

SIMATIC NET

Industrial Wireless LAN SCALANCE W760 / W720 according to IEEE 802.11n Web Based Management V6.5 Configuration Manual

Introduction	1
Security recommendations	2
Description	3
Technical basics	4
IP addresses	5
Configuring with Web Based Management	6
Upkeep and maintenance	7
Troubleshooting/FAQ	8
Appendix A "Supported MIB Modules"	A
Appendix B "Private MIBs"	B
Appendix C "Underlying Standards"	C
Appendix D "Log Messages"	D
Appendix "Syslog Messages"	E
Appendix F (Supported Security Mechanisms)	F
Appendix G "Permitted characters in names, passwords and descriptions"	G

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 Aktiengesellschaft. 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.

Table of contents

1	Introduction	9
1.1	Purpose of the configuration manual	9
1.2	Scope of the manual	9
1.3	Information on the Configuration Manual	9
1.4	Terms used	11
1.5	Structure of the type designation	12
1.6	Cybersecurity information	12
1.7	Firmware	12
1.8	Open source license conditions	13
1.9	Error/fault	13
1.10	Decommissioning	13
1.11	Recycling and disposal	14
1.12	Marken	14
2	Security recommendations.....	15
2.1	Security recommendations.....	15
2.2	Available services.....	19
3	Description.....	23
3.1	Network structures	23
3.2	Possible applications of SCALANCE W700 devices	27
3.3	Product characteristics	28
3.4	Planned operating environment	30
3.5	IEEE 802.11n	30
3.6	Requirements for installation and operation	33
3.7	ConfigPack.....	33
4	Technical basics	35
4.1	Configuration limits for WBM and CLI.....	35
4.2	Interfaces and system functions	36
4.3	EtherNet/IP	39
4.4	PROFINET.....	40
4.5	VLAN	40
4.6	MAC-based communication	41

4.7	iPCF / iPCF-HT / iPCF-MC	42
4.8	iPRP	45
4.9	NAT/NAPT	48
4.10	SNMP	49
4.11	Spanning Tree	51
4.11.1	RSTP, MSTP, CIST	52
4.12	User management	53
5	IP addresses	55
5.1	IPv4 / IPv6	55
5.2	IPv4 address.....	57
5.2.1	Structure of an IPv4 address	57
5.2.2	Initial assignment of an IPv4 address	58
5.2.3	Address assignment via DHCPv4	59
5.2.4	Address assignment with SINEC PNI.....	60
5.2.5	Address assignment with STEP 7	61
5.3	IPv6 address.....	61
5.3.1	IPv6 terms	61
5.3.2	Structure of an IPv6 address	62
6	Configuring with Web Based Management.....	65
6.1	Web Based Management.....	65
6.2	Login	67
6.3	"Wizard" menu	70
6.3.1	Basic Wizard.....	70
6.3.1.1	System Settings	71
6.3.1.2	Country Settings	73
6.3.1.3	IP Address Settings.....	74
6.3.1.4	Management Interfaces	76
6.3.1.5	Antenna Settings	78
6.3.1.6	Radio Settings.....	79
6.3.1.7	Access Point Settings.....	81
6.3.1.8	Client Settings	82
6.3.1.9	Client Allowed Channel Settings.....	84
6.3.1.10	Security Settings	86
6.3.1.11	Dot1x Supplicant Settings	88
6.3.1.12	Dot1x RADIUS Server Settings	89
6.3.1.13	Summary.....	90
6.4	"Information" menu	91
6.4.1	Start Page	91
6.4.2	Versions.....	97
6.4.3	Identification & Maintenance.....	98
6.4.4	ARP / neighbors.....	100
6.4.4.1	ARP Table.....	100
6.4.4.2	IPv6 Neighbor Table	101
6.4.5	Log Tables	102
6.4.5.1	Event log	102

6.4.5.2	WLAN authentication log	104
6.4.6	Faults	105
6.4.7	Redundancy	106
6.4.8	Ethernet Statistics	110
6.4.8.1	Interface Statistics	110
6.4.8.2	Packet Size	111
6.4.8.3	Frame Type	112
6.4.8.4	Packet Error	112
6.4.9	Learning Table	113
6.4.10	LLDP	114
6.4.11	IPv6 routing	115
6.4.12	DHCP-Server	116
6.4.13	SNMP	117
6.4.14	Security	118
6.4.14.1	Overview	118
6.4.14.2	Supported Function Rights	120
6.4.14.3	Roles	120
6.4.14.4	Groups	121
6.4.15	WLAN	122
6.4.15.1	Overview AP	122
6.4.15.2	Client List	125
6.4.15.3	WDS List	126
6.4.15.4	Overlap AP	127
6.4.15.5	Force Roaming	129
6.4.15.6	Overview Client	130
6.4.15.7	Available AP	133
6.4.15.8	IP Mapping	134
6.4.15.9	Background noise	136
6.4.15.10	Funkschnittstellen-Info	137
6.4.16	WLAN Statistics	138
6.4.16.1	Errors	138
6.4.16.2	Management Sent	139
6.4.16.3	Management Received	141
6.4.16.4	Data Sent	142
6.4.16.5	Data Received	143
6.4.17	WLAN iFeatures	144
6.4.17.1	iPRP	144
6.5	"System" menu	145
6.5.1	Configuration	145
6.5.2	General	150
6.5.2.1	Device	150
6.5.2.2	Coordinates	151
6.5.3	Agent IPv4	153
6.5.4	Agent IPv6	155
6.5.4.1	IPv6 default routes	157
6.5.5	DNS	158
6.5.6	Restart	160
6.5.7	Commit Control	161
6.5.8	Load & Save	163
6.5.8.1	File list	163
6.5.8.2	HTTP	169
6.5.8.3	TFTP	173

6.5.8.4	SFTP	175
6.5.8.5	Passwords.....	179
6.5.9	Events	181
6.5.9.1	Configuration.....	181
6.5.9.2	Severity	183
6.5.10	SMTP Client	184
6.5.11	DHCPv4	186
6.5.11.1	DHCP client.....	186
6.5.11.2	DHCP Server	188
6.5.11.3	DHCP Options	190
6.5.11.4	Static Leases	192
6.5.12	SNMP	194
6.5.12.1	General	194
6.5.12.2	Traps	196
6.5.12.3	v3 Groups	198
6.5.12.4	v3 Users	200
6.5.13	System Time	202
6.5.13.1	Manual Setting	203
6.5.13.2	DST Overview	204
6.5.13.3	DST Configuration	206
6.5.13.4	SNTP Client	209
6.5.13.5	NTP Client.....	213
6.5.13.6	SIMATIC Time Client	215
6.5.14	Auto Logout.....	216
6.5.15	Syslog client	217
6.5.16	Fault Monitoring	219
6.5.16.1	Power Supply.....	219
6.5.16.2	Link Change.....	220
6.5.17	PROFINET.....	221
6.5.18	EtherNet/IP	223
6.5.19	Ping.....	225
6.6	"Interfaces" menu	226
6.6.1	Ethernet	226
6.6.1.1	Overview	226
6.6.1.2	Configuration.....	228
6.6.2	WLAN	230
6.6.2.1	Basic.....	230
6.6.2.2	Advanced	235
6.6.2.3	Antennas	237
6.6.2.4	Allowed Channels	240
6.6.2.5	802.11n	242
6.6.2.6	AP	243
6.6.2.7	AP WDS	247
6.6.2.8	AP 802.11a/b/g Rates	248
6.6.2.9	AP 802.11n Rates.....	251
6.6.2.10	Client.....	253
6.6.2.11	Force roaming	258
6.6.2.12	Signal recorder	260
6.6.2.13	Spectrum analyzer	270
6.6.3	Remote Capture	277
6.7	"Layer 2" menu	280

6.7.1	VLAN	280
6.7.1.1	General	280
6.7.1.2	Port-based VLAN	283
6.7.2	Dynamic MAC Aging	286
6.7.3	Spanning Tree	287
6.7.3.1	General	287
6.7.3.2	CIST General	289
6.7.3.3	CIST Port	291
6.7.3.4	MST General	295
6.7.3.5	MST Port	297
6.7.4	DCP Forwarding	299
6.7.5	LLDP	300
6.8	"Layer 3" menu	301
6.8.1	NAT	301
6.8.1.1	Basic	301
6.8.1.2	NAPT	304
6.9	"Security" menu	306
6.9.1	Users	306
6.9.1.1	Local Users	306
6.9.1.2	Roles	309
6.9.1.3	Groups	310
6.9.2	Passwords	312
6.9.2.1	Passwords	312
6.9.2.2	Options	314
6.9.3	AAA	314
6.9.3.1	General	314
6.9.3.2	RADIUS client	315
6.9.4	WLAN	318
6.9.4.1	Basic (Access Point)	318
6.9.4.2	Basic (Client)	321
6.9.4.3	AP communication	325
6.9.4.4	AP RADIUS Authenticator	326
6.9.4.5	Client RADIUS Supplicant	329
6.9.4.6	Keys	331
6.9.5	MAC ACL	332
6.9.5.1	Rules Configuration	332
6.9.5.2	Ingress Rules	334
6.9.5.3	Egress Rules	335
6.9.6	IP ACL	337
6.9.6.1	Rules Configuration	337
6.9.6.2	Protocol Configuration	338
6.9.6.3	Ingress Rules	340
6.9.6.4	Egress Rules	342
6.9.7	Management ACL	344
6.10	"iFeatures" menu	347
6.10.1	iPCF	347
6.10.2	iPCF-HT	348
6.10.3	iPCF-MC	350
6.10.4	iPRP	352

7	Upkeep and maintenance.....	355
7.1	Firmware update - via WBM.....	355
7.2	Embedding firmware in ConfigPack.....	356
7.3	Restoring the factory settings.....	357
8	Troubleshooting/FAQ	359
8.1	Firmware update via WBM or CLI not possible	359
8.2	Disrupted data transmission due to the received power being too high	360
8.3	Compatibility with predecessor products	361
8.4	Instructions for secure network design	362
8.5	WLAN client Trigger handover via SNMP	362
8.6	Configuring the device using the TIA Portal.....	363
8.6.1	Message: SINEMA configuration not yet accepted	365
A	Appendix A "Supported MIB Modules"	367
A.1	Supported MIB files	367
B	Appendix B "Private MIBs".....	369
B.1	Private MIB variables	369
C	Appendix C "Underlying Standards"	371
C.1	Underlying standards	371
D	Appendix D "Log Messages".....	373
D.1	Messages in the event log	373
D.2	Messages in the WLAN Authentication Log	376
E	Appendix "Syslog Messages"	379
E.1	Format of the syslog messages.....	379
E.2	Parameters in Syslog messages	380
E.3	Syslog Messages	381
F	Appendix F (Supported Security Mechanisms)	389
F.1	WLAN security mechanisms	389
F.2	Security mechanisms supported for RADIUS authentication.	389
G	Appendix G "Permitted characters in names, passwords and descriptions".....	391
G.1	Permitted characters	391
	Index.....	393

Introduction

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 the manual

This Configuration Manual covers the following products:

- SCALANCE W721-1 RJ45
- SCALANCE W722-1 RJ45
- SCALANCE W761-1 RJ45

The Configuration Manual applies to the following firmware version:

- SCALANCE W700 IEEE 802.11n Firmware as of version V6.5

1.3 Information on the Configuration Manual

Documentation on the Internet

You can find the current version of the documents on the Internet at (<https://sieportal.siemens.com/su/bjSDr>).

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 W760/W720 Command Line Interface
This document contains the CLI commands that are supported by SCALANCE W700 devices.
- 802.11 abgn SCALANCE W760/W720 performance data
This document contains information about the frequency, modulation, transmit power and receiver sensitivity.
- SCALANCE W700 802.11n approvals
This document contains information on currently available country approvals.

- Operating instructions SCALANCE W760/W720
This document contains information on installing and connecting up the following products and their approvals.
 - SCALANCE W721-1 RJ45
 - SCALANCE W722-1 RJ45
 - SCALANCE W761-1 RJ45
- System Manual Structure of an Industrial Wireless LAN
Apart from the description of the physical basics and a presentation of the main IEEE standards, this also contains information on data security and a description of the industrial applications of wireless LAN.
You should read this manual if you want to set up WLAN networks with a more complex structure (not simply a connection between two devices).
- System manual RCoax
This system manual contains both an explanation of the fundamental technical aspects as well as a description of the individual RCoax components and their functionality. Installation/ commissioning and connection of RCoax components and their operating principle are explained. The possible applications of the various SIMATIC NET components are described.
- System manual - Passive Network Components IWLAN
This system manual explains the entire IWLAN cabling that you require for your IWLAN application. For a flexible combination and installation of the individual IWLAN components both indoors and outdoors, a wide ranging selection of compatible coaxial accessories are available. The system manual also covers connecting cables as well as a variety of plug-in connectors, lightning protectors, a power splitter and an attenuator.

SIMATIC NET manuals

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

- Using the search function:
Siemens Industry Online Support (<https://support.industry.siemens.com/cs/ww/en/>)
Enter the entry ID of the relevant manual as the search item.
- In the navigation panel on the left-hand side in the area "Industrial Communication":
Industrial communication (<https://support.industry.siemens.com/cs/ww/en/ps/15247/man>)
Go to the required product group and make the following settings:
tab "Entry list", Entry type "Manuals"

Further documentation

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

The "SIMATIC NET Industrial Ethernet Network Manual" can be found on the Internet pages of Siemens Industry Online Support under the following entry ID:
27069465 (<https://support.industry.siemens.com/cs/ww/en/view/27069465>)

SIMATIC NET glossary

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

You will find the SIMATIC NET glossary here:

- SIMATIC NET Manual Collection or product DVD
The DVD ships with certain SIMATIC NET products.
- On the Internet under the following address:
50305045 (<https://support.industry.siemens.com/cs/ww/en/view/50305045>)

Training, Service & Support

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

1.4 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.

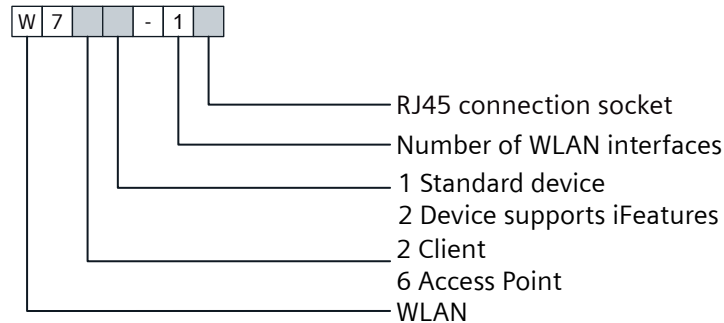
Abbreviations used

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

Product group	The designation . . . stands for . . .	Product name
Access point	W761-1	SCALANCE W761-1 RJ-45
Client	W721-1	SCALANCE W721-1 RJ-45
Client with iFeatures	W722-1	SCALANCE W722-1 RJ-45
All SCALANCE W devices	W700	SCALANCE W761-1 RJ-45 SCALANCE W721-1 RJ-45 SCALANCE W722-1 RJ-45

1.5 Structure of the type designation

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



1.6 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/cybersecurity-industry> (<https://www.siemens.com/industrialsecurity>).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase 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/cert> (<https://www.siemens.com/cert>).

1.7 Firmware

The firmware is available on the Internet pages of the Siemens Industry Online Support: (<https://support.industry.siemens.com/cs/de/en/ps/15860/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.

1.8 Open source license conditions

License conditions

Note**Open source software**

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

You will find license conditions in the following documents on the supplied data medium:

- OSS_Scalance-W700_86.pdf

1.9 Error/fault

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

1.10 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.

1.11

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.

1.12

Marken

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

SCALANCE, C-PLUG, RCoax

Security recommendations

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.

2.1 Security recommendations

- 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 2048 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 access the system without authorization.
- 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 (for example 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".
- 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.

2.1 Security recommendations

- 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 163)".
- 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 194)".
 - 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 306)".
- 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 306)".

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
- **Default port status**
This is the status of the port in the delivery state (factory setting).
- **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
			Port	Service		
DHCP Client IPv4	UDP/68	Outgoing only	--	✓	--	--
DHCP Client IPv6	UDP/546	Outgoing only	--	✓	--	--
DHCP Server	UDP/67	Closed	--	✓	--	--

2.2 Available services

Service	Protocol / Port number	Default port status	Configurable		Authentication	Encryption
			Port	Service		
DNS Client	TCP/53 UDP/53	Outgoing only	--	✓	--	--
EthernetIP	TCP/44818 UDP/2222 UDP/44818	Closed	--	✓	--	--
HTTP	TCP/80	Open	✓	✓	✓	--
HTTPS	TCP/443	Open	✓	✓	✓	✓
NTP Client	UDP/123	Outgoing only	✓	✓	--	--
PROFINET	UDP/34964 UDP/49154 UDP/49155	Open	--	✓	--	--
RADIUS Client	UDP/1812	Outgoing only	✓	✓	✓	--
Remote Capture	TCP/2002	Closed	--	✓	--	--
SFTP Client	TCP/22	Closed	✓	✓	✓	✓
SMTP Client	TCP/25	Closed	✓	✓	--	--
SMTP Client (secure) ¹⁾	TCP/465	Closed	✓	✓	✓	✓
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 (secure) Client	TCP/6514	Closed	✓	✓	--	✓
Telnet	TCP/23	Closed ¹⁾ / Open ²⁾	✓	✓	✓	--
TFTP Client	UDP/69	Outgoing only	✓	✓	--	--

1) Only for SCALANCE W1700ac

2) Only for SCALANCE W700n

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	Open	✓
iPRP	Open	✓
MSTP	Closed	✓
SIMATIC NET TIME	Closed	✓

Description

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 Network structures

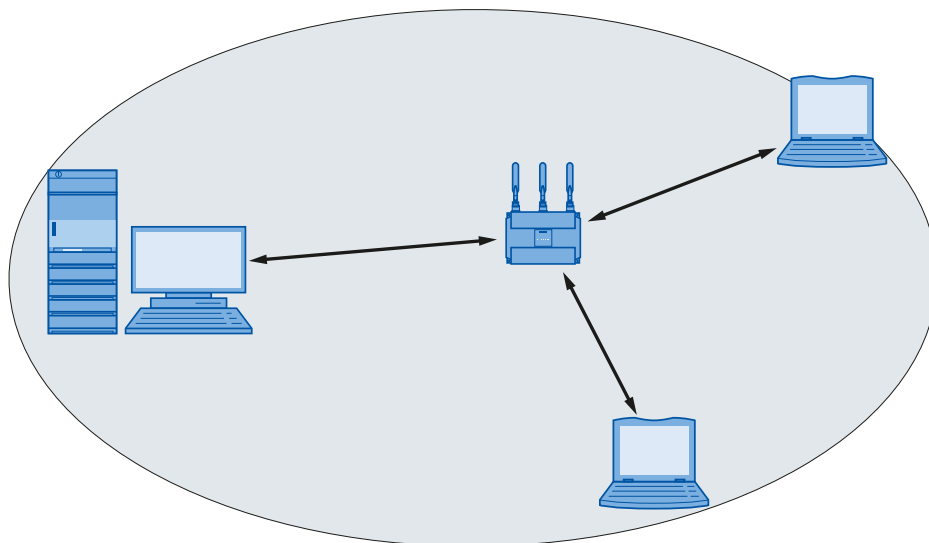
The following article deals with the setting up of various network structures using access points and clients. A client is also an access point in client mode.

Standalone configuration with access point

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

The wireless network has a unique name. All the SCALANCE W700 devices exchanging data within this network must be configured with this name.

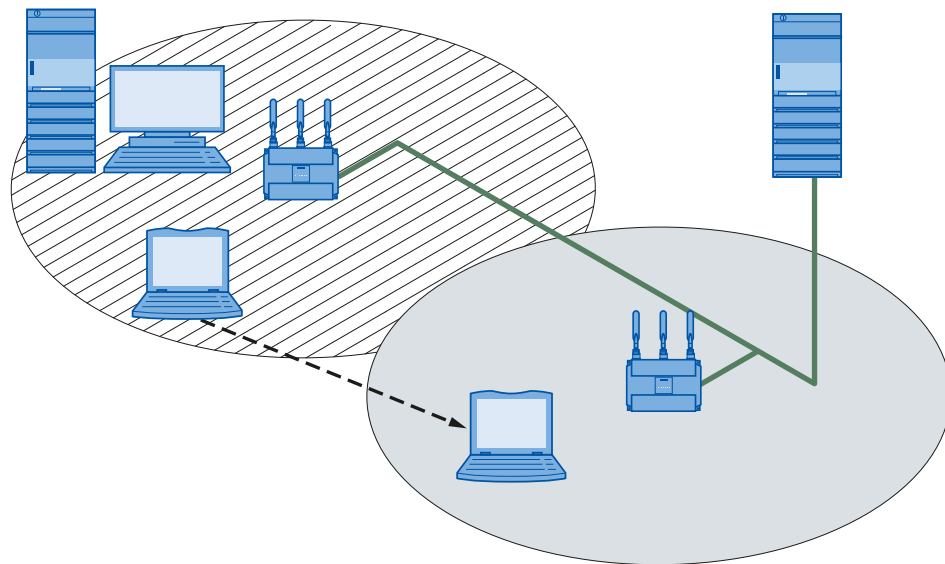
The gray area in the graphic symbolizes the wireless range of the access point.



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).



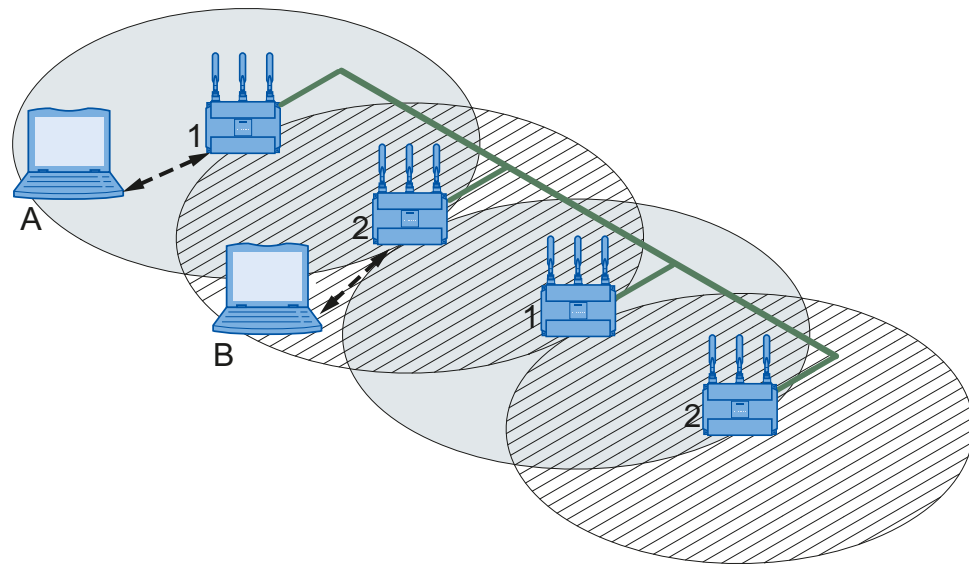
Multichannel configuration

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.

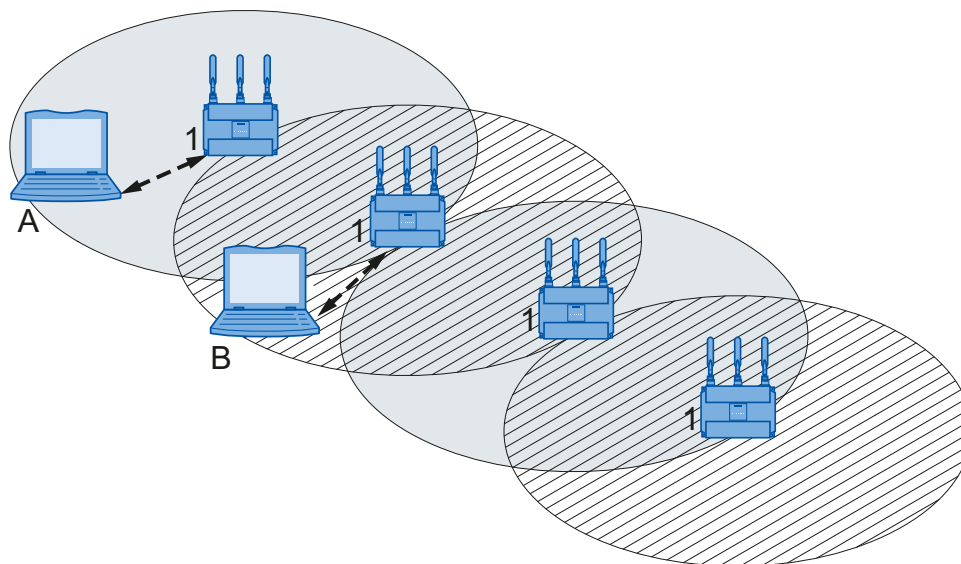


Wireless Distribution System (WDS)

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

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

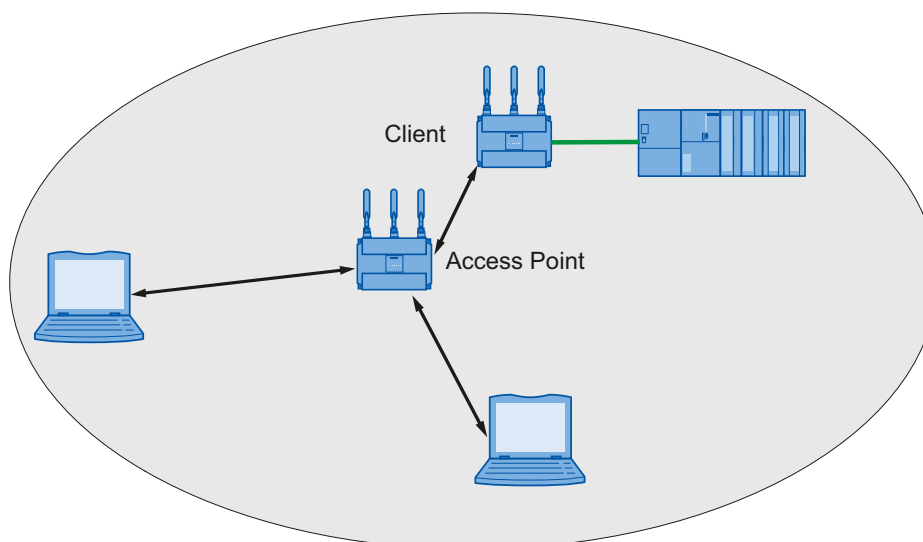
The following graphic shows the implementation of WDS with four access points.



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

The SCALANCE W700 device can be used to integrate wired Ethernet devices (for example SIMATIC S7 PLC) in a wireless network.

The following graphic shows the connection of a SIMATIC S7 PLC to a wireless LAN.



3.2 Possible applications of SCALANCE W700 devices

Note

The SIMATIC NET WLAN products use OpenSSL.

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

Please refer to the current license conditions.

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

Possible applications of the SCALANCE W761

The SCALANCE W761 is equipped with an Ethernet interface and a WLAN interface. This makes the SCALANCE W700 device suitable for the following applications:

- The SCALANCE W761 forwards data within its transmission range from one node to another without a connection to wired Ethernet being necessary.
- The SCALANCE W761 can be used as a gateway from a wired to a wireless network.
- The SCALANCE W761 supports protection class IP20.

Possible applications of the SCALANCE W722

The SCALANCE W722 is equipped with an Ethernet interface and a WLAN interface. This makes the SCALANCE W700 device suitable for the following applications:

- The SCALANCE W722 can be used as a gateway from a wired to a wireless network.
- The SCALANCE W722 can be used with iPCF as a client.
- The SCALANCE W722 supports protection class IP20.

Possible applications of the SCALANCE W721

The SCALANCE W721 is equipped with two Ethernet interfaces and a WLAN interface. This makes the SCALANCE W700 device suitable for the following applications:

- The SCALANCE W721 can be used as a gateway from a wired to a wireless network.
- The SCALANCE W721 supports protection class IP20.

3.3 Product characteristics

Properties of the SCALANCE W700 devices

- The Ethernet interface supports the following:
 - 10 Mbps and 100 Mbps both in full and half duplex
 - Autocrossing
 - Autopolarity
- Operating the WLAN interface in the frequency bands 2.4 GHz and 5 GHz.
- The WLAN interface is compatible with the standards IEEE 802.11a , IEEE 802.11b , and IEEE 802.11g. In the 802.11a and 802.11g mode, the gross transmission rate is up to 54 Mbps.
- IEEE 802.11n
High-speed WLAN standard (wireless LAN) and can operate in the 2.4 GHz and in the 5 GHz range.
- IEEE 802.11h - Supplement to IEEE 802.11a
In the 802.11h mode, the methods "Transmit Power Control (TPC)" as well as "Dynamic Frequency Selection (DFS)" are used in the range 5.25 - 5.35 and 5.47 - 5.75 GHz. In some countries, this allows the frequency subband of 5.47 - 5.725 GHz to be used 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, WPA-PSK, WPA2, WPA2-PSK and IEEE 802.1x and the encryption methods WEP, AES and TKIP.

Note

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

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

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

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

Note

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

Features of the SCALANCE W700

Type	Number of WLAN ports	Antennas	Number and type of Ether- net interface	Degree of protec- tion	Article number
SCALANCE W761-1 RJ45	1	external	1 x 10/100 Mbps Ethernet (cop- per)	IP20	6GK5761-1FC00-0AA0 6GK5761-1FC00-0AB0 ⁽¹⁾
SCALANCE W722-1 RJ45	1	external	1 x 10/100 Mbps Ethernet (cop- per)	IP20	6GK5722-1FC00-0AA0 6GK5722-1FC00-0AB0 ⁽¹⁾ 6GK5722-1FC00-0AC0 ⁽²⁾
SCALANCE W721-1 RJ45	1	external	1 x 10/100 Mbps Ethernet (cop- per)	IP20	6GK5721-1FC00-0AA0 6GK5721-1FC00-0AB0 ⁽¹⁾

(1) US device version

(2) ME device version

3.4 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.

3.5 IEEE 802.11n

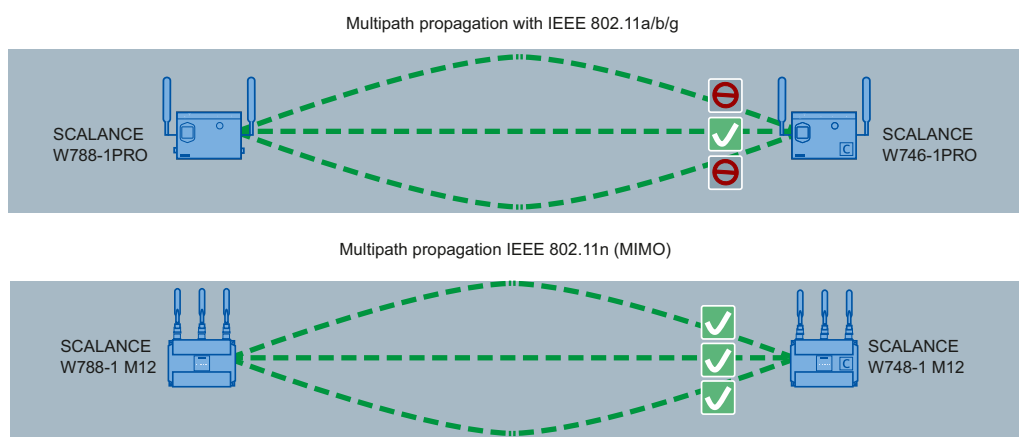
Overview

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

- MIMO antenna technology
- Maximum ratio combining (MRC)
- Spatial multiplexing
- Channel bonding
- Frame aggregation
- Accelerated guard interval
- Modulation and coding scheme
- Data throughput rates up to 450 Mbps (gross)
This is not possible on all SCALANCE W700 devices.

MIMO antenna technology

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



Maximum ratio combining (MRC)

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

Spatial mutliplexing

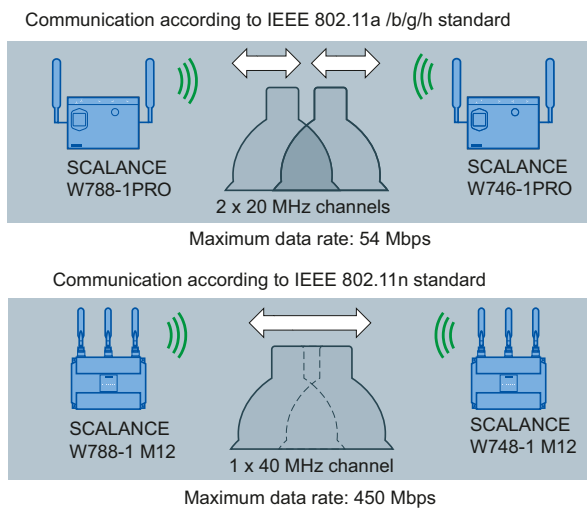
With spatial multiplexing, different information is sent using the same frequency. The data stream is distributed over n transmitting antennas; in other words, each antenna sends only $1/n$ of the data stream. The division of the data stream is restricted by the number of antennas. At the receiver end, the signal is reconstructed.

Due to the spatial multiplexing, there is a higher signal-to-noise ratio and a higher data throughput.

Channel bonding

With IEEE 802.11n, data can be transferred via two directly neighboring channels. The two 20 MHz channels are put together to form one channel with 40 MHz. This allows the channel bandwidth to be doubled and the data throughput to be increased.

To be able to use channel bonding, the recipient must support 40 MHz transmissions. If the recipient does not support 40 MHz transmissions, the band is automatically reduced to 20 MHz. This means that IEEE 802.11n can also communicate with IEEE 802.11a/b/g devices. The channel bundling is set on the "AP (Page 243)" WBM page with the "HT Channel Width [MHz]" parameter.



Frame aggregation

With IEEE 802.11n, it is possible to group together individual data packets to form a single larger packet; this is known as frame aggregation. There are two types of frame aggregation:

- Aggregated MAC Protocol Data Unit (A-MPDU)
With A-MPDU, multiple MPDU data packets with the same destination address are bundled and sent as one large A-MPDU.
- Aggregated Mac Service Data Unit (A-MSDU)
With A-MSDU, multiple MSDU data packets with the same destination address are chained together and sent.

The SCALANCE W devices support both types of frame aggregation. You make the settings on the WBM page "AP 802.11n (Page 242)".

Accelerated guard interval

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

The guard interval of IEEE 802.11a /b/g is 800 ns. IEEE 802.11n can use the reduced guard interval of 400 ns. You specify the guard interval on the WBM page "AP 802.11n (Page 242)".

Modulation and coding schemes

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

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 ConfigPack

Configuration information in the ConfigPack

With ConfigPack it is possible to install ta device configuration on several devices.

Note

Using configurations with DHCP

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.

The device configuration, user accounts and certificates are stored in the ConfigPack.

The storage of the active firmware of the creating device must be released in the CLI.

You save and load the ConfigPack using the WBM.

if the firmware was stored as well, when installing the firmware the device performs a firmware upgrade/downgrade if the firmware versions differ from each other.

For more information, refer to the section Upkeep and maintenance (Page 355).

Technical basics

4.1 Configuration limits for WBM and CLI

Configuration limits of the device

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

Depending on your device, some functions are not available.

	Configurable function		Maximum number
System	Syslog server		3
	DNS server	manual (IPv4/IPv6)	3
		learned (IPv4/IPv6)	2
		in total	7
	SMTP server		3
	SNMPv1 trap recipient		10
	SNMP queries		50
	SNTP server		2
	NTP server		1
	DHCP pools		1
	IPv4 addresses managed by the DHCP server (dynamic + static)		100
	DHCP static assignments per DHCP pool		20
	DHCP options		20
Interfa- ces	Force destination addresses for roaming		10
	Connected clients per VAP		100
Layer 2	Virtual LANs (port-based, including VLAN 1)		3
	Multiple Spanning Tree instances		16

	Configurable function	Maximum number
Security	IP addresses from RADIUS servers	<ul style="list-style-type: none"> AAA: 4 WLAN: 2
	Management ACLs (access rules for management)	10
	MAC ACL rule configuration	20
	Ingress and egress rules for MAC ACL (total)	40 per interface (20 ingress rules / 20 egress rules) <ul style="list-style-type: none"> Client: 80 (P1, WLAN) Access point: 680 (P1, WDS 1.Y, VAP 1.Y)
	IP ACL rule configuration	20
	Ingress and egress rules for IP ACL IP (total)	40 per interface (20 ingress rules / 20 egress rules) <ul style="list-style-type: none"> Client: 120 (P1, WLAN, management VLAN) Access point: 720 (P1, WDS 1.Y, VAP 1.Y, management VLAN) Dual access point: 1360 (P1, WDS X.Y, VAP X.Y, management VLAN)
	User roles	28
	User groups	32
	Users	28

4.2 Interfaces and system functions

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.

	Client device W721-1 RJ45 W722-1 RJ45	Access points W761-1 RJ45
Wireless interface (WLAN)	WLAN 1	WLAN 1
IP interface:		
LAN interface	P1	P1
VLAN	ManagementVLAN	ManagementVLAN
VAP interface ¹⁾	-	VAP 1.1

	Client device W721-1 RJ45 W722-1 RJ45	Access points W761-1 RJ45
WDS interface ¹⁾	—	WDS 1.1
VLAN	3	3

¹⁾ only in access point mode

Availability of the system functions

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

We reserve the right to make technical changes.

			Access point mode	Access points in client mode Client devices
Informa- tion	WLAN	Overview AP	✓	-
		Client List	✓	-
		WDS List	✓	-
		Overlap AP	✓	-
		Force Roam- ing	✓	-
		Overview Client	-	✓
		Available AP	-	✓
		IP Mapping	-	✓
	WLAN Statis- tics	Faults	✓	✓
		Manage- ment Sent	✓	✓
		Manage- ment Re- ceived	✓	✓
		Data Sent	✓	✓
		Data Re- ceived	✓	✓
System		PROFINET	✓	✓
		EtherNet/IP	✓	✓

4.2 Interfaces and system functions

			Access point mode	Access points in client mode Client devices
Interfaces	WLAN	Basic	✓	✓
		Advanced	✓	✓
		Antennas	✓	✓
		Allowed Channels	✓	✓
		802.11n	✓	✓
		AP	✓	-
		AP WDS	✓	-
		AP 802.11a/b/g Rates	✓	-
		AP 802.11n Rates	✓	-
		Force Roaming	✓	✓
		Signal recorder	-	✓
		Spectrum Analyzer	✓	-
Layer 3	NAT	Basic	-	✓
		NAPT	-	✓
Security	WLAN	Basic	✓	✓
		AP Communication	✓	-
		AP RADIUS Authenticator	✓	-
		Client RADIUS Supplicant	-	✓
		Keys	✓	✓
iFeatures	iPCF		-	✓ Only W722-1 RJ45 This can be integrated in a WLAN with iPCF, iPCF-MC.
	iPCF-HT		-	✓ Only W722-1 RJ45
	iPCF-MC		-	✓ Only W722-1 RJ45 This can be integrated in a WLAN with iPCF, iPCF-MC.
	iPRP		-	✓ Only W722-1 RJ-45

Support of IPv6

The following system functions do not support IPv6 addresses:

- Inter AP blocking
- Force roaming

4.3 EtherNet/IP

EtherNet/IP

EtherNet/IP (Ethernet/Industrial Protocol) is an open industry standard for industrial real-time Ethernet based on TCP/IP and UDP/IP. With EtherNet/IP, Ethernet is expanded by the Common Industrial Protocol (CIP) at the application layer. In EtherNet/IP, the lower layers of the OSI reference model are adopted by Ethernet with the physical, network and transport functions.

You configure EtherNet/IP in "System > EtherNet/IP (Page 223)".

Common Industrial Protocol

The Common Industrial Protocol (CIP) is an application protocol for automation that supports transition of the field buses in Industrial Ethernet and in IP networks. This industry protocol is used by field buses/industrial networks such as DeviceNet, ControlNet and EtherNet/IP at the application layer as an interface between the deterministic fieldbus world and the automation application (controller, I/O, HMI, OPC, ...). The CIP is located above the transport layer and expands the pure transport services with communications services for automation engineering. These include services for cyclic, time-critical and event-controlled data traffic. CIP distinguishes between time-critical I/O messages (implicit messages) and individual query/response frames for configuration and data acquisition (explicit messages). CIP is object-oriented; all data "visible" from the outside is accessible in the form of objects. CIP has a common configuration basis: EDS (Electronic Data Sheet).

Electronic Data Sheet

Electronic Data Sheet (EDS) is an electronic datasheet for describing devices.

The EDS required for EtherNet/IP operation can be found in "System > Load&Save (Page 163)".

4.4 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 221)".

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).

4.5 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.

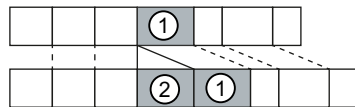
Options for the VLAN assignment

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 283)".
- 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.

4.6 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 "Automatic", "Manual" and "Own"

If the MAC address of a device connected to the client is adopted (Automatic) or is set manually (Manual), both the MAC-based and the IP-based frames find their destination for precisely this device. 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

Notes on the "Automatic" setting:

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

Note

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

MAC mode "Layer 2 Tunnel"

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

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

Maximum possible number of Ethernet nodes downstream from the client: 4

4.7 iPCF / iPCF-HT / iPCF-MC

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

If very fast update times are required, for example for PROFINET communication, access points and client modules need to be used that use the proprietary methods iPCF / iPCF-HT or iPCF-MC for fast roaming and deterministic data traffic.

iPCF / iPCF-HT / iPCF-MC can only be operated alone. A combination with each other is not possible, e.g. iPCF with iPCF-HT or iPCF-MC.

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.

You configure iPCF in "iFeatures > iPCF > iPCF (Page 347)".

iPCF-HT

If a higher data throughput is required for iPCF, iPCF-HT is used. With this you can, for example, alongside PROFINET also transfer video data. This is achieved by more effective transfer of data packets using frame-bursting (A-MPDU). The individual data packets are grouped together that are intended for the same receiver station (client) and that have the same prioritization.

