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.

<table>
<thead>
<tr>
<th>Degree of Danger</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DANGER</strong></td>
<td>indicates that death or severe personal injury <strong>will</strong> result if proper precautions are not taken.</td>
</tr>
<tr>
<td><strong>WARNING</strong></td>
<td>indicates that death or severe personal injury <strong>may</strong> result if proper precautions are not taken.</td>
</tr>
<tr>
<td><strong>CAUTION</strong></td>
<td>indicates that minor personal injury can result if proper precautions are not taken.</td>
</tr>
<tr>
<td><strong>NOTICE</strong></td>
<td>indicates that property damage can result if proper precautions are not taken.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Degree of Danger</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WARNING</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

Trademarks

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

Disclaimer of Liability

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

1 Introduction .............................................................................................................................................. 9  
  1.1 Information on the Configuration Manual .................................................................................. 9  
  1.2 Type designations ....................................................................................................................... 13  

2 Description ............................................................................................................................................... 15  
  2.1 Network structures ..................................................................................................................... 16  
  2.2 Possible applications of SCALANCE W700 devices ................................................................. 21  
  2.3 Product characteristics .............................................................................................................. 22  
  2.4 IEEE 802.11n ............................................................................................................................. 24  
  2.5 Requirements for installation and operation of SCALANCE W700 devices ......................... 28  
  2.6 C-PLUG and KEY-PLUG .......................................................................................................... 29  
  2.7 Power over Ethernet (PoE) ....................................................................................................... 31  

3 Security recommendations .................................................................................................................... 35  

4 Technical basics ..................................................................................................................................... 41  
  4.1 Configuration limits for WBM and CLI ...................................................................................... 41  
  4.2 Interfaces and system functions ............................................................................................... 43  
  4.3 EtherNet/IP ................................................................................................................................... 48  
  4.4 PROFINET ................................................................................................................................... 49  
  4.5 VLAN ......................................................................................................................................... 50  
  4.6 MAC-based communication ........................................................................................................ 51  
  4.7 iPCF / iPCF-MC ......................................................................................................................... 52  
  4.8 iREF ......................................................................................................................................... 55  
  4.9 iPRP ......................................................................................................................................... 57  
  4.10 AeroScout .................................................................................................................................. 60  
  4.11 NAT/NAPT ............................................................................................................................... 62  
  4.12 SNMP ....................................................................................................................................... 63  
  4.13 Spanning Tree ........................................................................................................................... 66  
  4.13.1 RSTP, MSTP, CIST ................................................................................................................ 67  

5 Assignment of an IP address .................................................................................................................. 69  
  5.1 Structure of an IP address .......................................................................................................... 69  
  5.2 Initial assignment of an IP address ........................................................................................... 71  
  5.3 Address assignment with DHCP ............................................................................................... 72
# Table of contents

6 Configuring with Web Based Management ................................................................. 75

6.1 Web Based Management ......................................................................................... 75

6.2 Login ....................................................................................................................... 77

6.3 "Wizard" menu ......................................................................................................... 80

6.3.1 Basic Wizard ......................................................................................................... 80

6.3.1.1 System Settings ................................................................................................. 81

6.3.1.2 Country Settings ............................................................................................... 83

6.3.1.3 IP Address Settings .......................................................................................... 84

6.3.1.4 Management Interfaces ..................................................................................... 85

6.3.1.5 Antenna Settings .............................................................................................. 87

6.3.1.6 Radio Settings ................................................................................................... 88

6.3.1.7 Access Point Settings ....................................................................................... 91

6.3.1.8 Client Settings ................................................................................................ 93

6.3.1.9 Client Setting Allowed Channels ...................................................................... 95

6.3.1.10 Security settings ............................................................................................ 97

6.3.1.11 Dot1x Supplicant Settings ................................................................................ 100

6.3.1.12 Dot1x RADIUS Server Settings ..................................................................... 101

6.3.1.13 Summary of the settings ................................................................................ 102

6.4 "Information" menu ................................................................................................. 103

6.4.1 Start page ............................................................................................................. 103

6.4.2 Version information ............................................................................................ 108

6.4.3 Identification & Maintenance ............................................................................. 110

6.4.4 Address Resolution Protocol (ARP) table ......................................................... 111

6.4.5 Log Tables .......................................................................................................... 112

6.4.5.1 Event log .......................................................................................................... 112

6.4.5.2 WLAN authentication log ................................................................................ 115

6.4.6 Faults .................................................................................................................. 117

6.4.7 Spanning Tree ..................................................................................................... 118

6.4.8 Ethernet Statistik .................................................................................................. 122

6.4.8.1 Interface statistics ............................................................................................ 122

6.4.8.2 Packet Size ...................................................................................................... 123

6.4.8.3 Frame Type ...................................................................................................... 124

6.4.8.4 Packet Error .................................................................................................... 125

6.4.9 Learning Table .................................................................................................... 126

6.4.10 DHCP Server Bindings ..................................................................................... 127

6.4.11 Simple Network Management Protocol v3 (SNMPv3) group overview ............ 129

6.4.12 Security .............................................................................................................. 130

6.4.12.1 Overview ........................................................................................................ 130

6.4.12.2 Supported Function Rights ............................................................................ 133

6.4.12.3 Roles .............................................................................................................. 134

6.4.12.4 Groups .......................................................................................................... 135

6.4.12.5 Inter AP Blocking .......................................................................................... 135

6.4.13 WLAN ................................................................................................................ 137

6.4.13.1 Overview AP .................................................................................................. 137

6.4.13.2 Client List ...................................................................................................... 139

6.4.13.3 WDS List ...................................................................................................... 141

6.4.13.4 Overlap AP .................................................................................................... 142

5.4 Address assignment with the Primary Setup Tool .................................................. 73

5.5 Address assignment with STEP 7 .......................................................................... 74

75
6.5.11.3 v3 Groups ............................................................................................................................. 198
6.5.12.1 Manual Setting ...................................................................................................................... 206
6.5.12 System Time ......................................................................................................................... 205
6.5.11.1 General ................................................................................................................................. 198
6.5.11 SNMP .................................................................................................................................... 198
6.5.10.4 Static Leases ........................................................................................................................ 196
6.5.10.3 DHCP Options ...................................................................................................................... 194
6.5.12.3 DST Configuration ................................................................................................................ 210
6.5.12.5 NTP Client ............................................................................................................................. 216
6.5.12.4 SNTP Client .......................................................................................................................... 213
6.5.12.6 SIMATIC Time Client ............................................................................................................ 218
6.5.15.1 Power Supply ........................................................................................................................ 222
6.5.14 iREF Client List ....................................................................................................................... 157
6.5.15.2 iREF WDS List ..................................................................................................................... 158
6.5.15.3 AeroScout ............................................................................................................................. 160
6.5 "System" menu .............................................................................................................................. 162
6.5.1 System Configuration............................................................................................................ 162
6.5.2 General ................................................................................................................................. 165
6.5.2.1 Device ................................................................................................................................... 165
6.5.2.2 Coordinates ........................................................................................................................... 166
6.5.3 Agent Internet Protocol (IP) .................................................................................................... 168
6.5.4 Domain Name System (DNS) client ..................................................................................... 169
6.5.5 Restart ..................................................................................................................................... 171
6.5.6 Commit Control ....................................................................................................................... 172
6.5.7 Load & Save ................................................................................................................................ 174
6.5.7.1 HTTP ..................................................................................................................................... 176
6.5.7.2 TFTP ..................................................................................................................................... 180
6.5.7.3 Passwords ............................................................................................................................. 183
6.5.8 Events .................................................................................................................................... 185
6.5.8.1 Configuration ......................................................................................................................... 185
6.5.8.2 Severity Filters ....................................................................................................................... 187
6.5.9 Client for Simple Mail Transfer Protocol (SMTP)................................................................. 188
6.5.10 DHCP................................................................................................................................. 190
6.5.10.1 DHCP Client ....................................................................................................................... 190
6.5.10.2 DHCP Server ....................................................................................................................... 192
6.5.10.3 DHCP Options .................................................................................................................... 194
6.5.10.4 Static Leases ....................................................................................................................... 196
6.5.11 SNTP.................................................................................................................................... 198
6.5.11.1 General ................................................................................................................................. 198
6.5.11.2 Traps .................................................................................................................................. 200
6.5.11.3 v3 Groups ............................................................................................................................. 201
6.5.11.4 v3 Users ............................................................................................................................... 201
6.5.12 System Time .......................................................................................................................... 205
6.5.12.1 Manual Setting .................................................................................................................. 206
6.5.12.2 DST Overview .................................................................................................................. 208
6.5.12.3 DST Configuration .......................................................................................................... 210
6.5.12.4 SNTP Client ....................................................................................................................... 213
6.5.12.5 NTP Client .......................................................................................................................... 216
6.5.12.6 SIMATIC Time Client ........................................................................................................ 218
6.5.13 Automatic Logout ............................................................................................................... 220
6.5.14 System Logging (Syslog) Client ......................................................................................... 221
6.5.15 Fault Monitoring ................................................................................................................... 222
6.5.15.1 Power Supply ..................................................................................................................... 222
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.5.15.2</td>
<td>Link Change</td>
<td>224</td>
</tr>
<tr>
<td>6.5.16</td>
<td>PROFINET</td>
<td>225</td>
</tr>
<tr>
<td>6.5.17</td>
<td>EtherNet/IP</td>
<td>227</td>
</tr>
<tr>
<td>6.5.18</td>
<td>PLUG</td>
<td>229</td>
</tr>
<tr>
<td>6.5.18.1</td>
<td>Configuration</td>
<td>229</td>
</tr>
<tr>
<td>6.5.18.2</td>
<td>License</td>
<td>232</td>
</tr>
<tr>
<td>6.5.19</td>
<td>Ping</td>
<td>234</td>
</tr>
<tr>
<td>6.6</td>
<td>&quot;Interfaces&quot; menu</td>
<td>235</td>
</tr>
<tr>
<td>6.6.1</td>
<td>Ethernet</td>
<td>235</td>
</tr>
<tr>
<td>6.6.1.1</td>
<td>Overview</td>
<td>235</td>
</tr>
<tr>
<td>6.6.1.2</td>
<td>Configuration</td>
<td>237</td>
</tr>
<tr>
<td>6.6.2</td>
<td>WLAN</td>
<td>239</td>
</tr>
<tr>
<td>6.6.2.1</td>
<td>Basic</td>
<td>239</td>
</tr>
<tr>
<td>6.6.2.2</td>
<td>Advanced</td>
<td>243</td>
</tr>
<tr>
<td>6.6.2.3</td>
<td>Antennas</td>
<td>246</td>
</tr>
<tr>
<td>6.6.2.4</td>
<td>Allowed Channels</td>
<td>249</td>
</tr>
<tr>
<td>6.6.2.5</td>
<td>802.11n</td>
<td>251</td>
</tr>
<tr>
<td>6.6.2.6</td>
<td>AP</td>
<td>253</td>
</tr>
<tr>
<td>6.6.2.7</td>
<td>AP WDS</td>
<td>256</td>
</tr>
<tr>
<td>6.6.2.8</td>
<td>AP 802.11a/b/g Rates</td>
<td>258</td>
</tr>
<tr>
<td>6.6.2.9</td>
<td>AP 802.11n Rates</td>
<td>261</td>
</tr>
<tr>
<td>6.6.2.10</td>
<td>Client</td>
<td>264</td>
</tr>
<tr>
<td>6.6.2.11</td>
<td>Force Roaming</td>
<td>267</td>
</tr>
<tr>
<td>6.6.2.12</td>
<td>Signal recorder</td>
<td>269</td>
</tr>
<tr>
<td>6.6.2.13</td>
<td>Spectrum Analyzer</td>
<td>277</td>
</tr>
<tr>
<td>6.7</td>
<td>&quot;Layer 2&quot; menu</td>
<td>284</td>
</tr>
<tr>
<td>6.7.1</td>
<td>VLAN</td>
<td>284</td>
</tr>
<tr>
<td>6.7.1.1</td>
<td>General</td>
<td>284</td>
</tr>
<tr>
<td>6.7.1.2</td>
<td>Port-based VLAN</td>
<td>288</td>
</tr>
<tr>
<td>6.7.2</td>
<td>Dynamic Media Access Control (MAC) Aging</td>
<td>290</td>
</tr>
<tr>
<td>6.7.3</td>
<td>Spanning Tree</td>
<td>291</td>
</tr>
<tr>
<td>6.7.3.1</td>
<td>General</td>
<td>291</td>
</tr>
<tr>
<td>6.7.3.2</td>
<td>CIST General</td>
<td>293</td>
</tr>
<tr>
<td>6.7.3.3</td>
<td>CIST Port</td>
<td>295</td>
</tr>
<tr>
<td>6.7.3.4</td>
<td>MST General</td>
<td>299</td>
</tr>
<tr>
<td>6.7.3.5</td>
<td>MST Port</td>
<td>301</td>
</tr>
<tr>
<td>6.7.4</td>
<td>DCP Forwarding</td>
<td>303</td>
</tr>
<tr>
<td>6.7.5</td>
<td>LLDP</td>
<td>304</td>
</tr>
<tr>
<td>6.8</td>
<td>&quot;Layer 3&quot; menu</td>
<td>306</td>
</tr>
<tr>
<td>6.8.1</td>
<td>NAT</td>
<td>306</td>
</tr>
<tr>
<td>6.8.1.1</td>
<td>Basic</td>
<td>306</td>
</tr>
<tr>
<td>6.8.1.2</td>
<td>NAPT</td>
<td>307</td>
</tr>
<tr>
<td>6.9</td>
<td>&quot;Security&quot; menu</td>
<td>310</td>
</tr>
<tr>
<td>6.9.1</td>
<td>Users</td>
<td>310</td>
</tr>
<tr>
<td>6.9.1.1</td>
<td>Roles</td>
<td>310</td>
</tr>
<tr>
<td>6.9.1.2</td>
<td>Groups</td>
<td>312</td>
</tr>
<tr>
<td>6.9.1.3</td>
<td>Local Users</td>
<td>314</td>
</tr>
<tr>
<td>6.9.2</td>
<td>Passwords</td>
<td>317</td>
</tr>
<tr>
<td>6.9.2.1</td>
<td>Device passwords</td>
<td>317</td>
</tr>
<tr>
<td>6.9.2.2</td>
<td>Password options</td>
<td>319</td>
</tr>
</tbody>
</table>
# Table of contents

6.9.3  AAA .................................................................................................................. 320
6.9.3.1 User management .......................................................................................... 320
6.9.3.2 General ......................................................................................................... 322
6.9.3.3 RADIUS client ............................................................................................. 323
6.9.4  WLAN ................................................................................................................ 326
6.9.4.1 Basic (Access Point) .................................................................................... 326
6.9.4.2 Basic ............................................................................................................ 329
6.9.4.3 AP Communication ..................................................................................... 333
6.9.4.4 AP RADIUS Authenticator .......................................................................... 334
6.9.4.5 Client Radius Supplicant ............................................................................. 337
6.9.4.6 Keys ............................................................................................................. 339
6.9.5  MAC ACL .......................................................................................................... 340
6.9.5.1 Rules Configuration ..................................................................................... 340
6.9.5.2 Ingress Rules ............................................................................................... 341
6.9.5.3 Egress Rules ............................................................................................... 343
6.9.6  IP ACL ............................................................................................................. 345
6.9.6.1 Rules Configuration ..................................................................................... 345
6.9.6.2 Protocol Configuration ................................................................................ 347
6.9.6.3 Ingress Rules ............................................................................................... 348
6.9.6.4 Egress Rules ............................................................................................... 351
6.9.7  Management Access Control List .................................................................. 354
6.9.8  Inter AP blocking ............................................................................................ 357
6.9.8.1 Basic ........................................................................................................... 357
6.9.8.2 Allowed Addresses .................................................................................... 359
6.10  "iFeatures" menu .............................................................................................. 361
6.10.1 iPCF .............................................................................................................. 361
6.10.2 iPCF-MC ....................................................................................................... 364
6.10.3 iREF .............................................................................................................. 366
6.10.4 iPRP .............................................................................................................. 368
6.10.5 AeroScout ..................................................................................................... 371

7  Upkeep and maintenance ....................................................................................... 373
   7.1  Firmware update - via WBM ........................................................................... 373
   7.2  Device configuration with PRESET-PLUG ................................................... 374
   7.3  Embedding firmware in ConfigPack ............................................................... 377
   7.4  Restoring the default parameter settings ....................................................... 379

8  Troubleshooting/FAQ .......................................................................................... 381
   8.1  Firmware update via WBM or CLI not possible .......................................... 381
   8.2  Disrupted data transmission due to the received power being too high ........ 383
   8.3  Compatibility with predecessor products ................................................... 384
   8.4  Instructions for secure network design ......................................................... 385
   8.5  Configuring the device using the TIA Portal .............................................. 386
     8.5.1 Message: SINEMA configuration not yet accepted ......................... 387

A  Appendix A ........................................................................................................... 389
   A.1  MIB files supported by SCALANCE W700 ............................................. 389

B  Appendix B .......................................................................................................... 391
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>B.1 Private MIB variables of the SCALANCE W700</td>
<td>391</td>
</tr>
<tr>
<td>C Appendix C</td>
<td>393</td>
</tr>
<tr>
<td>C.1 Underlying standards</td>
<td>393</td>
</tr>
<tr>
<td>D Appendix D</td>
<td>395</td>
</tr>
<tr>
<td>D.1 Messages in the event log</td>
<td>395</td>
</tr>
<tr>
<td>D.2 Messages in the WLAN Authentication Log</td>
<td>400</td>
</tr>
<tr>
<td>Index</td>
<td>401</td>
</tr>
</tbody>
</table>
Introduction

1.1 Information on the Configuration Manual

Validity of the configuration manual
This Configuration Manual covers the following products:
- SCALANCE W734-1 RJ-45
- SCALANCE W774-1 RJ-45
This Configuration Manual applies to the following software version:
- SCALANCE W700 firmware as of version V 6.0

Purpose of the Configuration Manual
This Configuration Manual is intended to provide you with the information you require to commission and operate SCALANCE W700 devices correctly. It explains how to configure the SCALANCE W700 devices and how to integrate them in a WLAN network.
The operating instructions for the corresponding SCALANCE W700 devices describe how to install and connect up the devices correctly.

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 W770 / W730 Command Line Interface
  This document contains the CLI commands that are supported by SCALANCE W700 devices.
- Performance data 802.11 abgn SCALANCE W770/W730
  This document contains information about the frequency, modulation, transmit power and receiver sensitivity.
- SCALANCE W734-1/W774-1 Operating Instructions
  This document contains information on installing and connecting up the following products and their approvals.
  - SCALANCE W734-1 RJ-45
  - SCALANCE W774-1 RJ-45
- System Manual Structure of an Industrial Wireless LAN
  Apart from the description of the physical basics and a presentation of the main IEEE standards, this also contains information on data security and a description of the industrial applications of wireless LAN.
You should read this manual if you want to set up WLAN networks with a more complex structure (not simply a connection between two devices).

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

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

### SIMATIC NET manuals

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

- Using the search function:
  
  support.automation.siemens.com
  
  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
  
  Go to the required product group and make the following settings:
  
  tab "Entry list", Entry type "Manuals"

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

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

The "SIMATIC NET Industrial Ethernet Network Manual" contains information on other SIMATIC NET products that you can operate along with the SCALANCE W700 devices of this product line in an Industrial Ethernet network. There, you will find among other things optical performance data of the communication partners that you require for the installation.

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

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens’ products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. You will find more information about Industrial Security in: Industrial security (http://www.siemens.com/industrialsecurity)

To stay informed about product updates as they occur, sign up for a product-specific newsletter. You will find more information about this in Product support (https://support.industry.siemens.com/cs/ww/en/p/15247/pm)

SIMATIC NET glossary

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

You will find the SIMATIC NET glossary here:
- SIMATIC NET Manual Collection or product DVD
  The DVD ships with certain SIMATIC NET products.
- On the Internet under the following address:
  50305045 (http://support.automation.siemens.com/WW/view/en/50305045)
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.htm
- OSS_Scalance-W700_86.pdf

Trademarks

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

SIMATIC NET, SCALANCE, C-PLUG, RCOAX

Firmware

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

Abbreviations used

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

<table>
<thead>
<tr>
<th>Product group</th>
<th>The designation . . . stands for . . .</th>
<th>Product name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access point</td>
<td>W774-1</td>
<td>SCALANCE W774-1 RJ-45</td>
</tr>
<tr>
<td>Client</td>
<td>W734-1</td>
<td>SCALANCE W734-1 RJ-45</td>
</tr>
<tr>
<td>All SCALANCE W devices</td>
<td>W700</td>
<td>SCALANCE W774-1 RJ-45 SCALANCE W734-1 RJ-45</td>
</tr>
</tbody>
</table>

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

- **W74-1**: Access point
- **RJ-45**: RJ-45 jacks
- **M12 EEC**: M12 sockets
- Number of IWLAN interfaces
- **7**: Access point
- **3**: Client
Introduction

1.2 Type designations
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.
2.1 Network structures

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

Standalone configuration with access point

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

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

Figure 2-1 Standalone configuration of an access point. The gray area symbolizes the wireless range of the access point.
**Wireless access to a wired Ethernet network**

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

- **A single device as gateway:**
  A wireless network can be connected to a wired network via an access point.

- **Span of wireless coverage for the wireless network with several access points:**
  The access points are all configured with the same unique SSID (network name). All nodes that want to communicate over this network must also be configured with this SSID.

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

![Wireless connection of a mobile station over two cells (roaming)](image)
Multichannel configuration

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

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

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

Figure 2-3  Multichannel configuration on channels 1 and 2 with four access points
Wireless Distribution System (WDS)

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

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

![Figure 2-4 Implementation of WDS with four access points](image)
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.

Figure 2-5  Connecting a SIMATIC S7 PLC to a wireless LAN.
2.2 Possible applications of SCALANCE W700 devices

Note
The SIMATIC NET WLAN products use OpenSSL.
This is open source code with license conditions (BSD).
Please refer to the current license conditions.
Since the driver includes encryption software, you should also adhere to the appropriate regulations for your specific country.

Possible applications of the SCALANCE W774
The SCALANCE W774 is equipped with two Ethernet interfaces and a WLAN interface. This makes the device suitable for the following applications:

- The SCALANCE W774 forwards data within its transmission range from one node to another without a connection to wired Ethernet being necessary.
- The SCALANCE W774 can be used as a gateway from a wired to a wireless network.
- The SCALANCE W774 can be used as a wireless bridge between two networks.
- The SCALANCE W774 can be used as a bridge between two different frequencies.
- The SCALANCE W774 supports protection class IP30.

Possible applications of the SCALANCE W734
The SCALANCE W734 is equipped with two Ethernet interfaces and a WLAN interface. This makes the device suitable for the following applications:

- The SCALANCE W734 forwards data within its transmission range from one node to another without a connection to wired Ethernet being necessary.
- The SCALANCE W734 can be used as a gateway from a wired to a wireless network.
- The SCALANCE W734 can be used as a wireless bridge between two networks.
2.3 Product characteristics

Properties of the SCALANCE W700 devices

- The Ethernet interface supports the following:
  - 10 Mbps and 100 Mbps both in full and half duplex
  - 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)
  - Can operate in the 2.4 GHz and in the 5 GHz range

- IEEE 802.11h - Supplement to IEEE 802.11a
  In the 802.11h mode, the methods “Transmit Power Control (TPC)” as well as “Dynamic Frequency Selection (DFS)” are used in the range 5.25 - 5.35 and 5.47 - 5.75 GHz. In some countries, this allows the frequency subband of 5.47 - 5.725 GHz to be used in the outdoor area even with higher transmit powers.
  TPC is a method of adapting the transmit power.
  With DFS, the access point searches for primary users for 60 seconds before starting communication on the selected channel. During this time the access point does not send beacons. If signals are found on the channel, the channel is blocked for 30 minutes, the access point changes channel and repeats the check. Primary users are also searched for during operation.

- Support of the authentication standards WPA, WPA-PSK, WPA2, WPA2-PSK and IEEE 802.1x and the encryption methods WEP, AES and TKIP.

Note

The transmission standard IEEE 802.11n 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:

<table>
<thead>
<tr>
<th>IWLAN channel</th>
<th>WHART channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.11 b/g/n</td>
<td>IEEE 802.15.4</td>
</tr>
<tr>
<td>1</td>
<td>11 - 16</td>
</tr>
<tr>
<td>6</td>
<td>15 - 20</td>
</tr>
<tr>
<td>7</td>
<td>16 - 21</td>
</tr>
<tr>
<td>11</td>
<td>20 - 25</td>
</tr>
<tr>
<td>13</td>
<td>21 - 25</td>
</tr>
</tbody>
</table>

**Note**

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

**Features of the SCALANCE W700**

<table>
<thead>
<tr>
<th>Type</th>
<th>Number of WLAN ports</th>
<th>Antennas</th>
<th>Number and type of Ethernet interface</th>
<th>Degree of protection</th>
<th>Order no.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCALANCE W774-1 RJ-45</td>
<td>1</td>
<td>external</td>
<td>2 x 10/100 Mbps Ethernet (copper)</td>
<td>IP30</td>
<td>6GK5774-1FC00-0AA0 (1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6GK5774-1FC00-0AB0</td>
</tr>
<tr>
<td>SCALANCE W734-1 RJ-45</td>
<td>1</td>
<td>external</td>
<td>2 x 10/100 Mbps Ethernet (copper)</td>
<td>IP30</td>
<td>6GK5734-1FC00-0AA0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6GK5734-1FC00-0AB0 (1)</td>
</tr>
</tbody>
</table>

(1) US variant
2.4 IEEE 802.11n

Overview

The standard IEEE 802.11n is an expansion of the 802.11 standard and was approved in 2009.
Previous standards worked either in the 2.4 GHz frequency band (IEEE 802.11g/b) or in the 5 GHz frequency band (IEEE 802.11a). IEEE 802.11n can operate in both frequency band.

In the IEEE 802.11n standard, there are mechanisms implemented in PHY and MAC layers that increase the data throughput and improve the wireless coverage.

- MIMO antenna technology
- Maximum ratio combining (MRC)
- Spatial multiplexing
- Channel bonding
- Frame aggregation
- Accelerated guard interval
- Modulation and coding scheme
- Data throughput rates up to 450 Mbps (gross)

This is not possible on all 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 multiplexing

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

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

To be able to use channel bonding, the recipient must support 40 MHz transmissions. If the recipient does not support 40 MHz transmissions, the band is automatically reduced to 20 MHz. This means that IEEE 802.11n can also communicate with IEEE 802.11a/b/g devices.

The channel bonding is set on the "AP" WBM page with the "HT Channel Width [MHz]" parameter.

