Industrial-Managed-Switch

8 Ports 1000BASE-T; MAC Security

852-1322

Produkthandbuch | Version 1.3.0

WAGO Kontakttechnik GmbH & Co. KG
Hansastraße 27
D-32423 Minden
Tel: +49 (0) 571/887 – 0
Fax: +49 (0) 571/887 – 844 169
E-Mail: ✉ **info@wago.com**
Web: **www.wago.com**

Technischer Support
Tel: +49 (0) 571/887 – 44555
Fax: +49 (0) 571/887 – 844555
E-Mail: ✉ **support@wago.com**

Es wurden alle erdenklichen Maßnahmen getroffen, um die Richtigkeit und Vollständigkeit der vorliegenden Dokumentation zu gewährleisten. Da sich Fehler, trotz aller Sorgfalt, nie vollständig vermeiden lassen, sind wir für Hinweise und Anregungen jederzeit dankbar.

E-Mail: ✉ **documentation@wago.com**

Inhaltsverzeichnis

Bestimmungen 6
1.1 Bestimmungsgemäße Verwendung 6
1.2 Darstellungskonventionen 7
1.3 Rechtliche Informationen 8

Sicherheit 10
2.1 Allgemeine Sicherheitsbestimmungen 10
2.2 Elektrische Sicherheit 10
2.3 Mechanische Sicherheit 11
2.4 Indirekte Sicherheit 12

Überblick 13

Eigenschaften 14
4.1 Ansichten 14
4.1.1 Frontansicht 14
4.1.2 Draufsicht 15
4.2 Etikett 16
4.3 Anschlüsse 16
4.3.1 Erdungsschraube 16
4.3.2 Spannungsversorgung 16
4.3.3 Netzwerkanschlüsse 17
4.3.3.1 10/100/1000BASE-T(X)-Anschlüsse 18
4.3.3.2 10/100/1000BASE-T(X) (MACsec)-Anschlüsse 18
4.4 Anzeigeelemente 18
4.4.1 Produkt-LEDs 18
4.4.2 Anschluss-LEDs 19
4.5 Technische Daten 19
4.5.1 Produkt 19
4.5.2 Systemdaten 19
4.5.3 Spannungsversorgung 19
4.5.4 Kommunikation 19
4.5.5 Umgebungsanforderungen 20
4.6 Richtlinien, Zulassungen und Normen 20
4.6.1 Zulassungen 20
4.6.2 Richtlinien und Normen 21

Funktionen 22
5.1 Security 22
5.1.1 IEEE 802.1X 22
5.1.2 RADIUS 22
5.1.3 MAC Security (MACSec) 23

Planung 24
6.1 Aufbaurichtlinien 24

6.1.1 Montageort ... 24

Transport und Lagerung ... 25

Montieren und Demontieren ... 26

8.1 Montieren ... 26
8.1.1 Montage auf Tragschiene ... 26
8.2 Demontieren ... 26
8.2.1 Demontage von der Tragschiene ... 26

Anschließen ... 27

9.1 Erden ... 27
9.2 Versorgungsspannung anschließen ... 27
9.3 10/100/1000BASE-T-Ports anschließen ... 28

Konfigurieren im WBM ... 29

10.1 Anmeldung ... 29
10.2 Anmeldefehler ... 32
10.3 Informationen ... 34
10.3.1 System Information (System Information) ... 34
10.3.2 Legal Information (Rechtliche Information) ... 35
10.4 Configuration (Konfiguration) ... 36
10.4.1 System Settings (Systemeinstellungen) ... 36
10.4.2 Device Discovery - LLDP (Geräteerkennung – LLDP) ... 37
10.4.3 System Management - SNTP (Systemmanagement – SNTP) ... 38
10.4.3.1 Allgemeine Informationen ... 38
10.4.3.2 SNTP-Einrichtung ... 39
10.4.4 Network Settings (Netzwerkeinstellungen) ... 42
10.4.5 Port Settings (Port-Einstellungen) ... 43
10.4.5.1 Setting (Einstellung) ... 43
10.4.6 Interface - Mirror (Interface - Port-Mirroring) ... 44
10.4.6.1 Allgemeine Informationen ... 44
10.4.6.2 Port-Mirroring – Einrichtung ... 45
10.4.7 Password (Passwort) ... 46
10.5 Diagnostics (Diagnose) ... 47
10.5.1 SNMP ... 47
10.5.1.1 SNMP Agent (SNMP-Agent) ... 50
10.5.1.2 SNMPv1/v2c-Community (SNMPv1/v2c-Community-String) ... 51
10.5.1.3 SNMP Trap (SNMP-Trap) ... 52
10.5.1.4 SNMP-V3-Auth. (SNMP-V3-Authentifizierung) ... 54
10.5.2 Modbus TCP ... 55
10.5.3 System-Log (System-Log) ... 57
10.5.3.1 Setting (Einstellung) ... 57
10.5.3.2 Log ... 58
10.5.4 Port Monitor (Port-Überwachung) ... 60
10.6 Security (Sicherheit) ... 61
10.6.1 Static SAK (Einstellungen für statischen SAK) ... 61
10.6.2 Secure Code (Sicherheitscode) ... 63
10.6.3 802.1X (IEEE 802.1X) ... 63
10.6.3.1 Setting (IEEE 802.1X-Einstellungen) ... 64

10.6.3.2 Parameters Setting (IEEE 802.1X-Parametereinstellungen) ... 65
10.6.3.3 Port Setting (IEEE 802.1X-Port-Einstellungen) ... 66
10.6.4 Port Security (Port Sicherheit) ... 68
10.6.5 VLAN ... 70
10.6.5.1 Port-Isolation ... 70
10.6.5.2 VLAN-Einrichtung ... 71
10.6.5.3 Management-VLAN ... 73
10.7 Redundancy (Redundanz) ... 74
10.7.1 RSTP ... 74
10.7.1.1 Allgemeine Informationen ... 74
10.7.1.2 RSTP-Einrichtung ... 77
10.7.1.3 RSTP-Port-Einrichtung ... 78
10.7.1.4 RSTP-Failover und Recovery-Zeiten ... 79
10.8 Maintenance (Wartung) ... 79
10.8.1 Firmware Upgrade (Firmware-Upgrade) ... 79
10.8.2 Reset to Default (Rücksetzen auf Default-Werte) ... 80
10.8.3 Backup/Restore (Sichern/Wiederherstellen) ... 81
10.8.4 Reboot (Neustart) ... 82
10.8.5 Logout (Abmelden) ... 82

In Betrieb nehmen ... 83

Diagnose ... 84

Service ... 85

Außer Betrieb nehmen ... 86

14.1 Entsorgung und Recycling ... 86

Anhang ... 87

15.1 MODBUS/TCP-Tabellen ... 87
15.1.1 Modbus-Register ... 87

Bestimmungen

Die vorliegende Dokumentation gilt für das Produkt:

852-1322

1.1 Bestimmungsgemäße Verwendung

Das Produkt ist für die Schutzart IP30 ausgelegt. Es ist geschützt gegen das Eindringen von Festkörpern und festen Verunreinigungen bis zu einem Durchmesser von 2,5 mm, aber nicht gegen das Eindringen von Wasser. Sofern nicht anders angegeben, ist der Betrieb des Produktes in nasser und staubiger Umgebung nicht gestattet.

Gewährleistung und Haftung

Es gelten die Bestimmungen der allgemeinen Geschäfts- und Vertragsbedingungen für Lieferungen und Leistungen der WAGO Kontakttechnik GmbH & Co. KG sowie für Softwareprodukte und Produkte mit integrierter Software der WAGO Softwarelizenzvertrag, beide abrufbar unter: **www.wago.com**. Danach ist die Gewährleistung insbesondere in folgenden Fällen ausgeschlossen:

- Das Produkt wird sachwidrig verwendet.
- Der Mangel beruht auf speziellen Vorgaben (Hard- und Softwarekonfigurationen).
- Es wurden Modifikationen der Hard- oder Software durch den Nutzer oder Dritte durchgeführt, die nicht in dieser Dokumentation beschrieben sind und für das Auftreten des Mangels zumindest mitursächlich sind.

Einzelvertragliche Abreden haben stets Vorrang.

Pflichten von Errichter/Betreiber

Die Verantwortung für die Sicherheit einer mit dem Produkt errichteten Anlage bzw. eines Systems liegt beim Errichter/Betreiber. Der Errichter/Betreiber ist für den sachgemäßen Einbau und die Sicherheit in den Anlagen verantwortlich. Dieser muss die geltenden Gesetze, Normen, Bestimmungen, örtlichen Vorschriften, den Stand und die Regeln der Technik zum Zeitpunkt der Installation einhalten und die in der Gebrauchsanleitung beschriebenen Vorgaben beachten. Ferner müssen die Errichtungsbestimmungen der Zulassungen eingehalten werden. Bei Nichteinhaltung darf das Produkt nicht im Geltungsbereich der Zulassung betrieben werden.

Sachwidrige Verwendung

Eine sachwidrige Verwendung des Produktes ist nicht gestattet. Die sachwidrige Verwendung ist insbesondere in den folgenden Fällen gegeben:

- Nichtbeachten der bestimmungsgemäßen Verwendung.
- Einsatz ohne Schutzmaßnahmen in einer Umgebung, in der Feuchtigkeit, Salzwasser, Salzsprühnebel, Staub, ätzende Dämpfe, Gase, direkte Sonneneinstrahlung oder ionisierende Strahlung auftreten können.
- Verwendung des Produktes in Bereichen mit besonderem Risiko, die einen fehlerfreien Dauerbetrieb erfordern und in denen ein Ausfall oder Betrieb des Produktes zu einer unmittelbaren Gefahr für Leben, Körper oder Gesundheit oder zu erheblichen Sach- oder Umweltschäden führen kann (wie der Betrieb von Kernkraftwerken, Waffensystemen, Luft- und Kraftfahrzeugen).

1.2 Darstellungskonventionen

Zahlensysteme

100	Dezimal: Normale Schreibweise
0x64	Hexadezimal: C-Notation
'100'	Binär: In Hochkomma
'0110.0100'	Nibbles durch Punkt getrennt

Textauszeichnungen

kursiv	Namen von Pfaden oder Dateien
fett	Bezeichnungen von Menüpunkten, Eingabe- oder Auswahlfelder, Hervorhebungen
`Code`	Ausschnitte von Programmcode
>	Auswahl eines Menüpunktes aus einem Menü
„Wert“	Werteingaben
[F5]	Beschriftungen von Schaltflächen oder Tasten

Querverweise/Links

	Querverweis/Link zu einem Thema im Dokument
	Querverweis/Link zu einer Dokumentation
	Querverweis/Link zu einer Website
	Querverweis/Link zu einer E-Mail-Adresse

Handlungsanweisung

✓ Dieses Symbol kennzeichnet eine Voraussetzung.

1. Handlungsschritt
2. Handlungsschritt
   ⇨ Dieses Symbol kennzeichnet ein Zwischenergebnis.

⇨ Dieses Symbol kennzeichnet ein Handlungsresultat.

Aufzählung

- Aufzählung erste Ebene
  – Aufzählung zweite Ebene

Abbildungen

Abbildungen in dieser Dokumentation dienen dem besseren Verständnis und können von der tatsächlichen Ausführung der Produkte abweichen.

Hinweise

⚠ GEFAHR

Art und Quelle der Gefahr

Mögliche Folge der Gefahr, die auch Tod oder irreversible Verletzung umfasst

- Handlungsschritt zur Risikoreduktion

⚠ WARNUNG

Art und Quelle der Gefahr

Mögliche Folge der Gefahr, die auch schwere Verletzung umfasst

- Handlungsschritt zur Risikoreduktion

⚠ VORSICHT

Art und Quelle der Gefahr

Mögliche Folge der Gefahr, die zumindest leichte Verletzung umfasst

- Handlungsschritt zur Risikoreduktion

ACHTUNG

Art und Quelle der Störung (nur Sachschäden)

Mögliche Störungen, die den Funktionsumfang bzw. die Ergonomie des Produktes einschränken, aber nicht vorhersehbar zu Gefährdung von Personen führen

- Handlungsschritt zur Risikoreduktion

Hinweis

Hinweis und Information

Kennzeichnet Informationen, Erklärungen, Empfehlungen, Verweise etc.

1.3 Rechtliche Informationen

Geistiges Eigentum

Vorbehaltlich anderslautender gesetzlicher Bestimmungen ist die Weitergabe oder Vervielfältigung dieses Dokumentes sowie die Verwertung und Mitteilung seines Inhalts ausdrücklich untersagt, es sei denn, es wurden abweichende Vereinbarungen getroffen. Fremdprodukte werden stets ohne Vermerk etwaiger Patentrechte genannt. Alle Rechte für den Fall der Patent-, Gebrauchsmuster- oder Designeintragung sind der WAGO Kontakttechnik GmbH & Co. KG, bei Fremdprodukten dem jeweiligen Hersteller, vorbehalten.

In der Dokumentation der Produkte werden Marken Dritter verwendet. Im Weiteren wird auf das Mitführen der Zeichen „®“ und „™“ verzichtet. Die Marken sind im Anhang aufgeführt (Schutzrechte).

Änderungsvorbehalt

Die in diesem Handbuch aufgeführten Vorschriften, Richtlinien, Normen usw. entsprechen dem Stand während der Ausarbeitung und unterliegen keinem Änderungsdienst. Sie sind vom Errichter/Betreiber in Eigenverantwortung in ihrer jeweils gültigen Fassung anzuwenden. Die WAGO Kontakttechnik GmbH & Co. KG behält sich das Recht vor, jederzeit technische Änderungen und Verbesserungen der Produkte und der Daten, Anga-

ben und Abbildungen dieses Handbuchs vorzunehmen. Ein Anspruch auf Änderung oder Nachbesserung von bereits ausgelieferten Produkten ist – mit Ausnahme von Nachbesserungen im Rahmen der Gewährleistung – ausgeschlossen.

Lizenzen

Die Produkte können Open-Source-Software enthalten. Die notwendigen Informationen zu den Lizenzen sind in den Produkten gespeichert. Diese Informationen finden Sie auch unter: **www.wago.com**.

Sicherheit

Dieses Kapitel enthält Sicherheitsbestimmungen, die für die gefahrlose Nutzung des Produktes einzuhalten sind.

Dieses Kapitel richtet sich an die folgenden Zielgruppen:

- Planer und Errichter
- Betreiber
- Fachpersonal für Montage
- Fachpersonal für Installation (elektrisch, netzwerktechnisch usw.)
- Fachpersonal für Bedienung
- Fachpersonal für Service und Wartung

Befolgen Sie die folgenden Sicherheitsbestimmungen:

2.1 Allgemeine Sicherheitsbestimmungen

- Diese Dokumentation ist Teil des Produktes. Bewahren Sie deshalb die Dokumentation während der gesamten Nutzungsdauer des Produktes auf. Geben Sie die Dokumentation an den nachfolgenden Benutzer des Produktes weiter. Stellen Sie darüber hinaus sicher, dass gegebenenfalls jede erhaltene Ergänzung in die Dokumentation mit aufgenommen wird.
- Sämtliche Arbeitsschritte, die im Zusammenhang mit der Verwendung von WAGO Software stehen, dürfen nur von Fachkräften durchgeführt werden, die über ausreichende Kenntnisse im Umgang mit dem jeweils eingesetzten PC-System verfügen.
  Arbeitsschritte, in deren Folge Dateien auf dem PC-System erzeugt oder verändert werden, dürfen nur von Fachkräften durchgeführt werden, die zusätzlich zu den oben genannten auch über ausreichende Kenntnisse in der Administration des eingesetzten PC-Systems verfügen.
  Arbeitsschritte, in deren Folge das Verhalten des PC-Systems in einem Netzwerk verändert wird, dürfen nur von Fachkräften durchgeführt werden, die zusätzlich zu den oben genannten auch über ausreichende Kenntnisse in der Administration des jeweils eingesetzten Netzwerks verfügen.
- Alle Eingriffe in die Konfiguration der Switches im Netzwerk sind stets von Fachkräften mit ausreichenden Kenntnissen durchzuführen.
- Halten Sie die geltenden Gesetze, Normen, Bestimmungen, örtlichen Vorschriften, den Stand der Technik und die Regeln der Technik zum Zeitpunkt der Installation ein.
- Ist ein Fernzugriff auf Steuerungskomponenten und Steuerungsnetzwerke erforderlich, sollte ein „Virtual Private Network“ (VPN) genutzt werden.

2.2 Elektrische Sicherheit

- Gefährliche elektrische Spannung kann zu elektrischem Schlag und Verbrennungen führen! Trennen Sie immer alle verwendeten Spannungsversorgungen vom Produkt, bevor Sie das Produkt montieren, installieren, Störungen beheben oder Wartungsarbeiten vornehmen.

Versorgung

- Das Aufschalten von unzulässigen Spannungs- oder Frequenzwerten kann zur Zerstörung des Produktes führen.

- Schalten Sie die Versorgungsspannung sofort ab, wenn eine Funktionsstörung oder Beschädigung am Produkt vorliegt.

Erden/Schutz/Sicherung

- Sichern Sie das Produkt mit einer geeigneten Sicherung ab.
- Wenden Sie die Überspannungs- und Blitzschutzkonzepte an, die für das Gebäude vorgesehen sind.
- Achten Sie beim Umgang mit dem Produkt auf den Potentialausgleich der Umgebung (Personen, Arbeitsplatz und Verpackung). Berühren Sie keine elektrisch leitenden Bauteile.

Leitungen

- Verlegen Sie Steuer-/Signal-/Datenleitungen räumlich getrennt von Versorgungsleitungen.
- Beachten Sie den zulässigen Temperaturbereich der Anschlussleitungen.
- Verwenden Sie eine geeignete Zugentlastung.
- Achten Sie auf die korrekte Anschlussbelegung.
- Vermeiden Sie die Verpolung der Daten- und Versorgungsleitungen, da dies zu Schäden an den Produkten führen kann.

Schirmung/Netzwerk

- Beachten Sie die entsprechenden Normen für EMV-gerechte Installationen.

Funk etc.

- Dies ist ein Produkt der Klasse A. Das Produkt kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen.
- Für industriellen Einsatz: Die ETHERNET-Switches der Baureihe 852 von WAGO sind für den Einsatz in Wohn- und Industriegebieten zugelassen. Für den Einsatz in Industriegebieten gelten sie als offene Betriebsmittel. Daher dürfen sie in Industriegebieten nur in abschließbaren Gehäusen, Schränken oder in elektrischen Betriebsräumen installiert werden. Ermöglichen Sie nur autorisiertem Fachpersonal den Zugang mittels Schlüssel oder Werkzeug.
- Verwenden Sie Geräte mit ETHERNET-/RJ-45-Anschluss ausschließlich in LANs. Verbinden Sie diese Geräte niemals mit Telekommunikationsnetzen.

Komponenten

- Tauschen Sie defekte oder beschädigte Geräte/Bausteine aus (z. B. bei deformierten Kontakten).

2.3 Mechanische Sicherheit

- Die Sicherstellung eines notwendigen Berührungsschutzes liegt in Ihrer Verantwortung als Anlagenerrichter. Halten Sie die für den jeweiligen Anwendungsfall zu beachtenden Errichtungsbestimmungen ein.
- Die in den technischen Daten angegebene Umgebungstemperatur für den Betrieb gilt für die Nenneinbaulage. Abweichende Einbaulagen können die zulässige Umgebungstemperatur für den Betrieb beeinflussen.

- Die Kühlung des Produktes darf nicht beeinträchtigt werden. Stellen Sie eine ungehinderte Luftzufuhr und die Mindestabstände zu benachbarten Produkten/Bereichen sicher.
- Montieren Sie das Produkt nicht auf oder an leicht entzündlichen Materialien.
- Beachten Sie bei der Auswahl des Montageortes, dass der Schaltschrank für Wartungszwecke zugänglich bleiben muss.
- Prüfen Sie das Produkt vor Inbetriebnahme auf eventuelle Transportschäden. Bei Beschädigungen darf das Produkt nicht in Betrieb genommen werden.
- Benutzen Sie das Produkt nur in einer geschützten Umgebung.
- Öffnen Sie nicht das Produktgehäuse.
- Vermeiden Sie leitfähige Verschmutzungen.

2.4 Indirekte Sicherheit

- Verwenden Sie zur Reinigung keine harten Gegenstände, die zu Kratzern führen könnten.
- Verwenden Sie zur Reinigung kein Kontaktspray.
- Verwenden Sie generell zur Handhabung des Produktes saubere Werkzeuge und Materialien.
- Die Produkte sind unbeständig gegen Stoffe, die kriechende und isolierende Eigenschaften besitzen, z. B. Aerosole, Silikone, Triglyceride (Bestandteil einiger Handcremes). Wenn diese Stoffe im Umfeld der Produkte auftreten, bauen Sie die Produkte in ein zusätzliches Gehäuse ein, das auch resistent gegen oben genannte Stoffe ist.
- Lesen Sie vor Einbau, Betrieb oder Bedienung des Produktes vollständig und sorgfältig die vorliegende Produktdokumentation. Beachten Sie zusätzlich die Angaben auf dem Produktgehäuse sowie die weiterführenden Informationen, z. B. unter **www.wago.com**/<Artikelnummer>.
- Ändern Sie das Passwort. Die werksseitige Voreinstellung ist allgemein bekannt und bietet keinen ausreichenden Schutz.
- Stellen Sie alle Produkte in einem Netzwerk auf unterschiedliche IP-Adressen ein.
- Verwenden Sie nur aktuelle Firmware.
- Führen Sie regelmäßig eine Bedrohungsanalyse durch. So können Sie prüfen, ob die getroffenen Maßnahmen Ihrem Schutzbedürfnis entsprechen.
- Wenden Sie in der sicherheitsgerichteten Gestaltung Ihrer Anlage „Defense-in-depth“-Mechanismen an, um den Zugriff und die Kontrolle auf individuelle Produkte und Netzwerke einzuschränken.

Überblick

Der Industrial-Managed-Switch 852-1322 von WAGO ist ein Switch mit 8 Gigabit-Ports 10/100/1000 BASE-T(X) RJ-45, von denen zwei Ports MAC Security-Verschlüsselung unterstützen.

Der Industrial-Managed-Switch lässt sich einfach konfigurieren und installieren und ist deshalb in zahlreichen Anwendungen, wie etwa Anwendungen in Wohnbereichen, einsetzbar. Dank des integrierten „MACsec Key Agreement“ eignet er sich ideal für den Schutz lokaler Plug-and-Play-Netzwerke.

MACsec nutzt GCM-AES, um eine Punkt-zu-Punkt-Verschlüsselung bei ETHERNET-Links zwischen Switchen zu realisieren. Anders gesagt wird das Netzwerk vor einer ganzen Reihe von Sicherheitsbedrohungen geschützt, wie etwa Eindringversuche, Man-in-the-middle-Angriffe, Masquerading, passives Abhören und Playback-Angriffe. Und weil die MACsec-Verschlüsselung hardwarebasiert erfolgt, gibt es keine nennenswerte Latenz.

WAGOs 852-1322 bietet Ihnen eine zusätzliche Sicherheitsstufe für Wohn- und Industrieanwendungen, in denen es auf kompakte Lösungen mit hoher garantierter Netzwerkleistung von bis zu 97 % Datendurchsatz ohne nennenswerte zusätzliche Latenz geht.

Außerdem unterstützt er einen großen Betriebstemperaturbereich von -20 °C bis 70 °C und entspricht den Normen EN/IEC(CB)/UL62368-1 sowie IEC 60068-2-6, IEC 60068-2-27 und IEC 60068-2-32. Die Switches 852-1322 von WAGO sind leistungsstarke und kompakte Produkte, die verschiedensten Umgebungsbedingungen widerstehen können, wie etwa Eingangsüberspannungen oder Einwirkung von Stößen, Fallstößen und Vibrationen.

Eigenschaften

4.1 Ansichten

4.1.1 Frontansicht

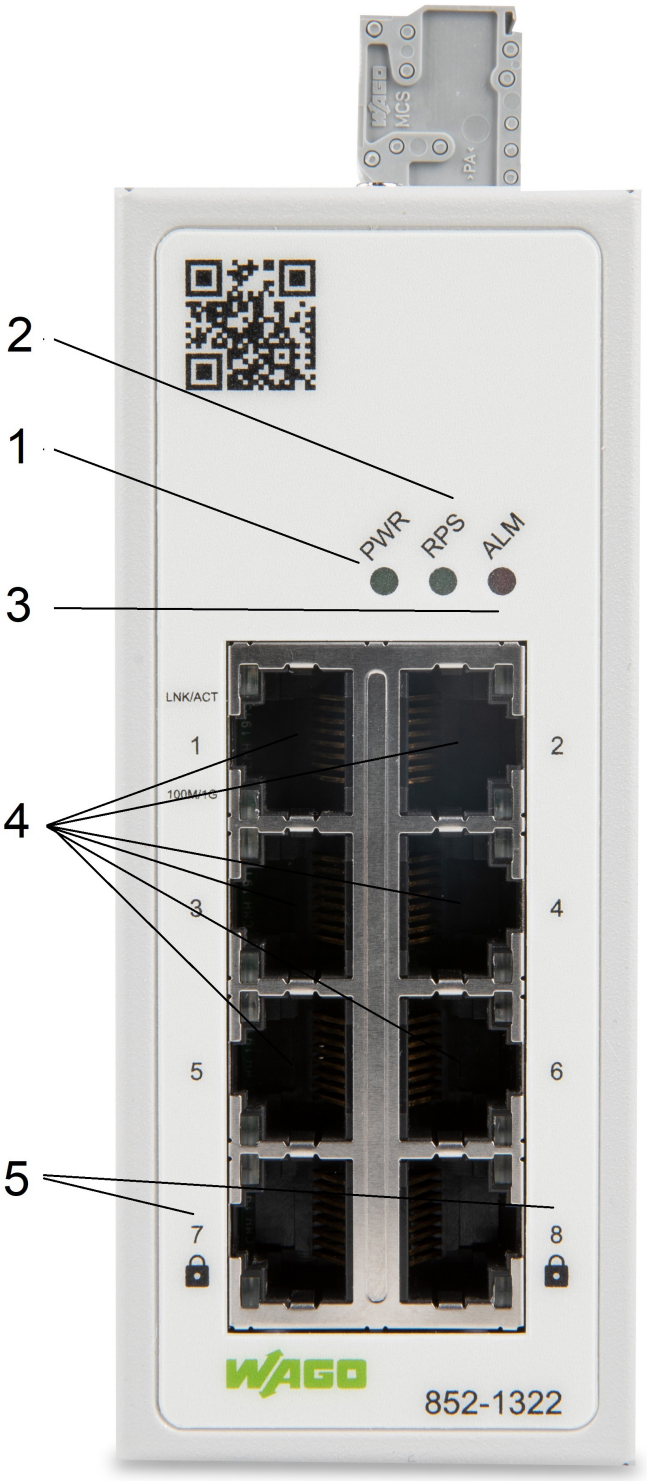

Abbildung 1: Frontansicht des Industrial-Managed-Switches

Tabelle 1: Legende zur Abbildung "Frontansicht des Industrial-Managed-Switches"

Pos.	Bezeichnung	Bedeutung	
1	PWR	Status-LED Versorgungsspannung	Anzeigeelemente [▶ 18]
2	RPS	Status-LED Redundante Versorgungs-spannung	Anzeigeelemente [▶ 18]
3	ALM	Status-LED Alarm	Anzeigeelemente [▶ 18]
4		Anschluss RJ-45 (10/100/1000BASE-T(X)) (6)	Anschluss-LEDs [▶ 19]
5		Anschluss RJ-45 (10/100/1000BASE-T(X) (MACsec) (2)	Anschluss-LEDs [▶ 19]

4.1.2 Draufsicht

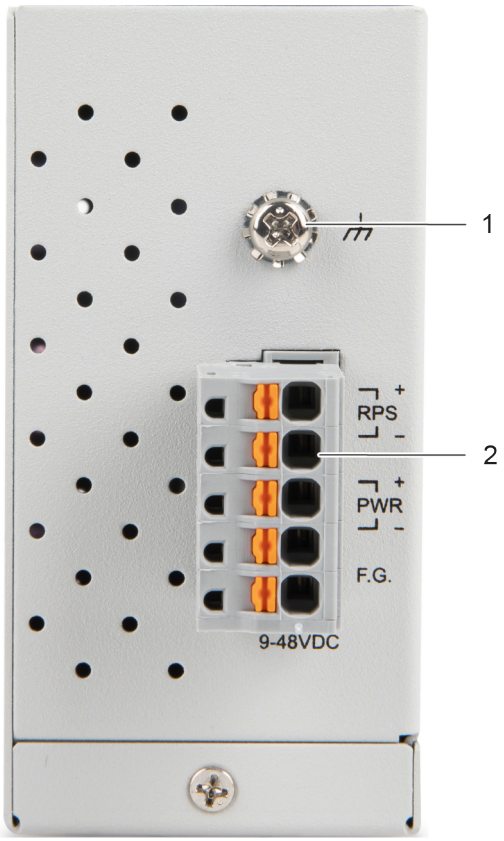

Abbildung 2: Draufsicht des Industrial-Managed-Switches

Tabelle 2: Legende zur Abbildung "Draufsicht des Industrial-Managed-Switches"

Pos.	Bezeichnung	Bedeutung	
1	-	Erdungsschraube	Erdungsschraube [▶ 16]
2	-	Stecker (Stiftleiste) für Leistungsauf-nahme (RPS/PWR/F.G.) (Artikelnummer 2231-105/026-000)	Spannungsversorgung [▶ 16]

4.2 Etikett

Abbildung 3: Etikett

Tabelle 3: Legende zur Abbildung „Etikett“

Bezeichnung	Beschreibung
Item-No	Artikelnummer
IN	Spannungsbereich und maximale Stromstärke am Eingang des Produktes
Ambient Temp	Betriebstemperatur
MAC	MAC-Adresse des Produktes
Default-IP	Default-IP-Adresse des Produktes
Serial NO	Seriennummer des Produktes
QR code	QR-Code mit weiteren Produktinformationen
Serial No.	Seriennummer des Produktes
	Firmwareversion (linke Ziffernfolge) (02)
	Hardwareversion (rechte Ziffernfolge) (02)

4.3 Anschlüsse

4.3.1 Erdungsschraube

Der Switch muss geerdet werden. Verbinden Sie dazu die Erdungsschraube mit dem Erdpotential. Betreiben Sie den Switch nicht ohne einen entsprechend installierten Schutzleiter.