You configure iPCF-HT in "iFeatures > iPCF > iPCF-HT (Page 348)".

iPCF-MC

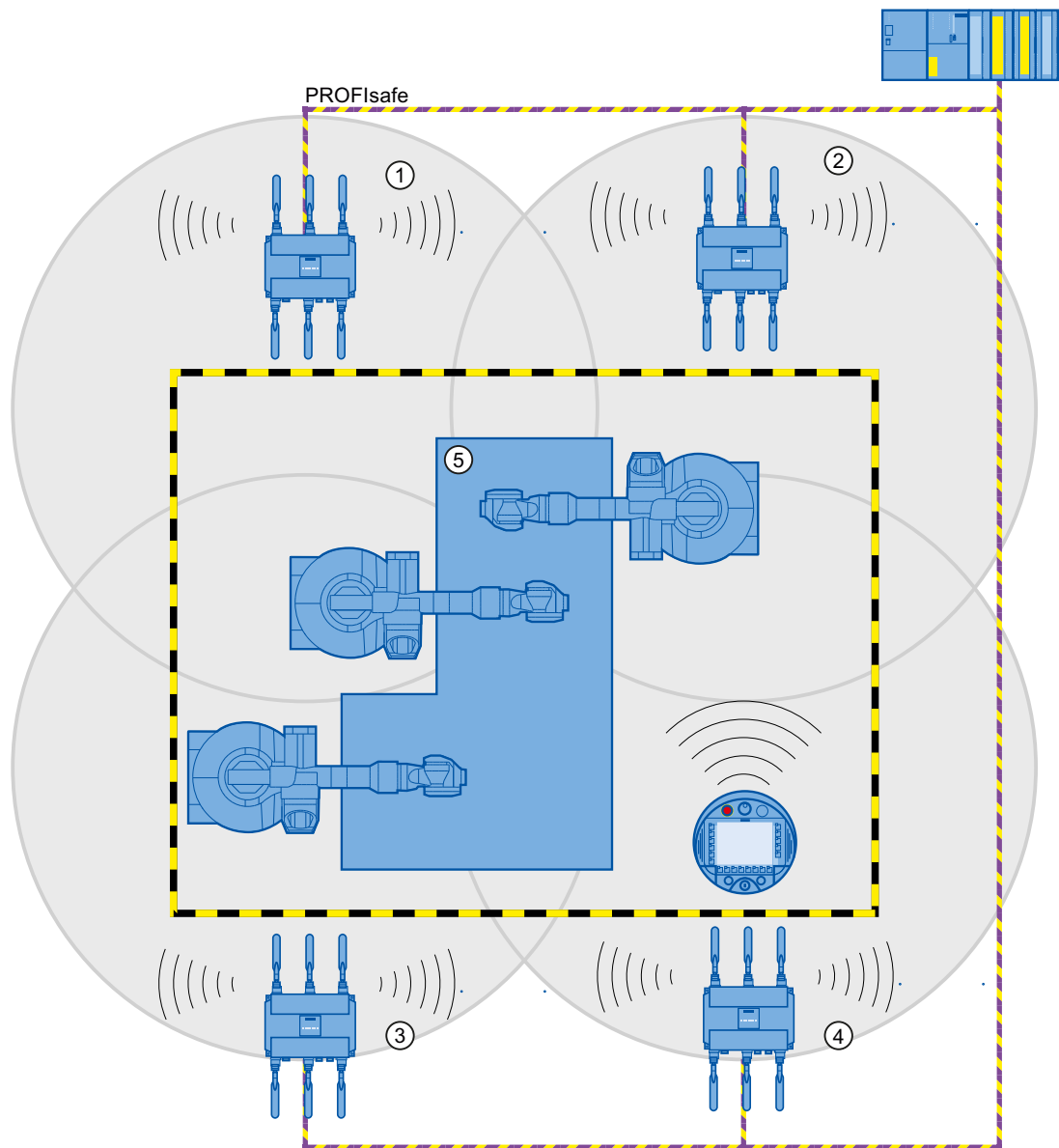
For freely moving nodes that communicate independently of a RCoax cable or directional antennas, iPCF-MC should be used. With iPCF-MC, the client also searches for potentially suitable access points when it receives iPCF queries from the access point and the existing connection to an access point is working problem-free. This means that if a change to a different access point is necessary, this is achieved extremely quickly. In contrast to iPCF, the handover times for iPCF-MC are not dependent on the number of wireless channels being used.

It is necessary to use an access point with two wireless interfaces a so-called dual access point. The one interface operates as management channel and sends short frames (beacons) with administrative information (e.g. channel setting of the data channel and SSID). The other interface (data channel) exclusively transfers the user data.

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.

You configure iPCF-MC in "iFeatures > iPCF > iPCF-MC (Page 350)".

The following graphic shows a configuration example for iPCF-MC.



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

Restrictions

- iPCF / iPCF-HT and iPCF-MC are developments of Siemens AG and function only with nodes on which iPCF / iPCFv2 / iPCF-MC is implemented.
- With an access point with several WLAN interfaces, it is possible to use both iPCF / iPCF-HT as well as standard WLAN at the same time. Parallel operation of iPCF on both interfaces is not recommended.

- Access points with a WLAN interface cannot take part in the iPCF-MC procedures, iPCF is, however, possible.
- iPCF-HT is available only on WLAN interface 1 and can only be used in the 5 GHz band with WLAN mode "(only) IEEE 802.11n".

Note

If both interfaces are operated in the same frequency range for access points with two WLAN interfaces:

- The distance between the antennas connected to R1A1, R1A2, R1A3 and those connected to R2A1, R2A2, R2A3 must be at least 1 m.
 - There may be wireless interference on one or both WLAN interfaces if the transmit power is higher than 15 dB.
-

Requirements for iPCF-MC

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

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

- Only SCALANCE W700 devices with two WLAN interfaces can be used as access points
- The data interface (WLAN1) and management interface (WLAN2) must be operated in the same frequency band and must match in terms of their wireless coverage. iPCF-MC will not work if the two wireless interfaces are equipped with directional antennas that cover different areas.
- The management interfaces of all access points to which a client can change must use the same channel. A client scans only this one channel to find accessible access points.
- Transmission based on IEEE 802.11h (DFS) cannot be used for the management interface. 802.11h (DFS) is possible for the data interface.
- A client must support this feature on its WLAN interface.

4.8 iPRP

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

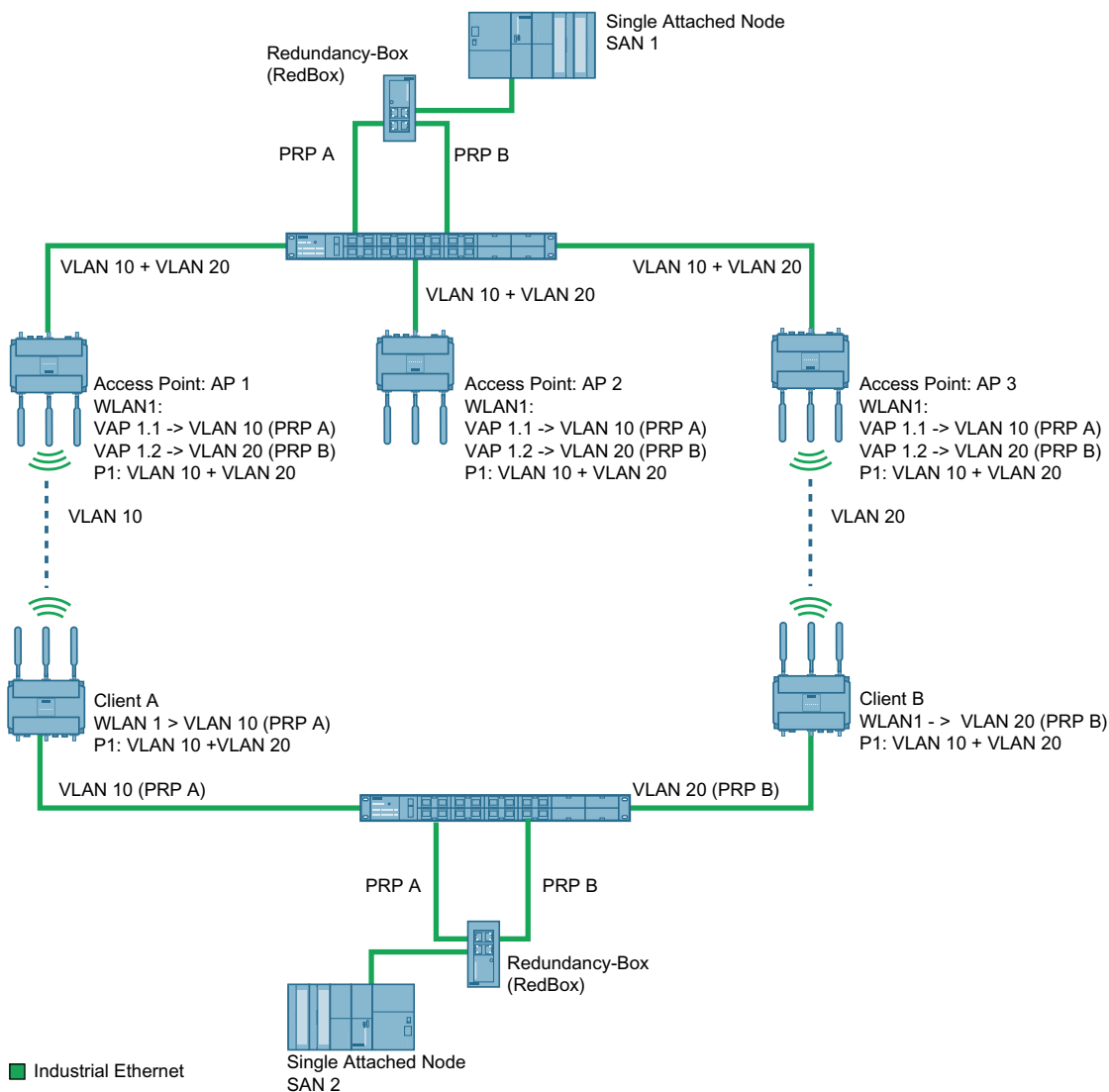
With the "industrial Parallel Redundancy Protocol" (iPRP) the PRP technology can be used in wireless networks. This improves the availability of wireless communication.

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 W700 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.

Note

On the interfaces of the switches to the SCALANCE W700 devices, only the VLANs that are also set on the VAP or WLAN interfaces of the SCALANCE W700 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 352)".

Requirement

- The base bridge mode "802.1Q VLAN Bridge" is set.
- The VLANs have been created.
- Access point mode: The VAP interface is enabled.
- In client mode:
 - For "MAC Mode", "Layer 2 Tunnel" is set.
 - For "Background Scan mode", either "Always", "Deactivated" or "Current channel" is set.
- Depending on the configuration the clients can communicate with every access point.

4.9 NAT/NAPT

What is NAT?

NAT (Network Address Translation) is a simplified source NAT and is also referred to as IP masquerading. 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.

You configure NAT under "Layer 3 > NAT > Basic" (Page 301).

What is NAPT?

NAPT (Network Address and Port Translation) is a form of destination NAT and is also referred to as port forwarding. The device replaces the external IP address of the terminal device with the internal IP address of the device. The device also exchanges the port number.

The assignment IP address and port number is stored in the NAT table. If the device receives data packages on a certain port, it searches for the corresponding entry in the NAT table. If an entry exists, it adds the IP address and the port number as the destination and forwards the data packet.

Note

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

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

You configure the NAT table under "Layer 3 > NAT > NAPT" (Page 304).

4.10 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 or replacing the C-PLUG.

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

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

Restriction when using the function

Use the "SNMPv3 User Migration" function only to transfer configured SNMPv3 users to a substitute device when replacing a device.

Do not use the function to transfer configured SNMPv3 users to multiple devices. If you load a configuration with created SNMPv3 users on several devices, these devices use the same SNMP engine ID. If you use these devices in the same network, your configuration contradicts the SNMP standard.

Compatibility with predecessor products

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

4.11 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.

4.11.1 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. For 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.

4.12 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.

IP addresses

5.1 IPv4 / IPv6

What are the essential differences?

	IPv4	IPv6
IP configuration	<ul style="list-style-type: none"> DHCP server Manual 	<ul style="list-style-type: none"> Stateless Address Autoconfiguration (SLAAC): Stateless autoconfiguration using NDP (Neighbor Discovery Protocol) <ul style="list-style-type: none"> 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: $4,294,967,296$ addresses	128-bit: $3,402,823,669,209,384,639,693,953,762,264,160,000$ 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 <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Checksum Variable length Fragmentation in the header No security 	<ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 DHCPv6 messages are exchanged between client and server: <ol style="list-style-type: none"> 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 IP addresses. It has the following characteristics:

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

- There is normally no fixed address assignment; in other words, when a client requests an IP address again, it normally receives a different address from the previous address. It is possible to configure the DHCP server so that the DHCP client always receives the same fixed address in response to its request. The parameter with which the DHCP client is identified for the fixed address assignment is set on the DHCP client. The address can be assigned via the MAC address, the DHCP client ID, PROFINET device name or the device name. You configure the parameter in "System > DHCP Client (Page 186)".
- The following DHCP options are supported:
 - DHCP option 3: Assignment of a router address
 - DHCP option 6: Assignment of a DNS server address
 - 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/ww/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".

5.3 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

6.1 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.

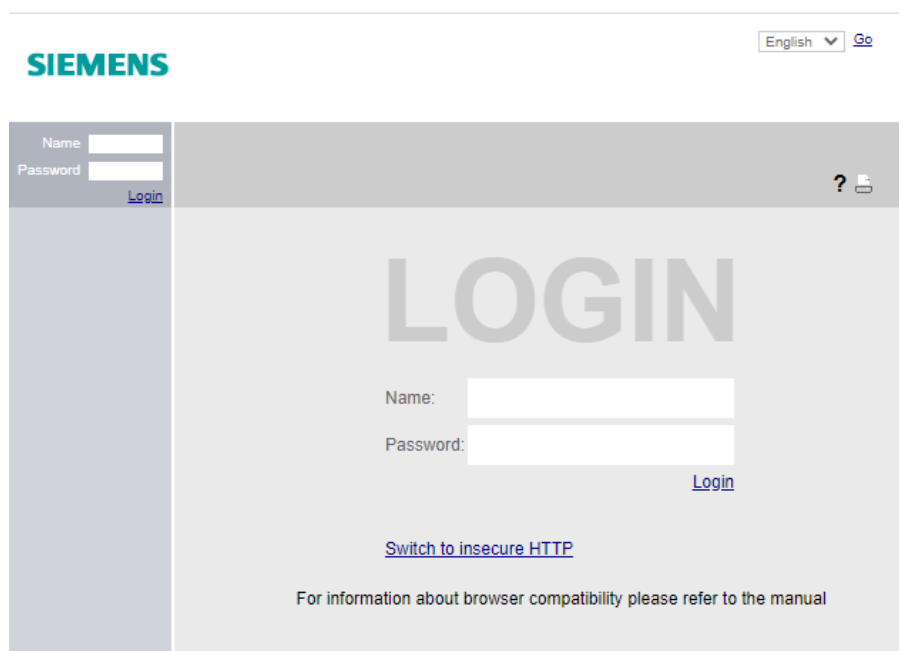
A message relating to the security certificate appears. Acknowledge this message and continue loading the page.

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.



The image shows the Siemens Web Based Management (WBM) login interface. At the top left is the Siemens logo. At the top right is a language selection dropdown set to 'English' and a 'Go' button. On the left side, there is a sidebar with 'Name:' and 'Password:' labels and input fields, followed by a 'Login' link. The main content area has a large 'LOGIN' heading, followed by 'Name:' and 'Password:' labels with input fields, and a 'Login' link. Below this is a link to 'Switch to insecure HTTP' and a note: 'For information about browser compatibility please refer to the manual'.

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 \ ^ ¢ ° € 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 "Wizard" menu

6.3.1 Basic Wizard

Introduction

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

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

Requirement

- The device is in the status it was when it was shipped and can be reached via the Ethernet interface.
- You have assigned an IP address to the device. For more detailed information, refer to the section "IP addresses (Page 55)".
- You are logged in to the WBM as a user with administrator rights. For more detailed information, refer to the section "Login (Page 67)".

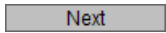

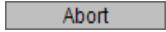

Starting the Basic Wizard

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

When you log in for the first time or following a "Restore Factory Defaults", the Basic wizard is started automatically after you have changed the default password.

Buttons you require often

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

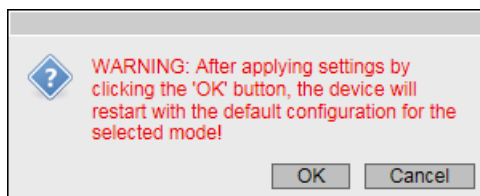
Button	Description
	Goes to the next page
	Goes back to the previous page
	The Basic Wizard is closed without adopting the settings.
	Saves the configuration and exits the Wizard.

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

6.3.1.1 System Settings

Introduction

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



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

Note

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

Basic Wizard: System Settings

System	Country	IP	Management Interfaces	Antenna	Radio	AP	Security	Dot1x RADIUS	Summary
--------	---------	----	-----------------------	---------	-------	----	----------	--------------	---------

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

Restore Memory Defaults and Restart

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

Device Mode: **AP**

Abort **Next**

Description

The Basic Wizard page contains the following boxes:

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

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

- **Device Mode**

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

- AP: Access point mode
- Client: Client mode

6.3.1.2 Country Settings

Introduction

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

Basic Wizard: Country Settings

System	Country	IP	Management Interfaces	Antenna	Radio	AP	Security	Dot1x RADIUS	Summary
--------	---------	----	-----------------------	---------	-------	----	----------	--------------	---------

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

Country Code:

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

System Name:

Description

The Basic Wizard page contains the following boxes

- **Country Code**

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

Note

Locale setting

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

- **System Name**

You can enter the name of the device. If you configure this box, this configuration is adopted and displayed in the selection area. A maximum of 255 characters are possible.

The system name is also displayed in the CLI input prompt. The number of characters in the CLI input prompt is limited. The system name is truncated after 16 characters.

6.3.1.3 IP Address Settings

Introduction

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

Basic Wizard: IP Address Settings

System

Country

IP

Management Interfaces

Antenna

Radio

AP

Security

Dot1x RADIUS

Summary

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

☐ DHCP Client

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

IP Address: 192.168.16.107

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

Previous Abort Next

Description

The Basic Wizard page contains the following boxes:

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

6.3.1.4 Management Interfaces

System configuration

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

Basic Wizard: Management Interfaces

System	Country	IP	Management Interfaces	Antenna	Radio	AP	Security	Dot1X RADIUS	Summary
--------	---------	----	-----------------------	---------	-------	----	----------	--------------	---------

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

☐ Telnet Server

☒ SSH Server

DCP Server:

Read/Write

SNMP:

SNMPv1/v2c/v3

☐ SNMPv1/v2 Read-Only

☒ SINEMA Configuration Interface

Previous

Abort

Next

Description

The page contains the following boxes:

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

- **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.
- **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 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.

6.3.1.5 Antenna Settings

Introduction

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

Basic Wizard: Antenna Settings

SystemCountryIPManagement InterfacesAntennaRadioAPSecurityDot1X RADIUSSummary

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

Connector	Antenna Type	Antenna Gain 2.4 GHz [dBi]	Antenna Gain 5 GHz [dBi]	Cable Length [m]	Additional Attenuation [dB]
R1 A1	Omni-Direct-Mount: ANT795-4MC	3	5	0	0

Previous

Abort

Next

Description

This table contains the following columns:

- Connector**
Shows the name of the relevant antenna connector.
- Antenna Type**
Select the type of external antenna connected to the device. If the type of your antenna is not available, select the entry "User defined".
- Antenna Gain [dBi]**
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]
Enter the antenna gain the antenna has in the 2.4 GHz frequency band.
 - Antenna Gain 5 GHz [dBi]
Enter the antenna gain the antenna has in the 5 GHz frequency band.
- Cable length [m]**
Enter the length of the flexible antenna connecting cable in meters between the device and the external antenna.
- Additional Attenuation [dB]**
Here, specify the additional attenuation caused, for example, by an additional splitter.

Note

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

6.3.1.6 Radio Settings

Introduction

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

Basic Wizard: Radio Settings

SystemCountryIPManagement InterfacesAntennaRadioAPSecurityDot1X RADIUSSummary

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

Radio	Enabled	Radio Mode	Frequency Band	WLAN Mode 2.4 GHz	WLAN Mode 5 GHz	DFS (802.11h)	Outdoor Mode	max. Tx Power
WLAN 1	<input type="checkbox"/>	AP	2.4 GHz	802.11 n	802.11 n	<input type="checkbox"/>	<input type="checkbox"/>	20 dBm

Tx Power Check: Following channels are not allowed in current configuration:

WLAN 1: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13

Previous

Abort

Next

Description

This table contains the following columns:

- Radio**
Shows the available WLAN interfaces.
- Enabled**
Enable or disable the WLAN interface. The WLAN interface is disabled when the device is supplied.
- Radio Mode**
Shows the mode of the WLAN interface.
- Frequency Band**
Specify the frequency band.
- WLAN-Modus**
Select the required transmission standard for the configured frequency band.
 - WLAN Mode 2.4 GHz
Specify the transmission standard for the 2.4 GHz frequency band.
 - WLAN Mode 5 GHz
Specify the transmission standard for the 5 GHz frequency band. The selection depends on the country setting.

- **DFS (802.11h)**
 - Activated
With the DFS function, it is possible to also use the higher 5 Ghz channels. These channels are country-specific and subject to specific DFS specifications. 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
In outdoor mode, the selection of country-dependent channels and the transmit power for operation are extended for outdoor use.
 - Disabled
The device is being operated in indoor mode. In indoor mode, the selection of country-dependent channels and the transmit power for operation in a building are restricted.
- **max. Tx Power**
Specify the transmit power of the device. It may be necessary to reduce the transmit power depending on the antennas being used to avoid exceeding the maximum legal transmit power. Reducing the transmit power effectively reduces cell size.

Note

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

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

6.3.1.7 Access Point Settings

Introduction

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

Note

This page is available only in access point mode.

Basic Wizard: Access Point Settings

System	Country	IP	Management Interfaces	Antenna	Radio	AP	Security	Dot1x RADIUS	Summary
--------	---------	----	-----------------------	---------	-------	----	----------	--------------	---------

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

Radio	Channel	Alternative DFS Channel	HT Channel Width [MHz]
WLAN 1	Auto	-	20

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

Port	SSID
VAP 1.1	Siemens Wireless Network

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

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

Previous

Abort

Next

Description of the displayed boxes

Table 1 contains the following columns:

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

6.3 "Wizard" menu

- **Alternative DFS Channel**

If you have enabled the DFS function on the Basic Wizard page "Radio", specify the alternative channel here. If you want the access point to search for a free channel itself, use "Auto". If you want to use a fixed channel, select the required channel from the drop-down list.

- **HT Channel Width [MHz]**

You can specify the channel bandwidth with the IEEE 802.11n transmission standard. The following settings are possible.

- 20
Channel bandwidth 20 MHz
- 40 up
Channel bandwidth 40 MHz. The configured channel and the neighboring channel above it are used.
- 40 down
Channel bandwidth 40 MHz. The configured channel and the neighboring channel below it are used.

Table 2 contains the following columns:

- **Port**

Shows the first VAP interface per WLAN interface.

- **SSID**

Enter the SSID. The length of the character string for SSID it is 1 to 32 characters.

The ASCII code 0x20 to 0x7e is used for the SSID.

After completing the Basic Wizard, you can define further SSIDs with "Interfaces > WLAN > Access Point Settings".

6.3.1.8 Client Settings

Introduction

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

Note

This page is only available in client mode.

Basic Wizard: Client Settings

System	Country	IP	Management Interfaces	Antenna	Radio	Client	Channels	Security	Dot1x Supplicant	Summary
--------	---------	----	-----------------------	---------	-------	--------	----------	----------	------------------	---------

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

Radio	MAC Mode	MAC Address	Any SSID
WLAN 1	Automatic	00-00-00-00-00-00	<input checked="" type="checkbox"/>

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

Radio	SSID	Security Context
WLAN 1		1

Previous

Abort

Next

Description

Table 1 contains the following columns:

- Radio**
Shows the available WLAN interfaces.
- MAC Mode**
Specify how the MAC address is assigned to the client. The following are possible:
 - Automatic
The client automatically adopts the source MAC address of the first frame that it receives over the Ethernet interface.
 - Manual
If you select "Manual", enter the MAC address in the "MAC Address" column.
 - Own
The client uses the MAC address of the Ethernet interface for the WLAN interface.
 - Layer 2 Tunnel
The client uses the MAC address of the Ethernet interface for the WLAN interface. The network is also informed of the MAC addresses connected to the Ethernet interface of the client. Up to eight MAC addresses can be used.

6.3 "Wizard" menu

- **MAC Address**
Enter the MAC address of the client. The input box can only be edited if you have set "Manual" for the "MAC Mode".
- **Any SSID**
 - Enabled
In client mode, the device attempts to connect to the network with the best transmission quality and that has suitable security settings.
 - Disabled
The client attempts to connect to the network from the SSID list that has the best transmission quality.

Table 2 contains the following columns:

- **Radio**
Shows the available WLAN interfaces.
- **SSID**
Enter the SSID of the access point with which the client connects. In the Basic Wizard, you can only specify one SSID. After completing the Basic Wizard, you can define further SSIDs with "Interfaces > WLAN > Client".
- **Security Context**
Shows the assigned security context. In the Basic Wizard only one security context is available. After completing the Basic Wizard, you can create and configure further security contexts in "Security > WLAN > Basic".

6.3.1.9 Client Allowed Channel Settings

Introduction

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

Note

This page is only available in client mode.

Basic Wizard: Client Allowed Channel Settings

System	Country	IP	Management Interfaces	Antenna	Radio	Client	Channels	Security	Dot1x Supplicant	Summary
--------	---------	----	-----------------------	---------	-------	--------	----------	----------	------------------	---------

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

Radio ☒ Use Allowed Channels only

WLAN 1 ☐

Frequency Band: 2.4 GHz

☒ Select / Deselect all

Radio	Radio Mode	1	2	3	4	5	6	7	8	9	10	11	12	13
WLAN 1	Client	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Frequency Band: 5 GHz

☒ Select / Deselect all

Radio	Radio Mode	36	40	44	48	52	56	60	64	100	104	108	112	116	132	136	140
WLAN 1	Client	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Previous Abort Next

Description

Table 1 contains the following columns:

- **Radio**
Shows the available WLAN interfaces.
- **Use Allowed Channels only**
If you enable the option, you restrict the selection of channels via which the client is allowed to establish the connection.
In the following tables, you define the channels on which the client searches for an AP. The tables are divided up according to frequency bands.
If the option is disabled, the channels available based on the settings (country code, antennas, transmit power etc.) are used.

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

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

6.3 "Wizard" menu

The tables of the frequency bands have the following columns:

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

Note

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

6.3.1.10 Security Settings

Introduction

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

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

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

Basic Wizard: Security Settings

System	Country	IP	Management Interfaces	Antenna	Radio	Client	Channels	Security	Dot1x Supplicant	Summary
--------	---------	----	-----------------------	---------	-------	--------	----------	----------	------------------	---------

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

Security Context	Authentication Type	Cipher	WPA(2) Pass Phrase	WPA(2) Pass Phrase Confirmation
1	Open System	WEP		

Previous

Abort

Next

Description

The table contains the following columns:

- **Interface** (only in Access Point mode)
Shows the interface to which the settings relate.
- **Security Context** (in client mode only)
Shows the security context to which the settings relate.
- **Authentication Type**
Select the type of authentication.

Note

WLAN mode IEEE 802.11 n

With devices operated in WLAN mode IEEE8002.11n only WPA2 (WPA2-PSK and WPA2 Radius) encryption is possible.

- Open System
Without authentication
- **WEP**
- WPA-PSK
WPA authentication with WPA key. Enter the WPA key in ""WPA(2) Pass Phrase.
- WPA (RADIUS)
WPA authentication with RADIUS server. You configure the access data on the next Basic Wizard page.
- WPA2-PSK
WPA2 authentication with WPA2 key. Enter the WPA2 key in ""WPA(2) Pass Phrase.
- WPA2 (RADIUS)
WPA2 authentication with RADIUS server. You configure the access data on the next Basic Wizard page.
- iPCF authentication
This authentication type is shown when iPCF, iPCF-HT or iPCF-MC mode is enabled at the corresponding WLAN interface.
You can enable iPCF authentication in the "iFeatures (Page 347)" menu.
- **Cipher**
Select the encryption method.
 - AUTO
AES or TKIP is selected automatically depending on the capability of the other station.
 - TKIP (Temporal Key Integrity Protocol)
A symmetrical encryption method with the RC4 algorithm (Ron's Code 4). In contrast to the weak WEP encryption, TKIP uses changing keys derived from a main key. TKIP can also recognize corrupted data frames.
 - AES
(Advanced Encryption Standard)
Strong symmetrical block encryption method based on the Rijndael algorithm that further improves the functions of TKIP.

6.3 "Wizard" menu

- **WPA(2) Pass Phrase**
Enter a WPA(2) key. The key can be 8 to 63 ASCII characters or exactly 64 hexadecimal characters long. This WPA(2) key must be known on both the client and the access point and is entered by the user at both ends.

Note

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

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

6.3.1.11 Dot1x Supplicant Settings

Introduction

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

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

Note

This page is only available in client mode.

Basic Wizard: Dot1x Supplicant Settings

System	Country	IP	Management Interfaces	Antenna	Radio	Client	Channels	Security	Dot1x Supplicant	Summary
--------	---------	----	-----------------------	---------	-------	--------	----------	----------	------------------	---------

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

Security Context	Dot1x User Name	Dot1x User Password	Dot1x User Password Confirmation
1			

Previous

Abort

Next

Description

Table 1 contains the following columns:

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

6.3.1.12 Dot1x RADIUS Server Settings

Introduction

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

Note

This page is available only in access point mode.

Basic Wizard: Dot1x RADIUS Server Settings

System	Country	IP	Management Interfaces	Antenna	Radio	AP	Security	Dot1x RADIUS	Summary
--------	---------	----	-----------------------	---------	-------	----	----------	--------------	---------

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

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

Previous

Abort

Next

6.3 "Wizard" menu

Description

This table contains the following columns:

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

6.3.1.13 Summary

Introduction

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

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

Basic Wizard: Summary of Settings

System	Country	IP	Management Interfaces	Antenna	Radio	Client	Channels	Security	Dot1x Supplicant	Summary
--------	---------	----	-----------------------	---------	-------	--------	----------	----------	------------------	---------

Device Mode: Client

Country: Angola

System Name: sysName Not Set

IP Assignment Method: Static

IP Address: 192.168.16.107

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

Interface WLAN1: Enabled

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

Scan Channels: 1,2,3,4,5,6,7,8,9,10,11,12,13

Antenna 1: Type ANT795-4MC, Gain 3 dBi, Additional Attenuation 0 dB, Cable Length 0 m

Antenna 2: Type ANT795-4MD, Gain 3 dBi, Additional Attenuation 0 dB, Cable Length 0 m

SSID: Any SSID

MAC Mode: Automatic

Security: Open System

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

Previous

Abort

Set Values

Set Values

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

6.4 "Information" menu

6.4.1 Start Page

View of the Start page

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

General layout of the WBM pages

The following areas are generally available on every WBM page:

- Selection area (1): Top area
- Display area (2): Top area
- Navigation area (3): Left-hand area
- Content area (4): Middle area

The screenshot shows the Siemens WBM interface for a SCALANCE W761-1 RJ45 device. The interface is divided into four numbered areas:




- Area 1 (Top area):** Contains the Siemens logo and the device address `192.168.16.7/SCALANCE W761-1 RJ45` along with the date and time `08/02/2017 10:30:56`.
- Area 2 (Top area):** Contains a 'Welcome admin' message and a 'Logout' link.
- Area 3 (Left-hand area):** Contains a navigation menu with the following items: Wizards, Information, Start Page, Versions, I&M, ARP / Neighbors, Log Tables, Faults, Redundancy, Ethernet Statistics, Learning Table, IPv6 Routing, DHCP Server, SNMP, Security, WLAN, WLAN Statistics, System, Interfaces, Layer 2, and Security.
- Area 4 (Middle area):** Contains the main content area. It starts with a message 'Please select one item of the menu on the left'. Below this is a small image of the device. Further down, it displays the following information:
 - PROFINET Name of Station: [empty field]
 - Diagnostics Mode: PROFINET
 - System Name: sysName Not Set
 - Device Type: SCALANCE W761-1 RJ45
 - PROFINET AR Status: Offline
 - Power Line 1: Up
 - Fault Status: No Fault
 - Remote Capture: disabled
 - A 'Refresh' button is located at the bottom of the content area.

Selection area (1)

The following is available in the selection area:

- **Logo of Siemens AG**
When you click on the logo, you arrive at the Internet page of the corresponding basic device in Siemens Industry Online Support.
- **Display of: "System Location/System Name".**
 - "System Location" contains the location of the device.
With the settings when the device ships, the IP address of the Ethernet interface is displayed.
 - "System Name" is the device name. With the settings when the device ships, the device type is displayed.


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

- **Drop-down list for language selection**
- **System time and date**
You can change the content of this display with "System > System Time".
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:

- **Logging out**
You can log out from any WBM page by clicking the "Logout" link.
- **Device name**
Shows the name of the device.
- **Mode**
Shows whether the device is an access point or a client.
- **Help ?**
When you click this button, the help page of the currently selected menu item is opened in a new browser window.
- **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.



- **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. You can show this window during a change of menu and move it as necessary. To close the LED simulation, click the close button in the LED simulation window.
- **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 enabled on the WBM page.

Navigation area (3)

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

Content area (4)

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.
- **Diagnostics Mode**
Shows whether EtherNet/IP or PROFINET is enabled.
- **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 will find further information on this in the compact operating instructions.
- **PLUG Configuration**
Shows the status of the configuration data on the PLUG, refer to the section "System > PLUG > Configuration".
- **Fault Status**
Shows the fault status of the device.
- **Remote Capture**
Shows whether or not the function is enabled.

Buttons you require often

The pages of the WBM contain the following standard buttons:

- **Refresh the display with "Refresh"**
Web Based Management pages that display current parameters have a "Refresh" button at the lower edge of the page. Click this button to request up-to-date information from the device for the current page.

Note

If you click the "Refresh" button, before you have transferred your configuration changes to the device using the "Set Values" button, your changes will be deleted and the previous configuration will be loaded from the device and displayed here.

- **Save entries with "Set Values"**
Pages in which you can make configuration settings have a "Set Values" button at the lower edge. The button only becomes active if you change at least one value on the page. Click this button to save the configuration data you have entered on the device. Once you have saved, the button becomes inactive again.

Note

Changing configuration data is possible only with the "admin" login.

- **Create entries with "Create"**
Pages in which you can make new entries have a "Create" button at the lower edge. Click this button to create a new entry.

- **Delete entries with "Delete"**
Pages in which you can delete entries have a "Delete" button at the lower edge. Click this button to delete the previously selected entries from the device memory. Deleting also results in an update of the page in the WBM.
- **Cancel with "Cancel"**
The Basic Wizard pages have the "Cancel" button at the lower edge of the page. Click this button to close the Basic Wizard without applying the settings.
- **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 record.
- **Button "Show all"**
You can show all entries in pages with a large number of data records. 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 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.
-

6.4.2 Versions

Versions of hardware and software

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

Version Information			
Hardware	Name	Revision	Order ID
Basic Device	SCALANCE W761-1 RJ45	2	6GK5 761-1FC00-0AA0
WLAN 1	WLAN 1 Radio Card	-	-
Software	Description	Version	Date
Firmware	SCALANCE W700 Firmware	V06.03.00	06/07/2018 20:00:00
Bootloader	SCALANCE W700 Bootloader	V01.22.00	12/19/2016 21:01:00
Firmware_Running	Current running Firmware	V06.03.00	06/07/2018 20:00:00
<input type="button" value="Refresh"/>			

Description

Table 1 has the following columns:

- **Hardware**
 - Basic Device
Shows the basic device
 - WLAN1
Shows the available wireless card
- **Name**
Shows the name of the device or module.
- **Revision**
Shows the hardware version of the device. For the wireless card, only one version is then displayed if the WLAN interface is enabled.
- **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.

6.4.3 Identification & Maintenance

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.

Identification & Maintenance

Manufacturer ID: 42

Order ID: 6GK5 786-2FC00-0AA0

Serial Number: VPC3544970

Hardware Revision: 1

Software Revision: V06.01.00

Revision Counter: 0

Revision Date: 00/00/0 00:00:00

Function Tag:

Location Tag:

Date:

Descriptor:

Description of the displayed values

The table has the following rows:

- **Manufacturer ID**
Shows the manufacturer ID.
- **Article number**
Shows the article number.
- **Serial Number**
Shows the serial number.
- **Hardware Revision**
Shows the hardware version.
- **Software Revision**
Shows the software version.
- **Revision Counter**
As of firmware version 4.0, the value "0" is always shown here regardless of the version change.
- **Revision Date**
Date of the revision: Date and time of the last revision
- **Function tag**
Shows the function tag (plant designation) of the device. The plant designation (HID) is created during configuration of the device with HW Config of STEP 7.
- **Location tag**
Shows the location tag 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 during configuration of the device with HW Config of STEP 7.
- **Descriptor**
Shows the description created during configuration of the device with HW Config of STEP 7.

6.4.4 ARP / neighbors

6.4.4.1 ARP Table

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.

Address Resolution Protocol (ARP) Table			
ARP Table		IPv6 Neighbor Table	
Interface	MAC Address	IP Address	Media Type
vlan1	68-05-ca-36-39-0d	192.168.16.20	Dynamic
vlan1	68-05-ca-25-e8-62	192.168.16.55	Dynamic
2 entries.			
<input type="button" value="Refresh"/>			

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.

6.4.4.2 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.

Address Resolution Protocol (ARP) Table			
Interface	MAC Address	IP Address	Media Type
vlan1	00-13-ce-63-59-bf	192.168.0.97	Dynamic
vlan1	6c-62-6d-6f-38-31	192.168.0.100	Dynamic
2 entries.			
<input type="button" value="Refresh"/>			

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.

6.4.5 Log Tables

6.4.5.1 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.

Log Table

Event Log
WLAN Authentication Log

Severity Filters
☐ Info
☐ Warning
☐ Critical

Restart	System Up Time	System Time	Severity	Log Message
5	00:31:26	Date/time not set	6 - Info	Device configuration changed
5	00:25:47	Date/time not set	6 - Info	Device configuration changed
5	00:23:56	Date/time not set	2 - Critical	Error by reconfiguration of Wlan Config Daemon.
5	00:16:05	Date/time not set	6 - Info	Device configuration changed
5	00:00:14	Date/time not set	6 - Info	Spanning Tree: topology change detected.
5	00:00:11	Date/time not set	6 - Info	Link up on P2.
5	00:00:09	Date/time not set	2 - Critical	Error by reconfiguration of Wlan Config Daemon.
5	00:00:09	Date/time not set	6 - Info	Link down on P1.
5	00:00:00	Date/time not set	6 - Info	Cold start performed, Ver: T01.00.00.00_20.01.01 - event/status summary after startup:
5	00:00:00	Date/time not set	6 - Info	Startup configuration: Internal storage PLUG: Not present

1 - 10 of 62 entries [Show all](#)
1 [Next](#)

Clear

Refresh

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

For each severity, a maximum of 400 entries in the table are possible. 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 date and time when the described event occurred.

- **Severity**

Shows the severity of the message.

- **Log Message**

Displays a brief description of the event that has occurred. You will find the list of possible messages in Appendix D (Page 373) of the configuration manual.

If the system time is set, the time is also displayed at which the event occurred.

6.4.5.2 WLAN authentication log

Logging authentication attempts

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

WLAN Authentication Log

Event Log

WLAN Authentication Log

Severity Filters

☐ Info

☐ Warning

☐ Critical

Restart

System Up Time

System Time

Severity

Log Message

0 entries.

Clear

Refresh

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
For each severity, a maximum of 400 entries in the table are possible. 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 date and time when the described event occurred.
- **Severity**
Shows the severity of the message.
- **Log Message**
Displays a brief description of the event that has occurred. You will find the list of possible messages in Appendix D (Page 373) of the configuration manual.

If the system time is set, the time is also displayed at which the event occurred.

6.4.6 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.

Faults

No. of Signaled Faults: 1

[Reset Counters](#)

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

[Refresh](#)

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.

6.4.7 Redundancy

Introduction

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

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

Spanning Tree

Spanning Tree Mode: MSTP

Instance ID: 0

Bridge Priority: 32768

Bridge Address: 00-1b-1b-a5-5d-98

Root Priority: 32768

Root Address: 00-1b-1b-a5-5d-98

Root Cost: 0

Bridge Status: This bridge is the root

Regional Root Priority: 32768

Regional Root Address: 00-1b-1b-a5-5d-98

Regional Root Cost: 0

Refresh

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

Spanning Tree

Spanning Tree Mode: MSTP

Instance ID: 0

Bridge Priority: 32768

Bridge Address: 00-af-fe-af-fe-00

Root Priority: 32768

Root Address: 00-1b-1b-40-91-23

Root Cost: 240000

Regional Root Priority: 32768

Regional Root Address: 00-af-fe-af-fe-00

Regional Root Cost: 0

Port	Role	State	Oper. Version	Priority	Path Cost	Edge Type	P.t.P. Type
P1	Root	Forwarding	MSTP	128	200000	No Edge Port	P.t.P

Refresh

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.

6.4.8 Ethernet Statistics

6.4.8.1 Interface Statistics

Interface statistics

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

Ethernet Statistics: Interface Statistics							
Interface Statistics	Packet Size	Packet Type	Packet Error				
	In Octet	Out Octet	In Unicast	In Non-Unicast	Out Unicast	Out Non-Unicast	In Errors
P1	711533	1677547	3753	717	4214	297	0
<input type="button" value="Reset Counter"/>							
<input type="button" value="Refresh"/>							

Displayed values

The table has the following columns:

- **In Octet**
Shows the number of received bytes.
- **Out Octet**
Shows the number of sent bytes.
- **In Unicast**
Shows the number of received unicast frames.
- **In Non Unicast**
Shows the number of received frames that are not of the type unicast.
- **Out Unicast**
Shows the number of sent unicast frames.
- **Out Non Unicast**
Shows the number of sent frames that are not of the type unicast.
- **In Errors**
Shows the number of all possible RX errors, refer to the "Packet Error" tab.

6.4.8.2 Packet Size

Frames sorted by length

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

Ethernet Statistics: Packet Size						
Interface	Statistics	Packet Size	Packet Type	Packet Error		
Port	64	65-127	128-255	256-511	512-1023	1024-max
P1	6941	1474	1467	2230	19	0
Reset Counter						
Refresh						

Description

The table has the following columns:

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

6.4.8.3 Frame Type

Received frames sorted by type

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

Ethernet Statistics: Packet Type			
Interface Statistics	Packet Size	Packet Type	Packet Error
Port	Unicast	Multicast	Broadcast
P1	9378	2052	16
Reset Counter			
Refresh			

Description

The table has the following columns:

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

6.4.8.4 Packet Error

Bad received frames

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

Ethernet Statistics: Packet Error						
Interface Statistics	Packet Size	Packet Type	Packet Error			
Port	CRC	Undersize	Oversize	Fragments	Jabbers	Collisions
P1	0	0	0	0	0	0
Reset Counter						
Refresh						

Description

The table has the following columns:

- **Port**
Shows the available ports.
- **Error types**
The other columns after the port number contain the absolute numbers of the incoming frames according to their error type.
In the columns of the table, a distinction is made according to the following error types:
 - CRC (Cyclic Redundancy Code)
The packet length is between 64 and 1518 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 length is more than 1518 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 1518 bytes. The CRC of the packet is invalid.
 - Collisions
Frames in which a collision event was detected.

6.4.9 Learning Table

Address filtering

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

Learning Table			
VLAN ID	MAC Address	Status	Port
1	00-1b-1b-40-91-23	Learnt	P1
1	00-1b-1b-a5-5d-98	Learnt	P1
1	00-1b-1b-c7-f5-a2	Learnt	P1
1	00-1b-1b-c8-70-3b	Learnt	P1
1	08-00-06-70-56-00	Learnt	P1
1	68-05-ca-19-40-bb	Learnt	P1
1	68-05-ca-36-39-0d	Learnt	P1
1	94-b8-c5-41-b3-5d	Learnt	P1

8 entries.

Description

This table contains the following columns:

- **VLAN ID**

Shows the VLAN ID of the node.

Note

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

- **MAC Address**

Shows the MAC address of the node.

- **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.

6.4.10 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".

Link Layer Discovery Protocol (LLDP) Neighbors

System Name	Device ID	Local Interface	Hold Time[s]	Capability	Port ID
sysName Not Set	08:00:06:70:29:d7	P1	20	Bridge	port-008

[Refresh](#)

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.

6.4.11 IPv6 routing

Introduction

This page shows the IPv6 routes currently being used.

Layer 3: IPv6 Routing Table					
Destination Network	Prefix Length	Gateway	Interface	Metric	Routing Protocol
2002:C0A8:1296::	48	::	vlan1	1	connected
1 entry.					
<input type="button" value="Refresh"/>					

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

6.4.12 DHCP-Server

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

DHCP Server Bindings						
IP Address	Pool ID	Identification Method	Identification Value	Allocation Method	Binding State	Expire Time
192.168.16.90	1	Client ID	08-EC74BA03FED2	dynamic	assigned	01/01/2000 05:21:03
1 entry.						
<button>Refresh</button>						

Description

- **IP Address**
Shows the IPv4 address assigned to the DHCP client.
- **Pool ID**
Shows the number of the IPv4 address band.

