SIEMENS

SIMATIC NET

Industrial Wireless LAN SCALANCE W1780 / W1740 nach IEEE 802.11ac Web Based Management V3.0

Projektierungshandbuch

03/2022
C79000-G8900-C485-04

Rechtliche Hinweise

Warnhinweiskonzept

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

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

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

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

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

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

Qualifiziertes Personal

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

Bestimmungsgemäßer Gebrauch von Siemens-Produkten

Beachten Sie Folgendes:

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

Marken

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

Haftungsausschluss

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

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

C79000-G8900-C485-04
Ⓟ 03/2022 Änderungen vorbehalten

Inhaltsverzeichnis

Einleitung

1

1.1 Informationen zum Projektierungshandbuch

Gültigkeitsbereich des Projektierungshandbuchs

Dieses Projektierungshandbuch behandelt die folgenden Produkte:

- SCALANCE W1788-1 M12
- SCALANCE W1788-2 M12
- SCALANCE W1788-2 M12 EEC
- SCALANCE W1788-2IA M12
- SCALANCE W1748-1 M12

Das Projektierungshandbuch gilt für folgende Software-Version:

- SCALANCE W1700 Firmware ab Version V 3.0

Zweck dieses Projektierungshandbuchs

Dieses Projektierungshandbuch soll Sie in die Lage versetzen, Geräte fachgerecht zu montieren, in Betrieb zu nehmen und zu bedienen. Es vermittelt die notwendigen Kenntnisse über die Konfiguration der Geräte sowie die Einbindung der Geräte in ein WLAN-Netz.

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

Einordnung in die Dokumentationslandschaft

Zum Thema Industrial Wireless LAN gibt es von SIMATIC NET außer dem Projektierungshandbuch, das Sie gerade lesen, noch folgende Dokumentationen:

- Projektierungshandbuch: SCALANCE W1780/W1740 Command Line Interface
  Dieses Dokument enthält die CLI-Befehle, die von SCALANCE W1700-Geräten unterstützt werden.
- Leistungsdaten 802.11ac
  Dieses Dokument enthält Informationen zu Frequenz, Modulation, Sendeleistung und Empfangsempfindlichkeit der Funkkarte.

- Betriebsanleitung SCALANCE W1788-x/W1748-1
  Dieses Dokument enthält Informationen zu Montage, Anschließen, Instandhalten und Warten der folgenden Produkte:
  - SCALANCE W1788-1 M12
  - SCALANCE W1788-2 M12
  - SCALANCE W1788-2 M12 EEC
  - SCALANCE W1788-2IA M12
  - SCALANCE W1748-1 M12
- Systemhandbuch Aufbau eines Industrial Wireless LAN
  Es enthält neben der Beschreibung der physikalischen Grundlagen und einer Darstellung der wichtigsten IEEE-Standards auch Informationen über die Datensicherheit und eine Beschreibung von Industrieanwendungen von Wireless LAN.
  Sie sollten dieses Handbuch lesen, wenn Sie WLAN-Netze mit einer komplexeren Struktur aufbauen wollen (nicht nur Verbindung zwischen zwei Geräten).
- Systemhandbuch RCoax
  Dieses Systemhandbuch enthält sowohl eine Erklärung der technischen Grundlagen als auch eine Beschreibung der einzelnen RCoax-Komponenten und deren Arbeitsweise. Die Montage/Inbetriebnahme sowie der Anschluss von RCoax-Komponenten und deren prinzipielle Arbeitsweise wird erläutert. Die Anwendungsmöglichkeiten der verschiedenen SIMATIC NET-Komponenten werden beschrieben.
- Systemhandbuch Passive Netzkomponenten IWLAN
  Dieses Systemhandbuch erläutert Ihnen die gesamte IWLAN-Verkabelungstechnik, die Sie für Ihre IWLAN-Anwendung benötigen. Für eine flexible Kombination und Installation der einzelnen IWLAN-Komponenten im Innen- wie Außenbereich wird ein umfangreiches, aufeinander abgestimmtes Sortiment an koaxialen Zubehörteilen angeboten. Das Systemhandbuch umfasst sowohl Anschlussleitungen als auch diverse Steckverbinder, Blitzschutzelemente, einen Power Splitter und ein Dämpfungsglied.

Verwendete Begriffe

Die Bezeichnung . . .	**steht für . . .**
IPv4-Adresse	IPv4-Adresse
IPv6-Adresse	IPv6-Adresse
IP-Adresse	IPv4-/IPv6-Adresse
IPv4-Schnittstelle	Schnittstelle, die IPv4 unterstützt.
IPv6-Schnittstelle	Schnittstelle, die IPv6 unterstützt. Die Schnittstelle kann mehr als eine IPv6-Adresse besitzen. Die IPv6-Adressen haben verschiedene Reichweiten (Scope), z. B. Link-lokal.
IP-Schnittstelle	Schnittstelle, die sowohl IPv4 als auch IPv6 unterstützt. Standardmäßig ist die IPv4 Unterstützung bereits aktiviert. Die IPv6 Unterstützung muss zusätzlich aktiviert werden.

SIMATIC NET-Handbücher

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

- über die Suchfunktion:
  Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/de/)
  Geben Sie die Beitrags-ID des jeweiligen Handbuchs als Suchbegriff ein.
- über die Navigation auf der linken Seite im Bereich "Industrielle Kommunikation":
  Industrielle Kommunikation (https://support.industry.siemens.com/cs/ww/de/ps/15247/man)
  Navigieren Sie zu der gewünschten Produktgruppe und nehmen Sie folgende Einstellungen vor:
  Register "Beitragsliste", Beitragstyp "Handbücher / Betriebsanleitungen"

Weiterführende Dokumentation

Im Handbuch "SIMATIC NET Industrial Ethernet Netzhandbuch" erhalten Sie Hinweise zu weiteren SIMATIC NET-Produkten, die Sie gemeinsam mit den Geräten dieser Produktlinie in einem Industrial Ethernet Netzwerk betreiben können. Sie finden dort u. a. optische Leistungsdaten der Kommunikationspartner, die Sie für den Aufbau benötigen.

Das "SIMATIC NET Industrial Ethernet Netzhandbuch" finden Sie auf den Internetseiten des Siemens Industry Online Support unter folgender Beitrags-ID:
27069465 (https://support.industry.siemens.com/cs/ww/de/view/27069465)

Security-Hinweise

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

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen einen Bestandteil eines solchen Konzepts.

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

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

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

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

Firmware

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

Die Firmware inden Sie auf den Internetseiten des Siemens Industry Online Support: (https://support.industry.siemens.com/cs/ww/de/ps/25169/dl)

Hinweis zum Firmware-/Software-Support

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

Außerbetriebnahme

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

Setzen Sie das Gerät hierzu auf Werkseinstellungen zurück.

Setzen Sie auch das Speichermedium auf Werkseinstellungen zurück.

Recycling und Entsorgung

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

Entsorgen Sie die Produkte nicht bei öffentlichen Entsorgungsstellen.

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

Beachten Sie unterschiedliche länderspezifische Regelungen.

Gerät defekt

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

Marken

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

SCALANCE, RCoax

Lizenzbedingungen

Hinweis

Open Source Software

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

Die Lizenzbedingungen und Copyright-Hinweise können Sie über das WBM oder CLI als zip-Datei herunterladen.

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

1.2 Typenbezeichnungen

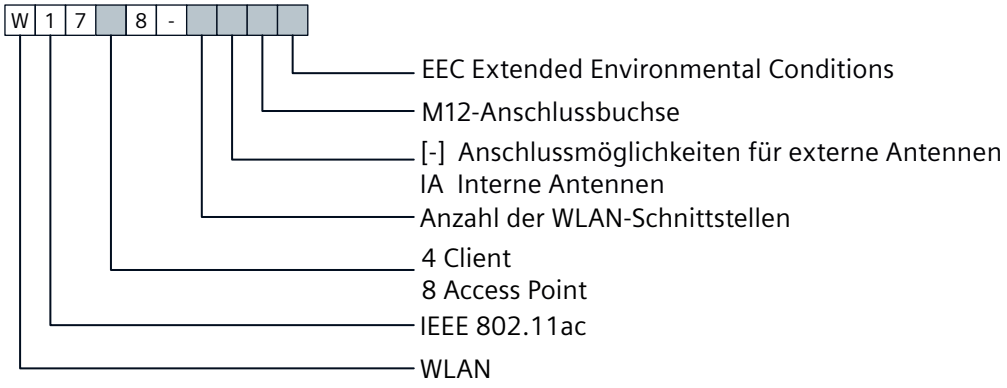
Verwendete Abkürzungen

Die Informationen in den Handbüchern der SCALANCE W1700-Produktfamilie gelten häufig nicht nur für eine Produktvariante. In diesen Fällen werden abkürzende Bezeichnungen verwendet, um nicht alle Typenbezeichnungen aufzählen zu müssen. Die folgende Tabelle zeigt die Zuordnung von Abkürzungen und Produktvarianten.

Produktgruppe	Die Bezeichnung . . . steht für . . .	Produktname
SCALANCE W1700 ac	SCALANCE W1700	• SCALANCE W1788-1 M12 • SCALANCE W1788-2 M12 • SCALANCE W1788-2 M12 EEC • SCALANCE W1788-2IA M12 • SCALANCE W1748-1 M12
Access Points (IP 65)	SCALANCE W1780	• SCALANCE W1788-1 M12 • SCALANCE W1788-2 M12 • SCALANCE W1788-2 M12 EEC • SCALANCE W1788-2IA M12
Client (IP65)	SCALANCE W1740	• SCALANCE W1748-1 M12

Aufbau der Typenbezeichnung

Die Typenbezeichnung des Geräts setzt sich aus mehreren Teilen zusammen, die folgende Bedeutung haben:



Beschreibung

2

Hinweis

Unterbrechung der WLAN-Kommunikation

Die WLAN-Kommunikation kann durch entsprechend hochfrequente Störsignale beeinflusst und vollständig unterbrochen werden.

Beachten Sie dies und treffen Sie entsprechende Vorkehrungen.

2.1 Netzstrukturen

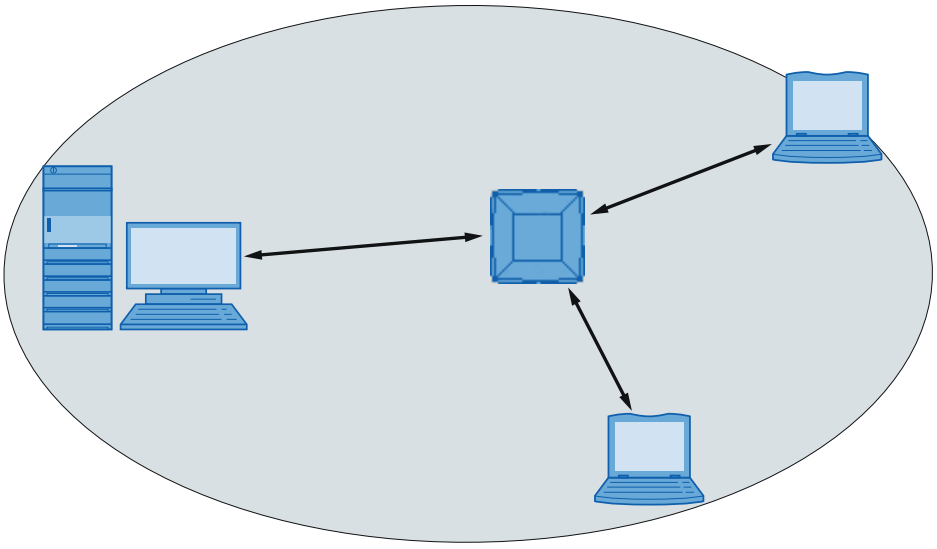
Der nachfolgende Artikel behandelt den Aufbau verschiedener Netzstrukturen mit Hilfe von Access Points.

Standalone-Konfiguration mit Access Point

Diese Konfiguration erfordert keinen Server und der Access Point verfügt nicht über eine Verbindung zu einem drahtgebundenen Ethernet. Der Access Point leitet innerhalb seiner Reichweite Daten von einem WLAN-Teilnehmer zu einem anderen.

Das Funknetz hat einen eindeutigen Namen. Alle SCALANCE W-Geräte, die innerhalb dieses Netzes Daten austauschen wollen, müssen mit diesem Namen konfiguriert sein.

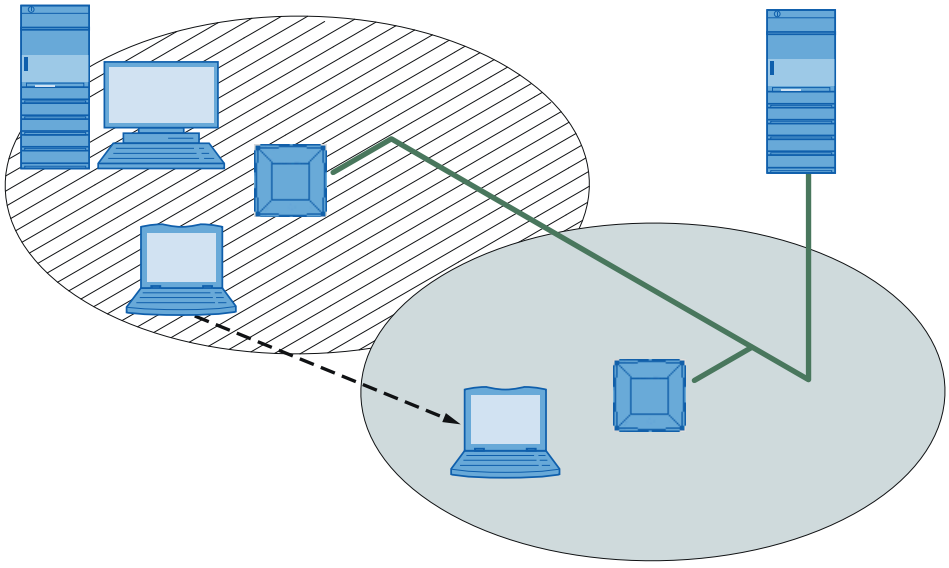
Die graue Fläche in der Grafik symbolisiert die Funkreichweite des Access Points.



Funkzugang zu einem drahtgebundenen Ethernet-Netzwerk

Wenn ein (oder mehrere) Access Points Verbindung zu einem drahtgebundenen Ethernet haben, bieten sich folgende Einsatzmöglichkeiten an:

- Ein einzelner als Netzübergang:
  Ein drahtloses Netz kann mit einem drahtgebundenen Netz über einen Access Point verbunden werden.
- Ausdehnung der Funkabdeckung für das drahtlose Netz mit mehreren Access Points:
  Die Access Points sind alle mit der gleichen eindeutigen SSID (Netzwerknamen) konfiguriert. Alle Teilnehmer, die über dieses Netz kommunizieren wollen, müssen ebenfalls mit dieser SSID konfiguriert sein.
  Wird eine mobile Station aus dem Bereich eines Access Points in den Bereich eines anderen Access Points verschoben, bleibt die Funkverbindung bestehen (Roaming).
  Die folgende Grafik zeigt die Funkverbindung einer mobilen Station über zwei Funkzellen (Roaming).



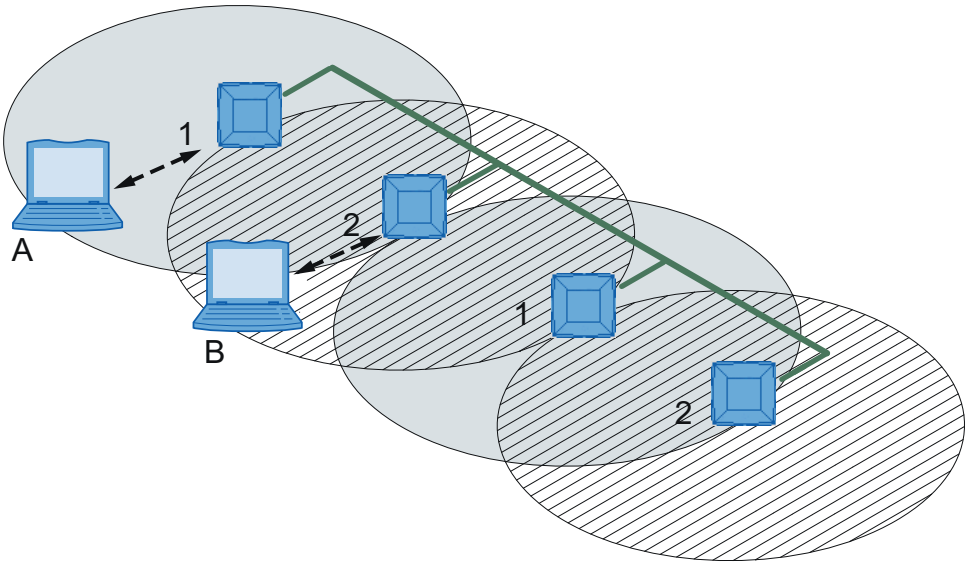
Mehrkanal-Konfiguration

Nutzen benachbarte Access Points den gleichen Frequenzkanal, kann es zu längeren Antwortzeiten wegen eventuell auftretender Kollisionen kommen. Würde die in der Abbildung dargestellte Konfiguration als Einkanal-System realisiert, könnten Computer A und B nicht gleichzeitig mit den entsprechenden Access Points in ihrer Funkzelle kommunizieren.

Wenn benachbarte Access Points für unterschiedliche Frequenzen eingerichtet werden, führt das zu einer erheblichen Performance-Verbesserung. Dadurch wird benachbarten Funkzellen jeweils ein eigenes Medium zur Verfügung gestellt und die Verzögerungen durch zeitversetztes Senden entfallen.

Der Kanalabstand sollte möglichst groß sein, ein sinnvoller Wert ist 25 MHz. Auch bei der Mehrkanal-Konfiguration können alle Access Points mit dem gleichen Netznamen konfiguriert werden.

Die folgende Grafik zeigt eine Mehrkanalkonfiguration auf den Kanälen 1 und 2 mit vier Access Points.

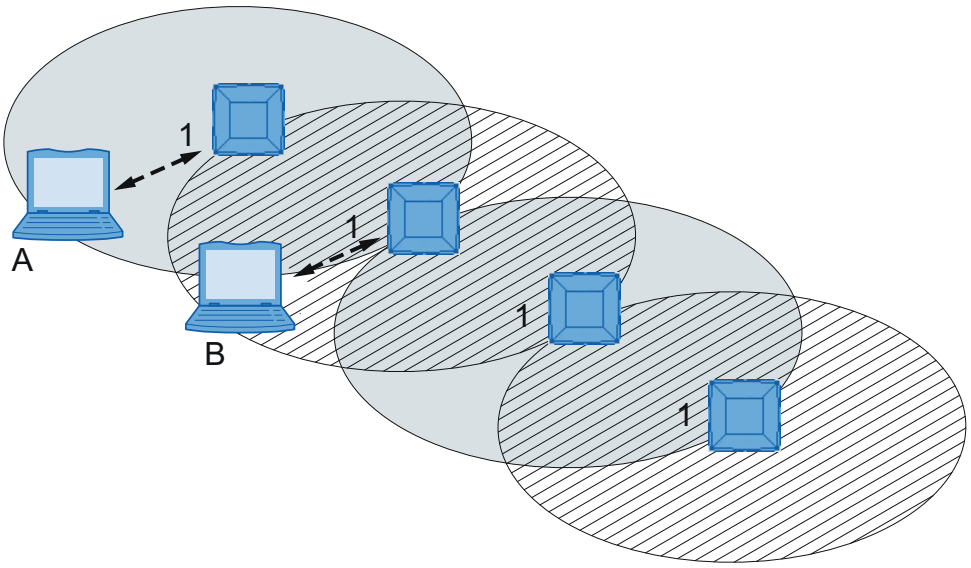


Wireless Distribution System (WDS)

WDS ermöglicht direkte Verbindungen zwischen Access Points oder zwischen Access Points und anderen WDS-fähigen Geräten. Sie dienen zum Aufbau eines Wireless Backbone oder zur Anbindung eines einzelnen Access Points an ein Netzwerk, der auf Grund seiner Lage nicht direkt an die Kabelinfrastruktur angeschlossen werden kann.

Bei der Konfiguration bieten sich zwei Alternativen. Der WDS-Partner kann sowohl über die WDS ID als auch über seine MAC-Adresse konfiguriert werden.

Die folgende Grafik zeigt die Realisierung von WDS mit vier Access Points.



2.2 Einsatzmöglichkeiten

Hinweis

Die SIMATIC NET WLAN-Produkte verwenden OpenSSL.

Hierbei handelt es sich um "Open Source Code" mit Lizenzbedingungen (BSD).

Bitte beachten Sie hierzu die aktuellen Lizenzbedingungen.

Da der Treiber Verschlüsselungs-Software enthält, sollten Sie zudem die entsprechenden länderspezifischen Bestimmungen beachten.

Einsatzmöglichkeiten für den SCALANCE W1788

Der SCALANCE W1788 ist mit zwei Ethernet-Schnittstellen und bis zu zwei WLAN-Schnittstellen ausgestattet. Dadurch ist dieses Gerät für folgende Einsatzfälle geeignet:

- Der SCALANCE W1788 leitet innerhalb seiner Reichweite Daten von einem Teilnehmer zu einem anderen, ohne dass eine Verbindung zu einem drahtgebundenen Ethernet bestehen muss.
- Der SCALANCE W1788 kann als Netzübergang von einem drahtgebundenen zu einem drahtlosen Netz verwendet werden.
- Der SCALANCE W1788 kann als drahtlose Brücke zwischen zwei Netzen eingesetzt werden.

- Der SCALANCE W1788 kann als Brücke zwischen zwei Funkzellen mit verschiedenen Frequenzen dienen.
- Der SCALANCE W1788 verfügt über einen integrierten Switch und lässt sich über seine zwei managed Ethernet Gigabit-Ports vielfältig vernetzen.
- Der SCALANCE W1788 unterstützt die Schutzklasse IP65 und ist somit staubdicht sowie vollständig gegen Berührung und gegen Strahlwasser (Düse) aus beliebigem Winkel geschützt.
- Der SCALANCE W1788 M12 EEC eignet sich für Einsätze in rauer Umgebung.

Darüber hinaus können Sie mit einem SCALANCE W1788 mit mehr als einer WLAN-Schnittstelle auch eine redundante Funkverbindung zu einem SCALANCE W1788 mit maximal zwei WLAN-Schnittstellen realisieren.

2.3 Produkteigenschaften

Eigenschaften der SCALANCE W1700-Geräte

- Die Ethernet-Schnittstelle unterstützt Folgendes:
  - 10 Mbit/s und 100 Mbit/s jeweils Voll- und Halb-Duplex
  - 1000 Mbit/s Voll-Duplex
  - Auto-Crossing
  - Auto-Polarity
- Betrieb der WLAN-Schnittstelle in den Frequenzbändern 2,4 GHz und 5 GHz.
- IEEE 802.11ac
  High Speed WLAN-Standard (Funk-LAN) mit einer Brutto-Übertragungsgeschwindigkeit bis zu 1733 Mbit/s.
- IEEE 802.11r
  Optimierung des Roamings (Fast BSS Transition)
- Die WLAN-Schnittstelle ist kompatibel zu den Standards IEEE 802.11n.

- IEEE 802.11h - Ergänzung von IEEE 802.11a
  Im 802.11h-Modus werden die beiden Verfahren "Transmit Power Control (TPC)" sowie "Dynamic Frequency Selection (DFS)" im Bereich von 5,25 - 5,35 und 5,47 - 5,75 GHz verwendet. Dadurch kann in einigen Ländern das Frequenz-Subband von 5,47 - 5,725 GHz im Outdoor-Bereich auch mit höheren Sendeleistungen genutzt werden.
  TPC ist ein Verfahren zur Anpassung der Sendeleistung.
  Bei DFS sucht der Access Point vor Aufnahme der Kommunikation auf dem gewählten Kanal 60 Sekunden nach nach konkurrierenden Radarsignale ab. Innerhalb der Suchdauer sendet der Access Point auch keine Beacons. Bei Wetter-Radar-Kanälen (5,6 - 5,65 GHz) beträgt die Suchdauer 10 Minuten.
  Wenn nach Ablauf der Suchdauer keine Radarsignale gefunden wurden, sendet der Access Point auf dem Kanal. Sonst wechselt der Access Point den Kanal und wiederholt die Prüfung. Auch während des Betriebs sucht der Access Point ständig nach Radarsignalen.
  Wenn der Access Point auf dem aktuellen Kanal ein Radarsignal entdeckt, kündigt er den Kanalwechsel den Clients an. Danach wechselt er automatisch auf einen alternativen DFS-Kanal und der aktuelle Kanal wird für 30 Minuten gesperrt
- Unterstützung der Authentifizierungs-Standards WPA (RADIUS), WPA-PSK, WPA2 (RADIUS), WPA2-PSK und IEEE 802.1X sowie der Verschlüsselungsverfahren WEP, AES und TKIP.

Hinweis

Bei Geräten, die im WLAN-Modus IEEE 802.11n/ac betrieben werden, ist nur die WPA2 (WPA2-PSK u. WPA2 Radius) Verschlüsselung möglich.

- Für die bessere Übertragung über WLAN ist die Funktion WMM (Wireless Multimedia) aktiviert. Die Frames werden nach ihrer Priorität bewertet und priorisiert über die WLAN-Schnittstelle gesendet.
- Geeignet für die Einbeziehung eines RADIUS-Servers für die Authentifizierung.
- Gerätebezogene und anwendungsbezogene Überwachung der Funkverbindung.
- Die Interoperabilität der Geräte mit Wi-Fi-Geräten anderer Hersteller wurde ausführlich getestet.
- Vor der Inbetriebnahme des SCALANCE W1700 müssen Sie die Funkverhältnisse vor Ort überprüfen. Beim gleichzeitigen Betrieb von Industrial Wireless LAN-Systemen und WirelessHART-Systemen im 2,4 GHz-Band müssen Sie eine Kanalplanung vornehmen. Vermeiden Sie unbedingt die parallele Nutzung von sich überschneidenden Frequenzbereichen. Es gibt folgende Überschneidungen bei Industrial Wireless LAN und WirelessHART:

IWLAN-Kanal IEEE 802.11 b/g/n	**WHART-Kanal IEEE 802.15.4**
1	11 - 16
6	15 - 20
7	16 - 21
11	20 - 25
13	21 - 25

Merkmale des SCALANCE W1700

Typ	Anzahl WLAN-Schnittstellen	Antennen	Anzahl und Art der Ethernet-Schnittstelle	Schutzart	Artikelnummer
SCALANCE W1788-1 M12	1	4 x extern	2 x Gigabit-Ethernet (Kupfer) 1 x PoE	IP65	6GK5788-1GY01-0AA0
SCALANCE W1788-2 M12	2	8 x extern	2 x Gigabit-Ethernet (Kupfer) 1 x PoE	IP65	6GK5788-2GY01-0AA0
SCALANCE W1788-2 M12 EEC	2	8 x extern	2 x Gigabit-Ethernet (Kupfer) 1 x PoE	IP65	6GK5788-2GY01-0TA0
SCALANCE W1788-2IA M12	2	8 x intern	2 x Gigabit-Ethernet (Kupfer) 1 x PoE	IP65	6GK5788-2HY01-0AA0
SCALANCE W1748-1 M12	1	4 x extern	2 x Gigabit-Ethernet (Kupfer) 1 x PoE	IP65	6GK5748-1GY01-0AA0

2.4 IEEE 802.11n/ac

Überblick

Der Standard IEEE 802.11ac ist eine Weiterentwicklung des Standard IEEE 802.11n, der abwärtskompatibel zu den Standards IEEE 802.11a, IEEE 802.11h und IEEE 802.11n ist. Die im Standard IEEE 802.11n implementierten Mechanismen der PHY- und MAC-Schicht wurden verbessert.

In der folgenden Tabelle sind die wichtigsten Unterschiede aufgeführt.

	IEEE 802.11n	IEEE 802.11ac
Frequenzband	2,4 GHz und 5 GHz	5 GHz
Kanalbandbreite	20MHz, 40 MHz	20 MHz, 40 MHz, 80 MHz Optional: 160 MHz
Spatial Streams (Datenströme)	1 bis 4	1 bis 8 Bis zu 4 pro Client
MIMO	Single-User MIMO	Multi-User MIMO
Modulationsschema	OFDM (BPSK, QPSK, 16-QAM, 64-QAM)	OFDM (BPSK, QPSK, 16-QAM, 64-QAM, 128-QAM, optional 256-QAM)

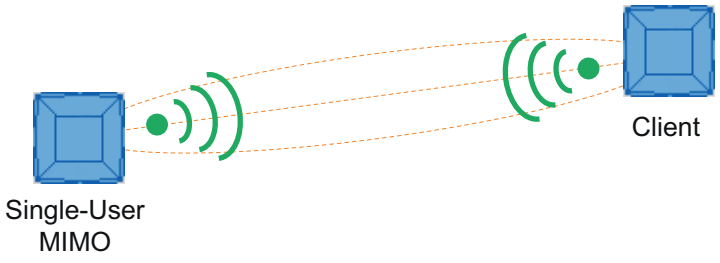
MIMO-Antennentechnik

MIMO (Multiple Input - Multiple Output) basiert auf einem intelligenten Mehrantennensystem. Dabei haben der Sender und der Empfänger jeweils mehrere räumlich getrennte Antennen. Diese getrennten Antennen strahlen die Datenströme (Spatial Streams) zur gleichen Zeit aus. Bei IEEE 802.11n sind bis zu vier Datenströme möglich und bei IEEE 802.11ac bis zu 8 Datenströme.

Die Datenströme werden dabei räumlich verteilt ausgestrahlt und legen durch Beugung, Brechung, Fading und Reflexion (Mehrwegausbreitung) verschiedene Wege zurück. Die Mehrwegeausbreitung bewirkt, dass am Empfangsort ein komplexes, raum- und zeitabhängiges Muster als Summensignal der einzelnen Sendesignale entsteht. Dieses eindeutige Muster nutzt MIMO, indem es die in ihrer räumlichen Position charakteristischen Signale erfasst. Dabei unterscheidet sich jede Raumposition von der benachbarten. Durch die spezifische Charakteristik jedes Senders ist der Empfänger in der Lage, mehrere Signale voneinander zu trennen.

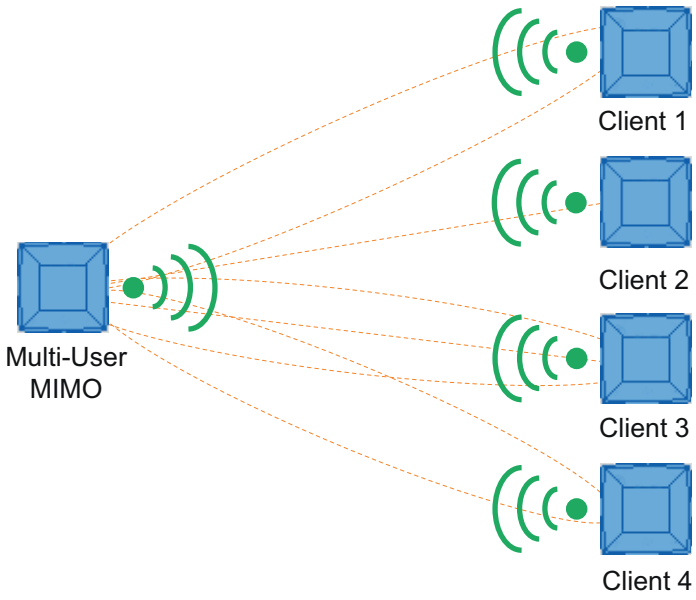
Single-User MIMO

Beim Single-User MIMO wird ein und dasselbe Telegramm über mehrere Datenströme an einen einzigen WLAN-Client gesendet. Ein Single-User MIMO kann bis zu vier Geräte abwechselnd bedienen, aber zu jedem Zeitpunkt immer nur ein Gerät.



Multi-User MIMO

Beim Multi-User MIMO werden mehrere Telegramme an unterschiedliche Multi-User MIMO-Clients über das gleiche Frequenzspektrum gleichzeitig übertragen. Ein Multi-User MIMO versorgt somit bis zu vier Multi-User MIMO-Clients mit Daten zur selben Zeit.



Spatial Mutliplexing

Beim räumlichen Multiplexen (Spatial Multiplexing) werden verschiedene Informationen über die gleiche Frequenz gesendet. Der Datenstrom wird auf n Sendeantennen verteilt, d. h. jede Antenne sendet nur 1/n des Datenstroms. Das Aufteilen des Datenstroms ist durch die Anzahl der Antennen beschränkt. Auf der Empfängerseite wird das Signal wieder zusammengesetzt. Durch das räumliche Multiplexen ergeben sich ein höheres Signal-Rausch-Verhältnis und ein höherer Datendurchsatz.

Verkürztes Guard-Intervall

Das Guard-Intervall verhindert, dass sich verschiedene Übertragungen vermischen. In der Nachrichtentechnik wird dieses Vermischen auch als Intersymbolinterferenz (ISI) bezeichnet. Nach Ablauf der Sendezeit wird eine Sendepause (Guard-Intervall) eingelegt, bevor die nächste Übertragung beginnt.

Das Guard-Intervall von IEEE 802.11a/b/g beträgt 800 ns. IEEE 802.11n/ac kann das verkürzte Guard-Intervall von 400 ns benutzen. Das Guard-Intervall legen Sie auf der WBM-Seite "AP 802.11n/ac (Seite 264)" fest.

Frame Aggregation

Bei IEEE 802.11n/ac ist es möglich einzelne Frames zu einem größeren Frame zusammenzufassen, was als Frame Aggregation bezeichnet wird. Es gibt zwei Arten der Frame Aggregation:

- Aggregated MAC Service Data Unit (A-MSDU)
  Mehrere MSDU-Frames mit der gleichen Zieladresse werden aneinanderhängt und zusammen als ein A-MSDU versendet. Dadurch wird die Netzwerklast verringert. A-MSDUs eignen sich durch ihre kürzere maximale Länge eher für die Bündelung mehrerer kürzerer Frames.
- Aggregated MAC Protocol Data Unit (A-MPDU)
  Mehrere MPDU-Frames mit der gleichen Zieladresse werden zusammengefasst und als ein großes A-MPDU versendet. Dadurch kann der Gesamtdurchsatz vergrößert werden.

Die SCALANCE W-Geräte unterstützen beide Arten der Frame Aggregation. Die Einstellungen legen Sie auf der WBM-Seite "AP 802.11n/ac (Seite 264)" fest.

Maximum Ratio Combining (MRC)

Beim Mehrantennensystem werden die Funksignale von den einzelnen Antennen empfangen und zu einem Signal kombiniert. Zum Kombinieren der Funksignale wird das MRC-Verfahren verwendet. Das MRC-Verfahren gewichtet die Funksignale nach ihrem Signal-Rausch-Verhältnis und kombiniert die Funksignale zu einem Signal. Das Signal-Rausch-Verhältnis wird verbessert und die Fehlerrate wird verringert.

2.5 IEEE 802.11r

Beim Roaming wandert der WLAN-Client von einem Access Point zum nächsten. Beim Verbindungsübergang kann eine Verzögerungszeit von mehreren 100 ms entstehen.

In dieser Zeit können die folgenden Schritte durchlaufen werden:

- Client sucht nach einem neuen Access Point (Scanning)
- Anmeldung an einem neuen Access Point (Authentication und Association)
- Ermöglichen einer Datenverbindung über den neuen Access Point

Bei zeitkritischen Anwendungen sind geringere Verzögerungszeiten notwendig, z. B. für Voice over IP. Der Standard IEEE 802.11r enthält Erweiterungen, die das Roaming optimieren, und wird deshalb auch Fast BSS Transition (FT) genannt.

Beim FT muss sich der WLAN-Client nicht bei jedem Wechsel des Access Points erneut authentifizieren. Dazu werden die Access Points in einer Mobilitätsdomäne zusammengefasst. Von dem ersten Access Point, an dem sich der WLAN-Client anmeldet, erhält er die ID der Mobilitätsdomäne mitgeteilt. Die Anmeldeinformation wird innerhalb der Mobilitätsdomäne zwischengespeichert. Diese Anmeldung gilt für alle Mitglieder der Mobilitätsdomäne.

Anhand der ID erkennt der WLAN-Client, ob der Access Point dergleichen Mobilitätsdomäne angehört und sich somit ohne Verzögerung anmelden kann. Nur die WLAN-Clients mit IEEE 802.11r-Unterstützung können das verbesserte Roaming bzw. Handover nutzen.

Voraussetzung

- Die Access Points sind Mitglieder der gleichen Mobilitätsdomäne
- Nur mit WPA2-Verschlüsselung (WPA2-PSK u. WPA2 RADIUS) möglich

2.6 Voraussetzungen für Installation und Betrieb

Für die Konfiguration der SCALANCE W-Geräte muss ein PG/PC mit Netzwerkanschluss vorhanden sein. Falls kein DHCP-Server zur Verfügung steht, ist für die erstmalige Zuordnung einer IP-Adresse an den SCALANCE W-Geräten ein PC erforderlich, auf dem das SINEC PNI installiert ist. Für die weitere Konfiguration ist ein Computer mit Telnet oder einem Webbrowser notwendig.

2.7 Configuration License PLUG (CLP)

Den PLUG gibt es in folgenden Varianten:

- PLUG-Konfiguration: Das Wechselmedium speichert ausschließlich die Konfigurationsdaten des Geräts.
- PLUG-Lizenz: Das Wechselmedium enthält zusätzlich zu den Konfigurationsdaten eine Lizenz, mit der spezielle Funktionen freigeschalten werden, z B. die iFeatures.

Funktionsweise

ACHTUNG
Den 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, startet das Gerät neu. War in dem Gerät ein gültiger PLUG-Lizenz gesteckt, wird das Gerät nach dem Neustart in einen definierten Fehlerzustand versetzt. Bei SCALANCE W werden in diesem Fall die verfügbaren Funkschnittstellen deaktiviert. Wenn das Gerät einmal mit einem PLUG-Lizenz konfiguriert wurde, kann das Gerät ohne diesen PLUG nicht mehr genutzt werden. Um das Gerät wieder nutzen zu können, setzen Sie das Gerät auf Werkseinstellungen zurück.

Geräte mit CLP-Steckplatz unterstützen die folgenden Betriebsarten:

- **Ohne PLUG**
  Das Gerät speichert die Konfigurationsdaten auf dem internen Speicher. Dieser Modus ist aktiv, wenn kein PLUG gesteckt ist.
- **Mit PLUG**
  Wenn ein unbeschriebener PLUG (Auslieferungszustand) in das Gerät gesteckt wird, sichert das Gerät beim Anlauf automatisch die Konfigurationsdaten auf dem PLUG. Enthält der PLUG eine Lizenz, werden außerdem zusätzliche Funktionen freigeschaltet. Änderungen der Konfiguration werden direkt auf dem PLUG und auf dem internen Speicher gesichert.
  Die Konfiguration, die auf dem PLUG gespeichert ist, wird über die Benutzerschnittstellen angezeigt.
  Ein Gerät übernimmt beim Hochlauf automatisch die Konfiguration des gesteckten, beschriebenen PLUG. Voraussetzung ist, dass die Konfigurationsdaten von einem kompatiblen Gerätetyp beschrieben wurden.
  Einen Ausnahmefall kann die IP-Konfiguration darstellen, wenn sie per DHCP eingestellt wird und der DHCP-Server nicht entsprechend umkonfiguriert wurde. Eine Nachkonfiguration ist erforderlich, wenn Sie Funktionen verwenden, die auf MAC-Adressen basieren.

Firmware auf PLUG

Neben einem kompatiblen Gerätetyp ist auch die Version der Firmware für einen erfolgreichen Gerätetausch mittels CLP relevant.

Die Übertragung der Konfiguration auf ein Ersatzgerät funktioniert nur, wenn die Firmware-Version auf dem Ersatzgerät gleich oder neuer ist als die des ausgefallenen Geräts. Ein Gerät mit einer älteren Firmware akzeptiert den CLP nicht und startet mit der Konfiguration aus seinem internen Speicher.

Ein Gerät kann daher nicht nur seine Konfiguration sondern auch seine aktuelle Firmware auf dem CLP speichern. Sie können konfigurieren, ob die Firmware auf dem CLP gespeichert werden soll oder nicht:

- Wenn die Funktion aktiviert ist, speichert das Gerät seine aktuelle Firmware auf dem CLP. Wenn die Firmware-Datei auf dem Gerät aktualisiert wird, wird die aktualisierte Version auch auf dem CLP gespeichert.
- Wenn die Funktion deaktiviert ist, wird die Firmware von dem CLP gelöscht.
- Wenn die Einstellung geändert wird, reagiert das Gerät direkt und speichert bzw. löscht die Firmware von dem CLP.

In der Anlaufphase prüft das Gerät nicht, ob die Funktion aktiviert oder deaktivert ist. Wenn die Daten des gesteckten CLPs kompatibel sind und der CLP eine gültige, aber abweichende Firmware enthält, wird die Firmware des CLPs auf das Gerät übertragen.

Komponente	Beschreibung	Artikelnummer
CLP Configuration License PLUG	Wechselmedium zur Speicherung von Konfigurationsdaten	
	SCALANCE CLP 2GB	6GK1900-0UB00-0AA0
	SCALANCE CLP EEC 2GB	6GK1900-0UQ00-0AA0
	SCALANCE CLP 32GB	6GK1900-0UB40-0AA0

Komponente	Beschreibung	Artikelnummer
CLP iFeatures	Wechselmedium zur Speicherung von Konfigurationsdaten und zum Freischalten von iFeatures	
	SCALANCE CLP 2GB W700 AP iFeatures	6GK5907-8UA00-0AA0
	SCALANCE CLP 2GB W700 Client iFeatures	6GK5907-4UA00-0AA0

2.8 PRESET-PLUG

CLP mit Preset-Funktion (PRESET-PLUG)

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

Hinweis

Konfigurationen mit DHCP verwenden

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

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

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

Hinweis

Auf Werkseinstellungen zurücksetzen und Neustart mit gestecktem PRESET-PLUG

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

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

Nähere Informationen zur Erstellung und Benutzung eine PRESET-PLUG finden Sie in Kapitel Gerätekonfiguration mit PRESET-PLUG (Seite 366).

2.9 Power over Ethernet (PoE)

Allgemeines

Power over Ethernet (PoE) ist ein Stromversorgungsverfahren für Netzkomponenten entsprechend IEEE bei 802.3af bzw. 802.3at.

Bei PoE erfolgt die Spannungs- und Datenübertragung zusammen über die verwendeten Ethernet-Leitungen, die die einzelnen Netzkomponenten verbinden. Somit werden auf eine

zusätzliche Energieleitung verzichtet und Investitions- und Wartungskosten gespart. PoE kann bei allen Netzwerkkomponenten eingesetzt werden, die wenig Leistung (max. 12,95 Watt) verbrauchen.

Welche Ethernet-Anschlüsse eines Geräts PoE-fähig sind, entnehmen Sie der Betriebsanleitung des betreffenden Geräts.

Für die Stromversorgung verwendete Leitungen

- **Variante 1 (Redundante Adern)**
  Bei Fast-Ethernet sind die Adernpaare 1, 2 und 3, 6 für die Datenübertragung zuständig. Die Adernpaare 4, 5 und 7, 8 werden in diesem Fall für die Spannungsversorgung verwendet. Sind nur vier Adern vorhanden, wird die Spannung auf die Adern 1,2 und 3,6 aufmoduliert (siehe Variante 2) Diese Alternative eignet sich für eine Datenübertragungsrate von 10/100Mbit/s. Diese Art der Spannungsversorgung ist für 1Gbit/s nicht geeignet, da bei Gigabit alle 8 Adern für die Datenübertragung belegt sind.
- **Variante 2 (Phantomspeisung)**
  Die Spannungsversorgung erfolgt bei Phantomspeisung über die Adernpaare, über die auch die Datenübertragung erfolgt d. h. die Spannung wird auf die Datenleitung aufmoduliert. Bei Gigabit werden entsprechend IEEE 802.3at alle acht Adern der Ethernet-Leitung für die Datenübertragung und Spannungsversorgung verwendet. Bei 10/100 MBit/s werden entsprechend 802.3af vier Adern der Ethernet-Leitung für die Datenübertragung und Spannungsversorgung verwendet,

Bei PoE gibt es Energieerzeuger (Power Source Equipment, PSE) und Energieverbraucher (Power Devices, PD).

Ob ein Gerät (Energieverbraucher) Variante 1 und Variante 2 oder nur Variante 2 unterstützt, entnehmen Sie der Betriebsanleitung des betreffenden Geräts.

Ein Energieerzeuger (PSE) kann den Energieverbraucher (PD) entweder über:

- Variante 1 oder
- Variante 2 oder
- Variante 1 und Variante 2 versorgen.

Endspan

Bei Endspan erfolgt die Stromversorgung über einen Switch, der ein Gerät über Ethernetkabel erreicht. Der Switch muss PoE-fähig sein, z. B. ein SCALANCE X108PoE, SCALANCE X308-2M POE, SCALANCE XR552-12M.

Midspan

Midspan wird dann eingesetzt, wenn der Switch nicht PoE-fähig ist. Der Strom wird über ein zusätzliches Gerät zwischen dem Switch und dem Endgerät eingespeist. In diesem Fall kann nur eine Datenübertragungsrate von 10/100Mbit/s erreicht werden, weil die Stromversorgung über redundante Adern erfolgt.

Als Schnittstelle für die Stromeinspeisung kann auch ein Power Insert von Siemens verwendet werden. Da Power Insert eine Spannungsversorgung von DC 24V unterstützt, ist es nicht

802.3af bzw. IEEE 802.3at konform. Beim Einsatz von Power Insert sind folgende Einschränkungen zu beachten:

⚠ WARNUNG

Betreiben Sie das Power Insert nur unter folgenden Bedingungen:

- an Kleinspannungen SELV, PELV nach IEC 60364-4-41
- in USA/CAN an Stromversorgungen nach NEC class 2
- in USA/CAN muss die Verkabelung die Anforderungen des NEC/CEC erfüllen
- Strombelastung maximal 0,5 A.

Leitungslängen

Tabelle 2-1 Zulässige Leitungslängen (Kupferleitung - Gigabit-Ethernet)

Leitungstyp	Zusatz	Zulässige Leitungslänge
IE FC TP Standard Cable GP 4x2 (AWG 24)	mit IE FC M12 Plug PRO 4x2 (X-kodiert)	0 ... 90 m
IE FC TP Flexible Cable GP 4x2 (AWG24)	mit IE FC M12 Plug PRO 4x2 (X-kodiert)	0 ... 70 m
IE TP Train Cable GP 4x2 (AWG 24)	mit IE FC M12 Plug PRO 4x2 (X-kodiert)	0 ... 100 m

Tabelle 2-2 Konfektionierung

PIN	Farbe der Ader CAT5	Farbe der Ader CAT6a	Verwendung	
			Speisung über ungenutzte Adern (nur 10/100Mbit)	Phantomspeisung
1	Gelb	Grün/Weiß	Daten	Daten/Spannung
2	Orange	Grün	Daten	Daten/Spannung
3	Weiß	Orange/Weiß	Daten	Daten/Spannung
6	Blau	Orange	Daten	Daten/Spannung
4		Blau	Spannung	unbenutzt bei 10/100Mbit
5		Blau/Weiß	Spannung	unbenutzt bei 10/100Mbit
7		Braun/Weiß	Spannung	unbenutzt bei 10/100Mbit
8		Braun	Spannung	unbenutzt bei 10/100Mbit

Leuchtdiodenanzeige für PoE am SCALANCE W1700-Gerät

Wenn das SCALANCE W1700-Gerät über PoE gespeist wird, leuchtet die grüne LED "PoE" am SCALANCE W1700-Gerät.

Security-Empfehlungen

3

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

Allgemein

- Prüfen Sie das Gerät regelmäßig, um sicherzustellen, dass diese Empfehlungen und/oder andere interne Sicherheitsrichtlinien eingehalten werden.
- Bewerten Sie Ihre Anlage ganzheitlich im Hinblick auf Sicherheit. Nutzen Sie ein Zellenschutzkonzept mit entsprechenden Produkten (https://www.siemens.com/industrialsecurity).
- Wenn das interne und externe Netzwerk entkoppelt sind, kann ein Angreifer nicht auf interne Daten zugreifen. Betreiben Sie das Gerät daher nur innerhalb eines geschützten Netzwerkbereichs.
- Für den Betrieb von unsicherer Infrastruktur wird keine Produkthaftung übernommen.
- Nutzen Sie VPN, um die Kommunikation von und zu den Geräten zu verschlüsseln und zu authentifizieren.
- Nutzen Sie für die Datenübertragung über ein unsicheres Netzwerk einen verschlüsselten VPN-Tunnel (IPsec, OpenVPN).
- Trennen Sie Verbindungen ordnungsgemäß (WBM, Telnet, SSH usw.).
- Prüfen Sie die Benutzerdokumentation anderer Siemens-Produkte, die zusammen mit dem Gerät verwendet werden, auf weitere Sicherheitsempfehlungen.
- Sorgen Sie mit Hilfe des Remote-Logging dafür, dass die Systemprotokolle an einen zentralen Logging-Server weitergeleitet werden. Achten Sie darauf, dass der Server sich innerhalb des geschützten Netzwerks befindet, und schauen Sie regelmäßig in den Protokollen nach, ob potenzielle Sicherheitsverletzungen oder Schwachstellen vorliegen.

WLAN

- Es wird empfohlen eine redundante Abdeckung für WLAN Clients zu gewährleisten.
- Weitere Informationen zu Datensicherheit und -verschlüsselung bei SCALANCE W finden Sie in SCALANCE W: Grundlagen zum Aufbau eines Industrial Wireless LAN (https://support.industry.siemens.com/cs/ww/de/view/22681042)

Authentifizierung

Hinweis

Zugänglichkeitsrisiko - Gefahr des Datenverlusts

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

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

Zertifikate und Schlüssel

- Im Gerät ist ein voreingestelltes SSL/TLS (RSA)-Zertifikat mit Schlüssellänge 4096 Bit vorhanden. Ersetzen Sie dieses Zertifikat durch ein selbst erstelltes höherwertiges Zertifikat mit Schlüssel. Verwenden Sie ein Zertifikat, das entweder durch eine zuverlässige externe oder interne Zertifizierungsstelle signiert ist. Sie können das Zertifikat über das WBM ("System > Laden und Speichern") installieren.
- Verwenden Sie Zertifikate mit einer Schlüssellänge von 4096 Bit.

- Nutzen Sie eine Zertifizierungsstelle inklusive Schlüsselwiderruf und -verwaltung, um die Zertifikate zu signieren.
- Stellen Sie sicher, dass benutzerdefinierte private Schlüssel geschützt und unzugänglich für unbefugte Personen sind.
- Ändern Sie bei Verdacht auf eine Sicherheitsverletzung sofort alle Zertifikate und Schlüssel.
- Verwenden Sie passwortgeschützte Zertifikate im Format "PKCS #12".
- Verifizieren Sie Zertifikate anhand des Fingerprints auf Server- und Clientseite, um "Man-in-the-middle"-Angriffe zu verhindern. Verwenden Sie hierzu einen zweiten, sicheren Übertragungsweg.
- Bevor Sie das Gerät zur Reparatur an Siemens zurückschicken, ersetzen Sie die aktuellen Zertifikate und Schlüssel durch temporäre Wegwerfzertifikate und -schlüssel, die bei der Rückkehr des Geräts zerstört werden können.

Physischer/ Remote-Zugriff

- Betreiben Sie die Geräte nur in einem geschützten Netzwerkbereich. Angreifer können von Außen nicht auf interne Daten zugreifen, wenn das interne und externe Netzwerk voneinander getrennt sind.
- Beschränken Sie den physischen Zugang auf das Gerät ausschließlich auf vertrauenswürdiges Personal.
  Die Speicherkarte bzw. der PLUG (C-PLUG, KEY-PLUG, CLP) enthalten sensible Daten, wie Zertifikate und Schlüssel, die ausgelesen und verändert werden können. Ein Angreifer, der im Besitz der Wechselmedien des Geräts ist, könnte kritische Informationen wie Zertifikate, Schlüssel usw. extrahieren oder die Medien neu programmieren.
- Sperren Sie ungenutzte physische Ports auf dem Gerät. Ungenutzte Ports können verwendet werden, um unerlaubt auf die Anlage zuzugreifen.
- Verwenden Sie für die Kommunikation über nicht sichere Netzwerke zusätzliche Geräte mit VPN-Funktionalität, um die Kommunikation zu verschlüsseln und zu authentifizieren.
- Wenn Sie eine sichere Verbindung zu einem Server (beispielsweise für ein sicheres Upgrade) herstellen, achten Sie darauf, dass serverseitig starke Verschlüsselungsverfahren und Protokolle konfiguriert sind.
- Beenden Sie Managementverbindungen (z.B. HTTP, HTTPS, SSH) ordnungsgemäß.
- Stellen Sie sicher, dass das Gerät vollständig abgeschaltet wurde, bevor Sie es aus dem Betrieb nehmen. Für weitere Informationen siehe "Außerbetriebnahme (Seite 12)".
- Es wird empfohlen einen nicht verwendeten PLUG zu formatieren.

Hardware/ Software

- Verwenden Sie, wann immer möglich, VLANs als Schutz vor Denial-of-Service (DoS)-Angriffen und vor unbefugtem Zugriff.
- Beschränken Sie den Zugriff auf das Gerät durch Firewall-Regeln oder Regeln in einer Zugriffsliste (ACL – Access Control List).

- Ausgewählte Dienste sind in der Firmware standardmäßig aktiviert. Es wird empfohlen, nur die für Ihre Installation unbedingt erforderlichen Dienste zu aktivieren.
  Für weitere Informationen zu verfügbaren Diensten siehe "Liste verfügbarer Dienste (Seite 36)".
- Verwenden Sie die neueste mit dem Produkt kompatible Webbrowser-Version, um sicherzustellen, dass die sichersten verfügbaren Verschlüsselungsverfahren eingesetzt werden. Außerdem ist in den neuesten Webbrowser-Versionen von Mozilla Firefox, Google Chrome und Microsoft Edge die 1/n-1-Datensatzaufteilung aktiviert, wodurch das Risiko von Angriffen wie SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (z. B. BEAST) verringert wird.
- Stellen Sie sicher, dass die neueste Firmware-Version einschließlich aller sicherheitsrelevanten Patches installiert ist.
  Aktuelle Informationen zu Sicherheits-Patches für Siemens-Produkte finden Sie auf der Website Industrial Security (https://www.siemens.com/industrialsecurity) oder ProductCERT-Sicherheitshinweise (https://www.siemens.com/cert/de/cert-security-advisories.htm). Updates zu den Produkt-Sicherheitshinweisen von Siemens erhalten Sie, indem Sie sich beim RSS-Feed auf der Webseite der ProductCERT-Sicherheitshinweise anmelden oder
  @ProductCert auf Twitter folgen.
- Aktivieren Sie nur die Dienste, die auf dem Gerät verwendet werden, einschließlich physischer Ports. Freie physische Ports können potenziell dazu verwendet werden, Zugriff auf das Netzwerk hinter dem Gerät zu erlangen.
- Für optimale Sicherheit verwenden Sie die Authentifizierungs- und Verschlüsselungsmechanismen von SNMPv3, wann immer möglich, und nutzen starke Passwörter.
- Konfigurationsdateien können vom Gerät heruntergeladen werden. Stellen Sie sicher, dass die Konfigurationsdateien angemessen geschützt sind. Möglichkeiten hierzu sind beispielsweise, die Dateien digital zu signieren und zu verschlüsseln, sie an einem sicheren Ort zu speichern oder Konfigurationsdateien ausschließlich über sichere Kommunikationskanäle zu übertragen.
  Konfigurationsdateien können beim Download durch ein Passwort geschützt werden. Passwörter geben Sie auf der WBM-Seite "System > Laden & Speichern > Passwörter (Seite 185)" ein.
- Bei Verwendung von SNMP (Simple Network Management Protocol):
  - Konfigurieren Sie SNMP so, dass bei Authentifizierungsfehlern eine Benachrichtigung erzeugt wird.
    Für weitere Informationen siehe WBM "System > SNMP > Benachrichtigungen (Seite 208)".
  - Stellen Sie sicher, dass die Standard-Community-Strings in eindeutige Werte geändert werden.
  - Verwenden Sie SNMPv3, wann immer möglich. SNMPv1 und SNMPv2c gelten als unsicher und sollten nur bei absoluter Notwendigkeit verwendet werden.
  - Verhindern Sie nach Möglichkeit vor allem den Schreibzugriff.

- Nutzen Sie Security-Funktionen wie z. B. Adressumsetzung mit NAT (Network Address Translation) oder NAPT (Network Address Port Translation), um Empfangsports vor Zugriffen von Dritten zu schützen.
- Verwenden Sie WPA2/ WPA2-PSK mit AES, um das WLAN zu schützen. Weitere Informationen finden Sie im Projektierungshandbuch Web Based Management "Menü Security (Seite 337)".

Sichere/ nicht sichere Protokolle

- Verwenden Sie sichere Protokolle, wenn der Zugriff auf das Gerät nicht durch physische Schutzmaßnahmen verhindert wird.
- Deaktivieren oder beschränken Sie die Verwendung nicht sicherer Protokolle. Während einige Protokolle sicher sind (z. B. HTTPS, SSH, 802.1X usw.), wurden andere nicht zu dem Zweck entwickelt, Anwendungen abzusichern (z.B. SNMPv1/v2c, RSTP usw.).
  Treffen Sie daher geeignete Sicherheitsvorkehrungen gegen nicht sichere Protokolle, um unbefugten Zugriff auf das Gerät/Netzwerk zu verhindern. Setzen Sie unsichere Protokolle auf dem Gerät über eine gesicherte Verbindung (z. B. SINEMA RC) ein.
- Wenn nicht sichere Protokolle und Dienste erforderlich sind, stellen Sie sicher, dass das Gerät in einem geschützten Netzwerkbereich betrieben wird.
- Prüfen Sie die Notwendigkeit der Nutzung folgender Protokolle und Dienste:
  - Nicht authentifizierte und unverschlüsselte Ports
  - LLDP
  - Syslog
  - DHCP-Optionen 66/67
  - TFTP
  - Telnet
  - HTTP
  - SNMP v1/2c
  - Syslog
  - SNTP
- Die folgenden Protokolle bieten sichere Alternativen:
  - SNMPv1/v2c → SNMPv3
    Prüfen Sie die Notwendigkeit der Nutzung von SNMPv1/v2c. SNMPv1/v2c ist als unsicher eingestuft. Nutzen Sie die Möglichkeit den Schreibzugriff zu unterbinden. Das Produkt bietet entsprechende Einstellmöglichkeiten.
    Wenn SNMP aktiviert ist, ändern Sie die Community-Namen. Wenn kein uneingeschränkter Zugriff erforderlich ist, beschränken Sie den Zugriff über SNMP. Nutzen Sie SNMPv3 in Kombination mit Passwörtern.
  - HTTP → HTTPS
  - Telnet → SSH
  - TFTP → SFTP
  - Syslog Client → Syslog Client TLS

- Beschränken Sie mit einer Firewall die nach außen angebotenen Dienste und Protokolle auf das erforderliche Mindestmaß.
- Aktivieren Sie für die DCP-Funktion nach der Inbetriebnahme den Modus "Schreibgeschützt".

Liste verfügbarer Dienste

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

Die Tabelle umfasst folgende Spalten:

- **Dienst**
  Die Dienste, die das Gerät unterstützt
- **Voreingestellter Portstatus**
  Das ist Status des Ports im Auslieferungszustand (Werkseinstellung).
- **Port / Dienst konfigurierbar**
  Gibt an, ob die Port-Nummer oder der Dienst über das WBM / CLI konfigurierbar sind.
- **Authentifizierung**
  Gibt an, ob eine Authentifizierung des Kommunikationspartners stattfindet.
  Bei Optional ist die Authentifizierung bei Bedarf konfigurierbar.
- **Verschlüsselung**
  Gibt an, ob die Übertragung verschlüsselt wird.
  Bei Optional ist die Verschlüsselung bei Bedarf konfigurierbar.

Dienst	Protokoll/ Port-nummer	Voreingestell-ter Portstatus	Konfigurierbar		Authentifizie-rung	Verschlüsselung
			Port	Dienst		
DHCP Client IPv4	UDP/68	Nur ausgehend	--	✓	--	--
DHCP Client IPv6	UDP/546	Nur ausgehend	--	✓	--	--
DHCP Server	UDP/67	Geschlossen	--	✓	--	--
DNS Client	TCP/53 UDP/53	Nur ausgehend	--	✓	--	--
EthernetIP	TCP/44818 UDP/2222 UDP/44818	Geschlossen	--	✓	--	--
HTTP	TCP/80	Offen	✓	✓	✓	--
HTTPS	TCP/443	Offen	✓	✓	✓	✓
NTP Client	UDP/123	Nur ausgehend	✓	✓	--	--
PROFINET	UDP/34964 UDP/49154 UDP/49155	Offen	--	✓	--	--
RADIUS Client	UDP/1812	Nur ausgehend	✓	✓	✓	--
Remote Capture	TCP/2002	Geschlossen	--	✓	--	--
SFTP Client	TCP/22	Geschlossen	✓	✓	✓	✓
SMTP Client	TCP/25	Geschlossen	✓	✓	--	--
SMTP Client (secure) [1)]	TCP/465	Geschlossen	✓	✓	✓	✓
SNMPv1/v2c	UDP/161	Offen	✓	✓	--	--

Dienst	Protokoll/ Port-nummer	Voreingestell-ter Portstatus	Konfigurierbar		Authentifizie-rung	Verschlüsselung
			Port	Dienst		
SNMPv3	UDP/161	Offen	✓	✓	Optional	Optional
SNMP Traps	UDP/162	Nur ausgehend	--	✓	--	--
SNTP Client	UDP/123	Nur ausgehend	✓	✓	--	--
SSH	TCP/22	Offen	✓	✓	✓	✓
Syslog Client	UDP/514	Geschlossen	✓	✓	--	--
Syslog (secure) Client	TCP/6514	Geschlossen	✓	✓	--	✓
Telnet	TCP/23	Geschlossen [1] / Offen [2]	✓	✓	✓	--
TFTP Client	UDP/69	Nur ausgehend	✓	✓	--	--

1) Nur bei SCALANCE W1700ac

2) Nur bei SCALANCE W700n

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

Die Tabelle umfasst folgende Spalten:

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

Layer 2-Dienst	Voreingestellter Status	Dienst konfigu-rierbar
DCP	Offen	✓
LLDP	Offen	✓
RSTP	Offen	✓
iPRP	Offen	✓
MSTP	Geschlossen	✓
SIMATIC NET TIME	Geschlossen	✓

Technische Grundlagen

4

4.1 Mengengerüst

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

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

	Konfigurierbare Funktion		**Maximale Anzahl**
System	Syslog-Server		3
	DNS-Server	manual (IPv4/IPv6)	3
		learned (IPv4/IPv6)	2
		insgesamt	7
	SMTP-Server		2
	SNMPv1-Trap-Empfänger		10
	SNMP-Anfragen		50
	SNTP-Server		2
	NTP-Server		1
	DHCP-Pools		1
	IPv4-Adressen, die der DHCP-Server verwaltet (dynamisch + statisch)		100
	DHCP statische Zuordnungen pro DHCP-Pool		20
	DHCP-Optionen		20
	Backup der Konfiguration		31
Interfaces	Force destination addresses for roaming		10
	Connected clients per VAP interface		• 255 with security "Open System" • 128 with Security "WPA / WPA2 / Shared Key"
Layer 2	Virtual LANs (port-based, including VLAN 1)		24
	Multiple Spanning Tree instances		16
Layer 3	IP interface		2 1 subnet per IP interface
	DHCP client		1
Security	IP addresses from RADIUS servers		• AAA: 4 • WLAN: 2
	Management ACLs (access rules for management)		10
	User roles		32 (incl. the predefined roles)
	User groups		32
	Users		30 (incl. the predefined users)

4.2 Schnittstellen und Systemfunktionen

Verfügbarkeit der Schnittstellen

Die nachfolgende Tabelle zeigt die Verfügbarkeit der physischen und der logischen Schnittstellen an. Beachten Sie, dass in dieser Tabelle alle Schnittstellen aufgelistet sind. Abhängig von der Systemfunktion stehen Ihnen manche Schnittstellen nicht zur Verfügung. Auf den WBM-Seiten können Sie nur die verfügbaren Schnittstellen auswählen.

Technische Änderungen sind vorbehalten.

	Client	**Access Point**	
	W1748-1 M12	**W1788-1 M12**	**W1788-2 M12** **W1788-2 M12 EEC** **W1788-2IA M12**
Funkschnittstelle (WLAN)	WLAN 1	WLAN 1	WLAN 1 WLAN 2
LAN-Schnittstelle	P1 LAN P2 LAN PoE	P1 LAN P2 LAN PoE	P1 LAN P2 LAN PoE
VAP-Schnittstelle	-	VAP 1.Y Y = 1 ... 8	VAP X.Y X = 1 ... 2 Y = 1 ... 8
WDS-Schnittstelle	-	WDS 1.Y Y = 1 ... 8	WDS X.Y X = 1 ... 2 Y = 1 ... 8
VLAN	24	24	24

Verfügbarkeit der Systemfunktionen

Die nachfolgende Tabelle zeigt die Verfügbarkeit der Systemfunktionen auf den Geräten.

Technische Änderungen sind vorbehalten.

			Access Points-Modus	**Client-Geräte** **Access Points im Client-Modus**
Informationen	**Security**	Inter AP Blocking	✓	-
	WLAN	Übersicht AP	✓	-
		Client-Liste	✓	-
		WDS-Liste	✓	-
		Überlappung AP	✓	-
		Roaming erzwingen	✓	✓
		Übersicht Client	-	✓
		Verfügbare APs	-	✓
		IP-Zuordnung	-	✓
	WLAN-Statistiken	Fehler	✓	✓
		Management gesendet	✓	✓
		Management empfangen	✓	✓
		Gesendete Daten	✓	✓
		Empfangene Daten	✓	✓
	WLAN iFeatures	iPRP	✓	-
System		PROFINET	✓	-✓
		EtherNet/IP	✓	✓
	DHCP	DHCP-Client	✓	✓
		DHCP-Server	✓	-
		DHCP-Optionen	✓	-
		Statische Zuordnung	✓	-
Schnittstellen	**WLAN**	Basic	✓	-✓
		Erweiterungen	✓	✓
		Antennen	✓	✓
		Zugelassene Kanäle	✓	✓
		802.11n/ac	✓	✓
		AP	✓	-
		AP WDS	✓	-
		Client 802.11a/b/g-Datenraten	-	✓
		Client 802.11n-Datenraten	-	✓
		Roaming erzwingen	✓	✓
		Signalrekorder	-	✓
Layer 3 (IPv4 / IPv6)		Subnetze	-	✓
		Statische Route	-	✓

			Access Points-Modus	Client-Geräte Access Points im Client-Modus
Security	**WLAN**	Basic	✓	✓
		AP-Kommunikation	✓	-
		AP RADIUS-Authenticator	✓	-
		Client RADIUS-Supplicant	-	✓
		802.11r	✓	-
		Schlüssel	✓	✓
	Inter AP Blocking	Basic	✓	-
		Zugelassene Adressen	✓	-
iFeatures	**iPRP** [1]		✓	✓

[1] Nur mit CLP iFeatures, siehe Kapitel "Configuration License PLUG (CLP)".

Unterstützung von IPv6

Folgende Systemfunktionen unterstützen keine IPv6-Adressen:

- Inter AP Blocking
- Roaming erzwingen

4.3 EtherNet/IP

EtherNet/IP

EtherNet/IP (Ethernet/Industrial Protocol) ist ein offener Industriestandard für industrielles Echtzeit-Ethernet, basierend auf TCP/IP und UDP/IP. Mit EtherNet/IP wird Ethernet um das Common Industrial Protocol (CIP) auf der Anwendungsschicht erweitert. In EtherNet/IP werden die unteren Schichten des OSI-Referenzmodells von Ethernet mit den Übertragungs-, Vermittlungs-, Netzwerk- und Transportfunktionen übernommen.

EtherNet/IP konfigurieren Sie unter "System > EtherNet/IP (Seite 235)".

Common Industrial Protocol

Das Common Industrial Protocol (CIP) ist ein Anwendungsprotokoll der Automatisierung, das den Übergang der Feldbusse in industrielles Ethernet und in IP-Netze unterstützt. Dieses Industrieprotokoll benutzen Feldbusse/Industrienetzwerke wie DeviceNet, ControlNet und EtherNet/IP in der Anwendungsschicht als Schnittstelle zwischen der deterministischen Feldbus-Welt und der Automatisierungsapplikation (Steuerung, E/A, HMI, OPC, ...). Das CIP liegt oberhalb der Transportschicht und erweitert die reinen Transportdienste um Kommunikationsdienste für die Automatisierungstechnik. Dazu gehören Dienste für den zyklischen, den zeitkritischen und den ereignisgesteuerten Datenverkehr. CIP unterscheidet zwischen den zeitkritischen E/A-Nachrichten (implicit messages) und individuellen Frage/Antwort-Telegrammen zur Konfiguration und Datenerfassung (explicit messages). CIP ist objekt-orientiert; alle von außen "sichtbaren" Daten sind in Form von Objekten zugänglich. CIP hat eine gemeinsame Konfigurationsgrundlage: EDS (Electronic Data Sheet).

Electronic Data Sheet

Electronic Data Sheet (EDS) ist ein elektronisches Datenblatt zur Beschreibung von Geräten.

Das für den EtherNet/IP-Betrieb benötigte EDS finden Sie unter "System > Laden & Speichern (Seite 170)".

4.4 PROFINET

PROFINET

PROFINET ist ein offener Ethernet-Standard (IEC 61158/61784) für die industrielle Automatisierung basierend auf Industrial Ethernet. PROFINET nutzt existierende IT-Standards und ermöglicht eine durchgängige Kommunikation von der Feldebene bis in die Leitebene sowie ein anlagenweites Engineering. Weitere Eigenschaften von PROFINET sind:

- Nutzung von TCP/IP
- Automatisierung von Applikationen mit Echtzeit-Bedarf
  - Real-Time (RT)-Kommunikation
  - Isochronous Real-Time (IRT)-Kommunikation
- Nahtlose Integration von Feldbus-Systemen

PROFINET konfigurieren Sie unter "System > PROFINET (Seite 234)".

PROFINET IO

Im Rahmen von PROFINET ist PROFINET IO ein Kommunikationskonzept für die Realisierung modularer, dezentraler Applikationen. Die Umsetzung von PROFINET IO wird durch den PROFINET-Standard für Automatisierungsgeräte (IEC 61158-x-10) realisiert.

4.5 VLAN

Netzwerkdefinition unabhängig von der räumlichen Lage der Teilnehmer

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

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

Für die Kennung, welcher Frame welchem VLAN zugeordnet ist, wird der Frame um 4 Byte (VLAN-Tagging) erweitert. Diese Erweiterung enthält neben der VLAN-ID auch Prioritätsinformationen.

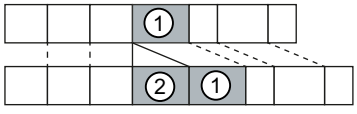
Möglichkeiten der VLAN-Zuordnung

Es gibt verschiedene Möglichkeiten der Zuordnung zu VLANs:

- Port-basiertes VLAN
  Jedem Port eines Geräts wird eine VLAN ID zugewiesen. Portbasiertes VLAN konfigurieren Sie unter "Layer 2 > VLAN (Seite 290)".
- Protokoll-basiertes VLAN
  Jedem Port eines Geräts wird eine Protokollgruppe zugewiesen.
- Subnetz-basiertes VLAN
  Der IP-Adresse des Geräts wird eine VLAN ID zugewiesen.

Doppel getaggter Frame (Q-in-Q)

Es gibt Geräte z. B. SCALANCE XR500, die die Funktion Q-in-Q unterstützen. Bei der Funktion Q-in-Q wird der eingehende Datenverkehr behandelt, als wäre er ungetagged. Bei bereits getaggten Frames ① bedeutet dies, dass sie um ein zweites VLAN-Tag erweitert werden, das äußere VLAN-Tag ②.



Wenn ein SCALANCE W-Gerät einen doppelt getaggten Frame erhält, verwendet es die VLAN-ID aus dem äußeren VLAN-Tag ② und die Prioritätsangabe aus dem inneren VLAN-Tag ①. Der Frame wird dann an das entsprechende VLAN weitergeleitet.

4.6 SNMP

Einleitung

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

Aufgaben von SNMP:

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

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

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

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

Standardwerte der Community-Strings:

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

Hinweis

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

Weitere einfache Schutzmechanismen auf Geräteebene:

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

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

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

Die Management-Station sendet Datenpakete folgenden Typs:

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

Der SNMP-Agent sendet Datenpakete folgenden Typs:

- RESPONSE
  Der SNMP-Agent sendet die vom Manager angeforderten Daten zurück.
- TRAP
  Wenn ein bestimmtes Ereignis eintritt, sendet der SNMP-Agent eigenständig Traps.

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

SNMPv3

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

SNMPv3 unterstützt:

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

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

Das SNMPv3-Protokoll verwendet gemäß des Standards eine eindeutige SNMP-Engine-ID als internen Bezeichner für einen SNMP-Agenten. Diese ID muss im Netzwerk eindeutig sein. Sie wird verwendet, um die Zugangsdaten von SNMPv3-Benutzern zu authentifizieren und zu verschlüsseln.

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

Einschränkung bei der Verwendung der Funktion

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

Kompatibilität mit Vorgängerprodukten

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

4.7 Spanning Tree

Vermeidung von Schleifenbildung

Das Spanning Tree-Verfahren ermittelt physikalisch redundante Netzwerkstrukturen und verhindert Schleifenbildung durch Abschalten redundanter Wege. Dazu wertet es die Entfernung, die Leistungsfähigkeit einer Verbindung oder auch Benutzervorgaben aus. Der Datenverkehr erfolgt dann ausschließlich auf den verbleibenden Verbindungswegen.

Wenn der bevorzugte Datenweg ausfällt, sucht der Spanning Tree-Algorithmus den effizientesten Weg, der mit den verbliebenen Netzteilnehmern möglich ist.

Root Bridge und Bridge Priority

Die Ermittlung der effizientesten Verbindung erfolgt immer in Bezug auf die so genannte "Root Bridge", eine Netzkomponente, die als Wurzelelement einer baumartigen Netzstruktur angesehen wird. Mit dem Parameter "Bridge Priority" können Sie die Wahl der Root Bridge beeinflussen. Der Rechner mit dem geringsten Wert für diesen Parameter wird zwangsläufig Root-Bridge. Wenn zwei Rechner den gleichen Prioritätswert haben, wird derjenige Rechner Root-Bridge, der die niedrigere MAC-Adresse hat.

Verhalten bei Veränderungen der Netztopologie

Wenn Teilnehmer zu einem Netz hinzukommen oder wegfallen hat das möglicherweise Auswirkungen auf die optimale Wegewahl der Datenpakete. Um diese Änderungen zu berücksichtigen, versendet die Root Bridge in regelmäßigen Abständen Konfigurationsmeldungen (BPDUs). Den Zeitabstand zwischen zwei Konfigurationsmeldungen können Sie mit dem Parameter "Hello Time" einstellen.

Aktualität der Konfigurationsinformation

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

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

4.7.1 RSTP, MSTP, CIST

Rapid Spanning Tree Protocol (RSTP)

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

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

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

Multiple Spanning Tree Protocol (MSTP)

Das Multiple Spanning Tree Protocol (MSTP) ist eine Weiterentwicklung des Rapid Spanning Tree Protocols. Es bietet u. a. die Möglichkeit, mehrere RSTP-Instanzen innerhalb verschiedener VLANs oder VLAN-Gruppen zu betreiben und so z. B. Pfade, die das einfache Rapid Spanning Tree Protocol für den Datenverkehr global sperren würde, innerhalb einzelner VLANs verfügbar zu machen.

Common and Internal Spanning Tree (CIST)

CIST bezeichnet die intern vom Switch verwendete Instanz, die im Prinzip einer internen RSTP-Instanz gleicht.

4.8 Benutzerverwaltung

Übersicht zur Benutzerverwaltung

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

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

Lokale Anmeldung

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

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

Anmeldung über einen externen RADIUS-Server

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

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

RADIUS-Autorisierungsmodus "Standard"

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

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

RADIUS-Autorisierungsmodus "Herstellerspezifisch"

Voraussetzung

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

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

Vorgehen

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

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

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

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

4.9 iFeatures

4.9.1 iPRP

Das "Parallel Redundancy Protocol" (PRP) ist ein Redundanzprotokoll für kabelgebundene Netzwerke. Es ist im Teil 3 des IEC 62439 Standards definiert.

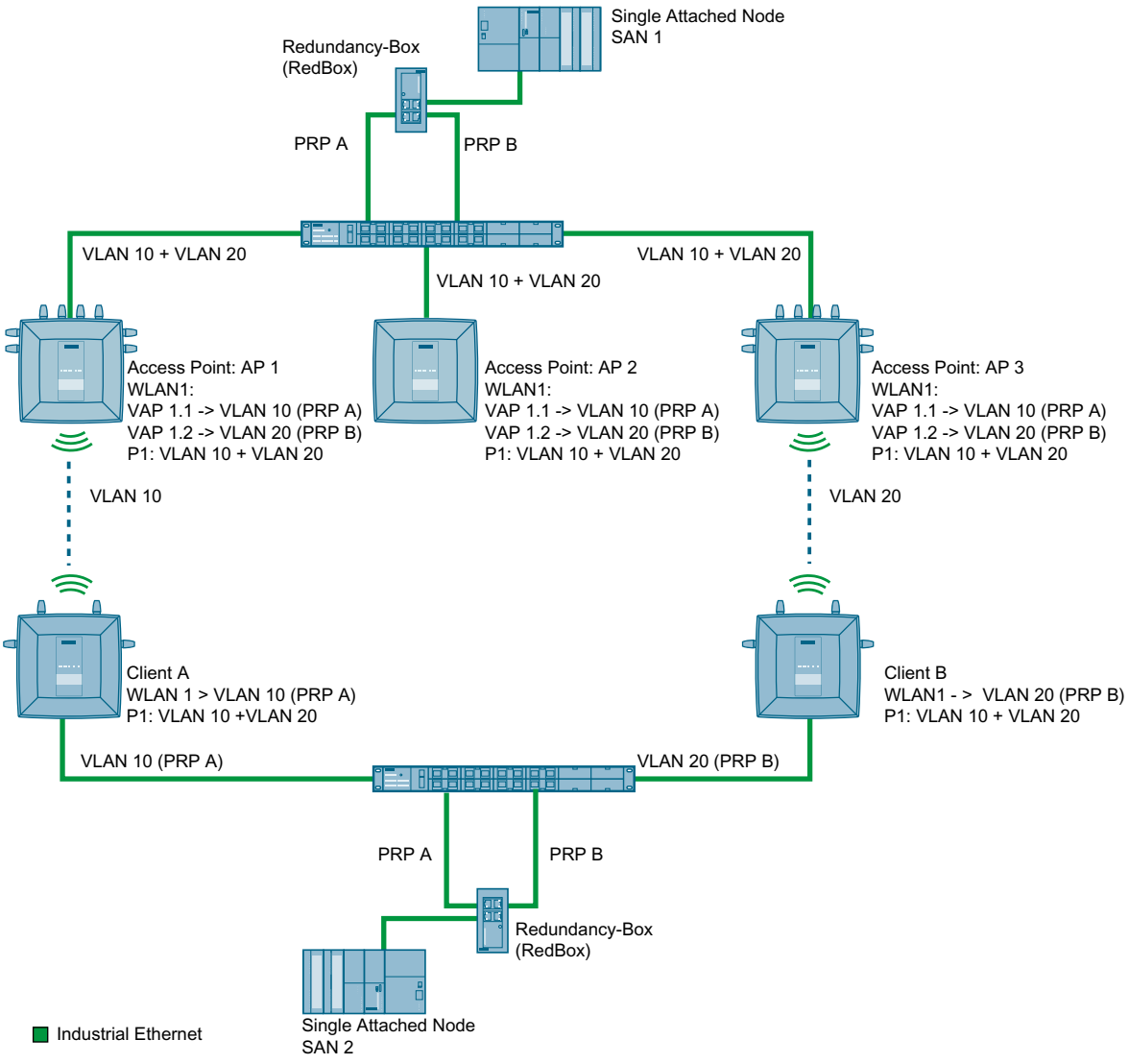
Mit "industrial Parallel Redundancy Protocol" (iPRP) kann die PRP-Technologie in drahtlosen Netzwerken eingesetzt werden. Damit wird die Verfügbarkeit der drahtlosen Kommunikation verbessert.

Funktionsprinzip

Ein PRP-Netzwerk besteht aus zwei völlig unabhängigen Netzwerken. Wenn eines der Netzwerke gestört ist, werden die Frames ohne Unterbrechung/Rekonfiguration über das parallele redundante Netzwerk gesendet. Dazu werden die Ethernet-Frames verdoppelt und über beide Netzwerke an den Empfänger übertragen. PRP-fähige Geräte haben jeweils mindestens zwei voneinander getrennte Ethernet-Schnittstellen, die an jeweils unabhängige Netzwerke angeschlossen sind.

Bei nicht PRP-fähigen Geräten wird eine Redundancy-Box (RedBox) vorgeschaltet. Diese schafft den Zugang für so genannte Single Attached Nodes (SAN) zu den PRP-Netzen. Die RedBox verdoppelt jeden zu sendenden Ethernet-Frame und fügt einen PRP-Trailer an den Frame, der u.a. eine Sequenznummer enthält. Die RedBox sendet gleichzeitig jeweils eine Kopie des Frames in das PRP A und PRP B Netzwerk. Auf der Empfängerseite wird von der RedBox das doppelte Frame verworfen. Dafür erfordert die RedBox bestimmte Übertragungszeiten, die für Ethernet Netzwerke ausgelegt sind. Aus diesem Grund kommt es bei der Verwendung von PRP in WLAN Netzen zu doppelten und verzögerten Frames.

Durch iPRP wird diese Problematik aufgelöst und die Verwendung von PRP in WLAN mit SCALANCE W-Geräten ermöglicht



Die Access Points (AP 1, AP 2 und AP 3) und die RedBox auf der AP Seite sind über einen Switch miteinander verbunden. PRP Netzwerk A und B sind über VLANs voneinander getrennt.

Sendet SAN1 einen Frame an SAN2, wird der Frame von der RedBox auf der AP-Seite dupliziert und die beiden redundanten Frames werden über den Switch an die Access Points übertragen. Über die zwei unterschiedlichen Funkstrecken werden die redundanten PRP-Frames an die RedBox auf der Client-Seite übermittelt. Die Clients sind ebenfalls über einen Switch mit ihrer RedBox verbunden. Diese leitet den ersten ankommenden PRP-Frame weiter an SAN2 und verwirft den Zweiten.

Bei ungleichen Übertragungspfaden reduziert iPRP die Anzahl an duplizierten und out-of-order Paketen. Die verwendete Applikation / das verwendete Protokoll muss mit den verbleibenden Duplikaten und out-of-order Paketen umgehen können.

Hinweis

An den Schnittstellen der Switche zu den SCALANCE W-Geräten dürfen jeweils nur die VLANs konfiguriert werden, die auch an den VAP- bzw. WLAN-Schnittstellen der SCALANCE W-Geräte eingestellt sind.

Bei iPRP kommunizieren die redundanten Partner (hier: AP1 und AP3 bzw. Client A und Client B) über einen Switch miteinander, um zu verhindern, dass die beiden redundanten PRP-Frames mit einem zu großen Zeitunterschied bei der RedBox ankommen.

Ist zum Beispiel die Kommunikation zwischen AP1 und Client A sehr langsam, wird das langsamere Frame auf der Empfangsseite verworfen.

iPRP konfigurieren Sie unter "iFeatures > iPRP (Seite 359)".

Voraussetzung

- iPRP ist nur mit dem CLP iFeatures (Seite 25) verwendbar.
- Der Base Bridge-Modus "802.1Q VLAN Bridge" ist eingestellt.
- Die VLANs sind angelegt.
- Access Point-Modus: Die VAP-Schnittstelle ist aktiviert.
- Client-Modus: Bei MAC-Modus ist "Layer-2-Tunnel" eingestellt.
- Je nach Konfiguration können die Clients mit jedem Access Point kommunizieren.
- Das Spanning Tree Protocol ist deaktiviert.

IP-Adressen

5

5.1 IPv4 / IPv6

Was sind die wesentlichen Unterschiede?

	IPv4	IPv6
IP-Konfiguration	• DHCP-Server • Manuell	• Stateless Address Autoconfiguration (SLAAC): zustandslose Autokonfiguration über NDP (Neighbor Discovery Protocol) – Erstellt eine Link-lokale Adresse für jede Schnittstelle, die keinen Router auf dem Link benötigt. – Prüft die Einmaligkeit der Adresse auf dem Link, die keinen Router auf dem Link benötigt. – Legt fest, ob die globalen Adressen über einen zustandslosen Mechanismus, einen zustandbehafteten Mechanismus oder über beide Mechanismen bezogen werden. (Erfordert einen Router auf dem Link.) • Manuell • DHCPv6 (Zustandbehaftet)
Verfügbare IP-Adressen	32-Bit: 4, 29 * 10^9 Adressen	128-Bit: 3,4 * 10^{38} Adressen
Adressformat	Dezimal: 192.168.1.1 mit Port: 192.168.1.1:20	Hexadezimal: 2a00:ad80::0123 mit Port: [2a00:ad80::0123]:20
Loopback	127.0.0.1	::1
IP-Adressen pro Schnittstelle	5 IP-Adressen	Mehrere IP-Adressen • LLA: Eine link lokale-Adresse (automatisch gebildet) fe80::/128 pro Schnittstelle • ULA: Mehrere Unique lokal Unicast-Adressen pro Schnittstelle • GUA: Mehrere Globale Unicast-Adressen pro Schnittstelle
Header	• Checksumme • variable Länge • Fragmentierung im Header • keine Sicherheit	• Überprüfung auf höherer Schicht • fest vorgeschriebene Größe • Fragmentierung im Extension Header
Fragmentierung	Host und Router	nur Endpunkt der Kommunikation
Quality of Service	Type of Service zur Priorisierung (ToS)	Die Priorisierung wird im Header-Feld "Traffic Class" angegeben.
Telegrammarten	Broadcast, Multicast, Unicast	Multicast, Unicast, Anycast

	IPv4	**IPv6**
Identifizierung von DHCP-Clients/-Server	Client-ID: • MAC-Adresse • DHCP Client ID • System Name • PROFINET-Stationsname • IAID und DUID	DUID + IAID(s) = genau eine Schnittstelle des Hosts DUID = DHCP Unique Identifier Identifiziert Server und Clients eindeutig. IAID = Identity Association Identifier Mindestens eine pro Schnittstelle wird vom Client generiert und bleibt bei Neustart des DHCP-Clients unverändert Drei Verfahren zum Ermitteln der DUID • DUID-LLT • DUID-EN • DUID-LL
DHCP	über UDP mittels Broadcast	über UDP mittels Unicast RFC 3315, RFC 3363 **Stateful DHCPv6** Zustandsbehaftete Konfiguration bei der die IPv6-Adresse und die Konfigurationseinstellungen übermittelt werden. Dabei werden vier DHCPv6-Nachrichten zwischen Client und Server ausgetauscht: 1. SOLICIT: Gesendet durch den DHCPv6-Client, um DHCPv6-Server zu lokalisieren. 2. ADVERTISE Die verfügbaren DHCPv6-Server antworten darauf. 3. REQUEST Der DHCPv6-Client fordert eine IPv6-Adresse und die Konfigurationseinstellungen beim DHCPv6-Server an. 4. REPLY Der DHCPv6-Server sendet die IPv6-Adresse und die Konfigurationseinstellungen. Wenn Client und Server die Funktion "Rapid commit" unterstützen, wird das Verfahren auf zwei DHCPv6-Nachrichten SOLICIT und REPLY gekürzt. **Stateless DHCPv6** Beim zustandslosen DHCPv6 werden nur die Konfigurationseinstellungen übermittelt. **Präfix-Delegation** Der DHCPv6-Server delegiert das Verteilen von IPv6-Präfixen an den DHCPv6-Client. Der DHCPv6-Client wird auch als PD-Router bezeichnet.
Auflösung von IP-Adressen in Hardware-Adressen	ARP (Address Resolution Protocol)	NDP (Neighbor Discovery Protocol)

5.2 IPv4-Adresse

5.2.1 Aufbau einer IPv4-Adresse

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

Beispiel: 192.168.16.2

Die IPv4-Adresse setzt sich zusammen aus:

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

Subnetzmaske

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

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

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

Beispiel:

richtige Werte

255.255.0.0 D = 1111 1111.1111 1111.0000 0000.0000 0000 B

255.255.128.0 D = 1111 1111.1111 1111.1000 0000.0000 0000 B

255.254.0.0 D = 1111 1111.1111 1110.0000 0000.0000.0000 B

falscher Wert:

255.255.1.0 D = 1111 1111.1111 1111.0000 0001.0000 0000 B

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

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

Allgemein gilt:

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

Classless Inter-Domain Routing (CIDR)

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

Beispiel:

IPv4-Adresse 192.168.0.0 mit Subnetzmaske 255.255.255.0

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

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

Weitere Subnetze maskieren

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

Beispiel:

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

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

Ergebnis:

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

Netzübergang (Router)

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

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

5.2.2 Erstmalige Vergabe einer IPv4-Adresse

Konfigurationsmöglichkeiten

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

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

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

Hinweis

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

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

5.2.3 Adressvergabe über DHCPv4

Eigenschaften von DHCP

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

- DHCP kann sowohl während des Hochlaufs eines Geräts als auch im laufenden Betrieb eingesetzt werden.
- Die vergebene IP-Adresse bleibt nur für eine begrenzte Zeitdauer (Lease Time) gültig. Nachdem die Gültigkeitsdauer zur Hälfte abgelaufen ist, kann der DHCP-Client die vergebene IPv4-Adresse verlängern. Nach Ablauf der gesamten Zeitdauer muss der DHCP-Client eine neue IPv4-Adresse anfordern.

- Normalerweise erfolgt keine feste Adresszuordnung, d. h. wenn ein Client erneut eine IP-Adresse anfordert, erhält er in der Regel eine andere Adresse als bei der vorhergehenden Anforderung. Es ist möglich, den DHCP-Server so zu konfigurieren, dass der DHCP-Client auf seine Anfrage immer dieselbe feste Adresse zugeordnet bekommt. Über welchen Parameter der DHCP-Client für die feste Adresszuordnung identifiziert wird, wird im DHCP-Client eingestellt. Die Adresse kann über die MAC-Adresse, die DHCP Client ID, PROFINET-Gerätename oder den Gerätenamen zugeordnet werden. Den Parameter konfigurieren Sie unter "System > DHCP-Client (Seite 198)".
- Folgende DHCP-Optionen werden unterstützt:
  - DHCP-Option 3: Vergabe einer Routeradresse
  - DHCP-Option 6: Vergabe einer DNS-Serveradresse
  - DHCP-Option 66: Vergabe eines dynamischen TFTP-Servernamens
  - DHCP-Option 67: Vergabe eines dynamischen Bootfile-Namens

Hinweis

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

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

5.2.4 Adressvergabe mit SINEC PNI

Einleitung

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

SINEC PNI

- Um dem Gerät mit SINEC PNI eine IP-Adresse zuweisen zu können, muss das Gerät über Ethernet erreichbar sein.
- Sie finden SINEC PNI auf den Internetseiten des Siemens Industry Online Support unter folgendem Link: (https://support.industry.siemens.com/cs/ww/de/view/109804190)
- Beachten Sie für weitere Informationen zur Vergabe der IP-Adresse mit SINEC PNI die Online-Hilfe oder die Betriebsanleitung "Netzwerkmanagement SINEC PNI".

5.2.5 Adressvergabe über STEP 7

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

STEP 7 V5.x und früher

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

STEP 7 ab V13

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

5.3 IPv6-Adresse

5.3.1 IPv6-Begriffe

Netzknoten

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

Router

Ein Netzknoten, der IPv6-Pakete weiterleitet.

Host

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

Link

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

Nachbar

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

IPv6-Schnittstelle

Physische oder logische Schnittstelle, an der IPv6 aktiviert ist.

Path MTU

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

Path MTU Discovery

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

LLA

Link lokale-Adresse FE80::/10

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

ULA

Unique lokal-Adresse

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

GUA

Globale Unicast-Adresse

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

Schnittstellen-ID

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

EUI-64

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

Beispiel:

MAC-Adresse = AA:BB:CC:DD:EE:FF

OUI = AA:BB:CC

NIC = DD:EE:FF

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

Scope

Definiert die Reichweite der IPv6-Adresse.

5.3.2 Aufbau einer IPv6-Adresse

Adressformat IPv6-Notation

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

Beispiel:

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

Regeln/Vereinfachungen:

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

Aufbau IPv6-Adresse

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

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

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

IPv6-Präfix

Festgelegt in: RFC 4291

Das IPv6-Präfix stellt die Subnetzkennung dar.

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

Aufbau

IPv6-Adresse / Präfixlänge

Beispiel

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

Präfix: 2001:0db8:1234::/48

Schnittstelle-ID: ::1111

Eingabe und Darstellung

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

Konfigurieren mit dem Web Based Management 6

6.1 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 Client-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.

Der Vorteil dieses Funktionsprinzips ist, dass auf der Client-Seite nur ein Webbrowser erforderlich ist.

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 > Konfiguration" nur den HTTPS-Server.

Voraussetzungen

Darstellung des WBM

- Das Gerät verfügt über eine IP-Adresse
- Zwischen dem Gerät und dem Client-Gerät besteht eine Verbindung. Mit dem Windows ping-Befehl können Sie nachprüfen, ob eine Verbindung besteht.
- Der Zugriff über HTTPS ist aktiviert.
- Im Webbrowser ist JavaScript aktiviert.

- Der Webbrowser darf nicht so eingestellt sein, dass er bei jedem Zugriff auf die Seite diese neu vom Server laden soll. Die Aktualität der dynamischen Seiteninhalte wird über andere Mechanismen sichergestellt. Beim Internet Explorer finden Sie eine entsprechende Einstellmöglichkeit im Menü "Extras > Internetoptionen > Allgemein" im Abschnitt "Browserverlauf" über die Schaltfläche "Einstellungen". Aktivieren Sie bei "Neuere Versionen der gespeicherten Seite suchen" "Automatisch".
- Wenn eine Firewall eingesetzt wird, müssen die entsprechenden Ports freigeschaltet sein.
  - Für den Zugriff über HTTP: Standardport 80 oder konfigurierter Port
  - Für den Zugriff über HTTPS: Standardport 443 oder konfigurierter Port

  Die Darstellung des WBM wurde mit folgenden Desktop-Webbrowsern getestet:
  - Mozilla Firefox 91 ESR
  - Google Chrome 93
  - Microsoft Edge Chromium 93

Darstellung des WBM auf mobilen Geräten

Für mobile Geräte gelten folgende minimale Voraussetzungen:

Auflösung	Betriebssystem	Internet-Browser
960 x 640 Pixel	Android ab Version 4.2.1 iOS ab Version 6.0.2	Chrome ab Version 18 auf Android Safari ab Version 6 auf iOS

- Getestet mit folgenden Internet-Browsern für mobile Geräte:
  - Safari ab Version 8 auf iOS ab Version 8.1.3 (iPad Mini Model A1432)
  - Chrome ab Version 46 auf Android ab Version 5.0.2 (Nexus 7C Asus)
  - Firefox ab Version 35 auf Android ab Version 5.0.2

Hinweis

Seitendarstellung und Bedienung des WBM auf mobilen Geräten

Die Darstellung und Bedienung der WBM-Seiten auf mobilen Geräten können von der Darstellung und Bedienung derselben Seiten auf Desktop-Geräten abweichen. Einige Seiten liegen auch in einer für mobile Geräte optimierten Darstellung vor.

6.2 Login

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 PC besteht eine Verbindung. Mit dem ping-Befehl können Sie prüfen, ob das Gerät erreichbar ist.
2. Geben Sie im Adressfeld des Internet-Browsers die IP-Adresse oder die URL des Geräts ein. Standardmäßig ist der Zugriff über HTTPS aktiviert. Wenn Sie über HTTP auf das Gerät zugreifen, wird die Adresse automatisch auf HTTPS umgeleitet.

   Hinweis

   Informationen zum Sicherheitszertifikat

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

   Eine Meldung zum Sicherheitszertifikat erscheint. Quittieren Sie diese Meldung und setzen Sie das Laden der Seite fort.
   Wenn Sie einen anderen Port als den Standardport verwenden, dann geben Sie zwischen der IP-Adresse und der Portnummer einen Doppelpunkt ":" als Trennzeichen ein.
   Beispiel: https://192.168.16.178:49152
   Den Port ändern Sie unter "System > Konfiguration".
3. Wenn eine Verbindung zum Gerät besteht, erscheint die Anmeldeseite des Web Based Managements (WBM).
   Wenn Sie über eine HTTP-Verbindung auf das WBM zugreifen möchten, konfigurieren Sie unter "System > Konfiguration" bei "HTTP-Dienste" "HTTP & HTTPS".

Sprache umschalten

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

Hinweis

Verfügbare Sprachen

Als Sprachen sind Englisch und Deutsch verfügbar. Weitere Sprachen folgen in einer späteren Version.

Am WBM anmelden

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

     Hinweis

     Für die Geräte der US-Version ist das Passwort für den Benutzer "admin" geändert. Das Passwort kann durch das Fachpersonal für professionelle WLAN-Installationen beim Siemens Support erfragt werden.

   - Geben Sie das Passwort des entsprechenden Benutzerkontos ein.
3. Klicken Sie auf die Schaltfläche "Anmelden" oder bestätigen Sie die Eingabe mit "Enter".

   Hinweis

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

   Wenn Sie sich das erste Mal oder nach einem "Auf Werkseinstellungen zurücksetzen und Neustart", werden Sie aufgefordert, das Passwort zu ändern.
   Das neue Passwort muss der Passwortrichtlinie "Hoch" entsprechen:
   - Passwortlänge: Mindestens 8 Zeichen, maximal 128 Zeichen
   - Mindestens 1 Großbuchstabe
   - Mindestens 1 Sonderzeichen
   - Mindestens 1 Zahl
   - Er darf folgende Zeichen nicht enthalten: ; : ' ? ß § " ² ³ ° | € µ ä ö ü Ä Ö Ü
   - Die Zeichen für Space und Delete dürfen auch nicht enthalten sein.
4. Zur Bestätigung müssen Sie das Passwort wiederholen. Beide Passworteingaben müssen übereinstimmen.
5. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen", um den Vorgang abzuschließen. Die Änderungen sind sofort wirksam.

Wenn Sie sich erfolgreich angemeldet haben, erscheint die Startseite.

Schutz vor Brute-Force-Angriffen

Zum Schutz vor Brute-Force-Angriffen wird der IP-Adresse eines Benutzers bzw. einem Benutzer nach 11 fehlgeschlagenen Anmeldeversuchen die Anmeldung am Gerät verweigert.

Servicetechniker-Login

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

6.3 Menü "Wizard"

6.3.1 Basic Wizard

Einleitung

Mit dem Basic Wizard lassen sich menügeführt die wichtigsten Parameter konfigurieren.

Auf den Basic Wizard-Seiten sind nur die Parameter konfigurierbar, die für die Basisfunktionalität wichtig sind. Weitere Einstellungen konfigurieren Sie nach Beenden des Basic Wizard.

Voraussetzung

- Das Gerät befindet sich im Auslieferungszustand und ist über die Ethernet-Schnittstelle erreichbar.
- Sie haben dem Gerät eine IP-Adresse zugeordnet. Weitere Informationen dazu finden Sie im Kapitel "IP-Adressen (Seite 55)".
- Sie sind im WBM als Benutzer mit Administratorrechten angemeldet. Weitere Informationen dazu finden Sie im Kapitel "Login (Seite 67)".

Basic Wizard starten

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

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

Häufig verwendete Schaltflächen

Die WBM-Seiten des Basic Wizards enthalten folgende Schaltflächen:

Schaltfläche	Beschreibung
Weiter	Geht zur nächsten Seite
Zurück	Geht zur vorherigen Seite zurück

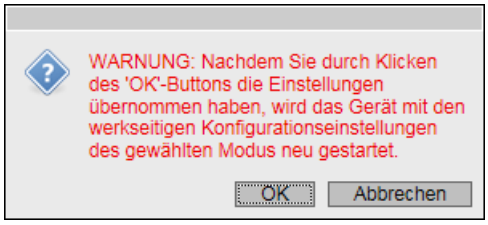
Schaltfläche	Beschreibung
Abbrechen	Der Basic Wizard wird ohne Übernahme der Einstellungen beendet.
Einstellungen übernehmen	Speichert die Konfiguration und beendet den Wizard.

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

6.3.1.1 Systemeinstellungen

Einleitung

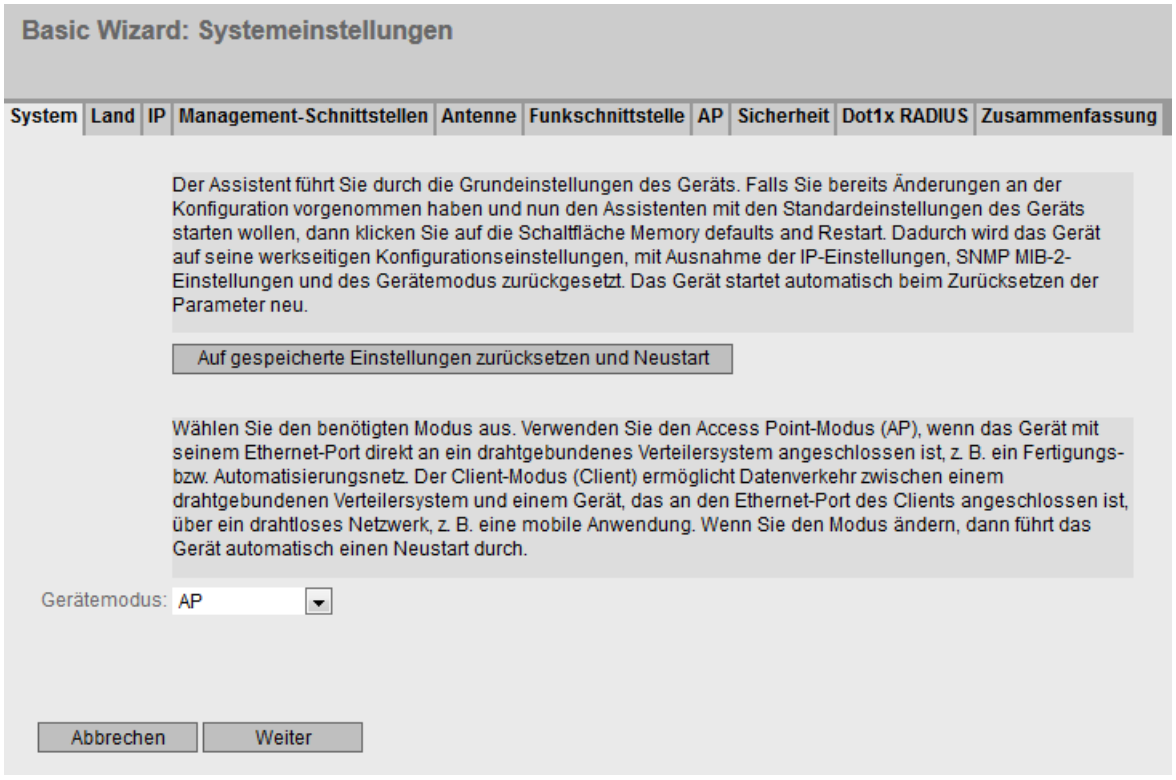
Auf dieser Basic Wizard-Seite legen Sie die Betriebsart für das Gerät fest. Nach dem Ändern der Betriebsart wird eine Meldung eingeblendet.



