

SIMATIC NET

Industrial Remote Communication Remote Networks SCALANCE M-800 and RUGGEDCOM RM1224 Web Based Management V8.2

Configuration Manual

Introduction	1
Security recommendation	2
Description	3
Technical basics	4
Configuring with Web Based Management	5
Upkeep and maintenance	6
Appendix A "SMS command"	A
Appendix B "Syslog messages"	B
Appendix C "Encryption methods used (ciphers)"	C
Appendix D "Permitted characters in names, passwords and descriptions"	D

Legal information

Warning notice system

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

DANGER

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

WARNING

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

CAUTION

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

NOTICE

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

WARNING

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

Trademarks

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

Disclaimer of Liability

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

Table of contents

1	Introduction	11
1.1	Purpose of the configuration manual.....	11
1.2	Scope of validity	11
1.3	Supplementary documentation	11
1.4	Further documentation	12
1.5	Service & Support	13
1.6	Training	13
1.7	New in this version	14
1.8	Symbols used	15
1.9	Designations used.....	16
1.10	SIMATIC NET glossary.....	17
1.11	Cybersecurity information	17
1.12	Error/fault	17
1.13	Decommissioning	17
1.14	Recycling and disposal	18
1.15	Firmware	18
1.16	Open source license conditions (SCALANCE MUx85x).....	18
1.17	Open source license conditions (SCALANCE M-800)	19
1.18	Trademarks.....	19
2	Security recommendation	21
2.1	Security recommendations.....	21
2.2	Available services.....	26
3	Description.....	31
3.1	Function	31
3.2	Configuration examples	33
3.2.1	Overview	33
3.2.2	SCALANCE MUM856/M81x as Internet access	33
3.2.3	Direct communication of stations.....	35
3.2.4	Telecontrol via the mobile wireless network.....	36
3.2.5	Telecontrol via dedicated line	37
3.2.6	Mobile access to plants and plant sections.....	38
3.2.7	Plant access via a remote maintenance center	40
3.2.8	TeleControl with SINEMA RC.....	41
3.3	Requirements for operation.....	42

3.3.1	For operation with MUB852	42
3.3.2	For operation with MUM853	44
3.3.3	For operation with MUM856	46
3.3.4	For operation with M87x / RM1224	49
3.3.5	For operation with M81x.....	50
3.3.6	For operation with M826	51
3.3.7	For operation with M804PB.....	53
3.3.8	Use in a PROFINET environment	53
3.3.9	TIA Portal Cloud Connector	54
3.4	Configuration limits for WBM and CLI.....	54
3.5	Configuration limits for SINEMA RC.....	56
3.6	Hardware equipment and system functions	57
3.7	PLUG	60
3.7.1	PLUG	60
3.7.2	PRESET PLUG.....	63
4	Technical basics	65
4.1	IP addresses	65
4.1.1	IPv4 / IPv6	65
4.1.2	IPv4 address.....	66
4.1.2.1	Structure of an IPv4 address	66
4.1.2.2	Initial assignment of an IPv4 address	68
4.1.2.3	Address assignment via DHCPv4	68
4.1.2.4	Address assignment with SINEC PNI.....	69
4.1.2.5	Address assignment with STEP 7	69
4.1.3	IPv6 address.....	70
4.1.3.1	IPv6 terms	70
4.1.3.2	Structure of an IPv6 address	71
4.2	VLAN	73
4.2.1	VLAN	73
4.2.2	VLAN tagging	74
4.3	VXLAN.....	76
4.4	SNMP	78
4.5	ICMP.....	80
4.6	Security functions	82
4.6.1	Adapting the MTU for IPsec VPN and SINEMA RC.....	82
4.6.2	User management	82
4.6.3	Firewall.....	84
4.6.3.1	Firewall rules	86
4.6.4	NAT	88
4.6.5	NAT and firewall.....	89
4.6.6	Certificates.....	91
4.6.7	VPN	92
4.6.7.1	IPsec VPN.....	92
4.6.7.2	OpenVPN.....	95
4.6.7.3	VPN connection establishment.....	96
4.7	Redundancy.....	102

4.7.1	Spanning Tree.....	102
4.7.1.1	RSTP	103
4.7.2	VRRPv3	103
5	Configuring with Web Based Management.....	105
5.1	Web Based Management.....	105
5.2	Starting and logging in	106
5.3	Updating the HTTPS certificate	110
5.4	"Wizard" menu	111
5.4.1	Basic Wizard.....	111
5.4.2	IP.....	113
5.4.3	Device	114
5.4.4	DSL.....	115
5.4.5	SHDSL	117
5.4.6	SIM.....	119
5.4.7	Operator.....	122
5.4.8	Time setting	125
5.4.9	DDNS.....	127
5.4.10	SINEMA RC.....	128
5.4.11	Cloud Connector	131
5.4.12	Summary.....	133
5.5	"Information" menu	135
5.5.1	Start Page	135
5.5.2	Dashboard	140
5.5.3	Versions.....	142
5.5.4	Identification & Maintenance.....	143
5.5.5	ARP / neighbors.....	145
5.5.5.1	ARP-Table	145
5.5.5.2	IPv6 Neighbor Table	146
5.5.6	Log Tables	147
5.5.6.1	Event Log	147
5.5.6.2	Security Log.....	149
5.5.6.3	Firewall Log	151
5.5.7	Faults	152
5.5.8	DHCP Server	153
5.5.9	Diagnostics	154
5.5.10	SNMP	156
5.5.11	Ethernet Statistics	156
5.5.11.1	Interface statistics.....	157
5.5.11.2	Packet Size.....	158
5.5.11.3	Packet Type.....	159
5.5.11.4	Packet Error	159
5.5.12	Learning Table	160
5.5.13	LLDP	161
5.5.14	IPv4 Routing	162
5.5.15	IPv6 Routing	163
5.5.16	Mobile	164
5.5.16.1	Overview	164
5.5.16.2	Signal Recorder.....	167
5.5.16.3	Data usage	168

5.5.16.4	Network Scan	170
5.5.17	DSL.....	171
5.5.17.1	Overview	171
5.5.17.2	DSL Data Rate	173
5.5.17.3	Streams	173
5.5.18	SHDSL	175
5.5.19	IPsec VPN.....	176
5.5.20	SINEMA RC.....	177
5.5.21	OpenVPN.....	179
5.5.21.1	Client.....	179
5.5.21.2	Server.....	180
5.5.22	Redundancy.....	181
5.5.22.1	Overview	181
5.5.22.2	Spanning Tree.....	183
5.5.23	VRRPv3 Statistics	186
5.5.24	Security	188
5.5.24.1	Overview	188
5.5.24.2	Supported Function Rights	191
5.5.24.3	Roles	191
5.5.24.4	Groups	192
5.5.25	VXLAN.....	193
5.5.26	System Time	194
5.5.27	Firewall Monitoring.....	196
5.6	"System" menu	197
5.6.1	Configuration.....	197
5.6.2	General	203
5.6.2.1	Device	203
5.6.2.2	Coordinates	205
5.6.3	Restart.....	208
5.6.3.1	Restart.....	208
5.6.3.2	Sleep Mode.....	210
5.6.4	Load&Save.....	212
5.6.4.1	File list.....	212
5.6.4.2	HTTP	216
5.6.4.3	TFTP	220
5.6.4.4	SFTP	224
5.6.4.5	Passwords.....	228
5.6.5	Events	230
5.6.5.1	Event Configuration	230
5.6.5.2	Severity Filters	235
5.6.6	SMTP client.....	236
5.6.6.1	General	236
5.6.6.2	Recipient	238
5.6.7	SNMP	240
5.6.7.1	General	240
5.6.7.2	SNMPv3 Users.....	242
5.6.7.3	SNMPv3 User to Group mapping	245
5.6.7.4	SNMPv3 Access.....	246
5.6.7.5	SNMPv3 Views.....	248
5.6.7.6	Notifications	250
5.6.8	System Time	252
5.6.8.1	Manual Setting	252

5.6.8.2	Protocol Switchover	254
5.6.8.3	DST Overview	255
5.6.8.4	DST Configuration	257
5.6.8.5	Mobile Time.....	260
5.6.8.6	SNTP Client.....	261
5.6.8.7	NTP Client.....	265
5.6.8.8	SIMATIC Time Client	269
5.6.8.9	NTP Server	270
5.6.9	Auto Logout.....	272
5.6.10	Button	273
5.6.11	Syslog Client.....	274
5.6.12	Fault Monitoring	276
5.6.12.1	Power Supply	276
5.6.12.2	Link Change.....	277
5.6.12.3	Mobile wireless	278
5.6.13	PLUG	279
5.6.13.1	Configuration.....	279
5.6.13.2	License	283
5.6.14	Ping.....	285
5.6.15	DCP Discovery.....	286
5.6.16	SMS.....	288
5.6.16.1	General	288
5.6.16.2	Event SMS	289
5.6.16.3	SMS Command	292
5.6.16.4	SMS Relay (Outgoing)	293
5.6.16.5	SMS Relay (Incoming)	295
5.6.16.6	Send SMS messages.....	297
5.6.17	DNS.....	299
5.6.17.1	DNS client.....	299
5.6.17.2	DNS Proxy.....	300
5.6.17.3	DDNS client	300
5.6.17.4	DNS record	302
5.6.18	DHCPv4	303
5.6.18.1	DHCP Client	303
5.6.18.2	DHCP Server	306
5.6.18.3	DHCP options.....	308
5.6.18.4	Static Leases	310
5.6.19	cRSP / SRS	312
5.6.20	Proxy Server.....	313
5.6.21	SINEMA RC.....	314
5.6.22	TIA Portal Cloud Connector	319
5.6.23	Connection Check.....	321
5.6.23.1	Connection Fallback.....	323
5.6.24	Configuration Backup.....	323
5.6.25	TCP event.....	324
5.6.26	GPS	328
5.6.26.1	Coordinates	328
5.6.26.2	Geofencing.....	330
5.6.27	iperf	332
5.7	"Interfaces" menu	334
5.7.1	Ethernet	334
5.7.1.1	Configuration.....	336

5.7.2	Mobile wireless	338
5.7.2.1	General	338
5.7.2.2	SIM	343
5.7.2.3	Mobile wireless provider	345
5.7.2.4	Band rejection filter	347
5.7.2.5	eSIM profile	348
5.7.2.6	SIM switchover	353
5.7.2.7	Tx Power Reduction	355
5.7.2.8	Modem diagnostics	356
5.7.2.9	Connection Check	357
5.7.3	DSL	359
5.7.4	SHDSL	361
5.7.4.1	Overview	361
5.7.4.2	Configuration	363
5.7.4.3	Connection Check	366
5.7.5	Packet Capture	367
5.8	"Layer 2" menu	370
5.8.1	Layer 2 configuration	370
5.8.2	VLAN	371
5.8.2.1	General	371
5.8.2.2	Port Based VLAN	375
5.8.3	VXLAN	376
5.8.3.1	VXLAN	376
5.8.3.2	VTEP	378
5.8.3.3	VLAN mapping	379
5.8.3.4	Ingress Replication	380
5.8.3.5	Static MAC	381
5.8.4	Dynamic MAC Aging	382
5.8.5	Spanning Tree	383
5.8.5.1	General	383
5.8.5.2	ST general	384
5.8.5.3	ST port	385
5.8.6	LLDP	389
5.9	Menu "Layer 3 (IPv4)"	391
5.9.1	Static routes	391
5.9.2	Subnets	393
5.9.2.1	Overview	393
5.9.2.2	Configuration	395
5.9.3	NAT	396
5.9.3.1	NAT General	396
5.9.3.2	Masquerading	397
5.9.3.3	NAPT	397
5.9.3.4	Source NAT	399
5.9.3.5	NETMAP	401
5.9.4	VRRPv3	405
5.9.4.1	Router	405
5.9.4.2	Configuration	407
5.9.4.3	Address overview	409
5.9.4.4	Address Configuration	410
5.9.4.5	Interface Tracking	411
5.9.4.6	Address monitoring	412

5.10	Menu "Layer 3 (IPv6)"	414
5.10.1	Subnets	414
5.10.2	NAT	417
5.10.2.1	Masquerading.....	417
5.11	"Security" menu	418
5.11.1	Users	418
5.11.1.1	Local users.....	418
5.11.1.2	Roles	421
5.11.1.3	Groups	423
5.11.2	Passwords.....	424
5.11.2.1	Options	426
5.11.2.2	Two-factor authentication	427
5.11.3	AAA.....	429
5.11.3.1	General	429
5.11.3.2	RADIUS Client	430
5.11.4	Certificates.....	433
5.11.4.1	Overview	433
5.11.4.2	Certificates.....	435
5.11.5	Firewall.....	438
5.11.5.1	General	438
5.11.5.2	Predefined	439
5.11.5.3	Dynamic Rules	442
5.11.5.4	IP services.....	446
5.11.5.5	ICMP services.....	447
5.11.5.6	IP protocols.....	448
5.11.5.7	IP rules	449
5.11.5.8	Predefined MAC rules	453
5.11.5.9	MAC services	454
5.11.5.10	MAC rules	456
5.11.6	IPsec VPN.....	458
5.11.6.1	General	458
5.11.6.2	Remote End	459
5.11.6.3	Connections	461
5.11.6.4	Authentication.....	465
5.11.6.5	Phase 1.....	466
5.11.6.6	Phase 2.....	468
5.11.7	OpenVPN.....	471
5.11.7.1	General	471
5.11.7.2	Connections	472
5.11.7.3	Local client	475
5.11.7.4	Authentication.....	476
5.11.7.5	Server.....	477
5.11.7.6	Remote client.....	478
5.11.7.7	Remote client subnet	478
5.11.8	Brute Force Prevention.....	479
6	Upkeep and maintenance.....	483
6.1	Device configuration with PRESET-PLUG.....	483
6.2	Firmware update - via WBM.....	485
6.3	Firmware update via WBM and CLI not possible	486

6.4	Restoring the factory settings.....	488
A	Appendix A "SMS command"	489
A.1	Command SMS message	489
B	Appendix B "Syslog messages"	493
B.1	Format of the syslog messages.....	493
B.2	Parameters in Syslog messages	494
B.3	Syslog messages	495
C	Appendix C "Encryption methods used (ciphers)"	505
C.1	SSL	505
C.2	OpenVPN.....	506
C.3	SINEMA RC.....	507
C.4	cSRP	507
C.5	SSH CLI	508
C.6	SNMP	509
C.7	RADIUS	510
C.8	IPsec.....	510
D	Appendix D "Permitted characters in names, passwords and descriptions".....	513
D.1	Permitted characters	513
	Index	517

Introduction

1.1 Purpose of the configuration manual

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

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

1.2 Scope of validity

This Configuration Manual covers the following products:

- SCALANCE M804PB
- SCALANCE M812-1
- SCALANCE M816-1
- SCALANCE M826-2
- SCALANCE M874-2
- SCALANCE M874-3
- SCALANCE M876-3
- SCALANCE M876-4
- SCALANCE MUB852-1
- SCALANCE MUM853-1
- SCALANCE MUM856-1
- RUGGEDCOM RM1224

This Configuration Manual is valid for the following firmware version:

- SCALANCE M800 / S615 firmware as of version V8.2

1.3 Supplementary documentation

Documentation on the Internet

You can find the current version of the documents on the Internet at (<https://support.industry.siemens.com/cs/ww/en/ps/15982/man>)

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

Orientation in the documentation

Apart from the Configuration Manual you are currently reading, the following documentation is also available on the topic of remote network:

- **Configuration Manual: SCALANCE M-800 Command Line Interface**
This document contains the CLI commands supported by SCALANCE M-800 devices.
- **Getting Started**
Based on examples, these documents explain the configuration of the SCALANCE M-800/ S615.
- **Operating instructions**
These documents contains information on installing, connecting, maintaining and servicing the following products.

Operating instructions	Products
SCALANCE M804PB	SCALANCE M804PB
SCALANCE M874, M876	SCALANCE M874-2 SCALANCE M874-3 SCALANCE M876-3 SCALANCE M876-4
SCALANCE M812, M816	SCALANCE M812-1 SCALANCE M816-1
SCALANCE M826	SCALANCE M826-2
SCALANCE MUM856-1	SCALANCE MUM856-1
SCALANCE MUM853-1	SCALANCE MUM853-1
RUGGEDCOM RM1224	RUGGEDCOM RM1224

- **Operating Instructions SINEMA RC Server**
You will find this document on the Internet pages of Siemens Industry Online Support. It contains information on the installation, configuration and operation of the application SINEMA Remote Connect Server.
- **IP-based remote networks**
In this document, the possible configurations of an IP-based remote network are explained in an overview with the requirements and a link to detailed configuration instructions. You will find this document on the Internet under the following entry ID: 26662448 (<https://support.industry.siemens.com/cs/ww/de/view/26662448>)
- **Introduction to Industrial Remote Communication**
In this entry, you can find an overview - arranged by topic - with links to the most important entries on Industrial Remote Communication in the Siemens Industry Online Support. You can find this entry under the following entry ID: 64721753 (<https://support.industry.siemens.com/cs/ww/en/view/64721753>)

1.4 Further documentation

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

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

You will find the system manuals on the Internet pages of Siemens Industry Online Support under the following entry IDs:

- 27069465 (<https://support.industry.siemens.com/cs/de/en/view/27069465>)
Industrial Ethernet / PROFINET Industrial Ethernet System Manual
- 84922825 (<https://support.industry.siemens.com/cs/de/en/view/84922825>)
Industrial Ethernet / PROFINET - Passive network components System Manual

1.5 Service & Support

Industry Online Support

In addition to the product documentation, you are supported by the comprehensive online information platform of Siemens Industry Online Support at the following Internet address:

Link: (<https://support.industry.siemens.com/cs/de/en/>)

Apart from news, there you will also find:

- Project information: Manuals, FAQs, downloads, application examples etc.
- Contacts, Technical Forum
- The option submitting a support query:
Link: (<https://support.industry.siemens.com/cs/my?lc=en-WW>)
- Our service offer:
Right across our products and systems, we provide numerous services that support you in every phase of the life of your machine or system - from planning and implementation to commissioning, through to maintenance and modernization.

You will find contact data on the Internet at the following address:

Link: (https://www.automation.siemens.com/aspa_app/?ci=yes&lang=en)

1.6 Training

SITRAIN - Training for Industry

The training offer includes more than 300 courses on basic topics, extended knowledge and special knowledge as well as advanced training for individual sectors - available at more than 130 locations. Courses can also be organized individually and held locally at your location.

You will find detailed information on the training curriculum and how to contact our customer consultants at the following Internet address:

Link: (<https://new.siemens.com/global/en/products/services/industry/sitrain/personal.html>)

Industrial Networks Education

Training and certification for Industrial Networks

In our Industrial Networks Education courses you'll learn to design and implement wired and wireless data networks and connect them to a corporate network. You will also receive instruction on how to secure, diagnose and optimize communication networks. Certification can also be offered to supplement almost all training courses.

Link: (<https://www.siemens.com/industrial-networks-education>)

1.7 New in this version

Below, you will find an overview of the most important function extensions:

- Information > OpenVPN server (Page 180)
- System > Configuration: Cache write cycle time (Page 197)
- System > Configuration: Checksum for the configuration file (Page 197)
- System > System Time > NTP secure: Support of the hash algorithm SHA256 (Page 265)
- System > DNS client: DNSSec (Page 299)
- System > SNMP > SNMPv3 users: Support of the hash algorithm SHA256 (Page 242)
- System > SINEMA RC: Alternative SINEMA RC address (Page 314)
- Security > AAA > RADIUS client: Support of the "Message Authenticator" attribute (Page 430)
- Security > Firewall > Predefined: Access to the device via OpenVPN (Page 439)
- Security > Firewall > IP rules: Support of FQDN (Page 449)
- Security > OpenVPN > Configuration option of an OpenVPN server (Page 477)

The following new functions are only available with SCALANCE MUM85x and SCALANCE MUB852:

- Information > Diagnostics (Page 154)
- Information > Ethernet Statistics (Page 156)
- Interfaces > Mobile: Extension by IP Passthrough (Page 338)

The new configuration page is available for the devices 6GK5856-2EA10-3BA1 (B1), 6GK5853-2EA10-2BA1 (B1) and 6GK5852-1EA10-1BA1 (B1):

- Interfaces > Mobile > Band rejection filter (Page 347)

The existing system function is enabled as of V8.2 for the devices 6GK5856-2EA10-3BA1 (B1) and 6GK5853-2EA10-2BA1 (B1):

- Interfaces > Mobile > Modem diagnostics (Page 356)

On the devices without PLUG slot, e.g. SCALANCE M826 and SCALANCE MUB852, the SINEMA RC Server service is available as of V8.2 with license. The license is made available in SINEMA RC Server.

The following devices are introduced with V8.2:

Device	Article number
SCALANCE MUB852-1	6GK5852-1EA10-1AA1 (A1)
	6GK5852-1EA10-1BA1 (B1)

See also

Layer 2 configuration (Page 370)

1.8 Symbols used

The symbols used in this manual have the following meaning:

MUM85x (Only with MUM85x)	The section/paragraph/parameter described is only relevant for SCALANCE MUM85x.
MUx85x (Only with MUx85x)	The section/paragraph/parameter described is only relevant for SCALANCE MUM85x and MUB852.
MUB852 (Only with MUB852)	The section/paragraph/parameter described is only relevant for SCALANCE MUB852.
~~MUB852~~ (not for MUB852)	The section/paragraph/parameter described is not relevant for SCALANCE MUB852.
M87x RM1224 or (only with M87x / RM1224)	The section/paragraph/parameter described is only relevant for SCALANCE M874-2 / M874-3 / M876-3 / M876-4 and RUGGED-COM1224.
(not with M874-2)	The parameter described is not relevant for SCALANCE M874-2.
(only with M876-4)	The parameter described is relevant only for SCALANCE M876-4.
M81x	The section/paragraph/parameter described is only relevant for SCALANCE M812-1 / M816-1.
M826	The section/paragraph/parameter described is only relevant for SCALANCE M826-2.
~~M812~~	The section/paragraph/parameter described is not relevant for SCALANCE M812-1.
~~M826~~	The section/paragraph/parameter described is not relevant for SCALANCE M826.
M804PB	The section/paragraph/parameter described is relevant for SCALANCE M804PB.
~~M804PB~~	The section/paragraph/parameter described is not relevant for SCALANCE M804PB.

1.9 Designations used

Abbreviations used

The information in the Configuration Manual 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.

The designation . . . stands for . . .	Product name
M-800	SCALANCE M874-2 SCALANCE M874-3 SCALANCE M876-3 SCALANCE M876-4 SCALANCE M812-1 SCALANCE M816-1 SCALANCE M826-2 SCALACNE M804PB SCALANCE MUB852 SCALANCE MUM856 SCALANCE MUM853
MUB852	SCALANCE MUB852-1
MUM853	SCALANCE MUM853-1
MUM856	SCALANCE MUM856-1
MUM85x	SCALANCE MUM856-1 SCALANCE MUM853-1
MUx85x	SCALANCE MUM856-1 SCALANCE MUM853-1 SCALANCE MUB852-1
M804PB	SCALACNE M804PB
M812	SCALANCE M812-1
M816	SCALANCE M816-1
M81x	SCALANCE M812-1 SCALANCE M816-1
M826	SCALANCE M826-2
M874-2	SCALANCE M874-2
M874-3	SCALANCE M874-3
M876-3	SCALANCE M876-3
M876-4	SCALANCE M876-4
M87x	SCALANCE M874-2 SCALANCE M874-3 SCALANCE M876-3 SCALANCE M876-4
RM1224	RUGGEDCOM RM1224

1.10 SIMATIC NET glossary

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

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

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

1.11 Cybersecurity information

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

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

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

For additional information on industrial cybersecurity measures that may be implemented, please visit

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

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

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under

<https://new.siemens.com/cert> (<https://www.siemens.com/cert>).

1.12 Error/fault

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

1.13 Decommissioning

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

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

Also restore the factory settings on the storage medium.

1.14 Recycling and disposal



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

Do not dispose of the products at public disposal sites.

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

Note the different national regulations.

1.15 Firmware

The firmware is available on the Internet pages of the Siemens Industry Online Support: (<https://support.industry.siemens.com/cs/ww/en/ps/28821/dl>)

Note on firmware/software support

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

1.16 Open source license conditions (SCALANCE MUX85x)

Note

Open source software

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

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

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

See also

Load&Save (Page 212)

1.17 Open source license conditions (SCALANCE M-800)

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-M-800-S615-RM1224_86.pdf

1.18 Trademarks

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

SCALANCE, SINEMA, KEY-PLUG, C-PLUG

RUGGEDCOM

Security recommendation

2.1 Security recommendations

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

Note

Note that GNSS signals can be obfuscated or blocked by malicious third-party devices.

General

- Check the device regularly to ensure that these recommendations and/or other internal security policies are complied with.
- Evaluate the security of your location and use a cell protection concept with suitable products. For more information, refer to:
Link: (<https://www.siemens.com/industrialsecurity>)
- When the internal and external network are disconnected, an attacker cannot access internal data from the outside. If possible, operate the device only within a protected network area.
- Use VPN to encrypt and authenticate communication from and to the devices.
- For data transmission via a non-secure network, use an encrypted VPN tunnel (IPsec, OpenVPN).
- Check the user documentation of other Siemens products that are used together with the device for additional security recommendations.
- Using remote logging, ensure that the system protocols are forwarded to a central logging server. Make sure that the server is within the protected network and check the protocols regularly for potential security violations or vulnerabilities.

Authentication

Note**Accessibility risk - Risk of data loss**

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

- Replace the default passwords for all user accounts, access modes and applications (if applicable) before you use the device. Create a separate user account for each user that will receive access to the device.
- Define rules for the assignment of passwords.

2.1 Security recommendations

- Use passwords with a high password strength. Avoid weak passwords, (e.g. Passwort1, 123456789, abcdefgh) or recurring characters (e.g. abcabc).
This recommendation also applies to symmetrical passwords/keys configured on the device.
- Make sure that passwords are protected and only disclosed to authorized personnel.
- Do not use the same passwords for multiple user names and systems.
- Store the user account details in a safe location to have them available if they are lost. You can use password managers or encrypted files/drives for this purpose.
- A password must be changed if it is known or suspected to be known by unauthorized persons.
- When user authentication is performed via RADIUS, make sure that all communication takes place within the security environment or is protected by a secure channel. Use a RADIUS connection with changing passwords, expiry time, etc.
- Watch out for link layer protocols that do not offer their own authentication between endpoints, such as ARP. An attacker could use vulnerabilities in these protocols to attack hosts, switches and routers connected to your layer 2 network, for example, through manipulation (poisoning) of the ARP caches of systems in the subnet and subsequent interception of the data traffic. Appropriate security measures must be taken for non-secure layer 2 protocols to prevent unauthorized access to the network. Physical access to the local network can be secured or secure, higher layer protocols can be used, among other things.
- Use TOTP-based two-factor authentication of the user. You can find more information on this under "Security > Passwords > Two-Factor Authentication".

Certificates and keys

- There is a pre-installed Web server certificate and an SSH Private Key in the device. Replace this certificate with a user-generated, high-quality certificate with key. Use a certificate signed by a reliable external or internal certification authority. You can install the certificate in the WBM via "System > Load & Save".
- Use the certification authority including key revocation and management to sign the certificates.
- Use password-protected certificates in the format "PKCS #12".
- Use certificates with a key length of 4096 bits.
- Update certificates every three months.
- Make sure that user-defined private keys are protected and inaccessible to unauthorized persons.
- If there is a suspected security violation, change all certificates and keys immediately.
- SSH and SSL keys are available for admin users. Make sure that you take appropriate security measures when shipping the device outside of the trusted environment:
 - Reset the device to the factory settings. Replace the SSH and SSL keys with disposable keys prior to shipping to Siemens.
 - Decommission the existing SSH and SSL keys. Create and program new keys when the device is returned.

- Verify certificates based on the fingerprint on the server and client side to prevent "man in the middle" attacks. Use a second, secure transmission path for this.
- Before sending the device to Siemens for repair, reset it to factory settings and replace the current certificates and keys with temporary throwaway certificates and keys that can be destroyed when the device is returned.

Physical/remote access

- If possible, operate the devices only within a protected network area. Attackers cannot access internal data from the outside when the internal and the external network are separate from each other.
- Limit physical access to the device exclusively to trusted personnel.
The memory card or the PLUG (C-PLUG, KEY-PLUG, CLP) contains sensitive data such as certificates and keys that can be read out and modified. An attacker with control of the device's removable media could extract critical information such as certificates, keys, etc. or reprogram the media.
- Lock unused physical ports on the device. Unused ports can be used to gain forbidden access to the plant.
- We highly recommend that you keep the protection from brute force attacks (BFA) activated to prevent third parties from gaining access to the device. For more information, see the configuration manuals, section "Brute Force Prevention (Page 479)".
- If possible, use the VPN functionality to encrypt and authenticate communication for communication via non-secure networks.
- When you establish a secure connection to a server (for example for an upgrade), make sure that strong encryption methods and protocols are configured for the server.
- Terminate the management connections (e.g. HTTPS, SSH) properly.
- Make sure that the device has been powered down completely before you decommission it. For more information, refer to "Decommissioning (Page 17)".
- We recommend formatting a PLUG that is not being used.

Hardware / Software

- Use VLANs whenever possible as protection against denial-of-service (DoS) attacks and unauthorized access.
- Restrict access to the device using firewall rules.
- Selected services are enabled by default in the firmware. It is recommended to enable only the services that are absolutely necessary for your installation.
For more information on available services, see "List of available services (Page 26)".
- To ensure you are using the most secure encryption methods available, use the latest web browser version compatible with the product. Also, the latest web browser versions of Mozilla Firefox, Google Chrome, and Microsoft Edge have 1/n-1 record splitting enabled, which reduces the risk of attacks such as SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (for example, BEAST).

2.1 Security recommendations

- Ensure that the latest firmware version is installed, including all security-related patches. You can find the latest information on security patches for Siemens products at the Industrial Security (<https://www.siemens.com/industrialsecurity>) or ProductCERT Security Advisories (<https://www.siemens.com/cert/en/cert-security-advisories.htm>) website. For updates on Siemens product security advisories, subscribe to the RSS feed on the ProductCERT Security Advisories website or follow @ProductCert on Twitter.
- Enable only those services that are used on the device, including physical ports. Free physical ports can potentially be used to gain access to the network behind the device.
- Use the authentication and encryption mechanisms of SNMPv3 if possible. Use strong passwords.
- Configuration files can be downloaded from the device. Ensure that configuration files are adequately protected. Configuration files can be password protected during download. You enter passwords on the WBM page "System > Load & Save > Passwords (Page 228)".
- When using SNMP (Simple Network Management Protocol):
 - Configure SNMP to generate a notification when authentication errors occur. For more information, see WBM "System > SNMP > Notifications (Page 250)".
 - Ensure that the default community strings are changed to unique values.
 - Use SNMPv3 whenever possible. SNMPv1 and SNMPv2c are considered non-secure and should only be used when absolutely necessary.
 - If possible, prevent write access.
- The names of the configuration files can be changed. To improve security, do not use spaces in the TFTP file name.

Secure/non-secure protocols

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

- Check whether use of the following protocols is necessary:
 - Telnet
 - HTTP
 - Broadcast pings
 - Non authenticated and unencrypted interfaces
 - ICMP (redirect)
 - LLDP
 - DHCP Options 66/67
 - SNMP
 - NTP
 - TFTP
 - TIA Portal Cloud Connector (not available with SCALANCE MUX85x)
 - VRRPv3
 - DNS
 - SNMPv1/V2c
- If a secure alternative is available for a protocol, use it.
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.
 - HTTP → HTTPS
 - Telnet → SSH
 - NTP → Secure NTP
 - TFTP → SFTP
 - TIA Portal Cloud Connector using a secure connection (not available with SCALANCE MUX85x). Use the "TIA Portal Cloud Connector" integrated in the product over a VPN solution (e.g. SINEMA RC).
Configure the firewall settings of the SCALANCE M800/S615 (e.g. predefined IPv4 rules "Cloud Connector" to prevent unauthorized access of network devices to the "TIA Portal Cloud Connector Server").
 - DNS > DNSSec
- Using a firewall, restrict the services and protocols available to the outside to a minimum.
- Select a trusted DNS provider.
Enable the DNSSec option on the WBM page "System > DNS client" or with the CLI command `dnssec`.

- SCALANCE MUM85x, SCALANCE M87x and RUGGEDCOM RM1224:
For command SMS, use the identifier to secure your SMS messages. You can set a configurable value for a SCALANCE M device that, in addition to the phone number, must match the received identifier of the SMS. You configure the identifier on the WBM page "System > SMS > SMS Command (Page 292)" or with the CLI commands `sms-cmd idx identifier` and `sms-cmd sender`.
- The TCP Diagnostics Stream is considered non-secure without encryption. As of V8.1, encryption that enables secure use in productive operation is supported. Enable encryption of the function to use it securely.
- Only use the TCP Event function in secured networks or VPN. The firewall must be activated beforehand.
- With authentication on the RADIUS server and RADIUS client, use the Message Authenticator attribute to check packets.

2.2 Available services

List of available services

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

The table includes the following columns:

- **Service**
The services that the device supports.
- **Protocol / Port number**
Port number assigned to the protocol.
- **Default port status**
The port status on delivery (factory setting) distinguishes between local and external access.
 - Local access: The port is accessed via a local connection (vlan1).
 - External access: The port is accessed via an external connection (vlan2).
- **Configurable port/service**
Indicates whether the port number or the service can be configured via WBM / CLI.
- **Authentication**
Specifies whether an authentication of the communication partner takes place or whether an authentication can be configured.
- **Encryption**
Specifies whether the transfer is encrypted or whether the encryption can be configured.

Service	Protocol/ Port number	Default port status		Configurable		Authentica- tion	Encryption ²⁾
		Local access	External access ¹⁾	Port	Service		
DHCPv4 Client	UDP/68	Closed ³⁾	Closed	--	✓	--	--
DHCPv6 Client	TCP/546 UDP/546	Open	Open	--	--	--	--
DHCPv4-Server	UDP/67	Closed	Closed ⁴⁾	--	✓	--	--
DNS Client	TCP/53 UDP/53	Outgoing only	Outgoing only	--	✓	--	--
DNS Server	TCP/53 UDP/53 UDP/49000 ... UDP/65535	Open ⁵⁾	Closed	--	✓	--	--
DynDNS	TCP/80 UDP/80 TCP/443 UDP/443	Outgoing only	Outgoing only	--	✓	✓	--
HTTP	TCP/80	Open	Closed	✓	✓	✓	--
HTTP Proxy	TCP/3128 TCP/8080	Outgoing only	Outgoing only	✓	✓	Optional	--
HTTPS WBM Server/Client	TCP/443	Open	Closed	✓	✓	✓	✓
IPsec/IKE	UDP/500 UDP/4500	Closed	Closed	--	✓	✓	✓
iperf3 ⁸⁾	TCP/5201	Closed	Closed	✓	✓	--	--
NTP Client	UDP/123	Outgoing only	Outgoing only	✓	✓	--	--
NTP Client (se- cure)	UDP/123	Outgoing only	Outgoing only	✓	✓	✓	--
NTP Server	UDP/123	Closed	Closed	✓	✓	--	--
NTP Server (se- cure)	UDP/123	Closed	Closed	✓	✓	✓	--
OpenVPN ¹⁰⁾	UDP/1194 TCP/1194	Outgoing only	Outgoing only	✓	✓	✓	✓
Packet Capture ¹¹⁾	TCP/2002	Disabled	Disabled	✓	✓	--	--
Ping	ICMP	Open	Closed	--	✓	--	--
RADIUS Client	UDP/1812	Closed	Closed	✓	✓	✓	Optional
	UDP/1813						--
SFTP Server	TCP/22	Outgoing only	Outgoing only	✓	✓	✓	✓
Siemens Re- mote Service (cRSP/SRS) ¹⁰⁾	TCP/443	Outgoing only	Outgoing only	--	✓	Optional	✓
SINEMA RC	HTTPS/443 and TCP/UDP depending on the server config- uration	Outgoing only	Outgoing only	✓	✓	✓	✓
SMS Relay ⁷⁾	TCP/26864	Closed	Closed	✓	✓	--	--

2.2 Available services

Service	Protocol/ Port number	Default port status		Configurable		Authentica- tion	Encryption ²⁾
		Local access	External access ¹⁾	Port	Service		
SMTP Client	TCP/25	Outgoing only	Outgoing only	✓	✓	--	--
SMTP (secure)	TCP/465 TCP/587	Outgoing only	Outgoing only	✓	✓	Optional	✓
SNMPv1/v2c ¹²⁾	UDP/161	Open	Closed	✓	✓	--	--
SNMPv3 Server	UDP/161	Open	Closed	✓	✓	Optional	Optional
SNMP Trap	UDP/161	Open	Closed	✓	✓	Optional	Optional
SNTP Client	UDP/123	Closed	Closed	✓	✓	--	--
SSH CLI	TCP/22	Open	Closed	✓	✓	✓	✓
Syslog Client	UDP/514	Outgoing only	Outgoing only	✓	✓	--	--
Syslog Client TLS	TCP/6514	Outgoing only	Outgoing only	✓	✓	--	✓
Telnet	TCP/23	Closed	Closed	✓	✓	✓	--
TFTP	UDP/69	Outgoing only	Outgoing only	✓	✓	--	--
TIA Portal Cloud Connector ⁶⁾	TCP/9023	Closed	Closed	✓	✓	--	--
TCP Diagnostic Stream ¹¹⁾	TCP/5510 TCP/5511	Closed	Closed	✓	✓	--	✓
TCP Event	TCP/26864	Closed	Closed	✓	✓	--	--
VXLAN ⁹⁾	UDP/4789	Closed	Closed	✓	✓	--	--

¹⁾ With SCALANCE M826 and M804PB, only access via vlan1 is possible in the delivery state (factory setting).

²⁾ You can find additional information on the encryption methods used in the WBM appendix "Ciphers used (Page 505)".

³⁾ Only open with SCALANCE M826

⁴⁾ Only open with SCALANCE S615

⁵⁾ Only closed with SCALANCE S615

⁶⁾ Not available with SCALANCE MUX85x

⁷⁾ Only available with SCALANCE M87x, MUM85x and RUGGEDCOM RM1224

⁸⁾ Only available with SCALANCE MUM85x

⁹⁾ Only available with SCALANCE M87x, MUX85x, S615 and RUGGEDCOM RM1224

¹⁰⁾ Not available with SCALANCE MUB852

¹¹⁾ Only available with SCALANCE MUX85x

¹²⁾ Read Only

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

The table includes the following columns:

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

Layer 2 service	Default port status	Configurable
DCP	Open (when configured)	✓
LLDP	Open (when configured)	✓
SIMATIC NET TIME	Open (when configured)	✓
VLAN	Open (when configured)	✓
VXLAN ¹⁾	Open (when configured)	✓

¹⁾ Only available with SCALANCE M87x, MUX85x, S615 and RUGGEDCOM RM1224

Description

3.1 Function

Configuration

Configuration of all parameters using the

- Web Based Management (WBM) via HTTPS
- Command Line Interface (CLI) via SSH

Security functions

- Router with NAT function
 - IP masquerading
 - NAT
 - SourceNAT
 - NETMAP
- Password protection
- Two-factor authentication
- Firewall function
 - Port forwarding
 - MAC firewall (Layer 2) (only SCALANCE MUx85x)
 - IP firewall with stateful packet inspection (layer 3 and 4)
 - Global and user-defined firewall rules
- VPN functions
To establish a VPN (Virtual Private Network), the following functions are available
 - IPsec VPN
 - OpenVPN client
- SINEMA RC client
- Use of proxy servers
- Siemens Remote Service (SRS)
- Brute Force Prevention

Monitoring / diagnostics / maintenance

- LEDs
Display of operating statuses via the LED display. You will find further information on this in the Operating Instructions of the device.
- Logging
For monitoring have the events logged.
- SNMP
For monitoring and controlling network components such as routers or switches from a central station.

Other functions

- Time-of-day synchronization
 - NTP client and NTP server
 - Secure NTP server
 - SIMATIC Time Client
 - SNTP Client
 - GPS time (only SCALANCE MUM85x)
- DHCP
 - DHCP server (local network)
 - DHCP client
- Virtual networks (VLAN)
To structure Industrial Ethernet networks with a fast growing number of devices, a physical network can be divided into several virtual subnets
- VXLANs (Virtual eXtensible LAN) (SCALANCE MUX85x, M87x, S615 and RUGGEDCOM RM1224 only)
Allows the transmission of Layer 2 packets via Layer 3 networks.
- Digital input/digital output
- Dynamic DNS client
- DNS client, DNS proxy and DNS records
- SMTP client
- TIA Portal Cloud Connector (not with SCALANCE MUX85x)
- GPS localization (only SCALANCE MUM85x)

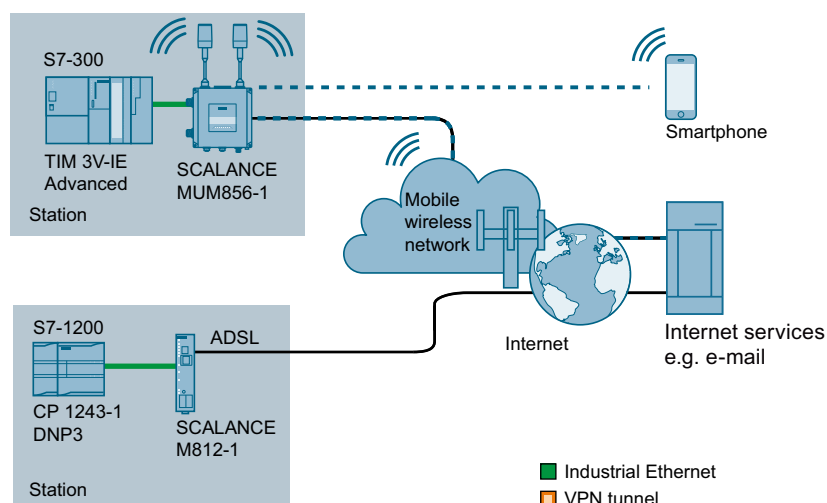
3.2 Configuration examples

3.2.1 Overview

With a SCALANCE M-800, you can link IP-based networks. The link can be via cable or wireless via public or private communications infrastructures.

Device			Communications infrastructure
M874-2	Wireless	GPRS	Public network / Internet
M874-3	Wireless	UMTS	Public network / Internet
M876-3	Wireless	UMTS	Public network / Internet
M876-4	Wireless	LTE	Public network / Internet
RM1224			
MUM856-1	Wireless	5G	Public network / Internet
MUM853-1			
MUB852-1			
M812-1	Via cable	ADSL	Public network / Internet
M816-1			
M826-2	Via cable	SHDSL	Private network / company-owned copper cables

3.2.2 SCALANCE MUM856/M81x as Internet access



You can connect a station to the Internet using the mobile wireless network or using ADSL. This makes Internet services available such as sending and receiving e-mails.

The device can automatically send an e-mail if an alarm event occurs, for example to the network administrator. When an e-mail event message is received, the WBM can be started by the Web browser using the identification of the sender to read out further diagnostics information.

The M874 can send an SMS message to a mobile phone if an alarm event occurs.

Requirement

- The M-800 is reachable via an Admin PC

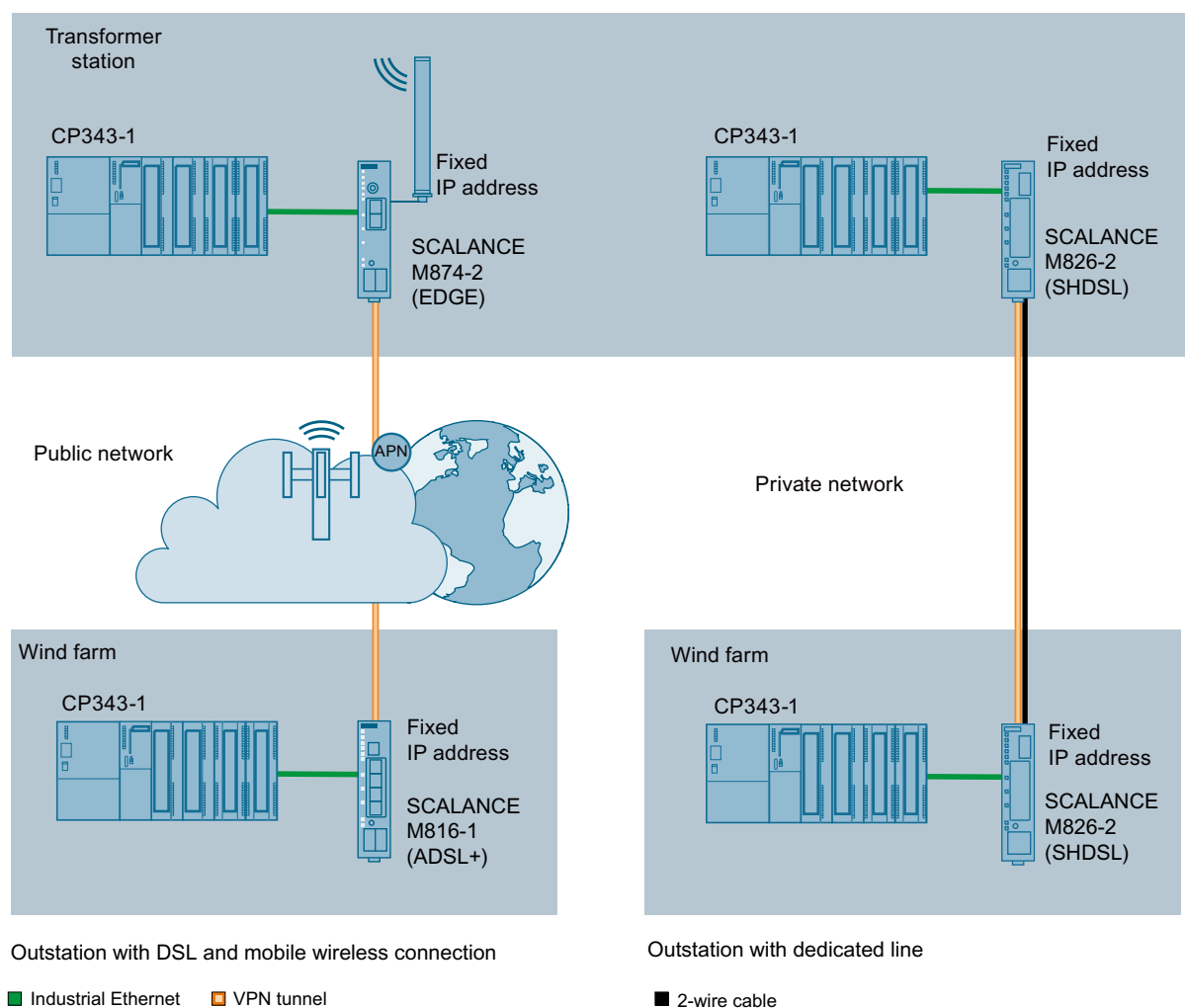
Procedure

To configure Internet access, follow the steps below:

1. Establish a connection to the WAN, see section Interfaces (Page 334).
2. To allow access to the required Internet services, set up firewall rules, see section Firewall (Page 438).
3. Setup your application for the Internet services.

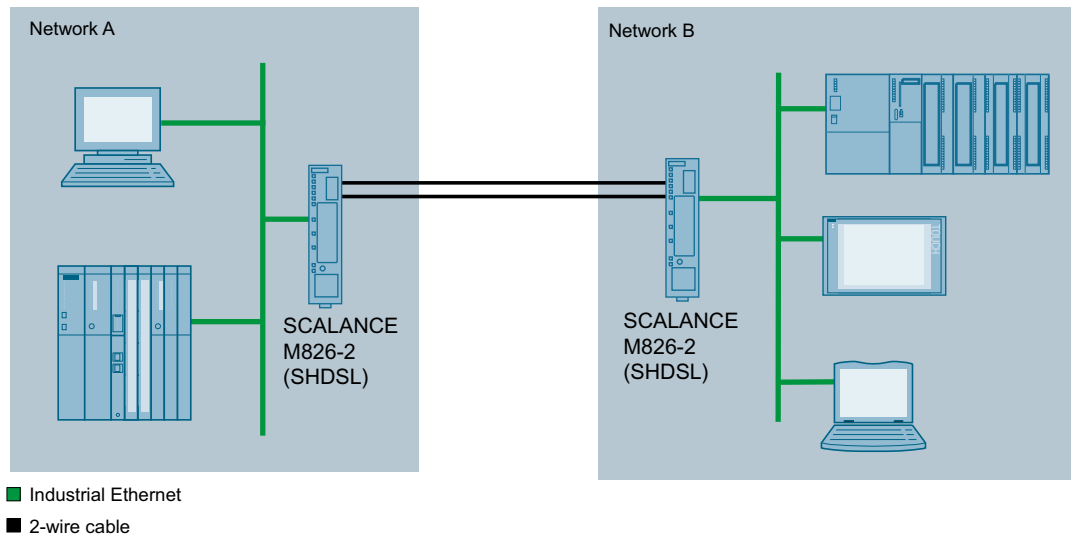
3.2.3 Direct communication of stations

In this configuration, two distributed stations are connected using the SCALANCE M-800 and can exchange data with each other. The devices communicate directly with each other, for example a wind farm and a transformer station. The data can be exchanged either via a public or a private network. The data is transferred via a secure VPN tunnel. To establish the VPN tunnel, the network provider has the required services, for example, a fixed IP address for mobile wireless routers and/or access to the Internet via a private APN.



The SCALANCE M826 modules can communicate with each other either in 2-wire mode or in 4-wire mode. In 4-wire mode, 2 x 2-wire cables are aggregated to form a virtual connection with twice the data rate.

3.2 Configuration examples



Requirements

- The M-800 is reachable via an Admin PC.
- To establish a VPN tunnel:
 - M81x and M874
The network provider offers the required services, for example, a fixed IP address for mobile wireless routers and/or an access to the Internet via a private APN.
 - M826
The devices have a fixed IP address and are in routing mode.

Procedure

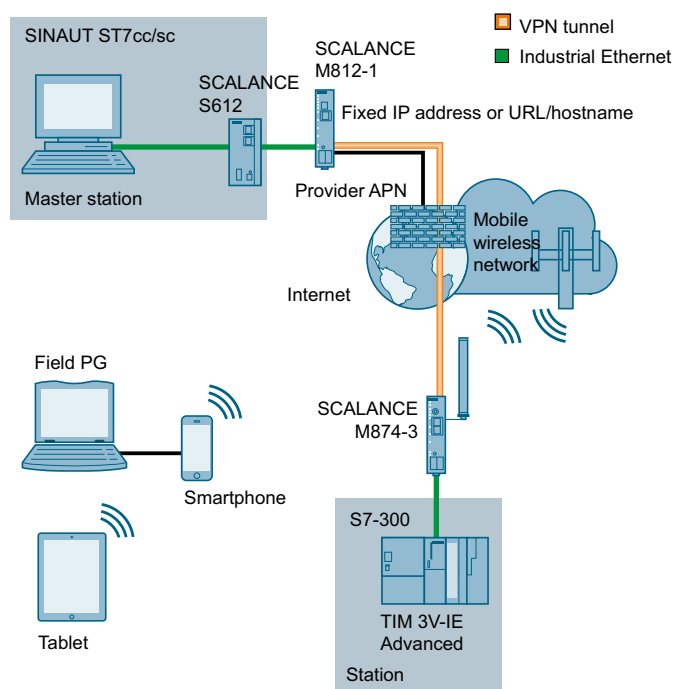
To configure data transfer via a VPN tunnel, follow the steps below:

1. Establish a connection to the public or private network, refer to the section Interfaces (Page 334).
2. Connect a controller, for example using a CP 343-1 to an Ethernet interface of the M-800.
3. Establish a VPN connection between the two M800 devices, refer to the section IPsec VPN (Page 458).
4. Set up the connected controllers for data communication.

3.2.4 Telecontrol via the mobile wireless network

You can use the M874 to transfer process data from remote stations via the mobile wireless network to the master station if, for example, no telephone network is available.

As an option, the software of the master station can be expanded with the Alarm Control Center (ACC) software package. This allows fault/error messages from the plant to be forwarded to service personnel using SMS messages, fax or e-mail.



Requirements

- The M-800 is reachable via an Admin PC.
- To establish a VPN tunnel:
Fixed IP address or hostname of the DSL router.

Procedure

To set up one or more VPN tunnels for data transfer, follow the steps below:

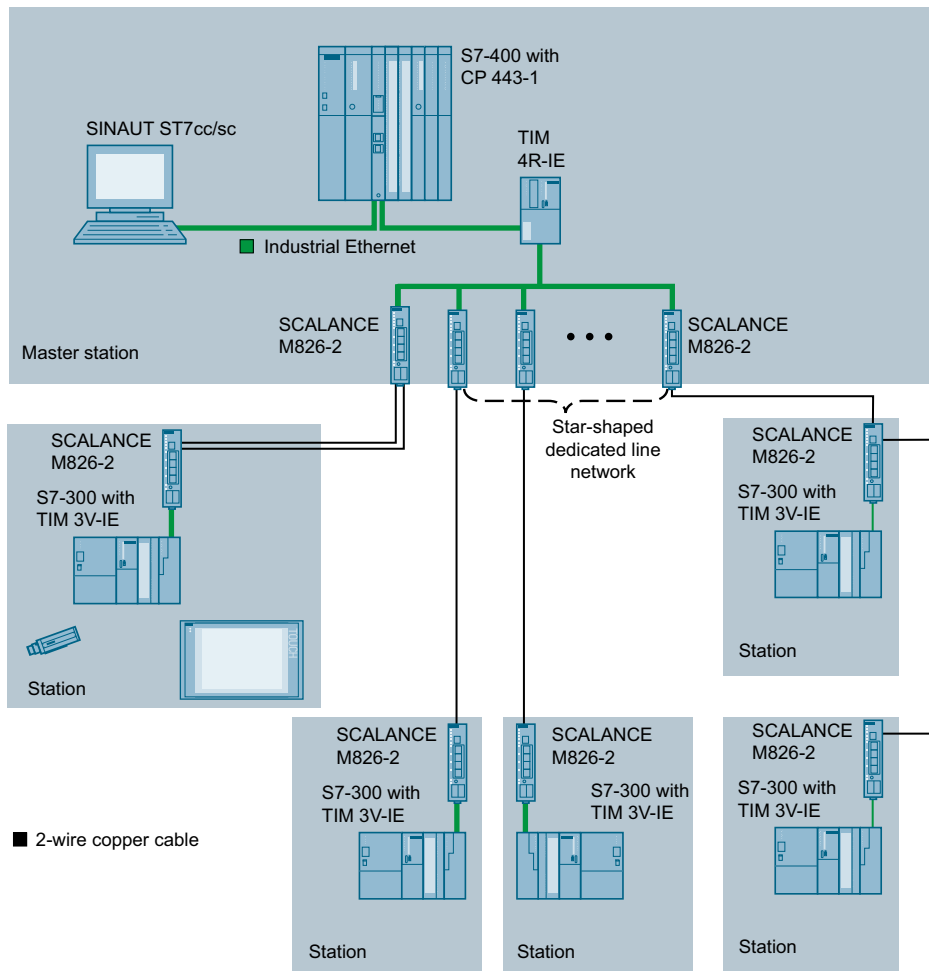
1. Establish a connection to the WAN, see section Interfaces (Page 334).
2. Connect local SINAUT applications, for example TIM 4R-IE to one of the Ethernet interfaces.
3. Establish a VPN connection, see section IPsec VPN (Page 458).
4. Set up the connected SINAUT applications for data communication.

3.2.5 Telecontrol via dedicated line

In this configuration, the outstations are connected to the master station via company owned copper cables.

Point-to-point, bus and star structures as well as mixed configurations of these basic structures can be set up.

3.2 Configuration examples

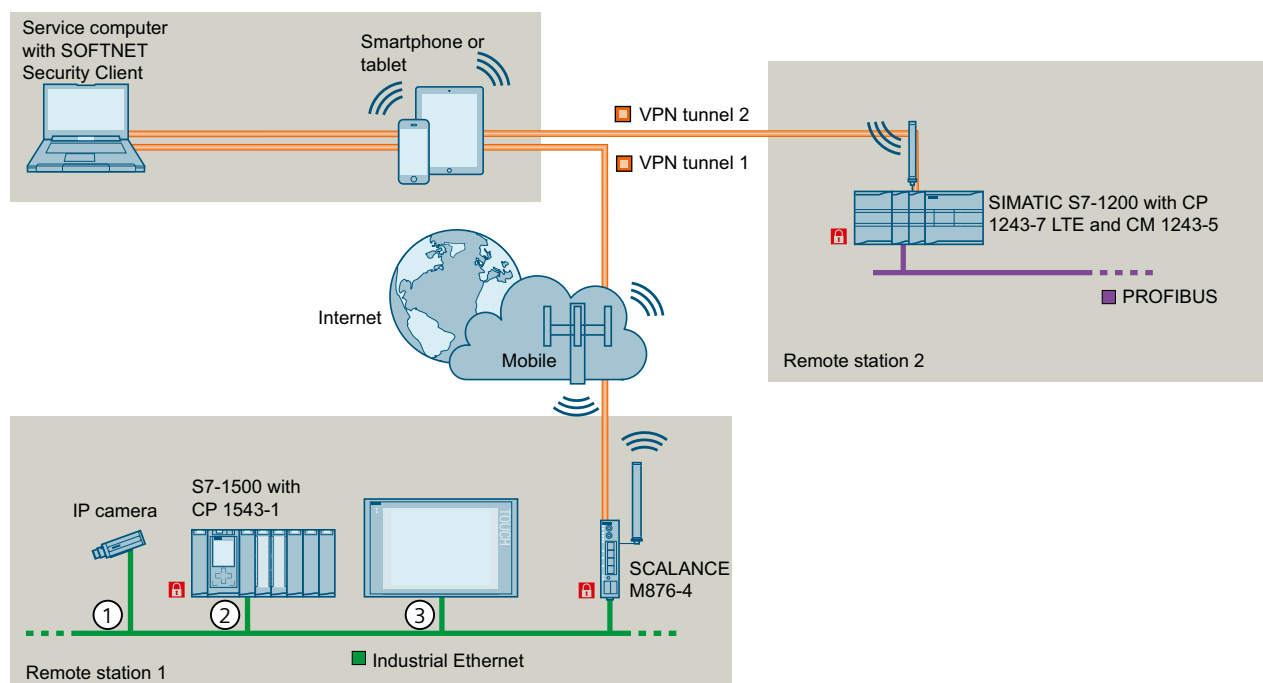


3.2.6 Mobile access to plants and plant sections

The service technician can access the remote plant while traveling and perform remote maintenance work via the M874.

For mobile access, the technician uses a mobile field PG equipped with a cell phone or tablet.

The VPN functionality ensures secure data transmission worldwide. The access options can be restricted with the integrated firewall function.



- ① Image transfer
- ② Station
- ③ Panel with web access to CP

Requirements

- The M874 is reachable via an Admin PC.

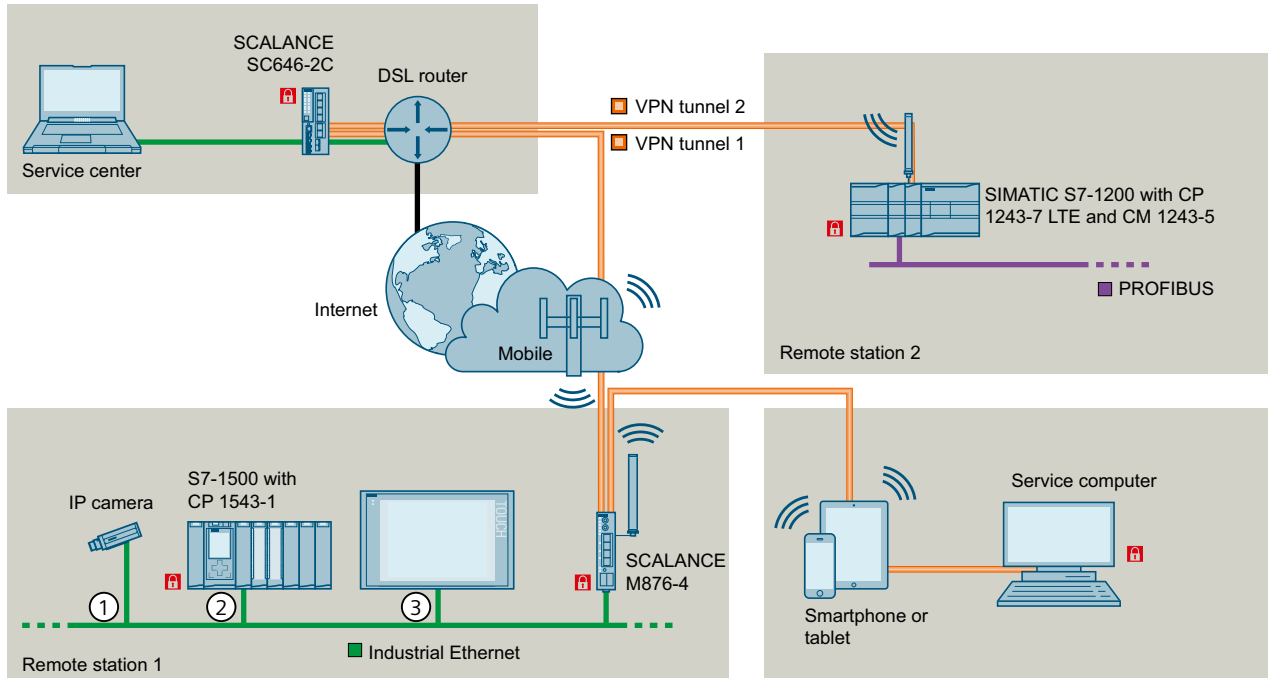
Procedure

To be able to access a plant via a VPN tunnel when traveling, note the following points and the relevant sections in these operating instructions:

- Establish a connection to the mobile wireless network; see section Mobile wireless (Page 338).
- Set up a VPN tunnel in Roadwarrior mode for the M874-x, refer to the section IPsec VPN (Page 458).
- Set up a VPN tunnel on the mobile access page in the SOFTNET Security Client.
Note: Points 3 and 4 can also be performed with the Security Configuration Tool.
- Set up the connected applications of the plant for data communication.

3.2.7 Plant access via a remote maintenance center

Another variant is client access from a remote maintenance master station. The remote maintenance master station is connected to the Internet via the SCALANCE SC600 VPN server. This protects the remote maintenance master station against unauthorized access. The plant communicates with remote station 1 via the SCALANCE M-800 that establishes a VPN tunnel with the SCALANCE SC600. This allows, for example, a service technician to control and monitor a plant from the remote maintenance master station.



- ① Image transfer
- ② Station
- ③ Panel with web access to CP

Procedure

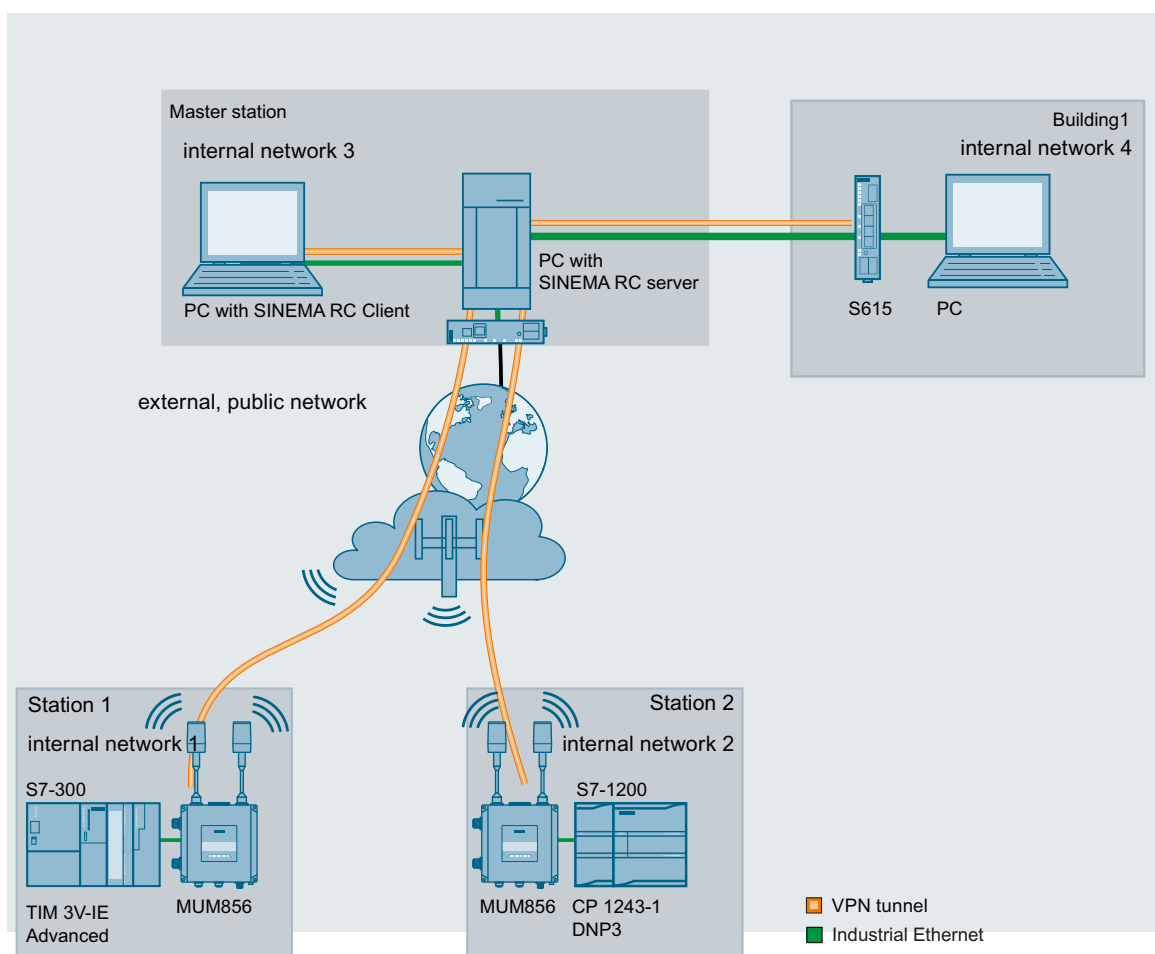
To be able to access a plant via a remote maintenance master station, follow the steps below:

1. Establish the Ethernet connection between the M-800 and the connected Admin PC.
2. Establish a connection to the mobile wireless network; see section Mobile wireless (Page 338).
3. Configure the VPN connection for the remote maintenance master station on the SCALANCE SC600.
4. Set up a VPN tunnel in standard mode, see section IPsec VPN (Page 458).
5. Set up the connected applications of the plant for data communication.

3.2.8 TeleControl with SINEMA RC

In this configuration, the remote maintenance master station is connected to the Internet/intranet via the SINEMA Remote Connect Server. The stations communicate via SCALANCE MUM856 or SCALANCE S615 that establish a VPN tunnel to the SINEMA RC server. In the master station, the SINEMA RC client establishes a VPN tunnel to the SINEMA RC server.

The devices must log on to the SINEMA RC server. The VPN tunnel between the device and the SINEMA RC Server is established only after successful authentication. Depending on the configured communications relations and the security settings, the SINEMA RC server connects the individual VPN tunnels.



Procedure

To be able to access a plant via a remote maintenance master station, follow the steps below:

1. Establish the Ethernet connection between the S615 and the connected Admin PC.
2. Create the devices and node groups on the SINEMA RC Server.
3. Configure the connection to the SINEMA RC server on the device, refer to the section SINEMA RC (Page 314).
4. Set up the connected applications of the plant for data communication.

3.3 Requirements for operation

3.3.1 For operation with MUB852

Antenna

The following table provides an overview of the frequency bands supported by the device:

6GK5852-1EA10-1AA1 (A1)	5G Standalone (SA)	n1, n2, n3, n5, n7, n8, n20, n25, n28, n30, n38, n40, n41, n48, n66, n71, n75(DL), n77, n78, n79
	5G Non-Standalone (NSA)	n1, n2, n3, n5, n7, n8, n20, n25, n28, n30, n38, n40, n41, n66, n71, n77, n78, n79
	LTE	B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29(DL), B30, B32(DL), B34, B38, B39, B40, B41, B42, B43, B46(DL), B48, B66, B71
	UMTS	B1, B2, B4, B5, B6, B8, B19
6GK5852-1EA10-1BA1 (B1)	5G Standalone (SA)	n1, n3, n5, n8, n28, n41, n77, n78, n79
	5G Non-Standalone (NSA)	n41, n77, n78, n79
	LTE	B1, B3, B5, B8, B34, B38, B39, B40, B41
	UMTS	B1, B5, B8

Use antennas from the accessories program of the SCALANCE M-800 device. You will find further information on this in the device-specific operating instructions.

Depending on the frequency bands used by your mobile wireless provider, antennas must be tuned to the suitable frequencies. Check with your mobile wireless provider for the frequency bands.

Note

You should also note the national approvals for the SCALANCE M-800 devices. You will find the current status of the national approval on the Internet at the following address: SIOS (<https://support.industry.siemens.com/cs/ww/de/view/91438171/en>)

Note

Antennas

- An antenna must always be connected to all antenna ports in order to use 3/4/5G connectivity.

Protective caps

Keep the removed protective cap for later use.

Power supply

You will find further information on this in the device-specific operating instructions.

SIM card

A nano SIM card with SCALANCE MUB852 from the chosen mobile wireless provider

PIN

The PIN (= Personal Identification Number) for the SIM card

5 G / LTE / UMTS activation

The SIM card must be activated for the services in the mobile wireless network by your mobile wireless provider.

The access data must be known:

- Access point name (APN)
- User name
- Password

Configuration

In the factory settings, the SCALANCE MUM853 can be reached as follows for initial configuration:

	Default values set in the factory
Ethernet interface for the configuration	P1
IP address	192.168.1.1
Subnet mask	255.255.255.0
WBM	Access using HTTPS: TCP port 443
CLI	Access using SSH, TCP port 22
User name	admin The user name can be changed after the first logon or after a "Restore Factory Defaults and Restart". Afterwards, renaming "admin" is no longer possible.
Password	admin The password needs to be changed after the first logon or after a "Restore Factory Defaults and Restart"

You will find more information in "Web Based Management (Page 105)" and in "Starting and logging in".

3.3.2 For operation with MUM853

Antenna

The following table provides an overview of the frequency bands supported by the device:

6GK5853-2EA00-2DA1	5G Standalone (SA)	n1, n3, n5, n7, n8, n12, n20, n28, n38, n40, n41, n48, n71, n77, n78, n79
	5G Non-Standalone (NSA)	n1, n3, n5, n7, n8, n20, n28, n38, n40, n41, n48, n66, n77, n78, n79
	LTE	B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29, B30, B32, B66, B71, B34, B38, B39, B40, B41, B42, B43, B46, B48
	UMTS	B1, B2, B3, B4, B5, B8
	GNSS	GPS L1 (1575.42 MHz) GPS L5 (1176.45 MHz) For GNSS operation, connect an antenna with a clear view of the sky to antenna port A4.
6GK5853-2EA10-2AA1 (A1)	5G Standalone (SA)	n1, n2, n3, n5, n7, n8, n20, n25, n28, n30, n38, n40, n41, n48, n66, n71, n75(DL), n77, n78, n79
	5G Non-Standalone (NSA)	n1, n2, n3, n5, n7, n8, n20, n25, n28, n30, n38, n40, n41, n66, n71, n77, n78, n79
	LTE	B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29(DL), B30, B32(DL), B34, B38, B39, B40, B41, B42, B43, B46(DL), B48, B66, B71
	UMTS	B1, B2, B4, B5, B6, B8, B19
	GNSS	GPS L1 (1575.42 MHz) Galileo E1 (1575.42 MHz) For GNSS operation, connect an antenna with a clear view of the sky to antenna port A4.
6GK5853-2EA10-2BA1 (B1)	5G Standalone (SA)	n1, n3, n5, n8, n28, n41, n77, n78, n79
	5G Non-Standalone (NSA)	n41, n77, n78, n79
	LTE	B1, B3, B5, B8, B34, B38, B39, B40, B41
	UMTS	B1, B5, B8
	GNSS	Not supported

Use antennas from the accessories program of the SCALANCE M-800 device. You will find further information on this in the device-specific operating instructions.

Depending on the frequency bands used by your mobile wireless provider, antennas must be tuned to the suitable frequencies. Check with your mobile wireless provider for the frequency bands.

Note

You should also note the national approvals for the SCALANCE M-800 devices. You will find the current status of the national approval on the Internet at the following address: SIOS (<https://support.industry.siemens.com/cs/ww/de/view/91438171/en>)

Note**Antennas**

- An antenna must always be connected to all antenna ports in order to use 3/4/5G connectivity.
- If you want to use GNSS, connect a passive antenna with a clear view of the sky to the A4 port.

Protective caps

Keep the removed protective cap for later use.

Power supply

You will find further information on this in the device-specific operating instructions.

SIM card

A micro SIM card from the chosen mobile wireless provider.

PIN

The PIN (= Personal Identification Number) for the SIM card

5 G / LTE / UMTS activation

The SIM card must be activated for the services in the mobile wireless network by your mobile wireless provider.

The access data must be known:

- Access point name (APN)
- User name
- Password

Configuration

In the factory settings, the SCALANCE MUM853 can be reached as follows for initial configuration:

	Default values set in the factory
Ethernet interface for the configuration	P1 ... P4
IP address	192.168.1.1
Subnet mask	255.255.255.0
WBM	Access using HTTPS: TCP port 443
CLI	Access using SSH, TCP port 22
User name	admin The user name can be changed after the first logon or after a "Restore Factory Defaults and Restart". Afterwards, renaming "admin" is no longer possible.
Password	admin The password needs to be changed after the first logon or after a "Restore Factory Defaults and Restart"

You will find more information in "Web Based Management (Page 105)" and in "Starting and logging in".

3.3.3 For operation with MUM856

Antenna

The following table provides an overview of the frequency bands supported by the device:

6GK5856-2EA00-3DA1 (EU)	5G Standalone (SA)	n1, n3, n5, n7, n8, n12, n20, n28, n38, n40, n41, n48, n71, n77, n78, n79
	5G Non-Standalone (NSA)	n1, n3, n5, n7, n8, n20, n28, n38, n40, n41, n48, n66, n77, n78, n79
	LTE	B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29, B30, B32, B66, B71, B34, B38, B39, B40, B41, B42, B43, B46, B48
	UMTS	B1, B2, B3, B4, B5, B8
	GNSS	GPS L1 (1575.42 MHz) GPS L5 (1176.45 MHz) For GNSS operation, connect an antenna with a clear view of the sky to antenna port A4.

3.3 Requirements for operation

6GK5856-2EA00-3FA1 (CN)	5G Standalone (SA)	n1, n2, n3, n5, n7, n8, n12, n20, n28, n38, n40, n41, n48, n66, n71, n77, n78, n79
	5G Non-Standalone (NSA)	n41, n77, n78, n79
	LTE	B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29, B30, B32, B66, B71, B34, B38, B39, B40, B41, B42, B43, B46, B48
	UMTS	B1, B2, B3, B4, B5, B8
	GNSS	GPS L1 (1575.42 MHz) GPS L5 (1176.45 MHz) For GNSS operation, connect an antenna with a clear view of the sky to antenna port A4.
6GK5856-2EA10-3AA1 (A1)	5G Standalone (SA)	n1, n2, n3, n5, n7, n8, n20, n25, n28, n30, n38, n40, n41, n48, n66, n71, n75(DL), n77, n78, n79
	5G Non-Standalone (NSA)	n1, n2, n3, n5, n7, n8, n20, n25, n28, n30, n38, n40, n41, n66, n71, n77, n78, n79
	LTE	B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29(DL), B30, B32(DL), B34, B38, B39, B40, B41, B42, B43, B46(DL), B48, B66, B71
	UMTS	B1, B2, B4, B5, B6, B8, B19
	GNSS	GPS L1 (1575.42 MHz) Galileo E1 (1575.42 MHz) For GNSS operation, connect an antenna with a clear view of the sky to antenna port A4.
6GK5856-2EA10-3BA1 (B1)	5G Standalone (SA)	n1, n3, n5, n8, n28, n41, n77, n78, n79
	5G Non-Standalone (NSA)	n41, n77, n78, n79
	LTE	B1, B3, B5, B8, B34, B38, B39, B40, B41
	UMTS	B1, B5, B8
	GNSS	Not supported

Use antennas from the accessories program of the SCALANCE M-800 device. You will find further information on this in the device-specific operating instructions.

