g (2.4 GHz) is set. This transmission standard is downwards compatible with IEEE 802.11b.
  – 802.11n
    The transmission standard IEEE 802.11n (2.4 GHz and 5 GHz) is set. This transmission standard is downwards compatible with IEEE 802.11a and IEEE 802.11g.
  – 802.11a
    The transmission standard IEEE 802.11a (5 GHz) is set.
  – 802.11ac
    The transmission standard IEEE 802.11ac (5 GHz) is set.
  – 802.11ax
    The transmission standard IEEE 802.11ax (2.4 GHz and 5 GHz) is set.

  Note

  Data rate

  The data rate is adjusted automatically.

- **DFS (802.11h)**
  Enables or disables the "Dynamic Frequency Selection (DFS)" function.
  - Enabled
    With the DFS function, it is possible to also use the higher 5 Ghz channels.
    These channels are country-specific and are subject to certain DFS regulations. You can find additional information on this in the country-specific DFS documentation.
    Before the access point transmits over one of these channels, it checks for competing radar signals for 60 seconds according to the CAC (Channel Availability Check). The access point also does not send any beacons for the duration of the search. With weather radar channels (5.6 - 5.65 GHz), the duration of the search is 10 minutes.
    If no radar signals are detected after the search period has elapsed, the access point transmits on the channel. Otherwise, the access point changes channel and repeats the check.
    The access point also searches for radar signals continuously during operation.
    If the access point discovers a radar signal on the current channel, it notifies the clients of the channel change. It then automatically switches to an alternative DFS channel and the current channel is blocked for 30 minutes.
  - Disabled
    The DFS function is not used.
- **Outdoor Mode**
  - Enabled
    If you have enabled Outdoor Mode, only the channels that are permitted for outdoor operation are available to you.
  - Disabled
    If you have disabled Outdoor Mode, only the channels that are permitted for operation in a building are available to you.

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. From the "WLAN Mode" drop down list, select the required transmission standard for the configured frequency band.
4. Click the "Set Values" button.

6.5.2.2 Antennas&Power

Overview

The following figures provide an overview of the IWLAN antennas that are suitable for use with SCALANCE W devices.

Type of antenna	Frequency range (GHz)	Antennas		SCALANCE W780/W740	SCALANCE W760/W720, W770/W730	SCALANCE W770/W730 IP65	SCALANCE W1780/W1740	SCALANCE WAM766-1/ WUM766-1	SCALANCE WAM763-1/ WUM763-1
directional	2.4		ANT792-8DN	●			●	●	●
	5		ANT793-8DP	●	●	●	●*	●	●
			ANT793-8DJ	●	●	●	●*	●	●
			ANT793-8DK	●	●	●	●*	●	●
			ANT793-8DL	●	●	●	●*	●	●
RCoax	2.4		RCoax radiating cables 2.4 GHz	●	●	●	●	●	●
			ANT792-4DN	●	●	●	●	●	●
	5		RCoax radiating cables 5 GHz	●	●	●	●	●	●
			ANT793-4MN	●	●	●	●	●	●

G_IK10_XX_30317

*Antennas can only be used on one antenna connector per radio interface (R1A1 or R2A1) and the rest of the antenna connectors have to be fitted with a terminating resistor.

Type of antenna	Frequency range (GHz)	Antennas		SCALANCE W780/W740	SCALANCE W760/W720, W770/W730	SCALANCE W770/W730 IP65	SCALANCE W1780/W1740	SCALANCE WAM766-1/ WUM766-1	SCALANCE WAM763-1/ WUM763-1
omnidirectional	2.4		ANT792-6MN	●	●	●	●	●	●
	2.4 and 5		ANT795-4MA	●	●				●
			ANT795-4MB	●	●				●
			ANT795-4MC	●		●	●	●	
			ANT795-4MD	●		●	●	●	
			ANT795-4MX	●		●	●	●	
			ANT795-6MN	●	●	●	●	●	●
			ANT795-6MT	●			●		
			ANT795-6MP	●	●	●	●	●	●
Sector	2.4 and 5		ANT795-6DC	●	●	●	●	●	●
	5		ANT793-6DG	●	●	●	●	●	●

G_IK10_XX_30318

Configuration of external antennas

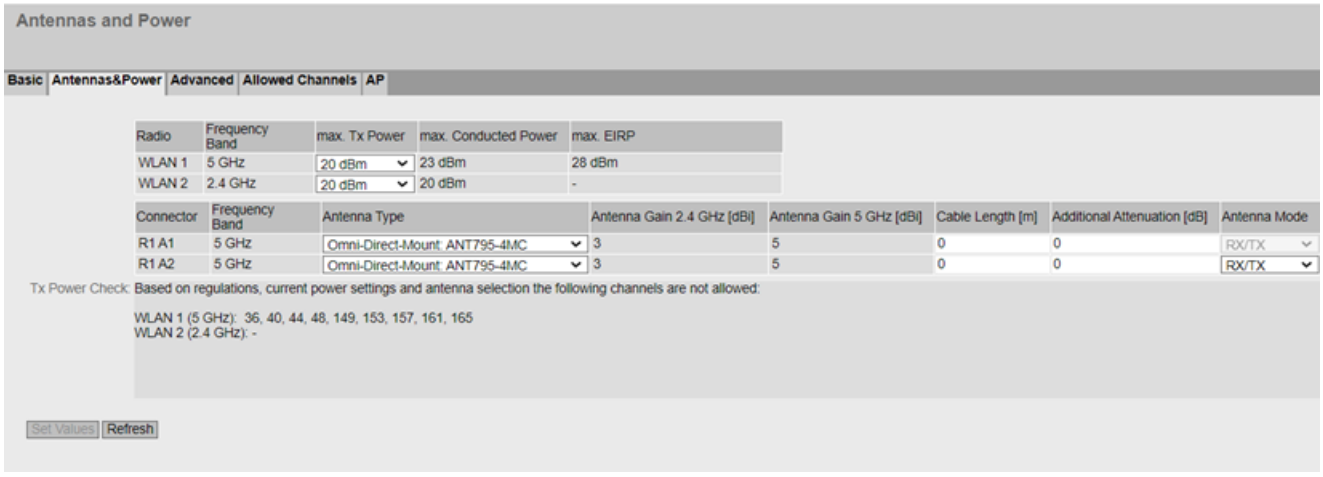
On this page, you configure the settings for the connected external antennas.

Note

50 Ω terminating resistor

Each WLAN interface has two antenna connections. Connectors that are not used must have a 50 Ω terminating resistor fitted.

An antenna must always be connected to the R1 A1 antenna connection as soon as the WLAN interface is switched on. If no antenna is connected, the relevant interface must also be disabled for Rx and Tx. Otherwise, there may be transmission disruptions.



Description

Table 1 has the following columns:

- **Radio**
  Shows the available WLAN interfaces.
- **Frequency Band** (only in access point mode)
  Shows the frequency band.
  - 2.4 GHz
  - 5 GHz
- **Max. Tx Power**
  The value you set here corresponds to the transmit power per antenna port. With transmit power greater than 15 dBm, the transmit speed may be reduced.

  Note

  The maximum possible transmit power varies depending on the channel and data rate. For more information on transmit power, refer to the documentation "Characteristics SCALANCE W700 801.11ax".

- **Max. conducted power**
  The value is the summed transmit power of all active antenna connections.
  The calculation is made according to the following scheme:
  - 1 antenna port
    max. Tx power = max. conducted power
  - 2 antenna connections
    max. Tx power + 3 dBm = max. conducted power
- **max. EIRP (Effective Isotropic Radiated Power)**
  Shows the current radiant power of the antenna, in relation to a non-directional antenna (isotrop).
  max. EIRP = max. conducted power + antenna gain – attenuation (antenna connections, cable length and additional attenuation)

Table 2 has the following columns:

- **Connector**
  Shows the name of the relevant antenna connector.
- **Frequency Band** (only in access point mode)
  Shows the frequency band.
  - 2.4 GHz
  - 5 GHz
  - 2.4 GHz + 5 GHz
    Dual mode in access point mode, only available when CLP 2GB W700 AP iFeatures is plugged in.
- **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 connector using a 50 Ω terminating resistor, select the entry "Not used (Connect 50 Ohm Termination)".
  Only dual-band antennas are available in dual mode. To simplify the configuration in the web-based management, an antenna interface is displayed and the configuration is applied to both logical interfaces.
  Mixed configuration via the CLI and web-based management is not recommended to avoid configuration inconsistencies.

  Note

  When you select an antenna, keep in mind:
  - The antennas with national approval for your device You can find additional information under Wireless approval (https://www.siemens.com/wireless-approvals).
  - The country-specific and channel-dependent maximum permissible antenna gain You can find additional information on this in the reference document "Approvals for SCALANCE W700 802.11ax".

- **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 connection R1 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	R1 A2
Rx/Tx	Rx/Tx
Rx/Tx	Rx
Rx/Tx	Tx
Rx/Tx	--[1)]

1) Antenna type "Not used (Connect 50 Ohm Termination)"

- **Tx power check**
  Indicates whether the settings that have been made will violate the permitted transmit power restrictions of the selected country. The calculated value of "max. EIRP" is checked to determine whether this value violates the transmit power restriction of specific channels in the set country. If "Use Allowed Channels only" is set, only the channels selected there are checked.

  Note

  If you use the setting "Auto" or DFS for channels, you need to exclude the channels that are not permitted using the "Allowed Channels" list.

  - Channel numbers
    Indicates the channels on which the current transmit power exceeds the maximum permitted transmit power.
  - "-"
    The channels can be used with the current settings.

Procedure

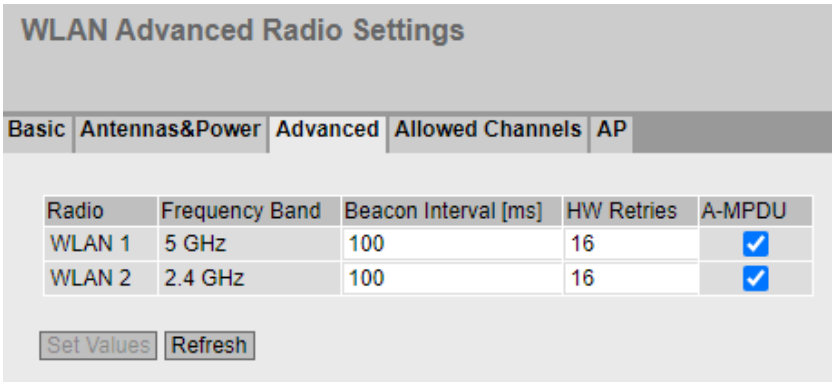
Follow these steps to configure both antenna connections:

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. The "Antenna mode" entry cannot be changed at antenna connection R1A1.
3. For the second antenna connection (R1 A2), select the appropriate type of the second antenna in the"Antenna Type" drop-down list and enter a value for "Cable length".
   If you terminate the second antenna connection using a 50 Ω terminating resistor, select the entry "Not used (Connect 50 Ohm Termination)".
4. Click the "Set Values" button.

6.5.2.3 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 SCALANCE W700 device cannot be used as it is intended with the default settings.



Description

The table has the following columns:

- **Radio**
  Shows the available WLAN interfaces in this column.
- **Frequency Band** (only in access point mode)
  Shows the frequency band.
  - 2.4 GHz
  - 5 GHz
- **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.

  Note

  Interval with more than 2 VAP interfaces

  With more than 2 VAP interfaces, use an interval greater than or equal to 100 ms.

- **HW Retries**
  Specify the number of hardware retries. The max. number of hardware retries is 32.
  The hardware retry is performed by the WLAN chip itself when it tries to repeat an unacknowledged packet immediately.
  If all hardware retries were unsuccessful, the packet is deleted and the WLAN client is removed from the list.

  Note

  Hardware retries after an update to V2.1

  If the number of hardware retries was set to more than 32 in an older firmware version, the value is automatically set to 32 after the update to V2.1. This information is recorded in the event log.

- **A-MPDU**
  Aggregated MAC Protocol Data Unit (A-MPDU)
  - Enabled
    Multiple MPDU frames with the same destination address are bundled and sent as one large A-MPDU. This allows the total throughput to be increased.
  - Disabled
    A-MPDU frames are received but not sent.

Procedure

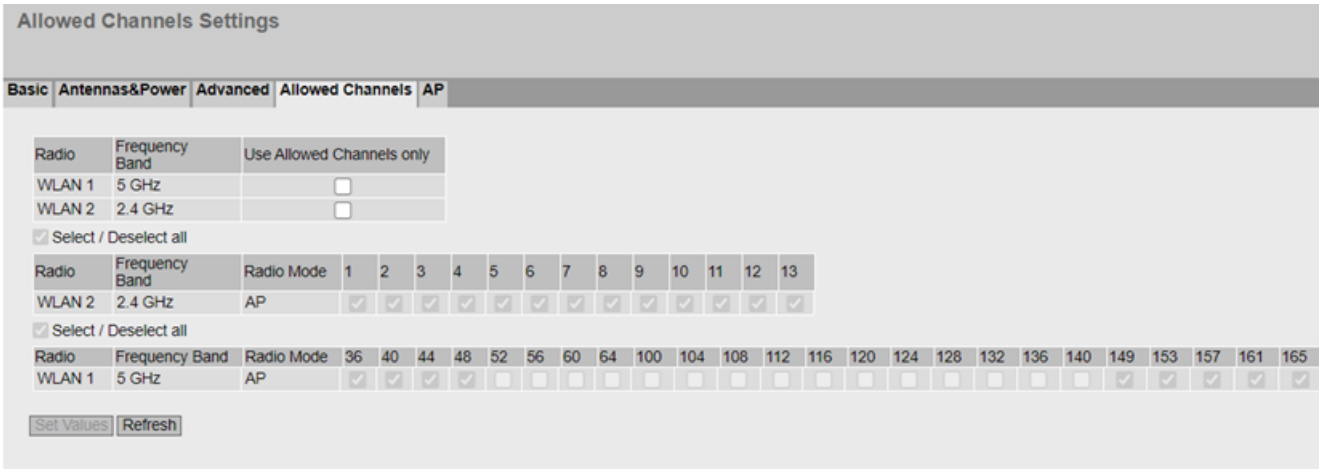
1. Enter the values to be set in the input boxes as follows.
2. Select the option checkmark of the required functions.
3. Click the "Set Values" button.

6.5.2.4 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.



Description

Table 1 contains the following columns:

- **Radio**
  Shows the available WLAN interfaces.
- **Frequency Band (only in access point mode)**
  Shows the frequency band.
  - 2.4 GHz
  - 5 GHz
- **Use Allowed Channels only**
  If you enable the option, you restrict the selection of channels via which the connection is established.
  In the following tables, you define which channels can be used to establish a wireless cell. 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.
- **Frequency Band**
  Shows the frequency band.
  - 2.4 GHz
  - 5 GHz
- **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. Select the "Use Allowed Channels only" option for the required WLAN interface.
2. Deselect the check box "Select / Deselect all".
3. Select the relevant check box for the required channel number.
4. Click the "Set Values" button.

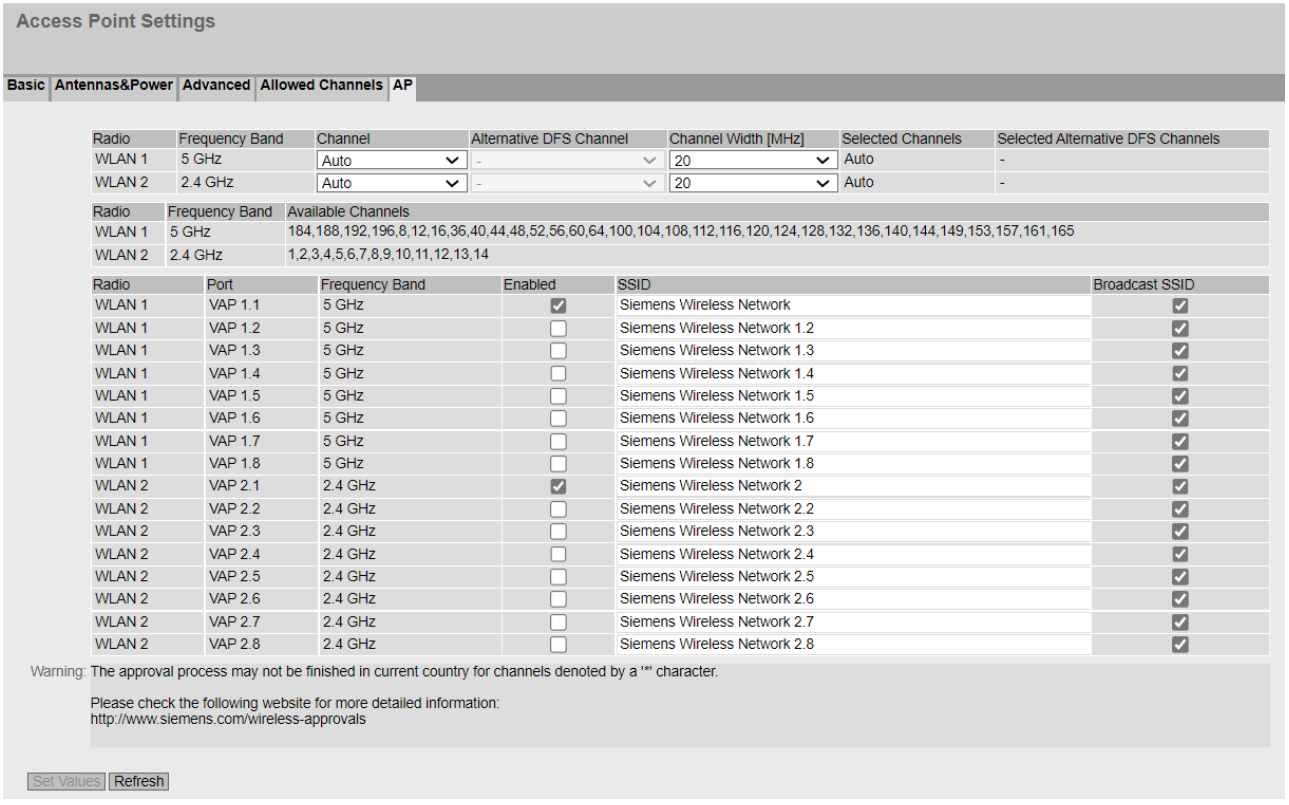
6.5.2.5 AP

Note

This WBM page is only available in access point mode.

Configuration

On this WBM page, you specify the configuration for the access point.



Description

Table 1 has the following columns:

- **Radio**
  Shows the available WLAN interfaces.
- **Frequency Band**
  Shows the frequency band.
  - 2.4 GHz
  - 5 GHz
- **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" page.
  .If you want to use a fixed channel, select the required channel from the drop-down list.

- **Alternative DFS Channel**
  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 competing radar signal 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.
- **Channel Width [MHz]**
  You can only specify the channel bandwidth for the IEEE 802.11n, IEEE 802.11ac and IEEE 802.11 ax transmission standards.
  The following settings are possible.
  - 20 MHz
  - 40 MHz

  Only with IEEE 802.11ac/ax:
  - 80 MHz
- **Selected Channels**
  - Channel number (frequency) or Auto
    When a fixed channel is set for "Channel", this channel is shown including frequency.
  - At 80 MHz only and with fixed channel: Channel range
    Four channels are required for the 80 MHz channel bandwidth in the corresponding channel range. The channel range consists of the channel configured for "Channel" and the three next channels.
- **Selected Alternative DFS Channels**
  - Channel number (frequency) or Auto
    When a fixed channel is set for "Alternative DFS Channel", this channel is shown including frequency.
  - At 80 MHz only and with fixed channel: Channel range
    Four channels are required for the 80 MHz channel bandwidth in the corresponding channel range. The channel range consists of the channel configured for "Channel" and the three next channels.

Table 2 has the following columns:

- **Radio**
  Shows the available WLAN interfaces.
- **Frequency Band**
  Shows the frequency band.
  - 2.4 GHz
  - 5 GHz
- **Available Channels**
  This box displays the permitted channels. The display depends on the wireless approvals of the currently selected country and the settings on the "Allowed Channels" page.

Table 3 has the following columns:

- **Radio**
  Shows the WLAN interface.
- **Port**
  Shows the VAP interface.
- **Frequency Band**
  Shows the frequency band.
  - 2.4 GHz
  - 5 GHz
- **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.
  - activated
    The SSID is sent in the Beacon frame of the access point and is visible for other devices.

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)/WPA3-SAE, if this is not possible WPA2-PSK) provides higher security. You must also expect that certain terminal devices may have problems with access to a hidden SSID.

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. For the relevant WLAN interface and the port, select the "Enabled" check box.
4. Click the "Set Values" button.

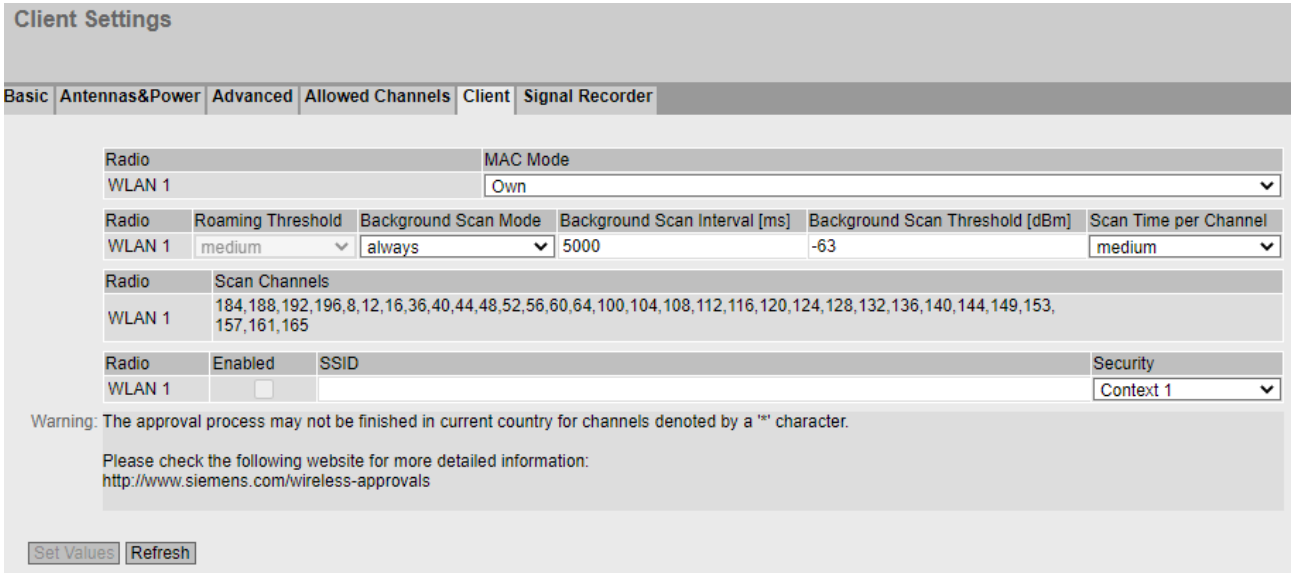
6.5.2.6 Client

Connecting to a network

On this WBM page, you can specify how the device connects to a network as client.

Note

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



Description

Table 1 has 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:
  - 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.

Table 2 has the following columns:

- **Radio**
  Shows the available WLAN interfaces.
- **Roaming Threshold**
  The client switches at a moderately 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.
  - Disabled
    As long as the client is connected, there is no scan for further access points.
    The client updates its scan list based on the beacons (management frames) that it has received on the current channel.
- **Background Scan Interval [ms]**
  Specify the interval at which further access points are scanned.
- **Background Scan Threshold [dBm]**
  Set the threshold value for the signal strength. If the threshold is undershot, the client searches for further access points.
  Range of values: -95 dBm to 0 dBm

  Note

  Set a higher background scan threshold

  Enter a somewhat higher value for the threshold than the signal strength at which the client starts scanning.

  Example: Roaming should take place at under -65 dBm. In this case, enter -63 dBm for the threshold.

- **Scan time per channel**
  Define the scan time per channel.
  There are three pre-defined settings for the scan time:
  - Short: Active scan time: 50 ms, passive scan time: 90 ms
  - Medium: Active scan time: 200 ms, passive scan time: 300 ms
  - Long: Active scan time: 300 ms, passive scan time: 800 ms

  You need to adapt the beacon interval accordingly on the access point. The beacon interval should be no more than half of the passive scan time.

Table 3 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 4 has the following columns:

- **Radio**
  Shows the WLAN interface.
- **Enabled**
  Enables or disables the relevant SSID.

- **SSID**
  Enter the SSID of the access point with which the client will connect.
  For the SSID, ASCII code 0x20 to 0x7e is used.
- **Security**
  Select a security context. You create and configure a security context in "Security > WLAN > Basic".
  Default setting: Context 1

Procedure

1. From the "MAC Mode" drop-down list, select the required assignment of the MAC address.
2. Select the desired mode from the "Background Scan Mode" drop-down list and set the background scan interval.
3. Select the required scan time from the "Scan Time per Channel" drop-down list.
4. In table 3, enter an SSID for "SSID".
5. Select a security context.
6. Enable the required SSID.
7. Click the "Set Values" button.