Wenn Sie die Meldung mit "OK" bestätigen, startet das Gerät mit den werkseitigen Konfigurationseinstellungen neu. Melden Sie sich dann erneut an und starten den Basic-Wizard, um die Konfiguration des Geräts für die gewählte Betriebsart fortzusetzen.

Hinweis

Weil nur Access Points auch im Client-Modus arbeiten können kann die Betriebsart auch nur bei diesen Geräten ausgewählt werden.



Beschreibung

Die Basic Wizard-Seite enthält folgende Felder:

- **Auf gespeicherte Einstellungen zurücksetzen und Neustart**
  Wenn Sie auf die Schaltfläche klicken, werden die werkseitigen Konfigurationseinstellungen mit Ausnahme der folgenden Parameter wiederhergestellt und es wird ein Neustart ausgeführt.
  - IP-Adresse
  - Subnetzmaske
  - IP-Adresse des Default-Gateways
  - DHCP Client ID
  - DHCP
  - Systemname
  - System-Aufstellungsort
  - System-Ansprechpartner
  - Benutzernamen und Passwörter
  - Betriebsart des Geräts

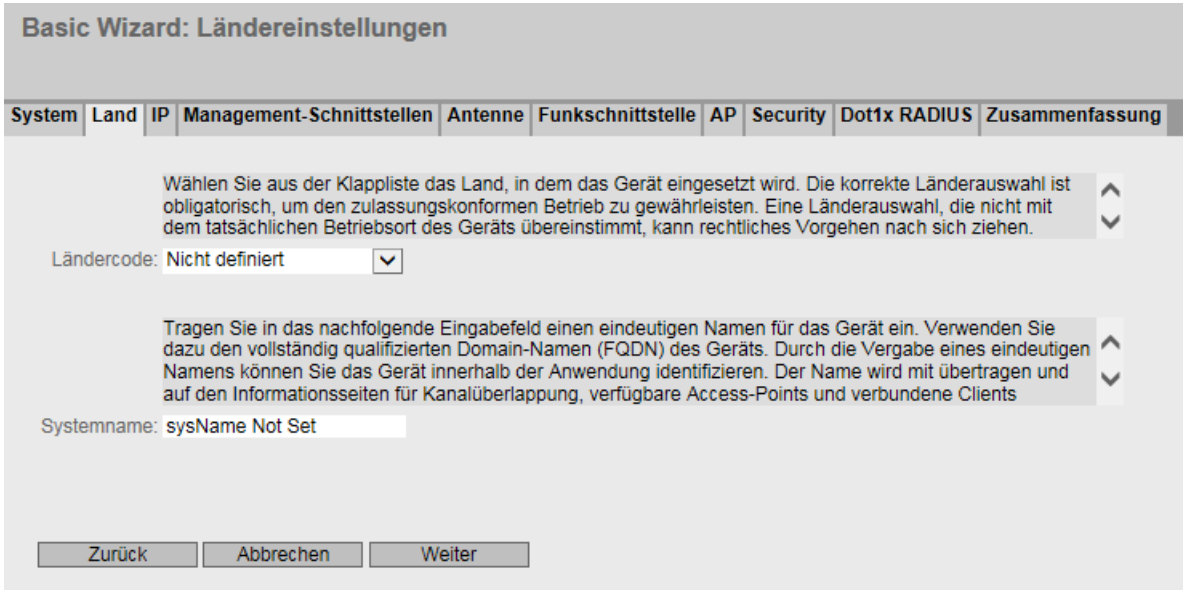
Nach dem Neustart des Geräts müssen Sie sich neu anmelden und den Basic Wizard erneut starten, um die Konfiguration des Geräts durchzuführen.

- **Gerätemodus**
  Wählen Sie die Betriebsart des Geräts aus. Diese Auswahl steht nur bei Access Points zur Verfügung.
  Folgende Betriebsarten sind möglich:
  - AP: Access Point-Modus
  - Client: Client-Modus

6.3.1.2 Ländereinstellungen

Einleitung

Auf dieser Basic Wizard-Seite konfigurieren Sie das Land und den Systemnamen.



Beschreibung

Die Basic Wizard-Seite enthält folgende Felder

- **Ländercode**
  Wählen Sie in der Klappliste das Land aus, in dem das Gerät eingesetzt wird. Sie brauchen die landesspezifischen Daten nicht zu kennen, die richtige Kanaleinteilung und Festlegung der Sendeleistung erfolgt entsprechend Ihrer Länderauswahl durch das Gerät.

  Hinweis

  Ländereinstellung

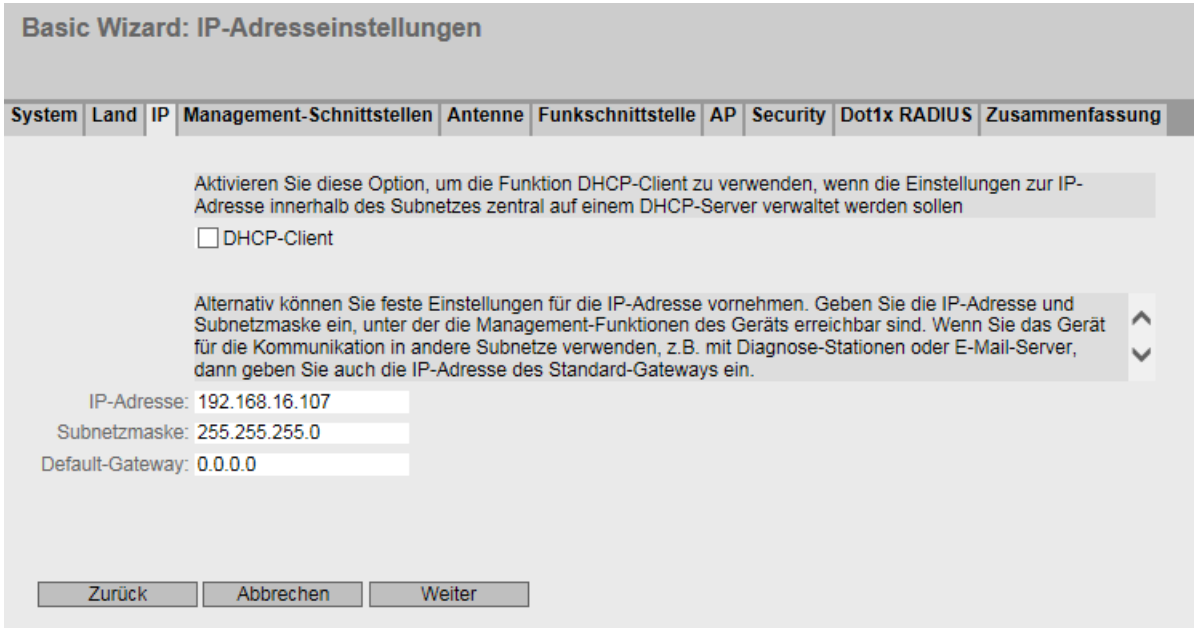
  Die richtige Ländereinstellung ist für einen zulassungskonformen Betrieb unbedingt notwendig. Die Auswahl eines vom Anwenderland abweichenden Landes kann strafrechtlich geahndet werden.

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

6.3.1.3 IP-Adresseinstellungen

Einleitung

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



Beschreibung

Die Basic Wizard-Seite enthält folgende Felder:

- **DHCP-Client**
  Legen Sie fest, wie die IP-Adresse zugeordnet wird. Für die Zuordnung von IP-Adressen gibt es zwei Möglichkeiten.
  - Aktiviert
    Das Gerät bezieht eine dynamische IP-Adresse von einem DHCP-Server.
  - Deaktiviert
    Die IP-Einstellungen tragen Sie in den Eingabefeldern "IP-Adresse" und "Subnetzmaske" ein.
- **IP-Adresse**
  Tragen Sie eine IP-Adresse ein, die innerhalb Ihres Netzes eindeutig ist.
- **Subnetzmaske**
  Tragen Sie die Subnetzmaske des Geräts ein.
- **Default-Gateway**
  Tragen Sie die IP-Adresse des Default-Gateways ein, damit das Gerät mit Geräten in anderen Subnetzen kommunizieren kann, z.B. Diagnose-Stationen, E-Mail-Server.

6.3.1.4 Management-Schnittstellen

Systemkonfiguration

Auf dieser Basic Wizard-Seite legen Sie fest, über welche Dienste auf das Gerät zugegriffen wird. Zu einigen Diensten gibt es weitere Konfigurationsseiten, auf denen detailliertere Einstellungen möglich sind. Konfigurieren Sie diese Dienste nach Beenden des Basic Wizard.

Beschreibung

Die Seite enthält folgende Felder:

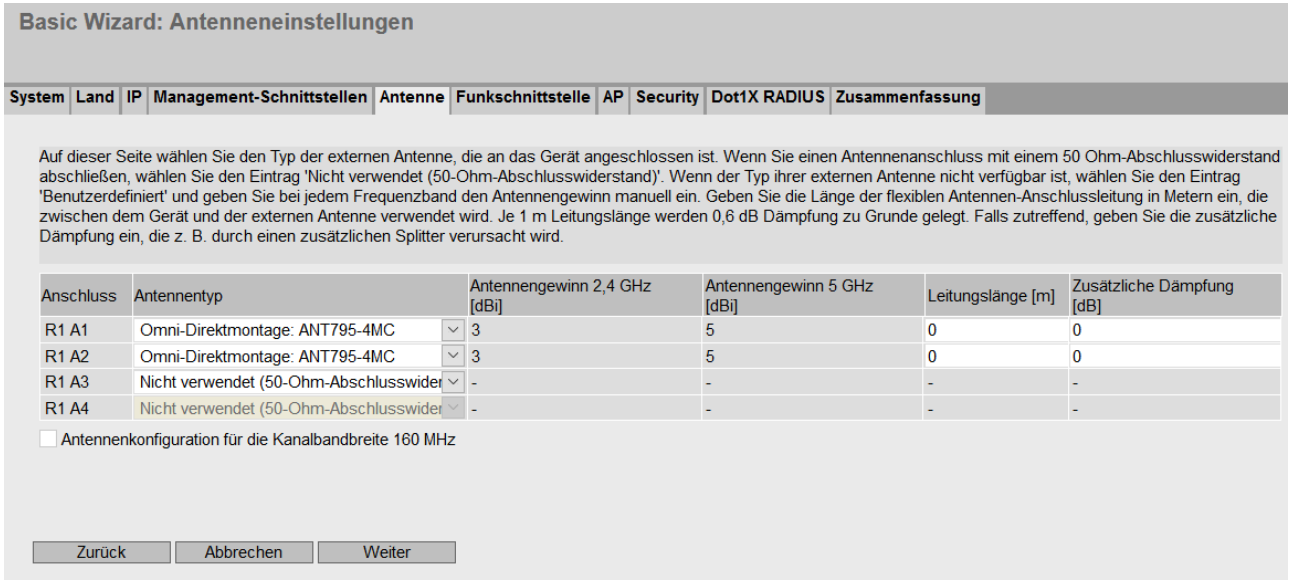
- **Telnet-Server**
  Aktivieren oder deaktivieren Sie den Dienst "Telnet-Server" für den unverschlüsselten Zugriff auf das CLI.
- **SSH-Server**
  Aktivieren oder deaktivieren Sie den Dienst "SSH-Server" für den verschlüsselten Zugriff auf das CLI.

- **DCP-Server**
  Legen Sie fest, ob auf das Gerät mit DCP (Discovery and Configuration Protocol) zugegriffen werden kann:
  - "-" (Deaktiviert)
    DCP ist deaktiviert. Geräteparameter können weder gelesen noch geändert werden.
  - Lesen/Schreiben
    Mit DCP können Geräteparameter sowohl gelesen als auch verändert werden.
  - Schreibgeschützt
    Mit DCP können Geräteparameter zwar gelesen, aber nicht verändert werden.
- **SNMP**
  Wählen Sie aus der Klappliste das Protokoll. Folgende Einstellungen sind möglich:
  - "-" (SNMP deaktiviert)
    Ein Zugriff auf die Geräteparameter ist über SNMP nicht möglich.
  - SNMPv1/v2c/v3
    Ein Zugriff auf die Geräteparameter ist mit den SNMP Versionen 1, 2c oder 3 möglich. Weitere Einstellungen konfigurieren Sie unter "System > SNMP > Allgemein".
  - SNMPv3
    Ein Zugriff auf die Geräteparameter ist mit der SNMP Version 3 möglich. Weitere Einstellungen konfigurieren Sie unter " System > SNMP > Allgemein".
- **SNMPv1/v2 schreibgeschützt**
  Aktivieren oder deaktivieren Sie den schreibenden Zugriff auf SNMP-Variablen bei SNMPv1/v2c.
- **SINEMA-Konfigurationsschnittstelle**
  Wenn die SINEMA Konfigurationsschnittstelle aktiviert ist, können Sie Konfigurationen über das TIA-Portal auf das Gerät laden.

6.3.1.5 Antenneneinstellungen

Einleitung

Auf dieser Basic Wizard-Seite konfigurieren Sie die Einstellungen für die externen Antennen.



Beschreibung

Die Tabelle enthält folgende Spalten:

- **Anschluss**
  Zeigt die Bezeichnung des jeweiligen Antennenanschlusses an.

  Hinweis

  Kanalbandbreite 160 MHz

  - Für Betrieb bei 160 MHz werden zwei Antennen verwendet
    – Spatial Stream 1: erste Antenne RxA1 + zweite Antenne RxA4

    Damit die Konfiguration beider Antennen gleich ist, werden die Einstellungen für die erste Antenne konfiguriert und für die zweite Antenne automatisch übernommen.
  - Nach der Tabelle wird die Einstellung "Antennenkonfiguration für Kanalbandbreite 160 MHz" eingeblendet.
  - Nur der Antennenmodus RX/TX ist erlaubt.

  Antennen

  Folgende Antennen unterstützen keinen Betrieb bei 160 MHz:

  - ANT793-8DJ
  - ANT793-8DK
  - ANT793-8DP
  - ANT793-8DL
  - ANT793-8DQ

- **Antennentyp**
  Wählen Sie den Typ der externen Antenne aus, die an das Gerät angeschlossen ist. Wenn der Typ ihrer Antenne nicht verfügbar ist, wählen Sie den Eintrag "Benutzerdefiniert".
  Nicht verwendete Anschlüsse müssen mit einem 50 Ω-Abschlusswiderstand versehen werden. Wählen Sie dazu den Eintrag "Not used (Connect 50 Ohm Termination)".

  Hinweis

  50 Ω-Abschlusswiderstand

  Jede WLAN-Schnittstelle verfügt über vier Antennenanschlüsse. Ungenutzte Anschlüsse müssen mit einem 50 Ω-Abschlusswiderstand versehen werden.

  An den Antennen-Anschlüssen R1 A1 und R2 A1 muss immer eine Antenne angeschlossen sein, sobald die WLAN-Schnittstelle eingeschaltet wird. Wenn keine Antenne angeschlossen ist, muss auch die entsprechende Schnittstelle für Rx und Tx deaktiviert sein. Andernfalls kann es zu Übertragungsstörungen kommen.

- **Antennengewinn [dBi]**
  Wenn Sie bei "Antennentyp" den Eintrag "Benutzerdefiniert" wählen, tragen Sie manuell den Antennengewinn in der Einheit "dBi" ein.

  – Antennengewinn 2,4 GHz [dBi]
    Tragen Sie den Antennengewinn ein, den die Antenne im Frequenzband 2.4 GHz hat.
  – Antennengewinn 5 GHz [dBi]
    Tragen Sie den Antennengewinn ein, den die Antenne im Frequenzband 5 GHz hat.

- **Leitungslänge [m]**
  Tragen Sie die Länge der flexiblen Antennen-Anschlussleitung in Metern ein, die zwischen dem Gerät und der externen Antenne verwendet wird.
- **Zusätzliche Dämpfung [dB]**
  Tragen Sie die zusätzliche Dämpfung ein, die z. B. durch einen zusätzlichen Splitter verursacht wird.
- **Antennenkonfiguration für Kanalbandbreite 160 MHz** (Nicht beim SCALANCE W1788-2IA M12)
  - Access Point-Modus (nicht konfigurierbar)
    Wenn an WLAN 1 oder WLAN 2 die Kanalbandbreite auf 160 MHz eingestellt ist, wird die Einstellung eingeblendet. Die Kanalbandbreite wird unter "Schnittstellen > WLAN > AP" konfiguriert.
  - Client-Modus (konfigurierbar)
    Wenn aktiviert, wird an der WLAN-Schnittstelle die Kanalbandbreite auf 160 MHz eingestellt. Vorausgesetzt DFS und IEEE 802.11ac sind aktiviert. Nur wenn DFS aktiviert ist, sind für den Betrieb von 160 MHz genügend Kanäle verfügbar.

6.3.1.6 Funkeinstellungen

Einleitung

Auf dieser Basic Wizard-Seite legen Sie die Konfiguration für die WLAN-Schnittstellen fest.

Beschreibung

Die Tabelle enthält folgende Spalten:

- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen an.
- **Aktiviert**
  Aktivieren oder deaktivieren Sie die WLAN-Schnittstelle. Die WLAN-Schnittstellen sind im Auslieferungszustand deaktiviert.
- **Modus der Funkschnittstelle**
  Zeigt die Betriebsart der WLAN-Schnittstelle an.
- **Frequenzband**
  Legen Sie das Frequenzband fest.
  - 2.4 GHz
  - 5 GHz
- **WLAN-Modus 2.4 GHz / WLAN-Modus 5 GHz**
  Wählen Sie für das projektierte Frequenzband den gewünschten Übertragungsstandard aus. Die Auswahl ist abhängig von der Ländereinstellung.
  - 802.11g
    Der Übertragungsstandard IEEE 802.11g (2.4 GHz) ist eingestellt. Dieser Übertragungsstandard ist abwärts kompatibel zu IEEE 802.11b.
  - 802.11n
    Der Übertragungsstandard IEEE 802.11n (2.4 GHz und 5 GHz) ist eingestellt. Dieser Übertragungsstandard ist abwärts kompatibel zu IEEE802.11a und IEEE 802.11g.
  - 802.11a
    Der Übertragungsstandard IEEE 802.11a (5 GHz) ist eingestellt.
  - 802.11ac
    Der Übertragungsstandard IEEE 802.11ac (5 GHz) ist eingestellt.

Hinweis

Datenrate

Die Datenrate wird automatisch angepasst.

- **DFS (802.11h)**
  - Aktiviert
    Mit der Funktion DFS ist es möglich, auch die oberen 5-GHz-Kanäle zu verwenden. Diese Kanäle sind länderspezifisch und unterliegen bestimmten DFS-Vorgaben. Weiterführende Informationen dazu finden Sie in der länderspezifischen DFS-Dokumentation.
    Bevor der Access Point über einen dieser Kanäle sendet, prüft er 60 Sekunden gemäß CAC (Channel Availability Check) nach konkurrierenden Radarsignalen.
    Innerhalb der Suchdauer sendet der Access Point auch keine Beacons. Bei Wetter-Radar-Kanälen (5,6 - 5,65 GHz) beträgt die Suchdauer 10 Minuten.
    Wenn nach Ablauf der Suchdauer keine Radarsignale gefunden wurden, sendet der Access Point auf dem Kanal. Sonst wechselt der Access Point den Kanal und wiederholt die Prüfung.
    Auch während des Betriebs sucht der Access Point ständig nach Radarsignalen.
    Wenn der Access Point auf dem aktuellen Kanal ein Radarsignal entdeckt, kündigt er den Kanalwechsel den Clients an. Danach wechselt er automatisch auf einen alternativen DFS-Kanal und der aktuelle Kanal wird für 30 Minuten gesperrt.

    Hinweis

    Kanalbandbreite 160 MHz nutzen

    Nur wenn DFS aktiviert ist, sind für den Betrieb von 160 MHz genügend Kanäle verfügbar.

  - Deaktiviert
    Die Funktion DFS wird nicht verwendet.

- **Outdoor-Modus**
  - Aktiviert
    Wenn Sie den Outdoor-Modus aktiviert haben, stehen Ihnen nur die Kanäle zur Verfügung, die für den Outdoor-Betrieb zugelassen sind.
  - Deaktiviert
    Wenn Sie den Outdoor-Modus deaktiviert haben, stehen Ihnen nur die Kanäle zur Verfügung, die für den Betrieb in einem Gebäude zugelassen sind.
- **max. Tx-Leistung**
  Legen Sie die maximal mögliche Sendeleistung des Geräts fest.
  Wenn die Sendeleistung zu hoch eingestellt ist, kann das empfangene Signal beim Client übersteuert sein. Kontrollieren Sie beim Client die Empfangssignalstärke (dBm).
  Abhängig von den verwendeten Antennen kann eine Verminderung der Sendeleistung notwendig werden, um die gesetzlich vorgeschriebene maximale Sendeleistung nicht zu überschreiten. Eine Verminderung der Sendeleistung bewirkt eine gezielte Reduktion der Zellengröße.

Hinweis

Je nach Kanal und Datenrate variiert die maximal mögliche Sendeleistung. Beachten Sie für weitere Informationen zur Sendeleistung die Dokumentation "Leistungsdaten 801.11ac SCALANCE W1700".

Hinweis

Werden beim Access Point beide Schnittstellen im gleichen Frequenzbereich betrieben, kann es bei einer Sendeleistung größer 15 dBm zu Funkstörungen an einer bzw. an beiden Schnittstellen kommen.

Prüfung der Tx-Leistung

Zeigt an, ob mit den vorgenommenen Einstellungen die zulässigen Sendeleistungsbeschränkungen des eingestellten Landes verletzt werden. Der errechnete Wert von "max. EIRP" wird geprüft, ob dieser Wert die Sendeleistungsbeschränkung auf bestimmten Kanälen in dem eingestellten Land verletzt. Wenn "Nur zugelassene Kanäle verwenden" eingestellt ist, werden auch nur die dort gewählten Kanäle geprüft.

- -
  Die Kanäle können mit den aktuellen Einstellungen benutzt werden.
- Kanalnummern
  Gibt an, bei welchen Kanälen, die aktuelle Sendeleistung die maximal erlaubte Sendeleistung überschreitet.

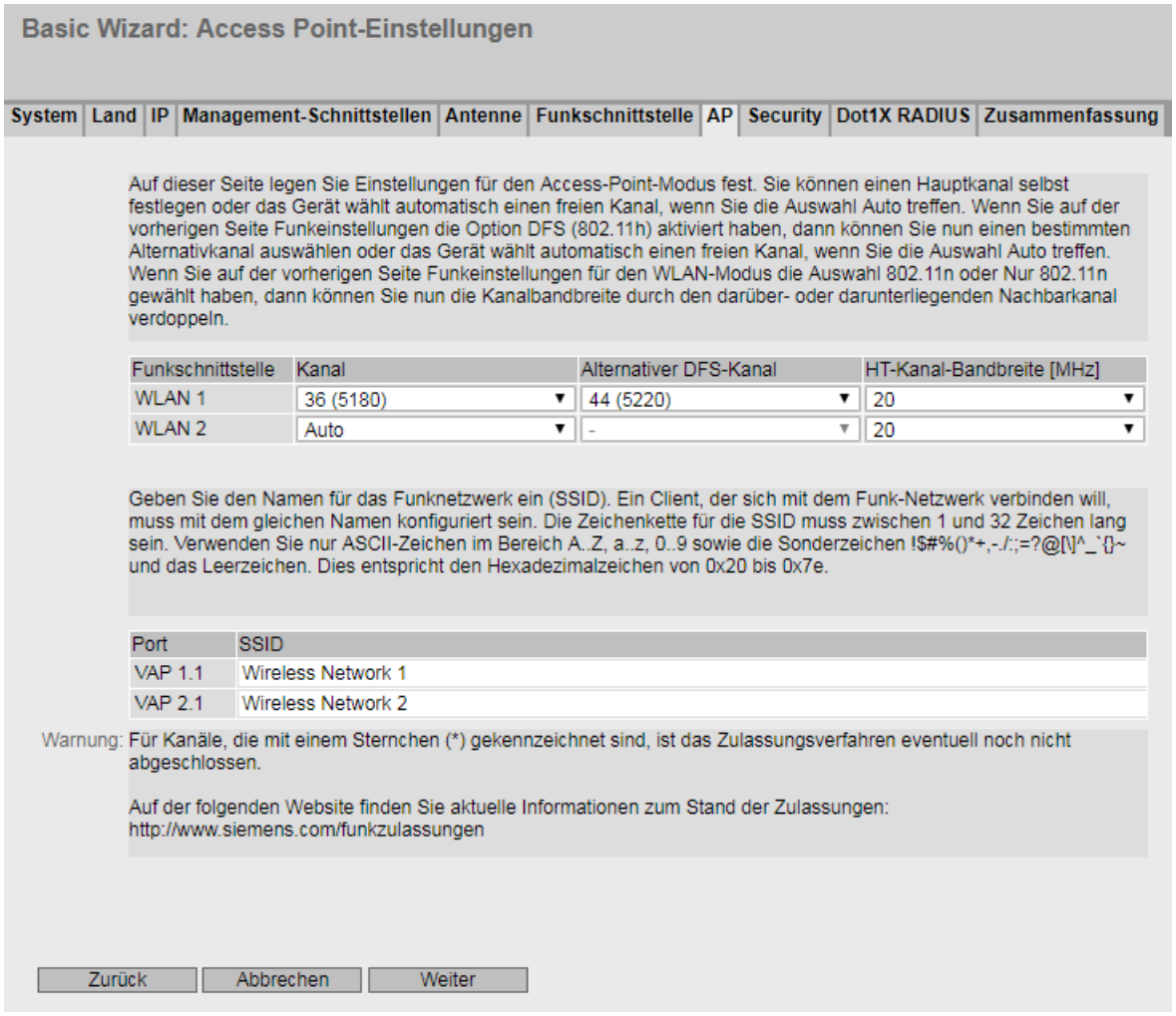
6.3.1.7 Access Point-Einstellungen

Hinweis

Diese Seite ist nur im Access Point-Modus verfügbar.

Einleitung

Auf dieser Basic Wizard-Seite legen Sie die Konfiguration für den Access Point fest.



Beschreibung

Die Tabelle 1 enthält folgende Spalten:

- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen an.
- **Kanal**
  Legen Sie den Hauptkanal fest. Wenn sich der Access Point selbst einen freien Kanal suchen soll, verwenden Sie "Auto". Wenn Sie einen festen Kanal nutzen wollen, wählen Sie den gewünschten Kanal aus der Klappliste.

- **Alternativer DFS-Kanal**
  Wenn Sie auf der Basic Wizard-Seite "Funkeinstellungen" die Funktion "DFS" aktiviert haben, legen Sie hier den Alternativ-Kanal fest. Wenn sich der Access Point selbst einen freien Kanal suchen soll, verwenden Sie "Auto". Wenn Sie einen festen Kanal nutzen wollen, wählen Sie den gewünschten Kanal in der Klappliste aus.
- **Kanalbandbreite [MHz]**
  Nur bei den Übertragungsstandards IEEE 802.11n und IEEE 802.11ac können Sie die Kanalbandbreite festlegen.
  Folgende Einstellungen sind möglich.
  - 20 MHz
  - 40 MHz

  Nur bei IEEE 802.11ac:
  - 80 MHz
  - 160 MHz (Nicht beim SCALANCE W1788-2IA M12)
    Nur wenn DFS aktiviert ist, sind für den Betrieb von 160 MHz genügend Kanäle verfügbar.

Die Tabelle 2 enthält folgende Spalten:

- **Port**
  Zeigt die erste VAP-Schnittstelle pro WLAN-Schnittstelle an.
- **SSID**
  Tragen Sie die SSID ein. Die Länge der Zeichenkette für SSID beträgt 1 bis 32 Zeichen.
  Für die SSID wird der ASCII-Code 0x20 bis 0x7e verwendet.
  Nach Beenden des Basic Wizards können Sie unter "Schnittstellen > WLAN > Access Point-Einstellungen" weitere SSIDs definieren.

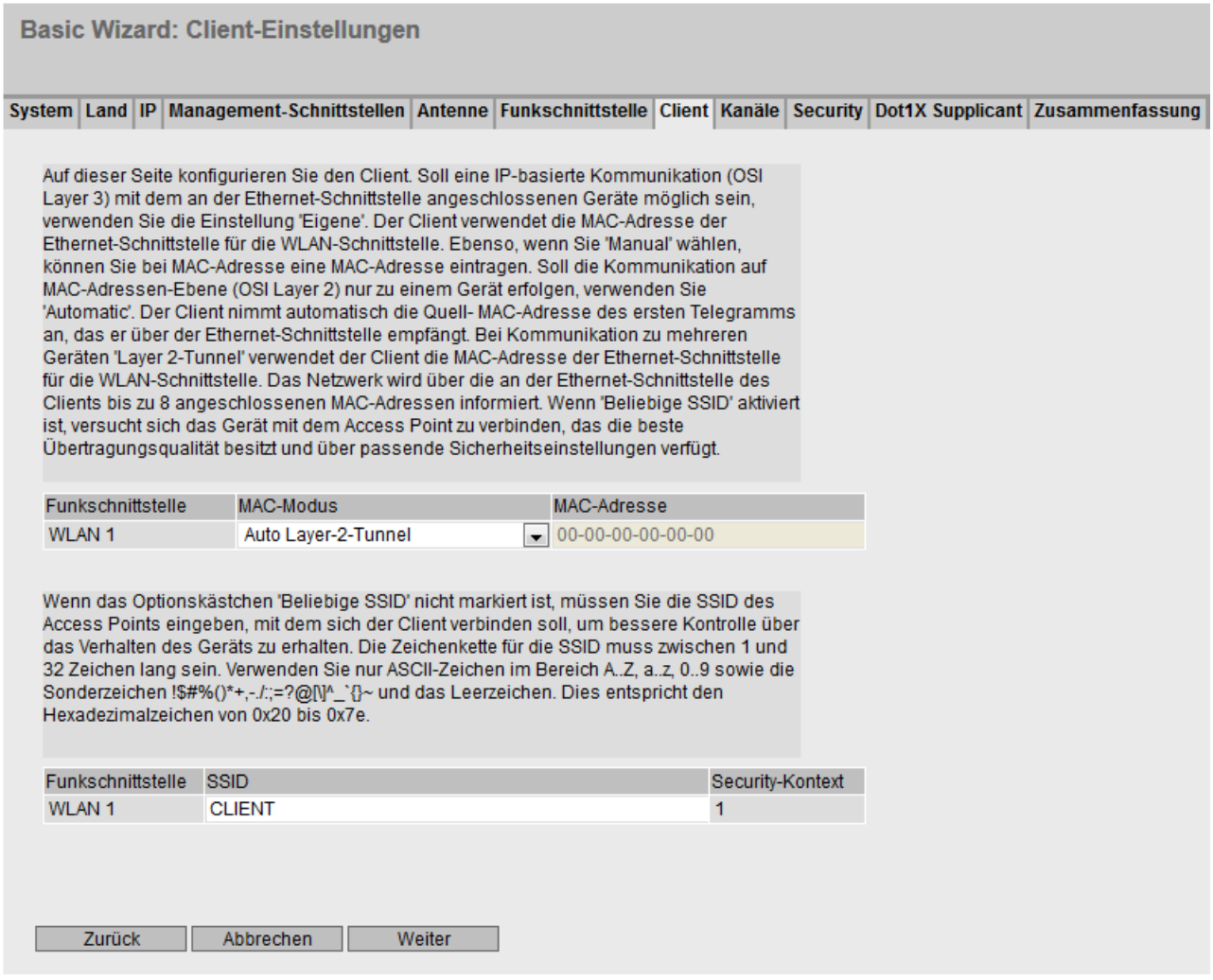
6.3.1.8 Client-Einstellungen

Einleitung

Auf dieser Basic Wizard-Seite legen Sie die Konfiguration für Clients fest, z.B. die Zuordnung der MAC-Adresse.

Hinweis

Diese Seite ist nur bei Clients oder bei Access Points im Client-Modus verfügbar.


Basic Wizard: Client-Einstellungen
System
Land
IP
Management-Schnittstellen
Antenne
Funkschnittstelle
Client
Kanäle
Security
Dot1X Supplicant
Zusammenfassung
Auf dieser Seite konfigurieren Sie den Client. Soll eine IP-basierte Kommunikation (OSI Layer 3) mit dem an der Ethernet-Schnittstelle angeschlossenen Geräte möglich sein, verwenden Sie die Einstellung 'Eigene'. Der Client verwendet die MAC-Adresse der Ethernet-Schnittstelle für die WLAN-Schnittstelle. Ebenso, wenn Sie 'Manual' wählen, können Sie bei MAC-Adresse eine MAC-Adresse eintragen. Soll die Kommunikation auf MAC-Adressen-Ebene (OSI Layer 2) nur zu einem Gerät erfolgen, verwenden Sie 'Automatic'. Der Client nimmt automatisch die Quell- MAC-Adresse des ersten Telegramms an, das er über der Ethernet-Schnittstelle empfängt. Bei Kommunikation zu mehreren Geräten 'Layer 2-Tunnel' verwendet der Client die MAC-Adresse der Ethernet-Schnittstelle für die WLAN-Schnittstelle. Das Netzwerk wird über die an der Ethernet-Schnittstelle des Clients bis zu 8 angeschlossenen MAC-Adressen informiert. Wenn 'Beliebige SSID' aktiviert ist, versucht sich das Gerät mit dem Access Point zu verbinden, das die beste Übertragungsqualität besitzt und über passende Sicherheitseinstellungen verfügt.
Funkschnittstelle
MAC-Modus
MAC-Adresse
WLAN 1
Auto Layer-2-Tunnel
00-00-00-00-00-00
Wenn das Optionskästchen 'Beliebige SSID' nicht markiert ist, müssen Sie die SSID des Access Points eingeben, mit dem sich der Client verbinden soll, um bessere Kontrolle über das Verhalten des Geräts zu erhalten. Die Zeichenkette für die SSID muss zwischen 1 und 32 Zeichen lang sein. Verwenden Sie nur ASCII-Zeichen im Bereich A..Z, a..z, 0..9 sowie die Sonderzeichen !$#%()*+,-./:;=?@[\]^_`{}~ und das Leerzeichen. Dies entspricht den Hexadezimalzeichen von 0x20 bis 0x7e.
Funkschnittstelle
SSID
Security-Kontext
WLAN 1
CLIENT
1
Zurück
Abbrechen
Weiter

Beschreibung

Die Tabelle 1 enthält folgende Spalten:

- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen an.
- **MAC-Modus**
  Legen Sie fest, wie dem Client die MAC-Adresse zugeordnet wird. Es gibt die folgenden Möglichkeiten.
  - Auto Layer 2-Tunnel
    Der Client verwendet entweder den MAC-Modus "Eigene" oder "Layer-2-Tunnel".
  - Manuell
    Wenn Sie "Manuell" wählen, geben Sie die MAC-Adresse in der Spalte "MAC-Adresse" ein.
  - Eigene
    Der Client verwendet die MAC-Adresse der Ethernet-Schnittstelle für die WLAN-Schnittstelle.
  - Layer-2-Tunnel
    Der Client verwendet die MAC-Adresse der Ethernet-Schnittstelle für die WLAN-Schnittstelle. Zusätzlich wird das Netzwerk über die an der Ethernet-Schnittstelle des Clients angeschlossenen MAC-Adressen informiert. Es können bis zu acht MAC-Adressen verwendet werden.
- **MAC-Adresse**
  Tragen Sie die MAC-Adresse des Clients ein. Das Eingabefeld ist nur editierbar, wenn Sie bei "MAC-Modus" "Manuell" eingestellt haben.

Die Tabelle 2 enthält folgende Spalten:

- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen an.
- **SSID**
  Tragen Sie die SSID des Access Points ein, mit der sich der Client verbindet. Im Basic Wizard können Sie nur eine SSID festlegen. Nach Beenden des Basic Wizards können Sie unter "Schnittstellen > WLAN > Client" weitere SSIDs definieren.
- **Security-Kontext**
  Zeigt den zugeordneten Security-Kontext an. Im Basic Wizard steht nur ein Security-Kontext zur Verfügung. Nach Beenden des Basic Wizards können Sie unter "Security > WLAN > Basic" weitere Security-Kontexte erstellen und konfigurieren.

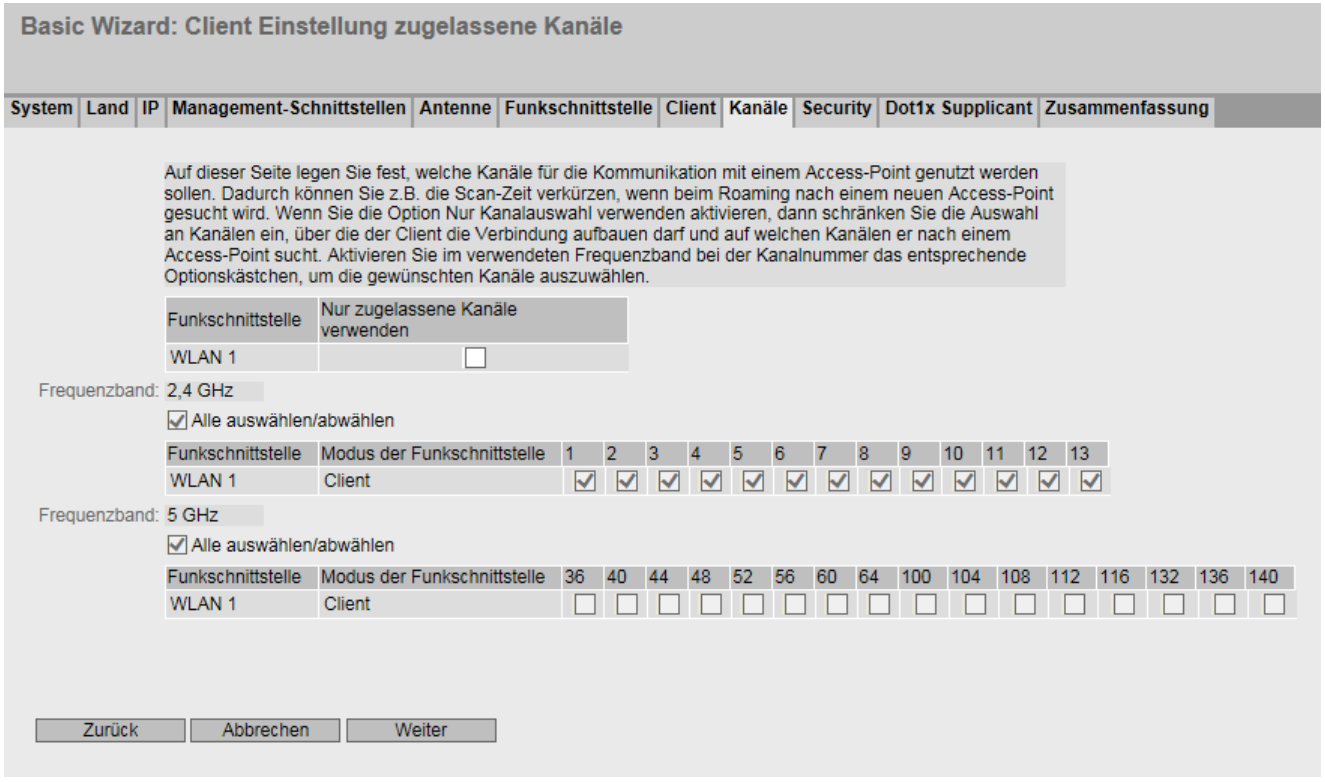
6.3.1.9 Client-Einstellung zugelassene Kanäle

Einleitung

Für die Kommunikation wird ein bestimmter Kanal innerhalb eines Frequenzbandes verwendet. Auf dieser Seite können Sie diesen Kanal entweder fest vorgeben oder so konfigurieren, dass eine automatische Kanalauswahl erfolgt.

Hinweis

Diese Seite ist nur bei Clients oder bei Access Points im Client-Modus verfügbar.



Beschreibung

Die Tabelle 1 enthält folgende Spalten:

- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen an.
- **Nur zugelassene Kanäle verwenden**
  Wenn Sie die Option aktivieren, schränken Sie damit die Auswahl an Kanälen ein, über die der Client die Verbindung aufbauen darf.
  In den folgenden Tabellen definieren Sie, auf welchen Kanälen der Client nach einem AP sucht.
  Die Tabellen sind nach den Frequenzbändern getrennt.
  Wenn die Option deaktiviert ist, werden die entsprechend den Einstellungen (Ländercode, Antennen, Sendeleistung etc.) verfügbaren Kanäle benutzt.

Über den Tabellen der Frequenzbänder befindet sich jeweils folgendes Optionskästchen:

- **Alle auswählen/abwählen**
  - Aktiviert
    Wenn Sie das Optionskästchen aktivieren, werden alle Kanäle markiert.
  - Deaktiviert
    Wenn Sie das Optionskästchen deaktivieren, bleibt nur der erste gültige Kanal des Frequenzbands aktiviert.

Die Tabellen der Frequenzbänder enthalten folgende Spalten:

- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen an.
- **Modus der Funkschnittstelle**
  Zeigt die Betriebsart des Geräts an.
- **Kanalnummer**
  Um die gültigen Kanäle für das gewünschte Frequenzband festzulegen, aktivieren Sie bei der Kanalnummer das entsprechende Optionskästchen.
  In der Tabelle werden die zulässigen Kanäle des Landes angezeigt. Nur die gültigen Kanäle lassen sich aktivieren. Nicht gültige Kanäle sind gegraut und können nicht aktiviert werden.

Hinweis

Um die Kanäle festzulegen, muss die Einstellung "Nur zugelassene Kanäle verwenden" aktiviert sein.

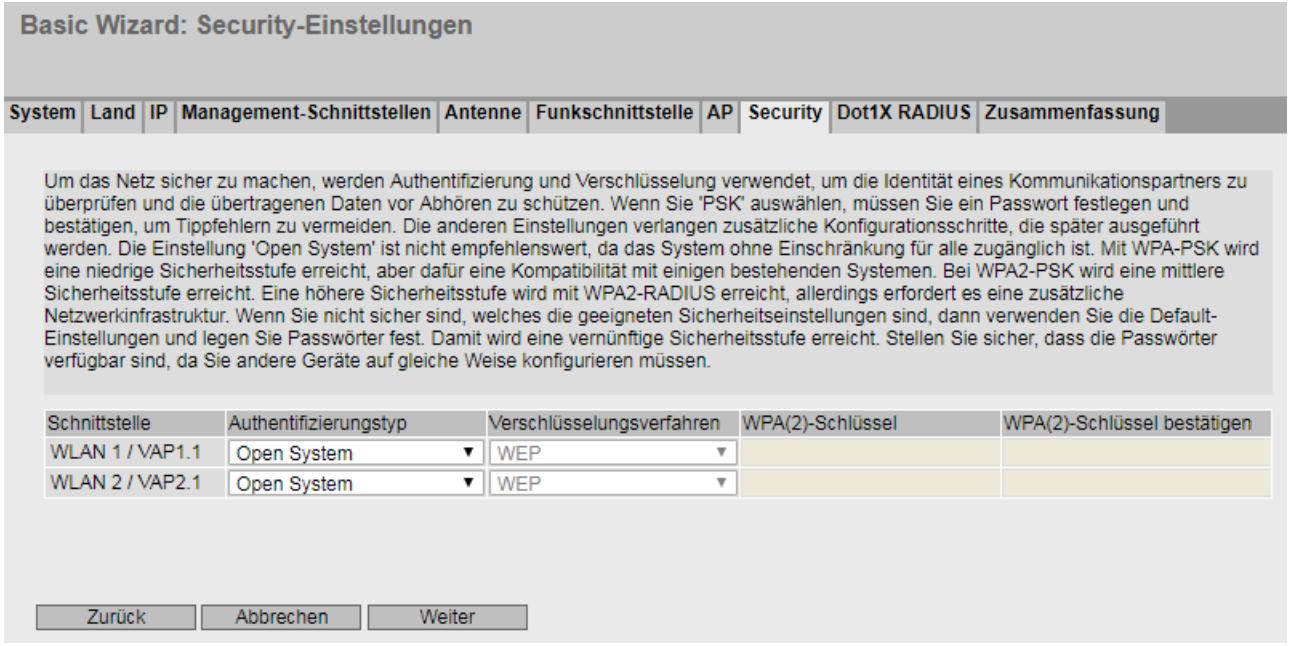
6.3.1.10 Security-Einstellungen

Einleitung

Um das Netzwerk zu sichern, werden Authentifizierung und Verschlüsselung verwendet. Die Sicherheitsstufen legen Sie durch die Authentifizierungsart und durch das Verschlüsselungsverfahren fest.

Verwenden Sie WPA2/AES, um einen Passwortmissbrauch zu verhindern. WPA2 (RADIUS)/ WPA2-PSK mit AES bietet die größte Sicherheit.

Die Sicherheitseinstellungen an beiden Geräten müssen übereinstimmen, damit ein Client mit einem Access Point kommunizieren kann.



Beschreibung

Die Tabelle enthält folgende Spalten:

- **Schnittstelle** (nur im Access Point-Modus)
  Zeigt die Schnittstelle an, auf die sich die Einstellungen beziehen.
- **Security-Kontext** (nur im Client-Modus)
  Zeigt den Security-Kontext an, auf den sich die Einstellungen beziehen.
- **Authentifizierungstyp**
  Wählen Sie die Authentifizierungsart aus. Die Auswahl ist abhängig von der Betriebsart und dem Übertragungsstandard.

  Hinweis

  WLAN-Modus IEEE 802.11 n / ac

  Im WLAN-Modus IEEE 802.11n / ac ist nur die WPA2 (WPA2-PSK u. WPA2 RADIUS) Verschlüsselung möglich.

  – Open System
  Es wird keine Authentifizierung vorgenommen. Eine Verschlüsselung mit einem festen (nicht wechselnden) WEP-Schlüssel kann optional ausgewählt werden. Um den Schlüssel zu verwenden, aktivieren Sie "Verschlüsselung". Den WEP-Schlüssel definieren auf der Seite "Schlüssel".

  – Shared Key
  Bei der Shared Key Authentifizierung wird am Client und am Access Point ein fester Schlüssel hinterlegt. Dieser WEP-Schlüssel wird dann zur Authentifizierung und Verschlüsselung verwendet. Den WEP-Schlüssel definieren auf der Seite "Schlüssel".

  Hinweis

  Damit Sie "Open System" mit "Verschlüsselung" oder "Shared Key" aktivieren können, müssen Sie den Schlüssel 1 unter "Security > WLAN >Schlüssel" konfigurieren. Wenn Sie eine dieser Authentifizierungsmethoden verwenden wollen, konfigurieren Sie diese nach Beendigung des Basic Wizards.

  – WPA (RADIUS)
  Wi-Fi Protected Access (WPA) ist eine Methode, die durch die Wi-Fi Alliance spezifiziert wird, um die Sicherheitslücken von WEP zu schließen. Dabei ist die Authentifizierung durch einen Server (802.1x) fest vorgeschrieben. Durch den dynamischen Austausch der Schlüssel bei jedem Datenframe wird eine weitere Sicherheit eingebaut.

  – WPA-PSK
  WPA Pre Shared Key (WPA-PSK) ist die abgeschwächte Version von WPA. Bei diesem Verfahren wird keine Authentifizierung durch einen Server durchgeführt, sondern anhand eines Passworts. Dieses Passwort wird auf dem Client wie auf dem Server manuell konfiguriert.

  – WPA2 (RADIUS)
  WPA2 (Wi-Fi Protected Access 2) ist die Weiterentwicklung von WPA und implementiert die Funktionen des Sicherheitsstandards IEEE 802.11i. Die WPA-Authentifizierung arbeitet jedoch mit dem RADIUS-Server.

  - WPA2-PSK
    WPA2-PSK basiert auf dem Standard 802.11i. Die WPA-Authentifizierung arbeitet jedoch ohne RADIUS-Server. Stattdessen wird auf jedem Client und Access Point ein WPA(2)-Schlüssel (WPA(2) Pass phrase) hinterlegt. Die WPA(2) Pass phrase wird zur Authentifizierung und weiteren Verschlüsselung verwendet.

- **Verschlüsselungsverfahren**
  Wählen Sie das Verschlüsselungsverfahren.

  - AUTO
    Je nach Fähigkeit der Gegenstation wird entweder AES oder TKIP automatisch ausgewählt.
  - WEP (Wired Equivalent Privacy)
    Ein symmetrisches Stromverschlüsselungsverfahren mit lediglich 40 bzw. 104 Bit langen Schlüsseln, die auf dem RC4-Algorithmus (Ron's Code 4) basieren.
  - TKIP (Temporal Key Integrity Protocol)
    Ein symmetrisches Stromverschlüsselungsverfahren mit dem RC4-Algorithmus (Ron's Code 4). TKIP verwendet im Gegensatz zur schwachen WEP-Verschlüsselung wechselnde Schlüssel, die von einem Hauptschlüssel abgeleitet werden. TKIP kann außerdem gefälschte Datentelegramme erkennen.
  - AES (Advanced Encryption Standard)
    Starkes symmetrisches Blockverschlüsselungsverfahren nach dem Rijndael-Algorithmus, der die Funktionen von TKIP weiter verbessert.

    Hinweis

    Um Ihre Daten besser vor Angriffen zu schützen, verwenden Sie WPA2/ WPA2-PSK mit AES.

- **WPA(2)-Schlüssel**
  Tragen Sie hier einen WPA(2)-Schlüssel ein. Dieser WPA(2)-Schlüssel muss sowohl auf der Client-Seite als auch dem Access Point bekannt sein und wird vom Benutzer auf beiden Seiten eingegeben.
  - Bei einem Schlüssel mit 8 bis 63 Zeichen können Sie nur folgende lesbare ASCII-Zeichen verwenden: 0x20 - 0x7e.
  - Bei einem Schlüssel mit genau 64 Zeichen können Sie folgende ASCII-Zeichen verwenden: 0 - 9, a - f und A - F.
- **WPA(2)-Schlüssel bestätigen**
  Bestätigen Sie den oben eingegebenen WPA(2)-Schlüssel.

6.3.1.11 Dot1x Supplicant Einstellungen

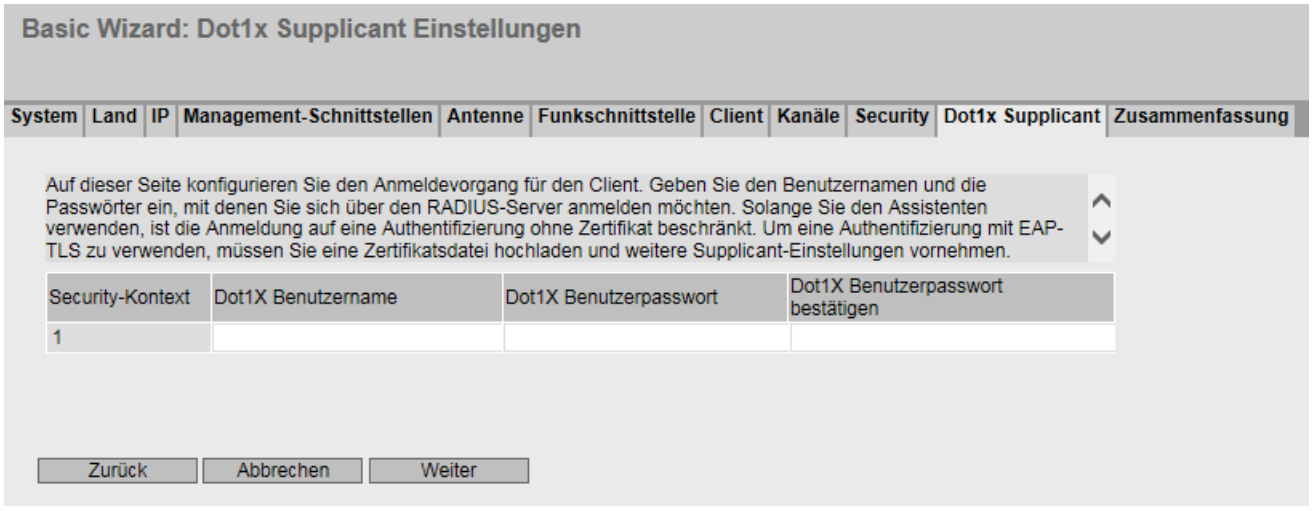
Einleitung

Auf dieser Basic Wizard-Seite konfigurieren Sie den Benutzernamen und das Passwort, mit denen der Client am RADIUS-Server angemeldet wird.

Wenn Sie zusätzliche Authentifizierungsverfahren benötigen, können Sie dies nach Beenden des Basic Wizard unter "Security > WLAN > Client Radius Supplicant" konfigurieren.

Hinweis

Diese Seite ist nur bei Clients oder bei Access Points im Client-Modus verfügbar.



Beschreibung

Die Tabelle 1 enthält folgende Spalten:

- **Security-Kontext**
  Zeigt den Security-Kontext 1 an.
- **Dot1x Benutzername**
  Tragen Sie den Benutzernamen ein, mit dem der Client am RADIUS-Server angemeldet wird.
- **Dot1x Benutzerpasswort**
  Tragen Sie für den oben genannten Benutzernamen das Passwort ein. Mit dieser Kombination wird der Client am RADIUS-Server angemeldet.
  Für die Passwort-Vergabe wird der ASCII-Code 0x20 bis 0x7e verwendet.
- **Dot1x Benutzerpasswort bestätigen**
  Tragen Sie in dieses Eingabefeld erneut das Passwort ein.

6.3.1.12 Dot1x RADIUS Server Settings

Einleitung

Auf dieser Basic Wizard-Seite konfigurieren Sie die Einstellungen für den primären RADIUS Server.

Nach Beenden des Basic Wizards können Sie unter "Security > WLAN > AP Radius-Authenticator" einen Backup-Server und weitere Einstellungen konfigurieren, z. B. Anzahl der Anmeldeversuche.

Hinweis

Diese Seite ist nur im Access Point-Modus verfügbar.

Beschreibung

Die Tabelle enthält folgende Spalten:

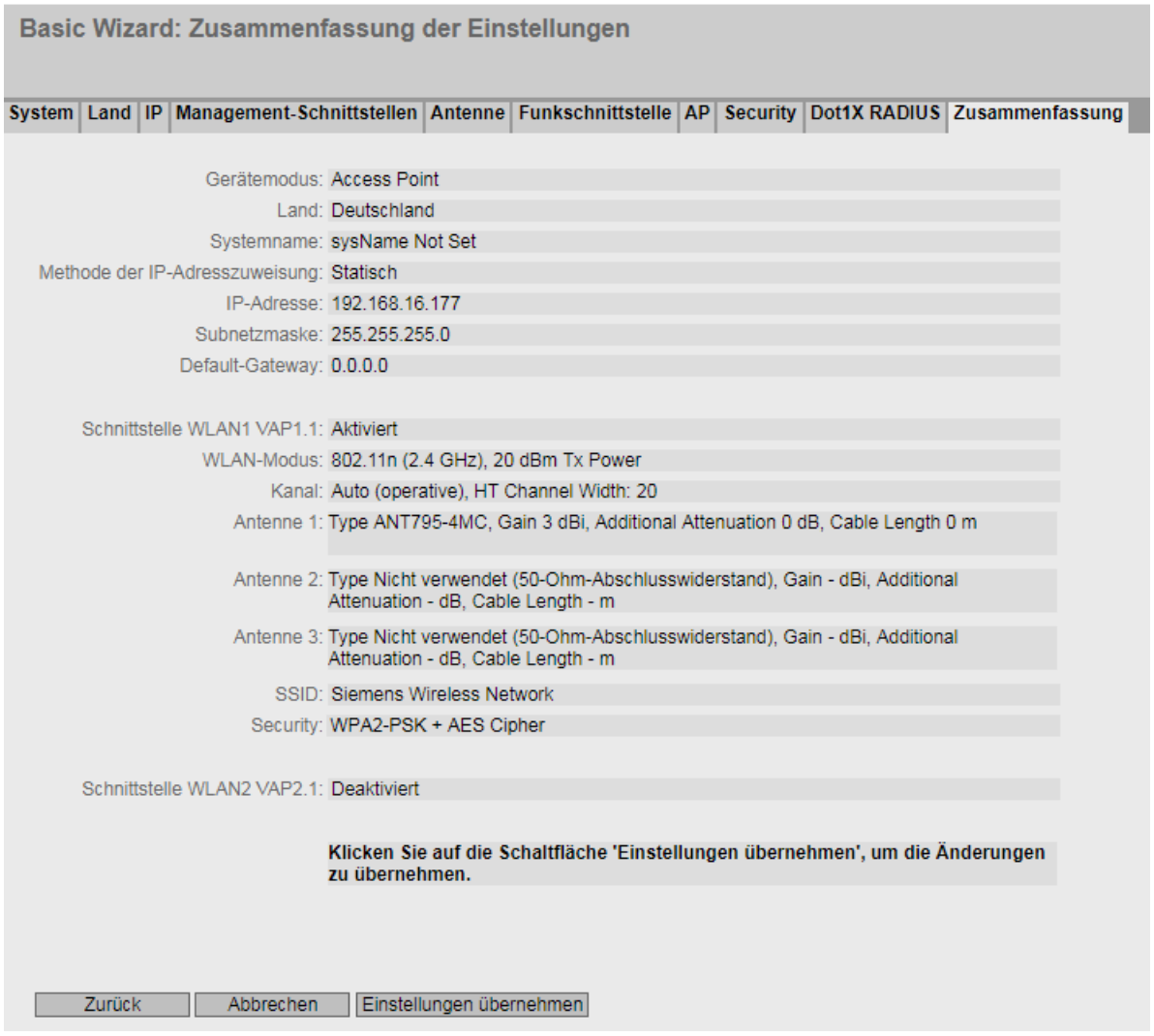
- **Serverrolle**
  Zeigt die Rolle des Servers an.
- **IP-Adresse des Servers**
  Tragen Sie die IP-Adresse des RADIUS Servers ein. Die Verwendung des Computernamens (Namensauflösung via DNS) anstelle der IP-Adresse wird nicht unterstützt.
- **Server-Port**
  Tragen Sie den Port des RADIUS Servers ein.
- **Shared Secret**
  Tragen Sie das Passwort des RADIUS Servers ein.
- **Shared Secret bestätigen**
  Tragen Sie in dieses Eingabefeld erneut das Passwort ein.

6.3.1.13 Zusammenfassung der Einstellungen

Einleitung

Auf dieser Seite werden die Einstellungen zusammengefasst. Der Inhalt der Seite ist abhängig von den eingestellten Parametern und von der Betriebsart des Geräts.

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



Einstellungen übernehmen

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

6.4 Menü "Information"

6.4.1 Startseite

Ansicht der Startseite

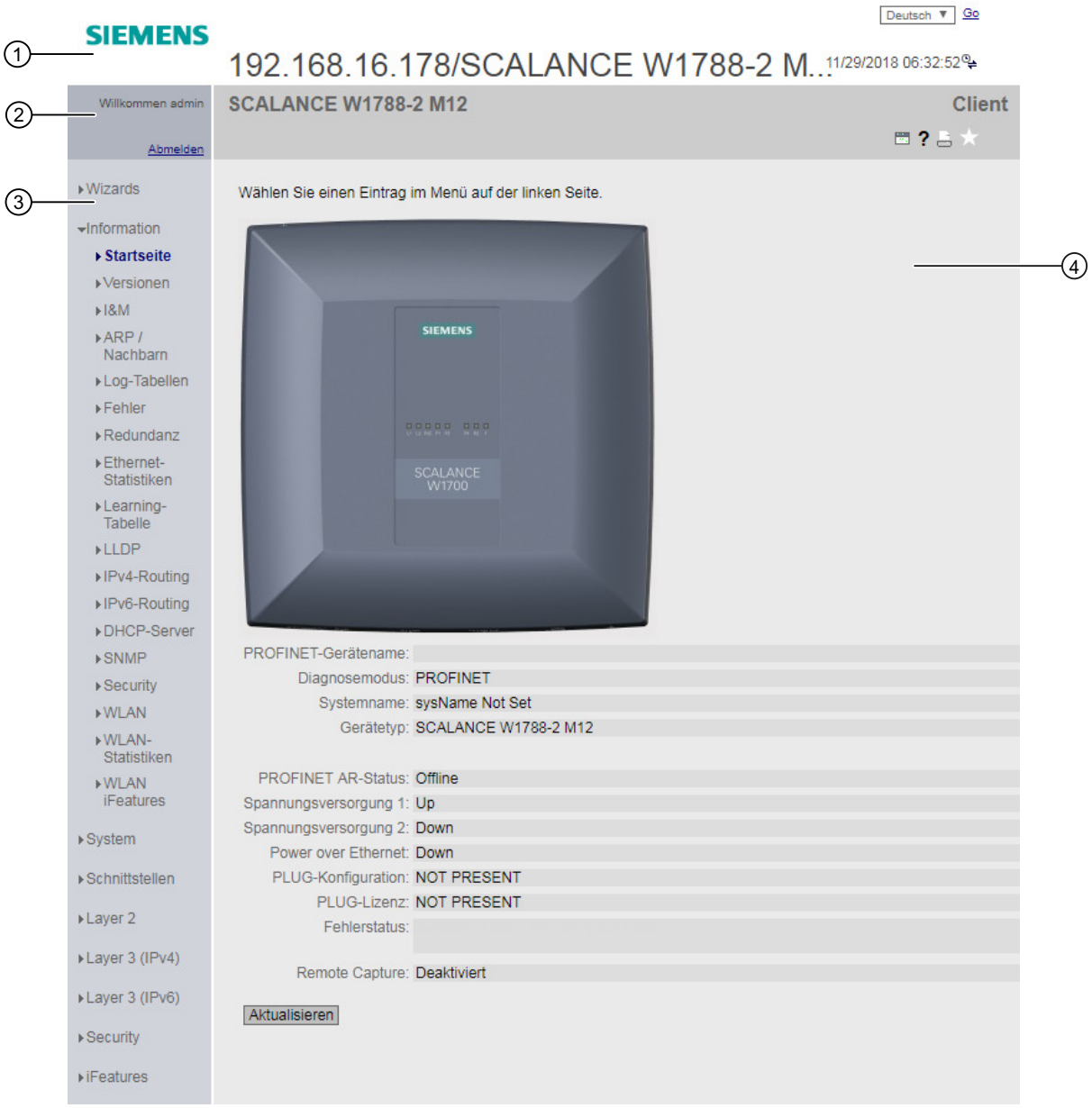
Wenn Sie die IP-Adresse des Geräts eingeben, dann wird Ihnen nach erfolgreicher Anmeldung die Startseite angezeigt. Sie können auf dieser Seite keine Konfigurationen vornehmen.

Allgemeiner Aufbau der WBM-Seiten

Ihnen stehen allgemein folgende Bereiche 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: "Gerätestandort/Systemnamen".
  - "Gerätestandort" enthält die Ortsangabe des Geräts.
    Im Auslieferungszustand wird die IP-Adresse der Ethernet-Schnittstelle angezeigt.
  - "Systemname" ist der Gerätename. Im Auslieferungszustand wird der Gerätetyp angezeigt.

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

Anzeigebereich (2)

Im oberen Teil des Anzeigebereichs befindet sich der Name des aktuell angemeldeten Benutzers sowie der vollständige Titel des aktuell gewählten Menüpunkts.

Im unteren Teil des Anzeigebereichs befindet sich:

- **Abmelden**
  Sie können sich auf jeder WBM-Seite abmelden, indem Sie auf den Link "Abmelden" klicken.
- **Gerätename**
  Zeigt den Namen des Geräts an.
- **Betriebsart**
  Zeigt die Betriebsart an: Access Point.
- **Leuchtdiodensimulation**
  Jedes Gerät verfügt über mehrere Leuchtdioden, die Informationen über den Betriebszustand des Geräts liefern. Abhängig vom Aufstellort ist der direkte Zugang zum Gerät jedoch nicht immer möglich. Aus diesem Grund bietet das Web Based Management eine Simulationsdarstellung für die Leuchtdioden. Nicht belegte Anschlüsse werden als graue LEDs dargestellt. Die Bedeutung der Leuchtdiodenanzeigen ist in der Betriebsanleitung beschrieben.
  Wenn Sie diese Schaltfläche anklicken, rufen Sie das Fenster der Leuchtdiodensimulation auf. Sie können dieses Fenster während des Menüwechsels einblenden und beliebig verschieben. Um die Leuchtdiodensimulation zu schließen, klicken Sie innerhalb des Fensters der Leuchtdiodensimulation auf die Schließen-Schaltfläche.

- **Hilfe** 
  Wenn Sie diese Schaltfläche anklicken, wird die Hilfeseite des aktuell gewählten Menüpunktes in einem neuen Browser-Fenster aufgerufen.
  Auf jeder Hilfeseite gibt es am oberen Rand ein Eingabefeld für die Suchfunktion. Geben Sie dort einen Begriff ein, zu dem Sie weitere Informationen benötigen und starten Sie die Suche durch Betätigen der Eingabetaste. In einem Dialogfeld wird eine Liste mit WBM-Seiten angezeigt, die den gesuchten Begriff enthalten. Nach dem Anklicken eines Listenelements wird die entsprechende WBM-Seite in einem neuen Register des Browsers geöffnet
- **Drucker** 
  Wenn Sie diese Schaltfläche anklicken, wird ein Popup-Fenster geöffnet. Das Popup-Fenster enthält eine Ansicht des Seiteninhalts, die für Drucker optimiert ist.

  Hinweis

  Drucken großer Tabellen

  Wenn Sie große Tabellen ausdrucken wollen, verwenden Sie bitte die "Print-Preview" Funktion Ihres Internet-Browsers.

- **Favoriten**
  Im Lieferzustand ist die Schaltfläche auf allen Seiten deaktiviert  .
  Wenn Sie diese Schaltfläche anklicken, ändert sich das Symbol  und die aktuell geöffnete Seite oder das aktuell geöffnete Register wird als Favorit markiert. Sobald Sie die Schaltfläche einmal aktiviert haben, wird der Navigationsbereich in zwei Register unterteilt. Das erste Register "Menü" enthält alle verfügbaren Menüs, wie bisher. Das zweite Register "Favoriten" enthält alle Seiten/Register, die Sie als Favoriten markiert haben. Im Register "Favoriten" werden die Seiten/Register entsprechend der Struktur im Register "Menü" angeordnet.
  Wenn Sie alle angelegten Favoriten wieder deaktivieren, wird auch das Register "Favoriten" wieder entfernt. Klicken Sie hierzu auf den entsprechenden Seiten/Registern die Schaltfläche  an.
  Sie können die Favoriten-Konfiguration eines Geräts auf der Seite "System > Laden & Speichern" über HTTP oder TFTP speichern, hochladen und löschen.
- **Aktualisieren an**  **/ 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)

Der Inhaltsbereich enthält eine Grafik des Geräts. Die Grafik zeigt immer das Gerät, dessen WBM Sie aufgerufen haben.

Unter dem Gerätebild wird Folgendes angezeigt:

- **PROFINET-Gerätename**
  Zeigt den PROFINET-Gerätenamen an.
- **Diagnosemodus**
  Zeigt an, ob EtherNet/IP oder PROFINET aktiviert ist.
- **Systemname**
  Zeigt den Namen des Geräts an.
- **Gerätetyp**
  Zeigt die Typenbezeichnung des Geräts an.
- **PROFINET AR-Status**
  Zeigt den PROFINET Application Relation Status an.
  - Online
    Zu einem PROFINET Controller besteht eine Verbindung. Der PROFINET Controller hat seine Konfigurationsdaten in das Gerät geladen. Das Gerät kann Statusdaten zum PROFINET Controller senden.
    In diesem Zustand sind die Parameter, die über den PROFINET Controller eingestellt werden, nicht am Gerät konfigurierbar.
  - Offline
    Zu einem PROFINET Controller besteht keine Verbindung.
- **Spannungsversorgung 1 / Spannungsversorgung 2 / Power over Ethernet**
  Status der Spannungsversorgungen 1 und 2 bzw. Power over Ethernet. Die Spannungsversorgung 2 und Power over Ethernet werden nur angezeigt, wenn es die jeweilige Hardware unterstützt. Weitere Informationen dazu finden Sie in der Betriebsanleitung.
- **PLUG-Konfiguration**
  Zeigt den Status der Konfigurationsdaten auf dem PLUG an, siehe Kapitel "System > PLUG > PLUG-Konfiguration".
- **PLUG-Lizenz**
  Zeigt den Status der Lizenz auf dem PLUG an, siehe Kapitel "System > PLUG > PLUG Lizenz".
- **Fehlerstatus**
  Zeigt den Fehlerstatus des Geräts an.
- **Remote Capture**
  Zeigt an, ob die Funktion aktiviert ist.

Häufig verwendete Schaltflächen

Die Seiten des WBM enthalten standardmäßig die folgenden Schaltflächen:

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

  Hinweis

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

  Hinweis

  Das Ändern der Konfigurationsdaten ist nur mit dem Login "admin" möglich.

- **Anlegen von Einträgen mit "Erstellen"**
  Seiten, auf denen Sie neue Einträge erstellen können, haben am unteren Rand die Schaltfläche "Erstellen". Klicken Sie auf diese Schaltfläche, um einen neuen Eintrag zu erstellen.
- **Löschen von Einträgen mit "Löschen"**
  Seiten, auf denen Sie Einträge löschen können, haben am unteren Rand die Schaltfläche "Löschen". Klicken Sie auf diese Schaltfläche, um die zuvor markierten Einträge aus dem Gerätespeicher zu löschen. Der Löschvorgang bewirkt auch eine Aktualisierung der Seite im WBM.
- **Vorwärts blättern mit "Weiter"**
  Bei Seiten mit sehr vielen Datensätzen ist die Anzahl der auf einer Seite darstellbaren Datensätze beschränkt. Klicken Sie auf die Schaltfläche "Weiter", um innerhalb der Datensätze vorwärts zu blättern.
- **Rückwärts blättern mit "Zurück"**
  Bei Seiten mit sehr vielen Datensätzen ist die Anzahl der auf einer Seite darstellbaren Datensätze beschränkt. Klicken Sie auf die Schaltfläche "Zurück", um innerhalb der Datensätze rückwärts zu blättern.
- **Löschen der Anzeige mit "Leeren"**
  Bei Seiten mit Ablaufprotokollen können Sie alle Tabelleneinträge gleichzeitig löschen, unabhängig davon, ob Filter ausgewählt sind. Die Anzeige wird dabei geleert. Erst wenn nach dem Wiederherstellen der Werkseinstellungen das Gerät neu gestartet ist, wird der Neustart-Zähler zurückgesetzt.
  Klicken Sie auf die Schaltfläche "Leeren", um den Datensatz komplett zu löschen.
- **Schaltfläche "Alle anzeigen"**
  Bei Seiten mit sehr vielen Datensätzen können Sie alle Einträge anzeigen lassen. Klicken Sie auf die Schaltfläche "Alle anzeigen", um alle Einträge auf der Seite anzuzeigen. Beachten Sie, dass das Anzeigen aller Meldungen einige Zeit beanspruchen kann.

- **Klappliste für Seitenwechsel**
  Bei Seiten mit sehr vielen Datensätzen können Sie zur gewünschten Seite navigieren. Wählen Sie aus der Klappliste die betreffende Seite aus, um diese anzeigen zu lassen.
- **Schaltfläche "Zähler zurücksetzen"**
  Klicken Sie auf "Zähler zurücksetzen", um alle Zähler zurückzusetzen. Die Zähler werden durch einen Neustart zurückgesetzt.

Meldungen

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

Hinweis

Unterbrechung des Speichervorgangs

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

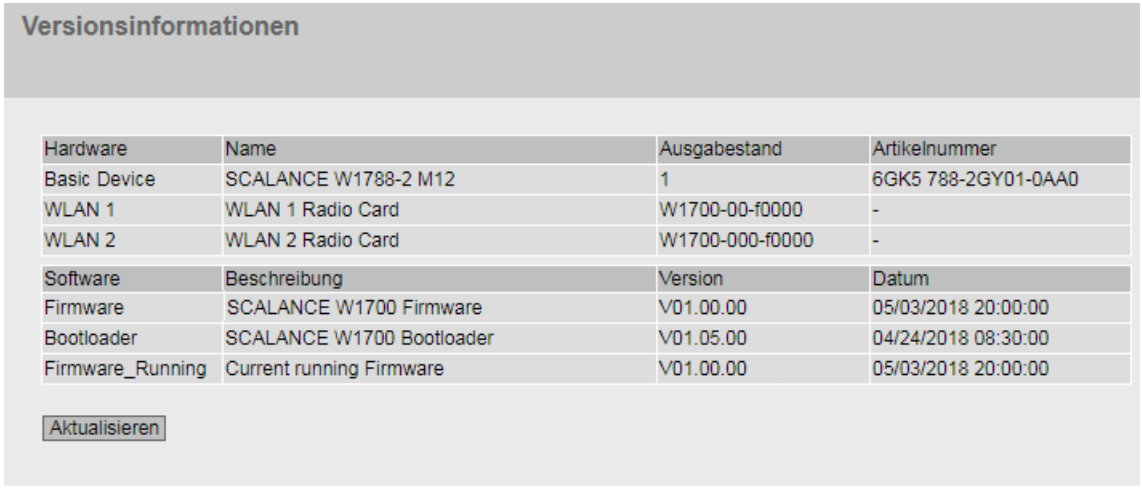
Während des Speichervorgangs wird die Meldung "Die Konfigurationsdaten werden gespeichert. Schalten Sie das Gerät nicht aus." angezeigt.

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

6.4.2 Versionen

Versionen von Hardware und Software

Diese Seite zeigt die Ausgabestände der Hardware und der Software des Geräts. Sie können auf dieser Seite keine Konfigurationen vornehmen.



Beschreibung

Die Tabelle 1 gliedert sich in folgende Spalten:

- **Hardware**
  - Basic Device
    Zeigt das Grundgerät an
  - WLAN1 / WLAN 2
    Zeigt die verfügbare Funkkarte an
- **Name**
  Zeigt den Namen des Geräts oder des Moduls an.
- **Ausgabestand**
  Zeigt den Hardware Ausgabestand des Geräts an. Bei der Funkkarte wird nur dann ein Ausgabestand angezeigt, wenn die WLAN-Schnittstelle eingeschaltet ist.
- **Artikelnummer**
  Zeigt die Artikelnummer des Geräts oder des beschriebenen Moduls an.

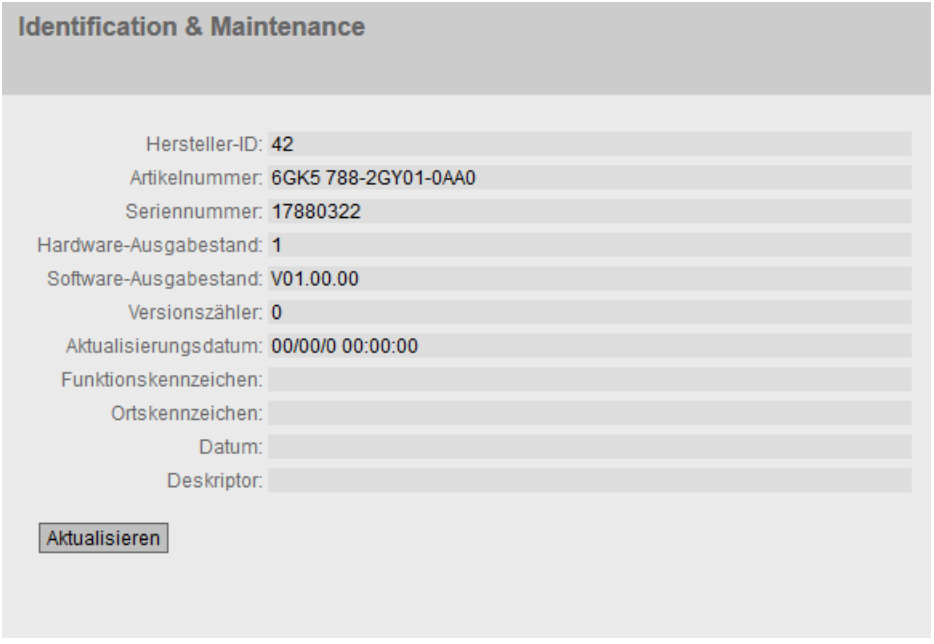
Die Tabelle 2 gliedert sich in folgende Spalten:

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

6.4.3 I&M

Hersteller- und Wartungsdaten

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



Beschreibung

Die Tabelle gliedert sich in folgende Zeilen:

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

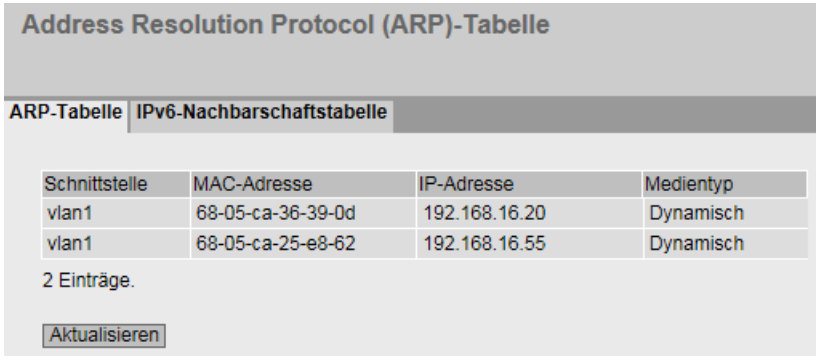
- **Funktionskennzeichen**
  Zeigt das Funktionskennzeichen (Anlagenkennzeichen) des Geräts an. Das Anlagenkennzeichen (AKZ) wird bei der Projektierung des Geräts mit HWKonfig von STEP7 angelegt.
- **Ortskennzeichen**
  Zeigt das Ortskennzeichen des Geräts an. Das Ortskennzeichen (OKZ) wird bei der Projektierung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

6.4.4 ARP / Nachbarn

6.4.4.1 ARP-Tabelle

Zuordnung von MAC-Adresse und IPv4-Adresse

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



Beschreibung der angezeigten Werte

Die Tabelle gliedert sich in folgende Spalten:

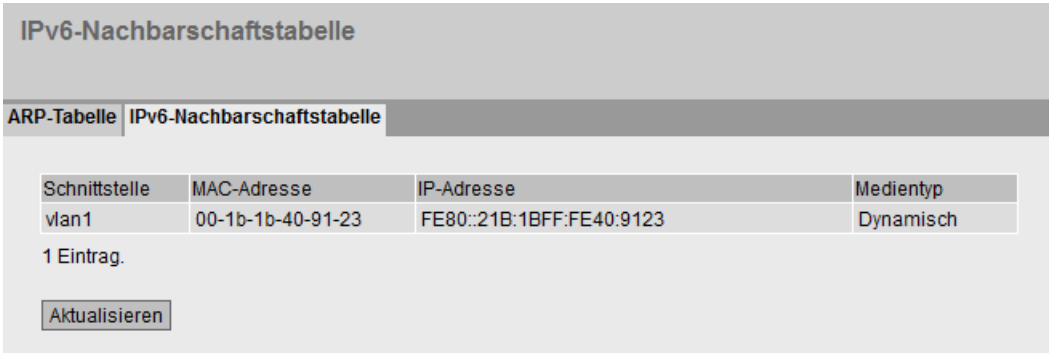
- **Schnittstelle**
  Zeigt die Schnittstelle an, über die der Zeileneintrag gelernt wurde.
- **MAC-Adresse**
  Zeigt die MAC-Adresse des Ziel- oder Quellgeräts an.

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

6.4.4.2 IPv6-Nachbarschaftstabelle

Zuordnung von MAC-Adresse und IPv6-Adresse

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



Beschreibung der angezeigten Werte

Die Tabelle gliedert sich in folgende Spalten:

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

6.4.5 Log-Tabellen

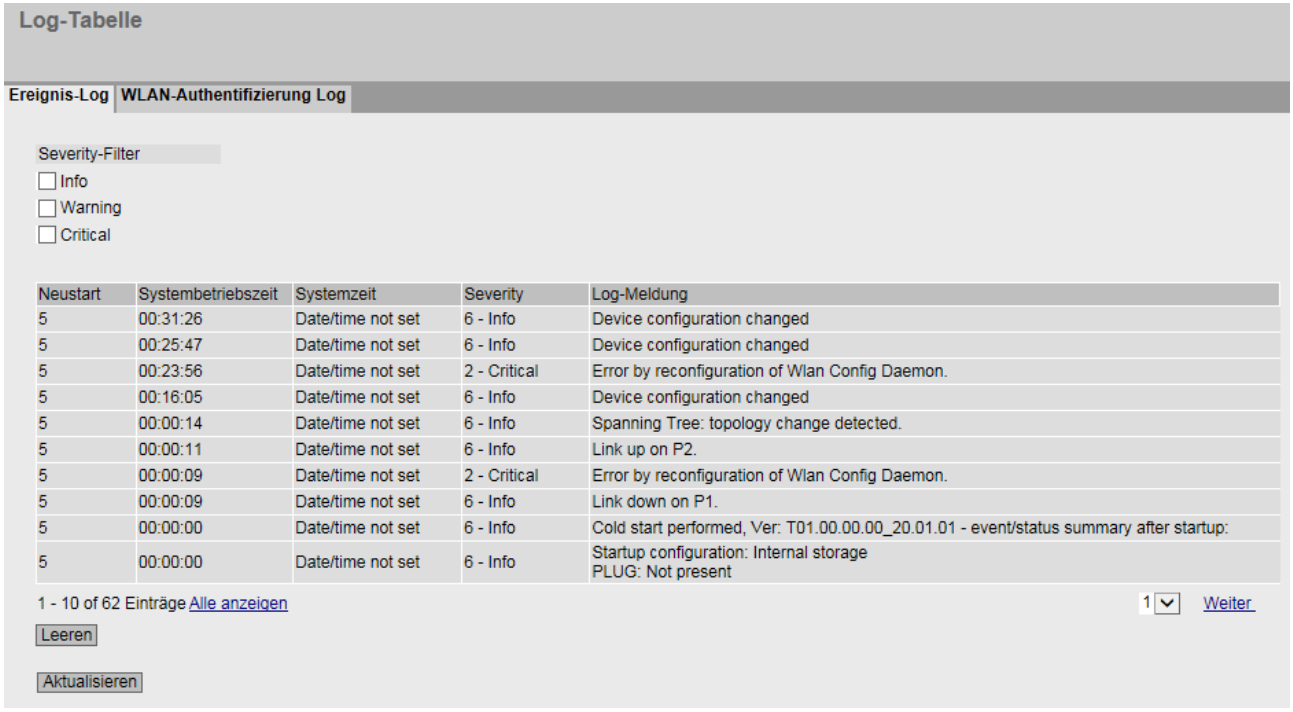
6.4.5.1 Ereignis-Log

Protokollierung von Ereignissen

Das Gerät bietet die Möglichkeit, auftretende Ereignisse zu protokollieren, die Sie zum Teil auf der Seite des Menüs System > Ereignisse festlegen können. So kann beispielsweise festgehalten werden, wann ein Authentifizierungsversuch fehlgeschlagen ist, oder wann sich der Verbindungsstatus eines Ports geändert hat.

Der Inhalt der Ereignisprotokoll-Tabelle bleibt auch nach dem Ausschalten des Geräts erhalten.

Sie können auf dieser Seite keine Konfigurationen vornehmen.



Beschreibung

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

  Hinweis

  Pro Severity sind maximal 2000 Einträge in der Tabelle möglich. Wenn bei einer Severity die maximale Anzahl der Einträge erreicht ist, werden die ältesten Einträge dieser Severity in der Tabelle überschrieben. Die Tabelle verbleibt permanent im Speicher.

  - Info
    Information
    Wenn dieser Parameter aktiviert ist, werden alle Einträge der Kategorien "Info" angezeigt.
  - Warning
    Warnungen
    Wenn dieser Parameter aktiviert ist, werden alle Einträge der Kategorien "Warning" angezeigt.
  - Critical
    Kritisch
    Wenn dieser Parameter aktiviert ist, werden alle Einträge der Kategorien "Critical" angezeigt.

Die Tabelle gliedert sich in folgende Spalten:

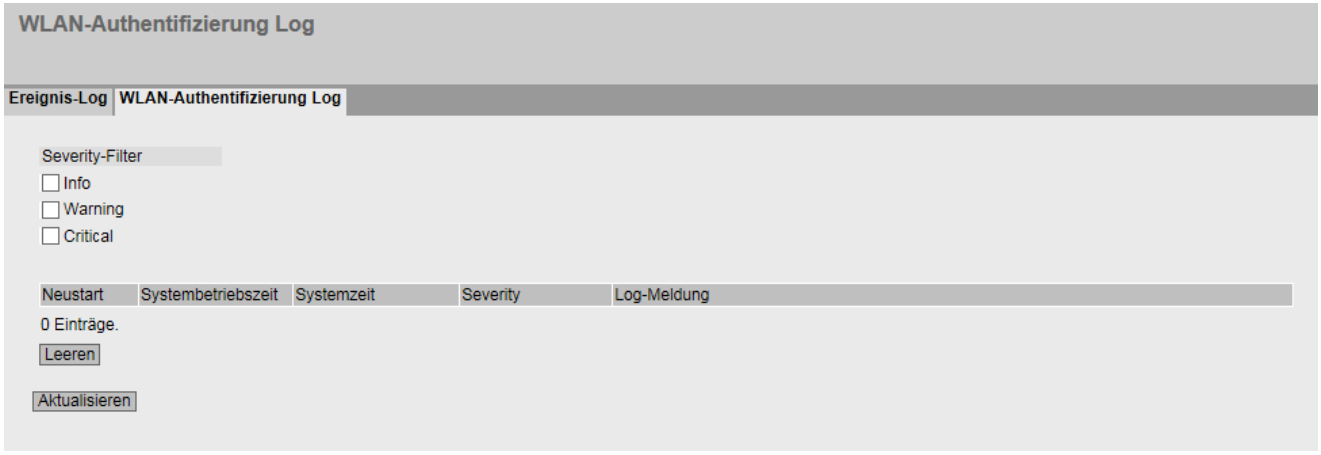
- **Neustart**
  Zählt die Anzahl der Neustarts seit dem letzten Zurücksetzen auf Werkseinstellungen und gibt an, nach welchem Neustart des Geräts das entsprechende Ereignis aufgetreten ist.
- **Systembetriebszeit**
  Zeigt die Laufzeit des Geräts seit dem letzten Neustart an, zu der das beschriebene Ereignis aufgetreten ist.
- **Systemzeit**
  Zeigt das Datum und die Uhrzeit an, zu der das beschriebene Ereignis aufgetreten ist.
- **Severity**
  Zeigt den Schweregrad der Meldung an.
- **Log-Meldung**
  Zeigt eine Kurzbeschreibung des eingetretenen Ereignisses an. Eine Liste der möglichen Meldungen finden Sie im Anhang D (Seite 381) des Projektierungshandbuches.

Wenn die Systemzeit gesetzt ist, wird auch die Zeit angezeigt, bei der das Ereignis eingetreten ist.

6.4.5.2 WLAN-Authentifizierung Log

Protokollierung von Authentifizierungsversuchen

Die Seite zeigt in tabellarischer Form Informationen zu erfolgreichen oder fehlgeschlagenen Authentifizierungsversuchen.



Sie können auf dieser Seite keine Konfigurationen vornehmen.

Beschreibung

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

  Hinweis

  Pro Severity sind maximal 2000 Einträge in der Tabelle möglich. Wenn bei einer Severity die maximale Anzahl der Einträge erreicht ist, werden die ältesten Einträge dieser Severity in der Tabelle überschrieben. Die Tabelle verbleibt permanent im Speicher.

  - Info
    Information
    Wenn dieser Parameter aktiviert ist, werden alle Einträge der Kategorien "Info" angezeigt.
  - Warning
    Warnungen
    Wenn dieser Parameter aktiviert ist, werden alle Einträge der Kategorien "Warning" angezeigt.
  - Critical
    Kritisch
    Wenn dieser Parameter aktiviert ist, werden alle Einträge der Kategorien "Critical" angezeigt.

Die Tabelle gliedert sich in folgende Spalten:

- **Neustart**
  Zählt die Anzahl der Neustarts seit dem letzten Zurücksetzen auf Werkseinstellungen und gibt an, nach welchem Neustart des Geräts das entsprechende Ereignis aufgetreten ist.
- **Systembetriebszeit**
  Zeigt die Laufzeit des Geräts seit dem letzten Neustart an, zu der das beschriebene Ereignis aufgetreten ist.
- **Systemzeit**
  Zeigt das Datum und die Uhrzeit an, zu der das beschriebene Ereignis aufgetreten ist.
- **Severity**
  Zeigt den Schweregrad der Meldung an.
- **Log-Meldung**
  Zeigt eine Kurzbeschreibung des eingetretenen Ereignisses an. Eine Liste der möglichen Meldungen finden Sie im Anhang D (Seite 381) des Projektierungshandbuches.

Wenn die Systemzeit gesetzt ist, wird auch die Zeit angezeigt, bei der das Ereignis eingetreten ist.

6.4.6 Fehler

Fehlerstatus

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

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

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

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

Beschreibung

Die Seite enthält folgende Felder:

- **Anzahl der gemeldeten Fehler**
  Zeigt an, wie oft die Fehler-LED eingeschaltet wurde und nicht wie viele Fehler aufgetreten sind.
- **Schaltfläche "Zähler zurücksetzen"**
  Über die Schaltfläche wird die Anzahl zurückgesetzt. Der Zähler wird durch einen Neustart zurückgesetzt.

Die Tabelle enthält die folgenden Spalten:

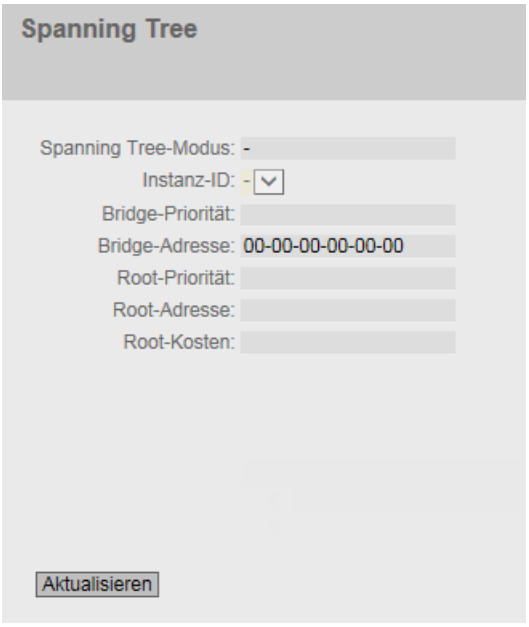
- **Fehlerzeitpunkt**
  Zeigt die Laufzeit des Geräts seit dem letzten Neustart an, zu der der beschriebene Fehler aufgetreten ist.
- **Fehlerbeschreibung**
  Zeigt eine Kurzbeschreibung des eingetretenen Fehlers an.
- **Fehlerstatus löschen**
  Manche Fehler lassen sich quittieren und damit aus der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

6.4.7 Redundanz

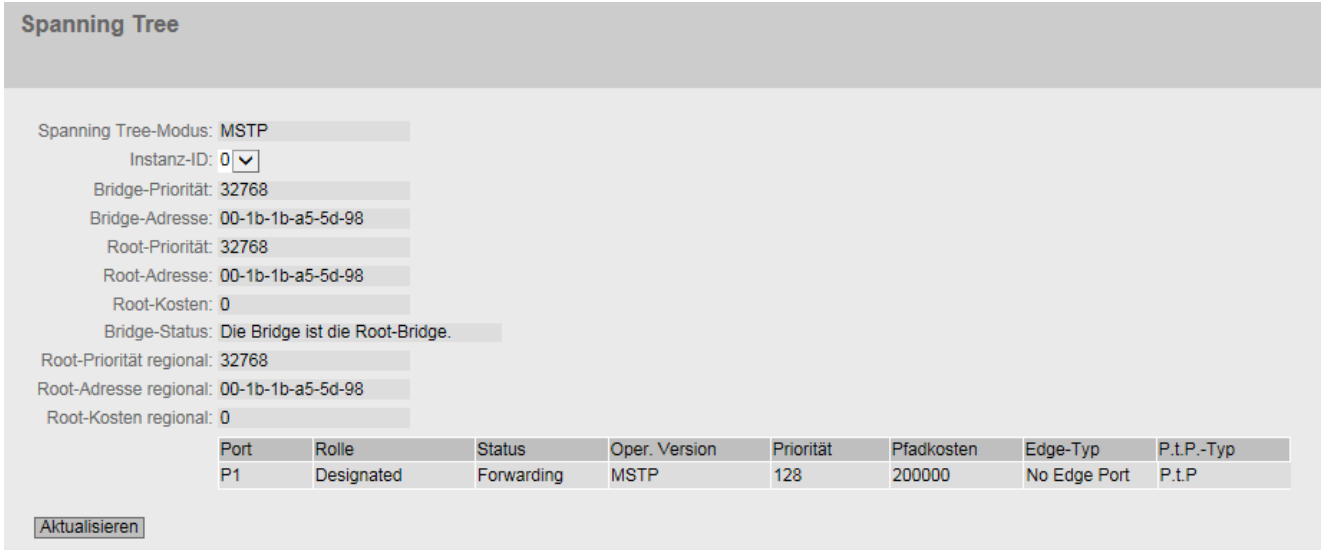
Einleitung

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

Wenn Spanning Tree ausgeschaltet ist, werden nur Basisinformationen zu diesem Gerät angezeigt.



Wenn Spanning Tree eingeschaltet ist, werden die Informationen zum Status der aus der Klappliste "Instanz-ID" ausgewählten Instanz und in der Tabelle die Informationen der konfigurierten Ports angezeigt. Dabei sind die dargestellten Informationen abhängig von Modus des Spanning Tree.



Beschreibung

Die Seite enthält folgende Felder:

- **Spanning Tree-Modus**
  Zeigt den eingestellten Modus an. Den Modus legen Sie bei "Layer 2 > Konfiguration" und bei "Layer 2 > MSTP > Allgemein" fest.
  Folgende Werte sind möglich:
  - '-'
  - STP
  - RSTP
  - MSTP
- **Instanz-ID**
  Zeigt die Nummer der Instanz an. Der Parameter ist abhängig vom projektierten Modus.
- **Bridge-Priorität / Root-Priorität**
  Anhand der Bridge-Priorität wird festgelegt, welches Gerät Root-Bridge wird. Die Bridge mit der höchsten Priorität (d. h. dem kleinsten Wert für diesen Parameter) wird Root-Bridge. Wenn in einem Netz mehrere Geräte die gleiche Priorität besitzen, dann wird das Gerät Root-Bridge, dessen MAC-Adresse den niedrigsten Zahlenwert hat. Beide Parameter, Bridge-Priorität und MAC-Adresse, bilden zusammen die Bridge-Kennung. Da die Root Bridge alle Wegeänderungen verwaltet, sollte sie wegen der Laufzeit der Telegramme möglichst zentral angeordnet sein. Der Wert für die Bridge-Priorität ist ein ganzzahliges Vielfaches von 4096 mit einem Wertebereich von 0 bis 32768.
- **Bridge-Adresse / Root-Adresse**
  Die Bridge-Adresse zeigt die MAC-Adresse des Geräts und die Root-Adresse zeigt die MAC-Adresse der Root-Bridge an.
- **Root-Kosten**
  Die Pfadkosten von diesem Gerät bis zur Root-Bridge.
- **Bridge-Status**
  Zeigt den Status der Bridge an, z. B. ob das Gerät die Root-Bridge ist.
- **Root-Priorität regional** (nur bei MSTP verfügbar)
  Beschreibung siehe Bridge-Priorität / Root-Priorität
- **Root-Adresse regional** (nur bei MSTP verfügbar)
  Zeigt die MAC-Adresse der regionalen Root Bridge.
- **Root-Kosten regional** (nur bei MSTP verfügbar)
  Zeigt die Pfadkosten von diesem Gerät bis zur regionalen Root Bridge an.

Die Tabelle enthält folgende Felder:

- **Port**
  Zeigt den Port an, über den das Gerät kommuniziert.
- **Rolle**
  Zeigt den Status des Ports an. Folgende Werte sind möglich:
  - Disabled
    Der Port wurde manuell aus dem Spanning Tree entfernt und wird vom Spanning Tree nicht mehr berücksichtigt.
  - Designated
    Die Ports, die von der Root-Bridge wegführen.
  - Alternate
    Der Port mit einem alternativen Weg zu einem Netzwerksegment
  - Backup
    Wenn ein Switch mehrere Ports zu dem gleichen Netzwerksegment hat, wird der "schlechtere" Port zum Backup-Port.
  - Root
    Der Port, der den besten Weg zur Root Bridge bietet.
  - Master
    Dieser Port zeigt zu einer Root-Bridge, die außerhalb der MST-Region liegt.
- **Status**
  Zeigt den momentanen Status an, in dem sich der Port befindet. Die Werte werden nur angezeigt. Der Parameter ist abhängig vom projektierten Protokoll. Folgende Status sind möglich:
  - Discarding
    Der Port empfängt BPDU-Telegramme. Andere aus- oder eingehende Telegramme werden verworfen.
  - Listening
    Der Port empfängt und sendet BPDU-Telegramme. Der Port ist in den Spanning Tree-Algorithmus einbezogen. Andere aus- und eingehende Telegramme werden verworfen.
  - Learning
    Der Port lernt aktiv die Topologie, d. h. die Teilnehmeradressen. Andere aus- und eingehende Telegramme werden verworfen.
  - Forwarding
    Der Port ist nach der Umkonfigurationszeit aktiv im Netz. Der Port empfängt und sendet Datentelegramme.
- **Oper. Version**
  Beschreibt die Art des Spanning Tree, in dem der Port arbeitet
- **Priorität**
  Kann der vom Spanning-Tree ermittelte Weg alternativ über mehrere Ports eines Geräts führen, so wird der Port mit der höchsten Priorität (d. h. dem kleinsten Wert für diesen Parameter) ausgewählt. Für die Priorität kann ein Wert von 0 bis 240 in 16er Schritte eingegeben werden. Wenn Sie einen Wert eingeben, der nicht durch 16 teilbar ist, wird der Wert automatisch angepasst. Der Standardwert ist 128.

- **Pfadkosten**
  Dieser Parameter dient zur Berechnung des zu wählenden Weges. Es wird die Strecke mit dem geringsten Wert als Weg ausgewählt. Haben mehrere Ports eines Geräts den gleichen Wert, wird der Port mit der niedrigsten Portnummer ausgewählt.
  Ist der Wert im Feld "kalk. Kosten" "0", so wird der automatisch ermittelte Wert angezeigt. Im anderen Fall wird der Wert des Feldes "kalk. Kosten" angezeigt.
  Die Ermittlung der Wegekosten richtet sich maßgeblich nach der Übertragungsgeschwindigkeit. Je höher die erzielbare Übertragungsgeschwindigkeit ist, umso kleiner ist der Wert für die Wegekosten.
  Typische Werte für Wegekosten bei Rapid Spanning Tree:
  - 10.000 Mbit/s = 2.000
  - 1000 Mbit/s = 20.000
  - 100 Mbit/s = 200.000
  - 10 Mbit/s = 2.000.000.
- **Edge-Typ**
  Zeigt den Typ der Verbindung an. Folgende Werte sind möglich:
  - Edge Port
    An diesem Port befindet sich ein Endgerät.
  - No Edge Port
    An diesem Port befindet sich ein Spanning Tree- oder Rapid Spanning Tree-Gerät.
- **P.t.P.-Typ**
  Zeigt die Art der Punkt-zu-Punkt-Verbindung an. Folgende Werte sind möglich:
  - P.t.P.
    Bei Halbduplex wird von einer Punkt-zu-Punkt-Verbindung ausgegangen.
  - Shared Media
    Bei einer Vollduplexverbindung wird nicht von einer Punkt-zu-Punkt-Verbindung ausgegangen.

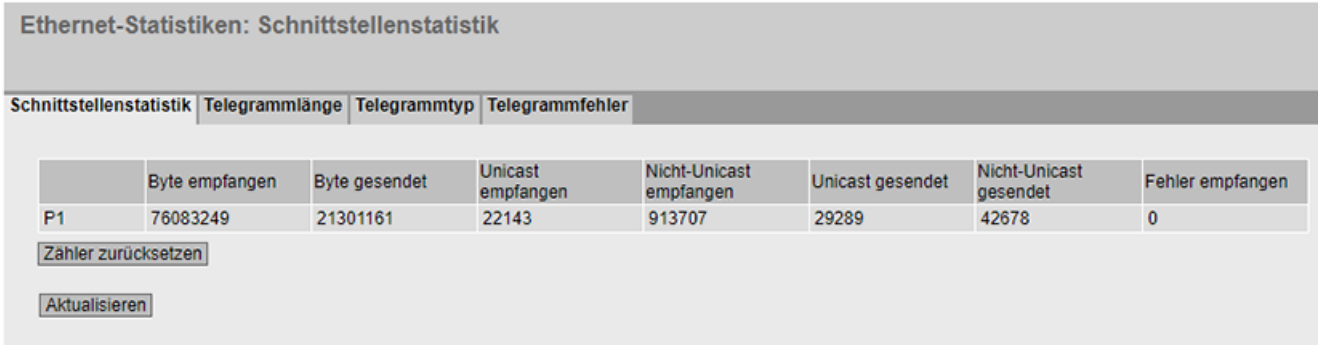
    Hinweis

    Punkt zu Punkt-Verbindung bedeutet eine direkte Verbindung zwischen zwei Geräten. Eine Shared Media-Verbindung ist z. B. eine Verbindung zu einem Hub.

