SIEMENS

SIMATIC NET

Industrial Ethernet Security SCALANCE S615 Web Based Management

Projektierungshandbuch

Vorwort

Beschreibung 1

Security-Empfehlung 2

Technische Grundlagen 3

Konfigurieren mit dem Web Based Management 4

Instandhalten und Warten 5

Anhang A

01/2019

C79000-G8900-C388-07

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
Division Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

Dokument-Bestellnummer: C79000-G8900-C388
℗ 01/2019 Änderungen vorbehalten

Copyright © Siemens AG 2015 - 2019.
Alle Rechte vorbehalten

Vorwort

Gültigkeitsbereich

Dieses Projektierungshandbuch behandelt das folgende Produkt:

- SCALANCE S615

Das Projektierungshandbuch gilt für folgende Softwareversion:

- SCALANCE S615 Firmware ab Version V 6.1

Zweck dieses Projektierungshandbuchs

Dieses Projektierungshandbuch soll Sie in die Lage versetzen das Gerät in Betrieb zu nehmen und zu bedienen. Es vermittelt die notwendigen Kenntnisse über die Konfiguration der Geräte.

Einordnung in die Dokumentationslandschaft

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

- Projektierungshandbuch: SCALANCE S615 Command Line Interface

  Dieses Dokument enthält die CLI-Befehle, die von SCALANCE S615-Geräten unterstützt werden.

- Getting Started

  Dieses Dokument zeigt anhand von Beispielen die Projektierung des SCALANCE M800/S 615-Geräts.

- Betriebsanleitung SCALANCE S615

  Dieses Dokument finden Sie auf den Internet-Seiten des Siemens Industry Online Support. Es enthält Informationen zu Montage, Anschließen und Zulassungen des SCALANCE S615.

- 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)

SIMATIC NET-Handbücher

Die SIMATIC NET-Handbücher finden Sie auf den Internetseiten des Siemens Industry Online Support:

- über die Suchfunktion:

  Link zum Siemens Industry Online Support
  (http://support.automation.siemens.com/WW/view/de)

  Geben Sie die Beitrags-ID des jeweiligen Handbuchs als Suchbegriff ein.

- über die Navigation auf der linken Seite im Bereich "Industrielle Kommunikation":

  Link zum Bereich "Industrielle Kommunikation"
  (http://support.automation.siemens.com/WW/view/de/10805878/130000)

  Navigieren Sie zu der gewünschten Produktgruppe und nehmen Sie folgende Einstellungen vor:
  Register "Beitragsliste", Beitragstyp "Handbücher / Betriebsanleitungen"

Die Dokumente der hier relevanten SIMATIC NET-Produkte finden Sie auch auf dem Datenträger, der manchen Produkten beiliegt:

- Produkt-CD / Produkt-DVD
- SIMATIC NET Manual Collection

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.

SIMATIC NET-Glossar

Erklärungen zu vielen Fachbegriffen, die in dieser Dokumentation vorkommen, sind im SIMATIC NET-Glossar enthalten.

Sie finden das SIMATIC NET-Glossar hier:

- SIMATIC NET Manual Collection oder Produkt-DVD

  Die DVD liegt einigen SIMATIC NET-Produkten bei.

- Im Internet unter folgender Adresse:

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

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.

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Aktualisierungen durchzuführen, sobald die entsprechenden Updates 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/industrialsecurity.

Firmware

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

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:

- M87x, M81x, M826, M804PB, S615: OSS_Scalance-M-800-S615_86.pdf

Marken

Folgende und eventuell weitere nicht mit dem Schutzrechtsvermerk ® gekennzeichnete Bezeichnungen sind eingetragene Marken der Siemens AG:

SCALANCE, SINEMA, KEY-PLUG, C-PLUG

Inhaltsverzeichnis

Vorwort 3

1 Beschreibung 13

1.1 Funktion 13

1.2 Konfigurationsbeispiele 15
1.2.1 TeleControl mit SINEMA RC 15
1.2.2 Sicherer Zugriff mit S615 17

1.3 Voraussetzungen für den Betrieb 18
1.3.1 Einsatz in einer PROFINET-Umgebung 19

1.4 Systemfunktionen 20

1.5 Mengengerüste für WBM und CLI 22

1.6 Mengengerüst für SINEMA RC 24

1.7 PLUG 25
1.7.1 C-PLUG und KEY-PLUG 25
1.7.2 PRESET-PLUG 26

2 Security-Empfehlung 27

3 Technische Grundlagen 33

3.1 Aufbau einer IPv4-Adresse 33

3.2 ICMP 35

3.3 VLAN 37
3.3.1 VLAN 37
3.3.2 VLAN-Tagging 38

3.4 SNMP 40

3.5 Security-Funktionen 43
3.5.1 Benutzerverwaltung 43
3.5.2 Firewall 45
3.5.2.1 Firewall 45
3.5.3 NAT 49
3.5.4 NAT und Firewall 50
3.5.5 Zertifikate 53
3.5.6 VPN 54
3.5.6.1 IPsec VPN 54
3.5.6.2 OpenVPN 58
3.5.6.3 VPN-Verbindungsaufbau 59

3.6 Redundanz 63
3.6.1 Spanning Tree 63
3.6.1.1 RSTP 64
3.6.2 VRRPv3 65

4 Konfigurieren mit dem Web Based Management 67

4.1 Web Based Management ... 67
4.2 Starten und anmelden ... 69
4.3 Menü "Wizard" ... 73
4.3.1 Basic Wizard ... 73
4.3.2 IP ... 74
4.3.3 Gerät ... 76
4.3.4 Zeiteinstellung ... 77
4.3.5 DDNS ... 79
4.3.6 SINEMA RC ... 81
4.3.7 Zusammenfassung ... 84
4.4 Menü "Information" ... 86
4.4.1 Startseite ... 86
4.4.2 Versionen ... 92
4.4.3 Identification & Maintenance ... 93
4.4.4 ARP-Tabelle ... 95
4.4.5 Log-Tabellen ... 96
4.4.5.1 Ereignis-Log ... 96
4.4.5.2 Security-Log ... 98
4.4.5.3 Firewall-Log ... 100
4.4.6 Fehler ... 101
4.4.7 DHCP-Server ... 102
4.4.8 SNMP ... 104
4.4.9 LLDP ... 104
4.4.10 Routing-Tabelle ... 106
4.4.11 IPsec VPN ... 107
4.4.12 SINEMA RC ... 108
4.4.13 OpenVPN-Client ... 110
4.4.14 Redundanz ... 111
4.4.14.1 Übersicht ... 111
4.4.14.2 Spanning Tree ... 113
4.4.15 VRRPv3-Statistiken ... 116
4.4.16 Security ... 118
4.4.16.1 Übersicht ... 118
4.4.16.2 Unterstützte Funktionsrechte ... 121
4.4.16.3 Rollen ... 122
4.4.16.4 Gruppen ... 123
4.5 Menü "System" ... 124
4.5.1 Konfiguration ... 124
4.5.2 Allgemein ... 128
4.5.2.1 Gerät ... 128
4.5.2.2 Koordinaten ... 130
4.5.3 Neustart ... 131
4.5.4 Laden & Speichern ... 133
4.5.4.1 Dateiliste ... 133
4.5.4.2 HTTP ... 134
4.5.4.3 TFTP ... 138
4.5.4.4 SFTP ... 142
4.5.4.5 Passwörter ... 146
4.5.5 Ereignisse ... 147
4.5.5.1 Konfiguration ... 147

4.5.5.2 Severity-Filter 151
4.5.6 SMTP-Client 152
4.5.6.1 Allgemein 152
4.5.6.2 Empfänger 155
4.5.7 SNMP 156
4.5.7.1 Allgemein 156
4.5.7.2 Traps 159
4.5.7.3 v3-Gruppen 160
4.5.7.4 v3-Benutzer 163
4.5.8 Systemzeit 165
4.5.8.1 Manuelle Einstellung 166
4.5.8.2 DST-Übersicht 168
4.5.8.3 DST-Konfiguration 170
4.5.8.4 SNTP-Client 173
4.5.8.5 NTP-Client 176
4.5.8.6 SIMATIC Time Client 180
4.5.8.7 NTP-Server 181
4.5.9 Auto-Logout 184
4.5.10 Taster 185
4.5.11 Syslog-Client 186
4.5.12 Fehlerkontrolle 187
4.5.12.1 Link Change 187
4.5.13 PLUG 190
4.5.13.1 Konfiguration 190
4.5.13.2 Lizenz 194
4.5.14 Ping 196
4.5.15 DCP Discovery 197
4.5.16 DNS 199
4.5.16.1 DNS-Client 199
4.5.16.2 DNS-Proxy 201
4.5.16.3 DDNS-Client 201
4.5.17 DHCP 203
4.5.17.1 DHCP-Client 203
4.5.17.2 DHCP-Server 205
4.5.17.3 DHCP-Optionen 208
4.5.17.4 Statische Zuordnung 210
4.5.18 cRSP / SRS 211
4.5.19 Proxy-Server 213
4.5.20 SINEMA RC 214

4.6 Menü "Schnittstellen" 219
4.6.1 Ethernet 219
4.6.1.1 Übersicht 219
4.6.1.2 Konfiguration 221
4.6.2 PPP 223
4.6.2.1 Übersicht 223
4.6.2.2 Konfiguration 225

4.7 Menü "Layer 2" 227
4.7.1 Layer 2-Konfiguration 227
4.7.2 VLAN 228
4.7.2.1 Allgemein 228
4.7.2.2 Port-basiertes VLAN 232

4.7.3 Dynamic MAC Aging ... 234
4.7.4 Spanning Tree ... 235
4.7.4.1 Allgemein ... 235
4.7.4.2 ST Allgemein ... 236
4.7.4.3 ST-Port ... 237
4.7.5 LLDP ... 241

4.8 Menü "Layer 3" ... 243
4.8.1 Statische Routen ... 243
4.8.2 Subnetze ... 245
4.8.2.1 Übersicht ... 245
4.8.2.2 Konfiguration ... 248
4.8.3 NAT ... 250
4.8.3.1 Masquerading ... 250
4.8.3.2 NAPT ... 250
4.8.3.3 Source-NAT ... 253
4.8.3.4 NETMAP ... 255
4.8.4 VRRPv3 ... 258
4.8.4.1 Router ... 258
4.8.4.2 Konfiguration ... 261
4.8.4.3 Adressübersicht ... 264
4.8.4.4 Adresskonfiguration ... 265
4.8.4.5 Schnittstellenüberwachung ... 266

4.9 Menü "Security" ... 268
4.9.1 Benutzer ... 268
4.9.1.1 Lokale Benutzer ... 268
4.9.1.2 Rollen ... 271
4.9.1.3 Gruppen ... 274
4.9.2 Passwörter ... 276
4.9.3 AAA ... 277
4.9.3.1 Allgemein ... 277
4.9.3.2 RADIUS-Client ... 278
4.9.4 Zertifikate ... 282
4.9.4.1 Übersicht ... 282
4.9.4.2 Zertifikate ... 283
4.9.5 Firewall ... 286
4.9.5.1 Allgemein ... 286
4.9.5.2 Vordefinierte IPv4-Regeln ... 287
4.9.5.3 Benutzerspezifisch ... 289
4.9.5.4 IP-Dienste ... 291
4.9.5.5 ICMP-Dienste ... 292
4.9.5.6 IP-Protokolle ... 293
4.9.5.7 IP-Regeln ... 294
4.9.6 IPsec VPN ... 297
4.9.6.1 Allgemein ... 297
4.9.6.2 Remote-Endpunkt ... 298
4.9.6.3 Verbindungen ... 300
4.9.6.4 Authentifizierung ... 303
4.9.6.5 Phase 1 ... 304
4.9.6.6 Phase 2 ... 307
4.9.7 OpenVPN Client ... 309
4.9.7.1 Allgemein ... 309

4.9.7.2 Verbindungen 310
4.9.7.3 Remote 312
4.9.7.4 Authentifizierung 313

5 Instandhalten und Warten 315

5.1 Gerätekonfiguration mit PRESET-PLUG 315

5.2 Firmware-Update über WBM nicht möglich 320

5.3 Wiederherstellen der Werkseinstellungen 322

A Anhang A 323

A.1 Format der Syslog-Meldungen 323

A.2 Parameter in Syslog-Meldungen 324

A.3 Syslog-Meldungen 326
A.3.1 Syslog-Meldungen SR7.4 336

Index 339

Beschreibung

1

1.1 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)

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)

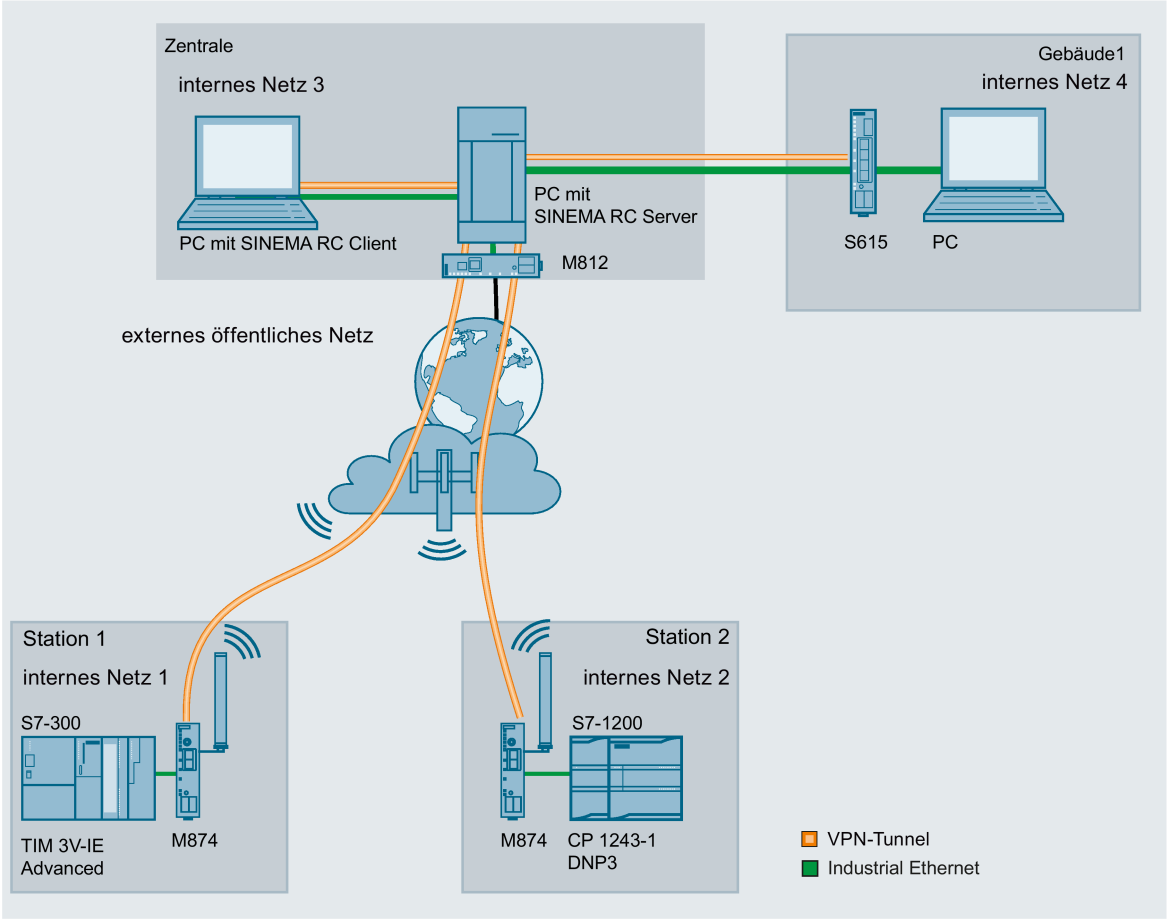
  Zur Strukturierung von Industrial Ethernet-Netzen mit stark wachsender Teilnehmeranzahl kann ein physikalisch vorhandenes Netz in mehrere virtuelle Teilnetze unterteilt werden
- Digitaler Eingang / Digitaler Ausgang
- Dynamischer DNS-Client
- DNS-Client und DNS-Proxy
- SMTP-Client
- TIA Portal Cloud Connector (SCALANCE M804PB)

1.2 Konfigurationsbeispiele

1.2.1 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 M874 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 214).
4. Richten Sie die angeschlossenen Applikationen der Anlage für die Datenkommunikation ein.

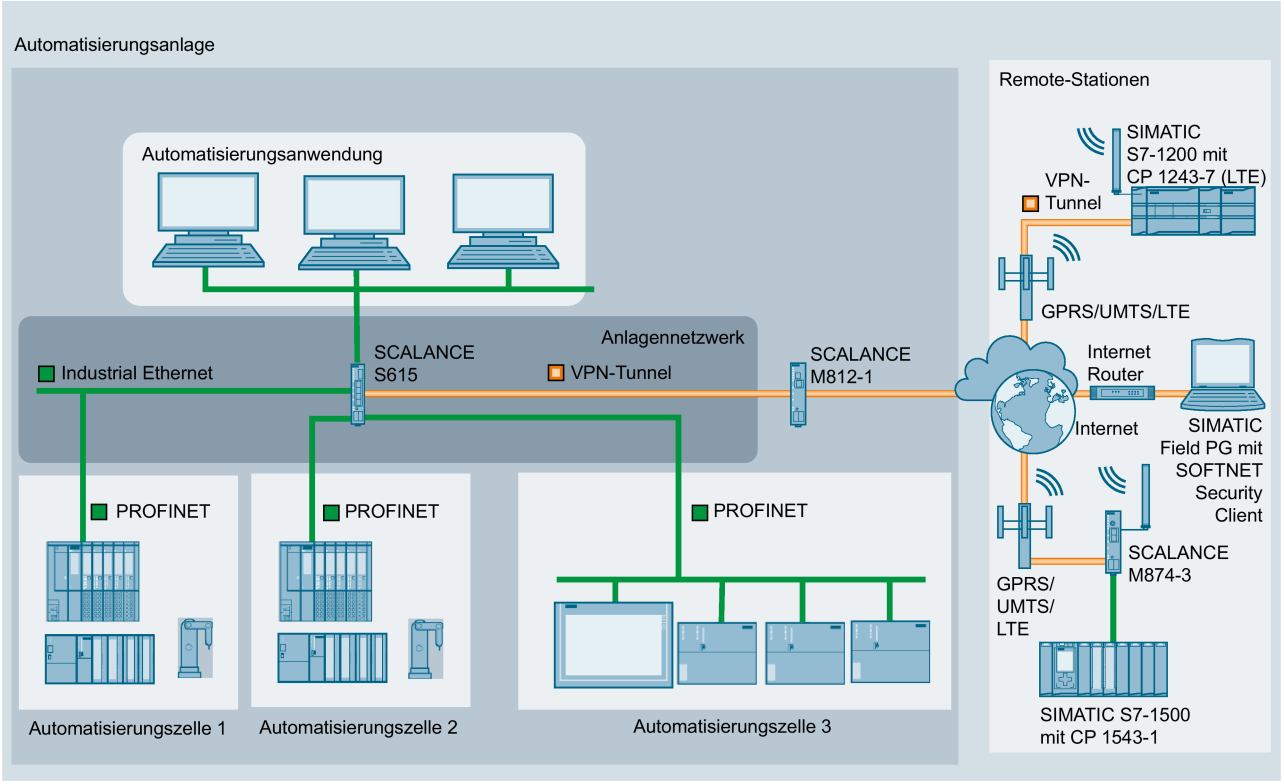
1.2.2 Sicherer Zugriff mit S615

Sicherer Fernzugriff und Netzsegmentierung mit SCALANCE S615

Zwischen einer Automatisierungsanlage und abgesetzten Stationen soll über das Internet und Mobilfunknetz eine sichere Verbindung zum Datenaustausch aufgebaut werden. Gleichzeitig soll für Servicezwecke bei Bedarf eine sichere Verbindung aufgebaut werden. Diese Verbindung wird jedoch auf ein bestimmtes Anlagenteil oder auf eine bestimmte Maschine eingeschränkt.

In der Automatisierungsanlage wird ein SCALANCE S615 über den ADSL+-Router M812-1 an das Internet angeschlossen. Die abgesetzten Stationen werden über den LTE-CP 1243-7 oder dem HSPA+-Router SCALANCE M874-3 an da Internet angeschlossen. Die Geräte stellen zum SCALANCE S615 eine VPN-Verbindung her über die Daten sicher ausgetauscht werden.

Der Servicetechniker verbindet sich bei Bedarf mit dem Internet. Mit dem SOFTNET Security Client baut er eine sichere VPN-Verbindung zum S615 auf. Am S615 sind verschiedene IP-Subnetze angeschlossen, zwischen denen die integrierte Firewall die Kommunikation kontrolliert. Damit lässt sich die Kommunikation des Servicetechnikers auf ein bestimmtes IP-Subnetz einschränken.



1.3 Voraussetzungen für den Betrieb

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 S615 für die erstmalige Konfiguration wie folgt erreichbar:

	Werkseitig voreingestellte Werte
Ethernet-Schnittstelle für die Konfiguration (Intern)	P1 ... P4 (vlan 1)
Ethernet-Schnittstelle für die Anbindung an WAN (Extern)	P5 (vlan 2)
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 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 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 67)" und bei "Starten und anmelden (Seite 69)".

1.3.1 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.

1.4 Systemfunktionen

Verfügbarkeit der Systemfunktionen

Die nachfolgende Tabelle zeigt die Verfügbarkeit der Systemfunktionen. 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 S615
Basic Wizard	IP-Einstellungen	✓
	Geräteeinstellungen	✓
	Zeiteinstellungen	✓
	SINEMA RC [1)]	✓
	DDNS	✓
Informationen	ARP-Tabelle	✓
	Log-Tabellen	✓
	VRRPv3-Statistiken	✓
	Redundanz	✓
	SINEMA RC [1)]	✓
System	SMTP-Client	✓
	SNMP	✓
	Zeiteinstellung	✓
	Automatisches Abmelden	✓
	Syslog-Client	✓
	Fehlerkontrolle	✓
	PLUG	✓
	SMS	✓
	DNS	✓
	DHCP-Client	✓
	DHCP-Server	✓
	cRSP/SRS	✓
	Proxy-Server	✓
	SINEMA RC[1)]	✓
Schnittstellen	Ethernet	✓
	PPP	✓
Layer 2	Konfiguration	✓
	VLAN	✓
	Dynamic MAC Aging	✓
	Spanning Tree	✓
	LLDP	✓

		SCALANCE S615
Layer 3	Statische Routen	✓
	Subnetze	✓
	NAT	✓
	VRRPv3	✓
Security	Benutzer	✓
	Passwörter	✓
	AAA (Authentication, Authorization, Accounting)	✓
	Zertifikate	✓
	Firewall	✓
	IPsec VPN	✓
	OpenVPN	✓

1) KEY-PLUG SINEMA Remote Connect 6GK5908-0PB00

1.5 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	Syslog-Server	3
	SMTP-Server	3
	E-Mail-Empfänger	60 20 pro SMTP-Server
	SNMPv1-Trap-Empfänger	10
	SNTP-Server	2
	NTP-Server	3 pro Layer 3-Schnittstelle 1
	DHCP-Pools	8
	IPv4-Adressen, die der DHCP-Server verwaltet (dynamisch + statisch)	100
	Statische Zuordnungen pro DHCP-Pool	20
	DHCP-Optionen (1, 2, 3, 4, 5, 6, 42, 66, 67)	9
	SINEMA RC	1
	Proxy Server	5
Layer 2	Virtuelle LANs (portbased; inklusive VLAN 1)	16
	Maximale Framegröße	2048 Bytes
Layer 3	IP-Schnittstellen	12
	Statische Routen	100
	NETMAP	256
	SourceNAT	32
	NAPT	32
	VRRPv3	VRRPv3-Instanzen (VRID): 2 Zugeordnete IP-Adressen: 1 pro VRID

	konfigurierbare Funktion	maximale Anzahl
Security	Benutzer	30 (inkl. werkseitig voreingestelltem Benutzer "admin")
	Gruppen	32
	Rollen	32 (inkl. der vordefinierten Rollen)
	RADIUS-Server	4
	Firewall	IP-Protokolle:16 IP-Dienste:32 ICMP-Dienste:16 IP-Regeln: 128 Benutzerspezifische Firewall: • Maximale Anzahl: 8 Regelsätze • Parallele Benutzerzugriffe: 4 • Maximal 128 IP-Regeln pro Firewall-Regelsatz
	IPsec VPN	20 Maximal 20 Phase 2-Verbindungen können pro Phase 1 angelegt werden.
	OpenVPN	Verbindungen: 5 Remote-Endpunkte: 25

1.6 Mengengerüst für SINEMA RC

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

Maximale Anzahl an gleichzeitig verbundenen Geräte 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 gleichzeitigen verbundenen Geräte und Benutzer: **200** miteinander kommunizierende Geräte mit je 8 Subnetzen

1.7 PLUG

1.7.1 C-PLUG und KEY-PLUG

Funktionsweise

Der C-PLUG bzw. KEY-PLUG dient dazu, im Fall eines Geräteaustausches die Konfiguration des alten Geräts auf das Neugerät zu übertragen.

ACHTUNG
C-PLUG / KEY-PLUG nicht im laufenden Betrieb ziehen oder stecken!
Ein PLUG darf nur bei ausgeschaltetem Gerät entnommen oder eingesetzt werden. 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 KEY-PLUG gesteckt, wird das Gerät nach dem Neustart in einen definierten Fehlerzustand versetzt.

Bei Start des neuen Geräts mit dem PLUG läuft dieses dann automatisch exakt mit der Konfiguration des alten Gerätes an. Ein 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.
Wenn ein falscher PLUG gesteckt wird, z. B. eines anderen Produkts oder ein beschädigter PLUG, signalisiert das Gerät mit der LED "F" einen Fehler.

Sie können den PLUG wieder entfernen oder durch die Anwahl einer entsprechenden Option den PLUG neu zu formatieren.

In Bezug auf den PLUG arbeiten Geräte in zwei Modi:

- Ohne PLUG

  Das Gerät speichert die Konfiguration auf dem internen Speicher. Dieser Modus ist aktiv, wenn kein PLUG gesteckt ist.

- Mit PLUG

  Die Konfiguration, die auf dem PLUG gespeichert ist, wird im WBM unter "Information > PLUG" angezeigt. Bei Änderungen der Konfiguration speichert das Gerät die Konfiguration direkt auf dem PLUG und auf dem internen Speicher. Dieser Modus ist aktiv, sobald ein PLUG gesteckt ist. Sobald das Gerät mit gestecktem PLUG gestartet wird, läuft das Gerät mit den Konfigurationsdaten auf dem PLUG an.

Lizenzinformation im KEY-PLUG

Der KEY-PLUG enthält zusätzlich zur Konfiguration noch eine Lizenz, die die Nutzung des Siemens Remote Services freischaltet.

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 Anbindungsfunktionalität an den SINEMA Remote Connect und zur Aufnahme von Konfigurationsdaten	6GK5908-0PB00

1.7.2 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 315).

Security-Empfehlung

2

Um nicht autorisierten Zugriff zu unterbinden, beachten Sie folgende Security-Empfehlungen.

Eine Checkliste unterstützt Sie beim Einrichten Ihres Geräts. Sie finden die Checkliste unter folgender Adresse: (https://support.industry.siemens.com/cs/ww/de/view/109745536)

Allgemein

- Stellen Sie regelmäßig sicher, dass das Gerät diese Empfehlungen und/oder andere interne Security-Richtlinien erfüllt.
- Bewerten Sie Ihre Anlage ganzheitlich im Hinblick auf Sicherheit. Nutzen Sie ein Zellenschutzkonzept mit entsprechenden Produkten:

  Link: (https://www.industry.siemens.com/topics/global/de/industrial-security/Seiten/default.aspx)
- Wenn das interne und externe Netzwerk entkoppelt sind, kann ein Angreifer nicht auf interne Daten zugreifen. Betreiben Sie das Gerät daher 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, Open VPN).
- Trennen Sie Verbindungen ordnungsgemäß (WBM, Telnet, SSH usw.).

Physischer Zugang

- Beschränken Sie den physischen Zugang zu dem Gerät auf qualifiziertes Personal. Die Speicherkarte bzw. der PLUG (C-PLUG, KEY-PLUG) enthalten sensible Daten, wie Zertifikate, Schlüssel usw., die ausgelesen und verändert werden können.
- Sperren Sie ungenutzte physische Ports auf dem Gerät. Ungenutzte Ports können verwendet werden, um unerlaubt auf die Anlage zuzugreifen.

Software (Security-Funktionen)

- Halten Sie die Software aktuell. Informieren Sie sich regelmäßig über Sicherheitsupdates des Produkts.
  Informationen hierzu finden Sie auf den Internetseiten "Industrial Security (https://www.siemens.com/industrialsecurity)".
- Informieren Sie sich regelmäßig über Security Advisories und Bulletins, die vom Siemens ProductCERT (https://www.siemens.com/cert/de/cert-security-advisories.htm)veröffentlicht werden.
- Aktivieren Sie nur Protokolle, die Sie wirklich für den Einsatz des Gerätes benötigen.

- Beschränken Sie den Zugriff auf das Management des Geräts durch Firewall-Regeln.
- Die Möglichkeit der VLAN-Strukturierung bietet guten Schutz gegen DoS-Attacken und nicht autorisierte Zugriffe. Prüfen Sie, ob dies in ihrem Umfeld sinnvoll ist.
- Nutzen Sie einen zentralen Logging-Server, um Änderungen und Zugriffe zu protokollieren. Betreiben Sie Ihren Logging-Server innerhalb des geschützten Netzwerkbereichs und prüfen Sie regelmäßig die Logging-Informationen.
- Es wird empfohlen einen nicht verwendeten PLUG zu formatieren.

Passwörter

- Definieren Sie Regeln für die Nutzung der Geräte und die Vergabe von Passwörtern.
- Aktualisieren Sie regelmäßig Passwörter und Schlüssel, um die Sicherheit zu erhöhen.
- Ändern Sie alle Standard-Passwörter für Benutzer, bevor Sie das Gerät betreiben.
- Verwenden Sie ausschließlich Passwörter mit hoher Passwortstärke. Vermeiden Sie schwache Passwörter, wie z. B. passwort1, 123456789, abcdefgh.
- Stellen Sie sicher, dass alle Passwörter geschützt und unzugänglich für unbefugtes Personal sind.
- Verwenden Sie dasselbe Passwort nicht für verschiedene Benutzer und Systeme oder nachdem es abgelaufen ist.

Schlüssel und Zertifikate

In diesem Abschnitt werden die Security-Schlüssel und -Zertifikate thematisiert, die Sie benötigen, um TLS, VPN (IPsec, OpenVPN) und SINEMA RC einzurichten.

- Im Gerät ist ein vorinstalliertes X.509-Zertifikat mit Schlüssel vorhanden. Ersetzen Sie dieses Zertifikat durch ein selbst erstelltes Zertifikat mit Schlüssel. Es wird empfohlen, ein Zertifikat zu verwenden, das entweder durch eine zuverlässige externe oder interne Zertifizierungsstelle signiert ist.
- Nutzen Sie eine Zertifizierungsstelle inklusive Schlüsselwiderruf und -verwaltung, um die Zertifikate zu signieren.
- Stellen Sie sicher, dass benutzerdefinierte private Schlüssel geschützt und unzugänglich für unbefugte Personen sind.
- Verifizieren Sie Zertifikate und Fingerprints auf Server- und Clientseite, um "Man-in-the-middle"-Angriffe zu verhindern.
- Es wird empfohlen, passwortgeschützte Zertifikate im PKCS#12-Format zu verwenden
- Es wird empfohlen, Zertifikate mit einer Schlüssellänge von mindestens 2048 Bit zu verwenden.
- Ändern Sie Schlüssel und Zertifikate umgehend, wenn der Verdacht auf Kompromittierung besteht.

Sichere/Unsichere Protokolle

- Vermeiden oder deaktivieren Sie unsichere Protokolle, wie z. B. Telnet und TFTP. Diese Protokolle sind aus historischen Gründen noch verfügbar, jedoch nicht für einen sicheren Einsatz gedacht. Setzen Sie unsichere Protokolle auf dem Gerät über eine gesicherte Verbindung (z. B. SINEMA RC) ein.
- Vermeiden oder deaktivieren Sie unsichere Protokolle. Prüfen Sie die Notwendigkeit der Nutzung folgender Protokolle:
  - Telnet
  - HTTP
  - Broadcast-Pings
  - Nicht authentifizierte und unverschlüsselte Schnittstellen
  - ICMP (redirect)
  - LLDP
  - Syslog
  - DHCP-Optionen 66/67
  - SNTP
  - NTP
  - TFTP
  - TIA Portal Cloud Connector
- 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
  - SNTP → 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).
- Nutzen Sie sichere Protokolle, wenn der Zugriff auf das Gerät nicht durch physische Schutzvorkehrungen gesichert ist.

- Um einem unbefugten Zugriff auf das Gerät bzw. Netzwerk vorzubeugen, treffen Sie angemessene Schutzvorkehrungen gegen unsichere Protokolle.
- Wenn Sie unsichere Protokolle und Dienste benötigen, aktivieren Sie diese an Schnittstellen, die sich in einem geschützten Netzwerkbereich befinden.
- 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 "DCP Read Only"-Modus.

Liste verfügbarer Protokolle

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

Dienst	Protokoll/ Portnummer	Voreingestellter Portstatus		Konfigurierbar		Authentifizierung	Verschlüsselung
		Lokaler Zugriff	Externer Zugriff [1]	Dienst	Port		
DHCP-Client	UDP/68	Geschlossen	Geschlossen	✓	--	--	--
DHCP-Server	UDP/67	Geschlossen [2]	Geschlossen [3]	✓	--	--	--
DNS-Client	TCP/53 UDP/53	Nur ausgehend	Nur ausgehend	✓	--	--	--
DNS-Server	TCP/53 UDP/53	Offen [4]	Geschlossen	✓	--	--	--
DynDNS	TCP/80	Nur ausgehend	Nur ausgehend	✓	--	✓	--
HTTP	TCP/80	Offen	Geschlossen	--	--	✓	--
HTTP Proxy	TCP/80 TCP/443	Nur ausgehend	Nur ausgehend	✓	✓	Optional	--
HTTPS	TCP/443	Offen	Geschlossen	✓	--	✓	✓
IPsec/IKE	UDP/500 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 TCP/1194	Nur ausgehend	Nur ausgehend	✓	✓	✓	✓
Ping	ICMP	Offen	Geschlossen	✓	--	✓	--
PROFINET	UDP/34964	Geschlossen	Geschlossen	--	--	--	--
RADIUS Client	TCP/1812 UDP/1812	Nur ausgehend	Nur ausgehend	✓	✓	✓	--
SFTP	TCP/22	Nur ausgehend	Nur ausgehend	✓	✓	✓	✓

Dienst	Protokoll/ Portnummer	Voreingestellter Portstatus		Konfigurierbar		Authentifizierung	Verschlüsselung
		Lokaler Zugriff	Externer Zugriff [1]	Dienst	Port		
Siemens Remote Service (cRSP/SRS)	TCP/443	Nur ausgehend	Nur ausgehend	✓	--	Optional	✓
SINEMA RC	HTTPS/443 und TCP/UDP abhängig von Server-konfigurati-on	Nur ausgehend	Nur ausgehend	✓	✓	✓	✓
SMTP	TCP/25	Nur ausgehend	Nur ausgehend	✓	✓	--	--
SMTP (Secure)	TCP/465 TCP/587	Nur ausgehend	Nur ausgehend	✓	✓	Optional	✓
SNMPv1	UDP/161	Offen	Geschlossen	✓	--	--	--
SNMPv3	UDP/161	Offen	Geschlossen	✓	--	Optional	Optional
SNTP	UDP/123	Geschlossen	Geschlossen	✓	--	--	--
SSH	TCP/22	Offen	Geschlossen	✓	--	✓	✓
Syslog	UDP/514	Nur ausgehend	Nur ausgehend	✓	✓	--	--
Telnet	TCP/23	Geschlossen	Geschlossen	✓	--	✓	--
TFTP	UDP/69	Nur ausgehend	Nur ausgehend	✓	✓	--	--
TIA Portal Cloud Connector [5]	TCP/9023	Geschlossen	Geschlossen	✓	✓	--	--

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

[2] Nur beim SCALANCE M826 offen

[3] Nur beim SCALANCE S615 offen

[4] Nur beim SCALANCE S615 geschlossen

[5] Nur beim SCALANCE M804PB

Erläuterung zu der Tabelle:

- 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.

- Dienst / Port 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.

  Bei Optional ist die Authentifizierung bei Bedarf konfigurierbar.

- Verschlüsselung

  Gibt an, ob die Übertragung verschlüsselt wird.

  Bei Optional ist die Verschlüsselung bei Bedarf konfigurierbar.

Technische Grundlagen

3

3.1 Aufbau einer IPv4-Adresse

Adressklassen

IP-Adressbereich	Max. Anzahl der Netzwerke	Max. Anzahl Hosts/Netzwerk	Klasse	CIDR
1.x.x.x bis 126.x.x.x	126	16777214	A	/8
128.0.x.x bis 191.255.x.x	16383	65534	B	/16
192.0.0.x bis 223.255.255.x	2097151	254	C	/24
224.0.0.0 - 239.255.255.255	Multicast-Anwendungen		D	
240.0.0.0 - 255.255.255.255	reserviert für zukünftige Anwendungen		E	

Eine IP-Adresse besteht aus 4 Byte. Jedes Byte wird dezimal dargestellt und ist durch einen Punkt vom vorherigen getrennt. Es ergibt sich also folgender Aufbau, wobei für XXX eine Zahl zwischen 0 und 255 zu setzen ist:

XXX.XXX.XXX.XXX

Die IP-Adresse besteht aus zwei Teilen, der Netzwerkadresse und der Endteilnehmeradresse. Dadurch ist es möglich, verschiedene Teilnetze zu bilden. Abhängig davon, welche Bytes der IP-Adresse als Netzwerkadresse und welche als Endteilnehmeradresse genutzt werden, kann eine IP-Adresse einer bestimmten Adressklasse zugeordnet werden.

Subnetzmaske

Die Bits der Endteilnehmer-Adresse können für die Bildung von Subnetzen verwendet werden. Dabei stellen die führenden Bits die Adresse des Subnetzes dar, die restlichen Bits werden als Adresse des Rechners im Subnetz interpretiert.

Ein Subnetz wird durch die Subnetzmaske definiert. Der Aufbau der Subnetzmaske entspricht dem einer IP-Adresse. Ist in der Subnetzmaske an einer Bitposition eine "1" gesetzt, gehört das Bit an der entsprechenden Stelle in der IP-Adresse zur Subnetzadresse, andernfalls zur Adresse des Rechners.

Beispiel für ein Klasse B-Netz:

Die Standard-Subnetz-Adresse für Klasse B-Netze ist 255.255.0.0, es stehen also die letzten beiden Bytes für die Festlegung eines Subnetzes zur Verfügung. Wenn 16 Teilnetze definiert werden sollen, muss das dritte Byte der Subnetzadresse auf 11110000 (Binärdarstellung) gesetzt werden. In diesem Fall ergibt sich die Subnetzmaske 255.255.240.0.

Um festzustellen, ob zwei IP-Adressen zum gleichen Subnetz gehören, werden auf die beiden IP-Adressen und die Subnetzmaske eine bitweise UND-Verknüpfung angewendet.

Wenn beide Verknüpfungen das gleiche Ergebnis haben, gehören beide IP-Adressen zum gleichen Subnetz, wie z. B. 141.120.246.210 und 141.120.252.108.

Außerhalb des lokalen Netzwerks ist die beschriebene Aufteilung der Endteilnehmer-Adresse ohne Bedeutung, dort ist für die Paketvermittlung nur die IP-Adresse in ihrer Gesamtheit von Interesse.

Hinweis

In der Bit-Darstellung der Subnetzmaske müssen die "Einsen" linksbündig gesetzt sein, d. h. es dürfen keine "Nullen" zwischen den "Einsen" stehen.

3.2 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 Art der Meldung		Code 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

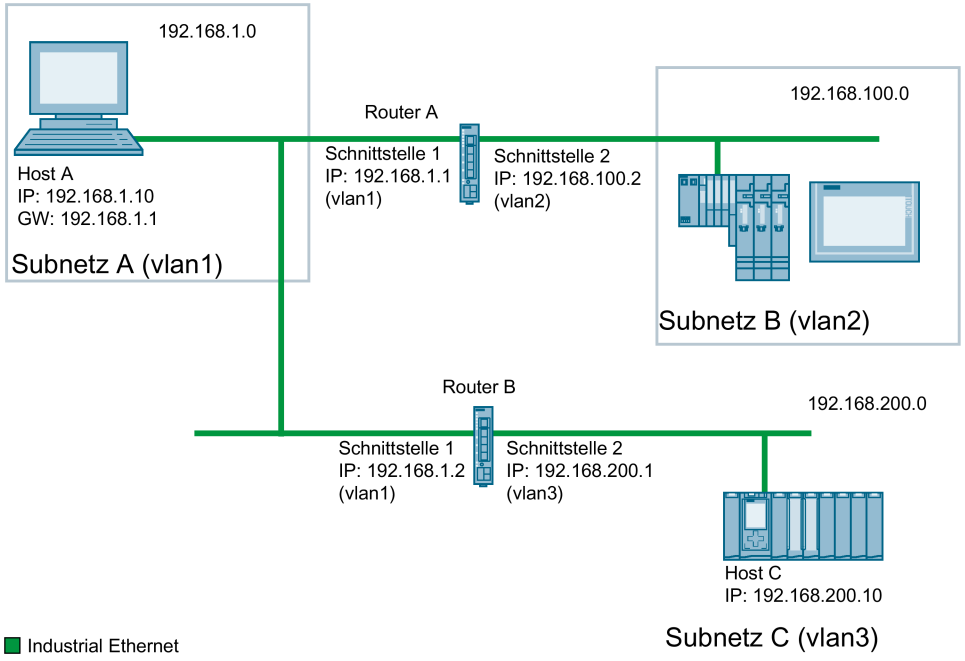
    Echo-Frage, besser bekannt als Ping.