Note

Roaming

For problem-free roaming of the client between the access points, it is important not to block LLC (Link Layer Control) frames in the wired network. The LLC frames are used to update the FDB (Forwarding Database) table on the network devices.

6.5.2.7 Signal recorder

Recording the effective user signal

The signal recorder is used to record the effective user signal between access point and client. Using this data, you can locate areas with an inadequate user signal. The signal recorder can be particularly useful when the client moves along a fixed path.

Note

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

The WLAN interface of the device must be enabled; otherwise, no recording is possible.

Description

The display is divided into two areas.

- **Client**
  Represents the measurement of the client.
- **Access point**
  Displays the measurement of the access point with which the client is currently connected. This requires that the setting "Bidirectional Recording" is enabled. The access point sends its data to a maximum of 3 clients on which signal recorders are running. The access point data is not displayed on other clients.

Both areas each contain two graphics.

The first graphic contains the following elements:

- Scroll bar
  With the scroll bar, you can look through the entire measurement. To do this you can use the "<<" and ">>" buttons or the arrow keys on the keyboard.
- Bar (left)
  In the bar on the left, the wanted signal from the client / access point is displayed in real time according to the color scheme shown.

- Color scheme
  The range > -35 dBm (blue) is the overmodulation range, in other words the WLAN signal is too strong and is received overmodulated. As of approximately -60 dBm (yellow) the WLAN signal is weaker.
- x axis
  The x axis shows the course of the measurement in random samples and seconds.
- Measurement data
  - Client
    The measurement data shows the value of the effective user signal according to the color scheme shown. The gray line shows the background noise.
    If the client changes access points during a measurement (roaming) or reconnects, this is displayed by a vertical black line. On the line the new AP system name and the BSSID are shown.
    If during a measurement the client has no connection to an access point, no user signal is displayed. To make it clear that there is no connection to an access point, the BSSID is set to 00:00:00:00:00:00 and shown in red.
  - Access point
    The measurement data shows the value of the effective user signal according to the color scheme shown. The gray line shows the background noise.
    If the client changes access points during a measurement (roaming) or reconnects, this is displayed by a vertical black line.
    If the access point does not support the setting "Bidirectional Recording" no user signal is displayed

The second graphic contains the following elements:

- Bar (left)
  In the bar, only the percentage of failed transfer attempts is displayed according to the color scheme.
- Color scheme
  The color scheme goes from green to red and shows the values of failed transfer attempts.
  - Green (0%): All transfer attempts were successful.
  - Red (100%): All transfer attempts have failed.

- x axis
  The x axis shows the course of the measurement in random samples and seconds.
- Measurement data
  - Client
    The measurement data shows the transfer attempts according to the color scheme shown. The transfer attempts are shown as a bar. The data rate of the sent data packets is represented as a gray line.
    If the client changes access points during a measurement (roaming) or reconnects, this is displayed by a vertical black line.
  - Access point
    The measurement data shows the transfer attempts according to the color scheme shown. The transfer attempts are shown as a bar. The data rate of the sent data packets is represented as a gray line.
    If the client changes access points during a measurement (roaming) or reconnects, this is displayed by a vertical black line. If the access point does not support the "Bidirectional Recording" setting, no data is displayed.

Beside the graphics the following values are displayed:

- Status
  Shows whether or not the signal recorder is recording values.
- Current Sample
  The number of the current measurement
- CL RX-Signal [dBm] / AP RX-Signal [dBm]
  The effective user signal of the client / access point in dBm
- CL NF [dBm] / AP NF [dBm]
  The background noise of the client / access point in dBm
- CL Retries [%] / AP Retries [%]
  The transfer repetitions of the client / access point as a percentage.
- CL RSSI / AP RSSI
  The raw value of the RSSI (Received Signal Strength Indication) of the client / access point
- CL TX-Rate [Mbps] / AP TX-Rate [Mbps]
  The average data rate of the sent data packets during the current random test
- Roaming Counter
  The roaming counter shows how often the client has changed access points during the recording. After 4,294,967,295 changes, the counter is reset.
- Operative Channel
  The current channel or the channel on which the client is connected to the access point
- AP System Name
  The system name of the access point
- BSSID
  The BSSID (Basic Service Set Identification) of the access point
- Connected Stations
  Number of clients connected to the access point over the same VAP interface.
- Bidirectional Status
  Shows whether the data of the access point are also being recorded.

The table below the graphic 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.
- **Interval [ms]**
  Specify the time interval between acquiring two measured values in milliseconds. The first measured value is displayed only after the set time interval has elapsed.
- **Samples**
  Specify how many measurements should be made.
- **Endless**
  If you enable the option check mark, the number of measurements is unlimited The "Samples" box is grayed out . The signal recorder runs until it is stopped manually or the device is reconfigured.
  You can only select this option starting at a time interval ≥ 100 milliseconds.
  If the recording contains more than 10000 measurements, the last 10000 measurements are listed in the csv file and the PDF file.
- **Bidirectional Recording**
  If you enable the setting the values of the access point as of a time interval of ≥ 10 milliseconds.
  The setting is supported by access points with the following versions: SCALANCE W700 11ax V1.1 or higher.
- **Start**
  Click the button in this column to start recording the wanted signal.

  Note

  - If you start a new recording, the previous recording will be overwritten.
  - If the recording has lasted less than 10 minutes and has not yet been completed (e.g. due to a restart or power down), the measured values are deleted.

  The signal recorder saves the recorded data automatically every 10 minutes. Following a restart, the recording contains all the values up to the last save action.
- **Stop**
  Click the button in this column to stop recording the wanted signal prematurely. If the specified number of measurements has been made, recording of the user data signal stops automatically.
- **Displayed Samples**
  Select how many measurements will be shown in the graphic.

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.
- 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 loss of the user data signal always occurs at the same position.
- Selective measurements at a fixed position should be made over a longer period of time.

Procedure

1. Enter the time interval between two measurements.
2. In "Samples" enter the number of measurements.
3. In "Displayed Samples" select how many measurements will be shown in the graphic.
4. Click the "Start" button.
   The status (to the right of the graphic) indicates whether the signal recorder is running. The first measured value is displayed only after the set time interval has elapsed.
5. To stop the recording, click the "Stop" button.
6. 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 / SFTP
     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 of the last column and click the "Save Values" button.
7. The ZIP file contains two files with the results of the recording:
   – A PDF file: The output is limited to 300 pages.
   – A CSV file: Complete listing of the recording.

Note

Number of stored measurements

The last 10000 measuring points are saved in the exported files.

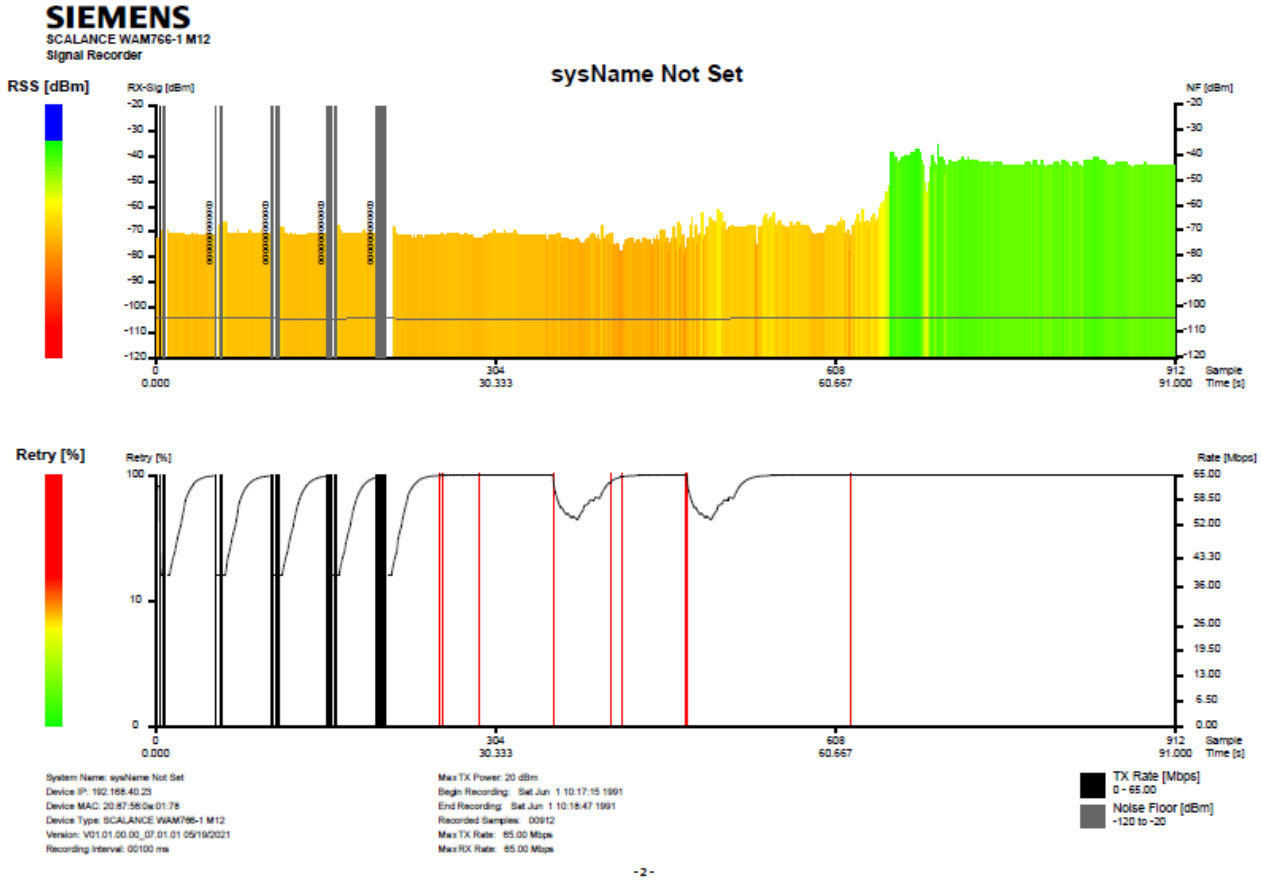
Measurement results

PDF file

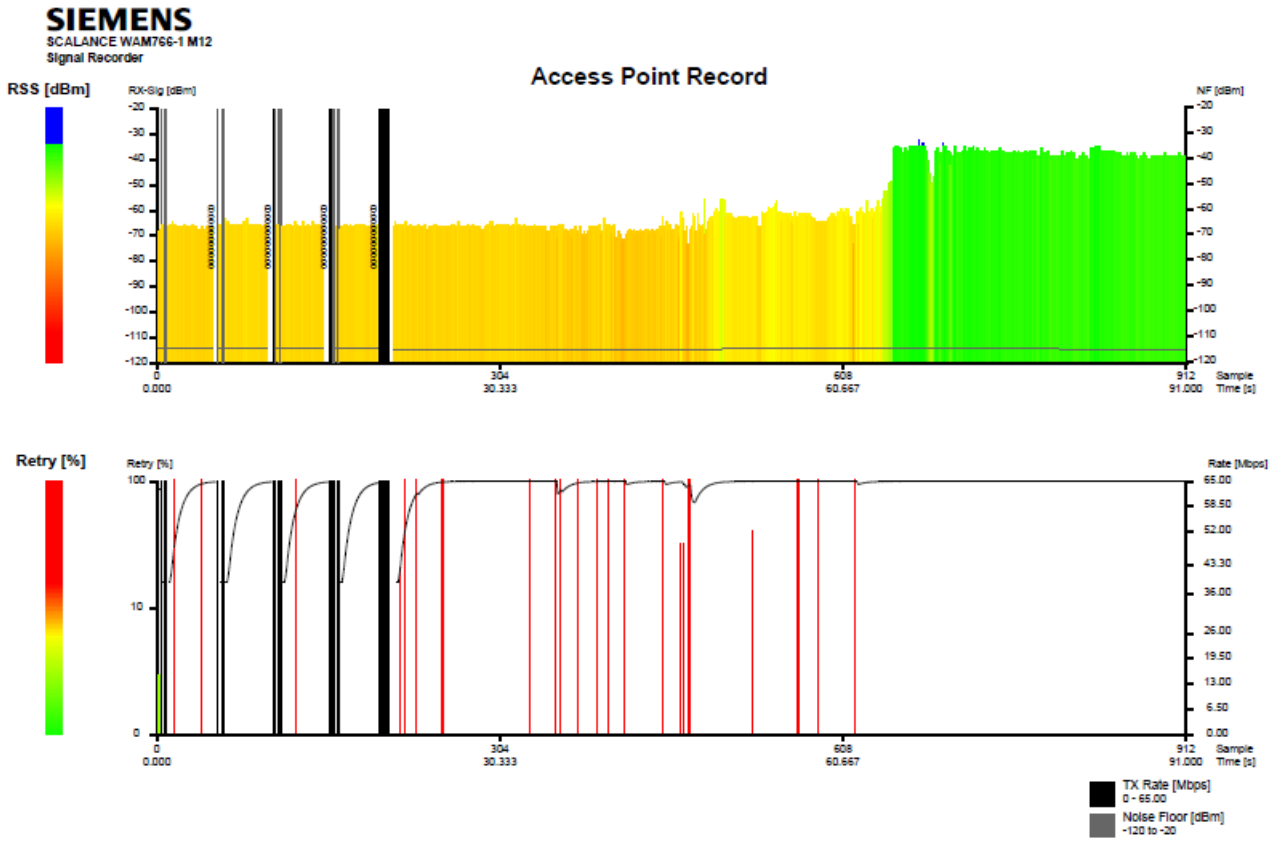
The PDF file contains a graphic representation of the course of the effective user data signal in dBm and the course of the data rate in Mbps. In terms of color, the graphic corresponds to the appearance in the Web Based Management. If the client changes the access point (roaming) during the measurement, this is indicated by vertical black bars with a black square at the tip.

The display is divided into two areas:

- Client
  Represents the measurement of the client. Below the graphic, the configuration data of the client is displayed.



- Access point
  Displays the measurement of the access point with which the client is currently connected. This requires that the setting "Bidirectional Recording" is enabled. The setting is supported by access points with the following versions: SCALANCE W700 11n > V6.1, SCALANCE W1700 11ac > V1.0 and SCALANCE W700 11ax as of V1.1. The access point sends its data to a maximum of 3 clients on which signal recorders are running. The access point data is not displayed on other clients.



The following pages contain the detailed information of all individual measurements in the form of a table.

The header row shows the IP address of the client and the BSSID and system name of the access point.

Per measurement the table contains two rows. The data of the client is in the first row and the data belonging to the access point in the second.

sysName Not Set						00:1b:1b:a6:0c:18						Scalance AP_18
Sample	Timestamp	Sig%	dBm	NF	RSSI	Roam	Retry%	Con-St	Ch	Width	TX-Rate	RX-Rate
1	16:45:31:241	44	-73	-104	22	0	0	1	44	20	62.01	62.84
		51	-69	-114	26		3					
2	16:45:31:341	42	-74	-104	21	0	0	1	44	20	62.01	63.11
		53	-68	-114	27		0					

Page 2 shows a legend of the abbreviations in the table. The data starts on a new page when the client changes access points.

Note

Note the description of the individual columns in the CSV file. These also apply to the columns of the PDF file.

CSV file

The CSV file contains information on the configuration of the SCALANCE W700 device and detailed information on all individual measurements and is divided into two areas.

System Name: sysName Not Set
Device IP: 192.168.40.23
Device MAC: 20:87:56:0a:01:78
Device Type: SCALANCE WAM766-1 M12
Version: V01.01.00.00_07.01.01.05192021
Recording Interval: 00100 ms
Max TX Power: 20 dBm
Begin Recording: Sat Jun 1 10:17:15 1991
End Recording: Sat Jun 1 10:18:47 1991
Recorded Samples: 00912
Max TX Rate: 65.00 Mbps
Max RX Rate: 65.00 Mbps

R1 Antenna Gain: 2 dB Add. Atten: Cable length: 0 m
R1 Antenna Gain: 2 dB Add. Atten: Cable length: 0 m

Sample	Timestamp	BSSID	CL RX-Sig	AP RX-Sig	CL RX-Sig	AP RX-Sig	CL NF [dBr	AP NF [dBr	CL RSSI	AP RSSI	Roam	CL Retry	AP Retry	Con Station	Operating I	Width	Scan Ch	TX-Rate	RX-Rate	AP System Name
1	16:45:31:241	00:1b:1b:a6:	44	51	-73	-69	-104	-114	22	26	0	0	3	1	44	20	44	62.01	62.84	Scalance AP_18
2	16:45:31:341	00:1b:1b:a6:	42	53	-74	-68	-104	-114	21	27	0	0	0	1	44	20	44	62.01	63.11	Scalance AP_18
3	16:45:31:541	00:1b:1b:a6:	0	51	----	-69	-104	-114	---	26	1	0	0	1	44	20	44	39.00	0.00	Scalance AP_18
4	16:45:31:641	00:1b:1b:a6:	0	57	----	-66	-104	-114	---	29	1	0	0	1	44	20	44	39.00	0.00	Scalance AP_18
5	16:45:31:741	00:1b:1b:a6:	49	55	-70	-67	-104	-114	25	28	1	0	0	1	44	20	44	40.62	39.00	Scalance AP_18

The first area contains the configured settings:

- System Name
  The system name of the client
- Device IP
  The IP address of the client
- Device MAC
  The MAC address of the client
- Recording Interval
  The interval between acquisition of two measured values.
- Max TX Power
  Maximum transmit power of the device
- Begin Recording
  Start of the recording
- End Recording
  End of the recording
- Recorded Samples
  The total number of measurements
- Max. TX Rate
  The maximum data rate of the sent data packets
- Max. RX Rate
  The maximum data rate of the received data packets
- Rx Antenna x type
  The setting of the external antennas

The second area is a table. The table contains the following for each measured value:

- Sample
  The current number of the measurement on the client (CL) / on the access point (AP)
- Timestamp
  The time stamp
- BSSID
  The BSSID (Basic Service Set Identification) of the access point

- CL / AP RX-Signal [%]
  The effective user data signal of the client (CL) / access point (AP) in %
- CL / AP RX-Signal [dBm]
  The effective user data signal of the client (CL) / access point (AP) in dBm
- CL / AP NF [dBm]
  The background noise in dBm
- CL / AP RSSI
  The raw value of the RSSI (Received Signal Strength Indication)
- Roam
  The roaming counter shows how often the client has changed access points during the recording. After 4 294 967 295 changes the counter is reset.
- CL / AP Retry
  The transfer repetitions of the client (CL) / access point (AP)
- Con Stations
  Number of clients connected to the access point.
- Operating Ch.
  The current channel or the channel on which the client is connected to the access point.
- Width
  The channel bandwidth 20, 40 or 80 MHz
- Scan CH
  The channel on which the client is currently scanning.
- TX-Rate
  The average data rate of the sent data packets
- RX-Rate
  The average data rate of the received data packets
- AP System Name
  The system name of the access point

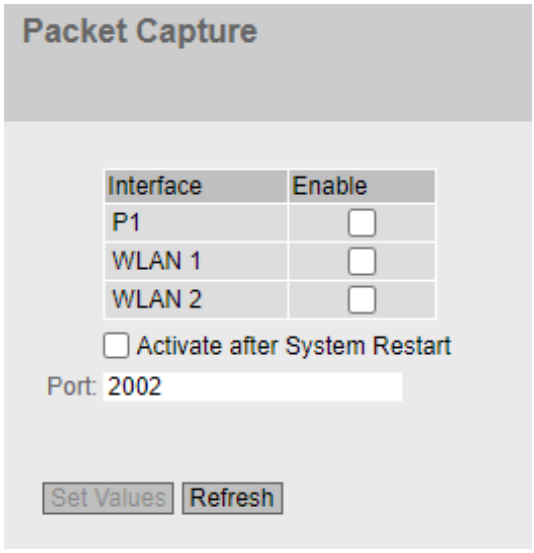
6.5.3 Packet Capture

Note

This page is available only in access point mode.

On this page, enable the function "Packet Capture" on the interface (Ethernet, WLAN). The function is for network diagnostics via a connected PC, e.g. to detect transfer errors.

You can also enable the function on several interfaces at the same time. When the function is enabled the interface can be linked in Wireshark. For a period Wireshark record the data traffic over the interface. Afterwards, you can view the content of the frames from the recording or filter according to certain contents.



Description

The table contains the following columns:

- **Interface**
  The interface to which the entry relates.
- **Enable**
  Enable or disable the "Packet Capture" function. As default, the function is disabled.

  Note

  The access point records all incoming frames. Encrypted data is not decrypted before the recording.

  Performance

  Enable the function only for diagnostics purposes. The increased data traffic could influence the performance of the device.

  Ethernet interface with SCALANCE WAM763-1

  - You can select one or more ports (P1 - P4) for the Ethernet interface.
  - Data traffic that is only forwarded and not received or sent by the WLAN interface is not displayed.

The page contains the following box:

- **Activate after System Restart**
  - Disabled
    After a restart, the configuration is reset to the default setting.
  - Enabled
    The configuration is saved and retained after a restart.
- **Port**
  Default port 2002 is preset. You can optionally enter a port number in the range 1 ... 65535. Make sure that the specified port is not already used.

Linking in the interface in Wireshark

Requirement:

- Wireshark V2.0.0 or higher is installed on the PC.
- The PC and device must be reachable via IP (layer 3).

Procedure

To analyze the data traffic e.g. of the WLAN interface 1 in Wireshark, follow the steps below:

1. Enable the function "Packet Capture" on WLAN 1 on the device.
2. Click "Set Values" to enable the function.
3. Start Wireshark.
4. Click "Options" in the "Capture" menu. The window "Wireshark - Capture Interfaces" opens.
5. Click the "Manage Interfaces..." button on the "Input" tab. In the following dialog, click on the "Remote Interfaces" tab.
6. To add the interface click on the Plus character in the "Remote Interfaces" tab.
7. In the following dialog, enter the IPv4 address of the device for "Host" and 2002 for "Port".
8. Enable "Null authentication" for "Authentication" and click the "OK" button.
9. On the "Remote Interfaces" tab, the host and the interfaces on which the function "Packet Capture" was previously enabled are displayed.
10. Select the interface and click the "OK" button.
    The remote interfaces displayed correspond to the following interfaces on the SCALANCE device:

Remote interface in Wireshark	Interface on the SCALANCE device	Comment
eth0	P1	-
eth1	P2	Only with SCALANCE WUM763
eth2	P3	
eth3	P4	
ath0_mon8	WLAN 1	Comprises VAP1.1 to VAP1.8
ath1_mon8	WLAN 2	Comprises VAP2.1 to VAP2.8

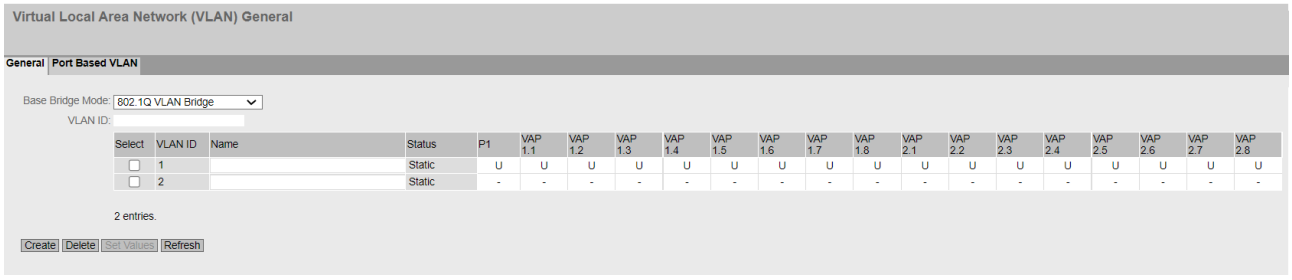
11. To start the recording, click "Start" in the "Capture" menu. You can obtain further information about handling the program in Wireshark.

If you analyze several interfaces, you can use a Wireshark instance for each interface.

6.6 "Layer 2" menu

6.6.1 VLAN

6.6.1.1 General



On this page you specify whether or not the device forwards frames with VLAN tags transparently (IEEE 802.1D/VLAN-unaware mode) or takes VLAN information into account (IEEE 802.1Q/VLAN-aware mode). If the device is in the "802.1Q VLAN Bridge" mode, you can define VLANs and specify the use of the ports .

Note

Changing the agent VLAN ID

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

Description

The page contains the following boxes:

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

  Note

  Changing Base Bridge mode

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

  - 802.1Q VLAN Bridge
    Sets the mode "VLAN-aware" for the device. In this mode, VLAN information is taken into account.
  - 802.1D Transparent Bridge
    Sets the mode "VLAN-unaware" for the device. In this mode, VLAN tags are not changed but are forwarded transparently. The VLAN priority is evaluated for CoS. In this mode, you cannot create any VLANs. Only a management VLAN is available: VLAN 1.