6.4.8 Ethernet-Statistiken

6.4.8.1 Schnittstellenstatistik

Die Seite zeigt die Statistik aus der Schnittstellentabelle der Management Information Base (MIB).



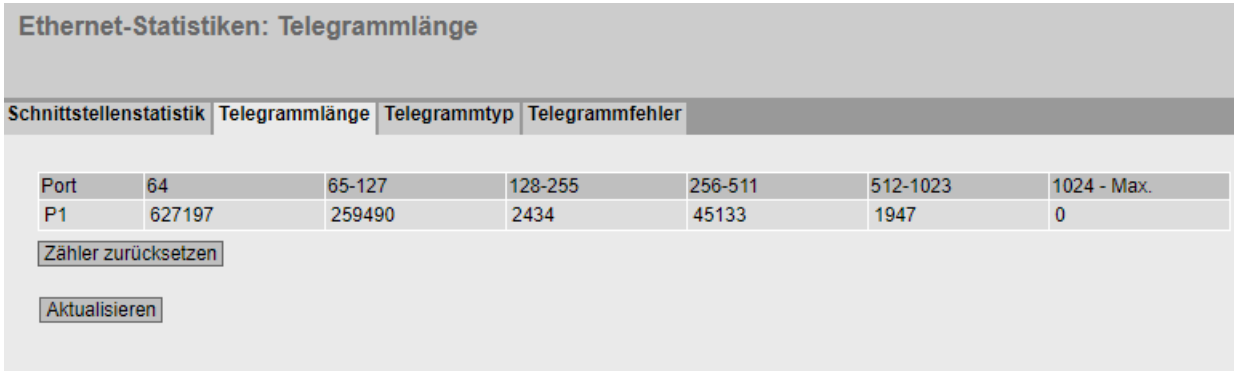
Beschreibung

- **Byte empfangen**
  Zeigt die Anzahl der empfangenen Bytes an.
- **Byte gesendet**
  Zeigt die Anzahl der gesendeten Bytes an.
- **Unicast empfangen**
  Zeigt die Anzahl der empfangenen Unicast-Telegramme an.
- **Nicht-Unicast empfangen**
  Zeigt die Anzahl der empfangenen Telegramme an, die nicht vom Telegrammtyp Unicast sind.
- **Unicast gesendet**
  Zeigt die Anzahl der gesendeten Unicast-Telegramme an.
- **Nicht-Unicast gesendet**
  Zeigt die Anzahl der gesendeten Telegramme an, die nicht vom Telegrammtyp Unicast sind.
- **Fehler empfangen**
  Zeigt die Anzahl aller möglichen RX-Fehler an, siehe Register "Telegrammfehler".
- **Schaltfläche "Zähler zurücksetzen"**
  Klicken Sie auf "Zähler zurücksetzen", um alle Zähler zurückzusetzen. Die Zähler werden durch einen Neustart zurückgesetzt.

6.4.8.2 Telegrammlänge

Telegramme sortiert nach Länge

Diese Seite zeigt, wie viele Telegramme mit welcher Größe an jedem Port empfangen wurden. Sie können auf dieser Seite keine Konfigurationen vornehmen.



Beschreibung

- **Port**
  Zeigt die verfügbaren Ports an.
- **Telegrammlängen**
  Die weiteren Spalten hinter der jeweiligen Portnummer enthalten die absoluten Zahlen der eingegangenen Telegramme entsprechend ihrer Telegrammlänge.
  Dabei wird in folgenden Telegrammlängen unterschieden:
  - 64 Byte
  - 65 - 127 Byte
  - 128 - 255 Byte
  - 256 - 511 Byte
  - 512 - 1023 Byte
  - 1024 - Max.
- **Schaltfläche "Zähler zurücksetzen"**
  Klicken Sie auf "Zähler zurücksetzen", um alle Zähler zurückzusetzen. Die Zähler werden durch einen Neustart zurückgesetzt.

6.4.8.3 Telegrammtyp

Empfangene Telegramme sortiert nach Telegrammtyp

Diese Seite zeigt, wie viele Telegramme des Typs "Unicast", "Multicast" und "Broadcast" an jedem Port empfangen wurden. Sie können auf dieser Seite keine Konfigurationen vornehmen.

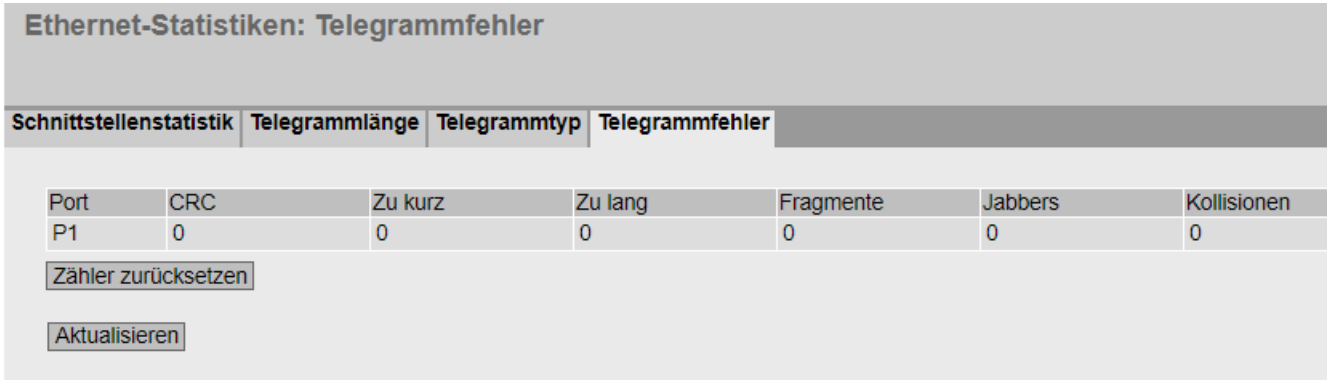
Beschreibung

- **Port**
  Zeigt die verfügbaren Ports an.
- **Unicast / Multicast / Broadcast**
  Die weiteren Spalten hinter der jeweiligen Portnummer enthalten die absoluten Zahlen der eingegangenen Telegramme entsprechend der Telegrammtypen "Unicast", "Multicast" und "Broadcast"
- **Schaltfläche "Zähler zurücksetzen"**
  Klicken Sie auf "Zähler zurücksetzen", um alle Zähler zurückzusetzen. Die Zähler werden durch einen Neustart zurückgesetzt.

6.4.8.4 Telegrammfehler

Fehlerhaft empfangene Telegramme

Die Seite zeigt, wie viele fehlerhafte Telegramme pro Port empfangen wurden. Sie können auf dieser Seite keine Konfigurationen vornehmen.



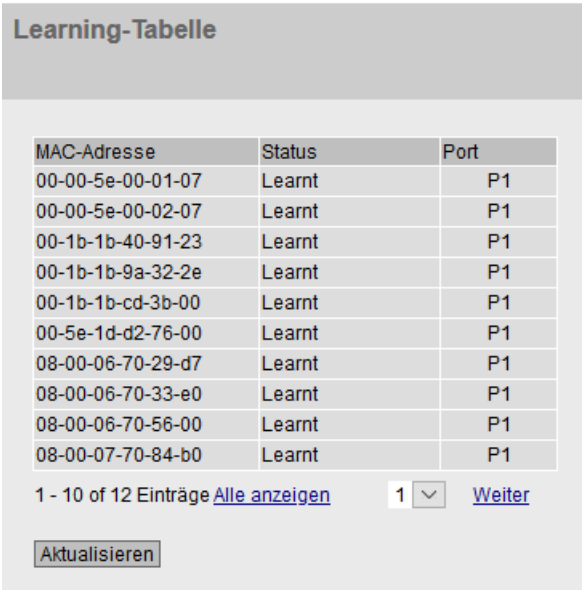
Beschreibung

- **Port**
  Zeigt die verfügbaren Ports an.
- **Fehlertypen**
  Die weiteren Spalten hinter der jeweiligen Portnummer enthalten die absoluten Zahlen der eingegangenen Telegramme entsprechend ihres Fehlers.
  Dabei wird in den Spalten der Tabelle nach folgenden Fehlern unterschieden:
  - CRC (Cyclic Redundancy Code)
    Die Paketlänge beträgt zwischen 64 und 2048 Byte. Die CRC des Pakets ist ungültig.
  - Zu kurz
    Die Paketlänge ist kleiner als 64 Byte. Die CRC des Pakets ist gültig.
  - Zu lang
    Die Paketlänge ist größer als 2048 Byte. Die CRC des Pakets ist gültig.
  - Fragmente
    Die Paketlänge ist kleiner als 64 Byte. Die CRC des Pakets ist ungültig.
  - Jabbers
    Die Telegrammlänge ist größer als 2048 Byte. Die CRC des Pakets ist ungültig.
  - Kollisionen
    Telegramme, bei denen ein Kollisions-Ereignis erkannt wurde.
- **Schaltfläche "Zähler zurücksetzen"**
  Klicken Sie auf "Zähler zurücksetzen", um alle Zähler zurückzusetzen. Die Zähler werden durch einen Neustart zurückgesetzt.

6.4.9 Learning-Tabelle

Adressfilterung

Diese WBM-Seite zeigt den aktuellen Inhalt der Learning Table. In dieser Tabelle sind die Quelladressen von Unicast-Adresstelegrammen aufgeführt.



Beschreibung

Die Tabelle enthält folgende Spalten:

- **VLAN-ID**
  Zeigt die VLAN-ID des Teilnehmers.

  Hinweis

  Diese Spalte erscheint nur dann in der Tabelle, wenn ein VLAN konfiguriert ist.

- **MAC-Adresse**
  Zeigt die MAC-Adresse des Teilnehmers.

- **Status**
  Zeigt den Status jedes Adresseintrags:
  - Learnt
    Die angegebene Adresse wurde durch Empfang eines Telegramms dieses Teilnehmers gelernt und werden nach Ablauf der Aging Time wieder gelöscht, sollten keine weiteren Pakete dieses Teilnehmers empfangen werden.
  - Invalid
    Diese Werte werden nicht ausgewertet.
- **Port**
  Zeigt an, über welchen Port der Teilnehmer mit der angegebenen Adresse erreichbar ist. Vom Gerät empfangene Telegramme, deren Zieladresse mit dieser Adresse übereinstimmen, werden an diesen Port weitergegeben.

6.4.10 LLDP

Status der Nachbarschaftstabelle

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

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

Beschreibung

Die Tabelle enthält folgende Spalten:

- **Systemname**
  Systemname des angeschlossenen Geräts.
- **Geräte-ID**
  Gerätekennung des angeschlossenen Geräts. Die Geräte-ID entspricht dem Gerätenamen, der über SINEC PNI (STEP 7) vergeben wird. Wenn kein Gerätename vergeben ist, wird die MAC-Adresse des Geräts angezeigt.
- **Lokale Schnittstelle**
  Der Port, an dem das Gerät die Informationen empfangen hat.

- **Speicherzeit**
  Speicherzeit in Sekunden
  Ein Eintrag bleibt für die hier angegebene Zeit im Gerät gespeichert. Wenn das Gerät in dieser Zeit keine neuen Informationen von dem angeschlossenen Gerät erhält, wird der Eintrag gelöscht.
- **Eigenschaft**
  Zeigt die Eigenschaften des angeschlossenen Geräts an:
  - Router
  - Bridge
  - Telephone
  - DOCSIS Cable Device
  - WLAN Access Point
  - Repeater
  - Station
  - Other
- **Port-ID**
  Port des angeschlossenen Geräts, mit dem das Gerät verbunden ist. Wenn keine Port-ID vergeben ist, wird die MAC-Adresse des angeschlossenen Geräts angezeigt.

6.4.11 IPv4-Routing

Einleitung

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

Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

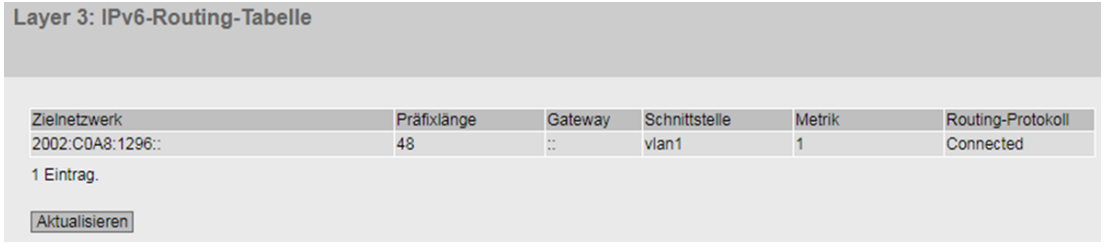
- **Zielnetzwerk**
  Zeigt die Zieladresse dieser Route an.
- **Subnetzmaske**
  Zeigt die Subnetzmaske dieser Route an.

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

6.4.12 IPv6-Routing

Einleitung

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



Beschreibung

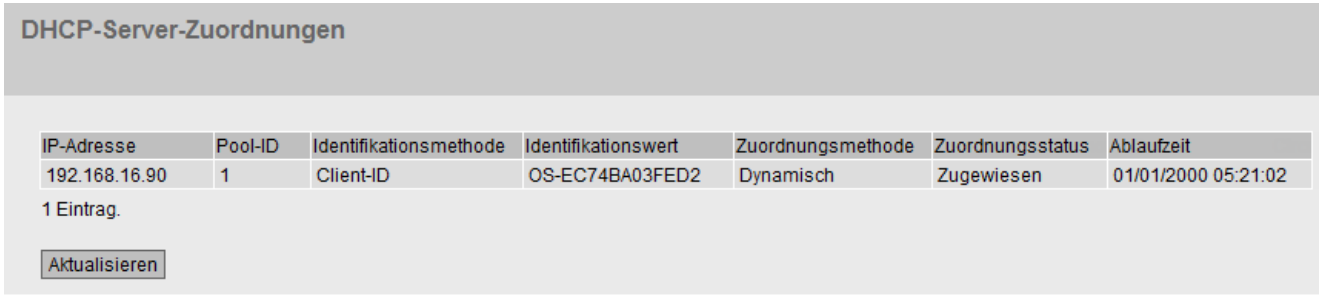
Die Tabelle gliedert sich in folgende Spalten:

- **Zielnetzwerk**
  Zeigt die Ziel-Adresse dieser Route an.
- **Präfixlänge**
  Zeigt die Präfixlänge dieser Route an.
- **Gateway**
  Zeigt das Gateway für diese Route an.
- **Schnittstelle**
  Zeigt die Schnittstelle für diese Route an.

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

6.4.13 DHCP-Server

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



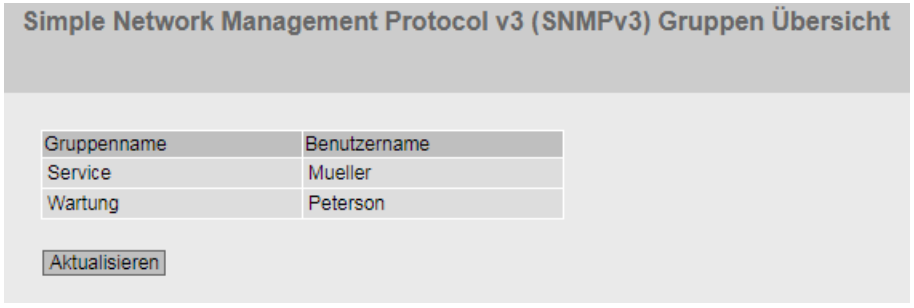
Beschreibung

- **IP-Adresse**
  Zeigt die IPv4-Adresse an, die dem DHCP-Client zugeordnet ist.
- **Pool-ID**
  Zeigt die Nummer des IPv4-Adressbands an.
- **Identifikationsmethode**
  Zeigt die Methode an, nach der der DHCP-Client identifiziert wird.
- **Identifikationswert**
  Zeigt die MAC-Adresse oder die Client-ID des DHCP-Clients an.
- **Zuordnungsmethode**
  Zeigt an, ob die IPv4-Adresse statisch oder dynamisch vergeben wurde. Die statischen Einträge konfigurieren Sie unter "System > DHCP > Statische Zuordnung".

- **Zuordnungsstatus**
  Zeigt den Status der Zuordnung an.
  - Zugewiesen
    Die Zuordnung wird verwendet.
  - Nicht verwendet
    Die Zuordnung wird nicht verwendet.
  - Wird geprüft
    Die Zuordnung wird geprüft.
  - Unbekannt
    Der Status der Zuordnung ist unbekannt.
- **Ablaufzeit**
  Zeigt an, bis wann die vergebene IPv4-Adresse noch gültig ist. Bis zu diesem Zeitpunkt muss der DHCP-Client entweder eine neue IPv4-Adresse anfordern oder die Gültigkeitsdauer der vergebenen IPv4-Adresse verlängern.

6.4.14 SNMP

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



Beschreibung

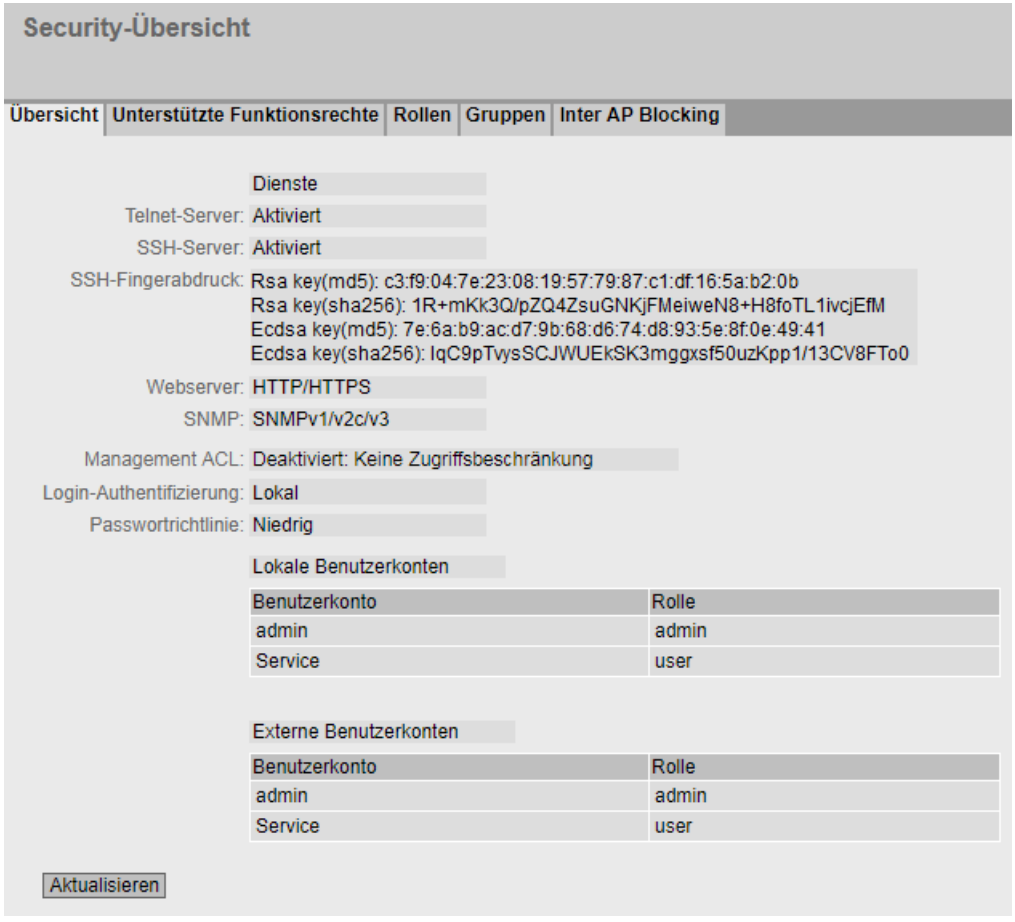
Die Tabelle gliedert sich in folgende Spalten:

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

6.4.15 Security

6.4.15.1 Übersicht

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



Beschreibung

Dienste

Die Liste "**Dienste**" zeigt die Sicherheitseinstellungen an.

- **Telnet-Server**
  Die Einstellung konfigurieren Sie unter "System > Konfiguration"
  - Aktiviert: Unverschlüsselter Zugriff auf das CLI
  - Deaktiviert: Kein unverschlüsselter Zugriff auf das CLI
- **SSH-Server**
  Die Einstellung konfigurieren Sie unter "System > Konfiguration".
  - Aktiviert: Verschlüsselter Zugriff auf das CLI
  - Deaktiviert: Kein verschlüsselter Zugriff auf das CLI
- **SSH-Fingerabdruck**
  Das Feld zeigt den SSH-Fingerprint an.
- **Webserver**
  Die Einstellung konfigurieren Sie unter "System > Konfiguration"
  - HTTP/HTTPS: Der Zugriff auf das WBM ist über HTTP und HTTPS möglich.
  - HTTPS: Der Zugriff auf das WBM ist nur noch über HTTPS möglich.
- **SNMP**
  Die Einstellung konfigurieren Sie unter "System > SNMP > Allgemein".
  - "-" (SNMP deaktiviert)
    Ein Zugriff auf die Geräteparameter ist über SNMP nicht möglich.
  - SNMPv1/v2c/v3
    Ein Zugriff auf die Geräteparameter ist mit den SNMP-Versionen 1, 2c oder 3 möglich.
  - SNMPv3
    Ein Zugriff auf die Geräteparameter ist nur mit der SNMP-Version 3 möglich.
- **Management ACL**
  Die Einstellung konfigurieren Sie unter "Security > Management ACL".
  - Aktiviert: Nur eingeschränkter Zugriff: Der Zugang wird über eine Access Control List (ACL) eingeschränkt.
  - Deaktiviert: Keine Zugriffsbeschränkung: Management ACL ist nicht aktiviert.

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

Lokale und externe Benutzerkonten

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

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

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

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

Hinweis

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

Über CLI können Sie auf die externen Benutzerkonten zugreifen.

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

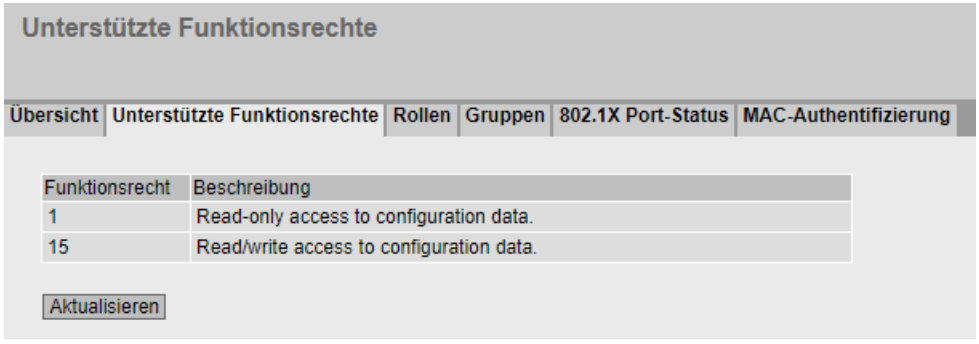
- **Benutzerkonto**
  Zeigt den Namen des lokalen Benutzers an.
- **Rolle**
  Zeigt die Rolle des Benutzers an. Weitere Informationen zu den Funktionsrechten der Rolle erhalten Sie unter "Information > Security > Rollen".

6.4.15.2 Unterstützte Funktionsrechte

Hinweis

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

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



Beschreibung der angezeigten Werte

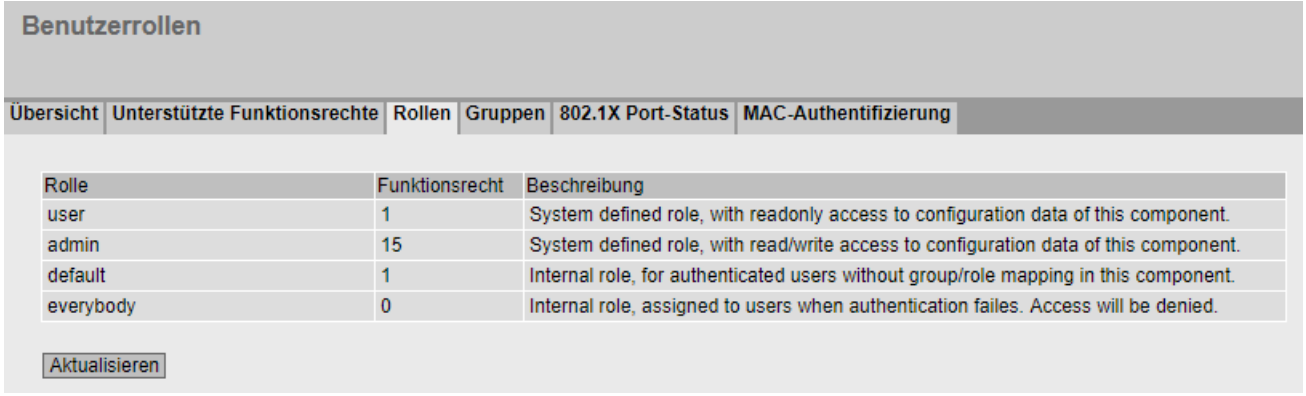
- **Funktionsrecht**
  Zeigt die Nummer des Funktionsrechts an. Den Nummern sind unterschiedliche Rechte in Bezug auf die Geräteparameter zugeordnet.
- **Beschreibung**
  Zeigt die Beschreibung des Funktionsrechts an.

6.4.15.3 Rollen

Hinweis

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

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



Beschreibung

Die Tabelle enthält folgende Spalten:

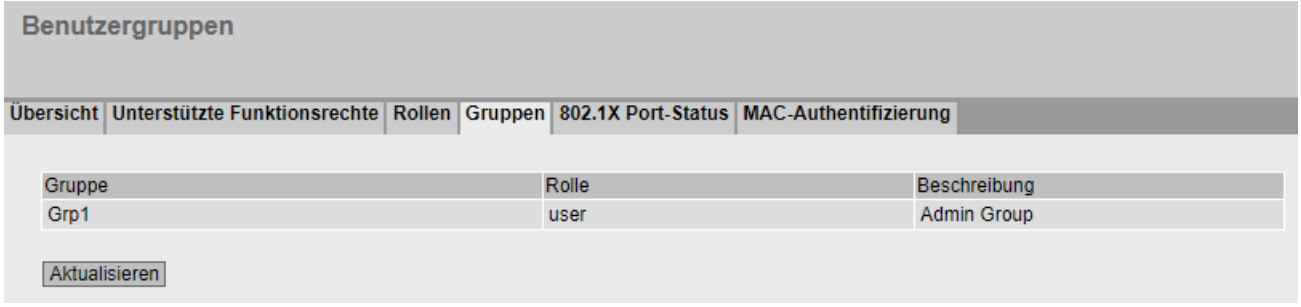
- **Rolle**
  Zeigt den Namen der Rolle an.
- **Funktionsrecht**
  Zeigt das Funktionsrecht der Rolle an:
  - 1
    Benutzer mit dieser Rolle können Geräteparameter lesen, aber nicht verändern.
  - 15
    Benutzer mit dieser Rolle können Geräteparameter sowohl lesen als auch verändern.
  - 0
    Hierbei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

6.4.15.4 Gruppen

Hinweis

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

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



Beschreibung der angezeigten Werte

Die Tabelle gliedert sich in folgende Spalten:

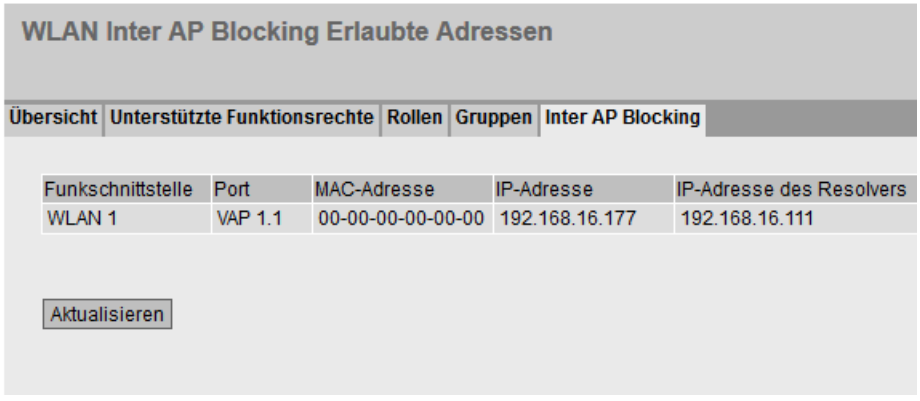
- **Gruppe**
  Zeigt den Namen der Gruppe an. Der Name entspricht der Gruppe auf dem RADIUS-Server.
- **Rolle**
  Zeigt den Namen der Rolle an. Benutzer, die über den RADIUS-Server mit der verknüpften Gruppe authentifiziert werden, erhalten die Rechte dieser Rolle lokal auf dem Gerät.
- **Beschreibung**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

6.4.15.5 Inter AP Blocking

Hinweis

Diese WBM-Seite ist nur im Access Point-Modus verfügbar.

Die WBM-Seite zeigt eine Liste der Geräte an, mit denen die Clients kommunizieren dürfen.



Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen an, auf die sich die Einstellungen beziehen.
- **Port**
  Zeigt die VAP-Schnittstelle an, auf die sich die Einstellungen beziehen.
- **MAC-Adresse**
  Zeigt die MAC-Adresse des Geräts, mit dem der Client kommunizieren darf.
- **IP-Adresse**
  Zeigt IPv4-Adresse des Geräts, mit dem der Client kommunizieren darf.
- **IP-Adresse des Resolvers**
  Zeigt IPv4-Adresse an, mit der der Access Point die erlaubte IPv4-Adresse aufgelöst.

6.4.16 WLAN

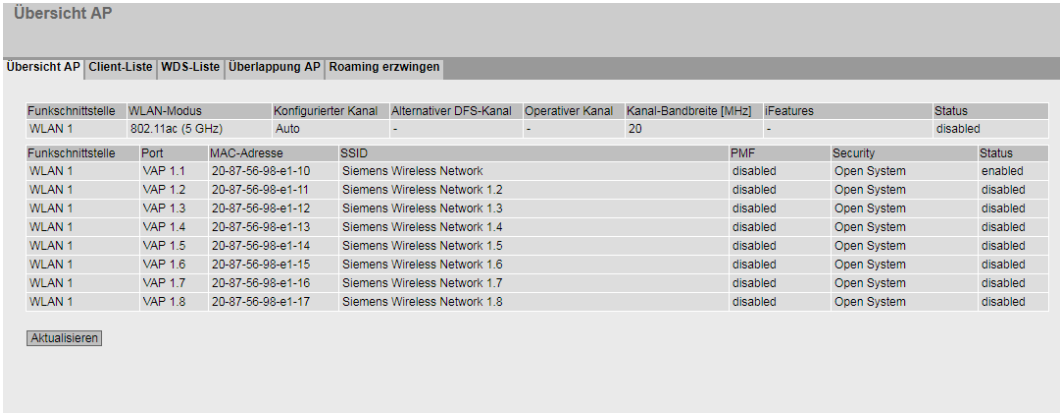
6.4.16.1 Übersicht AP

Hinweis

Diese WBM-Seite ist nur im Access Point-Modus verfügbar.

Konfigurationsübersicht

Diese Seite zeigt die Einstellungen/Eigenschaften des Access Points an.



Funkschnittstelle	WLAN-Modus	Konfigurierter Kanal	Alternativer DFS-Kanal	Operativer Kanal	Kanal-Bandbreite [MHz]	iFeatures	Status
WLAN 1	802.11ac (5 GHz)	Auto	-	-	20	-	disabled

Funkschnittstelle	Port	MAC-Adresse	SSID	PMF	Security	Status
WLAN 1	VAP 1.1	20-87-56-98-e1-10	Siemens Wireless Network	disabled	Open System	enabled
WLAN 1	VAP 1.2	20-87-56-98-e1-11	Siemens Wireless Network 1.2	disabled	Open System	disabled
WLAN 1	VAP 1.3	20-87-56-98-e1-12	Siemens Wireless Network 1.3	disabled	Open System	disabled
WLAN 1	VAP 1.4	20-87-56-98-e1-13	Siemens Wireless Network 1.4	disabled	Open System	disabled
WLAN 1	VAP 1.5	20-87-56-98-e1-14	Siemens Wireless Network 1.5	disabled	Open System	disabled
WLAN 1	VAP 1.6	20-87-56-98-e1-15	Siemens Wireless Network 1.6	disabled	Open System	disabled
WLAN 1	VAP 1.7	20-87-56-98-e1-16	Siemens Wireless Network 1.7	disabled	Open System	disabled
WLAN 1	VAP 1.8	20-87-56-98-e1-17	Siemens Wireless Network 1.8	disabled	Open System	disabled

Beschreibung

Die Tabelle 1 gliedert sich in folgende Spalten:

- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen an.
- **WLAN-Modus**
  Zeigt den Übertragungsstandard an. Bei aktiviertem DFS wird nicht zusätzlich der Übertragungsstandard "802.11h" angezeigt, sondern der konfigurierte Übertragungsstandard mit dem Zusatz "DFS".
- **Konfigurierter Kanal**
  Zeigt den projektierten Kanal an. Wenn "Auto" angezeigt wird, sucht der Access Point selbst nach einem freien Kanal.
- **Alternativer DFS-Kanal**
  Wenn die Funktion DFS aktiviert ist, wird der projektierte Alternativ-Kanal des Access Points angezeigt.
  Wenn "Auto" angezeigt wird, sucht der Access Point selbst nach einem Alternativ-Kanal.
  Wenn die Funktion DFS aktiviert ist, und der Access Point vor Aufnahme der Kommunikation auf dem gewählten Kanal 60 Sekunden nach konkurrierenden Radarsignalen sucht, wird anstatt des Kanals der Text "scanning ..." angezeigt.

- **Operativer Kanal**
  Zeigt den Kanal inklusive der Frequenz an, über den der Access Point kommuniziert. Bei 80 MHz wird zusätzlich der Kanalbereich angezeigt.
- **Kanalbandbreite [MHz]**
  Zeigt die eingestellte Kanalbandbreite an.
  - 20 MHz
  - 40 MHz (Nur bei IEEE 802.11n/ac)
  - 80 MHz oder 160 MHz (Nur bei IEEE 802.11ac)
- **iFeatures**
  Zeigt an, welche iFeatures verwendet werden.
  - - iFeatures werden nicht verwendet.
  - iPRP
- **Status**
  Zeigt den Status der WLAN-Schnittstelle an.
  - enabled
    WLAN-Schnittstelle ist aktiviert.
  - disabled
    WLAN-Schnittstelle ist deaktiviert.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen in dieser Spalte an.
- **Port**
  Zeigt den Port des Virtuellen Access Points (VAP) an.
- **MAC-Adresse**
  Zeigt die MAC-Adresse des Virtuellen Access Points an.
- **SSID**
  Zeigt die SSID an.
- **PMF**
  Zeigt an, ob die Management-Telegramme kryptografisch geschützt werden.
  - disabled
    Die Management-Telegramme sind nicht verschlüsselt.
  - required
    Die Management-Telegramme sind immer verschlüsselt. Eine Verbindung der WLAN-Clients zu dem Access Point ist nur möglich, wenn diese auch PMF unterstützen.
  - optional
    Die Management-Telegramme werden je nach Unterstützung des WLAN-Clients verschlüsselt oder unverschlüsselt.

- **Security**
  Zeigt an, welches Authentifizierungsverfahren verwendet wird.
  Wenn die Authentifizierungsverfahren "Open System + Verschlüsselung" oder "Shared Key" verwendet werden, wird für beide Authentifizierungsverfahren "Verschlüsselt (WEP/AES)" angezeigt.
- **Status**
  Zeigt den Status der WLAN-Schnittstelle an.
  - enabled
    WLAN-Schnittstelle ist aktiviert.
  - disabled
    WLAN-Schnittstelle ist deaktiviert.

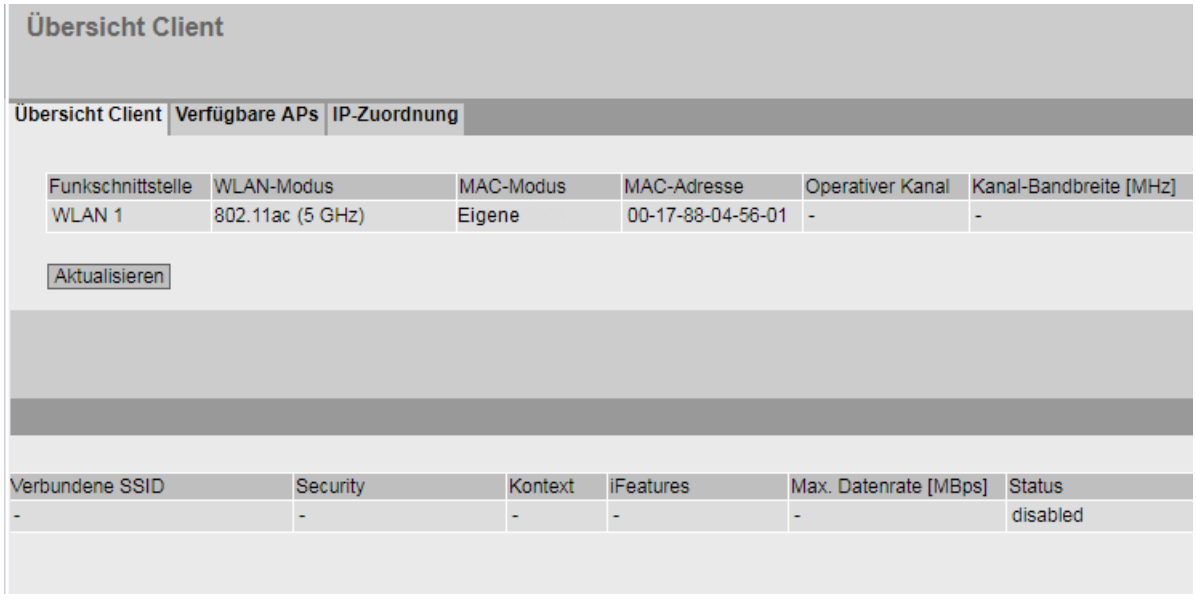
6.4.16.2 Übersicht Client

Konfigurationsübersicht

Hinweis

Diese Seite ist nur bei Clients oder bei Access Points im Client-Modus verfügbar.

Die Seite zeigt eine Übersicht der vorhandenen Clients und ihrer Konfiguration.



Beschreibung

- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen an.
- **WLAN-Modus**
  Zeigt den Übertragungsstandard an.

- **MAC-Modus**
  Zeigt an, wie der Schnittstelle die MAC-Adresse zugeordnet ist.
  - Auto Layer- 2-Tunnel
    Der Client verwendet entweder den MAC-Modus "Eigene" oder "Layer-2-Tunnel".
  - Manuell
    Die Adresse wurde manuell eingetragen.
  - Eigene
    Der Client verwendet die MAC-Adresse der Ethernet-Schnittstelle für die WLAN-Schnittstelle.
  - Layer 2-Tunnel
    Der Client verwendet die MAC-Adresse der Ethernet-Schnittstelle für die WLAN-Schnittstelle. Zusätzlich wird das Netzwerk über die, an der Ethernet-Schnittstelle des Clients, angeschlossenen MAC-Adressen informiert. Bis zu acht MAC-Adressen können verwendet werden.
- **MAC-Adresse**
  Zeigt die MAC-Adresse der WLAN-Schnittstelle an.
- **Operativer Kanal**
  Zeigt den Kanal inklusive Frequenz des Access Points an, mit dem der Client verbunden ist. Bei 80 MHz wird zusätzlich der Kanalbereich angezeigt.
- **Kanalbandbreite [MHz]**
  Zeigt die eingestellte Kanalbandbreite an.
  - 20 MHz
  - 40 MHz (Nur bei IEEE 802.11n/ac)
  - 80 MHz oder 160 MHz (Nur bei IEEE 802.11ac)
- **Verbundene BSSID**
  Zeigt die MAC-Adresse des Access Points an, mit dem der Client verbunden ist.
- **Verbundene SSID**
  Zeigt die SSID des Access Points an, mit dem der Client verbunden ist.
- **Security**
  Zeigt an, welches Authentifizierungsverfahren verwendet wird.
  Wenn die Authentifizierungsverfahren "Open System + Verschlüsselung" oder "Shared Key" verwendet werden, wird für beide Authentifizierungsverfahren "Verschlüsselt (WEP/AES)" angezeigt.
- **Kontext**
  Zeigt an, welcher Security-Kontext verwendet wird.
- **iFeatures**
  Zeigt an, welche iFeatures verwendet werden.
  - -
    iFeatures werden nicht verwendet.
  - iPRP

- **Max. Datenrate [Mbps]**
  Zeigt die maximale Datenübertragungsgeschwindigkeit in Megabits pro Sekunde an.
- **Status**
  Zeigt den Status der WLAN-Schnittstelle an.
  - enabled
    WLAN-Schnittstelle ist aktiviert.
  - disabled
    WLAN-Schnittstelle ist deaktiviert.

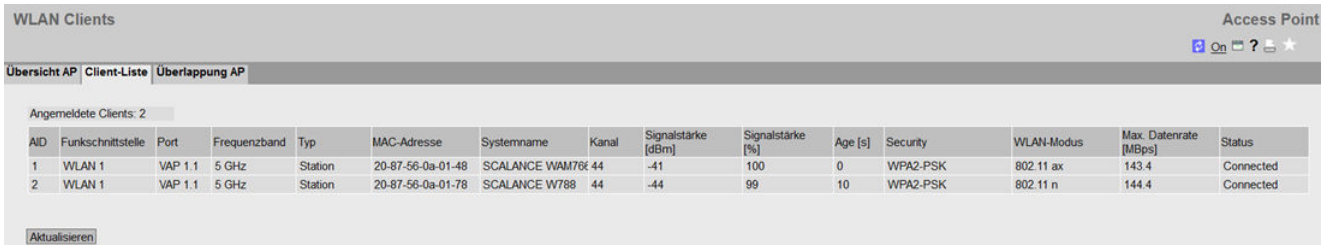
6.4.16.3 Client-Liste

Hinweis

Diese WBM-Seite ist nur im Access Point-Modus verfügbar.

Angemeldete Clients

Die WBM-Seite zeigt die am Access Point angemeldeten Clients sowie Zusatzinformationen z. B. Status, Signalstärke, MAC-Adresse.



Beschreibung

- **Angemeldete Clients**
  Zeigt die Anzahl der Clients an, die am Access Point angemeldet sind.

Die Tabelle gliedert sich in folgende Spalten:

- **AID** (Associated ID)
  Zeigt die Verbindungs-ID des Clients an. Wenn der Client sich über die VAP-Schnittstelle mit dem Access Point verbindet, bekommt der Client eine Verbindungs-ID zugewiesen. Die Verbindungs-ID ist innerhalb einer VAP-Schnittstelle eindeutig. Wenn sich zwei Clients an verschiedenen VAP-Schnittstellen anmelden, können beide Clients die gleiche ID erhalten.
- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen an.
- **Port**
  Zeigt die VAP-Schnittstelle an.
- **Typ**
  Zeigt die Client-Art an, z. B. "Sta" steht für IEEE 802.11 Standard-Client.

- **MAC-Adresse**
  Zeigt die MAC-Adresse des Clients an.
- **Systemname**
  Zeigt den Systemnamen des Clients an, wenn der Client diesen an den Access Point kommuniziert. Nicht alle Clients unterstützen diesen Parameter.
- **Kanal**
  Zeigt den Kanal an, über den der Client mit dem Access Point kommuniziert.
- **Signalstärke [dBm]**
  Zeigt die Signalstärke des verbundenen Clients in Dezibel Milliwatt an.
- **Signalstärke [%]**
  Zeigt die Signalstärke des verbundenen Clients in Prozent an.
- **Age [s]**
  Zeigt die Zeit an, die seit der letzten Aktivität des Clients vergangen ist.
- **Security**
  Zeigt an, welches Authentifizierungsverfahren verwendet wird.
  Wenn die Authentifizierungsverfahren "Open System + Verschlüsselung" oder "Shared Key" verwendet werden, wird für beide Authentifizierungsverfahren "Verschlüsselt (WEP/AES)" angezeigt.
- **WLAN-Modus**
  Zeigt den Übertragungsstandard an. Bei aktiviertem DFS wird nicht zusätzlich der Übertragungsstandard "802.11h" angezeigt, sondern nur der konfigurierte Übertragungsstandard "802.11a".
- **Max. Datenrate [MBps]**
  Zeigt die maximale Datenübertragungsgeschwindigkeit in Megabits pro Sekunde an.
- **Status**
  Zeigt den aktuellen Status der Verbindung an, z. B. "verbunden" bedeutet der Client ist mit dem Access Point verbunden und ist bereit mit dem AP zu kommunizieren.

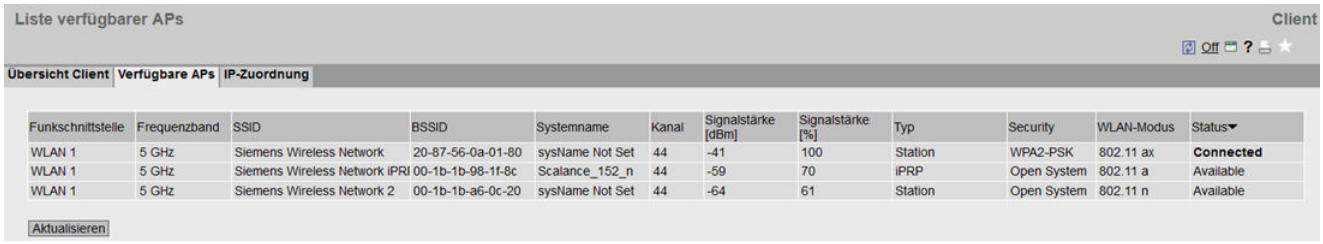
6.4.16.4 Verfügbare APs

Verfügbare Access Points

Hinweis

Diese Seite ist nur bei Clients oder bei Access Points im Client-Modus verfügbar.

Diese Seite zeigt alle Access Points an, die der Client sieht. In der Liste sind auch die Access Points enthalten, auf die sich der Client wegen seiner Konfiguration nicht verbinden kann.



Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Funkschnittstelle**
  Zeigt die WLAN-Schnittstelle, die den Access Point sieht.
- **SSID**
  Zeigt die SSID des Access Points an.
- **BSSID**
  Zeigt die MAC-Adresse des Access Points an.
- **Systemname**
  Zeigt den Systemnamen des Access Points an. Der Eintrag ist abhängig vom Access Point. Nicht alle Access Point unterstützen diesen Parameter.
- **Kanal**
  Zeigt den Kanal an auf dem der Access Point funkt bzw. kommuniziert.
- **Signalstärke [dBm]**
  Zeigt die Signalstärke des Access Points in dBm an.
- **Signalstärke [%]**
  Zeigt die Signalstärke des Access Points in Prozent an.
- **Typ**
  Zeigt die Betriebsart der WLAN-Schnittstelle an.
- **Security**
  Zeigt an, welches Authentifizierungsverfahren verwendet wird.
  Wenn die Authentifizierungsverfahren "Open System + Verschlüsselung" oder "Shared Key" verwendet werden, wird für beide Authentifizierungsverfahren "Verschlüsselt (WEP/AES)" angezeigt.
- **WLAN-Modus**
  Zeigt den Übertragungsstandard an. Bei aktiviertem DFS wird nicht zusätzlich der Übertragungsstandard "802.11h" angezeigt, sondern nur der konfigurierte Übertragungsstandard "802.11a" oder "802.11n".
- **Status**
  Zeigt den Status des Access Points an, z.B. ob der Access Point verfügbar ist.

6.4.16.5 IP Mapping-Tabelle

WLAN-Zugang für mehrere SCALANCE W-Geräte über einen Client

Hinweis

Diese WBM-Seite ist nur bei Clients oder bei Access Points im Client-Modus verfügbar.

Sie können mit einem Client mehreren SCALANCE W-Geräten den WLAN-Zugang ermöglichen, wenn Sie das sogenannte IP-Mapping einsetzen. So brauchen Sie nicht jedes SCALANCE W-Gerät mit einem eigenen WLAN-Client auszustatten. Voraussetzung hierfür ist, dass die angeschlossenen SCALANCE W-Geräte nur mit IP-Telegrammen angesprochen werden sollen. Eine Kommunikation auf MAC-Adressen-Ebene (ISO/OSI Schicht 2) kann

- zu einer Komponente erfolgen, deren MAC-Adresse im Client konfiguriert ist,
- zu maximal acht Komponenten erfolgen, wenn die Funktion "Layer-2-Tunnel" gewählt wird.

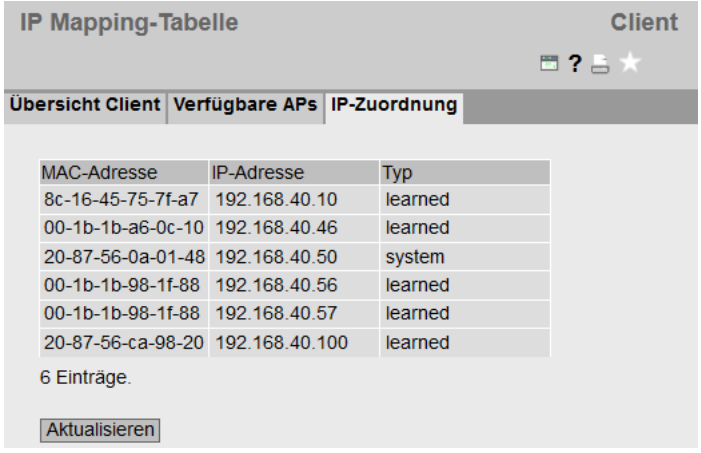
Die Einstellung "Layer 2-Tunnel" erfüllt Forderungen von Industrie-Applikationen, bei denen MAC-Adressen basierte Kommunikation zu mehreren SCALANCE W-Geräten hinter dem Client stattfindet. Clients mit dieser Einstellung können sich nicht auf Standard-Wifi-Access Points verbinden.

Der Client unterhält eine Tabelle mit der Zuordnung von MAC-Adresse und IP-Adresse, um eingehende IP-Frames an die richtige MAC-Adresse zu verschicken. Diese WBM-Seite zeigt diese Tabelle an.

Hinweis

IP-Mapping-Tabelle

Ist bei einem Client "Layer 2-Tunnel" konfiguriert, wird die IP-Mapping-Tabelle nicht angezeigt.



Beschreibung

Die Tabelle gliedert sich in folgende Spalten

- **MAC-Adresse**
  Die MAC-Adresse eines Geräts, das sich, aus Sicht des Access Points, hinter dem WLAN-Client befindet.
- **IP-Adresse**
  Die IP-Adresse, die vom WLAN-Client für dieses Gerät verwaltet wird.
- **Typ**
  Für den Typ gibt es zwei Optionen:
  - system
    Die Informationen beziehen sich auf den WLAN-Client selbst.
  - learned
    Die Informationen beziehen sich auf ein Gerät, das sich hinter dem WLAN-Client befindet.

MAC-Modus

Frames, die vom Client zum Access Point geschickt werden, enthalten als Quell-MAC-Adresse immer die MAC-Adresse des WLAN-Clients. In der "Learning-Tabelle" des Access Points steht daher nur die MAC-Adresse des WLAN-Clients.

Sind hinter dem Client mehrere SCALANCE W-Geräte, sollte nicht die Option "Automatisch" aktiviert sein. In diesem Falle würde die MAC-Adresse wahllos an das erste SCALANCE W-Gerät vergeben, das sich über Ethernet meldet. Wenn zwischen dem Access Point und dem Client nur IP-Kommunikation stattfindet, kann die Default-Einstellung "Eigene" beibehalten werden. Sollen MAC-basierte Frames auch von SCALANCE W700-Geräten hinter dem Client versendet werden können, müssen Sie die Einstellungen "Manuell", "Automatisch" oder "Layer 2-Tunnel" auswählen.

6.4.16.6 WDS-Liste

Hinweis

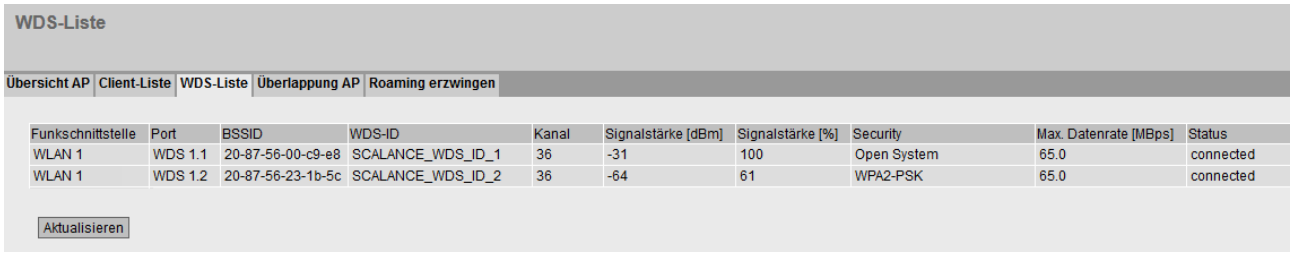
Diese WBM-Seite ist nur im Access Point-Modus verfügbar.

Kommunikation zwischen Access Points

Im normalen Betrieb ist der Access Point als Schnittstelle zu einem Netz eingesetzt und kommuniziert mit Clients. Es gibt allerdings auch den Anwendungsfall, dass mehrere Access Points miteinander kommunizieren müssen, z.B. zum Zweck der Reichweitenvergrößerung oder zum Aufbau eines Wireless-Backbones. Diese Betriebsart ist mit WDS (Wireless Distributed System) möglich.

Standardmäßig wird die Liste 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.

Die Seite zeigt Informationen über die WDS-Verbindungen des Access Points.



Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen an.
- **Port**
  Zeigt den Port an.
- **BSSID**
- Zeigt die MAC-Adresse des WDS-Partners an.
- **WDS-ID**
  Zeigt den Namen des WDS-Partners an.
- **Kanal**
  Zeigt den Kanal an, über den der Access Point mit dem WDS-Partner kommuniziert.
- **Signalstärke [dBm]**
  Zeigt die Signalstärke des verbundenen Access Points in dBm an.
- **Signalstärke [%]**
  Zeigt die Signalstärke des verbundenen Access Points in Prozent an.
- **Security**
  Zeigt an, welches Authentifizierungsverfahren verwendet wird.
  Wenn die Authentifizierungsverfahren "Open System + Verschlüsselung" oder "Shared Key" verwendet werden, wird für beide Authentifizierungsverfahren "Verschlüsselt (WEP/AES)" angezeigt.
- **Max. Datenrate [MBps]**
  Zeigt die maximale Datenübertragungsgeschwindigkeit für den entsprechenden WDS-Partner an.
- **Status**
  Zeigt den aktuellen Zustand der WDS-Verbindung an.

6.4.16.7 Überlappung AP

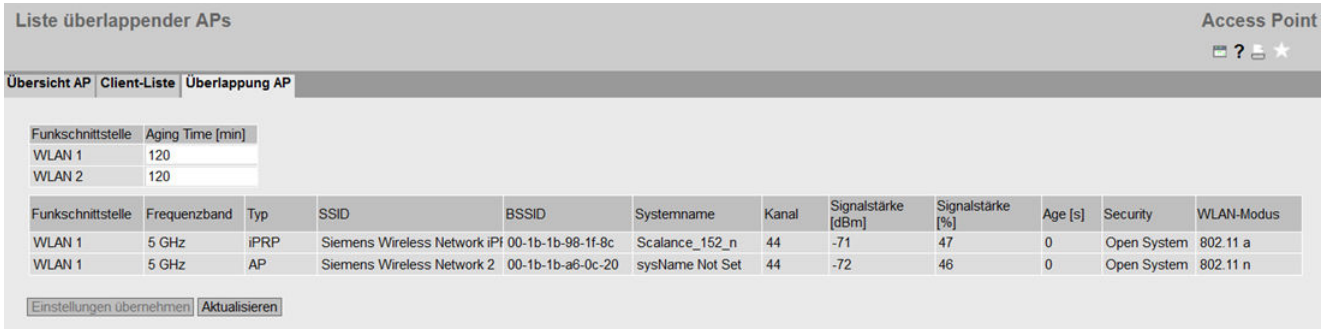
Hinweis

Diese WBM-Seite ist nur im Access Point-Modus verfügbar.

Überlappende Kanäle

Für einen optimalen Datendurchsatz ist es notwendig, dass der eingestellte Funkkanal nicht von anderen Access Points genutzt wird. Im 2,4 GHz Band (802.11b oder 802.11g) gibt es eine Überlappung der Kanäle, sodass ein Access Point nicht nur den eingestellten Kanal belegt, sondern zusätzlich die benachbarten 2-3 Kanäle. Achten Sie deshalb darauf, dass zu benachbarten Access Points ein ausreichend großer Kanalabstand besteht.

Die WBM-Seite zeigt alle Access Points, die auf dem eingestellten oder auf benachbarten Kanälen (bei 2,4 GHz) sichtbar sind. Wenn hier Einträge vorhanden sind, ist der maximale Datendurchsatz des Access Points und die Verfügbarkeit der Kommunikationsverbindung zum Access Point potenziell beeinträchtigt.



Beschreibung

Die Tabelle 1 gliedert sich in folgende Spalten:

- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen an.
- **Aging Time [min]**
  Legen Sie die Lebensdauer für die Einträge in der Liste fest. Ist ein Access Point länger als die eingestellte Zeit inaktiv, wird er aus der Liste entfernt.

  Hinweis

  Ändern der Aging Time

  Die Aging Time ist eine WLAN-Einstellung. Deshalb wird bei einer Änderung die WLAN Verbindung kurz unterbrochen, um den neuen Wert zu übernehmen.

Die Tabelle gliedert sich in folgende Spalten:

- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen in dieser Spalte an.
- **Typ**
  Zeigt die Betriebsart der WLAN-Schnittstelle an.
- **SSID**
  Zeigt die SSID des Access Points an.
- **BSSID**
  Zeigt die MAC-Adresse des Access Points an.

- **Systemname**
  Zeigt den Systemnamen des SCALANCE W-Geräts an. Der Eintrag ist abhängig vom Access Point. Nicht alle Access Point unterstützen diesen Parameter.
- **Kanal**
  Zeigt den Kanal an, über den der Client mit dem Access Point kommuniziert.
- **Signalstärke [dBm]**
  Zeigt die Signalstärke des Clients in dBm an.
- **Signalstärke [%]**
  Zeigt die Signalstärke des Clients in Prozent an.
- **Age [s]**
  Zeigt die Zeit an, die seit der letzten Aktivität des Access Points vergangen ist.
- **Security**
  Zeigt an, welches Authentifizierungsverfahren verwendet wird.
  Wenn die Authentifizierungsverfahren "Open System + Verschlüsselung" oder "Shared Key" verwendet werden, wird für beide Authentifizierungsverfahren "Verschlüsselt (WEP/AES)" angezeigt.
- **WLAN-Modus**
  Zeigt den Übertragungsstandard an. Bei aktiviertem DFS wird nicht zusätzlich der Übertragungsstandard "802.11h" angezeigt, sondern der konfigurierte Übertragungsstandard mit dem Zusatz "DFS".

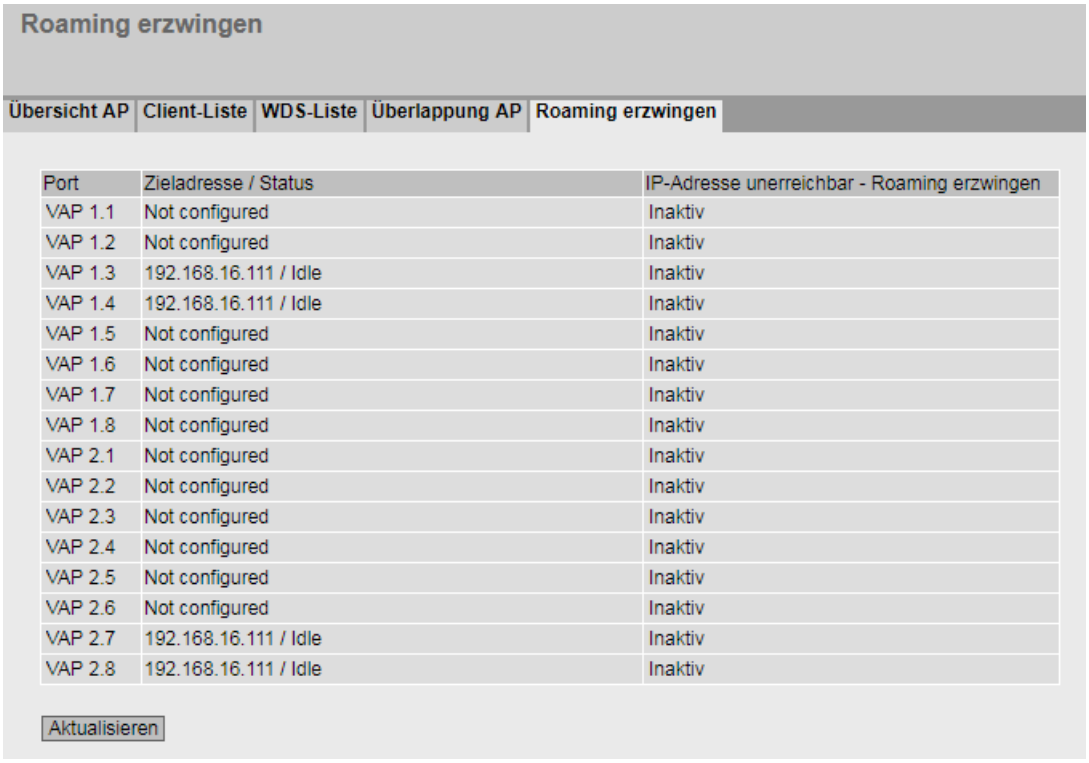
6.4.16.8 Roaming erzwingen

Hinweis

Diese WBM-Seite ist nur im Access Point-Modus verfügbar.

Auf dieser WBM-Seite wird angezeigt, welchen aktuellen Status die Verbindung hat. Zudem wird angezeigt, ob ein Roaming ausgeführt wird.

Das Gerät überwacht zyklisch die Verbindung zu bestimmten IPv4-Adressen. Dazu sendet das Gerät in regelmäßigen Abständen Echomeldungen (Ping) an die projektierten Zieladressen.



Beschreibung

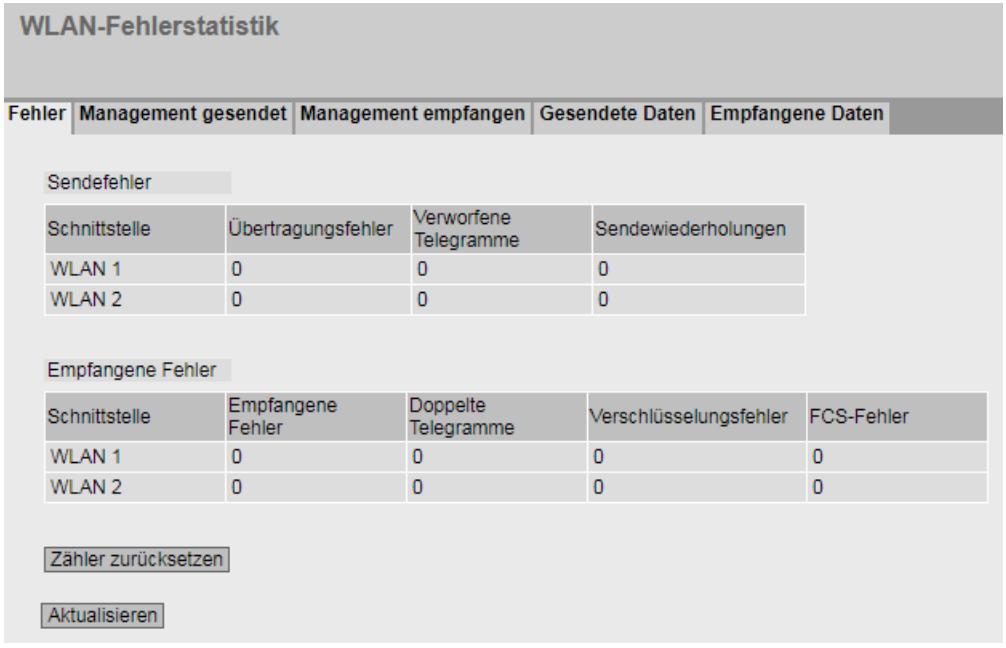
Die Tabelle gliedert sich in folgende Spalten:

- **Port**
  Zeigt die verfügbaren VAP-Schnittstellen an.
- **Zieladresse / Status**
  Zeigt an, welche Zieladresse überwacht wird und wie der Status der Verbindung ist. Die Zieladresse konfigurieren Sie unter "Schnittstellen > WLAN > Roaming erzwingen".
  - Not configured: Es ist keine Zieladresse konfiguriert.
  - Idle: Die Zieladresse wurde nicht gefunden.
  - Up: Die Zieladresse ist erreichbar.
  - Down: Die Zieladresse ist nicht erreichbar.
- **IP-Adresse nicht erreichbar - Roaming erzwingen**
  Zeigt an, ob aktuell ein Roaming durchgeführt wird.
  - Inaktiv: Der Client wird zu keinem Roaming gezwungen. Die entsprechende VAP-Schnittstelle wird nicht abgeschaltet.
  - Aktiv: Keine der Zieladressen ist erreichbar. Um die angemeldeten Clients zu einem Roaming zu zwingen, hat der Access Point die entsprechende VAP-Schnittstelle abgeschaltet.

6.4.17 WLAN-Statistiken

6.4.17.1 Fehler

Die WBM-Seite zeigt an, wie viele fehlerhafte Telegramme pro WLAN-Schnittstelle empfangen bzw. gesendet wurden. Wenn eine erhöhte Fehleranzahl auftritt, überprüfen Sie die Einstellungen für die WLAN-Schnittstelle(n), den Aufbau der SCALANCE W-Geräte und die Verbindungsqualität.



Beschreibung

Die Tabelle Sendefehler gliedert sich in folgende Spalten:

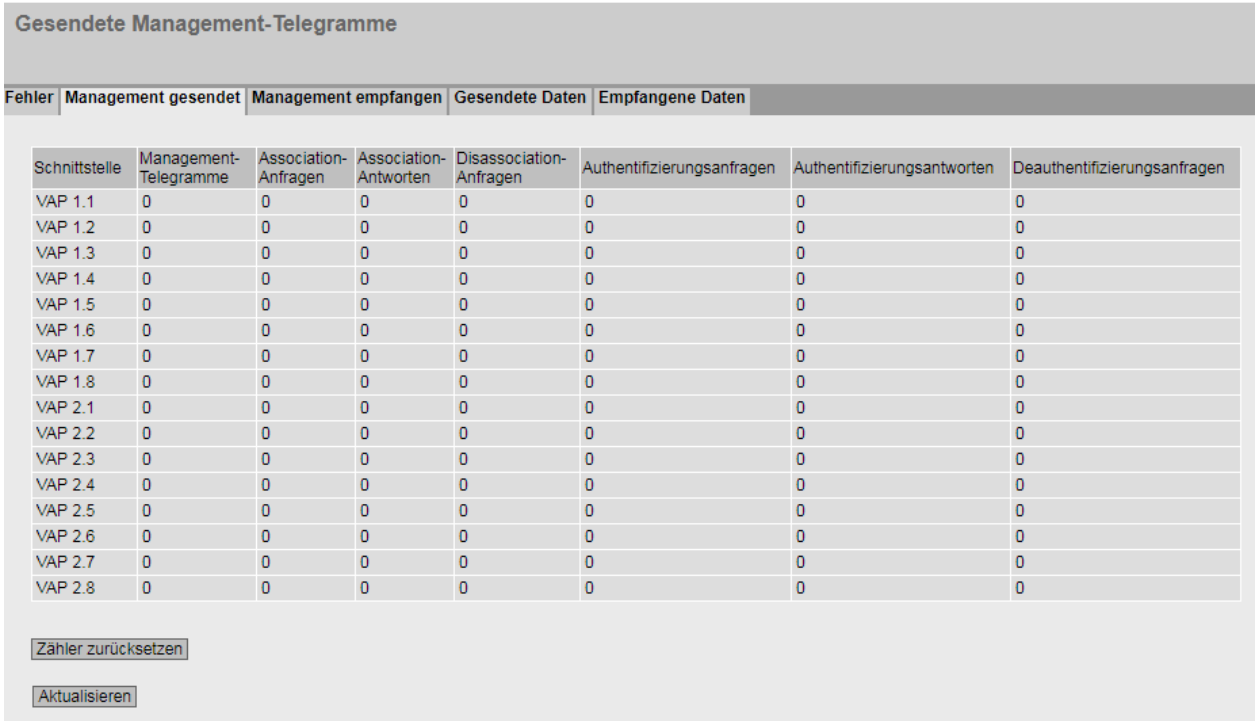
- **Schnittstelle**
  Zeigt die WLAN-Schnittstelle an, auf die sich die Einträge beziehen.
- **Fehlertypen**
  Die weiteren Spalten hinter der jeweiligen WLAN-Schnittstelle enthalten die absoluten Zahlen der gesendeten Telegramme entsprechend ihres Fehlertyps.
  Dabei wird in den Spalten der Tabelle nach folgenden Fehlertypen unterschieden:
  - Übertragungsfehler
    Zeigt die Anzahl und den prozentualen Anteil der fehlerhaften Telegramme an, die gesendet wurden.
  - Verworfene Telegramme
    Zeigt die Anzahl und den prozentualen Anteil der Telegramme an, die verworfen wurden. Das Telegramm konnte trotz aller Wiederholungen nicht erfolgreich gesendet werden. Das Telegramm wurde noch nicht gesendet und der Empfänger hat sich zwischenzeitlich abgemeldet.
  - Sendewiederholungen
    Zeigt die Anzahl und den prozentualen Anteil der erfolgreich gesendeten Telegramme an, die einen oder mehrere Wiederholungen (Retries) benötigt haben.

Die Tabelle Empfangene Fehler gliedert sich in folgende Spalten:

- **Schnittstelle**
  Zeigt die WLAN-Schnittstelle an, auf die sich die Einträge beziehen.
- **Fehlertypen**
  Die weiteren Spalten hinter der jeweiligen WLAN-Schnittstelle enthalten die absoluten Zahlen der empfangenen Telegramme ihres Fehlertyps.
  Dabei wird in den Spalten der Tabelle nach folgenden Fehlertypen unterschieden:
  - Empfangene Fehler
    Zeigt die Anzahl und den prozentualen Anteil der fehlerhaften Telegramme an, die empfangen wurden.
  - Doppelte Telegramme
    Zeigt die Anzahl und den prozentualen Anteil der Telegramme an, die doppelt empfangen wurden.
  - Verschlüsselungsfehler
    Zeigt die Anzahl und den prozentualen Anteil der fehlerhaften verschlüsselten Telegramme an.
  - FCS-Fehler
    Zeigt die Anzahl und den prozentualen Anteil der Telegramme an, bei denen die Prüfsumme nicht korrekt war.

6.4.17.2 Management gesendet

Die WBM-Seite zeigt an, wie viele Telegramme für den Anmeldevorgang bzw. Abmeldevorgang pro VAP-Schnittstelle gezählt wurden.



Schnittstelle	Management-Telegramme	Association-Anfragen	Association-Antworten	Disassociation-Anfragen	Authentifizierungsanfragen	Authentifizierungsantworten	Deauthentifizierungsanfragen
VAP 1.1	0	0	0	0	0	0	0
VAP 1.2	0	0	0	0	0	0	0
VAP 1.3	0	0	0	0	0	0	0
VAP 1.4	0	0	0	0	0	0	0
VAP 1.5	0	0	0	0	0	0	0
VAP 1.6	0	0	0	0	0	0	0
VAP 1.7	0	0	0	0	0	0	0
VAP 1.8	0	0	0	0	0	0	0
VAP 2.1	0	0	0	0	0	0	0
VAP 2.2	0	0	0	0	0	0	0
VAP 2.3	0	0	0	0	0	0	0
VAP 2.4	0	0	0	0	0	0	0
VAP 2.5	0	0	0	0	0	0	0
VAP 2.6	0	0	0	0	0	0	0
VAP 2.7	0	0	0	0	0	0	0
VAP 2.8	0	0	0	0	0	0	0

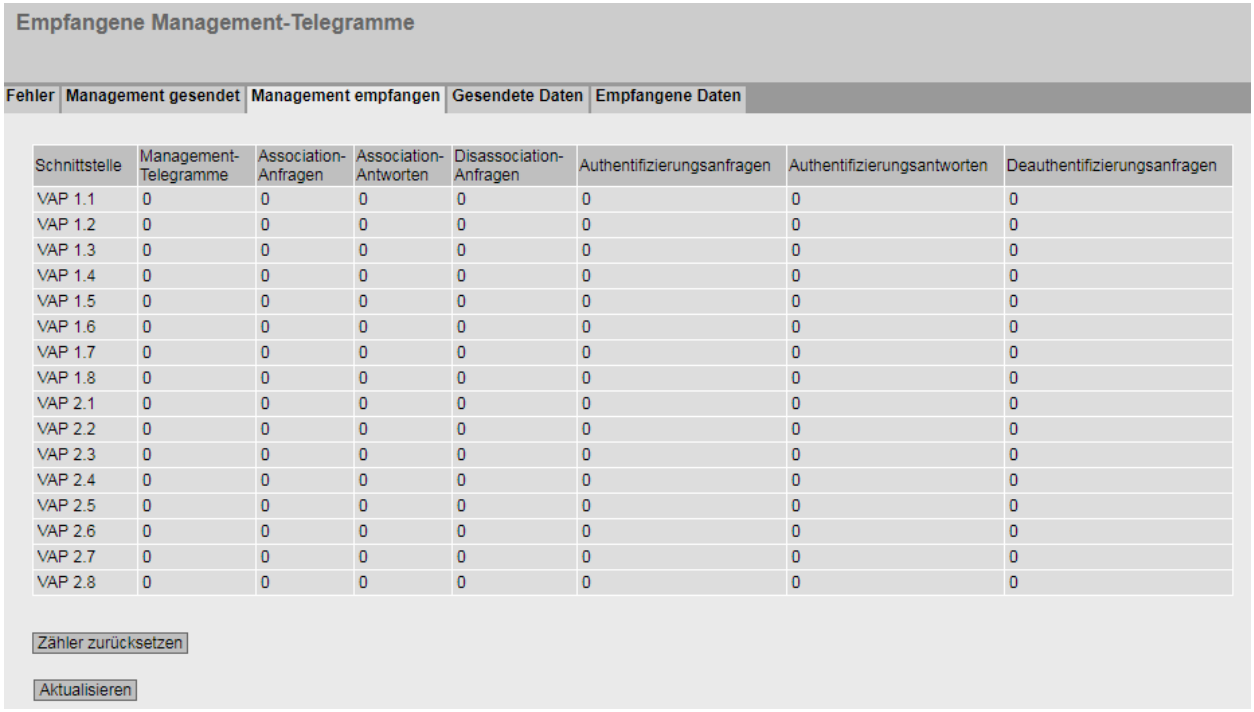
Beschreibung

Die Tabelle gliedert sich in Spalten wie folgt:

- **Schnittstelle**
  Zeigt die VAP-Schnittstelle an, auf die sich die Einträge beziehen.
- **Telegramm**
  - Management-Telegramme
    Zeigt die Anzahl der Management-Telegramme an
  - Association-Anfragen
    Zeigt die Anzahl der für einen Anmeldevorgang relevanten anfragenden Association-Telegramme an.
  - Association-Antworten
    Zeigt die Anzahl der für einen Anmeldevorgang relevanten antwortenden Association-Telegramme an.
  - Disassociation-Anfragen
    Zeigt die Anzahl der für einen Abmeldevorgang relevanten anfragenden Disassociation-Telegramme an.
  - Authentifizierungsanfragen
    Zeigt die Anzahl der für einen Anmeldevorgang relevanten anfragenden Authentifizierungstelegramme an.
  - Authentifizierungsantworten
    Zeigt die Anzahl der für einen Anmeldevorgang relevanten antwortenden Authentifizierungstelegramme an.
  - Deauthentifizierungsanfragen
    Zeigt die Anzahl der für einen Abmeldevorgang relevanten Deauthentifizierungstelegramme an.

6.4.17.3 Management empfangen

Die WBM-Seite zeigt an, wie viele Telegramme für den Anmeldevorgang bzw. Abmeldevorgang pro VAP-Schnittstelle gezählt wurden.



Schnittstelle	Management-Telegramme	Association-Anfragen	Association-Antworten	Disassociation-Anfragen	Authentifizierungsanfragen	Authentifizierungsantworten	Deauthentifizierungsanfragen
VAP 1.1	0	0	0	0	0	0	0
VAP 1.2	0	0	0	0	0	0	0
VAP 1.3	0	0	0	0	0	0	0
VAP 1.4	0	0	0	0	0	0	0
VAP 1.5	0	0	0	0	0	0	0
VAP 1.6	0	0	0	0	0	0	0
VAP 1.7	0	0	0	0	0	0	0
VAP 1.8	0	0	0	0	0	0	0
VAP 2.1	0	0	0	0	0	0	0
VAP 2.2	0	0	0	0	0	0	0
VAP 2.3	0	0	0	0	0	0	0
VAP 2.4	0	0	0	0	0	0	0
VAP 2.5	0	0	0	0	0	0	0
VAP 2.6	0	0	0	0	0	0	0
VAP 2.7	0	0	0	0	0	0	0
VAP 2.8	0	0	0	0	0	0	0

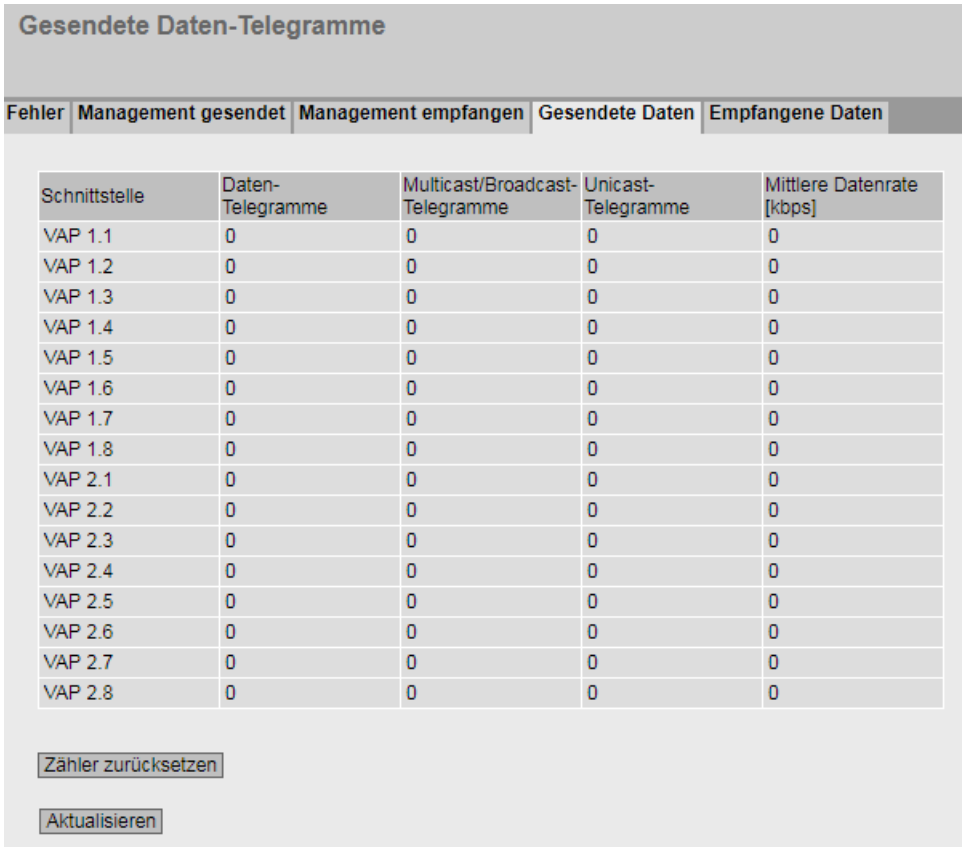
Beschreibung

Die Tabelle gliedert sich in Spalten wie folgt:

- **Schnittstelle**
  Zeigt die VAP-Schnittstelle an, auf die sich die Einträge beziehen.
- **Telegramm**
  - Management-Telegramme
    Zeigt die Anzahl der Management-Telegramme an
  - Association-Anfragen
    Zeigt die Anzahl der für einen Anmeldevorgang relevanten anfragenden Association-Telegramme an.
  - Association-Antworten
    Zeigt die Anzahl der für einen Anmeldevorgang relevanten antwortenden Association-Telegramme an.
  - Disassociation-Anfragen
    Zeigt die Anzahl der für einen Abmeldevorgang relevanten anfragenden Disassociation-Telegramme an.
  - Authentifizierungsanfragen
    Zeigt die Anzahl der für einen Anmeldevorgang relevanten anfragenden Authentifizierungstelegramme an.
  - Authentifizierungsantworten
    Zeigt die Anzahl der für einen Anmeldevorgang relevanten antwortenden Authentifizierungstelegramme an.
  - Deauthentifizierungsanfragen
    Zeigt die Anzahl der für einen Abmeldevorgang relevanten Deauthentifizierungstelegramme an.

6.4.17.4 Gesendete Daten

Die WBM-Seite zeigt an, wie viele Telegramme pro VAP-Schnittstelle gesendet wurden.



Schnittstelle	Daten-Telegramme	Multicast/Broadcast-Telegramme	Unicast-Telegramme	Mittlere Datenrate [kbps]
VAP 1.1	0	0	0	0
VAP 1.2	0	0	0	0
VAP 1.3	0	0	0	0
VAP 1.4	0	0	0	0
VAP 1.5	0	0	0	0
VAP 1.6	0	0	0	0
VAP 1.7	0	0	0	0
VAP 1.8	0	0	0	0
VAP 2.1	0	0	0	0
VAP 2.2	0	0	0	0
VAP 2.3	0	0	0	0
VAP 2.4	0	0	0	0
VAP 2.5	0	0	0	0
VAP 2.6	0	0	0	0
VAP 2.7	0	0	0	0
VAP 2.8	0	0	0	0

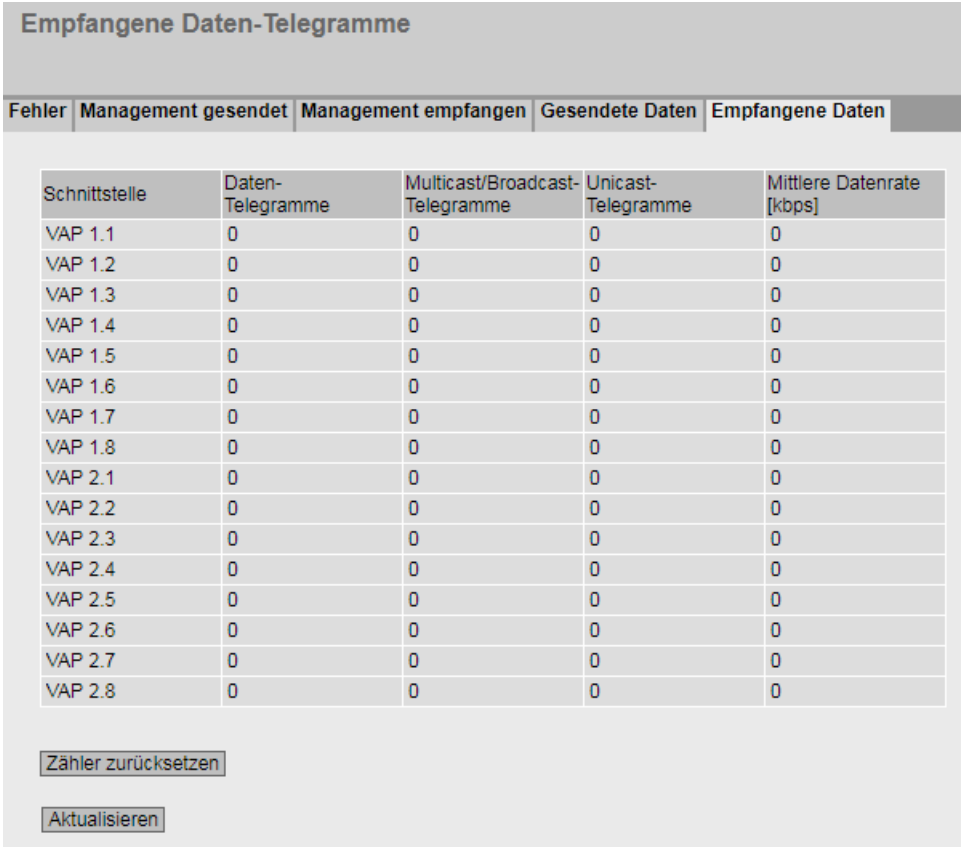
Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Schnittstelle**
  Zeigt die VAP-Schnittstelle an, auf die sich die Einträge beziehen.
- **Telegrammtypen**
  Die weiteren Spalten hinter der jeweiligen VAP-Schnittstelle enthalten die absoluten Zahlen der gesendeten Telegramme entsprechend der Telegrammtypen.
  Dabei wird in den Spalten der Tabelle nach folgenden Telegrammtypen unterschieden:
  - Daten-Telegramme
    Zeigt die Anzahl der gesendeten Datentelegramme an.
  - Multicast/Broadcast-Telegramme
    Zeigt die Anzahl der gesendeten Multicast- und Broadcast-Telegramme an.
  - Unicast-Telegramme
    Zeigt die Anzahl der gesendeten Unicast-Telegramme an.
  - Mittlere Datenrate [kbps]
    Zeigt die mittlere Datenrate der zuletzt gesendeten Datentelegramme an.

6.4.17.5 Empfangene Daten

Die WBM-Seite zeigt an, wie viele Telegramme pro VAP-Schnittstelle empfangen wurden.



Beschreibung

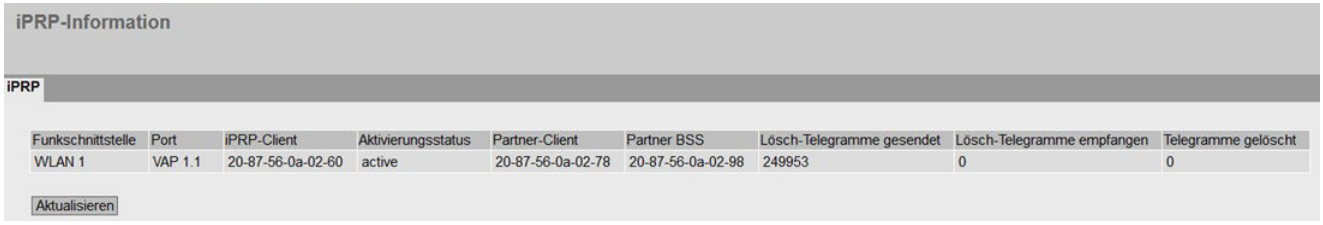
Die Tabelle gliedert sich in folgende Spalten:

- **Schnittstelle**
  Zeigt die VAP-Schnittstelle an, auf die sich die Einträge beziehen.
- **Telegrammtypen**
  Die weiteren Spalten hinter der jeweiligen VAP-Schnittstelle enthalten die absoluten Zahlen der empfangenen Telegramme entsprechend der Telegrammtypen.
  Dabei wird in den Spalten der Tabelle nach folgenden Telegrammtypen unterschieden:
  - Daten-Telegramme
    Zeigt die Anzahl der gesendeten Datentelegramme an.
  - Multicast/Broadcast-Telegramme
    Zeigt die Anzahl der gesendeten Multicast- und Broadcast-Telegramme an.
  - Unicast-Telegramme
    Zeigt die Anzahl der gesendeten Unicast-Telegramme an.
  - Mittlere Datenrate [kbps]
    Zeigt die mittlere Datenrate der zuletzt gesendeten Datentelegramme an.

6.4.18 WLAN iFeatures

6.4.18.1 iPRP

Auf dieser WBM-Seite können Sie prüfen, ob die Einstellungen für iPRP korrekt sind. Sie können z. B. sehen, welches Gerät der Partner-Client ist.



Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Funkschnittstelle**
  Zeigt die WLAN-Schnittstellen an, über die der Client mit dem Access Point verbunden ist.
- **Port** (nur im Access Point-Modus)
  Zeigt die VAP-Schnittstelle an, an der die iPRP-Clients angemeldet sind.
- **iPRP-Client**
  Zeigt die MAC-Adresse des iPRP-Clients an.
- **Aktivierungsstatus**
  Zeigt an, ob iPRP aktiv ist.
- **Partner-Client**
  Zeigt die MAC-Adresse des Partner-Clients an.
- **Partner BSS**
  Zeigt die MAC-Adresse des Access Points an, mit dem der Partner-Client verbunden ist.
- **Lösch-Telegramme gesendet**
  Zeigt die Anzahl der gesendeten iPRP-Lösch-Telegramme an, die das Gerät an sein Partnergerät gesendet hat.
- **Lösch-Telegramme empfangen**
  Zeigt die Anzahl der empfangenen iPRP-Lösch-Telegramme an, die das Gerät von seinem Partnergerät erhalten hat.
- **Telegramme gelöscht**
  Zeigt die Anzahl der noch nicht gesendeten Telegramme an, die aufgrund des iPRP-Lösch-Telegrammes aus der Warteschlange gelöscht wurden.

6.5 Menü "System"

6.5.1 Konfiguration

Systemkonfiguration

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

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

Zusätzlich ist bei einigen Diensten der Standard-Port änderbar.

Hinweis

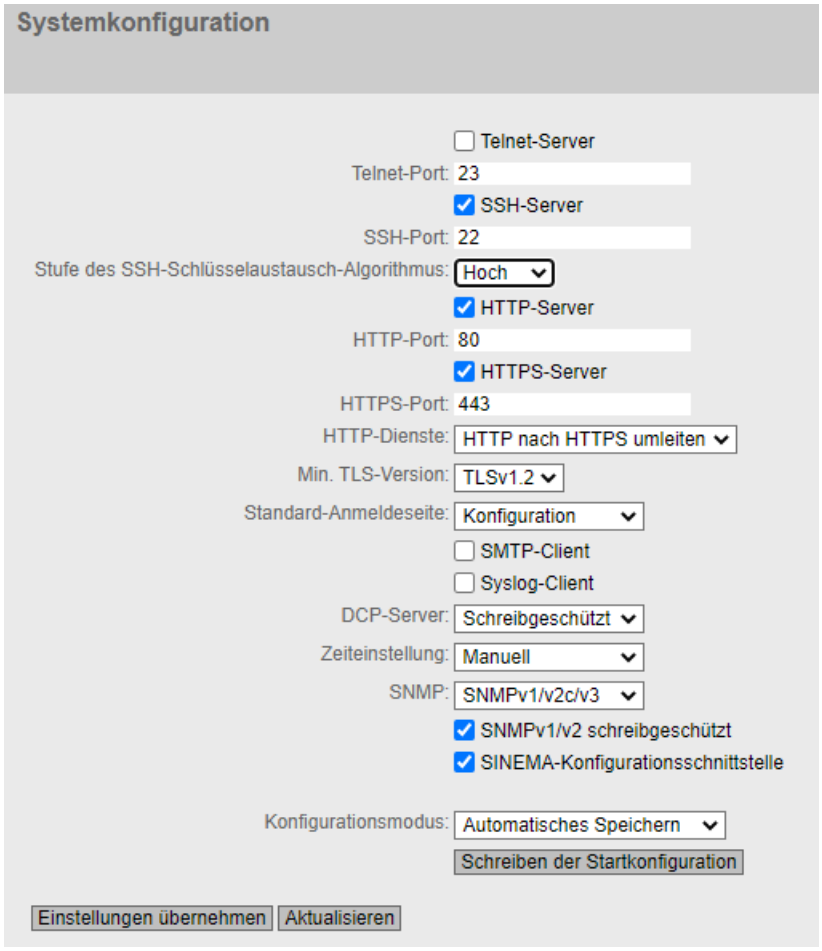
Standard-Port ändern

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

Wenn Sie den Standard-Port ändern, müssen Sie mit dem geänderten Port auf den Dienst zugreifen.

Reservierte Ports

Einige Ports sind fest reserviert. Stellen Sie sicher, dass der angegebene Port noch nicht verwendet wird. Die verwendeten Ports finden Sie in der "Liste verfügbarer Dienste".



Beschreibung

Die Seite enthält folgende Felder:

- **Telnet-Server**
  Aktivieren oder deaktivieren Sie den Dienst "Telnet-Server" für den unverschlüsselten Zugriff auf das CLI.
- **Telnet-Port**
  Voreingestellt ist der Standard-Port 23. Optional können Sie eine Portnummer im Bereich 1024 ... 49151oder 49500 ... 65535 eintragen.
- **SSH-Server**
  Aktivieren oder deaktivieren Sie den Dienst "SSH-Server" für den verschlüsselten Zugriff auf das CLI.
- **SSH-Port**
  Voreingestellt ist der Standard-Port 22. Optional können Sie eine Portnummer im Bereich 1024 ... 49151 oder 49500 ... 65535 eintragen.

- **Stufe des SSH-Schlüsselaustausch-Algorithmus**
  Wählen Sie aus der Klappliste die Stufe des SSH-Schlüsselaustausch-Algorithmus für den SSH-Zugriff auf das CLI. Es gibt die Einstellmöglichkeiten "Niedrig" und "Hoch". Die beiden Stufen beinhalten die folgenden Verschlüsselungsalgorithmen:

  – Hoch
    Curve25519-sha256
    Curve25519-sha256@libssh.org
    Ecdh-sha2-nistp256
    Ecdh-sha2-nistp384
    Ecdh-sha2-nistp521
    Diffie-hellman-group16-sha512
    Diffie-hellman-group18-sha512

  – Niedrig
    Curve25519-sha256
    Curve25519-sha256@libssh.org
    Ecdh-sha2-nistp256
    Ecdh-sha2-nistp384
    Ecdh-sha2-nistp521
    Diffie-hellman-group16-sha512
    Diffie-hellman-group18-sha512
    Diffie-hellman-group14-sha256
    Diffie-hellman-group14-sha1

  Mit der Einstellung "Niedrig" können Sie mit folgenden SSH-Clients keine Verbindung aufbauen, weil diese Programme die entsprechenden Algorithmen nicht unterstützen:

  – TeraTerm

  – PuTTY

  – STS

- **HTTP-Server**
  Aktivieren oder deaktivieren Sie den Dienst "HTTP-Server" für den unverschlüsselten Zugriff auf das WBM.

- **HTTP-Port**
  Voreingestellt ist der Standard-Port 80. Optional können Sie eine Portnummer im Bereich 1024 ... 49151 oder 49500 ... 65535 eintragen.

- **HTTPS-Server**
  Aktivieren oder deaktivieren Sie den Dienst HTTPS-Server für den verschlüsselten Zugriff auf das WBM.

- **HTTPS-Port**
  Voreingestellt ist der Standard-Port 443. Optional können Sie eine Portnummer im Bereich 1024 ... 49151 oder 49500 ... 65535 eintragen.

- **HTTP-Dienste**
  Legen Sie fest, wie auf das WBM zugegriffen wird:
  - HTTPS
    Zugriff auf das WBM nur über HTTPS möglich.
  - HTTP/HTTPS
    Zugriff auf das WBM über HTTP und HTTPS möglich.
  - HTTP nach HTTPS umleiten
    Beim Zugriff über HTTP wird automatisch nach HTTPS umgeleitet.
- **Min. TLS-Version**
  Wählen Sie aus der Klappliste die TLS-Version, die für die Verschlüsselung mindestens verwendet werden soll. Mit Geräten, die die geforderte TLS-Version nicht unterstützen, ist keine Kommunikation möglich.
- **SMTP-Client**
  Aktivieren oder deaktivieren Sie den SMTP-Client. Weitere Einstellungen konfigurieren Sie unter "System > SMTP-Client".
- **Syslog-Client**
  Aktivieren oder deaktivieren Sie den Syslog-Client. Weitere Einstellungen konfigurieren Sie unter "System > Syslog-Client".
- **DCP-Server**
  Legen Sie fest, ob auf das Gerät mit DCP (Discovery and Configuration Protocol) zugegriffen werden kann:
  - "-" (Deaktiviert)
    DCP ist deaktiviert. Geräteparameter können weder gelesen noch geändert werden.
  - Lesen/Schreiben
    Mit DCP können Geräteparameter sowohl gelesen als auch verändert werden.
  - Schreibgeschützt
    Mit DCP können Geräteparameter zwar gelesen aber nicht verändert werden.
- **Zeiteinstellung**
  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellungen sind möglich:
  - Manuell
    Die Systemzeit wird manuell eingestellt. Weitere Einstellungen konfigurieren Sie unter "System > Systemzeit > Manuelle Einstellung".
  - SIMATIC Time
    Die Systemzeit wird über einen SIMATIC Zeitgeber eingestellt. Weitere Einstellungen konfigurieren Sie unter "System > Systemzeit > SIMATIC Time Client".
  - SNTP-Client
    Die Systemzeit wird über einen SNTP Server eingestellt. Weitere Einstellungen konfigurieren Sie unter "System > Systemzeit > SNTP-Client".
  - NTP-Client
    Die Systemzeit wird über einen NTP Server eingestellt. Weitere Einstellungen konfigurieren Sie unter "System > Systemzeit > NTP-Client".

- **SNMP**
  Wählen Sie aus der Klappliste das Protokoll. Folgende Einstellungen sind möglich:
  - "-" (SNMP deaktiviert)
    Ein Zugriff auf die Geräteparameter ist über SNMP nicht möglich.
  - SNMPv1/v2c/v3
    Ein Zugriff auf die Geräteparameter ist mit den SNMP-Versionen 1, 2c oder 3 möglich. Weitere Einstellungen konfigurieren Sie unter "System > SNMP > Allgemein".
  - SNMPv3
    Ein Zugriff auf die Geräteparameter ist nur mit der SNMP-Version 3 möglich. Weitere Einstellungen konfigurieren Sie unter "System > SNMP > Allgemein".
- **SNMPv1/v2 schreibgeschützt**
  Aktivieren oder deaktivieren Sie den schreibenden Zugriff auf SNMP-Variablen bei SNMPv1/v2c.
- **SINEMA-Konfigurationsschnittstelle**
  Wenn die SINEMA-Konfigurationsschnittstelle aktiviert ist, können Sie Konfigurationen über das TIA-Portal auf das Gerät laden.
- **Konfigurationsmodus**
  Wählen Sie aus der Klappliste die Betriebsart. Folgende Betriebsarten sind möglich:
  - Automatisches Speichern
    Automatischer Sicherungsbetrieb. Ca. 1 Minute nach der letzten Parameteränderung oder beim Neustart des Geräts wird die Konfiguration automatisch abgespeichert. Zusätzlich wird im Anzeigebereich die Meldung "Die Änderungen werden automatisch in x Sekunden gespeichert. Um die Änderungen sofort zu speichern, klicken Sie auf 'Schreiben der Startkonfiguration'."

    Hinweis

    Unterbrechung des Speichervorgangs

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

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

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

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

Vorgehensweise

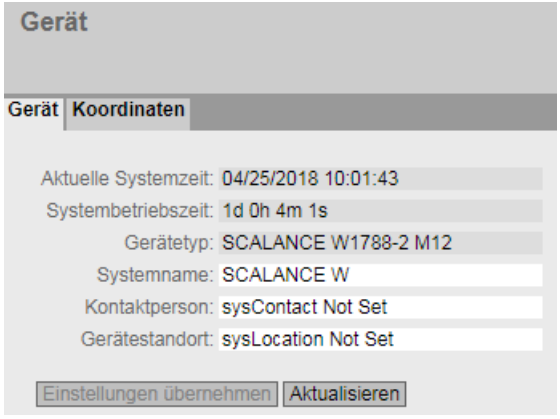
1. Um die gewünschte Funktion zu nutzen, aktivieren Sie das betreffende Optionskästchen.
2. Wählen Sie aus den Klapplisten die gewünschten Optionen.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.5.2 Allgemein

6.5.2.1 Gerät

Allgemeine Geräteinformationen

Diese Seite enthält die allgemeinen Geräteinformationen.



Die Felder "Aktuelle Systemzeit", "Systembetriebszeit" und "Gerätetyp" können nicht geändert werden.

Beschreibung

Die Seite enthält folgende Felder:

- **Aktuelle Systemzeit**
  Zeigt die aktuelle Systemuhrzeit an. Die Systemuhrzeit wird entweder vom Anwender eingestellt oder per Uhrzeittelegramm synchronisiert: entweder SINEC H1 Uhrzeittelegramm, NTP oder SNTP. (Nur lesbar)
- **Systembetriebszeit**
  Zeigt die Laufzeit des Geräts seit dem letzten Neustart an. (Nur lesbar)
- **Gerätetyp**
  Zeigt die Typenbezeichnung des Geräts an. (Nur lesbar)

- **Systemname**
  Sie können den Namen des Geräts eintragen. Der eingetragene Name wird im Auswahlbereich angezeigt. Es sind maximal 255 Zeichen möglich.
  Der Systemname wird auch in der CLI-Eingabeaufforderung (Prompt) angezeigt. In der CLI-Eingabeaufforderung ist die Anzahl der Zeichen begrenzt. Der Systemname wird nach 16 Zeichen abgeschnitten.
- **Kontaktperson**
  Sie können den Namen einer Kontaktperson eintragen, die für die Verwaltung des Geräts zuständig ist. Es sind maximal 255 Zeichen möglich.
- **Gerätestandort**
  Sie können den Montageort des Geräts eintragen. Der eingetragene Montageort wird im Auswahlbereich angezeigt. Es sind maximal 255 Zeichen möglich.

Hinweis

In den Eingabefeldern wird der ASCII-Code 0x20 bis 0x7e verwendet.