---

**Frame aggregation**

With IEEE 802.11n, it is possible to group together individual data packets to form a single larger packet; this is known as frame aggregation. There are two types of frame aggregation: Aggregated MAC Protocol Data Unit (A-MPDU) and Aggregated MAC Service Data Unit (A-MSDU).

The frame aggregation reduces the packet overheads. Frame aggregation can only be used if the individual data packets are intended for the same receiving station (client).

The SCALANCE W700 devices support both types of frame aggregation. You specify the settings for the A-MPDU data packet on the "AP 802.11n" WBM page.

---

**Accelerated guard interval**

The guard interval prevents different transmissions being mixed together. In telecommunications, this mixing is also known as intersymbol interference (ISI).

When the send time has elapsed, a send pause (guard interval) must be kept to before the next transmission begins.

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

The IEEE 802.11n standard supports different data rates. The data rates are based on the number of spatial streams, the modulation method and the channel coding. The various combinations are described in modulation and coding schemes.
2.5 Requirements for installation and operation of SCALANCE W700 devices

Requirements for installation and operation of SCALANCE W700 devices

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

Configuration information on the C-PLUG / KEY-PLUG

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

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

A PLUG may only be removed or inserted when the device is turned off. The device checks whether or not a PLUG is present at one second intervals. If it is detected that the PLUG was removed, there is a restart. If a valid KEY-PLUG was inserted in the device, the device changes to a defined error state following the restart. With SCALANCE W, the available wireless interfaces are deactivated in this case.

If the device was configured at some time with a PLUG, the device can no longer be used without this PLUG. To be able to use the device again, reset the device to the factory settings.

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

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

Note

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

• **Without PLUG**
  The device stores the configuration in internal memory. This mode is active when no PLUG is inserted.

• **With PLUG**
  The configuration stored on the PLUG is displayed over the user interfaces. If changes are made to the configuration, the device stores the configuration directly on the PLUG and in the internal memory. This mode is active as soon as a PLUG is inserted. As soon as the device is started with a PLUG inserted, the SCALANCE W700 starts up with the configuration data on the PLUG.

Note

**Incompatibility with previous versions with PLUG inserted**

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

License information on the KEY-PLUG

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

PLUG with preset function (PRESET-PLUG)

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

Note

Using configurations with DHCP

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

You assign fixed IP addresses extra following the basic installation.

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

Note

Restore factory defaults and restart with a PRESET PLUG inserted

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

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

For more detailed information on creating and using a PRESET PLUG refer to the section Upkeep and maintenance (Page 373).
2.7 Power over Ethernet (PoE)

General

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

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

Cable used for the power supply

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

- **Variant 2 (phantom power)**
  With phantom power, the power is supplied over the pairs that are used for data transfer, in other words, all eight (1 Gbps) or four (10/100 Mbps) wires are used both for the data transfer and the power supply.

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

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

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

Endspan

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

Midspan

Midspan is used when the switch is not PoE-compliant. The power is supplied by an additional device between the switch and end device. In this case, only data rates of 10/100 Mbps can be achieved because the power is supplied on redundant wires.
A Siemens power insert can also be used as the interface for the power input. Since a power insert supports a power supply of 24 VDC, it does not conform with 802.3af or IEEE 802.3at. The following restrictions relating to the use of power inserts should be noted:

WARNING

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

### Cable lengths

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

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

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

<table>
<thead>
<tr>
<th>Cable type</th>
<th>Accessory (plug, outlet, TP cord)</th>
<th>Permitted cable length</th>
</tr>
</thead>
<tbody>
<tr>
<td>IE FC standard cable, 4×2, 24 AWG</td>
<td>with IE FC RJ-45 Plug 180, 4x2</td>
<td>0 to 90 m</td>
</tr>
<tr>
<td>IE FC flexible cable, 4×2, 24 AWG</td>
<td>with IE FC RJ-45 Plug 180, 4x2</td>
<td>0 to 60 m</td>
</tr>
<tr>
<td>IE FC standard cable, 4×2, 22 AWG</td>
<td>with IE FC Outlet RJ-45 + 10 m TP cord</td>
<td>0 to 100 m + 10 m TP cord</td>
</tr>
</tbody>
</table>
2.7 Power over Ethernet (PoE)

Table 2- 3  Fitting connectors

<table>
<thead>
<tr>
<th>PIN</th>
<th>Color of the wire CAT5</th>
<th>Color of the wire CAT6a</th>
<th>Use</th>
<th>Phantom power</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Yellow</td>
<td>Green/white</td>
<td>Data</td>
<td>Data/power</td>
</tr>
<tr>
<td>2</td>
<td>Orange</td>
<td>Green</td>
<td>Data</td>
<td>Data/power</td>
</tr>
<tr>
<td>3</td>
<td>White</td>
<td>Orange/white</td>
<td>Data</td>
<td>Data/power</td>
</tr>
<tr>
<td>6</td>
<td>Blue</td>
<td>Orange</td>
<td>Data</td>
<td>Data/power</td>
</tr>
<tr>
<td>4</td>
<td>Blue</td>
<td>Power</td>
<td>unused at 10/100 Mbps</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Blue/white</td>
<td>Power</td>
<td>unused at 10/100 Mbps</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Brown/white</td>
<td>Power</td>
<td>unused at 10/100 Mbps</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Brown</td>
<td>Power</td>
<td>unused at 10/100 Mbps</td>
<td></td>
</tr>
</tbody>
</table>

LEDs for PoE on the SCALANCE W700 device

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

2.7 Power over Ethernet (PoE)
Security recommendations

To prevent unauthorized access, note the following security recommendations.

General

- You should make regular checks to make sure that the device meets these recommendations and/or other security guidelines.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products.
- When confidential zones are used, the internal and external network are disconnected, an attacker cannot access the data from the outside.
- Operate the device only within a protected network area.
- Use additional devices with VPN functionality (e.g. SCALANCE S) to encrypt and authenticate communication from and to the devices.
- For data transfer via a non-secure network, use an encrypted VPN tunnel (IPsec) by using additional devices with VPN functionality (e.g. SCALANCE S).
- For operation of the device in a non-secure infrastructure no product liability will be accepted.
- Separate connections correctly (WBM, Telnet, SSH etc.).

Physical access

- Restrict physical access to the device to qualified personnel.
- The memory card or the PLUG (C-PLUG, KEY-PLUG, security PLUG) contains sensitive data such as certificates, keys etc. that can be read out and modified.

Software (security functions)

- Keep the software up to date. Check regularly for security updates of the product. You will find information on this on the Internet pages "Industrial Security (http://www.siemens.com/industrialsecurity)"
- Inform yourself regularly about security advisories and bulletins published by Siemens ProductCERT.
- Only activate protocols that you really require to use the device.
- 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.
- Restrict access to the device with a firewall or rules in an access control list (ACL - Access Control List).
Security recommendations

- If RADIUS authentication is via remote access, make sure that the communication is within the secured network area or is via a secure channel.
- The option of VLAN structuring provides good protection against DoS attacks and unauthorized access. Check whether this is practical or useful in your environment.
- Enable logging functions. Use the central logging function to log changes and access attempts centrally. Check the logging information regularly.
- Configure a Syslog server to forward all logs to a central location.
- Use WPA2/ WPA2-PSK with AES to protect the WLAN. If iPCF or iPCF-MC is used, use the AES encryption.

Passwords

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

Keys and certificates

This section deals with the security keys and certificates you require to set up HTTPS (HyperText Transfer Protocol Secured Socket Layer).

- We strongly recommend that you create your own HTTPS certificates and make them available.
  There are preset certificates and keys on the device. The preset and automatically created HTTPS certificates are self-signed.
  We recommend that you use HTTPS certificates signed either by a reliable external or by an internal certification authority. The HTTPS certificate checks the identity of the device and controls the encrypted data exchange. You can install the HTTPS certificate via the WBM (System > Load and Save).
- Handle user-defined private keys with great caution if you use user-defined SSH or SSL keys.
- Use the certification authority including key revocation and management to sign the certificates.
- Verify certificates and fingerprints on the server and client to avoid "man in the middle" attacks.
- We recommend that you use certificates with a key length of 2048 bits.
- Change keys and certificates immediately, if there is a suspicion of compromise.
Secure/non-secure protocols

- For the DCP function, enable the "DCP read-only" mode after commissioning.
- Avoid and disable non-secure protocols, for example Telnet and TFTP. For historical reasons, these protocols are still available, however not intended for secure applications. Use non-secure protocols on the device with caution.
- The following protocols provide secure alternatives:
  - SNMPv1/v2 → SNMPv3
    Check whether use of SNMPv1 is necessary. SNMPv1 is classified as non-secure. Use the option of preventing write access. The product provides you with suitable setting options.
    If SNMP is enabled, change the community names. If no unrestricted access is necessary, restrict access with SNMP.
    Use SNMPv3 in conjunction with passwords.
  - HTTP → HTTPS
  - Telnet → SSH
  - SNTP → NTP
- Use secure protocols when access to the device is not prevented by physical protection measures.
- To prevent unauthorized access to the device or network, take suitable protective measures against non-secure protocols.
- If you require non-secure protocols and services, operate the device only within a protected network area.
- Restrict the services and protocols available to the outside to a minimum.
Available protocols per port

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

The table includes the following columns:

- **Protocol**
  - All protocols that the device supports

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

- **Port status**
  - Open
    - The port is always open and cannot be closed.
  - Open (when configured)
    - The port is open if it has been configured.

**Note**

With some protocols the port may be open although the corresponding protocol is disabled, for example TFTP.

- **Default status of the port**
  - Open
    - As default the port is open.
  - Closed
    - As default the port is closed.
### Security recommendations

**Authentication**

Specifies whether or not the protocol is authenticated during access.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port number</th>
<th>Port status</th>
<th>Default status of the port</th>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH</td>
<td>TCP/22</td>
<td>Open (when configured)</td>
<td>Open</td>
<td>Yes</td>
</tr>
<tr>
<td>TELNET</td>
<td>TCP/23</td>
<td>Open (when configured)</td>
<td>Open</td>
<td>Yes</td>
</tr>
<tr>
<td>HTTP</td>
<td>TCP/80</td>
<td>Open (when configured)</td>
<td>Open</td>
<td>Yes</td>
</tr>
<tr>
<td>HTTPS</td>
<td>TCP/443</td>
<td>Open (when configured)</td>
<td>Open</td>
<td>Yes</td>
</tr>
<tr>
<td>SNTP NTP</td>
<td>UDP/123</td>
<td>Open (when configured)</td>
<td>Closed</td>
<td>No</td>
</tr>
<tr>
<td>SNMP</td>
<td>UDP/161</td>
<td>Open (when configured)</td>
<td>Open</td>
<td>Yes</td>
</tr>
<tr>
<td>PROFINET</td>
<td>UDP/34964, UDP/49154, 49155</td>
<td>Open</td>
<td>Open</td>
<td>No</td>
</tr>
<tr>
<td>Syslog</td>
<td>UDP/514</td>
<td>Open (when configured)</td>
<td>Open</td>
<td>No</td>
</tr>
<tr>
<td>EtherNet/IP</td>
<td>TCP/44818, UDP/2222, 4818</td>
<td>Open (when configured)</td>
<td>Open</td>
<td>No</td>
</tr>
<tr>
<td>DHCP</td>
<td>UDP/67,68</td>
<td>Open (when configured)</td>
<td>Closed</td>
<td>No</td>
</tr>
<tr>
<td>RADIUS</td>
<td>UDP/1812,1813</td>
<td>Open (when configured)</td>
<td>Closed</td>
<td>No</td>
</tr>
<tr>
<td>TFTP</td>
<td>UDP/69</td>
<td>Open (when configured)</td>
<td>Closed</td>
<td>No</td>
</tr>
</tbody>
</table>
## 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.

<table>
<thead>
<tr>
<th>Configurable function</th>
<th>Maximum number</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System</strong></td>
<td></td>
</tr>
<tr>
<td>Syslog server</td>
<td>3</td>
</tr>
<tr>
<td>E-mail server</td>
<td>3</td>
</tr>
<tr>
<td>SNMPv1 trap recipient</td>
<td>10</td>
</tr>
<tr>
<td>SNTP server</td>
<td>1</td>
</tr>
<tr>
<td>NTP server</td>
<td>1</td>
</tr>
<tr>
<td>DHCP pools</td>
<td>1</td>
</tr>
<tr>
<td>IPv4 addresses managed by the DHCP server (dynamic + static)</td>
<td>100</td>
</tr>
<tr>
<td>DHCP static assignments per DHCP pool</td>
<td>20</td>
</tr>
<tr>
<td>DHCP options</td>
<td>20</td>
</tr>
<tr>
<td><strong>Interfaces</strong></td>
<td></td>
</tr>
<tr>
<td>Force destination addresses for roaming</td>
<td>10</td>
</tr>
<tr>
<td><strong>Layer 2</strong></td>
<td></td>
</tr>
<tr>
<td>Virtual LANs (port-based; including VLAN 1)</td>
<td>16</td>
</tr>
<tr>
<td>Multiple Spanning Tree instances</td>
<td>16</td>
</tr>
</tbody>
</table>
### Configurable function

<table>
<thead>
<tr>
<th>Security</th>
<th>Configurable function</th>
<th>Maximum number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IP addresses from RADIUS servers</td>
<td>• AAA: 4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• WLAN: 2</td>
</tr>
<tr>
<td></td>
<td>Management ACLs (access rules for management)</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>MAC ACL rule configuration</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Ingress and egress rules for MAC ACL (total)</td>
<td>40 per interface (20 ingress rules / 20 egress rules)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Client: 80 (P1, WLAN)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Access point: 680 (P1, WDS 1.Y, VAP 1.Y)</td>
</tr>
<tr>
<td></td>
<td>IP ACL rule configuration</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Ingress and egress rules for port ACL IP (total)</td>
<td>40 per interface (20 ingress rules / 20 egress rules)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Client: 120 (P1, WLAN, management VLAN)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Access point: 720 (P1, WDS 1.Y, VAP 1.Y, management VLAN)</td>
</tr>
<tr>
<td></td>
<td>User roles</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>User groups</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>Users</td>
<td>28</td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th></th>
<th>Client device SCALANCE W734-1 RJ-45</th>
<th>Access points W774-1 RJ-45</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless interface</td>
<td>WLAN 1</td>
<td>WLAN 1</td>
</tr>
<tr>
<td></td>
<td><strong>IP interface:</strong></td>
<td></td>
</tr>
<tr>
<td>LAN interface</td>
<td>P1</td>
<td>P1</td>
</tr>
<tr>
<td>VLAN</td>
<td>ManagementVLAN</td>
<td>ManagementVLAN</td>
</tr>
<tr>
<td></td>
<td><strong>VAP interface</strong> 1)</td>
<td>VAP 1.Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Y = 1 8</td>
</tr>
<tr>
<td>WDS interface 1)</td>
<td></td>
<td>WDS 1.Y</td>
</tr>
<tr>
<td>VLAN</td>
<td>16</td>
<td>16</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Information</th>
<th>Security</th>
<th>Access point mode</th>
<th>Access points in client mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Inter AP blocking</td>
<td>✓</td>
<td>W780 iFeatures (MLFB 6GK5 907-8PA00)</td>
</tr>
<tr>
<td></td>
<td>W700 Security (MLFB GK5907-0PA00)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| WLAN | Overview AP | ✓ | - |
| Client List | ✓ | - |
| WDS List | ✓ | - |
| Overlap AP | ✓ | - |
| Force Roaming | ✓ | - |
| Overview Client | - | ✓ |
| Available AP | - | ✓ |
| IP Mapping | - | ✓ |

| WLAN Statistics | Faults | ✓ | ✓ |
| Management Sent | ✓ | ✓ |
| Management Received | ✓ | ✓ |
| Data Sent | ✓ | ✓ |
| Data Received | ✓ | ✓ |

| WLAN iFeatures | iREF Client List | ✓ | W780 iFeatures (MLFB 6GK5 907-8PA00) | - |
| iREF WDS List | ✓ | W780 iFeatures (MLFB 6GK5 907-8PA00) | - |
## Technical basics

### 4.2 Interfaces and system functions

<table>
<thead>
<tr>
<th>System</th>
<th>Interfaces</th>
<th>WLAN</th>
<th>Layer 3</th>
<th>Access point mode</th>
<th>Access points in client mode</th>
<th>Client devices</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>W780 iFeatures (MLFB 6GK5 907-8PA00)</td>
<td>AeroScout</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PROFINET</td>
<td>System</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EtherNet/IP</td>
<td>Interfaces</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WLAN</td>
<td>Basic</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Expansions</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Antennas</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Allowed Channels</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>802.11n</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AP</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AP WDS</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AP 802.11a/b/g Rates</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AP 802.11n Rates</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Client 802.11a/b/g Rates</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Client 802.11n Rates</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Force Roaming</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Signal recorder</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Spectrum Analyzer</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>NAT</td>
<td>Basic</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NAPT</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Technical basics

#### 4.2 Interfaces and system functions

<table>
<thead>
<tr>
<th>Security</th>
<th>WLAN</th>
<th>Access point mode</th>
<th>Access points in client mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Basic</td>
<td>✓✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>AP Communication</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>AP RADIUS Authenticator</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Client RADIUS Supplicant</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Keys</td>
<td>✓✓</td>
<td>-</td>
</tr>
</tbody>
</table>

| Inter AP Blocking | Basic | ✓           | -                           |
|                   |       | W780 iFeatures (MLFB 6GK5 907-8PA00) |   |
|                   |       | W700 Security (MLFB 6GK5907-0PA00) |   |
| Allowed Addresses | ✓   | W780 iFeatures (MLFB 6GK5 907-8PA00) |   |
|                   |       | W700 Security (MLFB 6GK5907-0PA00) |   |

<table>
<thead>
<tr>
<th>iFeatures</th>
<th>iPCF</th>
<th>✓✓</th>
<th>✓✓</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>W780 iFeatures (MLFB 6GK5 907-8PA00)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>W780 iFeatures (MLFB 6GK5 907-8PA00)</td>
<td>Access point in client mode:</td>
<td>W780 iFeatures (MLFB 6GK5 907-8PA00)</td>
</tr>
<tr>
<td></td>
<td>Client: W740 iFeatures (MLFB 6GK5 907-4PA00)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

|                | iPCFv1 | ✓✓ | ✓✓ |
|                | W780 iFeatures (MLFB 6GK5 907-8PA00) | Access point in client mode: | W780 iFeatures (MLFB 6GK5 907-8PA00) |
|                | Client: W740 iFeatures (MLFB 6GK5 907-4PA00) |   |   |

|                | iPCF-MC | ✓✓ | ✓✓ |
|                | Only dual APs W780 iFeatures (MLFB 6GK5 907-8PA00) | Access point in client mode: | W780 iFeatures (MLFB 6GK5 907-8PA00) |
|                | Client: W740 iFeatures (MLFB 6GK5 907-4PA00) |   |   |
## 4.2 Interfaces and system functions

<table>
<thead>
<tr>
<th>Access point mode</th>
<th>Access points in client mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>iPRP</strong></td>
<td>✓ W780 iFeatures (MLFB 6GK5 907-8PA00)</td>
</tr>
<tr>
<td><strong>iREF</strong></td>
<td>✓ W780 iFeatures (MLFB 6GK5 907-8PA00)</td>
</tr>
<tr>
<td><strong>AeroScout</strong></td>
<td>✓ W780 iFeatures (MLFB 6GK5 907-8PA00)</td>
</tr>
</tbody>
</table>
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 227)".

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 Sheets (EDS) are electronic datasheets for describing devices.

The EDS required for EtherNet/IP operation can be found in "System > Load&Save (Page 174)".
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 225)".

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.

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

Options for the VLAN assignment

There are various options for the assignment to VLANs:

- Port-based VLAN
  Each port of a device is assigned a VLAN ID. You configure port-based VLAN in "Layer 2 > VLAN (Page 288)".

- 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.
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 the Primary Setup Tool and configured with WBM or CLI.
- As soon as there is a link on the Ethernet interface, the device adopts the source MAC address of the first received frame.

Note

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

MAC mode "Layer 2 Tunnel"

With the setting "Layer 2 Tunnel", the client provides information about the devices downstream from it when it logs in to 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: 8
4.7 iPCF / iPCF-MC

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

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

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

  You configure iPCF in "iFeatures > iPCF (Page 361)".

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

  You configure iPCF-MC in "iFeatures > iPCF-MC (Page 364)".

iPCF / iPCF-MC - how it works

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

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

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

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

This does not mean that the client needs to change when there is a signal strength < 60 % (< -65 dBm). Make sure that access points are available with adequate signal strength.
Figure 4-1  Configuration example of 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 and iPCF-MC are developments of Siemens AG and function only with nodes on which iPCF / iPCF-MC is implemented.
- With an access point with several WLAN interfaces, it is possible to use both iPCF as well as standard WLAN at the same time.
- Access points with a WLAN interface cannot take part in the iPCF-MC procedures, iPCF is, however, possible.

Requirements for iPCF-MC

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

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

- Only 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 iREF

How it works

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

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

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

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

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

You configure iREF in “iFeatures > iREF (Page 366)”

Requirement

- To be able to use iREF, the SCALANCE W700 device must have at least 2 activated antennas.
4.8 iREF

Restrictions

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

Advantages

- Due to the directional data transmission and dynamic deactivation of antennas that do not radiate in the direction of the particular client, interference can be reduced.
- The signal strength is improved because the active antenna always has the maximum permitted transmit power available.
4.9 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. iPRP 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 among other things adds the VLAN ID and a sequence number. The RedBox sends a copy of the frame at the same time on both Ethernet interfaces via both networks.

With PRP the SCALANCE W700 devices PRP can be used in wireless networks.
The access points (AP 1, AP 2 and AP 3) and the RedBox A are connected to each other via a switch. The PRP frames are sent to the access points via both networks (PRP A, PRP B). The access points receive the PRP frames.

The PRP frames are sent at the same time on two different wireless links to the recipients. The clients A and B are connected to different access points at the same time. The clients are never connected to the access point via the same interface.

The RedBox forwards the first frame to arrive and discards the second PRP frame.

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

If for example communication between AP1 and client A is not possible, the PRP frame comes to its destination via redundant client B.

You configure iPRP in "iFeatures > iPRP".
Requirement

- The base bridge mode "802.1Q VLAN Bridge" is set.
- The VLANs have been created.
- The VLANs are configured on the same interface.
- Access point mode: The VAP interface is enabled.
- Client mode: In MAC mode "Layer 2 Tunnel" is set.
- Depending on the configuration the clients can communicate with every access point.
4.10 AeroScout

AeroScout tags

SCALANCE W700 devices support tags of the AeroScout company. Tags are battery-operated RFID sensors that send their data cyclically as multicast frames.

Among other things, AeroScout tags have the following features:

- **Ambient temperature**
  If a tag is fitted to a SCALANCE W700 device or material, it is possible to monitor whether a selected ambient temperature is being maintained.

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

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

- **LED**
  This provides information on the operating status of the tag.

Note

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

How it works

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

If the WLAN interface of the access point receives the AeroScout frame, this is converted into a UDP datagram. The SCALANCE W700 device forwards the UDP datagram along with the information about the signal strength (RSSI) to a PC. The AeroScout Engine runs on the PC and evaluates the received information.

Note

It is not advisable to use PROFINET communication and AeroScout together on one wireless interface.
Accuracy of localization

To achieve optimum precision in the localization of AeroScout Tags,

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

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

To translate the internal into the global IP address, the NAT device maintains a translation list. The address assignment is automatic. You configure the address assignment in "Layer 3 > NAT > Basic (Page 306)".

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

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

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

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

If a client from the global network wants to use a service in the internal network, the translation list for the static address assignment needs to be configured. You configure the translation list for NAPT in "Layer 3 > NAT > NAPT (Page 307)".
Introduction

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

Tasks of SNMP:

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

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

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

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

Standard values of the community strings:

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

Note

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

Further simple protection mechanisms at the device level:

- Allowed Host
  The IP addresses of the monitoring systems are known to the monitored system.

- Read Only
  If you assign "Read Only" to a monitored device, monitoring stations can only read out data but cannot modify it.

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

The central station is also known as the management station. An SNMP agent is installed on the devices to be monitored with which the management station exchanges data.
The management station sends data packets of the following type:

- **GET**
  Request for a data record from the SNMP agent

- **GETNEXT**
  Calls up the next data record.

- **GETBULK** (available as of SNMPv2c)
  Requests multiple data records at one time, for example several rows of a table.

- **SET**
  Contains parameter assignment data for the relevant device.

The SNMP agent sends data packets of the following type:

- **RESPONSE**
  The SNMP agent returns the data requested by the manager.

- **TRAP**
  If a certain event occurs, the SNMP agent itself sends traps.

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

### SNMPv3

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

SNMPv3 supports:

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

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.
4.13 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.
4.13.1 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.
5 Assignment of an IP address

5.1 Structure of an IP address

Address classes

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

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

XXX.XXX.XXX.XXX

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

Subnet mask

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

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

Example of a class B network:

The standard subnet address for class B networks is 255.255.0.0; in other words, the last two bytes are available for defining a subnet. If 16 subnets must be defined, the third byte of the subnet address must be set to 11100000 (binary notation). In this case, this results in the subnet mask 255.255.240.0.

To find out whether two IP addresses belong to the same subnet, the two IP addresses and the subnet mask are ANDed bit by bit. If both logic operations have the same result, both IP addresses belong to the same subnet, for example, 141.120.246.210 and 141.120.252.108.
Outside the local area network, the distinction between network ID and host ID is of no significance, in this case packets are delivered based on the entire IP address.

**Note**

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

Configuration options

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

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

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

Note

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

Properties of DHCP

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

- DHCP can be used both when starting up a device and during ongoing operation.
- The assigned IP address remains valid only for a limited time known as the lease time. 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 or the system name. You configure the parameter in "System > DHCP Client (Page 190)".
- The following DHCP options are supported:
  - 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
  - DHCP option 82: Assignment of IP addresses depending on the device index, switch port, the VLAN ID or user-defined identification values of the DHCP relay agent.

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.
5.4 Address assignment with the Primary Setup Tool

Introduction

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

Requirement

The devices can be reached via Ethernet.

Note

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

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


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

How it works

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

The user enters the configuration data in the HTML pages sent by the device. The device evaluates this information and generates reply pages dynamically.

The advantage of this method is that only a Web browser is required on the client.