- **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/assignments/icmp-parameters).

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.

3.3 VLAN

3.3.1 VLAN

Netzwerkdefinition unabhängig von der räumlichen Lage der Teilnehmer

VLAN (Virtuelles Local Area Network) teilt ein physikalisches Netzwerk in mehrere logische 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 38). 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 (Seite 232)".

- 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

Werkseitig sind am SCALANCE S615 folgende Zuordnungen eingestellt:

P1 bis P4	vlan1 Für den Zugriff vom lokalen Netz (LAN) auf das Gerät
P5	vlan2 Für den Zugriff vom externen Netz (WAN) zum Gerät

Die Zuordnung können Sie unter "Layer 2 > VLAN > Allgemein (Seite 228)" ändern.

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

3.3.2 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:

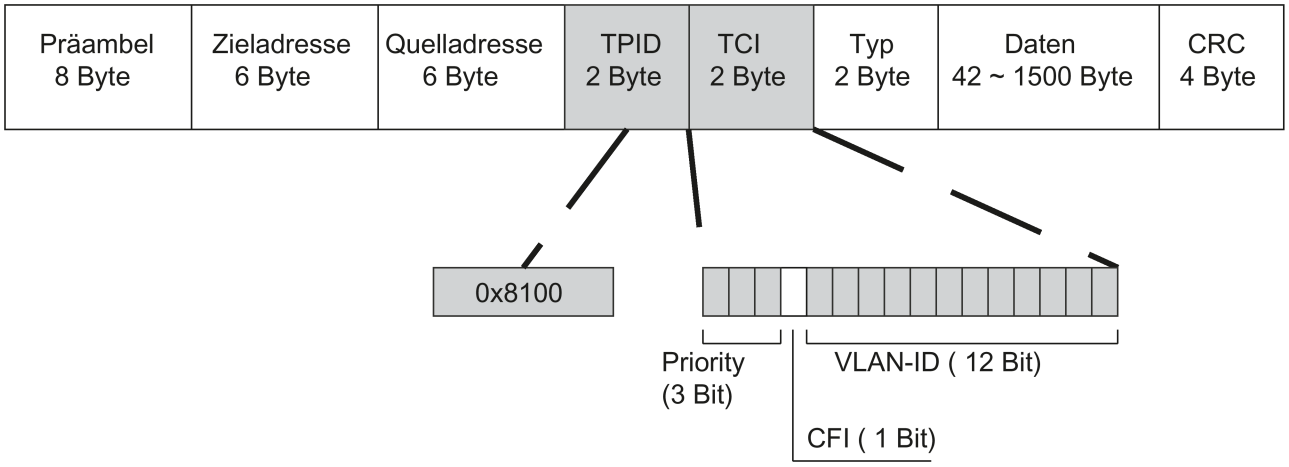


Bild 3-1 Aufbau des erweiterten Ethernet-Telegramms

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

3.4 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.

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 des Standards 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.

3.5 Security-Funktionen

3.5.1 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.

Anhängig 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.

3.5.2 Firewall

3.5.2.1 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".

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 x	vlan x	Zugriff vom IP-Subnetz vlan x auf das IP-Subnetz vlan x. Beispiel: vlan1 (INT) → vlan2 (EXT) Zugriff vom lokalen IP-Subnetz auf das externe IP-Subnetz.
	ppp2	Zugriff vom IP-Subnetz auf die WAN-Schnittstelle des Geräts.
	Gerät	Zugriff vom IP-Subnetz auf das Gerät.
	SINEMA RC	Zugriff vom IP-Subnetz auf die SINEMA RC-Verbindung.
	IPsec (all) IPsec <Connection Name> OpenVPN (all) OpenVPN <Connection Name>	Zugriff vom IP-Subnetz auf die VPN-Tunnelpartner, die über alle VPN-Verbindungen (all) oder über eine bestimmte VPN-Verbindung <Connection Name> zu erreichen sind.

von	nach	Bedeutung
Gerät	vlan x	Zugriff vom Gerät auf das IP-Subnetz.
	ppp2	Zugriff vom Gerät auf die WAN-Schnittstelle des Geräts.
	SINEMA RC	Zugriff vom Gerät auf die SINEMA RC-Verbindung.
	IPsec (all) IPsec <Connection Name> OpenVPN (all) 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 von SINEMA RC-Verbindungen auf das IP-Subnetz.
	ppp2	Zugriff vom IP-Subnetz auf die WAN-Schnittstelle des Geräts.
	Gerät	Zugriff von SINEMA RC-Verbindungen auf das Gerät.
	IPsec (all) IPsec <Connection Name> OpenVPN (all) OpenVPN <Connection Name>	Zugriff vom SINEMA RC-Server auf die VPN-Tunnelpartner, die über alle VPN-Verbindungen (all) oder über eine bestimmte VPN-Verbindung <Connection Name> zu erreichen sind.
IPsec (all) IPsec <Connection Name> OpenVPN (all) OpenVPN <Connection Name>	vlan x	Zugriff über VPN-Tunnelpartner auf das IP-Subnetz.
	ppp2	Zugriff vom IP-Subnetz auf die WAN-Schnittstelle des Geräts.
	Gerät	Zugriff über VPN-Tunnelpartner auf das Gerät.
	SINEMA RC	Zugriff über VPN-Tunnelpartner auf die SINEMA RC-Verbindung.
ppp0/usb	vlan x	Zugriff von der Mobilfunk-Schnittstelle auf das IP-Subnetz.
	Device	Zugriff von der Mobilfunk-Schnittstelle auf das Gerät.
	SINEMA RC	Zugriff von der Mobilfunk-Schnittstelle auf die SINEMA RC-Verbindung.
	IPsec (all) IPsec <Connection Name> OpenVPN (all) OpenVPN <Connection Name>	Zugriff von der Mobilfunk-Schnittstelle auf die VPN-Tunnelpartner, die über alle VPN-Verbindungen (all) oder über eine bestimmte VPN-Verbindung <Connection Name> zu erreichen sind.

Werkseinstellung der Firewall

Dienst	Zugriff	
	Lokaler Zugriff (vlan1) auf das Gerät	Externer Zugriff (vlan2) auf das Gerät [1)]
Cloud Connector (nur bei M804PB)	ja	-
DHCP	ja	ja (nur bei S615)
DNS	ja	nein
HTTP	ja	nein

Dienst	Zugriff	
	Lokaler Zugriff (vlan1) auf das Gerät	Externer Zugriff (vlan2) auf das Gerät [1]
HTTPS	ja	nein
IPsec VPN	nein	ja
Ping	ja	nein
SMS Relay (nur bei M87x)	ja	nein
SNMP	ja	nein
SSH	ja	nein
Systemzeit	ja	nein
Telnet	ja	nein

[1] SCALANCE M826 und M804PB ist im Auslieferungszustand (Werkseinstellung) nur vlan1 verfügbar.

Automatische Firewall-Regeln

Bei folgenden Funktionen werden automatisch Firewall-Regeln angelegt:

- System > SINEMA RC
- Security > IPsec VPN> Phase 2
- Security > OpenVPN Client> Verbindungen

SINEMA RC

- Telegramme von intern nach extern sind zugelassen.
- Telegramme von extern nach intern sind zugelassen.
- Folgende Telegramme von extern an das Gerät sind zugelassen:
  - ICMP-Echo-Request
  - SSH
  - HTTPS

IPsec VPN

- Telegramme von intern nach extern sind zugelassen.
- Telegramme von extern nach intern sind zugelassen.
- ICMP-Echo-Request von extern an das Gerät sind zugelassen.

OpenVPN Client

- Telegramme von intern nach extern sind zugelassen.
- Telegramme von extern nach intern sind zugelassen.
- Telegramme von dem Gerät nach extern sind zugelassen.
- ICMP-Echo-Request von extern an das Gerät sind zugelassen.

3.5.3 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 250)".

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 250)".

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 253)".

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 255)".

3.5.4 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-Schnittstelle**	**Ziel-Schnittstelle**	**Quell-IP-Subnetz**	**Quell-IP-Subnetzumsetzung**	**Ziel-IP-Subnetz**	**Ziel-IP-Subnetzumsetzung**
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. 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. 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. 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. 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. 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. 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.

3.5.5 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. 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 303)
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
Gerätezertifikat	Zertifikate mit dem privaten Schlüssel (Key file), mit denen sich das Gerät ausweist.	IPsec VPN (Seite 303)
Gegenstellenzertifikat	Zertifikate, mit denen sich das VPN-Gateway der Gegenstelle bei dem Gerät authentifiziert.	IPsec VPN (Seite 303)

Dateitypen

Dateityp	Beschreibung
*.crt	Datei, die das Zertifikat enthält.
*.p12	Bei der PKCS12-Zertifikatsdatei wird der private Schlüssel mit dem zugehörigen Zertifikat passwortgeschützt gespeichert. 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.

3.5.6 VPN

Das Gerät unterstützt folgende VPN-Systeme

- IPsec VPN
- OpenVPN

3.5.6.1 IPsec VPN

Die IPsec-Verbindungen konfigurieren Sie unter "Security" > "IPsec VPN (Seite 297)"

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 authentisieren 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	Schl□üsselableitung	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

Kombination			Phase 1		Phase 2	
Verschlüsselung	**Authentifizierung**	**Schlüsselableitung**	**IKEv1**	**IKEv2**	**IKEv1**	**IKEv2**
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.

3.5.6.2 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 309)".

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.

Authentifizierungsverfahren

- 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 authentisieren und digitale Signaturen zu erzeugen.

- Benutzername/Passwort

  Der Zugang wird über einen Benutzernamen und ein Passwort beschränkt.

Verschlüsselungsverfahren

Das Gerät unterstützt dabei die folgenden Verfahren:

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

3.5.6.3 VPN-Verbindungsaufbau

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

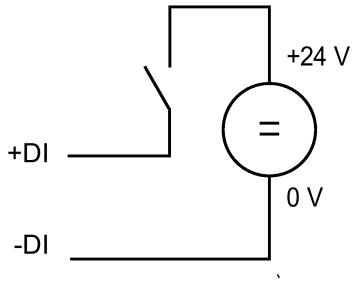
- OpenVPN: Security > OpenVPN > Verbindungen (Seite 310)
- IPsec VPN: Security > IPsec VPN > Verbindungen (Seite 300)
- SINEMA RC: System > SINEMA RC (Seite 214)

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 eine Verbindung zu einer Gegenstelle herzustellen. Die Annahme von Anfragen zum VPN-Verbindungsaufbau ist ebenfalls möglich. 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	-	
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 aufrecht erhalten.

[1] Für SCALANCE S615: 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" 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.

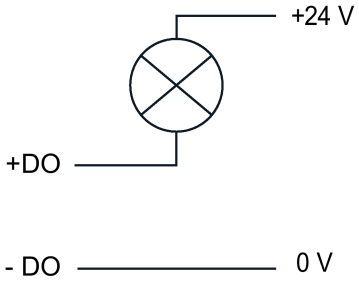
- Bei DI warten

  Wenn das Ereignis "Digitaler Eingang" eintritt, ist das Gerät "passiv". Das Gerät wartet, bis der Verbindungsaufbau von der Gegenstelle initiiert wird.

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 147)" mehrere Möglichkeiten der Benachrichtigung.

Art der Benachrichti-gung	Digital In	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. Voraussetzung: • Ein SMTP-Server ist eingerichtet. • 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. Voraussetzung: • Unter "System > Konfiguration" ist "SNMPv1 Traps" aktiviert. • 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. Voraussetzung: • Ein Syslog-Server ist eingerichtet. • 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 Benachrichti-gung	Digital In	VPN Tunnel	Verhalten bei Statusänderung
Digitaler Ein-gang	x	x	Steuert den digitalen Ausgang an oder signalisiert die Zustandsänderung mit der LED "DO". An dem digitalen Ausgang kann ein Verbraucher angeschlossen werden. Informationen zum Anschließen finden Sie in der Betriebsanleitung der Geräte. Der Verbraucher signalisiert eine Statusänderung.  **Hinweis** 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.
Status aus der MIB-Variable auslesen	x	-	Über die private MIB-Variable snMspsDigitalInputLevel können Sie den Status des digitalen Eingangs auslesen: • OID der privaten MIB-Variable snMspsDigitalInputLevel: `iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).siemens(4329).industrialComProducts(20).iComPlatforms(1).simaticNet(1).snMsps(1).snMspsCommon(1).snMspsDigitalIO(39).snMspsDigitalIOObjects(1).snMspsDigitalInputTable(2).snMspsDigitalInputEntry(1).snMspsDigitalInputLevel(6)` • Werte der MIB-Variable – 1: Signal 0 am digitalen Eingang (DI) – 2: Signal 1 am digitalen Eingang (DI)

3.6 Redundanz

3.6.1 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.

3.6.1.1 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.

3.6.2 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 wird 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".

Konfigurieren mit dem Web Based Management 4

4.1 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 (Seite 18)".
- 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" "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:
  - Microsoft Internet Explorer 11

    Hinweis

    Kompatibilitätsansicht

    Deaktivieren Sie im Microsoft Internet Explorer die Kompatibilitätsansicht, damit eine korrekte Darstellung gewährleistet ist und die einwandfreie Konfiguration über das WBM möglich ist.

  - Mozilla Firefox 57
  - Google Chrome V62

4.2 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 die IP-Adresse oder die URL des Geräts ein.

   Standardmäßig ist der Zugriff über HTTPS aktiviert. Wenn Sie über HTTP auf das Gerät zugreifen, wird die Adresse automatisch auf HTTPS umgeleitet.

   Eine Meldung zum Sicherheitszertifikat erscheint. Quittieren Sie diese Meldung und setzen Sie das Laden der Seite fort.

   Hinweis

   Informationen zum Sicherheitszertifikat

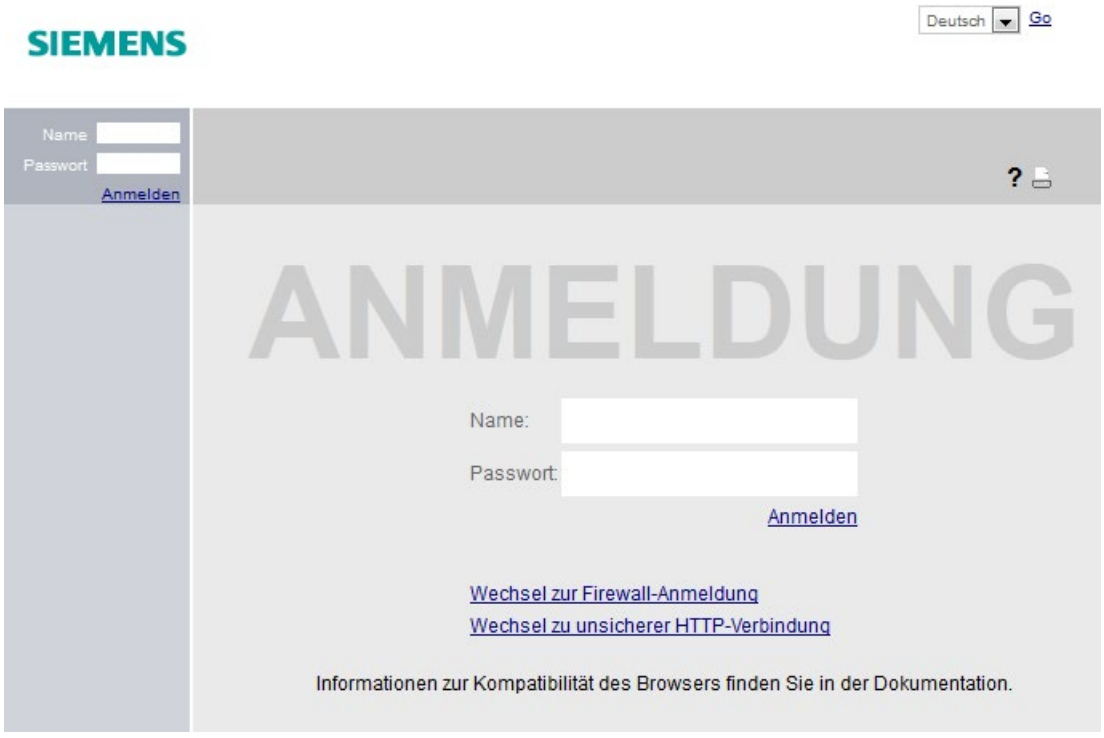
   Da das Gerät nur über verschlüsselte Zugänge administrierbar ist, wird es mit einem selbst unterzeichneten Zertifikat ausgeliefert. Bei Zertifikaten mit Unterschriften, die dem Betriebssystem nicht bekannt sind, erscheint ein Sicherheitshinweis. Sie können sich das Zertifikat anzeigen lassen.

3. Wenn eine Verbindung zum Gerät besteht, erscheint die Anmeldeseite des Web Based Managements (WBM).

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

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.



Standard-Anmeldeseite

Unter "System > Konfiguration > Standard-Anmeldeseite" können Sie festlegen welche Anmeldeseite standardmäßig geöffnet wird.

Über die Links "Wechsel zur..." können Sie die Art der Anmeldung wechseln.

Um sich anzumelden, gibt es folgende Möglichkeiten:

- Anmeldemöglichkeit in der Mitte des Browser-Fensters.
- Anmeldemöglichkeit im linken oberen Bereich des Browser-Fensters.

Am WBM anmelden

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 § und 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 dem Primary Setup Tool oder mit "DCP Discovery" zwar gelesen, aber nicht mehr geändert werden.

Wenn Sie sich erfolgreich angemeldet haben, erscheint die Startseite.

An der WBM-Seite für benutzerspezifische 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 "Benutzerdefinierte Firewall".

Vorgehensweise

1. Wenn nicht standardmäßig die Anmeldeseite für die benutzerspezifische 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".

   Nach erfolgreicher Anmeldung öffnet sich die WBM-Seite "Benutzerdefinierte Firewall-Informationen". Der aktuelle Regelsatz und die verbleibende Zeit wird angezeigt. Bei Bedarf kann der Benutzer die Zugriffszeit über die Schaltfläche "Timeout zurücksetzen" verlängern.

4.3 Menü "Wizard"

4.3.1 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.

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.
- 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 18)".

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:

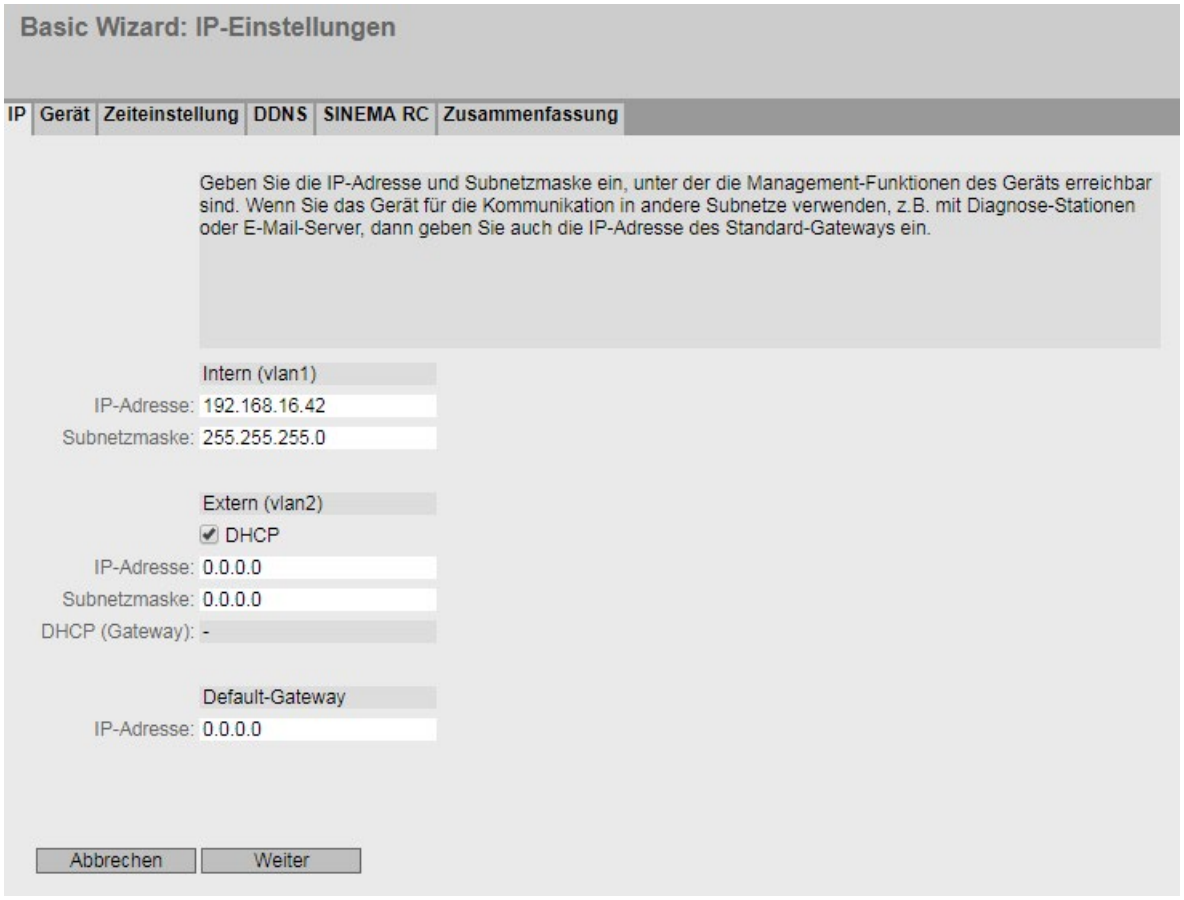
Schaltfläche	Beschreibung
Weiter	Geht zur nächsten Seite
Zurück	Geht zur vorherigen Seite zurück
Abbrechen	Der Basic Wizard wird ohne Übernahme der Einstellungen beendet.
Einstellungen übernehmen	Speichert die Konfiguration und beendet den Basic Wizard.

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

4.3.2 IP

Einleitung

Zu den grundlegenden Konfigurationsschritten für ein Gerät gehört das Festlegen der IPv4-Adresse. Mit der IP-Adresse wird ein Gerät im Netz eindeutig identifiziert.



Beschreibung

Die Basic Wizard-Seite enthält folgende Felder:

- **Intern (vlan1)**

  In diesem Bereich legen Sie die Einstellungen für Anbindung an das LAN fest.

  - **IP-Adresse**

    Geben Sie die IPv4-Adresse der Schnittstelle ein, die innerhalb Ihres Netzes eindeutig ist.

  - **Subnetzmaske**

    Geben Sie die Subnetzmaske des zu erstellenden Subnetzes ein.

- **Extern (vlan2)**

  In diesem Bereich legen Sie die Einstellungen für Anbindung an das WAN fest.

  - **DHCP**

    Wenn aktiviert, dann erhält die Schnittstelle die IPv4-Adresse von einem DHCP-Server.

  - **IP-Adresse**

    Geben Sie die IPv4-Adresse der Schnittstelle ein.

  - **Subnetzmaske**

    Geben Sie die Subnetzmaske des zu erstellenden Subnetzes ein. Subnetze an unterschiedlichen Schnittstellen dürfen sich nicht überlappen.

  - **DHCP (Gateway)**

    Wenn der DHCP-Server eine IP-Adresse für ein Gateway übermittelt, wird dieser hier angezeigt.

- **Neuen Gateway anlegen**

  In diesem Bereich legen Sie das Gateway fest.

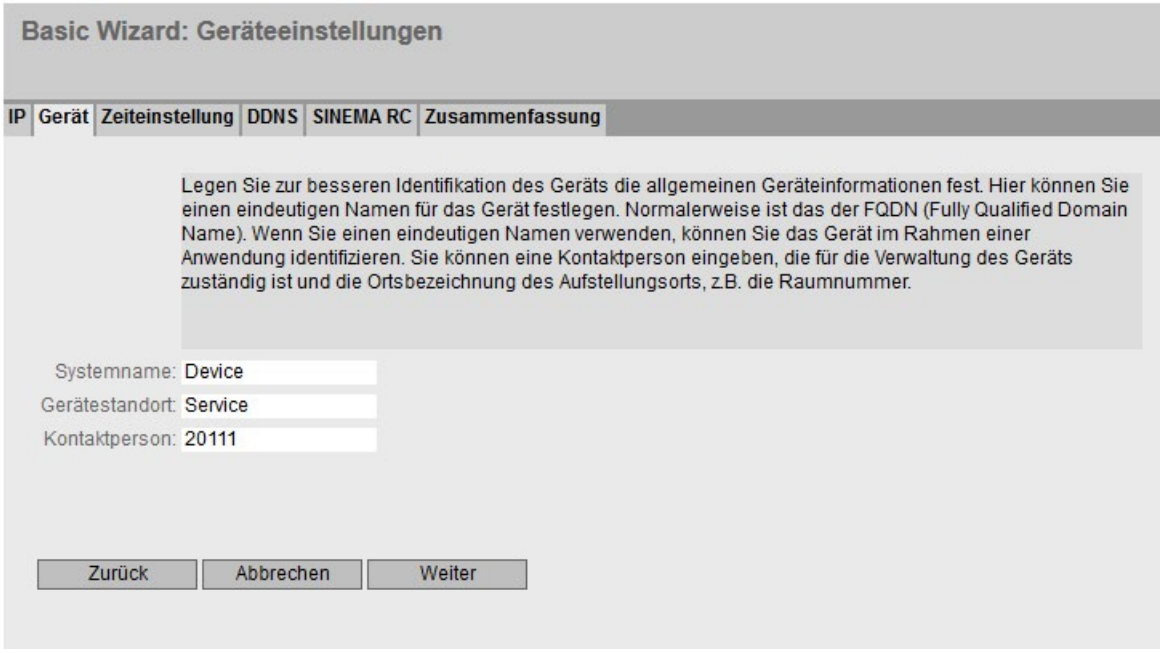
  - **IP-Adresse**

    Geben Sie die IP-Adresse des Default-Gateways ein, um mit Geräten in einem anderen Subnetz zu kommunizieren.

4.3.3 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.

4.3.4 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 (gesichert)**
  Wenn aktiviert, erhält das Gerät die Systemzeit von einem gesicherten NTP-Server. Die Einstellung gilt für alle Severeinträge.

  Um den gesicherten NTP-Client zu aktivieren, 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.

4.3.5 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**

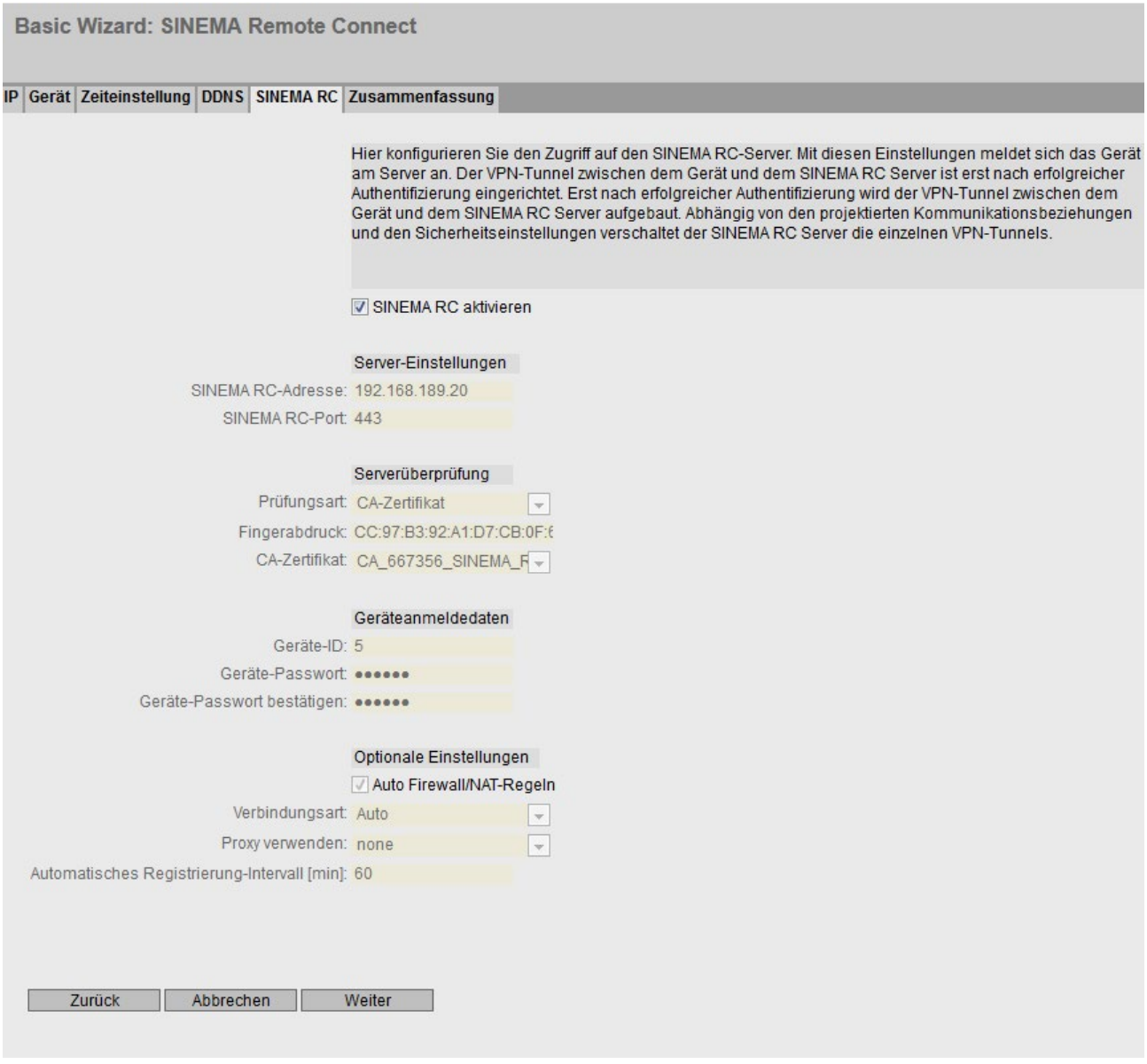
  Bestätigen Sie das Passwort.

4.3.6 SINEMA RC

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

Hinweis

Diese Funktion ist nur mit KEY PLUG (Seite 25) nutzbar.



Beschreibung

Die Basic Wizard-Seite enthält folgende Felder:

- **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 DNS-Hostnamen 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.

  - 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.

  - Digitaler Eingang

    Die Einstellungen des SINEMA RC-Servers werden ignoriert. Beim Eintreten des Ereignisses "Digitaler Eingang" 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".

- **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 Anfragen prüft das Gerät, ob auf dem SINEMA RC Server eine neuere Firmware-Datei vorhanden ist.

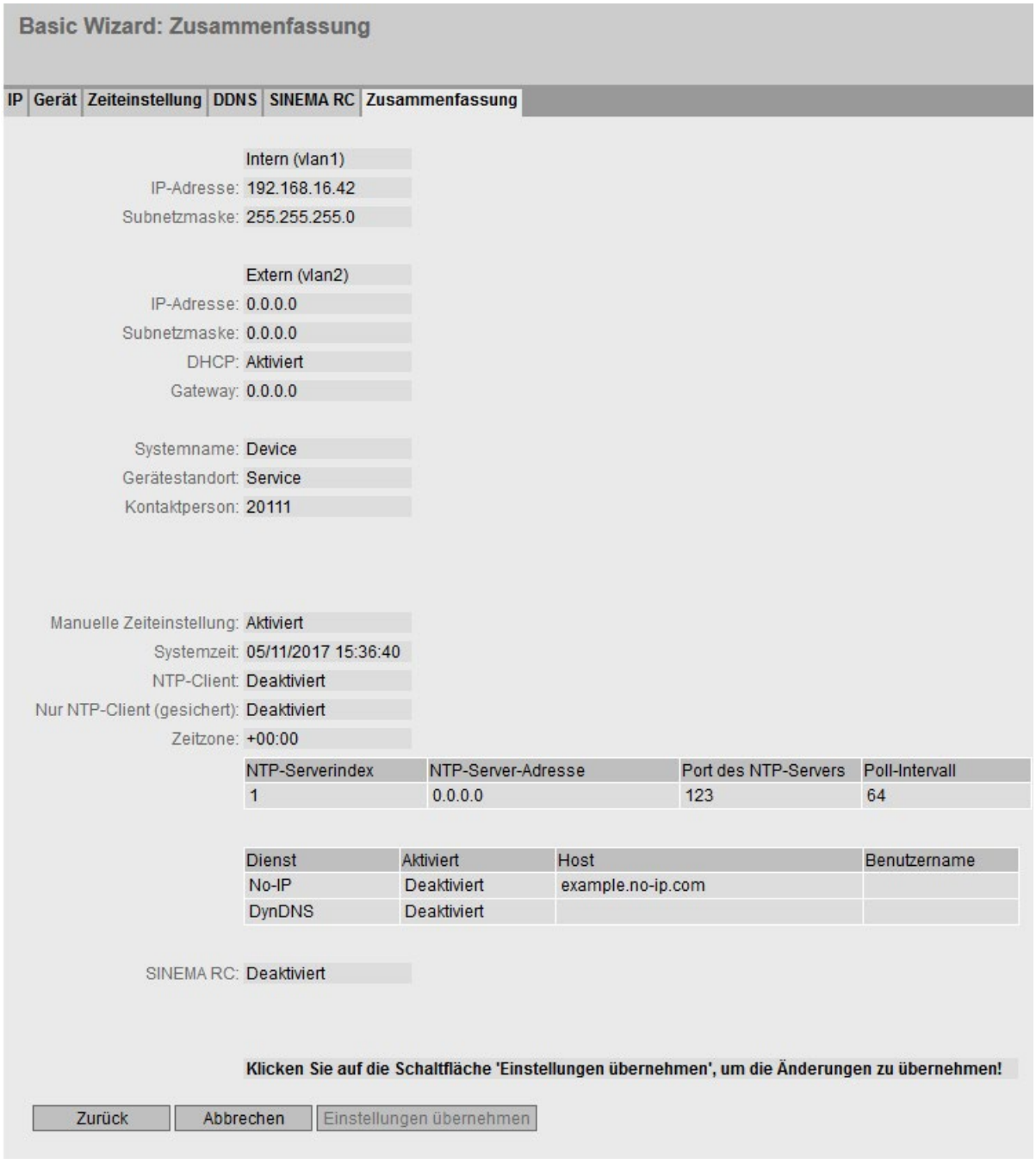
  Wenn Sie den Wert 0 eintragen, ist diese Funktion deaktiviert.

4.3.7 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.



Einstellungen übernehmen

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

4.4 Menü "Information"

4.4.1 Startseite

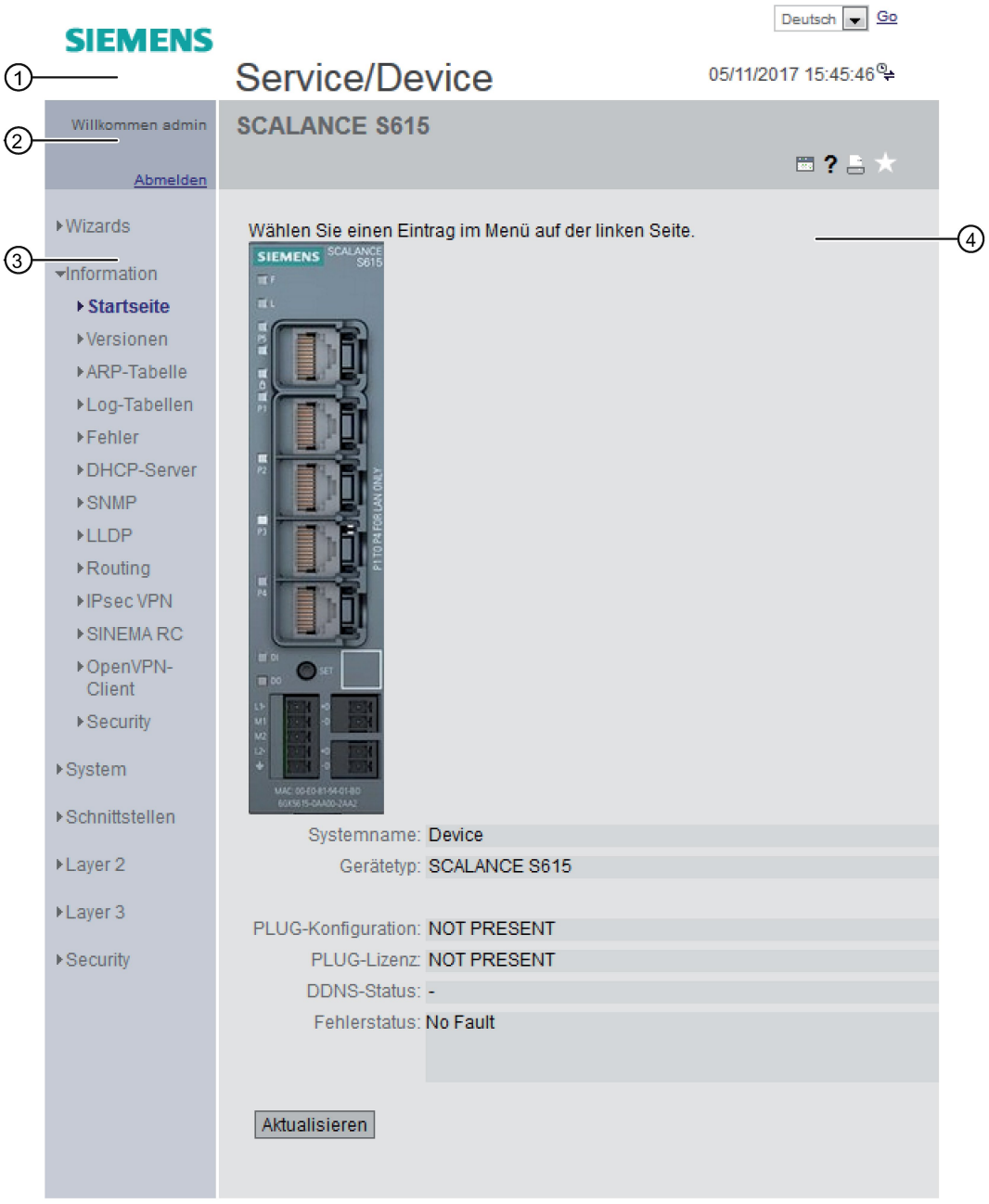
Ansicht der Startseite

Wenn Sie die IP-Adresse des Gerätes eingeben, dann wird Ihnen nach erfolgreicher Anmeldung die Startseite angezeigt.

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



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.

  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 zur Verfügung. Klicken Sie die einzelnen Menüs an, um sich die Untermenüs anzeigen zu lassen. Die Untermenüs enthalten Seiten, aus denen man Informationen entnehmen kann oder mit denen Sie Konfigurationen vornehmen können. Diese Seiten werden immer im Inhaltsbereich angezeigt.

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): Signalstärke der Verbindung

- 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.

4.4.2 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:

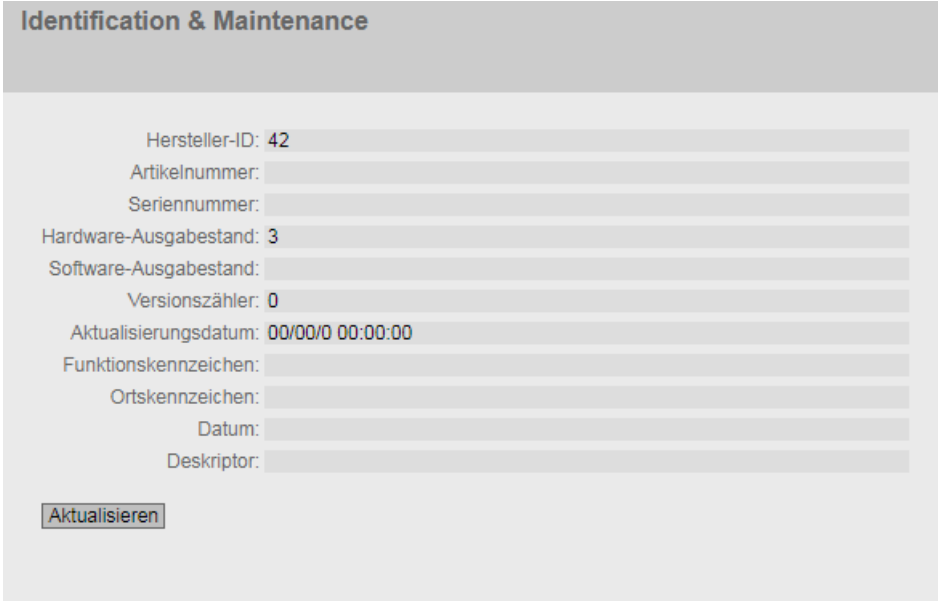
- **Hardware**
  - Basic Device
    Zeigt das Grundgerät an
- **Name**
  Zeigt den Namen des Geräts.
- **Ausgabestand**
  Zeigt den Hardware-Ausgabestand des Geräts an.
- **Artikelnummer**
  Zeigt die Artikelnummer des Geräts an.

- **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.