Vorgehensweise

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

6.5.2.2 Koordinaten

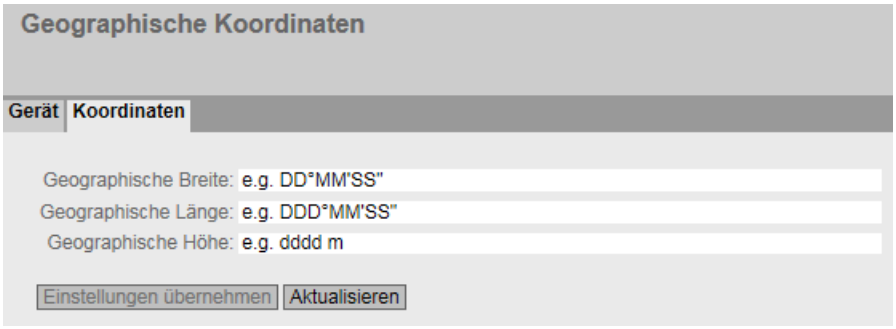
Informationen über die geografischen Koordinaten

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

Ermittlung der Koordinaten

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

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



Beschreibung

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

- **Eingabefeld "Geographische Breite"**
  Geografische Breite: Hier wird der Wert für nördliche oder südliche Breite für den Standort des Geräts eingegeben.
  Der Wert +49° 1´31.67" bedeutet, dass sich das Gerät auf 49 Grad, 1 Bogenminute und 31.67 Bogensekunden nördlicher Breite befindet.
  Die südliche Breite wird mit einem führenden Minuszeichen dargestellt.
  Sie können auch die Buchstaben N (nördliche Breite) oder S (südliche Breite) an die Zahlenangabe anhängen (49° 1´31.67" N).
- **Eingabefeld "Geographische Länge"**
  Geografische Länge: Hier wird der Wert für östliche oder westliche Länge für den Standort des Geräts eingegeben.
  Der Wert +8° 20´58.73" bedeutet, dass sich das Gerät auf 8 Grad, 20 Bogenminuten und 58.73 Bogensekunden östlicher Länge befindet.
  Die westliche Länge wird mit einem führenden Minuszeichen dargestellt.
  Sie können auch die Buchstaben O bzw. E (östliche Länge) oder W (westliche Länge) an die Zahlenangabe anhängen (8° 20´58.73" E).
- **Eingabefeld: "Geographische Höhe"**
  Geografische Höhe: Hier wird der Wert für geografische Höhe über oder unter normal Null (Meereshöhe) in Metern eingegeben.
  Z.B. 158 m bedeutet, dass sich das Gerät in einer Höhe von 158 m über normal Null befindet.
  Höhenangaben unterhalb von normal Null (z. B. am Toten Meer) werden mit einem führenden Minuszeichen dargestellt.

Vorgehensweise

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

6.5.3 Agent IPv4 / IPv6

Die Aufrufe verweisen auf folgende Menüpunkte:

- Agent IPv4: Layer 3 (IPv4) > Subnetze
- Agent IPv6: Layer 3 (IPv6) > Subnetze

6.5.4 DNS

6.5.4.1 DNS Client

Auf dieser Seite können Sie bis zu 3 DNS-Server mit IPv4- oder IPv6-Adressen manuell konfigurieren. Manuell konfigurierten DNS-Servern wird jeweils ein Index von 1 bis 3 zugeordnet. Das Gerät kann über DHCP 2 DNS-Server mit IPv4-Adressen lernen. Gelernten DNS-Servern wird automatisch ein Index von 4 bis 7 zugeordnet.

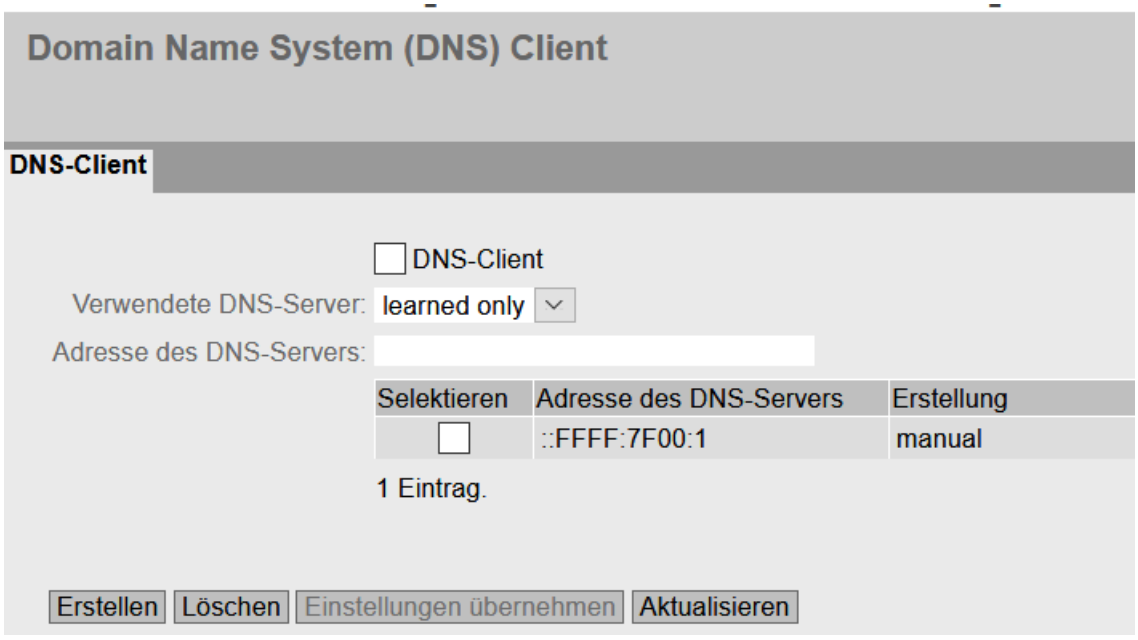
Bei mehreren DNS-Servern ist durch die Reihenfolge in der Tabelle festgelegt, in welcher Reihenfolge die Server angefragt werden. Der obere Server wird zuerst angefragt. Insgesamt können auf dem Gerät 7 DNS-Server konfiguriert sein. Manuell konfigurierte DNS-Server werden bevorzugt.

Der DNS-Server (Domain Name System) ordnet einer IP-Adresse einen Domainnamen zu, sodass ein Gerät eindeutig identifiziert werden kann.

Wenn diese Funktion aktiviert ist, kann das Gerät als DNS-Client mit einem DNS-Server kommunizieren. Sie haben die Möglichkeit Namen in IP-Adressfeldern einzutragen.

Hinweis

Um die Funktion "DNS-Client" zu nutzen, muss sich ein DNS-Server im Netzwerk befinden.



Beschreibung

Die Seite enthält folgende Felder:

- **DNS-Client**
  Aktivieren oder deaktivieren Sie das Optionskästchen, dass das Gerät als DNS-Client fungiert.
- **Verwendete DNS-Server**
  Hier legen Sie fest, welche DNS-Server das Gerät verwendet:
  - learned only
    Das Gerät verwendet nur die durch DHCP zugewiesenen DNS-Server.
  - manual only
    Das Gerät verwendet nur die manuell projektierten DNS-Server. Die DNS-Server müssen mit dem Internet verbunden sein. Maximal drei DNS-Server sind projektierbar.
  - all
    Das Gerät verwendet alle verfügbaren DNS-Server.
- **Adresse des DNS-Servers**
  Geben Sie die IP-Adresse des DNS-Servers ein.

Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Adresse des DNS-Servers**
  Zeigt die IP-Adresse des DNS-Servers an.
- **Erstellung**
  Hier wird angezeigt, ob der DNS-Server manuell konfiguriert wurde oder durch DHCP zugewiesen wurde.

Vorgehensweise

DNS aktivieren

1. Aktivieren Sie das Optionskästchen "DNS-Client".
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

DNS-Server anlegen

1. Geben Sie im Feld "Adresse des DNS-Servers" die IP-Adresse des DNS-Servers ein.
2. Klicken Sie auf die Schaltfläche "Erstellen".

DNS-Server filtern

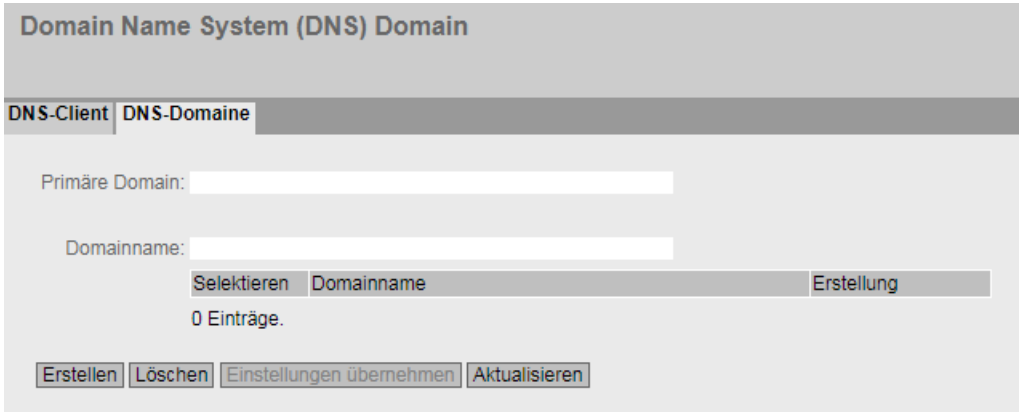
1. Wählen Sie in der Klappliste "Verwendete DNS-Server" aus, welche DNS-Server verwendet werden sollen.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.5.4.2 DNS Domain

Auf dieser Seite können Sie bis zu 4 Domainnamen festlegen. Der primäre Domainname wird zuerst herangezogen, um einen Hostnamen aufzulösen.

Die Domainnamen 2 bis 4 können gelernt oder auf dieser Seite manuell konfiguriert werden. Bei mehreren DNS-Servern ist durch die Reihenfolge in der Tabelle festgelegt, in welcher Reihenfolge die Domainnamen herangezogen werden.

Wenn Domainnamen hinterlegt sind, haben Sie bei einigen IP-Adressfeldern die Möglichkeit, den Hostnamen einzutragen.



Beschreibung

Die Seite enthält folgende Felder:

- **Primäre Domain**
  Geben Sie den Namen der primären Domain ein. Dieser Eintrag wird zuerst herangezogen, um einen Hostnamen aufzulösen.
- **Domainname**
  Geben Sie den Namen der weiteren Domain ein.

Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Domainname**
  Zeigt den Namen der weiteren Domain an.
- **Erstellung**
  Zeigt an, ob der Domainname manuell konfiguriert wurde oder durch DHCP zugewiesen wurde.

Vorgehensweise

Primäre Domain festlegen

1. Geben Sie im Feld "Primäre Domain" die Bezeichnung der primären Domain ein.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

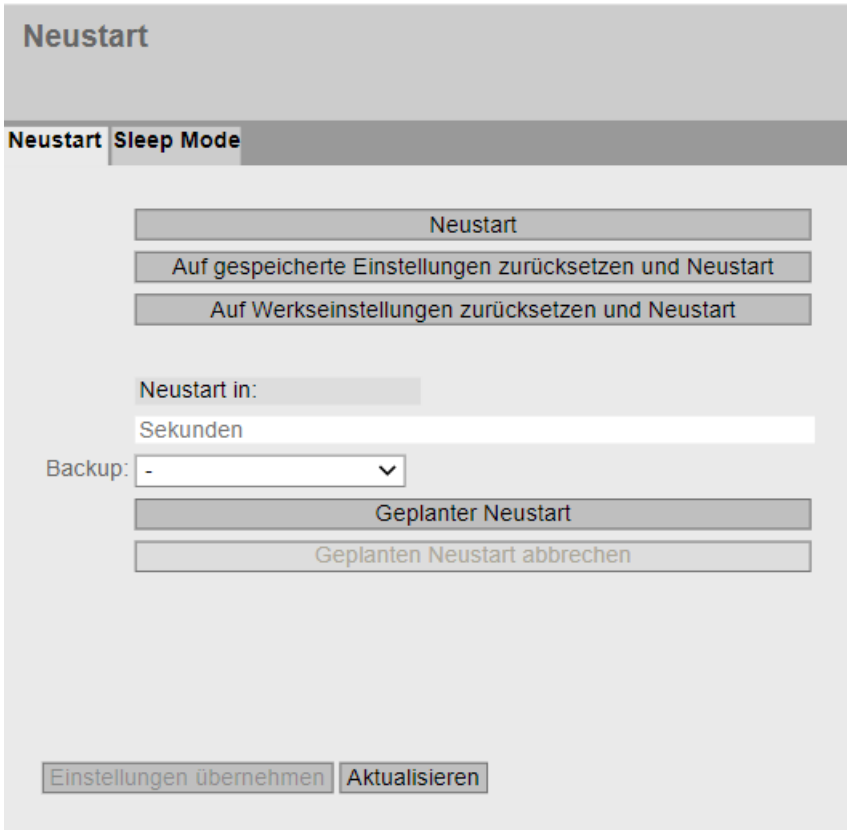
Weitere Domain festlegen

1. Geben Sie im Feld "Domainname" die Bezeichnung für die weiteren Domains ein.
2. Klicken Sie auf die Schaltfläche "Erstellen".

6.5.5 Neustart

Zurücksetzen der Voreinstellungen

Über diese WBM-Seite können Sie das Gerät geplant oder manuell neu starten. Außerdem gibt es verschiedene Möglichkeiten die Voreinstellungen des Geräts zurückzusetzen.



Neustart

Beachten Sie folgende Punkte beim Neustart eines Geräts:

- Sie können einen Neustart des Geräts nur mit Administrator-Rechten durchführen.
- Der Neustart eines Geräts sollte nur durch die Schaltflächen dieses Menüs oder durch die entsprechenden CLI-Befehle und nicht durch Aus- und Einschalten der Spannungsversorgung am Gerät erfolgen.
- Wenn sich das Gerät im Modus "Trial" befindet, müssen Konfigurationsänderungen vor einem Neustart manuell abgespeichert werden. Vorgenommene Änderungen werden erst nach dem Anklicken der Schaltfläche "Einstellungen übernehmen" auf der jeweiligen WBM-Seite im Gerät wirksam.
- Wenn sich das Gerät im Modus "Automatisches Speichern" befindet, werden die letzten Änderungen automatisch vor einem Neustart gespeichert.

Beschreibung

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

- **Neustart**
  Klicken Sie auf diese Schaltfläche, um das System neu zu starten. Sie müssen den Neustart in einer Dialogbox bestätigen. Bei einem Neustart wird das Gerät neu initialisiert, die interne Firmware wird neu geladen und das Gerät führt einen Selbsttest durch. Die Einstellungen der Startkonfiguration bleiben erhalten, z. B. die IP-Adresse des Geräts. Die gelernten Einträge in der Adresstabelle werden gelöscht. Sie können das Browser-Fenster geöffnet lassen, während das Gerät neu startet. Nach dem Neustart müssen Sie sich wieder neu anmelden.
- **Auf gespeicherte Einstellungen zurücksetzen und Neustart**
  Klicken Sie diese Schaltfläche, um die Werkseinstellungen des Geräts mit Ausnahme der folgenden Parameter wiederherzustellen und das Gerät neu zu starten:
  - IP-Adressen
  - Subnetzmaske
  - IP-Adresse des Standard-Gateways
  - DHCP Client ID
  - DHCP
  - Systemname
  - System-Aufstellungsort
  - System-Ansprechpartner
  - Benutzernamen und Passwörter
  - Betriebsart des Geräts
  - DHCPv6 Rapid Commit
- **Auf Werkseinstellungen zurücksetzen und Neustart**
  Klicken Sie auf diese Schaltfläche, um die werksseitigen Konfigurationseinstellungen wiederherzustellen und das Gerät neu zu starten. Sie müssen den Neustart in einer Dialogbox bestätigen.

  Hinweis

  Durch das Zurücksetzen aller Voreinstellungen auf die werkseitigen Konfigurationseinstellungen geht auch die IP-Adresse verloren. Das Gerät ist danach nur über SINEC PNI oder über DHCP ansprechbar.

  Bei entsprechendem Anschluss kann ein zuvor korrekt konfiguriertes Gerät kreisende Telegramme und damit den Ausfall des Datenverkehrs verursachen.

- **Neustart in Sekunden**
  Dieses Feld wird zum Einstellen des Timers benutzt. Das Feld ist nicht mehr editierbar, wenn der Timer läuft.
  Geben Sie die Zeitdauer in Sekunden an, nach der das Gerät neu startet.
  Wertebereich 300 ... 86400 Sekunden

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

  Hinweis

  Nicht gespeicherte Konfiguration geht nach Neustart verloren

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

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

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

6.5.6 Verwaltung von Änderungen

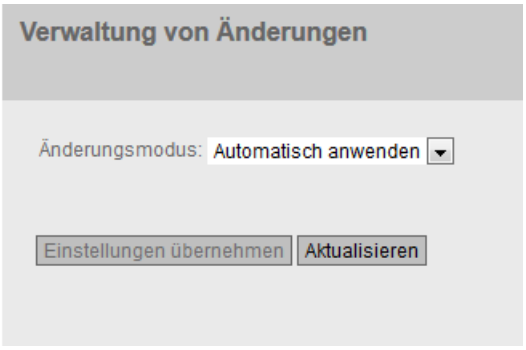
Änderungsverwaltung

Mit dieser Seite legen Sie fest, wann die WLAN-Einstellungen auf dem SCALANCE W-Gerät wirksam werden.
Wenn Sie eine WLAN-Einstellung ändern und die Änderung mit "Einstellungen übernehmen" bestätigen, wird diese Änderung übernommen und ist sofort wirksam. Hierfür wird die WLAN-Verbindung kurzzeitig unterbrochen. Somit können sie die WLAN-Verbindung zu ihrem SCALANCE W-Gerät verlieren, bevor es komplett konfiguriert ist.

Die Einstellung "Manuell anwenden" bietet Ihnen die Möglichkeit, das SCALANCE W-Gerät erst fertig zu konfigurieren. Die Änderungen werden zwar übernommen, sind aber nicht sofort wirksam. Die Änderungen werden erst wirksam, wenn Sie mit der Schaltfläche "Änderungen anwenden" die Änderungen bestätigen.

Hinweis

Wenn Sie das SCALANCE W-Gerät über die WLAN-Schnittstelle konfigurieren, wird empfohlen die Einstellung "Manuell anwenden" zu verwenden. Überprüfen Sie nochmals die Parameter, bevor Sie die Änderungen mit der Schaltfläche "Änderungen anwenden" bestätigen.



Beschreibung

Die Seite enthält folgende Felder:

- **Änderungsmodus**
  Wählen Sie aus der Klappliste die gewünschte Einstellung aus:
  - Automatisch anwenden
    Jede Änderung in den WLAN-Einstellungen wird übernommen und ist sofort wirksam, wenn Sie auf die Schaltfläche "Einstellungen übernehmen" klicken. Das SCALANCE W-Gerät ist in der Grundeinstellung auf "Automatisch anwenden" eingestellt.
  - Manuell anwenden
    Die Änderungen werden übernommen, sind aber nicht sofort wirksam. Die Änderungen werden erst wirksam, wenn Sie auf die Schaltfläche "Änderungen anwenden" klicken. Die Schaltfläche "Änderungen anwenden" wird eingeblendet, wenn Sie "Manuell anwenden" einstellen.
    Zusätzlich wird im Anzeigebereich die folgende Meldung angezeigt: "Der Änderungsmodus 'Manuell anwenden' ist aktiviert ". Klicken Sie auf die Schaltfläche 'Änderungen anwenden', um dem Treiber die aktuelle Konfiguration zu übergeben." angezeigt, sobald es WLAN-Änderungen gibt. Diese Meldung ist auf jeder WBM-Seite sichtbar, bis die vorgenommenen Änderungen entweder wirksam werden oder das SCALANCE W-Gerät neu gestartet wird.

    Hinweis

    Wenn die Änderungen wirksam werden, werden die WLAN-Verbindungen an allen WLAN-Schnittstellen für kurze Zeit unterbrochen. Der WLAN-Treiber wird mit den neuen Einstellungen gestartet.

6.5.7 Laden & Speichern

6.5.7.1 Dateiliste

Übersicht der Dateitypen

Tabelle 6-1 HTTP

Dateityp	Beschreibung	Laden	Speichern	Löschen
Config	Diese Datei enthält die Startkonfiguration. Diese Datei enthält unter anderem die Definitionen der Benutzer, Rollen, Gruppen und Funktionsrechte. Die Passwörter sind in der Datei "Users" abgespeichert. Die Datei kann vor dem Herunterladen mit einem Passwort versehen werden. Um die Datei erfolgreich ins Gerät zuladen, ist das festgelegte Passwort zu verwenden. Das Passwort geben Sie auf der WBM-Seite "Passwörter (Seite 185)" ein. Wenn die Datei mit einem Passwort geschützt ist, können Sie die Datei nicht über DHCP mit den Optionen 66 und 67 laden.	X	X	--
ConfigPack	Detaillierte Konfigurationsinformationen z. B. Startkonfiguration, Benutzer, Zertifikate, Favoriten Firmware des Geräts (wenn mitgespeichert). Die Datei kann vor dem Herunterladen mit einem Passwort versehen werden. Um die Datei erfolgreich ins Gerät zuladen, ist das festgelegte Passwort zu verwenden. Das Passwort geben Sie auf der WBM-Seite "Passwörter (Seite 185)" ein. Nähere Informationen zur Erstellung und Benutzung des ConfigPack inkl. Firmware finden Sie in Kapitel "Instandhalten und Warten (Seite 363)". Wenn die Datei mit einem Passwort geschützt ist, können Sie die Datei nicht über DHCP mit den Optionen 66 und 67 laden.	X	X	--
ConfigPackBackup	In dieser ZIP-Datei sind alle Konfigurationsbackups gespeichert, die Sie erstellt haben.	X	X	X
LicenseConditions	Die zip-Datei enthält die Lizenzbedingungen und Copyright-Hinweise	--	X	--
CountryList	Die Zip-Datei enthält die Länderliste als csv- und als pdf-Datei.	--	X	--
Debug	Diese Datei beinhaltet Informationen für den Siemens Support. Sie ist verschlüsselt und kann ohne Sicherheitsrisiko per E-Mail an den Siemens Support gesendet werden.	--	X	X
EDS	Electronic Data Sheet (EDS) Elektronische Datenblätter zur Beschreibung von Geräten im EtherNet/IP-Betrieb	--	X	--
Firmware	Die Firmware ist signiert und verschlüsselt. Damit ist sichergestellt, dass nur von Siemens erstellte Firmware in das Gerät geladen werden kann.	X	X	--
GSDML	Informationen über die Geräteeigenschaften (PROFINET)	--	X	--
HTTPS Cert	HTTPS-Zertifikat Maximale Dateigröße: 8192 Bit	X	X	X

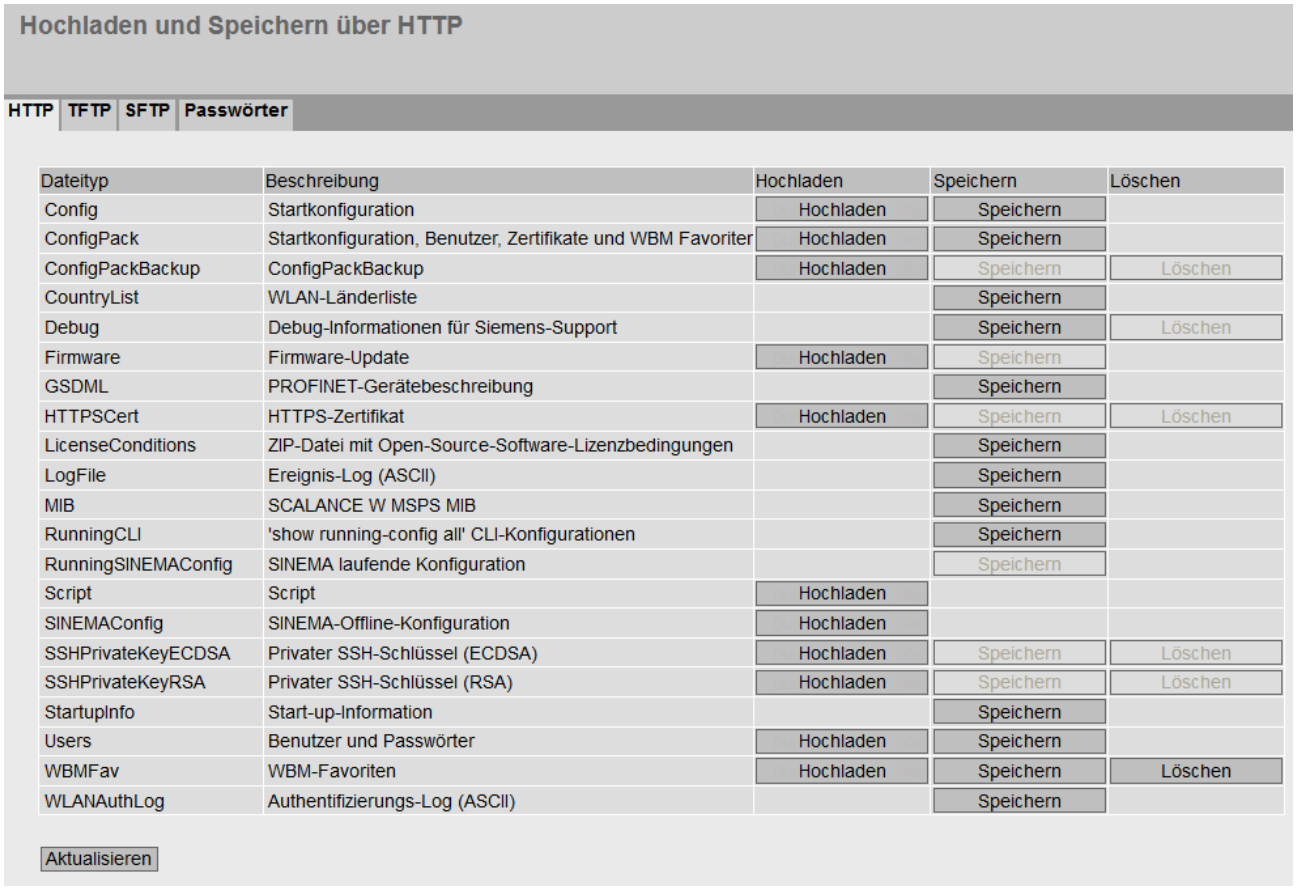
Dateityp	Beschreibung	Laden	Speichern	Löschen
LogFile	Datei mit Einträgen aus der Ereignisprotokolltabelle	--	X	--
MIB	Private MSPS MIB-Datei "Scalance_w_msps.mib"	--	X	--
RunningCLI	Textdatei mit CLI-Befehlen Diese Datei enthält eine Übersicht der aktuellen Konfiguration in Form von CLI-Befehlen. Passwörter sind in dieser Datei wie folgt maskiert: [PASSWORD] Sie können die Textdatei herunterladen. Die Datei ist nicht dafür vorgesehen, dass Sie sie unverändert wieder hochladen.	--	X	--
Script	Textdatei mit CLI-Befehlen	X	--	--
SSHPrivate-KeyECDSA	SSH Privater Schlüssel (ECDSA) Unterstützt wird der SSH-Schlüssel ecdsa-sha2-nistp521. Es gibt Dateien, deren Zugriff passwortgeschützt ist. Um die Datei erfolgreich ins Gerät zuladen, geben Sie auf der WBM-Seite "Passwörter (Seite 185)" das für die Datei festgelegte Passwort ein.	X	X	X
SSHPrivateKeyRSA	SSH Privater Schlüssel (RSA) mit und ohne Passwort Unterstützt werden die folgenden SSH-Schlüssel: • rsa-sha2-512 • rsa-sha2-256 Es gibt Dateien, deren Zugriff passwortgeschützt ist. Um die Datei erfolgreich ins Gerät zuladen, geben Sie auf der WBM-Seite "Passwörter (Seite 185)" das für die Datei festgelegte Passwort ein.	X	X	X
StartupInfo	Startup Logdatei Diese Datei enthält die Meldungen, die während des letzten Hochlaufs in der Logdatei eingetragen wurden.	--	X	--
Users	Datei mit Benutzernamen und Passwörter	X	X	--
WBMFav	WBM Favoriten Diese Datei enthält die Favoriten, die Sie im WBM angelegt haben. Sie können diese Datei herunterladen und in anderen Geräten hochladen.	X	X	X
WLANAuthlog	Datei mit Einträgen aus dem WLAN Authentication Log (Informationen zu erfolgreichen oder fehlgeschlagenen Authentifizierungsversuchen)	--	X	--
WLANCert (Nur im Client-Modus)	Benutzerzertifikat. Für das Benutzerzertifikat können Sie auf der WBM-Seite "Load&Save > Password" ein Passwort festlegen. Maximale Dateigröße: 8192 Bit	X	X	X
WLANServCert (Nur im Client-Modus)	Serverzertifikat Maximale Dateigröße: 8192 Bit	X	X	X
WLANSigRec (Nur im Client-Modus)	Die Zip-Datei enthält Folgendes: • csv-Datei mit den Messwerten des Signalrekorders • pdf-Datei mit den Messwerten und einer zusätzlichen grafischen Darstellung der Messwerte. Die Informationen zu den Messwerten und deren grafische Darstellung finden Sie im Kapitel "Signalrekorder (Seite 269)".	--	X	X

Tabelle 6-2 TFTP/SFTP

Dateityp	Beschreibung	Speichern	Laden
Config	Diese Datei enthält die Startkonfiguration. Diese Datei enthält unter anderem die Definitionen der Benutzer, Rollen, Gruppen und Funktionsrechte. Die Passwörter sind in der Datei "Users" abgespeichert. Die Datei kann vor dem Herunterladen mit einem Passwort versehen werden. Um die Datei erfolgreich ins Gerät zuladen, ist das festgelegte Passwort zu verwenden. Das Passwort geben Sie auf der WBM-Seite "Passwörter (Seite 185)" ein. Wenn die Datei mit einem Passwort geschützt ist, können Sie die Datei nicht über DHCP mit den Optionen 66 und 67 laden.	X	X
ConfigPack	Detaillierte Konfigurationsinformationen z. B. Startkonfiguration, Benutzer, Zertifikate, Favoriten Firmware des Geräts (wenn mitgespeichert). Die Datei kann vor dem Herunterladen mit einem Passwort versehen werden. Um die Datei erfolgreich ins Gerät zuladen, ist das festgelegte Passwort zu verwenden. Das Passwort geben Sie auf der WBM-Seite "Passwörter (Seite 185)" ein. Wenn die Datei mit einem Passwort geschützt ist, können Sie die Datei nicht über DHCP mit den Optionen 66 und 67 laden. Nähere Informationen zur Erstellung und Benutzung des ConfigPack inkl. Firmware finden Sie in Kapitel "Instandhalten und Warten (Seite 363)".	X	X
ConfigPackBackup	In dieser ZIP-Datei sind alle Konfigurationsbackups gespeichert, die Sie erstellt haben.	X	X
LicenseConditions	Die zip-Datei enthält die Lizenzbedingungen und Copyright-Hinweise	X	--
CountryList	Die Zip-Datei enthält die Länderliste als csv- und als pdf-Datei.	X	--
Debug	Diese Datei beinhaltet Informationen für den Siemens Support. Sie ist verschlüsselt und kann ohne Sicherheitsrisiko per E-Mail an den Siemens Support gesendet werden.	X	--
EDS	Electronic Data Sheet (EDS) Elektronische Datenblätter zur Beschreibung von Geräten im EtherNet/IP-Betrieb	X	--
Firmware	Die Firmware ist signiert und verschlüsselt. Damit ist sichergestellt, dass nur von Siemens erstellte Firmware in das Gerät geladen werden kann.	X	X
GSDML	Informationen über die Geräteeigenschaften (PROFINET)	X	--
HTTPSCert	Voreingestellte HTTPS-Zertifikate inkl. Schlüssel Die voreingestellten und automatisch erstellten HTTPS-Zertifikate sind selbstsigniert. Es wird dringend empfohlen eigene HTTPS-Zertifikate zu erstellen und bereitzustellen. Es wird empfohlen HTTPS-Zertifikate zu verwenden, die entweder durch eine zuverlässige externe oder eine interne Zertifizierungsstelle signiert sind. Das HTTPS-Zertifikat überprüft die Identität des Geräts und regelt den verschlüsselten Datenaustausch. Es gibt Dateien, deren Zugriff passwortgeschützt ist. Um die Datei erfolgreich ins Gerät zuladen, geben Sie auf der WBM-Seite "Passwörter (Seite 185)" das für die Datei festgelegte Passwort ein. Maximale Dateigröße: 8192 Bit	X	X
LogFile	Datei mit Einträgen aus der Ereignisprotokolltabelle	X	--
MIB	Private MSPS MIB-Datei "Scalance_w_msps.mib"	X	--

Dateityp	Beschreibung	Speichern	Laden
RunningCLI	Textdatei mit CLI-Befehlen Diese Datei enthält eine Übersicht der aktuellen Konfiguration in Form von CLI-Befehlen. Passwörter sind in dieser Datei wie folgt maskiert: [PASSWORD] Sie können die Textdatei herunterladen. Die Datei ist nicht dafür vorgesehen, dass Sie sie unverändert wieder hochladen.	X	--
Script	Textdatei mit CLI-Befehlen Sie können eine Skriptdatei in einem Gerät hochladen. Die enthaltenen CLI-Befehle werden entsprechend ausgeführt. CLI-Befehle zum Speichern und Laden von Dateien können nicht über die CLI-Skriptdatei ausgeführt werden.	--	X
SSHPrivate-KeyECDSA	SSH Privater Schlüssel (ECDSA) Unterstützt wird der SSH-Schlüssel ecdsa-sha2-nistp521. Es gibt Dateien, deren Zugriff passwortgeschützt ist. Um die Datei erfolgreich ins Gerät zuladen, geben Sie auf der WBM-Seite "Passwörter (Seite 185)" das für die Datei festgelegte Passwort ein.	X	--
SSHPrivateKeyRSA	SSH Privater Schlüssel (RSA) mit und ohne Passwort Unterstützt werden die folgenden SSH-Schlüssel: • rsa-sha2-512 • rsa-sha2-256 Es gibt Dateien, deren Zugriff passwortgeschützt ist. Um die Datei erfolgreich ins Gerät zuladen, geben Sie auf der WBM-Seite "Passwörter (Seite 185)" das für die Datei festgelegte Passwort ein.	X	--
StartupInfo	Startup Logdatei Diese Datei enthält die Meldungen, die während des letzten Hochlaufs in der Logdatei eingetragen wurden.	X	--
Users	Datei mit Benutzernamen und Passwörter	X	X
WBMFav	WBM Favoriten Diese Datei enthält die Favoriten, die Sie im WBM angelegt haben. Sie können diese Datei herunterladen und in anderen Geräten hochladen.	X	X
WLANAuthlog	Datei mit Einträgen aus dem WLAN Authentication Log (Informationen zu erfolgreichen oder fehlgeschlagenen Authentifizierungsversuchen)	X	--
WLANCert (Nur im Client-Modus)	Benutzerzertifikat. Für das Benutzerzertifikat können Sie auf der WBM-Seite "Load&Save > Password" ein Passwort festlegen. Maximale Dateigröße: 8192 Bit	X	X
WLANServerCert (Nur im Client-Modus)	Server-Zertifikat Maximale Dateigröße: 8192 Bit	X	X
WLANSigRec (Nur im Client-Modus)	Die Zip-Datei enthält Folgendes: • csv-Datei mit den Messwerten des Signalrekorders • pdf-Datei mit den Messwerten und einer zusätzlichen grafischen Darstellung der Messwerte. Die Informationen zu den Messwerten und deren grafische Darstellung finden Sie im Kapitel "Signalrekorder (Seite 269)".	X	--

6.5.7.2 HTTP



Laden und Speichern von Daten über HTTP

Das WBM bietet die Möglichkeit, Gerätedaten in einer externen Datei auf Ihrem Client-PC zu speichern bzw. solche Daten aus einer externen Datei vom PC in die Geräte zu laden. So können Sie z. B. eine neue Firmware aus einer Datei von Ihrem Client-PC laden.

Hinweis

Diese WBM-Seite ist sowohl für Verbindungen über HTTP als auch für Verbindungen über HTTPS verfügbar.

Firmware

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

Konfigurationsdateien

Hinweis

Konfigurationsdateien und Trial-Modus/Automatic Save-Modus

Im Automatic Save-Mode 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 "Schreiben der Startkonfiguration" auf der WBM-Seite "System > Konfiguration", um Änderungen in den Konfigurationsdateien abzuspeichern

CLI-Skriptdatei

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

Hinweis

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

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

Austausch von Konfigurationsdaten mit STEP7 Basic/Professional über eine Datei

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

Voraussetzungen:

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

Die Dateitypen können wie folgt genutzt werden:

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

Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Dateityp**
  Zeigt die Bezeichnung der Datei an.

  Hinweis

  Größe von Zertifikatsdateien

  Bei Zertifikatsdateien werden nur Zertifikate mit maximal 8192 Bits unterstützt.

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

  Hinweis

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

Vorgehensweise

Daten über HTTP laden

1. Starten Sie das Laden durch Anklicken einer der Schaltflächen "Hochladen".
   Es öffnet sich das Dialogfenster zum Laden einer Datei.
2. Navigieren Sie zu der gewünschten Datei, die geladen werden soll.
3. Klicken Sie im Dialogfenster auf die Schaltfläche "Öffnen".
   Die Datei wird nun geladen.

Ob ein Neustart notwendig ist, ist abhängig von der geladenen Datei. Wenn ein Neustart notwendig ist, wird eine entsprechende Meldung ausgegeben. Andere Dateien werden sofort ausgeführt, z. B. die CLI-Skriptdatei, und neue Einstellungen werden ohne Neustart übernommen.

Daten über HTTP speichern

1. Starten Sie das Speichern durch Anklicken einer der Schaltflächen "Speichern". Abhängig von der Größe der Datei kann dies einige Zeit in Anspruch nehmen.
2. Abhängig von Ihrer Browserkonfiguration werden Sie 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 "Speichern".

Daten über HTTP löschen

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

Konfigurationsdaten wiederverwenden

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

Gehen Sie folgendermaßen vor, um Konfigurationsdaten wiederzuverwenden:

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

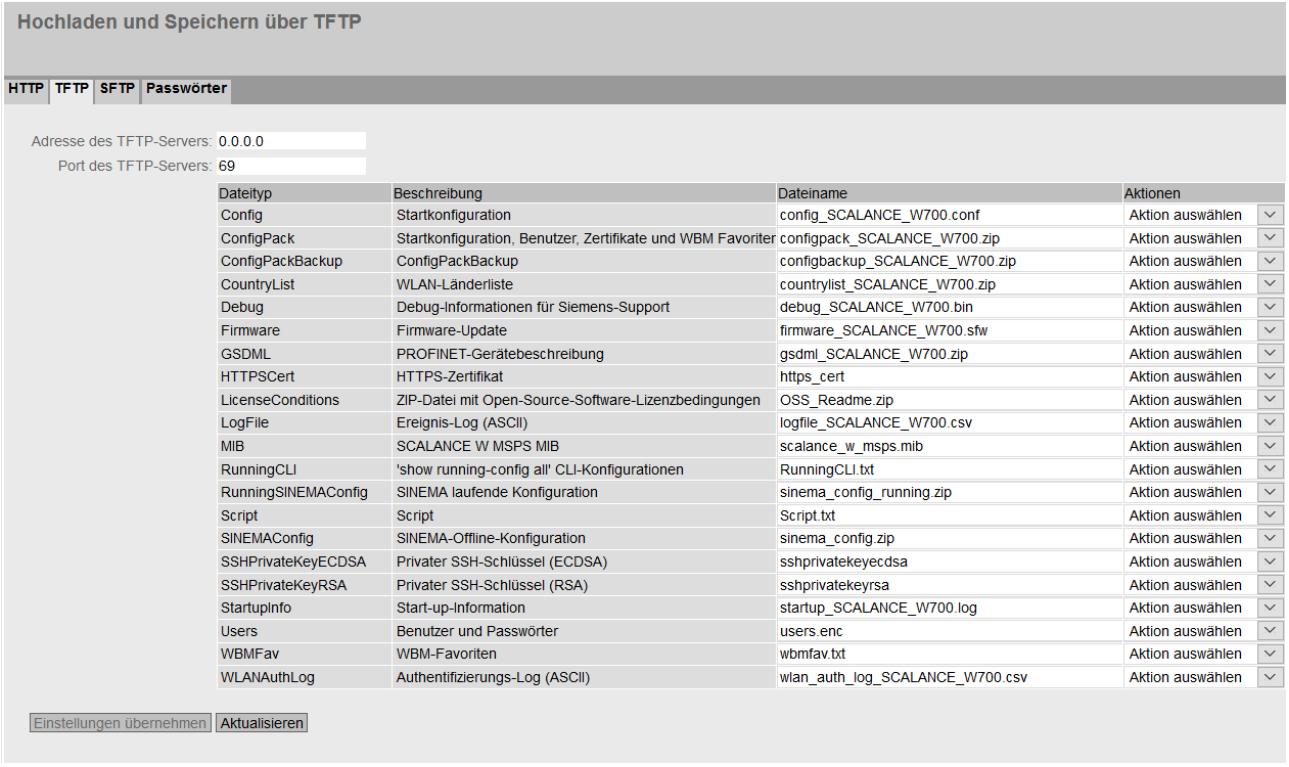
Hinweis

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

Passwortgeschützte Config-Datei

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

6.5.7.3 TFTP



Laden und Speichern von Daten über einen TFTP-Server

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

Firmware

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

Konfigurationsdateien

Hinweis

Konfigurationsdateien und Trial-Modus/Automatic Save-Modus

Im Automatic Save-Mode 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 "Schreiben der Startkonfiguration" auf der WBM-Seite "System > Konfiguration", um Änderungen in den Konfigurationsdateien abzuspeichern.

CLI-Skriptdatei

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

Hinweis

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

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

Austausch von Konfigurationsdaten mit STEP7 Basic/Professional über eine Datei

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

Voraussetzungen:

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

Die Dateitypen können wie folgt genutzt werden:

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

Beschreibung

Die Seite enthält folgende Felder:

- **Adresse des TFTP-Servers**
  Tragen Sie hier die IP-Adresse oder den FQDN (Fully Qualified Domain Name) des TFTP-Servers ein, mit dem Sie Daten austauschen.
- **Port des TFTP-Servers**
  Tragen Sie hier den Port des TFTP-Servers ein, über den der Datenaustausch abgewickelt werden soll. Gegebenenfalls können Sie den Standardwert 69 entsprechend Ihren spezifischen Anforderungen ändern.

Die Tabelle gliedert sich in folgende Spalten:

- **Dateityp**
  Zeigt die Bezeichnung der Datei an.

  Hinweis

  Größe von Zertifikatsdateien

  Bei Zertifikatsdateien werden nur Zertifikate mit maximal 8192 Bits unterstützt.

- **Beschreibung**
  Zeigt die Kurzbeschreibung des Dateityps an.
- **Dateiname**
  Tragen Sie einen Dateinamen ein.
- **Aktionen**
  Wählen Sie aus der Klappliste die Aktion aus. Die Auswahl ist abhängig vom gewählten Dateityp. z. B. die Log-Datei lässt sich nur speichern.
  Folgende Aktionen sind möglich:
  - **Datei speichern**
    Mit dieser Auswahl speichern Sie eine Datei auf den TFTP-Server.
  - **Datei hochladen**
    Mit dieser Auswahl laden Sie eine Datei vom TFTP-Server.

Vorgehensweise

Daten über TFTP laden bzw. speichern

1. Tragen Sie im Eingabefeld "Adresse des TFTP-Servers" die IP-Adresse oder den FQDN des TFTP-Servers ein.
2. Tragen Sie im Eingabefeld "Port des TFTP-Servers" den verwendeten Port des Servers ein.
3. Tragen Sie im Eingabefeld "Dateiname" den Namen einer Datei ein, in die Sie speichern bzw. aus der Sie Daten übernehmen wollen.
4. Wählen Sie aus der Klappliste "Aktionen" die Aktion, die Sie durchführen wollen.
5. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen", um die ausgewählten Aktionen zu starten. Abhängig von der Größe der Datei kann dies einige Zeit in Anspruch nehmen.
6. Starten Sie nach dem Laden der Konfiguration und des SSL-Zertifikats das Gerät neu. Erst nach einem Neustart werden die Änderungen aktiv.

Konfigurationsdaten wiederverwenden

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

Gehen Sie folgendermaßen vor, um Konfigurationsdaten wiederzuverwenden:

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

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

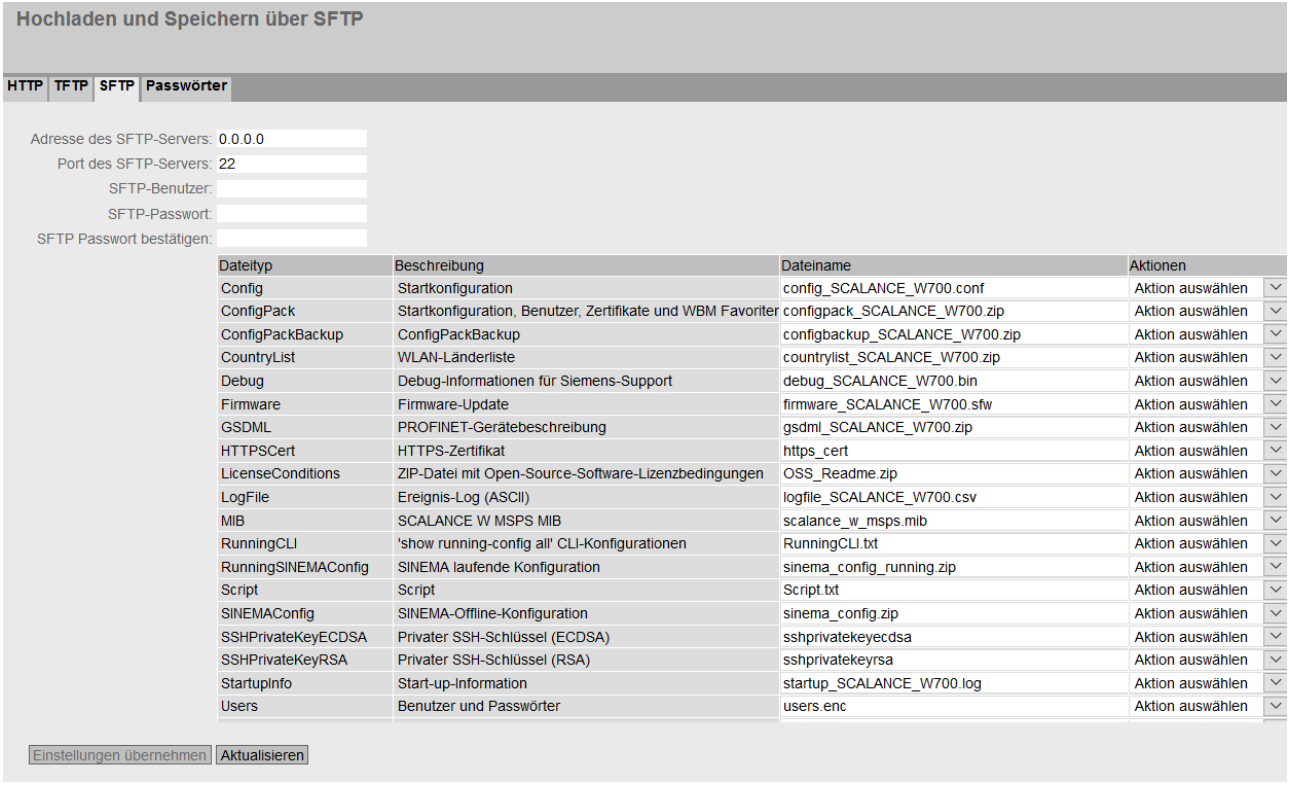
Hinweis

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

Passwortgeschützte Config-Datei

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

6.5.7.4 SFTP



Laden und Speichern von Daten über einen SFTP-Server

SFTP (SSH File Transfer Protocol) überträgt die Dateien verschlüsselt. Auf dieser Seite konfigurieren Sie die Zugangsdaten für den SFTP-Server.

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

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

Firmware

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

Konfigurationsdateien

Hinweis

Konfigurationsdateien und Modus Trial/Automatisches Speichern

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

CLI-Skriptdatei

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

Hinweis

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

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

Austausch von Konfigurationsdaten mit STEP7 Basic/Professional über eine Datei

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

Voraussetzungen:

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

Die Dateitypen können wie folgt genutzt werden:

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

Beschreibung

Die Seite enthält folgende Felder:

- **Adresse des SFTP-Servers**
  Geben Sie die IP-Adresse oder den FQDN des SFTP-Servers ein, mit dem Sie Daten austauschen.
- **Port des SFTP-Servers**
  Geben Sie den Port des SFTP-Servers ein, über den der Datenaustausch abgewickelt werden soll. Gegebenenfalls können Sie den Standardwert 22 entsprechend Ihren spezifischen Anforderungen ändern.
- **SFTP Benutzer**
  Geben Sie den Benutzer für den Zugriff auf den SFTP-Server ein. Vorausgesetzt, auf dem SFTP-Server ist ein Benutzer mit den entsprechenden Rechten angelegt.
  Der Name muss folgende Bedingungen erfüllen:
  - Er muss eindeutig sein.
  - Er muss zwischen 1 und 250 Zeichen lang sein.
  - Er darf folgende Zeichen nicht enthalten: § ? " ; :
    Die Zeichen für Space und Delete dürfen auch nicht enthalten sein.
- **SFTP Passwort**
  Geben Sie das Passwort für den Benutzer ein
- **SFTP Passwort bestätigen**
  Bestätigen Sie das Passwort.

Die Tabelle gliedert sich in folgende Spalten:

- **Dateityp**
  Zeigt den Dateityp an.
- **Beschreibung**
  Zeigt die Kurzbeschreibung des Dateityps an.

- **Dateiname**
  Für jeden Dateityp ist hier ein Dateiname vorgegeben.

  Hinweis

  Änderung des Dateinamens

  Sie können den in dieser Spalte vorgegebenen Dateinamen ändern. Nach dem Anklicken der Schaltfläche "Einstellungen übernehmen" ist der geänderte Name im Gerät gespeichert und kann auch mit dem Command Line Interface genutzt werden.

- **Aktionen**
  Wählen Sie aus der Klappliste die Aktion aus. Die Auswahl ist abhängig vom gewählten Dateityp. z. B. können Sie die Log-Datei nur speichern.
  Folgende Aktionen sind möglich:
  - **Datei speichern**
    Mit dieser Auswahl speichern Sie eine Datei auf dem SFTP-Server.
  - **Datei hochladen**
    Mit dieser Auswahl laden Sie eine Datei vom SFTP-Server.

Vorgehensweise

Daten über SFTP laden bzw. speichern

1. Geben Sie bei "Adresse des SFTP-Servers" die Adresse des SFTP-Servers ein.
2. Geben Sie bei "Port des SFTP-Servers" den verwendeten Port des SFTP-Servers ein.
3. Geben Sie die Benutzerdaten (Benutzername und Passwort) ein, die für den Zugriff auf den SFTP-Server notwendig sind.
4. Geben Sie ggf. bei "Dateiname" den Namen einer Datei ein, in die Sie speichern bzw. aus der Sie Daten übernehmen wollen.

   Hinweis

   Dateien, deren Zugriff passwortgeschützt ist

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

5. Wählen Sie in der Klappliste "Aktionen" die Aktion aus, die Sie durchführen wollen.
6. Klicken Sie auf "Einstellungen übernehmen", um die ausgewählte Aktion zu starten.
7. Wenn ein Neustart notwendig ist, wird eine entsprechende Meldung ausgegeben. Klicken Sie auf die Schaltfläche "OK", um den Neustart durchzuführen. Wenn Sie auf die Schalfläche "Abbrechen" klicken, wird kein Neustart des Geräts durchgeführt. Erst nach einem Neustart werden die Änderungen wirksam.

Konfigurationsdaten wiederverwenden

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

Gehen Sie folgendermaßen vor, um Konfigurationsdaten wiederzuverwenden:

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

Hinweis

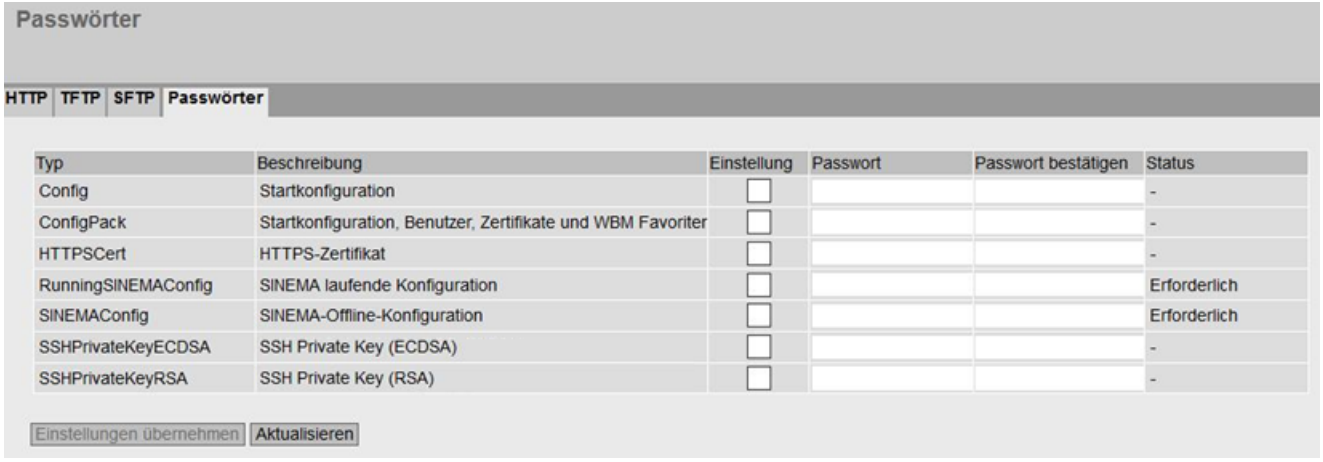
Konfigurationsdaten sind mit einer Prüfsumme versehen. Wenn Sie die Dateien bearbeiten, können Sie die Dateien nicht mehr auf das Gerät hochladen.

Passwortgeschützte Config-Datei

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

6.5.7.5 Passwörter

Es gibt Dateien, deren Zugriff passwortgeschützt ist. Um z. B. das HTTPS-Zertifikat verwenden zu können, müssen Sie auf dieser WBM-Seite das entsprechende Passwort angeben.



Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Typ**
  Zeigt den Dateityp an.
- **Beschreibung**
  Zeigt die Kurzbeschreibung des Dateityps an.
- **Einstellung**
- Wenn aktiviert, wird die Datei verwendet. Nur aktivierbar, wenn das Passwort konfiguriert ist.

- **Passwort**
  Geben Sie das Passwort für die Datei ein.
- **Passwort bestätigen**
  Bestätigen Sie das Passwort.
- **Status**
  Zeigt an, ob das Passwort zu der Datei auf dem Gerät passt.
  - gültig
    Das Optionskästchen "Aktiviert" ist aktiviert und das Passwort passt zu der Datei.
  - ungültig
    Das Optionskästchen "Aktiviert" ist aktiviert, aber das Passwort passt nicht zur Datei oder es ist noch keine Datei geladen.
  - '-'
    Das Passwort kann nicht ausgewertet werden oder wird noch nicht verwendet. Das Optionskästchen "Aktiviert" ist nicht aktiviert.
  - Erforderlich
    Zum Laden oder Speichern ist ein Passwort erforderlich

Vorgehensweise

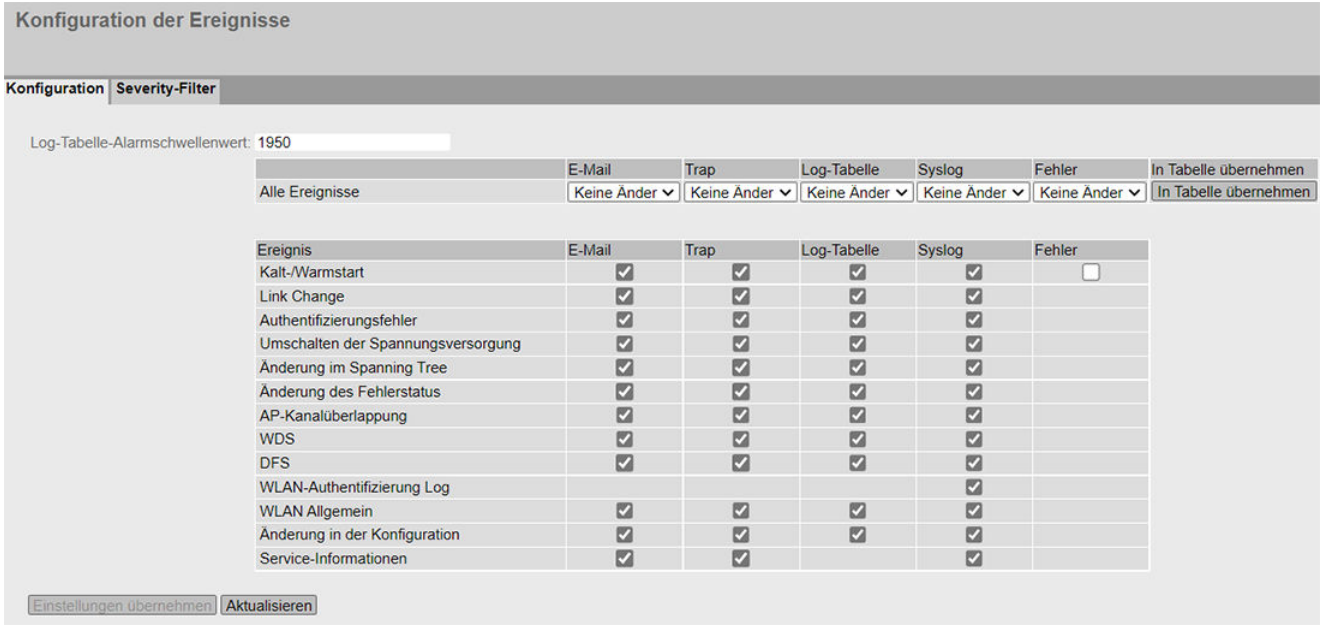
1. Tragen Sie bei "Passwort" das Passwort ein.
2. Um das Passwort zu bestätigen, tragen Sie bei "Passwort bestätigen" das Passwort nochmals ein.
3. Aktivieren Sie die Option "Aktiviert".
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.5.8 Ereignisse

6.5.8.1 Konfiguration

Systemereignisse auswählen

Auf dieser Seite legen Sie fest, wie ein Gerät auf Systemereignisse reagiert. Klicken Sie zum Aktivieren oder Deaktivieren der Optionen in die entsprechenden Optionskästchen der jeweiligen Spalte.



Beschreibung

Log-Tabelle-Alarmschwellenwert

Legen Sie den Grenzwert für die Einträge pro Severity fest. Wenn der Wert erreicht ist, wird eine Meldung ausgegeben. Pro Severity sind maximal 2000 Einträge möglich.

Mit Tabelle 1 können Sie alle Optionskästchen einer Spalte von Tabelle 2 auf einmal aktivieren oder deaktivieren. Die Tabelle 1 gliedert sich in folgende Spalten:

- **Alle Ereignisse**
  Zeigt an, dass die Einstellungen für alle Ereignisse der Tabelle 2 gültig sind.
- **E-Mail / Trap / Log-Tabelle / Syslog / Fehler**
  Aktivieren oder deaktivieren Sie die gewünschte Art der Benachrichtigung für alle Ereignisse. Wenn "Keine Änderung" ausgewählt ist, bleiben die Einträge der entsprechenden Spalte in der Tabelle 2 unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ereignisse der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Ereignis**
  Die Spalte enthält folgende Werte:
  - Kalt-/Warmstart
    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 > Fehlerkontrolle > Link Change".
  - Authentifizierungsfehler
    Dieses Ereignis tritt beim Versuch eines Zugriffs mit fehlerhaftem Kennwort auf.
  - Umschaltung der Spannungsversorgung
    Dieses Ereignis tritt auf, wenn die Spannungsversorgungsleitungen 1 und 2 überwacht werden. Es zeigt an, dass ein Wechsel auf Leitung 1 bzw. auf Leitung 2 stattgefunden hat. Das Ereignis tritt auch auf, wenn die PoE-Spannungsversorgung ausgefallen ist, siehe "System > Fehlerkontrolle > Spannungsversorgung".
  - Änderung im Spanning Tree
    Die STP- bzw. RSTP- oder MSTP-Topologie hat sich geändert.
  - Änderung des Fehlerstatus
    Der Fehlerstatus hat sich geändert. Der Fehlerstatus kann sich auf die aktivierte Portüberwachung, auf das Ansprechen der Meldekontakte oder die Spannungsüberwachung beziehen.
  - AP-Kanalüberlappung (Nur im Access Point-Modus)
    Bei einem Eintrag in die Liste "Überlappung AP" wird dieses Ereignis ausgelöst.
  - DFS (Nur im Access Point-Modus)
    Dieses Ereignis tritt ein, wenn ein Radarsignal empfangen worden ist oder der DFS-Scan gestartet bzw. gestoppt wurde.
  - WLAN-Authentifizierung Log
    Weiterleitung der Einträge aus WLAN Authentication Log an den Systemprotokoll-Server.
  - WLAN De-/Authentifizierung (Nur im Client-Modus)
    Bei erfolgten oder fehlgeschlagenen WLAN-Authentifizierungsversuchen.
  - WLAN Allgemein (Nur im Access Point-Modus)
    Dieses Ereignis tritt ein, wenn sich die Kanalbandbreite geändert hat.
  - Änderung in der Konfiguration
    Dieses Ereignis tritt ein, wenn sich die Konfiguration des Geräts geändert hat.
  - Service-Informationen
    Einige aufgetretenen Systemereignisse werden ohne Konfiguration in die Ereignisprotokoll-Tabelle eingetragen. Für diese Ereignisse können Sie weitere Arten der Benachrichtigung konfigurieren.

- **Art der Benachrichtigung**
  - E-Mail
    Das Gerät sendet eine E-Mail. Voraussetzung ist, dass der SMTP-Server eingerichtet und die Funktion "SMTP-Client" aktiviert ist.
  - Trap
    Das Gerät löst einen SNMP-Trap aus. Voraussetzung ist, dass unter "System > Konfiguration" "SNMPv1 Traps" aktiviert ist.
  - Log-Tabelle
    Das Gerät schreibt einen Eintrag in die Ereignisprotokoll-Tabelle. Den Inhalt der Ereignisprotokoll-Tabelle wird unter "Information > Log-Tabellen > Ereignis-Log " angezeigt
  - Syslog
    Das Gerät schreibt einen Eintrag auf den Systemprotokoll-Server. Voraussetzung ist, dass der Systemprotokoll-Server eingerichtet und die Funktion "Syslog-Client" aktiviert ist.
  - Fehler
    Das Gerät löst einen Fehler aus. Die Fehler-LED leuchtet auf und der aktuell anstehende Fehler wird unter "Information > Fehler" angezeigt.

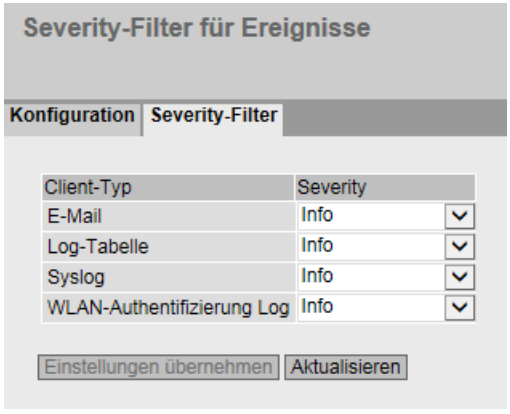
Vorgehensweise

Gehen Sie folgendermaßen vor, um Einträge zu ändern:

1. Aktivieren Sie das Optionskästchen in der Zeile des gewünschten Ereignisses. Wählen Sie dabei das Ereignis in der Spalte unter den folgenden Aktionen aus:
   - E-Mail
   - Trap
   - Log-Tabelle
   - Syslog
   - Fehler
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.5.8.2 Severity-Filter

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



Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Client-Typ**
  Wählen Sie den Client-Typ, für den Sie die Einstellungen vornehmen:
  - **E-Mail**
    Versand von Systemereignismeldungen per E-Mail
  - **Log-Tabelle**
    Eintragen von Systemereignissen in die Log-Tabelle
  - **Syslog**
    Eintragen von Systemereignissen in die Syslog-Datei
  - **WLAN-Authentifizierung Log**
    Eintragen von Systemereignissen in das WLAN Authentication Log
- **Severity**
  Wählen Sie die gewünschte Stufe aus. Folgende Einstellungen sind möglich:
  - **Critical**
    Systemereignisse werden ab dem Severity-Level Critical bearbeitet.
  - **Warning**
    Systemereignisse werden ab dem Severity-Level Warning bearbeitet.
  - **Info**
    Systemereignisse werden ab dem Severity-Level Info bearbeitet.

Vorgehensweise

Gehen Sie folgendermaßen vor, um die gewünschte Stufe zu konfigurieren:

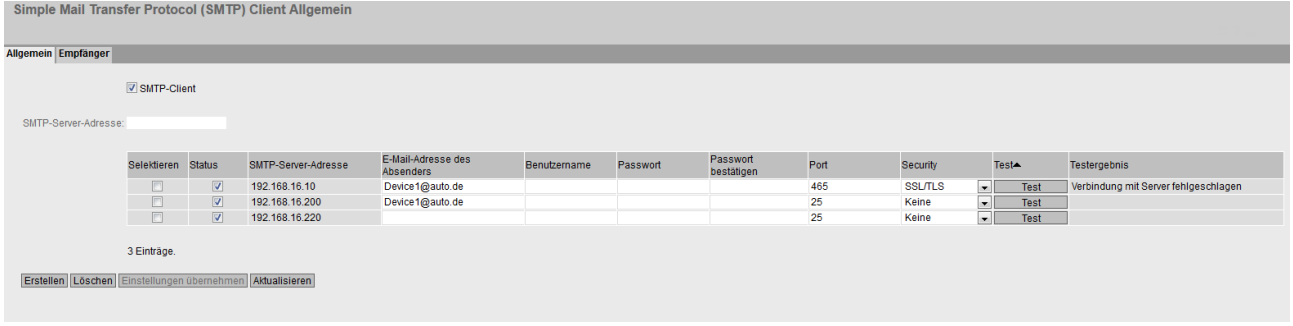
1. Wählen Sie aus den Klapplisten in der zweiten Tabellenspalte hinter den Client-Typen die gewünschten Werte aus.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.5.9 SMTP-Client

6.5.9.1 Allgemein

Netzüberwachung durch E-Mails

Beim Auftreten von Ereignissen kann das Gerät automatisch eine E-Mail versenden, z. B. an den Servicetechniker. Die E-Mail enthält die Identifikation des absendenden Geräts, eine Beschreibung der Ursache in Klartext sowie einen Zeitstempel. Damit kann für Netze mit wenigen Teilnehmern eine einfache zentrale Netzüberwachung auf Basis eines E-Mail-Systems aufgebaut werden.



Voraussetzung für das Senden der E-Mails

- Unter "System > Ereignisse > Konfiguration" ist beim entsprechenden Ereignis "E-Mail" aktiviert.
- Unter "System > Ereignisse > Severity-Level" ist die gewünschte Severity konfiguriert.
- Unter "System > SMTP-Client > Empfänger" ist mindestens ein Eintrag vorhanden und die Einstellung "Senden" ist aktiviert.

Beschreibung

Die Seite enthält folgende Felder:

- **SMTP-Client**
  Aktivieren oder deaktivieren Sie den SMTP-Client.
- **SMTP-Server-Adresse**
  Geben Sie die IP-Adresse des SMTP-Servers ein.

Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in einer zu löschenden Zeile das Optionskästchen.
- **Status**
  Legen Sie fest, ob dieser SMTP-Server verwendet wird.
- **SMTP-Server-Adresse**
  Zeigt die IP-Adresse des SMTP-Servers.
- **E-Mail-Adresse des Absenders**
  Geben Sie die E-Mail-Adresse des Absenders ein, der in der E-Mail angegeben wird.
- **Benutzername**
  Wenn erforderlich, geben Sie den Benutzernamen ein, der zur Authentifizierung am SMTP-Server verwendet wird.
- **Passwort**
  Wenn erforderlich, geben Sie das Passwort ein, das zur Authentifizierung am SMTP-Server verwendet wird.
- **Passwort bestätigen**
  Wiederholen Sie das Passwort.
- **Port**
  Geben Sie den Port ein, über den der SMTP-Server erreichbar ist.
  Werkseinstellung:
  - 25 (None)
  - 465 (SSL/TLS und StartTLS)
- **Security**
  Legen Sie fest, ob die Übertragung der E-Mail vom Gerät zum SMTP-Server verschlüsselt wird. D. h. Voraussetzung ist, dass der SMTP-Server die ausgewählte Einstellung unterstützt.

  Hinweis

  2-Faktor-Authentifizierung (2FA)

  Die 2-Faktor-Authentifizierung wird nicht unterstützt.

  - SSL/TLS
  - StartTLS
  - None: Die Übertragung der E-Mail ist unverschlüsselt.

- **Test**
  Verschickt an die konfigurierten Empfänger eine Test-E-Mail.
- **Testergebnis**
  Zeigt an, ob die E-Mail erfolgreich gesendet wurde oder nicht. Wenn das Senden nicht erfolgreich war, enthält die Meldung mögliche Ursachen.

Vorgehensweise

SMTP-Server konfigurieren

1. Aktivieren Sie die Funktion "SMTP-Client".
2. Geben Sie in "SMTP-Server-Adresse" die IP-Adresse des SMTP-Servers ein.
3. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag erzeugt.
4. Geben Sie bei "E-Mail-Adresse des Absenders" den Absendernamen ein, der in der E-Mail angegeben wird.
5. Wenn der SMTP-Server eine Anmeldung erfordert, geben Sie Benutzernamen und Passwort ein.
6. Legen Sie bei "Security" fest, ob die Übertragung zum SMTP-Server verschlüsselt wird.
7. Aktivieren Sie den SMTP-Servereintrag.
8. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Hinweis

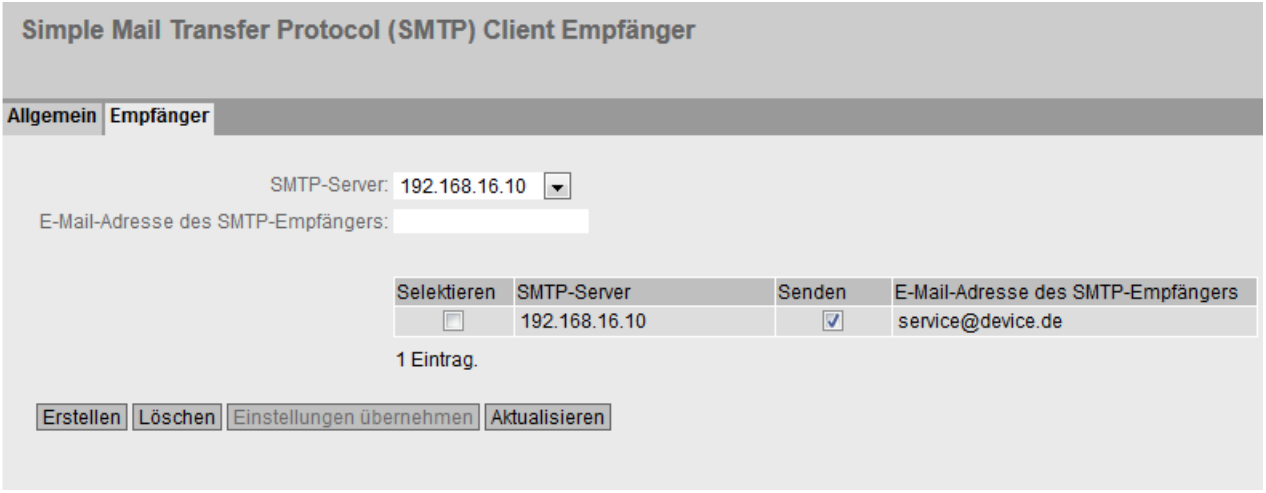
Je nach Eigenschaften und Konfiguration des SMTP-Servers kann es notwendig sein, die Eingabe von "E-Mail-Adresse des Absenders" anzupassen. Informieren Sie sich beim Administrator des SMTP-Servers.

Konfiguration des SMTP-Servers testen

1. Empfänger konfigurieren
   - Klicken Sie auf das Register "Empfänger".
   - Wählen Sie bei "SMTP-Server" den gewünschten SMTP-Server aus.
   - Geben Sie bei "E-Mail-Adresse des SMTP-Empfängers" die gewünschte Adresse an.
   - Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag erzeugt. Standardmäßig ist die Einstellung "Senden" aktiviert.
2. Test-E-Mail versenden
   - Klicken Sie auf das Register "Allgemein".
   - Klicken Sie bei dem SMTP-Servereintrag auf die Schaltfläche "Test". Das Gerät sendet jedem konfigurierten Empfänger eine Test-E-Mail.
   - Prüfen Sie das Testergebnis. Wenn das Senden nicht erfolgreich war, enthält die Meldung mögliche Ursachen.

6.5.9.2 Empfänger

Auf dieser Seite legen Sie fest, wer beim Auftreten eines Ereignisses eine E-Mail bekommt.



Beschreibung

Die Seite enthält folgende Felder:

- **SMTP-Server**
  Legen Sie fest, über welchen SMTP-Server die E-Mail versendet wird.
- **E-Mail-Adresse des SMTP-Empfängers**
  Geben Sie die E-Mail-Adresse ein, an die das Gerät eine E-Mail sendet.

Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in einer zu löschenden Zeile das Optionskästchen.
- **SMTP-Server**
  Zeigt die IP-Adresse des SMTP-Servers an, auf den sich der Eintrag bezieht.
- **Senden**
  Wenn aktiviert, sendet das Gerät an diesen Empfänger eine E-Mail.
- **E-Mail-Adresse des SMTP-Empfängers**
  Zeigt die E-Mail-Adresse an, an die das Gerät im Fehlerfall eine E-Mail sendet.

Vorgehensweise

SMTP-Empfänger konfigurieren

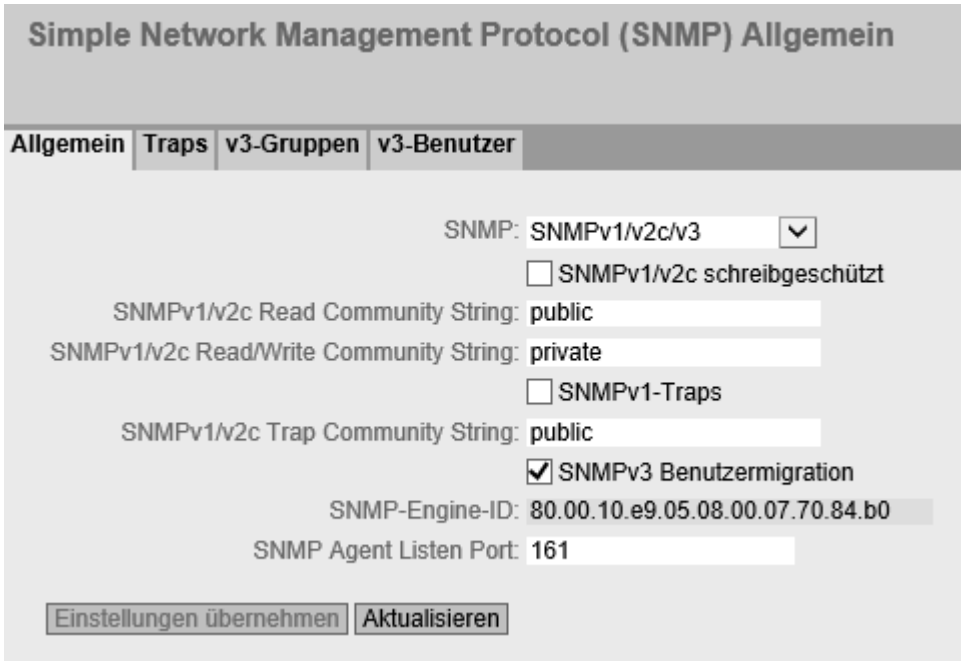
1. Wählen Sie den gewünschten "SMTP-Server".
2. Geben Sie die E-Mail-Adresse des SMTP-Empfängers ein.
3. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag erzeugt.
4. Aktivieren Sie für den Eintrag die Option "Senden".
5. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.5.10 DHCPv4

6.5.10.1 System_SNMP_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:

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

    Hinweis

    Beachten Sie, dass SNMP in den Versionen 1 und 2c über keine Sicherheitsmechanismen verfügt.
  - SNMPv3
    Nur SNMPv3 wird unterstützt.
- **SNMPv1/v2c schreibgeschützt**
  Wenn Sie diese Option aktivieren, kann SNMPv1/v2c nur lesend auf die SNMP-Variablen zugreifen.

  Hinweis

  Community String

  Verwenden Sie aus Sicherheitsgründen nicht die Standardwerte "public" oder "private". Ändern Sie die Community Strings nach der Erst-Installation.

  Die empfohlene Mindestlänge für Community Strings sind 6 Zeichen.

  Aus Sicherheitsgründen ist mit dem SNMPv1/v2c Read Community String nur eingeschränkter Zugriff auf Objekte der SNMPCommunityMIB möglich. Mit dem SNMPv1/v2c Read/Write Community String haben Sie vollen Zugriff auf die SNMPCommunityMIB.
- **SNMPv1/v2c Read Community String**
  Tragen Sie den Community String für den lesenden Zugriff des SNMP-Protokolls ein.
- **SNMPv1/v2c Read/Write Community String**
  Tragen Sie den Community String für den lesenden und schreibenden Zugriff des SNMP-Protokolls ein.
- **SNMPv1-Traps**
  Aktivieren oder deaktivieren Sie das Senden von SNMPv1-Traps (Alarmtelegramme). Im Register "Trap" legen Sie die IP-Adressen der Geräte fest, an die SNMPv1-Traps gesendet werden.
- **SNMPv1/v2c Trap Community String**
  Tragen Sie den Community String für das Senden von SNMPv1/v2c-Meldungen ein.

- **SNMPv3 Benutzermigration**
  - Aktiviert
    Wenn die Funktion aktiviert ist, wird eine SNMP-Engine-ID generiert, die migriert werden kann. Sie können konfigurierte SNMPv3-Benutzer auf ein anderes Gerät übertragen. Wenn Sie diese Funktion aktivieren und die Konfiguration des Geräts auf ein anderes Gerät laden, bleiben konfigurierte SNMPv3-Benutzer erhalten.
  - Deaktiviert
    Wenn die Funktion deaktiviert ist, wird eine gerätespezifische SNMP-Engine-ID generiert. Um die ID zu generieren, wird die Agent-MAC-Adresse des Geräts verwendet. Sie können diese SNMP-Benutzerkonfiguration nicht auf andere Geräte übertragen.
    Wenn Sie die Konfiguration des Geräts auf ein anderes Gerät laden, werden alle konfigurierten SNMPv3-Benutzer gelöscht.
- **SNMP-Engine-ID**
  Zeigt die SNMP-Engine-ID an.
- **SNMP Agent Listen Port**
  Legen Sie fest, an welchem Port der SNMP-Agent auf die SNMP-Anfragen wartet.

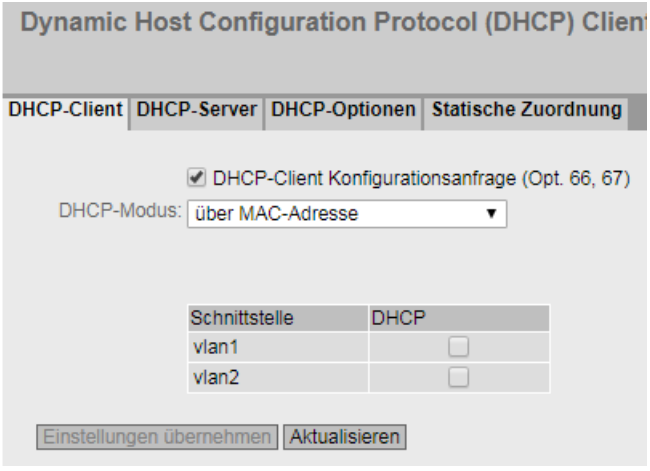
Vorgehensweise

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

6.5.10.2 DHCP-Client

Einstellung des DHCP-Modus

Wenn das Gerät als DHCP-Client konfiguriert ist, startet es eine DHCP-Anfrage. Das Gerät erhält vom DHCP-Server als Antwort eine IPv4-Adresse zugewiesen. Der Server verwaltet einen Adressbereich, aus welchem er IPv4-Adressen vergibt. Es ist auch möglich, den Server so zu konfigurieren, dass der Client auf seine Anfrage immer dieselbe IPv4-Adresse zugewiesen bekommt.



Beschreibung

Die Seite enthält folgende Felder:

- **DHCP-Client Konfigurationsanfrage (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.
- **DHCP-Modus**
  Wählen Sie aus der Klappliste den DHCP-Modus. Folgende Modi sind möglich:
  - über MAC-Adresse
    Die Identifikation läuft über die MAC-Adresse ab.
  - über DHCP-Client-ID
    Die Identifikation läuft über eine frei definierte DHCP-Client-ID ab.
  - über Systemname
    Die Identifikation läuft über den Systemnamen ab. Ist der Systemname 255 Zeichen lang, dann wird das letzte Zeichen nicht zur Identifikation benutzt.
  - über PROFINET-Gerätename
    Die Identifikation läuft über den PROFINET-Gerätenamen ab.

Die Tabelle gliedert sich in folgende Spalten:

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

Vorgehensweise

1. Wählen Sie aus der Klappliste "DHCP-Modus" den gewünschten Modus aus. Wenn Sie den DHCP-Modus "über DHCP-Client-ID" auswählen, erscheint ein Eingabefeld.
   – Geben Sie in das aktivierte Eingabefeld "DHCP-Client-ID" eine Zeichenkette zur Identifikation des Geräts ein. Diese wird dann vom DHCP-Server ausgewertet.
2. Wählen Sie die Option "DHCP-Client Konfigurationsanfrage (Opt. 66, 67)", wenn der DHCP-Client die Optionen 66 und 67 dazu verwenden soll, eine Konfigurationsdatei herunterzuladen und diese dann zu aktivieren.
3. Aktivieren Sie die Option "DHCP" in der Tabelle.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Hinweis

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

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

6.5.10.3 DHCP-Server

Hinweis

Diese Seite ist nur im Access Point-Modus verfügbar.

Das Gerät können Sie als DHCP-Server betreiben. Damit ist es möglich, den angeschlossenen Geräten automatisch IPv4-Adressen zuzuweisen. Die IPv4-Adressen werden entweder dynamisch aus einem von Ihnen vergebenen Adressband (Pool) verteilt oder es wird eine bestimmte IPv4-Adresse (statisch) einem bestimmten Gerät zugewiesen.

Auf dieser Seite legen Sie das IPv4-Adressband fest, aus dem das Gerät eine beliebige IPv4-Adresse erhält.

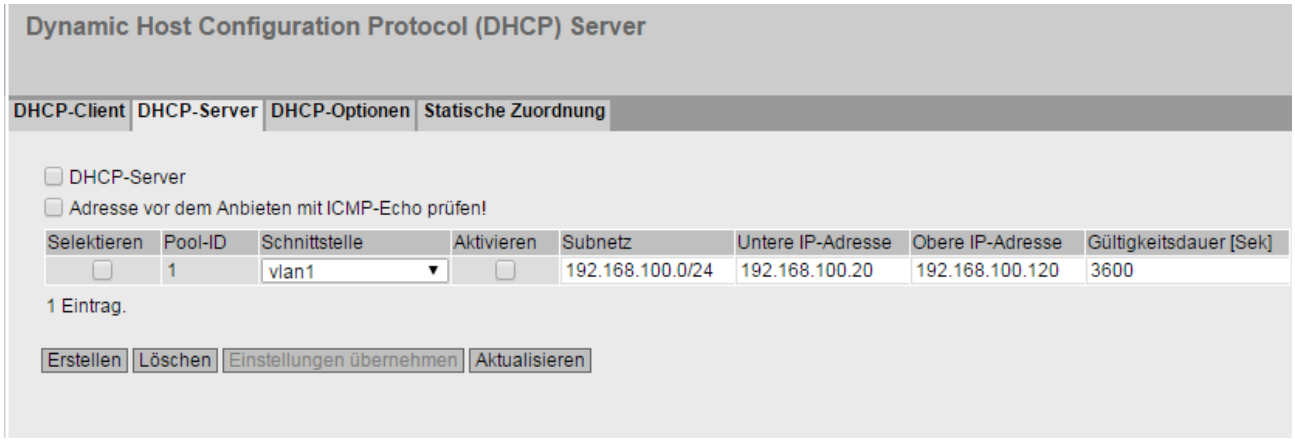
Die statische Zuordnung der IPv4-Adressen konfigurieren Sie unter "Statische Zuordnung".

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 für den DHCP-Server

- Im Access Point-Modus
  - Die angeschlossenen Geräte sind so konfiguriert, dass diese die IPv4-Adresse von einem DHCP-Server beziehen.
- Im Client-Modus
  - Die angeschlossenen Geräte sind so konfiguriert, dass diese die IPv4-Adresse von einem DHCP-Server beziehen.
  - NAT ist aktiviert. NAT aktivieren Sie unter "Layer 3 > NAT".

Beschreibung

Die Seite enthält folgende Felder:

- **DHCP-Server aktivieren**
  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.

  Hinweis

  Access Point

  Die Funktion "DHCP-Server" nur an dem Management zugeordneten VLAN (Agent VLAN ID) möglich.

- **Adresse vor dem Anbieten mit ICMP-Echo prüfen**
  Wenn aktiviert, prüft der DHCP-Server, ob die IP-Adresse schon vergeben ist. Dazu sendet der DHCP-Server ICMP-Echomeldungen (ping) an die IPv4-Adresse. Wenn keine Antwort zurückkommt, kann der DHCP-Server die IPv4-Adresse vergeben.

  Hinweis

  Wenn es in Ihrem Netzwerk Geräte gibt, bei denen der Echo-Dienst standardmäßig deaktiviert ist, kann es zu Konflikten bei den IPv4-Adressen kommen. Um dies zu vermeiden, vergeben Sie diesen Geräten eine IPv4-Adresse, die außerhalb des IPv4-Adressbands liegt.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Pool-ID**
  Zeigt die Nummer des IPv4-Adressbands an. Wenn Sie auf die Schaltfläche "Erstellen" klicken, wird eine neue Zeile mit einer eindeutigen Nummer (Pool-ID) angelegt.

  Hinweis

  Es kann nur eine Pool ID (ID = 1) angelegt werden.

- **Schnittstelle**
  Legen Sie die Schnittstelle fest, über die die IPv4-Adressen dynamisch vergeben werden. Voraussetzung für die Vergabe ist, dass die IPv4-Adresse der Schnittstelle innerhalb des IPv4-Adressbandes liegt. Wenn das nicht der Fall ist, vergibt die Schnittstelle keine IPv4-Adressen.
- **Aktivieren**
  Legen Sie fest, ob dieses IPv4-Adressband verwendet wird.

  Hinweis

  Wenn Sie das IPv4-Adressband aktivieren, werden die Einstellungen in diesem sowie in den weiteren DHCP-Registern ausgegraut und sind nicht mehr editierbar

- **Subnetz**
  Tragen Sie den Netzadressbereich ein, die den Geräten zugewiesen wird. Verwenden Sie die CIDR-Schreibweise.

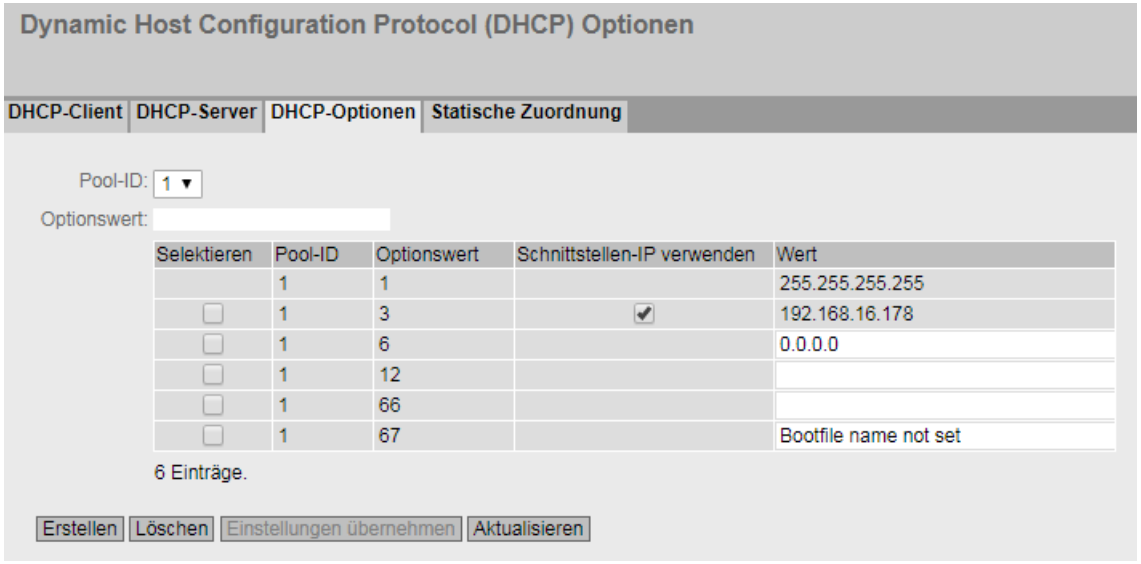
- **Untere IP-Adresse**
  Tragen Sie die IPv4-Adresse ein, die den Anfang des dynamischen IPv4-Adressbands festlegt. Die IPv4-Adresse muss innerhalb des Netzadressbereichs liegen, den Sie bei "Subnetz" konfiguriert haben.
- **Obere IP-Adresse**
  Tragen Sie die IPv4-Adresse ein, die das Ende des dynamischen IPv4-Adressbands festlegt. Die IPv4-Adresse muss innerhalb des Netzadressbereichs liegen, den Sie bei "Subnetz" konfiguriert haben.
- **Gültigkeitsdauer [Sek]**
  Legen Sie fest, für wie viele Sekunden die vergebene IPv4-Adresse gültig bleibt. Nachdem die Gültigkeitsdauer zur Hälfte abgelaufen ist, kann der DHCP-Client die vergebene IPv4-Adresse verlängern. Nach Ablauf der gesamten Zeitdauer muss der DHCP-Client eine neue IPv4-Adresse anfordern.

6.5.10.4 DHCP-Optionen

Hinweis

Diese Seite ist nur im Access Point-Modus verfügbar.

Auf dieser Seite legen Sie fest, welche DHCP-Optionen der DHCP-Server unterstützt. Die verschiedenen DHCP-Optionen sind im RFC 2132 definiert.



Beschreibung

Die Seite enthält folgende Felder:

- **Pool-ID**
  Wählen Sie das gewünschte IPv4-Adressband aus.
- **Optionswert**
  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, 12, 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 Geräts 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:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Pool-ID**
  Zeigt die Nummer des IPv4-Adressbands an.
- **Optionswert**
  Zeigt die Nummer der DHCP-Option an.
- **Schnittstellen-IP verwenden**
  Legen Sie fest, ob die interne IPv4-Adresse des Geräts verwendet wird oder nicht.
- **Wert**
  Geben Sie den DHCP-Parameter ein, der dem DHCP-Client übergeben wird. Der Inhalt ist abhängig von der DHCP-Option.
  - DHCP-Option 67 (Bootfilename)
    Geben Sie den Namen der Bootdatei im String-Format an.
  - DHCP-Optionen 3 (Router) und 6 (DNS):
    Geben Sie den DHCP-Parameter als IPv4-Adresse an, z. B. 192.168.100.2. Bei der DHCP-Option 6 können Sie mehrere IPv4-Adressen durch Komma getrennt angeben.
  - DHCP-Option 12 (Hostnamen):
    Geben Sie den Hostnamen im String-Format an.
  - DHCP-Option 66 (TFTP-Server):
    Geben Sie den TFTP-Server als IPv4-Adresse, z. B. 192.168.100.2, oder den FQDN-Namen an.
  - Alle anderen DHCP-Optionen
    Geben Sie den DHCP-Parameter in Hexadezimal an, z. B. die IPv4-Adresse 192.168.100.2 entspricht "C0A86402".

6.5.10.5 Statische Zuordnung

Hinweis

Diese Seite ist nur im Access Point-Modus verfügbar.

Auf dieser Seite legen Sie fest, dass Geräte mit einer bestimmten MAC-Adresse der vorgegebenen IPv4-Adresse zugeordnet werden.

Beschreibung

Die Seite enthält folgende Felder:

- **Pool-ID**
  Wählen Sie aus der Klappliste das gewünschte IPv4-Adressband aus.
- **Identifikationsmethode des Clients**
  Wählen Sie die Methode, nach der ein Client identifiziert wird.
  - Ethernet MAC
    Der Client wird über seine MAC-Adresse identifiziert.
  - Client-ID
    Der Client wird über eine frei definierte DHCP-Client-ID identifiziert. Die Client-ID kann maximal 254 Zeichen lang sein.
- **Wert**
  Tragen Sie die MAC-Adresse oder die Client-ID ein und klicken Sie auf die Schaltfläche "Erstellen", um den Eintrag anzulegen.

  Hinweis

  Maximal 20 Einträge sind möglich.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Pool-ID**

- Zeigt die Nummer des IPv4-Adressbands an.

  Hinweis

  Nur die Pool ID = 1 wird unterstützt.

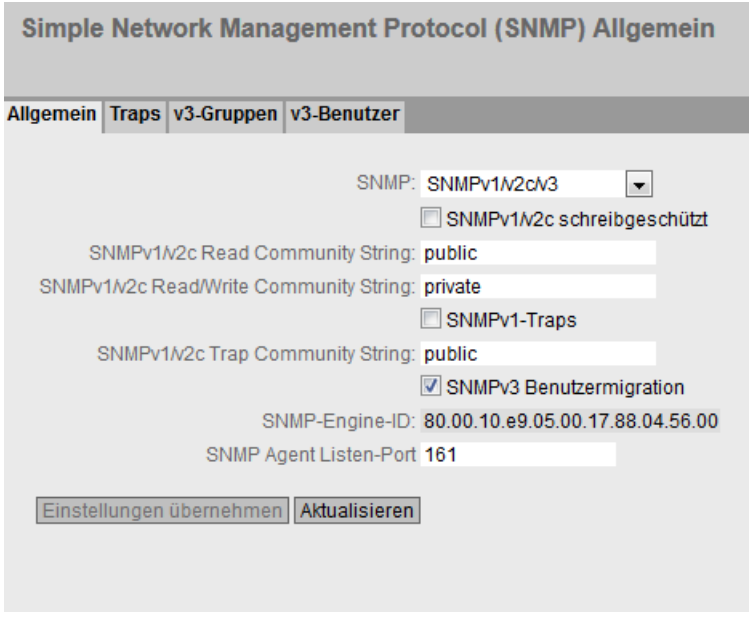
- **Identifikationsmethode**
  Zeigt an, ob der Client über seine MAC-Adresse oder die Client-ID identifiziert wird.
- **Wert**
  Zeigt die MAC-Adresse an, dem die IPv4-Adresse zugeordnet wird.
- **IP-Adresse**
  Legen Sie die IPv4-Adresse fest. Die IPv4-Adresse muss zum Subnetz des IPv4-Adressbands passen.

6.5.11 SNMP

6.5.11.1 Allgemein

Konfiguration von SNMP

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



Beschreibung

Die Seite enthält folgende Felder:

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

    Hinweis

    Beachten Sie, dass SNMP in den Versionen 1 und 2c über keine Sicherheitsmechanismen verfügt.
  - SNMPv3
    Nur SNMPv3 wird unterstützt.
- **SNMPv1/v2c schreibgeschützt**
  Wenn Sie diese Option aktivieren, kann SNMPv1/v2c nur lesend auf die SNMP-Variablen zugreifen.

  Hinweis

  Community String

  Verwenden Sie aus Sicherheitsgründen nicht die Standardwerte "public" oder "private". Ändern Sie die Community Strings nach der Erst-Installation.

  Die empfohlene Mindestlänge für Community Strings sind 6 Zeichen.

  Aus Sicherheitsgründen ist mit dem SNMPv1/v2c Read Community String nur eingeschränkter Zugriff auf Objekte der SNMPCommunityMIB möglich. Mit dem SNMPv1/v2c Read/Write Community String haben Sie vollen Zugriff auf die SNMPCommunityMIB.
- **SNMPv1/v2c Read Community String**
  Geben Sie den Community String für den lesenden Zugriff des SNMP-Protokolls ein.
- **SNMPv1/v2c Read/Write Community String**
  Geben Sie den Community String für den lesenden und schreibenden Zugriff des SNMP-Protokolls ein.
- **SNMPv1-Traps**
  Aktivieren oder deaktivieren Sie das Senden von SNMPv1-Traps (Alarmtelegramme). Im Register "Trap" legen Sie die IP-Adressen der Geräte fest, an die SNMPv1-Traps gesendet werden.
- **SNMPv1/v2c Trap Community String**
  Geben Sie den Community String für das Senden von SNMPv1/v2c-Meldungen ein.

- **SNMPv3 Benutzermigration**
  - **Aktiviert**
    Wenn die Funktion aktiviert ist, wird eine SNMP-Engine-ID generiert, die migriert werden kann. Sie können konfigurierte SNMPv3-Benutzer auf ein anderes Gerät übertragen. Wenn Sie diese Funktion aktivieren und die Konfiguration des Geräts auf ein anderes Gerät laden, bleiben konfigurierte SNMPv3-Benutzer erhalten.
  - **Deaktiviert**
    Wenn die Funktion deaktiviert ist, wird eine gerätespezifische SNMP-Engine-ID generiert. Um die ID zu generieren, wird die Agent-MAC-Adresse des Geräts verwendet. Sie können diese SNMP-Benutzerkonfiguration nicht auf andere Geräte übertragen.
    Wenn Sie die Konfiguration des Geräts auf ein anderes Gerät laden, werden alle konfigurierten SNMPv3-Benutzer gelöscht.
- **SNMP-Engine-ID**
  Zeigt die SNMP-Engine-ID an.
- **SNMP Agent Listen Port**
  Legen Sie fest, an welchem Port der SNMP-Agent auf die SNMP-Anfragen wartet.

Vorgehensweise

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

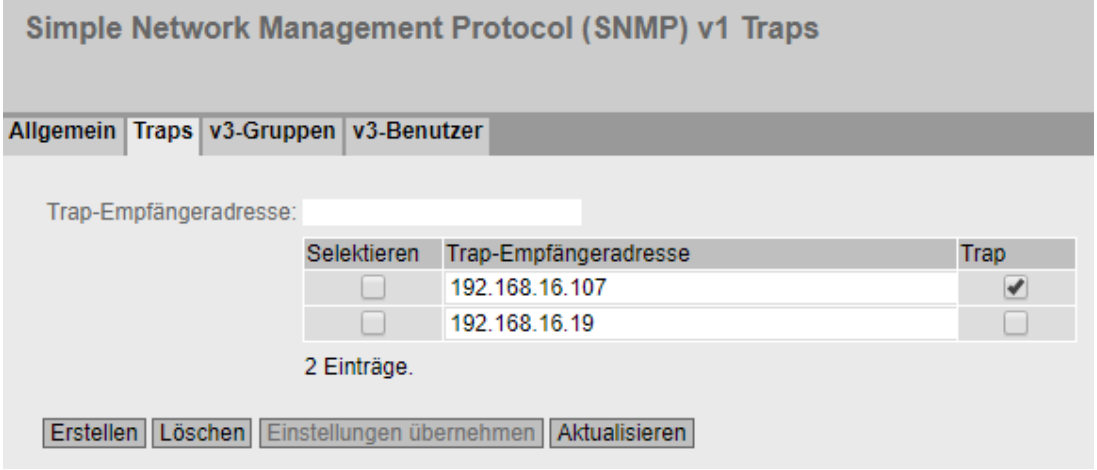
6.5.11.2 Traps

SNMP-Traps bei Alarmereignissen

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

Hinweis

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



Beschreibung

- **Trap-Empfängeradresse**
  Tragen Sie die IP-Adresse oder den FQDN (Fully Qualified Domain Name) der Station ein, an die das Gerät SNMP-Traps sendet. Sie können bis zu zehn verschiedene Empfänger angeben.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Trap-Empfängeradresse**
  Ändern Sie bei Bedarf die IP-Adresse oder den FQDN (Fully Qualified Domain Name) 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 "Trap-Empfängeradresse" die IP-Adresse oder den FQDN der Station ein, an die das Gerät Traps senden soll.
2. Klicken Sie auf die Schaltfläche "Erstellen", um einen neuen Trap-Eintrag zu erstellen.
3. Aktivieren Sie in der gewünschten Zeile "Trap".
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

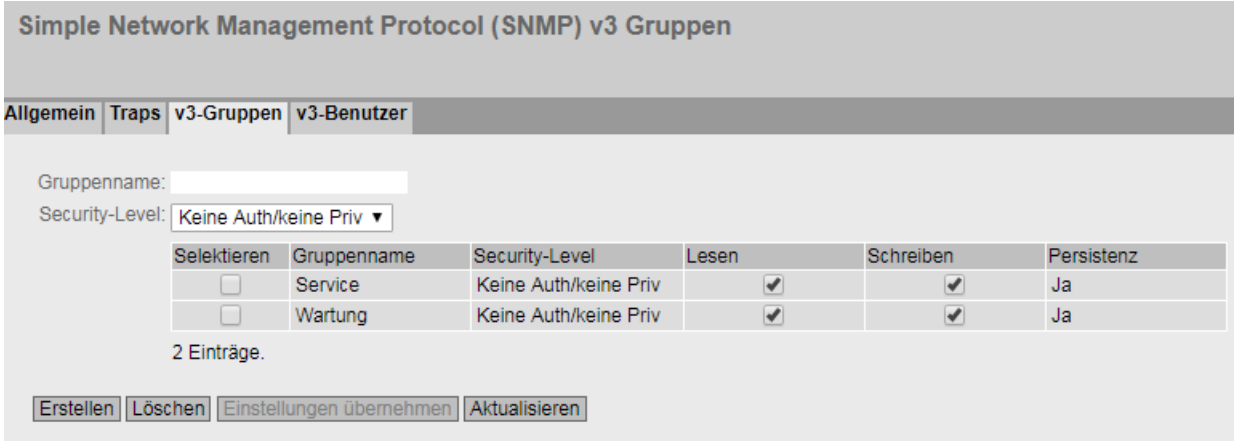
Trap-Eintrag löschen

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

6.5.11.3 v3-Gruppen

Security-Einstellungen und Rechtevergabe

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



Beschreibung

Die Seite enthält folgende Felder:

- **Gruppenname**
  Tragen Sie den Namen der Gruppe ein. Die maximale Länge beträgt 32 Zeichen.
- **Security-Level**
  Wählen Sie die Sicherheitsstufe (Authentifizierung, Verschlüsselung) aus, die für die gewählte Gruppe gültig ist. Es gibt folgende Möglichkeiten:
  - Keine Auth/keine Priv
    Keine Authentifizierung aktiviert / keine Verschlüsselung aktiviert.
  - Auth/keine Priv
    Authentifizierung aktiviert / keine Verschlüsselung aktiviert.
  - Auth/Priv
    Authentifizierung aktiviert / Verschlüsselung aktiviert.

