SIEMENS

SIMATIC NET

# Industrial Remote Communication Remote Networks SCALANCE M-800 Web Based Management V7.2

**Projektierungshandbuch**


Einleitung 1

Security-Empfehlung 2

Beschreibung 3

Technische Grundlagen 4

Konfigurieren mit dem Web Based Management 5

Instandhalten und Warten 6

Anhang A "Befehl-SMS" A

Anhang B "Syslog-Meldungen" B

Anhang C "Verwendete Verschlüsselungsverfahren (Ciphers)" C



**04/2023**
C79000-G8900-C330-16

## Rechtliche Hinweise

### Warnhinweiskonzept

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt.

| ⚠ **GEFAHR** |
| --- |
| bedeutet, dass Tod oder schwere Körperverletzung eintreten **wird**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden. |

| ⚠ **WARNUNG** |
| --- |
| bedeutet, dass Tod oder schwere Körperverletzung eintreten **kann**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden. |

| ⚠ **VORSICHT** |
| --- |
| bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden. |

| **ACHTUNG** |
| --- |
| bedeutet, dass Sachschaden eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden. |

Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis zur jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

### Qualifiziertes Personal

Das zu dieser Dokumentation zugehörige Produkt/System darf nur von für die jeweilige Aufgabenstellung **qualifiziertem Personal** gehandhabt werden unter Beachtung der für die jeweilige Aufgabenstellung zugehörigen Dokumentation, insbesondere der darin enthaltenen Sicherheits- und Warnhinweise. Qualifiziertes Personal ist auf Grund seiner Ausbildung und Erfahrung befähigt, im Umgang mit diesen Produkten/Systemen Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

### Bestimmungsgemäßer Gebrauch von Siemens-Produkten

Beachten Sie Folgendes:

| ⚠ **WARNUNG** |
| --- |
| Siemens-Produkte dürfen nur für die im Katalog und in der zugehörigen technischen Dokumentation vorgesehenen Einsatzfälle verwendet werden. Falls Fremdprodukte und -komponenten zum Einsatz kommen, müssen diese von Siemens empfohlen bzw. zugelassen sein. Der einwandfreie und sichere Betrieb der Produkte setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung, Montage, Installation, Inbetriebnahme, Bedienung und Instandhaltung voraus. Die zulässigen Umgebungsbedingungen müssen eingehalten werden. Hinweise in den zugehörigen Dokumentationen müssen beachtet werden. |

### Marken

Alle mit dem Schutzrechtsvermerk ® gekennzeichneten Bezeichnungen sind eingetragene Marken der Siemens AG. Die übrigen Bezeichnungen in dieser Schrift können Marken sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

### Haftungsausschluss

Wir haben den Inhalt der Druckschrift auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Druckschrift werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

Dokumentbestellnummer: C79000-G8900-C330
Ⓟ 05/2023 Änderungen vorbehalten

Copyright © Siemens AG 2013 - 2023.
Alle Rechte vorbehalten

# Inhaltsverzeichnis


**1 Einleitung ..... 11**

1.1 Zweck des Projektierungshandbuchs ..... 11
1.2 Gültigkeitsbereich ..... 11
1.3 Ergänzende Dokumentation ..... 11
1.4 Weiterführende Dokumentation ..... 13
1.5 Neu in der Version ..... 13
1.6 Verwendete Symbole ..... 14
1.7 Verwendete Bezeichnungen ..... 14
1.8 SIMATIC NET-Glossar ..... 15
1.9 Security-Hinweise ..... 15
1.10 Fehlerfall ..... 16
1.11 Außerbetriebnahme ..... 16
1.12 Recycling und Entsorgung ..... 16
1.13 Firmware ..... 17
1.14 Lizenzbedingungen Open Source ..... 17
1.15 Marken ..... 17

**2 Security-Empfehlung ..... 19**

2.1 Security-Empfehlungen ..... 19
2.2 Verfügbare Dienste ..... 24

**3 Beschreibung ..... 29**

3.1 Funktion ..... 29
3.2 Konfigurationsbeispiele ..... 31
3.2.1 Überblick ..... 31
3.2.2 SCALANCE MUM856/M81x als Internetzugang ..... 31
3.2.3 Direkte Kommunikation von Stationen ..... 33
3.2.4 TeleControl über das Mobilfunknetz ..... 34
3.2.5 TeleControl über Standleitung ..... 35
3.2.6 Mobiler Zugang zu Anlagen und Anlagenteilen ..... 36
3.2.7 Anlagenzugang über eine Fernwartungszentrale ..... 38
3.2.8 TeleControl mit SINEMA RC ..... 39
3.3 Voraussetzungen für den Betrieb ..... 40
3.3.1 Für den Betrieb mit MUM853 ..... 40
3.3.2 Für den Betrieb mit MUM856 ..... 42
3.3.3 Für den Betrieb mit M87x ..... 44
3.3.4 Für den Betrieb mit M81x ..... 45

3.3.5 Für den Betrieb mit M826 ... 46
3.3.6 Für den Betrieb mit M804PB ... 48
3.3.7 Einsatz in einer PROFINET-Umgebung ... 48
3.3.8 TIA Portal Cloud Connector ... 49

3.4 Mengengerüste für WBM und CLI ... 49

3.5 Mengengerüst für SINEMA RC ... 51

3.6 Hardware-Ausstattung und Systemfunktionen ... 52

3.7 PLUG ... 54
3.7.1 PLUG ... 54
3.7.2 PRESET-PLUG ... 57

**4 Technische Grundlagen ... 59**

4.1 IP-Adressen ... 59
4.1.1 IPv4 / IPv6 ... 59
4.1.2 IPv4-Adresse ... 60
4.1.2.1 Aufbau einer IPv4-Adresse ... 60
4.1.2.2 Erstmalige Vergabe einer IPv4-Adresse ... 62
4.1.2.3 Adressvergabe über DHCPv4 ... 63
4.1.2.4 Adressvergabe mit SINEC PNI ... 63
4.1.2.5 Adressvergabe über STEP 7 ... 64
4.1.3 IPv6-Adresse ... 64
4.1.3.1 IPv6-Begriffe ... 64
4.1.3.2 Aufbau einer IPv6-Adresse ... 66

4.2 VLAN ... 67
4.2.1 VLAN ... 67
4.2.2 VLAN-Tagging ... 68

4.3 VXLAN ... 70

4.4 SNMP ... 72

4.5 ICMP ... 74

4.6 Security-Funktionen ... 76
4.6.1 Anpassen der MTU für IPsec VPN und SINEMA RC ... 76
4.6.2 Benutzerverwaltung ... 76
4.6.3 Firewall ... 78
4.6.3.1 Firewall-Regeln ... 80
4.6.4 NAT ... 82
4.6.5 NAT und Firewall ... 84
4.6.6 Zertifikate ... 86
4.6.7 VPN ... 86
4.6.7.1 IPsec VPN ... 87
4.6.7.2 OpenVPN ... 90
4.6.7.3 VPN-Verbindungsaufbau ... 91

4.7 Redundanz ... 96
4.7.1 Spanning Tree ... 96
4.7.1.1 RSTP ... 97
4.7.2 VRRPv3 ... 97

**5 Konfigurieren mit dem Web Based Management ..... 99**

5.1 Web Based Management ..... 99
5.2 Starten und anmelden ..... 100
5.3 Menü "Wizard" ..... 104
5.3.1 Basic Wizard ..... 104
5.3.2 IP ..... 105
5.3.3 Gerät ..... 106
5.3.4 DSL ..... 107
5.3.5 SHDSL ..... 109
5.3.6 SIM ..... 111
5.3.7 Mobilfunkanbieter ..... 114
5.3.8 Zeiteinstellung ..... 116
5.3.9 DDNS ..... 118
5.3.10 SINEMA RC ..... 119
5.3.11 Cloud Connector ..... 122
5.3.12 Zusammenfassung ..... 123
5.4 Menü "Information" ..... 125
5.4.1 Startseite ..... 125
5.4.2 Versionen ..... 131
5.4.3 Identification & Maintenance ..... 133
5.4.4 ARP / Nachbarn ..... 134
5.4.4.1 ARP-Tabelle ..... 134
5.4.4.2 IPv6-Nachbarschaftstabelle ..... 135
5.4.5 Log-Tabellen ..... 136
5.4.5.1 Ereignis-Log ..... 136
5.4.5.2 Security-Log ..... 138
5.4.5.3 Firewall-Log ..... 140
5.4.6 Fehler ..... 141
5.4.7 DHCP-Server ..... 142
5.4.8 SNMP ..... 144
5.4.9 LLDP ..... 144
5.4.10 IPv4-Routing ..... 146
5.4.11 IPv6-Routing ..... 147
5.4.12 Mobilfunk ..... 147
5.4.12.1 Übersicht ..... 147
5.4.12.2 Signalrekorder ..... 150
5.4.12.3 Datennutzung ..... 151
5.4.13 DSL ..... 152
5.4.13.1 Übersicht ..... 152
5.4.13.2 DSL-Datenrate ..... 154
5.4.13.3 Streams ..... 154
5.4.14 SHDSL ..... 156
5.4.15 IPsec VPN ..... 157
5.4.16 SINEMA RC ..... 158
5.4.17 OpenVPN-Client ..... 160
5.4.18 Redundanz ..... 161
5.4.18.1 Übersicht ..... 161
5.4.18.2 Spanning Tree ..... 163
5.4.19 VRRPv3-Statistiken ..... 166
5.4.20 Security ..... 168

5.4.20.1 Übersicht ... 168
5.4.20.2 Unterstützte Funktionsrechte ... 171
5.4.20.3 Rollen ... 171
5.4.20.4 Gruppen ... 172
5.4.21 VXLAN ... 173
5.4.22 Systemzeit ... 174

5.5 Menü "System" ... 176
5.5.1 Konfiguration ... 176
5.5.2 Allgemein ... 183
5.5.2.1 Gerät ... 183
5.5.2.2 Koordinaten ... 185
5.5.3 Neustart ... 187
5.5.3.1 Neustart ... 187
5.5.3.2 Sleep Mode ... 190
5.5.4 Laden & Speichern ... 191
5.5.4.1 Dateiliste ... 191
5.5.4.2 HTTP ... 195
5.5.4.3 TFTP ... 200
5.5.4.4 SFTP ... 204
5.5.4.5 Passwörter ... 208
5.5.5 Ereignisse ... 210
5.5.5.1 Konfiguration der Ereignisse ... 210
5.5.5.2 Severity-Filter ... 215
5.5.6 SMTP-Client ... 216
5.5.6.1 Allgemein ... 216
5.5.6.2 Empfänger ... 219
5.5.7 SNMP ... 220
5.5.7.1 Allgemein ... 220
5.5.7.2 SNMPv3-Benutzer ... 222
5.5.7.3 Zuordnung von SNMPv3-Benutzern zu Gruppen ... 225
5.5.7.4 SNMPv3-Zugriff ... 226
5.5.7.5 SNMPv3-Ansichten ... 228
5.5.7.6 Benachrichtigungen ... 230
5.5.8 Systemzeit ... 232
5.5.8.1 Manuelle Einstellung ... 232
5.5.8.2 DST-Übersicht ... 234
5.5.8.3 DST-Konfiguration ... 236
5.5.8.4 Mobile Zeit ... 239
5.5.8.5 SNTP-Client ... 241
5.5.8.6 NTP-Client ... 245
5.5.8.7 SIMATIC Time Client ... 249
5.5.8.8 NTP-Server ... 250
5.5.9 Auto-Logout ... 252
5.5.10 Taster ... 253
5.5.11 Syslog-Client ... 254
5.5.12 Fehlerkontrolle ... 255
5.5.12.1 Spannungsversorgung ... 255
5.5.12.2 Link Change ... 257
5.5.12.3 Mobilfunk ... 259
5.5.13 PLUG ... 259
5.5.13.1 Konfiguration ... 259
5.5.13.2 Lizenz ... 263

5.5.14 Ping ... 266
5.5.15 DCP Discovery ... 267
5.5.16 SMS ... 269
5.5.16.1 Allgemein ... 269
5.5.16.2 Ereignis SMS ... 270
5.5.16.3 Befehl-SMS ... 273
5.5.16.4 SMS-Relay (Ausgehend) ... 274
5.5.16.5 SMS-Relay (Eingehend) ... 276
5.5.16.6 SMS senden ... 278
5.5.17 DNS ... 280
5.5.17.1 DNS-Client ... 280
5.5.17.2 DNS-Proxy ... 281
5.5.17.3 DDNS-Client ... 281
5.5.17.4 DNS-Record ... 283
5.5.18 DHCPv4 ... 284
5.5.18.1 DHCP-Client ... 284
5.5.18.2 DHCP-Server ... 287
5.5.18.3 DHCP-Optionen ... 289
5.5.18.4 Statische Zuordnung ... 291
5.5.19 cRSP / SRS ... 292
5.5.20 Proxy-Server ... 294
5.5.21 SINEMA RC ... 295
5.5.22 Cloud Connector ... 298
5.5.23 Backup der Konfiguration ... 300
5.5.24 Connection Check ... 301
5.5.24.1 Connection Fallback ... 303
5.5.25 TCP-Ereignis ... 304
5.5.26 GPS ... 307
5.5.26.1 Koordinaten ... 307
5.5.26.2 Geofencing ... 309

5.6 Menü "Schnittstellen" ... 312
5.6.1 Ethernet ... 312
5.6.1.1 Konfiguration ... 313
5.6.2 Mobilfunk ... 315
5.6.2.1 Allgemein ... 315
5.6.2.2 SIM ... 319
5.6.2.3 Mobilfunkanbieter ... 322
5.6.2.4 eSIM-Profil ... 325
5.6.2.5 Connection Check ... 329
5.6.3 DSL ... 331
5.6.4 SHDSL ... 333
5.6.4.1 Übersicht ... 333
5.6.4.2 Konfiguration ... 334
5.6.4.3 Connection Check ... 337
5.6.5 Packet Capture ... 339

5.7 Menü "Layer 2" ... 341
5.7.1 Layer 2-Konfiguration ... 341
5.7.2 VLAN ... 342
5.7.2.1 Allgemein ... 342
5.7.2.2 Port-basiertes VLAN ... 346
5.7.3 VXLAN (Nur beim MUM85x) ... 347

5.7.3.1 VXLAN ... 347
5.7.3.2 VTEP ... 349
5.7.3.3 VLAN Mapping ... 350
5.7.3.4 Ingress Replication ... 350
5.7.3.5 Statische MAC-Adresse ... 352
5.7.4 Dynamic MAC Aging ... 353
5.7.5 Spanning Tree ... 354
5.7.5.1 Allgemein ... 354
5.7.5.2 ST Allgemein ... 355
5.7.5.3 ST-Port ... 357
5.7.6 LLDP ... 360

5.8 Menü "Layer 3 (IPv4)" ... 362
5.8.1 Statische Routen ... 362
5.8.2 Subnetze ... 364
5.8.2.1 Übersicht ... 364
5.8.2.2 Konfiguration ... 366
5.8.3 NAT ... 367
5.8.3.1 NAT Allgemein ... 367
5.8.3.2 Masquerading ... 368
5.8.3.3 NAPT ... 368
5.8.3.4 Source-NAT ... 370
5.8.3.5 NETMAP ... 372
5.8.4 VRRPv3 ... 375
5.8.4.1 Router ... 375
5.8.4.2 Konfiguration ... 378
5.8.4.3 Adressübersicht ... 379
5.8.4.4 Adresskonfiguration ... 380
5.8.4.5 Schnittstellenüberwachung ... 381
5.8.4.6 Adressenüberwachung ... 383

5.9 Menü "Layer 3 (IPv6)" ... 384
5.9.1 Subnetze ... 384
5.9.2 NAT ... 387
5.9.2.1 Masquerading ... 387

5.10 Menü "Security" ... 388
5.10.1 Benutzer ... 388
5.10.1.1 Lokale Benutzer ... 388
5.10.1.2 Rollen ... 391
5.10.1.3 Gruppen ... 393
5.10.2 Passwörter ... 395
5.10.2.1 Optionen ... 396
5.10.3 AAA ... 397
5.10.3.1 Allgemein ... 397
5.10.3.2 RADIUS-Client ... 398
5.10.4 Zertifikate ... 401
5.10.4.1 Übersicht ... 401
5.10.4.2 Zertifikate ... 403
5.10.5 Firewall ... 406
5.10.5.1 Allgemein ... 406
5.10.5.2 Vordefinierte Regeln ... 407
5.10.5.3 Dynamische Regeln ... 409
5.10.5.4 IP-Dienste ... 414

5.10.5.5 ICMP-Dienste ... 415
5.10.5.6 IP-Protokolle ... 416
5.10.5.7 IP-Regeln ... 417
5.10.6 IPsec VPN ... 420
5.10.6.1 Allgemein ... 420
5.10.6.2 Remote-Endpunkt ... 421
5.10.6.3 Verbindungen ... 423
5.10.6.4 Authentifizierung ... 427
5.10.6.5 Phase 1 ... 428
5.10.6.6 Phase 2 ... 431
5.10.7 OpenVPN Client ... 434
5.10.7.1 Allgemein ... 434
5.10.7.2 Verbindungen ... 435
5.10.7.3 Remote ... 438
5.10.7.4 Authentifizierung ... 439
5.10.8 Brute Force Prevention ... 440

**6 Instandhalten und Warten ... 443**

6.1 Firmware ... 443
6.2 Gerätekonfiguration mit PRESET-PLUG ... 443
6.3 Firmware-Update über WBM ... 445
6.4 Firmware-Update über WBM und CLI nicht möglich ... 447
6.5 Wiederherstellen der Werkseinstellungen ... 448

**A Anhang A "Befehl-SMS" ... 451**

A.1 Befehl-SMS ... 451

**B Anhang B "Syslog-Meldungen" ... 455**

B.1 Format der Syslog-Meldungen ... 455
B.2 Parameter in Syslog-Meldungen ... 456
B.3 Syslog-Meldungen ... 457

**C Anhang C "Verwendete Verschlüsselungsverfahren (Ciphers)" ... 467**

C.1 SSL ... 467
C.2 OpenVPN ... 468
C.3 SINEMA RC ... 469
C.4 cSRP ... 469
C.5 SSH CLI ... 470
C.6 SNMP ... 472
C.7 RADIUS ... 472
C.8 IPsec ... 472

**Index ... 475**

# Einleitung 1

## 1.1 Zweck des Projektierungshandbuchs

Dieses Projektierungshandbuch soll Sie in die Lage versetzen, das Gerät in Betrieb zu nehmen und zu bedienen. Es richtet sich primär an Fachkräfte für Planung, Inbetriebnahme und Instandhaltung sowie an Security-Verantwortliche. Es vermittelt die notwendigen Kenntnisse über die Konfiguration der Geräte.

Wie Sie die Geräte fachgerecht montieren und anschließen, ist in der Betriebsanleitung des jeweiligen Geräts beschrieben.

## 1.2 Gültigkeitsbereich

Dieses Projektierungshandbuch behandelt die folgenden Produkte:

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

Das Projektierungshandbuch gilt für die folgende Firmware-Version:

- SCALANCE M800 / S615 Firmware ab Version V7.2

## 1.3 Ergänzende Dokumentation

### Dokumentation im Internet

Die aktuelle Version der Dokumente finden Sie im Internet unter (https://support.industry.siemens.com/cs/ww/de/ps/15982/man)

Geben Sie in den Suchfilter den Namen oder die Artikelnummer des Produkts ein.

## Einordnung in die Dokumentationslandschaft

Zum Thema Remote Network gibt es außer dem Projektierungshandbuch, das Sie gerade lesen, noch folgende Dokumentationen:

- Projektierungshandbuch: SCALANCE M-800 Command Line Interface
  Dieses Dokument enthält die CLI-Befehle, die von SCALANCE M-800-Geräten unterstützt werden.
- Getting Started
  Diese Dokumente zeigen anhand von Beispielen die Projektierung des SCALANCE M-800/ S615.
- Betriebsanleitungen
  Diese Dokumente enthalten Informationen zu Montage, Anschließen, Instandhalten und Warten der folgenden Produkte.

| Betriebsanleitung | Produkte |
|---|---|
| SCALANCE M804PB | SCALANCE M804PB |
| SCALANCE M874, M876 | SCALANCE M874-2<br>SCALANCE M874-3<br>SCALANCE M876-3<br>SCALANCE M876-4 |
| SCALANCE M812, M816 | SCALANCE M812-1<br>SCALANCE M816-1 |
| SCALANCE M826 | SCALANCE M826-2 |
| SCALANCE MUM856-1 | SCALANCE MUM856-1 |
| SCALANCE MUM853-1 | SCALANCE MUM853-1 |

- Betriebsanleitung SINEMA RC Server
  Dieses Dokument finden Sie auf den Internet-Seiten des Siemens Industry Online Support. Es enthält Informationen zur Installation, Konfiguration und Bedienung der Anwendung SINEMA Remote Connect Server.
- IP-basierte Remote Networks
  In diesem Dokument erhalten Sie eine Übersicht über die möglichen Konstellationen eines IP-basierten Remote Networks mit den Voraussetzungen und den Link zur ausführlichen Projektierungsanleitung erläutert.
  Sie finden dieses Dokument im Internet unter folgender Beitrags-ID: 26662448 (https://support.industry.siemens.com/cs/ww/de/view/26662448)
- Einstieg in Industrial Remote Communication
  In diesem Beitrag finden Sie - thematisch geordnet - eine Übersicht mit Links zu den wichtigsten Beiträgen zu Industrial Remote Communication im Siemens Industry Online Support.
  Sie finden diesen Beitrag unter folgender Beitrags-ID: 64721753 (https://support.industry.siemens.com/cs/ww/de/view/64721753)

## 1.4 Weiterführende Dokumentation

In den Systemhandbüchern "Industrial Ethernet / PROFINET Industrial Ethernet" und "Industrial Ethernet / PROFINET Passive Netzkomponenten" erhalten Sie Hinweise zu weiteren SIMATIC NET-Produkten, die Sie gemeinsam mit den Geräten dieser Produktlinie in einem Industrial Ethernet-Netzwerk betreiben können.

Sie finden dort u. a. optische Leistungsdaten der Kommunikationspartner, die Sie für den Aufbau benötigen.

Sie finden die Systemhandbücher hier:

- Auf den Internetseiten des Siemens Industry Online Support unter folgenden Beitrags-IDs:
  - 27069465 (https://support.industry.siemens.com/cs/de/de/view/27069465)
    Industrial Ethernet / PROFINET Industrial Ethernet Systemhandbuch
  - 84922825 (https://support.industry.siemens.com/cs/de/de/view/84922825)
    Industrial Ethernet / PROFINET Passive Netzkomponenten Systemhandbuch

## 1.5 Neu in der Version

Im Folgenden finden Sie eine Übersicht der wichtigsten Funktionserweiterungen:

- Standortbestimmung über GPS (nur beim MUM85x)
- Geofencing (nur beim MUM85x)
- GPS-Zeit (nur beim MUM85x)
- Packet Capture (nur beim MUM85x)
- Fast Engine Startup (nur beim MUM85x)
- eSIM-Unterstützung (nur beim MUM85x mit eingebauter eSIM)
- Secure Boot-Unterstützung (nur beim MUM85x)
- TCP-Ereignis: VPN

**Hinweis**

**eSIM und Secure Boot-Unterstützung**

Die Funktionen eSIM und Secure Boot sind in Geräten SCALANCE MUM85x ab Hardware-Ausgabestand 2 verfügbar. Der Hardware-Ausgabestand wird im WBM unter "Information > I&M" oder im CLI mit dem Befehl "`show im`" angezeigt.

### Siehe auch

Identification & Maintenance (Seite 133)

## 1.6 Verwendete Symbole

In diesem Handbuch verwendete Symbole haben folgende Bedeutung:

| | |
|---|---|
| MUM85x<br><br>(Nur beim MUM856) | Das beschriebene Kapitel / der beschriebene Abschnitt / der beschriebene Parameter ist nur für SCALANCE MUM856-1 relevant |
| M87x<br><br>oder<br>(bei M87x) | Das beschriebene Kapitel / der beschriebene Abschnitt / der beschriebene Parameter ist nur für<br>SCALANCE M874-2 / M874-3 / M876-3 / M876-4 relevant. |
| (nicht beim M874-2) | Der beschriebene Parameter ist nicht für SCALANCE M874-2 relevant. |
| (nur beim M876-4) | Der beschriebene Parameter ist nur für SCALANCE M876-4 relevant. |
| M81x | Das beschriebene Kapitel / der beschriebene Abschnitt / der beschriebene Parameter ist nur für<br>SCALANCE M812-1 / M816-1 relevant. |
| M826 | Das beschriebene Kapitel / der beschriebene Abschnitt / der beschriebene Parameter ist nur für<br>SCALANCE M826-2 relevant. |
| ~~M812~~ | Das beschriebene Kapitel / der beschriebene Abschnitt / der beschriebene Parameter ist nicht für<br>SCALANCE M812-1 relevant. |
| ~~M826~~ | Das beschriebene Kapitel / der beschriebene Abschnitt / der beschriebene Parameter ist nicht für<br>SCALANCE M826 relevant. |
| M804PB | Das beschriebene Kapitel / der beschriebene Abschnitt / der beschriebene Parameter ist für SCALANCE M804PB relevant. |
| ~~M804PB~~ | Das beschriebene Kapitel / der beschriebene Abschnitt / der beschriebene Parameter ist nicht für SCALANCE M804PB relevant. |

## 1.7 Verwendete Bezeichnungen

### Verwendete Abkürzungen

Die Informationen in dem Projektierungshandbuch gelten häufig nicht nur für eine Produktvariante.

In diesen Fällen werden abkürzende Bezeichnungen verwendet, um nicht alle Typenbezeichnungen aufzählen zu müssen.

Die folgende Tabelle zeigt die Zuordnung von Abkürzungen und Produktvarianten.

| **Die Bezeichnung . . . steht für . . .** | **Produktname** |
|---|---|
| M874-2 | SCALANCE M874-2 |
| M874-3 | SCALANCE M874-3 |
| M876-3 | SCALANCE M876-3 |

| Die Bezeichnung . . . steht für . . . | Produktname |
|---|---|
| M876-4 | SCALANCE M876-4 |
| M87x | SCALANCE M874-2<br>SCALANCE M874-3<br>SCALANCE M876-3<br>SCALANCE M876-4 |
| M812 | SCALANCE M812-1 |
| M816 | SCALANCE M816-1 |
| M81x | SCALANCE M812-1<br>SCALANCE M816-1 |
| M826 | SCALANCE M826-2 |
| M804PB | SCALACNE M804PB |
| M-800 | SCALANCE M874-2<br>SCALANCE M874-3<br>SCALANCE M876-3<br>SCALANCE M876-4<br>SCALANCE M812-1<br>SCALANCE M816-1<br>SCALANCE M826-2<br>SCALACNE M804PB<br>SCALANCE MUM856<br>SCALANCE MUM853 |
| MUM85x | SCALANCE MUM856<br>SCALANCE MUM853 |

## 1.8 SIMATIC NET-Glossar

### SIMATIC NET-Glossar

Das SIMATIC NET-Glossar beschreibt Fachbegriffe, die möglicherweise in diesem Dokument verwendet werden.

Sie finden das SIMATIC NET-Glossar beim Siemens Industry Online Support unter folgender Adresse:

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

## 1.9 Security-Hinweise

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen.

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und

kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen einen Bestandteil eines solchen Konzepts.

Die Kunden sind dafür verantwortlich, unbefugten Zugriff auf ihre Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Diese Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und nur wenn entsprechende Schutzmaßnahmen (z.B. Firewalls und/oder Netzwerksegmentierung) ergriffen wurden.

Weiterführende Informationen zu möglichen Schutzmaßnahmen im Bereich Industrial Security finden Sie unter:
https://www.siemens.com/industrialsecurity (https://www.siemens.com/industrialsecurity)

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Produkt-Updates anzuwenden, sobald sie zur Verfügung stehen und immer nur die aktuellen Produktversionen zu verwenden. Die Verwendung veralteter oder nicht mehr unterstützter Versionen kann das Risiko von Cyber-Bedrohungen erhöhen.

Um stets über Produkt-Updates informiert zu sein, abonnieren Sie den Siemens Industrial Security RSS Feed unter:
https://www.siemens.com/cert (https://www.siemens.com/cert)

## 1.10 Fehlerfall

Senden Sie das Gerät im Fehlerfall an Ihre Siemens-Vertretung zur Reparatur ein. Eine Reparatur vor Ort ist nicht erlaubt.

## 1.11 Außerbetriebnahme

Nehmen Sie das Gerät ordnungsgemäß außer Betrieb, um zu verhindern, dass unbefugte Personen an vertrauliche Daten im Gerätespeicher gelangen.

Setzen Sie das Gerät hierzu auf Werkseinstellungen zurück.

Setzen Sie auch das Speichermedium auf Werkseinstellungen zurück.

## 1.12 Recycling und Entsorgung



Die Produkte sind schadstoffarm, recyclingfähig und erfüllen die Anforderungen der WEEE-Richtlinie 2012/19/EU zur Entsorgung von Elektro- und Elektronik-Altgeräten.

Entsorgen Sie die Produkte nicht bei öffentlichen Entsorgungsstellen.

Für ein umweltverträgliches Recycling und die Entsorgung Ihres Altgeräts wenden Sie sich an einen zertifizierten Entsorgungsbetrieb für Elektronikschrott oder an Ihren Siemens-Ansprechpartner (Produktrückgabe (https://support.industry.siemens.com/cs/ww/de/view/109479891)).

Beachten Sie unterschiedliche länderspezifische Regelungen.

## 1.13 Firmware

Die Firmware finden Sie auf den Internetseiten des Siemens Industry Online Support: (https://support.industry.siemens.com/cs/ww/de/ps/28821/dl)

### Hinweis zum Firmware-/Software-Support

Informieren Sie sich regelmäßig über neue Firmware-/Software-Versionen oder Sicherheits-Updates und wenden Sie diese an. Ab der Veröffentlichung einer neuen Version werden Vorgängerversionen nicht mehr unterstützt und nicht gewartet.

### Training, Service & Support

Informationen zu Training, Service & Support finden Sie in dem mehrsprachigen Dokument "DC_support_99.pdf", welches sich auf dem mitgelieferten Datenträger mit Dokumentation befindet.

## 1.14 Lizenzbedingungen Open Source

### Lizenzbedingungen

**Hinweis**

**Open Source Software**

Lesen Sie die Lizenzbedingungen zur Open Source Software genau durch, bevor Sie das Produkt nutzen.

Sie finden die Lizenzbedingungen in folgenden Dokumenten, die sich auf dem mitgelieferten Datenträger befinden:

- OSS_Scalance-M-800-S615_86.pdf
- OSS_SCALANCE_MuM856_86.pdf

## 1.15 Marken

Die folgenden und möglicherweise andere Namen, die nicht mit dem Zeichen für eingetragene Marken ® gekennzeichnet sind, sind eingetragene Marken der Siemens AG:

SCALANCE, SINEMA, KEY-PLUG, C-PLUG

# Security-Empfehlung

# 2

## 2.1 Security-Empfehlungen

Um unbefugten Zugriff auf das Gerät und/oder Netzwerk zu verhindern, beachten Sie folgende Security-Empfehlungen.

**Hinweis**

Beachten Sie, dass GPS-Signale von schädlichen Drittgeräten verschleiert oder blockiert werden können.

### Allgemein

- Prüfen Sie das Gerät regelmäßig, um sicherzustellen, dass diese Empfehlungen und/oder andere interne Sicherheitsrichtlinien eingehalten werden.
- Bewerten Sie die Sicherheit Ihres Standorts und verwenden Sie ein Zellenschutzkonzept mit geeigneten Produkten. Für weitere Informationen siehe Link: (https://www.siemens.com/industrialsecurity)
- Wenn das interne und externe Netzwerk entkoppelt sind, kann ein Angreifer nicht auf interne Daten zugreifen. Wenn möglich, betreiben Sie das Gerät nur innerhalb eines geschützten Netzwerkbereichs.
- Nutzen Sie VPN, um die Kommunikation von und zu den Geräten zu verschlüsseln und zu authentifizieren.
- Nutzen Sie für die Datenübertragung über ein unsicheres Netzwerk einen verschlüsselten VPN-Tunnel (IPsec, OpenVPN).
- Prüfen Sie die Benutzerdokumentation anderer Siemens-Produkte, die zusammen mit dem Gerät verwendet werden, auf weitere Sicherheitsempfehlungen.
- Sorgen Sie mit Hilfe des Remote-Logging dafür, dass die Systemprotokolle an einen zentralen Logging-Server weitergeleitet werden. Achten Sie darauf, dass der Server sich innerhalb des geschützten Netzwerks befindet, und schauen Sie regelmäßig in den Protokollen nach, ob potenzielle Sicherheitsverletzungen oder Schwachstellen vorliegen.

### Authentifizierung

**Hinweis**

**Zugänglichkeitsrisiko - Gefahr des Datenverlusts**

Verlieren Sie die Passwörter für das Gerät nicht. Der Zugriff auf das Gerät kann nur durch Zurücksetzen des Geräts auf die Werkseinstellungen wiederhergestellt werden, wodurch sämtliche Konfigurationsdaten entfernt werden.

- Ersetzen Sie die Standardpasswörter für alle Benutzerkonten, Zugriffsmodi und Anwendungen (sofern zutreffend), bevor Sie das Gerät einsetzen.
- Definieren Sie Regeln für die Vergabe von Passwörtern.
- Verwenden Sie Passwörter mit hoher Passwortstärke. Vermeiden Sie schwache Passwörter (wie Passwort1, 123456789, abcdefgh) oder sich wiederholende Zeichen (wie abcabc). Diese Empfehlung gilt auch für auf dem Gerät konfigurierte symmetrische Passwörter/ Schlüssel.
- Stellen Sie sicher, dass Passwörter geschützt werden und nur berechtigtem Personal mitgeteilt werden.
- Verwenden Sie nicht für mehrere Benutzernamen und Systeme die gleichen Passwörter.
- Bewahren Sie Passwörter an einem sicheren Ort (nicht online) auf, damit Sie sie bei Verlust zur Hand haben.
- Ändern Sie regelmäßig Ihre Passwörter, um die Sicherheit zu erhöhen.
- Ein Passwort muss gewechselt werden, wenn es unbefugten Personen bekannt geworden ist oder der Verdacht dazu besteht.
- Wenn die Benutzerauthentifizierung über RADIUS ausgeführt wird, stellen Sie sicher, dass sämtliche Kommunikation innerhalb des Sicherheitsumfelds erfolgt oder durch einen sicheren Kanal geschützt wird.
- Achten Sie auf Link-Layer-Protokolle, die keine eigene Authentifizierung zwischen den Endpunkten bieten, wie ARP oder IPv4. Ein Angreifer könnte Schwachstellen in diesen Protokollen ausnutzen, um mit Ihrem Layer-2-Netzwerk verbundene Hosts, Switches und Router anzugreifen, zum Beispiel durch Manipulation (Poisoning) der ARP-Caches von Systemen im Subnetz und anschließendem Abfangen des Datenverkehrs. Gegen nicht sichere Layer-2-Protokolle sind angemessene Sicherheitsvorkehrungen zu ergreifen, um unbefugten Zugriff auf das Netzwerk zu verhindern. Unter anderem kann der physische Zugriff auf das lokale Netzwerk gesichert oder es können sichere höherschichtige Protokolle verwendet werden.

### Zertifikate und Schlüssel

- Im Gerät ist ein vorinstalliertes Webserver-Zertifikat (RSA, 2048 Bit-Schlüssellänge) und ein SSH Private Key vorhanden. Ersetzen Sie dieses Zertifikat durch ein selbst erstelltes höherwertiges Zertifikat mit Schlüssel. Verwenden Sie ein Zertifikat, das entweder durch eine zuverlässige externe oder interne Zertifizierungsstelle signiert ist. Sie können das Zertifikat im WBM über "System > Laden und Speichern" installieren.
- Nutzen Sie eine Zertifizierungsstelle inklusive Schlüsselwiderruf und -verwaltung, um die Zertifikate zu signieren.
- Verwenden Sie passwortgeschützte Zertifikate im Format "PKCS #12".
- Verwenden Sie Zertifikate mit einer Schlüssellänge von 4096 Bit.
- Stellen Sie sicher, dass benutzerdefinierte private Schlüssel geschützt und unzugänglich für unbefugte Personen sind.
- Ändern Sie bei Verdacht auf eine Sicherheitsverletzung sofort alle Zertifikate und Schlüssel.

- SSH- und SSL-Schlüssel stehen Admin-Benutzern zur Verfügung. Stellen Sie sicher, dass Sie geeignete Sicherheitsvorkehrungen ergreifen, wenn Sie das Gerät außerhalb der vertrauten Umgebung versenden:
  - Ersetzen Sie die SSH- und SSL-Schlüssel vor dem Versand durch Wegwerfschlüssel.
  - Nehmen Sie die vorhandenen SSH- und SSL-Schlüssel außer Betrieb. Erstellen und Programmieren Sie bei Rückkehr des Geräts neue Schlüssel für das Gerät.
- Verifizieren Sie Zertifikate anhand des Fingerprints auf Server- und Clientseite, um "Man-in-the-middle"-Angriffe zu verhindern. Verwenden Sie hierzu einen zweiten, sicheren Übertragungsweg.
- Bevor Sie das Gerät zur Reparatur an Siemens zurückschicken, ersetzen Sie die aktuellen Zertifikate und Schlüssel durch temporäre Wegwerfzertifikate und -schlüssel, die bei der Rückkehr des Geräts zerstört werden können.

### Physischer/ Remote-Zugriff

- Betreiben Sie die Geräte wenn möglich nur in einem geschützten Netzwerkbereich. Angreifer können von Außen nicht auf interne Daten zugreifen, wenn das interne und externe Netzwerk voneinander getrennt sind.
- Beschränken Sie den physischen Zugang auf das Gerät ausschließlich auf vertrauenswürdiges Personal.
  Die Speicherkarte bzw. der PLUG (C-PLUG, KEY-PLUG, CLP) enthalten sensible Daten, wie Zertifikate und Schlüssel, die ausgelesen und verändert werden können. Ein Angreifer, der im Besitz der Wechselmedien des Geräts ist, könnte kritische Informationen wie Zertifikate, Schlüssel usw. extrahieren oder die Medien neu programmieren.
- Sperren Sie ungenutzte physische Ports auf dem Gerät. Ungenutzte Ports können verwendet werden, um unerlaubt auf die Anlage zuzugreifen.
- Es wird dringend empfohlen, den Schutz vor Brute-Force-Angriffen (BFA) aktiviert zu lassen, um zu verhindern, dass sich Fremde unbefugten Zugriff auf das Gerät verschaffen. Für weitere Informationen siehe Projektierungshandbücher, Kapitel "Brute Force Prevention (Seite 440)".
- Verwenden Sie für die Kommunikation über nicht sichere Netzwerke, wenn möglich, die VPN-Funktionalität, um die Kommunikation zu verschlüsseln und zu authentifizieren.
- Wenn Sie eine sichere Verbindung zu einem Server (beispielsweise für ein sicheres Upgrade) herstellen, achten Sie darauf, dass serverseitig starke Verschlüsselungsverfahren und Protokolle konfiguriert sind.
- Beenden Sie Managementverbindungen (z.B. HTTPS, SSH) ordnungsgemäß.
- Stellen Sie sicher, dass das Gerät vollständig abgeschaltet wurde, bevor Sie es aus dem Betrieb nehmen. Für weitere Informationen siehe "Außerbetriebnahme (Seite 16)".
- Es wird empfohlen einen nicht verwendeten PLUG zu formatieren.

### Hardware/ Software

- Verwenden Sie, wann immer möglich, VLANs als Schutz vor Denial-of-Service (DoS)-Angriffen und vor unbefugtem Zugriff.
- Beschränken Sie den Zugriff auf das Gerät durch Firewall-Regeln oder Regeln in einer Zugriffsliste (ACL – Access Control List).
- Ausgewählte Dienste sind in der Firmware standardmäßig aktiviert. Es wird empfohlen, nur die für Ihre Installation unbedingt erforderlichen Dienste zu aktivieren.
  Für weitere Informationen zu verfügbaren Diensten siehe "Liste verfügbarer Dienste (Seite 24)".
- Um sicherzustellen, dass die sichersten verfügbaren Verschlüsselungsverfahren eingesetzt werden, verwenden Sie die neueste mit dem Produkt kompatible Webbrowser-Version,. Außerdem ist in den neuesten Webbrowser-Versionen von Mozilla Firefox, Google Chrome und Microsoft Edge die 1/n-1-Datensatzaufteilung aktiviert, wodurch das Risiko von Angriffen wie SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (z. B. BEAST) verringert wird.
- Stellen Sie sicher, dass die neueste Firmware-Version einschließlich aller sicherheitsrelevanten Patches installiert ist.
  Aktuelle Informationen zu Sicherheits-Patches für Siemens-Produkte finden Sie auf der Website Industrial Security (https://www.siemens.com/industrialsecurity) oder ProductCERT-Sicherheitshinweise (https://www.siemens.com/cert/de/cert-security-advisories.htm).
  Updates zu den Produkt-Sicherheitshinweisen von Siemens erhalten Sie, indem Sie sich beim RSS-Feed auf der Webseite der ProductCERT-Sicherheitshinweise anmelden oder @ProductCert auf Twitter folgen.
- Aktivieren Sie nur die Dienste, die auf dem Gerät verwendet werden, einschließlich physischer Ports. Freie physische Ports können potenziell dazu verwendet werden, Zugriff auf das Netzwerk hinter dem Gerät zu erlangen.
- Verwenden Sie die Authentifizierungs- und Verschlüsselungsmechanismen von SNMPv3 wenn möglich. Nutzen Sie starke Passwörter.
- Konfigurationsdateien können vom Gerät heruntergeladen werden. Stellen Sie sicher, dass die Konfigurationsdateien angemessen geschützt sind.
  Konfigurationsdateien können beim Download durch ein Passwort geschützt werden. Passwörter geben Sie auf der WBM-Seite "System > Laden & Speichern > Passwörter (Seite 208)" ein.
- Bei Verwendung von SNMP (Simple Network Management Protocol):
  - Konfigurieren Sie SNMP so, dass bei Authentifizierungsfehlern eine Benachrichtigung erzeugt wird.
    Für weitere Informationen siehe WBM "System > SNMP > Benachrichtigungen (Seite 230)".
  - Stellen Sie sicher, dass die Standard-Community-Strings in eindeutige Werte geändert werden.
  - Verwenden Sie SNMPv3, wann immer möglich. SNMPv1 und SNMPv2c gelten als unsicher und sollten nur bei absoluter Notwendigkeit verwendet werden.
  - Verhindern Sie nach Möglichkeit den Schreibzugriff.

### Sichere/ nicht sichere Protokolle

- Verwenden Sie sichere Protokolle, wenn der Zugriff auf das Gerät nicht durch physische Schutzmaßnahmen verhindert wird.
- Beschränken Sie die Verwendung nicht sicherer Protokolle. Während einige Protokolle sicher sind (z. B. HTTPS, SSH, 802.1X usw.), wurden andere nicht zu dem Zweck entwickelt, Anwendungen abzusichern (z.B. SNMPv1/v2c, RSTP usw.).
  Treffen Sie daher geeignete Sicherheitsvorkehrungen gegen nicht sichere Protokolle, um unbefugten Zugriff auf das Gerät/Netzwerk zu verhindern. Setzen Sie unsichere Protokolle auf dem Gerät über eine gesicherte Verbindung (z. B. SINEMA RC) ein.
- Wenn nicht sichere Protokolle und Dienste erforderlich sind, stellen Sie sicher, dass das Gerät in einem geschützten Netzwerkbereich betrieben wird.
- Prüfen Sie die Notwendigkeit der Nutzung folgender Protokolle:
  - Telnet
  - HTTP
  - Broadcast-Pings
  - Nicht authentifizierte und unverschlüsselte Schnittstellen
  - ICMP (redirect)
  - LLDP
  - DHCP-Optionen 66/67
  - SNTP
  - NTP
  - TFTP
  - TIA Portal Cloud Connector (beim SCALANCE MUM85x nicht verfügbar)
  - VRRPv3
  - DNS
  - SNMPv1/v2c

- Falls für ein Protokoll eine sichere Alternative verfügbar ist, nutzen Sie diese.
  Die folgenden Protokolle bieten sichere Alternativen:
  - SNMPv1/v2 → SNMPv3
    Prüfen Sie die Notwendigkeit der Nutzung von SNMPv1. SNMPv1 ist als unsicher eingestuft. Nutzen Sie die Möglichkeit den Schreibzugriff zu unterbinden. Das Produkt bietet entsprechende Einstellmöglichkeiten.
    Wenn SNMP aktiviert ist, ändern Sie die Community-Namen. Wenn kein uneingeschränkter Zugriff erforderlich ist, beschränken Sie den Zugriff über SNMP.
  - HTTP → HTTPS
  - Telnet → SSH
  - NTP → Secure NTP
  - TFTP → SFTP
  - TIA Portal Cloud Connector über eine sichere Verbindung. Verwenden Sie den im Produkt integrierten "TIA Portal Cloud Connector" über eine VPN-Lösung (z.B. SINEMA RC). Konfigurieren Sie die Firewall Einstellungen des SCALANCE M800/S615 (z.B. Vordefinierte IPv4 Regeln "Cloud Connector", um den unbefugten Zugriff von Netzteilnehmer auf den "TIA Portal Cloud Connector Server" zu verhindern).
- Beschränken Sie mit einer Firewall die nach außen angebotenen Dienste und Protokolle auf das erforderliche Mindestmaß.
- Aktivieren Sie für die DCP-Funktion nach der Inbetriebnahme den Modus "Schreibgeschützt".
- Verwenden Sie bei Befehl-SMS den Identifier, um Ihre SMS-Nachrichten abzusichern. Hierzu können Sie bei SCALANCE M-Gerät einen einstellbaren Wert definieren, der zusätzlich zur Rufnummer mit der empfangenen Kennung der SMS identisch sein muss. Sie konfigurieren den Identifier auf der WBM-Seite "System > SMS > Befehl-SMS (Seite 273)" oder mit den CLI-Befehlen `sms-cmd idx indentifier` und `sms-cmd sender`.

## 2.2 Verfügbare Dienste

### Liste verfügbarer Dienste

Nachfolgend werden alle verfügbaren Protokolle und Dienste sowie ihre Ports aufgelistet, über die auf das Gerät zugegriffen werden kann.

Die Tabelle umfasst folgende Spalten:

- **Dienst**
  Die Dienste, die das Gerät unterstützt.
- **Protokoll/ Portnummer**
  Portnummer, die dem Protokoll zugeordnet ist.
- **Voreingestellter Portstatus**
  Bei dem Status des Ports im Auslieferungszustand (Werkseinstellung) wird zwischen lokalem und externem Zugriff unterschieden.
  - Lokaler Zugriff: Auf den Port wird über eine lokale Verbindung (vlan1) zugegriffen.
  - Externer Zugriff: Auf den Port wird über eine externe Verbindung (vlan2) zugegriffen.

- **Port / Dienst konfigurierbar**
  Gibt an, ob die Port-Nummer oder der Dienst über das WBM / CLI konfigurierbar sind.
- **Authentifizierung**
  Gibt an, ob eine Authentifizierung des Kommunikationspartners stattfindet oder ob eine Authentifizierung konfiguriert werden kann.
- **Verschlüsselung**
  Gibt an, ob die Übertragung verschlüsselt ist oder ob die Verschlüsselung konfiguriert werden kann.

| Dienst | Protokoll/ Portnummer | Voreingestellter Portstatus | | Konfigurierbar | | Authentifizierung | Verschlüsselung [2] |
|---|---|---|---|---|---|---|---|
| | | Lokaler Zugriff | Externer Zugriff [1] | Port | Dienst | | |
| DHCPv4 Client | UDP/68 | Geschlossen [3] | Geschlossen | -- | ✓ | -- | -- |
| DHCPv6 Client | TCP/546<br>UDP/546 | Offen | Offen | -- | -- | -- | -- |
| DHCPv4-Server | UDP/67 | Geschlossen | Geschlossen [4] | -- | ✓ | -- | -- |
| DNS Client | TCP/53<br>UDP/53 | Nur ausgehend | Nur ausgehend | -- | ✓ | -- | -- |
| DNS Server | TCP/53<br>UDP/53 | Offen [5] | Geschlossen | -- | ✓ | -- | -- |
| DynDNS | TCP/80<br>UDP/80<br>TCP/443<br>UDP/443 | Nur ausgehend | Nur ausgehend | -- | ✓ | ✓ | -- |
| HTTP | TCP/80 | Offen | Geschlossen | ✓ | ✓ | ✓ | -- |
| HTTP Proxy | TCP/3128<br>TCP/8080 | Nur ausgehend | Nur ausgehend | ✓ | ✓ | Optional | -- |
| HTTPS WBM Server/Client | TCP/443 | Offen | Geschlossen | ✓ | ✓ | ✓ | ✓ |
| IPsec/IKE | UDP/500<br>UDP/4500 | Geschlossen | Geschlossen | -- | ✓ | ✓ | ✓ |
| NTP Client | UDP/123 | Nur ausgehend | Nur ausgehend | ✓ | ✓ | -- | -- |
| NTP Client (secure) | UDP/123 | Nur ausgehend | Nur ausgehend | ✓ | ✓ | ✓ | -- |
| NTP Server | UDP/123 | Geschlossen | Geschlossen | ✓ | ✓ | -- | -- |
| NTP Server (secure) | UDP/123 | Geschlossen | Geschlossen | ✓ | ✓ | ✓ | -- |
| OpenVPN | UDP/1194<br>TCP/1194 | Nur ausgehend | Nur ausgehend | ✓ | ✓ | ✓ | ✓ |
| Ping | ICMP | Offen | Geschlossen | -- | ✓ | -- | -- |
| PROFINET | UDP/34964<br>UDP/49154<br>UDP/49155 | Offen | Geschlossen | -- | ✓ | -- | -- |
| RADIUS Client | UDP/1812 | Geschlossen | Geschlossen | ✓ | ✓ | ✓ | Optional |
| | UDP/1813 | | | | | | -- |

| Dienst | Protokoll/ Portnummer | Voreingestellter Portstatus | | Konfigurierbar | | Authentifizierung | Verschlüsselung [2] |
|---|---|---|---|---|---|---|---|
| | | Lokaler Zugriff | Externer Zugriff [1] | Port | Dienst | | |
| SFTP Server | TCP/22 | Nur ausgehend | Nur ausgehend | ✓ | ✓ | ✓ | ✓ |
| Siemens Remote Service (cRSP/ SRS) | TCP/443 | Nur ausgehend | Nur ausgehend | -- | ✓ | Optional | ✓ |
| SINEMA RC | HTTPS/443 und TCP/UDP abhängig von Serverkonfiguration | Nur ausgehend | Nur ausgehend | ✓ | ✓ | ✓ | ✓ |
| SMTP Client | TCP/25 | Nur ausgehend | Nur ausgehend | ✓ | ✓ | -- | -- |
| SMTP (secure) | TCP/465 TCP/587 | Nur ausgehend | Nur ausgehend | ✓ | ✓ | Optional | ✓ |
| SNMPv1/v2c | UDP/161 | Offen | Geschlossen | ✓ | ✓ | -- | -- |
| SNMPv3 Server | UDP/161 | Offen | Geschlossen | ✓ | ✓ | Optional | Optional |
| SNMP Trap | UDP/161 | Offen | Geschlossen | ✓ | ✓ | Optional | Optional |
| SNTP Client | UDP/123 | Geschlossen | Geschlossen | ✓ | ✓ | -- | -- |
| SSH CLI | TCP/22 | Offen | Geschlossen | ✓ | ✓ | ✓ | ✓ |
| Syslog Client | UDP/514 | Nur ausgehend | Nur ausgehend | ✓ | ✓ | -- | -- |
| Syslog Client TLS | TCP/6514 | Nur ausgehend | Nur ausgehend | ✓ | ✓ | -- | ✓ |
| Telnet | TCP/23 | Geschlossen | Geschlossen | ✓ | ✓ | ✓ | -- |
| TFTP | UDP/69 | Nur ausgehend | Nur ausgehend | ✓ | ✓ | -- | -- |
| TIA Portal Cloud Connector [6] | TCP/9023 | Geschlossen | Geschlossen | ✓ | ✓ | -- | -- |
| TCP Event | TCP/26864 | Geschlossen | Geschlossen | ✓ | ✓ | -- | -- |
| SMS Relay [7] | TCP/26864 | Geschlossen | Geschlossen | ✓ | ✓ | -- | -- |
| VXLAN [8] | UDP/4789 | Geschlossen | Geschlossen | ✓ | ✓ | -- | -- |

[1] SCALANCE M826 und M804PB ist im Auslieferungszustand (Werkseinstellung) nur der Zugriff über vlan1 möglich.

[2] Weiterführende Informationen zu verwendeten Verschlüsselungsverfahren finden Sie im Anhang zum WBM "Verwendete Verschlüsselungsverfahren (Ciphers) (Seite 467)".

[3] Nur beim SCALANCE M826 offen

[4] Nur beim SCALANCE S615 offen

[5] Nur beim SCALANCE S615 geschlossen

[6] Beim SCALANCE MUM85x nicht verfügbar

[7] Nur beim SCALANCE M87x und MUM85x verfügbar

[8] Nur beim SCALANCE MUM85x verfügbar

Nachfolgend werden alle verfügbaren Layer 2-Dienste aufgelistet, über die auf das Gerät zugegriffen werden kann.

Die Tabelle umfasst folgende Spalten:

- **Layer 2-Dienst**
  Die Layer 2-Dienste, die das Gerät unterstützt**.**
- **Voreingestellter Status**
  Der voreingestellte Zustand des Diensts (offen oder geschlossen).
- **Dienst konfigurierbar**
  Gibt an, ob der Dienst über das WBM / CLI konfigurierbar sind.

| Layer 2-Dienst | Voreingestellter Status | Konfigurierbar |
|---|---|---|
| DCP | Offen (wenn konfiguriert) | ✓ |
| LLDP | Offen (wenn konfiguriert) | ✓ |
| SIMATIC NET TIME | Offen (wenn konfiguriert) | ✓ |
| VLAN | Offen (wenn konfiguriert) | ✓ |
| VXLAN [1] | Offen (wenn konfiguriert) | ✓ |

[1] Nur beim SCALANCE MUM85x

# Beschreibung

# 3

## 3.1 Funktion

### Projektierung

Konfiguration aller Parameter mithilfe des

- Web Based Management (WBM) über HTTP und HTTPS.
- Command Line Interface (CLI) über Telnet und SSH.

### Security-Funktionen

- Router mit NAT-Funktion
  - IP-Masquerading
  - NAPT
  - SourceNAT
  - NETMAP
- Passwortschutz
- Firewall-Funktion
  - Port-Weiterleitung
  - IP-Firewall mit Stateful Packet Inspection (Layer 3 und 4)
  - Globale und benutzerdefinierte Firewall-Regeln
- VPN-Funktionen
  Für den Aufbau eines VPN (Virtual Private Network) stehen folgende Funktionen zur Verfügung
  - IPsec VPN
  - OpenVPN-Client
- SINEMA RC-Client
- Proxy-Server
- Siemens Remote Service (SRS)
- Brute Force Prevention

### Überwachung / Diagnose / Instandhalten

- LEDs
  Anzeige von Betriebszuständen über die LED-Anzeige. Weiterführende Informationen dazu finden Sie in der Betriebsanleitung des Geräts.
- Logging
  Zur Überwachung lassen sich Ereignisse protokollieren.
- SNMP
  Zum Überwachen und Steuern von Netzwerkkomponenten, wie z. B. Router oder Switches, von einer zentralen Station aus.

### Sonstige Funktionen

- Uhrzeitsynchronisation
  - NTP-Client und NTP-Server
  - Gesicherter NTP-Server
  - SIMATIC Time Client
  - SNTP-Client
- DHCP
  - DHCP-Server (internes Netz)
  - DHCP-Client
- Virtuelle Netze (VLAN)
  Zur Strukturierung von Industrial Ethernet-Netzen mit stark wachsender Teilnehmeranzahl kann ein physikalisch vorhandenes Netz in mehrere virtuellen Teilnetze unterteilt werden
- Digitaler Eingang / Digitaler Ausgang
- Dynamischer DNS-Client
- DNS-Client, DNS-Proxy und DNS-Records
- SMTP-Client
- TIA Portal Cloud Connector

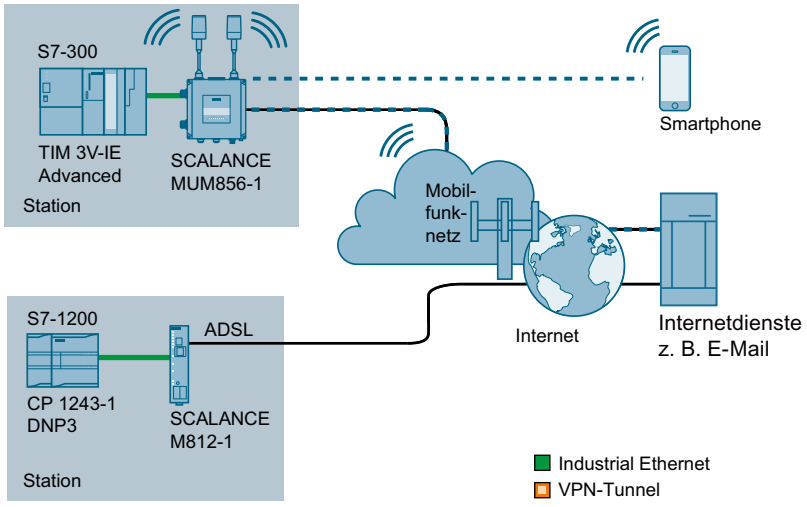
# 3.2 Konfigurationsbeispiele

## 3.2.1 Überblick

Mit SCALANCE M-800 lassen sich IP-basierte Netze anbinden. Die Anbindung kann sowohl kabelgebunden als auch drahtlos über öffentliche oder private Kommunikationsinfrastrukturen erfolgen.

| Gerät | | | Kommunikations-infrastruktur |
|---|---|---|---|
| M874-2 | Drahtlos | GPRS | Öffentliches Netz / Internet |
| M874-3 | Drahtlos | UMTS | Öffentliches Netz / Internet |
| M876-3 | Drahtlos | UMTS | Öffentliches Netz / Internet |
| M876-4 | Drahtlos | LTE | Öffentliches Netz / Internet |
| MUM856-1<br>MUM853-1 | Drahtlos | 5G | Öffentliches Netz / Internet |
| M812-1<br>M816-1 | Kabelgebunden | ADSL | Öffentliches Netz / Internet |
| M826-2 | Kabelgebunden | SHDSL | Privates Netz / Betriebseigene Kupferleitungen |

## 3.2.2 SCALANCE MUM856/M81x als Internetzugang




Eine Station können Sie über das Mobilfunknetz oder über ADSL an das Internet anbinden. Dadurch stehen Ihnen die Internetdienste zur Verfügung, z. B. E-Mail senden und empfangen.

Das Gerät kann beim Auftreten eines Alarmereignisses automatisch eine E-Mail senden, z. B. an den Netzwerkadministrator. Bei eintreffenden E-Mail-Störmeldungen kann über die Identifikation des Absenders per Webbrowser das WBM gestartet werden, um weitere Diagnoseinformationen auszulesen.

Das M874 kann beim Auftreten eines Alarmereignisses eine SMS an ein Mobiltelefon senden.

### Voraussetzung

- Das M-800 ist über einen Admin-PC erreichbar

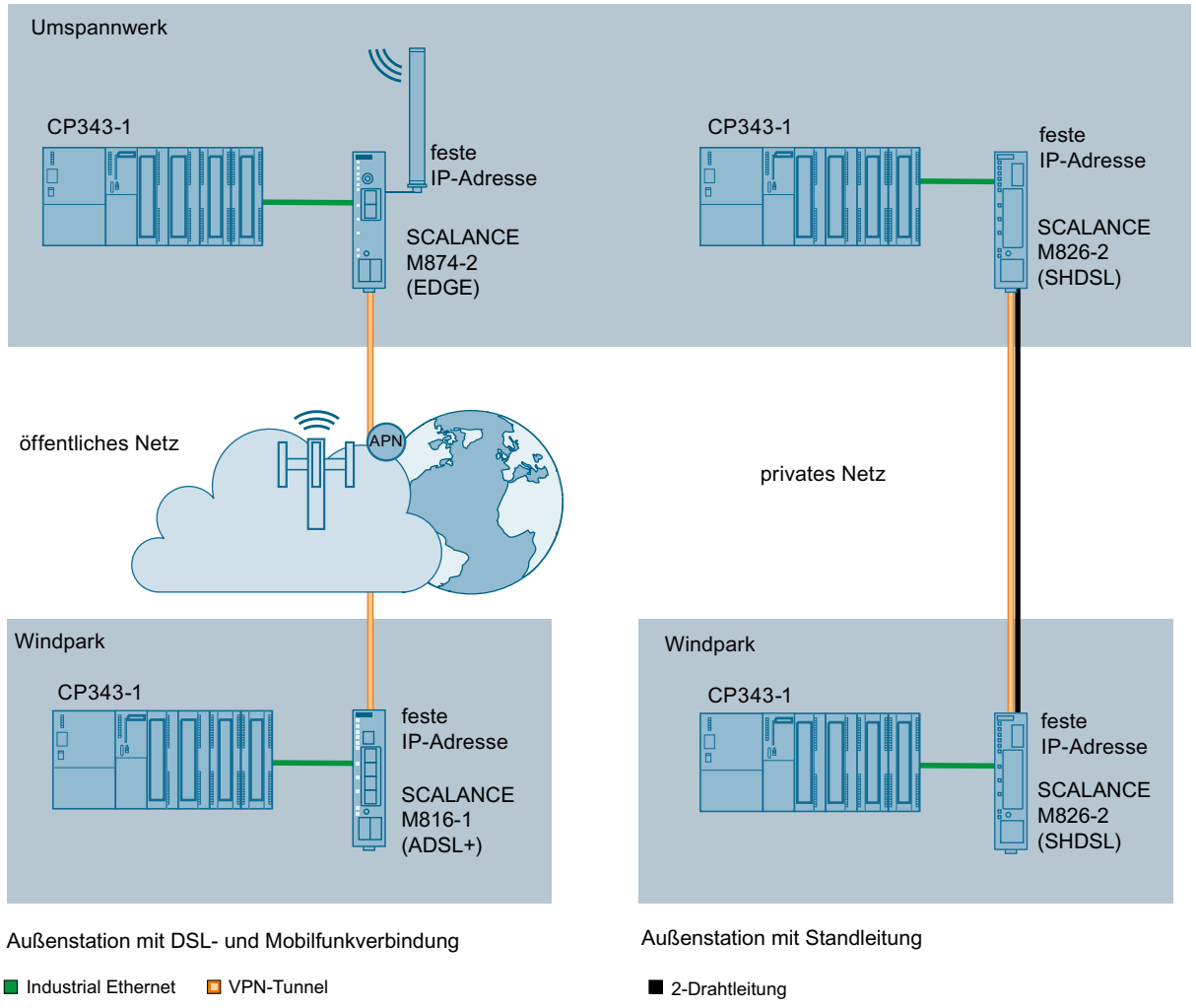
### Vorgehensweise

Um den Internetzugang einzurichten, gehen Sie folgendermaßen vor:

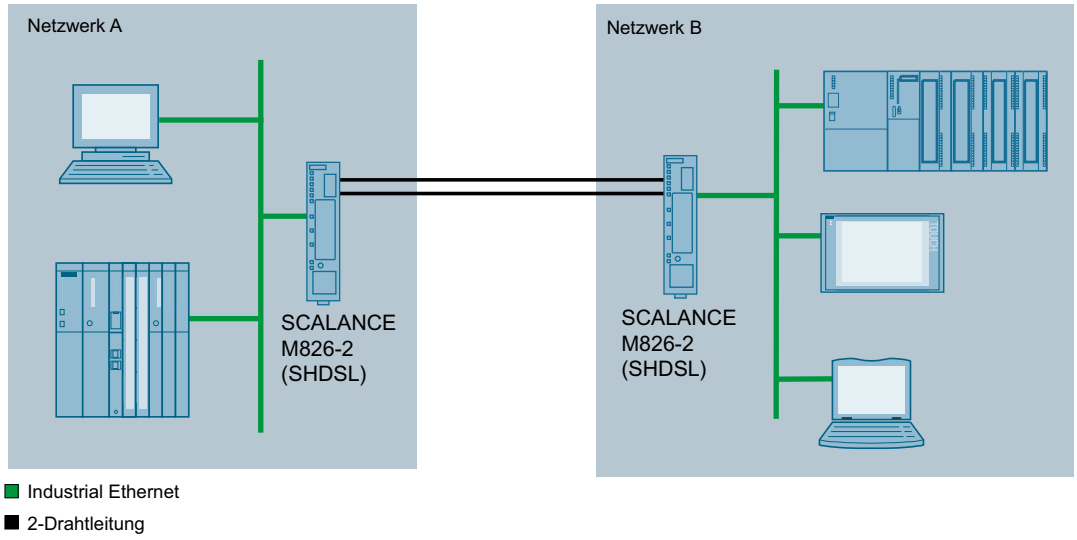
1. Stellen Sie eine Verbindung zum WAN her, siehe Kapitel Interfaces (Seite 312).
2. Um den Zugriff auf die gewünschten Internetdienste zu ermöglichen, richten Sie Firewall-Regeln ein, siehe Kapitel Firewall (Seite 406).
3. Richten Sie Ihre Anwendung für die Internetdienste ein.

### 3.2.3 Direkte Kommunikation von Stationen

In dieser Konfiguration sind zwei dezentrale Stationen mithilfe von SCALANCE M-800 angeschlossen und können miteinander Daten austauschen. Die Geräte kommunizieren dabei direkt miteinander, z. B. ein Windpark mit einem Umspannwerk. Die Daten können entweder über ein öffentliches oder ein privates Netz ausgetauscht werden. Die Daten werden über gesicherte VPN-Tunnel übertragen. Für den Aufbau des VPN-Tunnels verfügt der Netzbetreiber über die notwendigen Dienste, z. B. eine feste IP-Adresse für die Mobilfunkrouter und/oder ein Zugang zum Internet über einen privaten APN.




Die SCALANCE M826 können entweder im 2-Draht-Betrieb oder im 4-Draht-Betrieb miteinander kommunizieren. Im 4-Draht-Betrieb werden die 2 x 2-Drahtleitungen zu einer virtuellen Verbindung mit Verdopplung der Datenrate aggregiert.




### Voraussetzungen

- Das M-800 ist über einen Admin-PC erreichbar.
- Für den Aufbau eines VPN-Tunnels:
  - M81x und M874
    Der Netzbetreiber verfügt über die notwendigen Dienste, z. B. eine feste IP-Adresse für die Mobilfunkrouter und/oder ein Zugang zum Internet über einen privaten APN.
  - M826
    Die Geräte haben eine feste IP-Adresse und sind im Routing-Modus.

### Vorgehensweise

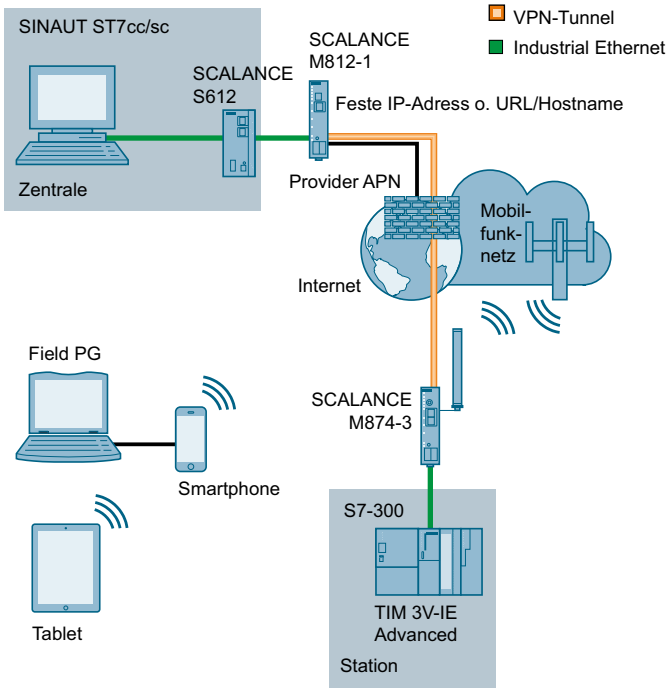
Um die Datenübertragung über einen VPN-Tunnel einzurichten, gehen Sie folgendermaßen vor:

1. Stellen Sie eine Verbindung zum öffentlichen oder privaten Netz her, siehe Kapitel Schnittstellen (Seite 312).
2. Schließen Sie je eine Steuerung z. B. über CP343-1 an eine Ethernet-Schnittstelle des M-800 an.
3. Stellen Sie eine VPN-Verbindung zwischen den beiden M-800-Geräten her, siehe Kapitel IPsec VPN (Seite 420).
4. Richten Sie die angeschlossenen Steuerungen für die Datenkommunikation ein.

## 3.2.4 TeleControl über das Mobilfunknetz

Das M874 können Sie dazu nutzen, Prozessdaten von entfernten Stationen über das Mobilfunknetz zur Zentrale zu übertragen, wenn z. B. kein Telefonnetz zur Verfügung steht.

Optional kann die Software der Zentrale um das Softwarepaket Alarm Control Center (ACC) ergänzt werden. Damit werden Störmeldungen aus der Anlage per SMS, Fax oder Email an das Servicepersonal weitergeleitet.




### Voraussetzungen

- Das M-800 ist über einen Admin-PC erreichbar.
- Für den Aufbau eines VPN-Tunnels:
  Feste IP-Adresse oder Hostname des DSL-Routers.

### Vorgehensweise

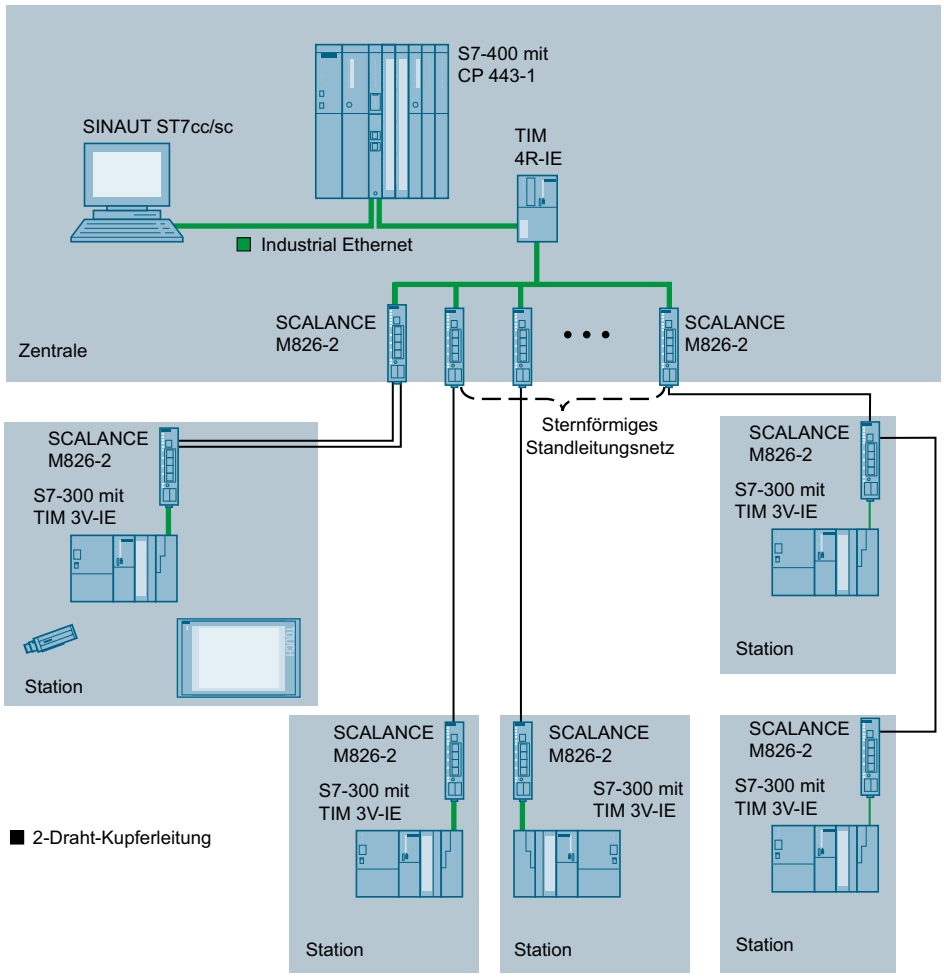
Um einen oder mehrere VPN-Tunnel zur Datenübertragung einzurichten, gehen Sie folgendermaßen vor:

1. Stellen Sie eine Verbindung zum WAN her, siehe Kapitel Schnittstellen (Seite 312).
2. Schließen Sie lokale SINAUT-Applikationen, z. B. TIM 4R-IE, an eine der Ethernet-Schnittstellen an.
3. Stellen Sie eine VPN-Verbindung her, siehe Kapitel IPsec VPN (Seite 420).
4. Richten Sie die angeschlossenen SINAUT-Applikationen für die Datenkommunikation ein.

## 3.2.5 TeleControl über Standleitung

In dieser Konfiguration werden die Außenstationen über betriebseigene Kupferleitungen mit der Zentrale verbunden.

Es lassen sich Punkt-zu-Punkt-, Linien- und Sternstrukturen und auch Mischkonfigurationen dieser Basisstrukturen aufbauen.

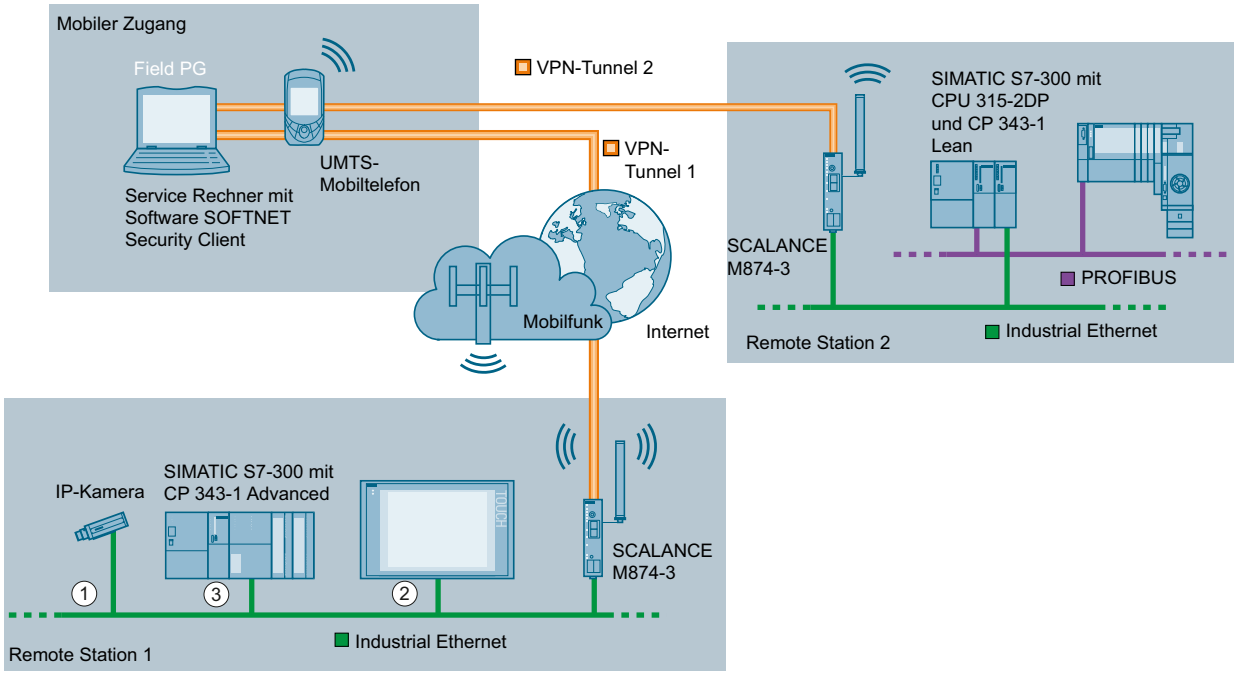



## 3.2.6 Mobiler Zugang zu Anlagen und Anlagenteilen

Der Servicetechniker kann von unterwegs für Fernwartungsarbeiten über das M874 auf die entfernte Anlage zugreifen.

Für den mobilen Zugang verwendet er einen mobilen Field-PG, der mit einem GPRS- oder UMTS-fähigen Mobiltelefon oder einer GPRS- oder UMTS-fähigen Netzwerkkarte ausgestattet ist.

Durch die VPN-Funktionalität ist die weltweit gesicherte Datenübertragung möglich. Die Zugriffsmöglichkeiten lassen sich mit der integrierten Firewall-Funktion einschränken.




① Bildübertragung
② WinCC flexible
③ Web-Zugriff auf CP 343-1

## Voraussetzungen

- Das M874 ist über einen Admin-PC erreichbar.

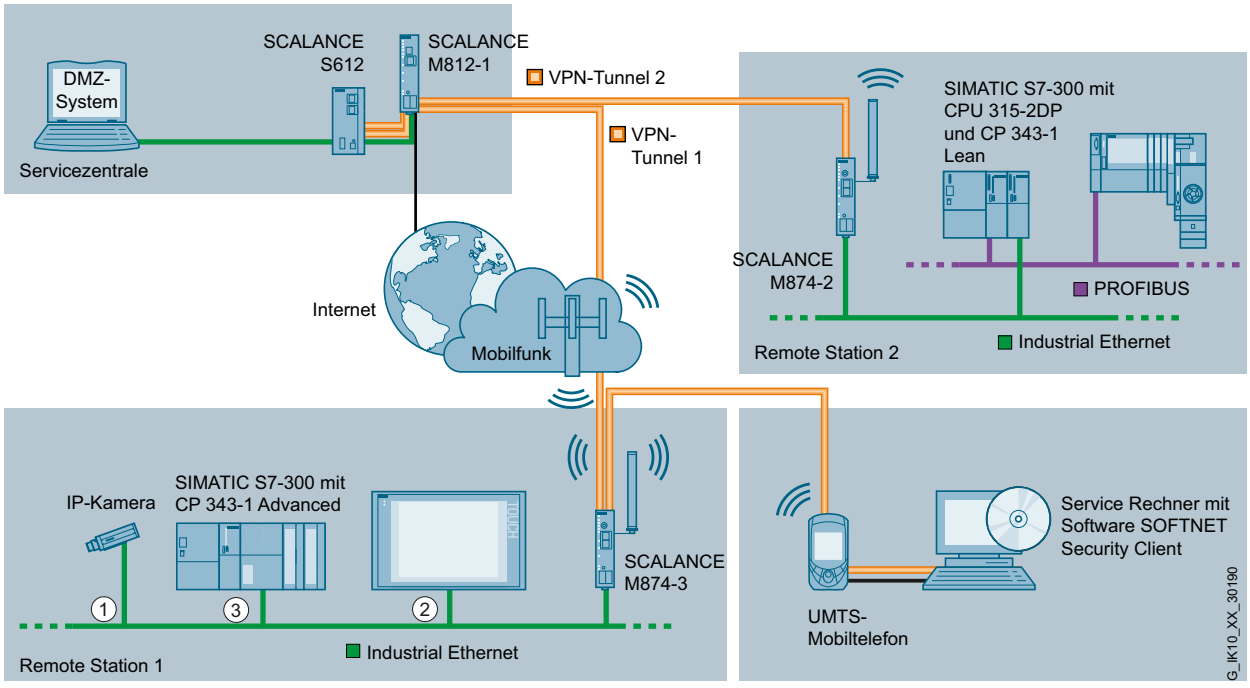
## Vorgehensweise

Um mobil über einen VPN-Tunnel auf eine Anlage zugreifen zu können, beachten Sie die nachfolgenden Punkte und die entsprechenden Kapitel in dieser Betriebsanleitung:

1. Stellen Sie eine Verbindung zum Mobilfunknetz her, siehe Kapitel Mobilfunk (Seite 315).
2. Richten Sie beim M874-x einen VPN-Tunnel im Roadwarrior-Modus ein, siehe Kapitel IPsec VPN (Seite 420).
3. Richten Sie auf der Seite des mobilen Zugangs im SOFTNET Security Client einen VPN-Tunnel ein.
   Hinweis: Die Punkte 3 und 4 können auch mit dem Security Configuration Tool durchgeführt werden.
4. Richten Sie die angeschlossenen Applikationen der Anlage für die Datenkommunikation ein.

## 3.2.7 Anlagenzugang über eine Fernwartungszentrale

Eine andere Variante ist der Anlagenzugang von einer Fernwartungszentrale aus. Die Fernwartungszentrale ist über den VPN-Server SCALANCE S612 mit dem Internet verbunden. Dadurch wird die Fernwartungszentrale vor unberechtigtem Zugriff geschützt. Die Anlage kommuniziert über das SCALANCE M874, das mit dem SCALANCE S612 einen VPN-Tunnel aufbaut. So kann z. B. ein Servicetechniker eine Anlage von einer Fernwartungszentrale aus steuern und überwachen.




① Web-Zugriff auf CP 343-1
② Bildübertragung
③ WinCC flexible

### Vorgehensweise

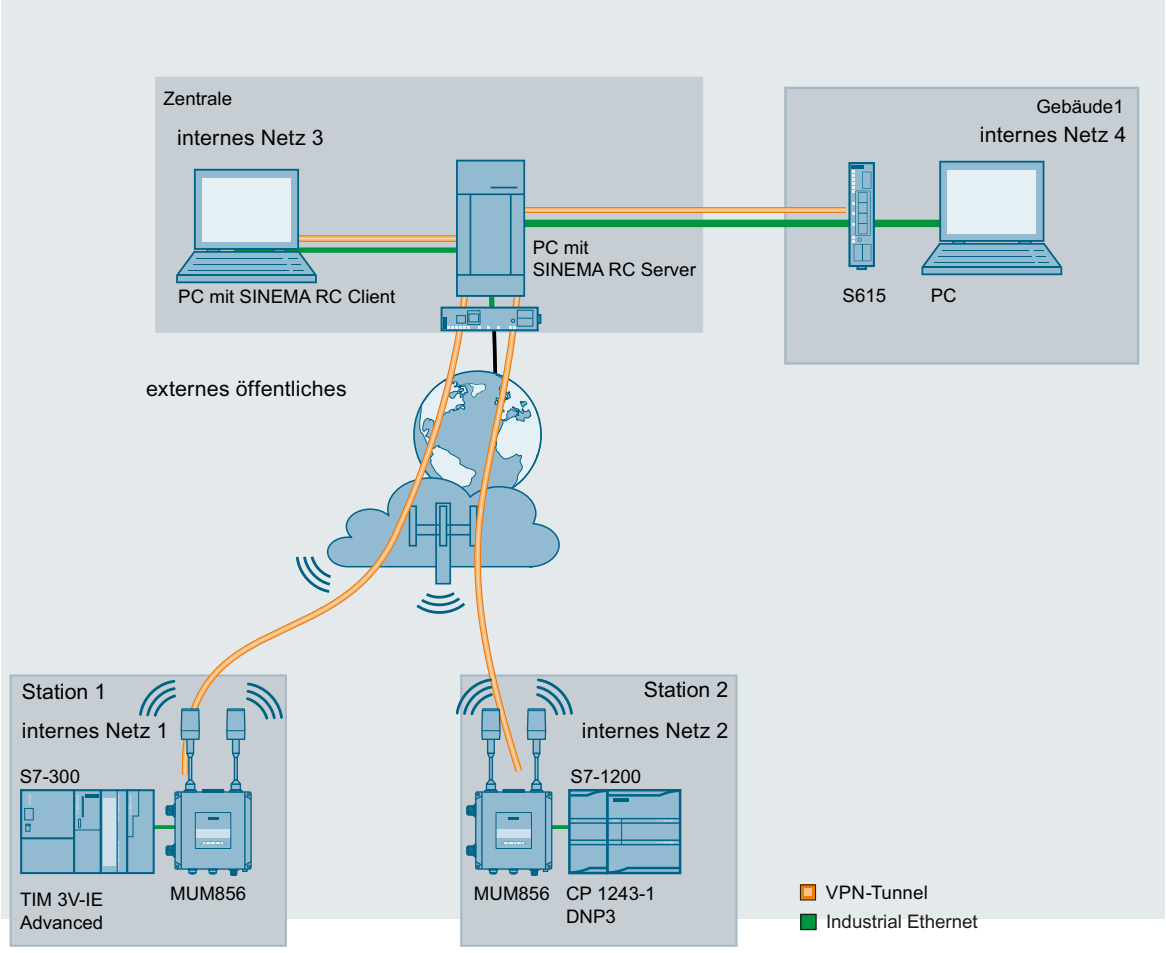
Um über eine Fernwartungszentrale auf eine Anlage zugreifen zu können, gehen Sie folgendermaßen vor:

1. Stellen Sie die Ethernet-Verbindung zwischen dem M874 und dem angeschlossenen Admin-PC her.
2. Stellen Sie eine Verbindung zum Mobilfunknetz her, siehe Kapitel Mobilfunk (Seite 315).
3. Projektieren Sie mit dem Security Configuration Tool im SCALANCE S612 die VPN-Verbindung für die Fernwartungszentrale.
4. Richten Sie einen VPN-Tunnel im Standard-Modus ein, siehe Kapitel IPsec VPN (Seite 420).
5. Richten Sie die angeschlossenen Applikationen der Anlage für die Datenkommunikation ein.

### 3.2.8 TeleControl mit SINEMA RC

In dieser Konfiguration ist die Fernwartungszentrale über den SINEMA Remote Connect Server mit dem Internet/Intranet verbunden. Die Stationen kommunizieren über SCALANCE MUM856 oder SCALANCE S615, die zu dem SINEMA RC Server einen VPN-Tunnel aufbauen. In der Zentrale baut der SINEMA RC-Client einen VPN-Tunnel zum SINEMA RC Server auf.

Die Geräte müssen sich am SINEMA RC Server anmelden. Erst nach erfolgreicher Authentifizierung wird der VPN-Tunnel zwischen dem Gerät und dem SINEMA RC Server aufgebaut. Abhängig von den projektierten Kommunikationsbeziehungen und den Sicherheitseinstellungen verschaltet der SINEMA RC-Server die einzelnen VPN-Tunnels.




#### Vorgehensweise

Um über eine Fernwartungszentrale auf eine Anlage zugreifen zu können, gehen Sie folgendermaßen vor:

1. Stellen Sie die Ethernet-Verbindung zwischen dem S615 und dem angeschlossenen Admin-PC her.
2. Legen Sie am SINEMA RC-Server die Geräte und die Teilnehmergruppen an.

3. Konfigurieren Sie am Gerät die Verbindung zum SINEMA RC-Server, siehe Kapitel SINEMA RC (Seite 295).
4. Richten Sie die angeschlossenen Applikationen der Anlage für die Datenkommunikation ein.

## 3.3 Voraussetzungen für den Betrieb

### 3.3.1 Für den Betrieb mit MUM853

#### Antenne

Das Gerät unterstützt die folgenden Frequenzbänder:

- 5G:
  - SA: n1, n2, n3, n5, n7, n8, n12, n20, n28, n38, n40, n41, n48, n66, n71, n77, n78, n79
  - 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/ B34/ B38/ B39/ B40/ B41/ B42/ B43/ B46/ B48/ B66/ B71
- UMTS:
  B1/ B2/ B3/ B4/ B5/ B8

Verwenden Sie Antennen aus dem Zubehörprogramm des SCALANCE M-800-Geräts. Weitere Informationen dazu finden Sie in der gerätespezifischen Betriebsanleitung.

Abhängig davon, welche Frequenzbänder Ihr Mobilfunkbetreiber verwendet, müssen Antennen auf die passenden Frequenzen abgestimmt sein. Erkundigen Sie sich bei Ihrem Mobilfunkbetreiber nach den Frequenzbändern.

**Hinweis**

Beachten Sie auch die Länderzulassungen für die SCALANCE M-800-Geräte.
Den aktuellen Stand der Länderzulassung finden Sie im Internet unter folgender Adresse:
(https://w3.siemens.com/mcms/industrial-communication/en/support/ik-info/Documents/Online_CountryApprovals_GSM_UMTS_products.pdf)

**Hinweis**

**Antennen**

- **A1+ A2**
  An den Antennen-Anschlüssen muss immer eine Antenne angeschlossen sein, um die 3/4/5G-Konnektivität zu nutzen.
- **A3 + A4**
  Optional. Die Antennen-Anschlüsse werden für zusätzliche MIMO Download Streams benötigt.

**Schutzkappen aufbewahren**

Bewahren Sie die entnommene Schutzkappe für eine spätere Verwendung auf.

## Spannungsversorgung

Weitere Informationen dazu finden Sie in der gerätespezifischen Betriebsanleitung.

## SIM-Karte

Eine Micro-SIM-Karte des ausgewählten Mobilfunkbetreibers.

**PIN**

Die PIN (= Personel Identification Number) der SIM-Karte

**5 G / LTE / UMTS-Freischaltung**

Die SIM-Karte muss von Ihrem Mobilfunkbetreiber für die Dienste im Mobilfunknetz freigeschaltet sein.

Die Zugangsdaten müssen bekannt sein:

- Access Point Name (APN)
- Benutzername
- Passwort

## Projektierung

Werkseitig ist das SCALANCE MUM853 für die erstmalige Konfiguration wie folgt erreichbar:

| | **Werkseitig voreingestellte Werte** |
|---|---|
| Ethernet-Schnittstelle für die Konfiguration | P1 ... P4 |
| IP-Adresse | 192.168.1.1 |
| Subnetzmaske | 255.255.255.0 |
| WBM | Zugriff über HTTPS, TCP-Port 443 |
| CLI | Zugriff über SSH, TCP-Port 22 |

| | **Werkseitig voreingestellte Werte** |
|---|---|
| Benutzername | admin<br>Der Benutzername ist nach der Erstanmeldung oder nach einem "Auf Werkseinstellungen zurücksetzen und Neustart" änderbar. Danach ist ein Umbenennen von "admin" nicht mehr möglich. |
| Passwort | admin<br>Das Passwort muss nach der Erstanmeldung oder nach einem "Auf Werkseinstellungen zurücksetzen und Neustart" geändert werden |

Weitere Informationen dazu finden Sie bei "Web Based Management (Seite 99)" und bei "Starten und anmelden (Seite 100)".

## 3.3.2 Für den Betrieb mit MUM856

### Antenne

Das Gerät unterstützt die folgenden Frequenzbänder:

- 5G:
  - SA: n1, n2, n3, n5, n7, n8, n12, n20, n28, n38, n40, n41, n48, n66, n71, n77, n78, n79
  - 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/ B34/ B38/ B39/ B40/ B41/ B42/ B43/ B46/ B48/ B66/ B71
- UMTS:
  B1/ B2/ B3/ B4/ B5/ B8

Verwenden Sie Antennen aus dem Zubehörprogramm des SCALANCE M-800-Geräts. Weitere Informationen dazu finden Sie in der gerätespezifischen Betriebsanleitung.

Abhängig davon, welche Frequenzbänder Ihr Mobilfunkbetreiber verwendet, müssen Antennen auf die passenden Frequenzen abgestimmt sein. Erkundigen Sie sich bei Ihrem Mobilfunkbetreiber nach den Frequenzbändern.

**Hinweis**

Beachten Sie auch die Länderzulassungen für die SCALANCE M-800-Geräte.
Den aktuellen Stand der Länderzulassung finden Sie im Internet unter folgender Adresse:
Online_CountryApprovals_GSM_UMTS_products.pdf
(https://w3.siemens.com/mcms/industrial-communication/en/support/ik-info/Documents/Online_CountryApprovals_GSM_UMTS_products.pdf)

**Hinweis**

**Antennen**

- **A1+ A2**
  An den Antennen-Anschlüssen muss immer eine Antenne angeschlossen sein, um die 3/4/5G-Konnektivität zu nutzen.
- **A3 + A4**
  Optional. Die Antennen-Anschlüsse werden für zusätzliche MIMO Download Streams benötigt.

**Schutzkappen aufbewahren**

Bewahren Sie die entnommene Schutzkappe für eine spätere Verwendung auf.

## Spannungsversorgung

Weitere Informationen dazu finden Sie in der gerätespezifischen Betriebsanleitung.

## SIM-Karte

Eine Micro-SIM-Karte des ausgewählten Mobilfunkbetreibers.

**PIN**

Die PIN (= Personel Identification Number) der SIM-Karte

**5 G / LTE / UMTS-Freischaltung**

Die SIM-Karte muss von Ihrem Mobilfunkbetreiber für die Dienste im Mobilfunknetz freigeschaltet sein.

Die Zugangsdaten müssen bekannt sein:

- Access Point Name (APN)
- Benutzername
- Passwort

## Projektierung

Werkseitig ist das SCALANCE MUM856 für die erstmalige Konfiguration wie folgt erreichbar:

| | **Werkseitig voreingestellte Werte** |
|---|---|
| Ethernet-Schnittstelle für die Konfiguration | P1 |
| IP-Adresse | 192.168.1.1 |
| Subnetzmaske | 255.255.255.0 |
| WBM | Zugriff über HTTPS, TCP-Port 443 |
| CLI | Zugriff über SSH, TCP-Port 22 |

| | **Werkseitig voreingestellte Werte** |
|---|---|
| Benutzername | admin<br>Der Benutzername ist nach der Erstanmeldung oder nach einem "Auf Werkseinstellungen zurücksetzen und Neustart" änderbar. Danach ist ein Umbenennen von "admin" nicht mehr möglich. |
| Passwort | admin<br>Das Passwort muss nach der Erstanmeldung oder nach einem "Auf Werkseinstellungen zurücksetzen und Neustart" geändert werden |

Weitere Informationen dazu finden Sie bei "Web Based Management" und bei "Starten und anmelden (Seite 100)".

### 3.3.3 Für den Betrieb mit M87x

#### Antenne

Der Frequenzbereich der Antenne ist abhängig vom verwendeten Gerät:

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

Verwenden Sie Antennen aus dem Zubehörprogramm des SCALANCE M-800-Geräts. Weitere Informationen dazu finden Sie in der gerätespezifischen Betriebsanleitung.

**Hinweis**

Beachten Sie auch die Länderzulassungen für die SCALANCE M-800-Geräte.
Den aktuellen Stand der Länderzulassung finden Sie im Internet unter folgender Adresse:
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)

#### Spannungsversorgung

Eine Spannungsversorgung mit einer Spannung zwischen 12 V DC und 24 V DC, die einen ausreichenden Strom liefern kann.

Weitere Informationen dazu finden Sie in der gerätespezifischen Betriebsanleitung.

#### SIM-Karte

Eine Mini-SIM-Karte des ausgewählten Mobilfunkbetreibers.

**PIN**

Die PIN (= Personel Identification Number) der SIM-Karte

**LTE / UMTS / EGPRS / GPRS Freischaltung**

Die SIM-Karte muss von Ihrem Mobilfunkbetreiber für die Dienste im Mobilfunknetz freigeschaltet sein.

Die Zugangsdaten müssen bekannt sein:

- Access Point Name (APN)
- Benutzername
- Passwort

### Projektierung

Werkseitig ist das SCALANCE M87x für die erstmalige Konfiguration wie folgt erreichbar:

| | **Werkseitig voreingestellte Werte** |
|---|---|
| Ethernet-Schnittstelle für die Konfiguration | M874: P1 ... P2<br>M876: P1 ... P4 |
| IP-Adresse | 192.168.1.1 |
| Subnetzmaske | 255.255.255.0 |
| WBM | Zugriff über HTTPS, TCP-Port 443 |
| CLI | Zugriff über SSH, TCP-Port 22 |
| Benutzername | admin<br>Der Benutzername ist nach der Erstanmeldung oder nach einem "Auf Werkseinstellungen zurücksetzen und Neustart" änderbar. Danach ist ein Umbenennen von "admin" nicht mehr möglich. |
| Passwort | admin<br>Das Passwort muss nach der Erstanmeldung oder nach einem "Auf Werkseinstellungen zurücksetzen und Neustart" geändert werden |

Weitere Informationen dazu finden Sie bei "Web Based Management" und bei "Starten und anmelden (Seite 100)".

## 3.3.4 Für den Betrieb mit M81x

### Spannungsversorgung

Eine Spannungsversorgung mit einer Spannung zwischen 12 V DC und 24 V DC, die einen ausreichenden Strom liefern kann.

Weitere Informationen dazu finden Sie in der gerätespezifischen Betriebsanleitung.

### ADSL-Anschluss

Ein ADSL-Anschluss des ausgewählten DSL-Anbieters.

**ADSL-Freischaltung**

Der DSL-Anschluss muss von ihrem DSL-Anbieter freigeschaltet sein.

Die Zugangsdaten müssen bekannt sein:

- Benutzername
- Passwort
- VCI / VPI
- Kapselung

### Projektierung

Werkseitig ist das SCALANCE M81x für die erstmalige Konfiguration wie folgt erreichbar:

| | **Werkseitig voreingestellte Werte** |
|---|---|
| Ethernet-Schnittstelle für die Konfiguration | M812: P1<br>M816: P1 ... P4 |
| IP-Adresse | 192.168.1.1 |
| WBM | Zugriff über HTTPS, TCP-Port 443 |
| CLI | Zugriff über SSH, TCP-Port 22 |
| Subnetzmaske | 255.255.255.0 |
| Benutzername | admin<br>Der Benutzername ist nach der Erstanmeldung oder nach einem "Auf Werkseinstellungen zurücksetzen und Neustart" änderbar. Danach ist ein Umbenennen von "admin" nicht mehr möglich. |
| Passwort | admin<br>Das Passwort muss nach der Erstanmeldung oder nach einem "Auf Werkseinstellungen zurücksetzen und Neustart" geändert werden |

Weitere Informationen dazu finden Sie bei "Web Based Management" und bei "Starten und anmelden (Seite 100)".

## 3.3.5 Für den Betrieb mit M826

### Spannungsversorgung

Eine Spannungsversorgung mit einer Spannung zwischen 12 V DC und 24 V DC, die einen ausreichenden Strom liefern kann.

Weitere Informationen dazu finden Sie in der gerätespezifischen Betriebsanleitung.

### SHDSL-Anschluss

Betriebseigene Kupferleitungen

## Projektierung

Werkseitig ist das SCALANCE M826 für die erstmalige Konfiguration wie folgt erreichbar:

| | **Werkseitig voreingestellte Werte** |
|---|---|
| Ethernet-Schnittstelle für die Konfiguration | P1 ... P4 |
| IP-Adresse | 0.0.0.0<br>Die erstmalige Vergabe einer IP-Adresse für einen SCALANCE M826 kann nicht mit dem Web Based Management (WBM) erfolgen, weil dieses Konfigurations-Werkzeug bereits eine IP-Adresse voraussetzt.<br>Es gibt folgende Möglichkeiten, einem unkonfigurierten Gerät eine IP-Adresse zuzuweisen:<br>• DHCP (Default)<br>• SINEC PNI<br>• STEP 7 |
| Subnetzmaske | 255.255.255.0 |
| WBM | Zugriff über HTTPS, TCP-Port 443 |
| CLI | Zugriff über SSH, TCP-Port 22 |
| Benutzername | admin<br>Der Benutzername ist nach der Erstanmeldung oder nach einem "Auf Werkseinstellungen zurücksetzen und Neustart" änderbar. Danach ist ein Umbenennen von "admin" nicht mehr möglich. |
| Passwort | admin<br>Das Passwort muss nach der Erstanmeldung oder nach einem "Auf Werkseinstellungen zurücksetzen und Neustart" geändert werden |

**Hinweis**

DHCP ist im Auslieferungszustand und nach "Auf Werkseinstellungen zurücksetzen und Neustart" eingeschaltet.

Wenn ein DHCP-Server im lokalen Netz verfügbar ist und dieser auf die DHCP-Anfrage eines SCALANCE M826 antwortet, so werden schon beim ersten Hochlauf automatisch IP-Adresse, Subnetzmaske und Gateway zugeteilt. Durch "Auf gespeicherte Einstellungen zurücksetzen und Neustart " wird weder eine durch DHCP noch eine vom Benutzer vergebene IP-Adresse gelöscht.

Weitere Informationen dazu finden Sie bei "Web Based Management" und bei "Starten und anmelden (Seite 100)".

**Hinweis**

**Betrieb M826**

Der volle Funktionsumfang wird nur unterstützt, wenn ausschließlich SCALANCE M826 eingesetzt werden. Wenn Sie als Endteilnehmer ein SHDSL-Modem eines Fremdherstellers einsetzen, kann ein einwandfreier Betrieb nicht garantiert werden.

## 3.3.6 Für den Betrieb mit M804PB

### Spannungsversorgung

Eine Spannungsversorgung mit einer Spannung zwischen 12 V DC und 24 V DC, die einen ausreichenden Strom liefern kann.

Weitere Informationen dazu finden Sie in der gerätespezifischen Betriebsanleitung.

### Projektierung

Werkseitig ist das SCALANCE M804PB für die erstmalige Konfiguration wie folgt erreichbar:

| | **Werkseitig voreingestellte Werte** |
|---|---|
| Ethernet-Schnittstelle für die Konfiguration<br>(Intern) | P1 ... P2 (vlan 1) |
| Anbindung an Automatisierungssystem | MPI/DP |
| IP-Adresse | 192.168.1.1 |
| Subnetzmaske | 255.255.255.0 |
| WBM | Zugriff über HTTPS, TCP-Port 443 |
| CLI | Zugriff über SSH, TCP-Port 22 |
| Benutzername | admin<br>Der Benutzername ist nach der Erstanmeldung oder nach einem "Auf Werkseinstellungen zurücksetzen und Neustart" änderbar. Danach ist ein Umbenennen von "admin" nicht mehr möglich. |
| Passwort | admin<br>Das Passwort muss nach der Erstanmeldung oder nach einem "Auf Werkseinstellungen zurücksetzen und Neustart" geändert werden |

Weitere Informationen dazu finden Sie bei "Web Based Management (Seite 99)" und bei "Starten und anmelden (Seite 100)".

## 3.3.7 Einsatz in einer PROFINET-Umgebung

**Hinweis**

**Gültigkeit CCA-Erklärung**

Die CCA Erklärung gilt für PROFINET RT ohne den Einsatz in Medienredundanz Strukturen.

### Konfigurationshinweise

Beachten Sie beim Einsatz des Geräts in einer PROFINET-Umgebung folgende Konfigurationshinweise:

- Stellen Sie die "Aging Time" auf 45 Sekunden.
- Deaktivieren Sie Spanning Tree und aktivieren Sie Passive Listening.
- Stellen Sie den Base Bridge-Modus (Layer 2 > VLAN > Allgemein) auf "802.1Q VLAN Bridge". Eine Ausnahme bildet der M826. Wenn bei SHDSL das gleiche Subnetz übertragen wird, verwenden Sie bei "Base-Bridge-Modus" "802.1D Transparent Bridge".

## 3.3.8 TIA Portal Cloud Connector

Eine Kommunikationsverbindung über den TIA Portal Cloud Connector ist mit folgenden Komponenten möglich:

- TIA Portal Cloud Connector V1.1 SP3
  Den TIA Portal Cloud Connector finden Sie auf den Internet-Seiten des Siemens Industry Online Support unter folgender Beitrags-ID: 109764115 (https://support.industry.siemens.com/cs/ww/de/view/109764115)
  Installieren Sie die Version, auch wenn bereits ein TIA Portal Cloud Connector installiert ist. Weiterführende Informationen zum TIA Portal Cloud Connector finden Sie in den Dokumentationen "Arbeiten mit dem TIA Portal Cloud Connector (https://support.industry.siemens.com/cs/ww/de/view/109747305)" und "SIMATIC Anleitung zum TIA Portal Cloud Connector (https://support.industry.siemens.com/cs/ww/de/view/109742490)".
- TIA-Portal V15 Update 2 oder STEP 7 V5.6

**Hinweis**

- Verwenden Sie den im Produkt integrierten "TIA Portal Cloud Connector" über eine VPN-Lösung (z.B. SINEMA RC).
- Konfigurieren Sie die Firewall Einstellungen des SCALANCE M800/S615 (z.B. Vordefinierte IPv4 Regeln "Cloud Connector", um den unbefugten Zugriff von Netzteilnehmer auf den "TIA Portal Cloud Connector Server" zu verhindern.

# 3.4 Mengengerüste für WBM und CLI

### Mengengerüst des Geräts

In der folgenden Tabelle ist das Mengengerüst für das Web Based Management und das Command Line Interface des Geräts aufgeführt.

Abhängig von Ihrem Gerät stehen Ihnen manche Funktionen nicht zur Verfügung.

| | **konfigurierbare Funktion** | | **maximale Anzahl** |
|---|---|---|---|
| **System** | DNS-Server | | 2 |
| | DNS Records | | 128 Einträge<br>FQDN: Maximal 256 Zeichen |
| | Syslog-Server | | 3 |
| | SMTP-Server | | 3 |
| | E-Mail-Empfänger | | 60<br>20 pro SMTP-Server |
| | SNMPv1-Trap-Empfänger | | 10 |
| | SMS-Empfänger | | 20 |
| | SNTP-Server | | 2 |
| | NTP / NTP (secure) Server | | 3<br>pro Layer 3-Schnittstelle 1 |
| | NTP / NTP (secure) Client | | 1 |
| | DHCP-Pools | | 8 |
| | Statische Zuordnungen pro DHCP-Pool | | 128 |
| | DHCP-Optionen<br>(1, 2, 3, 4, 5, 6, 42, 66, 67) | | 9 |
| | SINEMA RC | | 1 |
| | Proxy Server | | 5 |
| | Backup der Konfiguration | | Ohne PLUG:<br>• 2 ohne Firmware<br>• 0 mit Firmware |
| | | | Mit PLUG:<br>• 5 ohne Firmware<br>• 2 mit Firmware (Firmware on PLUG) |
| | Cloud Connector | | 1 Schnittstelle |
| **Layer 2** | VLAN | Virtuelle LANs (portbased; inklusive VLAN 1) | 16 |
| | | Maximale Framegröße | • M87x, MUM856x M81x, M804PB: 2048 Bytes<br>• M826: 2018 Bytes |
| | VXLAN | NVE-Schnittstelle / VNI | • MUM85x: 1 NVE/ 1 VNI |
| **Layer 3** | IP-Schnittstellen | | 12 |
| | Statische Routen | | 100 |
| | NETMAP | | 256 |
| | SourceNAT | | 32 |
| | NAPT | | 32 |
| | VRRPv3 | | VRRPv3-Instanzen (VRID): 2<br>Zugeordnete IP-Adressen: 1 pro VRID |

| | konfigurierbare Funktion | maximale Anzahl |
|---|---|---|
| **Security** | Benutzer | 30<br>(inkl. werkseitig voreingestelltem Benutzer "admin") |
| | Gruppen | 32 |
| | Rollen | 32<br>(inkl. der vordefinierten Rollen) |
| | RADIUS-Server | 4 |
| | Firewall | IP-Protokolle:16<br>IP-Dienste: 32<br>ICMP-Dienste:16<br>IP-Regeln: 128<br>Dynamische Firewall:<br>• Maximale Anzahl: 8 Regelsätze<br>• Parallele Benutzerzugriffe: 4<br>• Maximal 128 IP-Regeln pro Firewall-Regelsatz |
| | IPsec VPN | 20<br>Maximal 20 Phase 2-Verbindungen können pro Phase 1 (Remote-Endpunkt) angelegt werden.<br>Nur mit IKEv2:<br>• Mehrere Subnetze pro Phase 2-Verbindung; Maximal 5 |
| | OpenVPN | Verbindungen: 5<br>Remote-Endpunkte: 25 |

## 3.5 Mengengerüst für SINEMA RC

Maximaler, gesamter Datentransfer für alle Geräte: 800Mbit/s

Maximale Anzahl an gleichzeitig verbundenen Geräten und Benutzer: **1024** Geräte mit jeweils 1 Subnetz

Kombinationen Benutzer / Geräte sind bis zum maximalen Gesamt-Mengengerüst frei wählbar.

Da die Anzahl der Subnetze z.B. auch von der erlaubten Kommunikationsbeziehungen untereinander abhängt, sind diese genau zu prüfen/hinterfragen und ggf. entsprechend einzuschränken. Falls Geräte untereinander nicht kommunizieren müssen, sollte man dies unterbinden, um optimales Verhalten der Geräte sicherzustellen.

Wenn die Geräte miteinander kommunizieren sollen, dann ist die maximale Anzahl an gleichzeitig verbundenen Geräten und Benutzer: **200** miteinander kommunizierende Geräte mit je 8 Subnetzen

# 3.6 Hardware-Ausstattung und Systemfunktionen

## Verfügbarkeit der Hardware-Ausstattung

Die nachfolgende Tabelle zeigt die Hardware-Ausstattung der Geräte

Technische Änderungen sind vorbehalten.

| | SCALANCE | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **M874-2<br>M874-3** | **M876-3<br>M876-4** | **M812** | **M816** | **M826** | **M804PB** | **MUM856-1** | **MUM853-1** |
| Schnitt-stellen | 1 x SMA-An-tennenan-schluss | 2 x SMA-An-tennenan-schluss | 1 x DSL | 1 x DSL | 2 x SHDSL | 1 x RS 485 (MPI/DP) | 4 x N-connect | 4 x SMA-An-tennenan-schluss |
| | 2 x RJ45 | 4x RJ45 | 1x RJ45 (LAN) | 4 x RJ45 (LAN) | 4 x RJ45 | 2 x RJ45 | 1 x M12-Buch-se , X-kodiert | 4 x RJ45 |
| Digitaler Ein-/ Ausgang | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| PLUG-Steckplatz | ✓ | ✓ | - | ✓ | ✓ | ✓ | ✓ (CLP) | ✓ (CLP) |
| SET-Taster | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

## Verfügbarkeit der Systemfunktionen

Die nachfolgende Tabelle zeigt die Verfügbarkeit der Systemfunktionen auf den Geräten. Beachten Sie, dass in diesem Projektierungshandbuch und der Online-Hilfe alle Funktionen beschrieben sind. Abhängig dem KEY PLUG stehen Ihnen manche Funktionen nicht zur Verfügung.

Technische Änderungen sind vorbehalten.

| | | SCALANCE | | | | | |
|---|---|---|---|---|---|---|---|
| | | **M87x** | **MUM85x** | **M812** | **M816** | **M826** | **M804PB** |
| **Basic Wi-zard** | IP-Einstellungen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Geräteeinstellungen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | SIM | ✓ | ✓ | - | - | - | - |
| | Mobilfunkanbieter | ✓ | ✓ | - | - | - | - |
| | DSL | - | - | ✓ | ✓ | - | - |
| | SHDSL | - | - | - | - | ✓ | - |
| | TIA Portal Cloud Con-nector | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Zeiteinstellungen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | SINEMA RC [1)] | ✓ | ✓ | - | ✓ | ✓ | ✓ |
| | DDNS | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| | | SCALANCE | | | | | |
|---|---|---|---|---|---|---|---|
| | | **M87x** | **MUM85x** | **M812** | **M816** | **M826** | **M804PB** |
| **Informationen** | ARP-Tabelle | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | IPv6-Nachbarschaftstabelle | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Log-Tabellen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | IPv4-Routing | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | IPv6-Routing | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Mobilfunk | ✓ | ✓ | - | - | - | - |
| | DSL | - | - | ✓ | ✓ | - | - |
| | SHDSL | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| | Redundanz | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | VRRPv3 | ✓ | ✓ | ✓ | ✓ | - | - |
| | SINEMA RC [1)] | ✓ | ✓ | - | ✓ | ✓ | ✓ |
| **System** | SMTP-Client | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | SNMP | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Zeiteinstellung | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Automatisches Abmelden | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Syslog-Client | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Fehlerkontrolle | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | PLUG | ✓ | ✓ | - | ✓ | ✓ | ✓ |
| | SMS | ✓ | ✓ | - | - | - | - |
| | DNS | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | DHCPv4 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | cRSP/SRS | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Proxy-Server | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | TIA Portal Cloud Connector | ✓ | - | ✓ | ✓ | ✓ | ✓ |
| | SINEMA RC[1)] | ✓ | ✓ | - | ✓ | ✓ | ✓ |
| | Connection Check | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Schnittstellen** | Ethernet | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Mobilfunk | ✓ | ✓ | - | - | - | - |
| | DSL | - | - | ✓ | ✓ | - | - |
| | SHDSL | - | - | - | - | ✓ | - |
| **Layer 2** | Konfiguration | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | VLAN | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | VXLAN | - | ✓ | - | - | - | - |
| | Dynamic MAC Aging | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | LLDP | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Spanning Tree | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| | | SCALANCE | | | | | |
|---|---|---|---|---|---|---|---|
| | | **M87x** | **MUM85x** | **M812** | **M816** | **M826** | **M804PB** |
| **Layer 3 (IPv4)** | Statische Routen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Subnetze | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Spanning Tree | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | NAT | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | VRRPv3 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Layer 3 (IPv6)** | Subnetze | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | NAT | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Security** | Passwörter | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Benutzer | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | AAA (Authentication, Authorization, Accounting) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Zertifikate | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Firewall | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | IPsec VPN | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | OpenVPN | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

[1] KEY-PLUG SINEMA Remote Connect 6GK5908-0PB00 / SCALANCE CLP 2GB SINEMA RC 6GK5908-0UA00-0AA0

# 3.7 PLUG

## 3.7.1 PLUG

~~M812~~

| Typ | Eigenschaften | Artikelnummer |
|---|---|---|
| C-PLUG | Wechselmedium (32 MByte) zur Aufnahme von Konfigurationsdaten | 6GK1900-0AB00 |
| | Wechselmedium (256 MByte) zur Aufnahme von Konfigurationsdaten | 6GK1900-0AB10 |
| KEY-PLUG SINEMA RC | Wechselmedium (256 MByte) zum Freischalten der Anbindung an den SINEMA Remote Connect und zur Aufnahme von Konfigurationsdaten | 6GK5908-0PB00 |
| SCALANCE CLP 2GB | Wechselmedium zum einfachen Geräte-Tausch im Fehlerfall, zur Aufnahme von Projektierungsdaten, einsetzbar in folgenden SCALANCE-Produkten mit CLP-Steckplatz: SCALANCE MUM85x | 6GK1900-0UB00-0AA0 |

| Typ | Eigenschaften | Artikelnummer |
|---|---|---|
| SCALANCE CLP EEC 2GB | Wechselmedium mit lackierten Leiterplatten zum einfachen Tausch der Geräte im Fehlerfall zur Aufnahme von Projektierungsdaten; einsetzbar in SCALANCE-Produkten mit CLP-Steckplatz: SCALANCE MUM85x | 6GK1 900-0UQ00-0AA0 |
| SCALANCE CLP 2GB SINEMA RC | Wechselmedium (2 GB) zum Freischalten der Anbindung an den SINEMA Remote Connect und zur Aufnahme von Konfigurationsdaten; einsetzbar in SCALANCE-Produkten mit CLP-Steckplatz: SCALANCE MUM85x. | 6GK5908-0UA00-0AA0 |

Der PLUG ist ein Wechselmedium und dient dazu, im Fall eines Geräteaustausches die Konfiguration des alten Geräts auf das Neugerät zu übertragen.

Folgende PLUG-Typen gibt es:

- C-PLUG: Das Wechselmedium speichert ausschließlich die Konfigurationsdaten des Geräts.
- KEY-PLUG: Das Wechselmedium enthält zusätzlich zu den Konfigurationsdaten eine Lizenz, mit der speziellen Funktionen freigeschaltet werden, z B. SINEMA RC.
- CLP (Configuration License PLUG)
  Der SCALANCE CLP ist ein Wechselmedium zur Speicherung und Sicherung von Projektierungsdaten, das in allen SCALANCE-Geräten mit CLP-Steckplatz einsetzbar ist, z. B. SCALANCE MUM85x. Mit dem SCALANCE CLP wird im Fall eines Gerätetauschs die Konfiguration des alten Geräts auf das Neugerät übertragen. Der CLP dient als Nachfolger der zuvor beschriebenen PLUGs. Der CLP wird in der Beschreibung auch als PLUG bezeichnet. Den PLUG gibt es in folgenden Varianten:
  - PLUG-Konfiguration
  - PLUG-Lizenz

## Position

Der Steckplatz des PLUG befindet sich an der Rückseite des Geräts, siehe Kapitel Geräteansichten in der Betriebsanleitung des Geräts.

## Funktion

Geräte mit einem PLUG-Steckplatz unterstützen die folgenden Betriebsarten:

- **Ohne PLUG**
  Das Gerät speichert die Konfigurationsdaten auf dem internen Speicher. Dieser Modus ist aktiv, wenn kein PLUG gesteckt ist.
- **Mit PLUG**
  In der Anlaufphase:
  - Wenn ein **unbeschriebener** PLUG (Auslieferungszustand) in das Gerät gesteckt wird, sichert das Gerät beim Anlauf automatisch die Konfigurationsdaten auf dem PLUG. Danach verhält er sich wie ein beschriebener PLUG.
  - Wenn ein **beschriebener** PLUG in ein Gerät gesteckt wird, übernimmt das Gerät in der Anlaufphase automatisch die Konfiguration des PLUG. Voraussetzung ist, dass die Konfigurationsdaten von einem kompatiblen Gerätetyp beschrieben wurden.
    Einen Ausnahmefall kann die IP-Konfiguration darstellen, wenn sie per DHCP eingestellt wird und der DHCP-Server nicht entsprechend umkonfiguriert wurde. Eine Nachkonfiguration ist erforderlich, wenn Sie Funktionen verwenden, die auf MAC-Adressen basieren.
  - Enthält der PLUG eine Lizenz, werden außerdem zusätzliche Funktionen freigeschaltet.

    **Hinweis**

    Wenn das Gerät einmal mit einem KEY-PLUG oder einer PLUG-Lizenz konfiguriert wurde, kann das Gerät ohne diesen PLUG nicht mehr genutzt werden. Um das Gerät wieder nutzen zu können, setzen Sie das Gerät auf Werkseinstellungen zurück.

  Im Betrieb:
  - Im laufenden Betrieb werden Änderungen der Konfiguration auf dem PLUG und auf dem internen Speicher gesichert.
  - Die Projektierungsdaten des Geräts werden auf einem gesicherten Speicherbereich des PLUG abgelegt. Dieser gesicherte Speicherbereich kann nur über die Authentifizierung des Siemens-Geräts erreicht werden.
  - Das Gerät überprüft im Sekundenabstand, ob ein PLUG gesteckt ist. Wenn das Gerät feststellt, dass der PLUG entfernt wurde, startet es automatisch neu.

    | **ACHTUNG** |
    | --- |
    | **Bedienungsrisiko - Gefahr von Datenverlust**<br>Ziehen und stecken Sie den PLUG nur, wenn das Gerät spannungslos ist. |

  - Das Gerät signalisiert Abweichungen vom Normalbetrieb des PLUG (z. B. inkompatible Daten, fehlerhafte Bedienung oder Fehlfunktionen) über die vorhandenen Diagnose-Mechanismen (z. B. LEDs oder Benutzerschnittstellen). er Anwender hat dann die Möglichkeit, den PLUG wieder zu entfernen oder durch die Anwahl einer entsprechenden Option den PLUG neu zu formatieren.

Die Vorgehensweise zum Einsetzen und Entnehmen des PLUG finden Sie im Kapitel "PLUG tauschen" in der Betriebsanleitung des Geräts.

## 3.7.2 PRESET-PLUG




### PLUG mit Preset-Funktion (PRESET-PLUG)

Mittels PRESET-PLUG ist es möglich, dieselbe Gerätekonfiguration und die dazugehörige Firmware auf mehreren Geräten zu installieren.

**Hinweis**

**Konfigurationen mit DHCP verwenden**

Erstellen Sie einen PRESET-PLUG nur aus Gerätekonfigurationen, die DHCP verwenden. Es treten sonst Störungen im Netzwerkbetrieb durch mehrfache gleiche IP-Adressen auf.

Feste IP-Adressen weisen Sie nach der Grundinstallation gesondert zu.

In einem PLUG, der als PRESET-PLUG konfiguriert wurde, werden die Gerätekonfiguration, Benutzeraccounts, Zertifikate und die Firmware gespeichert.

**Hinweis**

**Auf Werkseinstellungen zurücksetzen und Neustart mit gestecktem PRESET-PLUG**

Wenn Sie das Gerät auf Werkseinstellungen zurücksetzen wird beim Neustart des Geräts ein gesteckter PRESET-PLUG formatiert und die Funktionalität PRESET-PLUG geht verloren. Sie müssen dann einen neuen PRESET-PLUG erstellen.

Wir empfehlen, den PRESET-PLUG zu entnehmen, bevor Sie das Gerät auf Werkseinstellungen zurücksetzen.

Nähere Informationen zur Erstellung und Benutzung eine PRESET-PLUG finden Sie in Kapitel Gerätekonfiguration mit PRESET-PLUG (Seite 443).

# Technische Grundlagen

# 4

## 4.1 IP-Adressen

### 4.1.1 IPv4 / IPv6

**Was sind die wesentlichen Unterschiede?**

| | IPv4 | IPv6 |
|---|---|---|
| IP-Konfiguration | • DHCP-Server<br>• Manuell | • Stateless Address Autoconfiguration (SLAAC): zustandslose Autokonfiguration über NDP (Neighbor Discovery Protocol)<br>– Erstellt eine Link-lokale Adresse für jede Schnittstelle, die keinen Router auf dem Link benötigt.<br>– Prüft die Einmaligkeit der Adresse auf dem Link, die keinen Router auf dem Link benötigt.<br>– Legt fest, ob die globalen Adressen über einen zustandslosen Mechanismus, einen zustandbehafteten Mechanismus oder über beide Mechanismen bezogen werden. (Erfordert einen Router auf dem Link.)<br>• Manuell<br>• DHCPv6 (Zustandbehaftet) |
| Verfügbare IP-Adressen | 32-Bit: 4, 29 * $10^9$ Adressen | 128-Bit: 3,4 * $10^{38}$ Adressen |
| Adressformat | Dezimal: 192.168.1.1<br>mit Port: 192.168.1.1:20 | Hexadezimal: 2a00:ad80::0123<br>mit Port: [2a00:ad80::0123]:20 |
| Loopback | 127.0.0.1 | ::1 |
| IP-Adressen pro Schnittstelle | 4 IP-Adressen | Mehrere IP-Adressen<br>• LLA: Eine link lokale-Adresse (automatisch gebildet) fe80::/128 pro Schnittstelle<br>• ULA: Mehrere Unique lokal Unicast-Adressen pro Schnittstelle<br>• GUA: Mehrere Globale Unicast-Adressen pro Schnittstelle |
| Header | • Checksumme<br>• variable Länge<br>• Fragmentierung im Header<br>• keine Sicherheit | • Überprüfung auf höherer Schicht<br>• fest vorgeschriebene Größe<br>• Fragmentierung im Extension Header |
| Fragmentierung | Host und Router | nur Endpunkt der Kommunikation |
| Quality of Service | Type of Service zur Priorisierung (ToS) | Die Priorisierung wird im Header-Feld "Traffic Class" angegeben. |

| | IPv4 | IPv6 |
|---|---|---|
| Telegrammarten | Broadcast, Multicast, Unicast | Multicast, Unicast, Anycast |
| Identifizierung von DHCP-Clients/-Server | Client-ID:<br>• MAC-Adresse<br>• DHCP Client ID<br>• System Name<br>• PROFINET-Stationsname<br>• IAID und DUID | DUID + IAID(s) = genau eine Schnittstelle des Hosts<br>DUID = DHCP Unique Identifier<br>Identifiziert Server und Clients eindeutig.<br>IAID = Identity Association Identifier<br>Mindestens eine pro Schnittstelle wird vom Client generiert und bleibt bei Neustart des DHCP-Clients unverändert<br>Drei Verfahren zum Ermitteln der DUID<br>• DUID-LLT<br>• DUID-EN<br>• DUID-LL |
| Auflösung von IP-Adressen in Hardware-Adressen | ARP (Address Resolution Protocol) | NDP (Neighbor Discovery Protocol) |

## 4.1.2 IPv4-Adresse

### 4.1.2.1 Aufbau einer IPv4-Adresse

Die IPv4-Adresse besteht aus 4 Dezimalzahlen, die durch einen Punkt voneinander getrennt sind. Jede Dezimalzahl kann einen Wert von 0 bis 255 annehmen.

Beispiel: 192.168.16.2

Die IPv4-Adresse setzt sich zusammen aus:

- Adresse des (Sub)-Netzes
- Der Adresse des Teilnehmers (im allgemeinen auch Endteilnehmer, Host oder Netzknoten genannt)

**Subnetzmaske**

Die Subnetzmaske besteht aus 4 Dezimalzahlen aus dem Wertebereich 0 bis 255, die durch einen Punkt voneinander getrennt sind; z. B. 255.255.0.0

Die 4 Dezimalzahlen der Subnetzmaske müssen in ihrer binären Darstellung von links eine Folge von lückenlosen Werten "1" und von rechts eine Folge von lückenlosen Werten "0" enthalten.

Die Werte "1" bestimmen die Netzadresse innerhalb der IPv4-Adresse. Die Werte "0" die Teilnehmer-Adresse innerhalb der IPv4-Adresse.

Beispiel:

richtige Werte

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

falscher Wert:

255.255.1.0 D = 1111 1111.1111 1111.0000 0001.0000 0000 B

Im Beispiel für die oben genannte IP-Adresse hat die hier gezeigte Subnetzmaske folgende Bedeutung:

Die ersten 2 Bytes der IP-Adresse bestimmen das Subnetz - also 192.168. Die letzten beiden Bytes adressieren den Teilnehmer - also 16.2.

Allgemein gilt:

- Die Netzadresse ergibt sich aus der UND-Verknüpfung von IPv4-Adresse und Subnetzmaske.
- Die Teilnehmeradresse ergibt sich aus der UND-NICHT-Verknüpfung von IPv4-Adresse und Subnetzmaske.

### Classless Inter-Domain Routing (CIDR)

CIDR ist ein Verfahren, das mehrerer IPv4-Adressen zu einem Adressbereich zusammenfasst, indem eine IPv4-Adresse mit ihrer Subnetzmaske kombiniert dargestellt wird. Dazu wird an die IPv4-Adresse ein Suffix angehängt, das die Anzahl der auf 1 gesetzten Bits der Netzmaske angibt. Durch die CIDR-Notation lassen sich Routing-Tabellen reduzieren und die verfügbaren Adressbereiche besser ausnutzen.

**Beispiel**:

IPv4-Adresse 192.168.0.0 mit Subnetzmaske 255.255.255.0

Der Netzanteil der Adresse umfasst in der binären Darstellung 3 x 8 Bits, also 24 Bits.

Daraus ergibt sich die CIDR-Notation 192.168.0.0/24.
Der Host-Anteil umfasst in der binären Darstellung 1 x 8 Bits. Daraus ergibt sich der Adressbereich von 28, also 256 mögliche Adressen.

### Weitere Subnetze maskieren

Über die Subnetzmaske können Sie ein Subnetz, das einer der Adressklassen A, B oder C zugeordnet ist, weiter strukturieren und "private" Subnetze bilden, indem Sie weitere niederwertige Stellen der Subnetzmaske auf "1" setzen. Pro jedem auf "1" gesetzten Bit verdoppelt sich die Anzahl der "privaten" Netze und halbiert sich die Anzahl der darin enthaltenen Teilnehmer. Nach außen wirkt das Netzwerk nach wie vor wie ein einzelnes Netzwerk.

Beispiel:

Sie ändern bei einem Subnetz der Adressklasse B (z. B. IP-Adresse 129.80.xxx.xxx) die Default-Subnetzmaske wie folgt:

| Masken | Dezimal | Binär |
|---|---|---|
| Default-Subnetzmaske | 255.255.0.0 | 11111111.11111111.00000000 .00000000 |
| Subnetzmaske | 255.255.128.0 | 11111111.11111111.10000000 .00000000 |

Ergebnis:

Alle Teilnehmer mit Adressen von 129.80.1.xxx bis 129.80.127.xxx befinden sich auf einem IP-Subnetz, alle Teilnehmer mit Adressen von 129.80.128.xxx bis 129.80.255.xxx auf einem anderen IP-Subnetz.

**Netzübergang (Router)**

Die Netzübergänge (Router) haben die Aufgabe, die IP-Subnetze zu verbinden. Wenn ein IP-Datagramm an ein anderes Netzwerk geschickt werden soll, muss es zunächst an einen Router vermittelt werden. Damit das möglich ist, müssen Sie für jeden Teilnehmer des IP-Subnetzes die Adresse des Routers eingeben.

Die IP-Adresse eines Teilnehmers im Subnetz und die IP-Adresse des Netzübergangs (Router) dürfen nur an den Stellen unterschiedlich sein, an denen in der Subnetzmaske "0" steht.

### 4.1.2.2 Erstmalige Vergabe einer IPv4-Adresse

**Konfigurationsmöglichkeiten**

Die erstmalige Vergabe einer IP-Adresse für ein SCALANCE W-Gerät kann nicht mit dem Web Based Management (WBM) oder dem Command Line Interface (CLI) über TELNET erfolgen, weil diese Konfigurations-Werkzeuge bereits eine IP-Adresse voraussetzen.

Es gibt folgende Möglichkeiten, einem unkonfigurierten Gerät ohne IP-Adresse eine solche Adresse zuzuweisen:

- DHCP (Default)
- SINEC PNI
- STEP 7
- SINEC NMS

**Hinweis**

DHCP ist im Auslieferungszustand und nach "Auf gespeicherte Einstellungen zurücksetzen und Neustart" eingeschaltet.

Wenn ein DHCP-Server im lokalen Netz verfügbar ist und dieser auf den DHCP-Request eines SCALANCE W-Geräts antwortet, so werden schon beim ersten Hochlauf automatisch IP-Adresse, Subnetzmaske und Gateway zugeteilt. Durch "Auf Werkseinstellungen zurücksetzen und Neustart" wird weder eine durch DHCP noch eine vom Benutzer vergebene IP-Adresse gelöscht.

SINEC INS kann als hauseigener DHCP-Server eingesetzt werden und Geräten im Netzwerk IP-Adressen zuweisen.

#### 4.1.2.3 Adressvergabe über DHCPv4

### Eigenschaften von DHCP

DHCP (Dynamic Host Configuration Protocol) ist ein Verfahren zur automatischen Vergabe von IP-Adressen. Es hat folgende Eigenschaften:

- DHCP kann sowohl während des Hochlaufs eines Geräts als auch im laufenden Betrieb eingesetzt werden.
- Die vergebene IP-Adresse bleibt nur für eine begrenzte Zeitdauer (Lease Time) gültig. Nachdem die Gültigkeitsdauer zur Hälfte abgelaufen ist, kann der DHCP-Client die vergebene IPv4-Adresse verlängern. Nach Ablauf der gesamten Zeitdauer muss der DHCP-Client eine neue IPv4-Adresse anfordern.
- Normalerweise erfolgt keine feste Adresszuordnung, d. h. wenn ein Client erneut eine IP-Adresse anfordert, erhält er in der Regel eine andere Adresse als bei der vorhergehenden Anforderung. Es ist möglich, den DHCP-Server so zu konfigurieren, dass der DHCP-Client auf seine Anfrage immer dieselbe feste Adresse zugeordnet bekommt. Über welchen Parameter der DHCP-Client für die feste Adresszuordnung identifiziert wird, wird im DHCP-Client eingestellt. Die Adresse kann über die MAC-Adresse, die DHCP Client ID, PROFINET-Gerätename oder den Gerätenamen zugeordnet werden. Den Parameter konfigurieren Sie unter "System > DHCP-Client".
- Folgende DHCP-Optionen werden unterstützt:
  - DHCP-Option 3: Vergabe einer Routeradresse
  - DHCP-Option 6: Vergabe einer DNS-Serveradresse
  - DHCP-Option 66: Vergabe eines dynamischen TFTP-Servernamens
  - DHCP-Option 67: Vergabe eines dynamischen Bootfile-Namens

**Hinweis**

DHCP sieht einen Mechanismus vor, nach dem die IP-Adresse nur für eine begrenzte Zeitdauer (Lease Time) zugeteilt wird. Wenn nach Ablauf der Lease Time das Gerät den DHCP Server nicht für einen erneuten Request erreicht, werden die zugewiesene IP-Adresse, die Subnetz-Maske und das Gateway weiterhin benutzt.

Das Gerät ist folglich auch ohne DHCP Server weiterhin unter der zuletzt vergebenen IP Adresse erreichbar. Dies entspricht nicht dem Standard-Verhalten von Office-Geräten, ist jedoch für einen reibungslosen Anlagenbetrieb notwendig.

#### 4.1.2.4 Adressvergabe mit SINEC PNI

### Einleitung

Das SINEC PNI ist in der Lage, unkonfigurierten Geräten, die noch keine IP-Adresse besitzen, eine solche Adresse zuzuweisen.

**SINEC PNI**

- Um dem Gerät mit SINEC PNI eine IP-Adresse zuweisen zu können, muss das Gerät über Ethernet erreichbar sein.
- Sie finden SINEC PNI auf den Internetseiten des Siemens Industry Online Support unter folgendem Link: (https://support.industry.siemens.com/cs/de/de/ps/26672/dl)
- Beachten Sie für weitere Informationen zur Vergabe der IP-Adresse mit SINEC PNI die Online-Hilfe oder die Betriebsanleitung "Netzwerkmanagement SINEC PNI".

#### 4.1.2.5 Adressvergabe über STEP 7

Sie können in STEP 7 die Topologie, den Gerätenamen und die IP-Adresse projektieren, d. h. für die MAC-Adresse des Geräts wird eine IP-Adresse festgelegt. Wenn Sie das unkonfigurierte Gerät mit dem Controller verbinden, weist der Controller dem Gerät den projektierten Gerätenamen und die IP-Adresse automatisch zu.

**STEP 7 V5.x und früher**

Beachten Sie für weitere Informationen zur Vergabe der IP-Adresse über STEP 7 V5.x und früher die Dokumentation "Hardware konfigurieren und Verbindungen projektieren mit STEP 7", Abschnitt "Schritte zum Konfigurieren eines PROFINET IO-Systems".

**STEP 7 ab V13**

Beachten Sie für weitere Informationen zur Vergabe der IP-Adresse über STEP 7 ab V13 die Online-Hilfe "Informationssystem", Abschnitt "Adressierung von PROFINET-Geräten".

### 4.1.3 IPv6-Adresse

#### 4.1.3.1 IPv6-Begriffe

**Netzknoten**

Ein Netzknoten ist ein Gerät, das über eine oder mehrere Schnittstellen an ein oder mehrere Netzwerke angeschlossen ist.

**Router**

Ein Netzknoten, der IPv6-Pakete weiterleitet.

**Host**

Ein Netzknoten, der einen Endpunkt für IPv6-Kommunikationsbeziehungen darstellt.

**Link**

Als Link wird in der IPv6-Terminologie eine direkte Layer 3-Verbindung innerhalb eines IPv6-Netzwerks bezeichnet.

**Nachbar**

Zwei Netzknoten werden als Nachbarn bezeichnet, wenn sie sich auf dem gleichen Link befinden.

**IPv6-Schnittstelle**

Physische oder logische Schnittstelle, an der IPv6 aktiviert ist.

**Path MTU**

Maximal zulässige Paketgröße auf einem Pfad, von einem Absender zu einem Empfänger.

**Path MTU Discovery**

Mechanismus zur Bestimmung der maximal zulässigen Paketgröße entlang des gesamten Pfades von einem Absender zu einem Empfänger.

**LLA**

Link lokale-Adresse FE80::/10

Sobald IPv6 auf der Schnittstelle aktiviert wird, wird automatisch eine link lokale-Adresse gebildet. Nur erreichbar für Knoten, die sich auf dem gleichen Link befinden.

**ULA**

Unique lokal-Adresse

Definiert in der RFC 4193. Über diese Adresse ist die IPv6-Schnittstelle im LAN erreichbar.

**GUA**

Globale Unicast-Adresse

Über diese Adresse ist die IPv6-Schnittstelle z. B. über das Internet erreichbar.

**Schnittstellen-ID**

Die Schnittstellen-ID wird mit dem EUI-64 Verfahren oder manuell gebildet.

**EUI-64**

Extended Unique Identifier (RFC 4291); Verfahren zur Bildung der Schnittstellen-ID. Bei Ethernet wird die Schnittstellen-ID aus der MAC-Adresse der Schnittstelle gebildet. Teilt die MAC-Adresse in den herstellerspezifischen Teil (OUI) und den netzwerkspezifischen Teil (NIC) und fügt zwischen den beiden Teilen FFFE ein.

Beispiel:

MAC-Adresse = 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**

Definiert die Reichweite der IPv6-Adresse.

### 4.1.3.2 Aufbau einer IPv6-Adresse

#### Adressformat IPv6-Notation

IPv6-Adressen bestehen aus 8 Blöcken mit jeweils vierstelligen Hexadezimalziffern (128 Bit insgesamt). Die Blöcke sind durch einen Doppelpunkt getrennt.

Beispiel:

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

Regeln/Vereinfachungen:

- Wenn ein oder mehr Blöcke den Wert 0 haben, ist eine verkürzte Schreibweise möglich.
  Die Adresse fd00:**0000:0000**:ffff:02d1:7d01:0000:8f21 kann verkürzt auch wie folgt notiert werden:
  fd00**::**ffff:02d1:7d01:0000:8f21
  Damit Eindeutigkeit gewahrt bleibt, darf diese Verkürzung nur einmal innerhalb der gesamten Adresse angewendet werden.
- Führende Nullen innerhalb eines Blocks dürfen weggelassen werden.
  Die Adresse fd00:0000:0000:ffff:**02d1**:7d01:0000:8f21 kann verkürzt auch wie folgt notiert werden:
  fd00**::**ffff:**2d1**:7d01:0000:8f21
- Dezimalnotation mit Punkt-Schreibweise
  Für die letzten 2 Blöcke bzw. 4 Byte kann die herkömmliche Dezimalnotation in Punkt-Schreibweise verwendet werden.
  Beispiel: Die IPv6-Adresse fd00::ffff.125.1.0.1 ist äquivalent zu fd00::ffff:7d01:1

#### Aufbau IPv6-Adresse

Das IPv6-Protokoll unterscheidet drei Adressarten: Unicast, Anycast und Multicast. Der folgende Abschnitt beschreibt den Aufbau der globalen Unicast-Adressen.

| **IPv6-Präfix** | | **Suffix** |
|---|---|---|
| Globales Präfix:<br>n Bit | Subnetz-ID<br>m Bit | Schnittstelle-ID<br>128 - n - m Bits |
| Zugewiesener Adress-bereich | Beschreibung des Standorts, auch Subnetzpräfix oder Subnetz | Eindeutige Zuordnung des Hosts im Netz.<br>Die ID wird aus der MAC-Adresse generiert. |

Das Präfix für die link local-Adresse ist immer fe80:0000:0000:0000. Das Präfix wird verkürzt und wie folgt notiert: fe80::

#### IPv6-Präfix

Festgelegt in: RFC 4291

Das IPv6-Präfix stellt die Subnetzkennung dar.

Präfixe und IPv6-Adressen werden auf dieselbe Weise angegeben wie bei der CIDR-Notation (Classless Inter-Domain Routing) für IPv4.

**Aufbau**

IPv6-Adresse / Präfixlänge

**Beispiel**

IPv6-Adresse: 2001:0db8:1234::1111/48

Präfix: 2001:0db8:1234::/48

Schnittstelle-ID: ::1111

### Eingabe und Darstellung

Die Eingabe von IPv6-Adressen ist in den zuvor beschriebenen Notationen möglich. IPv6-Adressen werden immer in der hexadezimalen Notation angezeigt.

