SIEMENS

SIMATIC NET

Industrial Ethernet Security SCALANCE S615 Web Based Management

Projektierungshandbuch

04/2015

C79000-G8900-C388-01

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

C79000-G8900-C388-01
℗ 04/2015 Änderungen vorbehalten

Vorwort

Gültigkeitsbereich

Dieses Projektierungshandbuch behandelt das folgenden Produkt:

- SCALANCE S615

Das Projektierungshandbuch gilt für folgende Softwareversion:

- SCALANCE S615 Firmware ab Version V04.00

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:

- Getting Started SCALANCE S615

  Dieses Dokument zeigt anhand von Beispielen die Projektierung des SCALANCE S615.

- Betriebsanleitung SCALANCE S615

  Dieses Dokument finden Sie auf den Internetseiten 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 Internetseiten des Siemens Industry Online Support. Es enthält Informationen zur Installation, Konfiguration und Bedienung der Anwendung SINEMA Remote Connect Server.

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

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 Beitrags-ID:

  50305045 (http://support.automation.siemens.com/WW/view/de/50305045)

Security-Hinweise

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Lösungen, Maschinen, Geräten und/oder Netzwerken unterstützen. Sie sind wichtige Komponenten in einem ganzheitlichen Industrial Security-Konzept. Die Produkte und Lösungen von Siemens werden unter diesem Gesichtspunkt ständig weiterentwickelt. Siemens empfiehlt, sich unbedingt regelmäßig über Produkt-Updates zu informieren.

Für den sicheren Betrieb von Produkten und Lösungen von Siemens ist es erforderlich, geeignete Schutzmaßnahmen (z. B. Zellenschutzkonzept) zu ergreifen und jede Komponente in ein ganzheitliches Industrial Security-Konzept zu integrieren, das dem aktuellen Stand der Technik entspricht. Dabei sind auch eingesetzte Produkte von anderen Herstellern zu berücksichtigen. Weitergehende Informationen über Industrial Security finden Sie unter http://www.siemens.com/industrialsecurity.

Um stets über Produkt-Updates informiert zu sein, melden Sie sich für unseren produktspezifischen Newsletter an. Weitere Informationen hierzu finden Sie unter http://support.automation.siemens.com.

Firmware

Die Firmware ist signiert und verschlüsselt. Damit 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:

- DC_LicenseSummaryScalanceS615_74.htm

Marken

Marken

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

SCALANCE

Inhaltsverzeichnis

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
  - IPsecVPN für bis zu 20 Verbindungen
- SINEMA RC-Client
- Proxy-Server

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
  - SNTP
- 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
- SMTP-Client

1.2 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	P1 ... P4
IP-Adresse	192.168.1.1
Subnetzmaske	255.255.255.0
Benutzername	admin (nicht änderbar)
Passwort	admin Das Passwort muss nach der Erstanmeldung oder nach einem "Restore Factory Defaults and Restart" geändert werden

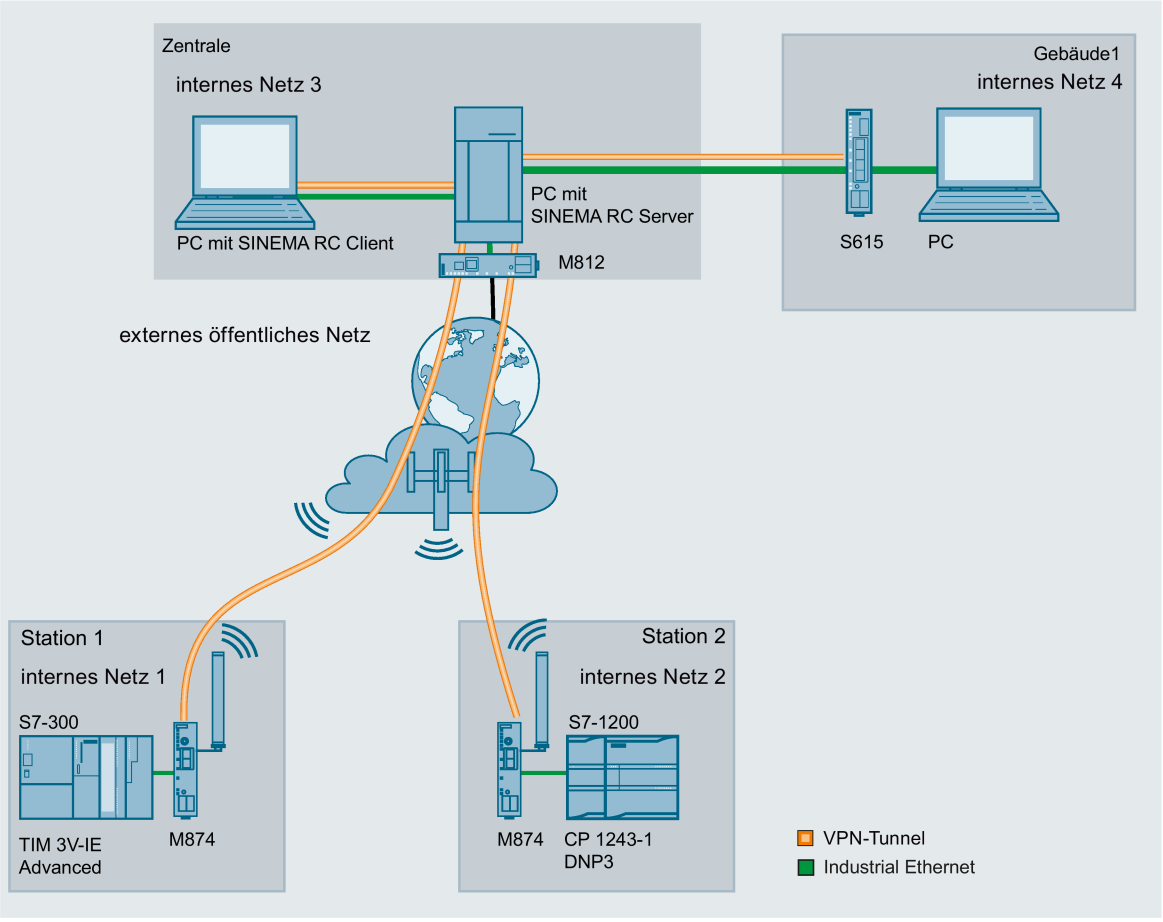
Weitere Informationen dazu finden Sie bei "Web Based Management (Seite 37)" und bei "Starten und anmelden (Seite 39)".

1.3 Konfigurationsbeispiele

1.3.1 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 SCLANCE M874 oder SCALANCE S615, die zu dem SINEMA RC-Server einen VPN-Tunnel aufbauen. In der Zentrale baut derSINEMA 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 RCServer 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 122).
4. Richten Sie die angeschlossenen Applikationen der Anlage für die Datenkommunikation ein.

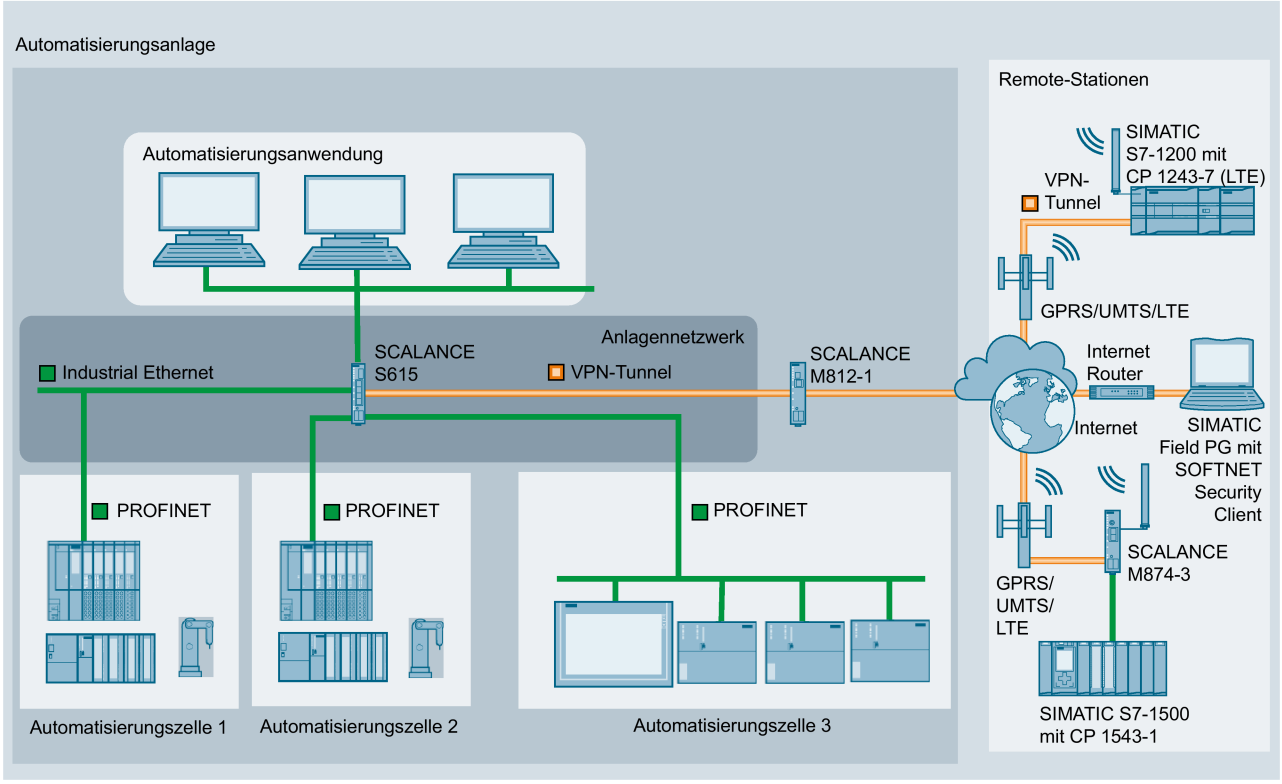
1.3.2 Sicherer Zugriff mit S615

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.



1.4 Digitaler Eingang / Ausgang

Einleitung

Die Geräte verfügen über einen digitalen Ein- / Ausgang.

Der Anschluss erfolgt über zwei 2-poligen Klemmenblöcke. Informationen zur Pin-Belegung finden Sie in der Betriebsanleitung der Geräte.

Anwendungsbeispiel

- Digitaler Eingang z. B. zum Aufbauen einer VPN-Verbindung
- Digitaler Ausgang z. B. zum Signalisieren bestehender VPN-Verbindungen.

Steuern des digitalen Ausgangs

Über CLI und über die private MIB-Variable snMspsDigitalOutputLevel können Sie den digitalen Ausgang (DO/1L) steuern.

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 Ausgang projektieren. Steuern Sie den digitalen Ausgang nicht direkt an, wenn Sie diesen im WBM und CLI verwenden.

Hinweis

Wenn der digitale Ausgang den Status ändert, wird ein Eintrag in der Ereignisprotokolltabelle erzeugt.

- OID der privaten MIB-Variable snMspsDigitalOutputLevel:

  ```
  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).snMspsDigitalOutputTable(3).snMspsDigitalOutputEntry(1).snMspsDigitalOutputLevel(6)
  ```

- Werte der MIB-Variable
  - 1: Digitaler Ausgang ist geöffnet (DO und 1L sind unterbrochen).
  - 2: Digitaler Ausgang ist geschlossen (DO und 1L sind gebrückt).

Digitaler Eingang

Über die private MIB-Variable snMspsDigitalInputLevel können Sie den Status des digitalen Eingangs auslesen.

Hinweis

Wenn der digitale Eingang den Status ändert, wird ein Eintrag in der Ereignisprotokolltabelle erzeugt.

- 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)

MIB-Datei

Die MIB-Variablen sind in der Datei "SN-MSPS-DIGITAL-IO-MIB" enthalten, die Bestandteil der privaten MIB-Datei "scalance_m_msps.mib" ist.

Technische Grundlagen 2

2.1 IPv4-Adresse, Subnetzmaske und Adresse des Netzübergangs

Wertebereich für IPv4-Adresse

Die IPv4-Adresse besteht aus 4 Dezimalzahlen aus dem Wertebereich 0 bis 255, die durch einen Punkt voneinander getrennt sind; z. B. 141.80.0.16

Adressformat IPv4 - Notation

Eine IPv4-Adresse besteht aus 4 Byte. Jedes Byte wird dezimal dargestellt und ist durch einen Punkt vom vorherigen getrennt.

XXX.XXX.XXX.XXX

XXX steht für eine Zahl zwischen 0 und 255

Die IPv4-Adresse besteht aus zwei Teilen:

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

Wertebereich für Subnetzmaske

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

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

Die Werte "1" bestimmen die Netznummer innerhalb der IPv4-Adresse. Die Werte "0" die Host-Adresse innerhalb der IPv4-Adresse.

Beispiel:

richtige Werte:

255.255.0.0 D = 1111 1111.1111 1111.0000 0000.0000 0000 B

255.255.128.0 D = 1111 1111.1111 1111.1000 0000.0000 0000 B

255.254.0.0 D = 1111 1111.1111 1110.0000 0000.0000.0000 B

falscher Wert:

255.255.1.0 D = 1111 1111.1111 1111.0000 0001.0000 0000 B

Zusammenhang IPv4-Adresse und Subnetzmaske

Die erste Dezimalzahl der IPv4-Adresse (von links) bestimmt den Aufbau der Subnetzmaske hinsichtlich der Anzahl der Werte "1" (binär) wie folgt (für "x" steht die Host-Adresse):

Erste Dezimalzahl der IPv4-Adresse	Subnetzmaske
0 bis 127	255.x.x.x
128 bis 191	255.255.x.x
192 bis 223	255.255.255.x

Classless Inter-Domain Routing (CIDR)

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

Beispiel:

IPv4-Adresse 192.168.0.0 mit Subnetzmaske 255.255.255.0

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

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

Wertebereich für Adresse des Netzübergangs

Die Adresse besteht aus 4 Dezimalzahlen aus dem Wertebereich 0 bis 255, die durch einen Punkt voneinander getrennt sind; z. B. 141.80.0.1

Zusammenhang IPv4-Adresse und Adresse des Netzübergangs

Die IPv4-Adresse und die Adresse des Netzübergangs dürfen nur an den Stellen unterschiedlich sein, an denen in der Subnetzmaske "0" steht.

Beispiel:

Sie haben eingegeben: für Subnetzmaske 255.255.255.0; für IPv4-Adresse 141.30.0.5 und für die Adresse des Netzübergangs 141.30.128.0. Die IPv4-Adresse und die Adresse des Netzübergangs dürfen nur in der 4. Dezimalzahl einen unterschiedlichen Wert haben. Im Beispiel ist aber die 3. Stelle schon unterschiedlich.

Im Beispiel müssen Sie also alternativ ändern:

die Subnetzmaske auf: 255.255.0.0 oder

die IPv4-Adresse auf: 141.30.128.5 oder

die Adresse des Netzübergangs auf: 141.30.0.0

2.2 VLAN

2.2.1 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 22). 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 Based VLAN (Seite 131)".

- 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 > General (Seite 129)" 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.

2.2.2 VLAN-Tagging

Erweiterung der Ethernet-Telegramme um vier Byte

Für CoS (Class of Service, Telegrammpriorisierung) und für VLAN (Virtuelles Netzwerk) wurde in der Norm IEEE 802.1 Q 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. Bei den IE-Switches beträgt die Standard Telegrammgröße mindestens 1536 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:

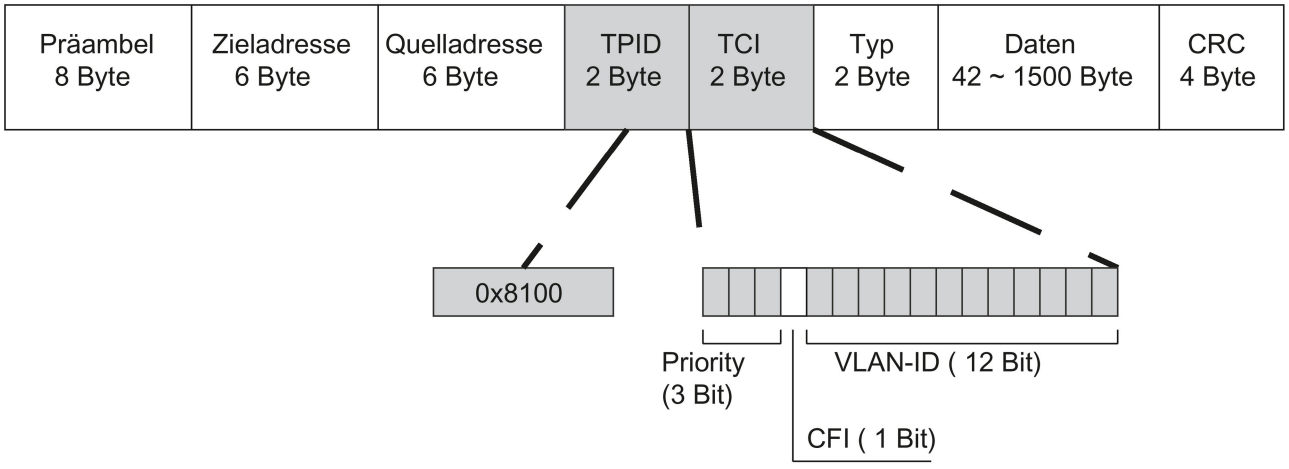


Bild 2-1 Aufbau des erweiterten Ethernet-Telegramms

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. Die Priorisierung nach IEEE 802.1p lautet wie folgt:

CoS-Bits	Typ der Daten
000	Zeitunkritischer Datenverkehr (less then best effort [Grundeinstellung])
001	Normaler Datenverkehr (best effort [Hintergrund])
010	Reserviert (Standard)
011	Reserviert (excellent effort)
100	Datenübertragung mit max. 100ms Verzögerung
101	Garantierter Service, interaktives Multimedia
110	Garantierter Service, interaktives Sprachübertragung
111	Reserviert

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. Dabei werden zuerst die Telegramme mit der höchsten Priorität abgearbeitet ("Strict Priority"-Verfahren). 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

2.3 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.

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 141)".

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 SourceNAT 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.

von	zu	Verhalten
einem Port-Bereich	einem anderen Port-Bereich	Die Telegramme werden auf einen beliebigen freien Port aus dem Zielbereich umgesetzt. Bei einzelnen Verbindungen wird meist auf den ersten Port im Zielbereich umgesetzt. Bei gleichzeitigen Verbindungen wird mittels einer Reih-um-Methode (round robin) auf einen freien Port im Zielbereich umgesetzt.
einem einzigen Port	einem Port-Bereich	Die Telegramme werden auf einen beliebigen freien Port aus dem Zielbereich umgesetzt. Bei einzelnen Verbindungen wird meist auf den ersten Port im Zielbereich umgesetzt. Bei gleichzeitigen Verbindungen wird mittels einer Reih-um-Methode (round robin) auf einen freien Port im Zielbereich umgesetzt.

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

NAPT konfigurieren Sie unter "Layer 3" > "NAT" > "NAPT (Seite 142)".

Source-NAT

Wie beim Masquerading wird beim Source-NAT die Quelladressse umgeschrieben. Zusätzlich können die ausgehenden Datenpakete beschränkt werden. Dazu gehören Beschränkungen auf bestimme IP-Adressen oder IP-Adressbereiche und Beschränkungen auf bestimmte Schnittstellen. Diese Regeln können auch auf VPN-Verbindungen angewendet werden.

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 144)".

NETMAP

Mit NETMAP ist es möglich, komplette Subnetze auf ein anderes Subnetz umzusetzen. Bei dieser Umsetzung wird der Subneztanteil 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.

1:1 NAT konfigurieren Sie unter "Layer 3" > "NAT" > "NETMAP (Seite 146)".

Siehe auch

NAPT (Seite 142)

2.4 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 wird ein SNMP-Agent installiert, mit dem die Management-Station Daten austauscht.

Die Management-Station sendet Datenpakete folgenden Typs:

- GET
  Anfordern eines Datensatzes vom Agenten
- GETNEXT
  Ruft den nächsten Datensatz auf.
- GETBULK (verfügbar ab SNMPv2)
  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 Agent sendet die vom Manager angeforderten Daten zurück.
- TRAP
  Wenn ein bestimmtes Ereignis eintritt, sendet der SNMP-Agent eigenständig Traps.

SNMPv1/v2/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 SNMPv2 ein umfangreicheres Sicherheitskonzept ein.

SNMPv3 unterstützt:

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

2.5 Security-Funktionen

2.5.1 Firewall

Zu den Sicherheitsfunktionen 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

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

Die Firewall konfigurieren Sie unter "Security > Firewall (Seite 154)".

2.5.2 IPsecVPN

Das Gerät ist in der Lage, bis zu 20 IPsecVPN-Verbindungen zu einem entfernten Netzwerk aufzubauen.

Die IPsec-Verbindungen konfigurieren Sie unter "Security" > "IPsSec VPN (Seite 162)"

Bei IPsecVPN 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 kann das Gerät nur als VPN-Server fungieren. Das Gerät kann nur auf VPN-Verbindungen warten, aber nicht als aktiver Partner einen VPN-Tunnel aufbauen. Die Adresse der Gegenstelle muss in diesem Modus nicht bekannt sein. Der Einsatz dynamischer IP-Adresse ist also möglich.

- **Standard-Modus**

  Im Standard-Modus muss die Adresse des VPN-Gateways der Gegenstelle bekannt sein, damit die VPN-Verbindung aufgebaut werden kann. 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 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

Das Gerät unterstützt dabei die folgenden Verfahren:

- 3DES-168
- AES-128

  AES-128 ist ein häufig benutztes Verfahren und ist deshalb als Standard eingestellt.
- AES-192
- AES-256

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 - 1
- 3DES- oder AES-Verschlüsselung
- MD5, SHA1 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-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 Gegenstelle. Wenn die Gegenstelle nicht antwortet, wird die IPsec-Verbindung nach einer Anzahl von erlaubten Fehlversuchen als unterbrochen angesehen.

2.5.3 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.	IPsecVPN (Seite 167)
Server-Zertifikat	Server-Zertifikate werden zum Aufbau einer gesicherten Kommunikation (z. B. HTTPS, VPN...) zwischen Gerät und einem weiteren Netzwerkteilnehmer benötigt. Bei dem Server-Zertifikat handelt es sich um ein verschlüsseltes SSL-Zertifikat. Das Server-Zertifikat wird von der ältesten gültigen CA abgeleitet, auch wenn dieses "außer Dienst" ist. Entscheidend ist das Gültigkeitsdatum der CA.	SINEMA RC (Seite 122)
Gerätezertifikat	Zertifikate mit dem privaten Schlüssel (Key file), mit denen sich das Gerät ausweist.	IPsecVPN (Seite 167)
Gegenstellenzertifikat	Zertifikate, mit denen sich das VPN-Gateway der Gegenstelle bei dem Gerät authentifiziert.	IPsecVPN (Seite 167)

Dateitypen

Dateityp	Beschreibung
*.crt	Datei, die das Zertifikat enhält.
*.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.

Security-Empfehlung

3

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

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.

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 unter: Link zum Bereich "Industrielle Kommunikation" (http://support.automation.siemens.com/WW/view/de/10805878/133400)
- Aktivieren Sie nur Protokolle, die sie wirklich für den Einsatz des Gerätes benötigen.
- Die Möglichkeit der VLAN-Strukturierung bietet guten Schutz gegen DoS-Zugriffe und nicht autorisierte Zugriffe. Prüfen Sie, ob dies in ihrem Umfeld sinnvoll ist.
- Beschränken Sie den Zugriff auf das Gerät durch Firewall, VPN (IPsec , OpenVPN) und NAT.
- Aktivieren Sie die Logging-Funktionen. Nutzen Sie die zentrale Logging-Funktion, um Änderungen und Zugriffe zentral zu protokollieren. Prüfen Sie regelmäßig die Logging-Informationen.
- Konfigurieren Sie einen Syslog-Server, um alle Logs an eine zentrale Stelle weiterzuleiten.

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 SSL, IPsec und SINEMA RC einzurichten.

- Es wird dringend empfohlen eigene SSL-Zertifikate zu erstellen und bereitzustellen.

  Im Gerät sind voreingestellte Zertifikate und Schlüssel vorhanden. Die voreingestellten und automatisch erstellten SSL-Zertifikate sind selbst-signiert. Es wird empfohlen SSL-Zertifikate zu verwenden, die entweder durch eine zuverlässige externe oder eine interne Zertifizierungsstelle signiert sind.
  Das Gerät hat eine Schnittstelle, über die Sie die Zertifikate und Schlüssel importieren können.
- Wir empfehlen Zertifikate mit einer Schlüssellänge von 2048 Bit zu verwenden.

Sichere/Unsichere Protokolle

- 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.
- Aktivieren Sie für die DCP-Funktion nach der Inbetriebnahme den "DCP Read Only"-Modus.
- Wenn SNMP aktiviert ist, ändern Sie die Community-Namen. Wenn kein uneingeschränkter Zugriff erforderlich ist, beschränken Sie den Zugriff über SNMP.
- Nutzen Sie sichere Protokolle, wenn der Zugriff auf das Gerät nicht durch physikalische Schutzvorkehrungen gesichert ist.

Die folgenden Protokolle bieten sichere Alternativen:

- SNMPv1 → SNMPv3
- HTTP → HTTPS
- Telnet → SSH
- SNTP → NTP (secure)

- 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 mit Bedacht ein.
- Um einem unbefugten Zugriff auf das Gerät bzw. Netzwerk vorzubeugen, treffen Sie angemessene Schutzvorkehrungen gegen unsichere Protokolle.

Verfügbare Protokolle pro Port

Die folgende Liste gibt Ihnen einen Überblick über die offenen Ports in diesem Gerät. Beachten Sie dies bei der Konfiguration einer Firewall.

Die Tabelle umfasst folgende Spalten:

- **Protokoll**

  Alle Protokolle, die das Gerät unterstützt

- **Portnummer**

  Portnummer, die dem Protokoll zugeordnet ist

- **Portzustand**
  - Offen

    Der Port ist immer offen und kann nicht geschlossen werden.
  - Offen (wenn konfiguriert)

    Der Port ist offen, wenn er konfiguriert wurde.

    Hinweis

    Bei manchen Protokollen kann der Port offen sein, obwohl das zugehörige Protokoll deaktiviert ist, z. B. TFTP.

- **Defaultzustand des Ports**
  - Offen

    Der Port ist standardmäßig offen.
  - Geschlossen

    Der Port ist standardmäßig geschlossen.

- **Authentifizierung**

  Gibt an, ob das Protokoll während des Zugriffs authentifiziert ist.

Protokoll	Portnummer	Portzustand	Defaultzustand des Ports	Authentifizierung
SSH	TCP/22	Offen	Offen	Ja
HTTP	TCP/80	Offen	Offen	Ja
HTTPS	TCP/443	Offen	Offen	Ja
SNTP	UDP/123	Offen (wenn konfiguriert)	Geschlossen	Nein
SNMP	UDP/161	Offen (wenn konfiguriert)	Offen	Ja
SNMP-Trap	UDP/162	Offen (wenn konfiguriert)	Offen	Ja

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.

Hinweis

Sichere Verbindung

Das WBM bietet auch die Möglichkeit, eine gesicherte Verbindung via HTTPS herzustellen.

Verwenden Sie HTTPS für die geschützte Übertragung ihrer Daten. Wenn Sie auf das WBM ausschließlich über eine sichere Verbindung zugreifen möchten, aktivieren Sie unter "System > Configuration" die Option "HTTPS Server only".

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 13)".
- Der Zugriff über HTTP oder 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". Prüfen Sie, ob bei "Neuere Versionen der gespeicherten Seite suchen" "Automatisch" aktiviert ist.

- Wenn eine Firewall eingesetzt wird, müssen die entsprechenden Ports freigeschaltet sein.
  - Für den Zugriff über HTTP: Port 80
  - Für den Zugriff über HTTPS: Port 443
- Die Darstellung des WBM wurde mit folgenden Desktop-Webbrowsern getestet:
  - MS IE 9

    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 ESR17

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 nachprüfen, ob eine Verbindung besteht.
2. Geben Sie im Adressfeld des Internet-Browsers die IP-Adresse oder die URL des Gerätes ein. Wenn eine einwandfreie Verbindung zum Gerät besteht, erscheint die Anmeldeseite des Web Based Managements (WBM).

Anmeldung mithilfe des Internet-Browsers

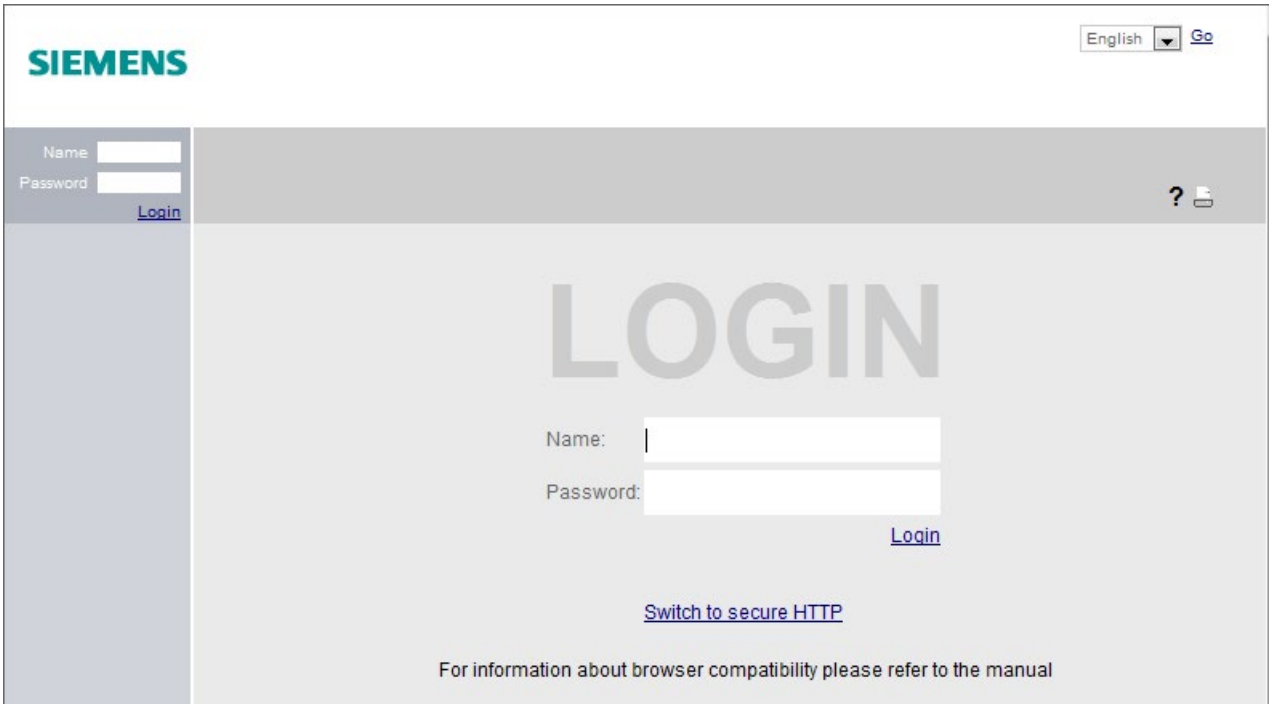
Auswahl der Sprache des WBM

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

Hinweis

Verfügbare Sprachen

In dieser Version ist nur Englisch verfügbar. Weitere Sprachen folgen in einer späteren Version.



Anmeldung über HTTP

Sie haben zwei Möglichkeiten, sich über HTTP anzumelden. Entweder benutzen Sie die Anmeldemöglichkeit in der Mitte des Browser-Fensters oder die Anmeldemöglichkeit im linken oberen Bereich des Browser-Fensters.

1. Geben Sie den Benutzernamen "admin" ein.
2. Geben Sie das zugehörige Passwort ein.

   Wenn Sie sich das erste Mal oder nach einem "Restore Factory Defaults and Restart" anmelden, geben Sie das Standard-Passwort "`admin`" ein.
3. Klicken Sie auf die Schaltfläche "Login" oder bestätigen Sie die Eingabe mit "Enter". Wenn Sie sich das erste Mal oder nach einem "Restore Factory Defaults and Restart" anmelden, werden Sie aufgefordert, das Passwort zu ändern. Das neue Passwort sollte die folgenden Passwortrichtlinien erfüllen:
   - Passwortlänge: mindestens 8 Zeichen
   - Mindestens 1 Großbuchstabe
   - Mindestens 1 Sonderzeichen
   - Mindestens 1 Zahl

   Zur Bestätigung müssen Sie das Passwort wiederholen. Beide Passworteingaben müssen übereinstimmen. Klicken Sie auf die Schaltfläche "Set Values", um den Vorgang abzuschließen und das neue Passwort zu aktivieren.

Wenn Sie sich erfolgreich angemeldet haben, erscheint die Startseite.

Anmeldung über HTTPS

Das Web Based Management bietet auch die Möglichkeit, sich über die gesicherte Verbindung des HTTPS-Protokolls mit dem Gerät zu verbinden. Gehen Sie folgendermaßen vor:

1. Klicken Sie auf den Link "Switch to secure HTTP" in der Anmeldeseite oder geben Sie im Adressfeld des Internet-Browsers "https://" und die IP-Adresse des Gerätes ein.
2. Bestätigen Sie die angezeigte Zertifikatswarnung.
   Die Anmeldeseite des Web Based Management erscheint.
3. Geben Sie den Benutzernamen "admin" ein.Geben Sie das zugehörige Passwort ein.Wenn Sie sich das erste Mal oder nach einem "Restore Factory Defaults and Restart" anmelden, geben Sie das Standard-Passwort "admin" ein.