4.4.3 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

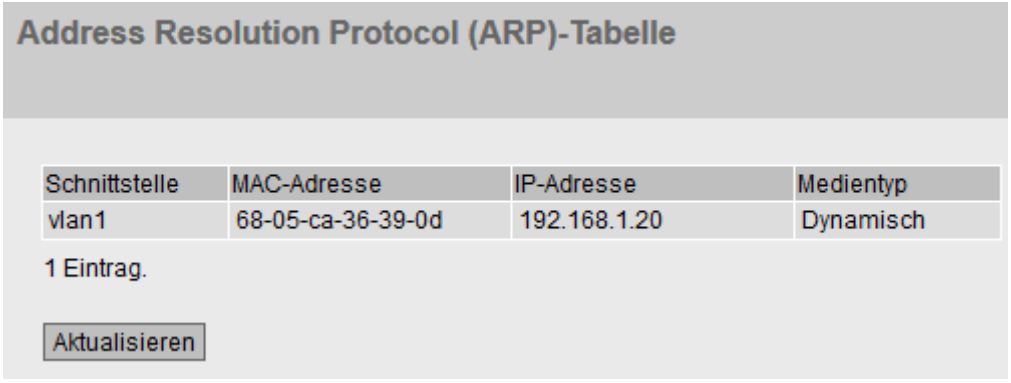
Die Tabelle gliedert sich in folgende Zeilen:

- **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.

4.4.4 ARP-Tabelle

Zuordnung von MAC-Adresse und IP-Adresse

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



Beschreibung

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.

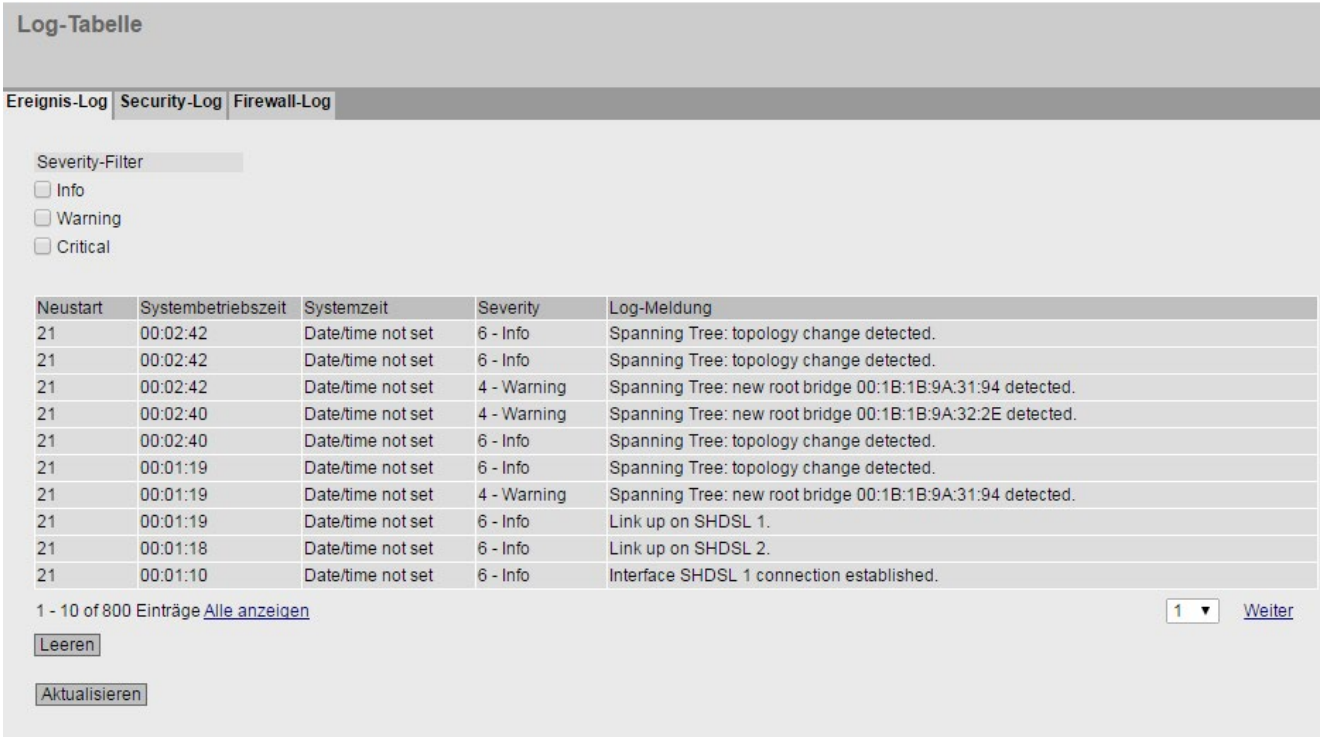
4.4.5 Log-Tabellen

4.4.5.1 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 400 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.

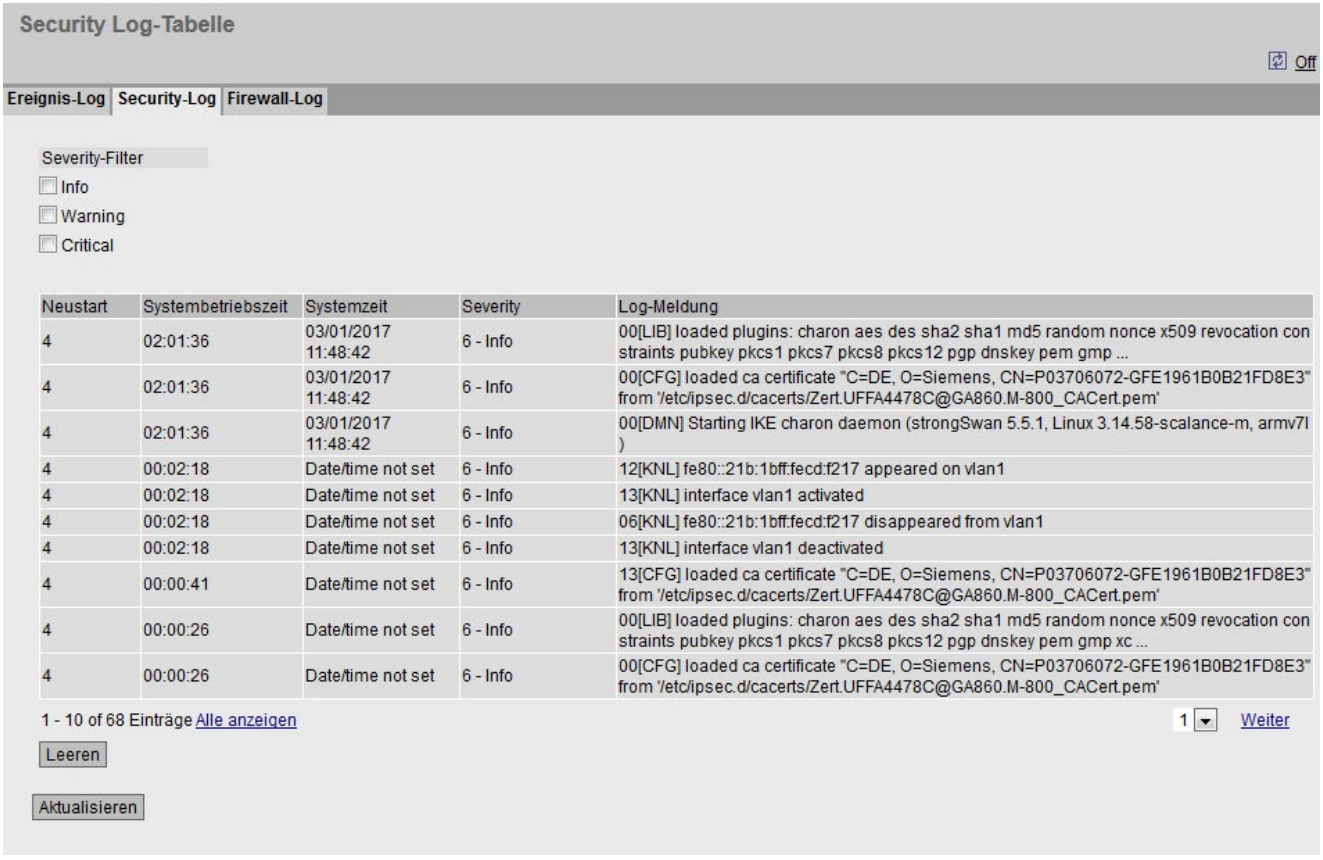
Die Tabelle gliedert sich in folgende Spalten:

- **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.

4.4.5.2 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 400 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.

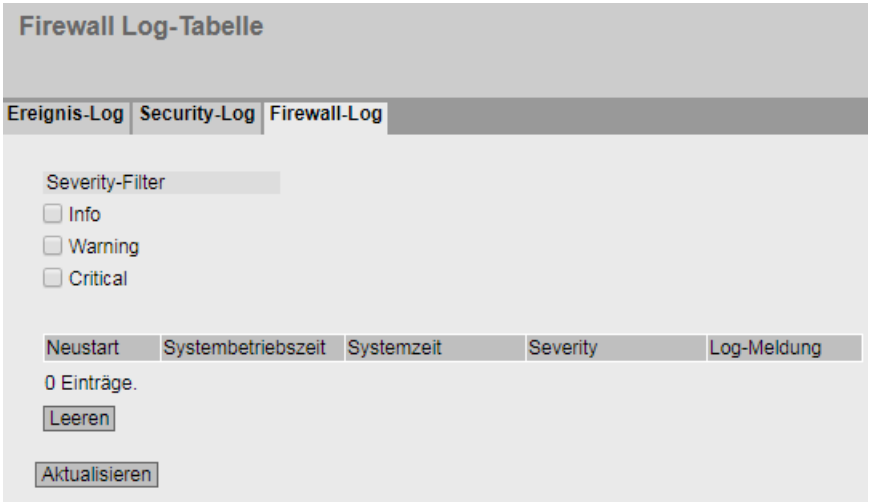
Die Tabelle gliedert sich in folgende Spalten:

- **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.

4.4.5.3 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 400 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.

4.4.6 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.

- **Schaltfläche Zähler zurücksetzen**

  Über die Schaltfläche wird die Anzahl zurückgesetzt. Der Zähler wird durch einen Neustart zurückgesetzt.

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.

4.4.7 DHCP-Server

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

  – Remote-ID

    Zeigt die Remote-ID des DHCP-Clients an.

  – Circuit-ID

    Zeigt die Circuit-ID des DHCP-Clients an.

  – DUID

    Zeigt die DUID des DHCP-Clients an.

- **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.

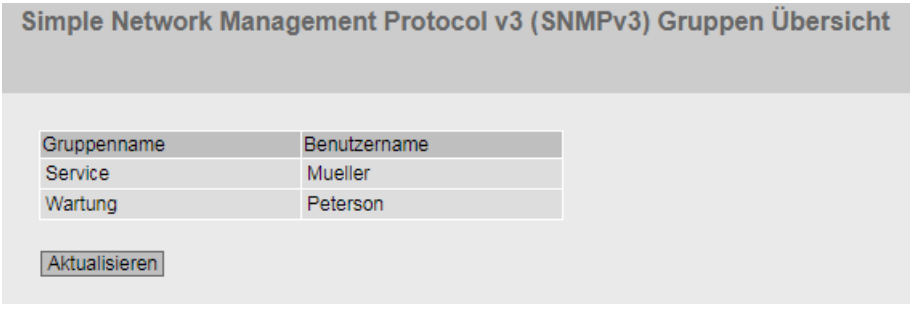
  – Wird geprüft
    Die Zuordnung wird geprüft.

  – 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.

4.4.8 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.

4.4.9 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**

  Zeigt den Systemnamen des angeschlossenen Geräts an.

- **Geräte-ID**

  Zeigt die Gerätekennung des angeschlossenen Geräts an. Die Geräte-ID entspricht dem Gerätenamen, der über PST (STEP 7) vergeben wird. Wenn kein Gerätename vergeben ist, wird die MAC-Adresse des Geräts angezeigt.

- **Lokale Schnittstelle**

  Zeigt den Port an, an dem das Gerät die Informationen empfangen hat.

- **Speicherzeit**

  Ein Eintrag bleibt für die hier angegebene Zeit im Gerät gespeichert. Wenn der IE-Switch 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**

  Zeigt den Port des Geräts an, der mit dem das Gerät verbunden ist.

4.4.10 Routing-Tabelle

Einleitung

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



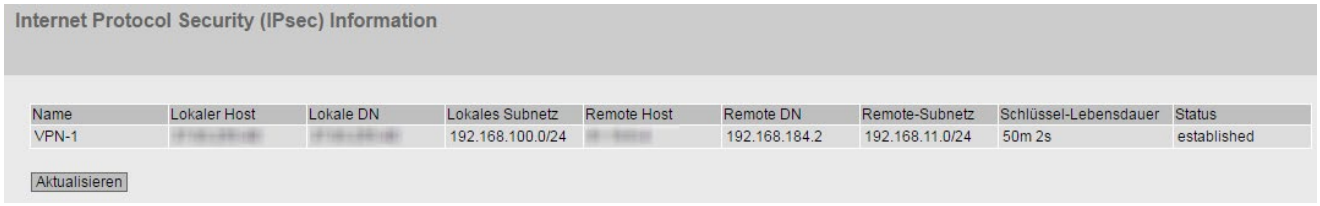
Beschreibung

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

4.4.11 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**

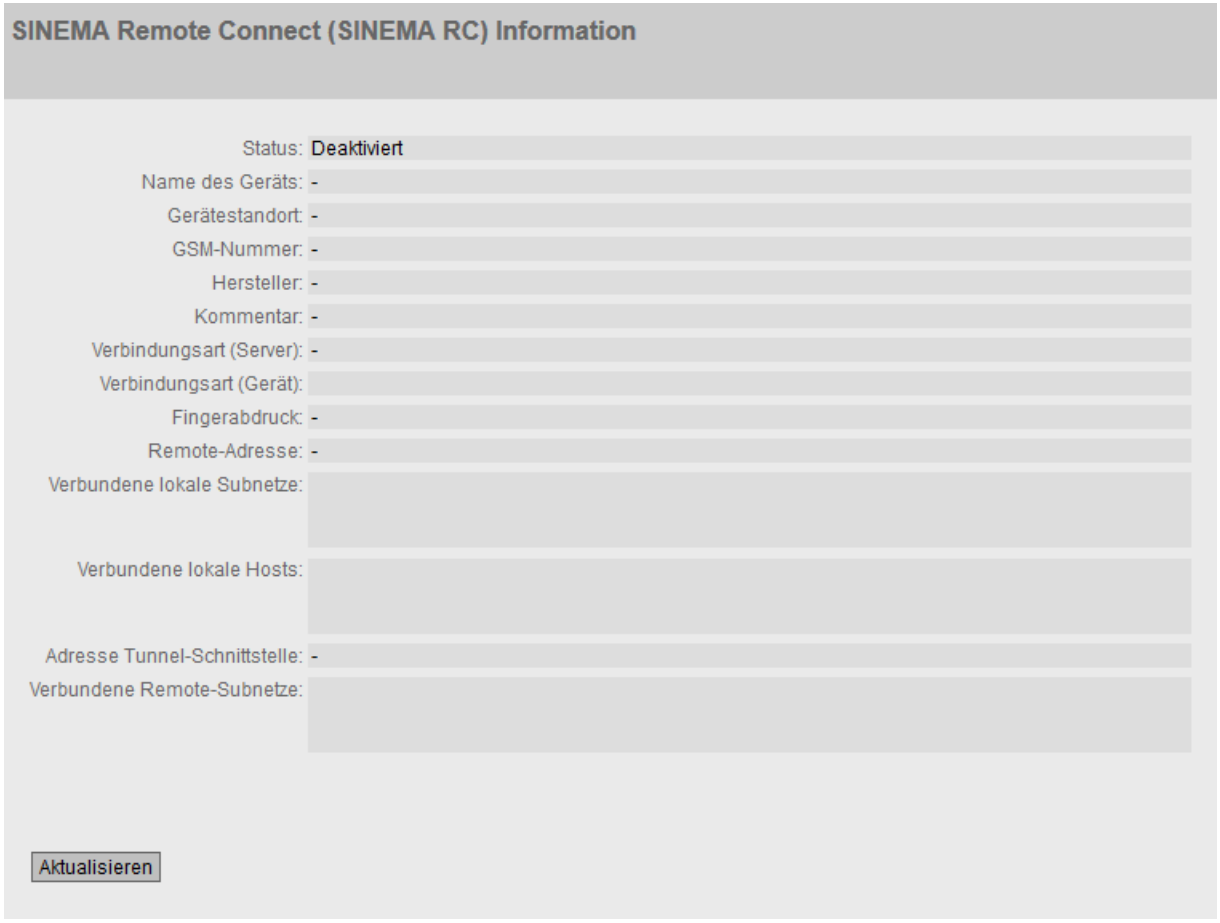
  Zeigt den Status der VPN-Verbindung an.

4.4.12 SINEMA RC

Zeigt Informationen zum SINEMARC-Server an.

Hinweis

Diese Funktion ist nur mit KEY PLUG nutzbar.



Beschreibung der angezeigten Werte

- **Status**

  Zeigt den Status der Verbindung 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.

4.4.13 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.

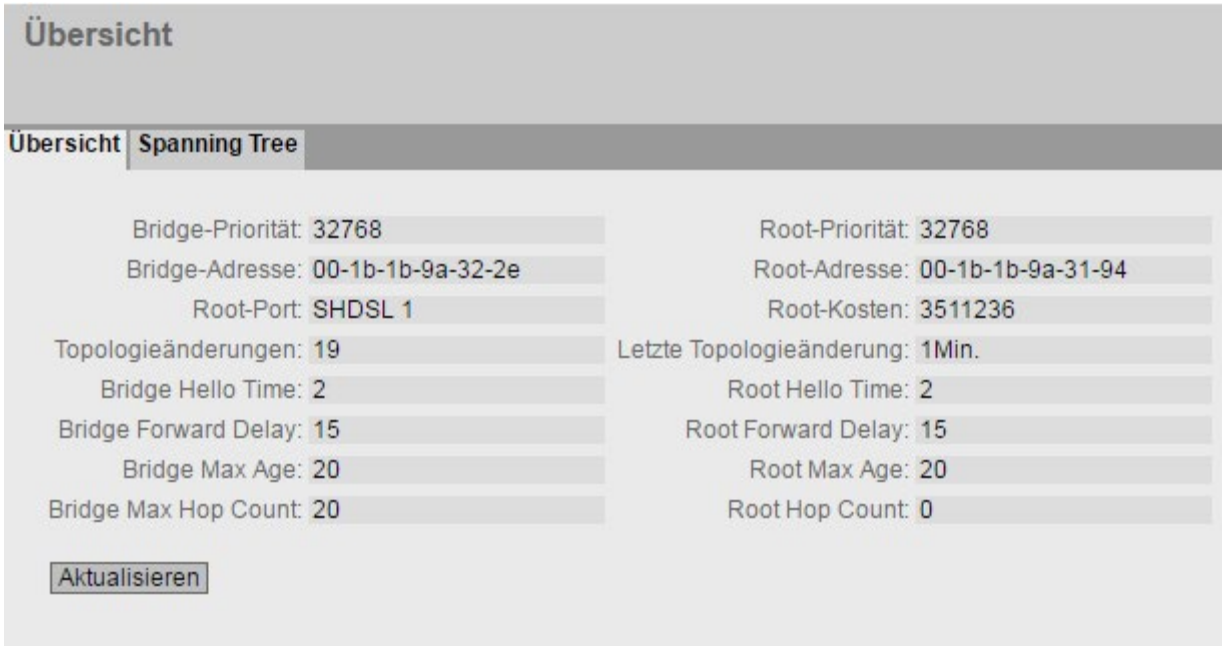
4.4.14 Redundanz

4.4.14.1 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.

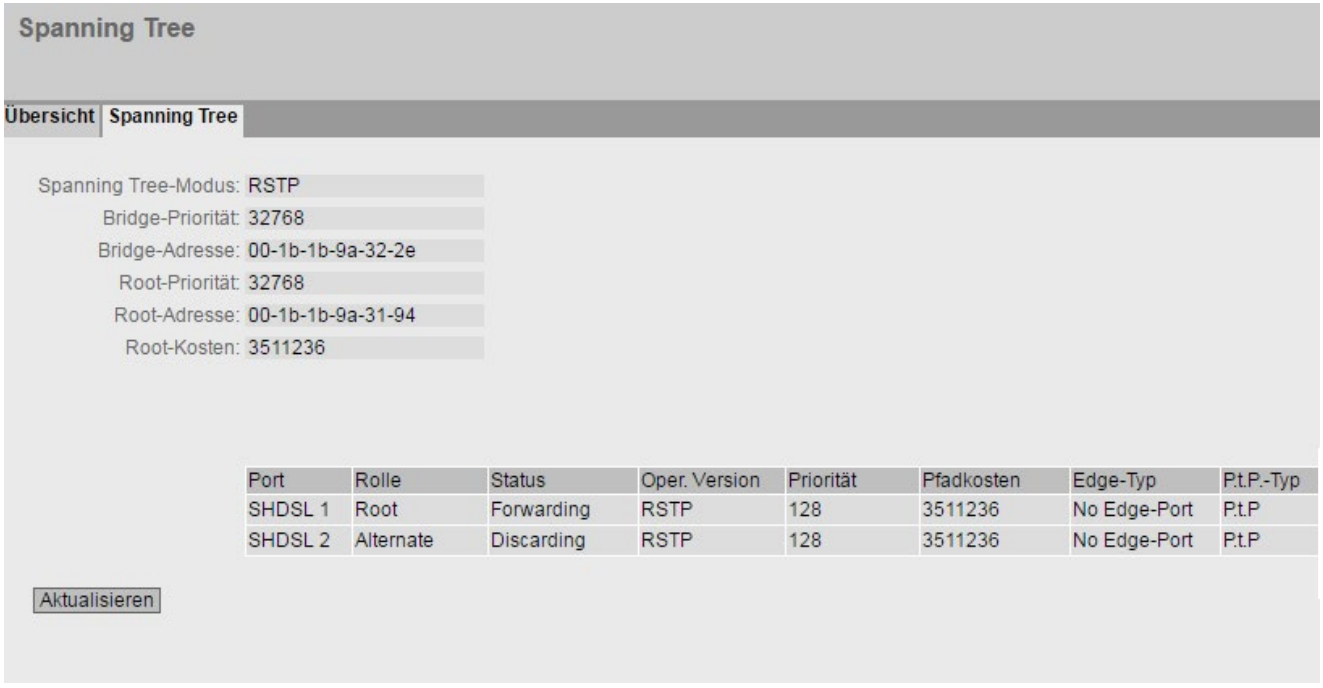
- **Root-Port**
  Zeigt den Port an, über den der Switch mit der Root-Bridge kommuniziert.
- **Root-Kosten**
  Die Pfadkosten von diesem Gerät bis zur Root-Bridge
- **Topologieänderungen / Letzte Topologieänderung**
  Die Angabe für das Gerät nennt die Zahl der Umkonfigurationen aufgrund des Spanning 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.

4.4.14.2 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.
  Ist der Wert im Feld "Cost Calc" "0", so wird der automatisch ermittelte Wert angezeigt. Im anderen Fall wird der Wert des Feldes "Cost Calc" 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
- **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. Type**
  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.

4.4.15 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 unterstütze 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**

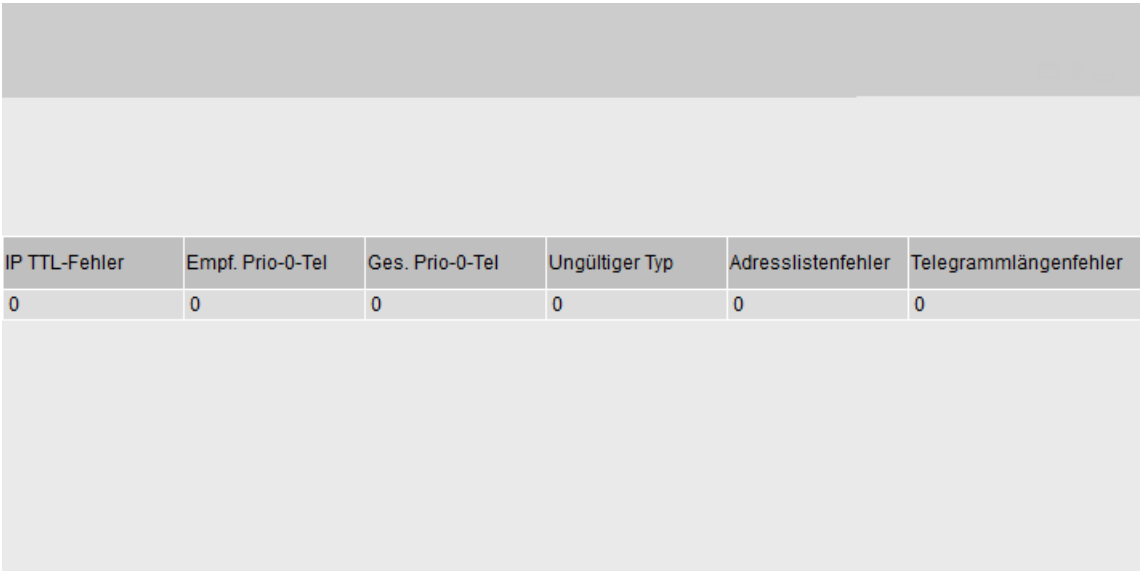
  Zeigt an, wie häufig dieser virtuelle Router in den Zustand "Master" ging.

- **Empf. Advertisements**

  Zeigt an, wie viele VRRPv3-Paket 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.

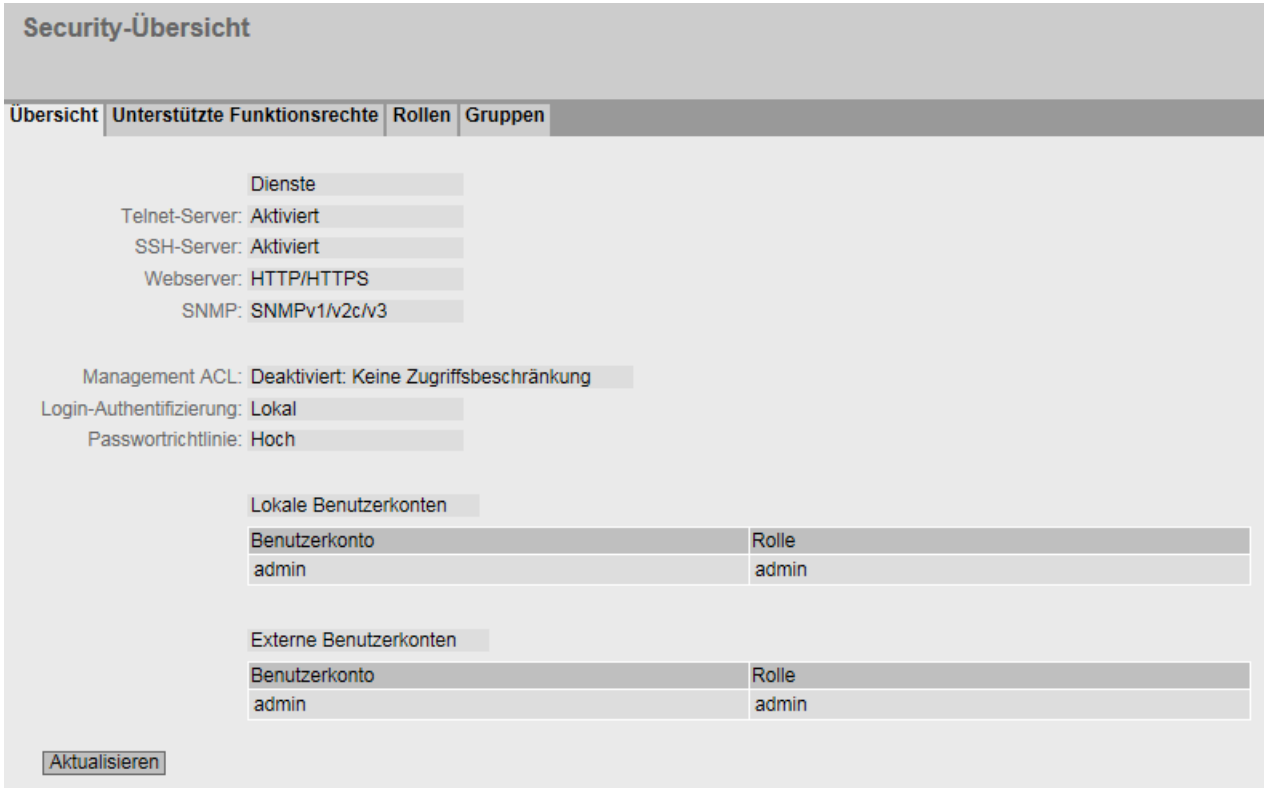
4.4.16 Security

4.4.16.1 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

- **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.

- **Management ACL**

  Einstellung konfigurieren Sie unter "Security > Management ACL"

  – Aktiviert: Nur eingeschränkter Zugriff: Der Zugang wird über eine Access Control List (ACL) eingeschränkt.

  – Deaktiviert: Keine Zugriffsbeschränkung: Management ACL ist nicht aktiviert.

  – Aktiviert: Keine Zugriffsbeschränkung: Management ACL ist aktiviert, aber der Zugang wird nicht über eine Access Control List (ACL) eingeschränkt.

- **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 mit 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.

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.

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

- **Benutzerkonto**

  Zeigt den Namen des lokalen Benutzers an.

- **Rolle**

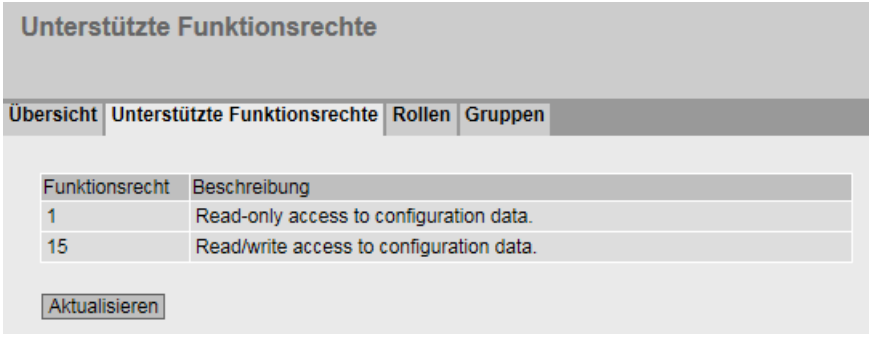
  Zeigt die Rolle des Benutzers an. Weitere Informationen zu den Funktionsrechten der Rolle erhalten Sie unter "Information > Security > Rollen".

4.4.16.2 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**

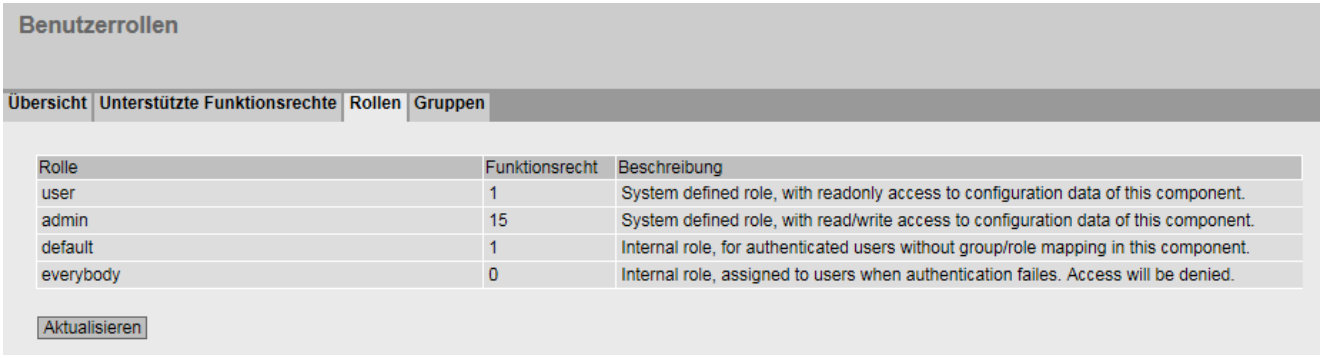
  Zeigt die Beschreibung des Funktionsrechts an.

4.4.16.3 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**

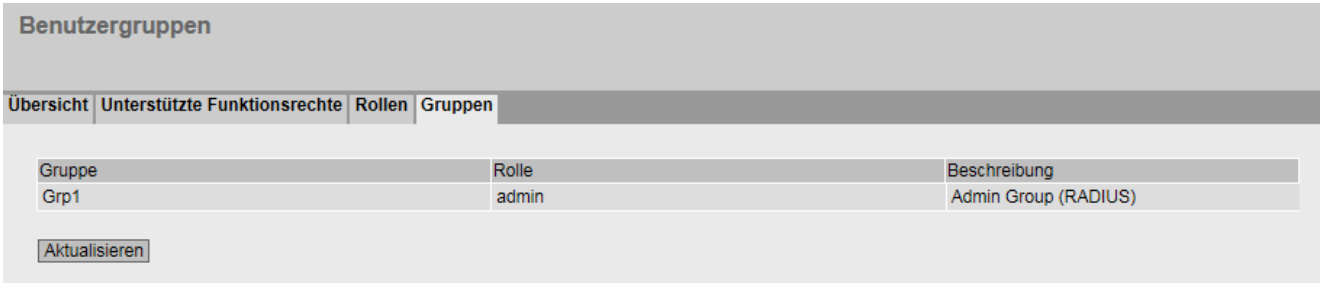
  Zeigt eine Beschreibung der Rolle an.

4.4.16.4 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.

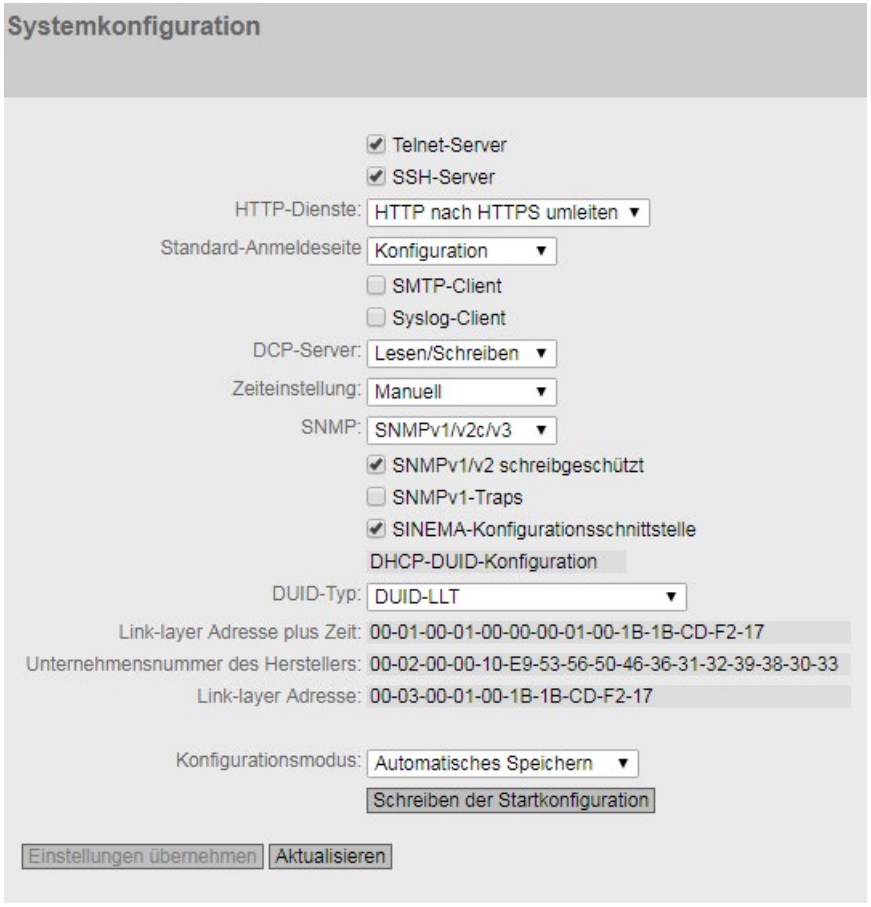
4.5 Menü "System"

4.5.1 Konfiguration

Systemkonfiguration

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

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



Beschreibung

Die Seite enthält folgende Felder:

- **Telnet-Server**
  Aktivieren oder deaktivieren Sie den Dienst Telnet-Server für den unverschlüsselten Zugriff auf das CLI.
- **SSH-Server**
  Aktivieren oder deaktivieren Sie den Dienst SSH-Server für den verschlüsselten Zugriff auf das CLI.
- **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.
- **Standard-Anmeldeseite**

  Legen Sie fest, mit welcher Anmeldeseite das WBM standardmäßig startet.

  – Firewall

    Anmelden an der WBM-Seite für benutzerspezifische 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.

- **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-Type**

  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.

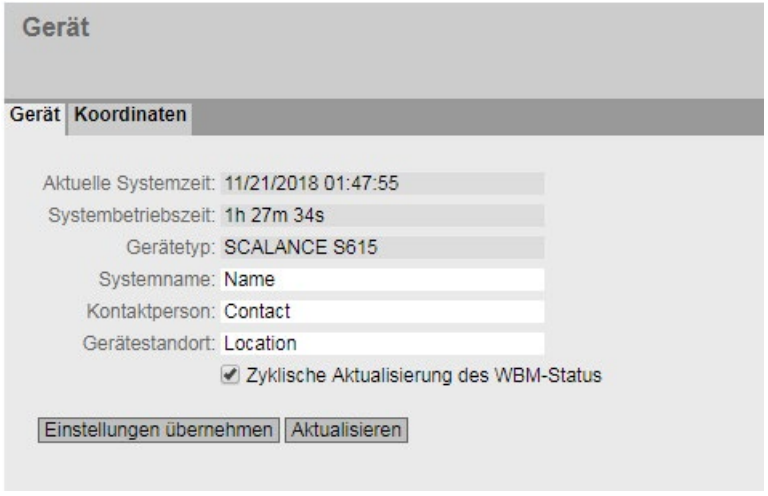
Vorgehensweise

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".

4.5.2 Allgemein

4.5.2.1 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 SINEC H1 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
- !"#$%&'()*+,-./:;<=>?@ [\]_{|}~^`

- **Zyklisches 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.

4.5.2.2 Koordinaten

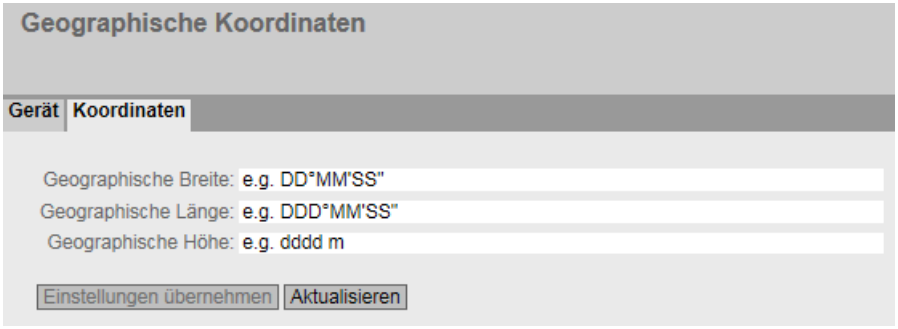
Informationen über die geografischen Koordinaten

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

Nutzen Sie zur Ermittlung der geografischen Koordinaten des Geräts entsprechendes Kartenmaterial.

Die geografischen Koordinaten können auch durch einen GPS-Empfänger ermittelt werden. Meist werden die geografischen Koordinaten von diesen Geräten direkt angezeigt und müssen nur noch in die Eingabefelder dieser Seite übertragen werden.



Beschreibung

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

- **Eingabefeld "Geographische Breite"**
  Geografische Breite: Hier wird der Wert für nördliche oder südliche Breite für den Standort des Geräts eingegeben.

  Der Wert +49° 1´31.67" bedeutet, dass sich das Gerät auf 49 Grad, 1 Bogenminute und 31.67 Bogensekunden nördlicher Breite befindet.
  Die südliche Breite wird mit einem führenden Minuszeichen dargestellt.
  Sie können auch die Buchstaben N (nördliche Breite) oder S (südliche Breite) an die Zahlenangabe anhängen (49° 1´31.67" N).
- **Eingabefeld "Geographische Länge"**
  Geografische Länge: Hier wird der Wert für östliche oder westliche Länge für den Standort des Geräts eingegeben.
  Der Wert +8° 20´58.73" bedeutet, dass sich das Gerät auf 8 Grad, 20 Bogenminuten und 58.73 Bogensekunden östlicher Länge befindet.
  Die westliche Länge wird mit einem führenden Minuszeichen dargestellt.
  Sie können auch die Buchstaben O bzw. E (östliche Länge) oder W (westliche Länge) an die Zahlenangabe anhängen (8° 20´58.73" E).

- **Eingabefeld: "Geographische Höhe"**
  Geografische Höhe: Hier wird der Wert für geografische Höhe über oder unter normal Null (Meereshöhe) in Metern eingegeben.
  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.

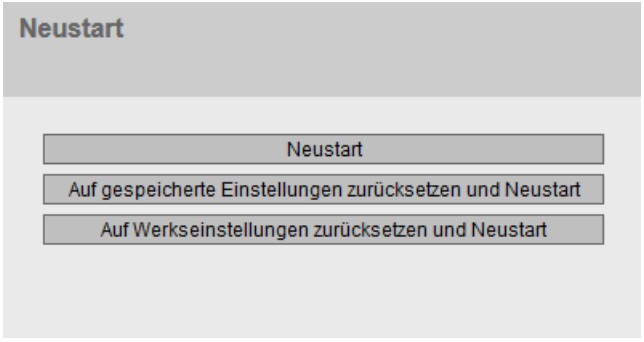
Vorgehensweise

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".