## 4.2 VLAN

### 4.2.1 VLAN

#### Netzwerkdefinition unabhängig von der räumlichen Lage der Teilnehmer

VLAN (Virtuelles Local Area Network) teilt ein physikalisches Netzwerk in mehrere logischen Netzwerke, die voneinander abgeschirmt sind. Hierbei werden Geräte zu logischen Gruppen zusammengefasst. Nur Teilnehmer des gleichen VLANs können sich untereinander adressieren. Da auch Multicast- und Broadcast-Telegramme nur innerhalb des jeweiligen VLANs weitergeleitet werden, wird von Broadcast-Domänen gesprochen.

Daraus ergibt sich als besonderer Vorteil von VLANs eine geringere Netzlast für die Teilnehmer bzw. Netzsegmente anderer VLANs.

Für die Kennung, welches Paket welchem VLAN zugeordnet ist, wird das Telegramm um 4 Byte erweitert, siehe VLAN-Tagging (Seite 68). Diese Erweiterung enthält neben der VLAN-ID auch Prioritätsinformationen.

#### Möglichkeiten der VLAN-Zuordnung

Es gibt verschiedene Möglichkeiten der Zuordnung zu VLANs:

- Port-basiertes VLAN
  Jedem Port eines Geräts wird eine VLAN-ID zugewiesen. Port-basiertes VLAN konfigurieren Sie unter "Layer 2 > VLAN > Port-basiertes VLAN".
- Protokoll-basiertes VLAN
  Jedem Port eines Geräts wird eine Protokollgruppe zugewiesen.
- Subnetz-basiertes VLAN
  Der IP-Adresse des Geräts wird eine VLAN-ID zugewiesen.

### VLAN-Zuordnung am Gerät

| | | |
|---|---|---|
| SCALANCE M812<br>SCALANCE MUM856 | P1 | vlan1<br>Für den Zugriff vom lokalen Netz (LAN) auf das Gerät |
| SCALANCE M874<br>SCALANCE M804PB | P1 und P2 | vlan1<br>Für den Zugriff vom lokalen Netz (LAN) auf das Gerät |
| SCALANCE M876<br>SCALANCE M816<br>SCALANCE MUM853 | P1 bis P4 | vlan1<br>Für den Zugriff vom lokalen Netz (LAN) auf das Gerät |
| SCALANCE M826 | P1 bis P4<br>SHDSL 1 und SHDSL 2 | vlan1<br>Für den Zugriff vom lokalen Netz (LAN) auf das Gerät |

Die VLANs sind in verschiedenen IP-Subnetzen. Damit diese miteinander kommunizieren können, müssen im Gerät die entsprechende Route und die Firewall-Regel konfiguriert sein.

Die Zuordnung können Sie unter "Layer 2 > VLAN > Allgemein (Seite 342)" ändern.

## 4.2.2 VLAN-Tagging

### Erweiterung der Ethernet-Telegramme um vier Byte

Für CoS (Class of Service, Telegrammpriorisierung) und für VLAN (Virtuelles Netzwerk) wurde in der Norm IEEE 802.1Q die Erweiterung der Ethernet-Telegramme um das VLAN-Tag festgelegt.

**Hinweis**

Durch das VLAN-Tag erhöht sich die zulässige Gesamtlänge des Telegramms von 1518 auf 1522 Byte.
Es muss geprüft werden, ob die Endteilnehmer im Netz diese Länge / diesen Telegrammtyp verarbeiten können. Ist dies nicht der Fall, dürfen an diese Teilnehmer nur Telegramme mit der Standardlänge gesendet werden.

Die zusätzlichen 4 Bytes befinden sich im Header des Ethernet-Telegramms zwischen der Quelladresse und dem Ethernet-Typ-/Längenfeld:

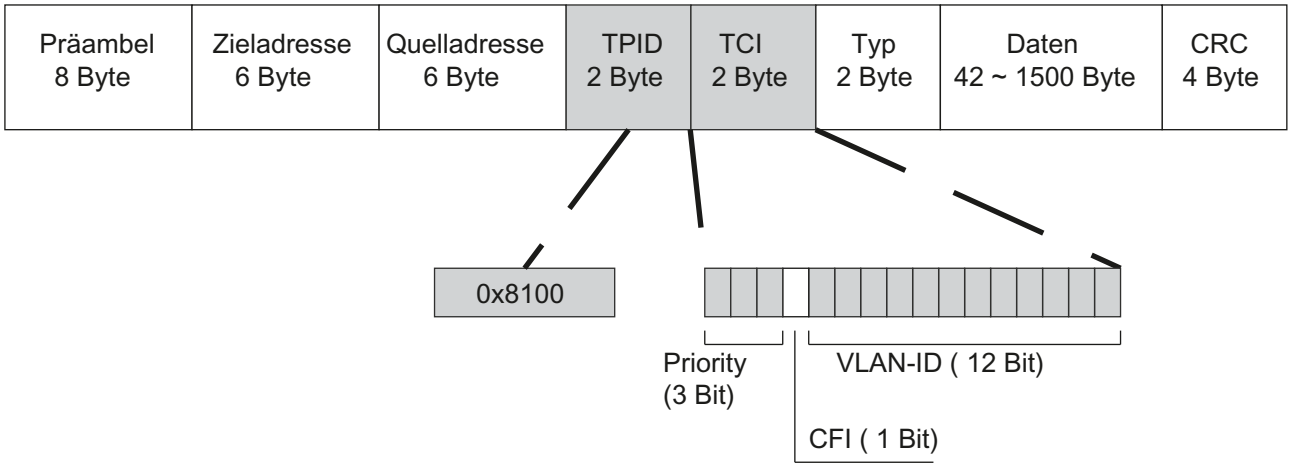



Bild 4-1 Aufbau des erweiterten Ethernet-Telegramms

Die zusätzlichen Bytes beinhalten den Tag Protocol Identifier (TPID) und die Tag Control Information (TCI).

### Tag Protocol Identifier (TPID)

Die ersten 2 Bytes bilden den Tag Protocol Identifier (TPID) und sind fest mit 0x8100 belegt. Dieser Wert gibt an, dass das Datenpaket VLAN-Informationen oder Prioritätsangaben beinhaltet.

### Tag Control Information (TCI)

Die 2 Bytes der Tag Control Information (TCI) beinhalten folgende Informationen:

**CoS-Priorisierung**

In dem getaggten Telegramm gibt es 3 Bits für die Priorität, die auch als Class of Service (CoS) bezeichnet werden, siehe auch IEEE 802.1Q.

| CoS-Bits | Priorität | Art des Datenverkehrs |
|---|---|---|
| 000 | 0 (niedrigste) | Background (Hintergrund) |
| 001 | 1 | Best Effort |
| 010 | 2 | Excellent Effort |
| 011 | 3 | Critical Applications (Kritische Anwendungen) |
| 100 | 4 | Video, < 100 ms Verzögerung (Latenz und Jitter) |
| 101 | 5 | Voice (Sprache), < 10 ms Verzögerung (Latenz und Jitter) |
| 110 | 6 | Internetwork Control |
| 111 | 7 (höchste) | Network Control |

Die Priorisierung der Datenpakete setzt eine Warteschlange in den Komponenten voraus, in der sie die Datenpakete mit der niedrigeren Priorität puffern können.

Das Gerät besitzt mehrere parallele Warteschlangen, in denen die verschieden priorisierten Telegramme abgearbeitet werden. Standardmäßig werden zuerst die Telegramme mit der höchsten Priorität abgearbeitet. Dieses Verfahren gewährleistet auch bei einem hohen

Datenaufkommen, dass die Telegramme mit der höchsten Priorität auf jeden Fall gesendet werden.

**Canonical Format Identifier (CFI)**

Der CFI wird für die Kompatibilität zwischen Ethernet und Token Ring benötigt.
Die Werte haben folgende Bedeutung:

| Wert | Bedeutung |
|---|---|
| 0 | Das Format der MAC-Adresse ist kanonisch. Bei kanonischer Darstellung der MAC-Adresse wird das niederwertigste Bit zuerst übertragen. Standardeinstellung für Ethernet-Switches. |
| 1 | Das Format der MAC-Adresse ist nicht kanonisch. |

**VLAN-ID**

Im 12 Bit-Datenfeld können bis zu 4096 VLAN-IDs gebildet werden. Dabei gelten folgende Festlegungen:

| VLAN-ID | Bedeutung |
|---|---|
| 0 | Das Telegramm beinhaltet nur Prioritätsinformation (Priority Tagged Frames) und keine gültige VLAN-Kennung. |
| 1 - 4094 | Gültige VLAN-Kennung, das Telegramm ist einem VLAN zugeordnet, es kann zusätzlich auch Prioritätsinformationen beinhalten. |
| 4095 | Reserviert |

## 4.3 VXLAN

VXLAN (Virtual eXtensible LAN) teilt wie VLAN ein Netzwerk in mehrere virtuelle Netzwerksegmente. Dabei wird der Ethernet-Frame (Layer 2) durch einen VXLAN-Tunnel über ein IP-Netzwerk (Layer 3) weitergeleitet.

**VNI / VNID**

Die VXLAN Netzwerk-ID (VNID / VNI) bestimmt die Zugehörigkeit eines Ethernet-Frames zu einem VXLAN und hat 24 Bit. Somit sind bis zu 16 Millionen Netzwerksegmente möglich, oft auch als VXLAN-Segmente bezeichnet. Die Teilnehmer mit der gleichen VNI befinden sich in einem VXLAN-Segment und können miteinander kommunizieren.

**VTEP**

Die Geräte (physisch oder virtuell), die den Tunnel aufbauen, werden als VXLAN Tunnel-Endpunkte (VTEP) bezeichnet. Zum Senden der Ethernet-Frame kapselt der Quell-VTEP den Frame in verschiedene Header. Der Ziel-VTEP, auch Remote-VTEP genannt, entkapselt den Ethernet-Frame und leitet ihn weiter.

Der VTEP besitzt zwei Schnittstellen.

- Physische Schnittstelle
  Über die physische Schnittstelle ist der VTEP mit dem lokalen Netzwerk und dessen Teilnehmer verbunden. An dieser Schnittstelle werden die Ethernet-Frames gekapselt und entkapselt.
  Je nach Konfiguration ist das lokale Netzwerk in mehrere VLANs eingeteilt. Damit der VTEP den Ethernet-Frame in das richtige VLAN weiterleitet, wird eine Zuordnung von VLAN-ID zu VNI konfiguriert. Das gilt auch für die Gegenrichtung. Wenn der VTEP einen Ethernet-Frame empfängt, verwendet dieser die VNI im VXLAN-Header, die diesem VLAN zugeordnet ist.
- Virtuelle Schnittstelle
  Über die Netzwerk Virtuelle Endpunkt-Schnittstelle (NVE) bauen die VTEP den VXLAN-Tunnel auf und leiten den gekapselten Ethernet-Frame weiter. Ein VTEP kann mehrere NVE-Schnittstellen haben, die sich durch eine eindeutige ID (NVE-ID (Seite 347)) unterscheiden.

**Frame-Format bei VXLAN**

<table>
<tr><th colspan="8">Header in die der Layer2 Ethernet-Frame eingekapselt wird</th><th>Layer2 Ethernet-Frame</th></tr>
<tr><th colspan="2">① Outer MAC-Header<br>18 Bytes</th><th colspan="2">② Outer IP-Header<br>IPv4: 20 Bytes<br>IPV6: 40 Bytes</th><th colspan="2">③ UDP-Header<br>8 Bytes</th><th colspan="2">④ VXLAN-Header<br>8 Bytes</th><th></th></tr>
<tr><th>Bit</th><th></th><th>Bit</th><th></th><th>Bit</th><th></th><th>Bit</th><th></th><th></th></tr>
<tr><td>48</td><td>Remote-VTEP MAC-Adresse (Seite 352)</td><td>72</td><td>Verschiedene Daten des IP-Headers</td><td>16</td><td>Quell-Port</td><td>8</td><td>VXLAN-Flag<br>00001000: VNI enthalten</td><td>⑤ Inner MAC-Header<br>• Ziel-MAC-Adresse<br>• Quell-MAC-Adresse<br>⑥ Inner IP-Header<br>• Ziel-MAC-Adresse<br>• Quell-MAC-Adresse<br>⑦ VLAN-Tag (Seite 350)<br>⑧ Payload<br>46 ... 1500 Bytes</td></tr>
<tr><td>48</td><td>Quell-VTEP MAC-Adresse</td><td>8</td><td>IP-Protokoll</td><td>16</td><td>Ziel-Port (VXLAN-Port) (Seite 347)</td><td>24</td><td>Reserviert</td><td rowspan="4">Frame Check Sequence</td></tr>
<tr><td>16</td><td>VLAN-Typ</td><td>16</td><td>Checksum</td><td>16</td><td>Länge</td><td>24</td><td>VNI (Seite 350)</td></tr>
<tr><td>16</td><td>VLAN-ID</td><td>32 /64</td><td>32: Quell-VTEP IPv4-Adresse (Seite 349)<br>64: Quell-IPv6-Adresse</td><td rowspan="2">16</td><td rowspan="2">Checksum</td><td rowspan="2">8</td><td rowspan="2">Reserviert</td></tr>
<tr><td>16</td><td>Ethernet-Typ</td><td>32 /64</td><td>32: Remote-VTEP IPv4-Adresse (Seite 350) oder Remote-VTEP IPv4-Adresse (Seite 352)<br>64: Ziel-IPv6-Adresse</td></tr>
</table>

### VXLAN und Firewall

Damit ein VTEP mit dem VTEP des Geräts einen VXLAN-Tunnel aufbauen kann, ist die vordefinierte Firewallregel "VXLAN" zu aktivieren.

## 4.4 SNMP

### Einleitung

Mit Hilfe des Simple Network Management Protocol (SNMP) überwachen und steuern Sie Netzwerkkomponenten, z. B. Router oder Switches, von einer zentralen Station aus. SNMP regelt dabei die Kommunikation zwischen den überwachten Geräten und der Überwachungsstation.

Aufgaben von SNMP:

- Überwachung von Netzwerkkomponenten
- Fernsteuerung und Fernparametrierung von Netzwerkkomponenten
- Fehlererkennung und Fehlerbenachrichtigung

In den Versionen v1 und v2c verfügt SNMP über keine Sicherheitsmechanismen. Jeder Nutzer im Netzwerk kann mit geeigneter Software auf die Daten zugreifen und auch Parametrierungen verändern.

Für die einfache Steuerung von Zugriffsrechten ohne Sicherheitsaspekte werden Community-Strings verwendet.

Der Community-String wird zusammen mit der Anfrage übertragen. Wenn der Community-String korrekt ist, antwortet der SNMP-Agent und sendet die geforderten Daten. Wenn der Community-String nicht korrekt ist, verwirft der SNMP-Agent die Anfrage. Für Lese- und Schreibrechte definieren Sie verschiedene Community-Strings. Die Community-Strings werden in Klartext übertragen.

Standardwerte der Community-Strings:

- public
  besitzt nur Leserechte
- private
  besitzt Lese- und Schreibrechte

**Hinweis**

Da es sich bei den SNMP-Community Strings um einen Zugriffsschutz handelt, verwenden Sie nicht die Standardwerte "public" oder "private". Ändern Sie diese Werte nach der Erst-Inbetriebnahme.

Weitere einfache Schutzmechanismen auf Geräteebene:

- Allowed Host
  Dem überwachten System sind die IP-Adressen der überwachenden Systeme bekannt.
- Read Only
  Wenn Sie einem überwachten Gerät "Read Only" zuweisen, können Überwachungsstationen nur Daten auslesen, aber nicht ändern.

SNMP-Datenpakete sind nicht verschlüsselt und können einfach mitgelesen werden.

Die zentrale Station wird auch als Management-Station bezeichnet. Auf den zu überwachenden Geräten ist ein SNMP-Agent installiert, mit dem die Management-Station Daten austauscht.

Die Management-Station sendet Datenpakete folgenden Typs:

- GET
  Anfordern eines Datensatzes vom SNMP-Agent
- GETNEXT
  Ruft den nächsten Datensatz auf.
- GETBULK (verfügbar ab SNMPv2c)
  Fordert mehrere Datensätze auf einmal an, z. B. mehrere Zeilen einer Tabelle.
- SET
  Beinhaltet Parametrierungsdaten für das entsprechende Gerät.

Der SNMP-Agent sendet Datenpakete folgenden Typs:

- RESPONSE
  Der SNMP-Agent sendet die vom Manager angeforderten Daten zurück.
- TRAP
  Wenn ein bestimmtes Ereignis eintritt, sendet der SNMP-Agent eigenständig Traps.
- INFORM
  Wie ein Trap, nur dass dieser vom Empfänger quittiert wird.

SNMPv1/v2c/v3 verwenden UDP (User Datagram Protocol) und nutzen die UDP-Ports 161 und 162. Die Beschreibung der Daten erfolgt in einer Management Information Base (MIB).

### SNMPv3

SNMPv3 führt gegenüber den Vorgängerversionen SNMPv1 und SNMPv2c ein umfangreicheres Sicherheitskonzept ein.

SNMPv3 unterstützt:

- Vollständig verschlüsselte Benutzerauthentifizierung
- Verschlüsselung des gesamten Datenverkehrs
- Zugriffskontrolle der MIB-Objekte auf Benutzer-/Gruppenebene

Mit der Einführung von SNMPv3 können Sie Benutzerkonfigurationen nicht mehr ohne Weiteres auf andere Geräte übertragen, z. B. indem Sie eine Konfigurationsdatei laden oder den C-PLUG austauschen.

Das SNMPv3-Protokoll verwendet gemäß dem Standard eine eindeutige SNMP-Engine-ID als internen Bezeichner für einen SNMP-Agenten. Diese ID muss im Netzwerk eindeutig sein. Sie

wird verwendet, um die Zugangsdaten von SNMPv3-Benutzern zu authentifizieren und zu verschlüsseln.

Abhängig davon, ob Sie die Funktion "SNMPv3 Benutzermigration" aktiviert oder deaktiviert haben, wird die SNMP-Engine-ID unterschiedlich generiert.

**Einschränkung bei der Verwendung der Funktion**

Verwenden Sie die Funktion "SNMPv3 Benutzermigration" nur, um im Ersatzteilfall Ihre konfigurierten SNMPv3-Benutzer auf ein Ersatzgerät zu übertragen.
Verwenden Sie die Funktion nicht, um konfigurierte SNMPv3-Benutzer auf mehrere Geräte zu übertragen. Wenn Sie eine Konfiguration mit angelegten SNMPv3-Benutzern in mehrere Geräte laden, verwenden diese Geräte hierdurch die gleiche SNMP-Engine-ID. Wenn Sie diese Geräte im gleichen Netzwerk verwenden, widerspricht Ihre Konfiguration dem SNMP-Standard.

**Kompatibilität mit Vorgängerprodukten**

Sie können SNMPv3-Benutzer nur auf ein anderes Gerät übertragen, wenn Sie die Benutzer als migrierbare Benutzer erstellt haben. Um einen migrierbaren Benutzer zu erstellen, muss die Funktion "SNMPv3 Benutzermigration" aktiviert sein, wenn Sie den Benutzer erstellen.

## 4.5 ICMP

Die Abkürzung ICMP steht für Internet Control Message Protocol (RFC792) und dient zum Austausch von Fehler- und Informationsmeldungen.

- Fehlermeldung
  Informiert den Absender des IP-Telegramms, dass beim Weiterleiten des Telegramms ein Fehler oder ein Parameterproblem aufgetreten ist.
- Informationsmeldung
  Kann Informationen zur Zeitmessung, zur Adressmaske, zur Erreichbarkeit des Ziels oder zum Auffinden des Routers enthalten.

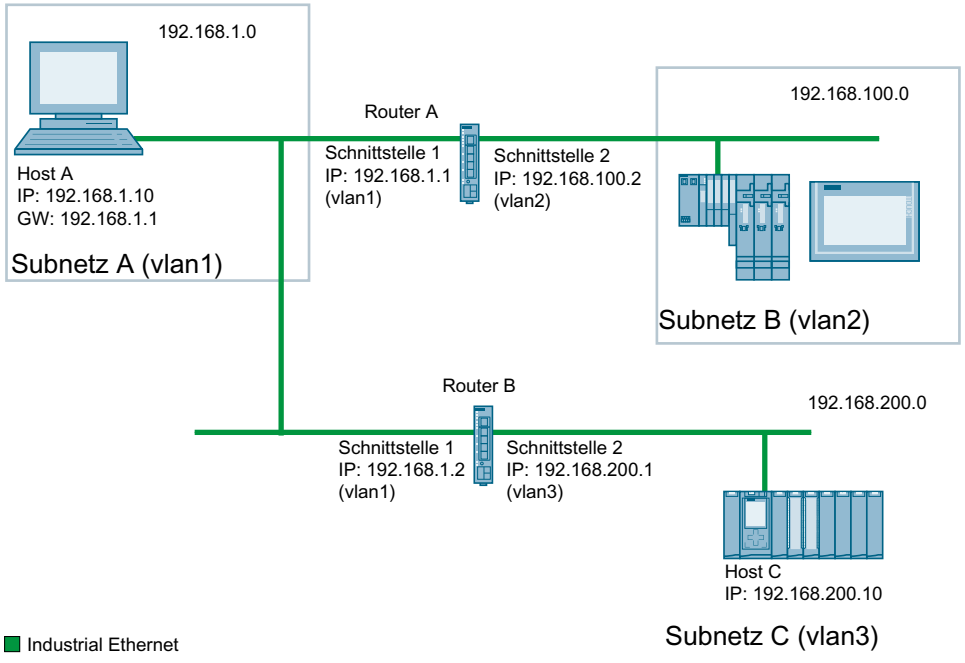
### Aufbau des ICMP-Datenpakets

| 0 | 4 | 8 | 12 | 16 | 20 | 24 | 28 | 31 |
|---|---|---|---|---|---|---|---|---|
| ICMP-Pakettyp<br>Art der Meldung | | Code<br>Weitere Details der Meldung | | Prüfsumme | | | | |
| Daten (optional) | | | | | | | | |

- **ICMP-Pakettyp**
  Die wichtigsten ICMP-Pakettypen sind:
  - Redirect
    Der Router teilt dem Host in einem seiner Subnetze mit, dass es eine bessere Route zum Ziel gibt. Auf diesen ICMP-Pakettyp wird in der folgenden Beschreibung näher eingegangen.
  - Destination Unreachable
    IP-Telegramm ist nicht zustellbar.
  - Time Exceeded
    Zeitlimit überschritten
  - Echo-Request
    Echo-Frage, besser bekannt als Ping.
- **Code**
  Der Code beschreibt den ICMP-Pakettyp genauer. Die Auswahl ist abhängig vom gewählten ICMP-Pakettyp. Bei "Destination Unreachable" ist z. B. "Code 1" Host ist nicht erreichbar.

Eine vollständige Liste der ICMP-Pakettypen und Codes finden Sie auf der Webseite von IANA (https://www.iana.org/).

## ICMP-Pakettyp 5 - Redirect




Der Host A will an den Host C ein IP-Telegramm senden. Der Host C liegt nicht im gleichen Subnetz wie der Host A. Deshalb sendet der Host A das IP-Telegramm an seinen Default-Gateway. Das Default-Gateway von Host A ist die Schnittstelle 1 des Routers A. Der Router A kann das IP-Telegramm nicht weiterleiten, da er das Zielnetzwerk nicht kennt. Über seine Routingtabelle weiß Router A jedoch, dass das Subnetz C über den Router B erreichbar ist. Der Router B verbindet das Subnetz A mit dem Subnetz C. Der Router A schickt an den Host A eine Redirect-Nachricht. Darin weist der Router A den Host A an, die IP-Telegramme an Host

C zukünftig über Router B zu senden, dessen IP-Adresse in der Redirect-Nachricht enthalten ist. Das initiale IP-Telegramm wird vom Router A direkt an Router B gesendet, der es an Host C weitergibt.

**Bedingungen für den Versand von Redirect-Nachrichten**

- Das IP-Telegramm wird über die gleiche Schnittstelle des Routers A empfangen und gesendet.
- Die Quell-IP-Adresse (Host A) ist aus dem gleichen Subnetz wie die Next-Hop-Adresse (Router B) in der Routingtabelle.
- Das IP-Telegramm ist nicht von einer Source NAT-Regel (Masquerading, Source-NAT oder NETMAP) betroffen.
- Damit der Router A das initiale IP-Telegramm an Router B weiterleitet, wird eine Firewall Regel vlanX → vlanX benötigt.

## 4.6 Security-Funktionen

### 4.6.1 Anpassen der MTU für IPsec VPN und SINEMA RC

#### Anpassen der MTU (Maximum Transmission Unit)

Die MTU legt die zulässige Größe eines Datenpaketes für die Übertragung im Netzwerk fest. Wenn diese Datenpakete nun vom Gerät über den IPsec Tunnel bzw. SINEMA RC übertragen werden, wird das ursprüngliche Datenpaket durch die zusätzlichen Header-Informationen größer und muss unter Umständen für die weitere Übertragung segmentiert werden. Dies ist abhängig von den MTU-Vorgaben im angeschlossenen Netzwerk. Eine erforderliche Segmentierung kann aber zu merklichen Performanceverlusten oder zum Abbruch der Datenübertragung führen.

Vermeiden können Sie dies, indem Sie auf dem Endgerät das MTU-Format anpassen, d. h. so reduzieren, dass die beim Gerät eintreffenden Datenpakete mit den benötigten Zusatzinformationen ergänzt werden können, ohne dass eine anschließende Segmentierung erforderlich ist. Eine sinnvolle Größe liegt im Bereich zwischen 1000 und 1400 Byte.

### 4.6.2 Benutzerverwaltung

#### Übersicht zur Benutzerverwaltung

Der Zugriff auf das Gerät wird durch konfigurierbare Benutzereinstellungen verwaltet. Richten Sie Benutzer mit jeweils einem Passwort zur Authentifizierung ein. Weisen Sie den Benutzern eine Rolle mit entsprechenden Rechten zu.

Die Authentifizierung von Benutzern kann entweder von dem Gerät lokal oder von einem externen RADIUS-Server durchgeführt werden. Wie die Authentifizierung erfolgen soll, konfigurieren Sie auf der Seite "Security > AAA > Allgemein".

## Lokale Anmeldung

Die lokale Anmeldung von Benutzern durch das Gerät läuft wie folgt ab:

1. Der Benutzer meldet sich mit seinem Benutzernamen und Passwort bei dem Gerät an.
2. Das Gerät prüft, ob ein Eintrag für den Benutzer vorhanden ist:
   → Wenn ein entsprechender Eintrag existiert, wird der Benutzer mit den Rechten der verknüpften Rolle angemeldet.
   → Wenn kein entsprechender Eintrag existiert, wird dem Benutzer der Zugriff verweigert.

## Anmeldung über einen externen RADIUS-Server

RADIUS (Remote Authentication Dial-In User Service) ist ein Protokoll zur Authentifizierung und Autorisierung von Benutzern durch Server, auf denen Benutzerdaten zentral abgelegt werden können.

Abhängig davon, welchen RADIUS-Autorisierungsmodus Sie auf der Seite "Security > AAA > RADIUS-Client" eingestellt haben, wertet das Gerät unterschiedliche Informationen des RADIUS-Servers aus.

**RADIUS-Autorisierungsmodus "Standard"**

Wenn Sie den RADIUS-Autorisierungsmodus "Standard" eingestellt haben, läuft die Authentifizierung von Benutzern über einen RADIUS-Server wie folgt ab:

1. Der Benutzer meldet sich mit seinem Benutzernamen und Passwort bei dem Gerät an.
2. Das Gerät schickt eine Authentifizierungsanfrage mit den Anmeldedaten an den RADIUS-Server.
3. Der RADIUS-Server führt eine Prüfung durch und meldet das Ergebnis an das Gerät zurück:
   - Der RADIUS-Server meldet eine erfolgreiche Authentifizierung und gibt für das Attribut "Service Type" den Wert "Administrative User" an das Gerät zurück:
     → Der Benutzer wird mit Administratorrechten angemeldet.
   - Der RADIUS-Server meldet eine erfolgreiche Authentifizierung und gibt einen anderen oder gar keinen Wert für das Attribut "Service Type" an das Gerät zurück:
     → Der Benutzer wird mit Leserechten angemeldet.
   - Der RADIUS-Server meldet eine fehlgeschlagene Authentifizierung an das Gerät zurück:
     → Dem Benutzer wird der Zugriff verweigert.

**RADIUS-Autorisierungsmodus "Herstellerspezifisch"**

**Voraussetzung**

Für den RADIUS-Autorisierungsmodus "Herstellerspezifisch" ist am RADIUS-Server Folgendes einzustellen:

- Herstellercode: 4196
- Attributnummer: 1
- Attributformat: Zeichenfolge (Gruppenname)

**Vorgehen**

Wenn Sie den RADIUS-Autorisierungsmodus "Herstellerspezifisch" eingestellt haben, läuft die Authentifizierung von Benutzern über einen RADIUS-Server wie folgt ab:

1. Der Benutzer meldet sich mit seinem Benutzernamen und Passwort bei dem Gerät an.
2. Das Gerät schickt eine Authentifizierungsanfrage mit den Anmeldedaten an den RADIUS-Server.
3. Der RADIUS-Server führt eine Prüfung durch und meldet das Ergebnis an das Gerät zurück:
   **Fall A**: Der RADIUS-Server meldet eine erfolgreiche Authentifizierung und gibt die dem Benutzer zugeordnete Gruppe an das Gerät zurück.
   - Die Gruppe ist auf dem Gerät bekannt und der Benutzer ist nicht in der Tabelle "Externe Benutzerkonten" eingetragen.
     → Der Benutzer wird mit den Rechten der zugeordneten Gruppe angemeldet.
   - Die Gruppe ist auf dem Gerät bekannt und der Benutzer ist in der Tabelle "Externe Benutzerkonten" eingetragen.
     → Der Benutzer wird der Rolle mit den größeren Rechten zugeordnet und mit diesen Rechten angemeldet.
   - Die Gruppe ist auf dem Gerät nicht bekannt und der Benutzer ist in der Tabelle "Externe Benutzerkonten" eingetragen:
     → Der Benutzer wird mit den Rechten der Rolle angemeldet, die mit seinem Benutzeraccount verknüpft ist.
   - Die Gruppe ist auf dem Gerät nicht bekannt und der Benutzer ist nicht in der Tabelle "Externe Benutzerkonten" eingetragen:
     → Der Benutzer wird mit den Rechten der Rolle "Default" angemeldet.

   **Fall B:** Der RADIUS-Server meldet eine erfolgreiche Authentifizierung, gibt jedoch keine Gruppe an das Gerät zurück:
   - Der Benutzer ist in der Tabelle "Externe Benutzerkonten" eingetragen:
     → Der Benutzer wird mit den Rechten der verknüpften Rolle angemeldet.
   - Der Benutzer ist nicht in der Tabelle "Externe Benutzerkonten" eingetragen:
     → Der Benutzer wird mit den Rechten der Rolle "Default" angemeldet.

   **Fall C:** Der RADIUS-Server meldet eine fehlgeschlagene Authentifizierung an das Gerät zurück:
   - Dem Benutzer wird der Zugriff verweigert.

### 4.6.3 Firewall

Zu den Security-Funktionen des Geräts gehört eine Stateful Inspection Firewall. Dabei handelt es sich um eine Methode der Paketfilterung bzw. Paketüberprüfung.

Die IP-Pakete werden anhand von Firewall-Regeln geprüft, in denen Folgendes festgelegt wird:

- Die erlaubten Protokolle
- IP-Adressen und Ports der erlaubten Quellen
- IP-Adressen und Ports der erlaubten Ziele

Wenn ein IP-Paket den festgelegten Parametern entspricht, dann darf es die Firewall passieren. Zusätzlich wird festgelegt, wie mit IP-Paketen verfahren wird, welche die Firewall nicht passieren dürfen.

Einfache Paketfiltertechniken benötigen pro Verbindung zwei Firewall-Regeln.

- Eine Regel für Anfragerichtung von der Quelle zum Ziel.
- Eine zweite Regel für die Antwortrichtung vom Ziel zur Quelle

### Stateful Inspection Firewall

Sie müssen nur eine Firewall-Regel für die Anfragerichtung von der Quelle zum Ziel festlegen. Die zweite Regel wird implizit hinzugefügt. Der Paketfilter merkt sich, wenn z. B. Rechner "A" mit Rechner "B" kommuniziert und erlaubt nur dann Antworten darauf. Eine Anfrage von Rechner "B" ist somit ohne vorherige Anforderung durch Rechner "A" nicht möglich.

Die Firewall konfigurieren Sie unter "Security > Firewall (Seite 406)".

**Hinweis**

**IP-Pakete über Layer 2 (innerhalb des gleichen VLANs)**

Wenn die IP-Pakete von dem Gerät über einen Switch-Port (Layer 2) gesendet werden, werden diese IP-Pakete nicht anhand von Firewall-Regeln geprüft. Die Firewall hat keine Wirkung auf Pakete, die auf der Layer 2-Ebene weitergeleitet werden.

### Kommunikationsrichtungen

| von | nach | Bedeutung |
|---|---|---|
| `vlan (1-x)`<br>`nve x` | `vlan (1-x)`<br>`nve x` | Zugriff vom V(X)LAN-Segment auf das V(X)LAN-Segment.<br>Beispiel:<br>vlan1 (INT) → vlan2 (EXT)<br>Zugriff vom lokalen IP-Subnetz und dem Gerät auf das externe IP-Subnetz. |
| | ppp0/usb | Zugriff vom IP-Subnetz auf die Mobilfunk-Schnittstelle des Geräts. |
| | Gerät | Zugriff vom IP-Subnetz auf das Gerät. |
| | SINEMA RC | Zugriff vom IP-Subnetz und dem Gerät auf die SINEMA RC-Verbindung. |
| | IPsec (all)<br>IPsec <Connection Name><br>OpenVPN (all)<br>OpenVPN <Connection Name> | Zugriff vom IP-Subnetz auf die Tunnelpartner, die über alle VPN-Verbindungen (all) oder über eine bestimmte VPN-Verbindung <Connection Name> zu erreichen sind. |

| von | nach | Bedeutung |
|---|---|---|
| Gerät | `vlan (1-x)`<br>`nve x` | Zugriff vom Gerät auf das IP-Subnetz. |
| | ppp0/usb | Zugriff vom Gerät auf die Mobilfunk-Schnittstelle des Geräts. |
| | SINEMA RC | Zugriff vom Gerät auf die SINEMA RC-Verbindung |
| | IPsec (all)<br>IPsec <Connection Name><br>OpenVPN (all)<br>OpenVPN <Connection Name> | Zugriff vom Gerät auf die Tunnelpartner, die über alle VPN-Verbindungen (all) oder über eine bestimmte VPN-Verbindung <Connection Name> zu erreichen sind. |
| SINEMA RC | vlan x | Zugriff vom SINEMA RC-Server auf das V(X)LAN-Segment. |
| | ppp0/usb | Zugriff vom SINEMA RC-Server auf die Mobilfunk-Schnittstelle des Geräts. |
| | Gerät | Zugriff vom SINEMA RC-Server auf das Gerät. |
| | IPsec (all)<br>IPsec <Connection Name><br>OpenVPN (all)<br>OpenVPN <Connection Name> | Zugriff vom SINEMA RC-Server auf die Tunnelpartner, die über alle VPN-Verbindungen (all) oder über eine bestimmte VPN-Verbindung <Connection Name> zu erreichen sind. |
| IPsec (all)<br>IPsec <Connection Name><br>OpenVPN (all)<br>OpenVPN <Connection Name> | `vlan (1-x)`<br>`nve x` | Zugriff über Tunnelpartner auf das V(X)LAN-Segment. |
| | ppp0/usb | Zugriff über Tunnelpartner auf die Mobilfunk-Schnittstelle des Geräts. |
| | Gerät | Zugriff über Tunnelpartner auf das Gerät. |
| | SINEMA RC | Zugriff über Tunnelpartner auf die SINEMA RC-Verbindung. |
| ppp0/usb | `vlan (1-x)`<br>`nve x` | Zugriff von der Mobilfunk-Schnittstelle auf das V(X)LAN-Segment. |
| | Gerät | Zugriff von der Mobilfunk-Schnittstelle auf das Gerät. |
| | SINEMA RC | Zugriff von der Mobilfunk-Schnittstelle auf die SINEMA RC-Verbindung. |
| | IPsec (all)<br>IPsec <Connection Name><br>OpenVPN (all)<br>OpenVPN <Connection Name> | Zugriff von der Mobilfunk-Schnittstelle auf die Tunnelpartner, die über alle VPN-Verbindungen (all) oder über eine bestimmte VPN-Verbindung <Connection Name> zu erreichen sind. |

#### 4.6.3.1 Firewall-Regeln

Firewall-Regeln sind automatisch erstellte, vordefinierte oder eigens konfigurierte IP-Regeln für den Datenverkehr.

### Automatische Firewall-Regeln

Bei den folgenden Funktionen gibt es die Einstellung "Auto Firewall-Regeln":

- System > SINEMA RC (Seite 158)
- Security > IPsec VPN> Phase 2 (Seite 431)
- Security > OpenVPN Client> Verbindungen (Seite 435)

Die automatisch erstellten Firewall-Regeln erlauben Pakete in folgender Richtung:

| Von | Nach | SINEMA RC | IPsec VPN | OpenVPN |
|---|---|---|---|---|
| Intern | Extern | ✓ | ✓ | ✓ |
| Extern | Intern | ✓ | ✓ | ✓ |
| Gerät | Extern | -- | -- | ✓ |
| Extern | Gerät | Vordefinierte IPv4-Regeln<br>Beim Anlegen der Verbindung werden folgende IPv4-Dienste aktiviert: | | |
| | | HTTP<br>HTTPS<br>SSH<br>Ping | Ping | Ping |

### Vordefinierte Firewall-Regeln

Die Firewall enthält vordefinierte IPv4-Regeln, die bestimmte IPv4-Dienste auf dem Gerät freischalten.

Unter "Security > Firewall > Vordefinierte IPv4-Regeln (Seite 407)" legen Sie fest, über welche Schnittstelle zugegriffen wird.

Folgende Möglichkeiten gibt es:

- VLANx: VLANs mit konfiguriertem Subnetz
- WAN-Schnittstelle des Geräts: pppx, usb0
- VPN-Verbindung: SINEMA RC, IPsec und OpenVPN

#### Werkseinstellung

Die Firewall ist standardmäßig aktiviert. Im Auslieferungszustand (Werkseinstellung) ist die Konfiguration der vordefinierten IPv4-Regeln wie folgt:

| Dienst | Zugriff | |
|---|---|---|
| | Lokaler Zugriff (vlan1) auf das Gerät [1)] | Externer Zugriff auf das Gerät<br>M87x, M81x, MUM85x: ppp0/ usb0<br>S615: vlan2 |
| Cloud Connector | - | - |
| DHCP | ✓ | ✓ (nur bei S615) |
| DNS | ✓ | -- |
| HTTP | ✓ | -- |

| Dienst | Zugriff | |
|---|---|---|
| | **Lokaler Zugriff (vlan1) auf das Gerät** [1] | **Externer Zugriff auf das Gerät**<br>**M87x, M81x, MUM85x: ppp0/ usb0**<br>**S615: vlan2** |
| HTTPS | ✓ | -- |
| IPsec VPN | -- | ✓ |
| Ping | ✓ | -- |
| SMS Relay (nur bei M87x / MUM856) | ✓ | -- |
| TCP Event | -- | -- |
| SNMP | ✓ | -- |
| SSH | ✓ | -- |
| Systemzeit | -- | -- |
| Telnet | ✓ | -- |
| VRRP | -- | -- |
| VXLAN (nur bei MUM85x) | -- | -- |

[1] Bei SCALANCE M826 und M804PB ist im Auslieferungszustand nur vlan1 verfügbar.

## 4.6.4 NAT

NAT (Network Address Translation) ist eine Methode IP-Adressen in Datenpaketen umzuschreiben. Damit können zwei verschiedene Netze (intern und extern) miteinander verbunden werden.

Man unterscheidet zwischen Source-NAT, bei dem die Quell-IP-Adresse umgeschrieben wird und Destination-NAT, bei dem die Ziel-IP-Adresse umgeschrieben wird.

Weitere Informationen zu NAT-Szenarien, die mit dem Gerät realisiert werden können, finden Sie unter folgender Adresse: (https://support.industry.siemens.com/cs/de/de/view/109744660)

### IP-Masquerading

IP-Masquerading ist ein vereinfachtes Source-NAT. Dabei wird bei jedem ausgehenden Datenpaket, das über diese Schnittstelle gesendet wird, die Quell-IP-Adresse durch die IP-Adresse der Schnittstelle ersetzt. Das angepasste Datenpaket wird an die Ziel-IP-Adresse gesendet. Für den Ziel-Host sieht es so aus, als kämen die Anfragen immer von dem gleichen Absender. Die internen Teilnehmer sind aus dem externen Netz nicht direkt erreichbar. Mithilfe von NAPT lassen sich die Dienste der internen Teilnehmer über die externe IP-Adresse des Geräts erreichbar machen.

IP-Masquerading kann benutzt werden, wenn die internen IP-Adressen extern nicht weitergeleitet werden können oder sollen, z. B. weil die interne Netzstruktur verborgen werden soll.

Masquerading konfigurieren Sie unter "Layer 3" > "NAT" > "IP-Masquerading (Seite 368)".

### NAPT

NAPT (Network Address and Port Translation) ist eine Form des Destination-NAT und wird oft auch als Portweiterleitung (Port Forwarding) bezeichnet. Damit lassen sich Dienste der internen Teilnehmer von außen erreichbar machen, die durch IP-Masquerading oder Source-NAT versteckt sind.

Umgesetzt werden eingehende Datenpakete, die vom externen Netz kommen und an eine externe IP-Adresse des Geräts (Ziel-IP-Adresse) gerichtet sind. Die Ziel-IP-Adresse wird mit der IP-Adresse des internen Teilnehmers ersetzt. Zusätzlich zur Adressumsetzung ist auch eine Port-Umsetzung möglich.

Es gibt folgende Möglichkeiten der Port-Umsetzung:

| von | zu | Verhalten |
|---|---|---|
| einem einzigen Port | dem gleichen Port | Wenn die Ports gleich sind, werden die Telegramme ohne Port-Umsetzung weitergeleitet. |
| einem einzigen Port | einem einzigen Port | Die Telegramme werden auf den Port umgesetzt. |
| einem Port-Bereich | einem einzigen Port | Die Telegramme aus dem Port-Bereich werden auf den gleichen Port umgesetzt (n:1). |
| einem Port-Bereich | dem gleichen Port-Bereich | Wenn die Port-Bereiche gleich sind, werden die Telegramme ohne Port-Umsetzung weitergeleitet. |

Port Forwarding kann benutzt werden, um externen Teilnehmern den Zugriff auf bestimmte Dienste des internen Netzes zu ermöglichen, z. B. FTP, HTTP.

NAPT konfigurieren Sie unter "Layer 3" > "NAT" > "NAPT (Seite 368)".

### Source-NAT

Wie beim Masquerading wird beim Source-NAT die Quelladresse umgeschrieben. Zusätzlich können die ausgehenden Datenpakete beschränkt werden. Dazu gehören Beschränkungen auf bestimme IP-Adressen oder IP-Adressbereiche und Beschränkungen auf bestimmte Schnittstellen.

Source-NAT kann benutzt werden, wenn die internen IP-Adressen extern nicht weitergeleitet werden können oder sollen, z. B. weil ein privater IP-Adressbereich wie 192.168.x.x benutzt wird.

Source-NAT konfigurieren Sie unter "Layer 3" > "NAT" > "Source NAT (Seite 370)".

### NETMAP

Mit NETMAP ist es möglich, komplette Subnetze auf ein anderes Subnetz umzusetzen. Bei dieser Umsetzung wird der Subnetzanteil der IP-Adresse geändert und der Hostanteil bleibt bestehen. Für die Umsetzung wird bei NETMAP nur eine Regel benötigt. NETMAP kann sowohl die Quell-IP-Adresse als auch die Ziel-IP-Adresse umsetzen. Um die Umsetzung mit Destination-NAT und Source-NAT durchzuführen, wären viele Regeln notwendig. NETMAP kann auch auf VPN-Verbindungen angewendet werden.

NETMAP konfigurieren Sie unter "Layer 3" > "NAT" > "NETMAP (Seite 372)".

## 4.6.5 NAT und Firewall

Firewall und NAT-Router unterstützen den Mechanismus "Stateful Inspection". Wenn der IP-Datenverkehr von intern nach extern freigegeben ist, können interne Teilnehmer eine Kommunikationsverbindung in das externe Netz initiieren.

Die Antworttelegramme aus dem externen Netz können den NAT-Router und die Firewall passieren, ohne dass deren Adressen in der Firewall-Regel und der NAT-Adressumsetzung zusätzlich aufgenommen werden müssen. Telegramme, die keine Antwort auf eine Anfrage aus dem internen Netz sind, werden ohne zutreffende Firewallregel verworfen.

### NAT-Umsetzung und Firewall-Regeln

**Beispiel für NAT-Umsetzungen**

| NAT-Regel | | | | | | | |
|---|---|---|---|---|---|---|---|
| | **Typ** | **Quell-Schnitt-stelle** | **Ziel-Schnitt-stelle** | **Quell-IP-Sub-netz** | **Quell-IP-Subnetzum-setzung** | **Ziel-IP-Sub-netz** | **Ziel-IP-Subnetzumset-zung** |
| ① | Quelle | vlan1 (intern) | vlan2 (extern) | 192.168.1.0/24 | 10.100.1.0/24 | 10.10.10.0/24 | - |
| | Die Regel gilt für Pakete, die von vlan1 (intern) nach vlan2 (extern) gesendet werden. Bei den Paketen, die an vlan1 ankommen, wird geprüft, ob die Regel zutrifft.<br>Wenn die Quell-IP-Adresse im Subnetz des Absenders (Quell-IP-Subnetz) und die Ziel-IP-Adresse im Subnetz des Empfängers (Quell-IP-Subnetz) liegen, wird die Quell-IP-Adresse durch die passende IP-Adresse aus dem "Quell-IP-Subnetzumsetzung" ersetzt. Der Subnetzanteil der Quell-IP-Adresse wird geändert und der Hostanteil bleibt unverändert.<br>Ein Paket z. B. mit der Quell-IP-Adresse 192.168.1.102 wird zu 10.100.1.102 geändert. Für die Geräte, die an vlan2 angeschlossen sind, sieht es so aus, als ob die Pakete aus dem IP-Subnetz 10.100.1.0/24 gesendet werden. Damit lassen sich z. B. Überschneidungen von IP-Subnetzen auflösen. Die Regel ist nur für die Senderichtung festzulegen. Die Rückübersetzung erfolgt implizit. Wenn die Regel nicht zutrifft, werden die Pakete ohne Umsetzung weitergeleitet. | | | | | | |
| ② | Ziel | vlan2 (extern) | vlan1 (intern) | 10.10.10.0/24 | - | 10.100.1.0/24 | 192.168.1.0/24 |
| | Die Regel gilt für Pakete, die von vlan2 (extern) nach vlan1 (intern) gesendet werden. Bei den Paketen, die an vlan2 ankommen, wird geprüft, ob die Regel zutrifft.<br>Wenn die Quell-IP-Adresse im Subnetz des Absenders Quell-IP-Subnetz) und die Ziel-IP-Adresse im Subnetz des Empfängers (Quell-IP-Subnetz) liegen, wird die Quell-IP-Adresse durch die passende IP-Adresse aus dem "Ziel-IP-Subnetzumsetzung" ersetzt.<br>Ein Paket z. B. mit der Quell-IP-Adresse 10.10.10.102 wird zu 192.168.1.102 geändert. Die an vlan1 angeschlossenen Geräte können mit den Geräten kommunizieren, die an vlan2 angeschlossen sind. Vorausgesetzt, die entsprechende Firewallregel ist gesetzt.<br>Die an vlan2 angeschlossenen Geräte müssen die am vlan1 angeschlossenen Geräte mit der virtuellen IP-Adresse aus dem Subnetz 10.100.1.0 adressieren. | | | | | | |

**Firewall-Regeln für die NAT-Regeln ① und ②**

**Beispiel 1:**

Diese IP-Regeln erlauben für die angegebene Richtung den IP-Datenverkehr für alle Geräte.

| NAT-Regel | IP-Regeln | | | | | | Beschreibung |
|---|---|---|---|---|---|---|---|
| | Aktion | Von | Nach | Quelle (Bereich) | Ziel (Bereich) | Dienst | |
| ① | Accept | vlan1 (intern) | vlan2 (extern) | 192.168.1.0/24 (Quell-IP-Subnetz) | 10.10.10.0/24 (Ziel-IP-Subnetz) | all | Alle Pakete, die von vlan1 (intern) nach vlan2 (extern) gesendet werden, werden durchgelassen.<br>Diese IP-Paketfilter-Regel gilt für die an vlan1 angeschlossenen Geräte sind. |
| ② | Accept | vlan2 (extern) | vlan1 (intern) | 192.168.1.0/24 (Ziel-IP-Subnetzumsetzung) | 10.100.1.0/24 (Ziel-IP-Subnetz) | all | Alle Pakete, die von vlan2 (extern) nach vlan1 (intern) gesendet werden, werden durchgelassen. |

**Beispiel 2:**

Diese IP-Regeln schränken den IP-Datenverkehr auf ein bestimmtes Gerät ein.

| NAT-Regel | IP-Regeln | | | | | | Beschreibung |
|---|---|---|---|---|---|---|---|
| | Aktion | Von | Nach | Quelle (Bereich) | Ziel (Bereich) | Dienst | |
| ① | Accept | vlan1 (intern) | vlan2 (extern) | 192.168.1.20/32 (Quell-IP-Subnetz) | 10.10.10.0/24 (Ziel-IP-Subnetz) | all | Nur die Pakete, die von der IP-Adresse 192.168.1.20 nach vlan2 (extern) gesendet werden, werden durchgelassen. |
| ② | Accept | vlan2 (extern) | vlan1 (intern) | 192.168.1.20/32 (Ziel-IP-Subnetzumsetzung) | 10.100.1.0/24 (Ziel-IP-Subnetz) | all | Nur die Pakete, die von vlan2 (extern) an die IP-Adresse 192.168.1.20 gesendet werden, werden durchgelassen. |

## 4.6.6 Zertifikate

### Zertifikatstypen

Das Gerät verwendet verschiedene Zertifikate, um die verschiedenen Teilnehmer zu authentifizieren.

| Zertifikat | | Wird verwendet in ... |
|---|---|---|
| CA-Zertifikat | Das CA-Zertifikat ist ein durch eine Zertifizierungsstelle, die so genannte "Certificate Authority", ausgestelltes Zertifikat, von denen die Server-, Geräte- und Gegenstellenzertifikate abgeleitet werden. Damit ein Zertifikat abgeleitet werden kann, besitzt das CA-Zertifikat einen privaten Schlüssel, der durch die Zertifizierungsstelle signiert wurde.<br>Der Schlüsselaustausch zwischen dem Gerät und dem VPN-Gateway der Gegenstelle erfolgt automatisch beim Aufbau der Verbindung. Es ist kein manueller Austausch von Schlüsseldateien notwendig. | IPsec VPN (Seite 420) |
| Serverzertifikat | Serverzertifikate werden zum Aufbau einer gesicherten Kommunikation (z. B. HTTPS, VPN ...) zwischen Gerät und einem weiteren Netzwerkteilnehmer benötigt. Bei dem Serverzertifikat handelt es sich um ein verschlüsseltes SSL-Zertifikat. Das Serverzertifikat wird von der ältesten gültigen CA abgeleitet, auch wenn dieses "außer Dienst" ist. Entscheidend ist das Gültigkeitsdatum der CA. | SINEMA RC (Seite 295) |
| Gerätezertifikat | Zertifikate mit dem privaten Schlüssel (Key file), mit denen sich das Gerät ausweist. | IPsec VPN (Seite 420) |
| Gegenstellenzertifikat | Zertifikate, mit denen sich das VPN-Gateway der Gegenstelle bei dem Gerät authentifiziert. | IPsec VPN (Seite 420) |

### Dateitypen

| Dateityp | Beschreibung |
|---|---|
| *.crt | Datei, die das Zertifikat enthält. |
| *.p12 | Bei der PKCS12-Zertifikatsdatei wird der private Schlüssel mit dem zugehörigen Zertifikat passwortgeschützt gespeichert.<br>Die CA erstellt für beide Gegenstellen einer VPN-Verbindung je eine Zertifikatsdatei (PKCS12) mit der Dateiendung ".p12". Diese Zertifikatsdatei enthält den öffentlichen und privaten Schlüssel der eigenen Station, das signierte Zertifikat der CA und den öffentlichen Schlüssel der CA. |
| *.pem | Zertifikat und Schlüssel als Base64-kodierten ASCII-Text. |

## 4.6.7 VPN

Das Gerät unterstützt folgende VPN-Systeme

- IPsec VPN
- OpenVPN

#### 4.6.7.1 IPsec VPN

Die IPsec-Verbindungen konfigurieren Sie unter "Security" > "IPsec VPN (Seite 420)"

Bei IPsec VPN werden die Telegramme im Tunnel-Modus übertragen. Damit das Gerät einen VPN-Tunnel aufbauen kann, muss das entfernte Netz über ein VPN-Gateway als Gegenstation verfügen.

Für die VPN-Verbindungen unterscheidet das Gerät zwei Modi:

- **Roadwarrior-Modus**
  In diesem Modus wird entweder die Adresse der Gegenstelle fest vorgegeben oder ein IP-Bereich eingetragen, aus dem Verbindungen entgegengenommen werden. Die erreichbaren Remote-Subnetze lernt das Gerät von der Gegenstelle.
- **Standard-Modus**
  In diesem Modus ist die Adresse der Gegenstelle oder das Remote-Subnetz fest eingetragen. Das Gerät kann entweder als VPN-Client die VPN-Verbindung aktiv aufbauen, oder passiv auf den Verbindungsaufbau durch die Gegenstelle warten.

### Das IPsec-Verfahren

Das Gerät verwendet für den VPN-Tunnel das IPsec-Verfahren im Tunnelmodus. Dabei werden die zu übertragenden Telegramme vollkommen verschlüsselt und mit einem neuen Header versehen, bevor sie zum VPN-Gateway der Gegenstelle gesendet werden. Von der Gegenstelle werden die empfangenen Telegramme entschlüsselt und an den Empfänger weitergeleitet.

Zum Absichern verwendet das IPsec-Verfahren verschiedene Protokolle:

- Der IP-Authentication-Header (**AH**) wickelt die Authentifizierung und Identifizierung der Quelle ab.
- Die Encapsulation Security Payload (**ESP**) verschlüsselt die Daten.
- Die Security Association (**SA**) enthält die Festlegungen, die zwischen den Partner ausgehandelt wurden, z. B. über die Lebensdauer des Schlüssels, den Verschlüsselungsalgorithmus, den Zeitraum für eine neue Authentifizierung etc.
- Das Internet Key Exchange (**IKE**) ist ein Schlüsselaustauschverfahren. Der Schlüsselaustausch erfolgt in zwei Phasen:
  - Phase 1
    In dieser Phase sind noch keine Sicherheitsdienste wie Verschlüsselung, Authentifizierung und Integritätsprüfung verfügbar, da die notwendigen Schlüssel und die IPsec-SA noch nicht erstellt wurden. Phase 1 dient zum Aufbau eines sicheren VPN-Tunnels für Phase 2. Dafür verhandeln die Kommunikationspartner eine ISAKMP Security Association (ISAKMP-SA), welche die notwendigen Sicherheitsdienste (verwendete Algorithmen, Authentifizierungsmethoden) definiert. Damit werden die weiteren Nachrichten und Phase 2 abgesichert.
  - Phase 2
    Phase 2 dient zur Aushandlung der benötigten IPsec-SA. Ähnlich wie bei Phase 1 wird durch das wechselseitige Anbieten eine Einigung über die Authentifizierungsmethoden, die Algorithmen und die Verschlüsselungsverfahren getroffen, um die IP-Pakete mit IPsec-AH und IPsec-ESP zu schützen.
    Geschützt wird der Nachrichtenaustausch über die ISAKMP-SA, die in Phase 1 vereinbart wurde. Durch die in Phase 1 ausgehandelte ISAKMP-SA ist die Identität der Teilnehmer sowie das Verfahren zur Integritätsprüfung bereits gegeben.

### Authentifizierungsverfahren

- CA-Zertifikat, Geräte- und Gegenstellenzertifikat (digitale Signaturen)
  Die Verwendung von Zertifikaten ist ein asymmetrisches Kryptosystem, wobei jeder Teilnehmer (Gerät) über ein Schlüsselpaar verfügt. Jeder Teilnehmer besitzt einen geheimen, privaten Schlüssel und einen öffentlichen Schlüssel der Gegenstelle. Der private Schlüssel ermöglicht es, sich zu authentifizieren und digitale Signaturen zu erzeugen.
- Preshared Key
  Die Verwendung eines Preshared Key ist ein symmetrisches Kryptosystem. Jeder Teilnehmer besitzt nur einen geheimen Schlüssel für die Ent- und Verschlüsselung von Datenpaketen. Die Authentifizierung erfolgt über ein gemeinsames Passwort.

### Lokale-ID und Remote-ID

Die Lokale-ID und die Remote-ID werden vom IPsec genutzt, um beim Aufbau der VPN-Verbindung die Gegenstellen (VPN-Endpunkt) eindeutig zu identifizieren.

### Verschlüsselungsverfahren

Folgende Verschlüsselungsverfahren werden unterstützt. Die Auswahl ist abhängig von der Phase und vom Schlüsselaustauschverfahren (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 |
| 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: wird unterstützt

-: wird nicht unterstützt

### Default-Chiffre

Beim Verbindungsaufbau kann eine vorgegebene Liste an den VPN-Verbindungspartner übermittelt werden. In der Liste sind Kombinationen aus den drei Algorithmen (Encryption, Authentication, Key Derivation) enthalten. Um eine VPN-Verbindung aufzubauen, muss der VPN-Verbindungspartner mindestens eine dieser Kombinationen unterstützen. Die Kombinationen sind abhängig von der Phase und vom Schlüsselaustauschverfahren (IKE).

| Kombination | | | Phase 1 | | Phase 2 | |
|---|---|---|---|---|---|---|
| **Verschlüsselung** | **Authentifizierung** | **Schlüsselableitung** | **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: Kombination ist Teil der Default-Chiffre

-: Kombination ist nicht Teil der Default-Chiffre

none: Für die Phase 2 werden keine separaten Schlüssel ausgetauscht. Damit ist Perfect Forward Secrecy (PFS) deaktiviert.

### Anforderungen an die VPN-Gegenstelle

Die VPN-Gegenstelle muss IPsec mit folgender Konfiguration unterstützen, um erfolgreich eine IPsec-Verbindung aufzubauen:

- Authentifizierung über Gegenstellenzertifikate, CA-Zertifikate oder Pre-Shared Key
- IKEv1 oder IKEv2
- Unterstützung von mindestens einer der folgenden DH-Gruppen: Diffie-Hellman Gruppe 1, 2, 5 und 14 - 18
- 3DES- oder AES-Verschlüsselung
- MD5, SHA1, SHA256, SHA384 oder SHA512
- Tunnel-Modus

Wenn sich die VPN-Gegenstelle hinter einem NAT-Router befindet, dann muss die Gegenstelle NAT-T unterstützen. Oder aber der NAT-Router muss das IPsec-Protokoll kennen (IPsec/VPN Passthrough).

### NAT-Traversal (NAT-T)

Eventuell befindet sich zwischen dem Gerät und dem VPN-Gateway des entfernten Netzes ein NAT-Router. Nicht alle NAT-Router lassen IPsec-Telegramme passieren. Daher kann es erforderlich sein, die IPsec-Telegramme in UDP-Pakete einzukapseln, um den NAT-Router passieren zu können.

### Dead Peer Detection

Voraussetzung ist, dass die VPN-Gegenstelle DPD unterstützt. DPD prüft, ob die Verbindung noch störungsfrei arbeitet oder ob es eine Unterbrechung auf der Strecke gab. Ohne DPD muss je nach Konfiguration bis zum Ablauf der SA-Lebensdauer gewartet oder die Verbindung manuell neu initiiert werden. Um zu prüfen, ob die IPsec-Verbindung noch störungsfrei arbeitet, sendet das Gerät selber DPD-Anfragen zur VPN-Gegenstelle. Wenn die VPN-Gegenstelle nicht antwortet, wird nach Ablauf einer bestimmten Zeitspanne die Verbindung zur VPN-Gegenstelle für ungültig erklärt. Die Einstellungen für DPD konfigurieren Sie bei der Phase 1.

## 4.6.7.2 OpenVPN

Mit OpenVPN lassen sich virtuelle private Netzwerke (VPN) aufbauen. Das Gerät kann als OpenVPN-Client eine VPN-Verbindung zu einem entfernten Netzwerk aufbauen.

Den OpenVPN-Client konfigurieren Sie unter "Security" > "OpenVPN-Client (Seite 434)".

Die VPN-Verbindung wird über virtuelle Gerätetreiber hergestellt, dem TAP- und TUN-Device. Dabei werden virtuelle Netzwerkschnittstellen angelegt, die wie eine physische Schnittstelle des Geräts wirken und den Endpunkt des VPN-Tunnels darstellen.

Das Gerät unterstützt Folgendes:

- TUN-Device: Routing-Modus
  Die LAN-Schnittstelle und die virtuelle Netzwerkschnittstelle befinden sich in verschiedenen IP-Subnetzen. Der virtuellen Tunnelschnittstelle wird vom OpenVPN-Server eine virtuelle IP-Adresse aus einem erdachten Subnetz zugewiesen. Die IP-Pakete (Layer 3) werden zwischen der virtuellen Tunnelschnittstelle und der LAN-Schnittstelle geroutet.

### Authentifizierung

Für die Authentifizierung des OpenVPN-Clients am OpenVPN-Server gibt es folgende Möglichkeiten:

- Zertifikate: CA-Zertifikat und Gerätezertifikat
  Die Verwendung von Zertifikaten ist ein asymmetrisches Kryptosystem. Jeder Teilnehmer (Gerät) besitzt einen geheimen, privaten Schlüssel und einen öffentlichen Schlüssel der Gegenstelle. Der private Schlüssel ermöglicht es, sich zu authentifizieren und digitale Signaturen zu erzeugen.
- Benutzername/Passwort
  Der Zugang wird über einen Benutzernamen und ein Passwort beschränkt.
- Zertifikate und Benutzername/Passwort
  Wenn beide Authentifizierungsverfahren erfolgreich sind, wird die VPN-Verbindung aufgebaut.

### Verschlüsselungsverfahren

Das Gerät unterstützt dabei die folgenden Verfahren:

- BF CBC
- AES128 CBC
- AES192 CBC

- AES256 CBC
- DES EDE3

### 4.6.7.3 VPN-Verbindungsaufbau

Das Gerät unterstützt folgende Möglichkeiten, um eine VPN-Verbindung aufzubauen.

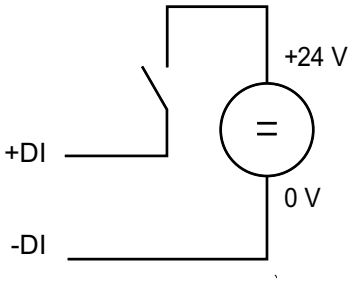
- OpenVPN: Security > OpenVPN > Verbindungen (Seite 435)
- IPsec VPN: Security > IPsec VPN > Verbindungen (Seite 423)
- SINEMA RC: System > SINEMA RC (Seite 295)

| Möglichkeiten | Verwendung | | | Beschreibung |
|---|---|---|---|---|
| | OpenVPN | IPsec VPN | SINEMA RC [1] | |
| Starten | x | x | - | Das Gerät ist "aktiv", d. h. es wird versucht, zu einer Gegenstelle eine Verbindung herzustellen. Die Adressierung der Gegenstelle erfolgt über deren projektierte WAN-IP-Adresse oder den projektierten FQDN. |
| Warten | - | x | - | Das Gerät ist "passiv", d. h. es wird gewartet, bis der Verbindungsaufbau von der Gegenstelle initiiert wird. |
| Auf Anforderung | - | x | - | Das Gerät versucht bei Bedarf zu einer Gegenstelle eine Verbindung herzustellen. Die Annahme von Anfragen zum VPN-Verbindungsaufbau ist ebenfalls möglich.<br>Für die projektierten lokalen und entfernten Subnetze wird in der Routing-Tabelle ein Eintrag angelegt. Wenn ein Teilnehmer aus einem der entsprechenden Netze versucht Datenpakete über den VPN-Tunnel zu senden, wird die VPN-Verbindung aufgebaut. Der einstellbare Timeout bewirkt, dass nach dieser Zeit ohne weitere Datenpakete der VPN-Tunnel wieder abgebaut wird. |
| Bei DI starten | x | x | x | Der Verbindungsaufbau wird über den digitalen Eingang (DI) gesteuert |
| Bei DI warten | - | x | - | |
| Digitaler Eingang & Weck-SMS | - | - | x | Der Verbindungsaufbau wird über den digitalen Eingang (DI) oder SMS gesteuert. |
| Weck-SMS | - | - | x | Der Verbindungsaufbau wird über SMS gesteuert |
| Bei SMS starten | x | x | - | |
| Auf SMS warten | - | x | - | |
| Auto | - | - | x | Das Gerät übernimmt die Einstellungen des SINEMA RC Server. Die Einstellungen auf dem SINEMA RC Server konfigurieren Sie unter "Fernverbindungen > Geräte". Weiterführende Informationen hierzu finden Sie in der Betriebsanleitung "SINEMA RC Server". |
| Permanent | - | - | x | Das Gerät baut eine VPN-Verbindung zum SINEMA RC-Server. Der VPN-Tunnel wird permanent aufrechterhalten. |

[1] KEY-PLUG SINEMA REMOTE CONNECT notwendig

## Digitaler Eingang (DI)

Der Aufbau des VPN-Tunnels kann auch über den digitalen Eingang gesteuert werden, z. B. über einen Taster. Wenn der Taster schließt, liegt am digitalen Eingang Spannung an und die LED vom digitalen Eingang leuchtet auf. Die aufleuchtende LED signalisiert, dass das Signal 1 (TRUE / HIGH) anliegt. Das Signal 1 löst auf dem Gerät ein Ereignis aus, mit dem der Aufbau des VPN-Tunnels gesteuert wird. Informationen zum Anschließen und zur maximalen Strombelastbarkeit finden Sie in der Betriebsanleitung der Geräte.




**Voraussetzung**

- Unter "System > Ereignisse > Konfiguration (Seite 210)" ist beim Ereignis "Digitaler Eingang" "VPN-Tunnel" aktiviert.
  Wenn diese Einstellung nicht aktiviert ist, wird das Ereignis nicht an die VPN-Verbindung weitergegeben.

**Möglichkeiten**

Das Gerät unterstützt folgende Möglichkeiten zur Steuerung des VPN-Tunnels über den digitalen Eingang:

- Bei DI starten
  Wenn das Ereignis "Digitaler Eingang" eintritt, wird das Gerät "aktiv". Das Gerät versucht, zu einer Gegenstelle eine VPN-Verbindung (OpenVPN, IPsec, SINEMA RC) herzustellen. Beim SCALANCE M804PB wird der integrierte TIA Portal Cloud Connector gestartet.
- Bei DI warten
  Wenn das Ereignis "Digitaler Eingang" eintritt, ist das Gerät "passiv". Das Gerät wartet, bis der Verbindungsaufbau von der Gegenstelle (OpenVPN, IPsec) initiiert wird.
- Digitaler Eingang & Weck-SMS (nur bei M87x / MUM856)
  Wenn das Ereignis "Digital In" eintritt oder das Gerät eine Wake-up SMS erhält, wird das Gerät "aktiv". Das Gerät versucht, zum SINEMA RC-Server eine VPN-Verbindung herzustellen.

## SMS (nur bei M87x / MUM85x)

**Voraussetzung**

- Unter "System > SMS > Befehl-SMS (Seite 273)" legen Sie fest, von wem eine Befehl-SMS der Klasse "System" akzeptiert wird.
- Unter "System > SMS > Ereignis-SMS" ist die Funktion aktiviert und die Telefonnummer eines Empfängers konfiguriert.
- Wenn diese Einstellung nicht aktiviert ist, wird das Ereignis nicht an die VPN-Verbindung weitergegeben.

**Möglichkeiten**

Das Gerät unterstützt folgende Möglichkeiten zur Steuerung des VPN-Tunnels über eine SMS:

- Bei SMS starten
  Wenn das Gerät eine Befehl-SMS erhält, wird das Gerät "aktiv". Die Befehl-SMS enthält den Namen der VPN-Verbindung (OpenVPN, IPsec). Das Gerät versucht zu der Gegenstelle eine Verbindung aufzubauen, die in der VPN-Verbindung angegeben ist.
  Format der SMS:
  Aufbau der VPN-Verbindung:
  - OpenVPN: SYS OVPN UP <Name der OpenVPN-Verbindung>, siehe Befehl-SMS (Seite 451).
    Wenn Sie bei <Name der OpenVPN-Verbindung> ein '*' eingeben, werden die OpenVPN-Verbindungen aufgebaut, die bei "Betrieb" "Bei SMS starten" eingestellt haben.
  - IPsec VPN: SYS IPSEC UP <Name der IPsec VPN-Verbindung>, siehe Befehl-SMS (Seite 451).
    Wenn Sie bei <Name der IPsec VPN-Verbindung> ein '*' eingeben, werden die IPsec VPN-Verbindungen aufgebaut, die bei "Betrieb" "Bei SMS starten" eingestellt haben.

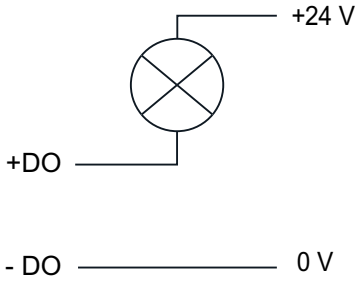
  Abbau der VPN-Verbindung:
  - OpenVPN: SYS OVPN DOWN <Name der OpenVPN-Verbindung>, siehe Befehl-SMS (Seite 451).
    Wenn Sie bei <Name der OpenVPN-Verbindung> ein '*' eingeben, werden die OpenVPN-Verbindungen beendet, die bei "Betrieb" "Bei SMS starten" eingestellt haben.
  - IPsec VPN: SYS IPSEC DOWN <Name der IPsec VPN-Verbindung>, siehe Befehl-SMS (Seite 451).
    Wenn Sie bei <Name der IPsec VPN-Verbindung> ein '*' eingeben, werden die IPsec VPN-Verbindungen beendet, die bei "Betrieb" "Bei SMS starten" eingestellt haben.
- Auf SMS warten
  Wenn das Gerät eine Befehl-SMS erhält, ist das Gerät "passiv". Die Befehl-SMS enthält den Namen der IPsec VPN-Verbindung. Das Gerät wartet, bis der Verbindungsaufbau von der Gegenstelle initiiert wird, die in derIPsec VPN-Verbindung angegeben ist.
  Format der SMS:
  Wenn Sie bei <Name der IPsec VPN-Verbindung> ein '*' eingeben, werden die IPsec VPN-Verbindungen aufgebaut, die bei "Betrieb" "Bei SMS starten" eingestellt haben.
  - IPsec VPN: SYS IPSEC UP <Name der IPsec VPN-Verbindung>, siehe Befehl-SMS (Seite 451).
    Wenn Sie bei <Name der IPsec VPN-Verbindung> ein '*' eingeben, werden die IPsec VPN-Verbindungen aufgebaut, die bei "Betrieb" "Bei SMS starten" eingestellt haben.
  - IPsec VPN: SYS IPSEC DOWN <Name der IPsec VPN-Verbindung>, siehe Befehl-SMS (Seite 451).
    Wenn Sie bei <Name der IPsec-VPN-Verbindung> ein '*' eingeben, werden die IPsec VPN-Verbindungen beendet, die bei "Betrieb" "Auf SMS warten" eingestellt haben.

- Digitaler Eingang & Weck-SMS
  Die Einstellungen des SINEMA RC-Servers werden ignoriert. Wenn das Ereignis "Digital In" eintritt oder das Gerät eine Weck-SMS erhält. Das Gerät versucht die VPN-Verbindung zum SINEMA RC-Server aufzubauen.
  Format der SMS: SYS SRC UP <Adresse des SINEMA RC-Servers>, siehe Befehl-SMS (Seite 451).
- Weck-SMS
  Die Einstellungen des SINEMA RC-Servers werden ignoriert. Wenn das eine Weck-SMS erhält, versucht das Gerät die VPN-Verbindung zum SINEMA RC-Server aufzubauen.
  Format der SMS:
  – SYS SRC UP <Adresse des SINEMA RC-Servers>, siehe Befehl-SMS (Seite 451).

### Benachrichtigungsmöglichkeiten

Wenn sich der Status des digitalen Eingangs oder eines VPN-Tunnels (IPsec, OpenVPN, SINEMA RC) ändert, bietet das Gerät auf der Seite "Ereignisse (Seite 210)" mehrere Möglichkeiten der Benachrichtigung.

| Art der Benachrichtigung | Digitaler Eingang | VPN Tunnel | Verhalten bei Statusänderung |
|---|---|---|---|
| E-Mail | x | x | Das Gerät sendet eine E-Mail. Die E-Mail enthält die Identifikation des absendenden Geräts, eine Beschreibung der Alarmursache in Klartext sowie einen Zeitstempel.<br>Voraussetzung:<br>• Ein SMTP-Server ist eingerichtet.<br>• Unter "System > SMTP-Client" ist die Funktion aktiviert, ein Empfänger und die IP-Adresse des SMTP-Servers konfiguriert. |
| Trap | x | x | Das Gerät löst einen SNMP-Trap aus.<br>Voraussetzung:<br>• Unter "System > Konfiguration" ist "SNMPv1 Traps" aktiviert.<br>• Unter "System > Konfiguration > Traps" ist ein Empfänger konfiguriert, an den das Gerät die SNMP-Traps sendet. |
| Log-Tabelle | x | x | Das Gerät schreibt einen Eintrag in die Ereignisprotokoll-Tabelle. Der Inhalt der Ereignisprotokoll-Tabelle wird unter "Information > Log Table" angezeigt. |
| Syslog | x | x | Das Gerät schreibt einen Eintrag auf den Syslog-Server.<br>Voraussetzung:<br>• Ein Syslog-Server ist eingerichtet.<br>• Unter "System > Syslog-Client" ist die Funktion aktiviert und die IP-Adresse des Syslog-Servers konfiguriert. |
| Fehler-LED | x | - | Die Fehler-LED am Gerät leuchtet auf. |

| Art der Benachrichtigung | Digitaler Eingang | VPN Tunnel | Verhalten bei Statusänderung |
|---|---|---|---|
| Digitaler Eingang | x | x | Steuert den digitalen Ausgang an oder signalisiert die Zustandsänderung mit der LED "DO".<br>An dem digitalen Ausgang kann ein Verbraucher angeschlossen werden. Informationen zum Anschließen finden Sie in der Betriebsanleitung der Geräte. Der Verbraucher signalisiert eine Statusänderung.<br><br><br>**Hinweis**<br>Über CLI und über SNMP können Sie den digitalen Ausgang direkt ansteuern. Im WBM und CLI können Sie bei den "Events" die Verwendung des digitalen Ausgangs projektieren. Steuern Sie den digitalen Ausgang nicht direkt an, wenn Sie diesen im WBM und CLI verwenden. |
| SMS (nur bei M87x, MUM85x) | x | x | Das Gerät sendet eine SMS mit einem Standardtext.<br>Voraussetzung:<br>• Unter "System > SMS > Ereignis-SMS" ist die Funktion aktiviert, die Telefonnummer eines Empfängers konfiguriert. |
| | x | - | Das Gerät sendet eine SMS mit einem benutzerdefinierten Text. Den Text konfigurieren Sie unter "System > SMS > Ereignis-SMS".<br>Voraussetzung:<br>• Unter "System > SMS > Ereignis-SMS" ist die Funktion aktiviert, die Telefonnummer eines Empfängers und der Text konfiguriert.<br>• Unter "System > Ereignisse > Konfiguration" ist beim Ereignis "Digitaler Eingang" "SMS" aktiviert. |
| Status aus der MIB-Variablen auslesen | x | - | Über die private MIB-Variable snMspsDigitalInputLevel können Sie den Status des digitalen Eingangs auslesen:<br>• OID der privaten MIB-Variable snMspsDigitalInputLevel:<br>`iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).siemens(4329).industrialComProducts(20).iComPlatforms(1).simaticNet(1).snMsps(1).snMspsCommon(1).snMspsDigitalIO(39).snMspsDigitalIOObjects(1).snMspsDigitalInputTable(2).snMspsDigitalInputEntry(1).snMspsDigitalInputLevel(6)`<br>• Werte der MIB-Variable<br>– 1: Signal 0 am digitalen Eingang (DI)<br>– 2: Signal 1 am digitalen Eingang (DI) |

# 4.7 Redundanz

## 4.7.1 Spanning Tree

### Vermeidung von Schleifenbildung bei redundanten Verbindungen

Das Spanning Tree-Verfahren ermöglicht es, Netzwerkstrukturen aufzubauen, bei denen es mehrere Verbindungen zwischen zwei IE-Switches/-Bridges gibt. Ein Spanning Tree verhindert, dass es zu einer Schleifenbildung im Netz kommt, indem er genau einen Pfad zulässt und die anderen (redundanten) Ports für den Datenverkehr deaktiviert. Bei einer Unterbrechung können die Daten über einen alternativen Pfad gesendet werden. Die Funktionalität des Spanning Tree-Verfahrens basiert auf dem Austausch von Konfigurations- und Topologieänderungs-Telegrammen.

### Definition der Netztopologie durch Konfigurationstelegramme

Die Geräte tauschen zur Berechnung der Topologie untereinander Konfigurationstelegramme aus, sogenannte BPDUs (Bridge Protocol Data Units). Mit diesen Telegrammen wird die Root Bridge ausgewählt und die Netztopologie erstellt. Darüber hinaus bewirken BPDU-Telegramme den Statuswechsel der Root-Ports.

Die Root Bridge ist die Bridge, die das Spanning Tree-Verfahren für alle beteiligten Komponenten steuert.

Nachdem die Root Bridge festgelegt ist, bestimmt jedes Gerät einen Root-Port. Der Root-Port ist der Port mit den geringsten Pfadkosten zur Root Bridge.

### Verhalten bei Veränderungen der Netztopologie

Wenn Teilnehmer zu einem Netz hinzukommen oder wegfallen, kann das Auswirkungen auf die optimale Wegewahl der Datenpakete haben. Um diese Änderungen zu berücksichtigen, versendet die Root Bridge in regelmäßigen Abständen Konfigurationsmeldungen. Der Zeitabstand zwischen zwei Konfigurationsmeldungen lässt sich mit dem Parameter "Hello Time" einstellen.

### Aktualität der Konfigurationsinformation

Mit dem Parameter "Max Age" legen Sie das maximale Alter von Konfigurationsinformationen fest. Erhält eine Bridge Konfigurationsinformationen, die älter sind als in "Max Age" festgelegt, verwirft sie diese Meldung und veranlasst eine Neuberechnung der Wege.

Neue Konfigurationsinformationen werden von einer Bridge jedoch nicht sofort, sondern erst nach dem im Parameter "Forward Delay" festgelegten Zeitraum angewendet. So wird sichergestellt, dass der Betrieb entsprechend der neuen Topologie erst gestartet wird, wenn alle Bridges die notwendigen Informationen haben.

#### 4.7.1.1 RSTP

**Rapid Spanning Tree Protocol (RSTP)**

Ein Nachteil des STP ist, dass sich das Netz bei einer Störung oder einem Geräteausfall rekonfigurieren muss: Die Geräte beginnen erst im Moment der Unterbrechung, neue Pfade auszuhandeln. Dieser Vorgang dauert bis zu 30 Sekunden. Aus diesem Grunde wurde STP zum "Rapid Spanning Tree Protocol" (RSTP, IEEE 802.1w) erweitert. Dies unterscheidet sich vom STP im Wesentlichen dadurch, dass die Geräte bereits zum Zeitpunkt des ungestörten Betriebs Informationen über Alternativrouten sammeln, die sie sich dann nicht erst beschaffen müssen, wenn eine Störung eingetreten ist. Damit lässt sich die Rekonfigurationszeit für ein RSTP-gesteuertes Netz auf wenige Sekunden reduzieren.
Das wird durch folgende Funktionen erreicht:

- Edge-Ports (Endteilnehmer-Port)
  Edge-Ports sind Ports, die mit einem Endgerät verbunden sind.
  Ein Port, der als Edge-Port definiert ist, wird direkt nach einem Verbindungsaufbau aktiviert. Wenn an einem Edge-Port eine Spanning Tree-BPDU empfangen wird, verliert der Port die Rolle als Edge-Port und nimmt wieder am (R)STP teil. Wird nach Ablauf einer Zeitspanne (3x Hello-Time) kein BPDU-Telegramm mehr empfangen, geht der Port wieder in den Edge-Port-Status über.
- Punkt-zu-Punkt (direkte Kommunikation zweier benachbarter Geräte)
  Durch die direkte Kopplung der Geräte kann eine Zustandsänderung (Umkonfiguration der Ports) ohne Verzögerungen durchgeführt werden.
- Alternativ-Port (Ersatz für den Root-Port)
  Es ist ein Ersatz für den Root-Port konfiguriert. Bei einem Verbindungsverlust zur Root-Bridge kann das Gerät deshalb ohne Verzögerung durch Neukonfiguration eine Verbindung über den Alternativ-Port aufbauen.
- Reaktion auf Ereignisse
  Ein Rapid Spanning Tree reagiert auf Ereignisse, beispielsweise einen Verbindungsabbruch, ohne Verzögerung. Es müssen also keine Zeitgeber wie beim Spanning Tree abgewartet werden.
- Zähler maximale Bridge-Sprünge
  Anzahl der Bridge-Sprünge, die ein Paket maximal ausführen darf, bevor es automatisch ungültig wird.

Prinzipiell werden also beim Rapid Spanning Tree für viele Parameter Alternativen vorkonfiguriert oder bestimmte Eigenschaften der Netzstruktur berücksichtigt, um die Rekonfigurationszeit zu verkürzen.

### 4.7.2 VRRPv3

**Router-Redundanz mit VRRPv3**

Mit dem Virtual Router Redundancy Protocol v3 (VRRPv3) kann dem Ausfall eines Routers in einem Netzwerk begegnet werden. Die Version 3 von VRRP (RFC 5798) basiert auf der Version 2 (RFC 5798).

VRRP kann nur bei virtuellen IP-Schnittstellen (VLAN-Schnittstellen) eingesetzt werden.

Mehrere VRRP-Router in einem Netzsegment werden zu einer logischen Gruppe zusammengefasst, die einen virtuellen Router (VR) darstellt. Definiert wird die Gruppe über die virtuelle ID (VRID). In der Gruppe muss die VRID gleich sein. Für andere Gruppen kann die VRID nicht mehr verwendet werden.

Dem virtuellen Router werden eine virtuelle IP-Adresse und eine virtuelle MAC-Adresse zugeordnet. Einer der VRRP-Router innerhalb der Gruppe wird als Master-Router festgelegt. Der Master-Router hat die Priorität 255. Die anderen VRRP-Router sind Backup-Router. Der Master-Router weist seiner Netzwerk-Schnittstelle die virtuelle IP-Adresse und die virtuelle MAC-Adresse zu. Der Master-Router sendet in bestimmten Intervallen VRRP-Pakete (Advertisements) an die Backup-Router. Mit den VRRP-Paketen signalisiert der Master-Router, dass er noch funktionsfähig ist. Der Master-Router beantwortet auch die ARP-Anfragen.

Wenn der virtuelle Master-Router ausfällt, übernimmt ein Backup-Router die Aufgabe des Master-Routers. Der Backup-Router mit der höchsten Priorität wird zum Master-Router. Wenn die Priorität der Backup-Router gleich ist, entscheidet die größere MAC-Adresse. Der Backup-Router wird zum neuen virtuellen Master-Router.

Der neue virtuelle Master-Router übernimmt die virtuelle MAC- und IP-Adresse. Dadurch müssen keine Routing-Tabellen oder ARP-Tabellen aktualisiert werden. Die Folgen eines Geräteausfalls werden dadurch minimiert.

VRRP konfigurieren Sie unter "Layer 3 > VRRPv3 (Seite 375)".

# Konfigurieren mit dem Web Based Management 5

## 5.1 Web Based Management

### Funktionsprinzip

Das Gerät verfügt über einen integrierten HTTP-Server für das Web Based Management (WBM). Wird das Gerät über einen Webbrowser angesprochen, liefert er abhängig von den Benutzereingaben HTML-Seiten an den Admin-PC zurück.

Der Benutzer trägt seine Konfigurationsdaten in die vom Gerät gesendeten HTML-Seiten ein. Das Gerät wertet diese Informationen aus und erzeugt dynamisch Antwortseiten.

In der Werkseinstellung ist der Zugriff über HTTPS aktiviert. Beim Zugriff über HTTP wird die Adresse automatisch auf HTTPS umgeleitet.

Wenn Sie über eine HTTP-Verbindung auf das WBM zugreifen möchten, müssen Sie unter "System > Konfiguration" bei "HTTP-Dienste" "HTTP & HTTPS" auswählen.

### Voraussetzungen

**Darstellung des WBM**

- Das Gerät verfügt über eine IP-Adresse.
- Zwischen dem Gerät und dem Admin-PC besteht eine Verbindung.
  Mit dem Windows ping-Befehl können Sie nachprüfen, ob eine Verbindung besteht.
  Ist das Gerät im Zustand der Werkseinstellungen, siehe "Voraussetzungen für den Betrieb".
- Der Zugriff über HTTPS ist aktiviert.
- Im Webbrowser ist JavaScript aktiviert.
- Der Webbrowser darf nicht so eingestellt sein, dass er bei jedem Zugriff auf die Seite diese neu vom Server laden soll. Die Aktualität der dynamischen Seiteninhalte wird über andere Mechanismen sichergestellt.
  Beim Internet Explorer finden Sie eine entsprechende Einstellmöglichkeit im Menü "Extras > Internetoptionen > Allgemein" im Abschnitt "Browserverlauf" über die Schaltfläche "Einstellungen". Aktivieren Sie bei "Neuere Versionen der gespeicherten Seite suchen" die Option "Automatisch".
- Wenn eine Firewall eingesetzt wird, müssen die entsprechenden Ports freigeschaltet sein.
  - Für den Zugriff über HTTPS: TCP-Port 443
- Die Darstellung des WBM wurde mit folgenden Desktop-Webbrowsern getestet:
  - Mozilla Firefox 91 ESR
  - Google Chrome 93
  - Microsoft Edge Chromium 93

# 5.2 Starten und anmelden

## Verbindung zu einem Gerät herstellen

Führen Sie folgende Schritte durch, um mit einem Internet-Browser eine Verbindung zu einem Gerät herzustellen:

1. Zwischen dem Gerät und dem Admin-PC besteht eine Verbindung. Mit dem ping-Befehl können Sie prüfen, ob das Gerät erreichbar ist.
2. Geben Sie im Adressfeld des Internet-Browsers "https://" gefolgt von der IP-Adresse des zu konfigurierenden Geräts oder seine URL ein, z.B. https://192.168.16.178.
   Standardmäßig ist der Zugriff über HTTPS aktiviert.

   **Hinweis**

   **Informationen zum Sicherheitszertifikat**

   Da das Gerät nur über verschlüsselte Zugänge administrierbar ist, wird es mit einem selbst unterzeichneten Zertifikat ausgeliefert. Bei Zertifikaten mit Unterschriften, die dem Betriebssystem nicht bekannt sind, erscheint ein Sicherheitshinweis. Sie können sich das Zertifikat anzeigen lassen.

   Eine Meldung zum Sicherheitszertifikat erscheint. Quittieren Sie diese Meldung und setzen Sie das Laden der Seite fort.
   Wenn Sie einen anderen Port als den Standardport verwenden, dann geben Sie zwischen der IP-Adresse und der Portnummer einen Doppelpunkt ":" als Trennzeichen ein.
   Beispiel: https://192.168.16.178:49152
   Den Port ändern Sie unter "System > Konfiguration".
3. Wenn eine Verbindung zum Gerät besteht, erscheint die Anmeldeseite des Web Based Managements (WBM).
   Wenn Sie über eine unsichere HTTP-Verbindung auf das WBM zugreifen möchten, aktivieren Sie den HTTP-Server unter "System > Konfiguration". Beim nächsten Anmelden klicken Sie auf den Link "Wechsel zu unsicherer HTTP-Verbindung" in der Anmeldeseite oder geben Sie im Adressfeld des Internet-Browsers "http://" und die IP-Adresse des Geräts ein.



### Sprache umschalten

1. Wählen Sie aus der Klappliste im oberen rechten Bereich die Sprachversion der WBM-Seiten aus.
2. Klicken Sie auf die Schaltfläche "Go", um zur ausgewählten Sprache zu wechseln.

**Hinweis**

**Verfügbare Sprachen**

Als Sprachen sind Englisch und Deutsch verfügbar.

### Anmeldeseite personalisieren

Auf der Anmeldeseite können Sie einen zusätzlichen Text einblenden.

1. Erstellen Sie eine txt-Datei, die den gewünschten Text oder die ASCII-Art enthält. Bei ASCII-Art werden Piktogramme z. B. das Firmenlogo Siemens auf Basis der verfügbaren Zeichen dargestellt. Unterstützt werden bis zu 50 Textzeilen mit jeweils 255 Zeichen einschließlich Leerzeichen.

   **Hinweis**

   Die Verwendung der folgenden Sonderzeichen wird nicht unterstützt:
   - Umgekehrter Schrägstrich (\)
   - Fragezeichen (?)
   - Tabulatoren: Verwenden Sie anstatt Tabulatoren Leerzeichen

2. Laden Sie die Textdatei über "System > Laden & Speichern" in das Gerät. Nutzen Sie dafür unabhängig vom verwendeten Protokoll die Schaltfläche "Hochladen" in der Tabellenzeile "LoginWelcomeMessage".
3. Melden Sie sich ab. Auf der Anmeldeseite wird der konfigurierte Text unterhalb der Anmeldedaten angezeigt.

### Am WBM anmelden

Sie haben folgende Möglichkeiten, sich über HTTPS anzumelden. Entweder benutzen Sie die Anmeldemöglichkeit in der Mitte des Browser-Fensters oder die Anmeldemöglichkeit im linken oberen Bereich des Browser-Fensters. Für beide Möglichkeiten gelten folgende Schritte.

1. Eingabefeld "Name":
   - Wenn Sie sich das erste Mal oder nach einem "Auf Werkseinstellungen zurücksetzen und Neustart" anmelden, geben Sie den werkseitig voreingestellten Benutzer "admin" ein. Mit diesem Benutzerkonto können Sie Einstellungen des Geräts verändern (lesender und schreibender Zugriff auf die Konfigurationsdaten).
   - Geben Sie den Benutzernamen des angelegten Benutzerkontos ein. Lokale Benutzerkonten und Rollen konfigurieren Sie unter "Security > Benutzer".
2. Eingabefeld "Passwort":
   - Wenn Sie sich das erste Mal oder nach einem "Auf Werkseinstellungen zurücksetzen und Neustart" anmelden, geben Sie das Passwort des werkseitig voreingestellten Benutzers "admin" ein: "admin".
   - Geben Sie das Passwort des entsprechenden Benutzerkontos ein
3. Klicken Sie auf die Schaltfläche "Anmelden" oder bestätigen Sie die Eingabe mit "Enter".

   **Hinweis**

   Wenn Sie sich das erste Mal oder nach einem "Auf Werkseinstellungen zurücksetzen und Neustart" anmelden, können Sie einmalig den werksseitig voreingestellten Benutzer "admin" umbenennen. Danach ist ein Umbenennen von "admin" nicht mehr möglich. Tragen Sie den neuen Namen in das entsprechende Eingabefeld ein.

   Wenn Sie sich das erste Mal oder nach einem "Auf Werkseinstellungen zurücksetzen und Neustart", werden Sie aufgefordert, das Passwort zu ändern.
   Das neue Passwort muss der Passwortrichtlinie "Hoch" entsprechen:
   - Passwortlänge: Mindestens 8 Zeichen, maximal 128 Zeichen
   - Mindestens 1 Großbuchstabe
   - Mindestens 1 Sonderzeichen (Sonderzeichen | § ? " ; : ß \ sind nicht erlaubt)
   - Mindestens 1 Zahl

   Zur Bestätigung müssen Sie das Passwort wiederholen. Beide Passworteingaben müssen übereinstimmen.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen", um den Vorgang abzuschließen.
   Die Änderungen sind sofort wirksam. Nach der Änderung des admin-Passworts wird der Zugriff über DCP schreibgeschützt. Die Netzwerkparameter können mit SINEC PNI oder mit "DCP Discovery" zwar gelesen, aber nicht mehr geändert werden.

Wenn Sie sich erfolgreich angemeldet haben, erscheint die Startseite.

## An der dynamischen Firewall anmelden

**Voraussetzung**

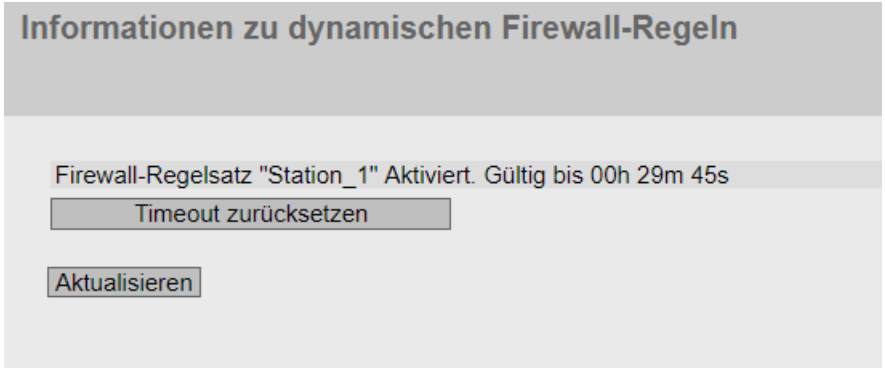
- Der Benutzer besitzt das Recht für den Remote-Zugriff. Die Einstellung konfigurieren Sie unter "Security > Benutzer > Lokale Benutzer".
- Dem Benutzer ist ein Regelsatz zugewiesen.
  Weiterführende Informationen dazu finden Sie im Getting Started "Dynamische  Firewall".

**Vorgehensweise**

1. Wenn nicht standardmäßig die Anmeldeseite für die dynamische Firewall eingestellt ist, klicken Sie auf den Link "Wechsel zur Firewall-Anmeldung".
2. Geben Sie den Benutzernamen des angelegten Benutzerkontos ein. Lokale Benutzerkonten und Rollen konfigurieren Sie unter "Security > Benutzer".
3. Geben Sie das Passwort des entsprechenden Benutzerkontos ein.
4. Klicken Sie auf die Schaltfläche "Anmelden" oder bestätigen Sie die Eingabe mit "Enter". Wenn Sie das Benutzerkonto mit einem Ereignis kombinieren, muss diese Bedingung zusätzlich erfüllt sein.

## Schutz vor Brute-Force-Angriffen

Zum Schutz vor Brute-Force-Angriffen wird einem Benutzer bzw. der IP-Adresse eines Benutzers nach mehreren fehlgeschlagenen Anmeldeversuchen die Anmeldung am Gerät verweigert. Standardmäßig ist die Anzahl der Anmeldeversuche pro Benutzer auf 12 und pro IP-Adresse auf 10 voreingestellt. Nach jedem unzulässigen Anmeldeversuch verlängert sich die Wartezeit, während der die Seite für neue Anmeldeversuchte gesperrt ist. Diese Einstellungen können Sie auf der Seite "Security > Brute Force Prevention" ändern.




Die WBM-Seite "Informationen zu dynamischen Firewall-Regeln" öffnet sich, wenn die Anmeldung erfolgreich war.

Der aktuelle Regelsatz und die verbleibende Zeit werden angezeigt. Bei Bedarf kann der Benutzer die Zugriffszeit über die Schaltfläche "Timeout zurücksetzen" verlängern.

## Servicetechniker-Login

Für Service-Zwecke verfügt das Gerät über einen Servicetechniker-Login. Dieser ist nur nach Aktivierung durch einen Administrator verfügbar und nur vom Siemens Support zu verwenden.

# 5.3 Menü "Wizard"

## 5.3.1 Basic Wizard

### Einleitung

Mit dem Basic Wizard lassen sich menügeführt die wichtigsten Parameter konfigurieren. Auf den Basic Wizard-Seiten sind nur die Parameter konfigurierbar, die für die Basisfunktionalität wichtig sind. Weitere Einstellungen konfigurieren Sie nach Beenden des Basic Wizard.

Der Umfang der Basic Wizard-Seiten ist von dem Gerät abhängig.

### Voraussetzung

- Das Gerät verfügt über eine IP-Adresse und ist über die Ethernet-Schnittstelle erreichbar.
- Sie sind im WBM mit einem Benutzer angemeldet, der Administratorrechte hat.
- M87x: Im Gerät ist eine Mini-SIM-Karte vorhanden.
- MUM856: Im Gerät ist eine Micro-SIM-Karte vorhanden
- Im Auslieferungszustand oder nach einem "Auf Werkseinstellungen zurücksetzen und Neustart" ist das Gerät mit den werkseitig voreingestellten Werten erreichbar. Weitere Informationen dazu finden Sie im Kapitel "Voraussetzungen für den Betrieb (Seite 40)".

### Basic Wizard starten

Klicken Sie im Navigations-Bereich auf "Wizard > Basic Wizard", um den Basic Wizard zu starten.

Wenn Sie sich das erste Mal oder nach einem "Auf Werkseinstellungen zurücksetzen und Neustart" anmelden, wird nach dem Ändern des Standard-Passworts automatisch der Basic Wizard gestartet.

### Häufig verwendete Schaltflächen

Die WBM-Seiten des Basic Wizards enthalten folgende Schaltflächen:

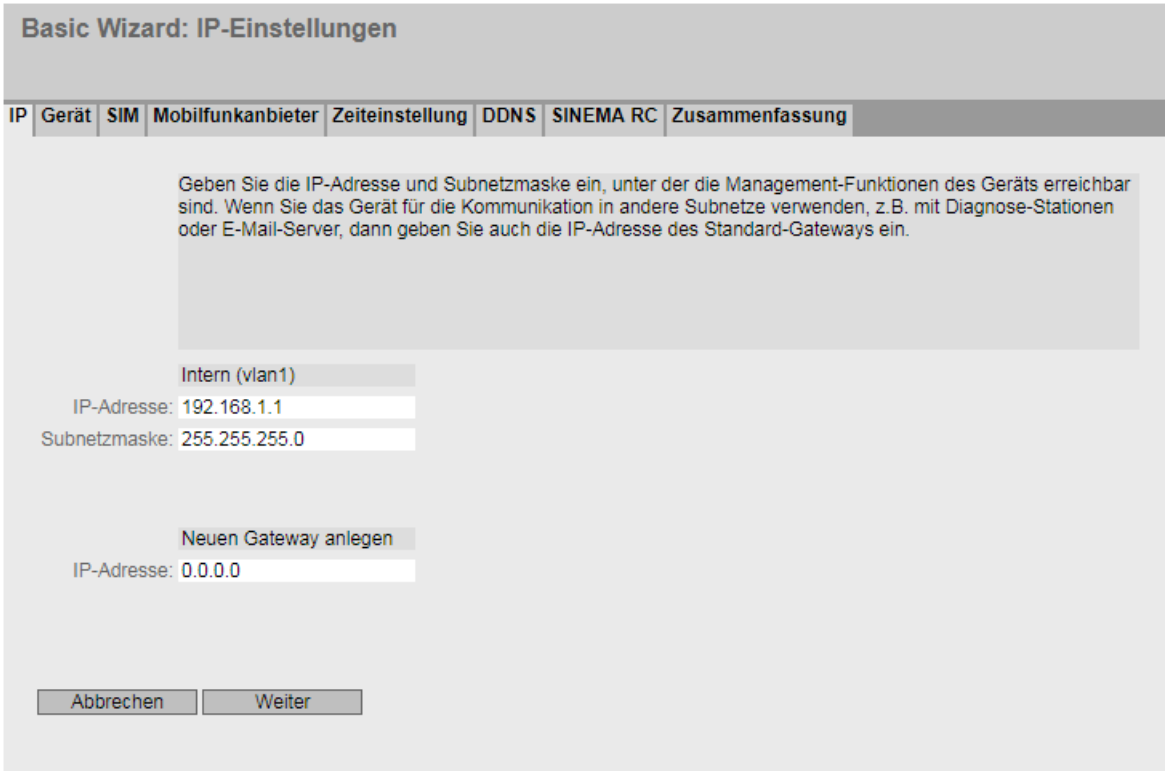
| Schaltfläche | Beschreibung |
|---|---|
| Weiter | Geht zur nächsten Seite |
| Zurück | Geht zur vorherigen Seite zurück |
| Abbrechen | Der Basic Wizard wird ohne Übernahme der Einstellungen beendet. |
| Einstellungen übernehmen | Speichert die Konfiguration und beendet den Basic Wizard. |

Die Navigation innerhalb der Seiten des Basic Wizard erfolgt ausschließlich mit Hilfe der Schaltflächen "Zurück" und "Weiter".

## 5.3.2 IP

### Einleitung

Zu den grundlegenden Konfigurationsschritten für ein Gerät gehört das Festlegen der IP-Adresse. Mit der IP-Adresse wird ein Gerät im Netz eindeutig identifiziert.




### Beschreibung

Die Basic Wizard-Seite enthält folgende Felder:

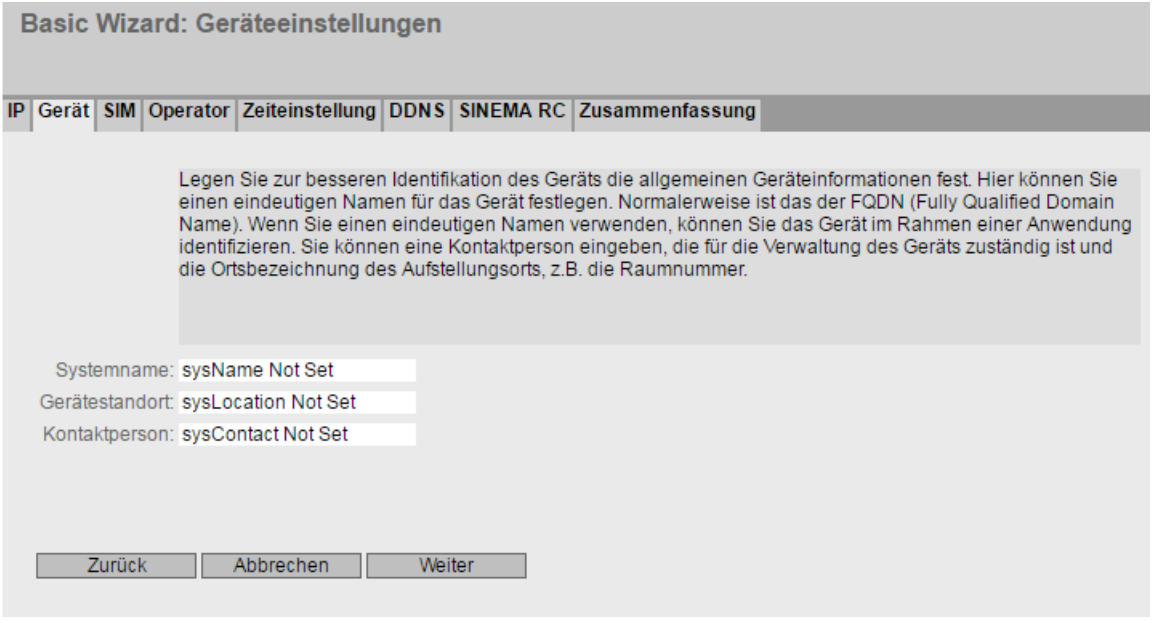
- **IP-Adresse**
  Tragen Sie eine IP-Adresse ein, die innerhalb Ihres Netzes eindeutig ist.
- **Subnetzmaske**
  Tragen Sie die Subnetzmaske des Geräts ein.
- **DHCP** (Nur beim M826)
  Zeigt die Einstellung des DHCP-Clients auf vlan1 an.
  Wenn aktiviert, erhält das Gerät die Einstellungen für die IP-Adresse und die Subnetzmaske von einem DHCP-Server.

- **Gateway (DHCP)** (Nur beim M826)
  Zeigt die IP-Adresse des Gateways, wenn der DHCP-Server diese übermittelt.
- **Neuen Gateway anlegen**
  In diesem Bereich legen Sie das Gateway fest.
  - IP-Adresse
    Geben Sie die IP-Adresse des Default-Gateways ein, um mit Geräten in einem anderen Subnetz zu kommunizieren.

## 5.3.3 Gerät

### Einleitung

Auf dieser Basic Wizard-Seite konfigurieren Sie die allgemeinen Geräteinformationen.



### Beschreibung

Die Basic Wizard-Seite enthält folgende Felder

- **Systemname**
  Sie können den Namen des Geräts eintragen. Wenn Sie dieses Feld konfigurieren, wird diese Konfiguration übernommen und im Auswahlbereich angezeigt. Es sind maximal 255 Zeichen möglich.
  Der Systemname wird auch in der CLI-Eingabeaufforderung (Prompt) angezeigt. In der CLI-Eingabeaufforderung ist die Anzahl der Zeichen begrenzt. Der Systemname wird nach 16 Zeichen abgeschnitten.
- **Gerätestandort**
  Sie können den Montageort des Geräts eingeben. Der Montageort wird im Auswahlbereich angezeigt. Es sind maximal 255 Zeichen möglich.

  **Hinweis**

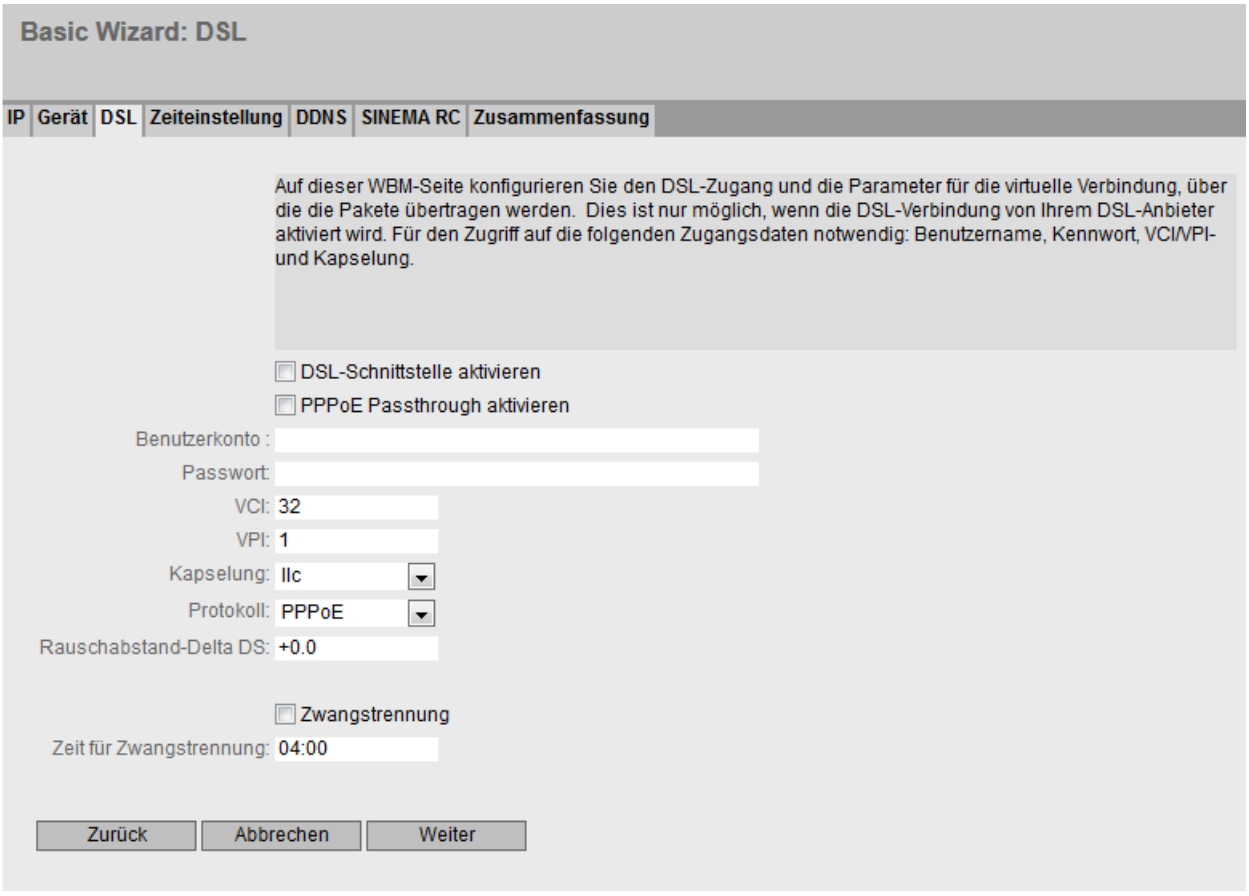
  **Erlaubte Zeichen**

  Folgende darstellbare ASCII-Zeichen (0x20 bis 0x7e) in den Eingabefeldern sind erlaubt:
  - 0123456789
  - A...Z a...z
  - !"#$%&'()*+,-./:;<=>?@ [\]_{|}~^`
- **Kontaktperson**
  Sie können eine Kontaktperson eingeben, die für die Verwaltung des Geräts zuständig ist. Es sind maximal 255 Zeichen möglich.

## 5.3.4 DSL

M81x

Auf dieser Basic Wizard-Seite konfigurieren Sie den DSL-Zugang und die Parameter für die virtuelle Verbindung, über die die Pakete übertragen werden.




## Beschreibung

Die Seite enthält Folgendes:

- **DSL-Schnittstelle aktivieren**
  Aktivieren oder deaktivieren Sie die DSL-Schnittstelle.
- **PPPoE Passthrough aktivieren**
  - Aktiviert
    Das Gerät agiert als Modem. Die Einstellungen "Benutzerkonto", "Passwort" und "Zwangstrennung" sind nicht editierbar. Nur ein angeschlossenes Gerät kann die DSL-Verbindung nutzen. Dieses Gerät übernimmt auch die Authentifizierung (Einwahl) beim Provider.
  - Deaktiviert
    Das Gerät agiert als Router und meldet sich mit Benutzernamen und Passwort an. Alle angeschlossenen Geräte können die DSL-Verbindung nutzen.
- **Benutzerkonto**
  Tragen Sie den Benutzernamen ein. Den Benutzernamen erhalten Sie von Ihrem DSL-Anbieter.
- **Passwort**
  Tragen Sie das Passwort ein. Das Passwort erhalten Sie von Ihrem DSL-Anbieter.

- **VCI** (Virtual Channel Identifier)
  Tragen Sie die ID für den virtuellen Kanal ein. Die Einstellung erhalten Sie von Ihrem DSL-Anbieter.
- **VPI** (Virtual Path Identifier)
  Tragen Sie die ID für den virtuellen Pfad ein. Die Einstellung erhalten Sie von Ihrem DSL-Anbieter.
- **Kapselung**
  Die Datenpakete werden in das gewünschte Protokoll eingepackt.
  Folgende Möglichkeiten gibt es:
  - vc-mux (Virtual circuit - multiplexing)
  - LLC (Logical Link Control)
- **Protokoll**
  Legen Sie das Protokoll für die Internetverbindung fest. Die Information erhalten Sie von ihrem DSL-Anbieter.
  - PPPoE (Point-to-Point over Ethernet)
    Die PPP-Daten werden in einen Ethernet-Frame eingekapselt.
  - PPPoA (Point-to-Point over ATM)
    Die PPP-Daten werden in ATM AAL5 (Adaptation Layer 5) eingekapselt. Wenn Sie PPPoA auswählen, wird die Einstellung "PPPoE Passthrough aktivieren" deaktiviert.
- **Rauschabstand-Delta DS**
  Legen Sie den Abstand zum Grundrauschen fest.
- **Zwangstrennung**
  Der DSL-Anbieter trennt nach einem bestimmten Zeitraum die Verbindung. Aktivieren Sie diese Option, wenn Sie die Zwangstrennung durch Ihren Provider auf eine bestimmte Uhrzeit verschieben wollen, z. B. Nachts außerhalb der üblichen Bürozeiten.
- **Zeit für Zwangstrennung**
  Legen Sie die Uhrzeit fest, zu der Sie die Zwangstrennung des DSL-Anbieters verschieben wollen. Vorausgesetzt, im Gerät ist die korrekte Systemzeit eingestellt.
  Eingabeformat: HH:MM

### 5.3.5 SHDSL

M826

Auf dieser Basic Wizard-Seite konfigurieren Sie die Rolle und das Übertragungsprofil für die Schnittstelle.




## Beschreibung

Die Seite enthält Folgendes:

- **PME Aggregation-Funktion aktivieren**
  PME = Physical Medium Entities
  Wenn aktiviert, werden die SHDSL-Schnittstellen bzw. die 2-Drathleitungen zu einer einzigen Verbindung mit höherer Übertragungsrate zusammengefasst.

  **Hinweis**

  Wenn die Funktion "PME Aggregation-Funktion aktivieren" aktiviert ist, müssen die Schnittstellen eines Geräts jeweils die gleiche Rolle besitzen.

Für jede SHDSL-Schnittstelle ist Folgendes konfigurierbar:

- **Status**
  Legen Sie fest, ob die Schnittstelle verwendet wird.
- **Rolle**
  Legen Sie die Rolle fest**:**
  - Central Office (CO)
    Die Schnittstelle ist eine Vermittlungsstelle.
  - Customer Premises Equipment (CPE)
    Die Schnittstelle ist ein Teilnehmerendgerät.
- **Vordefinierte Profile**
  Legen Sie das Profil für die Übertragung fest. Wenn Sie ein Profil verwenden, werden die nachfolgenden Parameter automatisch eingestellt.
  - Profile mit einem Übertragungsbereich
    Wenn beim Einmessen der Leitung der gemessene Wert innerhalb des Bereichs liegt, wird die SHDSL-Verbindung aufgebaut.

| | Link-Datenrate min - max | |
|---|---|---|
| Standard | 192 - 5696 | Für mittlere und längere Leitungslänge |
| Zuverläs-sig | 192 - 5696 | Beim gleichzeitigen Betrieb von mehreren SHDSL-Verbindun-gen. |
| Erweitert | 64 - 15296 | Für kurze und lange Leitungslänge |

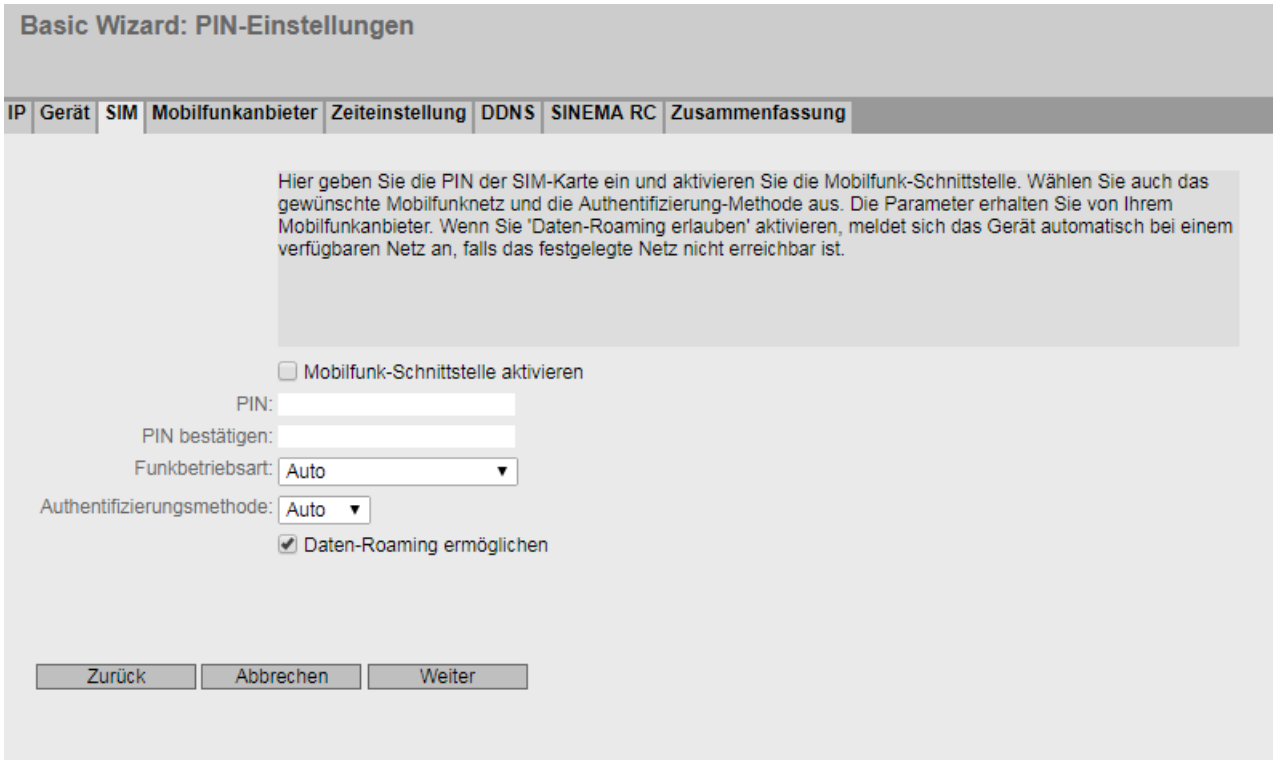
  - Profile mit einer fest vorgegebenen Übertragungsrate
    Nur wenn beim Einmessen der Leitung der gemessene Wert genau der fest vorgegebenen Übertragungsrate entspricht, wird eine SHDSL-Verbindung aufgebaut.

| | Link-Datenrate |
|---|---|
| Fest (Hohe Datenrate) | 5696 |
| Fest (Mittlere Datenrate) | 3072 |
| Fest (Niedrige Datenrate) | 512 |

## 5.3.6 SIM

M87x MUM85x

Für den Zugang zum Mobilfunknetz und zu den Mobilfunkdiensten sind folgende Zugangsparameter erforderlich. Die Zugangsparameter erhalten Sie von Ihrem Mobilfunkanbieter.




## Beschreibung

Die Basic Wizard-Seite enthält Folgendes:

- **Mobilfunk-Schnittstelle aktivieren**
  Aktivieren oder deaktivieren Sie die Mobilfunk-Schnittstelle. Die Mobilfunk-Schnittstellen sind im Auslieferungszustand deaktiviert.
- **PIN**
  Tragen Sie die PIN der SIM-Karte ein. Die PIN erhalten Sie von Ihrem Mobilfunkanbieter. Das Gerät arbeitet auch mit PIN-losen SIM-Karten, in diesem Fall lassen Sie das Feld leer.

  **Hinweis**

  **Bei Fehleingaben wird die SIM-Karte gesperrt**

  Achten Sie darauf, die PIN korrekt einzugeben. Wenn Sie die PIN öfter als 3 Mal falsch eingeben, wird die SIM-Karte gesperrt.

  Unter "Information > Mobile" können Sie den Status der SIM-Karte überprüfen. Wenn bei "SIM-Status" "PUK erforderlich" angezeigt wird, ist die SIM-Karte gesperrt.

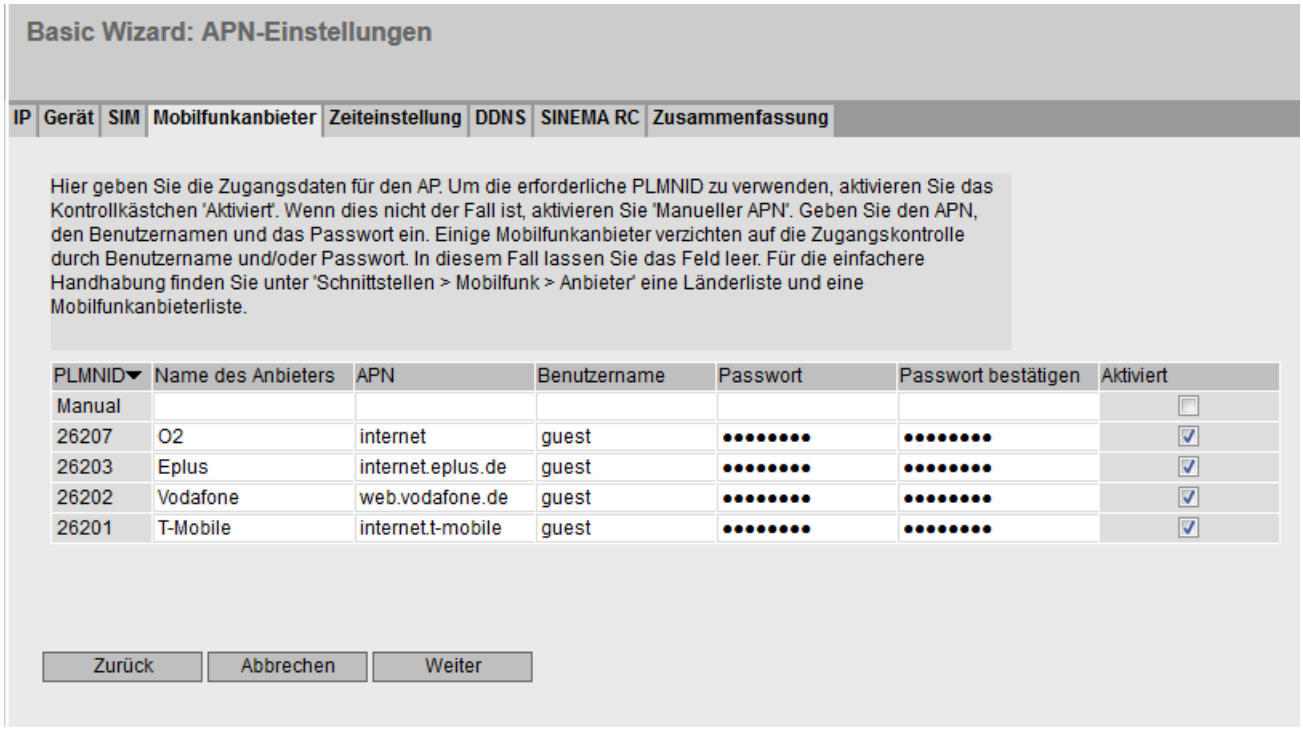
  Sie können unter "Schnittstellen > Mobilfunk > SIM" die PIN ändern oder die SIM-Karte entsperren.
- **PIN bestätigen**
  Wiederholen Sie die PIN.

- **Funkbetriebsart**
  Wählen Sie das gewünschte Mobilfunknetz aus. Folgende Optionen stehen zur Auswahl:
  - Auto (nicht beim M874-2)
    Alle Dienste. Das Gerät versucht bevorzugt mit dem schnellsten verfügbaren Mobilfunkverfahren eine Verbindung herzustellen.
  - Nur GSM
    Die Dienste EGPRS und GPRS.
    Das Gerät ignoriert das UMTS- und LTE-Netz und baut eine Verbindung zu dem GSM-Dienst auf, der vor Ort die höchste Bandbreite zur Verfügung stellt
  - Nur UMTS (nicht beim M874-2)
    Der Dienst UMTS und HSPA. Das Gerät ignoriert die Dienste EGPRS, GPRS und LTE und baut eine Verbindung im UMTS-Netz auf.
  - Nur LTE (nur bei M876-4 / MUM85x)
    Der Dienst LTE. Das Gerät ignoriert die Dienste EGPRS, GPRS und UMTS und baut eine Verbindung im LTE-Netz auf.
  - 5 G NR + LTE (NSA) (nur beim MUM85x)
    Die Dienste 5G New Radio (NR) und LTE Non-Standalone Operation (NSA)
  - Nur 5 G NR SA (nur beim MUM85x)
    Der Dienst 5G New Radio (NR) im Standalone-Betrieb (SA)
  - EVDO (nur beim M876-3 verfügbar)
    EVolution, Data-Optimized. Standard für CDMA-basiert Netzwerke.
    Folgende Substandards werden unterstützt:
    - EVDO Hybrid
    - EVDO 1xRTT
    - EVDO HDR - High Data Rate
  - Keine Datenverbindung
    Es besteht keine Datenverbindung. Geeignet, wenn das Gerät nur zum Senden oder Empfangen von SMS verwendet wird.
- **Authentifizierungsmethode**
  Wählen Sie das gewünschte Authentifizierungsverfahren aus.
  - CHAP
    Verschlüsselte Übertragung von Benutzername und Passwort über das Challenge Handshake Authentication Protocol (CHAP).
  - PAP
    Unverschlüsselte Übertragung von Benutzername und Passwort über das Password Authentication Protocol (PAP).
  - Auto
    Benutzername und Passwort werden automatisch mit einem der beiden Verfahren übertragen. CHAP hat die höhere Priorität. Wenn der Kommunikationspartner CHAP nicht unterstützt, werden Benutzername und Passwort per PAP übertragen.
- **Daten-Roaming ermöglichen**
  Wenn aktiviert, meldet sich das Gerät automatisch bei einem verfügbaren Netz an, falls das festgelegte Netz nicht erreichbar ist.

## 5.3.7 Mobilfunkanbieter

M87x | MUM85x

Der APN (Access Point Name) ist der Name des Zugangspunkts vom Mobilfunknetz zum Internet oder zu einem privaten Firmennetz. Abhängig vom Typ des angeschlossenen Netzes handelt es sich um einen öffentlichen oder privaten APN. Der APN wird vom Mobilfunkanbieter mitgeteilt.




### Beschreibung

Die Seite enthält folgende Felder:

- **Länderliste**
  Wählen Sie in der Liste das Land aus, in dem das Gerät eingesetzt wird.
- **Anbieter-Liste**
  Wählen Sie in der Liste den entsprechenden Mobilfunkanbieter aus. Die Liste ist abhängig von dem ausgewählten Land.
  Wenn der Mobilfunkanbieter nicht in der Liste der Provider enthalten ist, wählen Sie "-" aus.

**Hinweis**

**Funkbetriebsart "Nur 5G SA (Standalone)"**

Bei der Funktionsbetriebsart "Nur 5G SA " sind alle nicht benötigten Provider zu deaktivieren.

- **PLMNID**
  Jeder Mobilfunkanbieter hat eine weltweit einmalig vergebene Identifikationsnummer, die als Public Land Mobile Network ID (PLMN ID) bezeichnet wird. Sie finden die Net-ID in den Unterlagen Ihres Mobilfunkbetreibers oder auf dessen Internetseiten.
  - Wenn Sie die PLMNID des Mobilfunkanbieters kennen, geben Sie diese Nummer ein.
  - Wenn Sie die PLMNID nicht kennen, geben Sie in der Tabelle bei "Manual" die Daten ein.
- **APN**
  Tragen Sie den Namen des APNs ein. Den APN finden Sie in den Unterlagen Ihres Mobilfunkbetreibers, auf dessen Internetseite oder Sie erfragen den APN bei der Hotline Ihres Mobilfunkbetreibers.
- **Benutzername**
  Tragen Sie den Benutzernamen ein. Einige Mobilfunkbetreiber verzichten auf die Zugangskontrolle durch Benutzername und/oder Passwort. In diesem Fall lassen Sie das Feld leer.
- **Passwort**
  Tragen Sie das Passwort ein. Einige Mobilfunkbetreiber verzichten auf die Zugangskontrolle durch Benutzername und/oder Passwort. In diesem Fall lassen Sie das Feld leer.
- **Passwort bestätigen**
  Wiederholen Sie das Passwort.

Die Tabelle enthält folgende Spalten:

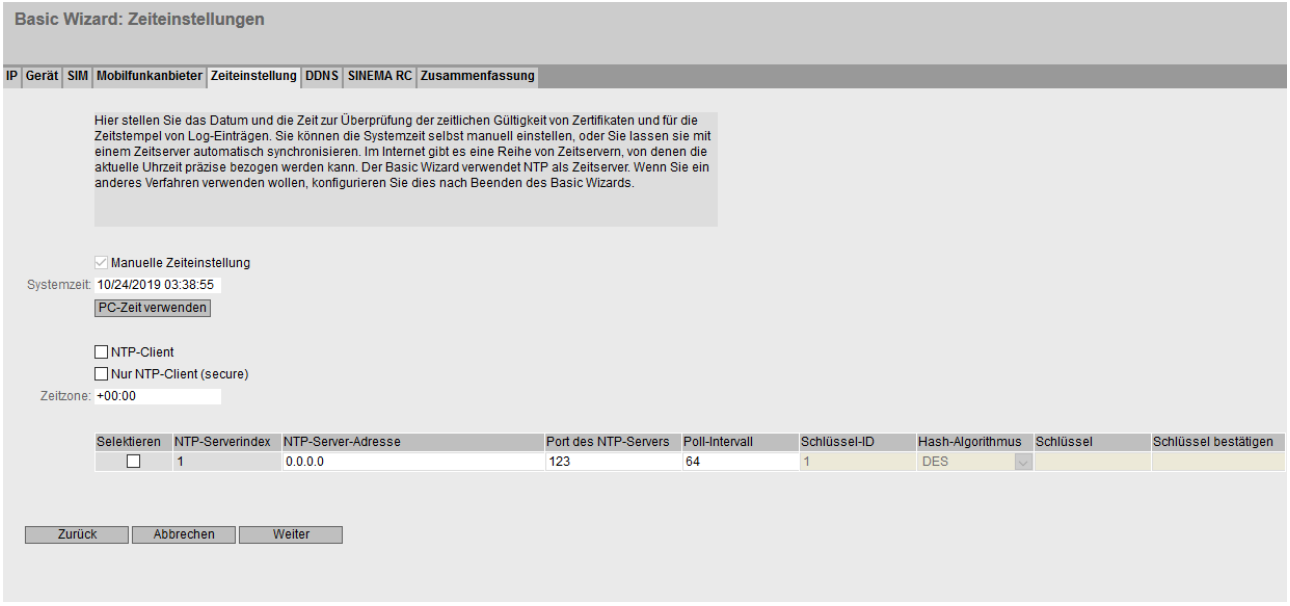
- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **PLMNID**
  - Identifikationsnummer (Net-ID)
    Zeigt die PLMNID des Mobilfunkanbieters an.
  - Manual (statischer APN)
    Wenn die PLMNID nicht bekannt ist, geben Sie den APN ihres Mobilfunkanbieters an.
  - Manual (dynamische APN)
    Nur beim M876-4 verfügbar
    Voraussetzung: Funkbetriebsart "Nur LTE"
    Wenn Sie keine Daten konfigurieren, wird der APN dynamisch zugewiesen.
- **Name des Anbieters**
  Tragen Sie den Namen Ihres Mobilfunkanbieters ein.
- **APN**
  Tragen Sie den Namen des APNs ein. Den APN finden Sie in den Unterlagen Ihres Mobilfunkanbieters, auf dessen Internetseite oder Sie erfragen den APN bei der Hotline Ihres Mobilfunkbetreibers.
- **Benutzername**
  Tragen Sie den Benutzernamen für den APN ein. Einige Mobilfunkanbieter verzichten auf die Zugangskontrolle durch Benutzername und/oder Passwort. In diesem Fall lassen Sie das Feld leer.

- **Passwort**
  Tragen Sie das Passwort für den APN ein. Einige Mobilfunkanbieter verzichten auf die Zugangskontrolle durch Benutzername und/oder Passwort. In diesem Fall lassen Sie das Feld leer.
- **Passwort bestätigen**
  Wiederholen Sie das Passwort.
- **Aktiviert**
  Der Eintrag wird verwendet.

## 5.3.8 Zeiteinstellung

### Zeiteinstellung

Auf dieser Basic Wizard-Seite stellen Sie das Datum und die Uhrzeit des Systems ein.




### Beschreibung

**Manuelle Zeiteinstellung**:

- **Manuelle Zeiteinstellung**
  Aktivieren oder deaktivieren Sie die manuelle Zeiteinstellung. Wenn Sie die Option aktivieren, wird das Eingabefeld "System Time" editierbar.
- **Systemzeit**
  Geben Sie Datum und Uhrzeit im Format "MM/DD/YYYY HH:MM:SS" ein.
  Nach dem Neustart beginnt die Uhrzeit mit 01/01/2000 00:00:00
- **PC-Zeit verwenden**
  Klicken Sie auf die Schaltfläche, um die Zeiteinstellung des PCs zu übernehmen.

**Automatische Zeiteinstellung über NTP**

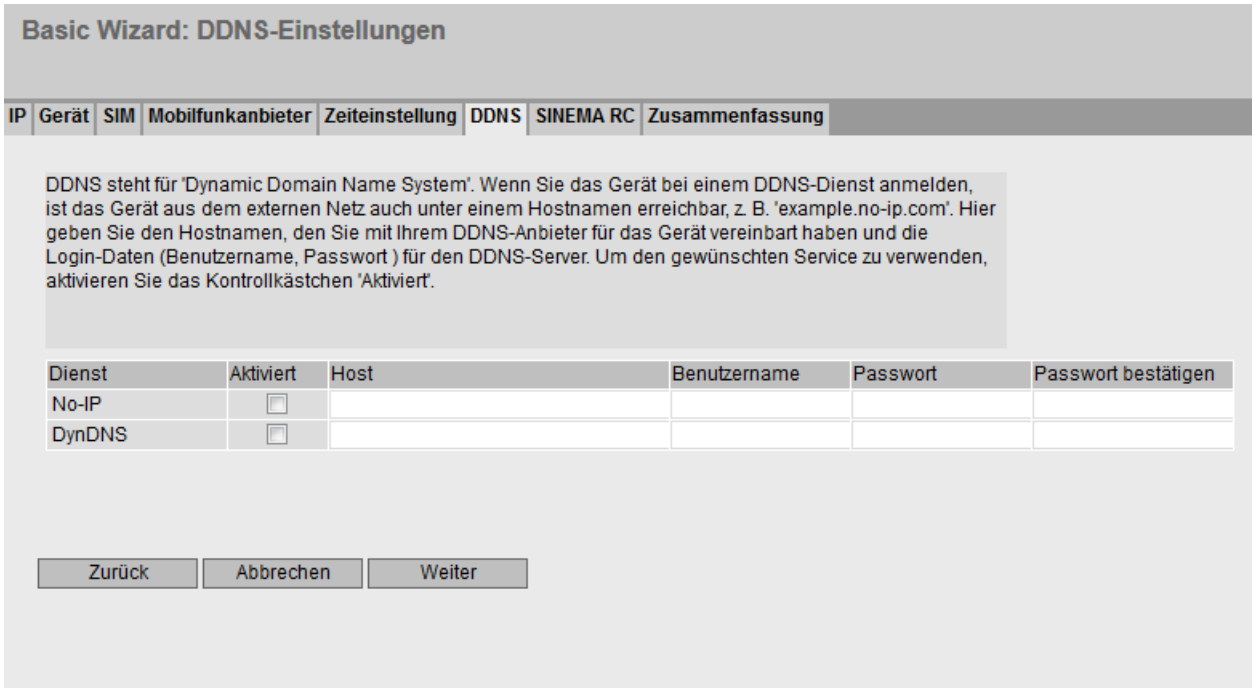
- **NTP-Client**
  Aktivieren oder deaktivieren Sie die Zeitsynchronisation über NTP.
- **Nur NTP-Client (secure)**
  Wenn aktiviert, erhält das Gerät die Systemzeit von einem gesicherten NTP-Server. Die Einstellung gilt für alle Servereinträge.
  Um den gesicherten NTP-Client zu verwenden, sind die Parameter für die Authentifizierung (Schlüssel-ID, Hash-Algorithmus, Schlüssel) zu konfigurieren.
- **Zeitzone**
  Geben Sie in diesem Feld Ihre verwendete Zeitzone im Format "+/- HH:MM" an. Die Zeitzone bezieht sich auf UTC Standard-Weltzeit. Einstellungen zu Sommer bzw. Winterzeit berücksichtigen Sie bei der Angabe des Zeit-Offset in diesem Feld.

In der Tabelle konfigurieren Sie den NTP-Server

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **NTP-Serverindex**
  Die Nummer, die einem bestimmten NTP-Servereintrag entspricht.
- **NTP-Server-Adresse**
  Geben Sie die IP-Adresse, den FQDN (Fully Qualified Domain Name) oder den Hostnamen des NTP-Servers an.
- **Port des NTP-Servers**
  Geben Sie den Port des NTP-Servers an.
  Folgende Ports sind möglich:
  - 123 (Standard-Port)
  - 1025 bis 36564
- **Poll-Intervall**
  Legen Sie den Zeitabstand zwischen zwei Uhrzeitanfragen fest. Je größer der Zeitabstand, desto ungenauer ist die Uhrzeit des Geräts.
  Mögliche Werte sind 64 bis 2592000 Sekunden (30 Tage).
- **Schlüssel-ID**
  Geben Sie die ID des Authentifizierungsschlüssels ein.
- **Hash-Algorithmus**
  Legen Sie das Format für den Authentifizierungsschlüssel fest.
- **Schlüssel**
  Geben Sie den Authentifizierungsschlüssel ein. Die Länge ist abhängig vom Hash-Algorithmus.
  Folgende Mindestlängen werden für den Hash-Algorithmus empfohlen:
  - MD5: ASCII 16 Zeichen
  - SHA1: ASCII 20 Zeichen
- **Schlüssel bestätigen**
  Geben Sie den Authentifizierungsschlüssel erneut ein, um ihn zu bestätigen.

## 5.3.9 DDNS

Auf dieser Basic Wizard-Seite konfigurieren Sie den dynamischen DNS-Client (DDNS-Client). Der DDNS-Client synchronisiert die zugewiesene IP-Adresse mit dem im DDNS-Provider registrierten Hostnamen. Damit ist das Gerät immer unter demselben Hostnamen erreichbar.




### Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Dienst**
  Zeigt an, welche Anbieter unterstützt werden.
- **Aktiviert**
  Wenn aktiviert, meldet sich das Gerät an dem DDNS-Server an.
- **Host**
  Geben Sie den Hostnamen ein, den Sie für das Gerät mit Ihrem DDNS-Anbieter vereinbart haben, z. B. example.no-ip-com.
- **Benutzername**
  Geben Sie den Benutzernamen ein, mit dem sich das Gerät am DDNS-Server anmeldet.
- **Passwort**
  Geben Sie das dem Benutzer zugeordnete Passwort ein.
- **Passwort bestätigen**
  Bestätigen Sie das Passwort.