Abbildung 4: Erdungsschraube

4.3.2 Spannungsversorgung

Die Federleiste (Artikelnr. 2231-105/026-000) kann problemlos mit der 5-poligen Stiftleiste (Artikelnr. 231-435/001-000) auf der Oberseite des Switches verbunden werden.

Sowohl PWR als auch RPS unterstützen Eingangsspannungen zwischen DC 9 und 48 V.

Die Stiftleiste hat folgende Belegung:

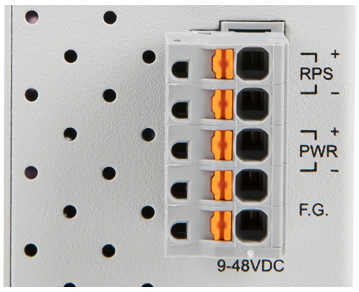

Abbildung 5: Spannungsversorgungsanschluss

Tabelle 4: Legende zur Abbildung "Spannungsversorgungsanschluss"

Anschluss	Bezeichnung	Beschreibung
+	RPS	Sekundärer Gleichstromeingang
-	RPS	Sekundärer Gleichstromeingang
+	PWR	Primärer Gleichstromeingang
-	PWR	Primärer Gleichstromeingang
	F.G.	Funktionserde

ACHTUNG

Sachschäden durch elektrostatische Entladung (ESD)

Switch für Gleichstrombetrieb: Die Stromversorgung erfolgt über eine externe Gleichstromquelle. Da der Switch keinen Netzschalter hat, schaltet er sich sofort ein, nachdem Sie das Produkt mit einer Spannung versorgen.

4.3.3 Netzwerkanschlüsse

Der Industrial-Managed-Switch verwendet Anschlüsse für Kupferkabel und unterstützt ETHERNET, Fast ETHERNET und Gigabit ETHERNET.

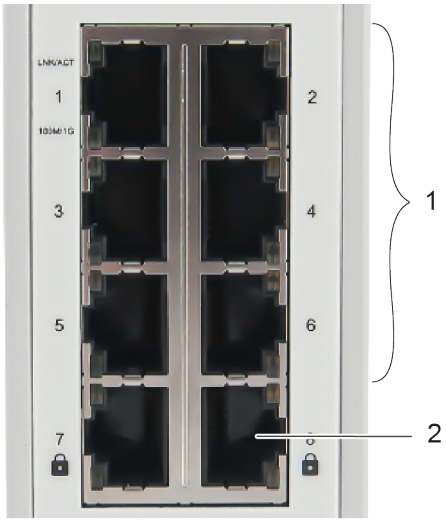

Abbildung 6: Netzwerkanschlüsse

Tabelle 5: Legende zur Abbildung "Netzwerkanschlüsse"

Pos.	Beschreibung	Details siehe Kapitel:
1	Anschluss RJ-45 (10/100/1000BASE-T(X)) (6)	10/100/1000BASE-T(X)-Anschlüsse [▶ 18]

Pos.	Beschreibung	Details siehe Kapitel:
2	Anschluss RJ-45 (10/100/1000BASE-T(X) (MACsec) (2)	10/100/1000BASE-T(X) (MACsec)-Anschlüsse [▶ 18]

4.3.3.1 10/100/1000BASE-T(X)-Anschlüsse

Die 10/100/1000BASE-T(X)-Anschlüsse unterstützen die Netzwerkgeschwindigkeiten 10 Mbit/s, 100 Mbit/s und 1000 Mbit/s und können im Halb- und im Vollduplex-Übertragungsmodus betrieben werden. Außerdem bieten die Ports eine automatische Crossover-Erkennung (Auto-MDI/MDI-X) und sind damit Plug-and-play-fähig. Stecken Sie einfach die Netzwerkkabel in die Ports – diese passen sich dann an die Endknotengeräte an.

Folgendes Kabel wird für die RJ-45-Anschlüsse empfohlen:
- Kat 5e oder besser mit einer Kabellänge von max. 100 m.

4.3.3.2 10/100/1000BASE-T(X) (MACsec)-Anschlüsse

Die 10/100/1000BASE-T(X) (MACsec)-Anschlüsse bieten neben den Netzwerkgeschwindigkeiten 10 Mbit/s, 100 Mbit/s und 1000 Mbit/s eine Verschlüsselung des Datenverkehrs durch den Sicherheitsstandard IEEE 802.1AE MAC Security..

4.4 Anzeigeelemente

Der Industrial-Managed-Switch ist mit Produkt-LEDs sowie mit Anschluss-LEDs ausgestattet. Anhand der Produkt-LEDs können Sie den Status des Switches schnell erkennen, die Anschluss-LEDs geben Auskunft über die Verbindungsaktionen.

4.4.1 Produkt-LEDs

Abbildung 7: Produkt-LEDs

Tabelle 6: Legende zur Abbildung „Produkt-LEDs“

LED	Name	Status	Beschreibung
PWR	Primary-Power-LED	Grün	Verwendung des primären Netzteils
		Aus	Primäres Netzteil ausgeschaltet oder Fehler
RPS	Redundant-Power-System-LED	Grün	Verwendung des sekundären Netzteils
		Aus	Sekundäres Netzteil ausgeschaltet oder Fehler
ALM	Alarm-LED	Rot	Es liegt keine Spannungsversorgung an der primären- oder sekundären (PWR bzw. RPS) Spannungsversorgung an.
		Aus	Kein Alarm gemeldet

4.4.2 Anschluss-LEDs

Abbildung 8: Anschluss-LEDs

Tabelle 7: Legende zur Abbildung „Anschluss-LEDs“

LED	Anschluss	Status	Beschreibung
LINK/ACT	10/100/1000 BASE T-Anschluss-LED (1 LED für jeden Anschluss)	Grün	Anschluss in Betrieb
		Blinkt	Datenverkehr über Anschluss.
		Aus	Anschluss getrennt oder keine Verbindung.
100M/1G	10/100/1000 BASE T-Anschluss-LED (1 LED für jeden Anschluss)	Gelb	Anschluss ist mit 100/1000 Mbit/s in Betrieb.
		Aus	Anschluss ist mit 10 Mbit/s in Betrieb oder nicht verbunden.

4.5 Technische Daten

4.5.1 Produkt

Tabelle 8: Technische Daten – Produkt

Eigenschaft	Wert
Breite	45,3 mm
Höhe	110 mm
Tiefe	92 mm
Gewicht	441 g
Schutzart	IP30

4.5.2 Systemdaten

Tabelle 9: Technische Daten – Systemdaten

Eigenschaft	Wert
MAC-Tabelle	16384 Einträge
Jumbo-Frame-Größe	10 kB
Maximale Längen	10/100/1000BASE-T(X): 100 m

4.5.3 Spannungsversorgung

Tabelle 10: Technische Daten – Spannungsversorgung

Eigenschaft	Wert
Versorgungsspannung	DC 9 … 48 V
Max. Leistungsaufnahme	5,8 W

4.5.4 Kommunikation

Tabelle 11: Technische Daten – Kommunikation

Eigenschaft	Wert
Ports (Kupfer, RJ-45)	6 x 10/100/1000BASE-T(X)

Eigenschaft	Wert
Ports (Kupfer, RJ-45, MAC Security)	2 x 10/100/1000BASE-T (MAC Security)
Normen	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T IEEE 802.3x Flow Control, back pressure Flow Control IEEE 802.1Q für VLAN Tagging (Priorisierung von Profinet-Paketen) IEEE 802.1p für CoS (Priorisierung von Profinet-Paketen) IEEE 802.1AE für MAC Security

4.5.5 Umgebungsanforderungen

Tabelle 12: Technische Daten – Umgebungsanforderungen

Eigenschaft		Wert
Umgebungstemperatur, Betrieb		-20 … +70 °C
Umgebungstemperatur, Lagerung		-40 … +85 °C
UL 62368-1	Nutzung	Indoor
	Verschmutzungsgrad	PD 2
Relative Feuchte		≤ 95 % bei ≤ +55 °C, ≤ 50 % bei +55 ... +70 °C
Vibrationsfestigkeit		IEC 60068-2-6
Schockfestigkeit		IEC 60068-2-27
EMV-Störfestigkeit		EN 55024 EN 61000-6-2 EN 61000-6-1
EMV-Störaussendung		FCC Part 15, Subpart B, Klasse A, Klasse B EN 55032 Klasse A und Klasse B EN 61000-6-4 EN 61000-6-3 EN 55011

4.6 Richtlinien, Zulassungen und Normen

4.6.1 Zulassungen

Folgende Zulassungen wurden für das Produkt erteilt:

CE	Konformitätskennzeichnung

c UL us	Ordinary Locations	UL62368 (E482462)

ⓘ Hinweis

Weitere Informationen zu Zulassungen

Detaillierte Hinweise zu den Zulassungen finden Sie im Internet unter: **www.wago.com**/<Artikelnummer>

4.6.2 Richtlinien und Normen

Bitte halten Sie die für die Installation und Verwendung der Industrial-Switches geltenden Normen und Bestimmungen ein:

- Die Daten- und Spannungsversorgungsleitungen müssen normgerecht verlegt und angeschlossen werden, um Störungen an Ihrer Anlage oder Gefahren für das Personal zu vermeiden.
- Beachten Sie bei der Montage, Inbetriebnahme, Wartung und Reparatur die für Ihre Anlage zutreffenden Unfallverhütungsvorschriften. Beispielsweise die Vorschrift der DGUV „Elektrische Anlagen und Betriebsmittel“.
- Die Not-Aus-Funktionen und -Einrichtungen dürfen nicht deaktiviert oder anderweitig unwirksam gemacht werden. Siehe dazu die einschlägigen Normen (z. B. die EN 418).
- Ihre Anlage muss den EMV-Richtlinien entsprechen, damit elektromagnetische Störungen ausgeschlossen werden können.
- Beachten Sie die Sicherheitsmaßnahmen gegen elektrostatische Entladung gemäß EN 61340-5-1/-3. Achten Sie beim Umgang mit den Komponenten auf gute Erdung der Umgebung (Personen, Arbeitsplatz und Verpackung).
- Die jeweils geltenden und anwendbaren Normen und Richtlinien zum Aufbau von Schaltschränken sind zu beachten.

Funktionen

5.1 Security

5.1.1 IEEE 802.1X

Der IEEE 802.1X ist ein IEEE-Standard für port-basierte Protokolle für Netzwerkzugriffssteuerungen. Er stellt einen Authentifizierungsmechanismus für Geräte bereit, die mit einem LAN verbunden werden sollen. Das Protokoll verhindert, dass sich nicht berechtigte Clients über Ports mit einem LAN verbinden, die für das Internet geöffnet sind. Die Authentifizierung umfasst im Grunde drei Parteien (siehe Abbildung „RADIUS-Authentifizierungssequenz“ im Kapitel RADIUS [▶ 22]): einen „Supplicant“ (Anfragesteller), einen „Authenticator“ (Authentikator) und einen Authentifizierungsserver.

- Supplicant: Ein Client-Gerät, das Zugang zum LAN anfordert.
- Authentifizierungsserver: Dieser Server führt die eigentliche Authentifizierung durch. Wir nutzen RADIUS („**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice“, ein Authentifizierungsdienst für sich einwählende Benutzer) als Authentifizierungsserver.
- Authenticator: Der Authenticator ist ein Netzwerkgerät (wie etwa der Industrial-Managed-Switch von WAGO), das als Proxy zwischen dem Supplicant und dem Authentifizierungsserver agiert. Er verteilt Informationen und verifiziert sie mit dem Server und leitet Antworten an den Supplicant weiter.

Der Authentikator agiert als eine Art Wächter vor einem geschützten Netzwerk. Der Supplicant erhält so lange keinen Zugriff auf die geschützte Seite des Netzwerks durch den Authentikator, bis seine Identität validiert und autorisiert wurde. Bei der Authentifizierung mit IEEE802.1X tauschen ein Supplicant und ein Authenticator Informationen über das **EAP** („**E**xtensible **A**uthentication **P**rotocol“, ein häufig von IEEE genutztes Authentifizierungsprotokoll) aus. Anschließend leitet der Authenticator die Informationen zum Authentifizierungsserver zur Verifizierung weiter. Wenn der Authentifizierungsserver die Anfrage bestätigt, erhält der Supplicant (das Client-Gerät) Zugriff auf die Ressourcen auf der geschützten Netzwerkseite.

5.1.2 RADIUS

Das RADIUS ist ein Netzwerkprotokoll für die Authentifizierung, Autorisierung und Abrechnung (AAA) von Geräten, die sich mit Netzwerkdiensten verbinden und sie nutzen möchten. Die Abbildung „RADIUS-Authentifizierungssequenz“ zeigt das Diagramm einer RADIUS-Authentifizierungssequenz.

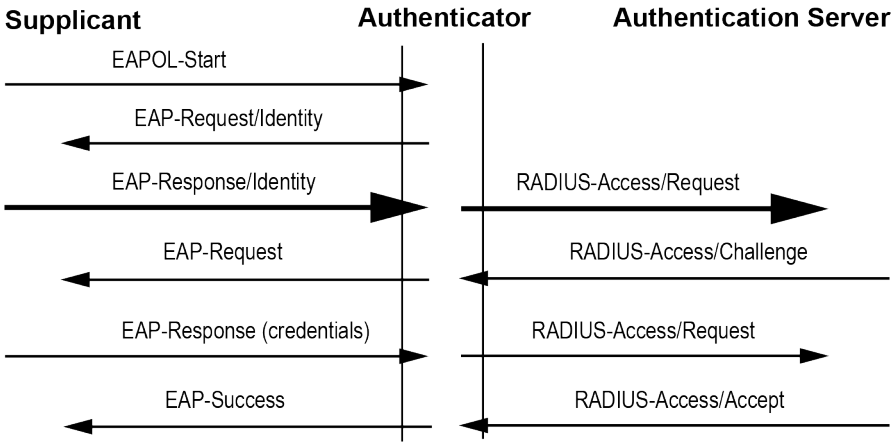

Abbildung 9: RADIUS-Authentifizierungssequenz

5.1.3 MAC Security (MACSec)

Die Industrial-Managed-Switches von WAGO unterstützen moderne Security-Funktionen, die eine Verschlüsselung des Datenverkehrs und hohen Durchsatz ermöglichen. MACsec oder „Media Access Control Security“ ist ein durch das IEEE spezifizierter Sicherheitsstandard, der auch als IEEE 802.1AE bezeichnet wird. Der Standard IEEE MACsec gewährleistet Vertraulichkeit von verbindungslosen Benutzerdaten, Rahmendatenintegrität und Authentizität von Datenquellen. MACsec kann eine Punkt-zu-Punkt-Sicherheit bei ETHERNET-Links zwischen direkt verbundenen Knoten sicherstellen. Die Industrial-Managed-Switches von WAGO unterstützen diese Sicherheitsfunktion und können zur Absicherung einer IEEE802-LAN-Verbindung zu einem Teilnehmergerät (etwa einem anderen Switch) genutzt werden, der ebenfalls MACsec unterstützt.

Bei der Einrichtung einer sicheren Kommunikation zwischen zwei Switches definiert MACsec zwei Begriffe: „Sicherer Kanal“ und „Konnektivitätsbeziehung“. Ein sicherer Kanal in MACsec verläuft unidirektional und wird zur Übertragung (ausgehender Verkehr) oder zum Empfang (eingehender Verkehr) von Daten genutzt. Wenn MACsec aktiviert ist, besteht eine Konnektivitätsbeziehung aus zwei sicheren Kanälen: einer für den eingehenden und einer für den ausgehenden Verkehr.

Die Punkt-zu-Punkt-Verbindungen werden durch MACsec abgesichert, indem zwischen zwei Ports auf sicheren Switches passende Sicherheitsschlüssel ausgetauscht und verifiziert werden.

Für den Sicherheitsmodus „Static Secure Association Key“ (SAK) konfiguriert ein Benutzer auf beiden Seiten der Verbindung manuell denselben „Static Secure Association Key“. In diesem Modus gibt es keinen Schlüsselserver und die Schlüssel müssen auf den Ports beider Switches übereinstimmen. Das kann als Einrichtung zweier sicherer Kanäle innerhalb einer Konnektivitätsbeziehung betrachtet werden. Es empfiehlt sich jedoch, den Schlüssel in regelmäßigen Abständen zu erneuern, um Brute-Force-Angriffen vorzubeugen.

Planung

6.1 Aufbaurichtlinien

6.1.1 Montageort

Die Auswahl des Montageortes für den Industrial-Managed-Switch kann sich entscheidend auf seine Leistung auswirken. Wir empfehlen, bei der Auswahl folgende Richtlinien zu beachten:

- Montieren Sie den Industrial-Managed-Switch an einem geeigneten Standort. Siehe Kapitel **Umgebungsanforderungen [▶ 20]**, um Informationen zu angemessenen Betriebsbereichen hinsichtlich Temperatur und Feuchtigkeit zu erhalten.
- Vergewissern Sie sich, dass die Wärmeabgabe vom Industrial-Managed-Switch und die Belüftung um ihn herum angemessen ist.
- Platzieren Sie keine schweren Objekte auf dem Industrial-Managed-Switch.

Transport und Lagerung

Die Originalverpackung bietet den optimalen Schutz bei Transport und Lagerung.

- Lagern Sie das Produkt in geeigneter Verpackung, möglichst in der Originalverpackung.
- Transportieren Sie das Produkt nur in geeigneten Behältern/Verpackung.
- Stellen Sie sicher, dass die Kontakte des Produktes beim Ein- und Auspacken nicht verschmutzt oder beschädigt werden.
- Beachten Sie die angegebenen klimatischen Umgebungsbedingungen für Transport und Lagerung (**Umgebungsanforderungen [▶ 20]**).

Montieren und Demontieren

8.1 Montieren

8.1.1 Montage auf Tragschiene

Die Hutschiene muss die im System integrierten EMV-Maßnahmen und die Abschirmung über die Netzwerkanschlüsse unterstützen.

Hängen Sie den Industrial-Managed-Switch von oben auf die Hutschiene und rasten Sie ihn ein.

8.2 Demontieren

8.2.1 Demontage von der Tragschiene

Zum Entfernen von der Hutschiene müssen Sie ein geeignetes Werkzeug in die unter dem Switch befindliche Metalllasche einführen und die Metalllasche nach unten auslenken.

Danach können Sie den Switch unten von der Hutschiene lösen und nach oben hin abnehmen.

Anschließen

9.1 Erden

Die Erdung erfolgt über die Erdungsschraube auf der Oberseite des Produktes.

Der Switch muss geerdet werden. Verbinden Sie dazu die Erdungsschraube mit dem Erdpotential. Betreiben Sie den Switch nicht ohne einen entsprechend installierten Schutzleiter.

9.2 Versorgungsspannung anschließen

Der Switch verwendet eine Gleichspannungsversorgung von DC 9 … 48 V .

Die Anschlussstifte, über die mit einer 5-poligen Steckverbindung die primäre und sekundäre Netzverbindung hergestellt wird, befinden sich an der Oberseite des Industrial-Managed-Switches.

Die Federleiste (Artikelnr. 2231-105/026-000) umfasst fünf Anschlussklemmen und kann problemlos per Hand mit der 5-poligen Stiftleiste auf der Oberseite des Switches verbunden und wieder gelöst werden.

1. Verbinden Sie einen geeigneten Erdungsleiter mit der Erdungsschraube an der Oberseite des Switches.

   ⓘ Hinweis **Erdung des Switches**

   Durch die Erdung des Switches werden elektromagnetische Störungen infolge von elektromagnetischer Abstrahlung verhindert.

   Beachten Sie dazu die entsprechenden Normen für EMV-gerechte Installationen.

2. Stecken Sie die Federleiste in die Stiftleiste des Switches, falls noch nicht geschehen. Überprüfen Sie den sicheren Sitz der Federleiste, indem Sie vorsichtig daran rütteln.
3. PWR +/-:
   Zum Anschließen oder Lösen der Leiter betätigen Sie direkt in der Federleiste die Feder mit einem Schraubendreher oder Betätigungswerkzeug und führen den Leiter ein oder lösen ihn.
4. Überprüfen Sie, ob die Netz-LED („PWR“) an der Oberseite leuchtet, wenn das Produkt mit Spannung versorgt wird. Ist dies nicht der Fall, vergewissern Sie sich, dass das Netzkabel richtig eingesteckt ist und fest sitzt.
5. RPS +/-:
   Zum Anschließen oder Lösen der Leiter betätigen Sie direkt in der Federleiste die Feder mit einem Schraubendreher oder Betätigungswerkzeug und führen den Leiter ein oder lösen ihn.
6. Überprüfen Sie, ob die Netz-LED („RPS“) an der Oberseite leuchtet, wenn das Produkt mit Spannung versorgt wird. Ist dies nicht der Fall, vergewissern Sie sich, dass das Netzkabel richtig eingesteckt ist und fest sitzt.

9.3 10/100/1000BASE-T-Ports anschließen

Die 10/100/1000BASE-T-Ports (RJ-45-Ethernet-Anschlüsse) des Industrial-Managed-Switch unterstützen sowohl Autosensing als auch Autonegotiation.

1. Verbinden Sie ein Ende eines verdrillten Kabels vom Typ Cat. 3/4/5/5e mit einem verfügbaren RJ-45-Port am Industrial-Managed-Switch und das andere Ende mit dem Port des ausgewählten Netzwerkknotens.
2. Überprüfen Sie die entsprechende Port-LED am Industrial-Managed-Switch darauf, ob die Verbindung hergestellt ist (siehe Kapitel **Anschluss-LEDs [▶ 19]**).

Konfigurieren im WBM

Für die Konfiguration und Verwaltung des Systems stehen ein internes File-System sowie ein integrierter Webserver zur Verfügung. Zusammen wird dieses System als „Web-Based-Management“ (WBM) bezeichnet.

Auf den intern gespeicherten HTML-Seiten erhalten Sie auslesbare Informationen über die Konfiguration und den Status des Industrial-Managed-Switches. Außerdem ändern Sie hier die Konfiguration des Produktes.

ⓘ Hinweis

Nach Änderungen an der Konfiguration immer einen Neustart durchführen!

Damit geänderte Konfigurationseinstellungen wirksam werden, führen Sie nach Ihren Änderungen immer einen Systemneustart durch.

10.1 Anmeldung

1. Zum Öffnen des WBM starten Sie einen Webbrowser (z. B. Microsoft Edge, Mozilla Firefox oder Google Chrome).
2. Geben Sie die IP-Adresse des Switches ein.
3. Beim Startvorgang sendet das Produkt die GARP-Pakete zum Netzwerk. Wenn Sie das DHCP-Protokoll zur Zuweisung der Produkt-IP-Adresse nutzen oder die statische IP-Adresse des Produktes vergessen haben, können Sie die GARP-Pakete, wie in der folgenden Abbildung gezeigt, mithilfe von Wireshark (eine Netzwerk-Sniffer-Software) erfassen, um die IP-Adresse des Produktes herauszufinden.

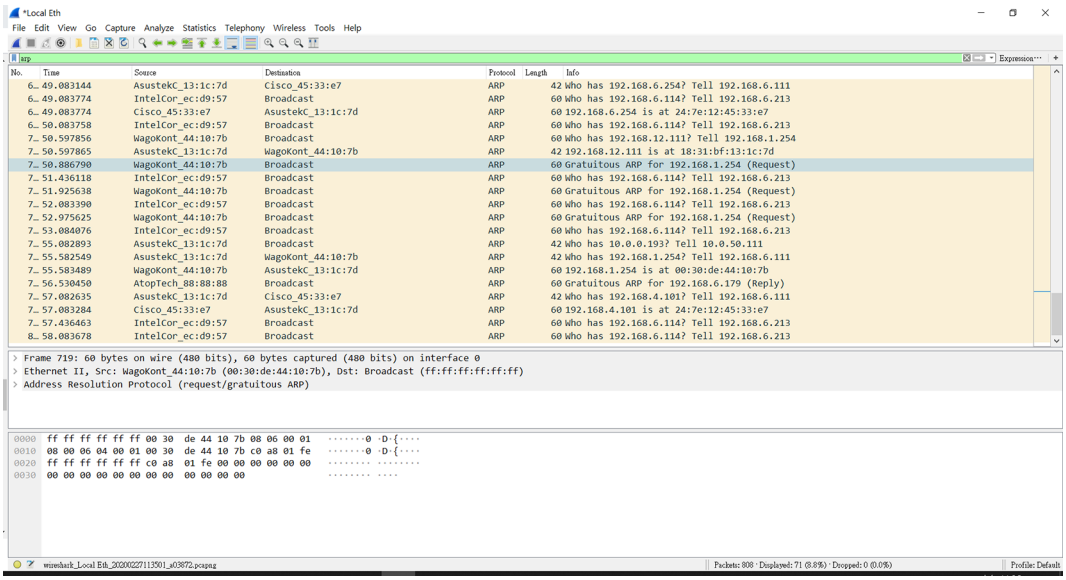

Abbildung 10: Beispiel mit der Sniffer-Software Wireshark zur Anzeige der IP-Adresse eines Switches

4. Bestätigen Sie mit **[Enter]** (Eingabe).
5. Wenn Sie mit Ihrem Webbrowser zum ersten Mal auf das Produkt zugreifen, könnten Sie folgende Sicherheitswarnung angezeigt bekommen.
   - Klicken Sie auf die Schaltflächen **[Advanced]** (Erweitert) und anschließend auf **[Accept the Risk and Continue]** (Risiko akzeptieren und fortfahren).