4.5.3 Neustart

Zurücksetzen der Voreinstellungen

In diesem Menü finden Sie eine Schaltfläche zum Neustart des Gerätes sowie verschiedene Möglichkeiten, die Voreinstellungen des Gerätes zurückzusetzen.



Hinweis

Beachten Sie folgende Punkte beim Neustart eines Gerätes:

- Sie können einen Neustart des Gerätes nur mit Administrator-Rechten durchführen.
- Der Neustart eines Gerätes sollte nur durch die Schaltflächen dieses Menüs und nicht durch Aus- und Einschalten der Spannungsversorgung am Gerät erfolgen.
- Vorgenommene Änderungen werden erst nach dem Anklicken der Schaltfläche "Einstellungen übernehmen" auf der jeweiligen WBM-Seite im Gerät wirksam. Wenn sich das Gerät im "Trial--Mode" befindet, müssen Konfigurationsänderungen vor einem Neustart manuell abgespeichert werden. Im "Autosave-Mode" 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 folgenden Parameter zurückzusetzen und einen Neustart auszuführen:
  - IP-Adressen
  - Subnetzmaske
  - IP-Adresse des Standard-Gateways
  - DHCP Client ID
  - DHCP
  - Systemname
  - System-Aufstellungsort
  - System-Ansprechpartner
  - Benutzernamen und Passwörter
- **Auf Werkseinstellungen zurücksetzen und Neustart**
  Klicken Sie auf diese Schaltfläche, um die werksseitigen Konfigurationseinstellungen wiederherzustellen. Es werden auch die geschützten Voreinstellungen zurückgesetzt. Es wird ein automatischer Neustart ausgeführt.

Hinweis

Durch das Zurücksetzen auf die werkseitigen Konfigurationseinstellungen ist das Gerät wieder über die werkseitig eingestellte IP-Adresse 192.168.1.1 zu erreichen, siehe Kapitel "Voraussetzungen für den Betrieb".

4.5.4 Laden & Speichern

4.5.4.1 Dateiliste

Übersicht der Dateitypen

Dateityp	Beschreibung
Config	Diese Datei enthält die Startkonfiguration. Diese Datei enthält unter anderem die Definitionen der Benutzer, Rollen, Gruppen und Funktionsrechte. Die Passwörter sind in der Datei "Users" abgespeichert.
ConfigPack	Detaillierte Konfigurationsinformationen z. B. Startkonfiguration, Benutzer, Zertifikate, WBM Favoriten ZIP-Datei, die aus der Config-, Users- und LSYS-Datei besteht.
Debug	Diese Datei beinhaltet Informationen für den Siemens Support. Sie ist verschlüsselt und kann ohne Sicherheitsrisiko per E-Mail an den Siemens Support gesendet werden.
Firmware	Die Firmware ist signiert und verschlüsselt. Damit ist sichergestellt, dass nur von Siemens erstellte Firmware in das Gerät geladen werden kann.
HTTPSCert	Voreingestellte HTTPS-Zertifikate inkl. Schlüssel Die voreingestellten und automatisch erstellten HTTPS-Zertifikate sind selbstsigniert. 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. Es gibt Dateien, deren Zugriff passwortgeschützt ist. Um die Datei erfolgreich ins Gerät zuladen, geben Sie auf der WBM-Seite "Passwörter (Seite 146)" das für die Datei festgelegte Passwort ein.
LogFile	Datei mit Einträgen aus der Ereignisprotokolltabelle
MIB	Private MSPS MIB-Datei
RunningCLI	Textdatei mit CLI-Befehlen Diese Datei enthält eine Übersicht der aktuellen Konfiguration in Form von CLI-Befehlen. Passwörter sind in dieser Datei wie folgt maskiert: [PASSWORD] Sie können die Textdatei herunterladen. Die Datei ist nicht dafür vorgesehen, dass Sie sie unverändert wieder hochladen
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. 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, siehe auch "SINEMAConfig".

Dateityp	Beschreibung
Script	Textdatei mit CLI-Befehlen Sie können eine Skriptdatei in einem Gerät hochladen. Die enthaltenen CLI-Befehle werden entsprechend ausgeführt. CLI-Befehle zum Speichern und Laden von Dateien können nicht über die CLI-Skriptdatei (Script) ausgeführt werden.
SINEMAConfig	Über diesen Dateityp laden Sie Konfigurationsdaten, die über STEP7 Basic/Professional für eine Übergabe an das WBM exportiert wurden. 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, siehe auch "RunningSINEMAConfig".
StartupInfo	Startup Logdatei Diese Datei enthält die Meldungen die während des letzten Hochlaufs im Logbook eingetragen wurden.
Users	Diese Datei enthält die Zuordnung der Benutzernamen zu den entsprechenden Passwörtern.
WBMFav	WBM Favoriten Diese Datei enthält die Favoriten, die Sie im WBM angelegt haben. Sie können diese Datei herunterladen und in anderen Geräten hochladen
X509Cert	Mit Zertifikaten werden verschiedene Teilnehmer zertifiziert. Folgende Dateitypen können in das Gerät geladen werden: • .crt, pem, zip: Maximale Dateinamenlänge 255 Zeichen • .p12: Maximale Dateinamenlänge 248 Zeichen Es gibt Dateien, deren Zugriff passwortgeschützt ist. Um die Datei erfolgreich ins Gerät zuladen, geben Sie auf der WBM-Seite "Passwörter (Seite 146)" das für die Datei festgelegte Passwort ein. Die geladenen Dateien werden auf "Security > Zertifikate > Übersicht (Seite 282)" aufgelistet. Weiterführende Information zu Zertifikaten finden Sie unter "Zertifikate (Seite 53)".

4.5.4.2 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.

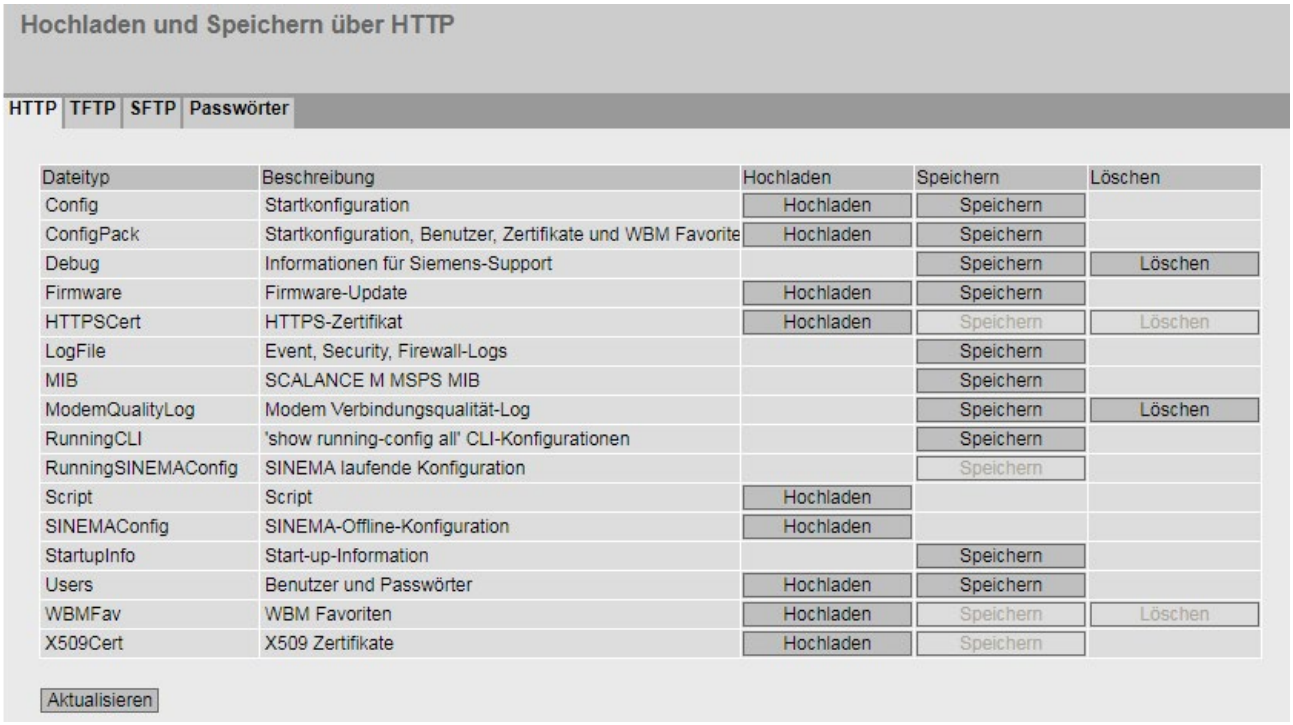
- Zur Konfiguration

  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 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 herunterladen. 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 Ihres Internet-Browsers.

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 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. Wählen Sie die gewünschte Datei aus und bestätigen Sie das Hochladen.

   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.

   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 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 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 den IE-Switch hochladen.

4.5.4.3 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.

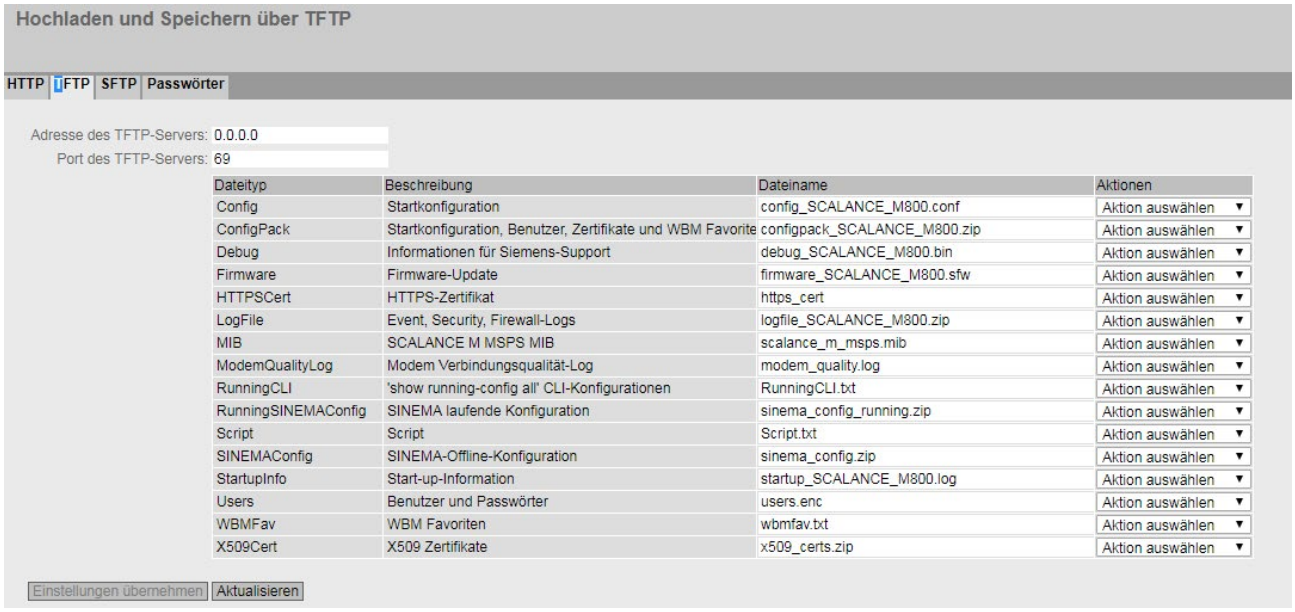
- Zur Konfiguration

  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 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. können Sie die Log-Datei nur speichern.
  Folgende Aktionen sind möglich:
  - **Datei speichern**
    Mit dieser Auswahl speichern Sie eine Datei auf dem 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 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 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 Daten verändern, können Sie sie nicht mehr auf das Gerät hochladen.

4.5.4.4 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.

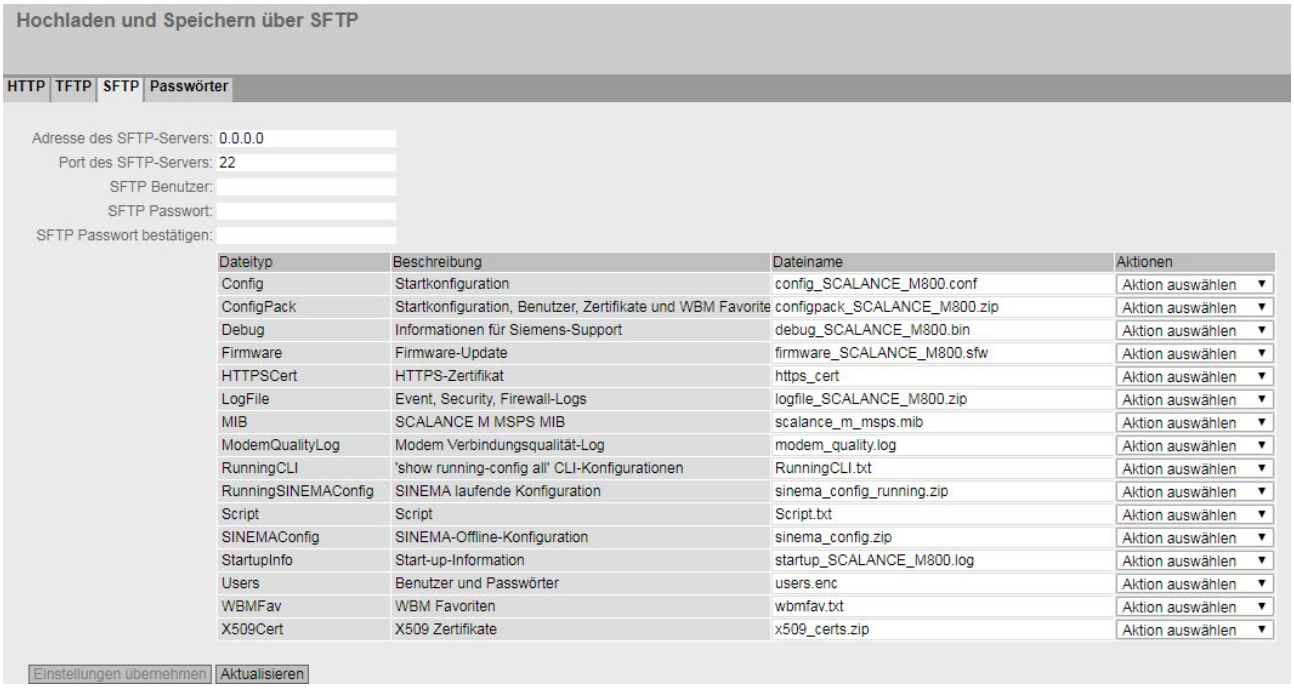
- Zur Konfiguration

  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 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. können Sie die Log-Datei 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 erfolgreich ins Gerät zuladen, 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:

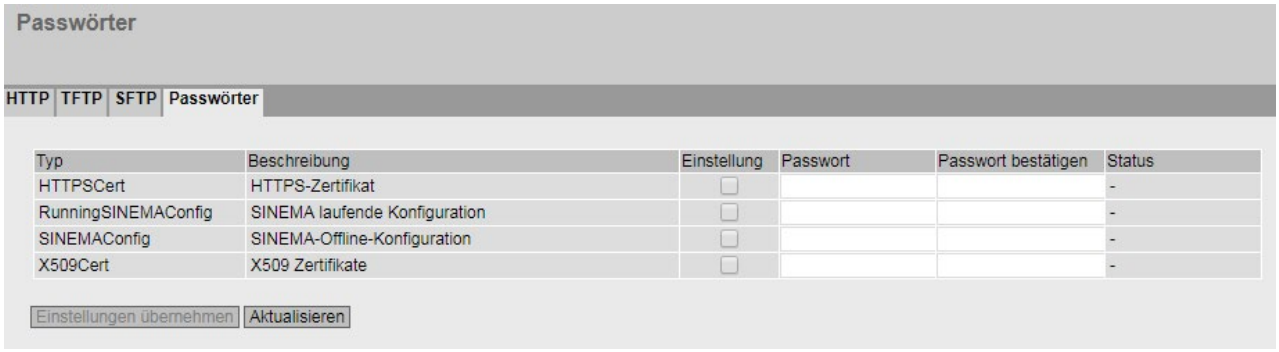
1. Speichern Sie die Konfigurationsdaten eines konfigurierten Geräts auf Ihrem PC.
2. Laden Sie diese Konfigurationsdateien auf alle weiteren Geräte, die Sie so konfigurieren wollen.
3. Falls für einzelne Geräte individuelle Einstellungen erforderlich sind, müssen Sie diese online am betreffenden Gerät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

Hinweis

Konfigurationsdaten sind mit einer Prüfsumme versehen. Wenn Sie die Daten verändern, können Sie sie nicht mehr auf den IE-Switch hochladen.

4.5.4.5 Passwörter

Es gibt Dateien, deren Zugriff passwortgeschützt ist. Um die Datei erfolgreich ins Gerät zu laden, geben Sie auf der WBM-Seite das für die Datei festgelegte Passwort ein.



Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Typ**
  Zeigt den Dateityp an.
- **Beschreibung**

  Zeigt die Kurzbeschreibung des Dateityps an.
- **Einstellung**

  Wenn aktiviert, wird das Passwort verwendet. Nur aktivierbar, wenn das Passwort konfiguriert ist.

- **Passwort**

  Geben Sie das Passwort für die Datei ein.

- **Passwort bestätigen**
  Bestätigen Sie das Passwort.

- **Status**
  Zeigt an, ob die aktuellen Einstellungen zur Datei auf dem Gerät passen.

  – Gültig

    Die Einstellungen sind gültig.

  – Ungültig
    Die Einstellungen sind ungültig

  – '-'
    Status nicht auswertbar.

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".

4.5.5 Ereignisse

4.5.5.1 Konfiguration

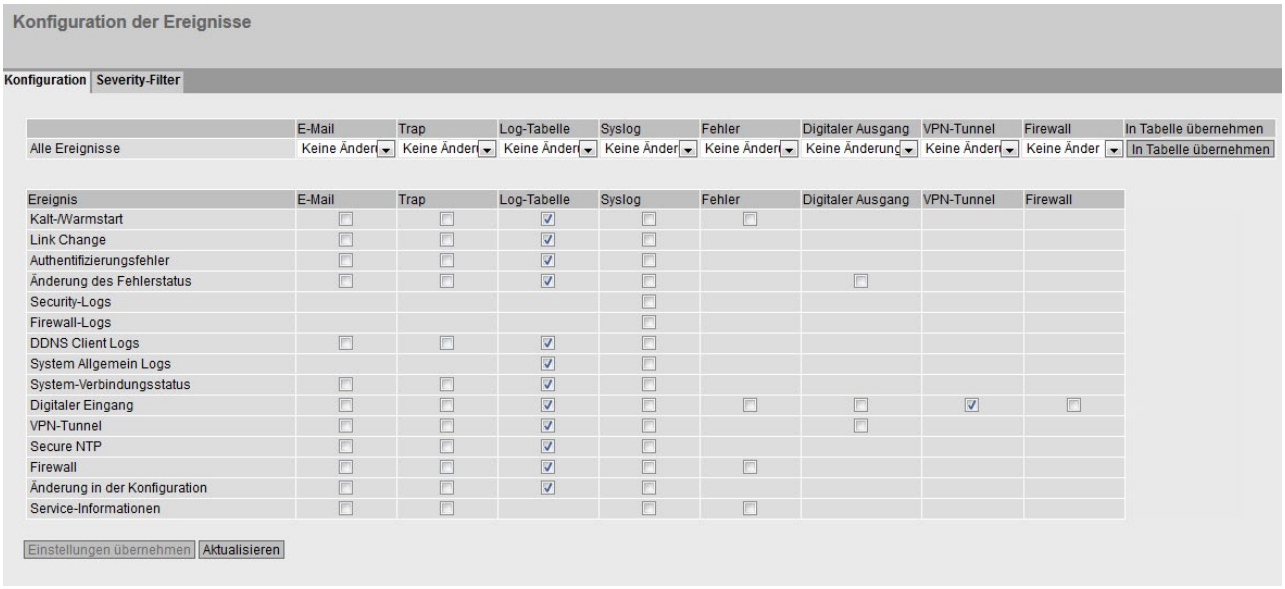
Systemereignisse auswählen

Auf der WBM-Seite legen Sie fest, welche Systemereignisse wie protokolliert werden.

Folgende Meldungen werden immer in die Ereignisprotokoll-Tabelle eingetragen und sind nicht abwählbar:

- Ändern des Admin-Kennworts
- Starten des Geräts
- Betriebstatus 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

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 / Digitaler Ausgang / VPN-Tunnel**
  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.

  – Änderung des Fehlerstatus
  Der Fehlerstatus hat sich geändert. Der Fehlerstatus kann sich auf die aktivierte

Portüberwachung, auf das Ansprechen des Meldekontakts oder die Spannungsüberwachung beziehen.

- Security-Logs
  Im Sicherheitslogbuch wird eingetragen, wenn das IPsec-Verfahren für VPN angewendet
- 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-Verbindungsstatus
  Der Verbindungsstatus hat sich geändert.
- System Allgemein Logs
  Verbindungsaufbau, Änderung der Konfiguration.
- 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.
- Secure NTP
  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).

- **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
- **Digitaler Ausgang**

  Steuert den digitalen Ausgang an oder signalisiert die Zustandsänderung mit der LED "DO".
- **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 > User-specific" dem digitalen Eingang ein Regelsatz zugewiesen ist.

Vorgehensweise

VPN-Tunnel über den Digitalen Eingang auf-/abbauen

1. Aktiveren Sie beim Ereignis "Digitaler Eingang" den Eintrag "VPN-Tunnel".
2. Konfigurieren Sie die VPN-Verbindung
   - IPsec:

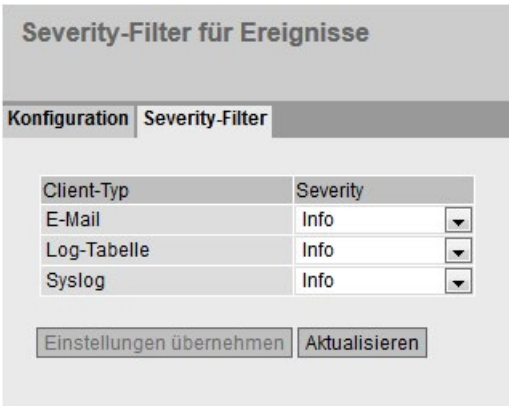
     Stellen Sie bei "Betrieb" "Auf DI warten" oder "Bei DI starten" ein. Weitere Informationen hierzu finden Sie unter "IPsec > Verbindungen" und unter "VPN-Verbindungsaufbau".
   - OpenVPN:

     Stellen Sie bei "Betrieb" "Bei DI starten" ein. Weiterführende Informationen hierzu finden Sie unter "OpenVPN > Verbindungen" und unter "VPN-Verbindungsaufbau".
   - SINEMA RC:

     Stellen Sie bei "Verbindungsart" "Auto" oder "Digitaler Eingang" ein. Bei der Verbindungsart "Auto", müssen Sie auf dem SINEMA RC Server unter "Fernverbindungen > Geräte" die Verbindungsart "Digitaler Eingang" einstellen. Weiterführende Informationen hierzu finden Sie in der Betriebsanleitung "SINEMA RC Server".
3. Klicken Sie auf "Einstellungen übernehmen"

4.5.5.2 Severity-Filter

Auf dieser Seite konfigurieren Sie die Fehlerschwere 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.
- **Severity**
  Wählen Sie die gewünschte Severity aus. Folgende Einstellungen sind möglich:
  - **Info**
    Die Meldungen aller Severity werden versendet bzw. protokolliert.
  - **Warning**
    Die Meldungen dieser Severity und der Severity "Critical" werden versendet bzw. protokolliert.
  - **Critical**
    Nur die Meldungen dieser Severity werden versendet bzw. protokolliert.

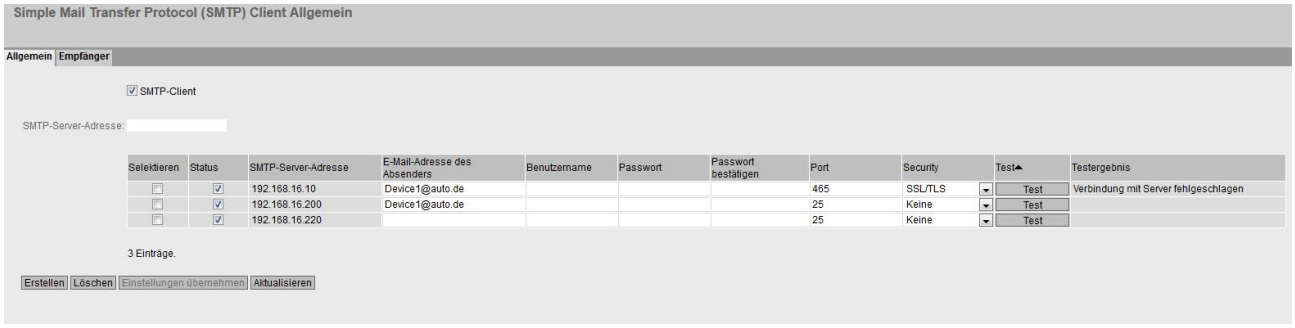
4.5.6 SMTP-Client

4.5.6.1 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.

Damit E-Mails versendet werden, muss bei den Ereignissen die Einstellung "E-Mail" aktiviert sein. Welche Meldungen gesendet werden, ist abhängig von der eingestellten Severity. Die dazugehörigen E-Mail-Adressen, an die das Gerät beim Testen oder im Fehlerfall eine E-Mail sendet, konfigurieren Sie im Register "Empfänger".



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 den E-Mail-Adresse des Absender 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

- **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 konfigurieren 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

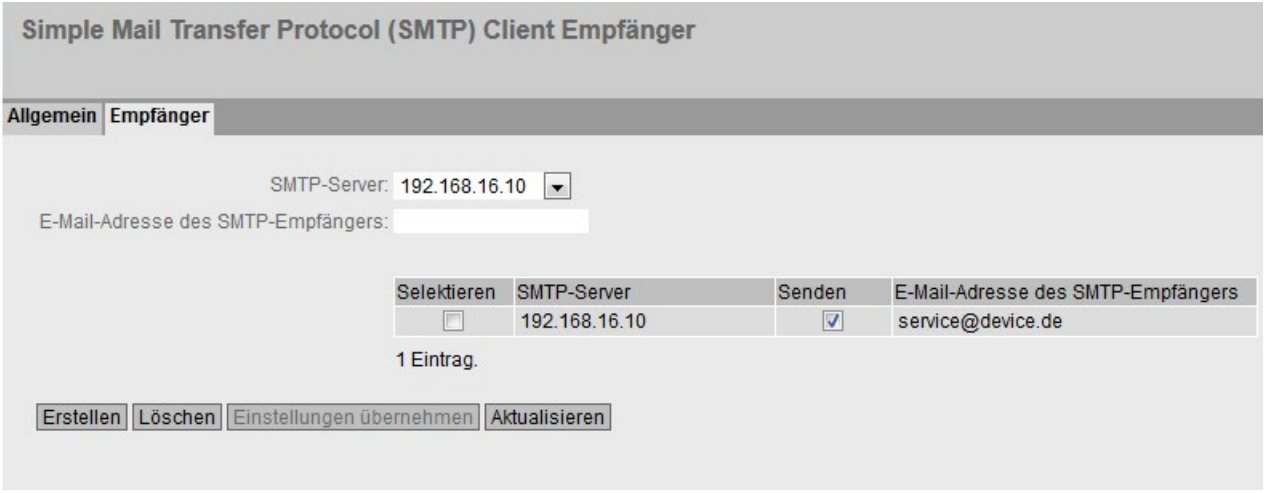
Je nach Eigenschaften und Konfiguration des SMTP-Servers kann es notwendig sein, die Eingabe von "E-Mail-Adresse des Absenders" anzupassen. Informieren Sie sich beim Administrator des SMTP-Servers.

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-Email versenden
   - Klicken Sie auf das Register "Allgemein".
   - Klicken Sie bei dem SMTP-Servereintrag auf die Schaltfläche "Test". Das Gerät sendet jedem konfigurierten Empfänger eine
   - Prüfen Sie das Testergebnis. Wenn das Senden nicht erfolgreich war, enthält die Meldung mögliche Ursachen.

4.5.6.2 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.

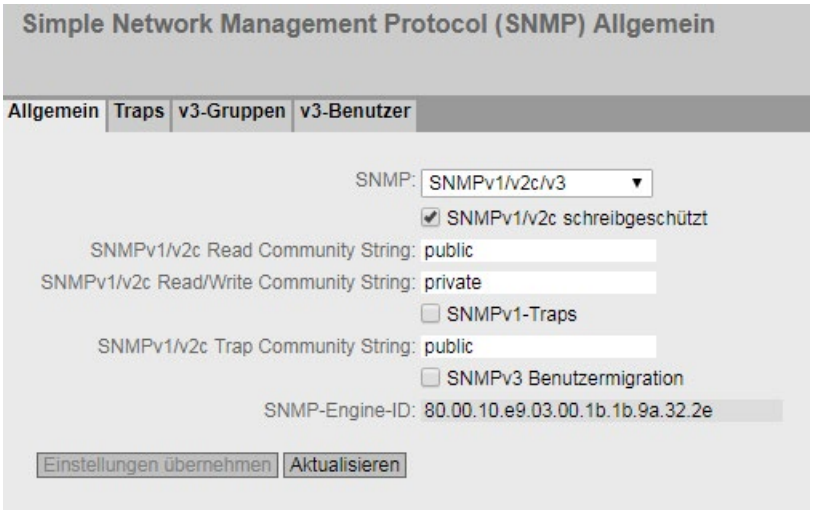
3. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag erzeugt.
4. Aktivieren Sie für den Eintrag die Option "Senden".
5. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

4.5.7 SNMP

4.5.7.1 Allgemein

Konfiguration von SNMP

Auf dieser Seite treffen Sie grundlegende Einstellungen für SNMP. Aktivieren Sie die Optionen abhängig von der Funktion, die Sie nutzen wollen. Beachten Sie hierzu auch die Informationen im Kapitel "Technische Grundlagen".



Beschreibung

Die Seite enthält folgende Felder:

- **SNMP**
  Wählen Sie aus der Klappliste das SNMP-Protokoll. Folgende Einstellungen sind möglich:
  - "-" (Deaktiviert)
    SNMP 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.

  Empfohlene Mindestlänge für Community Strings sind 6 Zeichen.
- **SNMPv1/v2c Read Community String**
  Geben Sie den Community String für den lesenden Zugriff des SNMP-Protokolls ein.
- **SNMPv1/v2c Read/Write Community String**
  Geben Sie den Community String für den lesenden und schreibenden Zugriff des SNMP-Protokolls ein.
- **SNMPv1-Traps**
  Aktivieren oder deaktivieren Sie das Senden von SNMPv1-Traps (Alarmtelegramme). Im Register "Trap" legen Sie die IP-Adressen der Geräte fest, an die SNMPv1-Traps gesendet werden.
- **SNMPv1/v2c Trap Community String**
  Geben Sie den Community String für das Senden von SNMPv1/v2c-Meldungen 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.

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. Geben Sie in das Eingabefeld "SNMPv1/v2c Read Community String" die gewünschte Zeichenkette ein.
4. Geben Sie in das 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".

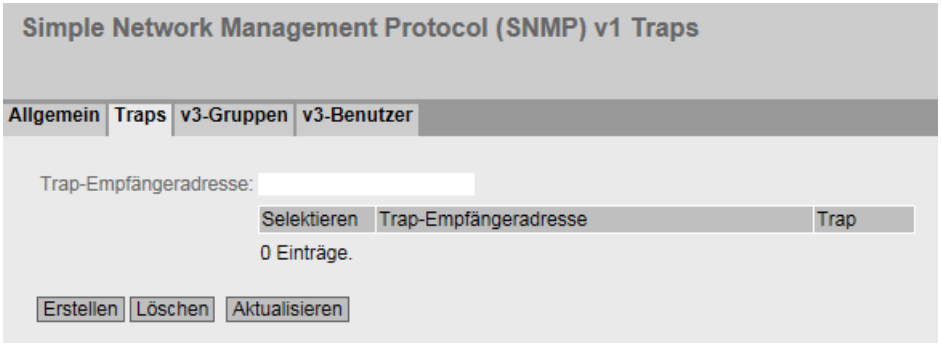
4.5.7.2 Traps

SNMP-Traps bei Alarmereignissen

Beim Eintreten eines Alarmereignisses kann ein Gerät SNMP-Traps (Alarmtelegramme) an bis zu zehn verschiedene Management-Stationen gleichzeitig senden. Es werden nur bei solchen Ereignissen Traps gesendet, die im Menüpunkt "Events" festgelegt wurden.

Hinweis

Traps werden nur dann versendet, wenn Sie im Register "Allgemein" oder unter "System > Konfiguration" die Option "SNMPv1-Traps" aktiviert haben.



Beschreibung

Die Seite enthält folgende Felder:

- **Trap-Empfängeradresse**
  Geben Sie die IP-Adresse, den FQDN (Fully Qualified Domain Name) oder den Hostnamen der Station ein, an die das Gerät SNMP-Traps 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.
- **Trap-Empfängeradresse**
  Ändern Sie bei Bedarf die IP-Adresse, den FQDN (Fully Qualified Domain Name) oder den Hostnamen der Stationen.
- **Trap**
  Aktivieren oder deaktivieren Sie das Senden von Traps. Stationen, die eingegeben, aber nicht selektiert sind, erhalten keine SNMP-Traps.

Vorgehensweise

Trap-Eintrag erstellen

1. Geben Sie bei "Trap-Empfängeradresse" die IP-Adresse, den FQDN oder den Hostnamen der Station ein, an die das Gerät Traps senden soll.
2. Klicken Sie auf die Schaltfläche "Erstellen", um einen neuen Trap-Eintrag zu erstellen.
3. Aktivieren Sie in der gewünschten Zeile "Trap".
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

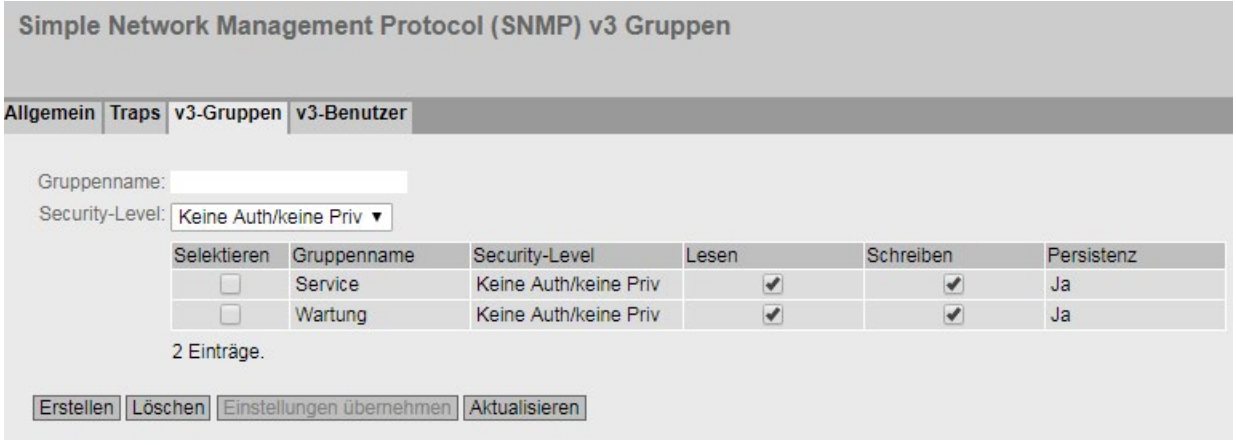
Trap-Eintrag löschen

1. Aktivieren Sie in der zu löschenden Zeile "Selektieren".
2. Klicken Sie auf die Schaltfläche "Löschen". Der Eintrag wird gelöscht.

4.5.7.3 v3-Gruppen

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.



Beschreibung

Die Seite enthält folgende Felder:

- **Gruppenname**
  Tragen Sie den Namen der Gruppe ein. Die maximale Länge beträgt 32 Zeichen.
- **Security-Level**
  Wählen Sie die Sicherheitsstufe (Authentifizierung, Verschlüsselung) aus, die für die gewählte Gruppe gültig ist. 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.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Gruppenname**
  Zeigt die definierten Gruppennamen an.
- **Security-Level**
  Zeigt die konfigurierte Sicherheitsstufe an.
- **Lesen**
  Aktivieren oder deaktivieren Sie den Lesezugriff für die gewünschte Gruppe.
- **Schreiben**
  Aktivieren oder deaktivieren Sie den Schreibzugriff für die gewünschte Gruppe.

  Hinweis

  Damit der Schreibzugriff funktioniert, müssen Sie ebenfalls den Lesezugriff aktivieren.

- **Persistenz**
  Zeigt an, ob die Gruppe einem SNMPv3-Benutzer zugeordnet ist. Wenn die Gruppe keinem SNMPv3-Benutzer zugeordnet ist, wird kein automatisches Speichern ausgelöst und die konfigurierte Gruppe ist nach einem Neustart des Geräts gelöscht.
  - Ja

    Die Gruppe ist einem SNMPv3-Benutzer zugeordnet.
  - Nein

    Die Gruppe ist keinem SNMPv3-Benutzer zugeordnet.

Vorgehensweise

Anlegen einer neuen Gruppe

1. Geben Sie bei "Gruppenname" den gewünschten Gruppennamen ein.
2. Wählen Sie aus der Klappliste "Security-Level" die gewünschte Sicherheitsstufe aus.
3. Klicken Sie auf die Schaltfläche "Erstellen", um einen neuen Eintrag zu erzeugen.
4. Legen Sie bei "Lesen" die gewünschten Leserechte für die Gruppe fest.
5. Legen Sie bei "Schreiben" die gewünschten Schreibrechte für die Gruppe fest.
6. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Ändern einer Gruppe

1. Legen Sie bei "Lesen" die gewünschten Leserechte für die Gruppe fest.
2. Legen Sie bei "Schreiben" die gewünschten Schreibrechte für die Gruppe fest.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Hinweis

Der einmal vergebene Gruppenname und die Sicherheitsstufe können nach dem Anlegen nicht mehr geändert werden. Wenn Sie den Gruppennamen oder die Sicherheitsstufe ändern wollen, müssen Sie die Gruppe löschen und mit dem neuen Namen neu anlegen und neu konfigurieren.

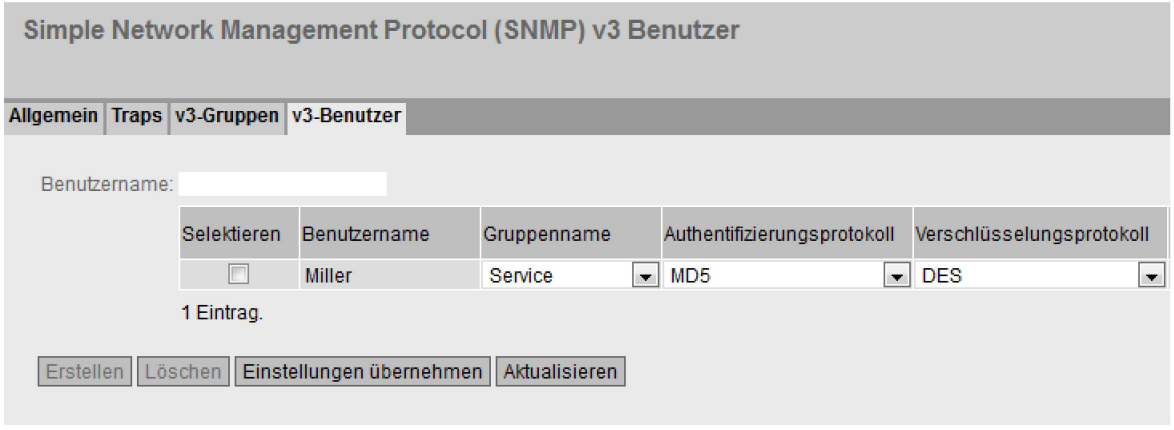
Löschen einer Gruppe

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.

4.5.7.4 v3-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.



SNMPv3-Benutzer - erster Teil der Tabelle



SNMPv3-Benutzer - zweiter Teil der Tabelle

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.
- **Gruppenname**
  Wählen Sie die Gruppe aus, die dem Benutzer zugeordnet wird.
- **Authentifizierungsprotokoll**

  Legen Sie das Authentifizierungsprotokoll fest, für das ein Passwort hinterlegt werden soll.

  Folgende Einstellungen gibt es:

  – Keine
  – MD5
  – SHA

- **Verschlüsselungsprotokoll**

  Legen Sie fest, ob ein Passwort zur Verschlüsselung mit dem DES-Algorithmus hinterlegt werden soll. Nur aktivierbar, wenn auch ein Authentifizierungsprotokoll ausgewählt wurde.

- **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.
- **Persistenz**
  Zeigt an, ob der Benutzer einer SNMPv3-Gruppe zugeordnet ist. Wenn der Benutzer keiner SNMPv3-Gruppe zugeordnet ist, wird kein automatisches Speichern ausgelöst und der konfigurierte Benutzer ist nach einem Neustart des Geräts gelöscht.
  - Ja

    Der Benutzer ist einer SNMPv3-Gruppe zugeordnet.
  - Nein

    Der Benutzer ist keiner SNMPv3-Gruppe zugeordnet.