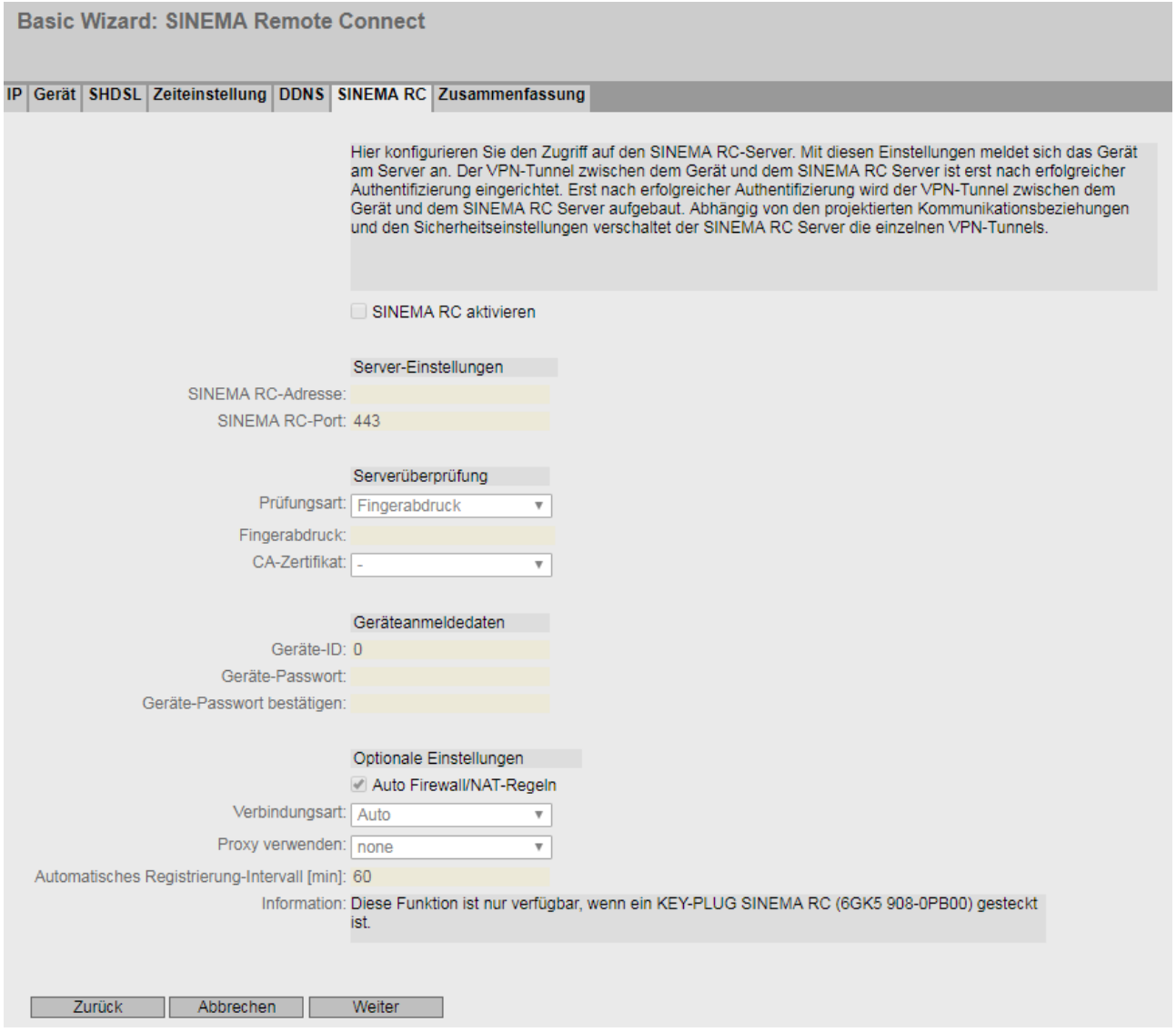
## 5.3.10 SINEMA RC

~~M812~~

Auf dieser Basic Wizard-Seite konfigurieren Sie den Zugriff zum SINEMA RC-Server.

**Hinweis**

Diese Funktion ist nur mit KEY PLUG (Seite 54) nutzbar.



## Beschreibung

Die Seite enthält Folgendes:

- **SINEMA RC aktivieren**
  - Aktiviert:
    Eine Verbindung zum konfigurierten SINEMA RC-Server wird aufgebaut. Die Felder sind nicht editierbar.
  - Deaktiviert:
    Die Felder lassen sich editieren. Eine eventuell bestehende Verbindung wird abgebaut.

**Bereich "Server-Einstellungen"**

- **SINEMA RC-Adresse**
  Geben Sie die IPv4-Adresse oder den FQDN (Fully Qualified Domain Name) des SINEMA RC-Servers ein.
- **SINEMA RC-Port**
  Geben Sie den Port ein, über den der SINEMA RC-Servers erreichbar ist.

**Bereich "Serverüberprüfung"**

- **Prüfungsart**
  - Fingerabdruck: Die Identität des Servers wird über den Fingerabdruck verifiziert.
  - CA-Zertifikat: Die Identität des Servers wird über das CA-Zertifikat verifiziert.
- **Fingerabdruck**
  Nur bei der Einstellung "Fingerabdruck" notwendig. Geben Sie den Fingerabdruck des Geräts ein. Der Fingerabdruck wird bei der Inbetriebnahme des SINEMA RC-Servers vergeben. Anhand des Fingerabdrucks überprüft das Gerät, ob es sich den korrekten SINEMA RC-Servers handelt. Weiterführende Informationen dazu finden Sie in der Betriebsanleitung zum SINEMA RC-Server.
- **CA-Zertifikat**
  Nur bei der Einstellung CA-Zertifikat" notwendig. Wählen Sie das CA-Zertifikat des Servers aus, das zur Signierung des Serverzertifikats verwendet wird. Nur geladene CA-Zertifikate sind auswählbar.

**Bereich "Geräteanmeldedaten"**

- **Geräte-ID**
  Geben Sie die Geräte-ID ein. Die Geräte-ID wird beim Konfigurieren des Geräts am SINEMA RC-Server vergeben. Weiterführende Informationen dazu finden Sie in der Betriebsanleitung zum SINEMA RC-Server.
- **Geräte-Passwort**
  Geben Sie das Passwort ein, mit dem sich das Gerät am SINEMA RC-Server anmeldet. Das Passwort wird beim Konfigurieren des Geräts am SINEMA RC-Server vergeben. Weiterführende Informationen dazu finden Sie in der Betriebsanleitung zum SINEMA RC-Server.
- **Geräte-Passwort bestätigen**
  Wiederholen Sie das Passwort.

**Bereich "Optionale Einstellungen"**

- **Auto Firewall/NAT-Regeln**
  - Aktiviert
    Für die VPN-Verbindung werden automatisch die Firewall und NAT-Regeln angelegt. Dabei werden die Verbindungen, die zwischen den projektierten exportierten Subnetzen und den Subnetzen, die über den SINEMA RC-Server erreichbar sind, zugelassen. Die NAT-Einstellungen werden wie im SINEMA RC-Server projektiert umgesetzt.
    Unter "Security > Firewall > vordefinierte IPv4-Regeln" können Sie SINEMA RC den Zugriff auf bestimmte Dienste des Geräts erlauben.
  - Deaktiviert
    Sie müssen selbst die Firewall und NAT-Regeln anlegen.
- **Verbindungsart**
  Legen Sie die Art der VPN-Verbindung fest. Weitere Informationen dazu finden Sie im Kapitel "VPN-Verbindungsaufbau".
  - Auto
    Das Gerät übernimmt die Einstellungen des SINEMA RC Server. Die Einstellungen auf dem SINEMA RC Server konfigurieren Sie unter "Fernverbindungen > Geräte". Weiterführende Informationen hierzu finden Sie in der Betriebsanleitung "SINEMA RC Server".
  - Permanent
    Die Einstellungen des SINEMA RC-Servers werden ignoriert. Das Gerät baut eine VPN-Verbindung zum SINEMA RC-Server. Der VPN-Tunnel wird permanent aufrechterhalten.
  - Weck-SMS (nur bei M87x / MUM85x)
    Die Einstellungen des SINEMA RC-Servers werden ignoriert. Wenn das Gerät eine Befehl-SMS (Wake-up SMS) erhält, versucht das Gerät zum SINEMA RC-Server aufzubauen. Vorausgesetzt unter "System > SMS > Befehl-SMS" ist festgelegt, von wem eine Befehl-SMS der Klasse "System" akzeptiert wird.
  - Digitaler Eingang
    Die Einstellungen des SINEMA RC-Servers werden ignoriert. Beim Eintreten des Ereignisses "Digital In" versucht das Gerät zum SINEMA RC-Server eine VPN-Verbindung aufzubauen. Vorausgesetzt ist, dass das Ereignis "Digitaler Eingang" an die VPN-Verbindung weitergegeben wird. Dazu aktivieren Sie unter "System > Ereignisse > Konfiguration" beim Ereignis "Digitaler Eingang" "VPN-Tunnel".
  - Digitaler Eingang & Weck-SMS (nur bei M87x / MUM85x)
    Die Einstellungen des SINEMA RC-Servers werden ignoriert. Wenn das Ereignis "Digitaler Eingang" eintritt oder wenn das Gerät eine Befehl-SMS erhält, versucht das Gerät eine VPN-Verbindung zum SINEMA RC-Server aufzubauen
- **Proxy verwenden**
  Legen Sie fest, ob Verbindung zu dem definierten SINEMA RC-Server über einen Proxy-Server aufgebaut wird. Es sind nur die Proxy-Server auswählbar, die Sie unter "System > Proxy Server" konfiguriert haben.

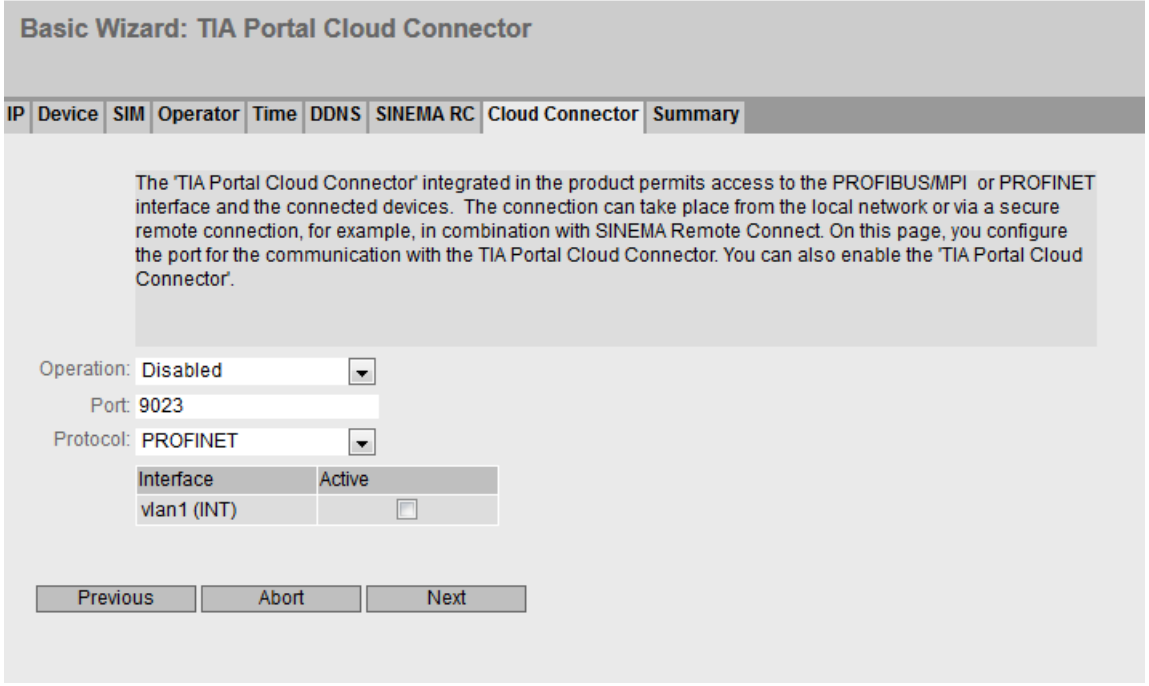
- **Automatisches Registrierung-Intervall [min]**
  Geben Sie die Zeitspanne in Minuten an, nach der Anfragen an den SINEMA RC Server gesendet werden. Mit dieser Anfrage prüft das Gerät, ob auf dem SINEMA RC Server eine neuere Firmware-Datei vorhanden ist oder ob sich die Verbindungseinstellungen geändert haben. Wenn Sie den Wert 0 eintragen, ist diese Funktion deaktiviert.
- **Timeout [min]**
  Geben Sie die Zeitspanne in Minuten an. Wenn kein Datenaustausch stattfindet, wird nach Ablauf dieser Zeitspanne der VPN-Tunnel automatisch abgebaut.

## 5.3.11 Cloud Connector

Auf dieser Wizard-Seite konfigurieren Sie die Parameter für die Kommunikation mit dem TIA Portal Cloud Connector.

**Hinweis**

- Verwenden Sie den im Produkt integrierten "TIA Portal Cloud Connector" über eine VPN-Lösung (z.B. SINEMA RC).
- Konfigurieren Sie die Firewall Einstellungen des SCALANCE M800/S615 (z.B. Vordefinierte IPv4 Regeln "Cloud Connector", um den unbefugten Zugriff von Netzteilnehmer auf den "TIA Portal Cloud Connector Server" zu verhindern.




### Voraussetzung

- Damit die eingehenden Pakete an das Gerät weitergeleitet werden, aktivieren Sie die vordefinierte IPv4-Regel "Cloud Connector".

### Beschreibung

Die Basic Wizard-Seite enthält Folgendes:

- **Betrieb**
  - Aktiviert
    Aktiviert den integrierten TIA Portal Cloud Connector.
  - Deaktiviert
    Deaktiviert den integrierten TIA Cloud Connector.
  - Bei DI starten
    Das Aktivieren wird über den digitalen Eingang (DI) gesteuert. Vorausgesetzt, unter "System > Ereignisse > Konfiguration" ist beim Ereignis "Digitaler Eingang" "Cloud Connector" aktiviert. Wenn diese Einstellung nicht aktiviert ist, wird das Ereignis nicht an den TIA Portal Cloud Connector weitergegeben.
- **Port**
  Über diesen Port wird die Kommunikation mit dem TIA Portal Cloud Connector aufgebaut.
- **Protokoll**
  Über dieses Protokoll wird auf das Anlagennetzwerk zugegriffen.
  - PROFINET über VLAN
    Die VLAN-Schnittstelle legen Sie in der folgenden Tabelle fest.

  Nur beim M804PB

  - PROFIBUS über die MPI/DP
  - PROFINET-PROFIBUS

Die folgende Tabelle ist nur bei PROFINET notwendig:

- Schnittstelle
  Nur VLANs mit konfiguriertem Subnetz sind verfügbar.
- Aktiv
  Wenn aktiviert, wird diese VLAN für PROFINET verwendet.

## 5.3.12 Zusammenfassung

### Einleitung

Auf dieser Seite werden die Einstellungen zusammengefasst. Der Inhalt der Seite ist abhängig von den eingestellten Parametern und dem Gerät.

Überprüfen Sie die Einstellungen, bevor Sie den Basic Wizard mit der Schaltfläche "Einstellungen übernehmen" beenden. Wenn Einstellungen nicht korrekt sind, navigieren Sie über die Schaltfläche "Zurück" zurück und ändern Sie die gewünschten Einstellungen.

## Basic Wizard: Zusammenfassung

IP | Gerät | SIM | Mobilfunkanbieter | Zeiteinstellung | DDNS | SINEMA RC | Zusammenfassung

| | |
|---|---|
| | Intern (vlan1) |
| IP-Adresse: | 192.168.1.1 |
| Subnetzmaske: | 255.255.255.0 |
| Systemname: | sysName Not Set |
| Gerätestandort: | sysLocation Not Set |
| Kontaktperson: | sysContact Not Set |
| Mobilfunk-Schnittstelle aktivieren: | Aktiviert |
| Funkbetriebsart: | Auto |
| Authentifizierungsmethode: | Auto |
| Daten-Roaming ermöglichen: | Aktiviert |

| PLMNID▲ | Name des Anbieters | APN | Benutzername | Aktiviert |
|---|---|---|---|---|
| 26201 | T-Mobile | internet.t-mobile | guest | Aktiviert |
| 26202 | Vodafone | web.vodafone.de | guest | Aktiviert |
| 26203 | Eplus | internet.eplus.de | guest | Aktiviert |
| 26207 | O2 | internet | guest | Aktiviert |
| Manual | | | | Deaktiviert |

| | |
|---|---|
| Manuelle Zeiteinstellung: | Aktiviert |
| Systemzeit: | 04/11/2017 16:51:14 |
| NTP-Client: | Deaktiviert |
| Nur NTP-Client (gesichert): | Deaktiviert |
| Zeitzone: | +00:00 |

| NTP-Serverindex | NTP-Server-Adresse | Port des NTP-Servers | Poll-Intervall |
|---|---|---|---|
| 1 | 0.0.0.0 | 123 | 64 |

| Dienst | Aktiviert | Host | Benutzername |
|---|---|---|---|
| No-IP | Deaktiviert | | |
| DynDNS | Deaktiviert | | |

| | |
|---|---|
| SINEMA RC: | Deaktiviert |

**Klicken Sie auf die Schaltfläche 'Einstellungen übernehmen', um die Änderungen zu übernehmen!**

Zurück | Abbrechen | Einstellungen übernehmen

#### Einstellungen übernehmen

Klicken Sie auf die Schaltfläche "Einstellungen übernehmen", um den Basic Wizard zu beenden. Die Einstellungen werden übernommen.

## 5.4 Menü "Information"

### 5.4.1 Startseite

#### Ansicht der Startseite

Nach erfolgreicher Anmeldung wird die Startseite des WBMs angezeigt. Sie können auf dieser Seite keine Konfigurationen vornehmen.

#### Allgemeiner Aufbau der WBM-Seite

Folgende Bereiche stehen auf jeder WBM-Seite zur Verfügung:

- Auswahlbereich (1): Oberer Bereich
- Anzeigebereich (2): Oberer Bereich
- Navigationsbereich (3): Linker Bereich
- Inhaltsbereich (4): Mittlerer Bereich


1
2
3
4
SIEMENS
Deutsch
Go
Location/System name
03/29/2017 07:21:38
Willkommen admin
Abmelden
SCALANCE M874-3
Wizards
Information
Startseite
Versionen
ARP-Tabelle
Log-Tabellen
Fehler
DHCP-Server
SNMP
LLDP
Routing
Mobilfunk
IPsec VPN
SINEMA RC
OpenVPN-Client
Security
System
Schnittstellen
Layer 2
Layer 3
Security
Wählen Sie einen Eintrag im Menü auf der linken Seite.
Systemname: System name
Gerätetyp: SCALANCE M874-3
PLUG-Konfiguration: ACCEPTED
PLUG-Lizenz: ACCEPTED
Verbindungsstatus: Mobilfunk-Schnittstelle deaktiviert
Signalstärke [dBm]: -
DDNS-Status: -
Fehlerstatus: No Fault
Aktualisieren

### Auswahlbereich (1)

Im Auswahlbereich wird Ihnen Folgendes angeboten:

- Logo der Siemens AG
  Wenn Sie auf das Logo klicken, gelangen Sie auf die Internetseite des entsprechenden Grundgeräts im Siemens Industry Online Support
- Anzeige von: "Gerätestandort / Systemnamen"
  - "Gerätestandort" enthält die Ortsangabe des Geräts.
    Im Auslieferzustand wird die IP-Adresse des Geräts angezeigt.
  - "Systemnamen" ist der Gerätename.
    Im Auslieferzustand wird der Gerätetyp angezeigt.

  Den Inhalt dieser Anzeige können Sie unter "System > Allgemein > Geräte" ändern.
- Klappliste für die Sprachauswahl
- Systemzeit und -datum
  Den Inhalt dieser Anzeige können Sie unter "System > Systemzeit" ändern.
  Wenn die Systemzeit nicht eingestellt ist, ist der Status . Ist die Systemzeit konfiguriert, aber die Systemzeit ist nicht synchronisierbar, ist ein gelbes Warndreieck zu sehen. Prüfen Sie, ob der Zeitserver erreichbar ist. Passen Sie gegebenenfalls Ihre Projektierung an. Wenn die Systemzeit eingestellt und/oder synchronisierbar ist, ist der Status .

### Anzeigebereich (2)

Im Anzeigebereich befindet sich im linken Bereich immer der vollständige Titel des aktuell gewählten Menüpunktes.

- **Leuchtdiodensimulation**
  Jedes Gerät verfügt über mehrere Leuchtdioden, die Informationen über den Betriebszustand des Geräts liefern. Abhängig vom Aufstellort ist der direkte Zugang zum Gerät jedoch nicht immer möglich. Aus diesem Grund bietet das Web Based Management eine Simulationsdarstellung für die Leuchtdioden. Die Bedeutung der Leuchtdiodenanzeigen ist in der Betriebsanleitung beschrieben.
  Wenn Sie diese Schaltfläche anklicken, rufen Sie das Fenster der Leuchtdiodensimulation auf. Sie können dieses Fenster während des Menüwechsels einblenden und beliebig verschieben. Um die Leuchtdiodensimulation zu schließen, klicken Sie innerhalb des Fensters der Leuchtdiodensimulation auf die Schließen-Schaltfläche.
- **Hilfe**
  Wenn Sie diese Schaltfläche anklicken, wird die Hilfeseite des aktuell gewählten Menüpunktes in einem neuen Browser-Fenster aufgerufen.
- **Drucker**
  Wenn Sie diese Schaltfläche anklicken, wird ein Popup-Fenster, mit einer für Drucker optimierten Ansicht des Seiteninhalts, geöffnet.

- **Favoriten**
  Im Lieferzustand ist die Schaltfläche auf allen Seiten deaktiviert .
  Wenn Sie diese Schaltfläche anklicken, ändert sich das Symbol und die aktuell geöffnete Seite oder das aktuell geöffnete Register wird als Favorit markiert. Sobald Sie die Schaltfläche einmal aktiviert haben, wird der Navigationsbereich in zwei Register unterteilt. Das erste Register "Menü" enthält alle verfügbaren Menüs, wie bisher. Das zweite Register "Favoriten" enthält alle Seiten/Register, die Sie als Favoriten markiert haben. Im Register "Favoriten" werden die Seiten/Register entsprechend der Struktur im Register "Menü" angeordnet.
  Wenn Sie alle angelegten Favoriten wieder deaktivieren, wird auch das Register "Favoriten" wieder entfernt. Klicken Sie hierzu auf den entsprechenden Seiten/Registern die Schaltfläche an.
  Sie können die Favoriten-Konfiguration eines Geräts auf der Seite "System > Laden & Speichern" über HTTP oder TFTP speichern, hochladen und löschen.
- **Aktualisieren an On / Aktualisieren aus Off**
  WBM-Seiten mit Übersichtlisten können zusätzlich die Schaltfläche "Aktualisieren" enthalten. Über diese Schaltfläche können Sie das Aktualisieren des Inhaltsbereichs an- oder ausschalten. Wenn das Aktualisieren angeschaltet ist, wird die Anzeige alle 2 Sekunden aktualisiert. Um das Aktualisieren auszuschalten, klicken Sie auf "On". Anstelle von "On" wird "Off" angezeigt. Standardmäßig ist auf der WBM-Seite immer das Aktualisieren angeschaltet.

### Navigationsbereich (3)

Im Navigationsbereich stehen Ihnen verschiedene Menüs mit Untermenüs zur Verfügung.

Die Untermenüs enthalten Seiten, aus denen man Informationen entnehmen kann oder mit denen Sie Konfigurationen vornehmen können. Diese Seiten werden immer im Inhaltsbereich angezeigt.

Über die Pfeile können Sie die Menüeinträge in der Navigation auf- oder zuklappen. Um die Menüeinträge aufzuklappen, klicken Sie auf den Pfeil-nach-rechts. Wenn Sie auf den Pfeil-nach-links klicken, werden die Menüeinträge wieder zugeklappt.

### Inhaltsbereich (4)

Klicken Sie im Navigationsbereich ein Menü an, um sich im Inhaltsbereich die Seiten des WBM anzeigen zu lassen.

Unter dem Gerätebild wird Folgendes angezeigt:

- Systemname: Systemname des Geräts
- Gerätetyp: Typenbezeichnung des Geräts
- PLUG-Konfiguration:
  Zeigt den Status der Konfigurationsdaten auf dem PLUG an, siehe Kapitel "System > PLUG > Konfiguration".
- PLUG-Lizenz**:**
  Zeigt den Status der Lizenz auf dem PLUG an, siehe Kapitel "System > PLUG > Lizenz".
- Verbindungsstatus: Status der Verbindung
- Signalstärke [dBm] (nur bei M87x / MUM85x):
  Zeigt die  Signalstärke der Verbindung an.

- DDNS-Status
  Wenn ein Dynamischer DNS-Dienst verwendet wird, wird der Hostnamen des Geräts angezeigt, z. B. example.no-ip.com. Zudem wird der Status der Aktualisierung angezeigt.
  - update successful
    Aktualisierung erfolgreich
  - update failed
    Aktualisierung fehlgeschlagen
  - status unknown
    Status unbekannt
- Fehlerstatus: Fehlerstatus des Geräts

### Häufig verwendete Schaltflächen

Die WBM-Seiten enthalten standardmäßig die folgenden Schaltflächen:

- **Aktualisieren der Anzeige mit "Aktualisieren"**
  WBM-Seiten, die aktuelle Parameter anzeigen, haben am unteren Rand die Schaltfläche "Aktualisieren". Klicken Sie auf diese Schaltfläche, wenn Sie für die angezeigte Seite aktuelle Daten vom Gerät anfordern wollen.

  **Hinweis**

  Wenn Sie auf die Schaltfläche "Aktualisieren" klicken, bevor Sie Ihre Konfigurationsänderungen mit Hilfe der Schaltfläche "Einstellungen übernehmen" auf das Gerät übertragen haben, dann werden Ihre Änderungen gelöscht und die bisherige Konfiguration wird aus dem Gerät geladen und hier angezeigt.

- **Speichern von Einträgen mit "Einstellungen übernehmen"**
  WBM-Seiten, auf denen Sie Konfigurationseinstellungen festlegen können, haben am unteren Rand die Schaltfläche "Einstellungen übernehmen". Die Schaltfläche wird erst aktiv, wenn Sie auf der Seite mindestens einen Wert ändern. Klicken Sie auf die Schaltfläche, um eingegebene Konfigurationsdaten im Gerät zu speichern. Nach dem Speichern ist die Schaltfläche wieder inaktiv.

  **Hinweis**

  Das Ändern der Konfigurationsdaten ist nur mit der Rolle "admin" möglich.

  **Hinweis**

  Die Änderungen sind sofort wirksam. Aber es dauert einige Zeit, bis die Änderungen in der Konfiguration abgespeichert sind.

- **Anlegen von Einträgen mit "Erstellen"**
  WBM-Seiten, auf denen Sie neue Einträge erstellen können, haben am unteren Rand die Schaltfläche "Erstellen". Klicken Sie auf diese Schaltfläche, um einen neuen Eintrag zu erstellen.
- **Löschen von Einträgen mit "Löschen"**
  WBM-Seiten, auf denen Sie Einträge löschen können, haben am unteren Rand die Schaltfläche "Löschen". Klicken Sie auf diese Schaltfläche, um die zuvor markierten Einträge aus dem Gerätespeicher zu löschen. Der Löschvorgang bewirkt auch eine Aktualisierung der Seite im WBM.

- **Vorwärts blättern mit "Weiter"**
  Auf WBM-Seiten mit sehr vielen Datensätzen ist die Anzahl der auf einer Seite darstellbaren Datensätze beschränkt. Klicken Sie auf die Schaltfläche "Weiter", um innerhalb der Datensätze vorwärts zu blättern.
- **Rückwärts blättern mit "Zurück"**
  Bei WBM-Seiten mit sehr vielen Datensätzen ist die Anzahl der auf einer Seite darstellbaren Datensätze beschränkt. Klicken Sie auf die Schaltfläche "Zurück", um innerhalb der Datensätze rückwärts zu blättern.
- **Löschen der Anzeige mit "Leeren"**
  Bei Seiten mit Ablaufprotokollen können Sie alle Tabelleneinträge gleichzeitig löschen, unabhängig davon, ob Filter ausgewählt sind. Die Anzeige wird dabei geleert. Erst wenn nach dem Wiederherstellen der Werkseinstellungen das Gerät neu gestartet ist, wird der Neustart-Zähler zurückgesetzt.
  Klicken Sie auf die Schaltfläche "Leeren", um den Datensatz komplett zu löschen.
- **Schaltfläche "Alle anzeigen"**
  Bei Seiten mit sehr vielen Datensätzen können Sie alle Einträge anzeigen lassen. Klicken Sie auf die Schaltfläche "Alle anzeigen", um alle Einträge auf der Seite anzuzeigen. Beachten Sie, dass das Anzeigen aller Meldungen einige Zeit beanspruchen kann.
- **Klappliste für Seitenwechsel**
  Bei Seiten mit sehr vielen Datensätzen können Sie zur gewünschten Seite navigieren. Wählen Sie aus der Klappliste die betreffende Seite aus, um diese anzeigen zu lassen.
- **Schaltfläche "Zähler zurücksetzen"**
  Klicken Sie auf "Zähler zurücksetzen", um alle Zähler zurückzusetzen. Die Zähler werden durch einen Neustart zurückgesetzt.

## Abmeldung

Sie können sich auf jeder WBM-Seite abmelden, indem Sie auf den Link "Abmelden" klicken.

## Meldungen

Wenn Sie die Betriebsart "Automatisches Speichern" aktiviert haben und einen Parameter ändern, erscheint im Anzeigebereich folgende Meldung "Die Änderungen werden automatisch in x Sekunden gespeichert. Um die Änderungen sofort zu speichern, klicken Sie auf 'Schreiben der Startkonfiguration'."

**Hinweis**

**Unterbrechung des Speichervorgangs**

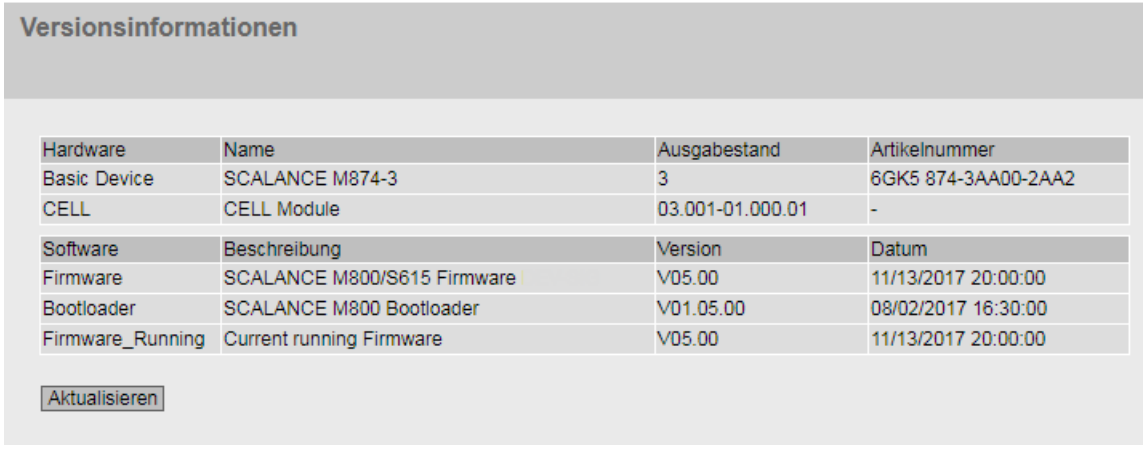
Der Speichervorgang startet erst, nachdem der Timer in der Meldung abgelaufen ist. Die Dauer des Speichervorgangs ist vom Gerät abhängig.

Während des Speichervorgangs wird die Meldung "Die Konfigurationsdaten werden gespeichert. Schalten Sie das Gerät nicht aus." angezeigt.

- Schalten Sie das Gerät nicht sofort aus, nachdem der Timer abgelaufen ist.

## 5.4.2 Versionen

Die WBM-Seite zeigt die Ausgabestände der Hardware und der Software für das Gerät an.




### Beschreibung

Die Tabelle 1 gliedert sich in folgende Spalten:

- **Hardware**
  - Basic Device
    Zeigt das Grundgerät an
  - CELL (nur bei M87x / MUM85x)
    Zeigt das verwendete Funkmodul an.
  - xDSL (nur bei M81x)
    Zeigt das verwendete DSL-Modul
- **Name**
  Zeigt den Namen des Geräts.
- **Ausgabestand**
  Zeigt den Hardware-Ausgabestand des Geräts an.
- **Artikelnummer**
  Zeigt die Artikelnummer des Geräts an.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Software**
  - Firmware
    Zeigt die aktuelle Firmware-Version an. Wenn eine neue Firmware-Datei geladen wurde und das Gerät noch nicht neu gestartet ist, wird hier die Firmware-Version der geladenen Firmware-Datei angezeigt. Nach dem nächsten Neustart wird die geladene Firmware aktiviert und verwendet.
  - Bootloader
    Zeigt die Version der Boot-Software an, die im Gerät gespeichert ist.
  - Firmware_Running
    Zeigt die Firmware-Version an, die aktuell vom Gerät verwendet wird.
- **Beschreibung**
  Zeigt die Kurzbeschreibung der Software an.
- **Version**
  Zeigt die Versionsnummer des Software-Ausgabestands an.
- **Datum**
  Zeigt das Erstellungsdatum des Software-Ausgabestands an.

## 5.4.3 Identification & Maintenance

### Hersteller- und Wartungsdaten

Diese Seite beinhaltet Informationen zu gerätespezifischen Hersteller- und Wartungsdaten wie Bestellnummer, Seriennummer, Versionsnummern etc. Sie können auf dieser Seite keine Konfigurationen vornehmen.




### Beschreibung der angezeigten Werte

Die Tabelle gliedert sich in folgende Zeilen:

- **Hersteller-ID**
  Zeigt die Herstellerkennung an.
- **Artikelnummer**
  Zeigt die Artikelnummer an.
- **Seriennummer**
  Zeigt die Seriennummer an.
- **Hardware-Ausgabestand**
  Zeigt den Hardware-Ausgabestand an.
- **Software-Ausgabestand**
  Zeigt den Software-Ausgabestand an.
- **Versionszähler**
  Unabhängig von einer Versionsänderung, zeigt dieses Feld immer den Wert "0" an.
- **Aktualisierungsdatum**
  Datum und Uhrzeit der letzten Versionsänderung

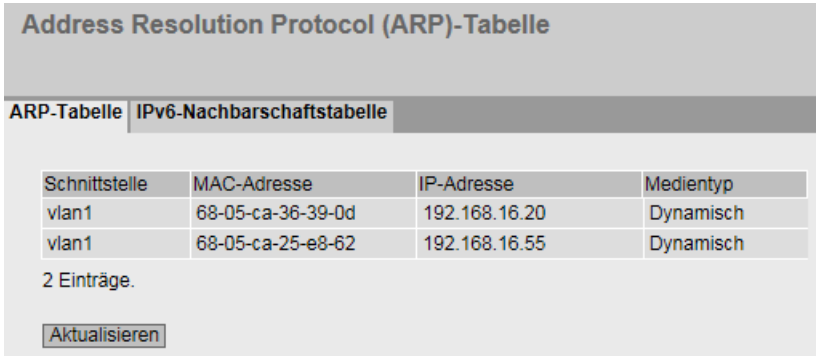
- **Funktionskennzeichen**
  Zeigt das Funktionskennzeichen (Anlagenkennzeichen) des Geräts an. Das Anlagenkennzeichen (AKZ) wird bei der Projektierung des Geräts mit HWKonfig von STEP7 angelegt.
- **Ortskennzeichen**
  Zeigt das Ortskennzeichen des Geräts an. Das Ortskennzeichen (OKZ) wird bei der Projektierung des Geräts mit HWKonfig von STEP7 angelegt.
- **Datum**
  Zeigt das Datum, das bei der Projektierung des Geräts mit HWKonfig von STEP7 angelegt wurde.
- **Deskriptor**
  Zeigt die Beschreibung, die bei der Projektierung des Geräts mit HWKonfig von STEP7 angelegt wurde.

## 5.4.4 ARP / Nachbarn

### 5.4.4.1 ARP-Tabelle

#### Zuordnung von MAC-Adresse und IPv4-Adresse

Über das Address Resolution Protocol (ARP) erfolgt die eindeutige Zuordnung von MAC-Adresse zu IPv4-Adresse. Diese Zuordnung wird von jedem Netzteilnehmer in seiner eigenen ARP-Tabelle gepflegt. Die WBM-Seite zeigt die ARP-Tabelle des Geräts.




#### Beschreibung der angezeigten Werte

Die Tabelle gliedert sich in folgende Spalten:

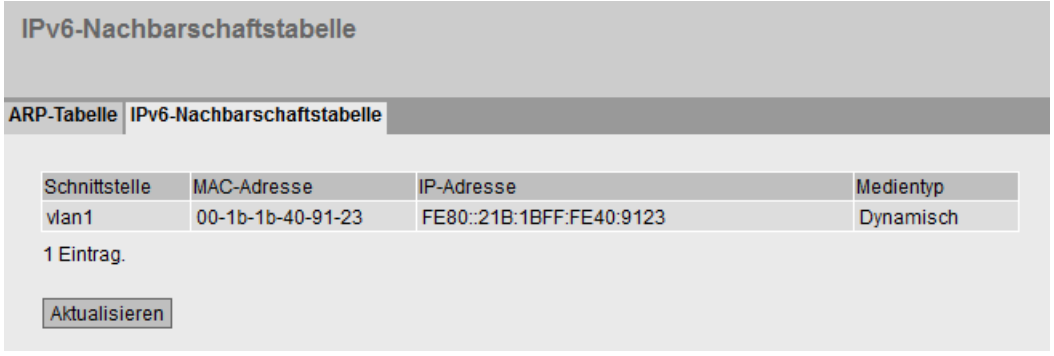
- **Schnittstelle**
  Zeigt die Schnittstelle an, über die der Zeileneintrag gelernt wurde.
- **MAC-Adresse**
  Zeigt die MAC-Adresse des Ziel- oder Quellgeräts an.

- **IP-Adresse**
  Zeigt die IPv4-Adresse des Zielgeräts an.
- **Medientyp**
  Zeigt die Art der Verbindung.
  - Dynamisch
    Das Gerät hat die Adressdaten automatisch erkannt.
  - Statisch
    Die Adressen wurden als statische Adressen eingetragen.

### 5.4.4.2 IPv6-Nachbarschaftstabelle

#### Zuordnung von MAC-Adresse und IPv6-Adresse

Über die IPv6-Nachbarschaftstabelle erfolgt die eindeutige Zuordnung von MAC-Adresse zu IPv6-Adresse. Diese Zuordnung wird von jedem Netzteilnehmer in seiner eigenen Nachbarschaftstabelle gepflegt.




#### Beschreibung der angezeigten Werte

Die Tabelle gliedert sich in folgende Spalten:

- **Schnittstelle**
  Zeigt die Schnittstelle an, über die der Zeileneintrag gelernt wurde.
- **MAC-Adresse**
  Zeigt die MAC-Adresse des Ziel- oder Quellgeräts an.
- **IP-Adresse**
  Zeigt die IPv6-Adresse des Zielgeräts an.
- **Medientyp**
  Zeigt die Art der Verbindung.
  - Dynamisch
    Das Gerät hat die Adressdaten automatisch erkannt.
  - Statisch
    Die Adressen wurden als statische Adressen eingetragen.

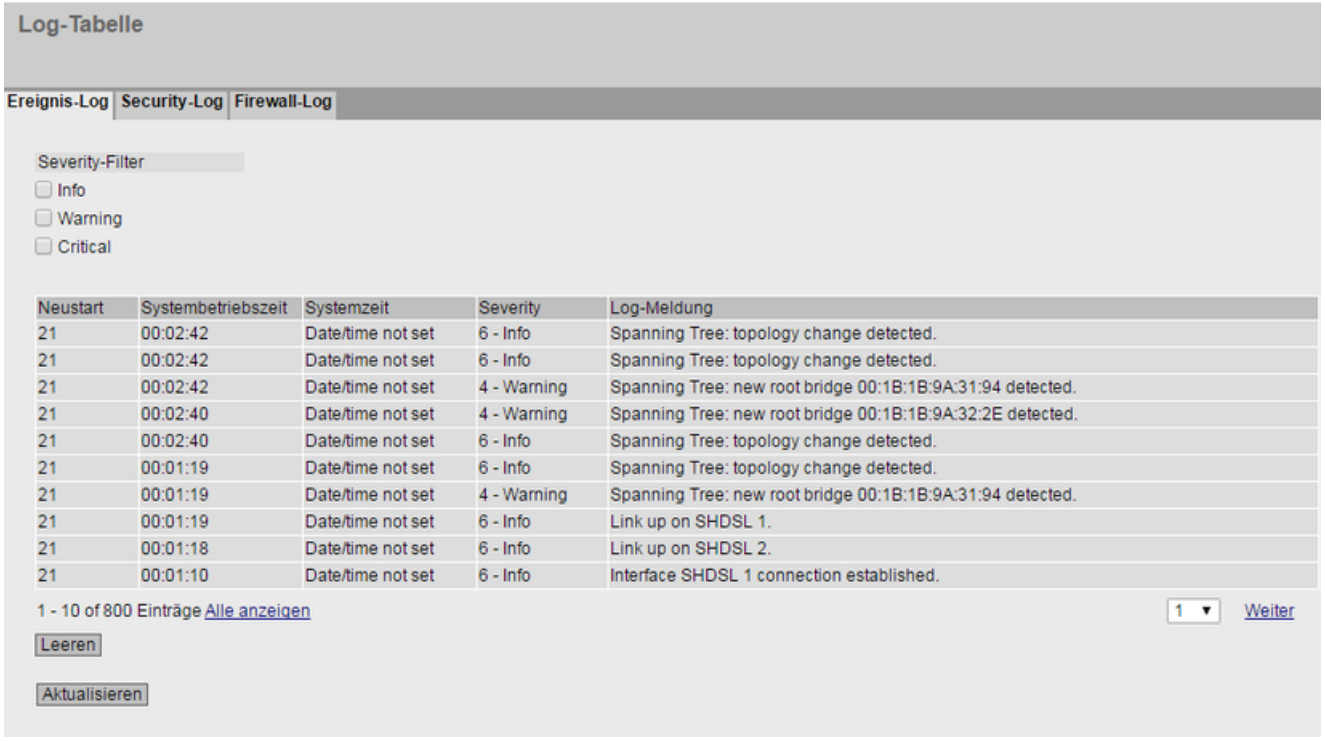
## 5.4.5 Log-Tabellen

### 5.4.5.1 Ereignis-Log

#### Protokollierung von Ereignissen

Die WBM-Seite zeigt in tabellarischer Form die aufgetretenen Systemereignisse an. Einige der Systemereignisse sind unter "System > Ereignisse" konfigurierbar, z. B. wann sich der Verbindungsstatus eines Ports geändert hat.

Der Inhalt der Tabelle bleibt auch nach dem Ausschalten des Gerätes erhalten. Die Ereignisprotokolldatei können Sie über HTTP, TFTP oder SFTP herunterladen.



## Beschreibung

- **Severity-Filter**
  Die Einträge der Tabelle können Sie nach Schweregrad filtern. Um alle Einträge anzuzeigen, aktivieren oder deaktivieren Sie alle Parameter.

  **Hinweis**

  Pro Severity sind maximal 800 Einträge in der Tabelle möglich. Wenn bei einer Severity die maximale Anzahl der Einträge erreicht ist, werden die ältesten Einträge dieser Severity in der Tabelle überschrieben. Die Tabelle verbleibt permanent im Speicher.

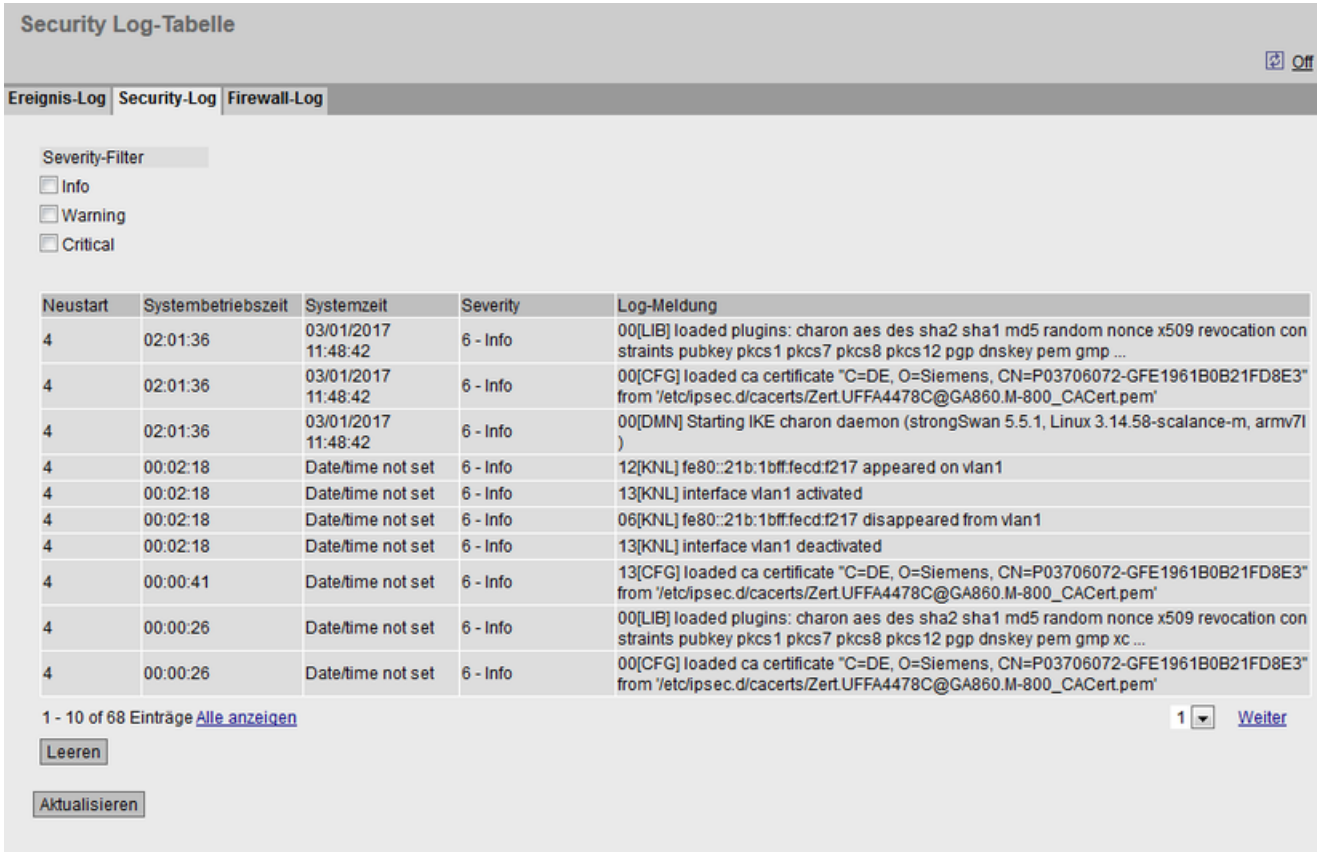
  - Critical
    kritisch
    Wenn dieser Parameter aktiviert ist, werden alle Einträge der Kategorien "Critical" angezeigt.
  - Warning
    warnend
    Wenn dieser Parameter aktiviert ist, werden alle Einträge der Kategorien "Warning" angezeigt.
  - Info
    informativ
    Wenn dieser Parameter aktiviert ist, werden alle Einträge der Kategorien "Info" angezeigt.

Die Tabelle gliedert sich in folgende Spalten:

- **Neustart**
  Zählt die Anzahl der Neustarts seit dem letzten Zurücksetzen auf Werkseinstellungen und gibt an, nach welchem Neustart des Geräts das entsprechende Ereignis eingetreten ist.
- **Systembetriebszeit**
  Zeigt die Laufzeit des Geräts seit dem letzten Neustart an, zu der das beschriebene Ereignis eingetreten ist.
- **Systemzeit**
  Zeigt das Datum und die Uhrzeit an, zu der das beschriebene Ereignis aufgetreten ist. Wenn keine Systemzeit eingestellt ist, enthält das Feld die Angabe "Date/time not set"
- **Severity**
  Einordnung des Eintrags in obige Kategorien.
- **Log-Meldung**
  Zeigt eine Kurzbeschreibung des eingetretenen Ereignisses an.

### 5.4.5.2 Security-Log

Die WBM-Seite zeigt in tabellarischer Form die Ereignisse an, die bei der Kommunikation über einen gesicherten VPN-Tunnel aufgetreten sind.



## Beschreibung

- **Severity-Filter**
  Die Einträge der Tabelle können Sie nach Schweregrad filtern. Um alle Einträge anzuzeigen, aktivieren oder deaktivieren Sie alle Parameter.

  **Hinweis**

  Pro Severity sind maximal 800 Einträge in der Tabelle möglich. Wenn bei einer Severity die maximale Anzahl der Einträge erreicht ist, werden die ältesten Einträge dieser Severity in der Tabelle überschrieben. Die Tabelle verbleibt permanent im Speicher.

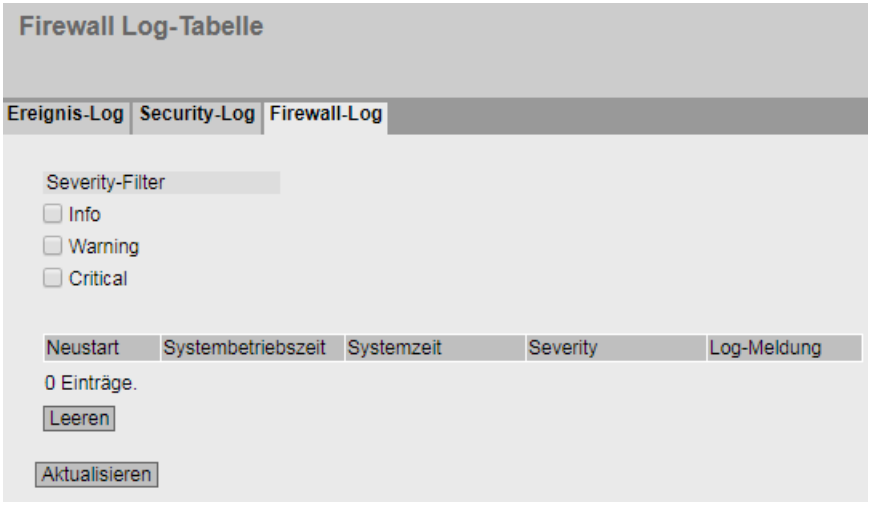
  - Critical
    kritisch
    Wenn dieser Parameter aktiviert ist, werden alle Einträge der Kategorien "Critical" angezeigt.
  - Warning
    warnend
    Wenn dieser Parameter aktiviert ist, werden alle Einträge der Kategorien "Warning" angezeigt.
  - Info
    informativ
    Wenn dieser Parameter aktiviert ist, werden alle Einträge der Kategorien "Info" angezeigt.

Die Tabelle gliedert sich in folgende Spalten:

- **Neustart**
  Zählt die Anzahl der Neustarts seit dem letzten Zurücksetzen auf Werkseinstellungen und gibt an, nach welchem Neustart des Geräts das entsprechende Ereignis eingetreten ist.
- **Systembetriebszeit**
  Zeigt die Laufzeit des Geräts seit dem letzten Neustart an, zu der das beschriebene Ereignis eingetreten ist.
- **Systemzeit**
  Zeigt das Datum und die Uhrzeit an, zu der das beschriebene Ereignis aufgetreten ist. Wenn keine Systemzeit eingestellt ist, enthält das Feld die Angabe "Date/time not set"
- **Severity**
  Einordnung des Eintrags in obige Kategorien.
- **Log-Meldung**
  Zeigt eine Kurzbeschreibung des eingetretenen Ereignisses an.

### 5.4.5.3 Firewall-Log

Das Firewall-Logbuch protokolliert die Ereignisse, die an der Firewall eingetreten sind. Beim Anlegen von Firewall-Regeln können Sie festlegen, mit welcher Ereignisschwere diese protokolliert werden.




## Beschreibung

- **Severity-Filter**
  Die Einträge der Tabelle können Sie nach Schweregrad filtern. Um alle Einträge anzuzeigen, aktivieren oder deaktivieren Sie alle Parameter.

  **Hinweis**

  Pro Severity sind maximal 800 Einträge in der Tabelle möglich. Wenn bei einer Severity die maximale Anzahl der Einträge erreicht ist, werden die ältesten Einträge dieser Severity in der Tabelle überschrieben. Die Tabelle verbleibt permanent im Speicher.

  - Critical
    kritisch
    Wenn dieser Parameter aktiviert ist, werden alle Einträge der Kategorien "Critical" angezeigt.
  - Warning
    warnend
    Wenn dieser Parameter aktiviert ist, werden alle Einträge der Kategorien "Warning" angezeigt.
  - Info
    informativ
    Wenn dieser Parameter aktiviert ist, werden alle Einträge der Kategorien "Info" angezeigt.

Die Tabelle gliedert sich in folgende Spalten:

- **Neustart**
  Zählt die Anzahl der Neustarts seit dem letzten Zurücksetzen auf Werkseinstellungen und gibt an, nach welchem Neustart des Geräts das entsprechende Ereignis eingetreten ist.
- **Systembetriebszeit**
  Zeigt die Laufzeit des Geräts seit dem letzten Neustart an, zu der das beschriebene Ereignis eingetreten ist.
- **Systemzeit**
  Zeigt das Datum und die Uhrzeit an, zu der das beschriebene Ereignis aufgetreten ist. Wenn keine Systemzeit eingestellt ist, enthält das Feld die Angabe "Date/time not set"
- **Severity**
  Einordnung des Eintrags in obige Kategorien.
- **Log-Meldung**
  Zeigt eine Kurzbeschreibung des eingetretenen Ereignisses an.

## 5.4.6 Fehler

### Fehlerstatus

Wenn ein Fehler auftritt, wird er auf dieser Seite angezeigt. Am Gerät werden Fehler dadurch signalisiert, dass die rote Fehler-LED leuchtet.

Gemeldet werden interne Fehler des Geräts sowie Fehler, die Sie auf folgenden Seiten konfigurieren:

- "System > Ereignisse"
- "System > Fehlerkontrolle"

Die Berechnung des Fehlerzeitpunkts beginnt jeweils nach dem letzten Systemstart. Wenn keine Fehler vorliegen, schaltet sich die Fehler-LED ab.



### Beschreibung

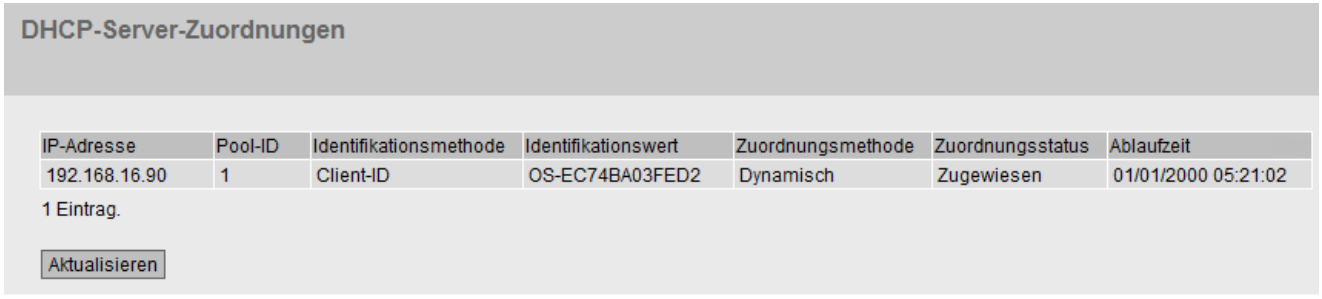
- **Anzahl der gemeldeten Fehler**
  Zeigt an, wie oft die Fehler-LED eingeschaltet wurde und nicht wie viele Fehler aufgetreten sind.

Die Tabelle enthält die folgenden Spalten:

- **Fehlerzeitpunkt**
  Zeigt die Laufzeit des Geräts seit dem letzten Systemstart an, zu der der beschriebene Fehler aufgetreten ist.
- **Fehlerbeschreibung**
  Zeigt eine Kurzbeschreibung des aufgetretenen Fehlers an.
- **Fehlerstatus löschen**
  Manche Fehler lassen sich quittieren und damit aus der Fehlerliste entfernen, z. B. ein Fehler des Ereignisses "Kalt-/Warmstart". Wenn die Schaltfläche "Fehlerstatus löschen" aktiv ist, können Sie den Fehler löschen.

## 5.4.7 DHCP-Server

Diese Seite zeigt an, welche IPv4-Adressen den Geräten vom DHCP-Server zugeordnet wurden.



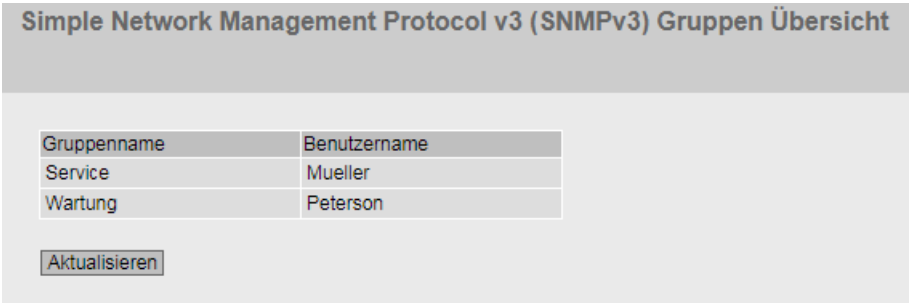

### Beschreibung der angezeigten Werte

- **IP-Adresse**
  Zeigt die IPv4-Adresse an, die dem DHCP-Client zugeordnet ist.
- **Pool-ID**
  Zeigt die Nummer des IPv4-Adressbands an.

- **Identifikationsmethode**
  Zeigt die Methode an, nach der der DHCP-Client identifiziert wird.
  - MAC-Adresse
    Die Identifikation läuft über die MAC-Adresse ab.
  - DHCP-Client-ID
    Die Identifikation läuft über eine frei definierte DHCP-Client-ID ab.
  - Systemnamen
    Die Identifikation läuft über den Systemnamen ab. Ist der Systemname 255 Zeichen lang, dann wird das letzte Zeichen nicht zur Identifikation benutzt.
  - IAID und DUID
    Damit kann sich der DHCP-Client an DHCP-Servern anmelden, die den Parallelbetrieb von IPv4-und IPv6 unterstützten.
    Die Identifikation läuft über die IAID und die DUID ab und bezeichnet genau eine IP-Schnittstelle des Geräts.
- **Identifikationswert**
  Zeigt den Wert an, der der Identifikationsmethode zugeordnet ist.
- **Zuordnungsmethode**
  Zeigt an, ob die IPv4-Adresse statisch oder dynamisch vergeben wurde. Die statischen Einträge konfigurieren Sie unter "System > DHCP > Statische Zuordnung".
- **Zuordnungsstatus**
  Zeigt den Status der Zuordnung an.
  - Zugeordnet
    Die Zuordnung wird verwendet.
  - Nicht verwendet
    Die Zuordnung wird nicht verwendet.
  - Wird geprüft
    Die Zuordnung wird geprüft.
  - Unbekannt
    Der Status der Zuordnung ist unbekannt.
- **Ablaufzeit**
  Zeigt an, wie lange die vergebene IPv4-Adresse noch gültig ist. Nachdem die Gültigkeitsdauer zur Hälfte abgelaufen ist, kann der DHCP-Client die vergebene IPv4-Adresse verlängern. Nach Ablauf der gesamten Zeitdauer muss der DHCP-Client eine neue IPv4-Adresse anfordern.

## 5.4.8 SNMP

Diese Seite zeigt die angelegten SNMPv3-Gruppen an. Die SNMPv3-Gruppen konfigurieren Sie unter "System > SNMP".




### Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

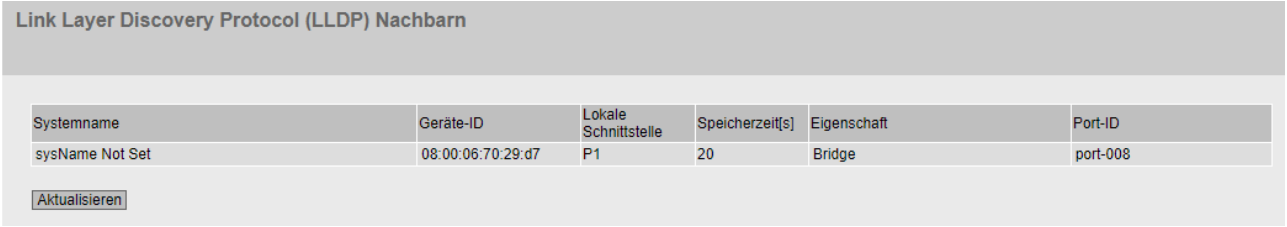
- **Gruppenname**
  Zeigt den Gruppennamen an.
- **Benutzername**
  Zeigt den Benutzer an, welcher der Gruppe zugeordnet ist.

## 5.4.9 LLDP

### Status der Nachbarschaftstabelle

Diese Seite zeigt den aktuellen Inhalt der Nachbarschaftstabelle. In dieser Tabelle sind die Informationen gespeichert, die der LLDP-Agent von angeschlossenen Geräten empfangen hat.

Über welche Schnittstellen der LLDP-Agent Informationen empfängt bzw. versendet, legen Sie in folgendem Kapitel fest: "Layer 2 > LLDP".



## Beschreibung

Die Tabelle enthält folgende Spalten:

- **Systemname**
  Systemname des angeschlossenen Geräts.
- **Geräte-ID**
  Gerätekennung des angeschlossenen Geräts. Die Geräte-ID entspricht dem Gerätenamen, der über SINEC PNI (STEP 7) vergeben wird. Wenn kein Gerätename vergeben ist, wird die MAC-Adresse des Geräts angezeigt.
- **Lokale Schnittstelle**
  Der Port, an dem das Gerät die Informationen empfangen hat.
- **Speicherzeit[s]**
  Speicherzeit in Sekunden
  Ein Eintrag bleibt für die hier angegebene Zeit im Gerät gespeichert. Wenn das Gerät in dieser Zeit keine neuen Informationen von dem angeschlossenen Gerät erhält, wird der Eintrag gelöscht.
- **Eigenschaft**
  Zeigt die Eigenschaften des angeschlossenen Geräts an:
  - Router
  - Bridge
  - Telephone
  - DOCSIS Cable Device
  - WLAN Access Point
  - Repeater
  - Station
  - Other
- **Port-ID**
  Port des angeschlossenen Geräts, mit dem das Gerät verbunden ist. Wenn keine Port-ID vergeben ist, wird die MAC-Adresse des angeschlossenen Geräts angezeigt.

## 5.4.10 IPv4-Routing

### Einleitung

Diese Seite zeigt die Routen an, die aktuell verwendet werden.




### Beschreibung

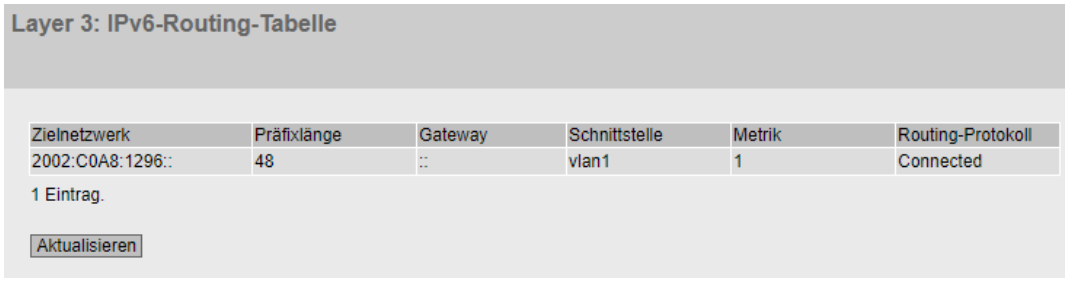
Die Tabelle gliedert sich in folgende Spalten:

- **Zielnetzwerk**
  Zeigt die Zieladresse dieser Route an.
- **Subnetzmaske**
  Zeigt die Subnetzmaske dieser Route an.
- **Gateway**
  Zeigt das Gateway für diese Route an.
- **Schnittstelle**
  Zeigt die Schnittstelle für diese Route an.
- **Metrik**
  Zeigt die Metrik der Route an. Je größer der Wert, desto länger benötigen Pakete zu Ihrem Ziel.
- **Routing-Protokoll**
  Zeigt an, aus welchem Routing-Protokoll der Eintrag der Routingtabelle stammt. Folgende Einträge sind möglich:
  - Connected: Verbundene Routen
  - Static: Statische Routen
  - DHCP: Route über DHCP

## 5.4.11 IPv6-Routing

### Einleitung

Diese Seite zeigt die IPv6-Routen an, die aktuell verwendet werden.




### Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Zielnetzwerk**
  Zeigt die Ziel-Adresse dieser Route an.
- **Präfixlänge**
  Zeigt die Präfixlänge dieser Route an.
- **Gateway**
  Zeigt das Gateway für diese Route an.
- **Schnittstelle**
  Zeigt die Schnittstelle für diese Route an.
- **Metrik**
  Zeigt die Metrik der Route an. Je größer der Wert, desto länger benötigen Pakete zu Ihrem Ziel.
- **Routing-Protokoll**
  Zeigt an, aus welchem Routing-Protokoll der Eintrag der Routingtabelle stammt. Folgende Einträge sind möglich:
  - Connected: Verbundene Routen
  - Static: Statische Routen
  - RIPng: Routen über RIPng
  - OSPFv3: Routen über OSPFv3
  - Other: Sonstige Routen

## 5.4.12 Mobilfunk

### 5.4.12.1 Übersicht

M87x MUM85x

Die WBM-Seite zeigt einen Überblick über den aktuellen Betriebsstatus des Geräts.




## Beschreibung der angezeigten Werte

Die Seite enthält Folgendes:

- **IMEI**
  Zeigt die IMEI-Nummer des verwendeten Funkmoduls an.
  Die IMEI (= International Mobile Equipment Identity) wird weltweit eindeutig vergeben.
- **SIM-Status**
  Zeigt den Status der SIM-Karte an.
  - Vorhanden
    SIM-Karte vorhanden
  - Fehlend
    SIM-Karte fehlt

- **PIN-Status**
  Zeigt den Status der PIN an.
  - PIN erforderlich
    PIN muss noch eingegeben werden.
  - Keine PIN erforderlich
    PIN wird nicht benötigt.
  - PUK erforderlich
    SIM-Karte gesperrt. Mit der PUK kann die Karte wieder entsperrt werden.
  - Falsche PIN
    Die PIN ist falsch.
  - PIN gültig
    Die PIN ist gültig.
- **IMSI**
  Zeigt die Teilnehmerkennung an, die auf der verwendeten SIM-Karte gespeichert ist.
- **Rufnummer**
  Zeigt die Rufnummer der SIM-Karte an.
  Wenn die Rufnummer nicht vorhanden ist oder nicht ausgelesen werden kann, wird "no number" angezeigt.
- **Verbindungsstatus**
  Zeigt an, ob eine Funkverbindung besteht, und falls ja, welche:
  - UMTS: IP-Verbindung über UMTS oder HSPA
  - GPRS: IP-Verbindung über EGPRS, GPRS oder LTE
- **Telegramm Switch-Status**
  Zeigt den Status der Paketvermittlung an.
- **Funkzellen-ID**
  Zeigt die Kennung der Funkzelle an, in welches sich das Gerät eingebucht hat.
- **LAC (Location Area Code)**
  Zeigt die Kennung für den aktuellen Aufenthaltsbereich des M87x innerhalb des Mobilfunknetzes an.
- **Signalstärke**
  Zeigt die Signalstärke an.
  - Signalstärke bei SCALANCE M87x:

    | dBm | Signalstärke |
    |---|---|
    | < -109 | Keine Verbindung |
    | -109 ... -89 | Schlechte Signalstärke |
    | -89 ...-73 | Mittlere Signalstärke |
    | > -73 | Gute Signalstärke |

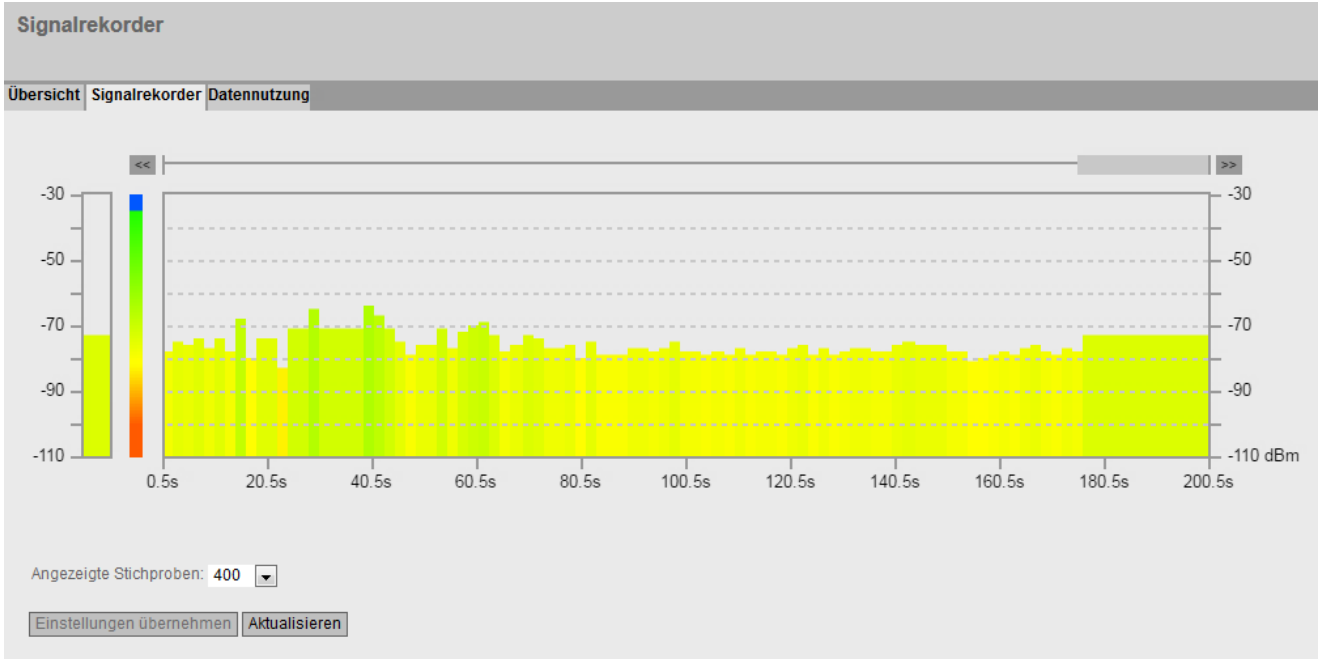
  - Signalstärke bei SCALANCE MUM85x:
    Kein Empfang / sehr schlecht / schlecht / mittel / gut / sehr gut
- **Mobilfunk Chip-Temperatur**
  Zeigt die aktuelle Temperatur des verbauten Chips an.

- **Anbieter**
  Zeigt den Mobilfunkbetreiber an.
- **APN**
  Zeigt den verwendeten APN (Access Point Name) der Funkverbindung an.
- **Externe IP-Adresse**
  Zeigt die WAN-IP-Adresse an, unter der das Gerät im Mobilfunknetz zu erreichen ist. Die WAN-IP-Adresse wird dem Gerät vom Dienst des Mobilfunkbetreibers zugewiesen.
- **DNS-Server**
  Zeigt den oder die vom Gerät verwendeten DNS-Server an.

### 5.4.12.2 Signalrekorder

M87x | MUM85x

Mit dem Signalrekorder wird die Signalstärke zur Funkzelle angezeigt, in der das Gerät eingebucht ist.




#### Beschreibung der angezeigten Werte

Die Grafik enthält die folgenden Elemente:

- Scrollbalken
  Mit dem Scrollbalken können Sie die gesamte Messung durchschauen. Dafür können Sie die Schaltflächen "<<" und ">>" oder die Pfeiltasten auf der Tastatur verwenden.
- Balken (links)
  In dem Balken auf der linken Seite wird die Signalstärke in Echtzeit angezeigt, entsprechend des abgebildeten Farbschemas.

- Farbschema
  Grün = Gut, Gelb = Mittel, Orange = Schwach, Rot = Sehr schwach
- x-Achse
  Die x-Achse zeigt den Verlauf der Messung in Sekunden.
- Verlaufsdaten
  Die Verlaufsdaten zeigen den Wert der Signalstärke entsprechend des abgebildeten Farbschemas.

**Angezeigte Stichproben**

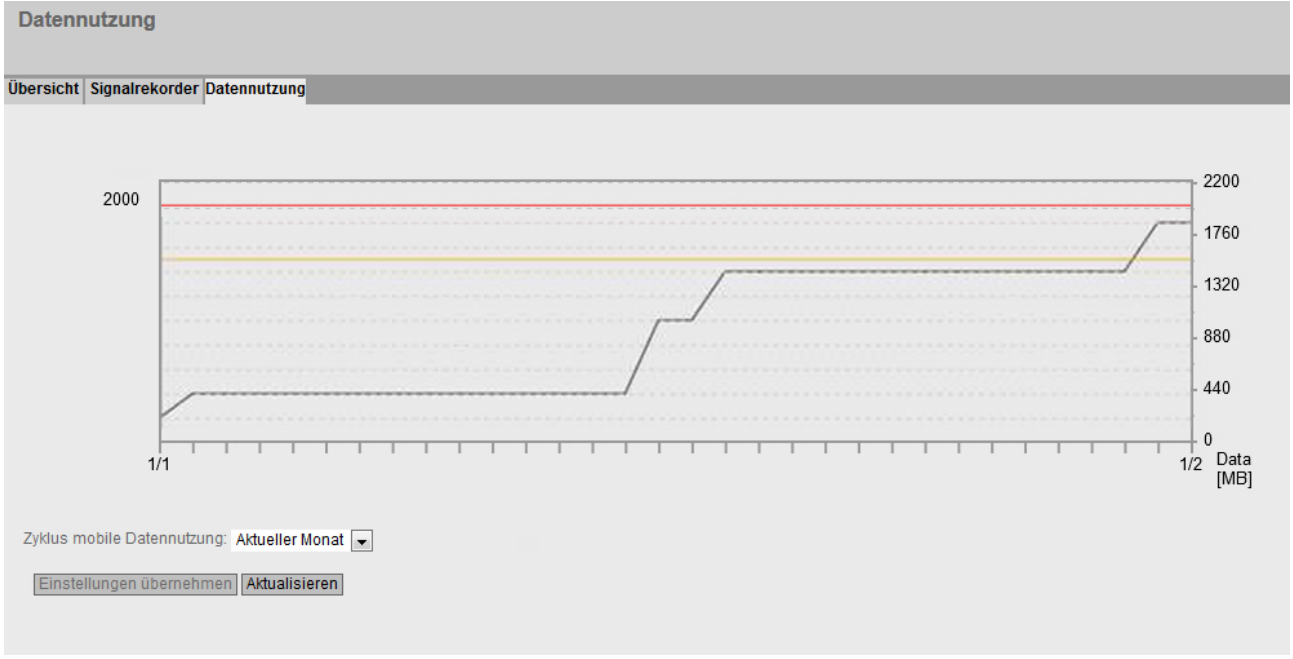
Wählen Sie aus, wie viele Messwerte in der Grafik angezeigt werden sollen.

### 5.4.12.3 Datennutzung

M87x | MUM85x

Auf dieser WBM-Seite wird das verbrauchte Datenvolumen in dem ausgewählten Monat angezeigt. Das Gerät berechnet die Datennutzung anhand der gezählten Datenpakete (Up- und Download) auf der WAN-Schnittstelle. Das ermittelte Datenvolumen kann aufgrund von Blockrundungen von der Abrechnung Ihres Mobilfunkanbieters abweichen.

Das verbrauchte Datenvolumen von 3 Monaten wird in den nicht-flüchtigen FLASH-Speicher des Geräts abgelegt. Die Werte werden in regelmäßigen Abständen oder bevor das Gerät herunterfährt gespeichert, aber nicht bei einem Spannungsausfall.




## Voraussetzung

- Unter "Schnittstellen > Mobile > Allgemein" ist die "Mobile Datennutzung" aktiviert.

### Beschreibung der angezeigten Werte

Die Grafik enthält die folgenden Elemente:

- x-Achse
  Einteilung des gewählten Monats in Tage.
- y-Achse
  Einteilung des festgelegten Datenvolumens.
- Linien
  - Rot: Das festgelegte Datenvolumen. Sie konfigurieren die Einstellung unter "Schnittstellen > Mobile > Allgemein".
  - Gelb: Entspricht 75 % des festgelegten Datenvolumens.
  - Schwarz: Das verbrauchte Datenvolumen.

**Zyklus mobile Datennutzung**

Wählen Sie den gewünschten Monat.

- Aktueller Monat
  Zeigt das bisher verbrauchte Datenvolumen.
- Letzter Monat / Vorletzter Monat
  Zeigt das gesamte verbrauchte Datenvolumen in dem gewünschten Monat.

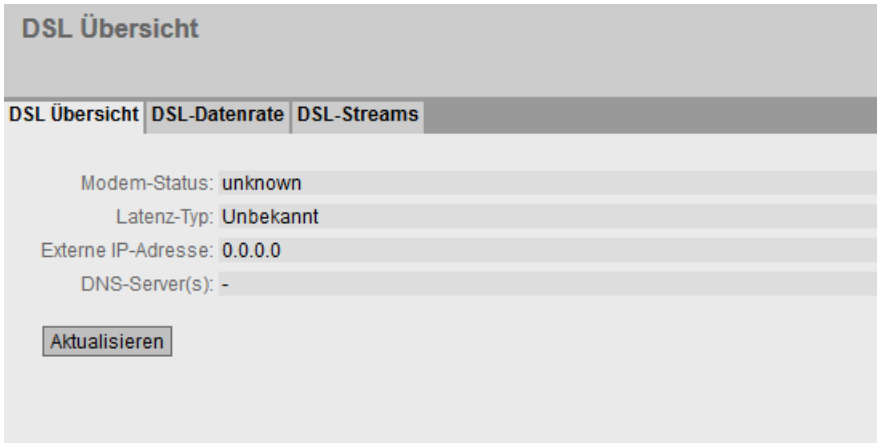
## 5.4.13 DSL

### 5.4.13.1 Übersicht

M81x

Eine ADSL-Verbindung besteht aus zwei Endpunkten, den sogenannten ADSL Transceiver Units (ATU). Die ADSL Transceiver Unit-Remote (ATU-R) ist dieses Gerät und die ADSL Transceiver Unit-Central (ATU-C) ist das Gerät in der Vermittlungsstelle.

Die WBM-Seite zeigt den aktuellen Betriebsstatus des Geräts und enthält Informationen zur ATU-C.




### Beschreibung der angezeigten Werte

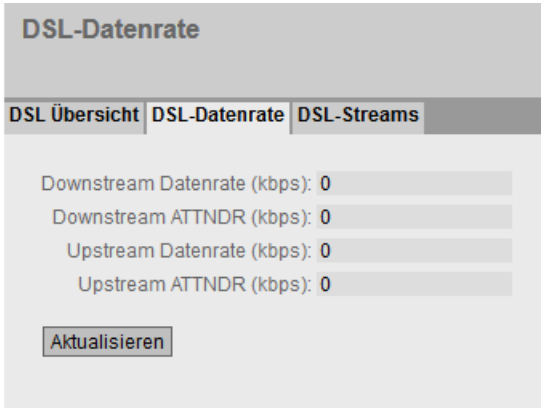
Die Seite enthält Folgendes:

- **Modem-Status**
  Zeigt den Status des Modems an.
  Z. B. beim Initialisieren und beim Aufbau der ADSL-Verbindung werden folgende Stati angezeigt:
  - showtime-sync
    ADSL-Verbindung ist aufgebaut. Datenverkehr möglich.
  - handshake
    ADSL-Verbindung wird geprüft und aufgebaut.
  - full-init
    Modem wird initialisiert.
  - silent
    Keine ADSL-Verbindung
- **Latenz-Typ**
  Zeigt an, welches Verfahren verwendet wird.
  - fast
    Fast Path: Kleine Antwortzeit. Geringere Störsicherheit.
  - slow
    Störsicherheit durch Interleaving. Beim Interleaving werden die Daten verschachtelt, dadurch verlängert sich die Antwortzeit.
  - unknown
    Verfahren unbekannt
- **Externe IP-Adresse**
  Zeigt die externe IP-Adresse an, unter der das Gerät zu erreichen ist. Die externe IP-Adresse wird dem Gerät vom Dienst des DSL-Anbieters zugewiesen.
- **DNS-Server**
  Zeigt den oder die vom Gerät verwendeten DNS-Server an

### 5.4.13.2 DSL-Datenrate

M81x

Die WBM-Seite enthält eine Übersicht der Datenübertragungsraten für die Empfangsrichtung (Downstream) und für die Senderichtung (Upstream).




#### Beschreibung der angezeigten Werte

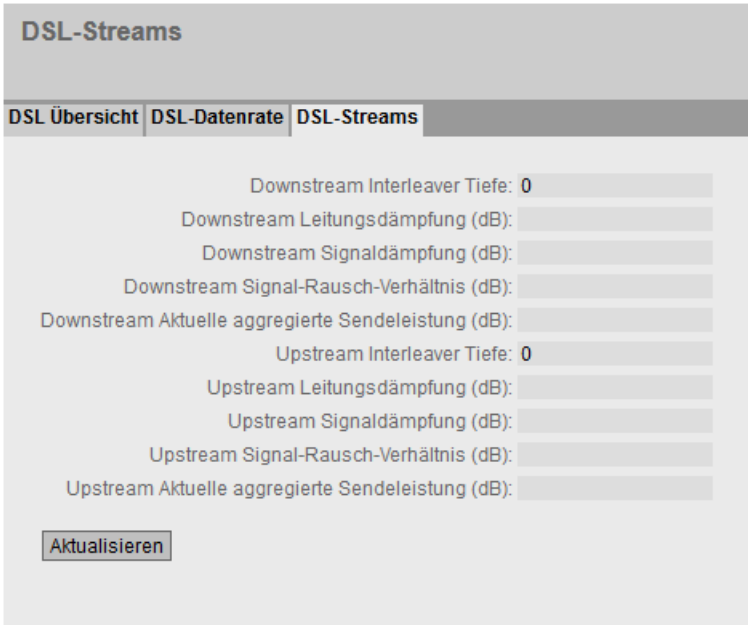
Die Seite enthält Folgendes:

- **Downstream Datenrate (kbps)**
  Zeigt die nutzbare Datenübertragungsrate für den Downstream an.
- **Downstream ATTNDR (kbps)**
  ATTNDR (Attainable data rate)
  Zeigt die maximal mögliche Datenübertragungsrate für den Downstream an.
- **Upstream Datenrate (kbps)**
  Zeigt die nutzbare Datenübertragungsrate für den Upstream an.
- **Upstream ATTNDR (kbps)**
  ATTNDR (Attainable data rate).
  Zeigt die maximal mögliche Datenübertragungsrate für den Upstream an.

### 5.4.13.3 Streams

M81x

Die WBM-Seite zeigt Parameter an, die die Datenübertragungsrate beeinflussen.




## Beschreibung der angezeigten Werte

Für die Empfangsrichtung (Downstream) werden folgende Werte angezeigt:

- **Downstream Interleaver-Tiefe**
  Zeigt an, mit welcher Tiefe die Daten verschachtelt werden. Je höher die Interleaving-Tiefe, desto länger die Antwortzeit.
- **Downstream Leitungsdämpfung [dB]**
  Zeigt die Leitungsdämpfung an. Die Leitungsdämpfung ist abhängig vom Leitungsdurchmesser und der Übertragungsfrequenz.
- **Downstream Signaldämpfung [dB]**
  Zeigt die Signaldämpfung an. Je kleiner der Wert, desto besser das Signal.
- **Downstream Signal-Rausch-Verhältnis[dB]**
  Zeigt das Signal-Rausch-Verhältnis an. Je größer der Wert, desto besser das Signal.
- **Downstream Aktuell aggregierte Sendeleistung [dB]**
  Zeigt die aktuelle Sendeleistung an, die im aggregierten Betrieb erreicht wird.

Für die Senderichtung (Upstream) werden folgende Werte angezeigt

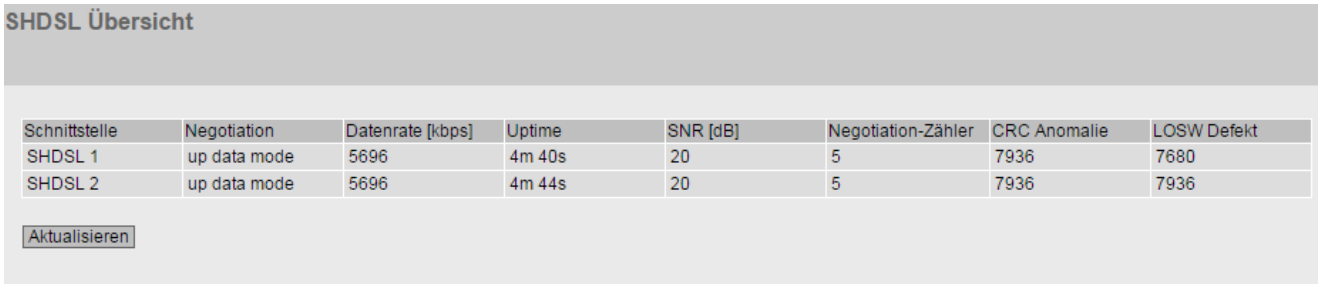
- **Upstream Interleaver -Tiefe**
  Zeigt an, mit welcher Tiefe die Daten verschachtelt werden. Je höher die Interleaving-Tiefe, desto länger die Antwortzeit.
- **Upstream Leitungsdämpfung [dB]**
  Zeigt die Leitungsdämpfung an. Die Leitungsdämpfung ist abhängig vom Leitungsdurchmesser und der Übertragungsfrequenz.
- **Upstream Signaldämpfung [dB]**
  Zeigt die Signaldämpfung an. Je kleiner der Wert, desto besser das Signal.

- **Upstream Signal-Rausch-Verhältnis [dB]**
  Zeigt das Signal-Rausch-Verhältnis an. Je größer der Wert, desto besser das Signal.
- **Upstream Aktuell aggregierte Sendeleistung [dB]**
  Zeigt die aktuelle Sendeleistung an, die im aggregierten Betrieb erreicht wird.

## 5.4.14 SHDSL

M826

Die WBM-Seite zeigt den Status der SHDSL-Schnittstelle an.




### Beschreibung der angezeigten Werte

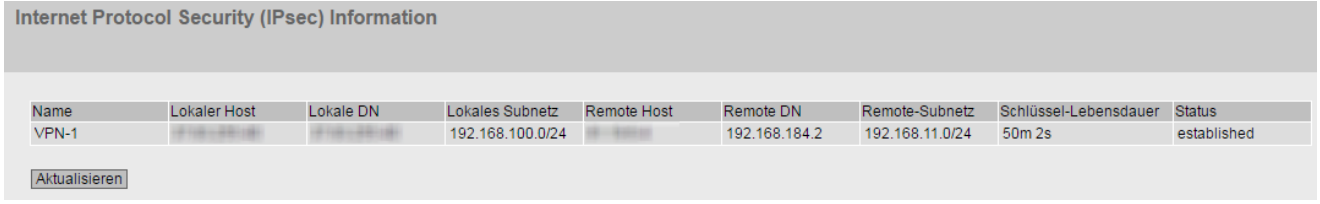
Die Tabelle enthält folgende Spalten:

- **Schnittstelle**
  Zeigt die SHDSL-Schnittstellen des Geräts.
- **Negotiation**
  Folgende Werte sind möglich:
  - down not ready (Nur bei der Rolle CO)
    Zum Kommunikationspartner ist keine elektrische Verbindung gesteckt. Der Treiber wird initialisiert und ist bereit zum Aushandeln der Verbindungsparameter.
  - down ready (nur bei der Rolle CPE)
    Zum Kommunikationspartner ist keine elektrische Verbindung gesteckt. Der Treiber wird initialisiert und ist bereit zum Aushandeln der Verbindungsparameter.
  - initialising
    Die Verbindungsparameter werden ausgehandelt.
  - up data mode
    Die Verbindungsparameter sind erfolgreich ausgehandelt. Die Datenübertragung ist möglich.
  - stop down ready
    Das Aushandeln der Verbindungsparameter war nicht erfolgreich oder die Verbindung wurde unterbrochen. Neuaushandlung der Parameter steht an.
  - unknown
    Die Treiberinitialisierung noch nicht abgeschlossen. Dieser Status tritt nach dem Gerätestart auf.

- **Datenrate [kbps]**
  Zeigt die nutzbare Datenübertragungsrate an.
- **Betriebszeit**
  Zeigt die Zeit seit dem letzten Aushandeln der Verbindungsparameter bzw. der letzten Verbindungsunterbrechung an.
- **SNR [dB]**
  Zeigt das Signal-Rausch-Verhältnis an. Je größer der Wert, desto besser das Signal.
- **CRC Anomalie**
  Cyclic Redundancy Check
  Zeigt an, wie viele SHDSL-Netzwerkpakete mit fehlerhafter Prüfsumme (CRC) entdeckt wurden.
- **LOSW Defekt**
  Loss of Synchronization Word
  Zeigt an, wie oft die Synchronisation auf der SHDSL-Verbindung verloren ging.
- **Negotiation-Zähler**
  Zeigt an, wie oft die Verbindungsparameter neu ausgehandelt wurden.

## 5.4.15 IPsec VPN

Die WBM-Seite zeigt den Status der aktivierten VPN-Verbindungen an.



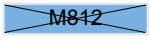

### Beschreibung der angezeigten Werte

Die Tabelle enthält folgende Spalten:

- **Name**
  Zeigt den Namen der VPN-Verbindung an.
- **Lokaler Host**
  Zeigt die IP-Adresse des Geräts an.
- **Lokale DN**
  Zeigt den Distinguished Name (DN) des Geräts an, der während des Verbindungsaufbaus an die Gegenstelle gemeldet wurde. Der Eintrag wird aus dem Feld "Local ID", dem Gerätezertifikat oder der IP-Adresse des Geräts übernommen.
- **Lokales Subnetz**
  Zeigt das lokale Netz an.
- **Remote-Host**
  Zeigt die IP-Adresse oder den Hostnamen der Gegenstelle an.

- **Remote-DN**
  Zeigt den Distinguished Name (DN) an, den die Gegenstelle beim Verbindungsaufbau gemeldet hat.
- **Remote Subnetz**
  Zeigt das entfernte Netz an.
- **Schlüssel-Lebensdauer**
  Zeigt an, wann die Gültigkeit des Schlüssels abläuft.
- **Status**
  Zeigt den Status der VPN-Verbindung an.

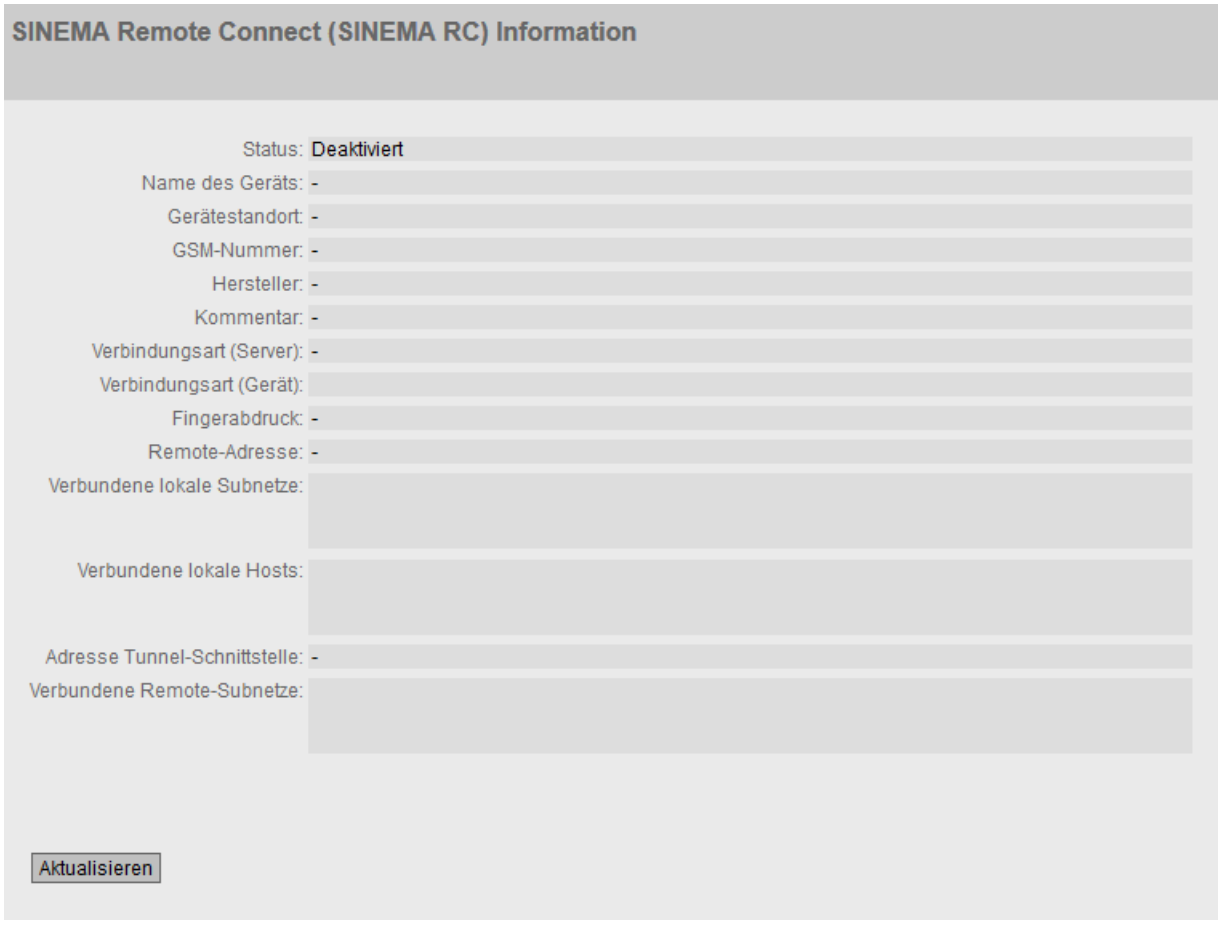
### 5.4.16 SINEMA RC




Zeigt Informationen zum SINEMARC-Server an.

**Hinweis**

Diese Funktion ist nur mit dem PLUG SINEMA RC (Seite 54) nutzbar.




### Beschreibung der angezeigten Werte

- **Status**
  Zeigt den Status der Verbindung zum SINEMA RC-Server an.
- **Name des Geräts**
  Wenn projektiert, wird der Namen des Geräts angezeigt.
- **Gerätestandort**
  Wenn projektiert, wird der Standort des Geräts angezeigt
- **GSM-Nummer**
  Wenn projektiert, wird die Rufnummer des Geräts angezeigt
- **Hersteller**
  Wenn projektiert, wird der Eintrag angezeigt
- **Kommentar**
  Wenn projektiert, wird der Kommentar angezeigt
- **Verbindungsart (Server)**
  Zeigt an, welche Verbindungsart auf dem SINEMA RC-Server eingestellt ist.
- **Verbindungsart (Gerät)**
  Zeigt an, welche Verbindungsart auf dem Gerät eingestellt ist

- **Fingerabdruck**
  Zeigt den Fingerabdruck des Serverzertifikats an. Wird nur angezeigt, wenn zum Verifizieren der Fingerabdruck verwendet wird.
- **Remote-Adresse**
  Zeigt die IP-Adresse des SINEMA RC-Servers an.
- **Verbundene lokale Subnetze**
  Zeigt die IP-Adressen der lokalen Subnetze an. Wird nur angezeigt, wenn auf dem SINEMA RC-Server die Option "Verbundene lokale Subnetze" aktiviert ist. Weiterführende Informationen dazu finden Sie in der Betriebsanleitung zum SINEMA RC-Server.
- **Verbundene lokale Hosts**
  Zeigt die Ziel-IP-Adresse der Hosts an, die erreichbar sind.
- **Adresse Tunnel-Schnittstelle**
  Zeigt die IP-Adresse der virtuellen Tunnelschnittstelle an.
- **Verbundene Remote-Subnetze**
  Zeigt die Subnetze des SINEMA RC-Servers an, die für das Gerät erreichbar sind. Welche Subnetze für das Gerät erreichbar sind, ist von den Kommunikationsbeziehungen auf dem SINEMA RC-Server abhängig. Weiterführende Informationen dazu finden Sie in der Betriebsanleitung zum SINEMA RC-Server.

## 5.4.17 OpenVPN-Client

Die WBM-Seite zeigt den Status der aktivierten OpenVPN-Verbindungen an.




### Beschreibung der angezeigten Werte

Die Tabelle enthält folgende Spalten:

- **Name**
  Zeigt den Namen der OpenVPN-Verbindung an.
- **Remote-Server**
  Zeigt die IP-Adresse oder den Hostnamen des OpenVPN-Servers an.
- **Tunnel-Schnittstelle IP**
  Zeigt die IP-Adresse der virtuellen Tunnelschnittstelle an.
- **Exportierte Subnetze**
  Zeigt die IP-Adresse der lokalen Subnetze an.

- **Geroutete Subnetze**
  Zeigt die Subnetze des Open VPN-Servers an.
- **Status**
  Zeigt den Status der OpenVPN-Verbindung an.

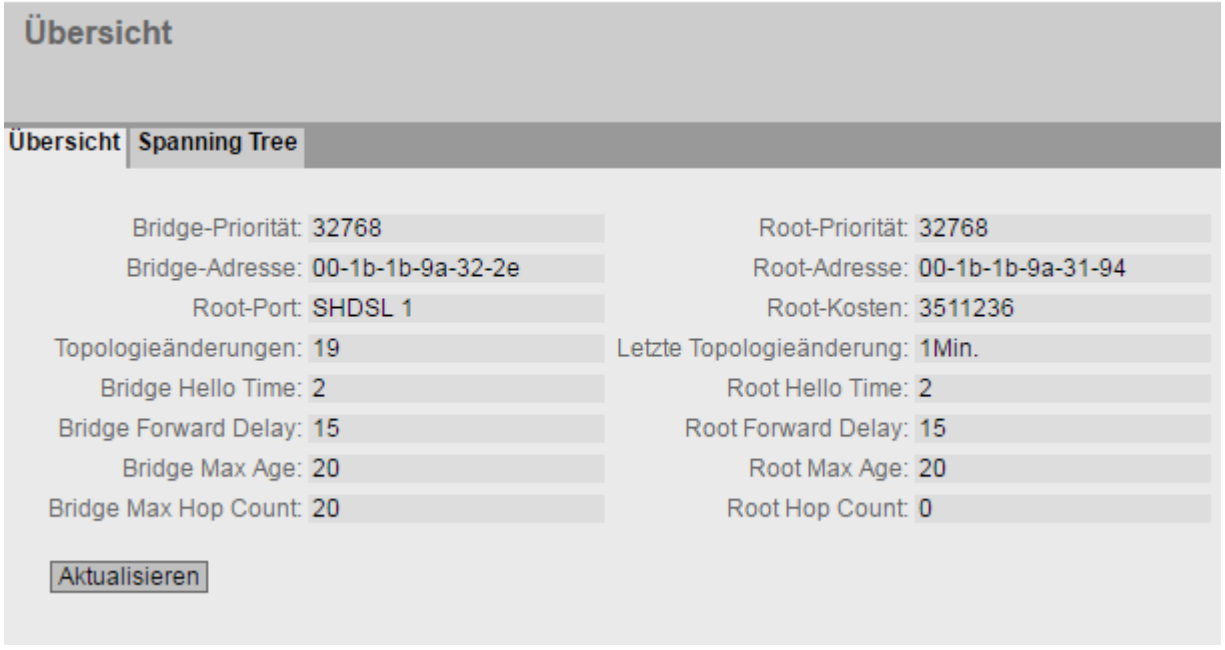
## 5.4.18 Redundanz

### 5.4.18.1 Übersicht

#### Konfiguration MSTP-CIST

Die Seite besteht aus folgenden Teilen.

- Der linke Teil der Seite zeigt die Konfiguration des Gerätes.
- Der rechte Teil zeigt die Konfiguration der Root-Bridge, wie sie aus Spanning Tree-Telegrammen abgeleitet werden kann, die ein Gerät empfangen hat.



### Beschreibung der angezeigten Werte

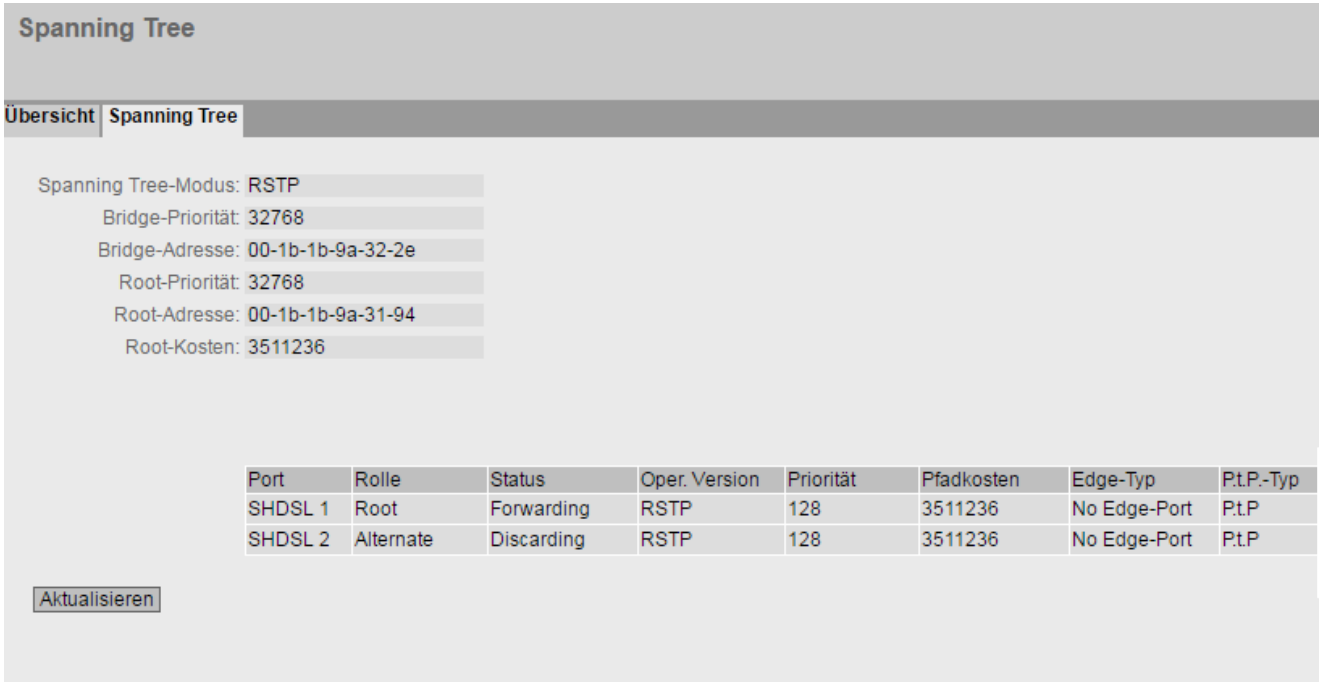
Die Seite enthält folgende Felder:

- **Bridge-Priorität / Root-Priorität**
  Anhand der Bridge-Priorität wird festgelegt, welches Gerät Root Bridge wird. Die Bridge mit der höchsten Priorität wird Root Bridge. Je kleiner der Wert, desto höher die Priorität. Wenn in einem Netz mehrere Geräte die gleiche Priorität besitzen, wird das Gerät Root-Bridge, dessen MAC-Adresse den niedrigsten Zahlenwert hat. Beide Parameter, Bridge Priority und MAC-Adresse, bilden zusammen die Bridge-Kennung. Da die Root Bridge alle Wegeänderungen verwaltet, sollte sie wegen der Laufzeit der Telegramme möglichst zentral angeordnet sein. Der Wert für die Bridge Priority ist ein ganzzahliges Vielfaches von 4096 mit einem Wertebereich von 0 bis 61440.
- **Bridge-Adresse / Root-Adresse**
  Die Bridge-Adresse zeigt die MAC-Adresse des Geräts und die Root-Adresse zeigt die MAC-Adresse der Root-Bridge an.
- **Root-Port**
  Zeigt den Port an, über den der Switch mit der Root-Bridge kommuniziert.
- **Root-Kosten**
  Die Pfadkosten von diesem Gerät bis zur Root-Bridge
- **Topologieänderungen / Letzte Topologieänderung**
  Die Angabe für das Gerät nennt die Zahl der Umkonfigurationen aufgrund des Spanning Tree-Mechanismus seit dem letzten Hochlauf. Für die Root-Bridge wird die Zeitdauer seit der letzten Umkonfiguration wie folgt angezeigt:
  - Sekunden: Zusatz "Sek." hinter der Zahlenangabe
  - Minuten: Zusatz "Min." hinter der Zahlenangabe
  - Stunden: Zusatz "Std." hinter der Zahlenangabe
- **Bridge Hello Time / Root Hello Time**
  Jede Bridge versendet regelmäßig Konfigurationstelegramme (BPDUs). Der Zeitabstand zwischen zwei solchen Telegrammen ist die Hello-Time. Der Standardwert für diesen Parameter beträgt 2 Sekunden.
- **Bridge Forward Delay / Root Forward Delay**
  Neue Konfigurationsinformationen werden von einer Bridge nicht sofort, sondern erst nach dem im Parameter Weiterleitungsverzögerung festgelegten Zeitraum angewendet. So wird sichergestellt, dass der Betrieb entsprechend der neuen Topologie erst gestartet wird, wenn alle Bridges die notwendigen Informationen haben. Der Standardwert für diesen Parameter beträgt 15 Sekunden.
- **Bridge Max Age / Root Max Age**
  Nach Ablauf des Max Age-Timers wird die empfangene BPDU verworfen, um vom Switch als gültig akzeptiert zu werden. Der Defaultwert liegt bei 20s.
- **Bridge Max Hop Count**
  Dieser Parameter gibt an, wie viele MSTP-Teilnehmer eine BPDU passieren darf. Wird eine MSTP-BPDU empfangen, deren Hop Count den hier konfigurierten Wert übersteigt, wird sie verworfen. Der Standardwert für diesen Parameter beträgt 20.
- **Root Hop Count**
  Die Anzahl der Teilnehmer,  die bis zur Root-Bridge durchlaufen werden müssen.

### 5.4.18.2 Spanning Tree

#### Einleitung

Die Seite zeigt die aktuellen Informationen zu Spanning Tree und die Einstellungen der Root Bridge an.




#### Beschreibung der angezeigten Werte

Folgende Felder werden angezeigt:

- **Spanning Tree-Modus**
  Zeigt den eingestellten Modus an. Den Modus legen Sie bei "Layer 2 > Konfiguration" und bei "Layer 2 > Spanning Tree > Allgemein" fest.
  Folgende Werte sind möglich:
  - '-'
  - RSTP
- **Bridge-Priorität / Root-Priorität**
  Anhand der Bridge-Priorität wird festgelegt, welches Gerät Root Bridge wird. Die Bridge mit der höchsten Priorität (d. h. dem kleinsten Wert für diesen Parameter) wird Root Bridge. Wenn in einem Netz mehrere Geräte die gleiche Priorität besitzen, dann wird das Gerät Root Bridge, dessen MAC-Adresse den niedrigsten Zahlenwert hat. Beide Parameter, Bridge-Priorität und MAC-Adresse, bilden zusammen die Bridge-Kennung. Da die Root Bridge alle Wegeänderungen verwaltet, sollte sie wegen der Laufzeit der Telegramme möglichst zentral angeordnet sein. Der Wert für die Bridge-Priorität ist ein ganzzahliges Vielfaches von 4096 mit einem Wertebereich von 0 bis 32768.

- **Bridge-Adresse / Root-Adresse**
  Die Bridge-Adresse zeigt die MAC-Adresse des Geräts und die Root-Adresse zeigt die MAC-Adresse der Root-Switch an.
- Root-Kosten
  Zeigt die Pfadkosten von dem Gerät bis zur Root Bridge.
- Bridge-Status
  Zeigt den Status der Bridge an, z. B. ob das Gerät die Root-Bridge ist.

Die Tabelle gliedert sich in folgende Spalten:

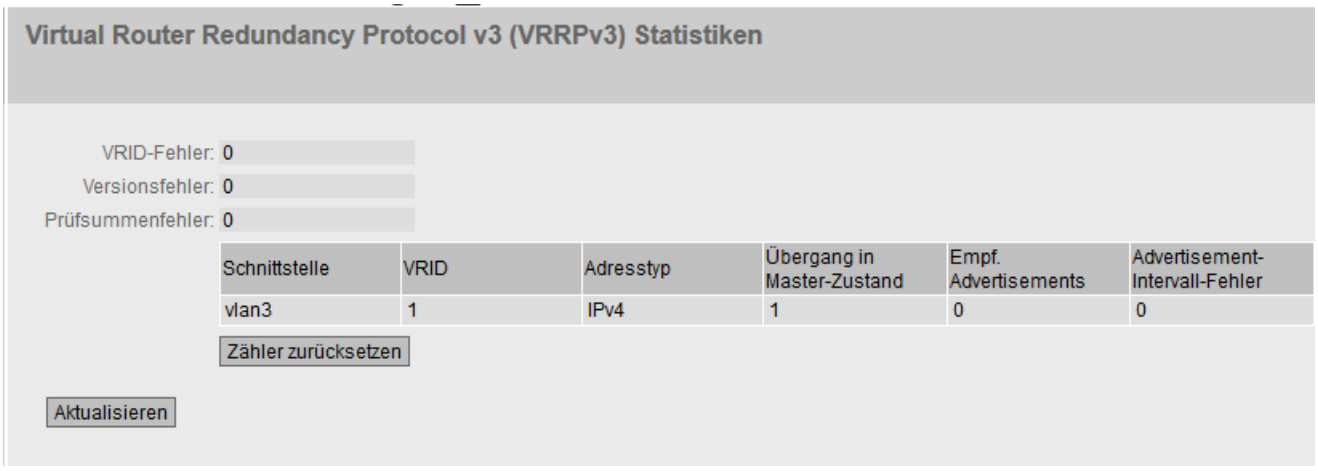
- **Port**
  Zeigt die Schnittstellen an, über den das Gerät kommuniziert.
- **Rolle**
  Zeigt den Status des Ports an. Folgende Werte sind möglich:
  - Disabled
    Der Port wurde manuell aus dem Spanning Tree entfernt und wird vom Spanning Tree nicht mehr berücksichtigt.
  - Designated
    Die Ports, die von der Root-Bridge wegführen.
  - Alternate
    Der Port mit einem alternativen Weg zu einem Netzwerksegment
  - Backup
    Wenn ein Switch mehrere Ports zu dem gleichen Netzwerksegment hat, wird der "schlechtere" Port zum Backup-Port.
  - Root
    Der Port, der den besten Weg zur Root Bridge bietet.
  - Master
    Dieser Port zeigt zu einer Root-Bridge, die außerhalb der MST-Region liegt.
- **Status**
  Zeigt den aktuellen Status an, in dem sich die Schnittstelle befindet. Die Werte werden nur angezeigt. Der Parameter ist abhängig vom projektierten Protokoll.
  - Discarding
    Der Port empfängt BPDU-Telegramme. Andere aus- oder eingehende Telegramme werden verworfen.
  - Listening
    Der Port empfängt und sendet BPDU-Telegramme. Der Port ist in den Spanning Tree-Algorithmus einbezogen. Andere aus- und eingehende Telegramme werden verworfen.
  - Learning
    Der Port lernt aktiv die Topologie, d. h. die Teilnehmeradressen. Andere aus- und eingehende Telegramme werden verworfen.
  - Forwarding
    Der Port ist nach der Umkonfigurationszeit aktiv im Netz. Der Port empfängt und sendet Datentelegramme.
- **Oper. Version**
  Zeigt den Kompatibilitätsmodus von Spanning Tree, der vom Port verwendet wird.

- **Priorität**
  Kann der vom Spanning-Tree ermittelte Weg alternativ über mehrere Ports eines Gerätes führen, so wird der Port mit der höchsten Priorität (d. h. dem kleinsten Wert für diesen Parameter) ausgewählt. Für die Priorität kann ein Wert von 0 bis 240 in 16er Schritte eingegeben werden. Wenn Sie einen Wert eingeben, der nicht durch 16 teilbar ist, wird der Wert automatisch angepasst. Der Standardwert ist 128.
- **Pfadkosten**
  Dieser Parameter dient zur Berechnung des zu wählenden Weges. Es wird die Strecke mit dem geringsten Wert als Weg ausgewählt. Haben mehrere Ports eines Gerätes den gleichen Wert, wird der Port mit der niedrigsten Portnummer ausgewählt.
  Die Ermittlung der Wegekosten richtet sich maßgeblich nach der Übertragungsgeschwindigkeit. Je höher die erzielbare Übertragungsgeschwindigkeit ist, umso kleiner ist der Wert für die Wegekosten.
  Typische Werte für Wegekosten bei Rapid Spanning Tree:
  - 10.000 Mbit/s = 2.000
  - 1000 Mbit/s = 20.000
  - 100 Mbit/s = 200.000
  - 10 Mbit/s = 2.000.000
- **Edge-Typ**
  Zeigt den Typ der Verbindung an. Folgende Werte sind möglich:
  - Edge Port
    An diesem Port befindet sich ein Endgerät.
  - No Edge Port
    An diesem Port befindet sich ein Spanning Tree- oder Rapid Spanning Tree-Gerät.
- **P.t.P. Typ**
  Zeigt die Art der Punkt-zu-Punkt-Verbindung an. Folgende Werte sind möglich:
  - P.t.P.
    Bei Halbduplex wird von einer Punkt-zu-Punkt-Verbindung ausgegangen.
  - Shared Media
    Bei einer Vollduplexverbindung wird nicht von einer Punkt-zu-Punkt-Verbindung ausgegangen.

## 5.4.19 VRRPv3-Statistiken

### Einleitung

Diese Seite zeigt die Statistiken des VRRPv3-Protokolls und aller konfigurierten virtuellen Router an.




### Beschreibung

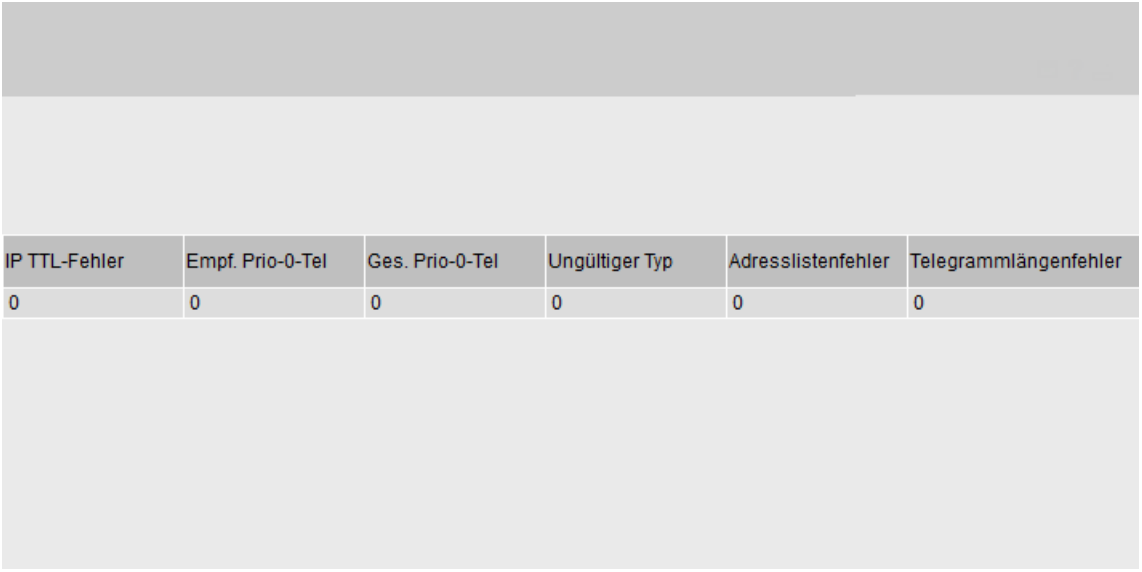
Folgende Felder werden angezeigt:

- **VRID-Fehler**
  Zeigt an, wie viele VRRPv3-Pakete empfangen wurden, die eine nicht unterstützte VRID enthalten.
- **Versionsfehler**
  Zeigt an, wie viele VRRPv3-Pakete empfangen wurden, die eine ungültige Versionsnummer enthalten.
- **Prüfsummenfehler**
  Zeigt an, wie viele VRRPv3-Pakete empfangen wurden, die eine ungültige Prüfsumme enthalten.

Die Tabelle gliedert sich in folgende Spalten:

- **Schnittstellen**
  Schnittstelle, auf die sich die Einstellungen beziehen.
- **VRID**
  Zeigt die ID des virtuellen Routers an. Gültige Werte sind 1 ... 255.
- **Adresstyp**
  Zeigt die Version des IP-Protokolls an
- **Übergang in Master-Zustand**
  Zeigt an, wie häufig dieser virtuelle Router in den Zustand "Master" ging.
- **Empf. Advertisements**
  Zeigt an, wie viele VRRPv3-Pakete empfangen wurden.

- **Advertisement-Intervall-Fehler**
  Zeigt an, wie viele fehlerhafte VRRPv3-Pakete empfangen wurden, deren Intervall nicht mit dem lokal gesetzten Wert übereinstimmt.



| IP TTL-Fehler | Empf. Prio-0-Tel | Ges. Prio-0-Tel | Ungültiger Typ | Adresslistenfehler | Telegrammlängenfehler |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |

- **IP TTL Fehler**
  Zeigt an, wie viele fehlerhafte VRRPv3-Pakete empfangen wurden, deren TTL (Time to live) Wert im IP-Header nicht stimmt.
- **Empf. Prio-0-Tel**
  Zeigt an, wie viele VRRPv3-Pakete mit der Priorität 0 empfangen wurden. VRRPv3-Pakete mit der Priorität 0 werden versendet, wenn ein Master-Router heruntergefahren wird. Diese Pakete ermöglichen dann eine schnelle Übergabe an den entsprechenden Backup Router.
- **Ges. Prio-0-Tel**
  Zeigt an, wie viele VRRPv3-Pakete mit der Priorität 0 versendet wurden. Pakete mit der Priorität 0 werden versendet, wenn ein Master-Router heruntergefahren wird. Diese Pakete ermöglichen dann eine schnelle Übergabe an den entsprechenden Backup Router.
- **Ungültiger Typ**
  Zeigt an, wie viele fehlerhafte VRRPv3-Pakete empfangen wurden, deren Wert im Feld "Typ" des IP-Headers ungültig ist.
- **Adresslistenfehler**
  Zeigt an, wie viele fehlerhafte VRRPv3-Pakete empfangen wurden, deren Adressliste nicht mit der lokal konfigurierten Liste übereinstimmt.
- **Telegrammlängenfehler**
  Zeigt an, wie viele fehlerhafte VRRPv3-Pakete empfangen wurden, deren Länge nicht korrekt ist.

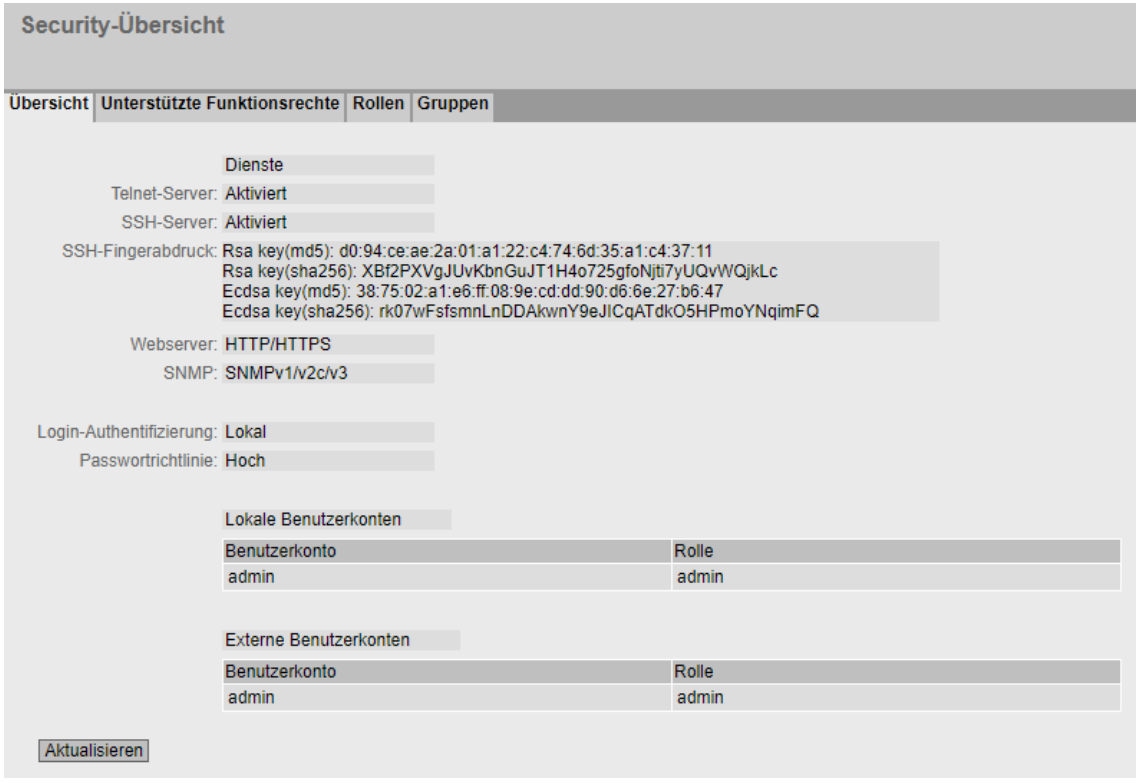
## 5.4.20 Security

### 5.4.20.1 Übersicht

**Hinweis**

Es ist von den Rechten des angemeldeten Benutzers abhängig, welche Werte angezeigt werden.

Die Seite zeigt die Sicherheitseinstellungen sowie die lokalen und externen Benutzerkonten an.




## Beschreibung

**Dienste**

Die Liste "Dienste" zeigt die Sicherheitseinstellungen an.

- **Telnet-Server**
  Die Einstellung konfigurieren Sie unter "System > Konfiguration".
  - Aktiviert: Unverschlüsselter Zugriff auf das CLI
  - Deaktiviert: Kein unverschlüsselter Zugriff auf das CLI
- **SSH-Server**
  Die Einstellung konfigurieren Sie unter "System > Konfiguration".
  - Aktiviert: Verschlüsselter Zugriff auf das CLI
  - Deaktiviert: Kein verschlüsselter Zugriff auf das CLI
- **SSH-Fingerabdruck**
  Folgende SSH-Fingerabdrücke werden angezeigt:
  - MD5
  - SHA256
- **Webserver**
  Die Einstellung konfigurieren Sie unter "System > Konfiguration"
  - HTTP/HTTPS: Der Zugriff auf das WBM ist über HTTP und HTTPS möglich.
  - HTTPS: Der Zugriff auf das WBM ist nur noch über HTTPS möglich.
- **SNMP**
  Die Einstellung konfigurieren Sie unter "System > SNMP > Allgemein".
  - "-" (SNMP deaktiviert)
    Ein Zugriff auf die Geräteparameter ist über SNMP nicht möglich.
  - SNMPv1/v2c/v3
    Ein Zugriff auf die Geräteparameter ist mit den SNMP Versionen 1, 2c oder 3 möglich.
  - SNMPv3
    Ein Zugriff auf die Geräteparameter ist nur mit der SNMP Version 3 möglich.

- **Login-Authentifizierung**
  Die Einstellung konfigurieren Sie unter "Security > AAA > Allgemein".
  - Lokal
    Die Authentifizierung muss lokal auf dem Gerät erfolgen.
  - RADIUS
    Die Authentifizierung muss über einen RADIUS-Server erfolgen.
  - Lokal und RADIUS
    Die Authentifizierung kann sowohl über die im Gerät vorhandenen Benutzer (Benutzername und Passwort) als auch über einen RADIUS-Server erfolgen.
    Es wird zuerst in der lokalen Datenbank nach dem Benutzer gesucht. Wenn der Benutzer dort nicht vorhanden ist, wird eine RADIUS-Anfrage geschickt.
  - RADIUS und Fallback Lokal
    Die Authentifizierung muss über einen RADIUS-Server erfolgen.
    Nur wenn der RADIUS-Server im Netz nicht erreichbar ist, wird eine lokale Authentifizierung durchgeführt.
- **Passwortrichtlinie**
  Zeigt an, welche Passwortrichtlinie aktuell verwendet wird.

Die Tabellen "Lokale Benutzerkonten" und "Externe Benutzerkonten" gliedern sich in folgende Spalten:

- **Benutzerkonto**
  Zeigt den Namen des lokalen Benutzers an.
- **Rolle**
  Zeigt die Rolle des Benutzers an. Weitere Informationen zu den Funktionsrechten der Rolle erhalten Sie unter "Information > Security > Rollen".

**Lokale und externe Benutzerkonten**

Lokale Benutzerkonten und Rollen konfigurieren Sie unter "Security > Benutzer".

Wenn Sie ein lokales Benutzerkonto anlegen, wird automatisch auch ein externes Benutzerkonto erzeugt.

Bei lokalen Benutzerkonten handelt es sich um Benutzer mit jeweils einem Passwort zur Anmeldung auf dem Gerät.

In der Tabelle "Externe Benutzerkonten" wird ein Benutzer mit einer Rolle verknüpft. In diesem Beispiel wird der Benutzer "Observer" mit der Rolle "user" verknüpft. Der Benutzer ist auf einem RADIUS-Server definiert. Die Rolle ist lokal auf dem Gerät definiert. Wenn ein RADIUS-Server einen Benutzer authentifiziert, die zugehörige Gruppe jedoch unbekannt oder nicht vorhanden ist, prüft das Gerät, ob es für den Benutzer einen Eintrag in der Tabelle "Externe Benutzerkonten" gibt. Wenn ein entsprechender Eintrag existiert, wird der Benutzer mit den Rechten der verknüpften Rolle angemeldet. Wenn die zugehörige Gruppe auf dem Gerät bekannt ist, werden beide Tabellen ausgewertet. Dem Benutzer wird die Rolle mit den größeren Rechten zugewiesen.

**Hinweis**

Die Tabelle "Externe Benutzerkonten" wird nur ausgewertet, wenn Sie im RADIUS-Autorisierungsmodus "Herstellerspezifisch" eingestellt haben.

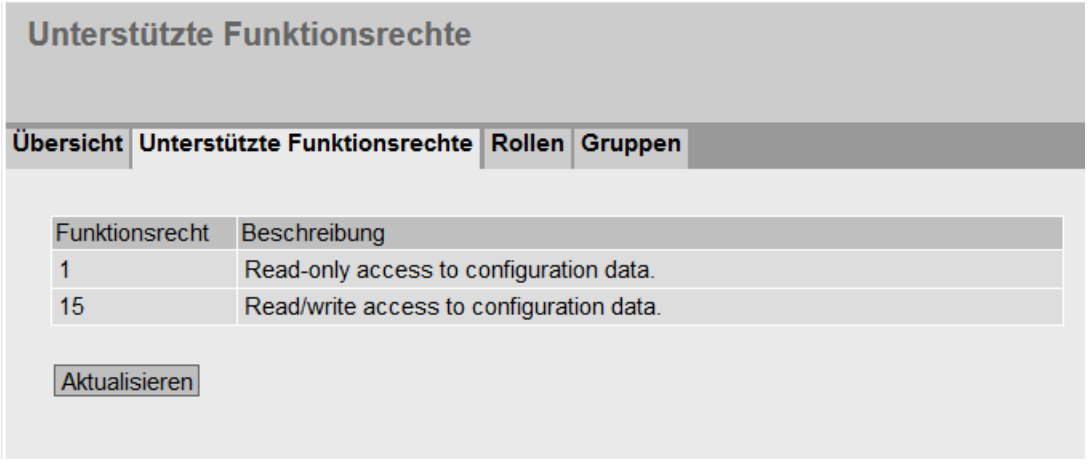
Über CLI können Sie auf die externen Benutzerkonten zugreifen.

### 5.4.20.2 Unterstützte Funktionsrechte

**Hinweis**

Es ist von der Rolle des angemeldeten Benutzers abhängig, welche Werte angezeigt werden.

Die Seite zeigt die Funktionsrechte an, die lokal auf dem Gerät verfügbar sind.




#### Beschreibung der angezeigten Werte

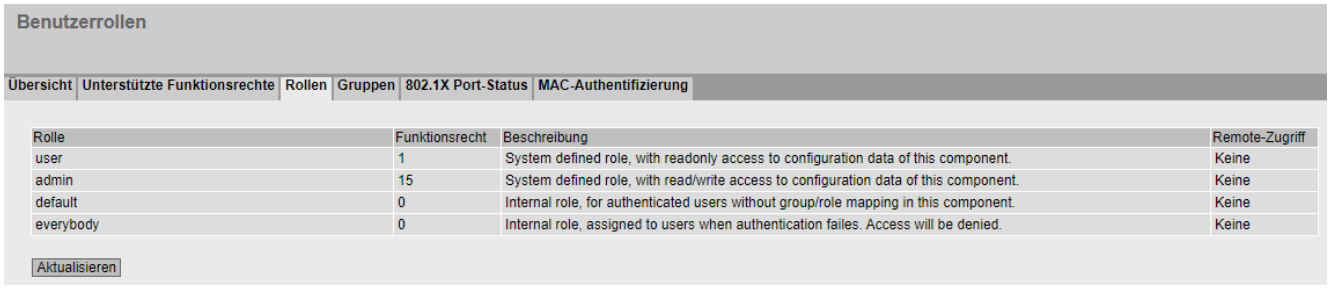
- **Funktionsrecht**
  Zeigt die Nummer des Funktionsrechts an. Den Nummern sind unterschiedliche Rechte in Bezug auf die Geräteparameter zugeordnet.
- **Beschreibung**
  Zeigt die Beschreibung des Funktionsrechts an.

### 5.4.20.3 Rollen

**Hinweis**

Es ist von der Rolle des angemeldeten Benutzers abhängig, welche Werte angezeigt werden.

Die Seite zeigt die Rollen an, die lokal auf dem Gerät gültig sind.




## Beschreibung

Die Tabelle enthält folgende Spalten:

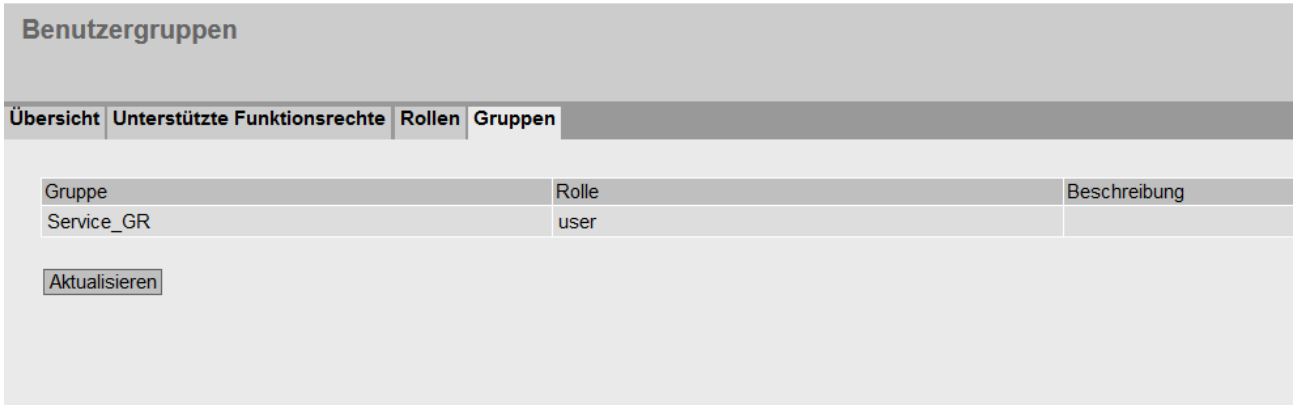
- **Rolle**
  Zeigt den Namen der Rolle an.
- **Funktionsrecht**
  Zeigt das Funktionsrecht der Rolle an:
  - 1
    Benutzer mit dieser Rolle können Geräteparameter lesen, aber nicht verändern.
  - 15
    Benutzer mit dieser Rolle können Geräteparameter sowohl lesen als auch verändern.
  - 0
    Hierbei handelt es sich um eine Rolle, die das Gerät intern vergibt, wenn ein Benutzer nicht authentifiziert werden konnte. Dem Benutzer wird der Zugriff auf das Gerät verweigert.
- **Beschreibung**
  Zeigt eine Beschreibung der Rolle an.
- **Remote-Zugriff**
  Zeigt an, welcher Remote-Zugriff aktuell verwendet wird.

### 5.4.20.4 Gruppen

**Hinweis**

Es ist von der Rolle des angemeldeten Benutzers abhängig, welche Werte angezeigt werden.

Diese Seite zeigt an, welche Gruppe mit welcher Rolle verknüpft ist. Die Gruppe ist auf einem RADIUS-Server definiert. Die Rolle ist lokal auf dem Gerät definiert.




### Beschreibung der angezeigten Werte

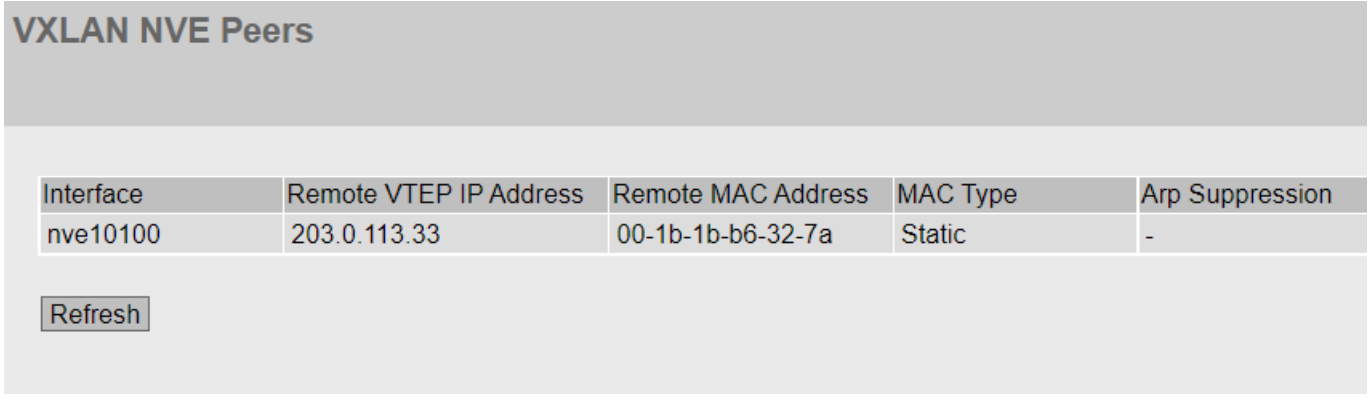
Die Tabelle gliedert sich in folgende Spalten:

- **Gruppe**
  Zeigt den Namen der Gruppe an. Der Name entspricht der Gruppe auf dem RADIUS-Server.
- **Rolle**
  Zeigt den Namen der Rolle an. Benutzer, die über den RADIUS-Server mit der verknüpften Gruppe authentifiziert werden, erhalten die Rechte dieser Rolle lokal auf dem Gerät.
- **Beschreibung**
  Zeigt die Beschreibung für die Verknüpfung an.

## 5.4.21 VXLAN

MUM85x

Diese Seite zeigt den aktuellen Inhalt der VXLAN NVE Peer-Tabelle.



### Beschreibung der angezeigten Werte

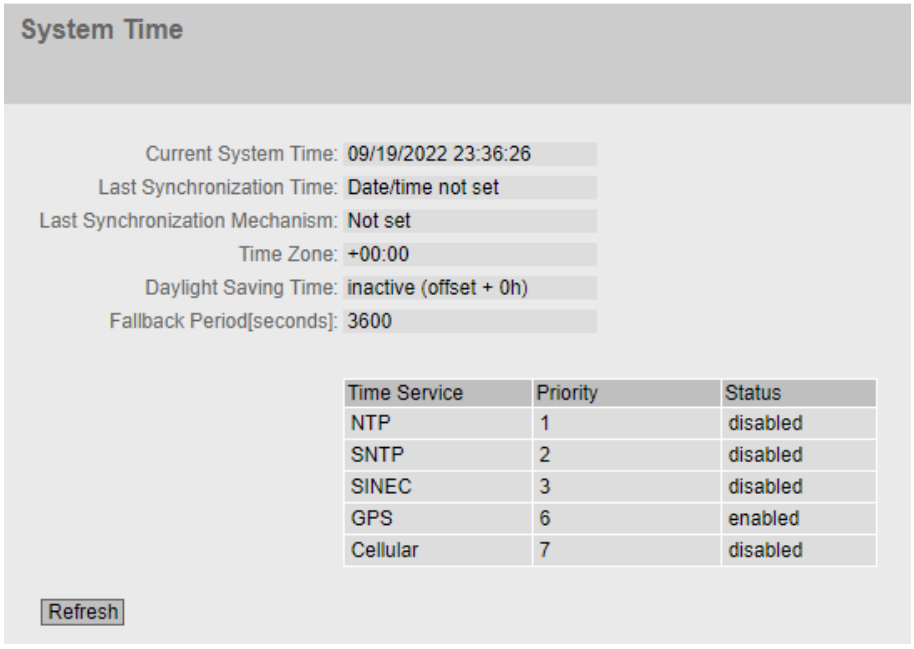
Die Tabelle enthält folgende Spalten:

- **Schnittstelle**
  Zeigt die NVE-Schnittstelle an, über die der Zeileneintrag gelernt wurde.
- **Remote VTEP-IP-Adresse**
  Zeigt die IPv4-Adresse des Remote-VTEPs an.
- **VNI-ID**
  Zeigt das VNI-Segment an, in dem der Remote-VTEP Mitglied ist.
- **Remote MAC-Adresse**
  Zeigt die MAC-Adresse des Remote-VTEPs an, die das Gerät gelernt hat oder die projektiert wurde.
- **MAC-Typ**
  Zeigt an, wie die MAC-Adresse des Remote-VTEPs bezogen wird.
  - Statisch:
    Die MAC- und IP-Adressen wurden unter "Layer 2 > VXLAN > Statische MAC-Adressen" projektiert. Die statischen Adressen sind permanent gespeichert, d. h. sie werden nicht nach Ablauf der Aging Time oder beim Neustart des Geräts gelöscht.
  - Dynamisch:
    Der VTEP des Geräts ermittelt die MAC-Adresse aus dem empfangenen Frame.
- **ARP-Unterdrückung**
  Funktion wird nicht unterstützt.

## 5.4.22 Systemzeit

MUM85x

Die Seite zeigt die Einstellungen der Systemzeit für das Gerät an.




## Beschreibung

Die Seite enthält folgende Felder:

- **Aktuelle Systemzeit**
  Zeigt das eingestellte Datum und die Uhrzeit im Format "MM/DD/YYYY HH:MM:SS" an.
- **Letzter Synchronisationszeitpunkt**
  Zeigt an, wann die letzte Uhrzeitsynchronisation stattgefunden hat. Wenn keine Uhrzeitsynchronisation möglich war, enthält das Feld die Angabe "Datum/Zeit nicht eingestellt".
- **Letzter Synchronisationsmechanismus**
  Zeigt an, wie die letzte Zeitsynchronisation durchgeführt wurde.
  - Nicht eingestellt
    Die Zeit wurde nicht eingestellt.
  - Manuell
    Manuelle Zeiteinstellung
  - NTP
    Automatische Zeitsynchronisation über NTP
  - SNTP
    Automatische Zeitsynchronisation über SNTP
  - SIMATIC Time Client
    Automatische Zeitsynchronisation über SIMATIC-Uhrzeittelegramm
  - GPS
    Zeigt an, ob die Zeit über das GPS-Signal erhalten wird.
  - Cellular
    Zeigt an, ob die Zeit über ein Mobilfunknetz abgerufen wird. Priorität

- **Zeitzone**
  Zeigt die verwendete Zeitzone im Format "(+/- )HH:MM" an. Die Zeitzone bezieht sich auf UTC Standard-Weltzeit.
- **GPS-Sommerzeit**
  Zeigt an, ob die Umstellung der Sommerzeit aktiv ist.
  - active (offset +1 h)
    Die Systemzeit wurde auf Sommerzeit umgestellt, d. h. es wird eine Stunde hinzugezählt. Die aktuelle Systemzeit sehen Sie oben rechts im Auswahlbereich des WBM.
    In dem Feld "Systemzeit" wird weiterhin die eingestellte Zeit angezeigt.
  - inactive (offset +0 h)
    Die aktuelle Systemzeit wird nicht verändert.
- **Fallback Period[seconds]**
  Zeigt die Wartezeit an, nach der der Ersatzzeitdienst die Systemzeit synchronisiert. Wertebereich 1 ... 86400. Default-Wert 3600.