- **VLAN ID**
  Enter the VLAN ID in the "VLAN ID" input box.
  Range of values: 1 ... 4094

The table has the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **VLAN ID**
  Shows the VLAN ID. The VLAN ID (a number between 1 and 4094) can only be assigned once when creating a new data record and can then no longer be changed. To make a change, the entire data record must be deleted and created again. Up to 24 VLANs can be defined.
- **Name**
  Enter a name for the VLAN. The name only provides information and has no effect on the configuration. The length is a maximum of 32 characters.

- **State**
  Shows the status type of the entry in the internal port filter table. Here, static means that the address was entered as a static address by the user.
- **List of ports**
  Specify the use of the port. The following options are available:
  - "-"
    The port is not a member of the specified VLAN.
    With a new definition, all ports have the identifier "-".
  - M
    The port is a member of the VLAN. Frames sent in this VLAN are forwarded with the corresponding VLAN tag.
  - U (uppercase)
    The port is an untagged member of the VLAN. Frames sent in this VLAN are forwarded without the VLAN tag. Frames without a VLAN tag are sent from this port.
  - u (lowercase)
    The port is an untagged member of the VLAN, but the VLAN is not configured as a port VLAN. Frames sent in this VLAN are forwarded without the VLAN tag.
  - F
    The port is not a member of the specified VLAN. You can configure other settings in "Layer 2 > VLAN > Port-based VLAN".
  - T
    This option is only displayed and cannot be selected in the WBM.
    This port is a trunk port, making it a member in all VLANs.
    You configure this function in the CLI (Command Line Interface) using the "`switchport mode trunk`" command.

Changing Base Bridge mode

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

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

- All static and dynamic unicast entries are deleted.

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

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

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

802.1Q VLAN Bridge: Important rules for VLANs

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

- Frames with the VLAN ID "0" are handled as untagged frames but retain their priority value.
- As default, all ports on the device send frames without a VLAN tag to ensure that the end node can receive these frames.
- 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).
- With a trunk port, the VLAN assignment is dynamic. Static configurations can only be created if, in addition to the trunk port property, the port is also entered statically as a member in the VLANs involved. An example of a static configuration is the assignment of multicast groups in certain VLANs.

Procedure

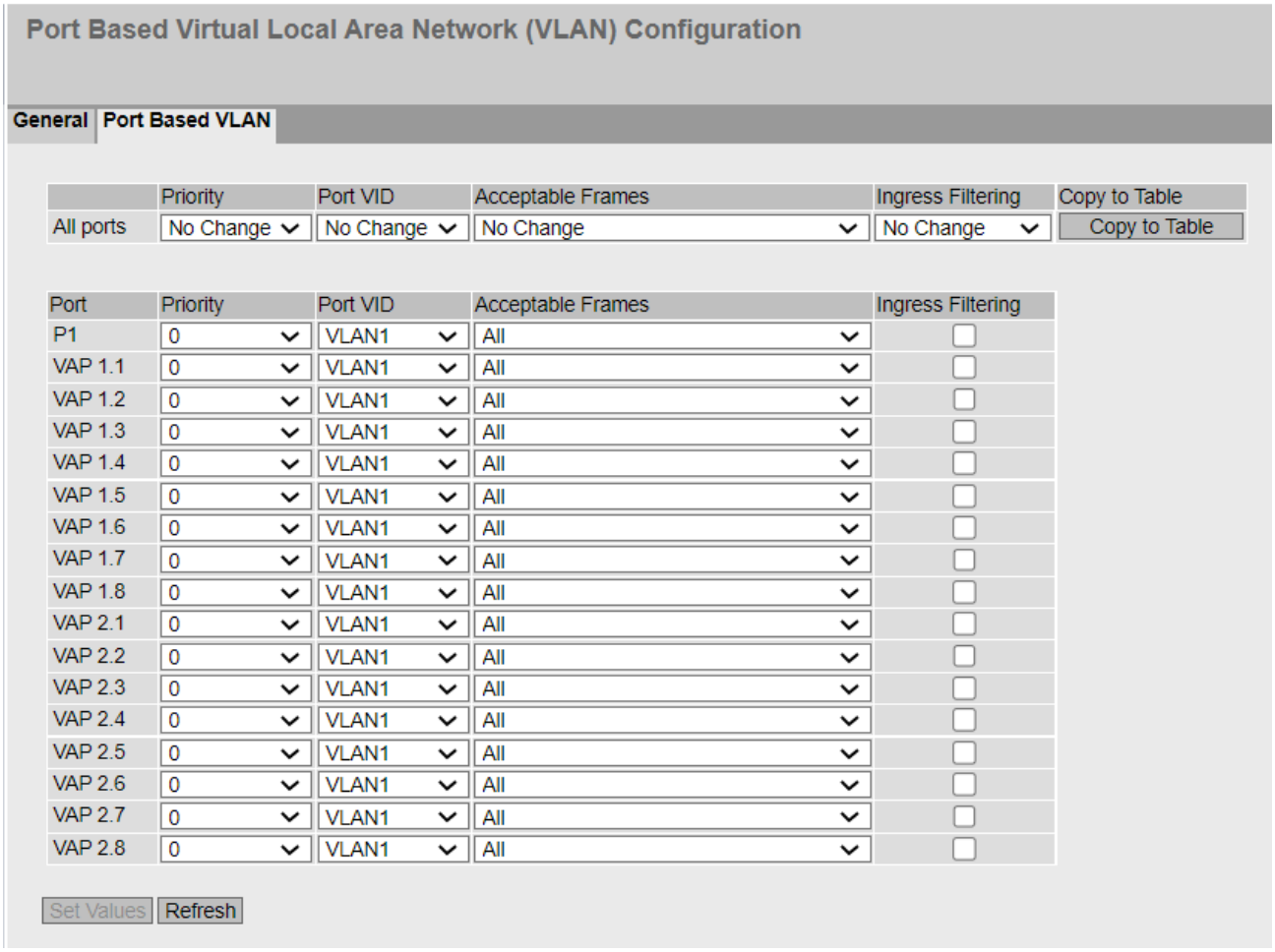
Requirement:

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

Creating a new VLAN

1. Enter an ID in the "VLAN ID" input box.
2. Click the "Create" button. A new entry is generated in the table. As default, the boxes have "-" entered.
3. Enter a name for the VLAN under Name.
4. Specify the use of the port in the VLAN. If, for example you select M, the port is a member of the VLAN. The frame sent in this VLAN is forwarded with the corresponding VLAN tag.
5. Click the "Set Values" button.

6.6.1.2 Port Based VLAN



Processing received frames

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

Requirement:

- On the "General" page, "802.1Q VLAN Bridge" is set for "Base Bridge Mode".

Description

Table 1 has the following columns:

Note

Table 1 is only available if at least one VLAN is configured.

- **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.

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. Frames tagged with "0" are treated like untagged frames. The device forwards all tagged frames. Otherwise, the forwarding rules apply according to the configuration.
  - All
    The device forwards all frames.
  - Untagged and Priority Tagged Only
    The device discards all tagged frames. The device forwards all untagged frames as well as frames with VLAN = 0 and a priority (Priority Tagged Frames). Otherwise, the forwarding rules apply according to the configuration.
- **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.

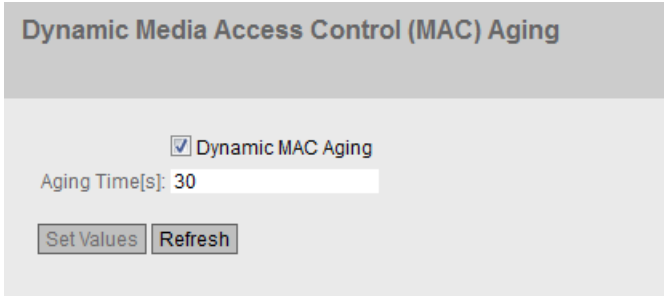
Procedure

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.

6.6.2 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 data frames to the nodes specifically involved. This reduces the network load for the other nodes.
If a device does not receive a frame whose source address matches a learnt address within a certain time, it deletes the learnt address. This mechanism is known as "Aging". Aging prevents frames being forwarded incorrectly, for example when an end device is connected to a different port.
If the check box is not enabled, a device does not delete learned addresses automatically.



Description of the displayed boxes

The page contains the following boxes:

- **Dynamic MAC Aging**
  Enable or disable the function for automatic aging of learned MAC addresses.
- **Aging Time[s]**
  Enter the time in seconds in steps of 15. After this time, a learned address is deleted if the device does not receive any further frames from this sender address.
  Range of values: 15 - 630 (seconds)

  Note

  Rounding of the values, deviation from desired value

  When you input the Aging Time, note that it is rounded to correct values. If you enter a value that cannot be divided by 15, the value is automatically rounded down.

Steps in configuration

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.

6.6.3 Spanning Tree

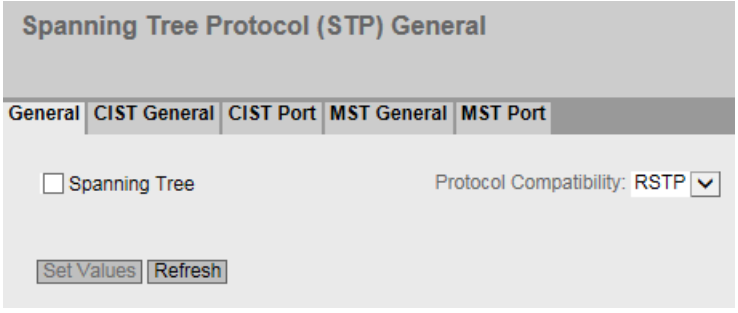
6.6.3.1 General

General settings of spanning tree

This is the basic page for spanning tree. Select the compatibility mode from the drop-down list. By default, RSTP is selected in the drop-down list and Spanning Tree is disabled.

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.



Description

The page contains the following boxes:

- **Spanning Tree**
  Enable or disable Spanning Tree.
- **Protocol Compatibility**
  Select the compatibility mode of Spanning Tree. For example if you select RSTP, Spanning Tree behaves like RSTP.
  The following settings are available:
  - STP
  - RSTP
  - MSTP

Procedure

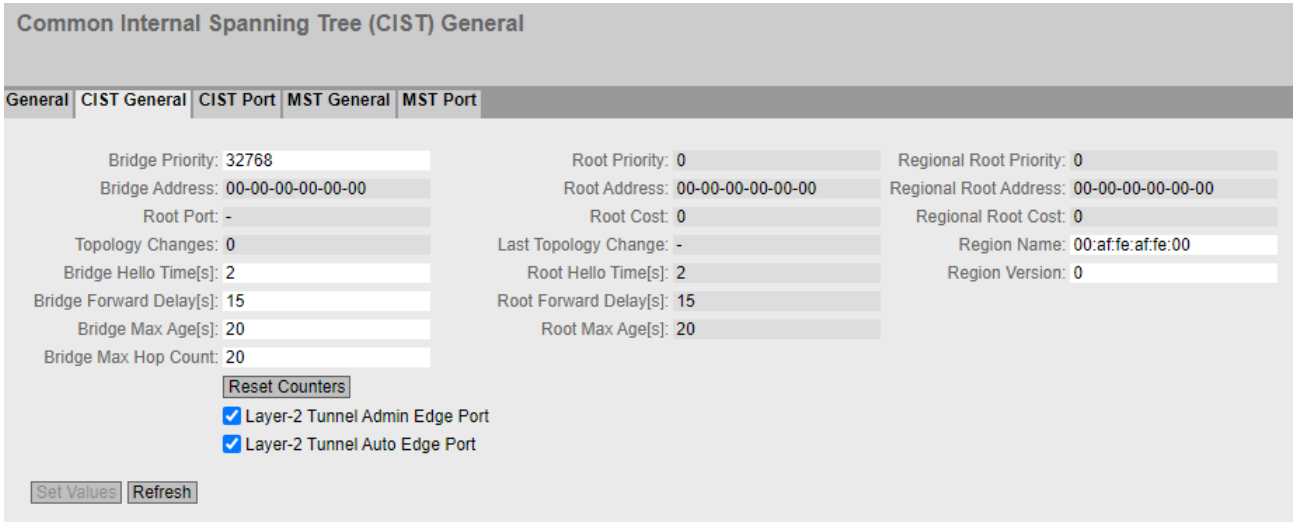
1. Select the "Spanning Tree" check box.
2. Select the compatibility mode from the "Protocol Compatibility" drop-down list.
3. Click the "Set Values" button.

6.6.3.2 CIST General

Configuration CIST

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 "Spanning Tree" on the "General" page and when "Protocol Compatibility" is set to "MSTP". 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.



Description

The page contains the following boxes:

- **Bridge Priority / Root Priority**
  Which device becomes the root bridge is decided based on the bridge priority . 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 Address / Root Address**
  The bridge address shows the MAC address of the device and the root address shows the MAC address of the root bridge.
- **Root port**
  Shows the port over which the device communicates with the root bridge.
- **Root Cost**
  The path costs from this device to the root bridge.
- **Topology Changes / Last Topology Change**
  The entry for the device shows the number of reconfiguration actions due to the spanning tree mechanism since the last startup. For the root bridge, the time since the last reconfiguration is displayed as follows:
  - Seconds: "sec" unit after the number
  - Minutes: "min" unit after the number
  - Hour: "hr" unit after the number
- **Bridge Hello Time[s] / Root Hello Time[s]**
  Each bridge 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]**
  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**
  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 seconds.
- **Bridge Max Hop Count**
  This parameter specifies how many MSTP nodes a BPDU may pass through. If an MSTP BPDU is received and has a hop count that exceeds the value configured here, it is discarded. The default for this parameter is 20.
- **Regional root priority**
  For a description of the displayed values, see Bridge priority / Root priority
- **Regional root address**
  Shows the MAC address of the regional root bridge.

- **Regional Root Cost**
  Shows the path costs from this device to the regional root bridge.
- **Region Name**
  Enter the name of the MSTP region to which this device belongs. By 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**
  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.
- **Layer-2 Tunnel Admin Edge Port (Only available 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 (Only available in access point mode)**
  Select this check box if you want to detect automatically whether an end device is connected at all layer 2 tunnel ports.

Procedure

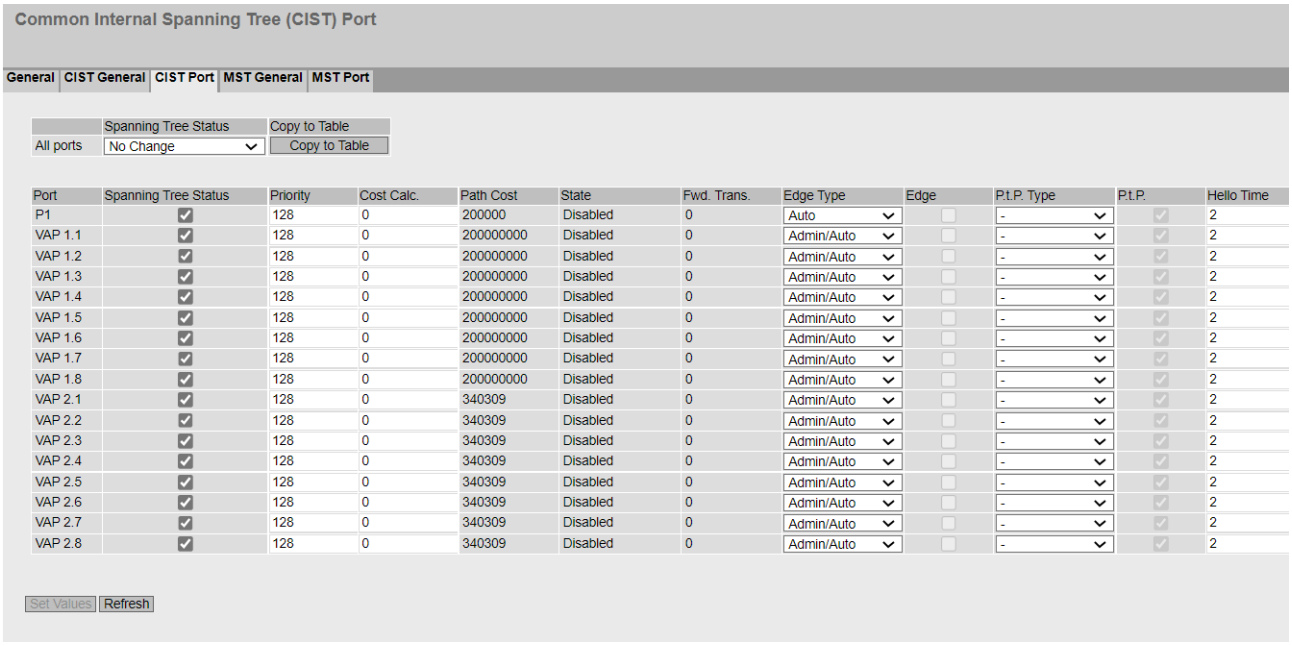
1. Enter the data required for the configuration in the input boxes.
2. Click the "Set Values" button.

6.6.3.3 CIST Port

Configuration of CIST ports

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

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



Description

Table 1 has the following columns:

- **Column 1**
  Shows that the settings are valid for all ports of table 2.
- **Spanning Tree Status**
  In the drop-down list, select the setting for all ports. If "No Change" is selected, the entries of the corresponding column in table 2 remain unchanged.
- **Copy to Table**
  If you click the button, the settings are adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
  Shows the available ports and interfaces.
- **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 will be selected.
  If the "Cost Calc." box has the value "0", the automatically calculated value is shown. Otherwise, the value of the "Cost Calc." box is displayed.
  The calculation of the path costs is largely based on the transmission speed. The higher the achievable transmission speed is, the lower the value of the path costs.
  Typical values for path costs with 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 state 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 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 switch 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 detected 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.

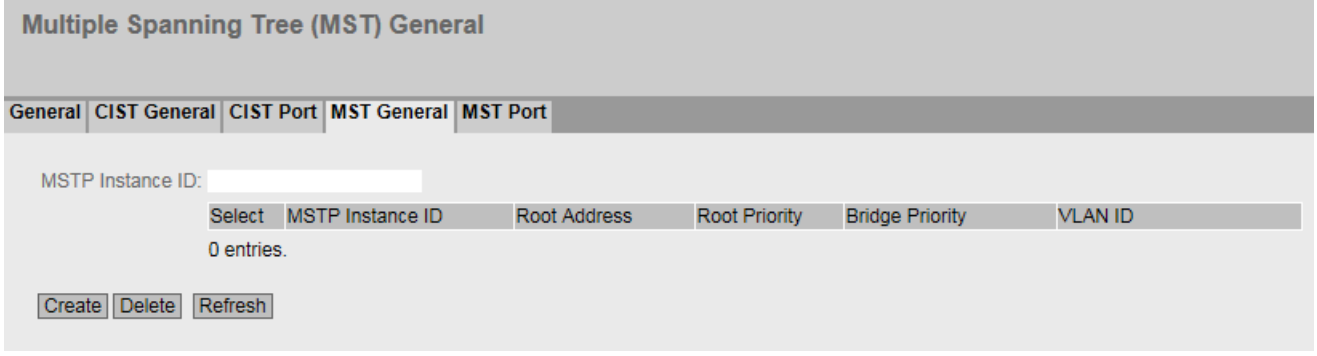
Procedure

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.

6.6.3.4 MST General

Multiple Spanning Tree configuration

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



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" box.
5. Click the "Set Values" button.

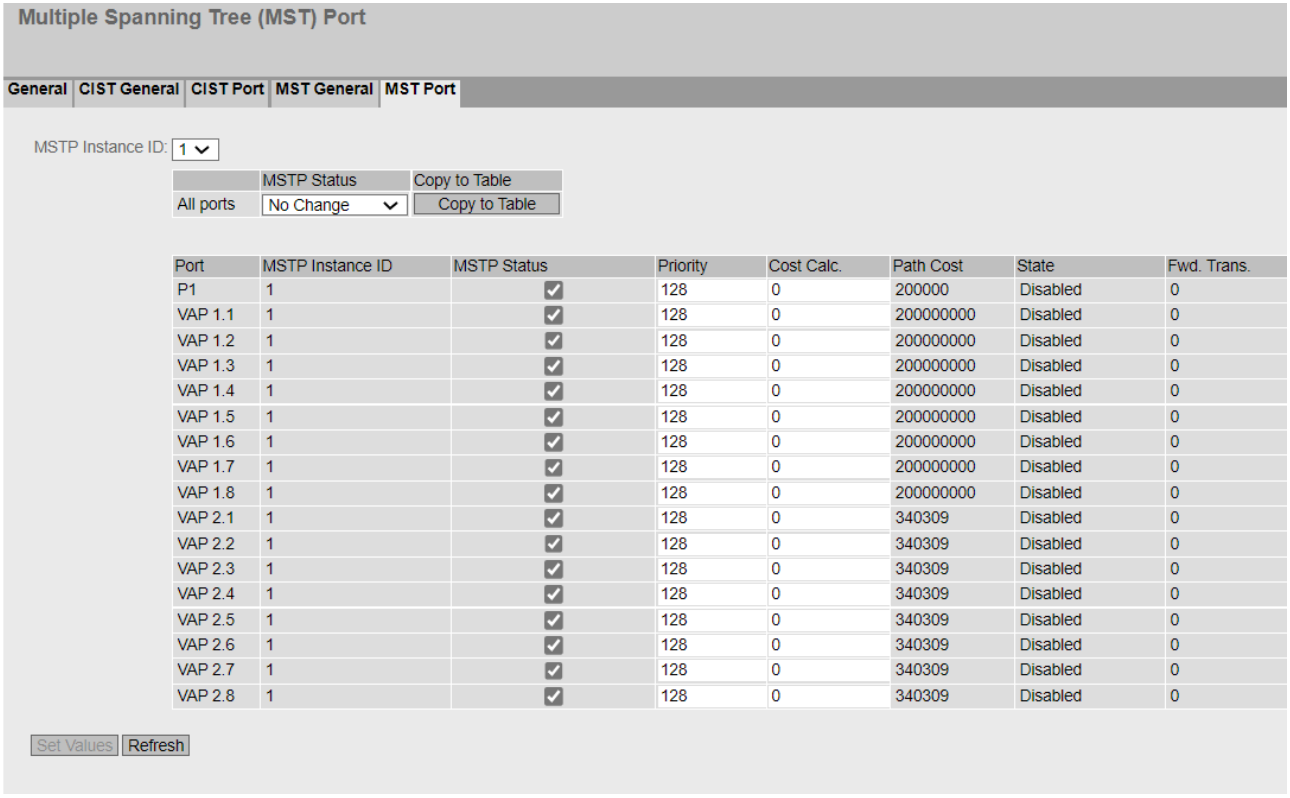
Deleting entries

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.

6.6.3.5 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.



Description

The page contains the following box:

- **MSTP Instance ID**
  In the drop-down list, select the ID of the MSTP instance.

Table 1 has the following columns:

- **Column 1**
  Shows that the settings are valid for all ports of table 2.
- **MSTP Status**
  In the drop-down list, select the setting for all ports. If "No Change" is selected, the entries of the corresponding column in table 2 remain unchanged.
- **Copy to Table**
  If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
  Shows all available ports and interfaces.
- **MSTP instance ID**
  Shows the 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 Costs".
- **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 will be selected.
  If the "Cost Calc." box has the value "0", the automatically calculated value is shown. Otherwise, the value of the "Cost Calc." box is displayed.
  The calculation of the path costs is largely based on the transmission speed. The higher the achievable transmission 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.
- **Status**
  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

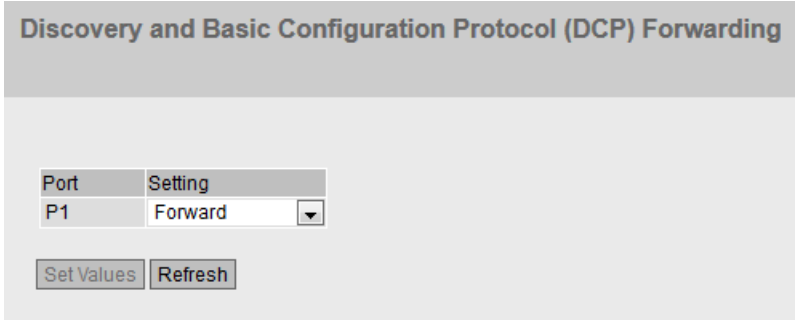
1. In the input cells of the table row, enter the values of the port you are configuring.
2. From the drop-down lists of the cells of the table row, select the values of the port you are configuring.
3. Click the "Set Values" button.

6.6.4 DCP Forwarding

Applications

The DCP protocol is used by STEP 7 and SINEC PNI for configuration and diagnostics. In the delivery state, DCP is enabled on all Ethernet ports; in other words, received DCP frames are forwarded on all ports. With this option, you can disable the sending of frames for individual ports, for example to prevent individual parts of the network from being configured with SINEC PNI 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.



Description

The table has the following columns:

- **Port**
  Shows the available Ethernet ports.
- **Setting**
  Specify whether the port should block or forward outgoing DCP frames. You have the following options available:
  - Forward
    DCP frames are forwarded at this port.
  - Block
    No outgoing DCP frames are forwarded at this port. It is nevertheless still possible to receive via this port.