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 "Gruppenname" die Gruppe aus, der der neue Benutzer angehören soll.

   Wenn die Gruppe noch nicht angelegt ist, wechseln Sie auf die Seite "v3-Gruppen" und legen Sie die Einstellungen für diese Gruppe fest.
4. Wenn für die ausgewählte Gruppe eine Authentifizierung notwendig ist, wählen Sie bei "Authentifizierungsprotokoll" den Authentifizierungsalgorithmus.
   Tragen Sie in die entsprechenden Eingabefelder das Authentifizierungspasswort sowie dessen Bestätigung ein.
5. Wenn für die Gruppe eine Verschlüsselung festgelegt wurde, wählen Sie bei "Verschlüsselungsprotokoll" den Algorithmus aus. Tragen Sie in die entsprechenden Eingabefelder das Verschlüsselungspasswort sowie dessen Bestätigung ein.
6. 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.

4.5.8 Systemzeit

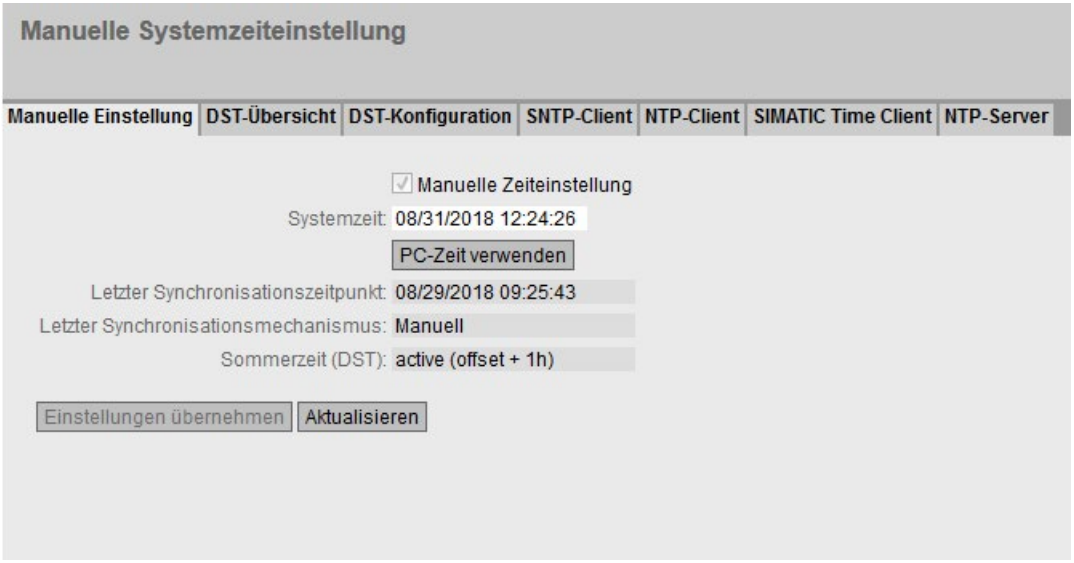
Um die Systemzeit des Geräts einzustellen, gibt es unterschiedliche Methoden. Es kann immer nur eine Methode aktiv sein.

Wenn eine Methode aktiviert wird, dann wird automatisch die bisher aktivierte Methode deaktiviert.

4.5.8.1 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.

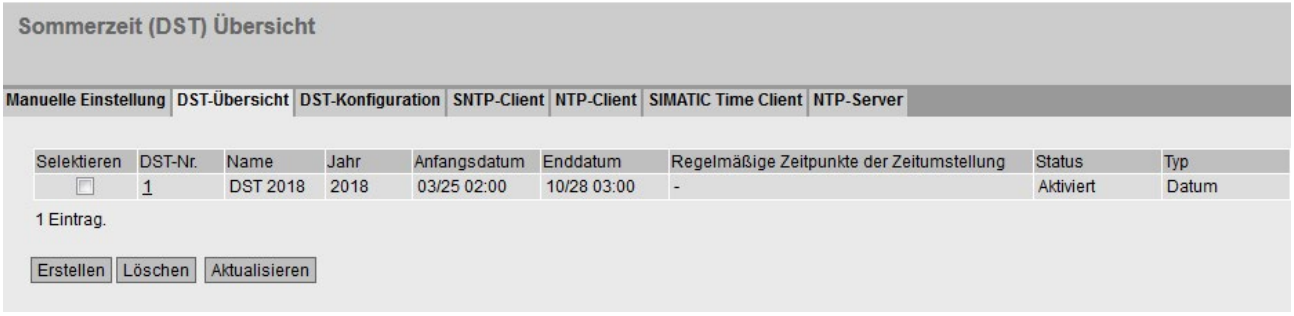
Vorgehensweise

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.

4.5.8.2 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 vorhanden 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.

4.5.8.3 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.

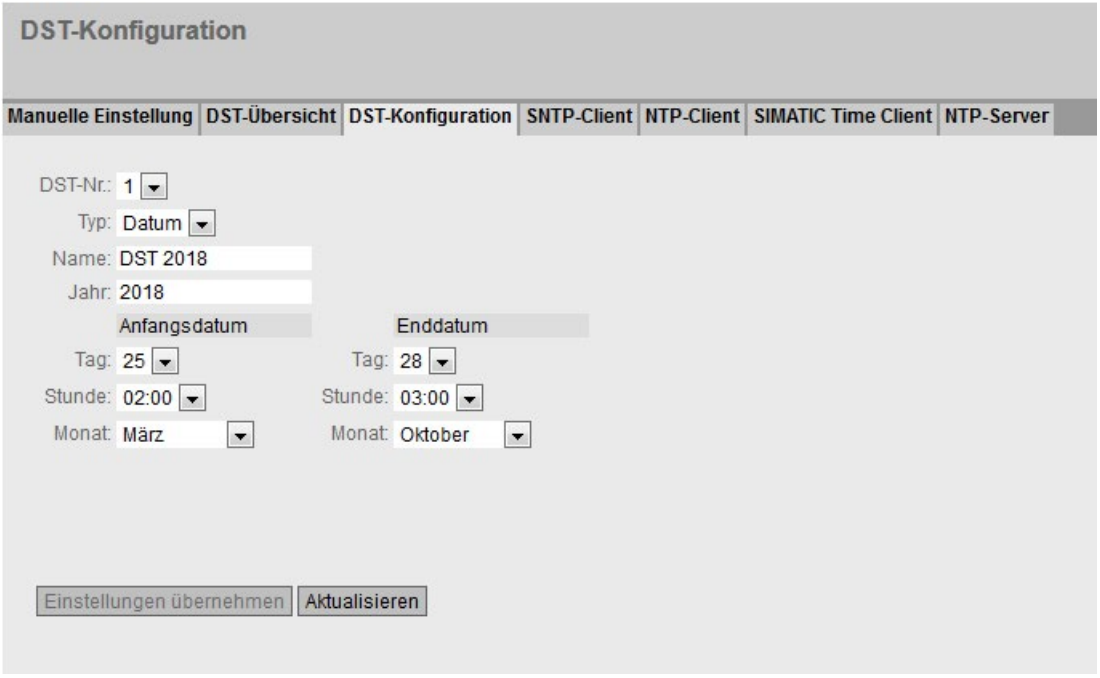
    Diese Einstellung eignet sich für Regionen, in denen die Sommerzeit immer an einem bestimmten Wochentag beginnt bzw. endet.

- **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.

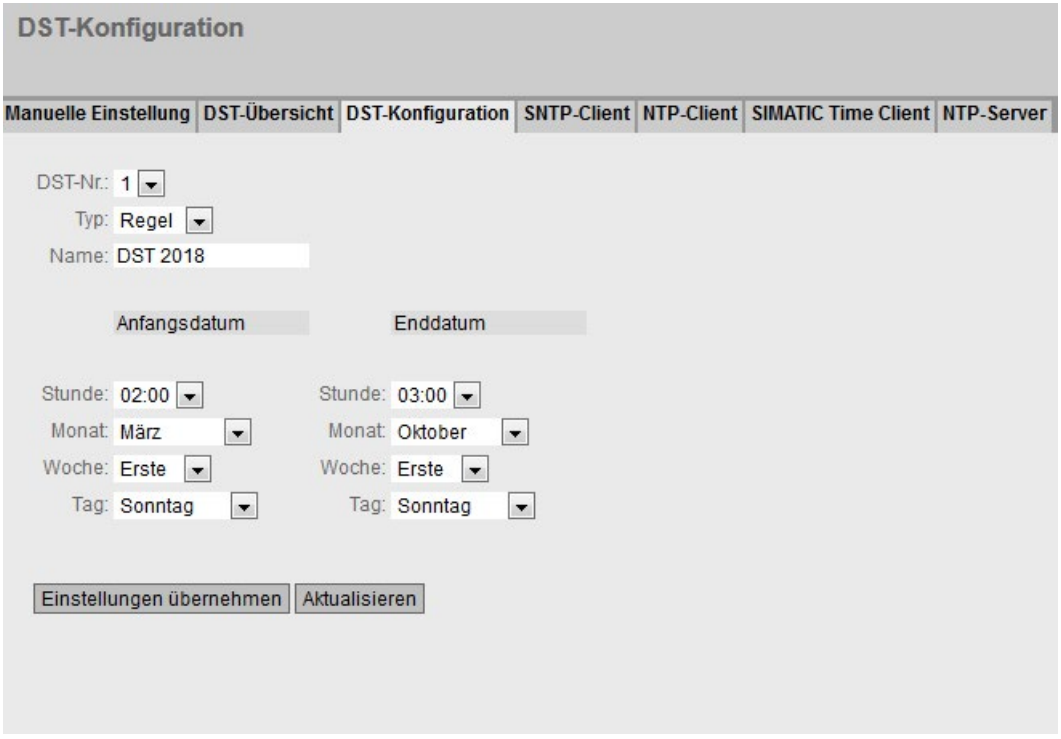
  – Stunde

    Geben Sie die Stunde ein.

  – Monat

    Geben Sie den Monat ein.

Einstellungen bei der Auswahl "Regel"



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.

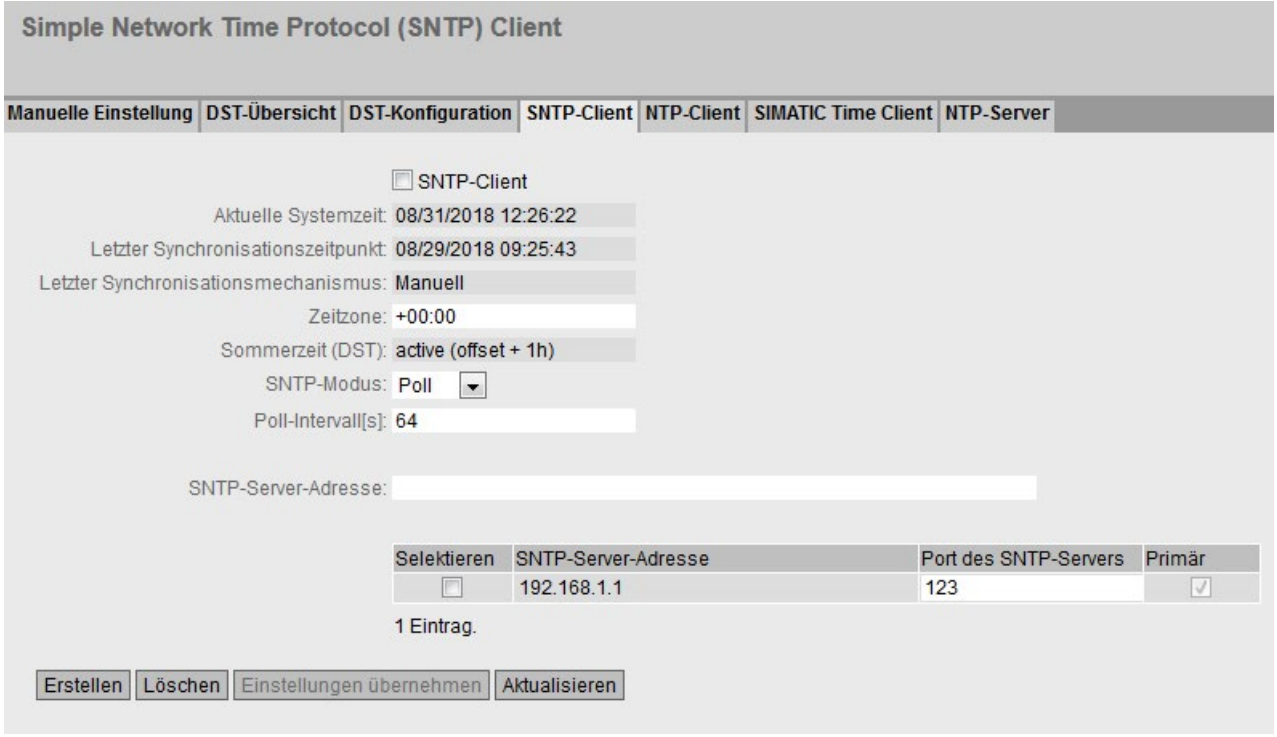
  – Tag

    Geben Sie den Wochentag ein.

4.5.8.4 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.



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 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. Legen Sie für diesen Modus manuell die folgenden Firewall-Regel von "VLANx" nach "Gerät" an. In diesem Modus werden nur IPv4-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.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**

  Wählen Sie die Zeile, die Sie löschen wollen.

- **SNTP-Server-Adresse**
  Geben Sie die IP-Adresse, den FQDN (Fully Qualified Domain Name) oder den Hostnamen des SNTP-Servers ein.

- **Port des SNTP-Servers**
  Geben Sie den Port des SNTP-Servers ein.
  Folgende Ports sind möglich:
  - 123 (Standard-Port)
  - 1025 bis 36564

- **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.

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.

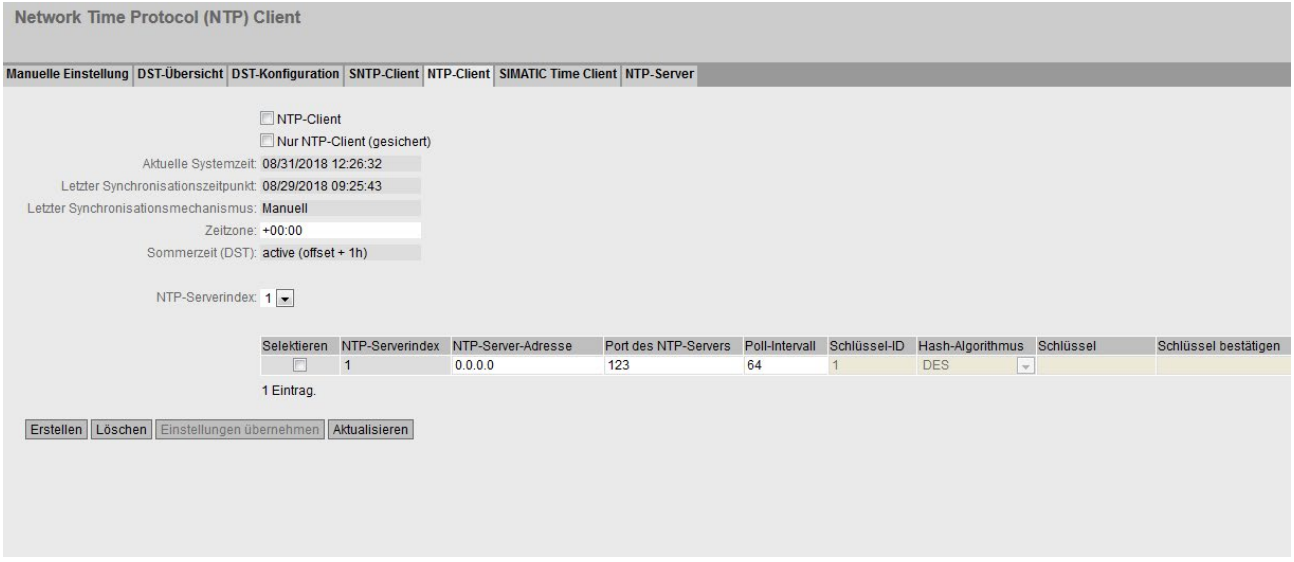
   Das Eingabeformat ist "+/-HH:MM", da der NTP-Server immer die UTC-Zeit sendet, z. B. +02:00 für MESZ, die mitteleuropäische Sommerzeit. Diese Zeit wird mithilfe der Angabe für die Zeitzone in die lokale Zeit umgerechnet.

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".

4.5.8.5 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.



Voraussetzung

Um die NTP-Telegramme zu empfangen, aktivieren Sie unter "Security > Firewall > Vordefinierte IPv4-Regelntra 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. Der Server mit dem kleinsten Index wird zuerst angefragt.

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.

  Folgende Mindestlängen werden für den Hash-Algorithmus empfohlen:

  – MD5: ASCII 16 Zeichen

  – SHA1: ASCII 20 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

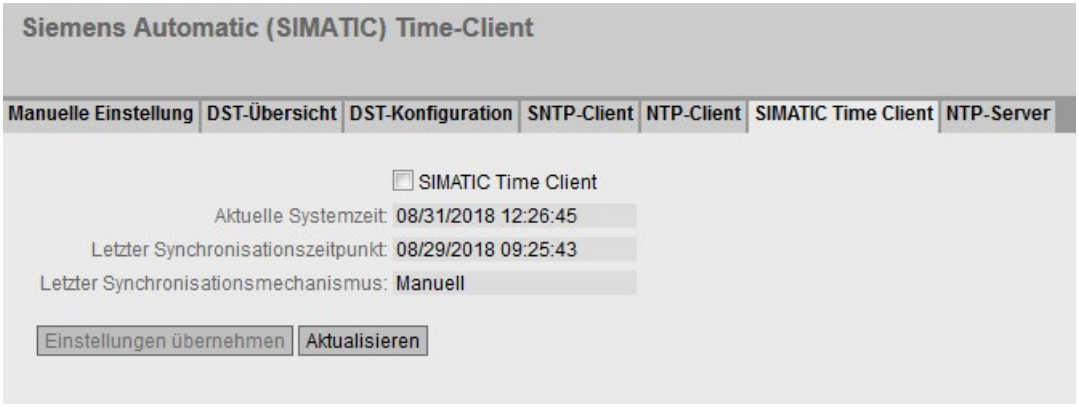
Um die Uhrzeit über einen Secure NTP-Server zu synchronisieren, sind folgende zusätzliche Schritte notwendig:

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".

4.5.8.6 SIMATIC Time Client

Zeiteinstellung über SIMATIC Time Client



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
- **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. Klicken Sie in das Optionskästchen "SIMATIC Time Client", um den SIMATIC Time Client zu aktivieren.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

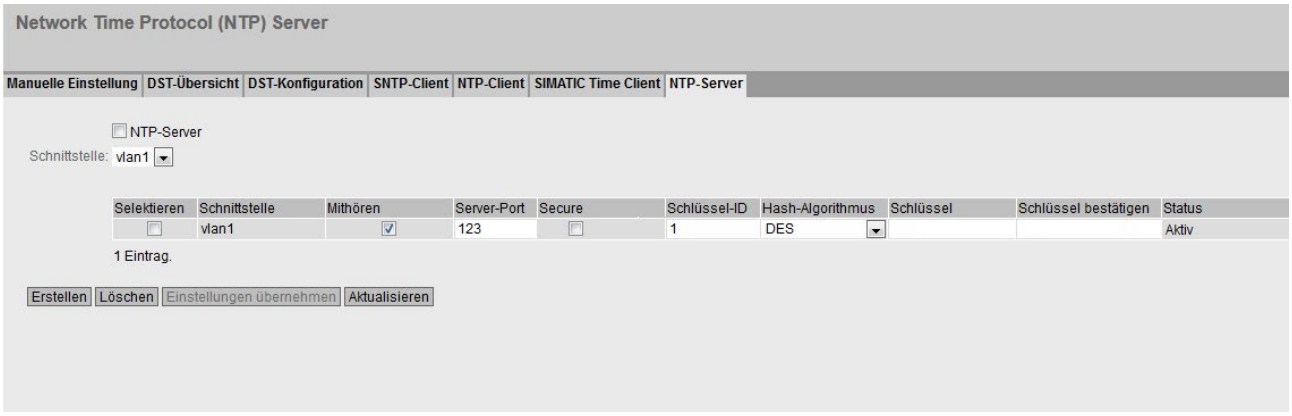
4.5.8.7 NTP-Server

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.



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:
  - MD5: ASCII 16 Zeichen
  - SHA1: ASCII 20 Zeichen
- **Schlüssel bestätigen**
  Geben Sie den Authentifizierungsschlüssel zur Bestätigung ein.
- **Status**
  Zeigt an, ob die Schnittstelle aktiv ist oder nicht.

4.5.9 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

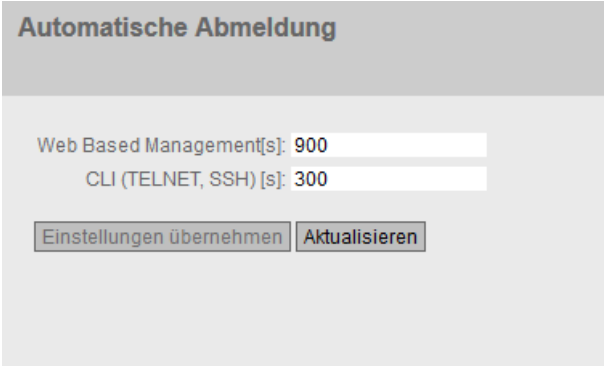
Keine automatische Abmeldung vom CLI

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".

4.5.10 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 322)".

4.5.11 Syslog-Client

Syslog nach RFC 3164 wird für die Übermittlung von kurzen, unverschlüsselten Textmeldungen per UDP im IP-Netz verwendet. Dazu wird ein Syslog-Server benötigt.

Voraussetzungen für das Versenden von Log-Einträgen

- Die Syslog-Funktion ist im Gerät aktiviert.
- Die Syslog-Funktion für das jeweilige Ereignis ist aktiviert.
- In Ihrem Netz befindet sich ein Syslog-Server, der die Log-Einträge entgegen nimmt. Da es sich um eine UDP-Verbindung handelt, gibt es keine Rückmeldung an den Absender.
- Die IP-Adresse des Syslog-Servers ist im Gerät eingetragen.



Beschreibung

Die Seite enthält folgende Felder:

- **Syslog-Client**

  Aktivieren oder deaktivieren Sie die Syslog-Funktion.
- **Adresse des Syslog-Servers**

  Geben Sie die IP-Adresse 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 des Syslog-Servers an.
- **Server-Port**

  Geben Sie den verwendeten Port des Syslog-Servers ein.

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 IP-Adresse des Syslog-Servers ein, auf dem die Log-Einträge gespeichert werden sollen.
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 UDP-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.

4.5.12 Fehlerkontrolle

4.5.12.1 Link Change

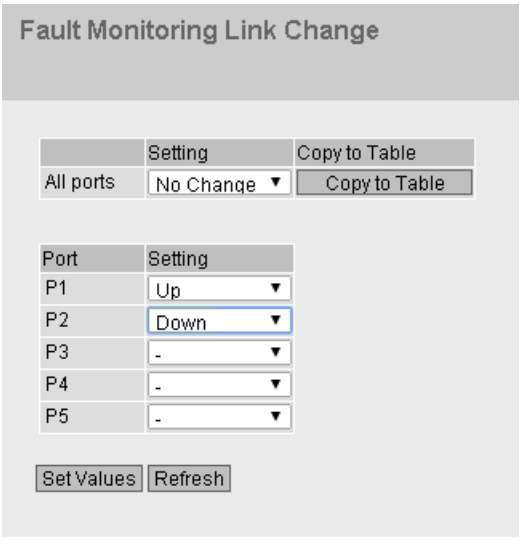
Konfiguration der Fehlerüberwachung von Zustandsänderungen bei Verbindungen

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 Aufleuchten der Fehler-LED am Gerät und kann abhängig von der Konfiguration einen Trap, eine E-Mail 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".

4.5.13 PLUG

4.5.13.1 Konfiguration

ACHTUNG
C-PLUG / KEY-PLUG nicht im laufenden Betrieb ziehen oder stecken! Ein PLUG darf nur bei ausgeschaltetem Gerät entnommen oder eingesetzt werden. 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 KEY-PLUG gesteckt, wird das Gerät nach dem Neustart in einen definierten Fehlerzustand versetzt. Bei SCALANCE M werden in diesem Fall die verfügbaren Funkschnittstellen deaktiviert. 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 des C-PLUG

Diese Seite liefert Detailinformationen über die Konfiguration, die im C-PLUG abgelegt ist. Darüber hinaus gibt es die Möglichkeit, den PLUG auf "Factory Default" zurückzusetzen oder mit einem neuen Inhalt zu versehen.

Hinweis

Inkompatibilität zu Vorgängerversionen mit gestecktem PLUG

Bei der Installation einer Vorgängerversion kann es zu Verlust der Konfigurationsdaten kommen. In diesem Fall startet das Gerät nach der Installation der Firmware mit den Werkseinstellungen. Wenn in diesem Fall ein PLUG im Gerät gesteckt ist, hat dieser nach dem Neustart den Status "Not Accepted", da die sich auf dem PLUG weiterhin die Konfigurationsdaten der vorherigen, aktuelleren Firmware befinden. Somit kann ohne Konfigurationsdatenverlust zur vorherigen, aktuelleren Firmware zurückgekehrt werden.

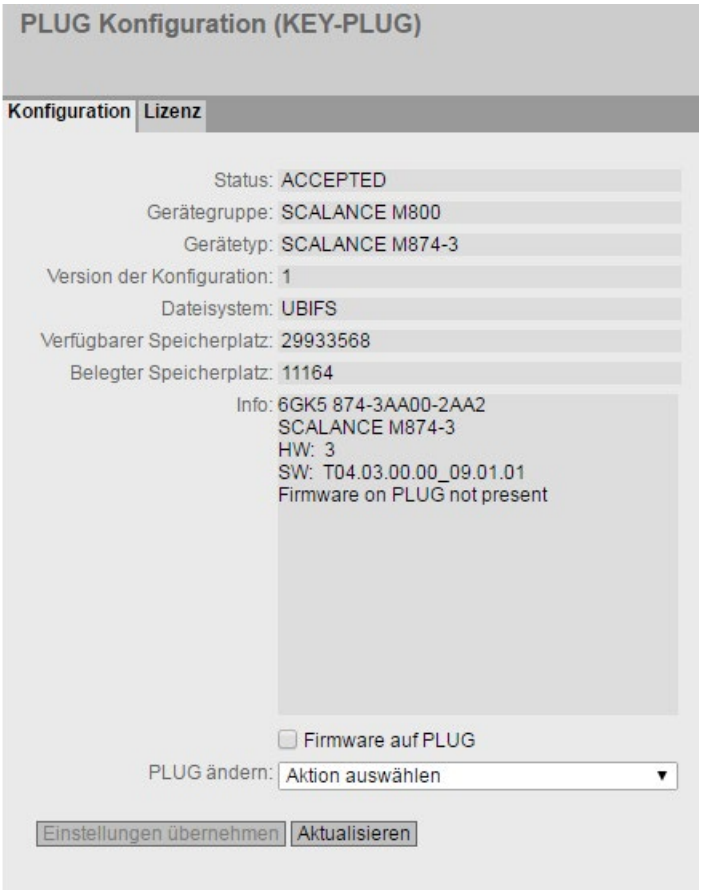
Falls die ursprüngliche Konfiguration auf dem PLUG nicht mehr benötigt wird, kann der PLUG manuell über "System > PLUG" gelöscht oder neu beschrieben werden.

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.



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 C-PLUG oder KEY-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 C-PLUG bzw. KEY-PLUG im vorangegangenen Betrieb genutzt wurde.
- **Gerätetyp**
  Zeigt den Gerätetyp innerhalb der Produktlinie an, von dem der C-PLUG bzw. KEY-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** (ab Firmware-Version 4.3)

  Wenn aktiviert, wird die Firmware auf dem PLUG abgespeichert. Damit können mit dem PLUG automatische Firmware-Updates/Downgrades durchgeführt werden.
- **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".
- **PLUG ändern**
  Wählen Sie aus der Klappliste die Einstellung. Sie haben folgende Möglichkeiten, um die Konfiguration auf dem C-PLUG bzw. KEY-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".

4.5.13.2 Lizenz

ACHTUNG
C-PLUG / KEY-PLUG nicht im laufenden Betrieb ziehen oder stecken! Ein PLUG darf nur bei ausgeschaltetem Gerät entnommen oder eingesetzt werden. 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 KEY-PLUG gesteckt, wird das Gerät nach dem Neustart in einen definierten Fehlerzustand versetzt. Bei SCALANCE M werden in diesem Fall die verfügbaren Funkschnittstellen deaktiviert. 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 Vorgängerversionen mit gestecktem PLUG

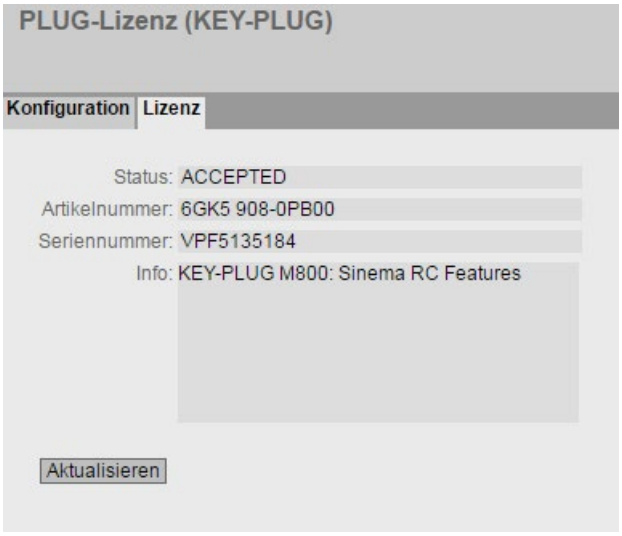
Bei der Installation einer Vorgängerversion kann es zu Verlust der Konfigurationsdaten kommen. In diesem Fall startet das Gerät nach der Installation der Firmware mit den Werkseinstellungen. Wenn in diesem Fall ein PLUG im Gerät gesteckt ist, hat dieser nach dem Neustart den Status "NOT ACCEPTED", da 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 des KEY-PLUG

Ein C-PLUG kann nur die Konfiguration eines Geräts speichern. Ein KEY-PLUG enthält zusätzlich zur Konfiguration eine Lizenz, die bestimmte Funktionen Ihres SIMATIC NET-Geräts freischaltet.

Diese Seite liefert Detailinformationen über die Lizenz auf dem KEY-PLUG.



Beschreibung

- **Status**

  Zeigt den Status des KEY-PLUG an. Es gibt die folgenden Möglichkeiten:

  – ACCEPTED
  Es ist ein KEY-PLUG mit einer gültigen und passenden Lizenz im Gerät vorhanden..

  – NOT ACCEPTED
  Die Lizenz des gesteckten KEY-PLUG ist nicht gültig.

  – NOT PRESENT
  Im Gerät ist kein KEY-PLUG gesteckt.

  – MISSING
  Es ist kein KEY-PLUG mit dem Status "FACTORY" gesteckt. Im Gerät sind Funktionen konfiguriert, für die eine Lizenz erforderlich ist.

  – WRONG
  Der gesteckte KEY-PLUG passt nicht zum Gerät.

  – UNKNOWN
  Unbekannter Inhalt des KEY-PLUG.

  – DEFECTIVE
  Der Inhalt des KEY-PLUG ist fehlerhaft.

- **Artikelnummer**

  Zeigt die Artikelnummer des KEY-PLUG an. Es gibt den KEY-PLUG für unterschiedliche Funktionserweiterungen und für verschiedene Zielsysteme.

- **Seriennummer**

  Zeigt die Seriennummer des KEY-PLUG.

- **Info**

  Zeigt zusätzliche Informationen über das Gerät an, das den KEY-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.

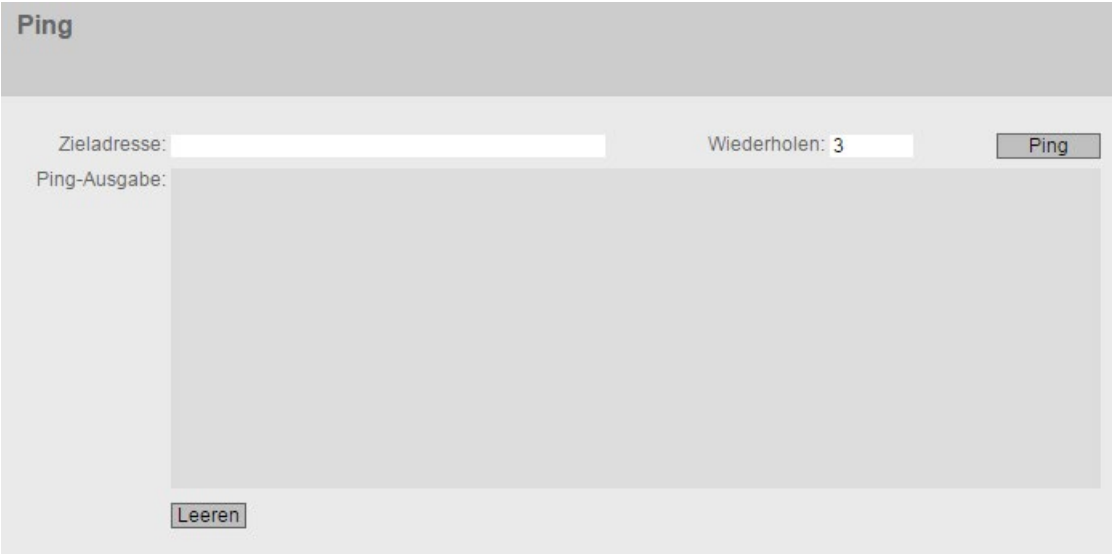
Hinweis

Beim Speichern der Konfiguration wird die Information mitgespeichert, ob zu diesem Zeitpunkt ein KEY-PLUG im Gerät gesteckt war. Diese Konfiguration ist dann auch nur lauffähig, wenn ein KEY-PLUG mit der gleichen Bestellnummer / Lizenz gesteckt ist.

4.5.14 Ping

Erreichbarkeit einer Adresse in einem IPv4-Netzwerk

Mit der Ping-Funktion können Sie überprüfen, ob eine bestimmte IPv4-Adresse im Netzwerk erreichbar ist.



Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Zieladresse**
  Geben Sie die IPv4-Adresse oder den FQDN des Geräts ein.
- **Wiederholen**
  Tragen Sie die Anzahl der Ping-Anforderungen ein.
- **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 das Feld "Ping-Ausgabe" zu leeren.

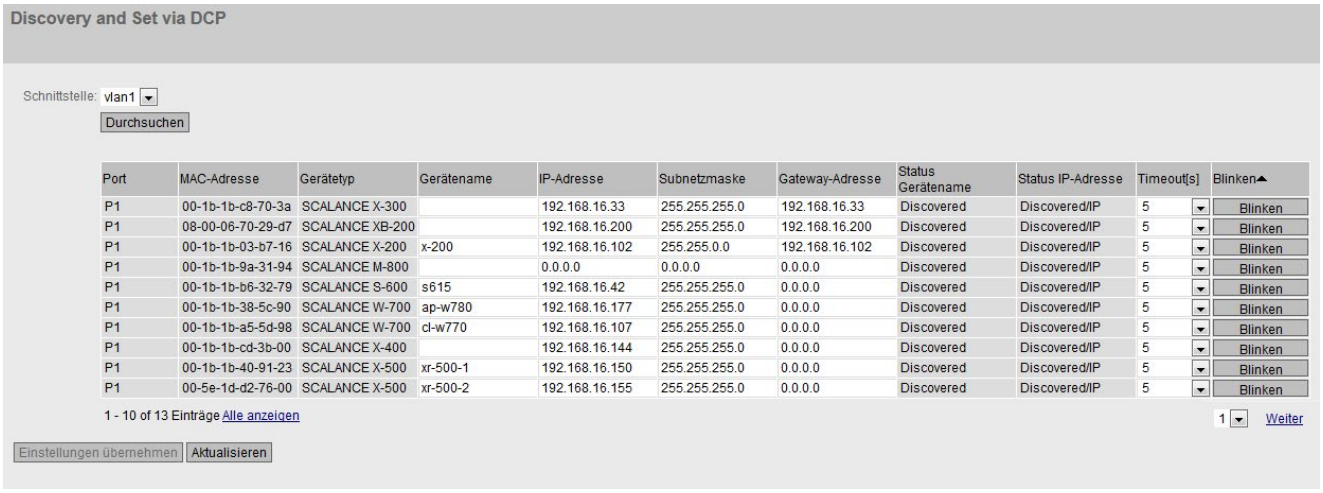
4.5.15 DCP Discovery

Auf dieser Seite können Sie eine Schnittstelle auswählen und nach den Geräten suchen, die über die Schnittstelle erreichbar sind. 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 konfigurieren unter "System > Konfiguration".

Beschreibung

Die Seite enthält folgende Felder:

- **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**

  Falls das Gerät diese Funktion unterstützt, können Sie dem Gerät einen PROFINET-Gerätenamen zuweisen.

- **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**

  Geben Sie bei Bedarf die IPv4-Adresse des Gateways an.

- **Status Gerätename**
  - Discoverd: 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**

  Legen Sie die Zeitdauer für das Blinken fest. Wenn die Zeit abgelaufen ist, wird das Blinken beendet.

- **Blinken**

  Lässt die Port-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 Schatfläche "Einstellungen übernehmen".

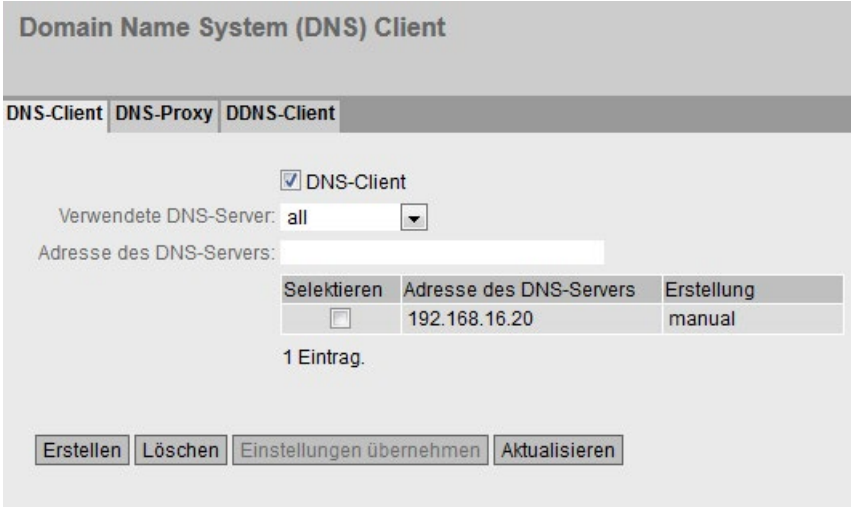
   Der Status der geänderten Eigenschaften ändert sich in "Configured".
5. Um sicherzustellen, dass die Eigenschaften korrekt übernommen wurden, klicken Sie erneut auf die Schaltfläche "Durchsuchen".

   Der Status der geänderten Eigenschaften ändert sich in "Discovered".

4.5.16 DNS

4.5.16.1 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**

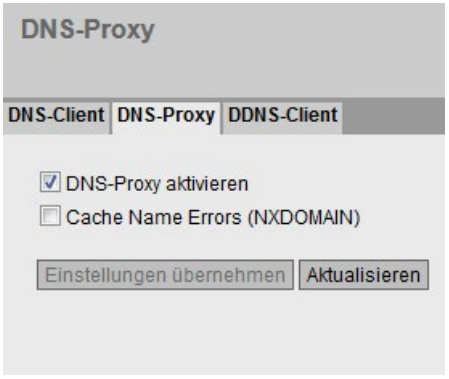
  Zeigt die IP-Adresse des DNS-Servers an.
- **Erstellung**

  Zeigt an, ob der DNS-Server manuell konfiguriert oder durch DHCP zugewiesen wurde.

4.5.16.2 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.

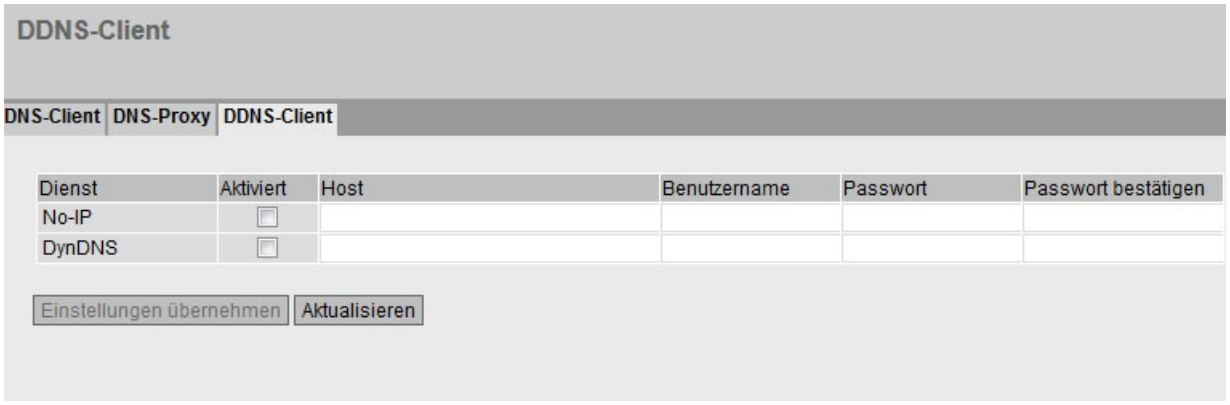
- **Cache Name Errors (NXDOMAIN)**

  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.