Die Tabelle gliedert sich in folgende Spalten:

- **Zeitdienst**
  - NTP
    Zeigt an, ob die Zeit über NTP synchronisiert wird.
  - SNTP
    Zeigt an, ob die Zeit über SNTP synchronisiert wird.
  - SIMATIC Time Client
    Zeigt an, ob die Zeit über SINEC synchronisiert wird.
  - GPS
    Zeigt an, ob die Zeit über das GPS-Signal erhalten wird.
  - Cellular
    Zeigt an, ob die Zeit über ein Mobilfunknetz abgerufen wird.
- **Priorität**
  Zeigt den Vorrang eines Zeitdienstes an.
- **Status**
  Zeigt den Status des Zeitdienstes an.

# 5.5 Menü "System"

## 5.5.1 Konfiguration

### Systemkonfiguration

Die WBM-Seite enthält die Konfigurationsübersicht über die Zugriffsmöglichkeiten des Geräts.

Legen Sie fest, über welche Dienste auf das Gerät zugegriffen wird. Zu einigen Diensten gibt es weitere Konfigurationsseiten, auf denen detailliertere Einstellungen möglich sind.

Zusätzlich ist bei einigen Diensten der Standard-Port änderbar.

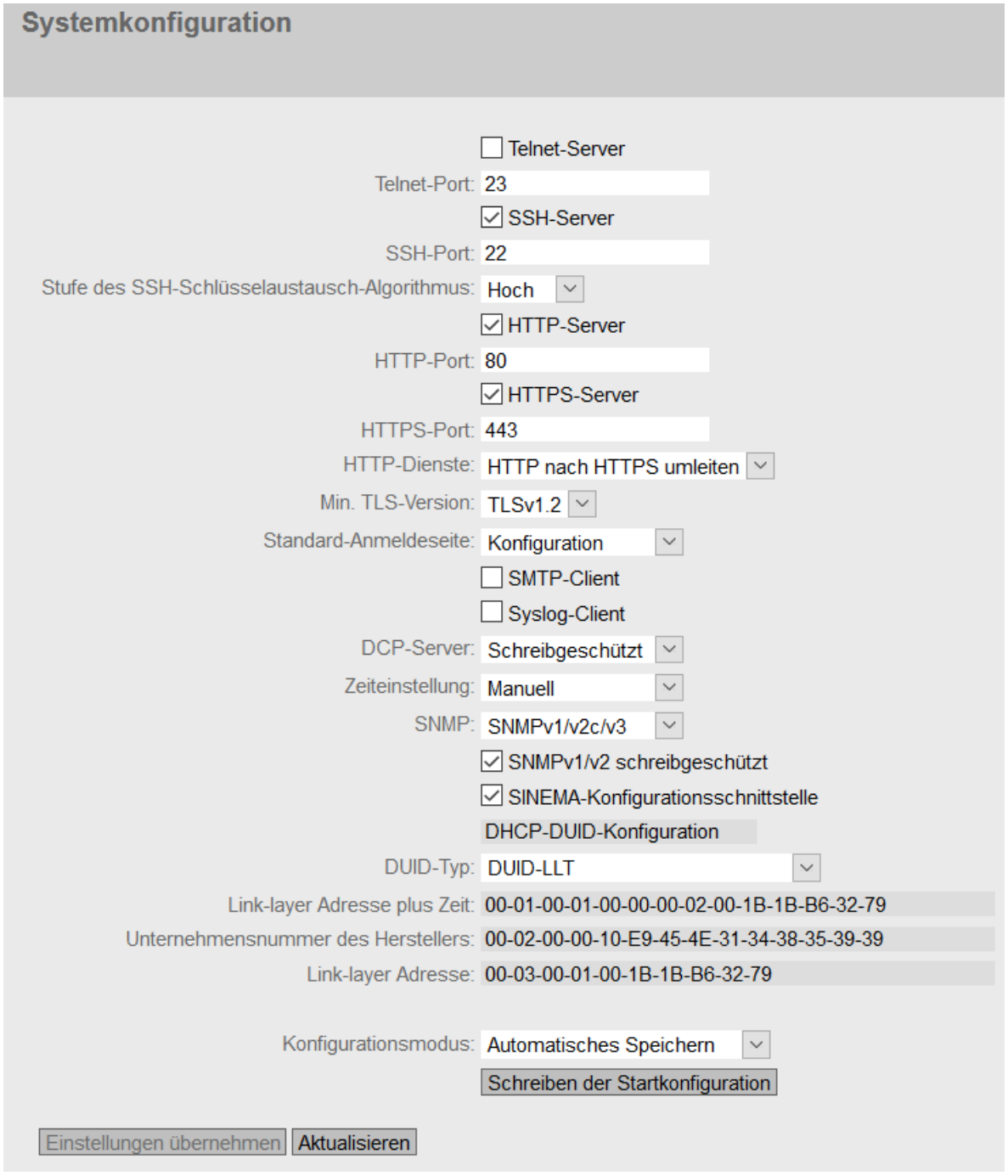
**Hinweis**

**Standard-Port ändern**

Manche Programme können nur über den Standard-Port auf den Dienst zugreifen, z. B. TIA-Portal greift über Standard-Port 443 auf HTTPS zu. Bevor Sie den Port ändern, prüfen Sie nach, welchen Port das Programm verwendet. Wenn Sie den Standard-Port ändern, müssen Sie über den geänderten Port auf den Dienst zugreifen.

**Firewall**

Nach dem Ändern der Ports wird die Firewall neu initialisiert. D. h. die geänderten Ports werden in die Firewallregeln übernommen. Bestehenden Verbindungen z. B. über die dynamische Firewall sind für diese Zeit eingeschränkt nutzbar.


Systemkonfiguration
Telnet-Server
Telnet-Port: 23
SSH-Server
SSH-Port: 22
Stufe des SSH-Schlüsselaustausch-Algorithmus: Hoch
HTTP-Server
HTTP-Port: 80
HTTPS-Server
HTTPS-Port: 443
HTTP-Dienste: HTTP nach HTTPS umleiten
Min. TLS-Version: TLSv1.2
Standard-Anmeldeseite: Konfiguration
SMTP-Client
Syslog-Client
DCP-Server: Schreibgeschützt
Zeiteinstellung: Manuell
SNMP: SNMPv1/v2c/v3
SNMPv1/v2 schreibgeschützt
SINEMA-Konfigurationsschnittstelle
DHCP-DUID-Konfiguration
DUID-Typ: DUID-LLT
Link-layer Adresse plus Zeit: 00-01-00-01-00-00-00-02-00-1B-1B-B6-32-79
Unternehmensnummer des Herstellers: 00-02-00-00-10-E9-45-4E-31-34-38-35-39-39
Link-layer Adresse: 00-03-00-01-00-1B-1B-B6-32-79
Konfigurationsmodus: Automatisches Speichern
Schreiben der Startkonfiguration
Einstellungen übernehmen
Aktualisieren

## Beschreibung

Die Seite enthält folgende Felder:

- **Telnet-Server**
  Aktivieren oder deaktivieren Sie den Dienst "Telnet Sever" für den unverschlüsselten Zugriff auf das CLI.
- **Telnet-Port**
  Legen Sie den Port für den Telnet-Zugriff auf das CLI fest.
- **SSH-Server**
  Aktivieren oder deaktivieren Sie den Dienst "SSH Server" für den verschlüsselten Zugriff auf das CLI.
- **SSH-Port**
  Legen Sie den Port für den SSH-Zugriff auf das CLI fest.
- **Stufe des SSH-Schlüsselaustausch-Algorithmus**
  Konfigurieren Sie die Stufe des SSH-Schlüsselaustausch-Algorithmus für den SSH-Zugriff auf das CLI.
  Hoch (Default)
  - Curve25519-sha256
  - Curve25519-sha256@libssh.org
  - Ecdh-sha2-nistp256
  - Ecdh-sha2-nistp384
  - Ecdh-sha2-nistp521
  - Diffie-hellman-group16-sha512
  - Diffie-hellman-group18-sha512

  Niedrig
  - 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
- **HTTP-Server**
  Aktivieren oder deaktivieren Sie den HTTP-Zugriff auf das WBM.
- **HTTP-Port**
  Legen Sie den Port für den HTTP-Zugriff auf das WBM fest.
- **HTTPS-Server**
  Aktivieren oder deaktivieren Sie den HTTPS-Zugriff auf das WBM.

- **HTTPS-Port**
  Legen Sie den Port für den HTTPS-Zugriff auf das WBM fest.
- **HTTP-Dienste**
  Legen Sie fest, wie auf das WBM zugegriffen wird:
  - HTTPS
    Zugriff auf das WBM nur über HTTPS möglich.
  - HTTP/HTTPS
    Zugriff auf das WBM nur über HTTP und HTTPS möglich.
  - HTTP nach HTTPS umleiten
    Beim Zugriff über HTTP wird automatisch nach HTTPS umgeleitet.
- **Min. TLS-Version**
  Legen Sie fest, welche Version von TLS mindestens verwendet wird.
- **Standard-Anmeldeseite**
  Legen Sie fest, mit welcher Anmeldeseite das WBM standardmäßig startet.
  - Firewall
    Anmelden an der WBM-Seite für dynamische Firewall.
  - Konfiguration
    Anmelden am WBM.
- **SMTP-Client**
  Aktivieren oder deaktivieren Sie den SMTP-Client. Weitere Einstellungen konfigurieren Sie unter "System > SMTP-Client".
- **Syslog-Client**
  Aktivieren oder deaktivieren Sie den Syslog-Client. Weitere Einstellungen konfigurieren Sie unter "System > Syslog-Client".
- **DCP-Server**
  Legen Sie fest, ob auf das Gerät mit DCP (Discovery and Configuration Protocol) zugegriffen werden kann:
  - "-" (Deaktiviert)
    DCP ist deaktiviert. Geräteparameter können weder gelesen noch geändert werden.
  - Lesen/Schreiben
    Mit DCP können Geräteparameter sowohl gelesen als auch verändert werden.
  - Schreibgeschützt
    Mit DCP können Geräteparameter zwar gelesen aber nicht verändert werden.
  - Lesen/Setup
    Solange das Standard-Passwort des Administrators nicht geändert ist, können die Geräteparameter über DCP sowohl gelesen als auch verändert werden. Nach dem Ändern des Standard-Passworts können die Gerätparameter über DCP nicht mehr verändert werden.

- **Zeiteinstellung**
  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellungen sind möglich:
  - Manuell
    Die Systemzeit wird manuell eingestellt. Weitere Einstellungen konfigurieren Sie unter "System > Systemzeit > Manuelle Einstellung".
  - SIMATIC Time
    Die Systemzeit wird über einen SIMATIC Zeitgeber eingestellt. Weitere Einstellungen konfigurieren Sie unter "System > Systemzeit > SIMATIC Time Client".
  - SNTP-Client
    Die Systemzeit wird über einen SNTP-Server eingestellt. Weitere Einstellungen konfigurieren Sie unter "System > Systemzeit > SNTP-Client".
  - NTP-Client
    Die Systemzeit wird über einen NTP-Server eingestellt. Weitere Einstellungen konfigurieren Sie unter "System > Systemzeit > NTP-Client".
- **SNMP**
  Wählen Sie aus der Klappliste das Protokoll. Folgende Einstellungen sind möglich:
  - "-" (SNMP deaktiviert)
    Ein Zugriff auf die Geräteparameter ist über SNMP nicht möglich.
  - SNMPv1/v2c/v3
    Ein Zugriff auf die Geräteparameter ist mit den SNMP Versionen 1, 2c oder 3 möglich. Weitere Einstellungen konfigurieren Sie unter "System > SNMP > Allgemein".
  - SNMPv3
    Ein Zugriff auf die Geräteparameter ist nur mit SNMP Version 3 möglich. Weitere Einstellungen konfigurieren Sie unter " System > SNMP > Allgemein".
- **SNMPv1/v2 schreibgeschützt**
  Aktivieren oder deaktivieren Sie den schreibenden Zugriff auf SNMP-Variablen bei SNMPv1/v2c.
- **SNMPv1-Traps**
  Aktivieren oder deaktivieren Sie das Versenden von SNMPv1-Traps (Alarmtelegramme). Weitere Einstellungen konfigurieren Sie unter "System > SNMP > Traps".
- **SINEMA-Konfigurationsschnittstelle**
  Wenn die SINEMA Konfigurationsschnittstelle aktiviert ist, können Sie Konfigurationen über STEP 7 Basic / Professional auf das Gerät laden.
- **DHCP-Client**
  Aktivieren oder deaktivieren Sie den DHCP-Client. Weitere Einstellungen konfigurieren Sie unter "System > DHCP"

- **DUID-Typ**
  Legen Sie fest, welcher DUID-Typ verwendet wird. Die DUID-Typen sind in der RFC 3315 definiert.
  - DUID-LLT
    DUID basiert auf der Link-layer-Adresse der Schnittstelle und einem Zeitstempel
  - DUID-EN
    DUID wird vom Hersteller (EN = Enterprise number) vergeben
  - DUID-LL
    DUID basiert auf der Link-layer-Adresse der Schnittstelle
- **Link-layer Adresse plus Zeit (LLT)**
  Der Wert basiert auf der Link-layer-Adresse der Schnittstelle und einem Zeitstempel. Der Wert wird nach jedem Zurücksetzen auf die Werkseinstellungen neu generiert.
- **Unternehmensnummer des Herstellers (EN)**
  Der Wert basiert auf der Unternehmensnummer, die spezifisch für den Hersteller ist. Der Wert wird nach jedem Zurücksetzen auf die Werkseinstellungen neu generiert.
- **Link-layer Adresse (LL)**
  Die Link-layer-Adresse basiert auf der MAC-Adresse. Der Wert wird nach jedem Zurücksetzen auf die Werkseinstellungen neu generiert.
- **Konfigurationsmodus**
  Wählen Sie aus der Klappliste die Betriebsart. Folgende Betriebsarten sind möglich:
  - Automatisches Speichern
    Automatischer Sicherungsbetrieb. Ca. 1 Minute nach der letzten Parameteränderung oder vor dem Neustart des Geräts wird die Konfiguration automatisch abgespeichert. Zusätzlich erscheint im Anzeigebereich folgende Meldung "Die Änderungen werden automatisch in x Sekunden gespeichert. Um die Änderungen sofort zu speichern, klicken Sie auf 'Schreiben der Startkonfiguration'."

    **Hinweis**

    **Unterbrechung des Speichervorgangs**

    Der Speichervorgang startet erst, nachdem der Timer in der Meldung abgelaufen ist. Die Dauer des Speichervorgangs ist vom Gerät abhängig.

    Während des Speichervorgangs wird die Meldung "Die Konfigurationsdaten werden gespeichert. Schalten Sie das Gerät nicht aus." angezeigt.
    - Schalten Sie das Gerät nicht sofort aus, nachdem der Timer abgelaufen ist.

  - Trial
    Trial-Modus. Im Trial-Modus werden Änderungen zwar übernommen aber nicht in der Konfigurationsdatei (Startup Configuration) gespeichert.
    Um Änderungen in der Konfigurationsdatei abzuspeichern, verwenden Sie die Schaltfläche "Schreiben der Startkonfiguration". Zusätzlich wird im Anzeigebereich die Meldung "Der Konfigurationsmodus Trial ist aktiv - Klicken Sie auf die Schaltfläche "Schreiben der Startkonfiguration" um Ihre Einstellungen zu speichern" angezeigt, sobald es ungespeicherte Änderungen gibt. Diese Meldung ist auf jeder WBM-Seite sichtbar, bis die vorgenommenen Änderungen entweder gespeichert werden oder das Gerät neu gestartet wird.

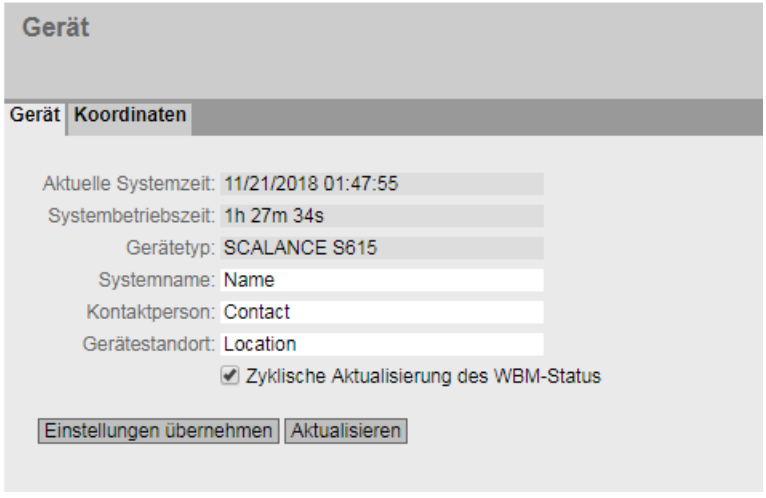
### Vorgehensweise

1. Um die gewünschte Funktion zu nutzen, aktivieren Sie das entsprechende Optionskästchen.
2. Wählen Sie aus den Klapplisten die gewünschten Optionen.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

## 5.5.2 Allgemein

### 5.5.2.1 Gerät

Diese WBM-Seite enthält die allgemeinen Geräteinformationen.




### Beschreibung

Die WBM-Seite enthält folgende Felder:

- **Aktuelle Systemzeit**
  Zeigt die aktuelle Systemuhrzeit an. Die Systemuhrzeit wird entweder vom Anwender eingestellt oder per Uhrzeittelegramm synchronisiert: entweder SIMATIC-Uhrzeittelegramm, NTP oder SNTP.
- **Systembetriebszeit**
  Zeigt die Laufzeit des Geräts seit dem letzten Neustart an.
- **Gerätetyp**
  Zeigt die Typenbezeichnung des Geräts an.
- **Systemname**
  Sie können den Namen des Geräts eintragen. Der eingetragene Name wird im Auswahlbereich angezeigt. Es sind maximal 255 Zeichen möglich.
  Der Systemname wird auch in der CLI-Eingabeaufforderung (Prompt) angezeigt. In der CLI-Eingabeaufforderung ist die Anzahl der Zeichen begrenzt. Der Systemname wird nach 16 Zeichen abgeschnitten.

- **Kontaktperson**
  Sie können den Namen einer Kontaktperson eintragen, die für die Verwaltung des Geräts zuständig ist. Es sind maximal 255 Zeichen möglich.
- **Gerätestandort**
  Sie können den Montageort des Geräts eintragen. Der eingetragene Montageort wird im Auswahlbereich angezeigt. Es sind maximal 255 Zeichen möglich.

**Hinweis**

**Erlaubte Zeichen**

Folgende darstellbare ASCII-Zeichen (0x20 bis 0x7e) in den Eingabefeldern **"Systemname"**, **"Kontaktperson"** und **"Gerätestandort"** sind erlaubt:

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

- **Zyklische Aktualisierung des WBM-Status**
  Wenn deaktiviert, ist das automatische Aktualisieren des WBM ausgeschaltet. Das ist geeignet für langsame 2G-Verbindungen oder bei Verträgen mit sehr begrenztem Datenvolumen.
  Dabei ist das Folgende zu beachten:
  - Keine Aktualisierung von Statusanzeigen
  - Keine automatische Abmeldung bei Inaktivität des Benutzers
  - Keine Meldung beim Trial-Modus
  - Keine Meldung beim automatischen Speichern
  - Keine Fortschrittsanzeige beim Speichern oder Hochladen von Dateien
  - Keine automatische Weiterleitung an die geänderte IP-Adresse

## Vorgehensweise

1. Geben Sie in das Eingabefeld "Kontaktperson" den für das Gerät zuständigen Ansprechpartner ein.
2. Geben Sie in das Eingabefeld "Gerätestandort" die Ortsbezeichnung des Aufstellungsorts ein.
3. Geben Sie in das Eingabefeld "Systemname" den Namen des Geräts ein.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Hinweis: Die Schritte 1 - 3 können auch mit einem SNMP Management Tool durchgeführt werden.

### 5.5.2.2 Koordinaten

#### Informationen über die geografischen Koordinaten

Im Fenster "Geografische Koordinaten" können Informationen über die geografischen Koordinaten eingetragen werden. Die Parameter der geografischen Koordinaten (Breitengrad, Längengrad und die Höhe über dem Ellipsoid gemäß WGS84) werden direkt in die Eingabefelder im Fenster "Geografische Koordinaten" eingetragen.

**Ermittlung der Koordinaten und die Eingabeformate**

Nutzen Sie zur Ermittlung der geografischen Koordinaten des Geräts eine interaktive Karte oder einen GPS-Empfänger.

Sie können die geografischen Koordinaten im Format Grad, Minuten, Sekunden (DDD°MM'SS") oder in Dezimalgrad (DD.dddddd) eingeben.

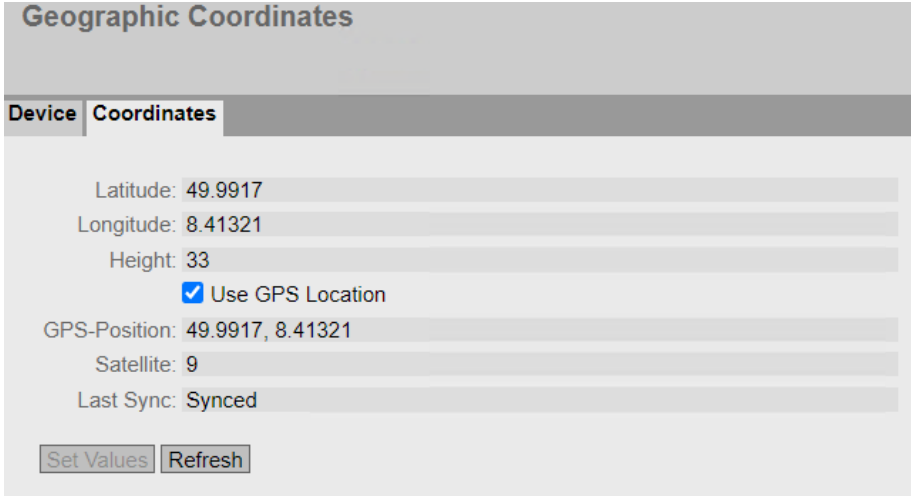
Das Format DDD°MM'SS" hat folgende Bedeutung:

Der Wert für die geografische Breite +49° 1´31.67" bedeutet, dass sich das Gerät auf 49 Grad, 1 Bogenminute und 31.67 Bogensekunden nördliche Breite befindet.
Die südliche Breite wird mit einem führenden Minuszeichen oder mit den Buchstaben N (nördliche Breite) oder S (südliche Breite) dargestellt, z. B. 49° 1´31.67" N.

Der Wert für die geografische Länge +8° 20´58.73" bedeutet, dass sich das Gerät auf 8 Grad, 20 Bogenminuten und 58.73 Bogensekunden östliche Länge befindet.
Die westliche Länge wird mit einem führenden Minuszeichen oder mit den Buchstaben O bzw. E (östliche Länge) oder W (westliche Länge) dargestellt, z. B. 8° 20´58.73" E.

Die GPS-Koordinaten werden im Format DD.dddddd angegeben. Dabei stehen "DD" für Breiten- bzw. Längengrad und "dddddd" für dezimalen Breiten- bzw. Längengrad.

Höhen werden im Format dddd m dargestellt. 33 m bedeutet, dass sich das Gerät in einer Höhe von 33 m über normal Null befindet. Höhenangaben unterhalb von normal Null (z. B. am Toten Meer) werden mit einem führenden Minuszeichen dargestellt.



## Beschreibung

Die Seite enthält folgende Eingabefelder mit einer maximalen Länge von 32 Zeichen:

- **Geographische Breite**
  Geben Sie den Wert für nördliche oder südliche Breite für den Standort des Gerätes an.
- **Geographische Länge**
  Geben Sie den Wert für östliche oder westliche Länge für den Standort des Gerätes an.
- **Geografische Höhe**
  Geben Sie den Wert für geografische Höhe über oder unter normal Null (Meereshöhe) in Metern an.

MUM85x :

Das Gerät MUM85x verfügt über die GPS-Funktion, durch die das Gerät seinen Standort ermittelt. Die Genauigkeit der Standortbestimmung liegt bei ca. 10 Meter. Die GPS-Position wird alle 60 Sekunden aktualisiert.

Zusätzliche Felder:

- **Use GPS Location**
  Aktiviert oder deaktiviert ein automatisches Auslesen des Standortes des Geräts.
  Wenn Sie die Option aktivieren, dann werden die Eingabefelder für die geografische Breite, Länge und Höhe nicht editierbar.
- **GPS-Position**
  Zeigt die aktuelle GPS-Position im Dezimal-System in der Reihenfolge "Breitengrad, Längengrad, Höhe" an.
- **Satellite**
  Zeigt die Anzahl verfügbarer Satelliten an.
- **Last Sync**
  Zeigt den Status der Synchronisierung an:
  - Synced
    Die Standortbestimmung wurde durchgeführt.
  - Not Synced
    Die Standortbestimmung wurde nicht durchgeführt.
  - >= <Zeit in Minuten>
    Die Zeit in Minuten seit dem letzten Standortbestimmungsversuch.

## Vorgehensweise

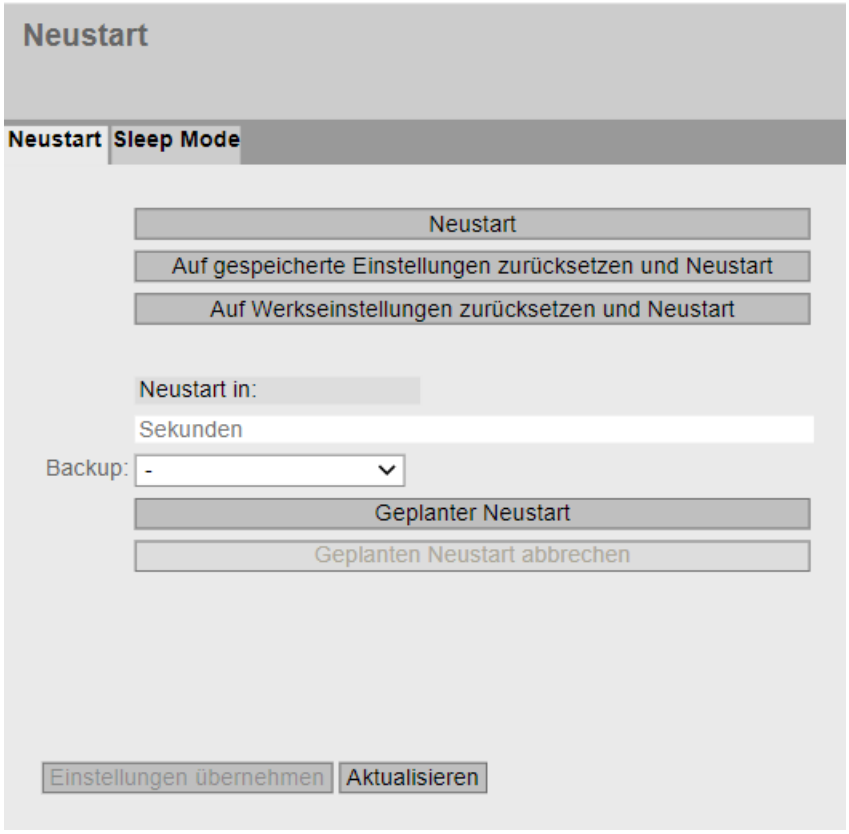
1. Geben Sie in das Eingabefeld "Geographische Breite" den ermittelten Breitengrad ein.
2. Geben Sie in das Eingabefeld "Geographische Länge" den ermittelten Längengrad ein.
3. Geben Sie in das Eingabefeld "Geographische Höhe" die ermittelte Höhe über dem Meeresspiegel ein.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

## 5.5.3 Neustart

### 5.5.3.1 Neustart

#### Zurücksetzen der Voreinstellungen

Über diese WBM-Seite kann der Neustart des Geräts manuell oder geplant erfolgen. Außerdem gibt es verschiedene Möglichkeiten die Voreinstellungen des Geräts zurückzusetzen.




#### Neustart

Beachten Sie folgende Punkte beim Neustart eines Geräts:

- Sie können einen Neustart des Geräts nur mit Administrator-Rechten durchführen.
- Der Neustart eines Geräts sollte nur durch die Schaltflächen dieses Menüs oder durch die entsprechenden CLI-Befehle und nicht durch Aus- und Einschalten der Spannungsversorgung am Gerät erfolgen.

- Wenn sich das Gerät im Modus "Trial" befindet, müssen Konfigurationsänderungen vor einem Neustart manuell abgespeichert werden. Vorgenommene Änderungen werden erst nach dem Anklicken der Schaltfläche "Einstellungen übernehmen" auf der jeweiligen WBM-Seite im Gerät wirksam.
- Wenn sich das Gerät im Modus "Automatisches Speichern" befindet, werden die letzten Änderungen automatisch vor einem Neustart gespeichert.

## Beschreibung

Für den Neustart des Geräts stehen Ihnen mit den Schaltflächen auf dieser Seite folgende Möglichkeiten zur Verfügung:

- **Neustart**
  Klicken Sie auf diese Schaltfläche, um das System neu zu starten. Sie müssen den Neustart in einer Dialogbox bestätigen. Bei einem Neustart wird das Gerät neu initialisiert, die interne Firmware wird neu geladen und das Gerät führt einen Selbsttest durch. Die Einstellungen der Startkonfiguration bleiben erhalten, z. B. die IP-Adresse des Geräts. Die gelernten Einträge in der Adresstabelle werden gelöscht. Sie können das Browser-Fenster geöffnet lassen, während das Gerät neu startet. Nach dem Neustart müssen Sie sich wieder neu anmelden.
- **Auf gespeicherte Einstellungen zurücksetzen und Neustart**
  Klicken Sie diese Schaltfläche, um die werksseitigen Konfigurationseinstellungen mit Ausnahme der geschützten Voreinstellungen wiederherzustellen und das Gerät neu zu starten.
  Die folgenden Parameter gehören zu den geschützten Voreinstellungen:
  - IP-Adressen
  - Subnetzmaske
  - IP-Adresse des Standard-Gateways
  - DHCP Client ID
  - DHCP
  - Systemname
  - System-Aufstellungsort
  - System-Ansprechpartner
  - Benutzernamen und Passwörter
  - Anmeldetext
  - PROFINET-Gerätename

- **Auf Werkseinstellungen zurücksetzen und Neustart**
  Klicken Sie auf diese Schaltfläche, um die werksseitigen Konfigurationseinstellungen wiederherzustellen. Es werden auch die geschützten Voreinstellungen zurückgesetzt. Bei SCALANCE MUM85x werden angelegte eSIM-Profile gelöscht.
  Es wird ein automatischer Neustart ausgeführt.
  **SCALANCE MUM85x:** Schalten Sie das Gerät nicht aus, bis es neu gestartet hat. Wird das Gerät während des Vorgangs ausgeschaltet, werden eSIM-Profile möglicherweise nicht vollständig gelöscht. Das führt dazu, dass keine Nachricht an Mobilfunkanbieter über freizugebende eSIM gesendet wird. In diesem Fall müssen Sie eine neue eSIM für den Mobilfunkvertrag beantragen.

  **Hinweis**

  Durch das Zurücksetzen auf die werkseitigen Konfigurationseinstellungen verliert das Gerät seine projektierte IP-Adresse, siehe Kapitel "Voraussetzungen für den Betrieb".

  - M87x, MUM856, M81x, M804PB: Das Gerät ist wieder über die werkseitig eingestellte IP-Adresse 192.168.1.1 zu erreichen.
  - M826: Dem Gerät muss eine IP-Adresse zugeordnet werden.

- **Neustart in**
  Geben Sie die Zeitdauer an, nach der das Gerät neu startet.
- **Backup**
  Auswählbar sind die unter "System **>** Backup der Konfiguration" erstellten Backups der Konfiguration. Vor dem geplanten Neustart, übernimmt das Gerät die Konfigurationen des ausgewählten Backups und arbeitet nach dem Neustart mit diesen weiter.
  Dabei gehen alle bis dahin vorgenommenen und nicht in einem Backup gespeicherten Konfigurationen verloren.
  Bei der Einstellung "-" ist keine Datei ausgewählt und das Gerät verwendet nach dem Neustart die aktuelle Konfiguration.
- **Geplanter Neustart**
  Wenn Sie auf die Schaltfläche klicken, startet ein Timer und läuft mit der definierten Zeit rückwärts. Wenn der Timer abgelaufen ist, startet das Gerät neu.
  Zusätzlich wird im Anzeigebereich die folgende Meldung angezeigt: "Der automatische Neustart beginnt in [..] Minuten. Klicken Sie auf 'Geplanten Neustart abbrechen', um den Neustart abzubrechen". Diese Meldung ist auf jeder WBM-Seite sichtbar, bis Sie das Neustarten abbrechen oder das SCALANCE-Gerät neu gestartet wird.

  **Hinweis**

  **Nicht gespeicherte Konfiguration geht nach Neustart verloren**

  Der geplante Neustart wird nach Ablauf der Zeit ohne weitere Meldung durchgeführt. Nicht gespeicherte Konfigurationsänderungen gehen verloren.

  Speichern Sie die aktuelle Konfiguration über "System > Backup der Konfiguration", bevor Sie den Timer für den Neustart einstellen.

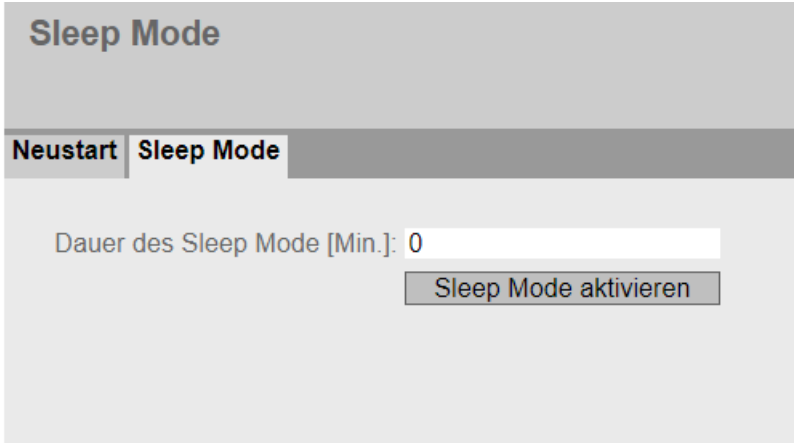
- **Geplanten Neustart abbrechen**
  Mit dieser Schalfläche deaktivieren Sie den Timer für den geplanten Neustart.

### 5.5.3.2 Sleep Mode

MUM85x

Um den Stromverbrauch des Geräts zu senken, können Sie den Energiesparmodus "Sleep Mode" nutzen. In diesem Modus befindet sich das Gerät im Ruhezustand und wechselt nach Ablauf der eingestellten Zeit in den vorherigen Zustand. Wenn der Sleep Mode aktiviert wird, werden alle Prozesse abgebrochen, z.B. Firmware-Update.

Auf dieser Seite legen Sie fest, nach welcher Zeit das im Energiesparmodus befindliche Gerät wieder aufwacht.




## Beschreibung

- **Dauer des Sleep Mode [Min.]**
  Geben Sie an, wie lange das Gerät im Energiesparmodus bleiben soll.
  Wertebereich 1 ... 44639. Standardwert 0: Energiesparmodus aus
- **Sleep Mode aktivieren**
  Mit dieser Schalfläche aktivieren Sie den Timer für die Ruhepause.

## Vorgehensweise

1. Geben Sie in das Eingabefeld "Dauer des Sleep Mode [Min.]" einen Wert von 1 ... 44639 Minuten ein.
2. Klicken Sie auf die Schaltfläche "Sleep Mode aktivieren".

**Ergebnis**

Das Gerät übernimmt die Einstellung für die Zeitdauer und schaltet unmittelbar in den Ruhezustand um. Nach Ablauf der Zeit kehrt das Gerät in den aktiven Zustand zurück. Der digitale Ausgang ist nach dem erneuten Anlauf deaktiviert.

## 5.5.4 Laden & Speichern

### 5.5.4.1 Dateiliste

#### Übersicht der Dateitypen

Die Dateiliste ist zur besseren Übersicht in verschiedene Bereiche getrennt.

| Bereich | Dateityp | Beschreibung | Laden | Speichern | Löschen[1)] |
|---|---|---|---|---|---|
| **Aktualisierung** | Firmware | Die Firmware ist signiert und verschlüsselt. Damit ist sichergestellt, dass nur von Siemens erstellte Firmware in das Gerät geladen werden kann. | X | X | -- |

| Bereich | Dateityp | Beschreibung | Laden | Speichern | Löschen[1)] |
|---|---|---|---|---|---|
| **Konfiguration** | Config | Diese Datei enthält die Startkonfiguration.<br>Diese Datei enthält unter anderem die Definitionen der Benutzer, Rollen, Gruppen und Funktionsrechte. Die Passwörter sind in der Datei "Users" abgespeichert.<br>Die Datei kann vor dem Herunterladen mit einem Passwort versehen werden. Um die Datei erfolgreich ins Gerät zuladen, ist das festgelegte Passwort zu verwenden. Das Passwort geben Sie auf der WBM-Seite "Passwörter (Seite 208)" ein.<br>Wenn die Datei mit einem Passwort geschützt ist, können Sie die Datei nicht über DHCP mit den Optionen 66 und 67 laden. | X | X | -- |
| | ConfigPack | Detaillierte Konfigurationsinformationen z. B. Startkonfiguration, Benutzer, Zertifikate, Favoriten Firmware des Geräts (wenn mitgespeichert).<br>Die Datei kann vor dem Herunterladen mit einem Passwort versehen werden. Um die Datei erfolgreich ins Gerät zuladen, ist das festgelegte Passwort zu verwenden. Das Passwort geben Sie auf der WBM-Seite "Passwörter (Seite 208)" ein.<br>Nähere Informationen zur Erstellung und Benutzung des ConfigPack inkl. Firmware finden Sie in Kapitel "Instandhalten und Warten".<br>Wenn die Datei mit einem Passwort geschützt ist, können Sie die Datei nicht über DHCP mit den Optionen 66 und 67 laden. | X | X | -- |
| | ConfigPack-Backup | In dieser ZIP-Datei sind alle Konfigurationsbackups gespeichert, die Sie erstellt haben. | X | X | X |
| | LoginWelcomeMessage | Die txt-Datei enthält den gewünschten Text oder die ASCII-Art. Unterstützt werden nur reine Textdateien im ASCII-Format. | X | X | X |
| | RunningCLI | Textdatei mit CLI-Befehlen<br>Diese Datei enthält eine Übersicht der aktuellen Konfiguration in Form von CLI-Befehlen. Passwörter sind in dieser Datei wie folgt maskiert: [PASSWORD]<br>Sie können die Textdatei herunterladen. Die Datei ist nicht dafür vorgesehen, dass Sie sie unverändert wieder hochladen. | -- | X | -- |
| | RunningSINEMAConfig | In diesen Dateityp speichern Sie die aktuelle Konfiguration des Geräts für eine Übergabe an STEP7 Basic/ Professional. Die Datei kann in STEP7 Basic/Professional importiert und auf ein Gerät mit gleicher Artikelnummer und Firmware-Version aufgespielt werden.<br>Bevor Sie eine Datei abspeichern können, müssen Sie im WBM unter "System > Laden&Speichern > Passwörter" ein Passwort für die "RunningSINEMAConfig" vergeben. Dieses Passwort benötigen Sie auch, um die Datei in STEP7 Basic/Professional zu importieren.<br>siehe auch "SINEMAConfig" | -- | X | -- |
| | Script | Textdatei mit CLI-Befehlen | X | -- | -- |

| Bereich | Dateityp | Beschreibung | Laden | Speichern | Löschen[1)] |
|---|---|---|---|---|---|
| | | Sie können eine Skriptdatei in einem Gerät hochladen. Die enthaltenen CLI-Befehle werden entsprechend ausgeführt.<br>CLI-Befehle zum Speichern und Laden von Dateien können nicht über die CLI-Skriptdatei ausgeführt werden. | | | |
| | SINEMAConfig | Über diesen Dateityp laden Sie Konfigurationsdaten, die über STEP7 Basic/Professional für eine Übergabe an das WBM exportiert wurden.<br>Um eine Datei laden zu können, müssen Sie unter "System > Laden&Speichern > Passwörter" ein Passwort für die "SINEMAConfig" vergeben. Dieses Passwort benötigen Sie auch, um die Datei aus STEP7 Basic/Professional zu exportieren.<br>siehe auch "RunningSINEMAConfig" | X | -- | -- |
| | Users | Datei mit Benutzernamen und Passwörter | X | X | -- |
| | WBMFav | WBM Favoriten<br>Diese Datei enthält die Favoriten, die Sie im WBM angelegt haben. Sie können diese Datei herunterladen und in anderen Geräten hochladen. | X | X | X |

| Bereich | Dateityp | Beschreibung | Laden | Speichern | Löschen[1)] |
|---|---|---|---|---|---|
| **Zertifikate & Schlüssel** | HTTPSCert | Voreingestellte HTTPS-Zertifikate inkl. Schlüssel<br>Die voreingestellten und automatisch erstellten HTTPS-Zertifikate sind selbst-signiert.<br>Es wird dringend empfohlen eigene HTTPS-Zertifikate zu erstellen und bereitzustellen. Es wird empfohlen HTTPS-Zertifikate zu verwenden, die entweder durch eine zuverlässige externe oder eine interne Zertifizierungsstelle signiert sind. Das HTTPS-Zertifikat überprüft die Identität des Geräts und regelt den verschlüsselten Datenaustausch.<br>Folgende Dateitypen können in das Gerät geladen werden.<br>• .pem<br>Um ein HTTPS-Zertifikat mit diesem Dateityp erfolgreich in das Gerät zu laden, muss bei dem Zertifikat der unverschlüsselte Private-Key enthalten sein.<br>• .p12<br>Bei HTTPS-Zertifikaten mit diesem Dateityp ist der Private-Key verschlüsselt und mit einem Passwort gesichert enthalten.<br>Um das Zertifikat erfolgreich ins Gerät zuladen, geben Sie auf der WBM-Seite "Passwörter (Seite 208)" das für die Datei festgelegte Passwort ein.<br>**Es wird empfohlen, passwortgeschützte Zertifikate im PKCS#12-Format mit einer Schlüssellänge von mindestens 4096 Bit zu verwenden.**<br>Maximale Schlüssellänge: 8192 Bit | X | X | X |
| | SSHPrivateKeyECDSA | SSH Privater Schlüssel (ECDSA)<br>Unterstützt wird der SSH-Schlüssel ecdsa-sha2-nistp521.<br>Es gibt Dateien, deren Zugriff passwortgeschützt ist. Um die Datei erfolgreich ins Gerät zuladen, geben Sie auf der WBM-Seite "Passwörter (Seite 208)" das für die Datei festgelegte Passwort ein. | X | X | X |
| | SSHPrivateKeyRSA | SSH Privater Schlüssel (RSA) mit und ohne Passwort<br>Unterstützt werden die folgenden SSH-Schlüssel:<br>• rsa-sha2-512<br>• rsa-sha2-256<br>Es gibt Dateien, deren Zugriff passwortgeschützt ist. Um die Datei erfolgreich ins Gerät zuladen, geben Sie auf der WBM-Seite "Passwörter (Seite 208)" das für die Datei festgelegte Passwort ein. | X | X | X |
| | X509Cert | Mit Zertifikaten werden verschiedene Teilnehmer zertifiziert.<br>Folgende Dateitypen können in das Gerät geladen werden: | X | X | -- |

| Bereich | Dateityp | Beschreibung | Laden | Speichern | Löschen[1)] |
|---|---|---|---|---|---|
| | | • .crt, pem, zip: Maximale Dateinamenlänge 255 Zeichen<br>• .p12: Maximale Dateinamenlänge 248 Zeichen<br>Es gibt Dateien, deren Zugriff passwortgeschützt ist. Um die Datei erfolgreich ins Gerät zuladen, geben Sie auf der WBM-Seite "Passwörter (Seite 208)" das für die Datei festgelegte Passwort ein.<br>Die geladenen Dateien werden auf "Security > Zertifikate > Übersicht (Seite 401)" aufgelistet.<br>Weiterführende Information zu Zertifikaten finden Sie unter "Zertifikate (Seite 403)". | | | |
| **Dienste & Log** | Debug | Diese Datei beinhaltet Informationen für den Siemens Support.<br>Sie ist verschlüsselt und kann ohne Sicherheitsrisiko per E-Mail an den Siemens Support gesendet werden. | -- | X | X |
| | DebugExt | Diese Datei beinhaltet ausführlichere Informationen für den Siemens Support.<br>Sie ist verschlüsselt und kann ohne Sicherheitsrisiko per E-Mail an den Siemens Support gesendet werden. Das Speichern der Datei kann einige Zeit in Anspruch nehmen. | -- | X | -- |
| | LogFile | Datei mit Einträgen aus der Ereignisprotokolltabelle | -- | X | -- |
| | ModemQualityLog | Textdatei<br>Diese Dateien enthält unter anderen Informationen zu Signalstärke, Signalqualität und die GPS-Position des Standorts.<br>Für die Erfassung der GPS-Postion, aktvieren Sie "GPS Standort verwenden" unter "System > Allgemein > Koordinaten" | -- | X | -- |
| | StartupInfo | Startup Logdatei<br>Diese Datei enthält die Meldungen, die während des letzten Hochlaufs in der Logdatei eingetragen wurden. | -- | X | -- |
| **Information** | MIB | Private MSPS MIB-Datei "Scalance_m_msps.mib" | -- | X | -- |

[1)] Löschen ist nur über HTTP/HTTPS möglich.

### 5.5.4.2 HTTP

#### Laden und Speichern von Daten über HTTP

Das WBM bietet die Möglichkeit, Gerätedaten in einer externen Datei auf Ihrem Client-PC zu speichern bzw. solche Daten aus einer externen Datei vom PC in die Geräte zu laden. So können Sie z. B. eine neue Firmware aus einer Datei von Ihrem Admin-PC laden. Zudem lassen sich auf dieser Seite die Zertifikate laden, die für den Aufbau einer gesicherten VPN-Verbindung notwendig sind.

**Firmware**

Die Firmware ist signiert und verschlüsselt. Damit ist sichergestellt, dass nur von Siemens erstellte Firmware in das Gerät geladen werden kann.

**Konfigurationsdateien**

---

**Hinweis**

**Konfigurationsdateien und Modus Trial/Automatisches Speichern**

Im Modus "Automatisches Speichern" wird eine automatische Sicherung durchgeführt, bevor die Konfigurationsdateien (ConfigPack und Config) übertragen werden.
Im Modus "Trial" werden Änderungen zwar übernommen aber nicht in den Konfigurationsdateien (ConfigPack und Config) gespeichert. Verwenden Sie die Schaltfläche "Schreiben der Startkonfiguration" auf der WBM-Seite "System > Konfiguration", um Änderungen in den Konfigurationsdateien abzuspeichern.

---

**CLI-Skriptdatei**

Sie können bestehende CLI-Konfigurationen herunterladen (RunningCLI) und eigene CLI-Skripte hochladen (Script).

---

**Hinweis**

Das herunterladbare CLI-Skript ist nicht dafür vorgesehen, dass Sie es unverändert wieder hochladen.

CLI-Befehle zum Speichern und Laden von Dateien können nicht über die CLI-Skriptdatei (Script) ausgeführt werden.

---

**Austausch von Konfigurationsdaten mit STEP7 Basic/Professional über eine Datei**

Über die beiden Dateitypen "RunningSINEMAConfig" und "SINEMAConfig" können Sie Konfigurationsdaten zwischen einem Gerät (WBM) und STEP7 Basic/Professional über eine Datei austauschen.

Voraussetzungen:

- Gleiche Artikelnummer
- Gleiche Firmware-Version
- Passwort
  Das Passwort vergeben Sie im WBM unter "System > Laden&Speichern > Passwörter".

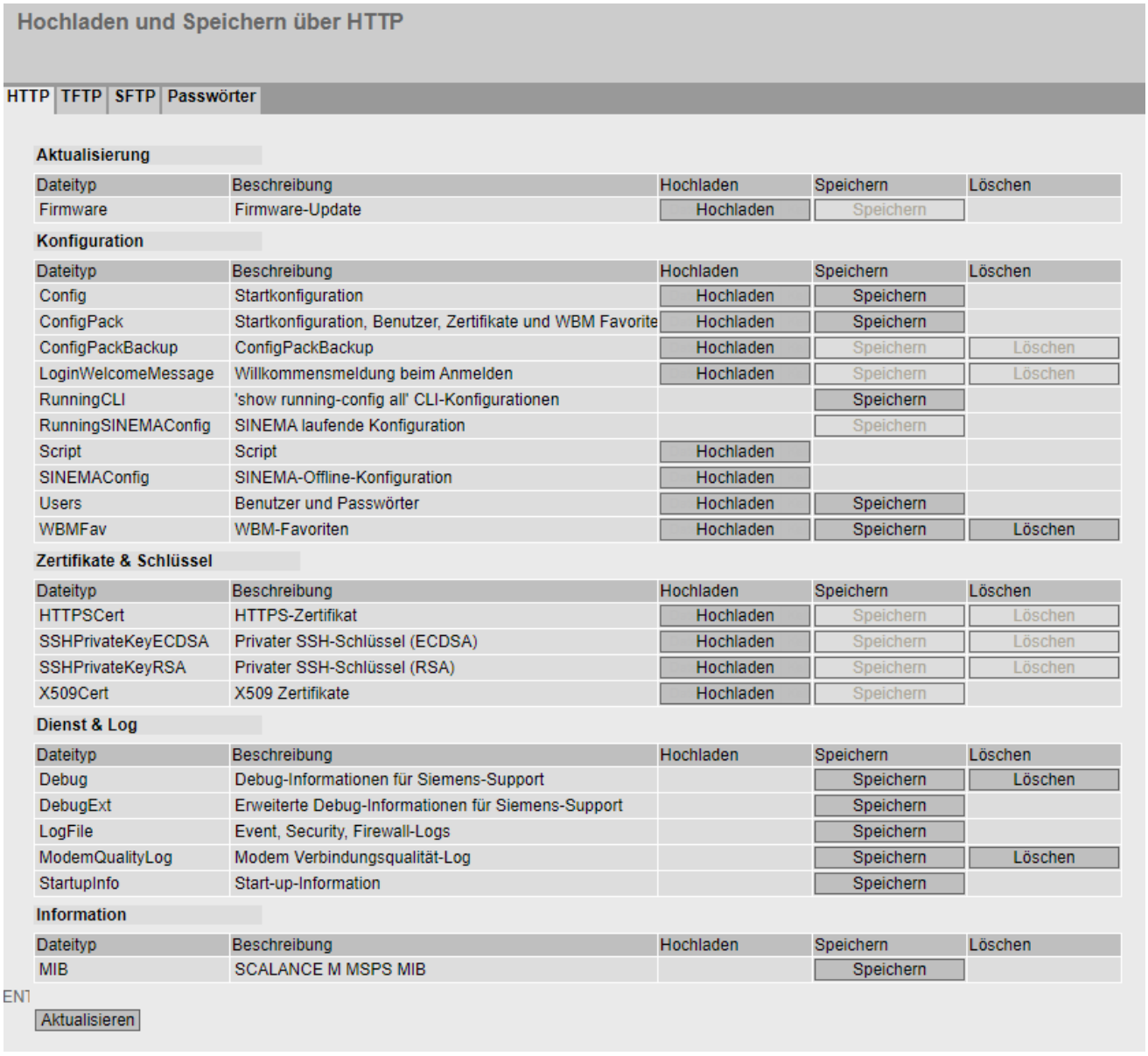
Die Dateitypen können wie folgt genutzt werden:

- Zur Offline-Diagnose
  Sie können die fehlerhafte Konfiguration eines Geräts als "RunningSINEMAConfig" über das WBM speichern und in STEP7 Basic/Professional importieren. Die Diagnose in STEP7 Basic/Professional erfolgt, ohne dass eine Verbindung zu einem realen Gerät besteht. Eine korrigierte Konfiguration kann exportiert und als "SINEMAConfig" wieder über das WBM geladen werden.
- Zur Konfiguration
  Sie können ein Gerät in STEP7 Basic/Professional konfigurieren, ohne dass eine Verbindung zu einem realen Gerät besteht. Die Konfiguration kann exportiert und als "SINEMAConfig" über das WBM in das reale Gerät geladen werden.

**X509-Zertifikate**

Folgende Dateitypen können in das Gerät geladen werden:

- .crt, pem, zip: Maximale Dateinamenlänge 255 Zeichen
- .p12: Maximale Dateinamenlänge 248 Zeichen



## Beschreibung

Die Tabellen sind zur besseren Übersicht in verschiedene Bereiche getrennt. Jede Tabelle gliedert sich in folgende Spalten:

- **Dateityp**
  Zeigt den Dateityp an.
- **Beschreibung**
  Zeigt die Kurzbeschreibung des Dateityps an.
- **Hochladen**
  Mit dieser Schaltfläche können Sie Dateien auf das Gerät hochladen. Die Schaltfläche ist aktivierbar, wenn diese Funktion von dem Dateityp unterstützt wird.
- **Speichern**
  Mit dieser Schaltfläche können Sie Dateien vom Gerät speichern. Die Schaltfläche ist nur aktivierbar, wenn diese Funktion von dem Dateityp unterstützt wird und die Datei auf dem Gerät vorhanden ist.
- **Löschen**
  Mit dieser Schaltfläche können Sie Dateien vom Gerät löschen. Die Schaltfläche ist nur aktivierbar, wenn diese Funktion von dem Dateityp unterstützt wird und die Datei auf dem Gerät vorhanden ist.

**Hinweis**

Löschen Sie nach einem Firmware-Update den Cache des Webbrowsers.

## Vorgehensweise

**Daten über HTTP hochladen**

1. Starten Sie das Hochladen durch Anklicken einer der Schaltflächen "Hochladen".

   **Hinweis**

   **Dateien, deren Zugriff passwortgeschützt ist**

   Um diese Dateien zu speichern oder erfolgreich ins Gerät zuladen, müssen Sie unter "System > Laden & Speichern > Passwörter" das für die Datei festgelegte Passwort eingeben.

   Es öffnet sich ein Dialogfenster zum Hochladen einer Datei.

2. Navigieren Sie zu der gewünschten Datei, die geladen werden soll, und klicken Sie im Dialogfenster auf die Schaltfläche "Öffnen".
   Die Datei wird hochgeladen.

3. Wenn ein Neustart notwendig ist, wird eine entsprechende Meldung ausgegeben. Klicken Sie auf die Schaltfläche "OK", um den Neustart durchzuführen. Wenn Sie auf die Schalfläche "Abbrechen" klicken, wird kein Neustart des Geräts durchgeführt. Erst nach einem Neustart werden die Änderungen wirksam.
   Ob ein Neustart notwendig ist, hängt von der geladenen Datei ab. Einige Dateien werden sofort ausgeführt, z. B. die CLI-Skriptdatei, und neue Einstellungen werden ohne Neustart übernommen.

   **Hinweis**

   **Cell-Firmware-Update M87x**

   Nach einem Cell-Firmware-Update führt das Gerät automatisch einen Neustart durch.

**Daten über HTTP herunterladen**

1. Starten Sie das Herunterladen durch Anklicken einer der Schaltflächen "Speichern".
2. Wählen Sie einen Speicherort und einen Namen für die Datei.
3. Speichern Sie die Datei.
   Die Datei wird heruntergeladen und gespeichert.

**Daten über HTTP löschen**

1. Starten Sie das Löschen durch Anklicken einer der Schaltflächen "Löschen".
   Die zu löschende Datei wird gelöscht.

**Konfigurationsdaten wiederverwenden**

Wenn mehrere Geräte die gleiche Konfiguration erhalten sollen und die Zuweisung der IP-Adressen über DHCP erfolgt, kann durch Abspeichern und Einlesen von Konfigurationsdaten der Aufwand zur Neukonfiguration reduziert werden.

Gehen Sie folgendermaßen vor, um Konfigurationsdaten wiederzuverwenden:

1. Speichern Sie die Konfigurationsdaten eines konfigurierten Geräts auf Ihrem PC.
2. Laden Sie diese Konfigurationsdatei auf alle weiteren Geräte, die Sie konfigurieren wollen.
3. Falls für einzelne Geräte individuelle Einstellungen erforderlich sind, müssen Sie diese online am betreffenden Gerät vornehmen.

**Hinweis**

Konfigurationsdaten sind mit einer Prüfsumme versehen. Wenn Sie die Dateien bearbeiten, können Sie die Dateien nicht mehr auf das Gerät hochladen.

**Passwortgeschützte Config-Datei**

Wenn die Datei mit einem Passwort geschützt ist, können Sie die Datei nicht über DHCP mit den Optionen 66 und 67 laden.

### 5.5.4.3 TFTP

#### Laden und Speichern von Daten über einen TFTP-Server

Auf der Seite können Sie den TFTP-Server und die Dateinamen konfigurieren. Weiter bietet das WBM die Möglichkeit, Gerätedaten in einer externen Datei auf Ihrem Client-PC zu speichern bzw. solche Daten aus einer externen Datei vom PC in die Geräte zu laden. So können Sie z. B. eine neue Firmware aus einer Datei von Ihrem Admin-PC laden.

Zudem lassen sich auf dieser Seite die Zertifikate laden, die für den Aufbau einer gesicherten VPN-Verbindung notwendig sind.

**Firmware**

Die Firmware ist signiert und verschlüsselt. Es ist sichergestellt, dass nur von Siemens erstellte Firmware in das Gerät geladen werden kann.

**Konfigurationsdateien**

**Hinweis**

**Konfigurationsdateien und Modus Trial/Automatisches Speichern**

Im Modus "Automatisches Speichern" wird eine automatische Sicherung durchgeführt, bevor die Konfigurationsdateien (ConfigPack und Config) übertragen werden.
Im Modus "Trial" werden Änderungen zwar übernommen aber nicht in den Konfigurationsdateien (ConfigPack und Config) gespeichert. Verwenden Sie die Schaltfläche "Schreiben der Startkonfiguration" auf der WBM-Seite "System > Konfiguration", um Änderungen in den Konfigurationsdateien abzuspeichern.

**CLI-Skriptdatei**

Sie können bestehende CLI-Konfigurationen herunterladen (RunningCLI) und eigene CLI-Skripte hochladen (Script).

**Hinweis**

Das herunterladbare CLI-Skript ist nicht dafür vorgesehen, dass Sie es unverändert wieder hochladen.

CLI-Befehle zum Speichern und Laden von Dateien können nicht über die CLI-Skriptdatei (Script) ausgeführt werden.

**Austausch von Konfigurationsdaten mit STEP7 Basic/Professional über eine Datei**

Über die beiden Dateitypen "RunningSINEMAConfig" und "SINEMAConfig" können Sie Konfigurationsdaten zwischen einem Gerät (WBM) und STEP7 Basic/Professional über eine Datei austauschen.

Voraussetzungen:

- Gleiche Artikelnummer
- Gleiche Firmware-Version
- Passwort
  Das Passwort vergeben Sie im WBM unter "System > Laden&Speichern > Passwörter".

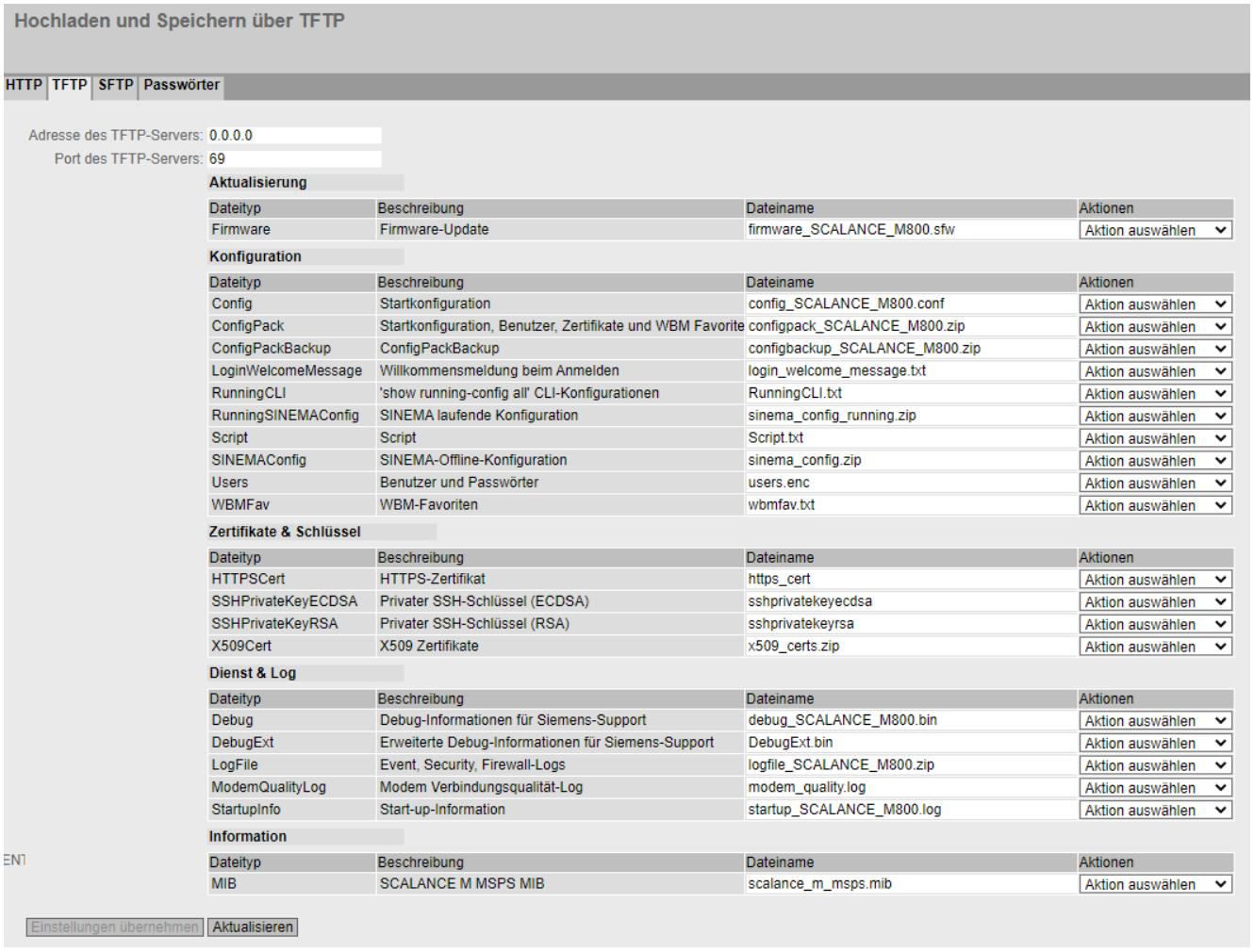
Die Dateitypen können wie folgt genutzt werden:

- Zur Offline-Diagnose
  Sie können die fehlerhafte Konfiguration eines Geräts als "RunningSINEMAConfig" über das WBM speichern und in STEP7 Basic/Professional importieren. Die Diagnose in STEP7 Basic/Professional erfolgt, ohne dass eine Verbindung zu einem realen Gerät besteht. Eine korrigierte Konfiguration kann exportiert und als "SINEMAConfig" wieder über das WBM geladen werden.
- Zur Konfiguration
  Sie können ein Gerät in STEP7 Basic/Professional konfigurieren, ohne dass eine Verbindung zu einem realen Gerät besteht. Die Konfiguration kann exportiert und als "SINEMAConfig" über das WBM in das reale Gerät geladen werden.

**X509-Zertifikate**

Folgende Dateitypen können in das Gerät geladen werden:

- .crt, pem, zip: Maximale Dateinamenlänge 255 Zeichen
- .p12: Maximale Dateinamenlänge 248 Zeichen




## Beschreibung

Die Seite enthält folgende Felder:

- **Adresse des TFTP-Servers**
  Geben Sie die IP-Adresse oder den FQDN (Fully Qualified Domain Name) des TFTP-Servers ein, mit dem Sie Daten austauschen.
- **Port des TFTP-Servers**
  Geben Sie den Port des TFTP-Servers ein, über den der Datenaustausch abgewickelt werden soll. Gegebenenfalls können Sie den Standardwert 69 entsprechend Ihren spezifischen Anforderungen ändern.

Die Tabellen sind zur besseren Übersicht in verschiedene Bereiche getrennt. Jede Tabelle gliedert sich in folgende Spalten:

- **Dateityp**
  Zeigt den Dateityp an.
- **Beschreibung**
  Zeigt die Kurzbeschreibung des Dateityps an.

- **Dateiname**
  Für jeden Dateityp ist hier ein Dateiname vorgegeben.

  **Hinweis**

  **Änderung des Dateinamens**

  Sie können den in dieser Spalte vorgegebenen Dateinamen ändern. Nach dem Laden auf das Gerät kann der geänderte Dateiname auch mit dem Command Line Interface genutzt werden.

- **Aktionen**
  Wählen Sie aus der Klappliste die Aktion aus. Die Auswahl ist abhängig vom gewählten Dateityp. z. B. eine Log-Datei können Sie nur speichern.
  Folgende Aktionen sind möglich:
  - **Datei speichern**
    Mit dieser Auswahl speichern Sie eine Datei auf den TFTP-Server.
  - **Datei hochladen**
    Mit dieser Auswahl laden Sie eine Datei vom TFTP-Server.

## Vorgehensweise

**Daten über TFTP laden bzw. speichern**

1. Geben Sie bei "Adresse des TFTP-Servers" die Adresse des TFTP-Servers ein.
2. Geben Sie bei "Port des TFTP-Servers" den verwendeten Port des TFTP-Servers ein.
3. Geben Sie ggf. bei "Dateiname" den Namen einer Datei ein, in die Sie speichern bzw. aus der Sie Daten übernehmen wollen.

   **Hinweis**

   **Dateien, deren Zugriff passwortgeschützt ist**

   Um diese Dateien zu speichern oder erfolgreich ins Gerät zuladen, müssen Sie unter "System > Laden & Speichern > Passwörter" das für die Datei festgelegte Passwort eingeben.

4. Wählen Sie in der Klappliste "Aktionen" die Aktion aus, die Sie durchführen wollen.
5. Klicken Sie auf "Einstellungen übernehmen", um die ausgewählte Aktion zu starten.
6. Wenn ein Neustart notwendig ist, wird eine entsprechende Meldung ausgegeben. Klicken Sie auf die Schaltfläche "OK", um den Neustart durchzuführen. Wenn Sie auf die Schalfläche "Abbrechen" klicken, wird kein Neustart des Geräts durchgeführt. Erst nach einem Neustart werden die Änderungen wirksam.

   **Hinweis**

   **Cell-Firmware-Update M87x**

   Nach einem Cell-Firmware-Update führt das Gerät automatisch einen Neustart durch.

**Konfigurationsdaten wiederverwenden**

Wenn mehrere identische Geräte die gleiche Konfiguration erhalten sollen und die Zuweisung der IP-Adressen über DHCP erfolgt, kann durch Abspeichern und Einlesen von Konfigurationsdaten der Aufwand zur Neukonfiguration reduziert werden.

Gehen Sie folgendermaßen vor, um Konfigurationsdaten wiederzuverwenden:

1. Speichern Sie die Konfigurationsdaten eines konfigurierten Geräts auf Ihrem PC.
2. Laden Sie diese Konfigurationsdatei auf alle weiteren Geräte, die Sie konfigurieren wollen.
3. Falls für einzelne Geräte individuelle Einstellungen erforderlich sind, müssen Sie diese online am betreffenden Gerät vornehmen.

Beachten Sie, dass die Konfigurationsdaten kodiert gespeichert werden. Deshalb können die Dateien nicht mit einem Texteditor bearbeitet werden.

**Hinweis**

Konfigurationsdaten sind mit einer Prüfsumme versehen. Wenn Sie die Dateien bearbeiten, können Sie die Dateien nicht mehr auf das Gerät hochladen.

**Passwortgeschützte Config-Datei**

Wenn die Datei mit einem Passwort geschützt ist, können Sie die Datei nicht über DHCP mit den Optionen 66 und 67 laden.

### 5.5.4.4 SFTP

#### Laden und Speichern von Daten über einen SFTP-Server

SFTP (SSH File Transfer Protocol) überträgt die Dateien verschlüsselt. Auf dieser Seite konfigurieren Sie die Zugangsdaten für den SFTP-Server.

Weiter können Sie Gerätedaten in einer externen Datei auf Ihrem Client-PC speichern bzw. solche Daten aus einer externen Datei vom PC in die Geräte laden. So können Sie z. B. eine neue Firmware aus einer Datei von Ihrem Admin-PC laden.

Zudem lassen sich auf dieser Seite die Zertifikate laden, die für den Aufbau einer gesicherten VPN-Verbindung notwendig sind.

**Firmware**

Die Firmware ist signiert und verschlüsselt. Es ist sichergestellt, dass nur von Siemens erstellte Firmware in das Gerät geladen werden kann.

**Konfigurationsdateien**

**Hinweis**

**Konfigurationsdateien und Modus Trial/Automatisches Speichern**

Im Modus "Automatisches Speichern" wird eine automatische Sicherung durchgeführt, bevor die Konfigurationsdateien (ConfigPack und Config) übertragen werden.
Im Modus "Trial" werden Änderungen zwar übernommen aber nicht in den Konfigurationsdateien (ConfigPack und Config) gespeichert. Verwenden Sie die Schaltfläche "Schreiben der Startkonfiguration" auf der WBM-Seite "System > Konfiguration", um Änderungen in den Konfigurationsdateien abzuspeichern.

**CLI-Skriptdatei**

Sie können bestehende CLI-Konfigurationen herunterladen (RunningCLI) und eigene CLI-Skripte hochladen (Script).

**Hinweis**

Das herunterladbare CLI-Skript ist nicht dafür vorgesehen, dass Sie es unverändert wieder hochladen.

CLI-Befehle zum Speichern und Laden von Dateien können nicht über die CLI-Skriptdatei (Script) ausgeführt werden.

**Austausch von Konfigurationsdaten mit STEP7 Basic/Professional über eine Datei**

Über die beiden Dateitypen "RunningSINEMAConfig" und "SINEMAConfig" können Sie Konfigurationsdaten zwischen einem Gerät (WBM) und STEP7 Basic/Professional über eine Datei austauschen.

Voraussetzungen:

- Gleiche Artikelnummer
- Gleiche Firmware-Version
- Passwort
  Das Passwort vergeben Sie im WBM unter "System > Laden&Speichern > Passwörter".

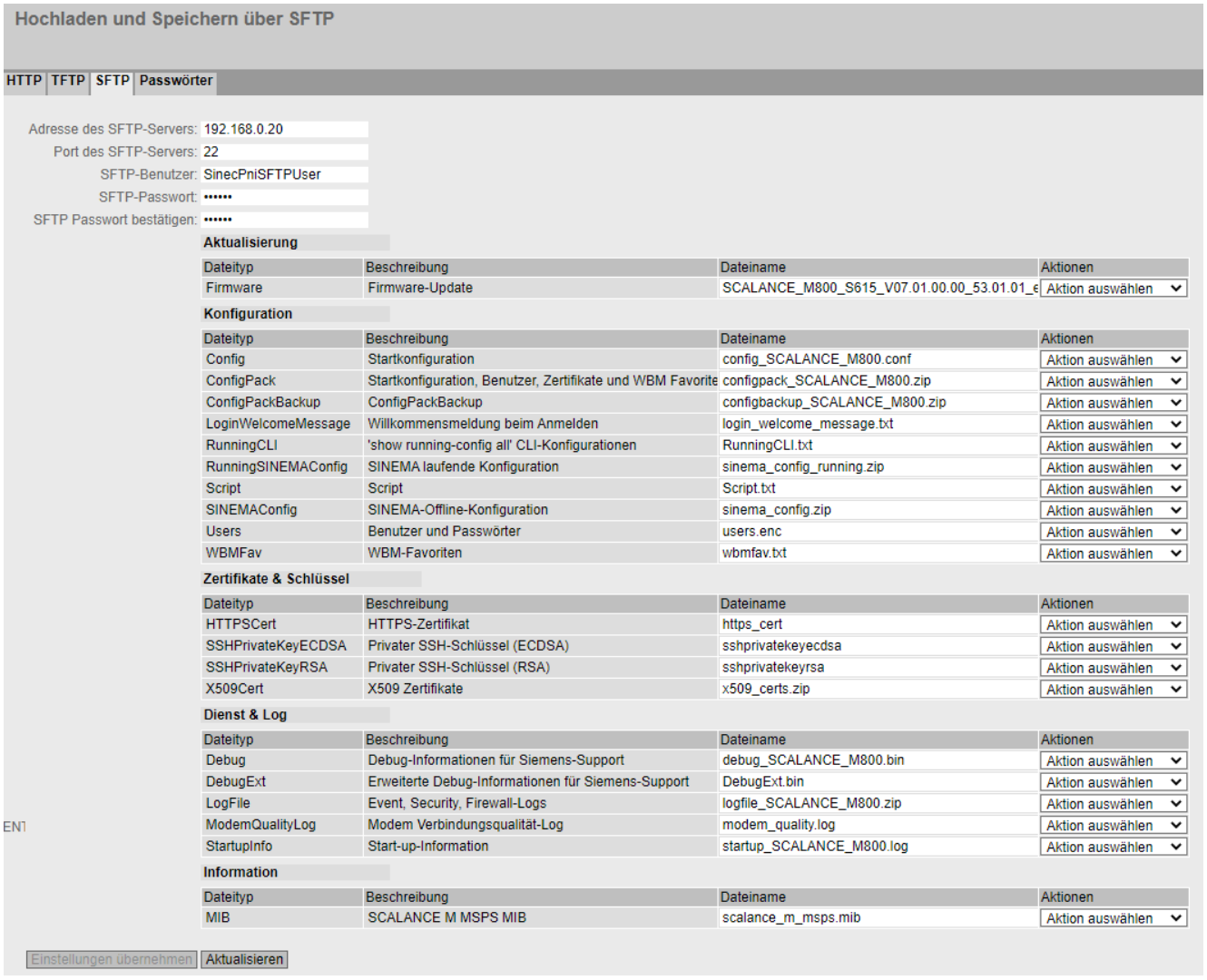
Die Dateitypen können wie folgt genutzt werden:

- Zur Offline-Diagnose
  Sie können die fehlerhafte Konfiguration eines Geräts als "RunningSINEMAConfig" über das WBM speichern und in STEP7 Basic/Professional importieren. Die Diagnose in STEP7 Basic/Professional erfolgt, ohne dass eine Verbindung zu einem realen Gerät besteht. Eine korrigierte Konfiguration kann exportiert und als "SINEMAConfig" wieder über das WBM geladen werden.
- Zur Konfiguration
  Sie können ein Gerät in STEP7 Basic/Professional konfigurieren, ohne dass eine Verbindung zu einem realen Gerät besteht. Die Konfiguration kann exportiert und als "SINEMAConfig" über das WBM in das reale Gerät geladen werden.

**X509-Zertifikate**

Folgende Dateitypen können in das Gerät geladen werden:

- .crt, pem, zip: Maximale Dateinamenlänge 255 Zeichen
- .p12: Maximale Dateinamenlänge 248 Zeichen




## Beschreibung

Die Seite enthält folgende Felder:

- **Adresse des SFTP-Servers**
  Geben Sie die IP-Adresse oder den FQDN des SFTP-Servers ein, mit dem Sie Daten austauschen.
- **Port des SFTP-Servers**
  Geben Sie den Port des SFTP-Servers ein, über den der Datenaustausch abgewickelt werden soll. Gegebenenfalls können Sie den Standardwert 22 entsprechend Ihren spezifischen Anforderungen ändern.
- **SFTP Benutzer**
  Geben Sie den Benutzer für den Zugriff auf den SFTP-Server ein. Vorausgesetzt, auf dem SFTP-Server ist ein Benutzer mit den entsprechenden Rechten angelegt.

- **SFTP Passwort**
  Geben Sie das Passwort für den Benutzer ein
- **SFTP Passwort bestätigen**
  Bestätigen Sie das Passwort.

Die Tabellen sind zur besseren Übersicht in verschiedene Bereiche getrennt. Jede Tabelle gliedert sich in folgende Spalten:

- **Dateityp**
  Zeigt den Dateityp an.
- **Beschreibung**
  Zeigt die Kurzbeschreibung des Dateityps an.
- **Dateiname**
  Für jeden Dateityp ist hier ein Dateiname vorgegeben.

  **Hinweis**

  **Änderung des Dateinamens**

  Sie können den in dieser Spalte vorgegebenen Dateinamen ändern. Nach dem Laden auf das Gerät kann der geänderte Dateiname auch mit dem Command Line Interface genutzt werden.

- **Aktionen**
  Wählen Sie aus der Klappliste die Aktion aus. Die Auswahl ist abhängig vom gewählten Dateityp. z. B. eine Log-Datei können Sie nur speichern.
  Folgende Aktionen sind möglich:
  - **Datei speichern**
    Mit dieser Auswahl speichern Sie eine Datei auf dem SFTP-Server.
  - **Datei hochladen**
    Mit dieser Auswahl laden Sie eine Datei vom SFTP-Server.

## Vorgehensweise

**Daten über SFTP laden bzw. speichern**

1. Geben Sie bei "Adresse des SFTP-Servers" die Adresse des SFTP-Servers ein.
2. Geben Sie bei "Port des SFTP-Servers" den verwendeten Port des SFTP-Servers ein.
3. Geben Sie die Benutzerdaten (Benutzername und Passwort) ein, die für den Zugriff auf den SFTP-Server notwendig sind.
4. Geben Sie ggf. bei "Dateiname" den Namen einer Datei ein, in die Sie speichern bzw. aus der Sie Daten übernehmen wollen.

   **Hinweis**

   **Dateien, deren Zugriff passwortgeschützt ist**

   Um diese Dateien zu speichern oder erfolgreich ins Gerät zu laden, müssen Sie unter "System > Laden & Speichern > Passwörter" das für die Datei festgelegte Passwort eingeben.

5. Wählen Sie in der Klappliste "Aktionen" die Aktion aus, die Sie durchführen wollen.

6. Klicken Sie auf "Einstellungen übernehmen", um die ausgewählte Aktion zu starten.
7. Wenn ein Neustart notwendig ist, wird eine entsprechende Meldung ausgegeben. Klicken Sie auf die Schaltfläche "OK", um den Neustart durchzuführen. Wenn Sie auf die Schalfläche "Abbrechen" klicken, wird kein Neustart des Geräts durchgeführt. Erst nach einem Neustart werden die Änderungen wirksam.

**Hinweis**

**Cell-Firmware-Update M87x**

Nach einem Cell-Firmware-Update führt das Gerät automatisch einen Neustart durch.

**Konfigurationsdaten wiederverwenden**

Wenn mehrere identische Geräte die gleiche Konfiguration erhalten sollen und die Zuweisung der IP-Adressen über DHCP erfolgt, kann durch Abspeichern und Einlesen von Konfigurationsdaten der Aufwand zur Neukonfiguration reduziert werden.

Gehen Sie folgendermaßen vor, um Konfigurationsdaten wiederzuverwenden:

1. Speichern Sie die Konfigurationsdaten eines konfigurierten Geräts auf Ihrem PC.
2. Laden Sie diese Konfigurationsdateien auf alle weiteren Geräte, die Sie so konfigurieren wollen.
3. Falls für einzelne Geräte individuelle Einstellungen erforderlich sind, müssen Sie diese online am betreffenden Gerät vornehmen.

**Hinweis**

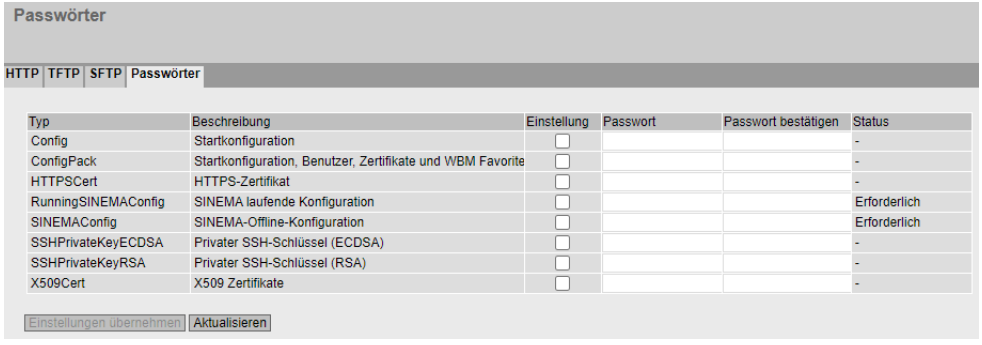
Konfigurationsdaten sind mit einer Prüfsumme versehen. Wenn Sie die Dateien bearbeiten, können Sie die Dateien nicht mehr auf das Gerät hochladen.

**Passwortgeschützte Config-Datei**

Wenn die Datei mit einem Passwort geschützt ist, können Sie die Datei nicht über DHCP mit den Optionen 66 und 67 laden.

### 5.5.4.5 Passwörter

Es gibt Dateien, deren Zugriff passwortgeschützt ist. Um z. B. das HTTPS-Zertifikat verwenden zu können, müssen Sie auf dieser WBM-Seite das entsprechende Passwort angeben.



## Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Typ**
  Zeigt den Dateityp an.
- **Beschreibung**
  Zeigt die Kurzbeschreibung des Dateityps an.
- **Einstellung**
  Nur aktivierbar, wenn ein Passwort konfiguriert ist.
  Wenn aktiviert, wird beim Laden geprüft, ob das Passwort dem für die Datei festgelegten Passwort entspricht.
- **Passwort**
  Geben Sie das Passwort für die Datei ein.
- **Passwort bestätigen**
  Bestätigen Sie das Passwort.
- **Status**
  - Gültig
    Das Optionskästchen "Aktiviert" ist aktiviert und das Passwort passt zu der Datei.
  - Ungültig
    Das Optionskästchen "Aktiviert" ist aktiviert, aber das Passwort passt nicht zur Datei oder es ist noch keine Datei geladen.
  - **"-"**
    Das Passwort kann nicht ausgewertet werden oder wird noch nicht verwendet. Das Optionskästchen "Aktiviert" ist nicht aktiviert.
  - Erforderlich
    Zum Laden oder Speichern ist ein Passwort erforderlich.

## Vorgehensweise

1. Tragen Sie bei "Passwort" das Passwort ein.
2. Um das Passwort zu bestätigen, tragen Sie bei "Passwort bestätigen" das Passwort nochmals ein.
3. Aktivieren Sie die Option "Aktiviert".
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

## 5.5.5 Ereignisse

### 5.5.5.1 Konfiguration der Ereignisse

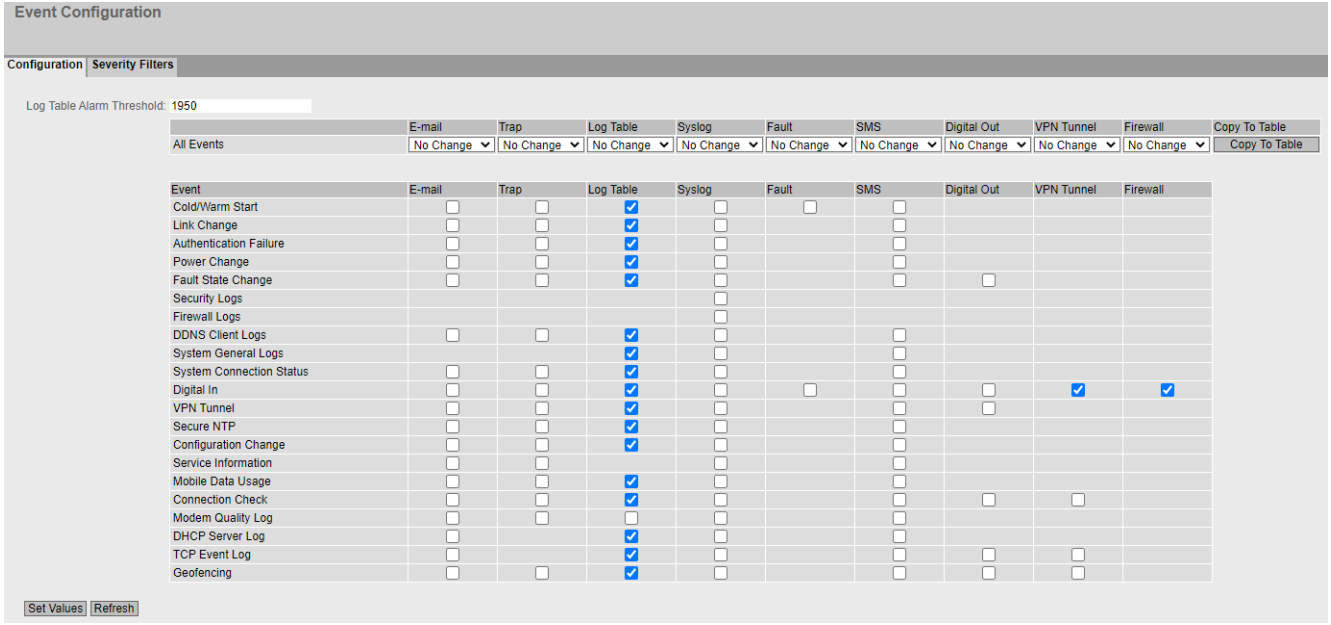
#### Systemereignisse auswählen

Auf der Seite legen Sie fest, welche Systemereignisse wie gemeldet werden oder eine Folgereaktion ausführen.

Folgende Meldungen werden immer in die Ereignisprotokoll-Tabelle eingetragen und sind nicht abwählbar:

- Ändern des Admin-Kennworts
- Starten des Geräts
- Betriebsstatus des Geräts, z. B. ob ein PLUG vorhanden ist oder nicht
- Status unerledigter Fehler

Um diese Meldungen zusätzlich an einen Syslog-Server zu senden, aktivieren Sie beim Ereignis "System Allgemein Logs" das Optionskästchen "Syslog".




#### Beschreibung

- **Log-Tabelle-Alarmschwellenwert**
  Legen Sie den Grenzwert für die Einträge pro Severity fest. Pro Severity sind maximal 2000 Einträge möglich.
  Wird der eingegebene Grenzwert mit dem nächsten Eintrag erreicht, wird eine Alarmmeldung ausgegeben, z.B. bei Eingabe 1950 kommt nach dem Eintrag 1949 die Meldung, dass der Grenzwert 1950 erreicht ist.

Mit Tabelle 1 können Sie alle Optionskästchen einer Spalte von Tabelle 2 auf einmal aktivieren oder deaktivieren.

Die Tabelle 1 gliedert sich in folgende Spalten:

- **Alle Ereignisse**
  Zeigt an, dass die Einstellungen für alle Ereignisse der Tabelle 2 gültig sind.
- **E-Mail / Trap / Log-Tabelle / Syslog / Fehler / SMS / Digitaler Ausgang / VPN-Tunnel / Cloud Connector / Firewall**
  Aktivieren oder deaktivieren Sie die gewünschte Art der Benachrichtigung für alle Ereignisse. Wenn "Keine Änderung" ausgewählt ist, bleiben die Einträge der entsprechenden Spalte in der Tabelle 2 unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ereignisse der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Ereignis**
  Die Spalte "Ereignis" enthält Folgendes:
  - Kalt-/Warmstart
    Das Gerät wurde eingeschaltet oder vom Anwender neu gestartet. Im Fehlerspeicher des Geräts wird ein neuer Eintrag mit der Art des durchgeführten Neustarts erzeugt.
  - Link Change
    Dieses Ereignis tritt nur auf, wenn der Port-Status überwacht wird und sich entsprechend geändert hat, siehe "System > Fehlerkontrolle > Link Change".
  - Authentifizierungsfehler
    Dieses Ereignis tritt beim Versuch eines Zugriffs mit fehlerhaftem Passwort auf.
  - Umschalten der Spannungsversorgung
    Dieses Ereignis tritt auf, wenn die Spannungsversorgungsleitungen 1 und 2 überwacht werden. Es zeigt an, dass ein Wechsel auf Leitung 1 bzw. auf Leitung 2 stattgefunden hat. Das Ereignis tritt auch auf, wenn die PoE-Spannungsversorgung ausgefallen ist, siehe "System > Fehlerkontrolle > Spannungsversorgung".
  - Änderung des Fehlerstatus
    Der Fehlerstatus hat sich geändert. Der Fehlerstatus kann sich auf die aktivierte Portüberwachung, auf das Ansprechen des digitalen Ausgangs oder die Spannungsüberwachung beziehen.
    Damit ein Fehler am digitalen Ausgang auch durch die Fehler-LED "F" signalisiert wird, müssen Sie "Änderung des Fehlerstatus" für den "Digitalen Ausgang" aktivieren. In diesem Fall leuchtet die Fehler-LED "F", wenn ein interner Fehler auftritt, und der digitale Eingang wird geschlossen.
  - Security-Logs
    Im Sicherheitslogbuch wird eingetragen, wenn das IPsec-Verfahren für VPN angewendet wird.
  - Firewall-Logs
    Im Firewall-Logbuch wird eingetragen, wann einzelne Firewall-Regeln angewendet wurden. Dazu muss zu den verschiedenen Firewall-Funktionen die LOG-Funktion aktiviert werden.
  - DDNS Client Logs
    Das Ereignis tritt auf, wenn der DDNS-Client die zugewiesene IP-Adresse mit dem im DDNS-Provider registrierten Hostnamen synchronisiert.
  - System Allgemein Logs
    Verbindungsaufbau, Änderung der Konfiguration.
  - System-Verbindungsstatus
    Der Verbindungsstatus hat sich geändert.
  - Digitaler Eingang
    Das Ereignis tritt auf, wenn sich der Zustand des digitalen Eingangs geändert hat.
  - VPN-Tunnel
    Das Ereignis tritt auf, wenn sich der Zustand von VPN (IPsec,OpenVPN, SINEMA RC) geändert hat.

  - NTP (secure)
    Dieses Ereignis tritt ein, wenn das Gerät die Systemzeit von einem gesicherten NTP-Server erhält.
  - Änderung in der Konfiguration
    Dieses Ereignis tritt ein, wenn sich die Konfiguration des Geräts geändert hat.
  - Service-Informationen
    Für bestimmte Ereignisse werden auch ohne Konfiguration Einträge in der Log-Tabelle erstellt. Für diese Ereignisse können Sie hier weitere Folgeaktionen konfigurieren (E-Mail, Trap, Syslog).
  - Mobile Datennutzung (nur beim M87x/MUM85x)
    Dieses Ereignis tritt auf, wenn 75% oder 100% des festgelegten Datenvolumens erreicht sind, siehe "Schnittstellen > Mobilfunk > Allgemein".
  - Cloud Connector
    Das Ereignis tritt auf, wenn sich der Betriebszustand des integrierten Cloud Connectors geändert hat.
  - Connection Check
    Das Ereignis tritt auf, wenn Verbindungen überwacht werden, siehe "System > Connection Check".
  - Modem Verbindungsqualität-Log
    Einträge zu Signalstärke, Signalqualität und die GPS-Position des Standorts. Das Modem Verbindungsqualität-Log wird alle 10 Minuten geschrieben.
  - DHCP-Server Log
    DHCP-Ereignisse werden protokoliert. Vorausgesetzt, auf dem Gerät ist der DHCP-Server aktiviert.
  - TCP-Ereignis Log
    Das Gerät hat ein TCP-Paket erhalten. Vorausgesetzt, die Funktion "TCP-Ereignis" ist aktiviert.
  - Geofencing (Nur beim MUM85x)
    Das festgelegte Ereignis tritt auf, wenn das Gerät je nach der konfigurierten Bedingung den definierten Bereich betritt, in dem Bereich bleibt oder ihn verlässt, siehe "System > Geofencing".

- **E-Mail**
  Das Gerät sendet eine E-Mail. Voraussetzung ist, dass der SMTP-Server eingerichtet und die Funktion "SMTP-Client" aktiviert ist.
- **Trap**
  Das Gerät löst einen SNMP-Trap aus. Voraussetzung ist, dass unter "System > Konfiguration" "SNMPv1 Traps" aktiviert ist.
- **Log-Tabelle**
  Das Gerät schreibt einen Eintrag in die Ereignisprotokoll-Tabelle, siehe "Information > Log-Tabelle".
- **Syslog**
  Das Gerät schreibt einen Eintrag auf den Systemprotokoll-Server. Voraussetzung ist, dass der Systemprotokoll-Server eingerichtet und die Funktion "Syslog-Client" aktiviert ist.

- **Fehler**
  Das Gerät löst einen Fehler aus. Die Fehler-LED leuchtet auf und der aktuell anstehende Fehler wird unter "Information > Fehler" angezeigt.
- **SMS** (nur beim M87x / MUM85x)
  Das Gerät sendet eine SMS. Voraussetzung ist, dass "System > SMS > Ereignis SMS" aktiviert und die Telefonnummer des Empfängers konfiguriert ist.
- **Digitaler Ausgang**
  Steuert den digitalen Ausgang an oder signalisiert die Zustandsänderung mit der LED "DO". Standardmäßig und nach jedem Neustart ist der digitale Ausgang offen. Der digitale Ausgang wird geschlossen, wenn Sie mindestens ein Ereignis für den digitalen Ausgang aktivieren. Außerdem ist er nicht automatisch mit der Fehler-LED verbunden. Sie verbinden den digitalen Ausgang mit der Fehler-LED unter "Änderung des Fehlerstatus".
- **VPN-Tunnel**
  Steuert die Weitergabe eines Ereignisses an eine VPN-Verbindung (IPsec, OpenVPN, SINEMA RC). Solange das Ereignis anliegt, wird die VPN-Verbindung aktiv geschaltet.
- **Firewall**
  Steuert das Anwenden des benutzerdefinierten Regelsatzes. Voraussetzung ist, dass bei "Security > Firewall > Dynamische Regeln" dem digitalen Eingang ein Regelsatz zugewiesen ist.
- **Cloud Connector**
  Steuert die Weitergabe eines Ereignisses an die TIA Portal Cloud Connector-Kommunikation. Solange das Ereignis anliegt, ist die Kommunikationsverbindung aktiv.

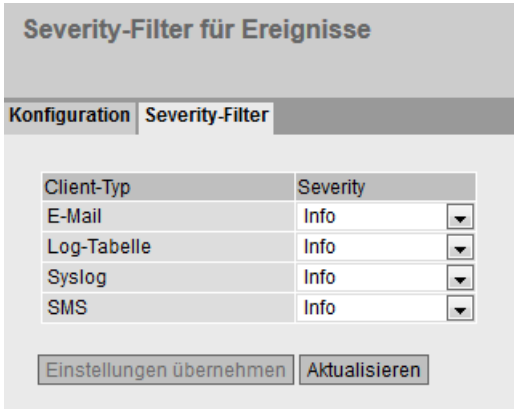
## Vorgehensweise

**VPN-Tunnel über den Digitalen Eingang auf-/abbauen**

1. Aktivieren Sie beim Ereignis "Digitaler Eingang" den Eintrag "VPN-Tunnel".
2. Konfigurieren Sie die VPN-Verbindung
   - IPsec:
     Stellen Sie bei "Betrieb" "Auf DI warten" oder "Bei DI starten" ein. Weitere Informationen hierzu finden Sie unter "IPsec > Verbindungen (Seite 423)" und unter "VPN-Verbindungsaufbau (Seite 91)".
   - OpenVPN:
     Stellen Sie bei "Betrieb" "Bei DI starten" ein. Weiterführende Informationen hierzu finden Sie unter "OpenVPN > Verbindungen (Seite 435)" und unter "VPN-Verbindungsaufbau (Seite 91)".
   - SINEMA RC:
     Stellen Sie bei "Verbindungsart" "Auto", "Digitaler Eingang" oder "Digitaler Eingang & Weck-SMS" (nur bei M87x/MUM85x) ein. Bei der Verbindungsart "Auto", müssen Sie auf dem SINEMA RC Server unter "Fernverbindungen > Geräte" die Verbindungsart "Digitaler Eingang" oder "Weck-SMS & Digitaler Eingang" (nur bei M87x/MUM85x) einstellen. Weiterführende Informationen hierzu finden Sie in der Betriebsanleitung "SINEMA RC Server".
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

### 5.5.5.2 Severity-Filter

Auf dieser Seite konfigurieren Sie den Schweregrad für das Versenden von Systemereignisbenachrichtigungen.




## Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Client-Typ**
  Wählen Sie den Client-Typ, für den Sie die Einstellungen vornehmen:
  - **E-Mail**
    Versand von Systemereignismeldungen per E-Mail.
  - **Log-Tabelle**
    Eintragen von Systemereignissen in die Log-Tabelle.
  - **Syslog**
    Eintragen von Systemereignissen in die Syslog-Datei.
  - **SMS** (nur bei M87x/MUM85x)
    Versand von Systemereignismeldungen per SMS.
- **Severity**
  Wählen Sie den gewünschten Schweregrad aus. Folgende Einstellungen sind möglich:
  - **Critical**
    Systemereignisse mit dem Schweregrad Critical (Kritisch) werden bearbeitet.
  - **Warning**
    Systemereignisse ab dem Schweregrad Warning (Warnungen) werden bearbeitet: es sind Ereignisse der Kategorien "Warning" und "Critical".
  - **Info**
    Systemereignisse ab dem Schweregrad Info (Information) werden bearbeitet: es sind Ereignisse der Kategorien "Info", "Warning" und "Critical".

### Vorgehensweise

Gehen Sie folgendermaßen vor, um die gewünschte Stufe zu konfigurieren:

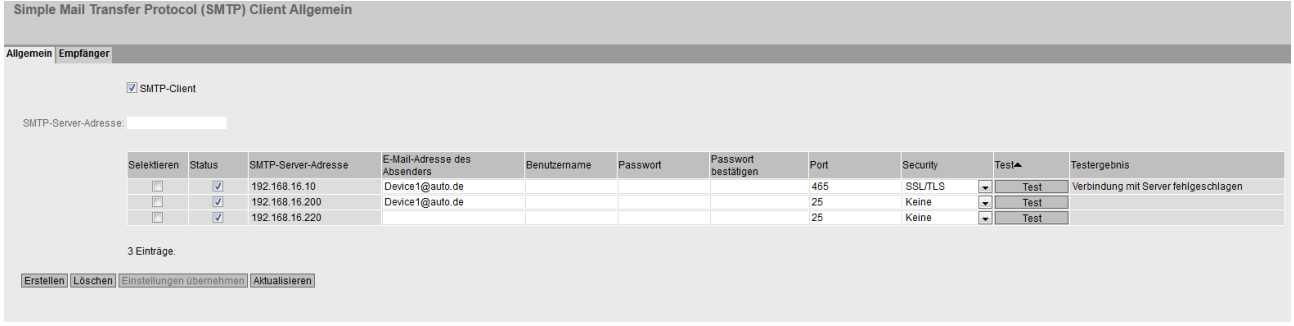
1. Wählen Sie aus den Klapplisten in der zweiten Tabellenspalte hinter den Client-Typen die gewünschten Werte aus.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

## 5.5.6 SMTP-Client

### 5.5.6.1 Allgemein

### Netzüberwachung durch E-Mails

Beim Auftreten von Ereignissen kann das Gerät automatisch eine E-Mail versenden, z. B. an den Servicetechniker. Die E-Mail enthält die Identifikation des absendenden Geräts, eine Beschreibung der Ursache in Klartext sowie einen Zeitstempel. Damit kann für Netze mit wenigen Teilnehmern eine einfache zentrale Netzüberwachung auf Basis eines E-Mail-Systems aufgebaut werden.




### Voraussetzung für das Senden der E-Mails

- Unter "System > Ereignisse > Konfiguration" ist beim entsprechenden Ereignis "E-Mail" aktiviert.
- Unter "System > Ereignisse > Severity-Level" ist die gewünschte Severity konfiguriert.
- Unter "System > SMTP-Client > Empfänger" ist mindestens ein Eintrag vorhanden und die Einstellung "Senden" ist aktiviert.

## Beschreibung

Die Seite enthält folgende Felder:

- **SMTP-Client**
  Aktivieren oder deaktivieren Sie den SMTP-Client.
- **SMTP-Server-Adresse**
  Geben Sie die IP-Adresse oder den FQDN (Fully Qualified Domain Name) des SMTP-Servers ein.

Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in einer zu löschenden Zeile das Optionskästchen.
- **Status**
  Legen Sie fest, ob dieser SMTP-Server verwendet wird.
- **SMTP-Server-Adresse**
  Zeigt die IP-Adresse oder den FQDN (Fully Qualified Domain Name) des SMTP-Servers.
- **E-Mail-Adresse des Absenders**
  Geben Sie die E-Mail-Adresse des Absenders ein, der in der E-Mail angegeben wird.
- **Benutzername**
  Wenn erforderlich, geben Sie den Benutzernamen ein, der zur Authentifizierung am SMTP-Server verwendet wird.
- **Passwort**
  Wenn erforderlich, geben Sie das Passwort ein, das zur Authentifizierung am SMTP-Server verwendet wird.
- **Passwort bestätigen**
  Wiederholen Sie das Passwort.
- **Port**
  Geben Sie den Port ein, über den der SMTP-Server erreichbar ist.
  Werkseinstellung:
  - 25 (None)
  - 465 (SSL/TLS und StartTLS)
- **Security**
  Legen Sie fest, ob die Übertragung der E-Mail vom Gerät zum SMTP-Server verschlüsselt wird. D. h. Voraussetzung ist, dass der SMTP-Server die ausgewählte Einstellung unterstützt.

  **Hinweis**

  **2-Faktor-Authentifizierung (2FA)**

  Die 2-Faktor-Authentifizierung wird nicht unterstützt.

  - SSL/TLS
  - StartTLS
  - None: Die Übertragung der E-Mail ist unverschlüsselt.

- **Test**
  Verschickt an die konfigurierten Empfänger eine Test-E-Mail.
- **Testergebnis**
  Zeigt an, ob die E-Mail erfolgreich gesendet wurde oder nicht. Wenn das Senden nicht erfolgreich war, enthält die Meldung mögliche Ursachen.

## Vorgehensweise

**SMTP-Server konfigurieren**

1. Aktivieren Sie die Funktion "SMTP-Client".
2. Geben Sie in bei "SMTP-Server-Adresse" die IP-Adresse oder den FQDN des SMTP-Servers ein.
3. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag erzeugt.
4. Geben Sie bei "E-Mail-Adresse des Absenders" den Absendernamen ein, der in der E-Mail angegeben wird.
5. Wenn der SMTP-Server eine Anmeldung erfordert, geben Sie Benutzernamen und Passwort ein.
6. Legen Sie bei "Security" fest, ob die Übertragung zum SMTP-Server verschlüsselt wird.
7. Aktivieren Sie den SMTP-Servereintrag.
8. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

**Hinweis**

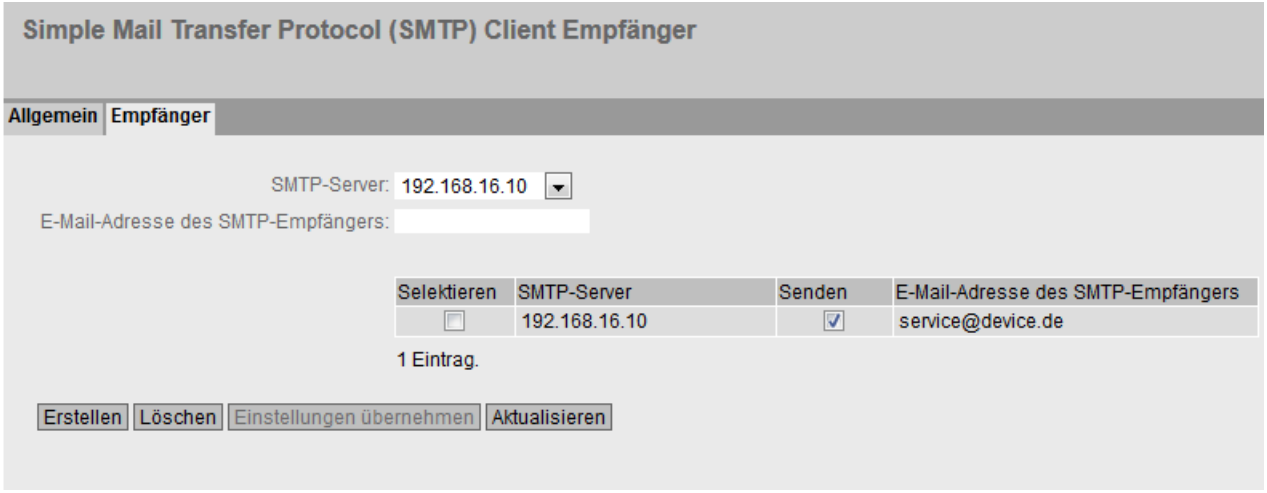
Je nach Eigenschaften und Konfiguration des SMTP-Servers kann es notwendig sein, die Eingabe von "E-Mail-Adresse des Absenders" anzupassen. Informieren Sie sich beim Administrator des SMTP-Servers.

**Konfiguration des SMTP-Servers testen**

1. Empfänger konfigurieren
   - Klicken Sie auf das Register "Empfänger".
   - Wählen Sie bei "SMTP-Server" den gewünschten SMTP-Server aus.
   - Geben Sie bei "E-Mail-Adresse des SMTP-Empfängers" die gewünschte Adresse an.
   - Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag erzeugt. Standardmäßig ist die Einstellung "Senden" aktiviert.
2. Test-E-Mail versenden
   - Klicken Sie auf das Register "Allgemein".
   - Klicken Sie bei dem SMTP-Servereintrag auf die Schaltfläche "Test". Das Gerät sendet jedem konfigurierten Empfänger eine Test-E-Mail.
   - Prüfen Sie das Testergebnis. Wenn das Senden nicht erfolgreich war, enthält die Meldung mögliche Ursachen.

### 5.5.6.2 Empfänger

Auf dieser Seite legen Sie fest, wer beim Auftreten eines Ereignisses eine E-Mail bekommt.




## Beschreibung

Die Seite enthält folgende Felder:

- **SMTP-Server**
  Legen Sie fest, über welchen SMTP-Server die E-Mail versendet wird.
- **E-Mail-Adresse des SMTP-Empfängers**
  Geben Sie die E-Mail-Adresse ein, an die das Gerät eine E-Mail sendet.

Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in einer zu löschenden Zeile das Optionskästchen.
- **SMTP-Server**
  Zeigt die IP-Adresse oder den FQDN (Fully Qualified Domain Name) SMTP-Servers an, auf den sich der Eintrag bezieht.
- **Senden**
  Wenn aktiviert, sendet das Gerät an diesen Empfänger eine E-Mail.
- **E-Mail-Adresse des SMTP-Empfängers**
  Zeigt die E-Mail-Adresse an, an die das Gerät im Fehlerfall eine E-Mail sendet.

## Vorgehensweise

**SMTP-Empfänger konfigurieren**

1. Wählen Sie den gewünschten "SMTP-Server".
2. Geben Sie die E-Mail-Adresse des SMTP-Empfängers ein.
3. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag erzeugt.

4. Aktivieren Sie für den Eintrag die Option "Senden".
5. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

## 5.5.7 SNMP

### 5.5.7.1 Allgemein

#### Konfiguration von SNMP

**Hinweis**

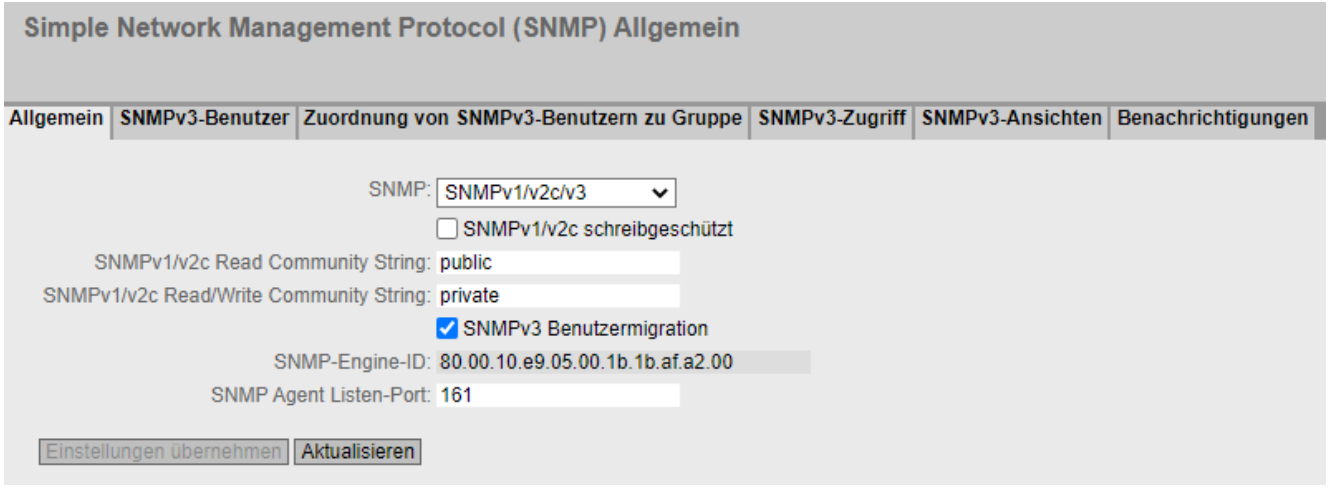
**SNMPv3-Konfiguration bei einem Firmware-Update**

Ab Firmware-Version 6.4 wurde die SNMP-Konfiguration auf mehrere WBM-Seiten verteilt.

Um die SNMPv3-Konfiguration zu löschen, müssen Sie wie folgt vorgehen:

1. Löschen Sie alle SNMPv3-Ansichten mit Ausnahme der vordefinierten Ansichten **SIMATICNETRD** und **SIMATICNETWR**.
2. Löschen Sie alle SNMPv3-Zugriffe.
3. Löschen Sie alle Einträge in der Tabelle "Zuordnung von SNMPv3-Benutzern zu Gruppe".
4. Löschen Sie alle SNMPv3-Benutzer.

Auf dieser Seite treffen Sie grundlegende Einstellungen für SNMP. Aktivieren Sie die Optionen abhängig von der Funktion, die Sie nutzen wollen.



## Beschreibung

Die Seite enthält folgende Felder:

- **SNMP**
  Wählen Sie aus der Klappliste das SNMP-Protokoll. Folgende Einstellungen sind möglich:
  - "-" (Deaktiviert)
    SNMP ist deaktiviert.
  - SNMPv1/v2c/v3
    SNMPv1/v2c/v3 wird unterstützt.

    **Hinweis**

    Beachten Sie, dass SNMP in den Versionen 1 und 2c über keine Sicherheitsmechanismen verfügt.
  - SNMPv3
    Nur SNMPv3 wird unterstützt.
- **SNMPv1/v2c schreibgeschützt**
  Wenn Sie diese Option aktivieren, kann SNMPv1/v2c nur lesend auf die SNMP-Variablen zugreifen.

  **Hinweis**

  **Community String**

  Verwenden Sie aus Sicherheitsgründen nicht die Standardwerte "public" oder "private". Ändern Sie die Community Strings nach der Erst-Installation.

  Die empfohlene Mindestlänge für Community Strings sind 6 Zeichen.

  Aus Sicherheitsgründen ist mit dem SNMPv1/v2c Read Community String nur eingeschränkter Zugriff auf Objekte der SNMPCommunityMIB möglich. Mit dem SNMPv1/v2c Read/Write Community String haben Sie vollen Zugriff auf die SNMPCommunityMIB.
- **SNMPv1/v2c Read Community String**
  Tragen Sie den Community String für den lesenden Zugriff des SNMP-Protokolls ein.
- **SNMPv1/v2c Read/Write Community String**
  Tragen Sie den Community String für den lesenden und schreibenden Zugriff des SNMP-Protokolls ein.
- **SNMPv3 Benutzermigration**
  - **Aktiviert**
    Wenn die Funktion aktiviert ist, wird eine SNMP-Engine-ID generiert, die migriert werden kann. Sie können konfigurierte SNMPv3-Benutzer auf ein anderes Gerät übertragen. Wenn Sie diese Funktion aktivieren und die Konfiguration des Geräts auf ein anderes Gerät laden, bleiben konfigurierte SNMPv3-Benutzer erhalten.
  - **Deaktiviert**
    Wenn die Funktion deaktiviert ist, wird eine gerätespezifische SNMP-Engine-ID generiert. Um die ID zu generieren, wird die Agent-MAC-Adresse des Geräts verwendet. Sie können diese SNMP-Benutzerkonfiguration nicht auf andere Geräte übertragen.
    Wenn Sie die Konfiguration des Geräts auf ein anderes Gerät laden, werden alle konfigurierten SNMPv3-Benutzer gelöscht.

- **SNMP-Engine-ID**
  Zeigt die SNMP-Engine-ID an.
- **SNMP Agent Listen Port**
  Legen Sie fest, an welchem Port der SNMP-Agent auf die SNMP-Anfragen wartet. Voreingestellt ist der Standard-Port 161. Optional können Sie den Standard-Port 162 oder eine Portnummer im Bereich 1024 ... 49151 oder 49500 ... 65535 eintragen.

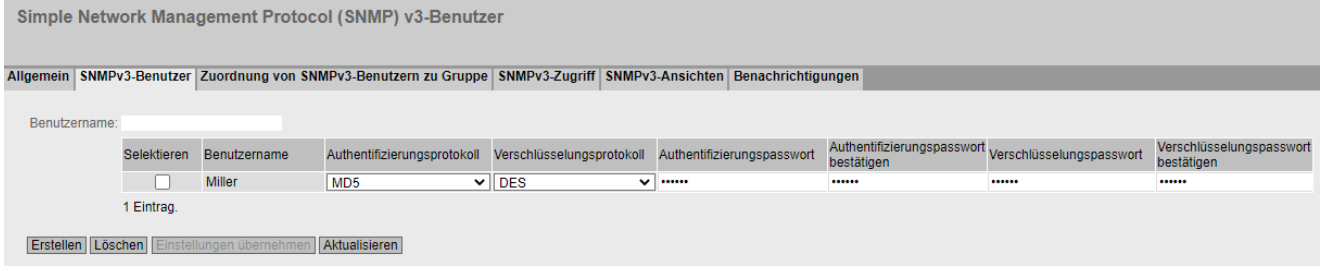
### Vorgehensweise

1. Wählen Sie aus der Klappliste "SNMP" die gewünschte Option:
   – "-" (Deaktiviert)
   – SNMPv1/v2c/v3
   – SNMPv3
2. Aktivieren Sie das Optionskästchen "SNMPv1/v2c schreibgeschützt", wenn Sie mit SNMPv1/v2c nur lesend auf SNMP-Variablen zugreifen wollen.
3. Tragen Sie im Eingabefeld "SNMPv1/v2c Read Community String" die gewünschte Zeichenkette ein.
4. Tragen Sie im Eingabefeld "SNMPv1/v2c Read/Write Community String" die gewünschte Zeichenkette ein.
5. Aktivieren Sie ggf. die SNMPv3 Benutzermigration.
6. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

## 5.5.7.2 SNMPv3-Benutzer

### Benutzerspezifische Sicherheitseinstellungen

Auf der WBM-Seite können Sie SNMPv3-Benutzer neu anlegen, ändern oder löschen. Das benutzerbasierte Sicherheitsmodell arbeitet mit dem Konzept des Benutzernamens, d. h. jedes Telegramm wird mit einer Benutzerkennung versehen. Diesen Benutzernamen und die betreffenden Sicherheitseinstellungen überprüfen sowohl der Absender wie auch der Empfänger.



## Beschreibung

Die Seite enthält folgende Felder:

- **Benutzername**
  Tragen Sie einen frei wählbaren Benutzernamen ein. Nach der Datenübernahme können Sie den Namen nicht mehr ändern.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Benutzername**
  Zeigt die angelegten Benutzer an.
- **Authentifizierungsprotokoll**
  Legen Sie das Authentifizierungsprotokoll fest, für das ein Passwort hinterlegt werden soll. Folgende Einstellungen gibt es:
  - Keine
  - MD5
  - SHA
- **Verschlüsselungsprotokoll**
  Legen Sie das Verschlüsselungsprotokoll fest, für das ein Passwort hinterlegt werden soll. Diese Klappliste ist nur dann aktiviert, wenn ein Authentifizierungsprotokoll ausgewählt wurde.
  Folgende Einstellungen gibt es:
  - Keine
  - DES
  - AES
- **Authentifizierungspasswort**
  Geben Sie in das erste Eingabefeld das Authentifizierungspasswort ein. Das Passwort muss mindestens 1 Zeichen lang sein, die maximale Länge beträgt 32 Zeichen.

  **Hinweis**

  **Länge des Passworts**

  Als wichtige Maßnahme zur Erhöhung der Sicherheit empfehlen wir, dass das Passwort mindestens 6 Zeichen lang ist und Sonderzeichen, Groß-/Kleinschreibung sowie Zahlen enthält.
- **Authentifizierungspasswort bestätigen**
  Bestätigen Sie das Passwort durch die Wiederholung der Eingabe.

- **Verschlüsselungspasswort**
  Geben Sie Ihr Verschlüsselungspasswort ein. Das Passwort muss mindestens 1 Zeichen lang sein, die maximale Länge beträgt 32 Zeichen.

  **Hinweis**

  **Länge des Passworts**

  Als wichtige Maßnahme zur Erhöhung der Sicherheit empfehlen wir, dass das Passwort mindestens 6 Zeichen lang ist und Sonderzeichen, Groß-/Kleinschreibung sowie Zahlen enthält.

- **Verschlüsselungspasswort bestätigen**
  Bestätigen Sie das Verschlüsselungspasswort durch die Wiederholung der Eingabe.

## Vorgehensweise

**Neuen Benutzer anlegen**

1. Geben Sie im Eingabefeld "Benutzername" den Namen des neuen Benutzers ein.
2. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag erzeugt.
3. Wählen Sie bei "Authentifizierungsprotokoll" den Authentifizierungsalgorithmus. Tragen Sie in die entsprechenden Eingabefelder das Authentifizierungspasswort sowie dessen Bestätigung ein.
4. Wählen Sie bei "Verschlüsselungsprotokoll" den Algorithmus aus. Tragen Sie in die entsprechenden Eingabefelder das Verschlüsselungspasswort sowie dessen Bestätigung ein.
5. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

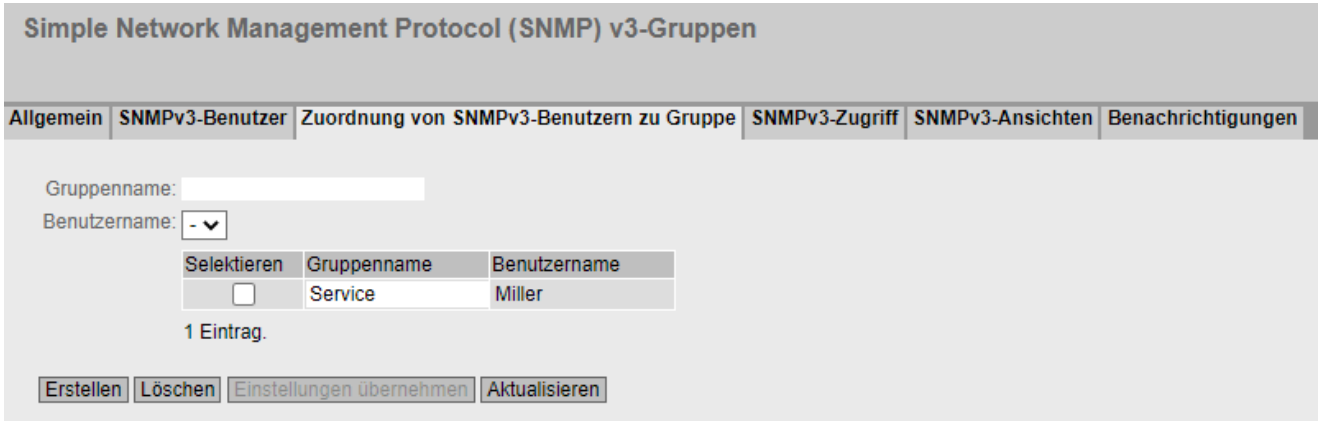
**Benutzer löschen**

1. Aktivieren Sie in der zu löschenden Zeile "Selektieren".
   Wiederholen Sie den Vorgang für alle Benutzer, die Sie löschen wollen.
2. Klicken Sie auf die Schaltfläche "Löschen". Der Eintrag wird gelöscht.

### 5.5.7.3 Zuordnung von SNMPv3-Benutzern zu Gruppen

#### Konfiguration von Gruppenmitgliedern

Auf dieser WBM-Seite ordnen Sie Benutzer SNMPv3-Gruppen zu. Jeder Benutzer kann nur in einer Gruppe Mitglied sein.




#### Beschreibung

Die Seite enthält folgende Felder:

- **Gruppenname**
  Tragen Sie die Gruppe ein, die dem Benutzer zugeordnet wird.
- **Benutzername**
  Wählen Sie den Benutzer aus, der Mitglied der angegebenen Gruppe werden soll. Die Klappliste enthält nur solche Benutzer, die noch keiner Gruppe zugeordnet sind.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Gruppenname**
  Zeigt die SNMPv3-Gruppe an. Ein Gruppenname kann nachträglich nur geändert werden, wenn für die Gruppe noch keine Zugriffsrechte definiert wurden.
- **Benutzername**
  Zeigt den Benutzer an, der in dieser Gruppe Mitglied ist.

### 5.5.7.4 SNMPv3-Zugriff

## Security-Einstellungen und Rechtevergabe

SNMP Version 3 bietet eine Rechtevergabe, Authentifizierung und Verschlüsselung auf Protokollebene. Das Security-Level und die Lese-/Schreibrechte werden gruppenspezifisch definiert. Für jedes Mitglied einer Gruppe gelten automatisch die entsprechenden Einstellungen.

**Hinweis**

Einer Gruppe können unterschiedliche Zugriffsberechtigungen für verschiedene Sicherheitsstufen zugeordnet werden. Ist für eine Sicherheitsstufe keine Zugriffsberechtigung definiert, so ist Mitgliedern der Gruppe unter Verwendung dieser Sicherheitsstufe kein Zugriff auf das Gerät möglich.




## Beschreibung

Die Seite enthält folgende Felder:

- **Gruppenname**
  Wählen Sie den Namen der Gruppe.
- **Security-Level**
  Wählen Sie die Sicherheitsstufe (Authentifizierung, Verschlüsselung) aus, für die sie die Zugriffsberechtigungen der Gruppe definieren wollen:
  - **Keine Auth/keine Priv**
    Keine Authentifizierung aktiviert / keine Verschlüsselung aktiviert.
  - **Auth/keine Priv**
    Authentifizierung aktiviert / keine Verschlüsselung aktiviert.
  - **Auth/Priv**
    Authentifizierung aktiviert / Verschlüsselung aktiviert.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Gruppenname**
  Zeigt den Namen der SNMPv3-Gruppe an.
- **Security-Level**
  Zeigt die Sicherheitsstufe an, für die diese Zugriffsberechtigung gilt.
- **Lesen Ansichtname**
  Geben Sie eine SNMPv3-Ansicht ein, die Mitgliedern der Gruppe mit dem festgelegten Security-Level Lesezugriff gewährt.
- **Schreiben Ansichtname**
  Geben Sie eine SNMPv3-Ansicht ein, die Mitgliedern der Gruppe mit dem festgelegten Security-Level Schreibzugriff gewährt.

  **Hinweis**

  Damit der Schreibzugriff funktioniert, müssen Sie ebenfalls den Lesezugriff aktivieren.

- **Benachrichtigung Ansichtname**
  Tragen Sie eine SNMPv3-Ansicht ein, die für SNMP-Benachrichtigung an Mitglieder der Gruppe mit der definierten Sicherheitsstufe verwendet werden soll.

## Vorgehensweise

**Anlegen einer neuen Gruppe**

1. Wählen Sie den Namen der Gruppe, für die Sie den SNMP-Zugriff konfigurieren.
2. Wählen Sie aus der Klappliste "Security-Level" die gewünschte Sicherheitsstufe aus.
3. Um einen neuen Eintrag zu erzeugen, klicken Sie auf die Schaltfläche "Erstellen" .
4. Tragen Sie im Feld "Lesen Ansichtname" die SNMPv3-Ansicht für lesenden Zugriff ein.
5. Tragen Sie im Feld "Schreiben Ansichtname" die SNMPv3-Ansicht für schreibenden Zugriff ein.
6. Tragen Sie im Feld "Benachrichtigung Ansichtname" die SNMPv3-Ansicht für Benachrichtigungen ein.
7. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

**Ändern einer Gruppe**

Der einmal vergebene Gruppenname und die Sicherheitsstufe können Sie nach dem Anlegen nicht mehr ändern. Wenn Sie den Gruppennamen oder die Sicherheitsstufe ändern wollen, müssen Sie die Gruppe löschen und mit dem neuen Namen anlegen und konfigurieren.

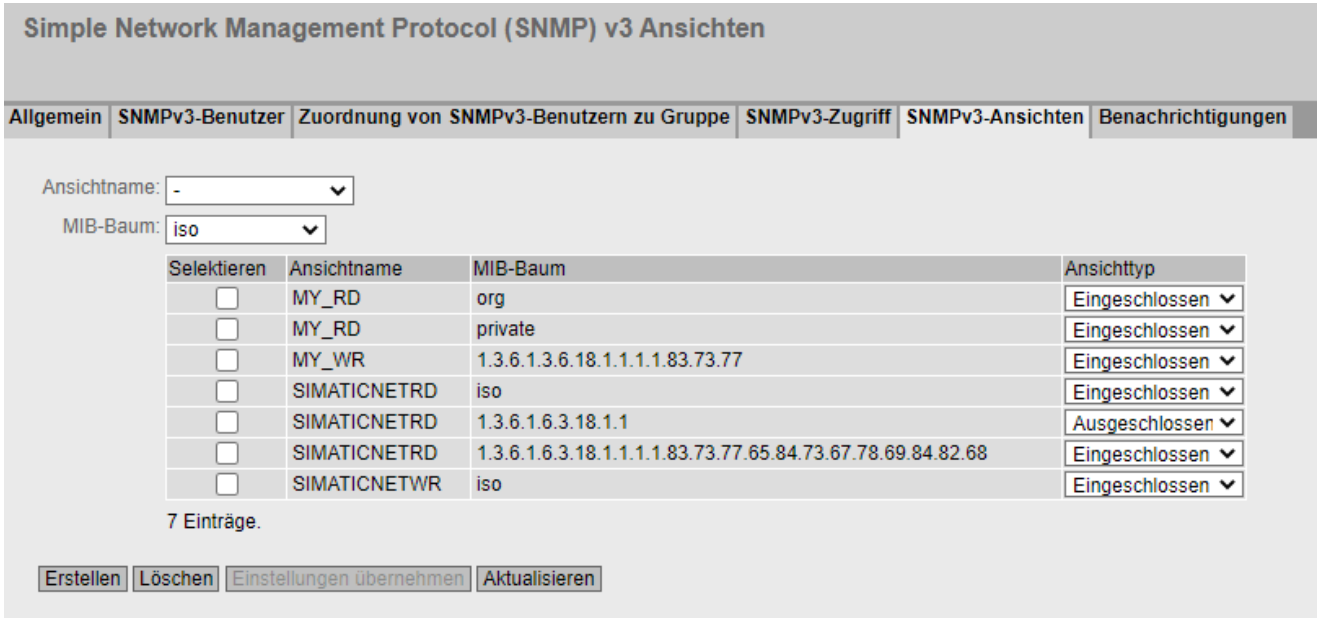
**Löschen einer Gruppe**

1. Aktivieren Sie in der zu löschenden Zeile "Selektieren".
   Wiederholen Sie den Vorgang für alle Gruppen, die Sie löschen wollen.
2. Klicken Sie auf die Schaltfläche "Löschen". Die Einträge werden gelöscht.

### 5.5.7.5 SNMPv3-Ansichten

#### Konfiguration von SNMPv3-Ansichten

Auf dieser WBM-Seite konfigurieren Sie die Parameter von SNMP-Ansichten.




**Hinweis**

**Steuerung der SNMPv1- und SNMPv2c-Zugriffe**

Die vorkonfigurierten Ansichten **SIMATICNETRD** und **SIMATICNETWR** werden intern zur Steuerung des SNMPv1- und SNMPv2c-Zugriffs verwendet. Wenn sie diese Ansichten löschen oder verändern, hat das unmittelbare Auswirkungen auf die SNMPv1- und SNMPv2c-Zugriffe.

## Beschreibung

Die Seite enthält folgende Felder:

- **Ansichtname**
  Wählen Sie den Namen der Ansicht aus, die Sie konfigurieren wollen. Eine SNMPv3-Ansicht muss immer einem SNMPv3-Zugriff zugeordnet sein. Deshalb müssen Sie eine neue SNMPv3-Ansicht in der Tabelle im Register "SNMPv3-Zugriff" eintragen.
- **MIB-Baum**
  Wählen Sie den Object Identifier (OID) des MIB-Bereichs aus, der für die SNMPv3-Ansicht verwendet werden soll. Es gibt folgende Möglichkeiten:
  - **iso**
  - **std**
  - **member-body**
  - **org**
  - **mgmt**
  - **private**
  - **snmpV2**

  In der Klappliste sind nur die OIDs enthalten, die in den meisten Fällen genutzt werden. Wenn die Konfiguration einer spezifischen, nicht aufgeführten OID notwendig ist, können Sie diese über das CLI mit dem Befehl `snmp view` konfigurieren. Diese OID wird anschließend auch im WBM in der Übersichtstabelle angezeigt.

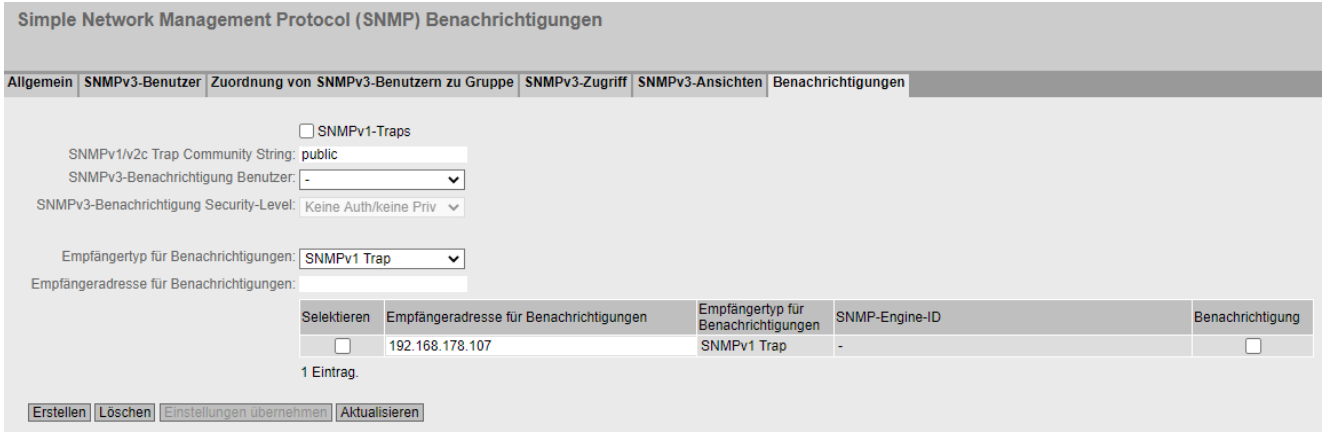
Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Ansichtname**
  Der Name der SNMPv3-Ansicht.
- **MIB-Baum**
  Der OID des MIB-Bereichs für die SNMPv3-Ansicht.
- **Ansichttyp**
  Es gibt folgende Möglichkeiten:
  - **Eingeschlossen**
    Der MIB-OID und dessen untergeordnete Knoten sind Teil der SNMPv3-Ansicht. Ein Zugriff auf die entsprechenden MIB-Objekte ist möglich.
  - **Ausgeschlossen**
    Der MIB-OID und dessen untergeordnete Knoten sind nicht Teil der SNMPv3-Ansicht. Ein Zugriff auf die entsprechenden MIB-Objekte ist nicht möglich.

### 5.5.7.6 Benachrichtigungen

## SNMP-Traps und SNMPv3-Benachrichtigungen

Beim Eintreten eines Alarmereignisses kann ein Gerät SNMP-Benachrichtigungen (Traps und Inform-Benachrichtigungen) an bis zu zehn verschiedene Management-Stationen gleichzeitig senden. Es werden nur bei solchen Ereignissen Benachrichtigungen gesendet, die im Menüpunkt "Ereignisse" festgelegt wurden.




## Beschreibung

Die Seite enthält folgende Felder:

- **SNMPv1-Traps**
  Aktivieren oder deaktivieren Sie das Senden von SNMPv1-Traps. Diese Einstellung betrifft alle Empfänger von SNMPv1-Traps und hat keine Auswirkungen auf Empfänger von SNMPv2c- oder SNMPv3-Benachrichtigungen.
- **SNMPv1/v2c Trap Community String**
  Tragen Sie den Community String für das Senden von SNMPv1/v2c-Benachrichtigungen ein.
- **SNMPv3-Benachrichtigung Benutzer**
  Wählen Sie aus, an welchen Benutzer SNMPv3-Benachrichtigungen gesendet werden sollen.
- **SNMPv3-Benachrichtigung Security-Level**
  Wählen Sie die Sicherheitsstufe (Authentifizierung, Verschlüsselung) aus, die für SNMPv3-Benachrichtigung verwendet werden sollen. Es gibt folgende Möglichkeiten:
  - Keine Auth/keine Priv
    Keine Authentifizierung aktiviert / keine Verschlüsselung aktiviert.
  - Auth/keine Priv
    Authentifizierung aktiviert / keine Verschlüsselung aktiviert.
  - Auth/Priv
    Authentifizierung aktiviert / Verschlüsselung aktiviert.

- **Empfängertyp für Benachrichtigungen**
  Der Empfängertyp legt die SNMP-Version und die Art der Benachrichtigung fest. SNMP-Inform-Benachrichtigungen müssen vom Empfänger quittiert werden, SNMP-Traps nicht. Es gibt folgende Möglichkeiten:
  - SNMPv1 Trap
  - SNMPv2c Trap
  - SNMPv2c Inform
  - SNMPv3 Trap
  - SNMPv3 Inform
- **Empfängeradresse für Benachrichtigungen**
  Geben Sie die IP-Adresse, den FQDN (Fully Qualified Domain Name) oder den Hostnamen der Empfängerstation ein, an die das Gerät SNMP-Benachrichtigungen sendet. Sie können bis zu zehn verschiedene Empfänger angeben.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Empfängeradresse für Benachrichtigungen**
  Ändern Sie bei Bedarf die IP-Adresse, den FQDN (Fully Qualified Domain Name) oder den Hostnamen der Stationen.
- **Empfängertyp für Benachrichtigungen**
  Zeigt den festgelegten Empfängertyp an.
- **SNMP-Engine-ID**
  Die ID der SNMP-Engine, an die SNMPv3-Inform-Benachrichtigungen versendet werden. Sie können diesen Parameter nur für den Empfängertyp "SNMPv3-Inform" konfigurieren.
- **Benachrichtigung**
  Aktivieren oder deaktivieren Sie das Senden von SNMP-Benachrichtigungen. Stationen, die eingetragen, aber nicht selektiert sind, erhalten keine SNMP-Benachrichtigungen.

**Hinweis**

Wenn eine Tabellenzeile gegraut ist, wurde die entsprechende Benachrichtigung über das CLI konfiguriert und kann auch nur über das CLI gelöscht werden.

## Vorgehensweise

**Benachrichtigung konfigurieren**

1. Wählen Sie in der Klappliste "SNMPv3-Benachrichtigung Benutzer" den Empfänger für SNMPv3-Benachrichtigungen.
2. Wählen Sie in der Klappliste "SNMPv3-Benachrichtigung Security-Level" die Sicherheitsstufe für die SNMPv3-Benachrichtigungen.
3. Wählen Sie in der Klappliste "Empfängertyp für Benachrichtigungen" den Empfängertyp.
4. Geben Sie bei "Empfängeradresse für Benachrichtigungen" die IP-Adresse, den FQDN oder den Hostnamen der Station ein, an die das Gerät Traps bzw. Benachrichtigungen senden soll.

5. Klicken Sie auf die Schaltfläche "Erstellen", um einen neuen Trap-Eintrag zu erstellen.
6. Aktivieren Sie in der gewünschten Zeile "Benachrichtigung".
7. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

**Trap-Eintrag löschen**

1. Aktivieren Sie in der zu löschenden Zeile "Selektieren".
2. Klicken Sie auf die Schaltfläche "Löschen". Der Eintrag wird gelöscht.

## 5.5.8 Systemzeit

Um die Systemzeit des Geräts einzustellen, gibt es unterschiedliche Methoden. Es kann immer nur eine Methode aktiv sein.

Wenn eine Methode aktiviert wird, dann wird automatisch die bisher aktivierte Methode deaktiviert.

### 5.5.8.1 Manuelle Einstellung

#### Manuelle Einstellung der Systemzeit

Auf dieser Seite stellen Sie selbst das Datum und die Uhrzeit des Systems ein. Damit diese Einstellung verwendet wird, aktivieren Sie "Manuelle Zeiteinstellung".



## Beschreibung

Die Seite enthält folgende Felder:

- **Manuelle Zeiteinstellung**
  Aktivieren oder deaktivieren Sie die manuelle Zeiteinstellung. Wenn Sie die Option aktivieren, wird das Eingabefeld "Systemzeit" editierbar.
- **Systemzeit**
  Geben Sie Datum und Uhrzeit im Format "MM/DD/YYYY HH:MM:SS" ein.
  Nach dem Neustart beginnt die Uhrzeit mit 01/01/2000 00:00:00
- **PC-Zeit verwenden**
  Klicken Sie auf die Schaltfläche, um die Zeiteinstellung des PCs zu übernehmen.
- **Letzter Synchronisationszeitpunkt**
  Zeigt an, wann die letzte Uhrzeitsynchronisation stattgefunden hat. Wenn keine Uhrzeitsynchronisation möglich war, enthält das Feld die Angabe "Datum/Zeit nicht eingestellt".
- **Letzter Synchronisationsmechanismus**
  Zeigt an, wie die letzte Zeitsynchronisation durchgeführt wurde.
  - Nicht eingestellt
    Die Zeit wurde nicht eingestellt.
  - Manuell
    Manuelle Zeiteinstellung
  - SNTP
    Automatische Zeitsynchronisation über SNTP
  - NTP
    Automatische Zeitsynchronisation über NTP
  - SIMATIC
    Automatische Zeitsynchronisation über SIMATIC-Uhrzeittelegramm
- **Sommerzeit (DST)**
  Zeigt an, ob die Umstellung der Sommerzeit aktiv ist.
  - active (offset +1 h)
    Die Systemzeit wurde auf Sommerzeit umgestellt, d. h. es wird eine Stunde hinzugezählt.
    Die aktuelle Systemzeit sehen Sie oben rechts im Auswahlbereich des WBM.
    In dem Feld "Systemzeit" wird weiterhin die eingestellte Zeit angezeigt.
  - inactive (offset +0 h)
    Die aktuelle Systemzeit wird nicht verändert.