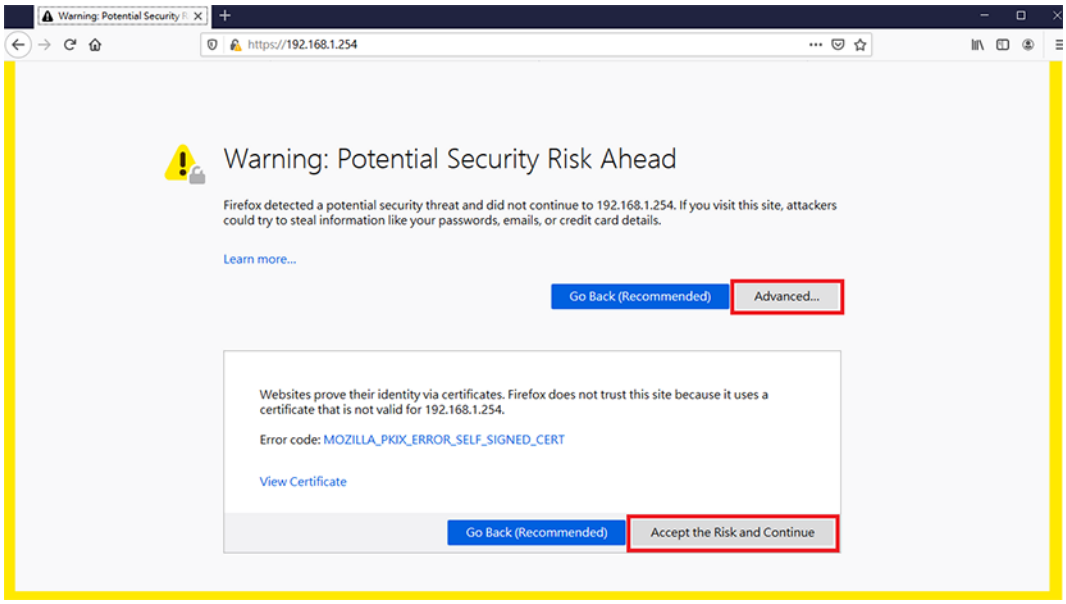

Abbildung 11: Seite mit Sicherheitswarnung

6. Bestätigen Sie mit **[Enter]**.

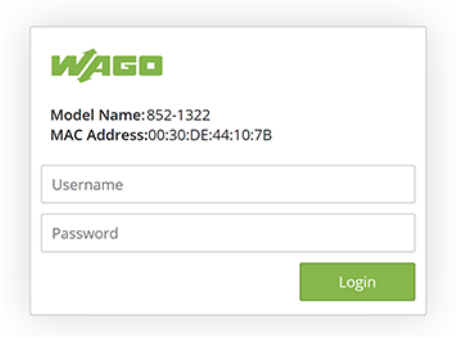

Abbildung 12: WAGO-Anmeldeseite

7. Geben Sie im Abfragedialog Ihren Benutzernamen und das Passwort ein:
   Username = „admin“
   Password = „wago“
8. Die Startseite des WBM wird geladen.

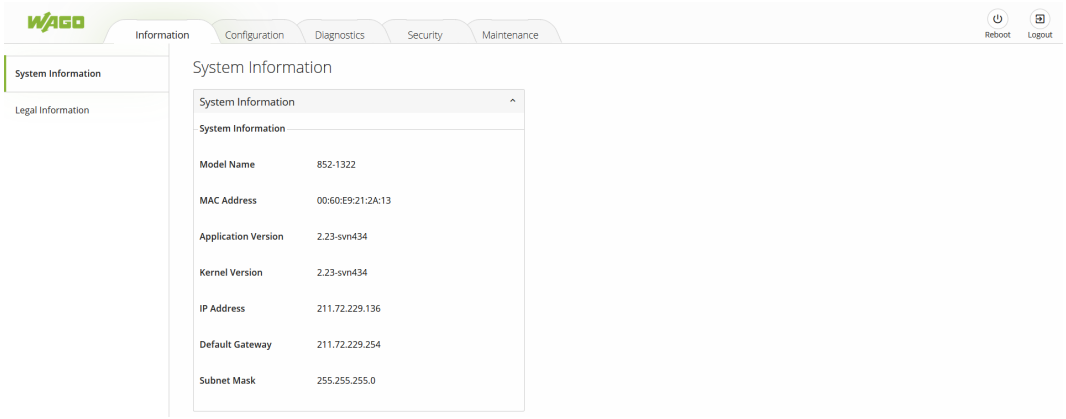

Abbildung 13: Startseite des WBM

9. Wählen Sie über die Navigationsleiste oben im Fenster das gewünschte Register und klicken Sie links im Fenster auf die entsprechende Seite.

10. Führen Sie auf der Website die gewünschten Einstellungen durch.
11. Klicken Sie auf **[Submit]** (Übertragen), **[Change]** (Ändern) oder **[Add]** (Hinzufügen), um Ihre Änderungen zu bestätigen oder zu aktualisieren bzw. die Einstellungen anzuwenden.
12. Das im Auslieferungszustand voreingestellte Standardpasswort bietet keinen hinreichenden Schutz. Deswegen wird Ihnen das Produkt nach der erfolgreichen Anmeldung mit dem Default-Passwort eine Pop-up-Warnung anzeigen, die Sie auffordert, das Passwort zu ändern, und Sie zur Seite für die Passwortänderung weiterleiten. Klicken Sie auf die Schaltfläche **[OK]**, um die Warnung zu quittieren.

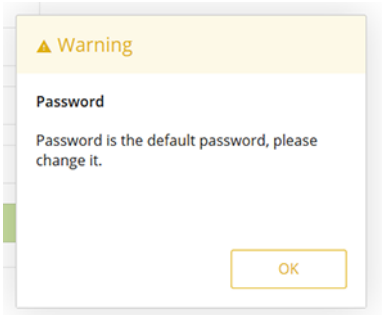

Abbildung 14: Pop-up-Warnung zum Default-Passwort auf der Passwort-Website

Über die Links der Navigationsleiste erreichen Sie die entsprechenden WBM-Seiten.

Tabelle 13: Übersicht – Navigationslinks und WBM-Seiten

Navigationslinks und WBM-Seiten
[Information] (Informationen)
• System Information (Systeminformation) • Legal Information (Rechtliche Informationen)
[Configuration] (Konfiguration)
• System Settings (Systemeinstellungen) • Device Discovery - LLDP (Geräteerkennung - LLDP) • System Management - SNTP (Systemmanagement - SNTP) • Network Settings (Netzwerkeinstellungen) • Port Settings (Port-Einstellungen) • Interface - Mirror (Interface - Port-Mirroring) • Password (Passwort)
[Diagnostics] (Diagnose)
• SNMP • Modbus® TCP • System-Log • Port Monitor (Port-Überwachung)
[Security] (Sicherheit)
• Static SAK (Einstellungen für Statischen SAK) • Secure Code (Sicherheitscode) • 802.1X (IEEE 802.1X) • Port Security (Port-Sicherheit) • VLAN
[Redundancy] (Redundanz)
• RSTP
[Maintenance] (Wartung)
• Firmware-Upgrade • Reset to Default (Rücksetzen auf Default-Werte) • Backup/Restore (Sichern/Wiederherstellen) • Reboot (Neustart)

Navigationslinks und WBM-Seiten
• Logout (Abmelden)

Auf diesen WBM-Seiten können die Einstellungen/Konfigurationen des Industrial-Managed-Switches vorgenommen werden.

Die Default-Werte sind **fett** hervorgehoben dargestellt.

10.2 Anmeldefehler

Wenn Ihre Anmeldung fehlschlägt, erscheint ein Fehlerdialog. Sie können daraufhin zwischen zwei Optionen wählen und auf die Schaltfläche **[Forget it]** (Vergiss es) oder **[Try again]** (Nochmal versuchen) klicken. Wenn Sie auf **[Try again]** klicken, werden Sie nach kurzer Wartezeit zur Anmeldeseite weitergeleitet. Dabei hängt die Wartezeit von der Anzahl fehlgeschlagener Anmeldeversuche ab. Nach dem ersten und zweiten Anmeldeversuch beträgt die Wartezeit 0 Sekunden. Nach dem dritten Anmeldeversuch beträgt die Wartezeit 10 Sekunden. Nach dem vierten Anmeldeversuch beträgt die Wartezeit 100 Sekunden. Nach dem fünften bis zehnten Anmeldeversuch beträgt die Wartezeit 1000 Sekunden. Schlagen mehr als zehn Anmeldeversuche fehl, kann der Benutzer nur noch auf **[Forget it]** klicken und sich mit einem durch die Sicherheitskarte erzeugten Sicherheitscode anmelden, wie in Abbildung „Anmeldefehlerdialog“ angezeigt.

ⓘ Hinweis

Funktionen der Sicherheitskarte

Die Verwendung der Sicherheitskarte und der Option **[Forget it]** werden vom Produkt standardmäßig aktiviert. Nach Ihrer Erstanmeldung können Sie diese Funktion unter der Registerseite „Security“ – „Sicherheitscode“ deaktivieren.

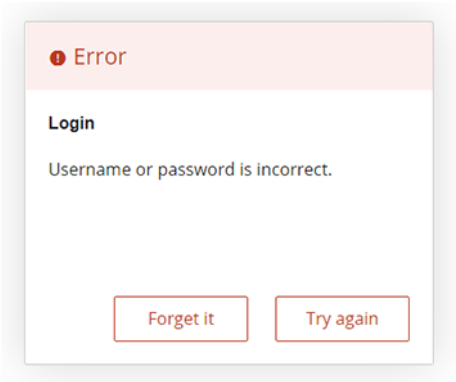

Abbildung 15: Anmeldefehlerdialog

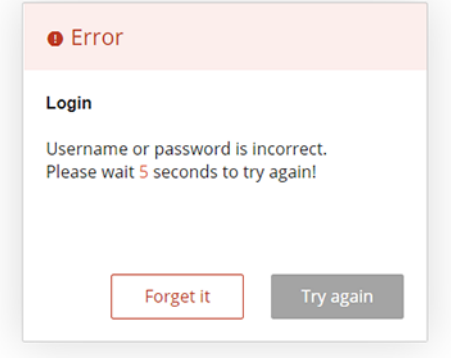

Abbildung 16: Anmeldefehlerdialog mit Schaltfläche [Forget it]

Wenn Sie auf **[Forget it]** klicken, wird das Produkt nach einem zufälligen Sicherheitscode fragen, der aus drei Zeichen besteht. Die drei Zeichen werden von der Sicherheitskarte nach dem Zufallsprinzip ausgewählt. Sie müssen diese Zeichen auf der Sicherheitskarte suchen und sie wie in Abbildung „Dialogbeispiel nach einem Klick auf die Schaltfläche **[Forget it]**. angezeigt in das Textfeld für den Sicherheitscode eingeben. Im Dialog für den Sicherheitscode, wie in Abbildung „Dialogbeispiel nach einem Klick auf die Schaltfläche **[Forget it]** angezeigt, erhalten Sie Hinweise zur Zusammensetzung des neuen Sicherheitscodes. Anhand der Zeichen auf der Sicherheitskarte, die in Abbildung „Beispiel einer Sicherheitskarte“ dargestellt ist, lautet der Sicherheitscode „NLS”. Im Dialog können Sie zwischen den Schaltflächen **[OK]** und **[Cancel]** (Abbrechen) wählen.

Abbildung 17: Dialogbeispiel nach einem Klick auf die Schaltfläche [Forget it]

Abbildung 18: Beispiel einer Sicherheitskarte

Nach der Eingabe des richtigen Sicherheitscodes und einem Klick auf **[OK]** werden Sie zur Registerseite für die Passwortänderung weitergeleitet, wo Sie, wie in Abbildung „Weiterleitung zur Registerseite für die Passwortänderung“ angezeigt, sofort das Passwort ändern müssen. Wenn Sie das neue Passwort eingegeben haben, klicken Sie auf die Schaltfläche **[Submit]**. Das System wird Ihnen daraufhin die WAGO-Anmeldeseite anzeigen, auf der Sie, wie in Abbildung „WAGO-Anmeldedialog nach Passworterneuerung“ angezeigt, das neue Passwort eingeben können.

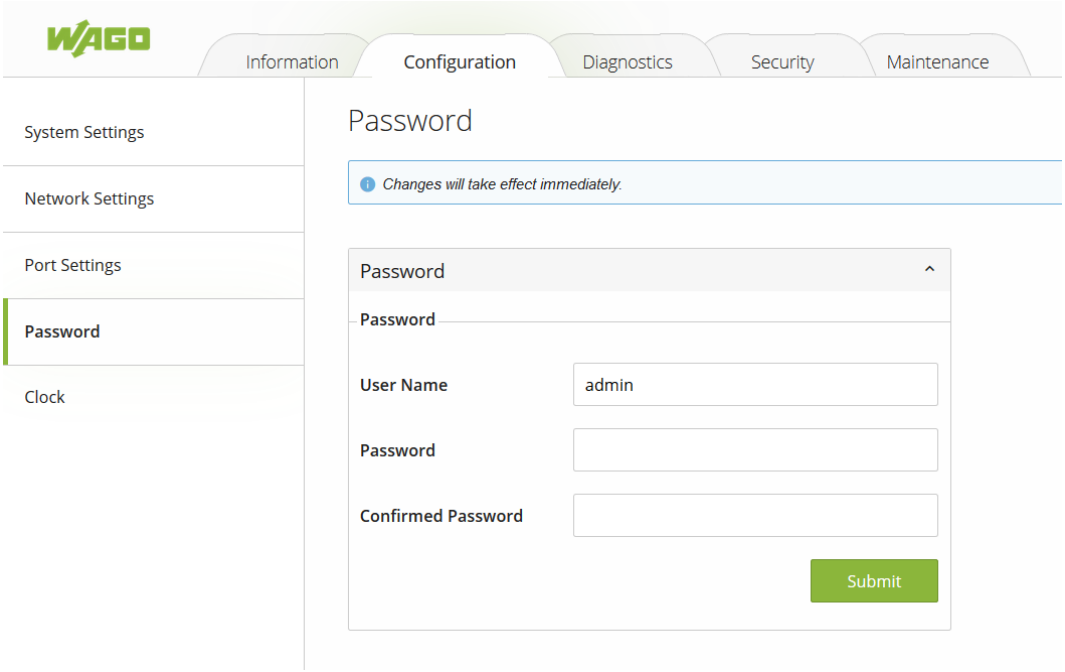

Abbildung 19: Weiterleitung zur Registerseite für die Passwortänderung

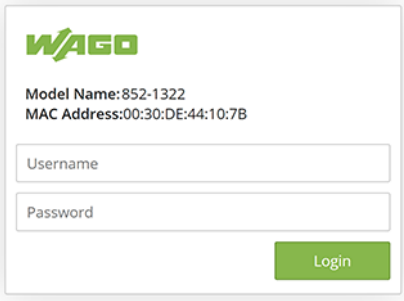

Abbildung 20: WAGO-Anmeldedialog nach Passworterneuerung

10.3 Informationen

10.3.1 System Information (System Information)

Damit sich Benutzer mit dem Produkt vertraut machen können, zeigt die Registerseite „System Information“ wichtige Informationen über den Industrial-Managed-Switch von WAGO. Nach der Anmeldung ist dies auch das Willkommensfenster für Benutzer. Die Informationen vereinfachen die Identifikation der verschiedenen Switches, die mit dem Netzwerk verbunden sind. Dem Benutzer werden verschiedene Information angezeigt, wie etwa Modellname, MAC-Adresse, Applikationsversion, Kernel-Version, IP-Adresse,

Default-Gateway und Subnetzmaske. Die Abbildung „WBM-Seite „Informationen“ – „Systeminformation“ zeigt ein Beispiel für Systeminformationen. Die Tabelle „WBM-Seite „Informationen“ – Registerseite „Systeminformation““ fasst die Beschreibungen für jedes Feld in den Systeminformationen zusammen.

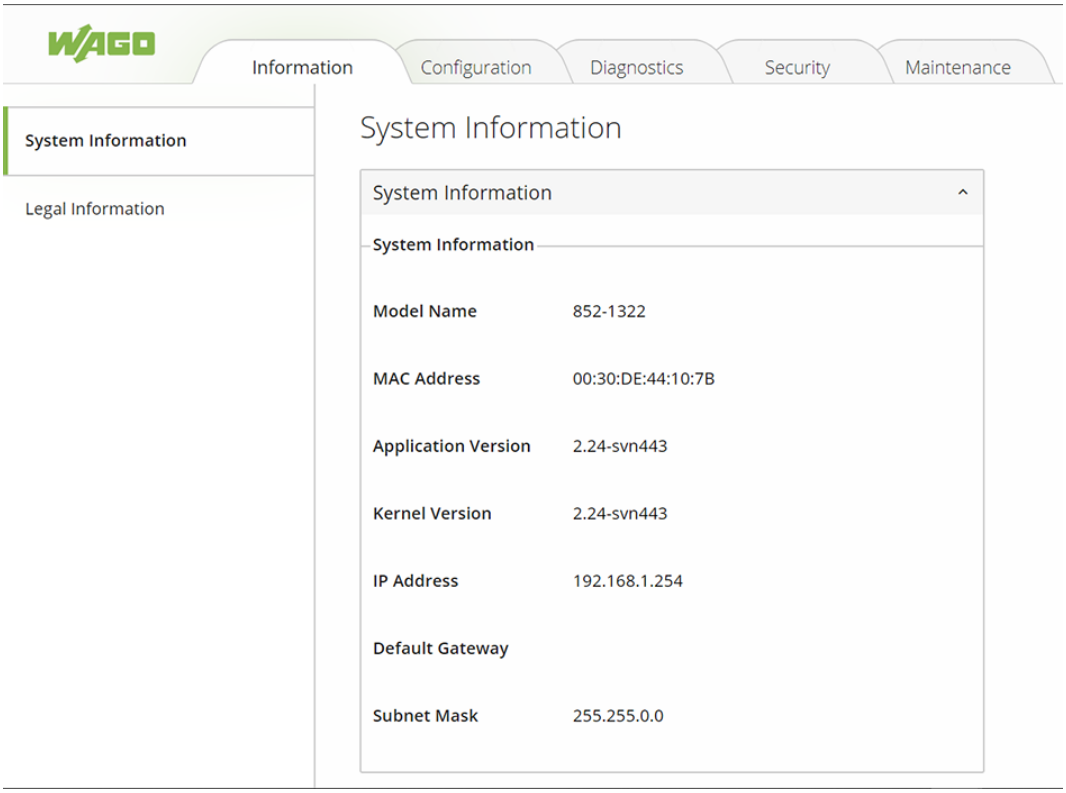

Abbildung 21: WBM-Seite „Informationen“ – „Systeminformation“

Tabelle 14: WBM-Seite „Informationen“ – Registerseite „Systeminformation“

Parameter	Beschreibung
Model Name	In diesem Anzeigefeld wird der Modellname des Switches angezeigt.
MAC Address	In diesem Anzeigefeld wird die MAC (Media-Access-Control)-Adresse des Switches angezeigt.
Application Version	In diesem Anzeigefeld wird die Firmware-Version im Switch angezeigt.
Kernel Version	In diesem Anzeigefeld wird die Kernel-Version der Firmware im Switch angezeigt.
IP Address	In diesem Anzeigefeld wird die IP-Adresse des Switches angezeigt. Sie ist gleichzeitig auch die IP-Adresse für die Anmeldung im Produkt.
Default Gateway	In diesem Anzeigefeld wird das Default-Gateway des Switches angezeigt.
Subnet Mask	In diesem Anzeigefeld wird die Subnetzmaske des Switches angezeigt.

10.3.2 Legal Information (Rechtliche Information)

Auf dieser Seite befinden sich die beiden Registerseiten „WAGO Licenses“ (WAGO-Lizenzen) und „Open Source Licenses“ (Open-Source-Lizenzen). Hier werden alle Informationen und Bedingungen des Software-Lizenzvertrages aufgeführt.

Wago Licenses (WAGO-Lizenzen)

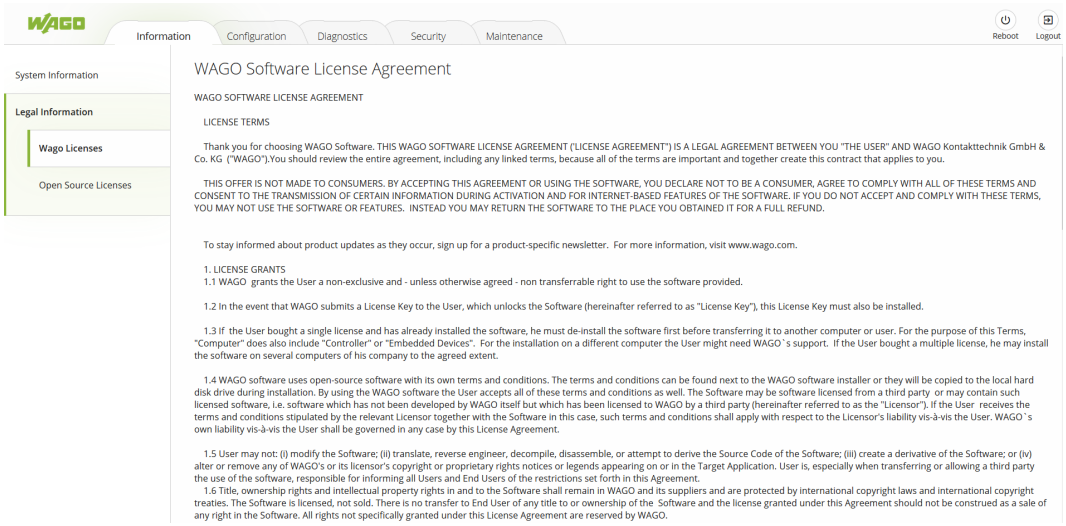

Abbildung 22: WBM-Seite „Informationen“ – „Rechtliche Information“ – Registerseite „WAGO-Lizenzen“

Open Source Licenses (Open-Source-Lizenzen)

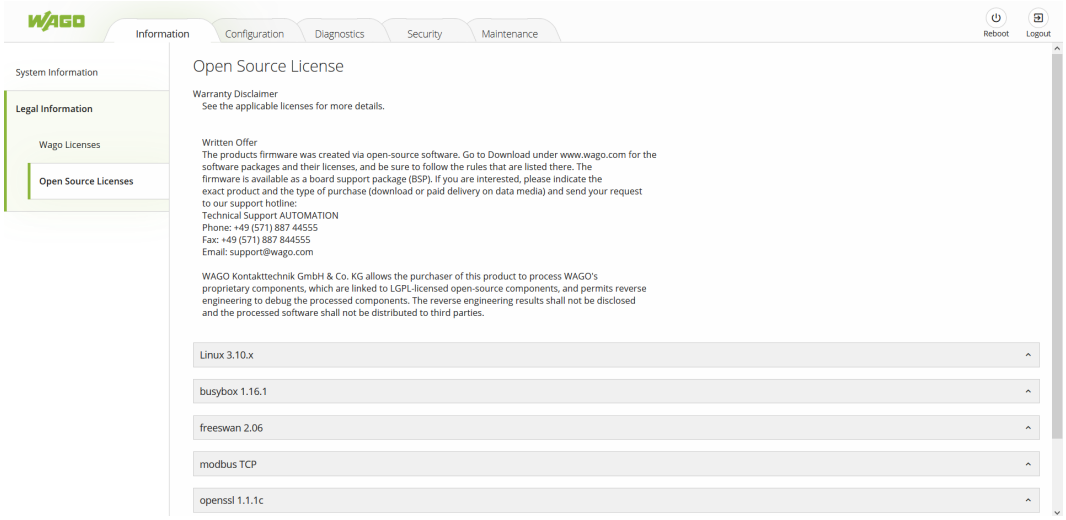

Abbildung 23: WBM-Seite „Informationen“ – „Rechtliche Information“ – Registerseite „Open-Source-Lizenzen“

10.4 Configuration (Konfiguration)

10.4.1 System Settings (Systemeinstellungen)

Auf der Registerseite „Systemeinstellungen“ können Benutzer Produkteinstellungen für den Industrial-Managed-Switch von WAGO vornehmen. Durch die Eingabe eindeutiger und relevanter Systeminformationen, wie etwa den Produktnamen, kann unter allen anderen Geräten im Netzwerk ein spezifischer Switch identifiziert werden. Bitte klicken Sie auf die Schaltfläche **[Submit]** (Übertragen), um die Informationen auf diesem Switch zu aktualisieren. Die Abbildung „WBM-Seite „Konfiguration“ – Registerseite „Systemeinstellungen““ zeigt die Seite „Systemeinstellungen“. Die Tabelle „WBM-Seite „Konfiguration“ – Registerseite „Systemeinstellungen““ fasst die Produktinformationen, Beschreibungen und entsprechenden Werkseinstellungen für das Produkt zusammen.

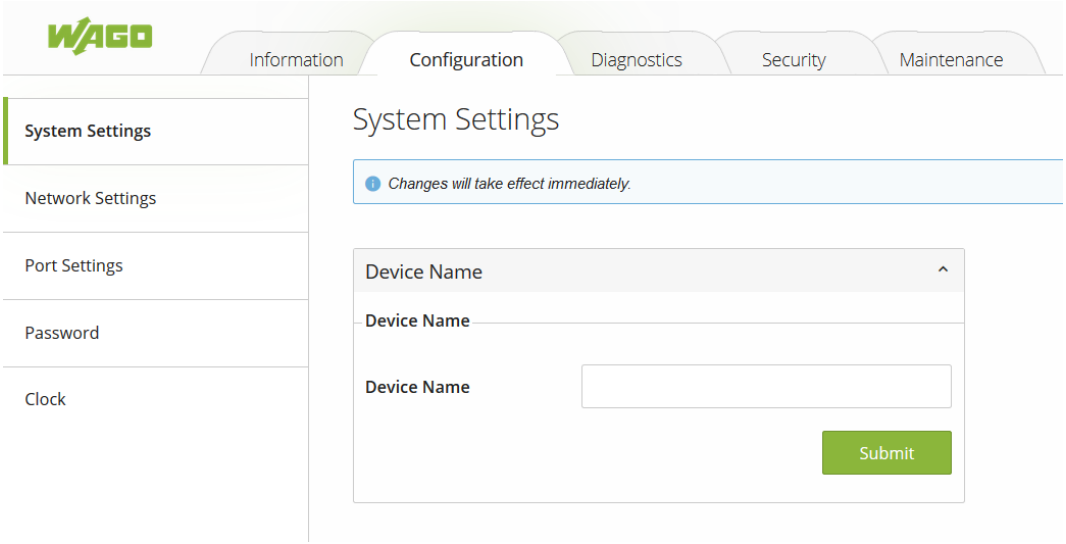

Abbildung 24: Seite "Konfiguration" - Registerkarte "Systemeinsetllungen"

Tabelle 15: WBM-Seite „Konfiguration“ – Registerseite „Systemeinstellungen“

Parameter	Werkseinstellung	Beschreibung
Device Name	(k. A.)	In diesen Textfeldern können bestimmte Rollen oder Anwendungen für verschiedene Switches definiert werden. In ein Textfeld können maximal 63 Zeichen eingetragen werden.

10.4.2 Device Discovery - LLDP (Geräteerkennung – LLDP)

Das LLDP („**L**ink **L**ayer **D**iscovery **P**rotocol“) ermöglicht es Stationen, die mit einem LAN gemäß IEEE 802.1ab verbunden sind, Informationen an andere, an dasselbe LAN angeschlossene Stationen, zu senden. Diese Informationen beinhalten wesentliche Funktionen des Systems dieser Station, einschließlich der Management-Adresse oder Adressen einer Entität oder Entitäten, die das Management dieser Funktionen bereitstellen, sowie die Identifizierung des Stationszugangspunktes zum IEEE802-LAN, den diese Managemententität oder -entitäten benötigen.

Es können nur LLDP-Informationen an ein Gerät gesendet oder von ihm empfangen werden. Es werden keine Informationen abgefragt und keine Zustandsänderungen zwischen den Knoten vorgenommen. Das Gerät kann die Funktionen zum Versand und Empfang unabhängig voneinander aktivieren und deaktivieren.