Die Tabelle gliedert sich in folgende Spalten:

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

  Hinweis

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

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

Vorgehensweise

Anlegen einer neuen Gruppe

1. Geben Sie bei "Gruppenname" den gewünschten Gruppennamen ein.
2. Wählen Sie aus der Klappliste "Security-Level" die gewünschte Sicherheitsstufe aus.
3. Klicken Sie auf die Schaltfläche "Erstellen", um einen neuen Eintrag zu erzeugen.

4. Legen Sie bei "Lesen" die gewünschten Leserechte für die Gruppe fest.
5. Legen Sie bei "Schreiben" die gewünschten Schreibrechte für die Gruppe fest.
6. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Ändern einer Gruppe

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

Hinweis

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

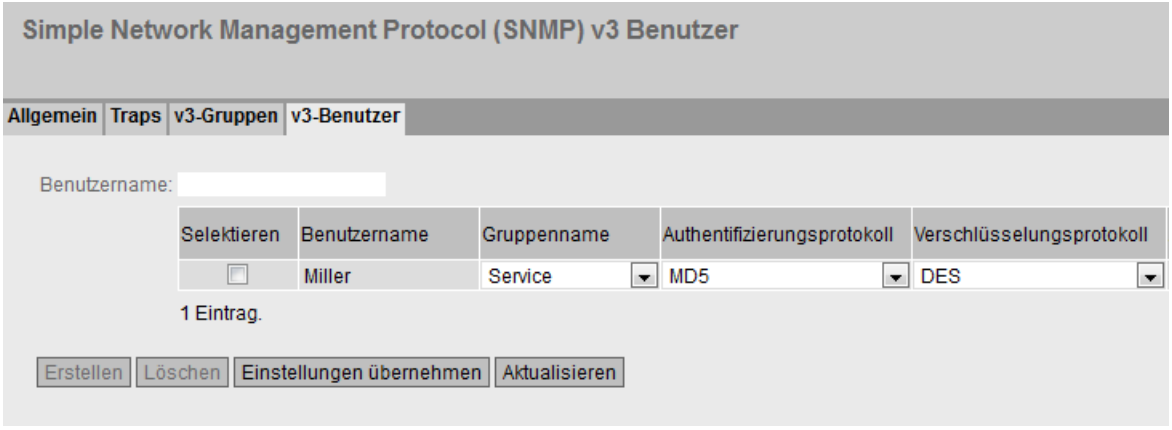
Löschen einer Gruppe

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

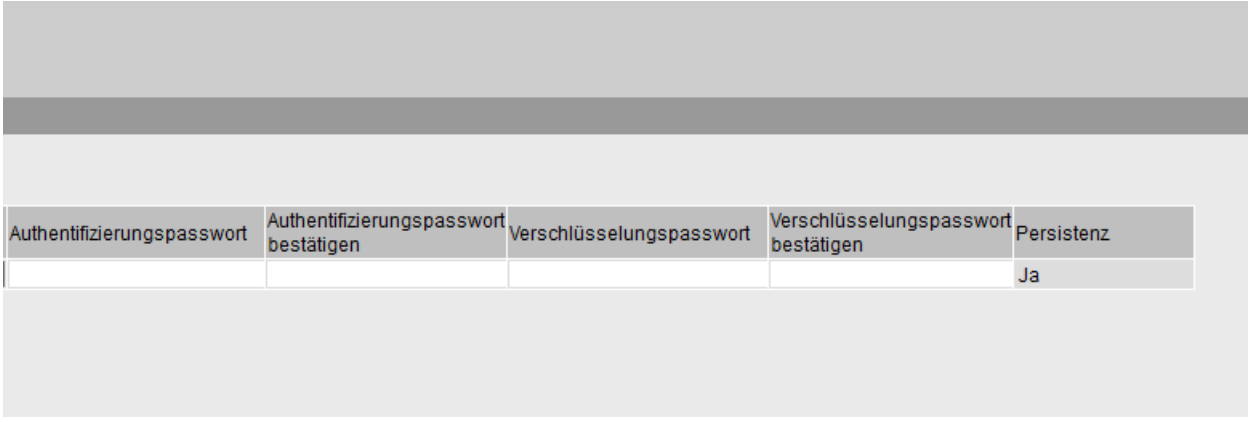
6.5.11.4 v3-Benutzer

Benutzerspezifische Sicherheitseinstellungen

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



SNMPv3-Benutzer - erster Teil der Tabelle



SNMPv3-Benutzer - zweiter Teil der Tabelle

Beschreibung

Die Seite enthält folgende Felder:

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

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Benutzername**
  Zeigt die angelegten Benutzer an.
- **Gruppenname**
  Wählen Sie die Gruppe aus, die dem Benutzer zugeordnet wird.
- **Authentifizierungsprotokoll**
  Legen Sie das Authentifizierungsprotokoll fest, für das ein Passwort hinterlegt werden soll. Folgende Einstellungen gibt es:
  - Keine
  - MD5
  - SHA
- **Verschlüsselungsprotokoll**
  Legen Sie fest, ob ein Passwort zur Verschlüsselung mit dem DES-Algorithmus hinterlegt werden soll. Nur aktivierbar, wenn auch ein Authentifizierungsprotokoll ausgewählt wurde.
- **Authentifizierungspasswort**
  Geben Sie in das erste Eingabefeld das Authentifizierungspasswort ein. Das Passwort muss mindestens 1 Zeichen lang sein, die maximale Länge beträgt 32 Zeichen.

  Hinweis

  Länge des Passworts

  Als wichtige Maßnahme zur Erhöhung der Sicherheit empfehlen wir, dass das Passwort mindestens 6 Zeichen lang ist und Sonderzeichen, Groß-/Kleinschreibung sowie Zahlen enthält.
- **Authentifizierungspasswort bestätigen**
  Bestätigen Sie das Passwort durch die Wiederholung der Eingabe.
- **Verschlüsselungspasswort**
  Geben Sie Ihr Verschlüsselungspasswort ein. Das Passwort muss mindestens 1 Zeichen lang sein, die maximale Länge beträgt 32 Zeichen.

  Hinweis

  Länge des Passworts

  Als wichtige Maßnahme zur Erhöhung der Sicherheit empfehlen wir, dass das Passwort mindestens 6 Zeichen lang ist und Sonderzeichen, Groß-/Kleinschreibung sowie Zahlen enthält.

- **Verschlüsselungspasswort bestätigen**
  Bestätigen Sie das Verschlüsselungspasswort durch die Wiederholung der Eingabe.
- **Persistenz**
  Zeigt an, ob der Benutzer einer SNMPv3-Gruppe zugeordnet ist. Wenn der Benutzer keiner SNMPv3-Gruppe zugeordnet ist, wird kein automatisches Speichern ausgelöst und der konfigurierte Benutzer ist nach einem Neustart des Geräts gelöscht.
  - Ja
    Der Benutzer ist einer SNMPv3-Gruppe zugeordnet.
  - Nein
    Der Benutzer ist keiner SNMPv3-Gruppe zugeordnet.

Vorgehensweise

Neuen Benutzer anlegen

1. Geben Sie im Eingabefeld "Benutzername" den Namen des neuen Benutzers ein.
2. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag erzeugt.
3. Wählen Sie bei "Gruppenname" die Gruppe aus, der der neue Benutzer angehören soll. Wenn die Gruppe noch nicht angelegt ist, wechseln Sie auf die Seite "v3-Gruppen" und legen Sie die Einstellungen für diese Gruppe fest.
4. Wenn für die ausgewählte Gruppe eine Authentifizierung notwendig ist, wählen Sie bei "Authentifizierungsprotokoll" den Authentifizierungsalgorithmus.
   Tragen Sie in die entsprechenden Eingabefelder das Authentifizierungspasswort sowie dessen Bestätigung ein.
5. Wenn für die Gruppe eine Verschlüsselung festgelegt wurde, wählen Sie bei "Verschlüsselungsprotokoll" den Algorithmus aus. Tragen Sie in die entsprechenden Eingabefelder das Verschlüsselungspasswort sowie dessen Bestätigung ein.
6. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Benutzer löschen

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

6.5.12 Systemzeit

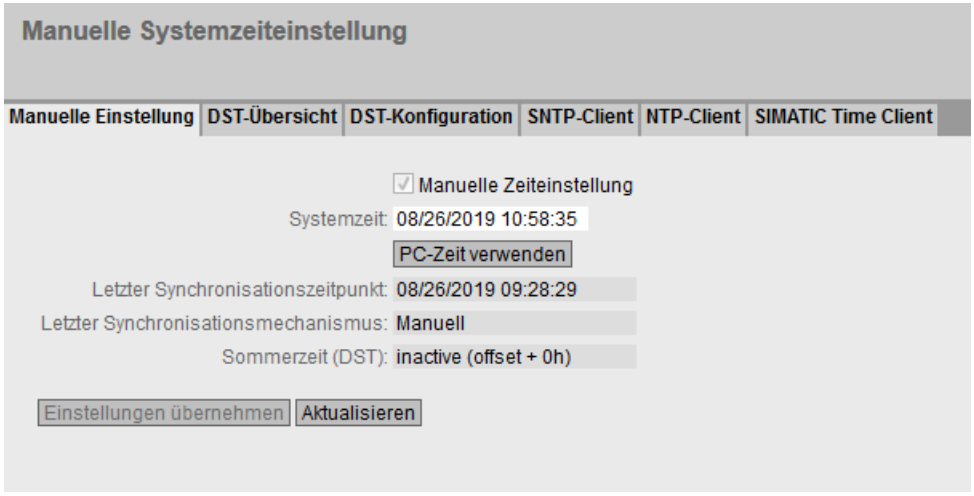
Um die Systemzeit des Geräts einzustellen, gibt es unterschiedliche Methoden. Es kann immer nur eine Methode aktiv sein.

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

6.5.12.1 Manuelle Einstellung

Manuelle Einstellung der Systemzeit

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



Beschreibung

Die Seite enthält folgende Felder:

- **Manuelle Zeiteinstellung**
  Aktivieren Sie die manuelle Zeiteinstellung. Wenn Sie die Option aktivieren, wird das Eingabefeld "Systemzeit" editierbar.
- **Systemzeit**
  Geben Sie Datum und Uhrzeit im Format "MM/DD/YYYY HH:MM:SS" ein.
  Nach einem Neustart beginnt die Uhrzeit mit 01/01/2000 00:00:00.
- **PC-Zeit verwenden**
  Klicken Sie auf die Schaltfläche, um die Zeiteinstellung des PCs zu übernehmen.
- **Letzter Synchronisationszeitpunkt**
  Zeigt an, wann die letzte Uhrzeitsynchronisation stattgefunden hat. Wenn keine Uhrzeitsynchronisation möglich war, enthält das Feld die Angabe "Date/time not set".

- **Letzter Synchronisationsmechanismus**
  Zeigt an, wie die letzte Zeitsynchronisation durchgeführt wurde.
  - Nicht eingestellt
    Die Zeit wurde nicht eingestellt.
  - Manuell
    Manuelle Zeiteinstellung
  - SNTP
    Automatische Zeitsynchronisation über SNTP
  - NTP
    Automatische Zeitsynchronisation über NTP
  - SIMATIC
    Automatische Zeitsynchronisation über SIMATIC-Uhrzeittelegramm
- **Sommerzeit (DST)**
  Zeigt an, ob die Umstellung der Sommerzeit aktiv ist.
  - active (offset +1 h)
    Die Systemzeit wurde auf Sommerzeit umgestellt, d. h. es wird eine Stunde hinzugezählt.
    Die aktuelle Systemzeit sehen Sie oben rechts im Auswahlbereich des WBM.
    In dem Feld "Systemzeit" wird die aktuelle Zeit inklusive der Sommerzeit angezeigt.
  - inactive (offset +0 h)
    Die aktuelle Systemzeit wird nicht verändert.

Vorgehensweise

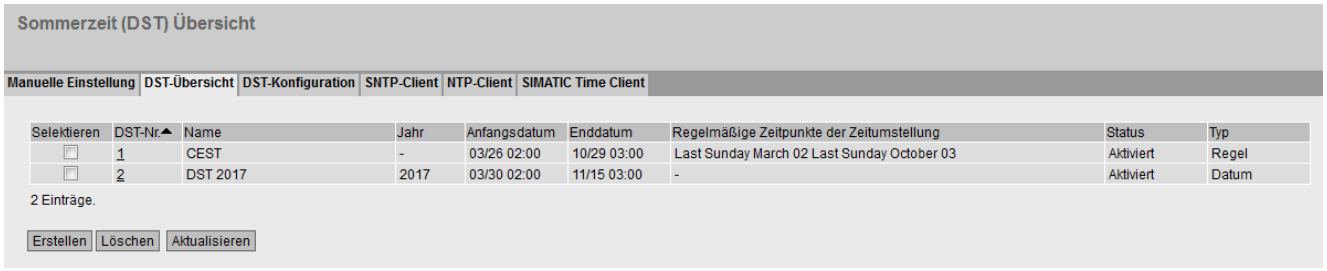
1. Aktivieren Sie die Option "Manuelle Zeiteinstellung".
2. Geben Sie im Eingabefeld "Systemzeit" Datum und Uhrzeit im Format " MM/DD/YYYY HH:MM:SS" ein.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
   Datum und Uhrzeit werden übernommen und im Feld "Letzter Synchronisationsmechanismus" wird "Manuell" eingetragen.

6.5.12.2 DST-Übersicht

Auf dieser Seite können Sie neue Einträge für die Umstellung der Sommerzeit anlegen.

Die Tabelle gibt Ihnen einen Überblick über die vorhandenen Einträge.

Einstellungen



- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **DST-Nr.**
  Zeigt die Nummer des Eintrags an.
  Wenn Sie einen neuen Eintrag anlegen, wird eine neue Zeile mit einer eindeutigen Nummer angelegt.
- **Name**
  Zeigt den Namen des Eintrags an.
- **Jahr**
  Zeigt das Jahr an, für das der Eintrag angelegt wurde.
- **Anfangsdatum**
  Zeigt Monat, Tag und Uhrzeit für den Start der Sommerzeit an.
- **Enddatum**
  Zeigt Monat, Tag und Uhrzeit für das Ende der Sommerzeit an.
- **Regelmäßige Zeitpunkte der Zeitumstellung**
  Bei einem Eintrag des Typs "Regel" wird die Zeitspanne angezeigt, bestehend aus Woche, Tag, Monat und Uhrzeit, in der die Sommerzeit aktiv ist.
  Bei einem Eintrag des Typs "Datum" wird ein "-" angezeigt.
- **Status**
  Zeigt der Status des Eintrags an:
  - Aktiviert
    Der Eintrag wurde korrekt angelegt.
  - Ungültig
    Der Eintrag wurde neu angelegt und Anfangs- und Enddatum sind identisch.
- **Typ**
  Zeigt an, wie die Umstellung der Sommerzeit erfolgt:
  - Datum
    Es ist ein festes Datum für die Umstellung der Sommerzeit eingetragen.
  - Regel
    Es ist eine Regel für die Umstellung der Sommerzeit definiert.

Vorgehensweise

Eintrag anlegen

1. Klicken Sie auf die Schaltfläche "Erstellen".
   In der Tabelle wird ein neuer Eintrag angelegt.
2. Klicken Sie in der Spalte "DST-Nr." auf den gewünschten Eintrag.
   Sie wechseln auf die Seite "DST-Konfiguration".
3. Wählen Sie in der Klappliste "Typ" den gewünschten Typ aus.
   Abhängig von dem gewählten Typ stehen Ihnen verschiedene Einstellungen zur Verfügung.
4. Geben Sie im Feld "Name" einen Namen ein.
5. Wenn Sie den Typ "Datum" ausgewählt haben, füllen Sie folgende Felder aus:
   - Jahr
   - Tag (für Anfangs- und Enddatum)
   - Stunde (für Anfangs- und Enddatum)
   - Monat (für Anfangs- und Enddatum)
6. Wenn Sie den Typ "Regel" ausgewählt haben, füllen Sie folgende Felder aus:
   - Stunde (für Anfangs- und Enddatum)
   - Monat (für Anfangs- und Enddatum)
   - Woche (für Anfangs- und Enddatum)
   - Tag (für Anfangs- und Enddatum)
7. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Eintrag löschen

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

6.5.12.3 DST-Konfiguration

Auf dieser Seite können Sie die Einträge für die Umstellung der Sommerzeit konfigurieren. Durch die Umstellung auf Sommer- bzw. Winterzeit ist die Systemzeit für die lokale Zeitzone korrekt eingestellt.

Sie können eine Regel für die Umstellung der Sommerzeit definieren oder ein festes Datum angeben.

Einstellungen

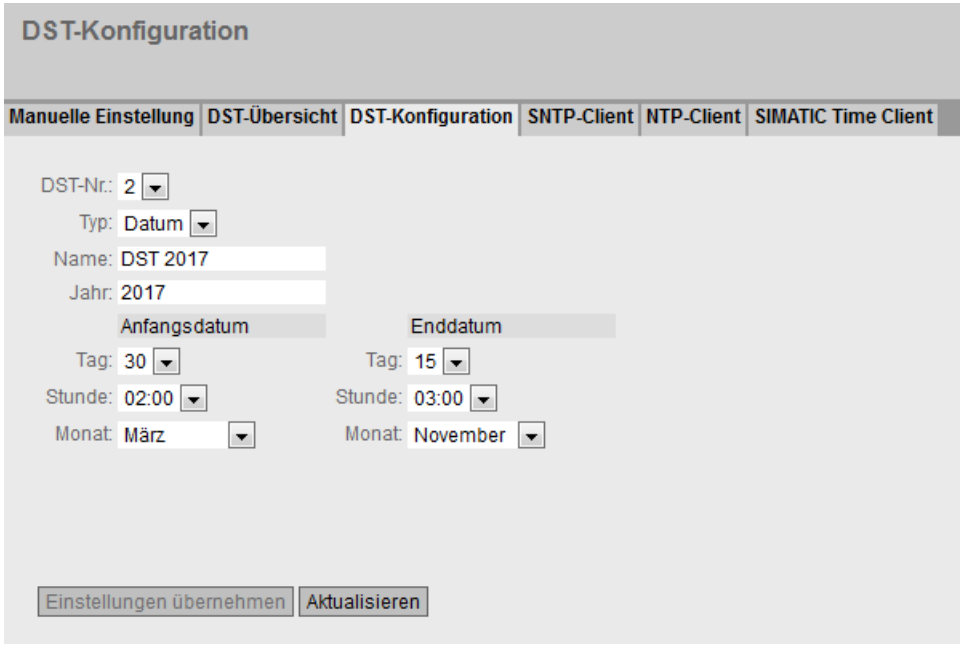
Hinweis

Der Inhalt dieser Seite ist abhängig davon, was Sie im Feld "Typ" auswählen.

Die Felder "DST-Nr.", "Typ" und "Name" werden immer angezeigt.

- **DST-Nr.**
  Wählen Sie die Nummer des Eintrags aus.
- **Typ**
  Wählen Sie aus, wie die Umstellung der Sommerzeit erfolgen soll:
  - Datum
    Sie können ein festes Datum für die Umstellung der Sommerzeit angeben.
    Diese Einstellung eignet sich für Regionen, in denen die Umstellung der Sommerzeit keiner Regel folgt.
  - Regel
    Sie können eine Regel für die Umstellung der Sommerzeit definieren.
    Diese Einstellung eignet sich für Regionen, in denen die Sommerzeit immer an einem bestimmten Wochentag beginnt bzw. endet.
- **Name**
  Geben Sie einen Namen für den Eintrag an.
  Der Name kann maximal 16 Zeichen lang sein.

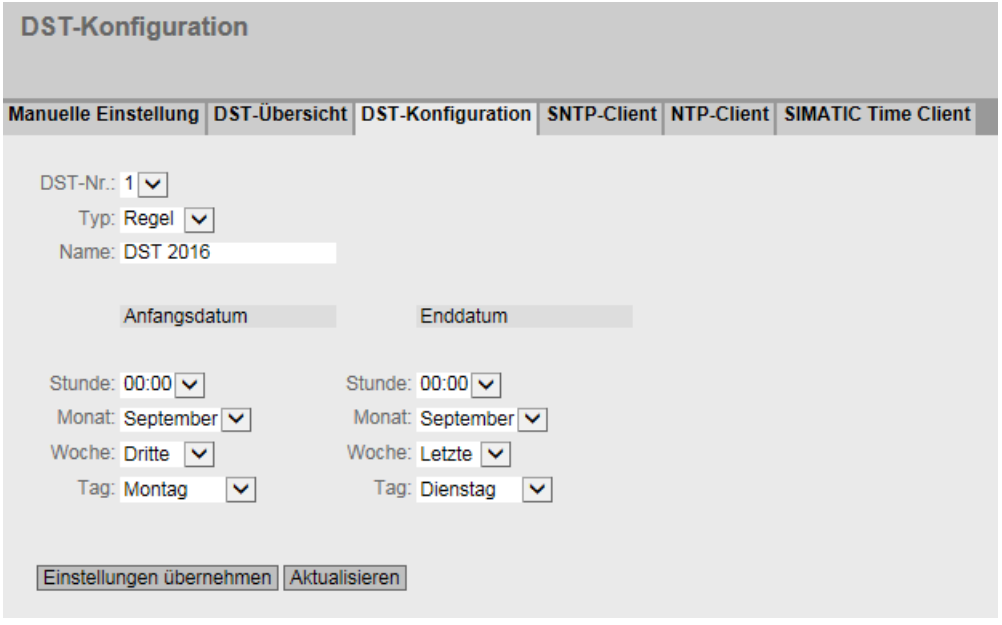
Einstellungen bei der Auswahl "Datum"



Sie können ein festes Datum für den Beginn und das Ende der Sommerzeit angeben.

- **Jahr**
  Geben Sie das Jahr für die Umstellung der Sommerzeit an.
- **Anfangsdatum**
  Geben Sie folgende Werte für den Beginn der Sommerzeit an:
  - Tag
    Geben Sie den Tag an.
  - Stunde
    Geben Sie die Stunde an.
  - Monat
    Geben Sie den Monat an.
- **Enddatum**
  Geben Sie folgende Werte für das Ende der Sommerzeit an:
  - Tag
    Geben Sie den Tag an.
  - Stunde
    Geben Sie die Stunde an.
  - Monat
    Geben Sie den Monat an.

Einstellungen bei der Auswahl "Regel"



Sie können eine Regel für die Umstellung der Sommerzeit erstellen.

- **Anfangsdatum**
  Geben Sie folgende Werte für den Beginn der Sommerzeit an:
  - Stunde
    Geben Sie die Stunde an.
  - Monat
    Geben Sie den Monat an.
  - Woche
    Geben Sie die Woche an.
    Sie können die erste bis fünfte oder die letzte Woche des Monats auswählen.
  - Tag
    Geben Sie den Wochentag an.
- **Enddatum**
  Geben Sie folgende Werte für das Ende der Sommerzeit an:
  - Stunde
    Geben Sie die Stunde an.
  - Monat
    Geben Sie den Monat an.
  - Woche
    Geben Sie die Woche an.
    Sie können die erste bis fünfte oder die letzte Woche des Monats auswählen.
  - Tag
    Geben Sie den Wochentag an.

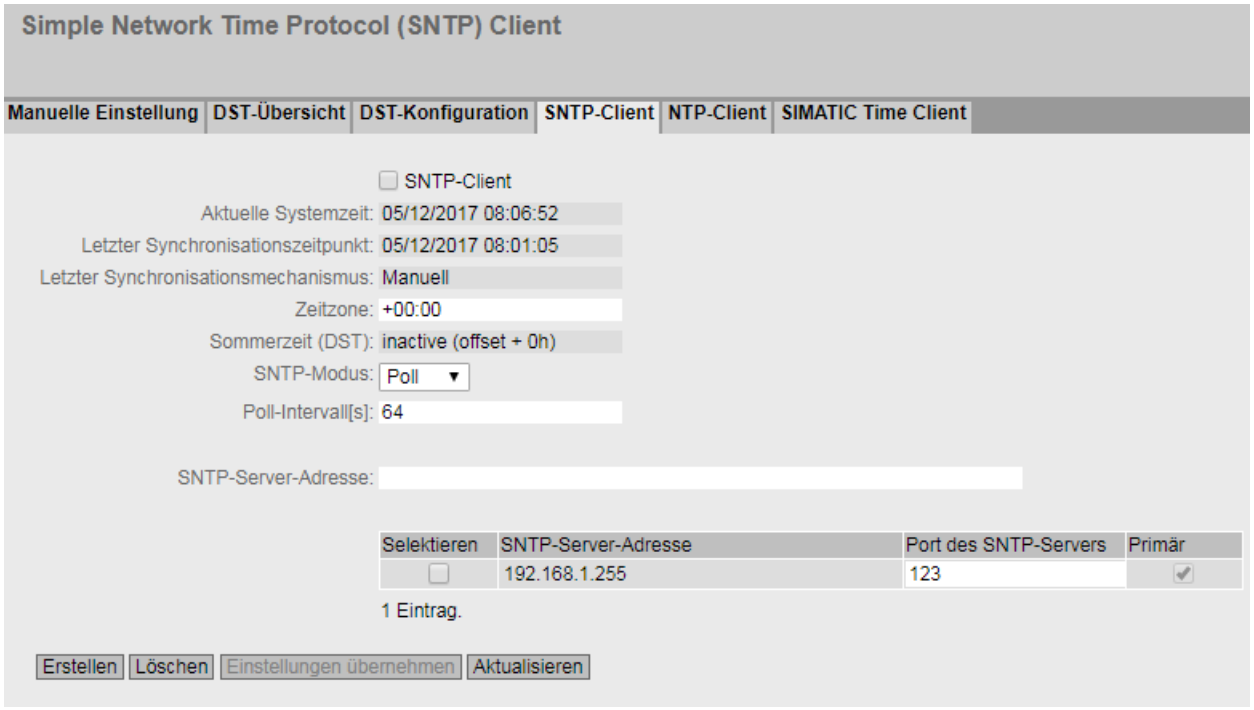
6.5.12.4 SNTP-Client

Uhrzeitsynchronisation im Netzwerk

Das SNTP (Simple Network Time Protocol) dient zur Zeitsynchronisation im Netzwerk. Die entsprechenden Telegramme werden von einem SNTP-Server im Netz versendet.

Hinweis

Um Zeitsprünge zu vermeiden, stellen Sie sicher, dass sich nur ein Zeitserver im Netz befindet.



Beschreibung

Die Seite enthält folgende Felder:

- **SNTP-Client**
  Aktivieren oder deaktivieren Sie die automatische Zeitsynchronisation über SNTP.
- **Aktuelle Systemzeit**
  Zeigt das aktuelle Datum und die aktuelle Normalzeit an, die vom Gerät empfangen wurden. Wenn Sie eine Zeitzone angeben, wird die Zeitangabe entsprechend angepasst.
- **Letzter Synchronisationszeitpunkt**
  Zeigt an, wann die letzte Uhrzeitsynchronisation stattgefunden hat.
- **Letzter Synchronisationsmechanismus**
  Zeigt an, wie die letzte Zeitsynchronisation durchgeführt wurde. Folgende Arten gibt es:
  - Nicht eingestellt
    Die Zeit wurde nicht eingestellt.
  - Manuell
    Manuelle Zeiteinstellung
  - SNTP
    Automatische Zeitsynchronisation über SNTP
  - NTP
    Automatische Zeitsynchronisation über NTP
  - SIMATIC
    Automatische Zeitsynchronisation über SIMATIC-Uhrzeittelegramm

- **Zeitzone**
  Geben Sie in diesem Feld Ihre verwendete Zeitzone im Format "+/- HH:MM" an. Die Zeitzone bezieht sich auf UTC Standard-Weltzeit.
  Die Zeitangabe im Feld "Aktuelle Systemzeit" wird entsprechend angepasst.
- **Sommerzeit (DST)**
  Zeigt an, ob die Umstellung der Sommerzeit aktiv ist.
  - active (offset +1 h)
    Die Systemzeit wurde auf Sommerzeit umgestellt, d. h. es wird eine Stunde hinzugezählt. Die aktuelle Systemzeit sehen Sie oben rechts im Auswahlbereich des WBM.
    In dem Feld "Systemzeit" wird die aktuelle Zeit inklusive der Sommerzeit angezeigt.
  - inactive (offset +0 h)
    Die aktuelle Systemzeit wird nicht verändert.
- **SNTP-Modus**
  Wählen Sie aus der Klappliste die Synchronisationsart aus. Folgende Synchronisierungsarten sind möglich:
  - Listen
    Bei diesem Modus ist das Gerät passiv und empfängt SNTP-Telegramme, die die Uhrzeit liefern. Einstellungen in den Eingabefeldern "SNTP-Server-Adresse" und "Port des SNTP-Servers" haben in diesem Modus keine Wirkung.
    In diesem Modus werden nur IPv4-Adressen unterstützt.
  - Poll
    Wenn Sie diesen Modus wählen, wird das Eingabefeld "Poll-Intervall[s]" zur weiteren Konfiguration eingeblendet. In diesem Modus werden die Einstellungen in den Eingabefeldern "SNTP-Server-Adresse" und "Port des SNTP-Servers" berücksichtigt. Bei dieser Synchronisationsart ist das Gerät aktiv und sendet eine Zeitabfrage an den SNTP-Server.
    In diesem Modus werden IPv4- und IPv6-Adressen unterstützt.
- **Poll-Intervall[s]**
  Geben Sie den Zeitabstand zwischen zwei Zeitanfragen ein. In diesem Feld geben Sie das Abfrageintervall in Sekunden an. Mögliche Werte sind 16 bis 16284 Sekunden.
- **SNTP-Server-Adresse**
  Geben Sie die IP-Adresse oder den FQDN (Fully Qualified Domain Name) des SNTP-Servers ein.
- **Port des SNTP-Servers**
  Geben Sie den Port des SNTP-Servers ein.
  Folgende Ports sind möglich:
  - 123 (Standard-Port)
  - 1025 bis 36564
- **Primär**
  Bei dem SNTP-Server, den Sie zuerst anlegen, wird das Häkchen gesetzt. Wenn mehrere SNTP-Server angelegt sind, wird der primäre Server zuerst angefragt.

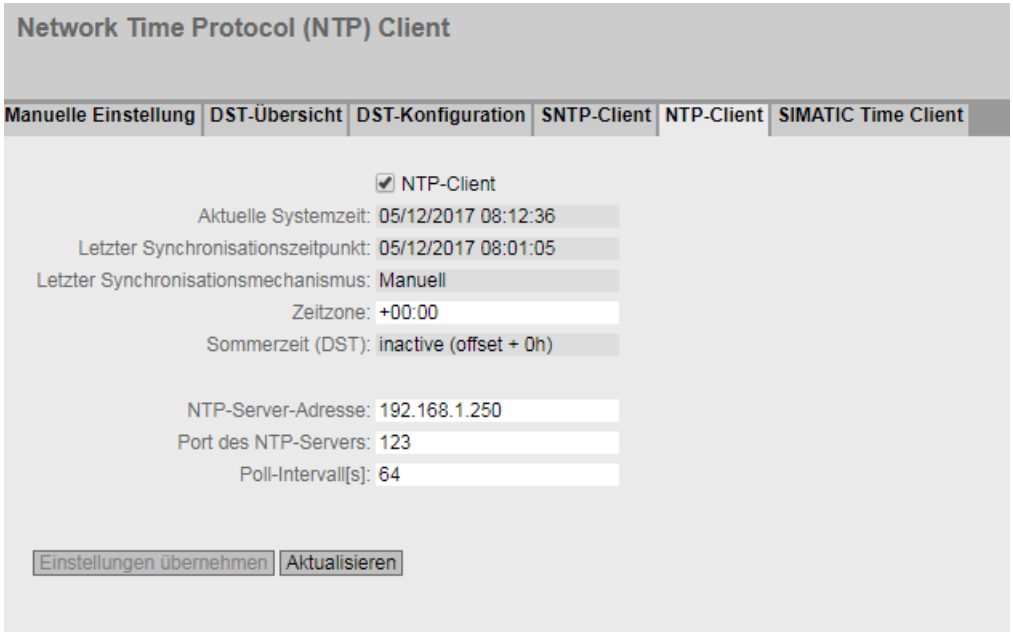
Vorgehensweise

1. Klicken Sie in das Optionskästchen "SNTP-Client", um die automatische Zeiteinstellung zu aktivieren.
2. Geben Sie in das Eingabefeld "Zeitzone" 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. Die Umstellung der Sommerzeit konfigurieren Sie auf den Seiten "System > Systemzeit > DST-Übersicht" und "System > Systemzeit > DST-Konfiguration". Dies müssen Sie ebenfalls bei der Eingabe in das Eingabefeld "Zeitzone" berücksichtigen.
3. Wählen Sie aus der Klappliste "SNTP-Modus" aus folgenden Optionen aus:
   - Poll
     Für diese Betriebsart müssen Sie Folgendes konfigurieren:
     - Zeitzonendifferenz (Schritt 2)
     - Abfrageintervall (Schritt 4)
     - Zeit-Server (Schritt 5)
     - Port (Schritt 7)
     - Schließen Sie die Konfiguration mit Schritt 8 ab.
   - Listen
     Für diese Betriebsart müssen Sie Folgendes konfigurieren:
     - Zeitdifferenz zu der vom Server gesendeten Zeit (Schritt 2)
     - Schließen Sie die Konfiguration mit Schritt 8 ab.
4. Geben Sie in das Eingabefeld "Poll-Intervall[s]" die Zeitspanne in Sekunden ein, nach der eine neue Zeitanfrage beim Zeit-Server gestartet werden soll.
5. Geben Sie im Eingabefeld "SNTP-Server-Adresse" die IP-Adresse oder den FQDN des SNTP-Servers ein, dessen Telegramme für die Synchronisation der Uhrzeit verwendet werden sollen.
6. Klicken Sie auf die Schaltfläche "Erstellen".
   In der Tabelle wird eine Zeile für den SNTP-Server angelegt.
7. Geben Sie in der Spalte "Port des SNTP-Servers" den Port ein, über den der SNTP-Server verfügbar ist. Der Port kann nur geändert werden, wenn die IPv4-Adresse oder den FQDN-Namen des SNTP-Servers eingetragen ist.
8. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen", um Ihre Änderungen in das Gerät zu übertragen.

6.5.12.5 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.
- **Aktuelle Systemzeit**
  Zeigt das aktuelle Datum und die aktuelle Normalzeit an, die vom Gerät empfangen wurden. Wenn Sie eine Zeitzone angeben, wird die Zeitangabe entsprechend angepasst.
- **Letzter Synchronisationszeitpunkt**
  Zeigt an, wann die letzte Uhrzeitsynchronisation stattgefunden hat.

- **Letzter Synchronisationsmechanismus**
  Zeigt an, wie die letzte Zeitsynchronisation durchgeführt wurde. Folgende Arten gibt es:
  - Nicht eingestellt
    Die Zeit wurde nicht eingestellt.
  - Manuell
    Manuelle Zeiteinstellung
  - SNTP
    Automatische Zeitsynchronisation über SNTP
  - NTP
    Automatische Zeitsynchronisation über NTP
  - SIMATIC
    Automatische Zeitsynchronisation über SIMATIC-Uhrzeittelegramm
- **Zeitzone**
  Geben Sie in diesem Feld Ihre verwendete Zeitzone im Format "+/- HH:MM" an. Die Zeitzone bezieht sich auf UTC Standard-Weltzeit.
  Die Zeitangabe im Feld "Aktuelle Systemzeit" wird entsprechend angepasst.
- **Sommerzeit (DST)**
  Zeigt an, ob die Umstellung der Sommerzeit aktiv ist.
  - active (offset +1 h)
    Die Systemzeit wurde auf Sommerzeit umgestellt, d. h. es wird eine Stunde hinzugezählt.
    Die aktuelle Systemzeit sehen Sie oben rechts im Auswahlbereich des WBM.
    In dem Feld "Systemzeit" wird die aktuelle Zeit inklusive der Sommerzeit angezeigt.
  - inactive (offset +0 h)
    Die aktuelle Systemzeit wird nicht verändert.
- **NTP-Server-Adresse**
  Geben Sie die IP-Adresse oder den FQDN (Fully Qualified Domain Name) des NTP-Servers an.
- **Port des NTP-Servers**
  Geben Sie den Port des NTP-Servers an.
  Folgende Ports sind möglich:
  - 123 (Standard-Port)
  - 1025 bis 36564
- **Poll-Intervall[s]**
  Geben Sie in diesem Feld den Zeitabstand zwischen zwei Zeitanfragen (Abfrageintervall) in Sekunden ein. Mögliche Werte sind 64 bis 1024 Sekunden.

Vorgehensweise

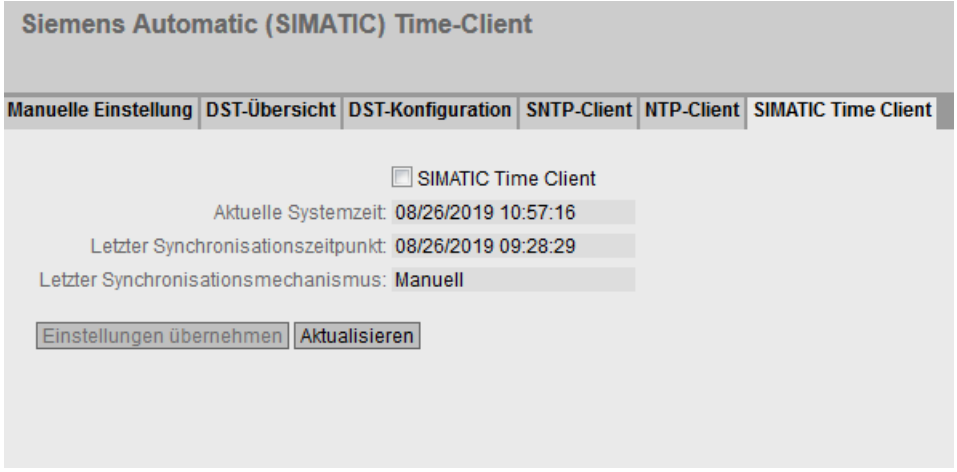
1. Klicken Sie in das Optionskästchen "NTP-Client", um die automatische Zeiteinstellung über NTP zu aktivieren.
2. Tragen Sie die erforderlichen Werte in die folgenden Felder ein:
   - Zeitzone
   - IP-Adresse oder FQDN des NTP-Servers
   - Port des NTP-Servers
   - Abfrageintervall
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.5.12.6 SIMATIC Time Client

Zeiteinstellung über SIMATIC Time Client

Hinweis

Um Zeitsprünge zu vermeiden, stellen Sie sicher, dass sich nur ein Zeitserver im Netz befindet.



Beschreibung

Die Seite enthält folgende Felder:

- **SIMATIC Time Client**
  Markieren Sie dieses Optionskästchen, um das Gerät als SIMATIC Time Client zu aktivieren.
- **Aktuelle Systemzeit**
  Zeigt die aktuelle Systemzeit an.

- **Letzter Synchronisationszeitpunkt**
  Zeigt an, wann die letzte Uhrzeitsynchronisation stattgefunden hat.
- **Letzter Synchronisationsmechanismus**
  Zeigt an, wie die letzte Zeitsynchronisation durchgeführt wurde. Folgende Arten gibt es:
  - Nicht eingestellt
    Die Zeit wurde nicht eingestellt.
  - Manuell
    Manuelle Zeiteinstellung
  - SNTP
    Automatische Zeitsynchronisation über SNTP
  - NTP
    Automatische Zeitsynchronisation über NTP
  - SIMATIC
    Automatische Zeitsynchronisation über SIMATIC-Uhrzeittelegramm

Vorgehensweise

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

6.5.13 Auto-Logout

Einstellung der automatischen Abmeldung

Auf dieser Seite legen Sie die Zeiten fest, nach denen bei Inaktivität des Benutzers eine automatische Abmeldung vom WBM oder dem CLI stattfindet.

Wenn Sie automatisch abgemeldet wurden, dann müssen Sie sich wieder neu anmelden.

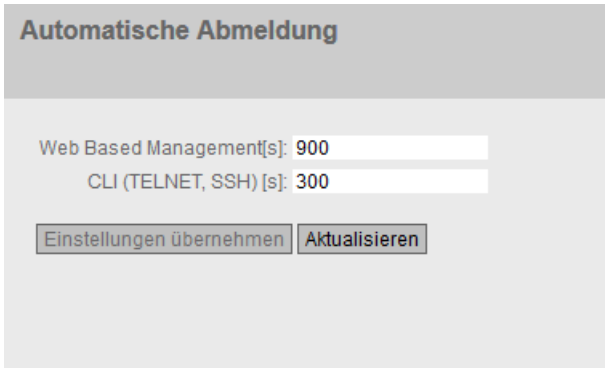
Hinweis

Keine automatische Abmeldung vom CLI

Wenn die Verbindung nach der eingestellten Zeit nicht beendet wird, prüfen Sie am Telnet Client die Einstellung von "Keep alive".

Ist die Intervallzeit für "Keep alive" kleiner als die projektierte Zeit, wird die Verbindung aufrechterhalten, obwohl keine Nutzdaten übertragen werden. Z. B. Sie haben bei der automatischen Abmeldung 300 Sekunden und bei "Keep alive" 120 Sekunden eingestellt. In diesem Fall wird alle 120 Sekunden ein Paket gesendet, das die Verbindung ununterbrochen aufrechterhält.

- Schalten Sie die "Keep alive" aus (Intervallzeit=0)
  oder
- Stellen Sie die Intervallzeit so hoch ein, dass die unterlagerte Verbindung bei Inaktivität beendet wird.



Vorgehensweise

1. Geben Sie in das Eingabefeld "Web Base Management [s]" einen Wert von 60-3600 Sekunden ein. Wenn Sie den Wert 0 eingeben, ist die automatische Abmeldung deaktiviert.
2. Geben Sie in das Eingabefeld "CLI (TELNET, SSH) [s]" einen Wert von 60-600 Sekunden ein. Wenn Sie den Wert 0 eingeben, ist die automatische Abmeldung deaktiviert.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.5.14 Syslog-Client

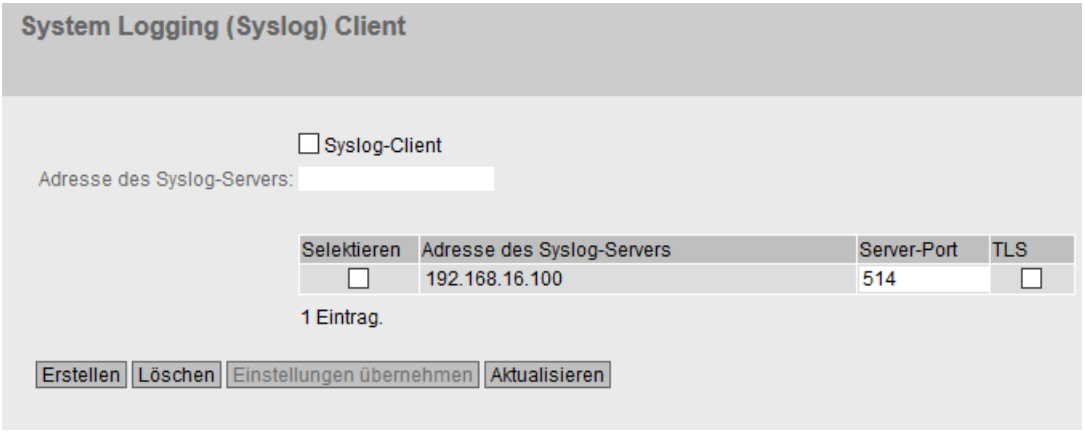
Systemereignis-Agent

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 entgegennimmt. (Da es sich um eine UDP-Verbindung handelt, gibt es keine Rückmeldung an den Absender.)
- Die IP-Adresse oder den FQDN (Fully Qualified Domain Name) des Syslog-Servers ist im Gerät eingetragen.



Beschreibung

Die Seite enthält folgende Felder:

- **Syslog-Client**
  Aktivieren oder deaktivieren Sie die Syslog-Funktion.
- **Adresse des Syslog-Servers**
  Geben Sie die IP-Adresse, den FQDN (Fully Qualified Domain Name) oder den Hostnamen des Syslog-Servers an.

Die Tabelle enthält folgende Spalten

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Adresse des Syslog-Servers**
  Zeigt die IP-Adresse, den FQDN (Fully Qualified Domain Name) oder den Hostnamen des Syslog-Servers an.
- **Server-Port**
  Geben Sie den verwendeten Port des Syslog-Servers ein.
- **TLS**
  Wenn diese Optionskästchen aktiviert ist, wird die Kommunikation mit dem Syslog-Server verschlüsselt.

Vorgehensweise

Funktion aktivieren

1. Aktivieren Sie das Optionskästchen "Syslog-Client".
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Neuen Eintrag anlegen

1. Geben Sie in das Eingabefeld "Adresse des Syslog-Servers" die IP-Adresse, den FQDN oder den Hostnamen des Syslog-Servers ein, auf dem die Protokolleinträge gespeichert werden sollen.
2. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird eine neue Zeile eingefügt.
3. Geben Sie in das Eingabefeld "Server-Port" die Nummer des UDP-Ports des Servers ein.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Hinweis

Die Standardeinstellung des Server Ports ist Port 514.

Eintrag ändern

1. Löschen Sie den Eintrag.
2. Legen Sie einen neuen Eintrag an.

Eintrag löschen

1. Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
2. Klicken Sie auf die Schaltfläche "Löschen". Alle markierten Einträge werden gelöscht und die Anzeige wird aktualisiert.

6.5.15 Fehlerkontrolle

6.5.15.1 Spannungsversorgung

Einstellungen zur Überwachung der Spannungsversorgung

Konfigurieren Sie, ob die Spannungsversorgung durch das Meldesystem überwacht werden soll. Je nach Hardware-Variante gibt es ein oder zwei Spannungsanschlüsse (Versorgung 1 / Versorgung 2) und eine PoE-Spannungsversorgung. Bei redundanter Spannungsversorgung konfigurieren Sie die Überwachung für jede einzelne Zuleitung getrennt.

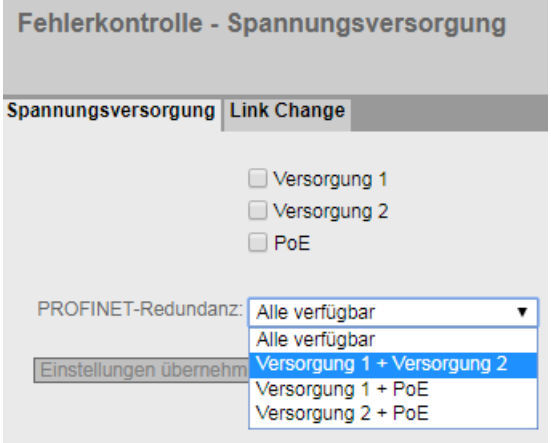
Es wird dann ein Fehler durch das Meldesystem signalisiert, wenn an einem überwachten Anschluss (Versorgung 1, Versorgung 2 oder PoE) keine oder eine zu geringe Spannung anliegt.

Hinweis

Die zulässigen Betriebsspannungsgrenzen entnehmen Sie der Betriebsanleitung des Geräts.

Wenn ein Fehler auftritt, leuchtet am Gerät die Fehler-LED auf. Der aktuell anstehende Fehler wird unter "Information > Fehler" angezeigt.

Zusätzlich wird die entsprechende Fehlermeldung in die Ereignisprotokoll-Tabelle eingetragen. Den Inhalt der Ereignisprotokoll-Tabelle wird unter "Information > Log-Tabellen > Ereignis-Log" angezeigt.



Vorgehensweise

1. Klicken Sie in das Optionskästchen vor dem entsprechenden Anschlussnamen, den Sie überwachen wollen, um die Überwachungsfunktion ein- oder auszuschalten.
2. Wählen Sie aus der Klappliste "PROFINET-Redundanz" den gewünschten Eintrag für redundante Spannungsversorgung aus, die durch PROFINET überwacht werden soll.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.5.15.2 Link Change

Konfiguration der Fehlerüberwachung von Zustandsänderungen bei Verbindungen

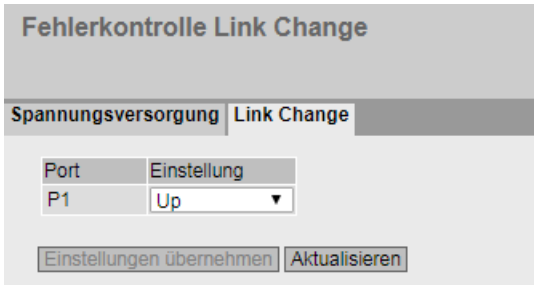
Auf dieser Seite konfigurieren Sie, ob bei einer Zustandsänderung einer Netzwerkverbindung eine Fehlermeldung ausgelöst wird.

Bei aktivierter Verbindungsüberwachung wird ein Fehler signalisiert,

- wenn an einem Port ein Link vorhanden sein soll und dieser fehlt.
- oder wenn an dem Port kein Link vorhanden sein soll und ein Link erkannt wird.

Wenn ein Fehler auftritt, leuchtet am Gerät die Fehler-LED auf. Der aktuell anstehende Fehler wird unter "Information > Fehler" angezeigt.

Zusätzlich wird die entsprechende Fehlermeldung in die Ereignisprotokoll-Tabelle eingetragen. Den Inhalt der Ereignisprotokoll-Tabelle wird unter "Information > Log-Tabellen > Ereignis-Log" angezeigt.



Beschreibung

Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports gültig sind.
- **Einstellung**
  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellungsmöglichkeiten haben Sie:
  - "-" (Deaktiviert)
  - Up
  - Down
  - Keine Änderung: Einstellung in der Tabelle 2 bleibt unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt die verfügbaren Ports an.
- **Einstellung**
  Wählen Sie aus der Klappliste die Einstellung aus. Folgende Möglichkeiten haben Sie:
  - Up
    Die Fehlerbehandlung wird beim Übergang in den aktiven Zustand des Ports ausgelöst. (Von "Link down" nach "Link up")
  - Down
    Die Fehlerbehandlung wird beim Übergang in den inaktiven Zustand des Ports ausgelöst. (Von "Link up" nach "Link down")
  - "-" (Deaktiviert)
    Die Fehlerbehandlung wird nicht ausgelöst.

Vorgehensweise

Fehlerüberwachung für einen Port konfigurieren

1. Wählen Sie aus der entsprechenden Klappliste die Optionen der Steckplätze/Ports, deren Verbindungsstatus Sie überwachen wollen.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

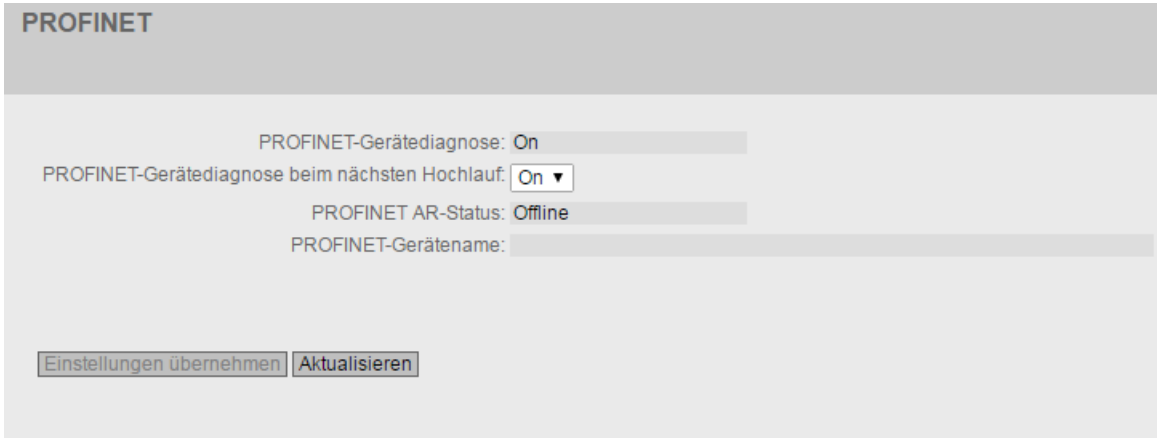
Fehlerüberwachung für alle Ports konfigurieren

1. Wählen Sie in der Klappliste der Spalte "Einstellung" die gewünschte Einstellung aus.
2. Klicken Sie auf die Schaltfläche "In Tabelle übernehmen". Die Einstellung wird für alle Ports der Tabelle 2 übernommen.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.5.16 PROFINET

Einstellungen für PROFINET

Diese Seite zeigt den PROFINET AR Status und den Gerätenamen an.



Beschreibung

Die Seite enthält folgende Felder:

- **PROFINET-Gerätediagnose**
  Zeigt an, ob PROFINET aktiviert ("On") oder deaktiviert ("Off") ist.
- **PROFINET-Gerätediagnose beim nächsten Hochlauf**
  Stellen Sie ein, ob PROFINET nach dem nächsten Neustart des Geräts aktiviert ("On") oder deaktiviert ("Off") sein soll.

Hinweis

PROFINET und EtherNet/IP

Wenn PROFINET eingeschaltet wird, wird EtherNet/IP ausgeschaltet. Das Umschalten von PROFINET und EtherNet/IP hat keine Auswirkungen auf DCP.

Hinweis

PROFINET AR-Status

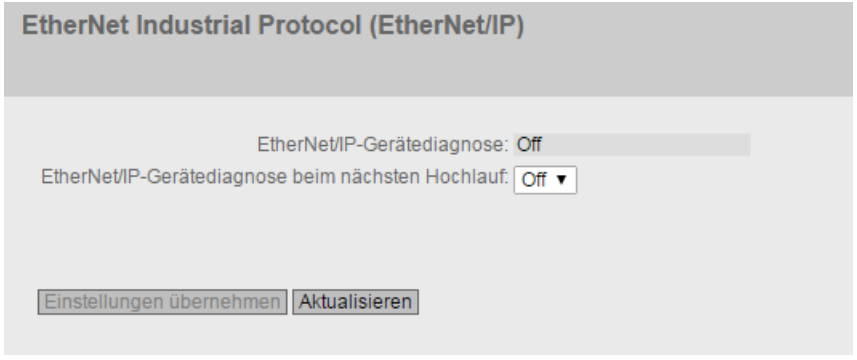
Wenn eine PROFINET-Verbindung aufgebaut ist, d. h. der PROFINET AR-Status "Online" ist, können Sie PROFINET nicht deaktivieren.

- **PROFINET AR-Status**
  Dieses Feld zeigt den Status des PROFINET-Verbindungsverhältnisses an, d.h. ob das Gerät mit einem PROFINET-Controller "Online" oder "Offline" verbunden ist.
  Online bedeutet hierbei, dass eine Verbindung zu einem PROFINET-Controller besteht, dass dieser seine Konfigurationsdaten auf das Gerät geladen hat und das Gerät Statusdaten zum PROFINET-Controller senden kann. In diesem Zustand, der auch "in Data exchange" genannt wird, sind die Parameter, die über den PROFINET-Controller eingestellt werden, nicht konfigurierbar.
- **PROFINET-Gerätename**
  In diesem Feld erscheint der PROFINET-Gerätenamen gemäß der Projektierung in der HW-Konfig von STEP 7.

6.5.17 EtherNet/IP

Einstellungen für EtherNet/IP

Auf dieser Seite konfigurieren Sie den Modus von EtherNet/IP.



Beschreibung

Die Seite enthält folgende Felder:

- **EtherNet/IP-Gerätediagnose**
  Zeigt an, ob EtherNet/IP aktiviert ("On") oder deaktiviert ("Off") ist.
- **EtherNet/IP-Gerätediagnose beim nächsten Hochlauf**
  Stellen Sie ein, ob EtherNet/IP nach dem nächsten Neustart des Geräts aktiviert ("On") oder deaktiviert ("Off") sein soll.

Hinweis

EtherNet/IP und PROFINET

Wenn EtherNet/IP eingeschaltet wird, wird PROFINET ausgeschaltet. Das Umschalten von EtherNet/IP und PROFINET hat keine Auswirkungen auf DCP.

Hinweis

PROFINET AR Status

Wenn eine PROFINET-Verbindung aufgebaut ist, d. h. der PROFINET AR-Status "Online" ist, können Sie EtherNet/IP nicht aktivieren.

6.5.18 PLUG

6.5.18.1 Konfiguration

ACHTUNG
Den 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, startet das Gerät neu. War in dem Gerät ein gültiger PLUG-Lizenz gesteckt, wird das Gerät nach dem Neustart in einen definierten Fehlerzustand versetzt. Bei SCALANCE W werden in diesem Fall die verfügbaren Funkschnittstellen deaktiviert. Wenn das Gerät einmal mit einem PLUG-Lizenz konfiguriert wurde, kann das Gerät ohne diesen PLUG nicht mehr genutzt werden. Um das Gerät wieder nutzen zu können, setzen Sie das Gerät auf Werkseinstellungen zurück.

Informationen über die Konfiguration des PLUG

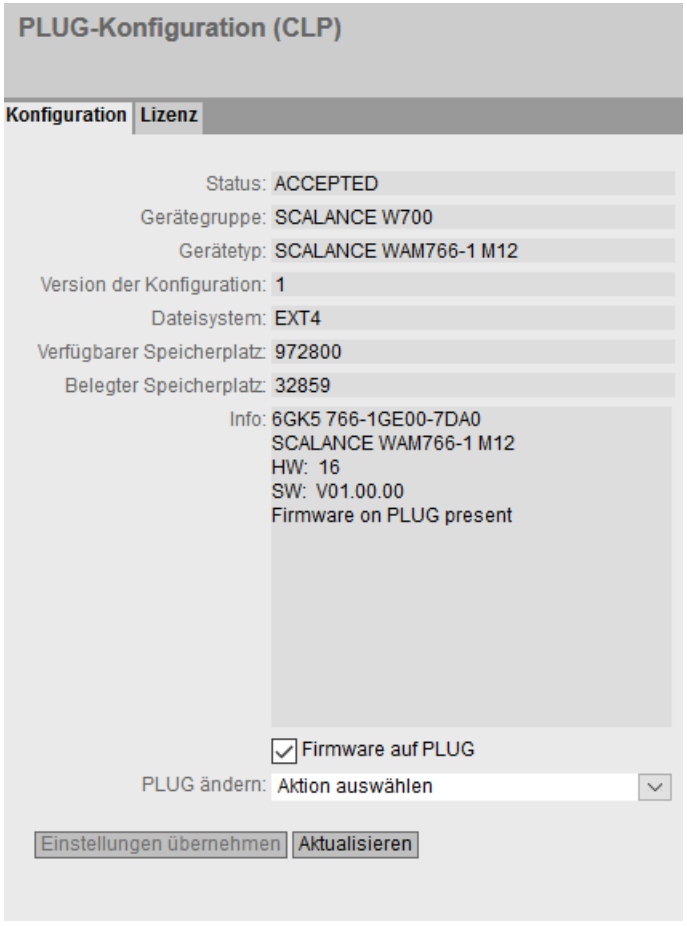
Diese Seite liefert Detailinformationen über die Konfiguration, die im PLUG abgelegt ist. Darüber hinaus gibt es die Möglichkeit, den PLUG auf "Werkeinstellungen" zurückzusetzen oder mit einem neuen Inhalt zu versehen.

Hinweis

Die Aktion wird erst dann durchgeführt, wenn Sie auf die Schaltfläche "Einstellungen übernehmen" klicken.

Die Aktion kann nicht rückgängig gemacht werden.

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



Beschreibung

Die Tabelle gliedert sich in folgende Zeilen:

- **Status**
  Zeigt den Status des PLUG an. Es gibt die folgenden Möglichkeiten:
  - ACCEPTED
    Es ist ein PLUG mit einer gültigen und passenden Konfiguration im Gerät vorhanden.
  - NOT ACCEPTED
    Ungültige bzw. inkompatible Konfiguration auf dem gesteckten PLUG.
  - NOT PRESENT
    Im Gerät ist kein PLUG gesteckt.
  - FACTORY
    PLUG ist gesteckt und enthält keine Konfiguration. Dieser Status wird auch angezeigt, wenn der PLUG im Betrieb formatiert wurde.
- **Gerätegruppe**
  Zeigt an, von welcher SIMATIC NET-Produktlinie der PLUG im vorangegangenen Betrieb genutzt wurde.
- **Gerätetyp**
  Zeigt den Gerätetyp innerhalb der Produktlinie an, von dem der PLUG im vorangegangenen Betrieb genutzt wurde.
- **Version der Konfiguration**
  Die Version der Konfigurationsstruktur. Diese Angabe betrifft die vom Gerät unterstützten Konfigurationsmöglichkeiten und hat nichts mit der konkreten Hardware-Konfiguration zu tun. Diese Revisionsangabe ändert sich also nicht, wenn Sie Zusatzkomponenten (z.B. Module bzw. Extender) hinzufügen oder entfernen, sie kann sich aber ändern, wenn Sie ein Firmware-Update durchführen.
- **Dateisystem**
  Zeigt den Typ des Dateisystems an, das auf dem PLUG vorhanden ist.
- **Verfügbarer Speicherplatz [KByte]**
  Zeigt die maximale Speicherkapazität des Dateisystems an, das auf dem PLUG vorhanden ist.
- **Belegter Speicherplatz [KByte]**
  Zeigt den belegten Speicherplatz im Dateisystem des PLUG an.
- **Info**
  Zeigt zusätzliche Informationen über das Gerät an, das den PLUG im vorangegangenen Betrieb genutzt hatte, z. B. Artikelnummer, Typenbezeichnung sowie die Ausgabestände von Hard- und Software. Der angezeigte Software-Ausgabestand entspricht dem Ausgabestand, in dem zuletzt die Konfiguration geändert wurde. Beim Status "NOT ACCEPTED" werden weitere Informationen zur Problemursache angezeigt.
  Wenn ein PLUG als PRESET-PLUG konfiguriert wurde, wird dies hier als Zusatzinformation in der ersten Zeile angezeigt. Nähere Informationen zur Erstellung und Benutzung eines PRESET-PLUG finden Sie in Kapitel "Instandhalten und Warten (Seite 366)".

- **Firmware auf PLUG**
  Wenn aktiviert, wird die Firmware auf dem PLUG abgespeichert. Damit können mit dem PLUG automatische Firmware-Updates/Downgrades durchgeführt werden. In dem Feld "Info" wird angezeigt, ob die Firmware auf dem PLUG gespeichert ist oder nicht. Weitere Informationen dazu finden Sie in Kapitel "Configuration License PLUG (CLP) (Seite 25)".
- **PLUG ändern**
  Wählen Sie aus der Klappliste die gewünschte Einstellung aus. Sie haben folgende Möglichkeiten, um die Konfiguration auf dem PLUG zu ändern:
  - Aktuelle Konfiguration auf den PLUG schreiben
    Diese Option ist nur verfügbar, wenn der Status des PLUG "NOT ACCEPTED" oder "FACTORY" ist.
    Die im internen Flash-Speicher des Gerätes vorhandene Konfiguration wird auf den PLUG kopiert.
  - PLUG auf Werkseinstellungen zurücksetzen
    Löscht alle Daten vom PLUG und führt eine Low-Level-Formatierung durch.

Vorgehensweise

Voraussetzung:

- Benutzer mit Administratorrechten

Konfiguration des PLUG ändern

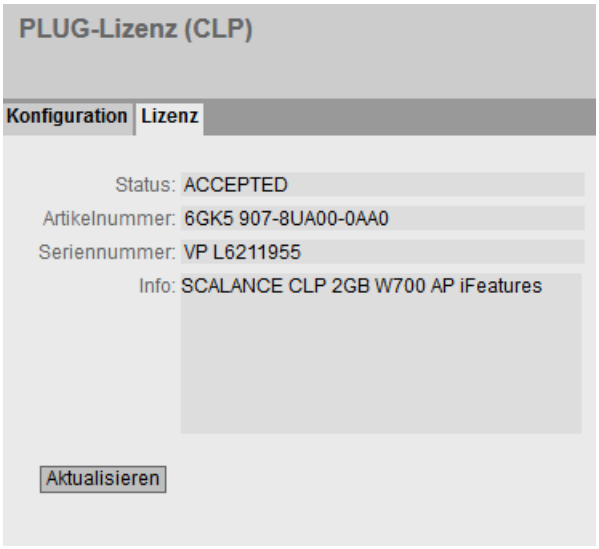
1. Wählen Sie aus der Klappliste "PLUG ändern" die gewünschte Option aus.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.5.18.2 Lizenz

ACHTUNG
Den 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, startet das Gerät neu. War in dem Gerät ein gültiger PLUG-Lizenz gesteckt, wird das Gerät nach dem Neustart in einen definierten Fehlerzustand versetzt. Bei SCALANCE W werden in diesem Fall die verfügbaren Funkschnittstellen deaktiviert. Wenn das Gerät einmal mit einem PLUG-Lizenz konfiguriert wurde, kann das Gerät ohne diesen PLUG nicht mehr genutzt werden. Um das Gerät wieder nutzen zu können, setzen Sie das Gerät auf Werkseinstellungen zurück.

Informationen über die Lizenz des PLUG

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



Beschreibung der angezeigten Felder

- **Status**
  Zeigt den Status der PLUG-Lizenz an. Es gibt die folgenden Möglichkeiten:
  - ACCEPTED
    Der im Gerät vorhandene PLUG enthält eine passende und gültige Lizenz.
  - NOT ACCEPTED
    Die Lizenz des gesteckten PLUG ist nicht gültig
  - NOT PRESENT
    Im Gerät ist kein PLUG gesteckt.
  - MISSING
    Es ist kein PLUG gesteckt. Im Gerät sind Funktionen konfiguriert, für die eine Lizenz erforderlich ist.
  - WRONG
    Der gesteckte PLUG passt nicht zum Gerät.
  - UNKNOWN
    Unbekannter Inhalt der PLUG-Lizenz.
  - DEFECTIVE
    Der Inhalt der PLUG-Lizenz ist fehlerhaft.
- **Artikelnummer**
  Zeigt die Artikelnummer des PLUG an. Es gibt den PLUG für unterschiedliche Funktionserweiterungen und für verschiedene Zielsysteme.

- **Seriennummer**
  Zeigt die Seriennummer des PLUG.
- **Info**
  Zeigt zusätzliche Informationen über den PLUG an.

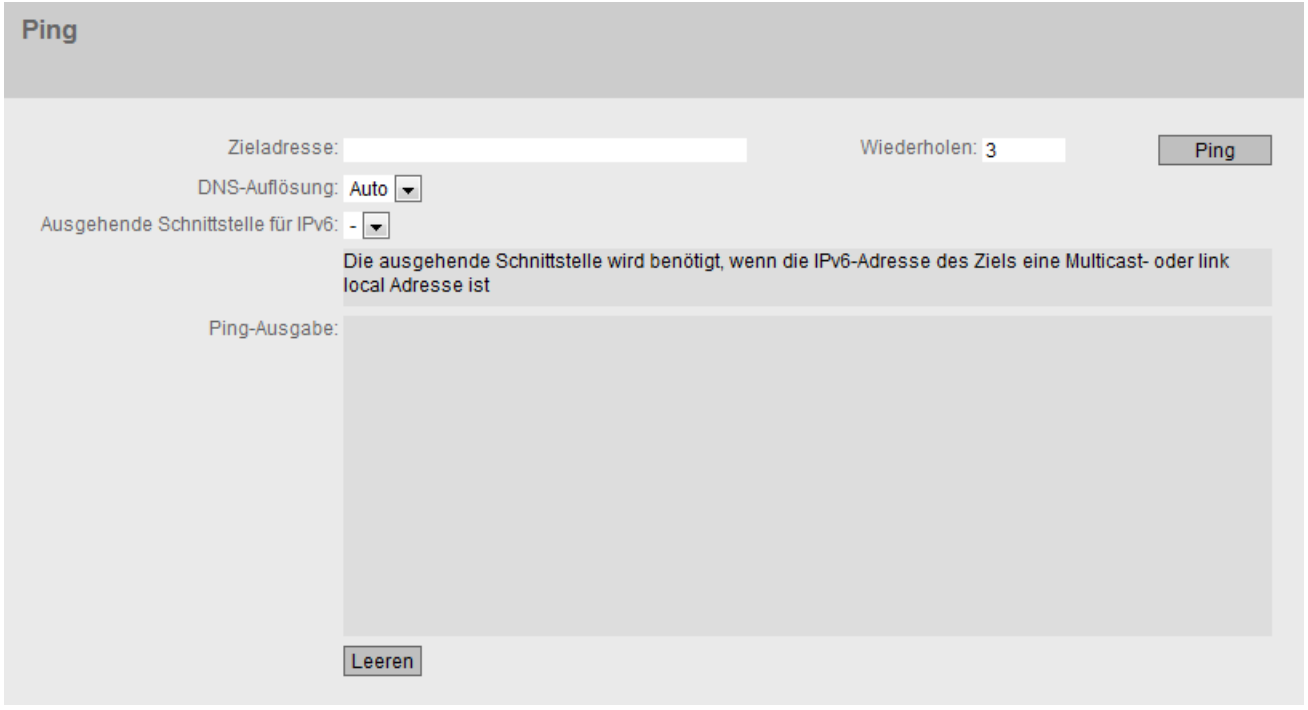
Hinweis

Beim Speichern der Konfiguration wird die Information mitgespeichert, ob zu diesem Zeitpunkt ein PLUG im Gerät gesteckt war. Diese Konfiguration ist dann auch nur lauffähig, wenn ein PLUG mit der gleichen Artikelnummer / Lizenz gesteckt ist. Das ist unabhängig davon, ob z. B. iFeatures konfiguriert sind.

6.5.19 Ping

Erreichbarkeit einer Adresse in einem IP-Netzwerk

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



Beschreibung

Die Seite enthält folgende Felder:

- **Zieladresse**
  Geben Sie die IPv4-, IPv6-Adresse oder den FQDN (Fully Qualified Domain Name) des Geräts ein.
- **Wiederholen**
  Tragen Sie die Anzahl der Ping-Anforderungen ein.
- **DNS-Auflösung**
  Wählen Sie aus in welchen IP-Adress-Typ ein eingegebener FQDN aufgelöst werden soll.
  - Auto
    In diesem Modus wird der IP-Adress-Typ automatisch gewählt.
  - IPv4
    Der eingegebene FQDN wird in einer IPv4-Adresse aufgelöst.
  - IPv6
    Der eingegebene FQDN wird in einer IPv6-Adresse aufgelöst.
- **Ausgehende Schnittstelle für IPv6**
  Diese Auswahl wird nur benötigt, wenn die Zieladresse eine Multicast- oder eine Link-lokale Adresse ist.
  - "-" (Werkseinstellung)
  - Wählen Sie die entsprechende IPv6-Schnittstelle aus.
- **Ping**
  Klicken Sie diese Schaltfläche, um die Ping-Funktion zu starten.
- **Ping-Ausgabe**
  Dieses Feld zeigt die Ausgabe der Ping-Funktion an.
- **Leeren**
  Klicken Sie diese Schaltfläche, um die Ping-Ausgabe zu leeren.

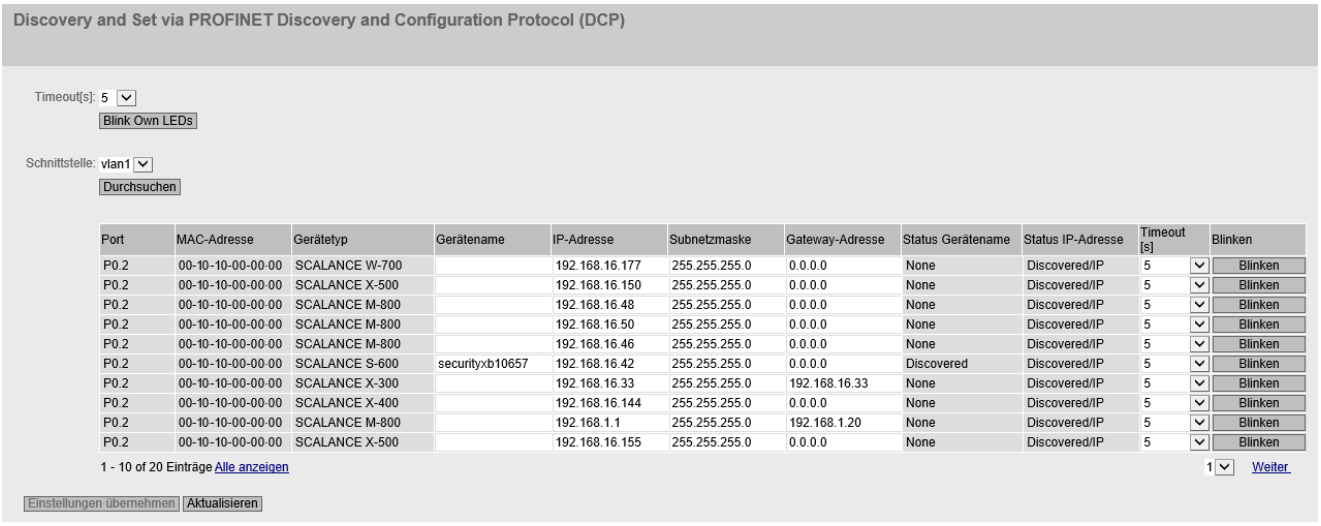
6.5.20 DCP Discovery

Auf dieser Seite können Sie eine Schnittstelle auswählen und nach den Geräten suchen, die über die Schnittstelle erreichbar sind und DCP unterstützen. DCP Discovery sucht nur nach Geräten, die im gleichen Subnetz liegen wie die Schnittstelle. Die erreichbaren Geräte werden in einer Tabelle aufgelistet. In der Tabelle können Sie die Netzwerkparameter der Geräte überprüfen und anpassen. Zum Identifizieren und zum Konfigurieren der Geräte wird das Discovery Configuration Protocol (DCP) verwendet.

Hinweis

DCP Discovery

Die Funktion ist nur in dem mit der TIA-Schnittstelle assoziierten VLAN verfügbar. Die TIA-Schnittstelle konfigurieren Sie unter "Layer 3 > Subnetze > Konfiguration".



Voraussetzung:

Um die Netzwerkparameter anzupassen, benötigt DCP Schreibrechte auf dem Gerät. Wenn der Zugriff schreibgeschützt ist, sind die Netzwerkparameter nicht konfigurierbar.

Auf den SCALANCE Geräten konfigurieren Sie den Zugriff unter "System > Konfiguration".

Beschreibung

Die Seite enthält folgende Felder:

- **Timeout[s]**
  Legen Sie die Zeitdauer für das Blinken fest. Wenn die Zeit abgelaufen ist, wird das Blinken beendet.
- **Blinken der eigenen LEDs aktivieren**
  Lässt die LEDs des eigenen Geräts blinken.
- **Schnittstelle**
  Wählen Sie die gewünschte Schnittstelle aus.
- **Durchsuchen**
  Startet die Suche nach Geräten, die über die gewählte Schnittstelle erreichbar sind.
  Nach dem Abschluss der Suche werden die erreichbaren Geräte in der Tabelle aufgelistet. Die Tabelle ist auf 100 Einträge begrenzt.

Die Tabelle gliedert sich in folgende Spalten:

- **Port**
  Zeigt den Port an, über den das Gerät erreichbar ist.
- **MAC-Adresse**
  Zeigt die MAC-Adresse des Geräts an.
- **Gerätetyp**
  Zeigt an, zu welcher Produktlinie bzw. Produktgruppe das Gerät gehört.

- **Gerätename**
  Passen Sie bei Bedarf den PROFINET-Gerätenamen an.
  Der Gerätename muss DNS-konform sein. Wenn der Gerätename nicht verwendet wird, ist das Feld leer
- **IP-Adresse**
  Passen Sie bei Bedarf die IPv4-Adresse des Geräts an.
  Die IPv4-Adresse sollte innerhalb Ihres Netzwerks eindeutig sein und zum Netzwerk passen.
  Die IPv4-Adresse 0.0.0.0 bedeutet, dass noch keine IPv4-Adresse eingestellt ist.
- **Subnetzmaske**
  Passen Sie bei Bedarf die Subnetzmaske des Geräts an.
- **Gateway-Adresse**
  Passen Sie bei Bedarf die IPv4-Adresse des Gateways an.
- **Status Gerätename**
  - None: Der Gerätename wird nicht verwendet.
  - Discovered: Der eingestellte Gerätename wird verwendet.
  - Configured: Dem Gerät wurde ein neuer Gerätename zugewiesen.
- **Status IP-Adress**
  - Discovered/IP: Das Gerät verwendet eine statische IPv4-Adresse.
  - Discovered/DHCP: Das Gerät hat die IPv4-Adresse von einem DHCP-Server bezogen.
  - Configured: Dem Gerät wurde eine neue IPv4-Adresse zugewiesen.
- **Timeout[s]**
  Legen Sie die Zeitdauer für das Blinken fest. Wenn die Zeit abgelaufen ist, wird das Blinken beendet.
- **Blinken**
  Lässt die LEDs des ausgewählten Geräts blinken.

Vorgehensweise

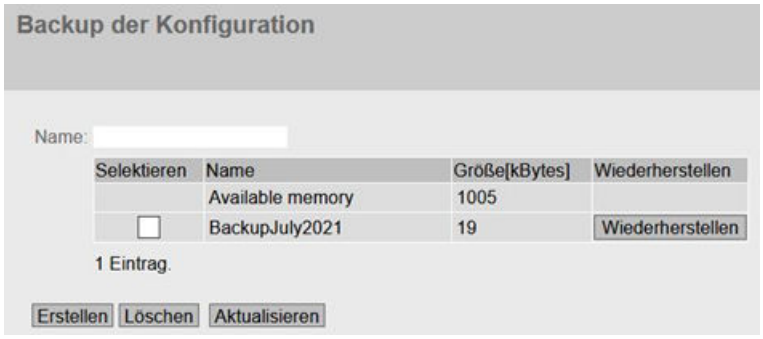
1. Wählen Sie die TIA-Schnittstelle aus.
2. Um alle Geräte anzuzeigen, die über die TIA-Schnittstelle erreichbar sind, klicken Sie auf die Schaltfläche "Durchsuchen".
3. Passen Sie die gewünschten Eigenschaften an.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
   Der Status der geänderten Eigenschaften ändert sich in "Configured".
5. Um sicherzustellen, dass die Eigenschaften korrekt übernommen wurden, klicken Sie erneut auf die Schaltfläche "Durchsuchen".
   Der Status der geänderten Eigenschaften ändert sich in "Discovered".

6.5.21 Backup der Konfiguration

Backup

Auf dieser Seite können Sie Backups der Konfiguration erstellen. Die maximale Anzahl hängt von der Größe der Backups und vom verfügbaren Speicherplatz ab.

Die erstellten Backups werden unter dem Dateityp "ConfigPackBackup" gespeichert. Auf der Seite "System > Laden & Speichern > HTTP/TFTP/SFTP" können Sie Konfigurationsbackups im ZIP-Format auf Ihrem Client-PC speichern bzw. von dort laden.



Beschreibung

Die Seite enthält folgende Felder:

- **Name**
  Geben Sie einen Namen für das Backup ein.

Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Name**
  Zeigt den Namen des Backups an.
- **Größe[kBytes]**
  Die erste Zeile "Available memory" zeigt an, wie viel Speicherplatz für Backups auf dem Gerät verfügbar ist. Wenn Sie ein Backup erstellen, verringert sich der verfügbare Speicherplatz entsprechend.
  In den weiteren Zeilen wird jeweils die Größe des Backups angezeigt.
- **Wiederherstellen**
  Klicken Sie auf die Schaltfläche "Wiederherstellen", um das entsprechende Backup wieder auf das Gerät zu laden.

Vorgehensweise

1. Geben Sie den gewünschten Namen ein.
2. Klicken Sie auf die Schaltfläche "Erstellen".
   Die aktuelle Konfiguration wird als Konfigurationsbackup gespeichert.
   Das Speichern des Backups kann einige Zeit in Anspruch nehmen. Für das Backup wird eine neue Zeile angelegt. Die Größe des Backups wird angezeigt und von dem verfügbaren Speicherplatz abgezogen.

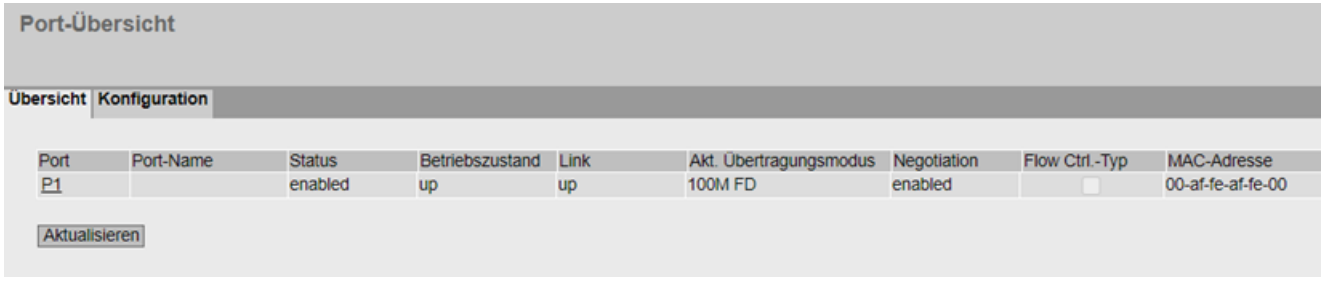
6.6 Menü "Schnittstellen"

6.6.1 Ethernet

6.6.1.1 Übersicht

Portkonfiguration im Überblick

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:

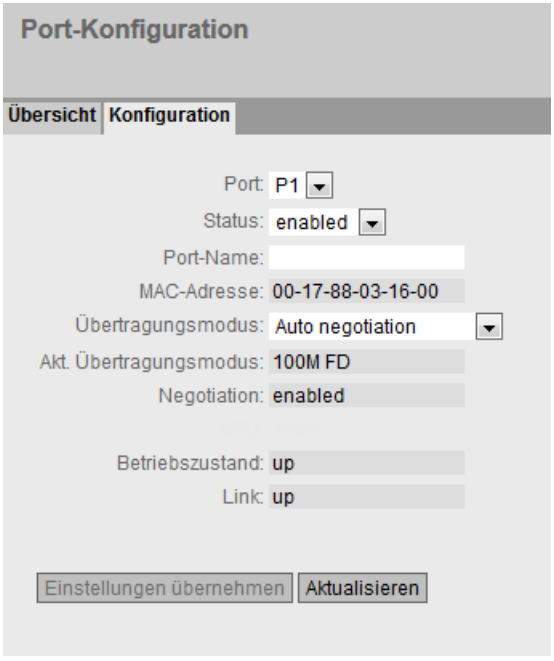
- **Port**
  Zeigt die konfigurierbaren Ports an. Wenn Sie auf den Link klicken, wird die entsprechende Konfigurationsseite geöffnet.
- **Port-Name**
  Zeigt den Namen des Ports.
- **Status**
  Zeigt an, ob der Port ein- oder ausgeschaltet ist. Datenverkehr ist nur über einen eingeschalteten Port möglich.

- **Betriebszustand**
  Zeigt den aktuellen Betriebszustand an. Der Betriebszustand ist vom konfigurierten "Status" und dem "Link" abhängig. Es gibt folgende Möglichkeiten:
  - up
    Sie haben für den Port den Status "enabled" konfiguriert und der Port hat eine gültige Verbindung zum Netzwerk.
  - down
    Sie haben für den Port den Status "disabled" oder "Link down" konfiguriert oder der Port hat keine Verbindung.
- **Link**
  Zeigt den Verbindungsstatus zum Netzwerk am. Beim Verbindungsstatus ist Folgendes möglich:
  - up
    Der Port hat eine gültige Verbindung zum Netzwerk, es wird ein "Link Integrity Signal" empfangen.
  - down
    Die Verbindung ist unterbrochen, weil beispielsweise das angeschlossene Gerät ausgeschaltet ist.
- **Akt. Übertragungsparameter**
  Zeigt die Übertragungsparameter des Ports an.
- **Negotiation**
  Zeigt an, ob die automatische Konfiguration aktiviert oder deaktiviert ist.
- **MAC-Adresse**
  Zeigt die MAC-Adresse des Ports an.

6.6.1.2 Konfiguration

Ports konfigurieren

Mit dieser Seite konfigurieren Sie die Ethernet-Ports des Geräts.



Beschreibung

Die Tabelle gliedert sich in folgende Zeilen:

- **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.
- **Port-Name**
  Tragen Sie hier einen Namen für den Port ein.
- **MAC-Adresse**
  Zeigt die MAC-Adresse des Ports an.

- **Übertragungsmodus**
  Wählen Sie aus dieser Klappliste die Übertragungsgeschwindigkeit und das Übertragungsverfahren des Ports. Die Übertragungsgeschwindigkeit kann 10 Mbit/s, 100 Mbit/ oder 1000 Mbit/s betragen. Als Übertragungsverfahren können Vollduplex (FD) oder Halbduplex (HD) konfiguriert werden. Wenn Sie die Betriebsart auf "Auto negotiation" stellen, werden diese Parameter automatisch mit dem angeschlossenen Endgerät 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.

  Hinweis

  Wenn für die Übertragungsgeschwindigkeit 10 Mbit/s oder für das Übertragungsverfahren Halbduplex (HD) konfiguriert ist, kann das zu Beeinträchtigungen der PROFINET-Kommunikation führen. Wählen Sie immer mindestens 100 Mbit/s und Vollduplex (FD) bzw. "Auto negotiation", wenn das Gerät PROFINET-Kommunikation durchführen soll.

- **Akt. Übertragungsmodus**
  Zeigt die Übertragungsgeschwindigkeit und das Übertragungsverfahren des Ports an.
- **Negotiation**
  Zeigt an, ob die automatische Anschlusskonfiguration zum Partner-Port aktiviert oder deaktiviert ist.
- **Betriebszustand**
  Zeigt den aktuellen Betriebszustand an. Der Betriebszustand ist vom konfigurierten "Status" und dem "Link" abhängig. Es gibt folgende Möglichkeiten:
  - up
    Sie haben für den Port den Status "enabled" konfiguriert und der Port hat eine gültige Verbindung zum Netzwerk.
  - down
    Sie haben für den Port den Status "disabled" oder "Link down" konfiguriert oder der Port hat keine Verbindung.
- **Link**
  Zeigt den Verbindungsstatus zum Netzwerk an. Es gibt folgende Möglichkeiten:
  - 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.

Vorgehensweise

Hinweis

Veränderung der Port-Konfiguration

Das Gerät verhindert oder reduziert bei Überlastung eines Ports durch verschiedene Automatismen die Rückwirkung auf andere Ports und Prioritätsklassen (Class of Service). Dies kann auch bei aktivierter Flusskontrolle dazu führen, dass Telegramme verworfen werden.

Port-Überlastungen treten auf, wenn das Gerät mehr Telegramme empfängt, als es senden kann, z.B. infolge unterschiedlicher Übertragungsgeschwindigkeiten.

Um die Konfiguration eines Ports zu ändern, gehen folgendermaßen vor:

1. Klicken Sie in das entsprechende Feld, um die Konfiguration zu ändern.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.6.2 WLAN

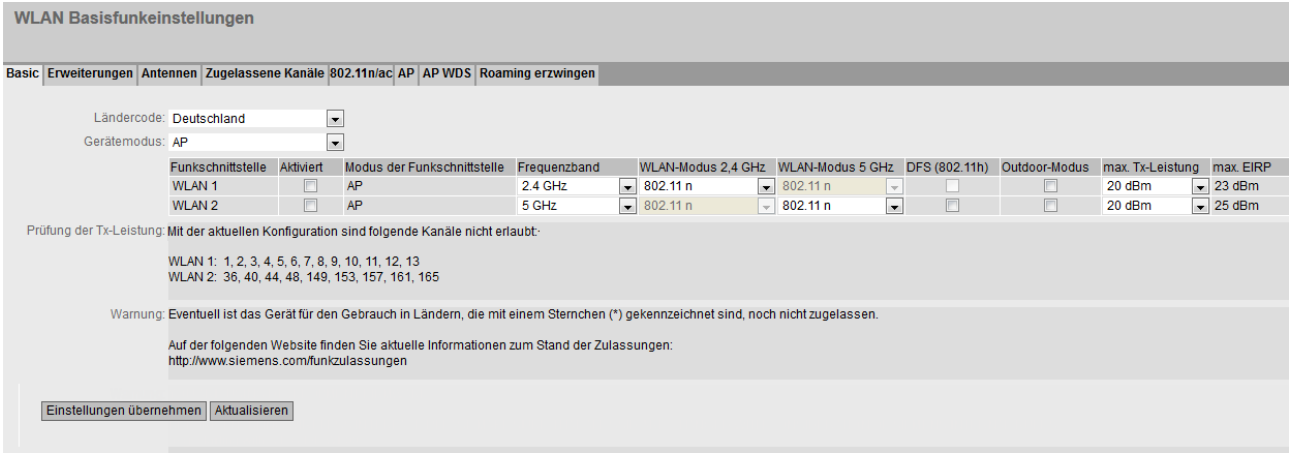
6.6.2.1 Basic

Grundeinstellungen

Auf dieser Seite nehmen Sie einige grundlegende Einstellungen für das Gerät vor, z. B. die Ländereinstellung und die Festlegung der Betriebsart.

Hinweis

Um die WLAN-Schnittstelle zu konfigurieren, müssen Sie immer zuerst den Ländercode festlegen. Einige Parameter sind abhängig von der Ländereinstellung, z. B. der Übertragungsstandard.



Beschreibung

- **Ländercode**
  Wählen Sie aus der Klappliste das Land aus, in dem das Gerät eingesetzt wird.
  Sie brauchen die landesspezifischen Daten nicht zu kennen, die richtige Kanaleinteilung und Festlegung der Sendeleistung erfolgt entsprechend Ihrer Länderauswahl durch das Gerät.
  Informationen zu den aktuell vorliegenden Länderzulassungen finden Sie in der Dokumentation "Zulassungen SCALANCE W1700 802.11ac (https://support.industry.siemens.com/cs/de/de/view/109759610)".

  Hinweis

  Ländereinstellung

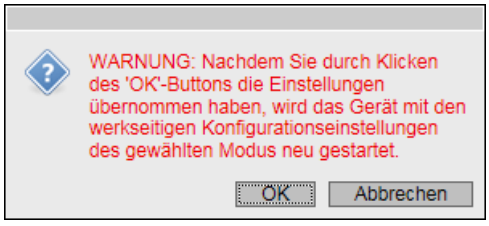
  Die richtige Ländereinstellung ist für einen zulassungskonformen Betrieb unbedingt notwendig. Die Auswahl eines vom Anwenderland abweichenden Landes kann strafrechtlich geahndet werden.

- **Gerätemodus**
  Wählen Sie die Betriebsart des Geräts aus. Diese Auswahl steht nur bei Access Points zur Verfügung.
  Folgende Betriebsarten sind möglich:
  - AP - Access Point-Modus
  - Client - Client-Modus

  Hinweis

  Nach dem Ändern der Betriebsart, wird eine Meldung eingeblendet. Wenn Sie die Meldung mit "OK" bestätigen, startet das Gerät mit den werkseitigen Konfigurationseinstellungen in der geänderten Betriebsart neu.

  Wenn das Gerät neu gestartet ist, müssen Sie sich erneut anmelden, um die Konfiguration fortsetzen zu können.



Die Tabelle gliedert sich in folgende Spalten:

- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen an.
- **Aktiviert**
  Status der WLAN-Schnittstelle. Um die WLAN-Schnittstelle zu aktivieren, markieren Sie das Optionskästchen.

  Hinweis

  WLAN-Schnittstelle aktivieren

  Die WLAN-Schnittstellen sind im Auslieferungszustand deaktiviert. Die WLAN-Schnittstellen sind aktivierbar, nachdem die Länder- und die Antenneneinstellungen konfiguriert sind.

- **Modus der Funkschnittstelle**
  Zeigt die Betriebsart der WLAN-Schnittstelle an.
- **Frequenzband**
  Legen Sie das Frequenzband fest.
  - 2.4 GHz
  - 5 GHz
- **WLAN-Modus 2.4 GHz / WLAN-Modus 5 GHz**
  Wählen Sie für das projektierte Frequenzband den gewünschten Übertragungsstandard aus. Die Auswahl ist abhängig von der Ländereinstellung.
  - 802.11g
    Der Übertragungsstandard IEEE 802.11g (2.4 GHz) ist eingestellt. Dieser Übertragungsstandard ist abwärts kompatibel zu IEEE 802.11b.
  - 802.11n
    Der Übertragungsstandard IEEE 802.11n (2.4 GHz und 5 GHz) ist eingestellt. Dieser Übertragungsstandard ist abwärts kompatibel zu IEEE802.11a und IEEE 802.11g.
  - 802.11a
    Der Übertragungsstandard IEEE 802.11a (5 GHz) ist eingestellt.
  - 802.11ac
    Der Übertragungsstandard IEEE 802.11ac (5 GHz) ist eingestellt.

  Hinweis

  Datenrate

  Die Datenrate wird automatisch angepasst.

- **DFS (802.11h)**
  Aktiviert oder deaktiviert die Funktion "Dynamic Frequency Selection (DFS)".

  – Aktiviert
  Mit der Funktion DFS ist es möglich, auch die oberen 5-GHz-Kanäle zu verwenden. Diese Kanäle sind länderspezifisch und unterliegen bestimmten DFS-Vorgaben. Weiterführende Informationen dazu finden Sie in der länderspezifischen DFS-Dokumentation.
  Bevor der Access Point über einen dieser Kanäle sendet, prüft er 60 Sekunden gemäß CAC (Channel Availability Check) nach konkurrierenden Radarsignalen. Innerhalb der Suchdauer sendet der Access Point auch keine Beacons. Bei Wetter-Radar-Kanälen (5,6 - 5,65 GHz) beträgt die Suchdauer 10 Minuten.
  Wenn nach Ablauf der Suchdauer keine Radarsignale gefunden wurden, sendet der Access Point auf dem Kanal. Sonst wechselt der Access Point den Kanal und wiederholt die Prüfung.
  Auch während des Betriebs sucht der Access Point ständig nach Radarsignalen.
  Wenn der Access Point auf dem aktuellen Kanal ein Radarsignal entdeckt, kündigt er den Kanalwechsel den Clients an. Danach wechselt er automatisch auf einen alternativen DFS-Kanal und der aktuelle Kanal wird für 30 Minuten gesperrt.

  Hinweis

  Kanalbandbreite 160 MHz nutzen

  Nur wenn DFS aktiviert ist, sind für den Betrieb von 160 MHz genügend Kanäle verfügbar.

  Deaktiviert
  Die Funktion DFS wird nicht verwendet.

- **Outdoor-Modus**

  – Aktiviert
  Wenn Sie den Outdoor-Modus aktiviert haben, stehen Ihnen nur die Kanäle zur Verfügung, die für den Outdoor-Betrieb zugelassen sind.

  – Deaktiviert
  Wenn Sie den Outdoor-Modus deaktiviert haben, stehen Ihnen nur die Kanäle zur Verfügung, die für den Betrieb in einem Gebäude zugelassen sind.

- **max. Tx-Leistung**
  Legen Sie die maximal mögliche Sendeleistung des Geräts fest.
  Wenn die Sendeleistung zu hoch eingestellt ist, kann das empfangene Signal beim Client übersteuert sein. Kontrollieren Sie beim Client die Empfangssignalstärke (dBm).
  Abhängig von den verwendeten Antennen kann eine Verminderung der Sendeleistung notwendig werden, um die gesetzlich vorgeschriebene maximale Sendeleistung nicht zu überschreiten. Eine Verminderung der Sendeleistung bewirkt eine gezielte Reduktion der Zellengröße.

  Hinweis

  Je nach Kanal und Datenrate variiert die maximal mögliche Sendeleistung. Beachten Sie für weitere Informationen zur Sendeleistung die Dokumentation "Leistungsdaten 801.11ac SCALANCE W1700 (https://support.industry.siemens.com/cs/de/de/view/109759606)".

  Hinweis

  Werden beim Access Point beide Schnittstellen im gleichen Frequenzbereich betrieben, kann es bei einer Sendeleistung größer 15 dBm zu Funkstörungen an einer bzw. an beiden Schnittstellen kommen.

- **max. EIRP (Effective Isotropic Radiated Power)**
  Zeigt die aktuelle Strahlungsleistung der Antenne an, bezogen auf eine ungerichtete Antenne (isotrop). Produkt aus Antennengewinn, Anzahl der Antennenanschlüsse, Kabellänge, Zusätzliche Dämpfung und eingestellter Tx-Leistung.
- **Prüfung der Tx-Leistung**
  Zeigt an, ob mit den vorgenommenen Einstellungen die zulässigen Sendeleistungsbeschränkungen des eingestellten Landes verletzt werden. Der errechnete Wert von "max. EIRP" wird geprüft, ob dieser Wert die Sendeleistungsbeschränkung auf bestimmten Kanälen in dem eingestellten Land verletzt. Wenn "Nur zugelassene Kanäle verwenden" eingestellt ist, werden auch nur die dort gewählten Kanäle geprüft.
  - -
    Die Kanäle können mit den aktuellen Einstellungen benutzt werden.
  - Kanalnummern
    Gibt an, bei welchen Kanälen, die aktuelle Sendeleistung die maximal erlaubte Sendeleistung überschreitet.

Vorgehensweise

1. Um die WLAN-Schnittstelle zu projektieren, müssen Sie immer zuerst das Land festlegen. Wählen Sie aus der Klappliste "Ländercode" das Land aus, in dem das Gerät eingesetzt wird.
2. Wählen Sie aus der Klappliste "Frequenzband" das gewünschte Frequenzband aus.
3. Wählen Sie aus der Klappliste "WLAN-Modus" den gewünschten Übertragungsstandard für das projektierte Frequenzband.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

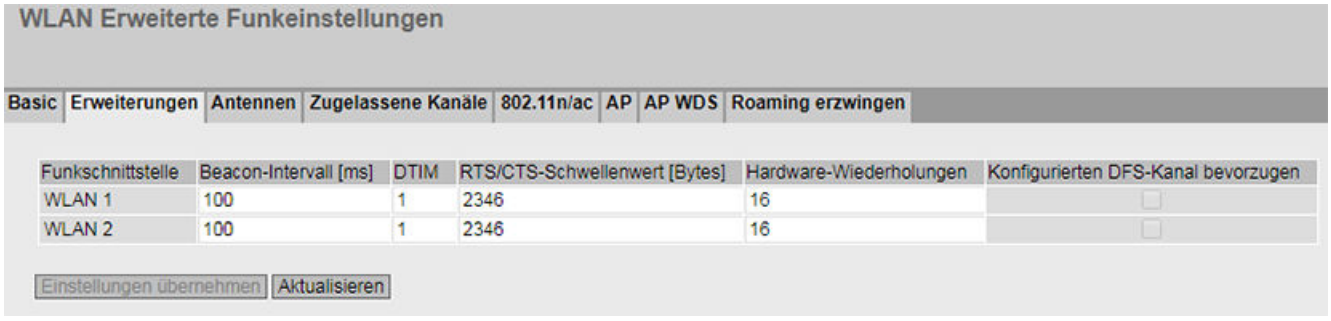
Siehe auch

Funkzulassungen (https://www.siemens.com/funkzulassungen)

6.6.2.2 Erweiterungen

Weitere Einstellungsmöglichkeiten

Auf dieser Seite können Sie Details des Sendeverhaltens festlegen. Sie müssen die Parameter dieser Seite nur anpassen, wenn das SCALANCE W1700-Gerät mit den Standardeinstellungen nicht in der vorgesehenen Art und Weise genutzt werden kann.



Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen in dieser Spalte an.
- **Beacon-Intervall [ms] (nur im Access Point-Modus)**
  Legen Sie das Intervall (40 - 1000 ms) fest, mit dem der Access Point Beacons sendet. Beacons sind zyklisch versendete Pakete, mit denen ein Access Point die Clients über seine Existenz informiert.

  Hinweis

  Intervall bei mehr als 2 VAP-Schnittstellen

  Verwenden Sie bei mehr als 2 VAP-Schnittstellen ein Intervall, das größer gleich 100 ms ist.

- **DTIM (nur im Access Point-Modus)**
  Das DTIM-Intervall (1-15) legt die Anzahl der Beacons fest, die versendet werden, bevor, nach dessen Ablauf der Access Point die gesammelten Pakete (Broadcast, Unicast, Multicast) an den Client sendet.
  - Wenn Sie in dieses Feld eine "1" eintragen, überträgt der Access Point Broadcast-, Unicast- und Multicast-Pakete direkt nach jedem Beacon (empfohlene Einstellung für normale Netzwerkumgebungen).
  - Wenn Sie in dieses Feld eine "5" eintragen, sammelt der Access Point die Pakete und sendet diese nach jedem fünften Beacon.

  Ein Vergrößern dieses Werts erlaubt den verbundenen Clients einen längeren Sleep-Modus auf Kosten einer höheren Verzögerung bei Paketen.

- **RTS/CTS-Schwellenwert [Bytes]**
  RTS/CTS (Request To Send/Clear To Send) ist ein Verfahren zur Kollisionsvermeidung. Das Verfahren beruht auf dem Austausch von Statusinformationen vor dem Senden der eigentlichen Daten (Hidden node problem). Um die Netzbelastung durch den zusätzlichen Protokollverkehr zu minimieren, wird dieses Verfahren erst ab einer bestimmten Paketgröße angewendet. Die Paketgröße legen Sie mit dem Parameter "RTS/CTS-Schwellenwert" fest.
- **Hardware-Wiederholungen (nur im Access Point-Modus)**
  Legen Sie die Anzahl der Hardware-Wiederholungen fest.
  Es werden keine Hardware-Wiederholungen >30 empfohlen.
  Die Hardware-Wiederholung wird vom WLAN-Chip selbst durchgeführt, indem er versucht, ein nicht quittiertes Paket sofort zu wiederholen.
  Waren alle Hardware-Wiederholungen erfolglos, wird das Paket gelöscht und der WLAN-Client aus der Liste entfernt.
- **Konfigurierten DFS-Kanal bevorzugen (nur im Access Point-Modus)**
  - Aktiviert
    Diese Funktion ist nur verfügbar, wenn Sie auf der Seite "Basic" die Funktion "DFS" aktiviert haben.
    Wenn der konfigurierte Kanal einer WLAN-Schnittstelle durch Radarerkennung gesperrt wurde und nach 30 Minuten wieder freigegeben wird, wechselt der Access Point automatisch wieder zu dem konfigurierten Kanal.
    Bevor der Access Point die Kommunikation auf dem konfigurierten Kanal startet, sucht er 60 Sekunden nach Primärnutzern auf dem Kanal. In dieser Zeit sendet der Access Point keine Beacons. Wenn Signale auf dem Kanal entdeckt werden, wechselt der Access Point den Kanal und wiederholt die Prüfung. Erst wenn nach Ablauf der 60 Sekunden keine Signale von Primärnutzern erkannt wurden, sendet der Access Point auf dem Kanal.
    Wenn Sie auf der Seite "Schnittstellen > WLAN > AP" für den Kanal "Auto" konfiguriert haben, hat das Gerät keinen konfigurierten Kanal, zu dem es zurückwechseln kann.
  - Deaktiviert
    Die Funktion wird nicht verwendet.