## Vorgehensweise

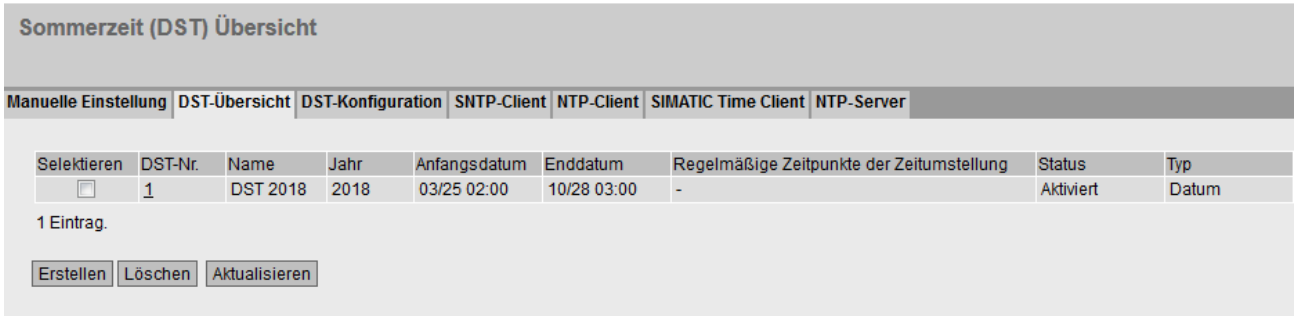
1. Aktivieren Sie die Option "Manuelle Zeiteinstellung".
2. Klicken Sie in das Eingabefeld "Systemzeit".

3. Geben Sie im Eingabefeld "Systemzeit" Datum und Uhrzeit im Format " MM/DD/YYYY HH:MM:SS" ein.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
   Datum und Uhrzeit werden übernommen und im Feld "Letzter Synchronisationsmechanismus" wird "Manuell" eingetragen.

### 5.5.8.2 DST-Übersicht

#### Umstellung der Sommerzeit

Auf dieser Seite können Sie neue Einträge für die Umstellung der Sommerzeit anlegen. Die Tabelle gibt Ihnen einen Überblick über die vorhandenen Einträge.




#### Einstellungen

Die Seite enthält folgende Felder:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **DST-Nr.**
  Zeigt die Nummer des Eintrags an.
  Wenn Sie einen neuen Eintrag anlegen, wird eine neue Zeile mit einer eindeutigen Nummer angelegt.
- **Name**
  Zeigt den Namen des Eintrags an.
- **Jahr**
  Zeigt das Jahr an, für das der Eintrag angelegt wurde.
- **Anfangsdatum**
  Zeigt Monat, Tag und Uhrzeit für den Start der Sommerzeit an.
- **Enddatum**
  Zeigt Monat, Tag und Uhrzeit für das Ende der Sommerzeit an.
- **Regelmäßige Zeitpunkte der Umstellung**
  Bei einem Eintrag des Typs "Regel" wird die Zeitspanne angezeigt, bestehend aus Woche, Tag, Monat und Uhrzeit, in der die Sommerzeit aktiv ist.
  Bei einem Eintrag des Typs "Datum" wird ein "-" angezeigt.

- **Status**
  Zeigt der Status des Eintrags an:
  - Aktiviert
    Der Eintrag wurde korrekt angelegt.
  - Ungültig
    Der Eintrag wurde neu angelegt und Anfangs- und Enddatum sind identisch.
- **Typ**
  Zeigt an, wie die Umstellung der Sommerzeit erfolgt:
  - Datum
    Es ist ein festes Datum für die Umstellung der Sommerzeit eingetragen.
  - Regel
    Es ist eine Regel für die Umstellung der Sommerzeit definiert.

## Vorgehensweise

**Eintrag anlegen**

1. Klicken Sie auf die Schaltfläche "Erstellen".
   In der Tabelle wird ein neuer Eintrag angelegt.
2. Klicken Sie in der Spalte "DST-Nr." auf den gewünschten Eintrag.
   Sie wechseln auf die Seite "DST-Konfiguration".
3. Wählen Sie in der Klappliste "Typ" den gewünschten Typ aus.
   Abhängig von dem gewählten Typ stehen Ihnen verschiedene Einstellungen zur Verfügung.
4. Geben Sie im Feld "Name" einen Namen ein.
5. Wenn Sie den Typ "Datum" ausgewählt haben, füllen Sie folgende Felder aus:
   - Jahr
   - Tag (für Start- und Enddatum)
   - Stunde (für Start- und Enddatum)
   - Monat (für Start- und Enddatum)
6. Wenn Sie den Typ "Regel" ausgewählt haben, füllen Sie folgende Felder aus:
   - Stunde (für Start- und Enddatum)
   - Monat (für Start- und Enddatum)
   - Woche (für Start- und Enddatum)
   - Tag (für Start- und Enddatum)
7. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

**Eintrag löschen**

1. Aktivieren Sie in der zu löschenden Zeile "Selektieren".
2. Klicken Sie auf die Schaltfläche "Löschen". Der Eintrag wird gelöscht.

### 5.5.8.3 DST-Konfiguration

#### Umstellung der Sommerzeit konfigurieren

Auf dieser Seite können Sie die Einträge für die Umstellung der Sommerzeit konfigurieren. Durch die Umstellung auf Sommer- bzw. Winterzeit ist die Systemzeit für die lokale Zeitzone korrekt eingestellt.

Sie können eine Regel für die Umstellung der Sommerzeit definieren oder ein festes Datum angeben.

#### Einstellungen

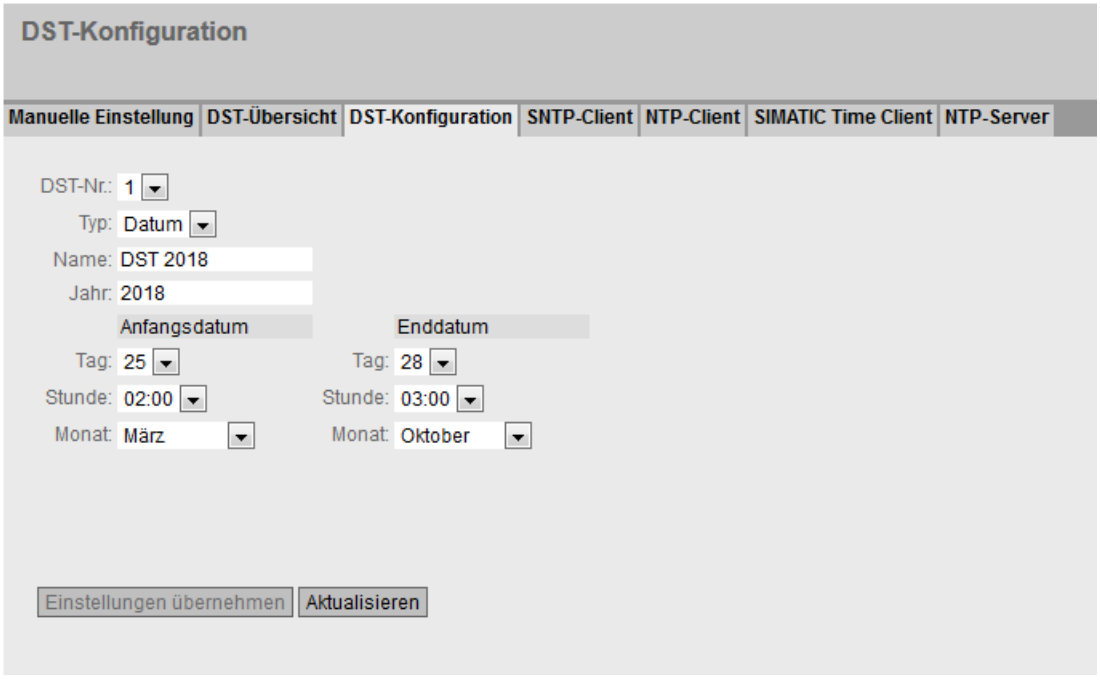
**Hinweis**

Der Inhalt dieser Seite ist abhängig davon, was Sie im Feld "Typ" auswählen.

Die Felder "DST-Nr.", "Typ" und "Name" werden immer angezeigt.

- **DST-Nr.**
  Wählen Sie die Nummer des Eintrags aus.
- **Typ**
  Wählen Sie aus, wie die Umstellung der Sommerzeit erfolgen soll:
  - Datum
    Sie können ein festes Datum für die Umstellung der Sommerzeit eingeben.
    Diese Einstellung eignet sich für Regionen, in denen die Umstellung der Sommerzeit keiner Regel folgt.
  - Regel
    Sie können eine Regel für die Umstellung der Sommerzeit definieren.
    Diese Einstellung eignet sich für Regionen, in denen die Sommerzeit immer an einem bestimmten Wochentag beginnt bzw. endet.
- **Name**
  Geben Sie einen Namen für den Eintrag ein.
  Der Name kann maximal 16 Zeichen lang sein.

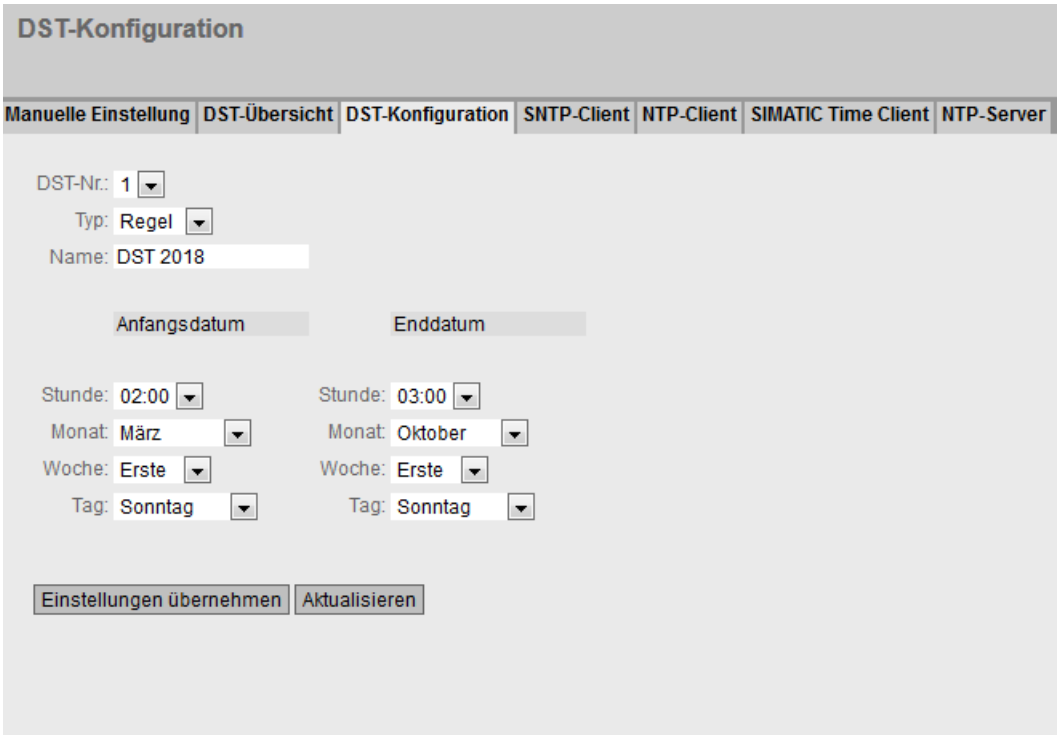
**Einstellungen bei der Auswahl "Datum"**




Sie können ein festes Datum für den Beginn und das Ende der Sommerzeit angeben.

- **Jahr**
  Geben Sie das Jahr für die Umstellung der Sommerzeit ein.
- **Anfangsdatum**
  Geben Sie folgende Werte für den Beginn der Sommerzeit ein:
  - Tag
    Geben Sie den Tag ein.
  - Stunde
    Geben Sie die Stunde ein.
  - Monat
    Geben Sie den Monat ein.
- **Enddatum**
  Geben Sie folgende Werte für das Ende der Sommerzeit ein:
  - Tag
    Geben Sie den Tag ein.
  - Stunde
    Geben Sie die Stunde ein.
  - Monat
    Geben Sie den Monat ein.

**Einstellungen bei der Auswahl "Regel"**


DST-Konfiguration
Manuelle Einstellung
DST-Übersicht
DST-Konfiguration
SNTP-Client
NTP-Client
SIMATIC Time Client
NTP-Server
DST-Nr.: 1
Typ: Regel
Name: DST 2018
Anfangsdatum
Enddatum
Stunde: 02:00
Monat: März
Woche: Erste
Tag: Sonntag
Stunde: 03:00
Monat: Oktober
Woche: Erste
Tag: Sonntag
Einstellungen übernehmen
Aktualisieren

Sie können eine Regel für die Umstellung der Sommerzeit erstellen.

- **Jahr**
  Geben Sie das Jahr für die Umstellung der Sommerzeit ein.
- **Anfangsdatum**
  Geben Sie folgende Werte für den Beginn der Sommerzeit ein:
  - Stunde
    Geben Sie die Stunde ein.
  - Monat
    Geben Sie den Monat ein.
  - Woche
    Geben Sie die Woche ein.
    Sie können die erste bis vierte oder die letzte Woche des Monats auswählen.
  - Tag
    Geben Sie den Wochentag ein.
- **Enddatum**
  Geben Sie folgende Werte für das Ende der Sommerzeit ein:
  - Stunde
    Geben Sie die Stunde ein.
  - Monat
    Geben Sie den Monat ein.
  - Woche
    Geben Sie die Woche ein.
    Sie können die erste bis vierte oder die letzte Woche des Monats auswählen.
  - Tag
    Geben Sie den Wochentag ein.

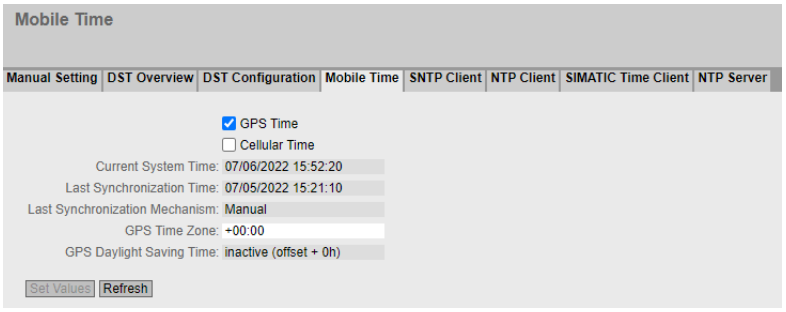
### 5.5.8.4 Mobile Zeit

MUM85x

#### Zeiteinstellung über GPS- oder Mobilfunksignal

**Hinweis**

Um Zeitsprünge zu vermeiden, stellen Sie sicher, dass sich nur ein Zeitserver im Netz befindet.




## Beschreibung

Die Seite enthält folgende Felder:

- **GPS Time**
  Wenn aktiviert, erhält das Gerät die Uhrzeit mit dem GPS-Signal von Navigationssatelliten. Die Uhrzeit wird alle 60 Sekunden aktualisiert.
- **Cellular Time**
  Wenn aktiviert, ruft das Gerät die Uhrzeit über ein Mobilfunknetz ab. Die Uhrzeit wird alle 60 Sekunden aktualisiert.
- **Aktuelle Systemzeit**
  Zeigt die aktuelle Systemzeit an.
- **Letzter Synchronisationszeitpunkt**
  Zeigt an, wann die letzte Uhrzeitsynchronisation stattgefunden hat.
- **Letzter Synchronisationsmechanismus**
  Zeigt an, wie die letzte Zeitsynchronisation durchgeführt wurde. Folgende Arten gibt es:
  - Nicht eingestellt
    Die Zeit wurde nicht eingestellt.
  - Manuell
    Manuelle Zeiteinstellung
  - SNTP
    Automatische Zeitsynchronisation über SNTP
  - NTP
    Automatische Zeitsynchronisation über NTP
  - SIMATIC
    Automatische Zeitsynchronisation über SIMATIC-Uhrzeittelegramm
  - Mobile Zeit
    Automatische Zeitsynchronisation über GPS oder Mobilfunk

- **GPS-Zeitzone**
  Geben Sie die verwendete Zeitzone im Format "(+/- )HH:MM" an. Die Zeitzone bezieht sich auf UTC Standard-Weltzeit.
  Die Zeitangabe im Feld "Aktuelle Systemzeit" wird entsprechend angepasst.
- **GPS-Sommerzeit**
  Zeigt an, ob die Umstellung der Sommerzeit aktiv ist.
  - active (offset +1 h)
    Die Systemzeit wurde auf Sommerzeit umgestellt, d. h. es wird eine Stunde hinzugezählt.
    Die aktuelle Systemzeit sehen Sie oben rechts im Auswahlbereich des WBM.
    In dem Feld "Systemzeit" wird weiterhin die eingestellte Zeit angezeigt.
  - inactive (offset +0 h)
    Die aktuelle Systemzeit wird nicht verändert.

### Vorgehensweise

1. Klicken Sie in das Optionskästchen "GPS Time" oder "Cellular Time", um das Abrufen der mobilen Uhrzeit zu aktivieren.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

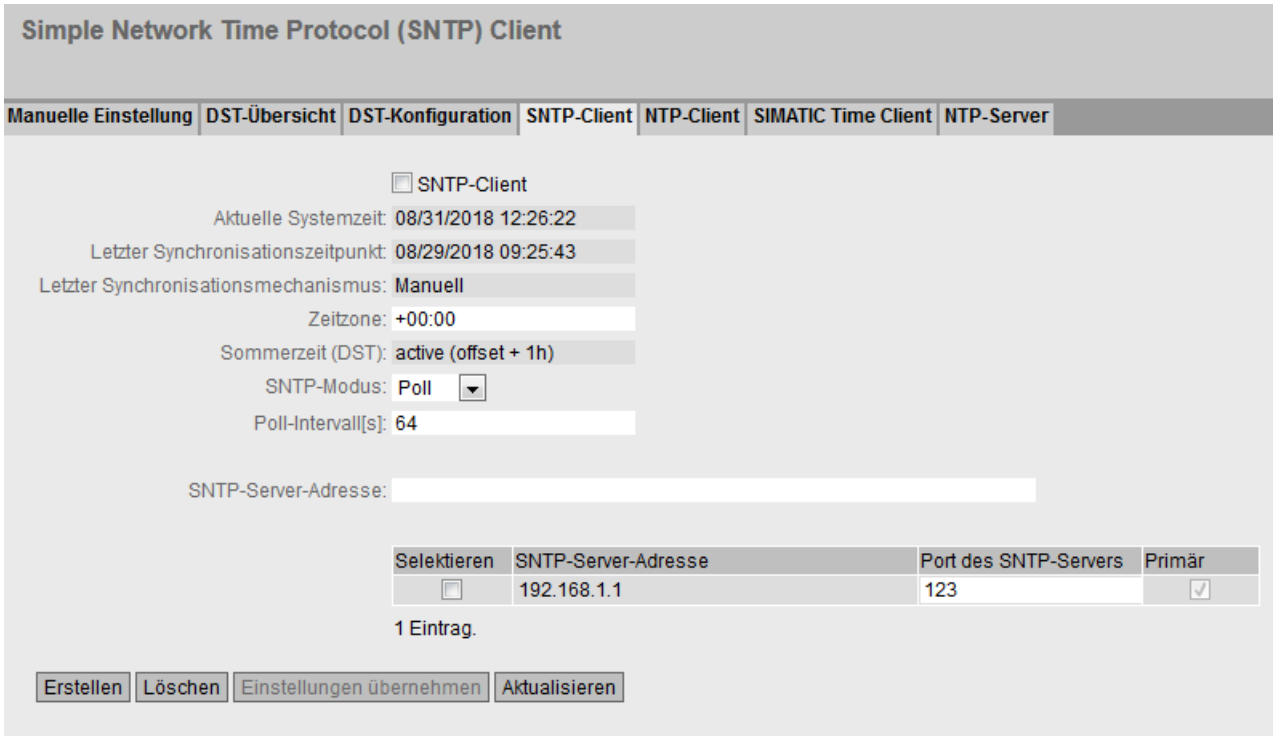
## 5.5.8.5 SNTP-Client

### Uhrzeitsynchronisation im Netzwerk

Das SNTP (**Simple Network Time Protocol**) dient zur Zeitsynchronisation im Netzwerk. Die entsprechenden Telegramme werden von einem SNTP-Server im Netz versendet.

**Hinweis**

Um Zeitsprünge zu vermeiden, stellen Sie sicher, dass sich nur ein Zeitserver im Netz befindet.




## Voraussetzung

Um die SNTP-Telegramme zu empfangen, aktivieren Sie unter "Security > Firewall > Vordefinierte IPv4-Regeln" den Eintrag "Systemzeit".

## Beschreibung

Die Seite enthält folgende Felder:

- **SNTP-Client**
  Wenn aktiviert, erhält das Gerät die Systemzeit von einem SNTP-Server.
- **Aktuelle Systemzeit**
  Zeigt das aktuelle Datum und die aktuelle Normalzeit an, die vom IE-Switch empfangen wurden. Wenn Sie eine Zeitzone angeben, wird die Zeitangabe entsprechend angepasst.
- **Letzter Synchronisationszeitpunkt**
  Zeigt an, wann die letzte Uhrzeitsynchronisation stattgefunden hat.

- **Letzter Synchronisationsmechanismus**
  Zeigt an, wie die letzte Zeitsynchronisation durchgeführt wurde. Folgende Arten sind möglich:
  - Nicht eingestellt
    Die Zeit wurde nicht eingestellt.
  - Manuell
    Manuelle Zeiteinstellung
  - SNTP
    Automatische Zeitsynchronisation über SNTP
  - NTP
    Automatische Zeitsynchronisation über NTP
  - SIMATIC
    Automatische Zeitsynchronisation über SIMATIC-Uhrzeittelegramm
- **Zeitzone**
  Geben Sie in diesem Feld Ihre verwendete Zeitzone im Format "+/- HH:MM" an. Die Zeitzone bezieht sich auf UTC Standard-Weltzeit.
  Die Zeitangabe im Feld "Aktuelle Systemzeit" wird entsprechend angepasst.
- **Sommerzeit (DST)**
  Zeigt an, ob die Umstellung der Sommerzeit aktiv ist.
  - active (offset +1 h)
    Die Systemzeit wurde auf Sommerzeit umgestellt, d. h. es wird eine Stunde hinzugezählt. Die aktuelle Systemzeit sehen Sie oben rechts im Auswahlbereich des WBM.
    In dem Feld "Systemzeit" wird weiterhin die eingestellte Zeit angezeigt.
  - inactive (offset +0 h)
    Die aktuelle Systemzeit wird nicht verändert.
- **SNTP-Modus**
  Wählen Sie aus der Klappliste die Synchronisationsart aus. Folgende Arten sind möglich:
  - Poll
    Wenn Sie diesen Modus wählen, werden die Eingabefelder "SNTP-Server-Adresse", "Port des SNTP Servers" und "Poll-Intervall[s]" zur weiteren Konfiguration eingeblendet. Bei dieser Synchronisationsart ist das Gerät aktiv und sendet eine Zeitabfrage an den SNTP-Server.
    In diesem Modus werden IPv4- und IPv6-Adressen unterstützt.
  - Listen
    Bei dieser Synchronisationsart ist das Gerät passiv und empfängt SNTP-Telegramme, die die Uhrzeit liefern. Die Einstellungen in den Eingabefeldern "SNTP-Server-Adresse" und "Port des SNTP-Servers" haben in diesem Modus keine Wirkung.
    In diesem Modus werden IPv4- und IPv6-Adressen unterstützt.

    **Hinweis**

    Der SNTP-Modus "Listen" des SNTP-Clients und der NTP-Server können nicht gleichzeitig aktiviert sein.

- **Poll-Intervall[s]**
  Geben Sie den Zeitabstand zwischen zwei Zeitanfragen ein. In diesem Feld geben Sie das Abfrageintervall in Sekunden an. Mögliche Werte sind 16 bis 16284 Sekunden.
- **SNTP-Server-Adresse**
  Geben Sie die IP-Adresse, den FQDN (Fully Qualified Domain Name) oder den Hostnamen des SNTP-Servers ein.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **SNTP-Server-Adresse**
  Zeigt die IP-Adresse, den FQDN (Fully Qualified Domain Name) oder den Hostnamen des SNTP-Servers an.
- **Port des SNTP-Servers**
  Geben Sie den Port des SNTP-Servers ein.
  Folgende Ports sind möglich:
  - 123 (Standard-Port)
  - 1025 bis 36564
- **Primär**
  Bei dem SNTP-Server, den Sie zuerst anlegen, wird das Häkchen gesetzt. Wenn mehrere SNTP-Server angelegt sind, wird der primäre Server zuerst angefragt.

### Vorgehensweise

1. Klicken Sie auf das Optionskästchen "SNTP-Client", um die automatische Zeiteinstellung zu aktivieren.
2. Geben Sie bei "Zeitzone" die lokale Zeitdifferenz zur Weltzeit (UTC) ein.
   Das Eingabeformat ist "+/-HH:MM", da der NTP-Server immer die UTC-Zeit sendet, z. B. +02:00 für MESZ, die mitteleuropäische Sommerzeit. Diese Zeit wird mithilfe der Angabe für die Zeitzone in die lokale Zeit umgerechnet.
3. Wählen Sie aus der Klappliste "SNTP-Modus" aus folgenden Optionen aus:
   - Poll
     Für diese Betriebsart müssen Sie Folgendes konfigurieren:
     - Zeitzonendifferenz (Schritt 2)
     - Abfrageintervall (Schritt 4)
     - Zeit-Server (Schritt 5)
     - Port (Schritt 7)
     - Schließen Sie die Konfiguration mit Schritt 8 ab.
   - Listen
     Für diese Betriebsart müssen Sie Folgendes konfigurieren:
     - Zeitdifferenz zu der vom Server gesendeten Zeit (Schritt 2)
     - Zeit-Server (Schritt 5)
     - Port (Schritt 7)
     - Schließen Sie die Konfiguration mit Schritt 8 ab.
4. Geben Sie bei "SNTP-Server-Adresse" die Adresse des SNTP-Servers ein, dessen Telegramme für die Synchronisation der Uhrzeit verwendet werden soll.

5. Geben Sie bei "Port des SNTP-Servers" den Port ein, über den der SNTP-Server verfügbar ist. Der Port kann nur geändert werden, wenn die IP-Adresse des SNTP-Servers eingetragen ist.
6. Geben Sie bei "Poll-Intervall[s]" die Zeitspanne in Sekunden ein, nach der eine neue Zeitanfrage beim Zeit-Server gestartet werden soll.
7. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

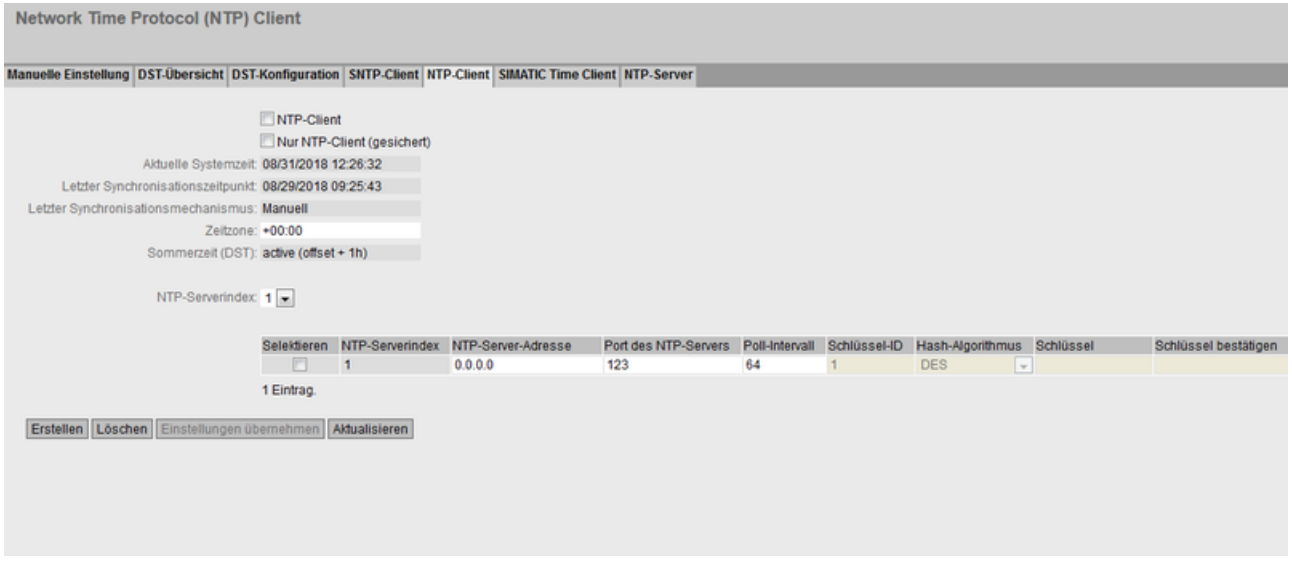
### 5.5.8.6 NTP-Client

#### Automatische Zeiteinstellung über NTP

Wenn die Uhrzeitsynchronisation über NTP erfolgen soll, legen Sie den Zeitserver fest, der zum Synchronisieren der Zeit verwendet wird.

**Hinweis**

Um Zeitsprünge zu vermeiden, stellen Sie sicher, dass sich nur ein Zeitserver im Netz befindet.




#### Voraussetzung

Um die NTP-Telegramme zu empfangen, aktivieren Sie unter "Security > Firewall > Vordefinierte IPv4-Regeln" den Eintrag "Systemzeit".

## Beschreibung

Die Seite enthält folgende Felder:

- **NTP-Client**
  Wenn aktiviert, erhält das Gerät die Systemzeit von einem NTP-Server.
- **Nur NTP-Client (gesichert)**
  Wenn aktiviert, erhält das Gerät die Systemzeit von einem gesicherten NTP-Server. Die Einstellung gilt für alle Servereinträge.
  Um den gesicherten NTP-Client zu nutzen, konfigurieren Sie die Parameter für die Authentifizierung (Schlüssel-ID, Hash-Algorithmus, Schlüssel).
- **Aktuelle Systemzeit**
  Zeigt das aktuelle Datum und die aktuelle Normalzeit an, die vom Gerät empfangen wurden. Wenn Sie eine Zeitzone angeben, wird die Zeitangabe entsprechend angepasst.
- **Letzter Synchronisationszeitpunkt**
  Zeigt an, wann die letzte Uhrzeitsynchronisation stattgefunden hat.
- **Letzter Synchronisationsmechanismus**
  Zeigt an, wie die letzte Zeitsynchronisation durchgeführt wurde. Folgende Arten gibt es:
  - Nicht eingestellt
    Die Zeit wurde nicht eingestellt.
  - Manuell
    Manuelle Zeiteinstellung
  - SNTP
    Automatische Zeitsynchronisation über SNTP
  - NTP
    Automatische Zeitsynchronisation über NTP
  - SIMATIC
    Automatische Zeitsynchronisation über SIMATIC-Uhrzeittelegramm
  - PTP
    Automatische Zeitsynchronisation über PTP
- **Zeitzone**
  Geben Sie die verwendete Zeitzone im Format "+/- HH:MM" an. Die Zeitzone bezieht sich auf UTC Standard-Weltzeit.
  Die Zeitangabe im Feld "Aktuelle Systemzeit" wird entsprechend angepasst.

- **Sommerzeit (DST)**
  Zeigt an, ob die Umstellung der Sommerzeit aktiv ist.
  - active (offset +1 h)
    Die Systemzeit wurde auf Sommerzeit umgestellt, d. h. es wird eine Stunde hinzugezählt.
    Die aktuelle Systemzeit sehen Sie oben rechts im Auswahlbereich des WBM.
    In dem Feld "Systemzeit" wird weiterhin die eingestellte Zeit angezeigt.
  - inactive (offset +0 h)
    Die aktuelle Systemzeit wird nicht verändert.
- **NTP-Serverindex**
  Wählen Sie den Index des NTP-Servers aus. Die NTP-Server werden in der Reihenfolge des NTP-Serverindex angefragt. Die Zeit des zuerst gefundenen Servers wird übernommen. Werden Zeit-Telegramme eines NTP-Servers mit einem kleineren Stratum-Wert empfangen, wird diese Zeit übernommen. Die Umschaltung auf die Zeit mit dem kleineren Stratum dauert ca. 30 Minuten

In der Tabelle konfigurieren Sie den NTP-Server

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **NTP-Serverindex**
  Die Nummer, die einem bestimmten NTP-Servereintrag entspricht.
- **NTP-Server-Adresse**
  Geben Sie die IP-Adresse, den FQDN (Fully Qualified Domain Name) oder den Hostnamen des NTP-Servers an.
- **Port des NTP-Servers**
  Geben Sie den Port des NTP-Servers an.
  Folgende Ports sind möglich:
  - 123 (Standard-Port)
  - 1025 bis 36564
- **Poll-Intervall**
  Legen Sie den Zeitabstand zwischen zwei Uhrzeitanfragen fest. Je größer der Zeitabstand, desto ungenauer ist die Uhrzeit des Geräts.
  Mögliche Werte sind 64 bis 2592000 Sekunden (30 Tage).

Die folgenden Spalten sind nur für einen gesicherten NTP-Client von Bedeutung. Wenn das Optionskästchen "Nur NTP-Client (gesichert)" nicht aktiviert ist, sind diese Felder gegraut:

- **Schlüssel-ID**
  Geben Sie die ID des Authentifizierungsschlüssels ein.
- **Hash-Algorithmus**
  Legen Sie das Format für den Authentifizierungsschlüssel fest.

- **Schlüssel**
  Geben Sie den Authentifizierungsschlüssel ein. Die Länge ist abhängig vom Hash-Algorithmus.
  - DES: ASCII 8 Zeichen
  - MD5: ASCII 16 – 128 Zeichen
  - SHA1: ASCII 20 – 128 Zeichen
- **Schlüssel bestätigen**
  Wiederholen Sie den Authentifizierungsschlüssel.

## Vorgehensweise

**Uhrzeitsynchronisation über NTP-Server**

1. Klicken Sie in das Optionskästchen "NTP-Client", um die automatische Zeiteinstellung über NTP zu aktivieren.
2. Geben Sie bei "Zeitzone" die lokale Zeitdifferenz zur Weltzeit (UTC) ein.
   Das Eingabeformat ist "+/-HH:MM", da der NTP-Server immer die UTC-Zeit sendet, z. B. +02:00 für MESZ, die mitteleuropäische Sommerzeit. Diese Zeit wird mithilfe der Angabe für die Zeitzone in die lokale Zeit umgerechnet.
3. Wählen Sie den "NTP-Serverindex" aus.
4. Klicken Sie auf die Schaltfläche "Erstellen".
   In der Tabelle wird eine Zeile für den NTP-Server angelegt.
5. Geben Sie bei "NTP-Server-Adresse" die Adresse des NTP-Servers ein, dessen Telegramme für die Synchronisation der Uhrzeit verwendet werden.
6. Geben Sie bei "Port des NTP-Servers" den Port ein, über den der NTP-Server verfügbar ist. Der Port ist nur änderbar, wenn Adresse des NTP-Servers eingetragen ist.
7. Geben Sie in der Spalte "Poll-Intervall" die Zeitspanne in Sekunden ein, nach der eine neue Uhrzeitanfrage beim Zeitserver gestartet wird.
8. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

**Uhrzeitsynchronisation über Secure NTP-Server**

Um die Uhrzeit über einen Secure NTP-Server zu synchronisieren, sind folgende zusätzliche Schritte notwendig:

1. Klicken Sie in das Optionskästchen "Nur NTP (secure)-Client", um die automatische Zeiteinstellung über Secure NTP zu aktivieren.
2. Konfigurieren Sie die Authentifizierung.
   - Geben Sie bei "Schlüssel-ID" die ID des Authentifizierungsschlüssels ein.
   - Wählen Sie bei "Hash-Algorithmus" das entsprechende Format aus.
   - Geben Sie bei "Schlüssel" den Authentifizierungsschlüssel ein.

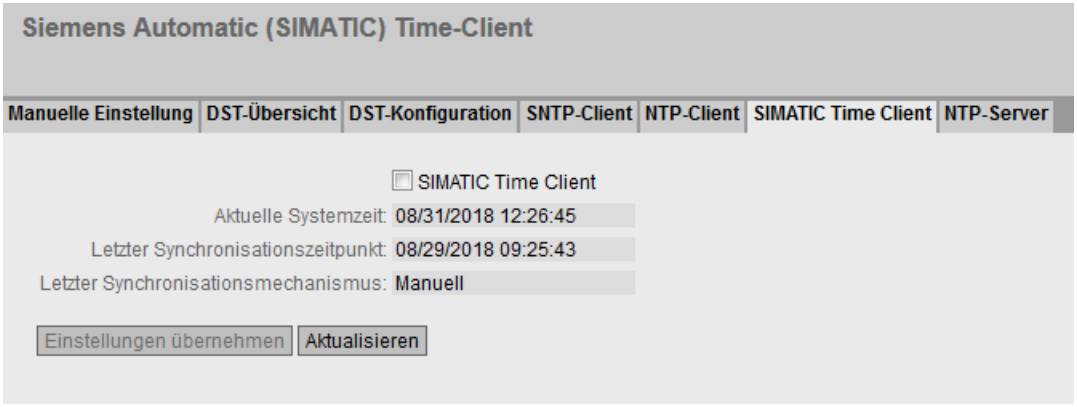
   Mit diesen Eingaben authentifiziert sich der NTP-Client am Secure NTP-Server. Auf dem Secure NTP-Server müssen diese Einträge vorhanden sein.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

### 5.5.8.7 SIMATIC Time Client

## Zeiteinstellung über SIMATIC Time Client

**Hinweis**

Um Zeitsprünge zu vermeiden, stellen Sie sicher, dass sich nur ein Zeitserver im Netz befindet.




## Beschreibung

Die Seite enthält folgende Felder:

- **SIMATIC Time Client**
  Markieren Sie dieses Optionskästchen, um das Gerät als SIMATIC Time Client zu aktivieren.
- **Aktuelle Systemzeit**
  Zeigt die aktuelle Systemzeit an.
- **Letzter Synchronisationszeitpunkt**
  Zeigt an, wann die letzte Uhrzeitsynchronisation stattgefunden hat.
- **Letzter Synchronisationsmechanismus**
  Zeigt an, wie die letzte Zeitsynchronisation durchgeführt wurde. Folgende Arten gibt es:
  - Nicht eingestellt
    Die Zeit wurde nicht eingestellt.
  - Manuell
    Manuelle Zeiteinstellung
  - SNTP
    Automatische Zeitsynchronisation über SNTP
  - NTP
    Automatische Zeitsynchronisation über NTP
  - SIMATIC
    Automatische Zeitsynchronisation über SIMATIC-Uhrzeittelegramm

### Vorgehensweise

1. Klicken Sie in das Optionskästchen "SIMATIC Time Client", um den SIMATIC Time Client zu aktivieren.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

## 5.5.8.8 NTP-Server

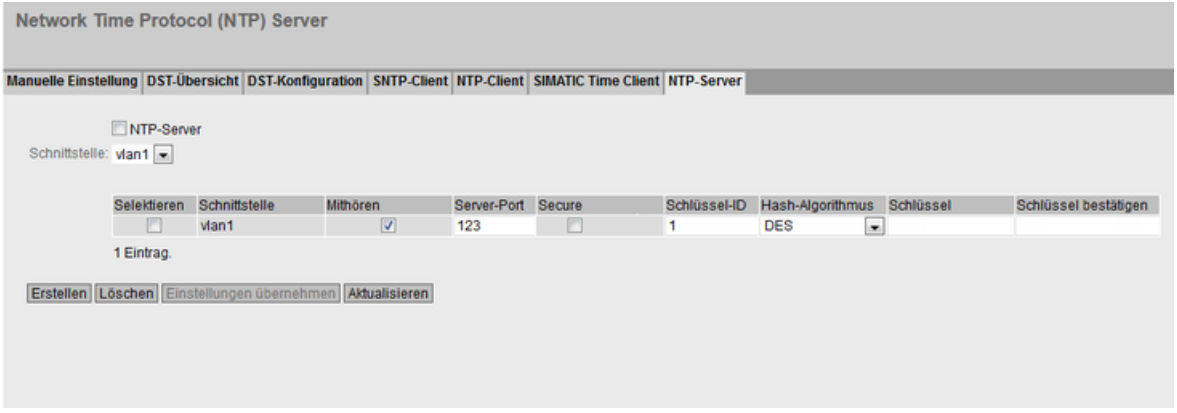
Auf dieser WBM-Seite konfigurieren Sie das Gerät als NTP-Server oder als NTP-Server vom Typ "NTP (secure)". Die anderen Geräte können über diesen NTP-Server die vom Gerät bereitgestellte Zeit abrufen. Damit sind die versorgten Geräte nicht auf eine Verbindung zu einem externen Zeitserver angewiesen.

**Hinweis**

**Zeitsynchronisation**

Damit das Gerät die angeschlossenen Geräte auf einen korrekten Zeitstand synchronisiert, konfigurieren Sie das Gerät auch als NTP-Client. Als NTP-Client bezieht das Gerät die präzise Zeit von einem externen Zeitserver und verteilt diese als NTP-Server an seine NTP-Clients.

Der NTP-Server sendet nicht von sich aus zyklisch Nachrichten mit Zeitinformationen, sondern antwortet nur auf entsprechende Anfragen. Einstellungen in der Funktion als Client (Zeitzone und Sommerzeit) beeinflussen nicht die Zeitinformationen, die das Gerät als Server aussendet.




### Voraussetzung

- Um die NTP-Telegramme zu empfangen, aktivieren Sie unter "Security > Firewall > Vordefinierte IPv4-Regeln" den Eintrag "Systemzeit".

## Beschreibung

Die Seite enthält folgende Felder:

- **NTP-Server**
  Aktivieren oder deaktivieren Sie den Dienst des NTP-Servers.

  **Hinweis**

  Der SNTP-Modus "Listen" des SNTP-Clients und der NTP-Server können nicht gleichzeitig aktiviert sein.

- **Schnittstelle**
  Legen Sie fest, über welche Schnittstelle die Zeit mittels NTP übermittelt wird.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Schnittstelle**
  Über diese Schnittstelle wird die Zeit mithilfe von NTP übermittelt.
- **Mithören**
  Wenn aktiviert, können die anderen Geräte über diese Schnittstelle die Uhrzeit abrufen.
- **Server-Port**
  Legen Sie den Port des NTP-Servers fest.
  Folgende Ports sind möglich:
  - 123 (Standard-Port)
  - 1025 bis 36564
- **Secure**
  Wenn aktiviert, wird aus dem NTP-Server ein NTP-Server vom Typ "NTP (secure)".

Die folgenden Spalten sind nur für "NTP (secure)" von Bedeutung. Ansonsten sind die Felder nicht editierbar:

- **Schlüssel-ID**
  Geben Sie die ID des Authentifizierungsschlüssels ein.
- **Hash-Algorithmus**
  Legen Sie das Format für den Authentifizierungsschlüssel fest.
- **Schlüssel**
  Geben Sie den Authentifizierungsschlüssel ein. Die Länge ist abhängig vom Hash-Algorithmus.
  Folgende Mindestlängen werden für den Hash-Algorithmus empfohlen:
  - DES: ASCII 8 Zeichen
  - MD5: ASCII 16 Zeichen
  - SHA1: ASCII 20 Zeichen
- **Schlüssel bestätigen**
  Geben Sie den Authentifizierungsschlüssel zur Bestätigung ein.

## 5.5.9 Auto-Logout

### Einstellung der automatischen Abmeldung

Auf dieser Seite legen Sie die Zeiten fest, nach denen bei Inaktivität des Benutzers eine automatische Abmeldung vom WBM oder dem CLI stattfindet.

Wenn Sie automatisch abgemeldet wurden, dann müssen Sie sich wieder neu anmelden.

---

**Hinweis**

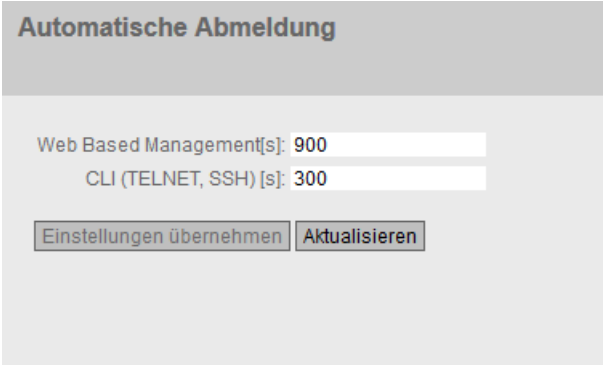
**Keine automatische Abmeldung vom CLI**

Wenn die Verbindung nach der eingestellten Zeit nicht beendet wird, prüfen Sie am Telnet Client die Einstellung von "Keep alive".

Ist die Intervallzeit für "Keep alive" kleiner als die projektierte Zeit, wird die Verbindung aufrechterhalten, obwohl keine Nutzdaten übertragen werden. Z. B. Sie haben bei der automatischen Abmeldung 300 Sekunden und bei "Keep alive" 120 Sekunden eingestellt. In diesem Fall wird alle 120 Sekunden ein Paket gesendet, das die Verbindung ununterbrochen aufrechterhält.

- Schalten Sie die "Keep alive" aus (Intervallzeit=0)
  oder
- Stellen Sie die Intervallzeit so hoch ein, dass die unterlagerte Verbindung bei Inaktivität beendet wird.

---




### Vorgehensweise

1. Geben Sie in das Eingabefeld "Web Base Management [s]" einen Wert von 60-3600 Sekunden ein. Wenn Sie den Wert 0 eingeben, ist die automatische Abmeldung deaktiviert.
2. Geben Sie in das Eingabefeld "CLI (TELNET, SSH) [s]" einen Wert von 60-600 Sekunden ein. Wenn Sie den Wert 0 eingeben, ist die automatische Abmeldung deaktiviert.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

## 5.5.10 Taster

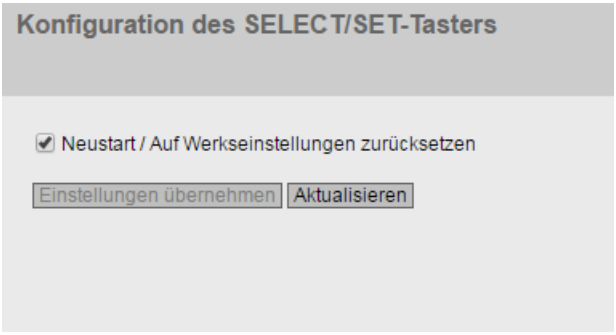
### Funktionalität

Der SELECT/SET-Taster dient zum:

- Neustart
- Laden einer neuen Firmware,
- Zurücksetzen auf Werkseinstellungen.

Eine detaillierte Beschreibung der Funktionen finden Sie in der Betriebsanleitung des Geräts.

Auf dieser Seite kann die Funktionalität des Tasters eingeschränkt werden.




### Beschreibung

Folgende Funktionalität ist möglich:

- **Neustart / Auf Werkseinstellungen zurücksetzen**
  Wenn deaktiviert, kann der SELECT/SET-Taster nicht zum Neustart oder zum Zurücksetzen auf Werkseinstellungen verwendet werden.

  **⚠ VORSICHT**

  **Tasterfunktion "Neustart / Auf Werkseinstellungen zurücksetzen" beim Hochlauf aktiv**

  Wenn Sie diese Funktion in ihrer Projektierung deaktiviert haben, ist die Deaktivierung nur im laufenden Betrieb gültig. Bei einem Hochlauf, z. B. nach "Stromaus", ist die Funktion bis zum Laden der Projektierung aktiv und das Gerät kann so auch unbeabsichtigt auf die Werkseinstellungen zurückgesetzt werden. Dies kann zu unerwünschten Störungen des Netzwerkbetriebs führen, da das Gerät dann neu projektiert werden muss. Ein gesteckter PLUG wird dabei ebenfalls gelöscht und in den Auslieferungszustand versetzt.

  Weitere Informationen, wie Sie das Gerät trotz deaktivierter Funktionen auf Werkseinstellungen zurücksetzen können, finden Sie im Kapitel "Instandhalten und Warten (Seite 448)".

## 5.5.11 Syslog-Client

Auf dieser Seite konfigurieren Sie den Syslog-Client. Die Syslog-Meldungen können unverschlüsselt oder verschlüsselt an den Syslog-Server versendet werden.

### Voraussetzungen für das Versenden von Syslog-Meldungen

- Der Syslog-Client ist aktiviert.
- Unter "System > Ereignisse > Konfiguration" ist beim entsprechenden Ereignis "Syslog" aktiviert.
- In Ihrem Netz befindet sich ein Syslog-Server, der die Syslog-Meldungen entgegennimmt.
- Die IP-Adresse oder der FQDN (Fully Qualified Domain Name) des Syslog-Servers ist im Gerät eingetragen.




### Beschreibung

Die Seite enthält folgende Felder:

- **Syslog-Client**
  Aktivieren oder deaktivieren Sie auf dem Gerät den Syslog-Client.
- **Adresse des Syslog-Servers**
  Geben Sie die IP-Adresse, den FQDN (Fully Qualified Domain Name) oder den Hostnamen des Syslog-Servers an.

Die Tabelle enthält folgende Spalten

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Adresse des Syslog-Servers**
  Zeigt die IP-Adresse, den FQDN (Fully Qualified Domain Name) oder den Hostnamen des Syslog-Servers an.

- **Server-Port**
  Geben Sie den verwendeten Port des Syslog-Servers ein.
- **TLS**
  - Aktiviert
    Die Syslog-Meldungen werden mit TLS-Verschlüsselung über TCP gesendet.
  - Deaktiviert
    Die Syslog-Meldungen werden unverschlüsselt über UDP gesendet.

### Vorgehensweise

**Funktion aktivieren**

1. Aktivieren Sie das Optionskästchen "Syslog-Client".
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

**Neuen Eintrag anlegen**

1. Geben Sie in das Eingabefeld "Adresse des Syslog-Servers" die Adresse des Syslog-Servers ein, an den die Syslog-Meldungen gesendet werden.
2. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird eine neue Zeile eingefügt.
3. Geben Sie in das Eingabefeld "Server-Port" die Nummer des Ports des Servers ein.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

**Hinweis**

Die Standardeinstellung des Server-Ports ist Port 514.

**Eintrag ändern**

1. Löschen Sie den Eintrag.
2. Legen Sie einen neuen Eintrag an.

**Eintrag löschen**

1. Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
2. Klicken Sie auf die Schaltfläche "Löschen". Alle markierten Einträge werden gelöscht und die Anzeige wird aktualisiert.

## 5.5.12 Fehlerkontrolle

### 5.5.12.1 Spannungsversorgung

MUM85x

## Einstellungen zur Überwachung der Spannungsversorgung

Konfigurieren Sie, ob die Spannungsversorgung durch das Meldesystem überwacht werden soll. Je nach Hardware-Variante gibt es ein oder zwei Spannungsanschlüsse (Versorgung 1 / Versorgung 2) und eine PoE-Spannungsversorgung. Bei redundanter Spannungsversorgung konfigurieren Sie die Überwachung für jede einzelne Zuleitung getrennt.

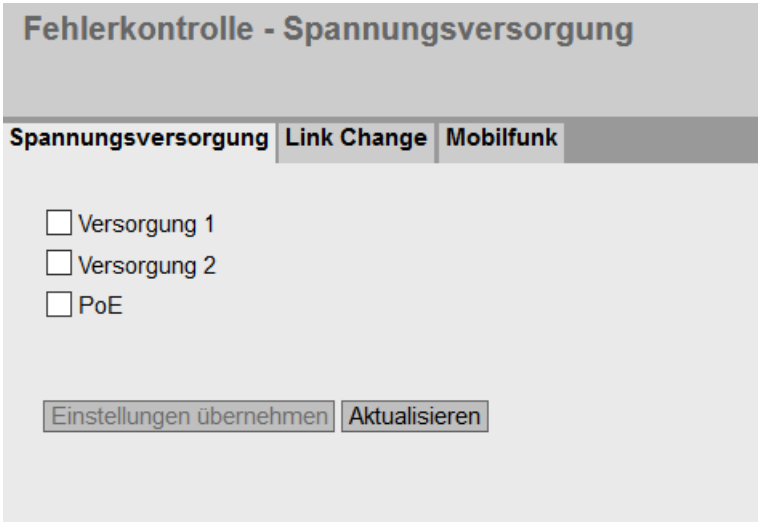
Es wird dann ein Fehler durch das Meldesystem signalisiert, wenn an einem überwachten Anschluss (Versorgung 1, Versorgung 2 oder PoE) keine oder eine zu geringe Spannung anliegt.

**Hinweis**

Die zulässigen Betriebsspannungsgrenzen entnehmen Sie der Betriebsanleitung des Geräts.

Wenn ein Fehler auftritt, leuchtet am Gerät die Fehler-LED auf. Der aktuell anstehende Fehler wird unter "Information > Fehler" angezeigt.

Zusätzlich wird die entsprechende Fehlermeldung in die Ereignisprotokoll-Tabelle eingetragen. Den Inhalt der Ereignisprotokoll-Tabelle wird unter "Information > Log-Tabellen > Ereignis-Log" angezeigt.




## Vorgehensweise

1. Klicken Sie in das Optionskästchen vor dem entsprechenden Anschlussnamen, den Sie überwachen wollen, um die Überwachungsfunktion ein- oder auszuschalten.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

### 5.5.12.2 Link Change

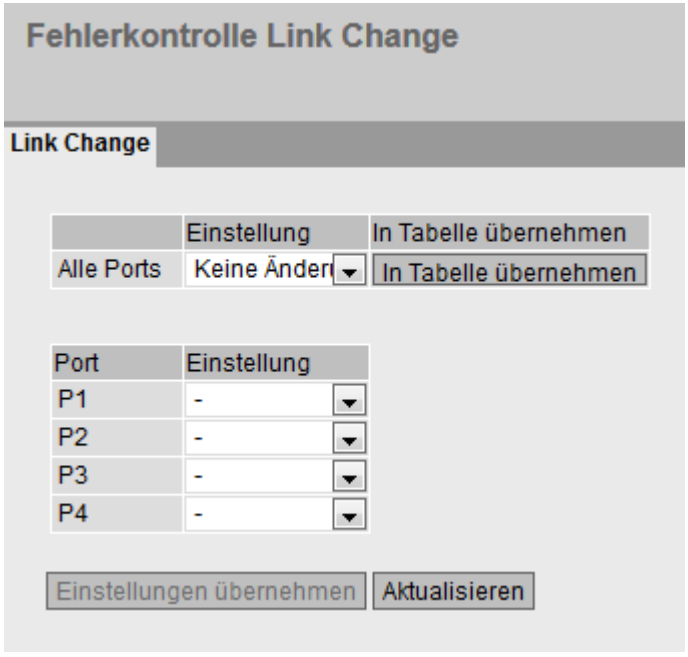
**Konfiguration der Fehlerüberwachung von Zustandsänderungen bei Verbindungen**

Auf dieser Seite konfigurieren Sie, ob bei einer Zustandsänderung einer Netzwerkverbindung eine Fehlermeldung ausgelöst wird.

Bei aktivierter Verbindungsüberwachung wird ein Fehler signalisiert,

- wenn an einem Port ein Link vorhanden sein soll und dieser fehlt.
- oder wenn an dem Port kein Link vorhanden sein soll und ein Link erkannt wird.

Ein Fehler führt zum Auslösen des Meldekontakts und zum Aufleuchten der Fehler-LED am Gerät und kann abhängig von der Konfiguration einen Trap, eine E-Mail, eine SMS oder einen Eintrag in der Ereignisprotokoll-Tabelle auslösen.



## Beschreibung

Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports gültig sind.
- **Einstellung**
  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellungsmöglichkeiten haben Sie:
  - "-" (Deaktiviert)
  - Up
  - Down
  - Keine Änderung: Einstellung in der Tabelle 2 bleibt unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt die verfügbaren Ports und Link Aggregationen an. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Einstellung**
  Wählen Sie aus der Klappliste die Einstellung aus. Folgende Möglichkeiten haben Sie:
  - Up
    Die Fehlerbehandlung wird beim Übergang in den aktiven Zustand des Ports ausgelöst. (Von "Link down" nach "Link up")
  - Down
    Die Fehlerbehandlung wird beim Übergang in den inaktiven Zustand des Ports ausgelöst. (Von "Link up" nach "Link down")
  - "-" (Deaktiviert)
    Die Fehlerbehandlung wird nicht ausgelöst.

## Vorgehensweise

**Fehlerüberwachung für einen Port konfigurieren**

1. Wählen Sie aus der entsprechenden Klappliste die Optionen der Steckplätze/Ports, deren Verbindungsstatus Sie überwachen wollen.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

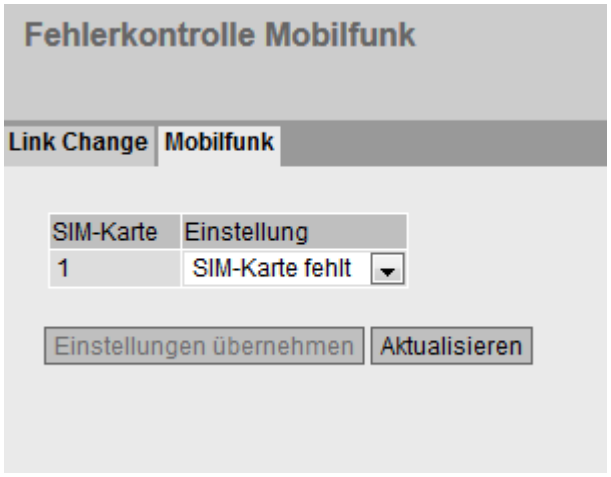
**Fehlerüberwachung für alle Ports konfigurieren**

1. Wählen Sie in der Klappliste der Spalte "Einstellung" die gewünschte Einstellung aus.
2. Klicken Sie auf die Schaltfläche "In Tabelle übernehmen". Die Einstellung wird für alle Ports der Tabelle 2 übernommen.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

### 5.5.12.3 Mobilfunk

M87x MUM856

Auf dieser Seite konfigurieren Sie, ob bei einer Zustandsänderung der SIM-Karte eine Fehlermeldung ausgelöst wird.




#### Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **SIM-Karte**
  Zeigt die verfügbaren SIM-Karten an.
- **Einstellung**
  Wählen Sie in der Klappliste die Einstellung aus. Folgende Möglichkeiten haben Sie:
  - "-" (Deaktiviert)
    Die Fehlerbehandlung wird nicht ausgelöst.
  - SIM-Karte fehlt
    Die Fehlerbehandlung wird ausgelöst, wenn keine SIM-Karte gesteckt ist. Ein Fehler führt zum Aufleuchten der Fehler-LED am Gerät.

## 5.5.13 PLUG

### 5.5.13.1 Konfiguration

~~M812~~

| **ACHTUNG** |
| --- |
| **PLUG nicht im laufenden Betrieb ziehen oder stecken!**<br>Ein PLUG darf nur bei ausgeschaltetem Gerät entnommen oder eingesetzt werden.<br>Das Gerät überprüft im Sekundenabstand, ob ein PLUG gesteckt ist. Wird festgestellt, dass der PLUG entfernt wurde, erfolgt ein Neustart. War in dem Gerät ein gültiger PLUG mit Lizenz gesteckt, wird das Gerät nach dem Neustart in einen definierten Fehlerzustand versetzt. Bei SCALANCE M werden in diesem Fall die verfügbaren Funkschnittstellen deaktiviert.<br>Wenn das Gerät einmal mit einem PLUG konfiguriert wurde, kann das Gerät ohne diesen PLUG nicht mehr genutzt werden. Um das Gerät wieder nutzen zu können, setzen Sie das Gerät auf Werkeinstellungen zurück. |

## Informationen über die Konfiguration

Diese Seite liefert Detailinformationen über die Konfiguration, die im PLUG abgelegt ist. Darüber hinaus gibt es die Möglichkeit, den PLUG auf Werkeinstellungen zurückzusetzen oder mit einem neuen Inhalt zu versehen.

**Hinweis**

**Inkompatibilität zu älteren Firmwareversionen mit gestecktem PLUG**

Bei der Installation einer älteren Firmwareversion kann es zu Verlust der Konfigurationsdaten kommen. Setzen Sie das Gerät in diesem Fall nach der Installation der Firmware auf Werkseinstellungen zurück.
Wenn in diesem Fall ein PLUG im Gerät gesteckt ist, hat dieser nach dem Neustart den Status "NOT ACCEPTED", da sich auf dem PLUG weiterhin die Konfigurationsdaten der vorherigen, aktuelleren Firmware befinden. Somit kann ohne Konfigurationsdatenverlust zur vorherigen, aktuelleren Firmware zurückgekehrt werden.

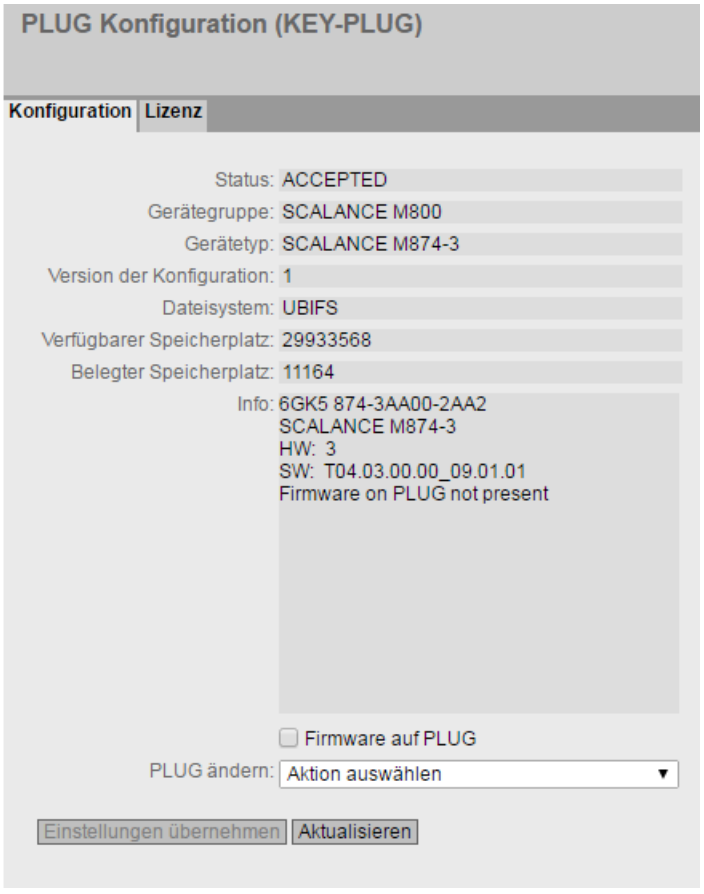
Falls die ursprüngliche Konfiguration auf dem PLUG nicht mehr benötigt wird, kann der PLUG manuell über "System > PLUG" gelöscht oder neu beschrieben werden.

**Hinweis**

Die Aktion wird erst dann durchgeführt, wenn Sie auf die Schaltfläche "Einstellungen übernehmen" klicken.

Die Aktion kann nicht rückgängig gemacht werden.

Wenn Sie sich nach der Auswahl gegen die Ausführung entscheiden, dann klicken Sie auf die Schaltfläche "Aktualisieren". Dadurch werden die Daten dieser Seite aus dem Gerät neu ausgelesen und Ihre Auswahl wird aufgehoben.


PLUG Konfiguration (KEY-PLUG)
Konfiguration
Lizenz
Status: ACCEPTED
Gerätegruppe: SCALANCE M800
Gerätetyp: SCALANCE M874-3
Version der Konfiguration: 1
Dateisystem: UBIFS
Verfügbarer Speicherplatz: 29933568
Belegter Speicherplatz: 11164
Info: 6GK5 874-3AA00-2AA2
SCALANCE M874-3
HW: 3
SW: T04.03.00.00_09.01.01
Firmware on PLUG not present
Firmware auf PLUG
PLUG ändern: Aktion auswählen
Einstellungen übernehmen
Aktualisieren

## Beschreibung

Die Tabelle gliedert sich in folgende Zeilen:

- **Status**
  Zeigt den Status des PLUG an. Es gibt die folgenden Möglichkeiten:
  - ACCEPTED
    Es ist ein PLUG mit einer gültigen und passenden Konfiguration im Gerät vorhanden.
  - NOT ACCEPTED
    Ungültige bzw. inkompatible Konfiguration auf dem gesteckten PLUG.
  - NOT PRESENT
    Im Gerät ist kein PLUG gesteckt.
  - FACTORY
    PLUG ist gesteckt und enthält keine Konfiguration. Dieser Status wird auch angezeigt, wenn der PLUG im Betrieb formatiert wurde.
  - MISSING
    Es ist kein PLUG gesteckt. Im Gerät sind Funktionen konfiguriert, für die eine Lizenz erforderlich ist.
- **Gerätegruppe**
  Zeigt an, von welcher SIMATIC NET-Produktlinie der PLUG im vorangegangenen Betrieb genutzt wurde.
- **Gerätetyp**
  Zeigt den Gerätetyp innerhalb der Produktlinie an, von dem der PLUG im vorangegangenen Betrieb genutzt wurde.
- **Version der Konfiguration**
  Die Version der Konfigurationsstruktur. Diese Angabe betrifft die vom Gerät unterstützten Konfigurationsmöglichkeiten und hat nichts mit der konkreten Hardware-Konfiguration zu tun. Diese Revisionsangabe ändert sich also nicht, wenn Sie Zusatzkomponenten (z.B. Module bzw. Extender) hinzufügen oder entfernen, sie kann sich aber ändern, wenn Sie ein Firmware-Update durchführen.
- **Dateisystem**
  Zeigt den Typ des Dateisystems an, das auf dem PLUG vorhanden ist.
- **Verfügbarer Speicherplatz**
  Zeigt die maximale Speicherkapazität des Dateisystems an, das auf dem PLUG vorhanden ist.
- **Belegter Speicherplatz**
  Zeigt den belegten Speicherplatz im Dateisystem des PLUG an.
- **Firmware auf PLUG**
  Wenn die Funktion aktiviert ist (Default), wird die Firmware auf dem PLUG abgespeichert. Damit können mit dem PLUG automatische Firmware-Updates/Downgrades durchgeführt werden. In dem Feld "Info" wird angezeigt, ob die Firmware auf dem PLUG gespeichert ist oder nicht.

- **Info**
  Zeigt zusätzliche Informationen über das Gerät an, das den PLUG im vorangegangenen Betrieb genutzt hatte, z. B. Artikelnummer, Typenbezeichnung sowie die Ausgabestände von Hard- und Software. Der angezeigte Software-Ausgabestand entspricht dem Ausgabestand, in dem zuletzt die Konfiguration geändert wurde. Beim Status "NOT ACCEPTED" werden weitere Informationen zur Problemursache angezeigt.
  Wenn ein PLUG als PRESET-PLUG konfiguriert wurde, wird dies hier als Zusatzinformation in der ersten Zeile angezeigt. Nähere Informationen zur Erstellung und Benutzung eines PRESET-PLUG finden Sie in Kapitel "Instandhalten und Warten (Seite 443)".
- **PLUG ändern**
  Wählen Sie aus der Klappliste die Einstellung. Sie haben folgende Möglichkeiten, um die Konfiguration auf dem PLUG zu ändern:
  - Aktuelle Konfiguration auf den PLUG schreiben
    Diese Option ist nur verfügbar, wenn der Status des PLUG "NOT ACCEPTED" oder "FACTORY" ist.
    Die im internen Flash-Speicher des Geräts vorhandene Konfiguration wird auf den PLUG kopiert.
  - PLUG auf Werkseinstellungen zurücksetzen
    Löscht alle Daten vom PLUG und führt eine Low-Level-Formatierung durch.

### Vorgehensweise

1. Sie können in diesem Feld nur dann Einstellungen vornehmen, wenn Sie als "Administrator" angemeldet sind. Wählen Sie hier aus, wie Sie den Inhalt des PLUG verändern wollen.
2. Wählen Sie aus der Klappliste "PLUG ändern" die gewünschte Option aus.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

## 5.5.13.2 Lizenz

M812

| **ACHTUNG** |
| --- |
| **Den PLUG nicht im laufenden Betrieb ziehen oder stecken!**<br>Ein PLUG darf nur bei ausgeschaltetem Gerät entnommen oder eingesetzt werden.<br>Das Gerät überprüft im Sekundenabstand, ob ein PLUG gesteckt ist. Wird festgestellt, dass der PLUG entfernt wurde, erfolgt ein Neustart. War in dem Gerät ein gültiger PLUG mit Lizenz gesteckt, wird das Gerät nach dem Neustart in einen definierten Fehlerzustand versetzt. Bei SCALANCE M werden in diesem Fall die verfügbaren Funkschnittstellen deaktiviert.<br>Wenn das Gerät einmal mit einem PLUG konfiguriert wurde, kann das Gerät ohne diesen PLUG nicht mehr genutzt werden. Um das Gerät wieder nutzen zu können, setzen Sie das Gerät auf Werkeinstellungen zurück. |

**Hinweis**

**Inkompatibilität zu älteren Firmwareversionen mit gestecktem PLUG**

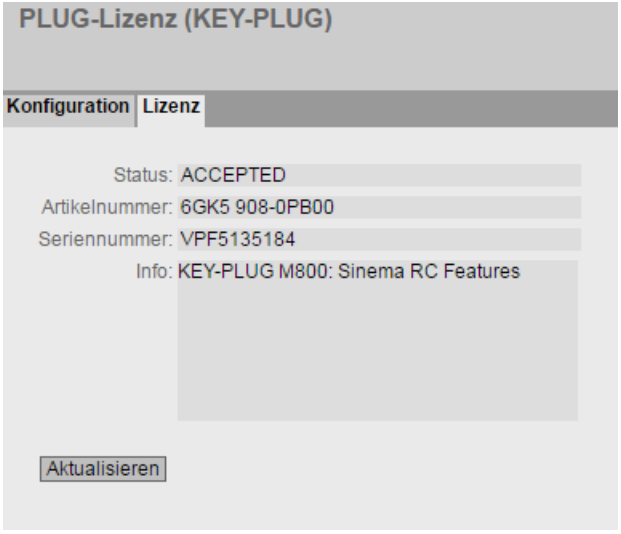
Bei der Installation einer älteren Firmwareversion kann es zu Verlust der Konfigurationsdaten kommen. Setzen Sie das Gerät in diesem Fall nach der Installation der Firmware auf Werkseinstellungen zurück.
Wenn in diesem Fall ein PLUG im Gerät gesteckt ist, hat dieser nach dem Neustart den Status "NOT ACCEPTED", da sich auf dem PLUG weiterhin die Konfigurationsdaten der vorherigen, aktuelleren Firmware befinden. Somit kann ohne Konfigurationsdatenverlust zur vorherigen, aktuelleren Firmware zurückgekehrt werden.

Falls die ursprüngliche Konfiguration auf dem PLUG nicht mehr benötigt wird, kann der PLUG manuell über "System > PLUG" gelöscht oder neu beschrieben werden.

## Informationen über die Lizenz auf dem PLUG

Ein PLUG mit Lizenz enthält zusätzlich zur Konfiguration eine Lizenz, die bestimmte Funktionen Ihres SIMATIC NET-Geräts freischaltet.

Diese Seite liefert Detailinformationen über die Lizenz auf dem PLUG.



## Beschreibung

- **Status**
  Zeigt den Status des PLUG an. Es gibt die folgenden Möglichkeiten:
  - ACCEPTED
    Es ist ein PLUG mit einer gültigen und passenden Lizenz im Gerät vorhanden.
  - NOT ACCEPTED
    Die Lizenz des gesteckten PLUG ist nicht gültig.
  - NOT PRESENT
    Im Gerät ist kein PLUG gesteckt.
  - MISSING
    Es ist kein PLUG mit dem Status "FACTORY" gesteckt. Im Gerät sind Funktionen konfiguriert, für die eine Lizenz erforderlich ist.
  - WRONG
    Der gesteckte PLUG passt nicht zum Gerät.
  - UNKNOWN
    Unbekannter Inhalt des PLUG.
  - DEFECTIVE
    Der Inhalt des PLUG ist fehlerhaft.
- **Artikelnummer**
  Zeigt die Artikelnummer des PLUG an. Es gibt den PLUG für unterschiedliche Funktionserweiterungen und für verschiedene Zielsysteme.
- **Seriennummer**
  Zeigt die Seriennummer des PLUG.
- **Info**
  Zeigt zusätzliche Informationen über das Gerät an, das den PLUG im vorangegangenen Betrieb genutzt hatte, z. B. Artikelnummer, Typenbezeichnung sowie die Ausgabestände von Hard- und Software. Der angezeigte Software-Ausgabestand entspricht dem Ausgabestand, in dem zuletzt die Konfiguration geändert wurde. Beim Status "NOT ACCEPTED" werden weitere Informationen zur Problemursache angezeigt.

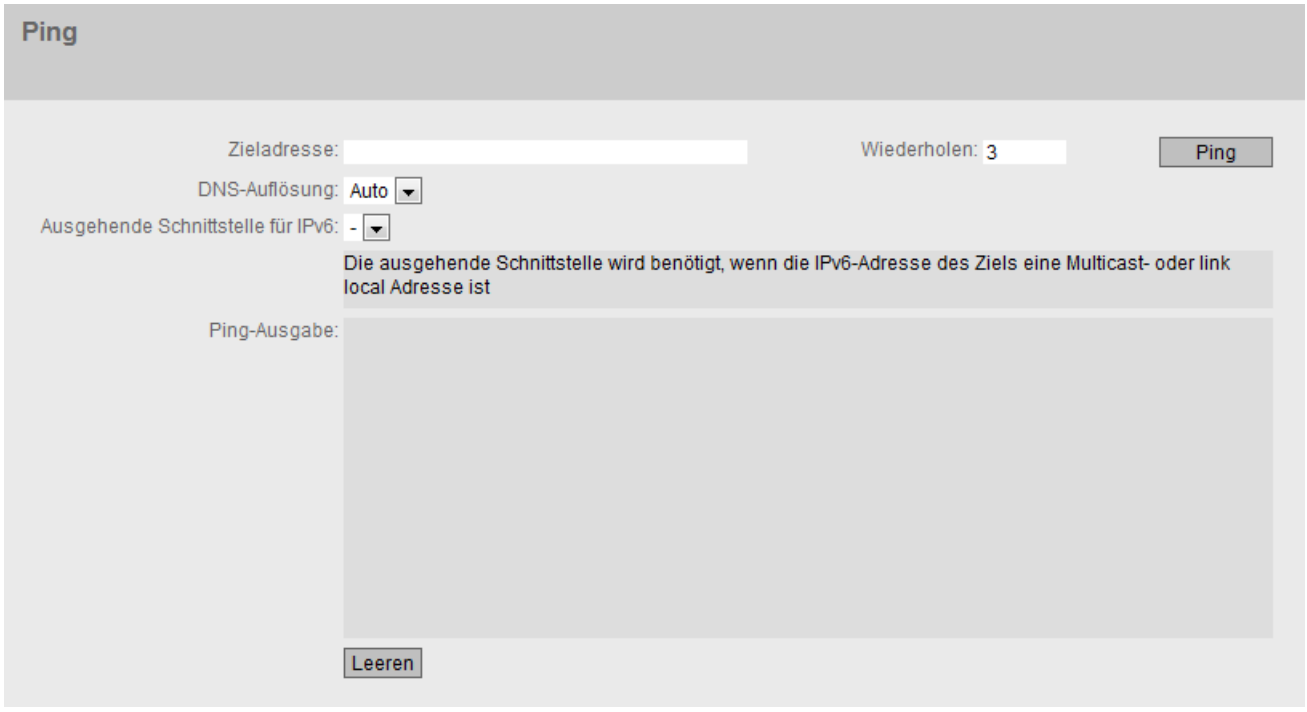
  **Hinweis**

  Beim Speichern der Konfiguration wird die Information mitgespeichert, ob zu diesem Zeitpunkt ein PLUG im Gerät gesteckt war. Diese Konfiguration ist dann auch nur lauffähig, wenn ein PLUG mit der gleichen Bestellnummer / Lizenz gesteckt ist.

## 5.5.14 Ping

### Erreichbarkeit einer Adresse in einem IP-Netzwerk

Mit der Ping-Funktion können Sie überprüfen, ob eine bestimmte IP-Adresse im Netzwerk erreichbar ist.




### Beschreibung

Die Seite enthält folgende Felder:

- **Zieladresse**
  Geben Sie die IPv4-, IPv6-Adresse oder den FQDN (Fully Qualified Domain Name) des Geräts ein.
- **Wiederholen**
  Tragen Sie die Anzahl der Ping-Anforderungen ein.
- **DNS-Auflösung**
  Wählen Sie aus in welchen IP-Adress-Typ ein eingegebener FQDN aufgelöst werden soll.
  - Auto
    In diesem Modus wird der IP-Adress-Typ automatisch gewählt.
  - IPv4
    Der eingegebene FQDN wird in einer IPv4-Adresse aufgelöst.
  - IPv6
    Der eingegebene FQDN wird in einer IPv6-Adresse aufgelöst.

- **Ausgehende Schnittstelle für IPv6**
  Diese Auswahl wird nur benötigt, wenn die Zieladresse eine Multicast- oder eine Link-lokale Adresse ist.
  - "-" (Werkseinstellung)
  - Wählen Sie die entsprechende IPv6-Schnittstelle aus.
- **Ping**
  Klicken Sie diese Schaltfläche, um die Ping-Funktion zu starten.
- **Ping-Ausgabe**
  Dieses Feld zeigt die Ausgabe der Ping-Funktion an.
- **Leeren**
  Klicken Sie diese Schaltfläche, um die Ping-Ausgabe zu leeren.

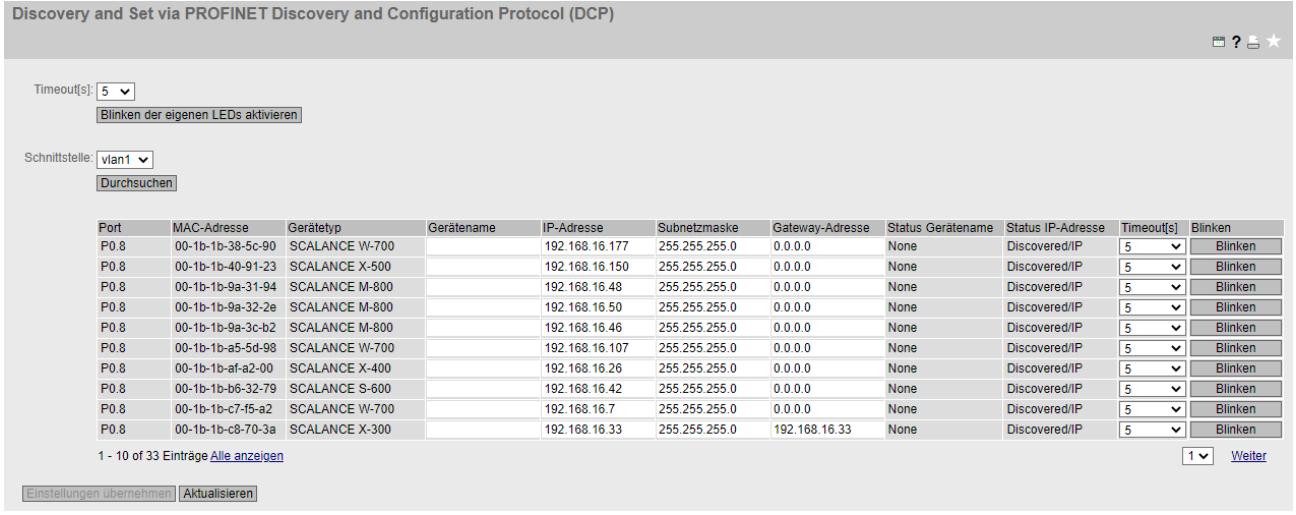
## 5.5.15 DCP Discovery

Auf dieser Seite können Sie eine Schnittstelle auswählen und nach den Geräten suchen, die über die Schnittstelle erreichbar sind und DCP unterstützen. DCP Discovery sucht nur nach Geräten, die im gleichen Subnetz liegen wie die Schnittstelle. Die erreichbaren Geräte werden in einer Tabelle aufgelistet. In der Tabelle können Sie die Netzwerkparameter der Geräte überprüfen und anpassen. Zum Identifizieren und zum Konfigurieren der Geräte wird das Discovery Configuration Protocol (DCP) verwendet.

**Hinweis**

**DCP Discovery**

Die Funktion ist nur in dem mit der TIA-Schnittstelle assoziierten VLAN verfügbar. Die TIA-Schnittstelle konfigurieren Sie unter "Layer 3 > Subnetze > Konfiguration".




**Voraussetzung**:

Um die Netzwerkparameter anzupassen, benötigt DCP Schreibrechte auf dem Gerät. Wenn der Zugriff schreibgeschützt ist, sind die Netzwerkparameter nicht konfigurierbar.

Auf den SCALANCE Geräten konfigurieren Sie den Zugriff unter "System > Konfiguration".

## Beschreibung

Die Seite enthält folgende Felder:

- **Timeout[s]**
  Legen Sie die Zeitdauer für das Blinken fest. Wenn die Zeit abgelaufen ist, wird das Blinken beendet.
- **Blinken der eigenen LEDs aktivieren**
  Lässt die LEDs des eigenen Geräts blinken.
- **Schnittstelle**
  Wählen Sie die gewünschte Schnittstelle aus.
- **Durchsuchen**
  Startet die Suche nach Geräten, die über die gewählte Schnittstelle erreichbar sind.
  Nach dem Abschluss der Suche werden die erreichbaren Geräte in der Tabelle aufgelistet. Die Tabelle ist auf 100 Einträge begrenzt.

Die Tabelle gliedert sich in folgende Spalten:

- **Port**
  Zeigt den Port an, über den das Gerät erreichbar ist.
- **MAC-Adresse**
  Zeigt die MAC-Adresse des Geräts an.
- **Gerätetyp**
  Zeigt an, zu welcher Produktlinie bzw. Produktgruppe das Gerät gehört.
- **Gerätename**
  Passen Sie bei Bedarf den PROFINET-Gerätenamen an.
  Der Gerätename muss DNS-konform sein. Wenn der Gerätename nicht verwendet wird, ist das Feld leer
- **IP-Adresse**
  Passen Sie bei Bedarf die IPv4-Adresse des Geräts an.
  Die IPv4-Adresse sollte innerhalb Ihres Netzwerks eindeutig sein und zum Netzwerk passen.
  Die IPv4-Adresse 0.0.0.0 bedeutet, dass noch keine IPv4-Adresse eingestellt ist.
- **Subnetzmaske**
  Passen Sie bei Bedarf die Subnetzmaske des Geräts an.
- **Gateway-Adresse**
  Passen Sie bei Bedarf die IPv4-Adresse des Gateways an.
- **Status Gerätename**
  - None: Der Gerätename wird nicht verwendet.
  - Discovered: Der eingestellte Gerätename wird verwendet.
  - Configured: Dem Gerät wurde ein neuer Gerätename zugewiesen.

- **Status IP-Adresse**
  - Discovered/IP: Das Gerät verwendet eine statische IPv4-Adresse.
  - Discovered/DHCP: Das Gerät hat die IPv4-Adresse von einem DHCP-Server bezogen.
  - Configured: Dem Gerät wurde eine neue IPv4-Adresse zugewiesen.
- **Timeout[s]**
  Legen Sie die Zeitdauer für das Blinken fest. Wenn die Zeit abgelaufen ist, wird das Blinken beendet.
- **Blinken**
  Lässt die LEDs des ausgewählten Geräts blinken.

### Vorgehensweise

1. Wählen Sie die TIA-Schnittstelle aus.
2. Um alle Geräte anzuzeigen, die über die TIA-Schnittstelle erreichbar sind, klicken Sie auf die Schaltfläche "Durchsuchen".
3. Passen Sie die gewünschten Eigenschaften an.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
   Der Status der geänderten Eigenschaften ändert sich in "Configured".
5. Um sicherzustellen, dass die Eigenschaften korrekt übernommen wurden, klicken Sie erneut auf die Schaltfläche "Durchsuchen".
   Der Status der geänderten Eigenschaften ändert sich in "Discovered".

## 5.5.16 SMS

### 5.5.16.1 Allgemein

M87x MUM85x

Damit das Gerät eine SMS versenden kann, müssen Sie eine bestimmte SMS-Zentrale (Short Message Service Center, SMS-C) Ihres Mobilfunkanbieters oder Ihres Service-Providers eintragen.

- Wenn Sie die Standard-SMS-Zentrale verwenden, müssen Sie auf dieser WBM-Seite nichts konfigurieren. Die SIM-Karte enthält bereits die richtigen Informationen.
- Wenn Sie nicht die Standard-SMS-Zentrale verwenden, können Sie mit dieser WBM-Seite die gespeicherte Rufnummer der Standard-SMS-Zentrale durch eine andere ersetzen. Das ist abhängig von Ihrem Vertrag.




### Beschreibung

Die Seite enthält folgende Felder:

- **Aktuelle SMS Service Center Rufnummer**
  Zeigt die gespeicherte Rufnummer der SMS-Zentrale an.
- **SMS Service Center Rufnummer überschreiben**
  Tragen Sie die Rufnummer der SMS-Zentrale inklusive Landesvorwahl ein. Bestätigen Sie die Eingabe mit "Einstellungen übernehmen", um die Rufnummer auf der SIM-Karte zu speichern. Wird die Rufnummer bei "Aktuelle SMS Service Center Rufnummer" angezeigt, wurde die gespeicherte Rufnummer der SMS-Zentrale überschrieben und das Eingabefeld geleert.

**Hinweis**

Wenn die Änderung wirksam wird, wird die Mobilfunk-Verbindung für kurze Zeit unterbrochen. Das Ändern kann bis zu einer Minute dauern.

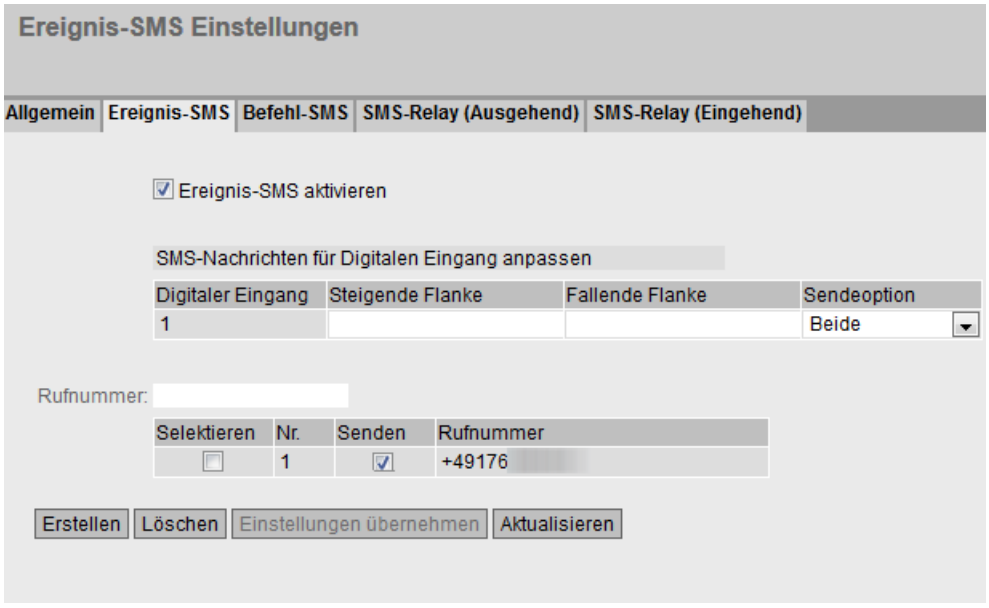
## 5.5.16.2 Ereignis SMS

M87x MUM85x

Beim Auftreten von Ereignissen kann das Gerät automatisch eine SMS versenden.

**Voraussetzung**:

- Unter "System > Ereignisse > Konfiguration" ist beim entsprechenden Ereignis "SMS" aktiviert.




## Beschreibung

Die Seite enthält Folgendes:

- **Ereignis-SMS aktivieren**
  Wenn aktiviert, dann versendet das Gerät eine SMS.

Im Bereich "SMS-Nachrichten für Digitalen Eingang anpassen" legen Sie den SMS-Text für den digitalen Eingang fest.

- **Digitaler Eingang**
  Zeigt die verfügbaren digitalen Eingänge an.
- **Steigende Flanke**
  Geben Sie den SMS-Text ein, der gesendet wird, wenn am digitalen Eingang das Signal von 0 (LOW) nach 1 (HIGH) wechselt.
- **Fallende Flanke**
  Geben Sie den SMS-Text ein, der gesendet wird, wenn am digitalen Eingang das Signal von 1 (HIGH) nach 0 (LOW) wechselt.

---

**Hinweis**

**Erlaubte Zeichen im Benutzernamen und Passwort**

Folgende Zeichen sind erlaubt:

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

Zusätzlich im Passwort erlaubt:

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

---

- **Sendeoption**
  Legen Sie fest, wann der SMS-Text versendet wird.
  - Keine
    Die Funktion ist deaktiviert.
  - Beide
    In beiden Fällen wird ein SMS-Text versendet.
  - Nur steigend
    Nur der SMS-Text wird gesendet, wenn am digitalen Eingang das Signal von 0 (LOW) nach 1 (HIGH) wechselt.
  - Nur fallend
    Nur der SMS-Text wird gesendet, wenn am digitalen Eingang das Signal von 1 (HIGH) nach 0 (LOW) wechselt.
- **Rufnummer**
  Geben Sie die vollständige Telefonnummer des Empfängers ein, das heißt inklusive der Landesvorwahl. Wenn Sie auf die Schaltfläche "Erstellen" klicken, wird eine neue Zeile mit einer eindeutigen Nummer angelegt.
- Die Tabelle enthält folgende Spalten:
  - **Selektieren**
    Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
  - **Nr.**
    Eindeutige Nummer, die beim Anlegen des Empfängers vergeben wird.
  - **Senden**
    Legen Sie fest, ob das Gerät eine SMS an diesen Empfänger sendet.
  - **Rufnummer**
    Zeigt die Telefonnummer des Empfängers an.

## Vorgehensweise

**Ereignis-SMS konfigurieren**

Um bei dem Wechsel des Signals von 0 (LOW) nach 1 (HIGH) eine SMS zu erhalten, gehen Sie wie folgt vor:

1. Legen Sie den bei "Steigender Flanke" den SMS-Text fest.
2. Wählen Sie bei "Sendeoption" "Nur Steigend" aus.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
4. Geben Sie in das Eingabefeld "Rufnummer" die Telefonnummer des Empfängers ein.
5. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird eine neue Zeile mit einer eindeutigen Nummer angelegt.
6. Legen Sie fest, ob das Gerät im Fehlerfall eine SMS an diesen Empfänger sendet.
7. Aktivieren Sie "Ereignis-SMS aktivieren".
8. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
9. Aktivieren Sie unter "System > Ereignisse > Konfiguration" beim Ereignis "Digitaler Eingang" die Benachrichtigungsart "SMS".

**Telefonnummer ändern**

1. Ändern Sie in der Spalte "Rufnummer" die gewünschte Telefonnummer.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

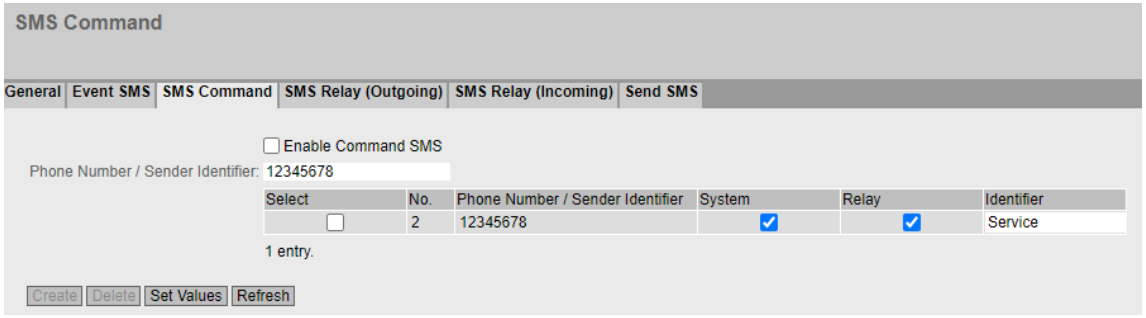
### 5.5.16.3 Befehl-SMS

M87x MUM85x

Befehle können auch per SMS abgesetzt werden. Auf dieser Seite legen Sie fest, von wem das Gerät gesteuert werden kann. Zur Identifikation wird entweder die Rufnummer oder die Absenderkennung angegeben. Die Absenderkennung kann z. B. eine IP-Adresse oder ein DNS-Name sein.

Mit einer Befehl-SMS können Sie z. B. eine VPN-Verbindung zu einer Anwendung wie dem SINEMA RC-Server aufbauen. Dazu sendet der SINEMA RC-Server eine Weck-SMS, die die notwendigen Befehle enthält. Weiterführende Informationen dazu erhalten Sie im Kapitel "Befehl-SMS (Seite 451)".

Um eine Antwort-SMS mit dem Status zu erhalten, müssen Sie zusätzlich auf der Seite die Rufnummer des Empfängers konfigurieren.



### Beschreibung

Die Seite enthält Folgendes:

- **Befehl-SMS aktivieren**
  Aktivieren oder deaktivieren Sie das Empfangen von Befehl-SMS.
- **Rufnummer / Absenderkennung**
  Geben Sie die Absenderkennung oder die Rufnummer inklusive der Landesvorwahl an. Wenn Sie auf die Schaltfläche "Erstellen" klicken, wird eine neue Zeile mit einer eindeutigen Nummer angelegt.
  Die Rufnummern können Sie mit dem Platzhalter Stern (*) beliebig viele Ziffern nach rechts ersetzen. Der Platzhalter kann nur am Ende einer Ziffernfolge stehen.
  Beispiel:
  +49177545* steht für alle Rufnummern, die mit 0177545 beginnen.

**Hinweis**

Bitte beachten Sie, wenn Sie den Platzhalter "*" verwenden, werden Befehl-SMS von einem großen Bereich an Rufnummern akzeptiert. Es wird empfohlen eine möglichst restriktive Eingabe zu verwenden.

Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Nr.**
  Zeigt die eindeutige Nummer des Eintrags an.
- **Rufnummer / Absenderkennung**
  Zeigt die Absenderkennung oder die Rufnummer an.
- **System / Relay**
  Legen Sie fest, welche Klasse (System / Relay) an Befehlen von diesem Absender akzeptiert wird. Weiterführende Informationen dazu erhalten Sie im Kapitel "Befehl-SMS (Seite 451)".
- **Identifier**
  Geben Sie einen Klartext-Wert ein, der mit dem empfangenen Identifier der SMS übereinstimmen muss. Verwenden Sie den Identifier, um SMS-Nachrichten zusätzlich zur Rufnummer abzusichern.

## 5.5.16.4 SMS-Relay (Ausgehend)

M87x | MUM85x

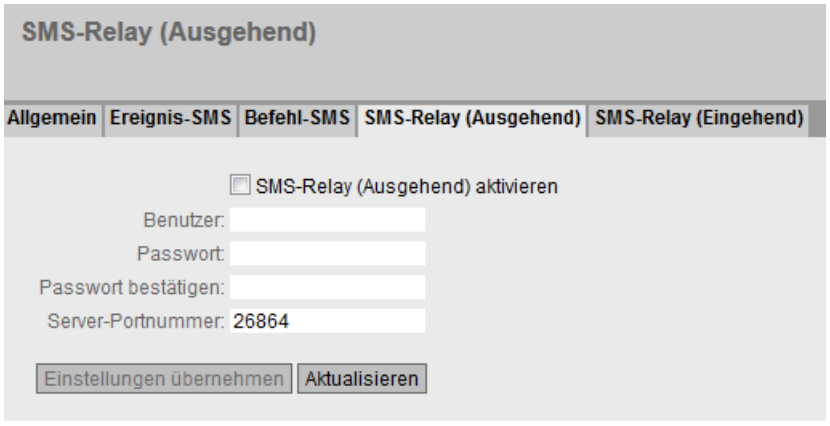
Mit der Funktion SMS-Versand können Anwendungen SMS verschicken, die an der Ethernet-Schnittstelle des Geräts angeschlossen sind. Zum Versand einer SMS muss die Anwendung an der Ethernet-Schnittstelle eine TCP/IP-Verbindung zum Gerät aufbauen. Über diese TCP/IP-

Verbindung sendet die Anwendung den Text der SMS an das Gerät, das den Text in eine SMS verpackt und verschickt.

**Hinweis**

Eine große Anzahl gesendeter SMS kann das Gerät überlasten. Beschränken Sie die SMS-Anzahl auf 20 Nachrichten pro Minute.

Das Gerät darf nicht Empfänger seiner eigenen SMS sein, dies würde zu einer Ereignisschleife führen.




**Format des SMS-Textes**

Der Text wird in einem Telegramm über die TCP/IP-Verbindung an das Gerät übermittelt, das folgendem Format entspricht:

<Benutzername>#<Passwort>#CommandCode#Seq-Num;<Rufnummer>;<Nachricht>:

Beispiel:

```
<Benutzername>#<Passwort>#105#01;<phone (phone number)>;<my-SMS-
text (sleep)>:
```

**Hinweis**

**Erlaubte Zeichen im Benutzernamen und Passwort**

Folgende Zeichen sind erlaubt:

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

Zusätzlich im Passwort erlaubt:

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

- **Benutzername**
  Geben Sie den Benutzernamen zur Prüfung der Sendeberechtigung einer SMS ein. Maximal 10 Zeichen.
- **Passwort**
  Geben Sie das zugehörige Passwort zum Benutzernamen ein. Maximal 10 Zeichen.
- **CommandCode**
  Kommando zum SMS-Versand aus dem lokalen Netz. Dieser Wert ist fest 105 und darf nicht verändert werden.
- **Seq-Num**
  Die Sequenznummer dient der Zuordnung mehrerer Anfragen gleichzeitig. Die Funktion wird derzeit nicht unterstützt.
  Die Sequenznummer besteht aus 2 nummerischen Zeichen von 01 bis 99.
- **Rufnummer**
  Rufnummer des SMS-Empfängers mit maximal 40 Zeichen. Internationale Nummern (+49...) sind zulässig.
- **Nachricht**
  SMS-Text mit maximal 160 Zeichen

### Beschreibung

Die Seite enthält Folgendes:

- **SMS-Relay (Ausgehend) aktivieren**
  Aktivieren oder deaktivieren Sie das Versenden von SMS aus dem lokalen Netzwerk.
- **Benutzer**
  Tragen Sie den Benutzernamen ein, der enthalten sein muss, bevor der Text per SMS versendet wird.
- **Passwort**
  Tragen Sie das Passwort ein, das enthalten sein muss, bevor der Text per SMS versendet wird.
- **Passwort bestätigen**
  Wiederholen Sie das Passwort, um es zu bestätigen.
- **Server-Portnummer**
  Tragen Sie den Port ein, auf dem der Server die SMS entgegennimmt.

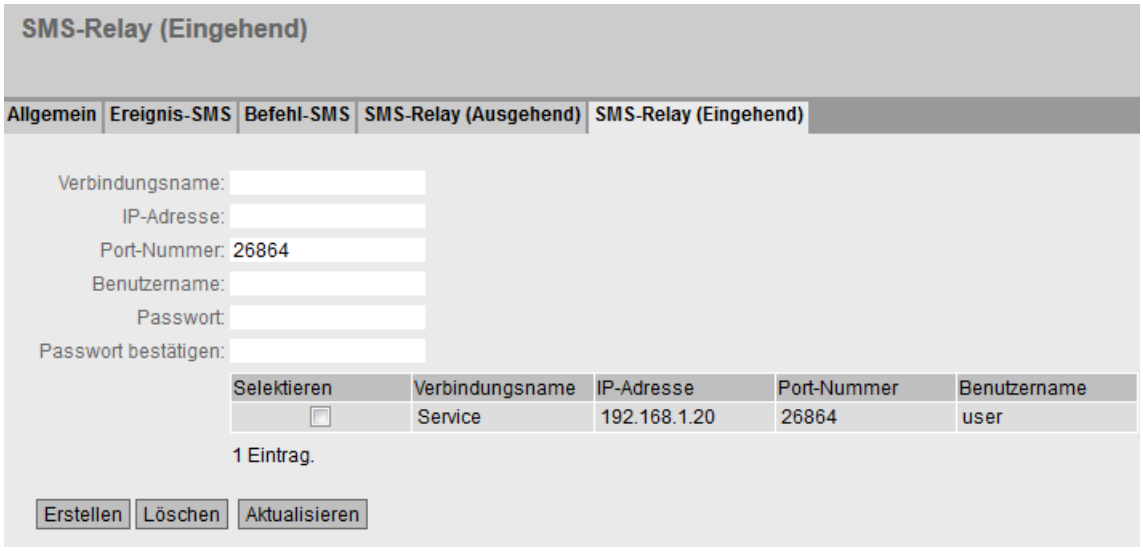
## 5.5.16.5 SMS-Relay (Eingehend)

M87x | MUM85x

Anwendungen können SMS empfangen, die an der Ethernet-Schnittstelle des Geräts angeschlossen sind. Zum Empfang einer SMS muss die Anwendung an der Ethernet-Schnittstelle eine TCP/IP-Verbindung zum Gerät aufbauen. Das Gerät empfängt eine Befehl-SMS und verschickt den enthaltenen Text weiter an die Anwendung.

**Hinweis**

Eine große Anzahl empfangener SMS kann das Gerät überlasten. Beschränken Sie die SMS-Anzahl auf 20 Nachrichten pro Minute.




**Format des SMS-Textes**

Der Text wird in einem Telegramm über die TCP/IP-Verbindung an die Anwendungen gesendet, das folgendem Format entspricht:

<Benutzername>#<Passwort>#CommandCode#Seq-Num;<Rufnummer>;<Nachricht>:

Benutzername#Passwort#CommandCode#Seq-Num;Rufnummer;Nachricht:

Beispiel:

```
<Benutzername>#<Passwort>#105#01;<phone (phone number)>;<my-SMS-
text (sleep)>:
```

---

**Hinweis**

**Erlaubte Zeichen im Benutzernamen und Passwort**

Folgende Zeichen sind erlaubt:

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

Zusätzlich im Passwort erlaubt:

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

---

- **Benutzername**
  Geben Sie den Benutzernamen zur Prüfung des Empfangs der Nachricht ein. Maximal 10 Zeichen.
- **Passwort**
  Geben Sie das zugehörige Passwort zum Benutzernamen ein. Maximal 10 Zeichen.
- **CommandCode**
  Kommando zum SMS-Versand in das lokale Netz. Dieser Wert ist fest 105.

- **Seq-Num**
  Die Sequenznummer dient der Zuordnung mehrerer Anfragen gleichzeitig. Die Funktion wird derzeit nicht unterstützt.
  Die Sequenznummer besteht aus 2 nummerischen Zeichen von 01 bis 99.
- **Rufnummer**
  Rufnummer des Absenders der Befehl-SMS mit maximal 40 Zeichen. Internationale Nummern (+49...) sind zulässig.
- **Nachricht**
  SMS-Text mit maximal 160 Zeichen

### Beschreibung

Die Seite enthält Folgendes:

- **Verbindungsname**
  Tragen Sie einen eindeutigen Namen für die Relay-Verbindung ein.
- **IP-Adresse**
  Tragen Sie die IP-Adresse des Empfängers ein. An diese IP-Adresse wird das Telegramm gesendet.
- **Port-Nummer**
  Tragen Sie den Port ein, an den das Telegramm gesendet wird.
- **Benutzername**
  Tragen Sie den Benutzernamen zur Prüfung des Empfangs der Nachricht ein. Der Benutzernamen wird in das Telegramm eingetragen.
- **Passwort**
  Tragen Sie das zum Benutzernamen zugehörige Passwort ein.
- **Passwort bestätigen**
  Wiederholen Sie das Passwort, um es zu bestätigen.

Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Verbindungsname**
  Zeigt den Namen der Relay-Verbindung an.
- **IP-Adresse**
  Zeigt die IP-Adresse des Empfängers an.
- **Portnummer**
  Zeigt den Port an.
- **Benutzername**
  Zeigt den Benutzernamen an, der im Telegramm enthalten ist.

## 5.5.16.6 SMS senden

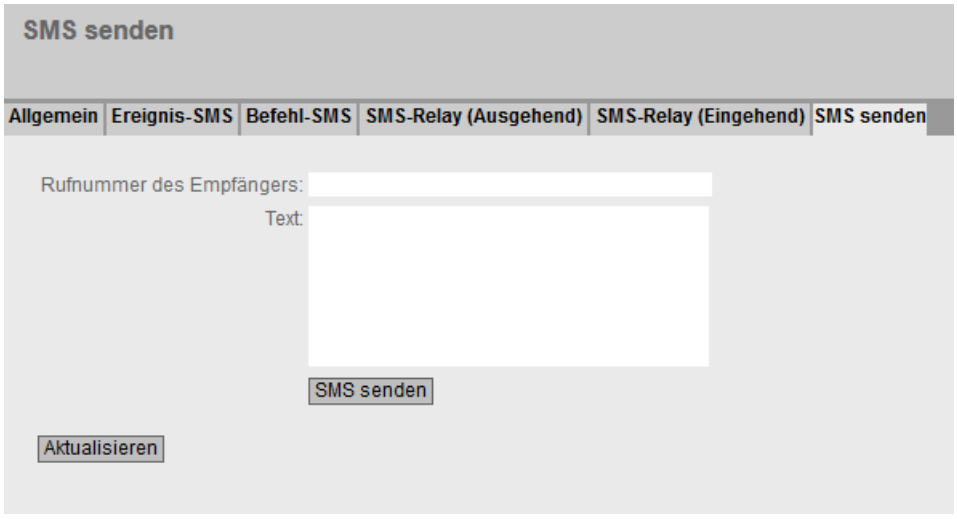
M87x | MUM85x

Diese Funktion sendet eine SMS direkt über das Gerät. Damit können Sie z. B. SMS-basierte Dienste wie Email2SMS testen.

**Hinweis**

Eine große Anzahl gesendeter SMS kann das Gerät überlasten. Beschränken Sie die SMS-Anzahl auf 20 Nachrichten pro Minute.

Das Gerät darf nicht Empfänger seiner eigenen SMS sein, dies würde zu einer Ereignisschleife führen.




## Beschreibung

Die Seite enthält Folgendes:

- **Rufnummer des Empfängers**
  Geben Sie die vollständige Telefonnummer des Empfängers ein, das heißt inklusive der Landesvorwahl.
- **Text**
  Geben Sie SMS-Text ein.

  **Hinweis**

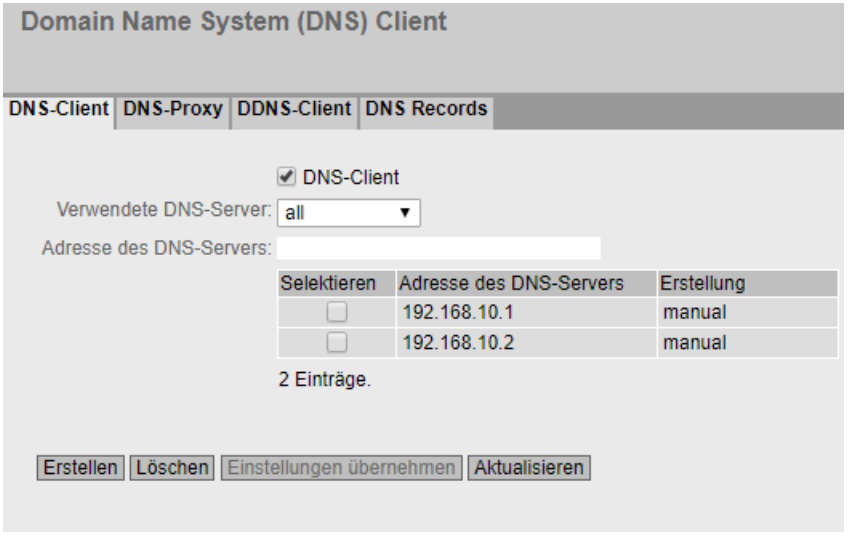
  **Erlaubte Zeichen für den SMS-Versand**

  In dem Text sind folgende Zeichen erlaubt:
  - 0123456789
  - A...Z a...z
  - Leerzeichen
  - ! " % & / ( ) = ? * + < > ' , . -
- **SMS senden**
  Das Gerät sendet die SMS an den Empfänger.

## 5.5.17 DNS

### 5.5.17.1 DNS-Client

Auf der WBM-Seite legen Sie fest, ob das Gerät den DNS-Server des Netzbetreibers oder einen anderen DNS-Server verwendet.




#### Beschreibung

Die Seite enthält folgende Felder:

- **DNS-Client**
  Aktivieren oder deaktivieren Sie, dass das Gerät als DNS-Client fungiert.
- **Verwendete DNS-Server**
  Legen Sie fest, welche DNS-Server das Gerät verwendet
  - learned only
    Das Gerät verwendet nur die durch DHCP zugewiesenen DNS-Server.
  - manual only
    Das Gerät verwendet nur die manuell projektierten DNS-Server. Die DNS-Server müssen mit dem Internet verbunden sein. Maximal zwei DNS-Server sind projektierbar.
  - all
    Das Gerät verwendet alle verfügbaren DNS-Server.
- **Adresse des DNS-Servers**
  Geben Sie die IP-Adresse des DNS-Servers ein.

Die Tabelle gliedert sich in folgende Spalten:

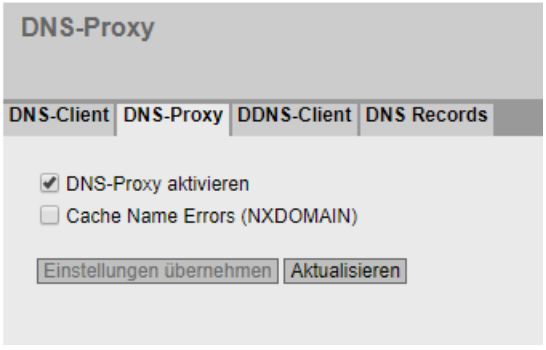
- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen

- **Adresse des DNS-Servers**
  Zeigt die IP-Adresse des DNS-Servers an.
- **Erstellung**
  Zeigt an, ob der DNS-Server manuell konfiguriert oder durch DHCP zugewiesen wurde.

### 5.5.17.2 DNS-Proxy

Das Gerät stellt dem lokalen Netz einen DNS-Server zur Verfügung. Wenn Sie in der lokalen Anwendung die IP-Adresse des Gerätes als DNS-Server eintragen, beantwortet das Gerät DNS-Anfragen aus seinem Cache.

Wenn das Gerät die IP-Adresse zu einer Domain-Adresse nicht kennt, leitet es die Anfrage an einen externen DNS-Server weiter. Wie lange das Gerät eine Domain-Adresse im Cache behält, ist abhängig vom adressierten Host. Die DNS-Anfrage an einen externen DNS-Server liefert außer der IP-Adresse auch die Lebensdauer dieser Information zurück.




#### Beschreibung

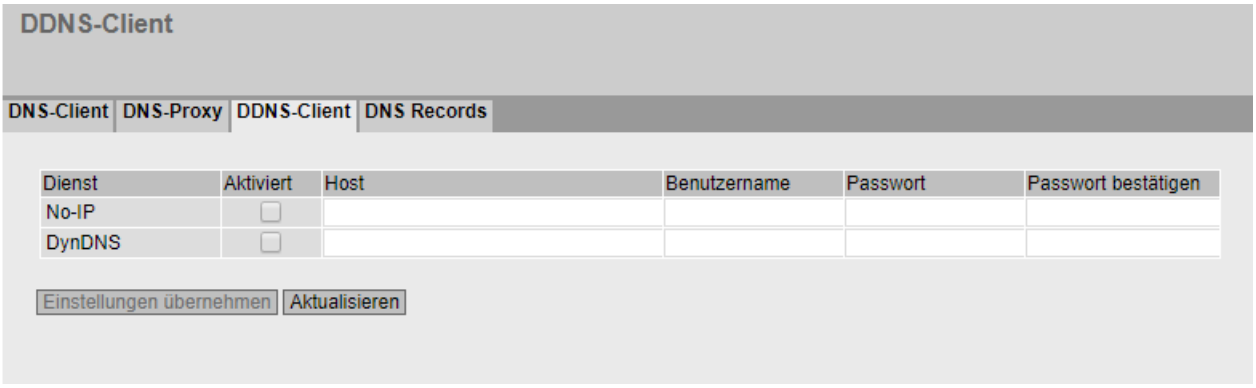
Die Seite enthält folgende Felder:

- **DNS-Proxy aktivieren**
  Aktivieren oder deaktivieren Sie den Proxy des DNS-Servers.
- **Cache Name Errors (NXDOMAIN)**
  Aktivieren oder deaktivieren Sie das Zwischenspeichern von NXDOMAIN-Antworten. Wenn Sie die Option aktivieren, verbleiben auch die Domain-Namen im Cache, die dem DNS-Server unbekannt waren.

### 5.5.17.3 DDNS-Client

Der DDNS (Dynamic Domain Name System) ist ein Internetdienst, der es ermöglicht, einen festen Hostnamen als Pseudonym für eine sich dynamisch ändernde IP-Adresse einzurichten.

Der DDNS-Client synchronisiert die zugewiesene IP-Adresse mit dem im DDNS-Provider registrierten Hostnamen. Damit ist das Gerät immer unter demselben Hostnamen erreichbar.




## Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Dienst**
  Zeigt an, welche Anbieter unterstützt werden.
- **Aktiviert**
  Wenn aktiviert, meldet sich das Gerät an dem DDNS-Server an.
- **Host**
  Tragen Sie den Hostnamen ein, den Sie für das Gerät mit Ihrem DDNS-Anbieter vereinbart haben, z. B. example.no-ip-com.
- **Benutzername**
  Tragen Sie den Benutzernamen ein, mit dem sich das Gerät am DDNS-Server anmeldet.
- **Passwort**
  Tragen Sie das dem Benutzer zugeordnete Passwort ein.
- **Passwort bestätigen**
  Bestätigen Sie das Passwort.

## Vorgehensweise

Voraussetzung:

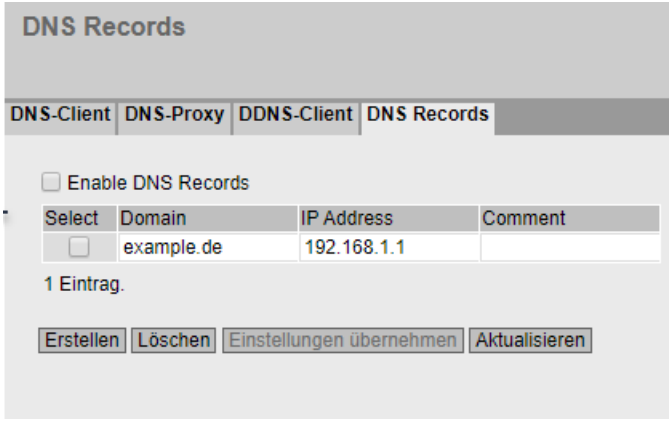
- Benutzernamen und Passwort, dass Sie zur Nutzung des DDNS-Dienstes berechtigt.
- Registrierter Hostname z. B. example.no-ip.com
- Der UDP-Port 53 für DNS ist freigeschaltet und wird nicht bei NAT verwendet.

1. Tragen Sie bei "Host" den Hostnamen ein, den Sie für das Gerät mit Ihrem DDNS-Anbieter vereinbart haben, z. B. example.no-ip-com.
2. Tragen Sie die Login-Daten (Benutzername, Passwort) für den DDNS-Server ein.
3. Aktivieren Sie "Aktiviert". Dieser Hostnamen wird für das Gerät verwendet.
4. Klicken Sie auf "Einstellungen übernehmen".

### 5.5.17.4 DNS-Record

Auf dieser WBM-Seite konfigurieren Sie ein DNS-Adressverzeichnis. Dazu geben Sie die zu einer FQDN zugehörige IPv4-Adresse ein.

Das Gerät prüft bei DNS-Anfragen, ob es einen Eintrag gibt, und wandelt die URL in die entsprechende IPv4-Adresse um.




## Beschreibung

Die Seite enthält folgende Felder:

- **DNS-Records aktivieren**
  Wenn aktiviert, wird das Adressverzeichnis verwendet.

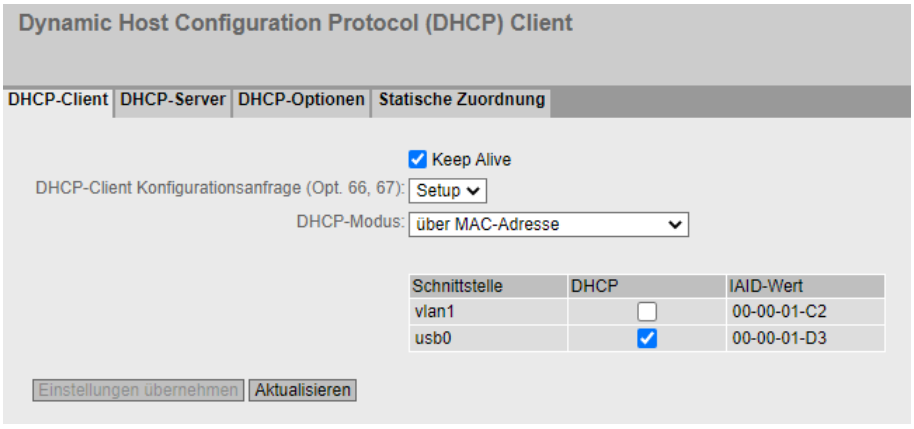
Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Domain**
  Geben Sie den FQDN (Fully Qualified Domain Name) ein.
- **IP-Adresse**
  Geben Sie die zugehörige IPv4-Adresse ein.
- **Kommentar**
  Wenn nötig, geben Sie einen Kommentar ein.

## 5.5.18 DHCPv4

### 5.5.18.1 DHCP-Client

Wenn das Gerät als DHCP-Client konfiguriert ist, startet es eine DHCP-Anfrage. Das Gerät erhält vom DHCP-Server als Antwort eine IPv4-Adresse zugewiesen. Der Server verwaltet einen Adressbereich, aus welchem er IPv4-Adressen vergibt. Es ist auch möglich, den Server so zu konfigurieren, dass der Client auf seine Anfrage immer dieselbe IPv4-Adresse zugewiesen bekommt.



## Beschreibung

Die Seite enthält folgende Felder:

- **Keep-Alive**
  Wenn aktiviert, wird die IP-Adresse bei einem Verbindungsabbruch beibehalten und nicht auf 0.0.0.0 zurückgesetzt. Keep-Alive ist per Default eingeschaltet. Wenn Keep-Alive deaktiviert ist, wird die IP-Adresse bei einem Verbindungsabbruch auf 0.0.0.0 zurückgesetzt.
- **DHCP-Client Konfigurationsanfrage (Opt. 66, 67)**
  Wenn aktiviert, verwendet der DHCP-Client die Optionen dazu, die Konfigurationsdatei (Option 67) vom TFTP-Server (Option 66) herunterzuladen. Nach dem Neustart verwendet das Gerät die Daten aus der Konfigurationsdatei.

| **ACHTUNG** |
| --- |
| **Sicherheitsrisiko - Risiko des unbefugten Zugriffs und/oder Missbrauchs**<br><br>Die Funktion kann potentiell dazu verwendet werden, die Funktionalität des Geräts zu verändern und damit den Ausfall des Datenverkehrs verursachen. Benutzer mit bösartigen Absichten können das Gerät veranlassen, eine manipulierte Konfigurationsdatei zu laden, um die Konfigration zu ihren Gunsten zu verändern.<br><br>Um unbefugten Zugriff und/oder Missbrauch zu verhindern, deaktivieren Sie die Funktion, wenn Sie sie nicht nutzen (**Off**).<br><br>Bei einem Gerät mit Default-Einstellung (**Setup**) wird nach der ersten Anmeldung mit dem voreingestellten Benutzerprofil **admin** und der Vergabe eines neuen Passworts keine Konfigurationsdatei mehr vom DHCP-Server geladen, selbst wenn in den DHCP-Anfragen des DHCP-Clients die Optionen 66 und 67 noch enthalten sind. |

**Hinweis**

**Konfigurationsdatei und Firmware-Version**

Die Konfigurationsdatei dient zum Abspeichern und Einlesen von Konfigurationsdaten innerhalb einer Firmware-Version z. B. 4.3. Konfigurationsdateien, die mit einer Firmware-Version <4.2 erstellt wurden, können nicht auf einem Gerät mit einer Firmware-Version 4.3 eingelesen werden.

  - Setup
    Default-Einstellung. Die Funktion ist abhängig vom Status des Geräts.
    Im Lieferzustand und nach dem Zurücksetzen auf Default-Einstellungen verhält sich die Funktion wie bei der Option On und die Funktion ist für alle DHCP-Client-Schnittstellen aktiviert.
    Die folgenden Ereignisse lösen eine Statusänderung des Geräts aus: Die erste Anmeldung mit dem voreingestellten Benutzerprofil admin und die damit verbundene Vergabe eines neuen Passworts oder das Laden einer Konfigurationsdatei. Danach befindet sich das Gerät im sicheren Betriebszustand und die Funktion verhält sich wie bei der Option Off: die Option ist für alle DHCP-Client-Schnittstellen deaktiviert.
    Der Status ändert sich automatisch.
  - On
    Die Funktion ist aktiviert. Der DHCP-Client fordert bei der nächsten DHCP-Anfrage eine Konfigurationsdatei an.

  - Off
    Die Funktion ist deaktiviert. Der DHCP-Client fordert keine Konfigurationsdatei an.

- **DHCP-Modus**
  Legen Sie fest, mit welcher Art von Kennung sich der DHCP-Client bei seinem DHCP-Server anmeldet:

  - über MAC-Adresse
    Die Identifikation läuft über die MAC-Adresse ab.
  - über DHCP-Client-ID
    Die Identifikation läuft über eine frei definierte DHCP-Client-ID ab.
  - über Systemnamen
    Die Identifikation läuft über den Systemnamen ab. Ist der Systemname 255 Zeichen lang, dann wird das letzte Zeichen nicht zur Identifikation benutzt.
  - über IAID und DUID
    Damit kann sich der DHCP-Client an DHCP-Servern anmelden, die den Parallelbetrieb von IPv4-und IPv6 unterstützten.
    Die Identifikation läuft über die IAID und die DUID ab und bezeichnet genau eine IP-Schnittstelle des Geräts.
    IAID (Interface Association Identifier): Für jede IP-Schnittstelle wird mindestens eine IAID generiert. Die IAID bleibt bei Neustart des DHCP-Clients unverändert.
    DUID (DHCP Unique Identifier): Identifiziert Server und Clients eindeutig und gilt für alle IP-Schnittstellen des Geräts. Die DUID bleibt bei Neustart unverändert.

**Hinweis**

**DHCP-Modus "über PROFINET-Gerätename"**

Mit der Firmware-Version 5.0 wurde die Einstellung "über PROFINET-Gerätename" entfernt.

Die Tabelle gliedert sich in folgende Spalten:

- **Schnittstelle**
  Schnittstelle, auf die sich die Einstellung bezieht.
- **DHCP**
  Aktivieren oder deaktivieren Sie den DHCP-Client für die entsprechende Schnittstelle.
- **IAID-Wert**
  Wert mit dem sich die Schnittstelle (DHCP-Client) am DHCP-Server identifiziert.

## Vorgehensweise

Gehen Sie folgendermaßen vor, um die IP-Adresse via DHCP Client ID zu konfigurieren:

1. Wählen Sie in der Klappliste "DHCP-Modus" die Identifikationsmethode aus.
   Wenn Sie den DHCP-Modus "über DHCP-Client-ID" auswählen, erscheint ein Eingabefeld. Geben Sie in das aktivierte Eingabefeld "DHCP-Client-ID" eine Zeichenkette zur Identifikation des Geräts ein. Diese wird dann vom DHCP-Server ausgewertet.
2. Wählen Sie die Option "DHCP-Client Konfigurationsanfrage (Opt. 66, 67)", wenn der DHCP-Client die Optionen 66 und 67 dazu verwenden soll, eine Konfigurationsdatei herunterzuladen und diese dann zu aktivieren.

3. Aktivieren Sie die Option "DHCP" in der Tabelle.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

**Hinweis**

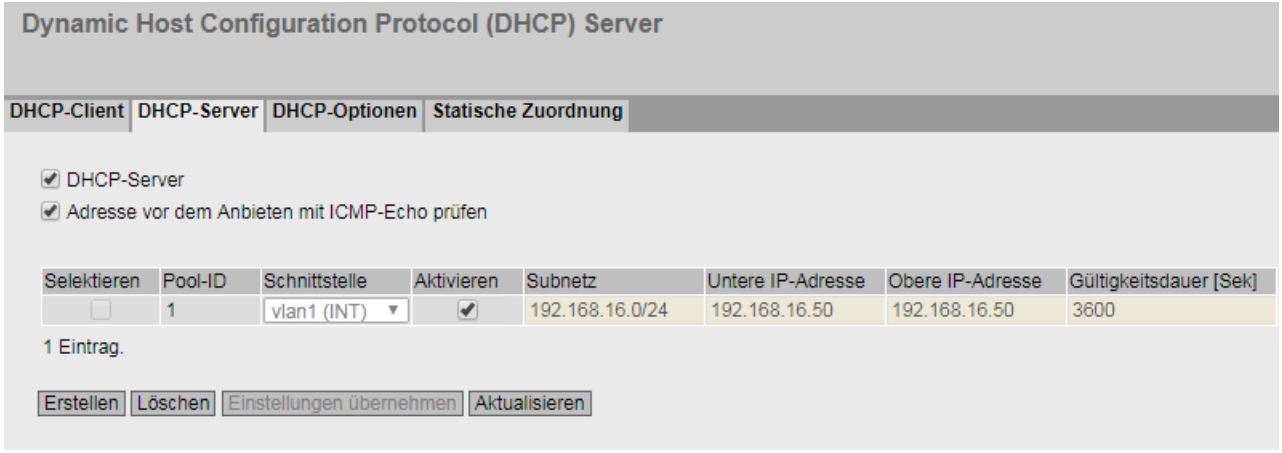
Wird eine Konfigurationsdatei heruntergeladen, so kann dies einen Neustart des Systems auslösen. Wenn sich die aktuell laufende Konfiguration und die Konfiguration in der heruntergeladenen Konfigurationsdatei unterscheiden, startet das System neu.

Achten Sie darauf, dass in dieser Konfigurationsdatei die Option "DHCP-Client Konfigurationsanfrage (Opt. 66, 67)" nicht mehr gesetzt ist.

### 5.5.18.2 DHCP-Server

Das Gerät können Sie als DHCP-Server betreiben. Damit ist es möglich, den angeschlossenen Geräten automatisch IP-Adressen zuzuweisen. Die IP-Adressen werden entweder dynamisch aus einem von Ihnen vergebenen Adressband (Pool) verteilt oder es wird eine bestimmte IP-Adresse einem bestimmten Gerät zugewiesen.

Auf dieser Seite legen Sie das Adressband fest, aus dem das Gerät eine beliebige IP-Adresse erhält. Die statische Zuordnung der IP-Adressen konfigurieren Sie unter "Statische Zuordnung".




## Voraussetzung

- Die angeschlossenen Geräte sind so konfiguriert, dass sie die IP-Adresse von einem DHCP-Server beziehen.

## Beschreibung

Die Seite enthält folgende Felder:

- **DHCP-Server**
  Aktivieren oder deaktivieren Sie den DHCP-Server auf dem Gerät**.**

  **Hinweis**

  Damit keine Konflikte mit IPv4-Adressen entstehen, darf im Netzwerk nur ein Gerät als DHCP-Server konfiguriert sein.

- **Adresse vor dem Anbieten mit ICMP-Echo prüfen**
  Wenn aktiviert, prüft der DHCP-Server, ob die IP-Adresse schon vergeben ist. Dazu sendet der DHCP-Server ICMP-Echomeldungen (ping) an die IPv4-Adresse. Wenn keine Antwort zurückkommt, kann der DHCP-Server die IPv4-Adresse vergeben.
  Bei statischen Zuordnungen wird diese Prüfung nicht durchgeführt.

  **Hinweis**

  Wenn es in Ihrem Netzwerk Geräte gibt, bei denen der Echo-Dienst standardmäßig deaktiviert ist, kann es zu Konflikten bei den IPv4-Adressen kommen. Um dies zu vermeiden, vergeben Sie diesen Geräten eine IPv4-Adresse, die außerhalb des IPv4-Adressbands liegt.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Pool-ID**
  Zeigt die Nummer des IPv4-Adressbands an. Wenn Sie auf die Schaltfläche "Erstellen" klicken, wird eine neue Zeile mit einer eindeutigen Nummer (Pool-ID) angelegt.
- **Schnittstelle**
  Wählen Sie eine VLAN-IP-Schnittstelle aus. Über diese Schnittstelle werden die IPv4-Adressen dynamisch vergeben.
  Voraussetzung für die Vergabe ist, dass die IPv4-Adresse der Schnittstelle im Subnetz des IPv4-Adressbands liegt. Wenn das nicht der Fall ist, vergibt die Schnittstelle keine IPv4-Adressen.
- **Aktivieren**
  Legen Sie fest, ob dieses IPv4-Adressband verwendet wird.

  **Hinweis**

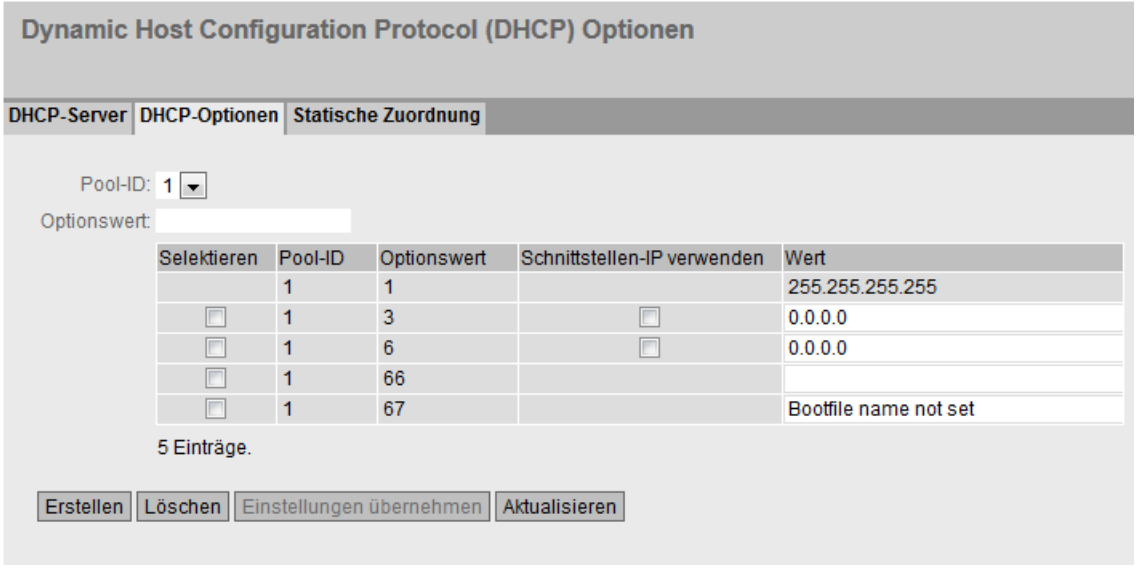
  Wenn Sie das IPv4-Adressband aktivieren, werden dessen Einstellungen in diesem sowie in den weiteren DHCP-Registern ausgegraut und sind nicht mehr editierbar.

- **Subnetz**
  Tragen Sie den Netzadressbereich ein, der den Geräten zugewiesen wird. Verwenden Sie die CIDR-Schreibweise.
- **Untere IP-Adresse**
  Tragen Sie die IPv4-Adresse ein, die den Anfang des dynamischen IPv4-Adressbands festlegt. Die IPv4-Adresse muss innerhalb des Netzadressbereichs liegen, den Sie bei "Subnetz" konfiguriert haben.

- **Obere IP-Adresse**
  Tragen Sie die IPv4-Adresse ein, die das Ende des dynamischen IPv4-Adressbands festlegt. Die IPv4-Adresse muss innerhalb des Netzadressbereichs liegen, den Sie bei "Subnetz" konfiguriert haben.
- **Gültigkeitsdauer [Sek]**
  Legen Sie fest, für wie viele Sekunden die vergebene IPv4-Adresse gültig bleibt. Nachdem die Gültigkeitsdauer zur Hälfte abgelaufen ist, kann der DHCP-Client die vergebene IPv4-Adresse verlängern. Nach Ablauf der gesamten Zeitdauer muss der DHCP-Client eine neue IPv4-Adresse anfordern.

### 5.5.18.3 DHCP-Optionen

Auf dieser Seite legen Sie fest, welche DHCP-Optionen der DHCP-Server unterstützt. Die verschiedenen DHCP-Optionen sind im RFC 2132 definiert.




## Beschreibung

Die Seite enthält folgende Felder:

- **Pool-ID**
  Wählen Sie das gewünschte Adressband aus.
- **Optionswert**
  Geben Sie die Nummer der gewünschten DHCP-Option ein.

---

**Hinweis**

**Unterstützte DHCP-Optionen**

Die DHCP-Optionen 1, 2, 3, 4, 5, 6, 42, 66, 67 werden unterstützt.

---

Die DHCP-Optionen 1, 3, 6, 66 und 67 werden automatisch beim Erstellen des IPv4-Adressbands angelegt. Mit Ausnahme der Option 1 sind die Optionen löschbar.

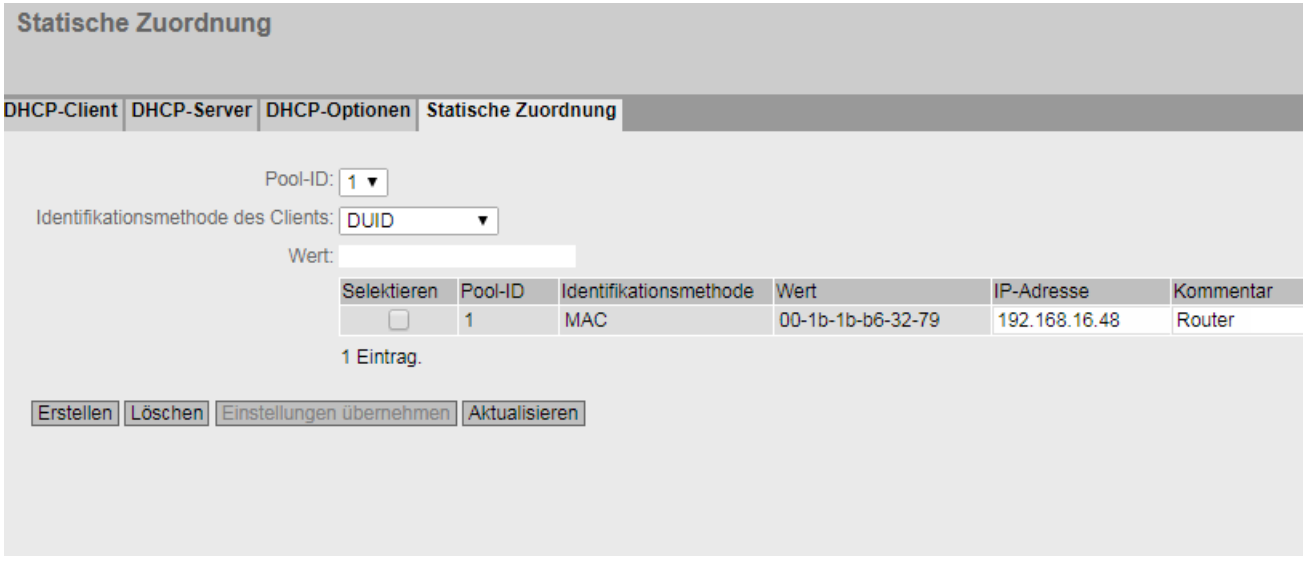
Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen
- **Pool-ID**
  Zeigt die Nummer des Adressbands an.
- **Optionswert**
  Zeigt die Nummer der DHCP-Option an.
- **Schnittstellen-IP verwenden**
  Legen Sie fest, ob die interne IP-Adresse des Geräts verwendet wird oder nicht.
- **Wert**
  Geben Sie den DHCP-Parameter ein, der dem DHCP-Client übergeben wird. Der Inhalt ist abhängig von der DHCP-Option.

| **Wert** | **Optionsname** | | |
|---|---|---|---|
| 1 | Subnetzmaske | Die Subnetzmaske wird automatisch eingetragen. | Option nicht löschbar. |
| 2 | Offset-Zeit | Offset-Zeit zu der koordinierten Weltzeit UTC. | Geben Sie die Offset-Zeit in Sekunden im Hexadezimal-Format an. |
| 3 | Router | Die IPv4-Adresse für Router im Subnetz des DHCP-Clients. Wenn das Gerät selbst der Router ist, wird die IPv4-Adresse der Schnittstelle verwendet. | Sie können mehrere IPv4-Adressen durch Komma getrennt angeben. |
| 4 | Zeitserver | Die IPv4-Adresse des Zeitservers, die dem DHCP-Client zur Verfügung steht . | |
| 5 | Nameserver | Die IPv4-Adresse des Nameservers, die DHCP-Client zur Verfügung steht. | |
| 6 | DNS-Server | Die IPv4-Adresse des DNS-Servers, die dem DHCP-Client zur Verfügung steht.<br>Wenn das Gerät selbst der DNS-Server ist, wird die IPv4-Adresse der Schnittstelle verwendet. | |
| 42 | NTP-Server | Die IPv4-Adresse des NTP-Servers, die dem DHCP-Client zur Verfügung stehen. | |
| 66 | TFTP-Server | Die IPv4-Adresse oder der Hostnamen des TFTP-Servers, die dem DHCP-Client zur Verfügung steht. | Geben Sie die Adresse des TFTP-Servers an. |
| 67 | Namen der Bootdatei | Der Namen der Bootdatei, die der Client vom TFTP-Server herunterlädt. | Geben Sie den Namen der Bootdatei im String-Format an. |

### 5.5.18.4 Statische Zuordnung

Auf dieser Seite legen Sie fest, dass bestimmten Geräten eine bestimmte IP-Adresse zugewiesen wird. Die Adresszuordnung erfolgt anhand der MAC-Adresse, anhand der Client-ID oder anhand der DUID.




## Beschreibung

Die Seite enthält folgende Felder:

- **Pool-ID**
  Wählen Sie das gewünschte Adressband aus.
- **Identifikationsmethode des Clients**
  Wählen Sie die Methode, nach der ein Client identifiziert wird.
  - Ethernet MAC
    Die Identifikation läuft über die MAC-Adresse ab. Tragen Sie bei "Wert" die MAC-Adresse ein. Die MAC-Adresse besteht aus sechs Bytes, die, durch Bindestriche getrennt, hexadezimal notiert werden, z. B. 00-ab-1d-df-b4-1d.
  - Client-ID
    Die Identifikation läuft über eine frei definierte DHCP-Client-ID ab. Tragen Sie bei "Wert" die gewünschte Bezeichnung ein.
  - DUID
    Die Identifikation läuft über DUID und IAID ab. Tragen Sie bei "Wert" die gewünschte Bezeichnung ein, z. B. 00-00-01-C2-00-01-00-01-00-00-00-72-00-1B-1B-B6-32-9D.
- **Wert**
  Tragen Sie den gewünschten Wert ein. Die Eingabe ist abhängig von der gewählten Identifikationsmethode des Clients.