4.5.16.3 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:

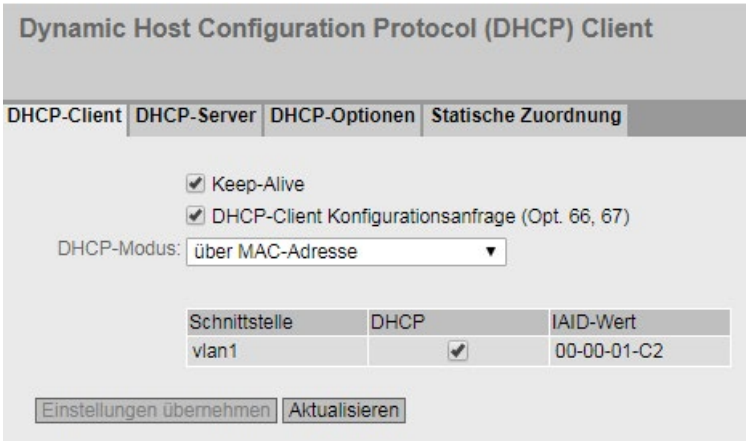
- Benutzernamen und Passwort, dass Sie zur Nutzung des DDNS-Dienstes berechtigt.
- Registrierter Hostname z. B. example.no-ip.com
- Der UDP-Port 53 für DNS ist freigeschaltet und wird nicht bei NAT verwendet.

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".

4.5.17 DHCP

4.5.17.1 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.

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.

- **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

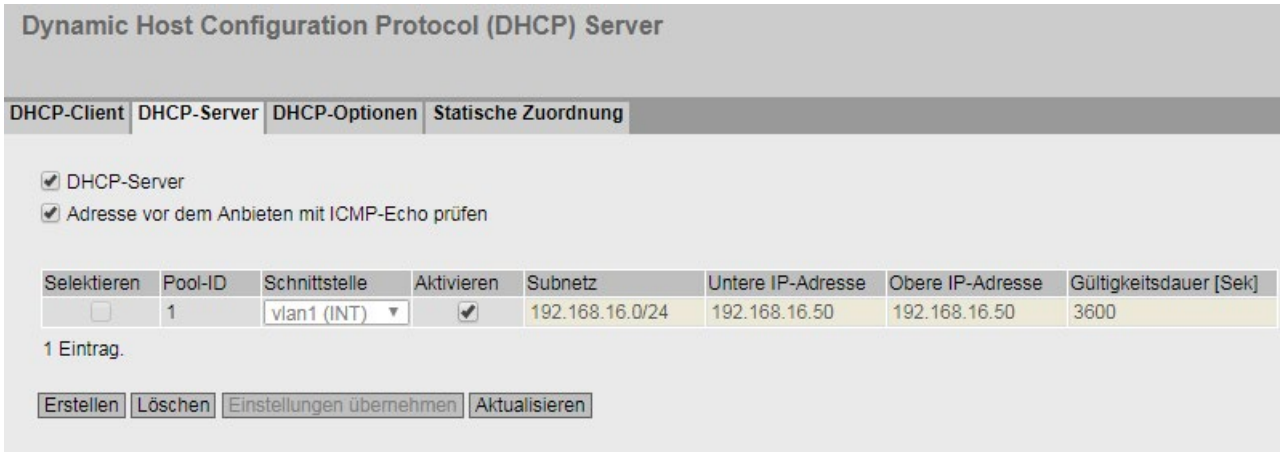
Wird eine Konfigurationsdatei heruntergeladen, so kann dies einen Neustart des Systems auslösen. Wenn sich die aktuell laufende Konfiguration und die Konfiguration in der heruntergeladenen Konfigurationsdatei unterscheiden, startet das System neu.

Achten Sie darauf, dass in dieser Konfigurationsdatei die Option "DHCP-Client Konfigurationsanfrage (Opt. 66, 67)" nicht mehr gesetzt ist.

4.5.17.2 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 Zuordnungen".



Voraussetzung

- Die angeschlossenen Geräte sind so konfiguriert, dass diese 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.

  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.

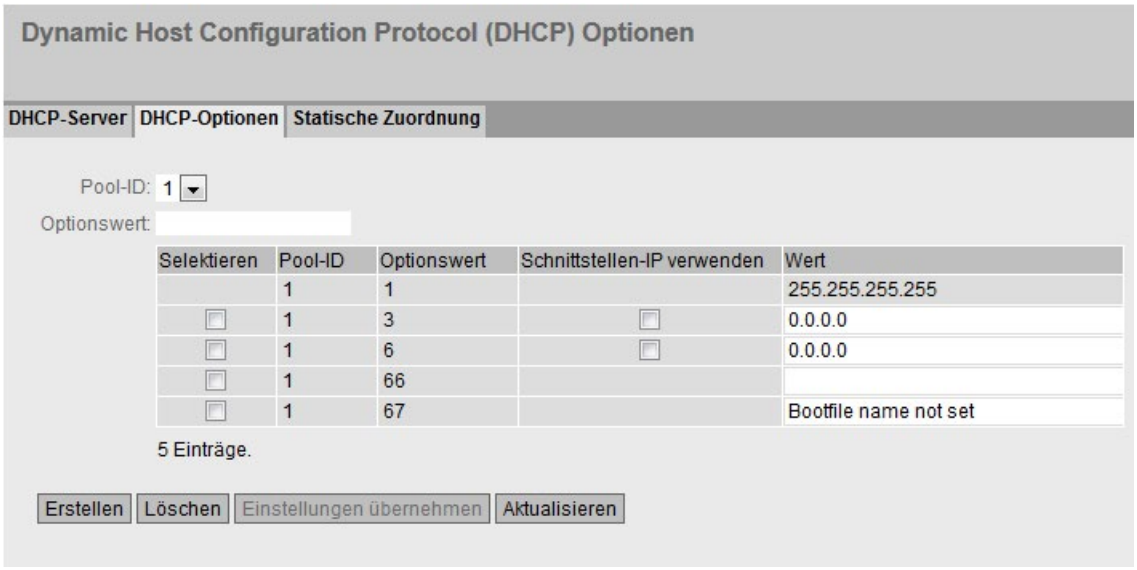
- **Obere IP-Adresse**

  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.

4.5.17.3 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. 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.

4.5.17.4 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 20 Einträge sind 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.

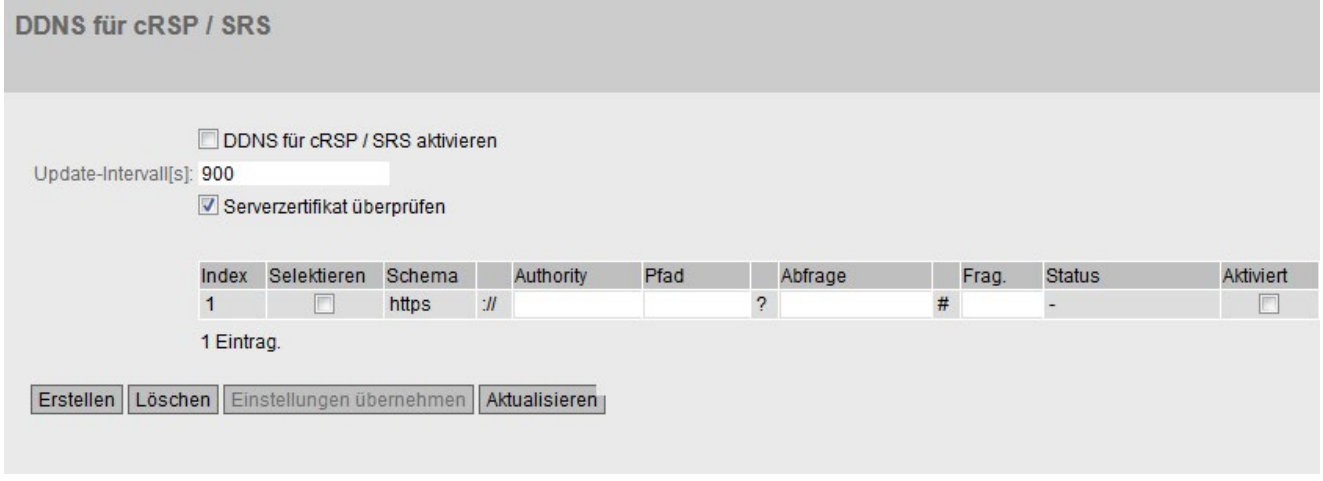
4.5.18 cRSP / SRS

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**

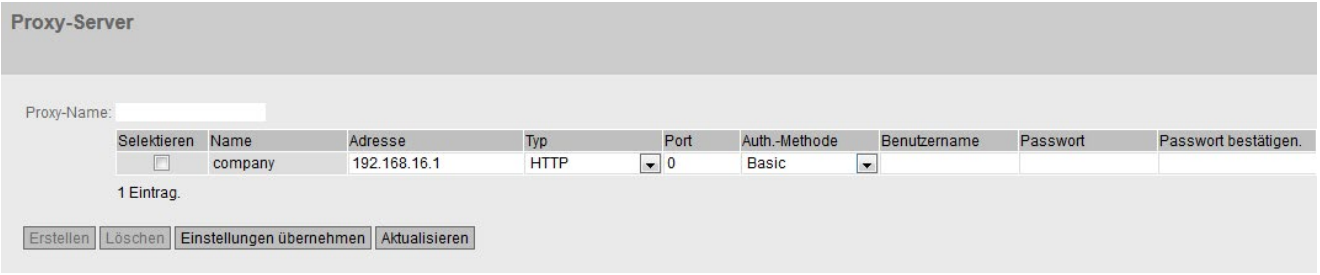
  Zeigt den Status des letzten cRSP / SRS-Zugriffs des Eintrags an.

- **Aktiviert**

  Wenn aktiviert, wird dieser Eintrag verwendet.

4.5.19 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**

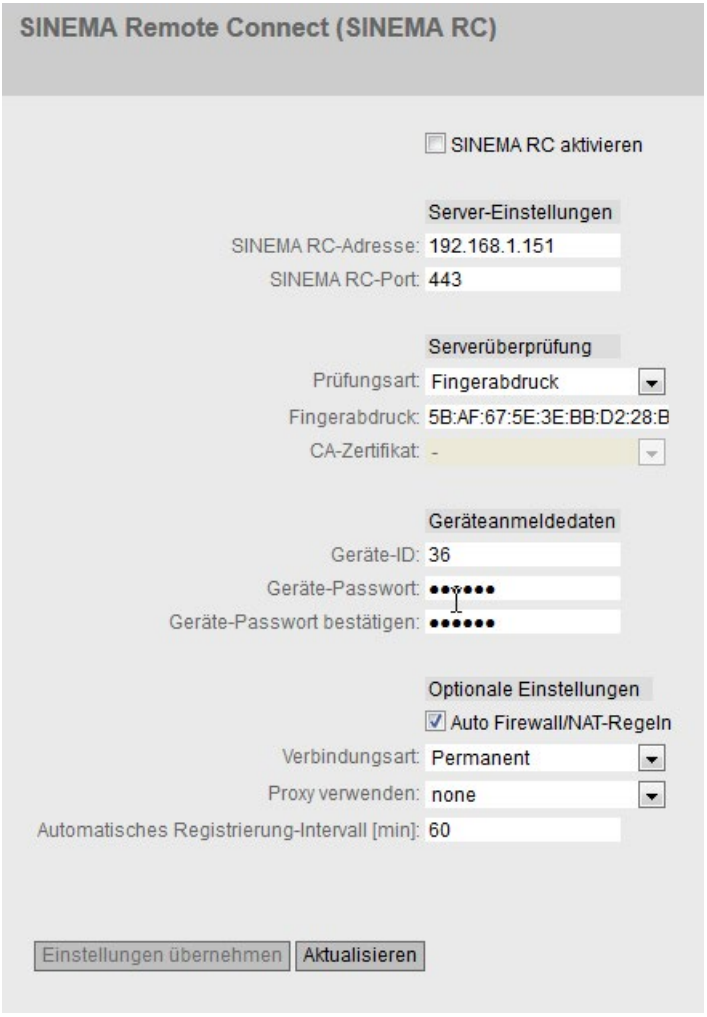
  Geben Sie nochmals das Passwort ein, um es zu bestätigen.

4.5.20 SINEMA RC

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

Hinweis

Diese Funktion ist nur mit KEY PLUG (Seite 25) 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 DNS-Hostnamen 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.

– Deaktiviert

  Sie müssen selbst die Firewall und NAT-Regeln anlegen.

Hinweis

Cloud Connector über SINEMA RC (Nur beim SCALANCE M804PB)

- Standard-Port 9023

  Für den Standard-Port wird die Firewall-Regel automatisch angelegt. Die Kommunikation über diesen Port mit dem TIA Portal Cloud Connector ist möglich.
- Beliebiger Port

  Wenn Sie den Standard-Port ändern, müssen Sie folgende Firewall-Regel konfigurieren:

  Security > Firewall > IP-Dienst:
  – Dienstname: "SINEMARC“
  – Transport: TCP
  – Quell-Port: *
  – Ziel-Port: Port des TIA Portal Cloud Connectors, siehe "System > Cloud Connector "

  Security > Firewall > IP-Regeln:
  – Protokoll: IPv4
  – Aktion: Accept
  – Von: SINEMA RC
  – Nach: Gerät
  – Quelle (Bereich): SINEMA RC-Adresse
  – Ziel (Bereich): 0.0.0.0/0
  – Dienste: SINEMARC

- **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)

    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)

  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.

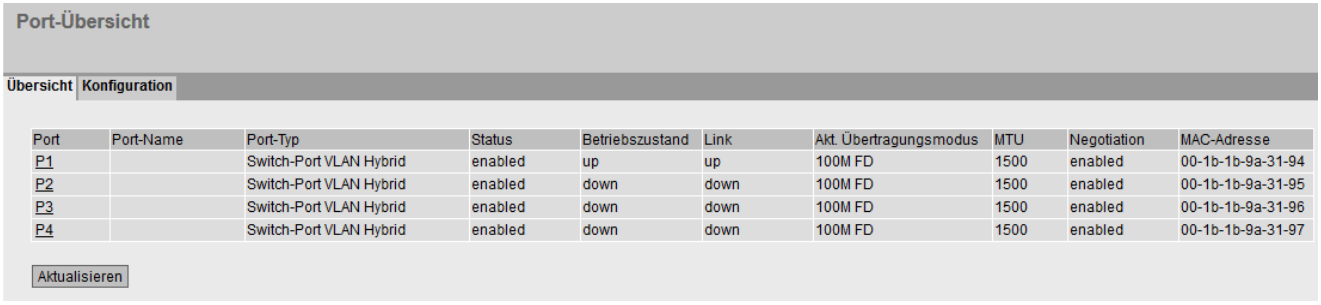
  Wenn Sie den Wert 0 eintragen, ist diese Funktion deaktiviert.

4.6 Menü "Schnittstellen"

4.6.1 Ethernet

4.6.1.1 Übersicht

Die Seite zeigt für alle Ports des Geräts die Konfiguration für den Datentransfer an. Sie können auf dieser Seite keine Konfigurationen vornehmen.



Port	Port-Name	Port-Typ	Status	Betriebszustand	Link	Akt. Übertragungsmodus	MTU	Negotiation	MAC-Adresse
P1		Switch-Port VLAN Hybrid	enabled	up	up	100M FD	1500	enabled	00-1b-1b-9a-31-94
P2		Switch-Port VLAN Hybrid	enabled	down	down	100M FD	1500	enabled	00-1b-1b-9a-31-95
P3		Switch-Port VLAN Hybrid	enabled	down	down	100M FD	1500	enabled	00-1b-1b-9a-31-96
P4		Switch-Port VLAN Hybrid	enabled	down	down	100M FD	1500	enabled	00-1b-1b-9a-31-97

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.

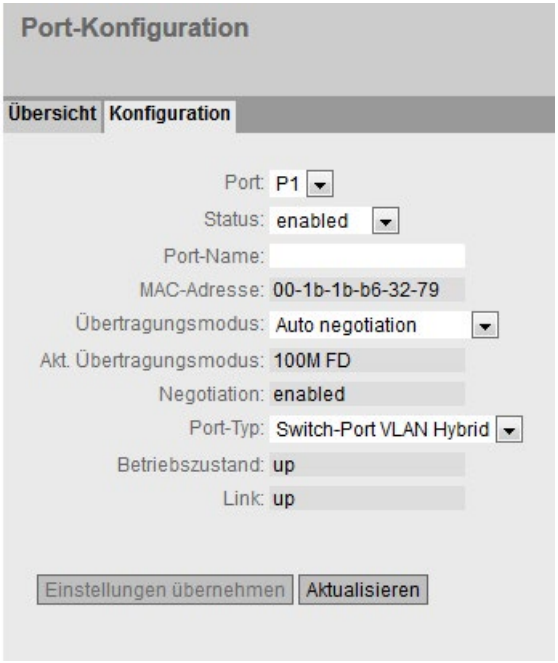
- **MAC-Adresse**

  Zeigt die MAC-Adresse des Ports an.

4.6.1.2 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:

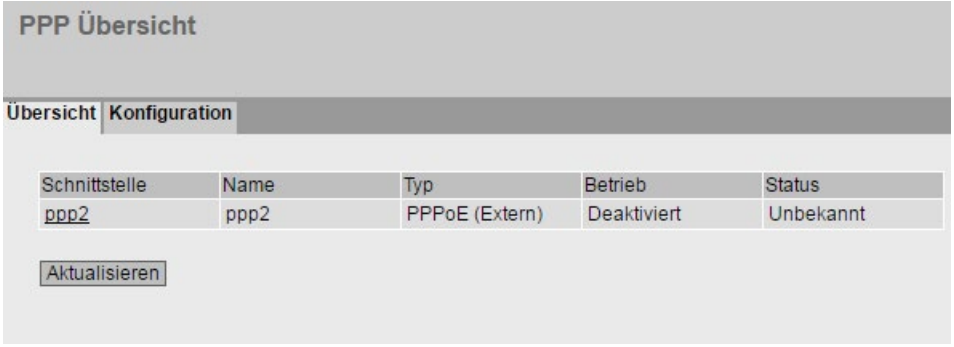
  – Up
  Der Port hat eine gültige Verbindung zum Netzwerk, es wird ein "Link IntegritySignal" empfangen.

  – Down
  Die Verbindung ist unterbrochen, weil z. B. das angeschlossene Gerät ausgeschaltet ist.

4.6.2 PPP

4.6.2.1 Übersicht

Die Seite zeigt den aktuellen Status der PPP-Verbindung an.



Beschreibung der angezeigten Werte

Die Tabelle enthält folgende Spalten:

- **Schnittstelle**

  Zeigt die PPP-Schnittstelle. Der Eintrag ist ein Link. Wenn Sie auf den Link klicken, wird die entsprechende Konfigurationsseite geöffnet.

- **Name**

  Zeigt den Namen der PPP-Schnittstelle an.

- **Typ**

  Zeigt das Protokoll der PPP-Verbindung an.

- **Betrieb**

  Zeigt an, ob die PPP-Verbindung aktiviert oder deaktiviert ist.

- **Status**

  Zeigt den Status der PPP-Verbindung an.

  – Bereit

    Die PPP-Verbindung kann konfiguriert und aktiviert werden.

  – Stellt Verbindung her

    Die PPP-Verbindung ist konfiguriert, aktiviert und der Verbindungsaufbau läuft.

  – Verbunden

    Die PPP-Verbindung ist aufgebaut.

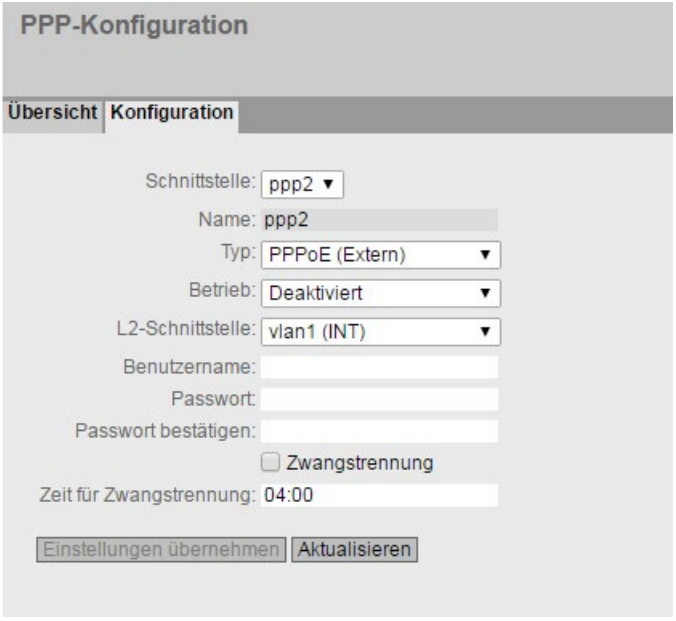
  – Fehler

    Fehlerzustand, in dem ein Benutzereingriff nötig ist, z. B. falsches Passwort.

4.6.2.2 Konfiguration

Auf dieser Seite konfigurieren Sie die PPP-Verbindung. Das Punkt-zu-Punkt-Protokoll (PPP) erlaubt den Anschluss eines externen ADSL-Modems an eine Ethernet-Schnittstelle und darüber dann die Verbindung ins Internet. Die Schnittstelle wird auch als PPP-Schnittstelle bezeichnet.

Das Gerät agiert als Router und meldet sich mit Benutzernamen und Passwort an. Alle angeschlossenen Geräte können die PPP-Verbindung nutzen.



Beschreibung

Die Seite enthält Folgendes:

- **Schnittstelle**

  Wählen Sie die zu konfigurierende PPP-Schnittstelle aus.

- **Name**

  Zeigt den Namen der PPP-Schnittstelle an. Den Namen können Sie unter "Layer 3 > Subnets" ändern.

- **Typ**

  Legen Sie das Protokoll für die PPP-Verbindung fest.

  – PPPoE (Point-to-Point over Ethernet)

    Die PPP-Daten wird in einen Ethernet-Frame eingekapselt.

- **Betrieb**

  Legen Sie fest, ob die PPP-Verbindung aktiviert oder deaktiviert ist.

- **L2-Schnittstelle**

  Legen Sie fest, über welche Schnittstelle die PPP-Verbindung aufgebaut wird. Nur VLANs mit konfigurierten Subnetz auswählbar.

- **Benutzername**

  Geben Sie den Benutzernamen ein. Den Benutzernamen erhalten Sie vom DSL-Anbieter.

- **Passwort**

  Geben Sie das Passwort ein. Das Password erhalten Sie vom DSL-Anbieter.

- **Passwort bestätigen**

  Wiederholen Sie das Passwort.

- **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

Vorgehensweise

1. Legen Sie fest, wie die PPP-Schnittstelle die IP-Adresse bezieht. Folgende Möglichkeiten gibt es:
   - Dynamisch

     Aktivieren Sie den an der PPP-Schnittstelle die Funktion DHCP. Diese Einstellung konfigurieren Sie unter "Layer 3 > Subnetze > Konfiguration".

     Hinweis
     - Bei den Subnets kann maximal eine Schnittstelle eine dynamische IP-Konfiguration haben.

   - Statische IP-Adresse

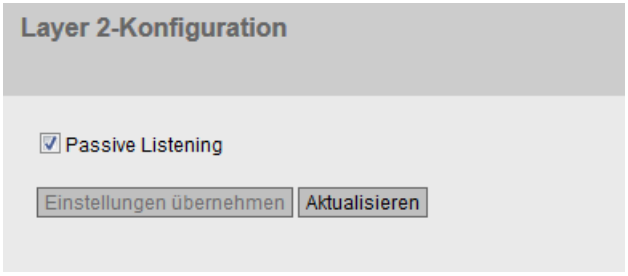
     Deaktivieren Sie den an der PPP-Schnittstelle die Funktion DHCP. Geben Sie die IP-Adresse und die Subnetzmaske ein.
2. Konfigurieren Sie die PPP-Schnittstelle.
3. Wählen Sie bei Operation "Aktiviert" aus, um die PPP-Schnittstelle zu aktvieren.
4. Klicken Sie auf "Einstellungen übernehmen" um die Einstellungen zu übernehmen.

4.7 Menü "Layer 2"

4.7.1 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.

4.7.2 VLAN

4.7.2.1 Allgemein

VLAN-Konfigurationsseite

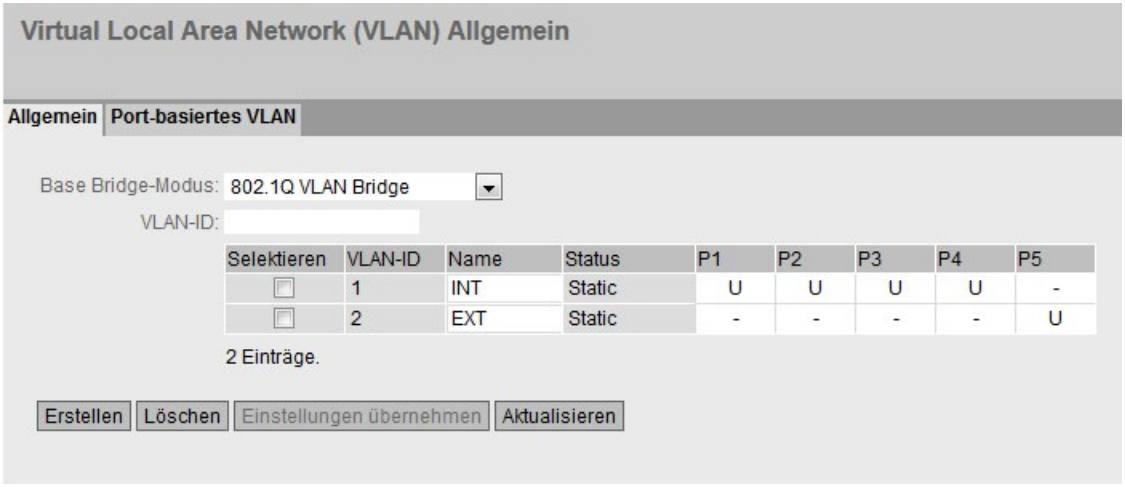
Auf dieser Seite legen Sie fest, ob das Gerät Telegramme mit VLAN-Tags transparent weiterleitet (IEEE 802.1D/VLAN-unaware-Modus) oder VLAN-Informationen berücksichtigt (IEEE 802.1Q/VLAN-aware-Modus). Wenn sich das Gerät im Modus "802.1Q VLAN Bridge" befindet, können Sie VLANs definieren und die Verwendung 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 37)".
- 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

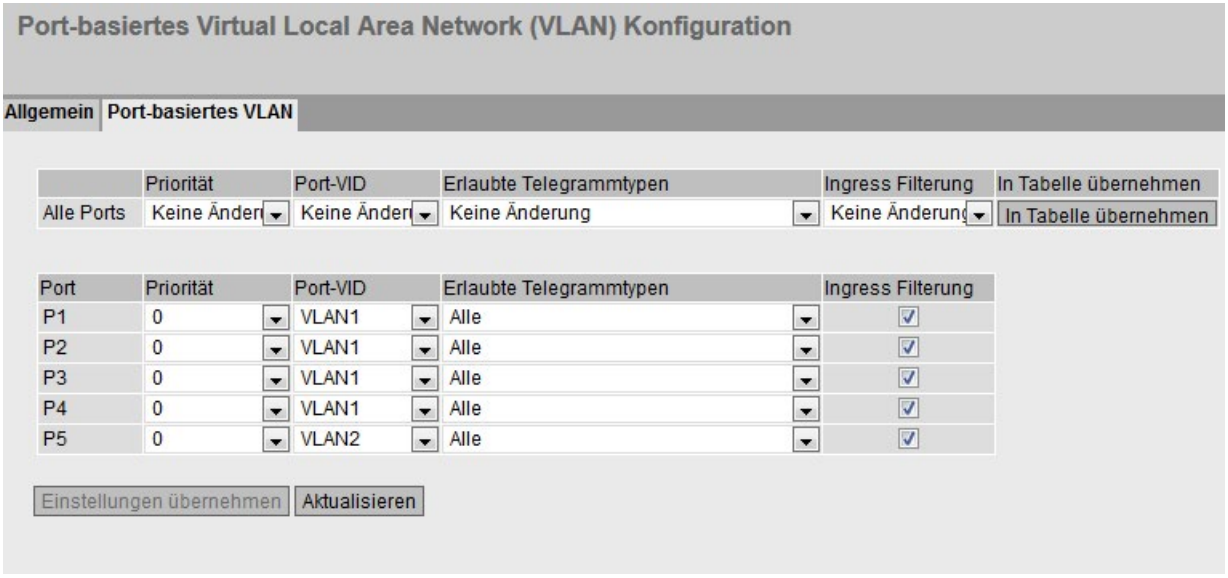
Neues VLAN anlegen

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".

4.7.2.2 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.

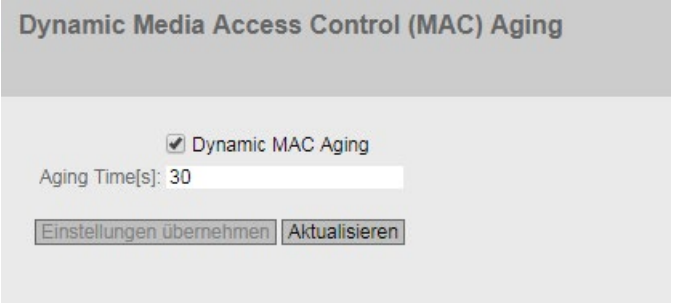
Vorgehensweise zur Konfiguration

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".

4.7.3 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".

4.7.4 Spanning Tree

4.7.4.1 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

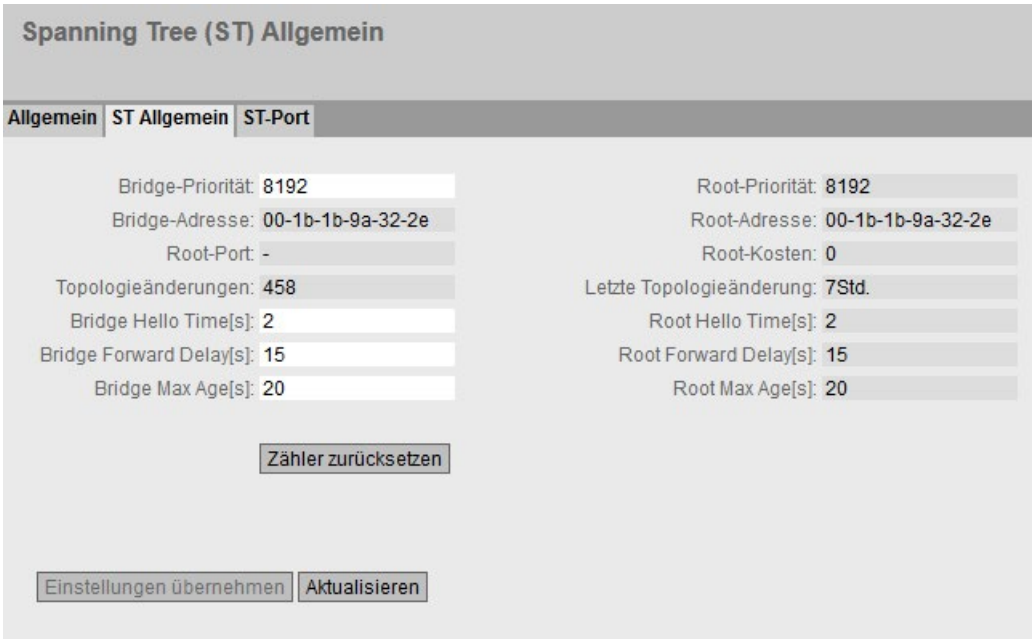
Vorgehensweise

1. Aktivieren Sie das Optionskästchen "Spanning Tree".
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

4.7.4.2 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.

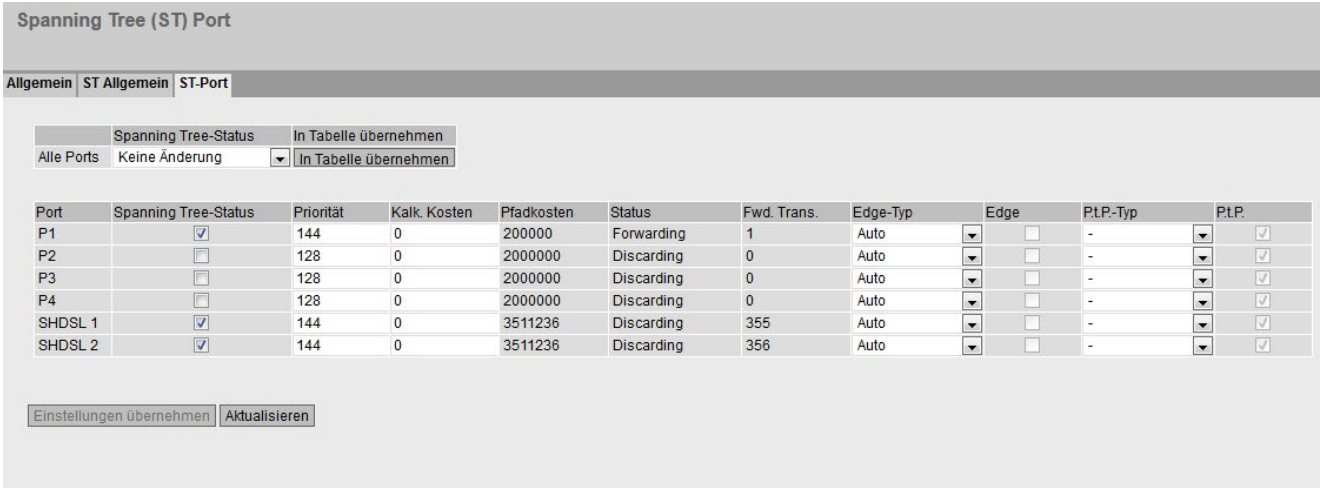
  Werkseinstellung: 20 Sekunden
- **Zähler zurücksetzen**

  Klicken Sie auf diese Schaltfläche, um die Zähler auf dieser Seite zurückzusetzen.

4.7.4.3 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.

4.7.5 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.

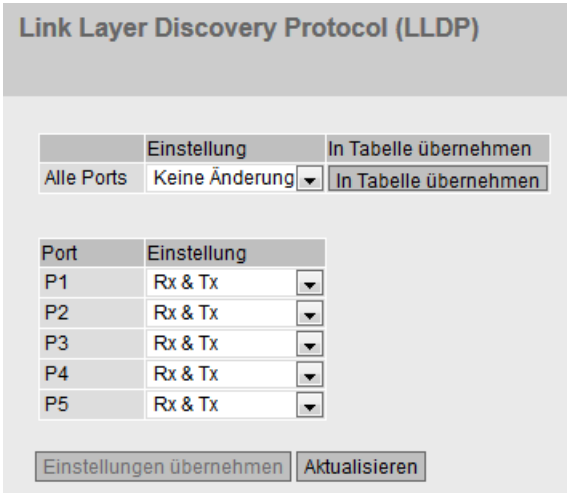
Netzwerkkomponenten, die LLDP unterstützen, verfügen über einen LLDP-Agenten. Der LLDP-Agent versendet in periodischen Abständen Informationen über sich selbst und empfängt Informationen von angeschlossenen Geräten. Die empfangenen Informationen werden in der MIB gespeichert.

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:

- **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.

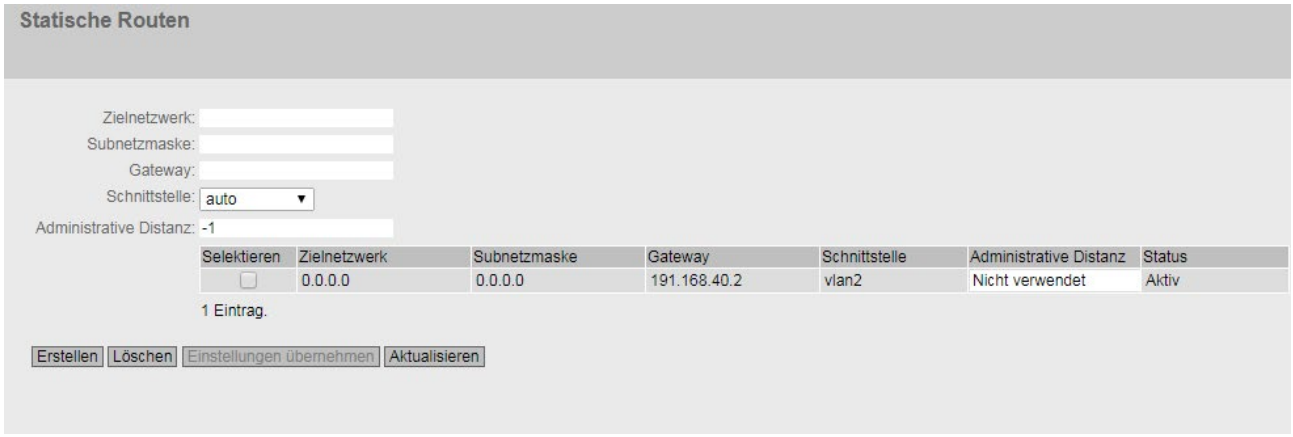
Vorgehensweise

1. Wählen Sie aus der Klappliste "Einstellung" die LLDP-Funktionalität des Ports aus.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

4.8 Menü "Layer 3"

4.8.1 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.
- **Schnittstelle**
  Legen Sie fest, ob die Netzwerkadresse über eine bestimmte Schnittstelle oder über das Gateway (auto) erreichbar ist.
- **Gateway**
  Tragen Sie die IPv4-Adresse des Gateways ein, über den diese Netzwerkadresse 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.

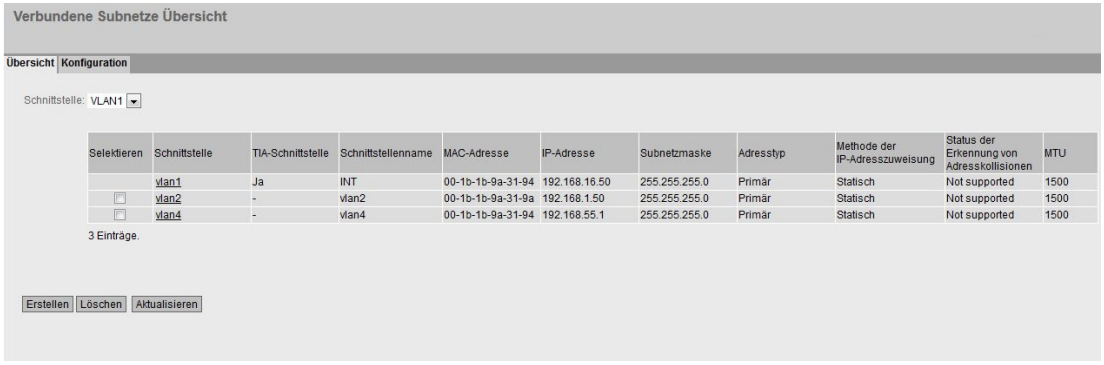
Vorgehensweise

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".

4.8.2 Subnetze

4.8.2.1 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 das ausgewählte TIA-Schnittstelle an.
- **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.

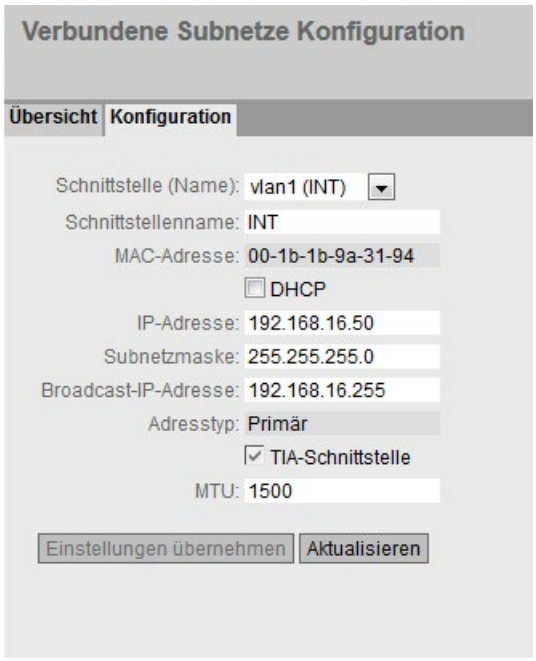
  – Disabled

    Die Funktion zur Erkennung von Adresskollisionen ist deaktiviert.

- **MTU**
  Zeigt die Paketgröße an.

4.8.2.2 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.
- **Schnittstellenname**
  Tragen Sie den Namen für die Schnittstelle ein.
- **MAC-Adresse**

  Zeigt die MAC-Adresse der ausgewählten Schnittstelle an.
- **DHCP**

  Aktivieren oder deaktivieren Sie den DHCP-Client für diese IPv4-Schnittstelle.

- **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.

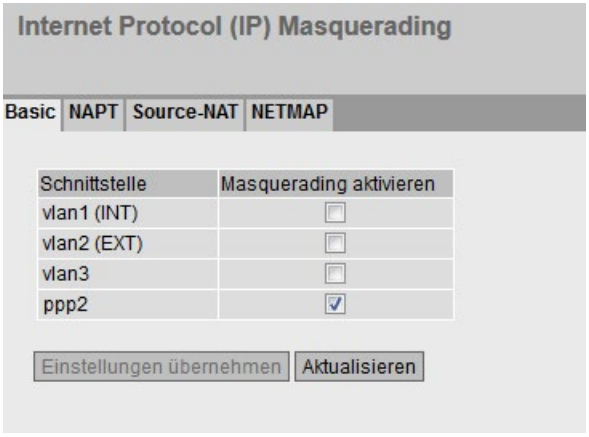
- **Adresstyp**
  Zeigt den Adressen Typ an. Folgende Werte sind möglich:
  - Primär
    Das erste Subnetz der Schnittstelle.
  - Sekundär
    Alle weiteren Subnetze der Schnittstelle.
- **TIA-Schnittstelle**
  Wählen Sie aus, ob diese Schnittstelle zum TIA-Schnittstelle werden soll. Über die TIA-Schnittstelle 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.