4. Klicken Sie auf die Schaltfläche "Login" oder bestätigen Sie die Eingabe mit "Enter". Wenn Sie sich das erste Mal oder nach einem "Restore Factory Defaults and Restart" anmelden, werden Sie aufgefordert, das Passwort zu ändern. Das neue Passwort sollte die folgenden Passwortrichtlinien erfüllen:
   - Passwortlänge: mindestens 8 Zeichen
   - Mindestens 1 Großbuchstabe
   - Mindestens 1 Sonderzeichen
   - Mindestens 1 Zahl

   Zur Bestätigung müssen Sie das Passwort wiederholen. Beide Passworteingaben müssen übereinstimmen. Klicken Sie auf die Schaltfläche "Set Values", um den Vorgang abzuschließen und das neue Passwort zu aktivieren.

Wenn Sie sich erfolgreich angemeldet haben, erscheint die Startseite.

4.3 Menü "Information"

4.3.1 Start Page

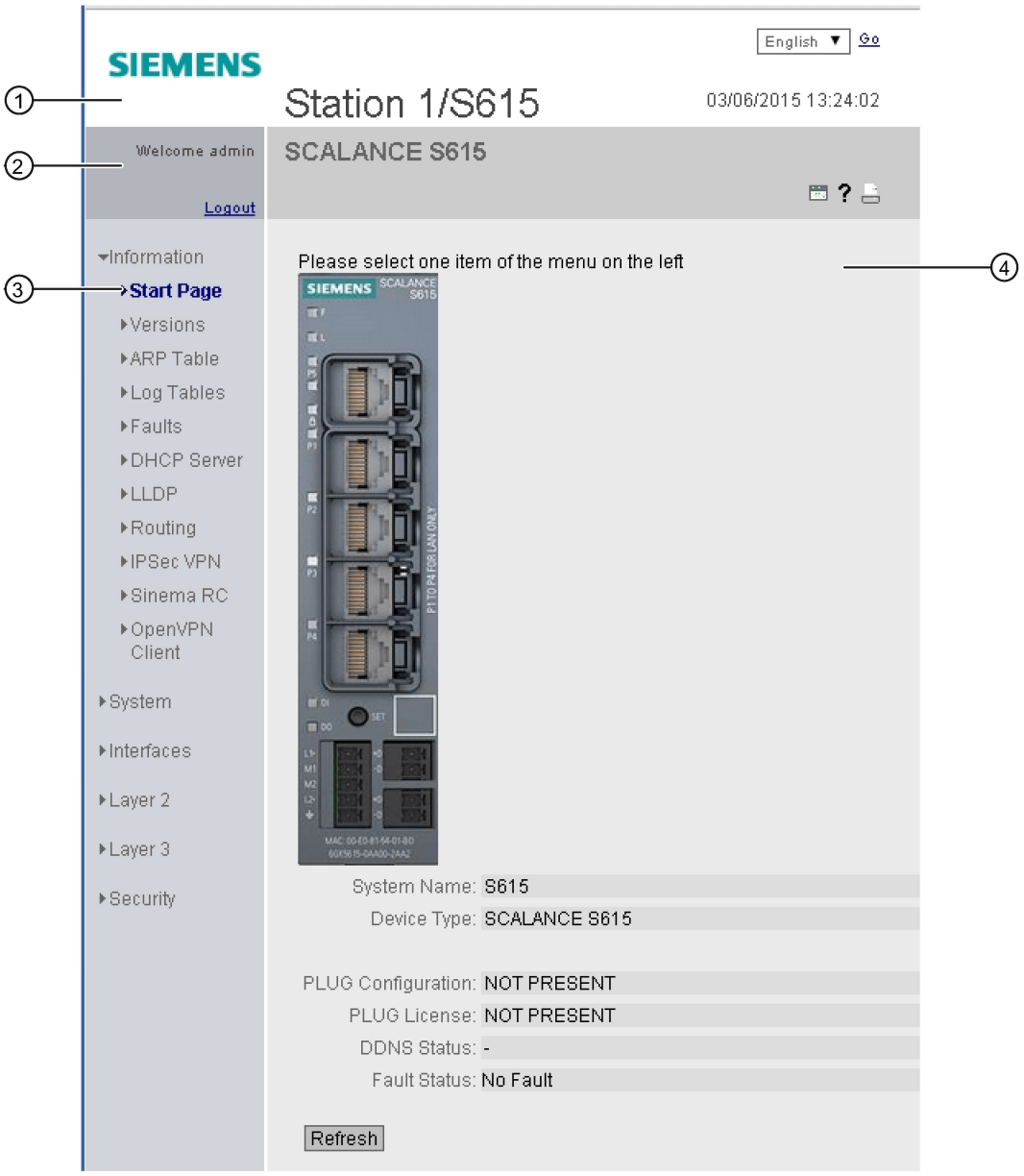
Ansicht der Startseite

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
- Anzeige von: "System Location/System Name".
  - "System Location" enthält die Ortsangabe des Geräts.
    Im Auslieferungszustand wird die IP-Adresse der Ethernet-Schnittstelle angezeigt.
  - "System Name" ist der Gerätename.

  Den Inhalt dieser Anzeige können Sie unter "System" > "General" > "Device" ändern.

- Klappliste für die Sprachauswahl
- Systemzeit und -datum

  Den Inhalt dieser Anzeige können Sie unter "System" > "System Time" ändern.

Anzeigebereich (2)

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

- **Drucker** 
  Wenn Sie diese Schaltfläche anklicken, wird ein Popup-Fenster, mit einer für Drucker optimierten Ansicht des Seiteninhalts, geöffnet.
- **Hilfe** 
  Wenn Sie diese Schaltfläche anklicken, wird die Hilfeseite des aktuell gewählten Menüpunktes in einem neuen Browser-Fenster aufgerufen.
- **Leuchtdiodensimulation** 
  Jede Komponente eines Geräts 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.
- **Aktualisieren an** 

  / Aktualisieren aus 

  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 sind folgende Einträge möglich:

- System Name: Systemname des Geräts
- Device Type: Typenbezeichnung des Geräts
- PLUG Configuration: Zeigt den Status der Konfigurationsdaten auf dem PLUG an, siehe Kapitel "System > PLUG > Configuration".
- PLUG License: Zeigt den Status der Lizenz auf dem PLUG an, siehe Kapitel "System > PLUG > License".
- 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 unkown
    Status unbekannt
- Fault Status: Zeigt den Fehlerstatus des Geräts an.

Häufig verwendete Schaltflächen

Die WBM-Seiten enthalten standardmäßig die folgenden Schaltflächen:

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

  Hinweis

  Wenn Sie auf die Schaltfläche "Refresh" klicken, bevor Sie Ihre Konfigurationsänderungen mit Hilfe der Schaltfläche "Set Values" 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 "Set Values"**
  WBM-Seiten, auf denen Sie Konfigurationseinstellungen festlegen können, haben am unteren Rand die Schaltfläche "Set Values". 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 dem Login "admin" möglich.

  Hinweis

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

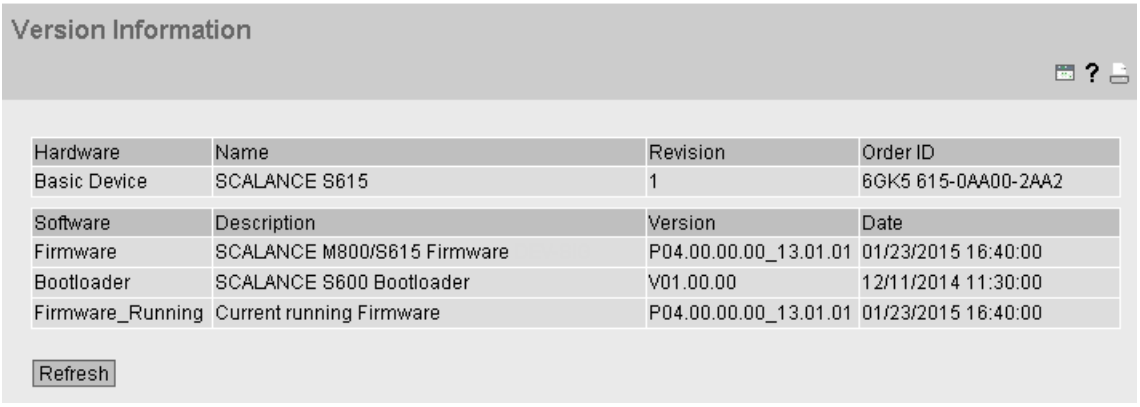
- **Anlegen von Einträgen mit "Create"**
  WBM-Seiten, auf denen Sie neue Einträge erstellen können, haben am unteren Rand die Schaltfläche "Create". Klicken Sie auf diese Schaltfläche, um einen neuen Eintrag zu erstellen.
- **Löschen von Einträgen mit "Delete"**
  WBM-Seiten, auf denen Sie Einträge löschen können, haben am unteren Rand die Schaltfläche "Delete". 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 "Next"**
  Bei WBM-Seiten mit sehr vielen Datensätzen ist die Anzahl der auf einer Seite darstellbaren Datensätze beschränkt. Klicken Sie auf die Schaltfläche "Next", um innerhalb der Datensätze vorwärts zu blättern.
- **Rückwärts blättern mit "Prev"**
  Bei Seiten mit sehr vielen Datensätzen ist die Anzahl der auf einer Seite darstellbaren Datensätze beschränkt. Klicken Sie auf die Schaltfläche "Prev", um innerhalb der Datensätze rückwärts zu blättern.

Abmeldung

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

4.3.2 Versions

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



Beschreibung

Die Tabelle 1 gliedert sich in folgende Spalten:

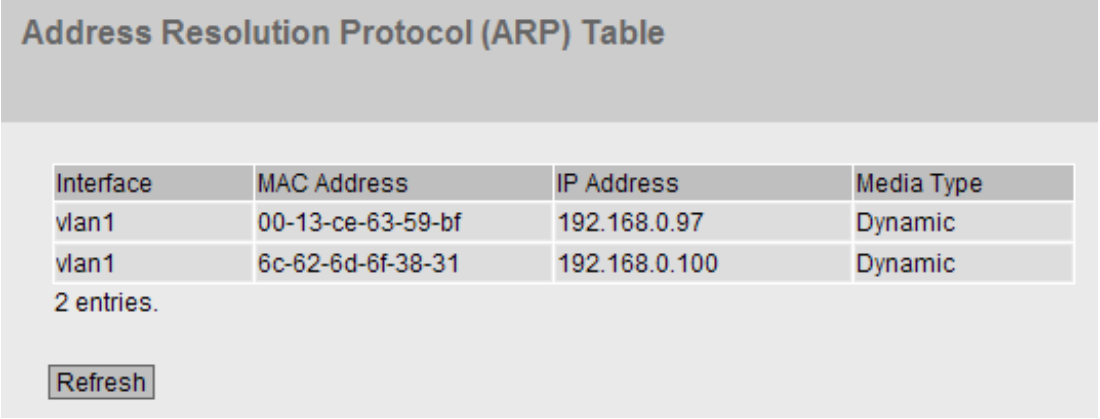
- **Hardware**
  - Basic Device
    Zeigt das Grundgerät an
- **Name**
  Zeigt den Namen des Geräts.
- **Revision**
  Zeigt den Hardware-Ausgabestand des Geräts an.
- **Order ID**
  Zeigt die Bestellnummer des Geräts an.
- **Software**
  - Firmware
    Zeigt die aktuelle Firmware-Version an. Wenn eine neue Firmware-Datei geladen wurde und das Gerät noch nicht neu gestartet ist, wird 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.
  -

- **Description**
  Zeigt die Kurzbeschreibung der Software an.
- **Version**
  Zeigt die Versionsnummer der Software an.
- **Date**
  Zeigt das Erstellungsdatum der Software an.

4.3.3 ARP Table

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:

- **Interface**
  Zeigt die Schnittstelle an, über die der Zeileneintrag gelernt wurde.
- **MAC Address**
  Zeigt die MAC-Adresse des Ziel- oder Quellgeräts an.
- **IP Address**
  Zeigt die IP-Adresse des Zielgeräts an.
- **Media Type**
  Zeigt die Art der Verbindung.
  - Dynamic
    Das Gerät hat die Adressdaten automatisch erkannt.
  - Static

    Die Adressen wurden als statische Adressen eingetragen.

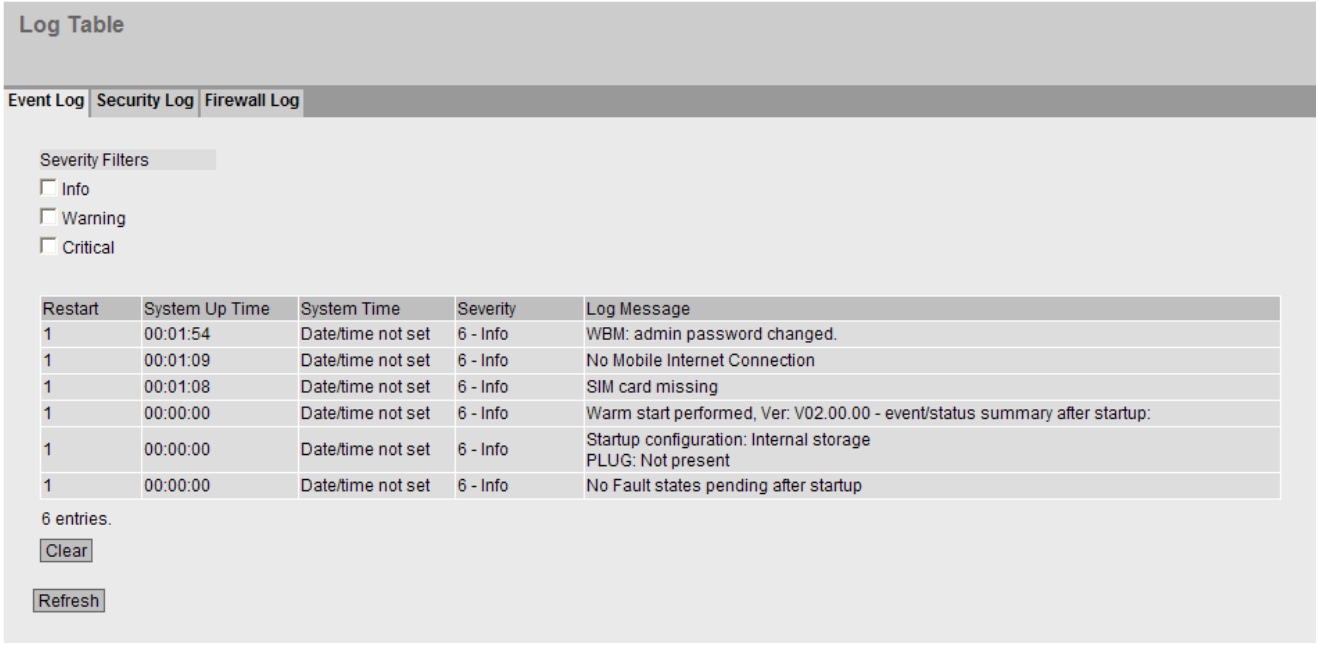
4.3.4 Log Tables

4.3.4.1 Event Log

Protokollierung von Ereignissen

Die WBM-Seite zeigt in tabellarischer Form die aufgetretenen Systemereignisse an. Einige der Systemereignisse sind unter "System > Events" 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 oder TFTP herunterladen.



Beschreibung

- **Severity Filters**
  Die Einträge der Tabelle können Sie nach Schweregrad filtern. Um alle Einträge anzuzeigen, aktivieren oder deaktivieren Sie alle Parameter.
  - 2 - Critical
    kritisch
  - 4 - Warning
    Warnungen
  - 6- Info
    informativ

Die Tabelle gliedert sich in folgende Spalten:

- **Restart**
  Zählt die Anzahl der Neustarts seit dem letzten Zurücksetzen auf Werkseinstellungen und gibt an, nach welchem Neustart des Gerätes das entsprechende Ereignis aufgetreten ist.
- **System Up Time**
  Zeigt die Laufzeit des Geräts seit dem letzten Neustart an, zu der das beschriebene Ereignis aufgetreten ist.
- **System time**
  Zeigt die Systemzeit des Geräts an. Wenn keine Systemzeit eingestellt ist, enthält das Feld die Angabe "Date/time not set".
- **Severity**
  Zeigt die Ereignisschwere an.
- **Log Message**
  Zeigt eine Kurzbeschreibung des eingetretenen Ereignisses an.

Beschreibung der Schaltfläche

Schaltfläche "Clear"

Klicken Sie auf diese Schaltfläche, um den Inhalt der Protokolldatei zu löschen. Die Anzeige wird dabei ebenfalls geleert. Erst wenn nach dem Wiederherstellen der Werkseinstellungen das Gerät neu gestartet ist, wird der Neustart-Zähler zurückgesetzt.

Hinweis

Die Anzahl der Einträge in dieser Tabelle ist auf 400 pro Schweregrad beschränkt. Wenn diese Zahl erreicht ist, werden die ältesten Einträge überschrieben. Die Tabelle verbleibt permanent im Speicher.

Schaltfläche "Show all"

Klicken Sie auf diese Schaltfläche, um alle Einträge auf der WBM-Seite anzuzeigen. Beachten Sie, dass das Anzeigen aller Meldungen einige Zeit beanspruchen kann.

Schaltfläche "Next"

Klicken Sie auf diese Schaltfläche, um zur nächsten Seite zu navigieren.

Schaltfläche "Prev"

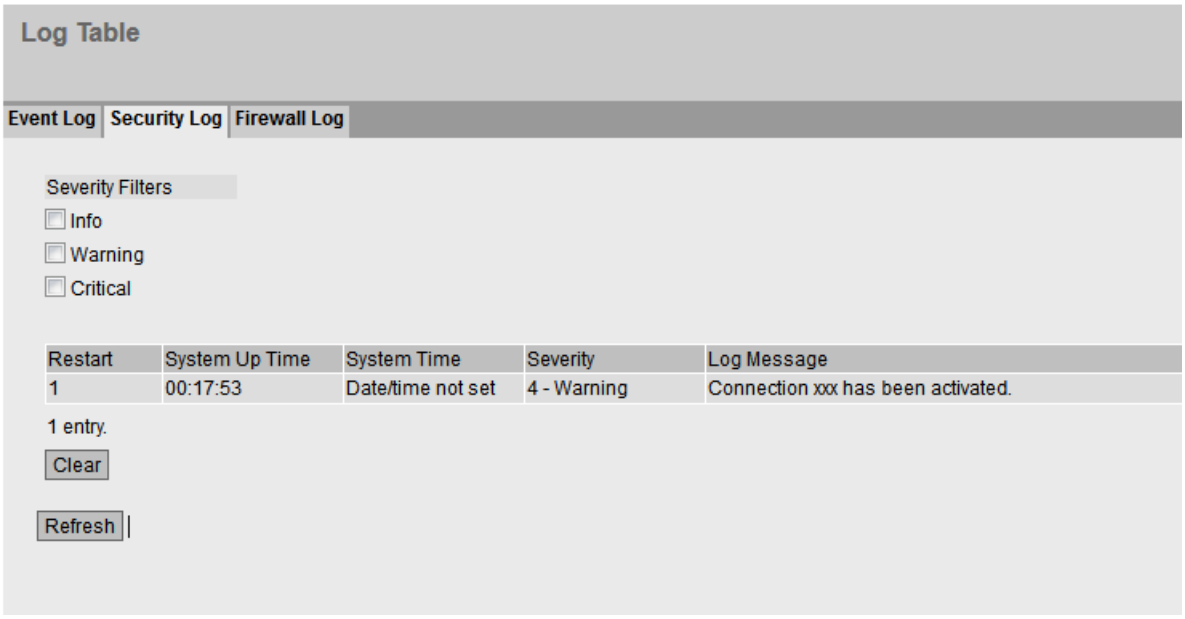
Klicken Sie auf diese Schaltfläche, um zur vorherigen Seite zu navigieren.

Klappliste für Seitenwechsel

Wählen Sie aus der Klappliste die gewünschte Seite aus, um zu einer bestimmten Seite zu navigieren.

4.3.4.2 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 Filters**
  Die Einträge der Tabelle können Sie nach Schweregrad filtern. Um alle Meldungen anzuzeigen, aktivieren oder deaktivieren Sie alle Parameter.
  - 2 - Critical
    kritisch
  - 4 - Warning
    Warnungen
  - 6 - Info
    informativ

Die Tabelle gliedert sich in folgende Spalten:

- **Restart**
  Zählt die Anzahl der Neustarts seit dem letzten Zurücksetzen auf Werkseinstellungen und gibt an, nach welchem Neustart des Gerätes die entsprechende Meldung aufgetreten ist.
- **System Up Time**
  Zeigt die Laufzeit des Geräts seit dem letzten Neustart an, zu der das Ereignis aufgetreten ist.
- **System time**
  Zeigt die Systemzeit des Geräts an. Wenn keine Systemzeit eingestellt ist, enthält das Feld die Angabe "Date/time not set".

- **Severity**
  Zeigt die Ereignisschwere an.
- **Log Message**
  Zeigt eine Kurzbeschreibung des eingetretenen Ereignisses an.
  Wenn die Systemzeit gesetzt ist, wird auch die Zeit angezeigt, bei der das Ereignis eingetreten ist.

Beschreibung der Schaltfläche

Schaltfläche "Clear"

Klicken Sie auf diese Schaltfläche, um den Inhalt der Protokolldatei zu löschen. Die Anzeige wird dabei ebenfalls geleert. Erst wenn nach dem Wiederherstellen der Werkseinstellungen das Gerät neu gestartet ist, wird der Neustartzähler zurückgesetzt.

Hinweis

Die Anzahl der Einträge in dieser Tabelle ist auf 400 pro Schweregrad beschränkt. Wenn diese Zahl erreicht ist, werden die ältesten Einträge überschrieben. Die Tabelle verbleibt permanent im Speicher.

Schaltfläche "Show all"

Klicken Sie auf diese Schaltfläche, um alle Einträge auf der WBM-Seite anzuzeigen. Beachten Sie, dass das Anzeigen aller Meldungen einige Zeit beanspruchen kann.

Schaltfläche "Next"

Klicken Sie auf diese Schaltfläche, um zur nächsten Seite zu navigieren.

Schaltfläche "Prev"

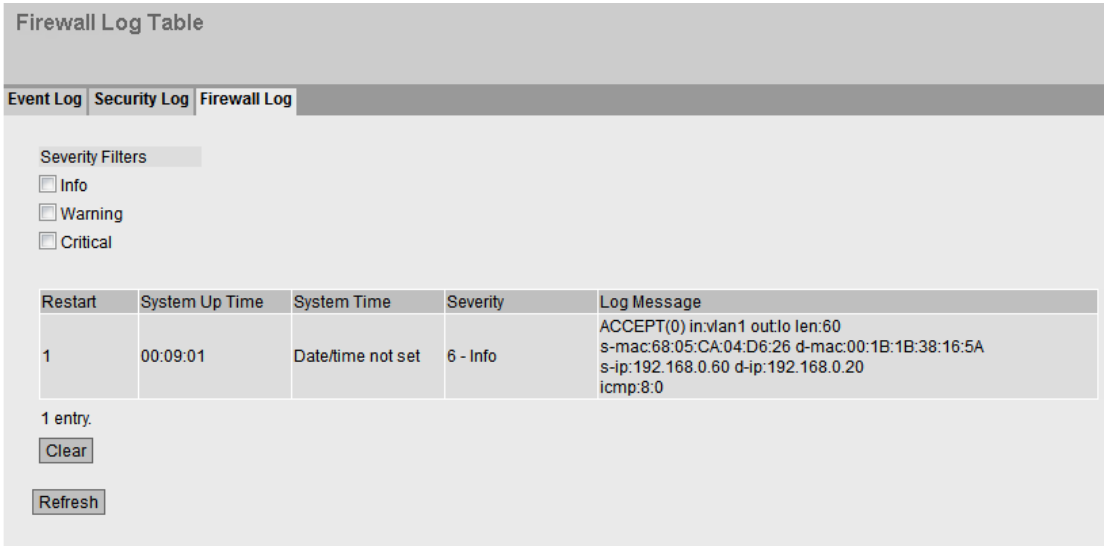
Klicken Sie auf diese Schaltfläche, um zur vorherigen Seite zu navigieren.

Klappliste für Seitenwechsel

Wählen Sie aus der Klappliste die gewünschte Seite aus, um zu einer bestimmten Seite zu navigieren.

4.3.4.3 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 Filters**
  Die Einträge der Tabelle können Sie nach Schweregrad filtern. Um alle Einträge anzuzeigen, aktivieren oder deaktivieren Sie alle Parameter.
  - 2 - Critical
    kritisch
  - 4 - Warning
    Warnungen
  - 6- Info
    informativ

Die Tabelle gliedert sich in folgende Spalten:

- **Restart**
  Zählt die Anzahl der Neustarts seit dem letzten Zurücksetzen auf Werkseinstellungen und gibt an, nach welchem Neustart des Gerätes das entsprechende Ereignis aufgetreten ist.
- **System Up Time**
  Zeigt die Laufzeit des Geräts seit dem letzten Neustart an, zu der das beschriebene Ereignis aufgetreten ist.
- **System time**
  Zeigt die Systemzeit des Geräts an. Wenn keine Systemzeit eingestellt ist, enthält das Feld die Angabe "Date/time not set".

- **Severity**
  Zeigt die Ereignisschwere an.
- **Log Message**
  Zeigt eine Kurzbeschreibung des eingetretenen Ereignisses an.

Beschreibung der Schaltfläche

Schaltfläche "Clear"

Klicken Sie auf diese Schaltfläche, um den Inhalt der Protokolldatei zu löschen. Die Anzeige wird dabei ebenfalls geleert. Erst wenn nach dem Wiederherstellen der Werkseinstellungen das Gerät neu gestartet ist, wird der Neustartzähler zurückgesetzt.

Hinweis

Die Anzahl der Einträge in dieser Tabelle ist auf 400 pro Schweregrad beschränkt. Wenn diese Zahl erreicht ist, werden die ältesten Einträge überschrieben. Die Tabelle verbleibt permanent im Speicher.

Schaltfläche "Show all"

Klicken Sie auf diese Schaltfläche, um alle Einträge auf der WBM-Seite anzuzeigen. Beachten Sie, dass das Anzeigen aller Meldungen einige Zeit beanspruchen kann.

Schaltfläche "Next"

Klicken Sie auf diese Schaltfläche, um zur nächsten Seite zu navigieren.

Schaltfläche "Prev"

Klicken Sie auf diese Schaltfläche, um zur vorherigen Seite zu navigieren.

Klappliste für Seitenwechsel

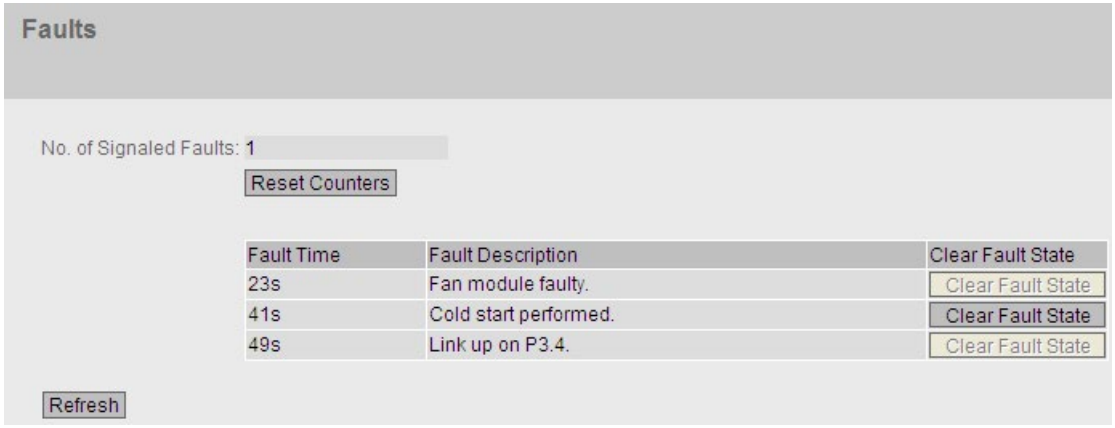
Wählen Sie aus der Klappliste die gewünschte Seite aus, um zu einer bestimmten Seite zu navigieren.

4.3.5 Faults

Fehlerstatus

Diese Seite zeigt auftretende Fehler an, die unter "Events" und "Fault Monitoring" konfiguriert sind. Fehler des Ereignisses "Cold/Warm Start" können nach einer Bestätigung wieder gelöscht werden.
Wenn es keine weitere unbeantwortete Fehlermeldungen gibt, schaltet sich die Fehler-LED ab.

Die Zeitrechnung beginnt jeweils nach dem letzten Systemstart. Bei einem Neustart des Systems wird im Fehlerspeicher ein neuer Eintrag mit der durchgeführten Startart erzeugt.



Beschreibung

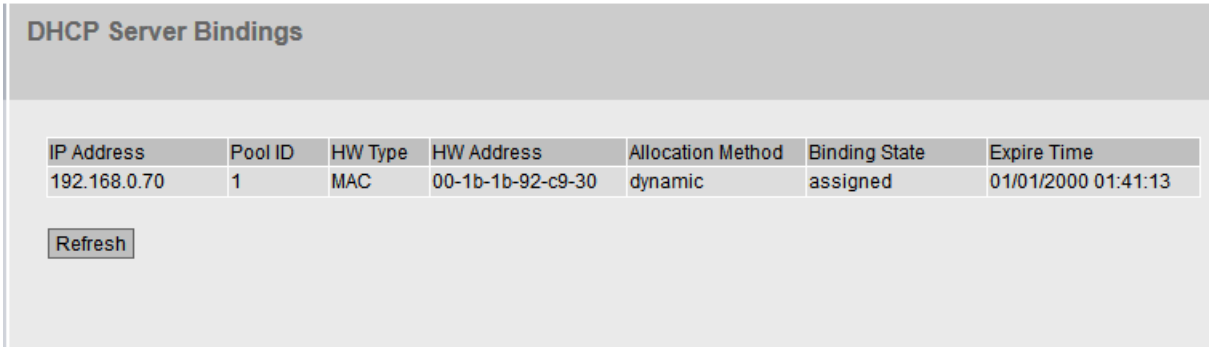
Das Feld "**No. of Signaled Faults**" bezeichnet die Anzahl der seit dem letzten Hochlauf angezeigten Fehler. Klicken sie auf die Schaltfläche "Reset Counters", um diesen Wert zurückzusetzen.

Die Tabelle enthält die folgenden Spalten:

- **Fault Time**
  Zeigt die Laufzeit des Geräts seit dem letzten Neustart an, zu der der beschriebene Fehler aufgetreten ist.
- **Fault Description**
  Zeigt eine Kurzbeschreibung des eingetretenen Fehlers an.
- **Clear Fault State**
  Um Fehler des Ereignisses "Cold/Warm Start" zu löschen, klicken Sie auf die Schaltfläche "Clear Fault State".

4.3.6 DHCP Server

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



Beschreibung

- **IP Address**
  Zeigt die IPv4-Adresse an, die dem Gerät zugeordnet ist.
- **Pool ID**
  Zeigt die Nummer des IPv4-Adressbands an.
- **HW Type**
  Zeigt an, dass der DHCP-Server die Geräte im Netzwerk anhand der MAC-Adresse identifiziert.
- **HW Address**

  Zeigt die MAC-Adresse des DHCP-Clients.
- **Allocation Method**
  Zeigt an, ob die IPv4-Adresse statisch oder dynamisch vergeben wurde. Die statischen Einträge konfigurieren Sie unter "System > DHCP > Static Leases".
- **Binding State**
  Zeigt den Status der Zuordnung an.
  - assigned
    Die Zuordung wird verwendet.
  - not assigned
    Die Zuordnung wird nicht verwendet.
  - probing
    Die Zuordnung wird geprüft.
  - unknown
    Der Status der Zurodnung ist unbekannt.
- **Expire Time**
  Zeigt an, wie lange die vergebene IPv4-Adresse noch gültig ist. Nach Ablauf dieser Zeitdauer muss das Gerät entweder eine neue IPv4-Adresse anfordern oder die Gültigkeitsdauer der vorhandenen IPv4-Adresse verlängern.

4.3.7 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".

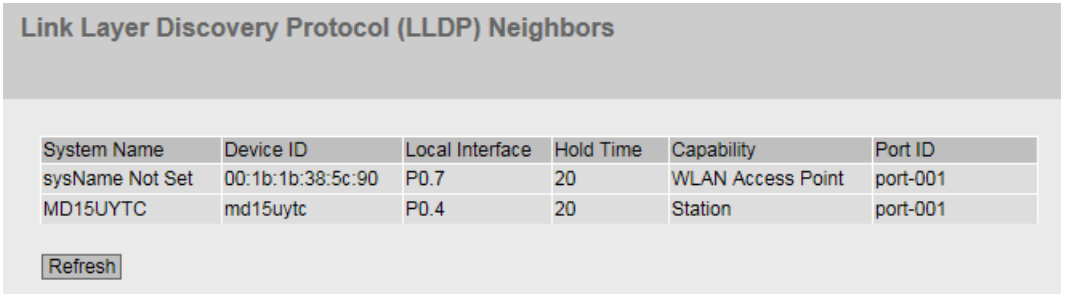


Bild 4-1 Information LLDP

Beschreibung der angezeigten Werte

Die Tabelle enthält folgende Spalten:

- **System Name**

  Systemname des angeschlossenen Geräts.

- **Device ID**

  Gerätekennung des angeschlossenen Geräts.

- **Local Interface**

  Port, an dem der IE-Switch die Informationen empfangen hat.

- **Hold Time**

  Ein Eintrag bleibt für die hier angegebene Zeit in der MIB gespeichert. Wenn der IE-Switch in dieser Zeit keine neuen Informationen von dem angeschlossenen Gerät erhält, wird der Eintrag gelöscht.