3.3 Requirements for operation

Depending on the frequency bands used by your mobile wireless provider, antennas must be tuned to the suitable frequencies. Check with your mobile wireless provider for the frequency bands.

Note

You should also note the national approvals for the SCALANCE M-800 devices. You will find the current status of the national approval on the Internet at the following address: SIOS (<https://support.industry.siemens.com/cs/ww/de/view/91438171/en>)

Note**Antennas**

- An antenna must always be connected to all antenna ports in order to use 3/4/5G connectivity.
- If you want to use GNSS, connect a passive antenna with a clear view of the sky to the A4 port.

Protective caps

Keep the removed protective cap for later use.

Power supply

You will find further information on this in the device-specific operating instructions.

SIM card

A micro SIM card with SCALANCE MUM85x from the chosen mobile wireless provider

PIN

The PIN (= Personal Identification Number) for the SIM card

5 G / LTE / UMTS activation

The SIM card must be activated for the services in the mobile wireless network by your mobile wireless provider.

The access data must be known:

- Access point name (APN)
- User name
- Password

Configuration

In the factory settings, the SCALANCE MUx85x can be reached as follows for initial configuration:

	Default values set in the factory
Ethernet interface for the configuration	P1
IP address	192.168.1.1

	Default values set in the factory
Subnet mask	255.255.255.0
WBM	Access using HTTPS: TCP port 443
CLI	Access using SSH, TCP port 22
User name	admin The user name can be changed after the first logon or after a "Restore Factory Defaults and Restart". Afterwards, renaming "admin" is no longer possible.
Password	admin The password needs to be changed after the first logon or after a "Restore Factory Defaults and Restart"

You will find more information in "Web Based Management (Page 105)" and in "Starting and logging in".

3.3.4 For operation with M87x / RM1224

Antenna

The frequency range of the antenna depends on the device being used:

- SCALANCE M874-2
EGPRS / GPRS (2G): 850, 900, 1800 or 1900 MHz
- SCALANCE M874-3 / M876-3
UMTS (3G): 800, 850, 900, 1900 or 2100 MHz
- SCALANCE M876-4/ RM1224
LTE (4G): 800, 900, 1800, 2100 or 2600 MHz

Use antennas from the accessories program of the SCALANCE M-800 device. You will find further information on this in the device-specific operating instructions.

Note

You should also note the national approvals for the SCALANCE M-800 devices. You will find the current status of the national approval on the Internet at the following address: http://www.automation.siemens.com/mcms/industrial-communication/en/support/ik-info/Documents/Online_CountryApprovals_GSM_UMTS_products.pdf (https://w3.siemens.com/mcms/industrial-communication/en/support/ik-info/Documents/Online_CountryApprovals_GSM_UMTS_products.pdf)

Power supply

A power supply with a voltage between 12 VDC and 24 VDC that can provide sufficient current. You will find further information on this in the device-specific operating instructions.

SIM card

A mini SIM card from the chosen mobile wireless provider.

PIN

The PIN (= Personal Identification Number) for the SIM card

LTE / UMTS / EGPRS / GPRS activation

The SIM card must be activated for the services in the mobile wireless network by your mobile wireless provider.

The access data must be known:

- Access point name (APN)
- User name
- Password

Configuration

By default, SCALANCE M87x / RUGGEDCOM RM1224 can be reached for initial configuration as follows:

	Default values set in the factory
Ethernet interface for the configuration	M874: P1 ... P2 M876: P1 ... P4
IP address	192.168.1.1
Subnet mask	255.255.255.0
WBM	Access using HTTPS: TCP port 443
CLI	Access using SSH, TCP port 22
User name	admin The user name can be changed after the first logon or after a "Restore Factory Defaults and Restart". Afterwards, renaming "admin" is no longer possible.
Password	admin The password needs to be changed after the first logon or after a "Restore Factory Defaults and Restart"

You will find more information in "Web Based Management (Page 105)" and in "Starting and logging in".

3.3.5 For operation with M81x

Power supply

A power supply with a voltage between 12 VDC and 24 VDC that can provide sufficient current.

You will find further information on this in the device-specific operating instructions.

ADSL connection

An ADSL connection of the chosen DSL provider.

ADSL activation

The DSL connection must be activated by your DSL provider.

The access data must be known:

- User name
- Password
- VCI / VPI
- Encapsulation

Configuration

In the factory settings, the SCALANCE M81x can be reached as follows for initial configuration:

	Default values set in the factory
Ethernet interface for the configuration	M812: P1 M816: P1 ... P4
IP address	192.168.1.1
WBM	Access using HTTPS: TCP port 443
CLI	Access using SSH, TCP port 22
Subnet mask	255.255.255.0
User name	admin The user name can be changed after the first logon or after a "Restore Factory Defaults and Restart". Afterwards, renaming "admin" is no longer possible.
Password	admin The password needs to be changed after the first logon or after a "Restore Factory Defaults and Restart"

You will find more information in "Web Based Management (Page 105)" and in "Starting and logging in".

3.3.6 For operation with M826

Power supply

A power supply with a voltage between 12 VDC and 24 VDC that can provide sufficient current.

You will find further information on this in the device-specific operating instructions.

SHDSL connection

Company-owned copper cables

Configuration

In the factory settings, the SCALANCE M826 can be reached as follows for initial configuration:

	Default values set in the factory
Ethernet interface for the configuration	P1 ... P4
IP address	0.0.0.0 An initial IP address for a SCALANCE M826 cannot be assigned using Web Based Management (WBM) because this configuration tool requires that an IP address already exists. The following options are available to assign an IP address to an unconfigured device: • DHCP (default) • SINEC PNI • STEP 7
Subnet mask	255.255.255.0
WBM	Access using HTTPS: TCP port 443
CLI	Access using SSH, TCP port 22
User name	admin The user name can be changed after the first logon or after a "Restore Factory Defaults and Restart". Afterwards, renaming "admin" is no longer possible.
Password	admin The password needs to be changed after the first logon or after a "Restore Factory Defaults and Restart"

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 M826, 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.

You will find more information in "Web Based Management (Page 105)" and in "Starting and logging in".

Note

M826 operation

The full range of functions is only supported when only SCALANCE M826 devices are used. If you use an SHDSL modem of another manufacturer as an end node, problem free operation cannot be guaranteed.

3.3.7 For operation with M804PB

Power supply

A power supply with a voltage between 12 VDC and 24 VDC that can provide sufficient current. You will find further information on this in the device-specific operating instructions.

Configuration

With the factory settings, the SCALANCE M804PB can be reached as follows for initial configuration:

	Default values set in the factory
Ethernet interface for the configuration (internal)	P1 ... P2 (vlan 1)
Connecting to the automation system	MPI/DP
IP address	192.168.1.1
Subnet mask	255.255.255.0
WBM	Access using HTTPS: TCP port 443
CLI	Access using SSH, TCP port 22
User name	admin The user name can be changed after the first logon or after a "Restore Factory Defaults and Restart". Afterwards, renaming "admin" is no longer possible.
Password	admin The password needs to be changed after the first logon or after a "Restore Factory Defaults and Restart"

You will find more information in "Web Based Management (Page 105)" and in "Starting and logging in".

3.3.8 Use in a PROFINET environment

Note

Validity of CCA declaration

The CCA declaration applies to PROFINET RT without the use in media redundancy structures.

Configuration information

When using the device in a PROFINET environment, follow the following configuration instructions:

- Set the "Aging Time" to 45 seconds.
- Disable Spanning Tree and enable Passive Listening.
- Set the Base Bridge Mode (Layer 2 > VLAN > General) to "802.1Q VLAN Bridge". The M826 is an exception. If the same subnet is transferred with SHDSL, use "802.1D Transparent Bridge" for "Base Bridge Mode".

3.3.9 TIA Portal Cloud Connector

A communication connection via the TIA Portal Cloud Connector is possible with the following components:

- TIA Portal Cloud Connector V1.1 SP3
You can find the TIA Portal Cloud Connector on the Internet pages of Siemens Industry Online Support under the following entry ID: 109764115 (<https://support.industry.siemens.com/cs/ww/en/view/109764115>)
Install the version even when a TIA Portal Cloud Connector is already installed.
You can find additional information on the TIA Portal Cloud Connector in the documentation "Working with the TIA Portal Cloud Connector (<https://support.industry.siemens.com/cs/ww/en/view/109747305>)" and "SIMATIC Instructions on the TIA Portal Cloud Connector (<https://support.industry.siemens.com/cs/ww/en/view/109742490>)".
- TIA Portal V15 Update 2 or STEP 7 V5.6

Note

- Use the "TIA Portal Cloud Connector" integrated in the product over a VPN solution (e.g. SINEMA RC).
 - Configure the firewall settings of the SCALANCE M800/S615 (e.g. predefined IPv4 rules "Cloud Connector") to prevent unauthorized access of network devices to the "TIA Portal Cloud Connector Server".
-

3.4 Configuration limits for WBM and CLI

Configuration limits of the device

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

Depending on your device, some functions are not available.

	Configurable function		Maximum number
System	DNS server		2
	DNS records ¹⁾		128 entries FQDN: Maximum of 256 characters
	Syslog server		3
	SMTP server		3
	E-mail recipient		60 20 per SMTP server
	SNMPv1 trap recipient		10
	SMS receiver ¹⁾		20
	SNTP server		2
	NTP / NTP (secure) server		16: One per VLAN
	NTP / NTP (secure) client		3
	DHCP pools		8
	IPv4 addresses managed by the DHCP server (dynamic + static)		100
	Static assignments per DHCP pool		128
	DHCP options (1, 2, 3, 4, 5, 6, 42, 66, 67)		9
	SINEMA RC		2 Only one of which is active
	Proxy server		5
	Cloud Connector ²⁾		1 interface
	Geofencing ³⁾		20
Layer 2	VLAN	Virtual LANs (port-based; including VLAN 1)	16
		Maximum frame size	- MUx85x, M87x, RM1224, M81x, M804PB: 2048 bytes - M826: 2018 bytes
	VXLAN	NVE interface / VNI	- MUM85x: 5 NVE / 1 VNI - MUB852: 1 NVE / 1 VNI
Layer 3	IP interfaces		12
	Static routes		100
	NAPT ¹⁾		32
	Source NAT		- MUM85x, M87x, RM1224, M81x, M804PB, M826: 32 - MUB852: 8
	NETMAP rules		- MUM85x, M87x, RM1224, M81x, M804PB, M826: 256 - MUB852: 32
	VRRPv3 ¹⁾		VRRPv3 instances (VRID): 2 Assigned IP addresses: 1 per VRID

3.5 Configuration limits for SINEMA RC

	Configurable function		Maximum number
Security	Users		30 (incl. user preset in the factory "admin")
	Groups		32
	Roles		32 (incl. the predefined roles)
	RADIUS server		4
	Firewall	Layer 3 firewall	IP protocols:16 IP services: 128 ICMP services:16 IP rules: - MUM85x, M87x, RM1224, M81x, M804PB, M826: 128 - MUB852: 32 Dynamic firewall: - Maximum number: 8 rule sets - Parallel user access: 4 - Maximum of 128 IP rules per firewall rule set
		Layer 2 firewall ³⁾	MAC rules:128
	IPsec VPN ¹⁾		You can create a maximum of 20 phase 2 connections per phase 1 (remote endpoint). Only with IKEv2: Multiple subnets per phase 2 connection; maximum 5
	OpenVPN		Clients: 5 Servers: 3 Maximum of 128 client connections to a device

1) Not available with SCALANCE MUB852

2) Not available with SCALANCE MUX85x

3) Only available with SCALANCE MUM85x

3.5 Configuration limits for SINEMA RC

Maximum overall data transfer for all devices: 800 Mbps

Maximum number of devices and users connected simultaneously: **1024** devices with 1 subnet each

User/device combinations can be freely selected up to the maximum overall quantity structure.

As the number of subnets is also dependent on the communication relationships permitted among one another, for example, these must be checked/questioned and restricted, where necessary. If devices do not need to communicate with one another, this function should be disabled to ensure optimum device behavior.

If the devices are to communicate with each other, the maximum number of devices and users connected simultaneously is: **200** devices with 8 subnets each communicating with each other

3.6 Hardware equipment and system functions

Availability of hardware

The following table shows the hardware of the devices

We reserve the right to make technical changes.

	M874-2 M874-3	M876-3 M876-4 RM1224	M812	M816	M826	M804PB	MUM856- 1	MUM853- 1	MUB852- 1
Interfaces	1 x SMA antenna connector	2 x SMA antenna connector	1 x DSL	1 x DSL	2 x SHDSL	1 x RS 485 (MPI/DP)	4 x N-Connect	4 x SMA antenna port	4 x SMA antenna port
	2 x RJ45	4 x RJ45	1x RJ45 (LAN)	4 x RJ45 (LAN)	4 x RJ45	2 x RJ45	1 x M12, X-coded	4 x RJ45	1 x RJ45
Digital input/output	✓	✓	✓	✓	✓	✓	✓	✓	✓
PLUG slot	✓	✓	-	✓	✓	✓	✓ (CLP)	✓ (CLP)	-
Button	✓	✓	✓	✓	✓	✓	✓	✓	✓

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 KEY-PLUG, some functions are not available.

3.6 Hardware equipment and system functions

We reserve the right to make technical changes.

		M87x RM1224	MUx85x	M812	M816	M826	M804PB
Basic Wizard	IP settings	✓	✓	✓	✓	✓	✓
	Device settings	✓	✓	✓	✓	✓	✓
	SIM	✓	✓	-	-	-	-
	Mobile network provider	✓	✓	-	-	-	-
	DSL	-	-	✓	✓	-	-
	SHDSL	-	-	-	-	✓	-
	TIA Portal Cloud Connector	✓	-	✓	✓	✓	✓
	Time settings	✓	✓	✓	✓	✓	✓
	SINEMA RC ¹⁾	✓	✓	-	✓	✓	✓
	DDNS	✓	✓	✓	✓	✓	✓
Information	Dashboard	-	✓	-	-	-	-
	ARP Table	✓	✓	✓	✓	✓	✓
	IPv6 Neighbor Table	✓	✓	✓	✓	✓	✓
	Log Tables	✓	✓	✓	✓	✓	✓
	DHCP Server Bindings	✓	✓	✓	✓	✓	✓
	Diagnostics	-	✓	-	-	-	-
	Ethernet Statistics	-	✓	-	-	-	-
	Learning Table	✓	✓	✓	✓	✓	✓
	Link Layer Discovery Protocol (LLDP) Neighbor	✓	✓	✓	✓	✓	✓
	IPv4 Routing	✓	✓	✓	✓	✓	✓
	IPv6 Routing	✓	✓	✓	✓	✓	✓
	Mobile wireless	✓	✓	-	-	-	-
	DSL	-	-	✓	✓	-	-
	SHDSL	✓	✓	✓	✓	✓	-
	IPsec VPN	✓	✓	✓	✓	✓	✓
	SINEMA RC ¹⁾	✓	✓	-	✓	✓	✓
	OpenVPN Client / Server	✓	✓	✓	✓	✓	✓
	Redundancy	✓	✓	✓	✓	✓	✓
	VRRPv3 Statistics	✓	✓	✓	✓	-	-
	VXLAN	✓ ²⁾	✓	-	-	-	-
	System Time	-	✓	-	-	-	-
	Firewall Monitoring	✓	✓	✓	✓	✓	✓

3.6 Hardware equipment and system functions

		M87x RM1224	MUx85x	M812	M816	M826	M804PB
System	SMTP Client	✓	✓	✓	✓	✓	✓
	SNMP	✓	✓	✓	✓	✓	✓
	Time Manually	✓	✓	✓	✓	✓	✓
	Time protocol switch-over	-	✓	-	-	-	-
	Daylight saving time (DST) switchover	✓	✓	✓	✓	✓	✓
	Mobile time	-	✓	-	-	-	-
	SNTP client	✓	✓	✓	✓	✓	✓
	NTP client (secure)	✓	✓	✓	✓	✓	✓
	SIMATIC time client	✓	✓	✓	✓	✓	✓
	NTP server (secure)	✓	✓	✓	✓	✓	✓
	Automatic logout	✓	✓	✓	✓	✓	✓
	Sleep Mode	-	✓ ³⁾	-	-	-	-
	Configuration of the SELECT/SET button	✓	-	✓	✓	✓	✓
	Syslog client	✓	✓	✓	✓	✓	✓
	Fault Monitoring	✓	✓	✓	✓	✓	✓
	PLUG	✓	✓ ³⁾	-	✓	✓	✓
	Ping	✓	✓	✓	✓	✓	✓
	DCP Discovery	✓	✓	✓	✓	✓	✓
	SMS	✓	✓ ³⁾	-	-	-	-
	DNS	✓	✓	✓	✓	✓	✓
	DDNS	✓	✓	✓	✓	✓	✓
	DNS Records	✓	✓ ³⁾	✓	✓	✓	✓
	DHCPv4	✓	✓	✓	✓	✓	✓
	cRSP/SRS	✓	✓ ³⁾	✓	✓	✓	✓
	Proxy Server	✓	✓	✓	✓	✓	✓
	SINEMA RC ¹⁾	✓	✓	✓	✓	✓	✓
	TIA Portal Cloud Connector	✓	-	✓	✓	✓	✓
	Connection Check	✓	✓	✓	✓	✓	✓
	Connection Fallback	✓ ²⁾	✓ ³⁾	-	-	-	-
	Configuration Backup	✓	✓	✓	✓	✓	✓
	TCP Event	✓	✓	✓	✓	✓	✓
	GPS position, GPS time, geofencing	-	✓ ³⁾	-	-	-	-
	iperf	-	✓	-	-	-	-
Interfaces	Ethernet	✓	✓	✓	✓	✓	✓
	Mobile wireless	✓	✓	-	-	-	-
	DSL	-	-	✓	✓	-	-
	SHDSL	-	-	-	-	✓	-
	Packet Capture	-	✓	-	-	-	-

3.7 PLUG

		M87x RM1224	MUx85x	M812	M816	M826	M804PB
Layer 2	Configuration	✓	✓	✓	✓	✓	✓
	VLAN	✓	✓	✓	✓	✓	✓
	VXLAN	✓ ²⁾	✓	-	-	-	-
	Dynamic MAC Aging	✓	✓	✓	✓	✓	✓
	LLDP	✓	-	✓	✓	✓	✓
	Spanning Tree	✓	✓ ³⁾	✓	✓	✓	✓
Layer 3 (IPv4)	Static routes	✓	✓	✓	✓	✓	✓
	Subnets	✓	✓	✓	✓	✓	✓
	NAT	✓	✓	✓	✓	✓	✓
	NAPT	✓	✓ ³⁾	✓	✓	✓	✓
	NETMAP	✓	✓	✓	✓	✓	✓
	VRRPv3	✓	✓ ³⁾	✓	✓	✓	✓
Layer 3 (IPv6)	Subnets	✓	✓	✓	✓	✓	✓
	NAT	✓	✓	✓	✓	✓	✓
Security	Passwords	✓	✓	✓	✓	✓	✓
	Users	✓	✓	✓	✓	✓	✓
	Two-factor authentication	✓	✓	✓	✓	✓	✓
	AAA (Authentication, Authorization, Accounting)	✓	✓	✓	✓	✓	✓
	Certificates	✓	✓	✓	✓	✓	✓
	Layer 3 firewall	✓	✓	✓	✓	✓	✓
	Layer 2 firewall	-	✓ ³⁾	-	-	-	-
	IPsec VPN	✓	✓	✓	✓	✓	✓
	OpenVPN	✓	✓ ⁴⁾	✓	✓	✓	✓

¹⁾ Activation on the devices with a PLUG/CLP slot with KEY-PLUG SINEMA Remote Connect 6GK5908-0PB00 or SCALANCE CLP 2GB SINEMA RC 6GK5908-0UA00-0AA0;

on the SCALANCE MUB852-1 with license on SINEMA RC

²⁾ Only with M876 and RM1224

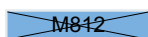
³⁾ Not available with SCALANCE MUB852-1

⁴⁾ With SCALANCE MUB852-1, only available through SINEMA RC, not freely configurable.

3.7 PLUG

3.7.1 PLUG

MUB852



Type	Properties	Article number
C-PLUG	Removable data storage medium (32 MB) for the configuration data	6GK1900-0AB00
	Removable data storage medium (256 MB) for the configuration data	6GK1900-0AB10
KEY-PLUG SINEMA RC	Removable data storage medium (256 MB) to enable the connection functionality to SINEMA Remote Connect and for storing configuration data	6GK5908-0PB00
SCALANCE CLP 2GB	Removable data storage medium for easy device replacement if a fault occurs, for storing configuration data, can be used in the following SCALANCE products with CLP slot: SCALANCE MUM85x	6GK1900-0UB00-0AA0
SCALANCE CLP EEC 2GB	Removable data storage medium with coated PCBs for simple device replacement in the event of a fault and storage of configuration data; can be used in SCALANCE products with CLP slot: SCALANCE MUM85x	6GK1900-0UQ00-0AA0
SCALANCE CLP 2GB SINEMA RC	Removable data storage medium (2 GB) to enable the connection functionality to SINEMA Remote Connect and for storing configuration data; can be used in SCALANCE products with CLP slot: SCALANCE MUM85x.	6GK5908-0UA00-0AA0

The PLUG is a removable medium and is used to transfer the configuration of the old device to the new device when a device is replaced.

The following PLUG types are available:

- C-PLUG: The removable data storage medium only saves the configuration data of the device.
- KEY-PLUG: In addition to the configuration data, the removable data storage medium contains a license with which specific functions can be enabled, e.g. SINEMA RC.
- CLP (Configuration License PLUG)
The SCALANCE CLP is a removable data storage medium for the storage and securing of configuration data that can be used in all SCALANCE devices with CLP slot, e.g. SCALANCE MUM85x. The SCALANCE CLP is used to transfer the configuration of the old device to the new device when a device is replaced. The CLP is a successor to the previously described PLUGs. The CLP is also referred to as PLUG in the description. The PLUG is available in the following variants:
 - PLUG Configuration
 - PLUG License

Position

The PLUG slot is located on the back of the device, see the Device views section in the Operating Instructions of the device.

Function

Devices with a PLUG slot support the following operating modes:

- **Without PLUG**

The device saves the configuration data in the internal memory. This mode is active when no PLUG is inserted.

- **With PLUG**

In the startup phase:

- If an **empty** PLUG (as supplied) is inserted in the device, the device automatically backs up the configuration data on the PLUG during startup. After that, it behaves like a PLUG with data.
- When a PLUG **with data** is plugged into a device, the device automatically adopts the configuration of the PLUG during the startup phase. The prerequisite for this is that the configuration data was written by a compatible device type.
One exception to this can be the IP configuration if it is set using DHCP and the DHCP server has not been reconfigured accordingly. Reconfiguration is necessary if you use functions based on MAC addresses.
- If the PLUG contains a license, additional functions are also enabled.

Note

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

During operation:

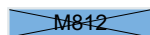
- During operation, changes to the configuration are saved on the PLUG and in the internal memory.
- The configuration data of the device is stored in a secured memory area of the PLUG. This secured memory area can only be accessed via the authentication of the Siemens device.
- The device checks whether or not a PLUG is inserted at one second intervals. If the device detects that the PLUG has been removed, it restarts automatically.

NOTICE
Operating risk - Danger of data loss
Only pull and plug the PLUG when the device is de-energized.

- The device signals deviations from normal operation of the PLUG (e.g., incompatible data, incorrect operation or malfunctions) via the existing diagnostic mechanisms (e.g., LEDs or user interfaces). The user then has the choice of either removing the PLUG again or selecting the option to reformat the PLUG.

The procedure for pulling and plugging the PLUG can be found in the section "Replacing the PLUG" in the operating instructions for the device.

3.7.2 PRESET PLUG



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 Device configuration with PRESET-PLUG (Page 483).

Technical basics

4.1 IP addresses

4.1.1 IPv4 / IPv6

What are the essential differences?

	IPv4	IPv6
IP configuration	- DHCP server - Manual	- Stateless Address Autoconfiguration (SLAAC): Stateless autoconfiguration using NDP (Neighbor Discovery Protocol) - Creates a link local address for every interface that does not require a router on the link. - Checks the uniqueness of the address on the link that requires no router on the link. - Specifies whether the global addresses are obtained via a stateless mechanism, a stateful mechanism or via both mechanisms. (Requires a router on the link.) - Manual - DHCPv6 (stateful)
Available IP addresses	32-bit: $4,294,967,296$ addresses	128-bit: $3,402,823,669,209,384,639,696,960,000$ addresses
Address format	Decimal: 192.168.1.1 with port: 192.168.1.1:20	Hexadecimal: 2a00:ad80::0123 with port: [2a00:ad80::0123]:20
Loopback	127.0.0.1	::1
IP addresses of the interface	4 IP addresses	Multiple IP addresses - LLA: A link local address (formed automatically) fe80::/128 per interface - ULA: Several unique local unicast addresses per interface - GUA: Several global unicast addresses per interface
Header	- Checksum - Variable length - Fragmentation in the header - No security	- Checking at a higher layer - Fixed size - Fragmentation in the extension header
Fragmentation	Host and router	Only endpoint of the communication
Quality of service	Type of Service (ToS) for prioritization	The prioritization is specified in the header field "Traffic Class".
Types of frame	Broadcast, multicast, unicast	Multicast, unicast, anycast

4.1 IP addresses

	IPv4	IPv6
Identification of DHCP clients/ server	Client ID: • MAC address • DHCP client ID • System name • PROFINET station name • IAID and DUID	DUID + IAID(s) = exactly one interface of the host DUID = DHCP unique identifier Unique identifier of server and clients IAID = Identity Association Identifier At least one per interface is generated by the client and remains unchanged when the DHCP client restarts Three methods of obtaining the DUID • DUID-LLT • DUID-EN • DUID-LL
Resolution of IP addresses in hardware addresses	ARP (Address Resolution Protocol)	NDP (Neighbor Discovery Protocol)

4.1.2 IPv4 address

4.1.2.1 Structure of an IPv4 address

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

Example: 192.168.16.2

The IPv4 address is composed of:

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

Subnet mask

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

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

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

Example:

Correct values

255.255.0.0 D = 1111 1111.1111 1111.0000 0000.0000 0000 B

255.255.128.0 D = 1111 1111.1111 1111.1000 0000.0000 0000 B

255.254.0.0 D = 1111 1111.1111 1110.0000 0000.0000.0000 B

Incorrect value:

255.255.1.0 D = 1111 1111.1111 1111.0000 0001.0000 0000 B

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

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

The following applies in general:

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

Classless Inter-Domain Routing (CIDR)

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

Example:

IPv4 address 192.168.0.0 with subnet mask 255.255.255.0

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

This results in the CIDR notation 192.168.0.0/24.

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

Masking additional subnets

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

Example:

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

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

Result:

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

Network gateway (router)

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

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

4.1.2.2 Initial assignment of an IPv4 address

Configuration options

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

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

- DHCP (default)
- SINEC PNI
- SIMATIC STEP 7
- SINEC NMS

Note

When the product ships and following "Restore Memory Defaults and Restart", DHCP is enabled.

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

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

4.1.2.3 Address assignment via DHCPv4

Properties of DHCP

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

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

- There is normally no fixed address assignment; in other words, when a client requests an IP address again, it normally receives a different address from the previous address. It is possible to configure the DHCP server so that the DHCP client always receives the same fixed address in response to its request. The parameter with which the DHCP client is identified for the fixed address assignment is set on the DHCP client. The address can be assigned via the MAC address, the DHCP client ID, PROFINET device name or the device name. You configure the parameter in "System > DHCP Client (Page 303)".
- The following DHCP options are supported:
 - DHCP option 3: Assignment of a router address
 - DHCP option 6: Assignment of a DNS server address
 - DHCP option 66: Assignment of a dynamic TFTP server name
 - DHCP option 67: Assignment of a dynamic boot file name

Note

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

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

4.1.2.4 Address assignment with SINEC PNI

Introduction

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

SINEC PNI

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

4.1.2.5 Address assignment with STEP 7

In SIMATIC 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.

SIMATIC STEP 7 V5.x and earlier

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

SIMATIC STEP 7 as of V13

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

4.1.3 IPv6 address

4.1.3.1 IPv6 terms

Network node

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

Router

A network node that forwards IPv6 packets.

Host

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

Link

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

Neighbor

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

IPv6 interface

Physical or logical interface on which IPv6 is activated.

Path MTU

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

Path MTU discovery

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

LLA

Link local address FE80::/10

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

ULA

Unique Local Address

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

GUA

Global unicast address

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

Interface ID

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

EUI-64

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

Example:

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

OUI = AA:BB:CC

NIC = DD:EE:FF

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

Scope

Defines the range of the IPv6 address.

4.1.3.2 Structure of an IPv6 address

IPv6 address format - notation

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

Example:

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

Rules / simplifications:

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

Structure of the IPv6 address

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

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

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

IPv6 prefix

Specified in: RFC 4291

The IPv6 prefix represents the subnet identifier.

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

Design

IPv6 address / prefix length

Example

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

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

Interface ID: ::1111

Entry and appearance

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

4.2 VLAN

4.2.1 VLAN

Network definition regardless of the spatial location of the nodes

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

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

To identify which packet belongs to which VLAN, the frame is expanded by 4 bytes, refer to VLAN tagging (Page 74). 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 > Port-based VLAN (Page 375)".
- 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.

VLAN assignment on the device

SCALANCE M812 SCALANCE MUM856 SCALANCE MUB852	P1	vlan1 For access from the local network (LAN) to the device
SCALANCE M874 SCALANCE M804PB	P1 and P2	vlan1 For access from the local network (LAN) to the device

4.2 VLAN

SCALANCE M876 SCALANCE M816 SCALANCE MUM853 RUGGEDCOM RM1224	P1 to P4	vlan1 For access from the local network (LAN) to the device
SCALANCE M826	P1 to P4 SHDSL 1 and SHDSL 2	vlan1 For access from the local network (LAN) to the device

The VLANs are in different IP subnets. To allow these to communicate with each other, the corresponding route and firewall rule must be configured on the device.

You can change the assignment in "Layer 2 > VLAN > General (Page 371)".

4.2.2 VLAN tagging

Expansion of the Ethernet frames by four bytes

For CoS (Class of Service, frame priority) and VLAN (virtual network), the IEEE 802.1Q standard defined the expansion of Ethernet frames by adding the VLAN tag.

Note

The VLAN tag increases the permitted total length of the frame from 1518 to 1522 bytes. The end nodes on the networks must be checked to find out whether they can process this length / this frame type. If this is not the case, only frames of the standard length may be sent to these nodes.

The additional 4 bytes are located in the header of the Ethernet frame between the source address and the Ethernet type / length field:

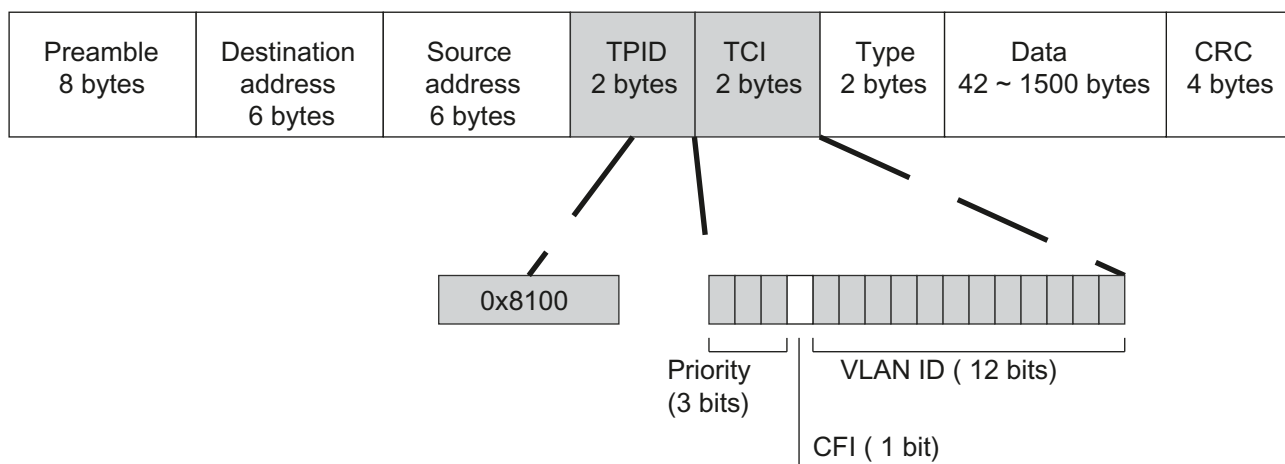


Figure 4-1 Structure of the expanded Ethernet frame

The additional bytes contain the tag protocol identifier (TPID) and the tag control information (TCI).

Tag protocol identifier (TPID)

The first 2 bytes form the Tag Protocol Identifier (TPID) and always have the value 0x8100. This value specifies that the data packet contains VLAN information or priority information.

Tag Control Information (TCI)

The 2 bytes of the Tag Control Information (TCI) contain the following information:

QoS Trust

The tagged frame has 3 bits for the priority that is also known as Class of Service (CoS), see also IEEE 802.1Q.

CoS bits	Priority	Type of the data traffic
000	0 (lowest)	Background
001	1	Best Effort
010	2	Excellent Effort
011	3	Critical Applications
100	4	Video, < 100 ms delay (latency and jitter)
101	5	Voice (language), < 10 ms delay (latency and jitter)
110	6	Internetwork Control
111	7 (highest)	Network Control

The prioritization of the data packets is possible only if there is a queue in the components in which they can buffer data packets with lower priority.

The device has multiple parallel queues in which the frames with different priorities can be processed. As default, first, the frames with the highest priority are processed. This method ensures that the frames with the highest priority are sent even if there is heavy data traffic.

Canonical Format Identifier (CFI)

The CFI is required for compatibility between Ethernet and the token Ring.
The values have the following meaning:

Value	Meaning
0	The format of the MAC address is canonical. In the canonical representation of the MAC address, the least significant bit is transferred first. Standard-setting for Ethernet switches.
1	The format of the MAC address is not canonical.

VLAN ID

4.3 VXLAN

In the 12-bit data field, up to 4096 VLAN IDs can be formed. The following conventions apply:

VLAN ID	Meaning
0	The frame contains only priority information (priority tagged frames) and no valid VLAN identifier.
1- 4094	Valid VLAN identifier, the frame is assigned to a VLAN and can also include priority information. Default VLAN ID: 1
4095	Reserved

4.3 VXLAN

VXLAN (Virtual eXtensible LAN), like VLAN, divides a network into multiple virtual network segments. The Ethernet frame (Layer 2) is forwarded through a VXLAN tunnel via an IP network (Layer 3).

VNI / VNID

The VXLAN network ID (VNID / VNI) determines membership of an Ethernet frame in a VXLAN and has 24 bits. This means that up to 16 million network segments, often also referred to as VXLAN segments, are possible. The nodes with the same VNI are in a VXLAN segment and can communicate with each other.

VTEP

The devices (physical or virtual) that establish the tunnel are referred to as VLAN tunnel endpoints (VTEP). The source VTEP encapsulates the frame in different headers to send the Ethernet frame. The destination VTEP, also called remote VTEP, decapsulates the Ethernet frame and forwards it.

The VTEP has two interfaces.

- **Physical interface**
The VTEP is connected to the local network and its nodes via the physical interface. The Ethernet frames are encapsulated and decapsulated at this interface.
Depending on the configuration, the local network is divided into multiple VLANs. To ensure that the VTEP forwards the Ethernet frame into the right VLAN, an assignment of VLAN ID to VNI is configured. This also applies for the opposite direction. If the VTEP receives an Ethernet frame, it uses the VNI in the VXLAN header that is assigned to this VLAN.
- **Virtual interface**
The VTEPs establish the VXLAN tunnel via the network virtual endpoint (NVE) interface and forward the encapsulated Ethernet frame. A VTEP can have multiple NVE interfaces that differ through a unique ID (NVE ID (Page 376)).

Frame format with VXLAN

Header in which the Layer 2 Ethernet frame is encapsulated								Layer2 Ethernet frame
① Outer MAC header 18 bytes		② Outer IP header IPv4: 20 bytes IPV6: 40 bytes		③ UDP header 8 bytes		④ VXLAN header 8 bytes		
Bit		Bit		Bit		Bit		⑤ Inner MAC header - Destination MAC address - Source MAC address ⑥ Inner IP header - Destination MAC address - Source MAC address ⑦ VLAN tag (Page 379) ⑧ Payload 46 ... 1500 bytes
48	Remote VTEP MAC address (Page 381)	72	Different data of the IP header	16	Source port	8	VXLAN flag 00001000: VNI contained	
48	Source VTEP MAC address	8	IP protocol	16	Destination port (VXLAN port) (Page 376)	24	Reserved	
16	VLAN type	16	Checksum	16	Length	24	VNI (Page 379)	
16	VLAN ID	32 / 64	32: Source VTEP IPv4 address (Page 378) 64: Source IPv6 address	16	Checksum	8	Reserved	Frame Check Sequence
16	Ethernet type	32 / 64	32: Remote VTEP IPv4 address (Page 380) or Remote VTEP IPv4 address (Page 381) 64: Destination IPv6 address					

VXLAN and firewall

The predefined "VXLAN" firewall rule must be enabled so that a VTEP can establish a VXLAN tunnel with the VTEP of the device.

4.4 SNMP

Introduction

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

Tasks of SNMP:

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

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

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

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

Standard values of the community strings:

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

Note

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

Further simple protection mechanisms at the device level:

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

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

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

The management station sends data packets of the following type:

- GET
Request a data record from the SNMP agent
- GETNEXT
Calls up the next data record.

- GETBULK (available as of SNMPv2c)
Requests multiple data records at once, for example several rows of a table.
- SET
Contains parameter assignment data for the relevant device.

The SNMP agent sends data packets of the following type:

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

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

SNMPv3

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

SNMPv3 supports:

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

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

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

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

Restriction when using the function

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

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

Compatibility with predecessor products

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

4.5 ICMP

The acronym ICMP stands for Internet Control Message Protocol (RFC792) and is used to exchange error and information messages.

- **Error message**
Informs the sender of the IP frame that when forwarding the frame an error or a parameter problem occurred.
- **Information message**
Can contain information about the time measurement, the address mask, the reachability of the destination or for finding the router.

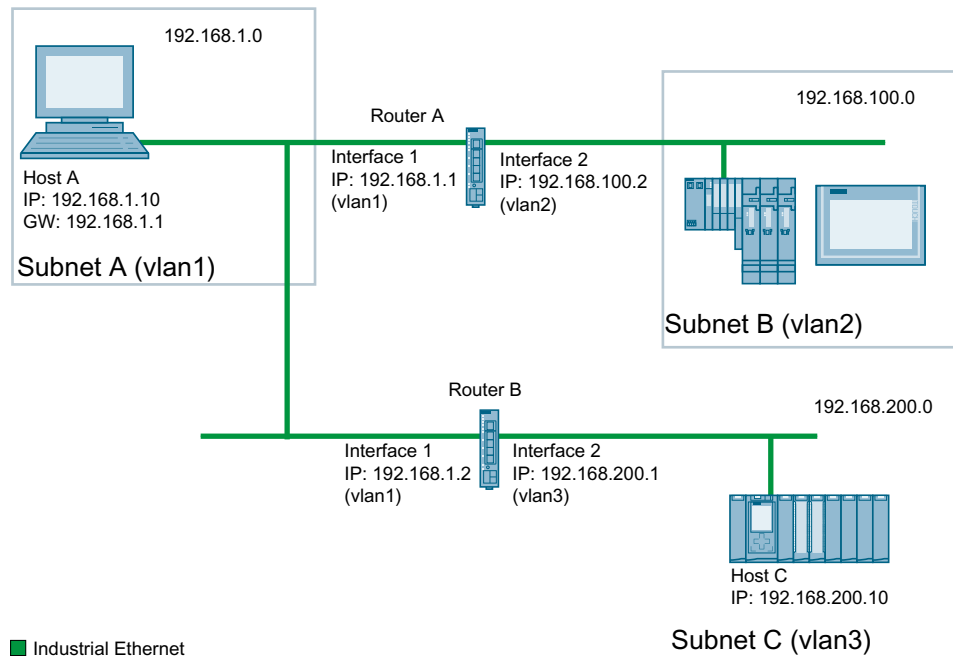
Structure of the ICMP data packet

0	4	8	12	16	20	24	28	31
ICMP packet type Type of message		Code Further details of the message		Checksum				
Data (optional)								

- **ICMP packet type**
The most important ICMP packet types are as follows:
 - **Redirect**
The router informs the host in one of its subnets that there is a better route to the destination. This ICMP packet type is dealt with in more detail in the following description.
 - **Destination Unreachable**
IP frame cannot be delivered.
 - **Time Exceeded**
Time limit exceeded
 - **Echo-Request**
Echo request, better known as ping.
- **Code**
The code describes the ICMP packet type in greater detail. The selection depends on the selected ICMP packet type. With "Destination Unreachable," for example "Code 1" host cannot be reached.

You will find a full list of the ICMP packet types and codes on the website of IANA (<https://www.iana.org/>).

ICMP packet type 5 - Redirect



Host A wants to send an IP frame to host C. Host C is not located in the same subnet as host A. For this reason host A sends the IP frame to its default gateway. The default gateway of host A is interface 1 of router A. Router A cannot forward the IP frame because it does not know the destination network. Via its routing table, however, router A knows that subnet C is reachable via router B. Router B connects subnet A with subnet C. Router A sends a redirect message to host A. In this, router A instructs host A in future to send IP frames to host C via router B whose IP address is contained in the redirect message. The initial IP frame is sent by router A directly to router B that forwards it to Host C.

Conditions for sending redirect messages

- The IP frame is received and sent via the same interface of router A.
- The source IP address (host A) is from the same subnet as the next hop address (router B) in the routing table.
- The IP frame is not affected by a source NAT rule (masquerading, source NAT or NETMAP).
- So that router A forwards the initial IP frame to router B, a firewall rule `vlanX → vlanX` is required.

4.6 Security functions

4.6.1 Adapting the MTU for IPsec VPN and SINEMA RC

Adapting the MTU (Maximum Transmission Unit)

The MTU specifies the permitted size of a data packet for transmission in the network. When these data packets are then transferred from the device via the IPsec tunnel or SINEMA RC, the original data packet becomes larger as a result of the additional header information and may need to be segmented for further transfer. This depends on the MTU specifications in the connected network. However, a necessary segmentation may lead to noticeable losses in performance or cancelation of the data transfer.

Avoid this by adapting the MTU format on the terminal device, which means reducing it in such a way that the data packets received by the device can be supplemented by the required additional information without the need for subsequent segmentation. A reasonable size is in the range of between 1000 and 1400 bytes.

4.6.2 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.

Note

Entered passwords cannot be read as plain text; instead asterisks * are displayed.

Local login

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

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

Login via an external RADIUS server

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

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

RADIUS authorization mode "Standard"

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

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

RADIUS authorization mode "Manufacturer-specific"

Requirement

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

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

Procedure

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

1. The user logs on with user name and password on the device.
2. The device sends an authentication request with the login data to the RADIUS server.
3. The RADIUS server runs a check and signals the result back to the device.

Case A: The RADIUS server reports a successful authentication and returns the group assigned to the user to the device.

- The group is known on the device and the user is not entered in the table "External User Accounts"
→ The user is logged in with the rights of the assigned group.
- The group is known on the device and the user is entered in the table "External User Accounts"
→ The user is assigned the role with the higher rights and logged in with these rights.
- The group is not known on the device and the user is entered in the table "External User Accounts"
→ The user is logged in with the rights of the role linked to the user account.
- The group is not known on the device and the user is not entered in the table "External User Accounts"
→ The user is logged in with the rights of the role "Default".

Case B: The RADIUS server reports a successful authentication but does not return a group to the device.

- The user is entered in the table "External User Accounts":
→ The user is logged in with the rights of the linked role.
- The user is not entered in the table "External User Accounts":
→ The user is logged in with the rights of the role "Default".

Case C: The RADIUS server reports a failed authentication to the device:

- The user is denied access.

4.6.3 Firewall

The security functions of the device include a stateful inspection firewall. This is a method of packet filtering or packet checking.

The IP packets are checked based on firewall rules in which the following is specified:

- The permitted protocols
- IP addresses and ports of the permitted sources
- IP addresses and ports of the permitted destinations

If an IP packet fits the specified parameters, it is allowed to pass through the firewall. The rules also specify what is done with IP packets that are not allowed to pass through the firewall.

Simple packet filter techniques require two firewall rules per connection.

- One rule for the query direction from the source to the destination.
- A second rule for the response direction from the destination to the source

Stateful inspection firewall

You only need to specify one firewall rule for the query direction from the source to the destination. The second rule is added implicitly. The packet filter recognizes when, for example, computer "A" is communicating with computer "B" and only then does it allow replies. A query by computer "B" is therefore not possible without a prior request by computer "A".

You configure the firewall in "Security > Firewall (Page 438)".

Note

IP packets via layer 2 (within the same VLAN)

If the IP packets from the device are sent via a switch port (layer 2), these IP packets are not checked based on firewall rules. The firewall has no effect on packets forwarded at the layer 2 level.

Communication directions

from	to	Meaning
vlan (1-x) nve x	vlan (1-x) nve x	Access from the V(X)LAN segment to the V(X)LAN segment. Example: vlan1 (INT) → vlan2 (EXT) Access from the local IP subnet and the device to the external IP subnet.
	ppp0/usb	Access from the IP subnet to the mobile wireless interface of the device.
	Device	Access from the IP subnet to the device.
	SINEMA RC	Access from the IP subnet and the device to the SINEMA RC connection.
	IPsec (all) IPsec <Connection Name> OpenVPN (all) OpenVPN <Connection Name>	Access from the IP subnet to the tunnel partners that can be reached via all VPN connections (all) or via a certain VPN connection (<Connection Name>).
Device	vlan (1-x) nve x	Access from the device to the IP subnet.
	ppp0/usb	Access from the device to the mobile wireless interface of the device.
	SINEMA RC	Access from the device to the SINEMA RC connection
	IPsec (all) IPsec <Connection Name> OpenVPN (all) OpenVPN <Connection Name>	Access from the device to the tunnel partners that can be reached via all VPN connections (all) or via a certain VPN connection (<Connection Name>).

4.6 Security functions

from	to	Meaning
SINEMA RC	vlan x	Access from the SINEMA RC server to the V(X)LAN segment.
	ppp0/usb	Access from the SINEMA RC server to the mobile wireless interface of the device.
	Device	Access from the SINEMA RC server to the device.
	IPsec (all) IPsec <Connection Name> OpenVPN (all) OpenVPN <Connection Name>	Access from the SINEMA RC Server to the tunnel partners that can be reached via all VPN connections (all) or via a certain VPN connection <Connection Name>.
IPsec (all) IPsec <Connection Name> OpenVPN (all) OpenVPN <Connection Name>	vlan (1-x) nve x	Access via tunnel partners to the V(X)LAN segment.
	ppp0/usb	Access via tunnel partners to the mobile wireless interface of the device.
	Device	Access via tunnel partners to the device.
	SINEMA RC	Access via tunnel partners to the SINEMA RC connection.
ppp0/usb	vlan (1-x) nve x	Access from the mobile wireless interface to the V(X)LAN segment.
	Device	Access from the mobile wireless interface to the device.
	SINEMA RC	Access from the mobile wireless interface to the SINEMA RC connection.
	IPsec (all) IPsec <Connection Name> OpenVPN (all) OpenVPN <Connection Name>	Access from the mobile wireless interface to the tunnel partners that can be reached via all VPN connections (all) or via a certain VPN connection (<Connection Name>).

4.6.3.1 Firewall rules

Firewall rules are automatically created, predefined or specially configured IP rules for data traffic.

Automatic IP firewall rules

The "Auto firewall rules" setting is available for the following functions:

- System > SINEMA RC (Page 177)
- Security > IPsec VPN> Phase 2 (Page 468)
- Security > OpenVPN Client > Connections (Page 472)

The automatically created firewall rules allow packets in the following direction:

From	To	SINEMA RC	IPsec VPN	OpenVPN
Internal	External	✓	✓	✓
External	Internal	✓	✓	✓
Device	External	--	--	✓

From	To	SINEMA RC	IPsec VPN	OpenVPN
External	Device	Predefined IPv4 rules When the connection is created, the following IPv4 services are enabled:		
		HTTP HTTPS SSH Ping	Ping	Ping

Predefined IP firewall rules

The firewall contains predefined IPv4 rules that enable specific IPv4 services on the device.

Specify the interface via which access takes place under "Security > Firewall > Predefined IPv4 (Page 439)".

The following options are available:

- VLANx: VLANs with configured subnet
- WAN interface of the device: pppx, usb0
- VPN connection: SINEMA RC, IPsec and OpenVPN

Factory setting

The firewall is enabled by default. In the delivery state (factory setting), the configuration of the predefined IPv4 rules is as follows:

Service	Access	
	Local access (vlan1) to the device ¹⁾	External access to the device M87x, RM1224, M81x, MUx85x: ppp0/usb0 S615: vlan2
Cloud Connector	-	-
DHCP	✓	✓ (only with S615)
DNS	✓	--
HTTP	✓	--
HTTPS	✓	--
IPsec VPN	--	✓
Ping	✓	--
SMS Relay (only with M87x / RM1224/ MUx85x)	✓	--
TCP event	--	--
SNMP	✓	--
SSH	✓	--
System Time	--	--
Telnet	✓	--

Service	Access	
	Local access (vlan1) to the device ¹⁾	External access to the device M87x, RM1224, M81x, MUx85x: ppp0/usb0 S615: vlan2
VRRP	--	--
VXLAN (only with M876 / RM1224 / MUx85x / S615)	--	--

¹⁾ With SCALANCE M826 and M804PB, only vlan1 is available in the delivery state.

4.6.4 NAT

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

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

You will find information on NAT scenarios that are implemented with the device at the following address: (<https://support.industry.siemens.com/cs/gb/en/view/109744660>)

IP masquerading

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

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

You configure masquerading in "Layer 3" > "NAT" > "IP Masquerading (Page 397)".

NAPT

NAPT (Network Address and Port Translation) is a form of destination NAT and is often called port forwarding. This allows the services of the internal nodes to be reached from external that are hidden by IP masquerading or source NAT.

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

The options are available for port translation:

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

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

You configure NAPT in "Layer 3" > "NAT" > "NAPT (Page 397)".

Source NAT

As with masquerading, in source NAT the source address is translated. In addition to this, the outgoing data packets can be restricted. These include limitation to certain IP addresses or IP address ranges and limitation to certain interfaces.

Source NAT can be used if the internal IP addresses cannot or should not be forwarded externally, for example because a private address range such as 192.168.x.x is used.

You configure source NAT in "Layer 3" > "NAT" > "Source NAT (Page 399)".

NETMAP

With NETMAP it is possible to translate complex subnets to a different subnet. In this translation, the subnet part of the IP address is changed and the host part remains. For translation with NETMAP only one rule is required. NETMAP can translate both the source IP address and the destination IP address. To perform the translation with destination NAT and source NAT, numerous rules would be necessary. NETMAP can also be applied to VPN connections.

You configure NETMAP in "Layer 3" > "NAT" > "NETMAP (Page 401)".

4.6.5 NAT and firewall

The firewall and NAT router support the "Stateful Inspection" mechanism. If the IP data traffic from internal to external is enabled, internal nodes can initiate a communications connection into the external network.

The reply frames from the external network can pass through the NAT router and firewall without it being necessary for their addresses to be included extra in the firewall rule and the NAT address translation. Frames that are not a reply to a query from the internal network are discarded without a matching firewall rule.

NAT translation and firewall rules

Example of NAT translations

NAT rule							
	Type	Source Interface	Destination Interface	Source IP Subnet	Source IP translated subnet	Destination IP Subnet	Translated destination IP
①	Source	vlan1 (internal)	vlan2 (external)	192.168.1.0/24	10.100.1.0/24	10.10.10.0/24	-
The rule applies to packets sent from vlan1 (internal) to vlan2 (external). With the packets that arrive at vlan1 there is a check to establish whether the rule applies. If the source IP address in the subnet of the sender (Source IP subnet) and the destination IP address in the subnet of the recipient (Source IP subnet), the source IP address is replaced by the suitable IP address from the "Translated source IP subnet". The subnet part of the source IP address is changed and the host part remains unchanged. A packet, for example with the source IP address 192.168.1.102 is changed to 10.100.1.102. For the devices connected to vlan2 it appears as if the packets were sent from the IP subnet 10.100.1.0/24. This allows for example overlaps of IP subnets to be resolved. The rule is only specified for the send direction. The retranslation is performed implicitly. If the rule does not apply, the packets are forwarded without translation.							
②	Destination	vlan2 (external)	vlan1 (internal)	10.10.10.0/24	-	10.100.1.0/24	192.168.1.0/24
The rule applies to packets sent from vlan2 (external) to vlan1 (internal). With the packets that arrive at vlan2 there is a check to establish whether the rule applies. If the source IP address in the subnet of the sender (Source IP subnet) and the destination IP address in the subnet of the recipient (Source IP subnet), the source IP address is replaced by the suitable IP address from the "Translated destination IP subnet". A packet, for example with the source IP address 10.10.10.102 is changed to 192.168.1.102. The devices connected to vlan1 can communicate with the devices connected to vlan2. This assumes that the corresponding firewall rule is set. The devices connected to vlan2 must address the devices connected to vlan1 with the virtual IP address from the subnet 10.100.1.0.							

Firewall rules for the NAT rules ① and ②

Example 1:

These IP rules allow the IP data traffic for all devices for the specified direction.

NAT rule	IP rules						Description
	Action	From	To	Source (Range)	Destination (Range)	Service	
①	Accept	vlan1 (internal)	vlan2 (external)	192.168.1.0/24 (Source IP subnet)	10.10.10.0/24 (Destination IP subnet)	all	All packets sent from vlan1 (internal) to vlan2 (external) are allowed to pass. This IP packet filter rule applies to the devices connected to vlan1.
②	Accept	vlan2 (external)	vlan1 (internal)	192.168.1.0/24 (Translated Destination IP Subnet)	10.100.1.0/24 (Destination IP subnet)	all	All packets sent from vlan2 (external) to vlan1 (internal) are allowed to pass.

Example 2:

These IP rules restrict the IP data traffic to a specific device.

NAT rule	IP rules						Description
	Action	From	To	Source (Range)	Destination (Range)	Service	
①	Accept	vlan1 (internal)	vlan2 (external)	192.168.1.20/32 (Source IP subnet)	10.10.10.0/24 (Destination IP subnet)	all	Only packets sent to vlan2 (external) from the IP address 192.168.1.20 are allowed to pass.
②	Accept	vlan2 (external)	vlan1 (internal)	192.168.1.20/32 (Translated Destination IP Subnet)	10.100.1.0/24 (Destination IP subnet)	all	Only packets sent from vlan2 (external) to the IP address 192.168.1.20 are allowed to pass.

4.6.6 Certificates

Certificate types

The device uses different certificates to authenticate the various nodes.

Certificate		Is used in...
CA certificate	The CA certificate is a certificate issued by a Certificate Authority from which the server, device and partner certificates are derived. To allow a certificate to be derived, the CA certificate has a private key signed by the certificate authority. The key exchange between the device and the VPN gateway of the partner takes place automatically when establishing the connection. No manual exchange of key files is necessary.	IPsec VPN (Page 458)
Server certificate	Server certificates are required to establish secure communication (e.g. HTTPS, VPN...) between the device and another network participant. The server certificate is an encrypted SSL certificate. The server certificate is derived from the oldest valid CA, even if this is "out of service". The crucial thing is the validity date of the CA.	SINEMA RC (Page 314)
Device certificate	Certificates with the private key (key file) with which the device identifies itself.	IPsec VPN (Page 458)
Partner certificate	Certificates with which the VPN gateway of the partner identifies itself with the device.	IPsec VPN (Page 458)

File types

File type	Description
*.crt	File that contains the certificate.
*.p12	In the PKCS12 certificate file, the private key is stored with the corresponding certificate and is password protected. The CA creates a certificate file (PKCS12) for both ends of a VPN connection with the file extension ".p12". This certificate file contains the public and private key of the local station, the signed certificate of the CA and the public key of the CA.
*.pem	Certificate and key as Base64-coded ASCII text.

4.6.7 VPN

The device supports the following VPN systems

- IPsec VPN
- OpenVPN

4.6.7.1 IPsec VPN

You configure the IPsec connections in "Security" > "IPsec VPN (Page 458)".

With IPsec VPN, the frames are transferred in tunnel mode. To allow the device to establish a VPN tunnel, the remote network must have a VPN gateway as the partner.

For the VPN connections, the device distinguishes two modes:

- **Roadwarrior mode**
In this mode either the address of the partner is fixed or an IP range is entered from which the connections are taken. The device learns the reachable remote subnets from the partner.
- **Standard mode**
In this mode the address of the partner or the remote subnet is entered permanently. The device can either establish the connection actively as a VPN client or wait passively for connection establishment by the partner.

The IPsec method

The device uses the IPsec method in the tunnel mode for the VPN tunnel. Here, the frames to be transferred are completely encrypted and provided with a new header before they are sent to the VPN gateway of the partner. The frames received by the partner are decrypted and forwarded to the recipient.

To provide security, the IPsec protocol suite uses various protocols:

- The IP Authentication Header (**AH**) handles the authentication and identification of the source.
- The Encapsulation Security Payload (**ESP**) encrypts the data.

- The Security Association (**SA**) contains the specifications negotiated between the partners, e.g. about the lifetime of the key, the encryption algorithm, the period for new authentication etc.
- Internet Key Exchange (**IKE**) is a key exchange method. The key exchange takes place in two phases:
 - Phase 1
In this phase, no security services such as encryption, authentication and integrity checks are available yet since the required keys and the IPsec SA still need to be created. Phase 1 serves to establish a secure VPN tunnel for phase 2. To achieve this, the communications partners negotiate an ISAKMP Security Association (ISAKMP SA) that defines the required security services (algorithms, authentication methods used). The subsequent messages and phase 2 are therefore secure.
 - Phase 2
Phase 2 serves to negotiate the required IPsec SA. Similar to phase 1, exchanging offers achieves agreement about the authentication methods, the algorithms and the encryption method to protect the IP packets with IPsec AH and IPsec ESP. The exchange of messages is protected by the ISAKMP SA negotiated in phase 1. Due to the ISAKMP SA negotiated in phase 1, the identity of the nodes is known and the method for the integrity check already exists.

Authentication method

- CA certificate, device and partner certificate (digital signatures)
The use of certificates is an asymmetrical cryptographic system in which every node (device) has a pair of keys. Each node has a secret, private key and a public key of the partner. The private key allows the device to authenticate itself and to generate digital signatures.
- Pre-shared key
The use of a pre-shared key is a symmetrical cryptographic system. Each node has only one secret key for decryption and encryption of data packets. The authentication is via a common password.

Local ID and remote ID

The local ID and the remote ID are used by IPsec to uniquely identify the partners (VPN end point) during establishment of a VPN connection.

Encryption methods

The following encryption methods are supported. The selection depends on the phase and the key exchange method (IKE)

	Phase 1		Phase 2	
	IKEv1	IKEv2	IKEv1	IKEv2
3DES	x	x	x	x
AES128 CBC	x	x	x	x
AES192 CBC	x	x	x	x
AES256 CBC	x	x	x	x

4.6 Security functions

	Phase 1		Phase 2	
	IKEv1	IKEv2	IKEv1	IKEv2
AES128 CTR	-	x	x	x
AES192 CTR	-	x	x	x
AES256 CTR	-	x	x	x
AES128 CCM 16	-	x	x	x
AES192 CCM 16	-	x	x	x
AES256 CCM 16	-	x	x	x
AES128 GCM 16	-	x	x	x
AES192 GCM 16	-	x	x	x
AES256 GCM 16	-	x	x	x

x: is supported

-: is not supported

Default Ciphers

During connection establishment a preset list can be transferred to the VPN connection partners. The list contains combinations of the three algorithms (Encryption, Authentication, Key Derivation). To establish a VPN connection, the VPN connection partner must support at least one of these combinations. The combinations depend on the phase and the key exchange method IKE).

Combination			Phase 1		Phase 2	
Encryption	Authenticat-ion	Key derivation	IKEv1	IKEv2	IKEv1	IKEv2
AES128	SHA1	DH Group 14	x	x	x	x
AES256	SHA512	DH Group 16	x	x	x	x
AES128 CCM 16	SHA256	DH Group 14	-	x	x	x
AES256 CCM 16	SHA512	DH Group 16	-	x	x	x
AES128	SHA1	none	-	-	x	x
AES256	SHA512	none	-	-	x	x
AES128 CCM 16	SHA256	none	-	-	x	x
AES256 CCM 16	SHA512	none	-	-	x	x

x: Combination is part of the default cipher

-: Combination is not part of the default cipher

none: For phase 2, no separate keys are exchanged. This means that Perfect Forward Secrecy (PFS) is disabled.

Requirements of the VPN partner

The VPN partner must support IPsec with the following configuration to be able to establish an IPsec connection successfully:

- Authentication with partner certificate, CA certificates or pre-shared key
- IKEv1 or IKEv2
- Support of at least one of the following DH groups: Diffie-Hellman group 1, 2, 5 and 14 - 18

- 3DES or AES encryption
- MD5, SHA1, SHA256, SHA384 or SHA512
- Tunnel mode

If the VPN partner is downstream from a NAT router, the partner must support NAT-T. Or, the NAT router must know the IPsec protocol (IPsec/VPN passthrough).

NAT traversal (NAT-T)

There may be a NAT router between the device and the VPN gateway of the remote network. Not all NAT routers allow IPsec frames to pass through. This means that it may be necessary to encapsulate the IPsec frames in UDP packets to be able to pass through the NAT router.

Dead peer detection

This is only possible when the VPN partner supports DPD. DPD checks whether the connection is still operating problem free or whether there has been an interruption on the line. Without DPD and depending on the configuration, it may be necessary to wait until the SA lifetime has expired or the connection must be reinitiated manually. To check whether the IPsec connection is still problem-free, the device itself sends DPD queries to the VPN partner station. If the VPN partner station does not reply after a certain time has elapsed, the connection to the VPN partner station will be declared invalid. You configure the settings for DPD in phase 1.

4.6.7.2 OpenVPN

With OpenVPN, virtual private networks (VPN) can be established. As an OpenVPN client, the device can establish a VPN connection to a remote network.

You configure the OpenVPN client in "Security" > "OpenVPN Client (Page 471)".

The VPN connection is established via virtual device drivers, the TAP and TUN device. During this, virtual network interfaces are created that act like a physical interface of the device and represent the endpoint of the VPN tunnel.

The device supports the following:

- TUN device: Routing mode
The LAN Interface and the virtual network interface are located in different IP subnets. The virtual tunnel interface is assigned a virtual IP address from a devised subnet by the OpenVPN server. The IP packets (layer 3) are routed between the virtual tunnel interface and the LAN interface.

Authentication

The following options are available for authenticating the OpenVPN client at the OpenVPN server:

- **Certificates: CA certificate and device certificate**
The use of certificates is an asymmetrical cryptographic system. Each node (device) has a secret, private key and a public key of the partner. The private key allows the device to authenticate itself and to generate digital signatures.
- **User name / password**
Access is restricted by a user name and a password.
- **Certificates and user name / password**
If both authentication methods are successful, the VPN connection is established.

Encryption methods

The device also supports the following methods:

- BF CBC
- AES128 CBC
- AES192 CBC
- AES256 CBC
- DES EDE3

4.6.7.3 VPN connection establishment

The device supports the following options for establishing a VPN connection.

- OpenVPN: Security > OpenVPN > Connections (Page 472)
- IPsec VPN: Security > IPsec VPN > Connections (Page 461)
- SINEMA RC: System > SINEMA RC (Page 314)

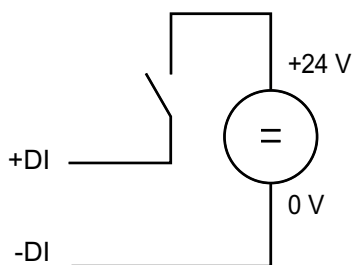
Options	Use			Description
	OpenVPN	IPsec VPN	SINEMA RC ¹⁾	
start	x	x	-	The device is "active", in other words, it attempts to establish a connection to a partner. The partner is addressed using its configured WAN IP address or the configured FQDN.
wait	-	x	-	The device is "passive", in other words, it waits for the partner to initiate the connection.

Options	Use			Description
	OpenVPN	IP-sec VPN	SINEMA RC ¹⁾	
on demand	-	x	-	The device attempts to establish a connection to a partner when necessary. The receipt of requests for VPN connection establishment is also possible. For the configured local and remote subnets, an entry is created in the routing table. If a node attempts to send data packets via the VPN tunnel from one of the networks, the VPN connection is established. The settable timeout has the effect that after this time without any further data packets the VPN tunnel is terminated again.
Start on DI	x	x	x	Connection establishment is controlled via the digital input (DI).
Wait on DI	-	x	-	
Digital Input & Wake-up SMS	-	-	x	Connection establishment is controlled via the digital input (DI) or SMS.
Wake-up SMS	-	-	x	Connection establishment is controlled via SMS.
start on SMS	x	x	-	
wait on SMS	-	x	-	
Auto	-	-	x	The device adopts the settings of the SINEMA RC server. You configure the settings on the SINEMA RC server in "Remote connections > Devices". You can find additional information on this topic in the operating instructions "SINEMA RC Server".
Permanent	-	-	x	The device establishes a VPN connection to the SINEMA RC Server. The VPN tunnel is maintained permanently.

¹⁾ KEY-PLUG SINEMA REMOTE CONNECT required

Digital input (DI)

The establishment of the VPN tunnel can also be controlled via the digital input, e.g. using a button. When the button is closed, voltage is applied to the digital input and the LED of the digital input lights up. The lit LED indicates that signal 1 (TRUE / HIGH) is applied. Signal 1 triggers an event on the device with which the establishment of the VPN tunnel is controlled. You will find information on connecting and the maximum current load in the operating instructions of the devices.



Requirement

- In "System > Events > Configuration (Page 230)" for the "Digital Input" event "VPN Tunnel" is activated.
If this setting is not activated, the event is not passed on to the VPN connection.

Options

The device supports the following options for controlling the VPN tunnel via the digital input:

- Start on DI
If the event "Digital Input" occurs, the device becomes "active". The device tries to establish a VPN connection to a remote station (OpenVPN, IPsec, SINEMA RC). SCALANCE M804PB starts the integrated TIA Portal Cloud Connector.
- Wait on DI
If the event "Digital Input" occurs, the device becomes "passive". The device waits until the connection establishment is initiated by the remote station (OpenVPN, IPsec).
- Digital input & Wake-up SMS (only with M87x / RM1224 / MUx85x)
If the event "Digital In" occurs or the device receives a wake-up SMS message, the device becomes "active". The device attempts to establish a VPN connection to the SINEMA RC server.

SMS (only with M87x / RM1224 / MUx85x)

Requirement

- In "System > SMS > SMS Command (Page 292)" you specify who a command SMS of the class "System" will be accepted from.
- In "System > SMS > Event SMS", the function is enabled and the telephone number of a recipient is configured.
- If this setting is not activated, the event is not passed on to the VPN connection.

Options

The device supports the following options for controlling the VPN tunnel via an SMS message:

- start on SMS
When the device receives a command SMS message, the device becomes "active". The command SMS message contains the name of the VPN connection (OpenVPN, IPsec). The device attempts to establish a connection to the partner specified in the VPN connection.
Format of the SMS message:
Establishment of the VPN connection:
 - OpenVPN: SYS OVPN UP <name of the OpenVPN connection>, see Command SMS message (Page 489).
If you enter a "*" for <name of the OpenVPN connection>, the OpenVPN connections are established that are set in "Operation" "start on SMS".
 - IPsec VPN: SYS IPSEC UP<name of the IPsec VPN connection>, see Command SMS message (Page 489).
If you enter a "*" for <name of the IPsec VPN connection>, the IPsec VPN connections are established that are set in "Operation" "start on SMS".Termination of the VPN connection:
 - OpenVPN: SYS OVPN DOWN <name of the OpenVPN connection>, see Command SMS message (Page 489).
If you enter a "*" for <name of the OpenVPN connection>, the OpenVPN connections are terminated that are set in "Operation" "start on SMS".
 - IPsec VPN: SYS IPSEC DOWN<name of the IPsec VPN connection>, see Command SMS message (Page 489).
If you enter a "*" for <name of the IPsec VPN connection>, the IPsec VPN connections are terminated that are set in "Operation" "start on SMS".
- wait on SMS
When the device receives a command SMS message, the device is "passive". The command SMS message contains the name of the IPsec VPN connection. The device waits for the partner specified in the IPsec VPN connection to initiate the connection.
Format of the SMS message:
If you enter a "*" for <name of the IPsec VPN connection>, the IPsec VPN connections are established that are set in "Operation" "start on SMS".
 - IPsec VPN: SYS IPSEC UP<name of the IPsec VPN connection>, see Command SMS message (Page 489).
If you enter a "*" for <name of the IPsec VPN connection>, the IPsec VPN connections are established that are set in "Operation" "start on SMS".
 - IPsec VPN: SYS IPSEC DOWN<name of the IPsec VPN connection>, see Command SMS message (Page 489).
If you enter a "*" for <name of the IPsec VPN connection>, the IPsec VPN connections that have "wait on SMS" set for "Operation" are terminated.

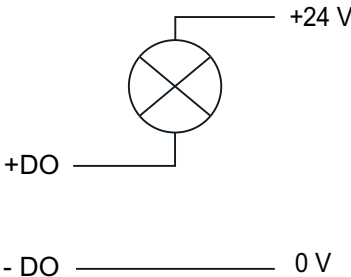
4.6 Security functions

- **Digital Input & Wake-up SMS**
The settings of the SINEMA RC server are ignored. If the event "Digital In" occurs or the device receives a wake-up SMS message. The device attempts to establish a VPN connection to the SINEMA RC Server.
Format of the SMS message: SYS SRC UP <address of the SINEMA RC Server>, see Command SMS message (Page 489).
- **Wake-up SMS**
The settings of the SINEMA RC server are ignored. When the device receives a wake-up SMS message, it attempts to establish a VPN connection to the SINEMA RC Server.
Format of the SMS message:
 - SYS SRC UP <address of the SINEMA RC Server>, see Command SMS message (Page 489).

Notification options

If the status of the digital input or a VPN tunnel (IPsec, OpenVPN, SINEMA RC) changes, the device provides several options for notification on the "Events (Page 230)" page.

Type of notification	Digital input	VPN tunnel	Behavior if there is a status change
E-mail	x	x	The device sends an e-mail. 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. Requirement: • An SMTP server is set up. • In "System > SMTP Client" the function is activated, a recipient and the IP address of the SMTP server are configured.
Trap	x	x	The device sends an SNMP trap. Requirement: • "SNMPv1 traps" is enabled in "System > Configuration". • In "System > Configuration > Traps" a recipient is configured to which the device sends the SNMP traps.
Log table	x	x	The device writes an entry in the event log table. The content of the event log table is displayed in "Information > Log Table".
Syslog	x	x	The device writes an entry to the Syslog server. Requirement: • A Syslog server has been set up. • In "System > Syslog Client" the function is activated and the IP address of the Syslog server is configured.
Fault LED	x	-	The fault LED lights up on the device.

Type of notification	Digital input	VPN tunnel	Behavior if there is a status change
Digital input	x	x	Controls the digital output or signals the status change with the "DO" LED. A consumer can be connected to the digital output. You will find information on connecting in the operating instructions of the devices. The consumer signals a status change.  Note You can control the digital output directly via CLI or SNMP. In WBM and CLI, you can configure the use of the digital output in "Events". Do not control the digital output directly when you use this in the WBM and CLI.
SMS (only with M87x, RM1224, MUx85x)	x	x	The device sends an SMS message with a standard text. Requirement: In "System > SMS > Event SMS " the function is activated and the telephone number of a recipient is configured.
	x	-	The device sends an SMS message with a user-defined text. You configure text in "System > SMS > Event SMS". Requirement: - In "System > SMS > Event SMS " the function is activated, the telephone number of a recipient and the text are configured. - In "System > Events > Configuration", "SMS" is activated for the "Digital Input" event.
Read the status of the MIB variable	x	-	Using the private MIB variable snMspDigitalInputLevel, you can read out the status of the digital input. - OID of the private MIB variable snMspDigitalInputLevel: <pre>iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).siemens(4329).industrialComProducts(20).iComPlatforms(1).simaticNet(1).snMsp(1).snMspCommon(1).snMspDigitalIO(39).snMspDigitalIOObjects(1).snMspDigitalInputTable(2).snMspDigitalInputEntry(1).snMspDigitalInputLevel(6)</pre> - values of the MIB variable 1: Signal 0 at the digital input (DI) 2: Signal 1 at the digital input (DI)

4.7 Redundancy

4.7.1 Spanning Tree

Avoiding loops on redundant connections

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

Definition of the network topology using the configuration frames

The devices exchange configuration frames known as BPDUs (Bridge Protocol Data Units) with each other to calculate the topology. The root bridge is selected and the network topology created using these frames. BPDU frames in connection with the Spanning Tree method also bring about the status change of the root ports.

The root bridge is the bridge that controls the spanning tree algorithm for all involved components.

Once the root bridge has been specified, each device sets a root port. The root port is the port with the lowest path costs to the root bridge.

Response to changes in the network topology

If nodes are added to a network or drop out of the network, this can affect the optimum path selection for data packets. To be able to respond to such changes, the root bridge sends configuration messages at regular intervals. The interval between two configuration messages can be set 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 only started with the new topology after all the bridges have the required information.

4.7.1.1 RSTP

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.

4.7.2 VRRPv3

Router redundancy with VRRPv3

With the Virtual Router Redundancy Protocol v3 (VRRPv3), the failure of a router in a network can be countered. Version 3 of VRRP (RFC 5798) is based on version 2 (RFC 5798).

VRRP can only be used with virtual IP interfaces (VLAN interfaces).

Several VRRP routers in a network segment are put together as a logical group representing a virtual router (VR). The group is defined using the virtual ID (VRID). Within the group, the VRID must be the same. The VRID can no longer be used for other groups.

A virtual IP address and a virtual MAC address are assigned to the virtual router. One of the VRRP routers within the group is specified as the master router. The master router has priority 255. The other VRRP routers are backup routers. The master router assigns the virtual IP address and the virtual MAC address to its network interface. The master router sends VRRP packets (advertisements) to the backup routers at specific intervals. With the VRRP packets, the master router signals that it is still functioning. The master router also replies to the ARP queries.

If the virtual master router fails, a backup router takes over the role of the master router. The backup router with the highest priority becomes the master router. If the priority of the backup routers is the same, the higher MAC address decides. The backup router becomes the new virtual master router.

The new virtual master router adopts the virtual MAC and IP address. This means that no routing tables or ARP tables need to be updated. The consequences of a device failure are therefore minimized.

You configure VRRP in "Layer 3 > VRRPv3 (Page 405)".

Configuring with Web Based Management

5.1 Web Based Management

To access Web Based Management (WBM) of the device, you establish a remote connection between a client PC and a device over the network.