Procedure

1. Specify whether the port blocks or forwards the DCP frames.
2. Click the "Set Values" button.

6.6.5 LLDP

Identifying the network topology

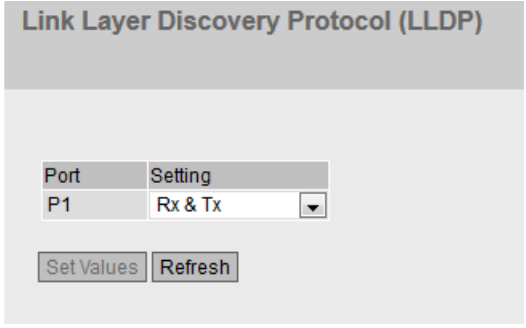
LLDP (Link Layer Discovery Protocol) is defined in the IEEE 802.AB standard.

LLDP is a method used to discover the network topology. Network components exchange information with their neighbor devices using LLDP.

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

Applications

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



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

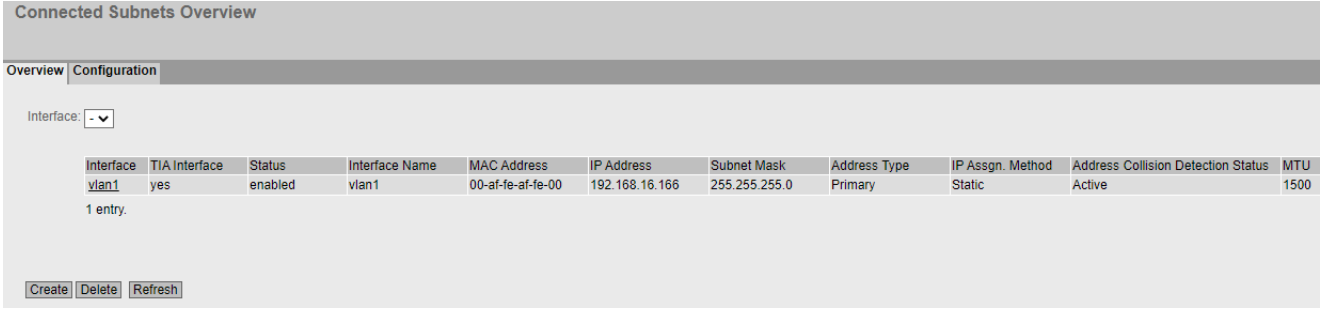
1. Select the required LLDP functionality from the drop-down list.
2. Click the "Set Values" button.

6.7 Menu "Layer 3 (IPv4)"

6.7.1 Subnets

6.7.1.1 Overview

The page shows the subnets for the selected VLAN interface. This VLAN interface is also called an IPv4 interface. A subnet always relates to an IPv4 interface. The IPv4 address is assigned in the "Configuration" tab.



Description

The page contains the following boxes:

- **Interface**
  Select the interface on which you want to configure the subnet.

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **Interface**
  Shows the interface.
- **TIA Interface**
  Shows whether or not the interface is used as TIA interface.
- **Status**
  Shows the status of the interface.
- **Interface Name**
  Shows the name of the interface.
- **MAC Address**
  Shows the MAC address.
- **IP Address**
  Shows the IPv4 address of the subnet.
- **Subnet Mask**
  Shows the subnet mask.
- **Address Type**
  Displays the address type. The following values are possible:
  - Primary
    The first IPv4 address that was configured on an IPv4 interface.
  - Secondary
    All other IPv4 addresses that were configured on an IPv4 interface.
- **IP Assign Method**
  Shows how the IPv4 address is assigned. The following values are possible:
  - Static
    The IPv4 address is static. You enter the settings in "IP Address" and "Subnet Mask".
  - Dynamic (DHCP)
    The device obtains a dynamic IPv4 address from a DHCPv4 server.

- **Address Collision Detection Status**
  If new IPv4 addresses become active in the network, the "Address Collision Detection" function checks whether this can result in address collisions. The allows IPv4 addresses that would be assigned twice to be detected.

  Note

  The function does not run a cyclic check.

  This column shows the current status of the function. The following values are possible:

  – Idle
    The interface is not enabled and does not have an IPv4 address.
  – Starting
    This status indicates the start-up phase. In this phase, the device initially sends a query as to whether the planned IPv4 address already exists. If the address is not yet been assigned, the device sends the message that it is using this IP address as of now.
  – Conflict
    The interface is not enabled. The interface is attempting to use an IPv4 address that has already been assigned.
  – Defending
    The interface uses a unique IPv4 address. Another interface is attempting to use the same IPv4 address.
  – Active
    The interface uses a unique IPv4 address. There are no collisions.
  – Not supported
    The function for detection of address collisions is not supported.
  – Disabled
    The function for detection of address collisions is disabled.

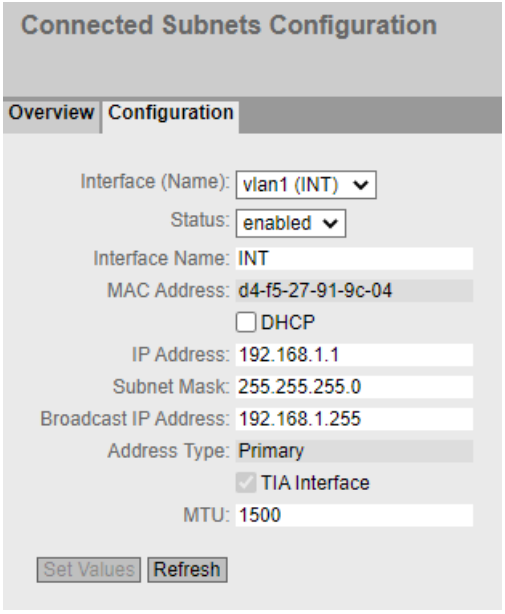
- **MTU**
  Shows the packet size.

Procedure

1. Select the VLAN interface from the "Interface" drop-down list.
2. Click the "Create" button. A new row is inserted in the table.
3. Configure the subnet on the "Configuration" tab.

6.7.1.2 Configuration

On this page, you configure the IPv4 interface.



Description

The page contains the following boxes:

- **Interface (Name)**
  Select the interface from the drop-down list.
- **Status**
  Specify whether the interface is enabled or disabled.
  - Enabled
    The interface is enabled. Data traffic is possible only over an enabled Interface.
  - Disabled
    The interface is disabled.
- **Interface Name**
  Enter the name of the interface.
- **MAC Address**
  Displays the MAC address of the selected interface.
- **DHCP**
  Enable or disable the DHCP client for this IPv4 interface.
- **IP Address**
  Enter the IPv4 address of the interface. The IPv4 addresses must not be used more than once.
- **Subnet Mask**
  Enter the subnet mask of the subnet you are creating. Subnets on different interfaces must not overlap.

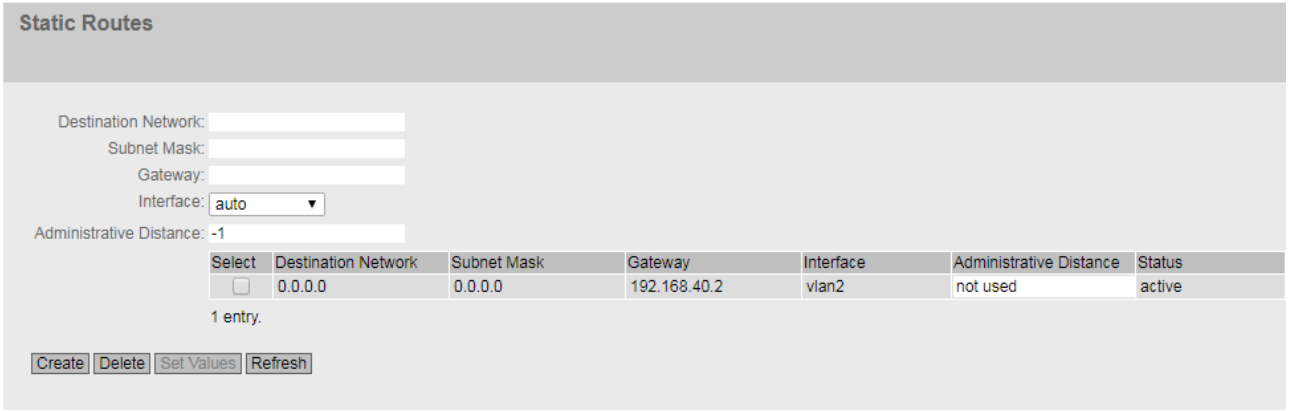
- **Address Type**
  Shows the address type.
  - Primary
    The first subnet of the interface.
- **TIA Interface**
  Select whether this interface should become the TIA interface. The TIA interface defines on which VLAN the PROFINET functionalities are available. This mainly affects the device search with or via DCP.
- **MTU**
  MTU (Maximum Transmission Unit) specifies the maximum size of the packet. If packets are longer than the set MTU, they are fragmented. The MTU covers the IP headers and the headers of the higher layers.
  Range of values:
  - With IPv4: 90 ... 1514
  - With IPv6: 1280 ... 1514

Procedure

1. Select the interface from the "Interface (Name)" drop-down list.
2. Select the status of the interface in the "Status" drop-down list.
3. Enter a name for the Interface in "Interface Name".
4. Enter the IPv4 address of the subnet in the "IP Address" column or enable the "DHCP" option.
5. Enter the subnet mask belonging to the IPv4 address in the "Subnet Mask" column.
6. Click the "Set Values" button.

6.7.2 Static Routes

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



Description

The page contains the following boxes:

- **Destination Network**
  Enter the network address of the destination that can be reached via this route.
- **Subnet Mask**
  Enter the corresponding subnet mask.
- **Gateway**
  Enter the IPv4 address of the gateway via which this network address is reachable.
- **Administrative Distance**
  Enter the metric for the route. The metric corresponds to the quality of a connection, for example speed, costs. If there are several equal routes, the route with the lowest metric value is used.
  If you do not enter anything, "not used" is entered automatically. The metric can be changed later.
  Range of values: 1 - 255 or -1 for "not used".
  Here, 1 is the value for the best possible route. The higher value, the longer packets require to their destination.

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **Destination Network**
  Shows the network address of the destination.
- **Subnet Mask**
  Shows the corresponding subnet mask.
- **Gateway**
  Shows the IPv4 address of the next gateway.
- **Interface**
  Shows the interface of the route.
- **Administrative Distance**
  Enter the metric for the route. When creating the route, "not used" is entered automatically. The metric corresponds to the quality of a connection, based for example on speed or costs. If there are several equal routes, the route with the lowest metric value is used.
  Range of values: 1 - 255
  Here, 1 is the value for the best possible route. The higher value, the longer the packets require to their destination.
- **Status**
  Shows whether or not the route is active.

Procedure

1. Enter the network address of the destination in the "Destination Network" input box.
2. Enter the corresponding subnet mask in the "Subnet Mask" input box.
3. Enter the gateway in the "Gateway" input box.

4. Enter the weighting of the route in "Administrative Distance".
5. Click the "Create" button. A new entry is generated in the table.

6.7.3 NAT

6.7.3.1 Masquerading

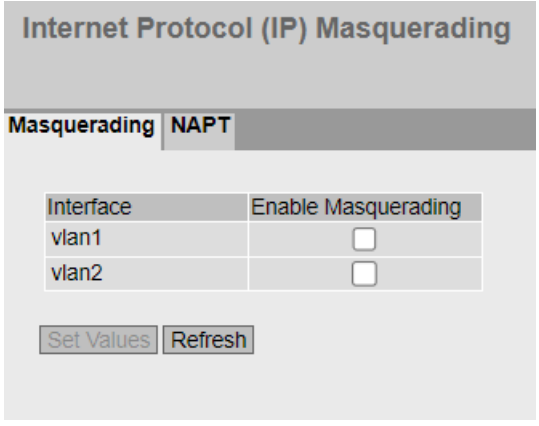
Note

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

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

Note

Enabling IP masquerading on at least one VLAN enables NAPT.



Requirements

- "802.1Q VLAN Bridge" is set for "Base bridge mode".
- A second VLAN is set up and the IPv4 interface is configured, see "Subnets (Page 259)".

Description

The table has the following columns:

- **Interface**
  Interface to which the setting relates. Only interfaces with a configured subnet are available.
- **Enable Masquerading**
  When enabled, with each outgoing data packet sent via this interface, the source IP address is replaced by the IP address of the interface.

6.7.3.2 NAPT

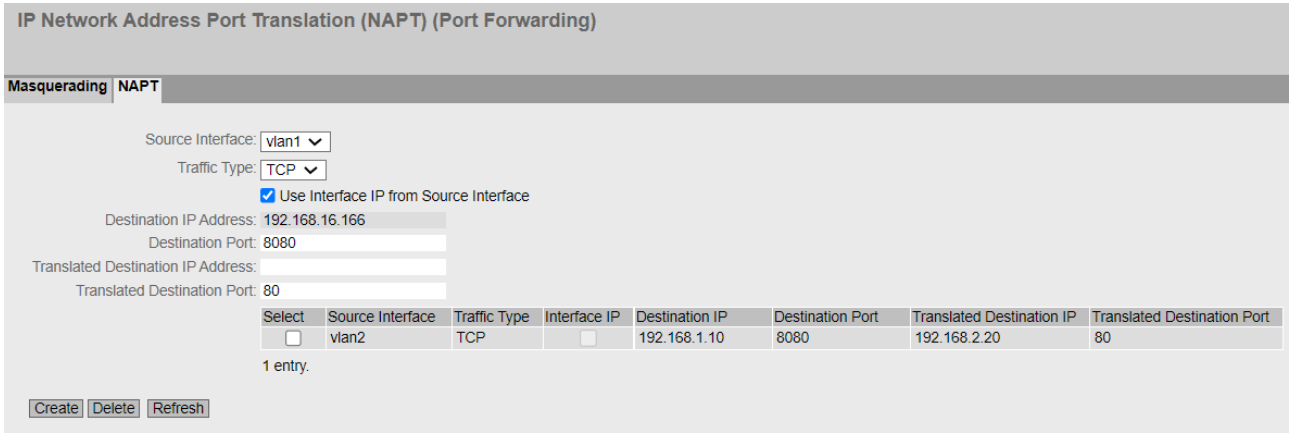
Note

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

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

The following port translations are possible:

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



Requirements

- IP masquerading is enabled.
- Under "Layer 2 > VLAN > Basic", "802.1Q VLAN Bridge" is set for "Base Bridge Mode".

Description

The page contains the following boxes:

- **Source Interface**
  Select the interface on which the queries will arrive.
- **Traffic Type**
  Specify the protocol for which the address assignment is valid.
- **Use Interface IP from Source Interface**
  When enabled, the IP address of the selected interface is used for "Dest IP Address".

- **Destination IP Address**
  Enter the destination IP address. The frames are received at this IP address. Can only be edited if "Use Interface IP from Source Interface" is disabled.

  Note

  The rule is only enabled if the IP address of the VLAN is the same.

- **Destination Port**
  Enter the destination port. Incoming frames with this port as the destination port are forwarded. If the setting is intended to apply to a port range, enter the range with start port "-" end port, for example 30 - 40.
- **Translated Destination IP**
  Enter the IP address of the node to which this frame will be forwarded.
- **Translated Destination Port**
  Enter the number of the port. This is the new destination port to which the incoming frame will be forwarded. If the setting is intended to apply to a port range, enter the range with start port "-" end port, for example 30 - 40.

The table has the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **Source Interface**
  Shows the interface from which the packets need to come. Only these packets are considered for port forwarding.
- **Traffic Type**
  Shows the protocol for which the address assignment applies.
- **Interface IP**
  Shows whether the IP address of the interface is used.
- **Destination IP**
  Shows the destination IP address. The frames are received at this IP address.
- **Destination Port**
  Shows the destination port. Incoming frames with this port as the destination port are forwarded.
- **Translated Destination IP**
  Shows the IP address of the node to which the packets will be forwarded.
- **Translated Destination Port**
  Shows the destination port to which the packets are translated.

6.8 Menu "Layer 3 (IPv6)"

6.8.1 Subnets

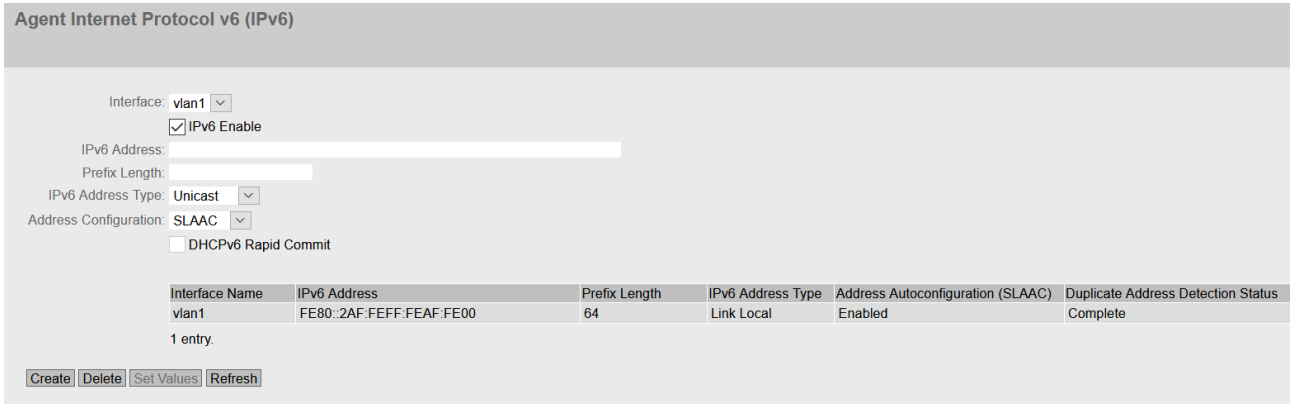
Configuration of the IP addresses

On this page, you enable IPv6 at the VLAN interface. This VLAN interface is also called an IPv6 interface. An IPv6 interface can have several IPv6 addresses.

Note

Update from V1.0 to V1.1

The configuration of the IPv6 addresses is not transferred with an update from V1.0 to V1.1.



Description

The page contains the following:

- **Interface**
  Shows the VLAN interface on which IPv6 will be enabled.
- **IPv6 Enable**
  Enable or disable IPv6 on the interface. When you enable the setting and accept it, the link-local address is created automatically.
- **IPv6 Address**
  Enter the IPv6 address. The input depends on the selected address type.
- **Prefix Length**
  Enter the number of left-hand bits belonging to the prefix
- **IPv6 Address Type**
  Select the address type:
  - Unicast
  - Link Local: IPv6 address is only valid on the link.

- **Address Configuration**
  Specify the mechanism for the address configuration:
  - DHCPv6
    Status dependent: Obtains the IPv6 address and the configuration file from the DHCPv6 server.
  - SLAAC (Stateless Address Auto Configuration) (Default)
    Stateless autoconfiguration using NDP (Neighbor Discovery Protocol)
  - Static
    Enter a static IPv6 address.
- **DHCPv6 Rapid Commit**
  When enabled the procedure for the IPv6 address assignment is shortened. Instead of 4 DHCPv6 messages (SOLICIT, ADVERTISE , REQUEST, REPLY) only 2 DHCPv6 messages (SOLICIT, REPLY) are used. You will find further information on the messages in RFC 3315.

The table has the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **Interface Name**
  Shows the name of the VLAN interface.
- **IPv6 Address**
  Shows the IPv6 address.
- **Prefix Length**
  Shows the prefix length.

- **IPv6 Address Type**
  Displays the address type. The following values are possible:
  - Unicast
  - Link Local
- **Duplicate Address Detection Status**
  In Address Autoconfiguration (SLAAC), the "Address Collision Detection Status" function prevents IPv6 addresses from being assigned twice. The device can only use free IPv6 addresses during autoconfiguration.
  When the function is activated, the check via NDP takes place automatically.

  Note

  The function does not run a cyclic check.

  This column shows the current status of the function. The following values are possible:
  - Tentative
    This status indicates that the selected IPv6 address is being checked. The device sends a neighbor solicitation message to the selected IPv6 address.
  - Conflict
    This status indicates that the IPv6 address is already being used. In this case, a neighbor advertisement message with the selected IPv6 address is returned to the device. The device forms a new IPv6 address and checks this again.
  - Complete
    This status indicates that the selected IPv6 address can be used. In this case, the device did not receive feedback within a period of time and assumes that the IPv6 address is not yet assigned.
  - Down
    This status indicates that the interface is not active. No check is carried out.

Procedure

Automatically form link-local address

1. Enable IPv6.
2. Click the "Set Values" button. In the table an entry with the interface is created and the automatically formed link-local IPv6 address is displayed.

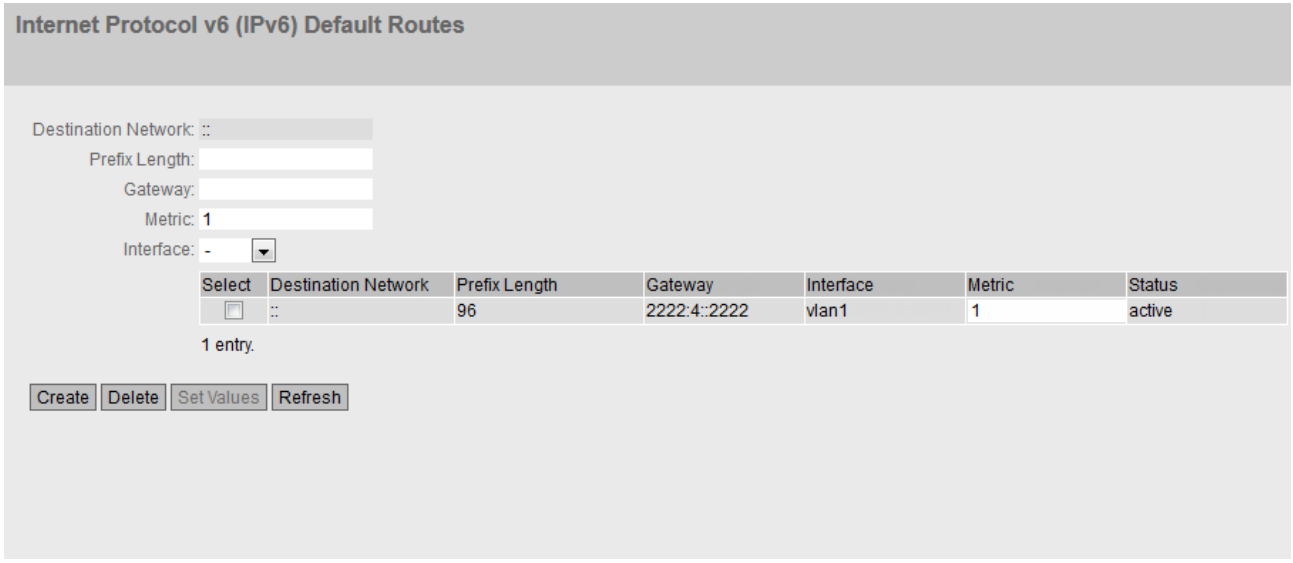
Assign link-local address

1. Enable IPv6.
2. In "IPv6 Address", enter the link-local address, e.g. FE80::21B:1BFF:FE40:9155
3. Enter "128" in "Prefix Length".
4. For "IPv6 Address Type" select the entry "Link Local".
5. For "Address Configuration" select the entry "Static".
6. Click the "Create" button. In the table an entry with the interface is created and the IPv6 address is displayed.
   The automatically created link-local address is overwritten.

6.8.2 Static Routes

On this page, you configure the IPv6 default route. The IPv6 default route is an IPv6 route, that applies to all IPv6 addresses. The device only needs to know the default gateway and sends all IPv6 packets to it.

The default gateway either knows all routes itself or has a default route to another default gateway.



Description

The page contains the following:

- **Destination Network**
  Destination Network (:: or 0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0) applies to all IPv6 addresses.
- **Prefix Length**
  Enter the number of left-hand bits belonging to the prefix
- **Gateway**
  Enter the IPv6 address of the gateway to which the IPv6 packets will be sent.
- **Metric**
  Enter the metric for the route. The metric corresponds to the quality of a connection, based for example on speed or costs. If there are several equal routes, the route with the lowest metric value is used.
  Range of values: 1 - 254
- **Interface**
  Specify the interface via which the network address of the destination is reached.

This table contains the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **Destination Network**
  Shows the network address of the destination.

- **Prefix Length**
  Shows the prefix length.
- **Gateway**
  Shows the IPv6 address of the next gateway.
- **Interface**
  Shows the Interface of the route.
- **Metric**
  Enter the metric for the route. When creating the route, "not used" is entered automatically. The metric corresponds to the quality of a connection, based for example on speed or costs. If there are several equal routes, the route with the lowest metric value is used.
  Range of values: 1 - 254
- **Status**
  Shows whether or not the route is active.

Steps in configuration

1. Enter the prefix length.
2. Enter the IPv6 address of the gateway.
3. Enter the metric of the route.
4. Select the interface through which the network address of the destination is reached.
5. Click the "Create" button. A new entry is generated in the table.