Note

Secure connection

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

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

Requirements

WBM display

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

The display of the WBM was tested with the following desktop Web browsers:
- Microsoft Internet Explorer 11

**Note**

**Compatibility view**

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

- Mozilla Firefox 38 ESR
- Chrome V46

**Display of the WBM on mobile devices**

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

<table>
<thead>
<tr>
<th>Resolution</th>
<th>Operating system</th>
<th>Internet browser</th>
</tr>
</thead>
<tbody>
<tr>
<td>960 x 640 pixels</td>
<td>Android as of version 4.2.1</td>
<td>Chrome as of version 18 on Android</td>
</tr>
<tr>
<td></td>
<td>iOS as of version 6.0.2</td>
<td>Safari as of version 6 on iOS</td>
</tr>
</tbody>
</table>

- 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 on the WBM pages and how you work with them on mobile devices may differ compared with the same pages on desktop devices. Some pages also have an optimized display for mobile devices.
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 client PC. With the ping command, you can check whether or not a connection exists.
2. In the address box of the Internet browser, enter the IP address or the URL of the device. If there is a problem-free connection to the device, the logon page of Web Based Management (WBM) is displayed.
### Configuring with Web Based Management

#### 6.2 Login

Logging in using the Internet browser

**Selecting the language of the WBM**

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

---

**Note**

**Available languages**

As of version 5.2 English and German are available. Other languages will follow in a later version.

---

Logon with HTTP

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

![Login Screen](image-url)

---

SCALANCE W770/W730 to IEEE 802.11n Web Based Management
Configuration Manual, 06/2016, C79000-G8976-C323-06
The following steps apply when logging on, whichever of the above options you choose:

1. Enter the following in the "Name" input box:
   - "admin": With this user type, you can change the settings of the device (read and write access to the configuration data).

2. Enter your password in the "Password" input box.
   When you log in for the first time or following a "Restore Factory Defaults and Restart", enter the standard password in the "Password" input box.
   - "admin": Standard password "admin"

3. Click the "Login" button or confirm your entry with "Enter".
   When you log in for the first time or following a "Restore Factory Defaults and Restart", with the default user "admin" you will be prompted to change the password.
   You need to repeat the password as confirmation. The password entries must match.
   Click the "Set Values" button to complete the action and activate the new password.

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

Logon with HTTPS

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

1. Click on the link "Switch to secure HTTP" on the login page or enter "https://" and the IP address of the device in the address box of the Internet browser.

2. Check the displayed certificate warning and confirm it if applicable.
   The logon page of Web Based Management appears.

3. Enter the following in the "Name" input box:
   - "admin": With this user type, you can change the settings of the device (read and write access to the configuration data).

4. Enter your password in the "Password" input box.
   When you log in for the first time or following a "Restore Factory Defaults and Restart", enter the standard password in the "Password" input box.
   - "admin": Standard password "admin"

5. Click the "Login" button or confirm your entry with "Enter".
   When you log on for the first time or following a "Restore Factory Defaults and Restart", with the default user "admin" you will be prompted to change the password.
   You need to repeat the password as confirmation. The password entries must match.
   Click the "Set Values" button to complete the action and activate the new password.

Once you have logged in successfully, the start page appears.
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 "Assignment of an IP address (Page 69)".
- You are logged on in WBM as the "admin" user. For more detailed information, refer to the section "Login (Page 77)".

Starting the Basic Wizard

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

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

Buttons you require often

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

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next</td>
<td>Goes to the next page</td>
</tr>
<tr>
<td>Previous</td>
<td>Goes back to the previous page</td>
</tr>
<tr>
<td>Adopt</td>
<td>The Basic Wizard is closed without adopting the settings.</td>
</tr>
<tr>
<td>Set Values</td>
<td>Saves the configuration and exits the Wizard.</td>
</tr>
</tbody>
</table>

Navigation within the pages of the Basic Wizard is possible only with the "Prev" 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.
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](image)

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.

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.

Description

The page contains the following boxes:

- **Telnet Server**
  enable or disable the "Telnet Server" service for unencrypted access to the CLI.