4.8.3 NAT

4.8.3.1 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 konfigurierten 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

4.8.3.2 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

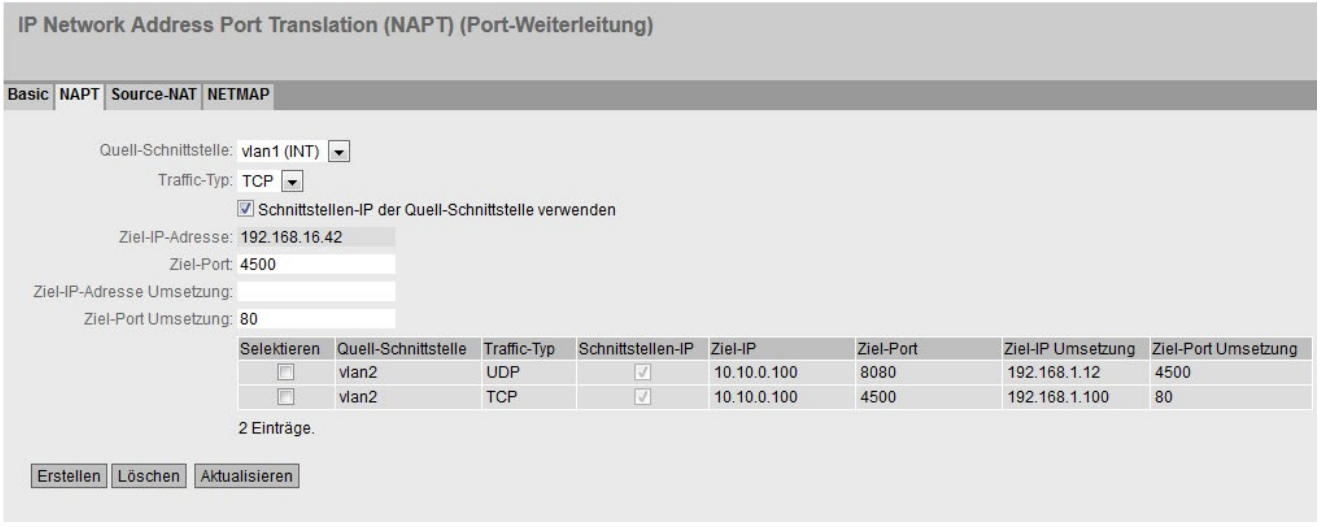
  Die Telegramme werden auf den Port umgesetzt.

- 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-Adresse**

  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**

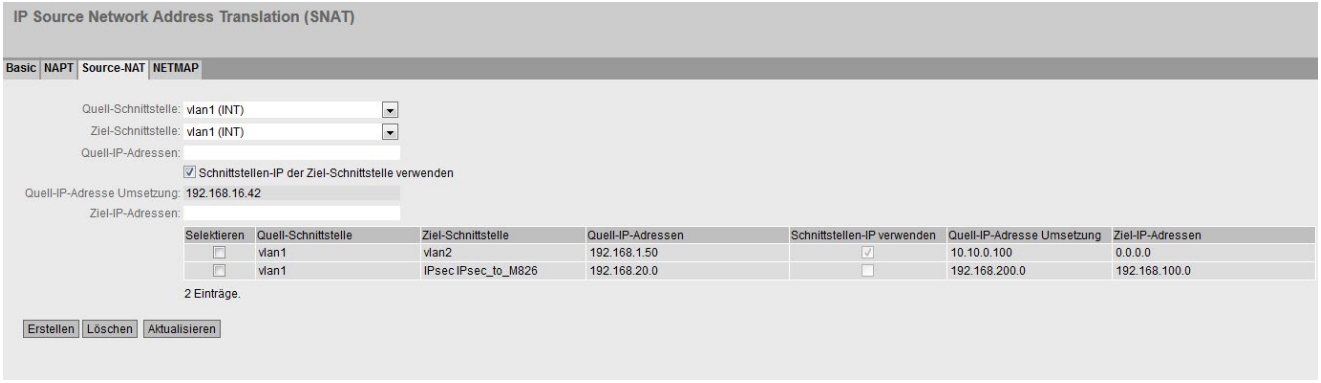
  Zeigt die IP-Adresse Teilnehmers an, an dem die Pakete weitergeleitet werden.

- **Ziel-Port Umsetzung**

  Zeigt an auf welchen Ziel-Port übersetzt wird.

4.8.3.3 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 konfigurierten Subnetz

  – ppp0 bzw. usb0 (nur beim M876-4): 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 der 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-Adress 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.

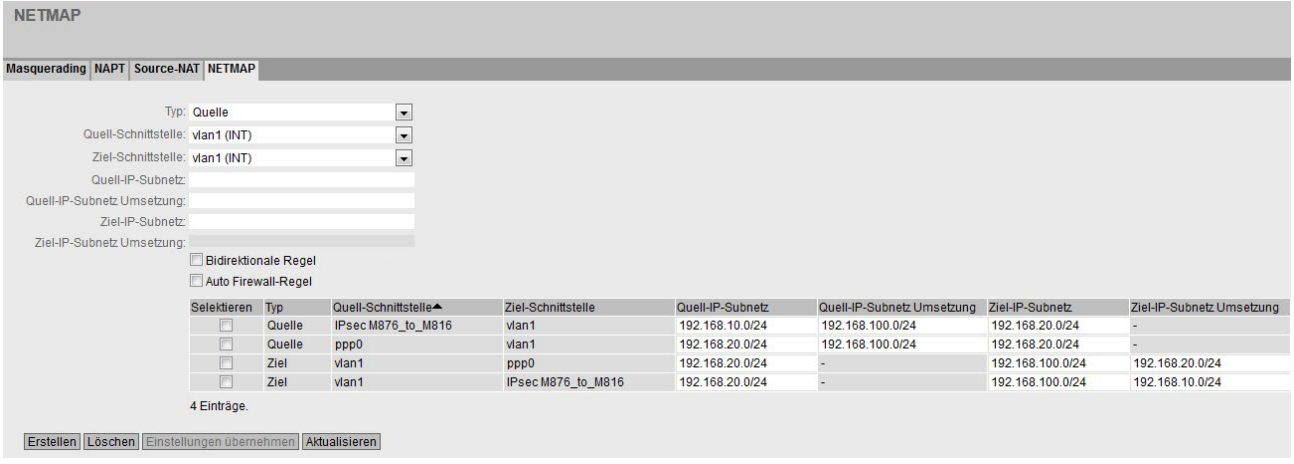
- Quell-IP-Adresse-Umsetzung
  Zeigt die IP-Adresse an, mit der die IP-Adresse der Absender ersetzt wird.
- Ziel-IP-Adressen
  Zeigt die IP-Adressen der Empfänger an, für die eine Adressumsetzung gewünscht ist.

Siehe auch

NAT und Firewall (Seite 50)

4.8.3.4 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 49)".



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 konfigurierten Subnetz

  – ppp0 bzw. usb0 (nur beim M876-4): 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 konfigurierten Subnetz

  – ppp0 bzw. usb0 (nur beim M876-4): 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 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 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 Bearf 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.

Siehe auch

NAT und Firewall (Seite 50)

4.8.4 VRRPv3

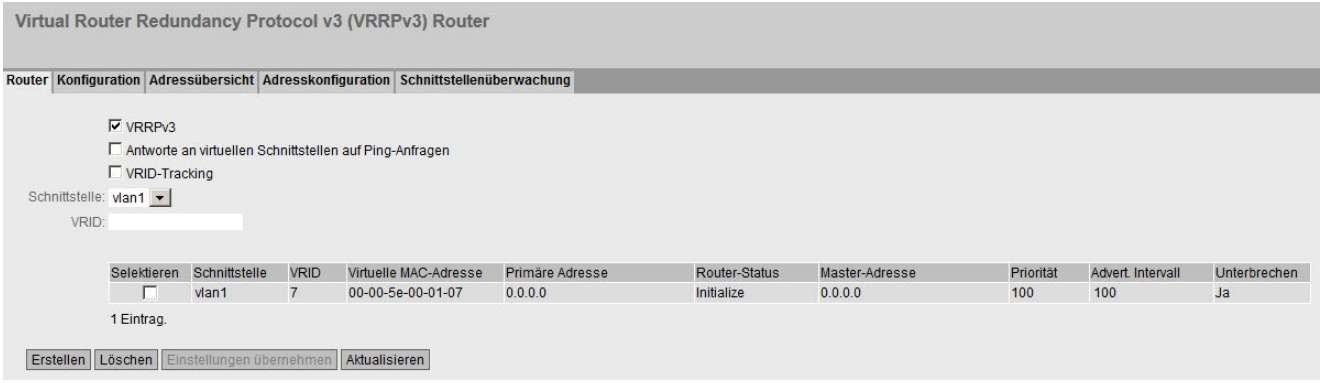
4.8.4.1 Router

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 VRRP-Pakete an das Gerät weitergeleitet werden, ist folgende Firewallregel zu konfigurieren:

Security > Firewall > IP-Protokoll:

- Protokollname: „VRRP“
- Protokollnummer: 112

Security > Firewall > IP-Regeln:

- Protokoll: IPv4
- Aktion: Accept
- Von: <Schnittstelle>
- Nach: Gerät
- Quelle (Bereich): 0.0.0.0/0
- Ziel (Bereich): 224.0.0.18/32
- Dienste: VRRP

Beschreibung

Die Seite enthält Folgendes:

- **VRRPv3**

  Aktivieren oder deaktivieren Sie das Routing über VRRPv3.

- **Antworte an virtuellen Schnittstellen auf Ping-Anfragen**

  Wenn aktiviert, antworten auch die virtuellen IPv4-Adressen auf den Ping.

- **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.

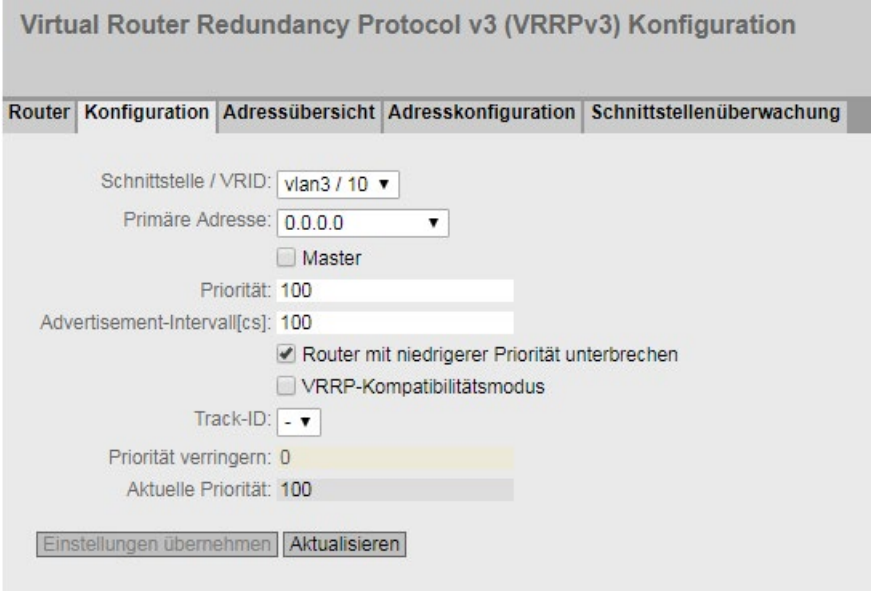
Vorgehensweise

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".

4.8.4.2 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.

- **Master**

  Wenn aktiviert, wird die numerisch kleinste IPv4-Adresse bei "Zugeordnete IP-Adresse" eingetragen. Damit wird die numerisch kleinste IPv4-Adresse des VRRPv3-Routers als virtuelle IP-Adresse des virtuellen Master-Routers verwendet. Die Backup-Router in dieser Gruppe, müssen die Option deaktivieren und die IPv4-Adresse des Routers bei "Zugeordnete IP-Adresse" verwenden.

- **Priorität**

  Gegen 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 in Sekunden ein, nach dem ein Master-Router erneut ein VRRPv3-Paket verschickt.

- **Router mit niedrigerer Priorität unterbrechen**

  Erlauben sie die Bevorzugung zum Rollenwechsel zwischen Backup und Master basierend auf dem Auswahlprozess.

- **VRRP-Kompatibilitätsmodus**

  Wenn aktiviert, sendet und empfängt der VRRPv3-Router für konfigurierte IPv4-Adressen zusätzlich zu den VRRPv3-Telegrammen auch VRRPv2-Telegramme. Nur notwendig, wenn nicht alle VRRP-Router VRRPv3 unterstützen.

- **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

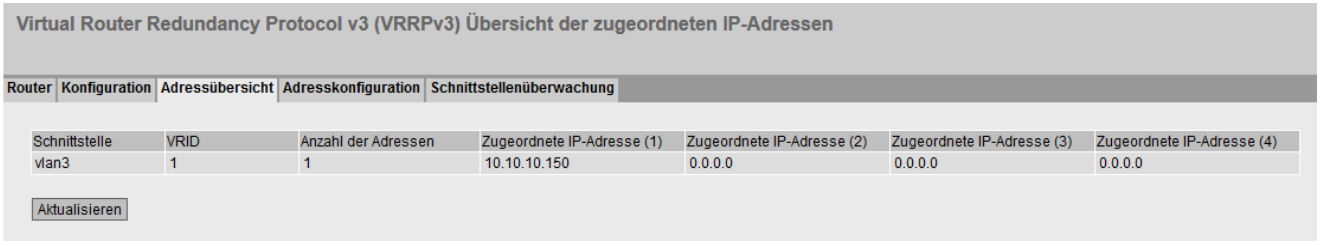
Um einen virtuellen Router als Master-Router zu konfigurieren, gehen Sie folgendermaßen vor:

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. Aktivieren Sie das Optionskästchen "Master".
6. Tragen Sie bei "Advertisement-Intervall" das Zeitintervall ein.
7. Aktivieren Sie das Optionskästchen "Router mit niedrigerer Priorität unterbrechen".
8. Aktivieren Sie das Optionskästchen "VRRP-Kompatibilitätsmodus".
9. Wählen Sie eine Track-ID aus.
10. Geben Sie den Wert ein, um den die Priorität der VRRPv3-Schnittstelle verringert wird.
11. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

4.8.4.3 Adressübersicht

Übersicht

Diese Seite zeigt an, welche IPv4-Adressen der virtuelle Router überwacht. Jeder virtueller 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.

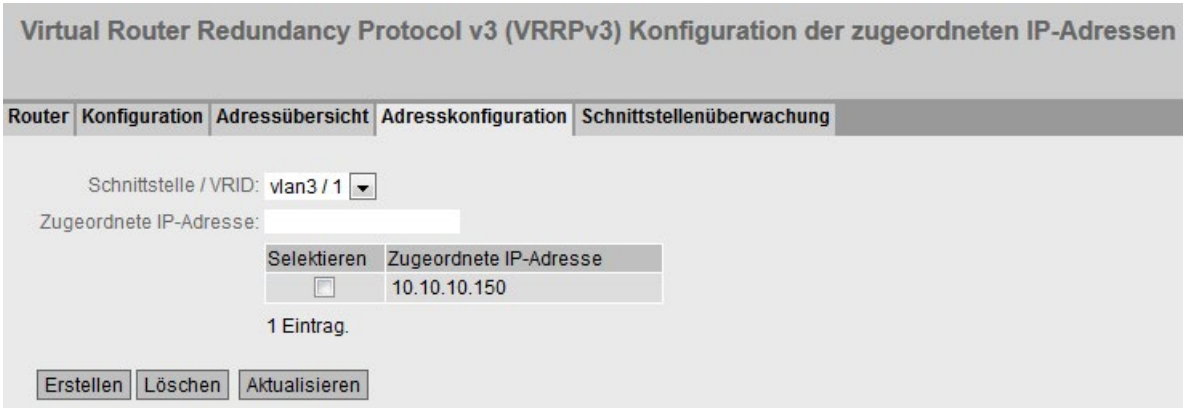
- **Zugeordnete IP-Adresse (1) ...Zugeordnete IP-Adresse (4)**

  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.

4.8.4.4 Adresskonfiguration

Anlegen oder ändern der überwachten IP-Adressen

Auf dieser Seite können Sie die zu überwachenden IPv4-Adressen anlegen, ändern oder löschen. Jeder virtueller 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.

4.8.4.5 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".

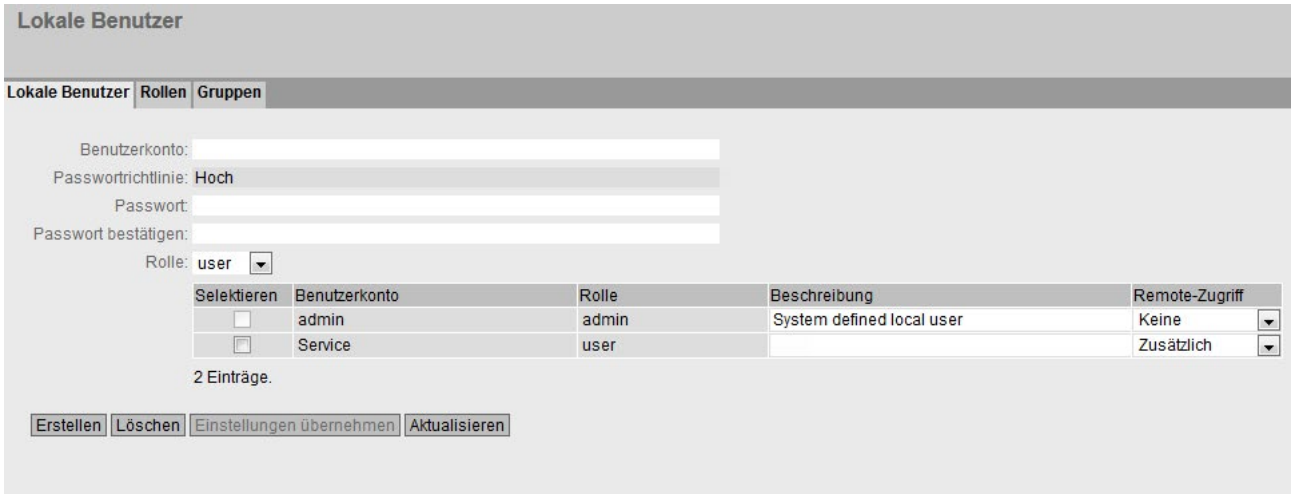
4.9 Menü "Security"

4.9.1 Benutzer

4.9.1.1 Lokale Benutzer

Benutzerkonten

Auf dieser Seite erstellen Sie lokale Benutzeraccounts 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 dürfen folgende Zeichen nicht enthalten: § ? " ; :

  – 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

  – Niedrig

    Passwortlänge: mindestens 6 Zeichen, maximal 128 Zeichen

  Sie konfigurieren die Passwortrichtlinie auf der Seite "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: § und 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.

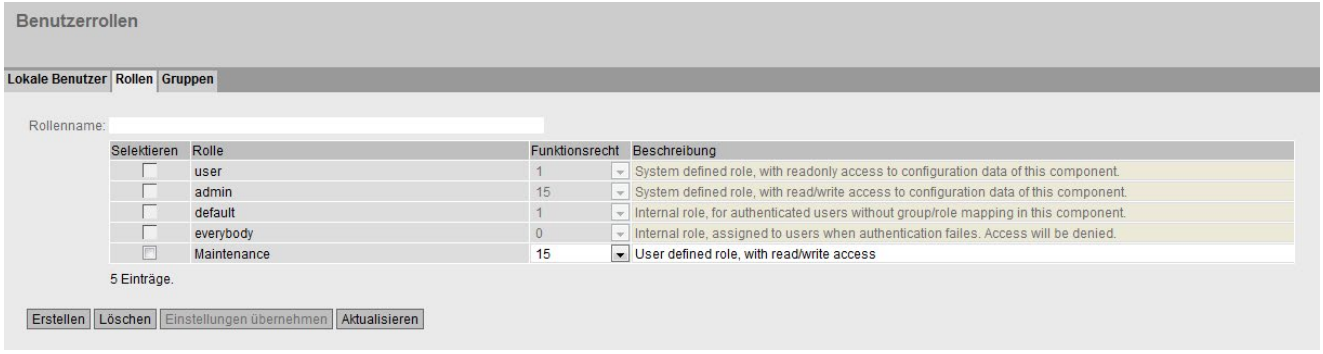
4.9.1.2 Rollen

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.

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.

4.9.1.3 Gruppen

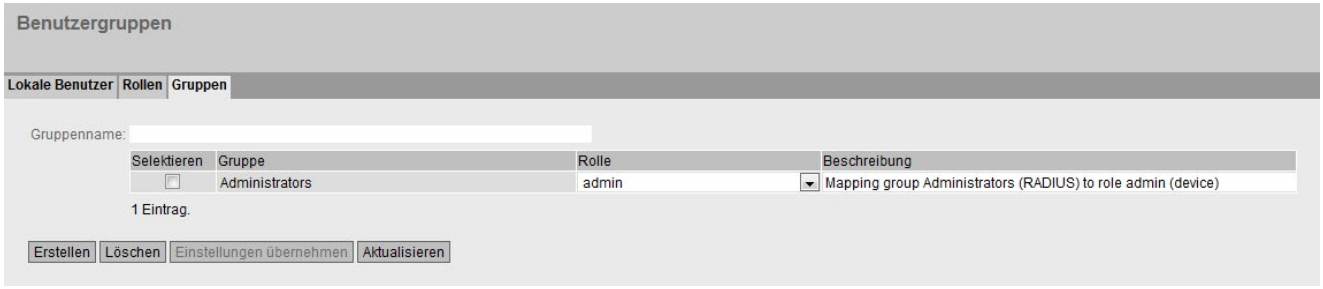
Benutzergruppen

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.

4.9.2 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

  – Niedrig

    Passwortlänge: mindestens 6 Zeichen, maximal 128 Zeichen

- **Neues Passwort**

  Geben Sie das neue Passwort für den ausgewählten Benutzer ein.

  Es dürfen folgende Zeichen nicht enthalten: § und 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.

4.9.3 AAA

4.9.3.1 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 den 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.

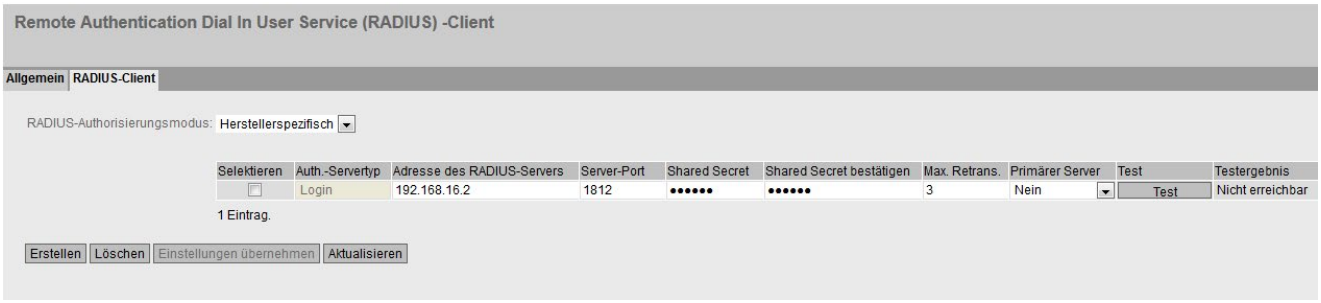
4.9.3.2 RADIUS-Client

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 der angezeigten Felder

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 zurück gibt. 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 zurück gibt 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 IPv4-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.

4.9.4 Zertifikate

4.9.4.1 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 4-1 Teil 1



Bild 4-2 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.

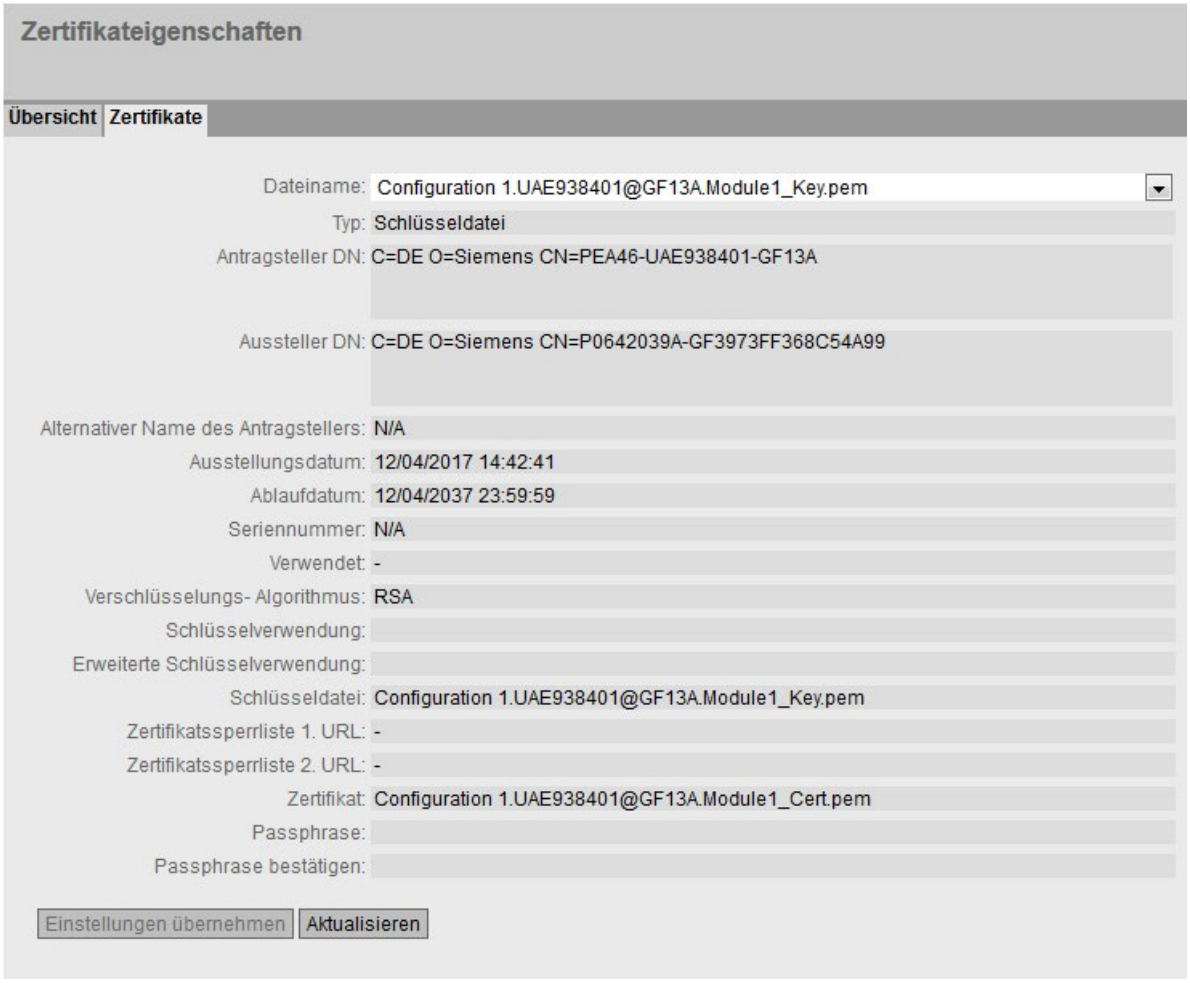
- **Verwendet**

  Zeigt an, welche Funktion das Zertifikat nutzt.

4.9.4.2 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.

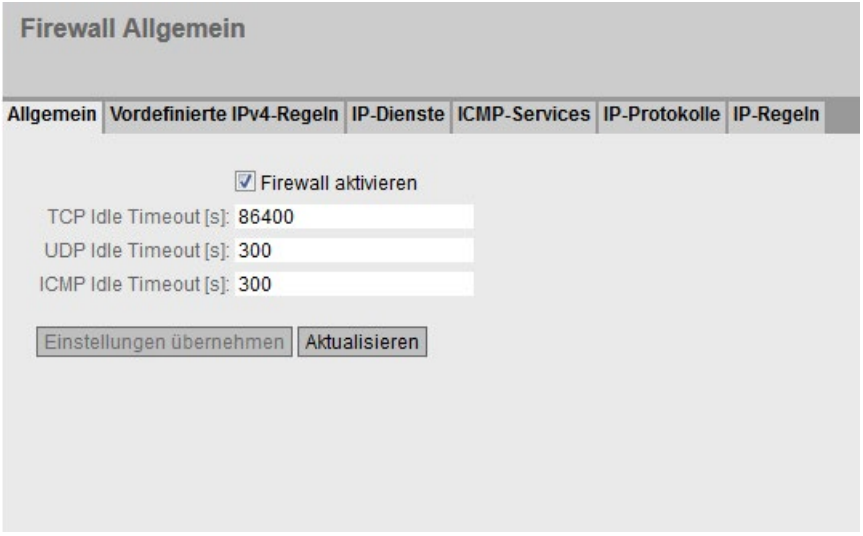
4.9.5 Firewall

4.9.5.1 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.

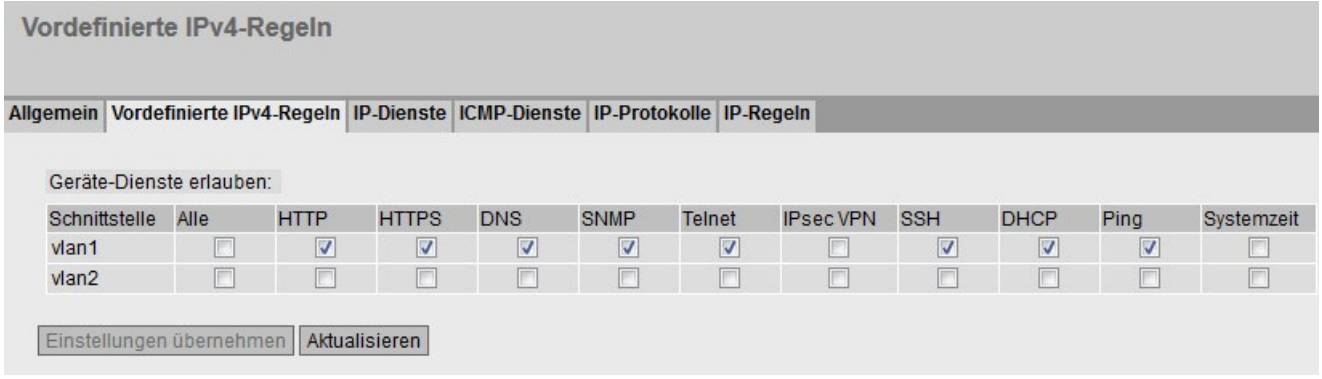
  Der Wertebereich ist 1 bis 21474836.

  Default-Einstellung: 300 Sekunden

4.9.5.2 Vordefinierte IPv4-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.

Hier kann man einstellen, welche Dienste des Gerätes von welcher Schnittstelle/Subnetz aus erreichbar sein sollen.



Beschreibung

- **Schnittstelle**

  Schnittstelle, auf die sich die Einstellung bezieht. Die Liste der Schnittstellen/Subnetze ist dynamisch und richtet sich nach den Einstellungen aus "Layer 3 >Subnetz".

  – VLANx: Erlaubt den Zugriff vom IP-Subnetz auf das Gerät.
- 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 oder SINEMA Server auf die SNMP-Informationen des Geräts zuzugreifen.

– Telnet
Zum unverschlüsselten Zugriff auf das CLI.

– 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

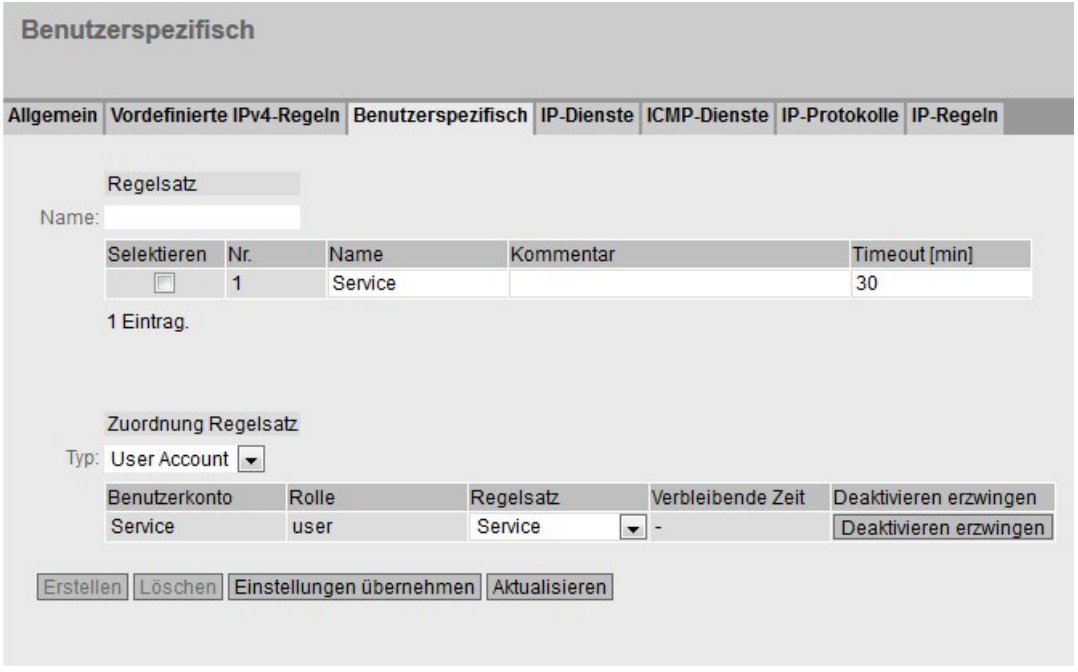
– Systemzeit
Zugriff auf NTP und SNTP.

4.9.5.3 Benutzerspezifisch

Auf dieser Seite definieren Sie benutzerspezifische 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.



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 Regelsatz. Bei Bedarf ist der Name änderbar.

- **Kommentar**

  Kommentar, der den Regelsatz näher beschreibt.

- **Timeout**

  Der Zugriff ist zeitlich begrenzt. Legen Sie die Dauer des Zugriffs fest. Bei Bedarf kann der Benutzer auf der Seite "Benutzerspezifische 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 "Type".

  – User Account

    Der Regelsatz wird über ein Benutzerkonto aktiviert.

  – Digital Input

    Durch das Ansteuern des digitalen Eingangs wird der Regelsatz ausgeführt. Voraussetzung ist, dass unter "System > Ereignis > Konfiguration" beim Ereignis "Firewall" der Eintrag "Digitaler Eingang" aktiviert ist.

Die Tabelle "Benutzerkonto" enthält folgende Spalten:

- Benutzerkonto

  Nur die Benutzer mit dem Remotezugriff "only" oder "additional" werden angezeigt.

- Rolle

  Zeigt die Rolle des Benutzers an.

- Regelsatz

  Legen Sie den Regelsatz fest, der für diesen Benutzer gültig 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 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)

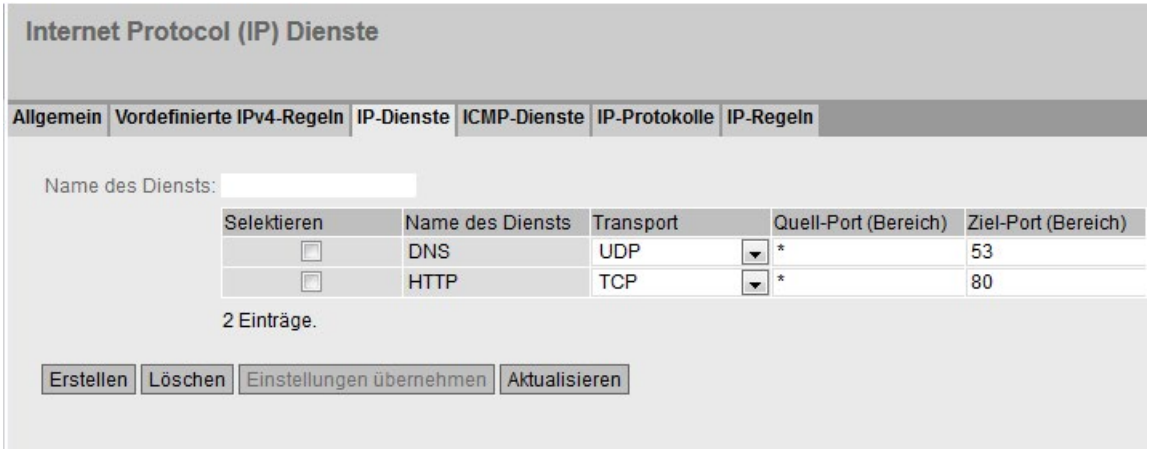
  Tragen Sie die IP-Adresse oder einen IP-Bereich ein, die die IP-Pakete senden darf.

- Status

  Zeigt die verbleibende Zeit für den Zugriff an.

4.9.5.4 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:

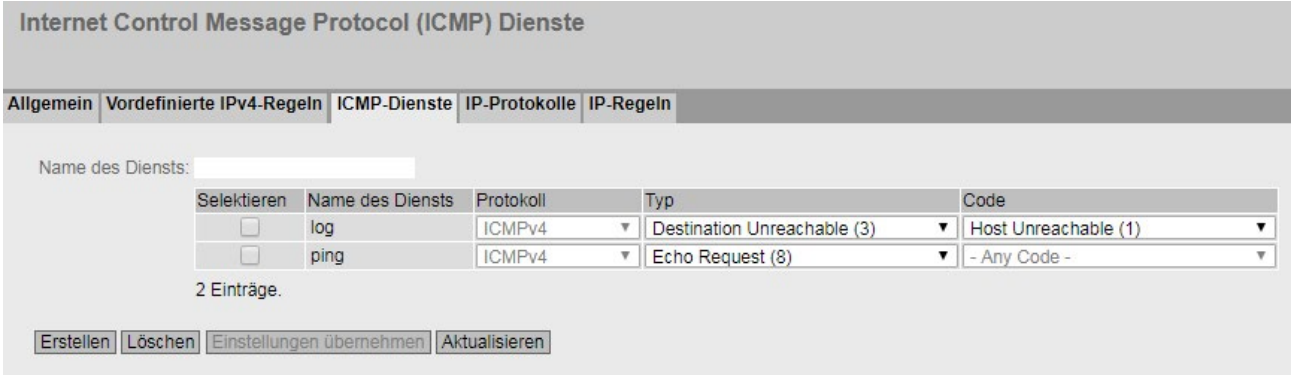
- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Name des Diensts**

  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.

4.9.5.5 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.

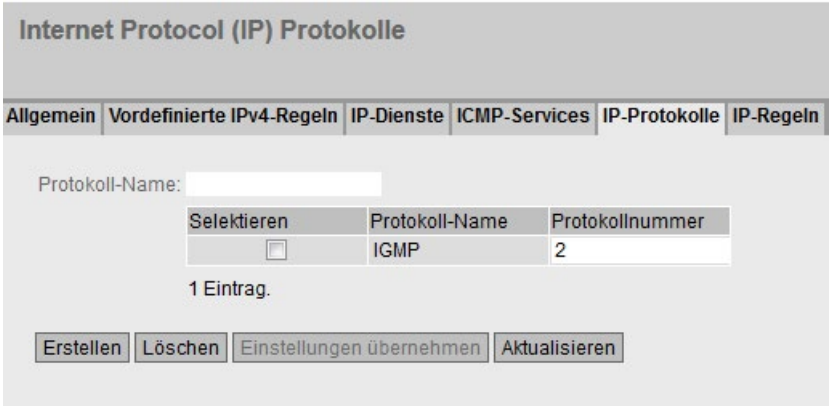
Die Tabelle enthält folgende Spalten:

- **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.

4.9.5.6 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

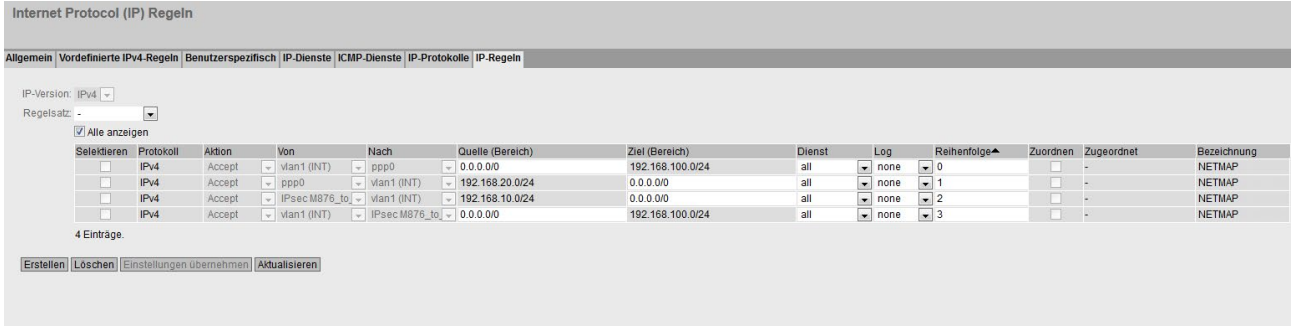
1. Tragen Sie bei "Protokollname" IGMP ein.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen". In der Tabelle wird ein neuer Eintrag erzeugt.
3. Tragen Sie bei "Protokollnummer" 2 ein.