6.9 "Security" menu

6.9.1 Users

6.9.1.1 Local Users

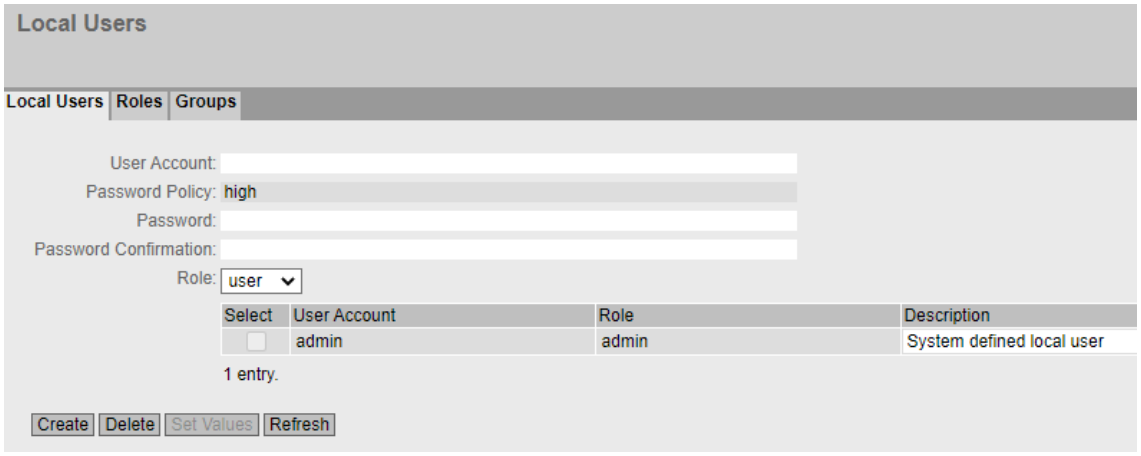
Local users

On this page, you create local users with the corresponding rights.

When you create or delete a local user this change is also made automatically in the table "External User Accounts". If you want to make change explicitly for the internal or external user table, use the CLI commands.

Note

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


Local Users
Local Users
Roles
Groups
User Account:
Password Policy:
high
Password:
Password Confirmation:
Role:
user
Select
User Account
Role
Description
admin
admin
System defined local user
1 entry.
Create
Delete
Set Values
Refresh

Description

The page contains the following:

- **User Account**
  Enter the name for the user. The name must meet the following conditions:
  - It must be unique.
  - It must be between 1 and 250 characters long.
  - The following characters must not be included: :;"|€´?§³²°µ ä ö ü Ä Ö Ü
    The characters for Space and Delete also cannot be contained.

  Note

  User name cannot be changed

  After creating a user, the user name can no longer be modified.

  If a user name needs to be changed, the user must be deleted and a new user created.

  Note

  User names: admin

  You can configure the device with this user name.

  When you log in for the first time or log in after a "Restore Factory Defaults and Restart", you will be prompted to change the predefined password "admin". You can also rename the "admin" user preset in the factory once. Afterwards, renaming "admin" is no longer possible.

- **Password Policy**
  Shows which password policy is being used:
  - High
    Password length: at least 8 characters, maximum 128 characters
    At least 1 uppercase letter
    At least 1 special character
    At least 1 number
  - Low
    Password length: at least 6 characters, maximum 128 characters
  - Custom
    You configure the password policy on the page "Security > Passwords > Options".
- **Password**
  Enter the password. The strength of the password depends on its length and complexity.
  - It must not contain the following characters: ; : ' ? ß § " ² ³ ° | € µ ä ö ü Ä Ö Ü
  - The characters for Space and Delete also cannot be contained.
- **Password Confirmation**
  Enter the password again to confirm it.
- **Role**
  Select a role.
  You can choose between system-defined and self-defined roles, refer to the page "Security > Users > Roles".

The table contains the following columns:

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

  Note

  The preset users as well as logged in users cannot be deleted or changed.

- **User Account**
  Shows the user name.
- **Role**
  Shows the role of the user.
- **Description**
  Displays a description of the user account. The description text can be up to 100 characters long.

Procedure

Note

Changes in "Trial" mode

Even if the device is in "Trial" mode, changes that you carry out on this page are saved immediately.

Creating users

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

Deleting users

1. Select the check box in the row to be deleted.
2. Click the "Delete" button. The entries are deleted and the page is updated.

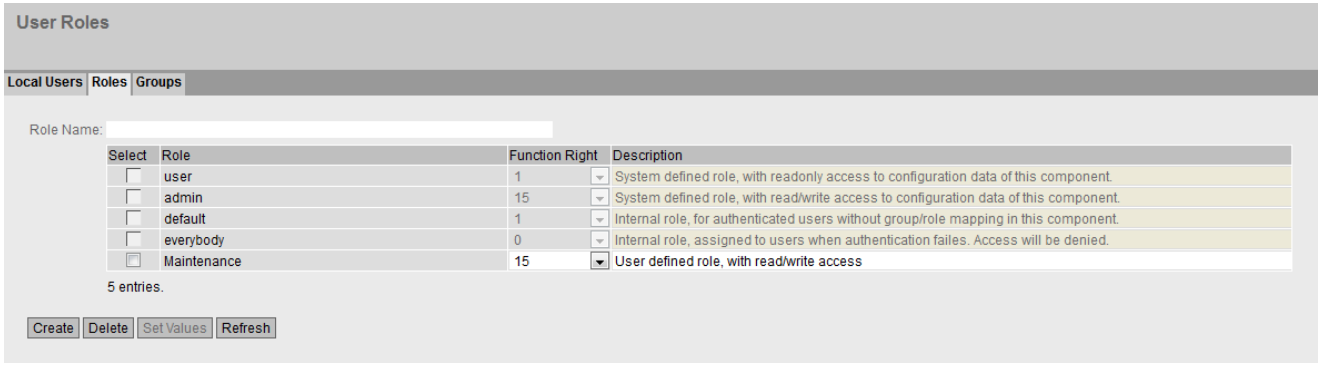
6.9.1.2 Roles

Roles

On this page, you create roles that are valid locally on the device.

Note

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



Description

The page contains the following:

- **Role Name**
  Enter the name for the role. The name must meet the following conditions:
  - It must be unique.
  - It must be between 1 and 64 characters long.
  - It must not contain the following characters: ;"|€´?§^{32o}µ ä ö ü Ä Ö Ü
    The characters for Space and Delete also cannot be contained.

  Note

  Role name cannot be changed

  After creating a role, the name of the role can no longer be changed.

  If a name of a role needs to be changed, the role must be deleted and a new role created.

The table contains the following columns:

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

  Note

  Predefined roles and assigned roles cannot be deleted or modified.

- **Role**
  Shows the name of the role.
- **Function Right**
  Select the function rights of the role:
  - **1**
    Users with this role can read device parameters but cannot change them. Users with this role can change their own password.
  - **15**
    Users with this role can both read and change device parameters.

  Note

  Function right cannot be changed

  If you have assigned a role, you can no longer change the function right of the role.

  If you want to change the function right of a role, follow the steps outlined below:
  1. Delete all assigned users.
  2. Change the function right of the role:
  3. Assign the role again.

- **Description**
  Enter a description for the role. With predefined roles a description is displayed. The description text can be up to 100 characters long.

Procedure

Creating a role

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

Deleting a role

1. Select the check box in the row to be deleted.
2. Click the "Delete" button. The entries are deleted and the page is updated.

6.9.1.3 Groups

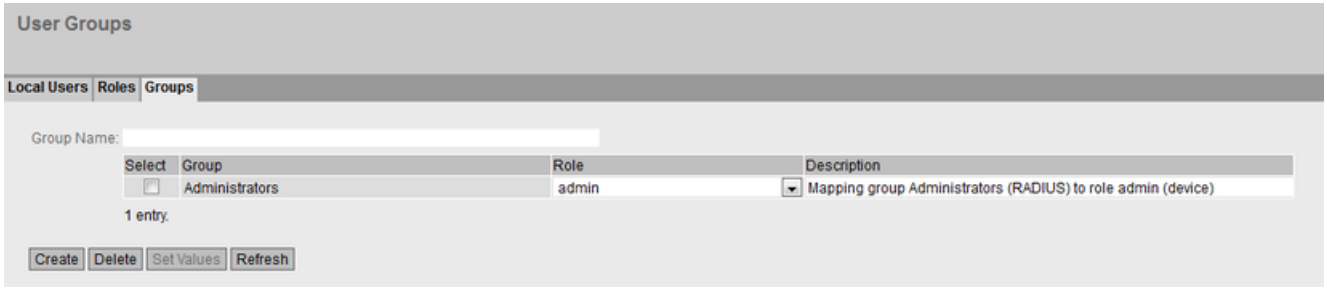
User groups

On this page you link a group with a role.

In this example the group "Administrators" is linked to the "admin" role: The group is defined on a RADIUS server. The role is defined locally on the device. When a RADIUS server authenticates a user and assigns the user to the "Administrators" group, this user is given rights of the "admin" role.

Note

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



Description

The page contains the following:

- **Group Name**
  Enter the name of the group. The name must match the group on the RADIUS server. The name must meet the following conditions:
  - It must be unique.
  - It must be between 1 and 64 characters long.
  - The following are not permitted: § ? " ; :

The table contains the following columns:

- **Select**
  Select the check box in the row to be deleted.
- **Group**
  Shows the name of the group.

- **Role**
  Select a role. Users who are authenticated with the linked group on the RADIUS server receive the rights of this role locally on the device.
  You can choose between system-defined and self-defined roles, refer to the page "Security > Users > Roles.".
- **Description**
  Enter a description for the link of the group.to a role. The description text can be up to 100 characters long.

Procedure

Linking a group to a role.

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

Deleting the link between a group and a role

1. Select the check box in the row to be deleted.
2. Click the "Delete" button. The entries are deleted and the page is updated.

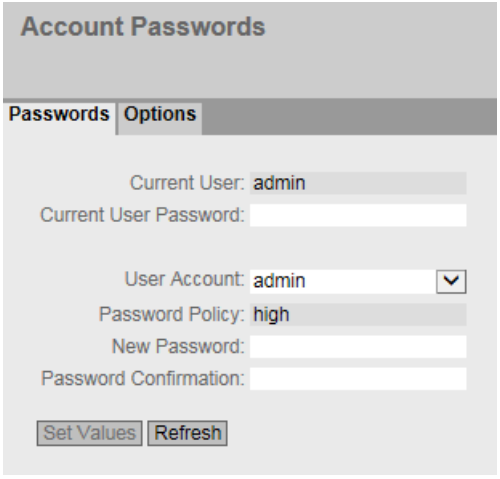
6.9.2 Passwords

Configuration of the passwords

Note

If you are logged in via a RADIUS server, you cannot change any passwords.

On this page, you can change passwords. If you are logged in with the right to change device parameters, you can change the passwords for all user accounts. If you are logged in as user, you can only change your own password.



Description of the displayed boxes

- **Current User**
  Shows the user that is currently logged in.
- **Current User Password**
  Enter the password for the currently logged in user.
- **User Account**
  Select the user whose password you want to change.
- **Password Policy**
  Shows which password policy is being used when assigning new passwords.

  Note

  Checking the password policy of existing users

  The set password policy is used when assigning new passwords. Existing passwords are not checked. If you change the password policy from "Low" to "High", the previously used passwords remain valid. As an important measure for increasing security, change the passwords used up to now.

  – High
    Password length: at least 8 characters, maximum 128 characters
    At least 1 uppercase letter
    At least 1 special character
    At least 1 number
  – Low
    Password length: at least 6 characters, maximum 128 characters
  – Custom
    You configure the password policy on the page "Security > Passwords > Options".

- **New Password**
  Enter the new password for the selected user.
  - It must not contain the following characters: ; : ' ? ß § " ² ³ ° | € µ ä ö ü Ä Ö Ü
  - The characters for Space and Delete also cannot be contained.
- **Password Confirmation**
  Enter the new password again to confirm it.

Procedure

1. From the "User Account" drop-down list, select the user whose password you want to change.
2. Enter the valid password for the currently logged in user in the "Current User Password" input box.
3. Enter the new password for the selected user in the "New Password" input box.
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

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

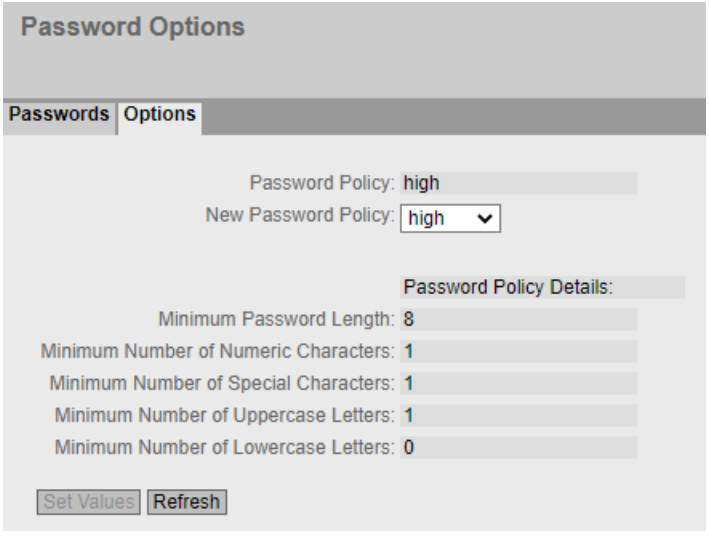
Note

Changing the password in Trial mode

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

6.9.2.1 Options

On this page, you specify which password policy will be used when assigning new passwords.



Description

- **Password Policy**
  Shows which password policy is currently being used.
- **New Password Policy**
  Select the required setting from the drop-down list.
  - High
    Password length: at least 8 characters, maximum 128 characters
    At least 1 number
    At least 1 special character
    At least 1 uppercase letter
  - Low
    Password length: at least 6 characters, maximum 128 characters
  - User-defined
    Configure the desired password requirements under "Password Policy Details".
- **Password Policy Details**
  When you have selected the "High" or "Low" password policy, the relevant password requirements are displayed.
  When you have selected the "User-defined" password policy, you can configure the relevant password requirements.
  - Minimum Password Length
    Specifies the minimum length of a password.
  - Minimum Number of Numeric Characters
    Specifies the minimum number of numeric characters in a password.
  - Minimum Number of Special Characters
    Specifies the minimum number of special characters in a password.
  - Minimum Number of Uppercase Letters
    Specifies the minimum number of uppercase characters in a password.
  - Minimum Number of Lowercase Letters
    Specifies the minimum number of lowercase characters in a password.

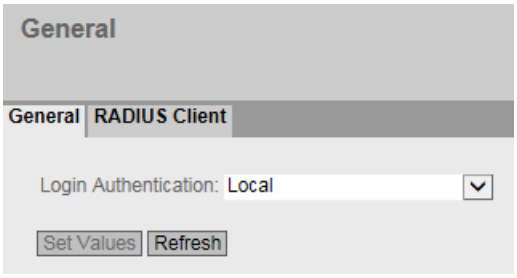
6.9.3 AAA

6.9.3.1 General

Login of network nodes

The designation "AAA" stands for "Authentication, Authorization, Accounting". This feature is used to identify and allow network nodes, to make the corresponding services available to them and to specify the range of use.

On this page, you configure the login.



Description

The page contains the following boxes:

Note

To be able to use the login authentication "RADIUS", "Local and RADIUS" or "RADIUS and fallback Local", a RADIUS server must be stored and configured for user authentication.

- **Login Authentication**
  Specify how the login is made:
  - Local
    The authentication must be made locally on the device.
  - RADIUS
    The authentication must be handled via a RADIUS server.
  - Local and RADIUS
    The authentication is possible both with the users that exist on the device (user name and password) and via a RADIUS server.
    The user is first searched for in the local database. If the user does not exist there, a RADIUS request is sent.
  - RADIUS and fallback Local
    The authentication must be handled via a RADIUS server.
    A local authentication is performed only when the RADIUS server cannot be reached in the network.

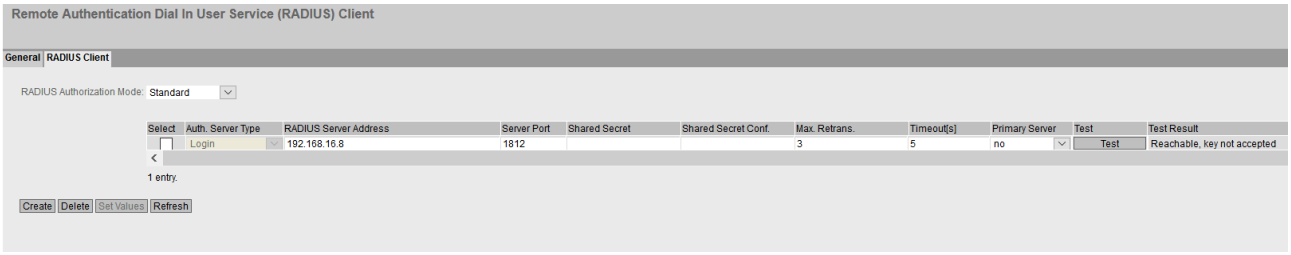
6.9.3.2 RADIUS-Client

Authentication over an external server

The concept of RADIUS is based on an external authentication server.

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

If no server responds, there is no authentication.



Description

The page contains the following boxes:

- **RADIUS Authorization Mode**
  For the login authentication, the RADIUS authorization mode specifies how the rights are assigned to the user with a successful authentication.
  - Standard
    In this mode the user is logged in with administrator rights if the server returns the value "Administrative User" to the device for the attribute "Service Type". In all other cases the user is logged in with read rights.
  - Vendor Specific
    In this mode the assignment of rights depends on whether and which group the server returns for the user and whether or not there is an entry for the user in the table "External User Accounts".

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **Auth. Server Type**
  Shows which authentication method the server will be used for.
  - Login
    The server is used only for the login authentication.
- **RADIUS Server Address**
  Enter the IP address or the FQDN (Fully Qualified Domain Name) of the RADIUS server.
- **Server Port**
  Here, enter the input port on the RADIUS server. As default, input port 1812 is set. The range of values is 1 to 65535.
- **Shared Secret**
  Enter your access ID here. The range of values is 1...128 characters.
- **Shared Secret Conf.**
  Enter your access ID again as confirmation.
- **Max. Retrans.**
  Enter the maximum number of retries for an attempted query.
  The initial connection attempt is repeated the number of times specified here before another configured RADIUS server is queried or the login counts as having failed. As default 3 retries are set, this means 4 connection attempts. The range of values is 1 to 5.

- **Timeout[s]**
  Specify how long the RADIUS client waits for a response from the RADIUS server before attempting login again.
- **Primary Server**
  Using the options in the drop-down list, specify whether or not this server is the primary server. You can select one of the options "yes" or "no".
- **Test**
  With this button, you can test whether or not the specified RADIUS server is available. The test is performed once and not repeated cyclically.
- **Test Result**
  Shows whether or not the RADIUS server is available:
  - Not reachable
    The IP address is not reachable.
    The IP address is reachable, the RADIUS server is, however, not running.
  - Reachable, key not accepted
    The IP address is reachable, the RADIUS server does not, however accept the shared secret.
  - Reachable, key accepted
    The IP address is reachable, the RADIUS server accepts the specified shared secret.

Steps in configuration

Entering a new server

1. Click the "Create" button. A new entry is generated in the table.
   The following default values are entered in the table:
   - RADIUS Server Address: 0.0.0.0
   - Server Port: 1812
   - Max. Retrans.: 3
   - Primary server: No
2. In the relevant row, enter the following data in the input boxes:
   - RADIUS Server Address
   - Server Port
   - Shared Secret
   - Shared Secret Conf
   - Max. Retrans.: 3
   - Primary server: No
3. If necessary check the reachability of the RADIUS server.
4. Click the "Set Values" button.

Repeat this procedure for every server you want to enter.

Modifying servers

1. In the relevant row, enter the following data in the input boxes:
   - RADIUS Server Address
   - Server Port
   - Shared Secret
   - Shared Secret Conf
   - Max. Retrans.
   - Primary Server
2. If necessary check the reachability of the RADIUS server.
3. Click the "Set Values" button.

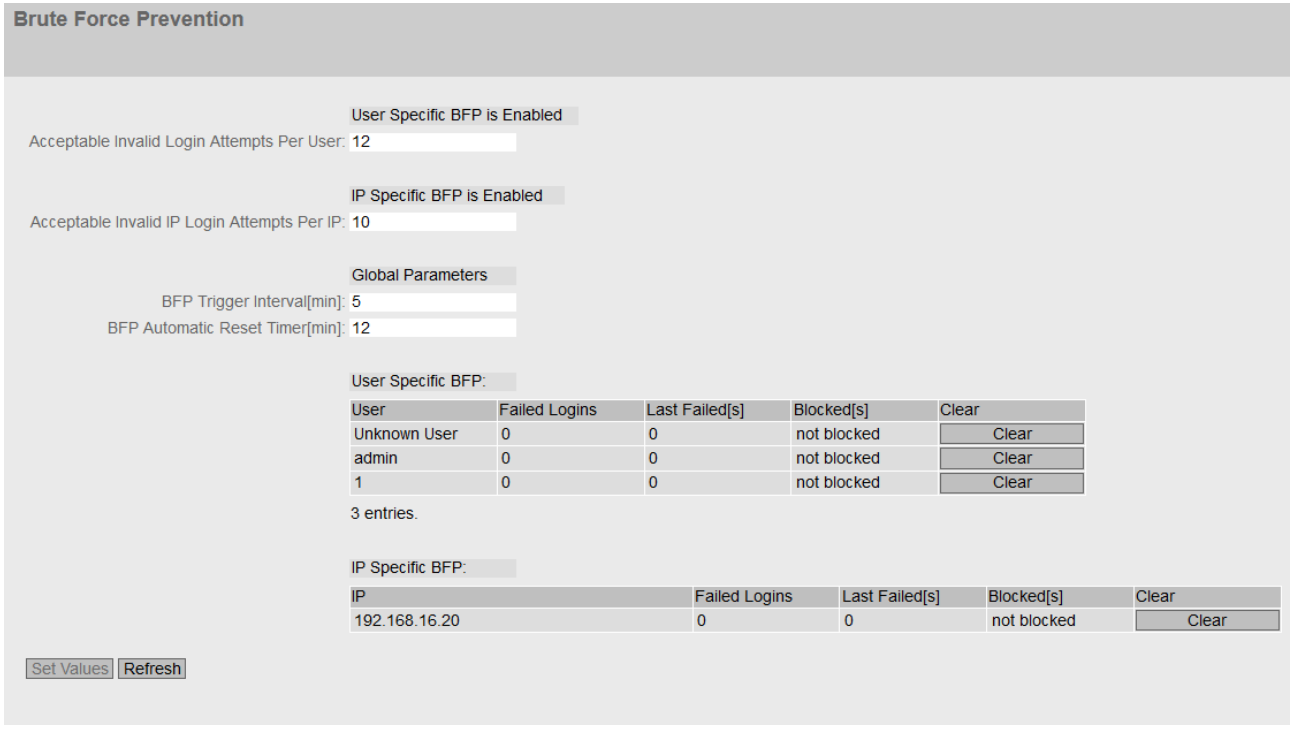
Repeat this procedure for every server whose entry you want to modify

Deleting servers

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

6.9.4 Brute Force Prevention

Brute Force Prevention (BFP) refers to the protection of the device from unauthorized access by trying a sufficiently large number of passwords. The number of incorrect login attempts within a specific time period is limited for this purpose.



Description

The page contains the following boxes:

- **User Specific BFP is Enabled. / User Specific BFP is Disabled.**
  - Enabled:
    With login authentication, the "Local" or "Local and RADIUS" mode is set and the maximum number of invalid login attempts is greater than 0.
  - Disabled:
    With login authentication, the "RADIUS" or "RADIUS and fallback Local" mode is set or the maximum number of invalid login attempts is 0.

  You configure the login authentication under "Security > AAA > General > Login Authentication".
- **Acceptable Invalid Login Attempts Per User**
  The maximum number of invalid login attempts for a user accepted by the device. Further login attempts for this user are blocked for a specific time.
  The users that are not configured as local users for the device are summarized under the user name "UnknownUser".
  0: User Specific BFP is Disabled.

- **IP Specific BFP is Enabled. / IP Specific BFP is Disabled.**
  Shows whether the IP-specific Brute Force Prevention is enabled.
- **Acceptable Invalid IP Login Attempts Per IP**
  The maximum number of invalid login attempts for an IP address accepted by the device. Further login attempts for this IP address are blocked for a specific time.
  0: IP Specific BFP is Disabled.
- **BFP Trigger Interval [min]**
  The time in minutes that is relevant for counting invalid login attempts.
  If the maximum number of invalid login attempts is exceeded during this time, the device blocks login for a specific period of time.
  Invalid login attempts per user and per IP address are handled independently of one another.
- **BFP Automatic Reset Timer[min]**
  Time in minutes for which the device blocks login because the maximum number of invalid login attempts was exceeded.
  0: The timer is disabled.