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

- **HTTPS Server only**
  Enable or disable access using HTTPS.
• **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.

```
<table>
<thead>
<tr>
<th>Connector</th>
<th>Antenna Type</th>
<th>2.4 GHz Gain [dB]</th>
<th>5 GHz Gain [dB]</th>
<th>Cable Length [m]</th>
<th>Additional Attenuation [dB]</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1 A1</td>
<td>Not defined</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>R1 A2</td>
<td>Not defined</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

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".

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

**Note**

50 Ω terminating resistor

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

- **Antenna Gain [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.
6.3.1.6 Radio Settings

Introduction

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

Description

This table contains the following columns:

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

- **Enabled**
  Enable or disable the WLAN interface. The WLAN interfaces are disabled when the device is supplied.

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

- **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.
• **Frequency Band**
  Specify the frequency band. In client mode, dual-frequency operation is also possible.

  **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**
  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)**
  - Enabled
    If the access point discovers a disruption on the current channel, for example due to a primary user, it automatically switches to an alternative channel. You specify the alternative channel on the "Access Point Settings" Basic Wizard page. DFS is also the requirement for the use of certain wireless channels. This can only be enabled in the 5 GHz band.
  - Disabled
    The DFS function is not used.

• **Outdoor Mode**
  - Enabled
    In outdoor mode, the selection of country-dependent channels and the transmit power for operation are extended for outdoor use.
  - Disabled
    The device is being operated in indoor mode. In indoor mode, the selection of country-dependent channels and the transmit power for operation in a building are restricted.
6.3 "Wizard" menu

- **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".

---

**Note**

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

---

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

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.
• **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.
Description

Table 1 contains the following columns:

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

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

- **MAC Address**
  Enter the MAC address of the client. The input box can only be edited if you have set "Manual" for the "MAC Mode".

- **Any SSID**
  - **Enabled**
    In client mode, the device attempts to connect to the network with the best transmission quality and that has suitable security settings.
  - **Disabled**
    The client attempts to connect to the network from the SSID list that has the best transmission quality.

Table 2 contains the following columns:

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

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

- **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 Setting Allowed Channels

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.

Description
Table 1 contains the following columns:

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

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

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

The tables of the frequency bands have the following columns:

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

- **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.

Note

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

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

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

Note

This page has different columns in access point and in client mode.

---

![Basic Wizard: Security Settings](image)

Figure 6-1 Basic Wizard: Security settings - in client mode
Description

This 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**

**IEEE 802.11n devices**

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

- **Cipher**

  Select the encryption method.

  - **AUTO**
    AES or TKIP is used depending on the capability of the other station.

  - **TKIP (Temporal Key Integrity Protocol)**
    A symmetrical encryption method with the RC4 algorithm (Ron’s Code 4). In contrast to the weak WEP encryption, TKIP uses changing keys derived from a main key. TKIP can also recognize corrupted data frames.

  - **AES (Advanced Encryption Standard)**
    Strong symmetrical block encryption method based on the Rijndael algorithm that further improves the functions of TKIP.
• **WPA(2) Pass Phrase**

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

---

**Note**

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

---

• **WPA(2) Pass Phrase Confirmation**

Confirm the entered WPA(2) 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.

Description

Table 1 contains the following columns:

- **Security Context**
  Show 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.

<table>
<thead>
<tr>
<th>Server Role</th>
<th>Server IP Address</th>
<th>Server Port</th>
<th>Shared Secret</th>
<th>Shared Secret Conf</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td></td>
<td>1812</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 of the settings

Introduction

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

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

![Basic Wizard: Summary of Settings](image)

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
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.
6.4 "Information" menu

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

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

- Drop-down list for language selection

- System time and date

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

Display area (2)

In the 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.

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

- **Printer**
  If you click this button, a popup window opens. The popup window contains a view of the page content optimized for printers.

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

- **LED simulation**
  Each device has one or more LEDs that provide information on the operating state of the device. Depending on its location, direct access to the device may not always be possible. Web Based Management therefore displays simulated LEDs. 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.

- **Update on** / **Update 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.

Buttons you require often

The pages of the WBM contain the following standard buttons:

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

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

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

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

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

- **Delete entries with "Delete"**
  Pages in which you can delete entries have a "Delete" button at the lower edge. Click this button to delete the previously selected entries from the device memory. Deleting also results in an update of the page in the WBM.

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

- **Page 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.

**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.

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

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.

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Name</th>
<th>Revision</th>
<th>Order ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Device</td>
<td>SCALANCE W774-1 RJ45</td>
<td>1</td>
<td>69K5 774-1FXDD-AAA0</td>
</tr>
<tr>
<td>WLAN 1</td>
<td>WLAN 1 Radio Card</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Software</th>
<th>Description</th>
<th>Version</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firmware</td>
<td>SCALANCE W700 Firmware DEV-SIG</td>
<td>T06.00.00.00-00.01.01</td>
<td>02/09/2016 20:01:00</td>
</tr>
<tr>
<td>Bootloader</td>
<td>SCALANCE W700 Bootloader</td>
<td>V01.16.00</td>
<td>08/12/2014 09:15:00</td>
</tr>
<tr>
<td>Firmware_Running</td>
<td>Current running Firmware</td>
<td>T06.00.00.00-00.01.01</td>
<td>02/09/2016 20:01:00</td>
</tr>
</tbody>
</table>

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.

- **Order ID**
  Shows the order number of the device or module.
Table 2 has the following columns:

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

- **Description**
  Shows the short description of the software.

- **Version**
  Shows the version number of the software version.

- **Date**
  Shows the date on which the software version was created.
6.4.3 Identification & Maintenance

Identification and maintenance data

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

Description of the displayed values

The table has the following rows:

- **Manufacturer ID**
  Shows the manufacturer ID.

- **Order ID**
  Shows the order number.

- **Serial Number**
  Shows the serial number.

- **Hardware Revision**
  Shows the hardware version.

- **Software Revision**
  Shows the software version.

- **Revision Counter**
  As of firmware version 4.0, the value "0" is always shown here regardless of the version change.

- **Revision Date**
  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.
6.4.4 Address Resolution Protocol (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.

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.
6.4.5 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

<table>
<thead>
<tr>
<th>Event Log</th>
<th>WLAN Authentication Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity Filters</td>
<td></td>
</tr>
<tr>
<td>Info</td>
<td>Warning</td>
</tr>
<tr>
<td>Restart</td>
<td>System Up Time</td>
</tr>
<tr>
<td>5</td>
<td>00:00:24</td>
</tr>
<tr>
<td>5</td>
<td>00:00:00</td>
</tr>
<tr>
<td>5</td>
<td>00:00:00</td>
</tr>
<tr>
<td>5</td>
<td>00:00:00</td>
</tr>
<tr>
<td>5</td>
<td>00:00:00</td>
</tr>
<tr>
<td>5</td>
<td>00:00:00</td>
</tr>
<tr>
<td>4</td>
<td>00:00:24</td>
</tr>
<tr>
<td>4</td>
<td>00:00:00</td>
</tr>
<tr>
<td>4</td>
<td>00:00:00</td>
</tr>
<tr>
<td>4</td>
<td>00:00:00</td>
</tr>
</tbody>
</table>

1 - 10 of 221 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.
  - **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 of the configuration manual.

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

"Clear" button
Click this button to delete the content of the event log file. All entries are deleted regardless of what you have selected in "Severity Filters".

The display is also cleared. The restart counter is only reset after you have restored the device to the factory settings and restarted the device.

Note
The table can contain 400 entries for each severity. The number of entries in this table is restricted to 1200. When this number is reached, the oldest entries are discarded. The table remains permanently in memory.

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

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

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

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

"Update" button
Refreshes the display of the values in the table.
6.4.5.2 WLAN authentication log

Logging authentication attempts

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

<table>
<thead>
<tr>
<th>Restart</th>
<th>System Up Time</th>
<th>System Time</th>
<th>Severity</th>
<th>Log Message</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.
  - **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.
6.4 "Information" menu

- **System Time**
  Shows the date and time when the described event occurred.

- **Severity**
  Shows the severity of the message.

- **Log Message**
  Displays a brief description of the event that has occurred. You will find the list of possible messages in Appendix D of the configuration manual.

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

**Description of the button**

**"Clear" button**
Click this button to delete the content of the log file. All entries are deleted regardless of what you have selected under "Severity Filters".

The display is also cleared. The restart counter is only reset after you have restored the device to the factory settings and restarted the device.

**Note**
The table can contain 400 entries for each severity. The number of entries in this table is restricted to 1200. When this number is reached, the oldest entries are discarded. The table remains permanently in memory.

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

**"Next" button**
Click this button to go to the next page.

**"Prev" button**
Click this button to go to the previous page.

**Drop-down list for page change**
From the drop-down list, select the page you want to go to.

**"Update" button**
Refreshes the display of the values in the table.
6.4.6 Faults

Error status

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

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

<table>
<thead>
<tr>
<th>Fault Time</th>
<th>Fault Description</th>
<th>Clear Fault State</th>
</tr>
</thead>
<tbody>
<tr>
<td>18s</td>
<td>Link down on P1</td>
<td>Clear Fault State</td>
</tr>
<tr>
<td>17s</td>
<td>Warm start performed</td>
<td>Clear Fault State</td>
</tr>
</tbody>
</table>

Description

The page contains the following boxes:

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

- **"Reset Counters" button**
  The number is reset with this button.

The table contains the following columns:

- **Fault Time**
  Shows the time the device has been running since the last restart when the described fault occurred.

- **Fault Description**
  Displays a brief description of the error/fault that has occurred.

- **Clear Fault State**
  To delete errors of the "Cold/Warm Start" event, click the "Clear Fault State" button.
6.4.7 Spanning Tree

Introduction

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

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

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

The page contains the following boxes:

- **Spanning Tree Mode**
  Shows the set mode. You specify the mode in "Layer 2 > Configuration" and in "Layer 2 > MSTP > General".
  The following values are possible:
  - `-`
  - STP
  - RSTP
  - MSTP

- **Instance ID**
  Shows the number of the instance. The parameter depends on the configured mode.

- **Bridge Priority / Root Priority**
  Which device becomes the root bridge is decided based on the bridge priority. The bridge with the highest priority (in other words, with the lowest value for this parameter) becomes the root bridge. If several devices in a network have the same priority, the device whose MAC address has the lowest numeric value will become the root bridge. Both parameters, bridge priority and MAC address together form the bridge identifier. Since the root bridge manages all path changes, it should be located as centrally as possible due to the delay of the frames. The value for the bridge priority is a whole multiple of 4096 with a range of values from 0 to 32768.

- **Bridge 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.

- **Bridge Status**
  Shows the status of the bridge, e.g. whether or not the device is 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 device.

- **Regional Root Cost** (available only with MSTP)
  Shows the path costs from the regional root bridge to the root bridge.
The table contains the following boxes:

- **Port**
  Shows the port via which the device communicates.

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

- **State**
  Displays the current state of the port. The values are only displayed. The parameter depends on the configured protocol. The following statuses are possible:
  - **Discarding**
    The port receives BPDU frames. Other incoming or outgoing frames are discarded.
  - **Listening**
    The port receives and sends BPDU frames. The port is involved in the spanning tree algorithm. Other outgoing and incoming frames are discarded.
  - **Learning**
    The port actively learns the topology; in other words, the node addresses. Other outgoing and incoming frames are discarded.
  - **Forwarding**
    Following the reconfiguration time, the port is active in the network. The port receives and sends data frames.

- **Oper. Version**
  Describes the type of spanning tree in which the port operates

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

This parameter is used to calculate the path that will be selected. The path with the lowest value is selected as the route. If several ports of a device have the same value, the port with the lowest port number will be selected. If the value "Cost Calc." box is "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:

- 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 Statistiken

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](image)

**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.

**Description of the button**

* "Reset Counters" button
  
  Click "Reset Counters" to reset all counters. The counters are reset by a restart.
### 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](image)

#### Description

The table has the following columns:

- **Port**
  Shows the available ports.

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

#### Description of the button

"Reset Counters" button

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

Description

The table has the following columns:

- **Port**
  Shows the available ports.

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

Description of the button

"Reset Counters" button

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

Description

The table has the following columns:

- **Port**
  Shows the available ports.

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

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

- **CRC**
  Packets whose content does not match the CRC checksum.

- **Undersize**
  Packets with a length less than 64 bytes.

- **Oversize**
  Packets discarded because they were too long.

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

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

- **Collisions**
  Collisions that were detected.

Description of the button

"Reset Counters" button

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

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.

"Show all" button

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

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

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Pool ID</th>
<th>Identification Method</th>
<th>Identification Value</th>
<th>Remote ID</th>
<th>Circuit ID</th>
<th>Allocation Method</th>
<th>Binding State</th>
<th>Expiry Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.15.90</td>
<td>1</td>
<td>Client ID</td>
<td>00-EC74BA03FED2</td>
<td></td>
<td></td>
<td>dynamic</td>
<td>assigned</td>
<td>01/01/2000 05:21:03</td>
</tr>
</tbody>
</table>

Description

- **IP Address**
  Shows the IPv4 address assigned to the device.

- **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 of the client ID of the DHCP client.

- **Remote ID**
  Shows the remote ID of the DHCP client.

- **Circuit ID**
  Shows the circuit 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 how long the assigned IPv4 address is still valid. Once this period has elapsed, the device must either request a new IPv4 address or extend the lease time of the existing IPv4 address.

**Description of the buttons and input boxes**

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

**"Next" button**  
Click this button to go to the next page.

**"Prev" button**  
Click this button to go to the previous page.

**Drop-down list for page change**  
From the drop-down list, select the page you want to go to.

**"Refresh" button**  
Refreshes the display of the values in the table.
6.4.11 **Simple Network Management Protocol v3 (SNMPv3) group overview**

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

<table>
<thead>
<tr>
<th>Group Name</th>
<th>User Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>service</td>
<td>Miller</td>
</tr>
<tr>
<td>maintenance</td>
<td>Peterson</td>
</tr>
</tbody>
</table>

**Description**

The table has the following columns:

- **Group Name**
  - Shows the group name.

- **User Name**
  - Shows the user that is assigned to the group.
6.4.12 Security

6.4.12.1 Overview

Note
The values displayed depend on the rights of the logged-on user.

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

### Security Overview

<table>
<thead>
<tr>
<th>Overview</th>
<th>Supported Function Rights</th>
<th>Roles</th>
<th>Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telnet Server</td>
<td>enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSH Server</td>
<td>enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Server</td>
<td>HTTP/HTTPS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMPv1/V2c/V3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management ACL</td>
<td>disabled; no access restriction</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login Authentication</td>
<td>Local</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password Policy</td>
<td>high</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Local User Accounts

<table>
<thead>
<tr>
<th>User Account</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>admin</td>
</tr>
<tr>
<td>wcm</td>
<td>admin</td>
</tr>
</tbody>
</table>

#### External User Accounts

<table>
<thead>
<tr>
<th>User Account</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>admin</td>
</tr>
<tr>
<td>wcm</td>
<td>admin</td>
</tr>
</tbody>
</table>
Description

Services
The "Services" list shows the security settings.

- **Telnet Server**
  You configure the setting in "System > Configuration".
  - **Enabled**: Unencrypted access to the CLI.
  - **Disabled**: No unencrypted access to the CLI.

- **SSH Server**
  You configure the setting in "System > Configuration".
  - **Enabled**: Encrypted access to the CLI.
  - **Disabled**: No encrypted access to the CLI.

- **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 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".
  - **Enabled**: Restricted access only: Access is restricted using an Access Control List (ACL).
  - **Disabled**: No access restriction: Management ACL is not enabled.
  - **Enabled**: No access restriction: Management ACL is enabled, but access is not restricted using an Access Control List (ACL).
● **Login Authentication**

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

- Local
  The authentication must be made locally on the device.

- RADIUS
  The authentication must be handled via a RADIUS server.

- Local and RADIUS
  The authentication is possible both with the users that exist on the device (user name and password) and via a RADIUS server.

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

- RADIUS and fallback local
  The authentication must be handled via a RADIUS server.

  A local authentication is performed only when the RADIUS server cannot be reached in the network.

● **Password Policy**

Shows which password policy is currently being used.

**Local and external user accounts**

You configure local user accounts and roles in "Security > User Accounts"

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

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

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

**Note**

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

With CLI you can access external user accounts.
The table "Local User Accounts" has the following columns:

- **User Account**
  Shows the name of the local user.

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

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

- **User Account**
  Shows the name of the user on the RADIUS server.

- **Role**
  Shows the role assigned to the user on the device. You can obtain more information on this in "Information > Security > Roles".

### 6.4.12.2 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.

<table>
<thead>
<tr>
<th>Function Right</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Read-only access to configuration data.</td>
</tr>
<tr>
<td>15</td>
<td>Read/write access to configuration data.</td>
</tr>
</tbody>
</table>

**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.
6.4.12.3 Roles

**Note**

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

The page shows the roles valid locally on the device.

### Description of the displayed values

This 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.
6.4.12.4 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](image)

**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.

6.4.12.5 Inter AP Blocking

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

The WBM page shows a list of the SCALANCE W700 devices with which the clients are allowed to communicate.
Description

The table has the following columns:

- **Radio**
  Shows the available WLAN interfaces to which the settings relate.

- **Port**
  Shows the VAP interface to which the settings relate.

- **MAC Address**
  Shows the MAC address of the SCALANCE W700 device with which the client may communicate.

- **IP Address**
  Shows the IP address of the SCALANCE W700 device with which the client may communicate.

- **Resolver IP Address**
  Shows the IP address with which the permitted IP address is resolved.
6.4.13 WLAN

6.4.13.1 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.

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
</table>

Table 1 has the following columns:

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

- **WLAN Mode**
  Shows the transmission standard. If DFS is activated, the transmission standard "802.11h" is not shown additionally but only the configured transmission standard "802.11a".

- **Configured Channel**
  Shows the configured channel. If "Auto" is displayed, the access point searches for a free channel itself.

- **Alternative DFS Channel**
  If the DFS function is enabled, the configured alternative channel of the access point is displayed.
  If "Auto" is displayed, the access point searches for an alternative channel itself.
  If the DFS function is activated and the access point browses for primary users for 60 seconds before starting communication with the selected channel, the text "scanning ..." is displayed instead of the channel.

- **Operational channel**
  Shows the channel of the access point via which the access point communicates.
6.4 "Information" menu

- **HT Channel Width [MHz]**
  Shows the channel bandwidth.
  - 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.

- **iFeatures**
  Shows which iFeatures are used.
  - -
    iFeatures are not used.
  - iPCF
    iPCF is enabled

- **State**
  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.
6.4 “Information” menu

- **Security**
  Shows which authentication method is used.
  If the authentication method "Open System + Encryptionor "Shared Key" is used, the "Encrypted (WEP/AES)" authentication method is displayed for both.

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

6.4.13.2 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.

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
</table>
| **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 + Encryptionor "Shared Key" is used, the "Encrypted (WEP/AES)" authentication method is displayed for both.

• **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.
6.4.13.3 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.

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.
Configuring with Web Based Management

6.4 "Information" menu

- **Security**
  Shows which authentication method is used.
  If the authentication method "Open System + Encryptionor "Shared Key" is used, the "Encrypted (WEP/AES)" authentication method is displayed for both.

- **Max. Data Rate (Mbps)**
  Shows the maximum data transmission speed for the relevant WDS partner.

- **State**
  Shows the current status of the WDS connection.

### 6.4.13.4 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.

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

Table 1 has the following columns:

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

- **Aging Time [min]**
  Specify the lifetime 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 client in dBm.

- **Signal strength [%]**
  Shows the signal strength of the client as a percentage.

- **Age [s]**
  Shows the time that has elapsed since the last access point activity.
6.4 "Information" menu

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

- **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".

### 6.4.13.5 Force Roaming

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

**Note**

This WBM page is only available in access point mode.

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 VAP interfaces.

- **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.
  - active: Roaming is being performed. None of the destination addresses is reachable.
6.4.13.6 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.

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Radio</strong></td>
</tr>
<tr>
<td>Shows the available WLAN interfaces in this column.</td>
</tr>
<tr>
<td><strong>WLAN Mode</strong></td>
</tr>
<tr>
<td>Shows the transmission standard.</td>
</tr>
<tr>
<td><strong>MAC Mode</strong></td>
</tr>
<tr>
<td>Shows how the MAC address is assigned to the interface.</td>
</tr>
<tr>
<td>- <strong>Automatic</strong></td>
</tr>
<tr>
<td>The client automatically adopts the source MAC address of the first frame that it receives over the Ethernet interface.</td>
</tr>
<tr>
<td>- <strong>Manual</strong></td>
</tr>
<tr>
<td>The address was entered manually.</td>
</tr>
<tr>
<td>- <strong>Own</strong></td>
</tr>
<tr>
<td>The client uses the MAC address of the Ethernet interface for the WLAN interface.</td>
</tr>
<tr>
<td>- <strong>Layer 2 Tunnel</strong></td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td><strong>MAC Address</strong></td>
</tr>
<tr>
<td>Shows the MAC address of the WLAN interface.</td>
</tr>
<tr>
<td><strong>Operational channel</strong></td>
</tr>
<tr>
<td>Shows the channel of the access point with which the client is connected.</td>
</tr>
</tbody>
</table>
Configuring with Web Based Management

6.4 "Information" menu

- **HT Channel Width [MHz]**
  Shows the channel bandwidth.
  - 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.

- **Connected BSSID**
  Shows the MAC address of the access point with which the client is connected.

- **Connected SSID**
  Shows the SSID of the access point with which the client is connected.

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

- **iFeatures**
  Shows which iFeatures are used.
  - 
    iFeatures are not used.
  - iPCF
    iPCF is enabled.

- **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.
6.4.13.7 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.

<table>
<thead>
<tr>
<th>Radio</th>
<th>SSID</th>
<th>BSSID</th>
<th>System Name</th>
<th>Channel</th>
<th>Signal Strength [dBm]</th>
<th>Signal Strength [%]</th>
<th>Type</th>
<th>Security</th>
<th>WLAN Mode</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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 + Encryptionor "Shared Key" is used, the "Encrypted (WEP/AES)" authentication method is displayed for both.

• **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.

### 6.4.13.8 IP mapping table

**WLAN access for several SCALANCE W700 devices via 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 SCALANCE W700 devices with one client if you use IP mapping. This means that you do not need to equip every SCALANCE W700 device with its own WLAN client. This is possible only if the connected SCALANCE W700 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 SCALANCE W700 devices downstream from the client. Clients with this setting cannot connect on standard Wifi access points.
The client maintains a table with the assignment of MAC address and IP address to send incoming IP frames to the correct MAC address. This WBM page shows this table.

**Note**

**IP mapping table**

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

---

**Description**

The table has the following columns:

- **MAC Address**
  
The MAC address of a device located downstream from the WLAN client from the perspective of the access point.

- **IP Address**
  
The IP address managed for this device by the WLAN client.

- **Type**
  
  There are two options for the type:
  
  - system
    
    The information relates to the WLAN client itself.
  
  - learned
    
    The information relates to a device downstream from the WLAN client.

---

**MAC mode**

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

If there are further SCALANCE W700 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 SCALANCE W700 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 SCALANCE W700 devices downstream from the client, you need to select the settings "Automatic", "Manual" or "Layer 2 Tunnel".
6.4.14 WLAN Statistics

6.4.14.1 Faults

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 W700 devices and the connection quality.

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 of bad frames that were sent.
  
  - Dropped Frames
    Shows the number of frames that were discarded.

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

    The frame has not yet been sent and the recipient has logged off in the meantime.

  - Send Retries
    Shows the number of frames sent successfully that required one or more retries.
The Received Errors table has the following columns:

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

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

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

### 6.4.14.2 Management Sent

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

**Note**
This WBM page is only available in access point mode.
Description

The table has the following columns:

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

- **Frame**
  - Management Frames
    Shows the number of management frames
  - Association 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.

"Reset Counters" button
Click this button to reset the counters.
6.4.14.3 Management Received

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

**Note**

This WBM page is only available in access point mode.

---

**Description**

The table has the following columns:

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

- **Frame**
  - Management Frames
    Shows the number of management frames
  - Association 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 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.
"Reset Counters" button
Click this button to reset the counters.

6.4.14.4 Data Sent

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

<table>
<thead>
<tr>
<th>Interface</th>
<th>Data Frames</th>
<th>Multicast/Broadcast Frames</th>
<th>Unicast Frames</th>
<th>Average Data Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>VAP 1.1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>VAP 1.2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>VAP 1.3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>VAP 1.4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

Description

The table has the following columns:

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

- **Frame types**
  The other columns after the VAP interface contain the absolute numbers of the sent frames according to the frame types.
  In the columns of the table, a distinction is made according to the following frame types:
  - Data Frames
    Shows the number of sent data frames.
  - Multicast/Broadcast Frames
    Shows the number of sent multicast and broadcast frames.
  - Unicast Frames
    Shows the number of sent unicast frames.
  - Average Data Rate
    Shows the average data rate of the last data frames sent.

"Reset Counters" button
Click this button to reset the counters.
6.4.14.5 Data Received

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

![WLAN Data Traffic Received Statistics](image)

**Description**

The table has the following columns:

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

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

  In the columns of the table, a distinction is made according to the following frame types:
  - **Data Frames**
    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.

**"Reset Counters" button**

Click this button to reset the counters.
6.4.15  WLAN iFeatures

6.4.15.1  iREF Client List

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

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

Description

The page contains the following box:

- **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.

- **MAC Address**
  Shows the MAC address of the client.
6.4 "Information" menu

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

- **Tx Chain**
  Shows the antenna connector over which the client communicates with the access point.

- **Signal Strength [dBm]**
  Shows the signal strength of the connected client in decibel milliwatts.

- **Signal strength [%]**
  Shows the signal strength of the connected client as a percentage.

- **Age [s]**
  Shows the age of the listed client.

6.4.15.2 iREF WDS List

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

**Note**

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

The page contains the following box:

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

The table has the following columns:

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

- **Port**
  Shows the WDS interface.

- **BSSID**
  Shows the MAC address of the WDS partner.

- **WDS ID**
  Shows the name of the WDS partner.

- **Tx Chain**
  Shows the antenna connector over which the two access points communicate with each other.

- **Signal Strength [dBm]**
  Shows the signal strength of the connected access point in decibel milliwatts.

- **Signal strength [%]**
  Shows the signal strength of the connected access point as a percentage.
6.4.15.3 AeroScout

This page shows information on forwarding AeroScout frames.

**Note**

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

**Note**

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

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

- **Tag information forwarding**
  In the management program that evaluates the AeroScout frames, you can specify whether or not a SCALANCE W700 device will forward frames. Here, you can see which setting was made in the management program.

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

- **AeroScout status**
  Shows whether AeroScout is enabled or disabled.

- **Engine port**
  The SCALANCE W700 device expects UDP packets from the management program at port 1144.

- **Response IP**
  The IP address of the computer on which the management program for evaluation of the AeroScout frames is running.

- **Multicast address**
  The tag sends frames as multicast. This multicast address is configured in the management program and displayed here.

- **Sent confirmations**
  The number of confirmations sent by the SCALANCE W700 device to the management program as a result of cyclic queries or manual configuration changes in the management program (UDP packets).

- **Discarded messages**
  The number of frames not forwarded. If, for example, an AeroScout tag is configured so that it sends on channel 1, the SCALANCE W700 device does not forward a frame received on channel 6.
6.5 "System" menu

6.5.1 System Configuration

System configuration

The WBM page contains the configuration overview of the access options of the device. Specify the services that access the device. With some services, there are further configuration pages on which more detailed settings can be made.

Description of the displayed boxes

The page contains the following boxes:

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

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

- **HTTPS Server only**
  Enable or disable access using HTTPS.
- **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.

- **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".

- **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.
  - **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 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.
6.5 "System" menu

- **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.

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

---

**Procedure**

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

---

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.
Description

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

- **"Latitude" input box**
  Geographical latitude: Here, enter the value for the northerly or southerly latitude of the location of the device.
  For example, the value +49° 1´31.67" means that the device is located at 49 degrees, 1 arc minute and 31.67 arc seconds northerly latitude.
  A southerly latitude is shown by a preceding minus character.
  You can also append the letters N (northerly latitude) or S (southerly latitude) to the numeric information (49° 1´31.67" N).

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

- **Input box: "Height"**
  Height Here, you enter the value of the geographic height above sea level in meters.
  For example, 158 m means that the device is located at a height of 158 m above sea level.
  Heights below sea level (for example the Dead Sea) are indicated by a preceding minus sign.

Procedure

1. Enter the calculated latitude in the "Latitude" input box.
2. Enter the calculated longitude in the "Longitude" input box.
3. Enter the height above sea level in the "Height" input box.
4. Click the "Set Values" button.
### 6.5.3 Agent Internet Protocol (IP)

#### Configuration of the IP addresses

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

![Agent Internet Protocol (IP)](image)

#### Description

The page contains the following boxes:

- **IP Assign. Method**
  - Shows how the IP address is assigned.
    - Static
      - The IP address is static. You enter the IP settings in the input boxes "IP Address" and "Subnet Mask".
    - Dynamic (DHCP)
      - The device obtains a dynamic IP address from a DHCP server.

- **IP Address**
  Enter the IP address of the device. After clicking the "Set Values" button, this IP address is also displayed in the address bar of the Web browser. If this does not take place automatically, you will need to enter the IP address in the address bar of the Web browser manually.

- **Subnet Mask**
  Enter the subnet mask of the device.

- **Default gateway**
  Enter the IP address of the default gateway to be able to communicate with devices in another subnet, for example diagnostics stations, e-mail server.

- **Agent VLAN ID**
  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 "802.1Q VLAN Bridge". You configure the parameter in "Layer 2 > VLAN > General".
3. Click the "Set Values" button.

### 6.5.4 Domain Name System (DNS) client

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

**Note**

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

**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.
6.5.5 Restart

Resetting to the defaults

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

![Restart Screen](image)

**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, 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

• **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. Following this, the device can only be accessed using the Primary Setup Tool or using DHCP.

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

---

### 6.5.6 Commit Control

**Change management**

On this page, you specify when the WLAN settings become effective on the SCALANCE W700 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 W700 device before it is fully configured.
With the "Manual Commit" setting, you have the opportunity of first fully configuring the SCALANCE W700 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 W700 device via the WLAN interface, we recommend that you use the "Manual Commit" setting. Check the parameters again before you confirm the changes with the "Commit Changes" button.

---

**Commit Control**

**Commit Mode**

Select the required setting from the drop-down list.

- **Automatic Commit**
  
  Each change in the WLAN settings is adopted and is immediately effective when you click the "Set Values" button. With its default setting, the SCALANCE W700 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". In addition to this the message "Manual Commit Mode active - Press 'Commit Changes' button to provide current configuration to driver." appears as soon as there are WLAN changes. This message can be seen on every WBM page until the changes made have either taken effect or the SCALANCE W700 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.
6.5.7 Load & Save

Overview of the file types

Table 6-1 HTTP

<table>
<thead>
<tr>
<th>File type</th>
<th>Description</th>
<th>Download</th>
<th>Save</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config</td>
<td>Start configuration</td>
<td>X</td>
<td>X</td>
<td>--</td>
</tr>
<tr>
<td>ConfigPack</td>
<td>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 &quot;Maintenance&quot;.</td>
<td>X</td>
<td>X</td>
<td>--</td>
</tr>
<tr>
<td>CountryList</td>
<td>The zip file contains the country list as a csv and as a pdf.</td>
<td>--</td>
<td>X</td>
<td>--</td>
</tr>
<tr>
<td>Debug</td>
<td>This file contains information for Siemens Support.</td>
<td>--</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>EDS</td>
<td>Electronic Data Sheet (EDS) Electronic data sheets for describing devices in the EtherNet/IP mode</td>
<td>--</td>
<td>X</td>
<td>--</td>
</tr>
<tr>
<td>Firmware</td>
<td>Loading firmware updates</td>
<td>X</td>
<td>X</td>
<td>--</td>
</tr>
<tr>
<td>GSDML</td>
<td>Information on the device properties (PROFINET)</td>
<td>--</td>
<td>X</td>
<td>--</td>
</tr>
<tr>
<td>HTTPS Cert</td>
<td>HTTPS certificate</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>LogFile</td>
<td>File with entries from the event log table</td>
<td>--</td>
<td>X</td>
<td>--</td>
</tr>
<tr>
<td>MIB</td>
<td>Private MSPS MIB file &quot;Scalance_w_mspars.mib&quot;</td>
<td>--</td>
<td>X</td>
<td>--</td>
</tr>
<tr>
<td>RunningCLI</td>
<td>This file contains an overview of the current configuration in the form of CLI commands. You can download the text file. The file is not intended to be uploaded again unchanged.</td>
<td>--</td>
<td>X</td>
<td>--</td>
</tr>
<tr>
<td>Script</td>
<td>CLI script file</td>
<td>X</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>StartupInfo</td>
<td>Startup log file</td>
<td>--</td>
<td>X</td>
<td>--</td>
</tr>
<tr>
<td>Users</td>
<td>File with user names and passwords</td>
<td>X</td>
<td>X</td>
<td>--</td>
</tr>
<tr>
<td>WLANAuthlog</td>
<td>File with entries from the WLAN Authentication Log (information on successful or failed authentication attempts)</td>
<td>--</td>
<td>X</td>
<td>--</td>
</tr>
<tr>
<td>WLANCert</td>
<td>User certificate. You can specify a password for the user certificate on the WBM page &quot;Load&amp;Save &gt; Password&quot;. Maximum file size: 8 KB</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>WLANServCert</td>
<td>Server certificate. Maximum file size: 8 KB</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
6.5 "System" menu

<table>
<thead>
<tr>
<th>File type</th>
<th>Description</th>
<th>Download</th>
<th>Save</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>W LansigRec</td>
<td>The zip file contains the following:</td>
<td>--</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>(in client mode only)</td>
<td>• csv file with the measured values of the signal recorder</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• pdf file with the measured values and an additional graphic representation of the measured values.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>You will find information about the measured values and their graphic representation in the section &quot;Signal recorder (Page 269)&quot;.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>W Lanspectrum-Analyzer</td>
<td>The Zip file contains a csv file with the measured values of the spectrum analyzer.</td>
<td>--</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>(Only in access point mode)</td>
<td>You will find information about the measured values and their graphic representation in the section &quot;Spectrum Analyzer (Page 277)&quot;.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 6-2 TFTP

<table>
<thead>
<tr>
<th>File type</th>
<th>Description</th>
<th>Save</th>
<th>Download</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config</td>
<td>Start configuration</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>ConfigPack</td>
<td>Detailed configuration information. for example, start configuration, users, certificates, firmware of the device (if saved as well).</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>For more detailed information on creating and using the ConfigPack incl. firmware, refer to the section &quot;Maintenance&quot;.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CountryList</td>
<td>The zip file contains the country list as a csv and as a pdf file.</td>
<td>X</td>
<td>--</td>
</tr>
<tr>
<td>Debug</td>
<td>This file contains information for Siemens Support.</td>
<td>X</td>
<td>--</td>
</tr>
<tr>
<td>EDS</td>
<td>Electronic Data Sheet (EDS)</td>
<td>X</td>
<td>--</td>
</tr>
<tr>
<td></td>
<td>Electronic data sheets for describing devices in the EtherNet/IP mode</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firmware</td>
<td>Loading firmware updates</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>GSDML</td>
<td>Information on the device properties (PROFINET)</td>
<td>X</td>
<td>--</td>
</tr>
<tr>
<td>HTTPS Cert</td>
<td>HTTPS certificate</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Maximum file size: 8 KB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LogFile</td>
<td>File with entries from the event log table</td>
<td>X</td>
<td>--</td>
</tr>
<tr>
<td>MIB</td>
<td>Private MSPS MIB file &quot;Scalance_w_mps.mib&quot;</td>
<td>X</td>
<td>--</td>
</tr>
<tr>
<td>RunningCLI</td>
<td>This file contains an overview of the current configuration in the form of CLI commands. You can download the text file. The file is not intended to be uploaded again unchanged.</td>
<td>X</td>
<td>--</td>
</tr>
<tr>
<td>Script</td>
<td>CLI script file</td>
<td>--</td>
<td>X</td>
</tr>
<tr>
<td>StartupInfo</td>
<td>Startup log file</td>
<td>X</td>
<td>--</td>
</tr>
<tr>
<td>Users</td>
<td>File with user names and passwords</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
### File type | Description | Save | Download
--- | --- | --- | ---
WLANAuthlog | File with entries from the WLAN Authentication Log (information on successful or failed authentication attempts) | X | --
WLANCert (in client mode only) | User certificate. You can specify a password for the user certificate on the WBM page "Load&Save > Password". Maximum file size: 8 KB | X | X
WLANServerCert (in client mode only) | Server certificate Maximum file size: 8 KB | X | X
WLANSigRec (in client mode only) | The zip file contains the following:
- csv file with the measured values of the signal recorder
- pdf file with the measured values and an additional graphic representation of the measured values.
You will find information about the measured values and their graphic representation in the section "Signal recorder (Page 269)". | X | --
WLANSpectrum-Analyzer (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 277)". | X | --

### 6.5.7.1 HTTP

#### Loading and saving data via HTTP

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

**Note**

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.

Incompatibility with previous versions with PLUG inserted

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

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.
### Description

The table has the following columns:

- **File type**
  Shows the name of the file.

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

- **Load**
  With this button, you can load files on the device. The button can be enabled, if this function is supported by the file type.

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

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

#### Note

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

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Load</th>
<th>Save</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config</td>
<td>Startup Configuration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ConfigPack</td>
<td>Startup Config, Users and Certificates</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CountryList</td>
<td>WLAN Country List</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Debug</td>
<td>Debug Information for Siemens Support</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EDS</td>
<td>Ethernet/IP Device Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firmware</td>
<td>Firmware Update</td>
<td>Load</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GSDML</td>
<td>PROFINET Device Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTPSCert</td>
<td>HTTPS Certificate</td>
<td>Load</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LogFile</td>
<td>Event Log (ASCII)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MIB</td>
<td>SCALANCE W MIB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RunningCLI</td>
<td>'show running-config all' CLI settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Script</td>
<td>Script</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>StartupInfo</td>
<td>Startup Information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td>Users and Passwords</td>
<td>Load</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WLANAuthLog</td>
<td>Authentication Log (ASCII)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WLAN Spectrum Analyzer</td>
<td>Spectrum Analyzer</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

![Figure 6-3 Example of a device in client mode](image_url)
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 executed immediately, for example the CLI script file and new settings are applied without a restart.

Saving files using HTTP
1. Start the save function by clicking 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
Configuration data has a checksum. If you edit the files, you can no longer upload them to the device.
6.5.7.2 TFTP

Loading and saving data via a TFTP server

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

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.

Incompatibility with previous versions with PLUG inserted

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

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.
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:

- **File types**
  Shows the name of the file.

- **Description**
  Shows the short description of the file type.
• **Filename**
  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 in which you want to save the data or take the data from in the "File name" input box.
4. Select the action you want to execute from the "Actions" drop-down list.
5. Click the "Set Values" button to start the selected actions. Depending on the size of the file this may take some time.
6. After loading the configuration and the SSL certificate, restart the device. The changes only take effect a restart.

**Reusing configuration data**

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

Follow the steps below to reuse configuration data:

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

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

Password for certificates

With this menu item, you can enter a password for encrypted certificates. User, server or HTTPS certificates can exist as PKCS#12 certificates (.p12 and .pfx) and PEM certificates (.pem).

---

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.

---

Note

In Access Point mode, only the HTTPS certificate is available.

---

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Aktiviert</th>
<th>Password</th>
<th>Passwort bestätigen</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPSCert</td>
<td>HTTPS-Zertifikat</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Description

The table has the following columns:

- **Type**
  Shows the certificate.

- **Description**
  Shows a short description of the certificate.

- **Enabled**
  Specifies whether the certificate needs a password. If you enable the setting, specify the password in "Password".
6.5 "System" menu

- **Password**
  
Enter the password for the certificate.

**Note**

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

- **Password Confirmation**
  
Confirm the password.

- **State**
  
Shows whether the current settings for the file match the device.
  
  - **Valid**
    
    the "Enabled" check box is selected and the password matches the certificate.
  
  - **Invalid**
    
    the "Enabled" check box is selected but the password does not match the certificate or no certificate has been loaded yet.
  
  - **'.'**
    
    The password cannot be evaluated or is not yet being used. The "Enabled" check box is not selected.

**Procedure**

**Assigning the password**

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.
6.5.8 Events

6.5.8.1 Configuration

Selecting system events

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

**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 / Faults**
  Enable or disable the required type of notification for all events. If "No Change" is selected, the entries of the corresponding column in table 2 remain unchanged.

- **Copy to table**
  If you click the button, the setting is adopted for all events of table 2.
Table 2 has the following columns:

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

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

- **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
   - Error

2. Click the "Set Values" button.

6.5.8.2 Severity Filters

**Setting the Severity Filters**

On this page, set the threshold levels for sending system event notifications.
6.5 "System" menu

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

- **E-mail**
  Sending system event messages by e-mail

- **Log Table**
  Entry of system events in the log table

- **Syslog**
  Entry of system events in the Syslog file

- **WLAN Authentication Log**
  Entering system events in the WLAN authentication log

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

You can select from the following values:

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

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

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

**Procedure**

Follow the steps below to configure the required level:

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

**6.5.9 Client for Simple Mail Transfer Protocol (SMTP)**

**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.
Description

The page contains the following boxes:

- **SMTP Client**
  Enable or disable the SMTP client.

- **Sender Email Address**
  Enter the name of the sender to be included in the e-mail, for example the device name.
  This setting applies to all configured SMTP servers.

- **Send Test Mail**
  Send a test e-mail to check your configuration.

- **SMTP Port**
  Enter the port via which your SMTP server can be reached.
  Factory settings: 25
  This setting applies to all configured SMTP servers.

- **SMTP Server Address**
  Enter the IP address or the FQDN (Fully Qualified Domain Name) of the SMTP server.
  This table contains the following columns:

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

  - **SMTP Server Address**
    Shows the IP address or the FQDN (Fully Qualified Domain Name) of the SMTP server.

  - **Receiver Email Address**
    Enter the e-mail address to which the device sends an e-mail if a fault occurs.
### Procedure

1. Enable the "SMTP Client" option.
2. Enter the IP address of the SMTP server or the FQDN 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.

### 6.5.10 DHCP

#### 6.5.10.1 DHCP Client

**Setting of the DHCP mode**

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

The page contains the following boxes:

- "DHCP Client Configuration Request (Opt. 66, 67)"
  Enable 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)" option, 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 in this configuration file.
6.5.10.2 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.

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:

- **Enable 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.

- **Prior to offering, check the address with ICMP echo**
  
  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".

• **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.

### 6.5.10.3 DHCP Options

On this page you specify which DHCP options the DHCP server supports. The various DHCP options are defined in RFC 2132.
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.
6.5 “System” menu

- **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 TFTP server as an IPv4 address, e.g. 192.168.100.2 or the FQDN name.
  - All other DHCP options
    Enter the DHCP parameter in hexadecimal, e.g. the IPv4 address 192.168.100.2 corresponds to “C0A86402”.

### 6.5.10.4 Static Leases

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

![Static Leases Table](image)
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.
6.5.11 SNMPP

6.5.11.1 General

Configuration of SNMP

On this page, you make the basic settings for SNMP. Enable the check boxes according to the function you want to use. Note the information in the section "Technical basics (Page 41)".

![SNMP Configuration Page]

**Description**

The page contains the following boxes:

- **SNMP**
  Select the SNMP protocol from the drop-down list. The following settings are possible:
  - "-" (disabled)
    SNMP is disabled.
  - SNMPv1/v2c/v3
    SNMPv1/v2c/v3 is supported.
  - SNMPv3
    Only SNMPv3 is supported.

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

**Note**

**Community String**

For security reasons, do not use the standard values "public" or "private". Change the community strings following the initial installation.
• **SNMPv1/v2c Read Community String**
Enter the community string for read access of the SNMP protocol.

• **SNMPv1/v2c Read/Write Community String**
Enter the community string for read and write access of the SNMP protocol.

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

• **SNMPv1/v2c Trap Community String**
Enter the community string for sending SNMPv1/v2 messages.

• **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.

**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.
6.5.11.2 Traps

SNMP traps for alarm events

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

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

Description

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

The table has the following columns:

- **Select**
  Select the row you want to delete.

- **Trap Receiver Address**
  If necessary, change the IP addresses or the FQDN names of the stations.

- **Trap**
  Enable or disable the sending of traps. Stations that are entered but not selected do not receive SNMP traps.

Procedure

**Creating a trap entry**

1. In "Trap Receiver Address", enter the IP address or the FQDN name of the station to which the device sends traps.

2. Click the "Create" button to create a new trap entry.
3. Select the check box in the required row "Trap".
4. Click the "Set Values" button.

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

6.5.11.3 v3 Groups

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

Description
The page contains the following boxes:

- **Group Name**
  Enter the name of the group. The maximum length is 32 characters.

- **Security Level**
  Select the security level (authentication, encryption) valid for the selected group. In the security levels, the following options:
  - no Auth/no Priv
    No authentication enabled / no encryption enabled.
  - Auth/no Priv
    Authentication enabled / no encryption enabled.
  - Auth/Priv
    Authentication enabled / encryption enabled.
The table has the following columns:

- **Select**
  Select the row you want to delete.

- **Group Name**
  Shows the defined group names.

- **Security Level**
  Shows the configured security level.

- **Read**
  Enable or disable read access for the required group.

- **Write**
  Enable or disable 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 disappears again after restarting the device.
  - **Yes**
    The group is assigned to an SNMPV3 user.
  - **No**
    The group is not assigned to an SNMPV3 user.

---

**Procedure**

**Creating a new group**

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

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

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

6.5.11.4 v3 Users

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

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 6 characters, the maximum length is 32 characters.

- **Authentication Password Confirmation**
  Confirm the password by repeating the entry.

- **Privacy Password**
  Enter your encryption password. This password must have at least 6 characters, the maximum length is 32 characters.

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

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

Create a new user
1. Enter the name of the new user in the "User Name" input box.
2. Click the "Create" button. A new entry is generated in the table.
3. In "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.

---

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

---

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

If one method is activated, the previously activated method is automatically deactivated.
6.5.12.1 Manual Setting

Manual setting of the system time

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

The page contains the following boxes:

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

- **System Time**
  Enter the date and time in the format "MM/DD/YYYY HH:MM:SS".
  After a restart, the time of day begins at 01/01/2000 00:00:00.

- **Use PC Time**
  Click the button to use the time setting of the PC.

- **Last Synchronization Time**
  Shows when the last time-of-day synchronization took place. If no time-of-day synchronization was possible, the box displays "Date/time not set".
• **Last Synchronization Mechanism**
  Shows how the last time synchronization was performed.
  - Not set
    The time was not set.
  - Manual
    Manual time setting
  - SNTP
    Automatic time-of-day synchronization with SNTP
  - NTP
    Automatic time-of-day synchronization with NTP
  - SIMATIC
    Automatic time-of-day synchronization using the SIMATIC time frame

• **Daylight Saving Time (DST)**
  Shows whether the daylight saving time changeover is active.
  - active (offset +1 h)
    The system time was changed to daylight saving time; in other words an hour was added. You can see the current system time at the top right in the selection area of the WBM.
    The set time continues to be 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. Click in the "System Time" input box.
3. In the "System Time" input box, enter the date and time in the format "MM/DD/YYYY HH:MM:SS".
4. Click the "Set Values" button.
   The date and time are adopted and "Manual" is entered in "Last Synchronization Mechanism" box.
6.5.12.2 DST Overview

On this page, you can create new entries for the daylight saving time changeover.
The table provides an overview of the existing entries.

Settings

<table>
<thead>
<tr>
<th>DST No.</th>
<th>Name</th>
<th>Year</th>
<th>Start Date</th>
<th>End Date</th>
<th>Recurring Date</th>
<th>State</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CEST</td>
<td>2017</td>
<td>03/28 02:00</td>
<td>10/29 02:00</td>
<td>Last Sunday March 02, Last Sunday October 03</td>
<td>enabled</td>
<td>Recurring</td>
</tr>
<tr>
<td>2</td>
<td>DST 2017</td>
<td>2017</td>
<td>09/30 02:00</td>
<td>11/15 03:00</td>
<td>-</td>
<td>enabled</td>
<td>Date</td>
</tr>
</tbody>
</table>

- **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 name in the "Name" box.
5. If you have selected the type "Date", fill in the following boxes.
   - Year
   - Day (for start and end date)
   - Hour (for start and end date)
   - Month (for start and end date)
6. If you have selected the type "Rule", fill in the following boxes.
   - Hour (for start and end date)
   - Month (for start and end date)
   - Week (for start and end date)
   - Day (for start and end date)
7. Click the "Set Values" button.
Deleting an entry

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

6.5.12.3 DST Configuration

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

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

Settings

Note

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

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

- DST No.
  Select the type of the entry.

- Type
  Select how the daylight saving time changeover is made:
  - Date
    You can set a fixed date for the daylight saving time changeover.
    This setting is suitable for regions in which the daylight saving time changeover is not governed by rules.
  - Rule
    You can define a rule for the daylight saving time changeover.
    This setting is suitable for regions in which the daylight saving time always begins or ends on a certain weekday.

- Name
  Enter a name for the entry.
  The name can be a maximum of 16 characters long.
Settings with "Date" selected

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

- **Year**
  
Enter the year for the daylight saving time changeover.

- **Start Date**
  
Enter the following values for the start of daylight saving time:
  
  - **Day**
    
    Specify the day.
  
  - **Hour**
    
    Specify the hour.
  
  - **Month**
    
    Specify the month.
• **End Date**
  Enter the following values for the end of daylight saving time:
  – Day
    Specify the day.
  – Hour
    Specify the hour.
  – Month
    Specify the month.

*Settings with "Rule" selected*

![DST Configuration](image)

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 fourth 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 fourth or the last week of the month.
  - **Day**
    Specify the weekday.

### 6.5.12.4 SNTP Client

**Time-of-day synchronization in the network**

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

---

**Note**

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

The page contains the following boxes:

- **SNTP Client**
  Enable or disable automatic time-of-day synchronization using SNTP.

- **Current System Time**
  Shows the current date and current normal time received from the server. 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 normal time including the time zone continues to be displayed in the "Current 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:
  - **Poll**
    If you select this protocol type, the input boxes "SNTP Server Address", "SNTP Server Port" and "Poll Interval[s]" are displayed to allow further configuration. With this type of synchronization, the device is active and sends a time query to the SNTP server.
  - **Listen**
    With this type of synchronization, the device is passive and receives SNTP frames that deliver the time of day.

• **SNTP Server Address**
  Enter the IPV4 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

• **Poll Interval[s]**
  Here, enter the interval between two-time queries. In this box, you enter the query interval in seconds. Possible values are 16 to 16284 seconds.

**Procedure**

1. Click the "SNTP Client" check box to enable the automatic time setting.
2. In the "Time Zone" input box, enter the local time difference to world time (UTC). The input format is "+/-HH:MM" (for example +02:00 for CEST), because the SNTP server always sends the UTC time. This time is then recalculated and displayed as the local time based on the specified time zone. On the device itself, there is no changeover from the daylight saving to standard time. You also need to take this into account when completing the "Time Zone" input box.
3. Select one of the following options from the "SNTP Mode" drop-down list:
   - **Poll**
     For this mode, you need to configure the following:
     - time zone difference (step 2)
     - time server (step 4)
     - Port (step 5)
     - query interval (step 6)
     - complete the configuration with step 7.
   - **Listen**
     For this mode, you need to configure the following:
     - time difference to the time sent by the server (step 2)
     - complete the configuration with step 7.
4. In the "SNTP Server Address" input box, enter the IPv4 address or the FQDN of the SNTP server whose frames will be used to synchronize the time of day.
5. In the "SNTP Server Port" input box, enter the port via which the SNTP server is available. The port can only be modified if the IPv4 address or the FQDN name of the SNTP server is entered.

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

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

6.5.12.5 NTP Client

Automatic time-of-day setting with NTP

If you require time-of-day synchronization using NTP, you can make the relevant settings here.

Note

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

**Network Time Protocol (NTP) Client**

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 IE switch. 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 normal time including the time zone continues to be displayed in the "Current System Time" box.
  - **inactive (offset +0 h)**
    The current system time is not changed.

• **NTP Server Address**
  Enter the IPv4 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]**
  Here, enter the interval between two time queries. In this box, you enter the query interval in seconds. Possible values are 64 to 1024 seconds.
6.5 "System" menu

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
   - IPv4 address or FQDN of the NTP server
   - NTP server port
   - Query interval
3. Click the "Set Values" button.

6.5.12.6 SIMATIC Time Client

Time setting via SIMATIC time client

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

Description
The page contains the following boxes:

- **SIMATIC Time Client**
  Select this check box to enable the device as a SIMATIC time client.

- **Current System Time**
  Shows the current system time.
• **Last Synchronization Time**  
  Shows when the last time-of-day synchronization took place.

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

**Procedure**

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

Setting the automatic logout

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

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

Note
No automatic logout from the CLI

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

Automatic Logout

<table>
<thead>
<tr>
<th>Web Base Management (s): 900</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI (TELNET, SSH) (s): 300</td>
</tr>
</tbody>
</table>

Set Values

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.
6.5.14 System Logging (Syslog) Client

System event agent

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

Requirements for sending log entries:

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

Description

The page contains the following boxes:

- **Syslog Client**
  Enable or disable the Syslog function.

- **Syslog Server Address**
  Enter the IP address or the FQDN (Fully Qualified Domain 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 or the FQDN (Fully Qualified Domain Name) of the Syslog server.

- **Server Port**
  Enter the port of the Syslog server being used.
### Procedure

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

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

---

**Note**
The default setting of the server port is 514.

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

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

### 6.5.15 Fault Monitoring

#### 6.5.15.1 Power Supply

**Settings for monitoring the power supply**

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

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

---

**Note**
You will find the permitted operating voltage limits in the operating instructions of the device.
A fault causes the signaling contact to trigger and the fault LED on the device to light up and, depending on the configuration, can trigger a trap, an e-mail, or an entry in the event log table.

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

**Procedure**

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

**Monitoring of the redundant power supply by PROFINET**

With the following devices, you can also configure which power supply will be monitored by PROFINET:

- SCALANCE W788-x (RJ-45 variants)
- SCALANCE W748-1 RJ-45
- SCALANCE W774-1 (RJ-45 and M12 variant)
- SCALANCE W734-1 RJ-45
### Procedure

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

#### 6.5.15.2 Link Change

**Configuration of fault monitoring of status changes on connections**

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

If connection monitoring is enabled, an error is signaled
- when there should be a link on a port and this is missing.
- or when there should not be a link on a port and a link is detected.

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

6.5.16 PROFINET

Settings for PROFINET

This page shows the PROFINET AR status and the device name.
### 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 LLPD 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 RJ-45**
  - **SCALANCE W774-1 M12 EEC**
  - **SCALANCE W734-1 RJ-45**
SCALANCE W700 and STEP 7

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

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

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

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.

6.5.17 EtherNet/IP

 EtherNet/IP

On this page, you configure the mode of EtherNet/IP.
### 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 RJ-45
- SCALANCE W774-1 M12 EEC
- SCALANCE W734-1 RJ-45

### 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.
6.5.18 PLUG

6.5.18.1 Configuration

**NOTICE**

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

A PLUG may only be removed or inserted when the device is turned off. The device checks whether or not a PLUG is present at one second intervals. If it is detected that the PLUG was removed, there is a restart. If a valid KEY-PLUG was inserted in the device, the device changes to a defined error state following the restart. With SCALANCE W, the available wireless interfaces are deactivated in this case.

If the device was configured at some time with a PLUG, the device can no longer be used without this PLUG. To be able to use the device again, reset the device to the factory settings.

**Information about the configuration of the C-PLUG / KEY-PLUG**

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

**Note**

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

The action cannot be undone.

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

**Note**

Incompatibility with previous versions with PLUG inserted

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

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

The table has the following rows:

- **Status**
  Shows the status of the PLUG. The following are possible:
  - **ACCEPTED**
    There is a PLUG with a valid and suitable configuration in the device.
  - **NOT ACCEPTED**
    Invalid or incompatible configuration on the inserted PLUG.
  - **NOT PRESENT**
    There is no C-PLUG or KEY-PLUG inserted in the device.
  - **FACTORY**
    PLUG is inserted and does not contain a configuration. This status is also displayed when the PLUG was formatted during operation.
  - **MISSING**
    There is no PLUG inserted. Functions are configured on the device for which a license is required.

- **Device Group**
  Shows the SIMATIC NET product line that used the C-PLUG or KEY-PLUG previously.

- **Device Type**
  Shows the device type within the product line that used the C-PLUG or KEY-PLUG previously.

- **Configuration Revision**
  The version of the configuration structure. This information relates to the configuration options supported by the device and has nothing to do with the concrete hardware configuration. This revision information does not therefore change if you add or remove...
additional components (modules or extenders), it can, however, change if you update the firmware.

- **File System**
  Displays the type of file system on the PLUG.