Das LLDP ist für die Verwaltung durch das SNMP konzipiert. Zu den Applikationen, die dieses Protokoll nutzen, gehören die Bereiche Topologieerkennung, Bestandsverwaltung, Notfalldienste, VLAN-Zuweisungen und Inline-Spannungsversorgungen.

ⓘ Hinweis

Nach der Aktivierung erscheinen auf der Topologiekarte von Lean-Managed-Switches Informationen über Geräte mit LLDP. Die Switch-Informationen werden mit anderen Geräten geteilt, die mit demselben Netzwerk verbunden sind.

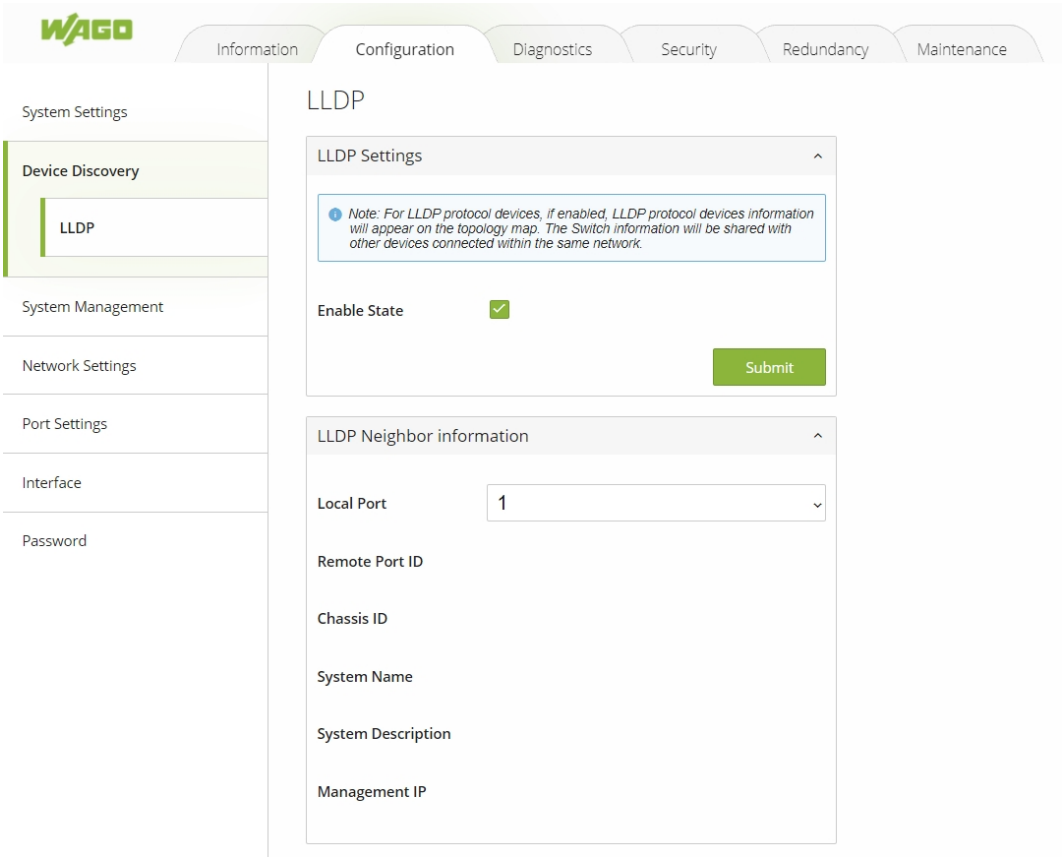

Abbildung 25: WBM-Seite „Konfiguration“ – Registerseite „LLDP Einstellungen“

Tabelle 16: WBM-Seite „Konfiguration“ – Registerseite „LLDP-Einstellungen“

Parameter	Beschreibung
Enable State	Aktivieren Sie „Enable State“, um LLDP im Switch zu aktivieren. Deaktivieren Sie „Enable State“, um LLDP im Switch zu deaktivieren. Denken Sie daran, Ihre Änderungen mit der Schaltfläche [SUBMIT] zu bestätigen.
LLDP-Nachbarinformationen	Hier wird eine Statusübersicht der erkannten LLDP-Nachbarn angezeigt.
Local Port (Lokaler Port)	Spezifizieren Sie den Port im lokalen Switch, für den die LLDP-Nachbarinformationen angezeigt werden sollen. Daraufhin werden die an diesem Port empfangenen Informationen über Geräte mit aktiviertem LLDP angezeigt.

10.4.3 System Management - SNTP (Systemmanagement – SNTP)

10.4.3.1 Allgemeine Informationen

Das SNTP („**S**imple **N**etwork **T**ime **P**rotocol“) ist ein Protokoll zur Synchronisierung von Uhren in Computersystemen. Es ist eine weniger komplexe Implementierung eines NTP („**N**etwork **T**ime **P**rotocol“).

SNTP verwendet die Koordinierte Weltzeit UTC. Es werden keine Informationen über Zeitzonen oder Sommerzeiten übertragen. Diese Informationen liegen außerhalb des Protokollbereichs und müssen separat bezogen werden. Der SNTP-Port ist 123.

Zusätzlich:

- Der SNTP-Server antwortet immer mit der aktuellen UTC-Zeit.
- Empfängt der Switch die SNTP-Antwortzeit, gleicht er diese Zeit mit der Zeitzonenkonfiguration ab und konfiguriert die Zeit für den Switch entsprechend.

- Ist keine IP-Adresse für einen Zeitserver spezifiziert, versendet der Switch keine SNTP-Abfragepakete.
- Empfängt der Switch keine SNTP-Antwortpakete, wiederholt er die Abfrage ohne zeitliche Beschränkung alle zehn Sekunden.
- Erhält der Switch eine SNTP-Antwort, wiederholt er die Zeitabfrage an den NTP-Server stündlich.
- Nach Änderung der Zeitzone und des NTP-Servers wiederholt der Switch den Abfrageprozess.
- Es gibt keinen Default-SNTP-Server.

10.4.3.2 SNTP-Einrichtung

Zuerst muss aus der Pull-down-Liste ein Modus gewählt werden. Der Modus „Manual“ (manuell) deaktiviert das SNTP. Die Zeit muss dann manuell eingestellt werden. Der Modus „Network Time Protocol“ aktiviert das SNTP. Beide Modi werden unten beschrieben.

Modus: Manuell

Wählen Sie den Modus „Manual“ aus, um das SNTP zu deaktivieren. Die Zeit muss dann manuell eingestellt werden.

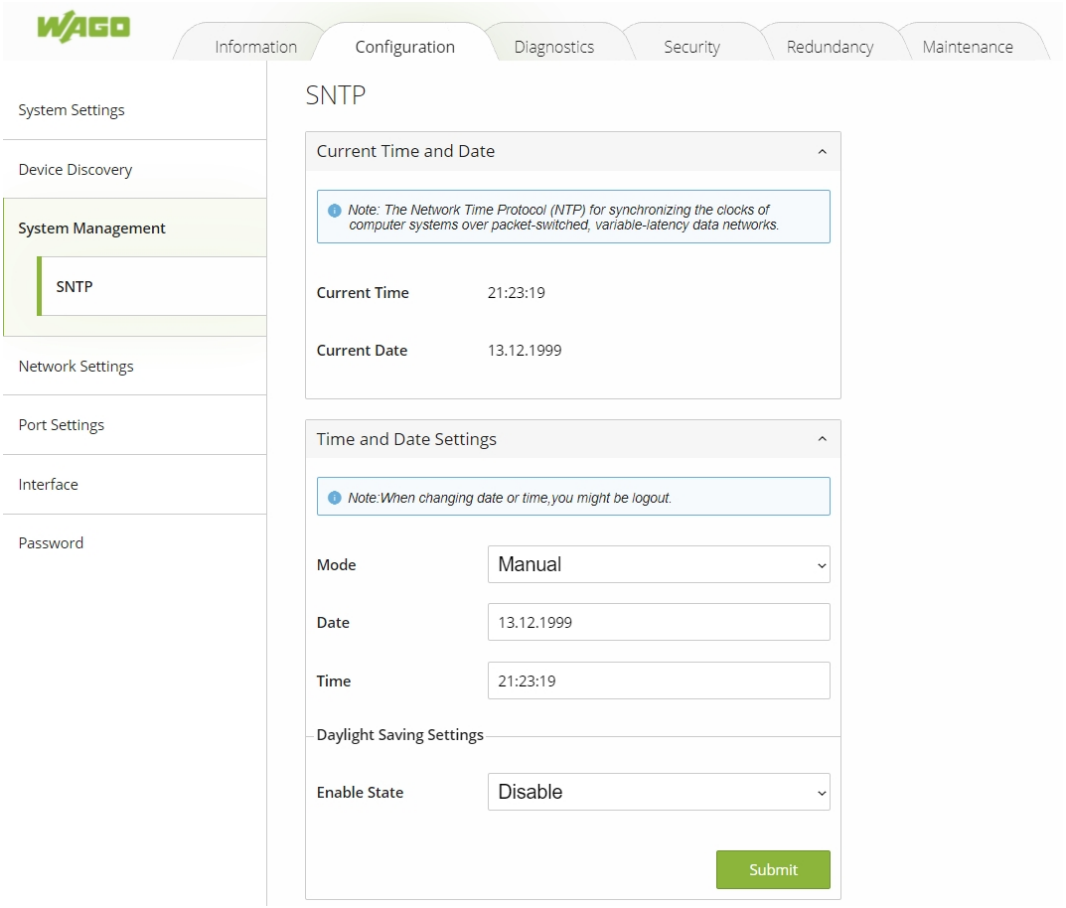

Abbildung 26: WBM-Seite „Konfiguration“ – Registerseite „SNTP“

Tabelle 17: WBM-Seite „Konfiguration“ – Registerseite „SNTP“

Parameter	Beschreibung
Current Time and Date (Aktuelle Uhrzeit und aktuelles Datum)	

Parameter	Beschreibung
Current Time	In diesem Anzeigefeld wird die aktuelle Uhrzeit angezeigt, wenn Sie das WBM öffnen bzw. aktualisieren.
Current Date	In diesem Anzeigefeld wird das aktuelle Datum angezeigt, wenn Sie das WBM öffnen bzw. aktualisieren.
Time and Date Settings (Uhrzeit- und Datumseinstellungen)	
Date	Tragen Sie das Datum für das System manuell im Format Jahr/Monat/Tag ein.
Time	Tragen Sie die Uhrzeit für das System manuell im Format Stunden/Minuten/Sekunden ein.
Daylight Saving Settings (Sommerzeiteinstellungen)	
Enable State	Wählen Sie „Enable“ oder „Disable“, um die Sommerzeiteinstellungen zu aktivieren bzw. zu deaktivieren.
Start Day (Starttag)	Tragen Sie Datum und Uhrzeit für den Beginn der Sommerzeit ein, falls Sie diese Option aktiviert haben. Die Zeit wird im 24-Stunden-Format angezeigt.
End Day (Endtag)	Tragen Sie Datum und Uhrzeit für das Ende der Sommerzeit ein, falls Sie diese Option aktiviert haben. Die Zeit wird im 24-Stunden-Format angezeigt.

Modus: Network Time Protocol

Wählen Sie den Modus „Network Time Protocol“, um das SNTP zu aktivieren. Anschließend muss ein NTP-Server spezifiziert werden.

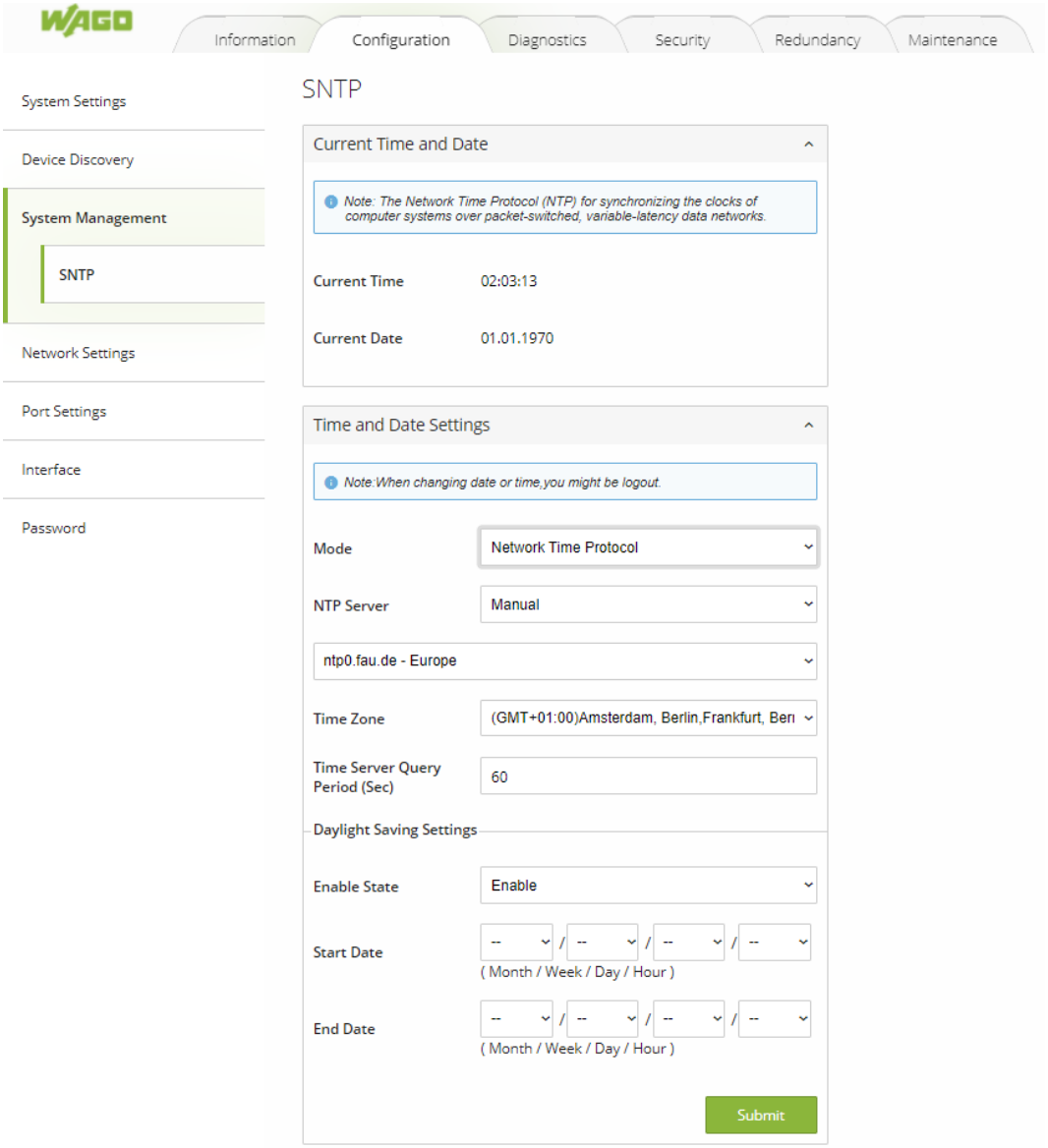

Abbildung 27: WBM-Seite „Konfiguration“ – Registerseite „SNTP“

Tabelle 18: WBM-Seite „Konfiguration“ – Registerseite „SNTP“

Parameter	Beschreibung	
Current Time and Date (Aktuelle Uhrzeit und aktuelles Datum)		
Current Time	In diesem Anzeigefeld wird die aktuelle Uhrzeit angezeigt, wenn Sie das WBM öffnen bzw. aktualisieren.	
Current Date	In diesem Anzeigefeld wird das aktuelle Datum angezeigt, wenn Sie das WBM öffnen bzw. aktualisieren.	
Time and Date Settings (Uhrzeit- und Datumseinstellungen)		
NTP Server	Wählen Sie einen vordefinierten Zeitserver aus („public“) oder tragen Sie manuell die IP-Adresse eines Zeitservers ein („manual“).	
Public (öffentlich)	Wählen Sie einen der vordefinierten Zeitserver aus.	
Manual (manuell)	IP/Domain	Wählen Sie aus, ob Sie eine IP-Adresse oder ob Sie einen vollständigen Domain-Namen für den Zeitserver spezifizieren möchten.
Manual	Wählen Sie im Textfeld unten aus, ob Sie eine IP-Adresse oder ob Sie einen vollständigen Domain-Namen für den Zeitserver spezifizieren möchten.	
Timezone (Zeitzone)	Wählen Sie die Zeitzone aus, in der Sie sich befinden.	

Parameter	Beschreibung
Daylight Saving Settings (Sommerzeiteinstellungen)	
Enable State	Wählen Sie „Enable“ oder „Disable“, um die Sommerzeiteinstellungen zu aktivieren bzw. zu deaktivieren.
Start Day (Starttag)	Tragen Sie Datum und Uhrzeit für den Beginn der Sommerzeit ein, falls Sie diese Option aktiviert haben. Die Zeit wird im 24-Stunden-Format angezeigt.
End Day (Endtag)	Tragen Sie Datum und Uhrzeit für das Ende der Sommerzeit ein, falls Sie diese Option aktiviert haben. Die Zeit wird im 24-Stunden-Format angezeigt.

10.4.4 Network Settings (Netzwerkeinstellungen)

Auf dieser Registerseite können Benutzer Netzwerkeinstellungen in der Internetprotokollversion 4 (IPv4) für den Industrial-Managed-Switch von WAGO vornehmen.

Die Registerseite „Netzwerkeinstellungen“ wird in Abbildung „WBM-Seite „Konfiguration“ – Registerseite „Netzwerkeinstellungen““ angezeigt. Unter den Netzwerkeinstellungen können Benutzer durch die Aktivierung des Kontrollkästchens den Client für das „Dynamic Host Configuration Protocol“ (DHCP) im Switch aktivieren. Dadurch kann der Switch die IP-Adresseinstellungen von einem im lokalen Netzwerk verfügbaren DHCP-Server automatisch beziehen. Wenn das DHCP aktiviert ist, werden die restlichen Felder deaktiviert. Benutzer sollten sich an den Administrator Ihres lokalen Netzwerks wenden, um zu erfahren, ob ein DHCP-Server verfügbar ist. Soll eine statische IP-Einstellung verwendet werden, kann der Benutzer mit der Eingabe von IP-Adresse, Subnetzmaske, Gateway und primärem DNS fortfahren. Bei Angabe von Gateway oder DNS auf dieser Seite wird der Industrial-Managed-Switch weder Gateway noch DNS vom DHCP-Server nutzen. Wenn Sie alle gewünschten Informationen eingetragen haben, klicken Sie bitte auf **[Submit]**, um die IP-Einstellungen zu übertragen.

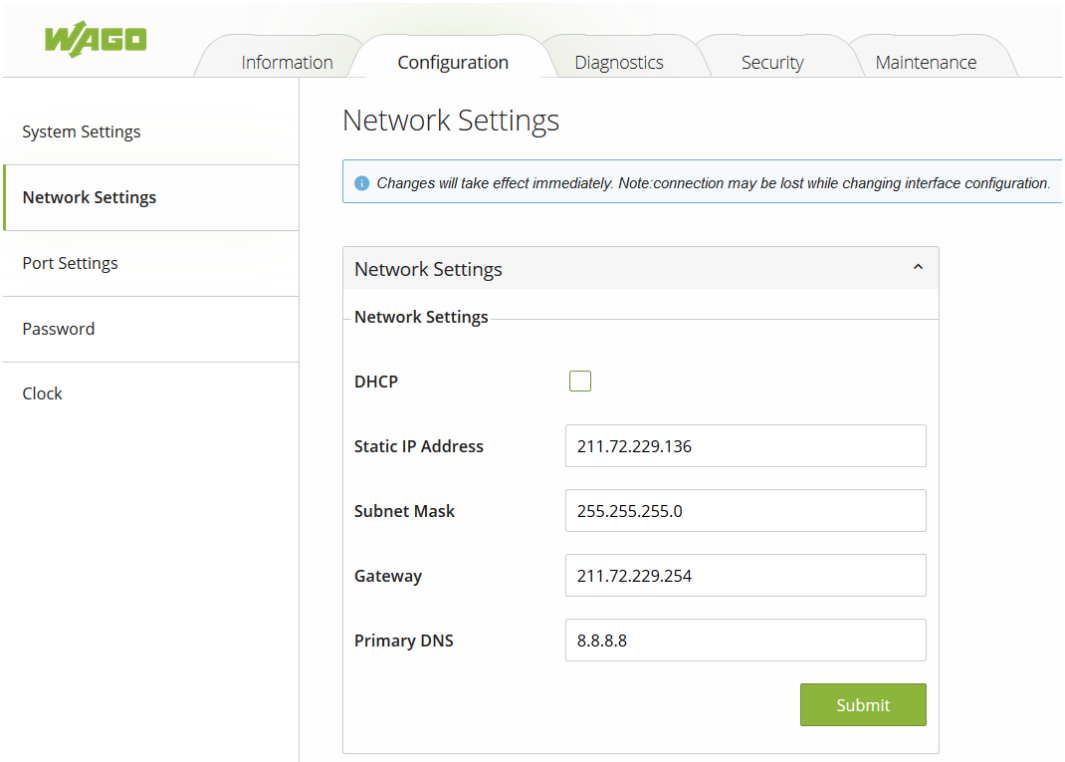

Abbildung 28: WBM-Seite „Konfiguration“ – Registerseite „Netzwerkeinstellungen“

Die Beschreibungen der einzelnen Parameter und ihrer Default-Werte auf der Registerseite der Netzwerkeinstellungen werden in Tabelle „WBM-Seite „Konfiguration“ – Registerseite „Netzwerkeinstellungen““ zusammengefasst.

Tabelle 19: WBM- Seite „Konfiguration“ – Registerseite „Netzwerkeinstellungen“

Parameter	Werkseinstellung	Beschreibung
DHCP	Deaktiviert	Durch Aktivierung dieses Kontrollkästchens werden IP-Adresse und zugehörige Parameter automatisch zugewiesen. Ansonsten können Benutzer auch eine statische IP-Adresse angeben und zugehörige Felder manuell ausfüllen.
Static IP Address	192.168.1.254	In diesem Feld wird die aktuelle IP-Adresse angezeigt. Benutzer können auch eine neue statische IP-Adresse für das Produkt angeben.
Subnet Mask	255.255.255.0	In diesem Feld wird die aktuelle Subnetzmaske angezeigt. Benutzer können in diesem Feld auch eine neue Subnetzmaske angeben.
Gateway	0.0.0.0	In diesem Anzeigefeld wird die aktuelle IP-Adresse des Gateways angezeigt. Benutzer können in diesem Feld auch eine neue IP-Adresse für das Gateway angeben.
Primary DNS	Null	Benutzer können in diesem Feld die primäre IP-Adresse für das DNS in ihrem Netzwerk angeben.

10.4.5 Port Settings (Port-Einstellungen)

10.4.5.1 Setting (Einstellung)

Benutzer können durch Auswahl von „Enable“ (Aktivieren) oder „Disable“ (Deaktivieren) im Drop-down-Menü den Zustand jedes Ports steuern (siehe Abbildung „WBM-Seite „Konfiguration“ – Registerseite „Port-Einstellungen““). Klicken Sie nach jeder Änderung an den Port-Einstellungen auf die Schaltfläche **[Submit]**.

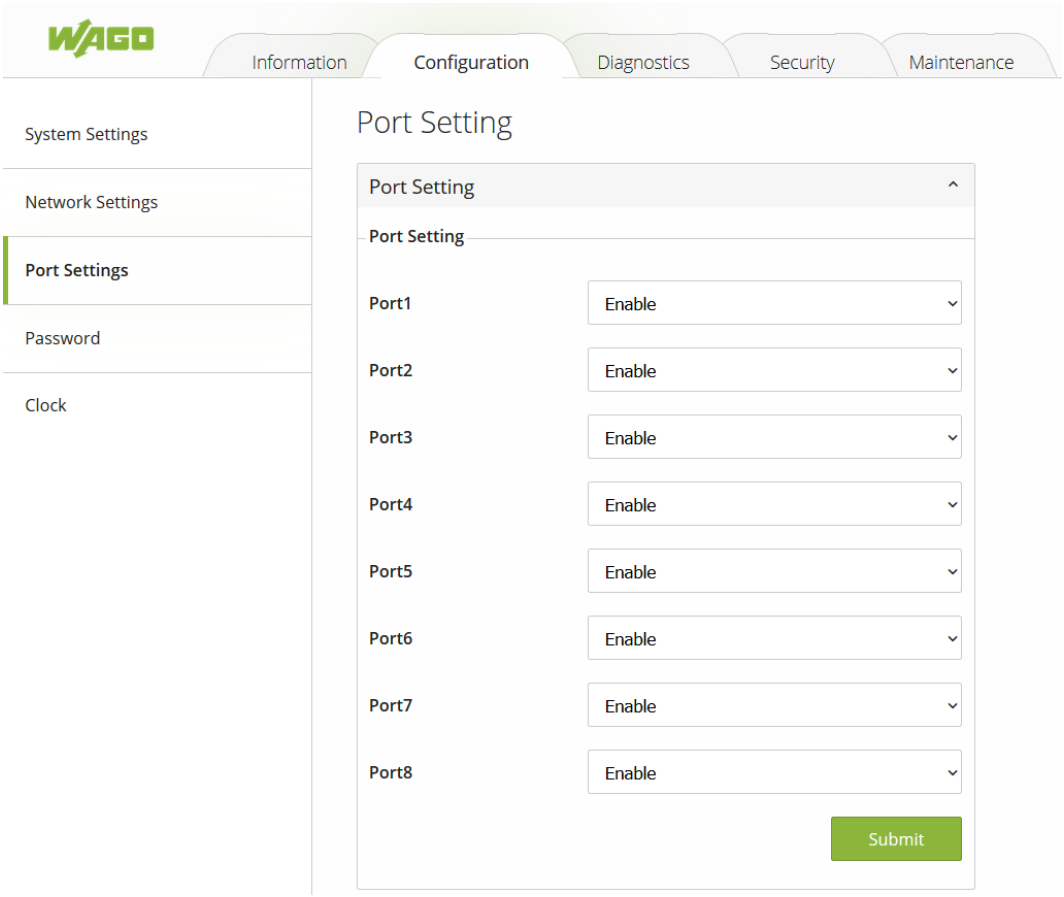

Abbildung 29: WBM-Seite „Konfiguration“ – Registerseite „Port-Einstellungen“

Die Beschreibungen der einzelnen Parameter und ihrer Default-Werte auf der Registerseite der Port-Einstellungen werden in Tabelle „WBM-Seite „Konfiguration“ – Registerseite „Port-Einstellungen““ zusammengefasst.

Tabelle 20: WBM- Seite „Konfiguration“ – Registerseite „Port-Einstellungen“

Parameter	Werkseinstellung	Beschreibung
Port n	Aktiviert	In diesem Feld wird die Nummer des Ports am Industrial-Managed-Switch angezeigt. Durch Auswahl von „Enable“ oder „Disable“ im Drop-down-Menü kann der Zustand eines Ports geändert werden. Im aktivierten Zustand wird das Senden und Empfangen von Daten über diesen bestimmten Port ermöglicht.

10.4.6 Interface - Mirror (Interface - Port-Mirroring)

10.4.6.1 Allgemeine Informationen

Das „Port-based Mirroring“ (Portbasierte Spiegelung) wird bei Netzwerk-Switches eingesetzt, um Kopien von an einen Switch-Port oder Switch-Port-Bereich gesendete/empfangene Netzwerkpakete an eine Netzwerküberwachung zu senden, die mit einem anderen Port („Monitor-Port“) verbunden ist.

Dies wird häufig in Netzwerkgeräten eingesetzt, bei denen eine Überwachung des Netzwerkverkehrs erforderlich ist, wie etwa in einem „Intrusion Detection System“ (Angriffserkennungssystem).

Das „Port Mirroring“ kann zusammen mit einem „Network Traffic Analyzer“ (Programm zur Analyse des Netzwerkverkehrs) dabei helfen, den Netzwerkverkehr zu überwachen. Dabei können Benutzer bei ausgewählten Ports („Source Ports“, Quell-Ports) die eingehenden und ausgehenden Datenpakete überwachen lassen.