The **User Specific BFP** table has the following columns:

- **User**
  The users configured locally on the device. The users that are not locally configured on the device are summarized under the user name "UnknownUser".
- **Failed Logins**
  The number of failed login attempts.
- **Last Failed [s]**
  Time in seconds (s) since the last failed login attempt. To display the current value, click the "Refresh" button.
- **Blocked [s]**
  The time in seconds (s) until the blocking will be removed. To display the current value, click the "Refresh" button.
  When a blocked user attempts to log in before the timer expires, the timer restarts.
- **Delete**
  Ends blocking for the user and resets the displays in the "Last Failed [s]" and "Blocked [s]" boxes.

The **IP Specific BFP** table has the following columns:

- **IP**
  The IP address of the device for the login attempt.
- **Failed Logins**
  The current number of failed login attempts.
- **Last Failed [s]**
  Time in seconds (s) since the last failed login attempt. To display the current value, click the "Refresh" button.

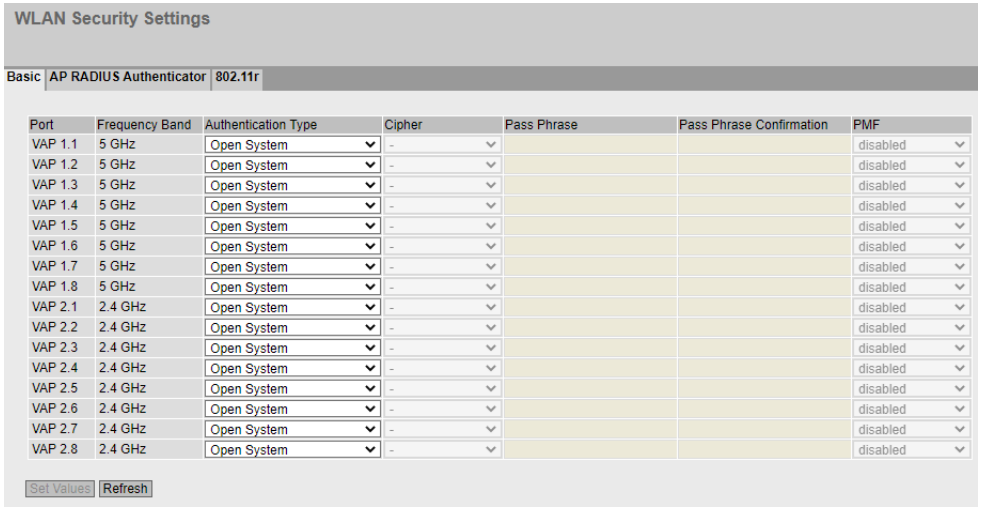
- **Blocked [s]**
  The time in seconds (s) until the blocking will be removed. To display the current value, click the "Refresh" button.
  When a blocked IP address attempts to log in before the timer expires, the timer restarts.
- **Delete**
  Ends blocking for the IP address and resets the displays in the "Last Failed [s]" and "Blocked [s]" boxes.

6.9.5 WLAN

6.9.5.1 Basic (Access Point)

Safety levels

To make the network secure, authentication and encryption are used. On this page, you specify the security settings.



Description

The table has the following columns:

- **Port**
  Shows the available ports.
- **Frequency Band**
  Shows the frequency band.

- **Authentication Type**
  Select the type of authentication. The selection depends on the operating mode and the transmission standard.
  - Open System
    There is no authentication.
  - WPA (RADIUS)
    Wi-Fi Protected Access (WPA) is a method specified by the Wi-Fi Alliance to close security gaps in WEP. Authentication using a server (802.1x) is mandatory. 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 carried out 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. However, WPA authentication works with the RADIUS server.
  - WPA2-PSK
    WPA2-PSK is based on the 802.11i standard. However, WPA authentication works without a RADIUS server. Instead of this, a key (pass phrase) is stored on each client and access point. The pass phrase is used for authentication and further encryption.
  - WPA/WPA2-AUTO-PSK
    First try to connect with WPA2. If the client is not WPA2-enabled, the connection is made using WPA.
  - WPA/WPA2 AUTO (RADIUS)
    First try to connect using WPA2 (RADIUS). If the client is not WPA2-enabled, the connection is made using WPA (RADIUS).
  - WPA3-SAE
    Only configurable in WLAN mode "802.11ax"
    WPA3 replaces WPA2 and uses the Simultaneous Authentication of Equals (SAE) to authenticate access points and clients. With SAE, keys are mutually stored and exchanged, but the pass phrase is not made public, so attackers cannot find the keys through brute force dictionary attacks. With WPA3, PMF must be negotiated for all WPA3 connections, which offers additional protection against deauthentication and disassociation attacks.

- **Cipher**
  - AUTO
    Either AES or TKIP is automatically selected, depending on the capability of the other station.
  - TKIP (Temporal Key Integrity Protocol)
    A symmetrical stream encryption method with the RC4 (Ron's Code 4) algorithm. 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.
- **Key**
  Enter a key here. This key must be known on both the client and the access point and is entered by the user at both ends.
  - For a key with 8 to 63 characters, you can only use the following readable ASCII characters: 0x20 - 0x7e.
  - For a key with precisely 64 characters, you can use the following ASCII characters: 0 - 9, a - f and A - F.
- **Key Confirmation**
  Confirm the key entered above.
- **PMF (Protected Management Frames)**
  Can only be used with the following:
  - WLAN mode: IEEE 802.11n/ac/ax
  - Authentication type: WPA2-PSK, WPA2 (RADIUS) and WPA3-SAE

  With this setting, the management frames are cryptographically protected. This prevents, for example, the WLAN client being separated from the access point due to corrupted disassociation / deauthenticate frames. You can find more information on this in the IEEE 802.11w standard.
  The following settings are possible:
  - disabled
    The management frames are not encrypted.
  - required
    The management frames are always encrypted. A connection of the WLAN clients to the access point is only possible when these also support PMF. With the WPA3-SAE authentication type, this setting is always selected and cannot be configured.
  - optional
    The management frames are encrypted or unencrypted depending on support of the WLAN client.

Procedure

1. Select the required security settings.
2. Click the "Set Values" button.

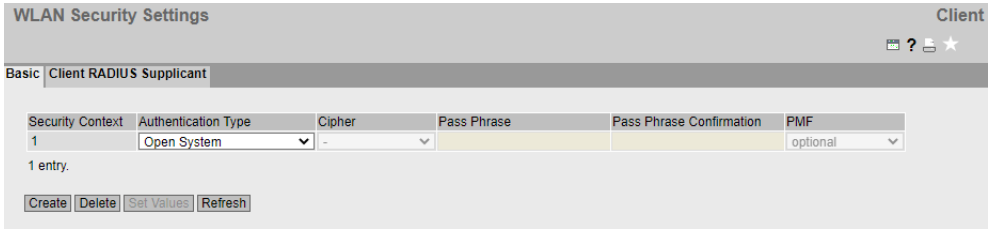
6.9.5.2 Basic (Client)

Safety levels

To make the network secure, authentication and encryption are used. On this page, you specify the security settings.

Note

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



Description

The table has the following columns:

- **Security Context**
  Shows the security context.
- **Authentication Type**
  Select the type of authentication. The selection depends on the operating mode and the transmission standard.
  - Open System
    There is no authentication.
  - WPA (RADIUS)
    Wi-Fi Protected Access (WPA) is a method specified by the Wi-Fi Alliance to close security gaps in WEP. Authentication using a server (802.1x) is mandatory. The dynamic exchange of keys at each data frame introduces further security.

    Note

    Make the relevant RADIUS settings initially on the page "Security > WLAN > Client RADIUS Supplicant".
  - WPA-PSK
    WPA Pre Shared Key (WPA-PSK) is a weakened form of WPA. In this method, authentication is not carried out 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. However, WPA authentication works with the RADIUS server.

    Note

    Make the relevant RADIUS settings initially on the page "Security > WLAN > Client RADIUS Supplicant".
  - WPA2-PSK
    WPA2-PSK is based on the 802.11i standard. However, WPA authentication works without a RADIUS server. Instead of this, a key (pass phrase) is stored on each client and access point. The pass phrase is used for authentication and further encryption.
  - WPA3-SAE
    Only configurable in WLAN mode "802.11ax"
    WPA3 replaces WPA2 and uses the Simultaneous Authentication of Equals (SAE) to authenticate access points and clients. With SAE, keys are mutually stored and exchanged, but the pass phrase is not made public, so attackers cannot find the keys through brute force dictionary attacks. With WPA3, PMF must be negotiated for all WPA3 connections, which offers additional protection against deauthentication and disassociation attacks.
- **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**
  - AUTO
    Either AES or TKIP is automatically selected, depending on the capability of the other station.
  - TKIP (Temporal Key Integrity Protocol)
    A symmetrical stream encryption method with the RC4 (Ron's Code 4) algorithm. 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.

- **Key**
  Enter a key here for authentication with the WPA2-PSK or WPA3-SAE . This key must be known on both the client and the access point and is entered by the user at both ends.
  For a key with 8 to 63 characters, you can only use the following readable ASCII characters: 0x20 - 0x7e.
  For a key with precisely 64 characters, you can use the following ASCII characters: 0 - 9, a - f and A - F.

  Note

  New key when the authentication type is changed

  When the authentication type is changed, the previous key is deleted.

- **Key Confirmation**
  Confirm the key entered above.
- **PMF (Protected Management Frames)**
  Can only be used with the following:
  - WLAN mode: IEEE 802.11n/ac/ax
  - Authentication type: WPA2-PSK, WPA2 (RADIUS) and WPA3-SAE

  With this setting, the management frames are cryptographically protected. This prevents, for example, the WLAN client being separated from the access point due to corrupted disassociation / deauthenticate frames. You can find more information on this in the IEEE 802.11w standard.
  The following settings are possible:
  - disabled
    The management frames are not encrypted.
  - required
    The management frames are always encrypted. A connection of the WLAN clients to the access point is only possible when these also support PMF. With the WPA3 authentication type, this setting is preset and cannot be configured.
  - optional
    The management frames are encrypted or unencrypted depending on support of the access point.

Procedure

1. Select the required security settings. The settings that are possible depend on the set "Authentication Type".
2. Click the "Set Values" button.

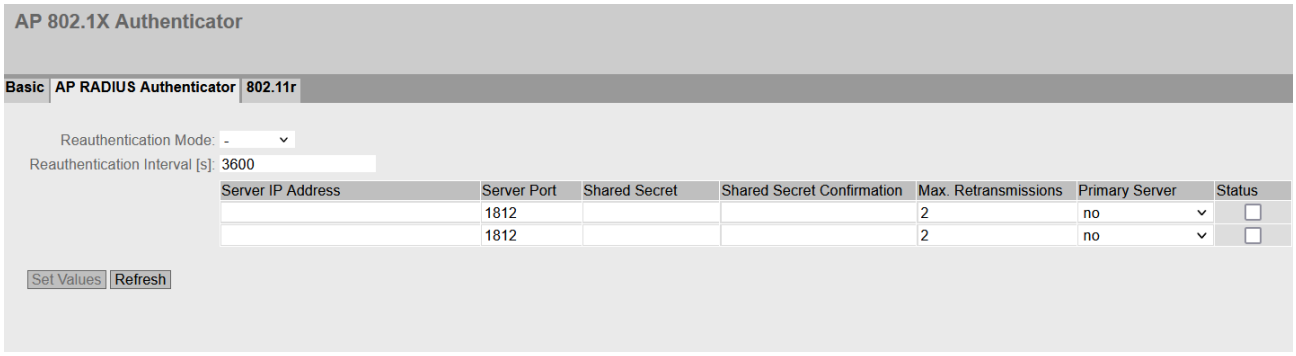
6.9.5.3 AP RADIUS Authenticator

Note

This WBM page is only available in access point mode.

Configuration of the RADIUS server

On this WBM page, you define the RADIUS servers and the RADIUS authentication of the access point. You can enter data for two RADIUS servers.



Description

The page contains the following boxes:

- **Reauthentication Mode**
  Specify who sets the time after which the clients are forced to reauthenticate.
  - - (disabled)
    The reauthentication mode is disabled.
  - Server
    Enables time management on the server.
  - Local
    Enables local time management. Set the validity period for "Reauthentication Interval".
- **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**
  Enter the IP address or the FQDN (Fully Qualified Domain Name) of the RADIUS server.
- **Server Port**
  Here, enter the input port on the RADIUS server.
- **Shared Secret**
  Enter the password of the RADIUS server.
  For the password, ASCII code 0x20 to 0x7e is used.
- **Shared Secret Conf**
  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 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:
   - IP address or FQDN of the RADIUS server
   - Port number of the input port
   - Password
   - Confirmation of the password
   - Maximum number of transmission retries
   - Primary server
2. Select the "Status" check box to enable the RADIUS server.
3. Click the "Set Values" button.

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

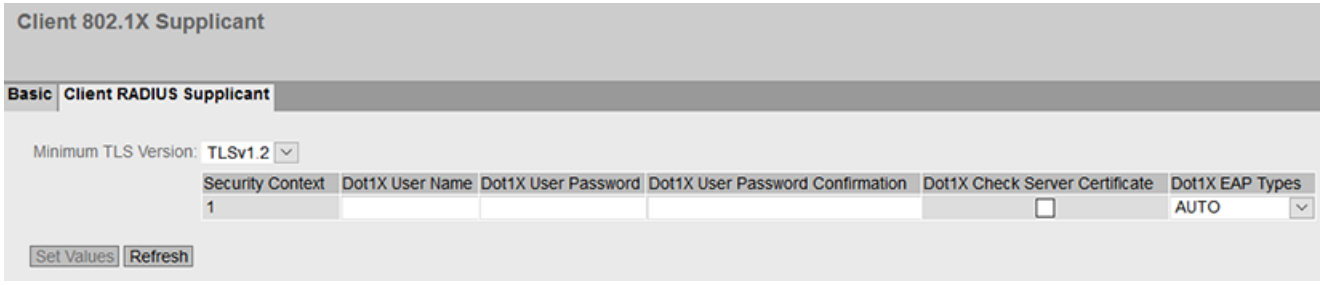
6.9.5.4 Client RADIUS Supplicant

Client Supplicant

On this WBM page, you configure the settings for the RADIUS authorization of the client.

Note

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



Description

- **Minimum TLS Version**
  Specify the minimum TLS version to be used for WLAN RADIUS authentication.

  Note

  RADIUS Server

  This is only possible when the RADIUS Server supports the TLS version.

  Note

  Minimum TLS version must be appropriate to the security level of the SSL certificates

  Authentication attempts with WLAN client and server certificates whose encryption mechanisms do not correspond to the requirements of the selected min. TLS version fail. Select a suitable minimum TLS version.

  Example: The SHA1 signature algorithm is not supported by TLS V1.2 as of version V3.0. If you want to use SHA1 certificates, the min. TLS version cannot be higher than V1.1. You can find information on the supported security mechanisms with RADIUS authentication in the WBM, appendix "Ciphers used > RADIUS (Page 345)".

The table has the following columns:

- **Security Context**
  Shows the security context.
- **Dot1x User Name**
  Enter the user name with which you want to log in to the RADIUS server.

- **Dot1x User Password**
  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.

Note

Dot1X user name and Dot1X user password

With WPA (RADIUS), WPA2 (RADIUS), EAP-TLS, EAP-TTLS and PEAP the Dot1X user name and the Dot1X user password must be configured.

With the setting "Auto" either the certificate must be loaded or the Dot1X user name and the Dot1X user passport must be configured.

- **Verifying tghe Dot1X server certifcate**
  Specify whether or not the RADIUS server identifies itself to the client using a certificate.

  Note

  Using certificates

  Renew the certificate before it expires. If you do not renew the certificate in time, it will not be possible to establish a connection after expiry.

- **Dot1x EAP Types**
  Specify the authentication methods. The following methods exist:
  - Auto
    Client offers RADIUS server all methods.
  - EAP-TLS
    Extensible Authentication Protocol - Transport Layer Security
    Uses certificates for authentication.
  - EAP-TTLS
    Extensible Authentication Protocol - Tunnel Transport Layer Security
    After setting up the TLS tunnel, MS-CHAPv2 is used for internal authentication.
  - PEAP
    Protected Extensible Authentication Protocol
    Alternative draft protocol of IETF for EAP-TTLS

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.

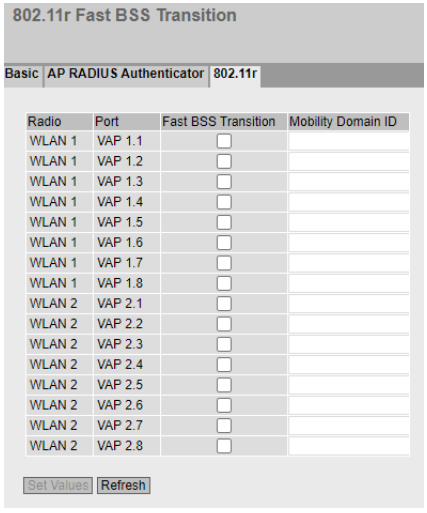
6.9.5.5 802.11r

On this WBM page, you configure the setting for Fast BSS Transition.

Note

This WBM page is only available in access point mode.

You can find additional information under "Description > IEEE 802.11r".



Requirement

- The access points are members of the same mobility domain.
- Only possible with WPA2 (WPA2-PSK and WPA2 RADIUS) and WPA3 encryption.

Description

The table has the following columns:

- **Radio**
  Shows the available WLAN interfaces.
- **Port**
  Shows the VAP interface.

- **Fast BSS Transition**
  When enabled, the "Fast BSS Transition" function is supported. Can only be enabled when the mobility domain is entered.

  Note

  Restriction of the Fast BSS Transition function in V2.0

  The access point and the client only support "Fast Transition over the Air".

- **Mobility Domain ID**
  Enter the ID of the mobility domain. The access points with the same ID are members of one mobility domain. Based on the ID, the WLAN client recognizes whether the access point is a member of the same mobility domain and can therefore log on without delay.

6.9.6 Inter AP Blocking

6.9.6.1 Basic

Note

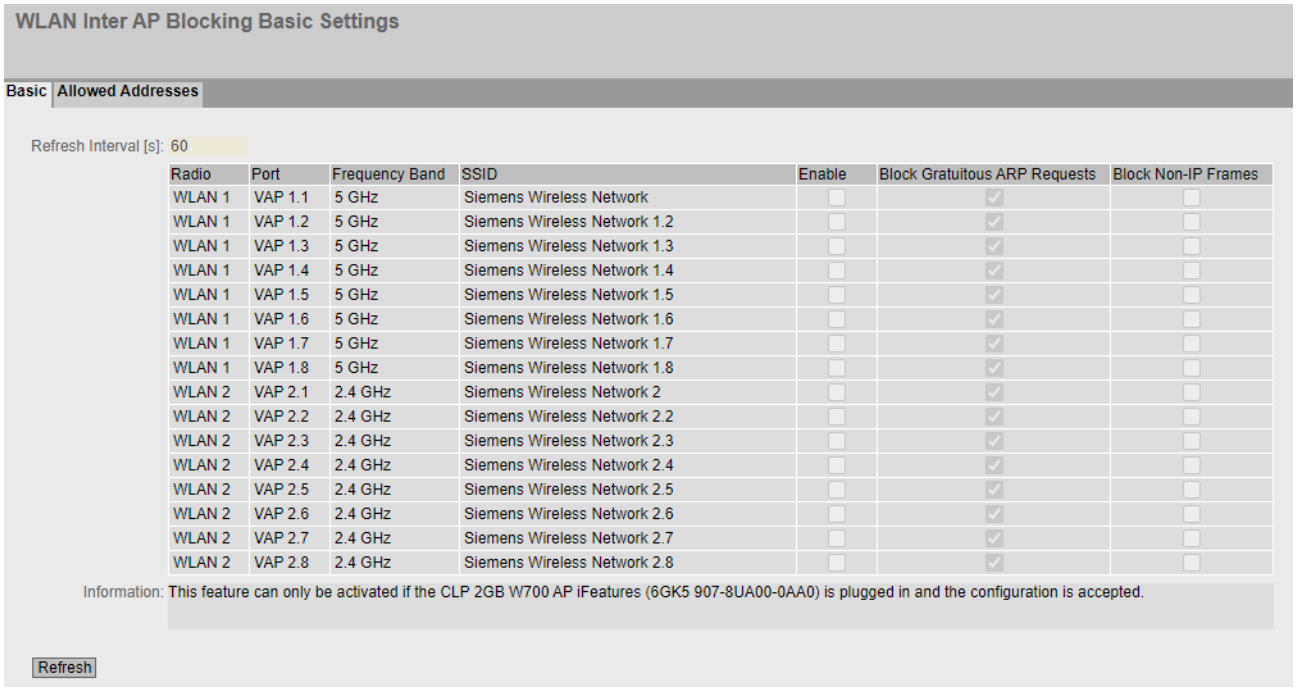
This WBM page is only available in access point mode.

This function can only be enabled when the CLP 2GB W700 AP iFeatures (6GK5 907-8UA00-0AA0) is inserted in the device and the configuration has been applied.

When should Inter AP blocking be used?

The clients connected to an access point can normally communicate with all devices of the cabled 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.



Radio	Port	Frequency Band	SSID	Enable	Block Gratuitous ARP Requests	Block Non-IP Frames
WLAN 1	VAP 1.1	5 GHz	Siemens Wireless Network	☐	☑	☐
WLAN 1	VAP 1.2	5 GHz	Siemens Wireless Network 1.2	☐	☑	☐
WLAN 1	VAP 1.3	5 GHz	Siemens Wireless Network 1.3	☐	☑	☐
WLAN 1	VAP 1.4	5 GHz	Siemens Wireless Network 1.4	☐	☑	☐
WLAN 1	VAP 1.5	5 GHz	Siemens Wireless Network 1.5	☐	☑	☐
WLAN 1	VAP 1.6	5 GHz	Siemens Wireless Network 1.6	☐	☑	☐
WLAN 1	VAP 1.7	5 GHz	Siemens Wireless Network 1.7	☐	☑	☐
WLAN 1	VAP 1.8	5 GHz	Siemens Wireless Network 1.8	☐	☑	☐
WLAN 2	VAP 2.1	2.4 GHz	Siemens Wireless Network 2	☐	☑	☐
WLAN 2	VAP 2.2	2.4 GHz	Siemens Wireless Network 2.2	☐	☑	☐
WLAN 2	VAP 2.3	2.4 GHz	Siemens Wireless Network 2.3	☐	☑	☐
WLAN 2	VAP 2.4	2.4 GHz	Siemens Wireless Network 2.4	☐	☑	☐
WLAN 2	VAP 2.5	2.4 GHz	Siemens Wireless Network 2.5	☐	☑	☐
WLAN 2	VAP 2.6	2.4 GHz	Siemens Wireless Network 2.6	☐	☑	☐
WLAN 2	VAP 2.7	2.4 GHz	Siemens Wireless Network 2.7	☐	☑	☐
WLAN 2	VAP 2.8	2.4 GHz	Siemens Wireless Network 2.8	☐	☑	☐

Description

The page contains the following box:

- **Update interval [s]**
  Enter the update interval for the ARP resolution of the allowed IP addresses. The resolved MAC addresses are displayed under "Information > Security > Inter AP Blocking".

The table has the following columns:

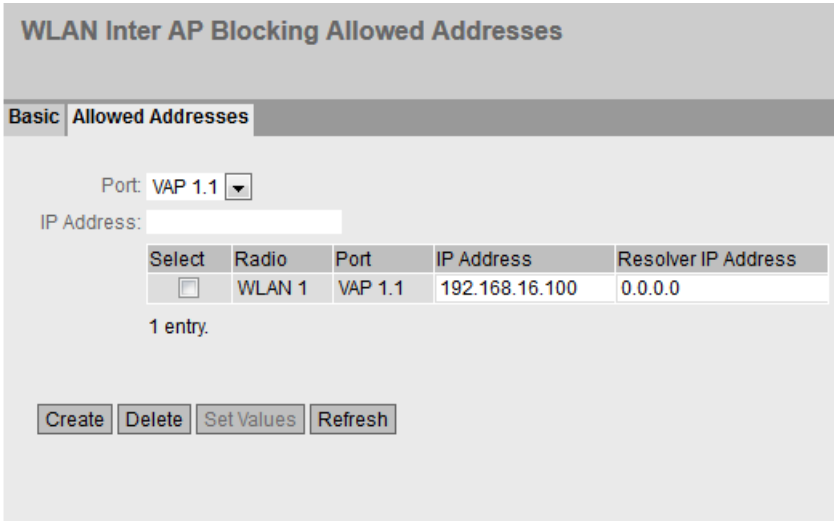
- **Radio**
  Shows the WLAN interface to which the settings relate.
- **Port**
  Shows the VAP interface to which the settings relate.
- **Frequency Band**
  Shows the frequency band to which the settings relate.
- **SSID**
  Shows the SSID to which the settings relate.
- **Enable**
  When enabled, the access restriction is used. You configure which devices are accessible to the clients in "Security > Inter AP Blocking > Allowed Addresses".
- **Block Gratuitous ARP Requests**
  When enabled, gratuitous ARP packets from this VAP interface are not forwarded to Ethernet.
- **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.

6.9.6.2 Allowed Addresses

Note

This WBM page is only available in access point mode.

On this WBM page, you specify which devices are accessible to the clients.