**Hinweis**

Maximal sind 128 Einträge möglich.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Pool-ID**
  Zeigt die Nummer des Adressbands an.
- **Identifikationsmethode**
  Zeigt an, mit welcher Methode sich der Client am DHCP-Server identifiziert.
- **Wert**
  Zeigt die MAC-Adresse, die Client-ID oder DUID des Clients an.
- **IP-Adresse**
  Legen Sie die IPv4-Adresse fest, die dem Client zugewiesen wird. Die IPv4-Adresse muss innerhalb des Adressbands liegen.
- **Kommentar**
  Geben Sie eine Beschreibung für die Adresszuordnung ein.
  Maximal sind 32 Zeichen möglich.

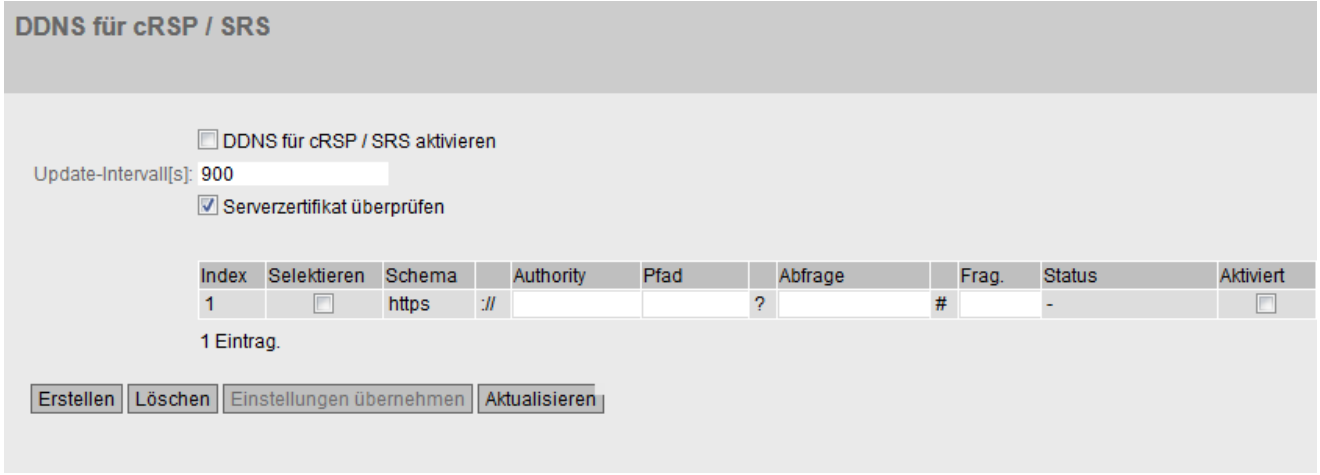
## 5.5.19 cRSP / SRS

**Hinweis**

Common Remote Service Platform (cRSP) / Siemens Remote Service (SRS) ist eine Fernwartungsplattform, über die der Fernwartungszugriff durchgeführt wird.

Zur Nutzung der Plattform sind zusätzliche Serviceverträge notwendig und Randbedingungen zu beachten. Bei Interesse an cRSP / SRS wenden Sie sich an Ihren Siemens-Ansprechpartner vor Ort und besuchen Sie folgende Webseite (https://support.industry.siemens.com/cs/de/de/sc/2281).

Auf dieser Seite konfigurieren Sie die Zugangsdaten für SRS / cRSP nach der URI-Syntax. Der Uniform Resource Identifier (URI) ist in der RFC 3986 definiert.



## Beschreibung

Die Seite enthält folgende Felder:

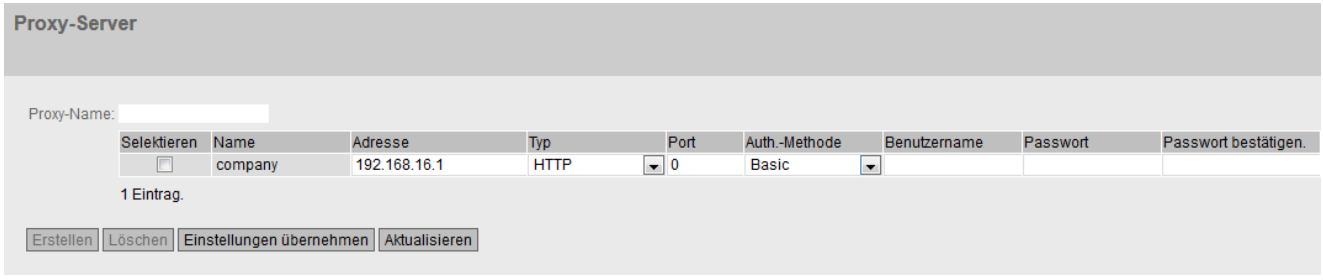
- **DDNS für cRSP / SRS aktivieren**
  Aktivieren oder deaktivieren Sie die Nutzung von cRSP / SRS.
- **Update-Intervall**
  Geben Sie die Zeitspanne ein.
- **Serverzertifikat überprüfen**
  Wenn aktiviert, überprüft das Gerät das empfangene Serverzertifikat auf Gültigkeit.

Die Tabelle gliedert sich in folgende Spalten:

- **Index**
  Die Nummer des Eintrags.
- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Schema**
  Identifiziert die Zugriffsmethode und den Ressourcentyp.
  https: Gesicherter Zugriff auf eine Webseite.
- **Authority**
  Enthält die Adresse des Zielservers
- **Pfad**
  Enthält den Zielpfad zur Ressource. Der Zielpfad kann einem Verzeichnisnamen oder Dateinamen entsprechen.
- **Abfrage**
  Eine Anfrage kann Parameterwerte für eine Anwendung enthalten.
  - WAN_IP (Schlüsselwort): Ersetzt WAN_IP durch die aktuelle externe IP-Adresse des Geräts an den Zielserver.
- **Frag**.
  Adressiert lokale Teile der Ressource, z. B. das Anker-Attribut einer Webseite.
- **Status**
  Zeigt den Status des letzten cRSP / SRS-Zugriffs des Eintrags an.
- **Aktiviert**
  Wenn aktiviert, wird dieser Eintrag verwendet.

## 5.5.20 Proxy-Server

Auf dieser WBM-Seite konfigurieren Sie den Proxy-Server, der von verschiedenen Komponenten verwendet wird, z. B. SINEMA RC.




### Beschreibung

- **Proxy-Name**
  Tragen Sie einen Namen für den Proxy-Server ein.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Name**
  Zeigt den Namen des Proxy-Servers an.
- **Adresse**
  Tragen Sie die IPv4-Adresse des Proxy-Servers ein.
- **Typ**
  Legen Sie die Art des Proxy-Servers fest.
  - HTTP: Proxy-Server nur für Zugriffe über HTTP.
  - SOCKS: Universeller Proxy-Server
- **Port**
  Geben Sie den Port ein, auf dem der Proxydienst läuft.
- **Auth.-Methode**
  Legen Sie die Authentifizierungsmethode fest.
  - None
    Ohne Authentifizierung
  - Basic
    Standardauthentifizierung. Benutzernamen und Passwort werden unverschlüsselt gesendet.
  - NTLM (NT LAN Manager)
    Authentifizierung nach NTLM Standard (Windows-Benutzeranmeldung)
- **Benutzername**
  Geben Sie den Benutzernamen für den Zugang zum Proxy-Server ein.

- **Passwort**
  Geben Sie das Passwort für den Zugang zum Proxy-Server ein.
- **Passwort bestätigen**
  Geben Sie nochmals das Passwort ein, um es zu bestätigen.

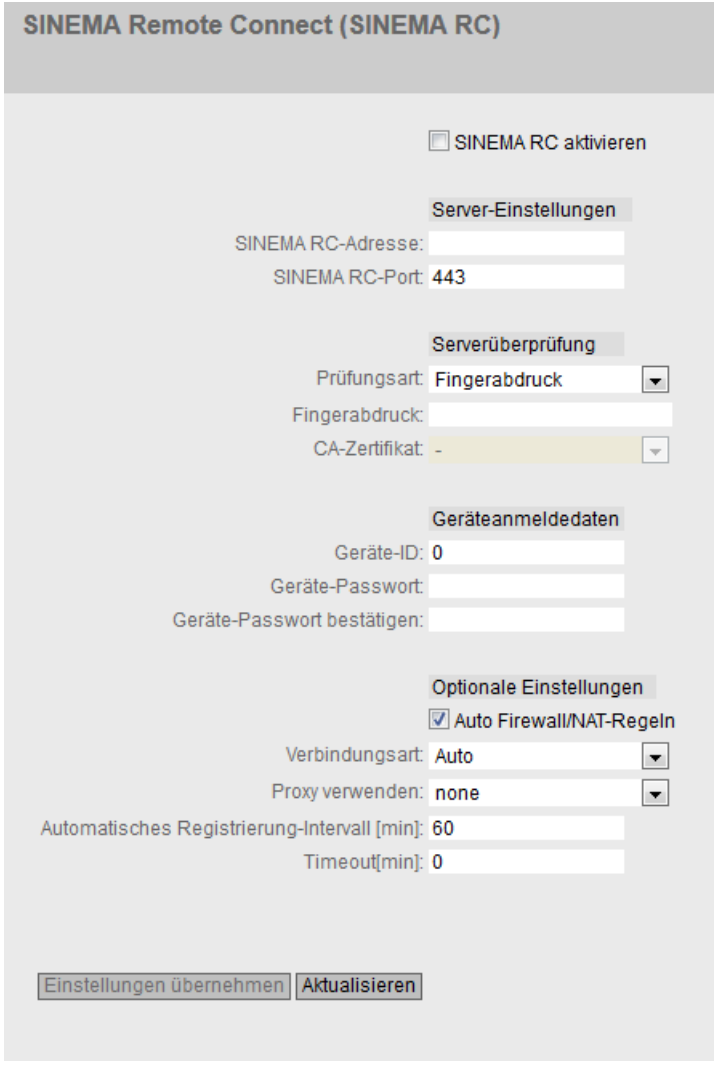
## 5.5.21 SINEMA RC

~~M812~~

Auf dieser WBM-Seite konfigurieren Sie den Zugriff zum SINEMA RC-Server.

**Hinweis**

Diese Funktion ist nur mit KEY PLUG (Seite 54) nutzbar.



## Beschreibung

Die Seite enthält Folgendes:

- **SINEMA RC aktivieren**
  - Aktiviert:
    Eine Verbindung zum konfigurierten SINEMA RC-Server wird aufgebaut. Die Felder sind nicht editierbar.
  - Deaktiviert:
    Die Felder lassen sich editieren. Eine eventuell bestehende Verbindung wird abgebaut.

**Bereich "Server-Einstellungen"**

- **SINEMA RC-Adresse**
  Geben Sie die IPv4-Adresse oder den FQDN (Fully Qualified Domain Name) des SINEMA RC-Servers ein.
- **SINEMA RC-Port**
  Geben Sie den Port ein, über den der SINEMA RC-Servers erreichbar ist.

**Bereich "Serverüberprüfung"**

- **Prüfungsart**
  - Fingerabdruck: Die Identität des Servers wird über den Fingerabdruck verifiziert.
  - CA-Zertifikat: Die Identität des Servers wird über das CA-Zertifikat verifiziert
- **Fingerabdruck**
  Nur bei der Einstellung "Fingerabdruck" notwendig. Geben Sie den Fingerabdruck des Geräts ein. Der Fingerabdruck wird bei der Inbetriebnahme des SINEMA RC-Servers vergeben. Anhand des Fingerabdrucks überprüft das Gerät, ob es sich den korrekten SINEMA RC-Servers handelt. Weiterführende Informationen dazu finden Sie in der Betriebsanleitung zum SINEMA RC-Server.
- **CA-Zertifikat**
  Nur bei der Einstellung "CA-Zertifikat" notwendig. Wählen Sie das CA-Zertifikat des Servers aus, das zur Signierung des Serverzertifikats verwendet wird. Nur geladene CA-Zertifikate sind auswählbar.

**Bereich "Geräteanmeldedaten"**

- **Geräte-ID**
  Geben Sie die Geräte-ID ein. Die Geräte-ID wird beim Konfigurieren des Geräts am SINEMA RC-Server vergeben. Weiterführende Informationen dazu finden Sie in der Betriebsanleitung zum SINEMA RC-Server.
- **Geräte-Passwort**
  Geben Sie das Passwort ein, mit dem sich das Gerät am SINEMA RC-Server anmeldet. Das Passwort wird beim Konfigurieren des Geräts am SINEMA RC-Server vergeben. Weiterführende Informationen dazu finden Sie in der Betriebsanleitung zum SINEMA RC-Server.
- **Geräte-Passwort bestätigen**
  Wiederholen Sie das Passwort.

**Bereich "Optionale Einstellungen"**

- **Auto Firewall/NAT-Regeln**
  - Aktiviert
    Für die VPN-Verbindung werden automatisch die Firewall und NAT-Regeln angelegt. Dabei werden die Verbindungen, die zwischen den projektierten exportierten Subnetzen und den Subnetzen, die über den SINEMA RC-Server erreichbar sind, zugelassen. Die NAT-Einstellungen werden wie im SINEMA RC-Server projektiert umgesetzt.
    Unter "Security > Firewall > vordefinierte IPv4-Regeln" können Sie SINEMA RC den Zugriff auf bestimmte Dienste des Geräts erlauben.
  - Deaktiviert
    Sie müssen selbst die Firewall und NAT-Regeln anlegen.
- **Verbindungsart**
  Legen Sie die Art der VPN-Verbindung fest. Weitere Informationen dazu finden Sie im Kapitel "VPN-Verbindungsaufbau".
  - Auto
    Das Gerät übernimmt die Einstellungen des SINEMA RC Server. Die Einstellungen auf dem SINEMA RC Server konfigurieren Sie unter "Fernverbindungen > Geräte". Weiterführende Informationen hierzu finden Sie in der Betriebsanleitung "SINEMA RC Server".

  Bei folgenden Verbindungsarten werden die Einstellungen des SINEMA RC Servers nicht verwendet.
  - Permanent
    Das Gerät baut eine VPN-Verbindung zum SINEMA RC-Server. Der VPN-Tunnel wird permanent aufrechterhalten.
  - Weck-SMS (nur bei M87x / MUM85x)
    Wenn das Gerät eine Befehl-SMS (Wake-up SMS) erhält, versucht das Gerät zum SINEMA RC-Server eine VPN-Verbindung aufzubauen. Vorausgesetzt unter "System > SMS > Befehl-SMS" ist festgelegt, von wem eine Befehl-SMS der Klasse "System" akzeptiert wird.
  - Digitaler Eingang
    Beim Eintreten des Ereignisses "Digital In" versucht das Gerät zum SINEMA RC-Server eine VPN-Verbindung aufzubauen.
    Vorausgesetzt, dass das Ereignis "Digitaler Eingang" an die VPN-Verbindung weitergegeben wird. Dazu aktivieren Sie unter "System > Ereignisse > Konfiguration" beim Ereignis "Digitaler Eingang" "VPN-Tunnel".
  - Digitaler Eingang & Weck-SMS (nur bei M87x /MUM 85x)
    Wenn das Ereignis "Digitaler Eingang" eintritt oder wenn das Gerät eine Befehl-SMS erhält, versucht das Gerät eine VPN-Verbindung zum SINEMA RC-Server aufzubauen
  - TCP event
    Wenn das ankommende TCP-Paket konforme Daten enthält, versucht das Gerät zum SINEMA RC-Server eine VPN-Verbindung aufzubauen. Vorausgesetzt unter "System > TCP-Ereignis" ist das Ereignis "VPN" aktiviert.
  - Conn. Check Action
    Wenn die Aktionen "VPN Reset" oder "VPN enable" ausgelöst werden, versucht das Gerät zum SINEMA RC-Server eine VPN-Verbindung aufzubauen. Dazu konfigurieren Sie unter "System > Connection Check" die entsprechende Aktion.

  - GPS (Nur bei MUM85x)
    Wenn die Aktion "SINEMA RC (all) enable" ausgelöst wird, versucht das Gerät zum SINEMA RC-Server eine VPN-Verbindung aufzubauen. Dazu konfigurieren Sie unter "System > GPS > Geofencing" die entsprechende Aktion.
  - All
    Das Gerät verwendet alle Verbindungsarten. Ausgenommen davon ist "AUTO".

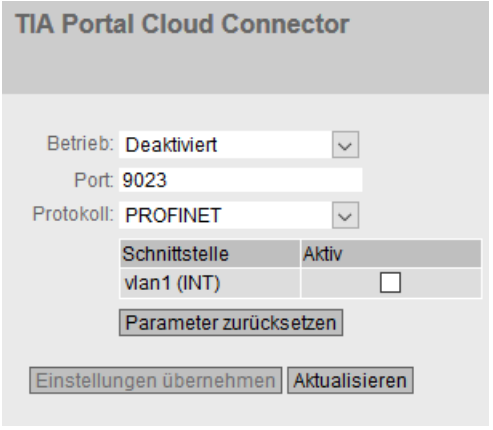
- **Proxy verwenden**
  Legen Sie fest, ob Verbindung zu dem definierten SINEMA RC-Server über einen Proxy-Server aufgebaut wird. Es sind nur die Proxy-Server auswählbar, die Sie unter "System > Proxy Server" konfiguriert haben.
- **Automatisches Registrierung-Intervall [min]**
  Geben Sie die Zeitspanne in Minuten an, nach der Anfragen an den SINEMA RC Server gesendet werden. Mit dieser Anfrage prüft das Gerät, ob auf dem SINEMA RC Server eine neuere Firmware-Datei vorhanden ist oder ob sich die Verbindungseinstellungen geändert haben. Wenn Sie den Wert 0 eintragen, ist diese Funktion deaktiviert.
- **Timeout [min]**
  Geben Sie die Zeitspanne in Minuten an. Wenn kein Datenaustausch stattfindet, wird nach Ablauf dieser Zeitspanne der VPN-Tunnel automatisch abgebaut.

## 5.5.22 Cloud Connector

Auf dieser WBM-Seite konfigurieren Sie die Parameter für die Kommunikation mit dem TIA Portal Cloud Connector.

**Hinweis**

- Verwenden Sie den im Produkt integrierten "TIA Portal Cloud Connector" über eine VPN-Lösung (z. B. SINEMA RC).
- Um den unbefugten Zugriff von Netzteilnehmer auf den "TIA Portal Cloud Connector Server" zu verhindern, aktivieren Sie unter "Security > Firewall > Vordefinierte IPv4-Regeln" den Eintrag "Cloud Connector".
- Die Funktion können Sie immer nur auf einer Schnittstelle aktivieren.



### Voraussetzung

- Damit die eingehenden Pakete an das Gerät weitergeleitet werden, aktivieren Sie die vordefinierte IPv4-Regel "Cloud Connector".

### Beschreibung

Die Seite enthält Folgendes:

- **Betrieb**
  - Aktiviert
    Aktiviert den integrierten TIA Portal Cloud Connector.
  - Deaktiviert
    Deaktiviert den integrierten TIA Portal Cloud Connector.
  - Bei DI starten
    Das Aktivieren wird über den digitalen Eingang (DI) gesteuert. Vorausgesetzt, unter "System > Ereignisse > Konfiguration" ist beim Ereignis "Digitaler Eingang" "Cloud Connector" aktiviert. Wenn diese Einstellung nicht aktiviert ist, wird das Ereignis nicht an den TIA Portal Cloud Connector weitergegeben.
- **Port**
  Über diesen Port wird die Kommunikation mit dem TIA Portal Cloud Connector aufgebaut.
- **Protokoll**
  Über dieses Protokoll wird auf das Anlagennetzwerk zugegriffen.
  - PROFINET über VLAN
    Die VLAN-Schnittstelle legen Sie in der folgenden Tabelle fest.

  Nur beim M804PB

  - PROFIBUS über die MPI/DP
  - PROFINET-PROFIBUS

Die folgende Tabelle ist nur bei PROFINET notwendig:

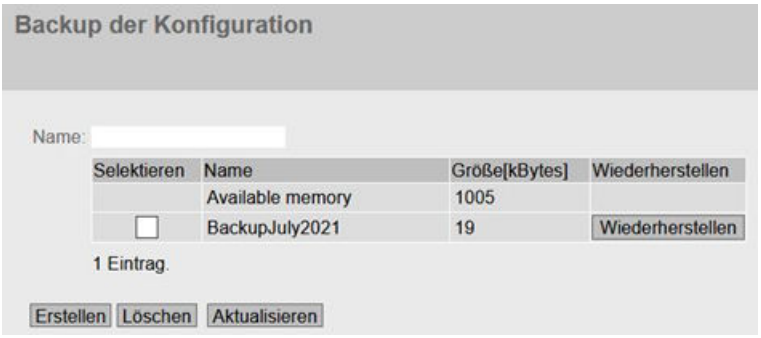
- Schnittstelle
  Nur VLANs mit konfiguriertem Subnetz sind verfügbar.
- Aktiv
  Wenn aktiviert, wird diese VLAN für PROFINET verwendet.
- **Parameter zurücksetzen**
  Setzt die Eigenschaften der Schnittstelle auf die Standardwerte zurück.

## 5.5.23 Backup der Konfiguration

### Backup

Auf dieser Seite können Sie Backups der Konfiguration erstellen und auf dem Gerät speichern. Die Backups werden im Format "ConfigPack" erstellt und umfassen neben der Konfiguration auch Benutzer mit Passwörter, Zertifikate und Favoriten. Diese Backups können Sie direkt vom Gerät wiederherstellen. Nach dem Wiederherstellen startet das Gerät neu. Die maximale Anzahl hängt von der Größe der Backups und vom verfügbaren Speicherplatz ab.

Die erstellten Backups können Sie auf der Seite "System > Laden & Speichern > HTTP/TFTP/SFTP" unter "ConfigPackBackup" im ZIP-Format auf Ihrem Client-PC abspeichern, um sie nachher von dort zu laden. Weiterführende Informationen finden Sie im Kapitel "Laden & Speichern (Seite 191)".




### Beschreibung

Die Seite enthält folgende Felder:

- **Name**
  Geben Sie einen Namen für das Backup ein.

Die Tabelle enthält folgende Spalten:

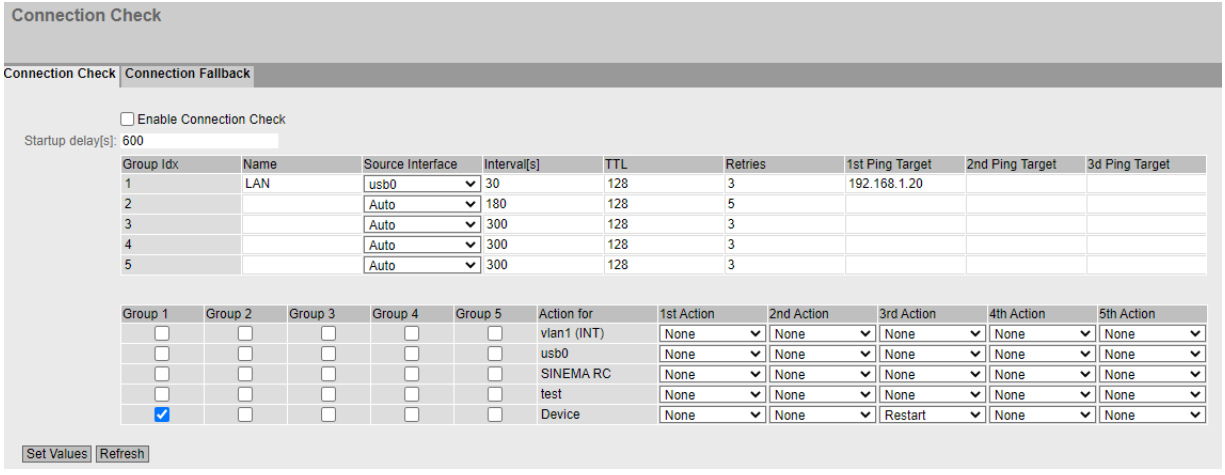
- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Name**
  Zeigt den Namen des Backups an.
- **Größe[kBytes]**
  Die erste Zeile "Available memory" zeigt an, wie viel Speicherplatz für Backups auf dem Gerät verfügbar ist. Wenn Sie ein Backup erstellen, verringert sich der verfügbare Speicherplatz entsprechend.
  In den weiteren Zeilen wird jeweils die Größe des Backups angezeigt.
- **Wiederherstellen**
  Klicken Sie auf die Schaltfläche "Wiederherstellen", um das entsprechende Backup wieder auf das Gerät zu laden.

### Vorgehensweise

1. Geben Sie den gewünschten Namen ein.
2. Klicken Sie auf die Schaltfläche "Erstellen".
   Die aktuelle Konfiguration wird als Konfigurationsbackup gespeichert.
   Das Speichern des Backups kann einige Zeit in Anspruch nehmen. Für das Backup wird eine neue Zeile angelegt. Die Größe des Backups wird angezeigt und von dem verfügbaren Speicherplatz abgezogen.

## 5.5.24 Connection Check

Auf dieser Seite aktivieren Sie einen Ping-Test, der die Verbindungen überwacht. Beim Ping-Test sendet das Gerät in regelmäßigen Abständen (Intervall) ICMP-Echo-Request-Pakete (Ping) an die projektierte Zieladresse. Wenn diese Zieladresse nicht antwortet, versucht das Gerät die Zieladresse erneut zu erreichen. Sind alle Ping-Versuche (Retries) erfolglos, gilt der Ping-Test als fehlgeschlagen bzw. die Gruppe als nicht erreichbar. Wenn die Gruppe nicht erreichbar ist, löst das Gerät auf der gewählten Schnittstelle die konfigurierte Aktion aus. Wenn alle 5 Aktionen abgearbeitet sind oder nach einem Neustart, fängt das Gerät wieder mit der ersten Aktion an.




### Beschreibung

- **Connection Check aktivieren**
  Aktivieren oder deaktivieren Sie den Ping-Test für die Verbindungsüberwachung.
- **Startup delay[s]**
  Legen Sie die Wartezeit nach dem Neustart des Geräts fest, nach der das Gerät einen Ping an die erste Zieladresse sendet.
  Wertebereich: 0 bis 3600 Sekunden, Default-Wert 600 Sekunden. Wenn Sie "0" angeben, wird die Startverzögerung deaktiviert.

Die erste Tabelle enthält folgende Spalten:

- **Gruppen-ID**
  Index der Gruppe
- **Name**
  Geben Sie einen Namen für die Gruppe an. Der Eintrag wird als Spaltenname in der Tabelle "Aktion" angezeigt.
- **Quell-Schnittstelle**
  Legen Sie fest, mit welcher Schnittstelle die Erreichbarkeit der Zieladressen überwacht wird.
- **Intervall**
  Legen Sie fest, mit welchem Zeitabstand die Ping-Tests stattfinden.
- **TTL (Time to live)**
  Geben Sie den TTL-Wert an.
- **Wiederholungen**
  Legen Sie fest, wie oft der Ping-Versuch wiederholt wird.
  Der Zeitabstand bei den Ping-Versuchen beträgt 100 ms. Bei einer hohen Anzahl von Ping-Versuchen kann das zu einem Zeitverzug führen.
  Wenn keine der konfigurierten Adressen antwortet, wird der Ping-Test als fehlgeschlagen (Fehler) gewertet. In der Tabelle "Aktion" legen Sie fest, ob eine bestimmte Aktion ausgeführt wird.
- **1. - 3. Ping-Ziel**
  Geben Sie die Zieladresse an, die als Referenz für die Erreichbarkeit verwendet werden.

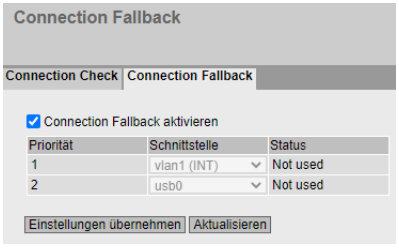
Die zweite Tabelle enthält folgende Spalten:

- **Gruppe 1 - 5**
  Wenn ein Name konfiguriert ist, wird dieser als Spaltennamen verwendet. Weisen Sie die Gruppen der gewünschten Schnittstelle zu. Die Schnittstelle gilt als erreichbar, wenn alle zugewiesenen Gruppen erreichbar sind. Wenn nur eine der Gruppen nicht erreichbar ist, wird auf der gewählten Schnittstelle die konfigurierte Aktion ausgeführt.
- **Aktion auf**
  Zeigt die Schnittstelle, auf der die Aktion ausgeführt wird.
- **1. Aktion - 5. Aktion**
  Folgende Aktionen sind möglich. Die Auswahl ist von der Schnittstelle abhängig, auf der die Aktion ausgeführt wird.
  - Keine (Default)
  - Neustart
    Neustart des Geräts. Nach dem Neustart wartet das Gerät, bis die im Eingabefeld "Startverzögerung[s]" vorgegebene Zeit abgelaufen ist, und sendet dann einen Ping an die erste Zieladresse.
  - Soft-Reset (Nur beim M87x / MUM85x)
    Neustart der Mobilfunk-Engine über die Software
  - Hard-Reset (Nur beim M87x / MUM85x)
    Neustart der Mobilfunk-Engine
  - Fallback (Nur beim M876 / MUM85x / S615 / M826)
    Fällt die Hauptverbindung aus, wird der Datenverkehr über die Ersatzverbindung abgewickelt. Vorausgesetzt die Funktion "Connection Fallback" ist konfiguriert.
  - VPN Reset
    Neustart der VPN-Verbindung
  - VPN enable
    Baut eine VPN-Verbindung zum VPN-Server auf.
  - VPN disable
    Baut die VPN-Verbindung zum VPN-Server ab.
  - Digital Output
    Schaltet den digitalen Ausgang aus.

### 5.5.24.1 Connection Fallback

| M876-x | MUM85x | S615 | M826 |
|---|---|---|---|

Über die Funktion "Connection Fallback" können Sie ein Netzwerk über 2 Schnittstellen anbinden, z. B. das Internet. Durch die Priorität wird festgelegt, ob die Schnittstelle die Hauptverbindung oder die Ersatzverbindung ist. Wenn die Hauptverbindung ausfällt, wird auf die Ersatzverbindung umgeschaltet. Ist die Hauptverbindung wieder verfügbar, wird wieder umgeschaltet. Um die Hauptverbindung zu überwachen, verwenden Sie die Funktion "Connection Check".




### Beschreibung

- **Connection Fallback aktivieren**
  Aktivieren oder deaktivieren Sie die Fallback-Funktion.
- **Priorität**
  - 1 - Hauptverbindung
  - 2 - Ersatzverbindung (Fallback)
- **Schnittstelle**
  Legen Sie die Schnittstelle für die Verbindung fest.
- **Status**
  Zeigt den Status der Verbindung:
  - Active: Der gesamte Datenverkehr wird über die Schnittstelle abgewickelt.
  - Fallback: Wenn die Hauptverbindung ausfällt, wird der Datenverkehr über die Ersatzverbindung abgewickelt.
  - Not used: Die Verbindung wird nicht verwendet.
  - Not reachable: Wenn die Hauptverbindung ausfällt, ändert sich der Status in "Not reachable".

## 5.5.25 TCP-Ereignis

Wenn Sie auf der Seite die Funktion "TCP-Ereignis" aktivieren, wartet das Gerät auf dem eingestellten Port auf eingehende TCP-Pakete. Die Autorisierung erfolgt durch den Abgleich der Benutzerdaten.

Mit TCP-Paketen haben Sie folgende Möglichkeiten:

- Den digitalen Ausgang öffnen oder schließen.
- Eine VPN-Verbindung (OpenVPN, IPsec, SINEMA RC) zu einer Gegenstelle herstellen.

- Nur M87x / MUM85x: Eine SMS versenden.
- Nur MUM85x: Die Funktion "Sleep Mode" auslösen.

Wenn das ankommende TCP-Paket konforme Daten enthält, wird das darin enthaltene Kommando ausgeführt.

**Format des TCP Pakets**

Der Befehl wird in einem TCP-Paket gesendet, das folgendem Format entspricht:

`<Benutzername>#<Passwort>#<command code>#<command string>:`

Der Parameter `<command code>` legt das TCP-Ereignis fest. Folgende Werte sind möglich:

- 105 SMS (Nur beim M87x und MUM85x)
- 106 Digitaler Ausgang
- 107 Sleep Mode (Nur beim MUM85x)
- 108 VPN

In der Befehlszeichenfolge `<command string>` geben Sie die Parameter des TCP-Ereignisses an. Die Parameter werden durch Semikolons getrennt und mit einem Doppelpunkt beendet.

---

**Hinweis**

**Erlaubte Zeichen im Benutzernamen und Passwort**

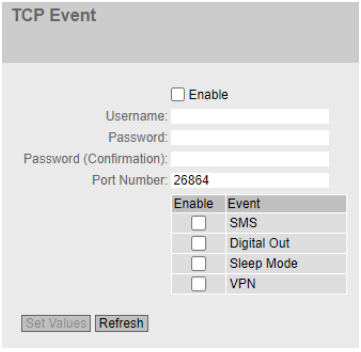
Folgende Zeichen sind erlaubt:

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

Zusätzlich im Passwort erlaubt:

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

---



## Beschreibung

Die Seite enthält Folgendes:

- **Aktivieren**
  Aktivieren oder deaktivieren Sie das Empfangen der TCP-Pakete. Um dies zu protokollieren, aktivieren Sie unter "System > Ereignis" das Ereignis "TCP Ereignis-Log".
- **Benutzername**
  Geben Sie den Benutzernamen zur Prüfung des Empfangs des TCP-Pakets an. Der Benutzernamen und das Passwort werden in das TCP-Paket eingetragen.
- **Passwort**
  Geben Sie das zum Benutzernamen zugehörige Passwort an.
- **Passwort bestätigen**
  Wiederholen Sie das Passwort, um es zu bestätigen.
- **Portnummer**
  Legen Sie fest, an welchem Port das Gerät auf die TCP-Pakete wartet. Voreingestellt ist der Standard-Port 26864.
  Optional können Sie den Standard-Port 26864 oder eine Portnummer im Bereich 1 ... 65535 eintragen.

**Hinweis**

**Reservierte Ports**

Einige Ports sind fest reserviert. Stellen Sie sicher, dass der angegebene Port noch nicht verwendet wird. Die verwendeten Ports finden Sie in der "Liste verfügbarer Dienste (Seite 24)".

Die Tabelle enthält folgende Spalten:

- **Aktivieren**
  Aktivieren oder deaktivieren Sie das Ereignis.
- **Ereignis**
  - SMS (Nur beim M87x und MUM85x)
    Versenden einer SMS:
    `<Benutzername>#<Passwort>#105#01;<phone (phone number)>;<my-SMS-text (sleep)>:`
    Der vorletzte Parameter steht für die Mobilrufnummer und der letzte für die zu versendende Nachricht.
  - Digitaler Ausgang
    Öffnen oder Schließen des digitalen Ausgangs
    Der digitale Ausgang ist standardmäßig und beim Neustart geöffnet (eingeschaltet).
    Wenn ein TCP-Ereignis oder ein konfigurierter Fehler auftritt, wird der digitale Ausgang geschlossen (ausgeschaltet).
    `<Benutzername>#<Passwort>#106#<(1,2)>:`
    Der letzte Parameter gibt die Sequenznummer an: 1 (offen) oder 2 (geschlossen).
    Öffnen:
    `<Benutzername>#<Passwort>#106#1:`
    Schließen:
    `<Benutzername>#<Passwort>#106#2:`
  - Sleep Mode (Nur beim MUM85x)
    Auslösen der Funktion "Sleep Mode":
    `<Benutzername>#<Passwort>#107#1;<Zeit>:`
    Der letzte Parameter gibt die Sleep-Zeit in Minuten an.
    In folgendem Beispiel wird der Sleep Mode für 10 Minuten ausgelöst:
    `<Benutzername>#<Passwort>#107#1;10:`
  - VPN
    Aktivieren der VPN-Verbindung (IPsec, OpenVPN, SINEMA RC).
    `<Benutzername>#<Passwort>#108:`

## 5.5.26 GPS

### 5.5.26.1 Koordinaten

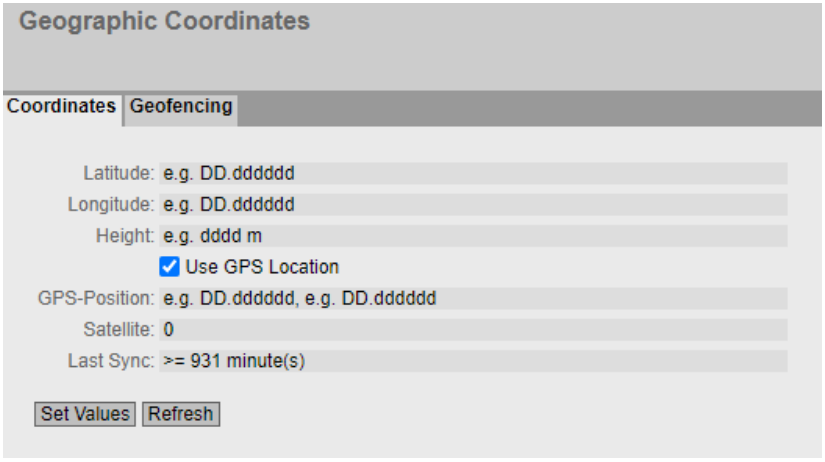
MUM85x

#### Informationen über die geografischen Koordinaten

Im Fenster "Geografische Koordinaten" können Informationen über die geografischen Koordinaten eingetragen werden. Die Parameter der geografischen Koordinaten (Breitengrad, Längengrad und die Höhe über dem Ellipsoid gemäß WGS84) werden direkt in die Eingabefelder im Fenster "Geografische Koordinaten" eingetragen.

**Ermittlung der Koordinaten**

Nutzen Sie zur Ermittlung der geografischen Koordinaten des Geräts eine interaktive Karte oder lassen Sie die Koordinaten vom Gerät auslesen. Die GPS-Koordinaten (Breiten- und Längengrad) müssen in Dezimalgrad angegeben werden.




## Beschreibung

Die Seite enthält folgende Eingabefelder:

- **Geographische Breite**
  Geben Sie den Wert für nördliche oder südliche Breite für den Standort des Gerätes im Format "DD.dddddd" an. Dabei steht "DD" für Breitengrad und "dddddd" für dezimalen Breitengrad. Die südliche Breite wird mit einem führenden Minuszeichen dargestellt.
- **Geographische Länge**
  Geben Sie den Wert für östliche oder westliche Länge für den Standort des Gerätes im Format "DD.dddddd" an. Dabei steht "DD" für Längengrad und "dddddd" für dezimalen Längengrad. Die westliche Länge wird mit einem führenden Minuszeichen dargestellt.
- **Geografische Höhe**
  Geben Sie den Wert für geografische Höhe über oder unter normal Null (Meereshöhe) in Metern an.
  Z.B. 158 m bedeutet, dass sich das Gerät in einer Höhe von 158 m über normal Null befindet. Höhenangaben unterhalb von normal Null (z. B. am Toten Meer) werden mit einem führenden Minuszeichen dargestellt.
- **Use GPS Location**
  Aktiviert oder deaktiviert ein automatisches Auslesen des Standortes des Geräts. Die Genauigkeit der Standortbestimmung liegt bei ca. 10 Meter. Die GPS-Position wird alle 60 Sekunden aktualisiert.
  Wenn Sie die Option aktivieren, dann werden die Eingabefelder für die geografische Breite, Länge und Höhe nicht editierbar.
- **GPS-Position**
  Zeigt die aktuelle GPS-Position im Dezimal-System in der Reihenfolge "Breitengrad, Längengrad, Höhe" an.

- **Satellite**
  Zeigt die Anzahl verfügbarer Satelliten an.
- **Last Sync**
  Zeigt den Status der Synchronisierung an:
  - Synced
    Die Standortbestimmung wurde durchgeführt.
  - Not Synced
    Die Standortbestimmung wurde nicht durchgeführt.
  - >= <Zeit in Minuten>
    Die Zeit in Minuten seit dem letzten Standortbestimmungsversuch.

### Vorgehensweise

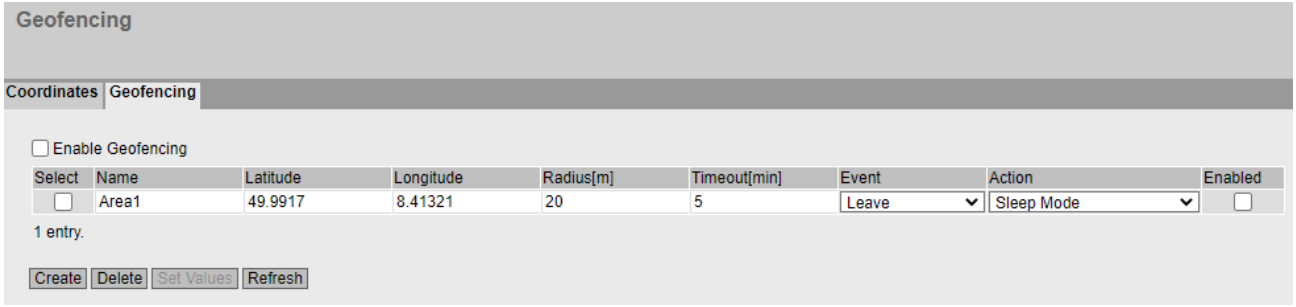
1. Aktivieren Sie die Option "Use GPS Location", um den Standort automatisch zu ermitteln.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

## 5.5.26.2 Geofencing

MUM85x

Mit Geofencing können Sie geografische Bereiche definieren, innerhalb oder außerhalb deren Sie Ihr SCALANCE M-Gerät steuern können.

Auf dieser Seite legen Sie Bereiche fest, in denen bestimmte Ereignisse nach ihrem Eintritt gewünschte Aktionen auf dem Gerät auslösen. Sie können bis zu 20 Bereiche konfigurieren.




### Beschreibung

Die Seite enthält Folgendes:

- Enable Geofencing
  Aktiviert oder deaktiviert das Geofencing.
  Um dies zu protokollieren, aktivieren Sie unter "System > Ereignis" das Ereignis "Geofencing".

Die Tabelle enthält folgende Spalten:

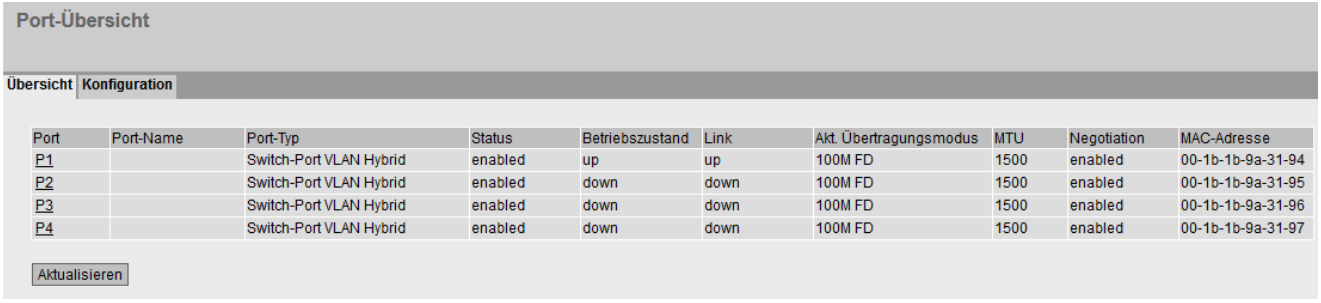
- **Select**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Name**
  Geben Sie den Namen für den abzugrenzenden Bereich an.
  Maximal 64 Zeichen.
- **Latitude**
  Geben Sie die nördliche oder südliche Breite des abzugrenzenden Bereichs im Format "DD.dddddd" an. Dabei steht "DD" für Breitengrad und "dddddd" für dezimalen Breitengrad. Die südliche Breite wird mit einem führenden Minuszeichen dargestellt.
- **Longitude**
  Geben Sie die östliche oder westliche Länge des abzugrenzenden Bereichs im Format "DD.dddddd" an. Dabei steht "DD" für Längengrad und "dddddd" für dezimalen Längengrad. Die westliche Länge wird mit einem führenden Minuszeichen dargestellt.
- **Radius[m]**
  Geben Sie den Radius des abzugrenzenden Bereichs in Meter an.
  Wertebereich: 10 ... 2147483647. Standardwert 20.
- **Timeout[min]**
  Geben Sie die Zeitspanne in Minuten an, nach der die Aktion ausgelöst wird.
  Wertebereich: 1 ... 2147483647. Standardwert 5.
- **Event**
  Wählen Sie ein Ereignis aus, das die Aktion auslöst, wenn es eintritt.
  - Leave
    Das Gerät verlässt den abgegrenzten Bereich.
  - Enter
    Das Gerät betritt den abgegrenzten Bereich.
  - In
    Das Gerät befindet sich im abgegrenzten Bereich.
  - Out
    Das Gerät befindet sich außerhalb des abgegrenzten Bereichs.

- **Action**
  Wählen Sie aus der Klappliste eine Aktion aus, die ausgeführt werden muss, wenn das festgelegte Ereignis eintritt.
  - Event System
    Löst das Ereignis aus, das unter "System > Ereignisse" konfiguriert ist.
  - Restart
    Startet das Gerät neu.
  - Restart Factory
    Setzt das Gerät auf Werkeinstellungen zurück und startet es neu.
  - Fault enable/ Fault disable
    Schaltet die Fehlerkontrolle ein/aus.
  - Digital Output close/ Digital Output open
    Schließt/öffnet den Digitalen Ausgang.
  - Sleep Mode
    Aktiviert den Sleep Mode.
  - Engine HW reset
    Führt den Hard-Reset mit einem Neustart der Mobilfunk-Engine durch.
  - Engine SW reset
    Fuhrt den Neustart der Mobilfunk-Engine über die Software durch.
  - IPsec (all) enable/ IPsec (all) disable
    Baut eine VPN-Verbindung zum IPsec-Server auf/ab.
  - OpenVPN (all) enable/ OpenVPN (all) disable
    Baut eine VPN-Verbindung zum OpenVPN-Server auf/ab.
  - SINEMA RC (all) enable/ SINEMA RC (all) disable
    Baut eine VPN-Verbindung zum SINEMA RC Server auf/ab.
- **Enabled**
  Aktiviert die Ausführung der Aktion zu den gegebenen Bedingungen.

# 5.6 Menü "Schnittstellen"

## 5.6.1 Ethernet

Die Seite zeigt für alle Ports des Geräts die Konfiguration für den Datentransfer an. Sie können auf dieser Seite keine Konfigurationen vornehmen.




### Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

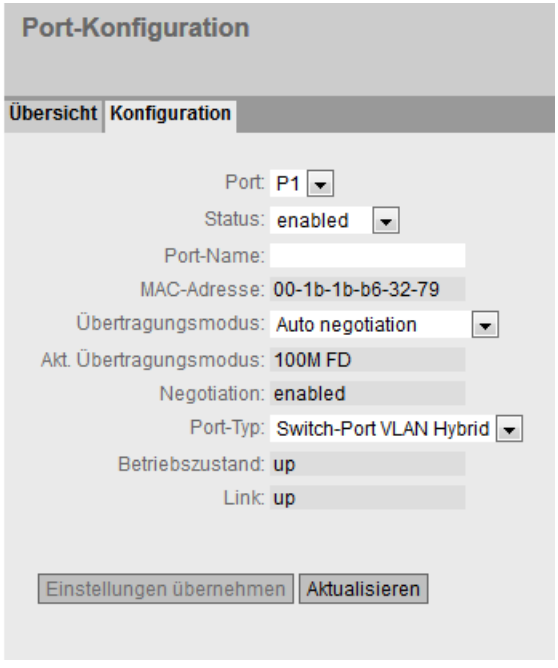
- **Port**
  Zeigt die konfigurierbaren Ports an. Der Eintrag ist ein Link. Wenn Sie auf den Link klicken, wird die entsprechende Konfigurationsseite geöffnet.
- **Port-Name**
  Zeigt den Namen des Ports.
- **Port-Typ** (Nur bei Routing)
  Zeigt den Typ des Ports an. Folgende Typen sind möglich:
  - Switch-Port VLAN Hybrid
  - Switch-Port VLAN Trunk
- **Status**
  Zeigt an, ob der Port ein- oder ausgeschaltet ist. Datenverkehr ist nur über einen eingeschalteten Port möglich.
- **Betriebszustand**
  Zeigt den aktuellen Betriebszustand an. Der Betriebszustand ist vom konfigurierten "Status" und dem "Link" abhängig. Es gibt folgende Möglichkeiten:
  - Up
    Sie haben für den Port den Status "enabled" konfiguriert und der Port hat eine gültige Verbindung zum Netzwerk.
  - Down
    Sie haben für den Port den Status "disabled" oder "Link down" konfiguriert oder der Port hat keine Verbindung.

- **Link**
  Zeigt den Verbindungsstatus zum Netzwerk am. Beim Verbindungsstatus ist Folgendes möglich:
  - Up
    Der Port hat eine gültige Verbindung zum Netzwerk, es wird ein "Link Integrity Signal" empfangen.
  - Down
    Die Verbindung ist unterbrochen, weil beispielsweise das angeschlossene Gerät ausgeschaltet ist.
- **Akt. Übertragungsmodus**
  Zeigt die Übertragungsparameter des Ports an.
- **Negotiation**
  Zeigt an, ob die automatische Konfiguration aktiviert oder deaktiviert ist.
- **MAC-Adresse**
  Zeigt die MAC-Adresse des Ports an.

#### 5.6.1.1 Konfiguration

### Ports konfigurieren

Mit dieser Seite können Sie alle Ports des Geräts konfigurieren.



## Beschreibung

- **Port**
  Wählen Sie in der Klappliste den zu konfigurierenden Port aus.
- **Status**
  Legen Sie fest, ob der Port ein oder ausgeschaltet ist.
  - enabled
    Der Port ist eingeschaltet. Der Datenverkehr ist nur über einen eingeschalteten Port möglich.
  - disabled
    Der Port ist ausgeschaltet, aber die Verbindung besteht noch.

    **Hinweis**

    Schalten Sie nicht genutzte Ports aus.

  - link down
    Der Port ist ausgeschaltet und die Verbindung zum Partnergerät ist abgebaut.
- **Port-Name**
  Tragen Sie hier einen Namen für den Port ein.
- **MAC-Adresse**
  Zeigt die MAC-Adresse des Ports an.
- **Übertragungsmodus**
  Wählen Sie aus dieser Klappliste die Übertragungsgeschwindigkeit und das Übertragungsverfahren des Ports aus.
  Folgende Einstellungen sind möglich:
  - 10 MBit/s  Vollduplex (FD) oder Halbduplex (HD)
  - 100 MBit/s  Vollduplex (FD) oder Halbduplex (HD)
  - Auto negotiation

  Wenn Sie die Betriebsart auf "Auto negotiation" stellen, werden diese Parameter automatisch mit dem angeschlossenen Endgerät oder der Netzkomponente ausgehandelt. Dieses muss sich hierzu ebenfalls in der Betriebsart "Auto negotiation" befinden.

  **Hinweis**

  Damit der Port und der Partner-Port miteinander kommunizieren können, müssen die Einstellungen auf beiden Seiten übereinstimmen.

- **Akt. Übertragungsmodus**
  Zeigt die Übertragungsgeschwindigkeit und das Übertragungsverfahren des Ports an. Die Anzeige ist abhängig von dem eingestellten "Mode Type".
- **Negotiation**
  Zeigt an, ob die automatische Anschlusskonfiguration zum Partner-Port aktiviert oder deaktiviert ist.

- **Port-Typ**
  Wählen Sie aus der Klappliste die Art des Ports aus.
  - Switch-Port VLAN Hybrid
    Der Port sendet getaggte und ungetaggte Telegramme. Er ist nicht automatisch Mitglied eines VLANs.
  - Switch-Port VLAN Trunk
    Der Port sendet nur getaggte Telegramme und ist automatisch Mitglied in allen VLANs.
- **Betriebszustand**
  Zeigt den aktuellen Betriebszustand an. Der Betriebszustand ist vom konfigurierten "Status" und dem "Link" abhängig. Es gibt folgende Möglichkeiten:
  - Up
    Sie haben für den Port den Status "enabled" konfiguriert und der Port hat eine gültige Verbindung zum Netzwerk.
  - Down
    Sie haben für den Port den Status "disabled" oder "Link down" konfiguriert oder der Port hat keine Verbindung.
- **Link**
  Zeigt den physischen Verbindungsstatus zum Netzwerk an. Es gibt folgende Möglichkeiten:
  - Up
    Der Port hat eine gültige Verbindung zum Netzwerk, es wird ein "Link IntegritySignal" empfangen.
  - Down
    Die Verbindung ist unterbrochen, weil z. B. das angeschlossene Gerät ausgeschaltet ist.

## 5.6.2 Mobilfunk

### 5.6.2.1 Allgemein

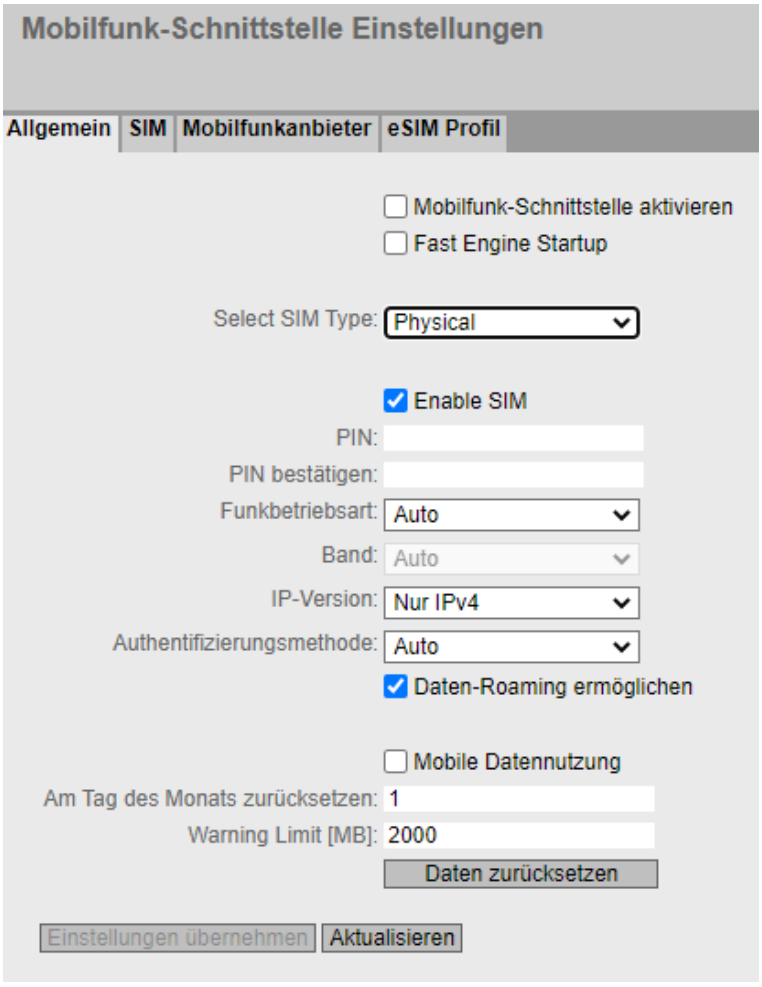
M87x | MUM85x

Für den Zugang zum Mobilfunknetz und zu den Mobilfunkdiensten benötigen Sie Zugangsparameter, die Sie auf dieser Seite angeben. Die Zugangsparameter erhalten Sie von Ihrem Mobilfunkanbieter.

Mit der Funktion "Mobile Datennutzung" können Sie das verbrauchte Datenvolumen kontrollieren.

**Hinweis**

Um eine fehlerhafte Erfassung des verbrauchten Datenvolumens zu vermeiden, verwenden Sie einen Zeitserver.




Vorgenommene Änderungen an der SIM-Karte werden im Ereignis-Log protokolliert. Log-Meldungen für eine austauschbare SIM-Karte beginnen mit "Primary-Modem Physical-SIM: < Log-Meldung>" und für eine eSIM-Karte mit "Primary-Modem e-SIM: < Log-Meldung>".

## Beschreibung

Die Seite enthält Folgendes:

- **Mobilfunk-Schnittstelle aktivieren**
  Aktiviert oder deaktiviert die Mobilfunk-Schnittstelle. Bevor Sie die Mobilfunk-Schnittstelle aktivieren, wählen Sie bei "SIM-Typ auswählen" den gewünschten SIM-Kartentyp aus und aktivieren Sie die SIM-Karte bei "SIM aktivieren".
- **Fast Engine Startup** (Nur beim SCALANCE MUM85x)
  Beschleunigt die Verbindung zum Mobilfunknetz durch Entfallen des Engine-Resets nach dem Starten des Geräts.
  Aktivieren Sie die Option, um die Zeit für den Aufbau der Mobilfunkverbindung zu verringern.

- **Select SIM Type**
  Wählen Sie den Typ der SIM-Karte aus:
  - Physical
    Austauschbare SIM-Karte
  - eSIM (Nur beim SCALANCE MUM85x mit eingebauter eSIM)
    Festverbaute SIM-Karte (embedded SIM)

  **Hinweis**

  Die eSIM-Funktion ist in Geräten SCALANCE MUM85x ab Hardware-Ausgabestand 2 verfügbar. Die Information zum Hardware-Ausgabestand finden Sie unter "Information > I&M (Seite 133)".

- **Enable SIM**
  Aktiviert die SIM-Karte. In V7.2 können Sie nur eine SIM-Karte aktivieren.
- **PIN**
  Persönliche Identifikationsnummer
  Wenn die Mobilfunk-Schnittstelle aktiviert ist, wird die aktuell gültige PIN der SIM-Karte abgefragt.
  Tragen Sie die aktuell gültige PIN für die gewählte SIM-Karte ein. Das Gerät arbeitet auch mit SIM-Karten, die keine PIN erfordern oder bei denen die PIN-Abfrage deaktiviert wurde.

  **Hinweis**

  **Bei Fehleingaben wird die SIM-Karte gesperrt**

  Achten Sie darauf, die PIN korrekt einzugeben. Wenn Sie die PIN dreimal falsch eingeben, wird die SIM-Karte gesperrt.

  Unter "Information > Mobilfunk" können Sie den Status der SIM-Karte überprüfen. Wenn bei "SIM-Status" "PUK erforderlich" angezeigt wird, ist die SIM-Karte gesperrt. Unter "Schnittstellen > Mobilfunk > SIM" können Sie die SIM-Karte wieder entsperren.

- **PIN bestätigen**
  Wiederholen Sie die PIN.

- **Funkbetriebsart**
  Wählen Sie das gewünschte Mobilfunknetz aus. Folgende Optionen stehen zur Auswahl:
  - Auto (nicht beim SCALANCE M874-2)
    Alle Dienste. Das Gerät versucht bevorzugt mit dem schnellsten verfügbaren Mobilfunkverfahren eine Verbindung herzustellen.
  - Nur GSM
    Die Dienste EGPRS und GPRS. Das Gerät ignoriert das UMTS- und LTE-Netz und baut eine Verbindung zu dem GSM-Dienst auf, der vor Ort die höchste Bandbreite zur Verfügung stellt
  - Nur UMTS (nicht beim SCALANCE M874-2)
    Der Dienst UMTS und HSPA. Das Gerät ignoriert die Dienste EGPRS, GPRS und LTE und baut eine Verbindung im UMTS-Netz auf.
  - Nur LTE (nur bei SCALANCE M876-4/MUM85x)
    Der Dienst LTE. Das Gerät ignoriert die Dienste EGPRS, GPRS und UMTS und baut eine Verbindung im LTE-Netz auf.
  - 5 G NR + LTE (NSA) (nur beim SCALANCE MUM85x)
    Die Dienste 5G New Radio (NR) und LTE Non-Standalone Operation (NSA)
  - Nur 5 G NR SA (nur beim SCALANCE MUM85x)
    Der Dienst 5G New Radio (NR) im Standalone-Betrieb (SA)
  - EVDO (nur beim SCALANCE M876-3)
    EVolution, Data-Optimized. Standard für CDMA-basiert Netzwerke.
    Folgende Substandards werden unterstützt:
    - EVDO Hybrid
    - EVDO 1xRTT
    - EVDO HDR - High Data Rate
  - Keine Datenverbindung
    Es besteht keine Datenverbindung. Geeignet, wenn das Gerät nur zum Senden oder Empfangen von SMS verwendet wird.
- **IP-Version**
  Legen Sie fest, welche IP-Version das Gerät unterstützt.
- **Authentifizierungsmethode**
  Wählen Sie das gewünschte Authentifizierungsverfahren.
  - CHAP
    Challenge Handshake Authentication Protocol
    Verschlüsselte Übertragung von Benutzername und Passwort per CHAP.
  - PAP
    Password Authentication Protocol
    Unverschlüsselte Übertragung von Benutzername und Passwort per PAP.
  - Auto
    Benutzername und Passwort werden automatisch mit einem der beiden Verfahren übertragen. CHAP hat die höhere Priorität. Wenn der Kommunikationspartner CHAP nicht unterstützt, werden Benutzername und Passwort per PAP übertragen.
- **Daten-Roaming ermöglichen**
  Wenn aktiviert, meldet sich das Gerät automatisch bei einem verfügbaren Netz an. Vorausgesetzt das festgelegte Netz ist nicht erreichbar.

- **Mobile Datennutzung**
  Wenn aktiviert, wird überwacht, wann der festgelegte Grenzwert erreicht wird. Der Grenzwert, den Sie selbst festlegen, definiert das maximale Datenvolumen pro Monat. Der Verbrauch des Datenvolumens wird unter "Information > Mobilfunk > Datennutzung" angezeigt.
- **Am Tag des Monats zurücksetzen**
  Nicht immer beginnt der Abrechnungszeitraum am Ersten eines Monats, sondern an dem Tag, an dem der Vertrag abgeschlossen wurde.
  Geben Sie den Tag an, an dem der monatliche Abrechnungszeitraum beginnt. An diesem Tag wird das verbrauchte Datenvolumen auf 0 gesetzt.
- **Warnung Limit [ MB]**
  Geben Sie den Grenzwert des monatlichen Datenvolumens ein.
  Zusätzlich können Sie Datenwarnungen erhalten, sobald 75 % und 100 % des festgelegten Datenvolumens erreicht sind. Vorausgesetzt unter "System > Ereignisse > Konfiguration" ist beim Ereignis "Mobile Datennutzung" die gewünschte Art der Benachrichtigung aktiviert.
- **Daten zurücksetzen**
  Löscht die gespeicherten Werte.

### Vorgehen

**Warnmeldungen via SMS erhalten:**

1. Geben Sie bei "Am Tag des Monats zurücksetzen" den Beginn des Abrechnungszeitraums an.
2. Legen Sie bei "Warnung Limit" das Datenvolumen in MB fest.
3. Aktivieren Sie "Mobile Datennutzung" und klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
4. Legen Sie unter "System > SMS > Ereignis-SMS" den Empfänger fest.
   - Geben Sie in das Eingabefeld "Rufnummer" die Telefonnummer an.
   - Klicken Sie auf die Schaltfläche "Erstellen".
   - Aktivieren Sie "Ereignis-SMS aktivieren" und beim Empfänger "Senden".
   - Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
5. Aktivieren Sie unter "System > Ereignisse > Konfiguration" beim Ereignis "Datenlimit überschritten" die Benachrichtigungsart "SMS".
6. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

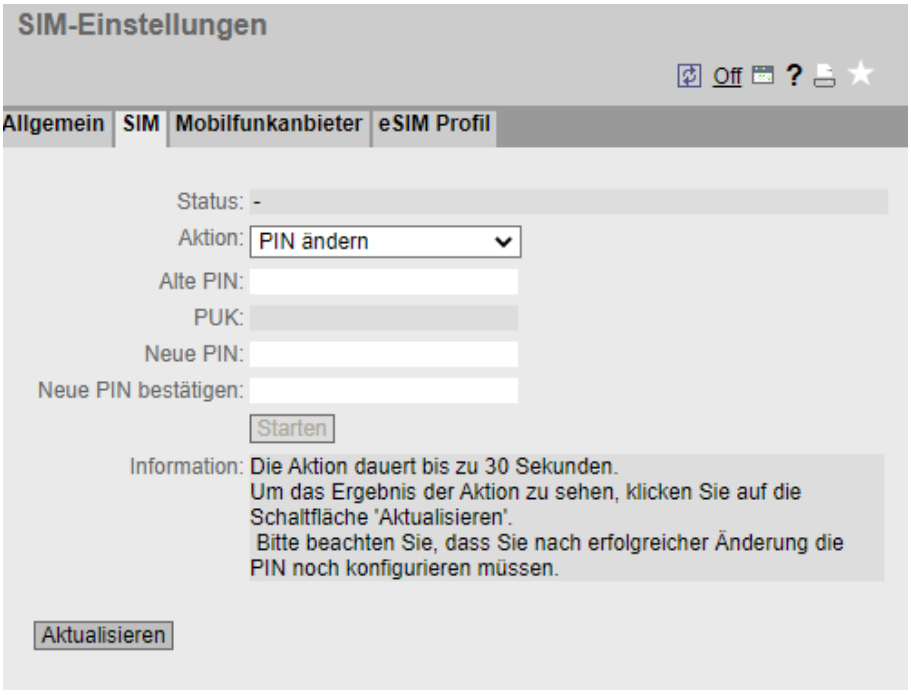
**Ergebnis**:

Der Empfänger erhält die Warnmeldungen via SMS.

## 5.6.2.2 SIM

M87x | MUM85x

Die PIN erhalten Sie mit der SIM-Karte. Auf dieser Seite können Sie für ausgewählte SIM-Karte die PIN ändern oder bei Bedarf die gesperrte SIM-Karte wieder entsperren.




### Voraussetzung

- Die Mobilfunk-Schnittstelle ist deaktiviert.
- Die gewünschte SIM-Karte ist auf der Seite "Schnittstellen > Mobilfunk > Allgemein" bei "SIM-Kartentyp wählen" ausgewählt und aktiviert.

## Beschreibung

Die Seite enthält Folgendes:

- **Status**
  Zeigt den Status der Aktion an. Folgende Einträge sind möglich:
  - -
    Es wurde keine Aktion ausgeführt.
  - Aktion startet
    Das Ausführen der ausgewählten Aktion beginnt.
  - Aktion wird ausgeführt... Zurücksetzen des Funkmoduls
    Nach dem Ausführen der Aktion wird automatisch das Funkmodul zurückgesetzt.
  - SIM-Aktion war erfolgreich
    Die ausgewählte Aktion war erfolgreich.
  - SIM-Karte ist gesperrt
    Die SIM-Karte ist unwiderruflich gesperrt, da der PUK zehnmal in Folge falsch eingegeben wurde.
  - SIM ist nicht gesperrt, verwenden Sie "PIN ändern".
    Die Eingabe bei "PUK" ist nicht notwendig.
  - SIM ist gesperrt, verwenden Sie "SIM entsperren".
    Die SIM-Karte ist gesperrt, da die PIN dreimal in Folge falsch eingegeben wurde. Entsperren Sie die SIM-Karte mit der Aktion "SIM entsperren".
  - PIN falsch (Verbleibende Versuche %d )
    Die Eingabe bei "Alter PIN" ist falsch. Zeigt die verbleibenden Versuche an.
  - PUK falsch (Verbleibende Versuche %d )
    Die Eingabe bei "PUK" ist falsch. Zeigt die verbleibenden Versuche an.
- **Aktion**
  Wählen Sie die gewünschte Aktion aus:
  - PIN ändern
    Ändert die PIN der ausgewählten Karte.
  - SIM entsperren (PUK)
    Entsperrt durch den PUK die SIM-Karte und legt eine neue PIN fest.
  - PIN aktivieren
    Schaltet die PIN-Abfrage ein.
  - PIN deaktivieren
    Schaltet die PIN-Abfrage aus.

  **Hinweis**

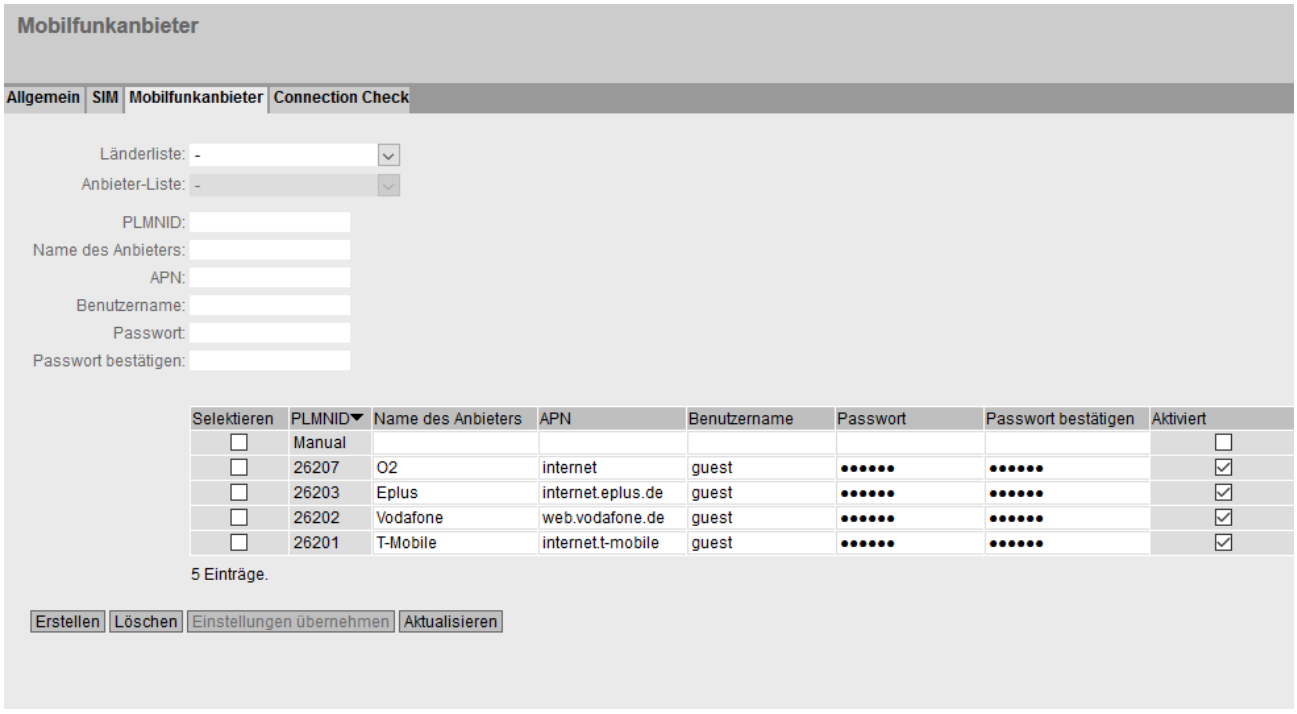
  Wenn Sie die PIN ändern, müssen Sie unter "Schnittstellen > Mobilfunk > Allgemein" die PIN anpassen.
- **Alte PIN**
  Geben Sie die aktuell gültige PIN ein.

- **PUK**
  Personal Unblocking Key
  Geben Sie den PUK ein. Den PUK haben Sie von Ihrem Mobilfunkanbieter zusammen mit der SIM-Karte erhalten.
  Wenn Sie den PUK zehnmal in Folge falsch eingeben, wird die SIM-Karte unwiderruflich gesperrt.
- **Neue PIN**
  Geben Sie die PIN ein, in die Sie die bisherige PIN ändern möchten.
- **Neue PIN bestätigen**
  Wiederholen Sie die neue PIN.
- **Start**
  Führt die gewählte Aktion aus. Je nach Aktion kann das Ausführen bis zu 30 Sekunden dauern.
  Um zu prüfen, ob die Aktion erfolgreich war, prüfen Sie die Anzeige bei "Status". Die Anzeige können Sie entweder automatisch oder manuell aktualisieren.
  - Automatisch
    In der rechten oberen Ecke des Anzeigebereichs auf dieser Seite können Sie über die Schalflächen "on/off" das automatische Aktualisieren des Inhaltsbereichs ein- oder ausschalten. Wenn aktiviert, wird die Anzeige alle 2 Sekunden aktualisiert.
  - Manuell
    Klicken Sie auf die Schaltfläche "Aktualisieren".

### 5.6.2.3 Mobilfunkanbieter

M87x | MUM85x

Der APN (Access Point Name) ist der Name des Zugangspunkts vom Mobilfunknetz zum Internet oder zu einem privaten Firmennetz. Abhängig vom Typ des angeschlossenen Netzes handelt es sich um einen öffentlichen oder privaten APN. Der APN wird vom Mobilfunkanbieter mitgeteilt.




## Beschreibung

Die Seite enthält Folgendes:

- **Länderliste**
  Wählen Sie in der Liste das Land aus, in dem das Gerät eingesetzt wird.
- **Anbieter-Liste**
  Wählen Sie in der Liste den entsprechenden Mobilfunkanbieter aus. Die Liste ist abhängig von dem ausgewählten Land.
  Wenn der Mobilfunkbetreiber nicht in der Liste der Provider enthalten ist, wählen Sie "-" aus.

  **Hinweis**

  **Funkbetriebsart "Nur 5G SA (Standalone)"**

  Bei der Funktionsbetriebsart "Nur 5G SA " sind alle nicht benötigten Provider zu deaktivieren.

- **PLMNID**
  Jeder Mobilfunkanbieter hat eine weltweit einmalig vergebene Identifikationsnummer, die als Public Land Mobile Network ID (PLMN ID) bezeichnet wird. Sie finden die Net-ID in den Unterlagen Ihres Mobilfunkanbieters oder auf dessen Internet-Seiten.
  - Wenn Sie die PLMNID des Mobilfunkanbieters kennen, geben Sie diese Nummer ein.
  - Wenn Sie die PLMNID nicht kennen, geben Sie in der Tabelle bei "Manual" die Daten ein.
- **Name des Anbieters**
  Tragen Sie den Namen Ihres Mobilfunkanbieters ein.

- **APN**
  Tragen Sie den Namen des APNs ein. Den APN finden Sie in den Unterlagen Ihres Mobilfunkanbieters, auf dessen Internet-Seite oder Sie erfragen den APN bei der Hotline Ihres Mobilfunkbetreibers.
- **Benutzername**
  Tragen Sie den Benutzernamen ein. Einige Mobilfunkanbieter verzichten auf die Zugangskontrolle durch Benutzername und/oder Passwort. In diesem Fall lassen Sie das Feld leer.
- **Passwort**
  Tragen Sie das Passwort ein. Einige Mobilfunkanbieter verzichten auf die Zugangskontrolle durch Benutzername und/oder Passwort. In diesem Fall lassen Sie das Feld leer.
- **Passwort bestätigen**
  Wiederholen Sie das Passwort.

Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **PLMNID**
  - Identifikationsnummer (Net-ID)
    Zeigt die PLMNID des Mobilfunkanbieters an.
  - Manual (statischer APN)
    Wenn die PLMNID nicht bekannt ist, geben Sie den APN ihres Mobilfunkanbieters an.
  - Manual (dynamische APN)
    Nur beim M876-4 verfügbar
    Voraussetzung: Funkbetriebsart "Nur LTE"
    Wenn Sie keine Daten konfigurieren, wird der APN dynamisch zugewiesen.
- **Name des Anbieters**
  Tragen Sie den Namen Ihres Mobilfunkanbieters ein.
- **APN**
  Tragen Sie den Namen des APNs ein. Den APN finden Sie in den Unterlagen Ihres Mobilfunkanbieters, auf dessen Internet-Seite oder Sie erfragen den APN bei der Hotline Ihres Mobilfunkbetreibers.
- **Benutzername**
  Tragen Sie den Benutzernamen für den APN ein. Einige Mobilfunkanbieter verzichten auf die Zugangskontrolle durch Benutzername und/oder Passwort. In diesem Fall lassen Sie das Feld leer.
- **Passwort**
  Tragen Sie das Passwort für den APN ein. Einige Mobilfunkanbieter verzichten auf die Zugangskontrolle durch Benutzername und/oder Passwort. In diesem Fall lassen Sie das Feld leer.
- **Passwort bestätigen**
  Wiederholen Sie das Passwort.
- **Aktiviert**
  Der Eintrag wird verwendet.

### 5.6.2.4 eSIM-Profil

MUM85x

**Hinweis**

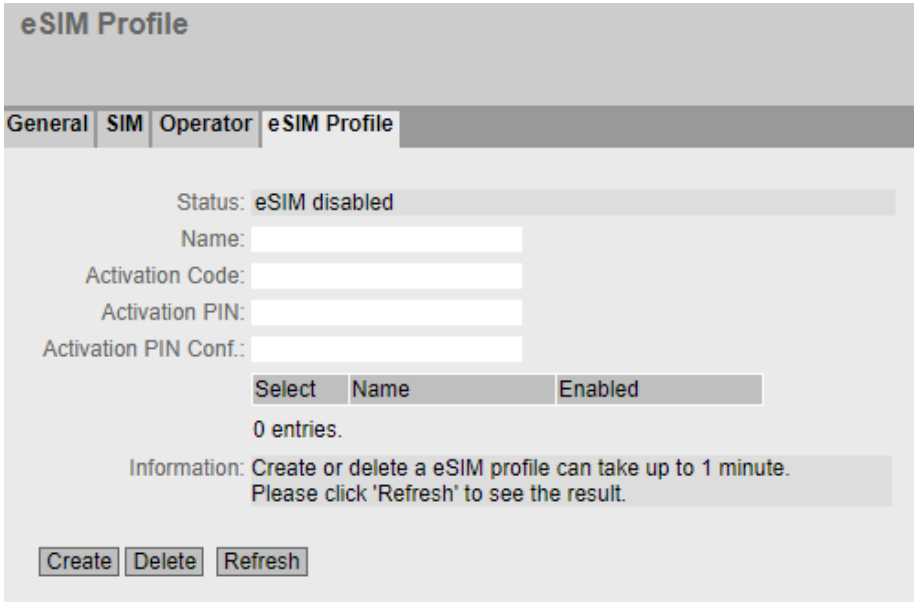
Die eSIM-Funktion ist in Geräten SCALANCE MUM85x ab Hardware-Ausgabestand 2 verfügbar. Die Information zum Hardware-Ausgabestand finden Sie unter "Information > I&M (Seite 133)".

Eine eSIM ist eine eingebettete SIM, die Sie über den vom Mobilfunkanbieter erhaltenen QR-Code aktivieren, um den Mobilfunktarif zu nutzen.

Auf dieser Seite legen Sie auf dem Gerät ein eSIM-Profil Ihrer eSIM-Karte an. Die Seite dient der Ersteinrichtung der eSIM.

Über eine an Ihrem PC angeschlossene Kamera können Sie den QR-Code einscannen. Durch Auslesen des QR-Codes wird das Profil mit den vom Mobilfunkanbieter hinterlegten Daten vervollständigt und die eSIM-Nutzung vom Mobilfunkanbieter freigeschaltet. Es erspart Ihnen die manuelle Eingabe des Aktivierungscodes. Beachten Sie die Voraussetzungen für diesen Vorgang.

Wenn Sie die PIN der eSIM-Karte ändern oder die gesperrte eSIM entsperren wollen, nutzen Sie die Seite "Schnittstellen > Mobilfunk > SIM".



### Voraussetzungen

Bevor Sie ein eSIM-Profil anlegen, überprüfen Sie folgendes:

- Das Datum und die Uhrzeit sind aktuell.
  Sie legen die Systemzeit auf der Seite "System > Systemzeit > Manuelle Einstellung" mit der Schaltfläche "PC-Zeit verwenden" fest.
- Eine Internet-Verbindung ist vorhanden, z. B. über die Ethernet-Schnittstelle.
  Sie legen eine Default-Route auf der Seite "Layer 3 (IPv4) > Statische Routen" fest. Geben Sie als Gateway die IP-Adresse Ihres WLAN-Routers an.
- Der DNS-Server ist konfiguriert.
  Sie legen den DNS-Server auf der Seite "System > DNS > DNS-Client" fest. Geben Sie die IP-Adresse des DNS-Servers an, z. B. die IP-Adresse Ihres WLAN-Routers.
- Die Mobilfunk-Schnittstelle ist deaktiviert.

### Beschreibung

Die Seite enthält Folgendes:

- **Status**
  Zeigt den Status der eSIM an.
  - eSIM enabled
    Die eSIM-Karte ist aktiviert.
  - eSIM disabled
    Die eSIM-Karte ist deaktiviert.
  - Write progress started
    Das eSIM-Profil wird gesucht oder installiert.
  - eSIM available
    Das eSIM-Profil ist vorhanden.
  - Write progress failed
    Der Vorgang ist fehlgeschlagen.
- **Name**
  Geben Sie einen Namen für die eSIM-Karte an.
- **Activation Code**
  Den Aktivierungscode erhalten Sie vom Mobilfunkanbieter.
  Durch Eingabe des Aktivierungscodes werden notwendige Daten vom Mobilfunkanbieter für die zu aktivierende eSIM übermittelt.
  Halten Sie den QR-Code vor die an Ihrem PC angeschlossenen Kamera. Im oberen Bereich der Seite wird Ihnen der Scanbereich der Kamera angezeigt. Der Aktivierungscode wird automatisch ausgelesen und in das Eingabefeld übernommen.
- **Activation PIN**
  Aktivierungs-PIN (ePIN) für die Aktivierung der eSIM-Karte
  Geben Sie die Aktivierungs-PIN für die eSIM-Karte an. Die Aktivierungs-PIN erhalten Sie vom Mobilfunkanbieter.
- **Activation PIN Conf**
  Wiederholen Sie die Aktivierungs-PIN.

Die Tabelle enthält folgende Spalten:

- **Select**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Name**
  Zeigt den Namen der eSIM-Karte an.
- **Enabled**
  Zeigt den Status der eSIM-Karte an.

### Ein neues eSIM-Profil auf dem Gerät anlegen

Sie können bis zu drei eSIM-Profile beliebiger Mobilfunkanbieter anlegen.

Um ein eSIM-Profil anzulegen, gehen Sie wie folgt vor:

1. Wählen Sie auf der Seite "Schnittstellen > Mobilfunk > Allgemein" aus der Klappliste "SIM-Typ auswählen" den Eintrag "eSIM" aus.
2. Aktivieren Sie das Optionskästchen "SIM aktivieren".
3. Klicken Sie auf "Einstellungen übernehmen".
4. Öffnen Sie das Register "eSIM-Profil" und aktualisieren Sie die Seite mit der Schaltfläche On im rechten oberen Anzeigebereich der Seite.
   Während das Gerät nach einer eSIM sucht, wird der Status "Write progress started" angezeigt. Das kann bis zu einer Minute dauern. Nach einer erfolgreichen Suche ändert sich der Status in "eSIM available" und der Scanbereich der Kamera wird angezeigt.
5. Geben Sie einen Namen für das eSIM-Profil ein. Sonderzeichen sind nicht erlaubt.
6. Halten Sie den QR-Code vor die Kamera, um den Aktivierungscode abzulesen.
   Der Aktivierungscode wird in die Zeile "Aktivierungscode" automatisch übernommen. Im CLI sollte der Aktivierungscode händisch eingetragen bzw. kopiert werden.

   **Hinweis**

   **Aktivierungscode ist nur einmal verwendbar**

   Der Aktivierungscode kann nicht auf mehreren Geräten gleichzeitig verwendet werden. Ein Einspielen des gleichen Aktivierungscodes auf ein weiteres Gerät ist nicht möglich. Das gilt auch wenn der Aktivierungscode bereits auf einem Endgerät, z. B. einem Smartphone verwendet wurde.

7. Geben Sie die Aktivierungs-PIN ein.
   Sie finden die Aktivierungs-PIN (häufig als ePIN bezeichnet) im Schreiben des Mobilfunkanbieters zu der zugesandten eSIM.
8. Bestätigen Sie die Aktivierungs-PIN durch die erneute Eingabe und speichern Sie das Profil mit "Erstellen".
   Nach dem Speichern ändert sich der Status in "Write progress started ". Das eSIM-Profil wird nun heruntergeladen und installiert. Im Hintergrund wird eine Internetverbindung zum Mobilfunkanbieter aufgebaut, der prüft, ob die PIN zur eSIM passt. Das Anlegen kann bis zu einer Minute dauern. Sie können den Vorgang während dieser Zeit über die Schaltfläche On aktualisieren lassen. Nach einer erfolgreichen Suche ändert sich der Status in "eSIM available". Falls das Überprüfen fehlschlägt, erscheint eine Meldung darüber.

Wenn Sie später den Namen im eSIM-Profil ändern, wird das Profil erneut geladen und die Aktualisierung kann einige Minuten in Anspruch nehmen.

### Bereits angelegtes eSIM-Profil auf dem Gerät aktivieren

Ein neu angelegtes eSIM-Profil ist auf dem Gerät zunächst deaktiviert. Der angezeigte SIM-Status im Menü "Information > Mobilfunk > Übersicht" ist "Fehlend" und es kann keine Mobilfunkverbindung aufbaut werden. Zu diesem Zeitpunkt ist es nicht möglich, das Optionskästchen "Mobilfunk-Schnittstelle aktivieren" auf der Seite "Schnittstellen > Mobilfunk > Allgemein" zu aktivieren. Bei Versuchen kommt die Meldung "Keine SIM-Karte erkannt".

**Hinweis**

Zum Aktivieren, Deaktivieren oder Umbenennen eines eSIM-Profils wird keine Internetverbindung benötigt. Nur zum Einspielen eines neuen eSIM-Profils über den Aktivierungscode ist eine Internetverbindung notwendig.

Es kann nur ein eSIM-Profil aktiv sein. Wenn Sie ein anderes eSIM-Profil aktivieren möchten, müssen Sie zuerst das derzeit aktive eSIM-Profil deaktivieren.

1. Aktivieren Sie das gewünschte eSIM-Profil über das Optionskästchen "Enabled" und klicken Sie auf "Einstellungen übernehmen".
   Der SIM-Status im Menü "Information > Mobilfunk > Übersicht" ändert sich in "Vorhanden". Nun verhält sich die eSIM wie eine SIM-Karte und Sie können ihr optional eine PIN vergeben. Beachten Sie, dass nach dem Löschen des eSIM-Profils alle Änderungen verworfen werden.
2. Aktivieren Sie das Optionskästchen "Mobilfunk-Schnittstelle aktivieren" auf der Seite "Schnittstellen > Mobilfunk > Allgemein".
   Nach dem Aktivieren der Mobilfunkschnittstelle sind die Konfigurationsfelder der SIM ausgegraut. Dadurch wird jede Änderung an SIM oder ein Wechsel zwischen SIMs im laufenden Betrieb verhindert.

### eSIM-Profil vom Gerät löschen

Sie können ein oder mehrere eSIM-Profile löschen. Für diesen Vorgang brauchen Sie keine Internetverbindung. Bei einer aktiven Internetverbindung wird der Mobilfunkanbieter über die freizugebende eSIM benachrichtigt.

Um ein eSIM-Profil zu löschen, gehen Sie wie folgt vor:

1. Deaktivieren Sie das Optionskästchen "Mobilfunk-Schnittstelle aktivieren" auf der Seite "Schnittstellen > Mobilfunk > Allgemein".
2. Öffnen Sie das Register "eSIM-Profil". Wenn das zu löschende eSIM-Profil aktiviert ist, deaktivieren Sie es in der Tabellenspalte "Enabled" und klicken Sie auf "Einstellungen übernehmen".
3. Selektieren Sie das zu löschende eSIM-Profil und klicken Sie auf "Löschen".
   Das eSIM-Profil wird vom Gerät gelöscht.

**Hinweis**

**eSIM für weitere Verwendung freigeben**

Bei einer aktiven Internetverbindung wird der Aktivierungscode nach dem Löschen des eSIM-Profils und einer Bestätigung des Mobilfunkanbieters über die Freigabe der betreffenden eSIM weiter nutzbar. Bei einigen Mobilfunkanbietern wird der Aktivierungscode jedoch mit dem ersten Aktivieren verbraucht und Sie müssen ihn nach dem Löschen des eSIM-Profils wieder bestellen.

### Auf physische SIM umschalten

1. Deaktivieren Sie das Optionskästchen "Mobilfunk-Schnittstelle aktivieren" auf der Seite "Schnittstellen > Mobilfunk > Allgemein".
2. Wählen Sie aus der Klappliste "SIM-Typ auswählen" den Eintrag "Physical" aus.
   Nach dem Aktivieren der physikalischen SIM sind die angelegten eSIM-Profile nicht mehr sichtbar.

## 5.6.2.5 Connection Check

M87x

Verwenden Sie diese Funktion, um sicherzustellen, dass die Verbindung zum Mobilfunknetz besteht. Auf dieser Seite legen Sie fest, welche WAN-IP-Adressen als Referenz für die Verbindungsüberwachung verwendet werden.

Das Gerät sendet in regelmäßigen Abständen (Ping Time Interval) Echomeldungen (Ping) an die projektierten WAN-IP-Adressen.

Wenn Sie z. B. drei WAN-IP-Adressen projektieren, dann sendet das Gerät an die erste WAN-IP-Adresse einen Ping. Wenn diese WAN-IP-Adresse erreichbar ist, sendet diese eine Antwort. Nach Ablauf des projektieren Intervalls sendet das Gerät den nächsten Ping. Wenn die erste WAN-IP-Adresse nicht erreichbar ist, sendet das Gerät nach Ablauf einer Wartezeit (10s) einen weiteren Ping. Insgesamt werden drei Pings an die WAN-IP-Adresse gesendet. Wenn das Gerät nach dem dritten Ping keine Antwort erhält, wird die zweite WAN-IP-Adresse überprüft. Ist auch diese WAN-IP-Adresse nicht erreichbar, wird die nächste WAN-IP-Adresse überprüft.

Wenn keine der drei WAN-IP-Adressen erreichbar ist, startet das Gerät die Mobilfunkschnittstelle neu und protokolliert den Neustart mit folgender Meldung "Detected a problem with the provider connection. Trying to reconnect to the provider. Attempt no.: x".

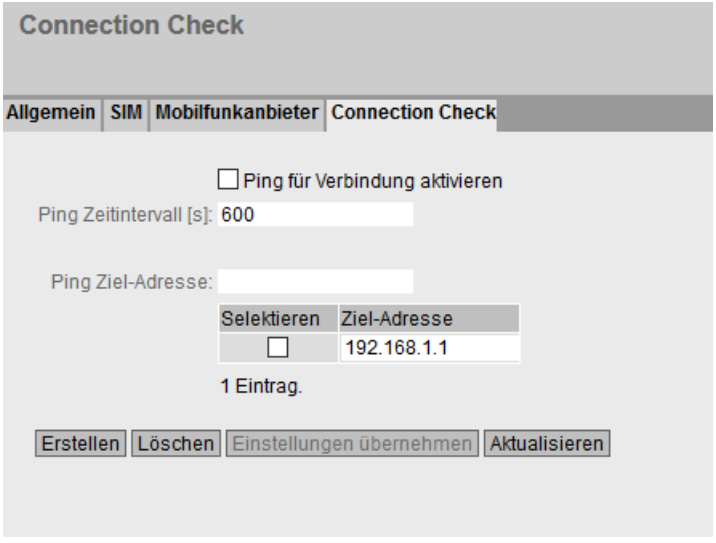
Das x steht für die Anzahl der Versuche. Insgesamt führt das Gerät 10 Versuche durch. Nach dem Neustart der Mobilfunkschnittstelle wartet das Gerät einige Zeit und sendet dann

einen Ping an die erste WAN-IP-Adresse. Die Wartezeit beträgt beim ersten Neustart der Mobilfunkschnittstelle 2 Minuten. Bei jedem weiteren Neustart der Mobilfunkschnittstelle verlängert sich die Wartezeit um eine Minute.

Wenn die 10 Versuche erfolglos sind, startet das Gerät neu und protokolliert den Neustart mit folgender Meldung: "Detected a problem with the provider connection. Reconnect to the provider had no effect. Device will restart now."

**Hinweis**

Projektieren Sie stets mehrere WAN-IP-Adressen. Wenn Sie nur eine WAN-IP-Adresse projektieren, kann der sporadische Ausfall der einzelnen WAN-IP-Adresse dazu führen, dass die WAN-Verbindung ständig neu aufgebaut wird.




## Beschreibung

Die Seite enthält Folgendes:

- **Ping für Verbindung aktivieren**
  Aktivieren oder deaktivieren Sie die Funktion. Nur aktivierbar, wenn mindestens eine IP-Adresse projektiert ist.
- **Ping Zeitintervall [s]**
  Legen Sie fest, in welchem Abstand die Pings gesendet werden.
- **Ping Ziel-Adresse**
  Tragen Sie die WAN-IP-Adresse ein, die für die Verbindungsüberwachung verwendet wird. Klicken Sie auf "Create", um den Eintrag in der Tabelle abzuspeichern

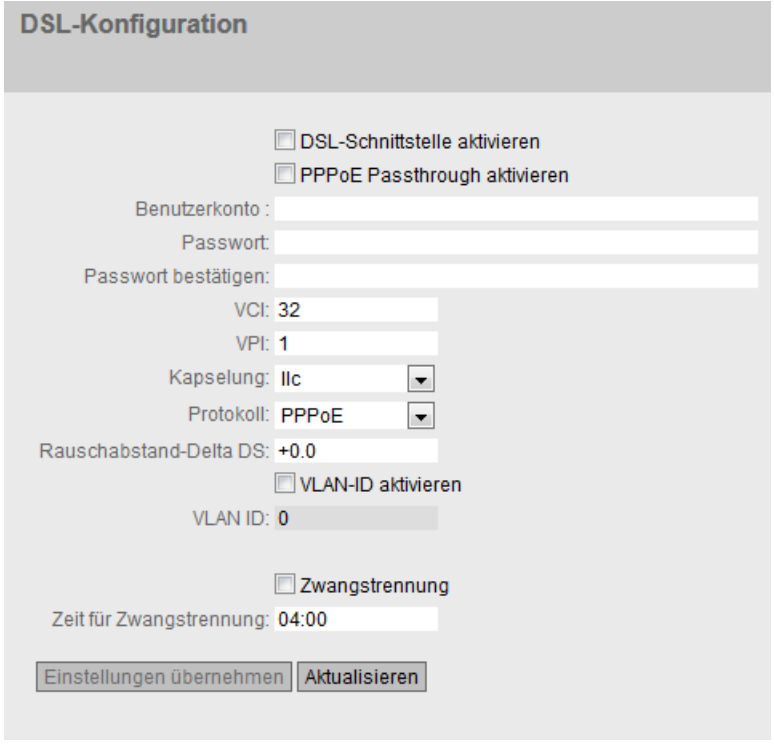
Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Ziel-Adresse**
  Zeigt die WAN-IP-Adresse an.

## 5.6.3 DSL

M81x

Auf dieser WBM-Seite konfigurieren Sie den DSL-Zugang und die Parameter für die virtuelle Verbindung, über die die Pakete übertragen werden.



## Beschreibung

Die Seite enthält Folgendes:

- **DSL-Schnittstelle aktivieren**
  Aktivieren oder deaktivieren Sie die DSL-Schnittstelle.
- **PPPoE Passthrough aktivieren**
  - Aktiviert
    Das Gerät agiert als Modem. Die Einstellungen "Account", "Password" und "Enable Force Disconnect" sind nicht editierbar. Nur ein angeschlossenes Gerät kann die DSL-Verbindung nutzen. Dieses Gerät übernimmt auch die Authentifizierung (Einwahl) beim Provider.
  - Deaktiviert
    Das Gerät agiert als Router und meldet sich mit Benutzernamen und Passwort an. Alle angeschlossenen Geräte können die DSL-Verbindung nutzen.
- **Benutzerkonto**
  Tragen Sie den Benutzernamen ein. Den Benutzernamen erhalten Sie von Ihrem DSL-Anbieter.
- **Passwort**
  Tragen Sie das Passwort ein. Das Password erhalten Sie von Ihrem DSL-Anbieter.
- **Passwort bestätigen**
  Wiederholen Sie das Passwort.
- **VCI** (Virtual Channel Identifier)
  Tragen Sie die ID für den virtuellen Kanal ein. Die Einstellung erhalten Sie von Ihrem DSL-Anbieter.
- **VPI** (Virtual Path Identifier)
  Tragen Sie die ID für den virtuellen Pfad ein. Die Einstellung erhalten Sie von Ihrem DSL-Anbieter.
- **Kapselung**
  Die Datenpakete werden in das gewünschte Protokoll eingepackt.
  Folgende Möglichkeiten gibt es:
  - vc-mux (Virtual circuit - multiplexing)
  - LLC (Logical Link Control)
- **Protokoll**
  Legen Sie das Protokoll für die Internetverbindung fest. Die Information erhalten Sie von ihrem DSL-Anbieter.
  - PPPoE (Point-to-Point over Ethernet)
    Die PPP-Daten werden in einen Ethernet-Frame eingekapselt.
  - PPPoA (Point-to-Point over ATM)
    Die PPP-Daten werden in ATM AAL5 (Adaptation Layer 5) eingekapselt. Wenn Sie PPPoA auswählen, wird die Einstellung "PPPoE Passthrough aktivieren" deaktiviert.
- **Rauschabstand-Delta DS:**
  Legen Sie den Abstand zum Grundrauschen fest.
  Wertebereich -5dB ... +5dB

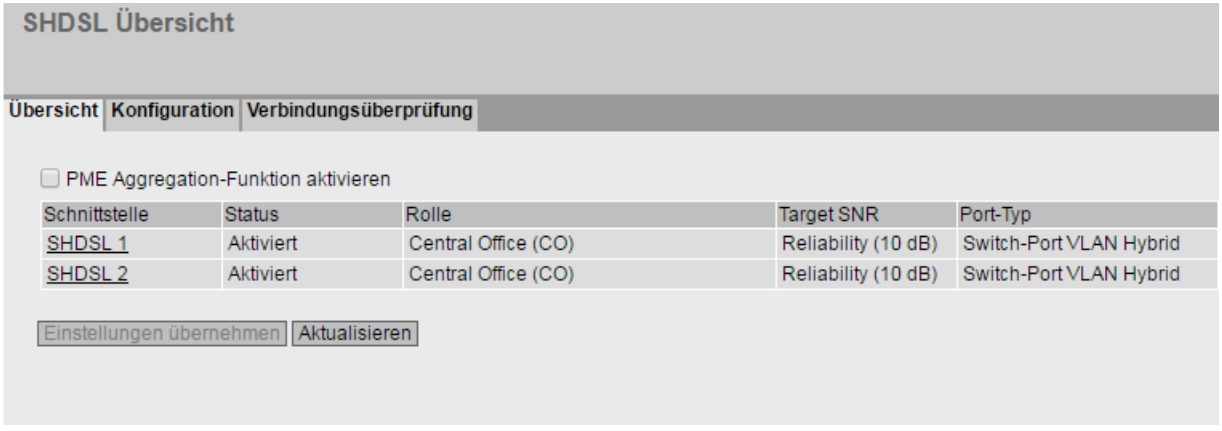
- **VLAN-ID aktivieren**
  Wenn aktiviert, können Sie eine VLAN-ID konfigurieren. Nur notwendig, wenn für den DSL-Zugang die Angabe einer VLAN-ID erforderlich ist.
- **VLAN ID**
  Geben Sie die VLAN-ID für den DSL-Zugang an. Die Einstellung erhalten Sie von Ihrem DSL-Anbieter.
- **Zwangstrennung**
  Der DSL-Anbieter trennt nach einem bestimmten Zeitraum die Verbindung. Aktivieren Sie diese Option, wenn Sie die Zwangstrennung durch Ihren Provider auf eine bestimmte Uhrzeit verschieben wollen, z. B. Nachts außerhalb der üblichen Bürozeiten.
- **Zeit für Zwangstrennung**
  Legen Sie die Uhrzeit fest, zu der Sie die Zwangstrennung des DSL-Anbieters verschieben wollen. Vorausgesetzt, im Gerät ist die korrekte Systemzeit eingestellt.
  Eingabeformat: HH:MM

## 5.6.4 SHDSL

### 5.6.4.1 Übersicht

M826

Die WBM-Seite zeigt die Konfiguration der SHDSL-Schnittstellen an.



### Beschreibung

Die Seite enthält Folgendes:

- **PME Aggregation-Funktion aktivieren**
  PME = Physical Medium Entities
  Wenn aktiviert, werden die SHDSL-Schnittstellen bzw. die 2-Drahtleitungen zu einer einzigen Verbindung mit höherer Übertragungsrate zusammengefasst.

  **Hinweis**

  Wenn die Funktion "PME Aggregation" aktiviert ist, müssen die Schnittstellen eines Geräts jeweils die gleiche Rolle besitzen.

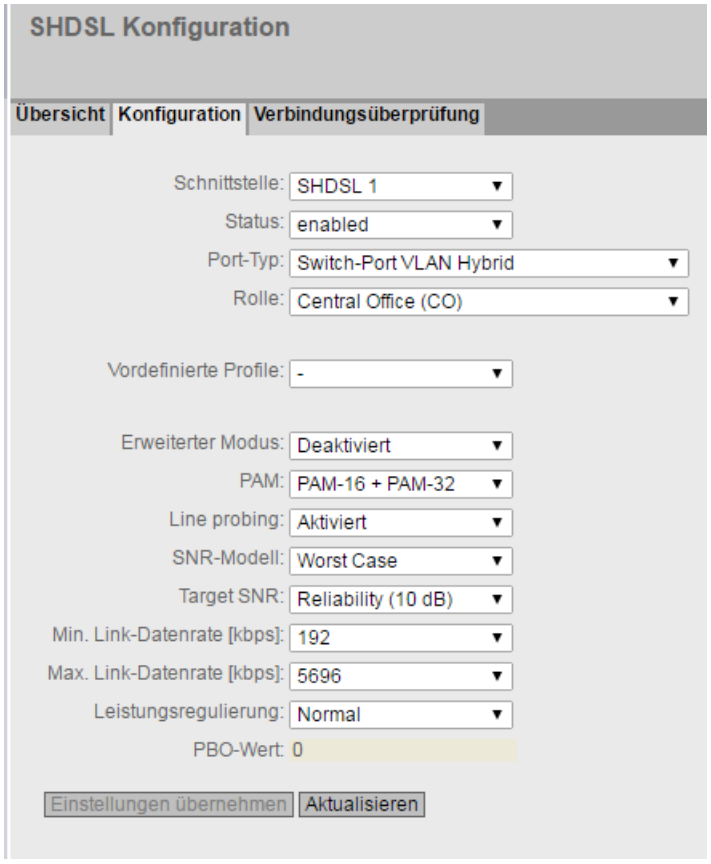
Die Tabelle enthält folgende Spalten:

- **Schnittstelle**
  Zeigt die verfügbaren SHDSL-Schnittstellen an.
- **Status**
  Zeigt an, ob die Schnittstelle verwendet wird oder nicht.
- **Rolle**
  Zeigt die Rolle der SHDSL-Schnittstelle an:
  - Central Office (CO)
    Die Schnittstelle ist eine Vermittlungsstelle.
  - Customer Premises Equipment (CPE)
    Die Schnittstelle ist ein Teilnehmerendgerät.
- **Target SNR**
  Zeigt das Signal-Rausch-Verhältnis an:
  - Zuverlässig (10 dB)
    Zuverlässige Übertragung
  - Normal (6 dB)
    Normale Übertragung
  - High-speed (0 dB)
    Hochgeschwindigkeits-Übertragung
- **Port-Typ**
  Zeigt den Betriebsmodus des Switch-Ports an:
  - Switch-Port VLAN Hybrid
    Der Port akzeptiert getaggte und ungetaggte Telegramme.
  - Switch-Port VLAN Trunk
    Der Port sendet nur getaggte Telegramme und ist automatisch Mitglied in allen VLANs.

## 5.6.4.2 Konfiguration

M826

Auf dieser WBM-Seite legen Sie die Einstellungen für die Verbindung fest und welche Rolle das Gerät übernimmt. Weitere Informationen zu den Einstellungen finden Sie in der ITU-T G.991.2.




## Beschreibung

Die Seite enthält Folgendes:

- **Schnittstelle**
  Wählen Sie die Schnittstelle aus.
- **Status**
  Legen Sie fest, ob die Schnittstelle verwendet wird.
- **Port -Typ**
  Legen Sie den Betriebsmodus für den Switch-Port fest.
  - Switch-Port VLAN Hybrid
    Der Port akzeptiert getaggte und ungetaggte Telegramme.
  - Switch-Port VLAN Trunk
    Der Port sendet nur getaggte Telegramme und ist automatisch Mitglied in allen VLANs.
- **Rolle**
  Legen Sie die Rolle fest**:**
  - Central Office (CO)
    Die Schnittstelle ist eine Vermittlungsstelle.
  - Customer Premises Equipment (CPE)
    Die Schnittstelle ist ein Teilnehmerendgerät.

- **Vordefinierte Profile**
  Legen Sie das Profil für die Übertragung fest. Wenn Sie ein Profil verwenden, werden die nachfolgenden Parameter automatisch eingestellt.
  - Profile mit einem Übertragungsbereich
    Wenn beim Einmessen der Leitung der gemessene Wert innerhalb des Bereichs liegt, wird die SHDSL-Verbindung aufgebaut.

| | Link-Datenrate min - max | |
|---|---|---|
| Standard | 192 - 5696 | Für mittlere und längere Leitungslänge |
| Zuverlässig | 192 - 5696 | Beim gleichzeitigen Betrieb von mehreren SHDSL-Verbindungen. |
| Erweitert | 64 - 15296 | Für kurze und lange Leitungslänge |

  - Profile mit einer fest vorgegebenen Übertragungsrate
    Nur wenn beim Einmessen der Leitung der gemessene Wert genau der fest vorgegebenen Übertragungsrate entspricht, wird eine SHDSL-Verbindung aufgebaut.

| | Link-Datenrate |
|---|---|
| Fest (Hohe Datenrate) | 5696 |
| Fest (Mittlere Datenrate) | 3072 |
| Fest (Niedrige Datenrate) | 512 |

- **Erweiterter Modus**
  Aktivieren oder deaktivieren Sie den erweiterten Modus. Abhängig von der Einstellung, ändert Sie die Auswahl in den nachfolgenden Feldern.
- **PAM**
  Pulse Amplitude Modulation
  Legen Sie das Modulationsverfahren fest.
- **Line probing**
  Wenn aktiviert, wird die Leitung gemäß ITU-T G.991.2 eingemessen.
- **SNR-Modell**
  Legen Sie das Modell zum Berechnen des Signal-Rausch-Verhältnisses fest.
  - Aktuelle Bedingung
    Der Wert für Rauschen wird verwendet, der beim Einmessen der Leitung gemessen wurde.
  - Worst Case
    Der Wert für Rauschen wird angenommen, der über mehrere Leitungen eines Kabelbündels auftreten könnte.

- **Target SNR**
  Legen Sie den Übertragungsmodus für das Signal-Rausch-Verhältnis fest. Unter "Information > SHDSL" wird das aktuelle Signal-Rausch-Verhältnis angezeigt.
  - Zuverlässig (10 dB)
    Zuverlässige Übertragung
  - Normal (6 dB)
    Normale Übertragung
  - High-speed (0 dB)
    Hochgeschwindigkeits-Übertragung
- **Min. Link Datenrate [kbps]**
  Legen Sie die minimale Übertragungsrate für das Senden und das Empfangen von Daten fest.
  - Auto (0)
    Das Gerät passt die Übertragungsrate je nach Modus automatisch an.
  - 192 bis 5696
    Die Übertragungsrate ist fest vorgegeben.
- **Max. Link Datenrate [kbps]**
  Legen Sie die maximale Übertragungsrate für das Senden und das Empfangen von Daten fest.
  - Auto (0)
    Das Gerät passt die Übertragungsrate je nach Modus automatisch an.
  - 192 bis 5696
    Die Übertragungsrate ist fest vorgegeben.
- **Leistungsregulierung**
  Legen Sie die fest, ob die Sendeleistung reduziert wird.
  - Deaktiviert
    Die Funktion ist deaktiviert
  - Normal
    Die Funktion ist aktiviert.
  - Erzwingen
    Bei PBO Value geben Sie den Wert für die Dämpfung an.
- **PBO-Wert**
  Power Back Off Values
  Geben Sie den Wert für die Dämpfung an. Nur wenn der Wert erreicht wird, wird eine SHDSL-Verbindung aufgebaut.
  - Bereich: 0 - 31 dB, wobei "0" keine Dämpfung bedeutet.

### 5.6.4.3 Connection Check

M826

Verwenden Sie diese Funktion, um sicherzustellen, dass die Verbindung zum SHDSL-Netz besteht. Auf dieser Seite legen Sie fest, welche WAN-IP-Adressen als Referenz für die Verbindungsüberwachung verwendet werden.

Das Gerät sendet in regelmäßigen Abständen (Ping Time Interval) Echomeldungen (Ping) an die projektierten WAN-IP-Adressen.

Wenn Sie z. B. drei WAN-IP-Adressen projektieren, dann sendet das Gerät an die WAN-IP-Adressen einen Ping. Wenn nur eine der drei WAN-IP-Adressen nicht erreichbar ist, wird das folgender Meldung protokolliert: "Could not reach remote device a.b.c.d  (Failure count x)".

Dabei steht "a.b.c.d" für die IP-Adresse des Geräts und das x steht für die Anzahl der Versuche. Insgesamt führt das Gerät 5 Versuche durch.

Wenn die IP-Adresse wieder erreichbar ist, wird dies mit folgender Meldung protokolliert: SHDSL connection check: Remote devices are reachable again.

Wenn die 5 Versuche erfolglos sind, startet das Gerät neu und protokolliert den Neustart mit folgender Meldung: "SHDSL connection check: Maximum failure count reached, restarting device."




## Beschreibung

Die Seite enthält Folgendes:

- **Ping für Verbindung aktivieren**
  Aktivieren oder deaktivieren Sie die Funktion. Nur aktivierbar, wenn mindestens eine IP-Adresse projektiert ist.
- **Ping Zeitintervall [s]**
  Legen Sie fest, in welchem Abstand die Pings gesendet werden.
- **Ping Ziel-Adresse**
  Tragen Sie die WAN-IP-Adresse ein, die für die Verbindungsüberwachung verwendet wird. Klicken Sie auf "Erstellen", um den Eintrag in der Tabelle anzulegen.

Die Tabelle enthält folgende Spalten:

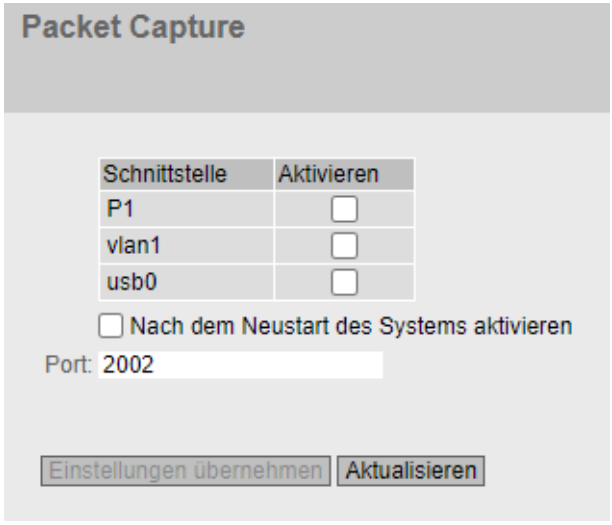
- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Ziel-Adresse**
  Zeigt die WAN-IP-Adresse an.

## 5.6.5 Packet Capture

MUM85x

Auf dieser WBM-Seite aktivieren Sie an der Schnittstelle (Ethernet, WLAN) die Funktion "Packet Capture". Die Funktion dient der Netzwerkdiagnose über einen angeschlossenen PC, z. B. um Übertragungsfehlern auf die Spur zu kommen.

Die Funktion können Sie auch an mehreren Schnittstellen gleichzeitig aktivieren. Wenn die Funktion aktiviert ist, lässt sich die Schnittstelle in Wireshark einbinden. Wireshark zeichnet über einen Zeitraum den Datenverkehr auf, der über die Schnittstelle fließt. Danach können Sie aus dem Mitschnitt heraus den Inhalt der Frames ansehen oder nach bestimmten Inhalten filtern.




### Beschreibung

Die Tabelle enthält folgende Spalten:

- **Schnittstelle**
  Die Schnittstelle, auf die sich der Eintrag bezieht.
- **Aktivieren**
  Aktivieren oder deaktivieren Sie die Funktion "Packet Capture". Defaultmäßig ist die Funktion deaktiviert.

**Hinweis**

**Performance**

Aktivieren Sie die Funktion nur zu Diagnosezwecke. Der erhöhte Datenverkehr könnte die Performance des Geräts beeinflussen.

Die Seite enthält folgende Felder:

- **Nach dem Systemstart aktivieren**
  - Deaktiviert
    Nach einem Neustart wird die Konfiguration auf die Default-Einstellung zurückgesetzt.
  - Aktiviert
    Die Konfiguration wird gespeichert und bleibt nach einem Neustart enthalten.
- **Port**
  Sie können den Port ggf. ändern. Default-Port: 2002

### Schnittstelle in Wireshark einbinden

**Voraussetzung:**

- Wireshark ab V2.0.0 ist auf dem PC installiert.
- Der PC und das Gerät müssen über IP (Layer 3) erreichbar sein.

**Vorgehensweise**

Um den Datenverkehr z. B. der VLAN-Schnittstelle 1 in Wireshark zu analysieren, gehen Sie folgendermaßen vor:

1. Aktivieren Sie am Gerät an der Schnittstelle vlan1 die Funktion "Packet Capture".
2. Klicken Sie auf "Einstellungen übernehmen", um die Funktion zu aktivieren.
3. Aktivieren Sie im Menü "Security > Firewall > Vordefinierte Regeln" auf der betreffenden Eingangsschnittstelle den Zugriff auf Capture.
4. Starten Sie Wireshark.
5. Klicken Sie im Menü "Aufzeichnen" auf "Optionen". Das Fenster "Wireshark - Mitschnittschnittstellen" wird geöffnet.
6. Klicken Sie auf dem Register "Eingabe" auf die Schaltfläche "Schnittstellen verwalten...". Klicken Sie im folgenden Dialog auf das Register "Entfernte Schnittstellen".
7. Um die Schnittstelle hinzuzufügen, klicken Sie im Register "Entfernte Schnittstellen" das Pluszeichen.
8. Geben Sie im folgenden Dialog bei "Host" die IPv4-Adresse des Geräts und bei "Port" 2002 ein.
9. Aktivieren Sie bei "Authentifizierung" "Keine Authentifizierung" und klicken Sie auf die Schaltfläche "OK".
10. Auf dem Register "Entfernte Schnittstellen" wird der Host und die Schnittstellen angezeigt, an denen zuvor die Funktion "Packet Capture" aktiviert wurde.

11. Wählen Sie die Schnittstelle aus und klicken Sie auf die Schaltfläche "OK".
    Die angezeigten entfernten Schnittstellen entsprechen folgenden Schnittstellen am SCALANCE M-Gerät:

| Entfernte Schnittstelle in Wireshark | Schnittstelle am SCALANCE-Gerät | Kommentar |
|---|---|---|
| eth0 | P1 | - |
| eth1 | P2 | Nur bei SCALANCE MUM853 |
| eth2 | P3 | |
| eth3 | P4 | |
| vlanX | VLAN X | Wertebereich: 1 ... 4094 |
| usb0 | usb0 | - |

12. Um die Aufzeichnung zu starten, klicken Sie Menü "Aufzeichnen" auf "Starten". Weitere Informationen zum Umgang mit dem Programm erhalten Sie bei Wireshark.

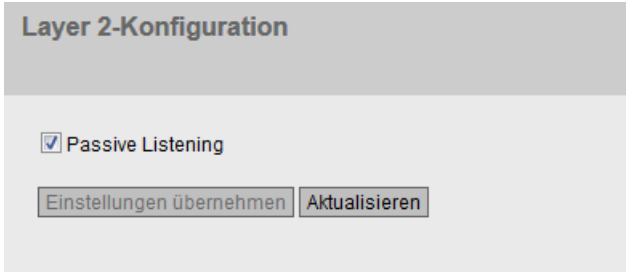
Wenn Sie mehrere Schnittstellen analysieren, können Sie für jede Schnittstelle eine Wireshark-Instanz verwenden.

# 5.7 Menü "Layer 2"

## 5.7.1 Layer 2-Konfiguration

### Layer 2 konfigurieren

Auf dieser Seite nehmen Sie eine Basiskonfiguration der Funktionen des Layer 2 vor.




### Beschreibung

- **Passive Listening**
  Wenn aktiviert, sorgt die Funktion dafür, dass die BPDUs aus dem RSTP-Netzwerk transparent weitergeleitet werden und auch wieder zurückgelangen. Wäre dies nicht der Fall, würde es zur Schleifenbildung an der Verbindungsstelle zwischen RSTP und Ring kommen.

## 5.7.2 VLAN

### 5.7.2.1 Allgemein

#### VLAN-Konfigurationsseite

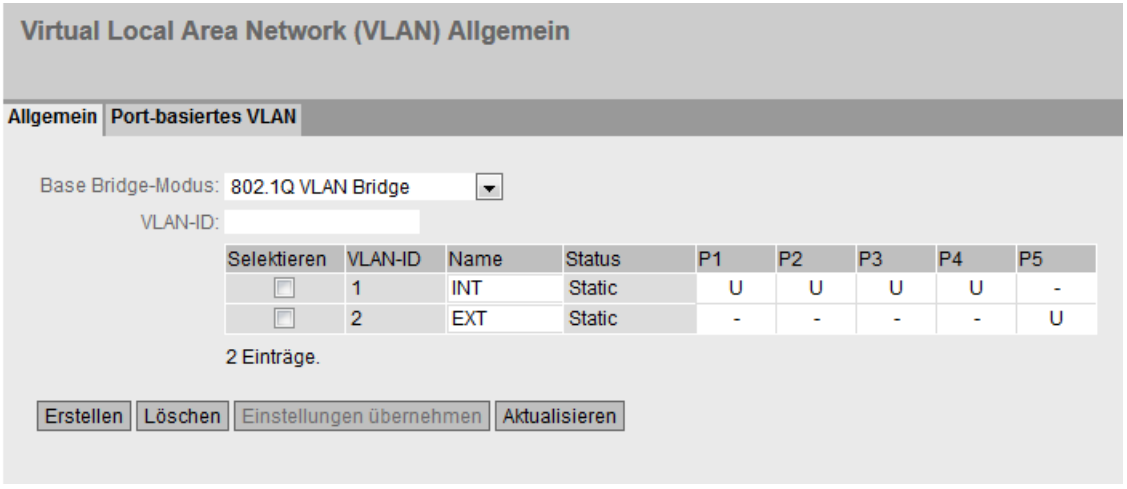
Auf dieser Seite legen Sie fest, ob das Gerät Telegramme mit VLAN-Tags transparent weiterleitet (IEEE 802.1D/VLAN-unaware-Modus) oder VLAN-Informationen berücksichtigt (IEEE 802.1Q/ VLAN-aware-Modus). Wenn sich das Gerät im Modus "802.1Q VLAN Bridge" befindet, können Sie VLANs definieren und die Verwendung der Ports festlegen.

Die Einstellmöglichkeiten auf dieser Seite sind abhängig davon, was Sie im Feld "Base Bridge Mode" auswählen.

**Hinweis**

**Ändern der Agent VLAN ID**

Wenn der Konfigurations-PC direkt über Ethernet mit dem Gerät verbunden ist und Sie die Agent VLAN-ID ändern, ist nach der Änderung das Gerät über Ethernet nicht mehr erreichbar.



## Beschreibung

Die Seite enthält folgende Felder:

- **Base Bridge-Modus**

  **Hinweis**

  **Base Bridge-Modus wechseln**

  Beachten Sie den Abschnitt "Base Bridge-Modus" wechseln" in diesem Kapitel. Der Abschnitt beschreibt, wie sich ein Wechsel auf die bestehende Konfiguration auswirkt.

  Wählen Sie aus der Klappliste den gewünschten Modus aus. Folgende Modi sind möglich:

  – 802.1Q VLAN Bridge
  Stellt bei dem Gerät den Modus "VLAN-aware" ein. In diesem Modus werden VLAN-Informationen berücksichtigt.

  – 802.1D Transparent Bridge
  Stellt bei dem Gerät den Modus "VLAN-unaware" ein. In diesem Modus werden VLAN-Tags nicht berücksichtigt bzw. verändert, sondern transparent weitergeleitet. Sie können in diesem Modus keine VLANs anlegen. Es ist nur ein Management-VLAN verfügbar: VLAN 1.

- **VLAN-ID**
  Tragen Sie im Eingabefeld "VLAN-ID" die VLAN-ID ein.
  Wertebereich: 1 ... 4094

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **VLAN-ID**
  Zeigt die VLAN-ID an. Die VLAN-ID (eine Zahl zwischen 1 und 4094) kann nur beim Anlegen eines neuen Datensatzes einmalig vergeben werden und ist danach nicht mehr änderbar. Zur Änderung muss der gesamte Datensatz gelöscht und neu angelegt werden.
- **Name**
  Tragen Sie einen Namen für das VLAN ein. Der Name hat nur informativen Charakter und keine Auswirkungen auf die Konfiguration. Die Länge ist max. 32 Zeichen.

- **Status**
  Zeigt die Statusart des Eintrags in der internen Portfiltertabelle an. Dabei bedeutet "Static", dass das VLAN vom Anwender statisch eingetragen wurde.
- **Liste der Ports**
  Legen Sie die Verwendung des Ports fest. Folgende Möglichkeiten gibt es:
  - "-"
    Der Port ist kein Mitglied des angegebenen VLANs.
    Bei der Neudefinition sind alle Ports mit der Kennung "-" belegt.
  - M
    Der Port ist Mitglied des VLANs. In diesem VLAN gesendete Telegramme werden mit dem entsprechenden VLAN-Tag weitergeleitet.
  - U (Großbuchstabe)
    Der Port ist ungetaggtes Mitglied des VLANs. In diesem VLAN gesendete Telegramme werden ohne VLAN-Tag weitergeleitet. Von diesem Port werden Telegramme ohne VLAN-Tag gesendet.
  - u (Kleinbuchstabe)
    Der Port ist ungetaggtes Mitglied des VLANs, jedoch ist das VLAN nicht als Port-VLAN konfiguriert. In diesem VLAN gesendete Telegramme werden ohne VLAN-Tag weitergeleitet.
  - F
    Der Port ist kein Mitglied des angegebenen VLANs und kann kein Mitglied dieses VLAN werden, auch dann nicht, wenn er als Trunk-Port konfiguriert wird.
  - T
    Diese Option wird nur angezeigt und kann im WBM nicht ausgewählt werden.
    Dieser Port ist Trunk-Port und wurde dadurch Mitglied in allen VLANs.
    Sie konfigurieren diese Funktion im CLI (Command Line Interface) mit Hilfe des Befehls "`switchport mode trunk`" oder im WBM unter "Schnittstellen > Ethernet > Konfiguration".

## Base Bridge-Modus wechseln

**VLAN-unaware (802.1D Transparent Bridge) → VLAN-aware (802.1Q VLAN Bridge)**

Wenn Sie den Base Bridge-Modus von VLAN-unaware in VLAN-aware ändern, hat dies folgende Auswirkungen:

- Alle statischen und dynamischen Unicast-Einträge werden gelöscht.

**VLAN-aware (802.1Q VLAN Bridge) → VLAN-unaware (802.1D Transparent Bridge)**

Wenn Sie den Base Bridge-Modus von VLAN-aware in VLAN-unaware ändern, hat dies folgende Auswirkungen:

- Alle VLAN-Konfigurationen werden gelöscht.
- Es wird ein Management-VLAN angelegt: VLAN 1.
- Alle statischen und dynamischen Unicast-Einträge werden gelöscht.

### 802.1Q VLAN Bridge: Wichtige Regeln für VLANs

Berücksichtigen Sie bei der Konfiguration und beim Betrieb Ihrer VLANs folgende Regeln:

- Telegramme mit der VLAN-ID "0" werden wie ungetaggte Telegramme behandelt, behalten jedoch ihren Prioritätswert.
- Alle Ports am Gerät senden standardmäßig Telegramme ohne VLAN-Tag, um sicher zu gehen, dass der Endteilnehmer diese Telegramme empfangen kann.
- Die werkseitige Zuordnung der Ports finden Sie im Kapitel "VLAN (Seite 67)".
- Die VLANs sind in verschiedenen IP-Subnetzen. Damit diese miteinander kommunizieren können, muss im Gerät die entsprechende Route und die Firewall-Regel konfiguriert sein.
- Wenn an einem Port ein Endteilnehmer angebunden ist, dann sollen ausgehende Telegramme ohne Tag versendet werden (statischer Zugriffs-Port). Wenn sich an dem Port ein weiterer Switch befindet, so ist das Telegramm mit einem Tag zu versehen (Trunk-Port).

### Vorgehensweise

**Voraussetzung:**

Bei Base Bridge-Modus ist "802.1Q VLAN Bridge" eingestellt

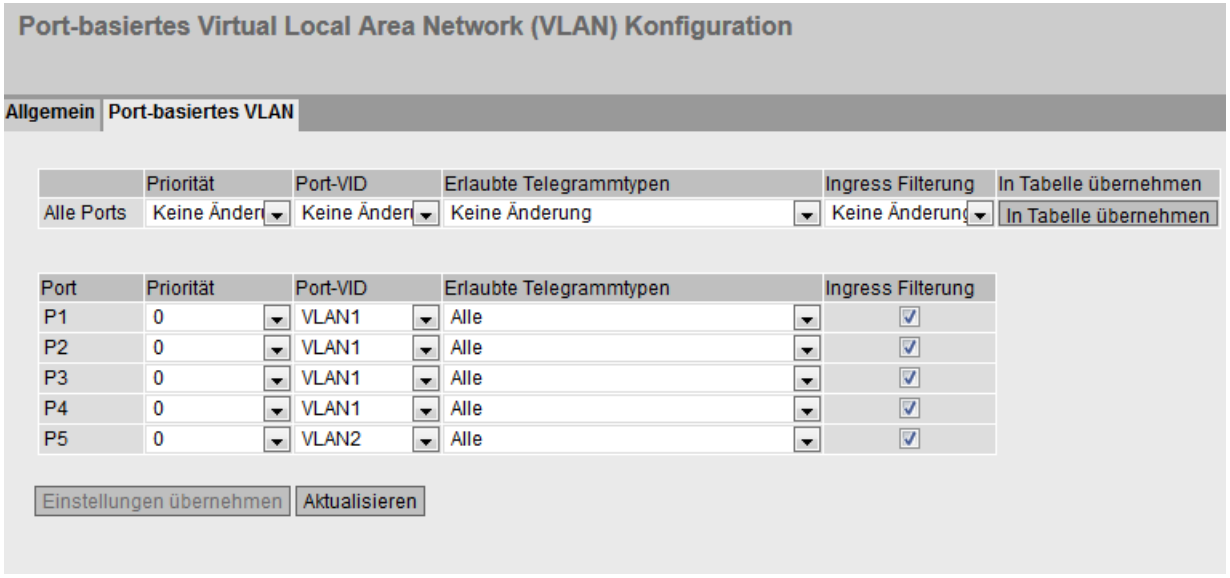
**Neues VLAN anlegen**

1. Tragen Sie im Eingabefeld "VLAN-ID" eine ID ein.
2. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag erzeugt. Die Felder sind standardmäßig mit "-" belegt.
3. Tragen Sie bei Name einen Namen für das VLAN ein.
4. Legen Sie die Verwendung der Ports in dem VLAN fest. Wenn Sie z. B. M auswählen, ist der Port Mitglied des VLANs. Das in diesem VLAN gesendete Telegramm wird mit dem entsprechenden VLAN-Tag weitergeleitet.
5. Legen Sie den Modus des Geräts fest.
6. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

### 5.7.2.2 Port-basiertes VLAN

#### Verarbeitung empfangener Telegramme

Auf dieser WBM-Seite legen Sie die Konfiguration der Port-Eigenschaften für den Telegrammempfang fest.




#### Beschreibung

Die Tabelle 1 gliedert sich in folgende Spalten:

- **Alle Ports**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **Priorität / Port-VID / Erlaubte Telegrammtypen / Ingress-Filterung**
  Wählen Sie in der Klappliste die Einstellung für alle Ports aus. Wenn "Keine Änderung" ausgewählt ist, bleiben die Einträge der entsprechenden Spalte in der Tabelle 2 unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt die verfügbaren Ports an.
- **Priorität**
  Wählen Sie die gewünschte Priorität aus, mit der ungetaggte Telegramme versehen werden. Die CoS-Priorität (Class of Service), die im VLAN-Tag verwendet wird. Wird ein Telegramm ohne Tag empfangen, wird ihm diese Priorität zugeordnet. Diese Priorität legt fest, wie dieses Telegramm im Vergleich zu anderen Telegrammen weiterhin bearbeitet wird.
  Es gibt insgesamt acht Prioritäten, mit den Werten 0 bis 7, wobei 7 der höchsten Priorität entspricht (IEEE 802.1p Port Priority).

- **Port-VID**
  Wählen Sie die gewünschte VLAN-ID aus. Nur die VLAN-IDs sind wählbar, die Sie unter "VLAN > Allgemein" definiert haben.
  Wenn ein empfangenes Telegramm kein VLAN-Tag hat, so wird es um ein Tag mit der hier angegebenen VLAN-ID ergänzt und entsprechend den Regeln am Port gesendet.
- **Erlaubte Telegrammtypen**
  Legen Sie fest, welche Arten von Telegrammen akzeptiert werden. Es gibt folgende Alternativen:
  - Nur getaggte Frames
    Das Gerät verwirft alle ungetaggten Telegramme. Andernfalls gelten die Weiterleitungsregeln entsprechend der Konfiguration.
  - All
    Das Gerät leitet alle Telegramme weiter.
- **Ingress Filterung**
  Legen Sie fest, ob die VID von empfangenen Telegrammen ausgewertet wird.
  Sie haben folgende Möglichkeiten:
  - Aktiviert
    Die VLAN ID empfangener Telegramme bestimmt die Weiterleitung: Für die Weiterleitung eines VLAN-getaggten Telegramms muss der Empfangsport Mitglied im selben VLAN sein. Am Empfangsport werden Telegramme aus unbekannten VLANs verworfen.
  - Deaktiviert
    Alle Telegramme werden weitergeleitet.

### Vorgehensweise zur Konfiguration

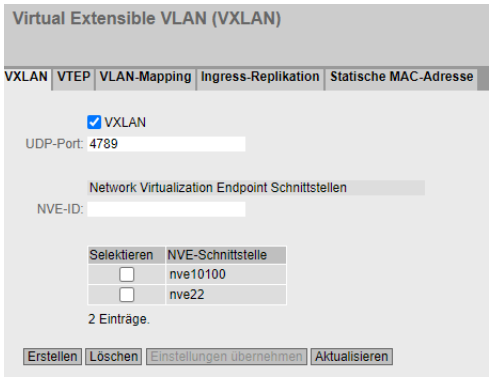
1. Klicken Sie in der Zeile des zu konfigurierenden Ports in das entsprechende Feld der Tabelle, um es zu konfigurieren.
2. Tragen Sie in die Eingabefelder die einzustellenden Werte ein.
3. Wählen Sie aus den Klapplisten die einzustellenden Werte aus.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

## 5.7.3 VXLAN (Nur beim MUM85x)

### 5.7.3.1 VXLAN

Auf dieser Seite definieren Sie VXLANs (Virtual eXtensible LAN). VXLAN ist eine virtuelle Netzwerktechnologie zur Erweiterung von VLAN und ermöglicht die Übertragung von Layer-2-Paketen über Layer-3-Netzwerke.

Die maximale Größe eines Pakets (MTU) bei VXLAN beträgt 1500 Bytes. Größere Pakete werden fragmentiert.




## Beschreibung

Die Seite enthält folgende Felder:

- **VXLAN**
  Aktiviert die Funktion VXLAN.
- **UDP-Port**
  Geben Sie den Ziel-Port des VXLAN ein.
  Wertebereich: 1000 ... 65535
  Standardmäßig ist der UDP-Port 4789 zugewiesen.
- **Network Virtual Endpoint Interface (NVE)**
  In diesem Bereich konfigurieren Sie die virtuelle Schnittstelle, über die der VXLAN-Tunnel aufgebaut wird.
  - **NVE-ID**
    Geben Sie eine Nummer für die NVE-Schnittstelle ein.
    Wertebereich: 1 ... 65535
- Die Tabelle enthält folgende Spalten.
  - **Selektieren**
    Wählen Sie die Zeile, die Sie löschen wollen.
  - **NVE-Schnittstelle**
    Zeigt die NVE-Schnittstelle an. Die Bezeichnung wird automatisch aus "nve" und der eingetragenen Nummer zusammengesetzt.

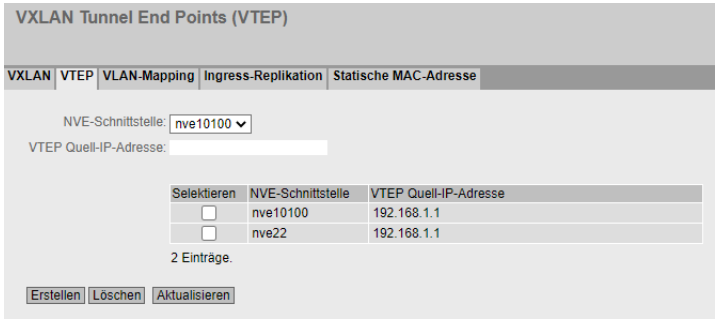
## Vorgehensweise

### Neues VXLAN anlegen

1. Aktivieren Sie das Optionskästchen "VXLAN".
2. Tragen Sie in den "UDP-Port" und die "NVE-ID" ein.
3. Klicken Sie auf die Schaltfläche "Erstellen".

### 5.7.3.2 VTEP

Auf dieser Seite nehmen Sie Einstellungen zu den VTEPs (VXLAN Tunnel End Point) vor. Die VTEPs bilden die Endpunkte im VXLAN, über welche die Verbindung abläuft. Endgeräte, die über einen VTEP im Zielnetz erreichbar sein sollen, stellen Sie im Register "Statische MAC-Adresse" ein.




## Beschreibung

Die Seite enthält folgende Felder:

- **NVE-Schnittstelle**
  Wählen Sie die gewünschte NVE-Schnittstelle aus. Nur die Schnittstellen auswählbar, die Sie im Register "VXLAN" angelegt haben.
- **VTEP Quell-IP-Adresse**
  Tragen Sie die IPv4-Adresse des Quell-VTEPs ein. Voraussetzung ist, dass die IPv4-Adresse auf dem Gerät angelegt ist. Die IPv4-Adresse konfigurieren unter "Layer 3 > Subnetze".

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **NVE-Schnittstelle**
  Zeigt die NVE-Schnittstelle an. Die ID der NVE-Schnittstelle kann nur beim Anlegen eines neuen Datensatzes einmalig vergeben werden und ist danach nicht mehr änderbar. Zur Änderung muss der gesamte Datensatz gelöscht und neu angelegt werden.
- **VTEP Quell-IP-Adresse**
  Zeigt die IPv4-Adresse des Quell-VTEPs an.

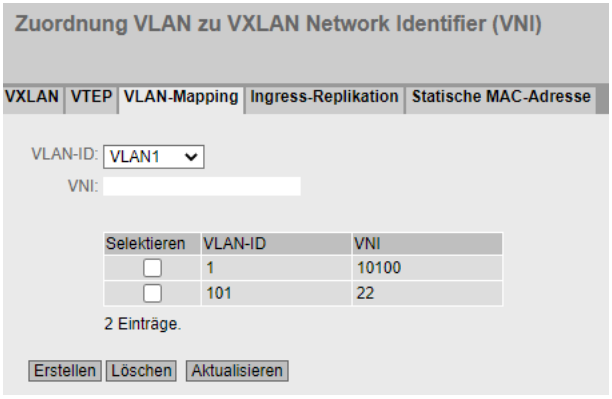
## Vorgehensweise

**Quell-IP-Adresse anlegen**

1. Wählen Sie die NVE-Schnittstelle aus.
2. Tragen Sie die entsprechende VTEP Quell-IP-Adresse ein.
3. Klicken Sie auf die Schaltfläche "Erstellen".

### 5.7.3.3 VLAN Mapping

Damit der VTEP den Ethernet-Frame in das richtige VLAN bzw. VXLAN weiterleitet, müssen Sie eine Zuordnung von VLAN-ID zu VNI konfigurieren.




## Beschreibung

Die Seite enthält folgende Felder:

- **VLAN-ID**
  Wählen Sie die gewünschte VLAN-ID aus. Nur VLANs mit konfiguriertem Subnetz sind auswählbar.
- **VNI**
  Tragen Sie die VNI ein, die der VLAN-ID zugeordnet wird. Die VNI kann mehreren VLAN-IDs zugeordnet werden.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **VLAN-ID**
  Zeigt die VLAN-ID an.
- **VNI**
  Zeigt die VNI an, die dem VLAN zugeordnet ist.

## Vorgehensweise

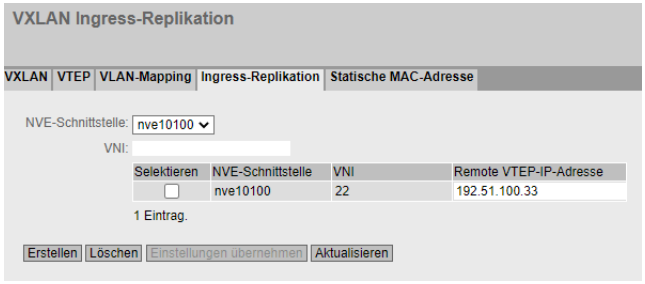
**Zuordnung anlegen**

1. Wählen Sie die gewünschte VLAN-ID aus.
2. Tragen Sie die VNI-ID ein, die der VLAN-ID zugeordnet wird.
3. Klicken Sie auf die Schaltfläche "Erstellen".

### 5.7.3.4 Ingress Replication

Wenn in einem VNI-Segment mehrere VTEPs vorhanden sind, weiß der Quell-VTEP nicht, hinter welchem Remote-VTEP sich der Empfänger des Ethernet-Frames befindet.

Auf dieser Seite tragen Sie ein, an welche Remote VTEP-IP-Adressen Ethernet-Frame gesendet werden. Der Quell-VTEP repliziert den empfangenen Ethernet-Frame und sendet den gekapselten Ethernet-Frame an die Remote-VTEPs.




## Beschreibung

Die Seite enthält folgende Felder:

- **NVE-Schnittstelle**
  Wählen Sie die gewünschte NVE-Schnittstelle aus.
- **VNI-ID**
  Tragen Sie die gewünschte VNI ein. Nur VXLAN-Netzwerke mit gleicher VNI-ID können miteinander kommunizieren.
  Wertebereich: 1 ... 16777215

Die Tabelle gliedert sich in folgende Spalten:

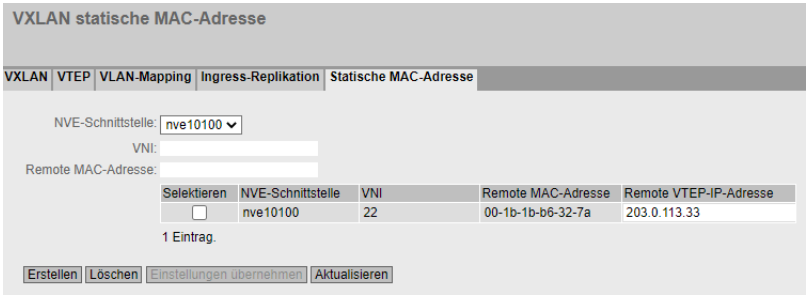
- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **NVE-Schnittstelle**
  Zeigt die ausgewählte NVE-Schnittstelle an.
- **VNI-ID**
  Zeigt die VNI-ID an.
- **Remote VTEP-IP-Adresse**
  Tragen Sie die IPv4-Adresse des Remote-VTEPs ein.
  Der replizierte Ethernet-Frame wird gekapselt und an diesen Remote-VTEP gesendet. Vorausgesetzt, der Remote-VTEP ist Mitglied in dem VNI-Segment.