4.9.5.7 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 IPv4-Regeln und
- vor den IP-Regeln, die aufgrund einer Verbindungsprojektierung (SINEMA RC) automatisch angelegt werden.



Beschreibung

- **IP-Version**

  Die Version des IP-Protokolls.

- **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 konfigurierten Subnetz

  – Device: Gerät

  – ppp0 bzw. usb0 (nur beim M876-4): 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 IPv4-Adresse an.

  – IP-Bereich

    Geben Sie den Bereich mit Startadresse "-" Endadresse an, z. B. 192.168.100.10 - 192.168.100.20.

  – Alle IP-Adressen

    Geben Sie "0.0.0.0/0" an.

  – DYNAMIC

    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 > Benutzerspezifisch".

  Ziel (Bereich)

  Tragen Sie die IP-Adresse oder einen IP-Bereich ein, die IP-Pakete empfangen darf.

  – Einzelne IP-Adresse:

    Geben Sie die IPv4-Adresse an.

  – IP-Bereich

    Geben Sie den Bereich mit Startadresse "-" Endadresse an, z. B. 192.168.100.10 - 192.168.100.20.

  – Alle IP-Adressen

    Geben Sie "0.0.0.0/0" an.

- **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

4.9.6 IPsec VPN

4.9.6.1 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

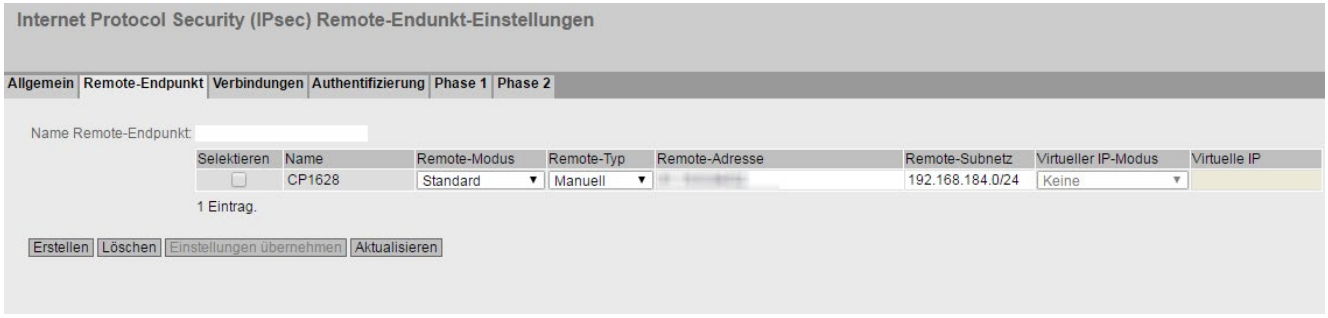
Ablaufdatum ihre Gültigkeit verloren haben. Welche Zertifikatssperrliste verwendet wird, konfigurieren Sie auf der WBM-Seite "Zertifikate (Seite 283)".

- **NAT Keep Alive-Zeitintervall**

  Legen Sie fest, in welchen Zeitabständen 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.

4.9.6.2 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.

  – Im Roadwarrior-Modus teilt die Gegenstelle dem Gerät seinen 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".

4.9.6.3 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 59)".
  - 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".
- **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**

  Tragen Sie das lokale Subnetz ein. Verwenden Sie die CIDR-Schreibweise. Das lokale Netz kann auch nur ein einzelner PC, oder eine andere Untermenge des lokalen Netzes sein.
- **Virtuelle IP anfordern**

  Wenn aktiviert, wird beim Verbindungsaufbau eine virtuelle IP-Adresse von der Gegenstelle angefordert.
- **Timeout [Sek]**

  Nur bei der Einstellung "Auf Anforderung" notwendig. Tragen Sie die Zeitspanne ein, nach der die VPN-Verbindung getrennt wird. Wenn innerhalb dieser Zeit keine Pakete gesendet werden, wird der VPN-Verbindung automatisch getrennt.

4.9.6.4 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 Authentisierungsverfahren 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".
- **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.

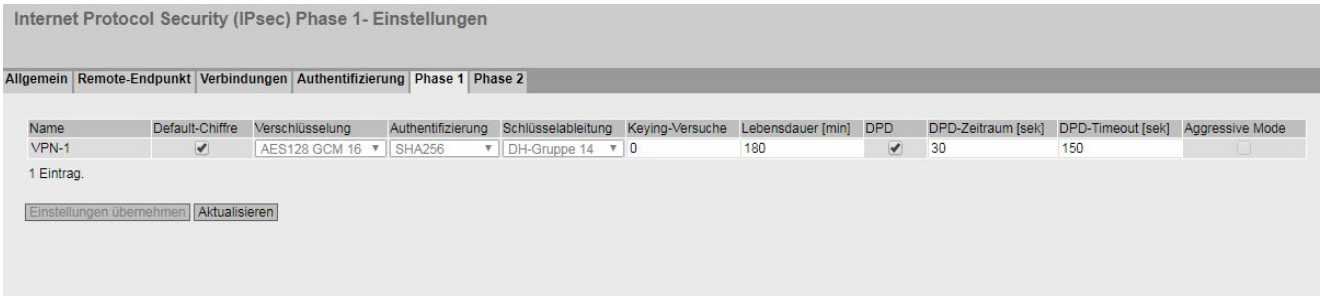
- **Remote-Zertifikat**
  Wählen Sie das Gegenstellenzertifikat aus. Nur geladene Gegenstellenzertifikate sind auswählbar.

  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.

4.9.6.5 Phase 1

Phase 1: Verschlüsselungsvereinbarung und Authentisierung (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".

- **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".

  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 Authentisierung 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]**

  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.

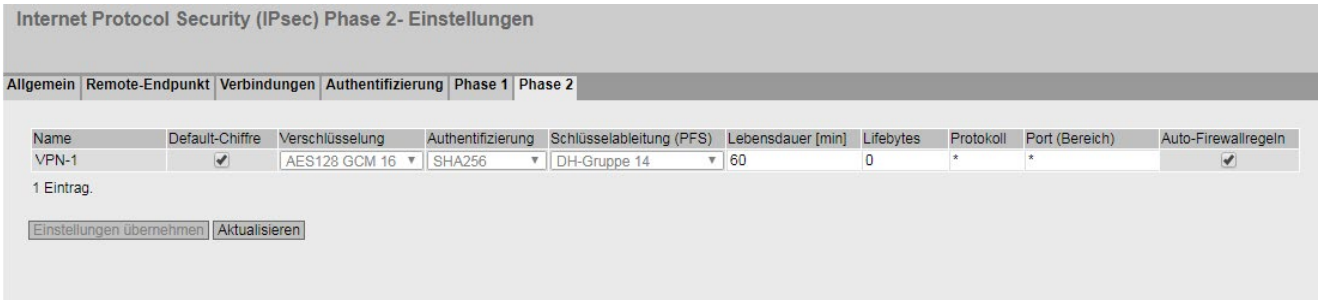
- **Aggressive Mode**
  - Deaktiviert:
    Main Mode wird verwendet.
  - Aktiviert
    Aggressive Mode wird verwendet

  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.

4.9.6.6 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 (Encryption, Authentication, Key Derivation) enthalten. Um eine VPN-Verbindung aufzubauen, muss der VPN-Verbindungspartner mindestens eine dieser Kombinationen unterstützen. Weitere Informationen dazu erhalten Sie bei "IPsec VPN".

- **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".

  Hinweis

  Die AES-Modi CCM und GCM beinhalten separate Mechanismen für die Authentisierung von Daten. Wenn Sie bei "Verschlüsselung" einen Modus AES x CCM oder AES x GCM verwenden, dann wird dieser auch zur Authentisierung 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**
  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:

  – None: Für die Phase 2 werden keine separaten Schlüssel ausgetauscht. Damit ist Perfect Forward Secrecy (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.

- **Lifebytes**
  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 angelegt.

  – deaktiviert
  Sie müssen selbst die Firewall-Regeln anlegen.

4.9.7 OpenVPN Client

4.9.7.1 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.

4.9.7.2 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 "Create", 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 59)".

  – 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".

  – 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 angelegt.

  – 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 49)".

4.9.7.3 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**

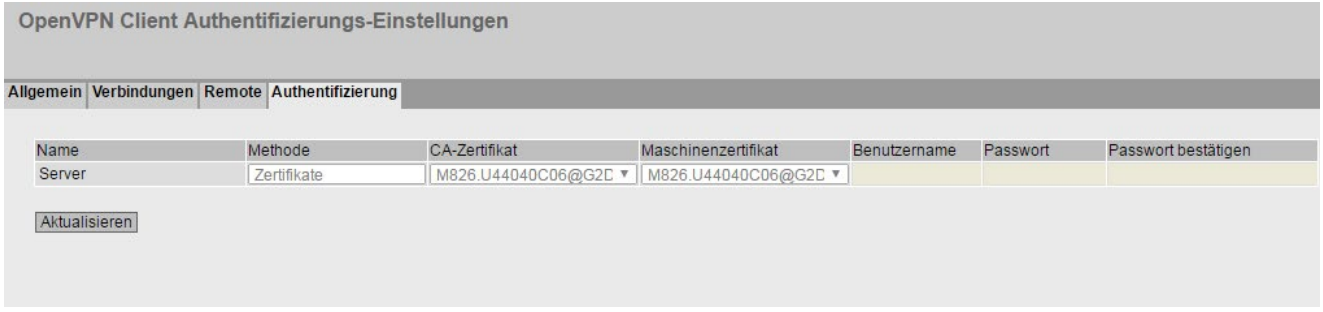
  Legen Sie fest, für welches Protokoll die OpenVPN-Verbindung genutzt werden soll.

- **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.

4.9.7.4 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.

- **Methode**

  Wählen Sie das Authentifizierungsverfahren aus. Voraussetzung für die VPN-Verbindung ist, dass die Gegenstelle das gleiche Authentisierungsverfahren 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.

- **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**

  Bestätigen Sie das Passwort.

Instandhalten und Warten

5

5.1 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!
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 Konfigurations Modus 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".

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.

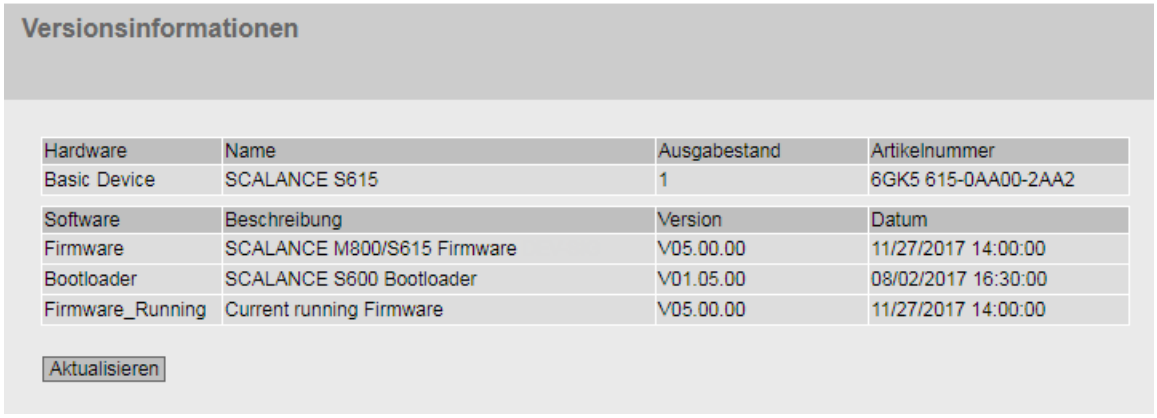
Firmware-Update über SFTP

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.



5.2 Firmware-Update über WBM 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 Schnittstellen (P1 – P4) 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 (P1 - P4) 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 dem Primary Setup Tool überprüfen.

   Hinweis

   Verwenden von TFTP

   Wenn Sie unter Windows 7 auf TFTP zugreifen wollen, achten Sie darauf, dass die entsprechende Windowsfunktion im Betriebssystem freigeschaltet ist.

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.

5.3 Wiederherstellen der Werkseinstellungen

ACHTUNG
Bisherige Einstellungen
Durch das Zurücksetzen werden alle von Ihnen vorgenommenen Einstellungen durch werksseitige Voreinstellungen überschrieben.

ACHTUNG
Versehentliches Rücksetzen
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" in 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.

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

A

A.1 Format der Syslog-Meldungen

Die Geräte generieren Syslog-Meldungen (UDP-Standardport 514) gemäß RFC 5424, die die folgenden Felder enthalten.

PRIORITY

Innerhalb **PRIORITY** steht codiert die Priorität der Syslog-Meldung aufgeteilt in ein Severity- und Facility-Feld.

- Facility
- Severity

VERSION

- Auf 1 gesetzt.

HEADER

- TIMESTAMP gemäß RFC 3339
- Hostname
- APPNAME, PROGID und MSGID: Sind keine Angaben bekannt, wird das Zeichen "-" ausgegeben.

STRUCTURED DATA

- timeQuality-Block

MESSAGE:

- ASCII-String in Englisch

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

Hinweis

Weitere Informationen über die Bedeutung der Felder sind im RFC 5424 nachzulesen.

https://tools.ietf.org/html/rfc5424

A.2 Parameter in Syslog-Meldungen

Die Syslog-Meldungen können folgende Parameter beinhalten:

Parameter	Beschreibung	Mögliche Werte oder Beispiel
ip address	IPv4- oder IPv6-Adresse	P-Adresse nach RFC1035 oder RFC4291 Abschnitt 2.2
src port dest port	Port, der als deizimale Nummer dargestellt wird. Format: %d	0 ... 65535
client mac dest mac src mac	MAC-Adresse 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. Format: %s	Mögliche Einträge von: UDP | TCP | WBM | Telnet | SSH | Console | TFTP | SFTP
group	Zeichenkette, die die Gruppe anhand ihres Namens identifiziert Format: %s	it-service
user name	Zeichenkette, die den authentifizierten Benutzer anhand seines Namens identifiziert ohne Leerzeichen Format: %s	maier
local interface	Symbolischer Name für die lokale Schnittstelle Format: %s	Console
action user name	Identifiziert den Benutzer anhand seines Namens. Dies ist nicht der authentifizierte Benutzer Format: %s	Peter.Maier
role	Symbolischer Name für die Gruppenrolle Format: %s	Administrator
time minute timeout	Minutenanzahl Format: %d	44
time second	Sekundenanzahl Format: %d	44
failed login count	Anzahl der fehlgeschlagenen Loggins Format: %d	10
max sessions	Anzahl der Sitzungen Format: %d	10
vap	Symbolischer Name der virtuellen Access Point-Schnittstelle Format: (%s) oder (%s %s)	VAP1.1
status reason	Zusätzliche Statusinformation als lesbare Zeichenfolge. Sie kann mehrere Wörter enthalten. Damit die Zeichenfolge analysiert werden kann, muss sie mit „(“ beginnen und mit „)“ enden.	(Invalid group cipher) (Unknown peer)

Parameter	Beschreibung	Mögliche Werte oder Beispiel
wlan interface	Symbolischer Name der WLAN-Schnittstelle Format: %s	WLAN1
ssid	SSID in ASCII-Darstellung beliebig viele Leerzeichen Format: %s	MyWLAN
channel	Bezeichnung des Kanal Format: %s	12
signal strength	Signalstärke Format: %d	12
version	Bezeichnung der Version ohne Leerzeichen Format: %s	V1.0.3SP1
resource	Durch das Schutzstufenkonzept geschützter Ressourcenname ohne Leerzeichen Format: %s	FullReadAccess
trigger condition	Zeichenkette für eine Auslösebedingung, mit der die betreffende Funktion aktiviert wird ohne Leerzeichen Format: %s	E/A-Pin FB-88
trigger pin	Zeichenkette für einen IO-Pin, der das Ereignis ausgelöst ohne Leerzeichen Format: %s	DI1
firewall rule	Zeichenkette für einen Firewall-Regelsatz mit Leerzeichen Format: %s	Rule1
subject	Zeichenkette für den Betreff im Zertifikat. Wird verwendet als Teil der zertifikatbasierten Authentifizierung mit Leerzeichen und muss zusätzlich Unicode-Zeichen enthalten Format: (% S) oder (% S% S) bei UTF8-Code.	(Peter Maier)
config detail	Zeichenkette für die Konfiguration mit Leerzeichen 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) Format: %d	52
network interface	Symbolischer Name einer Netzwerkschnittstelle Format: %s	vlan 1

A.3 Syslog-Meldungen

In diesem Kapitel werden ausgewählte Syslog-Meldungen beschrieben. Die Auswahl orientiert sich an der IEC 62443-3-3. Damit können Sie diese Ereignisse in ein zentrales Überwachungssystem (SIEM) integrieren.

Identifizierung und Authentifizierung von menschlichen Nutzern

Log-Meldung	Console: User {user name} logged in.
Norm	IEC 62443-3-3 Reference: SR1.1
Beschreibung	Gültige Anmeldeinformationen, die bei der lokalen Anmeldung angegeben werden.
Beispiel	Console: User admin logged in.
Severity	Info
Facility	local0

Log-Text	Console: Default user {user name} logged in.
Norm	IEC 62443-3-3 Reference: n/a (NERC-CIP 007-R5)
Beschreibung	Benutzer mit Standardbenutzername und Kennwort ist angemeldet.
Beispiel	Console: Default user admin logged in.
Severity	Info
Facility	local0

Log-Text	{protocol}: User {user name} logged in from {ip address}.
Norm	IEC 62443-3-3 Reference: SR1.1
Beschreibung	Gültige Anmeldeinformationen, die bei der Remote-Anmeldung angegeben werden.
Beispiel	WBM: User admin logged in from 192.168.0.1.
Severity	Info
Facility	local0

Log-Text	{protocol}: Default user {user name} logged in from {ip address}.
Norm	IEC 62443-3-3 Reference: n/a (NERC-CIP 007-R5)
Beschreibung	User logged in with default user name and password.
Beispiel	SSH: Default user admin logged in from 192.168.0.1.
Severity	Info
Facility	local0

Log-Text	Console: User {user name} logged out.
Norm	IEC 62443-3-3 Reference: SR1.1
Beschreibung	Benutzersitzung beendet - Abmeldung erfolgt.
Beispiel	Console: User admin logged out.
Severity	Info
Facility	local0

Log-Text	{protocol}: User {user name} logged out from {ip address}.
Norm	IEC 62443-3-3 Reference: SR1.1
Beschreibung	Benutzersitzung beendet - Abmeldung erfolgt.
Beispiel	SSH: User admin logged out from 192.168.0.1.
Severity	Info
Facility	local0

Log-Text	Console: User {user name} failed to log in.
Norm	IEC 62443-3-3 Reference: SR1.1
Beschreibung	Falscher Benutzername oder falsches Passwort (Anmeldeinformationen) bei der lokalen Anmeldung angegeben.
Beispiel	Console: User testuser failed to log in.
Severity	Warning
Facility	local0

Log-Text	{protocol}: User {user name} failed to log in from {ip address}.
Norm	IEC 62443-3-3 Reference: SR1.1
Beschreibung	Falscher Benutzername oder falsches Kennwort (Anmeldeinformationen) bei der Remote-Anmeldung angegeben.
Beispiel	SSH: User testuser failed to log in from 192.168.0.1.
Severity	Warning
Facility	local0

Identifizierung und Authentifizierung von Geräten (Zugriff über Firewall)

Log-Text	{firewall action accept}(1) in:{network interface} out:{network interface} len:{length} s-mac:{src mac} d-mac:{dest mac} s-ip:{ip address} d-ip:{ip address} {protocol}:{src port}->{dest port}
Norm	IEC 62443-3-3 Reference: SR 1.2
Beschreibung	Ein bekanntes Gerät hat eine Verbindung angefordert.
Beispiel	ACCEPT(1) in:vlan1 out:ppp0 len:52 s-mac:58:EF:68:B3:FA:CE d-mac:00:1B:1B:A7:5B:D8 s-ip:172.23.1.6 d-ip:158.85.11.68 tcp:53788->443

Severity	Info or Warning or Error (configurable)
Facility	local0

Log-Text	{firewall action reject}(1) in:{network interface} out:{network interface} len:{length} s-mac:{src mac} d-mac:{dest mac} s-ip:{ip address} d-ip:{ip address} {protocol}:{src port}->{dest port}
Norm	IEC 62443-3-3 Reference: SR 1.2
Beschreibung	Ein unbekanntes Gerät hat eine Verbindung angefordert. Anfrage wurde abgelehnt.
Beispiel	REJECT(1) in:vlan1 out:ppp0 len:52 s-mac:58:EF:68:B3:FA:CE d-mac:00:1B:1B:A7:5B:D8 s-ip:172.23.1.6 d-ip:217.194.40.109 tcp:53773->443
Severity	Info or Warning or Error (configurable)
Facility	local0

Identifizierung und Authentifizierung von Geräten (Verbindung über TIA Portal Cloud Connector)

Log-Text	Cloud Connector:Connection number {config detail} from {ip address} established.
Norm	IEC 62443-3-3 Reference: SR 1.2
Beschreibung	Ein bekanntes Gerät hat eine Verbindung angefordert. (Verbindung über TIA Portal Cloud Connector)
Beispiel	Cloud Connector: Connection number 10 from 192.168.55.111 established.
Severity	Info
Facility	local0

Log-Text	Cloud Connector: Connection number {config detail} from {ip address} closed.
Norm	IEC 62443-3-3 Reference: SR 1.2
Beschreibung	Ein unbekanntes Gerät hat eine Verbindung angefordert. Anfrage wurde abgelehnt. (Verbindung über TIA Portal Cloud Connector)
Beispiel	Cloud Connector: Connection number 6 from 192.168.55.111 closed.
Severity	Info
Facility	local0

Nutzerkontenverwaltung

Log-Text	{protocol}: User {user name} changed own password.
Norm	IEC 62443-3-3 Reference: SR1.3
Beschreibung	Benutzer hat sein Passwort geändert.
Beispiel	WBM: User admin changed own password.
Severity	Info
Facility	local0

Log-Text	{protocol}: User {user name} changed password of user {action user name}.
Norm	IEC 62443-3-3 Reference: SR1.3
Beschreibung	Benutzer hat ein anderes Passwort geändert.
Beispiel	Console: User admin changed password of user test.
Severity	Info
Facility	local0

Log-Text	{protocol}: User {user name} created user-account {action user name}.
Norm	IEC 62443-3-3 Reference: SR1.3
Beschreibung	Der Administrator hat ein neues Konto erstellt.
Beispiel	WBM: User admin created user-account joachim.
Severity	Info
Facility	local0

Log-Text	{protocol}: User {user name} deleted user-account {action user name}.
Norm	IEC 62443-3-3 Reference: SR1.3
Beschreibung	Der Administrator hat ein vorhandenes Konto gelöscht.
Beispiel	WBM: User admin deleted user-account joachim.
Severity	Info
Facility	local0

Verwaltung der Kennungen

Log-Text	{protocol}: User {user name} created group {group}.
Norm	IEC 62443-3-3 Reference: SR1.4
Beschreibung	Der Administrator hat eine Gruppe erstellt.
Beispiel	WBM: User admin created group it-service.
Severity	Info
Facility	local0

Log-Text	{protocol}: User {user name} deleted group {group}.
Norm	IEC 62443-3-3 Reference: SR1.4
Beschreibung	Der Administrator hat eine vorhandene Gruppe gelöscht.
Beispiel	WBM: User admin deleted group it-service.
Severity	Info
Facility	local0

Erfolglose Anmeldeversuche

Log-Text	User {user name} account is locked for {time} minutes after {failed login count} unsuccessful login attempts.
Norm	IEC 62443-3-3 Reference: SR1.11
Beschreibung	Bei zu vielen fehlgeschlagenen Anmeldungen wurde das entsprechende Benutzerkonto für einen bestimmten Zeitraum gesperrt.
Beispiel	User admin account is locked for 10 minutes after 30 unsuccessful login attempts.
Severity	Warning
Facility	local0

Zugriff über nicht vertrauenswürdige Netze (IPsec)

Log-Text	[IKE] <{connection name}|{config detail}> IKE_SA {connection name}[{config detail}] established between {ip address}[{config detail}]...{ip address}[{config detail}]
Norm	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1)
Beschreibung	VPN-Verbindung ist hergestellt. (IPsec)
Beispiel	[IKE] <c1|3> IKE_SA c1[1] established between 192.168.55.210[lokal].. 192.168.55.211[remote]
Severity	Info
Facility	local0

Log-Text	[IKE] <{connection name}|{config detail}> deleting IKE_SA {connection name}[{config detail}] between {ip address}[{config detail}]...{ip address}[{config detail}]
Norm	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1)
Beschreibung	VPN-Tunnel ist geschlossen. (IPsec)
Beispiel	[IKE] <c1|3> deleting IKE_SA c2[1] between 192.168.55.211[lokal].. 192.168.55.210[remote]
Severity	Info
Facility	local0

Log-Text	[IKE] <{connection name}|{config detail}> received AUTHENTICATION_FAILED notify error
Norm	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R3)
Beschreibung	Authentifizierung der VPN-Verbindung ist fehlgeschlagen (IPsec).
Beispiel	[IKE] <c1|1> received AUTHENTICATION_FAILED notify error
Severity	Warning
Facility	local0

Zugriff über nicht vertrauenswürdige Netze (OpenVPN)

Log-Text	OVPN_{connection name}[{config detail}]: Initialization Sequence Completed
Norm	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1)
Beschreibung	VPN-Verbindung ist hergestellt. (OpenVPN)
Beispiel	OVPN_Conn_1[2427]: Initialization Sequence Completed
Severity	Info
Facility	local0

Log-Text	OpenVPN connection {connection name} has been deactivated.
Norm	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1)
Beschreibung	VPN-Verbindung wurde geschlossen (OpenVPN).

Beispiel	OpenVPN connection c1 has been deactivated.
Severity	Critical
Facility	local0

Zugriff über nicht vertrauenswürdige Netze (SINEMA Remote Connect)

Log-Text	SINEMA RC - State of Digital Input changed to HIGH. SINEMA RC - OpenVPN connection established.
Norm	IEC 62443-3-3 Reference: SR 1.13
Beschreibung	Fernzugriff ist erlaubt. (SINEMA RC, Digitaler Eingang)
Beispiel	SINEMA RC - State of Digital Input changed to HIGH. SINEMA RC - OpenVPN connection established.
Severity	Info
Facility	local0

Log-Text	SINEMA RC - Received Wakeup SMS. SINEMA RC - OpenVPN connection established.
Norm	IEC 62443-3-3 Reference: SR 1.13
Beschreibung	Fernzugriff ist erlaubt. (SINEMA RC, Wakeup SMS)
Beispiel	SINEMA RC - Received Wakeup SMS. SINEMA RC - OpenVPN connection established.
Severity	Info
Facility	local0

Log-Text	SINEMA RC - State of Digital Input changed to LOW. SINEMA RC - OpenVPN terminated.
Norm	IEC 62443-3-3 Reference: SR 1.13
Beschreibung	Fernzugriff verweigert (SINEMA RC, Digitaler Eingang)
Beispiel	SINEMA RC - State of Digital Input changed to LOW. SINEMA RC - OpenVPN terminated.
Severity	Info
Facility	local0

Log-Text	SINEMA RC - Received Shutdown SMS. SINEMA RC - OpenVPN terminated.
Norm	IEC 62443-3-3 Reference: SR 1.13
Beschreibung	Fernzugriff verweigert (SINEMA RC, Wakeup SMS)
Beispiel	SINEMA RC - Received Shutdown SMS. SINEMA RC - OpenVPN terminated.
Severity	Info
Facility	local0

Durchsetzung der Autorisierung (Zugriff über benutzerspezifische Firewall)

Log-Text	User specific firewall user "{user name}" activated rule set "{firewall rule}" with ip address "{ip address}". Timeout is set to {timeout} minutes.
Norm	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R2)
Beschreibung	Benutzer hat sich an der benutzerspezifischen Firewall angemeldet. (USF Digital User Login)
Beispiel	User specific firewall user "usf" activated rule set "rs1" with ip address "172.23.1.14". Timeout is set to 5 minutes.
Severity	Info
Facility	local0

Log-Text	User specific firewall user "{user name}" activated rule set "{firewall rule}" with ip address "{ip address}". Timeout is set to {timeout} minutes.
Norm	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R2)
Beschreibung	Benutzer hat sich an der benutzerspezifischen Firewall angemeldet. (USF Digital Input Login)
Beispiel	User specific firewall digital input {trigger pin} activated rule set "{firewall rule}" with ip address "{ip address}".
Severity	Info
Facility	local0

Log-Text	User specific firewall user "{user name}" ruleset "{firewall rule}" time expired.
Norm	IEC 62443-3-3 Reference: SR 2.1
Beschreibung	Zugriff auf die benutzerspezifische Firewall verweigert. Zugriffszeit abgelaufen. (USF User Logout)
Beispiel	User specific firewall user "usf" ruleset "rs1" time expired.
Severity	Warning
Facility	local0

Log-Text	User specific firewall user "{user name}" logged out by administrator configura-tion.
Norm	IEC 62443-3-3 Reference: SR 2.1
Beschreibung	Zugriff auf die benutzerspezifische Firewall verweigert. Der Geräteadministrator hat den Benutzer über die Schaltfläche "Deaktiviert erzwingen "deaktiviert . (USF user force logout by admin)
Beispiel	User specific firewall user "usf" logged out by administrator configuration.
Severity	Warning
Facility	local0

Log-Text	User specific firewall user "{user name}" deactivated by administrator configuration.
Norm	IEC 62443-3-3 Reference: SR 2.1
Beschreibung	Zugriff auf die benutzerspezifische Firewall verweigert. Der Geräteadministrator hat den Benutzer deaktiviert. (USF user deactivated by admin)
Beispiel	User specific firewall user "usf" deactivated by administrator configuration.
Severity	Warning
Facility	local0

Log-Text	User specific firewall digital input {trigger pin} deactivated rule set "{firewall rule}".
Norm	IEC 62443-3-3 Reference: SR 2.1
Beschreibung	Zugriff auf die benutzerspezifische Firewall verweigert. entsprechende Regelsatz wurde deaktiviert. (USF Digital Input Logout)
Beispiel	User specific firewall digital input 1 deactivated rule set "rs1".
Severity	Warning
Facility	local0

Sitzungssperrung

Log-Text	The session of user {user name} was closed after {time} seconds of inactivity.
Norm	IEC 62443-3-3 Reference: SR2.5
Beschreibung	Die aktuelle Sitzung wurde aufgrund der Inaktivität gesperrt.
Beispiel	The session of user admin was closed after 60 seconds of inactivity.
Severity	Warning
Facility	local0

Beendigung einer Fernzugriffssitzung

Log-Text	[JOB] <{connection name}|{config detail}> deleting CHILD_SA after {time second} seconds of inactivity
Norm	IEC 62443-3-3 Reference: SR 2.6
Beschreibung	Die Remote-Sitzung wurde nach Inaktivitätszeit beendet. (IPsec)
Beispiel	[JOB] <to_Baugruppe1|21> deleting CHILD_SA after 20 seconds of inactivity
Severity	Info
Facility	local0

Log-Text	OVPN_{connection name}[{config detail}]: [{config detail}] Inactivity timeout (--ping- restart), restarting
Norm	IEC 62443-3-3 Reference: SR 2.6
Beschreibung	Die Remote-Sitzung wurde nach Inaktivitätszeit beendet. (OpenVPN)
Beispiel	OVPN_c1[26296]: [router] Inactivity timeout (--ping-restart), restarting
Severity	Info
Facility	local0

Begrenzung der Anzahl gleichzeitiger Sitzungen

Log-Text	{protocol}: The maximum number of {max sessions} concurrent login session exceeded.
Norm	IEC 62443-3-3 Reference: SR2.7
Beschreibung	Die maximale Anzahl gleichzeitiger Sitzungen ist überschritten.
Beispiel	WBM: The maximum number of 8 concurrent login session exceeded.
Severity	Warning
Facility	local0

In diesem Kapitel werden ausgewählte Syslog-Meldungen beschrieben. Die Auswahl orientiert sich an der IEC 62443-3-3. Damit können Sie diese Ereignisse in ein zentrales Überwachungssystem (SIEM) integrieren.

Nicht-Abstreitbarkeit (Konfiguration ändern)

Log-Text	Device configuration changed.
Norm	IEC 62443-3-3 Reference: SR2.12
Beschreibung	Die Gerätekonfiguration ist dauerhaft geändert.
Beispiel	Device configuration changed.
Severity	Info
Facility	local0

Kommunikationsintegrität

Log-Text	[IKE] <{connection name}|{config detail}> received invalid DPD sequence number {config detail} (expected {config detail}), ignored
Norm	IEC 62443-3-3 Reference: SR 3.1
Beschreibung	Integritätsprüfung fehlgeschlagen. (IPsec)
Beispiel	[IKE] <c1|1> received invalid DPD sequence number 10 (expected 12), ignored
Severity	Info
Facility	local0

Log-Text	OVPN_{connection name}[{config detail}]: Authenticate/Decrypt packet error: packet HMAC authentication failed
Norm	IEC 62443-3-3 Reference: SR 3.1
Beschreibung	Integritätsprüfung ist fehlgeschlagen (OpenVPN).
Beispiel	OVPN_c1[25409]: Authenticate/Decrypt packet error: packet HMAC authentication failed
Severity	Warning
Facility	local0

A.3.1 Syslog-Meldungen SR7.4

Wiederherstellung des Automatisierungssystems

Log-Text	{protocol}: Loaded file type Firmware {version} (restart required).
Norm	IEC 62443-3-3 Reference: SR7.4
Beschreibung	Firmware-Update ist erfolgreich hochgeladen.
Beispiel	TFTP: Loaded file type Firmware V02.00.00 (restart required).
Severity	Info
Facility	local0

Log-Text	{protocol}: User {user name} loaded file type Firmware {version} (restart required).
Norm	IEC 62443-3-3 Reference: SR7.4
Beschreibung	Firmware-Update ist erfolgreich hochgeladen.
Beispiel	WBM: User admin loaded file type Firmware V02.00.00 (restart required).
Severity	Info
Facility	local0

Log-Text	{protocol}: Failed to load file type Firmware.
Norm	IEC 62443-3-3 Reference: SR7.4
Beschreibung	Fehler beim Bereitstellen des Firmware-Updates.
Beispiel	WBM: Failed to load file type Firmware.
Severity	Warning
Facility	local0

Log-Text	{protocol}: Loaded file type Config (restart required).
Norm	IEC 62443-3-3 Reference: SR7.4
Beschreibung	Die Konfiguration wird angewendet.
Beispiel	TFTP: Loaded file type Config (restart required).
Severity	Info
Facility	local0

Log-Text	{protocol}: Loaded file type ConfigPack (restart required).
Norm	IEC 62443-3-3 Reference: SR7.4
Beschreibung	Die Konfiguration wird angewendet.
Beispiel	TFTP: Loaded file type ConfigPack (restart required).
Severity	Info
Facility	local0

Log-Text	{protocol}: User {user name} loaded file type Config (restart required).
Norm	IEC 62443-3-3 Reference: SR7.4
Beschreibung	Die Konfiguration wird angewendet.
Beispiel	WBM: User admin loaded file type Config (restart required).
Severity	Info
Facility	local0

Log-Text	{protocol}: User {user name} loaded file type ConfigPack (restart required).
Norm	IEC 62443-3-3 Reference: SR7.4
Beschreibung	Die Konfiguration wird angewendet.
Beispiel	WBM: User admin loaded file type ConfigPack (restart required).
Severity	Info
Facility	local0

Index

A

Abmeldung
  automatisch, 184
Aging
  Dynamic MAC Aging, 234
Auf Werkseinstellungen zurücksetzen, 322
Aufstellungsort, 130
Authentifizierung, 164

B

Basic Wizard
  starten, 73
Benutzergruppen, 274
Bestellnummer, 94
Bridge, 111, 236
  Bridge Priority, 111, 236
  Root Bridge, 111, 236
Bridge Max Age, 112, 237
Bridge Max Hop Count, 112

C

CA-Zertifikat, 53
Certificates, 284
Configuration
  PPP, 225
CoS (Class of Service), 39
CoS-Priorisierung, 39
C-PLUG, 25
  Formatieren, 192
  Konfiguration speichern, 192

D

DCP Discovery, 197
DCP-Server, 125
Dead Peer Detection, 57
Device
  System, 128
DHCP
  Client, 203
DST
  Sommerzeit, 168, 170

E

E-Mail-Funktion, 152
  Ereignisse, 152
  Netzüberwachung, 152

F

Fehlerstatus, 101
Fehlerüberwachung
  Verbindungszustandsänderung, 187
Forward Delay, 112, 237

G

geografische Koordinaten, 130
Gerät
  Basic Wizard, 76
Gerät zurücksetzen, 322, 322
Gerätezertifikat, 53
Glossar, 4
Gruppen, 274

H

Hardwareausgabestand, 94
Hello Time, 112, 237
Hersteller, 93
Herstellerkennung, 94

I

ICMP, 36
Information
  ARP Table, 95
  Gruppen, 123
  Hardware, 92
  IPsec VPN, 107
  LLDP, 104
  Log Table, 96, 100
  OpenVPN Client, 110
  Rolle, 122
  Security, 119, 121
  Security Log, 98
  SINEMA RC, 108

SNMP, 104, 104
Software, 92
Spanning Tree, 113
Start Page, 86
Versions, 92
IP-Adresse
Konfiguration, 248
IPsec VPN
NETMAP, 50
Source-NAT, 50
IPsec-Verfahren, 54
IPv4
VRRPv3, 65
IPv4 Routing
Routing-Tabelle, 106

K

KEY-PLUG, 25, 194, 194
Formatieren, 192
Konfigurationsmodus, 127

L

Layer 2, 227
Layer 3, 194, 194
LLDP, 104, 241
Log Table
Event Log, 96
Firewall Log, 100
Security Log, 98

N

NAPT
konfigurieren, 251
NAT
1-to-1 NAT, 256
konfigurieren, 250
Masquerading, 49
NAPT, 49
NAT-Traversal, 57
NETMAP, 50
Source-NAT, 50
NAT-Traversal, 57
Netzüberwachung, 152
Neustart, 131
NTP
Client, 176
Server, 182

P

Passwort, 268, 276
Ping, 196
PLUG, 194, 194
C-PLUG, (C-PLUG)
Port
Portkonfiguration, 219
PPP
Configuration, 225
Overview, 223
Projektierungshandbücher, 322
Punkt zu Punkt, 64

R

RADIUS, 278
redundante Netzwerke, 111, 236
RESET-Taster, 185
Rollen, 271
Root Max Age, 112, 237
Routing, 243
ICMP, 36
IPv4 Routing-Tabelle, 106
statische Routen, 243
RSTP, 235
Rücksetzen, 131

S

SELECT/SET-Taster, 185
Seriennummer, 94
Serverzertifikat, 53
Service & Support, 4
SFTP
Laden/Speichern, 142
SHA-Algorithmus, 161
Sicherheitseinstellungen, 160
SIMATIC NET-Glossar, 4
SIMATIC NET-Handbuch, 4
SMTP
Client, 125
SNAT
konfigurieren, 253
SNMP, 40, 126, 156, 160
Benutzer, 163
Gruppen, 160
SNMPv1, 40
SNMPv2c, 40
SNMPv3, 40
Trap, 159
Übersicht, 104

Softwareausgabestand, 94
Source-NAT
  Masquerading, 49
Spanning Tree, 235
  Information, 113
  Rapid Spanning Tree, 64
SSH
  Server, 125
Standard-Modus, 54
Startseite, 86
Stateful Inspection Firewall, 46
Subnetz
  Konfiguration, 248
  Übersicht, 245
Subnetzmaske, 33
Syslog, 186
  Client, 125
System
  Allgemeine Informationen, 128
  Device, 128
  Konfiguration, 124
  Load and Save via HTTP, 134
Systemereignisprotokoll
  Agent, 186
Systemereignisse
  Konfiguration, 147
  Severity Filter, 151

T

Taster, 185
Telnet
  Server, 125
TFTP
  Laden/Speichern, 138
Training, 4

U

Uhrzeit
  manuelle Einstellung, 78, 166
  NTP-Client, 78
  SIMATIC Time Client, 180
  SNTP (Simple Network Time Protocol), 173
  Systemzeit, 77, 166
  Uhrzeitsynchronisation, 173
  UTC-Zeit, 175, 179
  Zeitzone, 175, 179

V

Verfügbare Systemfunktionen, 20
VLAN, 37
  Port VID, 233
  Priorität, 233
  Tag, 233
  VLAN-ID, 39
  VLAN-Tag, 38
Voraussetzung
  Spannungsversorgung, 18
VPN-Verbindung
  Status, 107
  Status OpenVPN-Client, 110
VRRP
  VRRPv3 Adressenkonfiguration (IPv4), 265
  VRRPv3 Adressenübersicht (IPv4), 264
  VRRPv3 Konfiguration (IPv4), 261
  VRRPv3 Router (IPv4), 258
VRRPv3
  Backup-Router, 65
  Master-Router, 65
  Schnittstellenüberwachung, 266
  Virtueller Router, 65
  VRRPv3-Router, 65
  VRRPv3-Statistik, 116

W

Wartungsdaten, 93
Web Based Management, 67
  Voraussetzung, 67
Werkseinstellung, 322
Werksseitige Voreinstellung, 322

Z

Zeiteinstellung, 126