Source Mode (Quellmodus)

- „Ingress“ (Eingang): Die eingehenden Datenpakete werden kopiert und zum Monitor-Port weitergeleitet.
- „Egress“ (Ausgang): Die ausgehenden Datenpakete werden kopiert und zum Monitor-Port weitergeleitet.

ⓘ Hinweis

- Der Monitor-Port kann kein Mitglied einer „Trunk Port“-Gruppe sein.

- Die Firmwareversion 2.53 für den Switch erlaubt es Ihnen nicht, einen Port-Bereich zu einem Monitor-Port zu kopieren.

- Die Firmwareversion 2.53 für den Switch erlaubt es Ihnen nicht, zwischen verschiedenen Quellmodi zu wählen. Es werden standardmäßig sowohl eingehende als auch ausgehende Datenpakete kopiert und zum Monitor-Port weitergeleitet.

10.4.6.2 Port-Mirroring – Einrichtung

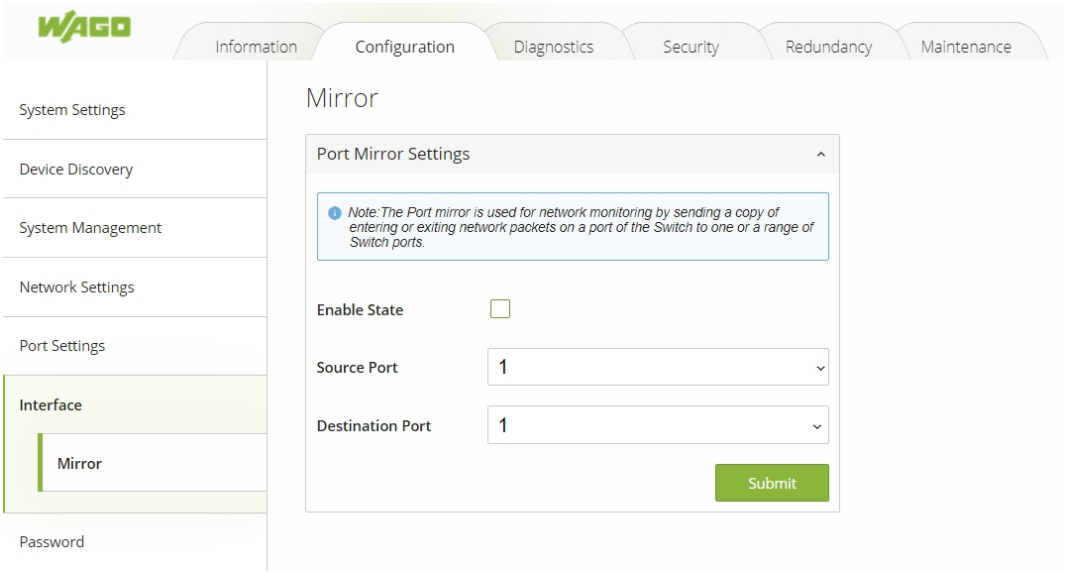

Abbildung 30: WBM-Seite „Konfiguration“ – Registerseite „Mirror“

Tabelle 21: WBM-Seite „Konfiguration“ – Registerseite „Mirror“

Parameter	Beschreibung
Enable State	Aktivieren Sie „Enable State“, um das Port-Mirroring zu aktivieren. Deaktivieren Sie „Enable State“, um das Port-Mirroring zu deaktivieren. Das Port-Mirroring muss aktiviert sein, bevor der ausgewählte Quell-Port oder Destination-Port geändert werden können.
Source Port	Wählen Sie einen Port aus, um seine eingehenden („ingress“) und ausgehenden („egress“) Daten zum Destination-Port zu kopieren.
Destination Port	Wählen Sie den Port aus, zu dem der Netzwerkverkehr des Quell-Ports kopiert werden soll.

10.4.7 Password (Passwort)

Bei der Fertigung des Produktes werden der Benutzername „admin“ und das Passwort „wago“ als Werkseinstellung vorgegeben. Benutzer können den Benutzernamen und das Passwort ändern, um die Gesamtsicherheit des Produktes zu sicherzustellen. Benutzername und Passwort können in dieser Registerseite, wie in Abbildung „WBM-Seite „Konfiguration“ – Registerseite „Passwort“ angezeigt, geändert werden. Das Passwort muss sowohl im Textfeld „Password“ (Passwort) als auch im Textfeld „Confirmed Password“ (Passwortbestätigung) eingetragen werden, damit dessen Richtigkeit bestätigt werden kann. Bitte klicken Sie auf die Schaltfläche **[Submit]**, um die Einträge für Benutzername und Passwort zu aktualisieren

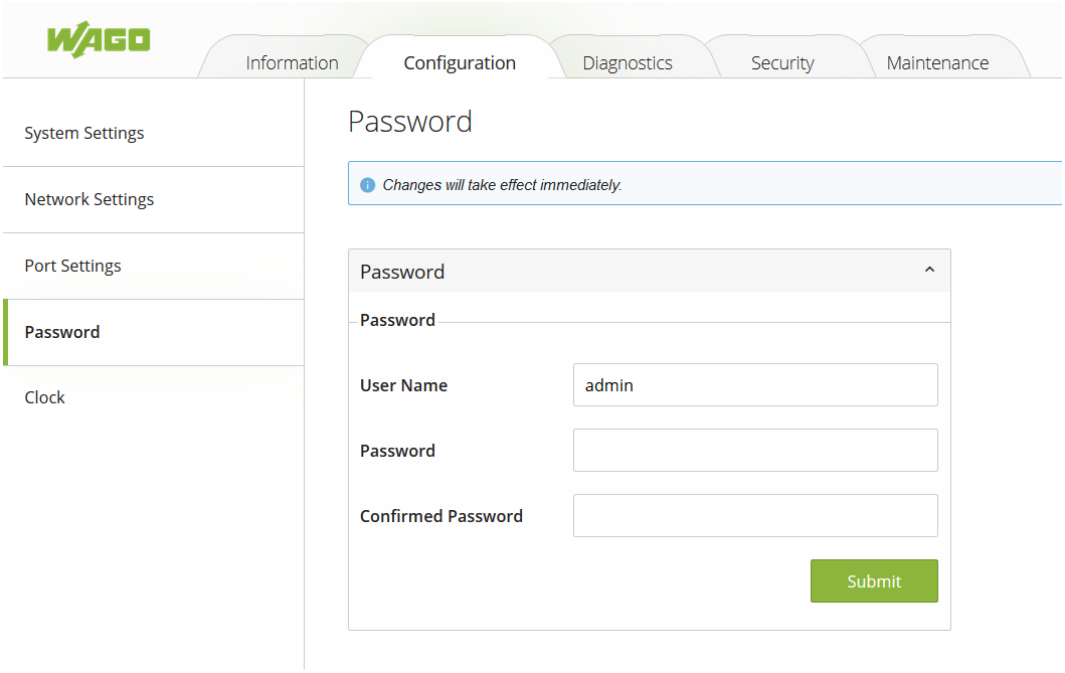

Abbildung 31: WBM-Seite „Konfiguration“ – Registerseite „Passwort“

Die Beschreibungen der einzelnen Parameter und ihrer Default-Werte auf der Registerseite der Passworteinstellungen werden in Tabelle „WBM-Seite „Konfiguration“ – Registerseite „Passwort“ zusammengefasst.

Tabelle 22: WBM- Seite „Konfiguration“ – Registerseite „Passwort“

Parameter	Werkseinstellung	Beschreibung
User Name	admin	Der Benutzername für die Anmeldung darf nicht mehr als 15 Zeichen lang sein.
Password	wago	Das Passwort für die Anmeldung darf nicht mehr als 15 Zeichen lang sein.
Confirmed Password	wago	Hier muss das Passwort erneut eingetragen werden. Es muss identisch mit dem im Feld darüber eingetragenen Passwort sein und darf nicht mehr als 15 Zeichen lang sein.

10.5 Diagnostics (Diagnose)

10.5.1 SNMP

Das SNMP („**S**imple **N**etwork **M**anagement **P**rotocol“) wird in Netzwerkverwaltungssystemen verwendet, um angeschlossene Geräte auf Zustände hin zu überwachen, die die Aufmerksamkeit eines Administrators erfordern. SNMP ist ein Bestandteil der durch die IETF („Internet Engineering Task Force“) definierten „Internet Protocol Suite“ (Internetprotokollfamilie). Es besteht aus einer Reihe von Standards für die Netzwerkverwaltung, einschließlich eines Anwendungsschichtprotokolls, eines Datenbankschemas und einer Reihe von Datenbankobjekten.

SNMP stellt Verwaltungsdaten in Form von Variablen der verwalteten Systeme dar, die die Systemkonfiguration beschreiben. Diese Variablen können daraufhin von Verwaltungsanwendungen abgefragt (und manchmal auch verändert) werden.

Ein „SNMP Community String“ ist ein Textelement, das als Passwort fungiert. Es wird zur Authentifizierung von Nachrichten verwendet, die zwischen der Managementstation (der SNMP-Manager) und einem Gerät (dem SNMP-Agenten) ausgetauscht werden. Dieser String ist in jedem Paket enthalten, das zwischen diesen beiden Punkten übertragen wird.

Die „SNMP Community“ fungiert als Passwort und wird zur Definition der Sicherheitsparameter von SNMP-Clients in SNMPv1- und SNMPv2c-Umgebungen verwendet. Die normale „SNMP Community“ für SNMPv1 und SNMPv2c lautet „public“, solange SNMPv3 nicht aktiviert ist. Ist SNMPv3 aktiviert, müssen die „Communities“ für SNMPv1 und v2c spezifisch sein und können nicht gemeinsam genutzt werden.

Der Industrial-Managed-Switch von WAGO unterstützt SNMP und kann auf dieser Registerseite, wie in Abbildung „WBM-Seite „Diagnose“ – Registerseite „SNMP““ angezeigt, konfiguriert werden. Die SNMP-Einstellung besteht aus folgenden vier Teilen:

- SNMP-Agent
- SNMPv1/v2c-Community
- SNMP-Trap
- SNMPv3-Authentifizierung (Auth.)

Bitte beachten Sie, dass die Einstellung für die „SNMPv1/v2c Community“ in Abbildung „WBM-Seite „Diagnose“ – Registerseite „SNMP““ nicht erscheint, weil sie erst dann angezeigt wird, wenn die Option für die SNMPv1/v2c-Version ausgewählt wurde.

ⓘ Hinweis

Nutzung von SNMPv3

Aus Sicherheitsgründen können Benutzer SNMPv1/v2c nicht dazu nutzen, das Produkt neu zu starten, sicherheitsrelevante Einstellungen zu ändern oder das Passwort des Produktes zu ändern. Diese Änderungen können nur mit SNMPv3 vorgenommen werden.

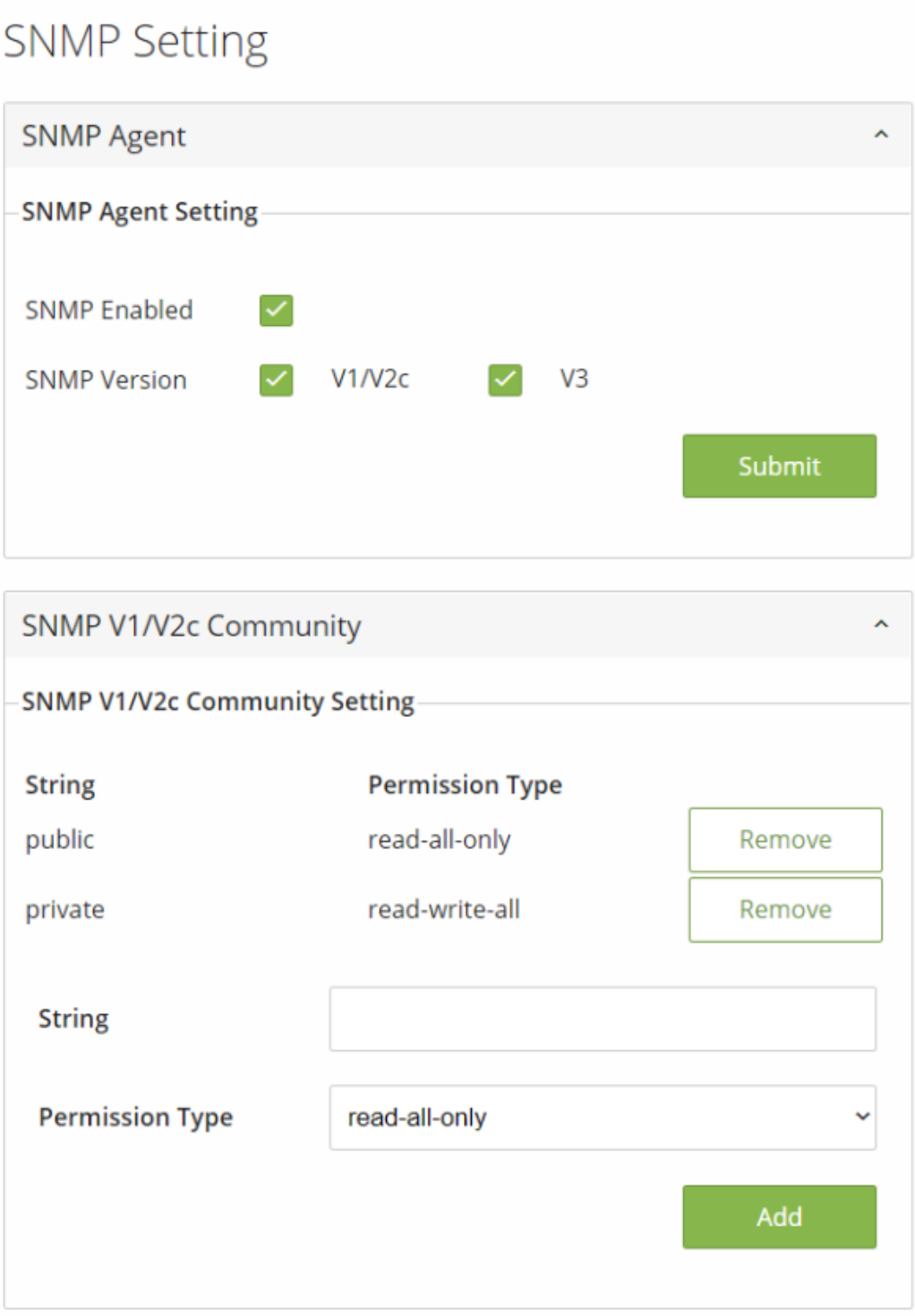

Abbildung 32: WBM-Seite „Diagnose“ – Registerseite „SNMP Setting Teil 1“

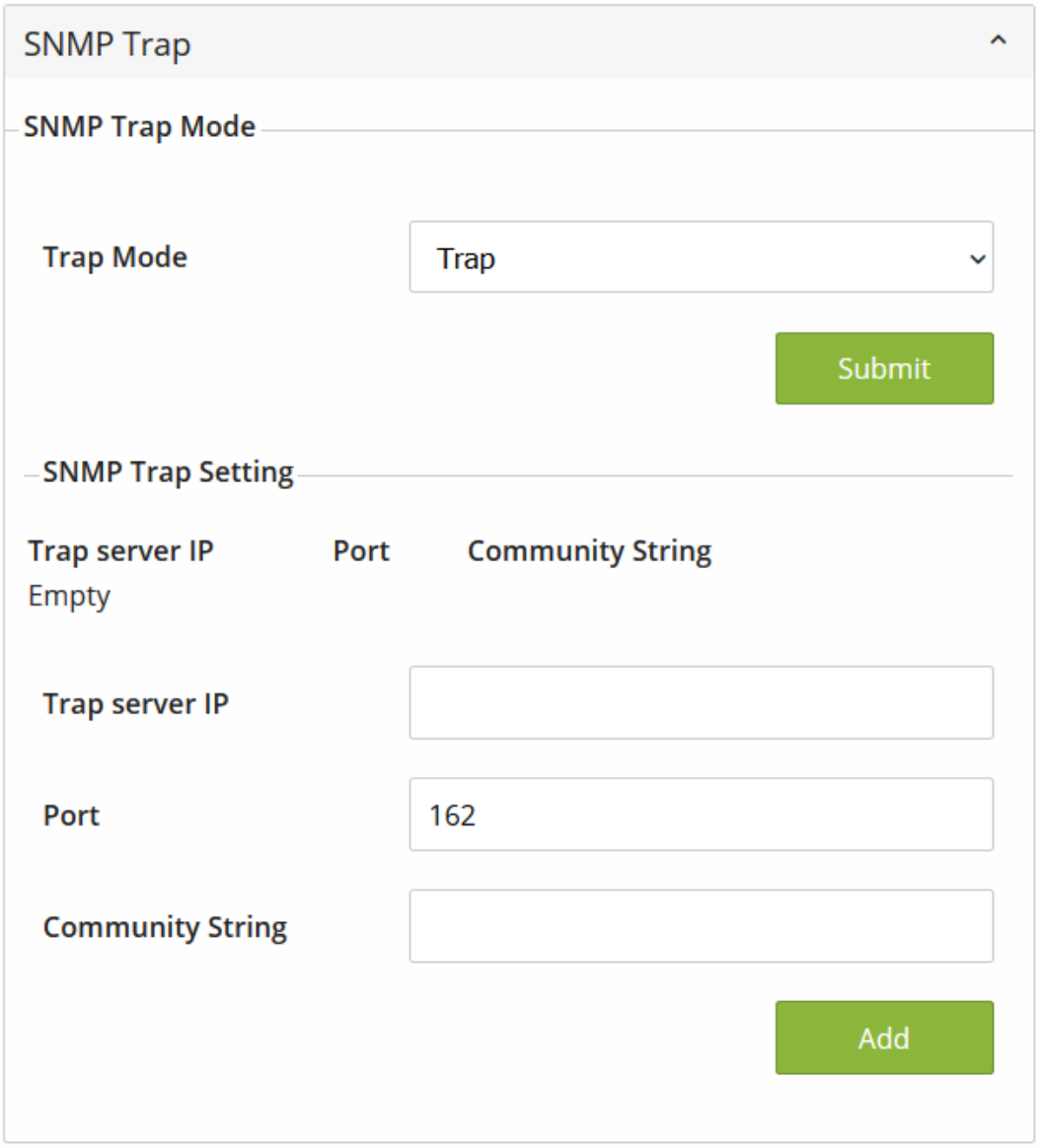

Abbildung 33: WBM-Seite „Diagnose“ – Registerseite „SNMP Setting Teil 2“

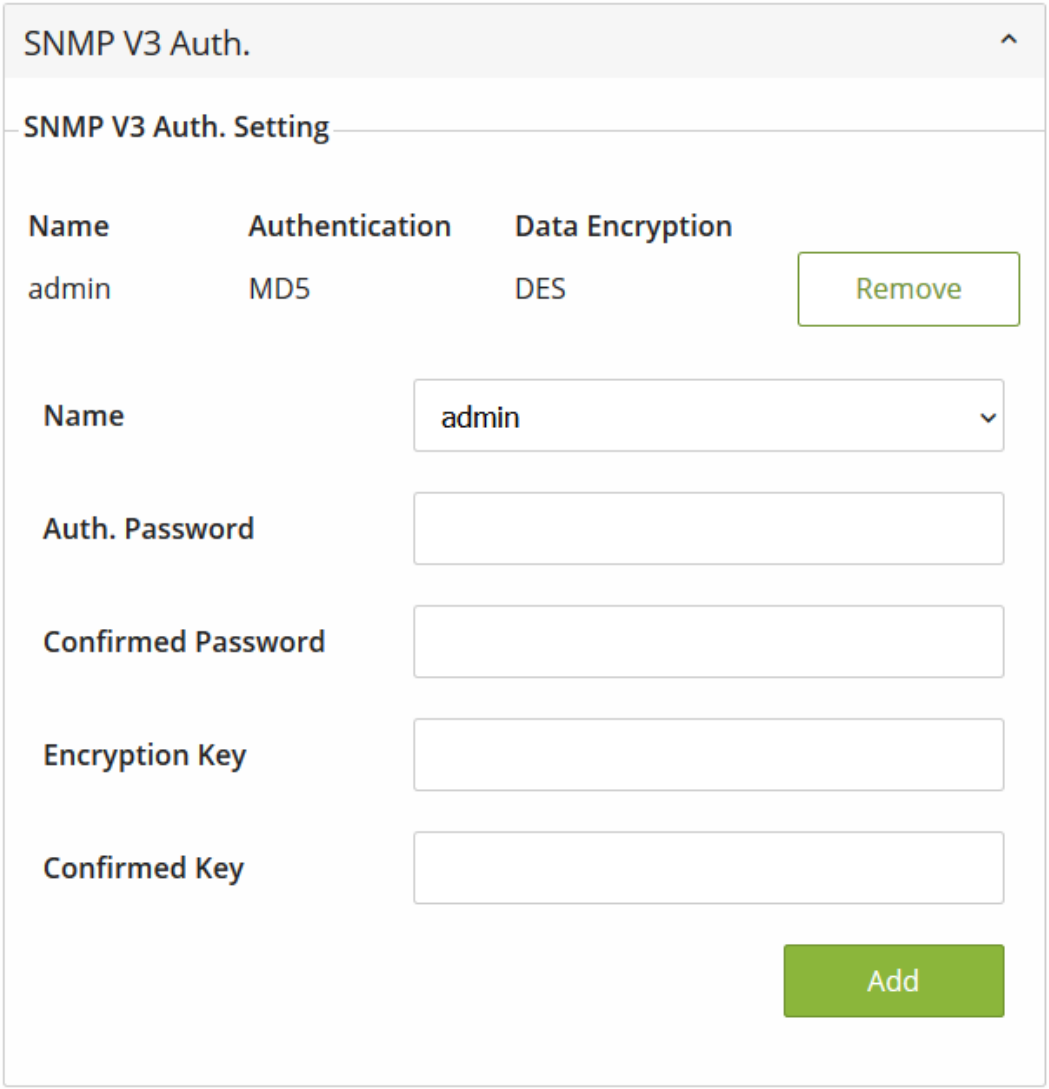

Abbildung 34: WBM-Seite „Diagnose“ – Registerseite „SNMP Setting Teil 3“

10.5.1.1 SNMP Agent (SNMP-Agent)

Aktivieren Sie das Kontrollkästchen „SNMP Enabled“, um den SNMP-Agent auf dem Managed-Switch zu starten, und klicken Sie auf die Schaltfläche **[Submit]**, wie in Abbildung „Einstellungen für den SNMP-Agent“ angezeigt. Die Managed-Switches von WAGO unterstützen SNMP in Version 1 (v1), Version 2c (v2c) und Version 3, wie in Tabelle „WBM-Seite „Diagnose“ – Registerseite „Einstellungen für den SNMP-Agent““ zusammengefasst. SNMPv1 und SNMPv2c nutzen im Grunde ein einfaches, auf „Community Strings“ basierendes Authentifizierungsprotokoll als ihren Sicherheitsmechanismus. SNMPv3 hingegen wird durch kryptografische Sicherheit verbessert. Die Default-Einstellung der SNMP-Version ist v3. Benutzer können die SNMP-Version durch Aktivierung des Kontrollkästchens für v1/v2c und/oder v3 auswählen.

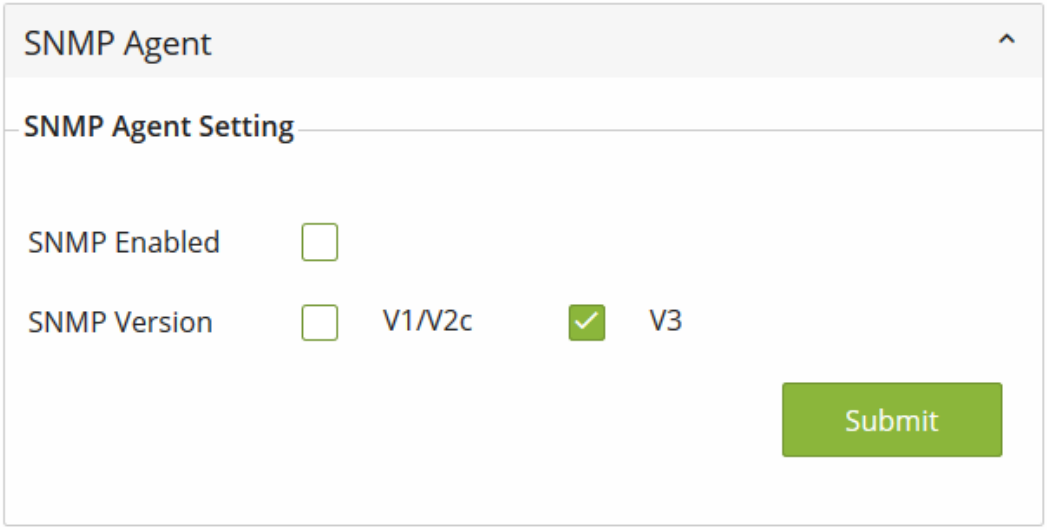

Abbildung 35: Einstellungen für den SNMP-Agent

Tabelle 23: WBM-Seite „Diagnose“ – Registerseite „Einstellungen für den SNMP-Agent“

Parameter	Werkseinstellung	Beschreibung
SNMP Enabled	Deaktiviert	Aktivieren Sie das Kontrollkästchen, um den SNMP-Agent zu aktivieren.
SNMP Version	V3	Aktivieren Sie die gewünschte SNMP-Version (V1/V2c und/oder V3).

10.5.1.2 SNMPv1/v2c-Community (SNMPv1/v2c-Community-String)

SNMPv1 und SNMPv2c verwenden übereinstimmende „Community Strings“ zur Authentifizierung. Diese Authentifizierung ermöglicht der Netzwerkverwaltungssoftware den Zugriff auf Informationen oder Datenobjekte, die durch „Management Information Bases“ (MIBs) auf dem Industrial-Managed-Switch definiert wurden. Bitte beachten Sie, dass diese einfache Authentifizierung als schwacher Sicherheitsmechanismus gilt. Sofern möglich, empfehlen wir die Verwendung von SNMPv3. Im WAGO 852-1322 gibt es zwei Authentifizierungsebenen oder Berechtigungstypen, welche die Berechtigungen „read-all-only“ (alles-nur-lesen-Modus) oder „read-write-all“ (alles-lesen/schreiben-Modus) vergeben. So kann etwa in unserer Default-Einstellung ein SNMP-Agent, wie in Abbildung „Einstellung für die „SNMPv1/v2c Community“ angezeigt, der ein Modul der Netzwerkverwaltungssoftware im Industrial-Managed-Switch darstellt, mit dem String „public“ auf alle Objekte mit der Berechtigung „read-all-only“ zugreifen. Ein weiteres Einstellungsbeispiel wäre der String „private“ mit der Berechtigung „read-write-all“.

Die Einstellung der „SNMPv1/v2c Community“, wie in Abbildung „Einstellung für die „SNMPv1/v2c Community“ angezeigt, ermöglicht Benutzern das Eintragen eines Community-Strings mit einem Berechtigungstyp für das Authentifizieren oder Entfernen eines vorhandenen „Community Strings“ aus der Liste durch einen Klick auf die Schaltfläche **[Remove]** (Entfernen) am Ende jedes „Community String“-Eintrags. Benutzer können einen neuen String-Namen spezifizieren, indem sie im String-Feld einen Text eingeben, und im Drop-down-Menü darunter einen Berechtigungstyp auswählen. Anschließend müssen sie auf die Schaltfläche **[Add]** klicken.