- **Capability**

  Zeigt die Eigenschaften des angeschlossenen Geräts an:

  – Router
  – Bridge
  – Telephone
  – DOCSIS Cable Device
  – WLAN Access Point
  – Repeater
  – Station
  – Other

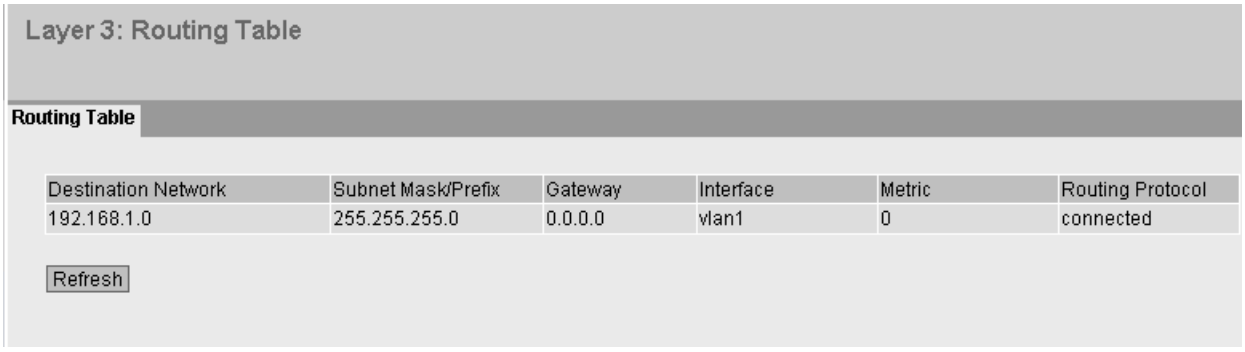
- **Port ID**

  Port des Geräts, der mit dem IE-Switch verbunden ist.

4.3.8 Routing Table

Einleitung

Diese Seite zeigt die Routing-Tabelle des Geräts an.



Beschreibung

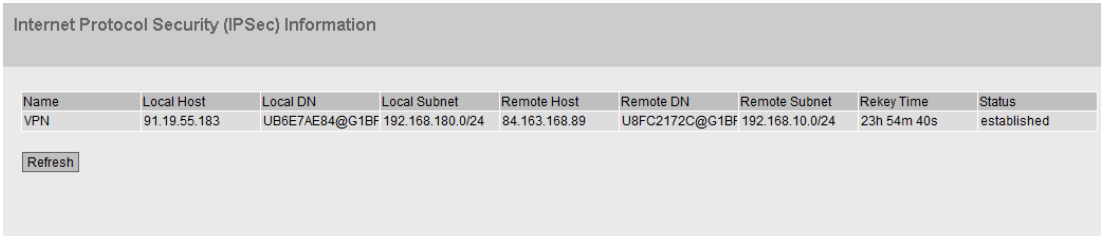
Die Tabelle gliedert sich in folgende Spalten:

- **Destination Network**
  Zeigt die Ziel-Adresse dieser Route an.
- **Subnet Mask/Prefix**
  Zeigt die Subnetzmaske (IPv4) bzw. die Präfixlänge (IPv6) dieser Route an.
- **Gateway**
  Zeigt das Gateway für diese Route an.
- **Interface**
  Zeigt die Schnittstelle für diese Route an.

- **Metric**
  Zeigt die Metrik der Route an. Je größer der Wert, desto länger benötigen Pakete zu Ihrem Ziel.
- **Routing Protocol**
  Zeigt an, aus welchem Routing-Protokoll der Eintrag der Routingtabelle stammt. Folgende Einträge sind möglich:
  - Connected: Verbundene Routen
  - Static: Statische Routen

4.3.9 IPSec VPN

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



Beschreibung

Die Tabelle enthält folgende Spalten:

- **Name**
  Zeigt den Namen der VPN-Verbindung an.
- **Local Host**
  Zeigt die IP-Adresse des Geräts an.
- **Local 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.
- **Local Subnet**
  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 Subnet**
  Zeigt das entfernte Netz an.

- **Rekey Time**
  Zeigt an, wann die Gültigkeit des Schlüssels abläuft.
- **Status**
  Zeigt den Status der VPN-Verbindung an.

4.3.10 SINEMA RC

Zeigt Informationen zum SINEMARC-Server ant.

Hinweis

Diese Funktion ist nur mit KEY PLUG nutzbar.

Beschreibung

- **Status**

  Zeigt den Status der Verbindung SINEMA RC-Server an.
- **Remote Address**

  Zeigt die IP-Adresse des SINEMA RC-Servers an.

- **Tunnel Interface Address**

  Zeigt die IP-Adresse der virtuellen Tunnelschnittstelle an.

- **Connected Local Subnet(s)**

  Zeigt die IP-Adresse des lokalen Subnetzes 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.

- **Connected Remote Subnet(s)**

  Zeigt die Subnetze des SINEMA RC-Servers an.

- **Fingerprint**

  Zeigt den Fingerabdruck des Serverzertifikats an. Wird nur angezeigt, wenn zum Verifizieren der Fingerabdruck verwendet wird.

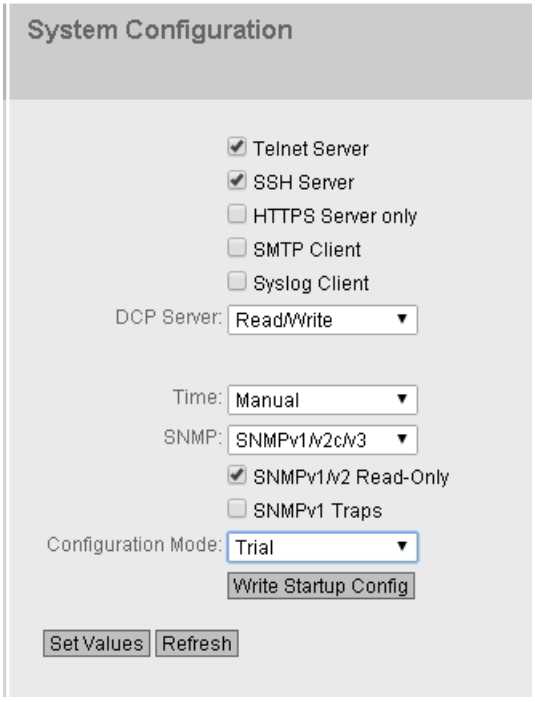
4.4 Menü "System"

4.4.1 Configuration

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:

- **Optionskästchen "Telnet Server"**
  Aktivieren oder deaktivieren Sie den Dienst "Telnet Sever" für den unverschlüsselten Zugriff auf das CLI.
- **Optionskästchen "SSH Server"**
  Aktivieren oder deaktivieren Sie den Dienst "SSH Server" für den verschlüsselten Zugriff auf das CLI.
- **Optionskästchen "HTTPS Server only"**
  Wenn aktiviert, können Sie nur noch über HTTPS auf das Gerät zugreifen.

- **Optionskästchen "SMTP Client"**
  Aktivieren oder deaktivieren Sie den SMTP-Client. Weitere Einstellungen konfigurieren Sie unter "System > SMTP Client".
- **Optionskästchen "Syslog Client"**
  Aktivieren oder deaktivieren Sie den Syslog-Client. Weitere Einstellungen konfigurieren Sie unter "System > Syslog Client".
- **Klappliste "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.
  - Read/Write
    Mit DCP können Geräteparameter sowohl gelesen als auch verändert werden.
  - Read-Only
    Mit DCP können Geräteparameter zwar gelesen aber nicht verändert werden.
- **Klappliste "Time"**
  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellungen sind möglich:
  - Manual
    Die Systemzeit wird manuell eingestellt. Weitere Einstellungen konfigurieren Sie unter "System > System Time > Manual Setting".
  - SNTP Client
    Die Systemzeit wird über einen SNTP Server eingestellt. Weitere Einstellungen konfigurieren Sie unter "System > System Time > SNTP Client".
  - NTP Client
    Die Systemzeit wird über einen NTP Server eingestellt. Weitere Einstellungen konfigurieren Sie unter "System > System Time > NTP Client".
  - SIMATIC Time
    Die Systemzeit wird über einen SIMATIC Zeitgeber eingestellt. Weitere Einstellungen konfigurieren Sie unter "System > System Time > SIMATIC Time Client".
- **Klappliste "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 > General".
  - SNMPv3
    Ein Zugriff auf die Geräteparameter ist nur mit der SNMP Version 3 möglich. Weitere Einstellungen konfigurieren Sie unter "System > SNMP > General".
- **Optionskästchen "SNMPv1/v2 Read-Only"**
  Aktivieren oder deaktivieren Sie den schreibenden Zugriff auf SNMP-Variablen bei SNMPv1/v2c.

- **Optionskästchen "SNMPv1 Traps"**
  Aktivieren oder deaktivieren Sie das Senden von SNMP-Traps (Alarmtelegramme). Weitere Einstellungen konfigurieren Sie unter "System > SNMP > Traps".
- **Klappliste "Configuration Mode":**

  Wählen Sie aus der Klappliste die Betriebsart. Folgende Betriebsarten sind möglich:

  – Automatic Save
  Automatischer Sicherungsbetrieb. Ca. 1 Minute nach der letzten Parameteränderung oder beim Neustart des Geräts wird die Konfiguration automatisch abgespeichert.

  – 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 "Write Startup Config". Die Schaltfläche "Write Startup Config" wird eingeblendet, wenn Sie den Trial-Modus einstellen. Zusätzlich wird im Anzeigebereich die Meldung "Trial Mode Active – Press "Write Startup Config" button to make your settings persistent." 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.

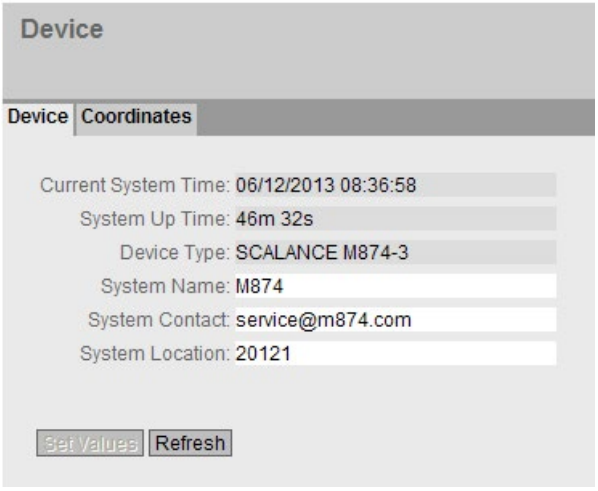
Vorgehensweise

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 "Set Values".

4.4.2 General

4.4.2.1 Device

Diese WBM-Seite enthält die allgemeinen Geräteinformationen.



Beschreibung

Die WBM-Seite enthält folgende Felder:

- **Current System Time**
  Zeigt die aktuelle Systemuhrzeit an. Die Systemuhrzeit wird entweder vom Anwender eingestellt oder per Uhrzeittelegramm synchronisiert: entweder SINEC H1 Uhrzeittelegramm, NTP oder SNTP.
- **System Up Time**
  Zeigt die Laufzeit des Geräts seit dem letzten Neustart an.
- **Device Type**
  Zeigt die Typenbezeichnung des Geräts an.
- **Eingabefeld "System Name"**
  Sie können den Namen des Geräts eingeben. Der Name wird im Auswahlbereich angezeigt. Es sind maximal 255 Zeichen möglich.

- **Eingabefeld "System Contact"**
  Sie können den Namen einer Kontaktperson eingeben, die für die Verwaltung des Geräts zuständig ist. Es sind maximal 255 Zeichen möglich.
- **Eingabefeld "System Location"**
  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
- !"#$%&'()*+,-./:;<=>?@ [\]_{|}~¦^`

Vorgehensweise

1. Geben Sie in das Eingabefeld "System Contact" den für das Gerät zuständigen Ansprechpartner ein.
2. Geben Sie in das Eingabefeld "System Location" die Ortsbezeichnung des Aufstellungsorts ein.
3. Geben Sie in das Eingabefeld "System Name" den Namen des Geräts ein.
4. Klicken Sie auf die Schaltfläche "Set Values".

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

4.4.2.2 Coordinates

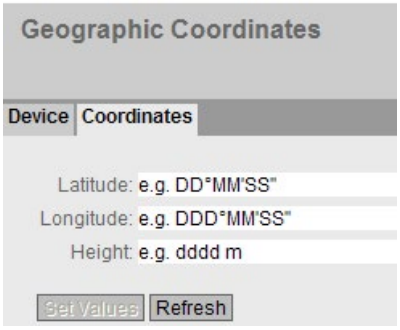
Informationen über die geografischen Koordinaten

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 Gerätes 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 Felder. Es sind reine Informationsfelder mit einer maximalen Länge von 32 Zeichen.

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

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

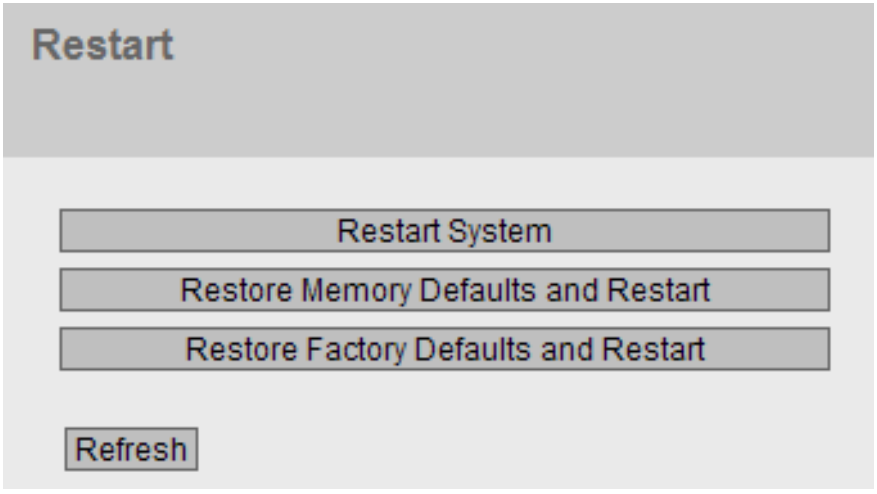
Vorgehensweise

1. Geben Sie in das Eingabefeld "Latitude" den ermittelten Breitengrad ein.
2. Geben Sie in das Eingabefeld "Longitude" den ermittelten Längengrad ein.
3. Geben Sie in das Eingabefeld "Height" die ermittelte Höhe über dem Meeresspiegel ein.
4. Klicken Sie auf die Schaltfläche "Set Values".

4.4.3 Restart

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 "Set Values" 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 der angezeigten Felder

Für den Neustart des Gerätes gibt es folgende Möglichkeiten:

- **Schaltfläche "Restart System"**
  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 gelernten Einträge in der Adresstabelle werden gelöscht. Sie können das Browser-Fenster geöffnet lassen, während das Gerät neu startet. Sie müssen sich wieder neu anmelden.
- **Schaltfläche "Restore Memory Defaults and Restart"**
  Klicken Sie diese Schaltfläche, um die werkseitigen 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
- **Schaltfläche "Restore Factory Defaults and Restart"**
  Klicken Sie auf diese Schaltfläche, um die werkseitigen Konfigurationseinstellungen wiederherzustellen. Es werden auch die geschützten Voreinstellungen zurückgesetzt. Es wird ein automatischer Neustart ausgeführt.

Hinweis

Durch das Zurücksetzen auf die werkseitigen Konfigurationseinstellungen verliert das Gerät seine projektierte IP-Adresse und ist
wieder über die werkseitig eingestellte IP-Adresse 192.168.1.1 zu erreichen.

4.4.4 Load&Save

4.4.4.1 HTTP

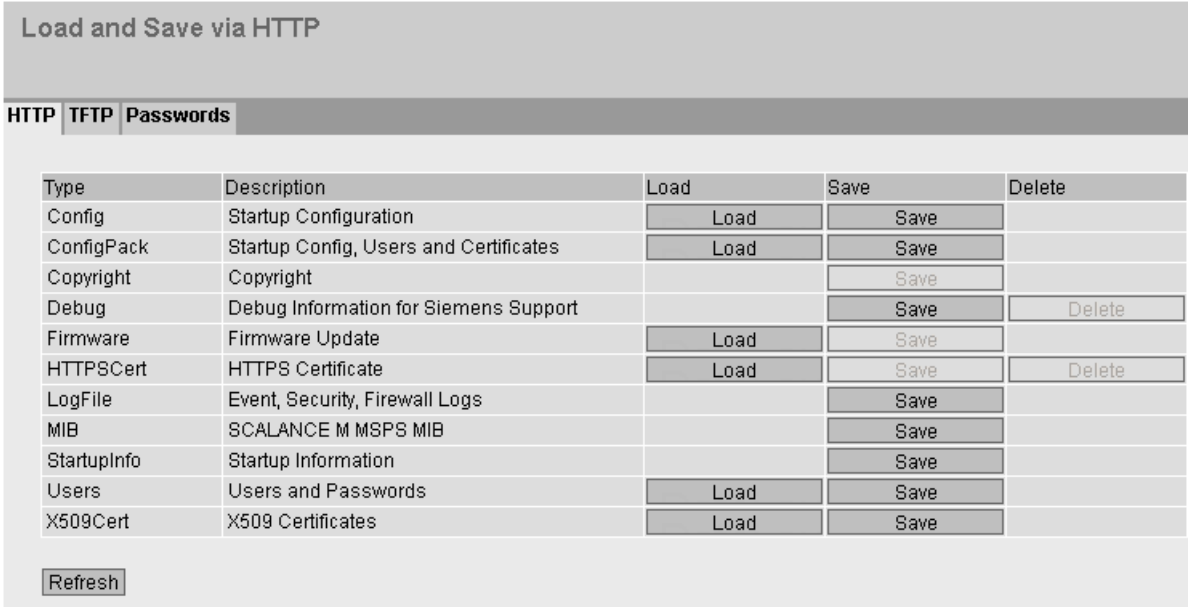
Laden und speichern von Daten über HTTP

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.

Hinweis

Konfigurationsdateien und Trial-Modus/Automatic Save-Modus

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



Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Type**
  Zeigt den Dateityp an.
- **Description**
  Zeigt die Kurzbeschreibung des Dateityps an.
- **Load**
  Mit dieser Schaltfläche können Sie Dateien auf das Gerät hochladen. Die Schaltfläche ist aktivierbar, wenn diese Funktion von dem Dateityp unterstützt wird.
- **Save**
  Mit dieser Schaltfläche können Sie Dateien vom Gerät speichern. Die Schaltfläche ist nur aktivierbar, wenn diese Funktion von dem Dateityp unterstützt wird und die Datei auf dem Gerät vorhanden ist.
- **Delete**
  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

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

Vorgehensweise

Daten über HTTP laden

1. Starten Sie das Laden durch Anklicken einer der Schaltflächen "Load".

   Das Dialogfenster zum Laden einer Datei wird geöffnet.

   Hinweis
   Dateien, deren Zugriff passwortgeschützt ist

   Um diese Dateien erfolgreich ins Gerät zuladen, müssen Sie unter "System" > "Load & Save" > "Password" das für die Datei festgelegte Passwort eingeben.

2. Navigieren Sie zu der gewünschten Datei
3. Klicken Sie im Dialogfenster auf die Schaltfläche "Öffnen".

   Die Datei wird nun geladen.
4. Wenn ein Neustart notwendig ist, wird eine entsprechende Meldung ausgegeben.

Daten über HTTP speichern

1. Starten Sie das Speichern durch Anklicken einer der Schaltflächen "Save".
2. Sie werden aufgefordert, einen Speicherort und einen Namen für die Datei zu wählen. Oder Sie übernehmen den vorgeschlagenen Dateinamen. Verwenden Sie zur Auswahl das Dialogfenster Ihres Browsers. Klicken Sie nach Ihrer Auswahl auf die Schaltfläche "Save".

Daten über HTTP löschen

1. Starten Sie das Löschen durch Anklicken einer der Schaltflächen "Delete".

   Die zu löschende Datei wird gelöscht.

Konfigurationsdaten wiederverwenden

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

Gehen Sie folgendermaßen vor, um Konfigurationsdaten wiederzuverwenden:

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

Beachten Sie, dass die Konfigurationsdaten kodiert gespeichert werden. Deshalb können die Dateien nicht mit einem Texteditor bearbeitet werden.

4.4.4.2 TFTP

Laden und speichern von Daten über einen TFTP-Server

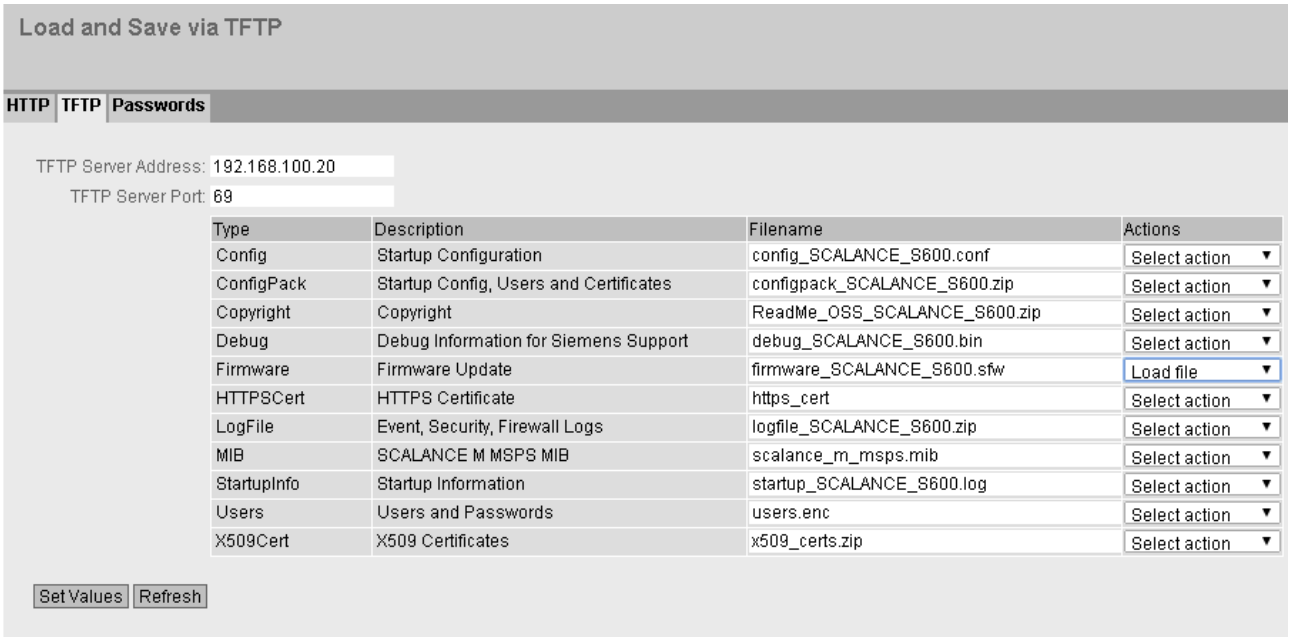
Auf der Seite können Sie den TFTP-Server und die Dateinamen konfigurieren. Weiter bietet das WBM die Möglichkeit, Gerätedaten in einer externen Datei auf Ihrem Client-PC zu speichern bzw. solche Daten aus einer externen Datei vom PC in die Geräte zu laden. So können Sie z. B. eine neue Firmware aus einer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

Hinweis

Konfigurationsdateien und Trial-Modus/Automatic Save-Modus

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



Beschreibung

Die Seite enthält folgende Felder:

- **Eingabefeld "TFTP Server IP Address"**
  Geben Sie die IP-Adresse des TFTP-Servers ein, mit dem Sie Daten austauschen.
- **Eingabefeld "TFTP Server IP Port"**
  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:

- **Type**
  Zeigt den Dateityp an.
- **Description**
  Zeigt die Kurzbeschreibung des Dateityps an.
- **Eingabefeld "Filename"**
  Geben Sie einen Dateinamen ein.
- **Klappliste "Actions"**
  Wählen Sie die gewünschte Aktion aus. Die Auswahl ist abhängig vom gewählten Dateityp. z. B. die Log-Datei lässt sich nur speichern.
  Folgende Aktionen sind möglich:
  - **Save file**
    Mit dieser Auswahl speichern Sie eine Datei auf dem TFTP-Server.
  - **Load file**
    Mit dieser Auswahl laden Sie eine Datei vom TFTP-Server.

Vorgehensweise

Daten über TFTP laden

1. Geben Sie im Eingabefeld "TFTP Server IP Address" die IP-Adresse des TFTP-Servers ein.
2. Geben Sie im Eingabefeld "TFTP Server Port" den verwendeten Port des Servers ein.
3. Geben Sie im Eingabefeld "Filename" den Dateinamen ein.

   Hinweis

   Dateien, deren Zugriff passwortgeschützt ist

   Um diese Dateien erfolgreich ins Gerät zuladen, müssen Sie unter "System" > "Load & Save" > "Password" das für die Datei festgelegte Passwort eingeben.

4. Wählen Sie aus der Klappliste "Actions" die Aktion "Load file".
5. Klicken Sie auf die Schaltfläche "Set Values", um das Laden zu starten.
6. Wenn ein Neustart notwendig ist, wird eine entsprechende Meldung ausgegeben.

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.

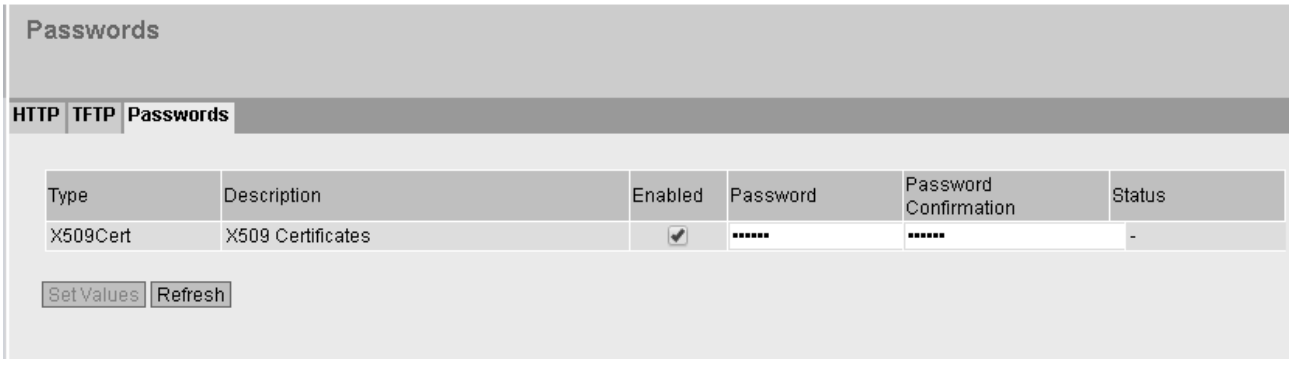
Gehen Sie folgendermaßen vor, um Konfigurationsdaten wiederzuverwenden:

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

Beachten Sie, dass die Konfigurationsdaten kodiert gespeichert werden. Deshalb können die Dateien nicht mit einem Texteditor bearbeitet werden.

4.4.4.3 Passwords

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



Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Type**
  Zeigt den Dateityp an.
- **Description**
  Zeigt die Kurzbeschreibung des Dateityps an.
- **Enabled**
  Wenn aktiviert, wird das Passwort verwendet. Nur aktivierbar, wenn das Passwort konfiguriert ist.
- **Password**
  Geben Sie das Passwort für die Datei ein.
- **Password Confirmation**
  Bestätigen Sie das Passwort.
- **Status**
  Zeigt an, ob die aktuellen Einstellungen zur Datei auf dem Gerät passen.
  - valid
    Die Einstellungen sind gültig.
  - invalid
    Die Einstellungen sind ungültig
  - '-'
    Status nicht auswertbar.

Vorgehensweise

1. Tragen Sie bei "Password" das Passwort ein.
2. Um das Passwort zu bestätigen, tragen Sie bei "Password Confirmation" das Passwort nochmals ein.
3. Aktivieren Sie die Option "Enabled".
4. Klicken Sie auf die Schaltfläche "Set Values".

4.4.5 Events

4.4.5.1 Configuration

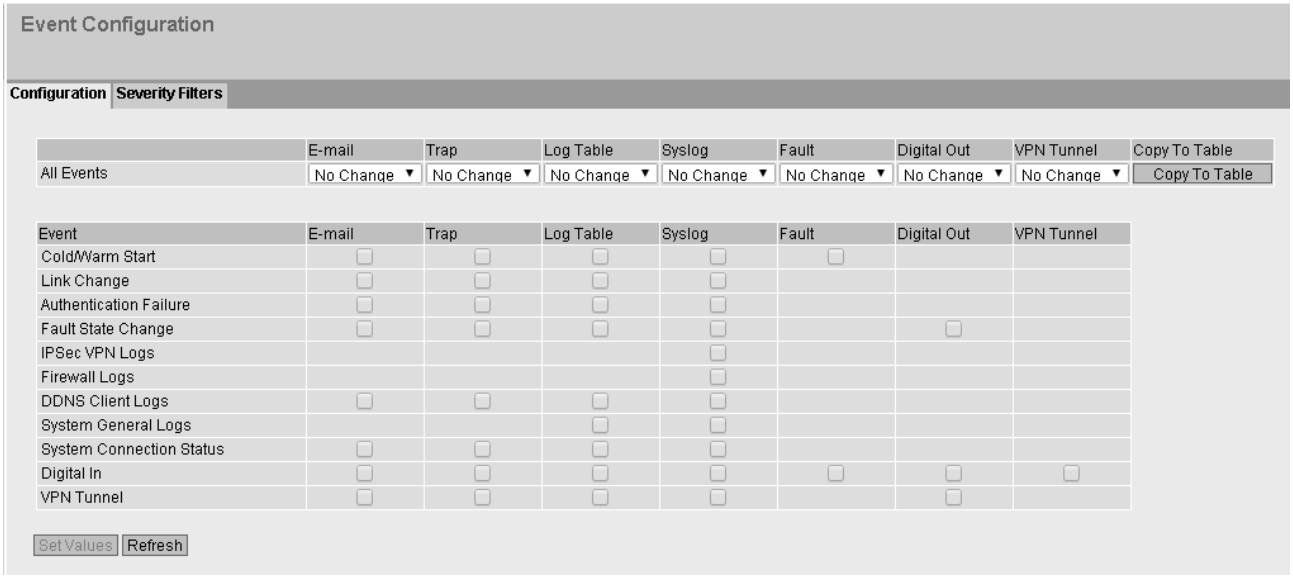
Systemereignisse auswählen

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
- Betriebsstatus des Geräts, z. B. ob ein PLUG vorhanden ist oder nicht.
- Status unerledigter Fehler

Um die Meldungen zusätzlich an einen Syslog-Server zu senden, aktivieren Sie bei "Syslog".



Beschreibung

Die Tabelle 1 gliedert sich in folgende Spalten:

- **Event**
  Zeigt an, dass die Einstellungen für alle Ereignisse der Tabelle 2 gültig sind.
- **E-Mail / Trap / Log Table / Syslog / Fault / Digital Out / VPN Tunnel**
  Aktivieren oder deaktivieren Sie die gewünschte Art der Benachrichtigung für alle Ereignisse. Wenn "No Change" ausgewählt ist, bleiben die Einträge der entsprechenden Spalte in der Tabelle 2 unverändert.

- **Copy to Table**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ereignisse der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Event**
  Die Spalte "Event" enthält Folgendes:
  - Cold/Warm Start
    Das Gerät wurde eingeschaltet oder vom Anwender neu gestartet.
  - Link Change
    Dieses Ereignis tritt nur auf, wenn der Port-Status überwacht wird und sich entsprechend geändert hat, siehe "System > Fault Monitoring > Link Change".
  - Authentication Failure
    Dieses Ereignis tritt beim Versuch eines Zugriffs mit fehlerhaftem Kennwort auf.
  - Fault State Change
    Der Fehlerstatus hat sich geändert. Der Fehlerstatus kann sich auf die aktivierte Portüberwachung, auf das Ansprechen der Meldekontakte oder die Spannungsüberwachung beziehen.
  - IPSec VPN Logs
    Im Sicherheitslogbuch wird eingetragen, wenn das IPsec-Verfahren für VPN angewendet wurde.
  - 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 Connection Status
    Der Verbindungsstatus hat sich geändert.
  - System General Logs
    Verbindungsaufbau, Änderung der Konfiguration.
  - Digital In
    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, SRC) geändert hat.

  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 > Configuration" "SNMPv1 Traps" aktiviert ist.
- **Log Table**
  Das Gerät schreibt einen Eintrag in die Ereignisprotokoll-Tabelle, siehe "Information > Log Table"

- **Syslog**
  Das Gerät schreibt einen Eintrag auf den Systemprotokoll-Server. Voraussetzung ist, dass der Systemprotokoll-Server eingerichtet und die Funktion "Syslog-Client" aktiviert ist.
- **Fault**
  Die Fehler-LED am Gerät leuchtet auf.
- **Digital Output**

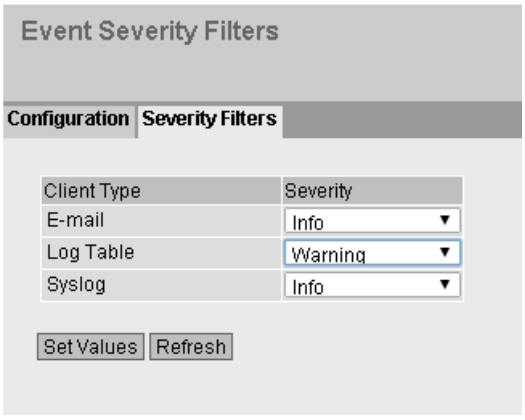
  Steuert den digitalen Ausgang an oder signalisiert die Zustandsänderung mit der LED "DO".
- **VPN Tunnel**
  Steuert die VPN-Verbindung (Aufbau/ Abbau).

Vorgehensweise zur Konfiguration

1. Aktivieren Sie in der Zeile des gewünschten Ereignisses das Optionskästchen. Wählen Sie dabei das Ereignis in der Spalte unter den folgenden Aktionen aus:
   - E-Mail
   - Trap
   - Log Table
   - Syslog
   - Fault
   - Digital Output
   - VPN Tunnel
2. Klicken Sie auf die Schaltfläche "Set Values".

4.4.5.2 Severity Filter

Auf dieser Seite konfigurieren Sie die Fehlerschwere für das Versenden von Systemereignisbenachrichtigungen.



Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

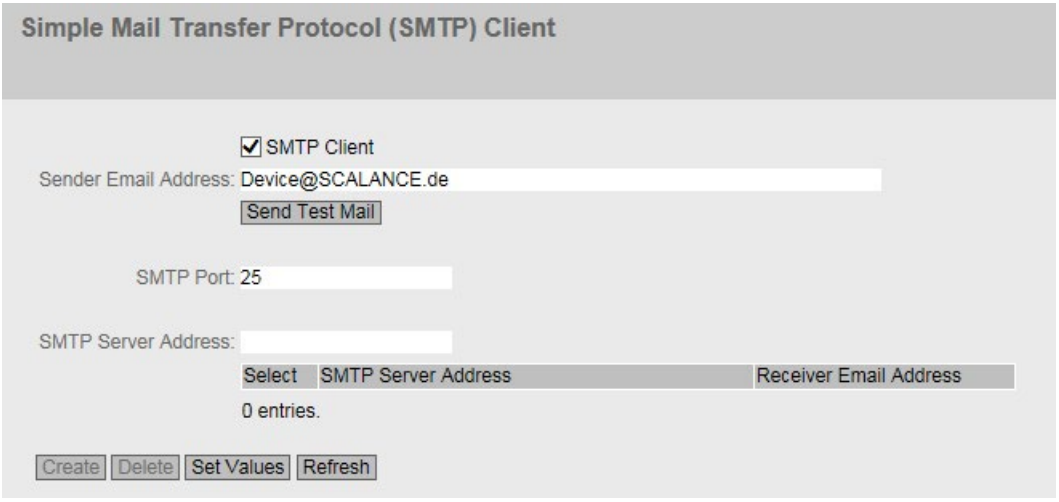
- **Client Type**
  Wählen Sie den Client-Typ, für den Sie die Einstellungen vornehmen:
  - **E-Mail**
    E-Mail Versand von Meldungen per E-Mail.
  - **Log Table**
    Eintragen von Meldungen in die Protokolltabelle.
  - **Syslog**
    Eintragen von Meldungen in die Syslog-Datei
- **Severity**
  Wählen Sie die gewünschte Stufe aus. Folgende Einstellungen sind möglich:
  - **Info**
    Die Meldungen aller Stufen werden versendet bzw. protokolliert.
  - **Warning**
    Die Meldung dieser Stufe und der Stufe "critical" werden versendet bzw. protokolliert.
  - **Critical**
    Nur die Meldungen dieser Stufe werden versendet bzw. protokolliert.

4.4.6 SMTP Client

Netzüberwachung durch E-Mails

Das Gerät bietet die Möglichkeit, beim Auftreten eines Alarmereignisses automatisch eine E-Mail (z.B. an den Netzwerkadministrator) zu senden. Die E-Mail enthält die Identifikation des absendenden Geräts, eine Beschreibung der Alarmursache in Klartext sowie einen Zeitstempel. Damit kann für Netze mit wenigen Teilnehmern eine einfache zentrale Netzüberwachung auf Basis eines E-Mail-Systems aufgebaut werden. Bei eintreffenden E-Mail-Störmeldungen kann über die Identifikation des Absenders per Internet-Browser das WBM gestartet werden, um weitere Diagnoseinformationen auszulesen.

Auf dieser Seite können Sie bis zu drei SMTP-Server und die dazugehörigen E-Mail-Adressen konfigurieren.



Beschreibung

Die Seite enthält folgende Felder:

- **SMTP Client**
  Aktivieren oder deaktivieren Sie den SMTP-Client.
- **Sender Email Address**
  Geben Sie den Absendernamen ein, der in der E-Mail angegeben werden soll, z. B. den Gerätenamen.

  Diese Einstellung gilt für alle konfigurierten SMTP-Server.
- **Send Test Mail**

  Verschicken Sie eine Test-E-Mail, um Ihre Konfiguration zu prüfen.

- **SMTP Port**

  Geben Sie den Port ein, über den Ihr SMTP-Server erreichbar ist.

  Werkseinstellung: 25

  Diese Einstellung gilt für alle konfigurierten SMTP-Server.

- **SMTP Server Address**
  Geben Sie die IP-Adresse oder den FQDN-Namen des SMTP-Servers ein.

Die Tabelle enthält folgende Spalten:

- **Select**
  Aktivieren Sie in einer zu löschenden Zeile das Optionskästchen.
- **SMTP Server Address**
  Zeigt die IP-Adresse oder den FQDN-Namen des SMTP-Servers.
- **Receiver Email Address**
  Geben Sie die E-Mail-Adresse ein, an die das Gerät im Fehlerfall eine E-Mail sendet.

Vorgehensweise

1. Aktivieren Sie die Option "SMTP Client".
2. Geben Sie in das Eingabefeld "SMTP Server Address" die IP-Adresse des SMTP-Servers oder den FQDN-Namen ein.
3. Klicken Sie auf die Schaltfläche "Create". In der Tabelle wird ein neuer Eintrag erzeugt.
4. Geben Sie in das Eingabefeld "Receiver Email Address" die E-Mail-Adresse ein, an die das Gerät im Fehlerfall eine E-Mail senden soll.
5. Klicken Sie auf die Schaltfläche "Set Values".

Hinweis

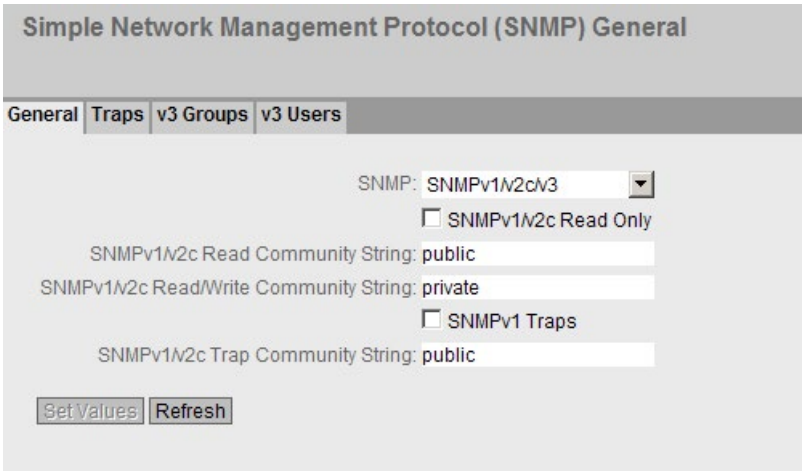
Je nach Eigenschaften und Konfiguration des SMTP-Servers kann es notwendig sein, das Eingabefeld "Sender Email Address" anzupassen. Informieren Sie sich beim Administrator des SMTP-Servers.

4.4.7 SNMP

4.4.7.1 General

Konfiguration von SNMP

Auf dieser Seite treffen Sie grundlegende Einstellungen für SNMP. Aktivieren Sie die Optionen abhängig von der Funktion, die Sie nutzen wollen.



Beschreibung

Die Seite enthält folgende Felder:

- **Klappliste "SNMPv1/v2c/v3"**
  Wählen Sie aus der Klappliste das SNMP-Protokoll. Folgende Einstellungen sind möglich:
  - "-" (Deaktiviert)
    SNMP deaktiviert.
  - SNMPv1/v2c/v3
    SNMPv1/v2c/v3 wird unterstützt.
  - SNMPv3
    Nur SNMPv3 wird unterstützt.
- **Optionskästchen "SNMPv1/v2c Read Only"**
  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.

- **Eingabefeld "SNMPv1/v2c Read Community String"**
  Tragen Sie den Community String für den lesenden Zugriff des SNMP-Protokolls ein.
- **Eingabefeld "SNMPv1/v2c Read/Write Community String"**
  Tragen Sie den Community String für den lesenden und schreibenden Zugriff des SNMP-Protokolls ein.
- **Optionskästchen "SNMPv1 Traps"**
  Aktivieren oder deaktivieren Sie das Senden von SNMP-Traps (Alarmtelegramme). Auf dem Register "Trap" legen Sie die IP-Adressen der Geräte fest, an die SNMP Traps gesendet werden.
- **Eingabefeld "SNMPv1/v2c Trap Community String"**
  Tragen Sie den Community String für das Senden von SNMPv1/v2-Meldungen ein.

Vorgehensweise

1. Wählen Sie aus der Klappliste "SNMP" die gewünschte Option:
   - "-" (Deaktiviert)
   - SNMPv1/v2c/v3
   - SNMPv3
2. Aktivieren Sie das Optionskästchen "SNMPv1/v2c Read only", wenn Sie mit SNMPv1/v2c nur lesend auf SNMP-Variablen zugreifen wollen.
3. Tragen Sie im Eingabefeld "SNMPv1/v2c Read Community String" die gewünschte Zeichenkette ein.
4. Tragen Sie in das Eingabefeld "SNMPv1/v2c Read/Write Community String" die gewünschte Zeichenkette ein.
5. Klicken Sie auf die Schaltfläche "Set Values".

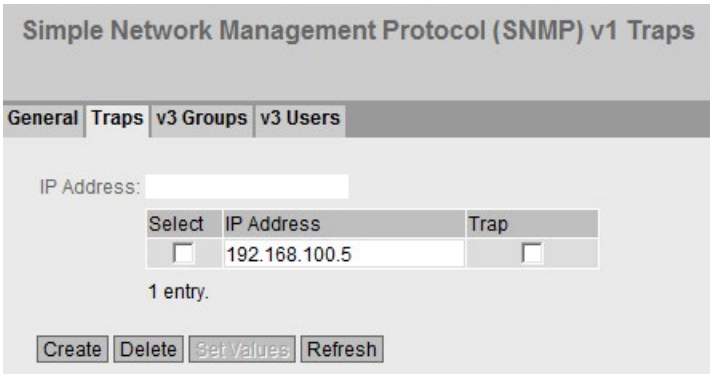
4.4.7.2 Traps

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 "General" oder unter "System > Confguration" die Option "SNMPv1 Traps" aktiviert haben.



Beschreibung

- **IP Address**
  Tragen Sie die IP-Adresse oder den FQDN-Namen 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:

- **Select**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **IP Address**
  Ändern Sie bei Bedarf die IP-Adressen oder die FQDN-Namen der Stationen.
- **Trap**
  Aktivieren oder deaktivieren Sie das Senden von Traps. Stationen, die eingetragen, aber nicht selektiert sind, erhalten keine SNMP-Traps.

Vorgehensweise

Trap-Eintrag erstellen

1. Tragen Sie bei "IP Address" die IP-Adresse oder den FQDN-Namen der Station ein, an die das Gerät Traps senden soll.
2. Klicken Sie auf die Schaltfläche "Create", um einen neuen Trap-Eintrag zu erstellen.
3. Aktivieren Sie in der gewünschten Zeile "Trap".
4. Klicken Sie auf die Schaltfläche "Set Values".

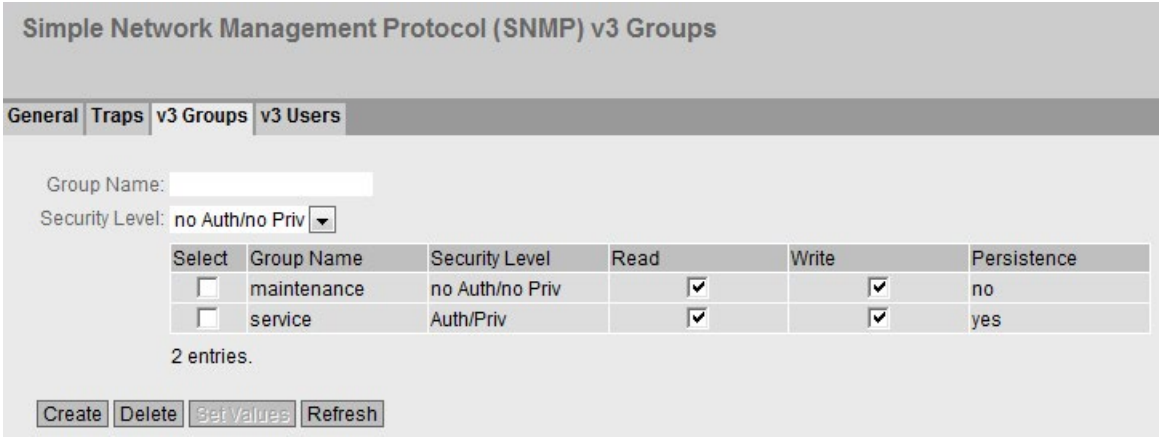
Trap-Eintrag löschen

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

4.4.7.3 Groups

Sicherheitseinstellungen und Rechtevergabe

SNMP Version 3 bietet eine Rechtevergabe, Authentifizierung und Verschlüsselung auf Protokollebene. Die Sicherheitsstufen und die Lese-/Schreibrechte werden gruppenspezifisch definiert. Für jedes Mitglied einer Gruppe gelten automatisch die entsprechenden Einstellungen.



Beschreibung

Die Seite enthält folgende Felder:

- **Group Name**
  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. Bei den Sicherheitsstufen die folgenden Möglichkeiten:

  – No Auth/no Priv
  Keine Authentifizierung aktiviert / keine Verschlüsselung aktiviert.

  – Auth/no Priv
  Authentifizierung aktiviert / keine Verschlüsselung aktiviert.

  – Auth/Priv
  Authentifizierung aktiviert / Verschlüsselung aktiviert.

Die Tabelle gliedert sich in folgende Spalten:

- **Select**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Group Name**
  Zeigt die definierten Gruppennamen an.
- **Security Level**
  Zeigt die konfigurierte Sicherheitsstufe an.

- **Read**
  Aktivieren oder deaktivieren Sie den Lesezugriff für die gewünschte Gruppe.
- **Write**
  Aktivieren oder deaktivieren Sie den Schreibzugriff für die gewünschte Gruppe.

  Hinweis

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

- **Persistence**
  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 Gerätes wieder verschwunden.
  - Yes

    Die Gruppe ist einem SNMPv3-Benutzer zugeordnet.
  - No

    Die Gruppe ist keinem SNMPv3-Benutzer zugeordnet.

Vorgehensweise

Anlegen einer neuen Gruppe

1. Geben Sie bei "Group Name" den gewünschten Gruppennamen ein.
2. Wählen Sie aus der Klappliste "Security Level" die gewünschte Sicherheitsstufe aus.
3. Klicken Sie auf die Schaltfläche "Create", um einen neuen Eintrag zu erzeugen.
4. Legen Sie bei "Read" die gewünschten Leserechte für die Gruppe fest.
5. Legen Sie bei "Write" die gewünschten Schreibrechte für die Gruppe fest.
6. Klicken Sie auf die Schaltfläche "Set Values".

Ändern einer Gruppe

1. Legen Sie bei "Read" die gewünschten Leserechte für die Gruppe fest.
2. Legen Sie bei "Write" die gewünschten Schreibrechte für die Gruppe fest.
3. Klicken Sie auf die Schaltfläche "Set Values".

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.

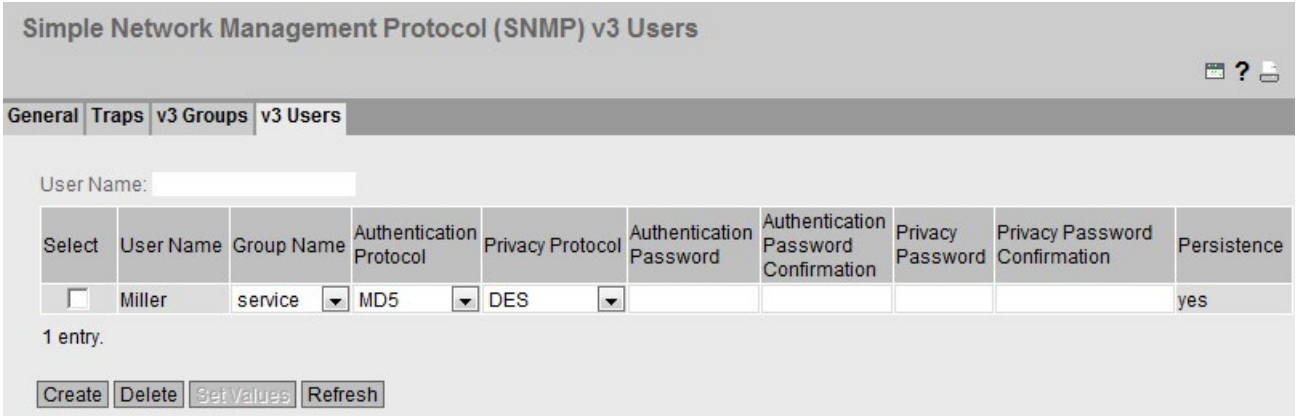
Löschen einer Gruppe

1. Aktivieren Sie in der zu löschenden Zeile "Select".
   Wiederholen Sie den Vorgang für alle Gruppen, die Sie löschen wollen.
2. Klicken Sie auf die Schaltfläche "Delete". Die Einträge werden gelöscht.

4.4.7.4 Users

Benutzerspezifische Sicherheitseinstellungen

Auf der WBM-Seite können Sie SNMPv3-Benutzer neu anlegen, ändern oder löschen. Das benutzerbasierte Sicherheitsmodell arbeitet mit dem Konzept des Benutzernamens, d. h. jedes Telegramm wird mit einer Benutzerkennung versehen. Diesen Benutzernamen und die betreffenden Sicherheitseinstellungen überprüfen sowohl der Absender wie auch der Empfänger.



Beschreibung

Die Seite enthält folgende Felder:

- **User Name**
  Tragen Sie einen frei wählbaren Benutzernamen ein. Nach der Datenübernahme können Sie den Namen nicht mehr ändern.

Die Tabelle gliedert sich in folgende Spalten:

- **Select**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **User Name**
  Zeigt die angelegten Benutzer an.
- **Group Name**
  Wählen Sie die Gruppe aus, die dem Benutzer zugeordnet wird.
- **Authentication Protocol**
  Legen Sie das Authentifizierungsprotokoll fest. Nur aktvierbar, wenn die Gruppe die Funktion unterstützt.

  Folgende Einstellungen gibt es:

  – none
  – MD5
  – SHA

- **Privacy Protocol**
  Legen Sie fest, ob der Benutzer den DES-Algorithmus verwendet. Nur aktivierbar, wenn die Gruppe diese Funktion unterstützt.
- **Authentication Password**
  Geben Sie in das erste Eingabefeld das Authentifizierungspasswort ein. Das Passwort muss mindestens 6 Zeichen lang sein, die maximale Länge beträgt 32 Zeichen.
- **Authentication Password Confirmation**
  Bestätigen Sie das Passwort durch die Wiederholung der Eingabe.
- **Privacy Password**
  Geben Sie Ihr Verschlüsselungspasswort ein. Das Passwort muss mindestens 6 Zeichen lang sein, die maximale Länge beträgt 32 Zeichen.
- **Privacy Password Confirmation**
  Bestätigen Sie das Verschlüsselungspasswort durch die Wiederholung der Eingabe.
- **Persistence**
  Zeigt an, ob der User einer SNMPv3-Gruppe zugeordnet ist. Wenn der User keiner SNMPv3-Gruppe zugeordnet ist, wird kein automatisches Speichern ausgelöst und der konfigurierte User ist nach einem Neustart des Gerätes wieder verschwunden.
  - Yes

    Der User ist einer SNMPv3-Gruppe zugeordnet.
  - No

    Der User ist keiner SNMPv3-Gruppe zugeordnet.

Vorgehensweise

Neuen Benutzer anlegen

1. Geben Sie im Eingabefeld "User Name" den Namen des neuen Benutzers ein.
2. Klicken Sie auf die Schaltfläche "Create". In der Tabelle wird ein neuer Eintrag erzeugt.
3. Wählen Sie bei "Groups" die Gruppe aus, der der neue Benutzer angehören soll.

   Wenn die Gruppe noch nicht angelegt ist, wechseln Sie auf die Seite "v3 Groups" und legen Sie die Einstellungen für diese Gruppe fest.
4. Wenn für die ausgewählte Gruppe eine Authentifizierung notwendig ist, wählen Sie bei "Authentification Protocol" 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 "Privacy Protocol" den Algorithmus aus. Tragen Sie in die entsprechenden Eingabefelder das Verschlüsselungspasswort sowie dessen Bestätigung ein.
6. Klicken Sie auf die Schaltfläche "Set Values".

Benutzer löschen

1. Aktivieren Sie in der zu löschenden Zeile "Select".
   Wiederholen Sie den Vorgang für alle Benutzer, die Sie löschen wollen.
2. Klicken Sie auf die Schaltfläche "Delete". Der Eintrag wird gelöscht.

Hinweis

Wenn Sie vor diesem Schritt eine andere Schaltfläche z. B. die Schaltfläche "Refresh" anklicken, wird der Löschvorgang abgebrochen. Die Daten der markierten Zeilen bleiben erhalten. Die Markierungen werden entfernt. Wenn Sie den Vorgang wiederholen wollen, dann müssen Sie die zu löschenden Datensätze neu markieren.

4.4.8 System Time

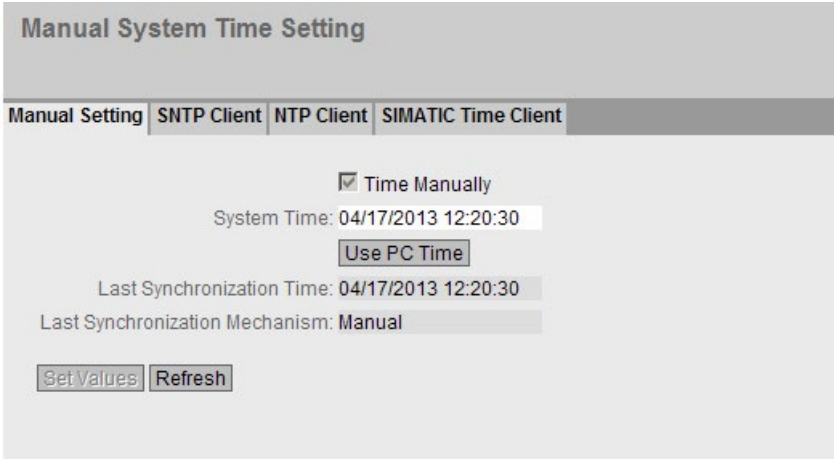
Um die Systemzeit des Geräts einzustellen, gibt es unterschiedliche Methoden. Es kann immer nur eine Methode aktiv sein.

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

4.4.8.1 Manual Setting

Manuelle Einstellung der Systemzeit

Auf dieser Seite stellen Sie selbst das Datum und die Uhrzeit des Systems ein. Damit diese Einstellung verwendet wird, müssen Sie "Time Manually" aktivieren.



Beschreibung

Die Seite enthält folgende Felder:

- **Time Manually**
  Aktivieren oder deaktivieren Sie die manuelle Zeiteinstellung. Wenn Sie die Option aktivieren, wird das Eingabefeld "System Time" editierbar.
- **System Time**
  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
- **Use PC Time**
  Klicken Sie auf die Schaltfläche, um die Zeiteinstellung des PCs zu übernehmen.
- **Last Synchronization Time**
  Dieses Feld ist nur lesbar und zeigt an, wann die letzte Uhrzeitsynchronisation stattgefunden hat. Wenn keine Uhrzeitsynchronisation möglich war, enthält das Feld die Angabe "Date/time not set".
- **Last Synchronization Mechanism**
  Dieses Feld zeigt an, wie die letzte Zeitsynchronisation durchgeführt wurde.
  - Not set
    Die Zeit wurde nicht eingestellt.
  - Manual
    Manuelle Zeiteinstellung
  - SNTP
    Automatische Zeitsynchronisation über SNTP
  - NTP
    Automatische Zeitsynchronisation über NTP
  - SIMATIC
    Automatische Zeitsynchronisation über SIMATIC-Uhrzeittelegramm
  - PTP
    Automatische Zeitsynchronisation über PTP

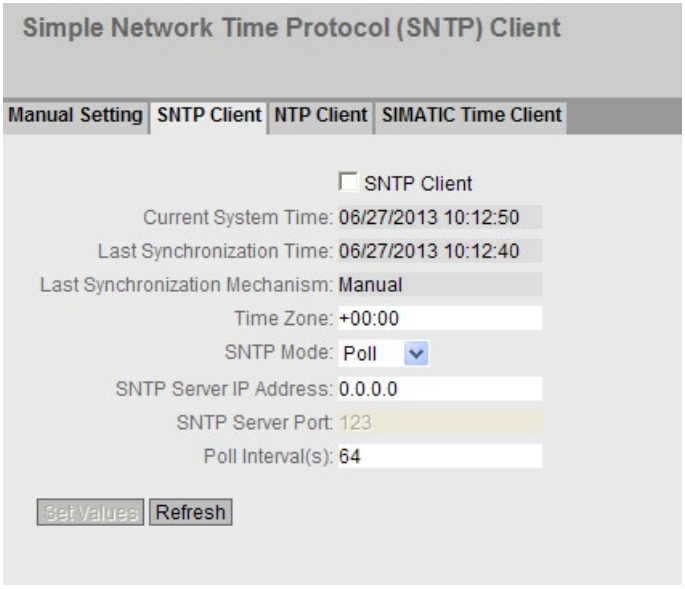
Vorgehensweise

1. Aktivieren Sie die Option "Time Manually".
2. Klicken Sie in das Eingabefeld "System Time".
3. Geben Sie im Eingabefeld "System Time" Datum und Uhrzeit im Format " MM/DD/YYYY HH:MM:SS" ein.
4. Klicken Sie auf die Schaltfläche "Set Values".
   Datum und Uhrzeit werden übernommen und im Feld "Last Synchronization Mechanism" wird "Manual" eingetragen.

4.4.8.2 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.



Beschreibung

Die Seite enthält folgende Felder:

- **SNTP Client**
  Aktivieren oder deaktivieren Sie die automatische Zeitsynchronisation über SNTP.
- **Current System Time**
  Zeigt die aktuell im System eingestellten Werte für Datum und Uhrzeit an.
- **Last Synchronization Time**
  Dieses Feld ist nur lesbar und zeigt an, wann die letzte Uhrzeitsynchronisation stattgefunden hat.
- **Last Synchronization Mechanism**
  Dieses Feld zeigt an, wie die letzte Zeitsynchronisation durchgeführt wurde. Folgende Arten gibt es:
  - Not set
    Die Zeit wurde nicht eingestellt.
  - Manual
    Manuelle Zeiteinstellung
  - SNTP
    Automatische Zeitsynchronisation über SNTP

  - NTP
    Automatische Zeitsynchronisation über NTP
  - SIMATIC
    Automatische Zeitsynchronisation über SIMATIC-Uhrzeittelegramm
  - PTP

    Automatische Zeitsynchronisation über PTP

- **Time Zone**
  Geben Sie die 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.
- **SNTP Mode**
  Wählen Sie aus der Klappliste die Synchronisationsart aus. Folgende Synchronisierungsarten sind möglich:
  - Poll
    Wenn Sie diese Protokollart wählen, werden die Eingabefelder "SNTP Server IP Address", "SNTP Server Port" und "Poll Interval(s)" zur weiteren Konfiguration eingeblendet. Bei dieser Synchronisationsart ist das Gerät aktiv und sendet eine Zeitabfrage an den SNTP-Server.
  - Listen
    Bei dieser Synchronisationsart ist das Gerät passiv und "hört" auf SNTP-Telegramme, die die Uhrzeit liefern.
- **SNTP Server IP Address**
  Geben Sie die IP-Adresse des SNTP-Servers ein.
- **SNTP Server Port**
  Geben Sie den Port des SNTP-Servers ein.
  Folgende Ports sind möglich:
  - 123 (Standard-Port)
  - 1025 bis 36564
- **Poll Interval(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.

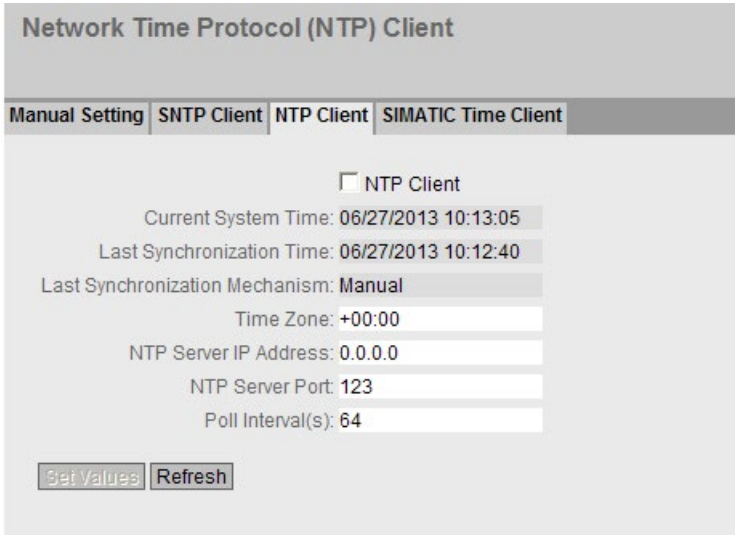
Vorgehensweise

1. Klicken Sie in das Optionskästchen "SNTP Client", um die automatische Zeiteinstellung zu aktivieren.
2. Geben Sie in das Eingabefeld "Time Zone" die lokale Zeitdifferenz zur Weltzeit (UTC) ein. Das Eingabeformat ist "+/-HH:MM" (z.B. +02:00 für MESZ, die mitteleuropäische Sommerzeit), da der SNTP-Server immer die UTC-Zeit sendet. Diese Zeit wird dann mithilfe der Angabe für die Zeitzone in die lokale Zeit umgerechnet. Im Gerät erfolgt keine Umstellung auf Sommerzeit oder Winterzeit. Dies müssen Sie ebenfalls bei der Eingabe in das Eingabefeld "Time Zone" berücksichtigen.
3. Wählen Sie aus der Klappliste "SNTP Mode" aus folgenden Optionen aus:
   - Poll
     Für diese Betriebsart müssen Sie Folgendes konfigurieren:
     - Zeitzonendifferenz (Schritt 2)
     - Zeit-Server (Schritt 4)
     - Port (Schritt 5)
     - Abfrageintervall (Schritt 6)
     - Schließen Sie die Konfiguration mit Schritt 7 ab.
   - Listen
     Für diese Betriebsart müssen Sie Folgendes konfigurieren:
     - Zeitdifferenz zu der vom Server gesendeten Zeit (Schritt 2)
     - Schließen Sie die Konfiguration mit Schritt 7 ab.
4. Geben Sie im Eingabefeld "SNTP Server IP Address" die IP-Adresse des SNTP-Servers ein, dessen Telegramme für die Synchronisation der Uhrzeit verwendet werden sollen.
5. Geben Sie im Eingabefeld "SNTP Server Port" 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 in das Eingabefeld "Poll Interval(s)" die Zeitspanne in Sekunden ein, nach der eine neue Zeitanfrage beim Zeit-Server gestartet werden soll.
7. Klicken Sie auf die Schaltfläche "Set Values", um Ihre Änderungen in das Gerät zu übertragen.

4.4.8.3 NTP Client

Automatische Zeiteinstellung über NTP

Wenn die Uhrzeitsynchronisation über NTP erfolgen soll, können Sie hier die entsprechenden Einstellungen vornehmen.



Beschreibung

Die Seite enthält folgende Felder:

- **NTP Client**
  Markieren Sie dieses Optionskästchen, um die automatische Zeitsynchronisation über NTP zu aktivieren.
- **Current System Time**
  Dieses Feld zeigt die aktuelle Systemzeit an.
- **Last Synchronization Time**
  Dieses Feld ist nur lesbar und zeigt an, wann die letzte Uhrzeitsynchronisation stattgefunden hat.

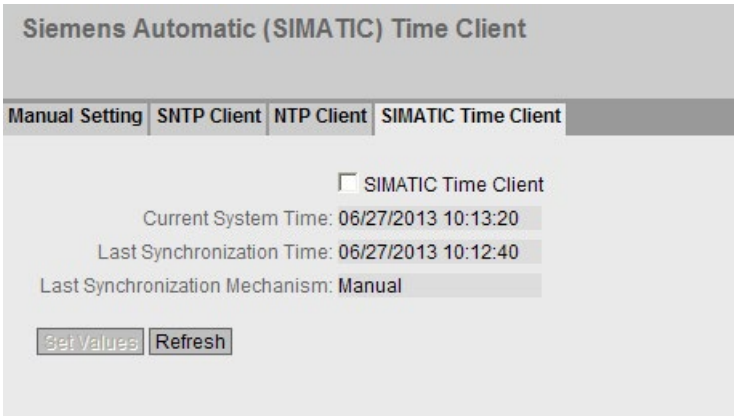
- **Last Synchronization Mechanism**
  Dieses Feld zeigt an, wie die letzte Zeitsynchronisation durchgeführt wurde. Folgende Arten gibt es:
  - Not set
    Die Zeit wurde nicht eingestellt.
  - Manual
    Manuelle Zeiteinstellung
  - SNTP
    Automatische Zeitsynchronisation über SNTP
  - NTP
    Automatische Zeitsynchronisation über NTP
  - SIMATIC
    Automatische Zeitsynchronisation über SIMATIC-Uhrzeittelegramm
  - PTP
    Automatische Zeitsynchronisation über PTP
- **Time Zone**
  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.
- **NTP Server IP Address**
  Geben Sie die IP-Adresse des NTP-Servers an.
- **NTP Server Port**
  Geben Sie den Port des NTP-Servers an.
  Folgende Ports sind möglich:
  - 123 (Standard-Port)
  - 1025 bis 36564
- **Poll Interval(s)**
  Tragen Sie hier den Zeitabstand zwischen zwei Zeitanfragen ein. In diesem Feld geben Sie das Abfrageintervall in Sekunden an. Mögliche Werte sind 64 bis 1024 Sekunden.

Vorgehensweise

1. Klicken Sie in das Optionskästchen "NTP Client", um die automatische Zeiteinstellung über NTP zu aktivieren.
2. Tragen Sie die erforderlichen Werte in die folgenden Felder ein:
   - Zeitzone
   - NTP-Server IP-Adresse
   - NTP-Server Port
   - Abfrageintervall
3. Klicken Sie auf die Schaltfläche "Set Values".