- **Identification Method**
Shows the method according to which the DHCP client is identified.
- **Identification value**
Shows the MAC address or the client ID of the DHCP client.
- **Allocation Method**
Shows whether the IPv4 address was assigned statically or dynamically. You configure the static entries in "System > DHCP > Static Leases".
- **Binding State**
Shows the status of the assignment.
 - Assigned
The assignment is used.
 - Not used
The assignment is not used.
 - Probing
The assignment is being checked.
 - Unknown
The status of the assignment is unknown.
- **Expire Time**
Shows until when the assigned IPv4 address is still valid. Up to this time, the DHCP client must either request a new IPv4 address or extend the lease time of the assigned IPv4 address.

6.4.13 SNMP

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

Simple Network Management Protocol v3 (SNMPv3) Groups Overview	
Group Name	User Name
Service	Mueller
Wartung	Peterson
Refresh	

Description

The table has the following columns:

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

6.4.14 Security

6.4.14.1 Overview

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

Security Overview

OverviewSupported Function RightsRolesGroupsInter AP Blocking

Services

Telnet Server: enabled

SSH Server: enabled

Web Server: HTTP/HTTPS

SNMP: SNMPv1/v2c/v3

Management ACL: disabled: no access restriction

Login Authentication: Local

Password Policy: low

Local User Accounts

User Account	Role
admin	admin

External User Accounts

User Account	Role
admin	admin

Refresh

Description

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.

- **Web Server**

You configure the setting in "System > Configuration".

- HTTP/HTTPS: Access to the WBM is possible with HTTP and HTTPS.
- HTTPS: Access to the WBM is now only possible with 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.

- **Management ACL**

You configure the setting in "Security > Management ACL".

- Disabled: no access restriction
The access control is disabled.
- Enabled: no access restriction
The access control is enabled but no access rules have been defined.
- Enabled: restricted access only
The access control is enabled and access rules have been defined.

- **Login Authentication**

You configure the setting in "Security > AAA > General".

- Local
Login with local user name and password.
- RADIUS
Login using a RADIUS server.
- Local and RADIUS
The login is possible both with the users that exist in the firmware (user name and password) and via a RADIUS server. The local users have priority.

Note

The user is first searched for in the local database. If the user does not exist there or the password does not match, a RADIUS query is sent.

- **Password Policy**

Shows which password policy is currently being used.

The "Local User Accounts" table has the following columns:

- **User Accounts**
Shows the name for the user.
- **Role**
Shows the role of the user.
 - admin
The user can create, edit or delete entries.
 - user
The user only has read rights.

You configure local user accounts in "Security > Users".

6.4.14.2 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.

Supported Function Rights

Overview	Supported Function Rights	Roles	Groups	802.1X Port Status	MAC Authentication
Function Right	Description				
1	Read-only access to configuration data.				
15	Read/write access to configuration data.				

Refresh

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.

6.4.14.3 Roles

Note

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

The page shows the roles valid locally on the device.

User Roles

Overview	Supported Function Rights	Roles	Groups	802.1X Port Status	MAC Authentication	
Role	Function Right	Description				
user	1	System defined role, with readonly access to configuration data of this component.				
admin	15	System defined role, with read/write access to configuration data of this component.				
default	1	Internal role, for authenticated users without group/role mapping in this component.				
everybody	0	Internal role, assigned to users when authentication failes. Access will be denied.				
<div>Refresh</div>						

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.

6.4.14.4 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.

User Groups

Overview	Supported Function Rights	Roles	Groups	802.1X Port Status	MAC Authentication	
----------	---------------------------	-------	--------	--------------------	--------------------	--

Group	Role	Description
Grp1	user	Admin Group

Refresh

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.

6.4.15 WLAN

6.4.15.1 Overview AP

Overview of the configuration

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

Note

This tab is available only in access point mode.

Overview AP

Overview APClient ListWDS ListOverlap APForce RoamingNoise Floor

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

Radio	Port	MAC Address	SSID	Security	Status
WLAN 1	VAP 1.1	00-1b-1b-c7-f5-a5	Siemens Wireless Network	Open System	enabled

Refresh

Description

Table 1 has the following columns:

- **Radio**
Shows the available WLAN interfaces.
- **Port**
Shows the available VAP interfaces.
- **WLAN Mode**
Shows the transmission standard. If DFS is activated, the transmission standard "802.11h" is not shown additionally but only the configured transmission standard "802.11a".
- **Configured Channel**
Shows the configured channel. If "Auto" is displayed, the access point searches for a free channel itself.
- **Alternative DFS Channel**
If the DFS function is enabled, the configured alternative channel of the access point is displayed.
If "Auto" is displayed, the access point searches for an alternative channel itself.
If the DFS function is activated and the access point browses for primary users for 60 seconds before starting communication with the selected channel, the text "scanning ..." is displayed instead of the channel.
- **Operational channel**
Shows the channel of the access point via which the access point communicates.
- **HT Channel Width [MHz]**
Shows the channel bandwidth.
 - 20
Channel bandwidth 20 MHz
 - 40 up
Channel bandwidth 40 MHz. The configured channel and the neighboring channel above it are used.
 - 40 down
Channel bandwidth 40 MHz. The configured channel and the neighboring channel below it are used.

Note

Channel bandwidth 40 MHz and frequency band 2.4 GHz

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

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

Table 2 has the following columns:

- **Radio**
Shows the available WLAN interfaces in this column.
- **Port**
Shows the port of the virtual access point.
- **MAC Address**
Shows the MAC address of the virtual access point.
- **SSID**
Shows the SSID.
- **Security**
 - If the authentication method "Open System + Encryption" or "Shared Key" is used, the "Encrypted (WEP/AES)" is displayed for both authentication methods.
 - Only with client SCALANCE W722-1 RJ45: If iPCF, iPCF-HT or iPCF-MC mode is enabled, the following is displayed depending on the encryption status:
iPCF Encrypted (AES): Encryption is enabled.
iPCF authentication: Encryption is disabled.
- **State**
Shows the status of the WLAN interface.
 - enabled
The WLAN interface is enabled.
 - disabled
The WLAN interface is disabled.

6.4.15.2 Client List

Logged-on clients

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

Note

This WBM page is only available in access point mode.

WLAN Clients

Overview APClient ListWDS ListOverlap APForce RoamingNoise Floor

Associated stations: 1

AID	Radio	Port	Type	MAC Address	System Name	Channel	Signal Strength [dBm]	Signal Strength [%]	Age [s]	Security	WLAN Mode	Max. Data Rate [Mbps]	State
1	WLAN 1	VAP 1.2	Station	00-1b-1b-c7-f5-a2	Client	36	-41	100	0	WPA2-PSK	-	-	-

Refresh

Description

- Logged-on clients**

Shows the number of clients logged on to the access point.

The table has the following columns:

- AID (Associated ID)**

Shows the connection ID of the client. If the client connects to the access point via the VAP interface, the client is assigned a connection ID. The connection ID is unique within a VAP interface. If two clients log on at different VAP interfaces, both clients can receive the same ID.

- Radio**

Shows the available WLAN interfaces.

- Port**

Shows the VAP interface.

- Type**

Shows the client type, for example "Sta" stands for IEEE 802.11 standard client.

- MAC Address**

Shows the MAC address of the client.

- System Name**

Shows the system name of the client if the client communicates this to the access point. Not all clients support this parameter.

- Channel**

Shows the channel over which the client communicates with the access point.

- Signal Strength [dBm]**

Shows the signal strength of the connected client in 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.
 - If the authentication method "Open System + Encryption" or "Shared Key" is used, the "Encrypted (WEP/AES)" is displayed for both authentication methods.
 - If iPCF, iPCF-HT or iPCF-MC mode is enabled on a WLAN interface, the following is displayed depending on the encryption status:
iPCF Encrypted (AES): Encryption is enabled.
iPCF authentication: Encryption is disabled.
- **WLAN Mode**
Shows the transmission standard. If DFS is activated, the transmission standard "802.11h" is not shown additionally but only the configured transmission standard "802.11a".
- **Max. Data Rate (Mbps)**
Shows the maximum data transmission speed in megabits per second.
- **State**
Shows the current status of the connection, for example connected means that the client is connected to the access point and is ready to communicate with the AP.

6.4.15.3 WDS List

Communication between access points





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

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

Note

This WBM page is only available in access point mode.

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

WDS List										Access Point
										   
Overview AP	Client List	WDS List	Overlap AP							
Radio	Port	BSSID	WDS ID	Channel	Signal Strength [dBm]	Signal Strength [%]	Security	Max. Data Rate [Mbps]	State	
WLAN 1	WDS 1.1	00-1b-1b-38-81-88	DIMA_WDS_PARTNER	7	-69	51	Open System	195.0	connected	
<input type="button" value="Refresh"/>										

Description

The table has the following columns:

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

6.4.15.4 Overlap AP

Overlapping channels

Note

This WBM page is only available in access point mode.

For optimum data throughput, it is important that the set wireless channel is not used by other access points. In the 2.4 GHz band (802.11b or 802.11g), there is overlapping of the channels so that an access point occupies not only the set channel but also the two or three adjacent channels. You should therefore make sure that there is adequate channel spacing to neighboring access points. For the 5 GHz band, ensure that you use the correct channel planning and do not inadvertently use the same channels.

This WBM page shows all access points that are visible on the set or adjacent channels (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. The displayed channel is read out from the beacon of the respective access point which is operated on the same channel as the SCALANCE W device.

Overlap APs List

Overview AP

Client List

WDS List

Overlap AP

Force Roaming

Radio

Aging Time [min]

WLAN 1

120

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

Set Values

Refresh

Description

Table 1 has the following columns:

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

Note

Changing the aging time

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

The table has the following columns:

- **Radio**
Shows the available WLAN interfaces in this column.
- **Type**
Shows the mode of the WLAN interface.
- **SSID**
Shows the SSID of the access point.
- **BSSID**
Shows the MAC address of the access point.
- **System Name**
Shows the system name of the SCALANCE W700-Geräts. The entry depends on the access point. Not all access points support this parameter.
- **Channel**
Shows the channel over which the client communicates with the access point.
- **Signal Strength [dBm]**
Shows the signal strength of the access point in dBm.

- **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.
 - If the authentication method "Open System + Encryption" or "Shared Key" is used, the "Encrypted (WEP/AES)" is displayed for both authentication methods.
 - If iPCF, iPCF-HT or iPCF-MC mode is enabled on the WLAN interface, the following is displayed depending on the encryption status:
iPCF Encrypted (AES): Encryption is enabled.
iPCF authentication: Encryption is disabled.
- **WLAN Mode**
Shows the transmission standard. If DFS is activated, the transmission standard "802.11h" is not shown additionally but only the configured transmission standard "802.11a" or "802.11n".

6.4.15.5 Force Roaming

Force Roaming		
Overview AP	Client List	WDS List
Overlap AP	Force Roaming	
Port	Destination Address / Status	Force Roaming on IP down
VAP 1.1	not configured	inactive
VAP 1.2	not configured	inactive
VAP 1.3	not configured	inactive
VAP 1.4	not configured	inactive
VAP 1.5	not configured	inactive
VAP 1.6	not configured	inactive
VAP 1.7	not configured	inactive
VAP 1.8	192.168.100.1 / idle	inactive
Refresh		

In client mode:

Force Roaming		
Overview Client	Available AP	IP Mapping
Force Roaming	Noise Floor	
Port	Destination Address / Status	Force Roaming on IP down
WLAN 1	192.111.20.20 / down	active
Refresh		

This WBM page shows the current status of the connection. It also shows whether there is roaming.

The device monitors the connection to certain addresses cyclically. To achieve this, the device sends echo messages (pings) to the configured destination addresses at regular intervals.

Description

The table has the following columns:

- **Port**
Shows the available interfaces.
 - VAP X.Y (in access point mode)
 - WLAN O/X (in client mode)
- **Destination Address / State**
Shows which destination address is monitored and the status of the connection. You configure the destination address in "Interfaces > WLAN > Force Roaming".
 - not configured: No destination address is configured.
 - idle: The configuration is incomplete.
 - up: The destination address is reachable.
 - down: The destination address is unreachable.
- **Force Roaming on IP down**
Indicates whether roaming is currently being performed.
 - Inactive: No roaming is being performed. No change to the WLAN interface.
 - Active: None of the destination addresses is reachable. To force the logged on clients / connected access points to roam, the device has disabled the corresponding interface.

6.4.15.6 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.

Übersicht Client

Übersicht ClientVerfügbare APsIP-ZuordnungRoaming erzwingenHintergrundrauschen

Funkschnittstelle	WLAN-Modus	MAC-Modus	MAC-Adresse	Operativer Kanal	HT-Kanal-Bandbreite [MHz]
WLAN 1	802.11n (2.4 GHz)	Layer-2-Tunnel	00-1b-1b-38-5c-90	-	-

Aktualisieren

Verbundene BSSID	Verbundene SSID	Security	Kontext	iFeatures	Max. Datenrate [Mbps]	Status
-	-	-	-	IPCF	-	disabled

Description

- **Radio**
Shows the available WLAN interfaces in this column.
- **WLAN Mode**
Shows the transmission standard.
- **MAC Mode**
Shows how the MAC address is assigned to the interface.
 - Automatic
The client automatically adopts the source MAC address of the first frame that it receives over the Ethernet interface.
 - Manual
The address was entered manually.
 - Own
The client uses the MAC address of the Ethernet interface for the WLAN interface.
 - Layer 2 Tunnel
The client uses the MAC address of the Ethernet interface for the WLAN interface. The network is also informed of the MAC addresses connected to the Ethernet interface of the client. Up to 4 MAC addresses can be used.

6.4 "Information" menu

- **MAC Address**
Shows the MAC address of the WLAN interface.
- **Operational channel**
Shows the channel of the access point with which the client is connected.
- **HT Channel Width [MHz]**
Shows the channel bandwidth.
 - 20
Channel bandwidth 20 MHz
 - 40 up
Channel bandwidth 40 MHz. The configured channel and the neighboring channel above it are used.
 - 40 down
Channel bandwidth 40 MHz. The configured channel and the neighboring channel below it are used.

Note

Channel bandwidth 40 MHz and frequency band 2.4 GHz

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

- **Connected BSSID**
Shows the MAC address of the access point with which the client is connected.
- **Connected SSID**
Shows the SSID of the access point with which the client is connected.
- **Security**
Shows which authentication method is used.
 - If the authentication method "Open System + Encryption" or "Shared Key" is used, the "Encrypted (WEP/AES)" is displayed for both authentication methods.
 - If iPCF, iPCF-HT or iPCF-MC mode is enabled on a WLAN interface, the following is displayed depending on the encryption status:
iPCF Encrypted (AES): Encryption is enabled.
iPCF authentication: Encryption is disabled.
- **Context**
Shows which security context is used.
- **iFeatures**
Shows which iFeatures are used.
 - -
iFeatures are not used.
 - iPCF
 - iPCF-HT
 - iPCF-MC
 - iPRP

- **Max. Data Rate [Mbps]**
Shows the maximum transmission rate of the interface.
- **State**
Shows the status of the WLAN interface.
 - enabled
The WLAN interface is enabled.
 - disabled
The WLAN interface is disabled.

6.4.15.7 Available AP

Available access points

Note

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

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

Note

Display when iPCF mode is activated

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

Available APs List										
Overview	Client	Available AP		IP Mapping	Force Roaming	Noise Floor				
Radio	SSID	BSSID	System Name	Channel	Signal Strength [dBm]	Signal Strength [%]	Type	Security	WLAN Mode	State
Refresh										

Description

The table has the following columns:

- **Radio**
Shows the WLAN interface visible to the access point.
- **SSID**
Shows the SSID of the access point.
- **BSSID**
Shows the MAC address of the access point.

- **System Name**
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.
 - If the authentication method "Open System + Encryption" or "Shared Key" is used, the "Encrypted (WEP/AES)" is displayed for both authentication methods.
 - If iPCF, iPCF-HT or iPCF-MC mode is enabled on a WLAN interface, the following is displayed depending on the encryption status:
iPCF Encrypted (AES): Encryption is enabled.
iPCF authentication: Encryption is disabled.
- **WLAN Mode**
Shows the transmission standard. If DFS is activated, the transmission standard "802.11h" is not shown additionally but only the configured transmission standard "802.11a" or "802.11n".
- **State**
Shows the status of the access point, for example whether or not the access point is available.

6.4.15.8 IP Mapping

WLAN access by several devices over a client

Note

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

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

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

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

MAC address/IPv4 address assignment

The client maintains a table with the assignment of MAC address and IPv4 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.

IP Mapping Table

Client

Overview

Client

Available AP

IP Mapping

MAC Address	IP Address	Type
8c-16-45-75-7f-a7	192.168.40.10	learned
00-1b-1b-a6-0c-10	192.168.40.46	learned
20-87-56-0a-01-48	192.168.40.50	system
00-1b-1b-98-1f-88	192.168.40.56	learned
00-1b-1b-98-1f-88	192.168.40.57	learned
20-87-56-ca-98-20	192.168.40.100	learned

6 entries.

Refresh

MAC mode

IP 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 are further devices downstream from the client, the "Automatic" option should not be enabled. In this case, the MAC address would be assigned indiscriminately to the first device that signals over Ethernet. If there is only IP communication between the access point and the client, the default setting "Own" can be retained. If MAC address-based frames are also to be sent by devices downstream from the client, you need to select the settings "Manual", "Automatic" or "Layer 2 Tunnel".

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.

6.4.15.9 Background noise

Note

This WBM page is only available in access point mode.

Noise Floor

Overview AP	Client List	WDS List	Overlap AP	Force Roaming	Noise Floor
Connector	Channel [dBm]	Extended Channel [dBm]			
R1 A1	-	-			
R1 A2	-	-			
R1 A3	-	-			
R2 A1	-	-			
R2 A2	-	-			
R2 A3	-	-			

Refresh

The page displays the background noise of the channel.

Description

- **Connector**
Shows the name of the relevant antenna connector.
- **Channel [dBm]**
Shows the background noise of the set channel.
- **Extended Channel [dBm]**
Shows the background noise of the extended channel (HT-40).

6.4.15.10 Funkschnittstellen-Info

Note

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

WLAN Radio Information

Overview Client

Available AP

IP Mapping

Force Roaming

Radio Information

Noise Floor

Connector	Channel [dBm]	Extended Channel [dBm]
R1 A1	-	-
R1 A2	-	-
R1 A3	-	-

Antenna Information

Radio	SSID	BSSID	Signal Strength R1 A1 [dBm]	Signal Strength R1 A2 [dBm]	Signal Strength R1 A3 [dBm]	DTAS
WLAN1	AP_Station_1	00-0e-8f-en-4b-98	-80	-	-	R1A1
WLAN1	AP_Station_2	00-1b-1c-19-03-05	-85	-95	-	R1A1
WLAN1	AP_Station_3	1a-2b-3c-4d-5e-6f	-96	-	-	R1A2

Refresh

The page contains information on background noise of the channel and antenna.

Description

The "Background noise" table contains the following columns:

- Connector
Shows the name of the relevant antenna connector.
- Channel [dBm]
Shows the background noise of the set channel.
- Extended Channel [dBm]
Shows the background noise of the extended channel (HT-40).

The "Antenna information" table contains the following columns:

- Radio interface
Shows the available WLAN interfaces.
- SSID
Shows the network name of the access point.
- BSSID
Shows the MAC address of the access point.
- Signal strength R1Ax
Shows the signal strength in dBm for each antenna.
- DTAS
Shows which transmitting antenna is being used.

6.4.16 WLAN Statistics

6.4.16.1 Errors

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

WLAN Errors Statistic

Errors	Management Sent	Management Received	Data Sent	Data Received
--------	-----------------	---------------------	-----------	---------------

Sent Errors

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

Received Errors

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

Reset Counter

Refresh

Description

The Sent Errors table has the following columns:

- **Interface**
Shows the WLAN interface to which the entries apply.
- **Error types**
The other columns after the WLAN interface contain the absolute numbers of the frames sent according to their error type.
The columns of the table distinguish the following error types:
 - Transmission Errors
Shows the number and percentage of bad frames that were sent.
 - Dropped Frames
Shows the number and percentage of frames that were discarded.
Despite all the retries, the frame could not be successfully sent.
The frame has not yet been sent and the recipient has logged off in the meantime.
 - Send Retries
Shows the number and percentage of frames sent successfully that required one or more retries.

The Receive Errors table has the following columns:

- **Interface**
Shows the WLAN interface to which the entries apply.
- **Error types**
The other columns after the WLAN interface contain the absolute numbers of the frames received according to their error type.
The columns of the table distinguish the following error types:
 - Receive errors
Shows only the number and percentage of bad frames that were received during the existing connection.
 - Duplicated Frames
Shows the number and percentage of frames that were received twice.
 - Decryption Errors
Shows the number and percentage of incorrectly encrypted frames.
 - FCS Errors
Shows the number and percentage of frames in which the checksum was incorrect.
 - Total receive errors
Shows the number and percentage of all bad frames that were received in total.

6.4.16.2 Management Sent

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

Note

This WBM page is only available in access point mode.

WLAN Management Traffic Sent Statistics							
Errors	Management Sent	Management Received	Data Sent	Data Received			
Interface	Management Frames	Association Requests	Association Responses	Disassociation Requests	Authentication Requests	Authentication Responses	Deauthentication Requests
VAP 1.1	0	0	0	0	0	0	0
VAP 1.2	0	0	0	0	0	0	0
VAP 1.3	0	0	0	0	0	0	0
VAP 1.4	0	0	0	0	0	0	0

Description

The table has the following columns:

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

6.4.16.3 Management Received

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

WLAN Management Traffic Received Statistics								
Errors	Management Sent	Management Received	Data Sent	Data Received				
Interface	Management Frames	Association Requests	Association Responses	Disassociation Requests	Authentication Requests	Authentication Responses	Deauthentication Requests	
VAP 1.1	0	0	0	0	0	0	0	
VAP 1.2	0	0	0	0	0	0	0	
VAP 1.3	0	0	0	0	0	0	0	
VAP 1.4	0	0	0	0	0	0	0	

Reset Counter

Refresh

Description

The table has the following columns:

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

6.4.16.4 Data Sent

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

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

Reset Counter

Refresh

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 Data Rate
Shows the average data rate of the last data frames sent.

6.4.16.5 Data Received

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

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

Reset Counter

Refresh

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 Data Rate
Shows the average data rate of the last data frames sent.

6.4.17 WLAN iFeatures

6.4.17.1 iPRP

On this WBM page you can check whether the settings for iPRP are correct. You can, for example, check whether the iPRP function is enabled on the partner device, see who the partner device is.

Note

This WBM page is only available on the client SCALANCE W722-1 RJ-45 (MLFB 6GK5722-1FC00-0AA0 / 6GK5722-1FC00-0AB0 (US version))

iPRP Information								
iPRP								
Radio	iPRP Client	Activity State	Partner Client	Partner BSS	Delete Frames Sent	Delete Frames Received	Frames Deleted	Scanning Sync. State
WLAN 1	00-1b-1b-a5-2c-d8	active	00-1b-1b-8e-61-31	00-1b-1b-19-03-10	25424	19956	4817	idle
<input type="button" value="Refresh"/>								

Description

The table has the following columns:

- **Radio**
Shows the WLAN interfaces via which the client is connected to the access point
- **iPRP Client**
Shows the MAC address of the iPRP client.
- **Activity status**
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 iPRP delete frames that the device (access point / client) has sent to its partner device.
- **Delete Frames Received**
Shows the number of iPRP delete frames that the device (access point / client) 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**
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: Idling No scanning
 - requested: Query to the partner client whether scanning is possible.
 - pending: Scanning is possible. Waits for the start of scanning 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.

6.5 "System" menu

6.5.1 Configuration

System configuration

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

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

System Configuration

☒ Telnet Server

Telnet Port:

☒ SSH Server

SSH Port:

☒ HTTP Server

HTTP Port:

☒ HTTPS Server

HTTPS Port:

HTTP Services:

Minimum TLS Version:

☒ DNS Client

☐ SMTP Client

☐ Syslog Client

DCP Server:

Time:

SNMP:

☐ SNMPv1/v2 Read-Only

☐ SNMPv1 Traps

☐ DHCP Client

☒ DHCPv6 Client

☒ SINEMA Configuration Interface

Configuration Mode:

Description

The page contains the following boxes:

- **Telnet Server**
Enable or disable the "Telnet Server" service for unencrypted access to the CLI.
- **Telnet Port**
Specify the port for Telnet access to the CLI.
- **SSH Server**
Enable or disable the "SSH Server" service for encrypted access to the CLI.

- **SSH Port**
Specify the port for SSH access to the CLI
- **HTTP Server**
Enable or disable HTTP access to the WBM.
- **HTTP Port**
Specify the port for HTTP access to the WBM.
- **HTTPS Server**
Enable or disable HTTPS access to the WBM.
- **HTTPS Port**
Enable or disable access using HTTPS.
- **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**
Specify the minimum TLS version to be used.
- **DNS Client**
Enable or disable the DNS client. You can configure other settings in "System > DNS".
- **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.

6.5 "System" menu

- **Time**
Select the setting from the drop-down list. The following settings are possible:
 - **Manual**
The system time is set manually. You can configure other settings in "System > System Time > Manual Setting".
 - **SIMATIC Time**
The system time is set using a SIMATIC time transmitter. You can configure other settings in "System > System Time > SIMATIC Time Client".
 - **SNTP Client**
The system time is set via an SNTP server. You can configure other settings in "System > System Time > SNTP Client".
 - **NTP Client**
The system time is set via an NTP server. You can configure other settings in "System > System Time > NTP Client".
- **SNMP**
Select the protocol from the drop-down list. The following settings are possible:
 - **"-" (SNMP disabled)**
Access to device parameters via SNMP is not possible.
 - **SNMPv1/v2c/v3**
Access to device parameters is possible with SNMP versions 1, 2c or 3. You can configure other settings in "System > SNMP > General".
 - **SNMPv3**
Access to device parameters is possible only with SNMP version 3. You can configure other settings in "System > SNMP > General".
- **SNMPv1/v2 Read-Only**
Enable or disable write access to SNMP variables with SNMPv1/v2c.
- **SNMPv1 Traps**
Enable or disable the sending of traps (alarm frames). You can configure other settings in "System > SNMP > Traps".
- **DHCP Client**
Enable or disable the DHCP client. You can configure other settings in "System > DHCP".
- **DHCPv6 Client**
Enable or disable the DHCPv6 client.

- **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 immediately.

Note

Interrupting the save

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

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

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

- **Trial**

Trial mode. In Trial mode, although changes are adopted, they are not saved in the configuration file (startup configuration).

To save changes in the configuration file, use the "Write startup config" button. The "Write startup config" button is displayed when you set trial mode. In addition to this after every parameter change the following message is displayed in the display area: "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.

Procedure

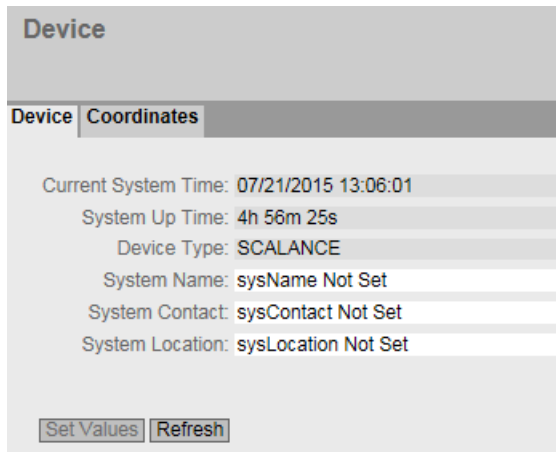
1. To use the required function, select the corresponding check box.
2. Select the options you require from the drop-down lists.
3. Click the "Set Values" button.

6.5.2 General

6.5.2.1 Device

General device information

This page contains the general device information.



The screenshot shows a web interface titled "Device". Below the title is a tabbed interface with two tabs: "Device" (selected) and "Coordinates". The "Device" tab contains the following information:

- Current System Time: 07/21/2015 13:06:01
- System Up Time: 4h 56m 25s
- Device Type: SCALANCE
- System Name: sysName Not Set
- System Contact: sysContact Not Set
- System Location: sysLocation Not Set

At the bottom of the form are two buttons: "Set Values" and "Refresh".

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.

6.5.2.2 Coordinates**Information on geographic coordinates**

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

Getting the coordinates

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

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

The screenshot shows a web form titled "Geographic Coordinates". It has a header bar with "Device" and "Coordinates" tabs. Below the tabs are three input fields: "Latitude: e.g. DD°MM'SS'", "Longitude: e.g. DDD°MM'SS'", and "Height: e.g. dddd m". At the bottom of the form are two buttons: "Set Values" and "Refresh".

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 $+49^{\circ} 1' 31.67''$ 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 ($49^{\circ} 1' 31.67''$ 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 $+8^{\circ} 20' 58.73''$ 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 ($8^{\circ} 20' 58.73''$ 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.

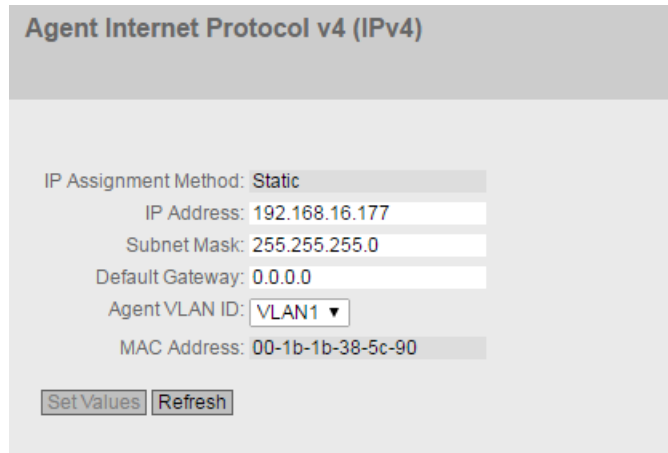
Procedure

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.

6.5.3 Agent IPv4

Configuration of the IP addresses

On this WBM page, you configure the IPv4 address for the device.



Agent Internet Protocol v4 (IPv4)

IP Assignment Method: **Static**

IP Address: **192.168.16.177**

Subnet Mask: **255.255.255.0**

Default Gateway: **0.0.0.0**

Agent VLAN ID: **VLAN1** ▼

MAC Address: **00-1b-1b-38-5c-90**

Set Values **Refresh**

Description

The page contains the following boxes:

- **IP Assgn. Method**
 - Shows how the IPv4 address is assigned.
 - **Static**
The IPv4 address is static. You enter the IP settings in the input boxes "IP Address" and "Subnet Mask".
 - **Dynamic (DHCP)**
The device obtains a dynamic IPv4 address from a DHCP server.
- **IP Address**
Enter the IPv4 address of the device.
After clicking the "Set Values" button, this IPv4 address is also displayed in the address bar of the Web browser. If this does not take place automatically, you will need to enter the IPv4 address in the address bar of the Web browser manually.
- **Subnet Mask**
Enter the subnet mask of the device.
- **Default Gateway**
Enter the IPv4 address of the default gateway to be able to communicate with devices in another subnet, for example diagnostics stations, e-mail server.

6.5 "System" menu

- **Agent VLAN ID**

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

Note

Changing the Agent VLAN ID

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

- **MAC Address**

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

Procedure

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

6.5.4 Agent IPv6

Configuration of the IP addresses

On this page, enable IPv6 on the management VLAN. This VLAN interface is also called an IPv6 interface. An IPv6 interface can have several IPv6 addresses.

Agent Internet Protocol v6 (IPv6)

Agent IPv6

IPv6 Default Routes

Interface:

vlan1

☒ IPv6 Enable

IPv6 Address:

Prefix Length:

IPv6 Address Type:

Unicast

Address Configuration:

Automatic

☐ DHCPv6 Rapid Commit

Select	Interface Name	IPv6 Address	Prefix Length	IPv6 Address Type	Loopback
<input type="checkbox"/>	vlan1	FE80::21B:1BFF:FE38:5C90	64	Link Local	

1 entry.

Create

Delete

Set Values

Refresh

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 entry 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:

- Automatic (default)
The IPv6 address is created using a stateless mechanism or a stateful mechanism.
- DHCPv6
Status dependent: Obtains the IPv6 address and the configuration file from the DHCPv6 server.
- SLAAC (Stateless Address Auto Configuration)
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
- **Loopback**
Shows whether or not the "loopback" property is enabled.

Procedure

Forming a link local address automatically

1. Enable IPv6.
2. Click the "Create" button. In the table an entry with the interface is created and the automatically formed link local IPv6 address is displayed.

Assigning 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 local address is overwritten.

6.5.4.1 IPv6 default routes

On this page, you configure the default IPv6 routes.

Internet Protocol v6 (IPv6) Default Routes

Agent IPv6 IPv6 Default Routes

Destination Network:
Prefix Length:
Gateway:
Metric:
Interface:

Select	Destination Network	Prefix Length	Gateway	Interface	Metric	Status
<input type="checkbox"/>	2222.4::2222	96	2222.4::2223	vlan1	1	active

1 entry.

Create Delete Set Values Refresh

Description

The page contains the following:

- **Destination Network**
Enter the network address of the destination that can be reached via this route.
- **Prefix Length**
Enter the number of left-hand bits belonging to the prefix
- **Gateway**
Enter the IPv4 address of the gateway via which this network address is reachable.
- **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.

6.5 "System" menu

- **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 network address of the destination.
2. Enter the prefix length.
3. Enter the IPv6 address of the gateway.
4. Select the required interface.
5. Enter the metric of the route.
6. Click the "Create" button. A new entry is generated in the table.
7. Click the "Set Values" button.

6.5.5 DNS

On this page, you can manually configure up to 3 DNS servers with IPv4 or IPv6 addresses. Manually configured DNS servers are each assigned an index from 1 to 3. Using DHCP, the device can learn 2 DNS servers with IPv4 addresses. An index from 4 to 7 is automatically assigned to learned DNS servers.

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 7 DNS servers can be configured on the device. Manually configured DNS servers are given preference.

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

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

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

Domain Name System (DNS) Client

☒ DNS Client

Used DNS Servers: all

DNS Server Address:

Select	DNS Server Address	Origin
<input type="checkbox"/>	192.1.1.1	manual

1 entry.

Create Delete Set Values Refresh

Description

The page contains the following boxes:

- DNS client**
 If the check box is enabled, the "DNS client" function is enabled.
- 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 three 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 for the DNS servers with 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.

6.5 "System" menu

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.

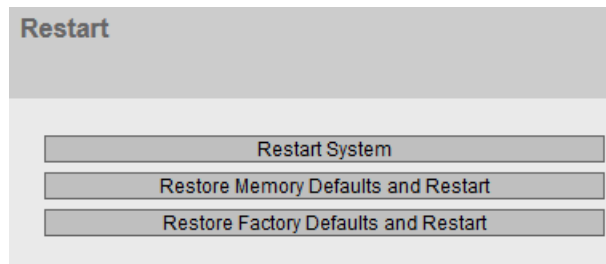
Deleting a DNS server

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

6.5.6 Restart

Resetting to the defaults

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



Note

Note the following points about restarting a device:

- You can only restart the device with administrator privileges.
 - A device should only be restarted with the buttons of this menu or with the appropriate CLI commands and not by a power cycle on the device.
 - Any modifications you have made only become active on the device after clicking the "Set values" button on the relevant WBM page. If the device is in "Trial" mode, configuration modifications must be saved manually before a restart. In "Automatic Save" mode, the last changes are saved automatically before a restart.
-

Description

To restart the device manually, 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 learned entries in the address table are deleted. You can leave the browser window open while the device restarts. You then need to log in again.
- **Restore Memory Defaults and Restart**
Click this button to restore the factory configuration settings with the exception of the following parameters and to restart:
 - IP addresses
 - Subnet mask
 - IP address of the default gateway.
 - DHCP client ID
 - DHCP
 - System name
 - System location
 - System contact
 - User names and passwords
 - Mode of the device
 - DHCPv6 Rapid Commit
- **Restore Factory Defaults and Restart**
Click this button to restore the factory defaults for the configuration. The protected defaults are also reset.
An automatic restart is triggered.

Note

By resetting all the defaults to the factory configuration settings, the IP address is also lost. The device can then only be addressed via SINEC PNI or via DHCP.

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

6.5.7 Commit Control

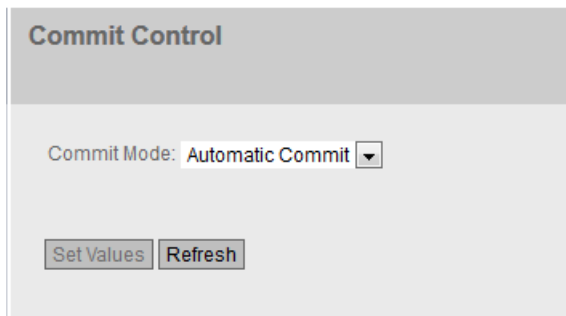
Change management

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.

6.5.8 Load & Save

6.5.8.1 File list

Note

The files that can be loaded from the device depends on the role of the logged-on.

Overview of the file types

Table 6-1 HTTP

File type	Description	Down-load	Save	Delete
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 "Users" file.	X	X	--
ConfigPack	Detailed configuration information. for example, start configuration, users, certificates, favorites, firm-ware of the device (if saved as well). For more detailed information on creating and using the ConfigPack incl. firmware, refer to the section "Maintenance (Page 355)".	X	X	--
CountryList	The zip file contains the country list as a csv and as a pdf file.	--	X	--
Debug	This file contains information for Siemens Support. It is encrypted and can be sent by e-mail to Siemens Support without any security risk.	--	X	X
EDS	Electronic Data Sheet (EDS) Electronic data sheets for describing devices in the EtherNet/IP mode. You can find EDS files on the download page for the firmware at Siemens Industry Online Support.	--	--	--
Firmware	The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be down-loaded to the device.	X	X	--
GSDML	Information on the device properties (PROFINET) You can find GSDML files on the download page for the firmware at Siemens Industry Online Support.	--	--	--

6.5 "System" menu

File type	Description	Down-load	Save	Delete
HTTPS Cert	<p>Default HTTPS certificates including key</p> <p>The preset and automatically created HTTPS certificates are self-signed.</p> <p>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 certificate authority. The HTTPS certificate checks the identity of the device and controls the encrypted data exchange.</p> <p>The following file types can be loaded into the device:</p> <ul style="list-style-type: none"> • .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 successfully load a certificate with this file type into the device, configure the password specified for the certificate on the WBM page "System > Load & Save > Passwords". <p>Certificates with a different format cannot be imported.</p> <p>Maximum file size: 8192 bits</p>	X	X	X
LogFile	File with entries from the event log table	--	X	--
LoginWelcomeMessage	The txt file contains the desired text or the ASCII type. Only pure text files in ASCII format are supported.	X	X	X
MIB	Private MSPS MIB file "Scalance_w_msps.mib"	--	X	--
RunningCLI	<p>Text file with CLI commands</p> <p>This file contains an overview of the current configuration in the form of CLI commands. Passwords are masked in this file as follows: [PASSWORD]</p> <p>You can download the text file. The file is not intended to be uploaded again unchanged.</p>	--	X	--
RunningSINEMAConfig	<p>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 installed on a device with the same article number and firmware version.</p> <p>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 STEP7 Basic/Professional.</p> <p>See also "SINEMAConfig"</p>	--	X	--

File type	Description	Down-load	Save	Delete
Script	Text file with CLI commands You can upload a script file in a device. The CLI commands it contains are executed accordingly. CLI commands for saving and loading files cannot be executed with the CLI script file.	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 "SINEMAConfig" under "System > Load&Save > Passwords". You also need this password to export the file from STEP 7 Basic/Professional. See also "RunningSINEMAConfig"	X	--	--
StartupInfo	Startup log file This file contains the messages that were entered in the log file during the last startup.	--	X	--
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
WLANAuth-log	File with entries from the WLAN Authentication Log (information on successful or failed authentication attempts)	--	X	--
WLANSpectrumAnalyzer (Only in access point mode)	The Zip file contains a csv file with the measured values of the spectrum analyzer. You will find information about the measured values and their graphic representation in the section "Spectrum analyzer (Page 270)".	--	X	X
WLANCert (in client mode only)	User certificate. You can specify a password for the user certificate on the WBM page "Load&Save > Password". Maximum file size: 8192 bits	X	X	X
WLANServ-Cert (in client mode only)	Server certificate Maximum file size: 8192 bits	X	X	X
WLANSigRec (in client mode only)	The zip file contains the following: <ul style="list-style-type: none"> 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 260)".	--	X	X

Table 6-2 TFTP/SFTP

File type	Description	Save	Down-load	
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 "Users" file.	X	X	
ConfigPack	Detailed configuration information. for example, start configuration, users, certificates, firmware of the device (if saved as well). For more detailed information on creating and using the ConfigPack incl. firmware, refer to the section "Maintenance (Page 355)".	X	X	
CountryList	The zip file contains the country list as a csv and as a pdf file.	X	--	
Debug	This file contains information for Siemens Support. It is encrypted and can be sent by e-mail to Siemens Support without any security risk.	X	--	
EDS	Electronic Data Sheet (EDS) Electronic data sheets for describing devices in the EtherNet/IP mode You can find EDS files on the download page for the firmware at Siemens Industry Online Support.	--	--	
Firmware	The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be downloaded to the device.	X	X	
GSDML	Information on the device properties (PROFINET) You can find GSDML files on the download page for the firmware at Siemens Industry Online Support.	--	--	

File type	Description	Save	Down-load	
HTTPS Cert	<p>Default HTTPS certificates including key</p> <p>The preset and automatically created HTTPS certificates are self-signed.</p> <p>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 certificate authority. The HTTPS certificate checks the identity of the device and controls the encrypted data exchange.</p> <p>The following file types can be loaded into the device:</p> <ul style="list-style-type: none"> • .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 successfully load a certificate with this file type into the device, configure the password specified for the certificate on the WBM page "System > Load & Save > Passwords". <p>Certificates with a different format cannot be imported.</p> <p>Maximum file size: 8192 bits</p>	X	X	
LogFile	File with entries from the event log table	X	--	
LoginWelcome-Message	The txt file contains the desired text or the ASCII type. Only pure text files in ASCII format are supported.	X	X	
MIB	Private MSPS MIB file "Scalance_w_msp.mib"	X	--	
RunningCLI	<p>Text file with CLI commands</p> <p>This file contains an overview of the current configuration in the form of CLI commands. Passwords are masked in this file as follows: [PASSWORD]</p> <p>You can download the text file. The file is not intended to be uploaded again unchanged.</p>	X	--	

6.5 "System" menu

File type	Description	Save	Down-load	
RunningSINE-MAConfig	You save the current device configuration in this file type for transfer to STEP7 Basic/Professional. The file can be imported in STEP 7 Basic/Professional and installed 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/Professional; see also "SINEMAConfig".	--	X	
Script	Text file with CLI commands You can upload a script file in a device. The CLI commands it contains are executed accordingly. CLI commands for saving and loading files cannot be executed with the CLI script file.	--	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 "SINEMAConfig" under "System > Load&Save > Passwords". You also need this password to export the file from STEP 7 Basic/Professional; see also "RunningSINEMAConfig".	X	--	
StartupInfo	Startup log file This file contains the messages that were entered in the log file during the last startup.	X	--	
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	
WLANAthlog	File with entries from the WLAN Authentication Log (information on successful or failed authentication attempts)	X	--	
WLANSpectrumAnalyzer (Only in access point mode)	The Zip file contains a csv file with the measured values of the spectrum analyzer. You will find information about the measured values and their graphic representation in the section "Spectrum analyzer (Page 270)".	--	X	X
WLANCert (in client mode only)	User certificate. You can specify a password for the user certificate on the WBM page "Load&Save > Password". Maximum file size: 8192 bits	X	X	

File type	Description	Save	Down-load	
WLANServer-Cert (in client mode only)	Server certificate Maximum file size: 8192 bits	X	X	
WLANSigRec (in client mode only)	<p>The zip file contains the following:</p> <ul style="list-style-type: none"> • 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. <p>You will find information about the measured values and their graphic representation in the section "Signal recorder (Page 260)".</p>	X	--	

6.5.8.2 HTTP

Loading and saving data via HTTP

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

Note

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

Firmware

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

Note

Incompatibility with predecessor versions

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

Configuration files

Note

Configuration files and trial mode/Automatic Save mode

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

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

CLI script file

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

Note

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

Load and Save via HTTP				
HTTP	TFTP	SFTP	Passwords	
Type	Description	Load	Save	Delete
Config	Startup Configuration	Load	Save	
ConfigPack	Startup Config, Users, Certificates and WBM favourites	Load	Save	
CountryList	WLAN Country List		Save	
Debug	Debug Information for Siemens Support		Save	Delete
EDS	EtherNet/IP Device Description		Save	
Firmware	Firmware Update	Load	Save	
GSDML	PROFINET Device Description		Save	
HTTPSCert	HTTPS Certificate	Load	Save	Delete
LogFile	Event Log (ASCII)		Save	
LoginWelcomeMessage	Login Welcome Message	Load	Save	Delete
MIB	SCALANCE W MSPS MIB		Save	
RunningCLI	'show running-config all' CLI settings		Save	
RunningSINEMAConfig	SINEMA Running Configuration		Save	
Script	Script	Load		
SINEMAConfig	SINEMA Offline Configuration	Load		
StartupInfo	Startup Information		Save	
Users	Users and Passwords	Load	Save	
WBMFav	WBM favourite pages	Load	Save	Delete
WLANAuthLog	Authentication Log (ASCII)		Save	
WLANCert	WLAN User Certificate	Load	Save	Delete
WLANServCert	WLAN Server Certificate	Load	Save	Delete
WLANSigRec	Signal Recorder		Save	Delete
Refresh				

Example of a device in client mode

Figure 6-1 Example of a device in client mode

Description

The table has the following columns:

- **Type**
Shows the designation 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 upload files to the device. The button can be enabled, if this function is supported by the file type.