## Vorgehensweise

1. Wählen Sie die NVE-Schnittstelle aus.
2. Tragen Sie im Eingabefeld "VNI-ID" eine ID ein.
3. Klicken Sie auf die Schaltfläche "Erstellen".
   In der Tabelle wird ein neuer Eintrag erzeugt.
4. Tragen Sie die Remote VTEP-IP-Adresse an.
5. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

### 5.7.3.5 Statische MAC-Adresse

Auf dieser Seite können Sie die MAC-Adressen von Geräten im Zielnetz eintragen, die über einen Remote VTEP erreicht werden sollen. Der Eintrag wird unter "Information > VXLAN" angezeigt.




## Beschreibung

Die Seite enthält folgende Felder:

- **NVE-Schnittstelle**
  Wählen Sie die NVE-Schnittstelle aus, über die der Remote-VTEP erreichbar sein kann. Es sind nur die Schnittstellen wählbar, die Sie im Register "VXLAN" angelegt haben.
- **VNI-ID**
  Tragen Sie die VNI-ID (VXLAN Network Identifier) ein. Nur VTEPs, die Mitglieder im gleichen VXLAN-Segment sind, können miteinander kommunizieren.
- **Remote MAC-Adresse**
  Tragen Sie die MAC-Adresse des Endgeräts im Zielnetz ein, das über den in der Tabelle eingetragenen VTEP erreicht werden soll.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **NVE-Schnittstelle**
  Zeigt die NVE-Schnittstelle an.
- **VNI**
  Zeigt den VNI an. Der VNI kann nur beim Anlegen eines neuen Datensatzes einmalig vergeben werden und ist danach nicht mehr änderbar. Zur Änderung muss der gesamte Datensatz gelöscht und neu angelegt werden.
- **Remote MAC-Adresse**
  Zeigt die MAC-Adresse des Endgeräts im Zielnetz an.
- **Remote VTEP-IP-Adresse**
  Tragen Sie die IPv4-Adresse des VTEP ein, über die das Endgerät mit der eingetragenen Remote MAC-Adresse im Zielnetz erreichbar ist.

## Vorgehensweise

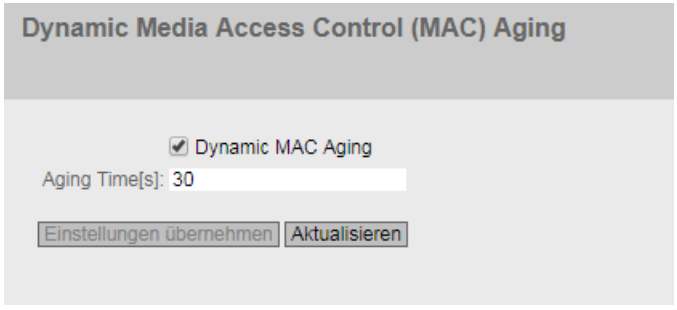
1. Wählen Sie die NVE-Schnittstelle aus.
2. Tragen Sie im Eingabefeld "VNI-ID" eine ID ein.

3. Tragen Sie die Remote MAC-Adresse ein.
4. Klicken Sie auf die Schaltfläche "Erstellen".
   In der Tabelle wird ein neuer Eintrag erzeugt.
5. Tragen Sie die Remote VTEP-IP-Adresse an.
6. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

## 5.7.4 Dynamic MAC Aging

### Protokolleinstellungen und Switch-Funktionalität

Das Gerät lernt automatisch die Quelladressen der angeschlossenen Teilnehmer. Diese Information wird dazu benutzt, um Datentelegramme gezielt an die betroffenen Teilnehmer weiterzuleiten. Dadurch wird die Netzlast für die anderen Teilnehmer reduziert.
Erhält ein Gerät innerhalb einer bestimmten Zeitspanne kein Telegramm, dessen Quelladresse mit einer gelernten Adresse übereinstimmt, dann löscht es die gelernte Adresse. Dieser Mechanismus wird als "Aging" bezeichnet. Durch Aging wird verhindert, dass Telegramme fehlgeleitet werden, wenn z. B. ein Endgerät an einen anderen Port angeschlossen wird.
Wenn die Option nicht aktiviert ist, löscht ein Gerät gelernte Adressen nicht automatisch.



### Beschreibung der angezeigten Felder

Die Seite enthält folgende Felder:

- **Dynamic MAC Aging**
  Aktivieren oder deaktivieren Sie die Funktion zum automatischen Aging von gelernten MAC-Adressen.
- **Aging Time[s]**
  Tragen Sie die Zeitspanne in Sekunden in 15er-Schritten ein. Nach dieser Zeitspanne wird eine gelernte Adresse gelöscht, wenn das Gerät keine weiteren Telegramme von dieser Absenderadresse mehr empfängt.
  Wertebereich: 15 - 630 Sekunden

**Hinweis**

**Rundungen der Werte, Abweichung vom Sollwert**

Beachten Sie bei der Eingabe der Aging Time, dass auf korrekte Werte gerundet wird. Wenn Sie einen Wert eingeben, der nicht durch 15 teilbar ist, wird der Wert automatisch abgerundet.

### Vorgehensweise zur Konfiguration

1. Aktivieren Sie das Optionskästchen "Dynamic MAC Aging".
2. Tragen Sie in das Eingabefeld "Aging Time[s]" die Zeitspanne in Sekunden ein.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

## 5.7.5 Spanning Tree

### 5.7.5.1 Allgemein

Dies ist die Basisseite zu Spanning Tree. Standardmäßig ist Rapid Spanning Tree aktiviert.



### Beschreibung

Die Seite enthält folgende Felder:

- **Spanning Tree**
  Aktivieren oder deaktivieren Sie Spanning Tree.
- **Protokollkompatibilität**
  Folgende Einstellung gibt es:
  – RSTP

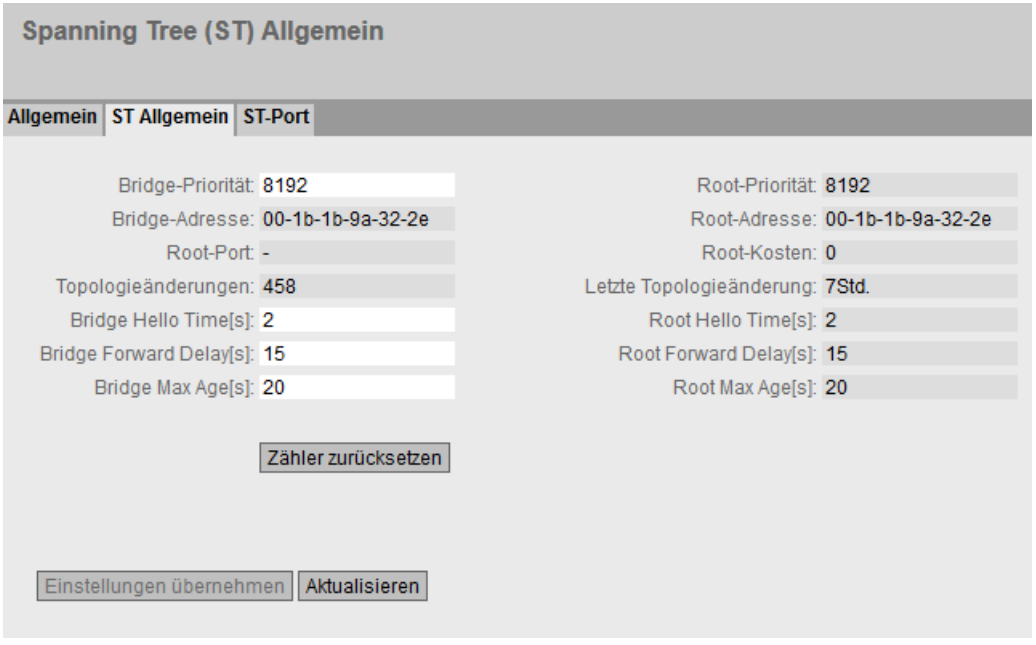
### Vorgehensweise

1. Aktivieren Sie das Optionskästchen "Spanning Tree".
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

## 5.7.5.2 ST Allgemein

Die Seite besteht aus folgenden Teilen:

- Der linke Teil der Seite zeigt die Konfiguration des Geräts.
- Der rechte Teil zeigt die Konfiguration der Root-Bridge, wie sie aus Spanning Tree-Telegrammen abgeleitet werden kann, die ein Gerät empfangen hat.



## Beschreibung

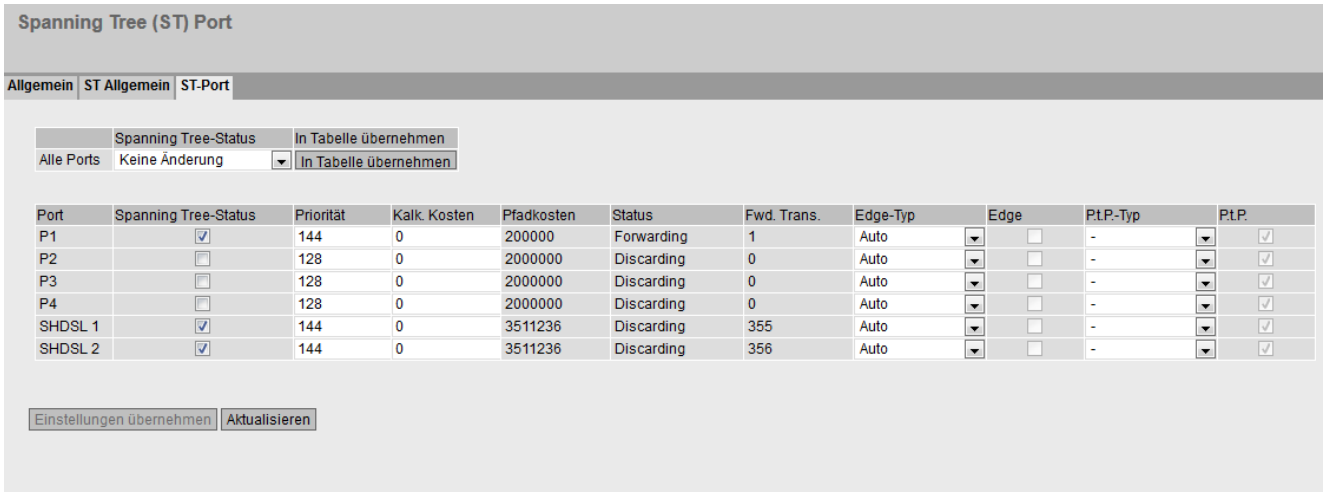
Die Seite enthält folgende Felder:

- **Bridge-Priorität / Root-Priorität**
  Anhand der Bridge-Priorität wird festgelegt, welches Gerät Root Bridge wird. Die Bridge mit der höchsten Priorität (d. h. dem kleinsten Wert für diesen Parameter) wird Root Bridge. Wenn in einem Netz mehrere Geräte die gleiche Priorität besitzen, dann wird das Gerät Root Bridge, dessen MAC-Adresse den niedrigsten Zahlenwert hat. Beide Parameter, Bridge-Priorität und MAC-Adresse, bilden zusammen die Bridge-Kennung. Da die Root Bridge alle Wegeänderungen verwaltet, sollte sie wegen der Laufzeit der Telegramme möglichst zentral angeordnet sein.
  Der Wert für die Bridge-Priorität ist ein ganzzahliges Vielfaches von 4096. Wertebereich: 0 - 61440
- **Bridge-Adresse / Root-Adresse**
  Die Bridge-Adresse zeigt die MAC-Adresse des Geräts und die Root-Adresse zeigt die MAC-Adresse der Root-Bridge an.
- **Root-Port**
  Zeigt den Port an, über den der Switch mit der Root-Bridge kommuniziert.
- **Root-Kosten**
  Die Pfadkosten von diesem Gerät bis zur Root-Bridge
- **Topologieänderungen / Letzte Topologieänderung**
  Die Angabe für das Gerät nennt die Zahl der Umkonfigurationen aufgrund des Spanning Tree-Mechanismus seit dem letzten Hochlauf. Für die Root-Bridge wird die Zeitdauer seit der letzten Umkonfiguration wie folgt angezeigt:
  - Sekunden: Zusatz "Sek." hinter der Zahlenangabe
  - Minuten: Zusatz "Min." hinter der Zahlenangabe
  - Stunden: Zusatz "Std." hinter der Zahlenangabe
- **Bridge Hello Time[s] / Root Hello Time[s]**
  Jede Bridge versendet regelmäßig Konfigurationstelegramme (BPDUs). Der Zeitabstand zwischen zwei Konfigurationstelegrammen ist die "Hello Time".
  Werkseinstellung: 2 Sekunden
- **Bridge Forward Delay[s] / Root Forward Delay[s]**
  Neue Konfigurationsinformationen werden von einer Bridge nicht sofort angewendet, sondern erst nach dem im Parameter "Forward Delay" festgelegten Zeitraum. So wird sichergestellt, dass der Betrieb entsprechend der neuen Topologie erst gestartet wird, wenn alle Bridges die notwendigen Informationen haben.
  Werkseinstellung: 15 Sekunden
- **Bridge Max Age[s] / Root Max Age[s]**
  Wenn die BPDU älter ist als das angegebene "Max Age", wird sie verworfen.
  Werkseinstellung: 20 Sekunden
- **Zähler zurücksetzen**
  Klicken Sie auf diese Schaltfläche, um die Zähler auf dieser Seite zurückzusetzen.

### 5.7.5.3 ST-Port

In der Tabelle wird beim Aufruf der Seite der aktuelle Stand der Konfiguration der Port-Parameter angezeigt.

Klicken Sie zur Konfiguration in die entsprechenden Felder der Port-Tabelle.




## Beschreibung

Die Tabelle 1 gliedert sich in folgende Spalten:

- **Alle Ports**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **Spanning Tree-Status**
  Wählen Sie in der Klappliste die Einstellung für alle Ports aus. Wenn "Keine Änderung" ausgewählt ist, bleiben die Einträge der entsprechenden Spalte in der Tabelle 2 unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt alle verfügbaren Ports an.
- **Spanning Tree-Status**
  Legen Sie fest, ob der Port im Spanning-Tree integriert ist oder nicht.

**Hinweis**

Wenn Sie die Option "Spanning Tree Status" für einen Port deaktivieren, kann es zur Schleifenbildung kommen. Die Topologie muss beachtet werden.

- **Priorität**
  Tragen Sie die Priorität des Ports ein. Die Priorität wird nur ausgewertet, wenn die Pfadkosten gleich sind.
  Der Wert muss durch 16 teilbar sein. Wenn der Wert nicht durch 16 teilbar ist, wird der Wert automatisch angepasst.
  Wertebereich: 0 - 240.
  Der Standardwert ist 128.
- **Kalk. Kosten**
  Tragen Sie die Wegekostenberechnung ein. Wenn Sie den Wert "0" eintragen, wird im Feld "Pfadkosten" der automatisch ermittelte Wert angezeigt.
- **Pfadkosten**
  Dieser Parameter dient zur Berechnung des zu wählenden Weges. Die Strecke mit dem geringsten Wert wird als Weg ausgewählt. Haben mehrere Ports eines Geräts den gleichen Wert bei gleichen Pfadkosten, wird der Port mit der niedrigsten Portnummer ausgewählt. Wenn im Feld "Kalk. Kosten" der Wert "0" ist, wird der automatisch ermittelte Wert angezeigt. Wenn ein Wert ungleich "0" eingetragen wird, wird der Wert des Feldes "Kalk. Kosten" angezeigt.
  Die Ermittlung der Wegekosten richtet sich maßgeblich nach der Übertragungsgeschwindigkeit. Je höher die erzielbare Übertragungsgeschwindigkeit ist, umso kleiner ist der Wert für die Wegekosten.
  Typische Werte für Wegekosten bei Rapid Spanning Tree:
  - 10.000 Mbit/s = 2.000
  - 1000 Mbit/s = 20.000
  - 100 Mbit/s = 200.000
  - 10 Mbit/s = 2.000.000

  Die Werte können aber auch individuell parametriert werden.
- **Status**
  Zeigt den momentanen Status an, in dem sich der Port befindet. Die Werte werden nur angezeigt und können nicht parametriert werden. Der Parameter "Status" ist abhängig von dem projektierten Protokoll. Folgende Werte sind möglich:
  - Disabled
    Der Port empfängt nur und nimmt nicht am STP, MSTP und RSTP teil.
  - Discarding
    In der Betriebsart "Discarding" werden BPDU-Telegramme empfangen. Andere aus- oder eingehende Telegramme werden verworfen.
  - Listening
    In diesem Status werden sowohl BPDU-Telegramme empfangen als auch gesendet. Der Port ist in den Spanning Tree-Algorithmus einbezogen.
  - Learning
    Vorstufe zum Status "Forwarding", der Port lernt aktiv die Topologie (d. h. die Teilnehmeradressen).
  - Forwarding
    Der Port ist nach der Umkonfigurationszeit aktiv im Netz, er empfängt und sendet Datentelegramme.

- **Fwd. Trans**
  Gibt die Anzahl der Wechsel vom Status "Discarding" zum Status "Forwarding" an.
- **Edge Type**
  Legen Sie die Art des "Edge Port" fest. Sie haben folgende Möglichkeiten:
  - "-"
    Edge Port ist deaktiviert. Der Port wird wie ein "no Edge Port" behandelt.
  - Admin
    Wählen Sie diese Option, wenn sich an diesem Port immer ein Endgerät befindet. Sonst wird bei jeder Verbindungsänderung eine Rekonfiguration des Netzwerks ausgelöst.
  - Auto
    Wählen Sie diese Option, wenn an diesem Port automatisch erkannt werden soll, ob ein Endgerät angeschlossen ist. Beim ersten Verbindungsaufbau wird der Port wie ein "no Edge Port" behandelt.
  - Admin/Auto
    Wählen Sie diese Optionen, wenn Sie an diesem Port eine Kombination aus beiden betreiben. Beim ersten Verbindungsaufbau wird der Port als "Edge Port" behandelt.
- **Edge**
  Zeigt an, in welchem Status der Port ist.
  - Aktiviert
    An diesem Port befindet sich ein Endgerät.
  - Deaktiviert
    An diesem Port befindet sich ein Spanning Tree- oder Rapid Spanning Tree-Gerät.

  Bei einem Endgerät kann ein Switch ohne Rücksicht auf Spanning Tree-Telegramme schneller den Port umschalten. Wird entgegen dieser Einstellung ein Spanning Tree-Telegramm empfangen, wechselt der Port automatisch auf die Einstellung "Deaktiviert".
- **P.t.P.-Typ**
  Wählen Sie in der Klappliste die gewünschte Option aus. Die Auswahl ist abhängig vom eingestellten Port.
  - "-"
    Punkt zu Punkt wird automatisch ermittelt. Steht der Port auf Halbduplex, wird nicht von einer Punkt-zu-Punkt-Verbindung ausgegangen.
  - P.t.P.
    Auch bei Halbduplex wird von einer Punkt-zu-Punkt-Verbindung ausgegangen.
  - Shared Media
    Auch bei einer Vollduplexverbindung wird nicht von einer Punkt-zu-Punkt-Verbindung ausgegangen.

    **Hinweis**

    Punkt-zu-Punkt-Verbindung bedeutet eine direkte Verbindung zwischen zwei Geräten. Eine Shared Media-Verbindung ist z. B. eine Verbindung zu einem Hub.

## 5.7.6 LLDP

### Bestimmung der Netzwerktopologie

LLDP (Link Layer Discovery Protocol) ist im Standard IEEE 802.1 AB definiert.

LLDP ist ein Verfahren zur Bestimmung der Netzwerktopologie. Netzwerkkomponenten tauschen über LLDP Informationen mit ihren Nachbargeräten aus.

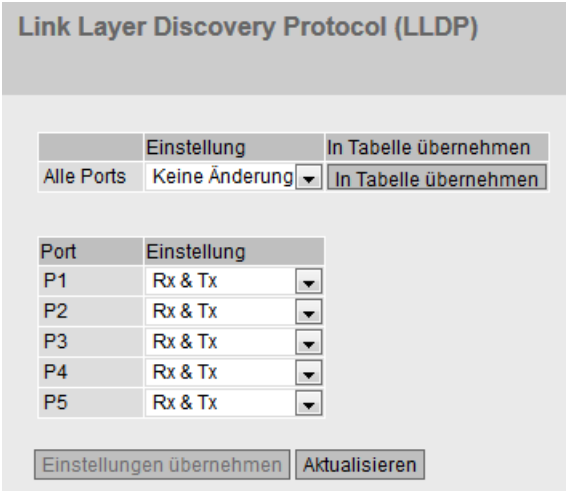
Netzwerkkomponenten, die LLDP unterstützen, verfügen über einen LLDP-Agenten. Der LLDP-Agent versendet in periodischen Abständen Informationen über sich selbst und empfängt Informationen von angeschlossenen Geräten. Die empfangenen Informationen werden in der MIB gespeichert.

### Anwendungen

PROFINET benutzt LLDP für die Topologie-Diagnose.  In der Werkseinstellung ist LLDP an allen verfügbaren Ports aktiviert, d. h. es werden LLDP-Telegramme auf den Ports gesendet.

Die gesendeten Informationen werden auf jedem LLDP-fähigen Gerät in einer LLDP-MIB-Datei gespeichert. Netzwerkmanagementsysteme können auf diese LLDP-MIB-Dateien mit Hilfe von SNMP zugreifen und damit die vorliegende Netzwerktopologie nachbilden.
Ein Administrator kann auf die Weise z. B. feststellen, welche Netzwerkkomponenten miteinander verbunden sind und auftretende Störungen lokalisieren.

Auf dieser Seite haben Sie die Möglichkeit das Aussenden und/oder Empfangen pro Port ein- oder auszuschalten.




### Beschreibung

Tabelle 1 gliedert sich in folgende Spalten:

Die Tabelle 1 ist nur verfügbar, wenn das Gerät mehr als einen Port hat.

- **Alle Ports**
  Zeigt an, dass die Einstellungen für alle Ports gültig sind.
- **Einstellung**
  Wählen Sie aus der Klappliste die Einstellung. Wenn "Keine Änderung" ausgewählt ist, bleibt der Eintrag in der Tabelle 2 unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt die verfügbaren Ports an.
- **Einstellung**
  Legen Sie die LLDP-Funktionalität fest. Folgende Möglichkeiten gibt es:
  - Rx
    Dieser Port kann LLDP-Telegramme nur empfangen.
  - Tx
    Dieser Port kann LLDP-Telegramme nur senden.
  - Rx & Tx
    Dieser Port kann LLDP-Telegramme empfangen und senden.
  - "-" (Deaktiviert)
    Dieser Port kann LLDP-Telegramme weder empfangen noch senden.

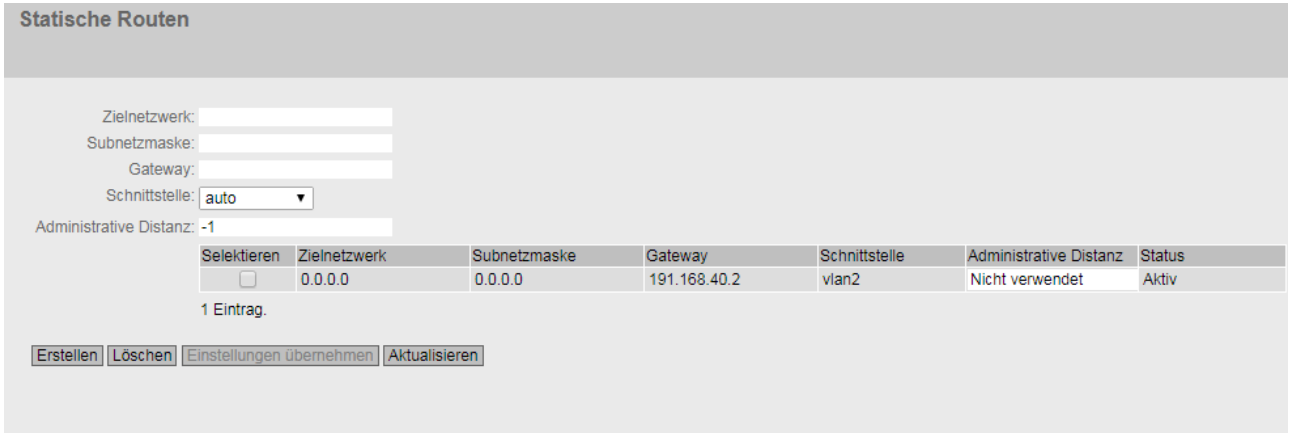
## Vorgehensweise

1. Wählen Sie aus der Klappliste "Einstellung" die LLDP-Funktionalität des Ports aus.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

# 5.8 Menü "Layer 3 (IPv4)"

## 5.8.1 Statische Routen

Auf dieser Seite legen Sie fest, über welche Routen ein Datenaustausch zwischen den verschiedenen Subnetzen stattfinden kann. Dynamische Routingprotokolle werden nicht unterstützt, z. B. RIP, OSPF.




### Beschreibung

Die Seite enthält folgende Felder:

- **Zielnetzwerk**
  Tragen Sie die Netzwerkadresse des Ziels ein, das über diese Route erreichbar ist.
- **Subnetzmaske**
  Tragen Sie die dazugehörende Subnetzmaske ein.
- **Gateway**
  Tragen Sie die IPv4-Adresse des Gateways ein, über den diese Netzwerkadresse erreichbar ist.
- **Schnittstelle**
  Legen Sie fest, ob die Netzwerkadresse über eine bestimmte Schnittstelle oder über das Gateway (auto) erreichbar ist.
- **Administrative Distanz**
  Tragen Sie die Metrik für die Route ein. Die Metrik entspricht der Güte einer Verbindung, z. B. Geschwindigkeit, Kosten. Bei mehreren gleichen Routen wird die Route mit dem kleinsten Metrik-Wert benutzt.
  Wenn Sie nicht eintragen, wird automatisch "nicht verwendet" eingetragen. Die Metrik ist nachträglich änderbar.
  Wertebereich: 1 - 255 oder -1 für "not used".
  Dabei ist 1 der Wert für die bestmögliche Route. Je größer der Wert, desto länger benötigen Pakete zu Ihrem Ziel.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Zielnetzwerk**
  Zeigt die Netzwerkadresse des Ziels an.
- **Subnetzmaske**
  Zeigt die dazugehörende Subnetzmaske an.
- **Gateway**
  Zeigt die IPv4-Adresse des nächsten Gateways an.
- **Schnittstelle**
  Zeigt die Schnittstelle der Route an.
- **Administrative Distanz**
  Tragen Sie die Metrik für die Route ein. Beim Erstellen der Route wird automatisch "nicht verwendet" eingetragen. Die Metrik entspricht der Güte einer Verbindung, basierend z. B. auf Geschwindigkeit oder Kosten. Bei mehreren gleichen Routen wird die Route mit dem kleinsten Metrik-Wert benutzt.
  Wertebereich: 1 - 255
  Dabei ist 1 der Wert für die bestmögliche Route. Je größer der Wert, desto länger benötigen die Pakete zu Ihrem Ziel.
- **Status**
  Zeigt an, ob die Route aktiv ist oder nicht.

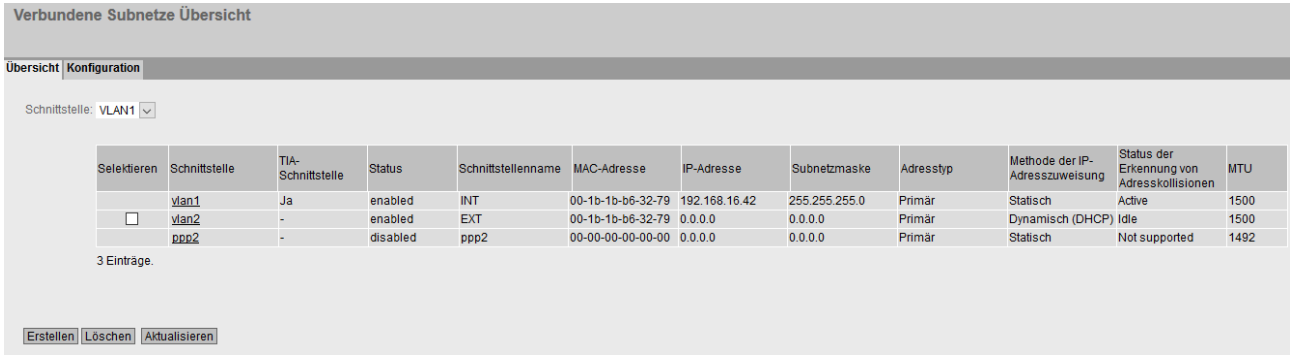
## Vorgehensweise

1. Tragen Sie in das Eingabefeld "Zielnetzwerk" die Netzwerkadresse des Ziels ein.
2. Tragen Sie in das Eingabefeld "Subnetzmaske" die dazugehörende Subnetzmaske ein.
3. Wählen Sie bei "Schnittstelle" den Eintrag "auto" aus.
4. Tragen Sie in das Eingabefeld "Gateway" das Gateway ein.
5. Tragen Sie bei "Administrative Distanz" die Gewichtung der Route ein.
6. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag erzeugt.
7. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

## 5.8.2 Subnetze

### 5.8.2.1 Übersicht

Die Seite zeigt die Subnetze für die ausgewählte Schnittstelle. Ein Subnetz bezieht sich immer auf eine Schnittstelle und wird auf dem Register "Konfiguration" angelegt.




### Beschreibung

Die Seite enthält folgendes Feld:

- **Schnittstelle**
  Wählen Sie die gewünschte Schnittstelle aus, an die Sie ein weiteres Subnetz projektieren.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Schnittstelle**
  Zeigt die Schnittstelle an.
- **TIA-Schnittstelle**
  Zeigt an, ob die Schnittstelle eine TIA-Schnittstelle ist.
- Status
  Zeigt an, ob die Schnittstelle aktiviert ist oder nicht.
- **Schnittstellenname**
  Zeigt den Namen der Schnittstelle.
- **MAC-Adresse**
  Zeigt die MAC-Adresse an.
- **IP-Adresse**
  Zeigt die IPv4-Adresse des Subnetzes an.
- **Subnetzmaske**
  Zeigt die Subnetzmaske.

- **Adresstyp**
  Zeigt den Adressentyp an. Folgende Werte sind möglich:
  - Primär
    Die erste IPv4-Adresse, die auf der IPv4-Schnittstelle konfiguriert wurde.
  - Sekundär
    Alle weiteren IPv4-Adressen, die auf der IPv4-Schnittstelle konfiguriert wurden.
- **Methode der IP-Adresszuweisung**
  Zeigt an, wie die IPv4-Adresse zugeordnet wird. Folgende Werte sind möglich:
  - Statisch
    Die IPv4-Adresse ist statisch. Tragen Sie die Einstellungen bei "IP-Adresse" und "Subnetzmaske" ein.
  - Dynamisch (DHCP)
    Das Gerät bezieht eine dynamische IPv4-Adresse von einem DHCPv4-Server.
- **Status der Erkennung von Adresskollisionen**
  Wenn neue IPv4-Adressen im Netz aktiv werden, prüft die Funktion "Erkennung von Adresskollisionen ", ob es zu Adresskollisionen kommen kann. Dadurch werden IPv4-Adressen erkannt, die doppelt vergeben werden sollen.

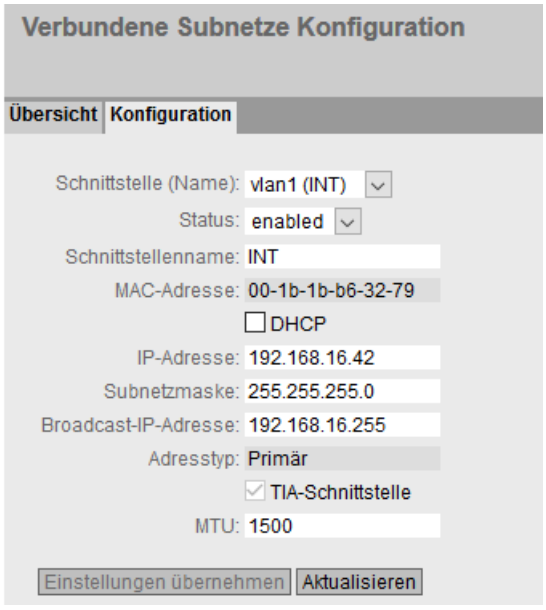
  **Hinweis**

  Die Funktion führt keine zyklische Prüfung durch.

  Diese Spalte zeigt an, in welchem Status sich die Funktion befindet. Folgende Werte sind möglich:
  - Idle
    Die Schnittstelle ist nicht aktiv und besitzt keine IPv4-Adresse.
  - Starting
    Dieser Status bezeichnet die Anlaufphase. In dieser Phase sendet das Gerät zunächst eine Anfrage, ob es die geplante IPv4-Adresse bereits gibt. Wenn die Adresse noch nicht vergeben ist, sendet das Gerät die Mitteilung, dass es ab jetzt diese IP-Adresse verwendet.
  - Conflict
    Die Schnittstelle ist nicht aktiv. Die Schnittstelle versucht eine IPv4-Adresse zu verwenden, die bereits vergeben ist.
  - Defending
    Die Schnittstelle verwendet eine eindeutige IPv4-Adresse. Eine andere Schnittstelle versucht die gleiche IPv4-Adresse zu verwenden.
  - Active
    Die Schnittstelle verwendet eine eindeutige IPv4-Adresse. Es gibt keine Kollisionen.
  - Not supported
    Die Funktion zur Erkennung von Adresskollisionen wird nicht unterstützt.
  - Disabled
    Die Funktion zur Erkennung von Adresskollisionen ist deaktiviert.
- **MTU**
  Zeigt die Paketgröße an.

### 5.8.2.2 Konfiguration

Auf dieser Seite konfigurieren Sie das Subnetz für die Schnittstelle.




## Beschreibung

Die Seite enthält Folgendes:

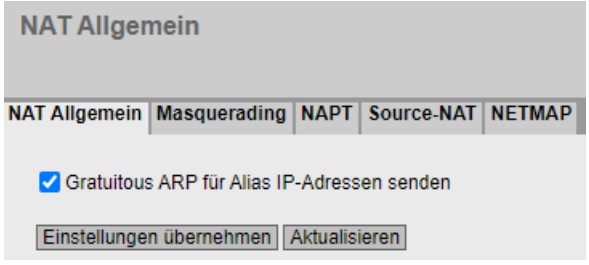
- **Schnittstelle (Name)**
  Wählen Sie aus Klappliste die Schnittstelle aus.
- **Status**
  Aktivieren oder deaktivieren Sie die Schnittstelle.
- **Schnittstellenname**
  Tragen Sie den Namen für die Schnittstelle ein.
- **MAC-Adresse**
  Zeigt die MAC-Adresse der ausgewählten Schnittstelle an.
- **DHCP**
  Wenn aktiviert, bezieht die Schnittstelle die IPv4-Adresse von einem DHCP-Server.
- **IP-Adresse**
  Tragen Sie die IPv4-Adresse der Schnittstelle ein. Die IPv4-Adressen dürfen nicht mehrfach verwendet werden.
- **Subnetzmaske**
  Tragen Sie die Subnetzmaske des zu erstellenden Subnetzes ein. Subnetze an unterschiedlichen Schnittstellen dürfen sich nicht überlappen.
- **Broadcast-IP-Adresse**
  Wenn eine bestimmte IP-Adresse als Broadcast-IP-Adresse des Subnetzes verwendet werden soll, dann tragen Sie diese ein. Ansonsten wird die letzte IP-Adresse des Subnetzes verwendet.

- **Adresstyp**
  Zeigt den Adressen Typ an. Folgende Werte sind möglich:
  - Primär
    Das erste Subnetz der Schnittstelle.
  - Sekundär
    Alle weiteren Subnetze der Schnittstelle.
- **TIA-Schnittstelle**
  Wählen Sie aus, ob diese Schnittstelle zur TIA-Schnittstelle wird. Über die TIA-Schnittstelle wird definiert, auf welchem VLAN die PROFINET Funktionalitäten zur Verfügung stehen. Dies betrifft hauptsächlich die Gerätesuche mit oder über DCP.
- **MTU**
  Mit MTU (Maximum Transmission Unit) wird die maximale Größe des Pakets festgelegt. Wenn die Pakete größer sind als die eingestellte MTU, werden Sie fragmentiert. Die MTU deckt die IP-Header und die Header der höheren Schichten (Layer) ab.
  Der Wertebereich ist von 90 bis 1500 Bytes.

## 5.8.3 NAT

### 5.8.3.1 NAT Allgemein

Auf dieser WBM-Seite aktivieren Sie Gratuitous ARP für Alias IP-Adressen.



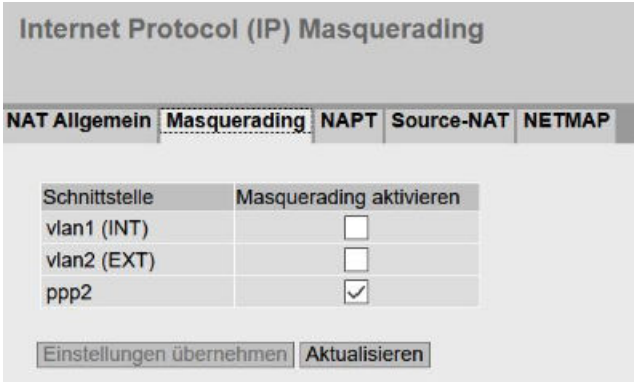

#### Beschreibung

Auf dieser Seite könne Sie die folgende Option aktivieren:

- **Gratuitous ARP für Alias IP-Adressen senden**
  Wenn die Option aktiviert ist, wird für jede Alias IP-Adresse ein Gratuitous ARP versendet. Dadurch wird die IP-Adresse im Netzwerk bekannt gemacht und die anderen Geräte können ihren ARP-Cache aktualisieren. Das Gratuitous ARP wird nur zum Konfigurationszeitpunkt versendet, also beim Gerätehochlauf oder wenn eine NAT-Regel (NETMAP) konfiguriert wird.

### 5.8.3.2 Masquerading

Auf dieser WBM-Seite aktivieren Sie die Regeln für IP-Masquerading.




#### Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

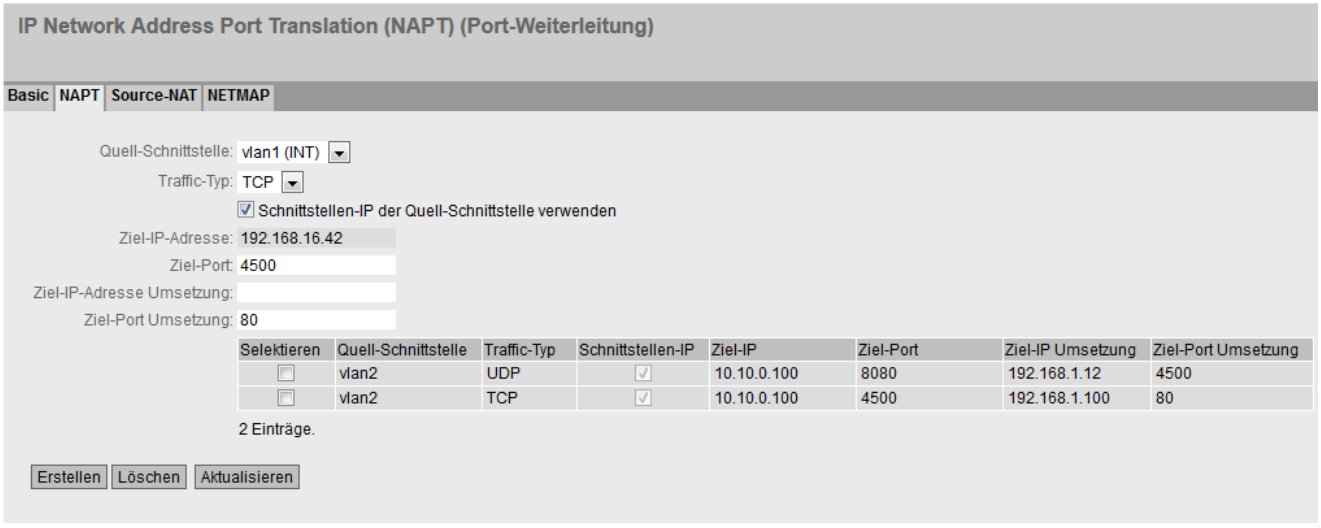
- **Schnittstelle**
  Schnittstelle, auf die sich die Einstellung bezieht. Nur Schnittstellen mit konfiguriertem Subnetz sind verfügbar.
- **Masquerading aktivieren**
  Wenn aktiviert, wird bei jedem ausgehenden Datenpaket, das über diese Schnittstelle gesendet wird, die Quell-IP-Adresse durch die IP-Adresse der Schnittstelle ersetzt.

### 5.8.3.3 NAPT

Auf dieser WBM-Seite können Sie zusätzlich zur Adressumsetzung auch eine Port-Umsetzung konfigurieren.

Folgende Port-Umsetzungen sind möglich:

- Von einem einzigen Port zu dem gleichen Port:
  Wenn die Ports gleich sind, werden die Telegramme ohne Port-Umsetzung weitergeleitet.
- Von einem einzigen Port zu einem einzigen Port
  Die Telegramme werden auf den Port umgesetzt.
- Von einem Port-Bereich zu einem einzigen Port
  Die Telegramme aus dem Port-Bereich werden auf den gleichen Port umgesetzt (n:1).
- Von einem Port-Bereich zu dem gleichen Port-Bereich
  Wenn die Port-Bereiche gleich sind, werden die Telegramme ohne Port-Umsetzung weitergeleitet.




## Beschreibung

Die Seite enthält folgende Felder:

- **Quell-Schnittstelle**
  Wählen Sie die Schnittstelle aus, auf der die Anfragen eintreffen sollen.
- **Traffic-Typ**
  Legen Sie fest, für welches Protokoll die Adresszuordnung gültig ist.
- **Schnittstellen-IP der Quell-Schnittstelle verwenden**
  Wenn aktiviert, wird bei "Ziel-IP-Adresse" die IP-Adresse der ausgewählten Schnittstelle verwendet.
- **Ziel-IP**
  Geben Sie die Ziel-IP-Adresse ein. An dieser IP-Adresse werden die Telegramme empfangen. Nur editierbar, wenn "Schnittstellen-IP der Quell-Schnittstelle verwenden" deaktiviert ist.
- **Ziel-Port**
  Geben Sie den Ziel-Port ein. Eingehende Telegramme mit diesem Port als Ziel-Port werden weitergeleitet. Wenn die Einstellung für einen Port-Bereich gelten soll, geben Sie den Bereich mit Start-Port "-" End-Port an, z. B. 30 - 40.
- **Ziel-IP-Umsetzung**
  Geben Sie die IP-Adresse des Teilnehmers an, an den dieses Telegramm weitergeleitet wird.
- **Ziel-Port-Umsetzung**
  Geben Sie die Nummer des Ports ein. Das ist der neue Ziel-Port, an den das eingehende Telegramm weitergeleitet wird. Wenn die Einstellung für einen Port-Bereich gelten soll, geben Sie den Bereich mit Start-Port "-" End-Port an, z. B. 30 - 40.

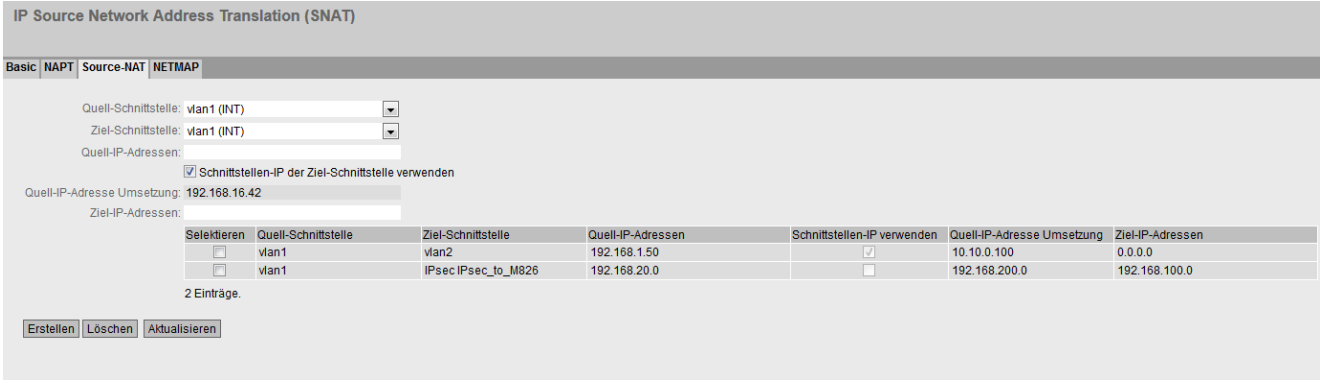
Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Quell-Schnittstelle**
  Zeigt die Schnittstelle an, von dem die Pakete kommen müssen. Nur diese Pakete kommen für eine Portweiterleitung in Frage.

- **Traffic-Typ**
  Zeigt an, für welches Protokoll die Adresszuordnung gilt.
- **Schnittstellen-IP**
  Zeigt an, ob die IP-Adresse der Schnittstelle verwendet wird.
- **Ziel-IP**
  Zeigt die Ziel-IP-Adresse an. An dieser IP-Adresse werden die Telegramme empfangen.
- **Ziel-Port**
  Zeigt den Ziel-Port an. Eingehende Telegramme mit diesem Port als Ziel-Port werden weitergeleitet.
- **Ziel-IP-Umsetzung**
  Zeigt die IP-Adresse Teilnehmers an, an dem die Pakete weitergeleitet werden.
- **Ziel-Port-Umsetzung**
  Zeigt an auf welchen Ziel-Port übersetzt wird.

### 5.8.3.4 Source-NAT

Auf dieser Seite konfigurieren Sie die Regeln für Source-NAT.




**Hinweis**

**Firewallregel bei Source-NAT**

Die Adressumsetzung mit Source-NAT wird erst nach der Firewall durchgeführt, deshalb werden die nicht umgesetzten Adressen verwendet.

Security > Firewall > IP-Regeln

- Quelle (Bereich): Eingabe aus "Quell-IP-Adressen"
- Ziel (Bereich): Eingabe aus "Ziel-IP-Adressen"

## Beschreibung

- **Quell-Schnittstelle / Ziel-Schnittstelle**
  Legen Sie die Richtung des Verbindungsaufbaus fest. Es werden nur Verbindungen berücksichtigt, die in dieser festgelegten Richtung aufgebaut werden.
  Zur Auswahl stehen auch die virtuellen Schnittstellen von VPN-Verbindungen:
  - VLANx: VLANs mit konfiguriertem Subnetz
  - pppx bzw. usb0: WAN-Schnittstelle
  - SINEMA RC: Verbindung zum SINEMA RC-Server
  - IPsec: Entweder alle IPsec VPN-Verbindungen (all) oder eine spezifische IPsec VPN-Verbindung
  - OpenVPN: Entweder alle OpenVPN-Verbindungen (all) oder eine spezifische OpenVPN-Verbindung

  **Hinweis**

  Wenn Sie eine NAT-Adressumsetzung in oder aus Richtung VPN-Tunnel konfigurieren, sind nur noch die beteiligten IP-Adressen der NAT-Adressumsetzungsregeln über VPN-Tunnel erreichbar.

- **Quell-IP-Adressen**
  Legen Sie fest, für welche Quell-IP-Adressen diese Source-NAT-Regel gültig ist. Nur die Pakete werden berücksichtigt, die den eingegebenen Adressen entsprechen.
  Folgende Eingaben sind möglich:
  - IP-Adresse: Gilt genau für die angegebene IP-Adresse.
  - IP-Adressbereich: Gilt für einen bestimmten IP-Adressbereich: Start-IP-Adresse "-" End-IP-Adresse an, z. B. 192.168.100.10 - 192.168.100.20
  - IP-Subnetz: Gilt für mehrere IPv4-Adressen, die zu einem IP-Adressbereich zusammengefasst werden: IP-Adresse/Anzahl Bits des Netzanteils (CIDR-Notation)
- **Schnittstellen-IP der Ziel-Schnittstelle verwenden**
  Wenn aktiviert, wird bei "Quell-IP-Adresse-Umsetzung" die IP-Adresse der ausgewählten Ziel-Schnittstelle verwendet.
- **Quell-IP-Adresse-Umsetzung**
  Geben Sie die IP-Adresse ein, mit der die IP-Adresse des Absenders ersetzt wird. Nur editierbar, wenn "Schnittstellen-IP der Ziel-Schnittstelle verwenden" deaktiviert ist.
- **Ziel-IP-Adressen**
  Legen Sie fest, für welche Ziel-IP-Adressen diese Source-NAT-Regel gültig ist. Nur die Pakete werden berücksichtigt, deren Ziel-IP-Adresse im Bereich der eingegebenen Adressen liegt.
  - IP-Adresse: Gilt genau für die angegebene IP-Adresse.
  - IP-Adressbereich: Gilt für einen bestimmten IP-Adressbereich: Start-IP-Adresse "-" End-IP-Adresse an, z. B. 192.168.100.10 - 192.168.100.20
  - IP-Subnetz: Gilt für mehrere IPv4-Adressen, die zu einem IP-Adressbereich zusammengefasst werden: IP-Adresse/Anzahl Bits des Netzanteils (CIDR-Notation)

Die Tabelle gliedert sich in folgende Spalten:

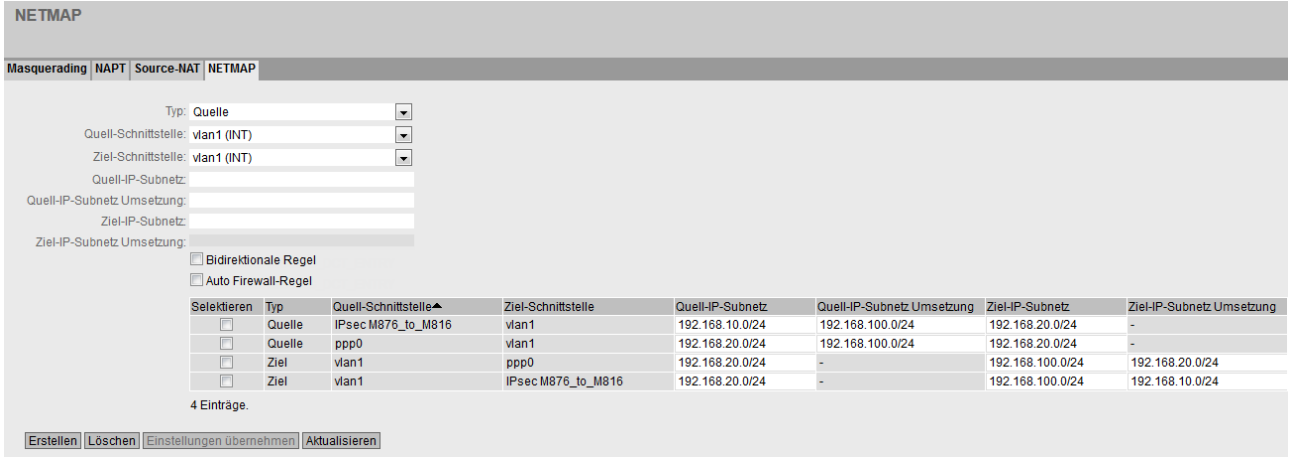
- Selektieren
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- Quell-Schnittstelle
  Zeigt die Quell-Schnittstelle an.
- Ziel-Schnittstelle
  Zeigt die Ziel-Schnittstelle an.
- Quell-IP-Adressen
  Zeigt die IP-Adressen der Absender an, für die eine Adressumsetzung gewünscht ist.
- Schnittstellen-IP verwenden
  Zeigt an, ob bei Quell-IP-Adresse-Umsetzung die IP-Adresse der ausgewählten Ziel-Schnittstelle verwendet wird.
- Quell-IP-Adresse-Umsetzung
  Zeigt die IP-Adresse an, mit der die IP-Adresse der Absender ersetzt wird.
- Ziel-IP-Adressen
  Zeigt die IP-Adressen der Empfänger an, für die eine Adressumsetzung gewünscht ist.

### Siehe auch

NAT und Firewall (Seite 84)

## 5.8.3.5 NETMAP

Auf dieser WBM-Seite legen Sie die Regeln für NETMAP fest. NETMAP ist ein statisches 1:1-Mapping von Netzwerkadressen, wobei der Hostanteil erhalten bleibt. Weitere Informationen dazu finden Sie im Kapitel "NAT und Firewall (Seite 84)".



**Hinweis**

**Firewallregel bei Source-NAT**

Die Adressumsetzung mit Source-NAT wird erst nach der Firewall durchgeführt, deshalb werden die nicht umgesetzten Adressen verwendet.

Security > Firewall > IP-Regeln

- Quelle (Bereich): Eingabe aus "Quell-IP-Subnetz"
- Ziel (Bereich): Eingabe aus "Ziel-IP-Subnetz"

**Firewallregel bei Destination-NAT**

Die Adressumsetzung mit NAT wurde bereits vor der Firewall durchgeführt, deshalb werden in der Firewall die umgesetzten Adressen verwendet.

Security > Firewall > IP-Regeln

- Quelle (Bereich): Eingabe aus "Quell-IP-Subnetz"
- Ziel (Bereich): Eingabe aus "Ziel-IP-Subnetz Umsetzung"

## Beschreibung

- **Typ**
  Legen Sie die Art der Adressumsetzung fest.
  - Quelle: Ersetzen der Quell-IP-Adresse
  - Ziel: Ersetzen der Ziel-IP-Adresse.
- **Quell-Schnittstelle**
  Legen Sie die Quell-Schnittstelle fest.
  - VLANx: VLANs mit konfiguriertem Subnetz
  - pppsx bzw. usb0: WAN-Schnittstelle
  - SINEMA RC: Verbindung zum SINEMA RC-Server
  - IPsec: Entweder alle IPsec VPN-Verbindungen (all) oder eine spezifische IPsec VPN-Verbindung
  - OpenVPN: Entweder alle OpenVPN-Verbindungen (all) oder eine spezifische OpenVPN-Verbindung
- **Ziel-Schnittstelle**
  Legen Sie die Ziel-Schnittstelle fest.
  - VLANx: VLANs mit konfiguriertem Subnetz
  - pppx bzw. usb0: WAN-Schnittstelle
  - SINEMA RC: Verbindung zum SINEMA RC-Server
  - IPsec: Entweder alle IPsec VPN-Verbindungen (all) oder eine spezifische IPsec VPN-Verbindung
  - OpenVPN: Entweder alle OpenVPN-Verbindungen (all) oder eine spezifische OpenVPN-Verbindung

- **Quell-IP-Subnetz**
  Tragen Sie das Subnetz des Absenders ein.
  Das Subnetz kann auch nur ein einzelner PC, oder eine andere Untermenge des Subnetzes sein. Verwenden Sie die CIDR-Schreibweise.
- **Quell-IP-Subnetz- Umsetzung**
  Tragen Sie das Subnetz ein, mit dem das Subnetz des Absenders ersetzt wird. Nur editierbar, bei der Einstellung "Quelle".
  Das Subnetz kann auch nur ein einzelner PC, oder eine andere Untermenge des Subnetzes sein. Verwenden Sie die CIDR-Schreibweise.
- **Ziel-IP-Subnetz**
  Tragen Sie das Subnetz des Empfängers ein.
  Das Subnetz kann auch nur ein einzelner PC, oder eine andere Untermenge des Subnetzes sein. Verwenden Sie die CIDR-Schreibweise.
- **Ziel-IP-Subnetz-Umsetzung**
  Tragen Sie das Subnetz ein, mit dem das Subnetz des Empfängers ersetzt wird. Nur editierbar, bei der Einstellung "Ziel".
  Das Subnetz kann auch nur ein einzelner PC, oder eine andere Untermenge des Subnetzes sein. Verwenden Sie die CIDR-Schreibweise.
- **Bidirektionale Regel**
  Wenn aktiviert, wird beim Erstellen der NETMAP-Regel automatisch die NETMAP-Regel für die Gegenrichtung angelegt.
  Die NETMAP-Regeln sind nach dem Anlegen nicht miteinander verbunden. D. h. es findet keine Synchronisierung der NETMAP-Regeln beim Ändern oder Löschen statt.
- **Auto Firewall-Regel**
  Wenn aktiviert, wird beim Erstellen der NETMAP-Regel automatisch die entsprechende Firewall-Regel erzeugt. Diese Firewall-Regeln werden unter "Security > Firewall > IP-Regeln" angezeigt. Wenn Sie die NETMAP-Regeln ändern oder löschen, wird die entsprechende Firewall-Regel angepasst oder gelöscht.

Die Tabelle gliedert sich in folgende Spalten:

- Selektieren
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- Typ
  Zeigt die Richtung der Adressumsetzung an.
- Quell-Schnittstelle
  Zeigt die Quell-Schnittstelle an.
- Ziel-Schnittstelle
  Zeigt die Ziel-Schnittstelle an.
- Quell-IP-Subnetz
  Zeigt das Subnetz des Absenders an. Der Eintrag kann bei Bedarf geändert werden.
- Quell-IP-Subnetz-Umsetzung
  Zeigt das Subnetz des Absenders an, mit dem das Subnetz des Absenders ersetzt wird. Der Eintrag kann bei Bedarf geändert werden.
- Ziel-IP-Subnetz
  Zeigt das Subnetz des Empfängers an. Der Eintrag kann bei Bedarf geändert werden.

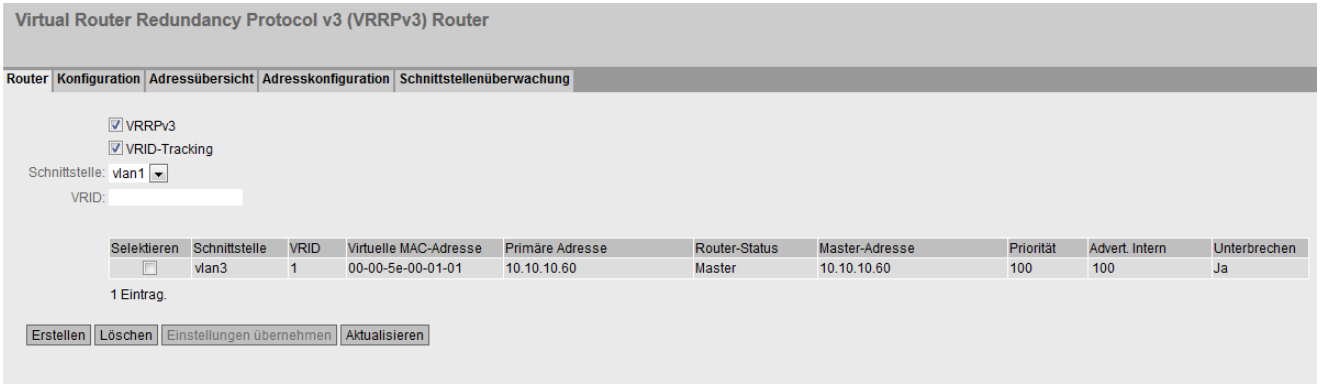
- Ziel-IP-Subnetz-Umsetzung
  Zeigt das Subnetz des Empfängers an, mit dem das Subnetz des Empfängers ersetzt wird. Der Eintrag kann bei Bedarf geändert werden.
- Kommentar
  Wenn nötig, geben Sie einen Kommentar ein.

## 5.8.4 VRRPv3

### 5.8.4.1 Router

#### Einleitung

Mit Hilfe der Schaltfläche "Erstellen" können Sie neue virtuelle Router anlegen. Maximal sind 2 virtuelle Router konfigurierbar. Weitere Parameter konfigurieren Sie auf dem Register "Konfiguration".




**Hinweis**

- Sie können VRRPv3 an VLAN-Schnittstellen nutzen.

#### Voraussetzung

Damit die eingehenden Pakete an das Gerät weitergeleitet werden, aktivieren Sie die vordefinierte IPv4-Regel "VRRP".

## Beschreibung

Die Seite enthält Folgendes:

- **VRRPv3**
  Aktivieren oder deaktivieren Sie das Routing über VRRPv3.
- **VRID-Tracking**
  Aktivieren oder deaktivieren Sie das VRID-Tracking.
  Wenn aktiviert, werden alle VRRP-Instanzen überwacht. Wenn sich der Status einer VRRP-Instanz nach "Initialize" ändert, wird die Priorität aller VRRP-Instanzen auf den Wert "1" verringert.
  Wenn sich der Status der VRRP-Instanz ändert, wird die ursprüngliche Priorität aller VRRP-Instanzen wiederhergestellt.
- **Schnittstelle**
  Wählen Sie die gewünschte VLAN-Schnittstelle aus, die als virtueller Router fungiert.
- **VRID**
  Geben Sie die ID des virtuellen Routers ein. Diese ID definiert die Gruppe der Router, die einen virtuellen Router (VR) bilden. In der Gruppe ist diese gleich. Für andere Gruppen kann sie nicht mehr verwendet werden.
  Gültige Werte sind 1...255.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Schnittstelle**
  Zeigt die Schnittstelle an, die als virtueller Router fungiert.
- **VRID**
  Zeigt die ID des virtuellen Routers an.
- **Virtuelle MAC-Adresse**
  Zeigt die virtuelle MAC-Adresse des virtuellen Routers an.
- **Primäre IP-Adresse**
  Zeigt die kleinste numerische IPv4-Adresse auf diesem VLAN an. Der Eintrag 0.0.0.0 bedeutet, dass die "Primäre" Adresse auf diesem VLAN verwendet wird. Ansonsten sind alle IPv4-Adressen, die auf diesem VLAN in dem Menü "Layer 3 (IPv4) > Subnetze" konfiguriert wurden, gültige Werte.
- **Router-Status**
  Zeigt den derzeitigen Zustand des virtuellen Routers an. Mögliche Werte sind:
  - Master
    Der Router ist der Master-Router und übernimmt die Routingfunktionalität für alle zugeordneten IPv4-Adressen.
  - Backup
    Der Router ist der Backup-Router. Wenn der Master-Router ausfällt, übernimmt der Backup-Router die Aufgaben des Master-Routers.
  - Initialize
    Der virtuelle Router wurde soeben eingeschaltet. In kurzer Zeit wird er in den Zustand "Master" oder "Backup" wechseln.

- **Master IP-Adresse**
  Zeigt die IPv4-Adresse des Master-Routers an.
- **Priorität**
  Zeigt die Priorität des virtuellen Routers an.
  Gültige Werte sind 1-254.
  Wenn eine IPv4-Adresse dem VRRP-Router zugeordnet wird, die auch tatsächlich an der lokalen IPv4-Schnittstelle konfiguriert ist, wird automatisch der Wert 255 eingetragen. Alle anderen Prioritäten können frei auf die VRRP-Router verteilt werden. Je größer eine Priorität ist, desto eher wird der VRRP-Router zum "Master".
- **Advert.-Intern**
  Zeigt das Intervall an, in dem der Master-Router VRRPv3-Pakete verschickt.
- **Unterbrechen**
  Zeigt die Bevorzugung eines Routers beim Rollenwechsel zwischen Backup und Master an.
  - ja
    Dieser Router ist beim Rollenwechsel bevorzugt.
  - nein
    Dieser Router ist beim Rollenwechsel nicht bevorzugt.

### VRRP und DHCP-Server

Wenn Sie auf den Geräten einer VRRP-Gruppe einen DHCP-Server betreiben wollen, muss der DHCP-Server auf dem Master-Router konfiguriert sein. Backup-Router reagieren nicht auf DHCP-Anfragen. Stellen Sie sicher, dass der Master-Router statisch konfiguriert ist und nach einem Ausfall wieder zum Master der VRRP-Gruppe wird.

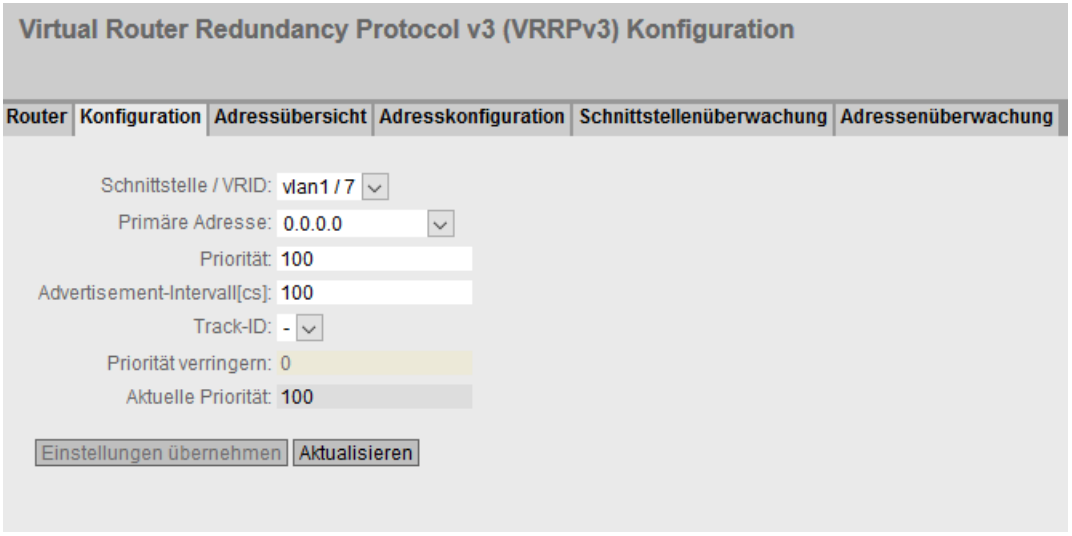
### Vorgehensweise

1. Aktivieren Sie das Optionskästchen "VRRPv3".
2. Wählen Sie die gewünschte Schnittstelle aus.
3. Geben Sie im Eingabefeld "VRID" die ID des virtuellen Routers ein.
4. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird eine neue Zeile eingefügt.
5. Aktivieren Sie das Optionskästchen "Antworte an virtuellen Schnittstellen auf Ping-Anfragen", damit auch virtuelle IPv4-Adressen auf Ping antworten.
6. Aktivieren Sie das Optionskästchen "VRID-Tracking", um die VRID zu überwachen.
7. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen". Um den virtuellen Router zu konfigurieren, klicken Sie auf die Registerkarte "Konfiguration".

### 5.8.4.2 Konfiguration

#### Einleitung

Auf dieser Seite konfigurieren Sie den virtuellen Router.




#### Beschreibung

Die Seite enthält Folgendes:

- **Schnittstelle / VRID**
  Wählen Sie die ID des zu konfigurierenden virtuellen Routers aus.
- **Primäre Adresse**
  Wählen Sie die vorrangige IPv4-Adresse aus. Wenn der Router zum Master-Router wird, verwendet der Router diese IPv4-Adresse.

  **Hinweis**

  Wenn Sie auf diesem VLAN nur ein Subnetz konfigurieren, ist keine Angabe erforderlich. Der Eintrag ist dann 0.0.0.0.
  Wenn Sie mehrere Subnetze am VLAN konfigurieren und Sie möchten, dass eine bestimmte IPv4-Adresse als Quelladresse für VRRP-Pakete genutzt wird, wählen Sie die entsprechende IPv4-Adresse aus. Ansonsten wird die numerisch kleinste IPv4-Adresse verwendet.

- **Priorität**
  Geben Sie die Priorität dieses virtuellen Routers ein. Gültige Werte sind 1-254.
  Wenn eine IPv4-Adresse dem VRRPv3-Router zugeordnet wird, die auch tatsächlich an der lokalen IPv4-Schnittstelle konfiguriert ist, wird automatisch der Wert 255 eingetragen. Alle anderen Prioritäten können frei auf die VRRPv3-Router verteilt werden. Je größer eine Priorität ist, desto eher wird der VRRPv3-Router zum "Master".

- **Advertisement-Intervall**
  Geben Sie das Zeitintervall ein, nach dem ein Master-Router erneut ein VRRPv3-Paket verschickt.
  Angabe in Zenti-Sekunden.
- **Track-ID**
  Wählen Sie eine Track-ID aus.
- **Priorität verringern**
  Geben Sie ein, um welchen Wert die Priorität der VRRPv3-Schnittstelle verringert wird.
- **Aktuelle Priorität**
  Zeigt die Priorität der VRRPv3-Schnittstelle an, nachdem die überwachte Schnittstelle in den Zustand "down" gewechselt hat.

### Vorgehensweise

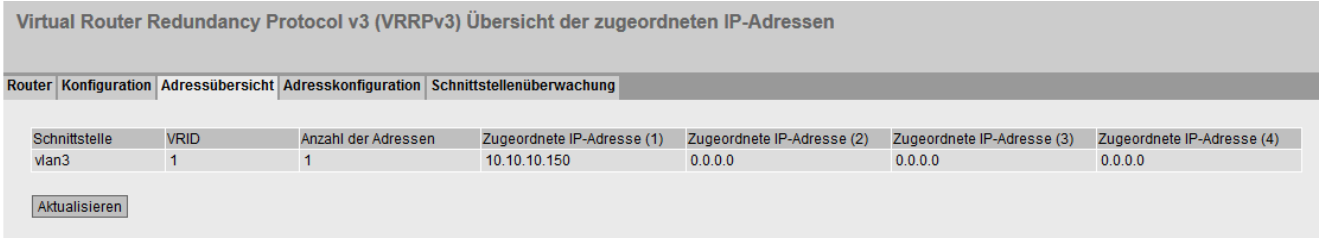
Um einen virtuellen Router als Master-Router zu konfigurieren, gehen Sie folgendermaßen vor:

1. Wählen Sie aus der Klappliste "Schnittstelle / VRID" die ID des zu konfigurierenden virtuellen Routers aus.
2. Aktivieren Sie das Optionskästchen "Status".
3. Wählen Sie aus der Klappliste "Primäre Adresse" die Quelladresse.
4. Tragen Sie aus der Klappliste "Priorität" die Priorität dieses virtuellen Routers ein.
5. Tragen Sie bei "Advertisement-Intervall" das Zeitintervall ein.
6. Wählen Sie eine Track-ID aus.
7. Geben Sie den Wert ein, um den die Priorität der VRRPv3-Schnittstelle verringert wird.
8. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

## 5.8.4.3 Adressübersicht

### Übersicht

Diese Seite zeigt an, welche IPv4-Adressen der virtuelle Router überwacht. Jeder virtuelle Router kann eine IPv4-Adresse überwachen.



### Beschreibung der angezeigten Werte

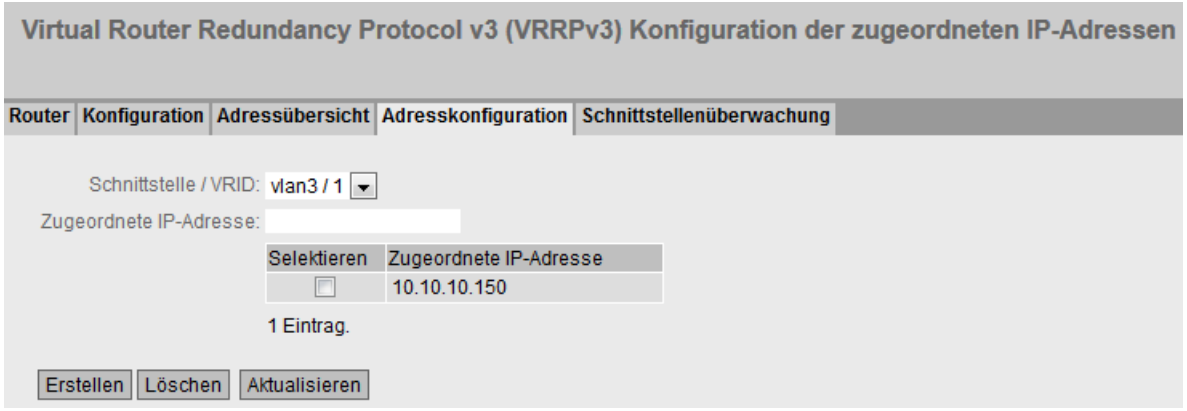
Die Tabelle gliedert sich in folgende Spalten:

- **Schnittstelle**
  Zeigt die Schnittstelle an, der als virtueller Router fungiert.
- **VRID**
  Zeigt die ID dieses virtuellen Routers an.
- **Anzahl der Adressen**
  Zeigt die Anzahl der IPv4-Adressen an.
- **Zugeordnete IP-Adresse (1) ...Zugeordnete IP-Adresse (4)**
  Zeigt die Router IPv4-Adressen, die durch diesen virtuellen Router überwacht werden. Wenn ein Router die Rolle des Masters übernimmt, wird die Routingfunktion all dieser IPv4-Adressen durch diesen Router übernommen.

## 5.8.4.4 Adresskonfiguration

### Anlegen oder ändern der überwachten IP-Adressen

Auf dieser Seite können Sie die zu überwachenden IPv4-Adressen anlegen, ändern oder löschen. Jeder virtuelle Router kann eine IPv4-Adresse überwachen.




### Beschreibung

Die Seite enthält Folgendes:

- **Schnittstelle / VRID**
  Wählen Sie die ID des virtuellen Routers aus.
- **Zugeordnete IP-Adresse**
  Geben Sie die IPv4-Adresse ein, die der virtuelle Router überwachen soll.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen
- **Zugeordnete IP-Adresse**
  Zeigt die IPv4-Adressen an, die der virtuelle Router überwacht.

### Vorgehensweise

1. Wählen Sie die ID des virtuellen Routers aus.
2. Geben Sie die IPv4-Adresse ein, die der virtuelle Router überwachen soll.
3. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag erzeugt.

## 5.8.4.5 Schnittstellenüberwachung

### Einleitung

Auf dieser Seite konfigurieren Sie die Überwachung von Schnittstellen.

Wenn sich der Link einer überwachten Schnittstelle von "up" nach "down" ändert, wird die Priorität der zugeordneten VRRP-Schnittstelle verringert. Um welchen Wert die Priorität verringert wird, konfigurieren Sie auf der Seite "Layer 3 > VRRPv3 > Konfiguration".

Wenn sich der Link der Schnittstelle wieder von "down" nach "up" ändert, wird die ursprüngliche Priorität der VRRP-Schnittstelle wiederhergestellt.



## Beschreibung

Die Seite enthält folgende Felder:

- **Schnittstelle**
  Wählen Sie aus der Klappliste die Schnittstelle aus, die überwacht werden soll.
- **Track-ID**
  Geben Sie eine Track-ID ein.
- **Track-ID**
  Wählen Sie eine Track-ID aus.
- **Track-Schnittstellenzähler**
  Geben Sie ein, wie viele der überwachten Schnittstellen in den Zustand "down" wechseln müssen, bevor die Priorität geändert wird.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Track-ID**
  Zeigt die Track-ID an.
- **Schnittstelle**
  Zeigt die Schnittstelle an, die überwacht wird.

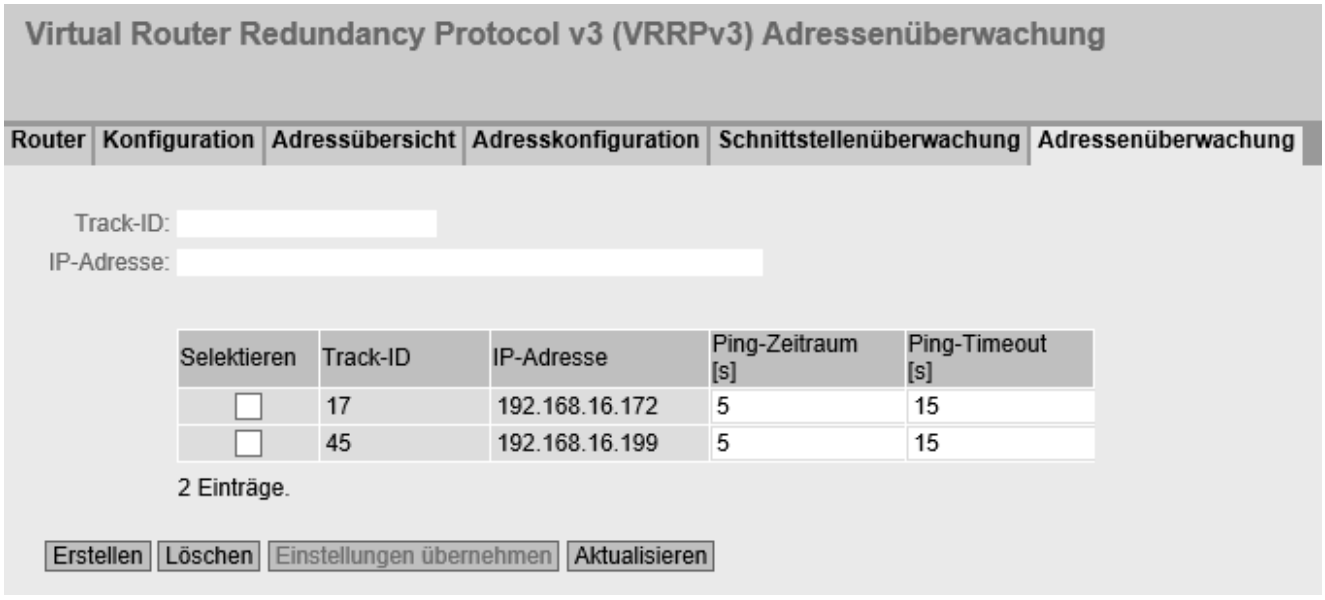
## Vorgehensweise

1. Wählen Sie aus der Klappliste "Schnittstelle" die gewünschte Schnittstelle aus.
2. Geben Sie im Feld "Track-ID" die gewünschte ID ein.
3. Klicken Sie auf die Schaltfläche "Erstellen".
4. Wählen Sie aus der Klappliste "Track-ID" eine ID aus.
5. Geben Sie im Feld "Track-Schnittstellenzähler" die Anzahl der Schnittstellen ein.
6. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
7. Verknüpfen Sie die Überwachung mit einer VRRP-Schnittstelle im Register "Konfiguration".

### 5.8.4.6 Adressenüberwachung

#### Einleitung

Auf dieser Seite konfigurieren Sie die Überwachung von IPv4-Adressen. Der Router sendet innerhalb des festgelegten Zeitraums eine Ping-Anfrage an jede der konfigurierten IPv4-Adressen. Wenn er innerhalb eines festgelegten Zeitraums keine Antwort erhält, wird die VRRP-Priorität der entsprechenden Schnittstelle vermindert.




#### Beschreibung

Die Seite enthält folgende Felder:

- **Track-ID**
  Geben Sie die Track-ID ein.
- **IP-Adresse**
  Geben Sie die zu überwachende IPv4-Adresse ein. Sie können maximal fünf IPv4-Adressen eingeben.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Track-ID**
  Zeigt die Track-ID an.
- **IP-Adresse**
  Zeigt die IPv4-Adresse an, die überwacht wird.

- **Ping-Zeitraum**
  Zeigt die Zyklusdauer in Sekunden zwischen zwei Ping-Anfragen an.
- **Ping-Timeout**
  Zeigt die Zeit in Sekunden an, die der Router auf eine Ping-Antwort wartet. Mindestzeitdauer ist der dreifache Ping-Zeitraum.

### Vorgehensweise

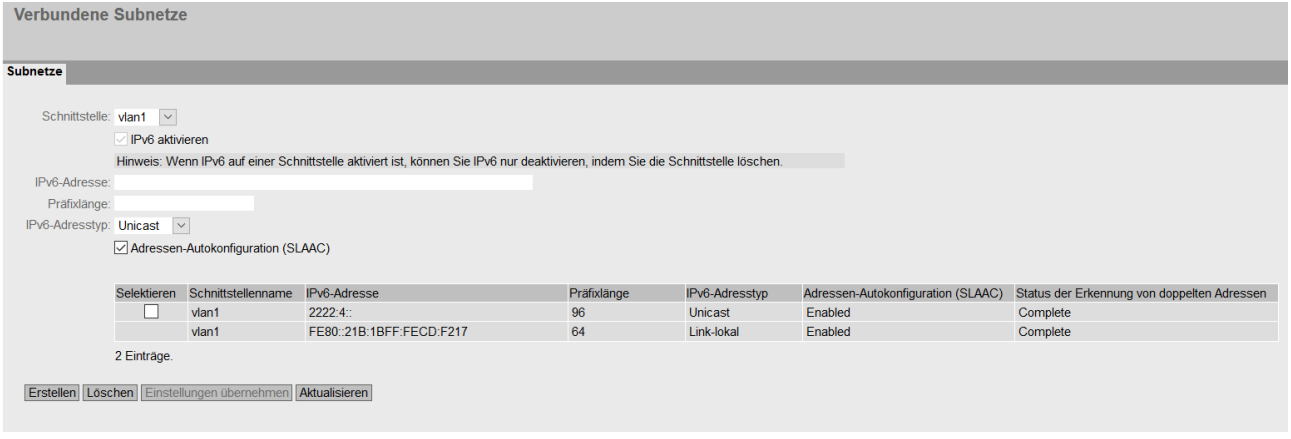
1. Geben Sie im Feld "Track-ID" die gewünschte ID ein.
2. Tragen Sie im Feld "IPv4-Adresse" die IPv4-Adresse ein, die der virtuelle Router überwachen soll.
3. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag erzeugt.

## 5.9 Menü "Layer 3 (IPv6)"

### 5.9.1 Subnetze

### Verbundene Subnetze

Auf dieser Seite können Sie IPv6 an der Schnittstelle aktivieren. Die Schnittstelle wird auch als IPv6-Schnittstelle bezeichnet. Eine IPv6-Schnittstelle kann mehrere IPv6-Adressen haben.



## Beschreibung

Die Seite enthält Folgendes:

- **Schnittstelle**
  Wählen Sie die IP-Schnittstelle aus, an der IPv6 aktiviert wird.
- **IPv6 aktivieren**
  Aktivieren oder deaktivieren Sie IPv6 auf der Schnittstelle.

  **Hinweis**

  **IPv6 deaktivieren**

  Wenn IPv6 auf einer Schnittstelle aktiviert ist, können Sie IPv6 nur deaktivieren, indem Sie die Schnittstelle löschen.

- **IPv6-Adresse**
  Geben Sie die IPv6-Adresse an. Die Eingabe ist abhängig von der gewählten Adressart.
- **Präfixlänge**
  Geben Sie die Anzahl der linksseitigen Bits an, die dem Präfix angehören.
- **IPv6-Adresstyp**
  Wählen Sie die Adressart aus:
  - Unicast
  - Anycast
  - Link-lokal: IPv6-Adresse ist nur auf dem Link gültig
- **Adressen-Autokonfiguration (SLAAC)**
  Aktivieren oder deaktivieren Sie den Mechanismus SLAAC (Stateless Address Auto Configuration) für die Adresskonfiguration.
  Wenn SLAAC aktiviert ist, erfolgt eine zustandslose Autokonfiguration über NDP (Neighbor Discovery Protocol).

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Schnittstellenname**
  Zeigt den Namen der Schnittstelle.
- **IPv6-Adresse**
  Zeigt die IP-Adresse des Subnetzes an.
- **Präfixlänge**
  Zeigt die Präfixlänge an.

- **IPv6-Adresstyp**
  Zeigt den Adressentyp an. Folgende Werte sind möglich:
  - Unicast
  - Anycast
  - Link-lokal
- **Status der Erkennung von doppelten Adressen**
  Bei der Adressen-Autokonfiguration (SLAAC) verhindert die Funktion "Status der Erkennung von doppelten Adressen", dass IPv6-Adressen doppelt vergeben werden. Das Gerät darf bei der Autokonfiguration nur unvergebene IPv6-Adressen verwenden.
  Wenn die Funktion aktiviert ist, läuft die Prüfung über NDP automatisch ab.

  **Hinweis**

  Die Funktion führt keine zyklische Prüfung durch.

  Diese Spalte zeigt an, in welchem Status sich die Funktion befindet. Folgende Werte sind möglich:
  - **Tentative**
    Dieser Status zeigt an, dass die ausgewählte IPv6-Adresse geprüft wird. Das Gerät sendet eine Neighbor Solicitation-Nachricht an die ausgewählte IPv6-Adresse.
  - **Conflict**
    Dieser Status zeigt an, die IPv6-Adresse bereits verwendet wird. Das Gerät erhält in diesem Fall eine Neighbor-Advertisement-Nachricht mit der ausgewählten IPv6-Adresse zurück.
  - **Complete**
    Dieser Status zeigt an, dass die ausgewählte IPv6-Adresse verwendet werden kann. Das Gerät hat in diesem Fall innerhalb einer Zeitspanne keine Rückmeldung erhalten und geht davon aus, dass die IPv6-Adresse noch nicht vergeben ist.
  - **Down**
    Dieser Status zeigt an, dass die Schnittstelle nicht aktiv ist. Es wird keine Prüfung durchgeführt.

## Vorgehensweise

**Link-lokale Adresse automatisch bilden**

1. Wählen Sie die gewünschte Schnittstelle aus.
2. Aktivieren Sie IPv6.
3. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein Eintrag mit der Schnittstelle erstellt und die automatisch gebildete IPv6-Adresse wird angezeigt.

**Link-lokale Adresse zuweisen**

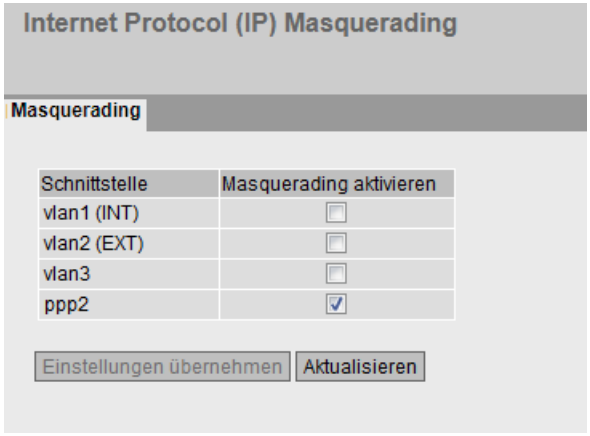
1. Wählen Sie die gewünschte Schnittstelle aus.
2. Aktivieren Sie IPv6.
3. Geben Sie bei "IPv6-Adresse" die link lokale-Adresse ein, z. B. FE80::21B:1BFF:FE40:9155
4. Geben Sie bei "Präfixlänge" "64" ein.

5. Wählen Sie bei "IPv6-Adresstyp" den Eintrag "Link-lokal" aus.
6. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein Eintrag mit der Schnittstelle erstellt und die IPv6-Adresse wird angezeigt.

## 5.9.2 NAT

### 5.9.2.1 Masquerading

Auf dieser WBM-Seite aktivieren Sie die Regeln für IPv6-Masquerading.




#### Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

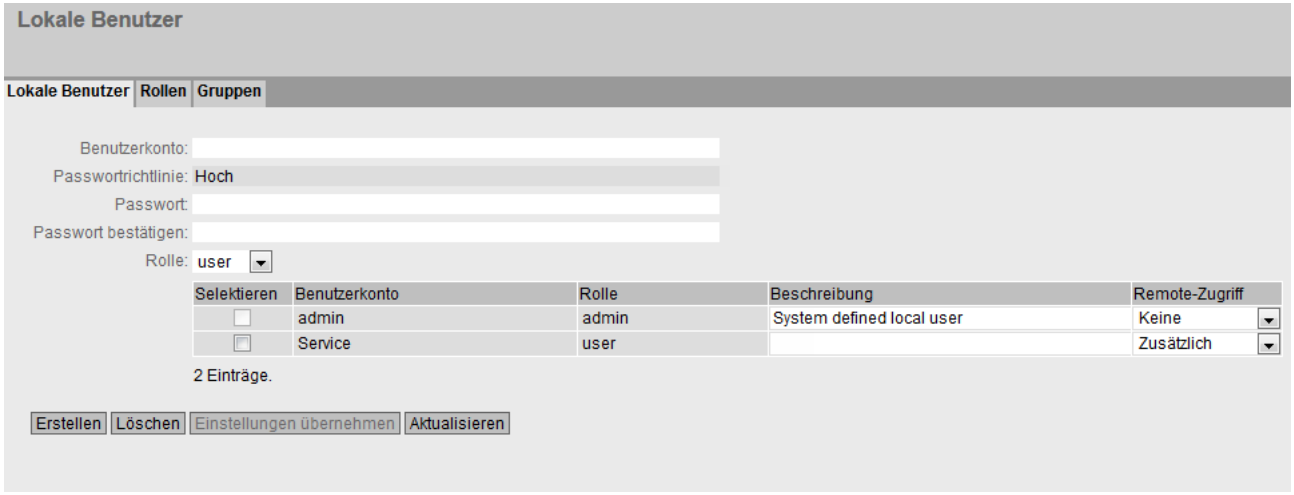
- **Schnittstelle**
  Schnittstelle, auf die sich die Einstellung bezieht. Nur Schnittstellen mit konfiguriertem Subnetz sind verfügbar.
- **Masquerading aktivieren**
  Wenn aktiviert, wird bei jedem ausgehenden Datenpaket, das über diese Schnittstelle gesendet wird, die Quell-IPv6-Adresse durch die IPv6-Adresse der Schnittstelle ersetzt.

# 5.10 Menü "Security"

## 5.10.1 Benutzer

### 5.10.1.1 Lokale Benutzer

Auf dieser Seite erstellen Sie lokale Benutzer mit den entsprechenden Rechten. Um ein Benutzerkonto anzulegen, muss der angemeldete Benutzer die Rolle "admin" besitzen.



## Beschreibung

Die Seite enthält Folgendes:

- **Benutzerkonto**
  Geben Sie den Namen für den Benutzer ein. Der Name muss folgende Bedingungen erfüllen:
  - Er muss eindeutig sein.
  - Er muss zwischen 1 und 250 Zeichen lang sein.
  - Er darf folgende Zeichen nicht enthalten: | § ? " ; : ß
  - Die Zeichen für Space und Delete dürfen auch nicht enthalten sein.

  **Hinweis**

  **Benutzername nicht änderbar**

  Nach dem Anlegen eines Benutzers kann der Benutzername nicht mehr geändert werden.

  Wenn ein Benutzername geändert werden soll, muss der Benutzer gelöscht und ein neuer Benutzer angelegt werden.

  **Hinweis**

  **Benutzernamen: admin**

  Mit diesem Benutzernamen können Sie das Gerät konfigurieren.

  Wenn Sie sich das erste Mal oder nach einem "Auf Werkseinstellungen zurücksetzen und Neustart" anmelden, werden Sie aufgefordert das vordefinierte Passwort "admin" zu ändern. Zusätzlich können Sie einmalig den werksseitig voreingestellten Benutzer "admin" umbenennen. Danach ist ein Umbenennen von "admin" nicht mehr möglich.

- **Passwortrichtlinie**
  Zeigt an, welche Passwortrichtlinie verwendet wird:
  - Hoch
    Passwortlänge: mindestens 8 Zeichen, maximal 128 Zeichen
    Mindestens 1 Großbuchstabe
    Mindestens 1 Sonderzeichen
    Mindestens 1 Zahl
  - Benutzerdefiniert
    Das Passwort muss den konfigurierten Anforderungen entsprechen. Die Anforderungen konfigurieren Sie unter "Security > Passwörter > Optionen".
- **Passwort**
  Geben Sie das Passwort an. Die Stärke des Passworts ist abhängig von der eingestellten Passwortrichtlinie.
  Es dürfen folgende Zeichen nicht enthalten sein: | § ? " ; : ß \
- **Passwort bestätigen**
  Geben Sie das Passwort erneut ein, um es zu bestätigen.
- **Rolle**
  Wählen Sie eine Rolle aus.
  Sie können zwischen den voreingestellten und selbst definierten Rollen wählen, siehe Seite "Security > Benutzer > Rollen".

Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.

  **Hinweis**

  Die werksseitig voreingestellten Benutzer sowie angemeldete Benutzer können nicht gelöscht oder geändert werden.

- **Benutzerkonto**
  Zeigt den Benutzernamen an.
- **Rolle**
  Zeigt die Rolle des Benutzers an.
- **Beschreibung**
  Zeigt eine Beschreibung des Benutzerkontos an. Der Beschreibungstext kann bis zu 100 Zeichen lang sein.
- **Remote-Zugriff**
  - Nur
    Nur Remote-Zugriff, d. h. keine Rechte außer das Anmelden an der WBM-Seite für benutzerspezifische Firewall.
  - Keine
    Kein Remote-Zugriff. Der Benutzer kann sich nicht an der benutzerspezifischen Firewall anmelden, sondern nur am WBM des Geräts.
  - Zusätzlich
    Der Benutzer kann sich sowohl am WBM des Geräts als auch an der benutzerspezifischen Firewall anmelden.

## Vorgehensweise

**Hinweis**
**Änderungen im Modus "Trial"**

Auch wenn sich das Gerät im Modus "Trial" befindet, werden Änderungen, die Sie auf dieser Seite durchführen, sofort gespeichert.

**Benutzer anlegen**

1. Geben Sie den Namen für den Benutzer ein.
2. Geben Sie das Passwort für den Benutzer ein.
3. Geben Sie das Passwort erneut ein, um es zu bestätigen.
4. Wählen Sie die Rolle des Benutzers aus.
5. Klicken Sie auf die Schaltfläche "Erstellen".
6. Geben Sie eine Beschreibung des Benutzers ein.
7. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

**Benutzer löschen**

1. Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
2. Klicken Sie auf die Schaltfläche "Löschen". Die Einträge werden gelöscht und die Seite wird aktualisiert.

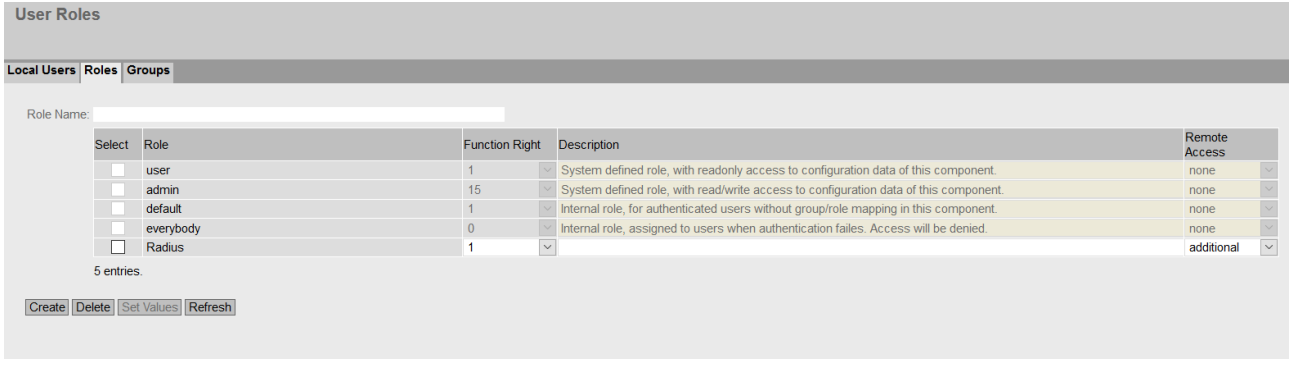
### 5.10.1.2 Rollen

## Rollen

Auf dieser Seite erstellen Sie Rollen, die lokal auf dem Gerät gültig sind.

**Hinweis**

Es ist von den Rechten des angemeldeten Benutzers abhängig, welche Werte angezeigt werden.




## Beschreibung

Die Seite enthält Folgendes:

- **Rollenname**
  Geben Sie den Namen für die Rolle ein. Der Name muss folgende Bedingungen erfüllen:
  - Er muss eindeutig sein.
  - Er muss zwischen 1 und 64 Zeichen lang sein.

  **Hinweis**

  **Rollenname nicht änderbar**

  Nach dem Anlegen einer Rolle kann der Rollenname nicht mehr geändert werden.

  Wenn ein Rollenname geändert werden soll, muss die Rolle gelöscht und eine neue Rolle angelegt werden.

Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.

  **Hinweis**

  Die voreingestellten Rollen sowie zugewiesene Rollen können nicht gelöscht oder geändert werden.

- **Rolle**
  Zeigt den Namen der Rolle an.
- **Funktionsrecht**
  Wählen Sie die Funktionsrechte der Rolle aus:
  - 1
    Benutzer mit dieser Rolle können Geräteparameter lesen aber nicht verändern. Benutzer mit dieser Rolle können ihr eigenes Passwort ändern.
  - 15
    Benutzer mit dieser Rolle können Geräteparameter sowohl lesen als auch verändern.

  **Hinweis**

  **Funktionsrecht nicht änderbar**

  Wenn Sie eine Rolle zugewiesen haben, können Sie das Funktionsrecht der Rolle nicht mehr ändern.

  Wenn Sie das Funktionsrecht einer Rolle ändern wollen, gehen Sie wie folgt vor:

  1. Löschen Sie alle zugewiesenen Benutzer.
  2. Ändern Sie das Funktionsrecht der Rolle.
  3. Weisen Sie die Rolle erneut zu.

- **Beschreibung**
  Geben Sie eine Beschreibung für die Rolle ein. Bei vordefinierten Rollen wird eine Beschreibung angezeigt. Der Beschreibungstext kann bis zu 100 Zeichen lang sein.
- **Remote-Zugriff**
  - Keine
    Kein Remote-Zugriff. Der Benutzer kann sich nicht an der dynamischen Firewall anmelden, sondern nur am WBM des Geräts.
  - Zusätzlich
    Der Benutzer kann sich sowohl am WBM des Geräts als auch an der dynamischen Firewall anmelden.
  - Nur
    Der Benutzer kann sich nur an der dynamischen Firewall anmelden.

### Vorgehensweise

**Rolle anlegen**

1. Geben Sie den Namen für die Rolle ein.
2. Klicken Sie auf die Schaltfläche "Erstellen".
3. Wählen Sie die Funktionsrechte der Rolle aus.
4. Geben Sie eine Beschreibung der Rolle ein.
5. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

**Rolle löschen**

1. Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
2. Klicken Sie auf die Schaltfläche "Löschen". Die Einträge werden gelöscht und die Seite wird aktualisiert.

## 5.10.1.3 Gruppen

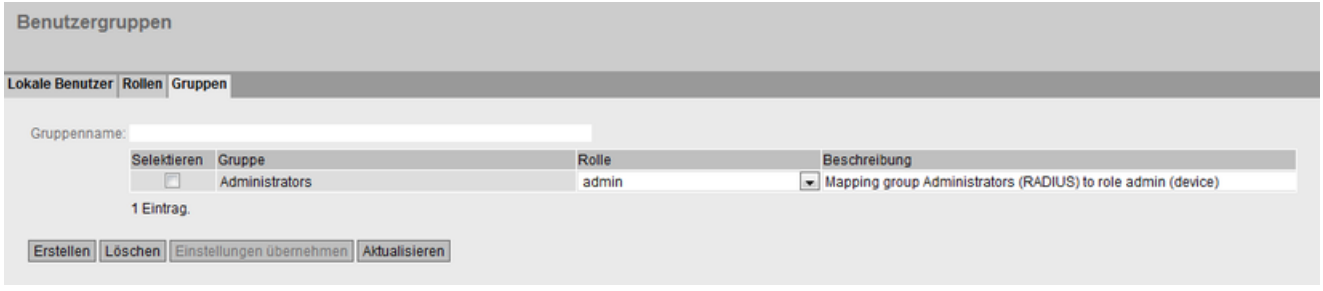
### Benutzergruppen

Auf dieser Seite verknüpfen Sie eine Gruppe mit einer Rolle.

In diesem Beispiel wird die Gruppe "Administrators" mit der Rolle "admin" verknüpft. Die Gruppe ist auf einem RADIUS-Server definiert. Die Rolle ist lokal auf dem Gerät definiert. Wenn ein RADIUS-Server einen Benutzer authentifiziert und der Gruppe "Administrators" zuordnet, erhält dieser Benutzer auf dem Gerät die Rechte der Rolle "admin".

**Hinweis**

Es ist von den Rechten des angemeldeten Benutzers abhängig, welche Werte angezeigt werden.



## Beschreibung

Die Seite enthält Folgendes:

- **Gruppenname**
  Geben Sie den Namen der Gruppe ein. Der Name muss der Gruppe auf dem RADIUS-Server entsprechen.
  Der Name muss folgende Bedingungen erfüllen:
  - Er muss eindeutig sein.
  - Er muss zwischen 1 und 64 Zeichen lang sein.
  - Nicht erlaubt sind: § ? " ; :

Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Gruppe**
  Zeigt den Namen der Gruppe an.
- **Rolle**
  Wählen Sie eine Rolle aus. Benutzer, die über den RADIUS-Server mit der verknüpften Gruppe authentifiziert werden, erhalten die Rechte dieser Rolle lokal auf dem Gerät.
  Sie können zwischen den voreingestellten und selbst definierten Rollen wählen, siehe Seite "Security > Benutzer > Rollen".
- **Beschreibung**
  Geben Sie eine Beschreibung für die Verknüpfung der Gruppe mit einer Rolle an. Der Beschreibungstext kann bis zu 100 Zeichen lang sein.

## Vorgehensweise

**Eine Gruppe mit einer Rolle verknüpfen**

1. Geben Sie den Namen einer Gruppe ein.
2. Klicken Sie auf die Schaltfläche "Erstellen".
3. Wählen Sie eine Rolle aus.
4. Geben Sie eine Beschreibung für die Verknüpfung einer Gruppe mit einer Rolle ein.
5. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

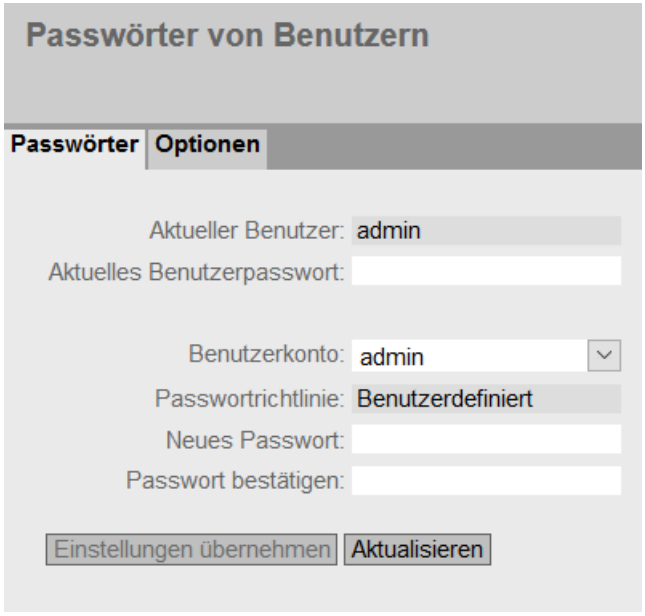
**Die Verknüpfung zwischen einer Gruppe und einer Rolle löschen**

1. Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
2. Klicken Sie auf die Schaltfläche "Löschen". Die Einträge werden gelöscht und die Seite wird aktualisiert.

## 5.10.2 Passwörter

### Konfiguration der Passwörter

Ein Benutzer mit der Rolle "admin" kann das Passwort von bereits angelegten Benutzern ändern. Mit der Rolle "user" kann der Benutzer nur das eigene Passwort ändern.




### Beschreibung

Die Seite enthält Folgendes:

- **Aktueller Benutzer**
  Zeigt den Benutzer an, der aktuell angemeldet ist.
- **Aktuelles Benutzerpasswort**
  Geben Sie das Passwort des aktuell angemeldeten Benutzers ein.
- **Benutzerkonto**
  Wählen Sie den Benutzer, dessen Passwort Sie ändern möchten.
- **Passwortrichtlinie**
  Zeigt an, welche Passwortrichtlinie bei der Vergabe von neuen Passwörtern verwendet wird.
  - Hoch
    Passwortlänge: mindestens 8 Zeichen, maximal 128 Zeichen
    Mindestens 1 Großbuchstabe
    Mindestens 1 Sonderzeichen
    Mindestens 1 Zahl
  - Benutzerdefiniert
    Das Passwort muss den konfigurierten Anforderungen entsprechen. Die Anforderungen konfigurieren Sie unter "Security > Passwörter > Optionen"

- **Neues Passwort**
  Geben Sie das neue Passwort für den ausgewählten Benutzer ein.
  Es dürfen folgende Zeichen nicht enthalten sein: | § ? " ; : ß \

  **Hinweis**

  Wenn Sie sich das erste Mal oder nach einem "Auf Werkseinstellungen zurücksetzen und Neustart" anmelden, werden Sie aufgefordert das vordefinierte Passwort "admin" zu ändern. Zusätzlich können Sie einmalig den werksseitig voreingestellten Benutzer "admin" umbenennen. Danach ist ein Umbenennen von "admin" nicht mehr möglich.

  Werksseitig ist das Passwort bei Auslieferung des Geräts wie folgt eingestellt:
  - admin: admin

  **Hinweis**

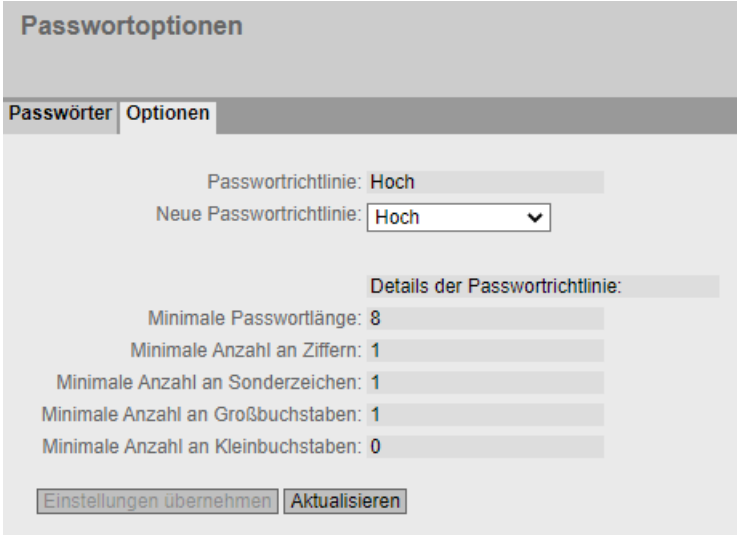
  **Passwort ändern im Trial-Modus**

  Auch wenn Sie im Trial-Modus das Passwort ändern, wird diese Änderung sofort gespeichert.

- **Passwort bestätigen**
  Geben Sie das neue Passwort erneut ein, um es zu bestätigen.

### 5.10.2.1 Optionen

Auf dieser Seite legen Sie fest, welche Passwortrichtlinie bei der Vergabe von neuen Passwörtern beachtet wird.



### Beschreibung

- **Passwortrichtlinie**
  Zeigt an, welche Passwortrichtlinie aktuell verwendet wird.
- **Neue Passwortrichtlinie**
  Wählen Sie aus der Klappliste die gewünschte Einstellung aus:
  - Hoch
    Passwortlänge: mindestens 8 Zeichen, maximal 128 Zeichen
    Mindestens 1 Ziffer
    Mindestens 1 Sonderzeichen
    Mindestens 1 Großbuchstabe
  - Benutzerdefiniert
    Konfigurieren Sie unter "Details der Passwortrichtlinie" die gewünschten Anforderungen an Passwörter.
- **Details der Passwortrichtlinie**
  Wenn Sie die Passwortrichtlinie "Hoch" ausgewählt haben, werden die jeweiligen Anforderungen an Passwörter angezeigt.
  Wenn Sie die Passwortrichtlinie "Benutzerdefiniert" ausgewählt haben, können Sie die Anforderungen an Passwörter konfigurieren.
  - Minimale Passwortlänge
    Gibt an, wie lang ein Passwort mindestens sein muss.
  - Minimale Anzahl an Ziffern
    Gibt an, wie viele Ziffern ein Passwort mindestens enthalten muss.
  - Minimale Anzahl an Sonderzeichen
    Gibt an, wie viele Sonderzeichen ein Passwort mindestens enthalten muss.
  - Minimale Anzahl an Großbuchstaben
    Gibt an, wie viele Großbuchstaben ein Passwort mindestens enthalten muss.
  - Minimale Anzahl an Kleinbuchstaben
    Gibt an, wie viele Kleinbuchstaben ein Passwort mindestens enthalten muss.

## 5.10.3 AAA

### 5.10.3.1 Allgemein

### Anmeldung von Netzteilnehmern

Die verwendete Bezeichnung "AAA" steht für "Authentication, Authorization, Accounting". Dieses Feature dient dazu, Netzteilnehmer zu identifizieren und zuzulassen, ihnen die entsprechenden Dienste bereitzustellen und den Nutzungsumfang festzustellen.

Auf dieser Seite konfigurieren Sie die Anmeldung.




### Beschreibung

Die Seite enthält folgende Felder:

**Hinweis**

Um die Login-Authentifizierung "RADIUS", "Lokal und RADIUS" oder "RADIUS und Fallback Lokal" nutzen zu können, muss ein RADIUS-Server hinterlegt und für die Benutzerauthentifizierung konfiguriert sein.

- **Login-Authentifizierung**
  Legen Sie fest, wie die Anmeldung erfolgt:
  - Lokal
    Die Authentifizierung muss lokal auf dem Gerät erfolgen.
  - RADIUS
    Die Authentifizierung muss über einen RADIUS-Server erfolgen.
  - Lokal und RADIUS
    Die Authentifizierung kann sowohl über die im Gerät vorhandenen Benutzer (Benutzername und Passwort) als auch über einen RADIUS-Server erfolgen.
    Es wird zuerst in der lokalen Datenbank nach dem Benutzer gesucht. Wenn der Benutzer dort nicht vorhanden ist, wird eine RADIUS-Anfrage geschickt.
  - RADIUS und Fallback Lokal
    Die Authentifizierung muss über einen RADIUS-Server erfolgen.
    Nur wenn der RADIUS-Server im Netz nicht erreichbar ist, wird eine lokale Authentifizierung durchgeführt.

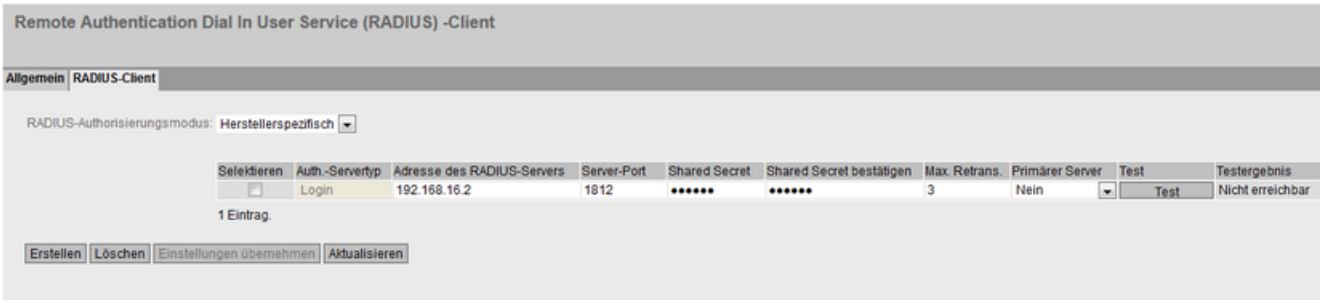
## 5.10.3.2 RADIUS-Client

### Authentifizierung über einen externen Server

Das Konzept von RADIUS basiert auf einem externen Authentifizierungs-Server.

Jede Zeile der Tabelle enthält die Zugangsdaten für je einen Server. In der Suchreihenfolge wird der primäre Server zuerst angefragt. Ist der primäre Server nicht erreichbar, werden in der eingetragenen Reihenfolge sekundäre Server angefragt.

Wenn keiner der Server antwortet, findet keine Authentifizierung statt.




## Beschreibung

Die Seite enthält folgende Felder:

- **RADIUS-Autorisierungsmodus**
  Der RADIUS-Autorisierungsmodus legt bei der Login-Authentifizierung fest, wie bei einer erfolgreichen Authentifizierung die Rechtevergabe für die Benutzer erfolgt.
  - Standard
    In diesem Modus wird der Benutzer mit Administratorrechten angemeldet, wenn der Server für das Attribut "Service Type" den Wert "Administrative User" an das Gerät zurückgibt. In allen anderen Fällen wird der Benutzer mit Leserechten angemeldet.
  - Herstellerspezifisch
    In diesem Modus ist die Rechtevergabe davon abhängig, ob und welche Gruppe der Server für den Benutzer zurückgibt und ob es für den Benutzer einen Eintrag in der Tabelle "Externe Benutzerkonten" gibt.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Adresse des RADIUS-Servers**
  Tragen Sie die IP-Adresse oder den FQDN (Fully Qualified Domain Name) des RADIUS Servers ein.
- **Server-Port**
  Tragen Sie hier den Eingangs-Port auf dem RADIUS-Server ein. Standardmäßig ist der Eingangs-Port 1812 eingestellt. Der Wertebereich ist 1...65535.
- **Shared Secret**
  Geben Sie hier Ihre Zugangskennung an. Der Wertebereich ist 1...128 Zeichen.
- **Shared Secret bestätigen**
  Geben Sie die Zugangskennung zur Bestätigung erneut ein.
- **Max. Retrans.**
  Geben Sie hier die maximale Anzahl der Wiederholungen eines Anfrageversuchs ein. Der initiale Verbindungsversuch wird um den hier angegebenen Wert wiederholt, bevor ein anderer konfigurierter RADIUS-Server angefragt wird oder die Anmeldung für gescheitert erklärt wird. Standardmäßig sind 3 Wiederholungen eingestellt, das bedeutet 4 Verbindungsversuche. Der Wertebereich ist 1...5.
- **Primärer Server**
  Legen Sie mit Hilfe der Optionen der Klappliste fest, ob dieser Server der primäre Server ist. Sie können aus den Optionen "ja" oder "nein" auswählen.

- **Test**
  Mit dieser Schaltfläche können Sie testen, ob der angegebene RADIUS-Server verfügbar ist oder nicht. Der Test wird einmalig durchgeführt und nicht zyklisch wiederholt.
- **Testergebnis**
  Zeigt an, ob der RADIUS-Server verfügbar ist oder nicht:
  - Nicht erreichbar
    Die IP-Adresse ist nicht erreichbar.
    Die IP-Adresse ist erreichbar, der RADIUS-Server läuft jedoch nicht.
  - Erreichbar, das Shared Secret wurde nicht akzeptiert
    Die IP-Adresse ist erreichbar, der RADIUS-Server akzeptiert jedoch das angegebene Shared Secret nicht.
  - Erreichbar, das Shared Secret wurde akzeptiert
    Die IP-Adresse ist erreichbar und der RADIUS-Server akzeptiert das angegebene Shared Secret.

## Vorgehensweise

**Neuen Server eintragen**

1. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag erzeugt. Folgende Standardwerte werden in die Tabelle eingetragen:
   - Adresse des RADIUS-Servers: 0.0.0.0
   - Server-Port: 1812
   - Max. Retrans.: 3
   - Primärer Server: Nein
2. Tragen Sie in der jeweiligen Zeile die folgenden Daten in die Eingabefelder ein:
   - Adresse des RADIUS-Servers
   - Server-Port
   - Shared Secret
   - Shared Secret bestätigen
   - Max. Retrans.: 3
   - Primärer Server: Nein
3. Testen Sie ggf. die Erreichbarkeit des RADIUS-Servers.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Wiederholen Sie den Vorgang für alle Server, die Sie eintragen wollen.

**Server ändern**

1. Tragen Sie in der jeweiligen Zeile die folgenden Daten in die Eingabefelder ein:
   - Adresse des RADIUS-Servers
   - Server-Port
   - Shared Secret
   - Shared Secret bestätigen
   - Max. Retrans
   - Primärer Server
2. Testen Sie ggf. die Erreichbarkeit des RADIUS-Servers.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Wiederholen Sie den Vorgang bei allen Servern, deren Eintrag Sie ändern wollen.

**Server löschen**

1. Klicken Sie in das Optionskästchen in der ersten Spalte vor der zu löschenden Zeile, um den Eintrag zum Löschen zu markieren.
   Wiederholen Sie den Vorgang für jeden Eintrag, den Sie löschen wollen.
2. Klicken Sie auf die Schaltfläche "Löschen". Die Daten werden aus dem Speicher des Gerätes gelöscht und die Seite wird aktualisiert.

## 5.10.4 Zertifikate

### 5.10.4.1 Übersicht

Auf dieser WBM-Seite werden die geladenen Dateien (Zertifikate und Schlüsseln) angezeigt. Folgende Möglichkeiten gibt es, um die Dateien ins Gerät zu laden:

- System > Laden & Speichern > HTTP
- System > Laden & Speichern > TFTP
- System > Laden & Speichern > SFTP

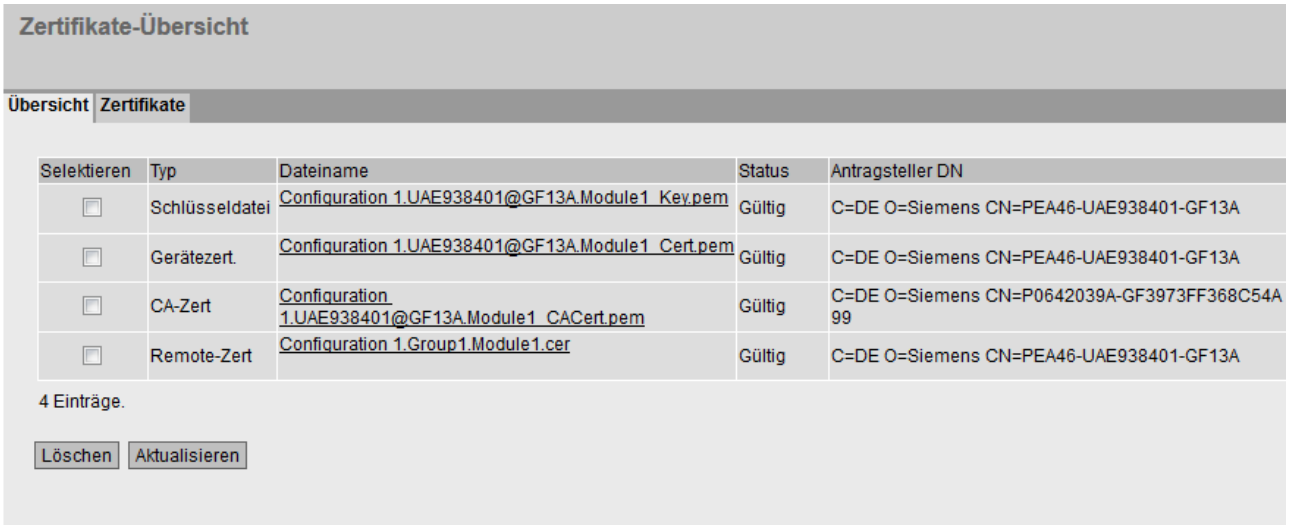



Bild 5-1 Teil 1




Bild 5-2 Teil 2

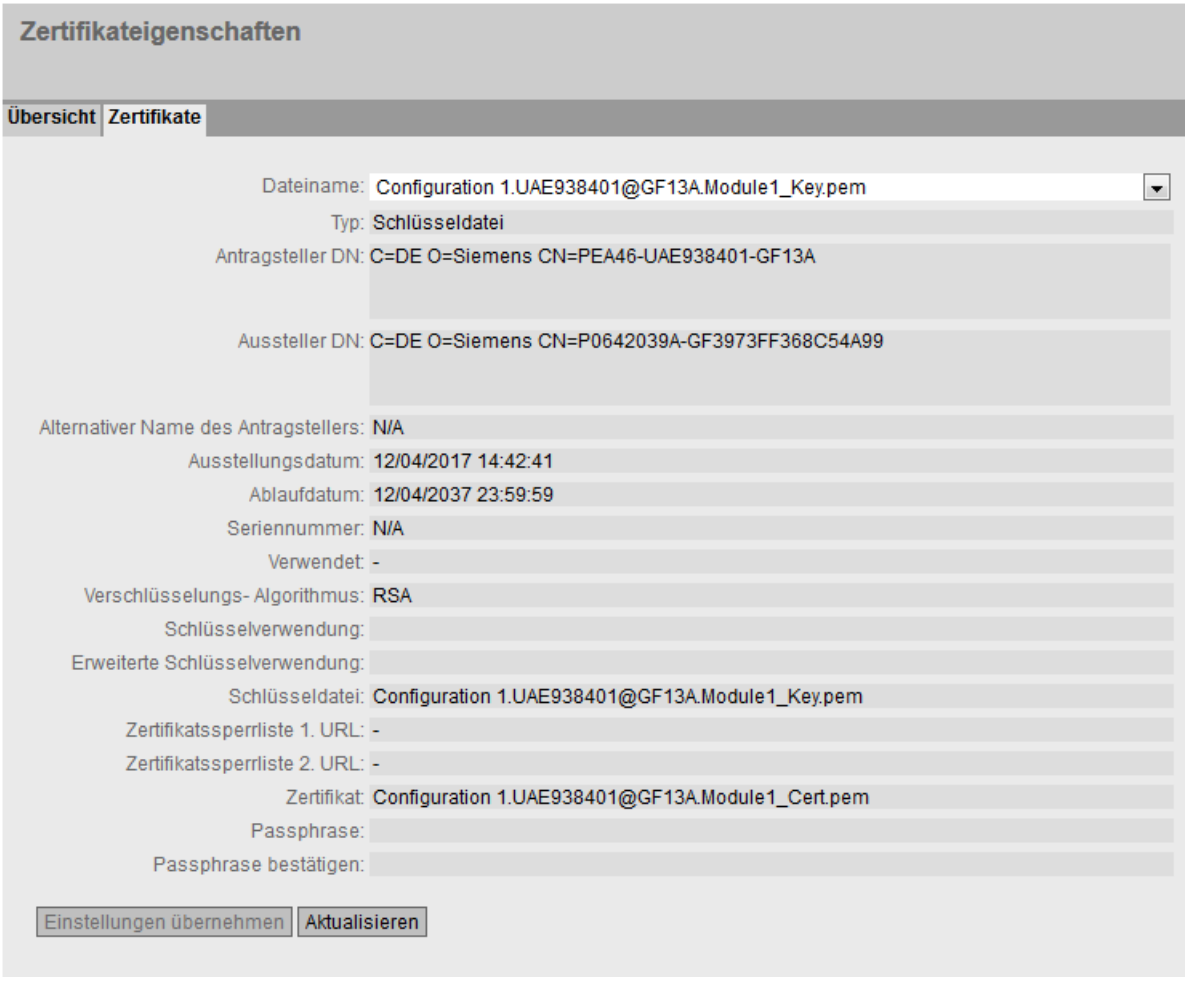
**Beschreibung**

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen. Nur nicht verwendete Zertifikate können gelöscht werden.
- **Typ**
  Zeigt die Art der geladenen Datei an.
  - CA-Zert
    Das CA-Zertifikat ist von einer zertifizierenden Stelle (CA = Certification Authority) signiert.
  - Gerätezertifikat
  - Schlüsseldatei
  - Remote-Zert
    Gegenstellenzertifikat
- **Dateiname**
  Zeigt den Dateinamen an.
- **Status**
  Zeigt an, ob das Zertifikat gültig oder bereits abgelaufen ist.
- **Antragsteller DN**
  Zeigt den Namen des Antragsstellers an.
- **Aussteller DN**
  Zeigt den Namen des Zertifikatsausstellers an.
- **Ausstellungsdatum**
  Zeigt den Beginn des Gültigkeitszeitraums des Zertifikats an
- **Ablaufdatum**
  Zeigt das Ende des Gültigkeitszeitraums des Zertifikats an.
- **Verwendet**
  Zeigt an, welche Funktion das Zertifikat nutzt.

### 5.10.4.2 Zertifikate

Das Format des Zertifikats basiert auf X.509, einem Standard der ITU-T zum Erstellen digitaler Zertifikate. In diesem Standard ist der schematische Aufbau von X.509-Zertifikaten beschrieben. Weitere Informationen dazu finden Sie im Internet unter "http://www.itu.int".

Auf dieser WBM-Seite kann der Inhalt folgender Strukturelemente angezeigt werden. Wenn in dem ausgewählten Zertifikat das Strukturelement nicht vorhanden oder befüllt ist, wird im Feld nichts angezeigt. Bestimmte Einträge sind nur editierbar, wenn Sie unterstützt werden.




## Beschreibung

- **Dateiname**
  Wählen Sie das gewünschte Zertifikat aus.
- **Typ**
  Zeigt die Art der geladenen Datei an.
  - CA-Zert
    Das CA-Zertifikat ist von einer zertifizierenden Stelle (CA = Certification Authority) signiert.
  - Gerätezertifikat
  - Schlüsseldatei
  - Remote-Zert
    Gegenstellenzertifikat
- **DN**
  Zeigt den Namen des Antragstellers an.

- **Aussteller DN**
  Zeigt den Namen des Zertifikatsausstellers an.
- **Alternativer Name des Antragstellers**
  Wenn vorhanden, wird ein alternativer Name des Antragstellers angezeigt.
- **Ausstellungsdatum**
  Zeigt den Beginn des Gültigkeitszeitraums des Zertifikats an
- **Ablaufdatum**
  Zeigt das Ende des Gültigkeitszeitraums des Zertifikats an.
- **Seriennummer**
  Zeigt die Seriennummer des Zertifikats an.
- **Verwendet**
  Zeigt an, welche Funktion das Zertifikat nutzt.
- **Verschlüsselungs-Algorithmus**
  Zeigt an, welches kryptografisches Verfahren verwendet wird.
- **Schlüsselverwendung**
  Zeigt an, für welchen Zweck der zum Zertifikat gehörende Schlüssel verwendet wird, z. B. zum Verifizieren digitaler Signaturen.
- **Erweiterte Schlüsselverwendung**
  Zeigt an, ob der Verwendungszweck noch zusätzlich beschränkt ist, z. B. nur zum Verifizieren von Signaturen des CA-Zertifikats.
- **Schlüsseldatei**
  Zeigt die Schlüsseldatei an.
- **Zertifikatssperrliste 1. URL**
  Tragen Sie die URL ein, über die die Sperrliste abgerufen werden kann. Nur editierbar, wenn vom Zertifikat unterstützt.
- **Zertifikatssperrliste 2. URL**
  Tragen Sie eine Alternativ-URL ein. Wenn die Sperrliste über die 1. URL nicht abrufbar ist, wird die Alternativ-URL verwendet. Nur editierbar, wenn vom Zertifikat unterstützt.
- **Zertifikat**
  Zeigt den Namen des Zertifikats an.
- **Passphrase**
  Tragen Sie das Passwort für das Zertifikat ein. Nur editierbar, wenn die verschlüsselte Datei Passwort-geschützt ist.
- **Passphrase bestätigen**
  Tragen Sie das Passwort nochmals ein. Nur editierbar, wenn die verschlüsselte Datei Passwort-geschützt ist.

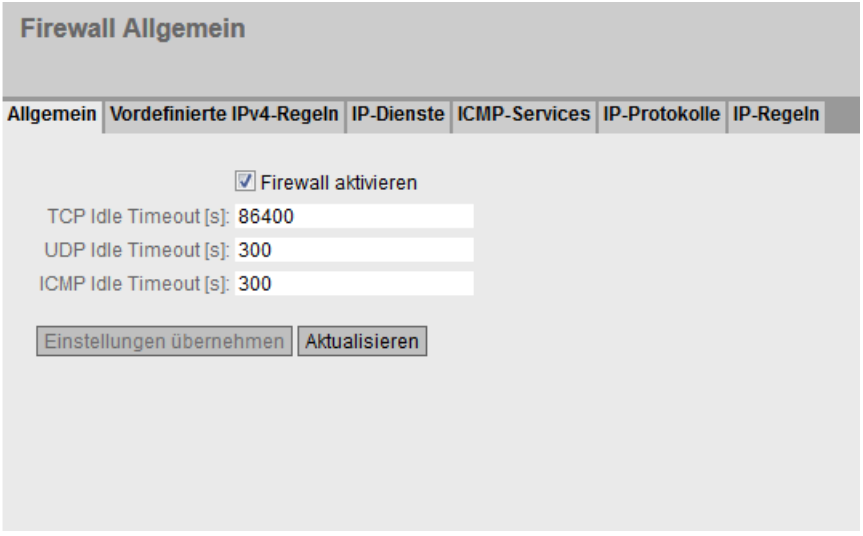
## 5.10.5 Firewall

### 5.10.5.1 Allgemein

Auf dieser WBM-Seite aktivieren Sie die Firewall.

**Hinweis**

Bitte beachten Sie, wenn Sie die Firewall deaktivieren, dann ist ihr internes Netz ungeschützt.




### Beschreibung

Die Seite enthält Folgendes:

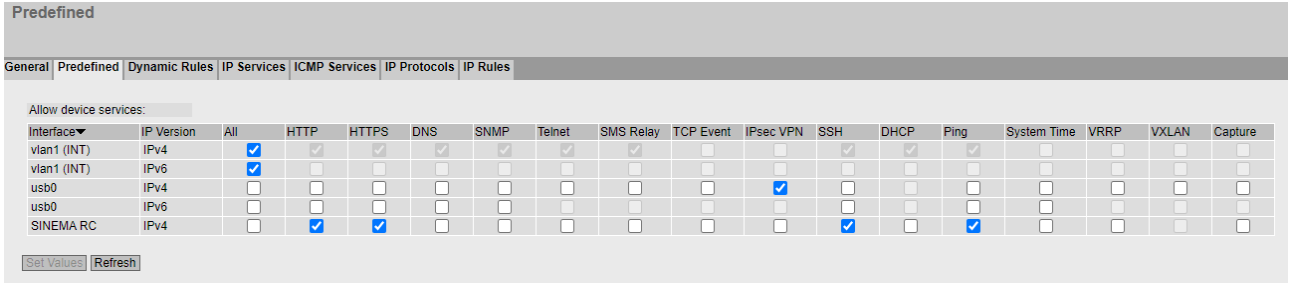
- **Firewall aktivieren**
  Wenn aktiviert, ist die Firewall aktiv.
- **TCP Idle Timeout [s]**
  Geben Sie die gewünschte Zeitspanne in Sekunden ein. Wenn kein Datenaustausch stattfindet, wird nach Ablauf dieser Zeitspanne die TCP-Verbindung automatisch getrennt.
  Der Wertebereich ist 1 bis 21474836.
  Default-Einstellung: 86400 Sekunden
- **UDP Idle Timeout [s]**
  Geben Sie die gewünschte Zeitspanne in Sekunden ein. Wenn kein Datenaustausch stattfindet, wird nach Ablauf dieser Zeitspanne die UDP-Verbindung automatisch getrennt.
  Der Wertebereich ist 1 bis 21474836.
  Default-Einstellung: 300 Sekunden
- **ICMP Idle Timeout [s]**
  Geben Sie die gewünschte Zeitspanne in Sekunden ein. Wenn kein Datenaustausch stattfindet, wird nach Ablauf dieser Zeitspanne die ICMP-Verbindung automatisch getrennt.
  Der Wertebereich ist 1 bis 21474836.
  Default-Einstellung: 300 Sekunden

- **Zustandssynchronisation aktivieren**
- **Lokale Schnittstelle**
  Schnittstellen mit DHCP können nicht gewählt werden.
- **Lokale IP-Adresse**
- **IP-Adresse Sync-Partner**
- Port Sync-Partner

### 5.10.5.2 Vordefinierte Regeln

Die WBM-Seite enthält vordefinierte IP-Paketfilter-Regeln. Wenn Sie eigene IP-Paketfilter-Regeln anlegen, haben diese eine höhere Priorität als die vordefinierten IP-Paketfilter-Regeln.

Stellen Sie ein, welche IPv4-Dienste des Gerätes von welcher Schnittstelle aus erreichbar sein sollen.



## Beschreibung

- **Schnittstelle**
  Die Liste ist dynamisch.
  - pppx bzw. usb0 (nur beim M876-4, MUM856)
    Erlaubt den Zugriff von der WAN-Schnittstelle auf das Gerät.
  - VLANx
    Erlaubt den Zugriff vom IP-Subnetz auf das Gerät. Verfügbar sind VLANs mit konfiguriertem IP-Subnetz.
  - SINEMA RC
    Erlaubt den Zugriff vom SINEMA RC-Server auf das Gerät. Nur mit KEY-PLUG SINEMA RC verfügbar.
  - OpenVPN-Verbindung, IPsec VPN-Verbindung
    Erlaubt den VPN-Tunnelpartner, die über die VPN-Verbindung erreichbar sind, den Zugriff auf das Gerät.
    Wenn Sie eine VPN-Verbindung angelegt haben, wird in der Liste der Verbindungsname angezeigt.
  - **IP-Version**
    Zeigt an, für welche IP-Version die Firewallregeln gelten.
    IPv4
    IPv6 (nur beim M876-4 und MUM85x)
- Der Zugriff über die Firewall auf folgende IPv4-Dienste des Geräts wird erlaubt:
  - Alle
    Alle vordefinierten IPv4-Dienste.
  - HTTP
    Zum Zugriff auf das Web Based Management.
  - HTTPS
    Zum gesicherten Zugriff auf das Web Based Management.

    **Hinweis**

    **HTTP und HTTPS deaktiviert**

    Wenn Sie HTTP und HTTPS deaktivieren, ist das WBM des Geräts nicht mehr erreichbar.

    **HTTPS deaktiviert**

    Wenn Sie HTTPS deaktivieren, können Sie nur noch über HTTP auf das WBM zugreifen. Vorausgesetzt, unter "System > Konfiguration > HTTP-Dienste" ist "HTTP & HTTPS" eingestellt. Ist z. B. "HTTP nach HTTPS umleiten" eingestellt, kann der Zugriff über HTTP nicht nach HTTPS umgeleitet werden. Somit ist das WBM des Geräts nicht mehr erreichbar.
  - DNS
    DNS-Anfragen an das Gerät. Nur notwendig, wenn am Gerät die Funktion "DNS-Relay" aktiv ist.
  - SNMP
    Eingehende SNMP-Verbindungen. Notwendig, um z. B. mit einem MIB-Browser auf die SNMP-Informationen des Geräts zuzugreifen.

- Telnet
  Zum unverschlüsselten Zugriff auf das CLI.
- SMS Relay (nur beim M87x / MUM85x)
  Zum Versenden von SMS aus dem lokalen Netz.
- TCP Event
  Für eingehende TCP-Pakete. Notwendig, um z. B. die Funktion "Sleep Mode" auszulösen.
- IPsec VPN
  Erlaubt den IKE (Internet Key Exchange) Datenverkehr vom externen Netz zum Gerät. Notwendig, wenn eine IPsec VPN-Gegenstelle eine Verbindung zu diesem Gerät herstellen soll.
- SSH
  Zum verschlüsselten Zugriff auf das CLI.
- DHCP
  Zugriff auf den DHCP-Server oder den DHCP-Client.
- Ping
  Zugriff auf die Ping-Funktion.
- Systemzeit
  Zugriff auf NTP und SNTP.
- Cloud Connector
  Zugriff auf den integrierten TIA Portal Cloud Connector Server und die Geräte, die über die Schnittstelle erreichbar sind.
- VRRP
  Zugriff auf VRRPv3
- VXLAN
  Zum Aufbau des VXLAN-Tunnels und zum Empfangen der Frames. Notwendig, wenn der Tunnelendpunkt eine Verbindung zu diesem Gerät herstellt.
- Capture
  Zugriff auf die Funktion "Packet Capture" von der aktivierten Schnittstelle.

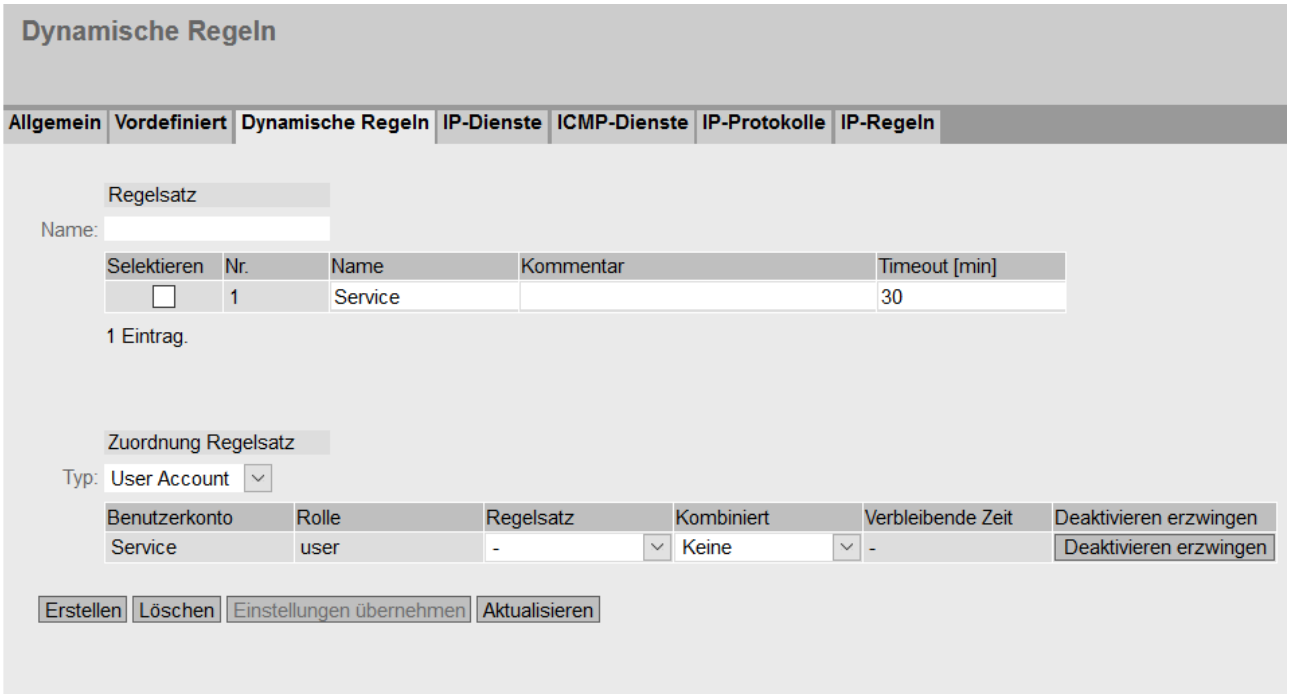
### 5.10.5.3 Dynamische Regeln

Auf dieser Seite definieren Sie dynamische Regelsätze. Mit einem Regelsatz lassen sich die Firewall-Regeln zusammenfassen, die z. B. für den Remote-Zugriff notwendig sind.

Sie können ein Regelsatz einem oder mehreren Benutzern zuordnen. Wenn die Anmeldung des Benutzers erfolgreich war, wird der für diesen Benutzer vorgesehene Firewall-Regelsatz aktiviert.

Nach der Anmeldung wird ein Timer gestartet. Nach Ablauf der Zeit wird der Benutzer automatisch vom Gerät abgemeldet.

Zusätzlich können Sie die Regelsätze über die Zeit steuern.  Es wird eine Start- und Endzeit konfiguriert. Zwischen den beiden Zeiten werden die dem Regelsatz zugewiesenen Firewall-Regeln aktiviert.




## Beschreibung

**Bereich "Regelsatz"**

- **Name**
  Legen Sie einen eindeutigen Namen für den Regelsatz fest. Wenn Sie auf die Schaltfläche "Erstellen" klicken, wird eine neue Zeile mit einer eindeutigen Nummer angelegt.

Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Nr.**
  Zeigt die eindeutige Nummer des Eintrags an.
- **Name**
  Name des Regelsatzes. Bei Bedarf ist der Name änderbar.
- **Kommentar**
  Kommentar, der den Regelsatz näher beschreibt.
- **Timeout [min]**
  Der Zugriff ist zeitlich begrenzt. Legen Sie die Dauer des Zugriffs fest. Bei Bedarf kann der Benutzer auf der Seite "Dynamische Firewall-Informationen" die Zugriffszeit über die Schaltfläche "Timeout zurücksetzen" verlängern.