4.4.8.4 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.
- **Current System Time**
  Dieses Feld zeigt die aktuelle Systemzeit an.
- **Last Synchronization Time**
  Dieses Feld ist nur lesbar und zeigt an, wann die letzte Uhrzeitsynchronisation stattgefunden hat.
- **Last Synchronization Mechanism**
  Dieses Feld zeigt an, wie die letzte Zeitsynchronisation durchgeführt wurde. Folgende Arten gibt es:
  - Not set
    Die Zeit wurde nicht eingestellt.
  - Manual
    Manuelle Zeiteinstellung
  - SNTP
    Automatische Zeitsynchronisation über SNTP
  - NTP
    Automatische Zeitsynchronisation über NTP
  - SIMATIC
    Automatische Zeitsynchronisation über SIMATIC-Uhrzeittelegramm
  - PTP
    Automatische Zeitsynchronisation über PTP

Vorgehensweise

1. Klicken Sie in das Optionskästchen "SIMATIC Time Client", um den SIMATIC Time Client zu aktivieren.
2. Klicken Sie auf die Schaltfläche "Set Values".

4.4.9 Auto Logout

Einstellung der automatischen Abmeldung

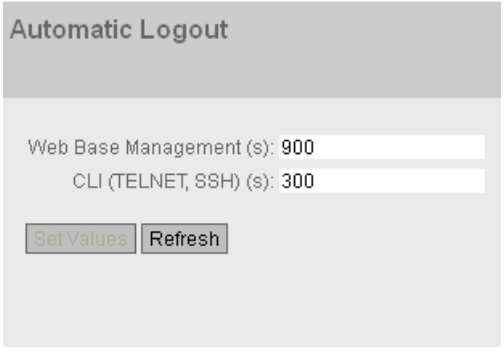
Stellen Sie in dieser Seite die Zeiten ein, nach denen bei Inaktivität des Benutzers automatisch eine Abmeldung vom WBM oder dem CLI erfolgt.

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 der "Keep alive"- Funktion. Ist das eingestellte Zeitintervall kleiner als die projektierte Zeit, dann gilt der kleinere Wert. Z. B. Sie haben bei der automatischen Abmeldung 300 Sekunden eingestellt und bei der "Keep alive"- Funktion steht 120 Sekunden. In diesem Fall wird alle 120 Sekunden ein Paket gesendet, das die Verbindung aufrechterhält.



Vorgehensweise

1. Tragen Sie in das Eingabefeld "Web Base Management (s)" einen Wert von 60-3600 Sekunden ein. Wenn Sie den Wert 0 eintragen, ist die automatische Abmeldung deaktiviert.
2. Tragen Sie in das Eingabefeld "CLI (TELNET, SSH) (s)" einen Wert von 60-600 Sekunden ein. Wenn Sie den Wert 0 eintragen, ist die automatische Abmeldung deaktiviert.
3. Klicken Sie auf die Schaltfläche "Set Values".

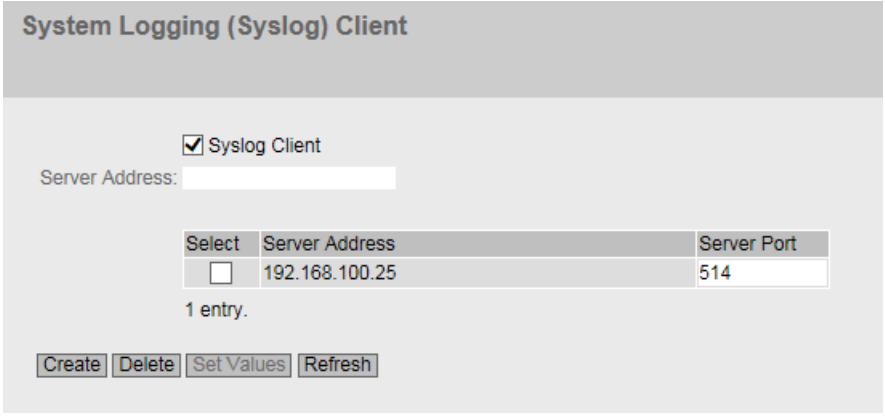
4.4.10 Syslog Client

Systemereignis-Agent

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 der Protokolleinträge:

- 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 oder der FQDN-Name des Syslog-Servers ist im Gerät eingetragen.



Beschreibung

Die Seite enthält folgende Felder:

- **Syslog Client**
  Aktivieren oder deaktivieren Sie die Syslog-Funktion.
- **Server IP Address**
  Geben Sie die IP-Adresse oder den FQDN-Namen des Syslog-Servers an.

Die Tabelle enthält folgende Spalten

- **Select**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Server Address**
  Zeigt die IP-Adresse oder den FQDN-Namen 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 "Set Values".

Neuen Eintrag anlegen

1. Geben Sie in das Eingabefeld "Server IP Address" die IP-Adresse oder den FQDN-Namen des Syslog-Servers ein, auf dem die Protokolleinträge gespeichert werden sollen.
2. Klicken Sie auf die Schaltfläche "Create". 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 "Set Values".

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 "Delete". Alle markierten Einträge werden gelöscht und die Anzeige wird aktualisiert.

4.4.11 Fault Monitoring

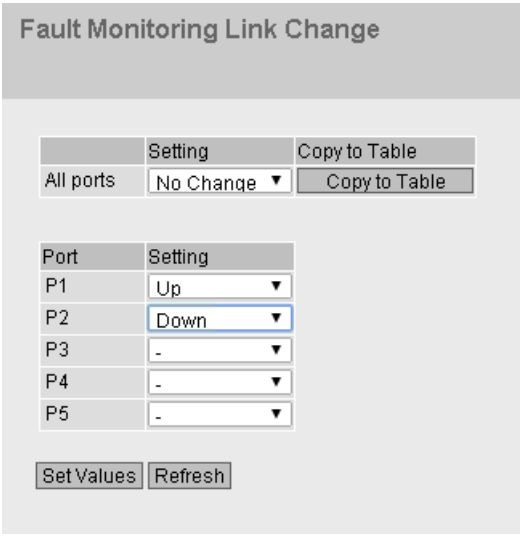
Konfiguration der Fehlerüberwachung von Zustandsänderungen bei Verbindungen

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.
- **Setting**
  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellungsmöglichkeiten haben Sie:
  - "-" (Deaktiviert)
  - Up
  - Down
  - No Change: Einstellung in der Tabelle 2 bleibt unverändert.

- **Copy to Table**

  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. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Setting**

  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 "Set Values".

Fehlerüberwachung für alle Ports konfigurieren

1. Wählen Sie in der Klappliste der Spalte "Setting" die gewünschte Einstellung aus.
2. Klicken Sie auf die Schaltfläche "Copy to Table". Die Einstellung wird für alle Ports der Tabelle 2 übernommen.
3. Klicken Sie auf die Schaltfläche "Set Values".

4.4.12 PLUG

4.4.12.1 Configuration

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. 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

Die Aktion wird erst dann durchgeführt, wenn Sie auf die Schaltfläche "Set Values" klicken.

Die Aktion kann nicht rückgängig gemacht werden.

Wenn Sie sich nach der Auswahl gegen die Ausführung entscheiden, dann klicken Sie auf die Schaltfläche "Refresh". Dadurch werden die Daten dieser Seite aus dem Gerät neu ausgelesen und Ihre Auswahl wird aufgehoben.

Beschreibung

Die Tabelle gliedert sich in folgende Zeilen:

- **State**
  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 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.
- **Device Group**
  Zeigt an, von welcher SIMATIC NET-Produktlinie der C-PLUG im vorangegangenen Betrieb genutzt wurde.

- **Device Type**
  Zeigt den Gerätetyp innerhalb der Produktlinie an, von dem der C-PLUG im vorangegangenen Betrieb genutzt wurde.
- **Configuration Revision**
  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.
- **File System**
  Zeigt den Typ des Dateisystems an, das auf dem PLUG vorhanden ist.
- **File System Size [Byte]**
  Zeigt die maximale Speicherkapazität des Dateisystems an, das auf dem PLUG vorhanden ist.
- **File System Usage [Byte]**
  Zeigt den belegten Speicherplatz im Dateisystem des PLUG an.
- **Info String**
  Zeigt zusätzliche Informationen über das Gerät an, das den PLUG im vorangegangenen Betrieb genutzt hatte, z. B. Bestellnummer, 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.
- **Klappliste "Modify PLUG"**
  Wählen Sie aus der Klappliste die Einstellung. Sie haben folgende Möglichkeiten, um die Konfiguration auf dem C-PLUG zu ändern:
  - Write current configuration to PLUG
    Diese Option ist nur verfügbar, wenn der Status des PLUG "NOT ACCEPTED" oder "FACTORY" ist.
    Die im internen Flash-Speicher des Gerätes vorhandene Konfiguration wird auf den PLUG kopiert.
  - Erase PLUG to factory default
    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 "Modify PLUG" die gewünschte Option aus.
3. Klicken Sie auf die Schaltfläche "Set Values".

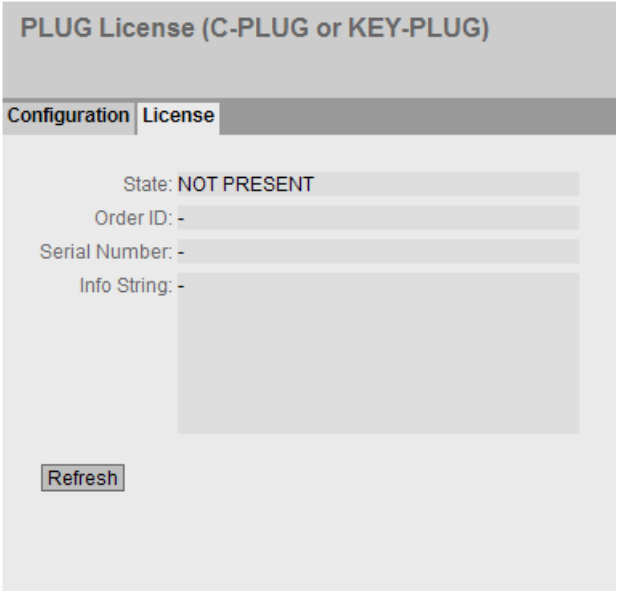
4.4.12.2 License

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. 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 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

- **State**
  Zeigt den Status des KEY-PLUG an. Es gibt die folgenden Möglichkeiten:
  - ACCEPTED
    Der im Gerät vorhandene KEY-PLUG enthält eine passende und gültigen Lizenz.
  - 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.
- **Order ID**
  Zeigt die Bestellnummer des KEY-PLUG an. Es gibt den KEY-PLUG für unterschiedliche Funktionserweiterungen und für verschiedene Zielsysteme.
- **Serial Number**
  Zeigt die Serien-Nummer des KEY-PLUG.
- **Info String**
  Zeigt zusätzliche Informationen über das Gerät an, das den KEY-PLUG im vorangegangenen Betrieb genutzt hatte, z. B. Bestellnummer, 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.

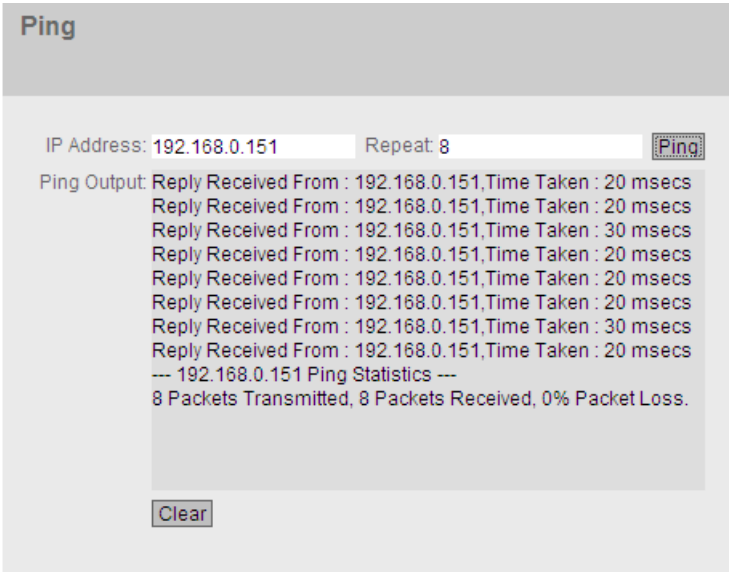
Hinweis

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 Artikelnummer / Lizenz gesteckt ist.

4.4.13 Ping

Erreichbarkeit einer Adresse in einem IP-Netzwerk

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



Beschreibung

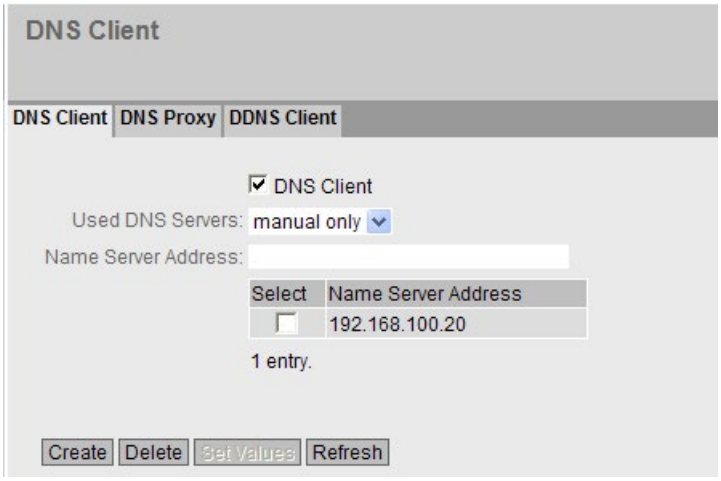
Die Tabelle gliedert sich in folgende Spalten:

- **Eingabefeld "IP Address"**
  Tragen Sie die IP-Adresse des Geräts ein.
- **Eingabefeld "Repeat"**
  Tragen Sie die Anzahl der Ping-Anforderungen ein.
- **Schaltfläche "Ping"**
  Klicken Sie diese Schaltfläche, um die Ping-Funktion zu starten.
- **Ping Output**
  Dieses Feld zeigt die Ausgabe der Ping-Funktion an.
- **Schaltfläche "Clear"**
  Klicken Sie diese Schaltfläche, um das Feld "Ping Output" zu leeren.

4.4.14 DNS

4.4.14.1 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:

- **Optionskästchen "DNS Client"**
  Aktivieren oder deaktivieren Sie, dass das Gerät als DNS-Client fungiert.
- **Klappliste "Used DNS Server"**
  - learned only
    Das Gerät verwendet die DNS-Server, die automatisch zugewiesen werden.
  - manual only
    Das Gerät verwendet den DNS-Server, den Sie bei "Name Server Address" eingetragen haben. Der DNS-Server muss mit dem Internet verbunden sein. Maximal zwei DNS-Server sind projektierbar.
  - all
    Das Gerät verwendet beides.
- **Eingabefeld "Name Server Address"**

  Geben Sie die IP-Adresse des DNS-Servers ein.

Die Tabelle gliedert sich in folgende Spalten:

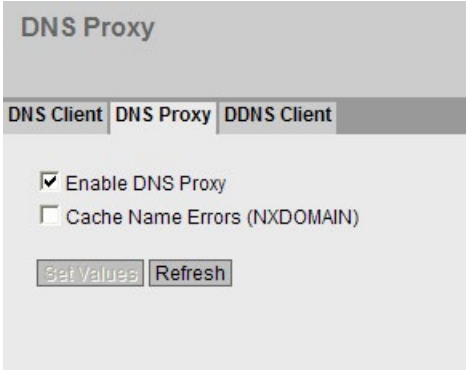
- **Select**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen

- **Name Server Address**
  Zeigt die IP-Adresse des DNS-Servers an.
- **Origin**
  Zeigt an, ob der DNS-Server manuell konfiguriert oder zugewiesen wurde

4.4.14.2 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:

- **Optionskästchen "Enable DNS Proxy"**
  Aktivieren oder deaktivieren Sie den Proxy des DNS-Servers.
- **Optionskästchen "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.

4.4.14.3 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:

- **Service**
  Zeigt an, welche Anbieter unterstützt werden.
- **Enabled**
  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.
- **User name**
  Tragen Sie den Benutzernamen ein, mit dem sich das Gerät am DDNS-Server anmeldet.
- **Password**
  Tragen Sie das dem Benutzer zugeordnete Passwort ein.
- **Password Confirmation**
  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.

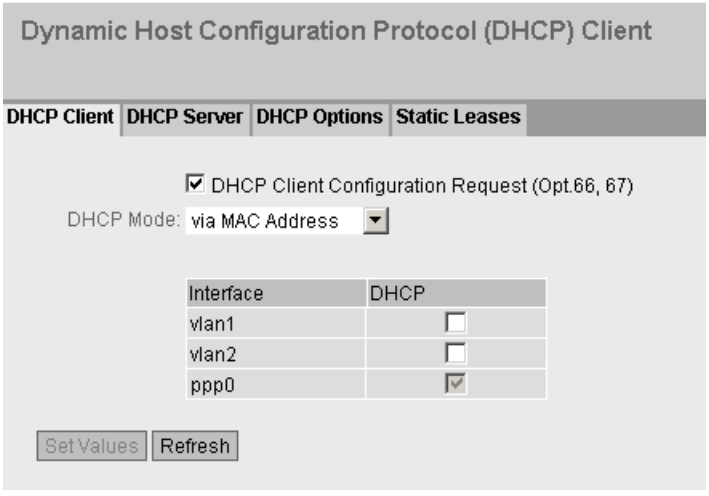
1. Tragen Sie bei "Host" den Hostnamen ein, den Sie für das Gerät mit Ihrem DDNS-Anbieter vereinbart haben, z. B. example.no-ip-com.
2. Tragen Sie die Login-Daten (Username, Password) für den DDNS-Server ein.
3. Aktivieren Sie "Enable". Dieser Hostnamen wird für das Gerät verwendet.
4. Klicken Sie auf "Set Values".

4.4.15 DHCP

4.4.15.1 DHCP Client

Einstellung der DHCP-Betriebsart

Wenn die DHCP-Betriebsart aktiviert ist, startet der DHCP-Client bei einem konfigurierten DHCP-Server eine DHCP-Anfrage und erhält als Antwort eine IP-Adresse zugewiesen. Der Server verwaltet einen Adressbereich, aus welchem er IP-Adressen vergibt. Es ist auch möglich den Server so zu konfigurieren, dass der Client auf seine Anfrage immer dieselbe IP-Adresse zugewiesen bekommt.



Beschreibung

Die Seite enthält folgende Felder:

- **Optionskästchen "DHCP Client Config File Request (Opt.66, 67)"**
  Aktivieren Sie diese Option, wenn der DHCP-Client die Optionen 66, und 67 dazu verwenden soll, eine Konfigurationsdatei herunterzuladen und diese dann zu aktivieren.
- **Klappliste "DHCP Mode"**
  Wählen Sie aus der Klappliste die DHCP-Betriebsart. Folgende Betriebsarten sind möglich:
  - via MAC Address
    Die Identifikation läuft über die MAC-Adresse ab.
  - via DHCP Client ID
    Die Identifikation läuft über eine frei definierte DHCP-Client-ID ab.
  - via System Name
    Die Identifikation läuft über den Systemnamen ab. Ist der Systemname 255 Zeichen lang, dann wird das letzte Zeichen nicht zur Identifikation benutzt.

Die Tabelle gliedert sich in folgende Spalten:

- **Interface**
  Schnittstelle, auf die sich die Einstellung bezieht.
- **DHCP**
  Aktivieren oder deaktivieren Sie den DHCP-Client für die entsprechende Schnittstelle.

Vorgehensweise

Gehen Sie folgendermaßen vor, um die IP-Adresse via DHCP Client ID zu konfigurieren:

1. Aktivieren Sie die Option "DHCP Client".
2. Wählen Sie aus der Klappliste "DHCP Mode" die DHCP-Betriebsart "via DHCP Client ID".
3. Geben Sie in das aktivierte Eingabefeld "DHCP Client ID" eine Zeichenkette zur Identifikation des Gerätes ein. Diese wird dann vom DHCP-Server ausgewertet.
4. Wählen Sie die Option "Client Config File Request (Opt.66, 67)", wenn der DHCP-Client die Optionen 66 und 67 dazu verwenden soll, eine Konfigurationsdatei herunterzuladen und diese dann zu aktivieren.
5. Klicken Sie auf die Schaltfläche "Set Values".

Hinweis

Wird eine Konfigurationsdatei heruntergeladen, so löst dies einen Neustart des Systems aus. Achten Sie darauf, dass in dieser Konfigurationsdatei die Option "Client Config File Request (Opt.66, 67)" nicht mehr gesetzt ist.

4.4.15.2 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 verteilt oder es wird eine bestimmte IP-Adresse einem bestimmten Gerät zugewiesen.

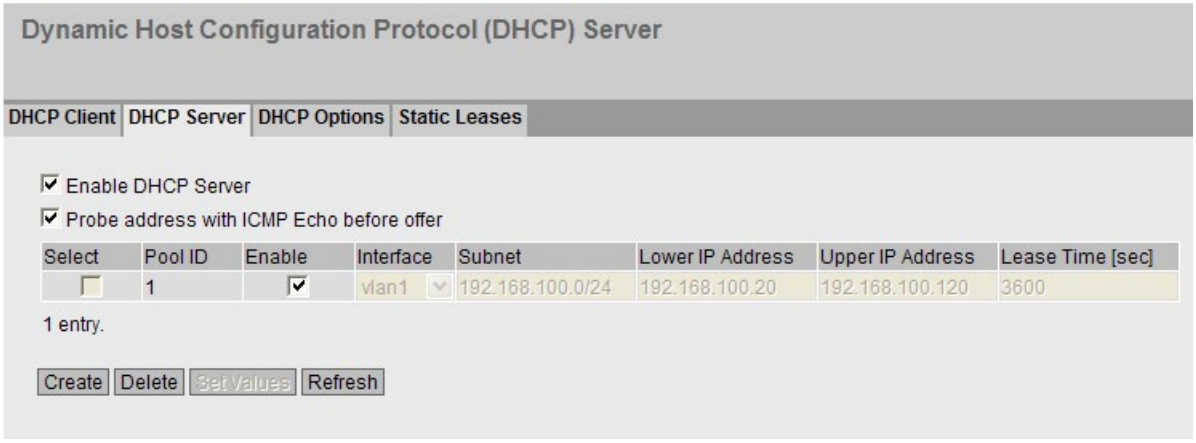
Auf dieser Seite legen Sie das Adressband fest, aus dem das Gerät eine beliebige IP-Adresse erhält. Die statische Zuordnung der IP-Adressen konfigurieren Sie unter "Static Leases".

Hinweis

Maximale Anzahl der IP-Adressen

Die maximale Anzahl der IPv4-Adressen, die der DHCP-Server unterstützt, ist 100. D. h. insgesamt 100 IPv4-Adressen (dynamisch + statisch).

Bei den statischen Zuordnungen können Sie maximal 20 Einträge anlegen.



Voraussetzung

- Die angeschlossenen Geräte sind so konfiguriert, dass diese die IP-Adresse von einem DHCP-Server beziehen.

Beschreibung

Die Seite enthält folgende Felder:

- **Optionskästchen "Enable DHCP Server"**
  Aktivieren oder deaktivieren Sie den DHCP-Server auf dem Gerät.

  Hinweis

  Damit keine Konflikte mit IPv4-Adressen entstehen, darf im Netzwek nur ein Gerät als DHCP-Server konfiguriert sein.

- **Optionskästchen "Probe address with ICMP Echo before offer"**
  Wenn aktiviert, prüft der DHCP-Server, ob die IP-Adresse schon vergeben ist. Dazu sendet der DHCP-Server ICMP-Echomeldungen (ping) an die IP-Adresse. Wenn keine Antwort zurückkommt, kann der DHCP-Server die IP-Adresse vergeben.

  Hinweis

  Wenn es in Ihrem Netzwerk Geräte gibt, bei denen der Echo-Dienst standardmäßig deaktiviert ist, kann es zu Konflikten bei den IP-Adressen kommen. Um dies zu vermeiden, vergeben Sie diesen Geräten eine IP-Adresse, die außerhalb des Adressbands liegt.

Die Tabelle gliedert sich in folgende Spalten:

- **Select**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen
- **Pool ID**
  Zeigt die Nummer des Adressbands an. Wenn Sie auf die Schaltfläche "Create" klicken, wird eine neue Zeile mit einer eindeutigen Nummer (Pool ID) angelegt.

- **Enable**
  Legen Sie fest, ob dieses Adressband verwendet wird.

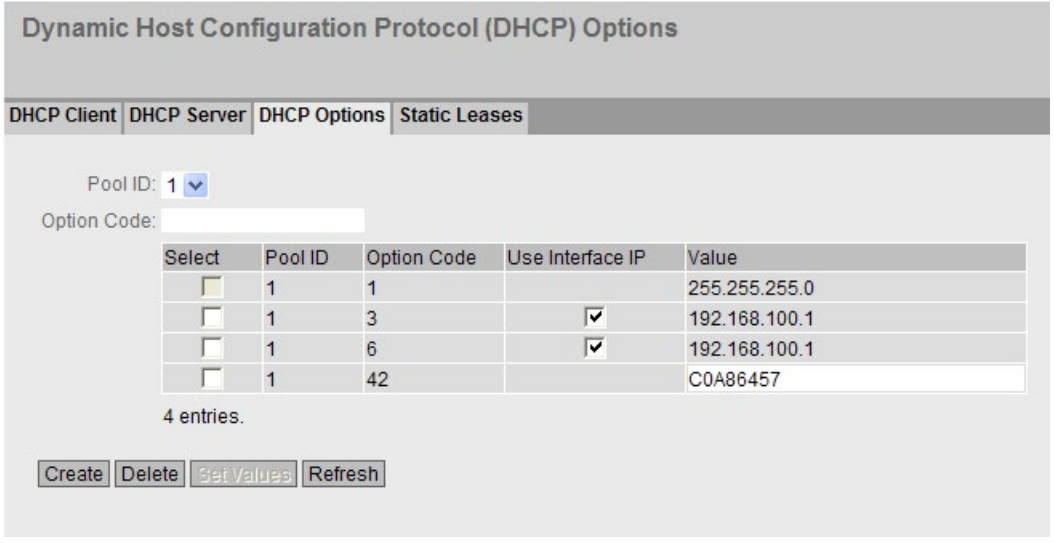
  Hinweis

  Wenn Sie das IPv4-Adressband aktivieren, werden die Register "DHCP Options" und "Static Leases" ausgegraut und sind nicht mehr editierbar.

- **Interface**
  Legen Sie die Schnittstelle fest, über die die IP-Adressen dynamisch vergeben werden.
- **Subnet**
  Tragen Sie den Netzadressbereich ein, die den Geräten zugewiesen wird. Verwenden Sie die CIDR-Schreibweise.
- **Lower IP Address**
  Tragen Sie die IP-Adresse ein, die den Anfang des dynamischen Adressbands festlegt. Die IP-Adresse muss innerhalb des Netzadressbereichs liegen, den Sie bei "Subnet" konfiguriert haben.
- **Upper IP Address**
  Tragen Sie die IP-Adresse ein, die das Ende des dynamischen Adressbands festlegt. Die IP-Adresse muss innerhalb des Netzadressbereichs liegen, den Sie bei "Subnet" konfiguriert haben.
- **Lease Time**
  Legen Sie fest, wie lange die vergebene IP-Adresse gültig bleibt. Nach Ablauf dieser Zeitdauer muss das Gerät entweder eine neue IP-Adresse anfordern oder die Gültigkeitsdauer der vorhandenen IP-Adresse verlängern.

4.4.15.3 DHCP Options

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:

- **Klappliste "Pool ID"**
  Wählen Sie das gewünschte Adressband aus.
- **Eingabefeld "Option Code"**
  Geben Sie die Nummer der gewünschten DHCP-Option ein. Maximal 20 DHCP-Optionen sind möglich.

  Die verschiedenen DHCP-Optionen sind im RFC 2132 definiert.

  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.

  Bei der DHCP-Option 3 wird automatisch die interne IPv4-Adresse des Gerätes als DHCP-Parameter eingestellt

  Hinweis

  Nicht unterstützte DHCP-Optionen

  Die DHCP-Optionen 50 - 60 und 255 werden nicht unterstützt.

Die Tabelle gliedert sich in folgende Spalten:

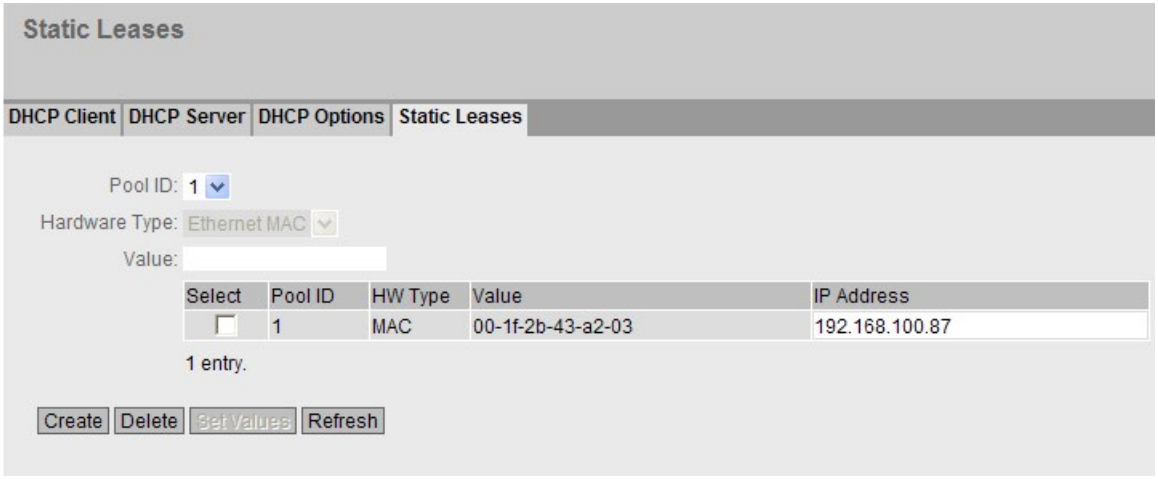
- **Select**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen
- **Pool ID**
  Zeigt die Nummer des Adressbands an.
- **Options Code**
  Zeigt Nummer der DHCP-Option an.
- **Use Interface IP**
  Legen Sie fest, ob die interne IP-Adresse des Geräts verwendet wird oder nicht.
- **Value**
  Geben Sie den Wert ein, der dem DHCP-Client übergeben wird. Der Inhalt ist abhängig von der DHCP-Option.
  - DHCP-Option 67 (Bootfilename)
  - Geben Sie den Namen der Bootdatei im String-Format an.
  - DHCP-Optionen 3 (Router), 6 (DNS) und 66 (TFTP-Server):

    Geben Sie den DHCP-Parameter als IPv4-Adresse an, z. B. 192.168.100.2. Mit Ausnahme der DHCP-Option 3 können Sie bei den DHCP-Optionen mehrere IPv4-Adressen durch Komma getrennt angeben.
  - Alle anderen DHCP-Optionen

    Geben Sie den DHCP-Parameter in Hexadezimal an, z. B. die IPv4-Adresse 192.168.100.2 entspricht "C0A86402".

4.4.15.4 Static Leases

Auf dieser Seite legen Sie fest, dass Geräte mit einer bestimmten MAC-Adresse oder Client-ID der vorgegebenen IP-Adresse zugeordnet werden.



Beschreibung

Die Seite enthält folgende Felder:

- **Klappliste "Pool ID"**
  Wählen Sie das gewünschte Adressband aus.
- **Klappliste "Hardware Type"**
  Legen Sie fest, nach welchem Kriterium die IP-Adresse festgelegt wird.
  - Ethernet MAC
    Die Identifikation läuft über die MAC-Adresse ab. Tragen Sie bei "Value" 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.
  - Non-HW-IP
    Die Identifikation läuft über eine frei definierte DHCP-Client-ID ab. Tragen Sie bei "Value" die gewünschte Bezeichnung ein.
- **Eingabefeld "Value"**
  Tragen Sie den Wert ein. Der Eintrag ist abhängig vom gewählten Kriterium bei "Hardware Type".

Hinweis

Maximal 20 Einträge sind möglich.

Die Tabelle gliedert sich in folgende Spalten:

- **Select**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Pool ID**
  Zeigt die Nummer des Adressbands an.

- **HW Type**
  Zeigt an, ob die IP-Adresse abhängig von der MAC-Adresse (MAC) ist oder nicht (Non-HW).
- **Value**
  Wert, dem die IP-Adresse zugeordnet wird.
- **IP Address**
  Legen Sie die IP-Adresse fest. Die IP-Adresse muss zum Subnetz des Adressbands passen.

4.4.16 SRS

Siemens Remote Service

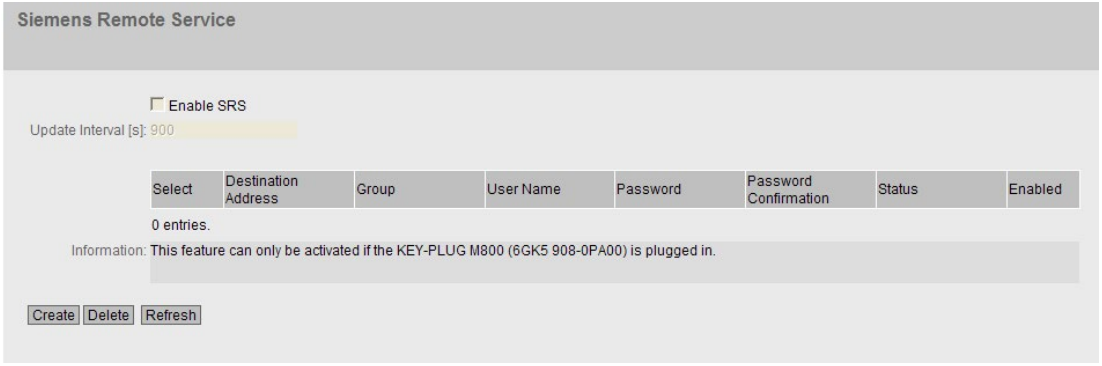
Hinweis

Diese Funktion ist nur mit KEY PLUG nutzbar.