Vorgehensweise

1. Tragen Sie in die Eingabefelder die einzustellenden Werte ein.
2. Aktivieren Sie die Optionshäkchen der gewünschten Funktionen.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.6.2.3 Antennen

Überblick

Die folgenden Bilder geben einen Überblick über die IWLAN-Antennen, die für den Einsatz mit SCALANCE W-Geräten geeignet sind.

Antennenart	Frequenz (GHz)	Antennen		SCALANCE W780/W740	SCALANCE W760/W720, W770/W730	SCALANCE W770/W730 IP65	SCALANCE W1780/W1740	SCALANCE WAM766-1/ WUM766-1
gerichtet	2,4		ANT792-8DN	●			●	●
	5		ANT793-8DP	●	●	●	●*	●
			ANT793-8DJ	●	●	●	●*	●
			ANT793-8DK	●	●	●	●*	●
			ANT793-8DL	●	●	●	●*	●
RCoax	2,4		RCoax Leckwellen-leiter 2,4 GHz	●	●	●	●	●
			ANT792-4DN	●	●	●	●	●
	5		RCoax Leckwellen-leiter 5 GHz	●	●	●	●	●
			ANT793-4MN	●	●	●	●	●

G_IK10_XX_30317

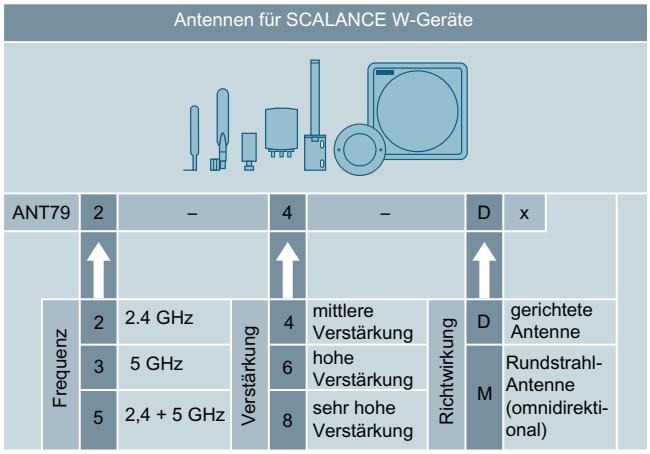
*Antennen nur an einem Antennenanschluss pro Funkschnittstelle des Geräts (R1A1 bzw. R2A1) verwenden und restliche Antennenanschlüsse mit Abschlusswiderstand versehen.

Antennenart	Frequenz (GHz)	Antennen		SCALANCE W780/W740	SCALANCE W760/W720, W770/W730	SCALANCE W770/W730 IP65	SCALANCE W1780/W1740	SCALANCE WAM766-1/ WUM766-1	
gerichtet	2,4		ANT792-8DN	●			●	●	
	5		ANT793-8DP	●	●	●	●*	●	
			ANT793-8DJ	●	●	●	●*	●	
			ANT793-8DK	●	●	●	●*	●	
			ANT793-8DL	●	●	●	●*	●	
RCoax	2,4		RCoax Leckwellen-leiter 2,4 GHz	●	●	●	●	●	
			ANT792-4DN	●	●	●	●	●	
	5		RCoax Leckwellen-leiter 5 GHz	●	●	●	●	●	
			ANT793-4MN	●	●	●	●	●	

G_IK10_XX_30317

*Antennen nur an einem Antennenanschluss pro Funkschnittstelle des Geräts (R1A1 bzw. R2A1) verwenden und restliche Antennenanschlüsse mit Abschlusswiderstand versehen.

Der Antennenname gibt Aufschluss über die Eigenschaften der in der IWLAN-Antennenübersicht dargestellten Antennen:



Antennen

Konfiguration von externen Antennen

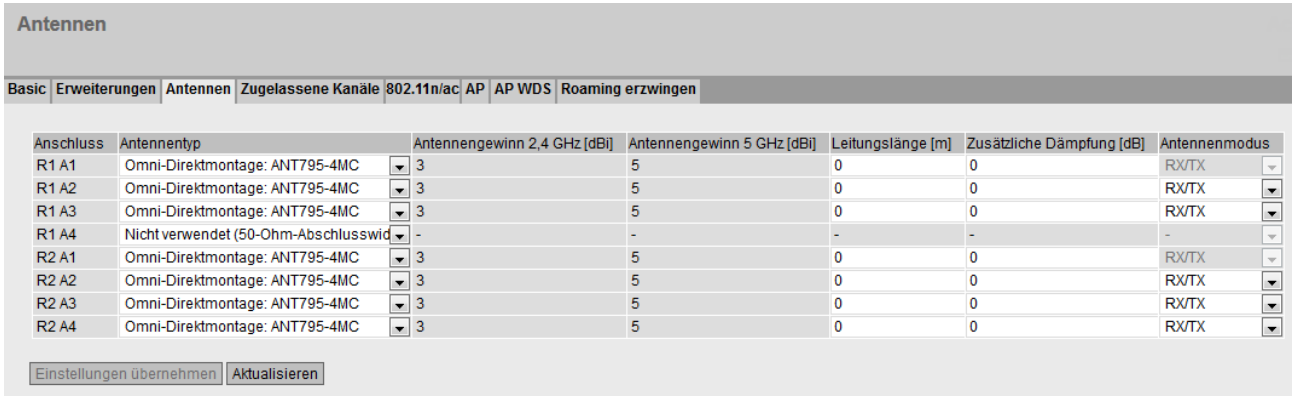
Auf dieser Seite konfigurieren Sie die Einstellungen für die angeschlossenen externen Antennen. Diese Einstellungen werden im Register "Schnittstellen > WLAN > Basic" für die Prüfung der Tx-Leistung verwendet, siehe "Basic (Seite 250)".

Hinweis

50 Ω-Abschlusswiderstand

Jede WLAN-Schnittstelle verfügt über vier Antennenanschlüsse. Ungenutzte Anschlüsse müssen mit einem 50 Ω-Abschlusswiderstand versehen werden.

An den Antennen-Anschlüssen R1 A1 und R2 A1 muss immer eine Antenne angeschlossen sein, sobald die WLAN-Schnittstelle eingeschaltet wird. Wenn keine Antenne angeschlossen ist, muss auch die entsprechende Schnittstelle für Rx und Tx deaktiviert sein. Andernfalls kann es zu Übertragungsstörungen kommen.



Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Anschluss**
  Zeigt die Bezeichnung des jeweiligen Antennenanschlusses an.

Hinweis

Kanalbandbreite 160 MHz

- Für Betrieb bei 160 MHz werden zwei Antennen verwendet
  - Spatial Stream 1: erste Antenne RxA1 + zweite Antenne RxA4

  Damit die Konfiguration beider Antennen gleich ist, werden die Einstellungen für die erste Antenne konfiguriert und für die zweite Antenne automatisch übernommen.
- Nach der Tabelle wird die Einstellung "Antennenkonfiguration für Kanalbandbreite 160 MHz" eingeblendet.
- Nur der Antennenmodus RX/TX ist erlaubt.

Antennen

Folgende Antennen unterstützen keinen Betrieb bei 160 MHz:

- ANT793-8DJ
- ANT793-8DK
- ANT793-8DP
- ANT793-8DL
- ANT793-8DQ

- **Antennentyp**
  Wählen Sie den Typ der externen Antenne aus, die an das Gerät angeschlossenen ist. Wenn der Typ ihrer externen Antenne nicht verfügbar ist, wählen Sie den Eintrag "Benutzerdefiniert".
  Wenn Sie einen Antennenanschluss mit einem 50 Ω-Abschlusswiderstand abschließen, wählen Sie den Eintrag " Nicht verwendet (50-Ohm-Abschlusswiderstand)".
- **Antennengewinn**
  Wenn Sie bei "Antennentyp" den Eintrag "Benutzerdefiniert" wählen, tragen Sie manuell den Antennengewinn in der Einheit "dBi" ein.
  - **Antennengewinn 2.4 GHz [dBi]**
    Tragen Sie hier den Antennengewinn ein, den die Antenne im Frequenzband 2.4 GHz hat.
  - **Antennengewinn 5 GHz [dBi]**
    Tragen Sie hier den Antennengewinn ein, den die Antenne im Frequenzband 5 GHz hat.
- **Leitungslänge [m]**
  Tragen Sie die Länge der flexiblen Antennen-Anschlussleitung in Metern ein, die zwischen dem Gerät und der externen Antenne verwendet wird.
  Für die Berechnung der aktuellen Strahlungsleistung wird die Dämpfung entsprechend der technischen Daten der flexiblen Verbindungsleitung berücksichtigt. Weitere Informationen finden Sie im Systemhandbuch "Passive Netzkomponenten (https://support.industry.siemens.com/cs/de/de/view/84922825)".
- **Zusätzliche Dämpfung [dB]**
  Tragen Sie hier die zusätzliche Dämpfung ein, die z. B. durch einen zusätzlichen Splitter verursacht wird.

- **Antennenmodus**
  Legen Sie die Verwendung der Antenne fest. Beim Antennenanschluss 1 (R1 A1 und R2 A1) ist der Eintrag nicht änderbar.

  – Tx
    Nur zum Senden

  – Rx
    Nur zum Empfangen

  – Rx/Tx
    Zum Empfangen und zum Senden

  Die folgende Tabelle zeigt, welche Kombinationen möglich sind:

R1 A1 **R2 A1**	**R1 A2** **R2 A2**	**R1 A3** **R2 A3**	**R1 A4** **R2 A4**
Rx/Tx	Rx/Tx	Rx/Tx	Rx/Tx
Rx/Tx	Rx/Tx	Rx/Tx	Rx
Rx/Tx	Rx/Tx	Rx	Rx
Rx/Tx	Rx	Rx	Rx
Rx/Tx	Rx/Tx	Rx/Tx	Tx
Rx/Tx	Rx/Tx	Tx	Tx
Rx/Tx	Tx	Tx	Tx
Rx/Tx	Rx/Tx	Rx/Tx	--[1)]
Rx/Tx	Rx/Tx	Rx	--[1)]
Rx/Tx	Rx	Rx	--[1)]
Rx/Tx	Rx/Tx	Tx	--[1)]
Rx/Tx	Tx	Tx	--[1)]
Rx/Tx	Rx/Tx	--[1)]	--[1)]
Rx/Tx	Tx	--[1)]	--[1)]
Rx/Tx	Rx	--[1)]	--[1)]
Rx/Tx	--[1)]	--[1)]	--[1)]

1) Antennentyp "Nicht verwendet (50-Ohm-Abschlusswiderstand)"

- **Antennenkonfiguration für Kanalbandbreite 160 MHz** (Nicht beim SCALANCE W1788-2IA M12)

  – Access Point-Modus (nicht konfigurierbar)
    Wenn an WLAN 1 oder WLAN 2 die Kanalbandbreite auf 160 MHz eingestellt ist, wird die Einstellung eingeblendet. Die Kanalbandbreite wird unter "Schnittstellen > WLAN > AP" konfiguriert.

  – Client-Modus (konfigurierbar)
    Wenn aktiviert, wird an der WLAN-Schnittstelle die Kanalbandbreite auf 160 MHz eingestellt. Vorausgesetzt DFS und IEEE 802.11ac sind aktiviert. Nur wenn DFS aktiviert ist, sind für den Betrieb von 160 MHz genügend Kanäle verfügbar.

Vorgehensweise

Um zwei Antennen zu konfigurieren, gehen Sie folgendermaßen vor:

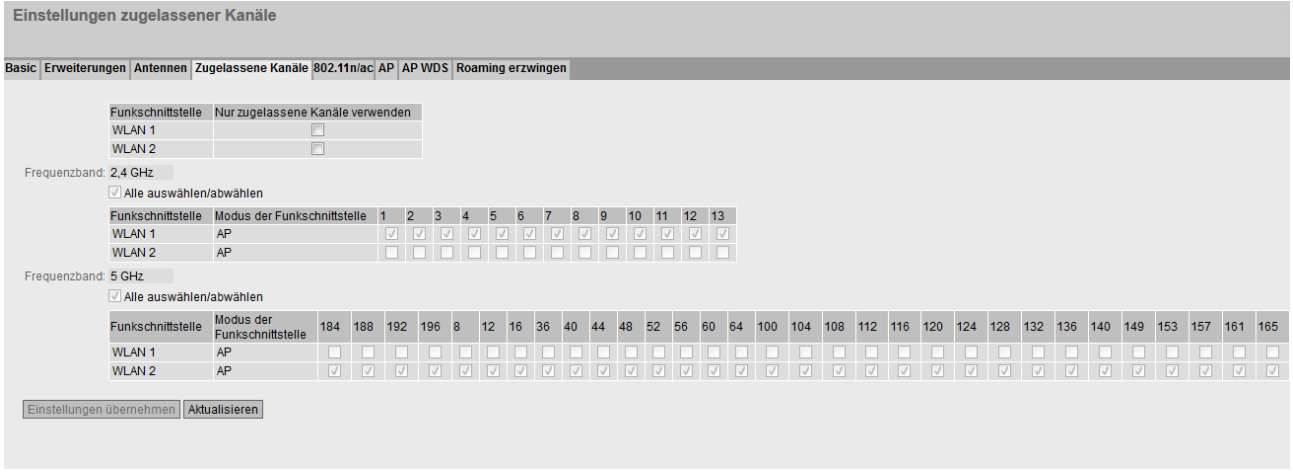
1. Wählen Sie beim ersten Antennenanschluss (R1 A1) aus der Klappliste "Antennentyp" den passenden Typ der Antenne.
2. Tragen Sie im Eingabefeld "Leitungslänge" die Länge der verwendeten Verbindungsleitung in Meter ein. Beim Antennenanschluss 1 (R1 A1 und R2 A1) ist der Eintrag "Antennenmodus" nicht änderbar.
3. Wählen Sie beim zweiten Antennenanschluss (R1 A2) aus der Klappliste "Antennentyp" den Eintrag "Nicht verwendet (50-Ohm-Abschlusswiderstand)".
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.6.2.4 Zugelassene Kanäle

Kanal-Einstellungen

Für die Kommunikation wird ein bestimmter Kanal innerhalb eines Frequenzbandes verwendet. Sie können diesen Kanal entweder fest vorgeben oder so konfigurieren, dass eine automatische Kanalauswahl erfolgt.

Auf der Seite legen Sie fest, welche Kanäle für die Kommunikation verwendet werden dürfen.



Beschreibung

Die Tabelle 1 enthält folgende Spalten:

- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen an.
- **Nur zugelassene Kanäle verwenden**
  Wenn Sie die Option aktivieren, schränken Sie damit die Auswahl an Kanälen ein, über die der AP die Verbindung aufbauen darf.
  In den folgenden Tabellen definieren Sie, welche Kanäle der AP zum Aufbau einer Funkzelle bei der Kanaleinstellung "Auto" nutzen darf.
  Die Tabellen sind nach den Frequenzbändern getrennt.
  Wenn die Option deaktiviert ist, werden die entsprechend den Einstellungen (Ländercode, Antennen, Sendeleistung etc.) verfügbaren Kanäle benutzt.

Über den Tabellen der Frequenzbänder befindet sich jeweils folgendes Optionskästchen:

- **Alle auswählen/abwählen**
  - Aktiviert
    Wenn Sie das Optionskästchen aktivieren, werden alle Kanäle markiert.
  - Deaktiviert
    Wenn Sie das Optionskästchen deaktivieren, bleibt der erste gültige Kanal des Frequenzbands aktiviert. Aktivieren Sie den gewünschten Kanal.

Die Tabellen der Frequenzbänder enthalten folgende Spalten:

- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen an.
- **Modus der Funkschnittstelle**
  Zeigt die Betriebsart an.
- **Kanalnummer**
  Um die gültigen Kanäle für das gewünschte Frequenzband festzulegen, aktivieren Sie bei der Kanalnummer das entsprechende Optionskästchen.
  In der Tabelle werden die zulässigen Kanäle des Landes angezeigt. Nur die gültigen Kanäle lassen sich aktivieren. Nicht gültige Kanäle sind gegraut und können nicht aktiviert werden.

Hinweis

Um die Kanäle festzulegen, muss die Einstellung "Nur zugelassene Kanäle verwenden" aktiviert sein.

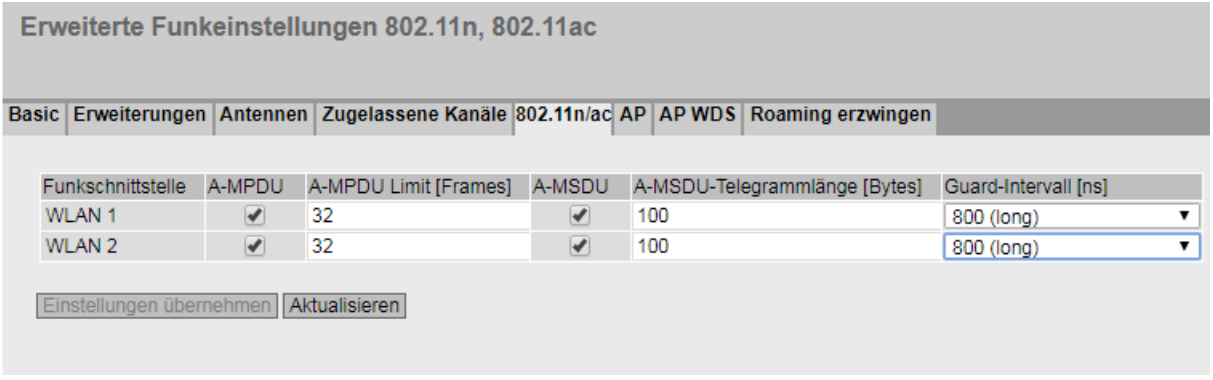
Vorgehensweise

1. Aktivieren Sie bei der gewünschten WLAN-Schnittstelle die Option "Nur zugelassene Kanäle verwenden".
2. Deaktivieren Sie das Optionskästchen "Alle auswählen/abwählen".
3. Aktivieren Sie bei der gewünschten Kanalnummer das entsprechende Optionskästchen.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.6.2.5 802.11n/ac

Eigenschaften des 802.11n/ac

Mit dem Standard IEEE 802.11n/ac ist es möglich Einzel-Frames zu einem größeren Frame zusammenzuführen, A-MPDU- und A-MSDU-Frames.
Auf dieser Seite legen Sie die Einstellungen für die A-MPDU-und A-MSDU-Frames fest. Einige der Einstellungen sind abhängig vom eingestellten Übertragungsstandard und von der gewählten Kanalbreite.



Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen an.
- **A-MPDU**
  Aggregated MAC Protocol Data Unit (A-MPDU)
  - Aktiviert
    Mehrere MPDU-Frames mit der gleichen Zieladresse werden zusammengefasst und als ein großes A-MPDU versendet. Dadurch kann der Gesamtdurchsatz vergrößert werden.
  - Deaktiviert
    A-MPDU-Frames werden empfangen, aber nicht versendet.
- **A-MPDU Limit [Frames]**
  Legen Sie die Anzahl der Einzel-Frames fest, die in einem A-MPDU-Frames zusammengefasst werden.
  Wertebereich: 2 - 64 Frames

- **A-MSDU**
  Aggregated MAC Service Data Unit (A-MSDU)
  - Aktiviert
    Mehrere MSDU-Frames mit der gleichen Zieladresse werden zu einem A-MSDU aneinanderhängt und zusammen versendet. Dadurch wird die Netzlast verringert. A-MSDUs eignen sich durch ihre kürzere maximale Länge eher für die Bündelung mehrerer kürzerer Frames.
  - Deaktiviert
    A-MSDU-Frames werden empfangen, aber nicht versendet.
- **A-MSDU Telegrammlänge [Bytes]**
  Legen Sie die Größe für das A-MSDU-Frame fest, die es maximal erreichen darf.
  Wertebereich: 50 - 200 Bytes
  Defaultwert: 100 Bytes
- **Guard-Intervall [ns]**
  Wählen Sie die Sendepause, die zwischen zwei übertragenen OFDM-Symbolen eingehalten werden muss.
  Folgende Einstellungen sind möglich. Die Auswahl ist abhängig vom gewählten Übertragungsstandard.
  - 400 (short)/800 (long): Die Einstellung 400 ns ist optional. Je nach Signalqualität können Pakete mit einer Sendepause von 400 ns oder 800 ns geschickt werden.
  - 800 (long): Die Sendepause beträgt 800 ns.

Vorgehensweise

1. Aktivieren Sie die Option "A-MPDU".
2. Tragen Sie in dem Eingabefeld "A-MPDU Limit [Frames]" den gewünschten Wert ein.
3. Aktivieren Sie die Option "A-MSDU".
4. Tragen Sie in dem Eingabefeld "A-MSDU Telegrammlänge" den gewünschten Wert ein.
5. Wählen Sie in der Klappliste "Guard-Intervall [ns]" den gewünschten Wert aus.
6. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

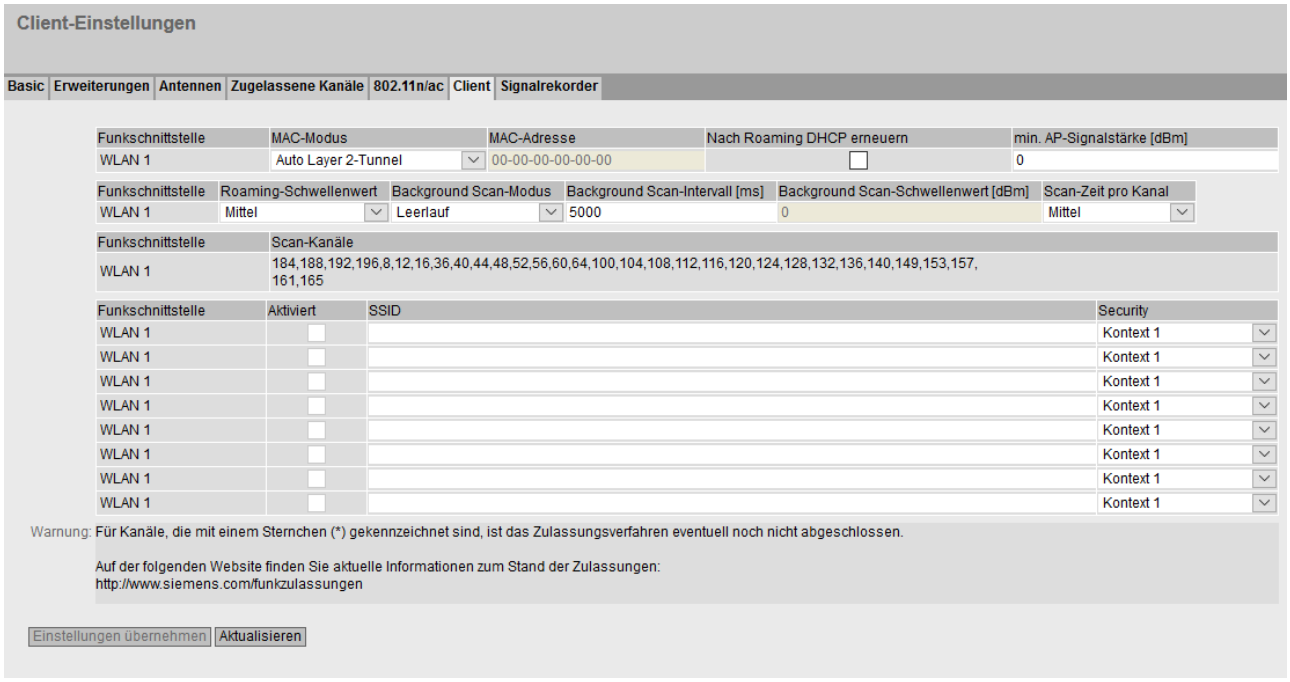
6.6.2.6 Client

Netzanbindung

Auf dieser WBM-Seite legen Sie fest, wie sich das Gerät als Client mit einem Netz verbindet.

Hinweis

Diese WBM-Seite ist nur bei Clients oder bei Access Points im Client-Modus verfügbar.



Hinweis

WLAN-Schnittstelle deaktiviert

Die WLAN-Schnittstelle wird deaktiviert, wenn nicht mindestens eine SSID konfiguriert ist.

Beschreibung

Die Tabelle 1 gliedert sich in folgende Spalten:

- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen an.
- **MAC-Modus**
  Legen Sie fest, wie dem Client eine MAC-Adresse zugeordnet wird. Es gibt die folgenden Möglichkeiten.
  - Auto Layer- 2-Tunnel
    Der Client verwendet entweder den MAC-Modus "Eigene" oder "Layer-2-Tunnel".
  - Manuell
    Wenn Sie Manual wählen, geben Sie die MAC-Adresse in der Spalte "MAC-Adresse" ein.
  - Eigene
    Der Client verwendet die MAC-Adresse der Ethernet-Schnittstelle für die WLAN-Schnittstelle.
  - Layer 2-Tunnel
    Der Client verwendet die MAC-Adresse der Ethernet-Schnittstelle für die WLAN-Schnittstelle. Zusätzlich wird das Netzwerk über die an der Ethernet-Schnittstelle des Clients angeschlossenen MAC-Adressen informiert. Es können bis zu acht MAC-Adressen verwendet werden.

- **MAC-Adresse**
  Wenn Sie bei "MAC-Modus" "Manuell" ausgewählt haben, geben Sie die MAC-Adresse des Clients ein.
- **Nach Roaming DHCP erneuern**
  - Aktiviert
    Nach dem Wechsel zu einem anderen Access Point, wird geprüft, ob die IPv4-Adresse des Clients noch gültig ist. Wenn die IPv4-Adresse ungültig ist, wird eine neue IPv4-Adresse vom DHCP-Server angefordert.
  - Deaktiviert
    Wenn der Client zu einem anderen Access Point wechselt, wird die IPv4-Adresse nicht geprüft.
- **min. AP-Signalstärke**
  Dem Client wird eine Signalstärke vorgegeben.
  Der Client muss das vom Access Point kommende Signal mindestens mit der vorgegebenen Signalstärke empfangen, um sich mit diesem Access Point zu verbinden.
  Die Signalstärke kann kurzfristig schwanken, z. B. durch Bewegung des Clients oder andere Störfaktoren. Um diese Schwankungen beim Signal herauszufiltern, wird mit einer Hysterese ein Bereich um diesen Wert festgelegt, in welchem der Client nicht den Access Point wechselt, bevor dieser Bereich unterschritten wird.
  Wenn das vom Access Point kommende Signal unter diesen Bereich fällt, trennt sich der Client von dem verbundenen Access Point und sucht nach einem neuen Access Point.
- **Roaming-Schwellenwert**
  Legen Sie die Schwelle fest, ab wann der Client zum neuen Access Point wechselt.
  - Hoch
    Wechselt erst bei deutlich höherer Feldstärke zum AP mit stärkerem Signal.
  - Mittel
    Wechselt bei mäßig höherer Feldstärke zum AP mit stärkerem Signal.
  - Niedrig
    Wechselt schon bei geringfügig höherer Feldstärke zum AP mit stärkerem Signal.
- **Background Scan-Modus**
  Während der Client mit einem Access Point verbunden ist, sucht er im Hintergrund nach weiteren Access Points, mit denen er sich gegebenenfalls verbinden kann. Legen Sie den Modus für die Suche fest.
  Folgende Möglichkeiten gibt es:
  - Immer
    Wenn der Background Scan-Schwellenwert unterschritten wird, sucht der Client kontinuierlich nach Access Points.
  - Leerlauf
    Wenn für eine bestimmte Zeit kein Datentransfer stattfindet, wird nach weiteren Access Points gesucht.
  - Deaktiviert
    Solange der Client verbunden ist, wird nicht nach weiteren Access Points gesucht.

- **Background Scan-Intervall [ms]**
  Legen Sie das Intervall fest, in dem nach weiteren Access Points gesucht wird.
- **Background Scan-Schwellenwert [dBm]**
  Legen Sie den Schwellenwert fest. Wenn der Schwellenwert unterschritten wird, sucht der Client nach weiteren Access Points.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Funkschnittstelle**
  Zeigt die WLAN-Schnittstelle an.
- **Scan-Kanäle**
  Zeigt die Kanäle an, auf welchen der Client nach einem Access Point sucht. Die Anzeige ist abhängig von den Funkzulassungen des gewählten Landes und den Einstellungen unter "Zugelassene Kanäle".
- **Scan-Zeit pro Kanal**
  Legen Sie die Scan-Zeit pro Kanal fest.
  Für die Scan-Zeit gibt es drei vordefinierte Einstellungen:
  - Kurz: Aktive Scan-Zeit: 50ms, Passive Scan-Zeit: 90ms
  - Mittel: Aktive Scan-Zeit: 200ms, Passive Scan-Zeit: 300ms
  - Lang: Aktive Scan-Zeit: 300ms, Passive Scan-Zeit: 800ms

  Auf dem Access Point müssen Sie das Beacon-Intervall entsprechend anpassen. Das Beacon-Intervall sollte maximal die Hälfte der passiven Scan-Zeit betragen.

Die Tabelle 3 gliedert sich in folgende Spalten:

- **Funkschnittstelle**
  Zeigt die WLAN-Schnittstelle an.
- **Aktiviert**
  Aktiviert oder deaktiviert die jeweilige SSID.
- **SSID**
  Tragen Sie die SSID des Access Points ein, mit der sich der Client verbinden soll.
  Für die SSID wird der ASCII-Code 0x20 bis 0x7e verwendet.
- **Security**
  Wählen Sie einen Security-Kontext aus. Sie erstellen und konfigurieren einen Security-Kontext unter "Security > WLAN > Basic".
  Default-Einstellung: Context 1

Vorgehensweise

1. Wählen Sie aus der Klappliste "MAC-Modus" die gewünschte Zuordnung der MAC-Adresse aus.
2. Tragen Sie in der Tabelle 3 bei "SSID" eine SSID ein.
3. Wählen Sie einen Security-Kontext aus.
4. Aktivieren Sie die gewünschte SSID.
   Die Funktion "Beliebige SSID" wird deaktiviert.
5. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.6.2.7 Signalrekorder

Aufzeichnung des effektiven Nutzsignals

Mit dem Signalrekorder wird das effektive Nutzsignal zwischen Access Point und Client aufgezeichnet. Mithilfe dieser Daten können Sie Gebiete mit unzureichendem Nutzsignal auffinden. Der Signalrekorder kann besonders dann vorteilhaft eingesetzt werden, wenn sich der Client auf einer fest vorgegebenen Strecke bewegt.

Hinweis

Diese WBM-Seite ist nur bei Clients oder bei Access Points im Client-Modus verfügbar.

Die WLAN-Schnittstelle des Geräts muss aktiviert sein, andernfalls kann keine Aufzeichnung durchgeführt werden.

Beschreibung

Die Darstellung ist in zwei Bereiche aufgeteilt.

- Client
  Stellt die Messung des Clients dar.
- Access Point
  Stellt die Messung des Access Points dar, mit dem der Client aktuell verbunden ist. Vorausgesetzt die Einstellung "Bidirektionale Aufzeichnung" ist aktiviert und auf dem Access Point ist eine Firmware-Version > 6.1 installiert. Der Access Point schickt seine Daten an maximal 3 Clients, auf denen der Signalrekorder läuft. Auf weiteren Clients werden die Access Point-Daten nicht dargestellt.

Beide Bereiche enthalten je zwei Grafiken.

Die erste Grafik enthält die folgenden Elemente:

- Scrollbalken
  Mit dem Scrollbalken können Sie die gesamte Messung durchschauen. Dafür können Sie die Schaltflächen "<<" und ">>" oder die Pfeiltasten auf der Tastatur verwenden.
- Balken (links)
  In dem Balken auf der linken Seite wird das Nutzsignal vom Client / Access Point in Echtzeit angezeigt, entsprechend des abgebildeten Farbschemas. Die graue Linie zeigt das Hintergrundrauschen an.
  Wenn der Client eine iPCF-MC-Verbindung hat, wird das Nutzsignal des Managementkanals mit einer schwarzen Linie dargestellt.
- Farbschema
  Der Bereich > - 35 dBm (Blau) ist der Übersteuerungsbereich, d. h. das WLAN-Signal ist zu stark und wird übersteuert empfangen. Ab ca. - 60 dBm (Gelb) wird das WLAN-Signal schwächer.
- x-Achse
  Die x-Achse zeigt den Verlauf der Messung, in Stichproben und Sekunden.
- Verlaufsdaten
  - Client
    Die Verlaufsdaten zeigen den Wert des effektiven Nutzsignals entsprechend des abgebildeten Farbschemas. Die graue Linie zeigt das Hintergrundrauschen an.
    Wenn der Client während einer Messung den Access Point wechselt (Roaming) oder sich neu verbindet, wird dies durch eine vertikale schwarze Linie angezeigt. An der Linie werden der neue AP Systemname und die BSSID angezeigt.
    Wenn der Client während einer Messung keine Verbindung zu einem Access Point hat, wird kein Nutzsignal angezeigt. Um zu verdeutlichen, dass keine Verbindung zu einem Access Point besteht, wird die BSSID auf 00:00:00:00:00:00 gesetzt und rot dargestellt.
  - Access Point
    Die Verlaufsdaten zeigen den Wert des effektiven Nutzsignals entsprechend des abgebildeten Farbschemas. Die graue Linie zeigt das Hintergrundrauschen an.
    Wenn der Client während einer Messung den Access Point wechselt (Roaming) oder sich neu verbindet, wird dies durch eine vertikale schwarze Linie angezeigt.
    Wenn der Access Point die Einstellung "Bidirektionale Aufzeichnung" nicht unterstützt, wird kein Nutzsignal angezeigt.

Die zweite Grafik enthält folgende Elemente:

- Balken (links)
  In dem Balken auf der linken Seite werden die Übertragungsversuche und die Datenrate des Clients / Access Points angezeigt, entsprechend des abgebildeten Farbschemas.
- Farbschema
  Der Bereich > - 35 dBm (Blau) ist der Übersteuerungsbereich, d. h. das WLAN-Signal ist zu stark und wird übersteuert empfangen. Ab ca. - 60 dBm (Gelb) wird das WLAN-Signal schwächer. Die einzelnen Farben werden nochmals unterhalb der Grafik beschrieben.
- x-Achse
  Die x-Achse zeigt den Verlauf der Messung, in Stichproben und Sekunden.
- Verlaufsdaten
  - Client
    Die Verlaufsdaten zeigen die Übertragungsversuche entsprechend des abgebildeten Farbschemas. Die Übertragungsversuche werden als Balken dargestellt. Die Datenrate der gesendeten Datenpakete wird als Linie dargestellt. Wenn der Client während einer Messung den Access Point wechselt (Roaming) oder sich neu verbindet, wird dies durch eine vertikale schwarze Linie angezeigt.
  - Access Point
    Die Verlaufsdaten zeigen die Übertragungsversuche entsprechend des abgebildeten Farbschemas. Die Übertragungsversuche werden als Balken dargestellt. Die Datenrate der gesendeten Datenpakete wird als Linie dargestellt.
    Wenn der Client während einer Messung den Access Point wechselt (Roaming) oder sich neu verbindet, wird dies durch eine vertikale schwarze Linie angezeigt. Wenn der Access Point die Einstellung "Bidirektionale Aufzeichnung" nicht unterstützt, wird keine Daten angezeigt.

Neben den Grafiken werden folgende Werte angezeigt:

- Status
  Zeigt an, ob der Signalrekorder Werte aufzeichnet oder nicht.
- Current Sample
  Die Nummer der aktuellen Messung
- CL RX-Signal [dBm] / AP RX-Signal [dBm]
  Das effektive Nutzsignal des Clients / des Access Points in dBm
- CL NF [dBm] / AP NF [dBm]
  Das Hintergrundrauschen des Clients / des Access Points in dBm
- CL Retries [%] / AP Retries [%]
  Die Übertragungswiederholungen des Clients / des Access Points in Prozent.
- CL RSSI / AP RSSI
  Der Rohwert der RSSI (Received Signal Strength Indication) des Clients / des Access Points
- CL TX-Rate [Mbps] / AP TX-Rate [Mbps]
  Die durchschnittliche Datenrate der gesendeten Datenpakete während der aktuellen Stichprobe
- CL M-Signal [dBm]
  Wenn der Client eine iPCF-MC-Verbindung hat, wird zusätzlich das Nutzsignal des Managementkanals angezeigt.

- Roaming Counter
  Der Roaming Counter zeigt an, wie oft der Client den Access Point, während der Aufzeichnung, gewechselt hat. Nach 4.294.967.295 Wechseln wird der Zähler zurückgesetzt.
- Operative Channel
  Der aktuelle Kanal bzw. der Kanal, auf dem der Client mit dem Access Point verbunden ist
- AP System Name
  Der Systemname des Access Points
- BSSID
  Die BSSID (Basic Service Set Identification) des Access Points.
- Connected Stations
  Anzahl der Clients, die über die gleiche VAP-Schnittstelle mit dem Access Point verbunden sind.
- Bidirectional Status
  Zeigt an, ob gleichzeitig die Daten des Access Points mit aufgezeichnet werden.

Die Tabelle unterhalb der Grafik enthält folgende Spalten:

- **Funkschnittstelle**
  Zeigt an, für welche WLAN-Schnittstelle die Angaben gelten. Da ein Client über eine WLAN-Schnittstelle verfügt, gibt es in dieser Tabelle immer nur eine Zeile für "WLAN 1".
- **Zeitintervall [ms]**
  Geben Sie das Zeitintervall zwischen der Erfassung von zwei Messwerten in Millisekunden an. Der erste Messwert wird erst nach Ablauf des eingestellten Zeitintervalls angezeigt.
- **Stichproben**
  Geben Sie an, wie viele Messungen durchgeführt werden sollen.
- **Unbegrenzt**
  Wenn Sie das Optionshäkchen aktivieren, ist die Anzahl der Messungen unbegrenzt. Das Feld "Stichproben" ist ausgegraut. Der Signalrekorder läuft so lange, bis er manuell gestoppt wird oder das Gerät umkonfiguriert wird.
  Diese Option können Sie erst ab einem Zeitintervall ≥ 100 Millisekunden auswählen.
  Wenn die Aufzeichnung über 10000 Messungen beinhaltet, werden in der csv-Datei und in der PDF-Datei immer die letzten 10000 Messungen aufgelistet.
- **Bidirektionale Aufzeichnung**
  Wenn Sie die Einstellung aktivieren, werden ab einem Zeitintervall ≥ 10 Millisekunden die Werte des Access Points aufgezeichnet.
  Die Einstellung wird von Access Points mit folgenden Versionen unterstützt: SCALANCE W700 11n > V6.1 und SCALANCE W1700 11ac > V1.0.

- **Starten**
  Klicken Sie die Schaltfläche in dieser Spalte, um die Aufzeichnung des Nutzsignals zu starten.

  Hinweis
  - Wenn Sie eine neue Aufzeichnung starten, wird die vorherige Aufzeichnung überschrieben.
  - Wenn die Aufzeichnung weniger als 10 Minuten gedauert hat und noch nicht beendet war (z. B. wegen Neustart oder Stromausfall), werden die Messwerte gelöscht.

  Der Signalrekorder führt alle 10 Minuten eine automatische Speicherung durch. Nach einem Neustart enthält die Aufzeichnung alle Werte bis zur letzten Speicherung.
- **Stoppen**
  Klicken Sie die Schaltfläche in dieser Spalte, um die Aufzeichnung des Nutzsignals vorzeitig zu beenden. Wenn die vorgegebene Anzahl an Messungen durchgeführt wurde, endet die Aufzeichnung des Nutzsignals automatisch.
- **Angezeigte Stichproben**
  Wählen Sie aus, wie viele Messungen in der Grafik angezeigt werden sollen.

Anwendungshinweise

Beachten Sie folgende Anwendungshinweise, um aussagekräftige Messungen mit dem Signalrekorder zu erhalten:

- Stellen Sie am Access Point eine feste Datenrate ein.
- Wenn Sie iPCF aktiviert haben, stellen Sie für die Messungen eine möglichst geringe Zykluszeit im Access Point ein.
- Es muss sichergestellt werden, dass genügend Datenkommunikation während der Messung besteht, weil die Statistik die ankommenden Datentelegramme auswertet.
- Die Messstrecke sollte 2 bis 3-mal mit den gleichen Parametern abgefahren werden, um herauszufinden, ob Einschnitte im Nutzsignal immer an der gleichen Position vorkommen.
- Punktuell sollten Messungen in einer festen Position über einen längeren Zeitraum durchgeführt werden.

Vorgehensweise

1. Tragen Sie das Zeitintervall zwischen zwei Messungen ein.
2. Tragen Sie bei "Stichproben" die Anzahl der Messungen ein.
3. Wählen Sie die bei "Angezeigte Stichproben" aus, wie viele Messungen in der Grafik angezeigt werden sollen.
4. Klicken Sie die Schaltfläche "Starten".
   Der Status (rechts neben der Grafik) gibt an, ob der Signalrekorder läuft. Der erste Messwert wird erst nach Ablauf des eingestellten Zeitintervalls angezeigt.
5. Um die Aufzeichnung anzuhalten, klicken Sie auf die Schaltfläche "Stoppen".

6. Wechseln Sie zu einem der folgenden Menüpunkte, um das Ergebnis der Aufzeichnung abzurufen:
   - System > Laden & Speichern > HTTP
     Klicken Sie die Schaltfläche "Speichern" in der Tabellenzeile "WLANSigRec", um die Datei "signal_recorder_SCALANCE_W700.zip" im Dateisystem des angeschlossenen PC zu speichern.
   - System > Laden & Speichern > TFTP
     Ändern Sie bei Bedarf den Dateinamen "signal_recorder_SCALANCE_W700.zip" in der Tabellenzeile "WLANSigRec". Wählen Sie in der Tabellenzeile "WLANSigRec" in der Klappliste der letzten Spalte den Eintrag "Datei speichern" und klicken Sie die Schaltfläche "Einstellungen übernehmen".
7. Die ZIP-Datei enthält zwei Dateien mit den Ergebnissen der Aufzeichnung:
   - Eine PDF-Datei: Die Ausgabe ist auf 300 Seiten begrenzt.
   - Eine CSV-Datei: Komplette Auflistung der Aufzeichnung.

Messergebnisse

PDF-Datei

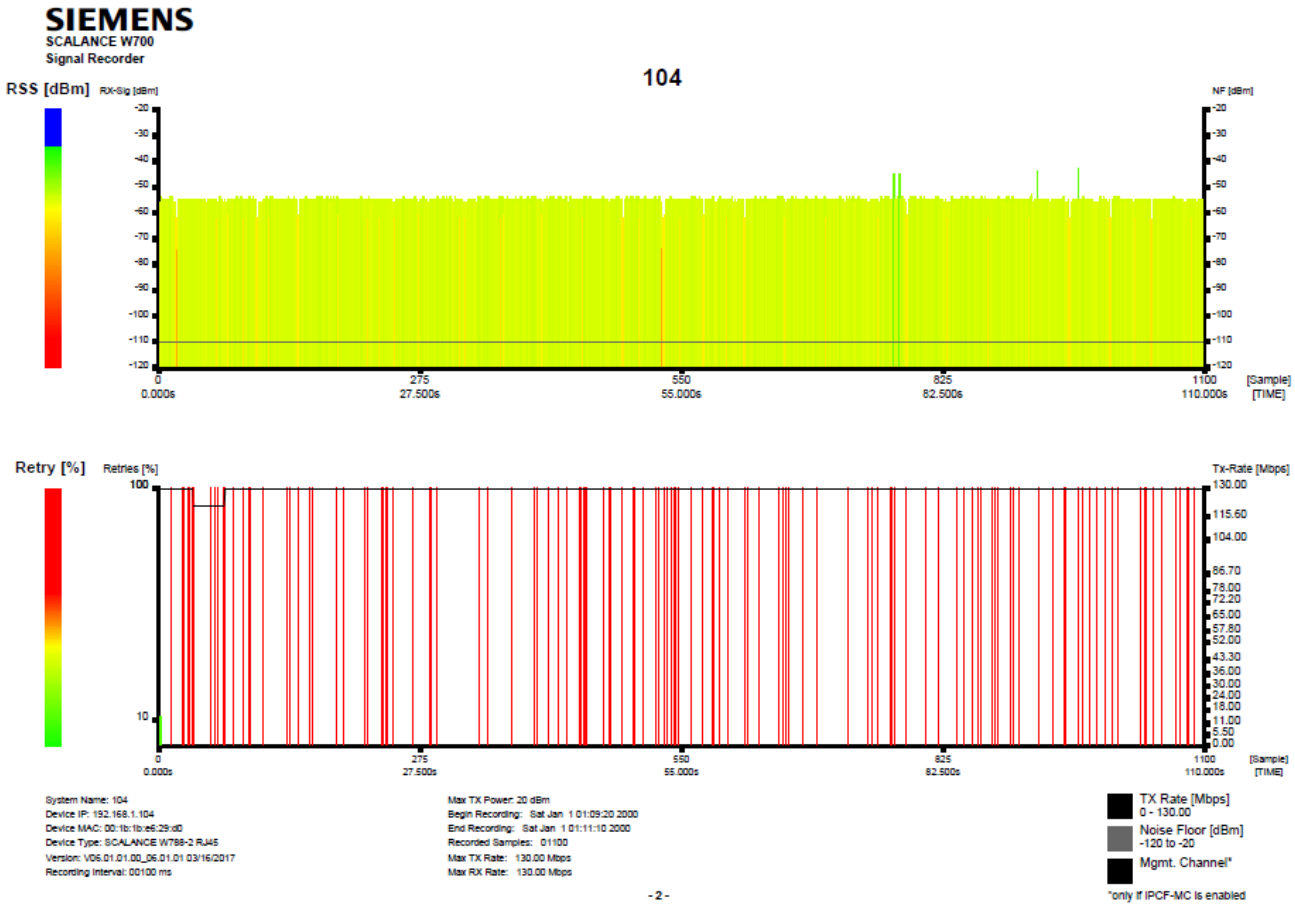
Die PDF-Datei enthält eine grafische Darstellung für den Verlauf des effektiven Nutzsignals in dBm und den Verlauf der Datenrate in Mbps. Farblich entspricht die Grafik der Darstellung im Web Based Management. Wechselt der Client während der Messung den Access Point (Roaming), weisen senkrechte, schwarze Balken mit einem schwarzen Quadrat an der Spitze auf das Ereignis hin.

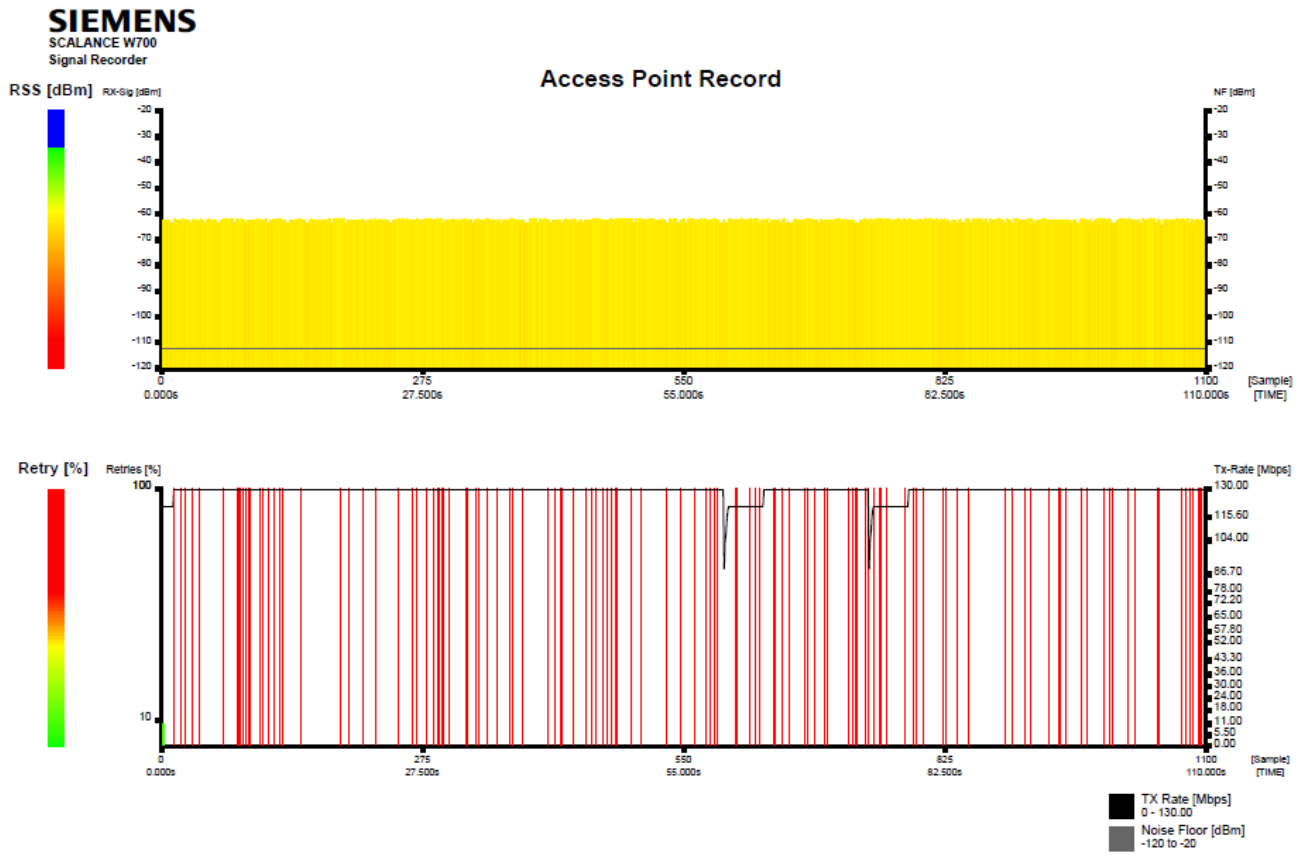
Die Darstellung ist in zwei Bereiche aufgeteilt:

- Client
  Stellt die Messung des Clients dar.
- Access Point
  Stellt die Messung des Access Points dar, mit dem der Client aktuell verbunden ist. Vorausgesetzt die Einstellung "Bidirektionale Aufzeichnung" ist aktiviert. Die Einstellung wird von Access Points mit folgenden Versionen unterstützt: SCALANCE W700 11n > V6.1 und SCALANCE W1700 11ac > V1.0. Der Access Point schickt seine Daten an maximal 3 Clients, auf denen der Signalrekorder läuft. Auf weiteren Clients werden die Access Point-Daten nicht dargestellt.

Wenn der Client eine iPCF-MC-Verbindung hat, wird zusätzlich das Nutzsignal des Managementkanals mit einer schwarzen Linie dargestellt.

Unterhalb der Grafik werden die Konfigurationsdaten des Clients angezeigt.


SIEMENS
SCALANCE W700
Signal Recorder
104
RSS [dBm]
RX-Sig [dBm]
NF [dBm]
-20
-30
-40
-50
-60
-70
-80
-90
-100
-110
-120
0
0.000s
275
27.500s
550
55.000s
825
82.500s
1100
110.000s
[Sample]
[TIME]
Retry [%]
Retries [%]
Tx-Rate [Mbps]
100
10
130.00
115.60
104.00
86.70
78.00
72.20
65.00
57.80
52.00
43.30
36.00
30.00
24.00
18.00
11.00
5.50
0.00
System Name: 104
Device IP: 192.168.1.104
Device MAC: 00:1b:1b:e6:29:d0
Device Type: SCALANCE W788-2 RJ45
Version: V06.01.01.00_06.01.01 03/16/2017
Recording Interval: 00100 ms
Max TX Power: 20 dBm
Begin Recording: Sat Jan 1 01:09:20 2000
End Recording: Sat Jan 1 01:11:10 2000
Recorded Samples: 01100
Max TX Rate: 130.00 Mbps
Max RX Rate: 130.00 Mbps
TX Rate [Mbps]
0 - 130.00
Noise Floor [dBm]
-120 to -20
Mgmt. Channel*
*only if IPCF-MC is enabled
- 2 -



Beispiel für eine erzeugte PDF-Datei

Die folgenden Seiten enthalten tabellarisch die Detailinformationen zu allen Einzelmessungen.

Die Kopfzeile zeigt die IP-Adresse des Clients sowie die BSSID und den Systemnamen des Access Points.

Pro Messung enthält die Tabelle zwei Zeilen. Die Daten des Clients stehen in der ersten Zeile und die dazugehörigen Daten des Access Points in der Zweiten.

Sample	Timestamp	Sig%	dBm	NF	RSSI	Roam	Ch	Retry%	HT-40	TX-Rate	RX-Rate	Con-St	M-Sig	M-Ch	M-NF
1	01:09:20:090	76	-56	-110	39	0	161	11	-	130.00	121.50	1	---	---	---
		63	-63	-112	32			8							

Auf der Seite 2 finden Sie die Legende zu den Abkürzungen in der Tabelle. Die Daten beginnen auf einer neuen Seite, wenn der Client den Access Point wechselt.

Hinweis

Beachten Sie die Beschreibung der einzelnen Spalten in der CSV-Datei. Diese gelten auch für die Spalten der PDF-Datei.

CSV-Datei

Die CSV-Datei enthält Informationen zur Konfiguration des SCALANCE W700-Geräts sowie Detailinformationen zu allen Einzelmessungen und gliedert sich in zwei Bereiche. Der erste Bereich enthält die konfigurierten Einstellungen:

- System Name
  Den Systemnamen des Clients
- Device IP
  Die IP-Adresse des Clients
- Device MAC
  Die MAC-Adresse des Clients
- Recording Interval
  Das Zeitintervall, welches zwischen der Erfassung zweier Messwerte liegt
- Max TX Power
  Maximale Sendeleistung des Geräts
- Begin Recording
  Start der Aufzeichnung
- End Recording
  Ende der Aufzeichnung
- Recorded Samples
  Die Gesamtzahl der Messungen
- Max. TX Rate
  Die maximale Datenrate der gesendeten Datenpakete.
- Max. RX Rate
  Die maximale Datenrate der empfangenen Datenpakete.
- Rx Antenna x type
  Die Einstellung der externen Antennen

Der zweite Bereich ist eine Tabelle. Die Tabelle enthält für jeden Messwert Folgendes:

- Sample
  Die laufende Nummer der Messung auf dem Client (CL) / auf dem Access Point (AP)
- Timestamp
  Der Zeitstempel
- BSSID
  Die BSSID (Basic Service Set Identification) des Access Points
- CL / AP RX-Signal [%]
  Das effektive Nutzsignal in % des Clients (CL)/des Access Points (AP)
- CL / AP RX-Signal [dBm]
  Das effektive Nutzsignal in dBm des Clients (CL)/des Access Points (AP)
- CL / AP NF [dBm]
  Das Hintergrundrauschen in dBm
- CL / AP RSSI
  Der Rohwert der RSSI (Received Signal Strength Indication)

- Roam
  Der Roaming Counter zeigt an, wie oft der Client den Access Point, während der Aufzeichnung, gewechselt hat. Nach 4 294 967 295 Wechseln wird der Zähler zurückgesetzt.
- CL / AP Retry
  Die Übertragungswiederholungen des Clients (CL)/des Access Points (AP)
- Con Stations
  Anzahl der Clients, die mit dem Access Point verbunden sind.
- Operating Ch.
  Der aktuelle Kanal bzw. der Kanal, auf dem der Client mit dem Access Point verbunden ist
- HT-40
  Die Kanalbandbreite 40 MHz
- Scan CH
  Der Kanal, den der Client gerade scannt.
- TX-Rate
  Die durchschnittliche Datenrate der gesendeten Datenpakete
- RX-Rate
  Die durchschnittliche Datenrate der empfangenen Datenpakete
- M-Ch
  Der Managementkanal
- M-Sig
  Das effektive Nutzsignal des Managementkanals
- M-NF
  Das Hintergrundrauschen des Managementkanals
- AP System Name
  Der Systemname des Access Points

System Name: 104
Device IP: 192.168.1.104
Device MAC: 00:1b:1b:e6:29:d0
Device Type: SCALANCE W788-2 RJ45
Version: V06.01.01.00_06.01.01 03/16/2017
Recording Interval: 00100 ms
Max TX Power: 20 dBm
Begin Recording: Sat Jan 1 01:09:20 2000
End Recording: Sat Jan 1 01:11:10 2000
Recorded Samples: 01100
Max TX Rate: 130.00 Mbps
Max RX Rate: 130.00 Mbps

R1 Anten Gain: 3 dBi Add. Attenua Cable length: 0 m
R1 Anten Gain: 3 dBi Add. Attenua Cable length: 0 m
R1 Anten Gain: 0 dBi Add. Attenua Cable length: 0 m

Sample	Timestamp	BSSID	CL RX-Signal	AP RX-Sign	CL RX-Sign	AP RX-Sign	CL NF [dBm	AP NF [dBm	CL RSSI	AP RSSI	Roam	CL Retry	AP Retry	Con Stations	Operating Ch.	HT-40	Scan Ch	TX-Rate	RX-Rate	M-Ch	M-Sig	M-NF	AP System Name
1	01:09:20:090	00:1b:1b:e6:	76	63	-56	-63	-110	-112	39	32	0	11	8	1	161	-	161	130.	121.	---	---	---	106
2	01:09:20:190	00:1b:1b:e6:	80	63	-54	-63	-110	-112	41	32	0	0	0	1	161	-	161	130.	121.	---	---	---	106
3	01:09:20:290	00:1b:1b:e6:	76	63	-56	-63	-110	-112	39	32	0	0	0	1	161	-	161	130.	121.	---	---	---	106
4	01:09:20:390	00:1b:1b:e6:	78	63	-55	-63	-110	-112	40	32	0	0	0	1	161	-	161	130.	121.	---	---	---	106
5	01:09:20:490	00:1b:1b:e6:	78	63	-55	-63	-110	-112	40	32	0	0	0	1	161	-	161	130.	121.	---	---	---	106

Beispiel für eine erzeugte CSV-Datei

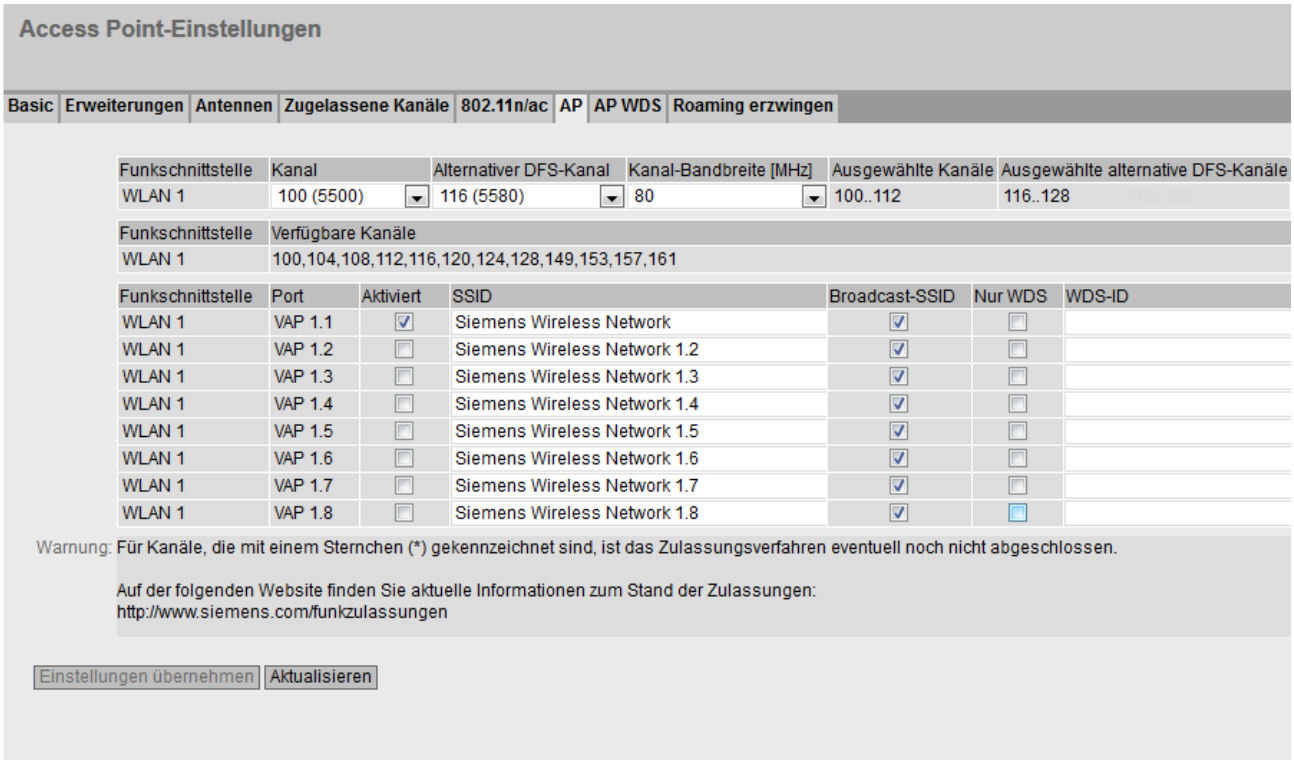
6.6.2.8 AP

Hinweis

Diese WBM-Seite ist nur im Access Point-Modus verfügbar.

Konfiguration

Auf dieser WBM-Seite legen Sie die Konfiguration für den Access Point fest.



Beschreibung

Die Tabelle 1 gliedert sich in folgende Spalten:

- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen an.
- **Kanal**
  Legen Sie den Hauptkanal fest.
  Wenn sich der Access Point selbst einen freien Kanal suchen soll, verwenden Sie "Auto". Die Auswahl der Kanäle, die ein Access Point beim Aufbau einer Funkzelle nutzt, kann begrenzt werden. Aktivieren Sie dazu auf der Seite "Zugelassene Kanäle" das Optionskästchen "Nur zugelassene Kanäle verwenden".
  Wenn Sie einen festen Kanal nutzen wollen, wählen Sie den gewünschten Kanal aus der Klappliste.

  Hinweis

  Kanalabstand bei WLAN-Schnittstellen

  Bei Betrieb einer zweiten WLAN-Schnittstelle müssen Sie auf einen ausreichenden Kanalabstand achten.

- **Alternativer DFS-Kanal**
  Wenn Sie auf der Seite "Basic" die Funktion "DFS" aktiviert haben, legen Sie hier den Alternativ-Kanal fest. Wenn sich der Access Point selbst einen freien Kanal suchen soll, verwenden Sie "Auto".
  Wurde sowohl auf dem Haupt- als auch auf dem Alternativkanal ein konkurrierendes Radarsignal entdeckt, sucht sich der Access Point selbstständig einen freien Kanal aus.
  Wenn Sie einen festen Kanal nutzen wollen, wählen Sie den gewünschten Kanal aus der Klappliste.
- **Kanalbandbreite [MHz]**
  Nur bei den Übertragungsstandards IEEE 802.11n und IEEE 802.11ac können Sie die Kanalbandbreite festlegen.
  Folgende Einstellungen sind möglich.
  - 20 MHz
  - 40 MHz

  Nur bei IEEE 802.11ac:
  - 80 MHz
  - 160 MHz (Nicht beim SCALANCE W1788-2IA M12)
    Nur wenn DFS aktiviert ist, sind für den Betrieb von 160 MHz genügend Kanäle verfügbar.

- **Ausgewählte Kanäle**
  - Kanalnummer (Frequenz) oder Auto
    Wenn bei "Kanal" ein fester Kanal eingestellt ist, wird dieser Kanal inklusive Frequenz angezeigt.
  - Nur bei 80 MHz und einem festen Kanal: Kanalbereich
    Für die Kanalbandbreite 80 MHz sind im entsprechenden Kanalbereich 4 Kanäle notwendig. Der Kanalbereich besteht aus dem bei "Kanal" projektierten Kanal und den drei Folgekanälen.
- **Ausgewählte alternative DFS-Kanäle**
  - Kanalnummer (Frequenz) oder Auto
    Wenn bei "Alternativer DFS-Kanal" ein fester Kanal eingestellt ist, wird dieser Kanal inklusive Frequenz angezeigt.
  - Nur bei 80 MHz und einem festen Kanal: Kanalbereich
    Für die Kanalbandbreite 80 MHz sind im entsprechenden Kanalbereich 4 Kanäle notwendig. Der Kanalbereich besteht aus dem bei "Kanal" projektierten Kanal und den drei Folgekanälen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen an.
- **Verfügbare Kanäle**
  Dieses Feld zeigt die zulässigen Kanäle an. Die Anzeige ist abhängig von den Funkzulassungen des aktuell gewählten Landes und den Einstellungen auf der Seite "Zugelassene Kanäle".

Die Tabelle 3 gliedert sich in folgende Spalten:

- **Funkschnittstelle**
  Zeigt die WLAN-Schnittstelle an.
- **Port**
  Zeigt die VAP-Schnittstelle an.
- **Aktiviert**
  Um die gewünschte VAP-Schnittstelle zu nutzen, aktivieren Sie dieses Optionskästchen.
- **SSID**
  Tragen Sie die SSID des WLANs ein. Die Länge der Zeichenkette für SSID beträgt 1 bis 32 Zeichen.
  Für die SSID wird der ASCII-Code 0x20 bis 0x7e verwendet.

- **Broadcast-SSID**
  - deaktiviert
    Die SSID wird nicht mehr im Beacon-Frame des Access Points versendet. Somit ist die SSID für andere Geräte nicht sichtbar. Nur die Clients können sich mit dem Access Point verbinden, denen die SSID des Access Points bekannt ist und mit dieser konfiguriert sind. Die Option "Beliebige SSID" muss auf diesen Clients deaktiviert sein.
  - aktiviert
    Die SSID wird im Beacon-Frame des Access Points versendet und ist für andere Geräte sichtbar. So können auch Clients sich mit dem Access Point verbinden, bei denen die Option "Beliebige SSID" aktiviert ist.

Hinweis

Da bei der SSID-Übertragung keine Verschlüsselung eingesetzt wird, kann diese Funktion nur grundlegend vor unberechtigten Zugriffen schützen. Die Nutzung einer Authentifizierungsmethode (z.B. WPA2 (RADIUS), wenn nicht möglich WPA2-PSK) bietet eine höhere Sicherheit. Es muss zudem damit gerechnet werden, dass gewisse Endgeräte Probleme mit dem Zugriff auf eine versteckte SSID haben können.

- **Nur WDS**
  Wenn Sie diese Option aktivieren, unterstützt der Access Point nur die Kommunikation über WDS. In der Betriebsart WDS müssen alle Access Points den gleichen Kanal benutzen.
- **WDS-ID**
  Tragen Sie die WDS-ID ein. Die WDS-ID darf maximal 32 Zeichen lang sein.
  Um eine WDS-Verbindung aufzubauen, tragen Sie beim WDS-Partner diese WDS ID ein.
  Für die WDS-ID wird der ASCII-Code 0x20 bis 0x7e verwendet.

Vorgehensweise

1. Wählen Sie aus der Klappliste "Kanal" den gewünschten Kanal.
2. Tragen Sie im Eingabefeld "SSID" bei der entsprechenden WLAN-Schnittstelle und dem Port den Netzwerknamen ein.
3. Aktivieren Sie bei der entsprechenden WLAN-Schnittstelle und dem Port das Optionskästchen "Aktiviert".
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

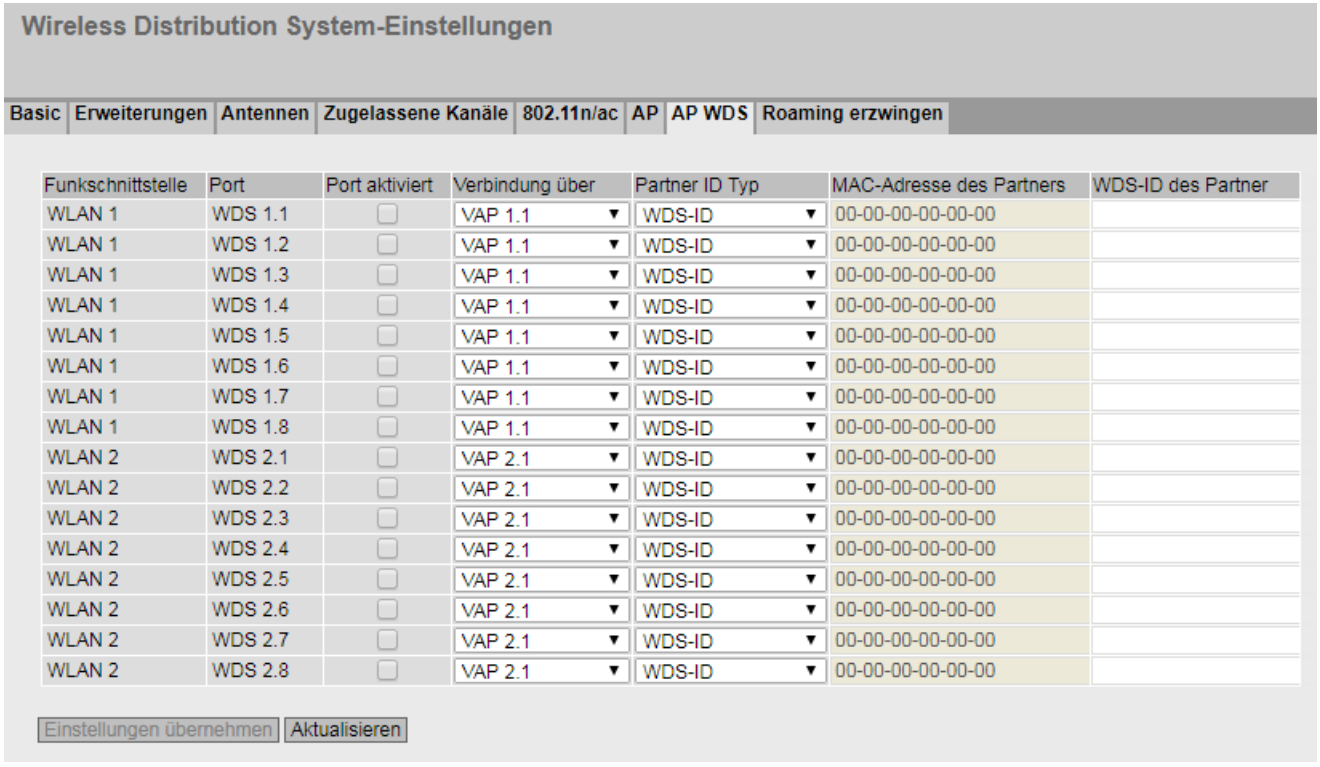
6.6.2.9 AP WDS

Hinweis

Diese WBM-Seite ist nur im Access Point-Modus verfügbar.

Kommunikation

Im normalen Betrieb ist der Access Point als Schnittstelle zu einem Netz eingesetzt und kommuniziert mit Clients. Es gibt allerdings auch den Anwendungsfall, dass mehrere Access Points miteinander kommunizieren müssen, beispielsweise zum Zweck der Reichweitenvergrößerung oder zum Aufbau eines Wireless-Backbones. Diese Betriebsart ist mit WDS (Wireless Distributed System) möglich.



Funkschnittstelle	Port	Port aktiviert	Verbindung über	Partner ID Typ	MAC-Adresse des Partners	WDS-ID des Partner
WLAN 1	WDS 1.1	☐	VAP 1.1	WDS-ID	00-00-00-00-00-00	
WLAN 1	WDS 1.2	☐	VAP 1.1	WDS-ID	00-00-00-00-00-00	
WLAN 1	WDS 1.3	☐	VAP 1.1	WDS-ID	00-00-00-00-00-00	
WLAN 1	WDS 1.4	☐	VAP 1.1	WDS-ID	00-00-00-00-00-00	
WLAN 1	WDS 1.5	☐	VAP 1.1	WDS-ID	00-00-00-00-00-00	
WLAN 1	WDS 1.6	☐	VAP 1.1	WDS-ID	00-00-00-00-00-00	
WLAN 1	WDS 1.7	☐	VAP 1.1	WDS-ID	00-00-00-00-00-00	
WLAN 1	WDS 1.8	☐	VAP 1.1	WDS-ID	00-00-00-00-00-00	
WLAN 2	WDS 2.1	☐	VAP 2.1	WDS-ID	00-00-00-00-00-00	
WLAN 2	WDS 2.2	☐	VAP 2.1	WDS-ID	00-00-00-00-00-00	
WLAN 2	WDS 2.3	☐	VAP 2.1	WDS-ID	00-00-00-00-00-00	
WLAN 2	WDS 2.4	☐	VAP 2.1	WDS-ID	00-00-00-00-00-00	
WLAN 2	WDS 2.5	☐	VAP 2.1	WDS-ID	00-00-00-00-00-00	
WLAN 2	WDS 2.6	☐	VAP 2.1	WDS-ID	00-00-00-00-00-00	
WLAN 2	WDS 2.7	☐	VAP 2.1	WDS-ID	00-00-00-00-00-00	
WLAN 2	WDS 2.8	☐	VAP 2.1	WDS-ID	00-00-00-00-00-00	

Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen an.
- **Port**
  Zeigt die WDS-Schnittstellen an.
- **Port aktiviert**
  Aktiviert die WDS-Schnittstelle.
- **Verbindung über**
  Legen Sie fest, über welche VAP-Schnittstelle die WDS-Verbindung hergestellt wird. Es werden sowohl die MAC-Adresse des VAPs als auch die Security-Einstellungen z.B. WPA2 benutzt.

- **Partner ID Typ**
  Legen Sie die Art der WDS-Kommunikation fest.
  - MAC-Adresse
    Die MAC-Adresse wird verwendet. Das Eingabefeld "WDS-ID des Partners" wird gegraut. Tragen Sie bei "MAC-Adresse des Partners" die MAC-Adresse des WDS-Partners ein.
  - WDS-ID
    Die WDS-ID wird verwendet. Das Eingabefeld "MAC-Adresse des Partners" wird gegraut. Tragen Sie bei "WDS-ID des Partners" die WDS ID des WDS-Partners ein.
- **MAC-Adresse des Partners**
  Tragen Sie die MAC-Adresse des WDS-Partners ein.
- **WDS-ID des Partners**
  Tragen Sie die WDS-ID des WDS-Partners ein. Für die WDS-ID sind die ASCII-Zeichen 0x20 bis 0x7e erlaubt.

Hinweis

Übereinstimmende Sicherheitseinstellungen im WDS-Betrieb

Achten Sie im WDS-Betrieb auf übereinstimmende Security-Einstellungen bei allen beteiligten Geräten. Bei fehlerhaften oder nicht kompatiblen Einstellungen bei den einzelnen Geräten kann kein Datenaustausch aufgrund fehlerhafter Authentifizierung stattfinden. Vermeiden Sie die Einstellung "Auto" auf der Basic Wizard-Seite "Security-Einstellungen". Mit dieser Einstellung ist eine Synchronisation der Sicherheitseinstellungen zwischen den Access Points nicht möglich.

Hinweis

Im WDS-Betrieb gelten für alle daran beteiligten Access Points folgende Einschränkungen:

- Alle Access Points, die miteinander kommunizieren sollen, müssen den gleichen Kanal, das gleiche Übertragungsverfahren und die gleiche Datenrate benutzen.
- Als Verschlüsselungsverfahren können Sie entweder WEP oder WPA(2)-PSK auswählen. Die Sicherheits-Einstelllungen konfigurieren Sie in der jeweils zugeordneten VAP-Schnittstelle: "Security > WLAN > Basic"
  Die Authentifizierung über RADIUS Server können Sie nicht für eine WDS-Verbindung nutzen.
- Im Übertragungsverfahren IEEE 802.11h ist es nicht sinnvoll, die Betriebsart WDS zu wählen. In der Betriebsart WDS müssen alle Access Points den gleichen Kanal benutzen. Wird jetzt von einem Access Point ein Signal eines Primärnutzers entdeckt, wird der Kanal automatisch gewechselt und dadurch die bestehende Verbindung unterbrochen.

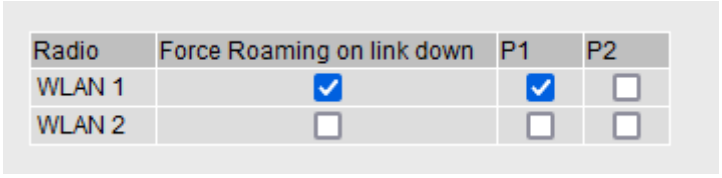
Vorgehensweise

1. Wählen Sie aus der Klappliste "Verbindung über" die gewünschte VAP-Schnittstelle.
2. Wählen Sie aus der Klappliste "Partner ID Typ" den Eintrag "WDS-ID".
3. Tragen Sie im Eingabefeld "WDS-ID des Partners" die WDS-ID des WDS-Partners ein. Das Eingabefeld "MAC-Adresse" wird gegraut.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.6.2.10 Roaming erzwingen

Auf dieser Seite legen Sie fest, wann ein Roaming durchgeführt wird.

- **Bei Verbindungsabbruch (nur im Access Point-Modus)**
  Wenn die Verbindung über die Ethernet-Schnittstelle abbricht, bekommt ein über das Funknetz angemeldeter Client davon nichts mit. Mögliche Ursachen für einen Verbindungsabbruch sind z. B. Kabelbruch, Netzkomponenten ausgefallen, Stecker gezogen. Der Access Point kann die angemeldeten Clients zu einem Roaming zwingen, indem er bei Verbindungsabbruch die entsprechende WLAN-Schnittstelle abschaltet. Die Clients roamen und verbinden sich dann auf einen anderen Access Point. Sobald die Ethernet-Schnittstelle wieder verfügbar ist, schaltet der Access Point seine WLAN-Schnittstellen wieder an.
  Bei mehreren Ethernet-Schnittstellen wird die WLAN-Schnittselle abgeschaltet, wenn alle konfigurierten Ethernet-Schnittstellen nicht erreichbar sind.

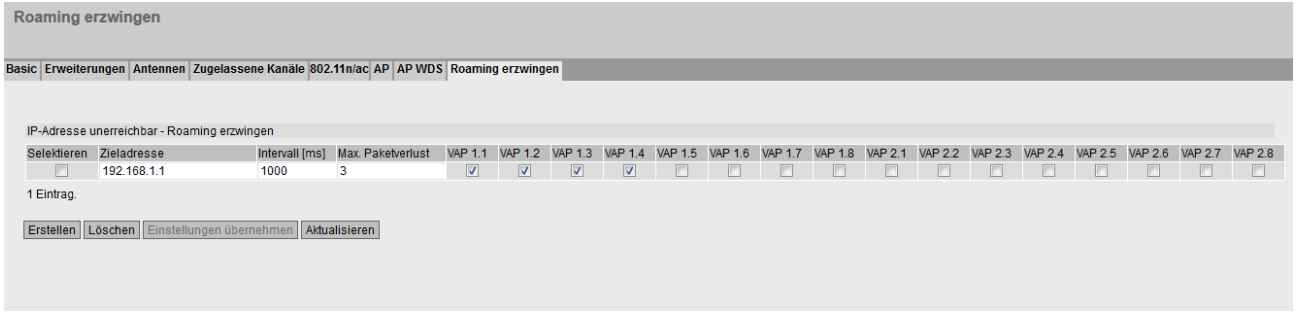


- **Bei Nicht-Erreichen der Zieladresse**
  Wenn die Zieladresse nicht erreichbar ist, erhält ein über das Funknetz angebundener Client davon keine Kenntnis. Der Access Point kann die angemeldeten Clients zu einem Roaming zwingen, indem er die entsprechende VAP-Schnittstelle abschaltet. Zum Überwachen sendet das Gerät in regelmäßigen Abständen Ping-Anforderung an die projektierten Zieladressen.

  – VAP-Schnittstelle überwacht durch eine Zieladresse
    Wenn von dieser Zieladresse keine Ping-Antwort empfangen wird, schaltet der Access Point die entsprechende VAP-Schnittstelle ab.

  – VAP-Schnittstelle überwacht durch mehrere Zieladressen
    Erst wenn von keiner dieser Zieladressen eine Ping-Antwort empfangen wird, schaltet der Access Point die entsprechende VAP-Schnittstelle ab. Solange mindestens eine Zieladresse erreichbar ist, bleibt die VAP-Schnittstelle angeschaltet.

  Der Access Point sendet an die WLAN-Clients, die über diese VAP-Schnittstelle verbunden sind, einen Disassociation-Frame. Die WLAN-Clients roamen und verbinden sich mit einer anderen VAP-Schnittstelle. Ist die Adresse wieder erreichbar, kann die Verbindung über diese VAP-Schnittstelle wieder aufgebaut werden.



Beschreibung

Die Tabelle "Roaming bei Verbindungsabbruch erzwingen" ist nur im Access Point-Modus verfügbar und gliedert sich in folgende Spalten:

- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen an.
- **Roaming bei Verbindungsabbruch erzwingen**
  Wenn aktiviert, wird beim Verbindungsabbruch über die Ethernet-Schnittstelle die WLAN-Schnittstelle abgeschaltet.
- **P1 / P2**
  Legen Sie fest, welche Ethernet-Schnittstelle überwacht wird. Bei mehreren Ethernet-Schnittstellen wird die WLAN-Schnittselle abgeshaltet, wenn alle konfigurierten Ethernet-Schnittstellen nicht erreichbar sind.

Die Tabelle "IP-Adresse nicht erreichbar - Roaming erzwingen" gliedert sich in folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Ziel-IP-Adresse**
  Geben Sie die IPv4-Adresse oder den FQDN (Fully Qualified Domain Name) des Ziels an, dessen Erreichbarkeit geprüft wird.

  Hinweis

  Zieladresse nicht im IPv4-Subnetz

  Wenn die Zieladresse nicht in dem IPv4-Subnetz liegt, ist bei "Layer 3 (IPv4) > Subnetze > Konfiguration" ein Gateway einzutragen.

  Base Bridge-Modus "802.1Q VLAN Bridge"

  Wenn Sie unter "Layer 2 > VLAN" den "Base Bridge-Modus" "802.1Q VLAN Bridge" konfiguriert haben, werden die Ping-Anforderungen in das Management-VLAN gesendet.

- **Intervall [ms]**
  Legen Sie fest, in welchen Zeitabständen Ping-Anforderung gesendet werden.
- **Max. Paketverlust**
  Legen Sie die maximale Anzahl der nacheinander verlorenen Ping- Antworten fest. Wenn diese Anzahl bei einer Zieladresse erreicht wird, dann gilt diese Zieladresse als nicht erreichbar (down).
- **VAP X.Y**
  Legen Sie fest, welche VAP-Schnittstelle überwacht wird. Die entsprechende VAP-Schnittstelle sollte auch aktiviert sein.

Vorgehensweise

Roaming erzwingen anlegen, wenn die Verbindung abgebrochen wurde:

1. Aktivieren Sie das Optionskästchen "Roaming bei Verbindungsabbruch erzwingen" bei der WLAN-Schnittselle, die bei Verbindungsabbruch abgeschaltet werden muss.
2. Wählen Sie einen oder mehrere Ethernet-Ports der WLAN-Schnittselle aus, deren Verbindungsstatus überwacht wird.

Roaming erzwingen anlegen, wenn die Zieladresse nicht erreichbar ist:

1. Klicken Sie auf die Schaltfläche "Erstellen".
2. Legen Sie folgende Einstellungen fest:
   - Zieladresse
   - Intervall
   - Max. Paketverlust
3. Legen Sie die VAP-Schnittstelle fest, die durch diese Zieladresse überwacht wird.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

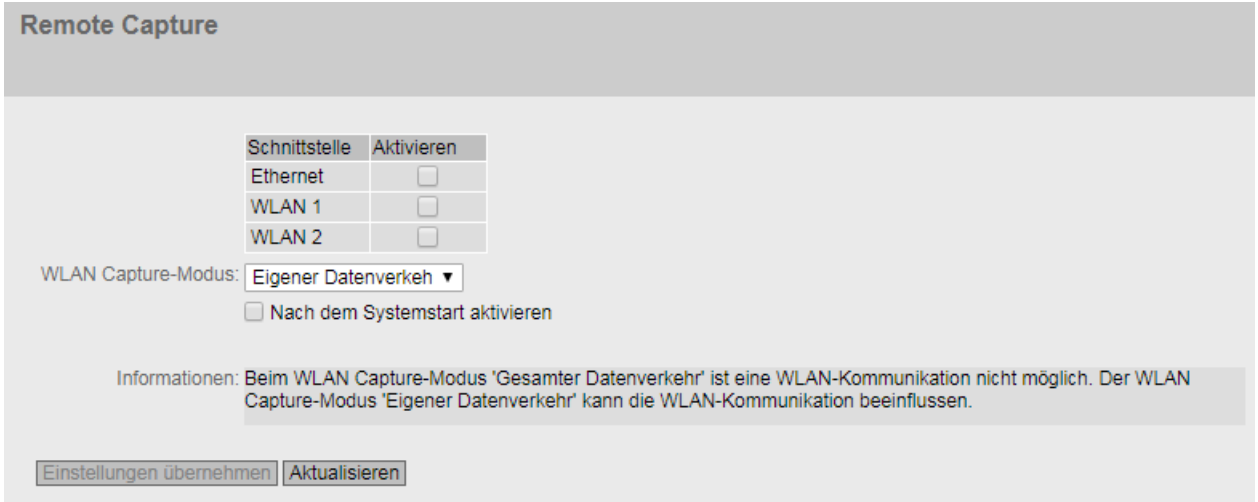
Roaming erzwingen löschen

1. Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
2. Klicken Sie auf die Schaltfläche "Löschen". Die Einträge werden gelöscht und die Seite wird aktualisiert.

6.6.3 Remote Capture

Auf dieser WBM-Seite aktivieren Sie an der Schnittstelle (Ethernet, WLAN) die Funktion "Remote Capture". Die Funktion ist für die Netzwerkdiagnose über einen angeschlossenen PC, z. B. um Übertragungsfehlern auf die Spur zu kommen.

Die Funktion können Sie auch an mehreren Schnittstellen gleichzeitig aktivieren. Wenn die Funktion aktiviert ist, lässt sich die Schnittstelle in Wireshark einbinden. Wireshark zeichnet über einen Zeitraum den Datenverkehr auf, der über die Schnittstelle fließt. Danach können Sie aus dem Mitschnitt heraus den Inhalt der Frames ansehen oder nach bestimmten Inhalten filtern.



Beschreibung

Die Tabelle enthält folgende Spalten:

- **Schnittstelle**
  Die Schnittstelle, auf die sich der Eintrag bezieht.
- **Aktivieren**
  Aktivieren oder deaktivieren Sie die Funktion "Remote Capture". Defaultmäßig ist die Funktion deaktiviert.

  Hinweis

  Performance

  Aktivieren Sie die Funktion nur zu Diagnosezwecke. Der erhöhte Datenverkehr könnte die Performance des Geräts beeinflussen.

  Ethernet

  - Bei der Auswahl von Ethernet wird nicht zwischen den beiden Ports (P1 und P2) unterschieden. Deshalb ist auch ein Aufzeichnen zwischen Port 1 und Port 2 nicht möglich.
  - Der Datenverkehr wird nicht angezeigt, der nur weitergeleitet und nicht von der WLAN-Schnittstelle empfangen oder gesendet wurde.

Die Seite enthält folgende Felder:

- **WLAN Capture-Modus**
  Legen Sie den Aufzeichnungsmodus für die WLAN-Schnittstelle fest:
  - Eigener Datenverkehr
    In diesem Fall werden die Frames aufgezeichnet, die vom Gerät empfangen und gesendet wurden.
    Ausnahme: Nicht angezeigt werden Frames, die direkt von der Hardware behandelt werden, z. B. Hardware-Wiederholungen, Acknowledgement-Frames.
  - Gesamter Datenverkehr
    Der Access Point sendet keine Frames mehr, sondern zeichnet alle eingehenden Frames auf.

    Hinweis

    Keine WLAN-Kommunikation zwischen Access Point und Clients

    Wenn die Einstellung "Gesamter Datenverkehr" verwendet wird, ist der Access Point für andere Teilnehmer nicht mehr erreichbar und verliert gegebenenfalls die verbundenen Clients.

- **Nach dem Systemstart aktivieren**
  - Deaktiviert
    Nach einem Neustart wird die Konfiguration auf die Default-Einstellung zurückgesetzt.
  - Aktiviert
    Die Konfiguration wird gespeichert und bleibt nach einem Neustart enthalten.

Schnittstelle in Wireshark einbinden

Voraussetzung:

- Wireshark ab V2.0.0 ist auf dem PC installiert.
- Der PC und das Gerät müssen über IP (Layer 3) erreichbar sein.

Vorgehensweise

Um den Datenverkehr z. B. der WLAN-Schnittstelle 1 in Wireshark zu analysieren, gehen Sie folgendermaßen vor:

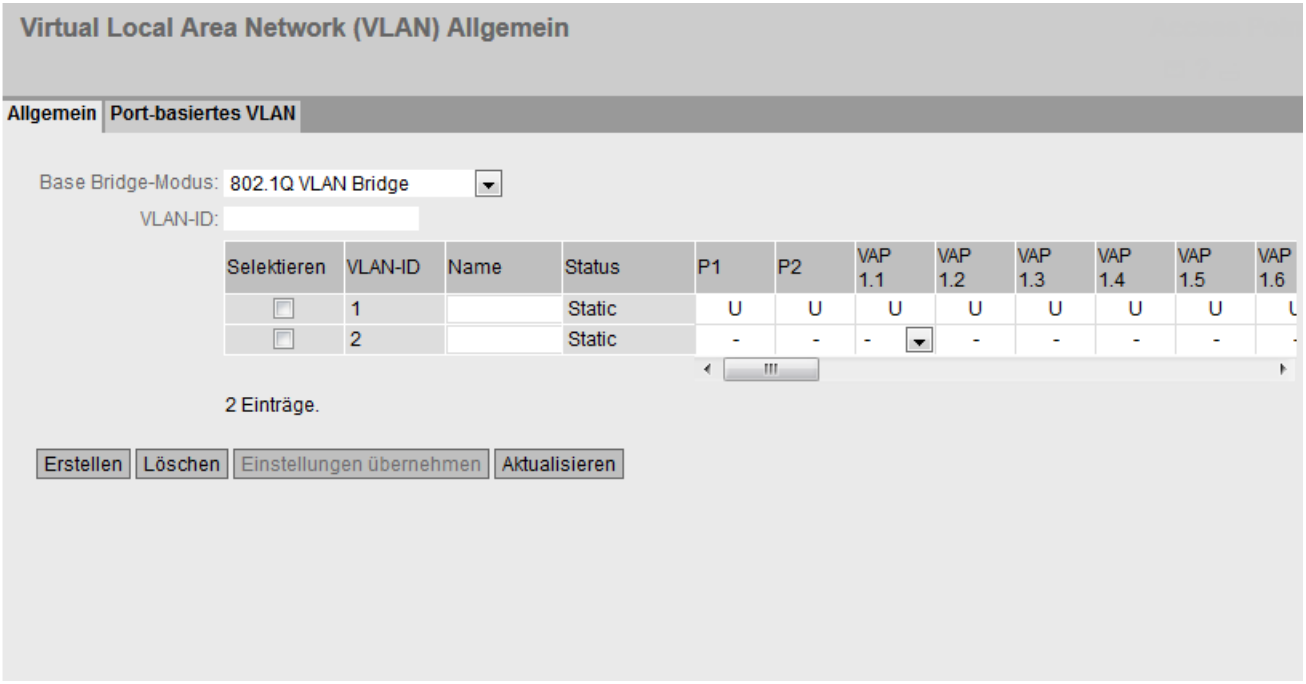
1. Aktivieren Sie am Gerät an der WLAN-Schnittstelle die Funktion "Remote Capture".
2. Wählen Sie bei Empfangsmodus "Eigener Datenverkehr" aus.
3. Klicken Sie auf "Einstellungen übernehmen", um die Funktion zu aktivieren.
4. Starten Sie Wireshark.
5. Klicken Sie im Menü "Aufzeichnen" auf "Optionen". Das Fenster "Wireshark - Mitschnittschnittstellen" wird geöffnet.
6. Klicken Sie auf dem Register "Eingabe" auf die Schaltfläche "Schnittstellen verwalten...". Klicken Sie im folgenden Dialog auf das Register "Entfernte Schnittstellen".
7. Um die Schnittstelle hinzuzufügen, klicken Sie im Register "Entfernte Schnittstellen" das Pluszeichen.
8. Geben Sie im folgenden Dialog bei "Host" die IPv4-Adresse des Geräts und bei "Port" 2002 ein.
9. Aktivieren Sie bei "Authentifizierung" "Keine Authentifizierung" und klicken Sie auf die Schaltfläche "OK".
10. Auf dem Register "Entfernte Schnittstellen" wird der Host und die Schnittstellen angezeigt, an denen zuvor die Funktion "Remote Capture" aktiviert wurde.
11. Wählen Sie die Schnittstelle aus und klicken Sie auf die Schaltfläche "OK".
12. Um die Aufzeichnung zu starten, klicken Sie Menü "Aufzeichnen" auf "Starten". Weitere Informationen zum Umgang mit dem Programm erhalten Sie bei Wireshark.

Wenn Sie mehrere Schnittstellen analysieren, können Sie für jede Schnittstelle eine Wireshark-Instanz verwenden.

6.7 Menü "Layer 2"

6.7.1 VLAN

6.7.1.1 Allgemein



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

Hinweis

Ändern der Agent VLAN-ID

Wenn der Konfigurations-PC direkt über Ethernet mit dem Gerät verbunden ist und Sie die Management VLAN-ID ändern, ist nach der Änderung das Gerät über Ethernet nicht mehr erreichbar.

Beschreibung

Die Seite enthält folgende Felder:

- **Base Bridge-Modus**
  Wählen Sie aus der Klappliste den gewünschten Modus aus. Folgende Modi sind möglich:

  Hinweis

  Base Bridge-Modus wechseln

  Beachten Sie den Abschnitt "Base Bridge Mode wechseln". In diesem Abschnitt ist beschrieben, wie sich ein Wechsel auf die bestehende Konfiguration auswirkt.

  - 802.1Q VLAN Bridge
    Stellt bei dem Gerät den Modus "VLAN-aware" ein. In diesem Modus werden VLAN-Informationen berücksichtigt.
  - 802.1D Transparent Bridge
    Stellt bei dem Gerät den Modus "VLAN-unaware" ein. In diesem Modus werden VLAN-Tags nicht verändert, sondern transparent weitergeleitet. Die VLAN-Priorität wird für CoS ausgewertet. Sie können in diesem Modus keine VLANs anlegen. Es ist nur ein Management-VLAN verfügbar: VLAN 1.

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

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **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 24 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 VLAN. Weitere Einstellungen konfigurieren Sie unter "Layer 2 > VLAN > Port-basiertes VLAN".
  - T
    Diese Option wird nur angezeigt und kann im WBM nicht ausgewählt werden.
    Dieser Port ist Trunk-Port und wurde dadurch Mitglied in allen VLANs.
    Sie konfigurieren diese Funktion im CLI (Command Line Interface) mit Hilfe des Befehls "`switchport mode trunk`".

Base Bridge-Modus wechseln

VLAN-unaware (802.1D Transparent Bridge) → VLAN-aware (802.1Q VLAN Bridge)

Wenn Sie den Base Bridge-Modus von VLAN-unaware in VLAN-aware ändern, hat dies folgende Auswirkungen:

- Alle statischen und dynamischen Unicast-Einträge werden gelöscht.

VLAN-aware (802.1Q VLAN Bridge) → VLAN-unaware (802.1D Transparent Bridge)

Wenn Sie den Base Bridge-Modus von VLAN-aware in VLAN-unaware ändern, hat dies folgende Auswirkungen:

- Alle VLAN-Konfigurationen werden gelöscht.
- Es wird ein Management-VLAN angelegt: VLAN 1.
- Alle statischen und dynamischen Unicast-Einträge werden gelöscht.

802.1Q VLAN Bridge: Wichtige Regeln für VLANs

Berücksichtigen Sie bei der Konfiguration und beim Betrieb Ihrer VLANs folgende Regeln:

- Telegramme mit der VLAN ID "0" werden wie ungetaggte Telegramme behandelt, behalten jedoch ihren Prioritätswert.
- Alle Ports am Gerät senden standardmäßig Telegramme ohne VLAN-Tag, um sicher zu gehen, dass der Endteilnehmer diese Telegramme empfangen kann.
- Bei SCALANCE W-Geräten ist an allen Ports die VLAN ID "1" voreingestellt.
- Wenn an einem Port ein Endteilnehmer angebunden ist, dann sollen ausgehende Telegramme ohne Tag versendet werden (statischer Zugriffs-Port). Wenn sich an dem Port ein weiterer Switch befindet, so ist das Telegramm mit einem Tag zu versehen (Trunk Port).
- Bei einem Trunk Port erfolgt die VLAN-Zuordnung dynamisch. Statische Konfigurationen können nur durchgeführt werden, wenn der Port zusätzlich zur Eigenschaft Trunk Port noch statisch als Member in den betreffenden VLANs eingetragen wird. Ein Beispiel für eine statische Konfiguration ist das Zuweisen von Multicastgruppen in bestimmten VLANs.

Vorgehensweise

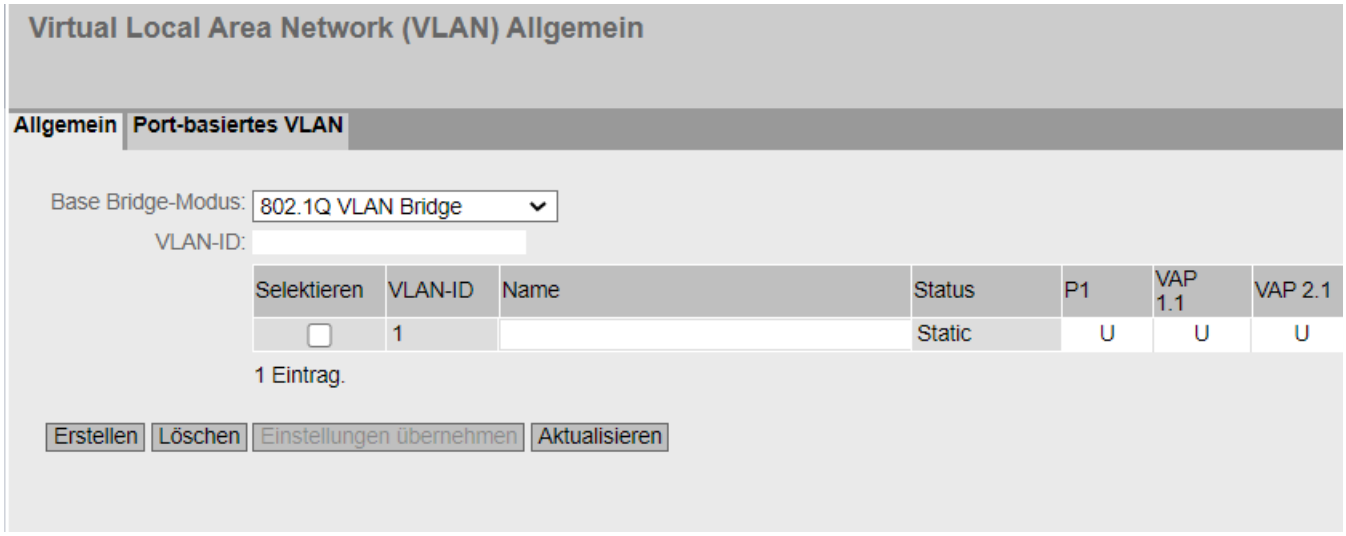
Voraussetzung:

Bei Base Bridge-Modus ist "802.1Q VLAN Bridge" eingestellt.

Neues VLAN anlegen

1. Tragen Sie im Eingabefeld "VLAN-ID" eine ID ein.
2. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag erzeugt. Die Felder sind standardmäßig mit "-" belegt.
3. Tragen Sie bei Name einen Namen für das VLAN ein.
4. Legen Sie die Verwendung der Ports in dem VLAN fest. Wenn Sie z. B. M auswählen, ist der Port Mitglied des VLANs. Das in diesem VLAN gesendete Telegramm wird mit dem entsprechenden VLAN-Tag weitergeleitet.
5. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.7.1.2 Port-basiertes VLAN

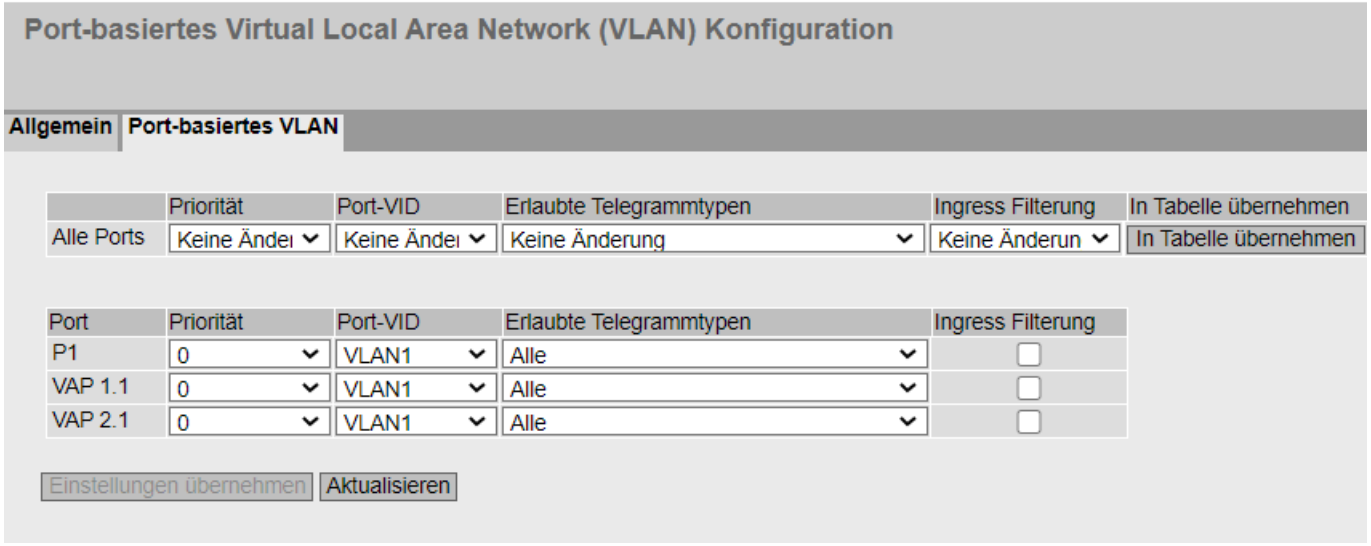


Verarbeitung empfangener Telegramme

Auf dieser Seite legen Sie die Konfiguration der Port-Eigenschaften für den Telegrammempfang fest.