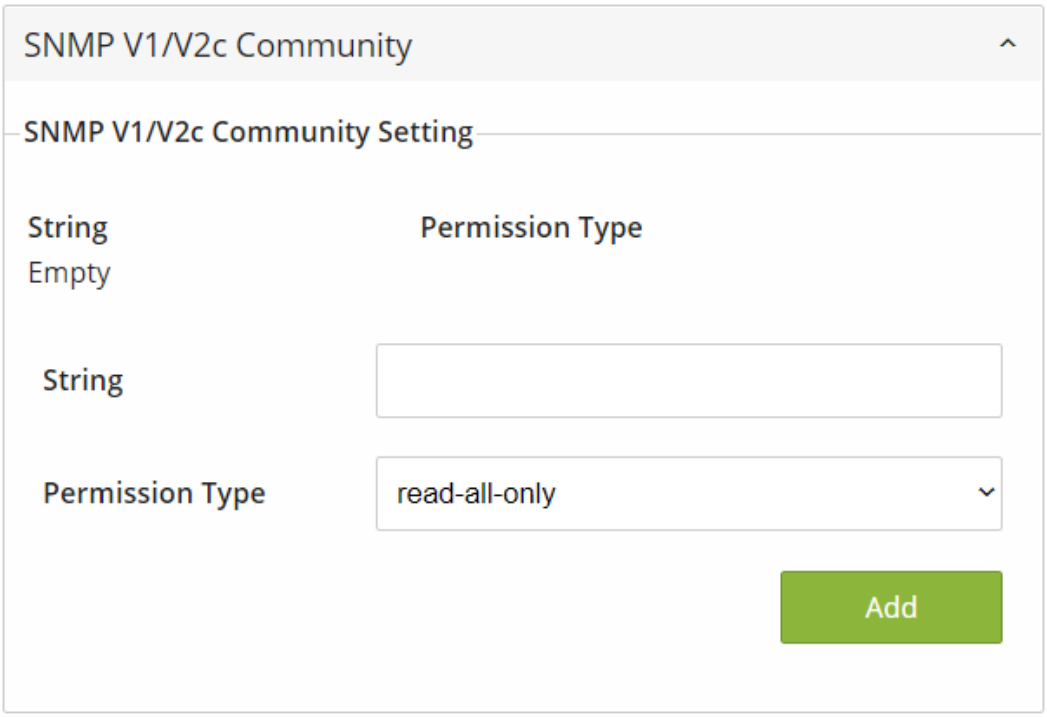

Abbildung 36: Einstellung für die „SNMPv1/v2c Community“

In Tabelle „WBM-Seite „Diagnose“ – Registerseite „Einstellung für die SNMPv1/v2c Community““ finden Sie eine kurze Beschreibung der Einstellungen für den „SNMPv1/v2c Community String“.

Tabelle 24: WBM-Seite „Diagnose“ – Registerseite „Einstellung für die SNMPv1/v2c Community“

Parameter	Werkseinstellung	Beschreibung
(Community) String	Public (read-all-only)	Definiert die Namen der Strings für die Authentifizierung. Der String darf nicht länger als 15 Zeichen sein.
	Private (read-write-all)	
Permission Type	-	Wählen Sie einen Berechtigungstyp aus dem Drop-down-Menü: „read-all-only“ oder „read-write-all“. In den Anmerkungen unten finden Sie eine kurze Erklärung dazu. • Read-all-only: Berechtigung zum Lesen des OID-1-Teilbaums • Read-write-all: Berechtigung zum Lesen und Schreiben des OID-1-Teilbaums

10.5.1.3 SNMP Trap (SNMP-Trap)

Der Industrial-Managed-Switch bietet eine Trap-Funktion, durch die er Nachrichten an Agents mit SNMP-Traps oder SNMP-Informs versenden kann. Die Nachrichten basieren auf Statusänderungen im Switch, wie etwa „Link up“ (verbunden), „Link down“ (nicht verbunden), „warm start“ (Warmstart) und „cold start“ (Kaltstart). Wenn der Switch im Inform-Modus nach dem Senden einer “SNMP Inform Request“ (SNMP-Informationsabfrage) nicht innerhalb von 10 Sekunden eine Antwort empfängt, sendet er die Anfrage erneut. Der Switch wird die Abfrage bis zu drei Mal erneut senden. Abbildung „WBM-Seite „Diagnose“ – Registerseite „SNMP“, Abschnitt „SNMP Trap“ zeigt den Abschnitt „SNMP Trap“.

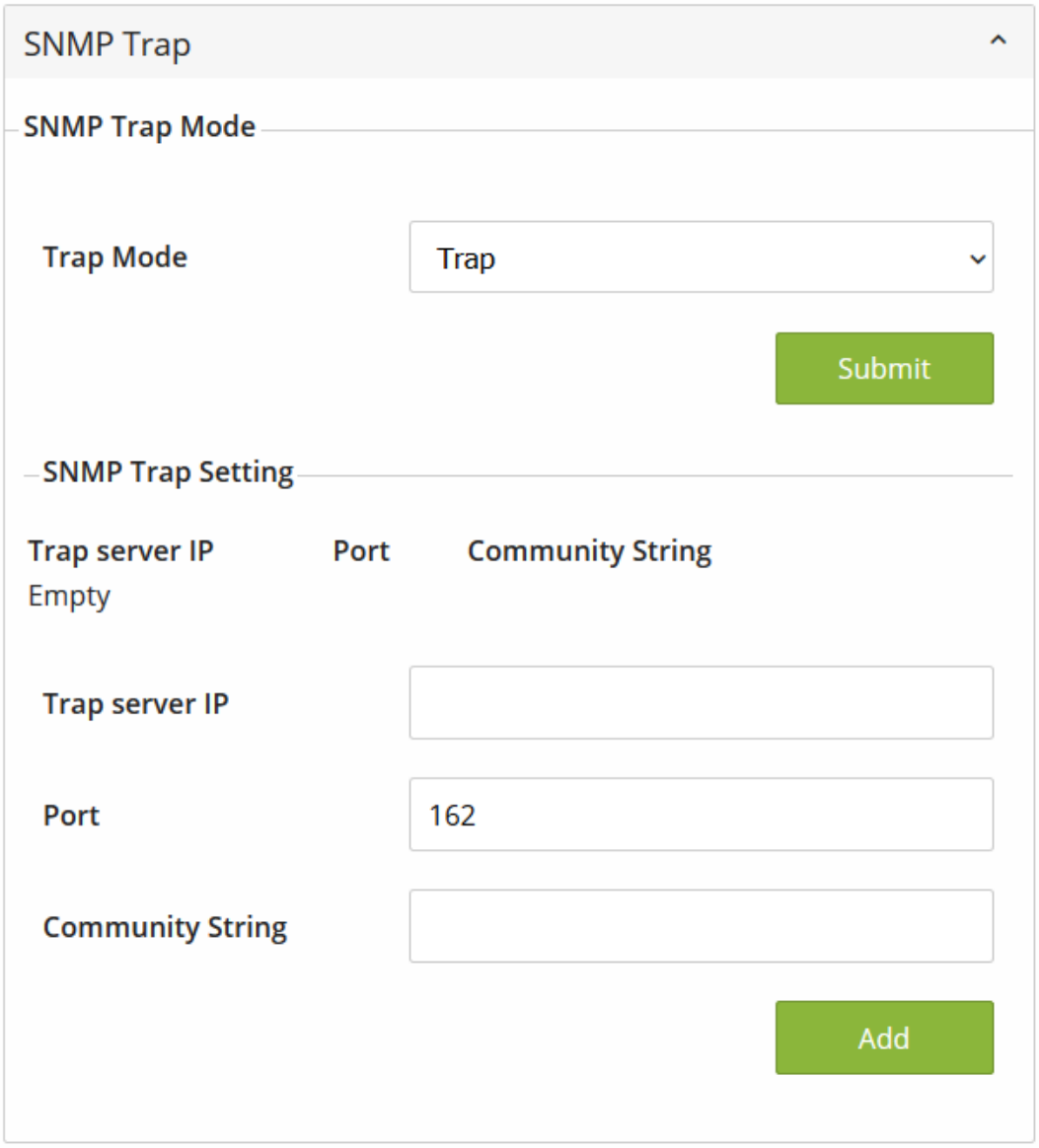

Abbildung 37: WBM-Seite „Diagnose“ – Registerseite „SNMP“, Abschnitt „SNMP Trap“

Der Modus „SNMP Trap“ ermöglicht Benutzern die Konfiguration der Modi „SNMP Trap“ oder „Inform“ über ein Drop-down-Menü, wie in Abbildung „WBM-Seite „Diagnose“ – Registerseite „SNMP“, Abschnitt „SNMP Trap“ angezeigt. Klicken Sie anschließend auf die Schaltfläche **[Submit]**, um den Modus zu ändern. Unter dem Abschnitt „SNMP Trap Setting“ wird eine Liste konfigurierter SNMP-Trap-Server angezeigt. Das Beispiel in Abbildung „WBM-Seite „Diagnose“ – Registerseite „SNMP“, Abschnitt „SNMP Trap“ zeigt eine leere Liste. Benutzer können im Feld „Trap server IP“ eine IP-Adresse sowie im Feld „Port“ eine Port-Nummer für den Trap-Server und im Feld „Community String“ einen String für die Authentifizierung angeben. Klicken Sie bitte nach dem Ausfüllen aller erforderlichen Felder unter „SNMP Trap Setting“ auf die Schaltfläche **[Add]**. Tabelle „WBM-Seite „Diagnose“ – Registerseite „SNMP“, Abschnitt „SNMP Trap“ fasst die Beschreibungen der Parameter unter „SNMP Trap“ zusammen.

Tabelle 25: WBM-Seite „Diagnose“ – Registerseite „SNMP“, Abschnitt „SNMP Trap“

Parameter	Werkseinstellung	Beschreibung
Trap Mode	Trap	Wählen Sie zwischen den Modi „Trap“ und „Inform“.
Trap server IP	Null	Hier geben Sie die IP-Adresse Ihres Trap-Servers ein.

Parameter	Werkseinstellung	Beschreibung
Port	162	Hier geben Sie den Service-Port des Trap-Servers ein.
Community String	Null	Hier geben Sie den „Community String“ für die Authentifizierung ein. Der String darf nicht länger als 15 Zeichen sein.

10.5.1.4 SNMP-V3-Auth. (SNMP-V3-Authentifizierung)

Wie zuvor erwähnt bietet das Protokoll SNMPv3 mehr Sicherheit. In diesem Abschnitt können Benutzer ein Passwort und einen Verschlüsselungscode angeben, um die Datensicherheit zu erhöhen. Bei Auswahl von SNMPv3 können Benutzer die Parameter für die Authentifizierung und Verschlüsselung konfigurieren. Für die Passwortauthentifizierung wird die Funktion MD5 (Message-Digest Algorithm 5) und als Datenverschlüsselungsalgorithmus wird DES (Data Encryption Standard) eingesetzt. Abbildung „WBM-Seite „Diagnose“ – Registerseite „SNMP“, Abschnitt „SNMP V3 Auth.“zeigt die Einstellungsoptionen für die SNMPv3-Authentifizierung (Auth.).

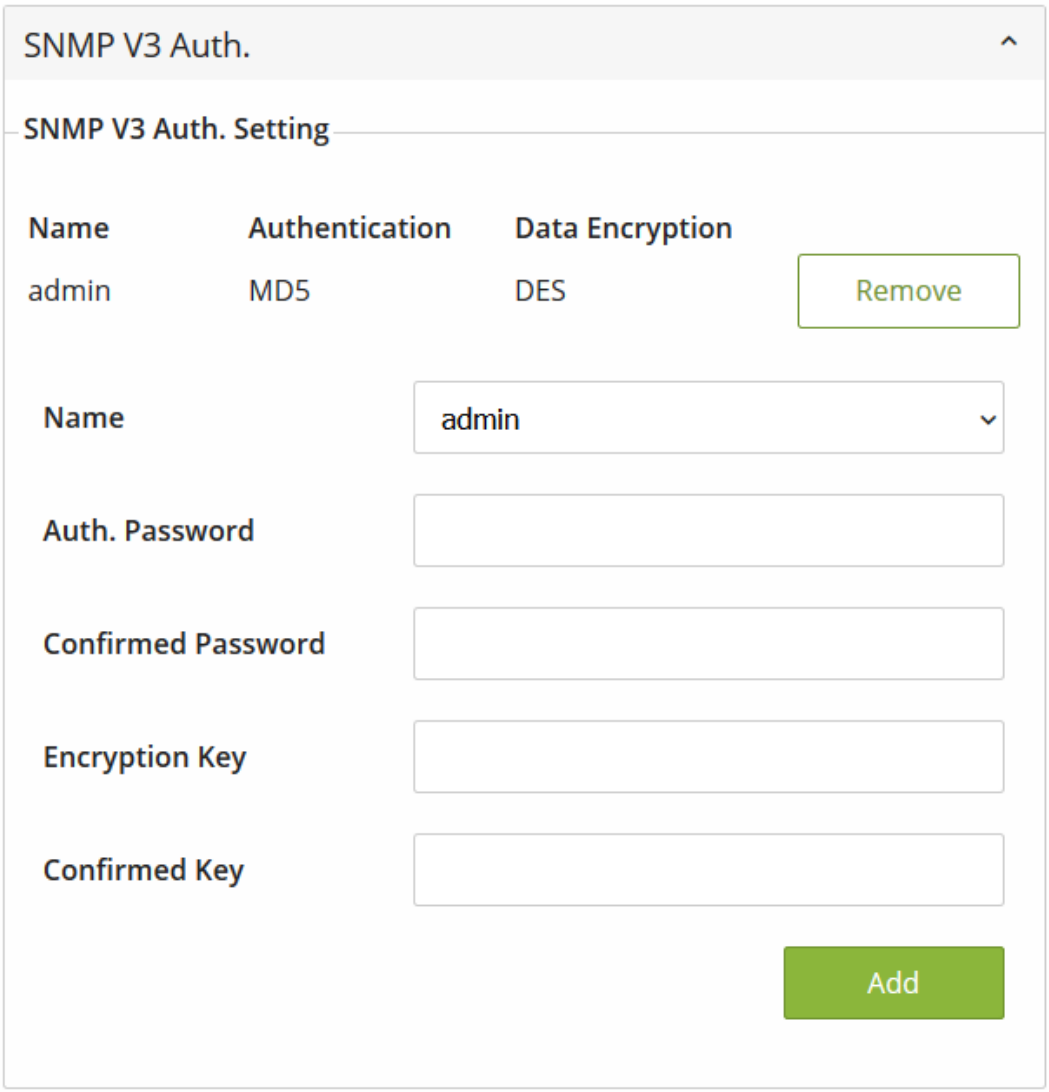

Abbildung 38: WBM-Seite „Diagnose“ – Registerseite „SNMP“, Abschnitt „SNMP V3 Auth.“

Benutzer können im oberen Teil des Abschnitts „SNMP V3 Auth.“ bereits vorhandene SNMPv3-Benutzereinstellungen sehen, wie in Abbildung „WBM-Seite „Diagnose“ – Registerseite „SNMP“, Abschnitt „SNMP V3 Auth.“ angezeigt. In der Liste sind Informationen

zu Benutzername, Authentifizierungstyp und Datenverschlüsselung verfügbar. Benutzer haben die Möglichkeit, vorhandene SNMPv3-Benutzer durch einen Klick auf die Schaltfläche **[Remove]** in der letzten Spaltenjedes Eintrags zu entfernen.

Zum Hinzufügen eines neuen SNMPv3-Benutzers muss ein Benutzername aus dem Drop-down-Menü gewählt werden (entweder „Admin“ oder „User“). Anschließend muss das Authentifizierungspasswort mit einer maximalen Länge von 31 Zeichen sowohl in das Feld „Auth. Password“ als auch in das Feld „Confirmed Password“ eingetragen werden. Bitte beachten Sie, dass bei einem fehlenden Passwort keine Authentifizierung für SNMPv3 erfolgt. Schließlich muss der Verschlüsselungscode mit einer maximalen Länge von 31 Zeichen sowohl in das Feld „Encryption Key“ (Verschlüsselungscode) als auch in das Feld „Confirmed Key“ (Codebestätigung) eingetragen werden. Bitte klicken Sie nach dem Ausfüllen aller erforderlichen Felder auf die Schaltfläche **[Add]**, um die Informationen auf dem Industrial-Managed-Switch zu aktualisieren. In Tabelle „WBM-Seite „Diagnose“ – Registerseite „SNMP“, Abschnitt „SNMP V3 Auth.“ finden Sie die Beschreibungen der SNMPv3-Einstellungen.

Tabelle 26: WBM-Seite „Diagnose“ – Registerseite „SNMP“, Abschnitt „SNMP V3 Auth.“

Parameter	Werkseinstellung	Beschreibung
Name	admin	Wählen Sie eine der folgenden Optionen: Admin: Administrationsebene (Default) User: Normale Benutzerebene
Auth. (Authentication) Password	wago0852	In diesem Feld geben Sie ein Passwort für die Authentifizierung des oben angegebenen Benutzernamens ein. Bitte beachten Sie, dass keine Authentifizierung erfolgt, wenn Sie das Feld leer lassen. Das Passwort für die Authentifizierung basiert auf MD5 und darf nicht länger als 31 Zeichen sein.
Confirmed Password	wago0852	Bestätigen Sie das Passwort für die Authentifizierung durch die erneute Eingabe.
Encryption Key	wago0852	Geben Sie einen Verschlüsselungscode ein, um die Sicherheit der SNMP-Kommunikation zu erhöhen. Ver Verschlüsselungsalgorithmus basiert auf DES und der Code darf nicht länger als 31 Zeichen sein.
Confirmed Key	wago0852	Bestätigen Sie den Verschlüsselungscode durch die erneute Eingabe.

10.5.2 Modbus TCP

Der Industrial-Managed-Switch von WAGO kann über das Modbus-TCP/IP-Protokoll mit einem Modbus-Netzwerk verbunden werden. Dies ist ein industrielles Netzwerkprotokoll zur Steuerung automatisierter Anlagen. Mit dem Modbus-TCP/IP-Protokoll, dessen Funktion dem Browser der „Management Information Base“ (MIB) ähnelt, können Status und Einstellungen des Switches ausgelesen werden. Hierbei fungiert der Switch als Modbus-Slave, der von einem Modbus-Master dezentral konfiguriert werden kann. Die für den Modbus-Slave eingetragene Adresse muss mit den Einstellungen im Modbus-Master übereinstimmen. Für den Zugriff auf den Switch muss, wie in diesem Unterabschnitt beschrieben, eine Modbus-Adresse zugewiesen werden. Im Anhang unter „Modbus-Speicherbelegung“ befindet sich eine Modbus-Speicherzuordnungstabelle, in der alle Adressen der Register innerhalb des Switches und ihre Beschreibungen aufgelistet sind. Abbildung „WBM-Seite „Diagnose“ – Registerseite „Modbus TCP“ zeigt die Registerseite „Modbus TCP“.

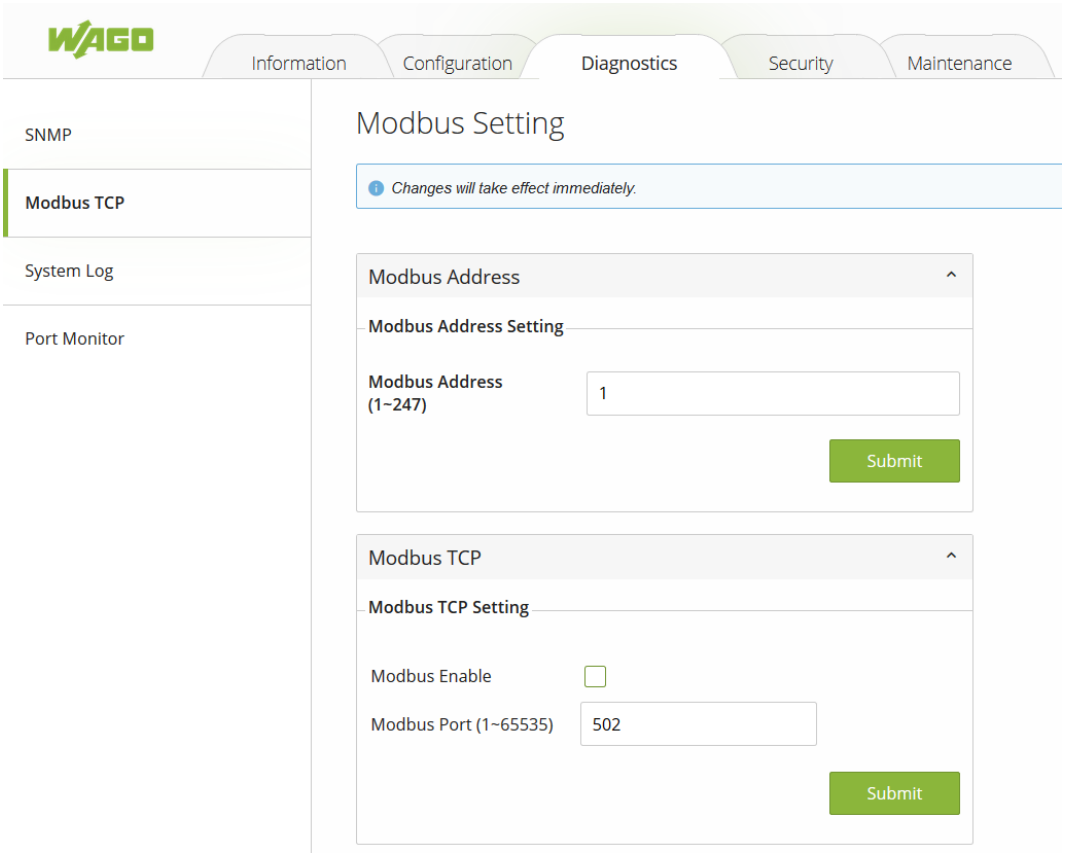

Abbildung 39: WBM-Seite „Diagnose“ – Registerseite „Modbus TCP“

Zur Vergabe einer Modbus-Adresse für den Industrial-Managed-Switch wählen Sie eine Nummer zwischen 1 und 247 und tragen Sie sie in das Feld „Modbus Address“ ein. Klicken Sie auf die Schaltfläche **[Submit]**, um sie zu konfigurieren. Zur Aktivierung des Modbus-Protokolls im Industrial-Managed-Switch aktivieren Sie das Kontrollkästchen neben „Modbus Enable“ (Modbus aktivieren) und tragen unter „Modbus Port“ eine Nummer zwischen 1 und 65535 für den Modbus-Port ein. Klicken Sie auf die Schaltfläche **[Submit]**, um „Modbus TCP“ zu aktivieren. Tabelle „WBM-Seite „Diagnose“ – Registerseite „Modbus TCP“ fasst die Beschreibungen der Parameter unter „Modbus TCP“ zusammen.

Die Modbus-Speicherbelegung finden Sie im Anhang (siehe Kapitel **Modbus-Register [▶ 87]**).

Tabelle 27: WBM-Seite „Diagnose“ – Registerseite „Modbus TCP“

Parameter	Werkseinstellung	Beschreibung
Modbus Address	1	Tragen Sie eine Nummer zwischen 1 und 247 ein, um eine Modbus-Adresse für den Industrial-Managed-Switch zu konfigurieren.
Modbus Enable	Deaktiviert	Aktivieren Sie das Kontrollkästchen neben „Modbus Enable“, um das Modbus-Protokoll im Industrial-Managed-Switch zu aktivieren.
Modbus Port	502	Tragen Sie eine Nummer zwischen 1 und 65535 ein, um die Nummer des Modbus-Service-Ports für den Industrial-Managed-Switch zu konfigurieren.

10.5.3 System-Log (System-Log)

10.5.3.1 Setting (Einstellung)

Unter der Registerseite „System Log > Setting“, wie in Abbildung „WBM-Seite „Diagnose“ – Registerseite „System Log“ – Abschnitt „Setting“ angezeigt, können Benutzer konfigurieren, wie das System-Log (syslog) gespeichert und/oder zu einem anderen System übertragen wird. Das Syslog kann im Flash-Speicher des Industrial-Managed-Switches gespeichert und/oder an einen dezentralen Log-Server übertragen werden. Dazu müssen Benutzer ein „Log Level“ (Protokollebene) wählen sowie die IP-Adresse eines dezentralen Log-Servers angeben und den Service-Port für den Log-Server eintragen. Bitte klicken Sie nach Abschluss aller Einstellungen auf die Schaltfläche **[Submit]**. Tabelle „WBM-Seite „Diagnose“ – Registerseite „System Log“ – Abschnitt „Setting“ fasst die Beschreibungen der Parameter unter „Syslog Settings“ zusammen.

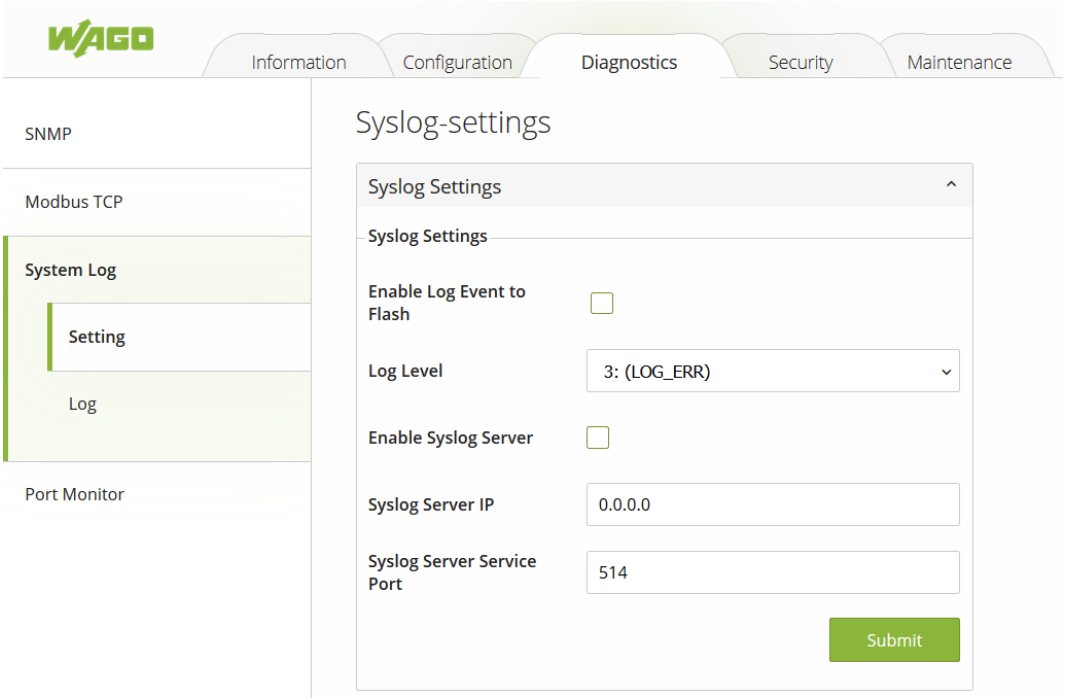

Abbildung 40: WBM-Seite „Diagnose“ – Registerseite „System Log“ – Abschnitt „Setting“

Tabelle 28: WBM-Seite „Diagnose“ – Registerseite „System Log“ – Abschnitt „Setting“

Parameter	Werkseinstellung	Beschreibung
Enable Log Event to Flash	Deaktiviert	**Aktiviert:** Speichert Log-Ereignisse im Flash-Speicher. Der Flash-Speicher behält die Log-Ereignisdateien, auch wenn der Switch neu gestartet wird. **Deaktiviert:** Speichert Log-Ereignisse im RAM-Speicher. Bei jedem Neustart des Switches gehen die Log-Ereignisdateien im Ram-Speicher verloren.
Log Level (Protokollebene)	3(:LOG_ERR)	Bestimmen Sie über das „Log Level“, welche Ereignisse auf der nächsten Webseite (Log) angezeigt werden sollen. Das schließt die Ebenenauswahl mit ein. Wählen Sie z. B. 3 (:Log_ERR), schließt das die Log-Ebenen 0, 1, 2 und 3 mit ein. Bereich: von Log 0 bis Log 7.
Enable Syslog Server	Deaktiviert	**Aktiviert:** Der Syslog-Server wird aktiviert. **Deaktiviert:** Der Syslog-Server wird deaktiviert. Bei Aktivierung werden alle Log-Ereignisse an den dezentralen System-Log-Server übertragen.