Hinweis

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 SRS wenden Sie sich an Ihren Siemens-Ansprechpartner vor Ort und besuchen Sie http://support.automation.siemens.com/WW/view/de/42346681 (http://support.automation.siemens.com/WW/view/de/42346681).



Beschreibung

Die Seite enthält folgende Felder

- **Optionskästchen "Enable SRS"**

  Aktivieren oder deaktivieren Sie die Nutzung von SRS.

- **Update Interval (s)**

  Tragen Sie die Zeitspanne ein, nach der die IP-Adresse an den gewünschten Zielserver übertragen wird.

Die Tabelle gliedert sich in folgende Spalten:

- **Select**

  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen. Klicken Sie auf "Delete", um den Eintrag zu löschen.

- **Destination Address**

  Geben Sie die IP-Adresse des Zielservers ein.

- **Group**

  Geben Sie den Gruppennamen ein.

- **User Name**

  Geben Sie den Benutzernamen für den Zugang am Zielserver ein.

- **Password**

  Geben Sie das Passwort für den Zugang am Zielserver ein.

Hinweis

Für Benutzername und Passwort sind folgende darstellbare ASCII-Zeichen erlaubt:

- a b c d e f g h I j k l m n o p q r s t u v w x y z
- A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
- 0 1 2 3 4 5 6 7 8 9
- ! $ % & ' ( ) * + , . / : ; < = > ? @ [\ ] ^ _ ` { | }

- **Password Confirmation**

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

- **Status**

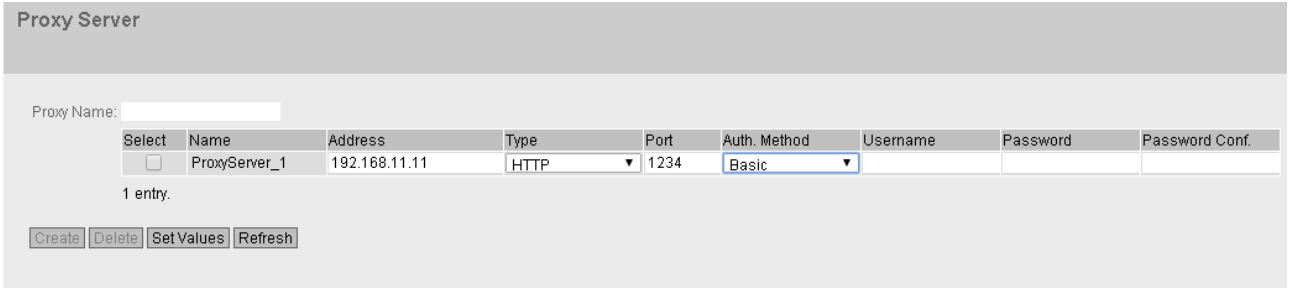
  Zeigt den Status der letzten Übermittlung der eigenen externen IP-Adresse zum Server an.

- **Enabled**

  Wenn aktiviert, wird die externe IP-Adresse an diesen Zielserver übermittelt. Die Übertragung erfolgt über das gesicherte HTTPS-Protokoll. Das Verfahren ist vergleichbar mit dem DDNS-Dienst und erfordert einen entsprechenden Zugang auf der Server-Seite.

4.4.17 Proxy Server

Auf dieser WBM-Seite konfigurieren Sie den Proxy-Server, der von verschiedenen Komponenten verwendet wird, z. B. OpenVPN, SINEMA RC.



Beschreibung

- **Proxy Name**

  Tragen Sie einen Namen für den Proxy-Server ein.

Die Tabelle gliedert sich in folgende Spalten:

- **Select**

  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen. Klicken Sie auf "Delete", um den Eintrag zu löschen.

- **Address**

  Tragen Sie die IPv4-Adresse des Proxy-Servers ein.

- **Type**

  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. Method**

  Legen Sie die Authentifizierungsmethode fest.

  – None
  Ohne Authentifizierung

  – Basic
  Standardauthentifizierung. Benutzernamen und Passwort werden unverschlüsselt gesendet.

  – NTML (NT LAN Manager)
  Authentifizierung nach NTML Standard (Windows-Benutzeranmeldung)

- **User Name**

  Geben Sie den Benutzernamen für den Zugang zum Proxy-Server ein.

- **Password**

  Geben Sie das Passwort für den Zugang zum Proxy-Server ein.

- **Password Conf.**

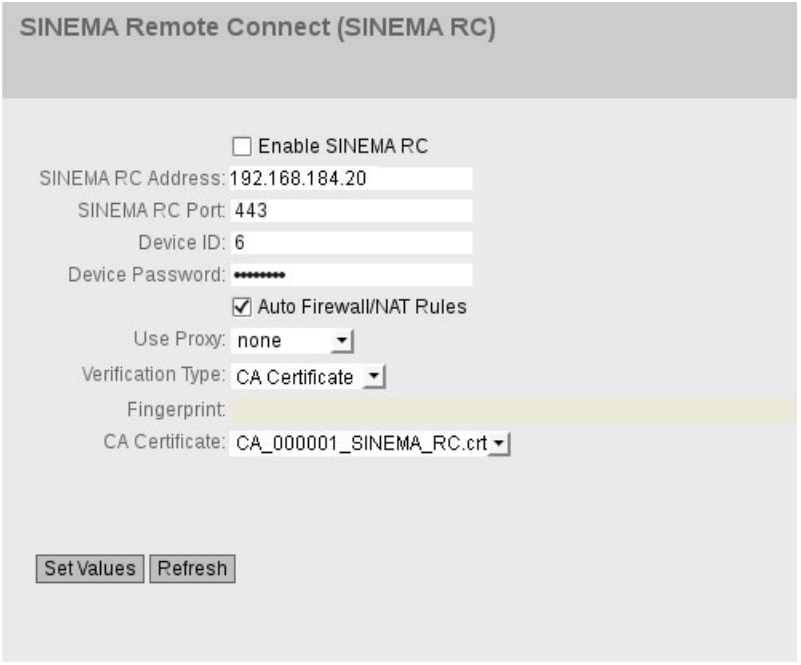
  Geben Sie nochmals das Passwort ein, um es zu bestätigen.

4.4.18 SINEMA RC

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

Hinweis

Diese Funktion ist nur mit KEY PLUG nutzbar.



Beschreibung

Die Seite enthält Folgendes:

- **Optionskästchen "Enable SINEMA RC"**
  - 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.

- **Eingabefeld "SINEMA RC Address"**

  Geben Sie die IPv4-Adresse oder den DNS-Hostnamen des SINEMA RC-Servers ein.

- **Eingabefeld "SINEMA RC Port"**

  Geben Sie den Port ein, über den das WBM des SINEMA RC-Servers erreichbar ist.

- **Eingabefeld "Device 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.

- **Eingabefeld "Device Password"**

  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.

- **Optionskästchen "Auto Firewall / NAT Rules"**

  – 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.

- **Klappliste "Use Proxy"**

  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.

- **Klappliste "Verfication Type"**

  – Fingerprint: Die Identität des Servers wird über den Fingerabdruck verifiziert.

  – CA Certificate: Die Identität des Servers wird über das CA-Zertifikat verifiziert

- **Eingabefeld "Fingerprint"**

  Nur bei der Einstellung "Fingerprint" notwendig. Geben Sie den Fingerabdruck des Geräts ein. Der Fingerabdruck wird bei der Inbetriebname 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.

- **Klappliste "CA Certificate"**

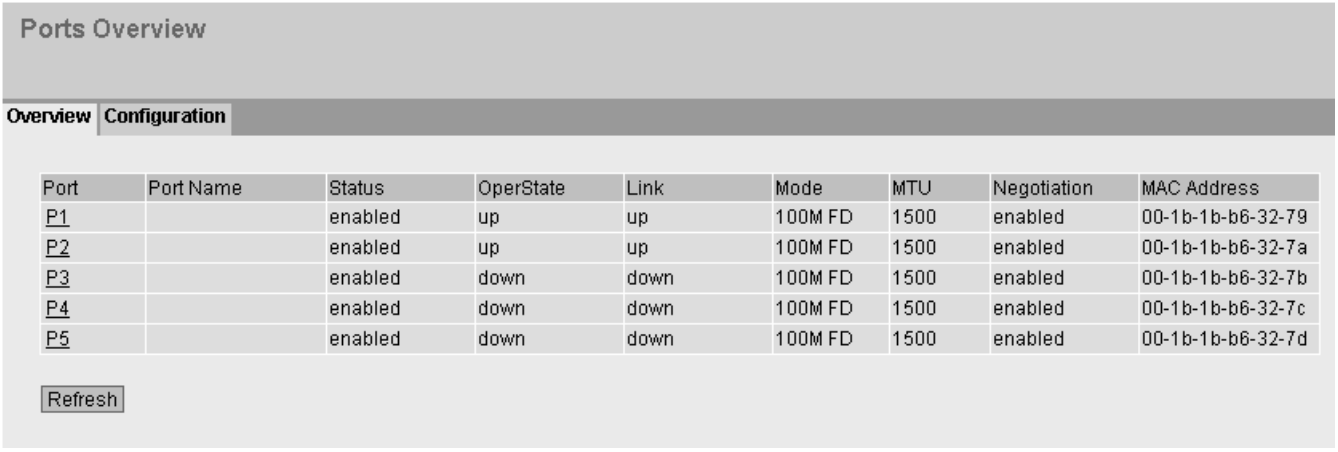
  Wählen Sie das CA-Zertifikat des Servers aus, das zur Signierung des Serverzertifikats verwendet wird. Nur geladene CA-Zertifikate sind auswählbar.

4.5 Menü "Interfaces"

4.5.1 Ethernet

4.5.1.1 Overview

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



Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Port**
  Zeigt die konfigurierbaren Ports an. Der Eintrag ist ein Link. Wenn Sie auf den Link klicken, wird die entsprechende Konfigurationsseite geöffnet.
- **Port Name**
  Zeigt den Namen des Ports.
- **Status**
  Zeigt an, ob der Port ein- oder ausgeschaltet ist. Datenverkehr ist nur über einen eingeschalteten Port möglich.
- **OperState**
  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.

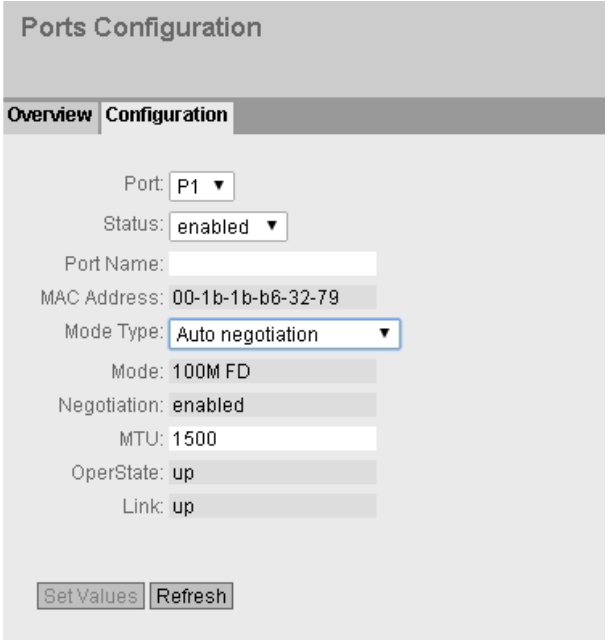
- **Link**
  Zeigt den Verbindungsstatus zum Netzwerk am. Beim Verbindungsstatus ist Folgendes möglich:
  - Up
    Der Port hat eine gültige Verbindung zum Netzwerk, es wird ein "Link Integrity Signal" empfangen.
  - Down
    Die Verbindung ist unterbrochen, weil beispielsweise das angeschlossene Gerät ausgeschaltet ist.
- **Mode**
  Zeigt die Übertragungsparameter des Ports an.
- **MTU (Maximum Transmission Unit)**
  Zeigt die Paketgröße an.
- **Negotiation**
  Zeigt an, ob die automatische Konfiguration aktiviert oder deaktiviert ist.
- **MAC Address**

  Zeigt die MAC-Adresse des Ports an.

4.5.1.2 Configuration

Ports konfigurieren

Mit dieser Seite können Sie alle Ports des Geräts konfigurieren.



Beschreibung der angezeigten Felder

- **Port**
  Wählen Sie aus 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 Address**
  Zeigt die MAC-Adresse des Ports an.
- **Mode Type**
  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.

- **Mode**
  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.

- **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.

  Der Wertebereich ist von 64 bis 1500 Bytes.

- **OperState**
  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.

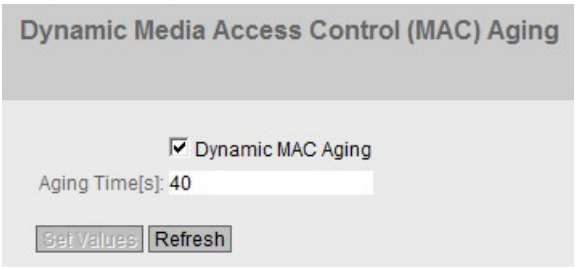
  – Down
    Die Verbindung ist unterbrochen, weil z. B. das angeschlossene Gerät ausgeschaltet ist.

4.6 Menü "Layer 2"

4.6.1 Dynamic MAC Aging

Protokolleinstellungen und Switch-Funktionalität

Das Gerät lernt automatisch die Quelladressen der angeschlossenen Teilnehmer. Diese Information wird dazu benutzt, um Telegramme 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 (beispielsweise ein Programmiergerät) an einen anderen Port angeschlossen wird.
Wenn die Option nicht aktiviert ist, löscht ein Gerät gelernte Adressen nicht automatisch.



Beschreibung

Die Seite enthält folgende Felder:

- **Optionskästchen "Dynamic MAC Aging"**
  Aktivieren oder deaktivieren Sie die Funktion zum automatischen Aging von gelernten MAC-Adressen:
- **Eingabefeld "Aging Time [s]"**
  Tragen Sie die Zeitspanne in Sekunden ein. Nach dieser Zeitspanne wird eine gelernte Adresse gelöscht, wenn das Gerät keine weiteren Telegramme von dieser Absenderadresse mehr empfängt. Der Wertebereich ist von 10 Sekunden bis 1000000 Sekunden

Vorgehensweise

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 "Set Values".

4.6.2 VLAN

4.6.2.1 General

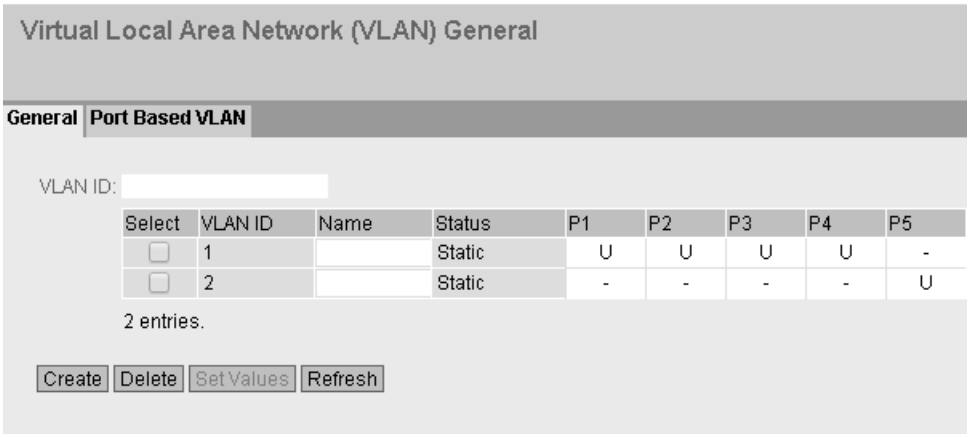
VLAN-Konfigurationsseite

Auf dieser WBM-Seite definieren Sie das VLAN und legen die Verwendung der Ports fest.

Hinweis

Ändern der Agent VLAN ID

Wenn der Admin-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.



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.
- Werkseitig ist an den Ports P1 bis P4 ist VLAN ID 1 und an P5 VLAN ID 2 eingestellt.
- 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 verbunden 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).

Beschreibung der angezeigten Felder

Die Seite enthält folgende Felder:

- **Eingabefeld "VLAN ID"**
  Tragen Sie im Eingabefeld "VLAN ID" die VLAN ID ein.
  Wertebereich: 1 ... 4094

Die Tabelle gliedert sich in folgende Spalten:

- **Select**
  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. Bis zu 257 VLANs können definiert 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 statisch, dass die Adresse 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.

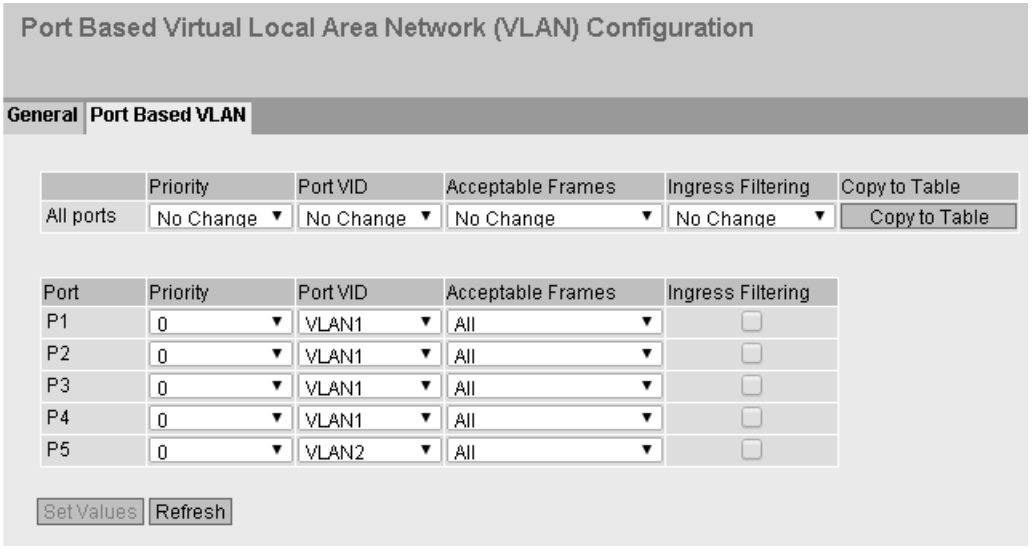
Vorgehensweise zur Konfiguration

1. Tragen Sie im Eingabefeld "VLAN ID" eine ID ein.
2. Klicken Sie auf die Schaltfläche "Create". 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 "Set Values".

4.6.2.2 Port Based 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:

- **All ports**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **Priority / Port VID / Acceptable Frames / Ingress Filtering**
  Wählen Sie in der Klappliste die Einstellung für alle Ports aus. Wenn "No Change" ausgewählt ist, bleiben die Einträge der entsprechenden Spalte in der Tabelle 2 unverändert.
- **Copy to Table**
  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.
- **Priority**
  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 > General" 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.
- **Acceptable Frames**
  Legen Sie fest, welche Arten von Telegrammen akzeptiert werden. Es gibt folgende Alternativen:
  - Tagged Frames Only
    Das Gerät verwirft alle ungetaggten Telegramme. Andernfalls gelten die Weiterleitungsregeln entsprechend der Konfiguration.
  - All
    Das Gerät leitet alle Telegramme weiter.
- **Ingress Filtering**
  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 werdenTelegramme 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 "Set Values".

4.6.3 LLDP

Bestimmung der Netzwerktopologie

LLDP (Link Layer Discovery Protocol) ist im Standard IEEE 802.AB definiert.

LLDP ist ein Verfahren zur Bestimmung der Netzwerktopologie. Netzwerkkomponenten tauschen über LLDP Informationen mit ihren Nachbargeräten aus.

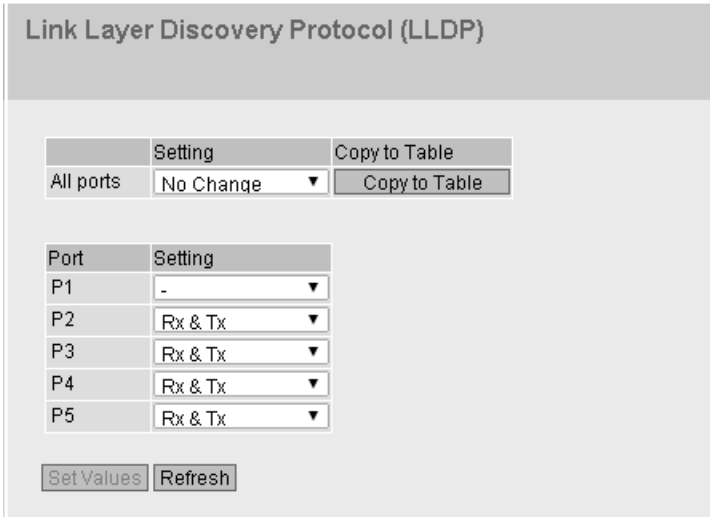
Netzwerkkomponenten, die LLDP unterstützen, verfügen über einen LLDP-Agenten. Der LLDP-Agent versendet in periodischen Abständen Informationen über sich selbst und empfängt Informationen von angeschlossenen Geräten. Die empfangenen Informationen werden in der MIB gespeichert.

Anwendungen

PROFINET benutzt LLDP für die Topologie-Diagnose. In der Werkseinstellung ist LLDP an den Ports P1 - P4 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 Netzwerkkomponenenten 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:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports gültig sind.
- **Setting**
  Wählen Sie aus der Klappliste die Einstellung. Wenn "No Change" ausgewählt ist, bleibt der Eintrag in der Tabelle 2 unverändert.
- **Copy to Table**
  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 den Port an.
- **Setting**
  Legen Sie die LLDP-Funktionalität fest. Folgende Möglichkeiten gibt es:
  - Tx
    Dieser Port kann LLDP-Telegramme nur senden.
  - Rx
    Dieser Port kann LLDP-Telegramme nur empfangen.
  - Rx & Tx
    Dieser Port kann LLDP-Telegramme empfangen und senden.
  - "-" (Deaktiviert)
    Dieser Port kann LLDP-Telegramme weder empfangen noch senden.

Vorgehensweise

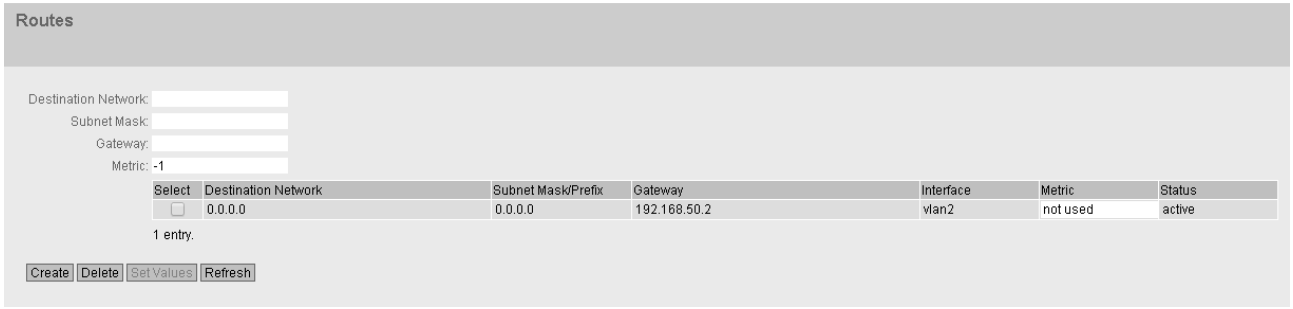
1. Wählen Sie in der Klappliste die gewünschte LLDP-Funktionalität aus.
2. Klicken Sie auf die Schaltfläche "Set Values".

4.7 Menü "Layer 3"

4.7.1 Routes

Statische Route

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:

- **Destination Network**
  Tragen Sie die die Netzwerkadresse des Ziels ein, das über diese Route erreichbar ist.
- **Subnet Mask**
  Tragen Sie die dazugehörende Subnetzmaske ein.
- **Gateway**
  Tragen Sie die IP-Adresse des Gateways ein, über den diese Netzwerkadresse erreichbar ist.
- **Metric**
  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 "not used" verwendet. Die Metrik ist nachträglich änderbar.

  Wertebereich: 1 - 254 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:

- **Select**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Destination Network**
  Zeigt die Netzwerkadresse des Ziels an.

- **Subnet Mask/Prefix**
  Zeigt die dazugehörende Subnetzmaske (IPv4) bzw. die Präfixlänge (IPv6) an.
- **Gateway**
  Zeigt die IP-Adresse des nächsten Gateways an.
- **Interface**
  Zeigt die Schnittstelle der Route an.
- **Metric**
  Beim Erstellen der Route wird automatisch "not used" eingetragen. Die Metrik entspricht der Güte einer Verbindung, z. B. Geschwindigkeit, Kosten. Bei mehreren gleichen Routen wird die Route mit dem kleinsten Metrik-Wert benutzt.
  Wertebereich: 1 - 254 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.
- **Status**
  Zeigt an, ob die Route aktiv ist oder nicht.

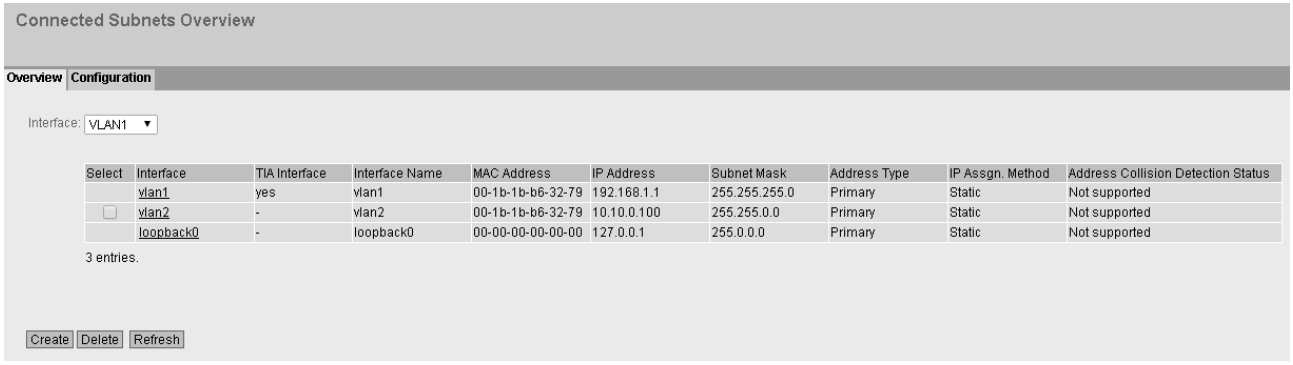
Vorgehensweise

1. Tragen Sie in das Eingabefeld "Destination Network" Netzwerkadresse des Ziels ein.
2. Tragen Sie in das Eingabefeld "Subnet Mask" die dazugehörende Subnetzmaske ein.
3. Tragen Sie in das Eingabefeld "Gateway" das Gateway ein.
4. Tragen Sie bei "Metric" die Gewichtung der Route ein.
5. Klicken Sie auf die Schaltfläche "Create". In der Tabelle wird ein neuer Eintrag erzeugt.

4.7.2 Subnets

4.7.2.1 Overview

Die Seite zeigt die Subnetze für die ausgewählte Schnittstelle. Ein Subnetz bezieht sich immer auf eine Schnittstelle und wird auf dem Register "Configuration" angelegt.



Beschreibung

Die Seite enthält folgendes Feld:

- **Interface**
  Wählen Sie aus der Klappliste "Interface" die Schnittstelle, an die Sie ein weiteres Subnetz projektieren.

Die Tabelle gliedert sich in folgende Spalten:

- **Interface**
  Zeigt die Schnittstelle an, auf die sich die Einstellungen beziehen.
- **Interface Name**
  Zeigt den Namen der Schnittstelle.
- **MAC Address**
  Zeigt die MAC-Adresse der Schnittstelle an.
- **IP Address**
  Zeigt die IP-Adresse des Subnetzes an.
- **Subnet Mask**
  Zeigt die Subnetzmaske.
- **Address Type**
  Zeigt den Adressentyp an. Folgende Werte sind möglich:
  - Primary
    Die erste IP-Adresse, die auf einem IP-Interface konfiguriert wurde.
  - Secondary
    Alle weiteren IP-Adressen, die auf einem IP-Interface konfiguriert wurden.

- **IP Assign. Method**
  Zeigt an, wie die IP-Adresse zugeordnet wird. Folgende Werte sind möglich:
  - Static
    Die IP-Adresse ist statisch. Tragen Sie die IP-Einstellungen bei "IP Address" und "Subnet Mask" ein.
  - Dynamic (DHCP)
    Das Gerät bezieht eine dynamische IP-Adresse von einem DHCP-Server.
- **Address Collision Detection Status**

  Zeigt an, in welchem Status sich die Funktion befindet. Wenn neue IP-Adressen im Netz aktiv werden, prüft die Funktion "Address Collision Detection", ob es zu Adresskollisionen kommen kann. Dadurch werden die IP-Adressen erkannt, die doppelt vergeben werden sollen.

  Hinweis

  Die Funktion führt keine zyklische Prüfung durch.

  Folgende Werte sind möglich:
  - Idle

    Die Schnittstelle ist nicht aktiv und besitzt keine IP-Adresse.
  - Starting

    Dieser Status bezeichnet die Anlaufphase. In dieser Phase sendet das Gerät zunächst eine Anfrage, ob es die geplante IP-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 IP-Adresse zu verwenden, die bereits vergeben ist.
  - Defending

    Die Schnittstelle verwendet eine eindeutige IP-Adresse. Eine andere Schnittstelle versucht die gleiche IP-Adresse zu verwenden.
  - Active

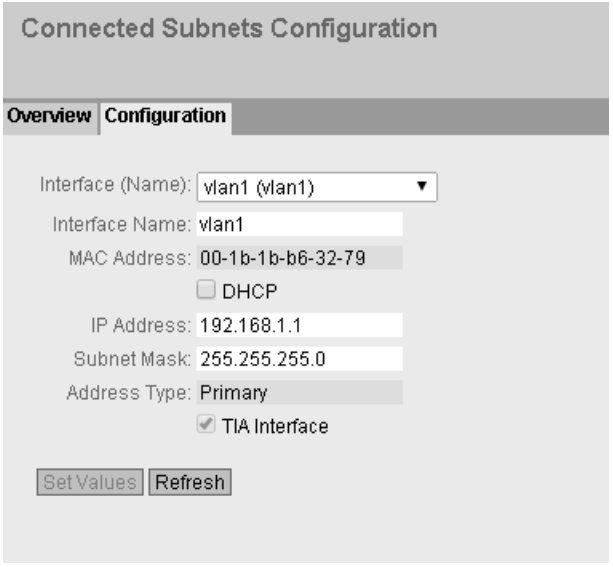
    Die Schnittstelle verwendet eine eindeutige IP-Adresse. Es gibt keine Kollisionen.
  - Not supported

    Die Funktion zur Erkennung von Adresskollisionen wird nicht unterstützt.
  - Disabled

    Die Funktion zur Erkennung von Adresskollisionen ist deaktiviert.

4.7.2.2 Configuration

Auf dieser Seite konfigurieren Sie das Subnetz für die Schnittstelle.



Beschreibung

Die Seite enthält Folgendes:

- **Interface (Name)**
  Wählen Sie die gewünschte Schnittstelle.
- **Interface Name**
  Tragen Sie den Namen für die Schnittstelle ein.
- **MAC Address**

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

  Aktivieren oder deaktivieren Sie den DHCP-Client für die Schnittstelle.

  Hinweis

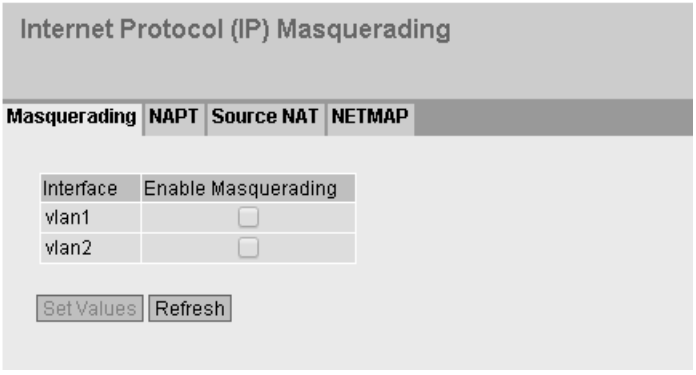
  Wenn Sie das Gerät als Router mit mehreren Schnittstellen betreiben wollen, deaktivieren Sie DHCP auf allen Schnittstellen.
- **IP Address**
  Tragen Sie die IP-Adresse der Schnittstelle ein. Die IP-Adressen dürfen nicht mehrfach verwendet werden.
- **Subnet Mask**
  Tragen Sie die Subnetzmaske des zu erstellenden Subnetzes ein. Subnetze an unterschiedlichen Schnittstellen dürfen sich nicht überlappen.

- **Address Type**
  Zeigt den Adressen Typ an. Folgende Werte sind möglich:
  - Primary
    Das erste Subnetz der Schnittstelle.
  - Secondary
    Alle weiteren Subnetze der Schnittstelle.
- **TIA Interface**
  Wählen Sie aus, ob dieses Interface zum TIA Interface werden soll.

4.7.3 NAT

4.7.3.1 Masquerading

Auf dieser WBM-Seite aktivieren Sie die Regeln für IP-Masquerading.