```
<table>
<thead>
<tr>
<th>NOTICE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New file system UBI</strong></td>
</tr>
</tbody>
</table>
| As of SCALANCE W firmware version 2.0 and SCALANCE X500 firmware version 3.0, UBI is the standard file system for the C-PLUG or KEY-PLUG. If a C-PLUG with the previous file system IECP is detected in such a device, this C-PLUG will be formatted for the UBI file system and the data will be rewritten to the C-PLUG.

This change in the file system also occurs following a firmware update to V2.0 with SCALANCE W or to V3.0 with SCALANCE X500. A downgrade to the previous version of the firmware then presents a problem. The firmware can neither read nor write the C-PLUG or KEY-PLUG and it is not even possible to "Restore factory defaults". |
```

- **File System Size [bytes]**
  Shows the maximum storage capacity of the file system on the PLUG.

- **File System Usage**
  Displays the storage space in use in the file system of the PLUG.

- **Info String**
  Shows additional information about the device that used the PLUG previously, for example, order number, type designation, and the versions of the hardware and software. The displayed software version corresponds to the version in which the configuration was last changed. With the "NOT ACCEPTED" status, further information on the cause of the problem is displayed.

- **"Modify PLUG drop-down list**
  Select the setting from the drop-down list. You have the following options for changing the configuration on the C-PLUG or KEY-PLUG:
  - Write current configuration to PLUG
    This option is available only if the status of the PLUG is "NOT ACCEPTED" or FACTORY.
    The configuration in the internal flash memory of the device is copied to the PLUG.
  - Erase PLUG to factory default
    Deletes all data from the C-PLUG and triggers low-level formatting.

**Procedure**

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

**NOTICE**

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

A PLUG may only be removed or inserted when the device is turned off. The device checks whether or not a PLUG is present at one second intervals. If it is detected that the PLUG was removed, there is a restart. If a valid KEY-PLUG was inserted in the device, the device changes to a defined error state following the restart. With SCALANCE W, the available wireless interfaces are deactivated in this case.

If the device was configured at some time with a PLUG, the device can no longer be used without this PLUG. To be able to use the device again, reset the device to the factory settings.

**Note**

Incompatibility with previous versions with PLUG inserted

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

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

**Information about the license of the KEY-PLUG**

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

This page provides detailed information about the license on the KEY-PLUG. In this example, the KEY-PLUG contains the data for enabling the layer 3 functions of the device.
**Description**

- **Status**
  Shows the status of the KEY-PLUG. The following are possible:
  - **ACCEPTED**
    The KEY-PLUG in the device contains a suitable and valid license.
  - **NOT ACCEPTED**
    The license of the inserted KEY-PLUG is not valid.
  - **NOT PRESENT**
    No KEY-PLUG is inserted in the device.
  - **MISSING**
    There is no KEY-PLUG or a C-PLUG with the status "FACTORY" inserted in the device. Functions are configured on the device for which a license is required.
  - **WRONG**
    The inserted KEY-PLUG is not suitable for the device.
  - **UNKNOWN**
    Unknown content of the KEY-PLUG.
  - **DEFECTIVE**
    The content of the KEY-PLUG contains errors.

- **Order ID**
  Shows the order number of the KEY-PLUG. The KEY-PLUG is available for various functional enhancements and for various target systems.

- **Serial Number**
  Shows the serial number of the KEY-PLUG.

- **Info String**
  Shows additional information about the device that used the KEY-PLUG previously, for example, order number, type designation, and the versions of the hardware and software. The displayed software version corresponds to the version in which the configuration was last changed. With the "NOT ACCEPTED" status, further information on the cause of the problem is displayed.

---

**Note**

When you save the configuration, the information about whether or not a KEY-PLUG was inserted in the device at the time is also saved. This configuration can then only work if a KEY-PLUG with the same order number / license is inserted. This applies regardless of whether or not iFeatures are configured.
6.5.19 Ping

Reachability of an address in an IPv4 network

With the ping function, you can check whether a certain IPv4 address is reachable in the network.

![Ping Interface](image)

Description

The table has the following columns:

- **Dest. address**
  Enter the IPv4 address or the FQDN (Fully Qualified Domain Name) of the device.

- **Repeat**
  Enter the number of ping requests.

- **Ping**
  Click this button to start the ping function.

- **Ping Output**
  This box shows the output of the ping function.

- **Clear**
  Click this button to empty the "Ping Output" box.
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.

<table>
<thead>
<tr>
<th>Port</th>
<th>Port Name</th>
<th>Status</th>
<th>OperState</th>
<th>Link</th>
<th>Mode</th>
<th>MTU</th>
<th>Negotiation</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td></td>
<td>enabled</td>
<td>up</td>
<td>up</td>
<td>100M FD</td>
<td>1500</td>
<td>enabled</td>
<td>00-1b-1b-a5-5d-5d</td>
</tr>
</tbody>
</table>

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.

• **Current Transmission Parameters**  
  Shows the transfer parameters of the port.

• **MTU (Maximum Transmission Unit)**  
  Shows the packet size.

• **Negotiation**  
  Shows whether the automatic configuration is enabled or disabled.

• **MAC Address**  
  Shows the MAC address of the port.
6.6.1.2 Configuration

Configuring ports

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

---

**Note**

The two Ethernet ports of a SCALANCE W770/W730 cannot be assigned parameters or diagnosed individually.

---

**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 W770/W730 devices. The value is preset to "Autonegotiation" for both ports.

• **Mode**
  Shows the transmission speed and the transmission method of the port.

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

• **MTU (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.

**Changing the port configuration**

Click the appropriate box to change the configuration.

**Note**

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

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

Follow the steps below to change the settings:

1. Change the settings according to your configuration.
2. Click the "Set Values" button.

6.6.2  WLAN

6.6.2.1  Basic

Basic settings

On this page, you make several basic settings for the SCALANCE W700 device, for example the country setting and mode.

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.
6.6 "Interfaces" menu

- **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.

- **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 W786-2IA RJ-45 for different frequency bands
If both WLAN interfaces are configured for the same frequency band on this device, there may be mutual influence or interference. This applies in particular when there is a high data throughput.
• **WLAN Mode 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**
    if you have enabled this function, additional DFS channels from the 5 GHz band are available to you. These channels are country-specific and are subject to certain DFS regulations.
    
    If the access point discovers a disturbance on the current channel, it changes automatically to an alternative channel and the current channel is blocked for 30 minutes. The disturbance can originate from a primary user or radar interference.
    
    Before the access point starts the communication on a 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 a channel.
    
    The access point also searches for primary users during operation.
  
  - **Disabled**
    The DFS function is not used.
• 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 enabled the outdoor mode, you only have the channels available that are permitted for outdoor operation.

• 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.

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

1. To configure the WLAN interface, you must always specify the country first. Select the country in which the SCALANCE W700 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**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN 1</td>
<td>100</td>
<td>1</td>
<td>2346</td>
<td>2346</td>
<td>16</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WLAN 2</td>
<td>100</td>
<td>1</td>
<td>2346</td>
<td>2346</td>
<td>16</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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.
6.6 "Interfaces" menu

- **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 their 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 checkmark of the required functions.
3. Click the "Set Values" button.
6.6.2.3 Antennas

Overview

Overview of IWLAN antennas:

<table>
<thead>
<tr>
<th>Antennas only for SCALANCE W700 acc. to IEEE 802.11n</th>
<th>Antennas for SCALANCE W700 acc. to IEEE 802.11n and IEEE 802.11a/b/g</th>
<th>Antennas only for SCALANCE W700 acc. to IEEE 802.11a/b/g</th>
</tr>
</thead>
<tbody>
<tr>
<td>with 1 connector</td>
<td>with 2 connectors (dual)</td>
<td>with 3 connectors (MIMO)</td>
</tr>
<tr>
<td>ANT795-4MA</td>
<td>ANT793-6DG</td>
<td>ANT795-6MT</td>
</tr>
<tr>
<td>ANT795-4MC</td>
<td>ANT793-8DJ</td>
<td>ANT793-6DT</td>
</tr>
<tr>
<td>ANT795-4MD</td>
<td>ANT793-8DK</td>
<td></td>
</tr>
<tr>
<td>ANT795-6DC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ANT793-8DP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The antenna name provides information about the properties of the antennas listed in the IWLAN antenna overview:

- **Frequency**
  - 2: 2.4 GHz
  - 3: 5 GHz
  - 5: 2.4 + 5 GHz

- **Gain**
  - 4: medium gain
  - 6: high gain
  - 8: very high gain

- **Directivity**
  - 2: directional antenna
  - 6: omnidirectional antenna (omnidirectional)
Antennas

Configuration of external antennas

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

**Note**

50 Ω terminating resistor

Each WLAN interface has up to 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.

Description of the displayed boxes

The table has 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 external antenna is not available, select the entry "User defined". If you terminate an antenna connection using a 50 Ω terminating resistor, select the entry "Not used (Connect 50 Ohm Termination)".

- **Antenna Gain**
  If you select the "User defined" entry for the "Antenna Type", enter the antenna gain manually in the "dBi" unit.

  - **Antenna Gain 2.4 GHz [dBi]**
    Here, enter the antenna gain the antenna has in the 2.4 GHz frequency band.

  - **Antenna Gain 5 GHz [dBi]**
    Here, enter the antenna gain the antenna has in the 5 GHz frequency band.
6.6 "Interfaces" menu

- **Cable Length [m]**
  Enter the length of the flexible antenna connecting cable in meters between the device and the external antenna.

- **Additional Attenuation [dB]**
  Here, specify the additional attenuation caused, for example, by an additional splitter.

- **Antenna Mode**
  Specify the use of the antenna. For antenna connector 1 (R1 A1 and R2 A1), the entry cannot be changed.
  - **Tx**
    For sending only
  - **Rx**
    For receiving only
  - **Rx\Tx**
    For receiving and sending

  The following table shows which combinations are possible:

<table>
<thead>
<tr>
<th>R1 A1</th>
<th>R1 A2</th>
<th>R2 A1</th>
<th>R2 A2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx\Tx</td>
<td>Rx\Tx</td>
<td>-- 1)</td>
<td>-- 1)</td>
</tr>
</tbody>
</table>

  1) Antenna type "50 Ohms Termination Impedance"

**Steps in configuration**

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

1. For the first antenna connector (R1 A1) in the "Antenna Type" drop-down list, select the type of antenna.
2. In the "Cable Length" input box, enter the length of the connecting cable you are using in meters. For antenna connector 1 (R1 A1 and R2 A1), the "Antenna Mode" cannot be changed.
3. For further antenna connectors (e.g. R1 A2), select the type of antenna from the "Antenna Type" drop-down list.
4. In the "Cable Length" input box, enter the length of the connecting cable you are using in meters.
5. Select the use of the antenna from the "Antenna Mode" drop-down list.
6. Repeat steps 3 to 5 for further antenna connectors.
7. 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.

### 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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN 1</td>
<td>✔</td>
<td>32</td>
<td>50000</td>
<td>✔</td>
<td>100</td>
<td>800 (long)</td>
</tr>
<tr>
<td>WLAN 2</td>
<td>✔</td>
<td>32</td>
<td>50000</td>
<td>✔</td>
<td>100</td>
<td>800 (long)</td>
</tr>
</tbody>
</table>

**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 option "A-MSDU".
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 option "A-MSDU".
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.

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1 has the following columns:</td>
</tr>
<tr>
<td>• <strong>Radio</strong> Shows the available WLAN interfaces in this column.</td>
</tr>
<tr>
<td>• <strong>Channel</strong> Specify the main channel.</td>
</tr>
<tr>
<td>If you want the access point to search for a free channel itself, use &quot;Auto&quot;. The selection of channels used by an access point when establishing a wireless cell can be restricted. To do this, select the &quot;Use Allowed Channels only&quot; check box on the &quot;Allowed Channels&quot;</td>
</tr>
</tbody>
</table>
If you want to use a fixed channel, select the required channel from the drop-down list.

**Note**

**Channel spacing with WLAN interfaces**

If you use a second WLAN interface, make sure that you have adequate channel spacing.

- **Alternative 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.

- **HT 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
  - 40 up
    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.

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.
• **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 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 certain end devices may have problems with access to a hidden SSID.

• **WDS only**
  If you enable this option, the access point only supports communication via WDS. In WDS mode, all access points must use the same channel.

• **WDS ID**
  Enter the WDS ID. The WDS ID can be a maximum of 32 characters long.
  To establish a WDS connection, enter this WDS ID on the WDS Partner.
  ASCII code 0x20 to 0x7e is used for the WDS ID.

**Procedure**
1. Select the required channel from the "Channel" drop-down list.
2. Enter network name in the "SSID" input box for the corresponding WLAN interface and port.
3. 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.

<table>
<thead>
<tr>
<th>Wireless Distribution System Settings</th>
</tr>
</thead>
</table>

**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. Use this option if you want to replace the access point later using the C-PLUG or KEY-PLUG.

• **Partner MAC**
  Enter the MAC address of the WDS partner.

• **Partner WDS ID**
  Enter the WDS ID of the WDS partner.
  For the WDS ID 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 SCALANCE W700 devices involved. If settings are incorrect or not compatible on the individual SCALANCE W700 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 "Partner MAC" 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 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.
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 rate settings**
  Shows that the setting is valid for all entries in Table 3.

- **Enabled / Basic**
  In the drop-down list, select the setting for all entries. If "No Change" is selected, the entry in table 3 remains unchanged.

- **Copy to table**
  If you click the button, the setting is adopted for all entries of table 3.

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

- **Radio**
  Specifies the WLAN interface to which the information relates.

- **Data Rate [Mbps]**
  Shows the supported data transmission speeds in megabits per second.

- **Enabled**
  Enable the option to assign the required data transmission speed to the WLAN interface.

**Note**
You need to enable at least one data transmission speed.

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

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

"Default Values" button
The "Default Values" button sets the selection of the values in compliance with the standard.
Procedure

To configure a certain data transmission speed on WLAN 1:
1. 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
This WBM page is only available in access point mode.
The WBM page can only be configured if "802.11n only" 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.
Description

Table 1 has the following columns:

- **Radio**
  Specifies the WLAN interface to which the information relates.

- **"Use selected data rates only"**.
  If you enable 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 of Table 3.

- **Enabled**
  In the drop-down list, select the setting for all entries. If "No Change" is selected, the entry in table 3 remains unchanged.

- **Copy to table**
  If you click the button, the setting is adopted for all entries of Table 3.

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

- **Radio**
  Specifies the WLAN interface to which the information relates.

- **MCS Index**
  Shows the supported MCS indexes. The displayed MCS indexes depend on the settings "Antenna Type" and "Antenna Mode". You will find the settings in "Interfaces > WLAN > Antennas". If, for example, you only use one antenna, only the MCS 0 to 7 are displayed.

- **Streams**
  Shows the maximum possible number of parallel data streams that can be transmitted with the selected MCS index.

- **Data Rate [Mbps]**
  Shows the supported data transmission speeds in megabits per second. The displayed data transmission speeds depend on the settings "Guard Interval" and "HT Channel Width". 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.
"Default Values" button
The "Default Values" button sets the selection of values to conform with the standard.

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 SCALANCE W700 device connects to a network as client.

**Note**
This WBM page is only available in client mode.

### Description

Table 1 has the following columns:

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

###configuring with web based management

6.6 "interfaces" menu

SCALANCE W770/W730 to IEEE 802.11n Web Based Management

Configuration Manual, 06/2016, C79000-G8976-C323-06
• 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 W700 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.

• Roaming Threshold
  Specify the threshold after which the client roams to the new access point.
  – High
    Changes only at a significantly higher field strength to the AP with the stronger signal.
  – Medium
    Changes at a moderately higher field strength to the AP with the stronger signal.
  – Low
    Changes at a slightly higher field strength to the AP with the stronger signal.
• **Background Scan Mode**

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

   The following options are available:
   - **always**
     The client scans continuously for access points.
   - **idle**
     If there is no data traffic for a certain time, a scan is started for further access points.
   - **disabled**
     As long as the client is connected, there is no scan for further access points.

• **Background Scan Interval [ms]**

   Specify the interval at which further access points are scanned.

Table 2 has the following columns:

• **Radio**

   Shows the WLAN interface.

• **Scan Channels**

   Shows the channels on which the client searches for an access point. The display depends on the wireless approvals of the selected country and the settings for "Allowed Channels".

Table 3 has the following columns:

• **Enabled**

   Enables or disables the relevant SSID.

• **Radio**

   Shows the WLAN interface.

• **SSID**

   Enter the SSID of the access point with which the client will connect. For the SSID, ASCII code 0x20 to 0x7e is used.

• **Security**

   Select a security context. You create and configure a security context in "Security > WLAN > Basic".

   Default setting: Context 1

---

**Note**

iPCF or iPCF-MC mode activated

If the iPCF 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**

**Note**

The WBM page is only available in access point mode.

If the interface is no longer available (cable break, network component faild, connector removed), a client connected over the wireless network is not aware of this. The access point can force the logged-on clients to roam by deactivating the relevant interface.

On this page you specify when roaming is performed.

- **On connection abort**
  
  If the wired Ethernet interface is no longer available the WLAN interface is turned off. The clients roam and then connect to a different access point. As soon as the first access point reaches the server again it switches its WLAN interfaces active again.

- **When the destination address is unreachable.**
  
  Roaming depends on destination addresses. To monitor the device sends pings to the configured destination addresses at regular intervals.
  
  - VAP interface monitored using a destination address
    
    If no ping response is received from this destination address, the access point turns the relevant VAP interface off.
  
  - VAP interface monitored using several destination addresses
    
    Only when no ping response is received from any of these destination addresses does the access point turn the relevant VAP interface off. As long as at least one destination address is reachable, the VAP interface remains active.

The access point sends a disassociation frame to the WAN 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.
Description

Table 1 has the following columns:

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

- **Force roaming on link down**
  When enabled if there is a connection abort via the Ethernet interface, the WLAN interface is turned off.

The table "Force Roaming on IP down" has the following columns:

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

- **Dest. IP**
  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.

- **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**
  Specify which VAP 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 which destination address the VAP interface will be monitored with.
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 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 is displayed in real time according to the color scheme. The gray line shows the background noise.

- **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 milliseconds.

• Measurement data
  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 previous 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.

Under the graphic the following values are displayed:

• Current Sample
  The number of the current measurement

• BSSID
  The BSSID (Basic Service Set Identification)

• AP System Name
  The system name of the access point

• Operative Channel
  The current channel or the channel on which the client is connected to the access point

• TX Rate [Mbps]
  The average data rate of the sent data packets during the current random test

• RX Rate [Mbps]
  The average data rate of the received data packets during the current random test

• Signal [dBm]
  The effective user data signal in dBm

• Signal [%]
  The effective user data signal in %

• RSSI
  The raw value of the RSSI (Received Signal Strength Indication)

• Noise Floor [dBm]
  The background noise in dBm

• Roaming Counter
  The roaming counter shows how often the client has changed the access point. After
  99999 changes the counter is reset.
This table contains the following columns:

- **Radio**
  Shows the WLAN interface to which the information applies. Since a client has a WLAN interface, there is only ever one row for "WLAN 1" in this table.

- **Interval [ms]**
  Specify the time interval between acquiring two measured values in milliseconds.

- **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.

- **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 measured values 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. Enter the number of random tests.
3. Reduce the number of random tests displayed.
4. Click the "Start" button.
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
   - A CSV file

Measurement results

PDF file

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

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.

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. The footer row 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.
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

- **Recorded Samples**
  The total number of measured values

- **Recording Interval**
  The interval between acquisition of two measured values
6.6 "Interfaces" menu

- Max. TX Rate
  The maximum data rate
- Rx Antenna x type
  The setting of the external antennas
- Max. TX Power
  The maximum possible transmit power

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
- BSSID
  The BSSID (Basic Service Set Identification) of the access point
- Sig%
  The effective user data signal in %
- dBm
  The effective user data signal in dBm
- NF
  The background noise in dBm
- RSSI
  The raw value of the RSSI (Received Signal Strength Indication)
- Roam
  The roaming counter shows how often the client has changed the access point. After 99999 changes the counter is reset.
- 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
  The channel on which the client is currently scanning
- RX-Rate
  The average data rate of the received data packets
- TX-Rate
  The average data rate of the sent data packets
Configuring with Web Based Management

6.6 "Interfaces" menu

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**
  System name of the access point

![Figure 6-6 Example of a generated CSV file](image-url)
6.6.2.13 Spectrum Analyzer

Technical information

The frequency range depends on the configuration.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amplitude accuracy</td>
<td></td>
</tr>
<tr>
<td>In 2.4 GHz</td>
<td>3 dBm</td>
</tr>
<tr>
<td>In 5 GHz</td>
<td>7 dBm</td>
</tr>
<tr>
<td>Resolution bandwidth</td>
<td>330 KHz</td>
</tr>
<tr>
<td>Min. signal strength</td>
<td>-100 dBm</td>
</tr>
<tr>
<td>Max. signal strength</td>
<td>0 dBm</td>
</tr>
<tr>
<td>Analysis time</td>
<td></td>
</tr>
<tr>
<td>At 40 MHz</td>
<td>120 ms</td>
</tr>
<tr>
<td>At 20 MHz</td>
<td>95 ms</td>
</tr>
<tr>
<td>Update time</td>
<td>1 s.</td>
</tr>
</tbody>
</table>

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.
Configuring with Web Based Management

6.6 "Interfaces" menu

When Spectrum Analyzer is running, no wireless communication is possible.

<table>
<thead>
<tr>
<th>Radio</th>
<th>Status</th>
<th>Frequency Band</th>
<th>Center Frequency</th>
<th>Start</th>
<th>Stop</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN 1</td>
<td>started</td>
<td>2.4 GHz</td>
<td>2452-2472 (Ch. 7-13)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WLAN 2</td>
<td>stopped</td>
<td>5 GHz</td>
<td>Not Selected</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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**

![Realtime Graph](image)

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.
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.
  - running
    The measurement is running.

- **Frequency Band**
  Specify the frequency band.

- **Center Frequency**
  Select the center frequency.

- **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.
6.7 "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

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

<table>
<thead>
<tr>
<th>Select</th>
<th>VLAN ID</th>
<th>Name</th>
<th>Status</th>
<th>P1</th>
<th>VAP 1.1</th>
<th>VAP 1.2</th>
<th>VAP 1.3</th>
<th>VAP 1.4</th>
<th>VAP 1.5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>Static</td>
<td>U</td>
<td>U</td>
<td>U</td>
<td>U</td>
<td>U</td>
<td>U</td>
<td>U</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Static</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Static</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

3 entries.
Description

The page contains the following boxes:

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

**Note**

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

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

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

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

The table has the following columns:

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

- **VLAN ID**
  Shows the VLAN ID. The VLAN ID (a number between 1 and 4094) can only be assigned once when creating a new data record and can then no longer be changed. To make a change, the entire data record must be deleted and created again. Up to 8 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".

### 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).

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".

<table>
<thead>
<tr>
<th>Port Based Virtual Local Area Network (VLAN) Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
</tr>
<tr>
<td>Priority</td>
</tr>
<tr>
<td>All ports</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Priority</th>
<th>Port VID</th>
<th>Acceptable Frames</th>
<th>Ingress Filtering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pt1</td>
<td>0</td>
<td>VLAN1</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>VAP 1.1</td>
<td>0</td>
<td>VLAN1</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>VAP 1.2</td>
<td>0</td>
<td>VLAN1</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>VAP 1.3</td>
<td>0</td>
<td>VLAN1</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>VAP 1.4</td>
<td>0</td>
<td>VLAN1</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>VAP 1.5</td>
<td>0</td>
<td>VLAN1</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>VAP 1.6</td>
<td>0</td>
<td>VLAN1</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>VAP 1.7</td>
<td>0</td>
<td>VLAN1</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>VAP 1.8</td>
<td>0</td>
<td>VLAN1</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>VAP 2.1</td>
<td>0</td>
<td>VLAN1</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>VAP 2.2</td>
<td>0</td>
<td>VLAN1</td>
<td>All</td>
<td></td>
</tr>
</tbody>
</table>

**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.

- **Ingress Filtering**
  Specify whether the VID of received frames is evaluated.
  You have the following options:
  - Enabled
    The VLAN ID of received frames decides whether they are forwarded: To forward a VLAN tagged frame, the receiving port must be a member in the same VLAN. Frames from unknown VLANs are discarded at the receiving port.
  - Disabled
    All frames are forwarded.

**Procedure**

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

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.

Description

The page contains the following boxes:

- **Spanning Tree**
  
  Enable or disable MSTP.
• **Protocol Compatibility**

  Select the compatibility mode of MSTP. For example if you select RSTP, MSTP behaves like RSTP.

  The following settings are available:
  - STP
  - RSTP
  - MSTP

  **Note**

  If iPCF mode is enabled, only the compatibility modes STP and RSTP are supported.

**Procedure**

1. Select the "MSTP" check box.
2. 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 an device.
- The right-hand side shows the configuration of the regional root bridge that can be derived from the MSTP frames received by an device. The displayed data is only visible if you have enabled “Spanning Tree” on the "General" page and when “Protocol Compatibility” is set to “MSTP”. This also applies to the "Bridge Max Hop Count" parameter. If the device is a root bridge, the information on the left and right matches.

![Common Internal Spanning Tree (CIST) General](image)

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.
Configuring with Web Based Management

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 device.

- **Regional Root Cost**
  Shows the path costs from this device to the 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.
6.7 "Layer 2" menu

- **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.
Description

Table 1 has the following columns:

- **Column 1**
  Shows that the settings are valid for all ports of table 2.

- **Spanning Tree Status**
  In the drop-down list, select the setting for all ports. If "No Change" is selected, the entries of the corresponding column in table 2 remain unchanged.

- **Copy to table**
  If you click the button, the settings are adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
  Shows the available ports and interfaces.
  - Port X
  - WLAN X
  - VAP X.Y
  - WDS X.Y

- **Spanning Tree Status**
  Specify whether the port is integrated in the spanning tree or not.

**Note**

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

- **Priority**
  Enter the priority of the port. The priority is only evaluated when the path costs are the same.
  The value must be divisible by 16. If the value that cannot be divided by 16, the value is automatically adapted.
  Range of values: 0 - 240.
  The default is 128.

- **Cost Calc.**
  Enter the path cost calculation. If you enter the value "0" here, the automatically calculated value is displayed in the "Path Cost" box.
• **Path Cost**

The path costs from this port to the root bridge. The path with the lowest value is selected as the path. If several ports of a device have the same value, the port with the lowest port number will be selected.

If the "Cost Calc." box has the value "0", the automatically calculated value is shown. Otherwise, the value of the "Cost Calc." box is displayed.

The calculation of the path costs is largely based on the transmission speed. The higher the achievable transmission speed is, the lower the value of the path costs.

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

The values can, however, also be set individually.

• **State**

Displays the current state of the port. The values are only displayed and cannot be configured. The "State" parameter depends on the configured protocol. The following is possible for status:
- **Disabled**
  The port only receives and is not involved in STP, MSTP and RSTP.
- **Discarding**
  In the "Discarding" mode, BPDU frames are received. Other incoming or outgoing frames are discarded.
- **Listening**
  In this status, BPDUs are both received and sent. The port is involved in the spanning tree algorithm.
- **Learning**
  Stage prior to the forwarding status, the port is actively learning the topology (in other words, the node addresses).
- **Forwarding**
  Following the reconfiguration time, the port is active in the network; it receives and forwards data frames.

• **Fwd. Trans**

Specifies the number of changes from the "Discarding" status to the "Forwarding" status.

• **Edge Type**

Specify the type of edge port. You have the following options:
- "."  
  Edge port is disabled. The port is treated as a "no EdgePort".
- **Admin**
  Select this option when there is always an end device on this port. Otherwise a reconfiguration of the network will be triggered each time a connection is changed.
6.7 "Layer 2" menu

- **Auto**
  Select this option if you want a connected end device to be detected automatically at this port. When the connection is established the first time, the port is treated as a "no Edge Port."

- **Admin/Auto**
  Select these options if you operate a combination of both on this port. When the connection is established the first time, the port is treated as an Edge Port.

- **Edge**
  Shows the status of the port.
  - **Enabled**
    An end device is connected to this port.
  - **Disabled**
    There is a spanning tree or rapid spanning tree device at this port.

With an end device, a switch can change over the port faster without taking into account spanning tree frames. If a spanning tree frame is received despite this setting, the port automatically changes to the "Disabled" setting for switches.

- **P.t.P. type**
  Select the required option from the drop-down list. The selection depends on the port that is set.
  - **P.t.P.**
    Even with half duplex, a point-to-point link is assumed.
  - **Shared Media**
    Even with a full duplex connection, a point-to-point link is not assumed.

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

  - **"-"**
    Point to point is 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.

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 8 MSTP instances.

The table has the following columns:

- **Select**
  Select the row you want to delete.

- **MSTP instance ID**
  Shows the number of the MSTP instance.

- **Root Address**
  Shows the MAC address of the root bridge.

- **Root Priority**
  Shows the priority of the root bridge.
• **Bridge Priority**  
Enter the bridge priority in this box. The value for the bridge priority is a whole multiple of 4096 with a range of values from 0 to 61440.

• **VLAN ID**  
Enter the VLAN ID. Here, you can also specify ranges with Start ID, "-", End ID. Several ranges or IDs are separated by ",".  