Parameter	Werkseinstellung	Beschreibung
Syslog Server IP	0.0.0.0	In diesem Feld tragen Sie die IP-Adresse des Syslog-Servers ein.
Syslog Server Service Port	514	In diesem Feld tragen Sie die Nummer des Service-Ports für den Syslog-Server ein. Bereich: von Port 1 bis Port 65535.

10.5.3.2 Log

Im Abschnitt „Log“ unter der Registerseite „System Log“ können, wie in Abbildung „WBM-Seite „System Log“ dargestellt, die Log-Informationen angezeigt werden. Sie basieren auf dem „Log Level“, das in der Registerseite „System Log Setting“ konfiguriert ist (vorangegangener Unterabschnitt). Benutzer haben die Wahl zwischen „Read all notifications“ (sich alle Log-Einträge anzeigen lassen) und „Read only the last n“ (sich nur die letzten n Log-Einträge anzeigen lassen). Klicken Sie auf das entsprechende Kontrollfeld, um die gewünschte Option auszuwählen.

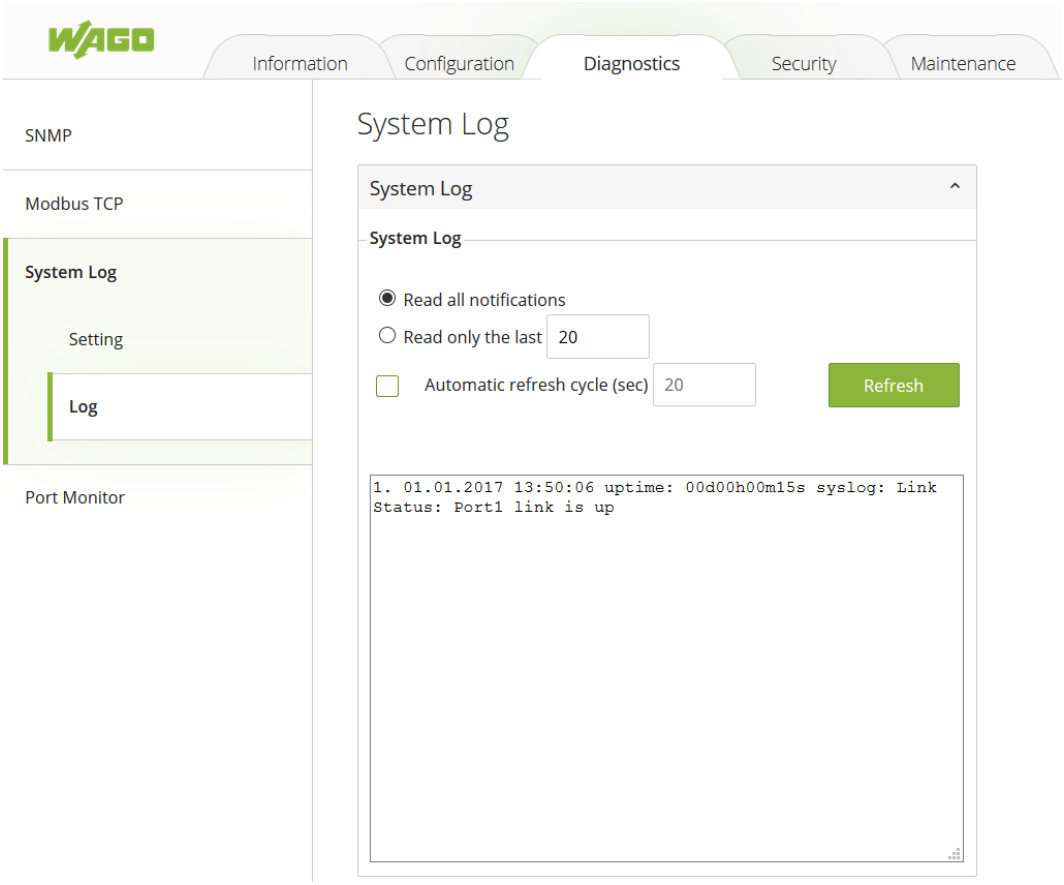

Abbildung 41: WBM-Seite „Diagnose“ – Registerseite „System Log“ – Abschnitt „Log“

Um die Anzeige zu aktualisieren oder die zyklische Aktualisierung zu aktivieren, klicken Sie auf die Schaltfläche **[Refresh]** (Aktualisieren). Die Schaltfläche **[Refresh]** ist nur sichtbar, wenn die zyklische Aktualisierung nicht eingeschaltet oder gestoppt ist. Um die zyklische Aktualisierung zu aktivieren, klicken Sie auf die Schaltfläche **[Start]**. Die Schaltfläche **[Start]** ist nur sichtbar, wenn das Kontrollkästchen bei „Automatic refresh cycle“ (automatische zyklische Aktualisierung) aktiviert ist und die Aktualisierung noch nicht gestartet wurde, wie in Abbildung „Die Schaltfläche **[Start]** ist sichtbar, wenn das Kontrollkästchen bei „Automatic refresh cycle“ aktiviert ist.“ angezeigt. Um die zyklische Aktualisierung wieder zu beenden, klicken Sie auf die Schaltfläche **[Stop]**. Die Schaltfläche **[Stop]** ist nur sichtbar, wenn die zyklische Aktualisierung aktiv ist. Benutzer können durch

Eingabe in das entsprechende Feld die Dauer der zyklischen Aktualisierung in Sekunden angeben. Bitte beachten Sie, dass die Log-Einträge nach Datum und Uhrzeit sortiert sind. Tabelle „WBM-Seite „Diagnose“ – Registerseite „System Log“ – Abschnitt „Log“ fasst die Beschreibungen der Parameter unter dem Abschnitt „Log“ zusammen. Tabelle „Beschreibung der Log-Ereignisse“ zeigt Beschreibungen eines Log-Ereignisses.

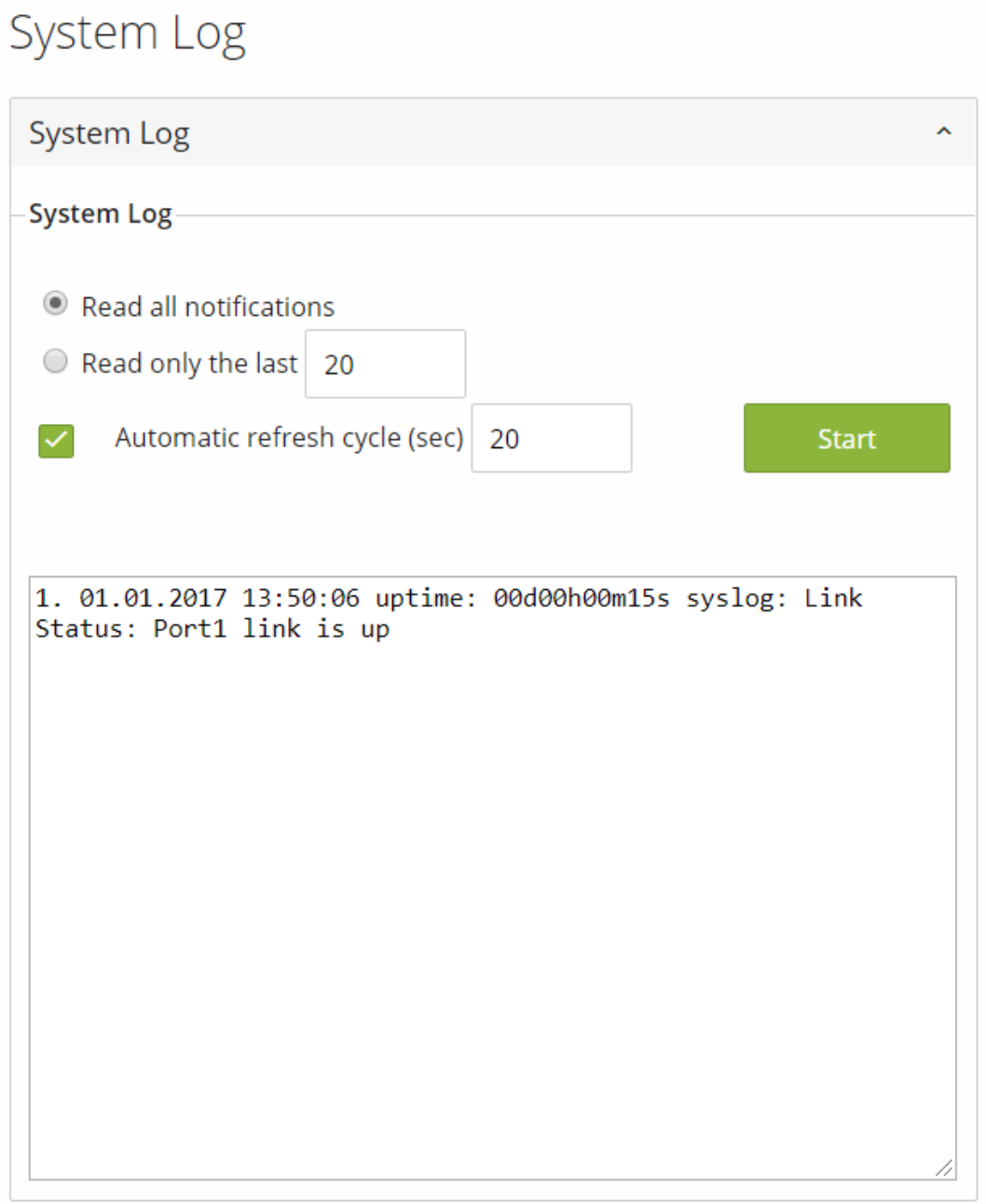

Abbildung 42: Die Schaltfläche [Start] ist sichtbar, wenn das Kontrollkästchen bei „Automatic refresh cycle“ aktiviert ist.

Tabelle 29: WBM-Seite „Diagnose“ – Registerseite „System Log“ – Abschnitt „Log“

Parameter	Werkseinstellung	Beschreibung
Read all notifications	Ausgewählt	Hier aktivieren Sie die Anzeige aller Log-Einträge.
Read only the last n	20	Hier aktivieren Sie die Anzeige der letzten n Log-Einträge. Benutzer können auch die Anzahl der angezeigten Einträge spezifizieren.

Parameter	Werkseinstellung	Beschreibung
Automatic refresh cycle (sec)	Deaktiviert, 20	Aktivieren Sie das Kontrollkästchen, um die zyklische Aktualisierung einzuschalten. Geben Sie die Zykluszeit in Sekunden ein, mit der eine zyklische Aktualisierung durchgeführt werden soll. Abhängig vom gewählten Status wechselt die Beschriftung der Schaltfläche („Refresh“/„Start“/„Stop“).

Tabelle 30: Beschreibung der Log-Ereignisse

Parameter	Beschreibung
Index	Zeigt den Index eines bestimmten Log-Ereignisses an.
Date	Zeigt das Systemdatum des eingetretenen Log-Ereignisses an.
Time	Zeigt die Uhrzeit an, zu der das Log-Ereignis eingetreten ist.
Startup Time	Zeigt an, wie lange das System (der Industrial-Managed-Switch) seit dem Eintreten des Log-Ereignisses bereits in Betrieb ist.
Event	Zeigt eine Beschreibung des Log-Ereignisses.

10.5.4 Port Monitor (Port-Überwachung)

Abbildung „WBM-Seite „Diagnose“ – Registerseite „Port Monitor““ zeigt die Registerseite „Port Monitor“ (Port-Überwachung). Auf dieser Seite wird der tatsächliche Verbindungsstatus für alle verfügbaren Ports des Industrial-Managed-Switch von WAGO abgebildet. Benutzer können anhand des Status erkennen, ob ein Port verbunden („Link Up“/grün), nicht verbunden („Link Down“/gelb) oder deaktiviert ist (schwarz). Tabelle „WBM-Seite „Diagnose“ – Registerseite „Port Monitor“ fasst die Beschreibungen der Legende für den Port-Status zusammen.

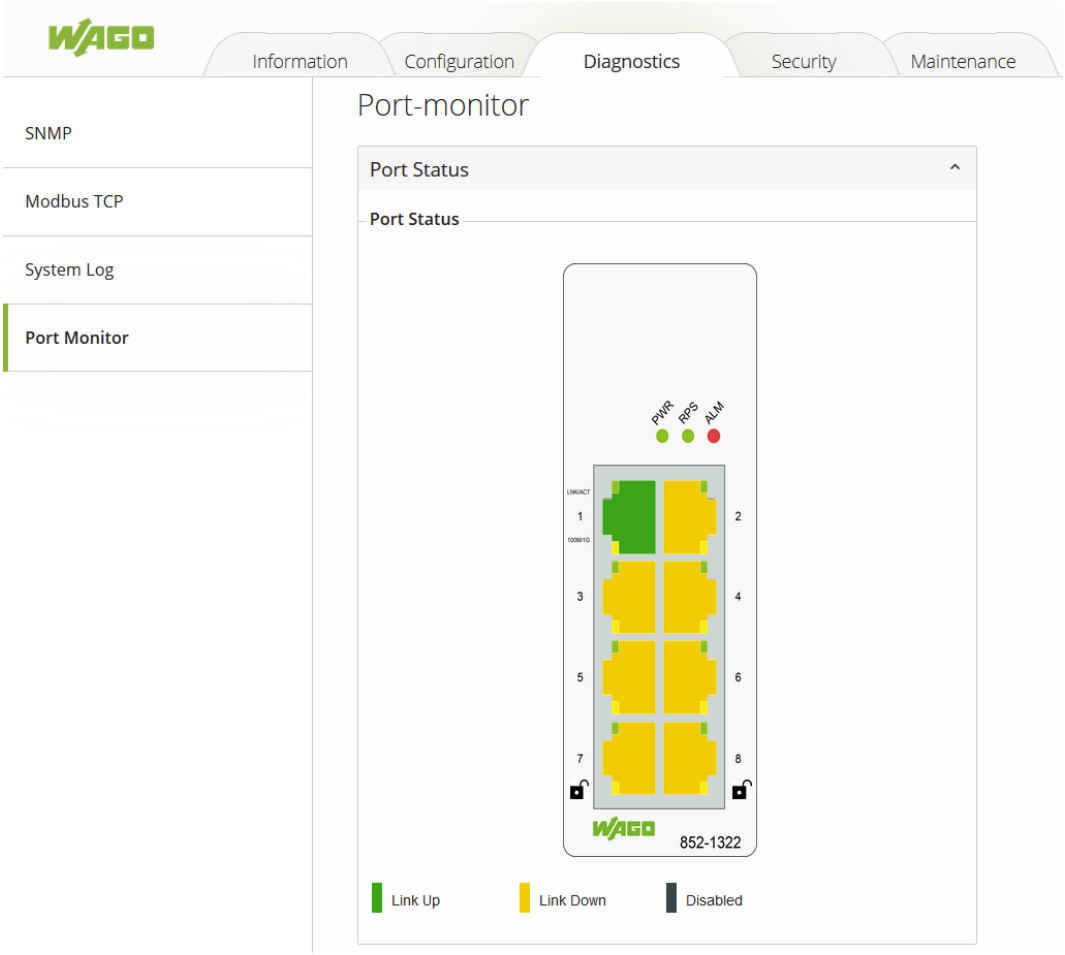

Abbildung 43: WBM-Seite „Diagnose“ – Registerseite „Port Monitor“

Tabelle 31: WBM-Seite „Diagnose“ – Registerseite „Port Monitor“

Parameter	Beschreibung
Port	Zeigt den Port-Namen an: Port 1 bis Port 8.
Verbindungsstatus	**Grün:** zeigt einen verbundenen Kupfer-Port an **Gelb:** zeigt einen nicht verbundenen Port an **Schwarz:** zeigt einen deaktivierten Port an.
sperren	Ist das Schloss geschlossen, ist der Port verschlüsselt.

10.6 Security (Sicherheit)

10.6.1 Static SAK (Einstellungen für statischen SAK)

Abbildung „WBM-Seite „Security“ – Registerseite „Static SAK“ zeigt die Registerseite für Einstellungen des „Static Secure Association Key“ (SAK). Bitte beachten Sie, dass WAGO 852-1322 auf Port 7 und 8 das MACSec-Protokoll unterstützen. Zur Aktivierung einer „Secure Association“ (Sicherheitsverbindung) an einem oder beiden Ports des Industrial-Managed-Switch müssen Sie zunächst aus dem Drop-down-Menü unter „Ports“ einen der zwei Ports auswählen. Aktivieren Sie anschließend das Kontrollkästchen neben „Enabled“. Tragen Sie dann den „Secure Channel Identifier“ (SCI, Sicherheitskanalkennung) mit einer 16-stelligen Hexadezimalzahl (z. B. 0,1,2,…,a,b,c,d,e,f) und den „Secure

Association Key“ (SAK, Sicherheitsverbindungsschlüssel) mit einer 32-stelligen Hexadezimalzahl ein. Klicken Sie schließlich auf die Schaltfläche **[Submit]**, um die Einstellungen für einen der Ports in die Tabelle „Static SAK Status“ im unteren Bereich zu übertragen.

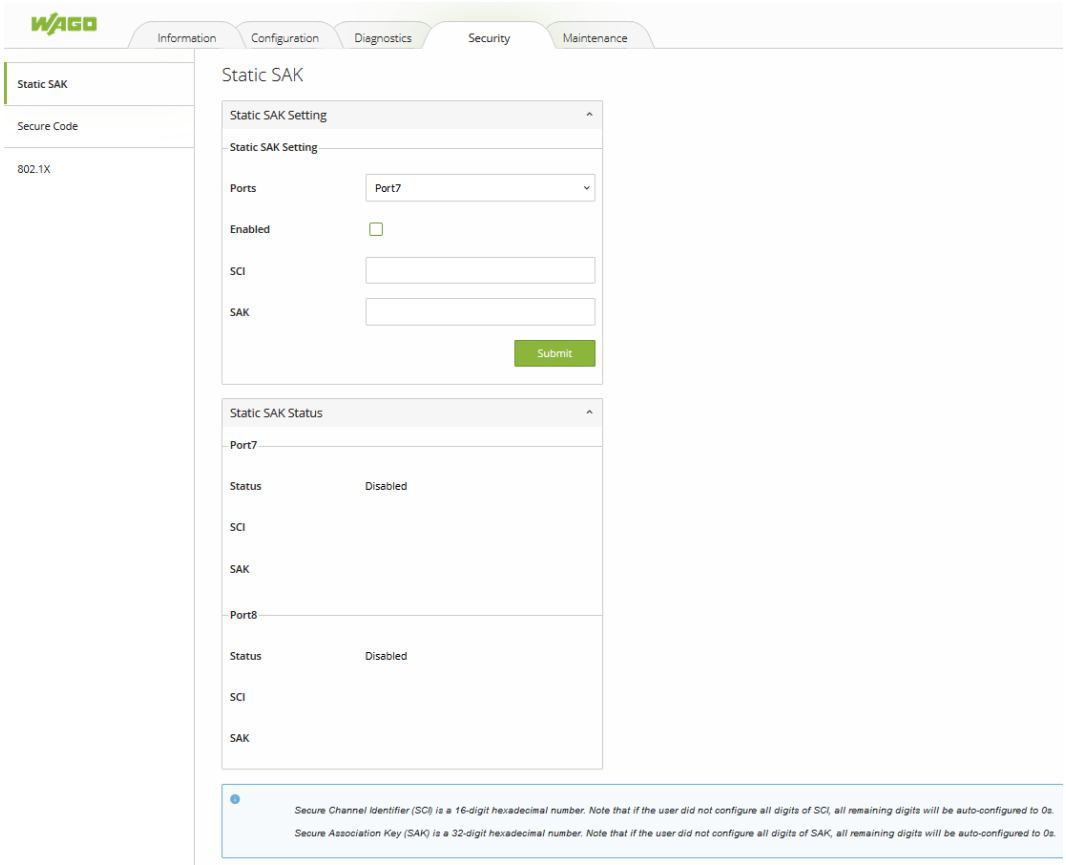

Abbildung 44: WBM-Seite „Security“ – Registerseite „Static SAK“

Der bzw. die ausgewählten Ports werden den vergebenen statischen SAK als Sicherheitsschlüssel zur Absicherung des gesamten Datenverkehrs nutzen. Wenn zwei beliebige Switches über denselben SCI und SAK verfügen, können sie sicher miteinander kommunizieren. Sollte ein nicht abgesicherter Verkehr einen falschen SCI und SAK nutzen, wird der Verkehr durch den Eingangsport des Switches verworfen. Tabelle „WBM-Seite „Security“ – Registerseite „Static SAK“ fasst die Beschreibungen der Einstellungen für den statischen SAK zusammen.

Wenn Sie die Einstellung für den statischen SAK für einen oder beide Ports deaktivieren möchten, wählen Sie einfach einen oder beide Ports aus dem Drop-down-Menü aus und deaktivieren Sie das Kontrollkästchen neben „Enabled“. Klicken Sie anschließend auf die Schaltfläche **[Submit]**. Dadurch wird der Status der Einstellungen in die Tabelle „Static SAK Status“ im unteren Bereich von Abbildung „WBM-Seite „Security“ – Registerseite „Static SAK“ übertragen

Tabelle 32: WBM-Seite „Security“ – Registerseite „Static SAK“

Parameter	Werkseinstellung	Beschreibung
Ports	Option	Wählen Sie einen Port aus dem Drop-down-Menü aus, den Sie konfigurieren möchten.
Enabled	Deaktiviert	Aktivieren Sie das Kontrollkästchen, um den Modus „Static Secure Association Key (SAK) des MACSec für den oder die ausgewählten Ports am Switch zu aktivieren.

Parameter	Werkseinstellung	Beschreibung
SCI	0	Der „Secure Channel Identifier“ (SCI) ist eine 16-stellige Hexadezimalzahl. Bitte beachten Sie, dass bei einer unvollständigen Eingabe der SCI-Zahl alle fehlenden Stellen automatisch mit „0“ konfiguriert werden.
SAK	0	Der „Secure Association Key“ (SAK) ist eine 32-stellige Hexadezimalzahl. Bitte beachten Sie, dass bei einer unvollständigen Eingabe der SAK-Zahl alle fehlenden Stellen automatisch mit „0“ konfiguriert werden.

10.6.2 Secure Code (Sicherheitscode)

Jeder Industrial-Managed-Switch von WAGO verfügt über acht Sicherheitscodes. Jeder Code besteht aus drei Zeichen. Die Sicherheitscodes sind bei jedem Switch einzigartig. Abbildung „Beispiel für Sicherheitscodes“ zeigt ein Beispiel für einen Sicherheitscode. Der Code kann für die Anmeldung im Industrial-Managed-Switch verwendet werden, wenn Benutzer das Passwort vergessen und im Anmeldedialog auf die Schaltfläche **[Forget it]** geklickt haben.

Die Verwendung der Sicherheitskarte wird vom Produkt standardmäßig aktiviert.

Deaktivieren Sie das Kontrollkästchen neben „Enabled“, um den Sicherheitscodemechanismus abzuschalten, und klicken Sie auf die Schaltfläche **[Submit]**, wie in Abbildung „WBM-Seite „Security“ – Registerseite „Sicherheitscode“ angezeigt. Mehr Informationen zur WAGO-Anmeldung finden Sie im Kapitel „Anmeldefehler.

Abbildung 45: Beispiel für Sicherheitscodes

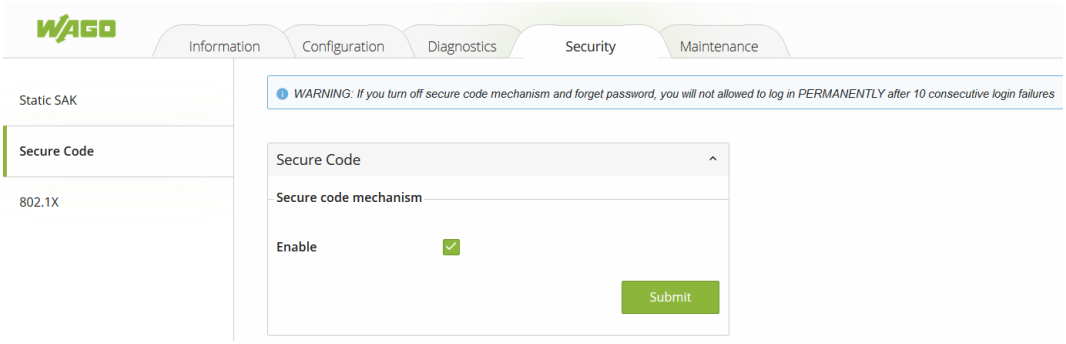

Abbildung 46: WBM-Seite „Security“ – Registerseite „Sicherheitscode“

10.6.3 802.1X (IEEE 802.1X)

Die Registerseite „802.1X“ unter „Security“ ist, wie unten angezeigt, in folgende drei Unterregister aufgeteilt: Einstellungen, Parametereinstellungen und Port-Einstellungen.