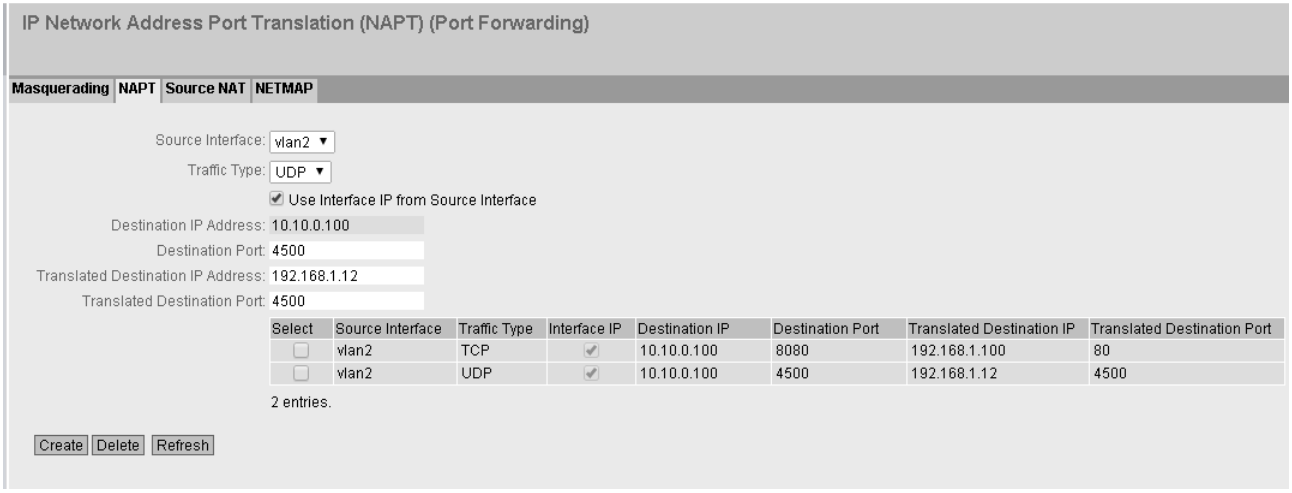
Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Interface**
  VLAN-Schittstelle, auf die sich die Einstellung bezieht. Nur VLANs mit konfigurierten Subnetz sind verfügbar.
- **Enable Masquerading**
  Wenn aktiviert, wird bei jedem ausgehenden Datenpaket, das über diese Schnittstelle gesendet wird, die Quell-IP-Adresse durch die IP-Adresse der Schnittstelle ersetzt

4.7.3.2 NAPT

Auf dieser WBM-Seite konfigurieren Sie die Portweiterleitung.



Beschreibung

Die Seite enthält folgende Felder:

- **Klappliste "Source Interface"**
  Schnittstelle, auf die sich die Einstellungen beziehen. Nur auswählbar, wenn das Gerät mehrere Schnittstellen besitzt.
- **Klappliste "Traffic Type"**
  Legen Sie fest, für welches Protokoll die Adresszuordnung gültig ist.
- **Optionskästchen "Use Interface IP from Source Interface"**
  Wenn aktiviert, wird bei "Destination IP Address" die IP-Adresse der ausgewählten Schnittstelle verwendet.
- **Eingabefeld "Destination IP Address"**
  Geben Sie die Ziel-IP-Adresse ein. An dieser IP-Adresse werden die Telegramme empfangen. Nur editierbar, wenn "Use Interface IP from Source Interface" deaktiviert ist.
- **Eingabefeld "Destination 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.

- **Eingabefeld "Translated Destination IP Address"**
  Geben Sie die IP-Adresse des Teilnehmers an, an den dieses Telegramm weitergeleitet wird.

  Eingabefeld "Translated Destination Port"
  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.

  Wenn der "Destination Port" und der "Translated Destination Port" gleich sind, werden die Telegramme ohne Port-Umsetzung weitergeleitet.

  Hinweis

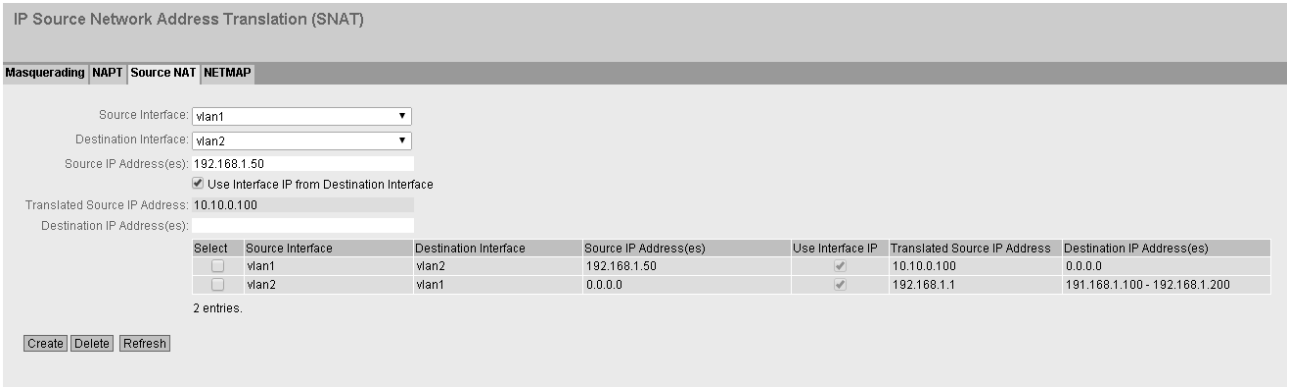
  Wenn der Port bereits durch einen lokalen Dienst z. B. Telnet belegt ist, wird eine Warnmeldung ausgegeben.
  Vermeiden Sie auf jeden Fall die Nutzung von folgenden Ports: TCP-Port 23 (Telnet), Port 22 (SSH), die Ports 80/443 (http/https: Erreichbarkeit des Clients mit dem WBM), UDP-Port 161 (SNMP), Port 500 (ISAKMP), Port 4500 (IPsec Nat-T).

Die Tabelle gliedert sich in folgende Spalten:

- **Select**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Source Interface**
  Zeigt die Schnittstelle an, von dem die Pakete kommen müssen. Nur diese Pakete kommen für eine Portweiterleitung in Frage.
- **Traffic Type**
  Zeigt an, für welches Protokoll die Adresszuordnung gilt.
- **Interface IP**
  Zeigt an, ob die IP-Adresse der Schnittselle verwendet wird.
- **Destination IP**
  Zeigt die Ziel-IP-Adresse an. An dieser IP-Adresse werden die Telegramme empfangen.
- **Destination Port**
  Zeigt den Ziel-Port an. Eingehende Telegramme mit diesem Port als Ziel-Port werden weitergeleitet.
- **Translated Destination IP**
  Zeigt die IP-Adresse Teilnehmers an, an dem die Pakete weitergeleitet werden.
- **Translated Destination Port**
  Zeigt an auf welchen Zielport übersetzt wird.

4.7.3.3 Source NAT

Auf dieser WBM-Seite konfigurieren Sie die Regeln für Source-NAT.



Beschreibung

- **Klappliste "Source Interface" / "Destination Interface"**

  Legen Sie Richtung des Verbindungsaufbaus festgelegt. 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

  – SINEMA RC: Verbindung zum SINEMA RC-Server

  – IPSecVPN: Entweder alle IPsecVPN-Verbindungen (all) oder eine spezifische IPsecVPN-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.

- **Eingabefeld "Source IP Address(es)"**

  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.

  – 0.0.0.0/0: Gilt für alle IP-Adressen

  – IP-Adressbereich: Gilt für den angegebenen IP-Adressbereich: Start-IP-Adresse "-" End-IP-Adresse, z. B. 192.168.100.10 - 192.168.100.20

  – IP-Adressband: Gilt für die im IP-Adressband erfassten IP-Adressen: IP-Adresse/Anzahl Bits des Netzanteils (CIDR-Notation)

Use Interface IP from Destination Interface

Wenn aktiviert, wird bei "Translated Source IP Address" die IP-Adresse der ausgewählten Ziel-Schnittstelle verwenden.

- **Eingabefeld "Translated Source IP Address"**
  Geben Sie die IP-Adresse ein, mit der die IP-Adresse des Absenders ersetzt wird. Nur editierbar, wenn "Use Interface IP from Destination Interface" deaktiviert ist.
- **Eingabefeld "Destination IP Address(es)"**

  Legen Sie fest, für welche Ziel-IP-Adressen diese Destination-NAT-Regel gültig ist. Nur die Pakete werden berücksichtigt, deren Ziel-IP-Adresse im Bereich der eingegebenen Adressen liegt.

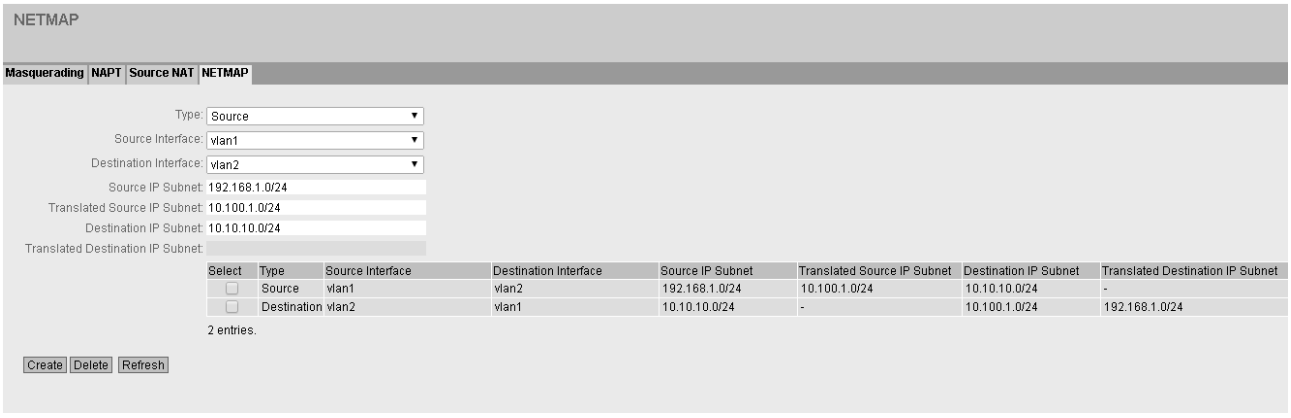
  – IP-Adresse: Gilt genau für die angegebene IP-Adresse.
  – 0.0.0.0/0: Gilt für alle IP-Adressen
  – IP-Adressbereich: Gilt für den angebenen IP-Adressbereich: Start-IP-Adresse "-" End-IP-Adresse an, z. B. 192.168.100.10 - 192.168.100.20
  – IP-Adressband: Gilt für die im IP-Adressband erfassten IP-Adressen: IP-Adresse/Anzahl Bits des Netzanteils (CIDR-Notation)

Die Tabelle gliedert sich in folgende Spalten:

- Select
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- Source Interface
  Zeigt die Quell-Schnittstelle an.
- Destination Interface
  Zeigt die Ziel-Schnittstelle an.
- Source IP Address(es)
  Zeigt die IP-Adressen der Absender an, für die eine Adressumsetzung gewünscht ist.
- Translated Source IP Address
  Zeigt die IP-Adresse an, mit der die IP-Adresse der Absender ersetzt wird.
- Destination IP Address(es)
  Zeigt die IP-Adressen der Empfänger an, für die eine Adressumsetzung gewünscht ist.

4.7.3.4 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.



Hinweis

Firewallregeln bei Source-NAT

Die Source-NAT-Regel wird nach dem Routing und der Firewall-Entscheidung statt. Bei der Firewall-Regel wird die Eingabe aus "Source IP Subnet" verwendet.

Firewallregeln bei Destination-NAT

Destination-NAT findet nach vor dem Routing und der Umsetzung der Firewall-Regel statt. Bei der Firewall-Regel wird die Eingabe aus "Translated Destination IP Subnet" verwendet.

Beschreibung

- **Klappliste "Type"**
  Legen Sie die Art der Adressumsetzung fest.
  - Source: Ersetzen der Quell-IP-Adresse
  - Destination: Ersetzen der Ziel-IP-Adresse.
- **Klappliste "Source Interface"**
  Legen Sie die Quell-Schnittstelle fest.
  - VLANx: VLANs mit konfigurierten Subnetz
  - SINEMA RC: Verbindung zum SINEMA RC-Server
  - IPSecVPN: Entweder alle IPsecVPN-Verbindungen (all) oder eine spezifische IPsecVPN-Verbindung
- **Klappliste "Destination Interface"**
  Legen Sie die Ziel-Schnittstelle fest.
  - VLANx: VLANs mit konfigurierten Subnetz
  - SINEMA RC: Verbindung zum SINEMA RC-Server
  - IPSecVPN: Entweder alle IPsecVPN-Verbindungen (all) oder eine spezifische IPsecVPN-Verbindung

- **Eingabefeld "Source IP Subnet"**

  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.

- **Eingabefeld "Translated Source IP Subnet"**
  Tragen Sie Subnetz ein, mit der das Subnetz des Absenders ersetzt wird. Nur editierbar, bei den Einstellungen "SourceNAT".
  Das Subnetz kann auch nur ein einzelner PC, oder eine andere Untermenge des Subnetzes sein. Verwenden Sie die CIDR-Schreibweise.

- **Eingabefeld "Destination IP Subnet"**
  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.

- **Eingabefeld "Translated Destination IP Subnet"**
  Tragen Sie Subnetz ein, mit der das Subnetz des Empfängers ersetzt wird. Nur editierbar, bei den Einstellungen "DestinationNAT" "
  Das Subnetz kann auch nur ein einzelner PC, oder eine andere Untermenge des Subnetzes sein. Verwenden Sie die CIDR-Schreibweise.

Die Tabelle gliedert sich in folgende Spalten:

- Select
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- Type
  Zeigt die Richtung der Adressumsetzung an.
- Source Interface
  Zeigt die Quell-Schnittstelle an.
- Destination Interface
  Zeigt die Ziel-Schnittstelle an.
- Source IP Subnet
  Zeigt das Subnetz des Absenders an.
- Translated Source IP Subnet
  Zeigt das Subnetz des Absenders an, mit der das Subnetz des Absenders ersetzt wird.
- Destination IP Subnet
  Zeigt das Subnetz des Empfängers an.
- Translated Destination IP Subnet
  Zeigt das Subnetz des Empfängers an, mit der das Subnetz des Empfängers ersetzt wird.

Beispiele

Beispiel 1

- Type: Source
- Source Interface: vlan1
- Destination Interface: vlan2
- Source IP Subnet: 192.168.1.0/24
- Translated Source IP Subnet: 10.100.1.0/24
- Destination IP Subnet: 10.10.10.0/24
- Translated Destination IP Subnet: -

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 (Source IP Subnet) und die Ziel-IP-Adresse im Subnetz des Empfängers (Destination IP Subnet) liegen, wird die Quell-IP-Adresse durch die passende IP-Adresse aus dem "Translated Source IP Subnet" 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.

Beispiel 2:

- Type: Destination
- Source Interface: vlan2
- Destination Interface: vlan1
- Source IP Subnet: 10.10.10.0/24
- Translated Source IP Subnet: -
- Destination IP Subnet: 10.100.1.0/24
- Translated Destination IP Subnet: 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.

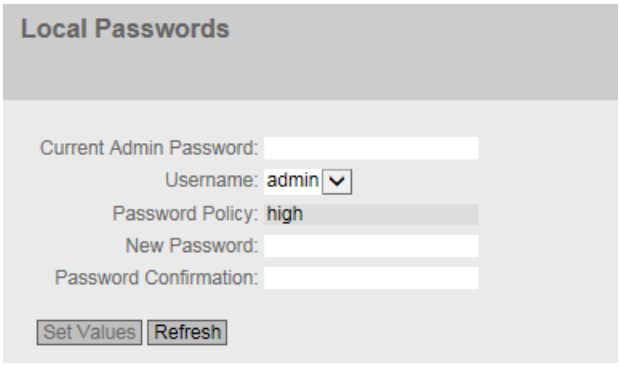
Wenn die Quell-IP-Adresse im Subnetz des Absenders (Source IP Subnet) und die Ziel-IP-Adresse im Subnetz des Empfängers (Destination IP Subnet) liegen, wird die Quell-IP-Adresse durch die passende IP-Adresse aus dem "Translated Destination IP Subnet" ersetzt. Ein Paket z. B. mit der Quell-IP-Adresse 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 vlan 2 angeschlossenen Geräte, müssen die am vlan1 angeschlossenen Geräte mit der virtuellen IP-Adresse aus dem Subnetz 10.100.1.0 adressieren.

4.8 Menü "Security"

4.8.1 Password

Konfiguration der Geräte-Passwörter

Auf dieser WBM-Seite können Sie das Administrator-Passwort ändern.



Vorgehensweise

1. Geben Sie bei "Current Admin Password" das gültige Administrator-Passwort ein.
2. Geben Sie bei "New Password" das neue Passwort ein.

Hinweis

Password Policy: high

Beachten Sie folgende Passwortrichtlinien:

- Passwortlänge: mindestens 8 Zeichen
- Mindestens 1 Großbuchstabe
- Mindestens 1 Sonderzeichen
- Mindestens 1 Zahl

3. Wiederholen Sie das neue Passwort im Eingabefeld "Password Confirmation".
4. Klicken Sie auf die Schaltfläche "Set Values".

Hinweis

Werksseitig ist das Passwort bei Auslieferung des Geräts wie folgt eingestellt:

- admin: admin

Wenn Sie sich das erste Mal anmelden oder nach einem "Restore Factory Defaults and Restart" anmelden, werden Sie aufgefordert das Passwort zu ändern.

Hinweis

Passwort ändern im Trial-Modus

Auch wenn Sie im Trial-Modus das Passwort ändern, wird diese Änderung sofort gespeichert.

4.8.2 Certificates

4.8.2.1 Overview

Auf dieser WBM-Seite werden die geladenen Dateien (Zertifikate und Schlüsseln) angezeigt. Folgende Möglichkeiten gibt es, um die Dateien ins Gerät zu laden:

- System > Load&Save > HTTP
- System > Load&Save > TFTP

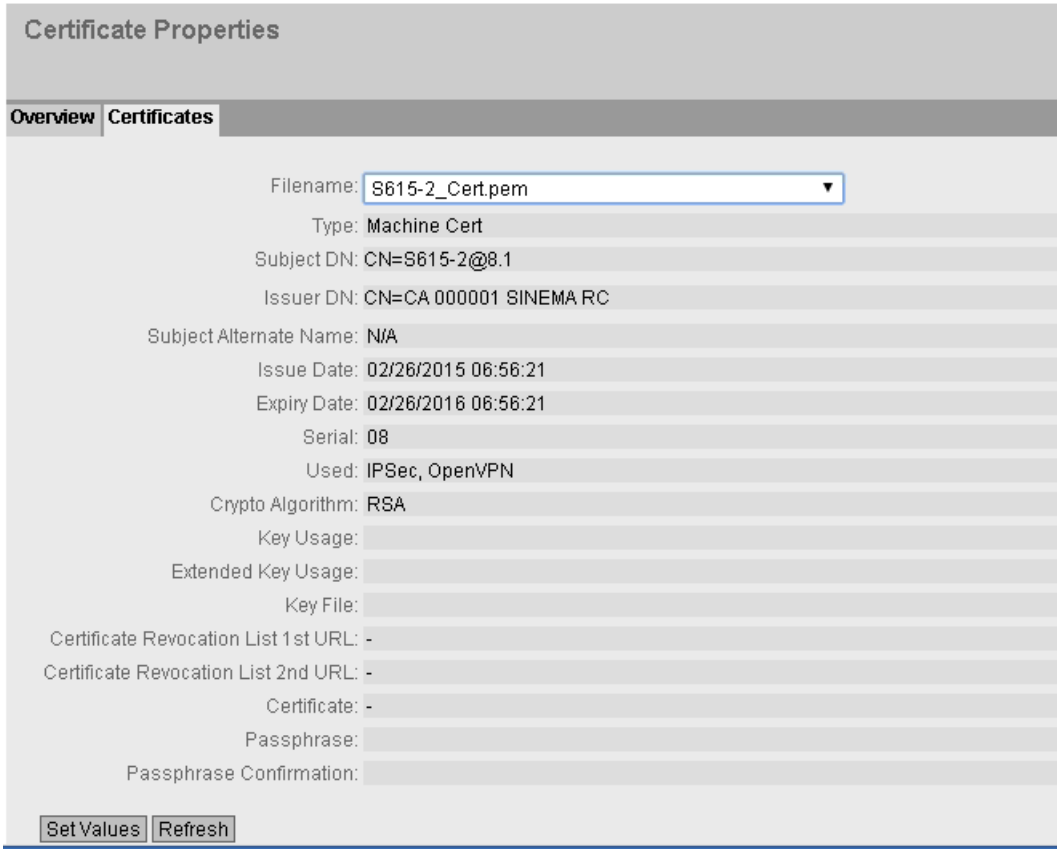
Beschreibung

- **Select**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen. Nur nicht verwendete Zertifikate können gelöscht werden.
- **Type**
  Zeigt die Art der geladenen Datei an.
  - CA Cert
    Das CA-Zertifikat ist von einer zertifizierenden Stelle (CA = Certification Authority) signiert.
  - Machine Cert
    Maschinenzertifikat
  - Key File
    Schlüsseldatei
  - Remote Cert
    Gegenstellenzertifikat
- **Filename**
  Zeigt den Dateinamen an.
- **State**
  Zeigt an, ob das Zertifikat gültig oder bereits abgelaufen ist.
- **Subject DN**
  Zeigt den Namen des Zertifikatsinhabers an.
- **Issuer DN**
  Zeigt den Namen des Zertifikatsausstellers an.
- **Issue Date**
  Zeigt den Beginn des Gültigkeitszeitraums des Zertifikats an
- **Expiry Date**
  Zeigt das Ende des Gültigkeitszeitraums des Zertifikats an.
- **Used**
  Zeigt an, welche Funktion das Zertifkat nutzt.

4.8.2.2 Certificates

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

- **Filename**
  Wählen Sie das gewünschte Zertifikat aus.
- **Type**
  Zeigt die Art der geladenen Datei an.
  - CA Cert
    Das CA-Zertifikat ist von einer zertifizierenden Stelle (CA = Certification Authority) signiert.
  - Machine Cert
    Maschinenzertifikat
  - Key File
    Schlüsseldatei
  - Remote Cert
    Gegenstellenzertifikat
- **Subject DN**
  Zeigt den Namen des Zertifikatsinhabers an.

- **Issuer DN**
  Zeigt den Namen des Zertifikatsausstellers an.
- **Subject Alternate Name**
  Wenn vorhanden, wird ein alternativer Name des Zertifikatsausstellers angezeigt.
- **Issue Date**
  Zeigt den Beginn des Gültigkeitszeitraums des Zertifikats an
- **Expiry Date**
  Zeigt das Ende des Gültigkeitszeitraums des Zertifikats an.
- **Serial**
  Zeigt die Seriennummer des Zertifikats an.
- **Used**
  Zeigt an, welche Funktion das Zertifikat nutzt.
- **Crypto Algorithm**
  Zeigt an, welches kryptografisches Verfahren verwendet wird.
- **Key Usage**
  Zeigt an, für welchen Zweck der zum Zertifikat gehörende Schlüssel verwendet wird, z. B. zum Verifizieren digitaler Signaturen.
- **Extended Key Usage**
  Zeigt an, ob der Verwendungszweck noch zusätzlich beschränkt ist, z. B. nur zum Verifizieren von Signaturen des CA-Zertifikats.
- **Key File**
  Zeigt die Schlüsseldatei an.
- **Certificate Revocation List 1st URL**
  Tragen Sie die URL ein, über die die Sperrliste abgerufen werden kann. Nur editierbar, wenn vom Zertifikat unterstützt.
- **Certificate Revocation List 2nd 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.
- **Certificate**
  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 Confirmation**
  Tragen Sie das Passwort nochmals ein. Nur editierbar, wenn die verschlüsselte Datei Passwort-geschützt ist.

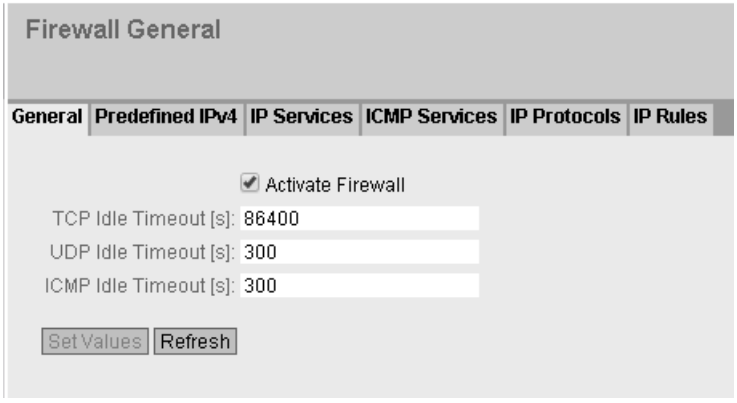
4.8.3 Firewall

4.8.3.1 General

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:

- **Optionskästchen "Activate Firewall"**

  Wenn aktiviert, ist die Firewall aktiv.

- **Eingabefeld "TCP Idle Timeout [s]"**

  Geben Sie die gewünschte Zeitspannne in Sekunden ein. Wenn kein Datenaustausch stattfindet, wird nach Ablauf dieser Zeitspanne die TCP-Verbindung automatisch getrennt.

  Der Wertebereich ist 1 bis 4294967295.

  Default-Einstellung: 86400 Sekunden

- **Eingabefeld "UDP Idle Timeout [s]"**
  Geben Sie die gewünschte Zeitspannne in Sekunden ein. Wenn kein Datenaustausch stattfindet, wird nach Ablauf dieser Zeitspanne die UDP-Verbindung automatisch getrennt.

  Der Wertebereich ist 1 bis 4294967295.

  Default-Einstellung: 300 Sekunden

- **Eingabefeld "ICMP Idle Timeout [s]"**
  Geben Sie die gewünschte Zeitspannne in Sekunden ein. Wenn kein Datenaustausch

stattfindet, wird nach Ablauf dieser Zeitspanne die ICMP-Verbindung automatisch getrennt.

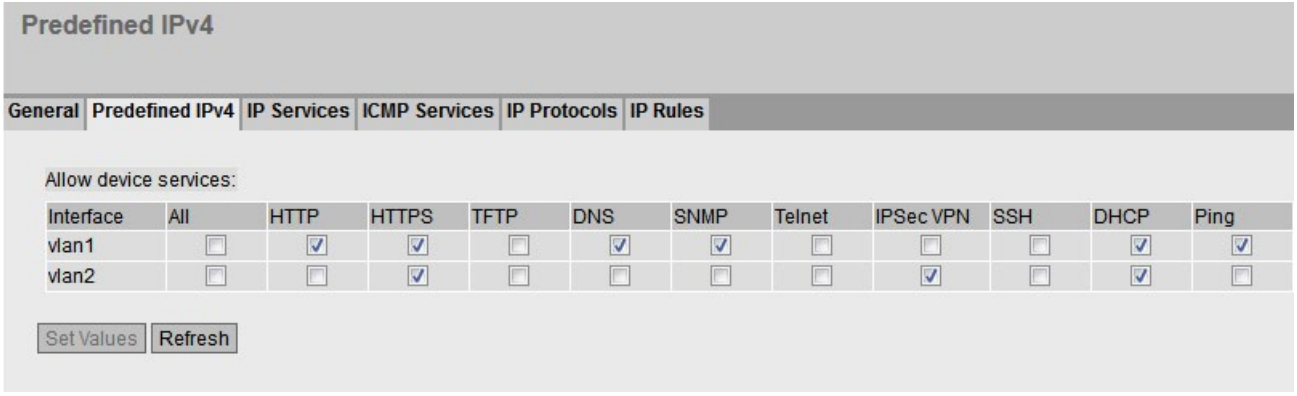
Der Wertebereich ist 1 bis 4294967295.

Default-Einstellung: 300 Sekunden

4.8.3.2 Predefined IPv4

Die WBM-Seite enthält vordefinierte IPv4-Regeln. Wenn Sie benutzerdefinierte IPv4-Regeln anlegen, haben diese eine höhere Priorität als die vordefinierten IPv4-Regeln.

Mir fehlt irgendwie eine Beschreibung was diese Seite macht. Hier kann man einstellen, welche Dienste des Gerätes von welcher VLAN-Schnittstelle/Subnetz aus erreichbar sein sollen. Die Liste der VLAN-Schnittstellen/Subnetze ist dynamisch und richtet sich nach den Einstellungen aus "Layer 3 >Subnetz".



Beschreibung

- **Interface**
  VLAN-Schittstelle, auf die sich die Einstellung bezieht. Nur VLANs mit konfigurierten Subnetz sind verfügbar.
- Der Zugriff auf folgende IPv4-Dienste wird erlaubt:
  - All
    Alle IPv4-Dienste
  - HTTP
    Zum Zugriff auf das Web Based Management.
  - HTTPS
    Zum gesicherten Zugriff auf das Web Based Management.

    Hinweis

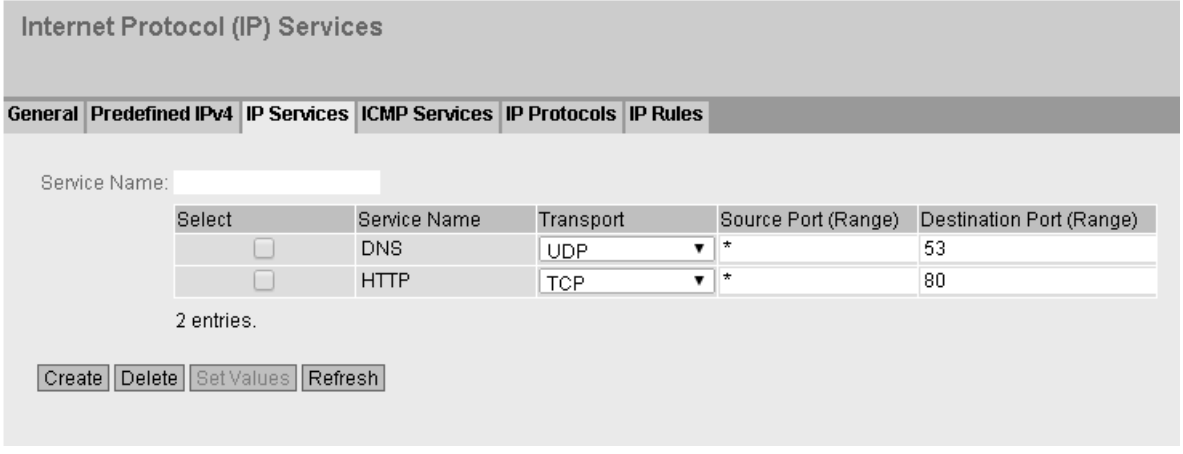
    Zugriff über HTTP / HTTPS

    Wenn Sie beide Firewall-Regeln deaktivieren, dann ist das WBM des Geräts nicht mehr erreichbar.
  - TFTP
    Zur Kommunikation über TFTP. Nur notwendig, um z. B. mit einem TFTP-Client auf das Gerät zuzugreifen.
  - DNS
    DNS-Anfragen an das Gerät. Nur notwendig, wenn am Gerät die Funktion "DNS-Relay" aktiv ist.

- SNMP
  Eingehende SNMP-Verbindungen. Notwendig, um z. B. mit einem MIB-Browser auf die SNMP-Informationen des Geräts zuzugreifen.
- Telnet
  Zum unverschlüsselten Zugriff auf das CLI.
- SMS Relay (nur beim M874)
  Zum Versenden von SMS aus dem lokalen Netz.
- 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

4.8.3.3 IP Services

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:

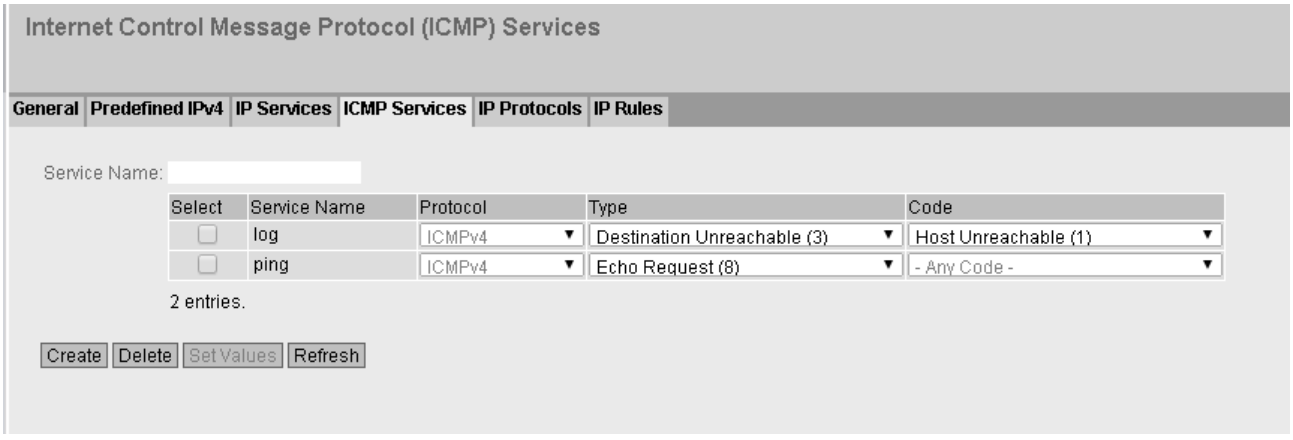
- **Eingabefeld "Service Name"**
  Tragen Sie den Namen für den IP-Dienst ein. Der Name muss eindeutig sein.

Die Tabelle enthält folgende Spalten:

- **Select**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Service Name**
  Zeigt den Namen des IP-Dienstes an.
- **Transport**
  Legen Sie den Protokolltyp fest.
  - UDP
    Die Regel gilt nur für UDP-Telegramme.
  - TCP
    Die Regel gilt nur für TCP-Telegramme.
- **Source Port (Range)**
  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.
- **Destination Port (Range)**
  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.