Permitted values: 1-4094

**Procedure**

**Creating a new entry**

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

**Deleting entries**

1. Use the check box at the beginning of the relevant row to select the entries to be deleted.
2. Click the "Delete" button to delete the selected entries from memory. The entries are deleted from the memory of the device and the display on this page is updated.
6.7.3.5 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.

### Description

The page contains the following box:

- **MSTP Instance ID**
  - In the drop-down list, select the ID of the MSTP instance.

Table 1 has the following columns:

- **Column 1**
  - Shows that the settings are valid for all ports of table 2.

- **MSTP Status**
  - In the drop-down list, select the setting for all ports. If "No Change" is selected, the entries of the corresponding column in table 2 remain unchanged.

- **Copy to table**
  - If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
  - Shows all available ports and interfaces.

- **MSTP instance ID**
  - Shows the ID of the MSTP instance.

- **MSTP Status**
  - Click the check box to enable or disable this option.
• **Priority**
  Enter the priority of the port. The priority is only evaluated when the path costs are the same. The value must be divisible by 16. If the value that cannot be divided by 16, the value is automatically adapted. Range of values: 0 - 240. The default is 128.

• **Cost Calc.**
  Enter the path cost calculation in the input box. If you enter the value "0" here, the automatically calculated value is displayed in the next box "Path Costs".

• **Path Cost**
  The path costs from this port to the root bridge. The path with the lowest value is selected as the path. If several ports of a device have the same value, the port with the lowest port number will be selected. If the "Cost Calc." box has the value "0", the automatically calculated value is shown. Otherwise, the value of the "Cost Calc." box is displayed. The calculation of the path costs is largely based on the transmission speed. The higher the achievable transmission rate, the lower the value for the path costs will be. Typical values for rapid spanning tree are as follows:
  - 1000 Mbps = 20,000
  - 100 Mbps = 200,000
  - 10 Mbps = 2,000,000
  The values can, however, also be set individually.

• **Status**
  Displays the current status of the port. The values are only displayed and cannot be configured. The following is possible for status:
  - Discarding
    The port exchanges MSTP information but is not involved in the data traffic.
  - Blocked
    In the blocking mode, BPDU frames are received.
  - Forwarding
    The port receives and sends data frames.

• **Fwd. Trans.**
  Specifies the number of status changes Discarding - Forwarding or Forwarding - Discarding.

**Procedure**

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

Applications

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

All the ports of the device are displayed on this WBM page.

---

Note

Empty table

If you have enabled NAT on the device, the table is empty or will be emptied.

---

Description

The table has the following columns:

- **Port**
  Shows the available ports.

- **Setting**
  Specify whether the port should block or forward outgoing DCP frames. You have the following options available:
  - **Block**
    No outgoing DCP frames are forwarded via this port. It is nevertheless still possible to receive via this port.
  - **Forward**
    The DCP frames are forwarded via this port.

Procedure

1. Specify whether the port blocks or forwards the DCP frames.
2. Click the "Set Values" button.
6.7.5 LLDP

Identifying the network topology

LLDP (Link Layer Discovery Protocol) is defined in the IEEE 802.1AB standard.

LLDP is a method used to discover the network topology. Network components exchange information with their neighbor devices using LLDP.

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

Applications

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

Description

The table has the following columns:

- **Port**
  Shows the port.

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

1. Select the required LLDP functionality from the drop-down list.
2. Click the "Set Values" button.
6.8 "Layer 3" menu

6.8.1 NAT

6.8.1.1 Basic

Note
This page is only available in client mode.

On this page, you specify the basic settings for NAT.

![IP Network Address Translation (NAT) Settings](image)

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. Can only be enabled if "Own" is set on the client for "MAC Mode".

- **TCP Idle Timeout [s]**
  Enter the required time in seconds. If no data exchange takes place, the TCP connection is deleted from the translation table when this time has elapsed.
  The range of values is 1 to 4294967295.
  Default setting: 86400 seconds

- **UDP Idle Timeout [s]**
  Enter the required time in seconds. If no data exchange takes place, the UDP connection is deleted from the translation table when this time has elapsed.
The range of values is 1 to 4294967295.
Default setting: 300 seconds

- **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.

**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. Click the "Set Values" button.

**6.8.1.2 NAPT**

**Note**

This page is only available in 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.
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.

- **Dynamic Global IP**
  Shows whether or not dynamic address translation is used.

- **Traffic Type**
  Shows whether UDP or TCP frames are assigned to the global port.

- **Global IP Address**
  Shows the global IP address to which the local IP address will be translated.
• **Global Port**
  Shows the global port.

• **Local IP Address**
  Shows the IP address of the node in the local network.

• **Local Port**
  Shows the number of the local port.

**Procedure**

1. From the "Traffic Type" drop-down list, select the protocol for which the address assignment is valid.
2. Enter the number of the global port or a port range in "Global Port".
3. Enter the IP address of the node in the local network in "Local IP Address".
4. Enter the number of the local port or a port range in "Local Port".
5. Click the "Create" button. A new entry is generated in the table.
6. Click the "Set Values" button. The device is restarted.
6.9 "Security" menu

6.9.1 Users

6.9.1.1 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.

<table>
<thead>
<tr>
<th>Role Name</th>
<th>Function Right</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>1</td>
<td>System defined role, with read-only access to configuration data of this component.</td>
</tr>
<tr>
<td>admin</td>
<td>15</td>
<td>System defined role, with read/write access to configuration data of this component.</td>
</tr>
<tr>
<td>default</td>
<td>1</td>
<td>Internal role, for authenticated users without group/role mapping in this component.</td>
</tr>
<tr>
<td>everybody</td>
<td>0</td>
<td>Internal role, assigned to users when authentication fails. Access will be denied.</td>
</tr>
</tbody>
</table>

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.
  - 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.

**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 of 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.
6.9.1.2 Groups

User Groups

On this page you link a group with a role.

In this example the group "Administrators" is linked to the "admin" role: The group is defined on a RADIUS server. The role is defined locally on the device. When a RADIUS server authenticates a user and assigns the user to the "Administrators" group, this user is given rights of the "admin" role.

**Note**
The values displayed depend on the rights of the logged-in user.

The page contains the following:

- **Group Name**
  Enter the name of the group. The name must match the group on the RADIUS server. The name must meet the following conditions:
  - It must be unique.
  - It must be between 1 and 64 characters long.

The 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 the 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.
6.9.1.3 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.
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.

  **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**
  **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 the set password policy.
6.9 "Security" menu

- **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.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>The preset users as well as logged in users cannot be deleted or changed.</td>
</tr>
</tbody>
</table>

- **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

#### 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.
6.9.2 Passwords

6.9.2.1 Device passwords

Configuration of the device passwords

Note

If you are logged in via a RADIUS server, you cannot change any passwords.

On this page, you can change passwords. If you are logged in with the right to change device parameters, you can change the passwords for all user accounts. If you are logged on as user, you can only change your own password.

Description of the displayed boxes

- **Current User**
  Shows the user that is currently logged in.

- **Current User Password**
  Enter the password for the currently logged in user.

- **User Account**
  Select the user whose password you want to change.
• **Password Policy**
  Shows which password policy is being used when assigning new passwords.

  **Note**
  **Checking the password policy of existing users**
  Up to now there was no special password policy. As of version V6.0 you can now assign passwords that correspond to the password policy "high".

  The set password policy is used when assigning new passwords. Existing passwords are not checked. If you change the password policy from "Low" to "High", the previously used passwords remain valid. As an important measure for increasing security, change the passwords used up to now.

  – **High**
    - Password length: at least 8 characters, maximum 128 characters
    - at least 1 uppercase letter
    - at least 1 special character
    - at least 1 number
  – **Low**
    - Password length: at least 6 characters, maximum 128 characters

• **New Password**
  Enter the new password for the selected user.

• **Password Confirmation**
  Enter the new password again to confirm it.

**Procedure**

1. In the "Current User Password" enter the valid password of the currently logged in user.
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 "aadmin" you will be prompted to change the password.

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

### 6.9.2.2 Password options
On this page you specify which password policy will be used when assigning new passwords.

![Password Options](image)

**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 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 "SiemensVSA"

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.
6.9.3.2 General

Login of network nodes

The designation "AAA" stands for "Authentication, Authorization, Accounting". This feature is used to identify and allow network nodes, to make the corresponding services available to them and to specify the range of use.

On this page, you configure the login.

Description of the displayed boxes

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.
6.9.3.3 **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**

<table>
<thead>
<tr>
<th>Select</th>
<th>Auth. Server Type</th>
<th>RADIUS Server Address</th>
<th>Server Port</th>
<th>Shared Secret</th>
<th>Shared Secret Conf</th>
<th>Fail. Retrans</th>
<th>Primary Server</th>
<th>Test</th>
<th>Test Result</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Login</td>
<td>192.168.16.2</td>
<td>1812</td>
<td>************</td>
<td>************</td>
<td>3</td>
<td>no</td>
<td>![Test]</td>
<td>Not reachable</td>
</tr>
</tbody>
</table>

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.
6.9 "Security" menu

- **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 254.

- **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

Transmission standard IEEE 802.11 n

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

iPCF or iPCF-MC mode activated

If iPCF or iPCF-MC mode is enabled, only "Open System" with the encryption method AES is supported in the security settings.
Description

The table has the following columns:

- **Interface**
  Shows the available interfaces.

- **Authentication Type**
  Select the type of authentication. The selection depends on the operating mode and the transmission standard.

  - **Open System**
    There is no authentication. Encryption with a fixed (unchanging) WEP key can be selected as an option. To use the key, enable "Encryption". You define the WEP key on the "Keys" page.
    If iPCF or iPCF-MC mode is enabled, only the encryption method AES with 128 bit key length is supported.

  - **Shared Key**
    In Shared Key authentication, a fixed key is stored on the client and access point. This WEP key is then used for authentication and encryption. You define the WEP key on the "Keys" page.

  **Note**

  If you use "Open System" with "Encryption" or "Shared Key", Key 1 must always be set on the "Keys" page.

  - **WPA (RADIUS)**
    Wi-Fi Protected Access (WPA) is a method specified by the Wi-Fi Alliance to close security gaps in WEP. Authentication using a server is stipulated (802.1x). The dynamic exchange of keys at each data frame introduces further security.

  - **WPA-PSK**
    WPA Pre Shared Key (WPA-PSK) is a weakened form of WPA. In this method, authentication is not established by a server but is based on a password. This password is configured manually on the client and server.

  - **WPA2 (RADIUS)**
    WPA2 (Wi-Fi Protected Access 2) is a further development of WPA and implements the functions of the IEEE 802.11i security standard. WPA authentication works, however, without the RADIUS server.

  - **WPA2-PSK**
    WPA2-PSK is based on the 802.11i standard. WPA authentication works, however, without a RADIUS server. Instead of this, a WPA(2) key (WPA(2) pass phrase) is stored on each client and access point. The WPA(2) pass phrase is used for authentication and further encryption.

  - **WPA/WPA2-Auto-PSK**
    Setting with which an access point can process both the "WPA-PSK" as well as the "WPA2-PSK" type of authentication. This is necessary when the access point communicates with different clients, some using "WPA-PSK" and others "WPA2-PSK". The same encryption method is set on the clients.
- **WPA/WPA2-Auto**
  Setting with which an access point can process both the "WPA" as well as the "WPA2" type of authentication. This is necessary when the access point communicates with different clients, some using "WPA" and others "WPA2". The same encryption method is set on the clients.

- **Encryption**
  Encryption protects the transferred data from eavesdropping and corruption. You can only disable encryption if you have selected "Open System" for authentication. All other security methods include both authentication and encryption.

- **Cipher**
  Select the encryption method. The selection depends on the transmission standard.
  - **AUTO**
    AES or TKIP is 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) pass phrase 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.

<table>
<thead>
<tr>
<th>Authentication Type</th>
<th>Encryption</th>
<th>Cipher</th>
<th>Encryption key source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open System</td>
<td>disabled</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Open System</td>
<td>enabled</td>
<td>WEP</td>
<td>Default Key</td>
</tr>
<tr>
<td>Open System</td>
<td>enabled</td>
<td>AES&lt;sup&gt;1)&lt;/sup&gt;</td>
<td>Default Key (128-bit)</td>
</tr>
<tr>
<td>Shared Key</td>
<td>enabled</td>
<td>WEP</td>
<td>Default Key</td>
</tr>
<tr>
<td>WPA (RADIUS)</td>
<td>enabled</td>
<td>Auto/TKIP/AES</td>
<td>RADIUS Server</td>
</tr>
<tr>
<td>WPA-PSK</td>
<td>enabled</td>
<td>Auto/TKIP/AES</td>
<td>WPA(2) Pass Phrase</td>
</tr>
<tr>
<td>WPA2 (RADIUS)</td>
<td>enabled</td>
<td>Auto/TKIP/AES</td>
<td>RADIUS Server</td>
</tr>
<tr>
<td>WPA2-PSK</td>
<td>enabled</td>
<td>Auto/TKIP/AES</td>
<td>WPA(2) Pass Phrase</td>
</tr>
<tr>
<td>WPA/WPA2-AutoPSK</td>
<td>enabled</td>
<td>Auto/TKIP/AES</td>
<td>WPA(2) Pass Phrase</td>
</tr>
<tr>
<td>WPA/WPA2-Auto</td>
<td>enabled</td>
<td>Auto/TKIP/AES</td>
<td>RADIUS Server</td>
</tr>
</tbody>
</table>

<sup>1)</sup> available only with iPCF or iPCF-MC

2. Click the "Set Values" button.

6.9.4.2 Basic

Safety levels

To make the network secure, authentication and encryption are used. On this page, you specify the security settings.

Note

Transmission standard IEEE 802.11 n

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

iPCF or iPCF-MC mode activated

If iPCF or iPCF-MC mode is enabled, only "Open System" with the encryption method AES is supported in the security settings with Security Context 1.
### WLAN Security Settings

<table>
<thead>
<tr>
<th>Security Context</th>
<th>Authentication Type</th>
<th>Encryption</th>
<th>Cipher</th>
<th>WPA(2) Pass Phrase</th>
<th>WPA(2) Pass Phrase Confirmation</th>
<th>Default Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Open System</td>
<td>WEP</td>
<td></td>
<td></td>
<td></td>
<td>Key 1</td>
</tr>
</tbody>
</table>

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 row 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.
      - If iPCF or iPCF-MC mode is enabled, only the encryption method AES with 128 bit key length is supported.
    - **Shared Key**
      - In Shared Key authentication, a fixed key is stored on the client and access point. This WEP key is then used for authentication and encryption. You define the WEP key on the "Keys" page.
    - **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 > Basic".
- **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.

- **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.
6.9 "Security" menu

- **Cipher**
  Select the encryption method. The selection depends on the transmission standard.
  - **AUTO**
    AES or TKIP is used depending on the capability of the other station.
  - **WEP**
    WEP (Wired Equivalent Privacy)
    A symmetrical stream encryption method with only 40- or 104-bit long keys based on the RC4 algorithm (Ron’s Code 4).
  - **TKIP (Temporal Key Integrity Protocol)**
    A symmetrical encryption method with the RC4 algorithm (Ron’s Code 4). In contrast to the weak WEP encryption, TKIP uses changing keys derived from a main key. TKIP can also recognize corrupted data frames.
  - **AES (Advanced Encryption Standard)**
    Strong symmetrical block encryption method based on the Rijndael algorithm that further improves the functions of TKIP.

**Note**
To provide better protection of your data against attacks, use WPA2/WPA2-PSK with AES.

- **WPA(2) Pass Phrase**
  Enter a WPA(2) key here. This WPA(2) key must be known 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. Which settings are possible depends on the "Authentication Type" you have selected.
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.

Description

Table 1 has the following columns:

- **Column 1**
  Shows that the settings are valid for all ports of table 2.

- **within own VAP / with other VAPs / with Ethernet**
  In the drop-down list, select the setting for all ports. If "No Change" is selected, the entry in table 3 remains unchanged.

- **Copy to Table**
  If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

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

- **Port**
  Shows the VAP interface.

<table>
<thead>
<tr>
<th>Radio</th>
<th>Port</th>
<th>within own VAP</th>
<th>with other VAPs</th>
<th>with Ethernet</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN 1</td>
<td>VAP 1.1</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>WLAN 1</td>
<td>VAP 1.2</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>WLAN 1</td>
<td>VAP 1.3</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>WLAN 1</td>
<td>VAP 1.4</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>WLAN 1</td>
<td>VAP 1.5</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>WLAN 1</td>
<td>VAP 1.6</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
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.

- **with other VAPs**
  - Enabled
    Clients logged on to different VAP interfaces of an access point can communicate with each other.

  **Note**
  For an access point, “with other VAPs” needs to be enabled on all WLAN interfaces or on all VAP interfaces to allow communication between clients logged on at different VAP interfaces of the access point.

  - Disabled
    Option is disabled.

  **Note**
  “within own VAP” or “with other VAPs” function disabled
  If the “within own VAP” or “with other VAPs” 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.

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.
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.
• **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 WBM page is only available in client mode.

Description

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 on 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.
• **Dot1x Check Server Certificate**
  Specify whether or not the RADIUS server identifies itself to the client using a certificate.

• **Dot1x EAP Types**
  Specify the authentication method. The following methods are available:
  
  – **Auto**
    EAP-TLS, EAP-TTLS or PEAP is used depending on the capability of the other station.
  
  – **EAP-TLS**
    Client logs on using a certificate.
  
  – **EAP-TTLS**
    The client logs on with the RADIUS server using the user name and password.
  
  – **PEAP**
    The client logs on with the RADIUS server using the user name and password.

**Procedure**

1. Enter the necessary values in the input boxes.
2. Select the required entry in the "Dot1x EAP Types" drop-down list.
3. Click the "Set Values" button.
### 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.

<table>
<thead>
<tr>
<th>Key 1 Confirmation</th>
<th>Key 2 Confirmation</th>
<th>Key 3 Confirmation</th>
<th>Key 4 Confirmation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description**

The table has the following columns:

- **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 "ABCDEF" (ASCII characters) and "4142434445" (hexadecimal characters) are therefore the same because the ASCII character "A" has hexadecimal code "0x41".

- **Key 1 - 4 Confirmation**
  Confirm the WEP key.

**Procedure**

1. Enter at least one WEP key.
2. Click the "Set Values" button.
6.9.5  MAC ACL

6.9.5.1  Rules Configuration

Introduction

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.

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 MAC**
  Enter the unicast MAC address of the source.

- **Dest. MAC**
  Enter the unicast 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

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.

Steps in configuration

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".
3. Enter the MAC address of the destination in "Dest MAC".
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

You cannot delete active entries.
1. Enable "Select" in the row to be deleted.
2. Click the "Delete" button. The entry is deleted.

6.9.5.2 Ingress Rules

Introduction

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.
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 43) 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**
  Shows the unicast MAC address of the source.

- **Dest. MAC**
  Shows the unicast 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.

Steps in configuration

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:

**Note**
active rules
You cannot delete active rules.

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

Introduction

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.

<table>
<thead>
<tr>
<th>MAC ACL Egress Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rules Configuration</td>
</tr>
</tbody>
</table>

- **Interface**: P1
- **Add Rule**: 
- **Remove Rule**: Rule 1

<table>
<thead>
<tr>
<th>Rule Order</th>
<th>Rule Number</th>
<th>Source MAC</th>
<th>Dest. MAC</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>00-00-00-00-00-00</td>
<td>00-00-00-00-00-00</td>
<td>Forward</td>
</tr>
</tbody>
</table>

1 entry.

**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 43) depend on your device.

- **Add Rule**
  In the drop-down list select the ACL rule to be assigned to the interface.
6.9 "Security" menu

- **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**
  Shows the unicast MAC address of the source.

- **Dest. MAC**
  Shows the unicast 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.

**Steps in configuration**

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:

**Note**

**active rules**

You cannot delete active rules.

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

Introduction

On this page, you specify the rules for the IP-based Access Control List. Using the IP-based ACL, you can specify whether frames of certain IPv4 addresses are forwarded or discarded.

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".

---

**Steps in configuration**

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 an entry**
You cannot delete active entries.

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.

**Settings**

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.

- **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.
6.9.6.3 **Ingress Rules**

**Introduction**

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.

---

**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.

---

**IP ACL Ingress Rules**

![Figure 6-8 IP ACL ingress rules - first part of the table](image1)

![Figure 6-9 IP ACL ingress rules - second part of the table](image2)
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 43) depend on your device.
  To select a VLAN interface, an IP interface must be configured.

- **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**
  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.

---

**Note**
If you use a VLAN interface, the ACL rule applies to all ports that belong to the VLAN.
- **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.

### Steps in configuration

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:

---

**Note active rules**

You cannot delete active rules.

---

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

Introduction

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.

Figure 6-10 IP ACL egress rules - first part of the table

Figure 6-11 IP ACL egress rules - second part of the table
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 43) 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.

- **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**
  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.
Configuring with Web Based Management

6.9 “Security” menu

- **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.

**Steps in configuration**

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.

**Note**

_active rules_

You cannot delete active rules.

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 Access Control List

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**
  - Enable or disable the function.

  **Note**
  - If the function is disabled, there is unrestricted access to the management of the IE switch. 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 IP address 0.0.0.0, the settings apply to all IP addresses.
• **Subnet Mask**
  Enter the subnet mask. The subnet mask 255.255.255.255 is for a specific IP address. If you want to allow a subnet, for example a C subnet, enter 255.255.255.0. The subnet mask 0.0.0.0 applies to all subnets.

The table has the following columns:

• **Select**
  Select the check box in the row to be deleted.

• **Rule Order**
  Shows the number of the rule. If you click the "Create" button, a new row with a unique number is created.

• **IP Address**
  Shows the IP address.

• **Subnet Mask**
  Shows the subnet mask.

• **VLANs Allowed**
  Only available if 802.1Q VLAN Bridge is set for "Layer 2 > VLAN > General". Enter the number of the VLAN in which the device is located. The station can only access the device if it is located in this configured VLAN. If this input box remains empty, there is no restriction relating to the VLANs.

• **SNMP**
  Specify whether the station (or the IP address) accesses the device using the SNMP protocol.

• **TELNET**
  Specify whether the station (or the IP address) accesses the device using the TELNET protocol.

• **HTTP**
  Specify whether the station (or the IP address) accesses the device using the HTTP protocol.

• **HTTPS**
  Specify whether the station (or the IP address) accesses the device using the HTTPS protocol.

• **SSH**
  Specify whether the station (or the IP address) accesses the device using the SSH protocol.

• **Px**
  Specify whether the station (or the IP address) accesses the device via this port.

• **WLAN 1** (client mode only)
  Specify whether or not the station (or the IP address) accesses the device via the WLAN interface.
Configuring with Web Based Management

6.9 "Security" menu

- **VAP X.Y** (access point mode only)
  Specify whether or not the station or the IP address accesses the device via the VAP interface.

- **WDS X.Y** (access point mode only)
  Specify whether or not the station or the IP address accesses the device via the WDS interface.

Procedure

**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" 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.
6.9.8 Inter AP blocking

6.9.8.1 Basic

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

**When should Inter AP blocking be used?**

The clients connected to an access point can normally communicate with all SCALANCE W700 devices of the layer 2 network.

With inter AP blocking, the communication of the clients connected to the access point can be restricted. Only the SCALANCE W700 devices whose IP addresses are configured in “Allowed Addresses” on the access point are accessible to the clients. Communication with other nodes in the network is therefore prevented.
Description

The page contains the following box:

- **Update interval [s]**
  
Enter the update interval for the ARP table.

The table has the following columns:

- **Radio**
  
  Specifies the WLAN interface to which the settings relate.

- **Port**
  
  Specifies the VAP interface to which the settings relate.

- **SSID**
  
  Specifies the SSID to which the settings relate.

- **Activate**
  
  When enabled, the access restriction is used. You configure which devices are accessible to the clients in "Security > Inter AP Blocking > Allowed Addresses".

- **Block Gratuitous ARP Requests**
  
  When enabled, gratuitous ARP packets are not forwarded.

- **Block Non-IP Frames**
  
  When enabled, there is no exchange of non-IP packets, for example layer 2 packets between the client and the devices configured on the access point as permitted communications partners.
6.9.8.2 Allowed Addresses

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

On this WBM page you specify which SCALANCE W700 devices are accessible to the clients.

Description

The page contains the following boxes:

- **Port**
  Select the required port from the drop-down list.

- **IP Address**
  Enter the IP address of the devices accessible to the client.

The table has the following columns:

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

- **Radio**
  Specifies the WLAN interface to which the settings relate

- **Port**
  Specifies the VAP interface to which the settings relate
- **IP Address**
  The IP Address of the devices accessible to the client. If necessary, you can change the IP address.

- **Resolver IP Address**
  The IP address with which the allowed IP address is resolved. The entry is necessary when the management IP address is located in a different subnet.
  If the IP address "0.0.0.0" is configured for "Resolver IP Address", the management IP address is used for resolution.

**Procedure**

**Creating an entry**
1. Select a port from the "Port" drop-down list.
2. In the "IP Address" box, enter the IP address accessible for the client.
3. Click the "Create" button. A new entry is created in the table.

**Deleting an entry**
1. Enable "Select" in the row to be deleted.
2. Click the "Delete" button. The entry is deleted.
6.10  "iFeatures" menu

6.10.1  iPCF

Note
This WBM page can only be configured with the following KEY-PLUGs:
- Access point: W780 iFeatures (MLFB 6GK5 907-8PA00)
- Client: W740 iFeatures (MLFB 6GK5 907-4PA00)

When should iPCF be used?
The use of iPCF is advisable particularly if you have a large number of nodes and want to implement highly deterministic operation. This is necessary, for example with PROFINET or other cyclic protocols. You will find a more detailed description of iPCF in the section "Technical basics" in the section "iPCF / iPCF-MC".

Note
Use of iPCF with other iFeatures
iPCF and other iFeatures (e.g. iPCF-MC, iPRP) are not compatible with each other and cannot be used at the same time on a device.

The possible settings differ for access point and client. Below, both will be described.
In both modes, the table has the following columns:

- **Radio**
  Specifies the WLAN interface to which the settings relate.

- **Enable iPCF**
  Enable or disable the 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).

In access point mode, the table has the following additional columns:
• **Protocol Support**
  Specify which protocol is handled with priority by the WLAN interface.
  - **PROFINET**
    if you set PROFINET, there must be no PROFINET controller downstream from the client.
  - **EtherNet/IP**
    If you set Ethernet/IP, there must be no scanner downstream from the client.
  - **Disabled**
    The function is disabled.

• **iPCF Cycle Time [ms]**
  Select the required cycle time from the drop-down list.
  The following points need to be taken into account when setting the cycle time. Otherwise it may not be possible to establish stable communication.
  - There is only one access point in the system; in other words, the clients move only in one wireless cell. In this case, update times $$\geq 16$$ ms are supported.
  - There are several access points in the system that communicate over different channels. The clients roam between the access points. In this case, select update times $$\geq 32$$ ms.

  In addition to the guide values shown above, remember that the shortest cycle time to be set is calculated according to the formula "$2 \text{ ms} \times \text{max. number of nodes}$".

• **Scanning Mode**
  The selected setting affects the scanning of the logged-on clients.
  The following settings are available:
  - **All Channels**
    The client scans all permitted channels and selects the access point with the best signal strength and connects to it.
  - **Next Channel**
    The client scans the next channel from its permitted channel list. If an access point is there, it connects to it. If it does not find an access point on this channel, it scans the next channel.

• **Signal Quality Threshold**
  Can only be configured if "Next Channel" is set for "Scanning Mode". The client is given a minimum signal strength with which the access point must be seen during the scan so that a connection can be established to it.
  The following threshold values exist for the signal strength:

<table>
<thead>
<tr>
<th>Level</th>
<th>Signal quality in RSSI</th>
<th>Signal quality in %</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>20</td>
<td>40</td>
</tr>
<tr>
<td>2</td>
<td>25</td>
<td>50</td>
</tr>
<tr>
<td>3</td>
<td>30</td>
<td>60</td>
</tr>
<tr>
<td>4</td>
<td>35</td>
<td>70</td>
</tr>
<tr>
<td>5</td>
<td>40</td>
<td>80</td>
</tr>
</tbody>
</table>
6.10 "iFeatures" menu

Procedure

In access point mode
1. Select the "Enable iPCF" option for the required WLAN interface.
2. Select the required cycle time for the access point from the "iPCF Cycle Time [ms]" drop-down list.
3. Select for example "All Channels" from the "Scanning Mode" drop-down list.
4. Click the "Set Values" button. You configure the security settings in "Security > WLAN > Basic".

In client mode
1. Select the "Enable iPCF" option for the required WLAN interface.
2. Click the "Set Values" button.
You configure the security settings in "Security > WLAN > Basic".

6.10.2 iPCF-MC

Note
Use of iPCF with other iFeatures
The function iPCF-MC 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.

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

Requirements to be able to use iPCF-MC:
- The access point has at least two WLAN interfaces (dual AP).
- Access point mode: Only dual APs with KEY-PLUG W780 iFeatures (MLFB 6GK5 907-8PA00)
- Client mode: Client with KEY-PLUG W740 iFeatures (MLFB 6GK5 907-4PA00)
- The management interface and data interface must be operated in the same frequency band and mode and must match in terms of their wireless coverage. iPCF-MC will not work if both wireless interfaces are equipped with directional antennas that cover different areas.
- The management interfaces of all access points to which a client can change must use the same channel. A client scans only this one channel to find accessible access points.
- Transmission based on IEEE801.11h (DFS) cannot be used for the management interface. For the data interface 801.11h (DFS) is possible.
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 security context 1. An SSID is active when the corresponding check box "Enabled" is selected on the "Interfaces > WLAN > Client" page.

In Japan, iPCF-MC cannot be enabled if the data or management interface uses a frequency of the 4920 MHz - 5080 MH 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.

**In client mode**