Description

The page contains the following boxes:

- **Port**
  Select the required port from the drop-down list.
- **IP Address**
  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 that the access point uses to resolve the allowed IP address. The entry is necessary when the management IP address of the access point is located in a different subnet.
  If the IP address "0.0.0.0" is configured for "Resolver IP Address", the management IP address is used for resolution.

Procedure

Creating an entry

1. Select a port from the "Port" drop-down list.
2. In the "IP Address" box, enter the IP address accessible for the client.
3. Click the "Create" button. A new entry is created in the table.

Deleting an entry

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

6.10 "iFeatures" menu

6.10.1 iPCF-2

On this page, you can enable iPCF-2.

iPCF-2 is recommended for use in environments that use automation protocols. With iPCF-2, cyclic data exchange between the access point and its logged-on clients is defined and maintained, provided that a dedicated free channel with sufficient reception strength is available for iPCF-2. In addition, depending on the application, no DFS channel should be used.

Note

This page is only available in connection with the inserted CLP iFeatures. For more detailed information, refer to the section "Configuration License PLUG (CLP) (Page 29)".

Note

Mutual interlock of iFeatures

iPRP and iPCF-2 are not compatible with each other and cannot be used at the same time on a device.
During dual operation of an access point, an iFeature cannot be enabled on a WLAN interface if an iFeature has already been enabled on the other interface.

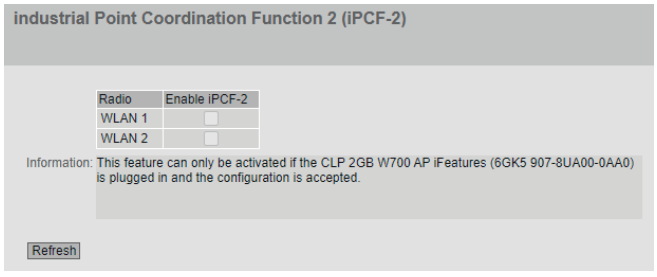
Requirements for enabling iPCF-2

- WLAN mode on the affected interface is set to 802.11ax.
- VAP x.1 is configured and enabled.
- The authentication type on the VAP x.1 is "Open System" or "WPA2-PSK".
- The function PMF on the VAPx.1 is disabled.

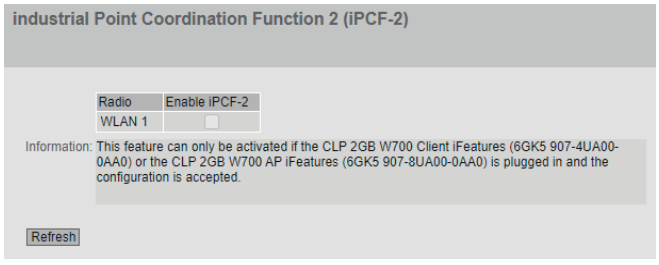
When should iPCF-2 be used?

iPCF-2 enables tested real-time communication in various scenarios and will be developed further in the future firmware versions. Tested and released scenarios are described in the document "Areas of Operation for Industrial Wireless LAN in a PROFINET IO Environment"; see the following entry ID:
22681042 (https://support.industry.siemens.com/cs/ww/en/view/22681042).

Display in access point mode



Display in client mode



Description

The table has the following columns:

- **Radio**
  Shows the WLAN interface to which the settings relate.
- **Enable iPCF-2**
  Enable or disable iPCF-2 mode.
  A message about changes in the settings is displayed.

Procedure

1. Select the "Enable iPCF-2" option for the required WLAN interface.
2. Click the "Update" button.

Result

iPCF-2 mode is enabled. Enabling this results in the following changes on the WLAN interface:

- VAPx.1 is enabled on the page "Interface > WLAN > AP". All other VAPs are disabled on the respective interface.
- If the authentication type on VAP x.1 is "WPA2-PSK", the settings on the page "Security > WLAN > 802.11r" are configured as follows:
  - The Mobility Domain ID is automatically generated on VAPx.1 based on the last two SSID characters. The value is applied for VAPx.1.
  - Fast BSS Transition is enabled on VAP x.1.

6.10.2 iPRP

On this page, you can enable iPRP.

Note

This page is only available in connection with the inserted CLP iFeatures. For more detailed information, refer to the section "Configuration License PLUG (CLP) (Page 29)".

Note

Mutual interlock of iFeatures

iPRP and iPCF-2 are not compatible with each other and cannot be used at the same time on a device.

During dual operation of an access point, an iFeature cannot be enabled on a WLAN interface if an iFeature has already been enabled on the other interface.

Requirements for using iPRP

- The Base Bridge Mode "802.1Q VLAN Bridge" is set.
- The VLANs have been created.
- Access Point mode: The VAP interfaces are enabled. The first two VAP interfaces per radio interface can be configured for iPRP.
- Client mode:
  - "Layer 2 Tunnel" is set for "MAC Mode".
  - Either "Always" or "Disabled" is set for "Background Scan Mode".
- The Spanning Tree Protocol is disabled.

Note

SCALANCE W700 IEEE802.11ax firmware does not support synchronization of the clients during scanning and roaming operations. Therefore, simultaneous scanning and roaming operations, which can result in brief transfer interruptions, can occur.

When should iPRP be used?

Note

iPRP with oversize frames (jumbo frames)

To be able to use oversize frames, oversize frames (jumbo frames) must be configured on all devices in the network.

Agent VLAN (management VLAN) with iPRP

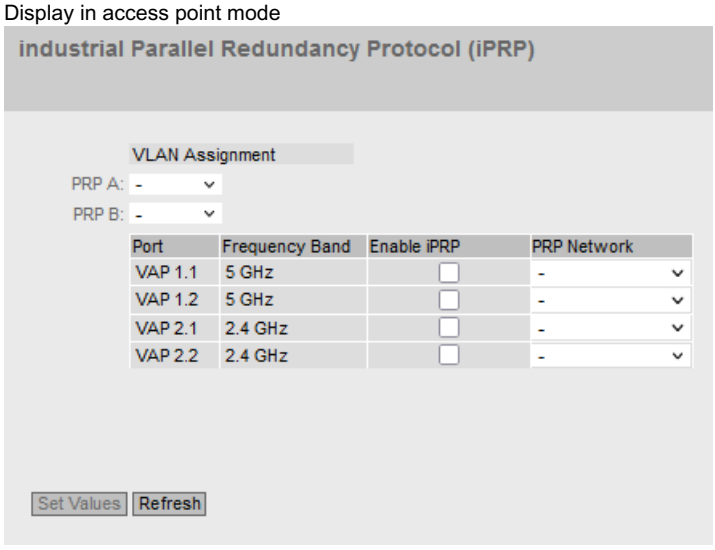
The iPRP VLAN can be used as the agent VLAN. This depends where the device is located.

- If the device is located in the PRP network A or PRP network B, use the VLAN that PRP A or PRP B is assigned to as the agent VLAN.
- If the access points are located in both PRP networks, you can use one of the two VLANs as the agent VLAN. As an alternative you can also use other VLANs as agent VLANs. The division into PRP networks A and B must remain. A single management VLAN for all devices in network A and B is not possible without further measures.

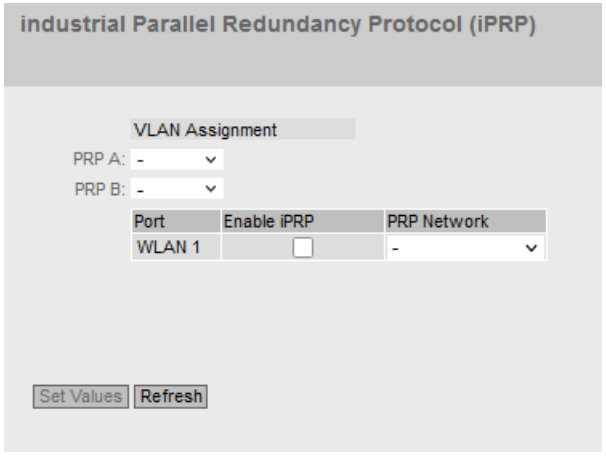
With the "industrial Parallel Redundancy Protocol" (iPRP), the PRP technology can be used in wireless networks. With IPRP the PRP frames are transferred parallel via two wireless links. The parallel transfer allows disruptions of the transfer on one wireless link to be compensated on the other.

With transfer paths that are not the same, iPRP reduces the number of duplicated and out-of-order packets. The application/protocol used must be able to handle the remaining duplicates and out-of-order packets.

Display in access point mode



Display in client mode



Description

The page contains the following:

- **Ethernet interface** (only with SCALANCE WxM763)
  Select the required Ethernet interface P1 ... P4 on which you want to enable iPRP.
- **PRP A**
  Select the VLAN assignment for PRP A.
- **PRP B**
  Select the VLAN assignment for PRP B.

The table contains the following columns:

- **Port** (only in access point mode)
  Shows the available ports.
- **Frequency Band** (only in access point mode)
  Shows the frequency band.
  - 2.4 GHz
  - 5 GHz
- **Enable iPRP**
  Enable or disable iPRP for the required port.
- **PRP Network**
  Specify the PRP network in which the port is a member.
  Note that both VAP interfaces of a radio interface cannot be used for the same iPRP network.

Procedure

1. For "PRP A", select the VLAN assignment for PRP A.
2. For "PRP B", select the VLAN assignment for PRP B.
3. Specify the PRP network in which the port is a member.
4. Select the "Enable iPRP" setting. Click the "Set Values" button.
   The appropriate VLAN settings are made automatically.

Upkeep and maintenance

7

7.1 Firmware update - via WBM

Requirement

- The device has an IP address.
- The user is logged in with administrator rights.

Firmware update via HTTP

1. Click "System > Load&Save" in the navigation area. Click the "HTTP" tab.
2. Click the "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 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.

Firmware update via SFTP

1. Click "System > Load&Save" in the navigation area. Click the "SFTP" tab.
2. Enter the IP address of the SFTP server in the "SFTP Server Address" input box.
3. Enter the port of the SFTP server in the "SFTP Server Port" input box.
4. If required, enter the user name and password.
5. Click the "Load file" button in the "Firmware" table row.
6. Go to the storage location of the firmware file.
7. Click the "Open" button in the dialog. The file is uploaded.

Result

The firmware has been transferred completely to the device.

On the "Information > Versions" there are the entries "Firmware" and "Firmware Running". Firmware Runningshows 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".

7.2 Embedding firmware in ConfigPack.

Please not the additional information and security notes in the operating instructions of your device.

With the the ConfigPack with embedded firmware file you can install a device configuration including the firmware belonging to it on one or more devices.

Creating ConfigPack with embedded firmware

To embed the firmware in a ConfigPack, you need to make a setting in the Command Line Interface (CLI). To do this, follow the steps outlined below:

Note

Using configurations with DHCP

If you want to use the ConfigPack with embedded firmware to commission multiple devices with the same configuration and firmware, create a ConfigPack only from device configurations that use DHCP. Otherwise, disruptions will occur in network operation due to multiple identical IP addresses.

You assign fixed IP addresses extra following the basic installation.

1. Start the remote configuration using Telnet (CLI) and log on with a user with the "admin" role.
2. Change to the global configuration mode with the command "configure terminal".
3. You change to the loadsave configuration mode with the "loadsave" command.
4. Enter the "firmware-in-configpack" command without parameters.
   The firmware currently on this device is now included as a separate file in the ConfigPack when you save it.

   Note

   Embedding firmware in ConfigPack.

   When the device is restarted this functionality is lost again and must be reactivated.

If you save a ConfigPack in the WBM or CLI, the firmware is embedded. The file can be supplied with a password before download. To load the file into the device successfully, use the specified password.

Refer to the information in the section Load & Save (Page 131).

Installing ConfigPack with embedded firmware

Note

Installing ConfigPack with DHCP options 66, 67

You can also install the ConfigPack using DHCP with options 66 and 67 activated.

You activate the options in the menu "System > DHCP > DHCP Client".

Password-protected ConfigPack and DHCP options 66.67

If the file is password-protected, you cannot install the file via DHCP with options 66 and 67.

If you install a ConfigPack using WBM or CLI, firmware stored there is also installed.

Procedure in the WBM

1. Connect to the WBM of the device on which you want to install the ConfigPack as administrator.
2. Go to the menu "System > Load&Save".
3. In the row "ConfigPack", click the "Load" button
4. Select the ConfigPack you want to install.
5. Restart the device with "System > Restart".
   If there is a different firmware version on the device to be installed compared with that in the ConfigPack, an upgrade/downgrade of the firmware is performed. You can recognize this by the red F-LED flashing (flashing interval; 2 sec on/0.2 sec off). Afterwards the device is restarted and the device configuration incl. users and certificates stored in the ConfigPack is transferred to the device.
6. Wait until the device has fully started up.
   (the red F-LED is off)
7. You can log on the device again or exit the WBM.

7.3 Device configuration with PRESET-PLUG

Please not the additional information and security notes in the operating instructions of your device.

NOTICE
Do not remove or insert a PLUG during operation
A PLUG may only be removed or inserted when the device is turned off.

Note

Support of PRESET-PLUG functionality

SCALANCE W700ax supports PRESET-PLUG functionality as of firmware version V1.0. SCALANCE W1700ac supports PRESET-PLUG functionality as of firmware version V1.1.

With the PRESET-PLUG, you can install the same device configuration (start configuration, user accounts, certificates) including the corresponding firmware on multiple devices.

The PRESET PLUG is write-protected.

You configure the PRESET PLUG using the Command Line Interface (CLI).

Creating a PRESET-PLUG

You create the PRESET PLUG using the Command Line Interface (CLI). You can create a PRESET-PLUG from any PLUG. To do this, follow the steps outlined below:

Note

Using configurations with DHCP

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

You assign fixed IP addresses extra following the basic installation.

Requirement

- A CLP on which you want to configure the PRESET-PLUG functionality is inserted in the device.

Procedure

1. Start the remote configuration using SSH (CLI) and log in as a user with the "admin" role.
2. Switch to the global configuration mode with the command "configure terminal".
3. You change to the PLUG configuration mode with the "plug" command.
4. Create the PRESET-PLUG with the "presetplug" command.
   The firmware version of the device and the current device configuration incl. user accounts and certificates are stored on the PLUG and the PLUG is then write protected.
5. Turn off the power to the device.
6. Remove the PRESET-PLUG.
7. Start the device either with a new CLP inserted or with the internal configuration.

Procedure for installation with the aid of the PRESET-PLUG

1. Turn off the power to the device.
2. If it is inserted, remove the CLP from the slot. You can find additional information on this in the operating instructions of your device.

3. Insert the PRESET-PLUG correctly oriented into the slot. The PRESET-PLUG is correctly inserted when it is completely inside the device and does not jut out of the slot.
4. Turn on the power to the device again.
   If there is a different firmware version on the device to be installed compared with that on the PRESET-PLUG, an upgrade/downgrade of the firmware is performed. You can recognize this by the red F-LED flashing (flashing interval: 2 sec on/0.2 sec off). Afterwards the device is restarted and the device configuration incl. users and certificates on the PRESET-PLUG is transferred to the device.
5. Wait until the device has fully started up.
   (the red F-LED is off)
6. Turn off the power to the device after the installation.
7. Remove the PRESET-PLUG.
8. Start the device either with a new CLP inserted or with the internal configuration.

Note

Restore factory defaults and restart with a PRESET PLUG inserted

If you reset the device to the factory defaults, when the device restarts an inserted PRESET PLUG is formatted and the PRESET PLUG functionality is lost. You then need to create a new PRESET PLUG. The keys stored on the KEY-PLUG for releasing functions are retained.

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

Formatting a PRESET-PLUG (resetting the preset function)

You format the PRESET PLUG using the Command Line Interface (CLI) to reset the preset function. To do this, follow the steps outlined below:

1. Start the remote configuration using SSH (CLI) and log in with a user with the "admin" role.
2. Switch to the global configuration mode with the command "configure terminal".
3. You change to the PLUG configuration mode with the "plug" command.
4. Enter the command "factoryclean".
   The PRESET-PLUG is formatted and the preset function is reset.
5. Write the current configuration of the device with the "write" command.

7.4 Restoring the factory settings

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

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

With the reset button

When pressing the button, make sure you observe the information in the "Reset button" section in the operating instructions.

Follow the steps below to reset the device parameters to the factory settings:

1. Turn off the power to the device.
2. Loosen the screws of the cover.
3. Remove the cover.
4. Now press the Reset button and reconnect the power to the device while holding down the button.
5. Hold down the button until the red fault LED (F) stops flashing after approximately 10 seconds and is permanently lit.
6. Now release the button and wait until the fault LED (F) goes off again.
7. The device then starts automatically with the factory settings.

With SINEC PNI

Follow the steps below to reset the device parameters to the factory settings with the SINEC PNI:

1. Select the device whose parameters you want to reset.
2. Click the "Reset device" button.
3. Select the "Reset to factory settings" option in the following dialog.

Via the configuration

You will find detailed information on resetting the device parameters using the WBM and CLI in the configuration manuals:

- Web Based Management, section "Restart (Page 126)"
- Command Line Interface, section "Reset and Defaults"

Troubleshooting/FAQ

8

8.1 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.

When pressing the button, be sure to read the information in the "Reset button" section of the operating instructions.

Solution

You can then also assign firmware to a SCALANCE W 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 W over the Ethernet interface.
6. Assign an IP address to the SCALANCE W with the SINEC PNI.
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.
8. Close the cover to ensure that the device is closed and water and dust proof.

Note

Use of CLI and TFTP in Windows 10

If you want to access the CLI or TFTP in Windows 10, make sure that the relevant functions are enabled in Windows 10.

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.

8.2 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 SCALANCE W device is too high, this overdrives the amplifier circuit. Overdrive can occur on clients and access points. If the received power on the SCALANCE W device is greater than -35 dBm, this can result in disrupted communication. Information about the signal strength [in dBm] is displayed in WBM in the following tabs:

Access point mode:

- Information > WLAN > Client List

Client mode:

- Information > WLAN > Available AP

The power of the input signal on the SCALANCE W device is influenced by the following factors:

- Distance between the WLAN partners
- Reflections of the electromagnetic waves by parts of the building
- Setting of the "max. Tx Power" and the antenna settings used (Interfaces > WLAN > Antennas & Power)

Solution

If communication is disrupted by an excessive signal strength (greater than -35 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.

8.3 Instructions for secure network design

Note the information below to protect your network against 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 131)".
- **Use WPA2/ WPA2-PSK / WPA3-SAE with AES**
  Use only WPA2/ WPA2-PSK / WPA3-SAE with AES to prevent password misuse. These authentication methods in combination with AES encryption offer the greatest security. For more detailed information, refer to the section "WLAN (Page 290)".
- **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 devices by arranging so that the Agent IP is only accessible via a single management VLAN. For more detailed information, refer to the section "Menu "Layer 3 (IPv4)" (Page 259)".
  - 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 via HTTP. For more detailed information, refer to the section "Load & Save (Page 131)".
- **Use SNMPv3**
  SNMPv3 provides you with highest possible security when accessing the devices via SNMP. For more detailed information, refer to the section "SNMP (Page 158)".

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 "Supported MIB Modules"

A

A.1 Supported MIB files

MIB files available for the SCALANCE W device

The following table shows the MIB files available for a SCALANCE W device:

MIB	Root OID	Reference
AUTOMATION-SYSTEM-MIB (Siemens) [1]	.1.3.6.1.4.1.4329.6.3.2	Vendor specific
AUTOMATION-SN-SYSTEM-MIB (Siemens) [1] [2]	.1.3.6.1.4.1.4329.6.1.2.100.2	Vendor specific
AUTOMATION-SN-AUTH-MIB (Siemens) [1] [2]	.1.3.6.1.4.1.4329.6.1.2.100.3	Vendor specific
AUTOMATION-SNTP (Siemens) [1] [2]	.1.3.6.1.4.1.4329.6.3.11	Vendor specific
AUTOMATION-SMTP (Siemens) [1] [2]	.1.3.6.1.4.1.4329.6.3.9	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
AUTOMATION-PS-MIB (Siemens) [1] [2]	.1.3.6.1.4.1.4329.6.3.5	Vendor specific
IF-MIB	.1.3.6.1.2.1.2	RFC 2863
EtherLike-MIB	.1.3.6.1.2.1.10.7.2	RFC 3635
MAU-MIB	.1.3.6.1.2.1.26	RFC 4836
ENTITY-MIB	.1.3.6.1.2.1.47	RFC 4133
Q-BRIDGE-MIB	.1.3.6.1.2.1.17.7	RFC 2674q
P-BRIDGE-MIB	.1.3.6.1.2.1.17.6	RFC 2674p
BRIDGE-MIB	.1.3.6.1.2.1.17	RFC 4188
IPV6-MIB	.1.3.6.1.2.1.55	RFC 2465
SNMPv2-MIB	.1.3.6.1.2.1.1	RFC 3418
SNMP-COMMUNITY-MIB	.1.3.6.1.6.3.18	RFC 3584
SNMP-USER-BASED-SM-MIB	.1.3.6.1.6.3.15	RFC 3414
SNMP-VIEW-BASED-ACM-MIB	.1.3.6.1.6.3.16	RFC 3415
SNMP-NOTIFICATION-MIB	.1.3.6.1.6.3.13	RFC 3413
SNMP-TARGET-MIB	.1.3.6.1.6.3.12	RFC 3413
SNMP-MPD-MIB	.1.3.6.1.6.3.10.2.1	RFC 3412
RADIUS-ACC-CLIENT-MIB	.1.3.6.1.2.1.67.2.2	RFC 2620
RADIUS-AUTH-CLIENT-MIB	.1.3.6.1.2.1.67.1.2	RFC 2618
RMON-MIB	.1.3.6.1.2.1.16	RFC 2819
IP-MIB	.1.3.6.1.2.1.4	RFC 4292
TCP-MIB	.1.3.6.1.2.1.6	RFC 4022
UDP-MIB	.1.3.6.1.2.1.7	RFC 4113
DNS-RESOLVER-MIB	.1.3.6.1.2.1.32.2	RFC 1612
IEEE802dot11-MIB	.1.2.840.10036	IEEE 802.11
IEEE 802.1AB 2005 LLDP-MIB (Siemens) [1] [2]	.1.0.8802.1.1.2	Vendor specific

MIB	Root OID	Reference
LLDP-EXT-DOT1-MIB (Siemens) [1) 2)]	.1.0.8802.1.1.2.1.5.32962	Vendor specific
LLDP-EXT-DOT3-MIB (Siemens) [1) 2)]	.1.0.8802.1.1.2.1.5.4623	Vendor specific
LLDP-EXT-PNO-MIB (Siemens) [1) 2)]	.1.0.8802.1.1.2.1.5.3791	Vendor specific
SN-MSPS-SNMP-MIB (Siemens) [2)]	.1.3.6.1.4.1.4329.20.1.1.1	Vendor specific
SN-MSPS-SCW-MIB (Siemens) [1) 2)]	.1.3.6.1.4.1.4329.20.1.1.1.1.27.1.10.19.3	Vendor specific
SN-MSPS-SCW-MIB (Siemens) [1) 2)]	.1.3.6.1.4.1.4329.20.1.1.1.1.1.100.10	Vendor specific

1) Part of the AUTOMATION.MIB

   You can download the AUTOMATION.MIB for SCALANCE W from Siemens Industry Automation and Drives Service & Support under the entry ID 67637278 (https://support.industry.siemens.com/cs/ww/en/view/67637278)

2) Part of the private MIB file "Scalance_w_msps.mib". You can download the file in the WBM with the "Save" button under "System > Load & Save > HTTP > MIB".

Appendix B "Private MIBs"

B

B.1 Private MIB variables

Downloading the MIB of the SCALANCE W via WBM

You can download the MIB of the SCALANCE W in WBM under "System > Load&Save > HTTP > MIB" using the "Save" button.

OID

The private MIB variables of the SCALANCE W have the following object identifier:
`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 "Underlying Standards"

C

C.1 Underlying standards

Standards met by SCALANCE W devices completely or partly

The following table lists some of the standards for SCALANCE W 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 802.11b/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
IEEE 802.11ax	Wi-Fi6
IEEE 802.11ac	Standard for very high transmission rates in the 5 GHz frequency band

Appendix D "Log Messages"

D

D.1 Messages in the event log

Messages during system startup (general)

Message	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 • PoE is connected • PoE 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
Spanning Tree disabled. Spanning Tree enabled.	Information on the status of the Spanning Tree protocol
No Fault states pending after startup.	Fault state following system start
Scheduled restart cancelled.	The scheduled restart was aborted.
Scheduled restart in xx seconds.	The device restarts in xx seconds.

Status of the power supply

You enable or disable the "Power Change" event in "System > Events".

Message	Description
Power up on line 1 / 2 / PoE.	Power supply available 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

You enable or disable the "Link Change" event in "System > Events".