The device has an integrated HTTPS server for Web Based Management (WBM). When you address the device using an Internet browser, it returns HTML pages to the client PC depending on the user inputs.

Requirements

- The device has an IP address.

Note

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

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

Note

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

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

WBM display

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

- Mozilla Firefox
- Google Chrome
- Microsoft Edge

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

5.2 Starting and logging in

Establishing a connection to a device

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

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

Note

Information on the security certificate

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

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

If you use a port other than the standard port, enter a colon ":" as separator between the IP address and the port number.

Example: https://192.168.16.178:49152

You change the port in "System > Configuration".

If there is a connection to the device, the login page of Web Based Management (WBM) is displayed.

If you wish to access the WBM via a non-secure HTTP connection, activate the HTTP server under "System > Configuration". On the next login, click on the link "Switch to insecure HTTP" on the login page or enter "http://" and the IP address of the device in the address box of the web browser.

SIEMENS

English Go

Name

Password

Login

?

LOGIN

Name:

Password:

Login

For information about browser compatibility please refer to the manual

Device is in Factory Settings

Changing language

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

Note

Available languages

English and German are available as languages.

Login with a configured user account

You have the following options for logging in via HTTPS. You either use the login option in the center of the browser window or the login option in the upper left area of the browser window. The following steps apply, whichever of the above options you choose.

1. "Name" input box:
Enter the user name of the created user account. You configure local user accounts and roles in "Security > Users".
2. "Password" input box:
Enter the password of the relevant user account.
3. Click "Log in" or confirm your input with "Enter".

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

Initial login

When you log in for the first time or following a "Restore Factory Defaults and Restart", use the following user name and the associated password:

Name	admin
Password	admin

Note

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

After you confirm your input with "Log in" or "Enter", a dialog is shown which prompts you to change the default password. You also have the possibility to replace the default HTTPS certificate with your own HTTPS certificate. For more information on certificates, refer to the WBM manual, section "File list (Page 212)".

Updating the HTTPS certificate

1. Click "Certificate Update" in the dialog.
You are redirected to the "Certificate Update" page.
2. Click the "Load" button.
The dialog for loading a file opens.
3. Go to the certificate file you want to load.
4. Click the "Open" button in the dialog.
The certificate is now loaded.
5. Enter a password for "Password" and confirm it by entering it again.
Click "Delete" to delete the certificate.
6. To continue, click "Skip to Default Password Change".

Changing the default user and their password

If you have confirmed the dialog with OK or updated the HTTPS certificate, you are redirected to the "Account Passwords" page.

1. "Current User Password" input box:
Enter the password "admin" for the factory-preset user "admin".

Note

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

2. "New name for the Admin user account" input box:
You can rename the user preset in the factory "admin" once. Afterwards, renaming "admin" is no longer possible.
Enter "admin" or a new name for the "admin" user.

3. "New Password" input box
Enter a new password for the admin user account.
The new password must meet the password policy "High":
 - Password length: At least 8 characters, maximum 128 characters
 - At least 1 uppercase letter
 - At least 1 special character (special characters | \$? " ; : \ ' ^ * ~ ° € μ ä ö ü Ä Ö Ü are not permitted)
 - At least 1 number
 - The characters for Space and Delete also cannot be contained.
 Repeat the password to confirm. The password entries must match.
4. Click the "Set Values" button to complete the action.
The changes take immediate effect. Access via DCP is write-protected after the admin password is changed. The network parameters can be read with SINEC PNI or with "DCP Discovery" but cannot be changed.

Personalizing the login page

You can show an additional text on the login page.

1. Create a txt file that contains the desired text or the ASCII type. With ASCII type, pictograms, e.g. the Siemens company logo, are displayed based on the available characters. Up to 50 text lines with 255 characters each including spaces are supported.

Note

The use of the following special characters is not supported:

- Backslash (\)
 - Question mark (?)
 - Tabs: Use spaces instead of tabs
-

2. Load the text file into the device using "System > Load&Save". To do so, use the "Upload" button in the table row "LoginWelcomeMessage" regardless of the protocol used.
3. Log out. The configured text is shown below the login data on the login page.

Protection from brute force attacks

To protect against brute force attacks, login to the device is denied for a user or for the IP address of a user after multiple failed login attempts. By default, the number of login attempts is preset to 12 per user and 10 per IP address. The wait time for which the page is locked for new login attempts increases after each invalid login attempt. You can change these settings on the page "Security > Brute Force Prevention (Page 479)".

5.3 Updating the HTTPS certificate

When you log in for the first time or after a "Restore Factory Defaults and Restart" action, you have the option of replacing the default HTTPS certificate with your own HTTPS certificate. After the initial login, click "Certificate Update" in the dialog. You are redirected to the "Certificate Update" page.

For more information on certificates, refer to the WBM manual, section "File list (Page 212)".

Certificate Update

Skip to Default Password Change

Description	Load	Delete	Password	Password Confirmation
HTTPS Certificate	Load	Delete		

Description

The page contains the following box:

- **Skip to Default Password Change**
Click the button to not update the certificate.

The table has the following columns:

- **Description**
Displays the short description of the file.
- **Upload**
With this button, you can load files onto the device.
- **Delete**
With this button, you can delete files from the device. The button can only be enabled if the file exists on the device.

Note

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

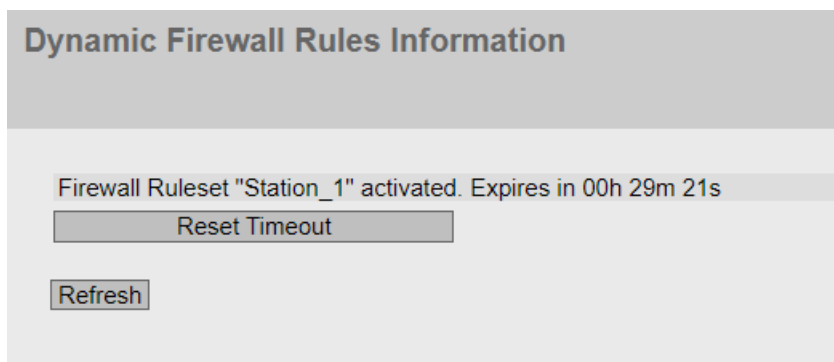
- **Password**
Enter the password for the file.
Entered passwords cannot be read as plain text; instead asterisks * are displayed.
- **Password Confirmation**
Confirm the new password.

Procedure

To upload a new HTTPS certificate to the device, do the following:

1. Click the "Load" button.
The dialog for loading a file opens.
2. Go to the certificate file you want to load.

3. Click the "Open" button in the dialog.
The certificate is now loaded.
4. Enter a password for "Password" and confirm it by entering it again.
Click "Delete" to delete the certificate.
5. To continue, click "Skip to Default Password Change".



After successful login, the WBM page "Information on dynamic firewall rules" opens.

The current ruleset and the remaining time are displayed. If needed, the user can extend the access time via the "Reset Timeout" button.

Service technician login

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

5.4 "Wizard" menu

5.4.1 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.

The scope of the Basic Wizard pages depends on the device.

Requirement

- The device has an IP address and can be reached via the Ethernet interface.
- You are logged on in the WBM as a user with administrator rights.
- M87x / RM1224: There is a mini SIM card in the device.

- MUM85x: There is a micro SIM card in the device
- When shipped or following a "Restore Factory Defaults and Restart" the device can be reached with the values preset in the factory. For more detailed information, refer to the section "Requirements for operation (Page 42)".

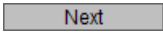
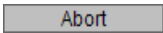
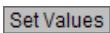
Starting the Basic Wizard

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

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

Buttons you require often

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

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

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

5.4.2 IP

Introduction

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

Basic Wizard: IP Settings

IP	Device	SIM	Operator	Time	DDNS	SINEMA RC	Summary

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

Internal (vlan1)

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Create new Gateway

IP Address: 0.0.0.0

Abort

Next

Description

The Basic Wizard page contains the following boxes:

- IP Address**
Enter an IP address that is unique within your network.
- Subnet Mask**
Enter the subnet mask of the device.
- DHCP (Only with M826)**
Shows the DHCP client setting on vlan1.
When enabled, the device receives the IP address and subnet mask settings from a DHCP server.

- **Gateway (DHCP)** (only with M826)
Shows the IP address of the gateway when the DHCP server transmits it.
- **Create new gateway**
You define the gateway in this area.
 - IP Address
Enter the IP address of the default gateway to be able to communicate with devices in another subnet.

5.4.3 Device

Introduction

On this Basic Wizard page, you configure the general device information.

Basic Wizard: Device Settings

IP	Device	Time	DDNS	SINEMA RC	Summary

To allow better identification of the device, you can specify general device information. Here, you can enter any name for this device providing it is unique. Normally, this is the node's fully-qualified domain name. By providing a unique name you can identify the device within the context of the application. You also can enter the contact person responsible for the device and the identifier for the location at which the device is installed, for example the room number.

System Name:

System Location:

System Contact:

Previous

Abort

Next

Description

The Basic Wizard page contains the following boxes

- **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.
- **System Location**
You can enter the location where the device is installed. The location is displayed in the selection area. A maximum of 255 characters are possible.

Note

Permitted characters

The following printable ASCII characters (0x20 to 0x7F) are permitted in the input fields:

- 0123456789
- A...Z a...z
- !"#\$%&'()*+,-./:;<=>?@ [\]_{}~^`

-
- **System Contact**
You can enter a contact person responsible for managing the device. A maximum of 255 characters are possible.

5.4.4

DSL

M81x

On this Basic Wizard page, you configure the DSL access and the parameters for the virtual connection via which the packets will be transferred.

Basic Wizard: DSL

IP	Device	DSL	Time	DDNS	SINEMA RC	Summary

Here, you configure the DSL access and the parameters for the virtual connection via which the packets will be transferred. This is only possible if the DSL connection is activated by your DSL provider. For the access you need the following access data: User name, Password, VCI / VPI and Encapsulation.

☐ Enable DSL Interface
☐ Enable PPPoE Passthrough

Account:
 Password:
 VCI:
 VPI:
 Encapsulation:
 Protocol:
 Noise Margin Delta DS:
☐ Forced Disconnect
 Time for Forced Disconnect:

Description

The page contains the following:

- **Enable DSL Interface.**
Enable or disable the DSL interface.
- **Enable PPPoE Passthrough**
 - Enabled
The device acts as a modem. The settings "User Account", "Password" and "Forced Disconnect" cannot be edited. Only a connected device can use the DSL connection. This device also handles the authentication (dial-in) with the provider.
 - Disabled
The device acts as a router and logs in with the user name and password. All connected devices can use the DSL connection.
- **Account**
Enter the user name. You will receive the user name from your DSL provider.
- **Password**
Enter the password. You will receive the password from your DSL provider.
- **VCI (Virtual Channel Identifier)**
Enter the ID for the virtual channel. You will receive setting from your DSL provider.

- **VPI (Virtual Path Identifier)**
Enter the ID for the virtual path. You will receive setting from your DSL provider.
- **Encapsulation**
The data packets are encapsulated in the required protocol.
The following options are available:
 - vc-mux (virtual circuit multiplexing)
 - LLC (Logical Link Control)
- **Protocol**
Specify the protocol for the Internet connection. You obtain this information from your DSL provider.
 - PPPoE (Point-to-Point over Ethernet)
The PPP data is encapsulated in an Ethernet frame.
 - PPPoA (Point-to-Point over ATM)
The PPP data is encapsulated in ATM AAL5 (Adaptation Layer 5). If you select PPPoA, the setting "Enable PPPoE Passthrough" is disabled.
- **Noise Margin Delta DS**
Specify the margin to the background noise.
- **Forced Disconnect**
After a certain time, the DSL provider terminates the connection. Enable this option if you want to shift the forced disconnect of your provider to a specific time of day, for example at night outside normal office hours.
- **Time for Forced Disconnect**
Specify the time of day to which you want to shift the forced disconnect of the DSL provider. This is only possible if the correct system time is set on the device.
Input format: HH:MM

5.4.5 SHDSL

M826

On this Basic Wizard page, you configure the role and the transfer profile for the interface.

SHDSL

IP

Device

SHDSL

Time

DDNS

SINEMA RC

Summary

Here, you configure the profile for the transfer and the role for the SHDSL interface. If you use a predefined profile, the Link Data Rate is set automatically. After completing the Basic Wizard, you can configure other settings, for example the modulation method.

☐ Enable PME Aggregation Function

SHDSL 1

Status:

enabled

Role:

Central Office (CO)

Predefined Profile:

Reliability

SHDSL 2

Status:

enabled

Role:

Customer Premises Equipment (CPE)

Predefined Profile:

Reliability

Previous

Abort

Next

Description

The page contains the following:

- Enable PME Aggregation Function**
PME = Physical Medium Entities
When enabled, the SHDSL interfaces or the 2-wire cables are put together to form a single connection with a higher transmission rate.

Note

If the "Enable PME Aggregation Function" is selected, each of the interfaces of a device must have the same role.

The following can be configured for every SHDSL interface:

- **Status**
Specify whether or not the interface will be used.
- **Role**
Specify the role:
 - Central Office (CO)
The interface is a central office.
 - Customer Premises Equipment (CPE)
The interface is an end node device.
- **Predefined Profile**
Specify the profile for the transfer. If you use a profile, the following parameters are set automatically.
 - Profiles with a transfer range
If during calibration of the cable the measured value is within the range, the SHDSL connection is established.

	Link data rate min - max	
Standard	192 - 5696	For medium and longer cable lengths
Reliability	192 - 5696	When operating several SHDSL connections simultaneously.
Extended	64 - 15296	For short and long cable length

- Profiles with a fixed preset transmission rate
If during calibration of the cable the measured value precisely matches the fixed preset transmission rate, and SHDSL connection is established.

	Link Data Rate
Fixed (high data rate)	5696
Fixed (medium data rate)	3072
Fixed (low data rate)	512

5.4.6 SIM

M87x

RM1224

MUx85x

For access to the mobile wireless network and the mobile wireless services, the following access parameters are necessary. You will receive the access parameters from your mobile wireless provider.

Description

The Basic Wizard page contains the following:

- **Enable Mobile Network Interface**
Enable or disable the mobile wireless interface. The mobile wireless WLAN interfaces are disabled when the device is supplied.
- **PIN**
Enter the PIN of the SIM card. You obtain the PIN from your mobile wireless provider. The device also works with SIM cards without a PIN, in this case leave the box empty.

Note

If you make incorrect entries, the SIM card is blocked

Make sure that you enter the PIN correctly. If you enter the PIN incorrectly more than three times, the SIM card will be blocked.

In "Information > Mobile", you can check the status of the SIM card. If "SIM Status" displays "PUK required", the SIM card is locked.

You can change the PIN or unlock the SIM card under "Interfaces > Mobile > SIM".

- **PIN Confirmation**
Repeat the PIN.

- **Radio Mode**

Select the required mobile wireless network. The following options are available:

- Auto (not with the M874-2)
All services. As first choice, the device attempts to establish a connection to the fastest available mobile wireless system.
- GSM only
The EGPRS and GPRS services.
The device ignores the UMTS and LTE network and establishes a connection to the GSM service that provides the highest bandwidth locally
- UMTS only (not with the M874-2)
The UMTS and HSPA service. The device ignores the EGPRS, GPRS and LTE services and establishes a connection in the UMTS network.
- Only LTE (only with M876-4 / RM1224 / MUX85x)
The service LTE. The device ignores the EGPRS and GPRS and UMTS services and establishes a connection in the LTE network.
- 5 G NR + LTE (NSA) (only with MUX85x)
The services 5G New Radio (NR) and LTE non-standalone operation (NSA)
- Only 5 G NR SA (only with MUX85x)
The service 5G New Radio (NR) in standalone operation (SA)
- EVDO (only available with M876-3)
EVolution, Data-Optimized. Default for CDMA-based networks.
The following sub-standards are supported:
 - EVDO Hybrid
 - EVDO 1xRTT
 - EVDO HDR - High Data Rate
- No data connection
There is no data connection. Suitable when the device is only used to send or receive SMS messages.

- **Authentication Method**

Select the required authentication method.

- CHAP
Encrypted transfer of user name and password using the Challenge Handshake Authentication Protocol (CHAP).
- PAP
Unencrypted transfer of user name and password using the Password Authentication Protocol (PAP).
- Auto
User name and password are transferred automatically with one of the following two methods. CHAP has the higher priority. If the communications partner does not support CHAP, the user name and password are transferred using PAP.

- **Allow Data Roaming**

Select the required roaming type. The following options are available:

- Allow roaming
The device automatically logs into an available network if the specified network is unreachable.
- No data roaming
The connection is interrupted when the specified network is not reachable.
- No roaming
The function is disabled.

5.4.7 Operator

M87x

RM1224

MUx85x

The APN (Access Point Name) is the name of the access point from the mobile network to the Internet or to a private company network. Depending on the type of network connected, this is a public or private APN. Information about the APN is provided by the mobile network provider.

Basic Wizard: APN Settings

IP | Device | SIM | Operator | Time | DDNS | SINEMA RC | Summary

Here, you specify the access data for the AP. To use the required PLMNID, select the check box 'Enabled'. If this is not the case, enable 'Manual APN'. Enter the APN, user name and password. Some mobile wireless providers do not use access control with a password. In this case, leave the box empty. For easier handling there is a country and provider list under 'Interfaces > Mobile > Operator'.

PLMNID▼	Operator Name	APN	User Name	Password	Password Confirmation	Enabled
Manual						☐
26207	O2	internet	guest			☒
26203	Eplus	internet.eplus.de	guest			☒
26202	Vodafone	web.vodafone.de	guest			☒
26201	T-Mobile	internet.t-mobile	guest			☒

Previous Abort Next

Description

The page contains the following boxes:

- **Country List**
From this list, select the country in which the device will be deployed.
- **Provider List**
From this list select the appropriate mobile network provider. The list depends on the selected country.
If the mobile network provider is not contained in the list of providers, select "-".

Note

"5G SA (Standalone) only" radio mode

For "5G SA only" radio mode, disable all providers that are not needed.

- **PLMNID**
Each mobile network provider has an identification number that is unique worldwide known as the Public Land Mobile Network ID (PLMN ID). You will find the Net ID in the documentation of your mobile network provider or on their Internet pages.
 - If you know the PLMNID of the mobile network provider, enter this number.
 - If you do not know the PLMNID, enter the data in the table under "Manual".
- **APN**
Enter the name of the APN. You will find the APN in the documentation of your mobile network provider on your provider's Website or ask your mobile network provider's hotline.

5.4 "Wizard" menu

- **User name**
Enter the user name. Some mobile network providers do not use access control with user names and/or passwords. In this case, leave the box empty.
- **Password**
Enter the password. Some mobile network providers do not use access control with user names and/or passwords. In this case, leave the box empty.
- **Password Confirmation**
Repeat the password.

The table contains the following columns:

- **Select**
Select the check box in the row to be deleted.
- **PLMNID**
 - Identification number (Net ID)
Displays the PLMNID of the mobile phone provider.
 - Manual (static APN)
If the PLMNID is not known, enter the APN of your mobile phone provider.
 - Manual (dynamic APN)
Only available with M876-4 / RM1224
Requirement: Radio mode "LTE only"
If you do not configure any data, the APN is assigned dynamically.
- **Operator Name**
Enter the name of your mobile network provider.
- **APN**
Enter the name of the APN. You will find the APN in the documentation of your mobile network provider on your provider's Website or ask your mobile network provider's hotline.
- **User name**
Enter the user name for the APN. Some mobile network providers do not use access control with user names and/or passwords. In this case, leave the box empty.
- **Password**
Enter the password for the APN. Some mobile network providers do not use access control with user names and/or passwords. In this case, leave the box empty.
- **Password Confirmation**
Repeat the password.
- **Enabled**
The entry is used

5.4.8 Time setting

Time setting

On this Basic Wizard page, you set the date and time of the system.

Basic Wizard: Time Settings

IPDeviceSIMOperatorTimeDDNSNEMA RCSummary

Here you set the date and time to check the validity (time) of certificates and for the time stamps of log entries. You can set the system time yourself manually or have it synchronized automatically with a time server. There are a number of time servers on the Internet that can be used to obtain the current time precisely. The Basic Wizard is using NTP for the time server. If you want to use another method, configure these method after completing the Basic Wizard.

☒ Cellular Time

☒ Time Manually

System Time: 10/31/2023 05:13:25

Use PC Time

☐ NTP Client

☐ Secure NTP Client only

Time Zone: +00:00

Select	NTP Server Index	NTP Server Address	NTP Server Port	Poll Interval	Key ID	Hash Algorithm	Key	Key Confirmation
☐	1	0.0.0.0	123	64	1	DES		

Previous

Abort

Next

Description

Manual time setting:

- Cellular Time** (only with MUx85x)
When enabled, the device fetches the time via a mobile wireless network. The time is updated every 60 seconds.
- Time Manually**
Enable or disable manual setting of the time. If you enable the option, the "System Time" input box can be edited.
- System Time**
Enter the date and time in the format "MM/DD/YYYY HH:MM:SS".
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.

Automatic time-of-day setting with NTP

- **NTP Client**
Enable or disable time synchronization using NTP.
- **NTP Client only (secure)**
When enabled, the device receives the system time from a secure NTP server. The setting applies to all server entries.
To use the secure NTP client, the parameters for authentication (key ID, hash algorithm, key) must be configured.
- **Time Zone**
In this box, enter the time zone you are using in the format "+/- HH:MM". The time zone relates to UTC coordinated universal time. Settings for daylight-saving and standard time are taken into account in this box by specifying the time offset.

In the table, configure the NTP server

- **Select**
Select the row you want to delete.
- **NTP Server Index**
Number corresponding to a specific NTP server entry.
- **NTP Server Address**
Enter the IP address, the FQDN (Fully Qualified Domain Name) or the host 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**
Specify the interval between two-time queries. The greater the interval, the less accurate the time of the device.
Possible values are 64 to 2592000 seconds (30 days).
- **Key ID**
Enter the ID of the authentication key.
- **Hash Algorithm**
Specify the format for the authentication key.
- **Key**
Enter the authentication key. The length depends on the hash algorithm.
The following minimum lengths are recommended for the hash algorithm:
 - DES: ASCII 8 characters
 - MD5: ASCII 16 characters
 - SHA1: ASCII 20 characters
 - SHA256: ASCII 32 characters
- **Key Confirmation**
Enter the authentication key again to confirm it.

5.4.9 DDNS

On this Basic Wizard page, you configure the dynamic DNS client (DDNS client). The DDNS client synchronizes the assigned IP address with the hostname registered at the DDNS provider. This means that the device can always be reached using the same hostname.

Basic Wizard: DDNS Settings

IP

Device

SIM

Operator

Time

DDNS

SINEMA RC

Summary

DDNS stands for 'dynamic domain name system'. If you log the device on to a DDNS service, the device can be reached from the external network under a hostname, e.g. 'example.no-ip.com'. Here you enter the hostname that you have agreed with your DDNS provider for the device and the login data (User name, Password) for the DDNS server. To use the required Service, select the check box 'Enabled'.

Service	Enabled	Host	User name	Password	Password confirmation
No-IP	☐				
DynDNS	☐				

Previous

Abort

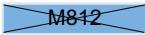
Next

Description

The table has the following columns:

- Service**
Shows which providers are supported.
- Enabled**
When enabled, the device logs on to the DDNS server.
- Host**
Enter the hostname that you have agreed with your DDNS provider for the device, e.g. example.no-ip-com.
- Username**
Enter the user name with which the device logs on to the DDNS server.
- Password**
Enter the password assigned to the user.
- Confirm password**
Confirm the password.

5.4.10 SINEMA RC



On this Basic Wizard page, you configure the access to the SINEMA RC server.

Note

This function can only be used with a KEY PLUG (Page 60).

Basic Wizard: SINEMA Remote Connect

IP	Device	SIM	Operator	Time	DDNS	SINEMA RC	Summary

Here, you configure the access to the SINEMA RC server. With these settings, the device logs on to the server. The VPN tunnel between the device and the SINEMA RC server is established only after successful authentication. Depending on the configured communications relations and the security settings, the SINEMA RC server connects the individual VPN tunnels.

☐ Enable SINEMA RC

☐ Layer 2 Support

Server Settings

SINEMA RC Address: 192.168.1.24

SINEMA RC Port: 443

Server Verification

Verification Type: Fingerprint

Fingerprint:

CA Certificate: -

Device Credentials

Device ID: 0

Device Password:

Device Password Confirmation:

Optional Settings

☒ Auto Firewall/NAT Rules

Type of connection: Digital Input

Use Proxy: none

Autoenrollment Interval [min]: 60

Previous

Abort

Next

Description

The page contains the following:

- **Enable SINEMA RC**

- Enabled:
A connection to the configured SINEMA RC Server is established. These boxes cannot be edited.
- Disabled:
The boxes can be edited. Any existing connection is terminated.

- **Layer2 support** (only with M87x / RM1224 / MUX85x)

When this option is enabled, the node can establish a connection to the SINEMA RC Server via Layer2 (VXLAN).

"Server settings" area

- **SINEMA RC Address**

Enter the IPv4 address or the FQDN (Fully Qualified Domain Name) of the SINEMA RC Server.

- **SINEMA RC Port**

Enter the port via which the SINEMA RC Server can be reached.

"Server Verification" area

- **Verification Type**

- Fingerprint: The identity of the server is verified based on the fingerprint.
- CA certificate: The identity of the server is verified based on the CA certificate.

- **Fingerprint**

Only necessary with the setting "Fingerprint". Enter the fingerprint of the device. The fingerprint is assigned during commissioning of the SINEMA RC Server. Based on the fingerprint, the device checks whether the correct SINEMA RC Server is involved. You will find further information on this in the Operating Instructions of the SINEMA RC Server.

- **CA Certificate**

Only necessary with the setting "CA Certificate". Select the CA certificate of the server used to sign the server certificate. Only loaded CA certificates can be selected.

"Device Credentials" area

- **Device ID**

Enter the device ID. The device ID is assigned when configuring the device on the SINEMA RC Server. You will find further information on this in the Operating Instructions of the SINEMA RC Server.

- **Device Password**

Enter the password with which the device logs on to the SINEMA RC Server. The password is assigned when configuring the device on the SINEMA RC Server. You will find further information on this in the Operating Instructions of the SINEMA RC Server.

- **Device Password Confirmation**

Repeat the password.

"Optional Settings" area

- **Auto Firewall/NAT Rules**

- Enabled

The firewall and NAT rules are created automatically for the VPN connection. The connections between the configured exported subnets and the subnets that can be reached via the SINEMA RC Server are allowed. The NAT settings are implemented as configured in the SINEMA RC Server.

You can enable SINEMA RC to access specific services of the device under "Security > Firewall > Predefined IPv4".

- Disabled

You will need to create the firewall and NAT rules yourself.

- **Type of connection**

Specify the type of VPN connection. For more detailed information, refer to the section "VPN connection establishment".

- Auto

The device adopts the settings of the SINEMA RC server. You configure the settings on the SINEMA RC server in "Remote connections > Devices". You can find additional information on this topic in the operating instructions "SINEMA RC Server".

With the following connection types, the settings of the SINEMA RC Server are not used.

- Permanent

The device establishes a VPN connection to the SINEMA RC Server. The VPN tunnel is maintained permanently.

- Digital Input

If the "Digital In" event occurs, the device attempts to establish a VPN connection to the SINEMA RC Server.

This is on condition that the event "Digital In" is forwarded to the VPN connection. To do this, enable "VPN Tunnel" for the "Digital In" event under "System > Events > Configuration".

- Wake up SMS (only with M87x / RM1224 / MUx85x)

When the device receives a command SMS (wake-up SMS), it attempts to establish a VPN connection to the SINEMA RC Server, provided that it is specified in "System > SMS > SMS Command" who a command SMS of the class "System" will be accepted from.

- Connection Check Action

If the "VPN Reset" or "VPN enable" actions are triggered, the device attempts to establish a VPN connection to the SINEMA RC Server. For this purpose, you configure the corresponding action under "System > Connection Check".

- TCP Event

If the incoming TCP packet contains conformant data, the device attempts to establish a VPN connection to the SINEMA RC Server. The prerequisite is that the "VPN" event is enabled under "System > TCP Event".

- GPS (only with MUx85x)

If the "SINEMA RC (all) enable" action is triggered, the device attempts to establish a VPN connection to the SINEMA RC Server. For this purpose, you configure the corresponding action under "System > GPS > Geofencing".

- All

The device uses all connection types. The exception is "Auto".

- **Use Proxy**
Specify whether a connection to the defined SINEMA RC Server is established via a proxy server. Only the proxy servers that you configured under "System > Proxy Server" can be selected.
- **Autoenrollment Interval [min]**
Specify the period of time in minutes after which queries are sent to the SINEMA RC server. With this query, the device checks whether there is a newer firmware file on the SINEMA RC server or whether the connection settings have changed. If you enter the value 0, this function is disabled.
- **Timeout [min]**
Specify the period of time in minutes. If no data exchange takes place, when this time has elapsed the VPN tunnel is automatically terminated.

5.4.11 Cloud Connector

On this wizard page, you configure the parameters for communication with the TIA Portal Cloud Connector.

Note

- Use the "TIA Portal Cloud Connector" integrated in the product over a VPN solution (e.g. SINEMA RC).
 - Configure the firewall settings of the SCALANCE M800/S615 (e.g. predefined IPv4 rules "Cloud Connector") to prevent unauthorized access of network devices to the "TIA Portal Cloud Connector Server".
-

Basic Wizard: TIA Portal Cloud Connector

IP	Device	Time	DDNS	SINEMA RC	Cloud Connector	Summary

The 'TIA Portal Cloud Connector' integrated in the product permits access to the PROFIBUS/MPI or PROFINET interface and the connected devices. The connection can take place from the local network or via a secure remote connection, for example, in combination with SINEMA Remote Connect. On this page, you configure the port for the communication with the TIA Portal Cloud Connector. You can also enable the 'TIA Portal Cloud Connector'.

Operation: Disabled ▼

Port:

Protocol: PROFINET ▼

Interface	Active
vlan1 (INT)	☐
vlan2 (EXT)	☐

Previous Abort Next

Requirement

- For the incoming packets to be forwarded to the device, enable the predefined IPv4 rule "Cloud Connector".

Description

The Basic Wizard page contains the following:

- **Operation**
 - Enabled
Enables the integrated TIA Portal Cloud Connector.
 - Disabled
Disables the integrated TIA Cloud Connector.
 - Start on DI
Enabling is controlled via the digital input (DI) if the "Cloud Connector" is enabled for the event "Digital input" under "System > Events > Configuration". If this setting is not enabled, the event is not passed on to the TIA Portal Cloud Connector.
- **Port**
Communication with the TIA Portal Cloud Connector is established via this port.
- **Protocol**
This protocol is used to access the plant network.
 - PROFINET via VLAN
You define the VLAN interface in the following table.

Only with M804PB

 - PROFIBUS via MPI/DP
 - PROFINET-PROFIBUS

The following table is only required for PROFINET:

- Interface
Only VLANs with a configured subnet are available.
- Active
When enabled, this VLAN is used for PROFINET.

5.4.12 Summary

Introduction

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

IP	Device	SIM	Operator	Time	DDNS	SINEMA RC	Summary

Internal (vlan1)
 IP Address: 192.168.1.1
 Subnet Mask: 255.255.255.0

System Name: sysName Not Set
 System Location: sysLocation Not Set
 System Contact: sysContact Not Set

Enable Mobile Network Interface: enabled
 Radio Mode: Auto
 Authentication Method: Auto
 Allow Data Roaming: enabled

PLMNID▲	Operator Name	APN	User Name	Enabled
26201	T-Mobile	internet.t-mobile	guest	enabled
26202	Vodafone	web.vodafone.de	guest	enabled
26203	Eplus	internet.eplus.de	guest	enabled
26207	O2	internet	guest	enabled
Manual				disabled

Time Manually: enabled
 System Time: 04/11/2017 16:52:47
 NTP Client: disabled
 Secure NTP Client only: disabled
 Time Zone: +00:00

NTP Server Index	NTP Server Address	NTP Server Port	Poll Interval
1	0.0.0.0	123	64

Service	Enabled	Host	User name
No-IP	disabled		
DynDNS	disabled		

SINEMA RC: disabled

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

Set Values

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

5.5 "Information" menu

5.5.1 Start Page

View of the Start page

After logging in successfully, the start page of the WBM is displayed. You cannot configure anything on this page.

General layout of the WBM page

The following areas are 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

1


English ▼ Go

2

Welcome admin
[Logout](#)

192.168.1.1/SCALANCE MUM856-1
SCALANCE MUM856-1

10/20/2023 02:12:14

Wizards

Information

3
Start Page

Versions

I&M

ARP / Neighbors

Log Tables

Faults

DHCP Server

SNMP

Learning Table

LLDP

IPv4 Routing

IPv6 Routing

Mobile

IPsec VPN

SINEMA RC

OpenVPN

Redundancy

VRRPv3 Statistics

Security

VXLAN

System Time

Firewall Monitoring

System

Interfaces

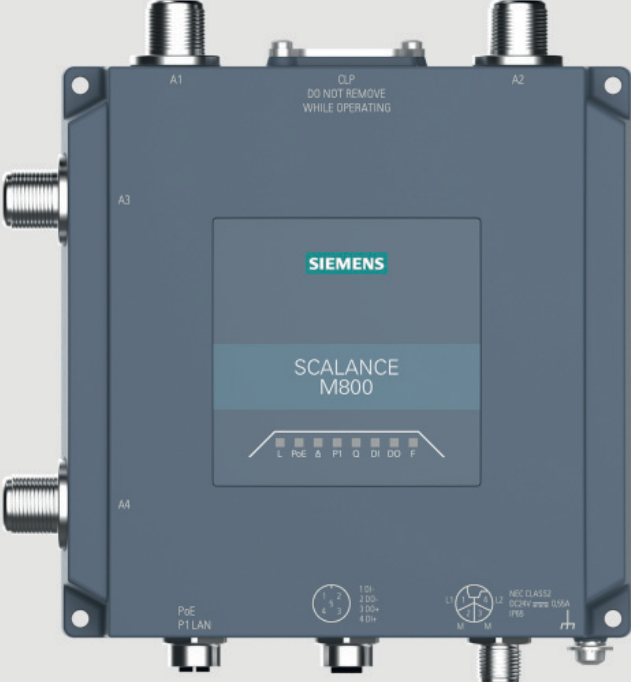
Layer 2

Layer 3 (IPv4)

Layer 3 (IPv6)

Security

Please select one item of the menu on the left



System Name: sysName Not Set
Device Type: SCALANCE MUM856-1

Power over Ethernet: Down
PLUG Configuration: ACCEPTED
PLUG License: ACCEPTED
Connection Status: Mobile interface disabled

Signal Level [dBm]: -
DDNS Status: -
Fault Status: No Fault

Packet Capture: disabled

Refresh

Selection area (1)

The following is available in the selection area:

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

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

Display area (2)

In the left-hand part of the display area, the full title of the currently selected menu item is always displayed.

- **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. 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.
- **Help** 
When you click this button, the help page of the currently selected menu item is opened in a new browser window.
- **Printer** 
When you click this button, a pop-up window opens with a view of the page content optimized for the printer.

- **Favorites**

When the product ships, the button is disabled on all pages .

If you click this button, the symbol  changes and the currently open page or currently open tab is marked as favorite. Once you have enabled the button once, the navigation area is divided into two tabs. The first tab "Menu" contains all the available menus as previously. The second tab "Favorites" contains all the pages/tabs that you selected as favorites. On the "Favorites" tab the pages/tabs are arranged according to the structure in the "Menu" tab. If you disable all the favorites you have created, the "Favorites" tab is removed again. To do this, click the  button on the relevant pages/tabs.

You can save, upload and delete the favorites configuration of a device on the "System > Load&Save" page using HTTP or TFTP.

- **Update on / 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 with submenus available.

The submenus contain pages on which information is available or with which you can create configurations. These pages are always displayed in the content area.

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

Content area (4)

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

The following is displayed below the picture of the device:

- System Name: System name of the device
- Device Type: The type of the device
- Power over Ethernet (only with MUX85x)
Shows the status of the power supply via PoE.
 - Up
The device supplies Ethernet-connected PoE-capable devices with power.
 - Down
The power supply is off.
- PLUG Configuration:
Shows the status of the configuration data on the PLUG, refer to the section "System > PLUG > Configuration".
- PLUG License:
Shows the status of the license on the PLUG, refer to the section "System > PLUG > License".
- Connection Status: Status of the connection

- Signal strength [dBm] (only with M87x / RM1224 / MUx85x)
Shows the signal strength of the connection.
- DDNS Status
If a dynamic DNS service is used, the host name of the device is displayed, e.g. example.no-ip.com. The status of the update is also displayed.
 - update successful
Update successful
 - update failed
Update unsuccessful
 - status unknown
Status unknown
- Fault Status Fault status of the device

Buttons you require often

The WBM pages contain the following standard buttons:

- **Refresh the display with "Refresh"**
WBM 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"**
WBM 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" role.

Note

The changes take immediate effect. But it takes some time for the changes in the configuration to be stored.

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

Logout

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

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. Click 'Write Startup Config' to save the changes immediately."

Note

Interrupting the save

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

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

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

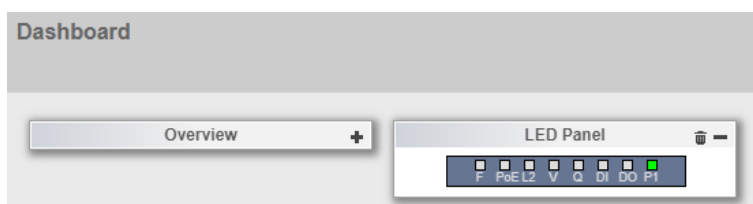
5.5.2 Dashboard

MUx85x

This page provides a quick overview of the most important device settings and status. You can compile your own dashboard from available dashboard contents. These contents can be shown or hidden, expanded and collapsed and placed at a desired position on the page. When you click on an individual information field or block, you are forwarded to the WBM page of the respective setting or statistic. This makes it easy to find related configuration pages.

The dashboard is updated every 60 seconds.

To manage the dashboard contents, you require a user role with the function right 15. Users with this role can both read and change device parameters. You configure the roles on the page "Security > Users > Roles (Page 421)".



Working with the dashboard

To show dashboard contents on the dashboard, click  in the upper right portion of the work area. Select the desired contents. These are shown as dashboard blocks on the dashboard.

You have the following options:

- Add new dashboard contents to the dashboard
- Delete dashboard contents
- Expand and collapse dashboard contents
- Arrange dashboard contents with drag-and-drop

The following dashboard contents are available for selection:

- System overview
- LED display
- Firewall
- VPN
- Mobile wireless
- Recording of the signal recorder etc.

Buttons

The availability of the buttons depends on the selected dashboard contents.

Icon	Meaning
	Opens the dialog with the selection of available dashboard contents
	Expands the dashboard contents.
	Collapses the dashboard contents.
	Deletes the dashboard contents

5.5.3 Versions

This WBM page shows the versions of the hardware and software of the device.

Version Information			
Hardware	Name	Revision	Order ID
Basic Device	SCALANCE M874-3	3	6GK5 874-3AA00-2AA2
CELL	CELL Module	03.001-01.000.01	-
Software	Description	Version	Date
Firmware	SCALANCE M800/S615 Firmware	V05.00.00	11/13/2017 20:00:00
Bootloader	SCALANCE M800 Bootloader	V01.05.00	08/02/2017 16:30:00
Firmware_Running	Current running Firmware	V05.00.00	11/13/2017 20:00:00
Refresh			

Description

Table 1 has the following columns:

- **Hardware**
 - Basic Device
Shows the basic device
 - CELL (only with M87x / RM1224 / MUx85x)
Shows the radio module used.
 - xDSL (only with M81x)
Shows the DSL module being used
- **Name**
Shows the name of the device.

- **Revision**
Shows the hardware version of the device.
- **Order ID**
Shows the article number of the device.

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 loaded firmware is activated and used.
 - Bootloader
Shows the version of the boot software stored on the device.
 - Firmware_Running
Shows the firmware version currently being used on the device.
- **Description**
Shows the short description of the software.
- **Version**
Shows the version number of the software version.
- **Date**
Shows the date on which the software version was created.

5.5.4 Identification & Maintenance

Identification and Maintenance data

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

Identification & Maintenance

Manufacturer ID: 42
Order ID: 6GK5 874-3AA00-2AA2
Basic MAC Address: 20-87-56-d3-0e-9c
Serial Number: SVPL3142515
Hardware Revision: 3
Software Revision: T08.00.00
Revision Counter: 0
Function Tag:
Location Tag:
Date:
Descriptor:

Refresh

Description of the displayed values

The table has the following rows:

- **Manufacturer ID**
Shows the manufacturer ID.
- **Order ID**
Shows the order ID.
- **Basic MAC address**
Shows the MAC address of the IPv4 interface.
- **Serial Number**
Shows the serial number.
- **Hardware Revision**
Shows the hardware version.
- **Software Revision**
Shows the software version.
- **Revision Counter**
Regardless of a version change, this box always displays the value "0".
- **Function tag**
Shows the function tag (plant designation) of the device. The plant designation (HID) is created during configuration of the device with HW Config of STEP 7.
- **Location tag**
Shows the location tag of the device. The location identifier (LID) is created during configuration of the device with HW Config of STEP 7.
- **Date**
Shows the date created during configuration of the device with HW Config of STEP 7.
- **Descriptor**
Shows the description created during configuration of the device with HW Config of STEP 7.

5.5.5 ARP / neighbors

5.5.5.1 ARP-Tabelle

Assignment of MAC address and IPv4 address

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

Address Resolution Protocol (ARP) Table			
ARP Table		IPv6 Neighbor Table	
Interface	MAC Address	IP Address	Media Type
vlan1	68-05-ca-36-39-0d	192.168.16.20	Dynamic
vlan1	68-05-ca-25-e8-62	192.168.16.55	Dynamic
2 entries.			
Refresh			

Description of the displayed values

The table has the following columns:

- **Interface**
Shows the interface via which the row entry was learnt.
- **MAC Address**
Shows the MAC address of the destination or source device.
- **IP Address**
Shows the IPv4 address of the destination device.
- **Media Type**
Shows the type of connection.
 - Dynamic
The device recognized the address data automatically.
 - Static
The addresses were entered as static addresses.

5.5.5.2 IPv6 Neighbor Table

Assignment of MAC address and IPv6 address

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

Address Resolution Protocol (ARP) Table			
Interface	MAC Address	IP Address	Media Type
vlan1	00-13-ce-63-59-bf	192.168.0.97	Dynamic
vlan1	6c-62-6d-6f-38-31	192.168.0.100	Dynamic
2 entries.			
Refresh			

Description of the displayed values

The table has the following columns:

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

5.5.6 Log Tables

5.5.6.1 Event Log

Logging events

The page shows the system events that have occurred in the form of a table. Some of the system events can be configured in "System > Events", for example if the connection status of a port has changed.

The content of the table is retained even when the device is turned off. The event log file can be loaded using HTTP, TFTP or SFTP.

Log Table

Event Log | Security Log | Firewall Log

Warning Events (last 24h): 0
Critical Events (last 24h): 0

Severity Filters
☐ Info
☐ Warning
☐ Critical

Restart	System Up Time	System Time	Severity	Log Message
3	20:38:15	07/06/2023 12:16:38.419	6 - Info	WBM: User admin has logged in from 192.168.1.20.
3	00:02:15	07/05/2023 15:40:39.020	6 - Info	Time synchronized via 'MANUAL'.

1 - 50 of 158 entries [Show all](#)

[Clear](#) [Next](#)

[Refresh](#)

Description

The page contains the following boxes:

- **Events of the type 'Warning' (last 24 hours)**
Shows how many events of the "Warning" category have occurred in the last 24 hours.
- **Events of the type 'Critical' (last 24 hours)**
Shows how many events of the "Critical" category have occurred in the last 24 hours.

Severity Filters

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

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

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

The table has the following columns:

- **Restart**
Counts the number of restarts since you last reset to factory settings and shows the device restart after which the corresponding event occurred.
- **System Up Time**
Shows the time the device has been running since the last restart when the described event occurred.
- **System Time**
Shows the system time at which the described event occurred in the format MM/DD/YYYY hh:mm:ss.000.
If no system time is set or time synchronization has not yet taken place, the system time that has elapsed since the last restart is shown. After a restart, the time of day begins at 01/01/2000 00:00:00.000.
- **Severity**
Sorts the entry into the categories above.
- **Log Message**
Displays a brief description of the event that has occurred.

Note

A maximum of 800 entries in the table are possible for each severity. If the maximum number of entries is reached for a severity, the oldest entries of this severity are discarded in the table. The table remains permanently in the memory.

5.5.6.2 Security Log

The WBM page shows the events that occurred during communication via a secure VPN tunnel in the form of the table.

Security Log-Tabelle

Ereignis-LogSecurity-LogFirewall-Log

Severity-Filter

☐ Info

☐ Warning

☐ Critical

Neustart	Systembetriebszeit	Systemzeit	Severity	Log-Meldung
21	00:02:47	Date/time not set	6 - Info	16[KNL] fe80::21b:1bff:fe9a:322e appeared on vlan1
21	00:02:47	Date/time not set	6 - Info	07[KNL] interface vlan1 activated
21	00:02:47	Date/time not set	6 - Info	09[KNL] fe80::21b:1bff:fe9a:322e disappeared from vlan1
21	00:02:47	Date/time not set	6 - Info	07[KNL] interface vlan1 deactivated
21	00:01:34	Date/time not set	6 - Info	16[CFG] loaded ca certificate "C=DE, O=Siemens, CN=P386A021C-G9FA6E9AE8D298B7D" from '/etc/ipsec.d/cacerts/M826.U7D262D88@GB985.M826b_CACert.pem'
21	00:01:34	Date/time not set	6 - Info	16[CFG] loaded RSA private key from '/etc/ipsec.d/private/M826.U7D262D88@GB985.M826b_Key.pem'
21	00:01:34	Date/time not set	6 - Info	06[CFG] added configuration 'VPN-1'
21	00:01:34	Date/time not set	6 - Info	06[CFG] CA certificate "C=DE O=Siemens CN=P386A021C-G9FA6E9AE8D298B7D" not found, discarding CA constraint
21	00:01:34	Date/time not set	6 - Info	06[CFG] CA certificate "C=DE O=Siemens CN=P386A021C-G9FA6E9AE8D298B7D" not found, discarding CA constraint
21	00:01:34	Date/time not set	6 - Info	06[CFG] id '%any' not confirmed by certificate, defaulting to 'C=DE, O=Siemens, CN=PBB5F-U7D262D88-GB985'

1 - 10 of 426 Einträge [Alle anzeigen](#)

1 [Weiter](#)

Leeren

Aktualisieren

Description

- **Severity Filters**

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

Note

A maximum of 800 entries in the table are possible for each severity. If the maximum number of entries is reached for a severity, the oldest entries of this severity are overwritten in the table. The table remains permanently in the memory.

- Critical
Critical
When this parameter is enabled, all entries of the category "Critical" are displayed.
- Warning
warning
When this parameter is enabled, all entries of the category "Warning" are displayed.
- Info
Informative
When this parameter is enabled, all entries of the category "Info" 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. If no system time is set, the box displays "Date/time not set".
- **Severity**
Sorts the entry into the categories above.
- **Log Message**
Displays a brief description of the event that has occurred.

5.5.6.3 Firewall Log

The firewall log logs the events that occurred on the firewall. When you create firewall rules, you can specify the event severity with which they are logged.

Firewall Log Table

Event LogSecurity LogFirewall Log

Severity Filters

☐ Info

☐ Warning

☐ Critical

Restart	System Up Time	System Time	Severity	Log Message
1	00:09:01	Date/time not set	6 - Info	ACCEPT(0) in:vlan1 out:lo len:60 s-mac:68:05:CA:04:D6:26 d-mac:00:1B:1B:38:16:5A s-ip:192.168.0.60 d-ip:192.168.0.20 icmp:8:0

1 entry.

Clear

Refresh

Description

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

Note

A maximum of 800 entries in the table are possible for each severity. If the maximum number of entries is reached for a severity, the oldest entries of this severity are overwritten in the table. The table remains permanently in the memory.

 - Critical
 Critical
 When this parameter is enabled, all entries of the category "Critical" are displayed.
 - Warning
 warning
 When this parameter is enabled, all entries of the category "Warning" are displayed.
 - Info
 Informative
 When this parameter is enabled, all entries of the category "Info" are displayed.
- Text Filter**
 Enter a text to filter by. Log entries in which the entered text occurs are then 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. If no system time is set, the box displays "Date/time not set".
- **Severity**
Sorts the entry into the categories above.
- **Log Message**
Displays a brief description of the event that has occurred.

5.5.7 Faults

Error status

if an error occurs, it is shown on this page. In addition, the red "Error" button flashes on every WBM page in the upper part of the display area. On the device, errors are indicated by red fault LED lighting up.

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

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

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

Faults

No. of Signaled Faults: 1

[Reset Counters](#)

Fault Time	Fault Description	Clear Fault State
16s	Link down on P0.1.	Clear Fault State
17s	Warm start performed.	Clear Fault State

[Refresh](#)

Description

- **No. of Signaled Faults**

Indicates how often the fault LED lit up and not how many faults occurred.

The table contains the following columns:

- **Fault Time**

Shows the time the device has been running since the last system restart when the described error/fault occurred.

- **Fault Description**

Displays a brief description of the fault/error that has occurred.

- **Clear Fault State**

Some faults can be acknowledged and thus removed from the fault list, e.g. a fault of the event "Cold/Warm Start". If the "Clear Fault State" button is enabled, you can delete the error.

5.5.8 DHCP Server

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

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

Description

- **IP Address**

Shows the IPv4 address assigned to the DHCP client.

- **Pool ID**

Shows the number of the IPv4 address band.

- **Identification Method**
Shows the method according to which the DHCP client is identified.
 - MAC address
Identification is based on the MAC address.
 - DHCP client ID
Identification is based on a freely defined DHCP client ID.
 - 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.
 - IAID and DUID
With this, the DHCP client can log onto DHCP servers that support parallel operation of IPv4 and IPv6.
The identification is via the IAID and the DUID and identifies precisely one IP interface of the device.
- **Identification value**
Shows the MAC address or the client ID of the DHCP client.
- **Allocation Method**
Shows whether the IPv4 address was assigned statically or dynamically. You configure the static entries in "System > DHCP > Static Leases".
- **Binding State**
Shows the status of the assignment.
 - Assigned
The assignment is used.
 - Not used
The assignment is not used.
 - probing
The assignment is being checked.
 - Unknown
The status of the assignment is unknown.
- **Expire Time**
Shows until when the assigned IPv4 address is still valid. Up to this time, the DHCP client must either request a new IPv4 address or extend the lease time of the assigned IPv4 address.

5.5.9 Diagnostics

MUx85x

This page shows the usage values of internal and external modules of the device. The modules are only shown if they make corresponding information available. If you add or remove a module, the display is automatically adapted. If the usage value exceeds the displayed threshold value, the status changes accordingly.

The threshold values are preset by the device and cannot be modified. If no threshold values are preset, "-" is displayed. On the "System > Events > Configuration" page, you can specify how the device signals the status change.

Diagnostics				
Usage Table				
Name	Status	Usage [%]	High Warning Threshold [%]	High Critical Threshold [%]
CPU	OK	-	-	-
RAM	OK	15	90	98
FLASH:Config	OK	4	90	-
eMMC SLC cells life span	OK	10	80	90
eMMC MLC cells life span	OK	10	80	90
eMMC EOL info	OK	30	80	90

Refresh

Description

The **Usage Table** has the following columns:

- **Name**
Shows the name of the module.
- **Status**
Depending on the relationship between the threshold values and the current usage, the following status values are displayed in ascending priority:
 - **OK**
The usage is within the preset threshold values.
 - **WARNING**
The upper threshold value of the severity level "Warning" was exceeded. The usage is still in a normal range. The operating conditions of the device should be checked.
 - **CRITICAL**
The upper threshold value of the severity level "Critical" was exceeded. The device must be checked. Overloading the device can lead to malfunctions.
 - **INVALID**
The usage could not be determined or is invalid. The "Usage [%]" box shows "-".
 - **INITIAL**
No data has been read out yet. "-" is displayed in all boxes.
- **Usage [%]**
Shows the current value for the usage of the device. The display is updated at regular intervals.

- **High Warning Threshold [%]**
If this value is exceeded, the status changes to "WARNING". You can configure that you are informed by a message.
- **High Critical Threshold [%]**
If this value is exceeded, the status changes to "CRITICAL". You can configure that you are informed by a message.

5.5.10 SNMP

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

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

Description

The table has the following columns:

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

5.5.11 Ethernet Statistics

MUx85x

5.5.11.1 Interface statistics

Interface Statistics

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

Note

The interface statistics specify the total number of received or sent bytes for each port. In contrast, the information for VLAN interfaces only relates to the Layer 3 data traffic of the corresponding interface.

Ethernet Statistics: Interface Statistics

Interface Statistics

Packet Size

Packet Type

Packet Error

Total In Errors: 0

Discarded packets (last 24h): 0

Discarded packets (last 7d): 0

Interface	In Octet	Out Octet	In Unicast	In Non-Unicast	Out Unicast	Out Non-Unicast	In Errors
P1	0	0	20038	12165	21261	662	0
P2	0	0	0	0	0	0	0
P3	0	0	0	0	0	0	0
P4	0	0	0	0	0	0	0

Reset Counter

Refresh

Description

The page contains the following boxes:

- **In Errors (total)**
Shows the sum of all received errors.
- **Discarded packets (last 24 hrs)**
Shows the sum of all discarded packets within the last 24 hours.
- **Discarded packets (last 7 days)**
Shows the sum of all discarded packets within the last 7 days.

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 tab "Packet Error".

5.5.11.2 Packet Size

Frames sorted by length

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

Ethernet Statistics: Packet Size						
Interface Statistics	Packet Size	Packet Type	Packet Error			
Port	64	65-127	128-255	256-511	512-1023	1024-max
P1	628415	259963	2579	45309	2019	0
Reset Counter						
Refresh						

Description

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

5.5.11.3 Packet Type

Received frames sorted by type

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

Ethernet Statistics: Packet Type			
Interface Statistics	Packet Size	Packet Type	Packet Error
Port	Unicast	Multicast	Broadcast
P1	23871	601938	312699
Reset Counter			
Refresh			

Description

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

5.5.11.4 Packet Error

Received bad frames

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

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

Description

- **Port**
Shows the available ports.
- **Error types**
The other columns after the port number contain the absolute numbers of the incoming frames according to their error.
In the columns of the table, a distinction is made according to the following errors:
 - CRC (Cyclic Redundancy Code)
The packet length is between 64 and 2048 bytes. The CRC of the packet is invalid.
 - Undersize
The packet length is less than 64 bytes. The CRC of the packet is valid.
 - Oversize
The packet size is more than 2048 bytes. The CRC of the packet is valid.
 - Fragments
The packet length is less than 64 bytes. The CRC of the packet is invalid.
 - Jabbers
The frame length is more than 2048 bytes. The CRC of the packet is invalid.
 - Collisions
Frames in which a collision event was detected.

5.5.12 Learning Table

Address filtering

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

Learning Table			
VLAN ID	MAC Address	Status	Port
1	00-00-5e-00-01-07	Learnt	P4
1	00-00-5e-00-02-07	Learnt	P4
1	00-1b-1b-40-91-23	Learnt	P4
1	00-1b-1b-9a-32-2e	Learnt	P2
1	00-1b-1b-cd-3b-00	Learnt	P4
1	00-5e-1d-d2-76-00	Learnt	P4
17 entries.			
Refresh			

Description

The table contains the following columns:

- **VLAN ID**
Shows the VLAN ID of the node.
-
- Note**
- This column appears in the table only if a VLAN is configured.
-
- **MAC Address**
Shows the MAC address of the node.
 - **Status**
Shows the status of each address entry:
 - **Learnt**
The specified address was learned by receiving a frame from this node and will be deleted when the aging time expires if no further packets are received from this node.
 - **Invalid**
These values are not evaluated.
 - **Port**
Shows the port 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.

5.5.13 LLDP

Status of the neighborhood table

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

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

Link Layer Discovery Protocol (LLDP) Neighbors					
System Name	Device ID	Local Interface	Hold Time[s]	Capability	Port ID
sysName Not Set	08:00:06:70:29:d7	P1	20	Bridge	port-008
Refresh					

Description

The table contains the following columns:

- **System Name**
System name of the connected device.
- **Device ID**
Device ID of the connected device. The device ID corresponds to the device name assigned via SINEC PNI (SIMATIC STEP 7). If no device name is assigned, the MAC address of the device is displayed.
- **Local Interface**
Port at which the device received the information.
- **Hold Time[s]**
Hold time in seconds
An entry remains stored on the device for the time specified here. If the device does not receive any new information from the connected device during this time, the entry is deleted.
- **Capability**
Shows the properties of the connected device:
 - Router
 - Bridge
 - Telephone
 - DOCSIS Cable Device
 - WLAN Access Point
 - Repeater
 - Station
 - Other
- **Port ID**
Port of the device with which the device is connected. If no port ID is assigned, the MAC address of the connected device is shown.

5.5.14 IPv4 Routing

Introduction

This page shows the routes currently being used.

Layer 3: IPv4 Routing Table					
Destination Network	Subnet Mask	Gateway	Interface	Metric	Routing Protocol
192.168.16.0	255.255.255.0	0.0.0.0	vlan1	0	connected
1 entry.					
Refresh					

Description

The table has the following columns:

- **Destination Network**
Shows the destination address of this route.
- **Subnet Mask**
Shows the subnet mask of this route.
- **Gateway**
Shows the gateway for this route.
- **Interface**
Shows the interface for this route.
- **Metric**
Shows the metric of the route. The higher value, the longer packets require to their destination.
- **Routing Protocol**
Shows the routing protocol from which the entry in the routing table originates. The following entries are possible:
 - Connected: Connected routes
 - Static: Static routes
 - DHCP: Routes via DHCP

5.5.15 IPv6 Routing

Introduction

This page shows the IPv6 routes currently being used.

Layer 3: IPv6 Routing Table					
Destination Network	Prefix Length	Gateway	Interface	Metric	Routing Protocol
2002:C0A8:1296::	48	::	vlan1	1	connected
1 entry.					
Refresh					

Description

The table has the following columns:

- **Destination Network**
Shows the destination address of this route.
- **Prefix Length**
Shows the prefix length of this route.

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

5.5.16 Mobile

5.5.16.1 Overview

M87x RM1224 MUx85x

The WBM page shows an overview of the current operating status of the device.

Mobile Overview

Overview | **Signal Recorder** | **Data Usage**

SIM Type: Physical

IMEI: [REDACTED]

SIM Status: present

PIN Status: No PIN required

IMSI: [REDACTED]

Phone Number: [REDACTED]

Connection Status: Searching

Packet Switch Status: -

Cell ID: -

LAC / TAC: -

Signal Strength: -

RSRQ: -

Band: -

ARFCN: -

Mobile Chip Temperature: 33°C

Provider: T-Mobile

APN: internet.t-mobile

External IP Address: 0.0.0.0

DNS Server(s): -

Refresh

Description

The page contains the following:

- **SIM Type**
Shows which SIM type is being used.
 - Physical
 - eSIM
- **IMEI**
Shows the IMEI number of the wireless module being used.
The IMEI (= International Mobile Equipment Identity) is assigned uniquely worldwide.
- **IMSI**
Shows the subscriber ID that is stored on the SIM card being used.

- **SIM Status**
Shows the status of the SIM card.
 - present
SIM card exists
 - missing
SIM card missing
- **ICCID (Integrated Circuit Card Identifier)**
Shows the SIM card identifier.
- **PIN Status**
Shows the status of the PIN.
 - PIN required
PIN still needs to be entered.
 - No PIN required
PIN is not needed.
 - PUK required
SIM card blocked. With the PUK, the SIM card can be unblocked again.
 - wrong PIN
The PIN is wrong.
 - PIN valid
The PIN is valid.
- **Phone Number**
Shows the phone number of the SIM card.
If the phone number does not exist or cannot be read out, "no number" is displayed.
- **Connection Status**
Shows whether a wireless connection exists, and, if it does, which one:
 - UMTS: IP connection via UMTS or HSPA
 - GPRS: IP connection via EGPRS, GPRS or LTE
- **Packet Switch Status**
Shows the status of the packet switching.
- **Cell ID**
Shows the ID of the wireless cell in which the device is logged in.
- **Physical Cell ID (PCI)**
Shows the cell ID of the physical layer in 4G LTE and 5G NR. With the PCI, the device can distinguish between wireless cells that transmit on the same frequency.
- **LAC (Location Area Code) / TAC (Tracking Area Code)**
Shows the identifier for the current location of the device within the mobile wireless network.

- **Signal Strength**

Shows the signal strength.

- Signal strength with SCALANCE M87x/ RM1224:

dBm	Signal strength
< -109	No connection
-109 ... -89	Bad signal strength
-89 ... -73	Medium signal strength
> -73	Good signal strength

- Signal strength with SCALANCE MUX85x:
No reception / Very bad / Bad / Medium / Good / Very good

- **RSRQ**

Shows the RSRQ value of the connection quality in dB.

- **Band**

Shows the band used.

- **ARFCN (Absolute Radio Frequency Channel Number)**

Shows the ARFCN value.

- **Mobile chip temperature**

Shows the current temperature of the installed chip.

- **Provider**

Shows the mobile wireless provider.

- **APN**

Shows the APN (= Access Point Name) of the wireless link that is being used.

- **External IP Address**

Shows the WAN IP address at which the device can be reached in the mobile wireless network. The WAN IP address is assigned to the device by the service of the mobile wireless provider.

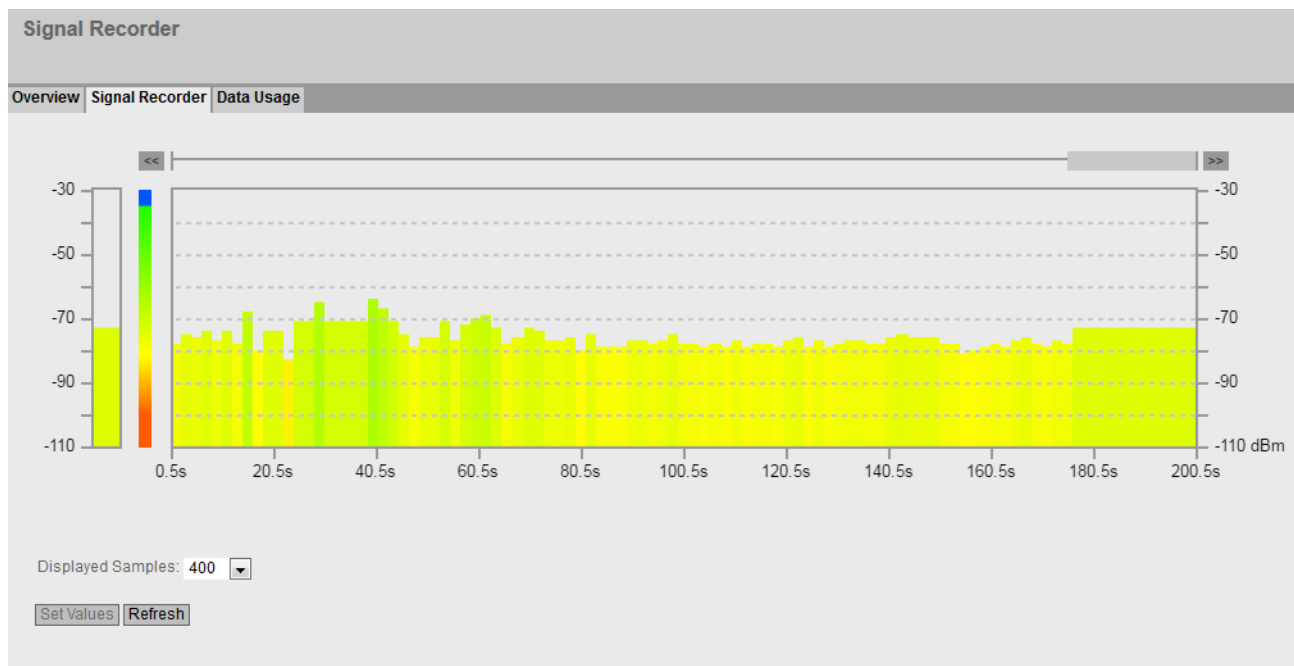
- **DNS Server(s)**

Shows the DNS server or servers used by the device.

5.5.16.2 Signal Recorder



The signal recorder shows the signal strength to the wireless cell in which the device is booked in.



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 signal strength is displayed in real time according to the color scheme.
- Color scheme
Green = Good, Yellow = Medium, Orange = Weak, Red = Very weak
- x axis
The x axis shows the course of the measurement in seconds.
- Measurement data
The measurement data shows the value of the signal strength to according to the color scheme shown.

Displayed Samples

Select how many measured values will be shown in the graphic.

5.5.16.3 Data usage

M87x

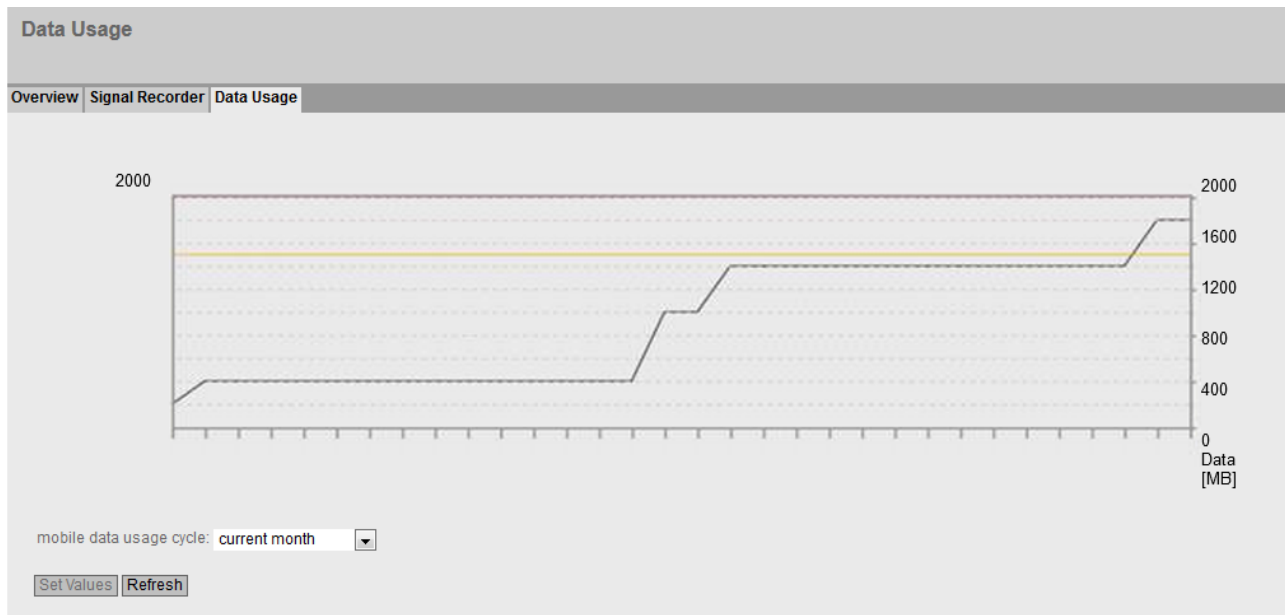
RM1224

MUx85x

This WBM page displays the data volume consumed in the selected month. The device calculates the data usage based on the counted data packets (upload and download) on the

WAN interface. The determined data volume can deviate from the invoice of your mobile network provider due to block rounding.

The consumed data volume of 3 months is stored in the non-volatile FLASH memory of the device. The values are stored at regular intervals or before the unit shuts down, but not in the event of a power failure.



Requirement

- "Mobile data usage" is activated under "Interfaces > Mobile > General".

Description

The graphic contains the following elements:

- x axis
Division of the selected month into days.
- y axis
Classification of the defined data volume.
- Lines
 - Red: The specified data volume. You configure the setting under "Interfaces > Mobile > General".
 - Yellow: Corresponds to 75 % of the specified data volume.
 - Black: The volume of data consumed.

Mobile data usage cycle

Select the desired month.

- **Current month**
Shows the data volume consumed to date.
- **Last month / Month before last**
Shows the total volume of data consumed in the desired month.

5.5.16.4 Network Scan

MUx85x

On this page, you can start the network scan to analyze the quality of the connection. The measured values are shown in a table.

Note

This function is available from HW release 16 (models MS5G16R and EL5G16R).

Network Scan								
Overview	Signal Recorder	Data Usage	Network Scan					
PLMNID	LAC	Cell ID	Technology▲	ARFCN	Signal Level[dBm]	RSRP[dBm]	RSRQ[dB]	Status
26203	36577	23087401	4G	1600	-101	-101	-14	CELL_SUITABLE
26203	36577	23087411	4G	300	-108	-108	-20	CELL_SUITABLE
26202	34641	19158542	4G	2850	-101	-101	-8	CELL_SUITABLE
26203	36577	23087381	4G	6200	-92	-92	-14	CELL_SUITABLE
26202	34641	19158537	4G	1801	-92	-92	-11	CELL_SUITABLE
26201	31665	30565129	4G	3749	-91	-91	-7	CELL_SUITABLE
26202	34641	19158530	4G	6300	-84	-84	-14	CELL_SUITABLE
26201	31665	30565123	4G	6400	-84	-84	-8	CELL_SUITABLE
26202	34641	19158548	4G	100	-94	-94	-8	CELL_SUITABLE
26201	31665	30565120	4G	1300	-96	-96	-8	CELL_SUITABLE

Start Scan

Refresh

Description

The table is comprised of the following columns:

- **PLMN ID** (Public Land Mobile Network ID)
Shows the network ID of the operator.
- **LAC** (Location Area Code) / **TAC** (Tracking Area Code)
Shows the identifier for the current location of the device within the mobile wireless network.
- **Cell ID**
Shows the identifier of the wireless cell in which the device is logged in.

- **Technology**
Shows the mobile network standard used:
 - GSM
 - UMTS
 - LTE
 - 5G
- **ARFCN (Absolute Radio Frequency Channel Number)**
Shows the ARFCN value.
- **Signal Strength[dBm]**
Shows the signal strength.
- **RSRP[dBm]**
RSRP (Referenz Signal Received Power) stands for the reference signal of the receive field strength. The RSRP values shows the signal strength at the end device in dBm.
- **RSRQ[dB]**
RSRQ (Reference Signal Received Quality) stands for the reference signal of the receive quality. The RSRQ value shows the signal quality at the end device in dB.
- **Status**
Shows whether the wireless cell can be used.

Note

The SIM card must be inserted.

- **"Start scan" button**
Click this button to start scanning.

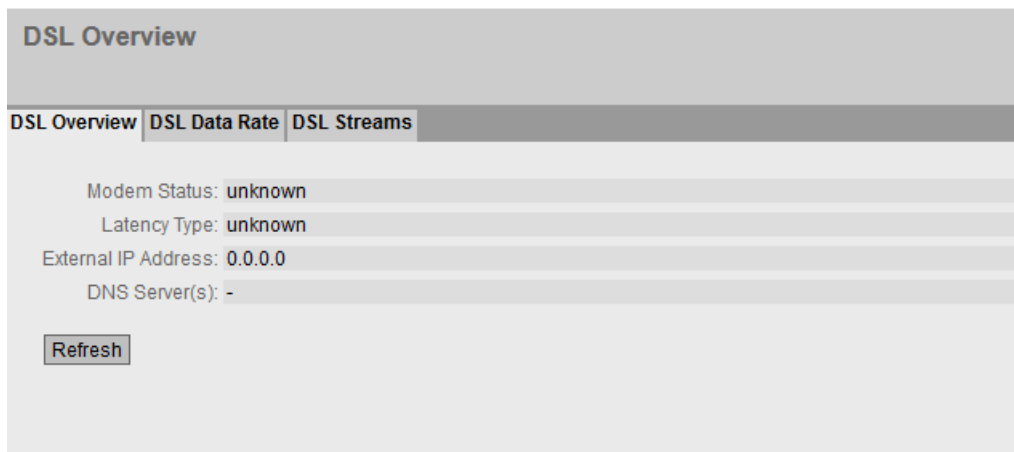
5.5.17 DSL

5.5.17.1 Overview

M81x

An ADSL connection consists of two endpoints known as ADSL Transceiver Units (ATU). The ADSL Transceiver Unit Remote (ATU-R) is this device and the ADSL Transceiver Unit Central (ATU-C) is the device in the central office.

The WBM page shows the current operating status of the device and contains information on the ATU-C.



Description

The page contains the following:

- **Modem Status**
Shows the status of the modem.
For example when initializing and when establishing the ADSL connection, the following statuses are displayed:
 - showtime-sync
ADSL connection is established. Data traffic possible.
 - handshake
ADSL connection is checked and established.
 - full-init
Modem is initialized.
 - silent
No ADSL connection
- **Latency Type**
Shows which method is used.
 - fast
Fast Path: Short reply time. Less protection against interference.
 - slow
Protection against interference by interleaving. Interleaving means that the sequence of bits is changed and this extends the reply time.
 - unknown
Method unknown
- **External IP Address**
Shows the external IP address at which the device can be reached. The IP address is assigned to the device by the service of the DSL provider.
- **DNS Server(s)**
Shows the DNS server or servers used by the device

5.5.17.2 DSL Data Rate

M81x

The WBM page contains an overview of the data transfer rates for the receive direction (downstream) and the send direction (upstream).

DSL Streams

DSL Overview

DSL Data Rate

DSL Streams

Downstream Interleaver Depth:

0

Downstream Line Attenuation (dB):

Downstream Signal Attenuation (dB):

Downstream Signal-to-Noise Ratio Margin (dB):

Downstream Actual Aggregate Transmit Power (dB):

Upstream Interleaver Depth:

0

Upstream Line Attenuation (dB):

Upstream Signal Attenuation (dB):

Upstream Signal-to-Noise Ratio Margin (dB):

Upstream Actual Aggregate Transmit Power (dB):

Refresh

Description of the displayed values

The page contains the following:

- Downstream Data Rate (kbps)**
Shows the usable data transfer rate for downstream.
- Downstream ATTNDR (kbps)**
ATTNDR (Attainable data rate).
Shows the maximum possible data transfer rate for downstream.
- Upstream Data Rate (kbps)**
Shows the usable data transfer rate for upstream.
- Upstream ATTNDR (kbps)**
ATTNDR (Attainable data rate).
Shows the maximum possible data transfer rate for upstream.

5.5.17.3 Streams

M81x

The WBM page shows parameters that influence the data transfer rate.

DSL Streams

DSL Overview | DSL Data Rate | **DSL Streams**

Downstream Interleaver Depth: 0

Downstream Line Attenuation (dB):

Downstream Signal Attenuation (dB):

Downstream Signal-to-Noise Ratio Margin (dB):

Downstream Actual Aggregate Transmit Power (dB):

Upstream Interleaver Depth: 0

Upstream Line Attenuation (dB):

Upstream Signal Attenuation (dB):

Upstream Signal-to-Noise Ratio Margin (dB):

Upstream Actual Aggregate Transmit Power (dB):

Refresh

Description of the displayed values

For the receive direction (downstream), the following values are displayed:

- **Downstream Interleaver Depth**
Shows the depth with which the data is interleaved. The higher the interleaving depth, the longer the reply time.
- **Downstream Line Attenuation (dB)**
Shows the line attenuation. The line attenuation depends on the cable diameter and the transmission frequency.
- **Downstream Signal Attenuation (dB)**
Shows the signal attenuation. The lower the value, the better the signal.
- **Downstream Signal-to-Noise Ratio Margin (dB)**
Shows the signal-to-noise ratio: The higher the value, the better the signal.
- **Downstream Actual Aggregate Transmit Power [dB]**
Shows the current transmit power that is achieved in aggregated operation.