Voraussetzung:

- Auf der Seite "Allgemein" ist bei "Base Bridge-Modus" "802.1Q VLAN Bridge" eingestellt.



Beschreibung

Die Tabelle 1 gliedert sich in folgende Spalten:

Hinweis

Die Tabelle 1 ist nur dann verfügbar, wenn mindestens ein VLAN konfiguriert ist.

- **Port**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **Priorität / Port-VID / Erlaubte Telegrammtypen / Ingress-Filterung**
  Wählen Sie in der Klappliste die Einstellung für alle Ports aus. Wenn "Keine Änderung" ausgewählt ist, bleiben die Einträge der entsprechenden Spalte in der Tabelle 2 unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt die verfügbaren Ports und Schnittstellen an.
- **Priorität**
  Wählen Sie aus der Klappliste die 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 aus der Klappliste die VLAN ID aus. Nur die VLAN IDs sind wählbar, die Sie auf der Seite "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.

- **Erlaubte Telegrammtypen**
  Legen Sie fest, welche Arten von Telegrammen akzeptiert werden. Es gibt folgende Alternativen:
  - Nur getaggte Frames
    Das Gerät verwirft alle ungetaggten Telegramme. Andernfalls gelten die Weiterleitungsregeln entsprechend der Konfiguration.
  - Alle
    Das Gerät leitet alle Telegramme weiter.
- **Ingress Filterung**
  Legen Sie fest, ob die VID von empfangenen Telegrammen ausgewertet wird.
  Sie haben folgende Möglichkeiten:
  - Aktiviert
    Die VLAN ID empfangener Telegramme bestimmt die Weiterleitung: Für die Weiterleitung eines VLAN-getaggten Telegramms muss der Empfangsport Mitglied im selben VLAN sein. Am Empfangsport werden Telegramme aus unbekannten VLANs verworfen.
  - Deaktiviert
    Alle Telegramme werden weitergeleitet.

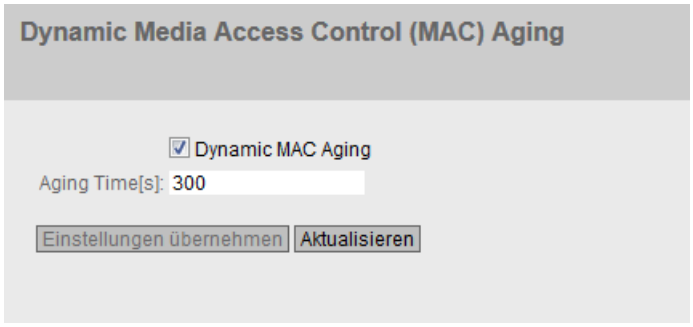
Vorgehensweise

1. Klicken Sie in der Zeile des zu konfigurierenden Ports in das entsprechende Feld der Tabelle, um es zu konfigurieren.
2. Tragen Sie in die Eingabefelder die einzustellenden Werte ein.
3. Wählen Sie aus den Klapplisten die einzustellenden Werte aus.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.7.2 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:

- **Dynamisches MAC-Aging**
  Aktivieren oder deaktivieren Sie die Funktion zum automatischen Aging von gelernten MAC-Adressen:
- **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 18 Sekunden bis 630 Sekunden.

Hinweis

Aging Time bei Inter AP Blocking

Die Aging Time sollte größer sein als das Aktualisierungsintervall bei Inter AP Blocking.

Vorgehensweise

1. Aktivieren Sie das Optionskästchen "Dynamisches MAC-Aging".
2. Tragen Sie in das Eingabefeld "Aging Time [s]" die Zeitspanne in Sekunden ein.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.7.3 Spanning Tree

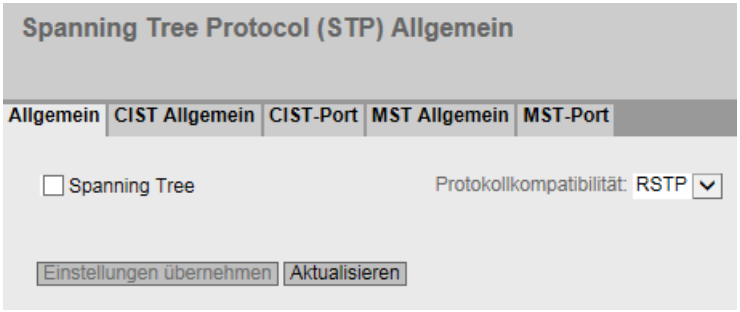
6.7.3.1 Allgemein

Allgemeine Einstellungen von Spanning Tree

Dies ist die Basisseite zu Spanning Tree. Wählen Sie aus der Klappliste den Kompatibilitätsmodus aus. Standardmäßig ist Multiple Spanning Tree aktiviert.

In der jeweiligen Konfigurationsseite dieser Funktionen sind detailliertere Einstellungen möglich.

Je nach Kompatibilitätsmodus können Sie in der jeweiligen Konfigurationsseite die entsprechende Funktion konfigurieren.



Beschreibung

Die Seite enthält folgende Felder:

- **Spanning Tree**
  Aktivieren oder deaktivieren Sie Spanning Tree .
- **Protokollkompatibilität**
  Wählen Sie den Kompatibilitätsmodus von Spanning Tree aus. Z. B. wenn Sie RSTP wählen, dann verhält sich Spanning Tree wie ein RSTP.
  Folgende Einstellungen gibt es:
  - STP
  - RSTP
  - MSTP

Vorgehensweise

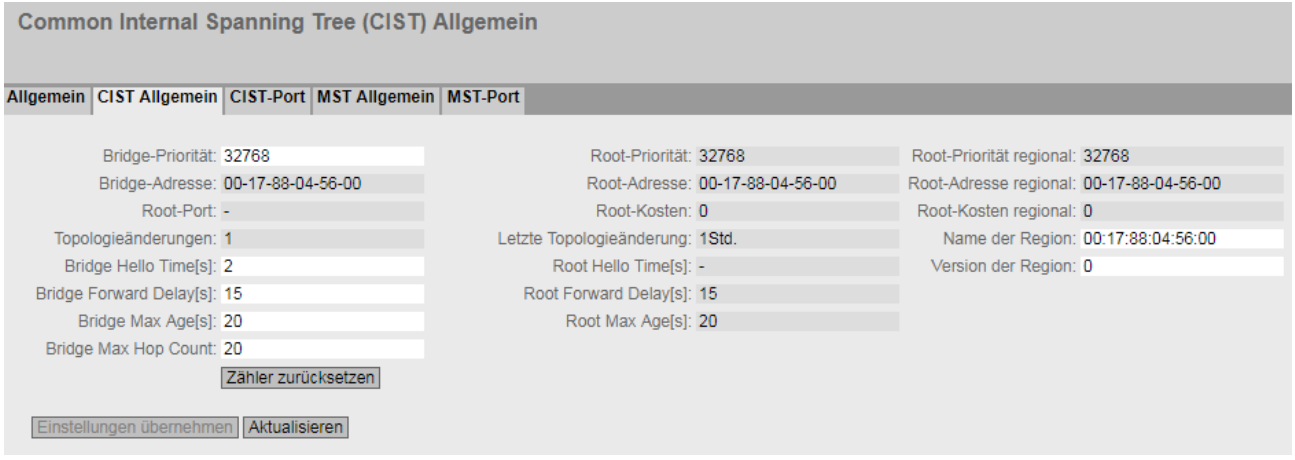
1. Aktivieren Sie das Optionskästchen "Spanning Tree".
2. Wählen Sie aus der Klappliste "Protokollkompatibilität" den Kompatibilitätsmodus aus.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.7.3.2 CIST Allgemein

Konfiguration CIST

Die Seite besteht aus folgenden Teilen.

- Der linke Teil der Seite zeigt die Konfiguration des Geräts.
- Der mittlere Teil zeigt die Konfiguration der Root Bridge, wie sie aus Spanning Tree-Telegrammen abgeleitet werden kann, die ein Gerät empfangen hat.
- Der rechte Teil zeigt die Konfiguration der Regionalen Root Bridge, wie sie aus den MSTP-Telegrammen abgeleitet werden kann. Die angezeigten Daten sind nur dann sichtbar, wenn auf der Seite "Allgemein" "Spanning Tree" aktiviert und bei "Protokollkompatibilität" "MSTP" eingestellt ist. Das gilt auch für den Parameter "Bridge Max Hop Count". Wenn das Gerät eine Root Bridge ist, stimmen die Informationen des linken und des rechten Teils überein.



Beschreibung

Die Seite enthält folgende Felder:

- **Bridge-Priorität / Root-Priorität**
  Anhand der Bridge-Priorität wird festgelegt, welches Gerät Root Bridge wird. Die Bridge mit der höchsten Priorität wird Root Bridge. Je kleiner der Wert, desto höher die Priorität. Wenn in einem Netz mehrere Geräte die gleiche Priorität besitzen, wird das Gerät Root Bridge, dessen MAC-Adresse den niedrigsten Zahlenwert hat. Beide Parameter, Bridge-Priorität und MAC-Adresse, bilden zusammen die Bridge-Kennung. Da die Root Bridge alle Wegeänderungen verwaltet, sollte sie wegen der Laufzeit der Telegramme möglichst zentral angeordnet sein. Der Wert für die Bridge-Priorität ist ein ganzzahliges Vielfaches von 4096 mit einem Wertebereich von 0 bis 61440.
- **Bridge-Adresse / Root-Adresse**
  Die Bridge-Adresse zeigt die MAC-Adresse des Geräts und die Root-Adresse zeigt die MAC-Adresse der Root Bridge an.
- **Root-Port**
  Zeigt den Port an, über den das Gerät mit der Root Bridge kommuniziert.

- **Root-Kosten**
  Die Pfadkosten von diesem Gerät bis zur Root Bridge.
- **Topologieänderungen / Letzte Topologieänderung**
  Die Angabe für das Gerät nennt die Zahl der Umkonfigurationen aufgrund des Spanning Tree-Mechanismus seit dem letzten Hochlauf. Für die Root Bridge wird die Zeitdauer seit der letzten Umkonfiguration wie folgt angezeigt:
  - Sekunden: Zusatz "sec" hinter der Zahlenangabe
  - Minuten: Zusatz "min" hinter der Zahlenangabe
  - Stunde: Zusatz "hr" hinter der Zahlenangabe
- **Bridge Hello Time[s] / Root Hello Time[s]**
  Jede Bridge versendet regelmäßig Konfigurationstelegramme (BPDUs). Der Zeitabstand zwischen zwei solchen Telegrammen ist die Hello-Time. Der Standardwert für diesen Parameter beträgt 2 Sekunden.
- **Bridge Forward Delay[s] / Root Forward Delay[s]**
  Neue Konfigurationsinformationen werden von einer Bridge nicht sofort, sondern erst nach dem im Parameter Weiterleitungsverzögerung festgelegten Zeitraum angewendet. So wird sichergestellt, dass der Betrieb entsprechend der neuen Topologie erst gestartet wird, wenn alle Bridges die notwendigen Informationen haben. Der Standardwert für diesen Parameter beträgt 15 Sekunden.
- **Bridge Max Age / Root Max Age**
  Bridge-Max-Age definiert das maximale "Alter", das eine empfangene BPDU haben darf, um vom Switch als gültig akzeptiert zu werden. Der Standardwert für diesen Parameter beträgt 20 Sekunden.
- **Bridge Max Hop Count**
  Dieser Parameter gibt an, wie viele MSTP-Teilnehmer eine BPDU passieren darf. Wird eine MSTP-BPDU empfangen, deren Hop Count den hier konfigurierten Wert übersteigt, wird sie verworfen. Der Standardwert für diesen Parameter beträgt 20.
- **Root-Priorität regional**
  Beschreibung der angezeigten Werte siehe Bridge-Priorität / Root-Priorität
- **Root-Adresse regional**
  Zeigt die MAC-Adresse der regionalen Root Bridge an.
- **Root-Kosten regional**
  Zeigt die Pfadkosten von diesem Gerät bis zur regionalen Root Bridge an.
- **Name der Region**
  Tragen Sie den Namen der MSTP-Region ein, zu der dieses Gerät gehört. Standardmäßig ist hier die MAC-Adresse des Geräts eingetragen. Dieser Wert muss auf allen Geräten, die zur selben MSTP-Region gehören, gleich sein.
- **Version der Region**
  Tragen Sie die Versionsnummer der MSTP-Region ein, in der sich das Gerät befindet. Dieser Wert muss auf allen Geräten, die zur selben MSTP-Region gehören, gleich sein.
- **Zähler zurücksetzen**
  Klicken Sie auf diese Schaltfläche, um die Zähler auf dieser Seite zurückzusetzen.

Vorgehensweise

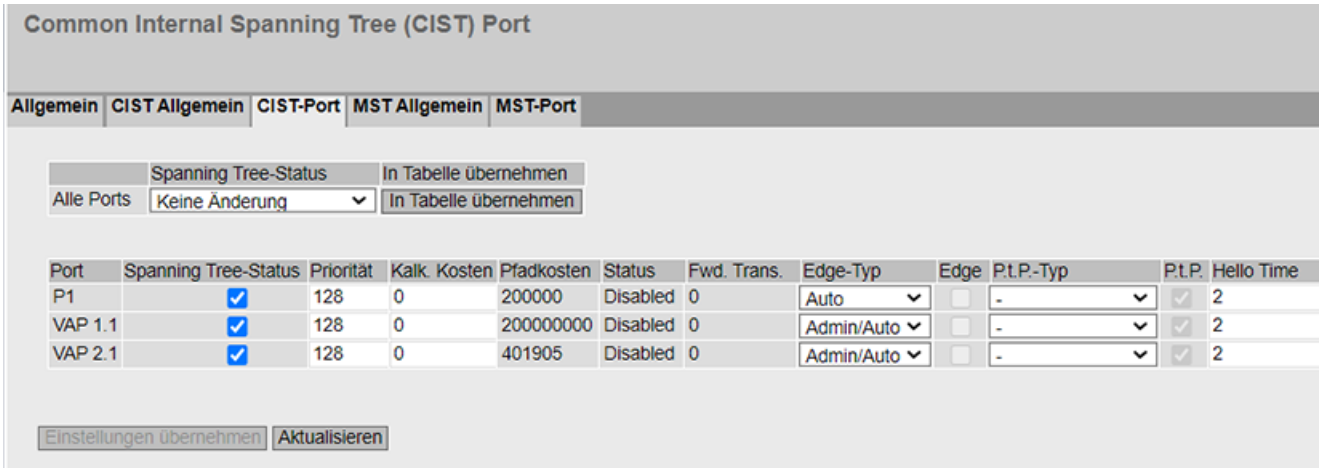
1. Tragen Sie in die Eingabefelder die für die Konfiguration benötigten Daten ein.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.7.3.3 CIST-Port

Konfiguration der CIST-Ports

In der Tabelle wird beim Aufruf der Seite der aktuelle Stand der Konfiguration der Port-Parameter angezeigt.

Klicken Sie zur Konfiguration in die entsprechenden Felder der Port-Tabelle.



Beschreibung

Die Tabelle 1 gliedert sich in folgende Spalten:

- **Spalte 1**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **Spanning Tree-Status**
  Wählen Sie in der Klappliste die Einstellung für alle Ports aus. Wenn "Keine Änderung" ausgewählt ist, bleiben die Einträge der entsprechenden Spalte in der Tabelle 2 unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, werden die Einstellungen für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt die verfügbaren Ports und Schnittstellen an.
- **Spanning Tree-Status**
  Legen Sie fest, ob der Port im Spanning Tree integriert ist oder nicht.

  Hinweis

  Wenn Sie die Option "Spanning Tree-Status" für einen Port deaktivieren, kann es zur Schleifenbildung kommen. Die Topologie muss beachtet werden.

- **Priorität**
  Tragen Sie die Priorität des Ports ein. Die Priorität wird nur ausgewertet, wenn die Pfadkosten gleich sind.
  Der Wert muss durch 16 teilbar sein. Wenn der Wert nicht durch 16 teilbar ist, wird der Wert automatisch angepasst.
  Wertebereich: 0 - 240.
  Der Standardwert ist 128.
- **Kalk. Kosten**
  Tragen Sie die Wegekostenberechnung ein. Wenn Sie den Wert "0" eintragen, wird im Feld "Pfadkosten" der automatisch ermittelte Wert angezeigt.
- **Pfadkosten**
  Die Pfadkosten von diesem Port zur Root-Bridge. Die Strecke mit dem geringsten Wert wird als Weg ausgewählt. Haben mehrere Ports eines Geräts den gleichen Wert, wird der Port mit der niedrigsten Portnummer ausgewählt.
  Wenn im Feld "Kalk. Kosten" der Wert "0" ist, so wird der automatisch ermittelte Wert angezeigt.
  Im anderen Fall wird der Wert des Feldes "Kalk. Kosten" angezeigt.
  Die Ermittlung der Wegekosten richtet sich maßgeblich nach der Übertragungsgeschwindigkeit. Je höher die erzielbare Übertragungsgeschwindigkeit ist, umso kleiner ist der Wert für die Wegekosten.
  Typische Werte für Wegekosten bei Rapid Spanning Tree:
  - 1000 Mbit/s = 20.000
  - 100 Mbit/s = 200.000
  - 10 Mbit/s = 2.000.000

  Die Werte können aber auch individuell parametriert werden.

- **Status**
  Zeigt den momentanen Status an, in dem sich der Port befindet. Die Werte werden nur angezeigt und können nicht parametriert werden. Der Parameter "Status" ist abhängig von dem projektierten Protokoll. Beim Status ist Folgendes möglich:
  - Disabled
    Der Port empfängt nur und nimmt nicht am STP, MSTP und RSTP teil.
  - Discarding
    In der Betriebsart "Discarding" werden BPDU-Telegramme empfangen. Andere aus- oder eingehende Telegramme werden verworfen.
  - Listening
    In diesem Status werden sowohl BPDU-Telegramme empfangen als auch gesendet. Der Port ist in den Spanning Tree-Algorithmus einbezogen.
  - Learning
    Vorstufe zum Weiterleitungsstatus, der Port lernt aktiv die Topologie (d. h. die Teilnehmeradressen).
  - Forwarding
    Der Port ist nach der Umkonfigurationszeit aktiv im Netz, er empfängt und sendet Datentelegramme.
- **Fwd. Trans**
  Gibt die Anzahl der Wechsel vom Status "Discarding" zum Status "Forwarding" an.
- **Edge-Typ**
  Legen Sie die Art des Edge-Ports fest. Sie haben folgende Möglichkeiten:
  - "-"
    Edge Port ist deaktiviert. Der Port wird wie ein "no EdgePort" behandelt.
  - Admin
    Wählen Sie diese Option, wenn sich an diesem Port immer ein Endgerät befindet. Sonst wird bei jeder Verbindungsänderung eine Rekonfiguration des Netzwerks ausgelöst.
  - Auto
    Wählen Sie diese Option, wenn an diesem Port automatisch erkannt werden soll, ob ein Endgerät angeschlossen ist. Beim ersten Verbindungsaufbau wird der Port wie ein "no Edge Port" behandelt.
  - Admin/Auto
    Wählen Sie diese Optionen, wenn Sie an diesem Port eine Kombination aus beiden betreiben. Beim ersten Verbindungsaufbau wird der Port als Edge Port behandelt.
- **Edge**
  Zeigt an, in welchem Status der Port ist.
  - Aktiviert
    An diesem Port befindet sich ein Endgerät.
  - Deaktiviert
    An diesem Port befindet sich ein Spanning Tree- oder Rapid Spanning Tree-Gerät.

  Bei einem Endgerät kann ein Switch ohne Rücksicht auf Spanning Tree-Telegramme schneller den Port umschalten. Wird entgegen dieser Einstellung ein Spanning Tree-Telegramm empfangen, wechselt der Port automatisch auf die Einstellung "Deaktiviert" für Switches

- **P.t.P. -Typ**
  Wählen Sie in der Klappliste die gewünschte Option aus. Die Auswahl ist abhängig vom eingestellten Port.
  - P.t.P.
    Auch bei Halbduplex wird von einer Punkt-zu-Punkt-Verbindung ausgegangen.
  - Shared Media
    Auch bei einer Vollduplexverbindung wird nicht von einer Punkt-zu-Punkt-Verbindung ausgegangen.

    Hinweis

    Punkt-zu-Punkt-Verbindung bedeutet eine direkte Verbindung zwischen zwei Geräten. Eine Shared Media-Verbindung ist z.B. eine Verbindung zu einem Hub.
  - "-"
    Punkt-zu-Punkt wird automatisch ermittelt. Steht der Port auf Halbduplex, wird nicht von einer Punkt-zu-Punkt-Verbindung ausgegangen.
- **P.t.P.**
  - Aktiviert
    Zeigt an, dass eine Punkt-zu-Punkt-Verbindung besteht.
  - Deaktiviert
    Zeigt an, dass keine Punkt-zu-Punkt-Verbindung besteht.
- **Hello Time**
  Tragen Sie das Intervall ein, nach der die Bridge Konfigurations-BPDUs sendet.
  Standardmäßig sind 2 Sekunden eingestellt.
  Wertebereich: 1-2 Sekunden

  Hinweis

  Die portspezifische Einstellung der Hello-Time ist nur mit MSTP kompatiblen Modus möglich.

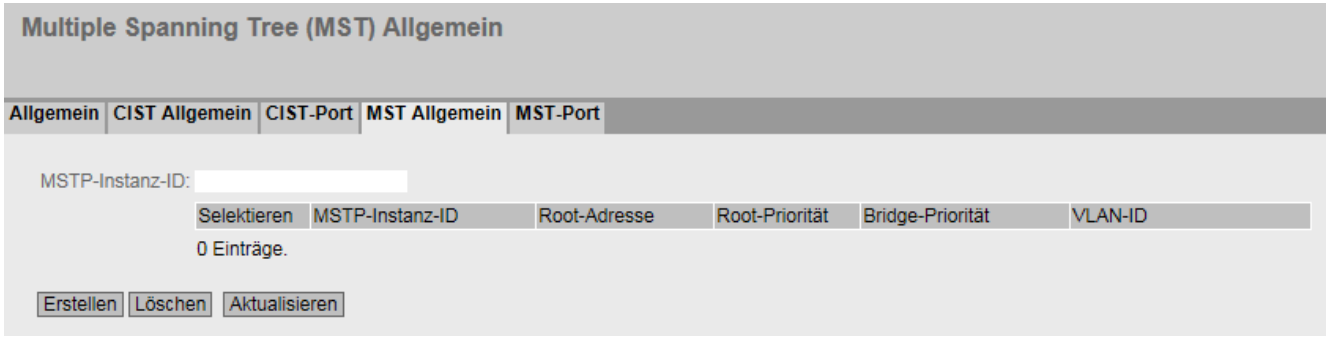
Vorgehensweise

1. Tragen Sie in den Eingabefeldern der Tabellenzeile des zu konfigurierenden Ports die Werte ein.
2. Wählen Sie aus den Klapplisten der Felder der Tabellenzeile des zu konfigurierenden Ports die Werte aus.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.7.3.4 MST Allgemein

Multiple Spanning Tree-Konfiguration

Bei MSTP können zusätzlich zu RSTP mehrere VLANs in einem LAN mit eigenen RSTP-Bäumen verwaltet werden.



Beschreibung

Die Seite enthält folgendes Feld:

- **MSTP-Instanz-ID**
  Tragen Sie die Nummer der MSTP-Instanz ein.
  Zulässige Werte: 1 - 64
  Sie können bis zu 16 MSTP-Instanzen definieren.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **MSTP-Instanz-ID**
  Zeigt die Nummer der MSTP-Instanz an.
- **Root-Adresse**
  Zeigt die MAC-Adresse der Root-Bridge an
- **Root-Priorität**
  Zeigt die Priorität der Root-Bridge an.
- **Bridge-Priorität**
  Tragen Sie in dieses Feld die Bridge-Priorität ein. Der Wert für die Bridge-Priorität ist ein ganzzahliges Vielfaches von 4096 mit einem Wertebereich von 0 bis 61440.
- **VLAN-ID**
  Tragen Sie die VLAN-ID ein. Sie können hier auch Bereiche mit Start-ID, "-", End-ID angeben. Mehrere Bereiche oder IDs werden durch "," separiert.
  Zulässige Werte: 1- 4094

Vorgehensweise

Neuen Eintrag erstellen

1. Tragen Sie in das Feld "MSTP-Instanz-ID" die Nummer der MSTP Instanz ein.
2. Klicken Sie auf die Schaltfläche "Erstellen".
3. Tragen Sie in das Feld "VLAN-ID" die Identifikationsmarke des virtuellen LANs ein.
4. Tragen Sie in das Feld "Bridge-Priorität" die Priorität der Bridge ein.
5. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

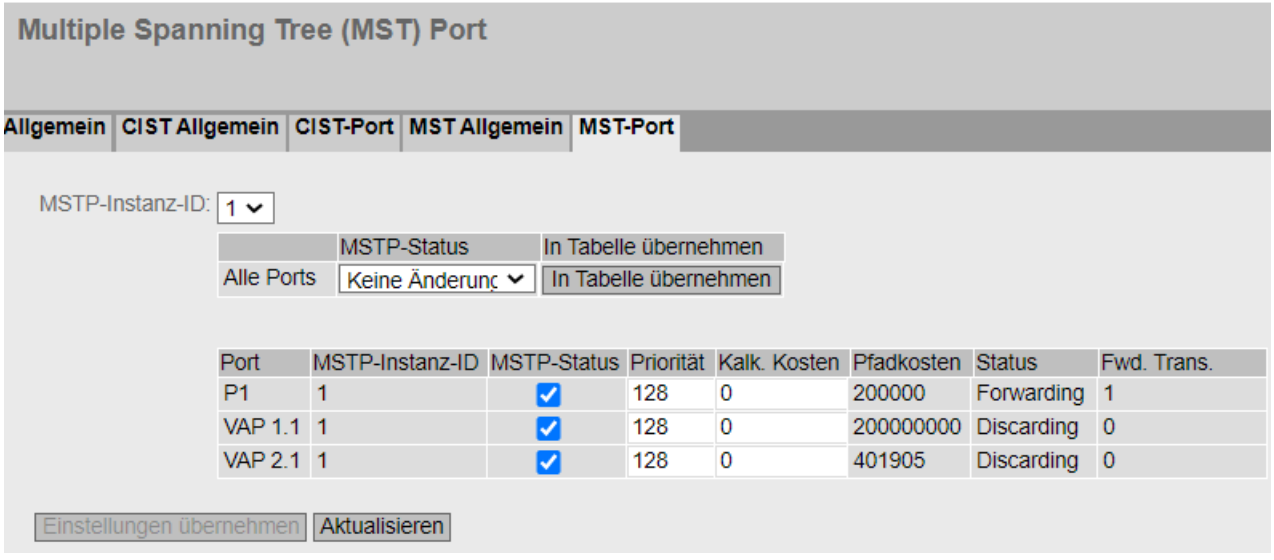
Einträge löschen

1. Markieren Sie mit Hilfe der Optionskästchen vor der entsprechenden Zeile die zu löschenden Einträge.
2. Klicken Sie auf die Schaltfläche "Löschen", um die markierten Einträge aus dem Speicher zu entfernen. Die Einträge werden aus dem Speicher des Geräts gelöscht und die Darstellung dieser Seite wird aktualisiert.

6.7.3.5 MST-Port

Konfiguration der Multiple Spanning Tree Port Parameter

Auf dieser Seite stellen Sie die Parameter für die Ports der konfigurierten Multiple Spanning Tree Instanzen ein.



Beschreibung

Die Seite enthält folgendes Feld:

- **MSTP-Instanz-ID**
  Wählen Sie in der Klappliste die ID der MSTP-Instanz aus.

Die Tabelle 1 gliedert sich in folgende Spalten:

- **Spalte 1**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **MSTP-Status**
  Wählen Sie in der Klappliste die Einstellung für alle Ports aus. Wenn "Keine Änderung" ausgewählt ist, bleiben die Einträge der entsprechenden Spalte in der Tabelle 2 unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt alle verfügbaren Ports und Schnittstellen an.
- **MSTP-Instanz-ID**
  Zeigt die ID der MSTP-Instanz an.
- **MSTP-Status**
  Klicken Sie in das Optionskästchen, um diese Option zu aktivieren oder zu deaktivieren.
- **Priorität**
  Tragen Sie die Priorität des Ports ein. Die Priorität wird nur dann ausgewertet, wenn die Pfadkosten gleich sind.
  Der Wert muss durch 16 teilbar sein. Wenn der Wert nicht durch 16 teilbar ist, wird der Wert automatisch angepasst.
  Wertebereich: 0 - 240.
  Der Standardwert ist 128.
- **Kalk. Kosten**
  Tragen Sie in das Eingabefeld die Wege-Kostenberechnung ein. Wenn Sie hier 0 eintragen, wird im nächsten Feld "Pfadkosten" der automatisch ermittelte Wert angezeigt.
- **Pfadkosten**
  Die Pfadkosten von diesem Port zur Root-Bridge. Die Strecke mit dem geringsten Wert wird als Weg ausgewählt. Haben mehrere Ports eines Geräts den gleichen Wert, wird der Port mit der niedrigsten Portnummer ausgewählt.
  Wenn im Feld "Kalk. Kosten" der Wert "0" ist, so wird der automatisch ermittelte Wert angezeigt.
  Im anderen Fall wird der Wert des Feldes "Kalk. Kosten" angezeigt.
  Die Ermittlung der Wegekosten richtet sich maßgeblich nach der Übertragungsgeschwindigkeit. Je höher die erzielbare Übertragungsgeschwindigkeit ist, umso kleiner ist der Wert für die Wegekosten.
  Typische Werte für Wegekosten bei Rapid Spanning Tree:
  - 1000 Mbit/s = 20.000
  - 100 Mbit/s = 200.000
  - 10 Mbit/s = 2.000.000

  Die Werte können aber auch individuell parametriert werden.

- **Status**
  Zeigt den momentanen Status an, in dem sich der Port befindet. Die Werte werden nur angezeigt und können nicht konfiguriert werden. Beim Status ist Folgendes möglich:
  - Discarding
    Der Port tauscht MSTP-Informationen aus, nimmt aber nicht am Datenverkehr teil.
  - Blocked
    Im Blocking-Modus werden BPDU-Telegramme empfangen.
  - Forwarding
    Der Port empfängt und sendet Datentelegramme.
- **Fwd. Trans.**
  Gibt die Anzahl der Statuswechsel Discarding - Forwarding bzw. Forwarding - Discarding für einen Port an.

Vorgehensweise

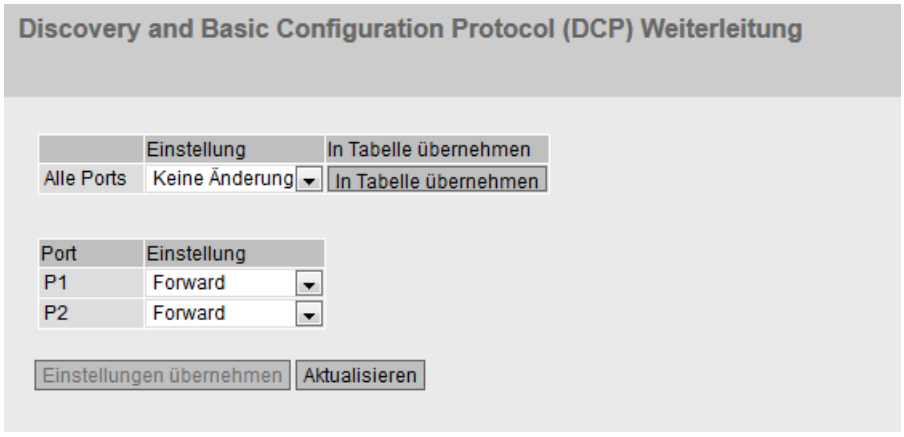
1. Tragen Sie in den Eingabefeldern der Tabellenzeile des zu konfigurierenden Ports die Werte ein.
2. Wählen Sie aus den Klapplisten der Felder der Tabellenzeile des zu konfigurierenden Ports die Werte aus.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.7.4 DCP-Weiterleitung

Anwendungen

Das DCP-Protokoll wird von STEP 7 und von SINEC PNI für die Konfiguration und Diagnose verwendet. In der Werkseinstellung ist DCP auf allen Ethernet-Schnittstellen aktiviert, d.h. empfangene DCP-Telegramme werden auf allen Ports weitergeleitet. Mit dieser Option haben Sie die Möglichkeit das Aussenden der Telegramme für einzelne Ports auszuschalten, um einzelne Netzbereiche von der Konfiguration per SINEC PNI abzuschotten, bzw. um das gesamte Netz in kleinere Teilnetze für die Konfiguration und Diagnose zu unterteilen.

Auf dieser WBM-Seite werden alle Ports des Geräts angezeigt.



Beschreibung

Die Tabelle 1 gliedert sich in folgende Spalten:

- **Spalte 1**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **Einstellung**
  Wählen Sie aus der Klappliste die Einstellung. Wenn "Keine Änderung" ausgewählt ist, bleibt der Eintrag in der Tabelle 2 unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt die verfügbaren Ethernet-Schnittstellen an.
- **Einstellung**
  Legen Sie fest, ob der Port die DCP-Telegramme ausgangsseitig blocken oder weiterleiten soll. Sie haben die folgenden Möglichkeiten zur Auswahl:
  - Forward
    An diesem Port werden DCP-Telegramme weitergeleitet.
  - Block
    An diesem Port werden ausgangsseitig keine DCP-Telegramme weitergeleitet. Ein Empfangen ist jedoch über diesen Port weiterhin möglich.

Vorgehensweise

1. Legen Sie fest, ob der gewünschte Port die DCP-Telegramme blockiert oder weiterleitet.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.7.5 LLDP

Bestimmung der Netzwerktopologie

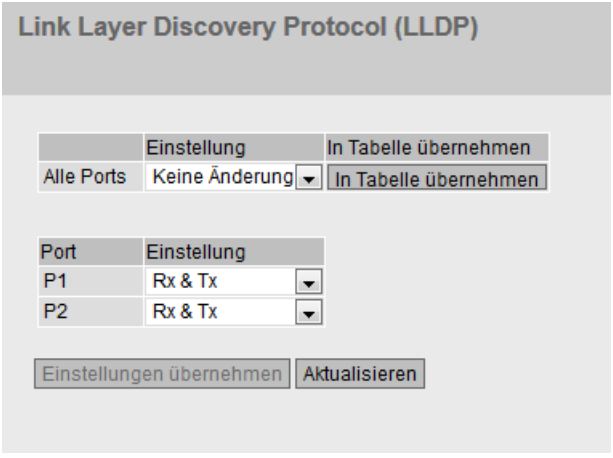
LLDP (Link Layer Discovery Protocol) ist im Standard IEEE 802.1 AB definiert.

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

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

Anwendungen

PROFINET benutzt LLDP für die Topologie-Diagnose. In der Werkseinstellung ist LLDP für alle Ports aktiviert, d. h. es werden LLDP-Telegramme auf allen Ports gesendet und empfangen. Mit dieser Funktion haben Sie die Möglichkeit das Aussenden und/oder Empfangen pro Port ein- oder auszuschalten.



Beschreibung

Tabelle 1 gliedert sich in folgende Spalten:

- **Alle Ports**
  Zeigt an, dass die Einstellungen für alle Ports gültig sind.
- **Einstellung**
  Wählen Sie aus der Klappliste die Einstellung. Wenn "Keine Änderung" ausgewählt ist, bleibt der Eintrag in der Tabelle 2 unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt den Port an.
- **Einstellung**
  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

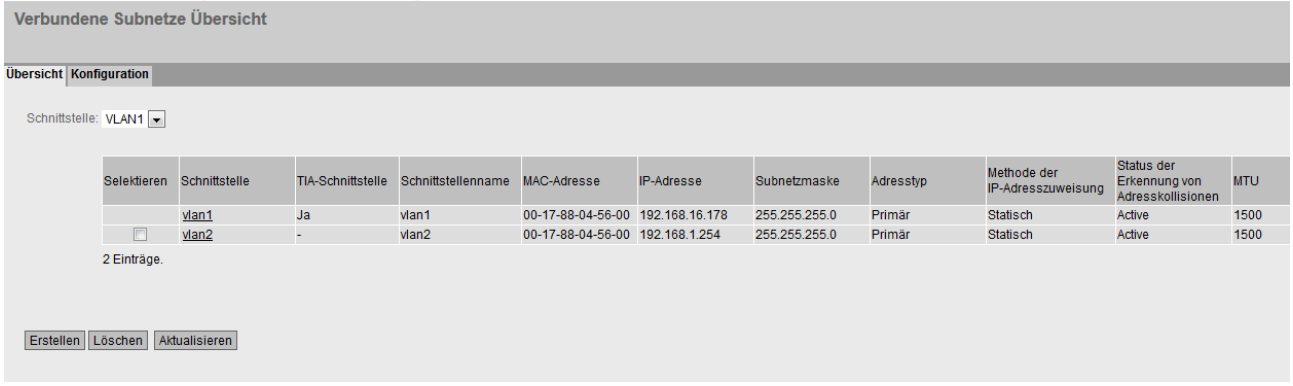
1. Wählen Sie in der Klappliste die gewünschte LLDP-Funktionalität aus.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.8 Menü "Layer 3 (IPv4)"

6.8.1 Subnetze

6.8.1.1 Übersicht

Die Seite zeigt die Subnetze für die ausgewählte VLAN-Schnittstelle an. Diese VLAN-Schnittstelle wird auch als IPv4-Schnittstelle bezeichnet. Ein Subnetz bezieht sich immer auf eine IPv4-Schnittstelle. Die IPv4-Adresse wird in dem Register "Konfiguration" zugeordnet.



Beschreibung

Die Seite enthält folgende Felder:

- **Schnittstelle**
  Wählen Sie die gewünschte Schnittstelle aus, an die Sie das Subnetz projektieren.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Schnittstelle**
  Zeigt die Schnittstelle an.
- **TIA-Schnittstelle**
  Zeigt die ausgewählte TIA-Schnittstelle an.
- **Status**
  Zeigt den Status der Schnittstelle an.
- **Schnittstellenname**
  Zeigt den Namen der Schnittstelle.
- **MAC-Adresse**
  Zeigt die MAC-Adresse an.
- **IP-Adresse**
  Zeigt die IPv4-Adresse des Subnetzes an.
- **Subnetzmaske**
  Zeigt die Subnetzmaske.
- **Adresstyp**
  Zeigt den Adressentyp an. Folgende Werte sind möglich:
  - Primär
    Die erste IPv4-Adresse, die auf einer IPv4-Schnittstelle konfiguriert wurde.
  - Sekundär
    Alle weiteren IPv4-Adressen, die auf einer IPv4-Schnittstelle konfiguriert wurden.
- **Methode der IP-Adresszuweisung**
  Zeigt an, wie die IPv4-Adresse zugeordnet wird. Folgende Werte sind möglich:
  - Statisch
    Die IPv4-Adresse ist statisch. Tragen Sie die Einstellungen bei "IP-Adresse" und "Subnetzmaske" ein.
  - Dynamisch (DHCP)
    Das Gerät bezieht eine dynamische IPv4-Adresse von einem DHCPv4-Server.

- **Status der Erkennung von Adresskollisionen**
  Wenn neue IPv4-Adressen im Netz aktiv werden, prüft die Funktion "Erkennung von Adresskollisionen ", ob es zu Adresskollisionen kommen kann. Dadurch werden IPv4-Adressen erkannt, die doppelt vergeben werden sollen.

  Hinweis

  Die Funktion führt keine zyklische Prüfung durch.

  Diese Spalte zeigt an, in welchem Status sich die Funktion befindet. Folgende Werte sind möglich:

  – Idle
    Die Schnittstelle ist nicht aktiv und besitzt keine IPv4-Adresse.
  – Starting
    Dieser Status bezeichnet die Anlaufphase. In dieser Phase sendet das Gerät zunächst eine Anfrage, ob es die geplante IPv4-Adresse bereits gibt. Wenn die Adresse noch nicht vergeben ist, sendet das Gerät die Mitteilung, dass es ab jetzt diese IP-Adresse verwendet.
  – Conflict
    Die Schnittstelle ist nicht aktiv. Die Schnittstelle versucht eine IPv4-Adresse zu verwenden, die bereits vergeben ist.
  – Defending
    Die Schnittstelle verwendet eine eindeutige IPv4-Adresse. Eine andere Schnittstelle versucht die gleiche IPv4-Adresse zu verwenden.
  – Active
    Die Schnittstelle verwendet eine eindeutige IPv4-Adresse. Es gibt keine Kollisionen.
  – Not supported
    Die Funktion zur Erkennung von Adresskollisionen wird nicht unterstützt.
  – Disabled
    Die Funktion zur Erkennung von Adresskollisionen ist deaktiviert.

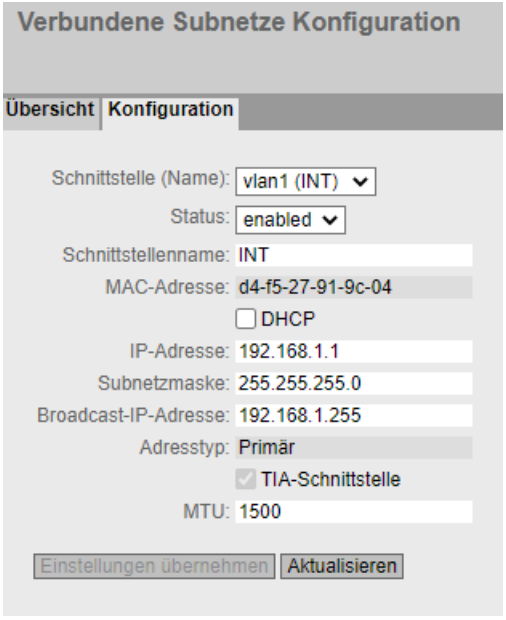
- **MTU**
  Zeigt die Paketgröße an.

Vorgehensweise

1. Wählen Sie in der Klappliste "Schnittstelle" die VLAN-Schnittstelle aus.
2. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird eine neue Zeile eingefügt.
3. Konfigurieren Sie das Subnetz auf dem Register "Konfiguration".

6.8.1.2 Konfiguration

Auf dieser Seite konfigurieren Sie die IPv4-Schnittstelle.



Beschreibung

Die Seite enthält folgende Felder:

- **Schnittstelle (Name)**
  Wählen Sie in der Klappliste die Schnittstelle aus.
- **Status**
  Legen Sie fest, ob die Schnittstelle ein- oder ausgeschaltet ist.
  - Enabled
    Die Schnittstelle ist eingeschaltet. Datenverkehr ist nur über eine eingeschaltete Schnittstelle möglich.
  - Disabled
    Die Schnittstelle ist ausgeschaltet.
- **Schnittstellenname**
  Tragen Sie den Namen für die Schnittstelle ein.
- **MAC-Adresse**
  Zeigt die MAC-Adresse der ausgewählten Schnittstelle an.
- **DHCP**
  Aktivieren oder deaktivieren Sie den DHCP-Client für dieses IPv4-Schnittstelle.
- **IP-Adresse**
  Tragen Sie die IPv4-Adresse der Schnittstelle ein. Die IPv4-Adressen dürfen nicht mehrfach verwendet werden.

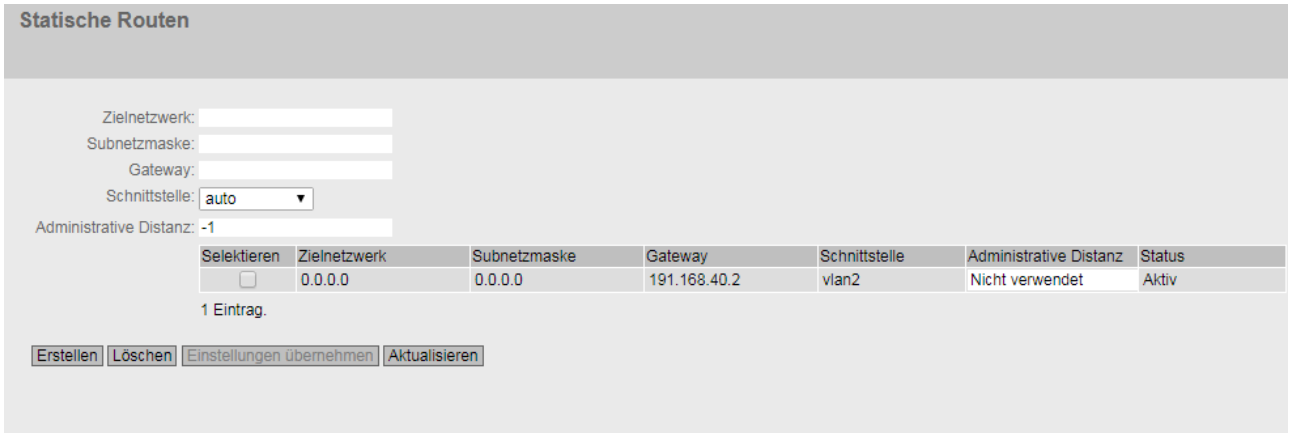
- **Subnetzmaske**
  Tragen Sie die Subnetzmaske des zu erstellenden Subnetzes ein. Subnetze an unterschiedlichen Schnittstellen dürfen sich nicht überlappen.
- **Adresstyp**
  Zeigt den Adressen Typ an.
  - Primär
    Das erste Subnetz der Schnittstelle.
- **TIA-Schnittstelle**
  Wählen Sie aus, ob diese Schnittstelle zur TIA-Schnittstelle werden soll. Über die TIA-Schnittstelle wird definiert, auf welchem VLAN die PROFINET Funktionalitäten zur Verfügung stehen. Dies betrifft hauptsächlich die Gerätesuche mit oder über DCP.
- **MTU**
  Mit MTU (Maximum Transmission Unit) wird die maximale Größe des Pakets festgelegt. Wenn die Pakete größer sind als die eingestellte MTU, werden Sie fragmentiert. Die MTU deckt die IP-Header und die Header der höheren Schichten (Layer) ab.
  Wertebereich:
  - Bei IPv4: 90 ... 1514
  - Bei IPv6: 1280 ... 1514

Vorgehensweise

1. Wählen Sie in der Klappliste "Schnittstelle (Name)" die Schnittstelle aus.
2. Wählen Sie in der Klappliste "Status" den Status der Schnittstelle aus.
3. Tragen Sie in bei "Schnittstellenname" einen Namen für die Schnittstelle ein.
4. Tragen Sie in der Spalte "IP-Adresse" die IPv4-Adresse des Subnetzes ein oder aktivieren Sie die Option "DHCP".
5. Tragen Sie in der Spalte "Subnetzmaske" die zur IPv4-Adresse gehörende Subnetzmaske ein.
6. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.8.2 Statische Routen

Auf dieser Seite legen Sie fest, über welche Routen ein Datenaustausch zwischen den verschiedenen Subnetzen stattfinden kann. Dynamische Routingprotokolle werden nicht unterstützt, z. B. RIP, OSPF.



Beschreibung

Die Seite enthält folgende Felder:

- **Zielnetzwerk**
  Tragen Sie die Netzwerkadresse des Ziels ein, das über diese Route erreichbar ist.
- **Subnetzmaske**
  Tragen Sie die dazugehörende Subnetzmaske ein.
- **Gateway**
  Tragen Sie die IPv4-Adresse des Gateways ein, über den diese Netzwerkadresse erreichbar ist.
- **Schnittstelle**
  Legen Sie fest, ob die Netzwerkadresse über eine bestimmte Schnittstelle oder über das Gateway (auto) erreichbar ist.
- **Administrative Distanz**
  Tragen Sie die Metrik für die Route ein. Die Metrik entspricht der Güte einer Verbindung, z. B. Geschwindigkeit, Kosten. Bei mehreren gleichen Routen wird die Route mit dem kleinsten Metrik-Wert benutzt.
  Wenn Sie nicht eintragen, wird automatisch "nicht verwendet" eingetragen. Die Metrik ist nachträglich änderbar.
  Wertebereich: 1 - 255 oder -1 für "not used".
  Dabei ist 1 der Wert für die bestmögliche Route. Je größer der Wert, desto länger benötigen Pakete zu Ihrem Ziel.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Zielnetzwerk**
  Zeigt die Netzwerkadresse des Ziels an.

- **Subnetzmaske**
  Zeigt die dazugehörende Subnetzmaske an.
- **Gateway**
  Zeigt die IPv4-Adresse des nächsten Gateways an.
- **Schnittstelle**
  Zeigt die Schnittstelle der Route an.
- **Administrative Distanz**
  Tragen Sie die Metrik für die Route ein. Beim Erstellen der Route wird automatisch "nicht verwendet" eingetragen. Die Metrik entspricht der Güte einer Verbindung, basierend z. B. auf Geschwindigkeit oder Kosten. Bei mehreren gleichen Routen wird die Route mit dem kleinsten Metrik-Wert benutzt.
  Wertebereich: 1 - 255
  Dabei ist 1 der Wert für die bestmögliche Route. Je größer der Wert, desto länger benötigen die Pakete zu Ihrem Ziel.
- **Status**
  Zeigt an, ob die Route aktiv ist oder nicht.

Vorgehensweise

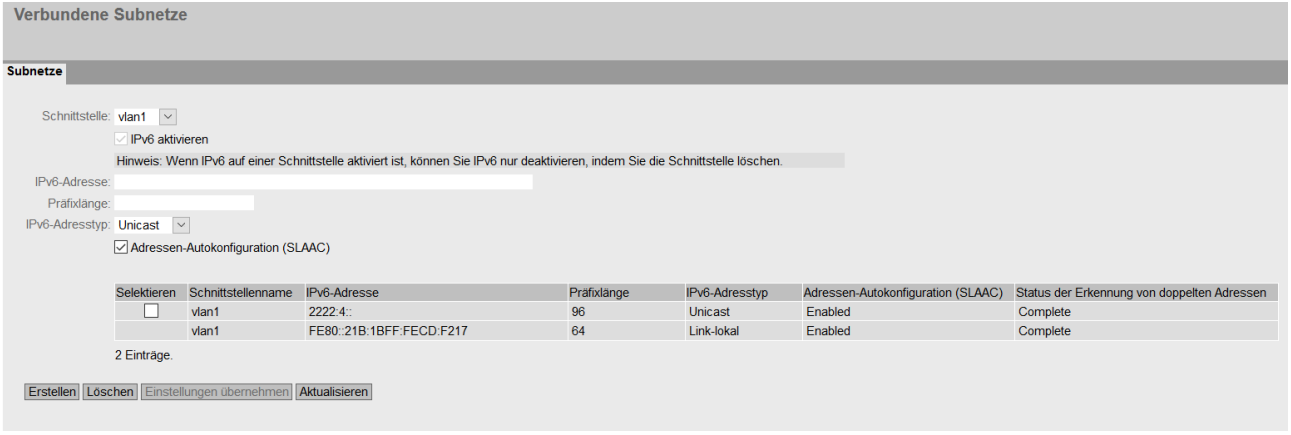
1. Tragen Sie in das Eingabefeld "Zielnetzwerk" die Netzwerkadresse des Ziels ein.
2. Tragen Sie in das Eingabefeld "Subnetzmaske" die dazugehörende Subnetzmaske ein.
3. Wählen Sie bei "Schnittstelle" den Eintrag "auto" aus.
4. Tragen Sie in das Eingabefeld "Gateway" das Gateway ein.
5. Tragen Sie bei "Administrative Distanz" die Gewichtung der Route ein.
6. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag erzeugt.
7. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.9 Menü "Layer 3 (IPv6)"

6.9.1 Subnetze

Konfiguration der IP-Adressen

Auf dieser Seite aktivieren Sie IPv6 an der VLAN-Schnittstelle. Diese VLAN-Schnittstelle wird auch als IPv6-Schnittstelle bezeichnet. Eine IPv6-Schnittstelle kann mehrere IPv6-Adressen haben.



Beschreibung

Die Seite enthält Folgendes:

- **Schnittstelle**
  Zeigt die VLAN-Schnittstelle an, an der IPv6 aktiviert wird.
- **IPv6 aktivieren**
  Aktivieren oder deaktivieren Sie IPv6 auf der Schnittstelle. Wenn Sie die Einstellung aktivieren und die Einstellung übernehmen, wird automatisch die link-lokale Adresse erstellt.
- **IPv6-Adresse**
  Geben Sie die IPv6-Adresse an. Die Eingabe ist abhängig vom gewählten Adresstyp.
- **Präfixlänge**
  Geben Sie die Anzahl der linksseitigen Bits an, die dem Präfix angehören.
- **IPv6-Adresstyp**
  Wählen Sie den Adresstyp aus:
  - Unicast
  - Link-lokal: IPv6-Adresse ist nur auf dem Link gültig.

- **Adresskonfiguration**
  Legen Sie den Mechanismus für die Adresskonfiguration fest:
  - Automatisch (Default)
    Die IPv6-Adresse wird entweder über einen zustandslosen Mechanismus oder einen zustandsbehafteten Mechanismus erstellt.
  - DHCPv6
    Zustandsbehaftet: Bezieht die IPv6-Adresse und die Konfigurationsdatei vom DHCPv6-Server.
  - SLAAC (Stateless Address Auto Configuration)
    Zustandslose Autokonfiguration über NDP (Neighbor Discovery Protocol.
  - Statisch
    Geben Sie eine statische IPv6-Adresse ein.
- **DHCPv6 Rapid Commit**
  Wenn aktiviert, wird das Verfahren für die IPv6-Adresszuweisung verkürzt. Anstatt 4 DHCPv6-Nachrichten (SOLICIT, ADVERTISE , REQUEST, REPLY) werden nur 2 DHCPv6-Nachrichten (SOLICIT, REPLY) verwendet. Weitere Informationen zu den Nachrichten finden Sie in der RFC 3315.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Schnittstellenname**
  Zeigt den Namen der VLAN-Schnittstelle an.
- **IPv6-Adresse**
  Zeigt die IPv6-Adresse an.
- **Präfixlänge**
  Zeigt die Präfixlänge an.

- **IPv6-Adresstyp**
  Zeigt den Adressentyp an. Folgende Werte sind möglich:
  - Unicast
  - Link-lokal
- **Status der Erkennung von doppelten Adressen**
  Bei der Adressen-Autokonfiguration (SLAAC) verhindert die Funktion "Status der Erkennung von doppelten Adressen", dass IPv6-Adressen doppelt vergeben werden. Das Gerät darf bei der Autokonfiguration nur freie IPv6-Adressen verwenden.
  Wenn die Funktion aktiviert ist, läuft die Prüfung über NDP automatisch ab.

  Hinweis

  Die Funktion führt keine zyklische Prüfung durch.

  Diese Spalte zeigt an, in welchem Status sich die Funktion befindet. Folgende Werte sind möglich:
  - Tentative
    Dieser Status zeigt an, dass die ausgewählte IPv6-Adresse geprüft wird. Das Gerät sendet eine Neighbor Solicitation-Nachricht an die ausgewählte IPv6-Adresse.
  - Conflict
    Dieser Status zeigt an, die IPv6-Adresse bereits verwendet wird. Das Gerät erhält in diesem Fall eine Neighbor-Advertisement-Nachricht mit der ausgewählten IPv6-Adresse zurück. Das Gerät bildet eine neue IPv6-Adresse und prüft diese erneut.
  - Complete
    Dieser Status zeigt an, dass die ausgewählte IPv6-Adresse verwendet werden kann. Das Gerät hat in diesem Fall innerhalb einer Zeitspanne keine Rückmeldung erhalten und geht davon aus, dass die IPv6-Adresse noch nicht vergeben ist.
  - Down
    Dieser Status zeigt an, dass die Schnittstelle nicht aktiv ist. Es wird keine Prüfung durchgeführt.

Vorgehensweise

Link-lokale Adresse automatisch bilden

1. Aktivieren Sie IPv6.
2. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein Eintrag mit der Schnittstelle erstellt und die automatisch gebildete link-lokale IPv6-Adresse wird angezeigt.

Link-lokale Adresse zuweisen

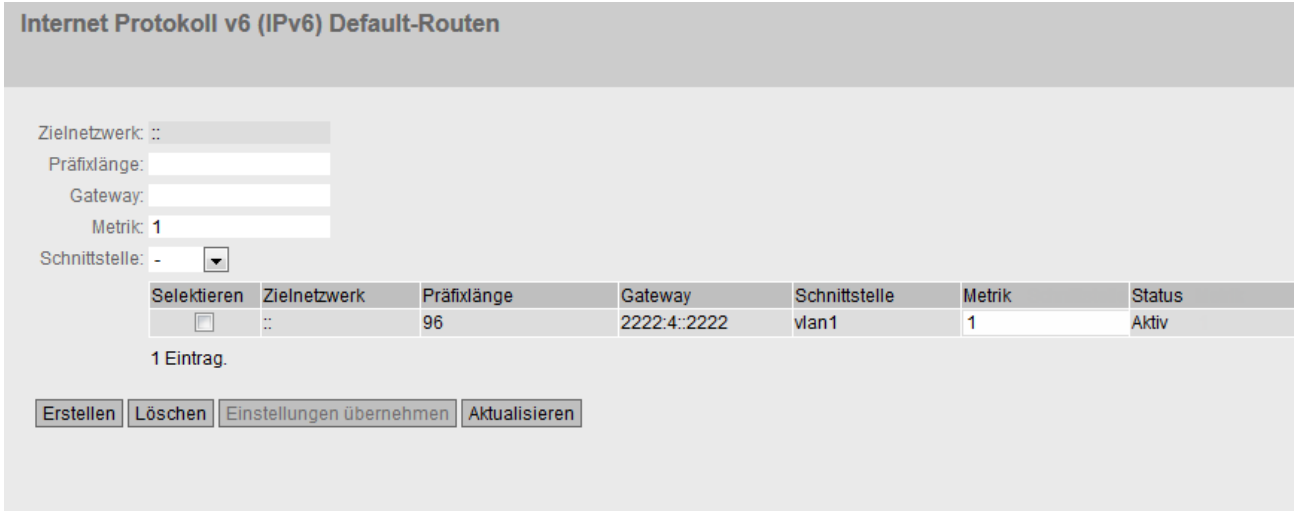
1. Aktivieren Sie IPv6.
2. Geben Sie bei "IPv6-Adresse" die link-lokale Adresse ein, z. B. FE80::21B:1BFF:FE40:9155
3. Geben Sie bei "Präfixlänge" "128" ein.
4. Wählen Sie bei "IPv6-Adresstyp" den Eintrag "Link-lokal" aus.

5. Wählen Sie bei "Adresskonfiguration" den Eintrag "Statisch" aus.
6. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein Eintrag mit der Schnittstelle erstellt und die IPv6-Adresse wird angezeigt.
   Die automatisch erstellte link-lokale Adresse wird überschrieben.

6.9.2 Statische Routen

Auf dieser Seite konfigurieren Sie die IPv6-Defaultroute. Die IPv6-Defaultroute ist eine IPv6-Route, die für alle IPv6-Adressen zutrifft. Das Gerät muss nur das Default-Gateway kennen und schickt alle IPv6-Pakete dahin.

Das Default-Gateway kennt entweder selbst alle Routen oder hat eine Default-Route zu einem weiteren Default-Gateway.



Beschreibung

Die Seite enthält Folgendes:

- **Zielnetzwerk**
  Das Zielnetzwerk (:: oder 0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0) gilt für alle IPv6-Adressen.
- **Präfixlänge**
  Geben Sie die Anzahl der linksseitigen Bits an, die dem Präfix angehören.
- **Gateway**
  Geben Sie die IPv6-Adresse des Gateways ein, an den die IPv6-Pakete gesendet werden.
- **Metrik**
  Geben Sie die Metrik für die Route ein. Die Metrik entspricht der Güte einer Verbindung, basierend z. B. auf Geschwindigkeit oder Kosten. Bei mehreren gleichen Routen wird die Route mit dem kleinsten Metrik-Wert benutzt.
  Wertebereich: 1 - 254
- **Schnittstelle**
  Legen Sie die Schnittstelle fest, über die die Netzwerkadresse des Ziels erreicht wird.

Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Zielnetzwerk**
  Zeigt die Netzwerkadresse des Ziels an.
- **Präfixlänge**
  Zeigt die Präfixlänge an.
- **Gateway**
  Zeigt die IPv6-Adresse des nächsten Gateways an.
- **Schnittstelle**
  Zeigt die Schnittstelle der Route an.
- **Metrik**
  Tragen Sie die Metrik für die Route ein. Beim Erstellen der Route wird automatisch "not used" eingetragen. Die Metrik entspricht der Güte einer Verbindung, basierend z. B. auf Geschwindigkeit oder Kosten. Bei mehreren gleichen Routen wird die Route mit dem kleinsten Metrik-Wert benutzt.
  Wertebereich: 1 - 254
- **Status**
  Zeigt an, ob die Route aktiv ist oder nicht.

Vorgehensweise zur Konfiguration

1. Geben Sie die Präfixlänge ein.
2. Geben Sie IPv6-Adresse des Gateways ein.
3. Geben Sie die Metrik der Route ein.
4. Wählen Sie die Schnittstelle aus, über die die Netzwerkadresse des Ziels erreicht wird.
5. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag erzeugt.

6.10 Menü "Security"

6.10.1 Benutzer

6.10.1.1 Lokale Benutzer

Lokale Benutzer

Auf dieser Seite erstellen Sie lokale Benutzer mit den entsprechenden Rechten.

Wenn Sie einen lokalen Benutzer anlegen oder löschen, wird diese Änderung automatisch auch in der Tabelle "Externe Benutzerkonten" durchgeführt. Wenn Sie eine Änderung explizit für die interne oder externe Benutzertabelle durchführen wollen, nutzen Sie die CLI-Befehle.

Hinweis

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

Beschreibung

Die Seite enthält Folgendes:

- **Benutzerkonto**
  Geben Sie den Namen für den Benutzer ein. Der Name muss folgende Bedingungen erfüllen:
  - Er muss eindeutig sein.
  - Er muss zwischen 1 und 250 Zeichen lang sein.
  - Er darf folgende Zeichen nicht enthalten: :;"|€´?§^{32o}µ ä ö ü Ä Ö Ü
    Die Zeichen für Space und Delete dürfen auch nicht enthalten sein.

Hinweis

Benutzername nicht änderbar

Nach dem Anlegen eines Benutzers kann der Benutzername nicht mehr geändert werden.

Wenn ein Benutzername geändert werden soll, muss der Benutzer gelöscht und ein neuer Benutzer angelegt werden.

Hinweis

Benutzernamen: admin

Mit diesem Benutzernamen können Sie das Gerät konfigurieren.

Wenn Sie sich das erste Mal oder nach einem "Auf Werkseinstellungen zurücksetzen und Neustart" anmelden, werden Sie aufgefordert das vordefinierte Passwort "admin" zu ändern. Zusätzlich können Sie einmalig den werksseitig voreingestellten Benutzer "admin" umbenennen. Danach ist ein Umbenennen von "admin" nicht mehr möglich.

- **Passwortrichtlinie**
  Zeigt an, welche Passwortrichtlinie verwendet wird:
  - Hoch
    Passwortlänge: mindestens 8 Zeichen, maximal 128 Zeichen
    Mindestens 1 Großbuchstabe
    Mindestens 1 Sonderzeichen
    Mindestens 1 Zahl
  - Niedrig
    Passwortlänge: mindestens 6 Zeichen, maximal 128 Zeichen
  - Benutzerdefiniert
    Sie konfigurieren die Passwortrichtlinie auf der Seite "Security > Passwörter > Optionen".
- **Passwort**
  Geben Sie das Passwort an. Die Stärke des Passworts ist abhängig von dessen Länge und Komplexität.
  - Er darf folgende Zeichen nicht enthalten: ; : ' ? ß § " ² ³ ° | € µ ä ö ü Ä Ö Ü
  - Die Zeichen für Space und Delete dürfen auch nicht enthalten sein.

- **Passwort bestätigen**
  Geben Sie das Passwort erneut ein, um es zu bestätigen.
- **Rolle**
  Wählen Sie eine Rolle aus.
  Sie können zwischen den voreingestellten und selbst definierten Rollen wählen, siehe Seite "Security > Benutzer > Rollen".

Die Tabelle enthält folgende Spalten:

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

  Hinweis

  Die voreingestellten Benutzer sowie angemeldete Benutzer können nicht gelöscht oder geändert werden.

- **Benutzerkonto**
  Zeigt den Benutzernamen an.
- **Rolle**
  Zeigt die Rolle des Benutzers an.
- **Beschreibung**
  Zeigt eine Beschreibung des Benutzerkontos an. Der Beschreibungstext kann bis zu 100 Zeichen lang sein.

Vorgehensweise

Hinweis

Änderungen im Modus "Trial"

Auch wenn sich das Gerät im Modus "Trial" befindet, werden Änderungen, die Sie auf dieser Seite durchführen, sofort gespeichert.

Benutzer anlegen

1. Geben Sie den Namen für den Benutzer ein.
2. Geben Sie das Passwort für den Benutzer ein.
3. Geben Sie das Passwort erneut ein, um es zu bestätigen.
4. Wählen Sie die Rolle des Benutzers aus.
5. Klicken Sie auf die Schaltfläche "Erstellen".
6. Geben Sie eine Beschreibung des Benutzers ein.
7. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Benutzer löschen

1. Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
2. Klicken Sie auf die Schaltfläche "Löschen". Die Einträge werden gelöscht und die Seite wird aktualisiert.

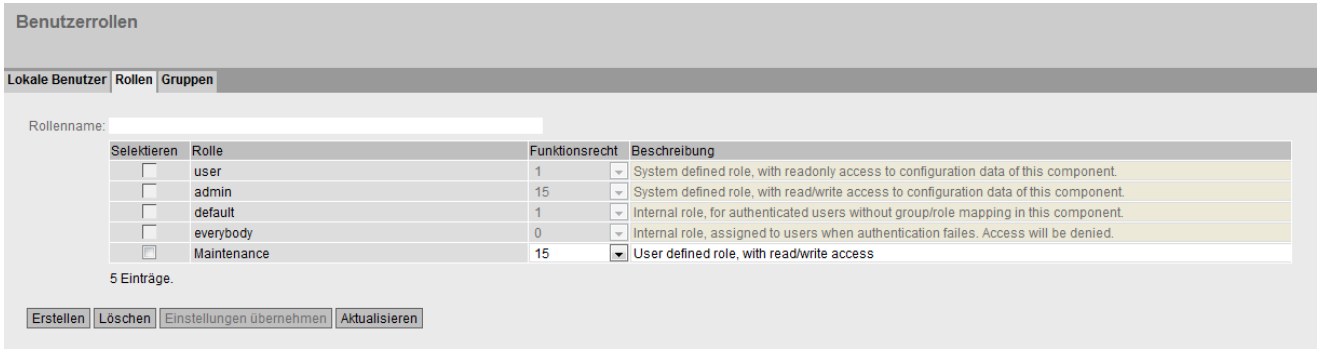
6.10.1.2 Rollen

Rollen

Auf dieser Seite erstellen Sie Rollen, die lokal auf dem Gerät gültig sind.

Hinweis

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



Beschreibung

Die Seite enthält Folgendes:

- **Rollenname**
  Geben Sie den Namen für die Rolle ein. Der Name muss folgende Bedingungen erfüllen:
  - Er muss eindeutig sein.
  - Er muss zwischen 1 und 64 Zeichen lang sein.

  Hinweis

  Rollenname nicht änderbar

  Nach dem Anlegen einer Rolle kann der Rollenname nicht mehr geändert werden.

  Wenn ein Rollenname geändert werden soll, muss die Rolle gelöscht und eine neue Rolle angelegt werden.

Die Tabelle enthält folgende Spalten:

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

  Hinweis

  Die voreingestellten Rollen sowie zugewiesene Rollen können nicht gelöscht oder geändert werden.

- **Rolle**
  Zeigt den Namen der Rolle an.

- **Funktionsrecht**
  Wählen Sie die Funktionsrechte der Rolle aus:
  - **0**
    Wenn die Authentifizierung fehlschlägt, wird dem Benutzer die Rolle zugewiesen. Ein Zugriff auf das Gerät ist nicht möglich.
  - **1**
    Benutzer mit dieser Rolle können Geräteparameter lesen aber nicht verändern. Benutzer mit dieser Rolle können ihr eigenes Passwort ändern.
  - **15**
    Benutzer mit dieser Rolle können Geräteparameter sowohl lesen als auch verändern.

  Hinweis

  Funktionsrecht nicht änderbar

  Wenn Sie eine Rolle zugewiesen haben, können Sie das Funktionsrecht der Rolle nicht mehr ändern.

  Wenn Sie das Funktionsrecht einer Rolle ändern wollen, gehen Sie wie folgt vor:
  1. Löschen Sie alle zugewiesenen Benutzer.
  2. Ändern Sie das Funktionsrecht der Rolle.
  3. Weisen Sie die Rolle erneut zu.

- **Beschreibung**
  Geben Sie eine Beschreibung für die Rolle ein. Bei vordefinierten Rollen wird eine Beschreibung angezeigt. Der Beschreibungstext kann bis zu 100 Zeichen lang sein.

Vorgehensweise

Rolle anlegen

1. Geben Sie den Namen für die Rolle ein.
2. Klicken Sie auf die Schaltfläche "Erstellen".
3. Wählen Sie die Funktionsrechte der Rolle aus.
4. Geben Sie eine Beschreibung der Rolle ein.
5. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Rolle löschen

1. Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
2. Klicken Sie auf die Schaltfläche "Löschen". Die Einträge werden gelöscht und die Seite wird aktualisiert.

6.10.1.3 Gruppen

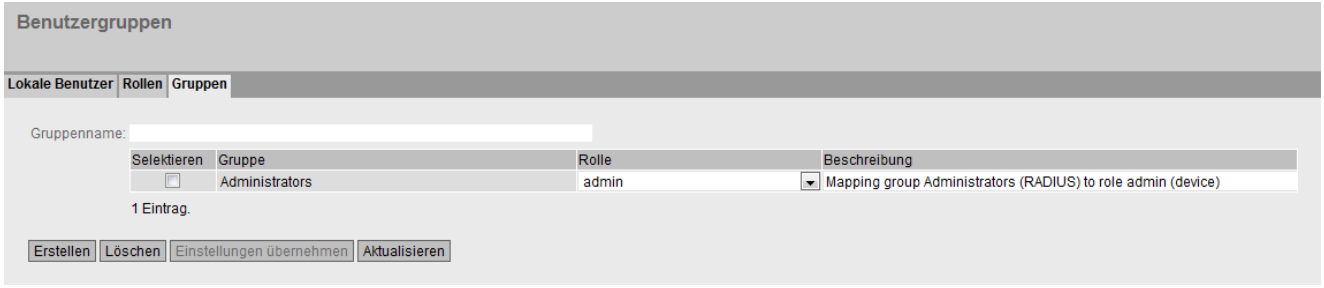
Benutzergruppen

Auf dieser Seite verknüpfen Sie eine Gruppe mit einer Rolle.

In diesem Beispiel wird die Gruppe "Administrators" mit der Rolle "admin" verknüpft. Die Gruppe ist auf einem RADIUS-Server definiert. Die Rolle ist lokal auf dem Gerät definiert. Wenn ein RADIUS-Server einen Benutzer authentifiziert und der Gruppe "Administrators" zuordnet, erhält dieser Benutzer auf dem Gerät die Rechte der Rolle "admin".

Hinweis

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



Beschreibung

Die Seite enthält Folgendes:

- **Gruppenname**
  Geben Sie den Namen der Gruppe ein. Der Name muss der Gruppe auf dem RADIUS-Server entsprechen.
  Der Name muss folgende Bedingungen erfüllen:
  - Er muss eindeutig sein.
  - Er muss zwischen 1 und 64 Zeichen lang sein.
  - Nicht erlaubt sind: § ? " ; :

Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Gruppe**
  Zeigt den Namen der Gruppe an.
- **Rolle**
  Wählen Sie eine Rolle aus. Benutzer, die über den RADIUS-Server mit der verknüpften Gruppe authentifiziert werden, erhalten die Rechte dieser Rolle lokal auf dem Gerät.
  Sie können zwischen den voreingestellten und selbst definierten Rollen wählen, siehe Seite "Security > Benutzer > Rollen".
- **Beschreibung**
  Geben Sie eine Beschreibung für die Verknüpfung der Gruppe mit einer Rolle an. Der Beschreibungstext kann bis zu 100 Zeichen lang sein.

Vorgehensweise

Eine Gruppe mit einer Rolle verknüpfen

1. Geben Sie den Namen einer Gruppe ein.
2. Klicken Sie auf die Schaltfläche "Erstellen".
3. Wählen Sie eine Rolle aus.
4. Geben Sie eine Beschreibung für die Verknüpfung einer Gruppe mit einer Rolle ein.
5. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Die Verknüpfung zwischen einer Gruppe und einer Rolle löschen

1. Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
2. Klicken Sie auf die Schaltfläche "Löschen". Die Einträge werden gelöscht und die Seite wird aktualisiert.

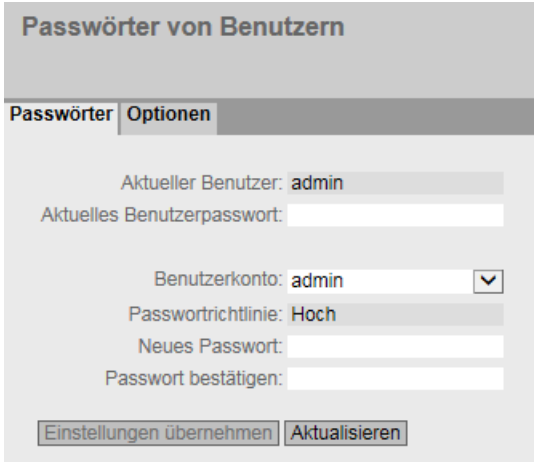
6.10.2 Passwörter

Konfiguration der Passwörter

Hinweis

Wenn Sie über einen RADIUS-Server angemeldet sind, können Sie keine Passwörter ändern.

Auf dieser Seite können Sie Passwörter ändern. Wenn Sie mit dem Recht zum Verändern von Geräteparametern angemeldet sind, können Sie die Passwörter für alle Benutzeraccounts ändern. Wenn Sie als User angemeldet sind, können Sie nur Ihr eigenes Passwort ändern.



Beschreibung der angezeigten Felder

- **Aktueller Benutzer**
  Zeigt den Benutzer an, der aktuell angemeldet ist.
- **Aktuelles Benutzerpasswort**
  Geben Sie das Passwort des aktuell angemeldeten Benutzers ein.
- **Benutzerkonto**
  Wählen Sie den Benutzer, dessen Passwort Sie ändern möchten.
- **Passwortrichtlinie**
  Zeigt an, welche Passwortrichtlinie bei der Vergabe von neuen Passwörtern verwendet wird.

  Hinweis

  Passwortrichtlinie von bereits bestehenden Benutzern

  Die eingestellte Passwortrichtlinie wird bei der Vergabe von neuen Passwörtern angewendet. Bestehende Passwörter werden nicht überprüft. Wenn Sie die Passwortrichtlinie von "Niedrig" nach "Hoch" ändern, bleiben die bisher verwendeten Passwörter gültig. Als wichtige Maßnahme zur Erhöhung der Sicherheit ändern Sie die bisher verwendeten Passwörter.

  – Hoch
    Passwortlänge: mindestens 8 Zeichen, maximal 128 Zeichen
    Mindestens 1 Großbuchstabe
    Mindestens 1 Sonderzeichen
    Mindestens 1 Zahl
  – Niedrig
    Passwortlänge: mindestens 6 Zeichen, maximal 128 Zeichen
  – Benutzerdefiniert
    Sie konfigurieren die Passwortrichtlinie auf der Seite "Security > Passwörter > Optionen".
- **Neues Passwort**
  Geben Sie das neue Passwort für den ausgewählten Benutzer ein.
  – Er darf folgende Zeichen nicht enthalten: ; : ' ? ß § " ² ³ ° | € µ ä ö ü Ä Ö Ü
  – Die Zeichen für Space und Delete dürfen auch nicht enthalten sein.
- **Passwort bestätigen**
  Geben Sie das neue Passwort erneut ein, um es zu bestätigen.

Vorgehensweise

1. Wählen Sie in der Klappliste "Benutzerkonto" den Benutzer aus, für den das Passwort geändert werden soll.
2. Geben Sie in das Eingabefeld "Aktuelles Benutzerpasswort" das gültige Passwort des aktuell angemeldeten Benutzers ein.
3. Geben Sie in das Eingabefeld "Neues Passwort" das neue Passwort für den ausgewählten Benutzer ein.

4. Wiederholen Sie das neue Passwort im Eingabefeld "Passwort bestätigen".
5. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Hinweis

Werksseitig sind die Passwörter bei Auslieferung des Geräts wie folgt eingestellt:

- admin: admin

Wenn Sie sich das erste Mal oder nach einem "Auf Werkseinstellungen zurücksetzen und Neustart" mit dem voreingestellten Benutzer "admin" anmelden, werden Sie aufgefordert das Passwort zu ändern.

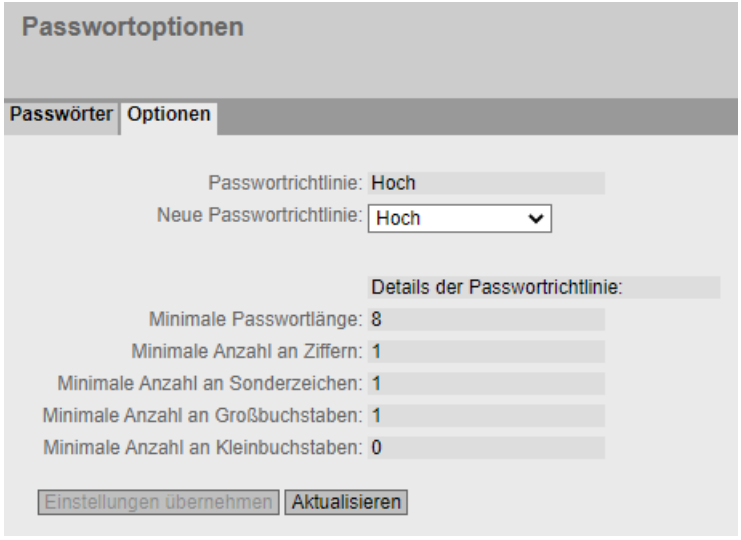
Hinweis

Passwort ändern im Trial-Modus

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

6.10.2.1 Passwortoptionen

Auf dieser Seite legen Sie fest, welche Passwortrichtlinie bei der Vergabe von neuen Passwörtern beachtet wird.



Beschreibung

- **Passwortrichtlinie**
  Zeigt an, welche Passwortrichtlinie aktuell verwendet wird.
- **Neue Passwortrichtlinie**
  Wählen Sie aus der Klappliste die gewünschte Einstellung aus:
  - Hoch
    Passwortlänge: mindestens 8 Zeichen, maximal 128 Zeichen
    Mindestens 1 Ziffer
    Mindestens 1 Sonderzeichen
    Mindestens 1 Großbuchstabe
  - Niedrig
    Passwortlänge: mindestens 6 Zeichen, maximal 128 Zeichen
  - Benutzerdefiniert
    Konfigurieren Sie unter "Details der Passwortrichtlinie" die gewünschten Anforderungen an Passwörter.
- **Details der Passwortrichtlinie**
  Wenn Sie die Passwortrichtlinie "Hoch" oder "Niedrig" ausgewählt haben, werden die jeweiligen Anforderungen an Passwörter angezeigt.
  Wenn Sie die Passwortrichtlinie "Benutzerdefiniert" ausgewählt haben, können Sie die Anforderungen an Passwörter konfigurieren.
  - Minimale Passwortlänge
    Gibt an, wie lang ein Passwort mindestens sein muss.
  - Minimale Anzahl an Ziffern
    Gibt an, wie viele Ziffern ein Passwort mindestens enthalten muss.
  - Minimale Anzahl an Sonderzeichen
    Gibt an, wie viele Sonderzeichen ein Passwort mindestens enthalten muss.
  - Minimale Anzahl an Großbuchstaben
    Gibt an, wie viele Großbuchstaben ein Passwort mindestens enthalten muss.
  - Minimale Anzahl an Kleinbuchstaben
    Gibt an, wie viele Kleinbuchstaben ein Passwort mindestens enthalten muss.

6.10.3 AAA

6.10.3.1 Allgemein

Anmeldung von Netzteilnehmern

Die verwendete Bezeichnung "AAA" steht für "Authentication, Authorization, Accounting". Dieses Feature dient dazu, Netzteilnehmer zu identifizieren und zuzulassen, ihnen die entsprechenden Dienste bereitzustellen und den Nutzungsumfang festzustellen.

Auf dieser Seite konfigurieren Sie die Anmeldung.

Beschreibung

Die Seite enthält folgende Felder:

Hinweis

Um die Login-Authentifizierung "RADIUS", "Lokal und RADIUS" oder "RADIUS und Fallback Lokal" nutzen zu können, muss ein RADIUS-Server hinterlegt und für die Benutzerauthentifizierung konfiguriert sein.

- **Login-Authentifizierung**
  Legen Sie fest, wie die Anmeldung erfolgt:
  - Lokal
    Die Authentifizierung muss lokal auf dem Gerät erfolgen.
  - RADIUS
    Die Authentifizierung muss über einen RADIUS-Server erfolgen.
  - Lokal und RADIUS
    Die Authentifizierung kann sowohl über die im Gerät vorhandenen Benutzer (Benutzername und Passwort) als auch über einen RADIUS-Server erfolgen.
    Es wird zuerst in der lokalen Datenbank nach dem Benutzer gesucht. Wenn der Benutzer dort nicht vorhanden ist, wird eine RADIUS-Anfrage geschickt.
  - RADIUS und Fallback Lokal
    Die Authentifizierung muss über einen RADIUS-Server erfolgen.
    Nur wenn der RADIUS-Server im Netz nicht erreichbar ist, wird eine lokale Authentifizierung durchgeführt.

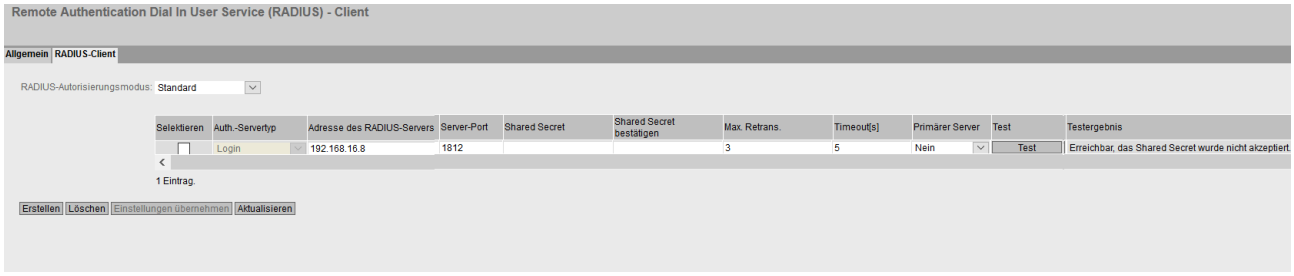
6.10.3.2 RADIUS-Client

Authentifizierung über einen externen Server

Das Konzept von RADIUS basiert auf einem externen Authentifizierungs-Server.

Jede Zeile der Tabelle enthält die Zugangsdaten für je einen Server. In der Suchreihenfolge wird der primäre Server zuerst angefragt. Ist der primäre Server nicht erreichbar, werden in der eingetragenen Reihenfolge sekundäre Server angefragt.

Wenn keiner der Server antwortet, findet keine Authentifizierung statt.



Beschreibung

Die Seite enthält folgende Felder:

- **RADIUS-Autorisierungsmodus**
  Der RADIUS-Autorisierungsmodus legt bei der Login-Authentifizierung fest, wie bei einer erfolgreichen Authentifizierung die Rechtevergabe für die Benutzer erfolgt.
  - Standard
    In diesem Modus wird der Benutzer mit Administratorrechten angemeldet, wenn der Server für das Attribut "Service Type" den Wert "Administrative User" an das Gerät zurück gibt. In allen anderen Fällen wird der Benutzer mit Leserechten angemeldet.
  - Herstellerspezifisch
    In diesem Modus ist die Rechtevergabe davon abhängig, ob und welche Gruppe der Server für den Benutzer zurück gibt und ob es für den Benutzer einen Eintrag in der Tabelle "Externe Benutzeraccounts" gibt.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Adresse des RADIUS-Servers**
  Geben Sie die IP-Adresse oder den FQDN (Fully Qualified Domain Name) des RADIUS Servers ein.
- **Server-Port**
  Geben Sie hier den Eingangs-Port auf dem RADIUS Server ein. Standardmäßig ist der Eingangs-Port 1812 eingestellt. Der Wertebereich ist 1...65535.
- **Shared Secret**
  Geben Sie hier Ihre Zugangskennung an. Der Wertebereich ist 1...128 Zeichen.
- **Shared Secret bestätigen**
  Geben Sie die Zugangskennung zur Bestätigung erneut ein.
- **Max. Retrans.**
  Geben Sie die maximale Anzahl der Wiederholungen eines Anfrageversuchs ein.
  Der initiale Verbindungsversuch wird um den hier angegebenen Wert wiederholt, bevor ein anderer konfigurierter RADIUS Server angefragt wird oder die Anmeldung für gescheitert erklärt wird. Standardmäßig sind 3 Wiederholungen eingestellt, das bedeutet 4 Verbindungsversuche. Der Wertebereich ist 1...5.
- **Timeout[s]**
  Legen Sie die Zeitdauer fest, die der RADIUS-Client auf eine Antwort des RADIUS-Severs wartet, bevor er die Anmeldung erneut versucht.

- **Primärer Server**
  Legen Sie mit Hilfe der Optionen der Klappliste fest, ob dieser Server der primäre Server ist. Sie können aus den Optionen "ja" oder "nein" auswählen.
- **Test**
  Mit dieser Schaltfläche können Sie testen, ob der angegebene RADIUS-Server verfügbar ist oder nicht. Der Test wird einmalig durchgeführt und nicht zyklisch wiederholt.
- **Testergebnis**
  Zeigt an, ob der RADIUS-Server verfügbar ist oder nicht:
  - Nicht erreichbar
    Die IP-Adresse ist nicht erreichbar.
    Die IP-Adresse ist erreichbar, der RADIUS-Server läuft jedoch nicht.
  - Erreichbar, das Shared Secret wurde nicht akzeptiert
    Die IP-Adresse ist erreichbar, der RADIUS-Server akzeptiert jedoch das angegebene Shared Secret nicht.
  - Erreichbar, das Shared Secret wurde akzeptiert
    Die IP-Adresse ist erreichbar und der RADIUS-Server akzeptiert das angegebene Shared Secret.

Vorgehensweise zur Konfiguration

Neuen Server eintragen

1. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag erzeugt. Folgende Standardwerte werden in die Tabelle eingetragen:
   - Adresse des RADIUS-Servers: 0.0.0.0
   - Server-Port: 1812
   - Max. Retrans.: 3
   - Primärer Server: Nein
2. Geben Sie in der jeweiligen Zeile die folgenden Daten in die Eingabefelder ein:
   - Adresse des RADIUS-Servers
   - Server-Port
   - Shared Secret
   - Shared Secret bestätigen
   - Max. Retrans.: 3
   - Primärer Server: Nein
3. Testen Sie ggf. die Erreichbarkeit des RADIUS-Servers.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Wiederholen Sie den Vorgang für alle Server, die Sie eintragen wollen.

Server ändern

1. Geben Sie in der jeweiligen Zeile die folgenden Daten in die Eingabefelder ein:
   - Adresse des RADIUS-Servers
   - Server-Port
   - Shared Secret
   - Shared Secret bestätigen
   - Max. Retrans
   - Primärer Server
2. Testen Sie ggf. die Erreichbarkeit des RADIUS-Servers.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Wiederholen sie den Vorgang bei allen Servern, deren Eintrag Sie ändern wollen

Server löschen

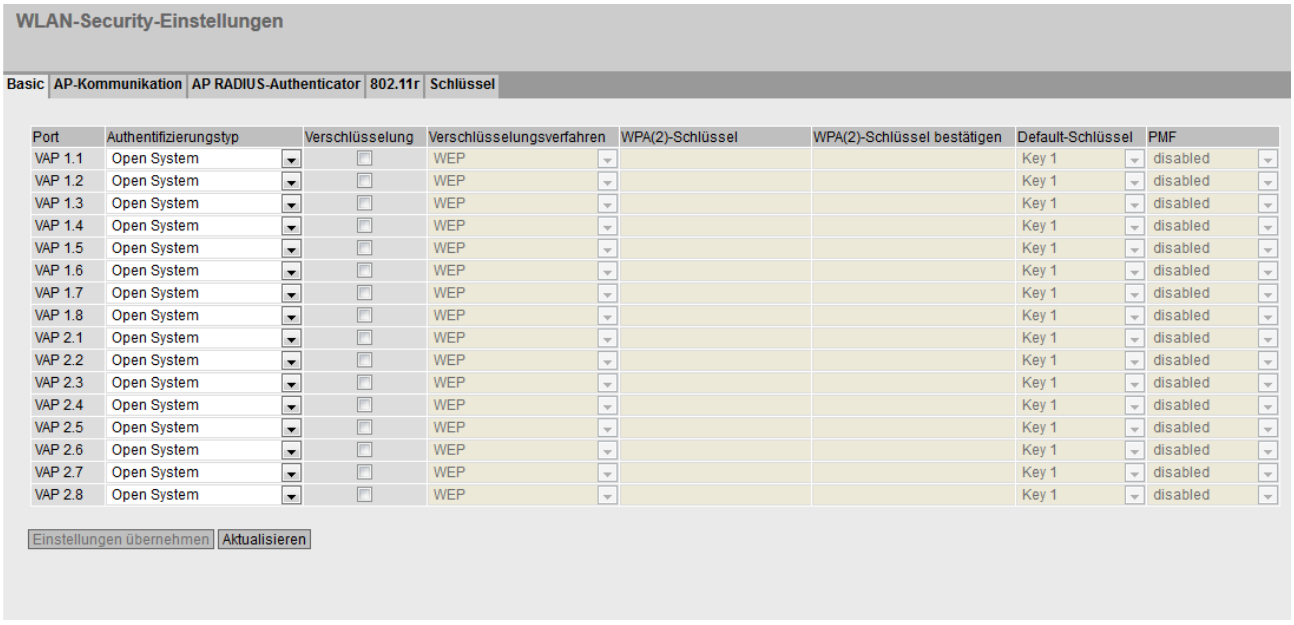
1. Klicken Sie in das Optionskästchen in der ersten Spalte vor der zu löschenden Zeile, um den Eintrag zum Löschen zu markieren.
   Wiederholen Sie den Vorgang für jeden Eintrag, den Sie löschen wollen.
2. Klicken Sie auf die Schaltfläche "Löschen". Die Daten werden aus dem Speicher des Gerätes gelöscht und die Seite wird aktualisiert.

6.10.4 WLAN

6.10.4.1 Basic (Access Point)

Sicherheitsstufen

Um das Netzwerk zu sichern, werden Authentifizierung und Verschlüsselung verwendet. Auf dieser Seite legen Sie Sicherheitseinstellungen fest.



Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Port**
  Zeigt die verfügbaren Ports an.
- **Authentifizierungstyp**
  Wählen Sie die Authentifizierungsart aus. Die Auswahl ist abhängig von der Betriebsart und dem Übertragungsstandard.

  Hinweis

  WLAN-Modus IEEE 802.11 n / ac

  Im WLAN-Modus IEEE 802.11n / ac ist nur die WPA2 (WPA2-PSK u. WPA2 RADIUS) Verschlüsselung möglich.

  – Open System
  Es wird keine Authentifizierung vorgenommen. Eine Verschlüsselung mit einem festen (nicht wechselnden) WEP-Schlüssel kann optional ausgewählt werden. Um den Schlüssel zu verwenden, aktivieren Sie "Verschlüsselung". Den WEP-Schlüssel definieren auf der Seite "Schlüssel".

  – Shared Key
  Bei der Shared Key Authentifizierung wird am Client und am Access Point ein fester Schlüssel hinterlegt. Dieser WEP-Schlüssel wird dann zur Authentifizierung und Verschlüsselung verwendet. Den WEP-Schlüssel definieren auf der Seite "Keys".

  Hinweis

  Bei Verwendung von "Open System" mit "Verschlüsselung" bzw. "Shared Key" muss immer Key 1 auf der Seite "Schlüssel" gesetzt sein.

  – WPA (RADIUS)
  Wi-Fi Protected Access (WPA) ist eine Methode, die durch die Wi-Fi Alliance spezifiziert wird, um die Sicherheitslücken von WEP zu schließen. Dabei ist die Authentifizierung durch einen Server (802.1x) fest vorgeschrieben. Durch den dynamischen Austausch der Schlüssel bei jedem Datenframe wird eine weitere Sicherheit eingebaut.

  – WPA-PSK
  WPA Pre Shared Key (WPA-PSK) ist die abgeschwächte Version von WPA. Bei diesem Verfahren wird keine Authentifizierung durch einen Server durchgeführt, sondern anhand eines Passworts. Dieses Passwort wird auf dem Client wie auf dem Server manuell konfiguriert.

  – WPA2 (RADIUS)
  WPA2 (Wi-Fi Protected Access 2) ist die Weiterentwicklung von WPA und implementiert die Funktionen des Sicherheitsstandards IEEE 802.11i. Die WPA-Authentifizierung arbeitet jedoch mit dem RADIUS-Server.

  – WPA2-PSK
  WPA2-PSK basiert auf dem Standard 802.11i. Die WPA-Authentifizierung arbeitet jedoch ohne RADIUS-Server. Stattdessen wird auf jedem Client und Access Point ein WPA(2)-Schlüssel (WPA(2) Pass phrase) hinterlegt. Die WPA(2) Pass phrase wird zur Authentifizierung und weiteren Verschlüsselung verwendet.

  - WPA/WPA2-Auto-PSK
    Einstellung, in der ein Access Point sowohl die Authentifizierungsart "WPA-PSK" als auch "WPA2-PSK" verarbeiten kann. Dies ist erforderlich, wenn der Access Point mit verschiedenen Clients kommuniziert, die einerseits "WPA-PSK" und andererseits "WPA2-PSK" verwenden. Bei den Clients wird das gleiche Verschlüsselungsverfahren eingesetzt.
  - WPA/WPA2-Auto
    Einstellung, in der ein Access Point sowohl die Authentifizierungsart "WPA" als auch "WPA2" verarbeiten kann. Dies ist erforderlich, wenn der Access Point mit verschiedenen Clients kommuniziert, die einerseits "WPA" und andererseits "WPA2" verwenden. Bei den Clients wird das gleiche Verschlüsselungsverfahren eingesetzt

- **Verschlüsselung**
  Die Verschlüsselung schützt die übertragenen Daten vor Abhören und Fälschen. Sie können die Verschlüsselung nur abschalten, wenn Sie bei der Authentifizierung "Open System" gewählt haben. Alle anderen Sicherungsverfahren beinhalten sowohl Authentifizierung als auch Verschlüsselung.
- **Verschlüsselungsverfahren**
  Wählen Sie das Verschlüsselungsverfahren. Die Auswahl ist abhängig vom Übertragungsstandard.
  - AUTO
    Je nach Fähigkeit der Gegenstation wird entweder AES oder TKIP automatisch ausgewählt.
  - WEP
    WEP (Wired Equivalent Privacy)
    Ein symmetrisches Stromverschlüsselungsverfahren mit lediglich 40 bzw. 104 Bit langen Schlüsseln, die auf dem RC4-Algorithmus (Ron's Code 4) basieren.
  - TKIP (Temporal Key Integrity Protocol)
    Ein symmetrisches Stromverschlüsselungsverfahren mit dem RC4-Algorithmus (Ron's Code 4). TKIP verwendet im Gegensatz zur schwachen WEP-Verschlüsselung wechselnde Schlüssel, die von einem Hauptschlüssel abgeleitet werden. TKIP kann außerdem gefälschte Datentelegramme erkennen.
  - AES (Advanced Encryption Standard)
    Starkes symmetrisches Blockverschlüsselungsverfahren nach dem Rijndael-Algorithmus, der die Funktionen von TKIP weiter verbessert.

    Hinweis

    Um Ihre Daten besser vor Angriffen zu schützen, verwenden Sie WPA2/ WPA2-PSK mit AES.

- **WPA(2)-Schlüssel**
  Tragen Sie hier einen WPA(2)-Schlüssel ein. Dieser WPA(2)-Schlüssel muss sowohl auf der Client-Seite als auch dem Access Point bekannt sein und wird vom Benutzer auf beiden Seiten eingegeben.
  - Bei einem Schlüssel mit 8 bis 63 Zeichen können Sie nur folgende lesbare ASCII-Zeichen verwenden: 0x20 - 0x7e.
  - Bei einem Schlüssel mit genau 64 Zeichen können Sie folgende ASCII-Zeichen verwenden: 0 - 9, a - f und A - F.
- **WPA(2)-Schlüssel bestätigen**
  Bestätigen Sie den oben eingegebenen WPA(2)-Schlüssel.

- **Default-Schlüssel**
  Legen Sie den WEP-Schlüssel fest, der zur Verschlüsselung der Daten verwendet wird. Den WEP-Schlüssel definieren auf der Seite "Schlüssel".
- **PMF (Protected Management Frames)**
  Nur mit folgenden verwendbar:
  – WLAN-Modus: IEEE 802.11n oder ac
  – Authentifizierungstyp: WPA2-PSK oder WPA2 (RADIUS)

  Mit dieser Einstellung werden die Management-Telegramme kryptografisch geschützt. Damit wird z. B. verhindert, dass durch gefälschte Disassociation- / Deauthenticate-Telegramme die WLAN-Clients vom Access Point getrennt werden. Weiterführende Informationen dazu finden Sie im Standard IEEE 802.11w.
  Folgende Einstellungen sind möglich:
  – Deaktiviert
    Die Management-Telegramme sind nicht verschlüsselt.
  – Erforderlich
    Die Management-Telegramme sind immer verschlüsselt. Eine Verbindung der WLAN-Clients zu dem Access Point ist nur möglich, wenn diese auch PMF unterstützen.
  – Optional
    Die Management-Telegramme werden je nach Unterstützung des WLAN-Clients verschlüsselt oder unverschlüsselt.

Vorgehensweise

1. Legen Sie die gewünschten Sicherheitseinstellungen fest. Welche Einstellungen möglich sind, hängt ab vom eingestellten "Authentifizierungstyp".

Authentifizierungstyp	Verschlüsse-lung	Verschlüsselungs-verfahren	Schlüsselherkunft
Open System	deaktiviert	--	--
Open System	aktiviert	WEP	Default-Schlüssel
Shared Key	aktiviert	WEP	Default-Schlüssel
WPA (RADIUS)	aktiviert	Auto/TKIP/AES	RADIUS-Server
WPA-PSK	aktiviert	Auto/TKIP/AES	WPA(2)-Schlüssel
WPA2 (RADIUS)	aktiviert	Auto/TKIP/AES	RADIUS-Server
WPA2-PSK	aktiviert	Auto/TKIP/AES	WPA(2)-Schlüssel

2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.10.4.2 Basic (Client)

Sicherheitsstufen

Um das Netzwerk zu sichern, werden Authentifizierung und Verschlüsselung verwendet. Auf dieser Seite legen Sie Sicherheitseinstellungen fest.

Hinweis

Diese Seite ist nur bei Clients oder bei Access Points im Client-Modus verfügbar.

Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen. Klicken Sie die Schaltfläche "Löschen", um einen Eintrag in der Liste zu löschen.
- **Security-Kontext**
  Zeigt die Nummer des Eintrags an. Wenn Sie einen neuen Eintrag anlegen, wird eine neue Zeile mit einer eindeutigen Nummer angelegt.
  Sie können bis zu 8 Security-Kontexte anlegen. Der Security-Kontext 1 kann nicht gelöscht werden.

- **Authentifizierungstyp**
  Wählen Sie die Authentifizierungsart aus. Die Auswahl ist abhängig von der Betriebsart und dem Übertragungsstandard.

  Hinweis

  WLAN-Modus IEEE 802.11 n / ac

  Im WLAN-Modus IEEE 802.11n / ac ist nur die WPA2 (WPA2-PSK u. WPA2 RADIUS) Verschlüsselung möglich.

  Authentifizierungstyp
  Wählen Sie die Authentifizierungsart aus. Die Auswahl ist abhängig von der Betriebsart und dem Übertragungsstandard.

  – Open System
    Es wird keine Authentifizierung vorgenommen. Eine Verschlüsselung mit einem festen (nicht wechselnden) WEP-Schlüssel kann optional ausgewählt werden. Um den Schlüssel zu verwenden, aktivieren Sie "Verschlüsselung". Den WEP-Schlüssel definieren auf der Seite "Schlüssel".

    Hinweis

    Bei Verwendung von "Open System" mit "Verschlüsselung" bzw. "Shared Key" muss immer Schlüssel 1 auf der Seite "Schlüssel" gesetzt sein.

  – Shared Key
    Bei der Shared Key Authentifizierung wird am Client und am Access Point ein fester Schlüssel hinterlegt. Dieser WEP-Schlüssel wird dann zur Authentifizierung und Verschlüsselung verwendet. Den WEP-Schlüssel definieren auf der Seite "Schlüssel".

  – WPA (RADIUS)
    Wi-Fi Protected Access (WPA) ist eine Methode, die durch die Wi-Fi Alliance spezifiziert wird, um die Sicherheitslücken von WEP zu schließen. Dabei ist die Authentifizierung durch einen Server (802.1x) fest vorgeschrieben. Durch den dynamischen Austausch der Schlüssel bei jedem Datenframe wird eine weitere Sicherheit eingebaut.

    Hinweis

    Nehmen Sie die entsprechenden RADIUS-Einstellungen zunächst auf der Seite "Security > WLAN > Client Radius Supplicant" vor.

  – WPA-PSK
    WPA Pre Shared Key (WPA-PSK) ist die abgeschwächte Version von WPA. Bei diesem Verfahren wird keine Authentifizierung durch einen Server durchgeführt, sondern anhand eines Passworts. Dieses Passwort wird auf dem Client wie auf dem Server manuell konfiguriert.

  – WPA2 (RADIUS)
    WPA2 (Wi-Fi Protected Access 2) ist die Weiterentwicklung von WPA und implementiert die Funktionen des Sicherheitsstandards IEEE 802.11i. Die WPA-Authentifizierung arbeitet jedoch mit dem RADIUS-Server.

    Hinweis

    Nehmen Sie die entsprechenden RADIUS-Einstellungen zunächst auf der Seite "Security > WLAN > Client Radius Supplicant" vor.