```
Industrial Point Coordination Function with Management Channel (iPCF-MC)

Enable iPCF-MC

Management Scan Period: 1

Set Values Refresh
```

**In access point mode**

```
Industrial Point Coordination Function with Management Channel (iPCF-MC)

Enable iPCF-MC

iPCF Cycle Time [ms]: 32

Protocol Support: PROFINET

Set Values Refresh
```
6.10 "iFeatures" menu

Description

The page contains the following boxes:

- **Enable iPCF-MC activated**
  
  Enable or disable the iPCF-MC mode of the SCALANCE W700 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).

- **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.

- **iPCF Cycle Time** (only in access point mode)
  
  Select the update time configured for the network to which the access point is connected. The lowest value for the update time is 32 ms.

- **Protocol Support** (only in access point mode)
  
  Specify which protocol is handled with priority.
  
  - PROFINET
    
    If you set PROFINET, there must be no PROFINET controller downstream from the client.
  
  - EtherNet/IP
    
    If you set Ethernet/IP, there must be no scanner downstream from the client.

6.10.3 iREF

**Note**

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

**Note**

**Use of iREF with other iFeatures**

iREF and other iFeatures (e.g. iPFC-MCiREF, iPRLiPFC) are not compatible with each other and cannot be used at the same time on a device.

With iREF, the data can be sent with the highest possible transmit power. In particular in applications in which MIMO cannot be used or brings no advantage, this allows data to be transmitted at the highest possible data transmission rate.

![Industrial Range Extension Function (iREF)](image)

### Description

The table has the following columns:

- **Radio**
  
  Specifies the WLAN interface to which the settings relate.

- **Enable iREF**
  
  Enable or disable iREF for the required WLAN interface. The result is shown in "Information > WLAN >iFeatures".

**Note**

To be able to use iREF, there must be at least two antennas.

The antennas are automatically switched to Mode RX/TX as soon as iREF is enabled.
6.10.4 iPRP

---

**Note**

This WBM page can only be configured with the following KEY-PLUGs:

- Access point: W780 iFeatures (MLFB 6GK5 907-8PA00)
- Client: W740 iFeatures (MLFB 6GK5 907-4PA00)

---

**When should iPRP be used?**

---

**Note**

**Use of iPRP with other iFeatures**

iPRP and other iFeatures (e.g. iPCF, iPCF-MC, ) are not compatible with each other and cannot be used at the same time on a device.

---

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.

Below, both will be described.
Requirements

- The Base Bridge mode "802.1Q VLAN Bridge" is set.
- The VLANs have been created.
- Access point mode: The VAP interface is enabled.
- Client mode: For "MAC Mode", Layer 2 Tunnel is set.

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:

- **Interface**
  Shows the available interfaces.

- **Enable iPRP**
  Enable or disable iPRP for the required interface.

- **PRP Network**
  Specify the PRP network in which the interface is a member.

**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 interface is a member.
4. Select the "Enable iPRP" setting. Click the "Apply settings" button.
   The appropriate VLAN settings are made automatically.
6.10.5 AeroScout

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

Note
Using AeroScout
- AeroScout and other iFeatures (e.g. iREF iPCF, iPFC-MC, iPRP) are not compatible with each other and cannot be used at the same time on a device.
- AeroScout can only be used in the 2.4 GHz band according to IEEE 802.11g, IEEE 802.11n and IEEE 802.11n only.
  For more detailed information, please refer to the documentation of the AeroScout company (www.aeroscout.com).

Description
The table has the following columns:
- **Radio**
  Specifies the WLAN interface to which the settings relate.
- **Enable AeroScout**
  Enable or disable AeroScout for the required WLAN interface. The result is shown in "Information > WLAN iFeatures > AeroScout".
Configuring with Web Based Management

6.10 "iFeatures" menu
Upkeep and maintenance

7.1 Firmware update - via WBM

Requirement

- The device has an IP address.
- The user is logged in with administrator rights.

Firmware update via HTTP

1. Click "System > Load&Save" in the navigation area. Click the "HTTP" tab.
2. Click the "Load" button in the "Firmware" table row.
3. Go to the storage location of the firmware file.
4. Click the "Open" button in the dialog. The file is uploaded.

Firmware update - via TFTP

1. Click "System > Load&Save" in the navigation area. Click the "TFTP" tab.
2. Enter the IP address of the TFTP server in the "TFTP Server Address" input box.
3. Enter the port of the TFTP server in the "TFTP Server Port" input box.
4. Click the "Load file" button in the "Firmware" table row.
5. Go to the storage location of the firmware file.
6. Click the "Open" button in the dialog. The file is uploaded.

Result

The firmware is 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 Device configuration with PRESET-PLUG

Please note the additional information and security notes in the operating instructions of your device.

NOTICE

Do not remove or insert a PLUG during operation
A PLUG may only be removed or inserted when the device is turned off.

Note

Support as of V6.0
The PRESET-PLUG functionality is supported as of firmware version V6.0.

With the PRESET-PLUG, you can install the same device configuration (start configuration, user accounts, certificates) including the corresponding firmware on multiple devices.

The PRESET PLUG is write-protected.

You configure the PRESET PLUG using the Command Line Interface (CLI).

Creating a PRESET-PLUG

You create the PRESET PLUG using the Command Line Interface (CLI). You can create a PRESET-PLUG from any PLUG. To do this, follow the steps outlined below:

Note

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

You assign fixed IP addresses extra following the basic installation.

Requirement

- A PLUG is inserted in the device on which you want to configure the PRESET-PLUG functionality.

Procedure

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 PLUG configuration mode with the "plug" command.
4. Create the PRESET-PLUG with the "presetplug" command.
   The firmware version of the device and the current device configuration incl. user accounts and certificates are stored on the PLUG and the PLUG is then write protected.
5. Turn off the power to the device.
6. Remove the PRESET-PLUG.
7. Start the device either with a new PLUG inserted or with the internal configuration.

**Procedure for installation with the aid of the PRESET-PLUG**

1. Turn off the power to the device.
2. If it exists, remove the PLUG from the slot. You will find further information on this in the operating instructions of your device.
3. Insert the PRESET-PLUG correctly oriented into the slot. The PRESET-PLUG is correctly inserted when it is completely inside the device and does not jut out of the slot.
4. Turn on the power to the device again.
   If there is a different firmware version on the device to be installed compared with that on the PRESET-PLUG, an upgrade/downgrade of the firmware is performed. You can recognize this by the red F-LED flashing (flashing interval 2 sec. on/2 sec. off). Afterwards the device is restarted and the device configuration incl. users and certificates on the PRESET-PLUG is transferred to the device.
5. Wait until the device has fully started up.
   (the red F-LED is off)
6. Turn off the power to the device after the installation.
7. Remove the PRESET-PLUG.
8. Start the device either with a new PLUG inserted or with the internal configuration.

**Note**

**KEY-PLUG**

If you have created the PRESET-PLUG from a KEY-PLUG, for operation with this configuration, you require an inserted KEY-PLUG.

In this case before recommissioning the device you need to insert the relevant KEY-PLUG.

**Note**

**Restore factory defaults and restart with a PRESET PLUG inserted**

If you reset a device to the factory defaults, when the device restarts an inserted PRESET PLUG is formatted and the PRESET PLUG functionality is lost. You then need to create a new PRESET PLUG. The keys stored on the KEY-PLUG for releasing functions are retained.

We recommend that you remove the PRESET PLUG before you reset the device to the factory settings.
You format the PRESET PLUG using the Command Line Interface (CLI) to reset the preset function. To do this, follow the steps outlined below:

1. Start the remote configuration using 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 PLUG configuration mode with the "plug" command.
4. Enter the command "factoryclean". The PRESET-PLUG is formatted and the preset function is reset.
5. Write the current configuration of the device with the "write" command.
7.3 Embedding firmware in ConfigPack.

Please note the additional information and security notes in the operating instructions of your device.

With 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 "fw in configpack" command without parameters.

   The firmware currently on this device is now embedded 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.

Refer to the information in the section Load & Save (Page 174).

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".

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/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.
7.4 Restoring the default parameter settings

Procedure

Follow the steps below to reset the device parameters to the factory settings:

---

**Note**
When you reset the device parameters, all previously changed settings are lost!

---

1. Turn off the power to the device.
2. Now press the Reset button and reconnect the power to the device while holding down the button.
3. Hold down the button until the red fault LED (F) stops flashing after approximately 10 seconds and is permanently lit.
4. Now release the button and wait until the fault LED (F) goes off again.
5. The device then starts automatically with the default parameters.
Upkeep and maintenance

7.4 Restoring the default parameter settings
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.

Solution

You can then also assign firmware to a SCALANCE W700 using TFTP. Follow the steps below to load new firmware using TFTP:

1. Turn off the power to the device.
2. Now press the Reset button and reconnect the power to the device while holding down the button.
3. Hold down the button until the red fault LED (F) starts to flash after approximately 2 seconds.
4. Now release the button. The bootloader waits in this state for a new firmware file that you can download by TFTP.
5. Connect a PC to the SCALANCE W700 over the Ethernet interface.
6. Assign an IP address to the SCALANCE W700 with the Primary Setup Tool.
7. Open a DOS box and change to the directory where the file with the new firmware is located and then execute the command "tftp -i <ip address> PUT <firmware>". As an alternative, you can use a different TFTP client.

Note

Use of CLI and TFTP in Windows 7

If you want to access the CLI or TFTP in Windows 7, make sure that the relevant functions are enabled in Windows 7.
8.1 Firmware update via WBM or CLI not possible

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 W700 device is too high, this overdrives the amplifier circuit. Overdrive can occur on clients and access points. If the received power on the SCALANCE W700 device is greater than -35 dBm, this can result in disrupted communication.

Information about the signal strength [in dBm] is displayed in WBM on the following tabs:

Access point mode:
- Information > WLAN > Client List

Client mode:
- Information > WLAN > Available AP
- Interfaces > WLAN > Signal recorder

The power of the input signal on the SCALANCE W700 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" (transmit power) (Interfaces > WLAN > Basic) and the antenna settings used (Interfaces > WLAN > Antennas).

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 transmission method IEEE 802.11b is not supported along with iPCF.
  The devices SCALANCE W700-xRR 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 354)" 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 following information about protecting your network from attacks:

- **Use a secure connection with HTTPS**
  
  In contrast to HTTP, HTTPS allows you secure access for configuring the WLAN clients and the access points using Web Based Management. For more detailed information, refer to the section "Load & Save (Page 174)".

- **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 310)".

- **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 Internet Protocol (IP) (Page 168)".
  
  - A further option is to install a separate HTTPS certificate on the WLAN client / access point. The HTTPS certificate checks the identity of the device and controls the encrypted data exchange. You can install the HTTPS certificate, for example using HTTP. For more detailed information, refer to the section "HTTP (Page 176)".

- **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 198)".

---

**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 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.

**8.5.1 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.
8.5 Configuring the device using the TIA Portal

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.
### MIB files supported by SCALANCE W700

#### MIB files available for the SCALANCE W700

The following table shows the MIB files available for a SCALANCE W700:

<table>
<thead>
<tr>
<th>MIB</th>
<th>Root OID</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTOMATION SNTP (Siemens) 1) 2)</td>
<td>.1.3.6.1.4.1.4329.6.3.11</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>AUTOMATION SYSTEM MIB (Siemens) 1) 2)</td>
<td>.1.3.6.1.4.1.4329.6.3.2</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>AUTOMATION TELNET (Siemens) 1) 2)</td>
<td>.1.3.6.1.4.1.4329.6.3.8</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>AUTOMATION TIME MIB (Siemens) 1) 2)</td>
<td>.1.3.6.1.4.1.4329.6.3.3</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>BRIDGE MIB</td>
<td>.1.3.6.1.2.1.1.17</td>
<td>RFC1493</td>
</tr>
<tr>
<td>ENTITY-MIB</td>
<td>.1.3.6.1.2.1.1.47</td>
<td></td>
</tr>
<tr>
<td>EtherLike-MIB</td>
<td>.1.3.6.1.2.1.1.10.7.2</td>
<td></td>
</tr>
<tr>
<td>IANA-MAU-MIB</td>
<td>.1.3.6.1.2.1.1.26.1.1</td>
<td></td>
</tr>
<tr>
<td>IEEE8021-PAE-MIB</td>
<td>.1.0.8802.1.1.1</td>
<td>IEEE 802.1X</td>
</tr>
<tr>
<td>IEEE802dot11-MIB</td>
<td>.1.2.840.10036</td>
<td>IEEE 802.11</td>
</tr>
<tr>
<td>IF-MIB:</td>
<td>.1.3.6.1.2.1.1.2</td>
<td>RFC2233</td>
</tr>
<tr>
<td>P-BRIDGE-MIB</td>
<td>.1.3.6.1.2.1.1.17.4.5</td>
<td></td>
</tr>
<tr>
<td>Q-BRIDGE-MIB</td>
<td>.1.3.6.1.2.1.1.17.7</td>
<td></td>
</tr>
<tr>
<td>RADIUS-ACC-CLIENT-MIB</td>
<td>.1.3.6.1.2.1.1.67.2.2</td>
<td></td>
</tr>
<tr>
<td>RADIUS-AUTH-CLIENT-MIB</td>
<td>.1.3.6.1.2.1.1.67.1.2</td>
<td></td>
</tr>
<tr>
<td>RFC1213-MIB</td>
<td>.1.3.6.1.2.1.1.4</td>
<td></td>
</tr>
<tr>
<td>RMON-MIB</td>
<td>.1.3.6.1.2.1.1.16</td>
<td></td>
</tr>
<tr>
<td>SNMP-COMMUNITY-MIB</td>
<td>.1.3.6.1.6.3.18</td>
<td></td>
</tr>
<tr>
<td>SNMP-FRAMEWORK-MIB</td>
<td>.1.3.6.1.6.3.10.2.1</td>
<td>RFC2571</td>
</tr>
<tr>
<td>SNMP NOTIFICATION MIB</td>
<td>.1.3.6.1.6.3.13</td>
<td>RFC2573</td>
</tr>
<tr>
<td>SNMP PROXY MIB</td>
<td>.1.3.6.1.6.3.14</td>
<td></td>
</tr>
<tr>
<td>SN-MSPS-ACL-MIB</td>
<td>.1.3.6.1.6.3.12</td>
<td>RFC2573</td>
</tr>
<tr>
<td>SN-MSPS-CONFIG-MIB (Siemens) 2)</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.30</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>SN-MSPS-CONFIG-MIB (Siemens) 2)</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.1</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>SN-MSPS-CPLUG-MIB (Siemens) 2)</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.23</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>SN-MSPS-DHCP-CLIENT-MIB (Siemens) 2)</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.17.1</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>SN-MSPS-DIGITAL-IO-MIB (Siemens) 2(3)</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.1.39</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>SN-MSPS-GENERAL-MIB (Siemens) 2)</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.1.2</td>
<td>Vendor specific</td>
</tr>
</tbody>
</table>
## Appendix A

### A.1 MIB files supported by SCALANCE W700

<table>
<thead>
<tr>
<th>MIB</th>
<th>Root OID</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>SN-MSPS-HTTP-MIB (Siemens) 2)</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.20</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>SN-MSPS-IF-MIB (Siemens) 2)</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.34</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>SN-MSPS-IP-MIB (Siemens) 2)</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.13</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>SN-MSPS-KEY-PLUG-MIB (Siemens) 2)</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.35</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>SN-MSPS-LOAD-SAVE-MIB (Siemens) 2)</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.26</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>SN-MSPS-LOG-MIB (Siemens) 2)</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.1.31</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>SN-MSPS-MSTP-MIB (Siemens) 2)</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.6</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>SN-MSPS-NTP-MIB (Siemens)</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.133</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>SN-MSPS-PNAC-MIB (Siemens) 2)</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.1.10</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>SN-MSPS-PORT-MIB (Siemens) 2)</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.1.29</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>SN-MSPS-RADIUS-SERVER-MIB (Siemens) 2)</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.1.11.2</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>SN-MSPS-REPORT-MIB (Siemens) 2)</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.1.28</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>SN-MSPS-RMON-MIB (Siemens) 2)</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.1.12</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>SN-MSPS-SINEMA-MIB (Siemens) 2)</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.1.25</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>SN-MSPS-SNMP-MIB (Siemens) 2)</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.1.4</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>SN-MSPS-SNTP-CLIENT-MIB (Siemens) 2)</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.1.19.1</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>SN-MSPS-STP-L2T-MIB (Siemens)</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.1.40</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>SN-MSPS-SYSLOG-CLIENT-MIB (Siemens) 2)</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.1.21.1</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>SN-MSPS-VLAN-MIB (Siemens) 2)</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.1.3</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>SN-MSPS-WLAN-MIB (Siemens) 2)</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.1.27</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>SN-MSPS-NAT-MIB</td>
<td>.1.3.6.1.4.1.4329.20.1.1.1.1.1.45</td>
<td>Vendor specific</td>
</tr>
<tr>
<td>TCP-MIB</td>
<td>.1.3.6.1.2.1.6</td>
<td></td>
</tr>
<tr>
<td>UDP-MIB</td>
<td>.1.3.6.1.2.1.1.7</td>
<td></td>
</tr>
</tbody>
</table>

1) Part of the AUTOMATION.MIB  
You can download the AUTOMATION.MIB for SCALANCE W700 from Siemens Industry Automation and Drives Service & Support under the following entry ID 67637278 (http://support.automation.siemens.com/WW/view/en/67637278)  

2) Part of the private MIB file "Scalance_w_msp.sib". The file can be downloaded in WBM using "System > Load&Save > HTTP > MIB" and the "Save" button.  

3) This MIB is not supported on devices without a digital input/output.
Appendix B

B.1 Private MIB variables of the SCALANCE W700

Downloading the MIB of the SCALANCE W700 via WBM

The MIB of the SCALANCE W700 in WBM using "System > Load&Save > HTTP > MIB" and the "Save" button.

OID

The private MIB variables of the SCALANCE W700 have the following object identifiers:

```
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1)
siemens(4329) industrialComProducts(20) iComPlatforms(1)
simaticNet(1) snMsps(1) snMspsCommon(1)
```

WLAN-specific MIB variables

The WLAN-specific MIB variables can be found in "snMspsWlan". You will find further information about the settings and values in the MIB file.
Appendix B

B.1 Private MIB variables of the SCALANCE W700
### Appendix C

#### C.1 Underlying standards

**Standards met by SCALANCE W700 devices completely or partly**

The following table lists some of the standards for SCALANCE W700 devices.

<table>
<thead>
<tr>
<th>Name of the standard</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.1AB</td>
<td>Link Layer Discovery Protocol (LLDP)</td>
</tr>
<tr>
<td>IEEE 802.1D-1998</td>
<td>Media Access Control (MAC), bridges</td>
</tr>
<tr>
<td>IEEE 802.1Q</td>
<td>Virtual Bridged LANs (VLAN Tagging, Port Based VLANs)</td>
</tr>
<tr>
<td>IEEE 802.1W-2004</td>
<td>Rapid Spanning Tree Protocol (RSTP)</td>
</tr>
<tr>
<td>IEEE 802.3-2002</td>
<td>Ethernet</td>
</tr>
<tr>
<td>IEEE 802.3af</td>
<td>Power over Ethernet (PoE)</td>
</tr>
<tr>
<td>IEEE 802.11</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>IEEE 802.11a</td>
<td>Wireless standard for use of the 5 GHz frequency band</td>
</tr>
<tr>
<td>IEEE 802.11b/g</td>
<td>Wireless standard for use of the 2.4 GHz frequency band</td>
</tr>
<tr>
<td>IEEE 802.11e</td>
<td>Quality of Service (QoS)</td>
</tr>
<tr>
<td>IEEE 802.11h</td>
<td>Expansion of the spectrum and transmit power for use of the 5 GHz frequency range in Europe.</td>
</tr>
<tr>
<td>IEEE 802.11i</td>
<td>Encryption of WLANS</td>
</tr>
<tr>
<td>IEEE 802.11n</td>
<td>Standard for high transmission rates</td>
</tr>
</tbody>
</table>
Appendix C

C.1 Underlying standards
## D.1 Messages in the event log

### Messages during system startup (general)

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warm start performed, Ver: V02.00.00 - event/status summary after startup</td>
<td>Type of startup and the loaded firmware version.</td>
</tr>
</tbody>
</table>
| Power supply:  
  - L1 is connected  
  - L2 is not connected | Status of the power supplies line 1 and line 2. |
| No line is monitored | Information about monitoring the power supply from the signaling system. |
| MSTP disabled | Information on the status of the Spanning Tree protocol. |
| MSTP enabled |  |
| 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".

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power up on line 1 / 2 / PoE.</td>
<td>Power supply exists on line 1, line 2 or PoE.</td>
</tr>
<tr>
<td>Power down on line 1 / 2 / PoE.</td>
<td>Power supply interrupted on line 1, line 2 or PoE.</td>
</tr>
</tbody>
</table>

### Status of the Ethernet interface

You enable or disable the "Link Change" event in "System > Events".

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link up on P1.</td>
<td>A connection exists on the Ethernet interface.</td>
</tr>
<tr>
<td>Link down on P1.</td>
<td>No connection exists on the Ethernet interface.</td>
</tr>
</tbody>
</table>

### Status of the WLAN interface (in access point mode only)

<table>
<thead>
<tr>
<th>Messages</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link down up VAP X.Y.</td>
<td>The VAP interface Y on the WLAN interface X is enabled.</td>
</tr>
<tr>
<td>Link down on VAP X.Y.</td>
<td>The VAP interface Y on the WLAN interface X is disabled.</td>
</tr>
<tr>
<td>WDS Y at WLAN X is up.</td>
<td>A link exists on the WDS interface Y of WLAN interface X.</td>
</tr>
</tbody>
</table>
**Appendix D**

**D.1 Messages in the event log**

<table>
<thead>
<tr>
<th>Messages</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WDS Y at WLAN X is down.</td>
<td>No link exists on the WDS interface Y of WLAN interface X.</td>
</tr>
<tr>
<td>Overlap-AP found on WLAN X: AP &lt;System Name&gt; &lt;MAC&gt; found on channel &lt;channel number&gt; &gt; &lt;RSSI value&gt;</td>
<td>A further access point was detected on the channel set for the WLAN interface X or on a neighboring channel.</td>
</tr>
<tr>
<td>Overlap-AP aged out on WLAN X: AP &lt;System Name&gt; &lt;MAC&gt; on channel &lt;channel number&gt; &gt; &lt;RSSI value&gt;</td>
<td>The overlapping access point could not be detected during the configured aging time and was removed from the &quot;Overlap AP&quot; list.</td>
</tr>
<tr>
<td>DFS: Radar interference detected on WLAN X at channel &lt;channel number&gt; &gt; (frequency &lt;frequency&gt; MHz). Changing to channel &lt;channel number&gt; (frequency &lt;frequency&gt; MHz)</td>
<td>A primary user (e.g. radar or weather station) was detected on the channel set for WLAN interface X or on a neighboring channel. The channel will be blocked for 30 min. The access point changes to the configured alternative channel or to the next free channel on which there is no primary user.</td>
</tr>
<tr>
<td>DFS: channel &lt;channel number&gt; (frequency &lt;frequency&gt; MHz) aged out from NOL at WLAN X and can be used again.</td>
<td>No primary user detected on the channel any longer. The channel was removed from the list of blocked channels and can be used again.</td>
</tr>
<tr>
<td>DFS: Radar interference detected on WLAN X at channel &lt;channel number&gt; &gt; (frequency &lt;frequency&gt; MHz). No more free channels to use!!</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Status of the WLAN interface (in client mode only)**

<table>
<thead>
<tr>
<th>Messages</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link up on WLAN X.</td>
<td>The WLAN interface X is enabled.</td>
</tr>
<tr>
<td>Link down on WLAN X.</td>
<td>The WLAN interface X is disabled.</td>
</tr>
</tbody>
</table>

**Messages on configuration**

<table>
<thead>
<tr>
<th>Messages</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WBM: Authentication failure.</td>
<td>When logging in with Web Based Management (WBM), the wrong password was entered. The event can be enabled or disabled in &quot;System -&gt; Events&quot; (authentication failure).</td>
</tr>
<tr>
<td>Telnet: Authentication failure.</td>
<td>When logging in via Telnet, the wrong password was entered. The event can be enabled or disabled in &quot;System -&gt; Events&quot; (authentication failure).</td>
</tr>
<tr>
<td>Restart requested</td>
<td>Restart due to a user request. The event can be enabled or disabled in &quot;System -&gt; Events&quot; (Cold/Warm Start).</td>
</tr>
</tbody>
</table>

**Messages about file upload or download**

<table>
<thead>
<tr>
<th>Messages</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File upload via HTTP(S): load of FileType &lt;file type&gt; OK -&gt; restart required</td>
<td>Loading the file via HTTP(S) was successful. A restart is required.</td>
</tr>
<tr>
<td>File upload via HTTP(S): load of FileType &lt;file type&gt; OK</td>
<td>Loading the file via HTTP(S) was successful.</td>
</tr>
<tr>
<td>File upload via HTTP(S): validation of FileType &lt;file type&gt; IDENTICAL</td>
<td>Loading the file via HTTP(S) was successful. The file is identical to the existing file.</td>
</tr>
<tr>
<td>File upload via HTTP(S): validation of FileType &lt;file type&gt; FAILED</td>
<td>Loading the file via HTTP(S) failed. The file contains errors or is invalid.</td>
</tr>
</tbody>
</table>
## D.1 Messages in the event log

<table>
<thead>
<tr>
<th>Messages</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File upload via TFTP: load of FileType &lt;file type&gt; OK → restart required</td>
<td>Loading the file using TFTP was successful. A restart is required.</td>
</tr>
<tr>
<td>File upload via TFTP: load of FileType &lt;file type&gt; OK</td>
<td>Loading the file using TFTP was successful.</td>
</tr>
<tr>
<td>File upload via TFTP: validation of FileType &lt;file type&gt; IDENTICAL</td>
<td>Loading the file using TFTP was successful. The file is identical to the existing file.</td>
</tr>
<tr>
<td>File upload via TFTP: validation of FileType &lt;file type&gt; FAILED</td>
<td>Loading the file using TFTP failed. The file contains errors or is invalid.</td>
</tr>
<tr>
<td>File upload via TFTP: file transfer of FileType &lt;file type&gt; FAILED</td>
<td>Loading the file using TFTP failed. The file name is incorrect or the file does not exist on the server.</td>
</tr>
<tr>
<td>File upload via TFTP: file transfer of FileType &lt;file type&gt; failed. Cannot connect to given IP address</td>
<td>Loading the file using TFTP failed. The TFTP server cannot be reached or the settings are incorrect.</td>
</tr>
<tr>
<td>File download via TFTP: file transfer of FileType &lt;file type&gt; failed. Cannot connect to given IP address</td>
<td>Saving the file using TFTP failed. The TFTP server cannot be reached or the settings are incorrect.</td>
</tr>
</tbody>
</table>

## Messages error status

<table>
<thead>
<tr>
<th>Messages</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Fault state: &lt;fault description&gt;</td>
<td>You configure the events in &quot;System &gt; Events&quot;.</td>
</tr>
<tr>
<td>New Fault state: &lt;fault description&gt;</td>
<td>You configure the monitoring of the power supply and the link on the Ethernet port in &quot;System &gt; Fault Monitoring&quot;.</td>
</tr>
<tr>
<td>Fault state gone: &lt;fault description&gt;</td>
<td>Incoming fault.</td>
</tr>
<tr>
<td>Fault state gone: &lt;fault description&gt;</td>
<td>Not all events automatically lead to a fault. On the &quot;Events&quot; WBM page, you specify which events will be logged, for example device restart, changed link on the Ethernet port.</td>
</tr>
<tr>
<td>New Fault state (reconfiguration): &lt;fault description&gt;</td>
<td>Outgoing fault.</td>
</tr>
<tr>
<td>Fault state gone (reconfiguration): &lt;fault description&gt;</td>
<td>The event was triggered due to a change in the configuration.</td>
</tr>
<tr>
<td>Fault state: &lt;fault description&gt; cleared.</td>
<td>Fault was acknowledged by the user.</td>
</tr>
<tr>
<td>Fault state: &lt;fault description&gt; cleared.</td>
<td></td>
</tr>
</tbody>
</table>
### Messages about MSTP

<table>
<thead>
<tr>
<th>Messages</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>You enable or disable the &quot;Spanning Tree&quot; event in &quot;System &gt; Events&quot;</td>
<td>You enable or disable the &quot;Spanning Tree&quot; event in &quot;System &gt; Events&quot;</td>
</tr>
<tr>
<td>Spanning Tree: topology change detected.</td>
<td>The topology of the network has changed; the network will be reorganized.</td>
</tr>
</tbody>
</table>

### Messages about security

<table>
<thead>
<tr>
<th>Messages</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS: Access accepted / rejected for client &lt;MAC&gt;.</td>
<td>The authentication of the client was successful or not successful.</td>
</tr>
</tbody>
</table>

### Messages about message system

<table>
<thead>
<tr>
<th>Messages</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog-Server not reachable!</td>
<td>The configured Syslog server is not accessible.</td>
</tr>
<tr>
<td>Unable to send messages to syslog server.</td>
<td>The syslog server configuration is incomplete.</td>
</tr>
<tr>
<td>Unable to send e-mail(s) because of IP connection failure.</td>
<td>Sending of e-mail(s) failed. SMTP server cannot be reached (e.g. network connection interrupted).</td>
</tr>
<tr>
<td>Unable to send e-mail(s) because of SMTP authentication failure.</td>
<td>Sending of e-mail(s) failed. Authentication of the client on the SMTP server incorrect.</td>
</tr>
<tr>
<td>Unable to send e-mail(s) because SMTP message transfer failed.</td>
<td>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).</td>
</tr>
<tr>
<td>SNMP: Authentication failure.</td>
<td>Authentication of an SNMP client failed; access not possible (e.g. SNMPv1/v2 read-only configured or Read Community String incorrectly configured).</td>
</tr>
<tr>
<td>IP communication is possible. Remote logging activated.</td>
<td>IP communication is possible. Remote logging is activated.</td>
</tr>
<tr>
<td>IP communication is not possible. Remote logging deactivated. Please check IP configuration and network connectivity.</td>
<td>IP communication is not possible. Remote logging is deactivated. Check whether or not the device has an IP address.</td>
</tr>
</tbody>
</table>

### Messages during system startup (PLUG)

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Startup configuration: Internal storage PLUG: Not present</td>
<td>There is no PLUG inserted.</td>
</tr>
<tr>
<td>Startup configuration: Internal storage PLUG: Missing PLUG: License missing</td>
<td>There is no PLUG inserted. There are functions configured on the device for which a license (KEY-PLUG) is required.</td>
</tr>
</tbody>
</table>
### D.1 Messages in the event log

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Startup configuration: Internal storage PLUG: Configuration not accepted PLUG: License missing</td>
<td>Invalid or incompatible configuration on the inserted PLUG. There are functions configured on the device for which a license (KEY-PLUG) is required.</td>
</tr>
<tr>
<td>Startup configuration: Internal storage PLUG: Factory clean → filled with internal configuration PLUG: Configuration accepted PLUG: License accepted</td>
<td>The internal configuration was written successfully to an empty KEY-PLUG.</td>
</tr>
<tr>
<td>Startup configuration: Internal storage PLUG: Factory clean → filled with internal configuration PLUG: Configuration accepted</td>
<td>The internal configuration was written successfully to an empty C-PLUG.</td>
</tr>
<tr>
<td>Startup configuration: PLUG storage PLUG: Configuration accepted PLUG: License accepted</td>
<td>The configuration was loaded successfully from the KEY-PLUG.</td>
</tr>
<tr>
<td>Startup configuration: PLUG storage PLUG: Configuration accepted</td>
<td>The configuration was loaded successfully from the C-PLUG.</td>
</tr>
</tbody>
</table>

#### Messages about PLUG

<table>
<thead>
<tr>
<th>Messages</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>An empty PLUG was found.</td>
<td>There is an empty or formatted PLUG in the device.</td>
</tr>
<tr>
<td>PLUG: Filled PLUG was found. PLUG: Configuration Accepted</td>
<td>There is a valid PLUG with a valid configuration in the device.</td>
</tr>
<tr>
<td>PLUG: Removed at runtime.</td>
<td>The C-PLUG / KEY-PLUG was removed during operation.</td>
</tr>
<tr>
<td>PLUG accepted.</td>
<td>PLUG was accepted.</td>
</tr>
</tbody>
</table>
## D.2 Messages in the WLAN Authentication Log

### Messages in access point mode

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client &lt;MAC address&gt; &lt;system name&gt; associated successfully.</td>
<td>The client has logged in successfully on the access point.</td>
</tr>
<tr>
<td>Client &lt;MAC address&gt; &lt;system name&gt; disassociated with reason &lt;reason description&gt;</td>
<td>The client was logged off from the access point.</td>
</tr>
<tr>
<td>VAP&lt;Num&gt;: Client &lt;MAC&gt; failed to associate; status (&lt;text&gt;)</td>
<td>The connection of the client to the VAP has failed. The reason is displayed as text.</td>
</tr>
<tr>
<td>VAP&lt;Num&gt;: Client &lt;MAC&gt; disassociated with reason (&lt;text&gt;)</td>
<td>The client was successfully disconnected from the VAP. The reason is displayed as text.</td>
</tr>
<tr>
<td>VAP&lt;Num&gt;: Client &lt;MAC&gt; deauthenticated with reason (&lt;text&gt;)</td>
<td>The client was logged off from the AP. The reason is displayed as text.</td>
</tr>
<tr>
<td>VAP&lt;number&gt; Client &lt;MAC&gt; failed to authenticate; status (&lt;status&gt;)</td>
<td>The authentication of the client failed. The reason is displayed as text.</td>
</tr>
<tr>
<td>VAP&lt;Num&gt;: Client &lt;MAC&gt; failed to disassociate; status (&lt;text&gt;)</td>
<td>The connection of the client could not be terminated. The reason is displayed as text.</td>
</tr>
<tr>
<td>VAP&lt;Num&gt;: Client &lt;MAC&gt; associated successfully</td>
<td>The client has connected successfully to the VAP or the client has logged on successfully to the VAP.</td>
</tr>
<tr>
<td>RADIUS: Access rejected for client &lt;MAC&gt;</td>
<td>The RADIUS server denies the client access.</td>
</tr>
<tr>
<td>RADIUS: Access accepted for client &lt;MAC&gt;</td>
<td>The RADIUS server allows the client access.</td>
</tr>
<tr>
<td>WDS Connection is established to AP &lt;MAC&gt;</td>
<td>The WDS connection is successfully established to the access point.</td>
</tr>
<tr>
<td>WDS disconnect from AP &lt;MAC&gt;</td>
<td>The WDS connection to the access point is terminated.</td>
</tr>
</tbody>
</table>

### Messages in client mode

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associated successfully to AP &lt;MAC address&gt; &lt;system name&gt; at channel &lt;channel number&gt; (frequency &lt;frequency&gt; MHz)</td>
<td>The client has logged in successfully on the access point.</td>
</tr>
<tr>
<td>Disassociated from AP &lt;MAC address&gt; &lt;sys name&gt; with reason (Disassociated because sending STA is leaving (or has left) BSS)</td>
<td>The client was logged off from the access point.</td>
</tr>
<tr>
<td>Failed to authenticate to AP &lt;MAC&gt;; status (&lt;Text&gt;)</td>
<td>The authentication of the client with the access point failed. The reason is displayed as text.</td>
</tr>
<tr>
<td>Failed to disassociate from AP &lt;MAC&gt;; status (&lt;Text&gt;)</td>
<td>The connection of the client to the access point could not be terminated. The reason is displayed as text.</td>
</tr>
<tr>
<td>Failed to associate to AP &lt;MAC&gt;; status (&lt;Text&gt;)</td>
<td>The connection of the client to the access point has failed. The reason is displayed as text.</td>
</tr>
</tbody>
</table>
Index

A
Access point
  Overlapping channels, 142
  Overview, 137
  Overview of logged-on clients, 139
  WDS list, 141
AeroScout
  Configuration, 371, 371
  Display configuration, 160
  Status code, 160
Alarm events, 188
Authentication, 204
Available system functions, 44

B
Basic Wizard
  Starting, 80
  System configuration, 85
Bridge priority, 66

C
Client
  Available access points, 148
  Overview, 146
  Client Supplicant, 337
  Collisions, 125
  Communications options, 333
  Configuration mode, 164
C-PLUG, 29
  Formatting, 231
  Saving the configuration, 231
CRC, 125

D
Data transmission speed, 258, 261
  802.11a/b/g, 258
  802.11n, 261
DCP server, 86, 163, 303
DHCP
  Client, 190
DNS client, 169

E
IEEE 802.11n, 24, 251
  Channel bonding, 26
  Frame aggregation, 26
  Guard interval, 26
  Maximum ratio combining, 25
  MIMO, 25
  Spatial multiplexing, 25
iFeatures
  iREF, 56
Information
- ARP table, 111
- Groups, 135
- Inter AP blocking, 136
- Log tables, 112
- Role, 134
- Security, 131, 133
- SNMP, 129, 129
- Spanning Tree, 118
- Start page, 103
- Versions, 108

Inter AP blocking
- Allowed Addresses, 359
- Basic, 358
- Configuration, 357
- Information, 136

IP address
- Assignment with STEP 7, 74

IP mapping, 149

iPCF, 52
- Configuration, 361
- How it works, 52, 52
- PNIO communication, 52
- Restriction, 54

iPCF-MC
- PNIO communication, 52

iPRP
- Configuration, 368

iREF, 55
- Client list, 157
- Configuration, 367
- WDS list, 159

J
- Jabbers, 125

K
- KEY-PLUG, 29, 229, 232, 232
  - Formatting, 231

L
- Layer 3, 232, 232
- Line monitoring, 188
- LLDP, 304
- Local users, 314
- Location, 166
- Log tables
  - WLAN authentication log, 115

Logging on
- via HTTP, 78
- via HTTPS, 78

Logout
- Automatic, 220

M
- MAC ACL, 340, 341
  - Configuration, 341, 343
- Maintenance data, 110
- MSTP, 299
  - Port, 295
  - Port parameters, 301
- MSTP instance, 301, 301
- Multichannel configuration, 18
- Multiple Spanning Tree, 295, 299

N
- NAPT, 62
  - Configuration, 308
- NAT, 62
  - Configuring, 306
- Negotiation, 236
- Network access, 20
- NTP
  - Client, 216

O
- Order number, 110
- Oversize, 125
- Overview
  - Access point, 137
  - Available access points, 148
  - Clients, 146
  - Logged-on clients, 139
  - Overlap APs, 142
  - Overlapping channels, 142
  - WDS partner, 141

P
- Packet error statistics, 125
- Password, 317
  - Options, 319
- Ping, 234
Index

PLUG, 232, 232
  C-PLUG, (C-PLUG)
  KEY-PLUG, (KEY-PLUG)
point-to-point, 67
Port
  Port configuration, 235, 238
Port configuration, 238
Power supply
  Monitoring, 222
PROFINET, 49, 225
PROFINET IO, 49
PST tool, 303

R
RADIUS, 323
Reboot, 171
Redundant networks, 293
Reset, 171
RFC
  RFC 1518, 69
Roles, 310
Root bridge, 66
Rule, 340, 341, 345
  Configuration, 345
  Egress, 343, 345
  Ingress, 341, 345
  IP ACL, 345

S
Scope of the manual, 9
Security settings, 201
Serial number, 110
SHA algorithm, 201
Signal recorder, 269
SIMATIC NET glossary, 11
SMTP
  Client, 163
SNMP, 63, 86, 163, 198, 201
  Groups, 201
  Overview, 129
  SNMPv1, 63
  SNMPv2cc, 63
  SNMPv3, 63
  Trap, 200
  Users, 203
Software version, 110
Spanning Tree
  Information, 118
  Rapid Spanning Tree, 67
Spectrum analyzer, 277
SSH
  Server, 162
Standalone configuration, 16
Start page, 103
STEP 7, 303
Subnet mask, 69
Syslog, 221
  Client, 163
System
  Configuration, 162
  General information, 165
System event log
  Agent, 221
System events
  Configuration, 185
  Severity filter, 187

T
Telnet
  Server, 162
TFTP
  Load/save, 180
Time, 163
Time of day
  Manual setting, 206
  SIMATIC Time Client, 218
  SNTP (Simple Network Time Protocol), 213
  System time, 206
  Time zone, 215
  Time-of-day synchronization, 213
  UTC time, 215
Time setting, 163

U
Undersize, 125
User Groups, 312

V
Vendor, 110
Vendor ID, 110
VLAN, 50
  Port VID, 289
  Priority, 289
  Tag, 289
Index

W
WDS, 256
Web Based Management, 75
  Requirement, 75
Wireless access, 17
WLAN statistics
  Bad frames, 151
  Received frames, 155
  Sent frames, 156