For the send direction (upstream), the following values are displayed:

- **Upstream Interleaver Depth**
Shows the depth with which the data is interleaved. The higher the interleaving depth, the longer the reply time.
- **Upstream Line Attenuation (dB)**
Shows the line attenuation. The line attenuation depends on the cable diameter and the transmission frequency.
- **Upstream Signal Attenuation (dB)**
Shows the signal attenuation. The lower the value, the better the signal.

- **Upstream Signal-to-Noise Ratio Margin [dB]**
Shows the signal-to-noise ratio: The higher the value, the better the signal.
- **Upstream Actual Aggregate Transmit Power [dB]**
Shows the current transmit power that is achieved in aggregated operation.

5.5.18 SHDSL

M826

The WBM page shows the status of the SHDSL interface.

SHDSL Overview

Interface	Negotiation	Data Rate [kbps]	Uptime	SNR [dB]	Negotiation Count	CRC Anomaly	LOSW Defect
SHDSL 1	up data mode	5696	4m 4s	20	1	0	0
SHDSL 2	up data mode	5696	4m 7s	20	1	0	0

Refresh

Description of the displayed values

This table contains the following columns:

- **Interface**
Shows the SHDSL interfaces of the device.
- **Negotiation**
The following values are possible:
 - down not ready (only with the CO role)
There is no electrical connection plugged into the communications partner. The driver is initialized and is ready to negotiate the connection parameters.
 - down ready (only with the CPE role)
There is no electrical connection plugged into the communications partner. The driver is initialized and is ready to negotiate the connection parameters.
 - initializing
The connection parameters are negotiated.
 - up data mode
The connection parameters have been negotiated successfully. The data transfer is now possible.
 - stop down ready
The negotiation of connection parameters was not successful or the connection was interrupted. Renegotiation of the parameters is pending.
 - unknown
Driver initialization not yet completed. This status occurs following device startup.

- **Data Rate [kbps]**
Shows the usable data transmission rate.
- **Uptime**
Shows the time since the last negotiation of the connection parameters or the last connection interruption.
- **SNR [dB]**
Shows the signal-to-noise ratio: The higher the value, the better the signal.
- **CRC Anomaly**
Cyclic Redundancy Check
Shows how many SHDSL network packets were discovered with a bad checksum (CRC).
- **LOSW Defect**
Loss of Synchronization Word
Shows how often the synchronization was lost on the SHDSL connection.
- **Negotiation Count**
Shows how often the connection parameters were renegotiated.

5.5.19 IPsec VPN

The WBM page shows the status of the activated VPN connections.

Internet Protocol Security (IPsec) Information								
Name	Local Host	Local DN	Local Subnet	Remote Host	Remote DN	Remote Subnet	Rekey Time	Status
VPN-1	192.168.100.1	192.168.100.1	192.168.100.0/24	192.168.184.2	192.168.184.2	192.168.11.0/24	50m 2s	established
Refresh								

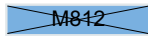
Description of the displayed values

This table contains the following columns:

- **Name**
Shows the name of the VPN connection.
- **Local Host**
Shows the IP address of the device.
- **Local DN**
Shows the Distinguished Name (DN) of the device that was signaled to the remote station during connection establishment. The entry is adopted from the "Local ID" box, the device certificate or the IP address of the device.
- **Local Subnet**
Shows the local subnet.
- **Remote Host**
Shows the IP address or the host name of the remote device.

- **Remote DN**
Shows the Distinguished Name (DN) signaled by the remote device during connection establishment.
- **Remote Subnet**
Shows the remote subnet.
- **Rekey Time**
Shows when the validity of the key expires.
- **Status**
Shows the status of the VPN connection.

5.5.20 SINEMA RC



Shows information on SINEMA RC Server.

Note

This function can only be used with the PLUG SINEMA RC (Page 60).

SINEMA Remote Connect (SINEMA RC) Information

Status:	disabled
Device Name:	-
Device Location:	-
GSM Number:	-
Vendor:	-
Comment:	-
Type of Connection (Server):	-
Type of Connection (Device):	Auto
Fingerprint:	-
Remote Address:	-
Connected Local Subnet(s):	
Connected Local Host (s):	
Tunnel Interface Address:	-
Connected Remote Subnet(s):	

Description of the displayed values

- **Status**
Shows the status of the connection to SINEMA RC Server.
- **Device Name**
If configured, the name of the device is displayed.
- **Device Location**
If configured, the location of the device is displayed.
- **GSM Number**
If configured, the phone number of the device is displayed.
- **Vendor**
If configured, the entry is displayed.
- **Comment**
If configured, the comment is displayed.
- **Type of Connection (Server)**
Shows which type of connection is set on the SINEMA RC Server.

- **Type of Connection (Device)**
Shows which type of connection is set on the device.
- **Fingerprint**
Shows the fingerprint of the server certificate. Is only displayed when the fingerprint is used for verification.
- **Remote Address**
Shows the IP address of the SINEMA RC Server.
- **Connected Local Subnet(s)**
Shows the IP addresses of the local subnets. Is only displayed when the option "Connected local subnets" is enabled on the SINEMA RC Server. You will find further information on this in the Operating Instructions of the SINEMA RC Server.
- **Connected Local Host (s)**
Shows the destination IP address of the hosts that can be reached.
- **Tunnel Interface Address**
Shows the IP address of the virtual tunnel interface.
- **Connected Remote Subnet(s)**
Shows the subnets of the SINEMA RC Server that are reachable for the device. Which subnets are reachable for the device depends on the communications relations on the SINEMA RC Server. You will find further information on this in the Operating Instructions of the SINEMA RC Server.

5.5.21 OpenVPN

5.5.21.1 Client

The WBM page shows the status of the activated OpenVPN connections.

OpenVPN Client Information						
Name	Remote Server	Port	Tunnel Interface IP	Exported Subnets	Routed Subnets	Status
Refresh						

Description

The table contains the following columns:

- **Name**
Shows the name of the OpenVPN connection.
- **Remote Server**
Shows the IP address or the hostname of the OpenVPN server.
- **Port**
Shows the port.

- **Tunnel Interface IP**
Shows the IP address of the virtual tunnel interface.
- **Exported Subnets**
Shows the IP address of the local subnets.
- **Routed Subnets**
Shows the subnets of the OpenVPN server.
- **Status**
Shows the status of the OpenVPN connection.

5.5.21.2 Server

The WBM page shows the status of the activated OpenVPN server.

OpenVPN Server Information						
Client Server						
Name	Server Port	Cert CN	Client IP	Bytes Received	Bytes Sent	Connected Since
Refresh						

Description of the displayed values

The table contains the following columns:

- **Name**
Shows the name of the OpenVPN server.
- **Server Port**
Shows the port via which the OpenVPN server sends data.
- **Certificate CN**
Shows the "Common Name" of the certificate used. The Common Name designates the domain for which the certificate is issued.
- **Client IP address**
Shows the IP address of the OpenVPN server.
- **Received bytes**
Shows how many bytes were received.
- **Sent bytes**
Shows how many bytes were sent.
- **Connected since**
Shows how long a connection has been present.

5.5.22 Redundancy

5.5.22.1 Overview

MSTP-CIST configuration

The page consists of the following parts.

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

Overview

Overview

Spanning Tree

Bridge Priority: 32768

Bridge Address: 00-1b-1b-9a-31-94

Root Port: -

Topology Changes: 2

Bridge Hello Time: 2

Bridge Forward Delay: 15

Bridge Max Age: 20

Bridge Max Hop Count: 20

Root Priority: 32768

Root Address: 00-1b-1b-9a-31-94

Root Cost: 0

Last Topology Change: 1min

Root Hello Time: 2

Root Forward Delay: 15

Root Max Age: 20

Root Hop Count: 0

Refresh

Description of the displayed values

The page contains the following boxes:

- **Bridge Priority / Root Priority**
The Bridge Priority decides which device becomes the Root Bridge. The Bridge with the highest priority becomes the Root Bridge. The lower the value, the higher the priority. If several devices in a network have the same priority, the device whose MAC address has the lowest numeric value will become the root bridge. Both parameters, bridge priority and MAC address together form the Bridge identifier. Since the root bridge manages all path changes, it should be located as centrally as possible due to the delay of the frames. The value for the bridge priority is a whole multiple of 4096 with a range of values from 0 through 61440.
- **Bridge Address / Root Address**
The bridge address shows the MAC address of the device and the root address shows the MAC address of the root bridge.

- **Root Port**
Shows the port 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: Supplement "sec" after the number
 - Minutes: Supplement "min" after the number
 - Hours: Supplement "hr" after the number
- **Bridge Hello Time / Root Hello Time**
Each bridge sends configuration frames (BPDUs) regularly. The interval between two such frames is the Hello time. The default for this parameter is 2 seconds.
- **Bridge Forward Delay / Root Forward Delay**
New configuration information is not used immediately by a bridge but only after the forwarding delay specified in the parameter. This ensures that operation is only started with the new topology after all the bridges have the required information. The default for this parameter is 15 seconds.
- **Bridge Max Age / Root Max Age**
When the max age timer elapses the received BPDU is discarded to be accepted as valid by the switch. The default value is 20s.
- **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.
- **Root Hop Count**
The number of nodes that need to be run through on the way to the root bridge.

5.5.22.2 Spanning Tree

Introduction

The page shows the current information about the spanning tree and the settings of the root bridge.

Spanning Tree

Overview

Spanning Tree

Spanning Tree Mode: RSTP

Bridge Priority: 32768

Bridge Address: d4-f5-27-a4-83-d8

Root Priority: 32768

Root Address: d4-f5-27-a4-83-d8

Root Cost: 0

Bridge Status: This bridge is the root

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

Refresh

Description

The following fields are displayed:

- Spanning Tree Mode**
Shows the set mode. You specify the mode in "Layer 2 > Configuration" and in "Layer 2 > Spanning Tree > General".
The following values are possible:
 - ' '
 - RSTP
- Bridge Priority / Root Priority**
Which device becomes the root bridge is decided by 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 switch.

- **Root Cost**
Shows the path costs from the device to the root bridge.
- **Bridge Status**
Shows the status of the bridge, e.g. whether or not the device is the root bridge.

The table has the following columns:

- **Port**
Shows the interfaces via which the device communicates.
- **Role**
Shows the status of the port. The following values are possible:
 - Disabled
The port was removed manually from the spanning tree and will no longer be taken into account by the spanning tree.
 - Designated
The port with the most favorable connection to a lower-level LAN segment. When RSTP starts, switches evaluate connections based on BPDUs. The most favorable connections are then used. Generally, all root bridge RSTP ports are Designated Ports because they are set to forwarding. The path costs and the port ID of the respective port determine which ports of the remaining nodes are selected as Designated Ports.
 - Alternate
The port with an alternative route to a network segment.
 - Backup
The port on which BPDUs from a port of the same switch that has a better connection to the root are received.
 - Root
The port that provides the best route to the root bridge.
 - Master
This port points to a root bridge located outside the MST region.
- **Status**
Shows the current status of the interface. The values are only displayed. The parameter depends on the configured protocol.
 - 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**
Shows the compatibility mode of Spanning Tree used by the port.

- **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. If several ports of a device have the same value, the port with the lowest port number is selected.

The calculation of the path costs is based largely on the transmission speed. The higher the achievable transmission speed is, the lower the value of the path costs.

Typical values for path costs with rapid spanning tree:

- 10,000 Mbps = 2,000
- 1000 Mbps = 20,000
- 100 Mbps = 200,000
- 10 Mbps = 2,000,000

- **Edge Type**

Shows the type of the connection. The following values are possible:

- Edge Port
There is an end device at 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 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.

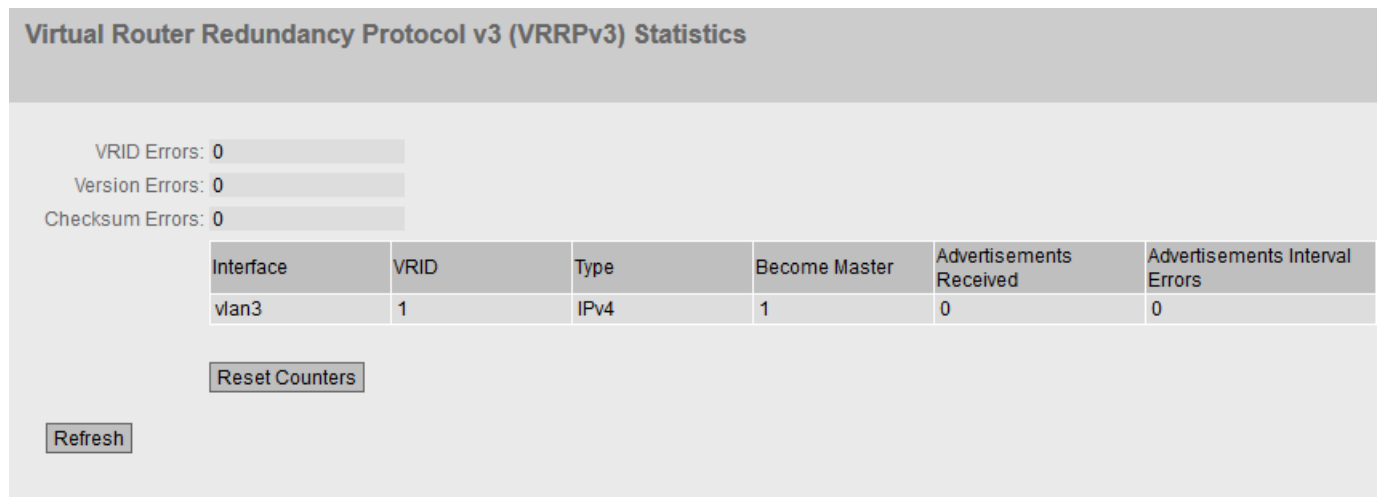
Note

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

5.5.23 VRRPv3 Statistics

Introduction

This page shows the statistics of the VRRPv3 protocol and all configured virtual routers.



Description

The following fields are displayed:

- **VRID Errors**
Shows how many VRRPv3 packets containing an unsupported VRID were received.
- **Version Errors**
Shows how many VRRPv3 packets containing an invalid version number were received.
- **Checksum Errors**
Shows how many VRRPv3 packets containing an invalid checksum were received.

The table has the following columns:

- **Interfaces**
Interface to which the settings relate.
- **VRID**
Shows the ID of the virtual router. Valid values are 1 ... 255.
- **Address Type**
Shows the version of the IP protocol.
- **Become Master**
Shows how often this virtual router changed to the "Master" status.
- **Advertisements Received**
Shows how many VRRPv3 packets were received.

- **Advertisement Interval Errors**
Shows how many bad VRRPv3 packets were received whose interval does not match the value set locally.

IP TTL Errors	Prio 0 received	Prio 0 sent	Invalid Type	Address List Errors	Packet Length Errors
0	0	0	0	0	0

- **IP TTL Errors**
Shows how many bad VRRPv3 packets were received whose TTL (Time to live) value in the IP header is incorrect.
- **Prio 0 received**
Shows how many VRRPv3 packets with priority 0 were received. VRRPv3 packets with priority 0 are sent when a master router is shut down. These packets allow a fast handover to the relevant backup router.
- **Prio 0 sent**
Shows how many VRRPv3 packets with priority 0 were sent. Packets with priority 0 are sent when a master router is shut down. These packets allow a fast handover to the relevant backup router.
- **Invalid Type**
Shows how many bad VRRPv3 packets were received whose value in the "Type" field of the IP header is invalid.
- **Address List Errors**
Shows how many bad VRRPv3 packets were received whose address list does not match the locally configured list.
- **Packet Length Errors**
Shows how many bad VRRPv3 packets were received whose length is not correct.

5.5.24 Security

5.5.24.1 Overview

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

Note

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

Security Overview

OverviewSupported Function RightsRolesGroups

Services

Telnet Server: enabledSSH Server: enabledSSH Fingerprint: Rsa key(md5): d0:94:ce:ae:2a:01:a1:22:c4:74:6d:35:a1:c4:37:11Rsa key(sha256): XBf2PXVgJUvKbnGuJT1H4o725gfoNjti7yUQvWQjkLcEcdsa key(md5): 38:75:02:a1:e6:ff:08:9e:cd:dd:90:d6:6e:27:b6:47Ecdsa key(sha256): rk07wFsfsmnLnDDAkwnY9eJICqATdkO5HPmoYNqimFQWeb Server: HTTP/HTTPS SNMP: SNMPv1/v2c/v3Login Authentication: Local Password Policy: high

Local User Accounts

User Account	Role
admin	admin

External User Accounts

User Account	Role
admin	admin

Refresh

Description

Services

The "Services" list shows the security settings.

- **Telnet Server**

You configure the setting in "System > Configuration".

- Enabled: Unencrypted access to the CLI.
- Disabled: No unencrypted access to the CLI.

- **SSH Server**

You configure the setting in "System > Configuration".

- Enabled: Encrypted access to the CLI.
- Disabled: No encrypted access to the CLI.

- **SSH fingerprint**

The following SSH fingerprints are displayed:

- MD5
- SHA256

- **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.

- **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.

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

- **User Account**

Shows the name of the local user.

- **Role**

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

Local and external user accounts

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

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

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

In the table "External User Accounts" a user is linked to a role. In this example, the user "admin" is linked to the role "admin". 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.

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.

5.5.24.2 Supported Function Rights

Note

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

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

Supported Function Rights	
Overview	Supported Function Rights
Roles	Groups
Function Right	Description
1	Read-only access to configuration data.
15	Read/write access to configuration data.
Refresh	

Description of the displayed values

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

5.5.24.3 Roles

Note

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

The page shows the roles valid locally on the device.

User Roles			
Overview	Supported Function Rights	Roles	Groups
Role	Function Right	Description	Remote Access
user	1	System defined role, with readonly access to configuration data of this component.	none
admin	15	System defined role, with read/write access to configuration data of this component.	none
default	1	Internal role, for authenticated users without group/role mapping in this component.	none
everybody	0	Internal role, assigned to users when authentication fails. Access will be denied.	none
Refresh			

Description

The table contains the following columns:

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

5.5.24.4 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 roll is defined locally on the device.

User Groups

OverviewSupported Function RightsRolesGroups

Group	Role	Description
Service_GR	user	

Refresh

Description of the displayed values

The table has the following columns:

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

5.5.25 VXLAN

M876RM1224MUx85x

This page shows the current content of the VXLAN NVE Peer table.

VXLAN NVE Peers

Interface	Remote VTEP IP Address	Remote MAC Address	MAC Type	Arp Suppression
nve10/100	203.0.113.33	00-1b-1b-b6-32-7a	Static	-

Refresh

Description

The table contains the following columns:

- **Interface**
Displays the NVE interface via which the row entry was learned.
- **Remote VTEP IP Address**
Shows the IPv4 address of the remote VTEP.
0.0.0.0 is displayed for locally connected MAC addresses.
- **VNI ID**
Shows the VNI segment of which the remote VTEP is a member.
- **Remote MAC Address**
Shows the MAC address of the remote VTEP that the device learned or that was configured.
- **MAC Type**
Shows how the MAC address of the remote VTEP is obtained.
 - Static:
The MAC and IP addresses were configured under "Layer 2 > VXLAN > Static MAC Addresses". The static addresses are stored permanently; in other words, they are not deleted when the aging time expires or when the device is restarted.
 - Dynamic:
The VTEP of the device obtains the MAC address from the received frame.
- **Arp Suppression**
This function is not supported.

5.5.26 System Time

MUx85x

This page shows the system time settings for the device.

System Time

Current System Time: 01/05/2024 10:08:13

Last Synchronization Time: Date/time not set

Last Synchronization Mechanism: Not set

Time Zone: +00:00

Daylight Saving Time: inactive (offset + 0h)

Fallback Period[seconds]: 3600

Time Service	Priority	Status
NTP	1	disabled
SNTP	2	disabled
SINEC	3	disabled
GPS	6	disabled
Cellular	7	enabled

Description

The page contains the following boxes:

- **Current System Time**
Shows the set date and the time in the format "MM/DD/YYYY HH:MM:SS".
- **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-of-day synchronization was performed.
 - Not set
The time was not set.
 - Manual
Manual time setting
 - NTP
Automatic time-of-day synchronization with NTP
 - SNTP
Automatic time-of-day synchronization with SNTP
 - SIMATIC Time Client
Automatic time-of-day synchronization using the SIMATIC time frame
 - GPS
Shows whether the time is received via the GPS signal.
 - Cellular
Shows whether the time is received via a mobile wireless network. Priority
- **Time Zone**
Shows the time zone you are using in the format "(+/-)HH:MM". The time zone relates to UTC coordinated universal time.
- **GPS Daylight Saving Time**
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.
- **Fallback period[seconds]**
Shows the wait time after which the replacement time service synchronizes the system time. Range of values 1 ... 86400. Default value 3600.

The table has the following columns:

- **Time Service**
 - NTP
Shows whether the time is synchronized via NTP.
 - SNTP
Shows whether the time is synchronized via SNTP.
 - SIMATIC Time Client
Shows whether the time is synchronized via SINEC.
 - GPS
Shows whether the time is received via the GPS signal.
 - Cellular
Shows whether the time is received via a mobile wireless network.
- **Priority**
Shows the priority of a time service.
- **Status**
Shows the status of the time service.

5.5.27 Firewall Monitoring

This page shows all connections currently running over the firewall (Firewall-State).

Firewall Monitoring								
Select	Proto L3	Proto L4	Src Addr	Src Port	Dst Addr	Dst Port	Timeout (s)	State
☐	IPv4	TCP	192.168.16.23	60261	192.168.16.153	443	300	ESTABLISHED
☐	IPv4	TCP	192.168.16.23	60241	192.168.16.153	443	3	TIME_WAIT

12 entries.

Description

The table contains the following columns:

- **Select**
Select the row you want to delete.
- **L3 protocol**
Shows the Layer 3 protocol (e.g. IPv4 or IPv6) of the connection.
- **L4 protocol**
Shows the Layer 4 protocol (e.g. TCP, UDP, ICMP) of the connection.
- **Source IP address**
The IP address of the device that initiates the connection.

- **Source port**
Source port from which the connection was initiated. With ICMP, the value is "0".
- **Destination IP address**
IP address of the device to which the connection was established.
- **Destination port**
Destination port to which the connection was established. With ICMP, the value is "0".
- **Timeout (s)**
Time in seconds after which the connection is automatically terminated if no communication takes place.
- **Status**
Status of the connection. Only relevant with TCP and SCTP.

5.6 "System" menu

5.6.1 Configuration

System configuration

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

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

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

Note

Change standard port

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

Reserved ports

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

Firewall

The firewall is reinitialized after the ports are changed. This means that the changed ports are applied in the firewall rules. Existing connections, for example, via the dynamic firewall, can be used with restrictions during this time.

System Configuration

☐ Telnet Server
Telnet Port: 23

☒ SSH Server
SSH Port: 22
SSH Key Exchange Algorithm Level: High ▼

☒ HTTP Server
HTTP Port: 80

☒ HTTPS Server
HTTPS Port: 443
HTTP Services: Redirect HTTP to HTTPS ▼

Minimum TLS Version: TLSv1.2 ▼

Default Login Page: Configuration ▼

☐ SMTP Client
☒ Syslog Client

DCP Server: Read/Setup ▼
Time: Manual ▼

SNMP: SNMPv1/v2c/v3 ▼
☒ SNMPv1/v2 Read-Only
☒ SINEMA Configuration Interface

Cache Write Cycle Time[s]: 100

DHCP DUID Configuration
DUID-Type: DUID-LLT ▼

Link-layer Address Plus Time: 00-01-00-01-00-00-00-30-2F-1E-53-88-08

Vendor Enterprise Number: 00-02-00-00-10-E9-56-50-53-34-31-39-31-33-32-32

Link-layer address: 00-03-00-01-30-2F-1E-53-88-08

Configuration Mode: Automatic Save ▼

Minimum Config-File Version: V1.0 ▼

☐ Invert Digital Output
☐ Retain Digital Output

Config-File Checksum: 715cbef0be56bfe7d692285001a8b6fd97abcc84e297 ...

[Write Startup Config](#)

[Set Values](#) [Refresh](#)

Description

The page contains the following boxes:

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

- **SSH Server**
Enable or disable the "SSH Server" service for encrypted access to the CLI.
- **SSH Port**
Standard port 22 is the default. You can optionally enter a port number in the range 1024 ... 49151 or 49500 ... 65535.
- **SSH key exchange algorithm level**
From the drop-down list, select the SSH key exchange algorithm level for SSH access to the CLI. The settings options are "Low" and "High". The two levels contain the following encryption algorithms:

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

Note

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

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

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

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

- TeraTerm
- PuTTY
- STS

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

5.6 "System" menu

- **HTTPS Port**
Standard port 443 is the default. You can optionally enter a port number in the range 1024 ... 49151 or 49500 ... 65535.
- **HTTP Services**
Specify how the WBM is accessed:
 - HTTPS
Access to the WBM is only possible with HTTPS.
 - HTTP/HTTPS
Access to the WBM is only possible with HTTP and HTTPS.
 - Redirect HTTP to HTTPS
Access via HTTP is automatically diverted to HTTPS.
- **Min. TLS version**
Specify which minimum TLS version is used.
- **Default Login Page**
Specify the login page with which the WBM starts by default.
 - Firewall
Logging into the WBM page for dynamic firewall
 - Configuration
Logging into the WBM
- **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 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.
 - Read/Setup
As long as the default password of the administrator has not been changed, the device parameters can be both read and changed via DCP. Once the default password has been changed, the device parameters can no longer be changed via DCP.

- **Time**
Select the setting from the drop-down list. The following settings are possible:
 - Manual
The system time is set manually. You can configure other settings in "System > System Time > Manual Setting".
 - SIMATIC Time
The system time is set using a SIMATIC time transmitter. You can configure other settings in "System > System Time > SIMATIC Time Client".
 - SNTP Client
The system time is set via an SNTP server. You can configure other settings in "System > System Time > SNTP Client".
 - NTP Client
The system time is set via an NTP server. You can configure other settings in "System > System Time > NTP Client".
- **SNMP**
Select the protocol from the drop-down list. The following settings are possible:
 - "-" (SNMP disabled)
Access to device parameters via SNMP is not possible.
 - SNMPv1/v2c/v3
Access to device parameters is possible with SNMP versions 1, 2c or 3. You can configure other settings in "System > SNMP > General".
 - SNMPv3
Access to device parameters is possible only with SNMP version 3. You can configure other settings in "System > SNMP > General".
- **SNMPv1/v2 Read Only**
Enable or disable write access to SNMP variables with SNMPv1/v2c.
- **SINEMA Configuration Interface**
If the SINEMA configuration interface is enabled, you can download configurations to the device using STEP 7 Basic / Professional.
- **Cache write cycle time[s]**
Specify the amount of time in seconds after which the log entry is written to the internal flash memory.
Range of values: 2 ... 200
Default value: 2
- **DUID-Type**
Specify which DUID type is used. The DUID types are defined in RFC 3315.
 - DUID-LLT
DUID is based on the link layer address of the interface and a time stamp
 - DUID-EN
DUID is assigned by the vendor (EN = enterprise number)
 - DUID-LL
DUID is based on the link layer address of the interface

- **Link-layer Address Plus Time**

The value is based on the link layer address of the interface and a time stamp. The value is regenerated each time the factory settings are restored.

- **Vendor Enterprise Number**

The value is based on the enterprise number specific to the vendor. The value is regenerated each time the factory settings are restored.

- **Link-layer address**

The link-layer address is based on the MAC address. The value is regenerated each time the factory settings are restored.

- **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 before 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. Click 'Write Startup Config' to save the changes immediately."

Note

Interrupting the save

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

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

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

- Trial

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

To save changes in the configuration file, use the "Write startup config" button. The display area also shows the message "Trial Mode Active – Press the "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.

- **Minimum Config-File Version**

Specify the minimum version that a configuration file must have to be loaded into the device. The versions differ in the signature of the file header. Configuration files of Version 2.0 have better protection against tampering.

The saving of a configuration file is independent of this setting. Configuration files that were saved with a firmware version $\leq$ V7.2 always correspond to V1.0. Configuration files that were saved with a firmware version $\geq$ 8.0 correspond to V2.0.

- V1.0

With this setting, you can load configuration files with V1.0 and V2.0 into the device.

- V2.0

With this setting, you can load only configuration files with V2.0 into the device.

- **Invert Digital Output**

If this is enabled, the digital output switches to the opposite state after an event occurs. The change will only take effect in the next switching phase.

Default value: Disabled.

Example: This option is disabled initially. If there is no VPN connection, the digital output is open. After all VPN tunnels have been established, the digital output is switched through (closed). After the option is enabled, the digital output switches to the opposite state and is closed as long as no VPN tunnels are established and opened as soon as the VPN tunnels are established.

- **Retain Digital Output** (only for device variants with DI/DO)

When the option is enabled, the current state of the digital output is saved in the configuration and restored after a restart.

Default value: Disabled.

- **Checksum for configuration file**

Shows the checksum to validate the currently running configuration file.

Procedure

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

5.6.2 General

5.6.2.1 Device

This WBM page contains the general device information.

Device

Device Coordinates

Current System Time: 11/21/2018 01:48:39

System Up Time: 1h 28m 18s

Device Type: SCALANCE S615

System Name: Name

System Contact: Contact

System Location: Location

☒ Cyclic WBM status update

Set Values Refresh

Description

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

Note

Permitted characters

The following printable ASCII characters (0x20 to 0x7e) are permitted in the input fields **"System Name"**, **"System Contact"** and **"Device Location"**:

- 0123456789
- A...Z a...z
- !"#\$%&'()*+,-./:;<=>?@ [\]_{}~^`

- **Cyclic WBM status update**
When this is disabled, automatic update of the WBM is switched off. This is suitable for slow 2G connections or contracts with very limited data volume.
The following must be taken into account here:
 - No status display update
 - No automatic logoff after user inactivity
 - No message in trial mode
 - No message on automatic saving
 - No progress display when saving or uploading files
 - No automatic forwarding to the changed IP address

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.

Note: Steps 1 to 3 can also be performed with the SNMP Management Tool.

5.6.2.2 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.

Determining the coordinates and the input formats

Use an interactive map or a GPS receiver to obtain the geographical coordinates of the device.

You can enter the geographical coordinates in the format degrees, minutes, seconds (DDD°MM'SS") or in decimal degrees (DD.dddddd).

The format DDD°MM'SS" has the following meaning:

The value for the geographical latitude +49° 1' 31.67" means that the device is located at 49 degrees, 1 arc minute and 31.67 arc seconds northerly latitude.

The southerly latitude is shown by a preceding minus sign or the letter N (northerly latitude) or S (southerly latitude), e.g. 49° 1' 31.67" N.

The value for the geographical longitude +8° 20' 58.73" means that the device is located at 8 degrees, 20 minutes and 58.73 seconds easterly longitude.

A western longitude is indicated by a preceding minus sign or the letter E (easterly longitude) or W (westerly longitude), e.g. 8° 20' 58.73" E.

The GPS coordinates are displayed in the format DD.dddddd. "DD" stands for the longitude and "dddddd" stands for the decimal longitude.

Heights are shown in dddd m format. 33 m means that the device is located at a height of 33 m above sea level. Heights below sea level (for example the Dead Sea) are indicated by a preceding minus sign.

Description

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

- **Latitude**
Here, enter the value for the northerly or southerly latitude of the location of the device.
- **Longitude**
Enter the value for easterly or westerly longitude for the location of the device.
- **Height**
Enter the value for the geographical height over or under zero (sea level) in meters.

MUM85x

The device MUM85x has the GPS function through which the device determines its location. The accuracy of the location determination is about 10 meters. Information on the GPS location is updated in the Event Log and Modem Quality Log every 10 minutes.

Additional fields:

- **Use GPS Location**
Enables or disables automatic read-out of the device location.
If you enable the option, the input fields for latitude, longitude and height are not editable.
- **GPS cycle time[s]**
Specify the amount of time in seconds after which the GPS location is updated. Default value: 60 seconds.
- **GPS position**
Shows the current GPS position in the decimal system in the order "Latitude, longitude, height".
- **Satellite**
Shows the number of available satellites.
- **HDOP (Horizontal Dilution Of Precision)**
Shows the accuracy of horizontal location detection. The lower the value, the more precise the position detection. The value 0 means no deviation from the actual position.

- **Speed**
Shows how fast the device moves.
- **Last synchronization**
Shows the status of the synchronization:
 - Synced
Location determination was performed.
 - Not Synced
Location determination was not performed.
 - $\geq$ <time in minutes>
The time in minutes since the last attempt to determine the location.

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.

5.6.3 Restart

5.6.3.1 Restart

Resetting to the defaults

Restart of the device can take place manually or as scheduled using this page. In addition, there are various options for resetting to the device defaults.

Restart

Restart | Sleep Mode

Restart System

Restore Memory Defaults and Restart

Restore Factory Defaults and Restart

Restart in:

Backup:

Schedule restart

Cancel scheduled restart

Set Values Refresh

Restart

Note the following points about restarting a device:

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

Note**SCALANCE MUX85x not reachable after changes in the 5G infrastructure**

Restart the device if fundamental parameters have been changed in the 5G infrastructure.

Description

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

- **Restart**

Click this button to restart the system. You must confirm the restart in a dialog box. During a restart, the device is reinitialized, the internal firmware is reloaded, and the device runs a self-test. The settings of the start configuration are retained, e.g. the IP address of the device. The learned entries in the address table are deleted. You can leave the browser window open while the device restarts. After the restart you will need to log in again.

- **Restore Memory Defaults and Restart**

Click this button to restore the factory configuration settings with the exception of the protected presets and to restart the device.

The protected presets include the following parameters:

- IP addresses
- Subnet mask
- IP address of the default gateway
- DHCP client ID
- DHCP
- System name
- System location
- System contact
- User names and passwords
- Login text
- PROFINET Name of Station

- **Restore Factory Defaults and Restart**

Click this button to restore the factory defaults for the configuration. The protected defaults are also reset. Created eSIM profiles are deleted on SCALANCE MUx85x.

An automatic restart takes place.

SCALANCE MUx85x: Do not switch off the device until it has finished restarting. If the device is switched off while it is restarting, eSIM profiles may not be fully deleted. As a result, no message is sent to the mobile network provider about the eSIM to be released. In this case, you must order a new eSIM for your mobile plan.

Note

By resetting to the factory configuration settings, the device loses its configured IP address, see section "Requirements for operation (Page 42)".

- M87x, RM1224, MUx85x, M81x, M804PB: The device can once again be reached at the IP address 192.168.1.1 that was set in the factory.
 - M826: An IP address must be assigned to the device.
-

- **Restart in**

Specify the time after which the device restarts.

- **Backup**

The configuration backups under "System > Configuration Backup" can be selected. Before the scheduled restart, the device applies the configurations of the selected backup and continues working with them after the restart.

All configurations made up to this point that have not been saved in a backup are lost.

With the "-" setting, no file is selected and the device uses the current configuration after the restart.

- **Schedule restart**

When you click this button, a timer starts and runs backwards with the defined time. When the timer has expired, the device restarts. The timer is not automatically updated.

The following message is also displayed in the display area: "The automatic restart starts in [...] minutes. Click 'Cancel scheduled restart' to cancel the restart". This message can be seen on every WBM page until you cancel the restart or the SCALANCE device is restarted.

Note

Unsaved configuration is lost after reboot

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

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

- **Cancel scheduled restart**

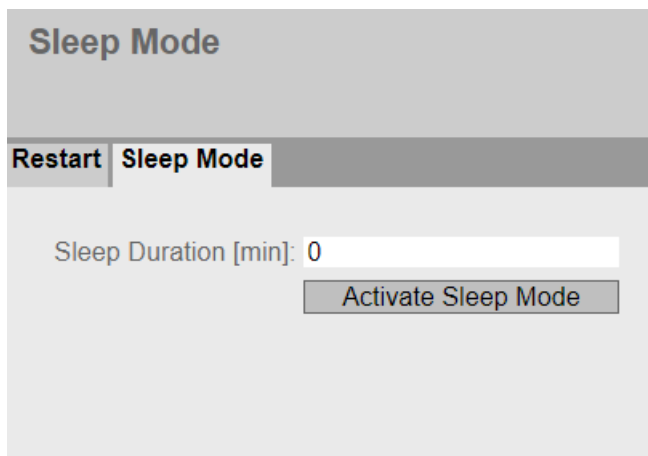
With this button you disable the timer for the scheduled restart.

5.6.3.2 Sleep Mode

MUM85x

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

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



Description

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

Procedure

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

Result

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

Note

Retaining the state of the digital output

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

5.6.4 Load&Save

5.6.4.1 File list

Overview of the file types

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

Area	File type	Description	Upload	Save	Delete ¹⁾
Update	Firmware	The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be downloaded to the device.	X	X	--

Area	File type	Description	Upload	Save	Delete ¹⁾
Configuration	Config	This file contains the start configuration. Among other things, this device contains the definitions of the users, roles, groups and function rights. The passwords are stored the file "Users". The file can be supplied with a password before download. To load the file into the device successfully, use the specified password. You enter the password on the WBM page "Passwords (Page 228)". If the file is password-protected, you cannot load the file via DHCP with options 66 and 67.	X	X	--
	ConfigPack	Detailed configuration information, for example, start-up configuration, users, certificates, favorites, firmware of the device (if saved as well). The file can be supplied with a password before download. To load the file into the device successfully, use the specified password. You enter the password on the WBM page "Passwords (Page 228)". For more detailed information on creating and using the ConfigPack incl. firmware, refer to the section "Maintenance (Page 483)". If the file is password-protected, you cannot load the file via DHCP with options 66 and 67.	X	X	--
	ConfigPack-Backup	This ZIP file stores all the configuration backups you have created.	X	X	X
	LoginWelcomeMessage	The txt file contains the desired text or the ASCII type. Only pure text files in ASCII format are supported.	X	X	X
	RunningCLI	Text file with CLI commands This file contains an overview of the current configuration in the form of CLI commands. Passwords are masked in this file as follows: [PASSWORD] You can download the text file. The file is not intended to be uploaded again unchanged.	--	X	--
	RunningSINEMAConfig	You save the current device configuration in this file type for transfer to STEP 7 Basic/Professional. The file can be imported in STEP 7 Basic/Professional and installed on a device with the same article number and firmware version. Before you can save a file, you must assign a password for the "RunningSINEMAConfig" in the WBM under "System > Load&Save > Passwords". You also need this password to import the file into STEP 7 Basic/Professional. See also "SINEMAConfig"	--	X	--
	Script	Text file with CLI commands You can upload a script file in a device. The CLI commands it contains are executed appropriately. CLI commands for saving and loading files cannot be executed with the CLI script file.	X	--	--

5.6 "System" menu

Area	File type	Description	Upload	Save	Delete ¹⁾
	SINEMAConfig	You load configuration data that was exported via STEP 7 Basic/Professional for transfer to the WBM with this file type. To load a file, you must assign a password for the "SINEMAConfig" under "System > Load&Save > Passwords". You also need this password to export the file from STEP 7 Basic/Professional. See also "RunningSINEMAConfig"	X	--	--
	Users	File with user names and passwords	X	X	--
	WBMFav	WBM favorites This file contains the favorites that you created in the WBM. You can download this file and upload it into other devices.	X	X	X

Area	File type	Description	Upload	Save	Delete ¹⁾
Certificate & Key	HTTPSCert	Default HTTPS certificates including key The preset and automatically created HTTPS certificates are self-signed. We strongly recommend that you create your own HTTPS certificates and make them available. We recommend that you use HTTPS certificates signed either by a reliable external or by an internal certification authority. The HTTPS certificate checks the identity of the device and controls the encrypted data exchange. The following file types can be loaded into the device. .pem To successfully load an HTTPS certificate with this data type into the device, the certificate must include the unencrypted private key. .p12 For HTTPS certificates with this file type, the private key is encrypted and secured with a password. To load the certificate successfully into the device, enter the password specified for the file on the WBM page "Passwords (Page 228)". It is recommended that you use password-protected certificates in the PKCS#12 format. The following certificates are supported: - ECDSA certificates created with secp521r1 (NIST P-521) - RSA certificates with a maximum key length of 4096 bits. The RSA web server certificate with a key length of 4096 bits is pre-installed on the device. - ECC certificates with a key length of 256 bits	X	X	X
	SSHPrivate-KeyECDSA	SSH private key (ECDSA) The SSH key ecdsa-sha2-nistp521 is supported. There are files to which access is password-protected. To successfully load the file into the device, enter the password specified for the file on the WBM page "Passwords (Page 228)".	X	X	X
	SSHPrivate-KeyRSA	SSH private key (RSA) with and without password The following SSH keys are supported: - rsa-sha2-512 - rsa-sha2-256 There are files to which access is password-protected. To successfully load the file into the device, enter the password specified for the file on the WBM page "Passwords (Page 228)".	X	X	X
	X509Cert	Various nodes are certified with certificates. The following file types can be loaded into the device: .crt, pem, zip: Maximum file name length 255 characters	X	X	--

Area	File type	Description	Upload	Save	Delete ¹⁾
		.p12: Maximum file name length 248 characters There are files to which access is password-protected. To successfully load the file into the device, enter the password specified for the file on the WBM page "Passwords (Page 228)". The loaded files are listed in "Security > Certificates > Overview (Page 433)". For more information on certificates, refer to section "Certificates (Page 435)".			
Services & log	Debug	This file contains information for Siemens Support. It is encrypted and can be sent by e-mail to Siemens Support without any security risk.	--	X	X
	DebugExt	This file contains more detailed information for Siemens Support. It is encrypted and can be sent by e-mail to Siemens Support without any security risk. Saving the file may take some time.	--	X	--
	LogFile	File with entries from the event log table	--	X	--
	ModemQualityLog	Text file Among other things, these files contain information on signal strength, signal quality and the GPS position of the location. To detect the GPS position, enable "Use GPS Location" under "System > General > Coordinates"	--	X	--
	StartupInfo	Startup log file This file contains the messages that were entered in the log file during the last startup.	--	X	--
Information	MIB	Private MSPS MIB file "Scalance_m_msps.mib"	--	X	--
License ²⁾	LicenseConditions	The ZIP file contains the licensing conditions and copyright information for the open source software.	--	X	--

¹⁾ Deletion is only possible via HTTP/HTTPS.

²⁾ Only with SCALANCE MUX85x

5.6.4.2 HTTP

Loading and saving data via HTTP

The WBM allows you to store device data in an external file on your client PC or to load such data from an external file from the PC to the devices. This means, for example, that you can also load new firmware from a file located on your Admin PC. On this page, the certificates required to establish a secure VPN connection can also be loaded.

Firmware

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

Configuration files

Note

Configuration files and Trial mode/Automatic Save

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

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

CLI script file

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

Note

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

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

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

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

Requirements:

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

You can use the file types as follows:

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

X509 certificates

The following file types can be loaded into the device:

- .crt, pem, zip: Maximum file name length 255 characters
- .p12: Maximum file name length 248 characters

Load and Save via HTTP

HTTP TFTP SFTP Passwords

Update

Type	Description	Load	Save	Delete
Firmware	Firmware Update	Load	Save	

Configuration

Type	Description	Load	Save	Delete
Config	Startup Configuration	Load	Save	
ConfigPack	Startup Config, Users, Certificates and WBM favourites	Load	Save	
ConfigPackBackup	ConfigPackBackup	Load	Save	Delete
LoginWelcomeMessage	Login Welcome Message	Load	Save	Delete
RunningCLI	'show running-config all' CLI settings		Save	
RunningSINEMAConfig	SINEMA Running Configuration		Save	
Script	Script	Load		
SINEMAConfig	SINEMA Offline Configuration	Load		
Users	Users and Passwords	Load	Save	
WBM Fav	WBM favourite pages	Load	Save	Delete

Certificate & Key

Type	Description	Load	Save	Delete
HTTPSCert	HTTPS Certificate	Load	Save	Delete
SSHPrivateKeyECDSA	SSH Private Key (ECDSA)	Load	Save	Delete
SSHPrivateKeyRSA	SSH Private Key (RSA)	Load	Save	Delete
X509Cert	X509 Certificates	Load	Save	

Service & Log

Type	Description	Load	Save	Delete
Debug	Debug Information for Siemens Support		Save	Delete
DebugExt	Extended Debug Information for Siemens Support		Save	
LogFile	Event, Security, Firewall Logs		Save	
ModemQualityLog	Modem Quality Log		Save	Delete
StartupInfo	Startup Information		Save	

Information

Type	Description	Load	Save	Delete
MIB	SCALANCE M MSPS MIB		Save	

License

Type	Description	Load	Save	Delete
LicenseConditions	ZIP File with Open Source Software License Conditions		Save	

Refresh

Description

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

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

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

Note

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

Procedure

Uploading data using HTTP

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

Note

Files whose access is password protected

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

A dialog for uploading a file opens.

2. Go to the file you want to load and click "Open" in the dialog window.
The file is uploaded.
3. If a restart is necessary, a message to this effect will be output. Click the "OK" button and run the restart. If you click the "Abort" button, there is no device restart. The changes only take effect after a restart.
Whether or not a restart is necessary depends on the loaded file. Some files are executed immediately, for example the CLI script file, and new settings are applied without a restart. A restart is also not required after a new HTTPS server certificate is uploaded.

Note

Cell firmware update M87x / RM1224 / MUx85x

After a cell firmware update, the device automatically restarts

Downloading data using HTTP

1. Start the download by clicking the one of the "Save" buttons.
2. Select a storage location and a name for the file.
3. Save the file.
The file is downloaded and saved.

Deleting files using HTTP

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

Reusing configuration data

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

Follow the steps below to reuse configuration data:

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

Note

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

Password-protected config file

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

5.6.4.3 TFTP

Loading and saving data via a TFTP server

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

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

Firmware

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

Configuration files

Note

Configuration files and Trial mode/Automatic Save

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

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

CLI script file

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

Note

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

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

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

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

Requirements:

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

You can use the file types as follows:

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

X509 certificates

The following file types can be loaded into the device:

- .crt, pem, zip: Maximum file name length 255 characters
- .p12: Maximum file name length 248 characters

5.6 "System" menu

Load and Save via TFTP

HTTP

TFTP

SFTP

Passwords

TFTP Server Address: 0.0.0.0

TFTP Server Port: 69

Update

Type	Description	Filename	Actions
Firmware	Firmware Update	firmware_SCALANCE_M800.sfw	Select action ▼

Configuration

Type	Description	Filename	Actions
Config	Startup Configuration	config_SCALANCE_M800.conf	Select action ▼
ConfigPack	Startup Config, Users, Certificates and WBM favourites	configpack_SCALANCE_M800.zip	Select action ▼
ConfigPackBackup	ConfigPackBackup	configbackup_SCALANCE_M800.zip	Select action ▼
LoginWelcomeMessage	Login Welcome Message	login_welcome_message.txt	Select action ▼
RunningCLI	'show running-config all' CLI settings	RunningCLI.txt	Select action ▼
RunningSINEMAConfig	SINEMA Running Configuration	sinema_config_running.zip	Select action ▼
Script	Script	Script.txt	Select action ▼
SINEMAConfig	SINEMA Offline Configuration	sinema_config.zip	Select action ▼
Users	Users and Passwords	users.enc	Select action ▼
WBM Fav	WBM favourite pages	wbmfav.txt	Select action ▼

Certificate & Key

Type	Description	Filename	Actions
HTTPSCert	HTTPS Certificate	https_cert	Select action ▼
SSHPrivateKeyECDSA	SSH Private Key (ECDSA)	sshprivatekeyecdsa	Select action ▼
SSHPrivateKeyRSA	SSH Private Key (RSA)	sshprivatekeyrsa	Select action ▼
X509Cert	X509 Certificates	x509_certs.zip	Select action ▼

Service & Log

Type	Description	Filename	Actions
Debug	Debug Information for Siemens Support	debug_SCALANCE_M800.bin	Select action ▼
DebugExt	Extended Debug Information for Siemens Support	DebugExt.bin	Select action ▼
LogFile	Event, Security, Firewall Logs	logfile_SCALANCE_M800.zip	Select action ▼
ModemQualityLog	Modem Quality Log	modem_quality.log	Select action ▼
StartupInfo	Startup Information	startup_SCALANCE_M800.log	Select action ▼

Information

Type	Description	Filename	Actions
MIB	SCALANCE M MSPS MIB	scalance_m_msps.mib	Select action ▼

License

Type	Description	Filename	Actions
LicenseConditions	ZIP File with Open Source Software License Conditions	OSS_Readme.zip	Select action ▼

Set Values

Refresh

Description

The page contains the following boxes:

- TFTP Server Address**
Enter the IP address or the FQDN (Fully Qualified Domain Name) of the TFTP server with which you exchange data.
- TFTP Server Port**
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.

222

SCALANCE M-800 and RUGGEDCOM RM1224 Web Based Management V8.2
Configuration Manual, 12/2024, C79000-G8976-C330-23

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

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

Note

Changing the file name

You can change the file name preset in this column.

To improve security, note the following:

- Assign the file a name as long as possible.
- Do not use spaces in the TFTP file name.
You can find information on the permitted characters in Appendix of the WBM (Page 513).

After clicking the "Set Values" button, the changed name is saved on the device and can also be used with the Command Line Interface.

- **Actions**
Select the action from the drop-down list. The selection depends on the selected file type, for example, you can only save a log file.
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 address of the TFTP server in "TFTP server address".
2. Enter the port of the TFTP server to be used in "TFTP Server Port".
3. If applicable, enter the name of a file in which you want to save the data or take the data from in "Filename".

Note

Files whose access is password protected

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

4. Select the action you want to execute from the "Actions" drop-down list.

5. Click "Set Values" to start the selected action.
6. If a restart is necessary, a message to this effect will be output. Click the "OK" button and run the restart. If you click the "Abort" button, there is no device restart. The changes only take effect after a restart.

Note

Cell firmware update M87x, MUx85x and RM1224

After a cell firmware update, the device automatically restarts

Reusing configuration data

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

Follow the steps below to reuse configuration data:

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

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

Note

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

Password-protected config file

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

5.6.4.4 SFTP

Loading and saving data via an SFTP server

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

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

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

Firmware

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

Configuration files

Note

Configuration files and Trial mode/Automatic Save

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

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

CLI script file

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

Note

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

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

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

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

Requirements:

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

You can use the file types as follows:

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

X509 certificates

The following file types can be loaded into the device:

- .crt, pem, zip: Maximum file name length 255 characters
- .p12: Maximum file name length 248 characters

5.6 "System" menu

Load and Save via SFTP

HTTP

TFTP

SFTP

Passwords

SFTP Server Address: 0.0.0.0

SFTP Server Port: 22

SFTP User:

SFTP Password:

SFTP Password Confirmation:

Update

Type	Description	Filename	Actions
Firmware	Firmware Update	firmware_SCALANCE_M800.sfw	Select action ▼

Configuration

Type	Description	Filename	Actions
Config	Startup Configuration	config_SCALANCE_M800.conf	Select action ▼
ConfigPack	Startup Config, Users, Certificates and WBM favourites	configpack_SCALANCE_M800.zip	Select action ▼
ConfigPackBackup	ConfigPackBackup	configbackup_SCALANCE_M800.zip	Select action ▼
LoginWelcomeMessage	Login Welcome Message	login_welcome_message.txt	Select action ▼
RunningCLI	'show running-config all' CLI settings	RunningCLI.txt	Select action ▼
RunningSINEMAConfig	SINEMA Running Configuration	sinema_config_running.zip	Select action ▼
Script	Script	Script.txt	Select action ▼
SINEMAConfig	SINEMA Offline Configuration	sinema_config.zip	Select action ▼
Users	Users and Passwords	users.enc	Select action ▼
WBM Fav	WBM favourite pages	wbmfav.txt	Select action ▼

Certificate & Key

Type	Description	Filename	Actions
HTTPSCert	HTTPS Certificate	https_cert	Select action ▼
SSHPrivateKeyECDSA	SSH Private Key (ECDSA)	sshprivatekeyecdsa	Select action ▼
SSHPrivateKeyRSA	SSH Private Key (RSA)	sshprivatekeyrsa	Select action ▼
X509Cert	X509 Certificates	x509_certs.zip	Select action ▼

Service & Log

Type	Description	Filename	Actions
Debug	Debug Information for Siemens Support	debug_SCALANCE_M800.bin	Select action ▼
DebugExt	Extended Debug Information for Siemens Support	DebugExt.bin	Select action ▼
LogFile	Event, Security, Firewall Logs	logfile_SCALANCE_M800.zip	Select action ▼
ModemQualityLog	Modem Quality Log	modem_quality.log	Select action ▼
StartupInfo	Startup Information	startup_SCALANCE_M800.log	Select action ▼

Information

Type	Description	Filename	Actions
MIB	SCALANCE M MSPS MIB	scalance_m_mspms.mib	Select action ▼

License

Type	Description	Filename	Actions
LicenseConditions	ZIP File with Open Source Software License Conditions	OSS_Readme.zip	Select action ▼

Set Values

Refresh

Description

The page contains the following boxes:

- SFTP Server Address**
Enter the IP address or the FQDN of the SFTP server with which you exchange data.
- SFTP Server Port**
Enter the port of the SFTP server via which data exchange will be handled. If necessary, you can change the default value 22 to your own requirements.
- SFTP User**
Enter the user for access to the SFTP server. This assumes that a user with the corresponding rights has been created on the SFTP server. You can find information on the permitted characters in Appendix of the WBM (Page 513).

226

SCALANCE M-800 and RUGGEDCOM RM1224 Web Based Management V8.2
Configuration Manual, 12/2024, C79000-G8976-C330-23

- **SFTP Password**
Enter the password for the user.
You can find information on the permitted characters in Appendix of the WBM (Page 513).

- **SFTP Password Confirmation**
Confirm the password.

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

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

Note

Changing the file name

You can change the file name preset in this column. After loading on the device, the changed file name can also be used with the Command Line Interface.

You can find information on the permitted characters in Appendix of the WBM (Page 513).

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

Procedure

Loading or saving data using SFTP

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

Note

Files whose access is password protected

To save these files or load them into the device successfully, you need to enter the password specified for the file in "System > Load&Save > Passwords".

5. Select the action you want to execute from the "Actions" drop-down list.

6. Click "Set Values" to start the selected action.
7. If a restart is necessary, a message to this effect will be output. Click the "OK" button to run the restart. If you click the "Abort" button, there is no device restart. The changes only take effect after a restart.

Note**Cell firmware update M87x, MUx85x and RM1224**

After a cell firmware update, the device automatically restarts

Reusing configuration data

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

Follow the steps below to reuse configuration data:

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

Note

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

Password-protected config file

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

5.6.4.5 Passwords

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

Passwords					
HTTP TFTP SFTP Passwords					
Type	Description	Setting	Password	Password Confirmation	Status
Config	Startup Configuration	☐			-
ConfigPack	Startup Config, Users, Certificates and WBM favourites	☐			-
HTTPSCert	HTTPS Certificate	☐			-
RunningSINEMAConfig	SINEMA Running Configuration	☐			Required
SINEMAConfig	SINEMA Offline Configuration	☐			Required
SSHPrivateKeyECDSA	SSH Private Key (ECDSA)	☐			-
SSHPrivateKeyRSA	SSH Private Key (RSA)	☐			-
X509Cert	X509 Certificates	☐			-

Description

The table has the following columns:

- **Type**
Shows the file type.
- **Description**
Shows the short description of the file type.
- **Setting**
Can only be enabled if a password is configured.
When enabled, a check is made during loading to ensure that the password matches the password set for the file.
- **Password**
Enter the password for the file.
Entered passwords cannot be read as plain text; instead asterisks * are displayed.
You can find information on the permitted characters in Appendix of the WBM (Page 513).
- **Password Confirmation**
Confirm the new password.
- **Status**
 - Valid
The "Enabled" check box is selected and the password matches the file.
 - Invalid
The "Enabled" check box is selected but the password does not match the file, or no file has been loaded yet.
 - "-"
The password cannot be evaluated or is not yet being used. The "Enabled" check box is not selected.
 - Required
A password is required for loading or saving.

Procedure

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

5.6.5 Events

5.6.5.1 Event Configuration

Selecting system events

On this page, you define which system events are reported and how, or execute a follow-up reaction.

The following messages are always entered in the event log table and cannot be deselected:

- Changing the admin password
- Starting the device
- Operational status of the device, e.g. whether or not a PLUG is inserted
- Status of errors not yet dealt with

To send these messages to a Syslog server as well, select the "Syslog" check box for the event "System General Logs".

Event Configuration

Configuration | Severity Filters

Log Table Alarm Threshold: 1950

Event	E-mail	Trap	Log Table	Syslog	Fault	SMS	Digital Out	VPN Tunnel	Firewall	SIM Switchover	Copy To Table
All Events	No Change	No Change	No Change	No Change	No Change	No Change	No Change	No Change	No Change	No Change	Copy To Table
Cold/Warm Start	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	
Link Change	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	
Authentication Failure	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	
Power Change	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	
Fault State Change	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	
Security Logs	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	
Firewall Logs	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	
DDNS Client Logs	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	
System General Logs	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	
System Connection Status	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	
Digital In	☐	☐	☒	☐	☐	☐	☐	☒	☒	☐	
VPN Tunnel	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	
Secure NTP	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	
Configuration Change	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	
Service Information	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	
Mobile Data Usage	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	
Connection Check	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	
Modem Quality Log	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	
DHCP Server Log	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	
TCP Event Log	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	
Geofencing	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	
SIM Switchover	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	

Set Values Refresh

Description

- **Log Table Alarm Threshold**

Set the limit for the entries for each severity. A maximum of 2000 entries are possible per severity for the MUX85x and 350 for the other devices.

If the specified limit will be reached with the next entry, an alarm message is output, e.g. if 1950 is specified, the message that limit 1950 has been reached is output after entry 1949.

With Table 1, you can enable or disable all check boxes of a column of Table 2 at once.

Table 1 has the following columns:

- **All Events**
Shows that the settings are valid for all events of table 2.
- **E-mail / Trap / Log Table / Syslog / Fault / SMS / Digital Out / VPN Tunnel / Cloud Connector / Firewall**
Enable or disable the desired 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 "Event" column contains the following:

- Cold/Warm Start
The device was turned on or restarted by the user. In the error memory of the device a new entry is generated with the type of restart performed.
- Link Change
This event occurs only when the port status is monitored and has changed, see "System > Fault Monitoring > Link Change".
- Authentication Failure
This event occurs when access is attempted with an incorrect password.
- Power Change (only with MUX85x)
This event occurs only when power supply lines 1 and 2 are monitored. If the monitored cable has no voltage, an error is displayed. The event also occurs when the PoE power supply has failed. You can find additional information in the section "System > Fault Monitoring > Power Supply".
- Fault State Change
The fault status has changed. The fault status can relate to the activated port monitoring, the response of the digital output or the power supply monitoring.
For a fault to also be signaled by the fault LED "F", you must enable "Fault State Change" for the "Digital Out". In this case, the fault LED "F" lights up when an internal error occurs and the digital input is closed.
- Security Logs
An entry is made in the security log if the IPsec method is used for VPN.
- Firewall Logs
Each time individual firewall rules are applied, this is recorded in the firewall log. To do this, the LOG function must be enabled for the various firewall functions.
- DDNS Client Logs
The event occurs when the DDNS client synchronizes the assigned IP address with the hostname registered at the DDNS provider.
- System General Logs
Connection establishment, change to the configuration.
- System Connection Status
The connection status has changed.
- Digital In
The event occurs when the status of the digital input has changed.
- VPN Tunnel
The event occurs when the status of VPN (IPsec, OpenVPN, SINEMA RC) has changed.
- NTP (secure)
This event occurs when the device receives the system time from a secure NTP server or the NTPsecure authentication key for the NTP server has been updated.
- Configuration Change
This event occurs when the configuration of the device has changed.

- **Service Information**
For certain events, entries are made in the log table even without configuration. For these events, you can configure additional subsequent actions here (e-mail, trap, syslog).
- **Mobile data usage (only with M87x/ RM1224/ MUx85x)**
This event occurs when 75% or 100% of the defined data volume has been reached, see "Interfaces > Mobile > General".
- **Cloud Connector**
This event occurs when the operating state of the Cloud Connector has changed.
- **Connection Check**
This event occurs when connections are being monitored, see "System > Connection Check".
- **Modem Quality Log**
Entries on signal strength, signal quality and the GPS position of the location. The Modem Quality Log is written every 10 minutes.
- **DHCP Server Log**
DHCP events are logged. The prerequisite is that the DHCP server is enabled on the device.
- **TCP Event Log**
The device has received a TCP packet. The prerequisite is that the "TCP Event" function is enabled.
- **Geofencing (Only with MUM85x)**
The specified event occurs if the device enters the defined area or leaves it, depending on the configured condition; see "System > Geofencing".
- **SIM Switchover (only with MUM85x)**
The event occurs when the SIM card type has been changed, see "Interfaces > Mobile > General".
- **E-mail**
The device sends an e-mail. This is only possible if the SMTP server is set up and the "SMTP Client" function is enabled.
- **Trap**
The device sends an SNMP trap. This is only possible if "SNMPv1 Traps" is enabled in "System > Configuration".
- **Log Table**
The device writes an entry in the event log table, see "Information > 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 and the currently pending error is displayed under "Information > Faults".
- **SMS (only with M87x / RM1224 / MUx85x)**
The device sends an SMS. This is only possible if "System > SMS > Event SMS" is enabled and the telephone number of the receiver is configured.

- **Digital Out**
Controls the digital output or signals the status change with the "DO" LED.
The digital output is open by default and after every restart. The digital output is closed when you activate at least one event for the digital output. It also is no longer automatically connected to the fault LED. You connect the digital output with the fault LED under "Fault State Change".
- **VPN Tunnel**
Controls the forwarding of an event to a VPN connection (IPsec, OpenVPN, SINEMA RC). As long as the event is present, the VPN connection is switched to active.
- **Firewall**
Controls application of the user-defined rule set. The prerequisite is that a rule set is assigned to the digital input under "Security > Firewall > Dynamic rules".
- **Cloud Connector**
Controls the forwarding of an event to the TIA Portal Cloud Connector communication. The communication connection is active as long as the event is present.
- **SIM Switchover**
Controls the digital input or signals the status change with the "DI" LED.

Procedure

Establishing/terminating a VPN tunnel via the digital input

1. For the "Digital Input" event, enable the "VPN Tunnel" entry.
2. Configure the VPN connection
 - IPsec:
In "Operation", set "wait on DI" or "start on DI". You will find more information on this under "IPsec > Connections (Page 461)" and under "VPN connection establishment (Page 96)".
 - OpenVPN:
In "Operation" set "start on DI". You will find more information on this under "OpenVPN > Connections (Page 472)" and under "VPN connection establishment (Page 96)".
 - SINEMA RC:
In "Type of connection", set "Auto", "Digital Input" or "Digital Input & Wake-up SMS" (only with M87x/ RM1224/ MUX85x). With the "Auto" type of connection, you need to set the type of connection "Digital Input" or "Wake-up SMS & Digital Input" (only with M87x/ RM1224/ MUX85x) on the SINEMA RC Server under "Remote connections > Devices". You will find more information on this topic in the "SINEMA RC Server" operating instructions.
3. Click the "Set Values" button.

5.6.5.2

Severity Filters

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

Event Severity Filters

Configuration

Severity Filters

Client Type	Severity
E-Mail	Info
Log Table	Info
Syslog	Warning
SMS	Critical

Set Values

Refresh

Description

The table has the following columns:

- Client Type**
 Select the client type for which you want to make settings:
 - E-mail**
 Sending system event messages by e-mail.
 - Log Table**
 Entry of system events in the log table.
 - Syslog**
 Entry of system events in the Syslog file.
 - SMS** (only with M87x / RM1224 / MUx85x)
 System event messages sent per SMS.
- Severity**
 Select the desired severity. The following settings are possible:
 - Critical**
 System events with the severity Critical (Critical) are processed.
 - Warning**
 System events with the severity Warning (Warnings) or higher are processed: This means events of the categories "Warning" and "Critical".
 - Info**
 System events with the severity Info (Information) or higher are processed: This means events of the categories "Info", "Warning" and "Critical".

5.6 "System" menu

Procedure

Follow the steps below to configure the required level:

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

5.6.6 SMTP client

5.6.6.1 General

Network monitoring with e-mails

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

Simple Mail Transfer Protocol (SMTP) Client General

General Receiver

☒ SMTP Client

SMTP Server Address:

Select	Status	SMTP Server Address	Sender Address	Username	Password	Password Confirmation	Port	Security	Test	Test Result
☐	☒	192.168.16.10	Device1@auto.de				465	SSL/TLS	Test	Connection with server failed
☐	☒	192.168.16.200	Device1@auto.de				25	None	Test	
☐	☒	192.168.16.220					25	None	Test	

3 entries.

Requirements for sending e-mails

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

Description

The page contains the following boxes:

- **SMTP Client**
Enable or disable the SMTP client.
- **SMTP Server Address**
Enter the IP address or the FQDN (Fully Qualified Domain Name) of the SMTP server.

The table contains the following columns:

- **Select**
Select the check box in a row to be deleted.
 - **Status**
Specify whether this SMTP server will be used.
 - **SMTP Server Address**
Shows the IP address or the FQDN (Fully Qualified Domain Name) of the SMTP server.
 - **Sender Email Address**
Enter the e-mail address of the sender that is specified in the e-mail.
 - **User Name**
If necessary, enter the user name used for authentication on the SMTP server.
 - **Password**
If necessary, enter the password used for authentication on the SMTP server.
 - **Password Confirmation**
Repeat the password.
 - **Port**
Enter the port via which your SMTP server can be reached.
Factory settings:
 - 25 (None)
 - 465 (SSL/TLS and StartTLS)
 - **Security**
Specify whether transfer of the e-mail from the device to the SMTP server is encrypted. This is only possible when the SMTP server supports the selected setting.
-
- Note**
- 2-factor authentication (2FA)**
- 2-factor authentication is not supported.
-
- SSL/TLS
 - StartTLS
 - None: The e-mail is transferred unencrypted.
- **Test**
Sends a test email to the configured receivers.
 - **Test Result**
Shows whether the e-mail was sent successfully or not. If sending was not successful, the message contains possible causes.

Procedure

Configuring the SMTP server

1. Enable the "SMTP Client" function.
2. Enter the IP address or the FQDN of the SMTP server for "SMTP Server Address".

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

Note

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

Testing the configuration of the SMTP server

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

5.6.6.2 Recipient

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

Simple Mail Transfer Protocol (SMTP) Client Receiver

General **Receiver**

SMTP Server: 192.168.16.10 ▼

SMTP Receiver Email Address:

Select	SMTP Server	Send	SMTP Receiver Email Address
☐	192.168.16.10	☒	service@device.de

1 entry.

Description

The page contains the following boxes:

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

The table contains the following columns:

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

Procedure

Configuring an SMTP receiver

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

5.6.7 SNMP

5.6.7.1 General

Configuration of SNMP

Note

SNMPv3 configuration during a firmware update
As of firmware version 6.4, the SNMP configuration has been distributed across multiple WBM pages.
To delete the SNMPv3 configuration, follow these steps:

1. Delete all SNMPv3 views except for the predefined views **SIMATICNETRD** and **SIMATICNETWR**.
2. Delete all SNMPv3 access.
3. Delete all entries in the "SNMPv3 User to Group mapping" table.
4. Delete all SNMPv3 users.

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

Simple Network Management Protocol (SNMP) General

General

SNMPv3 Users

SNMPv3 User to Group mapping

SNMPv3 Access

SNMPv3 Views

Notifications

SNMP:

SNMPv1/v2c/v3

☐ SNMPv1/v2c Read Only

SNMPv1/v2c Read Community String:

public

SNMPv1/v2c Read/Write Community String:

private

☒ SNMPv3 User Migration

SNMP Engine ID:

80.00.10.e9.05.00.1b.1b.af.a2.00

SNMP Agent Listen Port:

161

Set Values

Refresh

Description

The page contains the following boxes:

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

Note

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

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

Note

Community String

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

The recommended minimum length for community strings is 6 characters.

For security reasons, only limited access to objects of the SNMPCommunityMIB is possible with the SNMPv1/v2c Read Community String. With the SNMPv1/v2c Read/Write Community String, you have full access to the SNMPCommunityMIB.

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

5.6 "System" menu

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

Procedure

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

5.6.7.2 SNMPv3 Users

User-specific security settings

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

Simple Network Management Protocol (SNMP) v3 Users

General | **SNMPv3 Users** | SNMPv3 User to Group mapping | SNMPv3 Access | SNMPv3 Views | Notifications

User Name:

Select	User Name	Authentication Protocol	Privacy Protocol	Authentication Password	Authentication Password Confirmation	Privacy Password	Privacy Password Confirmation
☐	Miller	MD5	DES	*****	*****	*****	*****

1 entry.

Description

The page contains the following boxes:

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

The table has the following columns:

- **Select**
Select the row you want to delete.
- **User Name**
Shows the created users.
- **Authentication Protocol**
Specify the authentication protocol for which a password will be stored.
The following settings are available:
 - None
 - MD5
 - SHA
 - SHA256
- **Privacy Protocol**
Specify the encryption protocol for which a password will be stored. This drop-down list is only enabled when an authentication protocol has been selected.
The following settings are available:
 - None
 - DES
 - AES
 - AES-256
- **Authentication Password**
Enter the authentication password in the first input box. This password must have at least 1 character, the maximum length is 32 characters.
Use passwords that are as long as possible with a high password strength.
- **Authentication Password Confirmation**
Confirm the password by repeating the entry.

5.6 "System" menu

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

Note**Length of the password**

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

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

Procedure

Create a new user

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

Delete user

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

5.6.7.3 SNMPv3 User to Group mapping

Configuration of group members

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

Simple Network Management Protocol (SNMP) v3 Groups

General

SNMPv3 Users

SNMPv3 User to Group mapping

SNMPv3 Access

SNMPv3 Views

Notifications

Group Name:

User Name:

- ▾

Select	Group Name	User Name
☐	Service	Miller

1 entry.

Create

Delete

Set Values

Refresh

Description

The page contains the following boxes:

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

The table has the following columns:

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

5.6.7.4 SNMPv3 Access

Security settings and assigning permissions

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

Note

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

Simple Network Management Protocol (SNMP) v3 Access

General

SNMPv3 Users

SNMPv3 User to Group mapping

SNMPv3 Access

SNMPv3 Views

Notifications

Group Name:

-

Security Level:

no Auth/no Priv

Select	Group Name	Security Level	Read View Name	Write View Name	Notify View Name
☐	Service	no Auth/no Priv	SIMATICNETRD	SIMATICNETWR	SIMATICNETRD

1 entry.

Create

Delete

Refresh

Description

The page contains the following boxes:

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

The table has the following columns:

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

Note

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

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

Procedure

Creating a new group

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

Modifying a group

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

Deleting a group

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

5.6.7.5 SNMPv3 Views

Configuration of SNMPv3 views

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

Simple Network Management Protocol (SNMP) v3 Views

GeneralSNMPv3 UsersSNMPv3 User to Group mappingSNMPv3 AccessSNMPv3 ViewsNotifications

View Name: -MIB Tree: iso

Select	View Name	MIB Tree	View Type
☐	MY_RD	org	Included
☐	MY_RD	private	Included
☐	MY_WR	1.3.6.1.3.6.18.1.1.1.1.83.73.77	Included
☐	SIMATICNETRD	iso	Included
☐	SIMATICNETRD	1.3.6.1.6.3.18.1.1	Excluded
☐	SIMATICNETRD	1.3.6.1.6.3.18.1.1.1.1.83.73.77.65.84.73.67.78.69.84.82.68	Included
☐	SIMATICNETWR	iso	Included

7 entries.

CreateDeleteSet ValuesRefresh

Note

Controlling the SNMPv1 and SNMPv2c access

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

Description

The page contains the following boxes:

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

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

The table has the following columns:

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

5.6.7.6 Notifications

SNMP traps and SNMPv3 notifications

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

Simple Network Management Protocol (SNMP) Notifications

General

SNMPv3 Users

SNMPv3 User to Group mapping

SNMPv3 Access

SNMPv3 Views

Notifications

☐ SNMPv1 Traps

SNMPv1/v2c Trap Community String: public

SNMPv3 Notify User: -

SNMPv3 Notify Security Level: no Auth/no Priv

Notification Receiver Type: SNMPv1 Trap

Notification Receiver Address:

Select	Notification Receiver Address	Notification Receiver Type	SNMP Engine ID	Notification
☐	192.168.178.107	SNMPv1 Trap	-	☐

1 entry.

Create

Delete

Set Values

Refresh

Description

The page contains the following boxes:

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

- **Notification Receiver Type**
The recipient type defines the SNMP version and the type of notification. SNMP inform notifications have to be acknowledged by the recipient, SNMP traps do not. The following options are possible:
 - SNMPv1 Trap
 - SNMPv2c Trap
 - SNMPv2c Inform
 - SNMPv3 Trap
 - SNMPv3 Inform
- **Notification Receiver Address**
Enter the IP address, the FQDN (Fully Qualified Domain Name) or the host name of the recipient station to which the device sends SNMP notifications. You can specify up to ten different recipients servers.

The table has the following columns:

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

Note

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

Procedure

Configuring a notification

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

5.6 "System" menu

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

Deleting a trap entry

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

5.6.8 System Time

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

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

5.6.8.1 Manual Setting

Manual setting of the system time

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

Manual System Time Setting

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

☒ Time Manually

System Time: 08/31/2018 12:27:05

Last Synchronization Time: 08/29/2018 09:25:43

Last Synchronization Mechanism: Manual

Daylight Saving Time: active (offset + 1h)

Description

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-of-day synchronization was performed.
 - Not set
The time was not set.
 - Manual
Manual time setting
 - SNTP
Automatic time-of-day synchronization with SNTP
 - NTP
Automatic time-of-day synchronization with NTP
 - SIMATIC
Automatic time-of-day synchronization using the SIMATIC time frame
- **Daylight Saving Time**
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.

5.6.8.2 Protocol Switchover

MUx85x

If the enabled service fails for the system time, another service can take over time synchronization. On this page, you can make settings for a backup time service if the preferred time service is temporarily not available.

Time Protocol Switchover

Manual Setting
Protocol Switchover
DST Overview
DST Configuration
Mobile Time
SNTP Client
NTP Client
SIMATIC Time Client
NTP Server

Fallback Period[seconds]: 3600

Time Service	Priority	Status
NTP	1	disabled
SNTP	2	disabled
SINEC	3	disabled
GPS	6	disabled
Cellular	7	disabled

Set Values
Refresh

Description

The page contains the following boxes:

- **Fallback period[seconds]**
Enter the wait time after which the replacement time service synchronizes the system time. Range of values 1 ... 86400. Default value 3600.

The table has the following columns:

- **Time Service**
 - NTP
Shows whether the time is synchronized via NTP.
 - SNTP
Shows whether the time is synchronized via SNTP.
 - SIMATIC NET
Shows whether the time is synchronized via SIMATIC time frame.
 - GPS
Shows whether the time is received via the GPS signal.
 - Cellular
Shows whether the time is received via a mobile wireless network.
- **Priority**
Enter the priority of the time services.
Range of values: 1 ... 255
- **Status**
Shows the status of the time service.

5.6.8.3 DST Overview

Daylight saving time switchover

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

Daylight Saving Time (DST) Overview								
Manual Setting	DST Overview	DST Configuration	SNTP Client	NTP Client	SIMATIC Time Client	NTP Server		
Select	DST No	Name	Year	Start Date	End Date	Recurring Date	State	Type
☐	1	DST 2018	2018	03/25 02:00	10/28 03:00	-	enabled	Date
1 entry.								
Create Delete Refresh								

Settings

The page contains the following boxes:

- **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 "Recurring", 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.

5.6 "System" menu

- **Status**
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.
 - Recurring
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 "Recurring", 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.