Message	Description
Link up on P1.	There is a connection on the Ethernet interface.
Link down on P1.	There is no connection on the Ethernet interface.
Link up on P1: <Speed>	The speed that is currently present is >= 100 Mbps and full duplex (FD)
New Fault state: "Result of autonegotiation on P1: <Speed> Result of autonegotiation on P1: <Speed> Link up on P1: <Speed>	The speed is < 100 Mbps or half duplex (HD)

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.
Overlap-AP found on WLAN X: AP <System Name> <MAC Address> 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 Address> 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 WLANX at channel <channel number> (frequency <frequency> MHz) DFS: start DFS scan on WLANX at channel <channel number> (frequency <frequency> MHz) DFS: finished DFS scan on WLANX at channel <channel number> (frequency <frequency> MHz)	If the access point discovers a radar signal on the current channel, it notifies the clients of the channel change. It then automatically switches to an alternative DFS channel and the current channel is blocked for 30 minutes.
DFS: channel <channel number> (frequency <frequency> MHz) aged out from NOL at WLANX and can be used again	No radar signal 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 WLANX at channel <channel number> (frequency <frequency> MHz) DFS: No Channels are available al WLANX.	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/SSH/Telnet: User {user name} failed to log in from {ip address}.	An incorrect password was entered during login. 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).
Device configuration changed.	The configuration was changed.
WBM/SSH/Telnet: User {user name} is locked for %d minutes after %d unsuccessful login attempts.	The user / IP address was locked for the duration (in minutes) after the failed login.
WBM/SSH/Telnet: The session of user {user name} was closed after %d seconds of inactivity.	The session was ended.

Messages on log files

Message	Description
Log file cleared.	The log entries are deleted.

Status about DNS server entries

Message	Description
Update DNS: empty nameservers list.	No DNS server has been created.

Messages about TCP events

Messages	Description
Messages about sleep mode:	
Device changed to Sleep Mode for %d minutes.	Sleep mode was triggered on the device for the duration (in minutes).
DI/DO messages:	
TCP Event {ip address} Result: 1 aborted - wrong TCP packet format	The format of the TCP packet does not match.
TCP Event {ip address} Result: 1 aborted - wrong username or password	Wrong user name or password specified
TCP Event {ip address} Result: 1 aborted - internal storage failed	Save failed due to an internal error
TCP Event {ip address} Result: 1 aborted - incorrect action	Invalid action
TCP Event {ip address} Result: 1 aborted - wrong command code	Invalid command
TCP Event {ip address} Result: 1 aborted - incorrect Digital Out action	Invalid action for digital output
TCP Event {ip address} Result: 1 aborted - invalid Sleep Mode duration	Invalid sleep mode duration
TCP Event {ip address} Result: 1 aborted - invalid Sleep Mode action	Invalid action for sleep mode
TCP Event {ip address} Result: 1 incoming - Digital Out activated	The digital output has been activated.
TCP Event {ip address} Result: 1 incoming - Digital Out deactivated	The digital output has been deactivated.
TCP Event {ip address} Result: 1 incoming - Sleep Mode activated	The sleep mode has been activated.
TCP Event {ip address} Result: 1 aborted	The action failed.
Messages on WLAN roaming:	
WLAN roaming triggered by TCP Event	A connection transition to another access point was initiated.
WLAN roaming by TCP Event: Client is already connected to BSSID: <BSSID>	The client has already logged in on the access point.

Messages for file upload/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.
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

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".

Messages	Description
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" "PLUG not accepted. See System PLUG mask for details."	Outgoing fault

Messages	Description
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 for backup restore

Messages	Description
Backup Restore: Loaded file type <File type> (restart required).	The file was successfully loaded after restoring the configuration backup to the device. A restart is required. Possible file types: • Config • ConfigPack • WBMFav • Users
Backup Restore: Loaded file type <File type> which is identical.	The file was successfully loaded after restoring the configuration backup to the device. The file is identical to the existing file.

Spanning Tree messages

Enable or disable the "Spanning Tree" event under "System > Events"

Messages	Description
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 Adress>.	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 accessible, configuration incomplete or faulty (e.g. receiver e-mail address wrong / not available).
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. Functions are configured on the device for which a PLUG License (CLP) is required.
Startup configuration: Internal storage PLUG: Configuration not accepted PLUG: License missing	Invalid or incompatible configuration on the inserted PLUG. Functions are configured on the device for which a PLUG License (CLP) is required.
Startup configuration: Internal storage PLUG: Configuration accepted PLUG: License wrong	The PLUG license (CLP) is wrong.
Startup configuration: Internal storage PLUG: Configuration not accepted PLUG: License accepted	Invalid or incompatible configuration on the inserted PLUG.
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 PLUG License (CLP).
Startup configuration: Internal storage PLUG: Factory clean → filled with internal configuration PLUG: Configuration accepted	The internal configuration was written successfully to an empty PLUG Configuration (CLP).

Alarm	Description
Startup configuration: PLUG storage PLUG: Configuration accepted PLUG: License accepted	The configuration was loaded successfully from the PLUG License (CLP).
Startup configuration: PLUG storage PLUG: Configuration accepted	The configuration was loaded successfully from the PLUG Configuration (CLP).

Messages about PLUG

Messages	Description
Factory default PLUG found.	There is an empty or formatted PLUG in the device.
PLUG: Filled PLUG was found. PLUG: Configuration Accepted	The PLUG in the device has been emptied. The current device configuration was written to the PLUG.
PLUG: Removed at runtime.	The PLUG License (CLP) or the PLUG Configuration (CLP) was removed during operation.
PLUG accepted.	PLUG was accepted.
PLUG: Different device type found.	Different device type

D.2 Messages in the WLAN Authentication Log

Messages in access point mode

Message	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.
VAP<Num>: Client <MAC address> failed to associated; status (<text>).	The connection of the client to the VAP has failed. The reason is displayed as text.
VAP<Num>: Client <MAC address> disassociated with reason (<text>).	The client was successfully disconnected from the VAP. The reason is displayed as text.
VAP<Num>: Client <MAC address> deauthenticated with reason (<text>).	The client was logged off from the AP. The reason is displayed as text.
VAP<Nummer> Client <MAC address> failed to authenticate; status (<text>).	The authentication of the client failed. The reason is displayed as text.
VAP<Num>: Client <MAC address> failed to disassociated; status (<text>).	The connection of the client could not be terminated. The reason is displayed as text.
VAP<Num>: Client <MAC address> associated successfully.	The client has connected successfully to the VAP or the client has logged on successfully to the VAP.
VAP<Num>: Client <MAC address> associated successfully using FT Over-the-air.	The client has connected successfully to the VAP or the client has logged on successfully to the VAP. Fast BSS Transition "Over-the-air" was used for the connection transition.
RADIUS: Access rejected for client <MAC address>.	The RADIUS server denies the client access.
RADIUS: Access accepted for client <MAC address>.	The RADIUS server allows the client access.

Messages in client mode

Message	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. If the client is not connected to any access point and then logs on to an access point for the first time, a WLAN Authentication Log is output. Example: Associated successfully to AP d4:f5:27:b2:46:60 at channel 40 (frequency 5200 MHz).
Associated successfully to AP <MAC address> <System Name> at channel <Channel number> (frequency <frequency> MHz) roaming time <time> ms.	The client has logged in successfully on the access point. The roaming time is specified on switching of access points.
Associated successfully to AP <MAC address> <System Name> using FT Over-the-air at channel <Channel number> (frequency <frequency> MHz) roaming time <time> ms.	The client has logged in successfully on the access point. Fast BSS Transition "Over-the-air" was used for the connection transition. The roaming time is specified.
Associated successfully to AP <BSSID> using FT Over-the-air at channel <Channel number> (frequency <frequency> MHz) roaming time <time> ms.	The client has logged in successfully on the access point. Fast BSS Transition "Over-the-air" was used for the connection transition. The roaming time is specified.
Disassociated from AP <MAC address> <System Name> with reason (Disassociated because sending STA is leaving (or has left) BSS).	The client was logged off from the access point.
Deauthenticated from AP <MAC address> with reason (<text>).	The client was logged off from the access point. The reason is displayed as text.
Failed to authenticate to AP <MAC address>; status (<text>).	The authentication of the client with the access point failed. The reason is displayed as text.
Failed to disassociate from AP <MAC address>; status (<text>).	The connection of the client to the access point could not be terminated. The reason is displayed as text.
Failed to associate to AP <MAC address>; status (<text>).	The connection of the client to the access point has failed. The reason is displayed as text.

Expansion of messages on the roaming operation in the access point and client mode

Expansion	Description
roaming time <time> ms	Additional information in the messages "Associated successfully" and "Reassociated successfully": Specifies the WLAN roaming time that is measured from the logical start of the login procedure in the client until receipt of the first positive response for connection.
roaming time including authorization <time> ms	Additional information in the messages "Authorized successfully": Specifies the WLAN roaming time that is measured from the logical start of the login procedure in the client until the end of key exchange.

Messages on log files

Message	Description
Log file cleared.	The log entries are deleted.

Appendix E "Syslog Messages"

E

E.1 Format of the syslog messages

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

HEADER

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

PRIORITY

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

- Facility
- Severity

VERSION

- Set to 1.

HOSTNAME_CONTENT:

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

STRUCTURED DATA

- timeQuality block

MESSAGE:

- ASCII string in English

Note

Additional information about the meaning of the boxes is available in RFC 5424 (https://datatracker.ietf.org/doc/html/rfc5424).

E.2 Parameters in Syslog messages

The Syslog messages can contain the following parameters:

Parameter	Description	Possible values or example
ip address	IPv4 or IPv6 address	IP address according to RFC1035 or RFC4291 Section 2.2
src port dest port	Port that is shown as decimal number. Format: %d	0 ... 65535
client mac dest mac src mac	MAC address Format: %02x:%02x:%02x;%02x:%02x:%02x	00:0C:29:2F:09:B3
protocol	Name of the service that has generated this event or of the Layer 4 protocol used. Format: %s	Possible entries of: UDP | TCP | WBM | Telnet | SSH | Console | TFTP | SFTP
group	String that identifies the group based on its name Format: %s	it-service
user name	String that identifies the authenticated user based on his/her name without spaces Format: %s	maier
action user name	Identifies the user based on his/her name This is not the authenticated user. Format: %s	Peter.Maier
role	Symbolic name for the group role Format: %s	Administrator
time minute timeout	Number of minutes Format: %d	44
time second	Number of seconds Format: %d	44
failed login count	Number of failed logins Format: %d	10
max sessions	Number of sessions Format: %d	10
vap	Symbolic name of the virtual access point interface Format: (%s) or (%s %s)	VAP1.1
status reason	Additional status information as legible string. It can contain multiple words. The string must start with " and end with " so that it can be analyzed.	(Invalid group cipher) (Unknown peer)
wlan interface	Symbolic name of the WLAN interface Format: %s	WLAN1
ssid	SSID in ASCII representation any number of spaces Format: %s	MyWLAN
channel	Name of the channel Format: %s	12

Parameter	Description	Possible values or example
signal strength	Signal strength Format: %d	12
version	Name of the version without spaces Format: %s	V1.0.3SP1
length	Length of the network packet (in bytes) Format: %d	52
network interface	Symbolic name of a network interface Format: %s	vlan 1

E.3 Syslog messages

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

Identification and authentication of human users

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

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

Log text	{protocol}: User {user name} logged out from {ip address}.
Standard	IEC 62443-3-3 Reference: SR1.1
Description	User session completed - logged out.
Example	SSH: User admin logged out from 192.168.0.1.
Severity	Info
Facility	local0

Log text	{protocol}: User {user name} failed to log in from {ip address}.
Standard	IEC 62443-3-3 Reference: SR1.1

Description	Incorrect user name or incorrect password (login information) specified during remote login.
Example	SSH: User testuser failed to log in from 192.168.0.1.
Severity	Warning
Facility	local0

User account management

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

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

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

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

Management of the identifiers

Log text	{protocol}: User {user name} created group {group} and assigned to role {role}.
Standard	IEC 62443-3-3 Reference: SR1.4
Description	The administrator has created a group and assigned it to a role.
Example	WBM: User admin created group it-service and assigned to role service.

Severity	Info
Facility	local0

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

Failed login attempts

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

Usage control of wireless connections (connection over WLAN)

Log text	{vap}: Client {client mac} associated successfully.
Standard	IEC 62443-3-3 Reference: SR 2.2
Description	WLAN client connected to AP.
Example	VAP1.1: Client 18:65:90:ab:78:f4 associated successfully.
Severity	Info
Facility	local0

Log text	Overlap-AP found on {wlan interface}: AP {ssid} {ap mac} found on channel {channel} rssi {signal strength}.
Standard	IEC 62443-3-3 Reference: SR 2.2
Description	Radio frequency is already in use.
Example	Overlap-AP found on WLAN 1: AP scalance 20:a8:b9:80:44:80 found on channel 11 rssi 12.
Severity	Info
Facility	local0

Log text	{vap}: Client {client mac} disassociated with reason {reason}.
Standard	IEC 62443-3-3 Reference: SR 2.2
Description	WLAN client disconnected from AP.

Example	VAP1.1: Client 18:65:90:ab:78:f4 disassociated with reason (Disassociated because sending STA is leaving or has left BSS).
Severity	Info
Facility	local0

Log text	{vap}: Client {client mac} failed to associate, status {status}.
Standard	IEC 62443-3-3 Reference: SR 2.2
Description	WLAN client connection to AP denied.
Example	VAP1.1: Client 18:65:90:ab:78:f4 failed to associate, status (Invalid group cipher).
Severity	Warning
Facility	local0

Log text	{vap}: Client {client mac} failed to authenticate, status {status}.
Standard	IEC 62443-3-3 Reference: SR 2.2
Description	The WLAN client was not able to authenticate itself.
Example	VAP1.1: Client 18:65:90:ab:78:f4 failed to authenticate, status (Invalid group cipher).
Severity	Warning
Facility	local0

Log text	RADIUS: {ip address} - No response from the RADIUS server.
Standard	IEC 62443-3-3 Reference: SR 2.2
Description	RADIUS server not found.
Example	RADIUS: 192.168.0.10 - No response from the RADIUS server.
Severity	Warning
Facility	local0

Session lock

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

Limiting the number of simultaneous sessions

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

Example	WBM: The maximum number of 8 concurrent login session exceeded.
Severity	Warning
Facility	local0

Non-deniability (change configuration)

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

Data backup in automation system (backup)

Log text	{protocol}: User {user name} saved file type ConfigPack
Standard	IEC 62443-3-3 Reference: SR7.3
Description	Backup completed
Example	WBM: User admin saved file type ConfigPack..
Severity	Info
Facility	local0

Log text	{protocol}: Saved file type ConfigPack.
Standard	IEC 62443-3-3 Reference: SR7.3
Description	Backup completed
Example	TFTP: Saved file type ConfigPack
Severity	Info
Facility	local0

Log text	{protocol}: User {user name} failed to save file type ConfigPack.
Standard	IEC 62443-3-3 Reference: SR7.3
Description	Backup failed
Example	WBM: User admin failed to save file type ConfigPack.
Severity	Warning
Facility	local0

Log text	{protocol}: Failed to save file type ConfigPack.
Standard	IEC 62443-3-3 Reference: SR7.3
Description	Backup failed
Example	TFTP: Failed to save file type ConfigPack.

Severity	Warning
Facility	local0

Restoration of the automation system

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

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

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

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

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

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

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

Appendix F "Encryption methods used (ciphers)"

F

The following tables list the encryption methods (ciphers) used by the SCALANCE W device.

F.1 WLAN security mechanisms

The following table shows the encryption methods and authentication that the SCALANCE W devices support.

Encryption method	
None	✓
WPA-TKIP	✓
WPA-AES	✓

Authentication	
Password / PSK	✓
Password / SAE	✓
IEEE 802.1X EAP PEAP	✓
IEEE 802.1X EAP TLS	✓
IEEE 802.1X EAP TTLS	✓
IEEE 802.1X EAP others	-
EAP protocol: MS-CHAPv2	✓
EAP protocol: TLS	✓
EAP protocol: GTC	✓

F.2 RADIUS

The following table shows cipher suites and signature algorithms that SCALANCE W devices support for RADIUS authentication.

Default setting TLS 1.2

Table F-1 WPA/WPA2 RADIUS authentication

Cipher suite	Signature algorithm
TLS 1.0/1.1	
AES256-GCM-SHA384	ECDSA with SHA256
AES128-GCM-SHA256	ECDSA with SHA384
AES256-SHA256	ECDSA with SHA512
AES128-SHA256	ECDSA with SHA224
ECDHE-ECDSA-AES256-SHA	ECDSA with SHA1

Cipher suite	Signature algorithm
ECDHE-RSA-AES256-SHA	SHA224 with RSA
DHE-RSA-AES256-SHA	SHA1 with RSA
ECDHE-ECDSA-AES128-SHA	DSA with SHA224
ECDHE-RSA-AES128-SHA	DSA with SHA1
DHE-RSA-AES128-SHA	EdDSA ed25519
AES256-SHA	EdDSA ed448
AES128-SHA	RSASSA-PSS with SHA256
ECDHE-ECDSA-AES256-GCM-SHA384	RSASSA-PSS with SHA384
ECDHE-RSA-AES256-GCM-SHA384	RSASSA-PSS with SHA512
DHE-RSA-AES256-GCM-SHA384	RSASSA-PSS (rsaEncryption) with SHA256
ECDHE-ECDSA-CHACHA20-POLY1305-SHA256	RSASSA-PSS (rsaEncryption) with SHA384
ECDHE-RSA-CHACHA20-POLY1305-SHA256	RSASSA-PSS (rsaEncryption) with SHA512
DHE-RSA-CHACHA20-POLY1305-SHA256	SHA256 with RSA
ECDHE-ECDSA-AES128-GCM-SHA256	SHA384 with RSA
ECDHE-RSA-AES128-GCM-SHA256	SHA512 with RSA
DHE-RSA-AES128-GCM-SHA256	DSA with SHA256
ECDHE-ECDSA-AES256-SHA384	DSA with SHA384
ECDHE-RSA-AES256-SHA384	DSA with SHA512
DHE-RSA-AES256-SHA256	
ECDHE-ECDSA-AES128-SHA256	
ECDHE-RSA-AES128-SHA256	
DHE-RSA-AES128-SHA256	
TLS 1.2	
ECDHE-ECDSA-AES256-GCM-SHA384	EdDSA ed25519
ECDHE-RSA-AES256-GCM-SHA384	EdDSA ed448
DHE-RSA-AES256-GCM-SHA384	RSASSA-PSS with SHA256
ECDHE-ECDSA-CHACHA20-POLY1305-SHA256	RSASSA-PSS with SHA384
ECDHE-RSA-CHACHA20-POLY1305-SHA256	RSASSA-PSS with SHA512
DHE-RSA-CHACHA20-POLY1305-SHA256	RSASSA-PSS (rsaEncryption) with SHA256
ECDHE-ECDSA-AES128-GCM-SHA256	RSASSA-PSS (rsaEncryption) with SHA384
ECDHE-RSA-AES128-GCM-SHA256	RSASSA-PSS (rsaEncryption) with SHA512
DHE-RSA-AES128-GCM-SHA256	SHA256 with RSA
ECDHE-ECDSA-AES256-SHA384	SHA384 with RSA
ECDHE-RSA-AES256-SHA384	SHA512 with RSA
DHE-RSA-AES256-SHA256	DSA with SHA256
ECDHE-ECDSA-AES128-SHA256	DSA with SHA384
ECDHE-RSA-AES128-SHA256	DSA with SHA512
DHE-RSA-AES128-SHA256	ECDSA with SHA256
	ECDSA with SHA384
	ECDSA with SHA512

F.3 SSL

HTTPS WBM Server

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_AES_128_GCM_SHA256	1301	✓
Encryption suite	TLS_CHACHA20_POLY1305_SHA256	1303	✓
Encryption suite	TLS_AES_256_GCM_SHA384	1302	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	c02f	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	c030	✓
Protocol version	TLSv1.2	-	✓
Protocol version	TLSv1.3	-	✓

SMTP Client (secure)

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_AES_128_GCM_SHA256	1301	✓
Encryption suite	TLS_CHACHA20_POLY1305_SHA256	1303	✓
Encryption suite	TLS_AES_256_GCM_SHA384	1302	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	c02c	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	c02b	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	c02f	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	c030	✓
Protocol version	TLSv1.2	-	✓
Protocol version	TLSv1.3	-	✓

Syslog Client TLS

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_AES_128_GCM_SHA256	1301	✓
Encryption suite	TLS_CHACHA20_POLY1305_SHA256	1303	✓
Encryption suite	TLS_AES_256_GCM_SHA384	1302	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	c02c	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	c02b	✓

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	c02f	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	c030	✓
Protocol version	TLSv1.2	-	✓
Protocol version	TLSv1.3	-	✓

RADIUS Client

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	c02c	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	c030	✓
Encryption suite	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	009f	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	cca9	✓
Encryption suite	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	cca8	✓
Encryption suite	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ccaa	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	c02b	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	c02f	✓
Encryption suite	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	009e	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	c024	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	c028	✓
Encryption suite	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	006b	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	c023	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	c027	✓
Encryption suite	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	0067	✓
Protocol version	TLSv1.2	-	✓

F.4 SSH CLI

SSH CLI Client

Category	Process	Hexadecimal value	Enabled by default
Encryption method (enc)	aes256-ctr	-	✓
Host key	ecdsa-sha2-nistp521	-	✓
Key exchange (kex)	curve25519-sha256	-	✓
Key exchange (kex)	curve25519-sha256@libssh.org	-	✓
Key exchange (kex)	ecdh-sha2-nistp256	-	✓
Key exchange (kex)	ecdh-sha2-nistp384	-	✓
Key exchange (kex)	ecdh-sha2-nistp521	-	✓
MAC	hmac-sha2-256	-	✓
Protocol version	SSHv2.0	-	✓

SSH Server

Category	Process	Hexadecimal value	Enabled by default
Encryption method (enc)	aes256-ctr	-	✓
Host key	ecdsa-sha2-nistp521	-	✓
Key exchange (kex)	curve25519-sha256	-	✓
Key exchange (kex)	curve25519-sha256@libssh.org	-	✓
Key exchange (kex)	ecdh-sha2-nistp256	-	✓
Key exchange (kex)	ecdh-sha2-nistp384	-	✓
Key exchange (kex)	ecdh-sha2-nistp521	-	✓
MAC	hmac-sha2-256	-	✓
Protocol version	SSHv2.0	-	✓

SFTP Client

Category	Process	Hexadecimal value	Enabled by default
Encryption method (enc)	aes256-ctr	-	✓
Host key	ecdsa-sha2-nistp521	-	✓
Host key	ecdsa-sha2-nistp256	-	✓
Key exchange (kex)	curve25519-sha256	-	✓
Key exchange (kex)	curve25519-sha256@libssh.org	-	✓
Key exchange (kex)	ecdh-sha2-nistp256	-	✓
Key exchange (kex)	ecdh-sha2-nistp384	-	✓

Category	Process	Hexadecimal value	Enabled by default
Key exchange (kex)	ecdh-sha2-nistp521	-	✓
MAC	hmac-sha2-256	-	✓
Protocol version	SSHv2.0	-	✓

Appendix G "Permitted characters in names, passwords and descriptions"

G

G.1 Permitted characters

Passwords

Observe the following rules when creating or changing the passwords:

Allowed characters of a character set according to ANSI X 3.4-1986	0123456789 A...Z a...z .-_#+'*~^!$%&/{([])}=\ `<>@, Space
Characters not allowed	:;"|€´?§³²°µ ä ö ü Ä Ö Ü
Length of the password	At least 8 characters and maximum 128 characters

Note

Passwords

To improve security, make sure that passwords are as long as possible.

Passwords must be at least 8 characters long and contain special characters, upper and lowercase characters as well as numbers.

User names

Observe the following rules when creating or changing the user names:

Allowed characters of a character set according to ANSI X 3.4-1986	0123456789 A...Z a...z .-_#+'*~^!$%&/{([])}=\ `<>@,
Characters not allowed	:;"|€´?§³²°µ ä ö ü Ä Ö Ü Space
Length of the user name	1 to 30 characters

Note

User names

To improve security, make sure that user names are as long as possible.

Role names

Observe the following rules when creating or changing the role names:

Allowed characters of a character set	0123456789 A...Z a...z .-_#+'*~^!$%&/{([])}=\ `<>@,: Space
Characters not allowed	;"|€´?§[320]µ ä ö ü Ä Ö Ü
Length of the role name	1 ... 64 characters

Group names

Observe the following rules when creating or changing the group names:

Allowed characters of a character set	0123456789 A...Z a...z .-_#+'*~^!$%&/{([])}=\ `<>@: Space
Characters not allowed	;",|€´?§[320]µ ä ö ü Ä Ö Ü
Length of the group name	1 ... 64 characters

User, role and group descriptions

Observe the following rules when creating or modifying descriptions:

Allowed characters of a character set		0123456789 A...Z a...z .-_#+'*~^!$%&/{([])}=\ `<>@, Space :;"| CLI only
Characters not allowed	WBM	:;"|€´?§[320]µ ä ö ü Ä Ö Ü
	CLI	€´?§[320]µ ä ö ü Ä Ö Ü
Length of description		1 ... 100 characters

Index

J

L

M

N

O

P

R

S

T

U

V

W