6.5 "System" menu

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

Note

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

Procedure

Loading files using HTTP

1. Start the load function by clicking 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 active and executed immediately, for example the CLI script file.

1. After loading, restart the device. The changes only take effect a restart.

Saving files using HTTP

1. Start the save function by clicking 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 files using HTTP

1. Start the delete function by clicking one of the "Delete" buttons.
The file will be deleted.

Reusing configuration data

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

Follow the steps below to reuse configuration data:

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

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

6.5.8.3 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.

Firmware

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

Note

Incompatibility with predecessor versions

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

Configuration files

Note

Configuration files and trial mode/Automatic Save mode

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

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

CLI script file

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

Note

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

6.5 "System" menu

Load and Save via TFTP

HTTP | TFTP | SFTP | Passwords

TFTP Server Address: 0.0.0.0

TFTP Server Port: 69

Type	Description	Filename	Actions
Config	Startup Configuration	config_SCALANCE_W700.conf	Select action
ConfigPack	Startup Config, Users, Certificates and WBM favourites	configpack_SCALANCE_W700.zip	Select action
CountryList	WLAN Country List	countrylist_SCALANCE_W700.zip	Select action
Debug	Debug Information for Siemens Support	debug_SCALANCE_W700.bin	Select action
EDS	EtherNet/IP Device Description	eds_SCALANCE_W700.zip	Select action
Firmware	Firmware Update	firmware_SCALANCE_W700.sfw	Select action
GSDML	PROFINET Device Description	gsdml_SCALANCE_W700.zip	Select action
HTTPSCert	HTTPS Certificate	https_cert	Select action
LogFile	Event Log (ASCII)	logfile_SCALANCE_W700.csv	Select action
LoginWelcomeMessage	Login Welcome Message	login_welcome_message.txt	Select action
MIB	SCALANCE W MSPS MIB	scalance_w_mspms.mib	Select action
RunningCLI	'show running-config all' CLI settings	RunningCLI.txt	Select action
RunningSINEMAConfig	SINEMA Running Configuration	sinema_config_running.zip	Select action
Script	Script	Script.txt	Select action
SINEMAConfig	SINEMA Offline Configuration	sinema_config.zip	Select action
StartupInfo	Startup Information	startup_SCALANCE_W700.log	Select action
Users	Users and Passwords	users.enc	Select action
WBM Fav	WBM favourite pages	wbmfav.txt	Select action
WLANAuthLog	Authentication Log (ASCII)	wlan_auth_log_SCALANCE_W700.csv	Select action
WLANCert	WLAN User Certificate	wlan_user_cert	Select action
WLANServCert	WLAN Server Certificate	wlan_serv_cert	Select action
WLANSigRec	Signal Recorder	signal_recorder_SCALANCE_W700.zip	Select action

Set Values

Refresh

Example of a device in client mode

Figure 6-2 Example of a device in client mode

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.

The 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.

- **File name**
Enter a file name.
- **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 "TFTP Server Port" input box.
3. Enter the name of a file where 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.

6.5.8.4 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.

6.5 "System" menu

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

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

Firmware

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

Configuration files

Note

Configuration files and Trial mode /Automatic Save

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

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

CLI script file

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

Note

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

Load and Save via SFTP

HTTP TFTP SFTP Passwords

SFTP Server Address: 0.0.0.0

SFTP Server Port: 22

SFTP User:

SFTP Password:

SFTP Password Confirmation:

Type	Description	Filename	Actions
Config	Startup Configuration	config_SCALANCE_W700.conf	Select action
ConfigPack	Startup Config, Users, Certificates and WBM favourites	configpack_SCALANCE_W700.zip	Select action
CountryList	WLAN Country List	countrylist_SCALANCE_W700.zip	Select action
Debug	Debug Information for Siemens Support	debug_SCALANCE_W700.bin	Select action
EDS	EtherNet/IP Device Description	eds_SCALANCE_W700.zip	Select action
Firmware	Firmware Update	firmware_SCALANCE_W700.sfw	Save file
GSDML	PROFINET Device Description	gsdml_SCALANCE_W700.zip	Select action
HTTPSCert	HTTPS Certificate	https_cert	Select action
LogFile	Event Log (ASCII)	logfile_SCALANCE_W700.csv	Select action
LoginWelcomeMessage	Login Welcome Message	login_welcome_message.txt	Select action
MIB	SCALANCE W MSPS MIB	scalance_w_mspms.mib	Select action
RunningCLI	'show running-config all' CLI settings	RunningCLI.txt	Select action
RunningSINEMAConfig	SINEMA Running Configuration	sinema_config_running.zip	Select action
Script	Script	Script.txt	Select action
SINEMAConfig	SINEMA Offline Configuration	sinema_config.zip	Select action
StartupInfo	Startup Information	startup_SCALANCE_W700.log	Select action
Users	Users and Passwords	users.enc	Select action
WBM Fav	WBM favourite pages	wbmfav.txt	Select action
WLANAuthLog	Authentication Log (ASCII)	wlan_auth_log_SCALANCE_W700.csv	Select action
WLANCert	WLAN User Certificate	wlan_user_cert	Select action
WLANServCert	WLAN Server Certificate	wlan_serv_cert	Select action
WLANSigRec	Signal Recorder	signal_recorder_SCALANCE_W700.zip	Select action

Set Values Refresh

Example of a device in client mode

Description

The page contains the following boxes:

- **SFTP Server Address**
Enter the IP address or the FQDN of the SFTP server with which you exchange data.
- **SFTP Server Port**
Enter the port of the SFTP server via which data exchange will be handled. If necessary, you can change the default value 22 to your own requirements.
- **SFTP User**
Enter the user for access to the SFTP server. This assumes that a user with the corresponding rights has been created on the SFTP server.
- **SFTP Password**
Enter the password for the user
- **SFTP Password Confirmation**
Confirm the password.

The table has the following columns:

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

Note**Changing the file name**

You can change the file name preset in this column. After 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 change the data, you can no longer upload it to the IE switch.

6.5.8.5 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.

Note

User and server certificate in one file

If the user and the server certificate are located in the same file, load this file on the device as the user certificate and as the server certificate.

Passwords

HTTP
TFTP
SFTP
Passwords

Type	Description	Setting	Password	Password Confirmation	Status
HTTPSCert	HTTPS Certificate	<input type="checkbox"/>			-
RunningSINEMAConfig	SINEMA Running Configuration	<input type="checkbox"/>			Required
SINEMAConfig	SINEMA Offline Configuration	<input type="checkbox"/>			Required
WLANCert	WLAN User Certificate	<input type="checkbox"/>			-
WLANServCert	WLAN Server Certificate	<input type="checkbox"/>			-

Set Values
Refresh

Description

The table has the following columns:

- **Type**
Shows the file type.
 - **Description**
Shows a brief description of the file.
 - **Setting**
Can only be enabled if a password is configured.
When enabled, a check is made during loading to ensure that the password matches the password set for the file.
 - **Password**
Enter the password set for the file.
-

Note

When assigning the password, you can only use the following readable ASCII characters:
0x20 - 0x7e.

- **Password Confirmation**
Confirm the password.
- **Status**
 - "-"
No password is specified or the password is enabled but no file is loaded yet.
 - Valid
The password is used and matches the file.
 - Invalid
The password is used, but the password does not match the file.
 - 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.

6.5.9 Events

6.5.9.1 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.

Event Configuration

Configuration
Severity Filters

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

Event	E-mail	Trap	Log Table	Syslog	Fault
Cold/Warm Start	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Link Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Authentication Failure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Power Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Spanning Tree Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Fault State Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Overlap AP Detection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
WDS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
DFS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
WLAN General	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Configuration Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Service Information	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	

Set Values
Refresh

Description

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

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

Table 2 has the following columns:

- **Event**

The column contains the following values:

- Cold/Warm Start
The device was turned on or restarted by the user.
- Link Change
This event occurs only when the port status is monitored and has changed, see "System > Fault Monitoring > Link Change".
- Authentication error
This event occurs when attempting access with a bad password.
- Power Change
This event occurs only when power supply line 1 is monitored. It indicates that there was a change to line 1, see "System > Fault Monitoring > Power Supply".
- Spanning Tree Change
The STP or RSTP or MSTP topology has changed.
- Fault State Change
The fault status has changed. The fault status can relate to the activated port monitoring, the response of the signaling contact or the power supply monitoring.
- Overlap AP Detection (Only in access point mode)
This event is triggered when there is an entry in the overlap AP list.
- WDS (Only in access point mode)
The connection status of a WDS link has changed.
- DFS (Only in access point mode)
This event occurs if a radar signal was received or the DFS scan was started or stopped.
- WLAN Authentication Log
Forwarding of the entries from the WLAN authentication log to the system protocol server.
- WLAN General (Only in access point mode)
This event occurs if a the channel bandwidth has changed.
- WLAN De/Authentication (Only in client mode)
With successful or failed WLAN authentication attempts.
- iPCF Poll size (available only with client SCALANCE W722-1)
This event occurs if the PROFINET data size is too large for transfer.
- 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.

- **E-Mail**

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

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

Procedure

Follow the steps below to change entries:

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

6.5.9.2 Severity

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

Event Severity Filters	
Configuration Severity Filters	
Client Type	Severity
E-mail	Info ▼
Log Table	Info ▼
Syslog	Info ▼
WLAN Authentication Log	Info ▼

Set Values Refresh

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.

6.5.10 SMTP Client

Network monitoring with e-mails

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

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

Simple Mail Transfer Protocol (SMTP) Client

☐ SMTP Client

Sender Email Address:

SMTP Port:

SMTP Server Address:

Select	SMTP Server Address	Receiver Email Address
<input type="checkbox"/>	192.168.16.20	service@scalance

1 entry.

Description

The page contains the following boxes:

- SMTP Client**
Enable or disable the SMTP client.
- Sender Email Address**
Enter the name of the sender to be included in the e-mail, for example the device name.
This setting applies to all configured SMTP servers.
- Send Test Mail**
Send a test e-mail to check your configuration.
- SMTP Port**
Enter the port via which your SMTP server can be reached.
Factory settings: 25
This setting applies to all configured SMTP servers.
- SMTP Server Address**
Enter the IP address, the FQDN (Fully Qualified Domain Name) or the host name of the SMTP server.

The table contains the following columns:

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

Procedure

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

Note

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

6.5.11 DHCPv4

6.5.11.1 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.

Dynamic Host Configuration Protocol (DHCP) Client

DHCP Client

DHCP Server

DHCP Options

Static Leases

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

DHCP Mode:

via MAC Address

Interface	DHCP
vlan1	<input type="checkbox"/>
vlan2	<input type="checkbox"/>

Set Values

Refresh

Description

The page contains the following boxes:

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

6.5.11.2 DHCP Server

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

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

Note

Maximum number of IP addresses

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

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

Dynamic Host Configuration Protocol (DHCP) Server

DHCP Client

DHCP Server

Port Range

DHCP Options

Relay Agent Information

Static Leases

☐ DHCP Server

☐ Probe address with ICMP Echo before offer

Select	Pool ID	Interface	Enable	Subnet	Lower IP Address	Upper IP Address	Lease Time [sec]
<input type="checkbox"/>	1	vlan1	<input type="checkbox"/>	0.0.0.0/0	0.0.0.0	0.0.0.0	3600

1 entry.

Create

Delete

Set Values

Refresh

Requirements for the DHCP server

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

Description

The page contains the following boxes:

- **DHCP Server**

Enable or disable the DHCP server on the device.

Note

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

- **Probe address with ICMP Echo before offer**

When selected, the DHCP server checks whether or not the IP address has already been assigned. To do this the DHCP server sends ICMP echo messages (ping) to the IPv4 address. If no reply is received, the DHCP server can assign the IPv4 address.

Note

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

The table has the following columns:

- **Select**

Select the check box in the row to be deleted.

- **Pool ID**

Shows the number of the IPv4 address band. If you click the "Create" button, a new row with a unique number is created (pool ID).

Note

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

- **Interface**

Specify the interface via which the IPv4 addresses are dynamically assigned.

The requirement for the assignment is that the IPv4 address of the interface is located within the IPv4 address band. If this is not the case, the interface does not assign any IPv4 addresses.

- **Enable**

Specify whether or not this IPv4 address band will be used.

Note

If you enable the IPv4 address band, the settings in this and the other DHCP tabs are grayed out and can no longer be edited.

- **Subnet**

Enter the network address range that will be assigned to the devices. Use the CIDR notation.

- **Lower IP address**

Enter the IPv4 address that specifies the start of the dynamic IPv4 address band. The IPv4 address must be within the network address range you configured for "Subnet".

6.5 "System" menu

- **Upper IP address**
Enter the IPv4 address that specifies the end of the dynamic IPv4 address band. The IPv4 address must be within the network address range you configured for "Subnet".
- **Lease Time (sec)**
Specify for how many seconds the assigned IPv4 address remains valid. When half the lease time 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.

6.5.11.3 DHCP Options

Note
This tab is available only on the access point SCALANCE W761-1 RJ45 and the client SCALANCE W722-1 RJ45.

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

Dynamic Host Configuration Protocol (DHCP) Options

DHCP Client

DHCP Server

DHCP Options

Static Leases

Pool ID: 1 ▼

Option Code:

Select	Pool ID	Option Code	Use Interface IP	Value
	1	1		255.255.255.255
<input type="checkbox"/>	1	3	<input checked="" type="checkbox"/>	192.168.16.178
<input type="checkbox"/>	1	6		0.0.0.0
<input type="checkbox"/>	1	12		
<input type="checkbox"/>	1	66		
<input type="checkbox"/>	1	67		Bootfile name not set

6 entries.

Create

Delete

Set Values

Refresh

Description

The page contains the following boxes:

- **Pool ID**
Select the required IPv4 address band.
- **Option Code**
Enter the number of the required DHCP option. A maximum of 20 DHCP options are possible. The various DHCP options are defined in RFC 2132. The DHCP options 1, 3, 6, 66 and 67 are created automatically when the IPv4 address band is created. With the exception of option 1, the options can be deleted.
With the DHCP option 3, the internal IPv4 address of the device is automatically set as a DHCP parameter

Note

DHCP options not supported

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

The table has the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Pool ID**
Shows the number of the IPv4 address band.
- **Option Code**
Shows the number of the DHCP option.
- **Use Interface IP**
Specify whether or not the internal IPv4 address of the device will be used.
- **Value**
Enter the DHCP parameter that is transferred to the DHCP client. The content depends on the DHCP option.
 - DHCP option 67 (boot file name)
Enter the name of the boot file in the string format.
 - DHCP options 3 (Router) and 6 (DNS):
Enter the DHCP parameter as an IPv4 address, e.g. 192.168.100.2. With DHCP option 6, you can specify several IPv4 addresses separated by commas.
 - DHCP option 12 (host name):
Enter the host name in the string format.
 - DHCP option 66 (TFTP Server):
Enter the DHCP parameter as an IPv4 address, e.g. 192.168.100.2 or the FQDN name. You can specify several IPv4 addresses separated by commas.
 - All other DHCP options
Enter the DHCP parameter in hexadecimal, e.g. the IPv4 address 192.168.100.2 corresponds to "C0A86402".

6.5.11.4 Static Leases

Note

This tab is available only on the access point SCALANCE W761-1 RJ45 and the client SCALANCE W722-1 RJ45.

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

Static Leases

DHCP Client

DHCP Server

Port Range

DHCP Options

Relay Agent Information

Static Leases

Pool ID: 1

Client Identification Method: Client ID

Value:

Select	Pool ID	Identification Method	Value	IP Address
<input type="checkbox"/>	2	Client ID	65756767	0.0.0.0

1 entry.

Create

Delete

Set Values

Refresh

Description

The page contains the following boxes:

- Pool ID**
From the drop-down list, select the required IPv4 address band.
- Hardware Type**
Select the method according to which a client is identified.
 - Ethernet MAC
The client is identified by its MAC address.
 - Client ID
The client is identified by a freely defined DHCP client ID. The client ID can be up to a maximum of 254 characters long.
- Value**
Enter the MAC address or the client ID and click the "Create" button to create the entry.

Note

A maximum of 20 entries are possible.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted.
 - **Pool ID**
Shows the number of the IPv4 address band.
-
- Note**
- Only Pool ID = 1 is supported.
-
- **Hardware Type**
Shows whether the client is identified by its MAC address or the client ID.
 - **Value**
Shows the MAC address to which the IPv4 address is assigned.
 - **IP Address**
Specify the IPv4 address. The IPv4 address must match the subnet of the IPv4 address band.
 - **Comment**
Enter a description for the address assignment. The maximum is 32 characters.

Procedure

Creating static leases

1. Select a Pool ID.
2. Select the Client identification method.
3. Enter the value.
4. Click the "Create" button.
5. Specify the IPv4 address that will be assigned to the client.
6. Click the "Set Values" button.

Deleting static leases

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

6.5.12 SNMP

6.5.12.1 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.

The screenshot shows the 'Simple Network Management Protocol (SNMP) General' configuration page. It features a tabbed interface with 'General', 'Traps', 'v3 Groups', and 'v3 Users' tabs. The 'General' tab is active. The configuration includes a dropdown for 'SNMP' set to 'SNMPv1v2c/v3', a checkbox for 'SNMPv1v2c Read Only' (unchecked), text fields for 'SNMPv1v2c Read Community String' (public) and 'SNMPv1v2c Read/Write Community String' (private), a checkbox for 'SNMPv1 Traps' (unchecked), a text field for 'SNMPv1v2c Trap Community String' (public), a checkbox for 'SNMPv3 User Migration' (checked), a text field for 'SNMP Engine ID' (80.00.10.e9.05.20.87.56.95.dc.f8), and a text field for 'SNMP Agent Listen Port' (161). At the bottom are 'Set Values' and 'Refresh' buttons.

SNMP	SNMPv1v2c/v3
SNMPv1v2c Read Only	<input type="checkbox"/>
SNMPv1v2c Read Community String	public
SNMPv1v2c Read/Write Community String	private
SNMPv1 Traps	<input type="checkbox"/>
SNMPv1v2c Trap Community String	public
SNMPv3 User Migration	<input checked="" type="checkbox"/>
SNMP Engine ID	80.00.10.e9.05.20.87.56.95.dc.f8
SNMP Agent Listen Port	161

Set Values Refresh

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.

- **SNMPv1 Traps**

Enable or disable the sending of SNMPv1 traps (alarm frames). On the "Trap" tab, specify the IP addresses of the devices to which SNMPv1 traps will be sent.

- **SNMPv1/v2c Trap Community String**

Enter the community string for sending SNMPv1/v2c messages.

6.5 "System" menu

- **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.

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.

6.5.12.2 Traps

SNMP traps for alarm events

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

Note

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

Simple Network Management Protocol (SNMP) v1 Traps

General Traps v3 Groups v3 Users

Trap Receiver Address:

Select	Trap Receiver Address	Trap
<input type="checkbox"/>	192.168.16.107	<input checked="" type="checkbox"/>
<input type="checkbox"/>	192.168.16.19	<input type="checkbox"/>

2 entries.

Description

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

The table has the following columns:

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

Procedure

Creating a trap entry

1. In "Trap Receiver Address", enter the IP address or the FQDN of the station to which the device will send traps.
2. Click the "Create" button to create a new trap entry.
3. Select the check box in the required row "Trap".
4. Click the "Set Values" button.

Deleting a trap entry

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

6.5.12.3 v3 Groups

Security settings and assigning permissions

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

Simple Network Management Protocol (SNMP) v3 Groups

General

Traps

v3 Groups

v3 Users

Group Name:

Security Level:

no Auth/no Priv

Select	Group Name	Security Level	Read	Write	Persistence
<input type="checkbox"/>	Service	no Auth/no Priv	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	yes
<input type="checkbox"/>	Wartung	no Auth/no Priv	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	yes

2 entries.

Create

Delete

Set Values

Refresh

Description

The page contains the following boxes:

- Group Name**
Enter the name of the group. The maximum length is 32 characters.
- Security Level**
Select the security level (authentication, encryption) valid for the selected group. The available options are as follows:
 - No Auth/no Priv
No authentication enabled/no encryption enabled.
 - Auth/no Priv
Authentication enabled/no encryption enabled.
 - Auth/Priv
Authentication enabled/encryption enabled.

The table has the following columns:

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

- **Write**
Enable or disable write access for the required group.

Note

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

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

Procedure

Creating a new group

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

Modifying a group

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

Note

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

Deleting a group

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

6.5.12.4 v3 Users

User-specific security settings

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

Simple Network Management Protocol (SNMP) v3 Users

General

Traps

v3 Groups

v3 Users

User Name:

Select	User Name	Group Name	Authentication Protocol	Privacy Protocol
<input type="checkbox"/>	Miller	Service	MD5	DES

1 entry.

Create

Delete

Set Values

Refresh

SNMPv3 Users - first part of the table

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

SNMPv3 Users - second part of the table

Description

The page contains the following boxes:

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

The table has the following columns:

- Select**
Select the row you want to delete.
- User Name**
Shows the created users.

- **Group Name**
Select the group which will be assigned to the user.
- **Authentication Protocol**
Specify the authentication protocol for which a password will be stored.
The following settings are available:
 - None
 - MD5
 - SHA
- **Encryption Protocol**
Specify whether or not a password should be stored for encryption with the DES algorithm.
Can only be enabled when an authentication protocol has been selected.
- **Authentication Password**
Enter the authentication password in the first input box. This password must have at least 1 character, the maximum length is 32 characters.

Note**Length of the password**

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

- **Authentication Password Confirmation**
Confirm the password by repeating the entry.
- **Privacy Password**
Enter your encryption password. This password must have at least 1 character, the maximum length is 32 characters.

Note**Length of the password**

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

- **Privacy Password Confirmation**
Confirm the encryption password by repeating the entry.
- **Persistence**
Shows whether or not the user is assigned to an SNMPv3 group. If the user is not assigned to an SNMPv3 group, no automatic saving is triggered and the configured user is deleted after restarting the device.
 - Yes
The user is assigned to an SNMPv3 group.
 - No
The user is not assigned to an SNMPv3 group.

Procedure

Create a new user

1. Enter the name of the new user in the "User Name" input box.
2. Click the "Create" button. A new entry is generated in the table.
3. In "Group Name", select the group to which the new user will belong.
If the group has not yet been created, change to the "v3 Groups" page and make the settings for this group.
4. If an authentication is necessary for the selected group, select the authentication algorithm in "Authentication Protocol".
In the relevant input boxes, enter the authentication password and its confirmation.
5. If encryption was specified for the group, select the algorithm in "Privacy Protocol". In the relevant input boxes, enter the encryption password and the confirmation.
6. Click the "Set Values" button.

Delete user

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

6.5.13 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.

6.5.13.1 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".

The screenshot shows the 'Manual System Time Setting' web interface. At the top, there is a title bar 'Manual System Time Setting' and a navigation bar with tabs: 'Manual Setting', 'DST Overview', 'DST Configuration', 'SNTP Client', 'NTP Client', and 'SIMATIC Time Client'. The 'Manual Setting' tab is active. Below the tabs, there is a checkbox labeled 'Time Manually' which is checked. Below this, the 'System Time' is displayed as '08/26/2019 10:59:16'. There is a button labeled 'Use PC Time'. Below the button, the 'Last Synchronization Time' is displayed as '08/26/2019 09:28:29'. Below that, the 'Last Synchronization Mechanism' is displayed as 'Manual'. Below that, the 'Daylight Saving Time' is displayed as 'inactive (offset + 0h)'. At the bottom, there are two buttons: 'Set Values' and 'Refresh'.

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".

6.5 "System" menu

- **Last Synchronization Mechanism**
Shows how the last time-of-day 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.

6.5.13.2 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

Daylight Saving Time (DST) Overview								Access Point
								  
Manual Setting	DST Overview	DST Configuration	SNTP Client	NTP Client	SIMATIC Time Client			
Select	DST No	Name	Year	Start Date	End Date	Recurring Date	State	Type
<input type="checkbox"/>	1	DST	2023	08/27 00:00	09/05 00:00	-	enabled	Date
1 entry.								
<input type="button" value="Create"/> <input type="button" value="Delete"/> <input type="button" value="Refresh"/>								

- **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.

6.5 "System" menu

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.

6.5.13.3 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

DST Configuration

Manual Setting | **DST Overview** | DST Configuration | SNTP Client | NTP Client | SIMATIC Time Client

DST No: 2 ▼

Type: Date ▼

Name: DST 2017

Year: 2017

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

Set Values
Refresh

6.5 "System" menu

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

DST Configuration

Manual Setting
DST Overview
DST Configuration
SNTP Client
NTP Client
SIMATIC Time Client

DST No: 1 ▼
Type: Recurring ▼
Name: DST 2016

Start Date

End Date

Hour: 00:00 ▼
Month: September ▼
Week: Third ▼
Day: Monday ▼

Hour: 00:00 ▼
Month: September ▼
Week: Fourth ▼
Day: Tuesday ▼

Set Values
Refresh

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.

6.5.13.4 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.

Simple Network Time Protocol (SNTP) Client

Manual Setting | DST Overview | DST Configuration | **SNTP Client** | NTP Client | SIMATIC Time Client

☐ SNTP Client

Current System Time: 01/11/2018 12:27:41

Last Synchronization Time: 01/11/2018 11:13:56

Last Synchronization Mechanism: Manual

Time Zone: +00:00

Daylight Saving Time: active (offset + 1h)

SNTP Mode: Poll

Poll Interval[s]: 64

SNTP Server Address:

Select	SNTP Server Address	SNTP Server Port	Primary
<input type="checkbox"/>	192.168.1.255	123	<input checked="" type="checkbox"/>

1 entry.

Create Delete Set Values Refresh

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), 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.

6.5.13.5 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.

Network Time Protocol (NTP) Client

Manual Setting | DST Overview | DST Configuration | SNTP Client | **NTP Client** | SIMATIC Time Client

☒ NTP Client

Current System Time: 01/11/2018 12:33:05

Last Synchronization Time: 01/11/2018 11:13:56

Last Synchronization Mechanism: Manual

Time Zone: +00:00

Daylight Saving Time: active (offset + 1h)

NTP Server Address: 192.168.1.250

NTP Server Port: 123

Poll Interval[s]: 64

Set Values Refresh

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.

6.5 "System" menu

- **Last Synchronization Mechanism**
Shows how the last time-of-day 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.

6.5.13.6 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.

The screenshot shows the 'Siemens Automatic (SIMATIC) Time Client' web interface. It features a navigation bar with tabs: 'Manual Setting', 'DST Overview', 'DST Configuration', 'SNTP Client', 'NTP Client', and 'SIMATIC Time Client'. The 'SIMATIC Time Client' tab is active. Below the tabs, there is a checkbox labeled 'SIMATIC Time Client' which is currently unchecked. Below this, three status fields are displayed: 'Current System Time: 08/26/2019 10:56:37', 'Last Synchronization Time: 08/26/2019 09:28:29', and 'Last Synchronization Mechanism: Manual'. At the bottom, there are two buttons: 'Set Values' and 'Refresh'.

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.

6.5 "System" menu

- **Last Synchronization Time**
Shows when the last time-of-day synchronization took place.
- **Last Synchronization Mechanism**
Shows how the last time-of-day 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.

6.5.14 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.

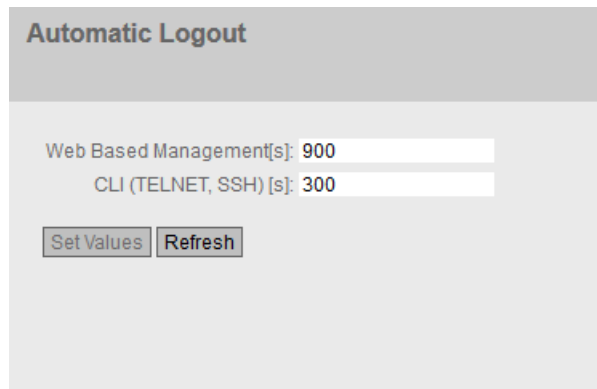
Note

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.
-



The image shows a web-based configuration interface titled "Automatic Logout". It contains two input fields: "Web Based Management[s]:" with the value "900" and "CLI (TELNET, SSH) [s]:" with the value "300". Below these fields are two buttons: "Set Values" and "Refresh".

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.

6.5.15 Syslog client

On this page, you configure the Syslog client. The Syslog messages can be sent to the Syslog server unencrypted or encrypted.

Requirements for sending Syslog messages

- The Syslog client is enabled.
- In "System > Events > Configuration", "Syslog" is activated for the relevant event.

- There is a Syslog server in your network that receives the Syslog messages.
- The IP address or the FQDN (Fully Qualified Domain Name) of the Syslog server is entered in the device.

System Logging (Syslog) Client

☐ Syslog Client

Syslog Server Address:

Select	Syslog Server Address	Server Port	TLS
<input type="checkbox"/>	192.168.16.100	514	<input type="checkbox"/>

1 entry.

Description

The page contains the following boxes:

- **Syslog Client**
Enable or disable the Syslog client on the device.
- **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**
 - Enabled
The syslog messages are sent using TLS encryption over TCP.
 - Disabled
Syslog messages are sent unencrypted over UDP.

Procedure

Enabling function

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

Creating a new entry

1. In the "Syslog Server Address" input box, enter the address of the Syslog server to which the Syslog messages are sent.
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 server port.
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.

6.5.16 Fault Monitoring

6.5.16.1 Power Supply

Settings for monitoring the power supply

Configure whether or not the power supply should be monitored by the messaging system.

A fault is then signaled by the message system when there is no power on the monitored line (Line 1) or when the voltage is too low.

Note

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

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

Fault Mask Power

Power Supply | Link Change

☐ Line 1

Set Values Refresh

Procedure

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

6.5.16.2 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 error is displayed under "Information > Errors".

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".

Fault Monitoring Link Change

Power Supply | Link Change

Port	Setting
P1	-

Set Values Refresh

Description

The table has the following columns:

- **Port**
Shows the available ports.
- **Setting**
Select the setting from the drop-down list. You have the following options:
 - Up
Error handling is triggered when the port changes to the active status.
(From "Link down" to "Link up")
 - Down
Error handling is triggered when the port changes to the inactive status.
(From "Link up" to "Link down")
 - "-" (disabled)
The error handling is not triggered.

Procedure

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

6.5.17 PROFINET

Settings for PROFINET

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

PROFINET

PROFINET Device Diagnostics: On

PROFINET Device Diagnostics for next boot: On ▼

PROFINET AR Status: Offline

PROFINET Name of Station:

Set Values
Refresh

Description of the displayed boxes

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 and EtherNet/IP

When PROFINET is turned on, EtherNet/IP is turned off. The switchover from PROFINET and EtherNet/IP has no effect on DCP.

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.

Note

Devices with two Ethernet ports

With devices that have two Ethernet interfaces, only interface P1 should be used for the PROFINET configuration because LLDP frames can only be sent and received via interface 1. They are blocked at interface P2 and are also not forwarded between the interfaces.

This applies to the following devices:

- SCALANCE W786-2 SFP
 - SCALANCE W774-1 RJ45
 - SCALANCE W774-1 M12 EEC
 - SCALANCE W778-1 M12
 - SCALANCE W778-1 M12 EEC
 - SCALANCE W734-1 RJ-45
 - SCALANCE W738-1 M12
-

SCALANCE W700 and STEP 7

The Ethernet interface can be configured in STEP 7 if the following requirements are met:

- STEP 7 V13 Update 3 with HSP0107 or
- STEP7 version 5.5.4 with GSDML version 2.31

The diagnostics functions can also be used. The WLAN interface cannot be configured with STEP 7.

PROFINET for client devices

If a client is to be used as a PROFINET device, the MAC address of the client must be specified as follows (MAC Mode):

- Own
In the network beyond the device, only IP communication and no PROFINET is possible.
- Layer 2 Tunnel
The client and the devices downstream from it can be used as PROFINET devices.

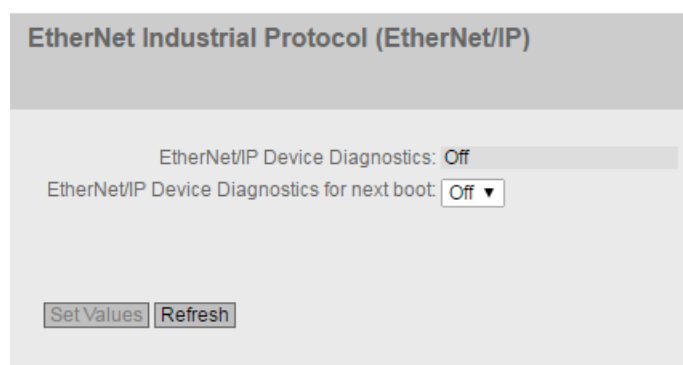
Note

If "Automatic" or "Manual" is configured as the MAC mode for a client, this device cannot be used as a PROFINET device.

6.5.18 EtherNet/IP

EtherNet/IP

On this page, you configure the mode of EtherNet/IP.



EtherNet Industrial Protocol (EtherNet/IP)

EtherNet/IP Device Diagnostics: Off

EtherNet/IP Device Diagnostics for next boot: Off ▼

Note

Devices with two Ethernet ports

On devices with two Ethernet interfaces only one of the interfaces (P1 or P2) may be used for the Ethernet configuration.

This applies to the following devices:

- SCALANCE W786-2 SFP
 - SCALANCE W774-1 RJ45
 - SCALANCE W774-1 M12 EEC
 - SCALANCE W778-1 M12
 - SCALANCE W778-1 M12 EEC
 - SCALANCE W734-1 RJ-45
 - SCALANCE W738-1 M12
-

Description

The page contains the following boxes:

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

Note

EtherNet/IP and PROFINET

When EtherNet/IP is turned on, PROFINET is turned off. The switchover from EtherNet/IP and PROFINET has no effect on DCP.

Note

PROFINET AR Status

If a PROFINET connection is established; in other words the PROFINET AR status is "Online", you cannot enable EtherNet/IP.

6.5.19 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.

The screenshot shows a web-based management interface for the 'Ping' function. The interface has a light gray background. At the top, there is a header bar with the word 'Ping' in a bold, dark font. Below the header, there are several input fields and a button. The 'Destination Address' field is a text input box. To its right is the 'Repeat' field, which is a text input box containing the number '3'. Further right is a 'Ping' button. Below these fields are two dropdown menus: 'DNS Resolution' with 'Auto' selected, and 'Out Interface for IPv6' with a minus sign '-' selected. A note below the dropdowns states: 'Out Interface is required only when pinging IPv6 multicast and link-local addresses'. Below this is a large, empty text area labeled 'Ping Output:'. At the bottom left of the text area is a 'Clear' button.

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.

6.6 "Interfaces" menu

6.6.1 Ethernet

6.6.1.1 Overview

Overview of the port configuration

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

Ports Overview								
Overview		Configuration						
Port	Port Name	Status	OperState	Link	Mode	MTU	Negotiation	MAC Address
P1		enabled	up	up	100M FD	1500	enabled	00-1b-1b-a5-5d-98
<input type="button" value="Refresh"/>								

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 transmission speed and the transmission method of the port.
- **MTU (Maximum Transmission Unit)**
Shows the packet size.
- **Negotiation**
Shows whether the automatic configuration is enabled or disabled.
- **MAC Address**
Shows the MAC address of the port.

6.6.1.2 Configuration

Configuring ports

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

Ports Configuration

Overview

Configuration

Port: P1

Status: enabled

Port Name:

MAC Address: 00-1b-1b-c7-f5-a2

Mode Type: -

Mode: 100M FD

Negotiation: enabled

MTU: 1500

OperState: up

Link: up

Set Values

Refresh

Description

The table has the following rows:

- Port**
Select the port to be configured from the drop-down list.
- Status**
Specify whether the port is enabled or disabled.
 - enabled
The port is enabled. Data traffic is possible only over an enabled port.
 - disabled
The port is disabled.
- Port Name**
Enter a name for the port here.
- MAC Address**
Shows the MAC address of the port.
- Mode Type**

Note

This parameter cannot be configured for the SCALANCE W760/W720 devices. The value is preset to "Autonegotiation".

- **Mode**
Shows the transmission speed and the transfer mode of the port.
- **Negotiation**
Shows whether the automatic configuration of the connection to the partner port is enabled or disabled.
- **MTU(Maximum Transmission Unit)**
Enter the packet size above which packets are fragmented.
- **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.

6.6 "Interfaces" menu

6.6.2 WLAN

6.6.2.1 Basic

Basic settings

On this page, you make several basic settings for the device, for example, the country setting and mode.

Note

To configure the WLAN interface, you must always specify the country code first. Some parameters are dependent on the country setting, for example the transmission standard.

WLAN Basic Radio Settings

Basic

Advanced

Antennas

Allowed Channels

802.11n

AP

AP WDS

AP 802.11a/b/g Rates

AP 802.11n Rates

Force Roaming

Spectrum Analyzer

Country Code: Germany

Device Mode: AP

Radio	Enabled	Radio Mode	Frequency Band	WLAN Mode 2.4 GHz	WLAN Mode 5 GHz	DFS (802.11h)	Outdoor Mode	max. Tx Power	max. EIRP
WLAN 1	<input type="checkbox"/>	AP	2.4 GHz	802.11 n	802.11 n	<input type="checkbox"/>	<input type="checkbox"/>	20 dBm	23 dBm

Tx Power Check:

Following channels are not allowed in current configuration:

WLAN 1: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13

Warning:

The device may not be permitted for use in countries denoted by a "*" character.

Please check the following website for more detailed information:

<http://www.siemens.com/wireless-approvals>

Set Values

Refresh

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.

Note

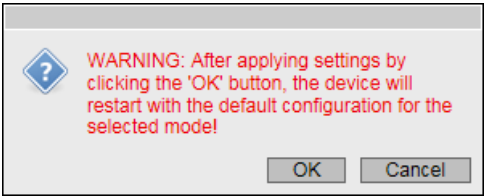
Locale setting

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 operating modes are possible:
 - AP: Access point mode
 - Client: Client mode

Note

After changing the mode, a message is displayed. If you confirm the message with "OK", the device restarts in the changed mode with the factory-set configuration settings.



If you have restarted the device after changing the mode, you will need to log on again to be able to continue the configuration.

The table has the following columns:

- **Radio**
Shows the available WLAN interfaces.
- **Enabled**
Status of the WLAN interface. To enable the WLAN interface, select the check box.

Note

Enabling the WLAN interface

The WLAN interfaces are disabled when the device is supplied. The WLAN interfaces are can be enabled once the country and the antenna settings are configured.

- **Radio Mode**
Shows the mode of the WLAN interface.

6.6 "Interfaces" menu

- **Frequency Band**
Specify the frequency band. In client mode, dual-frequency operation is also possible.
 - 2.4 GHz
 - 5 GHz
 - 2.4 GHz + 5 GHz (only in client mode)

Note

Configuring WLAN interfaces of the W786-21A RJ-45 for different frequency bands

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

- **WLAN Mode 2.4 GHz/WLAN Mode 5 GHz**
Select the required transmission standard for the configured frequency band. The selection depends on the country setting.
 - Auto (only in client mode)
The transmission standard is determined automatically (2.4 GHz + 5 GHz).
 - 802.11a
The transmission standard IEEE 802.11a (5 GHz) is set.
 - 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.
 - 802.11n only
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.

Note

If you select the transmission standard "802.11n", "802.11n only" or "Auto" (only in client mode), you cannot set the threshold value of the fragmentation length see "Fragmentation Length Threshold" in "Interfaces > WLAN > Advanced".

- **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.

Note

RCoax 5 GHz and DFS

In the USA and in countries that follow the FCC (Federal Communication Commission) when operating with DFS (Dynamic Frequency Selection), the IWLAN RCoax Cable 5 GHz may not be used. The current status of the approvals can be found on the Internet at:

<http://www.siemens.com/wireless-approvals>

- **Outdoor Mode**

- Enabled

If you have enabled the outdoor mode, you only have the channels available that are permitted for outdoor operation.

- Disabled

If you have disabled the outdoor mode, you only have the channels available that are permitted for operation in a building.

- **max. Tx Power**

Specify the maximum possible transmit power of the device.

If the transmit power is set too high the received signal at the client may be overmodulated.

Check the received signal strength at the client (dBm).

It may be necessary to reduce the transmit power depending on the antennas being used to avoid exceeding the maximum legal transmit power. Reducing the transmit power effectively reduces cell size.

Note

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

Note

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

- **max. EIRP (Effective Isotropic Radiated Power)**

Shows the current radiated power of the antenna, in relation to a non-directional antenna (isotrop). Product of antenna gain, number of antenna connectors, cable length, additional attenuation and set Tx power.

- **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.

- -

- The channels can be used with the current settings.

- Channel numbers

- Indicates the channels on which the current transmit power exceeds the maximum permitted transmit power.

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.

6.6.2.2 Advanced

Further possible settings

On this page, you can specify details of the transmission characteristics. You only need to adapt the parameters on this page if the SCALANCE W700 device cannot be used as it is intended with the default settings.

WLAN Advanced Radio Settings										
Basic	Advanced	Antennas	Allowed Channels	802.11n	AP	AP WDS	Force Roaming	AP 802.11a/b/g Rates	AP 802.11n Rates	Spectrum Analyzer
Radio	Beacon Interval [ms]	DTIM	RTS/CTS Threshold [Bytes]	Fragmentation Length Threshold [Bytes]		HW Retries	Multi Radar Detection	Prefer Configured DFS Channel		
WLAN 1	100	1	2346	2346		16	<input type="checkbox"/>	<input type="checkbox"/>		
Set Values Refresh										

Description

The table has the following columns:

- **Radio**
Shows the available WLAN interfaces in this column.
- **Beacon Interval [ms] (only in access point mode)**
Specify the interval (40 - 1000 ms) at which the access point sends beacons. Beacons are packets that are sent cyclically by an access point to inform clients of its existence.
- **DTIM (only in access point mode)**
The DTIM interval (1-15) specifies the number of beacons to be sent before the access point sends the collected packets (broadcast, unicast, multicast) to the client.
 - If you enter a "1" in this box, the access point transmits broadcast, unicast and multicast packets directly after each beacon (recommended setting for normal network environments).
 - If you entered a "5" in this field, this would mean that the access point collects the packets and sends them after every fifth beacon.