5.6.8.4 DST Configuration

Configuring the daylight saving time switchover

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

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

Settings

Note

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

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

- **DST No.**
Select the type of the entry.
- **Type**
Select how the daylight saving time changeover is made:
 - Date
You can enter a fixed date for the daylight saving time changeover.
This setting is suitable for regions in which the daylight saving time changeover is not governed by rules.
 - Recurring
You can define a rule for the daylight saving time changeover.
This setting is suitable for regions in which the daylight saving time always begins or ends on a certain weekday.
- **Name**
Enter a name for the entry.
The name can be a maximum of 16 characters long.

Settings with "Date" selected

DST Configuration

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

DST No: 1 ▼

Type: Date ▼

Name: DST 2018

Year: 2018

Start Date

Day: 25 ▼

Hour: 02:00 ▼

Month: March ▼

End Date

Day: 28 ▼

Hour: 03:00 ▼

Month: October ▼

Set Values Refresh

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

Settings with "Recurring" selected

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

- **Year**
Enter the year for the daylight saving time changeover.
- **Start Date**
Enter the following values for the start of daylight saving time:
 - Hour
Enter the hour.
 - Month
Enter the month.
 - Week
Enter the week.
You can select the first to fourth or the last week of the month.
 - Day
Enter the weekday.
- **End Date**
Enter the following values for the end of daylight saving time:
 - Hour
Enter the hour.
 - Month
Enter the month.
 - Week
Enter the week.
You can select the first to fourth or the last week of the month.
 - Day
Enter the weekday.

5.6.8.5 Mobile Time

MUM85x

Setting the time via GPS or mobile wireless signal

Note

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

The screenshot shows the 'Mobile Time' configuration page. At the top, there is a navigation bar with tabs: 'Manual Setting', 'Protocol Switchover', 'DST Overview', 'DST Configuration', 'Mobile Time' (selected), 'SNTP Client', and 'NTP Client'. Below the navigation bar, there are two sub-tabs: 'SIMATIC Time Client' and 'NTP Server'. The main content area displays the following settings:

- ☐ GPS Time
- ☒ Cellular Time
- Current System Time: 07/12/2023 13:23:55
- Last Synchronization Time: 07/10/2023 15:40:05
- Last Synchronization Mechanism: Manual
- GPS Time Zone: +00:00
- GPS Daylight Saving Time: inactive (offset + 0h)

At the bottom of the form, there are two buttons: 'Set Values' and 'Refresh'.

Description

The page contains the following boxes:

- **GPS Time**
When enabled, the device receives the time with the GPS signal from navigation satellites. The time is updated every 60 seconds.
- **Cellular Time**
When enabled, the device fetches the time via a mobile wireless network. The time is updated every 60 seconds.
- **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-of-day synchronization was performed. The following methods are possible:
 - Not set
The time was not set.
 - Manual
Manual time setting
 - SNTP
Automatic time-of-day synchronization with SNTP
 - NTP
Automatic time-of-day synchronization with NTP
 - SIMATIC
Automatic time-of-day synchronization using the SIMATIC time frame
 - Mobile Time
Automatic time synchronization via GPS or mobile wireless
- **GPS Time Zone**
Specify the time zone you are using in the format "(+/-)HH:MM". The time zone relates to UTC coordinated universal time.
The time in the "Current System Time" box is adapted accordingly.
- **GPS Daylight Saving Time**
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. Click the "GPS Time" or "Cellular Time" check box to activate fetching of the mobile time.
2. Click the "Set Values" button.

5.6.8.6 SNTP Client

Time-of-day synchronization in the network

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

Note

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

Simple Network Time Protocol (SNTP) Client

Manual Setting

DST Overview

DST Configuration

SNTP Client

NTP Client

SIMATIC Time Client

NTP Server

☐ SNTP Client

Current System Time: 08/31/2018 12:27:24

Last Synchronization Time: 08/29/2018 09:25:43

Last Synchronization Mechanism: Manual

Time Zone: +00:00

Daylight Saving Time: active (offset + 1h)

SNTP Mode: Poll

Poll Interval[s]: 64

SNTP Server Address:

Select	SNTP Server Address	SNTP Server Port	Primary
☐	192.168.1.1	123	☒

1 entry.

Create

Delete

Set Values

Refresh

Requirement

To receive the SNTP frames, enable the entry "System Time" under "Security > Firewall > Predefined IPv4 rules".

Description

The page contains the following boxes:

- SNTP Client**
When enabled, the device receives the system time from an SNTP server.
- 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-of-day synchronization was performed. The following types 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 coordinated universal time.

The time in the "Current System Time" box is adapted accordingly.

- **Daylight Saving Time**

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.

- **SNTP Mode**

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

- Poll
If you select this mode, the text 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. In this mode, IPv4 and IPv6 addresses are supported.
- Listen
With this type of synchronization, the device is passive and receives SNTP frames that deliver the time of day. The settings in the text boxes "SNTP Server Address" and "SNTP Server Port" have no effect in this mode. In this mode, IPv4 and IPv6 addresses are supported.

Note

SNTP Client in Listen mode and NTP Server cannot be enabled at the same time.

- **Poll Interval[s]**
Enter the interval between two time queries. In this box, you enter the polling interval in seconds. Possible values are 64 to 1024 seconds.
- **SNTP Server Address**
Enter the IP address, the FQDN (Fully Qualified Domain Name) or the host name of the SNTP server.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **SMTP Server Address**
Shows the IP address, the FQDN (Fully Qualified Domain Name) or the host name of the SMTP server.
- **SNTP Server Port**
Enter the port of the SNTP server.
The following ports are possible:
 - 123 (standard port)
 - 1025 to 36564
- **Primary**
The check mark is set for the SNTP server that you create first. If several SNTP servers have been created, the primary server is queried first.

Procedure

1. Click the "SNTP Client" check box to enable the automatic time setting.
2. In "Time Zone", enter the local time difference to world time (UTC).
The input format is "+/-HH:MM" because the NTP server always sends UTC time, for example +02:00 for CEST, the Central European Summer Time. This time is recalculated and displayed as the local time based on the specified time zone.
3. Select one of the following options from the "SNTP Mode" drop-down list:
 - Poll
For this mode, you need to configure the following:
 - time zone difference (step 2)
 - query interval (step 4)
 - time server (step 5)
 - Port (step 7)
 - complete the configuration with step 8.
 - Listen
For this mode, you need to configure the following:
 - time difference to the time sent by the server (step 2)
 - time server (step 5)
 - port (step 7)
 - complete the configuration with step 8.
4. In "SNTP Server Address", enter the address of the SNTP server whose frames will be used to synchronize the time of day.

5. In "SNTP Server Port", enter the port via which the SNTP server is available. The port can only be modified if the IP address of the SNTP server is entered.
6. In "Poll Interval[s]", enter the time in seconds after which a new time query is sent to the time server.
7. Click the "Set Values" button.

5.6.8.7 NTP Client

Automatic time-of-day setting with NTP

If time synchronization is to take place via NTP, define the time server that is used to synchronize the time.

Note

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

Network Time Protocol (NTP) Client

Manual Setting

Protocol Switchover

DST Overview

DST Configuration

Mobile Time

SNTP Client

NTP Client

SIMATIC Time Client

NTP Server

☐ NTP Client
☒ Secure NTP Client only

Current System Time: 07/12/2024 12:17:26

Last Synchronization Time: 07/12/2024 12:08:16

Last Synchronization Mechanism: Manual

Time Zone: +00:00

Daylight Saving Time: inactive (offset + 0h)

NTP Server Index: 1

Select	NTP Server Index	NTP Server Address	NTP Server Port	Poll Interval	Key ID	Hash Algorithm	Key	Key Confirmation
☐	1	192.168.1.250	123	64	1	SHA256	*****	*****

1 entry.

Create

Delete

Set Values

Refresh

Requirement

To receive the NTP frames, enable the entry "System Time" under "Security > Firewall > Predefined IPv4 rules".

Description

The page contains the following boxes:

- **NTP client**
When enabled, the device receives the system time from an NTP server.
- **NTP Client only (secure)**
When enabled, the device receives the system time from a secure NTP server. The setting applies to all server entries.
To use the secure NTP client, you configure the parameters for authentication (key ID, hash algorithm, key).
- **Current System Time**
Shows the current date and current normal time received by the device. If you specify a time zone, the time information is adapted accordingly.
- **Last Synchronization Time**
Shows when the last time-of-day synchronization took place.
- **Last Synchronization Mechanism**
Shows how the last time-of-day synchronization was performed. The following methods are possible:
 - Not set
The time was not set.
 - Manual
Manual time setting
 - SNTP
Automatic time-of-day synchronization with SNTP
 - NTP
Automatic time-of-day synchronization with NTP
 - SIMATIC
Automatic time-of-day synchronization using the SIMATIC time frame
 - PTP
Automatic time-of-day synchronization with PTP
- **Time Zone**
Enter the time zone you are using in the format "+/- HH:MM". The time zone relates to UTC coordinated universal time.
The time in the "Current System Time" box is adapted accordingly.

- **Daylight Saving Time**
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.

- **NTP Server Index**
Select the index of the NTP server. The NTP servers are queried in the order of the NTP Server Index. The time of the server that is found first is applied. If time frames of an NTP server with a smaller stratum value are received, this time is applied. The switchover to the time with the smaller stratum takes about 30 minutes.

In the table, configure the NTP server

- **Select**
Select the row you want to delete.
- **NTP Server Index**
Number corresponding to a specific NTP server entry.
- **NTP Server Address**
Enter the IP address, the FQDN (Fully Qualified Domain Name) or the host 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**
Specify the interval between two-time queries. The greater the interval, the less accurate the time of the device.
Possible values are 64 to 2592000 seconds (30 days).

The following columns are only relevant for a secure NTP client. If the check box "Secure NTP Client only" is not selected, these boxes are grayed out:

- **Key ID**
Enter the ID of the authentication key.
- **Hash Algorithm**
Specify the format for the authentication key.

- **Key**
Enter the authentication key. The length depends on the hash algorithm.
 - DES: ASCII 8 characters
 - MD5: ASCII 16 – 128 characters
 - SHA1: ASCII 20 – 128 characters
 - SHA256: ASCII 32 – 128 characters
- **Pass Phrase Confirmation**
Repeat the authentication key.

Procedure

Time-of-day synchronization with NTP server

1. Click in the "NTP Client" check box to enable the automatic time setting using NTP.
2. In "Time Zone", enter the local time difference to world time (UTC).
The input format is "+/-HH:MM" because the NTP server always sends UTC time, for example +02:00 for CEST, the Central European Summer Time. This time is recalculated and displayed as the local time based on the specified time zone.
3. Select the "NTP Server Index".
4. Click the "Create" button.
A new row is inserted in the table for the NTP server.
5. In "NTP Server Address", enter the address of the NTP server whose frames are used to synchronize the time of day.
6. In "NTP Server Port", enter the port via which the NTP server is available. The port can only be modified if the address of the NTP server is entered.
7. In the "Poll Interval" column, enter the interval in seconds after which a new time-of-day query is sent to the time server.
8. Click the "Set Values" button.

Time-of-day synchronization via a secure NTP server

To synchronize the time of day via a secure NTP server, the following additional steps are necessary:

1. Click the "Secure NTP Client only" check box to enable the automatic time setting using Secure NTP.
2. Configure the authentication.
 - In "Key ID" enter the ID of the authentication key.
 - In "Hash Algorithm" select the required format.
 - In "Key" enter the authentication key.

With these entries, the NTP client authenticates itself with the secure NTP server. These entries must be present on the secure NTP server.

3. Click the "Set Values" button.

5.6.8.8 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.

Siemens Automatic (SIMATIC) Time Client

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

☐ SIMATIC Time Client

Current System Time: 08/31/2018 12:27:38

Last Synchronization Time: 08/29/2018 09:25:43

Last Synchronization Mechanism: Manual

Set Values Refresh

Description

The page contains the following boxes:

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

5.6 "System" menu

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

Procedure

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

5.6.8.9 NTP Server

On this WBM page, you configure the device as an NTP server or as an NTP server of the type "NTP (secure)". The other devices can call up the time made available by the device via this NTP server. This means that the supplied devices are not dependent on a connection to an external time server.

Note

Time-of-day synchronization

Also configure the device as NTP client so that it synchronizes the connected devices to a correct time. As NTP client, the device gets the precise time from an external time server and as NTP server distributes it to its NTP clients.

The NTP server does not send cyclic messages with time information on its own, but only responds to corresponding requests. Settings in the function as a client (time zone and daylight saving time) do not influence the time information that the device sends as a server.

Network Time Protocol (NTP) Server

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

☐ NTP Server
Interface: vlan1

Select	Interface	Listen	Server Port	Secure	Key ID	Hash Algorithm	Key	Key Confirmation
☐	vlan1	☒	123	☐	1	DES		

1 entry.

Create
Delete
Set Values
Refresh

Requirement

- To receive the NTP frames, enable the entry "System Time" under "Security > Firewall > Predefined IPv4 rules".

Description

The page contains the following boxes:

- NTP Server**
Enable or disable the service of the NTP server.

Note

SNTP Client in Listen mode and NTP Server cannot be enabled at the same time.

- Interface**
Specify the interface via which the time is transferred using NTP.

The table has the following columns:

- Select**
Select the row you want to delete.
- Interface**
Via this interface the time is transferred using NTP.
- Listen**
When enabled, the other devices can call up the time via this interface.
- Server Port**
Enter the port of the NTP server.
The following ports are possible:
 - 123 (standard port)
 - 1025 to 36564
- Secure**
When this is enabled, the NTP server becomes an NTP server of the type "NTP (secure)".

5.6 "System" menu

The following columns are only relevant for "NTP (secure)". Otherwise, these boxes cannot be edited:

- **Key ID**
Enter the ID of the authentication key.
- **Hash Algorithm**
Specify the format for the authentication key.
- **Key**
Enter the authentication key. The length depends on the hash algorithm.
 - DES: ASCII 8 characters
 - MD5: ASCII 16 – 128 characters
 - SHA1: ASCII 20 – 128 characters
 - SHA256: ASCII 32 – 128 characters
- **Key Confirmation**
Enter the authentication key for confirmation.

5.6.9 Auto Logout

Setting the automatic logout

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

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

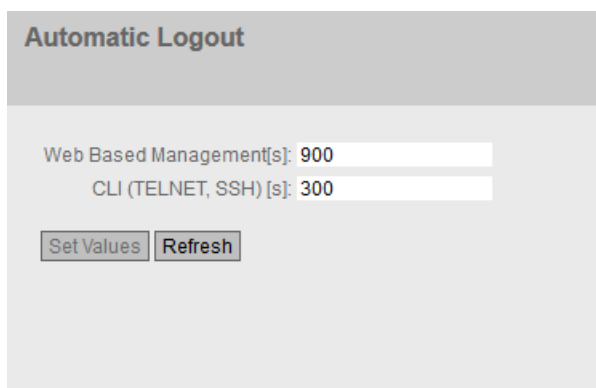
Note

No automatic logout from the CLI

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

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

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



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

Procedure

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

5.6.10 Button

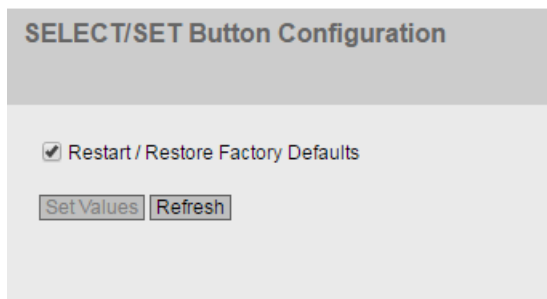
Functionality

The SELECT/SET button is used to:

- Restart
- Load new firmware
- Reset to factory settings.

You will find a detailed description of the functions in the operating instructions for the device.

On this page, the functionality of the button can be restricted.



The screenshot shows a web-based configuration interface titled "SELECT/SET Button Configuration". It contains a checkbox labeled "Restart / Restore Factory Defaults" which is checked. Below this checkbox are two buttons: "Set Values" and "Refresh".

Description

The following functionality is possible:

- **Restart / Restore Factory Defaults**
When disabled, the SELECT/SET button cannot be used for a restart or to restore factory settings.

 **CAUTION**

Button function "Restart / Restore Factory Defaults" active during startup
If you have disabled this function in your configuration, disabling is only valid during operation. When restarting, for example after power off, the function is active until the configuration is loaded and the device can therefore inadvertently be reset to the factory settings. This may cause unwanted disruption in network operation since the device then needs to be reconfigured. An inserted PLUG is also deleted and returned to the status as shipped.

You will find more information on how to restore the device to the factory defaults despite disabled functions in the section "Upkeep and maintenance (Page 488)".

5.6.11 Syslog Client

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

Requirements for sending Syslog messages

- The Syslog client is enabled.
- In "System > Events > Configuration", "Syslog" is activated for the relevant event.
- There is a Syslog server in your network that receives the Syslog messages.
- The IP address or the FQDN (Fully Qualified Domain Name) of the Syslog server is entered in the device.

System Logging (Syslog) Client

☐ Syslog Client

Syslog Server Address:

Select	Syslog Server Address	Server Port	TLS
☐	192.168.16.100	514	☐

1 entry.

Create

Delete

Set Values

Refresh

Description

The page contains the following boxes:

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

This table contains the following columns

- **Select**
Select the row you want to delete.
- **Syslog Server Address**
Shows the IP address, the FQDN (Fully Qualified Domain Name) or the host name of the Syslog server.
- **Server Port**
Enter the port of the Syslog server being used.
- **TLS**
 - Enabled
The syslog messages are sent using TLS encryption over TCP.
 - Disabled
Syslog messages are sent unencrypted over UDP.

Procedure

Enabling function

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

Creating a new entry

1. In the "Syslog Server Address" input box, enter the address of the Syslog server to which the Syslog messages are sent.
2. Click the "Create" button. A new row is inserted in the table.
3. In the "Server Port" input box, enter the number of the server port.
4. Click the "Set Values" button.

Note

The default setting of the server port is 514.

Changing the entry

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

Deleting an entry

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

5.6.12 Fault Monitoring

5.6.12.1 Power Supply

MUx85x

Settings for monitoring the power supply

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

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

Note

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

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

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

Fault Monitoring Power Supply

Power Supply

Link Change

Mobile

☐ Line 1

☐ Line 2

☐ PoE

Set Values

Refresh

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.

5.6.12.2 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, an SMS or an entry in the event log table.

Fault Monitoring Link Change

Link Change

	Setting	Copy to Table
All ports	No Change ▼	Copy to Table

Port	Setting
P1	- ▼
P2	- ▼
P3	- ▼
P4	- ▼

Set Values Refresh

Description

Table 1 has the following columns:

- **1st column**
Shows that the settings are valid for all ports.
- **Setting**
Select the setting from the drop-down list. You have the following setting options:
 - "-" (disabled)
 - Up
 - Down
 - No Change: The setting in table 2 remains unchanged.
- **Copy to Table**
If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
Shows the available ports and link aggregations. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.
- **Setting**
Select the setting from the drop-down list. You have the following options:
 - Up
Error handling is triggered when the port changes to the active status.
(From "Link down" to "Link up")
 - Down
Error handling is triggered when the port changes to the inactive status.
(From "Link up" to "Link down")
 - "-" (disabled)
The error handling is not triggered.

Procedure

Configure error monitoring for a port

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

Configure error monitoring for all ports

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

5.6.12.3 Mobile wireless

M87x

RM1224

MUx85x

On this page, you configure whether or not an error message is triggered if there is a status change of the SIM card.

SIM-Karte	Einstellung
1	-
2	SIM-Karte fehlt

Description

The table has the following columns:

- SIM card**
 Shows the available SIM cards:
 - 1: Physical, exchangeable SIM card
 - 2: eSIM, only for MUM85x with built-in eSIM
- Setting**
 Select the setting from the drop-down list. You have the following options:
 - "-" (disabled)
The error handling is not triggered.
 - SIM missing
Troubleshooting is triggered if no SIM card is activated. An error causes the fault LED to light up on the device.

5.6.13 PLUG

5.6.13.1 Configuration



NOTICE

Do not remove or insert a 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 PLUG with license was inserted in the device, the device changes to a defined error state following the restart. With SCALANCE M, 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

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

Note

Incompatibility with older firmware versions with PLUG inserted

During the installation of an older firmware version, the configuration data can be lost. In this case, reset the device to the factory settings after the firmware has been installed.

In this situation, when a PLUG is inserted in the device, this has the status "NOT ACCEPTED" following the restart because 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 via "System > PLUG".

Note

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

The action cannot be undone.

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

PLUG Configuration (KEY-PLUG)

Configuration

License

State: ACCEPTED

Device Group: SCALANCE M800

Device Type: SCALANCE M874-3

Configuration Revision: 1

File System: UBIFS

File System Size: 29933568

File System Usage: 11164

Info String: 6GK5 874-3AA00-2AA2
SCALANCE M874-3
HW: 3
SW: T04.03.00.00_09.01.01
Firmware on PLUG not present

☐ Firmware on PLUG

Modify PLUG:

Select action

Set Values

Refresh

Description

The table has the following rows:

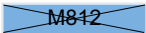
- Status**
 Shows the status of the PLUG. The following are possible:
 - ACCEPTED
There is a PLUG with a valid and suitable configuration in the device.
 - NOT ACCEPTED
Invalid or incompatible configuration on the inserted PLUG.
 - NOT PRESENT
No PLUG is inserted in the device.
 - FACTORY
PLUG is inserted and does not contain a configuration. This status is also displayed when the PLUG was formatted during operation.
 - 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 PLUG previously.

- **Device Type**
Shows the device type within the product line that used the PLUG previously.
- **Configuration Revision**
The version of the configuration structure. This information relates to the configuration options supported by the device and has nothing to do with the concrete hardware configuration. This revision information does not therefore change if you add or remove additional components (modules or extenders), it can, however, change if you update the firmware.
- **File System**
Displays the type of file system on the PLUG.
- **File System Size**
Displays the maximum storage capacity of the file system on the PLUG.
- **File System Usage**
Displays the memory utilization of the file system of the PLUG.
- **Firmware on PLUG**
When the function is enabled (default), the firmware will be stored on the PLUG. This means that automatic firmware updates/downgrades can be made with the PLUG. The "Info" box shows whether or not the firmware is stored on the PLUG.
- **Info String**
Shows additional information about the device that used the PLUG previously, for example, article number, type designation, and the versions of the hardware and software. The displayed software version corresponds to the version in which the configuration was last changed. With the "NOT ACCEPTED" status, further information on the cause of the problem is displayed.
If a PLUG was configured as a PRESET PLUG this is shown here as additional information in the first row. For more detailed information on creating and using a PRESET PLUG refer to the section "Maintenance (Page 483)".
- **Modify PLUG**
Select the setting from the drop-down list. You have the following options for changing the configuration on the PLUG:
 - Write Current Configuration to the PLUG
This option is available only if the status of the PLUG is "NOT ACCEPTED" or "FACTORY". The configuration in the internal flash memory of the device is copied to the PLUG.
 - Erase PLUG to factory default
Deletes all data from the PLUG and 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.

5.6.13.2 License



NOTICE
Do not remove or insert the PLUG during operation. A PLUG may only be removed or inserted when the device is turned off. The device checks whether 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 PLUG with license was inserted in the device, the device changes to a defined error state following the restart. With SCALANCE M, 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 older firmware versions with PLUG inserted During the installation of an older firmware version, the configuration data can be lost. In this case, reset the device to the factory settings after the firmware has been installed. In this situation, when a PLUG is inserted in the device, this has the status "NOT ACCEPTED" following the restart because 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 via "System > PLUG".

Information about the license on the PLUG

In addition to the configuration, a PLUG with license also contains a license that enables certain functions of your SIMATIC NET device.

This page provides detailed information about the license on the PLUG.

PLUG License (KEY-PLUG)

Configuration	License
State: ACCEPTED	
Order ID: 6GK5 908-0PB00	
Serial Number: VPF5135184	
Info String: KEY-PLUG M800: Sinema RC Features	

Refresh

Description

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

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

Note

When you save the configuration, the information about whether or not a PLUG was inserted in the device at the time is also saved. This configuration can then only work if a PLUG with the same order number / license is inserted.

5.6.14 Ping

Reachability of an address in an IP network

With the Ping function, you can check whether a certain IP address is reachable in the network.

The screenshot shows a web interface titled "Ping". It contains the following elements:

- Destination Address:** A text input field.
- Repeat:** A text input field with the value "3".
- Ping:** A button to execute the ping command.
- DNS Resolution:** A dropdown menu set to "Auto".
- Out Interface for IPv6:** A dropdown menu set to "-".
- Out Interface is required only when pinging IPv6 multicast and link-local addresses:** A note below the IPv6 interface dropdown.
- Ping Output:** A large text area for displaying the results of the ping command.
- Clear:** A button at the bottom left to clear the output area.

Description

The page contains the following boxes:

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

5.6.15 DCP Discovery

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

Note

DCP Discovery

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

Discovery and Set via PROFINET Discovery and Configuration Protocol (DCP)

Timeout[s]: [Blinken der eigenen LEDs aktivieren](#)

Schnittstelle: [Durchsuchen](#)

Port	MAC-Adresse	Gerätetyp	Gerätename	IP-Adresse	Subnetzmaske	Gateway-Adresse	Status	Gerätename	Status IP-Adresse	Timeout[s]	Blinken
P0.8	00-1b-1b-38-5c-90	SCALANCE W-700		192.168.16.177	255.255.255.0	0.0.0.0	None		Discovered/IP	5	Blinken
P0.8	00-1b-1b-40-91-23	SCALANCE X-500		192.168.16.150	255.255.255.0	0.0.0.0	None		Discovered/IP	5	Blinken
P0.8	00-1b-1b-9a-31-94	SCALANCE M-800		192.168.16.48	255.255.255.0	0.0.0.0	None		Discovered/IP	5	Blinken
P0.8	00-1b-1b-9a-32-2e	SCALANCE M-800		192.168.16.50	255.255.255.0	0.0.0.0	None		Discovered/IP	5	Blinken
P0.8	00-1b-1b-9a-3c-b2	SCALANCE M-800		192.168.16.46	255.255.255.0	0.0.0.0	None		Discovered/IP	5	Blinken
P0.8	00-1b-1b-a5-5d-98	SCALANCE W-700		192.168.16.107	255.255.255.0	0.0.0.0	None		Discovered/IP	5	Blinken
P0.8	00-1b-1b-af-a2-00	SCALANCE X-400		192.168.16.26	255.255.255.0	0.0.0.0	None		Discovered/IP	5	Blinken
P0.8	00-1b-1b-b6-32-79	SCALANCE S-600		192.168.16.42	255.255.255.0	0.0.0.0	None		Discovered/IP	5	Blinken
P0.8	00-1b-1b-c7-f5-a2	SCALANCE W-700		192.168.16.7	255.255.255.0	0.0.0.0	None		Discovered/IP	5	Blinken
P0.8	00-1b-1b-c8-70-3a	SCALANCE X-300		192.168.16.33	255.255.255.0	192.168.16.33	None		Discovered/IP	5	Blinken

1 - 10 of 33 Einträge [Alle anzeigen](#) [Weiter](#)

[Einstellungen übernehmen](#) [Aktualisieren](#)

Requirement:

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

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

Description

The page contains the following boxes:

- **Timeout[s]**
Specify the time for flashing. When the time elapses, flashing stops.
- **Blink Own LEDs**
Makes the LEDs of your own device flash.
You will find which LEDs flash in the operating instructions of the device, section "Device description > LED display", explanation on localization of the device.
- **Interface**
Select the required interface.
- **Discover**
Starts the search for devices reachable via the selected interface.
On completion of the search the reachable devices are listed in the table. The table is limited to 100 entries.

The table has the following columns:

- **Port**
Shows the port via which the device can be reached.
- **MAC Address**
Shows the MAC address of the device.
- **Device Type**
Shows the product line or product group to which the device belongs.

5.6 "System" menu

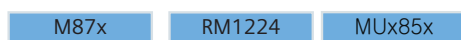
- **Device Name**
Adapt the PROFINET device name if necessary.
The device name must be DNS-compliant. If the device name is not used, the box is empty.
- **IP Address**
If necessary, adapt the IPv4 address of the device.
The IPv4 address should be unique within your network and should match the network.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

Procedure

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

5.6.16 SMS

5.6.16.1 General



For the device to be able to send an SMS message, you need to enter a specific SMS center (Short Message Server Center, SMS-C) of your mobile wireless provider or your service provider.

- If you use the standard SMS center, you do not need to configure anything on this WBM page. The SIM card already contains the correct information.
- If you do not use the standard SMS center, you can replace the stored call number of the standard SMS center with another number on this WBM page. This depends on your contract.

SMS General Settings

General

Event SMS

SMS Command

SMS Relay (Outgoing)

SMS Relay (Incoming)

Current SMS service center call number: +491710760000

Override SMS service center call number:

Set Values

Refresh

Description

The page contains the following boxes:

- **Current SMS service center call number**
Shows the stored call number of the SMS center.
- **Override SMS service center call number**
Enter the call number of the SMS center including the country dialing code. Confirm the entry with "Set Values" to store the phone number on the SIM card. If the call number is displayed in "Current SMS service center call number", the stored call number of the SMS center has been overwritten and the input box emptied.

Note

When the change takes effect, the mobile wireless connection will be interrupted for a short time. The change can take up to a minute.

5.6.16.2 Event SMS

M87x

RM1224

MUx85x

If events occur, the device can automatically send an SMS message.

Requirement:

- "SMS" is activated for the relevant event in "System > Events > Configuration".

Event SMS Settings

General

Event SMS

SMS Command

SMS Relay (Outgoing)

SMS Relay (Incoming)

☒ Enable Event SMS

Customize SMS messages for Digital Input

Digital Input	Rising edge	Falling edge	Sending Option
1			Both

Phone Number:

Select	No.	Send	Phone Number
☐	1	☒	+49176

Create

Delete

Set Values

Refresh

Description

The page contains the following:

- **Enable Event SMS**
When enabled, the device sends an SMS.

In the area "Customize SMS messages for Digital Input" you specify the SMS text for the digital input.

- **Digital Input**
Shows the available digital inputs.
- **Rising edge**
Enter the SMS text that is sent when the signal at the digital input changes from 0 (LOW) to 1 (HIGH).
- **Falling edge**
Enter the SMS text that is sent when the signal at the digital input changes from 1 (HIGH) to 0 (LOW).

Note

Permitted characters for user name and password

The following characters are permitted:

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

Additionally allowed in the password:

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

- **Sending Option**
Specify when the SMS text is sent.
 - None
The function is disabled.
 - Both
In both cases, an SMS text is sent.
 - Rising only
Only the SMS text is sent when the signal at the digital input changes from 0 (LOW) to 1 (HIGH).
 - Falling only
Only the SMS text is sent when the signal at the digital input changes from 1 (HIGH) to 0 (LOW).
- **Phone Number**
Enter the full telephone number of the recipient including the country dialing code. If you click the "Create" button, a new row with a unique number is created.
- The table contains the following columns:
 - **Select**
Activate the check box in the row to be deleted.
 - **No.**
Unique number that is assigned when the sender is created.
 - **Send**
Specify whether the device sends an SMS message to this recipient.
 - **Phone Number**
Shows the phone number of the recipient.

Procedure

Configuring an event SMS

To obtain an SMS message when the signal changes from 0 (LOW) to 1 (HIGH), follow the steps below:

1. Specify the SMS text at "Rising Edge".
2. For "Sending Option", select "Rising only".
3. Click the "Set Values" button.
4. Enter the phone number of the recipient in the "Phone Number" input box.
5. Click the "Create" button. A new row with a unique number is created in the table.
6. Specify whether the device sends an SMS message to this recipient if a fault occurs.
7. Select "Enable Event SMS".
8. Click the "Set Values" button.
9. In "System > Events > Configuration" activate the type of notification "SMS" for the "Digital In" event.

Change phone number

- 1. Select the required phone number in the "Phone Number" column.
- 2. Click the "Set Values" button.

5.6.16.3 SMS Command

M87x RM1224 MUx85x

Commands can also be sent with SMS messages. On this page, you specify who can control the device. As identification either the phone number or the sender ID is specified. The sender ID can, for example, be an IP address or a DNS name.

With an SMS command, you can, for example, establish a VPN connection to an application such as the SINEMA RC Server. To do this, the SINEMA RC Server sends a wake-up SMS message containing the required commands. Additional information can be found in the section "Command SMS (Page 489)".

To obtain a reply SMS with the status, you must also configure the phone number of the recipient on the page.

SMS Command

GeneralEvent SMS**SMS Command**SMS Relay (Outgoing)SMS Relay (Incoming)Send SMS

☐ Enable Command SMS

Phone Number / Sender Identifier:

Select	No.	Phone Number / Sender Identifier	System	Relay	Identifier
☐	2	+49177545	☒	☒	ID:SchmidtGmbH

1 entry.

CreateDeleteSet ValuesRefresh

Description

The page contains the following:

- **Enable Command SMS**
Enable or disable receipt of command SMS messages.
- **Phone Number / Sender Identifier**
Specify the sender ID or the phone number including the country code. If you click the "Create" button, a new row with a unique number is created.
In phone numbers, you can replace as numbers as required to the right with the asterisk (*) placeholder. The placeholder can only be positioned at the end of a number sequence.
Example:
+49177545* stands for all phone numbers that start with 0177545.

Note

Please note that when you use the placeholder "*", command text messages (SMS) from a wide range of phone numbers will be accepted. We therefore recommend that you use a more restrictive input, if possible.

The table contains the following columns:

- **Select**
Activate the check box in the row to be deleted.
- **No.**
Shows the unique number of the entry.
- **Phone Number / Sender Identifier**
Shows the sender ID or the phone number.
- **System / Relay**
Specify which class (System / Relay) of commands is accepted from this sender. Additional information can be found in the section "Command SMS (Page 489)".
- **Identifier**
Enter a plain text value, which must match the received identifier of the SMS. Use the identifier to secure SMS messages in addition to the phone number.
Start with "ID:" and then enter the identifier without spaces: ID:<identifier>.
Example:
ID:SchmidtGmbH

5.6.16.4 SMS Relay (Outgoing)

M87x RM1224 MUx85x

With the SMS messaging function, applications connected to the Ethernet interface of the device can send SMS messages. To send an SMS message, the application must establish a TCP/IP connection to the device via the Ethernet interface. Via this TCP/IP connection, the

application transfers the text of the SMS to the device that packs the text in an SMS message and sends it.

Note

A large number of sent SMS can overload the device. Restrict the number of SMS to 20 messages per minute.

The device cannot be the receiver of its own SMS; this would result in an event loop.

Format of the SMS text

The text is transferred in a frame via the TCP/IP connection to the device. The frame must have the following format:

`<User name>#<Password>#CommandCode#Seq-Num;<Phone number>;<Message>:`

Example:

`<User name>#<Password>#105#01;<phone (phone number)>;<my-SMS-text (sleep)>:`

Note

Permitted characters for user name and password

The following characters are permitted:

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

Additionally allowed in the password:

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

- **User name**
Enter a user name to check the permission for sending an SMS message. Maximum of 10 characters.
- **Password**
Enter the password belonging to the user name. Maximum of 10 characters.
- **CommandCode**
Command to send an SMS message from the local network. This value of 105 is fixed and must not be modified.
- **Seq-Num**
The sequence number is used to assign several requests at the same time. The function is not currently supported.
The sequence number consists of 2 numeric characters from 01 to 99.
- **Phone number**
Call number of the SMS recipient with a maximum of 40 characters. International numbers (+49) are permitted.
- **Message**
SMS text with a maximum of 160 characters

Description

The page contains the following:

- **Enable SMS Relay (Outgoing)**
Enable or disable the sending of SMS messages from the local network.
- **User**
Enter the user name that must be included before the text is sent as an SMS message.
- **Password**
Enter the password that must be included before the text is sent as an SMS message.
- **Password (Confirmation)**
Repeat the password to confirm it.
- **Server Port Number**
Enter the port at which the server receives the SMS.

5.6.16.5 SMS Relay (Incoming)

M87x

RM1224

MUx85x

Applications connected to the Ethernet interface of the device can receive SMS messages. To receive an SMS message, the application must establish a TCP/IP connection to the device via the Ethernet interface. The device receives a command SMS message and forwards the text it contains to the application.

Note

A large number of received SMS can overload the device. Restrict the number of SMS to 20 messages per minute.

SMS Relay (Incoming)

General

Event SMS

SMS Command

SMS Relay (Outgoing)

SMS Relay (Incoming)

Connection Name:

IP Address:

Port Number: 26864

Username:

Password:

Password (Confirmation):

Select	Connection Name	IP Address	Port Number	Username
☐	Service	192.168.1.20	26864	user

1 entry.

Create

Delete

Refresh

Format of the SMS text

The text is sent in a frame via the TCP/IP connection to the application. The frame must have the following format:

<User name>#<Password>#CommandCode#Seq-Num;<Phone number>;<Message>:

Username#Password#CommandCode#Seq-Num;Callnumber;Message:

Example:

<User name>#<Password>#105#01;<phone (phone number)>;<my-SMS-text (sleep)>:

Note

Permitted characters for user name and password

The following characters are permitted:

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

Additionally allowed in the password:

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

- **User name**
Enter a user name to check the receipt of the SMS message. Maximum of 10 characters.
- **Password**
Enter the password belonging to the user name. Maximum of 10 characters.
- **CommandCode**
Command to send an SMS message to the local network. This value of 105 is fixed.

- **Seq-Num**
The sequence number is used to assign several requests at the same time. The function is not currently supported.
The sequence number consists of 2 numeric characters from 01 to 99.
- **Phone number**
Phone number of the sender of the command SMS message with a maximum of 40 characters. International numbers (+49) are permitted.
- **Message**
SMS text with a maximum of 160 characters

Description

The page contains the following:

- **Connection Name**
Enter a unique name for the relay connection.
- **IP Address**
Enter the IP address of the recipient. The frame is sent to this IP address.
- **Port number**
Enter the port to which the frame will be sent.
- **Username**
Enter the user name to check receipt of the message. Enter the user name in the frame.
- **Password**
Enter the password belonging to the user name.
- **Password (Confirmation)**
Repeat the password to confirm it.

The table contains the following columns:

- **Select**
Activate the check box in the row to be deleted.
- **Connection Name**
Shows the name of the relay connection.
- **IP Address**
Shows the IP address of the recipient.
- **Port Number**
Shows the port.
- **Username**
Shows the user name contained in the frame.

5.6.16.6 Send SMS messages



5.6 "System" menu

This function sends an SMS directly via the device. This allows you to test SMS-based services such as Email2SMS.

Note

A large number of sent SMS can overload the device. Restrict the number of SMS to 20 messages per minute.

The device cannot be the receiver of its own SMS; this would result in an event loop.

Send SMS

General

Event SMS

SMS Command

SMS Relay (Outgoing)

SMS Relay (Incoming)

Send SMS

Receiver Phone Number:

Text:

Send SMS

Refresh

Description

The page contains the following:

- **Call number of the receiver**
Enter the full telephone number of the receiver including the country dialing code
- **Text**
Enter SMS text.

Note

Characters permitted for sending SMS messages

The following characters are permitted in the text:

- 0123456789
 - A...Z a...z
 - Space
 - ! " % & / () = ? * + < > ' , . -
- **Send SMS messages**
The device sends the SMS to the recipient.

5.6.17 DNS

5.6.17.1 DNS client

On the WBM page you specify whether or not the device uses the DNS server of the network provider or another DNS server.

Domain Name System (DNS) Client

DNS Client | DNS Proxy | DDNS Client | DNS Records

☒ DNS Client
☐ DNSSec

Used DNS Servers: all

DNS Server Address:

Select	DNS Server Address	Origin
☐	192.168.10.1	manual

1 entry.

[Create](#) [Delete](#) [Set Values](#) [Refresh](#)

Description

The page contains the following boxes:

- DNS client**
 Enable or disable depending on whether the device should operate as a DNS client.
- DNSSec**
 Can only be enabled if the "DNS Client" option is enabled.
 Enables or disables DNSSec on the DNS client. If enabled, only IP addresses from signed domains are accepted.
- Used DNS Servers**
 Specify which DNS server the device uses:
 - learned only
The device uses only the DNS servers assigned by DHCP.
 - manual only
The device uses only the manually configured DNS servers. The DNS servers must be connected to the Internet. A maximum of two DNS servers can be configured.
 - all
The device uses all available DNS servers.
- DNS Server Address**
 Enter the IP address of the DNS server.

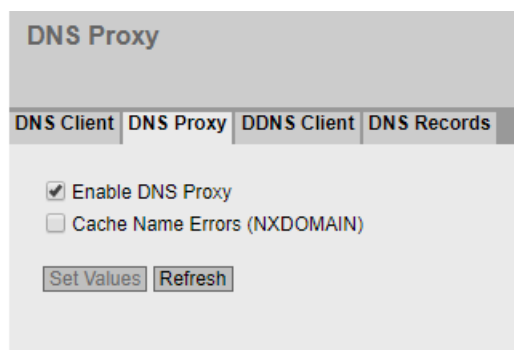
The table has the following columns:

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

5.6.17.2 DNS Proxy

The device provides a DNS server for the local network. If you enter the IP address of the device in the local application as a DNS server, the device answers the DNS requests from its cache.

If the device does not know the IP address for a domain address, it forwards the query to an external DNS server. How long the device keeps a domain address in the cache depends on the host being addressed. In addition to the IP address, a DNS request to an external DNS server also supplies the life span of this information.



Description

The page contains the following boxes:

- **Enable DNS Proxy**
Enable or disable the proxy of the DNS server.
- **Cache Name Errors (NXDOMAIN)**
Enable or disable the caching of NXDOMAIN replies. If you enable the option, the domain names that were unknown to the DNS server remain in the cache.

5.6.17.3 DDNS client

The DDNS (Dynamic Domain Name System) is an Internet service that allows a fixed hostname to be set up as a pseudonym for a dynamically changing IP address.

The DDNS client synchronizes the assigned IP address with the hostname registered at the DDNS provider. This means that the device can always be reached using the same hostname.

DDNS-Client

DNS-Client

DNS-Proxy

DDNS-Client

DNS Records

Dienst	Aktiviert	Host	Benutzername	Passwort	Passwort bestätigen
No-IP	☐				
DynDNS	☐				

Einstellungen übernehmen

Aktualisieren

Description

The table has the following columns:

- **Service**
Shows which providers are supported.
- **Enabled**
When enabled, the device logs on to the DDNS server.
- **Host**
Enter the host name that you have agreed with your DDNS provider for the device, e.g. example.no-ip-com.
- **User Name**
Enter the user name with which the device logs on to the DDNS server.
- **Password**
Enter the password assigned to the user.
- **Password Confirmation**
Confirm the password.

Procedure

Requirement:

- User name and password that gives you the right to use the DDNS service.
 - Registered hostname, e.g. example.no-ip.com
 - UDP port 53 for DNS is enabled and is not used for NAT.
1. In "Host", enter the hostname that you have agreed with your DDNS provider for the device, e.g. example.no-ip-com.
 2. Enter the login data (user name, password) for the DDNS server.
 3. Select "Enabled". This hostname is used for the device.
 4. Click on "Set Values".

5.6.17.4 DNS record

You configure a DNS address directory on this WBM page. To do this, enter the IPv4 address associated with an FQDN.

The device checks if there is an entry for DNS requests and converts the URL into the corresponding IPv4 address.

DNS Records

DNS Client **DNS Proxy** **DDNS Client** **DNS Records**

☒ Enable DNS Records

Select	Domain	IP Address	Comment
☐	example.de	192.168.1.1	

1 entry.

Create Delete Set Values Refresh

Description

The page contains the following boxes:

- **Enable DNS Records**
When this is enabled, the address directory is used.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Domain**
Enter the FQDN (Fully Qualified Domain Name).
- **IP Address**
Enter the corresponding IPv4 address.
- **Comment**
If needed, enter a comment.

5.6.18 DHCPv4

5.6.18.1 DHCP Client

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

Dynamic Host Configuration Protocol (DHCP) Client

DHCP Client | DHCP Server | DHCP Options | Static Leases

☒ Keep Alive

DHCP Client Configuration Request (Opt 66, 67):

setup

DHCP Mode:

via MAC Address

Interface	DHCP	IAID Value
vlan1	☐	00-00-01-C2
usb0	☒	00-00-01-D3

Set Values

Refresh

Description

The page contains the following boxes:

- **Keep Alive**
When this is enabled, the IP address is retained in the event of a connection breakdown and is not reset to 0.0.0.0. Keep Alive is enabled by default. When Keep Alive is disabled, the IP address is reset to 0.0.0.0 in the event of a communication breakdown.
- **DHCP Client Configuration Request (Opt. 66, 67)**
When enabled, the DHCP client uses the options to download the configuration file (option 67) from the TFTP server (option 66). After the restart, the device uses the data from the configuration file.

NOTICE
Security hazard - risk of unauthorized access and/or misuse
The function can potentially be used to change the functionality of the device and thus cause the failure of data traffic. Users with malicious intent could cause the device to load a manipulated configuration file in order to change the configuration to their benefit. To prevent unauthorized access and/or misuse, disable the function if you are not using it (Off). In a device with default setting (Setup), no configuration file is loaded from the DHCP server even if the options 66 and 67 are still contained in the DHCP queries of the DHCP client after the first login with the default user profile admin and the assignment of a new password.

Note
Configuration file and firmware version

The configuration file is used to store and read in configuration data within a firmware version, e.g. 4.3. Configuration files created with a firmware version <4.2 cannot be read in to a device with a firmware version 4.3.

- **Setup**
Default setting. The function depends on the status of the device.
In the delivery state and after reset to default settings, the function behaves as with the setting On and the function is enabled for all DHCP client interfaces.
The following events trigger a status change of the device: The first login with the default user profile admin and the associated assignment of a new password or the loading of a configuration file. Afterwards, the device is in the secure operating state and the function behaves as with the Off option: The option is disabled for all DHCP client interfaces.
The status changes automatically.
- **On**
The function is enabled. The DHCP client requests a configuration file with the next DHCP query.
- **Off**
The function is disabled. The DHCP client does not request a configuration file.
- **DHCP Mode**
Specify the type of identifier with which the DHCP client logs on with its DHCP server.
 - **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 laid and Duid
With this the DHCP client can log on with DHCP servers that support parallel operation of IPv4 and IPv6.
The identification is via the IAID and the DUID and identifies precisely one IP interface of the device.
IAID (Interface Association Identifier): At least one IAID is generated for each IP interface
The IAID remains unchanged when the DHCP client restarts
DUID (DHCP Unique Identifier): Uniquely identifies server and clients and applies to all IP interfaces of the device. The DUID remains unchanged when there is a restart.

Note

DHCP mode "via PROFINET device name"

With firmware version 5.0, the setting "via PROFINET device name" was removed.

The table has the following columns:

- **Interface**
Interface to which the setting relates.
- **DHCP**
Enable or disable the DHCP client for the relevant interface.
- **IAID Value**
Value with which the interface (DHCP client) identifies itself with the DHCP server.

Procedure

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

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

Note

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

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

5.6.18.2 DHCP Server

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

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

Dynamic Host Configuration Protocol (DHCP) Server

DHCP Client

DHCP Server

DHCP Options

Static Leases

☒ DHCP Server

☒ Probe address with ICMP Echo before offer

Select	Pool ID	Interface	Enable	Subnet	Lower IP Address	Upper IP Address	Lease Time [sec]
☐	1	vlan1 (INT)	☒	192.168.16.0/24	192.168.16.50	192.168.16.50	3600

1 entry.

Create

Delete

Set Values

Refresh

Requirement

- The connected devices are configured so that they obtain the IP address from a DHCP server.

Description

The page contains the following boxes:

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

Note

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

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

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).
- **Interface**
Select a VLAN IP interface. The IPv4 addresses are assigned dynamically via this interface. The requirement for the assignment is that the IPv4 address of the interface is located in the subnet of 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, its 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 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.

5.6.18.3 DHCP options

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

Dynamic Host Configuration Protocol (DHCP) Options

DHCP Server

DHCP Options

Static Leases

Pool ID: 1

Option Code:

Select	Pool ID	Option Code	Use Interface IP	Value
	1	1		255.255.255.255
☐	1	3	☐	0.0.0.0
☐	1	6	☐	0.0.0.0
☐	1	66		
☐	1	67		Bootfile name not set

5 entries.

Create

Delete

Set Values

Refresh

Description

The page contains the following boxes:

- Pool ID**
Select the required address band.
- Option Code**
Enter the number of the required DHCP option.

Note

DHCP options supported

The DHCP options 1, 2, 3, 4, 5, 6, 42, 66, 67 are supported.

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.

The table has the following columns:

- Select**
Select the check box in the row to be deleted
- Pool ID**
Shows the number of the address band.
- Option Code**
Shows the number of the DHCP option.

- **Use Interface IP**
Specify whether or not the internal IP 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.

Value	Option name		
1	Subnet Mask	The subnet mask is entered automatically.	Option cannot be deleted.
2	Offset time	Offset time to the coordinated universal time UTC.	Enter the offset time in seconds in hexadecimal format.
3	Router	The IPv4 address for router in the subnet of the DHCP client. If the device itself is the router, the IPv4 address of the interface is used.	Enter the address of the router.
4	Time server	The IPv4 address of the time server available to the DHCP client.	You can specify several IPv4 addresses separated by commas.
5	Name server	The IPv4 address of the name server available to the DHCP client.	
6	DNS Server	The IPv4 address of the DNS server available to the DHCP client. If the device itself is the DNS server, the IPv4 address of the interface is used.	
42	NTP Server	The IPv4 address of the NTP server available to the DHCP client.	
66	TFTP server	The IPv4 address or the hostname of the TFTP server available to the DHCP client.	Enter the address of the TFTP server.
67	Name of the boot file	The name of the boot file that the client downloads from the TFTP server.	Enter the name of the boot file in the string format.

5.6.18.4 Static Leases

On this page you specify that certain devices will be assigned a certain IP address. The address assignment is made based on the MAC address, the client ID or the DUID.

Static Leases

DHCP Client

DHCP Server

DHCP Options

Static Leases

Pool ID:

1

Client Identification Method:

DUID

Value:

Select	Pool ID	Identification Method	Value	IP Address	Comment
☐	1	MAC	00-1b-1b-b6-32-79	192.168.16.48	Router

1 entry.

Create

Delete

Set Values

Refresh

Description

The page contains the following boxes:

- **Pool ID**
Select the required address band.
- **Client Identification Method**
Select the method according to which a client is identified.
 - Ethernet MAC
Identification is based on the MAC address. Enter the MAC address in "Value". A MAC address consists of six bytes separated by hyphens in hexadecimal notation, e.g. 00-ab-1d-df-b4-1d.
 - Client ID
Identification is based on a freely defined DHCP client ID. Enter the required designation in "Value".
 - DUID
Identification is based on the DUID and IAID. Enter the required designation in "Value" e.g. 00-00-01-C2-00-01-00-01-00-00-00-72-00-1B-1B-B6-32-9D.
- **Value**
Enter the required value. The entry depends on the selected identification method of the client.

Note

The maximum is 128 entries.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Pool ID**
Shows the number of the address band.
- **Identification Method**
Shows the method with which the client identifies itself with the DHCP server.
- **Value**
Shows the MAC address or client ID or DUID of the client.
- **IP Address**
Specify the IPv4 address that will be assigned to the client. The IPv4 address must be within the address band.
- **Comment**
Enter a description for the address assignment.
The maximum is 32 characters.

5.6.19 cRSP / SRS

Note

Common Remote Service Platform (cRSP) / Siemens Remote Service (SRS) is a remote maintenance platform via which remote maintenance access is possible.

To use the platform, additional service contracts are necessary and certain constraints must be kept to. If you are interested in cRSP / SRS, call your local Siemens contact or visit Web page (<https://support.industry.siemens.com/cs/gb/en/sc/2281>).

On this page, you configure the access data for the SRS / cRSP acc. to URI syntax. The Uniform Resource Identifier (URI) is defined in RFC 3986.

DDNS for cRSP / SRS

☐ Enable DDNS for cRSP / SRS

Update Interval [s]:

☒ Validate Server Certificate

Index	Select	Scheme	Authority	Path	Query	Frag.	Status	Enabled	
1	☐	https	://		?		#	-	☐

1 entry.

Description

The page contains the following boxes:

- **Enable DDNS for cRSP / SRS**
Enable or disable the use of cRSP / SRS.
- **Update Interval**
Enter the time interval.
- **Validate Server Certificate**
When enabled, the device checks the validity of the received server certificate.

The table has the following columns:

- **Index**
The number of the entry.
- **Select**
Select the check box in the row to be deleted.

- **Scheme**
Identifies the access method and the resource type.
https: Secure access to a Web page.
- **Authority**
Contains the address of the destination server
- **Path**
Contains the target path to the resource. The target path can correspond to a directory name or file name.
- **Query**
A query can contain parameter values for an application.
 - WAN_IP (keyword): Replaces WAN_IP with current external IP address of the device to the destination server.
- **Frag.**
Addresses local parts of the resource, e.g. the anchor attribute of a Web page.
- **Status**
Shows the status of the last cRSP / SRS access of the entry.
- **Enabled**
When enabled, this entry is used.

5.6.20 Proxy Server

On this WBM page, you configure the proxy server that is used by various components, for example SINEMA RC.

Proxy Server

Proxy Name:

Select	Name	Address	Type	Port	Auth. Method	Username	Password	Password Conf.
☐	company	192.168.16.1	HTTP	0	Basic			

1 entry.

Create

Delete

Set Values

Refresh

Description

- **Proxy Name**
Enter a name for the proxy server.
- The table has the following columns:
- **Select**
Select the check box in the row to be deleted.
 - **Name**
Shows the name of the proxy server.

5.6 "System" menu

- **Address**
Enter the IPv4 address of the proxy server.
- **Type**
Specify the type of the proxy server.
 - HTTP: Proxy server only for access using HTTP.
 - SOCKS: Universal proxy server
- **Port**
Enter the port on which the proxy service runs.
- **Auth. Method**
Specify the authentication method.
 - None
Without authentication
 - Basic
Standard authentication. User name and password are sent unencrypted.
 - NTLM (NT LAN Manager)
Authentication according to the NTLM standard (Windows user login)
- **User Name**
Enter the user name for access to the proxy server.
- **Password**
Enter the password for access to the proxy server.
- **Password Confirmation**
Enter the password again to confirm it.

5.6.21 SINEMA RC

On the WBM page, you configure the access to the SINEMA RC server.

Note

This function can be used with the KEY PLUG (Page 60), CLP or via SINEMA RC license.
The SINEMA RC license is available as of V8.2.

SINEMA Remote Connect (SINEMA RC)

☐ Enable SINEMA RC

Server Selection:

Primary

☐ Layer 2 Support

Server Settings

SINEMA RC Address:

192.168.203.150

Alternative SINEMA RC Address:

SINEMA RC Port:

443

Server Verification

Verification Type:

Fingerprint

Fingerprint:

CA Certificate:

-

Device Credentials

Device ID:

4

Device Password:

Device Password Confirmation:

Optional Settings

☒ Auto Firewall/NAT Rules

Type of connection:

Auto

Use Proxy:

none

Autoenrollment Interval [min]:

60

Timeout[min]:

0

Information: No KEY-PLUG M800 (6GK5 908-0PB00 or 6GK5 908-0UA00-0AA0) plugged in - license will be handled by SINEMA RC Server.

Set Values

Refresh

Information

Description

The page contains the following:

- **Enable SINEMA RC**
 - Enabled:
A connection to the configured SINEMA RC Server is established. These boxes cannot be edited.
 - Disabled:
The boxes can be edited. Any existing connection is terminated.
- **Select server**
Select the type of the SINEMA RC server:
 - Primary
This server is used first to establish a remote connection.
 - Secondary
If the primary server cannot be reached, the secondary server is queried, as long as the "Switch SINEMA RC" action is configured under "System > Connection Check". If both servers do not respond, no connection is established. You will find additional information under "System > Connection Check (Page 321)".
- **Layer2 support** (only with M87x / RM1224 / MUx85x/ S615)
If the option is enabled, communication within the established tunnel takes place via Layer 2 (VXLAN).
However, the connection to the SINEMA RC Server is established via Layer 3.

"Server settings" area

- **SINEMA RC Address**
Enter the IPv4 address or the FQDN (Fully Qualified Domain Name) of the SINEMA RC Server.
- **Alternative SINEMA RC address**
Enter the IPv4 address or the FQDN (Fully Qualified Domain Name) of the SINEMA RC Server.
The server should be the same one but an alternative FQDN.
- **SINEMA RC Port**
Enter the port via which the SINEMA RC Server can be reached.

"Server Verification" area

- **Verification Type**
 - Fingerprint: The identity of the server is verified based on the fingerprint.
 - CA certificate: The identity of the server is verified based on the CA certificate.
- **Fingerprint**
Only necessary with the setting "Fingerprint". Enter the fingerprint of the device. The fingerprint is assigned during commissioning of the SINEMA RC Server. Based on the fingerprint, the device checks whether the correct SINEMA RC Server is involved. You will find further information on this in the Operating Instructions of the SINEMA RC Server.
- **CA Certificate**
Only necessary with the setting "CA Certificate". Select the CA certificate of the server used to sign the server certificate. Only loaded CA certificates can be selected.

"Device Credentials" area

- **Device ID**
Enter the device ID. The device ID is assigned when configuring the device on the SINEMA RC Server. You will find further information on this in the Operating Instructions of the SINEMA RC Server.
- **Device Password**
Enter the password with which the device logs on to the SINEMA RC Server. The password is assigned when configuring the device on the SINEMA RC Server. You will find further information on this in the Operating Instructions of the SINEMA RC Server.
- **Device Password Confirmation**
Repeat the password.

"Optional Settings" area

- **Auto Firewall/NAT Rules**

- Enabled
The firewall and NAT rules are created automatically for the VPN connection. The connections between the configured exported subnets and the subnets that can be reached via the SINEMA RC Server are allowed. The NAT settings are implemented as configured in the SINEMA RC server.
You can enable SINEMA RC to access specific services of the device under "Security > Firewall > Predefined IPv4".
- Disabled
You will need to create the firewall and NAT rules yourself.

- **Type of connection**

Specify the type of VPN connection. You will find more detailed information in the section "Technical basics > Security features > VPN connection establishment (Page 96)".

- Auto
The device adopts the settings of the SINEMA RC server. You configure the settings on the SINEMA RC server in "Remote connections > Devices". You can find additional information on this topic in the operating instructions "SINEMA RC Server".

With the following connection types, the settings of the SINEMA RC Server are not used:

- Permanent
The device establishes a VPN connection to the SINEMA RC Server. The VPN tunnel is maintained permanently.
- Digital Input
If the "Digital In" event occurs, the device attempts to establish a VPN connection to the SINEMA RC Server.
This is on condition that the event "Digital In" is forwarded to the VPN connection. To do this, enable "VPN Tunnel" for the "Digital In" event under "System > Events > Configuration".
- Wake up SMS (only with M87x / RM1224 / MUx85x)
When the device receives a command SMS (wake-up SMS), it attempts to establish a VPN connection to the SINEMA RC Server, Provided that it is specified in "System > SMS > SMS Command" who a command SMS of the class "System" will be accepted from.
- Connection Check Action
If the "VPN Reset" or "VPN enable" actions are triggered, the device attempts to establish a VPN connection to the SINEMA RC Server. For this purpose, you configure the corresponding action under "System > Connection Check".
- TCP Event
If the incoming TCP packet contains conformant data, the device attempts to establish a VPN connection to the SINEMA RC Server. The prerequisite is that the "VPN" event is enabled under "System > TCP Event".
- GPS (only with MUx85x)
If the "SINEMA RC (all) enable" action is triggered, the device attempts to establish a VPN connection to the SINEMA RC Server. For this purpose, you configure the corresponding action under "System > GPS > Geofencing".

- VRRP
The device establishes a VPN connection to the SINEMA RC server as soon as it changes to VRRP master. For this purpose, you configure the VRRP function under "Layer 3 > VRRPv3" and enable routing.
- All
The device uses all connection types. The exception is "Auto".
- **Use Proxy**
Specify whether a connection to the defined SINEMA RC Server is established via a proxy server. Only the proxy servers that you configured under "System > Proxy Server" can be selected.
- **Autoenrollment Interval[min]**
Specify the period of time in minutes after which queries are sent to the SINEMA RC server. With this query, the device checks whether there is a newer firmware file on the SINEMA RC server or whether the connection settings have changed. If you enter the value 0, this function is disabled.
- **Timeout[min]**
Specify the period of time in minutes. If no data exchange takes place, when this time has elapsed the VPN tunnel is automatically terminated.

5.6.22 TIA Portal Cloud Connector

On this WBM page, you configure the parameters for communication with the TIA Portal Cloud Connector.

Note

- Use the "TIA Portal Cloud Connector" integrated in the product via a VPN solution (e.g. SINEMA RC).
- To prevent unauthorized access by network nodes to the "TIA Portal Cloud Connector Server", enable the item "Cloud Connector" under "Security > Firewall > Pre-defined IPv4 Rules".
- You can only enable this function on one interface at a time.

TIA Portal Cloud Connector

Operation:

Port:

Protocol:

Interface	Active
vlan1 (INT)	☐

Requirement

- For the incoming packets to be forwarded to the device, enable the predefined IPv4 rule "Cloud Connector".

Description

The page contains the following:

- **Operation**
 - Enabled
Enables the integrated TIA Portal Cloud Connector.
 - Disabled
Disables the integrated TIA Portal Cloud Connector.
 - Start on DI
Enabling is controlled via the digital input (DI) if the "Cloud Connector" is enabled for the event "Digital input" under "System > Events > Configuration". If this setting is not enabled, the event is not passed on to the TIA Portal Cloud Connector.
- **Port**
Communication with the TIA Portal Cloud Connector is established via this port.
- **Protocol**
This protocol is used to access the plant network.
 - PROFINET via VLAN
You define the VLAN interface in the following table.
Only with M804PB
 - PROFIBUS via MPI/DP
 - PROFINET-PROFIBUS

The following table is only required for PROFINET:

- **Interface**
Only VLANs with a configured subnet are available.
- **Active**
When enabled, this VLAN is used for PROFINET.
- **Reset Parameters**
Resets the properties of the interface to the default values.

5.6.23 Connection Check

On this page, you activate a ping test that monitors connections. During the ping test, the device sends ICMP echo request packets (pings) to the configured destination address at regular intervals. If this destination address does not respond, the device tries to reach the destination address again. If all ping attempts (retries) are unsuccessful, the ping test is considered to have failed or the group is considered unreachable. If the group is not reachable, the device initiates the configured action on the selected interface. If all 5 actions have been executed or after a restart, the device starts again with the first action.

Connection Check

Connection Check

Connection Fallback

☐ Enable Connection Check
Startup delay[s]: 600

Group Idx	Name	Source Interface	Interval[s]	TTL	Retries	1st Ping Target	2nd Ping Target	3d Ping Target
1	LAN	usb0	30	128	3	192.168.1.20		
2		Auto	180	128	3			
3		Auto	300	128	3			
4		Auto	300	128	3			
5		Auto	300	128	3			

LAN	Group 2	Group 3	Group 4	Group 5	Action for	1st Action	2nd Action	3rd Action	4th Action	5th Action
☐	☐	☐	☐	☐	usb0	None	None	None	None	None
☐	☐	☐	☐	☐	SINEMA RC	None	None	None	None	None
☐	☐	☐	☐	☐	Device	None	None	Restart	None	None

Set Values

Refresh

Description

- **Enable Connection Check**
Enable or disable the ping test for connection monitoring.
- **Start delay[s]**
Define the wait time after restart of the device after which the device sends a ping to the first destination address.
Range of values: 0 to 3600 seconds, default value 600 seconds. If you enter "0", the start delay is disabled.

The first table contains the following columns:

- **Group Identifier**
Index of the group
- **Name**
Specify a name for the group. The entry is displayed in the "Action" table as column name.
- **Source Interface**
Specify the interface via which reachability of the destination addresses is monitored.
- **Interval [s]**
Specify the interval at which the ping tests take place.
- **TTL (Time to live)**
Specify the TTL value.

- **Retries**
Specify how often the ping attempt is repeated.
The time interval between the ping attempts is 100 ms. With a large number of ping attempts, this can result in a time delay.
If none of the configured addresses responds, the ping test is considered to have failed (error). In the "Action" table, you define whether a specific action is executed.

- **1 ... 3. Ping Target**
Specify the destination address that is used as reference for the reachability.

The second table contains the following columns:

- **Group 1 - 5**
If a name is configured, it is used as column name. Assign the groups to the desired interface. The interface is considered reachable when all assigned groups are reachable. If only one of the groups is not reachable, the configured action is executed on the selected interface.
- **Action for**
Indicates the interface on which the action is executed.
- **1 ... 5. Action**
The following actions are possible. The selection depends on the interface on which the action is executed.
 - None (default)
 - Restart
Restart the device. After the restart, the device waits until the time specified in the "Start delay[s]" input box has expired and then sends a ping to the first destination address.
 - Soft-Reset (only with M87x / RM1224 / MUx85x)
Restart of the mobile network engine via the software
 - Hard-Reset (only with M87x / RM1224 / MUx85x)
Restart of the mobile network engine
 - Fallback (only with M876 / RM1224 / MUx85x / S615 / M826)
If the main connection fails, the data traffic is handled via the fallback connection. Provided the "Connection Fallback" function is configured.
 - VPN Reset
Restart of the VPN connection
 - Switch SINEMA RC
If the primary SINEMA RC server cannot be reached, the secondary server is queried.
 - VPN enable
Establishes a VPN connection to the VPN server.
 - VPN disable
Terminates the VPN connection to the VPN server.
 - Digital Out
Switches off the digital output.
 - Switch to phys. SIM / Switch to eSIM (only with MUM85x)
Switches the SIM card type.

5.6.23.1 Connection Fallback

M876	RM1224	MUx85x	S615	M826

The "Connection Fallback" function allows you to connect a network via 2 interfaces, e.g. the Internet. The priority determines whether the interface is the main connection or the fallback connection. If the main connection fails, the system switches over to the fallback connection. If the main connection is available again, the system switches over again. To monitor the main connection, use the "Connection Check" function.

Connection Fallback

Connection Check

Connection Fallback

☒ Enable Connection Fallback

Priority	Interface	Status
1	vlan1 (INT)	Not used
2	usb0	Not used

Set Values

Refresh

Description

- Enable Connection Fallback**
 Enable or disable the fallback function.
- Priority**
 - 1 - Main connection
 - 2 - Fallback connection
- Interface**
 Specify the interface for the connection.
- Status**
 Shows the status of the connection:
 - Active: All data traffic is handled via the interface.
 - Fallback: If the main connection fails, the data traffic is processed via the fallback connection.
 - Not used: The connection is not used.
 - Not reachable: If the main connection fails, the status changes to "Not reachable".

5.6.24 Configuration Backup

Backup

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

5.6 "System" menu

On the "System > Load&Save > HTTP/TFTP/SFTP" page, you can save the created backups in ZIP format under "ConfigPackBackup" on your client PC to be able to load them from there later. You can find more detailed information in the section "Load&Save (Page 212)".

Configuration Package Backup

Name:

Select	Name	Size[kBytes]	Restore
	Available memory	950	
☐	BackupMay2023	74	Restore

1 entry.

Create

Delete

Refresh

Description

The page contains the following boxes:

- Name**
Enter a name for the backup.

The table contains the following columns:

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

Procedure

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

5.6.25 TCP event

If you enable the "TCP Event" function on the page, the device waits for incoming TCP packets on the configured port. Authorization is performed by comparing the user data.

You have the following options with TCP packets:

- Open or close the digital output.
- Establish a VPN connection (OpenVPN, IPsec, SINEMA RC) to a partner.
- Only M87x / RM1224 / MUx85x: Send an SMS.
- Only MUM85x: Trigger the "Sleep Mode" function.
- Only MUM85x: Switch between available SIM cards.
- Enable flashing of LEDs for localization of the device.
You will find which LEDs flash in the operating instructions of the device, section "Device description > LED display".

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

Format of the TCP packet

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

```
<user name>#<password>#<command code>#<command string>:
```

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

- 105 SMS (only with M87x / RM1224 / MUx85x)
- 106 Digital Out
- 107 Sleep Mode (Only with MUM85x)
- 108 VPN
- 110 SIM switchover (only with MUM85x)
- 111 Flash

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

Note

Permitted characters for user name and password

The following characters are permitted:

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

Additionally allowed in the password:

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

TCP Event

☐ **Enable**

Username:

Password:

Password (Confirmation):

Port Number:

Enable	Event
☐	SMS
☐	Digital Out
☐	Sleep Mode
☐	VPN
☐	SIM Switchover
☐	Blink

Description

The page contains the following:

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

Note

Reserved ports

Some ports are permanently reserved. Make sure that the specified port is not already in use. You can find the ports used in the "List of available services (Page 26)".

The table contains the following columns:

- **Enable**
Enable or disable the event.
- **Event**
 - SMS (only with M87x / RM1224 / MUX85x)
Sends an SMS
`<user name>#<password>#105#01;<phone (phone number)>;<my-SMS-text (sleep)>:`
 The second-to-last parameter represents the cell phone number and the last parameter represents the message to be sent.
 - Digital Out
Opens or closes the digital output
 The digital output is open (switched on) by default and on restart. If a TCP event or a configured error occurs, the digital output is closed (switched off).
`<user name>#<password>#106#<(1,2)>:`
 The last parameter specifies the sequence number: 1 = open or 2 = closed.
 Open:
`<user name>#<password>#106#1:`
 Close:
`<user name>#<password>#106#2:`
 - Sleep Mode (Only with MUM85x)
Triggers the "Sleep Mode" function
`<user name>#<password>#107#1;<time>:`
 The last parameter specifies the sleep time in minutes.
 In the following example, sleep mode is triggered for 10 minutes:
`<user name>#<password>#107#1;10:`
 - VPN
Activates the VPN connection (IPsec, OpenVPN, SINEMA RC).
`<user name>#<password>#108#<VPN Type>;<Activate/Deactivate>;<Connection>:`
 The parameters have the following meaning

Parameter	Description	Range of values/note
VPN Type	Type of the VPN connection	• 1 = IPsec • 2 = OpenVPN • 3 = SINEMA RC
Activate/Deactivate	The VPN connection is activated or deactivated	• 1 = Activate • 2 = Deactivate
Connection	VPN connection	• Name that corresponds to a specific VPN connection • * Applies to all VPN connections Enter a name for the VPN connection or "*".

All OpenVPN connections are activated in the following example:

```
<user name>#<password>#108#2;1;*:
```

5.6 "System" menu

- SIM Switchover (only with MUM85x)
Switches the SIM card type:
`<user name>#<password>#110#<(1,2)>:`
The last parameter specifies the type of the SIM card: 1 = physical SIM or 2 = eSIM.
Switches to the physical SIM card:
`<user name>#<password>#110#1:`
Switches to the eSIM:
`<user name>#<password>#110#2:`
- Flash
Enables flashing of LEDs for localization of the device:
`<user name>#<password>#111#<time>:`
The last parameter specifies the duration of flashing in seconds.

5.6.26 GPS

5.6.26.1 Coordinates

MUM85x

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 an interactive map to obtain the geographical coordinates of the device or read out the coordinates from the device. The GPS coordinates (longitude and latitude) must be specified in decimal degrees.

Information on the GPS location is updated in the Event Log and Modem Quality Log every 10 minutes.

Description

The page contains the following input boxes:

- **Latitude**
Here, enter the value for the northerly or southerly latitude of the location of the device in the format "DD.dddddd". "DD" stands for the latitude and "dddddd" for decimal latitude.
The southerly latitude is displayed with a preceding minus sign.
- **Longitude**
Enter the value for easterly or westerly longitude for the location of the device in the format "DD.dddddd". "DD" stands for the longitude and "dddddd" for decimal longitude.
The westerly longitude is displayed with a preceding minus sign.
- **Height**
Enter the value of the geographic height above sea level in meters.
For example, 33 m means that the device is located at a height of 33 m above sea level.
Heights below sea level (for example the Dead Sea) are indicated by a preceding minus sign.
- **Use GPS Location**
Enables or disables automatic read-out of the device location. The accuracy of the location determination is about 10 meters.
If you enable the option, the input fields for latitude, longitude and height are not editable.
- **GPS cycle time[s]**
Specify the amount of time in seconds after which the GPS location is updated.
Range of values: 1 ... 600 seconds. Default value: 60 seconds.
- **GPS position**
Shows the current GPS position in the decimal system in the order "Latitude, longitude, height".
- **Satellite**
Shows the number of available satellites.
- **HDOP (Horizontal Dilution Of Precision)**
Shows the accuracy of horizontal location detection. The lower the value, the more precise the position detection. The value 0 means no deviation from the actual position.
- **Speed**
Shows how fast the device moves.
- **Last synchronization**
Shows the status of the synchronization:
 - Synced
Location determination was performed.
 - Not Synced
Location determination was not performed.
 - >= <time in minutes>
The time in minutes since the last attempt to determine the location.

Procedure

1. Enable the "Use GPS Location" option to determine the location automatically.
2. Click the "Set Values" button.

5.6.26.2 Geofencing

MUM85x

With geofencing, you can define geographical areas within or outside of which you can control your SCALANCE M device.

On this page, you define areas in which specific events trigger desired actions on the device after their occurrence. You can configure up to 20 areas.

Geofencing

Coordinates | Geofencing

☐ Enable Geofencing

Select	Name	Latitude	Longitude	Radius[m]	Timeout[min]	Min. Satellites	Event	Action	Enabled
☐	Area1	49.9917	8.41321	20	5	3	Leave	Event System	☐

1 entry.

[Create](#) [Delete](#) [Set Values](#) [Refresh](#)

Description

The page contains the following:

- **Enable Geofencing**
Enables or disables geofencing.
To log this, activate the "Geofencing" event under "System > Event".

The table contains the following columns:

- **Select**
Select the row you want to delete.
- **Name**
Enter the name of the area to be delimited.
Maximum of 64 characters.
- **Latitude**
Enter the northerly or southerly latitude of the area to be delimited in the format "DD.dddddd". "DD" stands for the latitude and "dddddd" for decimal latitude.
The southerly latitude is displayed with a preceding minus sign.
- **Longitude**
Enter the easterly or westerly longitude of the area to be delimited in the format "DD.dddddd". "DD" stands for the longitude and "dddddd" for decimal longitude.
The westerly longitude is displayed with a preceding minus sign.
- **Radius[m]**
Enter the radius of the area to be delimited in meters.
Range of values: 10 ... 2147483647. Default value 20.
- **Timeout[min]**
Specify the period of time in minutes after which the action is triggered.
Range of values: 1 ... 2147483647. Default value 5.
- **Min. satellites**
Enter the number of satellites to be available for location detection.

- **Event**
Select an event that triggers the action when it occurs.
 - Leave
The device leaves the area to be delimited.
 - Enter
The device enters the area to be delimited.
 - In
The device is in the area to be delimited.
 - Out
The device is outside of the area to be delimited.
- **Action**
From the drop-down list, select the action to be performed when the specified event occurs.
 - Event System
Triggers the event that is configured under "System > Events".
 - Restart
Restarts the device.
 - Restart Factory
Restores the factory settings for the device and restarts it.
 - Fault enable / Fault disable
Switches fault monitoring on/off.
 - Digital Output close / Digital Output open
Closes/opens the digital output.
 - Sleep Mode
Activates sleep mode.
 - Engine HW Reset
Performs the hard reset with a restart of the mobile network engine.
 - Engine SW Reset
Performs the restart of the mobile network engine via the software.
 - Enable IPsec (all) / Disable IPsec (all)
Establishes/terminates a VPN connection to the IPsec server.
 - Enable OpenVPN (all) / Disable OpenVPN (all)
Establishes/terminates a VPN connection to the OpenVPN server.
 - Enable SINEMA RC (all) / Disable SINEMA RC (all)
Establishes/terminates a VPN connection to the SINEMA RC Server.
 - Switch to physical SIM/ Switch to eSIM
Switches the SIM card type to the selected type.
- **Enable**
Activates the execution of the action under the given conditions.