**Bereich "Zuordnung Regelsatz"**

- **Typ**
  Legen Sie fest welcher Regelsatz, wem zugeordnet wird. Die Anzeige der nachfolgenden Tabelle ist abhängig von der Auswahl bei "Typ".
  - Benutzerkonto
    Der Regelsatz wird über ein lokales Benutzerkonto aktiviert.
  - Digitaler Eingang
    Durch das Ansteuern des digitalen Eingangs wird der Regelsatz ausgeführt.
    Voraussetzung ist, dass unter "System > Ereignisse > Konfiguration" beim Ereignis "Firewall" der Eintrag "Digitaler Eingang" aktiviert ist.
  - Radius Rolle
    Der Regelsatz wird durch eine RADIUS-Rolle aktiviert.
  - RADIUS-Benutzer
    Der Regelsatz wird durch einen RADIUS-Benutzer aktiviert.
  - Zeitgesteuert
    Die Ausführung des Regelsatzes ist zeitgesteuert.

Die Tabelle "Benutzerkonto" enthält folgende Spalten:

- Benutzerkonto
  Nur die Benutzer mit dem Remote-Zugriff "Nur" oder "Zusätzlich" werden angezeigt.
- Rolle
  Zeigt die Rolle des Benutzers.
- Regelsatz
  Legen Sie den Regelsatz fest, der für diesen Benutzer gültig ist.
- Kombiniert mit
  Kombiniert die Benutzeranmeldung mit einem Ereignis, z. B. dem Ereignis "Digitaler Eingang". Um sich an der WBM-Seite für die dynamische Firewall anzumelden, müssen am digitalen Eingang die Spannung anliegen und die Benutzeranmeldung erfolgreich sein.
- Verbleibende Zeit
  Wenn dieser Benutzer angemeldet ist, wird die verbleibende Zeit für den Zugriff angezeigt.
- Deaktivieren erzwingen
  Ein Benutzer mit Administratorrechten kann über die Schaltfläche den aktiven Benutzer abmelden.

Die Tabelle "**Digitaler Eingang**" enthält folgende Spalten:

- Digitaler Eingang
  Die verfügbaren digitalen Eingänge.
- Regelsatz
  Legen Sie den Regelsatz fest, der über den digitalen Eingang gesteuert wird.
- Quelle dynamisch (Bereich)
  Tragen Sie die IP-Adresse oder einen IP-Bereich ein, die die IP-Pakete senden darf.
- Status
  Zeigt die verbleibende Zeit für den Zugriff an.

Die Tabelle "**RADIUS-Rolle**" enthält folgende Spalten:

- Rolle
  Zeigt den Rollenname an. Nur die Rollen mit dem Remote-Zugriff "Zusätzlich" werden angezeigt. Vorausgesetzt, die Rolle wurde auf dem RADIUS-Server angelegt und der Rolle wurden RADIUS-Benutzer zugeordnet.
- Regelsatz
  Legen Sie den Regelsatz fest, der für diese RADIUS-Rolle gültig ist.
- Kombiniert mit
  Kombiniert die Anmeldung mit einem Ereignis, z. B. dem Ereignis "Digitaler Eingang". Um sich an der WBM-Seite für die dynamische Firewall anzumelden, müssen am digitalen Eingang die Spannung anliegen und die Anmeldung erfolgreich sein.
- Anzahl
  Nach erfolgreicher Anmeldung wird die Anzahl der über RADIUS aktiven Benutzer angezeigt, die der RADIUS-Rolle zugeordnet sind.
- Deaktivieren erzwingen
  Ein Benutzer mit Administratorrechten kann über die Schaltfläche die RADIUS-Rolle abmelden.

Die Tabelle "**RADIUS-Benutzer**" enthält folgende Spalten:

- Benutzer
  Zeigt die Benutzer an, die der Rolle zugeordnet sind.
  Auf dem Gerät wird eine Rolle mit dem Remote-Zugriff "Zusätzlich" angelegt und einer Gruppe zugeordnet. Die Namen der Gruppe muss exakt mit den Namen der Benutzergruppen des RADIUS-Servers übereinstimmen.
- Rolle
  Die Rolle, die dem RADIUS-Benutzer zugeordnet ist.
- Verbleibende Zeit
  Wenn dieser Benutzer angemeldet ist, wird die verbleibende Zeit für den Zugriff angezeigt.
- Deaktivieren erzwingen
  Ein Benutzer mit Administratorrechten kann über die Schaltfläche die RADIUS-Rolle abmelden.

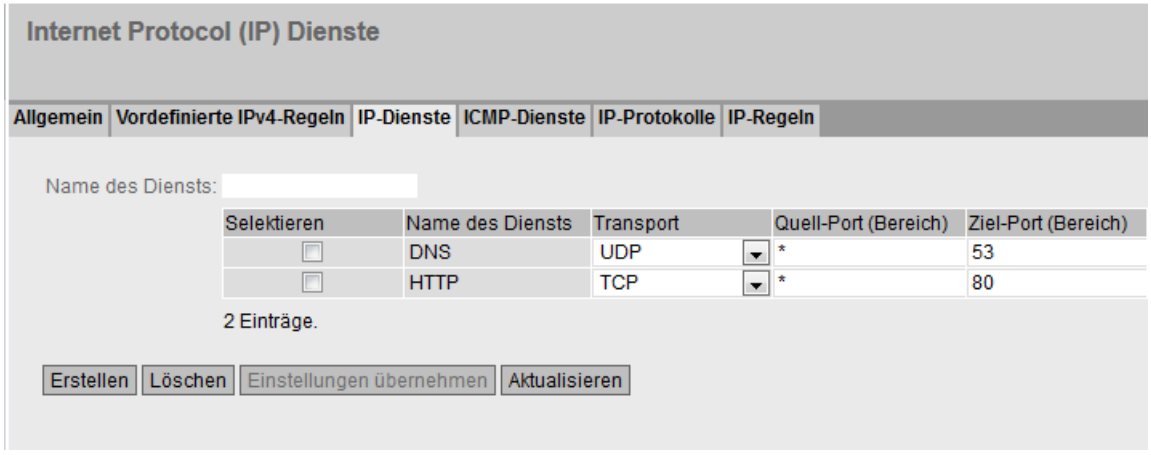
Die Tabelle "**Zeitgesteuert**" enthält folgende Spalten:

- Zeitgesteuert
  Index des Eintrags.
- Regelsatz
  Legen Sie den Regelsatz fest, der zeitgesteuert wird.
- Kombiniert mit
  Kombiniert die Zeitsteuerung mit einem Ereignis, z. B. dem Ereignis "Digitaler Eingang". Um sich an der WBM-Seite für die dynamische Firewall anzumelden, müssen am digitalen Eingang die Spannung anliegen und die Anmeldung erfolgreich sein.

- Zyklus
  Legen Sie den Ausführungszyklus für die Zeitsteuerung fest.
  - Täglich
  - Wöchentlich
  - Monatlich
- Tage
  Wenn beim Zyklus "Wöchentlich" und "Monatlich" eingestellt ist, legen Sie die Tage fest. Geben Sie die Tage durch Komma getrennt ein, z. B. 1,3,4
  - Wöchentlich: 1 - 7
  - Monatlich: 1 - 31
- Quelle dynamisch (Bereich)
  - Einzelne IP-Adresse: Geben Sie die IP-Adresse an
  - IP-Bereich: Geben Sie den Bereich mit Startadresse "-" Endadresse an, z. B.
    IPv4:192.168.100.10 - 192.168.100.20
    IPv6: fe80:: - febf::
  - Alle IP-Adressen:
    IPv4: " 0.0.0.0/0"
    IPv6: "::"
  - Wenn der Regelsatz durch einen Benutzer aktiviert wird, wird der Platzhalter DYNAMIC durch die IP-Adresse des verwendeten Endgeräts ersetzt..
- Startzeit
  Geben Sie die Startzeit im Format HH:MM ein.
- Endzeit
  Geben Sie die Endzeit im Format HH:MM ein.
- Aktivieren
  Wenn aktiviert, ist der Regelsatz zeitgesteuert. Beim Auslösen der zeitgesteuerten Firewall-Regeln wird die Verbindung kurzzeitig unterbrochen.

### 5.10.5.4 IP-Dienste

Auf dieser WBM-Seite definieren Sie IP-Dienste. Mithilfe der IP-Dienst-Definitionen können Sie Firewall-Regeln definieren, die auf bestimmte Dienste angewendet werden. Sie vergeben hierbei einen Namen und ordnen diesem die Dienstparameter zu. Bei der Projektierung der IP-Regeln verwenden Sie dann einfach diesen Namen.




## Beschreibung

Die Seite enthält Folgendes:

- **Name des Diensts**
  Tragen Sie den Namen für den IP-Dienst ein. Der Name muss eindeutig sein.

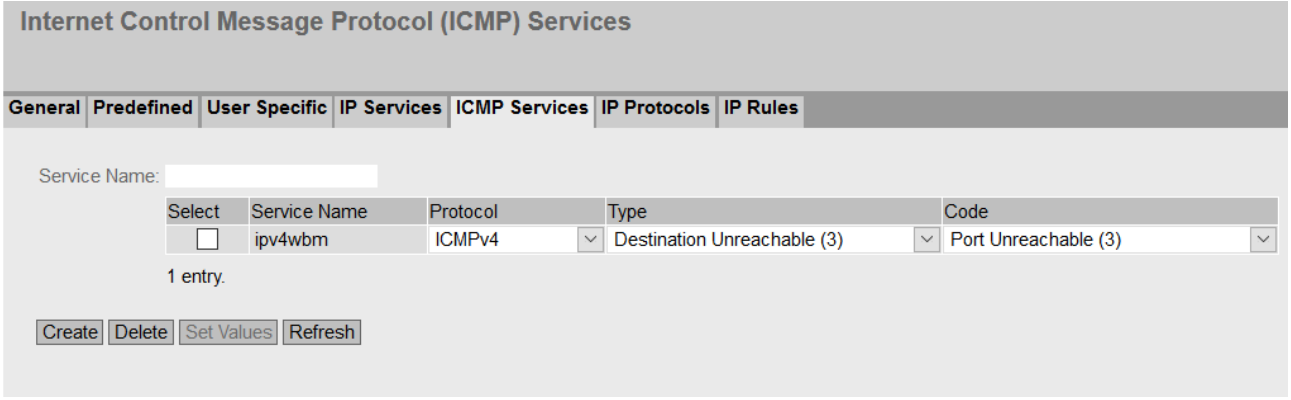
Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Name des Diensts**
  Zeigt den Namen des IP-Diensts an.
- **Transport**
  Legen Sie den Protokolltyp fest.
  - UDP
    Die Regel gilt nur für UDP-Telegramme.
  - TCP
    Die Regel gilt nur für TCP-Telegramme.

- **Quell-Port (Bereich)**
  Tragen Sie den Quell-Port ein. Die Regel gilt genau für den angegebenen Port.
  - Wenn die Regel für einen Port-Bereich gelten soll, geben Sie den Bereich mit Start-Port "-" End-Port an, z. B. 30 - 40.
  - Wenn die Regel für alle Ports gelten soll, geben Sie "*" ein.
- **Ziel-Port (Bereich)**
  Tragen Sie den Ziel-Port ein. Die Regel gilt genau für den angegebenen Port.
  - Wenn die Regel für einen Port-Bereich gelten soll, geben Sie den Bereich mit Start-Port "-" End-Port an, z. B. 30 - 40.
  - Wenn die Regel für alle Ports gelten soll, geben Sie "*" ein.

### 5.10.5.5 ICMP-Dienste

Auf dieser Seite definieren Sie ICMP-Dienste. Mithilfe der ICMP-Dienst-Definitionen können Sie Firewall-Regeln definieren, die auf bestimmte Dienste angewendet werden. Sie vergeben hierbei einen Namen und ordnen diesem die Dienstparameter zu. Bei der Projektierung der IP-Regeln verwenden Sie dann einfach diesen Namen.




## Beschreibung

Die Seite enthält Folgendes:

- **Name des Diensts**
  Tragen Sie einen Namen für den ICMP-Dienst ein. Der Name muss eindeutig sein.

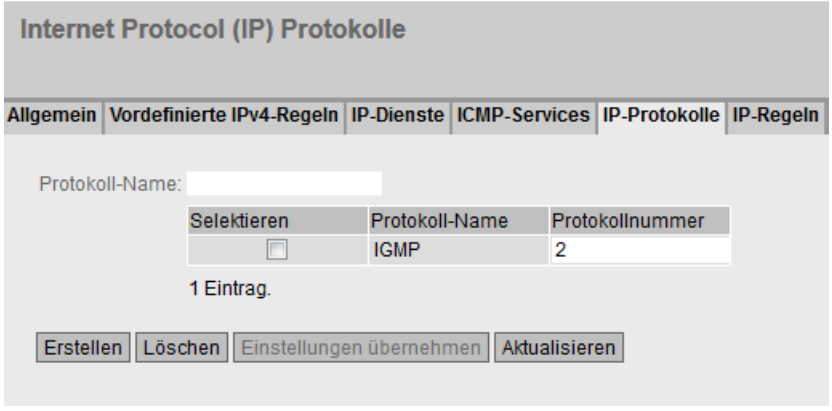
Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Name des Diensts**
  Zeigt den Namen des ICMP-Diensts an.
- **Protokoll**
  Zeigt die Version des ICMP-Protokolls an.

- **Typ**
  Legen Sie den ICMP-Pakettyp fest. Einige Beispiele sind:
  - Destination Unreachable
    IP-Telegramm kann nicht zugestellt werden.
  - Time Exceeded
    Zeitlimit überschritten
  - Echo-Request
    Echo-Frage, besser bekannt als Ping.
- **Code**
  Der Code beschreibt den ICMP-Pakettyp genauer. Die Auswahl ist abhängig vom gewählten ICMP-Pakettyp.
  Bei "Destination Unreachable" ist z. B. "Code 1" Host ist nicht erreichbar.

### 5.10.5.6 IP-Protokolle

Auf dieser WBM-Seite können Sie benutzerdefinierte Protokolle konfigurieren, z. B. IGMP für Multicast-Gruppen. Sie vergeben hierbei einen Protokollnamen und ordnen diesem die Dienstparameter zu. Bei der Projektierung der IP-Regeln verwenden Sie dann einfach diesen Protokollnamen.




## Beschreibung

Die Seite enthält Folgendes:

- **Protokollname**
  Tragen Sie einen Namen für das Protokoll ein.

Die Seite enthält folgende Optionskästchen:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Protokollname**
  Zeigt den Protokollnamen an.
- **Protokollnummer**
  Tragen Sie die Protokollnummer ein, z. B. 2. Eine Liste der Protokollnummern finden Sie auf den Internetseiten von iana.org

## Vorgehensweise

**Protokoll IGMP  anlegen**

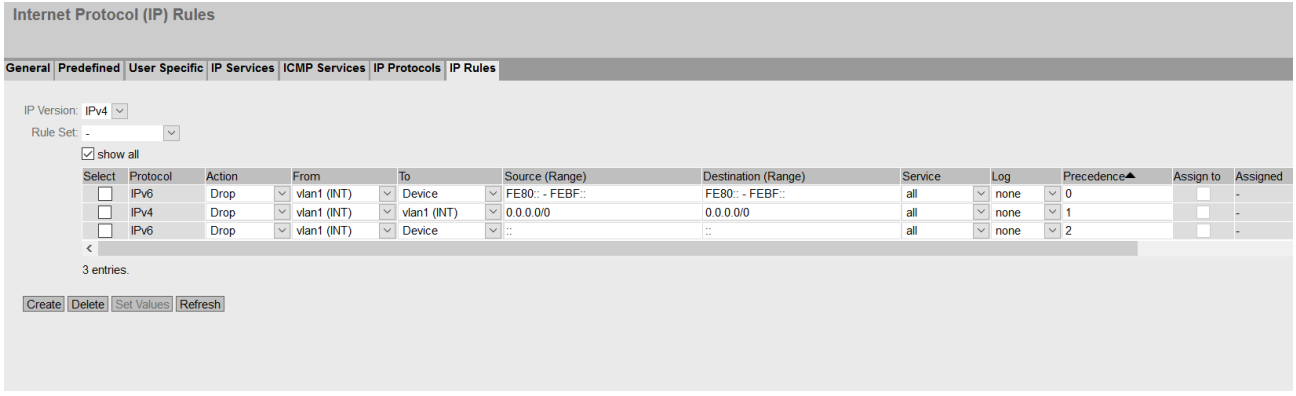
1. Tragen Sie bei "Protokollname" IGMP ein.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen". In der Tabelle wird ein neuer Eintrag erzeugt.
3. Tragen Sie bei "Protokollnummer" 2 ein.

### 5.10.5.7 IP-Regeln

Auf dieser WBM-Seite legen Sie eigene IP-Regeln für die Firewall fest.

Die hier erstellten IP-Regeln haben Vorrang:

- vor den vordefinierten IP-Regeln und
- vor den IP-Regeln, die aufgrund einer Verbindungsprojektierung (SINEMA RC) automatisch angelegt werden.




## Beschreibung

- **IP-Version**
  Legen Sie fest für welche IP-Version die Firewall-Regel gelten soll.
- **Regelsatz**
  Wählen Sie den gewünschten Regelsatz aus. In der Tabelle werden dann nur die IP-Regeln angezeigt, die diesem Regelsatz zugeordnet sind. Vorausgesetzt "Alle anzeigen" ist deaktiviert.
- **Alle anzeigen**
  Wenn aktiviert, werden alle verfügbaren IP-Regeln angezeigt. Mit der Einstellung "Zuordnen" weisen Sie eine IP-Regel dem ausgewählten Regelsatz zu.

Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Protokoll**
  Zeigt die Version des IP-Protokolls an.
- **Aktion**
  Wählen Sie aus, wie mit eintreffenden IP-Paketen zu verfahren ist:
  - "Accept" – Die Datenpakete dürfen passieren,
  - "Reject" – Die Datenpakete werden abgewiesen, der Absender erhält eine entsprechende Meldung,
  - "Drop" – Die Datenpakete werden ohne Rückmeldung an den Absender verworfen.
- **Von / Nach**
  Legen Sie die Kommunikationsrichtung der IP-Regel fest.
  - VLANx: VLANs mit konfiguriertem Subnetz
  - NVEx: Virtuelle Schnittstelle, über die der VXLAN-Tunnel aufgebaut wird.
  - Device: Gerät
  - ppp0 bzw. usb0 (nur bei M876-4 / MUM85x): WAN-Schnittstelle
  - SINEMA RC: Verbindung zum SINEMA RC-Server
  - IPsec: Entweder alle IPsec VPN-Verbindungen (all) oder eine spezifische IPsec VPN-Verbindung

- **Quelle (Bereich)**
  Tragen Sie die IP-Adresse oder einen IP-Bereich ein, die IP-Pakete empfangen darf.
  - Einzelne IP-Adresse: Geben Sie die IP-Adresse an
  - IP-Bereich: Geben Sie den Bereich mit Startadresse "-" Endadresse an, z. B.
    IPv4:192.168.100.10 - 192.168.100.20
    IPv6: fe80:: - febf::
  - Alle IP-Adressen:
    IPv4: " 0.0.0.0/0"
    IPv6; "::"
  - Wenn der Regelsatz durch einen Benutzer aktiviert wird, wird der Platzhalter DYNAMIC durch die IP-Adresse des verwendeten Endgeräts ersetzt.

    **Hinweis**

    **Digitaler Eingang und Platzhalter DYNAMIC**

    Wenn der Regelsatz durch das Ansteuern des digitalen Eingangs ausgeführt wird, wird der Platzhalter DYNAMIC durch die Einstellung bei "Quelle dynamisch (Bereich)" ersetzt. Die Einstellung konfigurieren Sie unter "Security > Firewall > Dynamisch Regeln".

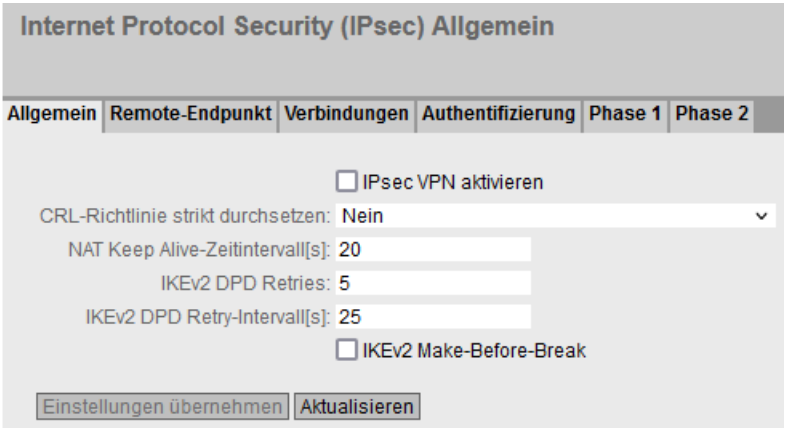
  **Ziel (Bereich)**
  Tragen Sie die IP-Adresse oder einen IP-Bereich ein, die IP-Pakete empfangen darf.
  - Einzelne IP-Adresse: Geben Sie die IP-Adresse an
  - IP-Bereich: Geben Sie den Bereich mit Startadresse "-" Endadresse an, z. B.
    IPv4:192.168.100.10 - 192.168.100.20
    IPv6: fe80:: - febf::
  - Alle IP-Adressen:
    IPv4: " 0.0.0.0/0"
    IPv6; "::"
  - Wenn der Regelsatz durch einen Benutzer aktiviert wird, wird der Platzhalter DYNAMIC durch die IP-Adresse des verwendeten Endgeräts ersetzt..
- **Dienst**
  Wählen Sie den Dienst oder den Protokollnamen aus, für den diese Regel gültig ist.
- **Log**
  Legen Sie fest, ob das Zutreffen der Regel protokolliert wird und welche Ereignisschwere der Eintrag hat.
  Folgende Einstellungen gibt es:
  - none
    Das Zutreffen wird nicht protokolliert.
  - info / warning / critical
    Das Zutreffen wird mit der gewählten Ereignisschwere protokolliert. Die Logdatei wird unter "Information" > "Log-Tabellen" > "Firewall-Log" angezeigt.
- **Reihenfolge**
  Aufsteigend, beginnend mit 0 legen Sie die Reihenfolge der IP-Regeln der Firewall fest, in der die ÍP-Regeln abgearbeitet werden.

- **Zuordnen**
  Um die IP-Regeln dem ausgewählten Regelsatz zuzuordnen, aktivieren Sie bei den gewünschten IP-Regeln die Einstellung und klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
- **Zugeordnet**
  Zeigt an, welchem Regelsatz diese IP-Regel zugeordnet ist. Die IP-Regeln sind auch mehreren Regelsätzen zuordenbar. Ist die IP-Regel allen Regelsätzen zugeordnet, wird "all" angezeigt.
- **Bezeichnung**
  Zeigt an, von wem die IP-Regel erstellt wurde.
  – NETMAP - Automatisch erstellte Firewallregel

## 5.10.6 IPsec VPN

### 5.10.6.1 Allgemein

Auf der WBM-Seite konfigurieren Sie die Grundeinstellungen für VPN.




#### Beschreibung

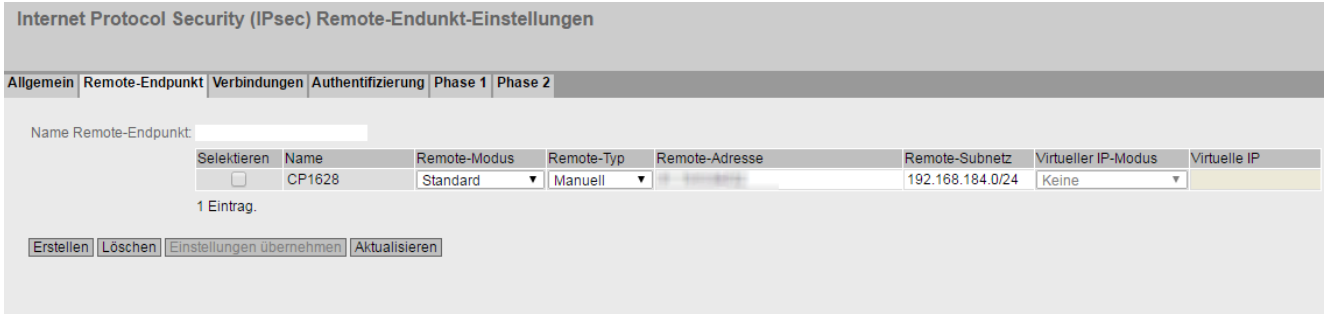
Die Seite enthält Folgendes:

- **IPsec VPN aktivieren**
  Aktivieren oder deaktivieren Sie das IPsec-Verfahren für VPN.
- **CRL-Richtlinie strikt durchsetzen**
  Wenn aktiviert, wird die Gültigkeit der Zertifikate anhand der Zertifikatssperrliste (CRL-Certificate Revocation List) überprüft. In der Zertifikatssperrliste sind die von der Zertifizierungsstelle ausgestellten Zertifikate aufgeführt, die vor ihrem gesetzten Ablaufdatum ihre Gültigkeit verloren haben. Welche Zertifikatssperrliste verwendet wird, konfigurieren Sie auf der WBM-Seite "Zertifikate (Seite 403)".

- **NAT Keep Alive-Zeitintervall**
  Legen Sie fest, in welchem Zeitabstand Lebenszeichentelegramme (Keep Alive) gesendet werden. Befindet sich ein NAT-Gerät zwischen zwei VPN-Endpunkten, dann wird bei Inaktivität die Verbindung aus dessen dynamischer NAT-Tabelle gelöscht. Um dies zu verhindern, werden die Lebenszeichentelegramme gesendet.
- **IKEv2 DPD Retries**
  Geben Sie die Anzahl der zulässigen Fehlversuche an, nach denen die IKEv2-Verbindung als unterbrochen angesehen wird. Die Einstellung gilt für alle IKEv2-Verbindungen.
- **IKEv2 DPD Retry Interval[s]**
  Legen Sie fest, in welchem Zeitabstand die Fehlversuche gesendet werden.
- **IKEv2 Make-Before-Break**
  Wenn aktiviert, wird bei einer Re-Authentifizierung ein Duplikat des IKE und aller IPSec-Sicherheitszuordnungen erstellt und die alten werden gelöscht. Dadurch wird verhindert, dass es zu  Unterbrechungen der VPN-Kommunikation während der Re-Authentifizierung kommt. Diese Einstellung erfordert, dass beide VPN-Endpunkte überlappende SAs verarbeiten können

### 5.10.6.2 Remote-Endpunkt

Auf dieser WBM-Seite konfigurieren Sie die Gegenstelle (VPN-Endpunkt).




## Beschreibung

Die Seite enthält Folgendes:

- **Name Remote-Endpunkt**
  Tragen Sie einen Namen für die Gegenstelle ein und klicken Sie auf "Erstellen", um eine neue Gegenstelle zu erstellen.

Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Name**
  Zeigt den Namen der Gegenstelle an.

- **Remote-Modus**
  Legen Sie fest, welche Rolle die Gegenstellen einnimmt.
  - Roadwarrior
    Die erreichbaren Gegenstellen (Remote-Adresse) werden eingetragen. Die erreichbaren Remote-Subnetze werden von der Gegenstelle gelernt.
  - Standard
    Die erreichbare Gegenstelle (Remote-Adresse) und die erreichbaren Remote-Subnetze werden fest eingetragen.
- **Remote-Typ**
  Legen Sie die Art der Gegenstellen-Adresse fest.
  - Manuell
    Die Adresse der Gegenstelle ist bekannt. Das Gerät kann entweder als VPN-Client die VPN-Verbindung aktiv aufbauen, oder passiv auf den Verbindungsaufbau durch die Gegenstelle warten.
  - Beliebig
    Nimmt die Verbindung von Gegenstellen mit beliebiger IP-Adresse an. Das Gerät kann nur auf VPN-Verbindungen warten, aber nicht als aktiver Partner einen VPN-Tunnel aufbauen.
- **Remote-Adresse**
  Nur beim Remote-Typ "Manuell" editierbar.
  - Im Standard-Modus tragen Sie die WAN-IP-Adresse oder den DDNS-Hostnamen der Gegenstelle ein. Die Netzmaske ist immer /32
  - Im Roadwarrior-Modus können Sie entweder die Adresse der Gegenstelle vorgeben oder einen IP-Bereich eintragen, aus dem Verbindungen entgegengenommen werden.
- **Remote-Subnetz**
  - Im Standard-Modus geben Sie das erreichbare Subnetz der Gegenstelle ein. Verwenden Sie die CIDR-Schreibweise.
    Nur mit IKEv2 können Sie mehrere Subnetze verwenden. Geben Sie dann die Subnetze durch ein Komma getrennt ein.
  - Im Roadwarrior-Modus teilt die Gegenstelle dem Gerät seine erreichbaren Subnetze mit und das Gerät lernt diese.
- **Virtueller IP-Modus**
  Legen Sie fest, ob der Gegenstelle eine virtuelle IP-Adresse angeboten wird.
  Folgende Möglichkeiten gibt es:
  - Benutzerdefinierte IPv4
    Die virtuelle IP-Adresse ist aus dem bei "Virtuelle IP" festgelegten Band.
  - Keine
    Keine virtuelle IP-Adresse. Der VPN-Tunnel wird dynamisch zur internen IP-Adresse der Gegenstelle aufgebaut.
- **Virtuelle IP**
  Legen Sie das Subnetz fest (CIDR), aus dem die Gegenstelle eine virtuelle IP-Adresse angeboten bekommt.
  Nur editierbar, wenn bei "Virtueller IP-Modus" "Benutzerdefinierte IPv4" ausgewählt ist.

## Vorgehensweise

**VPN-Standard-Modus projektieren**

1. Tragen Sie bei "Name Remote-Endpunkt" den Namen der Gegenstelle ein.
2. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag erzeugt.
3. Wählen Sie bei "Remote-Modus" "Standard" aus.
4. Wählen Sie bei "Remote-Typ" "Manuell" aus.
5. Tragen Sie bei "Remote-Adresse" die WAN-IP-Adresse und bei "Remote-Subnetz" das Subnetz der Gegenstelle ein.
6. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

**VPN-Roadwarrior-Modus projektieren**

1. Tragen Sie bei "Name Remote-Endpunkt" den Namen der Gegenstelle ein.
2. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag erzeugt.
3. Wählen Sie bei "Remote-Modus" "Roadwarrior" aus.
4. Wählen Sie bei "Remote-Typ" "Beliebig" aus.
5. Tragen Sie bei "Remote-Adresse" die IP-Adresse des entfernten Netzes ein.
6. Legen Sie bei "Virtueller IP-Modus" fest, wie die IP-Adresse des VPN-Gateways bezogen wird.
7. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

### 5.10.6.3 Verbindungen

Auf dieser WBM-Seite konfigurieren Sie die Grundeinstellungen für die VPN-Verbindung. Mit diesen Einstellungen kann das Gerät (lokaler Endpunkt) einen gesicherten VPN-Tunnel zur Gegenseite aufbauen. Die Sicherheitseinstellungen legen Sie auf der WBM-Seite "Authentifizierung" fest.

---

**Hinweis**

**Mehrere IPsec VPN-Verbindungen über denselben VPN-Endpunkt**

Wenn Sie über denselben VPN-Endpunkt IPsec VPN-Verbindungen zu verschiedenen Remote-Subnetzen angelegt haben, ist die zuerst projektierte VPN-Verbindung (niedrigster Index) die Hauptverbindung (Parent).

Über die Hauptverbindung werden alle weiteren IPsec VPN-Verbindungen (Child) angelegt und aufgebaut. Wenn nun alle VPN-Tunnel aufgebaut sind und die Hauptverbindung beendet wird, so werden allen Child-Verbindungen unterbrochen. Nach Ablauf des DPD-Timeouts werden alle IPsec VPN-Verbindungen wieder neu über Hauptverbindung aufgebaut.

Wenn nur eine Child-Verbindung beendet wird, bleiben die Hauptverbindung und die weiteren Child-Verbindungen bestehen.

---

**Hinweis**

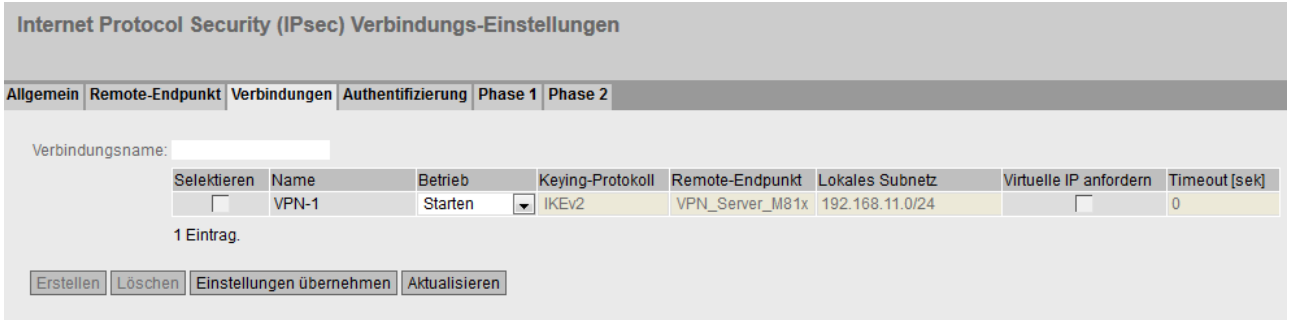
**IPsec: Einschränkungen für Phase 2-Verbindungen**

Legen Sie maximal 20 Phase 2-Verbindungen pro Phase 1 (Remote-Endpunkt) an.

**Hinweis**

Wenn Sie "NETMAP" verwenden,

- werden nur Auto-Firewall-Regeln unterstützt.
- ist bei "Betrieb" die Einstellung "Auf Anforderung" nicht auswählbar




## Beschreibung

Die Seite enthält folgende Felder:

- **Verbindungsname**
  Geben Sie einen Namen für die VPN-Verbindung ein und klicken Sie auf "Erstellen", um eine neue Verbindung zu erstellen.

Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Name**
  Zeigt den Namen der VPN-Verbindung an.

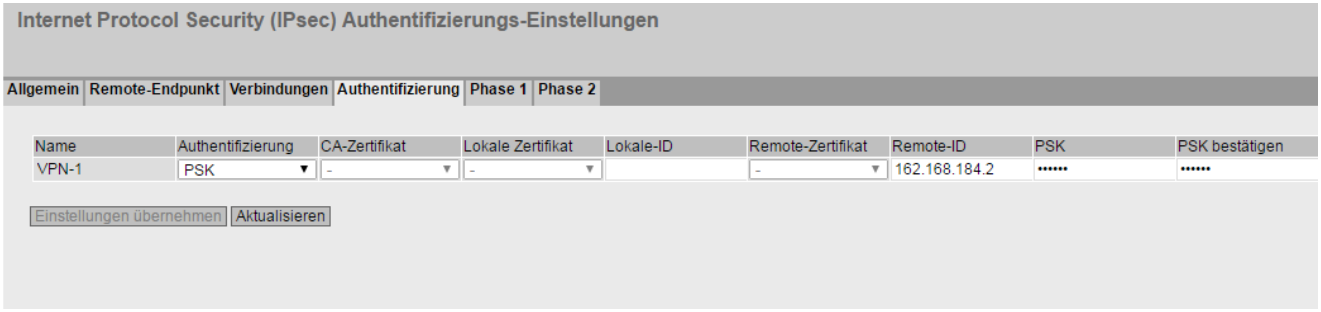
- **Betrieb**
  Legen Sie fest, von wem die VPN-Verbindung aufgebaut wird. Weitere Informationen dazu finden Sie unter "Technische Grundlagen > VPN-Verbindungsaufbau (Seite 91)".
  - Deaktiviert
    Die VPN-Verbindung ist deaktiviert.
  - Starten
    Das Gerät versucht, zu der Gegenstelle eine VPN-Verbindung aufzubauen.
  - Warten
    Das Gerät wartet, bis der Verbindungsaufbau von der Gegenstelle initiiert wird.
  - Auf Anforderung
    Die VPN-Verbindung wird bei Bedarf aufgebaut.
  - Bei DI starten
    Beim Eintreten des Ereignisses "Digitaler Eingang" versucht das Gerät zu der Gegenstelle eine VPN-Verbindung aufzubauen.
    Vorausgesetzt, dass das Ereignis "Digitaler Eingang" an die VPN-Verbindung weitergegeben wird. Dazu aktivieren Sie unter "System > Ereignisse > Konfiguration" beim Ereignis "Digitaler Eingang" "VPN-Tunnel".
  - Auf DI warten
    Beim Eintreten des Ereignisses "Digitaler Eingang" wartet das Gerät, bis der Verbindungsaufbau von der Gegenstelle initiiert wird.
    Vorausgesetzt, dass das Ereignis "Digitaler Eingang" an die VPN-Verbindung weitergegeben wird. Dazu aktivieren Sie unter "System > Ereignisse > Konfiguration" beim Ereignis "Digitaler Eingang" "VPN-Tunnel".
  - Bei SMS starten (nur beiM87x / MUM 856)
    Wenn das Gerät eine Befehl-SMS erhält, versucht das Gerät zu der Gegenstelle eine VPN-Verbindung aufzubauen. Vorausgesetzt, dass das Gerät eine Befehl-SMS der Klasse "System" von bestimmten Absendern akzeptiert. Die Absender konfigurieren Sie unter "System > SMS > Befehl-SMS".
  - Auf SMS warten (nur bei M87x / MUM 856)
    Wenn das Gerät eine Befehl-SMS erhält, wartet das Gerät, bis der Verbindungsaufbau von der Gegenstelle initiiert wird. Vorausgesetzt, dass das Gerät eine Befehl-SMS der Klasse "System" von bestimmten Absendern akzeptiert. Die Absender konfigurieren Sie unter "System > SMS > Befehl-SMS.
  - start on Action
    Wenn die Aktionen "VPN Reset" oder "VPN enable" ausgelöst werden, versucht das Gerät zu der Gegenstelle eine VPN-Verbindung aufzubauen. Dazu konfigurieren Sie unter "System > Connection Check" die entsprechende Aktion.
  - wait on Action
    Wenn die Aktionen "VPN Reset" oder "VPN enable" ausgelöst werden, wartet das Gerät, bis der Verbindungsaufbau von der Gegenstelle initiiert wird. Dazu konfigurieren Sie unter "System > Connection Check" die entsprechende Aktion.
  - start on TCP
    Wenn das ankommende TCP-Paket konforme Daten enthält, versucht das Gerät zu der Gegenstelle eine VPN-Verbindung aufzubauen. Vorausgesetzt unter "System > TCP-Ereignis" ist das Ereignis "VPN" aktiviert.

  - wait on TCP
    Wenn das ankommende TCP-Paket konforme Daten enthält, wartet das Gerät, bis der Verbindungsaufbau von der Gegenstelle initiiert wird. Vorausgesetzt unter "System > TCP-Ereignis" ist das Ereignis "VPN" aktiviert.
  - start on GPS (Nur bei MUM85x)
    Wenn die Aktion "OpenVPN (all) enable" ausgelöst wird, versucht das Gerät zu der Gegenstelle eine VPN-Verbindung aufzubauen. Dazu konfigurieren Sie unter "System > GPS > Geofencing" die entsprechende Aktion.
  - start on GPS (Nur bei MUM85x)
    Wenn die Aktion "OpenVPN (all) enable" ausgelöst wird, wartet das Gerät bis der Verbindungsaufbau von der Gegenstelle initiiert wird. Dazu konfigurieren Sie unter "System > GPS > Geofencing" die entsprechende Aktion.

- **Schnittstelle**
  Legen Sie fest, über welche Schnittstelle die VPN-Verbindung aufgebaut wird.
  - vlan1
    Für den Zugriff vom lokalen Netz (LAN) auf das Gerät
  - ppp0 bzw. usb0 (nur bei M87x und MUM85x):
    Zugriff von der Mobilfunk-Schnittstelle auf das Gerät.
- **Keying-Protokoll**
  Legen Sie fest, ob IKEv2 oder IKEv1 verwendet wird.
- **Remote-Endpunkt**
  Wählen Sie die gewünschte Gegenstelle aus. Nur die Gegenstellen sind projektierbar, die Sie auf der WBM-Seite "Remote-Endpunkt" konfiguriert haben.
- **Lokales Subnetz**
  Geben Sie das lokale Subnetz an. Verwenden Sie die CIDR-Schreibweise. Das lokale Netz kann auch nur ein einzelner PC oder eine andere Untermenge des lokalen Netzes sein.
  Nur mit IKEv2 können Sie mehrere Subnetze verwenden. Geben Sie dann die Subnetze durch ein Komma getrennt ein.
- **Virtuelle IP anfordern**
  Wenn aktiviert, wird beim Verbindungsaufbau eine virtuelle IP-Adresse von der Gegenstelle angefordert.
- **Timeout [min]**
  Geben Sie die Zeitspanne in Minuten an. Wenn kein Datenaustausch stattfindet, wird nach Ablauf dieser Zeitspanne der VPN-Tunnel automatisch abgebaut.

### 5.10.6.4 Authentifizierung

Auf dieser WBM-Seite legen Sie fest, wie sich die VPN-Verbindungspartner gegenseitig authentisieren.




## Beschreibung

Die Tabelle enthält folgende Spalten:

- **Name**
  Zeigt den Namen der VPN-Verbindung an, auf die sich die Einstellungen beziehen.
- **Authentifizierung**
  Wählen Sie das Authentifizierungsverfahren aus. Voraussetzung für die VPN-Verbindung ist, dass die Gegenstelle das gleiche Authentifizierungsverfahren verwendet.
  - Deaktiviert
    Es ist kein Authentifizierungsverfahren gewählt. Ein Verbindungsaufbau ist nicht möglich.
  - Remote-Zert
    Für die Authentifizierung wird das Gegenstellenzertifikat verwendet. Das Zertifikat legen Sie bei "Remote-Zertifikat" fest
  - CA-Zert
    Für die Authentifizierung wird das Zertifikat der Zertifizierungsstelle verwendet. Das Zertifikat legen Sie bei "CA-Zertifikat" fest.
  - PSK
    Für die Authentifizierung wird ein Schlüssel verwendet. Den Schlüssel konfigurieren Sie bei "PSK".

    **Hinweis**

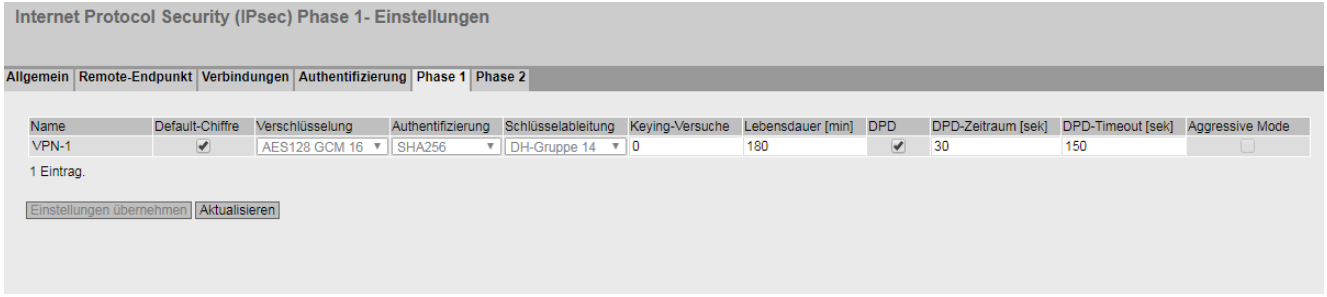
    Geben Sie bei der Authentifizierungsmethode "PSK" die "Lokale-ID" und die "Remote-ID" an. Wenn die Einträge leer bleiben, verwendet IPSec als ID die IP-Adresse der Schnittstelle und der Aufbau des VPN-Tunnels wird verhindert.
- **CA-Zertifikat**
  Wählen Sie das Zertifikat aus. Nur geladene Zertifikate sind auswählbar.
- **Lokales Zertifikat**
  Wählen Sie das Gerätezertifikat aus.
  Die Zertifikate laden Sie über "System > Laden & Speichern" in das Gerät. Auf der WBM-Seite "Security > Zertifikate" werden die geladenen Zertifikate und Schlüsseldateien angezeigt.

- **Lokale-ID**
  Geben Sie die Lokale-ID aus dem Gegenstellenzertifikat ein. Nur wenn Sie das Gegenstellenzertifikat verwenden, können Sie das Feld leer lassen. Das Feld wird automatisch mit dem Wert aus dem Gegenstellenzertifikat befüllt.
- **Remote-Zertifikat**
  Wählen Sie das Gegenstellenzertifikat aus. Nur geladene Gegenstellenzertifikate sind auswählbar.
  Die Zertifikate laden Sie über "System > Laden & Speichern" in das Gerät. Auf der WBM-Seite "Security > Zertifikate" werden die geladenen Zertifikate und Schlüsseldateien angezeigt.
- **Remote-ID**
  Geben Sie den "Distinguished Name" oder "Alternate Name" aus dem Gegenstellenzertifikat ein. Nur wenn Sie das Gegenstellenzertifikat verwenden, können Sie das Feld leer lassen. Das Feld wird automatisch mit dem Wert aus dem Gegenstellenzertifikat befüllt.
- **PSK**
  Geben Sie den Schlüssel ein.
- **PSK bestätigen**
  Wiederholen Sie den Schlüssel.

### 5.10.6.5 Phase 1

**Phase 1: Verschlüsselungsvereinbarung und Authentifizierung (IKE = Internet Key Exchange)**

Auf dieser WBM-Seite stellen Sie die Parameter für das Protokoll des IPsec-Schlüsselmanagements ein. Der Schlüsselaustausch erfolgt über das standardisierte Verfahren IKE, für das Sie folgende Protokollparameter einstellen können.



## Beschreibung

Die Tabelle enthält folgende Spalten:

- **Name**
  Zeigt den Namen der VPN-Verbindung an, auf die sich die Einstellungen beziehen.
- **Default-Chiffre**
  Wenn aktiviert, wird beim Verbindungsaufbau eine vorgegebene Liste an den VPN-Verbindungspartner übermittelt. In der Liste sind Kombinationen aus den drei Algorithmen (Encryption, Authentication, Key Derivation) enthalten. Um eine VPN-Verbindung aufzubauen, muss der VPN-Verbindungspartner mindestens eine dieser Kombinationen unterstützen. Die Auswahl ist abhängig vom Schlüsselaustauschverfahren. Weitere Informationen dazu erhalten Sie bei "IPsec VPN (Seite 87)".
- **Verschlüsselung**
  Wählen Sie für die Phase 1 den gewünschten Verschlüsselungsalgorithmus aus. Nur auswählbar, wenn "Default-Chiffre" deaktiviert ist.
  Die Auswahl ist abhängig vom Schlüsselaustauschverfahren. Weitere Informationen dazu erhalten Sie bei "IPsec VPN (Seite 87)".

  **Hinweis**

  Die AES-Modi CCM und GCM beinhalten separate Mechanismen für die Authentisierung von Daten. Wenn Sie bei "Verschlüsselung" einen Modus AES x CCM verwenden, dann wird dieser auch zur Authentifizierung verwendet. Von dem Parameter "Authentifizierung" wird dann nur noch die Pseudo-Random-Funktion abgeleitet. Damit eine VPN-Verbindung aufgebaut wird, müssen alle Geräte die gleichen Einstellungen verwenden.

- **Authentifizierung**
  Legen Sie das Verfahren zum Berechnen der Prüfsumme fest. Nur auswählbar, wenn "Default-Chiffre" deaktiviert ist.
  Folgende Verfahren werden unterstützt:
  - MD5
  - SHA1
  - SHA512
  - SHA256
  - SHA384

- **Schlüsselableitung**
  Wählen Sie die gewünschte Diffie-Hellmann-Gruppe (DH), aus der ein Schlüssel erzeugt wird. Nur auswählbar, wenn "Default-Chiffre" deaktiviert ist.
  Folgende DH-Gruppen werden unterstützt:
  - 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-Versuche**
  Tragen Sie die Anzahl der Wiederholungen für einen fehlgeschlagenen Verbindungsaufbau ein. Wenn Sie den Wert 0 eintragen, wird der Verbindungsaufbau unendlich oft zu versucht.
- **Lebensdauer [min]**
  Tragen Sie einen Zeitraum in Minuten ein, der die Lebensdauer der Authentisierung festlegt. Nach Ablauf der Zeit müssen sich die beteiligten VPN-Endpunkte erneut gegenseitig Authentisieren und einen neuen Schlüssel erzeugen
- **DPD**
  Wenn aktiviert, wird DPD (Dead Peer Detection) verwendet. Mit DPD lässt sich feststellen, ob die VPN-Verbindung noch besteht oder ob sie abgebrochen ist.

  **Hinweis**

  Durch das Versenden der DPD-Anfragen steigt die Anzahl der gesendeten und empfangenen Daten. Dies kann zu erhöhten Kosten führen.

- **DPD-Zeitraum [sek]**
  Tragen Sie eine Zeitspanne ein, nach der DPD-Anfragen gesendet werden. Diese Anfragen testen, ob die Gegenstelle noch verfügbar ist

- **DPD-Timeout [sek]**
  Nur bei IKEv1 einstellbar. Für IKEv2 konfigurieren Sie die Einstellung unter "Security > IPsec > Allgemein".
  Tragen Sie eine Zeitspanne ein. Wenn auf die DPD-Anfragen keine Antwort erfolgt, dann wird nach Ablauf dieser Zeit die Verbindung zur Gegenstelle für ungültig erklärt.

  **Hinweis**

  Um ungewollte Verbindungsabbrüche zu vermeiden, stellen Sie den DPD-Timeout wesentlich höher als den DPD-Zeitraum ein. Wir empfehlen mindestens 2 Minuten länger als der DPD-Zeitraum.

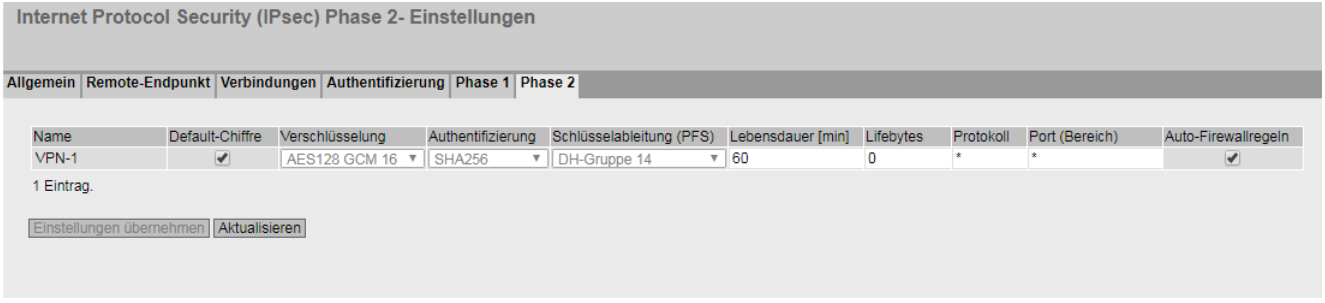
- **Aggressive Mode**
  - Deaktiviert:
    Main Mode wird verwendet.
  - Aktiviert
    Aggressive Mode wird verwendet

  Der Unterschied zwischen Main- und Aggressive Mode ist die "Identity-Protection", die im Main Mode verwendet wird. Die Identität wird im Main Mode verschlüsselt übertragen, im Aggressive Mode nicht.

### 5.10.6.6 Phase 2

**Phase 2: Datenaustausch (ESP = Encapsulating Security Payload)**

Auf dieser WBM-Seite stellen Sie die Parameter für das Protokoll des IPsec-Datenaustauschs ein. Die gesamte Kommunikation in dieser Phase erfolgt verschlüsselt über das standardisierte Sicherheitsprotokoll ESP, für das Sie folgende Protokollparameter einstellen können.



## Beschreibung

Die Tabelle enthält folgende Spalten:

- **Name**
  Zeigt den Namen der VPN-Verbindung an, auf die sich die Einstellungen beziehen.
- **Default-Chiffre**
  Wenn aktiviert, wird beim Verbindungsaufbau eine vorgegebene Liste an den VPN-Verbindungspartner übermittelt. In der Liste sind Kombinationen aus den drei Algorithmen (Verschlüsselung, Authentifizierung, Schlüsselableitung) enthalten. Um eine VPN-Verbindung aufzubauen, muss der VPN-Verbindungspartner mindestens eine dieser Kombinationen unterstützen. Weitere Informationen dazu erhalten Sie bei "IPsec VPN (Seite 87)".
- **Verschlüsselung**
  Wählen Sie für die Phase 2 den gewünschten Verschlüsselungsalgorithmus aus. Nur auswählbar, wenn "Default-Chiffre" deaktiviert ist.
  Weitere Informationen dazu erhalten Sie bei "IPsec VPN (Seite 87)".

  **Hinweis**

  Die AES-Modi CCM und GCM beinhalten separate Mechanismen für die Authentifizierung von Daten. Wenn Sie bei "Verschlüsselung" einen Modus AES x CCM oder AES x GCM verwenden, dann wird dieser auch zur Authentifizierung verwendet. Von dem Parameter "Authentifizierung" wird dann nur noch die Pseudo-Random-Funktion abgeleitet.

- **Authentifizierung**
  Legen Sie das Verfahren zum Berechnen der Prüfsumme fest. Nur auswählbar, wenn "Default-Chiffre" deaktiviert ist.
  Folgende Verfahren werden unterstützt:
  - MD5
  - SHA1
  - SHA512
  - SHA256
  - SHA384

- **Schlüsselableitung (PFS)**
  Das Gerät unterstützt den Deffie-Hellmann-Schlüsselaustausch (DH) mit der Eigenschaft Perfect Forward Secrecy (PFS).
  Wählen Sie die gewünschte DH-Gruppe, aus der ein Schlüssel erzeugt wird. Nur auswählbar, wenn "Default-Chiffre" deaktiviert ist.
  Folgende DH-Gruppen werden unterstützt:
  - None: Für die Phase 2 werden keine separaten Schlüssel ausgetauscht. Damit ist PFS deaktiviert.
  - DH Group 1
  - DH Group 2
  - DH Group 5
  - DH Group 14
  - DH Group 15
  - DH Group 16
  - DH Group 17
  - DH Group 18

  **Hinweis**

  Damit eine VPN-Verbindung aufgebaut wird, müssen alle Geräte die gleichen Einstellungen verwenden oder kompatible Verschlüsselungsverfahren anbieten.

- **Lebensdauer [min]**
  Tragen Sie einen Zeitraum in Minuten ein, der die Lebensdauer der vereinbarten Schlüssel festlegt. Nach Ablauf der Zeit wird der Schlüssel neu ausgehandelt.
- **Lifebyte**s
  Tragen Sie das Datenlimit in Bytes ein, das die Lebensdauer der vereinbarten Schlüssel festlegt. Nach Ablauf des Datenlimits wird der Schlüssel neu ausgehandelt.
- **Protokoll**
  Legen Sie fest, für welches Protokoll die VPN-Verbindung gültig ist, z. B. UDP, TCP, ICMP. Wenn die Einstellung für alle Protokolle gelten soll, geben Sie "*" ein.

- **Port (Bereich)**
  Legen Sie den Port fest, durch den der VPN-Tunnel kommunizieren kann. Die Einstellung gilt genau für den angegebenen Port
  - Wenn die Einstellung für einen Port-Bereich gelten soll, geben Sie den Bereich mit Start-Port "-" End-Port an, z. B. 30 - 40.
  - Wenn die Einstellung für alle Ports gelten soll, geben Sie "*" ein.

  Die Einstellung hat nur bei portbasierten Protokollen Auswirkungen.
- **Auto-Firewallregeln**
  - Aktiviert
    Für die VPN-Verbindung werden automatisch die Firewall-Regeln für den Zugriff von "extern" nach "intern" und umgekehrt angelegt. Unter "Security > Firewall > vordefinierte IPv4-Regeln" können Sie den Zugriff auf bestimmte Dienste des Geräts erlauben. Standardmäßig ist Ping freigeschaltet.
  - Deaktiviert
    Sie müssen selbst die Firewall-Regeln anlegen.

## 5.10.7 OpenVPN Client

### 5.10.7.1 Allgemein

Auf dieser WBM-Seite aktivieren Sie den OpenVPN-Client.



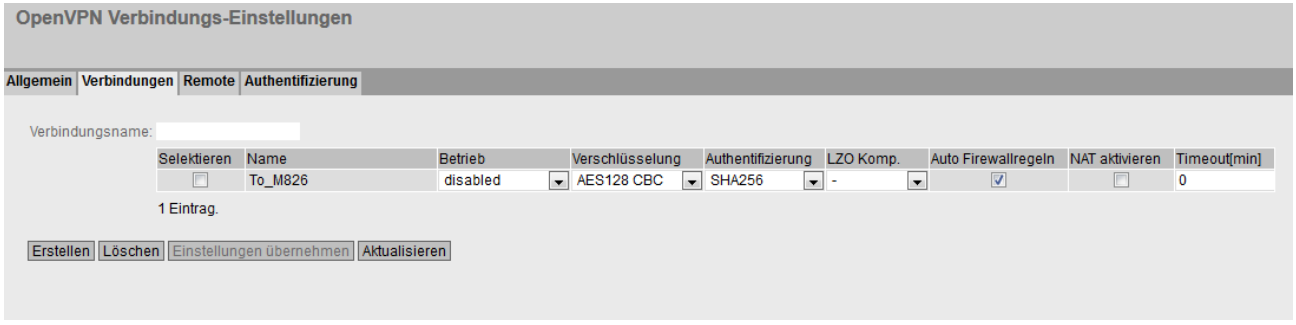

### Beschreibung

Die Seite enthält Folgendes:

- **OpenVPN-Client aktivieren**
  Aktivieren oder deaktivieren Sie den OpenVPN-Client.

### 5.10.7.2 Verbindungen

Auf dieser WBM-Seite konfigurieren Sie die Grundeinstellungen für die OpenVPN-Verbindung. Die Sicherheitseinstellungen legen Sie auf der WBM-Seite "Authentifizierung" fest.




## Beschreibung

- **Verbindungsname**
  Geben Sie einen eindeutigen Namen für die OpenVPN-Verbindung ein und klicken Sie auf "Erstellen", um eine neue Verbindung zu erstellen.

Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Name**
  Zeigt den Namen der OpenVPN-Verbindung an.

- **Betrieb**
  Legen Sie fest, wie die Verbindung aufgebaut wird. Weitere Informationen dazu finden Sie unter "Technische Grundlagen > VPN-Verbindungsaufbau (Seite 91)".
  - Starten
    Das Gerät versucht, zu der Gegenstelle eine VPN-Verbindung aufzubauen.
  - Bei DI starten
    Beim Eintreten des Ereignisses "Digitaler Eingang" versucht das Gerät zu der Gegenstelle eine VPN-Verbindung aufzubauen.
    Vorausgesetzt, dass das Ereignis "Digitaler Eingang" an die VPN-Verbindung weitergegeben wird. Dazu aktivieren Sie unter "System > Ereignisse > Konfiguration" beim Ereignis "Digitaler Eingang" "VPN-Tunnel".
  - Bei SMS starten (nur bei M87x / MUM85x)
    Wenn das Gerät eine Befehl-SMS erhält, versucht das Gerät zu der Gegenstelle eine VPN-Verbindung aufzubauen. Vorausgesetzt, dass das Gerät eine Befehl-SMS der Klasse "System" von bestimmten Absendern akzeptiert. Die Absender konfigurieren Sie unter "System > SMS > Befehl-SMS".
  - start on Action
    Wenn die Aktionen "VPN Reset" oder "VPN enable" ausgelöst werden, versucht das Gerät zu der Gegenstelle eine VPN-Verbindung aufzubauen. Dazu konfigurieren Sie unter "System > Connection Check" die entsprechende Aktion.
  - start on TCP
    Wenn das ankommende TCP-Paket konforme Daten enthält, versucht das Gerät zu der Gegenstelle eine VPN-Verbindung aufzubauen. Vorausgesetzt unter "System > TCP-Ereignis" ist das Ereignis "VPN" aktiviert.
  - start on GPS (Nur bei MUM85x)
    Wenn die Aktion "OpenVPN (all) enable" ausgelöst wird, versucht das Gerät zu der Gegenstelle eine VPN-Verbindung aufzubauen. Dazu konfigurieren Sie unter "System > GPS > Geofencing" die entsprechende Aktion.
  - Deaktiviert
    Die VPN-Verbindung ist deaktiviert.
- **Verschlüsselung**
  Wählen Sie den gewünschten Verschlüsselungsalgorithmus aus.
  - AES-128-CBC (Default)
  - AES-192-CBC
  - AES-256-CBC
  - DES-EDE3
  - BF-CBC

- **Authentifizierung**
  Legen Sie das Verfahren zum Berechnen der Prüfsumme fest.
  - SHA256 (Default)
  - SHA384
  - SHA512
  - SHA224
  - SHA1
  - MD5
- **LZO verwenden**
  Wenn aktiviert, werden die Daten mit dem LZO-Algorithmus komprimiert.
- **Auto-Firewallregeln**
  - Aktiviert
    Für die VPN-Verbindung werden automatisch die Firewall-Regeln für den Zugriff von "extern" nach "intern" und umgekehrt angelegt. Zusätzlich wird der Zugriff vom Gerät nach extern erlaubt. Unter "Security > Firewall > vordefinierte IPv4-Regeln" können Sie den Zugriff auf bestimmte Dienste des Geräts erlauben. Standardmäßig ist Ping freigeschaltet.
  - Deaktiviert
    Sie müssen selbst die geeigneten Firewall-Regeln anlegen.
- **NAT aktivieren**
  Mit dieser Einstellung aktivieren Sie automatisches IP-Masquerading für diese Schnittstelle. Die lokalen Geräte sind von außen nicht direkt erreichbar, sondern nur über die IP-Adresse der Schnittstelle. Die lokalen Geräte können sich aber mit den Geräten hinter dem OpenVPN-Server verbinden. Weitere Informationen zu NAT finden Sie unter "Technische Grundlagen > NAT (Seite 82)".
- **Timeout [min]**
  Geben Sie die Zeitspanne in Minuten an. Wenn kein Datenaustausch stattfindet, wird nach Ablauf dieser Zeitspanne der VPN-Tunnel automatisch abgebaut.

### 5.10.7.3 Remote

Auf dieser WBM-Seite konfigurieren Sie die Gegenstelle (OpenVPN-Endpunkt). Pro Verbindung können Sie mehrere OpenVPN-Gegenstellen festlegen. Das Gerät probiert alle projektierten OpenVPN-Gegenstellen der Reihe nach aus bis ein Verbindungsaufbau erfolgreich ist.




## Beschreibung

Die Seite enthält Folgendes:

- **Remote-Name**
  Geben Sie einen Namen für die OpenVPN-Gegenstelle ein und klicken Sie auf "Erstellen", um eine neue Gegenstelle zu erstellen.

Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Name**
  Zeigt den Namen der OpenVPN-Gegenstelle an.
- **Verbindung**
  Wählen Sie die zugehörige Verbindung aus. Nur die Verbindungen sind projektierbar, die Sie auf der WBM-Seite "Verbindungen" konfiguriert haben.
- **Remote-Adresse**
  Geben Sie die WAN-IP-Adresse oder den DNS-Hostnamen der OpenVPN-Gegenstelle ein.
- **Port**
  Legen Sie den Port fest, durch den der OpenVPN-Tunnel kommunizieren kann. Die Einstellung gilt genau für den angegebenen Port.
- **Protokoll**
  Legen Sie fest, für welches Protokoll die OpenVPN-Verbindung genutzt werden soll.
- **Proxy**
  Legen Sie fest, ob der OpenVPN-Tunnel zu der definierten OpenVPN-Gegenstelle über einen Proxy-Server aufgebaut wird. Es sind nur die Proxy-Server auswählbar, die Sie unter "System > Proxy-Server" konfiguriert haben.

### 5.10.7.4 Authentifizierung

Auf dieser WBM-Seite legen Sie fest, wie sich die VPN-Verbindungspartner gegenseitig authentisieren.




## Beschreibung

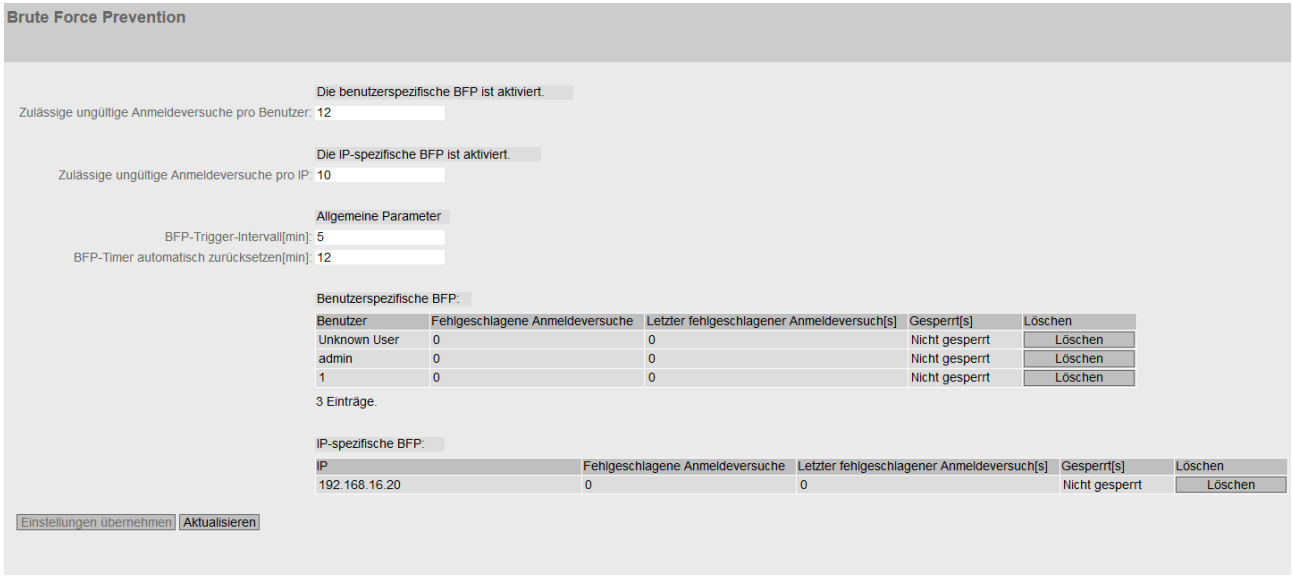
Die Tabelle enthält folgende Spalten:

- **Name**
  Zeigt den Namen der VPN-Verbindung an, auf die sich die Einstellungen beziehen.
- **TLS-Auth. Key**
  Wählen Sie die Schlüsseldatei, mit dem die TLS-Pakete signiert werden. Wenn die eingehenden TLS-Pakete nicht mit diesem Schlüssel signiert sind, werden diese verworfen.
- Richtung
  Legen Sie die Richtung fest. Wenn Sie 0 wählen, muss auf der Gegenstelle 1 eingestellt sein und umgekehrt. Mit dieser Einstellung schränken Sie die Clients ein, die sich authentifizieren dürfen.
  Verwenden Sie "none", wenn beim OpenVPN-Server nichts eingestellt ist. Bei "none" ist diese Einstellung deaktiviert.
- **Methode**
  Wählen Sie das Authentifizierungsverfahren aus. Voraussetzung für die VPN-Verbindung ist, dass die Gegenstelle das gleiche Authentifizierungsverfahren verwendet.
  - Deaktiviert
    Es ist kein Authentifizierungsverfahren gewählt. Ein Verbindungsaufbau ist nicht möglich.
  - Zertifikate
    Für die Authentifizierung werden Zertifikate verwendet.
  - Benutzername/Passwort
    Für die Authentifizierung werden Benutzername/Passwort verwendet.
  - Zert/Benutzername/Passwort
    Für die Authentifizierung sind zusätzlich zum Zertifikat noch ein Benutzername und ein Passwort notwendig. Nur wenn beide Verfahren erfolgreich sind, wird die VPN-Verbindung aufgebaut.
- **CA-Zertifikat**
  Wählen Sie das Zertifikat aus. Nur geladene Zertifikate sind auswählbar.
  Die Zertifikate laden Sie über "System > Laden & Speichern" in das Gerät. Auf der WBM-Seite "Security > Zertifikate" werden die geladenen Zertifikate und Schlüsseldateien angezeigt.

- **Gerätezertifikat**
  Wählen Sie das Gerätezertifikat aus. Nur geladene Zertifikate sind auswählbar.
  Die Zertifikate laden Sie über "System > Laden & Speichern" in das Gerät. Auf der WBM-Seite "Security > Zertifikate" werden die geladenen Zertifikate und Schlüsseldateien angezeigt.
- **Benutzername**
  Geben Sie den Benutzernamen an.
- **Passwort**
  Geben Sie das Passwort an.
- **Passwort bestätigen**
  Widerholen Sie das Passwort.

## 5.10.8 Brute Force Prevention

Unter Brute Force Prevention (BFP) versteht man den Schutz des Geräts gegen unberechtigten Zugriff durch das Ausprobieren einer hinreichend großen Anzahl von Passwörtern. Dazu wird die Anzahl der unzulässigen Anmeldeversuche innerhalb eines bestimmten Zeitraums beschränkt.



## Beschreibung

Die Seite enthält folgende Felder:

- **Die benutzerspezifische BFP ist aktiviert. / Die benutzerspezifische BFP ist deaktiviert.**
  - Aktiviert:
    Bei der Login-Authentifizierung ist das Verfahren "Lokal" oder "Lokal und RADIUS" eingestellt und die maximale Anzahl ungültiger Anmeldeversuche ist größer 0.
  - Deaktiviert:
    Bei der Login-Authentifizierung ist bei den Verfahren "RADIUS" oder "RADIUS und Fallback Lokal" eingestellt oder die maximale Anzahl ungültiger Anmeldeversuche ist gleich 0.

  Die Login-Authentifizierung konfigurieren Sie unter "Security > AAA > Allgemein > Login-Authentifizierung".
- **Zulässige ungültige Anmeldeversuche pro Benutzer**
  Die maximale Anzahl ungültiger Anmeldeversuche für einen Benutzer, die das Gerät akzeptiert. Weitere Anmeldeversuche für diesen Benutzer werden für eine bestimmte Zeit blockiert.
  Die Benutzer, die nicht als lokale Benutzer für das Gerät konfiguriert sind, werden unter dem Benutzernamen "UnknownUser" zusammengefasst.
  0: Die benutzerspezifische BFP ist deaktiviert.
- **Die IP-spezifische BFP ist aktiviert. / Die IP-spezifische BFP ist deaktiviert**
  Zeigt an, ob die IP-spezifische Brute Force Prevention aktiviert ist.
- **Zulässige ungültige Anmeldeversuche pro IP-Adresse**
  Die maximale Anzahl ungültiger Anmeldeversuche für eine IP-Adresse, die das Gerät akzeptiert. Weitere Anmeldeversuche für diese IP-Adresse werden für eine bestimmte Zeit blockiert.
  0: Die IP-spezifische BFP ist deaktiviert.
- **BFP-Trigger-Intervall[min]**
  Die Zeit in Minuten, die für das Zählen der unzulässigen Login-Versuche relevant ist. Wenn in dieser Zeit die maximale Anzahl der ungültigen Anmeldeversuche überschritten wird, blockiert das Gerät für einen bestimmten Zeitraum die Anmeldung.
  Unzulässige Login-Versuche pro Benutzer und pro IP-Adresse werden dabei unabhängig voneinander behandelt.
- **BFP-Timer automatisch zurücksetzen[min]**
  Die Zeit in Minuten, in der das Gerät die Anmeldung blockiert, weil die maximale Anzahl der ungültigen Anmeldeversuche überschritten wurde.
  0: Der Timer ist deaktiviert.

Die Tabelle **Benutzerspezifische BFP** gliedert sich in folgende Spalten:

- **Benutzer**
  Die Benutzer, die lokal auf dem Gerät konfiguriert sind. Die Benutzer, die nicht lokal auf dem Gerät konfiguriert sind, werden unter dem Benutzernamen "UnknownUser" zusammengefasst.
- **Fehlgeschlagene Anmeldeversuche**
  Die Anzahl der fehlgeschlagenen Anmeldeversuche.
- **Letzter fehlgeschlagener Anmeldeversuch [s]**
  Die Zeit in Sekunden (s) seit dem letzten fehlgeschlagenen Anmeldeversuch. Um den aktuellen Wert anzuzeigen, klicken Sie auf die Schaltfläche "Aktualisieren".

- **Gesperrt [s]**
  Die Zeit in Sekunden (s), bis die Blockierung aufgehoben wird. Um den aktuellen Wert anzuzeigen, klicken Sie auf die Schaltfläche "Aktualisieren".
  Wenn ein blockierter Benutzer versucht, sich vor Ablauf des Timers anzumelden, startet der Timer neu.
- **Löschen**
  Beendet die Blockierung für den Benutzer und setzt die Anzeigen in den Feldern "Letzter fehlgeschlagener Anmeldeversuch [s]" und "Gesperrt [s]" zurück.

Die Tabelle **IP-spezifische BFP** gliedert sich in folgende Spalten:

- **IP**
  Die IP-Adresse des Geräts für den Login-Versuch.
- **Fehlgeschlagene Anmeldeversuche**
  Die aktuelle Anzahl fehlgeschlagener Anmeldeversuche.
- **Letzter fehlgeschlagener Anmeldeversuch [s]**
  Die Zeit in Sekunden (s) seit dem letzten fehlgeschlagenen Anmeldeversuch. Um den aktuellen Wert anzuzeigen, klicken Sie auf die Schaltfläche "Aktualisieren".
- **Gesperrt [s]**
  Die Zeit in Sekunden (s), bis die Blockierung aufgehoben wird. Um den aktuellen Wert anzuzeigen, klicken Sie auf die Schaltfläche "Aktualisieren".
  Wenn eine blockierte IP-Adresse versucht, sich vor Ablauf des Timers anzumelden, startet der Timer neu.
- **Löschen**
  Beendet die Blockierung für die IP-Adresse und setzt die Anzeigen in den Feldern "Letzter fehlgeschlagener Anmeldeversuch [s]" und "Gesperrt [s]" zurück.

# Instandhalten und Warten 6

## 6.1 Firmware

### Firmware

Die Firmware ist signiert und verschlüsselt. Es ist sichergestellt, dass nur von Siemens erstellte Firmware in das Gerät geladen werden kann.

## 6.2 Gerätekonfiguration mit PRESET-PLUG

Bitte beachten Sie die ergänzenden Informationen und Sicherheitshinweise in der Betriebsanleitung ihres Geräts.

| **ACHTUNG** |
| --- |
| **PLUG nicht im laufenden Betrieb ziehen oder stecken!**<br>Ein PLUG darf nur bei ausgeschaltetem Gerät entnommen oder eingesetzt werden. |

**Hinweis**

**Unterstützung ab V4.3**

Die PRESET-PLUG Funktionalität wird ab der Firmwareversion V4.3 unterstützt.

Mit dem PRESET-PLUG können Sie dieselbe Gerätekonfiguration (Startkonfiguration, Benutzeraccounts, Zertifikate) inklusive der dazugehörigen Firmware auf mehreren Geräten installieren.

Der PRESET-PLUG ist schreibgeschützt.

Sie konfigurieren den PRESET-PLUG mit Hilfe des Command Line Interface (CLI).

### PRESET-PLUG erstellen

Erstellen Sie den PRESET-PLUG mit Hilfe des Command Line Interface (CLI). Sie können einen PRESET-PLUG aus jedem PLUG erstellen. Gehen Sie hierzu vor wie folgt:

**Hinweis**

**Konfigurationen mit DHCP verwenden**

Erstellen Sie einen PRESET-PLUG nur aus Gerätekonfigurationen, die DHCP verwenden. Es treten sonst Störungen im Netzwerkbetrieb durch mehrfache gleiche IP-Adressen auf.

Feste IP-Adressen weisen Sie nach der Grundinstallation gesondert zu.

**Voraussetzung**

- Im Gerät ist ein PLUG gesteckt, auf dem Sie die Funktionalität PRESET-PLUG konfigurieren wollen.

**Vorgehen**

1. Starten sie die Remote-Konfiguration über CLI und melden sich mit einem Benutzer an, der die Rolle "admin" besitzt.
   Die CLI-Verbindung geht entweder mit Telnet (Port 23) oder SSH (Port 22).
2. Wechseln Sie in den globalen Konfigurationsmodus mit dem Befehl "configure terminal".
3. Gehen Sie in den PLUG-Konfigurationsmodus mit dem Befehl "plug".
4. Erstellen Sie den PRESET-PLUG mit dem Befehl "presetplug".
   Die Firmwareversion des Geräts, sowie die aktuelle Gerätekonfiguration inkl. Benutzeraccounts und Zertifikate, werden auf dem PLUG gespeichert und der PLUG wird anschließend schreibgeschützt.
5. Schalten Sie das Gerät spannungslos.
6. Entnehmen sie den PRESET-PLUG.
7. Starten Sie das Gerät wahlweise mit einem gesteckten neuen PLUG oder mit der internen Konfiguration.

## Vorgehen zur Installation mit Hilfe des PRESET-PLUG

1. Schalten Sie das Gerät spannungslos.
2. Falls vorhanden, entnehmen Sie den PLUG aus dem Steckplatz. Weitere Informationen dazu finden Sie in der Betriebsanleitung ihres Geräts.
3. Setzen Sie den PRESET-PLUG in der richtigen Orientierung in den Steckplatz. Der PRESET-PLUG ist richtig eingesetzt, wenn er sich vollständig im Gerät befindet und nicht aus dem Steckplatz herausragt.
4. Schalten Sie das Gerät wieder ein.
   Wenn auf dem zu installierenden Gerät eine andere Firmwareversion als die auf dem PRESET-PLUG gespeicherte vorhanden ist, wird ein Up-/Downgrade der Firmware durchgeführt. Sie erkennen dies am Blinken der roten F-LED (Blinkintervall: 2Sek an/0.2Sek. aus). Danach wird das Gerät neu gestartet und die auf dem PRESET-PLUG gespeicherte Gerätekonfiguration, inkl. Benutzer und Zertifikate, auf das Gerät überspielt.
5. Warten Sie, bis das Gerät vollständig hochgefahren ist.
   (die rote F-LED ist aus)
6. Schalten Sie das Gerät nach der Installation ab.

7. Entnehmen Sie den PRESET-PLUG.
8. Starten Sie das Gerät wahlweise mit einem gesteckten neuen PLUG oder mit der internen Konfiguration.

**Hinweis**

**KEY-PLUG**

Wenn Sie den PRESET-PLUG aus einem KEY-PLUG erstellt haben benötigen Sie zum Betrieb mit dieser Konfiguration einen gesteckten KEY-PLUG mit Werkseinstellungen.

In diesem Fall müssen Sie vor der Wiederinbetriebnahme des Geräts den entsprechenden KEY-PLUG einsetzen.

**Hinweis**

**Auf Werkseinstellungen zurücksetzen und Neustart mit gestecktem PRESET-PLUG**

Wenn Sie das Gerät auf Werkseinstellungen zurücksetzen wird beim Neustart des Geräts ein gesteckter PRESET-PLUG formatiert und die Funktionalität PRESET-PLUG geht verloren. Sie müssen dann einen neuen PRESET-PLUG erstellen. Die auf einem KEY-PLUG gespeicherten Schlüssel zur Freischaltung von Funktionen bleiben erhalten.

Wir empfehlen, den PRESET-PLUG zu entnehmen, bevor Sie das Gerät auf Werkseinstellungen zurücksetzen.

### PRESET-PLUG formatieren (Preset-Funktion zurücksetzen)

Formatieren Sie den PRESET-PLUG mit Hilfe des Command Line Interface (CLI), um die Preset-Funktion zurückzusetzen. Gehen Sie hierzu vor wie folgt:

1. Starten sie die Remote-Konfiguration über Telnet (CLI) und melden sich mit einem Benutzer aln, der die Rolle "admin" besitzt.
2. Wechseln Sie in den globalen Konfigurationsmodus mit dem Befehl "configure terminal".
3. Gehen Sie in den PLUG-Konfigurationsmodus  mit dem Befehl "plug".
4. Geben Sie den Befehl "factoryclean" ein.
   Der PRESET-PLUG wird formatiert und die Preset-Funktion wird zurückgesetzt.
5. Schreiben Sie die aktuelle Konfiguration des Geräts auf den PLUG mit dem Befehl "write".

## 6.3 Firmware-Update über WBM

### Voraussetzung

- Das Gerät hat eine IP-Adresse.
- Der Benutzer ist mit Administratorrechten angemeldet.

### Firmware-Update über HTTP

1. Klicken Sie im Navigationsbereich auf "System > Laden & Speichern". Klicken Sie auf das Register "HTTP".
2. Klicken Sie bei "Firmware" auf die Schaltfläche "Laden".
3. Navigieren Sie zum Ablageort der Firmware-Datei.
4. Klicken Sie im Dialogfenster auf die Schaltfläche "Öffnen".

### Firmware-Update über TFTP

1. Klicken Sie im Navigationsbereich auf "System > Laden & Speichern". Klicken Sie auf das Register "TFTP".
2. Tragen Sie im Eingabefeld "Adresse des TFTP-Servers" die IP-Adresse des TFTP-Servers ein.
3. Tragen Sie im Eingabefeld "Port des TFTP-Servers" den Port des TFTP-Servers ein.
4. Klicken Sie in der Tabellenzeile "Firmware" auf die Schaltfläche "Datei hochladen".
5. Navigieren Sie zum Ablageort der Firmware-Datei.
6. Klicken Sie im Dialogfenster auf die Schaltfläche "Öffnen". Die Datei wird hochgeladen.

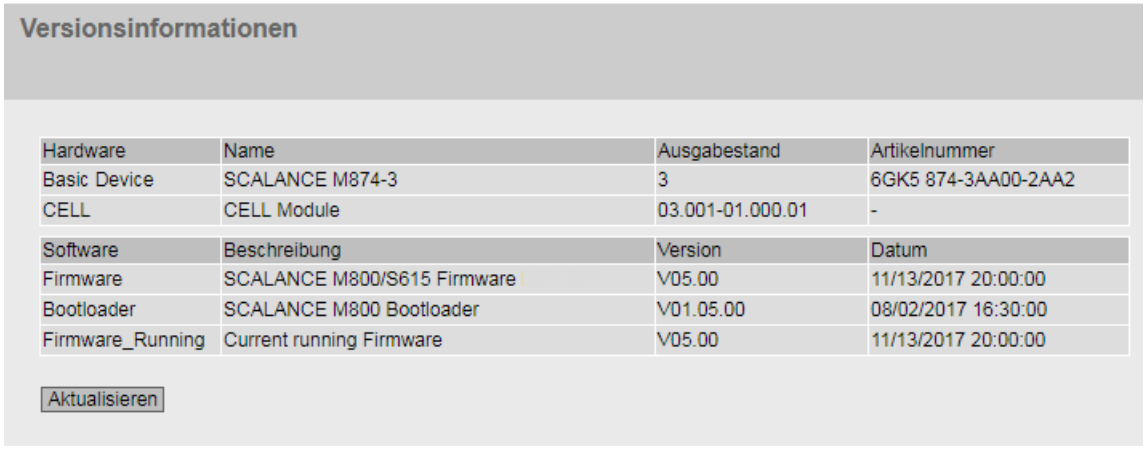
### Firmware-Update über SFTP

1. Klicken Sie im Navigationsbereich auf "System > Laden & Speichern". Klicken Sie auf das Register "SFTP".
2. Tragen Sie im Eingabefeld "Adresse des SFTP-Servers" die IP-Adresse des SFTP-Servers ein.
3. Tragen Sie im Eingabefeld "Port des SFTP-Servers" den Port des SFTP-Servers ein.
4. Tragen Sie den Benutzer und das Passwort für den Zugriff auf den SFTP-Server ein.
5. Klicken Sie in der Tabellenzeile "Firmware" auf die Schaltfläche "Datei hochladen".
6. Navigieren Sie zum Ablageort der Firmware-Datei.
7. Klicken Sie im Dialogfenster auf die Schaltfläche "Öffnen". Die Datei wird hochgeladen.

### Ergebnis

Wenn die Firmware erfolgreich geladen ist, wird ein Dialog angezeigt. Bestätigen Sie den Dialog mit "OK". Das Gerät wird neu gestartet.

Unter "Information > Versionen" gibt es zusätzlich den Eintrag "Firmware_Running". Bei Firmware_Running wird die Version der aktuellen Firmware angezeigt. Bei Firmware wird die Firmware-Version angezeigt, die nach dem Firmware-Laden abgespeichert ist.




## 6.4 Firmware-Update über WBM und CLI nicht möglich

### Ursache

Wenn es während eines Firmware-Updates zu einem Spannungsausfall kommt, kann es vorkommen, dass das Gerät über das WBM und CLI nicht zu erreichen ist.

### Voraussetzung

- Der PC ist über die Schnittstelle mit dem Gerät verbunden.
- Auf dem PC ist ein TFTP-Client installiert und die Firmware-Datei ist vorhanden.

### Abhilfe

Über TFTP können Sie das Gerät auch dann mit einer Firmware versehen.
Führen Sie folgende Schritte durch, um eine neue Firmware über TFTP zu laden:

1. Drücken Sie nun den SET-Taster.
2. Halten Sie den Taster so lange gedrückt, bis die rote Fehler LED (F) nach ca. 3 Sekunden anfängt zu blinken.

   **Hinweis**

   Wenn Sie den SET-Taster ca. 10 Sekunden drücken, dann wird das Gerät auf seine Werkseinstellungen zurückgesetzt und ist über die IP-Adresse 192.168.1.1 erreichbar.

3. Lassen Sie nun den Taster los. Der Bootloader wartet in diesem Zustand auf eine neue Firmware-Datei, die Sie per TFTP laden können.

   **Hinweis**

   Wenn Sie den Bootloader ohne Änderung beenden wolllen, drücken Sie kurz den SET-Taster. Das Gerät startet mit der geladenen Konfiguration neu.

4. Verbinden Sie einen PC über die Ethernet-Schnittstelle mit dem Gerät.
5. Wechseln Sie in einer DOS-Box in das Verzeichnis, in dem sich die neue Firmware-Datei befindet und rufen Sie danach den Befehl "tftp -i <ip-adresse> PUT <firmware>" auf. Alternativ dazu können Sie einen anderen TFTP-Client verwenden.
   Wenn Sie nicht sicher sind, ob die IP-Adresse korrekt ist, dann können Sie diese z. B. mit SINEC PNI überprüfen.

**Hinweis**

**Verwenden von CLI und TFTP unter Windows 10**

Wenn Sie unter Windows 10 auf CLI oder TFTP zugreifen wollen, achten Sie darauf, dass die entsprechenden Funktionen in Windows 10 freigeschaltet sind.

### Ergebnis

Die Firmware wird auf das Gerät übertragen.

**Hinweis**

Bitte beachten Sie, dass die Übertragung der Firmware einige Minuten dauern kann. Während der Übertragung blinkt die rote Fehler LED (F).

Nachdem die Firmware komplett auf das Gerät übertragen ist, wird das Gerät automatisch neu gestartet.

## 6.5 Wiederherstellen der Werkseinstellungen

| ACHTUNG |
| --- |
| **Bisherige Einstellungen**<br>Durch das Zurücksetzen werden alle von Ihnen vorgenommenen Einstellungen durch werksseitige Voreinstellungen überschrieben. Es werden auch die geschützten Voreinstellungen zurückgesetzt. Bei SCALANCE MUM85x werden angelegte eSIM-Profile gelöscht. |

| ACHTUNG |
| --- |
| **Versehentliches Rücksetzen**<br>Durch ein versehentliches Rücksetzen können in einem projektierten Netzwerk Störungen und Ausfälle mit weiteren Folgen auftreten. |

### Mit dem Reset-Taster

Beachten Sie zur Betätigung des Tasters unbedingt die Hinweise in Kapitel "Reset-Taster" der Betriebsanleitung.

Führen Sie folgende Schritte durch, um die Gerätparameter auf die Werkseinstellungen zurückzusetzen:

1. Schalten Sie das Gerät spannungslos.
2. Drücken Sie nun den Reset-Taster und schließen Sie das Gerät mit gedrücktem Taster wieder an die Versorgungsspannung an.
3. Halten Sie den Taster so lange gedrückt, bis die rote Fehler LED (F) nach ca. 10 Sekunden aufhört zu blinken und in Dauerlicht wechselt.
4. Lassen Sie nun den Taster los und warten Sie, bis die Fehler-LED (F) wieder erlischt.
5. Das Gerät startet dann automatisch mit den Werkseinstellungen.
   **SCALANCE MUM85x:** Schalten Sie das Gerät nicht aus, bis es neu gestartet hat. Wird das Gerät während des Vorgangs ausgeschaltet, werden eSIM-Profile möglicherweise nicht vollständig gelöscht. Das führt dazu, dass keine Nachricht an Mobilfunkanbieter über freizugebende eSIM gesendet wird. In diesem Fall müssen Sie eine neue eSIM für den Mobilfunkvertrag beantragen.

### Über die Projektierung

Ausführliche Informationen zum Zurücksetzen der Geräteparameter über WBM und CLI finden Sie in den Projektierungshandbüchern:

- Web Based Management, Kapitel "Neustart"
- Command Line Interface, Kapitel "Reset and Defaults"

# Anhang A "Befehl-SMS"

A

## A.1 Befehl-SMS

Mit einer Befehl-SMS können Sie Befehle an das Gerät absetzen. Von wem eine Befehl-SMS akzeptiert wird, legen Sie unter "System > SMS > Befehl-SMS (Seite 273)" fest.

### Format der Befehl-SMS

Die Befehl-SMS hat folgendes Format.

- Klasse Befehl Aktion Parameter

### Voraussetzung für Antwort-SMS (STATUS)

- Unter "System > SMS > Ereignis-SMS" ist eine Rufnummer hinterlegt.

## Unterstützte Befehle

| Klasse | Befehl | Aktion | Parameter | |
|---|---|---|---|---|
| SYS<br>System-Befehle | DI | STATUS | Pin-Nummer 1 | Eine Antwort-SMS mit dem Status des digitalen Eingangs wird gesendet. |
| | DO | STATUS | Pin-Nummer 1 | Eine Antwort-SMS mit dem Status des digitalen Ausgangs wird gesendet. |
| | | LOW | | Der digitale Ausgang wird geöffnet. |
| | | HIGH | | Der digitale Ausgang wird geschlossen. |
| | IPSEC | STATUS | Namen der IPsec VPN-Verbindung<br>Security > IPsec VPN> Verbindungen (Seite 423)<br>Bei '*' werden die IPsec-Verbindungen aufgebaut, die bei "Betrieb" "Bei SMS starten" oder "Auf SMS warten" verwenden. | Eine Antwort-SMS mit dem Status des IPsec VPN-Tunnels wird gesendet. |
| | | UP | | Der IPsec VPN-Tunnel wird aufgebaut. |
| | | DOWN | | Bestehender IPsec VPN-Tunnel wird abgebaut. |
| | OVPN | STATUS | Namen der OpenVPN-Verbindung<br>Security > OpenVPN> Verbindungen (Seite 435)<br>Bei '*' werden die OpenVPN-Verbindungen aufgebaut, die bei "Betrieb" "Bei SMS starten" verwenden. | Eine Antwort-SMS mit dem Status des OpenVPN-Tunnels wird gesendet. |
| | | UP | | Der OpenVPN-Tunnel wird aufgebaut. |
| | | DOWN | | Bestehender OpenVPN-Tunnel wird abgebaut. |
| | SRC | STATUS | Adresse des SINEMA RC-Servers<br>WAN-IP-Adresse oder der Hostnamen<br>SINEMA RC (Seite 158) | Eine Antwort-SMS mit dem Status der SINEMA RC-Verbindung wird gesendet. |
| | | UP | | Die Verbindung zum SINEMA RC-Server wird aufgebaut. |
| | | DOWN | | Die bestehende Verbindung zum SINEMA RC-Server wird abgebaut. |
| RLY<br>SMS Relay-Befehl | Name der Relay-Verbindung<br>System > SMS > SMS-Relay (Eingehend) (Seite 276) | - | Text | Der Text aus der SMS wird an den Empfänger weitergeleitet.<br>In dem Text sind folgende Zeichen erlaubt:<br>• 0123456789<br>• A...Z a...z<br>• Leerzeichen<br>• ! " % & / ( ) = ? * + < > ' , . - |

## Beispiele

**Weck-SMS**

SYS SRC UP 192.168.20.200

**SMS an eine Anwendung im LAN**

RLY conn2 mein SMS Text

Der Text "mein SMS Text" wird an die Anwendung weitergeleitet, die in der Relay-Verbindung "conn2" angegeben ist. Der Text wird als folgendes Telegramm weitergeleitet: benutzer#passwort#105#01;0049xxxxxxxxx;mein SMS Text:

# Anhang B "Syslog-Meldungen"

B

## B.1 Format der Syslog-Meldungen

Die Geräte generieren Syslog-Meldungen (UDP-Standardport 514) gemäß RFC 5424, die die folgenden Felder enthalten.

**HEADER**

- TIMESTAMP gemäß RFC 3339
- Hostname
- APPNAME, PROCID und MSGID: Sind keine Angaben bekannt, wird das Zeichen "-" ausgegeben.

**PRIORITY**

Innerhalb **PRIORITY** steht codiert die Priorität der Syslog-Meldung aufgeteilt in ein Severity- und Facility-Feld.

- Facility
- Severity

**VERSION**

- Auf 1 gesetzt.

**HOSTNAME_CONTENT:**

- IPv4-Adresse nach RFC1035: Jedes Byte wird dezimal dargestellt und ist durch einen Punkt vom vorherigen getrennt: XXX.XXX.XXX.XXX
- IPv6-Adresse nach RFC4291 Section 2.2

**STRUCTURED DATA**

- timeQuality-Block

**MESSAGE:**

- ASCII-String in Englisch

---

**Hinweis**

Weitere Informationen über die Bedeutung der Felder finden Sie im RFC 5424 (https://datatracker.ietf.org/doc/html/rfc5424).

---

## B.2 Parameter in Syslog-Meldungen

Die Syslog-Meldungen können folgende Parameter beinhalten:

| Parameter | Beschreibung | Mögliche Werte oder Beispiel |
|---|---|---|
| ip address | IPv4- oder IPv6-Adresse | IP-Adresse nach RFC1035 oder RFC4291 Abschnitt 2.2 |
| src port<br>dest port | Port, der als dezimale Nummer dargestellt wird.<br>Format: %d | 0 ... 65535 |
| dest mac<br>src mac | MAC-Adresse<br>Format: %02x:%02x:%02x;%02x:%02x:%02x | 00:0C:29:2F:09:B3 |
| protocol | Bezeichnung des Dienstes, der dieses Ereignis generiert hat, oder des verwendeten Layer-4-Protokolls.<br>Format: %s | Mögliche Einträge von:<br>UDP \| TCP \| WBM \| Telnet \| SSH \| TFTP \| SFTP |
| group | Zeichenkette, die die Gruppe anhand ihres Namens identifiziert<br>Format: %s | it-service |
| user name | Zeichenkette, die den authentifizierten Benutzer anhand seines Namens identifiziert<br>ohne Leerzeichen<br>Format: %s | maier |
| action user name | Identifiziert den Benutzer anhand seines Namens. Dies ist nicht der authentifizierte Benutzer<br>Format: %s | Peter.Maier |
| role | Symbolischer Name für die Gruppenrolle<br>Format: %s | Administrator |
| time minute<br>timeout | Minutenanzahl<br>Format: %d | 44 |
| failed login count | Anzahl der fehlgeschlagenen Logins<br>Format: %d | 10 |
| max sessions | Anzahl der Sitzungen<br>Format: %d | 10 |
| trigger pin | Zeichenkette für einen IO-Pin, der das Ereignis ausgelöst<br>ohne Leerzeichen<br>Format: %s | DI1 |
| firewall rule | Zeichenkette für einen Firewall-Regelsatz<br>mit Leerzeichen<br>Format: %s | Rule1 |
| subject | Zeichenkette für den Betreff im Zertifikat. Wird verwendet als Teil der zertifikatbasierten Authentifizierung<br>mit Leerzeichen und muss zusätzlich Unicode-Zeichen enthalten<br>Format: (% S) oder (% S% S) bei UTF8-Code. | (Peter Maier) |

| Parameter | Beschreibung | Mögliche Werte oder Beispiel |
|---|---|---|
| config detail | Zeichenkette für die Konfiguration mit Leerzeichen<br>Format: %s | OpenVPN |
| connection name | Name einer VPN-Verbindung | to_Baugruppe1 |
| firewall accept | Firewall-Aktion ausgeführt (akzeptiertes Paket) | ACCEPT |
| firewall action reject | Firewall-Aktion ausgeführt (abgelehntes Paket) | REJECT DROP |
| length | Länge des Netzwerkpakets (in Bytes)<br>Format: %d | 52 |
| network interface | Symbolischer Name einer Netzwerkschnittstelle<br>Format: %s | vlan1 |

## B.3 Syslog-Meldungen

**Identifizierung und Authentifizierung von menschlichen Nutzern**

| | |
|---|---|
| Meldungstext | {protocol}: User {User name} has logged in from {ip address}. |
| Beispiel | WBM: User "Admin" has logged in from 192.168.0.1. |
| Erläuterung | Gültige Anmeldeinformationen, die bei der Remote-Anmeldung angegeben werden. |
| Severity | Info |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR 1.1 |

| | |
|---|---|
| Meldungstext | {protocol}: User {User name} failed to log in from {ip address}. |
| Beispiel | WBM: User "Admin" has failed to log in from 192.168.0.1. |
| Erläuterung | Falscher Benutzername oder falsches Kennwort (Anmeldeinformationen) bei der Remote-Anmeldung angegeben. |
| Severity | Warning |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR 1.1 |

| | |
|---|---|
| Meldungstext | {protocol}: User {User name} has logged out from {ip address}. |
| Beispiel | SSH: User "Admin" has logged out from 192.168.0.1. |
| Erläuterung | Benutzersitzung beendet - Abmeldung erfolgt. |
| Severity | Info |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR 1.1 |

| | |
|---|---|
| Meldungstext | {protocol}: Default user {user name} logged in from {ip address}. |
| Beispiel | SSH: Default user admin logged in from 192.168.0.1. |
| Erläuterung | Standardnutzer ist angemeldet über die IP-Adresse. |

| | |
|---|---|
| Severity | Info |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: n/a (NERC-CIP 007-R5) |

**Identifizierung und Authentifizierung von Geräten (Zugriff über Firewall)**

| | |
|---|---|
| Meldungstext | {firewall action accept}(1) in:{network interface} out:{network interface} len: {length} s-mac:{src mac} d-mac:{dest mac}<br>s-ip:{ip address} d-ip:{ip address}<br>{protocol}:{src port}->{dest port} |
| Beispiel | ACCEPT(1) in:vlan1 out:ppp0 len:52<br>s-mac:58:EF:68:B3:FA:CE d-mac:00:1B:1B:A7:5B:D8<br>s-ip:172.23.1.6 d-ip:158.85.11.68 tcp:53788->443 |
| Erläuterung | Ein bekanntes Gerät hat eine Verbindung angefordert. |
| Severity | Info or Warning (configurable) |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR 1.2 |

| | |
|---|---|
| Meldungstext | {firewall action reject}(1) in:{network interface} out:{network interface} len: {length} s-mac:{src mac} d-mac:{dest mac}<br>s-ip:{ip address} d-ip:{ip address}<br>{protocol}:{src port}->{dest port} |
| Beispiel | REJECT(1) in:vlan1 out:ppp0 len:52<br>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<br>tcp:53773->443 |
| Erläuterung | Ein unbekanntes Gerät hat eine Verbindung angefordert. Die Anfrage wurde abgelehnt. |
| Severity | Info or Warning (configurable) |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR 1.2 |

**Nutzerkontenverwaltung**

| | |
|---|---|
| Meldungstext | {protocol}: User {user name} changed own password. |
| Beispiel | WBM: User admin changed own password. |
| Erläuterung | Benutzer hat sein Passwort geändert. |
| Severity | Notice |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR1.3 |

| | |
|---|---|
| Meldungstext | {protocol}: User {user name} changed password of user {action user name}. |
| Beispiel | Telnet: User admin changed password of user test. |
| Erläuterung | Benutzer hat das Passwort eines anderen Benutzers geändert. |
| Severity | Notice |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR1.3 |

| | |
|---|---|
| Meldungstext | {protocol}: User {user name} created user-account {action user name}. |
| Beispiel | WBM: User admin created user-account service. |
| Erläuterung | Der Benutzer hat ein Konto erstellt. |
| Severity | Notice |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR1.3 |

| | |
|---|---|
| Meldungstext | {protocol}: User {user name} deleted user-account {action user name}. |
| Beispiel | WBM: User admin deleted user-account service. |
| Erläuterung | Der Administrator hat ein vorhandenes Konto gelöscht. |
| Severity | Notice |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR1.3 |

### Verwaltung der Kennungen

| | |
|---|---|
| Meldungstext | {Protocol}: User {User name} created group {Group} and assigned to role {Role}. |
| Beispiel | WBM: User admin created group it-service and assigned to role service. |
| Erläuterung | Der Administrator hat eine Gruppe erstellt und einer Rolle zugeordnet. |
| Severity | Notice |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR 1.4 |

| | |
|---|---|
| Meldungstext | {Protocol}: User {User name} deleted group {Group} and the role {Role} assignment. |
| Beispiel | WBM: User maier deleted group it-service and the role service assignment. |
| Erläuterung | Der Administrator hat eine vorhandene Gruppe und die Rollenzuordnung gelöscht. |
| Severity | Notice |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR 1.4 |

### Erfolglose Anmeldeversuche

| | |
|---|---|
| Meldungstext | {User name} account is locked for {Time minute} minutes after {Failed login count} unsuccessful login attempts. |
| Beispiel | User service account is locked for 44 minutes after 10 unsuccessful login attempts. |
| Erläuterung | Bei zu vielen fehlgeschlagenen Anmeldungen wurde das entsprechende Benutzerkonto für einen bestimmten Zeitraum gesperrt. |
| Severity | Warning |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR 1.11 |

### Zugriff über nicht vertrauenswürdige Netze (IPsec)

| | |
|---|---|
| Meldungstext | [IKE] <{connection name}\|{config detail}> IKE_SA {connection name}[{config detail}] established between {ip address}[{config detail}]...{ip address}[{config detail}] |
| Beispiel | [IKE] <c1\|3> IKE_SA c1[1] established between 192.168.55.210[lokal].. 192.168.55.211[remote] |
| Erläuterung | VPN-Verbindung ist hergestellt (IPsec). |
| Severity | Info |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1) |

| | |
|---|---|
| Meldungstext | [IKE] <{connection name}\|{config detail}> deleting IKE_SA {connection name} [{config detail}] between {ip address}[{config detail}]...{ip address}[{config detail}] |
| Beispiel | [IKE] <c1\|3> deleting IKE_SA c2[1] between 192.168.55.211[lokal].. 192.168.55.210[remote] |
| Erläuterung | VPN-Tunnel ist geschlossen (IPsec). |
| Severity | Info |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1) |

| | |
|---|---|
| Meldungstext | [IKE] <{connection name}\|{config detail}> received AUTHENTICATION_FAILED notify error |
| Beispiel | [IKE] <c1\|1> received AUTHENTICATION_FAILED notify error |
| Erläuterung | Authentifizierung der VPN-Verbindung ist fehlgeschlagen (IPsec). |
| Severity | Warning |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: n/a (NERC CIP 005-R3) |

### Zugriff über nicht vertrauenswürdige Netze (OpenVPN)

| | |
|---|---|
| Meldungstext | OVPN_{connection name}[{config detail}]: Initialization Sequence Completed |
| Beispiel | OVPN_Conn_1[2427]: Initialization Sequence Completed |
| Erläuterung | VPN-Verbindung ist hergestellt (OpenVPN). |
| Severity | Info |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1) |

| | |
|---|---|
| Meldungstext | OpenVPN connection {connection name} has been deactivated. |
| Beispiel | OpenVPN connection c1 has been deactivated. |
| Erläuterung | VPN-Verbindung wurde geschlossen (OpenVPN). |
| Severity | Info |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1) |

### Zugriff über nicht vertrauenswürdige Netze (SINEMA Remote Connect)

| | |
|---|---|
| Meldungstext | SINEMA RC - State of Digital Input changed to HIGH. SINEMA RC - OpenVPN connection established. |
| Beispiel | SINEMA RC - State of Digital Input changed to HIGH.<br>SINEMA RC - OpenVPN connection established. |
| Erläuterung | Fernzugriff ist erlaubt. (SINEMA RC, Digitaler Eingang) |
| Severity | Info |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR 1.13 |

| | |
|---|---|
| Meldungstext | SINEMA RC - Received Wakeup SMS.<br>SINEMA RC - OpenVPN connection established. |
| Beispiel | SINEMA RC - Received Wakeup SMS.<br>SINEMA RC - OpenVPN connection established. |
| Erläuterung | Fernzugriff ist erlaubt. (SINEMA RC, Wakeup SMS) |
| Severity | Info |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR 1.13 |

| | |
|---|---|
| Meldungstext | SINEMA RC - State of Digital Input changed to LOW. SINEMA RC - OpenVPN terminated. |
| Beispiel | SINEMA RC - State of Digital Input changed to LOW.<br>SINEMA RC - OpenVPN terminated. |
| Erläuterung | Fernzugriff verweigert (SINEMA RC, Digitaler Eingang) |
| Severity | Info |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR 1.13 |

| | |
|---|---|
| Meldungstext | SINEMA RC - Received Shutdown SMS. SINEMA RC - OpenVPN terminated. |
| Beispiel | SINEMA RC - Received Shutdown SMS.<br>SINEMA RC - OpenVPN terminated. |
| Erläuterung | Fernzugriff verweigert (SINEMA RC, Wakeup SMS) |
| Severity | Info |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR 1.13 |

### Durchsetzung der Autorisierung (Zugriff über benutzerspezifische Firewall)

| | |
|---|---|
| Meldungstext | User specific firewall user "{user name}" activated rule set "{firewall rule}" with ip address "{ip address}". Timeout: {timeout} minutes. |
| Beispiel | User specific firewall user "usf" activated rule set "rs1" with ip address "172.23.1.14". Timeout 5 minutes. |
| Erläuterung | Der Benutzer hat sich an der benutzerspezifischen Firewall angemeldet. (USF Digital User Login) |
| Severity | Info |

| | |
|---|---|
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: n/a (NERC CIP 005-R2) |

| | |
|---|---|
| Meldungstext | User specific firewall digital input {trigger pin} activated rule set "{firewall rule}" with ip "{ip address}". |
| Beispiel | User specific firewall digital input 1 activated rule set "cpu2" with ip "192.168.16.1". |
| Erläuterung | Der Benutzer hat sich an der benutzerspezifischen Firewall angemeldet. (USF Digital Input Login) |
| Severity | Info |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: n/a (NERC CIP 005-R2)4820486 |

| | |
|---|---|
| Meldungstext | User specific firewall user "{user name}" ruleset "{firewall rule}" time expired. |
| Beispiel | User specific firewall user "usf" ruleset "rs1" time expired. |
| Erläuterung | Der Zugriff auf die benutzerspezifische Firewall wurde verweigert. Die Zugriffszeit abgelaufen. (USF User Logout) |
| Severity | Warning |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR 2.1 |

| | |
|---|---|
| Meldungstext | User specific firewall user "{user name}" logged out by administrator configuration. |
| Beispiel | User specific firewall user "usf" logged out by administrator configuration. |
| Erläuterung | Der Zugriff auf die benutzerspezifische Firewall wurde verweigert. Der Geräteadministrator hat den Benutzer über die Schaltfläche "Deaktivierung erzwingen" deaktiviert. (USF user force logout by admin) |
| Severity | Warning |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR 2.1 |

| | |
|---|---|
| Meldungstext | User specific firewall user "{user name}" deactivated by administrator configuration. |
| Beispiel | User specific firewall user "usf" deactivated by administrator configuration. |
| Erläuterung | Der Zugriff auf die benutzerspezifische Firewall wurde verweigert. Der Geräteadministrator hat den Benutzer deaktiviert. (USF user deactivated by admin) |
| Severity | Warning |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR 2.1 |

| | |
|---|---|
| Meldungstext | User specific firewall digital input {trigger pin} deactivated rule set "{firewall rule}". |
| Beispiel | User specific firewall digital input 1 deactivated rule set "rs1". |
| Erläuterung | Der Zugriff auf die benutzerspezifische Firewall wurde verweigert. Der entsprechende Regelsatz wurde deaktiviert. (USF Digital Input Logout) |
| Severity | Info |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR 2.1 |

### Sitzungssperrung

| | |
|---|---|
| Meldungstext | The session of user {user name} was closed after {time} seconds of inactivity. |
| Beispiel | The session of user admin was closed after 60 seconds of inactivity. |
| Erläuterung | Die aktuelle Sitzung wurde aufgrund der Inaktivität gesperrt. |
| Severity | Warning |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR 2.5 |

### Beendigung einer Fernzugriffssitzung

| | |
|---|---|
| Meldungstext | [JOB] <{connection name}\|{config detail}> deleting CHILD_SA after {time second} seconds of inactivity |
| Beispiel | [JOB] <to_Baugruppe1\|21> deleting CHILD_SA after 20 seconds of inactivity |
| Erläuterung | Die Remote-Sitzung wurde nach Inaktivitätszeit beendet (IPsec). |
| Severity | Notice |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR 2.6 |

| | |
|---|---|
| Meldungstext | OVPN_{connection name}[{config detail}]: [{config detail}] Inactivity timeout (--ping-restart), restarting |
| Beispiel | OVPN_c1[26296]: [router] Inactivity timeout (--ping-restart), restarting |
| Erläuterung | Die Remote-Sitzung wurde nach Inaktivitätszeit beendet (OpenVPN). |
| Severity | Notice |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR 2.6 |

### Begrenzung der Anzahl gleichzeitiger Sitzungen

| | |
|---|---|
| Meldungstext | {Protocol}: The maximum number of {Max sessions} concurrent login session exceeded. |
| Beispiel | WBM: The maximum number of 10 concurrent login sessions exceeded. |
| Erläuterung | Die maximale Anzahl gleichzeitiger Sitzungen ist überschritten. |
| Severity | Warning |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR 2.7 |

### Nicht-Abstreitbarkeit

| | |
|---|---|
| Meldungstext | Device configuration changed. |
| Beispiel | Device configuration changed. |
| Erläuterung | Die Gerätekonfiguration ist dauerhaft geändert. |
| Severity | Info |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR2.12 |

### Kommunikationsintegrität

| | |
|---|---|
| Meldungstext | [IKE] {connection name} {config detail} received invalid DPD sequence number {config detail} (expected {config detail}), ignored. |
| Beispiel | [IKE] "c1" "1" received invalid DPD sequence number 10 (expected 12), ignored. |
| Erläuterung | Integritätsprüfung ist fehlgeschlagen (IPsec) |
| Severity | Warning |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR 3.1 |

| | |
|---|---|
| Meldungstext | OVPN_{connection name}{config detail}: Authenticate/Decrypt packet error: packet HMAC authentication failed. |
| Beispiel | OVPN_c1[25409]: Authenticate/Decrypt packet error: packet HMAC authentication failed. |
| Erläuterung | Integritätsprüfung ist fehlgeschlagen (OpenVPN). |
| Severity | Warning |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR 3.1 |

### Sitzungsintegrität

| | |
|---|---|
| Meldungstext | {Protocol}: Session ID verification from {ipaddress} failed. |
| Beispiel | WBM Session ID verification from 192.168.1.1 failed. |
| Erläuterung | Die Sitzungs-ID von 192.168.1.1 ist ungültig. |
| Severity | Warning |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR 3.8 |

### Datensicherung im Automatisierungssystem (Backup)

| | |
|---|---|
| Log-Text | {protocol}: Saved file type ConfigPack. |
| Norm | IEC 62443-3-3 Reference: SR7.3 |
| Beschreibung | Die Datei ConfigPack wurde gespeichert. |
| Beispiel | TFTP: Saved file type ConfigPack |
| Severity | Notice |
| Facility | local0 |

| | |
|---|---|
| Log-Text | {protocol}: User {user name} saved file type ConfigPack |
| Norm | IEC 62443-3-3 Reference: SR7.3 |
| Beschreibung | Benutzer hat die Datei ConfigPack gespeichert. |
| Beispiel | WBM: User admin saved file type ConfigPack.. |
| Severity | Notice |
| Facility | local0 |

| | |
|---|---|
| Log-Text | {protocol}: User {user name} failed to save file type ConfigPack. |
| Norm | IEC 62443-3-3 Reference: SR7.3 |
| Beschreibung | Benutzer konnte die Datei ConfigPack nicht speichern. |

| | |
|---|---|
| Beispiel | WBM: User admin failed to save file type ConfigPack. |
| Severity | Info |
| Facility | local0 |

| | |
|---|---|
| Log-Text | {protocol}: Failed to save file type ConfigPack. |
| Norm | IEC 62443-3-3 Reference: SR7.3 |
| Beschreibung | Die Datei ConfigPack konnte nicht gespeichert werden. |
| Beispiel | TFTP: Failed to save file type ConfigPack. |
| Severity | Warning |
| Facility | local0 |

**Wiederherstellung des Automatisierungssystems**

| | |
|---|---|
| Meldungstext | {protocol}: Loaded file type Firmware {version} (restart required). |
| Beispiel | TFTP: Loaded file type Firmware V02.00.00 (restart required). |
| Erläuterung | Die Firmware wurde erfolgreich geladen. |
| Severity | Notice |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR7.4 |

| | |
|---|---|
| Meldungstext | {protocol}: User {user name} loaded file type Firmware {version} (restart required). |
| Beispiel | WBM: User admin loaded file type Firmware V02.00.00 (restart required). |
| Erläuterung | Der Benutzer hat die Firmware erfolgreich geladen. |
| Severity | Notice |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR7.4 |

| | |
|---|---|
| Meldungstext | {protocol}: Failed to load file type Firmware. |
| Beispiel | WBM: Failed to load file type Firmware. |
| Erläuterung | Hochladen der Firmware fehlgeschlagen. |
| Severity | Warning |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR7.4 |

| | |
|---|---|
| Meldungstext | {protocol}: Loaded file type Config (restart required). |
| Beispiel | TFTP: Loaded file type Config (restart required). |
| Erläuterung | Die Konfiguration wird angewendet. |
| Severity | Notice |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR7.4 |

| | |
|---|---|
| Meldungstext | {protocol}: Loaded file type ConfigPack (restart required). |
| Beispiel | TFTP: Loaded file type ConfigPack (restart required). |
| Erläuterung | Die Konfiguration wird angewendet. |
| Severity | Notice |

| | |
|---|---|
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR7.4 |

| | |
|---|---|
| Meldungstext | {protocol}: User {user name} loaded file type Config (restart required). |
| Beispiel | WBM: User admin loaded file type Config (restart required). |
| Erläuterung | Die Konfiguration wird angewendet. |
| Severity | Notice |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR7.4 |

| | |
|---|---|
| Meldungstext | {protocol}: User {user name} loaded file type ConfigPack (restart required). |
| Beispiel | WBM: User admin loaded file type ConfigPack (restart required). |
| Erläuterung | Die Konfiguration wird angewendet. |
| Severity | Notice |
| Facility | local0 |
| Norm | IEC 62443-3-3 Reference: SR7.4 |

# Anhang C "Verwendete Verschlüsselungsverfahren (Ciphers)"

C

In den nachfolgenden Tabellen sind die Verschlüsselungsverfahren (Ciphers) aufgelistet, die SCALANCE M-800 verwendet.

## C.1 SSL

### HTTPS WBM Server

| Kategorie | IANA-Name | Hexadezimal-wert | Standardmäßig aktiviert |
|---|---|---|---|
| Verschlüsselungssuite | TLS_AES_128_GCM_SHA256 | 1301 | ✓ |
| Verschlüsselungssuite | TLS_CHACHA20_POLY1305_SHA256 | 1303 | ✓ |
| Verschlüsselungssuite | TLS_AES_256_GCM_SHA384 | 1302 | ✓ |
| Verschlüsselungssuite | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | c02f | ✓ |
| Verschlüsselungssuite | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | c030 | ✓ |
| Protokollversion | TLSv1.2 | -- | ✓ |
| Protokollversion | TLSv1.3 | -- | ✓ |

### HTTPS WBM Client

| Kategorie | IANA-Name | Hexadezimal-wert | Standardmäßig aktiviert |
|---|---|---|---|
| Verschlüsselungssuite | TLS_AES_128_GCM_SHA256 | 1301 | ✓ |
| Verschlüsselungssuite | TLS_CHACHA20_POLY1305_SHA256 | 1303 | ✓ |
| Verschlüsselungssuite | TLS_AES_256_GCM_SHA384 | 1302 | ✓ |
| Verschlüsselungssuite | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 | c02c | ✓ |
| Verschlüsselungssuite | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 | c02b | ✓ |
| Verschlüsselungssuite | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | c02f | ✓ |
| Verschlüsselungssuite | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | c030 | ✓ |
| Protokollversion | TLSv1.2 | -- | ✓ |
| Protokollversion | TLSv1.3 | -- | ✓ |

### SMTP Client (secure)

| Kategorie | IANA-Name | Hexadezimal-wert | Standardmäßig aktiviert |
|---|---|---|---|
| Verschlüsselungssuite | TLS_AES_128_GCM_SHA256 | 1301 | ✓ |
| Verschlüsselungssuite | TLS_CHACHA20_POLY1305_SHA256 | 1303 | ✓ |
| Verschlüsselungssuite | TLS_AES_256_GCM_SHA384 | 1302 | ✓ |
| Verschlüsselungssuite | TLS_ECDHE_ECD-SA_WITH_AES_256_GCM_SHA384 | c02c | ✓ |
| Verschlüsselungssuite | TLS_ECDHE_ECD-SA_WITH_AES_128_GCM_SHA256 | c02b | ✓ |
| Verschlüsselungssuite | TLS_ECD-HE_RSA_WITH_AES_128_GCM_SHA256 | c02f | ✓ |
| Verschlüsselungssuite | TLS_ECD-HE_RSA_WITH_AES_256_GCM_SHA384 | c030 | ✓ |
| Protokollversion | TLSv1.2 | -- | ✓ |
| Protokollversion | TLSv1.3 | -- | ✓ |

### Syslog Client TLS

| Kategorie | IANA-Name | Hexadezimal-wert | Standardmäßig aktiviert |
|---|---|---|---|
| Verschlüsselungssuite | TLS_AES_128_GCM_SHA256 | 1301 | ✓ |
| Verschlüsselungssuite | TLS_CHACHA20_POLY1305_SHA256 | 1303 | ✓ |
| Verschlüsselungssuite | TLS_AES_256_GCM_SHA384 | 1302 | ✓ |
| Verschlüsselungssuite | TLS_ECDHE_ECD-SA_WITH_AES_256_GCM_SHA384 | c02c | ✓ |
| Verschlüsselungssuite | TLS_ECDHE_ECD-SA_WITH_AES_128_GCM_SHA256 | c02b | ✓ |
| Verschlüsselungssuite | TLS_ECD-HE_RSA_WITH_AES_128_GCM_SHA256 | c02f | ✓ |
| Verschlüsselungssuite | TLS_ECD-HE_RSA_WITH_AES_256_GCM_SHA384 | c030 | ✓ |
| Protokollversion | TLSv1.2 | -- | ✓ |
| Protokollversion | TLSv1.3 | -- | ✓ |

## C.2 OpenVPN

| Kategorie | IANA-Name | Hexadezimal-wert | Standardmäßig aktiviert |
|---|---|---|---|
| Verschlüsselungssuite | TLS_DHE_RSA_WITH_CHACHA20_PO-LY1305_SHA256 | ccaa | -- |
| Verschlüsselungssuite | TLS_DHE_RSA_WITH_AES_256_GCM_SHA 384 | 009f | -- |

| Kategorie | IANA-Name | Hexadezimal-wert | Standardmäßig aktiviert |
|---|---|---|---|
| Verschlüsselungssuite | TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 | 009e | -- |
| Verschlüsselungssuite | TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 | 006b | -- |
| Verschlüsselungssuite | TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 | 0067 | -- |
| Verschlüsselungssuite | TLS_DHE_RSA_WITH_AES_256_CBC_SHA | 0039 | -- |
| Verschlüsselungssuite | TLS_DHE_RSA_WITH_AES_128_CBC_SHA | 0033 | -- |
| Protokollversion | TLSv1.2 | -- | -- |

## C.3 SINEMA RC

### Client-Verbindung zu SINEMA RC

| Kategorie | IANA-Name | Hexadezimal-wert | Standardmäßig aktiviert |
|---|---|---|---|
| Verschlüsselungssuite | TLS_AES_128_GCM_SHA256 | 1301 | -- |
| Verschlüsselungssuite | TLS_CHACHA20_POLY1305_SHA256 | 1303 | -- |
| Verschlüsselungssuite | TLS_AES_256_GCM_SHA384 | 1302 | -- |
| Verschlüsselungssuite | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 | c02c | -- |
| Verschlüsselungssuite | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 | c02b | -- |
| Verschlüsselungssuite | TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 | 009e | -- |
| Verschlüsselungssuite | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | 009f | -- |
| Verschlüsselungssuite | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | c02f | -- |
| Verschlüsselungssuite | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | c030 | -- |
| Protokollversion | TLSv1.2 | -- | -- |
| Protokollversion | TLSv1.3 | -- | -- |

## C.4 cSRP

| Kategorie | IANA-Name | Hexadezimal-wert | Standardmäßig aktiviert |
|---|---|---|---|
| Verschlüsselungssuite | TLS_AES_128_GCM_SHA256 | 1301 | -- |
| Verschlüsselungssuite | TLS_CHACHA20_POLY1305_SHA256 | 1303 | -- |
| Verschlüsselungssuite | TLS_AES_256_GCM_SHA384 | 1302 | -- |

| Kategorie | IANA-Name | Hexadezimal-wert | Standardmä-ßig aktiviert |
|---|---|---|---|
| Verschlüsselungssuite | TLS_ECDHE_ECD-SA_WITH_AES_128_GCM_SHA256 | c02b | -- |
| Verschlüsselungssuite | TLS_ECD-HE_RSA_WITH_AES_128_GCM_SHA256 | c02f | -- |
| Verschlüsselungssuite | TLS_ECDHE_ECDSA_WITH_CHA-CHA20_POLY1305_SHA256 | cca9 | -- |
| Verschlüsselungssuite | TLS_ECDHE_RSA_WITH_CHACHA20_PO-LY1305_SHA256 | cca8 | -- |
| Verschlüsselungssuite | TLS_ECDHE_ECD-SA_WITH_AES_256_GCM_SHA384 | c02c | -- |
| Verschlüsselungssuite | TLS_ECD-HE_RSA_WITH_AES_256_GCM_SHA384 | c030 | -- |
| Verschlüsselungssuite | TLS_ECDHE_ECD-SA_WITH_AES_256_CBC_SHA | c00a | -- |
| Verschlüsselungssuite | TLS_ECDHE_ECD-SA_WITH_AES_128_CBC_SHA | c009 | -- |
| Verschlüsselungssuite | TLS_ECD-HE_RSA_WITH_AES_128_CBC_SHA | c013 | -- |
| Verschlüsselungssuite | TLS_ECD-HE_RSA_WITH_AES_256_CBC_SHA | c014 | -- |
| Verschlüsselungssuite | TLS_RSA_WITH_AES_128_GCM_SHA256 | 009c | -- |
| Verschlüsselungssuite | TLS_RSA_WITH_AES_256_GCM_SHA384 | 009d | -- |
| Verschlüsselungssuite | TLS_RSA_WITH_AES_128_CBC_SHA | 002f | -- |
| Verschlüsselungssuite | TLS_RSA_WITH_AES_256_CBC_SHA | 0035 | -- |
| Verschlüsselungssuite | TLS_RSA_WITH_3DES_EDE_CBC_SHA | 000a | -- |
| Protokollversion | TLS 1.2 ( 0x0303) | -- | -- |
| Protokollversion | TLS 1.3 (0x0304) | -- | -- |

## C.5 SSH CLI

### SSH CLI Server

| Kategorie | Verfahren | Hexadezimal-wert | Standardmä-ßig aktiviert |
|---|---|---|---|
| Verschlüsselungsverfah-ren (enc) | aes256-ctr | -- | ✓ |
| Host-Schlüssel (key) | ecdsa-sha2-nistp521 | -- | ✓ |
| Host-Schlüssel (key) | rsa-sha2-256 | -- | ✓ |
| Host-Schlüssel (key) | rsa-sha2-512 | -- | ✓ |
| Schlüsselaustausch (kex) | curve25519-sha256 | -- | ✓ |
| Schlüsselaustausch (kex) | curve25519-sha256@libssh.org | -- | ✓ |

| Kategorie | Verfahren | Hexadezimal-wert | Standardmä-ßig aktiviert |
|---|---|---|---|
| Schlüsselaustausch (kex) | ecdh-sha2-nistp256 | -- | ✓ |
| Schlüsselaustausch (kex) | ecdh-sha2-nistp384 | -- | ✓ |
| Schlüsselaustausch (kex) | ecdh-sha2-nistp521 | -- | ✓ |
| Schlüsselaustausch (kex) | diffie-hellman-group16-sha512 | -- | ✓ |
| Schlüsselaustausch (kex) | diffie-hellman-group18-sha512 | -- | ✓ |
| MAC | hmac-sha2-256 | -- | ✓ |
| Protokollversion | SSHv2.0 | -- | ✓ |

## SFTP Server

| Kategorie | Verfahren | Hexadezimal-wert | Standardmä-ßig aktiviert |
|---|---|---|---|
| Verschlüsselungsverfah-ren (enc) | aes256-ctr | -- | ✓ |
| Host-Schlüssel (key) | ecdsa-sha2-nistp521 | -- | ✓ |
| Host-Schlüssel (key) | rsa-sha2-256 | -- | ✓ |
| Host-Schlüssel (key) | rsa-sha2-512 | -- | ✓ |
| Schlüsselaustausch (kex) | curve25519-sha256 | -- | ✓ |
| Schlüsselaustausch (kex) | curve25519-sha256@libssh.org | -- | ✓ |
| Schlüsselaustausch (kex) | ecdh-sha2-nistp256 | -- | ✓ |
| Schlüsselaustausch (kex) | ecdh-sha2-nistp384 | -- | ✓ |
| Schlüsselaustausch (kex) | ecdh-sha2-nistp521 | -- | ✓ |
| Schlüsselaustausch (kex) | diffie-hellman-group16-sha512 | -- | ✓ |
| Schlüsselaustausch (kex) | diffie-hellman-group18-sha512 | -- | ✓ |
| MAC | hmac-sha2-256 | -- | ✓ |
| Protokollversion | SSHv2.0 | -- | ✓ |

## C.6 SNMP

### SNMP Server

| Kategorie | Verfahren | Hexadezimal-wert | Standardmäßig aktiviert |
|---|---|---|---|
| Authentifizierung | HMAC-MD5-96 | -- | -- |
| Authentifizierung | HMAC-SHA-96 | -- | -- |
| Verschlüsselung | des-cbc | -- | -- |
| Verschlüsselung | aes128-cbc | -- | -- |

### SNMP Trap

| Kategorie | Verfahren | Hexadezimal-wert | Standardmäßig aktiviert |
|---|---|---|---|
| Authentifizierung | HMAC-MD5-96 | -- | -- |
| Authentifizierung | HMAC-SHA-96 | -- | -- |
| Verschlüsselung | des-cbc | -- | -- |
| Verschlüsselung | aes128-cbc | -- | -- |

## C.7 RADIUS

### RADIUS Client

| Kategorie | Verfahren | Hexadezimal-wert | Standardmäßig aktiviert |
|---|---|---|---|
| Integritätsalgorithmus | MD5 | -- | -- |
| Integritätsalgorithmus | HMAC-SHA1 | -- | -- |

## C.8 IPsec

### IPsec Server

| Kategorie | Verfahren | Hexadezimal-wert | Standardmäßig aktiviert |
|---|---|---|---|
| ESP /AH-Authentifizierung | MD5 | -- | -- |
| ESP /AH-Authentifizierung | SHA1 | -- | -- |
| ESP /AH-Authentifizierung | SHA256 | -- | -- |

| Kategorie | Verfahren | Hexadezimal-wert | Standardmäßig aktiviert |
|---|---|---|---|
| ESP /AH-Authentifizierung | SHA384 | -- | -- |
| ESP /AH-Authentifizierung | SHA512 | -- | -- |
| ESP-Verschlüsselung | 3des-168-cbc | -- | -- |
| ESP-Verschlüsselung | aes128-cbc | -- | -- |
| ESP-Verschlüsselung | aes192-cbc | -- | -- |
| ESP-Verschlüsselung | aes256-cbc | -- | -- |
| ESP-Verschlüsselung | aes128-ctr | -- | -- |
| ESP-Verschlüsselung | aes192-ctr | -- | -- |
| ESP-Verschlüsselung | aes256-ctr | -- | -- |
| ESP-Verschlüsselung | aes128-CCM | -- | -- |
| ESP-Verschlüsselung | aes192-CCM | -- | -- |
| ESP-Verschlüsselung | aes256-CCM | -- | -- |
| ESP-Verschlüsselung | aes128-GCM | -- | -- |
| ESP-Verschlüsselung | aes192-GCM | -- | -- |
| ESP-Verschlüsselung | aes256-GCM | -- | -- |
| IKE-Authentifizierung | hmac-MD5 | -- | -- |
| IKE-Authentifizierung | hmac-SHA1 | -- | -- |
| IKE-Authentifizierung | hmac-SHA256 | -- | -- |
| IKE-Authentifizierung | hmac-SHA384 | -- | -- |
| IKE-Authentifizierung | hmac-SHA512 | -- | -- |
| IKE DH-Gruppe | Group 1 (modp768) | -- | -- |
| IKE DH-Gruppe | Group 2 (modp1024) | -- | -- |
| IKE DH-Gruppe | Group 5 (mod1536) | -- | -- |
| IKE DH-Gruppe | Group 14 (modp2048) | -- | -- |
| IKE DH-Gruppe | Group 16 (modp4096) | -- | -- |
| IKE DH-Gruppe | Group 18 (modp8192) | -- | -- |

## IPsec Client

| Kategorie | Verfahren | Hexadezimal-wert | Standardmäßig aktiviert |
|---|---|---|---|
| ESP /AH-Authentifizierung | MD5 | -- | ✓ |
| ESP /AH-Authentifizierung | SHA1 | -- | ✓ |
| ESP /AH-Authentifizierung | SHA256 | -- | ✓ |
| ESP /AH-Authentifizierung | SHA384 | -- | ✓ |
| ESP /AH-Authentifizierung | SHA512 | -- | ✓ |

| Kategorie | Verfahren | Hexadezimal-wert | Standardmä-ßig aktiviert |
|---|---|---|---|
| ESP-Verschlüsselung | 3des-168-cbc | -- | ✓ |
| ESP-Verschlüsselung | aes128-cbc | -- | ✓ |
| ESP-Verschlüsselung | aes192-cbc | -- | ✓ |
| ESP-Verschlüsselung | aes256-cbc | -- | ✓ |
| ESP-Verschlüsselung | aes128-ctr | -- | ✓ |
| ESP-Verschlüsselung | aes192-ctr | -- | ✓ |
| ESP-Verschlüsselung | aes256-ctr | -- | ✓ |
| ESP-Verschlüsselung | aes128-CCM | -- | ✓ |
| ESP-Verschlüsselung | aes192-CCM | -- | ✓ |
| ESP-Verschlüsselung | aes256-CCM | -- | ✓ |
| ESP-Verschlüsselung | aes128-GCM | -- | ✓ |
| ESP-Verschlüsselung | aes192-GCM | -- | ✓ |
| ESP-Verschlüsselung | aes256-GCM | -- | ✓ |
| IKE-Authentifizierung | hmac-MD5 | -- | ✓ |
| IKE-Authentifizierung | hmac-SHA1 | -- | ✓ |
| IKE-Authentifizierung | hmac-SHA256 | -- | ✓ |
| IKE-Authentifizierung | hmac-SHA384 | -- | ✓ |
| IKE-Authentifizierung | hmac-SHA512 | -- | ✓ |
| IKE DH-Gruppe | Group 1 (modp768) | -- | ✓ |
| IKE DH-Gruppe | Group 2 (modp1024) | -- | ✓ |
| IKE DH-Gruppe | Group 5 (mod1536) | -- | ✓ |
| IKE DH-Gruppe | Group 14 (modp2048) | -- | ✓ |
| IKE DH-Gruppe | Group 16 (modp4096) | -- | ✓ |
| IKE DH-Gruppe | Group 18 (modp8192) | -- | ✓ |

# Index


## A

Abmeldung
  automatisch, 252
Aging
  Dynamic MAC Aging, 353
Auf Werkseinstellungen zurücksetzen, 448
Aufstellungsort, 185, 307
Authentifizierung, 223

## B

Backup, 300
Basic Wizard
  starten, 104
Benutzergruppen, 393
Bestellnummer, 133
BFP, 440
Bridge, 162, 356
  Bridge Priority, 162, 356
  Root Bridge, 162, 356
Bridge Max Age, 162, 356
Bridge Max Hop Count, 162
Brute Force Prevention, 440

## C

CA-Zertifikat, 86
Certificates, 404
CLP, 260, 264
CoS (Class of Service), 69
CoS-Priorisierung, 69

## D

DCP Discovery, 267
DCP-Server, 180
Dead Peer Detection, 90
Device
  System, 183
DHCP
  Client, 285
Dokumentation im Internet, 11
DSL
  Übersicht, 152
DST
  Sommerzeit, 234, 236

## E

Ereignisse, 210
eSIM, 325

## F

Fehlerstatus, 141
Fehlerüberwachung
  SIM-Karte, 259
  Verbindungszustandsänderung, 257
Forward Delay, 162, 356

## G

geografische Koordinaten, 185
Gerät
  Basic Wizard, 106
Gerät zurücksetzen, 448
Gerätezertifikat, 86
Glossar, 15
GPS-Position ermitteln, 307
Gruppen, 393

## H

Hardwareausgabestand, 133
Hello Time, 162, 356
Hersteller, 133
Herstellerkennung, 133
HTTP
  Server, 179
HTTPS
  Server, 179

## I

ICMP, 75
Information
  ARP-Tabelle, 134
  DSL, 152
  Gruppen, 173
  Hardware, 131
  IPsec VPN, 157

IPv6-Nachbarschaftstabelle, 135
LLDP, 144
Log Table, 136, 140
Mobile, 148
OpenVPN Client, 160
Rolle, 172
Security, 168, 171
Security Log, 138
SHDSL, 156
SINEMA RC, 158
SNMP, 144
Software, 131
Spanning Tree, 163
Startseite, 125
Systemzeit, 174
Versions, 131
VXLAN, 173
IP-Adresse
Basic Wizard, 105
Konfiguration, 366
Vergabe über STEP 7, 64
IPsec VPN
NETMAP, 83
Source-NAT, 83
IPsec-Verfahren, 87
IPv4
VRRPv3, 97
IPv4 Routing
Routing-Tabelle, 146
IPv6
Notation, 66
IPv6 Routing
Routing-Tabelle, 147

## K

KEY-PLUG, 264
Konfigurationsmodus, 182
Konfigurieren des Netzes über Ethernet
Netze verbinden, 62

## L

Layer 2, 341
Layer 3, 264
LLDP, 144, 360
Log Table
Event Log, 136
Firewall Log, 140
Security Log, 138
Login, 440

## M

Mobile
Information, 148
Mobile Datennutzung, 152

## N

NAPT
konfigurieren, 369
NAT
1-to-1 NAT, 373
konfigurieren, 368, 387
Masquerading, 82
NAPT, 83
NAT-Traversal, 89
NETMAP, 83
Source-NAT, 83
NAT-Traversal, 89
Neustart, 187
NTP
Client, 245
Server, 251

## O

Operator
Interfaces, 322

## P

Packet Capture, 339
Passwort, 395
Optionen, 397
Ping, 266
PLUG, 55, 260, 264
Port
Portkonfiguration, 312
Projektierungshandbücher, 449
Punkt zu Punkt, 97

## R

RADIUS, 398
redundante Netzwerke, 161, 356
Reset Timer BFP, 440
RESET-Taster, 253
Rollen, 391
Root Max Age, 162, 356

Routing, 362
ICMP, 75
IPv4 Routing-Tabelle, 146
IPv6 Routing-Tabelle, 147
statische Routen, 362
RSTP, 355
Rücksetzen, 187

## S

Schnittstellen
Mobilfunk, 315
SELECT/SET-Taster, 253
Seriennummer, 133
Serverzertifikat, 86
Service & Support, 17
SFTP
Laden/Speichern, 204
SHA-Algorithmus, 226
SHDSL
Schnittstelle, 109, 334
Übersicht, 156, 333
Sicherheitseinstellungen, 226
Signal Recorder, 150
SIM
Basic Wizard, 111
Schnittstellen, 319
SIMATIC NET-Glossar, 15
SMS, 270
empfangen, 276
senden, 275, 279
SMTP
Client, 180
SNAT
konfigurieren, 371
SNMP, 72, 181, 220, 226
Gruppen, 225
SNMPv1, 72
SNMPv2c, 72
SNMPv3, 72
Trap, 230
Übersicht, 144
SNMPv3
Ansichten, 228
Benachrichtigungen, 230
Benutzer, 222
Gruppen, 225
Zugriff, 226
Softwareausgabestand, 133
Source-NAT
Masquerading, 82
Spanning Tree, 354
Information, 163
Rapid Spanning Tree, 97
Spannungsversorgung
Überwachung, 256
SSH
Server, 179
Standard-Modus, 87
Startseite, 125
Stateful Inspection Firewall, 79
Subnetz
Konfiguration, 366
Übersicht, 364
Subnetze
Konfiguration (IPv6), 384
Verbundene Subnetze (IPv6), 384
Syslog
Client, 180
System
Allgemeine Informationen, 183
Device, 183
Konfiguration, 176
Load and Save via HTTP, 195
Systemereignisprotokoll
Agent, 254
Systemereignisse, 210
Konfiguration, 210
Severity Filter, 215
Systemhandbuch, 13
Systemzeit, 232

## T

Taster, 253
TCP-Ereignis, 304
Telnet
Server, 179
TFTP
Laden/Speichern, 200
Training, 17
Trigger-Intervall BFP, 440

## U

Uhrzeit
GPS- und Mobilfunkgerät, 239
manuelle Einstellung, 116, 233
NTP-Client, 117
SIMATIC Time Client, 249
SNTP (Simple Network Time Protocol), 241
Systemzeit, 116, 232

Uhrzeitsynchronisation, 241
UTC-Zeit, 244, 248
Zeitzone, 244, 248

## V

Verfügbare Systemfunktionen, 52
VLAN, 67
Port VID, 347
Priorität, 346
Tag, 346
VLAN-ID, 70
VLAN-Tag, 68
Voraussetzung
ADSL-Anschluss, 45
Antenne, 40, 42, 44
SHDSL-Anschluss, 46
SIM-Karte, 41, 43, 44
Spannungsversorgung, 41, 43, 44, 45, 46
VPN-Verbindung
Status, 157
Status OpenVPN-Client, 160
VRRP
VRRPv3 Adressenkonfiguration (IPv4), 380
VRRPv3 Adressenübersicht (IPv4), 379
VRRPv3 Konfiguration (IPv4), 378
VRRPv3 Router (IPv4), 375
VRRPv3
Backup-Router, 97
Master-Router, 97
Schnittstellenüberwachung, 381
Virtueller Router, 97
VRRPv3-Router, 97
VRRPv3-Statistik, 166
VXLAN, 173

## W

Wartungsdaten, 133
Web Based Management, 99
Voraussetzung, 99
Werkseinstellung, 448
Werksseitige Voreinstellung, 448

## Z

Zeiteinstellung, 181