Increasing this value allows a longer sleep mode for the clients but means a greater delay for packets.

- **RTS/CTS Threshold [Bytes]**
RTS/CTS (Request To Send/Clear To Send) is a method for avoiding collisions. The method is based on the exchange of status information prior to sending the actual data (hidden node problem). To minimize the network load due to additional protocol traffic, this method is used only as of a certain packet size. You specify the packet size with the "RTS/CTS Threshold" parameter.

- **Fragmentation Length Threshold [Bytes]**

Specify the maximum packet size transferred on the wireless link. Large packets are divided up into small packets prior to transmission and then reassembled into the original size after they have been received. This can be beneficial if the transmission quality is poor because larger packets are more difficult to transmit. However fragmentation into smaller packets means a poorer throughput.

Note

You can only edit this value if the you have set the transmission standard "802.11g" (2.4 GHz) or "802.11 a" (5 GHz), see "WLAN Mode" in "Interfaces > WLAN > Basic".

- **HW Retries**

Specify the number of hardware retries. The hardware repetition is performed by the WLAN chip itself when it tries to repeat an unacknowledged packet immediately. If all hardware repetitions were unsuccessful, the packet is deleted.

- **Multi Radar Detection (only in access point mode)**

- Enabled

This function is only available if you have enabled the "DFS" function on the "Basic" page. This function is suitable for systems with several access points connected via an Ethernet network and that send on the same channel.

When an access point detects a radar signal it distributes this information to all connected access points. If at least one further access point verifies the radar signal within 40 ms, all connected access points are informed. All the devices sending on this channel change to a different channel. The channel is blocked for 30 minutes for the access points in the network.

If you have configured "Auto" for the channel on the "Interfaces > WLAN > AP" page, the function cannot be used reliably. In this case the verification of the radar signals is only possible when at least two connected access points happen to transmit on the same channel. If only one access point detects a signal on a channel, it treats this as a valid radar signal.

- Disabled

The function is not used. When an access point detects a radar signal it changes to another channel.. The configured channel is no longer taken into account.

- **Prefer Configured DFS Channel (only in access point mode)**

- Enabled

This function is only available if you have enabled the "DFS" function on the "Basic" page. If the configured channel of a WLAN interface was blocked due to radar detection and is released again after 30 minutes the access point changes automatically to the configured channel.

Before the access point starts the communication on the configured channel it searches 60 seconds for primary users on the channel. During this time the access point does not send beacons. If signals are found on the channel, the access point changes channel and repeats the check. Only when no signals from primary users are detected after 60 seconds does the access point send on the channel.

If you have configured "Auto" for the channel on the "Interfaces > WLAN > AP" page, the device does not have a configured channel to which it can return.

- Disabled

The function is not used.










Procedure

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

6.6.2.3 Antennas

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	●	●	●	●	●	●

*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.

G_IK10_XX_30317

6.6 "Interfaces" menu

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		ANT897-4ME				•	•
			ANT897-5PN				•	•
			ANT795-4MA	•	•			•
			ANT795-4MB	•	•			•
			ANT795-4MC	•		•	•	
			ANT795-4MD	•		•	•	
			ANT795-4MX	•		•	•	
			ANT795-6MN	•	•	•	•	•
			ANT795-6MP	•	•	•	•	•
Sector	2.4 and 5		ANT795-6DC	•	•	•	•	•
	5		ANT793-6DG	•	•	•	•	•

G_IK10_XX_30318

Antennas

Configuration of external antennas

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

Only the antenna mode can be configured for internal antennas.

Note

50 Ω terminating resistor

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

The antenna R1A1 must be always be connected as soon as the associated WLAN Interface is turned on. If no antenna is connected, the relevant interface must also be disabled for Rx and Tx. Otherwise, there may be transmission disruptions.

Antennas

Basic
Advanced
Antennas
Allowed Channels
802.11n
Client
Signal Recorder
Force Roaming

Connector	Antenna Type	Antenna Gain 2.4 GHz [dBi]	Antenna Gain 5 GHz [dBi]	Cable Length [m]	Additional Attenuation [dB]	Antenna Mode
R1 A1	Omni-Direct-Mount: ANT795-4MC	3	5	0	0	RX/TX
R1 A2	Omni-Direct-Mount: ANT795-4MC	3	5	0	0	RX/TX

☐ Dynamic Transmit Antenna Selection (DTAS)

Set Values
Refresh

Description

The table has the following columns:

- Connector**
Shows the name of the antenna connector.
- Antenna Type**
Select the type of external antenna connected to the SCALANCE W700 device. If the type of your antenna is not available, select the entry "User defined".
- 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 SCALANCE W700 device and the external antenna.
- Additional Attenuation [dB]**
Here, specify the additional attenuation caused, for example, by an additional splitter or a long antenna cable.

6.6 "Interfaces" menu

- **Antenna Mode**

For the antenna connector R1 A1, the entry Rx\Tx (transmit and receive) cannot be changed.

- **Dynamic transmitting antenna selection (DTAS) (in client mode only)**

When enabled, the antenna that offers the better signal to the access point is automatically selected for the transmission.

The signal strengths of the two antennas are displayed under "Information > WLAN > Radio interfaces information".

Requirements for DTAS:

- MCS ≤ 7 is set at the access point.
- Two antennas configured with the antenna mode "RX/TX".
- If three antennas are available, the "Antenna Type" "Not used (50 Ohm terminating resistor)" must be set for the third antenna.

Steps in configuration

To configure one or more antennas, follow the steps below:

1. For the antenna connector (R1 A1) in the "Antenna Type" drop-down list, select the type of antenna.
2. In the "Cable Length" input box, enter the length of the connecting cable you are using in meters. For the antenna connector R1 A1, the "Antenna Mode" cannot be changed.
3. Click the "Set Values" button.

6.6.2.4 Allowed Channels

Channel settings

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

On this page, you specify which channels may be used for communication.

Allowed Channels Settings

Basic | **Advanced** | Antennas | **Allowed Channels** | 802.11n | AP | AP WDS | AP 802.11a/b/g Rates | AP 802.11n Rates | Spectrum Analyzer

Radio: Use Allowed Channels only

WLAN 1: ☐

Frequency Band: 2.4 GHz

☒ Select / Deselect all

Radio	Radio Mode	1	2	3	4	5	6	7	8	9	10	11	12	13
WLAN 1	AP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Frequency Band: 5 GHz

☒ Select / Deselect all

Radio	Radio Mode	184	188	192	196	8	12	16	36	40	44	48	52	56	60	64	100	104	108
WLAN 1	AP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Description

Table 1 contains the following columns:

- **Radio**
Shows the available WLAN interfaces.
- **Use Allowed Channels only**
If you enable the option, you restrict the selection of channels via which the AP or the client is allowed to establish the connection.
In the following tables, you define the
 - channels that the AP can use to establish a wireless cell when the "Auto" channel setting is enabled.
 - the channels on which the client searches for an AP.The tables are divided up according to frequency bands.
If the option is disabled, the channels available based on the settings (country code, antennas, transmit power etc.) are used.

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

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

The tables of the frequency bands have the following columns:

- **Radio**
Shows the available WLAN interfaces.
- **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.

6.6.2.5 802.11n

Properties of 802.11n

With the IEEE 802.11n standard, it is possible to put together individual data packets in one larger data packet, the A-MPDU and A-MSDU data packets. This achieves a higher data throughput.

On this page, you make the settings for the A-MPDU and A-MSDU data packets. Some of the settings depend on the set transmission standard and the selected channel width.

802.11n Advanced Radio Settings

Basic	Advanced	Antennas	Allowed Channels	802.11n	AP	AP WDS	AP 802.11a/b/g Rates	AP 802.11n Rates	Spectrum Analyzer
-------	----------	----------	------------------	---------	----	--------	----------------------	------------------	-------------------

Radio	A-MPDU	A-MPDU Limit [Frames]	A-MPDU Limit [Bytes]	A-MSDU	A-MSDU Packet Size [Bytes]	Guard Interval [ns]
WLAN 1	<input checked="" type="checkbox"/>	32	50000	<input checked="" type="checkbox"/>	100	800 (long) ▼

Description

The table has the following columns:

- **Radio**
Shows the available WLAN interfaces.
- **A-MPDU**
Aggregated MAC Protocol Data Unit (A-MPDU)
Enables or disables that several MPDUs with the same destination address are sent as a large A-MPDU. This allows the total throughput to be increased.
If this check box is disabled, A-MPDU data packets are received but not sent.
- **A-MPDU Limit [Frames]**
Specify the number of individual data packets grouped together in one A-MPDU data packet.
Range of values: 2 - 64 frames
- **A-MPDU Limit [Bytes]**
Specify the maximum size of the A-MPDU data packet.
Range of values: 1024 - 65535 bytes
Default: 50000 bytes
- **A-MSDU**
Aggregated MAC Service Data Unit (A-MSDU)
Enables or disables that several MSDUs with the same destination address are bundled into an A-MSDU and are sent together. This reduces the network load. Due to their shorter maximum length A-MSDUs are more suitable for the bundling of several shorter frames.
If this check box is disabled, A-MSDU data packets are received but not sent.

- **A-MSDU Packet Size [Bytes]**
Specify the maximum size of the A-MSDU data packet.
Range of values: 50 - 200 bytes
Default: 100 bytes
- **Guard Interval [ns] (only in Access Point mode)**
Select the send pause that must be kept to between two transmitted OFDM symbols.
The following settings are possible. The selection depends on the selected transmission standard.
 - 400 (short)/800 (long): The setting 400 ns is optional. Depending on the signal quality, packets can be sent with a send pause of 400 ns or 800 ns.
 - 800 (long): The send pause is 800 ns.

Procedure

Configure 802.11n settings on the access point

1. Enable the "A-MPDU" option.
2. Enter the required values in the "A-MPDU Limit [Frames]" and "A-MPDU Limit [Bytes]" input boxes.
3. Enable the "A-MSDU" option.
4. Enter the required value in the "A-MSDU Packet Size" input box.
5. Select the required value from the "Guard Interval [ns]" drop-down list.
6. Click the "Set Values" button.

Configure 802.11n settings on the client

1. Enable the "A-MPDU" option.
2. Enter the required values in the "A-MPDU Limit [Frames]" and "A-MPDU Limit [Bytes]" input boxes.
3. Enable the "A-MSDU" option.
4. Enter the required value in the "A-MSDU Packet Size" input box.
5. Click the "Set Values" button.

6.6.2.6 AP

Configuration

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

Note

This tab is available only in access point mode.

Access Point-Einstellungen Access Point

? ? ? ?

Basic | Erweiterungen | Antennen | Zugelassene Kanäle | 802.11n | AP | AP WDS | AP 802.11a/b/g-Datenraten | AP 802.11n-Datenraten

Roaming erzwingen | **Spektrumanalysator**

Funkschnittstelle	Kanal	Alternativer DFS-Kanal	Kanalbandbreite [MHz]	Ausgewählte Kanäle	Ausgewählte alternative DFS-Kanäle
WLAN 1	Auto	-	20	Auto	-

< >

Funkschnittstelle	Verfügbare Kanäle
WLAN 1	1,2,3,4,5,6,7,8,9,10,11,12,13

< >

Funkschnittstelle	Port	Aktiviert	SSID	Broadcast-SSID	Nur WDS	WDS-ID
WLAN 1	VAP 1.1	<input checked="" type="checkbox"/>	Siemens Wireless Network	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

< >

Warnung: Für Kanäle, die mit einem Sternchen (*) gekennzeichnet sind, ist das Zulassungsverfahren eventuell noch nicht abgeschlossen.

Auf der folgenden Website finden Sie aktuelle Informationen zum Stand der Zulassungen:
<http://www.siemens.com/funkzulassungen>

Description

Table 1 has the following columns:

- **Radio**
Shows the available WLAN interfaces in this column.
- **Channel**
Specify the main channel.
If you want the access point to search for a free channel itself, use "Auto". The selection of channels used by an access point when establishing a wireless cell can be restricted. To do this, select the "Use Allowed Channels only" check box on the "Allowed Channels" tab.
.If you want to use a fixed channel, select the required channel from the drop-down list.
- **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 primary user was detected both on the main and alternative channel, the access point automatically searches for a free channel.
If you want to use a fixed channel, select the required channel from the drop-down list.

- **Channel Width [MHz]**

You can specify the channel bandwidth only with the IEEE 802.11n transmission standard. The following settings are possible.

- 20
Channel bandwidth 20 MHz
- 40up
Channel bandwidth 40 MHz. The configured channel and the neighboring channel above it are used.
- 40down
Channel bandwidth 40 MHz. The configured channel and the neighboring channel below it are used.

Note

Channel bandwidth 40 MHz and frequency band 2.4 GHz

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

- **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 in this column.

- **Available Channels**

This box displays the permitted channels. The display depends on the wireless approvals of the currently selected country and the settings for "Allowed Channels".

Table 3 has the following columns:

- **Radio**

Shows the WLAN interface.

- **Port**

Shows the VAP interface.

6.6 "Interfaces" menu

- **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**
 - disabled
The SSID is no longer sent in the beacon frame of the access point. This means that the SSID is not visible for other SCALANCE W700 devices. Only clients that know the SSID of the access point and that are configured with it can connect to the access point. The "Any SSID" option must be disabled on these clients.
 - enabled
The SSID is sent in the Beacon frame of the access point and is visible for other SCALANCE W700 devices. This means that clients on which the "Any SSID" option is enabled can also connect to the access point.

Note

Since no encryption is used for the SSID transfer, this function can only provide basic protection against unauthorized access. The use of an authentication method (for example WPA2 (RADIUS) or WPA2-PSK if this is not possible) provides higher security. You must also expect that end devices may have problems with access to a hidden SSID.

- **WDS only**
If you enable this option, the access point only supports communication via WDS. In WDS mode, all access points must use the same channel.
- **WDS ID**
Enter the WDS ID. The WDS ID can be a maximum of 32 characters long. To establish a WDS connection, enter this WDS ID on the WDS Partner. ASCII code 0x20 to 0x7e is used for the WDS ID.

Procedure

1. Select the required channel from the "Channel" drop-down list.
2. Enter network name in the "SSID" input box for the corresponding WLAN interface and port.
3. For the relevant WLAN interface and the port, select the "Enabled" check box.
4. Click the "Set Values" button.

6.6.2.7 AP WDS

Communication between access points

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

Note

This tab is available only in access point mode.

Wireless Distribution System Settings

Basic

Advanced

Antennas

Allowed Channels

802.11n

AP

AP WDS

AP 802.11a/b/g Rates

AP 802.11n Rates

Spectrum Analyzer

Radio	Port	Port enabled	Connection over	Partner ID Type	Partner MAC	Partner WDS ID
WLAN 1	WDS 1.1	<input type="checkbox"/>	VAP 1.1	WDS ID	00-00-00-00-00-00	

Set Values

Refresh

Description

The table has the following columns:

- Radio**
Shows the available WLAN interfaces in this column.
- Port**
Shows the port.
- Port enabled**
Enables the WDS interface.
- Connection over**
Specify the VAP interface via which the WDS connection is established. Both the MAC address of the VAP as well as security settings (for example WPA2) are used.
- Partner ID Type**
Specify the type of WDS communication.
 - MAC Address
The MAC address is used. The "Partner WDS ID" input box is grayed out. For "Partner MAC", enter the MAC address of the WDS partner.
 - WDS ID
The WDS ID is used. The "Partner MAC" input box is grayed out. For "Partner WDS ID" enter the WDS ID of the WDS partner.

6.6 "Interfaces" menu

- **Partner MAC**
Enter the MAC address of the WDS partner.
- **Partner WDS ID** Enter the WDS ID of the WDS partner.
For the WDS ID ASCII code 0x20 to 0x7e is used.

Note

Matching security settings in WDS mode

In WDS mode, make sure that the security settings match up for all devices involved. If settings are incorrect or not compatible on the individual devices, no data exchange is possible due to incorrect authentication. Avoid the "Auto" setting in the "Security Settings" tab of the Basic Wizard, because with this setting, synchronization of the security settings between the access points is not possible.

Note

In WDS operation, the following restrictions apply to all access points involved:

- All access points that will communicate with each other must use the same channel, the same transmission procedure and the same data rate.
- You can select either WEP or WPA(2)-PSK as the encryption method.
You configure the security settings in the assigned VAP interface: "Security > WLAN > Basic"
You cannot use authentication with a RADIUS server for a WDS connection.
- In the IEEE 802.11h transmission mode, it is not practical to select the WDS mode. In WDS mode, all access points must use the same channel. If a signal from a primary user is detected by an access point, the channel is changed automatically and the existing connection is then terminated.

Procedure

1. Select the required VAP interface from the "Connection over" drop-down list.
2. Select the entry "WDS ID" in the "Partner ID Type" drop-down list.
3. In the "WDS ID" input box, enter the WDS ID of the WDS partner. The "MAC Address" input box is grayed out.
4. Click the "Set Values" button.

6.6.2.8 AP 802.11a/b/g Rates

Data transmission speeds with IEEE 802.11a/b/g

Note

The tab is available only in access point mode.

The WBM page can only be configured if "802.11a", "802.11g" or "802.11n" is set for the WLAN mode.

The WBM page shows the available data transmission speeds for the WLAN mode 802.11a/b/g. If necessary, you can change the data transmission speeds. Otherwise, we recommend that you retain the default setting for data transmission speeds. The access point will then use only the selected data transmission speeds for communication with the clients.

AP 802.11 a/b/g Data Rates Settings

Basic	Advanced	Antennas	Allowed Channels	802.11n	AP	AP WDS	AP 802.11a/b/g Rates	AP 802.11n Rates
Force Roaming		Spectrum Analyzer						

Radio

Use selected data rates only

WLAN 1 ☐

Radio: WLAN 1 ▼

	Enabled	Basic	Copy to Table
All data rates settings	No Change ▼	No Change ▼	Copy to Table

Radio	Data Rate [Mbps]	Enabled	Basic
WLAN 1	1.0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WLAN 1	2.0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WLAN 1	5.5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WLAN 1	6.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
WLAN 1	9.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
WLAN 1	11.0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WLAN 1	12.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
WLAN 1	18.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
WLAN 1	24.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
WLAN 1	36.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
WLAN 1	48.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
WLAN 1	54.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Default Values

Set Values Refresh

Description

Table 1 has the following columns:

- **Radio**
Specifies the WLAN interface to which the information relates.
- **Use selected data rates only**
If you select this option, you can specify the data transmission speeds for the required WLAN interface.
If this option is disabled, the default values are used. As default, this option is disabled.

Radio"drop down list"

In this drop-down list, select the WLAN interfaces displayed in Table 3 (Data Rate).

With Table 2, you can enable or disable all check boxes of a column of Table 3 (Data Rate) at once. Table 2 has the following columns:

- **All data rates settings**
Shows that the setting is valid for all entries in Table 3.
- **Enabled / Basic**
In the drop-down list, select the setting for all entries. If "No Change" is selected, the entry in table 3 remains unchanged.
- **Transfer to table**
If you click the button, the setting is adopted for all entries of table 3.

Table 3 (Data Rate) consists of the following columns:

- **Radio**
Specifies the WLAN interface to which the information relates.
- **Data Rate [Mbps]**
Shows the supported data transmission speeds in megabits per second.
- **Enabled**
Enable the option to assign the required data transmission speed to the WLAN interface.

Note

You need to enable at least one data transmission speed.

- **Basic**
Enable the option to declare the required data transmission speed as "Basic". The "Basic" parameter specifies that a client must be capable of this speed to be able to connect to the access point. The "Basic" option can only be enabled if an available data transmission speed has been selected.

Note

At least one data transmission speed needs to be specified as "Basic".

Procedure**To configure a certain data transmission speed on WLAN 1:**

1. Enable the "Use selected data rates only" option for "WLAN 1".
2. From the "Radio" drop-down list, select the entry "WLAN 1".
3. Select the appropriate check box in the "Enabled" column and in the "Basic" column for the required data transmission speed.
4. Click the "Set Values" button.

To reset the selection:

1. Click the "Default Values" button. The selection is reset to the default setting.

6.6.2.9 AP 802.11n Rates

Data transmission speeds in IEEE 802.11n

Note

The tab is available only in access point mode.

The WBM page can only be configured if "Only 802.11n" or "802.11n" is set for WLAN Mode.

The WBM page shows the available data transmission speeds (MCS = Modulation and Coding Schemes) for the WLAN mode 802.11n. You can select any combination of these data transmission speeds. The access point will then use only the selected data transmission speeds for communication with the clients.

AP 802.11 n Data Rates Settings

Basic	Advanced	Antennas	Allowed Channels	802.11n	AP	AP WDS	AP 802.11a/b/g Rates	AP 802.11n Rates
Force Roaming	Spectrum Analyzer							

Radio

Use selected data rates only

WLAN 1

WLAN 2

Radio:

WLAN 1

				Enabled	Copy to Table
All data rates settings				No Change	Copy to Table
Radio	MCS Index	Streams	Data Rate [Mbps]	Enabled	
WLAN 1	0	1	6.5	<input checked="" type="checkbox"/>	
WLAN 1	1	1	13.0	<input checked="" type="checkbox"/>	
WLAN 1	2	1	19.5	<input checked="" type="checkbox"/>	
WLAN 1	3	1	26.0	<input checked="" type="checkbox"/>	
WLAN 1	4	1	39.0	<input checked="" type="checkbox"/>	
WLAN 1	5	1	52.0	<input checked="" type="checkbox"/>	
WLAN 1	6	1	58.5	<input checked="" type="checkbox"/>	
WLAN 1	7	1	65.0	<input checked="" type="checkbox"/>	

Default Values

Set Values

Refresh

Description

Table 1 has the following columns:

- **Radio**
Specifies the WLAN interface to which the information relates.
- **Use selected data rates only**
If you select this option, you can specify the data transmission speeds for the required WLAN interface.
If this option is disabled, the default values are used. As default, this option is disabled.

"Radio" drop-down list

In this drop-down list, select the WLAN interfaces displayed in Table 3 (MCS Index).

With Table 2, you can enable or disable all check boxes of a column of Table 3 (MCS Index) at once. Table 2 has the following columns:

- **All data rates settings**
Shows that the setting is valid for all entries in Table 3.
- **Enabled**
In the drop-down list, select the setting for all entries. If "No Change" is selected, the entry in table 3 remains unchanged.
- **Transfer to table**
If you click the button, the setting is adopted for all entries of table 3.

Table 3 (MCS Index) consists of the following columns:

- **Radio**
Specifies the WLAN interface to which the information relates.
- **MCS Index**
Shows the supported MCS indexes. The displayed MCS indexes depend on the settings "Antenna Type" and "Antenna Mode". You will find the settings in "Interfaces > WLAN > Antennas". If, for example, you only use one antenna, only the MCS 0 to 7 are displayed.
- **Streams**
Shows the maximum possible number of parallel data streams that can be transmitted with the selected MCS index.
- **Data rate [Mbps]**
Shows the supported data transmission speeds in megabits per second. The displayed data transmission speeds depend on the settings "Guard Interval" and "HT Channel Width". You will find the setting "HT Channel Width" in "Interfaces > WLAN > AP". The "Guard Interval" setting can be found in "Interfaces > WLAN > 802.11n".
- **Enabled**
Enable the option to assign the required data transmission speed to the WLAN interface.

Note

You need to enable at least one MCS index.

Procedure**To configure a certain data transmission speed on WLAN 1:**

1. Enable the "Use selected data rates only" option for "WLAN 1".
2. From the "Radio" drop-down list, select the entry "WLAN 1".
3. Select the corresponding check box in the "Enabled" column for the selected MCS index.
4. Click the "Set Values" button.

To reset the selection:

1. Click the "Default Values" button. The selection is reset to the default setting.

Or

1. Disable the "Use selected data rates only" option in Table 1.
2. Click the "Set Values" button.

6.6.2.10 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 in client mode.

Client Settings

BasicAdvancedAntennasAllowed Channels802.11nClientSignal RecorderForce Roaming

Radio	MAC Mode	MAC Address	Any SSID	DHCP Renew After Roaming	min. AP Signal Strength [dBm]
WLAN 1	Automatic	00-00-00-00-00-00	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0

Radio	Roaming Threshold	Background Scan Mode	Background Scan Interval [ms]	Background Scan Threshold [dBm]
WLAN 1	medium	idle	5000	0

Radio	Scan Channels			
WLAN 1	1,2,3,4,5,6,7,8,9,10,11,12,13			

Radio	Enabled	SSID	Security
WLAN 1	<input type="checkbox"/>		Context 1
WLAN 1	<input type="checkbox"/>		Context 1
WLAN 1	<input type="checkbox"/>		Context 1
WLAN 1	<input type="checkbox"/>		Context 1
WLAN 1	<input type="checkbox"/>		Context 1
WLAN 1	<input type="checkbox"/>		Context 1
WLAN 1	<input type="checkbox"/>		Context 1
WLAN 1	<input type="checkbox"/>		Context 1

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

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

Set ValuesRefresh

Note

WLAN interface disabled

The WLAN interface will be disabled unless at least one SSID is configured or the setting "Any SSID" is enabled.

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:
 - Automatic
The client automatically adopts the source MAC address of the first frame that it receives over the Ethernet interface.
 - Manual
If you select "Manual", enter the MAC address in the "MAC Address" column.
 - Own
The client uses the MAC address of the Ethernet interface for the WLAN interface.
 - Layer 2 Tunnel
The client uses the MAC address of the Ethernet interface for the WLAN interface. The network is also informed of the MAC addresses connected to the Ethernet interface of the client. Up to eight MAC addresses can be used.
- **MAC Address**
If you have selected "Manual" for "MAC Mode", enter the MAC address of the client.
- **Any SSID**
 - Enabled
In client mode, the SCALANCE W device attempts to connect to the access point that corresponds to the security settings of security context 1. The clients can only connect to the access point on which the "Broadcast SSID" option is enabled.
 - Disabled
The client attempts to connect to the access point from the SSID list whose security settings match one of the defined security contexts.
- **DHCP Renew After Roaming**
 - Enabled
After changing to a different access point, a check is made to find out whether the IPv4 address of the client is still valid. If the IPv4 address is invalid, a new IPv4 address is requested from the DHCP server.
 - Disabled
If the client changes to a different access point the IPv4 address is not checked.

- **min. AP signal strength**

The client has a signal strength set.

Note**iPCF / iPCF-HT / IPCF-MC enabled**

When iPCF / iPCF-HT / IPCF-MC is enabled, the signal strength cannot be set.

The client must receive the signal coming from the access point with at least the specified signal strength to be able to connect to this access point.

The signal strength can fluctuate briefly, e.g. due to the client moving or other disruptive factors. To filter out fluctuations of the signal a hysteresis is used to specify a range around this value, in which the client does not change access points before this range is undershot. If the signal coming from the access point falls below this range, the client disconnects from the connected access point and searches for a new access point.

- **Roaming Threshold**

Specify the threshold after which the client roams to the new access point.

- High
Changes only at a significantly higher field strength to the AP with the stronger signal.
- Medium
Changes at a moderately higher field strength to the AP with the stronger signal.
- Low
Changes at a slightly higher field strength to the AP with the stronger signal.

- **Background Scan Mode**

While the client is connected to an access point, it scans for other access points in the background with which it can connect when necessary. Specify the mode for the scan. The following options are available:

- Always
If the background scan threshold is undershot, the client searches continuously for access points.
- Idle
If there is no data transfer for a certain time, a scan is started for further access points.
- Disabled
As long as the client is connected, there is no scan for further access points.
- Current channel
The client updates its scan list based on the beacons (management frames) that it has received on the current channel. The scan list is evaluated within the background scan interval. If beacons from a better access point are included, the client switches to that access point after evaluation without changing the current channel.

Note**iPRP enabled**

When iPRP is enabled, the client sends special roaming advertisement frames to its redundant partner for each roaming operation. The redundant partner may not perform roaming itself for 500 ms after receiving this.

- **Background Scan Interval [ms]**
Specify the interval at which further access points are scanned.
- **Background Scan Threshold [dBm]**
Specify the threshold. If the threshold is undershot, the client searches for further access points.

Table 2 has the following columns:

- **Radio**
Shows the WLAN interface.
- **Scan Channels**
Shows the channels on which the client searches for an access point. The display depends on the wireless approvals of the selected country and the settings for "Allowed Channels".

Table 3 has the following columns:

- **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

Note

iPCF / iPCF-HT / IPCF-MC enabled

If the iPCF, iPCF-HT or iPCF-MC mode is enabled, you can only select security context 1.

Procedure

1. From the "MAC Mode" drop-down list, select the required assignment of the MAC address.
2. In table 3, enter an SSID for "SSID".
3. Select a security context.
4. Enable the required SSID.
The "Any SSID" function is disabled.
5. Click the "Set Values" button.

6.6.2.11 Force roaming

On this page you specify when roaming is performed.

- **On connection termination (only in access point mode)**

If the connection over the Ethernet interface is terminated, a client logged in over the wireless network will not notice anything. Possible causes for connection termination include, for example, wire break, failed network components, pulled plug. The access point can force the logged-in clients to roam by deactivating the relevant WLAN interface on connection termination. The clients roam and then connect to a different access point. As soon as the Ethernet interface is available again, the access point switches on its WLAN interfaces once again.

- **When the target address is not reached**

To monitor the device sends pings to the configured destination addresses at regular intervals.

- The interface is monitored by one target address

When this target address does not send a ping response, the access point turns off the corresponding VAP interface or the client restarts the WLAN interface.

- The interface is monitored by multiple target addresses

Only if none of the configured target addresses sends a ping response does the access point turn off the corresponding VAP interface or the client restart the WLAN interface. As long as at least one destination address can be reached, the interface remains active. The access point, for example, sends a disassociation frame to the WLAN clients connected via this VAP interface. The WLAN clients roam and connect to a different VAP interface. If the address becomes reachable again, the connection can be established again via this VAP interface.

The possible settings differ for access point and client.

In access point mode

Force Roaming

Basic | Advanced | Antennas | Allowed Channels | 802.11n | AP | AP WDS | AP 802.11a/b/g Rates | AP 802.11n Rates | Force Roaming | Spectrum Analyzer

Radio

Force Roaming on link down

WLAN 1

WLAN 2

Force Roaming on IP down

Select	Destination Address	Interval [ms]	Max. Lost Packets	VAP 1.1	VAP 1.2	VAP 1.3	VAP 1.4	VAP 1.5	VAP 1.6	VAP 1.7	VAP 1.8	VAP 2.1	VAP 2.2	VAP 2.3	VAP 2.4
<input type="checkbox"/>	0.0.0.0	1000	3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Create | Delete | Set Values | Refresh

In client mode

Force Roaming

Basic | Advanced | Antennas | Allowed Channels | 802.11n | Client | Signal Recorder | Force Roaming

Force Roaming on IP down

Select	Destination Address	Interval [ms]	Max. Lost Packets	WLAN 1
<input type="checkbox"/>	192.111.20.20	2000	2	<input checked="" type="checkbox"/>
<input type="checkbox"/>	0.0.0.0	1000	3	<input type="checkbox"/>

2 entries.

Create | Delete | Set Values | Refresh

Description

Table 1 is only available in access point mode and is divided into the following columns:

- **Radio**
Shows the available WLAN interfaces.
- **Force roaming on link down**
When enabled, the WLAN interface is turned off if there is a connection abort via the Ethernet interface.

The table "Force Roaming on IP down" has the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Destination Address**
Enter the IPv4 address or the FQDN (Fully Qualified Domain Name) of the destination whose reachability will be checked.

Note

Destination address not in the agent IP subnet

If the destination address is not in the agent IP subnet, a gateway must be entered for "Layer 2 > Agent IP".

The Base Bridge mode "802.1Q VLAN Bridge"

If you have configured the "Based Bridge Mode" "802.1Q VLAN Bridge" in "Layer 2 > VLAN", pings are sent into the management VLAN.

6.6 "Interfaces" menu

- **Interval [ms]**
Specify the interval at which pings are sent.
- **Max. Lost Packets**
Specify the maximum number of consecutive lost ping responses. When this number is reached for a destination address, this destination address counts as being unreachable (down).
- **VAP X.Y** (in access point mode)
Specify which VAP interface will be monitored.
- **WLAN 0/X** (in client mode)
Specify which WLAN interface will be monitored.

Procedure

Creating force roaming

1. Click the "Create" button.
2. Make the following settings:
 - Destination address
 - Interval
 - Max. Lost Packets
3. Specify through which destination address the following interface will be monitored:
 - VAP interface (in access point mode)
 - WLAN interface (in client mode)
4. Click the "Set Values" button.

Deleting force Roaming

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.

6.6.2.12 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 in client mode.

The WLAN interface of the SCALANCE W700 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 and that a firmware version > 6.1 is installed on the access point. 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-hand side the user signal of the client / access point is displayed in real time according to the color scheme. The gray line shows the background noise.
If the client has an iPCF-MC connection, the user signal of the management channel is shown with a black line.
- 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.
If the client has an iPCF-MC connection, the user signal of the management channel is shown with an additional black line.
 - 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 on the left-hand side the transfer attempts and the data rate of the client / access point are displayed according to the color scheme.
- 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. The individual colors are described again under the graphic.

- 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 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 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 setting "Bidirectional Recording" 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
- CL M-Signal [dBm]
If the client has an iPCF-MC connection, the user signal of the management channel is displayed.
- 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 8000 measurements, the last 8000 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 11n > V6.1 and SCALANCE W1700 11ac > V1.0.
- **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.
- If you have activated iPCF, set as low a cycle time on the access point as possible for the measurements.
- Make sure that there is enough data communication during the measurement because the statistics functions evaluate incoming data frames.
- The measurement path should be traveled 2 to 3 times with the same parameters to find out whether losses of the user data signal always occur 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
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 8000 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

6.6 "Interfaces" menu

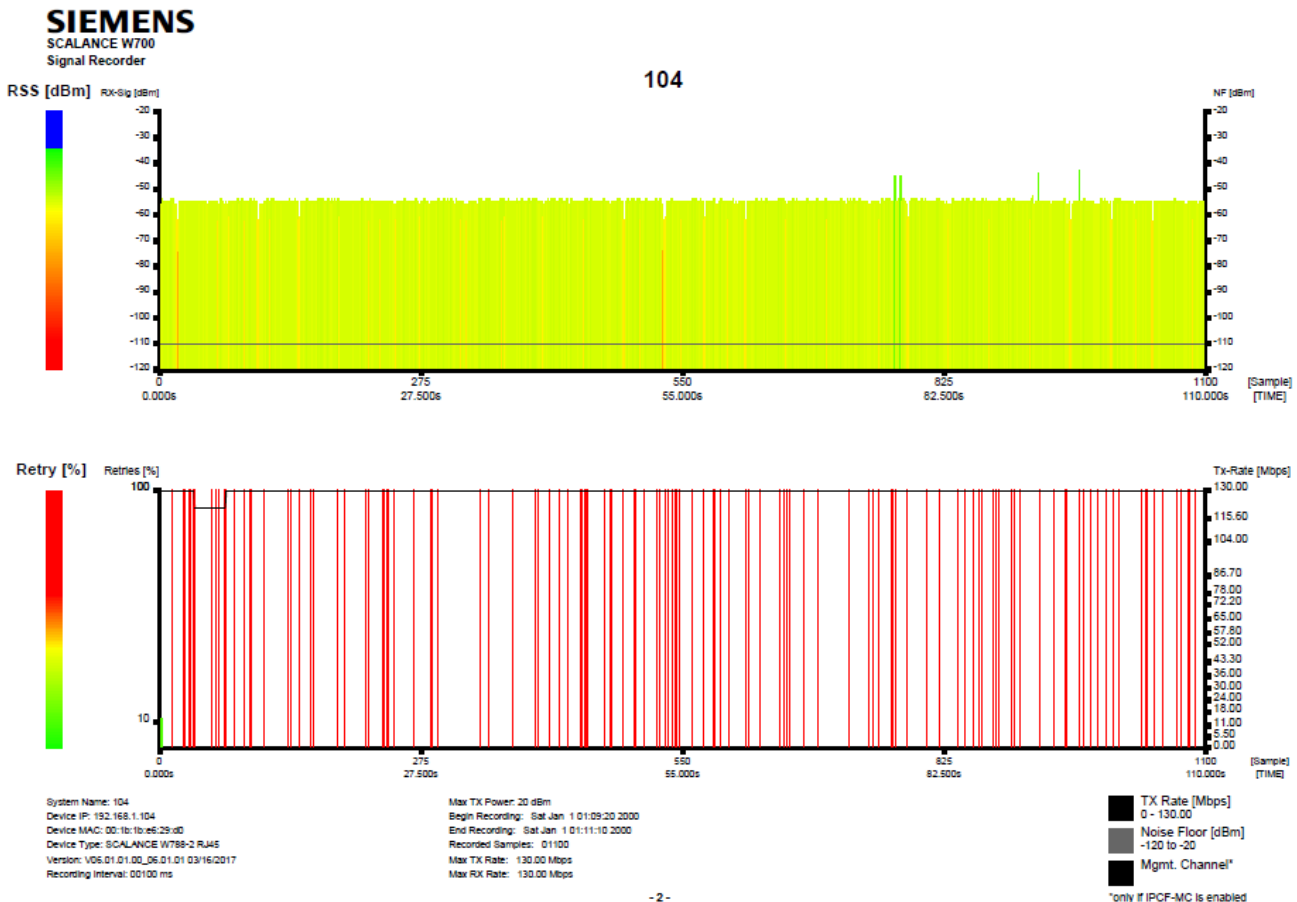
to the appearance in the Web Based Management. If the client changes the access point (roaming) during the measurement, this is indicated by vertical black bars with a black square at the tip.

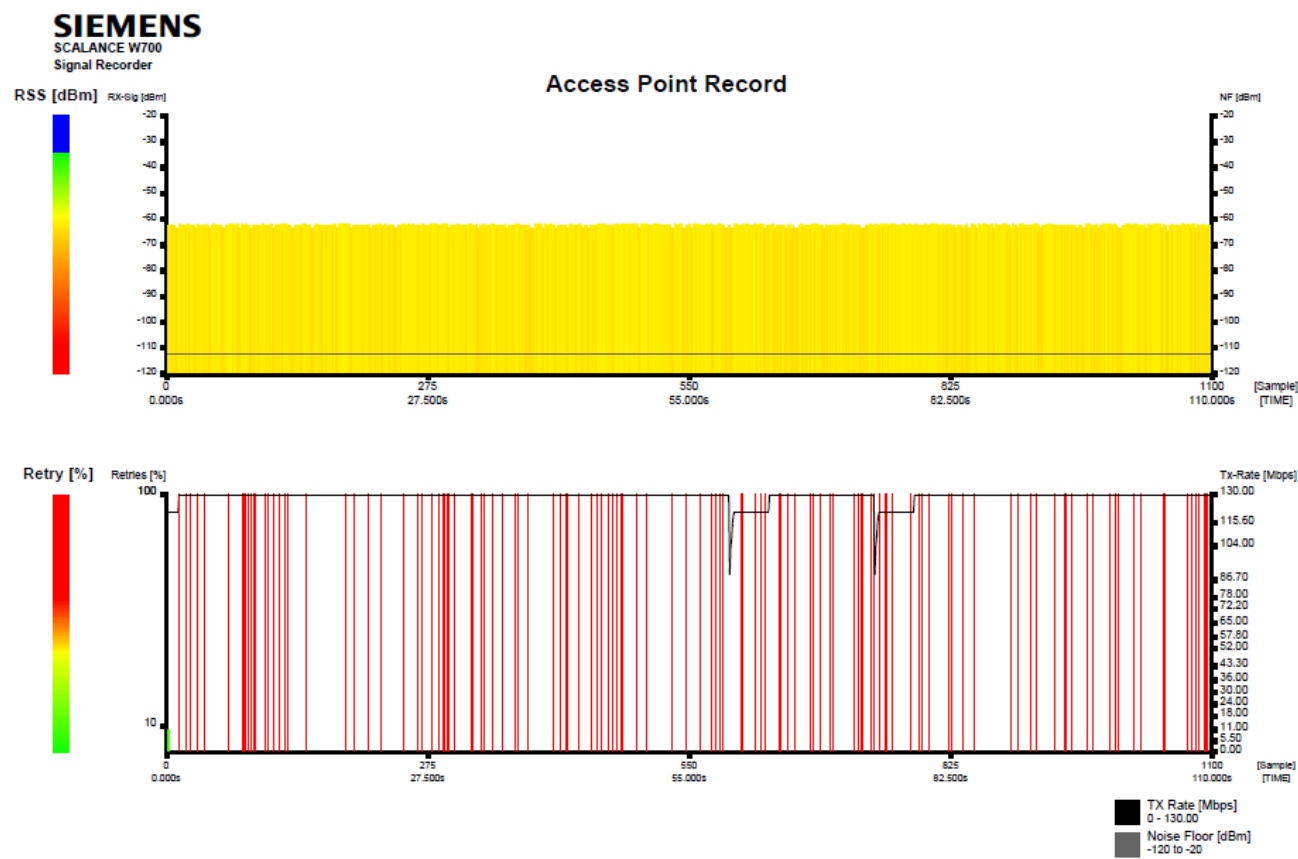
The display is divided into two areas:

- Client
Represents the measurement of the client.
- 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 and that a firmware version > 6.1 is installed on the access point. 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.

If the client has an iPCF-MC connection, the user signal of the management channel is shown with an additional black line.

Below the graphic, the configuration data of the client is displayed.





Example of a generated PDF file

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.

Sample	Timestamp	Sig%	dBm	NF	RSSI	Roam	Ch	Retry%	HT-40	TX-Rate	RX-Rate	Con-St	M-Sig	M-ChM	NF
1	01:09:20:090	78	-58	-110	39	0	181	11	-	130.00	121.50	1	---	---	---
		63	-83	-112	32			8							

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

6.6 "Interfaces" menu

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. 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
- HT-40
The channel bandwidth 40 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

Note

The columns that relate to the management channel only contain a value if there is an iPCF-MC connection.

- M-Ch
The management channel
- M-Sig
The effective user data signal of the management channel
- M-NF
The background noise of the management channel
- AP System Name
The system name of the access point

6.6 "Interfaces" menu

System Name:	104		
Device IP:	192.168.1.104		
Device MAC:	00:1b:1b:e6:29:d0		
Device Type:	SCALANCE W788-2 RJ45		
Version:	V06.01.01.00_06.01.01.03/16/2017		
Recording Interval:	00:100 ms		
Max TX Power:	20 dBm		
Begin Recording:	Sat Jan 1 01:09:20 2000		
End Recording:	Sat Jan 1 01:11:10 2000		
Recorded Samples:	01100		
Max TX Rate:	130.00 Mbps		
Max RX Rate:	130.00 Mbps		

R1 Anten	Gain: 3 dBi	Add. Attenua	Cable length: 0 m
R1 Anten	Gain: 3 dBi	Add. Attenua	Cable length: 0 m
R1 Anten	Gain: 0 dBi	Add. Attenua	Cable length: 0 m

				AP RX-	CL RX-	AP RX-	CL NF	AP NF	CL	AP			CL	AP	Con		HT-	Scan	TX-	RX-	M-Ch	M-Sig	M-NF	AP System
Sample	Timestamp	BSSID	CL RX-Signal	Sign	Sign	Sign	[dBm]	[dBm]	RSSI	RSSI	Roam	Retry	Retry	Stations	Operati ng Ch.	40	Ch	Rate	Rate					
1	01:09:20:090	00:1b:1b:e6:...	76	63	-56	-63	-110	-112	39	32	0	11	8	1	161	-	161	130.	121.	---	---	---	---	106
2	01:09:20:190	00:1b:1b:e6:...	80	63	-54	-63	-110	-112	41	32	0	0	0	1	161	-	161	130.	121.	---	---	---	---	106
3	01:09:20:290	00:1b:1b:e6:...	76	63	-56	-63	-110	-112	39	32	0	0	0	1	161	-	161	130.	121.	---	---	---	---	106
4	01:09:20:390	00:1b:1b:e6:...	78	63	-55	-63	-110	-112	40	32	0	0	0	1	161	-	161	130.	121.	---	---	---	---	106
5	01:09:20:490	00:1b:1b:e6:...	78	63	-55	-63	-110	-112	40	32	0	0	0	1	161	-	161	130.	121.	---	---	---	---	106

Example of a generated CSV file

6.6.2.13 Spectrum analyzer

Technical information

The frequency range depends on the configuration.