5.6.27 **iperf**

MUM85x

With the iperf tool, you can measure the data throughput in the network to determine the maximum reachable bandwidth. You need two connected SCALANCE MUM85x for measurement.

Note

Use iperf on two SCALANCE MUM85x with the same firmware version.

On this page, you configure the iperf function on the remote SCALANCE MUM device in server mode and on the local SCALANCE MUM device in client mode and start connection speed measurements between the two devices. You can measure data traffic in the two directions one after the other.

Note

The use of iperf can lead to device overload. Do not use the function in productive operation.

The screenshot shows the 'iperf' configuration page. It features a series of input fields and dropdown menus for configuring the iperf tool. The 'Type' is set to 'Client', 'Port' is 5201, 'Address' is empty, 'Direction' is 'Reverse', 'Streams' is 5, 'Timeout[s]' is 10, 'Omit[s]' is 0, 'Username' and 'Password' are empty, 'Certificate' is '-', 'Traffic Type' is 'TCP', and 'Bandwidth[MBit/s]' is 100. A 'Start' button is located below the bandwidth field. Below the 'Start' button is a text label 'iperf Output:' followed by a large, empty rectangular box for output. At the bottom left of the form is a 'Refresh' button.

Type:	Client
Port:	5201
Address:	
Direction:	Reverse
Streams:	5
Timeout[s]:	10
Omit[s]:	0
Username:	
Password:	
Certificate:	-
Traffic Type:	TCP
Bandwidth[MBit/s]:	100

Start

iperf Output:

Refresh

Description

The page contains the following:

- **Type**
Specify the measurement mode. The following options are available:
 - Client
For configuring the local device in client mode.
You specify the direction of measurement in the "Direction" drop-down list.
Measurements are always started on the client.
 - Server
For configuring the remote device in server mode.
- **Port**
Port that the server listens to and via which the client attempts to establish a connection to the server.
You can change the port number. The port number must be identical for the server and client.
Default value: 5201
- **Address**
Specify the IP address of the server.
- **Direction**
Specify the direction of measurement. The following options are available:
 - "-" (disabled)
Measurement takes place from client to server.
 - Reverse
Measurement takes place in the reverse direction. The server sends and the client receives.
- **Streams**
Specify the number of data flows to be measured.
Default value: 5
- **Timeout[s]**
Define the duration for the measurement. When the time elapses, measuring stops.
Default value: 10
- **Omit[s]**
Specify the time until measuring starts. This is necessary to skip the TCP slow start phase.
- **User name**
Specify the user name.
- **Password**
Specify the password.
- **Certificate**
Select the server certificate.
- **Traffic Type**
Select the protocol for data transfer.
 - TCP
 - UDP

5.7 "Interfaces" menu

- **Bandwidth[Mbps]**
Specify the maximum bandwidth to be expected.
- **"Start" button**
Click this button to start the iperf function.
- **iperf output**
This box shows the output of the iperf function.

5.7 "Interfaces" menu

5.7.1 Ethernet

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

Ports Overview

Overview	Configuration							
Port	Port Name	Port Type	Status	OperState	Link	Mode	Negotiation	MAC Address
P1		Switch-Port VLAN Hybrid	enabled	up	up	100M FD	enabled	d4-f5-27-a4-83-d8

Refresh

Description

The table has the following columns:

- **Port**
Shows the configurable ports. The entry is a link. If you click on the link, the corresponding configuration page is opened.
- **Port Name**
Shows the name of the port.
- **Port Type** (only with routing)
Shows the type of the port. The following types are possible:
 - Switch Port VLAN Hybrid
 - Switch Port VLAN Trunk
- **Status**
Shows whether the port is on or off. Data traffic is possible only over an enabled port.

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

5.7.1.1 Configuration

Configuring ports

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

Ports Configuration

Overview | **Configuration**

Port: P1 ▼

Status: enabled ▼

Port Name:

MAC Address: 00-1b-1b-9a-32-2e

Mode Type: Auto negotiation ▼

Mode: 100M FD

Negotiation: enabled

Port Type: Switch-Port VLAN Hybrid ▼

OperState: up

Link: up

Description

- **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 but the connection remains.

Note

Turn off unused ports.

- Link down
The port is disabled and the connection to the partner device is terminated.
- **Port Name**
Here, enter a name for the port.
- **MAC Address**
Shows the MAC address of the port.

- **Mode Type**

From this drop-down list, select the transmission speed and the transfer mode of the port. The following settings are possible:

- 10 Mbps full duplex (FD) or half duplex (HD)
- 100 Mbps full duplex (FD) or half duplex (HD)
- Auto negotiation

Additionally with the MUx85x:

- 1000 Mbps full duplex (FD)

If you set the mode to "Auto negotiation", these parameters are automatically negotiated with the connected end device or network component. This must also be in the "Autonegotiation" mode.

Note

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

- **Mode**

Shows the transmission speed and the transmission mode of the port. The display depends on the set "Mode Type".

- **Negotiation**

Shows whether the automatic configuration of the connection to the partner port is enabled or disabled.

- **Port Type**

Select the type of port from the drop-down list.

- Switch Port VLAN Hybrid
The port sends tagged and untagged frames. It is not automatically a member of a VLAN.
- Switch-Port VLAN Trunk
The port only sends tagged frames and is automatically a member of all VLANs.

- **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 physical 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" signal is being received.
- Down
The link is down, for example because the connected device is turned off.

5.7.2 Mobile wireless

5.7.2.1 General

MUX85x M87x RM1224

For access to the mobile network and the mobile wireless services, access parameters are required that you specify on this page. You will receive the access parameters from your mobile network provider.

You can use the "Mobile data usage" function to control the used data volume.

Note

Use a time server to avoid incorrect detection of the volume of data used.

Mobile Network Interface Settings

GeneralSIMOperatoreSIM ProfileSIM SwitchoverTX Power ReductionDiagnostics

☐ Enable Mobile Network Interface

☐ Fast Engine Startup

Select SIM Type: Physical

☒ Enable SIM

PIN:

PIN Confirmation:

Radio Mode: 5G NR SA only

Band: 78

IP Version: IPv4 only

Authentication Method: CHAP

Allow Roaming: Allow Roaming

☒ IP Passthrough

Passthrough MAC: af-fe-27-00-00-0d

☐ Mobile data usage

Reset day of month: 1

Warning Limit [MB]: 2000

Reset mobile data usage

Set ValuesRefreshInformation

Changes made to the SIM card are logged in the event log. Log messages start with "Primary-Modem Physical-SIM: < log message>" for an exchangeable SIM card and "Primary-Modem e-SIM: < Log message>" for an eSIM card.

Description

The page contains the following:

- **Enable Mobile Network Interface**
Enables or disables the mobile network interface. Before you enable the mobile network interface, select the desired SIM card type at "Select SIM type" and enable the SIM card at "Enable SIM".
- **Fast Engine Startup** (Only with SCALANCE MUM85x)
Accelerates the connection to the mobile network by eliminating the engine reset after the device starts.
Enable the option to reduce the time to establish the mobile wireless connection.
- **SIM Type**
Select the type of SIM card. The following card types are possible:
 - Physical
Exchangeable SIM card
 - eSIM (Only with SCALANCE MUM85x with built-in eSIM)
Embedded SIM card (embedded SIM)

Note

The eSIM function is available in SCALANCE MUM85x devices as of HW version 2. You can find information on the hardware version under "Information > I&M (Page 143)".

The eSIM function is not available with the 6GK5856-2EA00-3FA1 and 6GK5853-2EA10-2BA1 device variants.

- **Enable SIM**
Enables the SIM card. You can only enable one SIM card in V8.0.
- **PIN**
Personal identification number
If the mobile network interface is enabled, the currently valid PIN of the SIM card is queried. Enter the currently valid PIN for the selected SIM card. The device also operates with SIM cards that do not require a PIN or for which the PIN query has been deactivated.

Note

If you make incorrect entries, the SIM card is blocked

Make sure that you enter the PIN correctly. If you enter the PIN incorrectly three times, the SIM card will be locked.

In "Information > Mobile", you can check the status of the SIM card. If "SIM Status" displays "PUK required", the SIM card is locked. You can release the SIM card again under "Interfaces > Mobile > SIM".

- **PIN Confirmation**
Repeat the PIN.

- **Radio Mode**

Select the required mobile network. The following options are available:

- Auto (not with the M874-2)
All services. As first choice, the device attempts to establish a connection to the fastest available mobile wireless system.
- GSM only
The EGPRS and GPRS services. The device ignores the UMTS and LTE network and establishes a connection to the GSM service that provides the highest bandwidth locally
- UMTS only (not with the M874-2)
The UMTS and HSPA service. The device ignores the EGPRS, GPRS and LTE services and establishes a connection in the UMTS network.
- Only LTE (only with M876-4 / RM1224 / MUx85x)
The service LTE. The device ignores the EGPRS and GPRS and UMTS services and establishes a connection in the LTE network.
- 5 G NR + LTE (NSA) (only with MUx85x)
The services 5G New Radio (NR) and LTE non-standalone operation (NSA)
- 5 G NR SA only (only with MUx85x)
The service 5G New Radio (NR) in standalone operation (SA)
- EVDO (only with M876-3)
EVolution, Data-Optimized. Default for CDMA-based networks.
The following sub-standards are supported:
 - EVDO Hybrid
 - EVDO 1xRTT
 - EVDO HDR - High Data Rate
- No data connection
There is no data connection. Suitable when the device is only used to send or receive SMS messages.

- **Band**

Option for setting a band limitation. Can only be entered if "5G NR SA only" is selected as Radio Mode.

- Auto
There are no limitations for the 5G SA bands.
- N1, N3, N28, N78
Only the selected 5G band is used.

- **IP Version**

Specify which IP version the device supports. The following options are available:

- IPv4 only
- IPv6 only
- IPv4 + IPv6

- **Authentication Method**

Select the required authentication method.

- Auto
User name and password are transferred automatically with one of the following two methods. CHAP has the higher priority. If the communications partner does not support CHAP, the user name and password are transferred using PAP.
- CHAP
Challenge Handshake Authentication Protocol
Encrypted transfer of user name and password using CHAP.
- PAP
Password Authentication Protocol
Unencrypted transfer of user name and password using PAP.

- **Allow Data Roaming**

Select the required roaming type. The following options are available:

- Allow roaming
The device automatically logs into an available network if the specified network is unreachable.
- No data roaming
The connection is interrupted when the specified network is not reachable.
- No roaming
The function is disabled. Connection establishment is disabled.

- **IP Passthrough** (only with SCALANCE MUM85x)

Enables the IP Passthrough function.

IP Passthrough enables the device to bypass the router of the Internet service provider and receive an IP address directly from the modem of the Internet service provider. In this way, the device can communicate directly with the network of the Internet service provider. The TIA interface of the device is connected to the WAN interface.

The prerequisite is that Masquerading on the WAN interface and DHCP client on the local VLAN interface are disabled.

Note

Effect on the firewall

Note that IP Passthrough bypasses the set firewall of the router.

Changes to the Layer 2 or Layer 3 interface

IP Passthrough needs to be enabled again on changes to the Layer 2 or Layer 3 interface.

- **Passthrough MAC**

Specify the MAC address of the device that receives the public IP address in the network and directly receives the inbound data traffic of the Internet service provider.

- **Mobile data usage**

When enabled, you monitor when the defined limit is reached. The limit that you define defines the maximum data volume per month.

The consumption of the data volume is displayed under "Information > Mobile > Data Usage".

- **Reset on the day of the month**
The invoicing period does not always start on the first day of a month, but on the day on which the contract was concluded.
Specify the day on which the monthly invoicing period begins. The consumed data volume is set to 0 on this day.
- **Warning limit [MB]**
Enter the limit of the monthly data volume.
In addition, you can receive data warnings when 75 % and 100 % of the specified data volume is reached, provided that the desired type of notification is enabled for the "Mobile data usage" event under "System > Events > Configuration".
- **Reset data**
Deletes the stored values.

Warnings received via SMS

To receive warnings via SMS, do the following:

1. For "Reset on the day of the month", specify the start of the invoicing period.
2. For "Warning limit", set the data volume in MB.
3. Select "Mobile data usage" and click on the "Set Values" button.
4. Set the receiver under "System > SMS > Event SMS".
 - Enter the telephone number in the "Call number" text box.
 - Click the "Create" button.
 - Activate "Enable event SMS" and "Send" for the receiver.
 - Click the "Set Values" button.
5. Set the notification type "Apply SMS settings" for the "Exceed data limit" event under "System > Events > Configuration".
6. Click the "Set Values" button.

Result

The recipient receives the warnings via SMS.

Enabling IP Passthrough for an end device

To have a public IP address assigned to an end device connected to the SCALANCE MUM85x, do the following:

1. Under "Layer 3 (IPv4) > NAT > Masquerading", clear the "Masquerading" check box for theusb0 WAN interface.
2. Under "System > DHCPv4 > DHCP client", clear the "DHCP" check box for the vlan1 VLAN interface.
3. Under "Security > Firewall > IP Rules", create the "Accept from vlan1 to usb0" rule.
4. Select the "IP-Passthrough" check box on this page.

5. Enter the MAC address of the end device to be directly connected to the router of the Internet service provider.
6. On the end device under "System > DHCPv4 > DHCP client" and under "Security > Firewall > Predefined", select the "DHCP" check box for the local VLAN interface vlan1.

Result

The end device receives from the Internet service provider the external IP address which would be assigned to the SCALANCE MUM85x without IP Passthrough.

5.7.2.2 SIM

MUx85x

M87x

RM1224

You receive the PIN with the SIM card. On this page, you can change the PIN of the selected SIM card or release locked SIM cards, if necessary.

Requirement

- The mobile network interface is disabled.
- The desired SIM card is selected and enabled on the "Interfaces > Mobile > General" page under "Select SIM card type".

Description

The page contains the following:

- **Status**

Shows the status of the action. The following entries are possible:

- -
No action was performed.
- Action starts...
Execution of the selected action is starting.
- Action in progress... Reset mobile engine
The wireless module is automatically reset after execution of the action.
- SIM Action was successful
The selected action was successful.
- SIM Card locked
The SIM card is irreversibly locked because the incorrect PUK was entered ten times in succession.
- SIM not locked, please use "Change PIN".
The entry under "PUK" is not required.
- SIM is locked, use "Unlock SIM".
The SIM card is locked because the incorrect PIN was entered three times in succession. Unlock the SIM card with the action "Unlock SIM".
- Wrong PIN (remaining attempts %d)
The entry under "Old PIN" is incorrect. Shows the number of remaining attempts.
- Wrong PUK (remaining attempts %d)
The entry under "PUK" is incorrect. Shows the number of remaining attempts.

- **Action**

Select the required action:

- Change PIN
Changes the PIN of the selected card.
- Unlock SIM (PUK)
Unlocks the SIM card using the PUK and defines a new PIN.
- Enable PIN
Switches on PIN request.
- Disable PIN
Switches off PIN request.

Note

When you change the PIN, you need to adjust the PIN under "Interfaces > Mobile > General".

- **Old PIN**

Enter the currently valid PIN.

- **PUK**
Personal Unblocking Key
Enter the PUK. You will have received the PUK from your operator together with the SIM card. If you enter the PUK incorrectly ten times in succession, the SIM card will be irreversibly locked.
- **New PIN**
Enter the new PIN that you wish to use instead of the previous PIN.
- **New PIN Confirmation**
Repeat the new PIN.
- **Start**
Executes the selected action. Depending on the action, execution can take up to 30 seconds. Refer to the display under "Status" to check whether the action was successful. You can update the display either automatically or manually.
 - Automatic
In the top right corner of the display area on this page, you can switch automatic updating of the content area on or off using the "on/off" buttons. If enabled, the display is updated every 2 seconds.
 - Manual
Click the "Update" button.

5.7.2.3 Mobile wireless provider

M87x

RM1224

MUx85x

The APN (Access Point Name) is the name of the access point from the mobile network to the Internet or to a private company network. Depending on the type of network connected, this is a public or private APN. Information about the APN is provided by the mobile network provider.

Operator

GeneralSIMOperatorConnection Check

Country List: -

Provider List: -

PLMNID:

Operator Name:

APN:

User Name:

Password:

Password Confirmation:

Select	PLMNID▼	Operator Name	APN	User Name	Password	Password Confirmation	Enabled
☐	Manual						☐
☐	26207	O2	internet	guest	••••••	••••••	☒
☐	26203	Eplus	internet.eplus.de	guest	••••••	••••••	☒
☐	26202	Vodafone	web.vodafone.de	guest	••••••	••••••	☒
☐	26201	T-Mobile	internet-t-mobile	guest	••••••	••••••	☒

5 entries.

CreateDeleteSet ValuesRefresh

Description

The page contains the following:

- Country List**
From this list, select the country in which the device will be deployed.
- Provider List**
From this list select the appropriate mobile network provider. The list depends on the selected country.
If the mobile network provider is not contained in the list of providers, select "-".

Note

"5G SA (Standalone) only" radio mode

For "5G SA only" radio mode, disable all providers that are not needed.

- PLMNID**
Each mobile network provider has an identification number that is unique worldwide known as the Public Land Mobile Network ID (PLMN ID). You can find the Net ID in the documentation of your mobile network provider or on their Internet pages.
 - If you know the PLMNID of the mobile network provider, enter this number.
 - If you do not know the PLMNID, enter the data in the table under "Manual".
- Operator Name**
Enter the name of your mobile network provider.
- APN**
Enter the name of the APN. You can find the APN in the documentation of your mobile network provider on your provider's Website or ask your mobile network provider's hotline.

- **User Name**
Enter the user name. Some mobile network providers do not use access control with user names and/or passwords. In this case, leave the box empty.
- **Password**
Enter the password. Some mobile network providers do not use access control with user names and/or passwords. In this case, leave the box empty.
- **Password Confirmation**
Repeat the password.

The table contains the following columns:

- **Select**
Select the check box in the row to be deleted.
- **PLMNID**
 - Identification number (Net ID)
Displays the PLMNID of the mobile phone provider.
 - Manual (static APN)
If the PLMNID is not known, enter the APN of your mobile phone provider.
 - Manual (dynamic APN)
Only available with M876-4 / RM1224
Requirement: Radio mode "LTE only"
If you do not configure any data, the APN is assigned dynamically.
- **Operator Name**
Enter the name of your mobile network provider.
- **APN**
Enter the name of the APN. You can find the APN in the documentation of your mobile network provider on your provider's Website or ask your mobile network provider's hotline.
- **User Name**
Enter the user name for the APN. Some mobile network providers do not use access control with user names and/or passwords. In this case, leave the box empty.
- **Password**
Enter the password for the APN. Some mobile network providers do not use access control with user names and/or passwords. In this case, leave the box empty.
- **Password Confirmation**
Repeat the password.
- **Enabled**
The entry is used

5.7.2.4 Band rejection filter

Note

This WBM page is only available for the device variants 6GK5856-2EA10-3BA1 (B1), 6GK5853-2EA10-2BA1 (B1) and 6GK5852-1EA10-1BA1 (B1).

A private industrial 5G network can be divided into multiple cells. To allow differentiation between the cells that are in the same frequency band, each cell now has a unique PCI (Physical Cell ID). Individual radio channels within assigned frequency bands can be uniquely identified by the ARFCN (Absolute Radio Frequency Channel Number) value.

On this page, you specify which channel in which cell the device is permitted to use. The device can no longer access other cells in the same frequency band.

Radio Lock

General

SIM

Operator

Radio Lock

Diagnostics

Select	Index	Type	Value
☐	1	PCI	209
☐	2	ARFCN	152690

2 entries.

Create

Delete

Set Values

Refresh

Description

The table contains the following columns:

- Select**
Select the check box in the row to be deleted.
- Index**
Number of the entry
- Type**
 - PCI (Physical Cell ID)
Specify the cell in which the device is permitted to register.
 - ARFCN (Absolute Radio Frequency Channel Number)
Specify which channel the device will use.
The prerequisite is that the channel is within the frequency band of the cell.
- Value**
Specify the corresponding value.

5.7.2.5 eSIM profile

MUM85x

Note

The eSIM function is available in SCALANCE MUM85x devices as of HW version 2. You can find information on the hardware version under "Information > I&M (Page 143)".
The eSIM function is not available on the 6GK5856-2EA00-3FA1 device variant.

An eSIM is an embedded SIM that you activate using the QR code provided by the mobile network provider in order to use its mobile plan.

On this page, you create an eSIM profile of your eSIM card on the device. This page is used for initial setup of the eSIM.

Using a camera connected to your PC, you can scan in the QR code. By reading out the QR code, the profile is completed with the data provided by the mobile network provider and usage of the eSIM is activated by the mobile network provider. This means that you do not have to manually enter the activation code. Note the requirements for this operation.

If you want to change the PIN of the eSIM card or unlock the locked eSIM, use the "Interfaces > Mobile Network > SIM" page.

eSIM Profile

General SIM Operator **eSIM Profile**

Status: eSIM disabled

Name:

Activation Code:

Activation PIN:

Activation PIN Conf.:

Select	Name	Enabled
0 entries.		

Information: Create or delete a eSIM profile can take up to 1 minute. Please click 'Refresh' to see the result.

Create Delete Refresh

Requirements

Before you create an eSIM profile, check the following:

- The date and time are current.
You set the system time on the "System > System Time > Manual Setting" page with the "Use PC Time" button.
- An Internet connection exists, e.g. over the Ethernet interface.
You set a default route on the "Layer 3 (IPv4) > Static Routes" page. Enter the IP address of your WLAN router as the gateway.
- The DNS server has been configured.
You set the DNS server on the "System > DNS > DNS Client" page. Enter the IP address of the DNS server, e.g. the IP address of your WLAN router.
- The mobile network interface is disabled.

Description

The page contains the following:

- **Status**
Shows the status of the eSIM.
 - eSIM enabled
The eSIM card is enabled.
 - eSIM disabled
The eSIM card is disabled.
 - Write progress started
The eSIM profile is being searched for or installed.
 - eSIM available
The eSIM profile is available.
 - Write progress failed
The operation has failed.
- **Name**
Enter a name for the eSIM card.
- **Activation Code**
You receive the activation code from the mobile network provider.
By entering the activation code, data needed to activate the eSIM is transmitted by the mobile network provider.
Hold the QR code in front of the camera connected to your PC. The scan area of the camera is shown in the top area of the page. The activation code is automatically read out and entered in the input field.
- **Activation PIN**
Activation PIN (ePIN) for activating the eSIM card
Enter the Activation PIN for the eSIM card. You receive the Activation PIN from the mobile network provider.
- **Activation PIN Conf.**
Repeat the Activation PIN.

The table contains the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Name**
Shows the name of the eSIM card.
- **Activated**
Shows the status of the eSIM card.

Creating a new eSIM profile on the device

You can create up to three eSIM profiles of any mobile network providers.

To create an eSIM profile, follow these steps:

1. Select the entry "eSIM" in the "Select SIM Type" drop-down list on the "Interfaces > Mobile Network > General" page.
2. Select the "Enable SIM" check box.
3. Click "Set Values".
4. Open the "eSIM Profile" tab and refresh the page with the  button in the upper right display area of the page.
The status "Write progress started" is displayed while the device searches for an eSIM. This can take up to a minute. If the search is successful, the status changes to "eSIM available" and the scan area of the camera is displayed.
5. Enter a name for the eSIM profile. Special characters are not permitted.
6. Hold the QR code in front of the camera to read the activation code.
The activation code is automatically entered into the "Activation Code" line. In the CLI, the activation code should be manually entered or copied.

Note**Activation code can be used only once**

The activation code cannot be used simultaneously on more than one device. It is not possible to install the same activation code on an additional device. This is true even if the activation code was already used on an end device, e.g. a smartphone.

7. Enter the Activation PIN.
You will find the Activation PIN (often designated as the ePIN) in the correspondence from the mobile network provider for the sent eSIM.
8. Confirm the Activation PIN by re-entering it and save the profile with "Create".
After the profile is saved, the status changes to "Write progress started". The eSIM profile is now downloaded and installed. An Internet connection to the mobile network provider is established in the background to check if the PIN matches the eSIM. It can take up to a minute to create the profile. During this time, you can use the  button to refresh the operation. If the search is successful, the status changes to "eSIM available". If the check fails, a message is displayed indicating this.

If you change the name in the eSIM profile later, the profile will be reloaded, and the update can take a few minutes.

Activating a previously created eSIM profile on the device

A newly created eSIM profile is initially deactivated on the device. The displayed SIM status in the "Information > Mobile Network > Overview" menu is "Missing", and a mobile network connection cannot be established. At this point, it is not possible to select the "Enable Mobile Network Interface" check box on the "Interfaces > Mobile Network > General" page. If you try to do so, the message "No SIM card detected" is displayed.

Note

An Internet connection is not needed to activate, deactivate or rename an eSIM profile. An Internet connection is only needed when installing a new eSIM profile using the Activation Code.

Only one eSIM profile can be active. If you want to activate another eSIM profile, you must first deactivate the currently active eSIM profile.

1. Select the desired eSIM profile using the "Activated" check box and click "Set Values". The SIM status in the "Information > Mobile Network > Overview" menu changes to "Available". The eSIM now behaves like a SIM card, and you have the option of assigning it a PIN. Note that if the eSIM profile is deleted, all changes will be lost.
2. Select the "Enable Mobile Network Interface" check box on the "Interfaces > Mobile Network > General" page.
Once the mobile network interface has been enabled, the configuration fields of the SIM are grayed out. This prevents any change to the SIM or a change from one SIM to another during operation.

Deleting an eSIM profile from the device

You can delete one or more eSIM profiles. You do not need an Internet connection for this. If an Internet connection is active, the mobile network provider is notified about the eSIM to be released.

To delete an eSIM profile, follow these steps:

1. Clear the "Enable Mobile Network Interface" check box on the "Interfaces > Mobile Network > General" page.
2. Open the "eSIM Profile" tab. If the eSIM profile to be deleted has been enabled, disable it in the table column "Activated", and click "Set Values".
3. Select the eSIM profile to be deleted and click "Delete".
The eSIM profile is deleted from the device.

Note

Releasing eSIM for further use

With an active Internet connection, the activation code becomes usable again after deletion of the eSIM profile and confirmation of the mobile network provider of the release of the eSIM involved. In the case of some mobile network providers, however, the activation code is used up after the first activation, and you must reorder after deleting the eSIM profile.

Switching to a physical SIM

1. Clear the "Enable Mobile Network Interface" check box on the "Interfaces > Mobile Network > General" page.
2. Select the entry "Physical" from the "Select SIM Type" drop-down list.
After activation of the physical SIM, the created eSIM profiles are no longer visible.

5.7.2.6 SIM switchover

MUM85x

On this page, you can define the backup SIM cards (fallback SIM) and the time until switchover of the active SIM card to the fallback SIM card if a configured event occurs.

The fallback mechanism is triggered by the following changes:

- Status change of the digital input
- Geofencing Action
- TCP Event
- Connection Check Action

The digital input has the highest priority among the triggers for a SIM change. For the three triggers specified last, in contrast to the digital input, the configuration action "Switch to physical SIM" or "Switch to eSIM" is performed first and then the switch to the fallback card in sequence takes place in the next step.

SIM Switchover

General

SIM

Operator

eSIM Profile

SIM Switchover

Diagnostics

☒ SIM Switchover

Fallback Timeout[min]: 0

SIM Type	Priority	Digital Input	Status
Physical	3	☒	Active
eSIM	10	☐	Fallback

Set Values

Refresh

Note

During the SIM switchover, the connection to the mobile wireless network is interrupted. The switchover time can be up to three minutes.
A SIM switchover does not necessarily result in a successful connection. If there is no connection to the mobile wireless network after a switchover, the fallback list is started from the beginning again.

Requirement

- The eSIM and physical SIM are configured.

Description

The page contains the following:

- **SIM Switchover**
Enables the fallback function.
If the assigned SIM card fails, the fallback SIM is used for connection to the mobile wireless network.
Clear this check box to configure the fallback settings.
- **Fallback Timeout[min]**
Enter the time period after which switchover to the fallback SIM takes place if the mobile wireless network is not available.
Range of values: 0 = immediate switchover to the fallback SIM card or 10 ... 1440 minutes (24 hours).
Default value: 10 minutes
- **SIM Type**
Shows available SIM cards.
 - Physical
Exchangeable SIM card
 - eSIM (only with SCALANCE MUM85x with built-in eSIM; does not apply to 6GK5856-2EA00-3FA1)
Embedded SIM card (embedded SIM)
- **Priority**
Enter the priority of the SIM cards. The lower the value, the higher the priority. The SIM type with the lowest priority value is used as first fallback SIM.
- **Digital Input**
The fallback function can be controlled via the digital input, e.g. using a button. When the button is closed, voltage is applied to the digital input and the LED of the digital input lights up. The lit LED indicates that signal 1 (TRUE / HIGH) is applied. In this state, the assigned SIM type is used. Switchover to the next fallback SIM type in sequence takes place when the signal at the digital input changes from 1 (HIGH) to 0 (LOW).
You will find information on connecting and the maximum current load in the operating instructions of the devices.
The digital input can only be assigned to one SIM type.
- **Status**
Shows the current status of the SIM card.
 - "-"
The status is unknown.
 - Active
The SIM card is currently being used.
 - Fallback
The SIM card is stored as fallback SIM and can be activated by a trigger.
 - Disabled
The eSIM card is disabled.
 - Not used
The SIM card was previously active.

Procedure

To enable the fallback function, do the following:

1. For "Fallback Timeout[min]", enter the time until switchover to the fallback SIM card in minutes.
2. For "Priority", enter the priority of the SIM cards.
3. Select the "SIM Switchover" check box.
4. Click the "Set Values" button.

Result:

If the mobile wireless network remains unavailable via the SIM card for the specified time, the device switches to the fallback SIM.

5.7.2.7 Tx Power Reduction

Antenna configuration

MUx85x

This section shows you how to configure the settings for the connected antennas. You will find more information on the frequency bands supported by the device in the "Requirements for operation (Page 42)" section.

Note

This function is available from HW release 16 (models MS5G16R and EL5G16R).

TX Power Reduction

General

SIM

Operator

eSIM Profile

SIM Switchover

TX Power Reduction

Diagnostics

Technology	Band	Min TX Power[dBm]	Max TX Power[dBm]	TX Power[dBm]	Antenna Gain[dBi]	Total attenuation[dB]	EIRP[dBm]
5G NR	48	14	23	23	0	0	23

Set Values

Refresh

Note

Connectors that are not used must have a 50 Ω terminating resistor fitted.

To use 3/4/5G connectivity, one antenna must always be connected to each of the antenna connectors. If you want to use GNSS, connect a passive antenna with a clear view of the sky to the A4 port.

You will find more information on connecting the antennas in the operating instructions of the device.

Description

The table is comprised of the following columns:

- **Technology**
Shows the mobile network standard used:
 - GSM
 - UMTS
 - LTE
 - 5G
- **Band**
Shows the band used.
- **Min TX Power[dBm]**
Displays the minimum transmit power of all active antenna connectors.
- **Max TX Power[dBm]**
Displays the maximum transmit power of all active antenna connectors.
- **TX Power[dBm]**
The transmit power is entered here.
- **Antenna Gain[dBi]**
The antenna gain is entered here.
- **Total attenuation[dB]**
The attenuation caused by additional damping elements such as attenuators or connection cables, for example.
- **EIRP[dBm]**
Effective Isotropic Radiated Power
Shows the current radiant power of the antenna in relation to a non-directional antenna (isotrope).
$$\text{EIRP} = \text{Tx Power} + \text{Antenna Gain} - \text{Attenuation (antenna connectors, cable length, and additional attenuation)}$$

5.7.2.8 Modem diagnostics

MUx85x

On this page, you activate a diagnostics interface for the device.

Modem Diagnostics

General

SIM

Operator

eSIM Profile

SIM Switchover

Diagnostics

☐ Enable TCP Diagnostics Stream

Port:

☐ Enable Encryption

Local Certificate:

Remote Certificate:

Set Values

Refresh

Note

The TCP Diagnostics Stream generates network load and should not be used in productive operation.

Description

- Enable TCP Diagnostics Stream**
If you select this check box, TCP Diagnostics Stream allows diagnostics data to be collected on the device, prepared and read out using SNMP by a network management station that also supports TCP Diagnostics Stream. This diagnostic data allows problems in the mobile network to be detected early and eliminated.
- Port**
You can specify a port on which the statistics will be displayed.
Default value: 5511
- Enable Encryption**
Enables encryption for access to diagnostics data.

Note

Without encryption, TCP Diagnostics Stream is considered non-secure and therefore can only be used locally. As of V8.1, encryption that enables secure use in productive operation also is supported.

- Local Certificate**
Select the local certificate.
- Remote Certificate**
Select the remote certificate.

5.7.2.9 Connection Check

M87x

RM1224

Use this function to ensure that the connection to the mobile network is retained. On this page you specify which WAN-IP addresses are used as reference for the connection monitoring.

The device sends echo messages (pings) to the configured WAN IP addresses of the remote stations at regular intervals (Ping Time Interval).

If, for example, you configure three WAN-IP addresses, the device sends a ping to the first WAN-IP address. If this WAN-IP address is reachable, it sends a reply. When the configured interval has elapsed, the device sends the next ping. If the first WAN-IP address cannot be reached, the device sends a further ping after a waiting time has elapsed (10 s). In total three pings are sent to the WAN-IP address. If the device does not receive a reply after the third ping, the second WAN-IP address is checked. If this WAN-IP addresses is also unreachable, the next WAN-IP address is checked.

Is none of the three WAN-IP addresses is reachable, the device restarts the mobile network interface and logs the restart with the following message "Detected a problem with the provider connection. Trying to reconnect to the provider. Attempt no.: x".

The x stands for the number of attempts. In total the device makes 10 attempts. After restarting the mobile network interface, the device waits for some time and then sends a ping to the first WAN-IP address. Following the first restart of the mobile network interface the wait time is 2 minutes. With each further restart of the mobile network interface the wait time is extended by one minute.

If the 10 attempts are unsuccessful, the device restarts and logs the restart with the following message: "Detected a problem with the provider connection. Reconnect to the provider had no effect. Device will restart now."

Note

Always configure several WAN-IP addresses. If you only configure one WAN-IP address, the sporadic failure of the single WAN-IP address can lead to the WAN connection being constantly re-established.

The screenshot shows the 'Connection Check' configuration page. At the top, there are tabs: 'General', 'SIM', 'Operator', and 'Connection Check'. The 'Connection Check' tab is selected. Below the tabs, there is a checkbox labeled 'Enable Connection Ping' which is currently unchecked. Below this, there is a text field for 'Ping Time Interval [s]' with the value '600'. Below that, there is a text field for 'Ping Target Address:'. Below this field, there is a table with two columns: 'Select' and 'Target Address'. The table contains one entry with a checkbox in the 'Select' column and the IP address '192.168.16.1' in the 'Target Address' column. Below the table, it says '1 entry.' At the bottom of the page, there are four buttons: 'Create', 'Delete', 'Set Values', and 'Refresh'.

Select	Target Address
☐	192.168.16.1

Description

The page contains the following:

- **Enable Connection Ping**
Enable or disable the function. Can only be enabled if at least one IP address is configured.

Note

In a public network, the function is not secure. Please note that ping packets can be faked.

- **Ping Time Interval [s]**
Specify the interval at which the pings are sent.
- **Ping Target Address**
Enter the WAN-IP address that will be used for the connection monitoring. Click "Create" to save an entry to the table

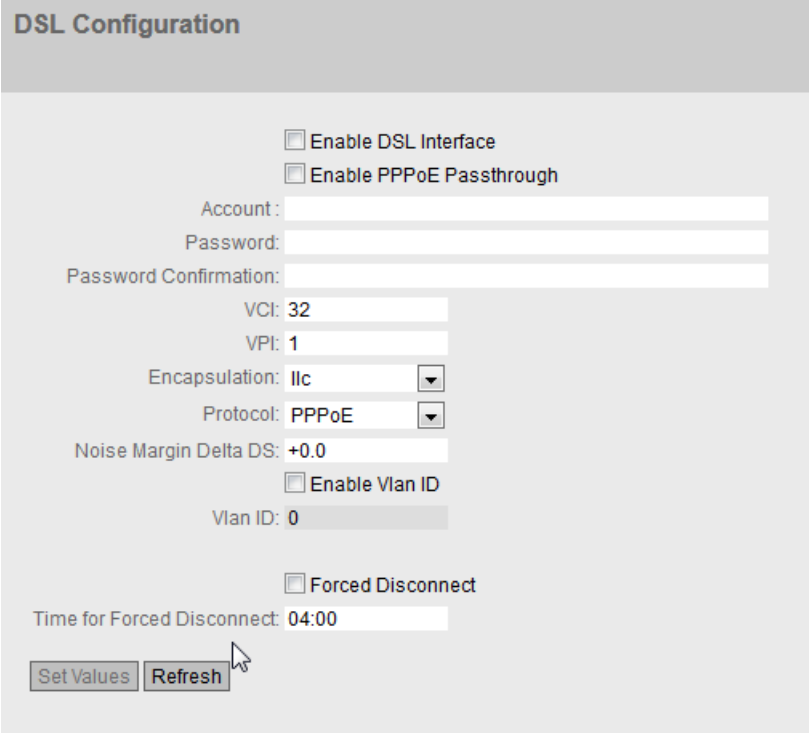
The table contains the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Target Address**
Shows the WAN-IP address.

5.7.3 DSL

M81x

On this WBM page, you configure the DSL access and the parameters for the virtual connection via which the packets will be transferred.

A screenshot of the 'DSL Configuration' web interface. The page has a grey header with the title 'DSL Configuration'. Below the header, there are several configuration options. At the top, there are two checkboxes: 'Enable DSL Interface' and 'Enable PPPoE Passthrough'. Below these are three text input fields: 'Account:', 'Password:', and 'Password Confirmation:'. Following these are three more text input fields: 'VCI: 32', 'VPI: 1', and 'Encapsulation: llc' (with a dropdown arrow). Below these are two more text input fields: 'Protocol: PPPoE' (with a dropdown arrow) and 'Noise Margin Delta DS: +0.0'. Below these are two checkboxes: 'Enable Vlan ID' and 'Vlan ID: 0'. Below these are two checkboxes: 'Forced Disconnect' and 'Time for Forced Disconnect: 04:00'. At the bottom, there are two buttons: 'Set Values' and 'Refresh'. A mouse cursor is pointing at the 'Refresh' button.

Description

The page contains the following:

- **Enable DSL Interface**
Enable or disable the DSL interface.
- **Enable PPPoE Passthrough**
 - Enabled
The device acts as a modem. The settings "Account", "Password" and "Enable Force Disconnect" cannot be edited. Only a connected device can use the DSL connection. This device also handles the authentication (dial-in) with the provider.
 - Disabled
The device acts as a router and logs in with the user name and password. All connected devices can use the DSL connection.
- **Account**
Enter the user name. You will receive the user name from your DSL provider.
- **Password**
Enter the password. You will receive the password name from your DSL provider.
- **Password Confirmation**
Repeat the password.
- **VCI (Virtual Channel Identifier)**
Enter the ID for the virtual channel. You will receive setting from your DSL provider.

- **VPI (Virtual Path Identifier)**
Enter the ID for the virtual path. You will receive setting from your DSL provider.
- **Encapsulation**
The data packets are encapsulated in the required protocol.
The following options are available:
 - vc-mux (virtual circuit multiplexing)
 - LLC (Logical Link Control)
- **Protocol**
Specify the protocol for the Internet connection. You obtain this information from your DSL provider.
 - PPPoE (Point-to-Point over Ethernet)
The PPP data is encapsulated in an Ethernet frame.
 - PPPoA (Point-to-Point over ATM)
The PPP data is encapsulated in ATM AAL5 (Adaptation Layer 5). If you select PPPoA, the setting "Enable PPPoE Passthrough" is disabled.
- **Noise Margin Delta DS:**
Specify the margin to the background noise.
Range of values -5dB ... +5dB
- **Enable Vlan ID**
When enabled, you can configure a VLAN ID. Only necessary when specification of a VLAN ID is required for the DSL access.
- **VLAN ID**
Enter the VLAN ID for the DSL access. You will receive setting from your DSL provider.
- **Forced Disconnect**
After a certain time, the DSL provider terminates the connection. Enable this option if you want to shift the forced disconnect of your provider to a specific time of day, for example at night outside normal office hours.
- **Time for Forced Disconnect**
Specify the time of day to which you want to shift the forced disconnect of the DSL provider. This is only possible if the correct system time is set on the device.
Input format: HH:MM

5.7.4 SHDSL

5.7.4.1 Overview

M826

The WBM page shows the configuration of the SHDSL interfaces.

SHDSL Overview

Overview | **Configuration** | **Connection Check**

☐ Enable PME Aggregation Function

Interface	Status	Role	Target SNR	Port Type
SHDSL 1	enabled	Central Office (CO)	Reliability (10 dB)	Switch-Port VLAN Hybrid
SHDSL 2	enabled	Central Office (CO)	Reliability (10 dB)	Switch-Port VLAN Hybrid

Description

The page contains the following:

- **Enable PME Aggregation Function**

PME = Physical Medium Entities

When enabled, the SHDSL interfaces or the 2-wire cables are put together to form a single connection with a higher transmission rate.

Note

If the "PME Aggregation" function is enabled, the interfaces of a device must each have the same role.

This table contains the following columns:

- **Interface**
Shows the available SHDSL interfaces.
- **Status**
Shows whether or not the interface is used.
- **Role**
Shows the role of the SHDSL interface:
 - Central Office (CO)
The interface is a central office.
 - Customer Premises Equipment (CPE)
The interface is an end node device.

- **Target SNR**
Shows the signal-to-noise ratio:
 - Reliability (10 dB)
Reliable transfer
 - Normal (6 dB)
Normal transfer
 - High-speed (0 dB)
High-speed transfer
- **Port Type**
Shows the operating mode of the switch port:
 - Switch-Port VLAN Hybrid
The port accepts tagged and untagged frames.
 - Switch-Port VLAN Trunk
The port only sends tagged frames and is automatically a member of all VLANs.

5.7.4.2 Configuration

M826

On this WBM page, you specify the settings for the connection and the role of the device. You will find additional information on the settings in ITU-T G.991.2.

SHDSL Configuration

Overview Configuration Connection Check

Interface: SHDSL 1

Status: enabled

Port Type: Switch-Port VLAN Hybrid

Role: Central Office (CO)

Predefined Profile: -

Extended Mode: Disabled

PAM: PAM-16 + PAM-32

Lineprobing: Enabled

SNR Model: Worst Case

Target SNR: Reliability (10 dB)

Min. Link Data Rate [kbps]: 192

Max. Link Data Rate [kbps]: 5696

Power Regulation: Normal

PBO Value: 0

Set Values Refresh

Description

The page contains the following:

- **Interface**
Select the interface.
- **Status**
Specify whether or not the interface will be used.
- **Port Type**
Specify the operating mode for the switch port.
 - Switch-Port VLAN Hybrid
The port accepts tagged and untagged frames.
 - Switch-Port VLAN Trunk
The port only sends tagged frames and is automatically a member of all VLANs.
- **Role**
Specify the role:
 - Central Office (CO)
The interface is a central office.
 - Customer Premises Equipment (CPE)
The interface is an end node device.

- **Predefined Profile**

Specify the profile for the transfer. If you use a profile, the following parameters are set automatically.

- Profiles with a transfer range
If during calibration of the cable the measured value is within the range, the SHDSL connection is established.

	Link data rate min - max	
Standard	192 - 5696	For medium and longer cable lengths
Reliability	192 - 5696	When operating several SHDSL connections simultaneously.
Extended	64 - 15296	For short and long cable length

- Profiles with a fixed preset transmission rate
If during calibration of the cable the measured value precisely matches the fixed preset transmission rate, and SHDSL connection is established.

	Link Data Rate
Fixed (high data rate)	5696
Fixed (medium data rate)	3072
Fixed (low data rate)	512

- **Extended Mode**

Enable or disable the extended mode. Depending on the setting, the selection in the following boxes changes.

- **PAM**

Pulse Amplitude Modulation

Specify the modulation method.

- **Line probing**

When enabled, the cable is calibrated according to ITU-T G.991.2.

- **SNR Model**

Specify the model for calculating the signal-to-noise ratio.

- Current condition
The value for noise is used that was measured when calibrating the cable.
- Worst Case
The value for noise is assumed that could occur over several cables of a cable bundle.

- **Target SNR**

Specify the transmission mode for the signal-to-noise ratio. The current signal-to-noise ratio is displayed under "Information > SHDSL".

- Reliability (10 dB)
Reliable transfer
- Normal (6 dB)
Normal transfer
- High-speed (0 dB)
High-speed transfer

- **Min. Link Data Rate [kbps]**
Specify the minimum transmission rate for sending and receiving data.
 - Auto (0)
The device adapts the transmission rate automatically depending on the mode.
 - 192 to 5696
The transmission rate is specified as a fixed value.
- **Max. Link Data Rate [kbps]**
Specify the maximum transmission rate for sending and receiving data.
 - Auto (0)
The device adapts the transmission rate automatically depending on the mode.
 - 192 to 5696
The transmission rate is specified as a fixed value.
- **Power Regulation**
Specify whether or not the transmit power is reduced.
 - Disabled
The function is disabled
 - Normal
The function is enabled.
 - Force
For PBO Value, enter the value for the attenuation.
- **PBO Value**
Power Back Off Values
Enter the value for the attenuation. An SHDSL connection is only established when the value is reached.
 - Range: 0 - 31 dB, where "0" means no attenuation.

5.7.4.3 Connection Check

M826

Use this function to ensure that the connection to the SHDSL network is retained. On this page you specify which WAN-IP addresses are used as reference for the connection monitoring.

The device sends echo messages (pings) to the configured WAN IP addresses of the remote stations at regular intervals (Ping Time Interval).

If, for example, you configure three WAN-IP addresses, the device sends a ping to the WAN-IP addresses. If only one of the three WAN-IP addresses is unreachable the following message is logged: "Could not reach remote device a.b.c.d (Failure count x)".

"a.b.c.d" stands for the IP address of the device and x stands for the number of attempts. In total the device makes 5 attempts.

If the IP address becomes reachable again, this is logged with the following message: SHDSL connection check: Remote devices are reachable again.

If the 5 attempts are unsuccessful, the device restarts and logs the restart with the following message: "SHDSL connection check: Maximum failure count reached, restarting device."

Connection Check

Overview

Configuration

Connection Check

☐ Enable Connection Ping

 Ping Time Interval [s]: 60

 Ping Target Address:

Select	Target Address
☐	192.168.16.42

 1 entry.

Create

Delete

Set Values

Refresh

Description

The page contains the following:

- Enable Connection Ping**
 Enable or disable the function. Can only be enabled if at least one IP address is configured.
- Ping Time Interval [s]**
 Specify the interval at which the pings are sent.
- Ping Target Address**
 Enter the WAN-IP address that will be used for the connection monitoring.. Click "Create" to create an entry in the table.

This table contains the following columns:

- Select**
 Select the check box in the row to be deleted.
- Target Address**
 Shows the WAN-IP address.

5.7.5 Packet Capture

MUx85x

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

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

Packet Capture

Interface	Enable
P1	☐
vlan1	☐
usb0	☐

☐ Activate after System Restart

Port: 2002

Set Values

Refresh

Description

The table contains the following columns:

- Interface**
The interface to which the entry relates.
 - Px: Ethernet interface
P1: With SCALANCE MUM856-1
P1 ... P4: With SCALANCE MUM853-1
 - vlanX: Addressed VLAN. VLANs with configured IP subnet are available.
 - usb0: WAN interface
 - SINEMA RC: Interface to the SINEMA RC Server. Only available with KEY-PLUG SINEMA RC.
- Enable**
Enable or disable the "Packet Capture" function. As default, the function is disabled.

Note

Performance

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

The page contains the following boxes:

- **Activate after System Restart**
 - Disabled
After a restart, the configuration is reset to the default setting.
 - Enabled
The configuration is saved and retained after a restart.
- **Port**
You can change the port if necessary. Default port: 2002

Linking in the interface in Wireshark

Requirement:

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

Procedure

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

1. Enable the function "Packet Capture" on the device on the vlan1 interface.
2. Click "Set Values" to enable the function.
3. Enable access to Capture on the relevant input interface in the menu "Security > Firewall > Predefined rules".
4. Start Wireshark.
5. Click "Options" in the "Capture" menu. The window "Wireshark - Capture Interfaces" opens.
6. Click the "Manage Interfaces..." button on the "Input" tab. In the following dialog, click on the "Remote Interfaces" tab.
7. To add the interface click on the Plus character in the "Remote Interfaces" tab.
8. In the following dialog, enter the IPv4 address for "Host" and 2002 for "Port".
9. Enable "Null authentication" for "Authentication" and click the "OK" button.
10. On the "Remote Interfaces" tab, the host and the interfaces on which the function "Packet Capture" was previously enabled are displayed.

5.8 "Layer 2" menu

11. Select the interface and click the "OK" button.

The remote interfaces displayed correspond to the following interfaces on the SCALANCE M device:

Remote interface in Wireshark	Interface on the SCALANCE device	Comment
eth0	P1	-
eth1	P2	Only with SCALANCE MUM853
eth2	P3	
eth3	P4	
vlanX	VLAN X	Range of values: 1 ... 4094
usb0	usb0	-

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

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

5.8 "Layer 2" menu

5.8.1 Layer 2 configuration

Configuring layer 2

On this page, you create a basic configuration for the functions of layer 2.



Description

- **Passive Listening**

When enabled the function ensures that the BPDUs from the RSTP network are forwarded transparently and return again. If this was not the case, loops would form at the connection point between RSTP and the ring.

5.8.2 VLAN

5.8.2.1 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.

The possible settings on this page depend on what you select in the "Base Bridge Mode" box.

Note

Changing the Agent VLAN ID

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

Virtual Local Area Network (VLAN) General

General

Port Based VLAN

Base Bridge Mode: 802.1Q VLAN Bridge

VLAN ID:

Select	VLAN ID	Name	Status	P1	P2	P3	P4
☐	1		Static	U	U	U	U
☐	2		Static	-	-	-	-

2 entries.

Create

Delete

Set Values

Refresh

Description

The page contains the following boxes:

- **Base Bridge Mode**

Note

Changing Base bridge mode

Note the section "Changing Base bridge mode" in this chapter. This section describes how a change affects the existing configuration.

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

- 802.1Q VLAN Bridge
Sets the mode "VLAN-aware" for the device. In this mode, VLAN information is taken into account.
- 802.1D Transparent Bridge
Sets the mode "VLAN-unaware" for the device. In this mode, VLAN tags are not 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 row you want to delete.
- **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.
- **Name**
Enter a name for the VLAN. The name only provides information and has no effect on the configuration. The length is a maximum of 32 characters.

- **Status**
Shows the status type of the entry in the internal port filter table. Here, "Static" means that the VLAN was entered statically 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 and cannot become a member of this VLAN even if it is configured as a trunk port.
 - T
This option is only displayed and cannot be selected in the WBM.
This port is a trunk port making it a member in all VLANs.
You configure this function in the CLI (Command Line Interface) using the "switchport mode trunk" command or in the WBM under "Interfaces > Ethernet > Configuration".

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.
- You will find the factory assignment of the ports in the section "VLAN (Page 73)".
- The VLANs are in different IP subnets. To allow these to communicate with each other, the route and firewall rule must be configured on the device.
- 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:

For 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.

5.8.2.2 Port Based VLAN

Processing received frames

On this WBM page, you specify the configuration of the port properties for receiving frames.

Port Based Virtual Local Area Network (VLAN) Configuration

General

Port Based VLAN

	Priority	Port VID	Acceptable Frames	Ingress Filtering	Copy to Table
All ports	No Change	No Change	No Change	No Change	Copy to Table

Port	Priority	Port VID	Acceptable Frames	Ingress Filtering
P1	0	VLAN1	All	☒
P2	0	VLAN1	All	☒
P3	0	VLAN1	All	☒
P4	0	VLAN1	All	☒

Set Values

Refresh

Description

Table 1 has the following columns:

- All ports**
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.
- Priority**
Select the required priority assigned to untagged frames.
The CoS priority (Class of Service) used in the VLAN tag. If a frame is received without a tag, it will be assigned this priority. This priority specifies how the frame is further processed compared with other frames.
There are a total of eight priorities with values 0 to 7, where 7 represents the highest priority (IEEE 802.1p Port Priority).
- Port VID**
Select the required VLAN ID. Only VLAN IDs defined in "VLAN > General" 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.
- Untagged and Priority Tagged Only
The device discards all tagged frames. The device forwards all untagged frames as well as frames with VLAN = 0 and a priority (Priority Tagged Frames). Otherwise, the forwarding rules apply according to the configuration.
- All
The device forwards all frames.

- **Ingress Filtering**

Specify whether the VID of received frames is evaluated.

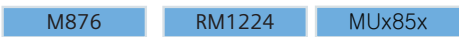
You have the following options:

- 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.

Steps in configuration

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

5.8.3 VXLAN

M876

RM1224

MUx85x

5.8.3.1 VXLAN

On this page, you define VXLANs (Virtual eXtensible LAN). VXLAN is a virtual network technology for extending VLAN and allows the transmission of Layer 2 packets via Layer 3 networks.

The maximum size of a packet (MTU) for VXLAN is 1500 bytes. Larger packets are fragmented.

Virtual Extensible VLAN (VXLAN)

VXLAN

VTEP

VLAN Mapping

Ingress Replication

Static MAC

☒ VXLAN

UDP Port: 4789

Network Virtualization Endpoint Interfaces

NVE ID:

Select	NVE Interface
☐	nve10100
☐	nve22

2 entries.

Create

Delete

Set Values

Refresh

Description

The page contains the following boxes:

- VXLAN**
 Enables the VXLAN function.
- UDP port**
 Enter the destination port of the VXLAN.
 Range of values: 1000 ... 65535
 UDP port 4789 is assigned by default.
- Network Virtual Endpoint interfaces (NVE)**
 In this area, you configure the virtual interface via which the VXLAN tunnel is established.
 - NVE ID**
 Enter a number for the NVE interface. You can create up to 5 NVE interfaces.
 Range of values: 1 ... 65535
- The table contains the following columns.
 - Select**
 Select the row you want to delete.
 - NVE Interface**
 Shows the NVE interface. The label is automatically composed of "nve" and the entered number.

Procedure

Creating a new VXLAN

1. Select the "VXLAN" check box.
2. Enter the "UDP Port" and the "NVE ID".
3. Click the "Create" button.

5.8.3.2 VTEP

On this page, you make settings relating to the VTEPs (VXLAN Tunnel End Points). The VTEPS form the endpoints in the VXLAN over which the connection runs. In the "Static MAC" tab, you set end devices that are to be reachable via a VTEP in the destination network.

VXLAN Tunnel End Points (VTEP)

VXLAN

VTEP

VLAN Mapping

Ingress Replication

Static MAC

NVE Interface:

nve10100

VTEP Source IP Address:

Select	NVE Interface	VTEP Source IP Address
☐	nve10100	192.168.1.1
☐	nve22	192.168.1.1

2 entries.

Create

Delete

Refresh

Description

The page contains the following boxes:

- NVE Interface**
Select the required NVE interface. Only the interfaces that you created in the "VXLAN" tab can be selected.
- VTEP Source IP Address**
Enter the IPv4 address of the source VTEP. The requirement is that the IPv4 address is created on the device. You configure the IPv4 address under "Layer 3 > Subnets".

The table has the following columns:

- Select**
Select the row you want to delete.
- NVE Interface**
Shows the NVE interface. The ID of the NVE interface can only be assigned once when you create 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.
- VTEP Source IP Address**
Shows the IPv4 address of the source VTEP.

Procedure

Creating the source IP address

- Select the NVE interface.
- Enter the corresponding VTEP source IP address.
- Click the "Create" button.

5.8.3.3 VLAN mapping

To ensure that the VTEP forwards the Ethernet frame into the right VLAN or VXLAN, you need to configure an assignment of VLAN ID to VNI.

VLAN to VXLAN Network Identifier (VNI) Mapping

VXLAN

VTEP

VLAN Mapping

Ingress Replication

Static MAC

VLAN ID:

VLAN1

VNI ID:

Select	VLAN ID	VNI ID
☐	1	10100
☐	101	22

2 entries.

Create

Delete

Refresh

Description

The page contains the following boxes:

- VLAN ID**
 Select the required VLAN ID. Only VLANs with a configured subnet can be selected.
- VNI**
 Enter the VNI that will be assigned to the VLAN ID. The VNI can be assigned to multiple VLAN IDs.

The table has the following columns:

- Select**
 Select the row you want to delete.
- VLAN ID**
 Shows the VLAN ID.
- VNI**
 Shows the VNI assigned to the VLAN.

Procedure

Creating an assignment

- Select the required VLAN ID.
- Enter the VNI ID that will be assigned to the VLAN ID.
- Click the "Create" button.

5.8.3.4 Ingress Replication

If there are multiple VTEPs in a VNI segment, the source VTEP does not know which remote VTEP the receiver of the Ethernet frame is behind.

On this page, you enter the remote VTEP IP addresses to which Ethernet frames are sent. The source VTEP replicates the received Ethernet frame and sends the encapsulated Ethernet frame to the remote VTEPs.

VXLAN Ingress Replication

VXLAN

VTEP

VLAN Mapping

Ingress Replication

Static MAC

NVE Interface:

nve10100

VNI ID:

Select	NVE Interface	VNI ID	Remote VTEP IP Address
☐	nve10100	22	192.51.100.33

1 entry.

Create

Delete

Set Values

Refresh

Description

The page contains the following boxes:

- NVE Interface**
Select the required NVE interface.
- VNI ID**
Enter the required VNI. Only VXLAN networks with the same VNI ID can communicate with one another.
Range of values: 1 ... 16777215

The table has the following columns:

- Select**
Select the row you want to delete.
- NVE Interface**
Shows the selected NVE interface.
- VNI ID**
Shows the VNI ID.
- Remote VTEP IP Address**
Requirement:
You need to enter an IP address for communication to work.
Enter the IPv4 address of the remote VTEP.
The replicated Ethernet frame is encapsulated and sent to this remote VTEP. The prerequisite is that the remote VTEP is a member of the VNI segment.

Procedure

1. Select the NVE interface.
2. Enter an ID in the "VNI ID" input box.

3. Click the "Create" button.
A new entry is generated in the table.
4. Enter the remote VTEP IP address.
5. Click the "Set Values" button.

5.8.3.5 Static MAC

On this page, you can enter the MAC addresses of devices in the destination network that should be reached over a remote VTEP. The entry is displayed under "Information > VXLAN".

VXLAN Static MAC

VXLAN

VTEP

VLAN Mapping

Ingress Replication

Static MAC

NVE Interface: nve10100

VNI ID:

Remote MAC Address:

Select	NVE Interface	VNI ID	Remote MAC Address	Remote VTEP IP Address
☐	nve10100	22	00-1b-1b-b6-32-7a	203.0.113.33

1 entry.

Create

Delete

Set Values

Refresh

Description

The page contains the following boxes:

- **NVE Interface**
Select the NVE interface via which the remote VTRP can be reached. Only the interfaces that you created in the "VXLAN" tab can be selected.
- **VNI ID**
Enter the VNI ID (VXLAN Network Identifier). Only VTEPs that are members of the same VXLAN segment can communicate with one another.
- **Remote MAC Address**
Enter the MAC address of the end device in the destination network to be reached via the VTEP entered in the table.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **NVE Interface**
Shows the NVE interface.
- **VNI**
Shows the VNI. The VNI can only be assigned once when you create 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.

- **Remote MAC Address**
Shows the MAC address of the end device in the destination network.
- **Remote VTEP IP Address**
Enter the IPv4 address of the VTEP via which the end device with the entered remote MAC address can be reached in the destination network.

Procedure

1. Select the NVE interface.
2. Enter an ID in the "VNI ID" input box.
3. Enter the remote MAC address.
4. Click the "Create" button.
A new entry is generated in the table.
5. Enter the remote VTEP IP address.
6. Click the "Set Values" button.

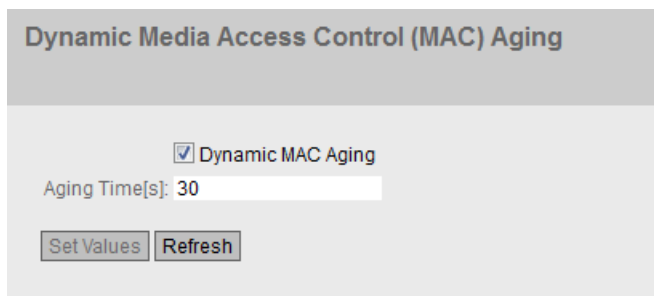
5.8.4 Dynamic MAC Aging

Protocol settings and switch functionality

The device automatically learns the source addresses of the connected nodes. This information is used to forward data frames to the nodes specifically involved. This reduces the network load for the other nodes.

If a device does not receive a frame whose source address matches a learnt address within a certain time, it deletes the learnt address. This mechanism is known as "Aging". Aging prevents frames being forwarded incorrectly, for example when an end device is connected to a different port.

If the check box is not enabled, a device does not delete learned addresses automatically.



The screenshot shows a web-based configuration interface for "Dynamic Media Access Control (MAC) Aging". It features a checkbox labeled "Dynamic MAC Aging" which is checked. Below the checkbox is a text input field labeled "Aging Time[s]:" with the value "30" entered. At the bottom of the form are two buttons: "Set Values" and "Refresh".

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 in steps of 15. After this time, a learned address is deleted if the device does not receive any further frames from this sender address.
Range of values: 15 ... 630

Note

Rounding of the values, deviation from desired value

When you input the Aging Time, note that it is rounded to correct values. If you enter a value that cannot be divided by 15, the value is automatically rounded down.

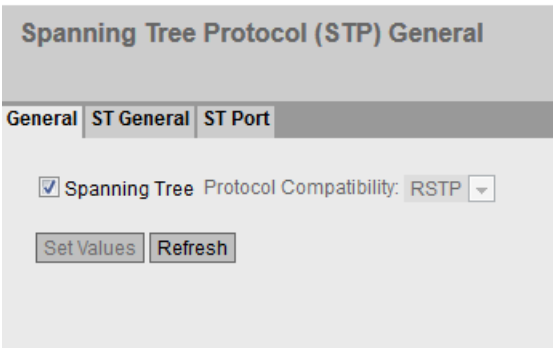
Steps in configuration

1. Select the "Dynamic MAC Aging" check box.
2. Enter the time in seconds in the "Aging Time[s]" input box.
3. Click the "Set Values" button.

5.8.5 Spanning Tree

5.8.5.1 General

This is the basic page for spanning tree. As default, Rapid Spanning Tree is enabled.



Description

The page contains the following boxes:

- **Spanning Tree**
Enable or disable spanning tree.
- **Protocol Compatibility**
The following setting is available:
 - RSTP

Procedure

1. Select the "Spanning Tree" check box.
2. Click the "Set Values" button.

5.8.5.2 ST general

The page consists of the following parts.

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

Spanning Tree (ST) General		
General	ST General	ST Port
Bridge Priority:	8192	Root Priority: 8192
Bridge Address:	00-1b-1b-9a-32-2e	Root Address: 00-1b-1b-9a-32-2e
Root Port:	-	Root Cost: 0
Topology Changes:	458	Last Topology Change: 7hr
Bridge Hello Time[s]:	2	Root Hello Time[s]: 2
Bridge Forward Delay[s]:	15	Root Forward Delay[s]: 15
Bridge Max Age[s]:	20	Root Max Age[s]: 20
<button>Reset Counters</button>		
<button>Set Values</button> <button>Refresh</button>		

Description

The page contains the following boxes:

- **Bridge Priority / Root Priority**
Which device becomes the root bridge is decided by 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. Range of values: 0 - 61440
- **Bridge Address / Root Address**
The bridge address shows the MAC address of the device and the root address shows the MAC address of the root bridge.
- **Root port**
Shows the port 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: Unit "sec" after the number
 - Minutes: Unit min after the number
 - Hours: Unit hr after the number
- **Bridge hello time [s] / Root hello time [s]**
Each bridge sends configuration frames (BPDUs) regularly. The interval between two configuration frames is the "Hello Time".
Factory setting: 2 seconds
- **Bridge Forward Delay[s] / Root Forward Delay[s]**
New configuration data is not used immediately by a bridge but only after the period specified in the Forward Delay parameter. This ensures that operation is only started with the new topology after all the bridges have the required information.
Factory setting: 15 seconds
- **Bridge Max Age[s] / Root Max Age[s]**
If the BPDU is older than the specified "Max Age" it is discarded.
Factory setting: 20 seconds
- **Reset Counters**
Click this button to reset the counters on this page.

5.8.5.3 ST port

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.

5.8 "Layer 2" menu

Spanning Tree (ST) Port

General | ST General | ST Port

Spanning Tree Status

Copy to Table

All ports No Change ▼ Copy to Table

Port	Spanning Tree Status	Priority	Cost Calc.	Path Cost	State	Fwd. Trans.	Edge Type	Edge	Pt.P. Type	Pt.P.
P1	☒	144	0	200000	Forwarding	1	Auto ▼	☐	- ▼	☒
P2	☐	128	0	2000000	Discarding	0	Auto ▼	☐	- ▼	☒
P3	☐	128	0	2000000	Discarding	0	Auto ▼	☐	- ▼	☒
P4	☐	128	0	2000000	Discarding	0	Auto ▼	☐	- ▼	☒
SHDSL 1	☒	144	0	3511236	Discarding	355	Auto ▼	☐	- ▼	☒
SHDSL 2	☒	144	0	3511236	Discarding	356	Auto ▼	☐	- ▼	☒

Set Values

Refresh

Description

Table 1 has the following columns:

- **All ports**
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 setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
Shows the available ports.
- **Spanning Tree Status**
Specify whether or not the port is integrated in the spanning tree.

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 costs" box.
- **Path Cost**
This parameter is used to calculate the path that will be selected. The path with the lowest value is selected as the path. If several ports of a device have the same value for the path costs, the port with the lowest port number is selected.
If the value in the box "Cost Calc." 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 = 2,000,000The values can, however, also be set individually.
- **Status**
Displays the current status of the port. The values are only displayed and cannot be configured. The "Status" parameter depends on the configured protocol. The following values are possible:
 - Disabled
The port only receives and is not involved in STP, MSTP and RSTP.
 - Discarding
In the "Discarding" mode, BPDU frames are received. Other incoming or outgoing frames are discarded.
 - Listening

In this status, BPDUs are both received and sent. The port is involved in the spanning tree algorithm.
 - Learning
Stage prior to the "Forwarding" status, the port is actively learning the topology (in other words, the node addresses).
 - 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 Edge Port".
- Admin
Select this option when there is always an end device on this port. Otherwise a reconfiguration of the network will be triggered each time a connection is changed.
- Auto
Select this option if you want a connected end device to be detected automatically at this port. When the connection is established the first time, the port is treated as a "no Edge Port".
- Admin/Auto
Select these options if you operate a combination of both on this port. When the connection is established the first time, the port is treated as an "Edge Port".

- **Edge**

Shows the status of the port.

- Enabled

An end device is connected to this port.
- Disabled
There is a Spanning Tree or Rapid Spanning Tree device at this port.

With an end device, a switch can change over the port faster without taking into account spanning tree frames. If a spanning tree frame is received despite this setting, the port automatically changes to the "Disabled" setting.

- **P.t.P. Type**

Select the required option from the drop-down list. The selection depends on the port that is set.

- "-"
Point to point is calculated automatically. If the port is set to half duplex, a point-to-point link is not assumed.
- P.t.P.

Also 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.

5.8.6 LLDP

Identifying the network topology

LLDP (Link Layer Discovery Protocol) is defined in the IEEE 802.1 AB standard.

LLDP is a method used to discover the network topology. Network components exchange information with their neighbor devices using LLDP.

Network components that support LLDP have an LLDP agent. The LLDP agent sends information about itself and receives information from connected devices at periodic intervals. The received information is stored in the MIB.

Applications

PROFINET uses LLDP for topology diagnostics. In the factory setting, LLDP is enabled for all available ports; in other words, LLDP frames are sent on the ports.

The information sent is stored on every device with LLDP capability in an LLDP MIB file. Network management systems can access these LLDP MIB files using SNMP and therefore recreate the existing network topology. In this way, an administrator can find out which network components are connected to each other and can localize disruptions.

On this page, you have the option of enabling or disabling sending and/or receiving per port.

Link Layer Discovery Protocol (LLDP)

	Setting	Copy to Table
All ports	No Change	Copy to Table

Port	Setting
P1	Rx & Tx
P2	Rx & Tx
P3	Rx & Tx
P4	Rx & Tx
P5	Rx & Tx

Set Values Refresh

Description

Table 1 has the following columns:

Table 1 is only available when the device has more than one port.

- **All Ports**
Shows that the settings are valid for all ports.
- **Setting**
Select the setting from the drop-down list. If "No Change" is selected, the entry in table 2 remains unchanged.
- **Copy to Table**
If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
Shows the available ports.
- **Setting**
Specify the LLDP functionality. The following options are available:
 - Rx
This port can only receive LLDP frames.
 - Tx
This port can only send LLDP frames.
 - Rx & Tx
This port can receive and send LLDP frames.
 - "-" (disabled)
This port can neither receive nor send LLDP frames.

Procedure

1. Select the LLDP functionality of the port from the "Setting" drop-down list.
2. Click the "Set Values" button.

5.9 Menu "Layer 3 (IPv4)"

5.9.1 Static routes

On this page, you specify the routes via which data exchange can take place between the various subnets. Dynamic routing protocols are not supported, for example RIP, OSPF.

Static Routes

Destination Network:

Subnet Mask:

Gateway:

Interface: auto

Administrative Distance: -1

Select	Destination Network	Subnet Mask	Gateway	Interface	Administrative Distance	Status
☐	0.0.0.0	0.0.0.0	192.168.40.2	vlan2	not used	active

1 entry.

Create

Delete

Set Values

Refresh

Description

The page contains the following boxes:

- Destination Network**
Enter the network address of the destination that can be reached via this route.
- Subnet Mask**
Enter the corresponding subnet mask.
- Gateway**
Enter the IPv4 address of the gateway via which this network address is reachable.
- Interface**
Specify whether the network address can be reached via a certain interface or via the gateway (auto).
- Administrative Distance**
Enter the metric for the route. The metric corresponds to the quality of a connection, for example speed, costs. If there are several equal routes, the route with the lowest metric value is used.
If you do not enter anything, "not used" is entered automatically. The metric can be changed later.
Range of values: 1 - 255 or -1 for "not used".
Here, 1 is the value for the best possible route. The higher value, the longer packets require to their destination.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Destination Network**
Shows the network address of the destination.
- **Subnet Mask**
Shows the corresponding subnet mask.
- **Gateway**
Shows the IPv4 address of the next gateway.
- **Interface**
Shows the interface of the route.
- **Administrative Distance**
Enter the metric for the route. When creating the route, "not used" is entered automatically. The metric corresponds to the quality of a connection, based for example on speed or costs. If there are several equal routes, the route with the lowest metric value is used.
Range of values: 1 - 255
Here, 1 is the value for the best possible route. The higher value, the longer the packets require to their destination.
- **Status**
Shows whether or not the route is active.

Procedure

1. Enter the network address of the destination in the "Destination Network" input box.
2. Enter the corresponding subnet mask in the "Subnet Mask" input box.
3. For "Interface", select the entry "auto".
4. Enter the gateway in the "Gateway" input box.
5. Enter the weighting of the route in "Administrative Distance".
6. Click the "Create" button. A new entry is generated in the table.
7. Click the "Set Values" button.

5.9.2 Subnets

5.9.2.1 Overview

The page shows the subnets for the selected interface. A subnet always relates to an interface and is created in the "Configuration" tab.

Connected Subnets Overview

Overview

Configuration

Interface:

Interface	TIA Interface	Status	Interface Name	MAC Address	IP Address	Subnet Mask	Address Type	IP Assgn. Method	Address Collision Detection Status	MTU
vlan1	yes	enabled	INT	00-1b-1b-cd-f2-17	192.168.1.1	255.255.255.0	Primary	Static	Active	1500
ppp0	-	disabled	ppp0	00-00-00-00-00-00	0.0.0.0	0.0.0.0	Primary	Dynamic (DHCP)	Not supported	1500

2 entries.

Create

Delete

Refresh

Description

The page contains the following box:

- **Interface**
Select the interface on which you want to configure another subnet.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Interface**
Shows the interface.
- **TIA Interface**
Shows whether the interface is a TIA interface.
- **Status**
Shows whether or not the interface is enabled.
- **Interface Name**
Shows the name of the interface.
- **MAC Address**
Shows the MAC address.
- **IP Address**
Shows the IPv4 address of the subnet.
- **Subnet Mask**
Shows the subnet mask.

- **Address Type**

Shows the address type. The following values are possible:

- Primary
The first IPv4 address that was configured on the IPv4 interface.
- Secondary
All other IPv4 addresses that were configured on the IPv4 interface.

- **IP Assignment Method**

Shows how the IPv4 address is assigned. The following values are possible:

- Static
The IPv4 address is static. You enter the settings in "IP Address" and "Subnet Mask".
- Dynamic (DHCP)
The device obtains a dynamic IPv4 address from a DHCPv4 server.

- **Address Collision Detection Status**

If new IPv4 addresses become active in the network, the "Address Collision Detection" function checks whether this can result in address collisions. The allows IPv4 addresses that would be assigned twice to be detected.

Note

The function does not run a cyclic check.

This column shows the current status of the function. The following values are possible:

- Idle
The interface is not enabled and does not have an IPv4 address.
- Starting
This status indicates the start-up phase. In this phase, the device initially sends a query as to whether the planned IPv4 address already exists. If the address is not yet been assigned, the device sends the message that it is using this IP address as of now.
- Conflict
The interface is not enabled. The interface is attempting to use an IPv4 address address that has already been assigned.
- Defending
The interface uses a unique IPv4 address. Another interface is attempting to use the same IPv4 address.
- Active
The interface uses a unique IPv4 address. There are no collisions.
- Not supported
The function for detection of address collisions is not supported.
- Disabled
The function for detection of address collisions is disabled.

- **MTU**

Shows the packet size.

5.9.2.2 Configuration

On this page, you configure the subnet for the interface.

Connected Subnets Configuration

Overview | **Configuration**

Interface (Name):

Status:

Interface Name:

MAC Address:

☐ DHCP

IP Address:

Subnet Mask:

Broadcast IP Address:

Address Type:

☒ TIA Interface

MTU:

Description

The page contains the following:

- **Interface (Name)**
Select the interface from the drop-down list.
- **Status**
Enable or disable the interface.
- **Interface Name**
Enter the name of the interface.
- **MAC Address**
Displays the MAC address of the selected interface.
- **DHCP**
When enabled, the interface obtains the IPv4 address from a DHCP server.
- **IP Address**
Enter the IPv4 address of the interface. The IPv4 addresses must not be used more than once.
- **Subnet Mask**
Enter the subnet mask of the subnet you are creating. Subnets on different interfaces must not overlap.
- **Broadcast IP Address**
If a specific IP address is to be used as the broadcast IP address of the subnet, enter this. Otherwise the last IP address of the subnet will be used.

- **Address Type**

Shows the address type. The following values are possible:

- Primary
The first subnet of the interface.
- Secondary
All further subnets of the interface.

- **TIA Interface**

Select whether this interface should become the TIA interface. The TIA interface defines on which VLAN the PROFINET functionalities are available. This mainly affects the device search with or via DCP.