4.8.3.4 ICMP Services

Auf dieser WBM-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:

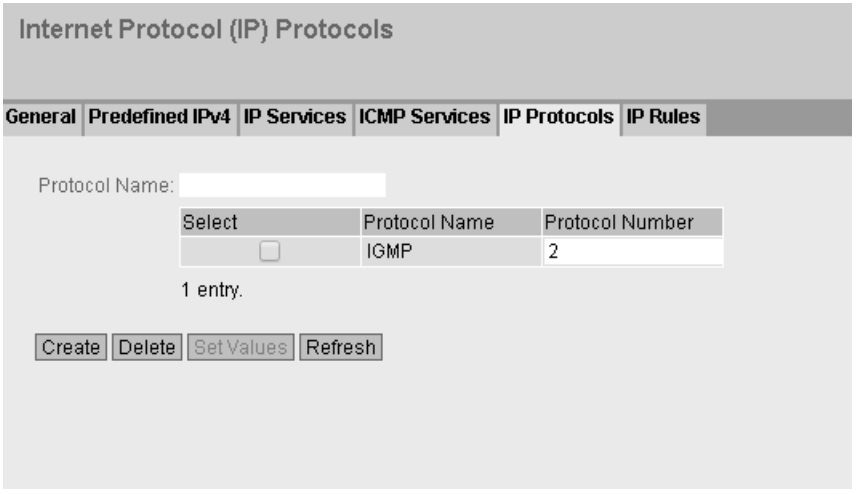
- **Eingabefeld "Service Name"**
  Tragen Sie einen Namen für den ICMP-Dienst ein. Der Name muss eindeutig sein.

Die Tabelle enthält folgende Spalten:

- **Select**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Service Name**
  Zeigt den Namen des ICMP-Diensts an.
- **Protocol**
  Zeigt die Version des ICMP-Protokolls an.
- **Type**
  Legen Sie den ICMP-Pakettyp fest. Einige Beispiele sind:
  - Destination Unreachable
    IP-Telegramm kann nicht zugestellt werden.
  - Time Exeeded
    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.

4.8.3.5 IP Protocols

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:

- **Eingabefeld "Protocol Name"**
  Tragen Sie einen Namen für das Protokoll ein.

Die Seite enthält folgende Optionskästchen:

- **Select**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Protocol Name**
  Zeigt den Protokollnamen an.
- **Protocol Number**
  Tragen Sie die Protokollnummer ein, z. B. 2. Eine Liste der Protokollnummern finden Sie auf den Internetseiten von iana.org

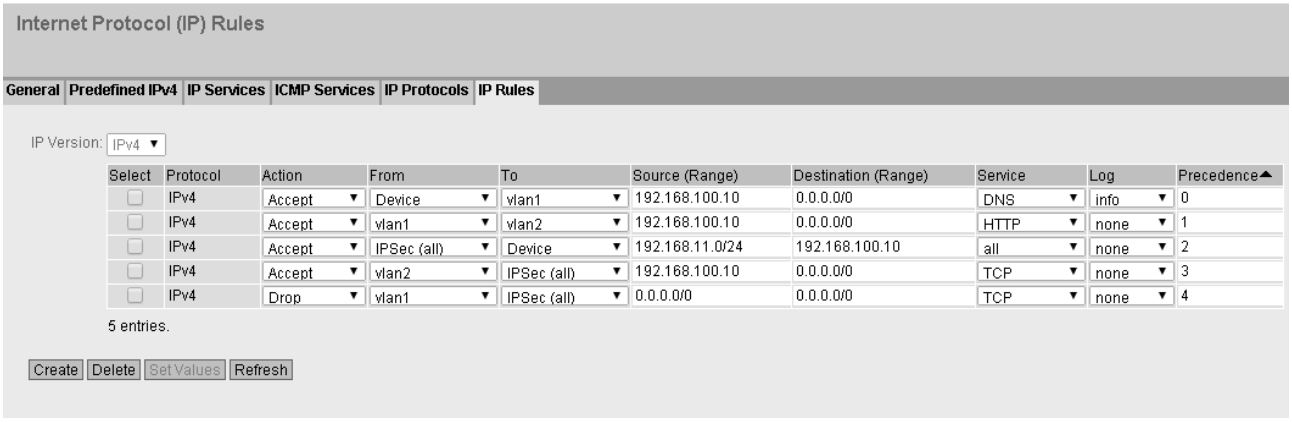
Vorgehensweise

Protokoll IGMP anlegen

1. Tragen Sie bei "Protocol Name" IGMP ein.
2. Klicken Sie auf die Schaltfläche "Set Values". In der Tabelle wird ein neuer Eintrag erzeugt.
3. Tragen Sie bei "Protocol Number" 2 ein.

4.8.3.6 IP Rules

Auf dieser WBM-Seite legen Sie eigene IP-Regeln für die Firewall fest. Diese IP-Regeln haben eine höhere Priorität als die vordefinierten IP-Regeln.



Beschreibung der angezeigten Felder

Die Tabelle enthält folgende Spalten:

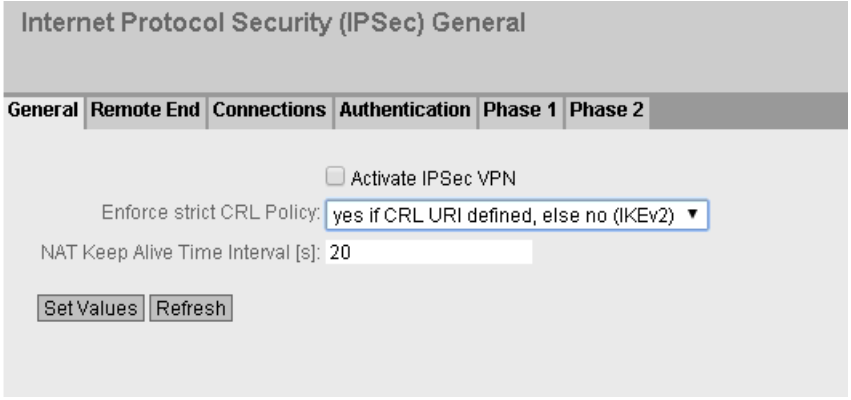
- **Select**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Protocol**
  Zeigt die Version des IP-Protokolls an.
- **Action**
  Wählen Sie aus, wie mit eintreffenden IP-Paketen zu verfahren ist:
  - "Accept" – Die Datenpakete dürfen passieren,
  - "Reject" – Die Datenpakete werden abgewiesen, der Absender erhält eine entsprechende Meldung,
  - "Drop" – Die Datenpakete werden ohne Rückmeldung an den Absender verworfen.
- **From / To**
  Legen Sie die Richtung der IP-Regel fest.
- **Source (Range)**
  Tragen Sie die IP-Adresse oder einen IP-Bereich ein, die IP-Pakete senden darf.
  - Wenn die Regel für einen IP-Bereich gelten soll, geben Sie den Bereich mit Startadresse "-" Endadresse an, z. B. 192.168.100.10 - 192.168.100.20.
  - Wenn die Regel für alle IP-Adressen gelten soll, geben Sie " 0.0.0.0/0" ein.

- **Destination (Range)**
  Tragen Sie die IP-Adresse oder einen IP-Bereich ein, die IP-Pakete empfangen darf.
  - Wenn die Regel für einen IP-Bereich gelten soll, geben Sie den Bereich mit Startadresse "-" Endadresse an, z. B. 192.168.100.10 - 192.168.100.20.
  - Wenn die Regel für alle IP-Adressen gelten soll, geben Sie " 0.0.0.0/0" ein.
- **Service**
  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 Tables" > "Firewall Log" angezeigt.
- **Precedence**
  Legen Sie die Reihenfolge der Regel fest.

4.8.4 IPSec VPN

4.8.4.1 General

Auf der WBM-Seite konfigurieren Sie die Grundeinstellungen für VPN.



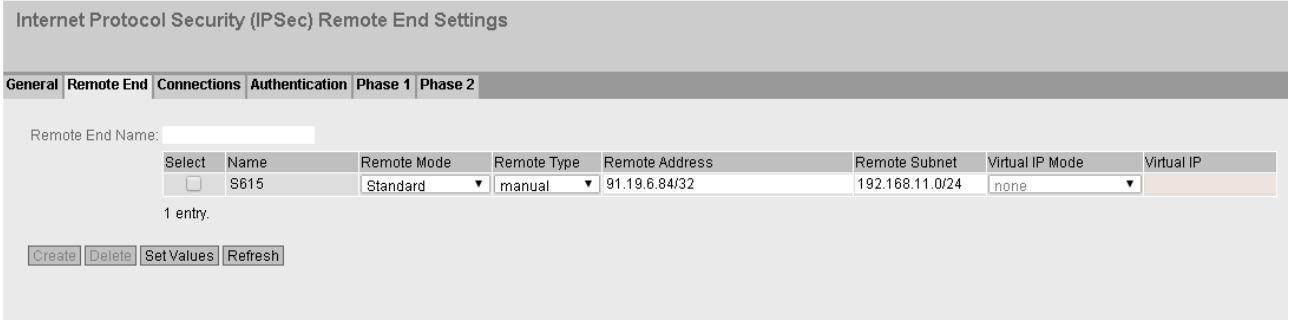
Beschreibung

Die Seite enthält Folgendes:

- **Optionskästchen "Activate IPsec VPN"**
  Aktivieren oder deaktivieren Sie das IPsec-Verfahren für VPN.
- **Klappliste "Enforce strict CRL Policy"**
  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 "Certificates (Seite 151)".
- **Eingabefeld "NAT Keep Alive Time Interval (s)"**
  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.

4.8.4.2 Remote End

Auf dieser WBM-Seite konfigurieren Sie die Gegenstelle (VPN-Endpunkt).



Beschreibung

Die Seite enthält Folgendes:

- **Eingabefeld "Remote End Name"**
  Tragen Sie einen Namen für die Gegenstelle ein und klicken Sie auf "Create", um eine neue Gegenstelle zu erstellen.

Die Tabelle enthält folgende Spalten:

- **Select**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Name**
  Zeigt den Namen der Gegenstelle an.

- **Remote Mode**
  Legen Sie fest, welche Rolle die Gegenstellen einnimmt.
  - Roadwarrior
    Im Roadwarrior-Modus nimmt das Gerät VPN-Verbindungen von Gegenstellen mit unbekannter Adresse an.
  - Standard
    Im Standard-Modus baut das Gerät eine Verbindung zu oder von einer bekannten Gegenstelle auf. Die Gegenstelle wird über die IP-Adresse oder den DDNS-Hostnamen identifiziert.
- **Remote Type**
  Legen Sie die Art der Gegenstellen-Adresse fest.
  - any (Nur bei Roadwarrior)
    Nimmt die Verbindung von Gegenstellen mit beliebiger IP-Adresse an.
  - manual (Bei Roadwarrior)
    Nimmt ausschließlich Verbindungen von Gegenstellen mit fester IP-Adresse (/32), festem IP-Subnetz (CIDR Notation), oder (D)DNS-Hostnamen an.
  - manual (Bei Standard)
    Baut ausschließlich Verbindung zu einer bestimmten Gegenstelle mit fester IP-Adresse oder mit (D)DNS-Hostnamen auf.
    Oder nimmt ausschließlich Verbindung von einer bestimmten Gegenstelle mit fester IP-Adresse oder mit (D)DNS-Hostnamen an.
- **Remote Address**
  - Im Standard-Modus tragen Sie die WAN-IP-Adresse oder den DDNS-Hostnamen ein.
  - Im Roadwarrior-Modus können Sie einen IP-Bereich eingeben, aus dem Verbindungen entgegengenommen werden. 0.0.0.0/0 bedeutet alle IP-Adressen werden akzeptiert.
- **Remote Subnet**
  Tragen Sie das entfernte Subnetz der Gegenstelle ein. Verwenden Sie die CIDR-Schreibweise. Nur editierbar, wenn bei "Remote Type" "manual" ausgewählt ist.
- **Virtual IP Mode**
  Legen Sie fest, ob der Gegenstelle eine virtuelle IP-Adresse angeboten wird.

  Folgende Möglichkeiten gibt es:
  - user defined IPv4
    Die virtuelle IP-Adresse ist aus dem bei "Virtual IP" festgelegten Band.
  - none
    Keine virtuelle IP Adresse. Der VPN-Tunnel wird dynamisch zur internen IP Adresse der Gegenstelle aufgebaut.
- **Virtual IP**
  Legen Sie das Subnetz fest (CIDR), aus dem die Gegenstelle eine virtuelle IP-Adresse angeboten bekommt. Nur editierbar, wenn bei "Virtual IP Mode" "user defined IPv4" ausgewählt ist.

Vorgehensweise

VPN-Standard-Modus projektieren

1. Tragen Sie bei "Remote End Name" den Namen der Gegenstelle ein.
2. Klicken Sie auf die Schaltfläche "Create". In der Tabelle wird ein neuer Eintrag erzeugt.
3. Wählen Sie bei "Remote Mode" "Standard" aus.
4. Wählen Sie bei "Remote Type" "manual" aus.
5. Tragen Sie bei "Remote Address" die WAN-IP-Adresse und bei "Remote Subnet" das Subnetz der Gegenstelle ein.
6. Klicken Sie auf die Schaltfläche "Set Values".

VPN-Roadwarrior-Modus projektieren

1. Tragen Sie bei "Remote End Name" den Namen der Gegenstelle ein.
2. Klicken Sie auf die Schaltfläche "Create". In der Tabelle wird ein neuer Eintrag erzeugt.
3. Wählen Sie bei "Remote Mode" "Roadwarrior" aus.
4. Wählen Sie bei "Remote Type" "any" aus.
5. Tragen Sie bei "Remote Address" die IP-Adresse des entfernten Netzes ein.
6. Legen Sie bei "Virtual IP Mode" fest, wie die IP-Adresse des VPN-Gateways bezogen wird.
7. Klicken Sie auf die Schaltfläche "Set Values".

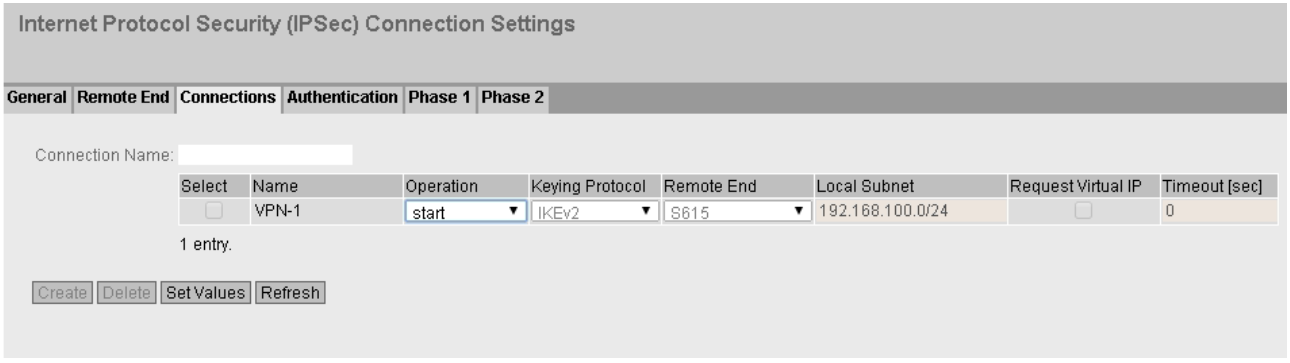
4.8.4.3 Connections

Auf dieser WBM-Seite konfigurieren Sie die Grundeinstellungen für die VPN-Verbindung. Mit diesen Einstellungen kann das Gerät einen ungesicherten VPN-Tunnel zur Gegenseite aufbauen. Die Sicherheitseinstellungen legen Sie auf der WBM-Seite "Authentication" fest.

Hinweis

Wenn Sie "1-to-1 NAT Local Subnet" verwenden,

- werden nur Auto-Firewall-Regeln unterstützt.
- ist bei "Operation" die Einstellung "on demand" nicht auswählbar



Beschreibung

Die Seite enthält folgende Felder:

- **Eingabefeld "Connection"**
  Geben Sie einen Namen für die VPN-Verbindung ein und klicken Sie auf "Create", um eine neue Verbindung zu erstellen.

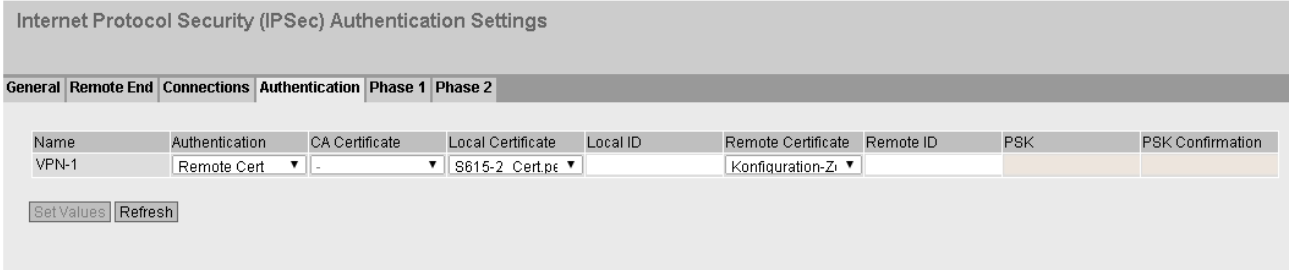
Die Tabelle enthält folgende Spalten:

- **Select**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Name**
  Zeigt den Namen der VPN-Verbindung an.

- **Operation**
  Legen Sie fest, von welchem Verbindungspartner die VPN-Verbindung aufgebaut wird.
  - disabled
    Die VPN-Verbindung ist deaktiviert.
  - start
    Die VPN-Verbindung wird vom lokalen Endpunkt initiiert.
  - wait
    Die VPN-Verbindung wird von der Gegenstelle aufgebaut.
  - on demand
    Die VPN-Verbindung wird bei Bedarf aufgebaut.
  - start on DI
    Die VPN-Verbindung wird beim Eintreten eines Ereignisses "Digital In" aufgebaut. Vorausgesetzt ist, dass beim Ereignis "Digital In" VPN-Tunnel aktiviert ist. Das Ereignis konfigurieren Sie unter "System > Events > Configuration".
- **Keying Protocol**
  Legen Sie fest, ob IKEv2 oder IKEv1 verwendet wird.
- **Remote End**
  Wählen Sie die gewünschte Gegenstelle aus. Nur die Gegenstellen sind projektierbar, die Sie auf der WBM-Seite "Remote End" konfiguriert haben.
- **Local Subnet**
  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.
- **Request Virtual IP**
  Wenn aktiviert, wird beim Verbindungsaufbau eine virtuelle IP-Adresse von der Gegenstelle angefordert.
- **Timeout [sec]**
  Nur bei der Einstellung "on demand". 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.

4.8.4.4 Authentication

Auf dieser WBM-Seite legen Sie fest, wie sich die VPN-Verbindungspartner gegenseitig authentisieren.



Beschreibung

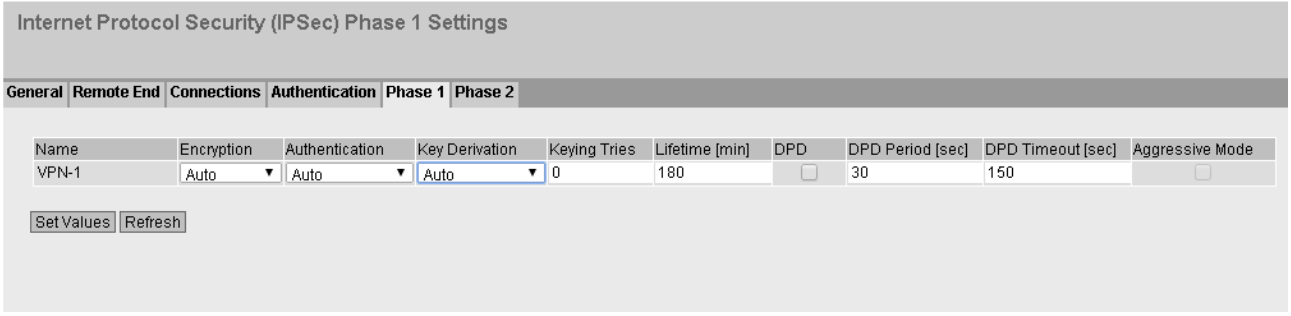
Die Tabelle enthält folgende Spalten:

- **Name**
  Zeigt den Namen der VPN-Verbindung an, auf die sich die Einstellungen beziehen.
- **Authentication**
  Wählen Sie das Authentisierungsverfahren aus. Voraussetzung für die VPN-Verbindung ist, dass die Gegenstelle das gleiche Authentisierungsverfahren verwendet.
  - disabled
    Es ist kein Authentisierungsverfahren gewählt. Ein Verbindungsaufbau ist nicht möglich.
  - CA Cert
    Für die Authentifizierung wird das Zertifikat der Zertifizierungsstelle verwendet. Das Zertifikat legen Sie bei "CA Certificate" fest.
  - Remote Cert
    Für die Authentifizierung wird das Gegenstellenzertifikat verwendet. Das Zertifikat legen Sie bei "Remote Certificate" fest
  - PSK
    Für die Authentifizierung wird ein Schlüssel verwendet. Den Schlüssel konfigurieren Sie bei "PSK".
- **CA Certificate**
  Wählen Sie das Zertifikat aus. Nur geladene Zertifikate sind auswählbar.
- **Local Cerificate**
  Wählen Sie das Gerätezertifikat aus.
- **Local 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 Cerificate**
  Wählen Sie das Gegenstellenzertifikat aus. Nur geladene Gegenstellenzertifikate sind auswählbar.
- **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 confirmation**
  Wiederholen Sie den Schlüssel.

4.8.4.5 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.
- **Encryption**
  Wählen Sie für die Phase 1 den gewünschten Verschlüsselungsalgorithmus aus. Folgende Verschlüsselungsalgorithmen werden unterstützt:
  - Auto: automatische Erkennung
  - 3DES-168
  - AES-128
  - AES-192
  - AES-256

Hinweis

Je mehr Bits ein Verschlüsselungsalgorithmus hat, desto sicherer ist der Algorithmus. Je nach gewähltem Algorithmus ist der Verschlüsselungsvorgang zeitaufwändiger und benötigt mehr Rechenleistung.

- **Authentication**
  Legen Sie das Verfahren zum Berechnen der Prüfsumme fest.
  Folgende Verfahren stehen zur Verfügung:
  - Auto: automatische Erkennung
  - MD5
  - SHA1
  - SHA512
- **IKE Key Derivation**
  Wählen Sie die gewünschte Diffie-Hellmann-Gruppe (DH), aus der ein Schlüssel erzeugt wird. Wenn "Auto" eingestellt ist, gilt keine Einschränkung. Es wird mit den Fähigkeiten der Gegenstelle abgeglichen und entsprechend gewählt.
- **Keying Tries**
  Tragen Sie die Anzahl der Wiederholungen für einen fehlgeschlagenen Verbindungsaufbau ein. Wenn Sie den Wert 0 eintragen, wird der Verbindungsaufbau unendlich oft zu versucht.
- **Lifetime [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 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

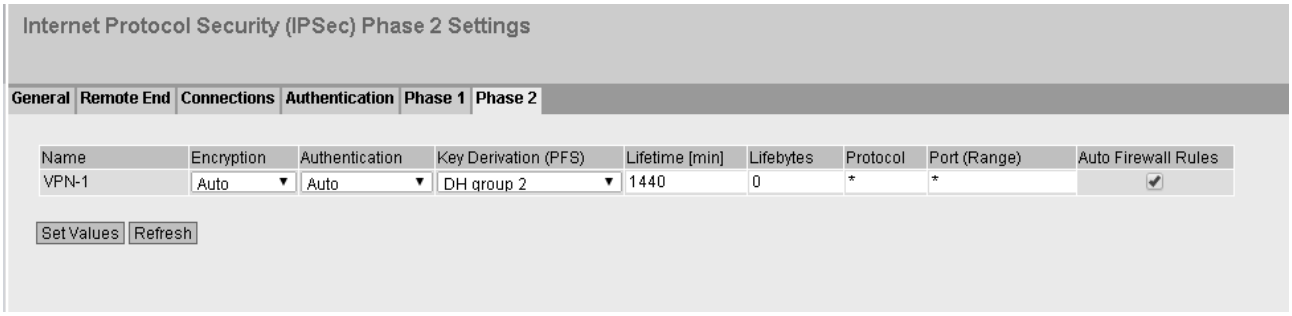
- **DPD Period [sec]**
  Tragen Sie eine Zeitspanne ein, nach der DPD-Anfragen gesendet werden. Diese Anfragen testen, ob die Gegenstelle noch verfügbar ist
- **DPD Timeout [sec]**
  Tragen Sie eine Zeitspanne ein. Wenn auf die DPD-Anfragen keine Antwort erfolgt, dann wird nach Ablauf dieser Zeit die Verbindung zur Gegenstelle für ungültig erklärt.
- **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.

4.8.4.6 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.
- **Encryption**
  Wählen Sie für die Phase 2 den gewünschten Verschlüsselungsalgorithmus aus. Folgende Verschlüsselungsalgorithmen werden unterstützt:
  - Auto: automatische Erkennung
  - 3DES-168
  - AES-128
  - AES-192
  - AES-256

Hinweis

Je mehr Bits ein Verschlüsselungsalgorithmus hat, desto sicherer ist der Algorithmus. Das Verfahren AES-256 Verfahren gilt daher als am sichersten. Allerdings ist der Verschlüsselungsvorgang zeitaufwändiger und benötigt mehr Rechenleistung.

- **Authentication**
  Legen Sie das Verfahren zum Berechnen der Prüfsumme fest.
  Folgende Verfahren stehen zur Verfügung:
  - Auto: automatische Erkennung
  - MD5
  - SHA1
  - SHA512
- **Key Derivation**
  Wählen Sie die gewünschte Diffie-Hellmann-Gruppe (DH), aus der ein Schlüssel erzeugt wird. Wenn "Auto" eingestellt ist, gilt keine Einschränkung. Es wird mit den Fähigkeiten der Gegenstelle abgeglichen und entsprechend gewählt.
- **Lifetime [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.
- **Protocol**
  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 (Range)**
  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 Firewall Rules**
  - akiviert
    Für die VPN-Verbindung werden automatisch die Firewall-Regeln angelegt.
  - deaktiviert
    Sie müssen selbst die Firewall-Regeln anlegen.

Instandhaltung und Wartung

5

5.1 Firmware-Update über HTTP

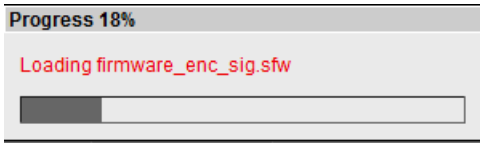
5.1.1 Firmware-Update über HTTP

Voraussetzung

- Das Gerät hat eine IP-Adresse und ist erreichbar.
- Das WBM ist gestartet und der Benutzer "admin" ist angemeldet.

Firmware-Update über HTTP

1. Klicken Sie im Navigationsbereich auf "System" > "Load&Save". Klicken Sie auf das Register "HTTP".
2. Klicken Sie bei "Firmware" auf die Schaltfläche "Load".
3. Navigieren Sie zum Ablageort der Firmware-Datei.
4. Klicken Sie im Dialogfenster auf die Schaltfläche "Öffnen". Die Firmeware-Datei wird geladen. Die Firmware selbst ist signiert und verschlüsselt. Damit ist sichergestellt, dass nur authentische Firmware auf das Gerät geladen wird.

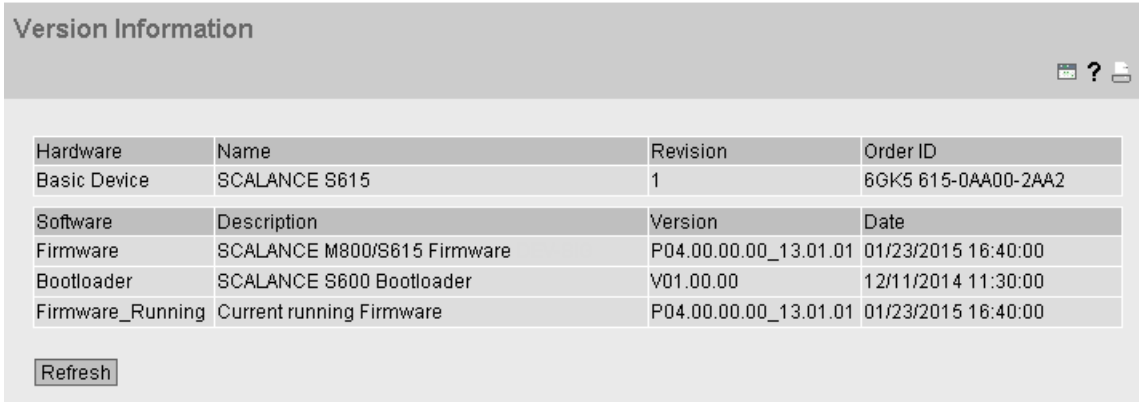


5. Wenn die Datei erfolgreich geladen ist, dann wird folgender Dialog angezeigt.

6. Klicken Sie auf "OK", um das Gerät neu zu starten. Wenn Sie auf "Cancel" klicken, dann müssen Sie das Gerät später über "System" > "Restart" neu starten.

Ergebnis

Die Firmware ist komplett auf das Gerät übertragen und unter "Information" > "Versions" 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.



Hardware	Name	Revision	Order ID
Basic Device	SCALANCE S615	1	6GK5 615-0AA00-2AA2

Software	Description	Version	Date
Firmware	SCALANCE M800/S615 Firmware	P04.00.00.00_13.01.01	01/23/2015 16:40:00
Bootloader	SCALANCE S600 Bootloader	V01.00.00	12/11/2014 11:30:00
Firmware_Running	Current running Firmware	P04.00.00.00_13.01.01	01/23/2015 16:40:00

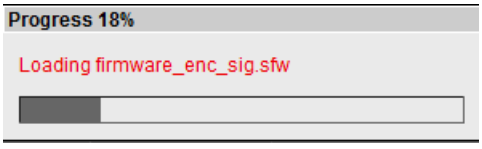
5.2 Firmware-Update über TFTP

Voraussetzung

- Das Gerät hat eine IP-Adresse und ist erreichbar.
- Das WBM ist gestartet und der Benutzer "admin" ist angemeldet.
- Ein TFTP-Server ist im Netzwerk vorhanden.
- Die Firmware-Datei liegt auf dem TFTP-Server.

Vorgehensweise

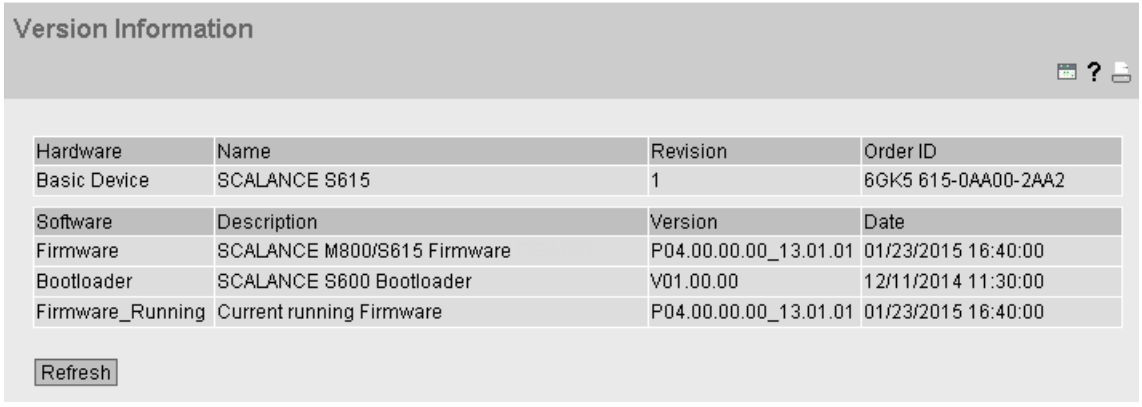
1. Klicken Sie im Navigationsbereich auf "System" > "Load&Save". Klicken Sie auf das Register "TFTP".
2. Tragen Sie bei "TFTP Server IP Address" die IP-Adresse des TFTP-Servers ein.
3. Tragen Sie bei "TFTP Server Port" den Port des TFTP-Servers ein
4. Ändern Sie in der Tabellenzeile "Firmware" bei Bedarf den Dateinamen.
5. Wählen Sie in der Tabellenzeile "Firmware" bei Aktion "Load file". Die Firmware selbst ist signiert und verschlüsselt. Damit ist sichergestellt, dass nur authentische Firmware auf das Gerät geladen wird.
6. Klicken Sie auf "Set Values". Die Firmware-Datei wird geladen. Die Firmware selbst ist signiert und verschlüsselt. Damit ist sichergestellt, dass nur authentische Firmware auf das Gerät geladen wird.



7. Wenn die Datei erfolgreich geladen ist, dann wird folgender Dialog angezeigt
8. Bestätigen Sie den Dialog mit "OK". Das Gerät wird neu gestartet.

Ergebnis

Die Firmware ist komplett auf das Gerät übertragen und unter "Information" > "Versions" 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.



5.3 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 Schnittstelle mit dem Gerät verbunden.
- Auf dem PC ist ein TFTP-Client installiert und die Firmware-Datei ist vorhanden.

Abhilfe

Über TFTP können Sie das Gerät auch dann mit einer Firmware versehen.
Führen Sie folgende Schritte durch, um eine neue Firmware über TFTP zu laden:

1. Drücken Sie nun den SET-Taster.
2. Halten Sie den Taster so lange gedrückt, bis die rote Fehler LED (F) nach ca. 3 Sekunden anfängt zu blinken.

   Hinweis

   Wenn Sie den SET-Taster ca. 10 Sekunden drücken, dann wird das Gerät auf seine Werkseinstellungen zurückgesetzt und ist über die IP-Adresse 192.168.1.1 erreichbar.

3. Lassen Sie nun den Taster los. Der Bootloader wartet in diesem Zustand auf eine neue Firmware-Datei, die Sie per TFTP laden können.

   Hinweis

   Wenn Sie den Bootloader ohne Änderung beenden wolllen, drücken Sie kurz den SET-Taster. Das Gerät startet mit der geladenen Konfiguration neu.

4. Verbinden Sie einen PC über die Ethernet-Schnittstelle mit dem Gerät.
5. Wechseln Sie in einer DOS-Box in das Verzeichnis, in dem sich die neue Firmware-Datei befindet und rufen Sie danach den Befehl "tftp -i <ip-adresse> PUT <firmware>" auf. Alternativ dazu können Sie einen anderen TFTP-Client verwenden.

   Wenn Sie nicht sicher sind, ob die IP-Adresse korrekt ist, dann können Sie diese z. B. mit 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.

5.4 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.

Index

N

P

R

S

T

U

V

W

Z