Parameters		Value
Amplitude accuracy	In 2.4 GHz	3 dBm
	In 5 GHz	7 dBm
Resolution bandwidth		330 KHz
Min. signal strength		-100 dBm
Max. signal strength		0 dBm
Analysis time	At 40 MHz	120 ms
	At 20 MHz	95 ms
Update time		1 s.

Representing signals of the frequency range

With the spectrum analyzer you can recognize and represent the electromagnetic signals of a frequency range. You can measure the strength of all signals located in the environment of the access point.

Note

This WBM page is only available in access point mode.

The WLAN interface of the device must be enabled, otherwise the frequency ranges cannot be scanned.

Note

We recommend that you do not use the spectrum analyzer in the change mode "Manual Commit".

Note

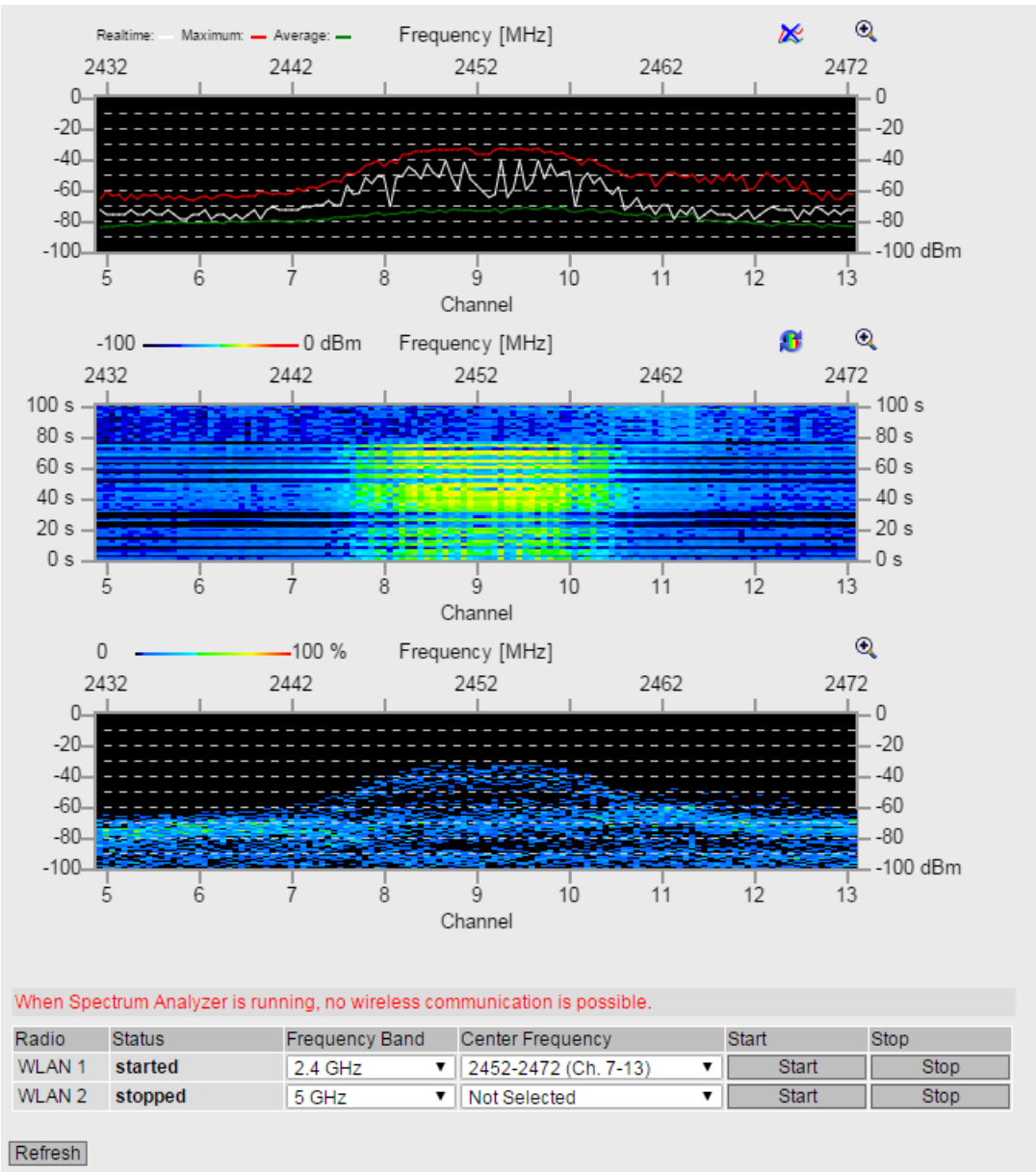
When the spectrum analyzer is started, all WLAN connections are terminated on both WLAN interfaces. The access point then also does not send any beacons.

Note

Do not enable the spectrum analyzer if the device is operating productively. This can influence the performance of the device.

Note

The functionality of the spectrum analyzer does not replace a dedicated spectrum analyzer.

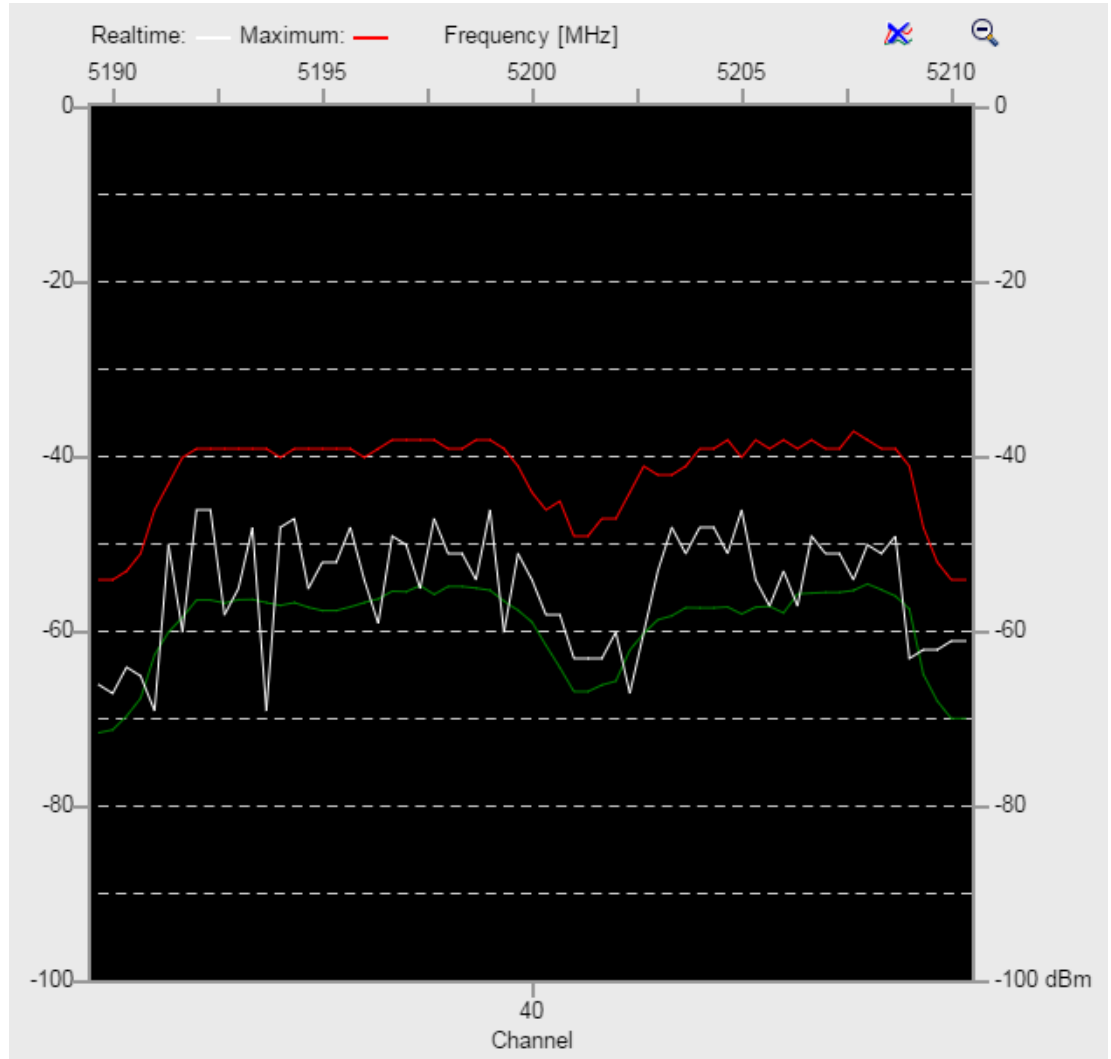


Description

The page contains the following graphics:

In all graphics, the lower x axis shows the channels around the selected center frequency for which the measurements are made. The upper x axis shows the frequency range. The display of the y axis depends on the selected graphic.

- Realtime

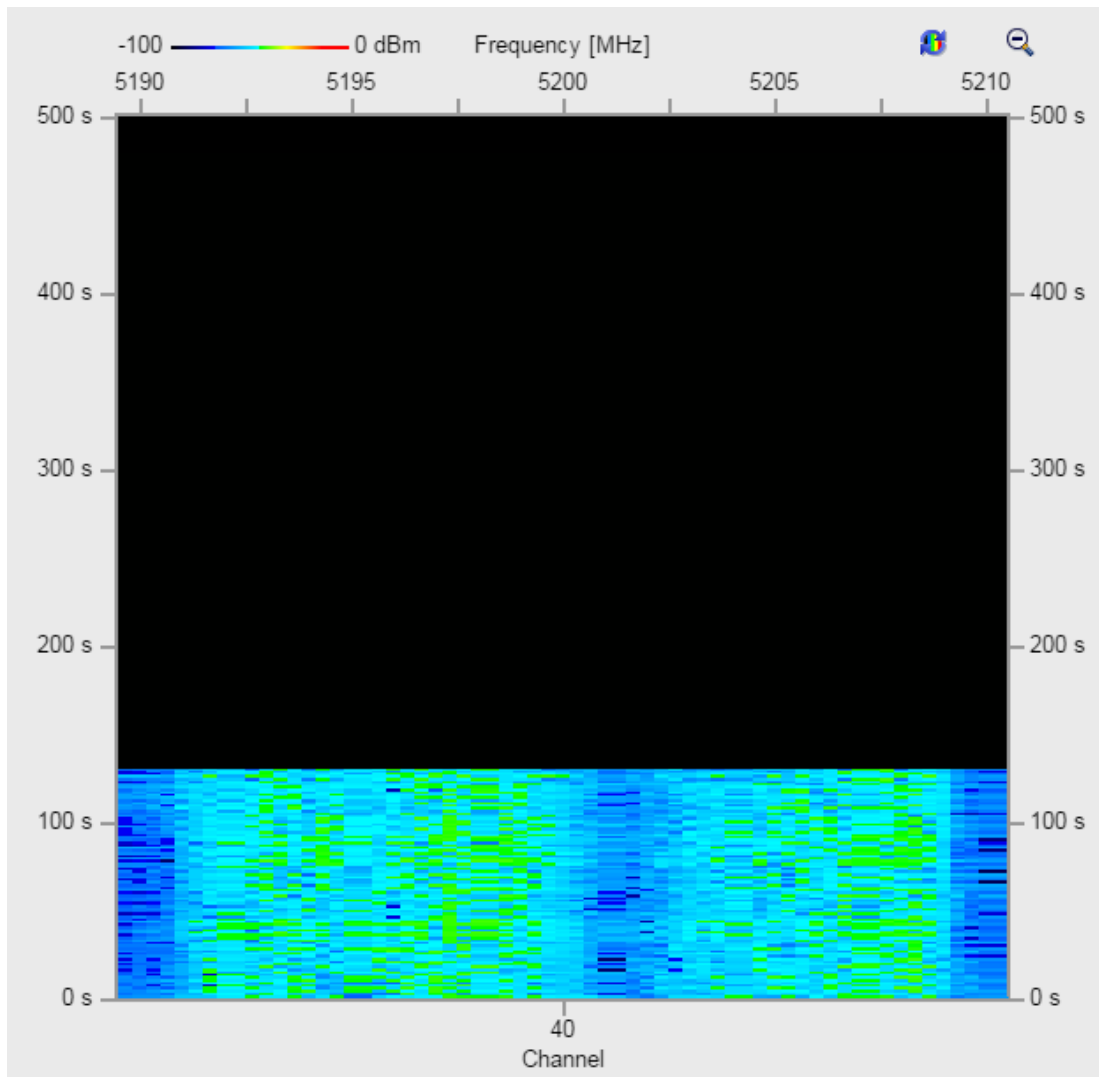


The y axis shows the signal strength in dBm.

The graphic shows the strength of all signals that the access point receives in its environment in the configured frequency range.

The red line shows the maximum values since the start of the measurement. The white line shows the current values. The green line shows the average values.

- Spectrogram

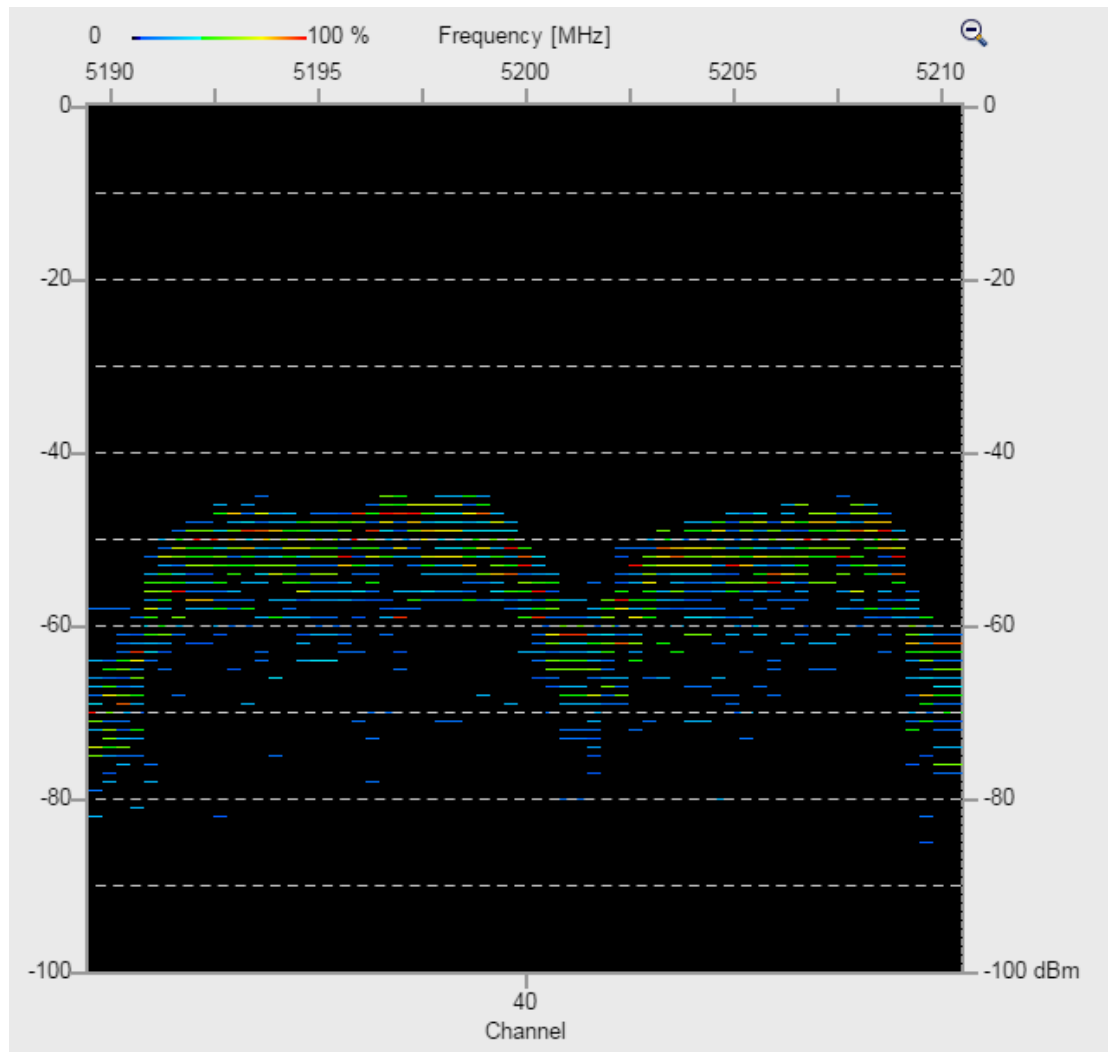


The y axis shows the course of the measured values over time from current (0 s) to the values received before 500 s.

The graphic shows the strength of all signals that the access point receives in its environment in the configured frequency range.

The color depends on the setting for "Color Scheme".

- Density Chart







The y axis shows the signal strength in dBm.

The graphic shows how often signals occur with a certain strength in the configured frequency range.

The color goes from the lowest value (0%) in black to the highest value (100%) in red.

The page contains the following buttons:

- Zoom in  With this icon you only show one graphic type in large format on the page.
- Zoom out  With this icon you return to the view with all three graphic types.

- Color Scheme 
With this icon, you change the color scheme for the graphic type "Spectrogram":
 - The color goes from the lowest value (-100 dBm) in black to the highest value (0 dBm) in red.
 - The color goes from the lowest value (-100 dBm) in red to the highest value (0 dBm) in black.
- Reset 
With this icon you reset the maximum and average values of the graphic type "Realtime".

This table contains the following columns:

- **Radio**
Shows the WLAN interface to which the information applies.
- **State**
Shows the status of the measurement. The following values are possible:
 - Stopped
The measurement was stopped.
 - Started
The measurement is running.
- **Frequency Band**
Specify the frequency band.
- **Center Frequency**
Select the center frequency.
- **Start**
Click the button in this column to start the measurement.
- **Stop**
Click the button in this column to end the measurement.

Procedure

1. Select the required frequency band from the "Frequency Band" drop-down list.
2. Select the required center frequency from the "Center Frequency" drop-down list.
3. Click the "Start" button.
4. To stop the measurement, click the "Stop" button.
5. You can adapt the settings in the second table during the measurement.

6. Change to one of the following menu items to call up the result of the measurement:
 - System > Load&Save > HTTP
Click the "Save" button in the "WLANSpectrumAnalyzer" table row to save the file "wlan_spectrum_analyzer_SCALANCE_W700.zip" in the file system of the connected PC.
 - System > Load&Save > TFTP
If necessary, change the file name "wlan_spectrum_analyzer_SCALANCE_W700.zip" in the "WLANSpectrumAnalyzer" table row. In the table row "WLANSpectrumAnalyzer", 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 a CSV file with the results of the measurement.

Measurement results

CSV file

The CSV file contains information on the configuration of the device and detailed information on all individual measurements and is divided into two areas. The first area contains the configured settings:

- System Name
The system name of the access point
- Device IP
The IP address of the device
- Device MAC
The MAC address of the device
- Recording Interval
The interval between acquisition of two measured values

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

- Sample
The consecutive number of the measurement
- Timestamp
The time stamp
- The following columns show all frequencies of the selected frequency band. The cells are only filled for the frequencies for which a value was measured. The measured values show the signal strength in dBm.

6.6.3 Remote Capture

On this WBM page activate the function "Remote 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 from the recording you can see the content of the frames or filter according to certain contents.

Remote Capture

Interface	Enable
P1	<input type="checkbox"/>
WLAN 1	<input type="checkbox"/>

WLAN Capture Mode:

Own Traffic

☐ Activate after System Restart

Information: The wireless communication is not possible in WLAN Capture Mode 'All Traffic'. WLAN Capture Mode 'Own Traffic' may influence the wireless communication.

Set Values

Refresh

Description

The table contains the following columns:

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

Note

Performance

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

The page contains the following boxes:

- **WLAN Capture Mode (only in access point mode)**

Specify the recording mode for the WLAN interface:

- Own Traffic

In this case, the frames are recorded that were received and sent by the device.

Exception: The data packets dealt with directly by the hardware are not displayed, for example hardware repetitions, acknowledgment frames.

- All Traffic

The access point sends no more frames but records all incoming data packets.

Note

No WLAN communication between access point and clients

If the setting "All Traffic" is used, the access point is no longer reachable for other nodes and loses the connected clients.

- **Activate after System Restart**

- Disabled

After a restart the configuration is reset to the default settings.

- Enabled

The configuration is saved and retained after a restart.

Linking in the interface in Wireshark

Requirement:

- Wireshark V2.0.0 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. Activate the function "Remote Capture" on the device on the WLAN interface.
2. As the receive mode, select "Own Traffic".
3. Click "Set Values" to enable the function.
4. Start Wireshark.
5. Click "Options" in the "Capture" menu. The window "Wireshark - Capture Interfaces" opens.
6. Click the "Manage Interfaces..." button on the "Input" tab. In the following dialog, click on the "Remote Interfaces" tab.
7. To add the interface click on the Plus character in the "Remote Interfaces" tab.
8. In the following dialog for "Host" enter the IPv4 address of the device and for "Port" 2002.
9. Enable "Null authentication" for "Authentication" and click the "OK" button.
10. On the "Remote Interfaces" tab, the host and the interfaces on which the function "Remote Capture" was previously enabled are displayed.

6.7 "Layer 2" menu

- 11. Select the interface and click the "OK" button.
 - 12. To start the recording click "Start". You can obtain additional information about handling the program from Wireshark.
- If you analyze several interfaces you can use a Wireshark instance for each interface.

6.7 "Layer 2" menu

6.7.1 VLAN

6.7.1.1 General

VLAN configuration page

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

Note

Changing the Agent VLAN ID

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

Virtual Local Area Network (VLAN) General

General

Port Based VLAN

Base Bridge Mode:

802.1Q VLAN Bridge

VLAN ID:

Select	VLAN ID	Name	Status	P1	VAP 1.1	WDS 1.1
<input type="checkbox"/>	1		Static	U	U	U

1 entry.

Create

Delete

Set Values

Refresh

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. In this mode, you can create additional VLANs.
- 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 2 VLANs can be defined.
- **Name**
Enter a name for the VLAN. The name only provides information and has no effect on the configuration. The length is a maximum of 32 characters.

- **Status**
Shows the status type of the entry in the 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. Specify the mode of the device.
6. Click the "Set Values" button.

6.7.1.2 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".

Port Based Virtual Local Area Network (VLAN) Configuration

General

Port Based VLAN

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

Port	Priority	Port VID	Acceptable Frames	Ingress Filtering
P1	0	VLAN1	All	<input type="checkbox"/>
VAP 1.1	0	VLAN1	All	<input type="checkbox"/>
WDS 1.1	0	VLAN1	All	<input type="checkbox"/>

Set Values

Refresh

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.
- All
The device forwards all frames.
- No Change
If "No Change" is selected, the entries of the corresponding column in table 2 remain unchanged.

- **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.
- No Change
If "No Change" is selected, the entries of the corresponding column in table 2 remain unchanged.

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.

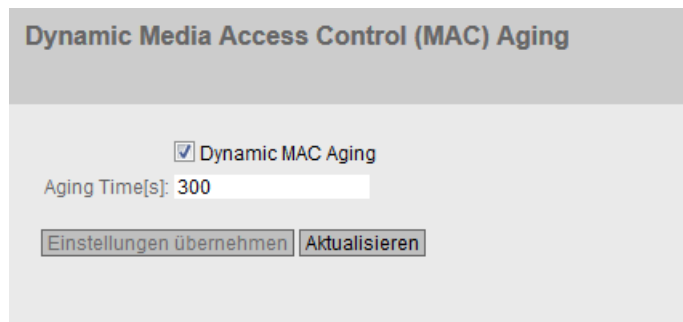
6.7.2 Dynamic MAC Aging

Protocol settings and switch functionality

The device automatically learns the source addresses of the connected nodes. This information is used to forward frames to the nodes specifically involved. This reduces the network load for the other nodes.

If a device does not receive a frame whose source address matches a learnt address within a certain time, it deletes the learnt address. This mechanism is known as "Aging". Aging prevents frames being forwarded incorrectly, for example when an end device (for example a programming device) is connected to a different port.

If the check box is not enabled, a device does not delete learnt addresses automatically.



Dynamic Media Access Control (MAC) Aging

☒ Dynamic MAC Aging

Aging Time[s]: 300

Description

The page contains the following boxes:

- **Dynamic MAC Aging**
Enable or disable the function for automatic aging of learned MAC addresses:
- **Aging Time [s]**
Enter the time in seconds. After this time, a learned address is deleted if the device does not receive any further frames from this sender address. The range of values is from 10 seconds to 630 seconds

Procedure

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

6.7.3 Spanning Tree

6.7.3.1 General

General settings of spanning tree

This is the basic page for spanning tree. Select the compatibility mode from the drop-down list. As default, Multiple Spanning Tree is enabled.

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

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

Note

Client device not as root

Using the configuration of priorities and path costs, make sure that a client device can never become the root node. If a client device becomes the root node the Rapid Spanning Tree function no longer works.

Spanning Tree Protocol (STP) General

General

CIST General

CIST Port

MST General

MST Port

☐ Spanning Tree

Protocol Compatibility: RSTP

Set Values

Refresh

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

Note

If iPCF mode is enabled, only the compatibility modes STP and RSTP are supported.

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.

6.7.3.2 CIST General

MSTP-CIST configuration

The page consists of the following parts.

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

Common Internal Spanning Tree (CIST) General

General	CIST General	CIST Port	MST General	MST Port
---------	--------------	-----------	-------------	----------

Bridge Priority: 32768
Bridge Address: 00-00-00-00-00-00
Root Port: -
Topology Changes: 0
Bridge Hello Time[s]: 2
Bridge Forward Delay[s]: 15
Bridge Max Age[s]: 20

Root Priority: 0
Root Address: 00-00-00-00-00-00
Root Cost: 0
Last Topology Change: -
Root Hello Time[s]: 2
Root Forward Delay[s]: 15
Root Max Age[s]: 20

Reset Counters
☒ Layer-2 Tunnel Admin Edge Port
☒ Layer-2 Tunnel Auto Edge Port

Set Values Refresh

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.

6.7 "Layer 2" menu

- **Root port**
Shows the port via which the switch communicates with the root bridge.
- **Root Cost**
The path costs from this device to the root bridge.
- **Topology Changes / Last Topology Change**
The entry for the device shows the number of reconfiguration actions due to the spanning tree mechanism since the last startup. For the root bridge, the time since the last reconfiguration is displayed as follows:
 - Seconds: sec unit after the number
 - Minutes: min unit after the number
 - Hour: hr unit after the number
- **Topology Changes / Last Topology Change**
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.
- **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. As default, the MAC address of the device is entered here. This value must be the same on all devices that belong to the same MSTP region.
- **Region Version**
Enter the version number of the MSTP region in which the device is located. This value must be the same on all devices that belong to the same MSTP region.
- **Reset Counters**
Click this button to reset the counters on this page.

- **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 or not an end device is connected at all layer 2 tunnel ports.

Procedure

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

6.7.3.3 CIST Port

MSTP-CIST port configuration

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

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

Common Internal Spanning Tree (CIST) Port

General | CIST General | CIST Port | MST General | MST Port

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

Port	Spanning Tree Status	Priority	Cost Calc.	Path Cost	State	Fwd. Trans.	Edge Type	Edge	P.t.P. Type	P.t.P.	Hello Time
P1	<input checked="" type="checkbox"/>	128	0	200000	Disabled	0	Auto	<input type="checkbox"/>	-	<input checked="" type="checkbox"/>	2
VAP 1.1	<input checked="" type="checkbox"/>	128	0	200000000	Disabled	0	Auto	<input type="checkbox"/>	-	<input checked="" type="checkbox"/>	2
WDS 1.1	<input checked="" type="checkbox"/>	128	0	200000000	Disabled	0	Auto	<input type="checkbox"/>	-	<input checked="" type="checkbox"/>	2

Description

Table 1 has the following columns:

- **Column 1**
Shows that the settings made in this table will be adopted for all ports of table 2 after clicking the "Copy to Table" button.
- **Spanning Tree Status**
Select the setting for all ports from the drop-down list. If "No Change" is selected, the entries of the corresponding column in table 2 remain unchanged.
- **Copy to table**
If you click the button, the settings are adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
Shows all available ports and the following interfaces.

- Port X
- WLAN X
- VAP X.Y
- WDS X.Y

- **Spanning Tree Status**
Specify whether or not the port is integrated in the Spanning Tree.

Note

If you disable the "Spanning Tree" 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.

- **Status**

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

- Disabled

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

- Discarding

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

- Listening

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

- Learning

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

- Forwarding

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

- **Fwd. Trans**

Specifies the number of changes from the "Discarding" status to the "Forwarding" status.

- **Edge Type**

Specify the type of the edge port. You have the following options:

- "-"

Edge port is disabled. The port is treated as a "no EdgePort".

- Admin

Select this option when there is always an end device on this port. Otherwise a reconfiguration of the network will be triggered each time a connection is changed.

- Auto

Select this option if you want a connected end device to be detected automatically at this port. When the connection is established the first time, the port is treated as a "no Edge Port".

- Admin/Auto

Select these options if you operate a combination of both on this port. When the connection is established the first time, the port is treated as an Edge Port.

6.7 "Layer 2" menu

- **Edge**

Shows the status of the port.

- Enabled

An end device is connected to this port.

- Disabled

There is a Spanning Tree or Rapid Spanning Tree device at this port.

With an end device, a switch can change over the port faster without taking into account spanning tree frames. If a spanning tree frame is received despite this setting, the port automatically changes to the "Disabled" setting for switches.

- **P.t.P. Type**

Select the required option from the drop-down list. The selection depends on the port that is set.

- P.t.P.

Even with half duplex, a point-to-point link is assumed.

- Shared Media

Even with a full duplex connection, a point-to-point link is not assumed.

Note

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

- "-"

Point to point is determined 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.

6.7.3.4 MST General

Multiple Spanning Tree configuration

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

Multiple Spanning Tree (MST) General

General

CIST General

CIST Port

MST General

MST Port

MSTP Instance ID:

Select

MSTP Instance ID

Root Address

Root Priority

Bridge Priority

VLAN ID

0 entries.

Create

Delete

Refresh

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.

6.7 "Layer 2" menu

- **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.

6.7.3.5 MST Port

Configuration of the Multiple Spanning Tree port parameters

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

Multiple Spanning Tree (MST) Port

General

CIST General

CIST Port

MST General

MST Port

MSTP Instance ID:

1

MSTP Status

Copy to Table

All ports

No Change

Copy to Table

Port	MSTP Instance ID	MSTP Status	Priority	Cost Calc.	Path Cost	State
P1	1	<input checked="" type="checkbox"/>	128	0	200000	Forward
VAP 1.1	1	<input checked="" type="checkbox"/>	128	0	200000000	Discard
VAP 2.1	1	<input checked="" type="checkbox"/>	128	0	401905	Discard

Set Values

Refresh

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.

6.7 "Layer 2" menu

- **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.

6.7.4 DCP Forwarding

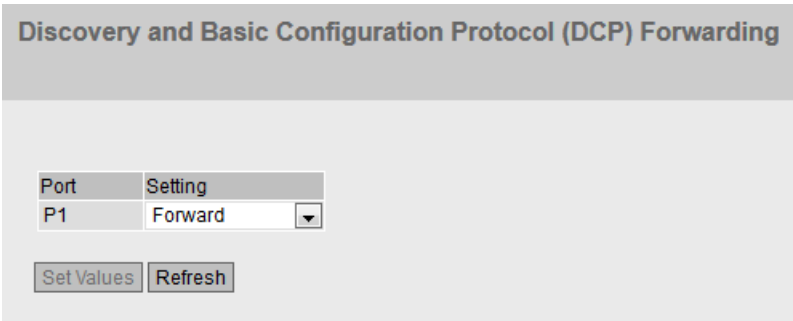
Applications

The DCP protocol is used by STEP 7 and SINEC PNI for configuration and diagnostics. When shipped, DCP is enabled on all ports; in other words, DCP frames are forwarded at all ports. With this option, you can disable the sending of 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.

Note**Empty table**

If you have enabled NAT on the device, the table is empty or will be emptied.



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:
 - Block
No outgoing DCP frames are forwarded via this port. It is nevertheless still possible to receive via this port.
 - Forward
The DCP frames are forwarded via this port.

Procedure

1. Specify whether the port blocks or forwards the DCP frames.
2. Click the "Set Values" button.

6.7.5 LLDP

Identifying the network topology

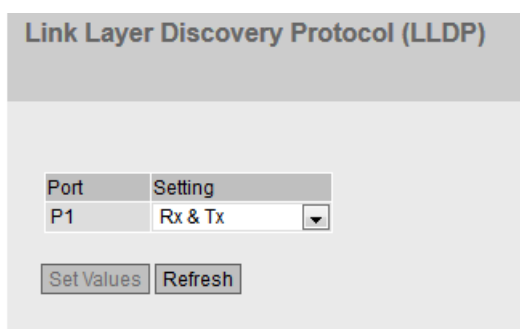
LLDP (Link Layer Discovery Protocol) is defined in the IEEE 802.3AB standard.

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.



Port	Setting
P1	Rx & Tx

Set Values Refresh

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.

6.8 "Layer 3" menu

6.8.1 NAT

6.8.1.1 Basic

Note

This tab is only available in the client mode.

On this page, you specify the basic settings for NAT.

Note

You can find an application example for NAT and NAPT at the following address:
<https://support.industry.siemens.com/cs/ww/en/view/37593580>

IP Network Address Translation (NAT) Settings

Basic **NAPT**

Interface: P1 ▾

☐ Enable NAT

TCP Idle Timeout [s]: 86400

UDP Idle Timeout [s]: 300

Local Interface IP address: 192.168.0.1

Local Interface Subnet Mask: 255.255.255.0

☐ IPv6 Transparent Mode

IPv4 Multicast Forwarding

☐ From Global to Local Interface

☐ From Local to Global Interface

☐ PROFINET Transparent Mode

PROFINET Station Name: station*;pumpe*

Set Values **Refresh**

Description

The page contains the following boxes:

- **Interface**
Select the required Ethernet interface from the drop-down list.
- **Enable NAT**
Enable or disable NAT for the Ethernet interface.
- **TCP Idle Timeout [s]**
Enter the required time in seconds. If no data exchange takes place, the TCP connection is deleted from the translation table when this time has elapsed.
The range of values is 1 to 2147483.
Default setting: 86400 seconds
- **UDP Idle Timeout [s]**
Enter the required time in seconds. If no data exchange takes place, the UDP connection is deleted from the translation table when this time has elapsed.
The range of values is 1 to 2147483.
Default setting: 300 seconds
- **Local Interface IP address**
Enter the local IP address of the Ethernet interface. This IP address is the gateway address of the local device.
- **Local Interface Subnet Mask**
Enter the subnet mask for the local Ethernet.

- **IPv6 Transparent Mode**

When enabled, IPv6 frames are forwarded unchanged between Ethernet and WLAN.

This requires that "Own" is not set for MAC mode and IPv6 is turned off.

If you have set "Manual" for the MAC mode, you need to enter the MAC address of the IPv6 device that receives or sends the IPv6 frames.

- **IPv4 Multicast Forwarding**

Specify whether or not the incoming multicast frames will be forwarded.

- From Global to Local Interface

The multicast frames incoming on the WLAN interface are forwarded via the Ethernet interface into the internal network.

- From Local to Global Interface

The multicast frames incoming on the local Ethernet interface are forwarded via the WLAN interface into the external network.

- **PROFINET transparent mode** (only for W722-1)

With NAT, communication with connected PROFINET devices via WLAN is not possible because they are not visible to the outside.

If you select this setting, you can make individual PROFINET devices visible again to the outside. Frames are also forwarded transparently. The exceptions are made with the PROFINET device names.

"Layer 2 tunnel" must be set in MAC mode for PROFINET transparent mode.

Note

PROFINET devices

When PROFINET transparent mode is activated, the connected PROFINET devices cannot obtain the IP address from a DHCP server. Use a fixed IP address for these devices.

- **PROFINET device name** (only for W722-1)

The PROFINET device name determines which PROFINET devices are allowed to communicate with the outside world despite NAT.

Maximum length: 240 characters. The box must not be empty.

The following characters are permitted: [a ... z] [0 ... 9] and [. ; - *]. Uppercase letters are not allowed.

For device names, you can replace any number of characters with the wildcard asterisk (*).

The asterisk can be anywhere, but may occur only once per device name.

You can specify multiple device names separated by a semicolon.

Examples:

- * (asterisk)

Communication is possible with all connected PROFINET devices.

- pump1

Communication is only possible with this PROFINET device.

- pump*

Stands for the device names that begin with "pump" e.g. pump1, pump2.

There are two pumping stations in a plant, for example. Station 1 contains "pump1" and station 2 contains "pump2". If you use this input, you can import the configuration on both WLAN clients.

- pump*;controller*

Stands for all device names that begin with "pump" or "controller".

6.8 "Layer 3" menu

Procedure

- 1. In the "Local Interface IP address" input box, enter the local IP address of the Ethernet interface.
- 2. In the "Local Interface Subnet Mask" input box, enter the subnet mask for the local Ethernet.
- 3. Enable NAT for the Ethernet interface.
- 4. Enter the PROFINET device name.
- 5. Click the "Set Values" button.

6.8.1.2 NAPT

Note

This tab is only available in the client mode.

On this WBM page, you define the translation list for communication from the global to the local network. Per WLAN client (NAT gateway), 60 entries are possible.

IP Network Address Port Translation (NAPT)

Basic NAPT

Interface: P1

Traffic Type: TCP

Global Port: 100

Local IP Address:

Local Port: 100

Select	Enable	Interface	Traffic Type	Dynamic Global IP	Global IP Address	Global Port	Local IP Address	Local Port
0 entries.								

Create

Delete

Refresh

Description

The page contains the following boxes:

- **Interface**
Interface to which the settings relate. Can only be selected if the device has several interfaces.
- **Traffic Type**
Specify the protocol for which the address assignment is valid. TCP and UDP frames must have parameters set separately.

- **Global Port**
Enter the global port. Incoming frames with this port as the destination port are forwarded. If the setting is intended to apply to a port range, enter the range with start port "-" end port, for example 30 - 40.

Note

If the port is already occupied by a local service, for example Telnet, a warning is displayed. In this case, avoid using TCP port 23 (Telnet), port 22 (SSH), ports 80/443 (http/https: reachability of the client with the WBM) and UDP port 161 (SNMP) as global port.

- **Local IP Address**
Enter the IP address of the node in the local network.
- **Local Port**
Enter the number of the port. This is the new destination port to which the incoming frame will be forwarded. If the setting is intended to apply to a port range, enter the range with start port "-" end port, for example 30 - 40.
If the local port and global port are the same, the frames will be forwarded without port translation.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Activate**
Select the check box in the required row. The entry is used for the address assignment
- **Interface**
Shows the interface to which the settings relate.
- **Traffic Type**
Shows whether UDP or TCP frames are assigned to the global port.
- **Dynamic Global IP**
Shows whether or not dynamic address translation is used.
- **Global IP Address**
Shows the global IP address to which the local IP address will be translated.
- **Global Port**
Shows the global port.
- **Local IP Address**
Shows the IP address of the node in the local network.
- **Local Port**
Shows the number of the local port.

Procedure

1. From the "Traffic Type" drop-down list, select the protocol for which the address assignment is valid.
2. Enter the number of the global port or a port range in "Global Port".
3. Enter the IP address of the node in the local network in "Local IP Address".

6.9 "Security" menu

- 4. Enter the number of the local port or a port range in "Local Port".
- 5. Click the "Create" button. A new entry is generated in the table.
- 6. Click the "Set Values" button. The device is restarted.

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
<input type="checkbox"/>	admin	admin	System defined local user
<input type="checkbox"/>	Service	user	

<

2 entries.

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: | ? " ; :
The characters for Space and Delete must also not be included.

Note

User name cannot be changed

After creating a user, the user name can no longer be modified.

If a user name needs to be changed, the user must be deleted and a new user created.

Note

User names: admin

You can configure the device with this user name.

When you log in for the first time or log in after a "Restore Factory Defaults and Restart", you are prompted to change the pre-defined password "admin". You can also rename the "admin" user preset in the factory once. Afterwards, renaming "admin" is no longer possible.

Note

Default user "user" set in the factory

As of firmware version 6.0 the default user set in the factory "user" is no longer available when the product ships.

If you update a device to the firmware V6.0 the default user set in the factory "user" is initially still available. If you reset the device to the factory settings ("Restore Factory Defaults and Restart") the default user set in the factory "user" is deleted.

You can create new users with the role "user".

- **Password Policy**

Shows which password policy is being used.

- High
Password length: at least 8 characters, maximum 128 characters
At least 1 uppercase letter
At least 1 special character
At least 1 number
- Low
Password length: at least 6 characters, maximum 128 characters

You configure the password policy on the page "Security > Passwords > Options".

- **Password**

Enter the password. The strength of the password depends on its length and complexity.

- **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.

User Roles

Local Users

Roles

Groups

Role Name:

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

5 entries.

Create

Delete

Set Values

Refresh

Description

The page contains the following:

- **Role Name**
Enter the name for the role. The name must meet the following conditions:
 - It must be unique.
 - It must be between 1 and 64 characters long.

Note**Role name cannot be changed**

After creating a role, the name of the role can no longer be changed.

If a name of a role needs to be changed, the role must be deleted and a new role created.

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:

- **0**
If authentication fails, the user is assigned the role. Access to the device is not possible.
- **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.

For 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.You can find information on the permitted characters in Appendix G of the WBM (Page 391).

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

6.9.2.1 Passwords

Configuration of the passwords of users

Note

If you are logged in via a RADIUS server, you cannot change any passwords.

On this page, you can change passwords of users. 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 on as user, you can only change your own password.

Description

- **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.
 - High
Password length: at least 8 characters, maximum 128 characters
At least 1 uppercase letter
At least 1 special character
At least 1 number
 - Low
Password length: at least 6 characters, maximum 128 characters
- **New Password**
Enter the new password for the selected user.
It cannot contain the following characters:
 - § ? " ; :
 - The characters for Space and Delete also cannot be contained.
- **Password Confirmation**
Enter the new password again to confirm it.

Procedure

1. Enter the valid password for the currently logged in user in the "Current User Password" input box.
2. From the "User Account" drop-down list, select the user whose password you want to change.
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 "admin" you will be prompted to change the password.

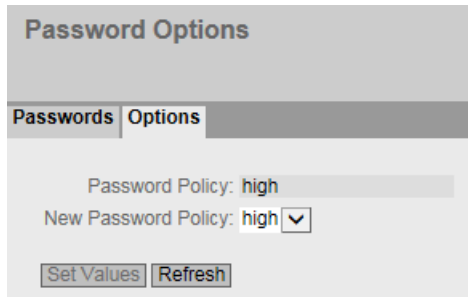
Note

Changing the password in Trial mode

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

6.9.2.2 Options

On this page, you specify which password policy will be used when assigning new passwords.