- **MTU**

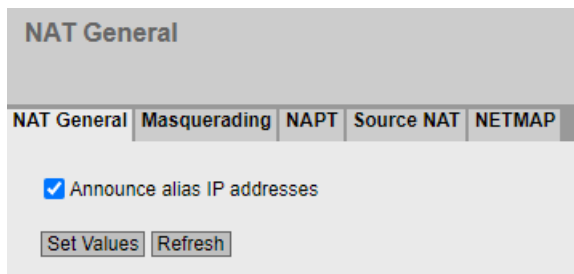
MTU (Maximum Transmission Unit) specifies the maximum size of the packet. If packets are longer than the set MTU, they are fragmented. The MTU covers the IP header and the headers of the higher layers.

The range of values is from 90 to 1500 bytes.

5.9.3 NAT

5.9.3.1 NAT General

On this WBM page, you enable Gratuitous ARP for alias IP addresses.



Description

On this page, you can enable the following option:

- **Announce alias IP addresses**

When the option is enabled, a Gratuitous ARP is sent for each alias IP address. This announces the IP address in the network, and the other devices can update their ARP cache. The Gratuitous ARP is only sent at the time of configuration, that is, during device startup or when an NAT rule (NETMAP) is being configured.

5.9.3.2 Masquerading

On this WBM page, you enable the rules for IP masquerading.

Internet Protocol (IP) Masquerading	
NAT General Masquerading NAPT Source NAT NETMAP	
Interface	Enable Masquerading
vlan1 (INT)	☐
usb0	☒

Set Values Refresh

Description

The table has the following columns:

- **Interface**
Interface to which the setting relates. Only interfaces with a configured subnet are available.
- **Enable Masquerading**
When enabled, with each outgoing data packet sent via this interface, the source IP address is replaced by the IP address of the interface.

5.9.3.3 NAPT

On this WBM page, you can configure a port translation in addition to the address translation.

The following port translations are possible:

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

IP Network Address Port Translation (NAPT) (Port Forwarding)

NAT GeneralMasqueradingNAPTSource NATNETMAP

Source Interface:usb0

Traffic Type:UDP

☒ Use Interface IP from Source Interface

Destination IP Address:

Destination Port:8080

Translated Destination IP Address:

Translated Destination Port:4500

Select	Source Interface	Traffic Type	Interface IP	Destination IP	Destination Port	Translated Destination IP	Translated Destination Port
☐	vlan1	UDP	☒	192.168.1.1	8080	192.168.1.12	4500
☐	vlan1	TCP	☐	10.10.0.100	4500	192.168.1.100	80

2 entries.

CreateDeleteRefresh

Description

The page contains the following boxes:

- Source Interface**
Select the interface on which the queries will arrive.
- Traffic Type**
Specify the protocol for which the address assignment is valid.
- Use Interface IP from Source Interface**
When enabled, the IP address of the selected interface is used for "Dest IP Address".
- Destination IP address**
Enter the destination IP address. The frames are received at this IP address. Can only be edited if "Use Interface IP from Source Interface" is disabled.
- Destination Port**
Enter the destination port. Incoming frames with this port as the destination port are forwarded. If the setting is intended to apply to a port range, enter the range with start port "-" end port, for example 30 - 40.
- Translated Destination IP**
Enter the IP address of the node to which this frame will be forwarded.
- Translated Destination Port**
Enter the number of the port. This is the new destination port to which the incoming frame will be forwarded. If the setting is intended to apply to a port range, enter the range with start port "-" end port, for example 30 - 40.

The table has the following columns:

- Select**
Select the check box in the row to be deleted.
- Source Interface**
Shows the interface from which the packets need to come. Only these packets are considered for port forwarding.
- Traffic Type**
Shows the protocol for which the address assignment applies.

- **Interface IP**
Shows whether the IP address of the interface is used.
- **Destination IP**
Shows the destination IP address. The frames are received at this IP address.
- **Destination Port**
Shows the destination port. Incoming frames with this port as the destination port are forwarded.
- **Translated Destination IP**
Shows the IP address of the node to which the packets will be forwarded.
- **Translated Destination Port**
Shows the destination port to which the packets are translated.

5.9.3.4 Source NAT

On this page, you configure the rules for source NAT.

IP Source Network Address Translation (SNAT)

Masquerading

NAPT

Source NAT

NETMAP

Source Interface:

vlan1 (INT)

Destination Interface:

vlan1 (INT)

Source IP Address(es):

☒ Use Interface IP from Destination Interface

Translated Source IP Address:

192.168.16.42

Destination IP Address(es):

Select	Source Interface	Destination Interface	Source IP Address(es)	Use Interface IP	Translated Source IP Address	Destination IP Address(es)
☐	vlan1	vlan2	192.168.1.50	☒	10.10.0.100	0.0.0.0
☐	vlan1	IPsec IPsec_to_M826	192.168.20.0	☐	192.168.200.0	192.168.100.0

2 entries.

Create

Delete

Refresh

Note

Firewall rule with source NAT

Address translation with source NAT was only performed after the firewall; the non-translated addresses are therefore used.

Security > Firewall > IP rules

- Source (Range): Input from "Source IP Addresses"
- Destination (Range): Input from "Destination IP Addresses"

Description

- **Source Interface / Destination Interface**

Specify the direction of the connection establishment. Only connections established in this specified direction are taken into account.

The virtual interfaces of VPN connections can also be selected:

- VLANx: VLANs with configured subnet
- pppx or usb0: WAN interface
- SINEMA RC: Connection to SINEMA RC Server
- IPsec: Either all IPsec VPN connections (all) or a specific IPsec VPN connection
- OpenVPN: Either all OpenVPN connections (all) or a specific OpenVPN connection

Note

When you configure a NAT address translation to or from the direction of the VPN tunnel, only the IP addresses involved in the NAT address translation rules can be reached via the VPN tunnel.

- **Source IP Address(es)**

Specify the source IP addresses for which this source NAT rule is valid. Only the packets that correspond to the addresses entered are taken into account.

The following entries are possible:

- IP address: Applies precisely to the specified IP address.
- IP address range: Applies to a certain IP address range: Start IP address "-" End IP address, e.g. 192.168.100.10 - 192.168.100.20
- IP subnet: Applies to several IPv4 addresses grouped together to form an IP address range: IP address/number of bits of the network part (CIDR notation)

- **Use Interface IP from Destination Interface**

When enabled, the IP address of the selected destination interface is used in "Translated Source IP Address".

- **Translated Source IP Address**

Enter the IP address with which the IP address of the sender is replaced. Can only be edited if "Use Interface IP from Destination Interface" is disabled.

- **Destination IP Address(es)**

Specify the destination IP addresses for which this source NAT rule is valid. Only the packets whose destination IP address is in the range of entered addresses are taken into account.

- IP address: Applies precisely to the specified IP address.
- IP address range: Applies to a certain IP address range: Start IP address "-" End IP address, e.g. 192.168.100.10 - 192.168.100.20
- IP subnet: Applies to several IPv4 addresses grouped together to form an IP address range: IP address/number of bits of the network part (CIDR notation)

The table has the following columns:

- Select
Activate the check box in the row to be deleted.
- Source Interface
Shows the source interface.
- Destination Interface
Shows the destination interface.
- Source IP Address(es)
Shows the IP addresses of the senders for which address translation is required.
- Use Interface IP
Shows whether the IP address of the selected destination interface is used in "Translated Source IP Address".
- Translated Source IP Address
Shows the IP address with which the IP address of the sender is replaced.
- Destination IP Address(es)
Shows the IP addresses of the recipients for which address translation is required.

See also

NAT and firewall (Page 89)

5.9.3.5 NETMAP

On this WBM page, you specify the rules for NETMAP. NETMAP is static 1:1 mapping of network addresses in which the host part is retained. For more information, refer to the section "NAT and firewall (Page 89)".

NETMAP

NAT General

Masquerading

NAPT

Source NAT

NETMAP

Type: Destination

Source Interface: IPsec (all)

Destination Interface: vlan1 (INT)

Source IP Subnet: 0.0.0.0/0

Translated Source IP Subnet:

Destination IP Subnet: 192.168.100.0/24

Translated Destination IP Subnet: 172.150.70.0/24

☐ Bidirectional Rule
 ☐ Auto Firewall Rule

Select	Type	Source Interface	Destination Interface	Source IP Subnet	Translated Source IP Subnet	Destination IP Subnet	Translated Destination IP Subnet	Alias IP	Comment
☐	Source	vlan1	usb0	172.150.70.0/24	192.168.100.0/24	0.0.0.0/0	-	☐	
☐	Destination	IPsec (all)	vlan1	0.0.0.0/0	-	192.168.100.0/24	172.150.70.0/24	☐	

2 entries.

Create

Delete

Set Values

Refresh

Note

Firewall rule with source NAT

Address translation with source NAT was only performed after the firewall; the non-translated addresses are therefore used.

Security > Firewall > IP rules

- Source (Range): Input from "Source IP Subnet"
- Destination (Range): Input from "Destination IP Subnet"

Firewall rule with destination NAT

Address translation with NAT was already performed before the firewall; the translated addresses are therefore used in the firewall.

Security > Firewall > IP rules

- Source (Range): Input from "Source IP Subnet"
 - Destination (Range): Input from "Translated Destination IP Subnet"
-

Description

- **Type**
Specify the type of address translation.
 - Source: Replacement of the source IP address
 - Destination: Replacement of the destination IP address
- **Source Interface**
Specify the source interface.
 - VLANx: VLANs with configured subnet
 - pppsx or usb0: WAN interface
 - SINEMA RC: Connection to the SINEMA RC server
 - IPsec: Either all IPsec VPN connections (all) or a specific IPsec VPN connection
 - OpenVPN: Either all OpenVPN connections (all) or a specific OpenVPN connection
- **Destination Interface**
Specify the destination interface.
 - VLANx: VLANs with configured subnet
 - pppx or usb0: WAN interface
 - SINEMA RC: Connection to the SINEMA RC server
 - IPsec: Either all IPsec VPN connections (all) or a specific IPsec VPN connection
 - OpenVPN: Either all OpenVPN connections (all) or a specific OpenVPN connection

- **Source IP Subnet**
Enter the subnet of the sender.
The subnet can also be a single PC or another subset of the subnet. Use the CIDR notation, for example, 192.168.10.10/32.
You can also specify the IP range with the start address "-" end address, e.g., 192.168.100.10 - 192.168.100.20.
For the entire IP range, enter "*".
- **Translated Source IP Subnet**
Enter the subnet with which the subnet of the sender will be replaced. Can only be edited in the "Source" settings.
The subnet can also be a single PC or another subset of the subnet. Use the CIDR notation, for example, 192.168.10.10/32.
You can also specify the IP range with the start address "-" end address, e.g., 192.168.100.10 - 192.168.100.20.
For the entire IP range, enter "*".
- **Destination IP Subnet**
Enter the subnet of the receiver.
The subnet can also be a single PC or another subset of the subnet. Use the CIDR notation, for example, 192.168.10.10/32.
You can also specify the IP range with the start address "-" end address, e.g., 192.168.100.10 - 192.168.100.20.
For the entire IP range, enter "*".
- **Translated Destination IP Subnet**
Enter the subnet with which the subnet of the receiver will be replaced. Can only be edited with the setting "Destination".
The subnet can also be a single PC or another subset of the subnet. Use the CIDR notation, for example, 192.168.10.10/32.
You can also specify the IP range with the start address "-" end address, e.g., 192.168.100.10 - 192.168.100.20.
For the entire IP range, enter "*".
- **Bidirectional rule**
When this is enabled, the NETMAP rule for the opposite direction is automatically created when the NETMAP rule is created.
The NETMAP rules are not connected to one another after creation. This means that no synchronization takes place between the NETMAP rules when they are changed or deleted.
- **Auto Firewall Rule**
When this is enabled, the corresponding firewall rule is automatically created when the NETMAP rule is created. These firewall rules are displayed under "Security > Firewall > IP rules". If you change or delete the NETMAP rules, the corresponding firewall rules are adjusted or deleted.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Type**
Shows the direction of the address translation.
- **Source Interface**
Shows the source interface.

- Destination Interface
Shows the destination interface.
- Source IP Subnet
Shows the subnet of the sender. This entry can be changed when necessary.
- Translated Source IP Subnet
Shows the subnet of the sender with which the subnet of the sender is replaced. This entry can be changed when necessary.
- Destination IP Subnet
Shows the subnet of the recipient. This entry can be changed when necessary.
- Translated Destination IP Subnet
Shows the subnet of the recipient with which the subnet of the recipient is replaced. This entry can be changed when necessary.
- Alias IP
When enabled, alias IP addresses are created for the translated address range. Enabled automatically when a /32 address is entered.
 - Source: For all IP addresses entered in the "Translated Source IP Subnet" field, alias IP addresses are created at the "Destination Interface".
 - Destination: For all IP addresses entered in the "Destination IP Subnet" field, alias IP addresses are created at the "Source Interface".

Note

Enabling in combination with network or address range

When you enable the option in combination with a network or address range, the alias IP addresses are reserved for the entire network or address range. This can lead to network problems.

- VRRP Interface / VRID
Selection is only possible when the "Alias IP" option is enabled.
Shows all configured routers of the type "VRRPv3" that are created in the "Layer 3 > VRRPv3 > Router" menu.
When you select a VRRP3 router, the Alias IP address associated with this NETMAP rule is only active when the VRRP3 router has the router status "Master".
- Comment
If needed, enter a comment.

5.9.4 VRRPv3

5.9.4.1 Router

Introduction

Using the "Create" button, you can create new virtual routers. A maximum of 2 virtual routers can be configured. You can configure other parameters on the "Configuration" tab.

Virtual Router Redundancy Protocol v3 (VRRPv3) Router

Router

Configuration

Addresses Overview

Addresses Configuration

Interface Tracking

☒ VRRPv3

☒ VRID-Tracking

Interface:

vlan1

VRID:

Select	Interface	VRID	Virtual MAC Address	Primary Address	Router State	Master Address	Priority	Advert. Interval	Preempt
☐	vlan3	1	00-00-5e-00-01-01	10.10.10.60	Master	10.10.10.60	100	100	yes

1 entry.

Create

Delete

Set Values

Refresh

Note

- You can use VRRPv3 on VLAN interfaces.

Requirement

For the incoming packets to be forwarded to the device, enable the predefined IPv4 rule "VRRP".

Description

The page contains the following:

- VRRPv3**
Enable or disable routing using VRRPv3.
- VRID-Tracking**
Enable or disable VRID tracking.
When enabled, all VRRP instances are monitored. If the status of a VRRP instance changes to "Initialize", the priority of all VRRP instances is reduced to the value "1".
If the status of a VRRP instance changes, the original priority of all VRRP instances is restored.
- Interface**
Select the required VLAN interface operating as virtual router.
- VRID**
Enter the ID of the virtual router. This ID defines the group of routers that form a virtual router (VR). In the group, this is the same. It can no longer be used for other groups.
Values 1...255 are valid.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Interface**
Shows the Interface that functions as the virtual router.
- **VRID**
Shows the ID of the virtual router.
- **Virtual MAC Address**
Shows the virtual MAC address of the virtual router.
- **Primary IP Address**
Shows the numerically lowest IPv4 address in this VLAN. The entry 0.0.0.0 means that the "Primary" address on this VLAN is used. Otherwise all IPv4 addresses configured on this VLAN in the "Layer 3 (IPv4) > Subnets" menu are valid values.
- **Router State**
Shows the current status of the virtual router. Possible values are:
 - Master
The router is the master router and handles the routing functionality for all assigned IPv4 addresses.
 - Backup
The router is the backup router. If the master router fails, the backup router takes over the tasks of the master router.
 - Initialize
The virtual router has just been turned on. It will soon change to the "Master" or "Backup" status.
- **Master IP Address**
Shows the IPv4 address of the master router.
- **Priority**
Shows the priority of the virtual router.
Valid values are 1-254.
If an IPv4 address is assigned to the VRRP router that is also actually configured on the local IPv4 interface, the value 255 is entered automatically. All other priorities can be distributed freely among the VRRP routers. The higher the priority, the earlier the VRRP router becomes "Master".
- **Advert. Interval**
Shows the interval at which the master router sends VRRPv3 packets.
- **Preempt**
Shows the precedence of a router when changing roles between backup and master.
 - yes
This router has precedence when changing roles.
 - no
This router does not have precedence when changing roles.

VRRP and DHCP server

If you want to operate a DHCP server on the devices of a VRRP group, the DHCP server must be configured on the master router. Backup routers do not react to DHCP queries. Make sure that the master router is statically configured and that after a failure, becomes the master of the VRRP group again.

Procedure

1. Select the "VRRPv3" check box.
2. Select the required interface.
3. Enter the ID of the virtual router in the "VRID" input box.
4. Click the "Create" button. A new row is inserted in the table.
5. Select the "Reply to pings on virtual interfaces" check box so that virtual IPv4 addresses reply to pings as well.
6. Select the "VRID Tracking" check box to monitor the VRID.
7. Click the "Set Values" button. To configure the virtual router, click on the "Configuration" tab.

5.9.4.2 Configuration

Introduction

On this page, you configure the virtual router.

Virtual Router Redundancy Protocol v3 (VRRPv3) Konfiguration

Router	Konfiguration	Adressübersicht	Adresskonfiguration	Schnittstellenüberwachung	Adressenüberwachung

Schnittstelle / VRID:

Primäre Adresse:

Priorität:

Advertisement-Intervall[cs]:

Track-ID:

Priorität verringern:

Aktuelle Priorität:

Description

The page contains the following:

- **Interface / VRID**
Select the ID of the virtual router to be configured.
- **Primary Address**
Select the primary IPv4 address. If the router becomes master router, the router uses this IPv4 address.

Note

If you only configure one subnet on this VLAN, no entry is necessary. The entry is then 0.0.0.0.

If you configure more than one subnet on the VLAN and you want a specific IPv4 address to be used as the source address for VRRP packets, select the IPv4 address. Otherwise, the numerically lowest IPv4 address will be used.

- **Priority**
Enter the priority of this virtual router. Valid values are 1-254.
If an IPv4 address is assigned to the VRRPv3 router that is also actually configured on the local IPv4 interface, the value 255 is entered automatically. All other priorities can be distributed freely among the VRRPv3 routers. The higher the priority, the earlier the VRRPv3 router becomes "Master".
- **Advertisement interval**
Enter the time interval after which a master router sends another VRRPv3 packet. Specified in centiseconds.
- **Track ID**
Select a track ID.
- **Decrement Priority**
Enter the value by which the priority of the VRRPv3 interface will be reduced.
- **Current Priority**
Shows the priority of the VRRPv3 interface after the monitored interface has changed to the "down" status.

Procedure

To configure a virtual router as the master router, follow the steps below:

1. Select the ID of the virtual router you want to configure from the "Interface / VRID" drop-down list.
2. Select the "Status" check box.
3. Select the source address from the "Primary Address" drop-down list.
4. From the "Priority" drop-down list, enter the priority of this virtual router.
5. Enter the interval in "Advertisement Interval".
6. Select a track ID.
7. Enter the value by which the priority of the VRRPv3 interface will be reduced
8. Click the "Set Values" button.

5.9.4.3 Address overview

Overview

This page shows which IPv4 addresses the virtual router monitors. Each virtual router can monitor one IPv4 address.

Virtual Router Redundancy Protocol v3 (VRRPv3) Associated IP Addresses Overview						
Router	Configuration	Addresses Overview	Addresses Configuration	Interface Tracking		
Interface	VRID	Number of Addresses	Associated IP Address (1)	Associated IP Address (2)	Associated IP Address (3)	Associated IP Address (4)
vlan3	1	1	10.10.10.150	0.0.0.0	0.0.0.0	0.0.0.0
Refresh						

Description of the displayed values

The table has the following columns:

- **Interface**
Shows the Interface that functions as the virtual router.
- **VRID**
Shows the ID of this virtual router.
- **Number of Addresses**
Shows the number of IPv4 addresses.
- **Associated IP Address (1) ...Associated IP Address (4)**
Shows the router IPv4 addresses monitored by this virtual router. If a router takes over the role of master, the routing function is taken over by this router for all these IPv4 addresses.

5.9.4.4 Address Configuration

Creating or changing the monitored IP addresses

On this page, you can create, modify or delete the IPv4 addresses to be monitored. Each virtual router can monitor one IPv4 address.

Virtual Router Redundancy Protocol v3 (VRRPv3) Associated IP Addresses Configuration

Router

Configuration

Addresses Overview

Addresses Configuration

Interface Tracking

Interface / VRID:

vlan3 / 1

Associated IP Address:

Select

Associated IP Address

☐

10.10.10.150

1 entry.

Create

Delete

Refresh

Description

The page contains the following:

- **Interface / VRID**
Select the ID of the virtual router.
- **Associated IP Address**
Enter the IPv4 address that the virtual router will monitor.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted
- **Associated IP Address**
Shows the IPv4 addresses that the virtual router monitors.

Procedure

1. Select the ID of the virtual router.
2. Enter the IPv4 address that the virtual router will monitor.
3. Click the "Create" button. A new entry is generated in the table.

5.9.4.5 Interface Tracking

Introduction

On this page, you configure the monitoring of interfaces.

When the link of a monitored interface changes from "up" to "down", the priority of the assigned VRRP interface is reduced. You configure the value by which the priority is reduced on the page "Layer 3 > VRRPv3 > Configuration".

When the link of the interface changes back from "down" to "up", the original priority of the VRRP interface is restored.

Virtual Router Redundancy Protocol v3 (VRRPv3) Interface Tracking

Router

Configuration

Addresses Overview

Addresses Configuration

Interface Tracking

Interface: P1

Track Id:

Track Id: All

Track Interface Count: 0

Select	Track Id	Interface
☐	1	vlan3

1 entry.

Create

Delete

Refresh

Description

The page contains the following boxes:

- **Interface**
From the drop-down list, select the interface to be monitored.
- **Track ID**
Enter a track ID.
- **Track ID**
Select a track ID.
- **Track Interface Count**
Enter how many monitored interfaces need to change to the "down" status, before the priority is changed.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Track ID**
Shows the track ID.
- **Interface**
Shows the interface that is being monitored.

Procedure

1. Select the required interface from the "Interface" drop-down list.
2. In the "Track ID" box, enter the required ID.
3. Click the "Create" button.
4. Select an ID from the "Track-ID" drop-down list:
5. In the "Track Interface Count" enter the number of interfaces.
6. Click the "Set Values" button.
7. Link the monitoring to a VRRP interface in the "Configuration" tab.

5.9.4.6 Address monitoring

Introduction

You configure the monitoring of IPv4 addresses on this page. The router sends a ping request to each of the configured IPv4 addresses within the specified time period. If no response is received within a specified time period, the VRRP priority of the corresponding interface is reduced.

Virtual Router Redundancy Protocol v3 (VRRPv3) Address Tracking

Router	Configuration	Addresses Overview	Addresses Configuration	Interface Tracking	Address Tracking

Track Id:
IP Address:

Select	Track Id	IP Address	Ping Period[s]	Ping Timeout [s]
☐	17	192.168.16.172	5	15
☐	45	192.168.16.199	5	15

2 entries.

Description

The page contains the following boxes:

- **Track ID**
Enter the track ID.
- **IP Address**
Enter the IPv4 address to be monitored. You can enter a maximum of five IPv4 addresses.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Track ID**
Shows the track ID.
- **IP Address**
Show the IPv4 address to be monitored.
- **Ping Period**
Shows the cycle time in seconds between two ping requests.
- **Ping Timeout**
Shows the time in seconds that the router waits for a ping response. The minimum duration is three times the ping period.

Procedure

1. In the "Track ID" box, enter the required ID.
2. In the "IPv4 Address" field, enter the IPv4 address that the virtual router is to monitor.
3. Click the "Create" button. A new entry is generated in the table.

5.10 Menu "Layer 3 (IPv6)"

5.10.1 Subnets

Connected Subnets

On this page, you can enable IPv6 on the interface. The interface is also called an IPv6 interface. An IPv6 interface can have several IPv6 addresses.

Connected Subnets

Subnets

Interface: vlan1

☒ IPv6 Enable

Note: Once IPv6 is enabled on an interface it currently can only be disabled by deleting the interface.

IPv6 Address:

Prefix Length:

IPv6 Address Type: Unicast

☒ Address Autoconfiguration (SLAAC)

Select	Interface Name	IPv6 Address	Prefix Length	IPv6 Address Type	Address Autoconfiguration (SLAAC)	Duplicate Address Detection Status
☐	vlan1	2222:4::	96	Unicast	Enabled	Complete
☐	vlan1	FE80::21B:1BFF:FECD:F217	64	Link Local	Enabled	Complete

2 entries.

Create

Delete

Set Values

Refresh

Description

The page contains the following:

- Interface**
Select the IP interface on which IPv6 will be enabled.
- IPv6 Enable**
Enable or disable IPv6 on the interface.

Note

Disabling IPv6

If IPv6 is enabled on an interface, you can only disable IPv6 by deleting interface.

- IPv6 Address**
Enter the IPv6 address. The entry depends on the selected address type.
- Prefix Length**
Enter the number of left-hand bits belonging to the prefix.

- **IPv6 Address Type**
Select the address type.
 - Unicast
 - Anycast
 - Link Local: IPv6 address is only valid on the link
- **Address Autoconfiguration (SLAAC)**
Enable or disable the SLAAC (Stateless Address Auto Configuration) mechanism for the address configuration.
If SLAAC is enabled, there will be stateless auto configuration via NDP (Neighbor Discovery Protocol).

The table has the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Interface Name**
Shows the name of the interface.
- **IPv6 Address**
Shows the IP address of the subnet.
- **Prefix Length**
Shows the prefix length.
- **IPv6 Address Type**
Displays the address type. The following values are possible:
 - Unicast
 - Anycast
 - Link Local

- **Duplicate Address Detection Status**

In Address Autoconfiguration (SLAAC), the "Duplicate Address Detection Status" function prevents IPv6 addresses from being assigned twice. The device can only use free IPv6 addresses during autoconfiguration.

When the function is enabled, the check via NDP takes place automatically.

Note

The function does not run a cyclic check.

This column shows the current status of the function. The following values are possible:

- **Tentative**

This status indicates that the selected IPv6 address is being checked. The device sends a neighbor solicitation message to the selected IPv6 address.

- **Conflict**

This status indicates that the IPv6 address is already being used. In this case, a neighbor advertisement message with the selected IPv6 address is returned to the device.

- **Complete**

This status indicates that the selected IPv6 address can be used. In this case, the device did not receive feedback within a period of time and assumes that the IPv6 address is not yet assigned.

- **Down**

This status indicates that the interface is not active. No check is carried out.

- **Loopback**

Shows whether or not the "Loopback" property is enabled.

Procedure

Automatically form link local address

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

Assign link-local address

1. Select the required interface.
2. Enable IPv6.
3. In "IPv6 Address" enter the link local address, e.g. FE80::21B:1BFF:FE40:9155
4. Enter "64" in "Prefix Length".
5. For "IPv6 Address Type" select the entry "Link Local".
6. Click the "Create" button. In the table an entry with the interface is created and the IPv6 address is displayed.

5.10.2 NAT

5.10.2.1 Masquerading

On this WBM page, you enable the rules for IPv6 masquerading.

Internet Protocol (IP) Masquerading

Masquerading

NAPT

Source NAT

NETMAP

Interface	Enable Masquerading
vlan1 (INT)	☐
vlan2 (EXT)	☐
vlan3	☐
ppp2	☒

Set Values

Refresh

Description

The table has the following columns:

- Interface**
Interface to which the setting relates. Only interfaces with a configured subnet are available.
- Enable Masquerading**
When enabled, with each outgoing data packet sent via this interface, the source IP address is replaced by the IPv6 address of the interface.

5.11 "Security" menu

5.11.1 Users

5.11.1.1 Local users

On this page, you create local users with the corresponding rights. To create a user account, the logged on user must have the "admin" role.

Local Users

Local Users

Roles

Groups

User Account:

Password Policy: high

Password:

Password Confirmation:

Role: user

Select	User Account	Role	Description	Remote Access	Two Factor Authentication
☐	admin	admin	System defined local user	none	☐
☐	Service	user		none	☐

2 entries.

Create

Delete

Set Values

Refresh

Description

The page contains the following:

- **User Account**

Enter the name for the user. The name must meet the following conditions:

- It must be unique.
- It must be between 1 and 250 characters long.
- The following characters must not be included: | § ? " ; : ß
- The characters for Space and Delete also cannot be included.

Note

User name cannot be changed

After creating a user, the user name can no longer be modified.

If a user name needs to be changed, the user must be deleted and a new user created.

Note

User names: admin

You can configure the device with this user name.

When you log in for the first time or log in after a "Restore Factory Defaults and Restart", you will be prompted to change the predefined password "admin". You can also rename the "admin" user preset in the factory once. Afterwards, renaming "admin" is no longer possible.

- **Password Policy**

Shows which password policy is being used:

- High
Password length: At least 8 characters, maximum 32 characters
At least 1 uppercase letter
At least 1 special character
At least 1 number
- User-defined
The password must meet the configured requirements. You configure the requirements under "Security > Passwords > Options".

- **Password**

Enter the password. Use passwords with a high password strength.

It must not contain any of the following characters: | § ? " ; : ß \

- **Password Confirmation**

Enter the password again to confirm it.

- **Role**

Select a role.

You can choose between default and self-defined roles, refer to the page "Security > Users > Roles."

The table contains the following columns:

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

Note

The users preset in the factory as well as logged in users cannot be deleted or changed.

- **User Account**
Shows the user name.
- **Role**
Shows the role of the user.
- **Description**
Enter a description of the user account. The description text can be up to 100 characters long.
- **Remote Access**
Select a type for the remote access.
 - Only
Only remote access, which means no rights other than logging into the WBM page for user-specific firewall.
 - None
No remote access. The user cannot log on to the user-specific firewall, but only to the WBM of the device.
 - Additional
The user can log on to both the WBM of the device and the user-specific firewall.
- **Two-Factor Authentication (2FA)**
Enables or disables TOTP-based two-factor authentication of the user. You can find more information on this under "Security > Passwords > Two-Factor Authentication".

Procedure

Note**Changes in "Trial" mode**

Even if the device is in "Trial" mode, changes that you carry out on this page are saved immediately.

Creating users

1. Enter the name for the user.
2. Enter the password for the user.
3. Enter the password again to confirm it.
4. Select the role of the user.
5. Click the "Create" button.
6. Enter a description of the user.
7. Click the "Set Values" button.

Deleting users

1. Select the check box in the row to be deleted.
2. Click the "Delete" button. The entries are deleted and the page is updated.

5.11.1.2 Roles

Roles

On this page, you create roles that are valid locally on the device.

Note

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

User Roles

Local Users

Roles

Groups

Role Name:

Select	Role	Function Right	Description	Remote Access
☐	user	1	System defined role, with readonly access to configuration data of this component.	none
☐	admin	15	System defined role, with read/write access to configuration data of this component.	none
☐	default	0	Internal role, for authenticated users without group/role mapping in this component.	none
☐	everybody	0	Internal role, assigned to users when authentication failes. Access will be denied.	none
☐	Layer2	1		none

5 entries.

Create

Delete

Set Values

Refresh

Description

The page contains the following:

- **Role Name**
Enter the name for the role. The name must meet the following conditions:
 - It must be unique.
 - It must be between 1 and 64 characters long.

Note

Role name cannot be changed

After creating a role, the name of the role can no longer be changed.

If a name of a role needs to be changed, the role must be deleted and a new role created.

The table contains the following columns:

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

Note

Predefined roles and assigned roles cannot be deleted or modified.

- **Role**
Shows the name of the role.
- **Function Right**
Select the function rights of the role:
 - 1
Users with this role can read device parameters but cannot change them. Users with this role can change their own password.
 - 15
Users with this role can both read and change device parameters.

Note

Function right cannot be changed

If you have assigned a role, you can no longer change the function right of the role.

If you want to change the function right of a role, follow the steps outlined below:

1. Delete all assigned users.
 2. Change the function right of the role:
 3. Assign the role again.
-

- **Description**
Enter a description for the role. With predefined roles a description is displayed. The description text can be up to 100 characters long.
- **Remote Access**
 - None
No remote access. The user cannot log in to the dynamic firewall, but only to the WBM of the device.
 - Additional
The user can log in to both the WBM of the device and the dynamic firewall.
 - Only
The user can only log into the dynamic firewall.

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.

5.11.1.3 Groups

User groups

On this page you link a group with a role.

In this example the group "Administrators" is linked to the "admin" role: The group is defined on a RADIUS server. The role is defined locally on the device. When a RADIUS server authenticates a user and assigns the user to the "Administrators" group, this user is given rights of the "admin" role.

Note

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

User Groups

Local Users

Roles

Groups

Group Name:

Select	Group	Role	Description
☐	Administrators	admin	Mapping group Administrators (RADIUS) to role admin (device)

1 entry.

Create

Delete

Set Values

Refresh

Description

The page contains the following:

- **Group Name**
Enter the name of the group. The name must match the group on the RADIUS server. The name must meet the following conditions:
 - It must be unique.
 - It must be between 1 and 64 characters long.
 - The following are not permitted: § ? " ; :

5.11 "Security" menu

The table contains the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Group**
Shows the name of the group.
- **Role**
Select a role. Users who are authenticated with the linked group on the RADIUS server receive the rights of this role locally on the device.
You can choose between system-defined and self-defined roles, refer to the page "Security > Users > Roles."
- **Description**
Enter a description for the link of the group.to a role. The description text can be up to 100 characters long.

Procedure

Linking a group to a role.

1. Enter the name of a group.
2. Click the "Create" button.
3. Select a role.
4. Enter a description for the link of a group.to a role.
5. Click the "Set Values" button.

Deleting the link between a group and a role

1. Select the check box in the row to be deleted.
2. Click the "Delete" button. The entries are deleted and the page is updated.

5.11.2 Passwords

Configuration of the passwords

Note

If you are logged in via a RADIUS server, you cannot change any passwords.

On this page, you can change passwords. If you are logged in with the right to change device parameters, you can change the passwords for all user accounts. If you are logged in as user, you can only change your own password.

Account Passwords

Passwords

Options

Current User: admin

Current User Password:

User Account: admin

Password Policy: high

New Password:

Password Confirmation:

Description

- **Current User**
Shows the user that is currently logged in.
- **Current User Password**
Enter the password for the currently logged in user.
- **User Account**
Select the user whose password you want to change.
- **Password Policy**
Shows which password policy is being used when assigning new passwords.

Note

Checking the password policy of existing users

The set password policy is used when assigning new passwords. Existing passwords are not checked. If you change the password policy from "Low" to "High", the previously used passwords remain valid. As an important measure for increasing security, change the passwords used up to now.

- High
Password length: At least 8 characters, maximum 32 characters
At least 1 uppercase letter
At least 1 special character
At least 1 number
 - Low
Password length: at least 6 characters, maximum 32 characters
 - Custom
You configure the password policy on the page "Security > Passwords > Options".
- **New Admin Account Name**
Only when logging in for the first time or after resetting the device to the factory settings
You can rename the user preset in the factory "admin" once. Afterwards, renaming "admin" is no longer possible.
Enter "admin" or a new name for the "admin" user.

5.11 "Security" menu

- **New Password**

Enter the new password for the selected user.

You can find information on the permitted characters in Appendix of the WBM "Permitted characters in names, passwords and descriptions" (Page 513).

- **Password Confirmation**

Enter the new password again to confirm it.

Procedure

1. From the "User Account" drop-down list, select the user whose password you want to change.
2. Enter the valid password for the currently logged in user in the "Current User Password" input box.
3. Enter the new password for the selected user in the "New Password" input box.
4. Repeat the new password in the "Password Confirmation" input box.
5. Click the "Set Values" button.

Note

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

- admin: admin

When you log in for the first time or following a "Restore Factory Defaults and Restart", with the preset user "admin" you will be prompted to change the password.

Note**Changing the password in Trial mode**

Even if you change the password in Trial mode, this change is saved immediately.

5.11.2.1 Options

On this page, you specify which password policy will be used when assigning new passwords.

Password Options

Passwords Options

Password Policy: high

New Password Policy: high ▼

Password Policy Details:

Minimum Password Length: 8

Minimum Number of Numeric Characters: 1

Minimum Number of Special Characters: 1

Minimum Number of Uppercase Letters: 1

Minimum Number of Lowercase Letters: 0

Set Values Refresh

Description

- **Password Policy**
Shows which password policy is currently being used.
- **New Password Policy**
Select the required setting from the drop-down list.
 - High
Password length: At least 8 characters, maximum 32 characters
At least 1 number
At least 1 special character
At least 1 uppercase letter
 - User-defined
Configure the desired password requirements under "Password Policy Details".
Password length: At least 8 characters, maximum 32 characters
- **Password Policy Details**
When you have selected the "High" password policy, the relevant password requirements are displayed.
When you have selected the "User-defined" password policy, you can configure the relevant password requirements.
 - Minimum Password Length
Specifies the minimum length of a password.
 - Minimum Number of Numeric Characters
Specifies the minimum number of numeric characters in a password.
 - Minimum Number of Special Characters
Specifies the minimum number of special characters in a password.
 - Minimum Number of Uppercase Letters
Specifies the minimum number of uppercase characters in a password.
 - Minimum Number of Lowercase Letters
Specifies the minimum number of lowercase characters in a password.

5.11.2.2 Two-factor authentication

With two-factor authentication (2FA), a second query is added after authentication with user name and password. To successfully log on to the device, you need a user name, a password and a one-time token. This is also referred to as a TOTP (Time-based One-Time Password) or Token. The one-time token is generated by an authentication app and is valid for 30 seconds.

Two-factor authentication can be enabled on the page "Security > Users > Local Users".



Two Factor Authentication

Passwords Options **Two-Factor Authentication**

2FA is disabled.
Scan the QR code or type the text below QR code manually in the authenticator application and then provide the generated 6-digit verification code.



CWK2BXDQU3JVEOSX

Current User Password:

6-digit code:

Security requirements for 2FA

- Keep the operating system on the mobile device and the authentication app up to date.
- The mobile device and the authentication app must be trusted.
- Keep your password safe on the device. If the smartphone is lost, the code generator can be lost. You can save a code for the QR code in a password manager.
- Store the QR code securely to prevent unauthorized access. The QR code can be scanned.
- For time synchronization, use cellular time, GPS time or NTP (secure).

Requirement

- An authentication app is installed on the smartphone.
- The "Two-Factor Authentication" check box can be selected on the page "Security > Passwords > Local Users".

Procedure

1. Enter the user name and the associated password.
After successful logon, the "Two-Factor Authentication" page opens.
2. First use of two-factor authentication: Scan the QR token with the authentication app or enter the alphanumeric token in the app.
3. Generate a one-time token using the authentication app.

- 4. Enter your password in the "Current User Password" input box.
- 5. Enter the one-time token in the "6-digit code" field and click "Set Values".

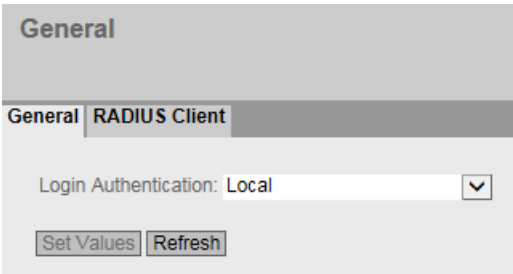
5.11.3 AAA

5.11.3.1 General

Login of network nodes

The designation "AAA" stands for "Authentication, Authorization, Accounting". This feature is used to identify and allow network nodes, to make the corresponding services available to them and to specify the range of use.

On this page, you configure the login.



Description

The page contains the following boxes:

Note

To be able to use the login authentication "RADIUS", "Local and RADIUS" or "RADIUS and fallback Local", a RADIUS server must be stored and configured for user authentication.

5.11 "Security" menu

- **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.

5.11.3.2 RADIUS Client

Authentication over an external server

The concept of RADIUS is based on an external authentication server.

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

If no server responds, there is no authentication.

Remote Authentication Dial In User Service (RADIUS) Client

General RADIUS Client

RADIUS Authorization Mode: Vendor Specific

Select	Auth. Server Type	RADIUS Server Address	Server Port	Shared Secret	Shared Secret Conf.	Max. Retrans.	Timeout(s)	Primary Server	Force Msg. Auth.	Test	Test Result
☐	Login	192.168.16.8	1812	*****	*****	3	5	no	☒	Test	Not reachable

1 entry.

CreateDeleteSet ValuesRefresh

Description

The page contains the following boxes:

- **RADIUS Authorization Mode**

For the login authentication, the RADIUS authorization mode specifies how the rights are assigned to the user with a successful authentication.

- Standard

In this mode the user is logged in with administrator rights if the server returns the value "Administrative User" to the device for the attribute "Service Type". In all other cases the user is logged in with read rights.

- Vendor Specific

In this mode, the assignment of rights depends on whether and which group the server returns for the user and whether or not there is an entry for the user in the table "External User Accounts".

The table has the following columns:

- **Select**

Select the row you want to delete.

- **RADIUS Server Address**

Enter the IP address or the FQDN (Fully Qualified Domain Name) of the RADIUS server.

- **Server Port**

Here, enter the input port on the RADIUS server. As default, input port 1812 is set. The range of values is 1 to 65535.

- **Shared Secret**

Enter your access ID here. The range of values is 1...128 characters.

You can find information on the permitted characters in Appendix of the WBM (Page 513).

- **Shared Secret Conf.**

Enter your access ID again as confirmation.

- **Max. Retrans.**

Here, enter the maximum number of retries for an attempted request.

The initial connection attempt is repeated the number of times specified here before another configured RADIUS server is queried or the login counts as having failed. As default 3 retries are set, this means 4 connection attempts. The range of values is 1 to 5.

- **Timeout[s]**

Specify the duration in seconds for a connection attempt. When the time elapses, the connection attempt ends.

Range of values: 1 ...120

Default value: 5

- **Primary Server**

Using the options in the drop-down list, specify whether or not this server is the primary server. You can select one of the options "yes" or "no".

- **Use Message Authenticator**

The "Message Authenticator" attribute is a HMAC-MD5 checksum for access request or access challenge, access accept and access reject packets. If it is enabled, the checksum of the packet is calculated and checked on the RADIUS client or RADIUS server.

If the Message Authenticator is not present or the check has failed, the RADIUS message is discarded.

- **Test**

With this button, you can test whether the credentials of the specified RADIUS user are on the server.

The authentication test is performed once. If there is a failed login to the RADIUS server, this event is logged. The log message of the category "Warning" displays the following description:

RADIUS: IP address <...>, Port <...> User Name <...>: "Test" - Unsuccessful user authentication.

- **Test Result**

Displays the test result:

- 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.

The test result is not automatically updated. To delete the test result, click the "Refresh" button.

Procedure

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
- Timeout[s]: 5
- Primary server: No

2. In the relevant row, enter the following data in the input boxes:

- RADIUS Server Address
- Shared Secret
- Shared Secret Conf

3. Enable the "Use Message Authenticator" option.

4. If necessary, perform the authentication test.

5. 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.
- Timeout[s]
- Primary Server

2. Perform the authentication test.

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.

5.11.4 Certificates

5.11.4.1 Overview

All loaded files (certificates and keys) are shown on this WBM page. You have the following options for loading files on the device:

- System > Load&Save > HTTP
- System > Load&Save > TFTP
- System > Load&Save > SFTP

Certificates Overview				
Overview Certificates				
Select	Type	Filename	State	Subject DN
☐	Key File	Configuration 1.UAE938401@GF13A.Module1_Key.pem	valid	C=DE O=Siemens CN=PEA46-UAE938401-GF13A
☐	Machine Cert	Configuration 1.UAE938401@GF13A.Module1_Cert.pem	valid	C=DE O=Siemens CN=PEA46-UAE938401-GF13A
☐	CA Cert	Configuration 1.UAE938401@GF13A.Module1_CACert.pem	valid	C=DE O=Siemens CN=P0642039A-GF3973FF368C54A99
☐	Remote Cert	Configuration 1.Group1.Module1.cer	valid	C=DE O=Siemens CN=PEA46-UAE938401-GF13A
4 entries.				
Delete Refresh				

Figure 5-1 Part 1

Issuer DN	Issue Date	Expiry Date	Used
C=DE O=Siemens CN=P0642039A-GF3973FF368C54A99	12/04/2017 14:42:41	12/04/2037 23:59:59	-
C=DE O=Siemens CN=P0642039A-GF3973FF368C54A99	12/04/2017 14:42:41	12/04/2037 23:59:59	-
C=DE O=Siemens CN=P0642039A-GF3973FF368C54A99	12/04/2017 14:42:36	12/04/2037 23:59:59	-
C=DE O=Siemens CN=P0642039A-GF3973FF368C54A99	12/04/2017 14:42:41	12/04/2037 23:59:59	-

Figure 5-2 Part 2

Description

- **Select**
Select the check box in the row to be deleted. Only unused certificates can be deleted.
- **Type**
Shows the type of the loaded file.
 - CA Cert
The CA certificate is signed by a CA (Certification Authority).
 - Machine certificate
 - Key File
 - Remote Cert
Partner certificate

- **Filename**
Shows the file name.
- **Status**
Shows whether the certificate is valid or has already expired.
- **Subject DN**
Shows the name of the applicant.
- **Issuer DN**
Shows the name of the certificate issuer.
- **Issue Date**
Shows the start of the period of validity of the certificate
- **Expiry Date**
Shows the end of the period of validity of the certificate.
- **Used**
Shows which function uses the certificate.

5.11.4.2 Certificates

The format of the certificate is based on X.509, a standard of the ITU-T for creating digital certificates. This standard describes the schematic structure of X509 certificates. You will find further information on this on the Internet at "<http://www.itu.int>".

On this page, the content of the following structure elements can be displayed. If the structure element does not exist or is not completed in the selected certificate, nothing is shown in the box on the right. Certain entries can only be edited if they are supported.

Certificate Properties

Overview **Certificates**

Filename: Configuration 1.UAE938401@GF13A.Module1_Key.pem

Type: Key File

Subject DN: C=DE O=Siemens CN=PEA46-UAE938401-GF13A

Issuer DN: C=DE O=Siemens CN=P0642039A-GF3973FF368C54A99

Subject Alternate Name: N/A

Issue Date: 12/04/2017 14:42:41

Expiry Date: 12/04/2037 23:59:59

Serial: N/A

Used: -

Crypto Algorithm: RSA

Key Usage:

Extended Key Usage:

Key File: Configuration 1.UAE938401@GF13A.Module1_Key.pem

Certificate Revocation List 1st URL: -

Certificate Revocation List 2nd URL: -

Certificate: Configuration 1.UAE938401@GF13A.Module1_Cert.pem

Passphrase:

Passphrase Confirmation:

Set Values

Refresh

Note**Supported encryption algorithms**

Only RSA and ECC certificates are supported.

Description

- **Filename**
Select the required certificate.
- **Type**
Shows the type of the loaded file.
 - CA Cert
The CA certificate is signed by a CA (Certification Authority).
 - Machine certificate
 - Key File
 - Remote Cert
Partner certificate
- **DN**
Shows the name of the applicant.
- **Issuer DN**
Shows the name of the certificate issuer.
- **Subject Alternate Name**
If it exists, an alternative name of the applicant is displayed.
- **Issue Date**
Shows the start of the period of validity of the certificate
- **Expiry Date**
Shows the end of the period of validity of the certificate.
- **Serial Number**
Shows the serial number of the certificate.
- **Used**
Shows which function uses the certificate.
- **Crypto Algorithm**
Shows which cryptographic method is used.
- **Key Usage**
Shows the purpose that the key belonging to the certificate is used for, e.g. to verify digital signatures.
- **Extended Key Usage**
Shows whether the purpose is additionally restricted, e.g. only to verify signatures of the CA certificate.
- **Key File**
Shows the key file.
- **Certificate Revocation List 1st URL**
Enter the URL with which the revocation list can be called up. Can only be edited if supported by the certificate.
- **Certificate Revocation List 2nd URL**
Enter an alternative URL. If the revocation list cannot be called up using the 1st URL, the alternative URL is used. Can only be edited if supported by the certificate.

- **Certificate**
Shows the name of the certificate.
- **Passphrase**
Enter the password for the certificate. Can only be edited if the encrypted file is password protected.
- **Passphrase Confirmation**
Enter the password again. Can only be edited if the encrypted file is password protected.

5.11.5 Firewall

5.11.5.1 General

On this page, you activate the firewall. You can activate the MAC firewall and/or the IP firewall. If both firewalls are activated, packets are checked based on L2 firewall rules first. If a packet passes through Layer 2, L3 firewall rules are applied to it.

Note

If you disable the firewall, your internal network is unprotected.

Firewall General

General Predefined Dynamic Rules IP Services ICMP Services IP Protocols IP Rules Predefined MAC MAC Services MAC Rules

☒ Activate L3-Firewall

☒ Activate L2-Firewall

Connection State Settings

TCP Idle Timeout [s]: 86400

UDP Idle Timeout [s]: 300

ICMP Idle Timeout [s]: 300

Set Values Refresh

Description

The page contains the following:

- **Activate L3 Firewall**
IP-based firewall (Layer 3 and 4)
If this option is enabled, data traffic is forwarded between subnets based on Layer 3 addresses that are used in the firewall rules as source and destination IP addresses. The source/destination IP addresses are changed.
- **Activate L2 Firewall**
MAC-based firewall (Layer 2)
When enabled, the device operates as a switch and forwards data traffic based on MAC addresses without changing the source/destination IP addresses between the local interface VLAN1 and the virtual interface NVEx.
You configure the MAC rules for the interfaces on the "Firewall > MAC rules (Page 456)" tab.

Note

No predefined MAC firewall rules are created for the data traffic between the device and the SINEMA RC (VXLAN).

The L2 firewall does not have to be activated for SINEMA RC (VXLAN) to work.

Connection State Settings:

- **TCP Idle Timeout [s]**
Enter the required time in seconds. If no data exchange takes place, the TCP connection is terminated automatically when this time has elapsed.
The value range is 1 ... 21474836.
Default setting: 86400 seconds
- **UDP Idle Timeout [s]**
Enter the required time in seconds. If no data exchange takes place, the UDP connection is terminated automatically when this time has elapsed.
The value range is 1 ... 21474836.
Default setting: 300 seconds
- **ICMP Idle Timeout [s]**
Enter the required time in seconds. If no data exchange takes place, the ICMP connection is terminated automatically when this time has elapsed.
The value range is 1 ... 21474836.
Default setting: 300 seconds

5.11.5.2 Predefined

The page contains predefined IP packet filter rules. If you create your own IP packet filter rules, these have a higher priority than the predefined IP packet filter rules.

Set which IPv4 services of the device should be reachable from which interface.

5.11 "Security" menu

Predefined

General | Predefined | Dynamic Rules | IP Services | ICMP Services | IP Protocols | IP Rules | Predefined MAC | MAC Services | MAC Rules

Allow device services:

Interface▼	IP Version	All	HTTP	HTTPS	DNS	SNMP	Telnet	SMS Relay	TCP Event	IPsec VPN	OpenVPN	SSH	DHCP	Ping	System Time	VRRP	VXLAN	Capture
vlan1 (INT)	IPv4	☐	☒	☒	☒	☒	☒	☒	☐	☐	☐	☒	☒	☒	☐	☐	☐	☐
vlan1 (INT)	IPv6	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
usb0	IPv4	☐	☐	☐	☐	☐	☐	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐
usb0	IPv6	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
a1	IPv4	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☒	☐	☐	☐	☐

Set Values Refresh

Description

- **Interface**

The list is dynamic.

- pppx or usb0 (only with M876-4 / RM1224 / MUx85x / S615)
Allows access from the WAN interface to the device.
- VLANx
Allows access from the IP subnet to the device. VLANs with configured IP subnet are available.
- SINEMA RC
Allows access from the SINEMA RC server to the device. Only available with KEY-PLUG SINEMA RC.
- OpenVPN connection, IPsec VPN connection
Allows the VPN tunnel partners reachable via the VPN connection to access the device. If you have created a VPN connection, the connection name will be displayed in the list.

- **IP Version**

Shows the IP version to which the firewall rules apply.

- IPv4
- IPv6 (not with M816)

Access over the firewall is permitted to the following IPv4 services:

- All
All IPv4 services
- HTTP
For access to Web Based Management

- HTTPS
For secure access to Web Based Management

Note**HTTP and HTTPS deactivated**

If you disable HTTP and HTTPS, the WBM of the device can no longer be reached.

HTTPS disabled

When you disable HTTPS, you can only access the WBM using HTTP. This assumes that "HTTP & HTTPS" is set in "System > Configuration > HTTP Services". If for example "Redirect HTTP to HTTPS" is set, access via HTTP cannot be redirected to HTTPS. This means that the WBM of the device can no longer be reached.

- DNS
DNS queries to the device. Necessary only if the "DNS-Relay" function is enabled on the device.
- SNMP
Incoming SNMP connections. Required, for example, to access the SNMP information of the device using a MIB browser.
- Telnet
For unencrypted access to the CLI
- SMS Relay (only with M87x / RM1224 / MUx85x)
For sending SMS messages from the local network
- TCP Event (not with M816)
For incoming TCP packets. Required to trigger the "Sleep Mode" function, for example.
- IPsec VPN
Allows IKE (Internet Key Exchange) data transfer from the external network to the device. Necessary if an IPsec VPN remote station needs to establish a connection to this device.
- OpenVPN
Allows OpenVPN data traffic from the external network to the device. Necessary if an OpenVPN client is to establish a connection to this device (as OpenVPN server).
- SSH
For encrypted access to the CLI
- DHCP
Access to the DHCP server or the DHCP client
- Ping
Access to the ping function.
- System time
Access to NTP and SNTP.
- Cloud Connector (only with MUx85x)
Access to the integrated TIA Portal Cloud Connector Server and the devices accessible via the interface.
- VRRP
Access to VRRPv3

5.11 "Security" menu

- VXLAN (only with M876-4 / RM1224 / MUx85x / S615)
For establishing the VXLAN tunnel and receiving the frames. Necessary if the tunnel endpoint establishes a connection to this device.
- Capture (only with MUx85x)
Access to the ping function "Packet Capture" function from the enabled interface.

5.11.5.3 Dynamic Rules

On this page, you define dynamic rule sets. Firewall rules that are required for remote access, for example, can be summarized with a rule set.

You can assign a rule set to one or more users. If login of this user was successful, the firewall rule set intended for this user is enabled.

A timer is started after login. When the time expires, the user is automatically logged out from the device.

You can also control the rule sets over time. A start time and an end time are configured. Between these times, the firewall rules assigned to the rule set are enabled.

Dynamic Rules

General

Predefined

Dynamic Rules

IP Services

ICMP Services

IP Protocols

IP Rules

Rule Set

Name:

Select	No.	Name	Comment	Timeout [min]
☐	1	Service		30

1 entry.

Rule Set Assignment

Type: User Account

User Account	Role	Rule Set	Combined	Remaining Time	Force Deactivate
Service	user	-	None	-	Force Deactivate

Create

Delete

Set Values

Refresh

Description

"Rule set" area

- **Name**
Define a unique name for the rule set. If you click the "Create" button, a new row with a unique number is created.

The table contains the following columns:

- **Select**
Select the check box in the row to be deleted.
- **No.**
Shows the unique number of the entry.
- **Name**
Name of the rule set. The name can be changed if required.
- **Comment**
Comment that describes the rule set in more detail.
- **Timeout [min]**
Access is time-limited. Specify the duration of the access. If needed, the user can extend the access time via the "Reset Timeout" button on the "Dynamic Firewall Rules Information" page.

"Rule Set Assignment" area

- **Type**
Specify which rule set will be assigned to whom. The display of the following table depends on the selection for "Type".
 - User Account
The rule set is activated through a local user account.
 - Digital Input
The rule set is executed by controlling the digital input. The prerequisite for this is that the entry "Digital Input" is activated for the "Firewall" event under "System > Events > Configuration".
 - RADIUS role
The rule set is activated through a RADIUS role.
 - RADIUS user
The rule set is activated through a RADIUS user.
 - Time triggered
Enforcement of the rule set is time-triggered.

The "**User Account**" table contains the following columns:

- User Accounts
Only users with the remote access "only" or "additional" are displayed.
- Role
Shows the role of the user.
- Rule set
Define the rule set that is valid for this user.
- Combined
Combines the user login with an event, e.g. the "Digital Input" event. To log in to the WBM page for the dynamic firewall, voltage must be present at the digital input and user login must be successful.

5.11 "Security" menu

- **Remaining Time**
When this user is logged on, the remaining time for access is displayed.
- **Force Deactivate**
A user with administrator rights can log off the active user with this button.

The "**Digital Input**" table contains the following columns:

- **Digital Input**
The available digital inputs.
- **Rule set**
Define the rule set that is controlled via the digital input.
- **Dynamic Source (Range)**
Enter the IP address or an IP range that is allowed to send IP packets.
- **Status**
Shows the remaining time for access.

The "**RADIUS role**" table contains the following columns:

- **Role Name**
Shows the role name.
- **Role**
Only roles with the remote access "additional" are displayed. The prerequisite is that the role was created on the RADIUS server and RADIUS users were assigned to the role.
- **Rule set**
Define the rule set that is valid for this RADIUS role.
- **Combined**
Combines the logon with an event, e.g. the "Digital Input" event. To log in to the WBM page for the dynamic firewall, voltage must be present at the digital input and login must be successful.
- **Counter**
After successful login, the number of users active via RADIUS that are assigned to the RADIUS role is displayed.
- **Force Deactivate**
A user with administrator rights can log out the RADIUS role with this button.

The "**RADIUS user**" table contains the following columns:

- **Users**
Shows the users assigned to the role.
A role with the remote access "additional" is created on the device and assigned to a group. The names of the group must match exactly the names of the user groups on the RADIUS server.
- **Role**
The role assigned to the RADIUS user.
- **Remaining Time**
When this user is logged on, the remaining time for access is displayed.
- **Force Deactivate**
A user with administrator rights can log out the RADIUS role with this button.

The "**Time triggered**" table contains the following columns:

- Time triggered
Index of the entry.
- Rule set
Define the rule set that is time triggered.
- Combined
Combines the time triggering with an event, for example, the "Digital Input" event. To log in to the WBM page for the dynamic firewall, voltage must be present at the digital input and login must be successful.
- Cycle
Specify the enforcement cycle for the time triggering.
 - Daily
 - Weekly
 - Monthly
- Days
If "Weekly" or "Monthly" is set for the cycle, specify the days.
Enter the days separated by commas, e.g. 1,3,4
 - Weekly: 1 - 7
 - Monthly: 1 - 31
- Dynamic Source (Range)
 - Individual IP address: Specify the IP address
 - IP range: Specify the range with start address "-" end address, e.g.
IPv4: 192.168.100.10 - 192.168.100.20
IPv6: fe80:: - febf::
 - All IP addresses:
IPv4: " 0.0.0.0/0"
IPv6: "::"
 - If the rule set is activated by a user, the placeholder DYNAMIC is replaced by the IP address of the end device used.
- Start Time
Enter the start time in the format HH:MM.
- End Time
Enter the end time in the format HH:MM.
- Enable
When enabled, the rule set is time-triggered. The connection is briefly interrupted when the time-triggered firewall rules are initiated.

5.11.5.4 IP services

On this WBM page, you define IP services. Using the IP service definitions, you can define firewall rules for specific services. You select a name and assign the service parameters to it. When you configure the IP rules, you simply use this name.

Internet Protocol (IP) Services

GeneralPredefined IPv4IP ServicesICMP ServicesIP ProtocolsIP Rules

Service Name:

Select	Service Name	Transport	Source Port (Range)	Destination Port (Range)
☐	DNS	UDP	*	53
☐	HTTP	TCP	*	80

2 entries.

CreateDeleteSet ValuesRefresh

Description

The page contains the following:

- **Service Name**
Enter the name of the IP service. The name must be unique.

This table contains the following columns:

- **Select**
Activate the check box in the row to be deleted.
- **Service Name**
Shows the name of the IP service.
- **Transport**
Specify the protocol type.
 - UDP
The rule applies only to UDP frames.
 - TCP
The rule applies only to TCP frames.

- **Source Port (Range)**
Enter the source port. The rule applies specifically to the specified port.
 - If the rule is intended to apply to a port range, enter the range with start port "-" end port, for example 30 - 40.
 - If the rule is intended to apply to all ports, enter "*".
- **Destination Port (Range)**
Enter the destination port. The rule applies specifically to the specified port.
 - If the rule is intended to apply to a port range, enter the range with start port "-" end port, for example 30 - 40.
 - If the rule is intended to apply to all ports, enter "*".

5.11.5.5 ICMP services

On this page, you define ICMP services. Using the ICMP service definitions, you can define firewall rules for specific services. You select a name and assign the service parameters to it. When you configure the IP rules, you simply use this name.

Internet Control Message Protocol (ICMP) Dienste

Allgemein Vordefiniert Dynamische Regeln IP-Dienste ICMP-Dienste IP-Protokolle IP-Regeln

Name des Diensts:

Selektieren	Name des Diensts	Protokoll	Typ	Code
☐	ipv4wbm	ICMPv4	Destination Unreachable (3)	Port Unreachable (3)

1 Eintrag.

Erstellen Löschen Einstellungen übernehmen Aktualisieren

Description

The page contains the following:

- **Service Name**
Enter a name for the ICMP service. The name must be unique.
- The table contains the following columns:
- **Select**
Select the check box in the row to be deleted.
 - **Service Name**
Shows the name of the ICMP service.
 - **Protocol**
Define the version of the ICMP protocol.

- **Type**
Specify the ICMP packet type. A few examples are shown below:
 - Destination Unreachable (3)
The IP frame cannot be delivered.
 - Echo Request (8)
Echo request, better known as ping.
 - Time Exceeded (11)
Time limit exceeded.
- **Code**
The code describes the ICMP packet type in greater detail. The selection depends on the selected ICMP packet type.
With "Destination Unreachable", for example, "Code 1": Host cannot be reached.

5.11.5.6 IP protocols

On this WBM page, you can configure user-defined protocols, e.g. IGMP for multicast groups. You select a protocol name and assign the service parameters to it. When you configure the IP rules, you simply use this protocol name.

Select	Protocol Name	Protocol Number
☐	IGMP	2

1 entry.

Create Delete Set Values Refresh

Description

The page contains the following:

- **Protocol Name**
Enter a name for the protocol.

The page contains the following check boxes:

- **Select**
Select the check box in the row to be deleted.
- **Protocol Name**
Shows the protocol name.
- **Protocol Number**
Enter the protocol number, for example 2. You will find list of the protocol numbers on the Internet pages of iana.org

Procedure

Create IGMP protocol

1. Enter IGMP in "Protocol Name".
2. Click the "Set Values" button. A new entry is generated in the table.
3. Enter "2" in "Protocol Number".

5.11.5.7 IP rules

On this page, you define and enable your own IP rules for the firewall.

The IP rules set here have priority:

- Over the predefined IP rules and
- Over the IP rules created automatically due to a connection configuration (SINEMA RC).

Internet Protocol (IP) Rules

General | Predefined | Dynamic Rules | IP Services | ICMP Services | IP Protocols | IP Rules | Predefined MAC | MAC Services | MAC Rules

IP Version:

Rule Set:

☒ show all

Select	Protocol	Enable	Action	From	To	Source (Range)	Destination (Range)	Service	Log	Prec	Bandwidth(kbps)	Assign to	Assigned	Label	Comment
☐	IPv4	☒	Accept	vlan1 (INT)	vlan1 (INT)	0.0.0.0/0	0.0.0.0/0	ipv4wbm	none	0	all	☐	-	-	
☐	IPv6	☒	Drop	usb0	Device	AFFE::	FE80::	all	none	1	200	☐	-	-	
☐	Any	☒	Reject	OpenVPN Con	Any	0.0.0.0/0	0.0.0.0/0	all	none	2	all	☐	-	-	

3 entries.

Description

- **IP Version**
Specify the IP version to which the firewall rule applies.
When "Any" is selected:
 - The IP version is determined automatically based on the entered source or destination IP address.
 - The rule for IPv4 and IPv6 applies if no source and destination address was entered.
- **Rule set**
Select the required rule set. Only the IP rules that are assigned to this rule set will then be displayed in the table, provided that "Show all" is disabled.
When "Any" is selected, all IPv4 and IPv6 rules are displayed.
- **Show all**
When enabled, all available IP rules are displayed. With the "Assign" setting, you assign an IP rule to the selected rule set.

5.11 "Security" menu

The table contains the following columns:

- **Select**
Activate the check box in the row to be deleted.
- **Protocol**
Shows the version of the IP protocol.
- **Enable**
Activate or deactivate the firewall rule.
- **Action**
Select how incoming IP packets are handled:
 - "Accept" – The data packets can pass through.
 - "Reject" – The data packets are rejected, and the sender receives a corresponding message.
 - "Drop" – The data packets are discarded without any notification to the sender.
- **From / To**
Specify the communications direction of the IP rule.
 - VLANx: VLANs with configured subnet
 - ppp0 or usb0 (only with M876-4 / MUX85x): WAN interface
 - Device: Device
 - OpenVPN (all): All OpenVPN connections
 - SINEMA RC: Connection to the SINEMA RC server
 - IPsec (all): All IPsec VPN connections
 - Any: Applies to every interface and client connection, except Device.
 - NVEx: Virtual interface via which the VXLAN tunnel is established.

- **Source (Range)**

To receive IP packets, enter the IP address or an IP range.

- Individual IP address: Specify the IP address.
- IP range: Specify the range with start address "-" end address, e.g.
IPv4: 192.168.100.10 - 192.168.100.20
IPv6: fe80:: - febf::
- All IP addresses:
IPv4: "0.0.0.0/0"
IPv6: ":::"
Any (IPv4 and IPv6): Empty
- FQDN
The prerequisite is that a DNS server is configured under "System > DNS > DNS Client". FQDN is resolved via DNS. The DNS server therefore needs to be configured and reachable.

Note

Protection through DNSSEC

DNS is a protocol that does not require authentication. To prevent firewall rules from manipulating the FQDNs, enable the "DNS" option on the "System" > "DNSSEC" > "DNS Client" page.

- DYNAMIC
If the rule set is enabled by a user, the DYNAMIC placeholder is replaced by the IP address of the terminal device used.

Note

Digital input and DYNAMIC placeholder

If the rule set is executed by controlling the digital input, the placeholder DYNAMIC is replaced by the setting for "Dynamic Source (Range)". You configure the setting under "Security > Firewall > Dynamic Rules".

- **Destination (Range)**

To receive IP packets, enter the IP address or an IP range.

- Individual IP address: Specify the IP address
- IP range: Specify the range with start address "-" end address, e.g.
IPv4: 192.168.100.10 - 192.168.100.20
IPv6: fe80:: - febf::
- All IP addresses:
IPv4: "0.0.0.0/0"
IPv6: ":::"
- DYNAMIC
If the rule set is enabled by a user, the placeholder DYNAMIC is replaced by the IP address of the end device used.
- FQDN
The FQDN is resolved via DNS. For this purpose, set a DNS server under "System" > "DNS" > "DNS Client" and make sure that the server is reachable.

Note

Protection through DNSSec

DNS is an unencrypted protocol. To prevent firewall rules from manipulating the FQDNs, enable the "DNS" option on the "System" > "DNSSec" > "DNS Client" page.

- **Service**

Select the service or the protocol name for which this rule is valid.

- **Log**

Specify whether or not there should be a log entry every time the rule comes into effect and specify the severity of the event.

The following settings are available:

- none
The rule coming into effect is not logged.
- info / warning / critical
The rule coming into effect is logged with the selected event severity. The log file is displayed in "Information > Log Tables > Firewall Log".

- **Precedence**

Define the sequence in which the IP rules of the firewall are processed (ascending from 0 ... 127).

- **Bandwidth (kpbs)** (only with MUx85x)
Option for setting a bandwidth limitation. Can only be set if "Accept" is selected as action. A packet passes through the firewall if the Accept rule applies and the permitted bandwidth for this rule has not yet been exceeded.

Note

If bandwidth limitation is configured, routing performance is reduced to 500 Mbps.

The set bandwidth of an interface (e.g. vlan2) to the device has a higher priority than a forwarding rule for the same interface, e.g. from vlan2 to usb0.

– Example:

Rule 1: From vlan2 -> To device (5000 kbps)

Rule 2: From vlan2 -> To usb0 (10000 kbps)

or

Rule 1: From vlan2 -> To usb0 (10000 kbps)

Rule 2: From vlan2 -> To device (5000 kbps)

Result: The data traffic coming via interface vlan 2 to any destination (device or usb0) is limited to 5000 kbps.

If the same rule is configured twice, the bandwidth setting of the first rule applies.

– Example:

Rule 1: From vlan2 -> To vlan1 (5000 kbps)

Rule 2: From vlan2 -> To vlan1 (10000 kbps)

Result: The bandwidth of 5000 kbps is applied.

- **Assign**
To assign the IP rules to the selected rule set, activate the setting for the desired IP rules and click the "Set Values" button.
- **Assigned**
Shows the rule set to which this IP rule is assigned. The IP rules can also be assigned to multiple rule sets. If the IP rule is assigned to all rule sets, "all" is displayed.
- **Name**
Shows who created the IP rule.
 - NETMAP - automatically created firewall rule
- **Comment**
Enter an optional comment.

5.11.5.8 Predefined MAC rules

MUx85x

The page contains predefined MAC packet filter rules. If you create your own MAC packet filter rules, these have a higher priority than the predefined MAC packet filter rules.

On this page, you specify which inbound MAC services are to be reachable from the local network (LAN). The predefined MAC rules only consider the source address of the MAC packets.

Predefined MAC

General | Predefined | Dynamic Rules | IP Services | ICMP Services | IP Protocols | IP Rules

Predefined MAC | MAC Services | MAC Rules

Allow incoming services:

Interface	All	ARP	DCP	IPv4
vlan1 (INT)	☒	☒	☒	☒

Set Values Refresh

Description

- **Interface**

- vlan1

Allows access from the local network (LAN) to the device.

Access over the firewall is permitted to the following MAC services of the device:

- All
All predefined MAC services, no filtering.
- ARP (Address Resolution Protocol)
For access to the device via ARP
Changes to this setting can have the result that the device is no longer reachable.
- DCP (Discovery and Configuration Protocol)
For access to the device with DCP
- IPv4
For access to the device via IPv4

5.11.5.9 MAC services

MUX85x

On this page, you define MAC services to which you can apply MAC firewall rules. You assign a name to the MAC service and define settings for this name. You configure your own MAC rules for the MAC services defined here on the "MAC Rules" tab.

MAC Services

General | Predefined | Dynamic Rules | IP Services | ICMP Services | IP Protocols | IP Rules | Predefined MAC | **MAC Services** | MAC Rules

Name:

Protocol: **ARP**

Select	Name	Protocol	Type/Len	DSAP	SSAP	CTRL	OUI	OUI Type
☐	ARP-Service	ARP	0x0806					
☐	ISO-Service	ISO		0xAA	0xAA	0x00		

2 entries.

[Create](#) [Delete](#) [Set Values](#) [Refresh](#)

Description

The page contains the following:

- **Name**
Assign a name for the MAC service. The name must be unique.
- **Protocol**
Select the protocol for the MAC service to be defined. Selection of the protocol type:

Protocol	Description
ARP	Frames with the following property: Ethertype=0x0806
DCP	The DCP protocol is used by SINEC PNI to set the IP parameters (node initialization) of SIMATIC NET network components.
PNIO	Frames with the following property: Ethertype = 0x8892
ISO	Frames with the following properties: Lengthfield <= 05DC (hex), DSAP=userdefined, SSAP=userdefined, CTRL=userdefined
SNAP	Frames with the following properties: Lengthfield <= 05DC (hex), DSAP=0xAA (hex), SSAP=0xAA (hex), CTRL=0x03 (hex), OUI=userdefined, OUI-Type=userdefined
Users	User-specific rules with the following inputs: Type: >=0x0600 Length: <= 0x05DC
SiClock	For filtering SiCLOCK time-of-day frames.
IPv4	Frames with the following property: Ethertype=0x0800

The table contains the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Name**
Shows the name of the MAC service.
- **Protocol**
Shows the name of the MAC protocol.

5.11 "Security" menu

Depending on the protocol, the following inputs are necessary:

- For Ethernet protocols:
 - Type/length
Range of values with packet type 0x0600 ... 0xFFFF and packet length 0x0040 ... 0x05DC
* (all): Applies to all packet types and lengths.
- For ISO-LLC protocols:

The setting applies to packages with an LLC header which consists of a DSAP (Destination Service Access Point), SSAP (Source Service Access Point) and a control field.

 - DSAP: LLC receiver address
 - SSAP: LLC sender address
 - CTRL: LLC Control Field
- For SNAP:

Applies to VoIP packages. The device checks the source MAC address to determine whether the received package is a language package, which is detected based on the OUI prefix in the source MAC address.

You can specify the OUI settings. The entire data traffic that is received at the voice VLAN ports by the respective IP telephone with a preset OUI is forwarded to the voice VLAN.

 - OUI (Organizationally Unique Identifier): The first three bytes of the MAC address = Manufacturer identification
 - OUI Type: Protocol type/identification

5.11.5.10 MAC rules

MUX85x

On this page, you define your own MAC rules for the Layer 2 firewall. The MAC rules set here have priority over the predefined MAC rules.

By default, MAC packet filter rules exist on the device that permit the exchange of ARP frames between device and vlan1. You can define your own ARP rules by selecting the entry "ARP" as protocol in a MAC packet filter rule. Your own ARP rules should also take into account the PC with which the device is configured.

MAC Rules

General | Predefined | Dynamic Rules | IP Services | ICMP Services | IP Protocols | IP Rules | Predefined MAC | MAC Services | **MAC Rules**

Select	Protocol	Action	From	To	Source	Destination	Service	Log	Prec.▲	Comment
☐	MAC	Accept ▼	vlan1 (INT) ▼	Device ▼	00-00-00-00-00-00	00-00-00-00-00-00	IPv4 ▼	warning ▼	0	
☐	MAC	Drop ▼	nve10 ▼	vlan1 (INT) ▼	00-00-00-00-00-00	00-00-00-00-00-00	DCP ▼	none ▼	1	

2 entries.

Create | Delete | Set Values | Refresh

Meaning

MAC packet filter rules are processed based on the following evaluations:

- Parameters entered in the rule
- Sequence of the rule within the rule set

Description

The table contains the following columns:

- **Select**
Activate the check box in the row to be deleted.
- **Protocol**
Shows the protocol used.
- **Action**
Select how incoming MAC packets are handled:
 - "Drop" – The data packets are discarded without any notification to the sender.
 - "Accept" – The data packets can pass through.
- **From / To**
Specify the communications direction of the MAC rule.
 - vlan1: Local interface (LAN)
 - Device: Device
 - Any: Applies to every interface and client connection, except Device.
 - NVEx: Virtual interface via which the VXLAN tunnel is established.
- **Source**
Enter the source address of the MAC packets.
- **Destination**
Enter the destination address of the MAC packets.
- **Service**
Select the service or the protocol name for which this rule is valid.
- **Log**
Specify whether there should be a log entry every time the rule comes into effect and specify the severity of the event.
The following settings are available:
 - none
The rule coming into effect is not logged.
 - info / warning / critical
The rule coming into effect is logged with the selected event severity. The log file is displayed in "Information > Log Tables > Firewall Log".

5.11 "Security" menu

- **Precedence**
Define the sequence in which the MAC rules of the firewall are processed (ascending from 0 ... 127).
- **Comment**
Enter a comment when necessary.

5.11.6 IPsec VPN

5.11.6.1 General

On this page, you configure the basic settings for VPN.