  - WPA2-PSK
    WPA2-PSK basiert auf dem Standard 802.11i. Die WPA-Authentifizierung arbeitet jedoch ohne RADIUS-Server. Stattdessen wird auf jedem Client und Access Point ein WPA(2)-Schlüssel (WPA(2) Pass phrase) hinterlegt. Die WPA(2) Pass phrase wird zur Authentifizierung und weiteren Verschlüsselung verwendet.
  - WPA/WPA2-Auto-PSK
    Einstellung, in der ein Access Point sowohl die Authentifizierungsart "WPA-PSK" als auch "WPA2-PSK" verarbeiten kann. Dies ist erforderlich, wenn der Access Point mit verschiedenen Clients kommuniziert, die einerseits "WPA-PSK" und andererseits "WPA2-PSK" verwenden. Bei den Clients wird das gleiche Verschlüsselungsverfahren eingesetzt.
  - WPA/WPA2-Auto
    Einstellung, in der ein Access Point sowohl die Authentifizierungsart "WPA" als auch "WPA2" verarbeiten kann. Dies ist erforderlich, wenn der Access Point mit verschiedenen Clients kommuniziert, die einerseits "WPA" und andererseits "WPA2" verwenden. Bei den Clients wird das gleiche Verschlüsselungsverfahren eingesetzt.

- **Verschlüsselung**
  Die Verschlüsselung schützt die übertragenen Daten vor Abhören und Fälschen. Sie können die Verschlüsselung nur abschalten, wenn Sie bei der Authentifizierung "Open System" gewählt haben. Alle anderen Sicherungsverfahren beinhalten sowohl Authentifizierung als auch Verschlüsselung.
- **Verschlüsselungsverfahren**
  Wählen Sie das Verschlüsselungsverfahren. Die Auswahl ist abhängig vom Übertragungsstandard.
  - AUTO
    Je nach Fähigkeit der Gegenstation wird entweder AES oder TKIP automatisch ausgewählt.
  - WEP
    WEP (Wired Equivalent Privacy)
    Ein symmetrisches Stromverschlüsselungsverfahren mit lediglich 40 bzw. 104 Bit langen Schlüsseln, die auf dem RC4-Algorithmus (Ron's Code 4) basieren.
  - TKIP (Temporal Key Integrity Protocol)
    Ein symmetrisches Stromverschlüsselungsverfahren mit dem RC4-Algorithmus (Ron's Code 4). TKIP verwendet im Gegensatz zur schwachen WEP-Verschlüsselung wechselnde Schlüssel, die von einem Hauptschlüssel abgeleitet werden. TKIP kann außerdem gefälschte Datentelegramme erkennen.
  - AES (Advanced Encryption Standard)
    Starkes symmetrisches Blockverschlüsselungsverfahren nach dem Rijndael-Algorithmus, der die Funktionen von TKIP weiter verbessert.

    Hinweis

    Um Ihre Daten besser vor Angriffen zu schützen, verwenden Sie WPA2/ WPA2-PSK mit AES.

- **WPA(2)-Schlüssel**
  Tragen Sie hier einen WPA(2)-Schlüssel ein. Dieser WPA(2)-Schlüssel muss sowohl auf der Client-Seite als auch dem Access Point bekannt sein und wird vom Benutzer auf beiden Seiten eingegeben.
  Bei einem Schlüssel mit 8 bis 63 Zeichen können Sie nur folgende, lesbare ASCII-Zeichen verwenden: 0x20 - 0x7e.
  Bei einem Schlüssel mit genau 64 Zeichen können Sie folgende ASCII-Zeichen verwenden: 0 - 9, a - f und A - F.
- **WPA(2)-Schlüssel bestätigen**
  Bestätigen Sie den oben eingegebenen WPA(2)-Schlüssel.
- **Default-Schlüssel**
  Legen Sie den WEP-Schlüssel fest, der zur Verschlüsselung der Daten verwendet wird. Den WEP-Schlüssel definieren auf der Seite "Keys".

Vorgehensweise

1. Um einen neuen Security-Kontext anzulegen, klicken Sie auf die Schaltfläche "Erstellen".
2. Legen Sie die gewünschten Sicherheitseinstellungen fest. Welche Einstellungen möglich sind, hängt ab vom eingestellten "Authentifizierungstyp".
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

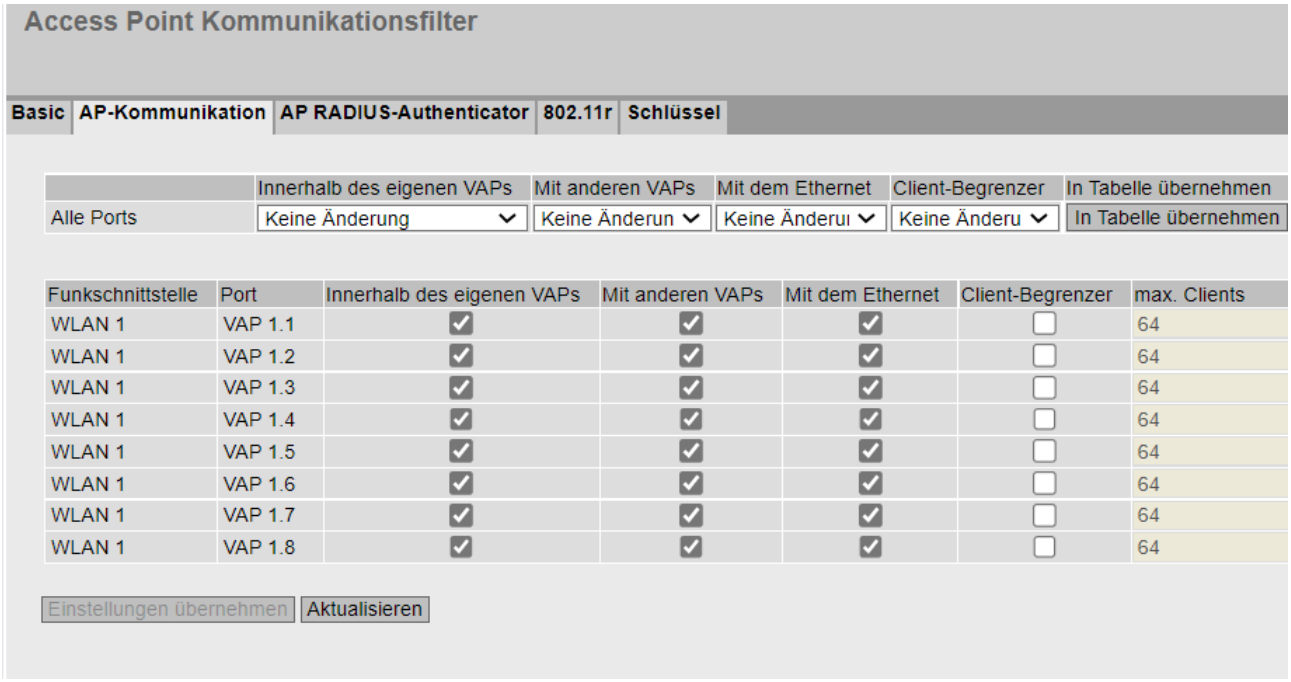
6.10.4.3 AP-Kommunikation

Kommunikationsmöglichkeiten

Auf dieser WBM-Seite legen Sie fest, welche Art von Kommunikation der Access Point erlaubt.

Hinweis

Diese WBM-Seite ist nur im Access Point-Modus verfügbar.



Beschreibung

Die Tabelle 1 gliedert sich in folgende Spalten:

- **Spalte 1**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **Innerhalb des eigenen VAPs / Mit anderen VAPs / Mit dem Ethernet / Client Begrenzer**
  Wählen Sie in der Klappliste die Einstellung für alle Ports aus. Wenn "Keine Änderung" ausgewählt ist, bleibt der Eintrag in der Tabelle 2 unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen an.
- **Port**
  Zeigt die VAP-Schnittstelle an.
- **Innerhalb des eigenen VAPs**
  - Aktiviert
    Clients, die an der gleichen VAP-Schnittstelle eines Access Point angemeldet sind, können miteinander kommunizieren.
  - Deaktiviert
    Option ist deaktiviert.

- **Mit anderen VAPs**
  - Aktiviert
    Clients, die an unterschiedlichen VAP-Schnittstellen eines Access Point angemeldet sind, können miteinander kommunizieren.

    Hinweis

    Bei einem Access Point ist auf allen WLAN-Schnittstellen beziehungsweise auf allen VAP-Schnittstellen "Mit anderen VAPs" zu aktivieren, um eine Kommunikation zwischen den Clients zu ermöglichen, die an verschiedenen VAP-Schnittstellen des Access Points angemeldet sind.

  - Deaktiviert
    Option ist deaktiviert.

Hinweis

Funktion "Innerhalb des eigenen VAPs" oder "Mit anderen VAPs" deaktiviert

Wenn die Funktion "Innerhalb des eigenen VAPs" oder "Mit anderen VAPs" deaktiviert ist, können sich die verschiedenen WLAN-Clients nicht mehr sehen. Damit funktioniert auch die Address Collision Detection (ACD) nicht mehr zuverlässig.

- **Mit dem Ethernet**
  - Aktiviert
    Clients können über die Ethernet-Schnittstelle des Access Points kommunizieren.
  - Deaktiviert
    Option ist deaktiviert.
- **Client-Begrenzer**
  - Aktiviert
    Die Anzahl der gleichzeitig anmeldbaren WLAN-Clients wird begrenzt.
  - Deaktiviert
    Option ist deaktiviert.
- **max. Clients**
  Legen Sie die maximale Anzahl der Clients fest, die sich gleichzeitig mit dieser Schnittstelle verbinden können. Wenn die Anzahl überschritten wird, werden weitere Clients abgewiesen.

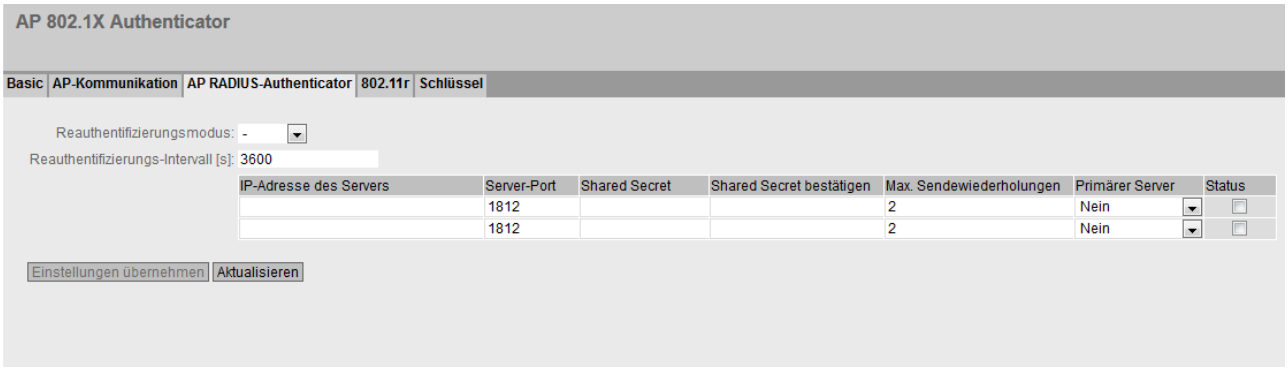
6.10.4.4 AP RADIUS-Authenticator

Hinweis

Diese WBM-Seite ist nur im Access Point-Modus verfügbar.

Konfigurieren des RADIUS-Server

Auf dieser WBM-Seite definieren Sie die RADIUS-Server sowie die RADIUS-Authentifizierung des Access Points. Sie können die Daten für zwei RADIUS-Server eingeben.



Beschreibung

Die Seite enthält folgende Felder:

- **Reauthentifizierungsmodus**
  Legen Sie fest, wer die Zeit bestimmen soll, bis die Clients zu einer neuen Reauthentifizierung gezwungen werden.
  - \- (deaktiviert)
    Reauthentication Mode ist deakviert.
  - Server
    Aktiviert die Zeitverwaltung auf dem Server.
  - Lokal
    Aktiviert die lokale Zeitverwaltung. Legen Sie bei "Reauthentication-Intervall" den Gültigkeitszeitraum fest.
- **Reauthentifizierungs-Intervall [s]**
  Bei der lokalen Zeitverwaltung geben Sie hier den Gültigkeitszeitraum für eine Authentifizierung in Sekunden an. Die minimale Zeitdauer beträgt 1 Minute (Eingabe 60), die maximale Zeitdauer 12 Stunden (Eingabe 43200). Der Standardwert ist eine Stunde (3.600 Sekunden).

Die Tabelle gliedert sich in folgende Spalten:

- **IP-Adresse des Servers**
  Tragen Sie die IP-Adresse oder den FQDN (Fully Qualified Domain Name) des RADIUS Servers ein.
- **Server-Port**
  Tragen Sie hier den Eingangs-Port auf dem RADIUS-Server ein.
- **Shared Secret**
  Tragen Sie das Passwort des RADIUS-Servers ein.
  Für das Passwort wird der ASCII-Code 0x20 bis 0x7e verwendet.
- **Shared Secret bestätigen**
  Bestätigen Sie das Passwort.

- **Max. Sendewiederholungen**
  Tragen Sie die maximale Anzahl der Verbindungsversuche ein.
- **Primärer Server**
  Legen Sie fest, ob dieser Server der primäre Server ist.
  - Ja: Primärer Server
  - Nein: Backup Server.
- **Status**
  Mit diesem Optionskästchen können Sie den RADIUS-Server aktivieren oder deaktivieren

Vorgehensweise

Neuen Server eintragen

Um einen neuen Server einzutragen, gehen Sie folgendermaßen vor:

1. Tragen Sie in der jeweiligen Zeile die folgenden Daten in die Eingabefelder ein:
   - IP-Adresse oder FQDN des RADIUS-Servers
   - Portnummer des Eingangsports
   - Passwort
   - Bestätigung des Passworts
   - Maximale Anzahl der Übertragungsversuche
   - Primärer Server
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Server ändern

1. Tragen Sie in der jeweiligen Zeile die folgenden Daten in die Eingabefelder ein:
   - IP-Adresse oder FQDN des RADIUS-Servers
   - Portnummer des Eingangs-Ports
   - Passwort
   - Bestätigung des Passworts
   - Maximale Anzahl der Übertragungsversuche
   - Primärer Server
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Wiederholen sie den Vorgang bei allen Servern, deren Eintrag Sie ändern wollen.

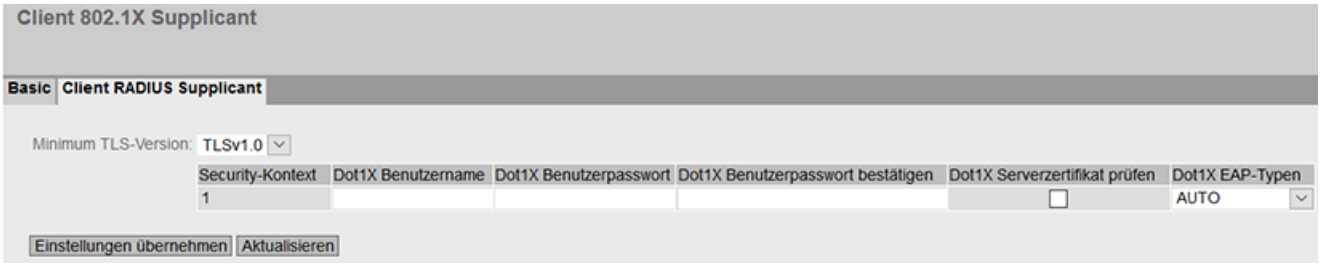
6.10.4.5 Client RADIUS-Supplicant

Client Supplicant

Auf dieser WBM-Seite konfigurieren Sie die Einstellungen für die RADIUS-Autorisierung des Clients.

Hinweis

Diese Seite ist nur bei Clients oder bei Access Points im Client-Modus verfügbar.



Beschreibung

- **Minimum TLS-Version**
  Legen Sie fest, welche Version von TLS mindestens bei der WLAN-RADIUS-Authentifizierung verwendet wird.

  Hinweis

  RADIUS-Server

  Voraussetzung ist, dass der RADIUS-Server die TLS-Version unterstützt.

Die Tabelle gliedert sich in folgende Spalten:

- **Security-Kontext**
  Zeigt den Security-Kontext an.
- **Dot1X Benutzername**
  Geben Sie den Benutzernamen ein, mit dem Sie sich am RADIUS-Server anmelden.
- **Dot1X Benutzerpasswort**
  Geben Sie für den oben genannten Benutzernamen das Passwort ein. Mit dieser Kombination meldet sich der Client beim RADIUS-Server an.
  Für die Passwort-Vergabe wird der ASCII-Code 0x20 bis 0x7e verwendet.
- **Dot1X Benutzerpasswort bestätigen**
  Bestätigen Sie das Passwort.

Hinweis

Dot1X-Benutzername und Dot1X-Benutzerpasswort

Bei WPA (RADIUS), WPA2 (RADIUS), EAP-TLS, EAP-TTLS und PEAP muss der Dot1X-Benutzername und das Dot1X-Benutzerpasswort konfiguriert werden.

Bei der Einstellung "Auto" muss entweder das Zertifikat geladen sein oder der Dot1X-Benutzername und das Dot1X-Benutzerpasswort konfiguriert werden.

- **Dot1X Serverzertifikat prüfen**
  Legen Sie fest, ob sich der RADIUS-Server mittels Zertifikat gegenüber dem Client ausweist.

  Hinweis

  Verwenden von Zertifikaten

  Erneuern Sie vor Ablauf das Zertifikat. Wenn Sie das Zertifikat nicht rechtzeitig erneuern, ist nach Ablauf ein Verbindungsaufbau nicht mehr möglich.

- **Dot1X EAP-Typen**
  Legen Sie die Authentifizierungsmethoden fest. Folgende Methoden gibt es:
  - Auto
    Client bietet RADIUS-Server alle Methoden an.
  - EAP-TLS
    Extensible Authentication Protocol - Transport Layer Security
    Nutzt Zertifikate zur Authentifizierung.
  - EAP-TTLS
    Extensible Authentication Protocol - Tunnel Transport Layer Security
    Nach Aufbau des TLS Tunnels wird MS-CHAPv2 zur inneren Authentifizierung genutzt.
  - PEAP
    Protected Extensible Authentication Protocol
    Alternativer Protokollentwurf der IETF zu EAP-TTLS.

Vorgehensweise

1. Tragen Sie in den Eingabefeldern die benötigten Werte ein.
2. Wählen Sie aus der Klappliste "Dot1x EAP-Type" den gewünschten Eintrag.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

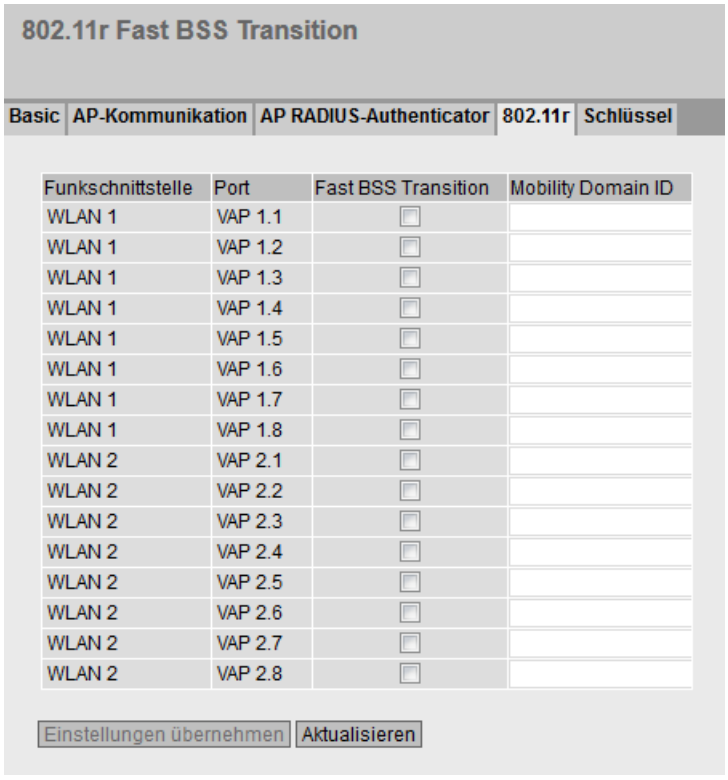
6.10.4.6 802.11r

Auf dieser WBM-Seite konfigurieren Sie die Einstellung für Fast BSS Transition.

Hinweis

Diese WBM-Seite ist nur im Access Point-Modus verfügbar.

Weitere Informationen dazu finden Sie unter "Beschreibung > IEEE 802.11r".



Voraussetzung

- Die Access Points sind Mitglieder der gleichen Mobilitätsdomäne.
- Nur mit WPA2 (WPA2-PSK u. WPA2 RADIUS) Verschlüsselung möglich.

Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen an.
- **Port**
  Zeigt die VAP-Schnittstelle an.
- **Fast BSS Transition**
  Wenn aktiviert, wird die Funktion "Fast BSS Transition" unterstützt. Nur aktivierbar, wenn die Mobility Domain eingetragen ist.
- **Mobility Domain ID**
  Tragen Sie die ID der Mobilitätsdomäne ein. Die Access Points mit der gleichen ID sind Mitglieder einer Mobilitätsdomäne. Anhand der ID erkennt der WLAN-Client, ob der Access Point dergleichen Mobilitätsdomäne angehört und sich somit ohne Verzögerung anmelden kann.

6.10.4.7 Schlüssel

Festlegung des WEP-Schlüssels

Damit Sie bei den Authentifizierungsmethoden "Open System" und "Shared Key" die Verschlüsselung aktivieren können, müssen Sie zuerst mindestens einen Schlüssel in der Schlüsseltabelle eintragen.

Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Funkschnittstelle**
  Zeigt die verfügbaren WLAN-Schnittstellen an, auf die sich die Einstellungen beziehen.
- **Schlüssel 1 - 4**
  Tragen Sie den WEP-Schlüssel bzw. den AES-Schlüssel ein.
  Für den WEP-Schlüssel sind Zeichen des ASCII-Code von 0x20 bis 0x7E oder hexadezimale Zeichen von 0x00 bis 0xFF zulässig.
  Zwischen folgenden Schlüssellängen kann gewählt werden:
  - 5 bzw. 13 ASCII- oder 10 bzw. 26 hexadezimale Zeichen (40/104 Bit)
  - 16 ASCII- oder 32 hexadezimale Zeichen (128 Bit)

  Hinweis

  Die Eingabe der hexadezimalen Zeichen erfolgt ohne vorangestelltes "0x". Mit einem Hexadezimalzeichen werden vier Bit kodiert. Die Eingaben "ABCDE" (ASCII-Zeichen) und "4142434445" (Hexadezimalzeichen) sind also gleichwertig, weil das ASCII-Zeichen "A" den Hexadezimalcode "0x41" hat.
- **Schlüssel 1 - 4 bestätigen**
  Bestätigen Sie den WEP-Schlüssel.

Vorgehensweise

1. Tragen Sie mindestens einen WEP-Schlüssel ein.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

6.10.5 Management ACL

Konfigurationsbeschreibung

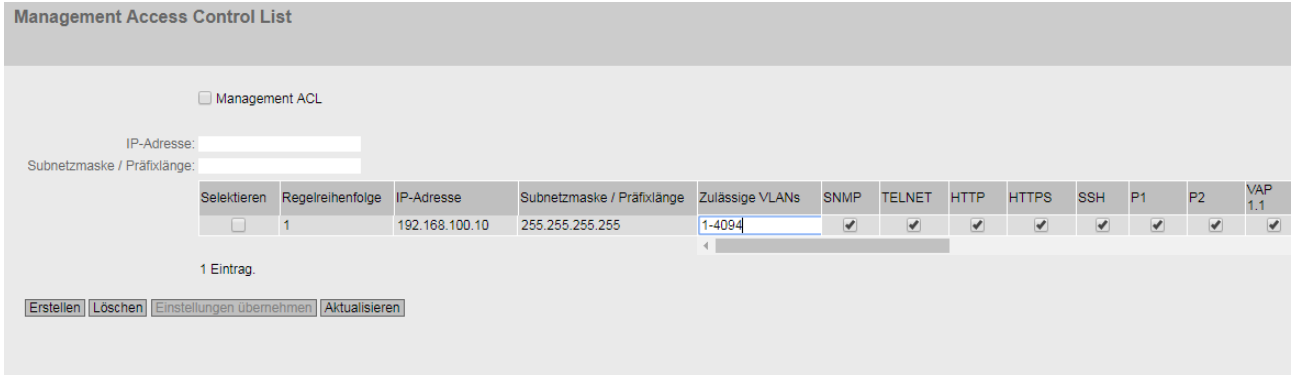
Auf dieser Seite können Sie die Sicherheit Ihres Geräts erhöhen. Um festzulegen, welche Station mit welcher IP-Adresse auf Ihrem Gerät zugreifen darf, konfigurieren Sie die IP-Adresse oder auch ein ganzes Adress-Band.

Sie können einstellen, mit welchen Protokollen und über welche Ports die Station auf dem Gerät zugreifen darf. Sie definieren, in welchem VLAN die Station liegen darf. Damit wird gewährleistet, dass nur bestimmte Stationen innerhalb eines VLANs Zugriff auf das Gerät haben.

Hinweis

Wenn Sie diese Funktion aktivieren, beachten Sie Folgendes

Eine fehlerhafte Projektierung auf der Seite "Management Access Control List" kann dazu führen, dass Sie nicht mehr auf das Gerät zugreifen können. Projektieren Sie daher eine Zugriffsregel, die Ihnen den Zugriff auf das Management erlaubt, bevor Sie die Funktion aktivieren.



Beschreibung

Die Seite enthält folgende Felder:

- **Management ACL**
  Aktivieren oder deaktivieren Sie die Funktion.

  Hinweis

  Wenn die Funktion deaktiviert ist, dann besteht uneingeschränkter Zugriff auf das Management des Geräts. Erst wenn die Funktion aktiviert ist, werden die projektierten Zugriffsregeln berücksichtigt.

- **IP-Adresse**
  Tragen Sie die IP-Adresse oder die Netzadresse ein, für die die Regel gelten soll.
  - Wenn Sie die IPv4-Adresse 0.0.0.0 verwenden, gelten die Einstellungen für alle IPv4-Adressen.
  - Wenn Sie die IPv6-Adresse :: verwenden, gelten die Einstellungen für alle IPv6-Adressen.
- **Subnetzmaske/Präfixlänge**
  Tragen Sie die Subnetzmaske oder die Präfixlänge ein.
  Die Subnetzmaske 255.255.255.255 ist für eine bestimmte IPv4-Adresse. Möchten Sie ein Subnetz zulassen, tragen Sie z. B. für ein C-Subnetz 255.255.255.0 ein. Die Subnetzmaske 0.0.0.0 gilt für alle Subnetze.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Regelreihenfolge**
  Zeigt die Nummer der Regel an. Wenn Sie auf die Schaltfläche "Erstellen" klicken, wird eine neue Zeile mit einer eindeutigen Nummer angelegt
- **IP-Adresse**
  Zeigt die IP-Adresse an.
- **Subnetzmaske/Präfixlänge**
  Zeigt die Subnetzmaske oder die Präfixlänge an.
- **Zulässige VLANs**
  Nur verfügbar, wenn 802.1Q VLAN Bridge unter "Layer 2 > VLAN > Allgemein" eingestellt ist. Tragen Sie die Nummer des VLANs ein, in dem sich das Gerät befindet. Nur die Station kann auf das Gerät zugreifen, wenn es sich in diesem konfigurierten VLAN befindet. Bleibt dieses Eingabefeld leer, gibt es keine Einschränkung bezüglich der VLANs.
- **SNMP**
  Legen Sie fest, ob die Station (bzw. die IP-Adresse) über das Protokoll SNMP auf das Gerät zugreift.
- **TELNET**
  Legen Sie fest, ob die Station (bzw. die IP-Adresse) über das Protokoll TELNET auf das Gerät zugreift.
- **HTTP**
  Legen Sie fest, ob die Station (bzw. die IP-Adresse) über das Protokoll HTTP auf das Gerät zugreift.

- **HTTPS**
  Legen Sie fest, ob die Station (bzw. die IP-Adresse) über das Protokoll HTTPS auf das Gerät zugreift.
- **SSH**
  Legen Sie fest, ob die Station (bzw. die IP-Adresse) über das Protokoll SSH auf das Gerät zugreift.
- **Px**
  Legen Sie fest, ob die Station (bzw. die IP-Adresse) über diesen Port auf das Gerät zugreift.
- **VAP X.Y**
  Legen Sie fest, ob die Station (bzw. die IP-Adresse) über die VAP-Schnittstelle auf das Gerät zugreift.
- **WDS X.Y**
  Legen Sie fest, ob die Station (bzw. die IP-Adresse) über die WDS-Schnittstelle auf das Gerät zugreift.

Vorgehensweise

Hinweis

Beachten Sie, eine fehlerhafte Konfiguration kann dazu führen, dass Sie nicht mehr auf das Gerät zugreifen können.

Abhilfe erhalten Sie dann nur durch ein Zurücksetzen des Geräts auf die Werkseinstellungen und anschließende Neukonfiguration.

Eintrag ändern

1. Konfigurieren Sie die Daten des Eintrags, den Sie ändern wollen.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen", um die Änderungen in das Gerät zu übertragen.

Neuen Eintrag anlegen

1. Tragen Sie in das Eingabefeld "IP-Adresse" die IP-Adresse des Geräts und in das Eingabefeld "Subnetzmaske/Präfixlänge" die dazugehörige Subnetzmaske ein.
2. Klicken Sie auf die Schaltfläche "Erstellen", um eine neue Zeile in der Tabelle anzulegen.
3. Konfigurieren Sie die Einträge der neuen Zeile.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen", um den neuen Eintrag in das Gerät zu übertragen.

Einträge löschen

1. Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
2. Wiederholen Sie den Vorgang für jeden Eintrag, den Sie löschen wollen.
3. Klicken Sie auf die Schaltfläche "Löschen". Die Einträge werden gelöscht und die Seite wird aktualisiert.

6.10.6 Inter AP Blocking

6.10.6.1 Basic

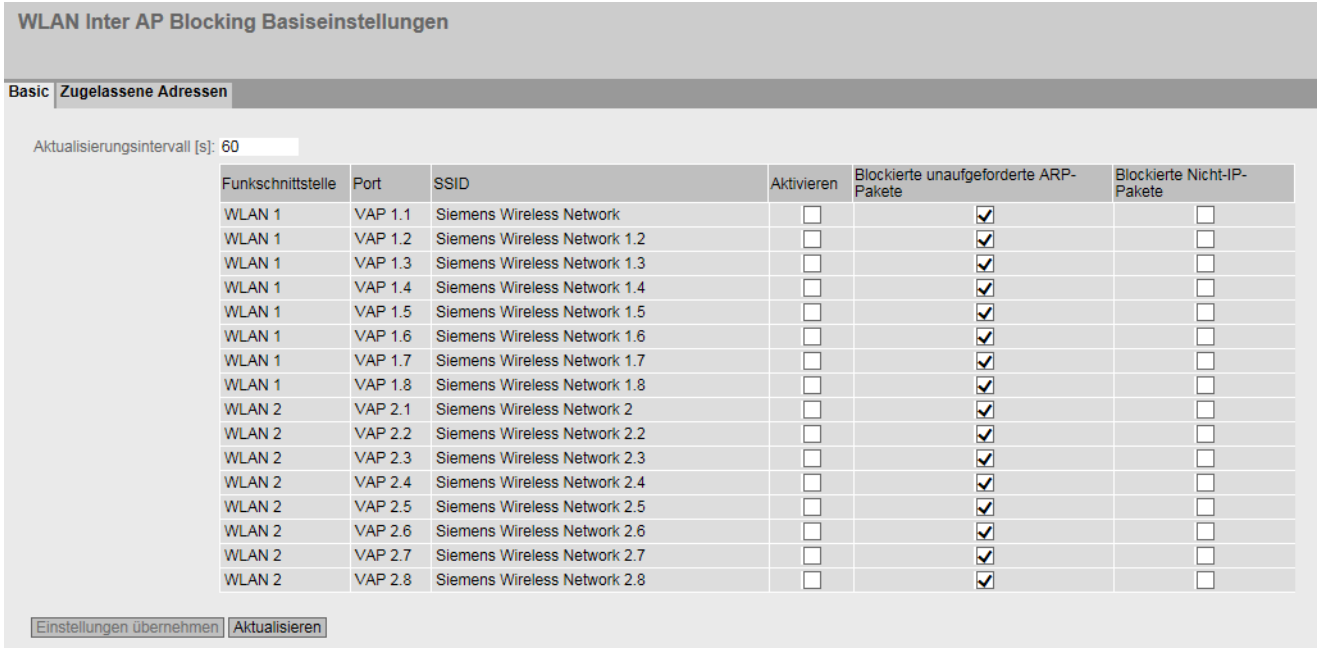
Hinweis

Diese WBM-Seite ist nur im Access Point-Modus verfügbar.

Wann sollte Inter AP Blocking eingesetzt werden?

Die Clients, die an einem Access Point verbunden sind, können im Normalfall mit allen Geräten des verkabelten Layer 2-Netzwerks kommunizieren.

Mit Inter AP Blocking lässt sich die Kommunikation der Clients einschränken, die mit dem Access Point verbunden sind. Nur die Geräte sind für die Clients zugänglich, deren IP-Adressen unter " Zugelassene Adressen" im Access Point konfiguriert sind. Eine Kommunikation mit anderen sich im Netz befindlichen Teilnehmern wird damit unterbunden.



Funkschnittstelle	Port	SSID	Aktivieren	Blockierte unaufgeforderte ARP-Pakete	Blockierte Nicht-IP-Pakete
WLAN 1	VAP 1.1	Siemens Wireless Network	☐	☑	☐
WLAN 1	VAP 1.2	Siemens Wireless Network 1.2	☐	☑	☐
WLAN 1	VAP 1.3	Siemens Wireless Network 1.3	☐	☑	☐
WLAN 1	VAP 1.4	Siemens Wireless Network 1.4	☐	☑	☐
WLAN 1	VAP 1.5	Siemens Wireless Network 1.5	☐	☑	☐
WLAN 1	VAP 1.6	Siemens Wireless Network 1.6	☐	☑	☐
WLAN 1	VAP 1.7	Siemens Wireless Network 1.7	☐	☑	☐
WLAN 1	VAP 1.8	Siemens Wireless Network 1.8	☐	☑	☐
WLAN 2	VAP 2.1	Siemens Wireless Network 2	☐	☑	☐
WLAN 2	VAP 2.2	Siemens Wireless Network 2.2	☐	☑	☐
WLAN 2	VAP 2.3	Siemens Wireless Network 2.3	☐	☑	☐
WLAN 2	VAP 2.4	Siemens Wireless Network 2.4	☐	☑	☐
WLAN 2	VAP 2.5	Siemens Wireless Network 2.5	☐	☑	☐
WLAN 2	VAP 2.6	Siemens Wireless Network 2.6	☐	☑	☐
WLAN 2	VAP 2.7	Siemens Wireless Network 2.7	☐	☑	☐
WLAN 2	VAP 2.8	Siemens Wireless Network 2.8	☐	☑	☐

Beschreibung

Die Seite enthält folgendes Feld:

- **Aktualisierungsintervall [s]**
  Tragen Sie das Aktualisierungsintervall für die ARP-Auflösung der zugelassenen IP-Adressen ein. Die aufgelösten MAC-Adressen werden unter "Information > Security > Inter AP Blocking" angezeigt.

Die Tabelle gliedert sich in folgende Spalten:

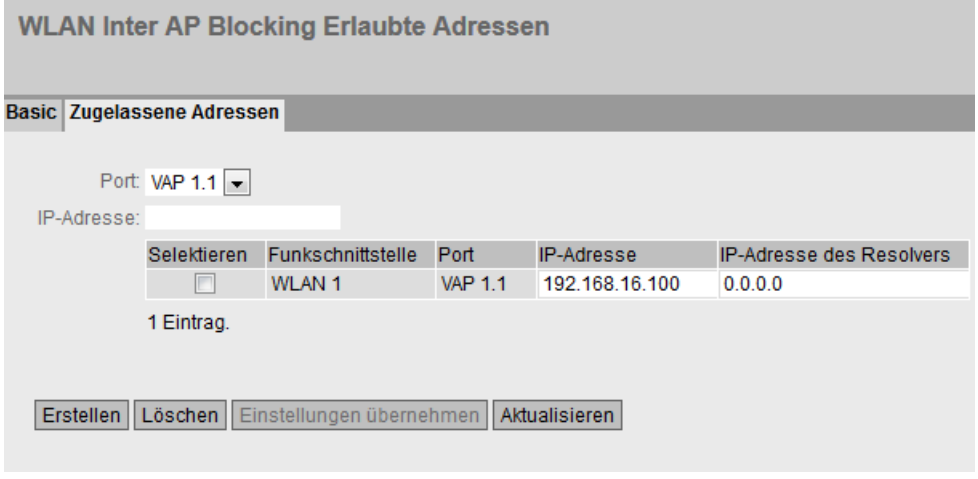
- **Funkschnittstelle**
  Angabe der WLAN-Schnittstelle, auf die sich die Einstellungen beziehen.
- **Port**
  Angabe der VAP-Schnittstelle, auf die sich die Einstellungen beziehen.
- **SSID**
  Angabe der SSID, auf die sich die Einstellungen beziehen.
- **Aktivieren**
  Wenn aktiviert, wird die Zugangsbeschränkung verwendet. Welche Geräte für die Clients zugänglich sind, konfigurieren Sie unter "Security > Inter AP Blocking > Zugelassene Adressen".
- **Blockierte unaufgeforderte ARP-Pakete**
  Wenn aktiviert, werden unaufgeforderte ARP-Pakete von dieser VAP-Schnittstelle nicht an Ethernet weitergeleitet.
- **Blockierte Nicht-IP-Pakete**
  Wenn aktiviert, erfolgt kein Austausch von Nicht-IP-Paketen, z. B. Layer 2-Paketen, zwischen dem Client und den Geräten, die im Access Points als zulässige Kommunikationspartner konfiguriert sind.

6.10.6.2 Zugelassene Adressen

Hinweis

Diese WBM-Seite ist nur im Access Point-Modus verfügbar.

Auf dieser WBM-Seite legen Sie fest, welche Geräte für die Clients zugänglich sind.



Beschreibung

Die Seite enthält folgende Felder:

- **Port**
  Wählen Sie aus der Klappliste den gewünschten Port aus.
- **IP-Adresse**
  Tragen Sie die IP-Adresse der Geräte ein, die für den Client zugänglich sind.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen
- **Funkschnittstelle**
  Angabe der WLAN-Schnittstelle, auf die sich die Einstellungen beziehen
- **Port**
  Angabe der VAP-Schnittstelle, auf die sich die Einstellungen beziehen
- **IP-Adresse**
  Die IP-Adresse der Geräte, die für den Client zugänglich sind. Bei Bedarf können Sie die IP-Adresse ändern.
- **IP-Adresse des Resolvers**
  Die IP-Adresse die der Access Point verwendet, um die zugelassene IP-Adresse aufzulösen. Der Eintrag ist notwendig, wenn sich die Management IP-Adresse des Access Point in einem anderen Subnetz befindet.
  Wenn bei "IP-Adresse des Resolvers" die IP-Adresse "0.0.0.0" konfiguriert wird, wird zum Auflösen die Management IP-Adresse verwendet.

Vorgehensweise

Eintrag anlegen

1. Wählen Sie aus der Klappliste "Port" einen Port aus.
2. Geben Sie im Feld "IP-Adresse" die IP-Adresse ein, die für den Client zugänglich ist.
3. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag angelegt.

Eintrag löschen

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

6.11 Menü "iFeatures"

6.11.1 iPRP

Voraussetzungen, um iPRP auszuführen

- iPRP ist nur mit dem CLP iFeatures verwendbar. Weitere Informationen dazu finden Sie im Kapitel "Configuration License PLUG (CLP) (Seite 25)".
- Der Base Bridge-Modus "802.1Q VLAN Bridge" ist eingestellt
- Die VLANs sind angelegt
- Access Point-Modus: Die VAP-Schnittstelle ist aktiviert
- Client-Modus:
  - Bei "MAC-Modus" ist "Layer 2-Tunnel" eingestellt
  - Bei "Background Scan-Modus" ist entweder "Immer", "Deaktiviert" oder "Aktueller Kanal" eingestellt

Wann sollte iPRP eingesetzt werden?

Hinweis

iPRP mit Oversize-Frames (Jumbo-Frames)

Um Oversize-Frames nutzen zu können, muss bei sämtlichen Geräten im Netzwerk Oversize-Frames (Jumbo-Frames) konfiguriert sein.

Agent VLAN (Management-VLAN) bei iPRP

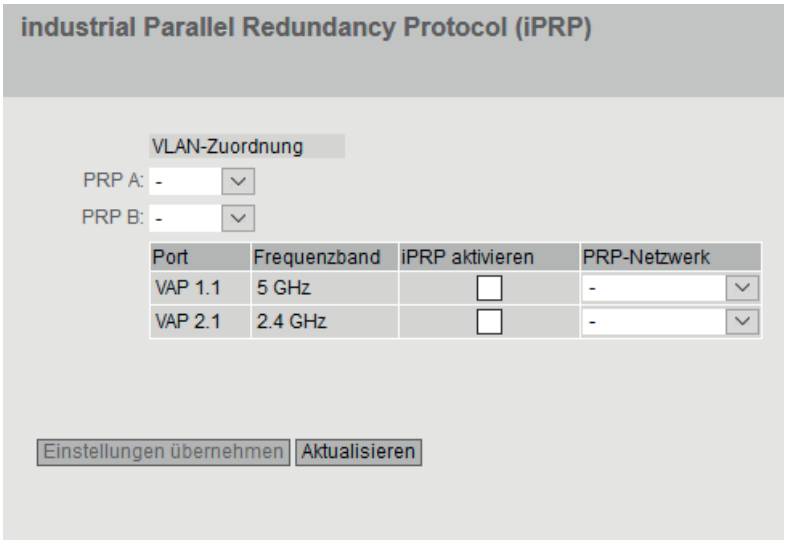
Als Agent-VLAN kann das jeweilige iPRP VLAN verwendet werden. Das ist davon abhängig, wo sich das Gerät befindet.

- Wenn sich das Gerät im PRP-Netzwerk A oder PRP-Netzwerk B befindet, verwenden Sie als Agent VLAN das entsprechende VLAN, das PRP A oder PRP B zugeordnet ist.
- Wenn sich die Access Points in beiden PRP-Netzwerken befinden, können Sie als Agent VLAN eines der beiden VLANs verwenden. Alternativ können Sie auch andere VLANs als Agent-VLANs verwenden. Die Unterteilung in die PRP-Netzwerke A und B muss bestehen bleiben. Ein einziges Management VLAN für alle Geräte in Netzwerk A und B ist nicht ohne Weiteres möglich.

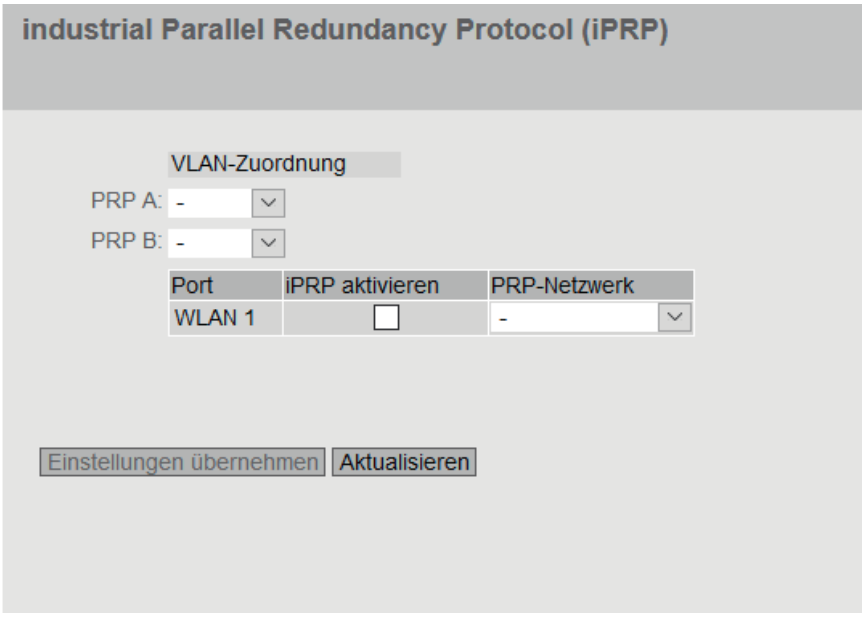
Mit "industrial Parallel Redundancy Protocol" (iPRP) kann die PRP-Technologie in drahtlosen Netzwerken genutzt werden. Bei iPRP werden die PRP-Frames parallel über zwei Funkstrecken übertragen. Dadurch können Störungen bei der Übertragung auf einer Funkstrecke durch die parallele Übertragung auf einer anderen kompensiert werden.

Bei ungleichen Übertragungspfaden reduziert iPRP die Anzahl an duplizierten und out-of-order Paketen. Die verwendete Applikation / das verwendete Protokoll muss mit den verbleibenden Duplikaten und out-of-order Paketen umgehen können.

Darstellung Access Point-Modus



Darstellung Client-Modus



Beschreibung

Die Seite enthält Folgendes:

- Ethernet-Schnittstelle
  Wählen Sie die Ethernet-Schnittstelle aus, für die Sie iPRP konfigurieren wollen.
- **PRP A**
  Wählen Sie die VLAN-Zuordnung für PRP A aus.
- **PRP B**
  Wählen Sie die VLAN-Zuordnung für PRP B aus.

Die Tabelle enthält folgende Spalten:

- **Port**
  Zeigt die verfügbaren Ports an.
- **iPRP aktivieren**
  Aktivieren oder deaktivieren Sie iPRP für den gewünschten Port.
- **PRP-Netzwerk**
  Legen Sie fest, in welchem PRP-Netzwerk der Port Mitglied ist.
- **AP-Redundanz (nur im Client-Modus)**
  - Funkschnittstelle
    Verhindert, dass sich die beiden Clients eines Client-Paares auf die gleiche WLAN-Schnittstelle des Access Points verbinden.
  - Deaktiviert
    Wenn der beste Access Point für einen Client der gleiche Access Point (gleiche WLAN-Schnittstelle) ist, wie der des Partner-Clients, wird geprüft, ob es einen weiteren Access Point gibt, dessen Signalstärke < 10dB schlechter als die des besten Access Points ist. In diesem Fall verbindet sich der Client mit diesem Access Point, ansonsten verbindet er sich mit dem gleichen, besten Access Point wie der Partner-Client.
  - Gerät
    Verhindert, dass sich die beiden Clients eines Client-Paares mit dem gleichen Access Points verbinden, egal auf welcher Schnittstelle.

Vorgehensweise

1. Wählen Sie bei "Ethernet-Schnittstelle" die Ethernet-Schnittstelle aus, die Sie für iPRP verwenden wollen.
2. Wählen Sie bei "PRP A" die VLAN-Zuordnung für PRP A aus.
3. Wählen Sie bei "PRP B" die VLAN-Zuordnung für PRP B aus.
4. Legen Sie fest, in welchem PRP-Netzwerk der Port Mitglied ist.
5. Legen Sie im Client-Modus die Einstellung für "AP-Redundanz" fest.
6. Aktivieren Sie die Einstellung "iPRP aktivieren". Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
   Die zugehörigen VLAN-Einstellungen werden automatisch gesetzt.

Instandhalten und Warten 7

7.1 Firmware-Update über WBM

Voraussetzung

- Das Gerät hat eine IP-Adresse.
- Der Benutzer ist mit Administratorrechten angemeldet.

Hinweis

Das Gerät muss mindestens über eine Firmware der Version 5.1 verfügen. Ein Firmware-Update ist nicht möglich, wenn auf dem Gerät eine Firmware älter als Version 5.1 vorhanden ist.

Firmware-Update über HTTP

1. Klicken Sie im Navigationsbereich auf "System > Laden & Speichern". Klicken Sie auf das Register "HTTP".
2. Klicken Sie in der Tabellenzeile "Firmware" auf die Schaltfläche "Laden".
3. Navigieren Sie zum Ablageort der Firmware-Datei.
4. Klicken Sie im Dialogfenster auf die Schaltfläche "Öffnen". Die Datei wird hochgeladen.

Firmware-Update über TFTP

1. Klicken Sie im Navigationsbereich auf "System > Laden & Speichern". Klicken Sie auf das Register "TFTP".
2. Tragen Sie im Eingabefeld "Adresse des TFTP-Servers" die IP-Adresse des TFTP-Servers ein.
3. Tragen Sie Im Eingabefeld "Port des TFTP-Servers" den Port des TFTP-Servers ein.
4. Klicken Sie in der Tabellenzeile "Firmware" auf die Schaltfläche "Datei hochladen".
5. Navigieren Sie zum Ablageort der Firmware-Datei.
6. Klicken Sie im Dialogfenster auf die Schaltfläche "Öffnen". Die Datei wird hochgeladen.

Firmware-Update über SFTP

1. Klicken Sie im Navigationsbereich auf "System > Laden & Speichern". Klicken Sie auf das Register "SFTP".
2. Tragen Sie im Eingabefeld "Adresse des SFTP-Servers" die IP-Adresse des SFTP-Servers ein.
3. Tragen Sie Im Eingabefeld "Port des SFTP-Servers" den Port des SFTP-Servers ein.
4. Klicken Sie in der Tabellenzeile "Firmware" auf die Schaltfläche "Datei hochladen".

5. Navigieren Sie zum Ablageort der Firmware-Datei.
6. Klicken Sie im Dialogfenster auf die Schaltfläche "Öffnen". Die Datei wird hochgeladen.

Ergebnis

Die Firmware ist komplett auf das Gerät übertragen.

Auf der Seite "Information > Versionen" gibt es die Einträge "Firmware" und "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. Um diese Firmware zu aktivieren, starten Sie über "System > Neustart" das Gerät neu.

7.2 Firmware in ConfigPack einbinden

Bitte beachten Sie die ergänzenden Informationen und Sicherheitshinweise in der Betriebsanleitung ihres Geräts.

Mit dem ConfigPack mit eingebundener Firmware-Datei können Sie eine Gerätekonfiguration inklusive der dazugehörigen Firmware auf einem oder auch mehreren Geräten installieren.

ConfigPack mit eingebundener Firmware erstellen

Um die Firmware in ein ConfigPack einzubinden, müssen sie eine Einstellung im Command Line Interface (CLI)vornehmen. Gehen Sie hierzu vor wie folgt:

Hinweis

Konfigurationen mit DHCP verwenden

Wenn Sie das ConfiPack mit eingebundener Firmware nutzen möchten, um mehrere Geräte mit gleicher Konfiguration und Firmware in Betrieb zu nehmen, erstellen Sie ein ConfigPack nur aus Gerätekonfigurationen, die DHCP verwenden. Es treten sonst Störungen im Netzwerkbetrieb durch mehrfache gleiche IP-Adressen auf.

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

1. Starten sie die Remote-Konfiguration über Telnet (CLI) und melden sich mit einem Benutzer an, der die Rolle "admin" besitzt.
2. Wechseln Sie in den globalen Konfigurationsmodus mit dem Befehl "configure terminal".

3. Gehen Sie in den Loadsave-Konfigurationsmodus ein mit dem Befehl "loadsave".
4. Geben Sie den Befehl "firmware-in-configpack" ohne Parameter ein.
   Die auf diesem Gerät aktuelle Firmware wird nun als eigene Datei in dem ConfigPack mit eingebunden, wenn Sie dieses speichern.

Hinweis

Firmware in ConfigPack einbinden

Bei einem Neustart des Geräts geht diese Funktionalität wieder verloren und muss erneut aktiviert werden.

Wenn Sie im WBM oder CLI ein ConfigPack speichern ist die Firmware eingebunden. Die Datei kann vor dem Herunterladen mit einem Passwort versehen werden. Um die Datei erfolgreich ins Gerät zuladen, ist das festgelegte Passwort zu verwenden.

Beachten Sie die Hinweise im Kapitel Laden & Speichern (Seite 170).

ConfigPack mit eingebundener Firmware installieren

Hinweis

ConfigPack mit DHCP Optionen 66, 67 installieren

Sie können das ConfigPack auch über DHCP mit den aktivierten Optionen 66 und 67 installieren.

Sie aktivieren die Optionen im Menü "System > DHCP > DHCP Client".

Passwortgeschützte ConfigPack und DHCP-Optionen 66.67

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

Wenn Sie über WBM oder CLI ein ConfigPack installieren, wird auch eine dort gespeicherte Firmware installiert.

Vorgehensweise beim WBM

1. Verbinden Sie sich als Administrator mit dem WBM des Geräts auf dem das ConfigPack installiert werden soll.
2. Navigieren sie in das Menü "System > Laden & Speichern".
3. Klicken Sie in der Zeile "ConfigPack" auf die Schaltfläche "Hochladen".
4. Wählen Sie das ConfigPack aus, das Sie installieren möchten.
5. Starten Sie über "System > Neustart" das Gerät neu.
   Wenn auf dem zu installierenden Gerät eine andere Firmwareversion als die im ConfigPack enthaltene vorhanden ist, wird ein Up-/Downgrade der Firmware durchgeführt. Sie erkennen dies am Blinken der roten F-LED (Blinkintervall: 2Sek an/0.2Sek. aus). Danach wird das Gerät neu gestartet und die indem ConfigPack gespeicherte Gerätekonfiguration, inkl. Benutzer und Zertifikate auf das Gerät überspielt.
6. Warten Sie, bis das Gerät vollständig hochgefahren ist.
   (die rote F-LED ist aus)
7. Sie können sich am Gerät neu anmelden oder das WBM beenden.

7.3 Gerätekonfiguration mit PRESET-PLUG

Bitte beachten Sie die ergänzenden Informationen und Sicherheitshinweise in der Betriebsanleitung ihres Geräts.

ACHTUNG
PLUG nicht im laufenden Betrieb ziehen oder stecken! Ein PLUG darf nur bei ausgeschaltetem Gerät entnommen oder eingesetzt werden.

Hinweis

Unterstützung der PRESET-PLUG Funktionalität

SCALANCE W700ax unterstützt die PRESET-PLUG-Funktionalität ab der Firmwareversion V1.0. Bei dem SCALANCE W1700ac wird die PRESET-PLUG Funktionalität ab V1.1 unterstützt.

Mit dem PRESET-PLUG können Sie dieselbe Gerätekonfiguration (Startkonfiguration, Benutzeraccounts, Zertifikate) inklusive der dazugehörigen Firmware auf mehreren Geräten installieren.

Der PRESET-PLUG ist schreibgeschützt.

Sie konfigurieren den PRESET-PLUG mit Hilfe des Command Line Interface (CLI).

PRESET-PLUG erstellen

Erstellen Sie den PRESET-PLUG mit Hilfe des Command Line Interface (CLI). Sie können einen PRESET-PLUG aus jedem PLUG erstellen. Gehen Sie hierzu vor wie folgt:

Hinweis

Konfigurationen mit DHCP verwenden

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

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

Voraussetzung

- Im Gerät ist ein CLP gesteckt, auf dem Sie die Funktionalität PRESET-PLUG konfigurieren wollen.

Vorgehen

1. Starten sie die Remote-Konfiguration über SSH (CLI) und melden sich mit einem Benutzer an, der die Rolle "admin" besitzt.
2. Wechseln Sie in den globalen Konfigurationsmodus mit dem Befehl "configure terminal".
3. Gehen Sie in den PLUG-Konfigurationsmodus mit dem Befehl "plug".

4. Erstellen Sie den PRESET-PLUG mit dem Befehl "presetplug".
   Die Firmwareversion des Geräts, sowie die aktuelle Gerätekonfiguration inkl. Benutzeraccounts und Zertifikate, werden auf dem PLUG gespeichert und der PLUG wird anschließend schreibgeschützt.
5. Schalten Sie das Gerät spannungslos.
6. Entnehmen sie den PRESET-PLUG.
7. Starten Sie das Gerät wahlweise mit einem gesteckten neuen CLP oder mit der internen Konfiguration.

Vorgehen zur Installation mit Hilfe des PRESET-PLUG

1. Schalten Sie das Gerät spannungslos.
2. Falls vorhanden, entnehmen Sie den CLP aus dem Steckplatz. Weitere Informationen dazu finden Sie in der Betriebsanleitung ihres Geräts.
3. Setzen Sie den PRESET-PLUG in der richtigen Orientierung in den Steckplatz. Der PRESET-PLUG ist richtig eingesetzt, wenn er sich vollständig im Gerät befindet und nicht aus dem Steckplatz herausragt.
4. Schalten Sie das Gerät wieder ein.
   Wenn auf dem zu installierenden Gerät eine andere Firmwareversion als die auf dem PRESET-PLUG gespeicherte vorhanden ist, wird ein Up-/Downgrade der Firmware durchgeführt. Sie erkennen dies am Blinken der roten F-LED (Blinkintervall: 2Sek an/0.2Sek. aus). Danach wird das Gerät neu gestartet und die auf dem PRESET-PLUG gespeicherte Gerätekonfiguration, inkl. Benutzer und Zertifikate, auf das Gerät überspielt.
5. Warten Sie, bis das Gerät vollständig hochgefahren ist.
   (die rote F-LED ist aus)
6. Schalten Sie das Gerät nach der Installation ab.
7. Entnehmen Sie den PRESET-PLUG.
8. Starten Sie das Gerät wahlweise mit einem gesteckten neuen CLP oder mit der internen Konfiguration.

Hinweis

Auf Werkseinstellungen zurücksetzen und Neustart mit gestecktem PRESET-PLUG

Wenn Sie das Gerät auf Werkseinstellungen zurücksetzen, wird beim Neustart des Geräts ein gesteckter PRESET-PLUG formatiert und die Funktionalität PRESET-PLUG geht verloren. Sie müssen dann einen neuen PRESET-PLUG erstellen. Die auf einem KEY-PLUG gespeicherten Schlüssel zur Freischaltung von Funktionen bleiben erhalten.

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

PRESET-PLUG formatieren (Preset-Funktion zurücksetzen)

Formatieren Sie den PRESET-PLUG mit Hilfe des Command Line Interface (CLI), um die Preset-Funktion zurückzusetzen. Gehen Sie hierzu vor wie folgt:

1. Starten sie die Remote-Konfiguration über SSH (CLI) und melden sich mit einem Benutzer aln, der die Rolle "admin" besitzt.
2. Wechseln Sie in den globalen Konfigurationsmodus mit dem Befehl "configure terminal".
3. Gehen Sie in den PLUG-Konfigurationsmodus mit dem Befehl "plug".
4. Geben Sie den Befehl "factoryclean" ein.
   Der PRESET-PLUG wird formatiert und die Preset-Funktion wird zurückgesetzt.
5. Schreiben Sie die aktuelle Konfiguration des Geräts auf den PLUG mit dem Befehl "write".

7.4 Wiederherstellen der Werkseinstellungen

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

ACHTUNG
Versehentliches Rücksetzen Durch ein versehentliches Rücksetzen können in einem projektierten Netzwerk Störungen und Ausfälle mit weiteren Folgen auftreten.

Mit dem Reset-Taster

Beachten Sie zur Betätigung des Tasters unbedingt die Hinweise in Kapitel "Reset-Taster" in der Betriebsanleitung.

Führen Sie folgende Schritte durch, um die Gerätparameter auf die Werkseinstellungen zurückzusetzen:

1. Schalten Sie das Gerät spannungslos.
2. Lösen Sie die Schrauben der Abdeckung.
3. Entfernen Sie die Abdeckung.
4. Drücken Sie nun den Reset-Taster und schließen Sie das Gerät mit gedrücktem Taster wieder an die Versorgungsspannung an.
5. Halten Sie den Taster so lange gedrückt, bis die rote Fehler LED (F) nach ca. 10 Sekunden aufhört zu blinken und in Dauerlicht wechselt.
6. Lassen Sie nun den Taster los und warten Sie, bis die Fehler-LED (F) wieder erlischt.
7. Das Gerät startet dann automatisch mit den Werkseinstellungen.

Mit SINEC PNI

Führen Sie folgende Schritte aus, um die Geräteparameter mit dem SINEC PNI auf die Werkseinstellungen zurückzusetzen:

1. Wählen Sie das Gerät aus, dessen Parameter Sie zurücksetzen wollen.
2. Klicken Sie auf die Schaltfläche "Gerät zurücksetzen".
3. Wählen Sie im folgenden Dialog die Option "Auf Werkseinstellungen zurücksetzen".

Über die Projektierung

Ausführliche Informationen zum Zurücksetzen der Geräteparameter über WBM und CLI finden Sie in den Projektierungshandbüchern:

- Web Based Management, Kapitel "Neustart"
- Command Line Interface, Kapitel "Reset and Defaults"

Troubleshooting/FAQ

8

8.1 Firmware-Update über WBM oder CLI nicht möglich

Ursache

Wenn es während eines Firmware-Updates zu einem Spannungsausfall kommt, kann es vorkommen, dass das Gerät weder über das Web Based Management oder das CLI erreichbar ist.

Beachten Sie zur Betätigung des Tasters unbedingt die Hinweise in Kapitel "Reset-Taster".

Abhilfe

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

1. Schalten Sie das Gerät spannungslos.
2. Drücken Sie nun den Reset-Taster und schließen Sie das Gerät mit gedrücktem Taster wieder an die Versorgungsspannung an.
3. Halten Sie den Taster so lange gedrückt, bis die rote Fehler LED (F) nach ca. 2 Sekunden anfängt zu blinken.
4. Lassen Sie nun den Taster los. Der Bootloader wartet in diesem Zustand auf eine neue Firmware-Datei, die Sie per TFTP laden können.
5. Verbinden Sie einen PC über die Ethernet-Schnittstelle mit dem SCALANCE W.
6. Vergeben Sie mit dem SINEC PNI eine IP-Adresse für den SCALANCE W.
7. Wechseln Sie in einer DOS-Box in das Verzeichnis, in dem sich die Datei mit der neuen Firmware befindet und rufen Sie danach den Befehl "tftp -i <ip-adresse> PUT <firmware>" auf. Alternativ dazu können Sie einen anderen TFTP-Client verwenden.
8. Verschließen Sie die Abdeckung, um sicherzustellen, dass das Gerät wasser- und staubdicht verschlossen ist.

Hinweis

Verwenden von CLI und TFTP unter Windows 10

Wenn Sie unter Windows 10 auf CLI oder TFTP zugreifen wollen, achten Sie darauf, dass die entsprechenden Funktionen in Windows 10 freigeschaltet sind.

Ergebnis

Die Firmware wird auf das Gerät übertragen.

Hinweis

Bitte beachten Sie, dass die Übertragung der Firmware einige Minuten dauern kann. Während der Übertragung blinkt die rote Fehler LED (F).

Nachdem die Firmware komplett auf das Gerät übertragen ist, wird das Gerät automatisch neu gestartet.

8.2 Störungen der Datenübertragung durch zu große Empfangsleistung

Ursachen und Auswirkungen zu großer Empfangsleistungen

Eine zu große Empfangsleistung am Eingang eines SCALANCE W-Geräts übersteuert dessen Verstärkerschaltung. Übersteuerung kann bei Clients und Access Points auftreten. Wenn die Empfangsleistung am SCALANCE W-Gerät größer als -35 dBm ist, kann es zu Kommunikationsstörungen kommen.
Informationen über die Signalstärke [in dBm] werden Ihnen im WBM auf folgenden Registern angezeigt:

Access Point-Modus:

- Informationen > WLAN > Client-Liste

Client-Modus:

- Informationen > WLAN > Verfügbare APs

Beeinflusst wird die Leistung des Eingangssignals am SCALANCE W-Gerät von folgenden Faktoren:

- Abstand zwischen den WLAN-Partnern
- Reflexionen der elektromagnetischen Wellen durch bauliche Gegebenheiten
- Einstellung der "max. Tx-Leistung" und die verwendeten Antennen-Einstellungen (Schnittstellen > WLAN > Antennen & Leistung)

Abhilfe

Wenn die Kommunikation durch eine zu große Signalstärke (größer -35 dBm) beeinträchtigt ist, haben Sie folgende Möglichkeiten, die Störung zu beseitigen:

- Vergrößern Sie den Abstand zwischen Sender und Empfänger.
- Reduzieren Sie gegebenenfalls die Sendeleistung des IWLAN-Partners über geeignete Einstellungen im WBM oder im CLI.

8.3 Hinweise für eine sichere Netzauslegung

Beachten Sie folgende Hinweise, um Ihr Netz vor Angriffen zu schützen:

- **Verwenden Sie eine sichere Verbindung mit HTTPS**
  HTTPS ermöglicht Ihnen im Gegensatz zu HTTP einen sicheren Zugang zur Konfiguration der WLAN Clients und der Access Points über das Web Based Management. Weitere Informationen dazu finden Sie im Kapitel "Laden & Speichern (Seite 170)".
- **Verwenden Sie WPA2/ WPA2-PSK mit AES**
  Verwenden Sie nur WPA2/AES, um einen Passwortmissbrauch zu verhindern. WPA2/ WPA2-PSK mit AES bietet die größte Sicherheit. Weitere Informationen dazu finden Sie im Kapitel "Menü "Security" (Seite 322)".
- **Schützen Sie ihr Netz vor Man-in-the-Middle-Angriffen**
  Um Ihr Netz vor Man-in-the-Middle-Angriffen zu schützen, wird ein Netzaufbau empfohlen, der es dem Angreifer erschwert, sich in den Kommunikationsweg zwischen zwei Endgeräten einzuschalten.
  - Geräte können Sie z. B. dadurch schützen, indem der Agent IP nur über ein eigenes Management VLAN zugänglich ist. Weitere Informationen dazu finden Sie im Kapitel "Menü "Layer 3 (IPv4)" (Seite 311)".
  - Eine weitere Möglichkeit besteht darin, am WLAN Client / Access Point ein eigenes HTTPS-Zertifikat zu installieren. Das HTTPS-Zertifikat überprüft die Identität des Geräts und regelt den verschlüsselten Datenaustausch. Sie können das HTTPS-Zertifikat z. B. über HTTP installieren. Weitere Informationen dazu finden Sie im Kapitel "HTTP (Seite 174)".
- **Verwenden Sie SNMPv3**
  SNMPv3 bietet Ihnen die größtmögliche Sicherheit beim Zugriff auf die Geräte über SNMP. Weitere Informationen dazu finden Sie im Kapitel "SNMP (Seite 205)".

ACHTUNG
Änderung des Default-Passworts nach Konfiguration über STEP 7 Wenn ein Gerät im Default-Zustand nur über STEP 7 konfiguriert wird, ist es nicht möglich, das Default-Passwort zu ändern. Diese Änderung muss über WBM oder CLI direkt am Gerät erfolgen. Andernfalls bleibt das Default-Passwort bestehen und jeder Nutzer könnte sich mit dem Default-Passwort einloggen.

Anhang A "Unterstützte MIB-Module"

A

A.1 Unterstützte MIB-Dateien

Beim SCALANCE W-Gerät zur Verfügung stehende MIB-Dateien

Die nachfolgende Tabelle zeigt die MIB-Dateien, die bei einem SCALANCE W-Gerät zur Verfügung stehen:

MIB	Root OID	Referenz
AUTOMATION-SYSTEM-MIB (Siemens) [1]	.1.3.6.1.4.1.4329.6.3.2	Vendor specific
AUTOMATION-SN-SYSTEM-MIB (Siemens) [1] [2]	.1.3.6.1.4.1.4329.6.1.2.100.2	Vendor specific
AUTOMATION-SN-AUTH-MIB (Siemens) [1] [2]	.1.3.6.1.4.1.4329.6.1.2.100.3	Vendor specific
AUTOMATION-SNTP (Siemens) [1] [2]	.1.3.6.1.4.1.4329.6.3.11	Vendor specific
AUTOMATION-SMTP (Siemens) [1] [2]	.1.3.6.1.4.1.4329.6.3.9	Vendor specific
AUTOMATION-TELNET (Siemens) [1] [2]	.1.3.6.1.4.1.4329.6.3.8	Vendor specific
AUTOMATION-TIME-MIB (Siemens) [1] [2]	.1.3.6.1.4.1.4329.6.3.3	Vendor specific
AUTOMATION-PS-MIB (Siemens) [1] [2]	.1.3.6.1.4.1.4329.6.3.5	Vendor specific
IF-MIB	.1.3.6.1.2.1.2	RFC 2863
EtherLike-MIB	.1.3.6.1.2.1.10.7.2	RFC 3635
MAU-MIB	.1.3.6.1.2.1.26	RFC 4836
ENTITY-MIB	.1.3.6.1.2.1.47	RFC 4133
Q-BRIDGE-MIB	.1.3.6.1.2.1.17.7	RFC 2674q
P-BRIDGE-MIB	.1.3.6.1.2.1.17.6	RFC 2674p
BRIDGE-MIB	.1.3.6.1.2.1.17	RFC 4188
IPV6-MIB	.1.3.6.1.2.1.55	RFC 2465
SNMPv2-MIB	.1.3.6.1.2.1.1	RFC 3418
SNMP-COMMUNITY-MIB	.1.3.6.1.6.3.18	RFC 3584
SNMP-USER-BASED-SM-MIB	.1.3.6.1.6.3.15	RFC 3414
SNMP-VIEW-BASED-ACM-MIB	.1.3.6.1.6.3.16	RFC 3415
SNMP-NOTIFICATION-MIB	.1.3.6.1.6.3.13	RFC 3413
SNMP-TARGET-MIB	.1.3.6.1.6.3.12	RFC 3413
SNMP-MPD-MIB	.1.3.6.1.6.3.10.2.1	RFC 3412
RADIUS-ACC-CLIENT-MIB	.1.3.6.1.2.1.67.2.2	RFC 2620
RADIUS-AUTH-CLIENT-MIB	.1.3.6.1.2.1.67.1.2	RFC 2618
RMON-MIB	.1.3.6.1.2.1.16	RFC 2819
IP-MIB	.1.3.6.1.2.1.4	RFC 4292
TCP-MIB	.1.3.6.1.2.1.6	RFC 4022
UDP-MIB	.1.3.6.1.2.1.7	RFC 4113
DNS-RESOLVER-MIB	.1.3.6.1.2.1.32.2	RFC 1612
NAT-MIB	.1.3.6.1.2.1.123	RFC 4008

MIB	Root OID	Referenz
IEEE802dot11-MIB	.1.2.840.10036	IEEE 802.11
IEEE 802.1AB 2005 LLDP-MIB (Siemens) [1) 2)]	.1.0.8802.1.1.2	Vendor specific
LLDP-EXT-DOT1-MIB (Siemens) [1) 2)]	.1.0.8802.1.1.2.1.5.32962	Vendor specific
LLDP-EXT-DOT3-MIB (Siemens) [1) 2)]	.1.0.8802.1.1.2.1.5.4623	Vendor specific
LLDP-EXT-PNO-MIB (Siemens) [1) 2)]	.1.0.8802.1.1.2.1.5.3791	Vendor specific
SN-MSPS-SNMP-MIB (Siemens) [2)]	.1.3.6.1.4.1.4329.20.1.1.1	Vendor specific
SN-MSPS-SCW-MIB (Siemens) [1) 2)]	.1.3.6.1.4.1.4329.20.1.1.1.1.27.1.10.19.3	Vendor specific
SN-MSPS-SCW-MIB (Siemens) [1) 2)]	.1.3.6.1.4.1.4329.20.1.1.1.1.1.100.10	Vendor specific

1) Bestandteil der AUTOMATION.MIB

   Die AUTOMATION.MIB für SCALANCE W können Sie bei Siemens Industry Automation and Drives Service & Support unter folgender Beitrags-ID 67637278 (https://support.industry.siemens.com/cs/ww/de/view/67637278) herunterladen

2) Bestandteil der Privaten MIB-Datei "Scalance_w_msps.mib". Die Datei können Sie im WBM unter "System > Laden & Speichern > HTTP > MIB" über die Schaltfläche "Speichern" herunterladen.

Anhang B "Private MIBs"

B

B.1 Private MIB-Variablen

Download der MIB des SCALANCE W über WBM

Die MIB des SCALANCE W können Sie im WBM unter "System > Laden & Speichern > HTTP > MIB" über die Schaltfläche "Speichern" herunterladen.

OID

Die Private MIB-Variablen des SCALANCE W haben folgenden Object Identifier:
`iso(1).org(3).dod(6).internet(1).private(4). enterprises(1) siemens(4329) industrialComProducts(20) iComPlatforms(1) simaticNet(1) snMsps(1) snMspsCommon(1)`

WLAN-spezifische MIB-Variablen

Die WLAN-spezifischen MIB-Variablen sind unter "`snMspsWlan`" zu finden. In der MIB-Datei finden Sie weitere Informationen zu den Einstellungen und Werten.

Anhang C "Zugrundeliegende Normen"

C

C.1 Zugrundeliegende Normen

Normen, die von SCALANCE W-Geräten vollständig oder teilweise erfüllt werden

Die folgende Tabelle enthält einen Teil der Normen für SCALANCE W-Geräte.

Bezeichnung der Norm	Thema
IEEE 802.1AB	Link Layer Discovery Protocol (LLDP)
IEEE 802.1D-1998	Media Access Control (MAC), bridges
IEEE 802.1Q	Virtual Bridged LANs (VLAN Tagging, Port Based VLANs)
IEEE 802.1W-2004	Rapid Spanning Tree Protocol (RSTP)
IEEE 802.1X	Port Based Network Access Control
IEEE 802.3-2002	Ethernet
IEEE 802.3af	Power over Ethernet (PoE)
IEEE 802.11	Wireless Local Area Network
IEEE 802.11a	Funkstandard zur Nutzung des Frequenzbereichs 5 GHz
IEEE 802.11at	POE +
IEEE 802.11b/g	Funkstandard zur Nutzung des Frequenzbereichs 2,4 GHz
IEEE 802.11e	Quality of Service (QoS)
IEEE 802.11 h	Erweiterung beim Spektrum und bei der Sendeleistung zur Nutzung des Frequenzbereichs 5 GHz in Europa.
IEEE 802.11i	Verschlüsselung von WLANS
IEEE 802.11n	Standard für hohe Übertragungsraten
IEEE 802.11ac	Standard für sehr hohe Übertragungsraten im 5 GHz Frequenzband
IEEE 802.11w	Standard für Verschlüsselung der übertragenen Management-Informationen zum Aufbau und Betrieb von Datenverbindungen

Anhang D "Log-Meldungen"

D

D.1 Meldungen im Ereignis-Log

Meldungen beim Systemanlauf (allgemein)

Meldung	Beschreibung
Warm start performed, Ver: V02.00.00 - event/ status summary after startup	Art des Anlaufs und die geladene Firmwareversion.
Power supply: • L1 is connected • L2 is not connected	Status der Spannungsversorgungen Line 1 und Line 2.
No line is monitored	Information über die Überwachung der Spannungsversorgung durch das Meldesystem.
MSTP disabled MSTP enabled	Information über den Status des Spanning Tree Protokolls.
No Fault states pending after startup	Fehlerstatus nach Systemstart.

Status der Spannungsversorgung

Das Ereignis "Umschalten der Spannungsversorgung" aktivieren oder deaktivieren Sie unter "System > Ereignisse".

Meldung	Beschreibung
Power up on line 1 / 2 / PoE.	Spannungsversorgung an Line 1, Line 2 bzw. über PoE vorhanden.
Power down on line 1 / 2 / PoE.	Spannungsversorgung an Line 1, Line 2 bzw. über PoE unterbrochen.

Status der Ethernet-Schnittstelle

Das Ereignis "Link Change" aktivieren oder deaktivieren Sie unter "System > Ereignisse".

Meldung	Beschreibung
Link up on P1.	An der Ethernet-Schnittstelle ist eine Verbindung vorhanden.
Link down on P1.	An der Ethernet-Schnittstelle ist keine Verbindung vorhanden.

Status der WLAN-Schnittstelle (im Access Point-Modus)

Meldungen	
Link down up VAP X.Y.	Die VAP-Schnittstelle Y an WLAN-Schnittstelle X ist aktiviert.
Link down on VAP X.Y.	Die VAP-Schnittstelle Y an WLAN-Schnittstelle X ist deaktiviert.
WDS Y at WLAN X is up.	An der WDS-Schnittstelle Y von WLAN-Schnittstelle X ist ein Link vorhanden.

Meldungen	
WDS Y at WLAN X is down.	An der WDS-Schnittstelle Y von WLAN-Schnittstelle X ist kein Link vorhanden.
Overlap-AP found on WLAN X: AP <System Name> <MAC> found on channel <Kanalnummer.> <RSSI Wert>	Auf dem, für die WLAN-Schnittstelle X, eingestellten Kanal oder auf einem benachbarten Kanal wurde ein weiterer Access Point detektiert.
Overlap-AP aged out on WLAN X: AP <System Name> <MAC> on channel <Kanalnummer.> <RSSI Wert>	Der überlappende Access Point konnte für die Dauer der konfigurierten Aging Time nicht mehr detektiert werden und wurde aus der Liste überlappender APs entfernt.
DFS: Radar interference detected on WLAN X at channel <Kanalnummer.> (frequency <Frequenz> MHz). Changing to channel <Kanalnummer> (frequency <Frequenz> MHz)	Auf dem, für die WLAN-Schnittstelle X, eingestellten Kanal oder auf einem benachbarten Kanal wurde ein Primärnutzer (z.B. Radar oder Wetterstation) detektiert. Der Kanal wird für 30 min gesperrt. Der Access Point wechselt auf den konfigurierten Alternativkanal oder auf den nächsten freien Kanal auf dem sich kein Primärnutzer befindet.
DFS: channel <Kanalnummer> (frequency <Frequenz> MHz) aged out from NOL at WLAN X and can be used again.	Auf dem Kanal konnte kein Primärnutzer mehr detektiert werden. Der Kanal wurde aus der Liste der gesperrten Kanäle ausgetragen und kann wieder verwendet werden
DFS: Radar interference detected on WLAN X at channel <Kanalnummer> (frequency <Frequenz> MHz). No more free channels to use!!	Auf allen verfügbaren Kanälen wurde ein Primärnutzer detektiert. Es steht kein freier Kanal zur Verfügung, die WLAN-Schnittstelle X wird deaktiviert, bis wieder einer der Kanäle zur Verfügung steht.

Status der WLAN-Schnittstelle (im Client-Modus)

Meldungen	Beschreibung
Link up on WLAN X.	Die WLAN-Schnittstelle X ist aktiviert.
Link down on WLAN X.	Die WLAN-Schnittstelle X ist deaktiviert.

Meldungen zur Konfiguration

Meldungen	Beschreibung
WBM: Authentication failure.	Beim Login über Web Based Management (WBM) erfolgte eine falsche Passworteingabe. Das Ereignis kann in "System > Ereignisse" aktiviert bzw. deaktiviert werden (Authentication Failure).
Telnet: Authentication failure.	Beim Login über Telnet erfolgte eine falsche Passworteingabe. Das Ereignis kann in "System > Ereignisse" aktiviert bzw. deaktiviert werden (Authentication Failure).
Restart requested	Neustart auf Grund einer Benutzeranforderung. Das Ereignis kann in "System > Ereignisse" aktiviert bzw. deaktiviert werden (Cold/Warm Start).

Meldungen zum Datei up- bzw. download

Meldungen	Beschreibung
File upload via HTTP(S): load of FileType <Dateityp> OK → restart required	Das Laden der Datei via HTTP(S) war erfolgreich. Ein Neustart ist erforderlich.
File upload via HTTP(S): load of FileType<Dateityp> OK	Das Laden der Datei via HTTP(S) war erfolgreich.

Meldungen	Beschreibung
File upload via HTTP(S): validation of FileType <Dateityp> IDENTICAL	Das Laden der Datei via HTTP(S) war erfolgreich. Die Datei ist identisch zu der bestehenden.
File upload via HTTP(S): validation of FileType <Dateityp> FAILED	Das Laden der Datei via HTTP(S) ist fehlgeschlagen. Die Datei ist fehlerhaft bzw. ungültig.
File upload via TFTP: load of FileType <Dateityp> OK → restart required	Das Laden der Datei via TFTP war erfolgreich. Ein Neustart ist erforderlich.
File upload via TFTP: load of FileType <Dateityp> OK	Das Laden der Datei via TFTP war erfolgreich.
File upload via TFTP: validation of FileType <Dateityp> IDENTICAL	Das Laden der Datei via TFTP war erfolgreich. Die Datei ist identisch zu der bestehenden.
File upload via TFTP: validation of FileType <Dateityp> FAILED	Das Laden der Datei via TFTP ist fehlgeschlagen. Die Datei ist fehlerhaft bzw. ungültig.
File upload via TFTP: file transfer of FileType <Dateityp> FAILED	Das Laden der Datei via TFTP ist fehlgeschlagen. Der Dateiname ist falsch bzw. die Datei ist nicht auf dem Server vorhanden.
File upload via TFTP: file transfer of FileType <Dateityp> failed. Cannot connect to given IP address	Das Laden der Datei via TFTP ist fehlgeschlagen. Der TFTP Server ist nicht erreichbar bzw. die Einstellungen sind fehlerhaft.
File download via TFTP: file transfer of FileType <Dateityp> failed. Cannot connect to given IP address	Das Speichern der Datei via TFTP ist fehlgeschlagen. Der TFTP Server ist nicht erreichbar bzw. die Einstellungen sind fehlerhaft.

Meldungen Fehlerstatus

Meldungen	Beschreibung
	Die Ereignisse konfigurieren Sie unter "System > Ereignisse". Die Überwachung der Spannungsversorgung und dem Link am Ethernet Port konfigurieren Sie unter "System > Fehlerkontrolle".
New Fault state: <Fehlerbeschreibung> <Fehlerbeschreibung>:"Warm start performed." "Cold start performed." "Link down on P1." "Link up on P1." "Power down on line L1 (L2)" "DFS: No channels are available at WLAN2"	Kommender Fehler. Nicht alle Ereignisse führen automatisch zu einem Fehler. Auf der WBM-Seite "Ereignisse" legen Sie fest, welche Ereignisse protokolliert werden, z. B. Neustart des Geräts, geänderter Link am Ethernet Port.
Fault state gone: <Fehlerbeschreibung> <Fehlerbeschreibung>:"Warm start performed." "Cold start performed." "Link down on P1." "Link up on P1." "Power down on line L1 (L2)" "DFS: No channels are available at WLAN2" "PLUG not accepted. See System PLUG mask for details."	Gehender Fehler
New Fault state (reconfiguration): <Fehlerbeschreibung> <Fehlerbeschreibung>:"Link down on P1." "Link up on P1." "Power down on line L1 (L2)"	Kommender Fehler. Das Ereignis wurde auf Grund einer Änderung der Konfiguration ausgelöst.

Meldungen	Beschreibung
Fault state gone (reconfiguration): <Fehlerbeschreibung> <Fehlerbeschreibung>:"Link down on P1." "Link up on P1." "Power down on line L1 (L2)".	Gehender Fehler. Das Ereignis wurde auf Grund einer Änderung der Konfiguration ausgelöst.
Fault state: <Fehlerbeschreibung> cleared. <Fehlerbeschreibung>:"Warm start performed" "Cold start performed".	Fehler wurde vom Anwender quittiert.

Meldungen zum MSTP

Meldungen	Beschreibung
	Das Ereignis "Spanning Tree" aktivieren oder deaktivieren Sie unter "System > Events"
Spanning Tree: topology change detected.	Die Topologie des Netzwerks hat sich geändert; das Netzwerk wird reorganisiert.
Spanning Tree: new root bridge xx:xx:xx:xx:xx:xx detected.	Die Topologie des Netzwerks hat sich geändert; im Netzwerk befindet sich eine neue Root Bridge mit der Mac-Adresse xx:xx:xx:xx:xx:xx.

Meldungen zur Sicherheit

Meldungen	Beschreibung
RADIUS: Access accepted / rejected for client <MAC>.	Die Authentifizierung des Clients war erfolgreich bzw. nicht erfolgreich.

Meldungen zum Meldesystem

Meldungen	Beschreibung
Syslog-Server not reachable!	Der konfigurierte Syslog-Server ist nicht erreichbar.
Unable to send messages to syslog server. Please check syslog socket configuration.	Die Syslog-Server Konfiguration ist unvollständig.
Unable to send e-mail(s) because of IP connection failure.	Versenden von E-Mail(s) fehlgeschlagen. SMTP-Server nicht erreichbar (z.B. Netzwerkverbindung unterbrochen).
Unable to send e-mail(s) because of SMTP authentication failure.	Versenden von E-Mail(s) fehlgeschlagen. Authentifizierung des Clients am SMTP-Server fehlerhaft.
Unable to send e-mail(s) because SMTP message transfer failed.	Versenden von E-Mail(s) fehlgeschlagen. SMTP-Server erreichbar, Konfiguration unvollständig bzw. fehlerhaft (z.B. Receiver Email Adress falsch / nicht vorhanden).
SNMP: Authentification failure.	Authentifizierung eines SNMP Clients fehlgeschlagen; Zugriff nicht möglich (z.B. SNMPv1/v2 Read-Only konfiguriert oder Read Community String falsch konfiguriert).
IP communication is possible. Remote logging activated.	IP-Kommunikation ist möglich. Remote Logging ist aktiviert.
IP communication is not possible. Remote logging deactivated. Please check IP configuration and network connectivity.	IP-Kommunikation ist nicht möglich. Remote Logging ist deaktiviert. Prüfen Sie, ob das Gerät nicht eine IP-Adresse hat.

Meldungen beim Systemanlauf (PLUG)

Meldung	Beschreibung
Startup configuration: Internal storage PLUG: Not present	Es ist kein PLUG gesteckt.
Startup configuration: Internal storage PLUG: Missing PLUG: License missing	Es ist kein PLUG gesteckt. Im Gerät sind Funktionen konfiguriert, für die eine PLUG-Lizenz (CLP) erforderlich ist.
Startup configuration: Internal storage PLUG: Configuration not accepted PLUG: License missing	Ungültige bzw. inkompatible Konfiguration auf dem gesteckten PLUG. Im Gerät sind Funktionen konfiguriert, für die eine PLUG-Lizenz (CLP) erforderlich ist.
Startup configuration: Internal storage PLUG: Configuration accepted PLUG: License wrong	Die PLUG-Lizenz (CLP) passt nicht.
Startup configuration: Internal storage PLUG: Configuration not accepted PLUG: License accepted	Ungültige bzw. inkompatible Konfiguration auf dem gesteckten PLUG.
Startup configuration: Internal storage PLUG: Factory clean → filled with internal configuration PLUG: Configuration accepted PLUG: License accepted	Die interne Konfiguration wurde erfolgreich auf einen leeren PLUG-Lizenz (CLP) geschrieben.
Startup configuration: Internal storage PLUG: Factory clean → filled with internal configuration PLUG: Configuration accepted	Die interne Konfiguration wurde erfolgreich auf einen leeren PLUG-Konfiguration (CLP) geschrieben.
Startup configuration: PLUG storage PLUG: Configuration accepted PLUG: License accepted	Die Konfiguration wurde erfolgreich von dem PLUG-Lizenz (CLP) geladen.
Startup configuration: PLUG storage PLUG: Configuration accepted	Die Konfiguration wurde erfolgreich von dem PLUG-Konfiguration (CLP) geladen.

Meldungen zum PLUG

Meldungen	Beschreibung
Factory default PLUG found.	Im Gerät befindet sich ein leerer bzw. formatierter PLUG.
PLUG: Filled PLUG was found. PLUG: Configuration Accepted	Der im Gerät befindliche PLUG wurde geleert. Die aktuelle Gerätekonfiguration wurde auf den PLUG geschrieben.
PLUG: Removed at runtime.	Der PLUG-Lizenz (CLP) oder der PLUG-Konfiguration (CLP) wurde im laufenden Betrieb gezogen.
PLUG accepted.	PLUG wurde akzeptiert.
PLUG: Different device type found.	Unterschiedlicher Gerätetyp

D.2 Meldungen im WLAN-Authentifizierung Log

Meldungen im Access Point-Modus

Meldung	Beschreibung
Client <MAC-Adresse> <System Name> associated successfully.	Der Client hat sich erfolgreich am Access Point angemeldet.
Client <MAC-Adresse> <System Name> disassociated with reason <reason description>	Der Client wurde vom Access Point abgemeldet.
VAP<Num>: Client <MAC> failed to associated; status (<text>)	Die Verbindung des Clients mit dem VAP ist fehlgeschlagen. Der Grund wird als Text ausgegeben.
VAP<Num>: Client <MAC> disassociated with reason (<text>)	Der Client wurde erfolgreich vom VAP getrennt. Der Grund wird als Text ausgegeben.
VAP<Num>: Client <MAC>deauthenticated with reason (<text>)	Der Client wurde vom AP abgemeldet. Der Grund wird als Text ausgegeben.
VAP<Nummer> Client <MAC> failed to authenticate; status (<status>)	Die Authentifizierung des Clients ist fehlgeschlagen. Der Grund wird als Text ausgegeben.
VAP<Num>: Client <MAC> failed to disassociated; status (<text>)	Die Verbindung des Clients konnte nicht getrennt werden. Der Grund wird als Text ausgegeben.
VAP<Num>: Client <MAC> associated successfully	Der Client hat sich erfolgreich mit dem VAP verbunden oder der Client hat sich erfolgreich an dem VAP angemeldet.
RADIUS: Access rejected for client <MAC>	Der RADIUS-Server verweigert dem Client den Zugriff.
RADIUS: Access accepted for client <MAC>	Der RADIUS-Server ermöglicht dem Client den Zugriff.
WDS Connection is established to AP <MAC>	Die WDS-Verbindug zum Access Point ist erfolgreich aufgebaut.
WDS disconnect from AP <MAC>	Die WDS-Verbindung zum Access Point ist abgebrochen.

Meldungen im Client-Modus

Meldung	Beschreibung
Associated successfully to AP <MAC-Adresse> <System Name> at channel <Kanalnummer> (frequency <Frequenz> MHz)	Der Client hat sich erfolgreich am Access Point angemeldet.
Disassociated from AP <MAC-Adresse> <'sys name'> with reason (Disassociated because sending STA is leaving (or has left) BSS)	Der Client wurde vom Access Point abgemeldet.
Failed to authenticate to AP <MAC>; status (<Text>)	Die Authentifizierung des Clients bei dem Access Point ist fehlgeschlagen. Der Grund wird als Text ausgegeben.
Failed to disassociate from AP <MAC>; status (<Text>)	Die Verbindung des Clients mit dem Access Point konnte nicht getrennt werden. Der Grund wird als Text ausgegeben.
Failed to associate to AP <MAC>; status (<Text>)	Die Verbindung des Clients mit dem Access Point ist fehlgeschlagen. Der Grund wird als Text ausgegeben.

Anhang E "Syslog-Meldungen"

E

E.1 Format der Syslog-Meldungen

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

HEADER

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

PRIORITY

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

- Facility
- Severity

VERSION

- Auf 1 gesetzt.

HOSTNAME_CONTENT:

- IPv4-Adresse nach RFC1035: Jedes Byte wird dezimal dargestellt und ist durch einen Punkt vom vorherigen getrennt: XXX.XXX.XXX.XXX
- IPv6-Adresse nach RFC4291 Section 2.2

STRUCTURED DATA

- timeQuality-Block

MESSAGE:

- ASCII-String in Englisch

Hinweis

Weitere Informationen über die Bedeutung der Felder finden Sie im RFC 5424 (https://datatracker.ietf.org/doc/html/rfc5424).

E.2 Parameter in Syslog-Meldungen

Die Syslog-Meldungen können folgende Parameter beinhalten:

Parameter	Beschreibung	Mögliche Werte oder Beispiel
ip address	IPv4- oder IPv6-Adresse	P-Adresse nach RFC1035 oder RFC4291 Abschnitt 2.2
src port dest port	Port, der als dezimale Nummer dargestellt wird. Format: %d	0 ... 65535
client mac dest mac src mac	MAC-Adresse Format: %02x:%02x:%02x;%02x:%02x:%02x	00:0C:29:2F:09:B3
protocol	Bezeichnung des Dienstes, der dieses Ereignis generiert hat, oder des verwendeten Layer-4-Protokolls. Format: %s	Mögliche Einträge von: UDP | TCP | WBM | Telnet | SSH | Console | TFTP | SFTP
group	Zeichenkette, die die Gruppe anhand ihres Namens identifiziert Format: %s	it-service
user name	Zeichenkette, die den authentifizierten Benutzer anhand seines Namens identifiziert ohne Leerzeichen Format: %s	maier
action user name	Identifiziert den Benutzer anhand seines Namens. Dies ist nicht der authentifizierte Benutzer Format: %s	Peter.Maier
role	Symbolischer Name für die Gruppenrolle Format: %s	Administrator
time minute timeout	Minutenanzahl Format: %d	44
time second	Sekundenanzahl Format: %d	44
failed login count	Anzahl der fehlgeschlagenen Loggins Format: %d	10
max sessions	Anzahl der Sitzungen Format: %d	10
vap	Symbolischer Name der virtuellen Access Point-Schnittstelle Format: (%s) oder (%s %s)	VAP1.1
status reason	Zusätzliche Statusinformation als lesbare Zeichenfolge. Sie kann mehrere Wörter enthalten. Damit die Zeichenfolge analysiert werden kann, muss sie mit „(" beginnen und mit „)" enden.	(Invalid group cipher) (Unknown peer)
wlan interface	Symbolischer Name der WLAN-Schnittstelle Format: %s	WLAN1

Parameter	Beschreibung	Mögliche Werte oder Beispiel
ssid	SSID in ASCII-Darstellung beliebig viele Leerzeichen Format: %s	MyWLAN
channel	Bezeichnung des Kanals Format: %s	12
signal strength	Signalstärke Format: %d	12
version	Bezeichnung der Version ohne Leerzeichen Format: %s	V1.0.3SP1
length	Länge des Netzwerkpakets (in Bytes) Format: %d	52
network interface	Symbolischer Name einer Netzwerkschnittstelle Format: %s	vlan 1

E.3 Syslog-Meldungen

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

Identifizierung und Authentifizierung von menschlichen Nutzern

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

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

Log-Text	{protocol}: User {user name} logged out from {ip address}.
Norm	IEC 62443-3-3 Reference: SR1.1

Beschreibung	Benutzersitzung beendet - Abmeldung erfolgt.
Beispiel	SSH: User admin logged out from 192.168.0.1.
Severity	Info
Facility	local0

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

Nutzerkontenverwaltung

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

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

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

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

Severity	Info
Facility	local0

Verwaltung der Kennungen

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

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

Erfolglose Anmeldeversuche

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

Nutzungskontrolle von Funkverbindungen (Verbindung über WLAN)

Log-Text	{vap}: Client {client mac} associated successfully.
Norm	IEC 62443-3-3 Reference: SR 2.2
Beschreibung	WLAN-Client mit AP verbunden.
Beispiel	VAP1.1: Client 18:65:90:ab:78:f4 associated successfully.
Severity	Info
Facility	local0

Log-Text	Overlap-AP found on {wlan interface}: AP {ssid} {ap mac} found on channel {channel} rssi {signal strength}.
Norm	IEC 62443-3-3 Reference: SR 2.2

Beschreibung	Radiofrequenz ist bereits verwendet.
Beispiel	Overlap-AP found on WLAN 1: AP scalance 20:a8:b9:80:44:80 found on channel 11 rssi 12.
Severity	Info
Facility	local0

Log-Text	{vap}: Client {client mac} disassociated with reason {reason}.
Norm	IEC 62443-3-3 Reference: SR 2.2
Beschreibung	WLAN-Client vom AP getrennt.
Beispiel	VAP1.1: Client 18:65:90:ab:78:f4 disassociated with reason (Disassociated because sending STA is leaving or has left BSS).
Severity	Info
Facility	local0

Log-Text	{vap}: Client {client mac} failed to associate, status {status}.
Norm	IEC 62443-3-3 Reference: SR 2.2
Beschreibung	WLAN-Clientverbindung zum AP abgelehnt.
Beispiel	VAP1.1: Client 18:65:90:ab:78:f4 failed to associate, status (Invalid group cipher).
Severity	Warning
Facility	local0

Log-Text	{vap}: Client {client mac} failed to authenticate, status {status}.
Norm	IEC 62443-3-3 Reference: SR 2.2
Beschreibung	Der WLAN-Client konnte sich nicht authentifizieren.
Beispiel	VAP1.1: Client 18:65:90:ab:78:f4 failed to authenticate, status (Invalid group cipher).
Severity	Warning
Facility	local0

Log-Text	RADIUS: {ip address} - No response from the RADIUS server.
Norm	IEC 62443-3-3 Reference: SR 2.2
Beschreibung	RADIDUS-Server nicht gefunden.
Beispiel	RADIUS: 192.168.0.10 - No response from the RADIUS server.
Severity	Warning
Facility	local0

Sitzungssperrung

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

Beispiel	The session of user admin was closed after 60 seconds of inactivity.
Severity	Warning
Facility	local0

Begrenzung der Anzahl gleichzeitiger Sitzungen

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

Nicht-Abstreitbarkeit (Konfiguration ändern)

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

Datensicherung im Automatisierungssystem (Backup)

Log-Text	{protocol}: User {user name} saved file type ConfigPack
Norm	IEC 62443-3-3 Reference: SR7.3
Beschreibung	Sicherung abgeschlossen
Beispiel	WBM: User admin saved file type ConfigPack..
Severity	Info
Facility	local0

Log-Text	{protocol}: Saved file type ConfigPack.
Norm	IEC 62443-3-3 Reference: SR7.3
Beschreibung	Sicherung abgeschlossen
Beispiel	TFTP: Saved file type ConfigPack
Severity	Info
Facility	local0

Log-Text	{protocol}: User {user name} failed to save file type ConfigPack.
Norm	IEC 62443-3-3 Reference: SR7.3
Beschreibung	Sicherung fehlgeschlagen

Beispiel	WBM: User admin failed to save file type ConfigPack.
Severity	Warning
Facility	local0

Log-Text	{protocol}: Failed to save file type ConfigPack.
Norm	IEC 62443-3-3 Reference: SR7.3
Beschreibung	Sicherung fehlgeschlagen
Beispiel	TFTP: Failed to save file type ConfigPack.
Severity	Warning
Facility	local0

Wiederherstellung des Automatisierungssystems

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

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

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

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

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

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

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

Anhang F "Unterstützte Sicherheitsmechanismen"

F

F.1 WLAN-Sicherheitsmechanismen

Die nachfolgende Tabelle zeigt die Verschlüsselungverfahren und die Authentifizierung, die die SCALANCE W-Geräte unterstützen.

Verschlüsselungsverfahren	
Keine	✓
WEP	✓
WPA-TKIP	-
WPA-AES	✓

Authentifizierung	
Passwort / PSK	✓
IEEE 802.1X EAP PEAP	✓
IEEE 802.1X EAP TLS	✓
IEEE 802.1X EAP TTLS	✓
IEEE 802.1X EAP andere	-
EAP-Portokoll: MS-CHAPv2	✓
EAP-Protokoll: TLS	✓
EAP-Protokoll: GTC	✓

F.2 Bei der RADIUS-Authentifizierung unterstützte Sicherheitsmechanismen

Die nachfolgende Tabelle zeigt Verschlüsselungssammlungen und Signaturalgorithmen, die SCALANCE W-Geräte bei der RADIUS-Authentifizierung unterstützen.

Default-Einstellung TLS 1.2

Tabelle F-1 WPA/WPA2 RADIUS-Authentifizierung

Verschlüsselungssammlung	**Signaturalgorithm**
TLS 1.0/1.1	
TLS_AES_256_GCM_SHA384	ECDSA with SHA256
TLS_CHACHA20_POLY1305_SHA256	ECDSA with SHA384
TLS_AES_128_GCM_SHA256	ECDSA with SHA512
AES256-GCM-SHA384	ECDSA with SHA224
AES128-GCM-SHA256	ECDSA with SHA1
AES256-SHA256	SHA224 with RSA
AES128-SHA256	SHA1 with RSA

Verschlüsselungssammlung	**Signaturalgorithm**
ECDHE-ECDSA-AES256-SHA	DSA with SHA224
ECDHE-RSA-AES256-SHA	DSA with SHA1
DHE-RSA-AES256-SHA	ECDSA with SHA256
ECDHE-ECDSA-AES128-SHA	ECDSA with SHA384
ECDHE-RSA-AES128-SHA	ECDSA with SHA512
DHE-RSA-AES128-SHA	EdDSA ed25519
AES256-SHA	EdDSA ed448
AES128-SHA	RSASSA-PSS with SHA256
ECDHE-ECDSA-AES256-GCM-SHA384	RSASSA-PSS (rsaEncryption) with SHA384
ECDHE-RSA-AES256-GCM-SHA384	RSASSA-PSS (rsaEncryption) with SHA512
DHE-RSA-AES256-GCM-SHA384	SHA256 with RSA
ECDHE-ECDSA-CHACHA20-POLY1305	SHA384 with RSA
ECDHE-RSA-CHACHA20-POLY1305	SHA512 with RSA
DHE-RSA-CHACHA20-POLY1305	DSA with SHA256
ECDHE-ECDSA-AES128-GCM-SHA256	DSA with SHA384
ECDHE-RSA-AES128-GCM-SHA256	DSA with SHA512
DHE-RSA-AES128-GCM-SHA256	
ECDHE-ECDSA-AES256-SHA384	
ECDHE-RSA-AES256-SHA384	
DHE-RSA-AES256-SHA256	
ECDHE-ECDSA-AES128-SHA256	
ECDHE-RSA-AES128-SHA256	
DHE-RSA-AES128-SHA256	
TLS 1.2	
ECDHE-ECDSA-AES256-GCM-SHA384	EdDSA ed25519
ECDHE-RSA-AES256-GCM-SHA384	EdDSA ed448
DHE-RSA-AES256-GCM-SHA384	RSASSA-PSS with SHA256
ECDHE-ECDSA-CHACHA20-POLY1305	RSASSA-PSS with SHA384
ECDHE-RSA-CHACHA20-POLY1305	RSASSA-PSS with SHA512
DHE-RSA-CHACHA20-POLY1305	RSASSA-PSS (rsaEncryption) with SHA256
ECDHE-ECDSA-AES128-GCM-SHA256	RSASSA-PSS (rsaEncryption) with SHA384
ECDHE-RSA-AES128-GCM-SHA256	RSASSA-PSS (rsaEncryption) with SHA512
DHE-RSA-AES128-GCM-SHA256	SHA256 with RSA
ECDHE-ECDSA-AES256-SHA384	SHA384 with RSA
ECDHE-RSA-AES256-SHA384	SHA512 with RSA
DHE-RSA-AES256-SHA256	DSA with SHA256
ECDHE-ECDSA-AES128-SHA256	DSA with SHA384
ECDHE-RSA-AES128-SHA256	DSA with SHA512
DHE-RSA-AES128-SHA256	

Index

S

T

U

V

W

Z