The screenshot shows a web interface titled "Password Options". It has two tabs: "Passwords" and "Options", with "Options" being the active tab. Below the tabs, there are two labels: "Password Policy: high" and "New Password Policy: high" followed by a dropdown arrow. At the bottom of the form are two buttons: "Set Values" and "Refresh".

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 uppercase letter
At least 1 special character
At least 1 number
 - Low
Password length: at least 6 characters, maximum 128 characters

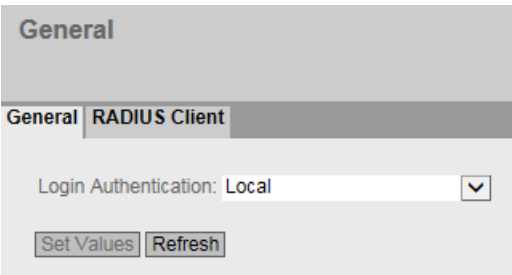
6.9.3 AAA

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.



The screenshot shows a web interface for configuring a RADIUS client. At the top, there's a 'General' tab selected. Below it, the 'RADIUS Client' section is visible. A dropdown menu for 'Login Authentication' is set to 'Local'. Below the dropdown are two buttons: 'Set Values' and 'Refresh'.

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.

Remote Authentication Dial In User Service (RADIUS) Client

General | RADIUS Client

RADIUS Authorization Mode: Vendor Specific

Select	Auth. Server Type	RADIUS Server Address	Server Port	Shared Secret	Shared Secret Conf.	Max. Retrans.	Primary Server	Test	Test Result
<input type="checkbox"/>	Login	192.168.16.2	1812	*****	*****	3	no	<input type="button" value="Test"/>	Not reachable

1 entry.

Description of the displayed boxes

The page contains the following boxes:

- RADIUS Authorization Mode**
For the login authentication, the RADIUS authorization mode specifies how the rights are assigned to the user with a successful authentication.
 - Conventional
In this mode the user is logged in with administrator rights if the server returns the value "Administrative User" to the device for the attribute "Service Type". In all other cases the user is logged in with read rights.
 - SiemensVSA
In this mode the assignment of rights depends on whether and which group the server returns for the user and whether 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.
- RADIUS Server Address**
Enter the IPv4 address or the FQDN (Fully Qualified Domain Name) of the RADIUS server.
- Server Port**
Here, enter the input port on the RADIUS server. As default, input port 1812 is set. The range of values is 1 to 65535.
- Shared Secret**
Enter your access ID here. The range of values is 1...128 characters
- Shared Secret Conf.**
Enter your access ID again as confirmation.
- Max. Retrans.**
Here, enter the maximum number of retries for an attempted request.
The initial connection attempt is repeated the number of times specified here before another configured RADIUS server is queried or the login counts as having failed. As default 3 retries are set, this means 4 connection attempts. The range of values is 1 to 5.
- Primary Server**
Using the options in the drop-down list, specify whether or not this server is the primary server. You can select one of the options "yes" or "no".

- **Test**
With this button, you can test whether or not the specified RADIUS server is available. The test is performed once and not repeated cyclically.
- **Test Result**
Shows whether or not the RADIUS server is available:
 - Not reachable
The IP address is not reachable.
The IP address is reachable, the RADIUS server is, however, not running.
 - Reachable, key not accepted
The IP address is reachable, the RADIUS server does not, however accept the shared secret.
 - Reachable, key accepted
The IP address is reachable, the RADIUS server accepts the specified shared secret.

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 WLAN

6.9.4.1 Basic (Access Point)

Safety levels

To make the network secure, authentication and encryption are used. On this page, you specify the security settings.

Note

WLAN mode IEEE 802.11 n

With devices operated in WLAN mode IEEE8002.11n only WPA2 (WPA2-PSK and WPA2 Radius) encryption is possible.

WLAN Security Settings

BasicAP CommunicationAP RADIUS AuthenticatorKeys

Port	Authentication Type	Encryption	Cipher	WPA(2) Pass Phrase	WPA(2) Pass Phrase Confirmation	Default Key
VAP 1	Open System	<input type="checkbox"/>	WEP			Key 1

Set ValuesRefresh

Description

The table has the following columns:

- **Interface**
Shows the available interfaces.
- **Authentication Type**
Select the type of authentication. The selection depends on the operating mode and the transmission standard.
 - Open System
There is no authentication. Encryption with a fixed (unchanging) WEP key can be selected as an option. To use the key, enable "Encryption". You define the WEP key on the "Keys" page.
 - Shared Key
In Shared Key authentication, a fixed key is stored on the client and access point. This WEP key is then used for authentication and encryption. You define the WEP key on the "Keys" page.

Note

If you use "Open System" with "Encryption" or "Shared Key", Key 1 must always be set on the "Keys" page.

- WPA (RADIUS)
Wi-Fi Protected Access is a method specified by the Wi-Fi Alliance to close security gaps in WEP. Authentication using a server is stipulated (802.1x). The dynamic exchange of keys at each data frame introduces further security.
- WPA-PSK
WPA Pre Shared Key (WPA-PSK) is a weakened form of WPA. In this method, authentication is not established by a server but is based on a password. This password is configured manually on the client and server.
- WPA2 (RADIUS)
WPA2 (Wi-Fi Protected Access 2) is a further development of WPA and implements the functions of the IEEE 802.11i security standard. WPA authentication works, however, without the RADIUS server.
- WPA2-PSK
WPA2-PSK is based on the 802.11i standard. WPA authentication works, however, without a RADIUS server. Instead of this, a WPA(2) key (WPA(2) Pass Phrase) is stored on each client and access point. The WPA(2) Pass Phrase is used for authentication and further encryption.
- WPA/WPA2-Auto-PSK
Setting with which an access point can process both the "WPA-PSK" and the "WPA2-PSK" type of authentication. This is necessary when the access point communicates with different clients, some using "WPA-PSK" and others "WPA2-PSK". The same encryption method is set on the clients.
- WPA/WPA2-Auto
Setting with which an access point can process both the "WPA" and the "WPA2" type of authentication. This is necessary when the access point communicates with different clients, some using "WPA" and others "WPA2". The same encryption method is set on the clients.

6.9 "Security" menu

- **Encryption**

Encryption protects the transferred data from eavesdropping and corruption. You can only disable encryption if you have selected "Open System" for authentication. All other security methods include both authentication and encryption.

- **Cipher**

Select the encryption method. The selection depends on the transmission standard.

- **AUTO**

AES or TKIP is selected automatically depending on the capability of the other station.

- **WEP**

WEP (Wired Equivalent Privacy)

A symmetrical stream encryption method with only 40- or 104-bit long keys based on the RC4 algorithm (Ron's Code 4).

- **TKIP (Temporal Key Integrity Protocol)**

A symmetrical encryption method with the RC4 algorithm (Ron's Code 4). In contrast to the weak WEP encryption, TKIP uses changing keys derived from a main key. TKIP can also recognize corrupted data frames.

- **AES (Advanced Encryption Standard)**

Strong symmetrical block encryption method based on the Rijndael algorithm that further improves the functions of TKIP.

Note

To provide better protection of your data against attacks, use WPA2/ WPA2-PSK with AES.

- **WPA(2) Pass Phrase**

Enter a WPA(2) key here. This WPA(2) key must be known 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.

- **WPA(2) Pass Phrase Confirmation**

Confirm the entered WPA(2) pass phrase.

- **Default Key**

Specify the WEP key used to encrypt the data. You define the WEP key on the "Keys" page.

Procedure

1. Select the required security settings. Which settings are possible depends on the "Authentication Type" you have selected.

Authentication Type	Encryption	Cipher	Encryption key source
Open System	disabled	--	--
Open System	enabled	WEP	Default Key
Open System	enabled	AES ¹⁾	Default Key (128-bit)
Shared Key	enabled	WEP	Default Key
WPA (RADIUS)	enabled	Auto/TKIP/AES	RADIUS Server
WPA-PSK	enabled	Auto/TKIP/AES	WPA(2) Pass Phrase
WPA2 (RADIUS)	enabled	Auto/TKIP/AES	RADIUS Server
WPA2-PSK	enabled	Auto/TKIP/AES	WPA(2) Pass Phrase
WPA/WPA2-AutoPSK	enabled	Auto/TKIP/AES	WPA(2) Pass Phrase
WPA/WPA2-Auto (RADIUS)	enabled	Auto/TKIP/AES	RADIUS Server

¹⁾ available only with iPCF, with iPCF-HT or with iPCF-MC

2. Click the "Set Values" button.

6.9.4.2 Basic (Client)

Safety levels

To make the network secure, authentication and encryption are used. On this page, you specify the security settings.

Note

WLAN mode IEEE 802.11 n

With devices operated in WLAN mode IEEE802.11n only WPA2 (WPA2-PSK and WPA2 Radius) encryption is possible.

iPCF, iPCF-HT or iPCF-MC mode activated

If iPCF, iPCF-HT or iPCF-MC mode is enabled, only "iPCF authentication" with or without the AES encryption is supported with security context 1.

WLAN Security Settings

Basic | Client RADIUS Supplicant | Keys

Security Context	Authentication Type	Encryption	Cipher	WPA(2) Pass Phrase	WPA(2) Pass Phrase Confirmation	Default Key
1	Open System	<input type="checkbox"/>	WEP			Key 1

1 entry.

Description

The table has the following columns:

- **Select**
Select the row you want to delete. Select a check box in this column and click the "Delete" button to delete an entry in the list.
- **Security Context**
Shows the number of the entry. If you create a new entry, a new line with a unique number is created.
You can create up to 8 security contexts. The security context 1 cannot be deleted.

- **Authentication Type**

Select the type of authentication. The selection depends on the operating mode and the transmission standard.

- **Open System**

There is no authentication. Encryption with a fixed (unchanging) WEP key can be selected as an option. To use the key, enable "Encryption". You define the WEP key on the "Keys" page.

- **Shared Key**

In Shared Key authentication, a fixed key is stored on the client and access point. This WEP key is then used for authentication and encryption. You define the WEP key on the "Keys" page.

- **WPA (RADIUS)**

Wi-Fi Protected Access is a method specified by the Wi-Fi Alliance to close security gaps in WEP. Authentication using a server is stipulated (802.1x). The dynamic exchange of keys at each data frame introduces further security.

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 established by a server but is based on a password. This password is configured manually on the client and server.

- **WPA2 (RADIUS)**

WPA2 (Wi-Fi Protected Access 2) is a further development of WPA and implements the functions of the IEEE 802.11i security standard. WPA authentication works, however, without the RADIUS server.

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. WPA authentication works, however, without a RADIUS server. Instead of this, a WPA(2) key (WPA(2) pass phrase) is stored on each client and access point. The WPA(2) pass phrase is used for authentication and further encryption.

- **WPA/WPA2-Auto-PSK**

Setting with which an access point can process both the "WPA-PSK" as well as the "WPA2-PSK" type of authentication. This is necessary when the access point communicates with different clients, some using "WPA-PSK" and others "WPA2-PSK". The same encryption method is set on the clients.

- **WPA/WPA2-Auto**

Setting with which an access point can process both the "WPA" as well as the "WPA2" type of authentication. This is necessary when the access point communicates with different clients, some using "WPA" and others "WPA2". The same encryption method is set on the clients.

- **iPCF authentication**

Authentication with optional AES encryption. Authentication is set automatically if iPCF, iPCF-HT or iPCF-MC mode is enabled on the WLAN interface. If you want encryption with AES, only keys with a 128 bit key length are supported.

- **Encryption**

Encryption protects the transferred data from eavesdropping and corruption. You can only disable encryption if you have selected "Open System" for authentication. All other security methods include both authentication and encryption.

- **Cipher**

Select the encryption method. The selection depends on the transmission standard.

- **AUTO**

AES or TKIP is selected automatically depending on the capability of the other station.

- **WEP**

WEP (Wired Equivalent Privacy)

A symmetrical stream encryption method with only 40- or 104-bit long keys based on the RC4 algorithm (Ron's Code 4).

- **TKIP (Temporal Key Integrity Protocol)**

A symmetrical encryption method with the RC4 algorithm (Ron's Code 4). In contrast to the weak WEP encryption, TKIP uses changing keys derived from a main key. TKIP can also recognize corrupted data frames.

- **AES (Advanced Encryption Standard)**

Strong symmetrical block encryption method based on the Rijndael algorithm that further improves the functions of TKIP.

Note

To provide better protection of your data against attacks, use WPA2/ WPA2-PSK with AES.

- **WPA(2) Pass Phrase**

Enter a WPA(2) key here. This WPA(2) key must be known 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.

- **WPA(2) Pass Phrase Confirmation**

Confirm the entered WPA(2) pass phrase.

- **Default Key**

Specify the WEP key used to encrypt the data. You define the WEP key on the "Keys" page.

Procedure

1. To create a new security context, click the "Create" button.
2. Select the required security settings. The settings that are possible depend on the "Authentication Type" you have selected.
When iPCF, iPCF-HT or iPCF-MC mode is enabled, it is not possible to select the "Authentication Type".
3. Click the "Set Values" button.

6.9.4.3 AP communication

Communications options

On this page, you specify the type of communication allowed by the access point.

Note

This tab is available only in access point mode.

Access Point Communication Filters

Basic

AP Communication

AP RADIUS Authenticator

Keys

Radio	Port	within own VAP	with Ethernet	Client Limiter	max. Clients
WLAN 1	VAP 1.1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	64

Set Values

Refresh

Description

The table has the following columns:

- **Radio**
Shows the available WLAN interfaces.
- **Port**
Shows the VAP interface.

6.9 "Security" menu

- **within own VAP**

- Enabled
Clients logged on to the same VAP interface of an access point can communicate with each other.
- Disabled
Option is disabled.

Note

"within own VAP" function disabled

if the "within own VAP" function is disabled the various WLAN clients can no longer see each other. This means that Address Collision Detection (ACD) also no longer works reliably.

- **with Ethernet**

- Enabled
Clients can communicate via the Ethernet interface of the access point.
- Disabled
Option is disabled.

- **Client limiter**

- Enabled
The number of WLAN clients that can be logged on simultaneously is limited.
- Disabled
Option is disabled.

- **Max. clients**

Set the maximum number of WLAN clients that can connect to this interface at the same time.
If the number is exceeded, additional clients are rejected.

6.9.4.4 AP RADIUS Authenticator

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.

Note

This WBM page is only available in access point mode.

AP 802.1X Authenticator

Basic

AP Communication

AP RADIUS Authenticator

802.11r

Keys

Reauthentication Mode: -

Reauthentication Interval [s]: 3600

Server IP Address	Server Port	Shared Secret	Shared Secret Confirmation	Max. Retransmissions	Primary Server	Status
	1812			2	no	<input type="checkbox"/>
	1812			2	no	<input type="checkbox"/>

Set Values

Refresh

Description

The page contains the following boxes:

- Reauthentication Mode**
Specify who sets the time after which the clients are forced to reauthenticate.
 - (disabled)
Reauthentication mode is disabled.
 - Server
Enables time management on the server.
 - Local
Enables local time management. In "Reauthentication Interval", specify the time of validity.
- Reauthentication Interval [s]**
If time management is local, enter the period of validity of the authentication in seconds. The minimum time is 1 minute (enter 60), the maximum time is 12 hours (enter 43200). The default is one hour (3,600 seconds).

The table has the following columns:

- Server IP Address**
Here, enter the IP address or the FQDN name of the RADIUS server.
- Server Port**
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.

6.9 "Security" menu

- **Primary Server**
Specify whether or not this server is the primary server.
 - Yes: Primary server
 - No: Backup server.
- **State**
With this check box, you can enable or disable the RADIUS server

Procedure

Entering a new server

To display a new server, follow the steps below:

1. In the relevant row, enter the following data in the input boxes:
 - IP address or FQDN name of the RADIUS server.
 - Port number of the input port
 - Password
 - Confirmation of the password
 - Maximum number of transmission retries
 - Primary server
2. Click the "Set Values" button.

Modifying servers

1. In the relevant row, enter the following data in the input boxes:
 - Server IP address
 - Port number of the input port
 - Password
 - Confirmation of the password
 - Maximum number of transmission retries
 - Primary server
2. Click the "Set Values" button.

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

6.9.4.5 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.

Client 802.1X Supplicant

Basic Client RADIUS Supplicant

Minimum TLS Version: TLSv1.2

Security Context	Dot1X User Name	Dot1X User Password	Dot1X User Password Confirmation	Dot1X Check Server Certificate	Dot1X EAP Types
1				<input type="checkbox"/>	AUTO

Set Values Refresh

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 389)".

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 the Dot1X server certificate**
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.

6.9.4.6 Keys

Specifying the WEP key

To allow you to enable the encryption for the "Open System" and "Shared Key" authentication methods, you must first enter at least one key in the key table.

Key Table

Basic

Client RADIUS Supplicant

Keys

Key 1	Key 1 Confirmation	Key 2	Key 2 Confirmation	Key 3	Key 3 Confirmation	Key 4	Key 4 Confirmation

Set Values

Refresh

Description

The table has the following columns:

- Radio**
Shows the available WLAN interfaces.
- Key 1 - 4**
Enter the WEP key or the AES key.
For the WEP key, characters of the ASCII code from 0x20 to 0x7E or hexadecimal characters from 0x00 to 0xFF are permitted.
If iPCF or iPCF-MC mode is enabled, only the encryption method AES with 128-bit key length is supported.
You can choose between the following key lengths:
 - 5 or 13 ASCII or 10 or 26 hexadecimal characters (40/104 bits)
 - 16 ASCII or 32 hexadecimal characters (128 bits)

Note

The hexadecimal characters are entered without being preceded by "0x". One hexadecimal character codes four bits. The entries "ABCDE" (ASCII characters) and "4142434445" (hexadecimal characters) are therefore the same because the ASCII character "A" has hexadecimal code "0x41".

- Key 1 - 4 Confirmation**
Confirm the WEP key.

Procedure

- Enter at least one WEP key.
- Click the "Set Values" button.

6.9.5 MAC ACL

6.9.5.1 Rules Configuration

On this page, you specify the access rules for the MAC-based Access Control List. Using the MAC-based ACL, you can specify whether frames of certain MAC addresses are forwarded or discarded.

MAC Access Control List Configuration

Rules Configuration
Ingress Rules
Egress Rules

Select	Rule Number	Source MAC	Dest. MAC	Action	Ingress Interfaces	Egress Interfaces
<input type="checkbox"/>	1	00-00-00-00-00-00	00-00-00-00-00-00	Forward <input type="button" value="v"/>	P0.1	
<input type="checkbox"/>	2	00-00-00-00-00-00	00-00-00-00-00-00	Forward <input type="button" value="v"/>	P0.1	
<input type="checkbox"/>	3	00-00-00-00-00-00	00-00-00-00-00-00	Forward <input type="button" value="v"/>	P0.1	
<input type="checkbox"/>	4	00-00-00-00-00-00	00-00-00-00-00-00	Forward <input type="button" value="v"/>	P0.1	
<input type="checkbox"/>	5	00-00-00-00-00-00	00-00-00-00-00-00	Forward <input type="button" value="v"/>		

5 entries.

Description

The table has the following columns:

- Select**
 Select the row you want to delete. If this entry is used, this is grayed out and you cannot delete it.
- Rule Number**
 Shows the number of the ACL rule. If you create a new entry, a new line with a unique number is created.
- Source MAC Address**
 Enter the MAC address of the source.
- Dest. MAC Address**
 Enter the MAC address of the destination.
- Action**
 Select whether the frame is forwarded or rejected when it corresponds to the ACL rule.
 - Forward
If the frame complies with the ACL rule, the frame is forwarded.
 - Discard
If the frame complies with the ACL rule, the frame is not forwarded.
- Ingress Interfaces**
 Shows a list of all ingress interfaces to which this rule applies.
- Egress Interfaces**
 Shows a list of all egress interfaces to which this rule applies.

Note**Entering the MAC addresses**

You can configure access rules for MAC addresses.

Only if you enter the address "00-00-00-00-00-00" for the source and/or destination MAC address, the rule created in this way applies to all source or destination MAC addresses.

Configuration procedure

1. Click the "Create" button. A new row with a unique number (rule number) is created in the table.
2. Enter the MAC address of the source in "Source MAC Address".
3. Enter the MAC address of the destination in "Dest. MAC Address".
4. In the "Action" drop-down list select whether the frame is forwarded or rejected when it corresponds to the ACL rule.
5. 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.

6.9.5.2 Ingress Rules

On this page, you specify the ACL rule according to which incoming frames are filtered at interfaces. You specify the ACL rules in the "Rules Configuration" tab. The rules are processed one after the other according to the number in the rule order.

MAC ACL Ingress Rules

Rules ConfigurationIngress RulesEgress Rules

Interface: P1.1

Add Rule: -

Add

Remove Rule: Rule 1

Remove

Rule Order	Rule Number	Source MAC	Dest. MAC	Action
1	1	00-00-00-00-00-00	00-00-00-00-00-00	Forward

1 entry.

Refresh

Description of the displayed boxes

The page contains the following boxes:

- Interface**
Select the required interface from the drop-down list. The available interfaces (Page 36) depend on your device.
- Add Rule**
In the drop-down list select the ACL rule to be assigned to the interface.
- Add**
To assign the ACL rule to the interface, click the "Add" button. The configuration is shown in the table.
- Remove Rule**
From the "Remove rule" drop-down list, select the ACL rule to be deleted.
- Remove**
To remove the ACL rule from the interface, click the "Remove" button.

The table has the following columns:

- Rule Order**
Shows the order of the ACL rules.
- Rule Number**
Shows the number of the ACL rule.
- Source MAC address**
Shows the MAC address of the source.

- **Dest. MAC Address**
Shows the MAC address of the destination.
- **Action**
Shows the action.
 - Forward
If the frame complies with the ACL rule, the frame is forwarded.
 - Discard
If the frame complies with the ACL rule, the frame is not forwarded.

Configuration procedure

Follow the steps below to assign an ACL rule to an interface:

1. Select the interface from the "Interface" drop-down list.
2. Select the ACL rule in the "Add Rule" drop-down list.
3. Click the "Add" button. A new entry is generated in the table.

Follow the steps below to remove an ACL rule from an interface:

1. Select the interface from the "Interface" drop-down list.
2. Select the ACL rule in the "Remove Rule" drop-down list.
3. Click the "Remove" button. The corresponding entry is removed in the table.

6.9.5.3 Egress Rules

On this page, you specify the ACL rule according to which outgoing frames are filtered at interfaces. You specify the ACL rule in the "Rules Configuration" tab. The rules are processed one after the other according to the number in the rule order.

MAC ACL Egress Rules

Rules Configuration
Ingress Rules
Egress Rules

Interface: P1.1 ▼
 Add Rule: - ▼
Add

Remove Rule: Rule 1 ▼
Remove

Rule Order	Rule Number	Source MAC	Dest. MAC	Action
1	1	00-00-00-00-00-00	00-00-00-00-00-00	Forward ▼

1 entry.

Refresh

Description of the displayed boxes

The page contains the following boxes:

- **Interface**
Select the required interface from the drop-down list. The available interfaces (Page 36) depend on your device.
- **Add Rule**
In the drop-down list select the ACL rule to be assigned to the interface.
- **Add**
To assign the ACL rule to the interface, click the "Add" button. The configuration is shown in the table.
- **Remove Rule**
From the "Remove rule" drop-down list, select the ACL rule to be deleted.
- **Remove**
To remove the ACL rule from the interface, click the "Remove" button.

The table has the following columns:

- **Rule Order**
Shows the order of the ACL rules.
- **Rule Number**
Shows the number of the ACL rule.
- **Source MAC address**
Shows the MAC address of the source.
- **Dest. MAC Address**
Shows the MAC address of the destination.
- **Action**
Shows the action.
 - Forward
If the frame complies with the ACL rule, the frame is forwarded.
 - Discard
If the frame complies with the ACL rule, the frame is not forwarded.

Configuration procedure

Follow the steps below to assign an ACL rule to an interface:

1. Select the interface from the "Interface" drop-down list.
2. Select the ACL rule in the "Add Rule" drop-down list.
3. Click the "Add" button. A new entry is generated in the table.

Follow the steps below to remove an ACL rule from an interface:

1. Select the interface from the "Interface" drop-down list.
2. Select the ACL rule in the "Remove Rule" drop-down list.
3. Click the "Remove" button. The corresponding entry is removed in the table.

6.9.6 IP ACL

6.9.6.1 Rules Configuration

On this page, you specify the rules for the IP-based Access Control List (IP ACL). IP ACLs can be used with physical ports and IP interfaces. Using the IP-based ACL, you can specify whether frames of certain IPv4 addresses are forwarded or discarded. The maximum number of ACL rules can be found in the WBM section "Configuration limits (Page 35)".

IP Access Control List Configuration

Rules Configuration

Protocol Configuration

Ingress Rules

Egress Rules

Select	Rule Number	Source IP	Source Subnet Mask	Dest. IP	Dest. Subnet Mask	Action	Ingress Interfaces	Egress Interfaces
<input type="checkbox"/>	1	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Forward	P1	VAP 1.1

1 entry.

Create

Delete

Refresh

Description of the displayed boxes

The table has the following columns:

- Select**
 Select the row you want to delete. If this entry is used, this is grayed out and you cannot delete it.
- Rule Number**
 Shows the number of the ACL rule. If you create a new entry, a new line with a unique number is created.
- Source IP**
 Enter the IPv4 address of the source.
- Source Subnet Mask**
 Enter the subnet mask of the source.
- Dest. IP**
 Enter the IPv4 address of the destination.
- Dest. Subnet Mask**
 Enter the subnet mask of the destination.
- Action**
 Select whether the frame is forwarded or rejected when it corresponds to the ACL rule:
 - Forward
If the frame complies with the ACL rule, the frame is forwarded.
 - Discard
If the frame complies with the ACL rule, the frame is not forwarded.
- Ingress Interfaces**
 Shows a list of all ingress interfaces to which this rule applies.
- Egress Interfaces**
 Shows a list of all egress interfaces to which this rule applies.

Note

Subnet mask for individual hosts

If you create the rule for a single system (one IPv4 address), specify the subnet mask "255.255.255.255".
If the rule is to apply to all IP addresses, enter the IP address "0.0.0.0" and the subnet mask "0.0.0.0".

Creating rules

- 1. Click the "Create" button. A new row with a unique number (rule number) is created in the table.
- 2. Enter the data of the source in "Source IP" and in "Source Subnet Mask".
- 3. Enter the data of the destination in "Dest. IP" and in "Dest. Subnet Mask".
- 4. In the "Action" drop-down list select whether the frame is forwarded or rejected when the frame corresponds to the ACL rule.
- 5. Click the "Set Values" button.

Deleting rules

Note

You cannot delete any active rules. Rules can only be deleted when they are not assigned to any interface.

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

6.9.6.2 Protocol Configuration

On this page, you specify the rules for protocols.

IP ACL Protocol Configuration

Rules Configuration | Protocol Configuration | Ingress Rules | Egress Rules

Rule Number	Protocol	Protocol Number	Source Port Min.	Source Port Max.	Dest. Port Min.	Dest. Port Max.	Message Type	Message Code	DSCP
1	Any	255	0	65535	0	65535	255	255	

1 entry.

Refresh

Description

The table has the following columns:

- **Rule Number**
Shows the number of the protocol rule. When you create a rule, a new row with a unique number is created.
- **Protocol**
Select the protocol for which this rule is valid.
 - IP
 - OSPF
 - VRRP
 - ICMP
 - TCP
 - UDP
 - Any
 - Other Protocol
- **Protocol Number**
Enter a protocol number to define further protocols.
This box can only be edited if you have set "Other Protocol" for the protocol.
- **Source Port Min.**
Enter the lowest possible port number of the source port.
This box can only be edited if you have set "TCP" or "UDP" for the protocol.
- **Source Port Max.**
Enter the highest possible port number of the source port.
This box can only be edited if you have set "TCP" or "UDP" for the protocol.
- **Dest. Port Min.**
Enter the lowest possible port number of the destination port.
This box can only be edited if you have set "TCP" or "UDP" for the protocol.
- **Dest. Port Max.**
Enter the highest possible port number of the destination port.
This box can only be edited if you have set "TCP" or "UDP" for the protocol.
- **Message Type**
Enter a message type to decide the format of the message.
This box can only be edited if you have set "ICMP" for the protocol.
- **Message Code**
Enter a message code to specify the function of the message.
This box can only be edited if you have set "ICMP" for the protocol.
- **DSCP**
Enter a value for classifying the priority.
This box cannot be edited if you have set "ICMP" for the protocol.

6.9.6.3 Ingress Rules

On this page, you specify the ACL rules according to which incoming frames are handled by interfaces. You specify the ACL rules in the "Rules Configuration" tab. The rules are processed one after the other according to the number in the rule order.

IP ACL Ingress Rules

Rules Configuration | Protocol Configuration | Ingress Rules | Egress Rules

Interface: P0.1

Add Rule: Rule 3

Add

Remove Rule: Rule 1

Remove

Rule Order▲	Rule Number	Protocol	Protocol Number	Source IP	Source Subnet Mask	Dest. IP	Dest. Subnet Mask
1	1	Any	255	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
2	2	Other Protocol	254	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

2 entries.

Refresh

Continuation of table

Action	Source Port Min.	Source Port Max.	Dest. Port Min.	Dest. Port Max.	Message Type	Message Code	DSCP
Forward	0	65535	0	65535	255	255	
Forward	0	65535	0	65535	255	255	

Description of the displayed boxes

The page contains the following boxes:

- Interface**
Select the required interface from the drop-down list. The available interfaces (Page 36) depend on your device.
To select a VLAN interface, an IP interface must be configured.

Note

If you use a VLAN interface, the ACL rule applies to all ports that belong to the VLAN.

- Add Rule**
In the drop-down list select the ACL rule to be assigned to the interface.
- Add**
To permanently assign the ACL rule to the interface, click the "Add" button. The configuration is shown in the table.
- Remove Rule**
From the "Remove rule" drop-down list, select the ACL rule to be deleted.
- Remove**
To remove the ACL rule from the interface, click the "Remove" button.

The table has the following columns:

- **Rule Order**
Shows the order of the ACL rules.
- **Rule Number**
Shows the number of the ACL rule.
- **Protocol**
Shows the protocol for which this rule is valid.
- **Protocol Number**
Shows the protocol number.
- **Source IP**
Shows the IPv4 address of the source.
- **Source Subnet Mask**
Shows the subnet mask of the source.
- **Dest IP**
Shows the IP address of the destination.
- **Dest. Subnet Mask**
Shows the subnet mask of the destination.
- **Action**
Shows the action.
 - Forward
If the frame complies with the ACL rule, the frame is forwarded.
 - Discard
If the frame complies with the ACL rule, the frame is not forwarded.
- **Source Port Min.**
Shows the lowest possible port number of the source port.
- **Source Port Max.**
Shows the highest possible port number of the source port.
- **Dest. Port Min.**
Shows the lowest possible port number of the destination port.
- **Dest. Port Max.**
Shows the highest possible port number of the destination port.
- **Message Type**
Shows a message type to decide the format of the message.
- **Message Code**
Shows a message code to specify the function of the message.
- **DSCP**
Shows a value for classifying the priority.

Configuration procedure

Follow the steps below to assign an ACL rule to an interface:

- 1. Select the interface from the "Interface" drop-down list.
- 2. Select the ACL rule in the "Add Rule" drop-down list.
- 3. Click the "Add" button. A new entry is generated in the table.

Follow the steps below to assign an ACL rule to an interface:

- 1. Select the interface from the "Interface" drop-down list.
- 2. Select the ACL rule in the "Remove Rule" drop-down list.
- 3. Click the "Remove" button. The corresponding entry is deleted.

6.9.6.4 Egress Rules

On this page, you specify the ACL rules according to which outgoing frames are handled by interfaces. You specify the ACL rules in the "Rules Configuration" tab. The rules are processed one after the other according to the number in the rule order.

IP ACL Egress Rules

Rules Configuration

Protocol Configuration

Ingress Rules

Egress Rules

Interface: P0.1

Add Rule: Rule 2

Add

Remove Rule: Rule 1

Remove

Rule Order	Rule Number	Protocol	Protocol Number	Source IP	Source Subnet Mask	Dest. IP	Dest. Subnet Mask
1	1	Any	255	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

<

1 entry.

Refresh

Continuation of table

Action	Source Port Min.	Source Port Max.	Dest. Port Min.	Dest. Port Max.	Message Type	Message Code	DSCP
Forward	0	65535	0	65535	255	255	

Description of the displayed boxes

The page contains the following boxes:

- **Interface**

Select the required interface from the drop-down list. The available interfaces (Page 36) depend on the device.

To select a VLAN interface, an IP interface must be configured.

Note

If you use a VLAN interface, the ACL rule applies to all ports that belong to the VLAN.

- **Add Rule**

In the drop-down list select the ACL rule to be assigned to the interface.

- **Add**

To assign the ACL rule to the interface, click the "Add" button. The configuration is shown in the table.

Note

An ACL rule with the content "deny any" must not be applied to outgoing frames.

- **Remove Rule**

From the "Remove rule" drop-down list, select the ACL rule to be deleted.

- **Remove**

To remove the ACL rule from the interface, click the "Remove" button.

The table has the following columns:

- **Rule Order**

Shows the order of the ACL rules.

- **Rule Number**

Shows the number of the ACL rule.

- **Protocol**

Shows the protocol for which this rule is valid.

- **Protocol Number**

Shows the protocol number.

- **Source IP**

Shows the IPv4 address of the source.

- **Source Subnet Mask**

Shows the subnet mask of the source.

- **Dest IP**

Shows the IP address of the destination.

- **Dest. Subnet Mask**

Shows the subnet mask of the destination.

6.9 "Security" menu

- **Action**
Shows the action.
 - Forward
If the frame complies with the ACL rule, the frame is forwarded.
 - Discard
If the frame complies with the ACL rule, the frame is not forwarded.
- **Source Port Min.**
Shows the lowest possible port number of the source port.
- **Source Port Max.**
Shows the highest possible port number of the source port.
- **Dest. Port Min.**
Shows the lowest possible port number of the destination port.
- **Dest. Port Max.**
Shows the highest possible port number of the destination port.
- **Message Type**
Shows a message type to decide the format of the message.
- **Message Code**
Shows a message code to specify the function of the message.
- **DSCP**
Shows a value for classifying the priority.

Configuration procedure

Follow the steps below to assign an ACL rule to an interface:

1. Select the interface from the "Interface" drop-down list.
2. Select the ACL rule in the "Add Rule" drop-down list.
3. Click the "Add" button. A new entry is generated in the table.

Follow the steps below to remove an ACL rule from an interface:

1. Select the interface from the "Interface" drop-down list.
2. Select the ACL rule in the "Remove Rule" drop-down list.
3. Click the "Remove" button. The corresponding entry is removed in the table.

6.9.7 Management ACL

Description of configuration

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

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

Note

If you enable this function, note the following

A bad configuration on the "Management Access Control List" page can result in you being unable to access the device. You should therefore configure an access rule that allows access to the management before you enable the function.

Management Access Control List

☐ Management ACL

IP Address:

Subnet Mask / Prefix Length:

Select	Rule Order	IP Address	Subnet Mask / Prefix Length	VLANs Allowed	SNMP	TELNET	HTTP	HTTPS	SSH	P1	P2	VAP 1.1
<input type="checkbox"/>	1	192.168.100.10	255.255.255.255	1-4094	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

1 entry.

Create

Delete

Set Values

Refresh

Description

The page contains the following boxes:

- **Management ACL**
Enable or disable the function.

Note

If the function is disabled, there is unrestricted access to the management of the device. The configured access rules are only taken into account when the function is enabled.

- **IP Address**
Enter the IP address or the network address to which the rule will apply.
 - If you use the IPv4 address 0.0.0.0, the settings apply to all IPv4 addresses.
 - If you use the IPv6 address :: the settings apply to all IPv6 addresses.
- **Subnet Mask / Prefix Length**
Enter the subnet mask or the prefix length.
The subnet mask 255.255.255.255 is for a specific IPv4 address. If you want to allow a subnet, for example a C subnet, enter 255.255.255.0. The subnet mask 0.0.0.0 applies to all subnets.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Rule Order**
Shows the number of the rule. If you click the "Create" button, a new row with a unique number is created.

6.9 "Security" menu

- **IP Address**
Shows the IP address.
- **Subnet Mask / Prefix Length**
Shows the subnet mask or the prefix length.
- **VLANs Allowed**
Only available if 802.1Q VLAN Bridge is set for "Layer 2 > VLAN > General".
Enter the number of the VLAN in which the device is located. The station can only access the device if it is located in this configured VLAN. If this input box remains empty, there is no restriction relating to the VLANs.
- **SNMP**
Specify whether the station (or the IP address) accesses the device using the SNMP protocol.
- **TELNET**
Specify whether the station (or the IP address) accesses the device using the TELNET protocol.
- **HTTP**
Specify whether the station (or the IP address) accesses the device using the HTTP protocol.
- **HTTPS**
Specify whether the station (or the IP address) accesses the device using the HTTPS protocol.
- **SSH**
Specify whether the station (or the IP address) accesses the device using the SSH protocol.
- **Px**
Specify whether the station (or the IP address) accesses the device via this port.
- **VAP X.Y**
Specify whether the station (or the IP address) accesses the device via the VAP interface.
- **WDS X.Y**
Specify whether the station (or the IP address) accesses the device via the WDS interface.

Procedure

Note

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

You can then only remedy this by resetting the device to the factory defaults and then reconfiguring.

Changing the entry

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

Creating new entry

1. In the "IP Address" input box, enter the IP address of the device and in the "Subnet Mask / Prefix Length" input box the corresponding subnet mask.
2. Click the "Create" button to create a new row in the table.

3. Configure the entries of the new row.
4. Click the "Set Values" button to transfer the new entry to the device.

Deleting entries

1. Select the check box in the row to be deleted.
2. Repeat this procedure for every entry you want to delete.
3. Click the "Delete" button. The entries are deleted and the page is updated.

6.10 "iFeatures" menu

iFeatures possible only with SCALANCE W722-1 RJ-45

The use of iPCF, iPCF-HT and iPCF-MC is possible only with the Client SCALANCE W722-1 RJ45. You can integrate this in a WLAN with iPCF, iPCF-HT and iPCF-MC.

You will find a more detailed description of iPCF in the section "Technical basics" in the section "iPCF / iPCF-HT / iPCF-MC (Page 42)".

6.10.1 iPCF

Requirements to be able to use iPCF:

- Client SCALANCE W722-1 RJ-45 (MLFB 6GK5722-1FC00-0AA0 / 6GK5722-1FC00-0AB0 (US version))

When should iPCF be used?

The use of iPCF is advisable particularly if you have a large number of nodes and want to implement highly deterministic operation. This is necessary, for example with PROFINET or other cyclic protocols.

Note**Use of iPCF with other iFeatures**

The iPCF function and other iFeatures (e.g. iPCF-MC, iPCF-HT, iPRP) are not compatible with each other and cannot be used at the same time on a device.

Radio	Enable iPCF	Legacy Free (iPCF-LF)
WLAN 1	<input type="checkbox"/>	<input type="checkbox"/>

Description

You have the following configuration options:

- **Enable iPCF**
Enable or disable iPCF mode. For PROFINET communication, we recommend that you enable the iPCF mode. By enabling iPCF, the data rates provided by the access point are adapted. We strongly recommend that you retain the default setting for the data rates (802.11 a/b/g = 12 Mbps and 802.11n = MCS 2).
- **Legacy Free (iPCF-LF)**
These settings determine which device generation can establish a connection to this device.
 - 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.
This setting prevents performance from being slowed down by the IEEE 802.11 a/b/g device generation.
 - Disabled
All device generations (IEEE 802.11 a/b/g/n) are accepted.

Procedure

1. Select the "Enable iPCF" option for the required WLAN interface.
2. If needed, enable the option "Legacy Free (iPCF-LF)".
3. Click the "Set Values" button.

You configure the security settings in "Security > WLAN > Basic".

6.10.2 iPCF-HT

Requirements to be able to use iPCF-HT:

- Client SCALANCE W722-1 RJ-45 (MLFB 6GK5722-1FC00-0AA0 / 6GK5722-1FC00-0AB0 (US version))

When should iPCF-HT be used?

Note

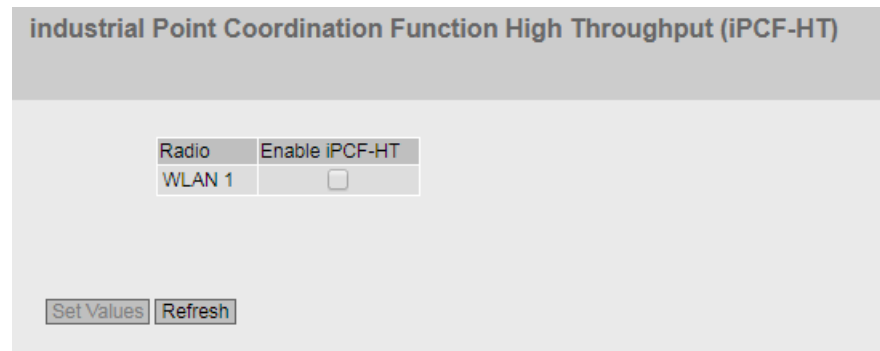
Use of iPCF-HT

The function iPCF-HT

- and other iFeatures (e.g. iPCF, iPCF-MC, iPRP) are not compatible with each other and cannot be used at the same time on a device.
- Can only be used in the frequency band 5 GHz and with WLAN mode "(only) IEEE 802.11n".
- Is available only on the WLAN interface 1.

It is advisable only to use one MCS index.

The use of iPCF-HT is particularly advisable when a higher data throughput is required. If, for example, alongside PROFINET you also want to transfer video data. The real-time behavior for PROFINET is retained.



Description

You have the following configuration options:

- **Enable iPCF-HT**
Enable or disable the iPCF mode. For PROFINET communication, we recommend that you enable the iPCF mode. By enabling iPCF-HT, the data rates provided by the access point are adapted.

Procedure

1. Select the "Enable iPCF-HT" option for the required WLAN interface.

You configure the security settings in "Security > WLAN > Basic".

6.10.3 iPCF-MC

Requirements to be able to use iPCF-MC:

- Client SCALANCE W722-1 RJ-45 (MLFB 6GK5722-1FC00-0AA0 / 6GK5722-1FC00-0AB0 (US version))
- The management interface and data interface must be operated in the same frequency band and mode and must match in terms of their wireless coverage. iPCF-MC will not work if both wireless interfaces are equipped with directional antennas that cover different areas.
- The management interfaces of all access points to which a client can change must use the same channel. A client scans only this one channel to find accessible access points.
- Transmission based on IEEE801.11h (DFS) cannot be used for the management interface. 801.11h (DFS) is possible for the data interface.
- The client cannot be operated with "Use Allowed Channels only".
- "Force roaming on link down" is automatically mirrored on the second interface.
- The following applies to clients: All configured and active SSIDs must be assigned to security context 1. An SSID is active when the corresponding check box "Enabled" is selected on the page "Interfaces > WLAN > Client".
- In Japan, iPCF-MC cannot be enabled if the data or management interface uses a frequency of the 4920 MHz - 5080 MHz frequency band.

When should iPCF-MC be used?

iPCF was developed to achieve short handover times when roaming between cells. The iPCF-MC technique allows short handover times even for freely mobile clients and when a lot of cells are involved or a large number of channels is being used.