Internet Protocol Security (IPsec) General

General Remote End Connections Authentication Phase 1 Phase 2

☐ Activate IPsec VPN

Enforce strict CRL Policy: no

NAT Keep Alive Time Interval[s]: 20

IKEv2 DPD Retries: 5

IKEv2 DPD Retry Interval[s]: 25

☐ IKEv2 Make-Before-Break

Set Values Refresh

Description

The page contains the following:

- **Activate IPsec VPN**
Enable or disable the IPsec protocol for VPN.
- **Enforce strict CRL Policy**
 - No
The CRL policy is not adhered to.
 - Yes / Yes if CLR URI defined, else no (IKEv2)
When enabled, the validity of the certificates is checked based on the CRL (Certificate Revocation List). The certificate revocation list lists the certificates issued by the certification authority that have lost their validity before the set expiry date. You configure the certificate revocation list to be used on the WBM page "Certificates (Page 435)".
- **NAT Keep Alive Time Interval[s]**
Specify the time interval at which keep alive telegrams are sent. If there is a NAT device between two VPN endpoints, when there is inactivity, the connection is deleted from its dynamic NAT table. To prevent this, keepalives are sent.

- **IKEv2 DPD retries**
Specify the number of allowed failed attempts after which the IKEv2 connection is considered disrupted. The setting applies to all IKEv2 connections.
- **IKEv2 DPD Retry Interval[s]**
Specify the interval at which the failed attempts are sent.
- **IKEv2 Make-Before-Break**
When enabled, a duplicate of the IKE and all IPSec security assignments is created and the old ones are deleted. This prevents interruptions in VPN communication from occurring during reauthentication. This setting requires that both VPN endpoints can process overlapping SAs.

5.11.6.2 Remote End

On this page, you configure the remote partner VPN end point.

Internet Protocol Security (IPsec) Remote End Settings

General Remote End Connections Authentication Phase 1 Phase 2

Remote End Name:

Select	Name	Remote Mode	Remote Type	Remote Address	Remote Subnet	Virtual IP Mode	Virtual IP
☐	CP1628	Standard	manual	192.168.184.0/24	192.168.184.0/24	none	

1 entry.

Create Delete Set Values Refresh

Description

The page contains the following:

- **Remote End Name**
Enter the name of the remote station and click "Create" to create a new remote station.
- **Select**
Select the check box in the row to be deleted.
- **Name**
Shows the name of the partner.
- **Remote Mode**
Specify the role the remote stations will adopt.
 - Roadwarrior
The reachable remote addresses are entered. The reachable remote subnets are learned from the partner.
 - Standard
The reachable remote address and the reachable remote subnets are entered permanently.

- **Remote Type**
Specify the type of remote station address.
 - Manual
The address of the partner is known. The device can either establish the VPN connection actively as a VPN client or wait passively for connection establishment by the partner.
 - Any
Accepts the connection from remote stations with any IP address. The device can only wait for VPN connections but cannot establish a VPN tunnel as the active partner.
- **Remote Address**
Can only be edited with the remote type "Manual".
 - In standard mode, enter the WAN IP address or the DDNS hostname of the partner. The network mask is always /32.
 - In Roadwarrior mode, you can specify either the address of the partner or enter an IP range from which connections will be accepted.
- **Remote Subnet**
 - In standard mode, enter the remote subnet of the remote station. Use the CIDR notation. Multiple subnets can be used only with IKEv2. The enter the subnets separated by a comma.
 - In Roadwarrior mode, the remote address informs the device of its accessible subnets and the device learns them.
- **Virtual IP Mode**
Specify whether or not the remote station is offered a virtual IP address.
The following options are available:
 - User defined IPv4
The virtual IP address is from the band specified in "Virtual IP".
 - None
No virtual IP address. The VPN tunnel is established dynamically to the internal IP address of the remote station.
- **Virtual IP address**
Specify the subnet (CIDR) from which the remote station is offered a virtual IP address.
Can only be edited if "user defined IPv4" is selected in "Virtual IP Mode".

Procedure

Configure VPN standard mode

1. Enter the name of the remote end in "Remote End Name".
2. Click the "Create" button.
A new entry is generated in the table.
3. For "Remote Mode", select "Standard".
4. For "Remote Type", select "Manual".
5. Enter the WAN IP address in "Remote Address" and the subnet of the remote end in "Remote Subnet".
6. Click the "Set Values" button.

Configure VPN Roadwarrior mode

1. Enter the name of the remote end in "Remote End Name".
2. Click the "Create" button.
A new entry is generated in the table.
3. For "Remote Mode", select "Roadwarrior".
4. For "Remote Type", select "Any".
5. For "Remote Address", enter the IP address of the remote network.
6. In "Virtual IP Mode", specify how the IP address of the VPN gateway is obtained.
7. Click the "Set Values" button.

5.11.6.3 Connections

On this page, you configure the basic settings for the VPN connection. With these settings, the device (local endpoint) can establish a secure VPN tunnel to the partner. You specify the security settings on the WBM page "Authentication".

Note**Several IPsec VPN connections via the same VPN endpoint**

If you have created IPsec VPN connections to different remote subnets via the same VPN endpoint, the first configured VPN connection (lowest index) is the main connection (parent).

Via the main connection all other IPsec VPN connections (children) are created and established. If all VPN tunnels are now established and the main (parent) connection is terminated, all child connections are interrupted. After the DPD timeout has expired, all IPsec VPN connections are reestablished via the main connection.

If only one child connection is terminated, the parent connection and the other child connections are retained.

Note**IPsec: Restrictions for phase 2 connections**

Create a maximum of 20 phase 2 connections per phase 1 (remote endpoint).

Note

If you use "NETMAP",

- only auto firewall rules are supported.
 - The setting "on demand" cannot be selected for "Operation"
-

Internet Protocol Security (IPsec) Connection Settings

?

GeneralRemote EndConnectionsAuthenticationPhase 1Phase 2

Connection Name:

Select	Name	Operation	Keying Protocol	Tunnel Interface	Remote End	Local Subnet	Request Virtual IP	Timeout[min]
☐	VPN-1	disabled	IKEv2	auto	test	192.168.11.0/24	☐	0

1 entry.

CreateDeleteSet ValuesRefresh

Description

- The page contains the following boxes:
- Connection Name**
Enter a name for the VPN connection and click "Create" to create a new connection.
- The table contains the following columns:
- Select**
Select the check box in the row to be deleted.
 - Name**
Shows the name of the VPN connection.

- **Operation**

Specify who establishes the VPN connection. You will find more detailed information in "Technical basics > VPN connection establishment (Page 96)".

- Disabled
The VPN connection is disabled.
- start
The device attempts to establish a VPN connection to the partner.
- wait
The device waits for the partner to initiate the connection.
- on demand
The VPN connection is established when necessary.
- Start on DI
If the event "Digital In" occurs, the device attempts to establish a VPN connection to the partner.
This is on condition that the event "Digital In" is forwarded to the VPN connection. To do this, enable "VPN Tunnel" for the "Digital In" event under "System > Events > Configuration".
- wait on DI
If the event "Digital In" occurs, the device waits for the partner to initiate connection establishment.
This is on condition that the event "Digital In" is forwarded to the VPN connection. To do this, enable "VPN Tunnel" for the "Digital In" event under "System > Events > Configuration".
- Start on SMS (only with M87x / RM1224 / MUX85x)
If the device receives a command SMS, the device attempts to establish a VPN connection to the remote station. This assumes that the device accepts a command SMS of the class "System" from certain senders. You configure the senders in "System > SMS > SMS Command".
- Wait on SMS (only with M87x / RM1224 / MUX85x)
When the device receives an SMS command, the device waits until the connection establishment is initiated by the remote station. This assumes that the device accepts a command SMS of the class "System" from certain senders. You configure the senders in "System > SMS > SMS Command".
- start on Action
If the "VPN Reset" or "VPN enable" actions are triggered, the device attempts to establish a VPN connection to the partner. For this purpose, you configure the corresponding action under "System > Connection Check".
- wait on Action
If the "VPN Reset" or "VPN enable" actions are triggered, the device waits for the partner to initiate connection establishment. For this purpose, you configure the corresponding action under "System > Connection Check".
- start on TCP
If the incoming TCP packet contains conformant data, the device attempts to establish a VPN connection to the partner. The prerequisite is that the "VPN" event is enabled under "System > TCP Event".

5.11 "Security" menu

- wait on TCP
If the incoming TCP packet contains conformant data, the device waits until the connection establishment is initiated by the partner. The prerequisite is that the "VPN" event is enabled under "System > TCP Event".
- Start on GPS (only with MUM85x)
If the "IPsec (all) enable" action is triggered, the device attempts to establish a VPN connection to the partner. For this purpose, you configure the corresponding action under "System > GPS > Geofencing".
- Wait on GPS (only with MUM85x)
If the "IPsec (all) enable" action is triggered, the device waits for the partner to initiate connection establishment. For this purpose, you configure the corresponding action under "System > GPS > Geofencing".
- **Keying Protocol**
Specify whether IKEv2 or IKEv1 will be used.
- **Tunnel Interface**
Specify the interface via which the VPN connection is established.
 - auto
The interface is specified automatically.
 - vlan1
For access from the local network (LAN) to the device
 - ppp0 or usb0 (only with M87x / RM1224 / MUX85x)
Access from the mobile wireless interface to the device.
- **Remote End**
Select the required remote station. Only remote stations that have been configured on the "Remote End" WBM page can be configured.
- **Local Subnet**
Enter the local subnet. Use the CIDR notation. The local network can also be a single PC or another subset of the local network.
Multiple subnets can be used only with IKEv2. The enter the subnets separated by a comma.
- **Request virtual IP address**
When enabled, a virtual IP address is requested from the remote station during connection establishment.
- **Timeout[min]**
Specify the period of time in minutes. If no data exchange takes place, when this time has elapsed the VPN tunnel is automatically terminated.

5.11.6.4 Authentication

On this WBM page, you specify how the VPN connection partners authenticate themselves with each other.

Internet Protocol Security (IPsec) Authentication Settings

GeneralRemote EndConnectionsAuthenticationPhase 1Phase 2

Name	Authentication	CA Certificate	Local Certificate	Local ID	Remote Certificate	Remote ID	PSK	PSK Confirmation
VPN-1	PSK	-	-		-	162.168.184.2	*****	*****

Set ValuesRefresh

Description

This table contains the following columns:

- Name**
Shows the name of the VPN connection to which the settings relate.
- Authentication**
Select the authentication method. For the VPN connection, it is essential that the partner uses the same authentication method.
 - Disabled
No authentication method is selected. Connection establishment is not possible.
 - Remote Cert
The remote certificate is used for authentication. You specify the certificate in "Remote Certificate"
 - CA Cert
The certificate of the certification authority is used for authentication. You specify the certificate in "CA Certificate".
 - PSK
A key is used for authentication. You configure the key in "PSK".

Note

For this "PSK" authentication method, specify the "Local ID" and "Remote ID". If the entries remain empty, IPsec uses the IP address of the interface as the ID and prevents the VPN tunnel from being set up.

- CA Certificate**
Select the certificate. Only loaded certificates can be selected.
- Local Certificate**
Select the machine certificate.
You load the certificates on the device with "System > Load&Save". The loaded certificates and key files are shown on the WBM page "Security > Certificates".

- **Local ID**
Enter the local ID from the partner certificate. Only when you use the partner certificate can you leave the box empty. The box is automatically filled with the value from the partner certificate.
- **Remote Certificate**
Select the remote station certificate. Only loaded remote certificates can be selected. You load the certificates on the device with "System > Load&Save". The loaded certificates and key files are shown on the WBM page "Security > Certificates".
- **Remote ID**
Enter the "Distinguished Name" or "Alternate Name" from the partner certificate. Only when you use the partner certificate can you leave the box empty. The box is automatically filled with the value from the partner certificate.
- **PSK**
Enter the key.
- **PSK Confirmation**
Repeat the key.

5.11.6.5 Phase 1

Phase 1: Encryption agreement and authentication (IKE = Internet Key Exchange)

On this WBM page, you set the parameters for the protocol of the IPsec key management. The key exchange uses the standardized IKE method for which you can set the following protocol parameters.

Internet Protocol Security (IPsec) Phase 1 Settings

General	Remote End	Connections	Authentication	Phase 1	Phase 2																						
<table border="1"> <thead> <tr> <th>Name</th> <th>Default Ciphers</th> <th>Encryption</th> <th>Authentication</th> <th>Key Derivation</th> <th>Keying Tries</th> <th>Lifetime [min]</th> <th>DPD</th> <th>DPD Period [sec]</th> <th>DPD Timeout [sec]</th> <th>Aggressive Mode</th> </tr> </thead> <tbody> <tr> <td>VPN-1</td> <td>☒</td> <td>AES128 GCM 16 ▾</td> <td>SHA256 ▾</td> <td>DH group 14 ▾</td> <td>0</td> <td>180</td> <td>☒</td> <td>30</td> <td>150</td> <td>☐</td> </tr> </tbody> </table>						Name	Default Ciphers	Encryption	Authentication	Key Derivation	Keying Tries	Lifetime [min]	DPD	DPD Period [sec]	DPD Timeout [sec]	Aggressive Mode	VPN-1	☒	AES128 GCM 16 ▾	SHA256 ▾	DH group 14 ▾	0	180	☒	30	150	☐
Name	Default Ciphers	Encryption	Authentication	Key Derivation	Keying Tries	Lifetime [min]	DPD	DPD Period [sec]	DPD Timeout [sec]	Aggressive Mode																	
VPN-1	☒	AES128 GCM 16 ▾	SHA256 ▾	DH group 14 ▾	0	180	☒	30	150	☐																	
1 entry.																											
Set Values Refresh																											

Description

The table contains the following columns:

- **Name**
Shows the name of the VPN connection to which the settings relate.
- **Default Ciphers**
When enabled, a preset list is transferred to the VPN connection partner during connection establishment. The list contains a combination of the three algorithms (Encryption, Authentication, Key Derivation). To establish a VPN connection, the VPN connection partner must support at least one of the combinations. The selection depends on the key exchange method. Additional information can be found in the section "IPsec VPN (Page 92)".

- **Encryption**

For phase 1, select the required encryption algorithm. Can only be selected if "Default Ciphers" is disabled.

The selection depends on the key exchange method. Additional information can be found in the section "IPsec VPN (Page 92)".

Note

The AES modes CCM and GCM contain separate mechanisms for authenticating data. If you use a mode AES x CCM for "Encryption", this is also used for authentication. Then only the pseudo random function will be derived from the "Authentication" parameter. So that a VPN connection can be established, all devices need to use the same settings.

- **Authentication**

Specify the method for calculating the checksum. Can only be selected if "Default Ciphers" is disabled.

The following methods are supported:

- MD5
- SHA1
- SHA512
- SHA256
- SHA384

- **Key derivation**

Select the required Diffie-Hellmann group (DH) from which a key will be generated. Can only be selected if "Default Ciphers" is disabled.

The following DH groups are supported:

- DH group 1
- DH group 2
- DH group 5
- DH group 14
- DH group 15
- DH group 16
- DH group 17
- DH group 18

- **Keying Tries**

Enter the number of repetitions for a failed connection establishment. If you enter the value 0, the connection establishment will be attempted endlessly.

- **Lifetime [min]**

Enter a period in minutes to specify the lifetime of the authentication. When the time has elapsed, the VPN endpoints involved must authenticate themselves with each other again and generate a new key

5.11 "Security" menu

- **DPD**

When enabled, DPD (Dead Peer Detection) is used. Using DPD, it is possible to find out whether the VPN connection still exists or whether it has aborted.

Note

Sending DPD queries increases the amount of data sent and received. This can lead to increased costs.

- **DPD Period [sec]**

Enter the period after which DPD requests are sent. These queries test whether or not the remote station is still available

- **DPD Timeout [sec]**

Only adjustable for IKEv1. For IKEv2, configure the setting under "Security > IPsec > General". Enter a period. If there is no response to the DPD queries, the connection to the remote station is declared to be invalid after this time has elapsed.

Note

To avoid unwanted connection breakdowns, set the DPD timeout significantly higher than the DPD period. We recommend setting it at least 2 minutes longer than the DPD period.

- **Aggressive Mode**

- Disabled:
Main Mode is used.
- Enabled
Aggressive Mode is used

The difference between main and aggressive mode is the "identity protection" used in main mode. The identity is transferred encrypted in main mode but not in aggressive mode.

5.11.6.6 Phase 2

Phase 2: Data exchange (ESP = Encapsulating Security Payload)

On this WBM page, you set the parameters for the protocol of the IPsec data exchange. The entire communication during this phase is encrypted using the standardized security protocol ESP for which you can set the following protocol parameters.

Internet Protocol Security (IPsec) Phase 2 Settings

General	Remote End	Connections	Authentication	Phase 1	Phase 2																				
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #f0f0f0;"> <th>Name</th> <th>Default Ciphers</th> <th>Encryption</th> <th>Authentication</th> <th>Key Derivation (PFS)</th> <th>Lifetime [min]</th> <th>Lifeytes</th> <th>Protocol</th> <th>Port (Range)</th> <th>Auto Firewall Rules</th> </tr> </thead> <tbody> <tr> <td>VPN-1</td> <td>☒</td> <td>AES128 GCM 16 ▾</td> <td>SHA256 ▾</td> <td>DH group 14 ▾</td> <td>60</td> <td>0</td> <td>*</td> <td>*</td> <td>☒</td> </tr> </tbody> </table>						Name	Default Ciphers	Encryption	Authentication	Key Derivation (PFS)	Lifetime [min]	Lifeytes	Protocol	Port (Range)	Auto Firewall Rules	VPN-1	☒	AES128 GCM 16 ▾	SHA256 ▾	DH group 14 ▾	60	0	*	*	☒
Name	Default Ciphers	Encryption	Authentication	Key Derivation (PFS)	Lifetime [min]	Lifeytes	Protocol	Port (Range)	Auto Firewall Rules																
VPN-1	☒	AES128 GCM 16 ▾	SHA256 ▾	DH group 14 ▾	60	0	*	*	☒																
1 entry.																									
Set Values Refresh																									

Description

The table contains the following columns:

- **Name**
Shows the name of the VPN connection to which the settings relate.
- **Default Ciphers**
When enabled, a preset list is transferred to the VPN connection partner during connection establishment. The list includes combinations of the three algorithms (encryption, authentication, key derivation). To establish a VPN connection, the VPN connection partner must support at least one of the combinations. Further information can be found in the section "IPsec VPN (Page 92)".
- **Encryption**
For phase 2, select the required encryption algorithm. Can only be selected if "Default Ciphers" is disabled.
Further information can be found in the section "IPsec VPN (Page 92)".

Note

The AES modes CCM and GCM contain separate mechanisms for authenticating data. If you use a mode AES x CCM or AES x GCM for "Encryption", this will also be used for authentication. Then only the pseudo random function will be derived from the "Authentication" parameter.

- **Authentication**
Specify the method for calculating the checksum. Can only be selected if "Default Ciphers" is disabled.
The following methods are supported:
 - MD5
 - SHA1
 - SHA512
 - SHA256
 - SHA384

5.11 "Security" menu

- **Key Derivation (PFS)**

The device supports Diffie-Hellmann key exchange (DH) with the Perfect Forward Secrecy (PFS) property.

Select the desired DH group from which a key is generated. Can only be selected if "Default Ciphers" is disabled.

The following DH groups are supported:

- None: For phase 2, no separate keys are exchanged. This disables PFS.
- DH group 1
- DH group 2
- DH group 5
- DH group 14
- DH group 15
- DH group 16
- DH group 17
- DH group 18

Note

So that a VPN connection can be established, all devices need to use the same settings or provide compatible key procedures..

- **Lifetime [min]**

Enter a period in minutes to specify the lifetime of the agreed keys. When the time expires, the key is renegotiated.

- **Lifeytes**

Enter the data limit in bytes that specifies the lifetime of the agreed key. When the data limit is reached, the key is renegotiated.

- **Protocol**

Specify the protocol for which the VPN connection is valid e.g. UDP, TCP, ICMP. If the setting is intended to apply to all protocols, enter "**".

- **Port (Range)**

Specify the port via which the VPN tunnel can communicate. The setting applies specifically to the specified port

- 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 setting is intended to apply to all ports, enter "*".

The setting is only effective for port-based protocols.

- **Auto Firewall Rules**

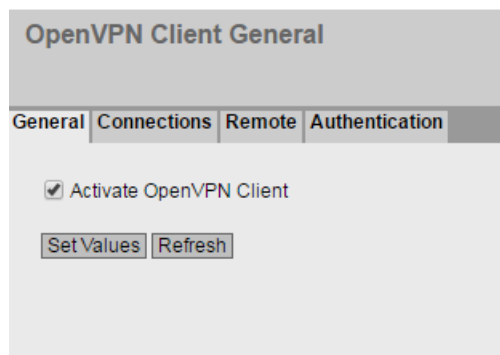
- Enabled
For the VPN connection, the firewall rules for access from "External" to "Internal" and vice versa are created automatically. You can enable access to specific services of the device under "Security > Firewall > Predefined IPv4". Ping is enabled by default.
- Disabled
You will need to create the firewall rules yourself.

5.11.7 OpenVPN



5.11.7.1 General

On this page, you activate the OpenVPN client.



Description

The page contains the following:

- **Activate OpenVPN**
Enable or disable the OpenVPN client.

5.11.7.2 Connections

On this page, you configure the basic settings for the OpenVPN connection. You specify the security settings on the WBM page "Authentication".

OpenVPN Connection Settings

GeneralConnectionsLocal ClientAuthentication

Connection Name:

Select	Name	Operation	Encryption	Authentication	LZO Comp.	Auto Firewall Rules	Enable NAT	Timeout[min]
☐	To_M826	disabled	AES128 GCM	SHA256	-	☒	☐	0

1 entry.

CreateDeleteSet ValuesRefresh

Description

- Connection Name**
Enter a unique name for the OpenVPN connection and click "Create" to create a new connection.
- The table contains the following columns:
- Select**
Select the check box in the row to be deleted.
 - Name**
Shows the name of the OpenVPN connection.

- **Operation**

Specify how the VPN connection is established. You will find more detailed information in "Technical basics > VPN connection establishment (Page 96)".

- start
The device attempts to establish a VPN connection to the partner.
- Start on DI
If the event "Digital In" occurs, the device attempts to establish a VPN connection to the partner.
This is on condition that the event "Digital In" is forwarded to the VPN connection. To do this, enable "VPN Tunnel" for the "Digital In" event under "System > Events > Configuration".
- Start on SMS (only with M87x / RM1224 / MUX85x)
If the device receives a command SMS, the device attempts to establish a VPN connection to the partner. This assumes that the device accepts a command SMS of the class "System" from certain senders. You configure the senders in "System > SMS > SMS Command".
- start on Action
If the "VPN Reset" or "VPN enable" actions are triggered, the device attempts to establish a VPN connection to the partner. For this purpose, you configure the corresponding action under "System > Connection Check".
- start on TCP
If the incoming TCP packet contains conformant data, the device attempts to establish a VPN connection to the partner. The prerequisite is that the "VPN" event is enabled under "System > TCP Event".
- Start on GPS (only with MUM85x)
If the "OpenVPN (all) enable" action is triggered, the device attempts to establish a VPN connection to the partner. For this purpose, you configure the corresponding action under "System > GPS > Geofencing".
- Disabled
The VPN connection is disabled.

- **Encryption**

Select the required encryption algorithm.

- AES128 CBC (default)
- AES192 CBC
- AES256 CBC
- DES EDE3
- BF CBC
- AES128 GCM
- AES128 CBC

5.11 "Security" menu

- **Authentication**
Specify the method for calculating the checksum.
 - SHA256 (default)
 - SHA384
 - SHA512
 - SHA224
 - SHA1
 - MD5
- **LZO Comp.**
 - Disabled (-)
The compression is disabled. The server cannot enable compression again.
 - No
The compression is disabled as default. The server can enable compression
 - Yes
The compression is enabled as default. The server can disable the compression
 - Adaptive
Adaptive compression is enabled by default. Compression is only used when the data is good to compress; otherwise, compression is disabled for a certain time.
- **Auto Firewall Rules**
 - Enabled
For the VPN connection, the firewall rules for access of OpenVPN to all existing VLANs and vice versa are created automatically. In addition to this, access from the device to the outside is allowed. You can enable access to specific services of the device under "Security > Firewall > Predefined IPv4". Ping is enabled by default.
 - Disabled
You will need to create the suitable firewall rules yourself.
- **Enable NAT**
With this setting, you enable automatic IP masquerading for this interface. The local devices are not directly reachable from the outside, but only via the IP address of the interface. The local devices can, however, connect to the devices downstream from the OpenVPN server. You will find more information on NAT in "Technical basics > NAT (Page 88)"
- **Timeout [min]**
Specify the period of time in minutes. If no data exchange takes place, when this time has elapsed the VPN tunnel is automatically terminated.

5.11.7.3 Local client

On this WBM page, you configure the partner (OpenVPN end point). Per connection, you can specify several OpenVPN partners. The device tries all configured OpenVPN partners one after the other until a connection is successfully established.

OpenVPN Remote End Settings

General

Connections

Local Client

Authentication

Client Name:

Select	Name	Connection	Server Address	Port	Protocol	Proxy
☐	Client1	none		1194	udp	none

1 entry.

Create

Delete

Set Values

Refresh

Description

The page contains the following:

- Client Name**
Enter a name for the OpenVPN remote partner and click "Create" to create a new partner.
- The table contains the following columns:
 - Select**
Select the check box in the row to be deleted.
 - Name**
Shows the name of the Open VPN partner.
 - Connection**
Select the corresponding connection. Only connections can be configured that have been configured on the "Connections" WBM page.
 - Server Address**
Enter the WAN IP address or the DNS host name of the OpenVPN partner.
 - Port**
Specify the port via which the OpenVPN tunnel can communicate. The setting applies specifically to the specified port.
 - Protocol**
Specify the protocol for which the OpenVPN connection will be used.
 - UDP
 - TCP
 - Proxy**
Specify whether the OpenVPN tunnel to the defined OpenVPN partner is established via a proxy server. Only the proxy servers can be selected that you configured in "System > Proxy Server".

5.11.7.4 Authentication

On this WBM page, you specify how the VPN connection partners authenticate themselves with each other.

OpenVPN Authentifizierungs-Einstellungen

Allgemein Verbindungen Client **Authentifizierung**

Name	TLS-Auth. Key	Richtung	Methode	CA-Zertifikat	Gerätezertifikat	Benutzername	Passwort	Passwort bestätigen
M826	-	none	Deaktiviert	-	-			

[Einstellungen übernehmen](#) [Aktualisieren](#)

Description

This table contains the following columns:

- **Name**
Shows the name of the VPN connection to which the settings relate.
- **TLS Auth. Key**
Select the key file used to sign the TLS packets. If the incoming TLS packets are not signed with this key, they are discarded.
- **Direction**
Specify the direction. If you select 0, 1 must be set on the partner and vice versa. With this setting, you restrict the clients that can authenticate themselves.
Select "none" if nothing is set on the OpenVPN server. With "none", this setting is disabled.
- **Method**
Select the authentication method. For the VPN connection, it is essential that the partner uses the same authentication method.
 - Disabled
No authentication method is selected. Connection establishment is not possible.
 - Certificates
Certificates are used for the authentication.
 - User Name/Password
The user name / password are used for the authentication.
 - Cert/User Name/Password
For authentication, a user name and password are required in addition to the certificate. The VPN connection is established only if both operations are successful.
- **CA Certificate**
Select the certificate. Only loaded certificates can be selected.
You load the certificates on the device with "System > Load&Save". The loaded certificates and key files are shown on the WBM page "Security > Certificates".
- **Machine certificate**
Select the machine certificate. Only loaded certificates can be selected.
You load the certificates on the device with "System > Load&Save". The loaded certificates and key files are shown on the WBM page "Security > Certificates".

- **User Name**
Specify the user name.
- **Password**
Enter the password.
- **Password Confirmation**
Repeat the password.

5.11.7.5 Server

On this WBM page, you can create multiple OpenVPN servers per connection.

OpenVPN Server Configuration

General

Connections

Local Client

Authentication

Server

Remote Client

Remote Client Subnet

Server Name:

Select	Name	Connection	OpenVPN Subnet	Max. Clients	Port	Protocol
☐	Server1	Connection1	0.0.0.0/0	128	1194	udp

1 entry.

Create

Delete

Set Values

Refresh

Description

The page contains the following:

- **Name**
Enter a name for the OpenVPN server and click "Create".

The table contains the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Name**
Shows the name of the OpenVPN server.
- **Connection**
Select the corresponding connection. Only connections can be configured that have been configured on the "Connections" WBM page.
- **OpenVPN subnet**
IP address range from which the OpenVPN clients connected to the server obtain their tunnel IP address. The first IP address of this range is assigned to the OpenVPN server.
- **Max. Clients**
Select the maximum number of clients to which the server can establish a connection at the same time.
- **Port**
Specify the port via which the OpenVPN tunnel can communicate. The setting applies specifically to the specified port.
- **Protocol**
Specify the protocol for which the OpenVPN connection will be used.

5.11.7.6 Remote client

On this page, you define which OpenVPN clients are permitted to connect to the server.

Client Config File

General

Connections

Local Client

Authentication

Server

Remote Client

Remote Client Subnet

Cert Common Name:

Select

Cert Common Name

Description

☐

Certificate1

1 entry.

Create

Delete

Set Values

Refresh

Description

The page contains the following:

- Cert CN**
Enter the "Common Name" from the certificate of the OpenVPN client which is to connect to the server. Then click "Create".

The table contains the following columns:

- Select**
Select the check box in the row to be deleted.
- Cert CN**
Shows the "Common Name" from the client certificate.
- Description**
Enter a description for the "Common Name".

5.11.7.7 Remote client subnet

On this page, you specify the remote subnets in which the server is permitted to communicate.

Client Subnet Config

General

Connections

Local Client

Authentication

Server

Remote Client

Remote Client Subnet

Cert Common Name:

none

Select

Cert Common Name

Subnet Addr

Description

☐

Certificate1

192.168.16.10/32

1 entry.

Create

Delete

Set Values

Refresh

Description

The page contains the following:

- **Cert CN**
Select the "Common Name" of the client for which you want to define the subnet to be reached.

The table contains the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Cert CN**
Shows the selected "Common Name".
- **Subnet Address**
Enter the address of the subnet to be connected to the server.
- **Description**
Shows the description for the "Common Name".

5.11.8 Brute Force Prevention

Brute Force Prevention (BFP) refers to the protection of the device from unauthorized access by trying a sufficiently large number of passwords. The number of incorrect login attempts within a specific time period is limited for this purpose.

Brute Force Prevention

User Specific BFP is Enabled

Acceptable Invalid Login Attempts Per User: 12

IP Specific BFP is Enabled

Acceptable Invalid IP Login Attempts Per IP: 10

Global Parameters

BFP Trigger Interval[min]: 5

BFP Automatic Reset Timer[min]: 12

User Specific BFP:

User	Failed Logins	Last Failed[s]	Blocked[s]	Clear
Unknown User	0	0	not blocked	Clear
admin	0	0	not blocked	Clear
1	0	0	not blocked	Clear

3 entries.

IP Specific BFP:

IP	Failed Logins	Last Failed[s]	Blocked[s]	Clear
192.168.16.20	0	0	not blocked	Clear

Set Values

Refresh

Description

The page contains the following boxes:

- **User Specific BFP is Enabled. / User Specific BFP is Disabled.**
 - Enabled:
With login authentication, the "Local" or "Local and RADIUS" mode is set and the maximum number of invalid login attempts is greater than 0.
 - Disabled:
With login authentication, the "RADIUS" or "RADIUS and fallback Local" mode is set or the maximum number of invalid login attempts is 0.

You configure the login authentication under "Security > AAA > General > Login Authentication".
- **Acceptable Invalid Login Attempts Per User**
The maximum number of invalid login attempts for a user accepted by the device. Further login attempts for this user are blocked for a specific time.
The users that are not configured as local users for the device are summarized under the user name "UnknownUser".
0: User Specific BFP is Disabled.
- **IP Specific BFP is Enabled. / IP Specific BFP is Disabled.**
Shows whether the IP-specific Brute Force Prevention is enabled.
- **Acceptable Invalid IP Login Attempts Per IP**
The maximum number of invalid login attempts for an IP address accepted by the device. Further login attempts for this IP address are blocked for a specific time.
0: IP Specific BFP is Disabled.
- **BFP Trigger Interval [min]**
The time in minutes that is relevant for counting invalid login attempts.
If the maximum number of invalid login attempts is exceeded during this time, the device blocks login for a specific period of time.
Invalid login attempts per user and per IP address are handled independently of one another.
- **BFP Automatic Reset Timer[min]**
Time in minutes for which the device blocks login because the maximum number of invalid login attempts was exceeded.
0: The timer is disabled.

The **User Specific BFP** table has the following columns:

- **User**
The users configured locally on the device. The users that are not locally configured on the device are summarized under the user name "UnknownUser".
- **Failed Logins**
The number of failed login attempts.
- **Last Failed[s]**
Time in seconds since the last failed login attempt. To display the current value, click the "Refresh" button.

- **Blocked[s]**
The time in seconds until the blocking will be removed. To display the current value, click the "Refresh" button.
When a blocked user attempts to log in before the timer expires, the timer restarts.
- **Delete**
Ends blocking for the user and resets the displays in the "Last Failed[s]" and "Blocked[s]" boxes.

The **IP Specific BFP** table has the following columns:

- **IP**
The IP address of the device for the login attempt.
- **Failed Logins**
The current number of failed login attempts.
- **Last Failed[s]**
Time in seconds since the last failed login attempt. To display the current value, click the "Refresh" button.
- **Blocked[s]**
The time in seconds until the blocking will be removed. To display the current value, click the "Refresh" button.
When a blocked IP address attempts to log in before the timer expires, the timer restarts.
- **Delete**
Ends blocking for the IP address and resets the displays in the "Last Failed[s]" and "Blocked[s]" boxes.

Upkeep and maintenance

Firmware

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

6.1 Device configuration with PRESET-PLUG

Please not the additional information and security notes in the operating instructions of your device.

NOTICE
Do not remove or insert a PLUG during operation
A PLUG may only be removed or inserted when the device is turned off.

Note**Support as of V4.3**

The PRESET-PLUG functionality is supported as of firmware version V4.3.

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.

6.1 Device configuration with PRESET-PLUG

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 CLI and log on as a user with the "admin" role. The CLI connection works either with Telnet (port 23) or SSH (port 22).
2. Switch to the global configuration mode with the command "configure terminal".
3. You change to the PLUG configuration mode with the "plug" command.
4. Create the PRESET-PLUG with the "presetplug" command.
The firmware version of the device and the current device configuration incl. user accounts and certificates are stored on the PLUG and the PLUG is then write protected.
5. Turn off the power to the device.
6. Remove the PRESET-PLUG.
7. Start the device either with a new 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/0.2 sec off). Afterwards the device is restarted and the device configuration incl. users and certificates on the PRESET-PLUG is transferred to the device.
5. Wait until the device has fully started up.
(the red F-LED is off)
6. Turn off the power to the device after the installation.
7. Remove the PRESET-PLUG.
8. Start the device either with a new 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 with factory settings.

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.

Formatting a PRESET-PLUG (resetting the preset function)

You format the PRESET PLUG using the Command Line Interface (CLI) to reset the preset function. To do this, follow the steps outlined below:

1. Start the remote configuration using Telnet (CLI) and log on with a user with the "admin" role.
2. Switch to the global configuration mode with the command "configure terminal".
3. You change to the PLUG configuration mode with the "plug" command.
4. Enter the command "factoryclean".
The PRESET-PLUG is formatted and the preset function is reset.
5. Write the current configuration of the device with the "write" command.

6.2 Firmware update - via WBM

Requirement

- The device has an IP address.
- The user is logged in with administrator rights.

Firmware update using HTTP

1. Click "System > Load&Save" in the navigation area. Click the "HTTP" tab.
2. Click the "Loading" button next to "Firmware".
3. Go to the storage location of the firmware file.
4. Click the "Open" button in the dialog.

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.

6.3 Firmware update via WBM and CLI not possible

5. Go to the storage location of the firmware file.
6. Click the "Open" button in the dialog. The file is uploaded.

Firmware update via SFTP

1. Click "System > Load&Save" in the navigation area. Click the "SFTP" tab.
2. Enter the IP address of the SFTP server in the "SFTP Server Address" input box.
3. Enter the port of the SFTP server in the "SFTP Server Port" input box.
4. Enter the user and the password for access to the SFTP server.
5. Click the "Load file" button in the "Firmware" table row.
6. Go to the storage location of the firmware file.
7. Click the "Open" button in the dialog. The file is uploaded.

Result

When the firmware is successfully loaded a dialog is displayed. Confirm the dialog with "OK". The device is restarted.

In "Information > Versions" there is the additional entry "Firmware_Running". Firmware_Running shows the version of the current firmware. Firmware shows the firmware version stored after loading the firmware.

Version Information			
Hardware	Name	Revision	Order ID
Basic Device	SCALANCE M874-3	3	6GK5 874-3AA00-2AA2
CELL	CELL Module	03.001-01.000.01	-
Software	Description	Version	Date
Firmware	SCALANCE M800/S615 Firmware	V05.00.00	11/13/2017 20:00:00
Bootloader	SCALANCE M800 Bootloader	V01.05.00	08/02/2017 16:30:00
Firmware_Running	Current running Firmware	V05.00.00	11/13/2017 20:00:00
Refresh			

6.3 Firmware update via WBM and 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 WBM and CLI.

Requirement

- The PC is connected to the device via the interface.
- A TFTP client is installed on the PC and the firmware file exists.

Solution

You can then also transfer firmware to the device using TFTP.
Follow the steps below to load new firmware using TFTP:

1. Now press the SET button.
2. Hold down the button until the red fault LED (F) starts to flash after approximately 3 seconds.

Note

If you hold down the SET button for approximately 10 seconds, the device is reset to its factory settings and can be reached with the IP address 192.168.1.1.

3. Now release the button. The bootloader waits in this state for new firmware file that you can download by TFTP.

Note

If you want to exit the boot loader without making changes, press the SET button briefly. The device restarts with the loaded configuration.

4. Connect a PC to the device over the Ethernet interface.
5. Open a DOS box and change to the directory where the new firmware file is located and then execute the command "tftp -i <ip address> PUT <firmware>". As an alternative, you can use a different TFTP client.
If you are not sure that the IP address is correct, you can check this, for example with SINEC PNI.

Note

Use of CLI and TFTP in Windows 10

If you want to access the CLI or TFTP in Windows 10, make sure that the relevant functions are enabled in Windows 10.

Result

The firmware is transferred to the device.

Note

Please note that the transfer of the firmware can take several minutes. During the transmission, the red error LED (F) flashes.

Once the firmware has been transferred completely to the device, the device is restarted automatically.

6.4 Restoring the factory settings

NOTICE
Previous settings If you reset, all the settings you have made will be overwritten by factory defaults. The protected defaults are also reset. Created eSIM profiles are deleted on SCALANCE MUX85x.

NOTICE
Inadvertent reset An inadvertent reset can cause disturbances and failures in a configured network with further consequences.

With the reset button

When pressing the button, make sure you follow the instructions in the section "Reset button".

Follow the steps below to reset the device parameters to the factory settings:

1. Turn off the power to the device.
2. Now press the Reset button and reconnect the power to the device while holding down the button.
3. Hold down the button until the red fault LED (F) stops flashing after approximately 10 seconds and is permanently lit.
4. Now release the button and wait until the fault LED (F) goes off again.
5. The device then starts automatically with the factory settings.
SCALANCE MUX85x: Do not switch off the device until it has finished restarting. If the device is switched off while it is restarting, eSIM profiles may not be fully deleted. As a result, no message is sent to the mobile network provider about the eSIM to be released. In this case, you must order a new eSIM for your mobile plan.

Via the configuration

You will find detailed information on resetting the device parameters using the WBM and CLI in the configuration manuals:

- Web Based Management, section "Restart"
- Command Line Interface, section "Reset and Defaults"

Appendix A "SMS command"

A.1 Command SMS message

With a command SMS message, you can send commands to the device. You specify from whom a command SMS will be accepted in "System > SMS > Command SMS (Page 472)".

Format of the command SMS message

The command SMS message has the following format:

- ID:<identifier> Class command action parameter

The ID:<identifier> specification is required when an identifier was stored for the command SMS in addition to the phone number for additional protection; see section "Command SMS (Page 292)".

Requirement for reply SMS (STATUS)

- A phone number is stored in "System > SMS > Event SMS".

Supported commands

Class	Command	Action	Parameter	
SYS System com- mands	DI	STATUS	Pin number 1	A reply SMS message with the status of the digital input is sent.
	DO	STATUS	Pin number 1	A reply SMS message with the status of the digital output is sent.
		LOW		The digital output is opened.
		HIGH		The digital output is closed.
	IPSEC	STATUS	Name of the IPsec VPN connection	A reply SMS message with the status of the IPsec VPN tunnel is sent.
		UP	Security > IPsec VPN> Connections (Page 461)	The IPsec VPN tunnel is being established.
		DOWN	With '*' IPsec connections are established that use "start on SMS" or "wait on SMS" for "Operation".	An existing IPsec VPN tunnel is terminated.
	OVPN	STATUS	Name of the OpenVPN connection	A reply SMS message with the status of the OpenVPN tunnel is sent.
		UP	Security > OpenVPN> Connections (Page 472)	The OpenVPN tunnel is being established.
		DOWN	With '*' OpenVPN connections are established that use "start on SMS" for "Operation".	An existing OpenVPN tunnel is terminated.
	SRC	STATUS	Address of the SINEMA RC Server	A reply SMS message with the status of the SINEMA RC connection is sent.
		UP	WAN IP address or the host name SINEMA RC (Page 177)	The connection to SINEMA RC Server is being established.
		DOWN		The existing connection to SINEMA RC Server is being terminated.
RLY SMS relay command	Name of the relay connection System > SMS > SMS Relay (Incoming) (Page 295)	-	Text	The text from the SMS message is forwarded to the recipient. The following characters are permitted in the text: • 0123456789 • A...Z a...z • Space • ! " % & / () = ? * + < > ' , . -

Examples

Wake SMS with the identifier

ID:Testidentifier SYS SRC UP 192.168.20.200

SMS message to an application in the LAN

RLY conn2 my SMS text

The text "my SMS Text" is forwarded to the application specified in the relay connection "conn2". The text is forwarded as the following frame:
user#password#105#01;0049xxxxxxxx;my SMS text:

Appendix B "Syslog messages"

B.1 Format of the syslog messages

The devices generate Syslog messages (UDP default port 514) according to RFC 5424 that contain the following boxes.

HEADER

- TIMESTAMP according to RFC 3339
- Host name
- APPNAME, PROCID and MSGID: If no information is known, the "-" character is output.

PRIORITY

PRIORITY contains the coded priority of the Syslog message broken down into a Severity and Facility box.

- Facility
- Severity

VERSION

- Set to 1.

HOSTNAME_CONTENT:

- IPv4 address according to RFC1035: Each byte is represented in decimal, with a dot separating it from the previous one. XXX.XXX.XXX.XXX
- IPv6 address according to RFC4291 Section 2.2

STRUCTURED DATA

- timeQuality block

MESSAGE:

- ASCII string in English

Note

Additional information about the meaning of the boxes is available in RFC 5424 (<https://datatracker.ietf.org/doc/html/rfc5424>).

B.2 Parameters in Syslog messages

The Syslog messages can contain the following parameters:

Parameter	Description	Possible values or example
ip address	IPv4 or IPv6 address	IP address according to RFC1035 or RFC4291 Section 2.2
src port	Port that is shown as decimal number.	0 ... 65535
dest port	Format: %d	
dest mac	MAC address	00:0C:29:2F:09:B3
src mac	Format: %02x:%02x:%02x;%02x:%02x:%02x	
protocol	Name of the service that has generated this event or of the Layer 4 protocol used. Format: %s	Possible entries of: UDP TCP WBM Telnet SSH TFTP SFTP
group	String that identifies the group based on its name Format: %s	it-service
user name	String that identifies the authenticated user based on his/her name without spaces Format: %s	maier
action user name	Identifies the user based on his/her name This is not the authenticated user. Format: %s	Peter.Maier
role	Symbolic name for the group role Format: %s	Administrator
time minute	Number of minutes	44
timeout	Format: %d	
failed login count	Number of failed logins Format: %d	10
max sessions	Number of sessions Format: %d	10
trigger pin	String for an IO pin that triggers the event without spaces Format: %s	DI1
firewall rule	String for a firewall rule with spaces Format: %s	Rule1
subject	String for the subject in the certificate. Used as part of the certificate-based authentication with spaces and must also include Unicode characters Format: (% S) or (% S% S) for UTF8 code.	(Peter Maier)
config detail	String for the configuration with spaces Format: %s	OpenVPN
connection name	Name of the VPN connection	to_Baugruppe1

Parameter	Description	Possible values or example
firewall accept	Firewall action executed (accepted package)	ACCEPT
firewall action reject	Firewall action executed (rejected package)	REJECT DROP
length	Length of the network packet (in bytes) Format: %d	52
network interface	Symbolic name of a network interface Format: %s	vlan1

B.3 Syslog messages

Human user identification and authentication

Message text	{protocol}: User {User name} has logged in from {ip address}.
Example	WBM: User "Admin" has logged in from 192.168.0.1.
Explanation	Valid login information that is specified during remote login.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{protocol}: User {User name} failed to log in from {ip address}.
Example	WBM: User "Admin" has failed to log in from 192.168.0.1.
Explanation	Incorrect user name or incorrect password (login information) specified during remote login.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{protocol}: User {User name} has logged out from {ip address}.
Example	SSH: User "Admin" has logged out from 192.168.0.1.
Explanation	User session completed - logged out.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{protocol}: Default user {user name} logged in from {ip address}.
Example	SSH: Default user admin logged in from 192.168.0.1.
Explanation	The default user is logged in via the IP address.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 007-R5)

Identification and authentication of devices (access via firewall)

Message text	{firewall action accept}(1) in:{network interface} out:{network interface} len:{length} s-mac:{src mac} d-mac:{dest mac} s-ip:{ip address} d-ip:{ip address} {protocol}:{src port}->{dest port}
Example	ACCEPT(1) in:vlan1 out:ppp0 len:52 s-mac:58:EF:68:B3:FA:CE d-mac:00:1B:1B:A7:5B:D8 s-ip:172.23.1.6 d-ip:158.85.11.68 tcp:53788->443
Explanation	A known device requested a connection.
Severity	Info or Warning (configurable)
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.2

Message text	{firewall action reject}(1) in:{network interface} out:{network interface} len:{length} s-mac:{src mac} d-mac:{dest mac} s-ip:{ip address} d-ip:{ip address} {protocol}:{src port}->{dest port}
Example	REJECT(1) in:vlan1 out:ppp0 len:52 s-mac:58:EF:68:B3:FA:CE d-mac:00:1B:1B:A7:5B:D8 s-ip:172.23.1.6 d-ip:217.194.40.109 tcp:53773->443
Explanation	An unknown device requested a connection. The request was denied.
Severity	Info or Warning (configurable)
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.2

Account management

Message text	{protocol}: User {user name} changed own password.
Example	WBM: User admin changed own password.
Explanation	User has changed own password.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR1.3

Message text	{protocol}: User {user name} changed password of user {action user name}.
Example	Telnet: User admin changed password of user test.
Explanation	User has changed the password of another user.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR1.3

Message text	{protocol}: User {user name} created user-account {action user name}.
Example	WBM: User admin created user-account service.
Explanation	The user has created an account.

Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR1.3

Message text	{protocol}: User {user name} deleted user-account {action user name}.
Example	WBM: User admin deleted user-account service.
Explanation	The administrator deleted an existing account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR1.3

Identifier management

Message text	{Protocol}: User {User name} created group {Group} and assigned to role {Role}.
Example	WBM: User admin created group it-service and assigned to role service.
Explanation	The administrator has created a group and assigned it to a role.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.4

Message text	{Protocol}: User {User name} deleted group {Group} and the role {Role} assignment.
Example	WBM: User maier deleted group it-service and the role service assignment.
Explanation	The administrator has deleted an existing group and the role assignment.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.4

Unsuccessful login attempts

Message text	{User name} account is locked for {Time minute} minutes after {Failed login count} unsuccessful login attempts.
Example	User service account is locked for 44 minutes after 10 unsuccessful login attempts.
Explanation	If there are too many failed logins, the corresponding user account was locked for a specific period of time.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.11

Access via untrusted networks (IPsec)

Message text	[IKE] <{connection name} [{config detail}]> IKE_SA {connection name} [{config detail}] established between {ip address} [{config detail}]...{ip address} [{config detail}]
Example	[IKE] <c1 3> IKE_SA c1 1 established between 192.168.55.210[lokal]..192.168.55.211[remote]
Explanation	VPN connection is established (IPsec).
Severity	Info

B.3 Syslog messages

Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1)

Message text	[IKE] <{connection name} [{config detail}]> deleting IKE_SA {connection name} [{config detail}] between {ip address} [{config detail}]...{ip address} [{config detail}]
Example	[IKE] <c1 3> deleting IKE_SA c2[1] between 192.168.55.211[lokal].. 192.168.55.210[remote]
Explanation	VPN tunnel is closed (IPsec).
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1)

Message text	[IKE] <{connection name} [{config detail}]> received AUTHENTICATION_FAILED notify error
Example	[IKE] <c1 1> received AUTHENTICATION_FAILED notify error
Explanation	Authentication of VPN connection failed (IPsec).
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R3)

Access via untrusted networks (OpenVPN)

Message text	OVPN_{connection name} [{config detail}]: Initialization Sequence Completed
Example	OVPN_Conn_1[2427]: Initialization Sequence Completed
Explanation	VPN connection is established (OpenVPN).
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1)

Message text	OpenVPN connection {connection name} has been deactivated.
Example	OpenVPN connection c1 has been deactivated.
Explanation	VPN connection was closed (OpenVPN).
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1)

Access via untrusted networks (SINEMA Remote Connect)

Message text	SINEMA RC - State of Digital Input changed to HIGH. SINEMA RC - OpenVPN connection established.
Example	SINEMA RC - State of Digital Input changed to HIGH. SINEMA RC - OpenVPN connection established.
Explanation	Remote access is permitted. (SINEMA RC, Digital Input)
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.13

Message text	SINEMA RC - Received Wakeup SMS. SINEMA RC - OpenVPN connection established.
Example	SINEMA RC - Received Wakeup SMS. SINEMA RC - OpenVPN connection established.
Explanation	Remote access is permitted. (SINEMA RC, Wakeup SMS)
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.13

Message text	SINEMA RC - State of Digital Input changed to LOW. SINEMA RC - OpenVPN terminated.
Example	SINEMA RC - State of Digital Input changed to LOW. SINEMA RC - OpenVPN terminated.
Explanation	Remote access denied (SINEMA RC, Digital Input)
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.13

Message text	SINEMA RC - Received Shutdown SMS. SINEMA RC - OpenVPN terminated.
Example	SINEMA RC - Received Shutdown SMS. SINEMA RC - OpenVPN terminated.
Explanation	Remote access denied (SINEMA RC, Wakeup SMS)
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.13

Authorization enforcement (access via custom firewall)

Message text	User specific firewall user "{user name}" activated rule set "{firewall rule}" with ip address "{ip address}". Timeout: {timeout} minutes.
Example	User specific firewall user "usf" activated rule set "rs1" with ip address "172.23.1.14". Timeout 5 minutes.
Explanation	The user has logged onto the user-specific firewall. (USF Digital User Login)
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R2)

Message text	User specific firewall digital input {trigger pin} activated rule set "{firewall rule}" with ip "{ip address}".
Example	User specific firewall digital input 1 activated rule set "cpu2" with ip "192.168.16.1".
Explanation	The user has logged onto the user-specific firewall. (USF Digital Input Login)
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R2)4820486

B.3 Syslog messages

Message text	User specific firewall user "{user name}" ruleset "{firewall rule}" time expired.
Example	User specific firewall user "usf" ruleset "rs1" time expired.
Explanation	The access to the user-specific firewall was denied. The access time is expired. (USF User Logout)
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.1

Message text	User specific firewall user "{user name}" logged out by administrator configuration.
Example	User specific firewall user "usf" logged out by administrator configuration.
Explanation	The access to the user-specific firewall was denied. The device administrator deactivates the user using the "Force Deactivate" button. (USF user force log out by admin)
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.1

Message text	User specific firewall user "{user name}" deactivated by administrator configuration.
Example	User specific firewall user "usf" deactivated by administrator configuration.
Explanation	The access to the user-specific firewall was denied. The device administrator has deactivated the user. (USF user deactivated by admin)
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.1

Message text	User specific firewall digital input {trigger pin} deactivated rule set "{firewall rule}".
Example	User specific firewall digital input 1 deactivated rule set "rs1".
Explanation	The access to the user-specific firewall was denied. The corresponding set of rules has been deactivated. (USF Digital Input Logout)
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.1

Session lock

Message text	The session of user {user name} was closed after {time} seconds of inactivity.
Example	The session of user admin was closed after 60 seconds of inactivity.
Explanation	The current session was locked due to inactivity.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.5

Remote session termination

Message text	[JOB] <{connection name} [{config detail}]> deleting CHILD_SA after {time second} seconds of inactivity
Example	[JOB] <to_Baugruppe1 21> deleting CHILD_SA after 20 seconds of inactivity
Explanation	The remote session was ended after a period of inactivity (IPsec).
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.6

Message text	OVPN_{connection name} [{config detail}]: [{config detail}] Inactivity timeout (--ping-restart), restarting
Example	OVPN_c1[26296]: [router] Inactivity timeout (--ping-restart), restarting
Explanation	The remote session was ended after a period of inactivity (OpenVPN).
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.6

Limiting the number of simultaneous sessions

Message text	{Protocol}: The maximum number of {Max sessions} concurrent login session exceeded.
Example	WBM: The maximum number of 10 concurrent login sessions exceeded.
Explanation	The maximum number of parallel connections is exceeded.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.7

Nonrepudiation

Message text	Device configuration changed.
Example	Device configuration changed.
Explanation	The device configuration has been changed permanently.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR2.12

Communication integrity

Message text	[IKE] {connection name} {config detail} received invalid DPD sequence number {config detail} (expected {config detail}), ignored.
Example	[IKE] "c1" "1" received invalid DPD sequence number 10 (expected 12), ignored.
Explanation	Integrity check failed (IPsec)
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.1

B.3 Syslog messages

Message text	OVPN_{connection name}{config detail}: Authenticate/Decrypt packet error: packet HMAC authentication failed.
Example	OVPN_c1[25409]: Authenticate/Decrypt packet error: packet HMAC authentication failed.
Explanation	Integrity check failed (OpenVPN).
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.1

Session integrity

Message text	{Protocol}: Session ID verification from {ipaddress} failed.
Example	WBM Session ID verification from 192.168.1.1 failed.
Explanation	The session ID of 192.168.1.1 is invalid.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.8

Data backup in automation system

Log text	{protocol}: Saved file type ConfigPack.
Standard	IEC 62443-3-3 Reference: SR7.3
Description	The ConfigPack file was saved.
Example	TFTP: Saved file type ConfigPack
Severity	Notice
Facility	local0

Log text	{protocol}: User {user name} saved file type ConfigPack
Standard	IEC 62443-3-3 Reference: SR7.3
Description	User has saved the ConfigPack file.
Example	WBM: User admin saved file type ConfigPack..
Severity	Notice
Facility	local0

Log text	{protocol}: User {user name} failed to save file type ConfigPack.
Standard	IEC 62443-3-3 Reference: SR7.3
Description	User failed to save the ConfigPack file.
Example	WBM: User admin failed to save file type ConfigPack.
Severity	Info
Facility	local0

Log text	{protocol}: Failed to save file type ConfigPack.
Standard	IEC 62443-3-3 Reference: SR7.3
Description	The ConfigPack file could not be saved.
Example	TFTP: Failed to save file type ConfigPack.

Severity	Warning
Facility	local0

Restoration of the automation system

Message text	{protocol}: Loaded file type Firmware {version} (restart required).
Example	TFTP: Loaded file type Firmware V02.00.00 (restart required).
Explanation	The firmware was successfully loaded.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.4

Message text	{protocol}: User {user name} loaded file type Firmware {version} (restart required).
Example	WBM: User admin loaded file type Firmware V02.00.00 (restart required).
Explanation	The user has successfully loaded the firmware.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.4

Message text	{protocol}: Failed to load file type Firmware.
Example	WBM: Failed to load file type Firmware.
Explanation	Firmware upload has failed.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.4

Message text	{protocol}: Loaded file type Config (restart required).
Example	TFTP: Loaded file type Config (restart required).
Explanation	The configuration is applied.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.4

Message text	{protocol}: Loaded file type ConfigPack (restart required).
Example	TFTP: Loaded file type ConfigPack (restart required).
Explanation	The configuration is applied.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.4

Message text	{protocol}: User {user name} loaded file type Config (restart required).
Example	WBM: User admin loaded file type Config (restart required).
Explanation	The configuration is applied.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.4

B.3 Syslog messages

Message text	{protocol}: User {user name} loaded file type ConfigPack (restart required).
Example	WBM: User admin loaded file type ConfigPack (restart required).
Explanation	The configuration is applied.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.4

Appendix C "Encryption methods used (ciphers)"

The following tables list the encryption methods (ciphers) used by SCALANCE M-800.

C.1 SSL

HTTPS WBM Server

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_AES_128_GCM_SHA256	1301	✓
Encryption suite	TLS_CHACHA20_POLY1305_SHA256	1303	✓
Encryption suite	TLS_AES_256_GCM_SHA384	1302	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	c02f	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	c030	✓
Protocol version	TLSv1.2	--	✓
Protocol version	TLSv1.3	--	✓

HTTPS WBM Client

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_AES_128_GCM_SHA256	1301	✓
Encryption suite	TLS_CHACHA20_POLY1305_SHA256	1303	✓
Encryption suite	TLS_AES_256_GCM_SHA384	1302	✓
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_256_GCM_SHA384	c02c	✓
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_128_GCM_SHA256	c02b	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	c02f	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	c030	✓
Protocol version	TLSv1.2	--	✓
Protocol version	TLSv1.3	--	✓

SMTP Client (secure)

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_AES_128_GCM_SHA256	1301	✓
Encryption suite	TLS_CHACHA20_POLY1305_SHA256	1303	✓
Encryption suite	TLS_AES_256_GCM_SHA384	1302	✓
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_256_GCM_SHA384	c02c	✓
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_128_GCM_SHA256	c02b	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	c02f	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	c030	✓
Protocol version	TLSv1.2	--	✓
Protocol version	TLSv1.3	--	✓

Syslog Client TLS

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_AES_128_GCM_SHA256	1301	✓
Encryption suite	TLS_CHACHA20_POLY1305_SHA256	1303	✓
Encryption suite	TLS_AES_256_GCM_SHA384	1302	✓
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_256_GCM_SHA384	c02c	✓
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_128_GCM_SHA256	c02b	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	c02f	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	c030	✓
Protocol version	TLSv1.2	--	✓
Protocol version	TLSv1.3	--	✓

C.2 OpenVPN

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	c00a	--
Encryption suite	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	009f	--

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	009e	--
Encryption suite	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	006b	--
Encryption suite	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	0067	--
Encryption suite	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	0039	--
Encryption suite	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	0033	--
Protocol version	TLSv1.2	--	--

C.3 SINEMA RC

Client connection to SINEMA RC

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_AES_128_GCM_SHA256	1301	--
Encryption suite	TLS_CHACHA20_POLY1305_SHA256	1303	--
Encryption suite	TLS_AES_256_GCM_SHA384	1302	--
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	c02c	--
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	c02b	--
Encryption suite	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	009e	--
Encryption suite	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	009f	--
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	c02f	--
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	c030	--
Protocol version	TLSv1.2	--	--
Protocol version	TLSv1.3	--	--

C.4 cSRP

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_AES_128_GCM_SHA256	1301	--
Encryption suite	TLS_CHACHA20_POLY1305_SHA256	1303	--
Encryption suite	TLS_AES_256_GCM_SHA384	1302	--

C.5 SSH CLI

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_128_GCM_SHA256	c02b	--
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	c02f	--
Encryption suite	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	cca9	--
Encryption suite	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	cca8	--
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_256_GCM_SHA384	c02c	--
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	c030	--
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_256_CBC_SHA	c00a	--
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_128_CBC_SHA	c009	--
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	c013	--
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	c014	--
Encryption suite	TLS_RSA_WITH_AES_128_GCM_SHA256	009c	--
Encryption suite	TLS_RSA_WITH_AES_256_GCM_SHA384	009d	--
Encryption suite	TLS_RSA_WITH_AES_128_CBC_SHA	002f	--
Encryption suite	TLS_RSA_WITH_AES_256_CBC_SHA	0035	--
Encryption suite	TLS_RSA_WITH_3DES_EDE_CBC_SHA	000a	--
Protocol version	TLS 1.2 (0x0303)	--	--
Protocol version	TLS 1.3 (0x0304)	--	--

C.5 SSH CLI

SSH CLI Server

Category	Process	Hexadecimal value	Enabled by default
Encryption method (enc)	aes256-ctr	--	✓
Host key	ecdsa-sha2-nistp521	--	✓
Host key	rsa-sha2-256	--	✓
Host key	rsa-sha2-512	--	✓
Key exchange (kex)	curve25519-sha256	--	✓
Key exchange (kex)	curve25519-sha256@libssh.org	--	✓
Key exchange (kex)	ecdh-sha2-nistp256	--	✓
Key exchange (kex)	ecdh-sha2-nistp384	--	✓

Category	Process	Hexadecimal value	Enabled by default
Key exchange (kex)	ecdh-sha2-nistp521	--	✓
Key exchange (kex)	diffie-hellman-group16-sha512	--	✓
Key exchange (kex)	diffie-hellman-group18-sha512	--	✓
MAC	hmac-sha2-256	--	✓
Protocol version	SSHv2.0	--	✓

SFTP Server

Category	Process	Hexadecimal value	Enabled by default
Encryption method (enc)	aes256-ctr	--	✓
Host key	ecdsa-sha2-nistp521	--	✓
Host key	rsa-sha2-256	--	✓
Host key	rsa-sha2-512	--	✓
Key exchange (kex)	curve25519-sha256	--	✓
Key exchange (kex)	curve25519-sha256@libssh.org	--	✓
Key exchange (kex)	ecdh-sha2-nistp256	--	✓
Key exchange (kex)	ecdh-sha2-nistp384	--	✓
Key exchange (kex)	ecdh-sha2-nistp521	--	✓
Key exchange (kex)	diffie-hellman-group16-sha512	--	✓
Key exchange (kex)	diffie-hellman-group18-sha512	--	✓
MAC	hmac-sha2-256	--	✓
Protocol version	SSHv2.0	--	✓

C.6 SNMP

SNMP Server

Category	Process	Hexadecimal value	Enabled by default
Authentication	HMAC-MD5-96	--	--
Authentication	HMAC-SHA-96	--	--
Encryption	des-cbc	--	--
Encryption	aes128-cbc	--	--

SNMP Trap

Category	Process	Hexadecimal value	Enabled by default
Authentication	HMAC-MD5-96	--	--
Authentication	HMAC-SHA-96	--	--
Encryption	des-cbc	--	--
Encryption	aes128-cbc	--	--

C.7 RADIUS**RADIUS Client**

Category	Process	Hexadecimal value	Enabled by default
Integrity algorithm	MD5	--	--
Integrity algorithm	HMAC-SHA1	--	--

C.8 IPsec**IPsec Server**

Category	Process	Hexadecimal value	Enabled by default
ESP /AH authentication	MD5	--	--
ESP /AH authentication	SHA1	--	--
ESP /AH authentication	SHA256	--	--
ESP /AH authentication	SHA384	--	--
ESP /AH authentication	SHA512	--	--
ESP encryption	3des-168-cbc	--	--
ESP encryption	aes128-cbc	--	--
ESP encryption	aes192-cbc	--	--
ESP encryption	aes256-cbc	--	--
ESP encryption	aes128-ctr	--	--
ESP encryption	aes192-ctr	--	--
ESP encryption	aes256-ctr	--	--
ESP encryption	aes128-CCM	--	--
ESP encryption	aes192-CCM	--	--
ESP encryption	aes256-CCM	--	--
ESP encryption	aes128-GCM	--	--
ESP encryption	aes192-GCM	--	--

Category	Process	Hexadecimal value	Enabled by default
ESP encryption	aes256-GCM	--	--
IKE authentication	hmac-MD5	--	--
IKE authentication	hmac-SHA1	--	--
IKE authentication	hmac-SHA256	--	--
IKE authentication	hmac-SHA384	--	--
IKE authentication	hmac-SHA512	--	--
IKE DH group	Group 1 (modp768)	--	--
IKE DH group	Group 2 (modp1024)	--	--
IKE DH group	Group 5 (mod1536)	--	--
IKE DH group	Group 14 (modp2048)	--	--
IKE DH group	Group 16 (modp4096)	--	--
IKE DH group	Group 18 (modp8192)	--	--

IPsec Client

Category	Process	Hexadecimal value	Enabled by default
ESP /AH authentication	MD5	--	✓
ESP /AH authentication	SHA1	--	✓
ESP /AH authentication	SHA256	--	✓
ESP /AH authentication	SHA384	--	✓
ESP /AH authentication	SHA512	--	✓
ESP encryption	3des-168-cbc	--	✓
ESP encryption	aes128-cbc	--	✓
ESP encryption	aes192-cbc	--	✓
ESP encryption	aes256-cbc	--	✓
ESP encryption	aes128-ctr	--	✓
ESP encryption	aes192-ctr	--	✓
ESP encryption	aes256-ctr	--	✓
ESP encryption	aes128-CCM	--	✓
ESP encryption	aes192-CCM	--	✓
ESP encryption	aes256-CCM	--	✓
ESP encryption	aes128-GCM	--	✓
ESP encryption	aes192-GCM	--	✓
ESP encryption	aes256-GCM	--	✓
IKE authentication	hmac-MD5	--	✓
IKE authentication	hmac-SHA1	--	✓
IKE authentication	hmac-SHA256	--	✓
IKE authentication	hmac-SHA384	--	✓
IKE authentication	hmac-SHA512	--	✓
IKE DH group	Group 1 (modp768)	--	✓
IKE DH group	Group 2 (modp1024)	--	✓

Category	Process	Hexadecimal value	Enabled by default
IKE DH group	Group 5 (mod1536)	--	✓
IKE DH group	Group 14 (modp2048)	--	✓
IKE DH group	Group 16 (modp4096)	--	✓
IKE DH group	Group 18 (modp8192)	--	✓

Appendix D "Permitted characters in names, passwords and descriptions"

D

D.1 Permitted characters

Passwords

Observe the following rules when creating or changing the passwords:

Allowed characters of a character set according to ANSI X 3.4-1986	0123456789 A...Z a...z .-_#+~^!%&= <>@, Space
Permitted in addition, except in passwords on the pages "System > Load@Save" and "System > System time > NTP client"	'*\${}{}[]`
Characters not allowed	;" €'?\$32°µ ä ö ü Ä Ö Ü
Length of the password	At least 8 characters and maximum 128 characters

Note

Passwords

To improve security, make sure that passwords are as long as possible.

Passwords must be at least 8 characters long and contain special characters, upper and lowercase characters as well as numbers.

User names

Observe the following rules when creating or changing the user names:

Allowed characters of a character set according to ANSI X 3.4-1986	0123456789 A...Z a...z .-_#+'*~^!\$%&/{}[]]=\`<>@,
Characters not allowed	;" €'?\$32°µ ä ö ü Ä Ö Ü Space
Length of the user name	1 to 30 characters

Note

User names

To improve security, make sure that user names are as long as possible.

D.1 Permitted characters

Role names

Observe the following rules when creating or changing the role names:

Allowed characters of a character set	0123456789 A...Z a...z .-_#+'*~^!\$%&/{([)]}= \ ` <>@,; Space
Characters not allowed	;" €'¿§³²ºµ ä ö ü Ä Ö Ü
Length of the role name	1 ... 64 characters

Group names

Observe the following rules when creating or changing the group names:

Allowed characters of a character set	0123456789 A...Z a...z .-_#+'*~^!\$%&/{([)]}= \ ` <>@; Space
Characters not allowed	;" €'¿§³²ºµ ä ö ü Ä Ö Ü
Length of the group name	1 ... 64 characters

User, role and group descriptions

Observe the following rules when creating or modifying descriptions:

Allowed characters of a character set	0123456789 A...Z a...z .-_#+'*~^!\$%&/{([)]}= \ ` <>@, Space ; " CLI only
Characters not allowed	WBM ;;" €'¿§³²ºµ ä ö ü Ä Ö Ü
	CLI €'¿§³²ºµ ä ö ü Ä Ö Ü
Length of description	1 ... 100 characters

Note**User names**

To improve security, make sure that user names are as long as possible.

File names

When creating or changing the file names, remember the following rules:

Allowed characters of a character set according to ANSI X 3.4-1986	0123456789 A...Z a...z .-_#+'~^!\$%&/{([])}= `@,
Characters not allowed	\ / : ; " € ' ? \$ * < > ³²⁰ µ ä ö ü Ä Ö Ü Space
Length of the file name	1 to 30 characters

Note

File names

To improve security, note the following:

- Assign the file a name as long as possible.
- Do not use spaces in the TFTP file name.

D.1 Permitted characters

Index

2

2FA, 427

A

Aging

Dynamic MAC Aging, 382

Authentication, 243

Available system functions, 58

B

Backup, 210, 323

Basic MAC address, 144

Basic Wizard

Starting, 111

BFP, 479

Bridge, 181, 385

Bridge priority, 181, 385

Root bridge, 181, 385

Bridge Max Age, 182, 385

Bridge Max Hop Count, 182

Brute Force Prevention, 479

button, 273

C

CA certificate, 91

Certificates, 437

CLP, 280, 283

Collisions, 160

Configuration manuals, 488

Configuration mode, 202

Configuring the network via Ethernet

Connecting to network, 68

CoS (Class of Service), 75

CRC, 160

D

DCP Discovery, 286

DCP server, 200

Dead peer detection, 95

Determine GPS position, 328

Device

Basic Wizard, 114

System, 203

Device certificate, 91

DHCP

Client, 304

Documentation on the Internet, 11

DSL

Overview, 171

DST

Daylight saving time, 255, 257

E

Error status, 152

eSIM, 349

Ethernet Statistics

Interface statistics, 157

Events, 230

F

Factory defaults, 488

Factory setting, 488

Fault monitoring

Connection status change, 277

SIM card, 279

File name

Permitted characters and length, 515

Firewall monitoring, 196

Forward Delay, 182, 385

Fragments, 160

G

Geographic coordinates, 205

Group name

Permitted characters, 514

Groups, 423

H

Hardware Revision, 144

Hello time, 182, 385

HTTP

Server, 199

HTTPS

Server, 199

I

ICMP, 81

Information

- ARP table, 145
- DSL, 171
- Groups, 193
- Hardware, 142
- IPsec VPN, 176
- IPv6 Neighbor Table, 146
- LLDP, 161
- Log table, 147, 151
- Mobile, 164
- Network Scan, 170
- OpenVPN client, 179
- OpenVPN server, 180
- Role, 192
- Security, 188, 191
- Security log, 149
- SHDSL, 175
- SINEMA RC, 177
- SNMP, 156
- Software, 142
- Spanning Tree, 183
- Start page, 135
- System Time, 194
- Versions, 142
- VXLAN, 193

Interfaces

Mobile, 338

IP address

- Assignment with SIMATIC STEP 7, 70
- Basic Wizard, 113
- Configuration, 395

iperf, 332

IPsec method, 92

IPsec VPN

- NETMAP, 89
- Source NAT, 89

IPv4

VRRPv3, 103

IPv4 routing

Routing table, 162

IPv6

Notation, 71

IPv6 routing

Routing table, 163

J

Jabbers, 160

K

KEY-PLUG, 283

L

Layer 2, 370

Layer 3, 283

LLDP, 161, 389

Location, 205, 328

Log table

- Event log, 147
- Firewall log, 151
- Security log, 149

Logging in, 106

Login, 479

Logout

Automatic, 272

M

Maintenance data, 143

Manufacturer, 143

Manufacturer ID, 144

Mobile

Information, 164

Mobile data usage, 169

Mobile wireless

SIM switchover, 353

N

NAPT

Configuring, 398

NAT

1-to-1 NAT, 402

Configuring, 397, 417

Masquerading, 88

NAPT, 88

NAT traversal, 95

NETMAP, 89

Source NAT, 89

NAT traversal, 95

NTP

- Client, 265
- Server, 271

O**Operator**

- Interfaces, 345

Order ID, 144**P****Packet Capture, 367****Packet error statistics, 159****Password, 424**

- Options, 427
- Permitted characters and length, 513

Permitted characters and length, 513**Ping, 285****PLUG, 61, 280, 283****point-to-point, 103****Port**

- Port configuration, 334

Power supply

- Monitoring, 276

Q**QoS Trust, 75****R****RADIUS, 430****Redundant networks, 181, 385****Requirement**

- ADSL connection, 51
- Antenna, 42, 44, 46, 49
- Power supply, 42, 45, 48, 49, 50, 51
- SHDSL connection, 51
- SIM card, 43, 45, 48, 50

Reset, 208**RESET button, 273****Reset device, 488****Reset timer BFP, 479****Restart, 208****Restore Factory Defaults, 488****Role name**

- Permitted characters, 514

Roles, 421**Root Max Age, 182, 385****Routing, 391**

- ICMP, 81
- IPv4 routing table, 162
- IPv6 routing table, 163
- Static routes, 391

RSTP, 384**S****Security settings, 246****SELECT/SET button, 273****Serial number, 144****Server certificate, 91****SFTP**

- Load/save, 224

SHA algorithm, 246**SHDSL**

- Interface, 117, 363
- Overview, 175, 361

Signal recorder, 168**SIM**

- Basic Wizard, 119
- Interfaces, 343

SIM switchover, 353**SMS, 289**

- receiving, 295
- Send, 298
- sending, 294

SMTP

- Client, 200

SNAT

- Configuring, 400

SNMP, 78, 201, 240, 246

- Groups, 245
- Overview, 156
- SNMPv1, 78
- SNMPv2c, 78
- SNMPv3, 78
- Trap, 250

SNMPv3

- Access, 246
- Groups, 245
- Notifications, 250
- Users, 242
- Views, 248

Software version, 144**Source NAT**

- Masquerading, 88

Spanning tree, 383**Spanning Tree**

- Information, 183
- Rapid Spanning Tree, 103

SSH

Server, 199

Standard mode, 92

Start page, 135

Stateful inspection firewall, 85

Subnet

Configuration, 395

Overview, 393

Subnets

Configuration (IPv6), 414

Connected Subnets (IPv6), 414

Syslog

Client, 200

System

Configuration, 197

Device, 203

General information, 204

Load and Save via HTTP, 216

System time service switchover, 254

System event log

Agent, 274

System events, 230

Configuration, 230

Severity filter, 235

System manual, 13

System Time, 252

T

TCP Event, 324

Telnet

Server, 198

TFTP

Load/save, 220

Time

Time zone, 268

UTC time, 268

Time of day

GPS and mobile wireless device, 260

Manual setting, 125, 253

NTP Client, 126

SIMATIC Time Client, 269

SNTP (Simple Network Time Protocol), 261

System time, 125, 252

Time zone, 264

Time-of-day synchronization, 261

UTC time, 264

Time setting, 201

Trigger interval BFP, 479

Two-factor authentication, 427

U

User groups, 423

User name

Permitted characters and length, 513

V

VLAN, 73

Port VID, 375

Priority, 375

Tag, 375

VLAN ID, 76

VLAN tag, 74

VPN connection

OpenVPN server, 180

Status, 176

Status OpenVPN client, 179

VRRP

VRRP addresses overview (IPv4), 409

VRRPv3 Addresses Configuration (IPv4), 410

VRRPv3 Configuration (IPv4), 407

VRRPv3 routers (IPv4), 405

VRRPv3

Backup router, 103

Interface Tracking, 411

Master router, 103

Virtual router, 103

VRRPv3 router, 103

VRRPv3 Statistics, 186

VXLAN, 193

W

Web Based Management

Requirement, 105