Note

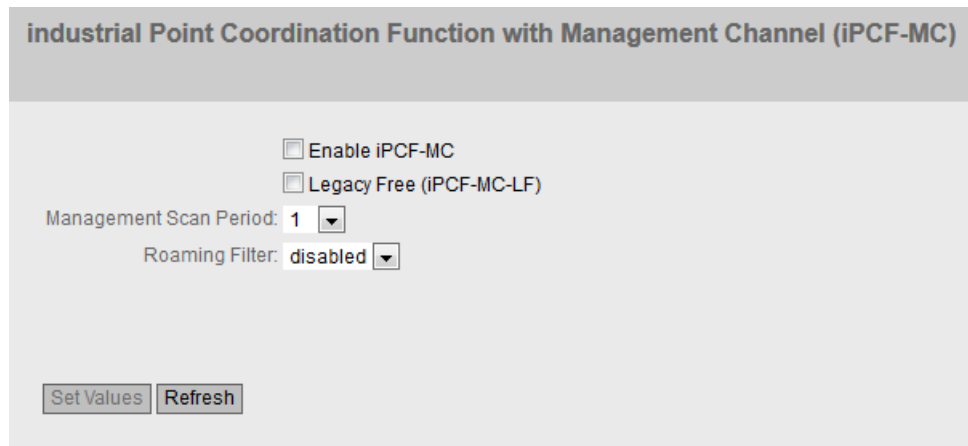
Use of iPCF with other iFeatures

The iPCF-MC function and other iFeatures (e.g. iPCF, iPCF-HT, iPRP) are not compatible with each other and cannot be used at the same time on a device.

Assignment of the interfaces

With 11n devices, remember that the assignment of the WLAN interfaces is fixed for iPCF-MC.

- WLAN1: Data interface
 - WLAN2: Management interface
-



Industrial Point Coordination Function with Management Channel (iPCF-MC)

☐ Enable iPCF-MC

☐ Legacy Free (iPCF-MC-LF)

Management Scan Period: 1

Roaming Filter: disabled

Set Values Refresh

Description

The page contains the following boxes:

- **Enable iPCF-MC activated**
Enable or disable the iPCF-MC mode of the device.
For PROFINET communication, we recommend enabling the iPCF-MC mode. By enabling iPCF-MC, the data rates provided by the access point are adapted.
We strongly recommend that you retain the default setting for the data rates (802.11 a/b/g = 6, 9 and 12 Mbps and 802.11n = MCS 2).
- **Legacy Free (iPCF-MC-LF)**
These settings determine which device generation can establish a connection to this device.
 - Enabled
Only the devices that communicate with the IEEE 802.11n standard and have the "Legacy Free (iPCF-MC-LF)" setting enabled are accepted. WLAN mode IEEE 802.11n need not be enabled for this, however.
This setting prevents performance from being slowed down by the IEEE 802.11 a/b/g device generation.
 - Disabled
All device generations (IEEE 802.11 a/b/g/n) are accepted.

- **Management Scan Period** (in client mode only)
This parameter specifies the time between two management channel scans (specified in iPCF cycles). If, for example, you select two, the client runs a management channel scan only in every second iPCF cycle.
A lower value for the scan interval provides the basis for fast roaming, however this means that no high data throughput can be achieved. A higher value should be selected for a high data throughput.
- **Roaming Filter** (in client mode only)
With this setting you specify the number of RSSI single measurements from which the median is determined. With 5, the last 5 measured RSSI values are considered.
 - Median with an odd number of measurements
The values are arranged in ascending order. The value exactly in the middle is the median.
 - Median with an even number of measurements
The values are arranged in ascending order. The median is calculated from the average of the two middle numbers.

If occasionally there are extreme outliers of the incoming signal, you can filter out the worst fluctuations with this roaming filter. This prevents premature roaming of the client.

6.10.4 iPRP

Requirements for using iPRP

- Client SCALANCE W722-1 RJ-45 (MLFB 6GK5722-1FC00-0AA0 / 6GK5722-1FC00-0AB0 (US version))
- The Base Bridge mode "802.1Q VLAN Bridge" is set.
- The VLANs have been created.
- For "MAC Mode", "Layer 2 Tunnel" is set.
- For "Background Scan mode", either "Always", "Deactivated" or "Current channel" is set

When should iPRP be used?

Note

Use of iPRP with other iFeatures

iPRP and other iFeatures (e.g. iPCF, iPCF-HT, , iPCF-MC) are not compatible with each other and cannot be used at the same time on a device.

iPRP with oversize frames (jumbo frames)

To be able to use oversize frames, oversize frames (jumbo frames) must be configured for 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, as the agent VLAN use the VLAN that PRPA or PRPB is assigned to.

With the "industrial Parallel Redundancy Protocol" (iPRP) the PRP technology can be used in a wireless network. 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.

industrial Parallel Redundancy Protocol (iPRP)

VLAN Assignment

PRP A: -

PRP B: -

Port	Enable iPRP	PRP Network	AP Radio Redundancy
WLAN 1	<input type="checkbox"/>	-	<input checked="" type="checkbox"/>

Set Values

Refresh

Description

The page contains the following:

- PRP A**
Select the VLAN assignment for PRP from the drop-down list.
- PRP B**
Select the VLAN assignment for PRP B from the drop-down list.

This table contains the following columns:

- Port**
Shows the available ports.
- Enable iPRP**
Enable or disable iPRP for the required port.

6.10 "iFeatures" menu

- **PRP Network**
Specify the PRP network in which the port is a member.
- **AP Radio Redundancy**
 - Radio
Prevents the two clients of a client pair connecting on the same WLAN interface of the access point.
 - Disabled
When the best access point for a client is the same access point (same WLAN interface) as that of the partner client, a check is made as to whether there is another access point whose signal strength is < 10 dB worse than that of the best access point. In this case the client connects to this access point, otherwise it connects to the same, best access point as the partner client.
 - Device
Prevents the two clients of a client pair from connecting to the same access point no matter which interface is used.

Procedure

1. Select the VLAN assignment for PRP A from the "PRP A" drop-down list.
2. Select the VLAN assignment for PRP B from the "PRP B" drop-down list.
3. Specify the PRP network in which the port is a member.
4. Enable the setting "AP Radio Redundancy".
5. Select the "Enable iPRP" setting. Click the "Set Values" button.
The appropriate VLAN settings are made automatically.

Upkeep and maintenance

7.1 Firmware update - via WBM

Requirement

- The device has an IP address.
- The user is logged in with administrator rights.

Note

The device must have at least firmware version 5.1. A firmware update is not possible if the firmware on the device is older than version 5.1.

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. Click the "Load file" button in the "Firmware" table row.
5. Go to the storage location of the firmware file.
6. Click the "Open" button in the dialog. The file is uploaded.

Result

The firmware has been transferred completely to the device.

On the "Information > Versions" there are the entries "Firmware" and "Firmware Running". Firmware Running shows 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 163).

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 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.

7.3 Restoring the factory settings

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. Now press the Reset button and reconnect the power to the device while holding down the button.
3. Hold down the button until the red fault LED (F) stops flashing after approximately 10 seconds and is permanently lit.
4. Now release the button and wait until the fault LED (F) goes off again.
5. The device then starts automatically with the factory settings.

Via the configuration

You will find detailed information on resetting the device parameters using the WBM and CLI in the configuration manuals:

- Web Based Management, section "Restart"
- Command Line Interface, section "Reset and Defaults"

Troubleshooting/FAQ

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 Compatibility with predecessor products

Mixed mode

Mixed operation with predecessor products (6GK57xx-xAA60-xAx0) is possible.

Further information about predecessor products can be found on the Internet at Siemens Industry Automation and Drives Service & Support, entry ID: 42784493 (<http://support.automation.siemens.com/WW/view/en/42784493>)

Note the following points if you want to make mixed operation possible:

- Transmission standard IEEE 802.11a/b/g/n
The transmission standards IEEE 802.11a/b/g/n are compatible with the predecessor products. The setting "802.11n only" is not compatible with the predecessor products. The transmission standards IEEE 802.11a/g/h Turbo of the predecessor products are not supported.
- Security settings
The transmission standards IEEE 802.11a/b/g support the same security settings as the predecessor products.
The transmission standard IEEE 802.11n with the setting "802.11n" or "802.11n only" only supports WPA2/ WPA2-PSK with AES in the security settings.
- iPCF / iPCF-MC
The IEEE 802.11b transmission method is not supported together with iPCF.
The SCALANCE W700-xRR devices must not be configured with the operating mode IEEE 802.11b in mixed operation.
- SSID
For SSID, use only the characters that were supported by the previous products.
- Management only over wired Ethernet interface
In the previous products, there was a function "Management only over wired Ethernet interface". In the new devices this function is covered by the "Management ACL (Page 344)" function.
- WDS ID
With WDS ID, do not use the ASCII character 0x22 (").
- Key for WEP or AES
With devices with firmware up to version 3.2, the keys for WEP or AES may only contain ASCII characters or hexadecimal characters from 0x20 to 0x7E.
- Key for WPA(2)-PSK
For devices with firmware version ≤ 5.0 , the keys for WPA(2)-PSK can only consist of ASCII characters or hexadecimal characters from 0x20 to 0x7E.
For devices with firmware version ≥ 5.1 , the following specifications apply to WPA(2)-PSK keys:
 - 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.

8.4 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 163)".
- **Use WPA2/ WPA2-PSK with AES**
Use only WPA2/AES to prevent password misuse. WPA2/ WPA2-PSK with AES provides the greatest security. For more detailed information, refer to the section ""Security" menu (Page 306)".
- **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 "Agent IPv4 (Page 153)".
 - 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 163)".
- **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 194)".

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.

8.5 WLAN client Trigger handover via SNMP

If the other handover mechanisms such as Roaming threshold value, Background Scan threshold value are inadequate, a specific handover can be triggered by setting the MIB variable snMpsWlanForceHandover.

A WLAN client drives, for example along a stretch where there are several access points. When the WLAN client passes a certain point, the value of the MIB variable is changed from 0 to 1. The WLAN client logs off from the connected access point and searches for reachable access points. It logs on to the best reachable access point. The value of the MIB variable is reset to 0.

Trigger handover

Using the private MIB variable snMspWlanForceHandover, you can force a handover.

Note

With Web Based Management (WBM) or using the Command Line Interface (CLI) you cannot configure this function.

OID of the private MIB variable snMspWlanForceHandover:

```
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).siemens(4329).industrialComProducts(20).iComPlatforms(1).simaticNet(1).snMsp
s(1).snMspCommon(1).snMspWlan(27).snMspWlanObjects(1).snMspWlan
Smt(1).snMspWlanRoamingConfigTable(4).snMspWlanRoamingConfigEntr
y(1).snMspWlanForceHandover(14)
```

values of the MIB variable

- 0: Function is disabled.
- 1: Triggers handover.

MIB file

The MIB variable snMspWlanForceHandover can be found in the private MIB file "Scalance_w_msp.mib".

8.6 Configuring the device using the TIA Portal

Once you have inserted the network component, you can edit the properties and parameters offline, for example the device name. Offline means there is no connection to the device.

To be able to see the changes on the device, the change must first be compiled and then loaded on the device.

Compiling and loading can be started in different ways:

- with the shortcut menu "Download to device > Hardware configuration"
- with the "Download" button in the toolbar.

Requirement

- The network component has been created in the project.
- The hardware configuration of the network component matches the hardware configuration of the device. If this is not case, the download will be aborted due to errors.
- The firmware version of the network component matches the firmware version of the device.
- The IP address has been set up.
- The device is connected to the configuration PC.
- The required properties and parameters have been configured.

Note

Activating the SINEMA configuration interface

You can only configure a device using the TIA Portal if you have enabled "SINEMA configuration interface" in the WBM in the menu "System > Configuration".

Downloading properties and parameters to the device

To download the change properties and parameters to the device, follow these steps:

1. Select the required network component in the project tree.
2. In the shortcut menu of the network component select the command "Download to device > Hardware configuration".
3. When the "Extended download to device" dialog opens, configure the "Settings for the download".
 - Select the protocol you are using, e.g. HTTPS.
 - Configure the relevant interface parameters on the configuration PC. When necessary, make interface or protocol specific settings on the operator panel. Click "Start search" The network component is displayed in the "Compatible devices in target subnet" table with its detected IP address.
 - Select the address entry in the table and click the "Load" button.
4. The "Load preview" dialog opens. At the same time the hardware configurations compiled. In this dialog you see messages and proposed revisions necessary for loading, e.g. password required. Check the messages and if necessary enable the actions in the "Action" column. As soon as loading is possible the button becomes active.
5. Click the "Load" button. Loading is performed and the dialog "Load results" is displayed.
6. If the loading is completed error-free, select "Save configuration" in "Action".
7. Click the "Finish" button.

Result

After successful loading, the project can be run on the network component.

Updating the SCALANCE configuration of the network component

To update the SCALANCE configuration of the network component, follow these steps:

1. Open the "Devices & Networks" editor and set the network view.
2. Select the network component in the network view.
3. In the shortcut menu of the network component select the command "SCALANCE configuration > Upload to PG/PC".

Result

Once the connection to the device is established you will be prompted to log in to the device. If the login was successful, the SCALANCE configuration will be loaded from the device to the TIA Portal. Afterwards the properties and parameters are updated in the TIA Portal.

8.6.1 Message: SINEMA configuration not yet accepted

When the following message is displayed in the display area an error has occurred transferring the configuration from STEP 7 Basic / Professional as of V13 to the device:

"SINEMA Configuration not accepted yet. With restart of device, all configuration changes will be lost."

One possible cause is, for example, that during transfer the device was not reachable.

If you now change a parameter directly on the device (WBM/CLI/SNMP) these changes are lost when the device restarts.

Solution

1. Open the relevant STEP 7 project in STEP 7 Basic / Professional
2. Open the project view.
3. Select the device in the project tree.
4. Select the "Go to network view" command in the shortcut menu.
5. Select the device in the network view.
6. In the shortcut menu of the selected device select the command "SCALANCE configuration > Save as start configuration".

Result

The configuration is saved on the device. The message is no longer visible in the display area. A configuration change directly on the device is no longer lost due to a restart of the device.

8.6 Configuring the device using the TIA Portal

Appendix A "Supported MIB Modules"

A.1 Supported MIB files

MIB files available for the SCALANCE W700

The following table shows the MIB files available for a SCALANCE W device:

MIB	Root OID	Reference
AUTOMATION-SNTP (Siemens) ^{1) 2)}	.1.3.6.1.4.1.4329.6.3.11	Vendor specific
AUTOMATION-SYSTEM-MIB (Siemens) ^{1) 2)}	.1.3.6.1.4.1.4329.6.3.2	Vendor specific
AUTOMATION-TELNET (Siemens) ^{1) 2)}	.1.3.6.1.4.1.4329.6.3.8	Vendor specific
AUTOMATION-TIME-MIB (Siemens) ^{1) 2)}	.1.3.6.1.4.1.4329.6.3.3	Vendor specific
BRIDGE-MIB	.1.3.6.1.2.1.17	RFC1493
ENTITY-MIB	.1.3.6.1.2.1.47	
EtherLike-MIB	.1.3.6.1.2.1.10.7.2	
IANA-MAU-MIB	.1.3.6.1.2.1.26.1.1	
IEEE8021-PAE-MIB	.1.0.8802.1.1.1	IEEE 802.1X
IEEE802dot11-MIB	.1.2.840.10036	IEEE 802.11
IF-MIB:	.1.3.6.1.2.1.2	RFC2233
P-BRIDGE-MIB	.1.3.6.1.2.1.17.4.5	
Q-BRIDGE-MIB	.1.3.6.1.2.1.17.7	
RADIUS-ACC-CLIENT-MIB	.1.3.6.1.2.1.67.2.2	
RADIUS-AUTH-CLIENT-MIB	.1.3.6.1.2.1.67.1.2	
RFC1213-MIB	.1.3.6.1.2.1.4	
RMON-MIB	.1.3.6.1.2.1.16	
SNMP-COMMUNITY-MIB	.1.3.6.1.6.3.18	
SNMP-FRAMEWORK-MIB	.1.3.6.1.6.3.10.2.1	RFC2571
SNMP-NOTIFICATION-MIB	.1.3.6.1.6.3.13	RFC2573
SNMP-PROXY-MIB	.1.3.6.1.6.3.14	
SNMP-TARGET-MIB	.1.3.6.1.6.3.12	RFC2573
SNMP-USER-BASED-SM-MIB	.1.3.6.1.6.3.15	RFC2574
SNMPv2-MIB	.1.3.6.1.2.1.1	RFC1907
SNMP-VIEW-BASED-ACM-MIB	.1.3.6.1.6.3.16	RFC2575
SN-MSPS-ACL-MIB (Siemens) ²⁾	.1.3.6.1.4.1.4329.20.1.1.1.1.30	Vendor specific
SN-MSPS-CONFIG-MIB (Siemens) ²⁾	.1.3.6.1.4.1.4329.20.1.1.1.1.1	Vendor specific
SN-MSPS-CPLUG-MIB (Siemens) ²⁾	.1.3.6.1.4.1.4329.20.1.1.1.1.23	Vendor specific
SN-MSPS-DHCP-CLIENT-MIB (Siemens) ²⁾	.1.3.6.1.4.1.4329.20.1.1.1.1.17.1	Vendor specific
SN-MSPS-DIGITAL-IO-MIB (Siemens) ^{2) 3)}	.1.3.6.1.4.1.4329.20.1.1.1.1.39	Vendor specific
SN-MSPS-GENERAL-MIB (Siemens) ²⁾	.1.3.6.1.4.1.4329.20.1.1.1.1.2	Vendor specific
SN-MSPS-HTTP-MIB (Siemens) ²⁾	.1.3.6.1.4.1.4329.20.1.1.1.1.20	Vendor specific

A.1 Supported MIB files

MIB	Root OID	Reference
SN-MSPS-IF-MIB (Siemens) ²⁾	.1.3.6.1.4.1.4329.20.1.1.1.1.34	Vendor specific
SN-MSPS-IP-MIB (Siemens) ²⁾	.1.3.6.1.4.1.4329.20.1.1.1.1.13	Vendor specific
SN-MSPS-LOAD-SAVE-MIB (Siemens) ²⁾	.1.3.6.1.4.1.4329.20.1.1.1.1.26	Vendor specific
SN-MSPS-LOG-MIB (Siemens) ²⁾	.1.3.6.1.4.1.4329.20.1.1.1.1.31	Vendor specific
SN-MSPS-MSTP-MIB (Siemens) ²⁾	.1.3.6.1.4.1.4329.20.1.1.1.1.6	Vendor specific
SN-MSPS-NTP-MIB (Siemens)	.1.3.6.1.4.1.4329.20.1.1.1.1.33	Vendor specific
SN-MSPS-PNAC-MIB (Siemens) ²⁾	.1.3.6.1.4.1.4329.20.1.1.1.1.10	Vendor specific
SN-MSPS-PORT-MIB (Siemens) ²⁾	.1.3.6.1.4.1.4329.20.1.1.1.1.29	Vendor specific
SN-MSPS-RADIUS-SERVER-MIB (Siemens) ²⁾	.1.3.6.1.4.1.4329.20.1.1.1.1.11.2	Vendor specific
SN-MSPS-REPORT-MIB (Siemens) ²⁾	.1.3.6.1.4.1.4329.20.1.1.1.1.28	Vendor specific
SN-MSPS-RMON-MIB (Siemens) ²⁾	.1.3.6.1.4.1.4329.20.1.1.1.1.12	Vendor specific
SN-MSPS-SCW-MIB (Siemens) ^{1) 2)}	.1.3.6.1.4.1.4329.20.1.1.1.1.100.10	Vendor specific
SN-MSPS-SINEMA-MIB (Siemens) ²⁾	.1.3.6.1.4.1.4329.20.1.1.1.1.25	Vendor specific
SN-MSPS-SNMP-MIB (Siemens) ²⁾	.1.3.6.1.4.1.4329.20.1.1.1.1.4	Vendor specific
SN-MSPS-SNTP-CLIENT-MIB (Siemens) ²⁾	.1.3.6.1.4.1.4329.20.1.1.1.1.19.1	Vendor specific
SN-MSPS-STP-L2T-MIB (Siemens)	.1.3.6.1.4.1.4329.20.1.1.1.1.40	Vendor specific
SN-MSPS-SYSLOG-CLIENT-MIB (Siemens) ²⁾	.1.3.6.1.4.1.4329.20.1.1.1.1.21.1	Vendor specific
SN-MSPS-VLAN-MIB (Siemens) ²⁾	.1.3.6.1.4.1.4329.20.1.1.1.1.3	Vendor specific
SN-MSPS-WLAN-MIB (Siemens) ²⁾	.1.3.6.1.4.1.4329.20.1.1.1.1.27	Vendor specific
TCP-MIB	.1.3.6.1.2.1.6	
UDP-MIB	.1.3.6.1.2.1.7	

- ¹⁾ Part of the AUTOMATION.MIB

You can download the AUTOMATION.MIB for SCALANCE W700 from Siemens Industry Automation and Drives Service & Support under the following entry ID 67637278 (<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".
- ³⁾ This MIB is not supported on devices without a digital input/output.

Appendix B "Private MIBs"

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).snMsp(1).snMspCommon(1)
```

WLAN-specific MIB variables

The WLAN-specific MIB variables can be found in "snMspWlan". You will find further information about the settings and values in the MIB file.

Appendix C "Underlying Standards"

C.1 Underlying standards

Standards met by SCALANCE W700 devices completely or partly

The following table lists some of the standards for SCALANCE W700 devices.

Name of the standard	Topic
IEEE 802.1AB	Link Layer Discovery Protocol (LLDP)
IEEE 802.1D-1998	Media Access Control (MAC), bridges
IEEE 802.1Q	Virtual Bridged LANs (VLAN Tagging, Port Based VLANs)
IEEE 802.1W-2004	Rapid Spanning Tree Protocol (RSTP)
IEEE 802.3-2002	Ethernet
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

Appendix D "Log Messages"

D.1 Messages in the event log

Messages during system startup (general)

Message	Description
Warm start performed, Ver: V03.00.00 - event/ status summary after startup	Type of startup and the loaded firmware version.
Power supply: <ul style="list-style-type: none"> L1 is connected L1 is not connected 	Status of the power supply line 1
No line is monitored	Information about monitoring the power supply from the signaling system.
MSTP disabled MSTP enabled	Information on the status of the Spanning Tree protocol.
No Fault states pending after startup	Fault state following system start.

Status of the power supply

You enable or disable the "Power Change" event in "System > Events".

Message	Description
Power up on line 1.	Power supply available on line 1
Power down on line 1.	Power supply interrupted on line 1

Status of the Ethernet interface

You enable or disable the "Link Change" event in "System > Events".

Message	Description
Link up on P1.	A connection exists on the Ethernet interface.
Link down on P1.	No connection exists on the Ethernet interface.

Status of the WLAN interface (in access point mode only)

Messages	
Link down up VAP X.Y	The VAP interface Y on the WLAN interface X is enabled.
Link down on VAP X.Y	The VAP interface Y on the WLAN interface X is disabled.
WDS Y at WLAN X is up	A link exists on the WDS interface Y of WLAN interface X.
WDS Y at WLAN X is down	No link exists on the WDS interface Y of WLAN interface X.

D.1 Messages in the event log

Messages	
Overlap-AP found on WLAN X: AP <System Name> <MAC address> found on channel <Channel number> <RSSI value>	A further access point was found 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 no longer be detected during the configured aging time and was removed from the "Overlap AP" list.
DFS: Radar interference detected on WLAN X at channel <channel number> (frequency <frequency> MHz). Changing to channel <channel number> (frequency <frequency> MHz)	A primary user (e.g. radar or weather station) was found on the channel set for WLAN interface X or on a neighboring channel. The channel will be blocked for 30 min. The access point changes to the configured alternative channel or to the next free channel on which there is no primary user.
DFS: channel <channel number> (frequency <frequency> MHz) aged out from NOL at WLAN X and can be used again.	No primary user found any longer on the channel. The channel was removed from the list of blocked channels and can be used again
DFS: Radar interference detected on WLAN X at channel <channel number> (frequency <frequency> MHz). No more free channels to use!!	A primary user was found on all available channels. There is no free channel available, the WLAN interface X will be deactivated until one of the channels becomes available.

Status of the WLAN interface (in client mode only)

Messages	Description
Link up on WLAN X	The WLAN interface X is enabled.
Link down on WLAN X	The WLAN interface X is disabled.

Messages on configuration

Messages	Description
WBM: Authentication failure	When logging in with Web Based Management (WBM), the wrong password was entered. The event can be enabled or disabled in "System -> Events" (authentication failure).
Telnet: Authentication failure	When logging in via Telnet, the wrong password was entered. The event can be enabled or disabled in "System -> Events" (authentication failure).
Restart requested	Restart due to a user request. The event can be enabled or disabled in "System -> Events" (Cold/Warm Start).

Messages about file upload or download

Messages	Description
File upload via HTTP(S): load of FileType <file type> OK → restart required	Loading the file via HTTP(S) was successful. A restart is required.
File upload via HTTP(S): load of FileType<file type> OK	Loading the file via HTTP(S) was successful.
File upload via HTTP(S): validation of FileType <file type> IDENTICAL	Loading the file via HTTP(S) was successful. The file is identical to the existing file.
File upload via HTTP(S): validation of FileType <file type> FAILED	Loading the file via HTTP(S) failed. The file contains errors or is invalid.
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.

Messages	Description
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" "DFS: No channels are available at WLAN1"	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" "DFS: No channels are available at WLAN1"	Outgoing fault
New Fault state (reconfiguration): <fault description> <fault description>:"Link down on P1." "Link up on P1." "Power down on line L1"	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".	Outgoing fault. The event was triggered due to a change in the configuration.
Fault state: <fault description> cleared. <fault description>:"Warm start performed" "Cold start performed".	Fault was acknowledged by the user.

Messages about MSTP

You enable or disable the "Spanning Tree" event in "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 address>	The authentication of the client was successful or not successful.

Messages about message system

Messages	Description
Syslog-Server not reachable!	The configured Syslog server is not accessible.
Unable to send messages to syslog server. Please check syslog socket configuration.	The syslog server configuration is incomplete.
Unable to send e-mail(s) because of IP connection failure.	Sending of e-mail(s) failed. SMTP server cannot be reached (e.g. network connection interrupted).
Unable to send e-mail(s) because of SMTP authentication failure.	Sending of e-mail(s) failed. Authentication of the client on the SMTP server incorrect.
Unable to send e-mail(s) because SMTP message transfer failed.	Sending of e-mail(s) failed. SMTP server can be reached, configuration incomplete or contains errors (e.g. receiver e-mail address wrong / does not exist).
SNMP: Authentication 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.

D.2 Messages in the WLAN Authentication Log**Messages in access point mode**

Alarm	Description
VAP<Num>: Client <MAC address> <System Name> associated successfully	The client has logged in successfully on the access point.
VAP<Num>: 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 associate; status (<text>)	The connection of the client to the VAP has failed. The reason is displayed as text.
VAP<Num>: Client<MAC address> failed to associate, status (Too many clients already associated)	The connection of the client to the VAP has failed. The maximum number of clients according to the Client Limiter setting has been exceeded, see "Security > WLAN > AP communication".
VAP<Num>: Client<MAC address> failed to associate, status (Too many clients join failure)	The connection of the client to the VAP has failed. It was not possible to log in successfully. This can occur when, e.g., too many clients attempt to log into the access point simultaneously.

D.2 Messages in the WLAN Authentication Log

Alarm	Description
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<Num>: Client <MAC address> <System Name> deauthenticated with reason (Disassociated due to inactivity)	The client was logged off from the AP after the client was inactive for a longer period of time.
VAP<Num>: 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 disassociate; 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.
RADIUS: Access rejected for client <MAC address><System Name>	The RADIUS server denies the client access.
RADIUS: Access accepted for client <MAC address><System Name>	The RADIUS server allows the client access.
WDS Connection is established to AP <MAC address>	The WDS connection is successfully established to the access point.
WDS disconnect from AP <MAC address>	The WDS connection to the access point is terminated.

Messages in client mode

Alarm	Description
Associated successfully to AP <MAC address> <System Name> at channel <Channel number> (frequency <Frequency> MHz)	The client has logged in successfully on the access point.
Disassociated from AP <MAC address> <System Name> with reason (Disassociated because sending STA is leaving (or has left) BSS)	The client was logged off from the access point.
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.
4-Way handshake to AP <MAC address> failed (Info element in 4-Way Handshake different from (Re)Association Request/Probe Response/Beacon)	An error occurred during authentication in the four-stage handshake procedure. The info element is different in the various frames of the access point for the 4-way handshake.

Appendix "Syslog Messages"

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

Human user identification and authentication

Message text	{protocol}: User {User name} has logged in from {ip address}.
Example	WBM: User "Admin" has logged in from 192.168.0.1.
Explanation	Valid login information that is specified during remote login.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{protocol}: Default user {user name} logged in from {ip address}.
Example	SSH: Default user admin logged in from 192.168.0.1.
Explanation	The default user is logged in via the IP address.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 007-R5)

Message text	{protocol}: User {User name} has logged out from {ip address}.
Example	SSH: User "Admin" has logged out from 192.168.0.1.
Explanation	User session completed - logged out.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{protocol}: User {User name} failed to log in from {ip address}.
Example	WBM: User "Admin" has failed to log in from 192.168.0.1.
Explanation	Incorrect user name or incorrect password (login information) specified during remote login.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{Protocol}: {IP address} - No response from the RADIUS server.
Example	WBM: 192.168.1.105 - No response from the RADIUS server.
Explanation	No access to the server or the server is not responding.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Account management

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

Message text	{protocol}: User {user name} changed password of user {action user name}.
Example	Telnet: User admin changed password of user test.
Explanation	User has changed the password of another user.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR1.3

Message text	{protocol}: User {user name} created user-account {action user name}.
Example	WBM: User admin created user-account service.
Explanation	The user has created an account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR1.3

Message text	{protocol}: User {user name} deleted user-account {action user name}.
Example	WBM: User admin deleted user-account service.
Explanation	The administrator deleted an existing account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR1.3

Identifier management

Message text	{Protocol}: User {User name} created group {Group} and assigned to role {Role}.
Example	WBM: User admin created group it-service and assigned to role service.
Explanation	The administrator has created a group and assigned it to a role.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.4

Message text	{Protocol}: User {User name} deleted group {Group} and the role {Role} assignment.
Example	WBM: User maier deleted group it-service and the role service assignment.
Explanation	The administrator has deleted an existing group and the role assignment.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.4

Unsuccessful login attempts

Message text	{User name} account is locked for {Time minute} minutes after {Failed login count} unsuccessful login attempts.
Example	User service account is locked for 44 minutes after 10 unsuccessful login attempts.
Explanation	If there are too many failed logins, the corresponding user account was locked for a specific period of time.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.11

Session lock

Message text	The session of user {user name} was closed after {time} seconds of inactivity.
Example	The session of user admin was closed after 60 seconds of inactivity.
Explanation	The current session was locked due to inactivity.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.5

Wireless use control

{vap}: Client {SRC mac} associated successfully.

Example	VAP1.1: Client 00:0C:29:2F:09:B3 associated successfully.
Explanation	WLAN client connected to AP.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.2

{vap}: Client {SRC mac} failed to associate, status {status}.

Example	VAP1.1: Client 00:0C:29:2F:09:B3 failed to associate, status (Invalid group cipher).
Explanation	WLAN client connection to AP denied.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.2

Overlap-AP found on {Wlan interface}: AP {ssid} {Src mac} found on channel {Channel} rssi {Signal strength}.

Example	Overlap-AP found on WLAN1: AP MyWLAN 00:0C:29:2F:09:B3 found on channel 12 rssi 12.
Explanation	Radio frequency is already in use.
Severity	Information
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.2

Overlap-AP found on {Wlan interface}: AP {ssid_Hex} {Src mac} found on channel {Channel} rssi {Signal strength}.

Example	Overlap-AP found on WLAN1: AP 050E081234 00:0C:29:2F:09:B3 found on channel 12 rssi 12.
Explanation	Radio frequency is already in use.
Severity	Information
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.2

{vap}: Client {SRC mac} disassociated with reason {reason}.

Example	VAP1.1: Client 00:0C:29:2F:09:B3 disassociated with reason (Unknown peer).
Explanation	WLAN client disconnected from AP.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.2

{vap}: Client {SRC mac} failed to authenticate, status {status}.

Example	VAP1.1: Client 00:0C:29:2F:09:B3 failed to authenticate, status (Invalid group cipher).
Explanation	WLAN client connection to AP denied.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.2

{Protocol}: {IP address} - No response from the RADIUS server.

Example	WBM: 192.168.1.105 - No response from the RADIUS server.
Explanation	RADIUS server not found.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.2

Limiting the number of simultaneous sessions

Message text	{Protocol}: The maximum number of {Max sessions} concurrent login session exceeded.
Example	WBM: The maximum number of 10 concurrent login sessions exceeded.
Explanation	The maximum number of parallel connections is exceeded.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.7

Nonrepudiation

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

Data backup in automation system

Log text	{protocol}: Saved file type ConfigPack.
Standard	IEC 62443-3-3 Reference: SR7.3
Description	The ConfigPack file was saved.
Example	TFTP: Saved file type ConfigPack
Severity	Notice
Facility	local0

Log text	{protocol}: User {user name} failed to save file type ConfigPack.
Standard	IEC 62443-3-3 Reference: SR7.3
Description	User failed to save the ConfigPack file.
Example	WBM: User admin failed to save file type ConfigPack.
Severity	Info
Facility	local0

Log text	{protocol}: User {user name} saved file type ConfigPack
Standard	IEC 62443-3-3 Reference: SR7.3
Description	User has saved the ConfigPack file.
Example	WBM: User admin saved file type ConfigPack..
Severity	Notice
Facility	local0

Log text	{protocol}: Failed to save file type ConfigPack.
Standard	IEC 62443-3-3 Reference: SR7.3
Description	The ConfigPack file could not be saved.
Example	TFTP: Failed to save file type ConfigPack.

Severity	Warning
Facility	local0

Restoration of the automation system

Message text	{protocol}: User {user name} loaded file type Config (restart required)..
Example	WBM: User admin loaded file type Config (restart required).
Explanation	The configuration is applied.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Message text	{protocol}: Loaded file type Config (restart required)..
Example	TFTP: Loaded file type Config (restart required).
Explanation	The configuration is applied.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Message text	{protocol}: User {user name} loaded file type ConfigPack (restart required)..
Example	WBM: User admin loaded file type ConfigPack (restart required).
Explanation	The configuration is applied.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Message text	{protocol}: Loaded file type ConfigPack (restart required)..
Example	TFTP: Loaded file type ConfigPack (restart required).
Explanation	The configuration is applied.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Message text	{protocol}: User {user name} loaded file type Firmware {version} (restart required).
Example	WBM: User admin loaded file type Firmware V02.00.00 (restart required).
Explanation	Firmware update was successfully uploaded.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Message text	{protocol}: Loaded file type Firmware {version} (restart required).
Example	TFTP: Loaded file type Firmware V02.00.00 (restart required).
Explanation	Firmware update was successfully uploaded.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Message text	{protocol}: Failed to load file type Firmware.
Example	WBM: Failed to load file type Firmware.
Explanation	Firmware activation failed.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Appendix F (Supported Security Mechanisms)

F.1 WLAN security mechanisms

The following table shows the encryption methods and authentication that the SCALANCE W devices support.

Encryption method	
None	✓
WEP	✓
WPA-TKIP	-
WPA-AES	✓

Authentication	
Password / PSK	✓
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 Security mechanisms supported for RADIUS authentication.

The following table shows cipher suites and signature algorithms that SCALANCE W devices support for RADIUS authentication.

Default setting TLS 1.0

Table F-1 WPA/WPA2 RADIUS authentication

Cipher suite	Signature algorithm
TLS 1.0/1.1	
AES256-GCM-SHA384	ECDSA with SHA224
AES128-GCM-SHA256	ECDSA with SHA1
AES256-SHA256	SHA224 with RSA
AES128-SHA256	SHA1 with RSA
ECDHE-ECDSA-AES256-SHA	DSA with SHA224
ECDHE-RSA-AES256-SHA	DSA with SHA1
DHE-RSA-AES256-SHA	ECDSA with SHA256
ECDHE-ECDSA-AES128-SHA	ECDSA with SHA384

Cipher suite	Signature algorithm
ECDHE-RSA-AES128-SHA	ECDSA with SHA512
DHE-RSA-AES128-SHA	EdDSA ed25519
AES256-SHA	EdDSA ed448
AES128-SHA	RSASSA-PSS with SHA256
TLS_AES_256_GCM_SHA384	RSASSA-PSS with SHA384
TLS_CHACHA20_POLY1305_SHA256	RSASSA-PSS with SHA512
TLS_AES_128_GCM_SHA256	RSASSA-PSS (rsaEncryption) with SHA256
ECDHE-ECDSA-AES256-GCM-SHA384	RSASSA-PSS (rsaEncryption) with SHA384
ECDHE-RSA-AES256-GCM-SHA384	RSASSA-PSS (rsaEncryption) with SHA512
DHE-RSA-AES256-GCM-SHA384	SHA256 with RSA
ECDHE-ECDSA-CHACHA20-POLY1305	SHA384 with RSA
ECDHE-RSA-CHACHA20-POLY1305	SHA512 with RSA
DHE-RSA-CHACHA20-POLY1305	DSA with SHA256
ECDHE-ECDSA-AES128-GCM-SHA256	DSA with SHA384
ECDHE-RSA-AES128-GCM-SHA256	DSA with SHA512
DHE-RSA-AES128-GCM-SHA256	
ECDHE-ECDSA-AES256-SHA384	
ECDHE-RSA-AES256-SHA384	
DHE-RSA-AES256-SHA256	
ECDHE-ECDSA-AES128-SHA256	
ECDHE-RSA-AES128-SHA256	
DHE-RSA-AES128-SHA256	
TLS 1.2	
TLS_AES_256_GCM_SHA384	ECDSA with SHA256
TLS_CHACHA20_POLY1305_SHA256	ECDSA with SHA384
TLS_AES_128_GCM_SHA256	ECDSA with SHA512
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	RSASSA-PSS with SHA384
ECDHE-RSA-CHACHA20-POLY1305	RSASSA-PSS with SHA512
DHE-RSA-CHACHA20-POLY1305	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	

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	;" €'?\$ ³²⁰ 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 .-_#+'*~^!\$%&/{([])}=\ `<>@, Space
Characters not allowed	;" €'?\$ ³²⁰ μ ä ö ü Ä Ö Ü
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.

G.1 Permitted characters

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

A

- Access point
 - Overlapping channels, 127
 - Overview, 122
 - Overview of logged-on clients, 125
 - WDS list, 126
- ACL
 - IP ACL, 337
- Alarm events, 184
- Article number, 99
- Authentication, 201
- Available system functions, 37

B

- Basic Wizard
 - Starting, 70
 - System configuration, 76
- Bridge priority, 51

C

- Client
 - Available access points, 133
 - Overview, 130
- Client Supplicant, 329
- Collisions, 113
- Communications options, 325
- Configuration manuals, 358
- Configuration mode, 149
- Configuring the network via Ethernet
 - Connecting to network, 58
- CRC, 113

D

- Data transmission speed, 248, 251
 - 802.11a/b/g, 248
 - 802.11n, 251
- DCP server, 77, 147, 299
- Default routes
 - IPv6 routes, 157
- DHCP
 - Client, 186
- Documentation on the Internet, 9

DST

- Daylight saving time, 204, 206

E

- E-Mail function, 184
 - Alarm events, 184
 - Line monitoring, 184
- Error status, 105
- Ethernet statistics
 - Interface statistics, 110
- Event
 - Log table, 102
- Event log table, 102

F

- Factory defaults, 357
- Factory setting, 357
- Fault monitoring
 - Connection status change, 220
- Forward Delay, 290
- Fragments, 113

G

- Geographic coordinates, 151
- Glossary, 11
- Group name
 - Permitted characters, 392
- Groups, 310

H

- Hardware version, 99
- HTTP
 - Server, 147
- HTTPS
 - Server, 147

I

- IEEE 802.11n, 30, 242
 - Channel bonding, 32
 - Frame aggregation, 32
 - Guard interval, 32
 - Maximum ratio combining, 31

- MIMO, 31
 - Spatial multiplexing, 31
- Information
 - ARP table, 100
 - Groups, 122
 - IPv6 Neighbor Table, 101
 - LLDP, 114
 - Log tables, 102
 - Role, 121
 - Security, 118, 120
 - SNMP, 117
 - Spanning Tree, 106
 - Start page, 91
 - Versions, 97
- IP ACL rules
 - Egress, 342
 - Ingress, 340
- IP address
 - Assignment with STEP 7, 61
- IP mapping, 134
- iPCF
 - Configuration, 347, 349
 - How it works, 42
 - PROFINET communication, 42
 - Restriction, 44
- iPCF-HT
 - How it works, 42
- iPCF-MC
 - PROFINET communication, 42
- iPRP
 - Configuration, 352
 - Information, 144
- IPv6
 - Notation, 62
- IPv6 routing
 - Default routes, 157
 - Routing table, 115

J

- Jabbers, 113

L

- Line monitoring, 184
- LLDP, 114, 300
- Local users, 306
- Location, 151
- Log tables
 - WLAN authentication log, 104
- Logging in, 67

- Logout
 - Automatic, 216

M

- MAC ACL rules
 - Egress, 335
 - Ingress, 334
- Maintenance data, 98
- MSTP, 295
 - Port, 291
 - Port parameters, 297
- MSTP instance, 297
- Multichannel configuration, 24
- Multiple Spanning Tree, 291, 295

N

- NAPT, 48
 - Configuring, 304
- NAT, 48
 - Configuring, 302
- Negotiation, 227
- Network access, 26
- NTP
 - Client, 213

O

- Oversize, 113
- Overview
 - Access point, 122
 - Available access points, 133
 - Clients, 130
 - Logged-on clients, 125
 - Overlap APs, 127
 - Overlapping channels, 127
 - WDS partner, 126

P

- Packet error statistics, 112
- Password, 312
 - Options, 314
 - Permitted characters and length, 391
- Permitted characters and length, 391
- Ping, 225
- point-to-point, 52
- Port
 - Port configuration, 226, 229

Port configuration, 229

Power supply

Monitoring, 219

PROFINET, 40, 221

PROFINET IO, 40

R

RADIUS, 315

Reboot, 160

Redundant networks, 289

Reset, 160

Reset device, 357

Restore Factory Defaults, 357

Role name

Permitted characters, 392

Roles, 309

Root bridge, 51

Routing

IPv6 routing table, 115

Rule, 332

Configuration, 332, 337

IP ACL, 337

MAC ACL, 332

S

Scope of the manual, 9

Security settings, 198

Serial number, 99

Service & Support, 11

SFTP

Load/save, 175

SHA algorithm, 198

Signal recorder, 260

SIMATIC NET glossary, 11

SINEC PNI, 299

SMTP

Client, 147

SNMP, 49, 77, 148, 194, 198

Groups, 198

Overview, 117

SNMPv1, 49

SNMPv2c, 49

SNMPv3, 49

Trap, 196

Users, 200

Software version, 99

Spanning Tree

Information, 106

Rapid Spanning Tree, 52

Spectrum analyzer, 270

SSH

Server, 146

Standalone configuration, 23

Start page, 91

STEP 7, 299

Syslog

Client, 147

System

Configuration, 145

General information, 150

System event log

Agent, 217

System events

Configuration, 181

Severity filter, 183

System Time, 202

T

Telnet

Server, 146

TFTP

Load/save, 173

Time, 148

Time of day

Manual setting, 203

SIMATIC Time Client, 215

SNTP (Simple Network Time Protocol), 209

System time, 203

Time zone, 212

Time-of-day synchronization, 209

UTC time, 212

Time setting, 148

Training, 11

U

Undersize, 113

User groups, 310

User name

Permitted characters and length, 391

V

Vendor, 98

Vendor ID, 99

VLAN, 40

Port VID, 284

Priority, 284

Tag, 284

W

WDS, 247

Web Based Management, 66

Wireless access, 24

WLAN statistics

- Bad frames, 138

- Received frames, 142

- Sent frames, 143