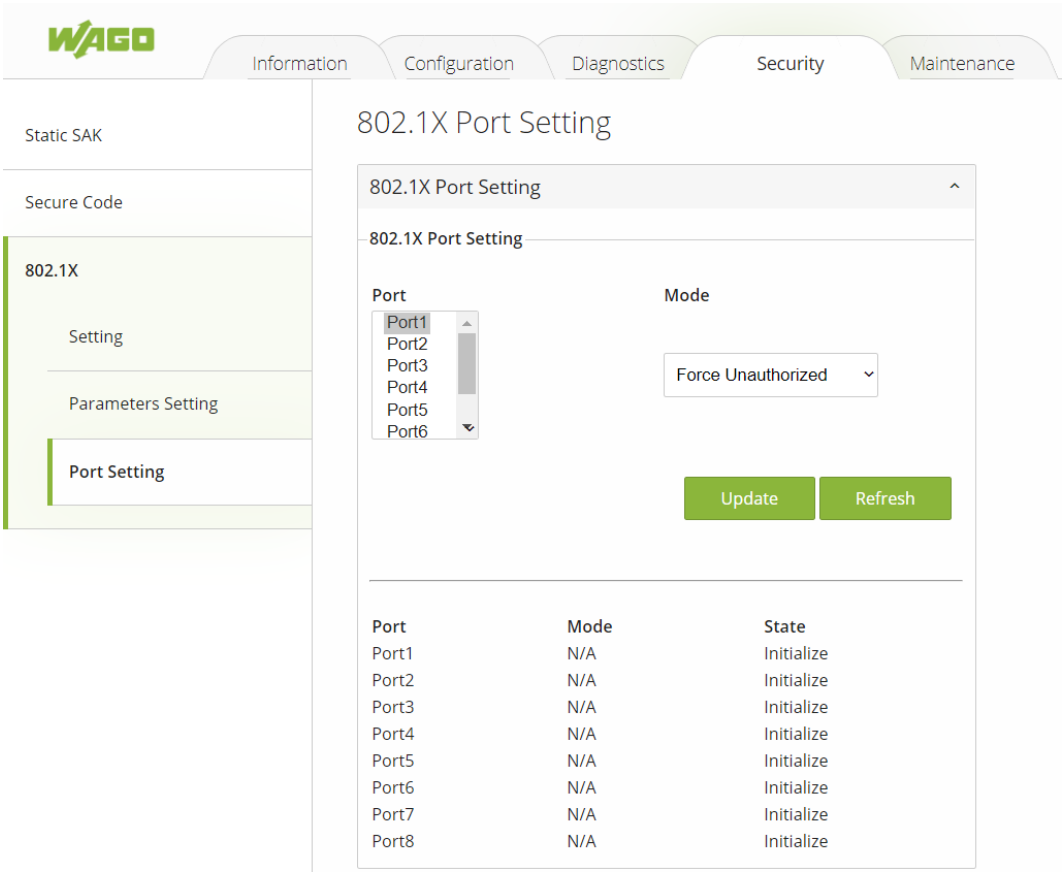

Abbildung 47: WBM-Seite „Security“ – Registerseite „802.1X“

10.6.3.1 Setting (IEEE 802.1X-Einstellungen)

Auf dieser Registerseite kann der Sicherheitsmechanismus 802.1X aktiviert werden, wie in Abbildung „WBM-Seite „Security“ – Registerseite „802.1X“ – Abschnitt „Einstellungen“ angezeigt. Wenn Benutzer das Kontrollkästchen neben „Enabled“ aktivieren, werden die restlichen Optionsfelder verfügbar. Anschließend können Benutzer alle erforderlichen Felder in den 802.1X-Einstellungen konfigurieren, wie etwa IP-Adresse, Port-Nummer und Accounting-Port-Nummer des RADIUS-Servers, NAS-Identifier und Shared-Key. Eine Zusammenfassung der Optionen für die 802.1X-Einstellungen finden Sie in Tabelle „WBM-Seite „Security“ – Registerseite „802.1X“ – Abschnitt „Einstellungen“. Klicken Sie nach dem Ausfüllen aller erforderlichen Felder auf die Schaltfläche **[Update]**, um die Einstellungen zu aktualisieren

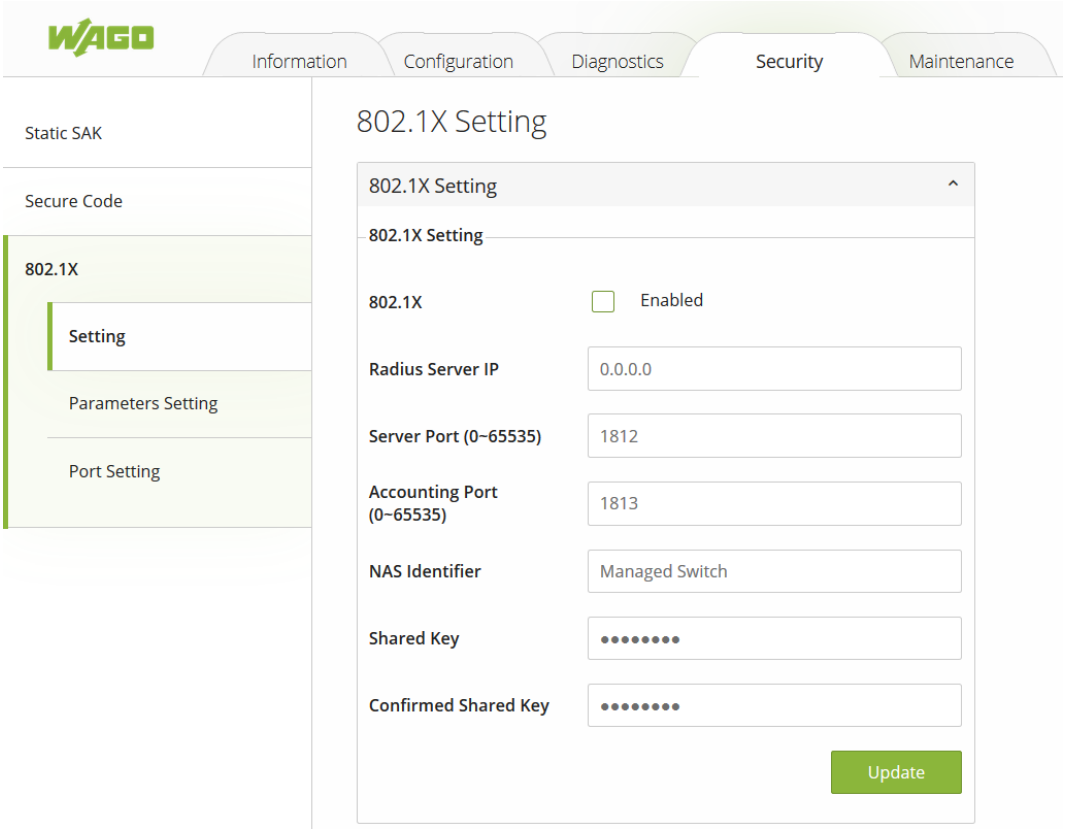

Abbildung 48: WBM-Seite „Security“ – Registerseite „802.1X“ – Abschnitt „Einstellungen“

Tabelle 33: WBM-Seite „Security“ – Registerseite „802.1X“ – Abschnitt „Einstellungen“

Parameter	Werkseinstellung	Beschreibung
802.1x	Deaktiviert	Wählen Sie hier aus, ob Sie 802.1X für alle Ports aktivieren oder deaktivieren möchten.
Radius Server IP	0.0.0.0	In diesem Feld tragen Sie die IP-Adresse des RADIUS-Servers ein.
Server Port	1812	In diesem Feld tragen Sie die Port-Nummer des RADIUS-Servers ein. Bereich: von 0 bis 65535.
Accounting Port	1813	In diesem Feld tragen Sie die Accounting-Port-Nummer des RADIUS-Servers ein. Bereich: von 0 bis 65535.
NAS Identifier	Managed-Switch	Tragen Sie hier den Identifier-String für den 802.1X-Network-Access-Server (NAS) ein. Die maximale Länge beträgt 30 Zeichen.
Shared Key	NULL	Dies ist der „Shared Key“ (vereinbarte Schlüssel) zwischen dem Managed-Switch und dem RADIUS-Server. Beide Produkte müssen für die Verwendung des gleichen Schlüssels konfiguriert werden. Die maximale Länge beträgt 30 Zeichen.
Confirmed Shared Key	Abhängig	Tragen Sie den „Shared Key“ erneut ein.

10.6.3.2 Parameters Setting (IEEE 802.1X-Parametereinstellungen)

Abbildung „WBM-Seite „Security“ – Registerseite „802.1X“ – Abschnitt „802.1X – Parametereinstellungen“ zeigt die Registerseite der 802.1X-Parametereinstellungen. Diese Parameter beziehen sich auf den Authentifizierungszeitraum, die Timeout-Dauer und die maximale Anzahl von Authentifizierungsanfragen. Tabelle „WBM-Seite „Security“ – Registerseite „802.1X“ – Abschnitt „802.1X – Parametereinstellungen“ fasst die Beschreibungen

der Parameter und ihrer Default-Einstellungen zusammen. Um die Änderungen bei den Eingabeparametern zu speichern, müssen Benutzer anschließend auf die Schaltfläche **[Update]** klicken.

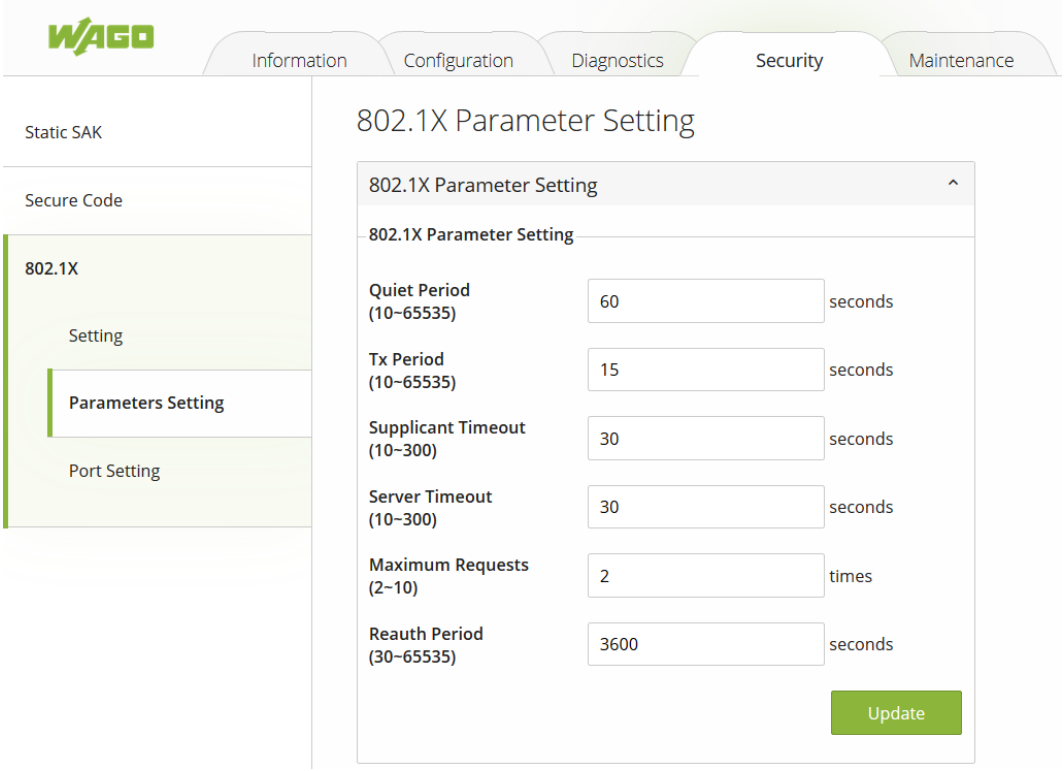

Abbildung 49: WBM-Seite „Security“ – Registerseite „802.1X“ – Abschnitt „802.1X – Parametereinstellungen“

Tabelle 34: WBM-Seite „Security“ – Registerseite „802.1X“ – Abschnitt „802.1X – Parametereinstellungen“

Parameter	Werkseinstellung	Beschreibung
Quiet Period	60	Dieses Feld beschreibt die Wartezeit nach einer fehlgeschlagenen Autorisierung, bevor eine neue Anfrage gesendet werden kann. Der Bereich liegt bei 10 bis 65535 Sekunden.
Tx Period	15	Dieses Feld beschreibt die Wartezeit auf die EAP-Antwort des Supplicants, bevor eine erneute EAP-Anfrage gesendet werden kann. Der Bereich liegt bei 10 bis 65535 Sekunden.
Supplicant Timeout	30	Dieses Feld beschreibt die Zeit, die dem Supplicant für die Beantwortung des EAP-Pakets vom Authentifizierungsserver bleibt. Der Bereich liegt bei 10 bis 300 Sekunden.
Server Timeout	30	Dieses Feld beschreibt die Zeit, die dem Authentifizierungsserver für die Beantwortung des EAP-Pakets vom Supplicant bleibt. Der Bereich liegt bei 10 bis 300 Sekunden.
Maximum Requests	2	Dieses Feld beschreibt die maximale Anzahl erneuter Übertragungen der EAP-Anfrage, die der Authentifizierungsserver an den Supplicant senden kann, bevor die Authentifizierungssitzung abläuft. Der Bereich liegt bei 2 bis 10 Mal.
Reauth Period	3600	Dieses Feld beschreibt die Zeit zwischen den regelmäßigen erneuten Authentifizierungen des Supplicants. Der Bereich liegt bei 30 bis 65535 Sekunden.

10.6.3.3 Port Setting (IEEE 802.1X-Port-Einstellungen)

Benutzer können für jeden Port des intelligenten und sicheren Switches von WAGO den 802.1x-Sicherheitsmechanismus einstellen, wie in Abbildung „WBM-Seite „Security“ – Registerseite „802.1X“ – Abschnitt „802.1X – Port-Einstellungen“ angezeigt. Für jeden

Port kann einer der folgenden vier Autorisierungsmodi verwendet werden: „Force Authorization“ (FA), „Force Unauthorization“ (FU), „IEEE 802.1X Standard Authorization“ (AU) und „No Authorization“ (NO), wie in Tabelle „WBM-Seite „Security“ – Registerseite „802.1X“ – Abschnitt „802.1X – Port-Einstellungen“ beschrieben.

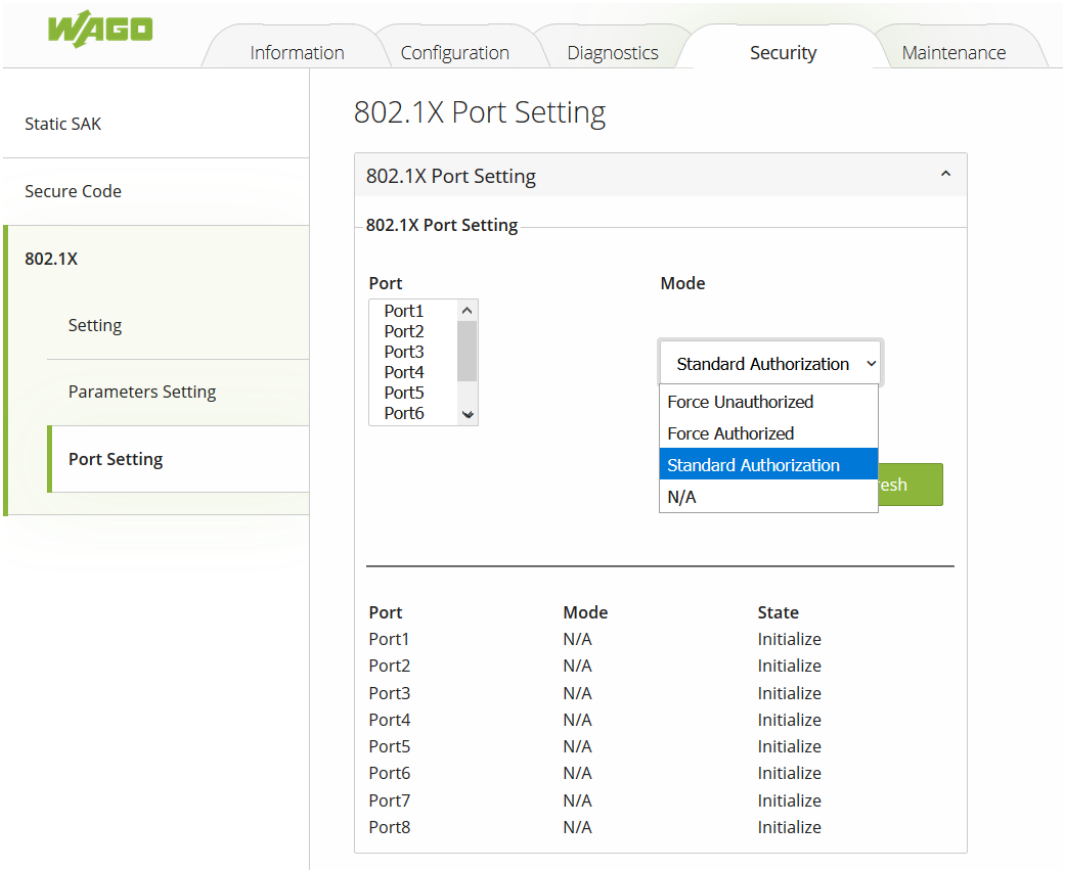

Abbildung 50: WBM-Seite „Security“ – Registerseite „802.1X“ – Abschnitt „802.1X – Port-Einstellungen“

Die Darstellung auf der Webseite ist in zwei Bereiche unterteilt. Im oberen Bereich der Webseite können die Port-Einstellungen geändert werden. Im unteren Bereich zeigt eine Tabelle den aktuellen Status des Autorisierungsmodus und den Zustand jedes Ports im Managed-Switch an. Klicken Sie zur Aktivierung der 802.1X-Security auf einen der Ports oder drücken Sie die Strg-Taste und anschließend auf mehrere Ports in der Liste. Wählen Sie dann den Autorisierungsmodus aus dem Drop-down-Menü aus und klicken Sie auf die Schaltfläche **[Update]**. Zur Überprüfung des aktuellen Status der 802.1X-Port-Einstellung können Benutzer auf die Schaltfläche **[Refresh]** klicken.

Tabelle 35: WBM-Seite „Security“ – Registerseite „802.1X“ – Abschnitt „802.1X – Port-Einstellungen“

Parameter	Werkseinstellung	Beschreibung
Port	Option	Wählen Sie hier den oder die Ports für die Konfiguration aus.
Mode	NO	Optionen: **FU (Force Unauthorized):** Spezifizieren Sie „Forced Unauthorized“ (nicht autorisiert). **FA (Force Authorized):** Spezifizieren Sie „Forced Authorized“ (immer autorisiert). **AU (Standard Authorization):** Spezifizieren Sie die Autorisierung auf Basis von IEEE 802.1X. **NO:** Spezifizieren Sie die Deaktivierung der Autorisierung.

10.6.4 Port Security (Port Sicherheit)

Port-Security ist eine Sicherheitsfunktion die es ermöglicht, jeden Port in einem Switch mit einer spezifischen Reihe von MAC-Adressen zu verknüpfen, sodass die Kommunikation nur mit autorisierten MAC-Adressen möglich ist. Bevor Benutzerdaten übertragen werden, prüft der Switch die MAC-Adresse des Senders jedes Mal, wenn eine Verbindung aufgebaut wird.

Mit den „Port Security“-Funktionen kann die maximale Anzahl von MAC-Adressen pro Schnittstelle spezifiziert werden. Wird diese Anzahl überschritten, werden eingehende Pakete mit neuen MAC-Adressen verworfen. Der Bereich der autorisierten MAC-Adressen wird nach der Aktivierung des entsprechenden Ports automatisch definiert. Nach der Aktivierung speichert der Switch bei jedem Verbindungsaufbau am Port die MAC-Adressen des Senders in einer Tabelle. Das geschieht so lange bis die vom Benutzer definierte maximale Anzahl erreicht ist.

Wenn der Port am Switch vom deaktivierten in den aktivierten Zustand versetzt wird, werden alle von diesem Port aufgezeichneten MAC-Adressen gelöscht.

ⓘ Hinweis

Konfiguration der Port-Sicherheitsfunktionen

In den Port-Sicherheitsfunktionen kann konfiguriert werden, welche MAC-Adressen an den Schnittstellen zulässig sind. Dieses Produkt unterstützt bis zu 1.000 MAC-Adressen für einen Port.

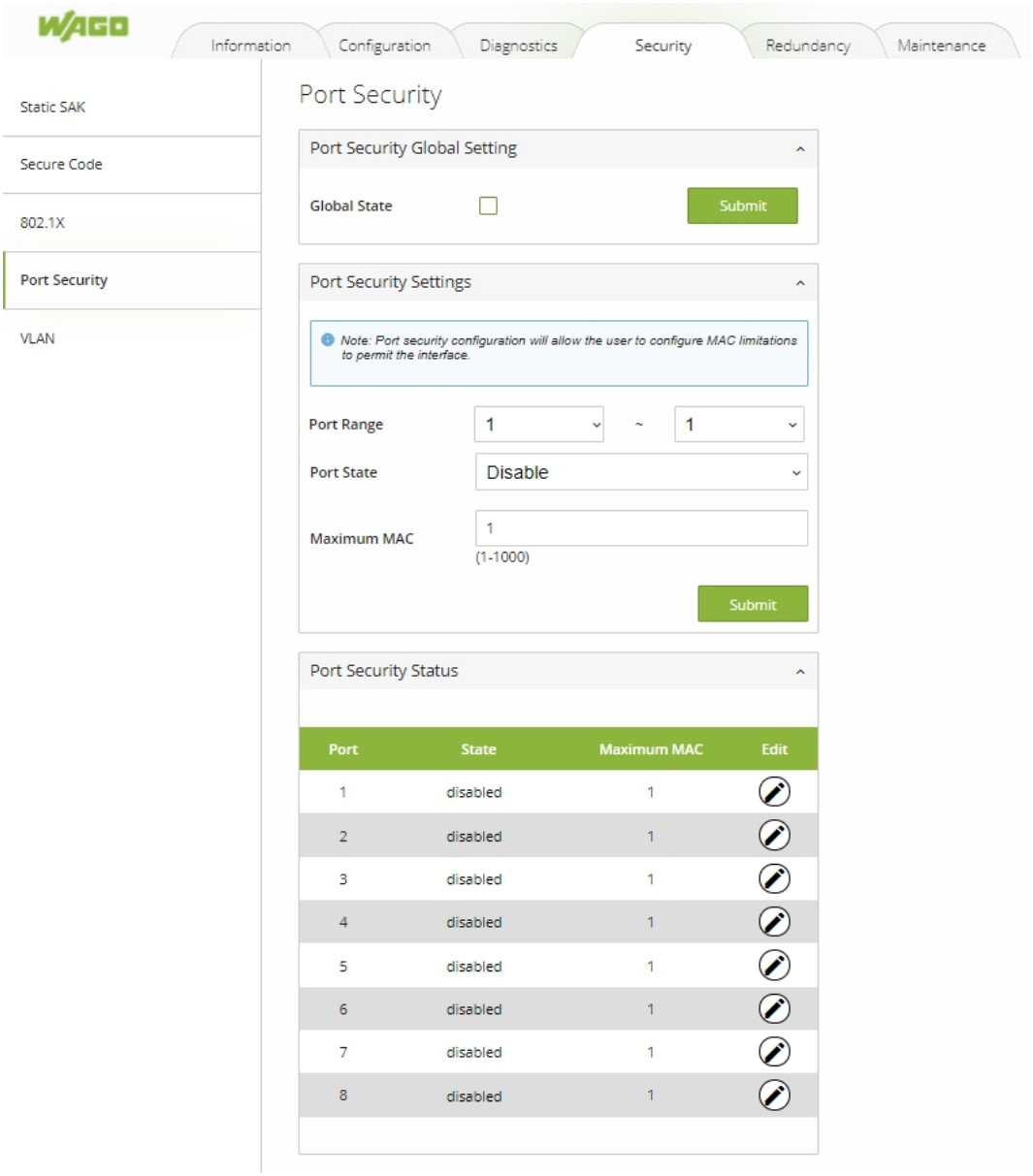

Abbildung 51: WBM-Seite „Security“ – Registerseite „Port-Security“

Tabelle 36: WBM-Seite „Security“ – Registerseite „Port-Security – Einstellungen“

Parameter	Beschreibung
Globale Einstellungen für die Port-Security	
Global State (globaler Zustand)	Aktivieren Sie „Global State“, um die Port-Security auf dem Switch zu aktivieren. Deaktivieren Sie „Global State“, um die Port-Security auf dem Switch zu deaktivieren.
Port-Sicherheitseinstellungen	
Port Range	Wählen Sie den Port-Bereich aus, für den Sie die Port-Security aktivieren/deaktivieren möchten.
Port State	Aktivieren oder deaktivieren Sie die Port-Security für den ausgewählten Port-Bereich.
Maximum MAC	Wählen Sie maximale Anzahl an MAC-Adressen für den ausgewählten Port-Bereich aus.

10.6.5 VLAN

10.6.5.1 Port-Isolation

Die „Portisolation“ (Porttrennung) ist eine portbasierte, virtuelle LAN-Funktion. Sie partitioniert die vermittelnden Ports in virtuelle private Domänen, die einzeln zugewiesen werden. Eine Datenvermittlung außerhalb der privaten Domäne des Switches ist nicht erlaubt. Die VLAN-Tag-Informationen der Pakete werden ignoriert.

Mit dieser Funktion können für jeden Port ein oder mehrere Ausgangsports konfiguriert werden, um für diesen spezifischen Port die von ihm empfangenen Daten weiterzuleiten.

Wenn Sie die Kommunikation zwischen zwei Teilnehmerports zulassen möchten, müssen Sie den Ausgangsport für beide Ports definieren. Er bildet standardmäßig ein VLAN mit allen ETHERNET-Ports.

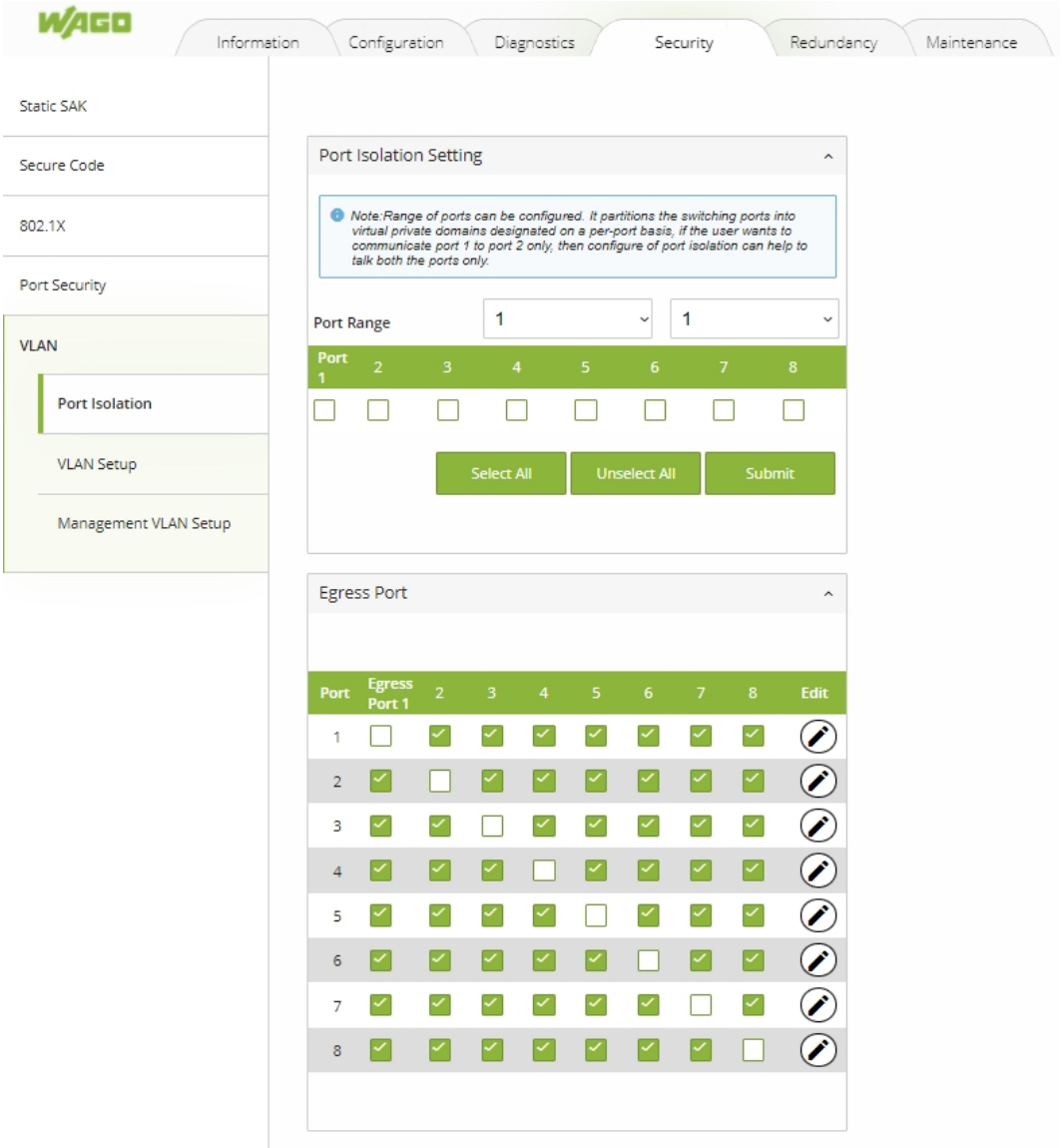

Abbildung 52: WBM-Seite „Security“ – Registerseite „Port-Isolation – Einstellung“

Tabelle 37: WBM-Seite „Security“ – Registerseite „Port-Isolation – Einstellungen

Parameter	Beschreibung
Port Range	Wählen Sie den Port-Bereich aus, auf den Sie die Einstellungen für die Port-Isolation übertragen möchten.

Parameter	Beschreibung
Port (1–8)	Wählen Sie Ausgangsports für den ausgewählten Port-Bereich aus.

10.6.5.2 VLAN-Einrichtung

Ein VLAN („**V**irtuelles **LAN**“) ist eine Gruppe aus Hosts mit einheitlichen Anforderungen, die unabhängig von ihrem physischen Standort so kommunizieren als würden sie einer Broadcast-Domäne angehören. Ein VLAN hat die gleichen Attribute wie ein physisches LAN, aber es ermöglicht die Gruppierung von Endstationen, auch wenn sich diese nicht am selben Netzwerk-Switch befinden. Die Neukonfiguration des Netzwerks kann so über Software, statt über räumlich versetzte Geräte erfolgen.

VID („**V**LAN-**ID**“) ist die Kennzeichnung des VLANs, die im Wesentlichen vom Standard 802.1Q verwendet wird. Sie besteht aus 12 Bit und ermöglicht die Kennzeichnung von 4096 (2^{12}) VLANs. Von den 4096 möglichen VIDs wird die VID 0 zur Kennzeichnung von „Priority Frames“ verwendet und der Wert 4095 (FFF) reserviert, sodass maximal 4094 VLAN-Konfigurationen möglich sind.

Ein „Tagged VLAN“ (VLAN mit Tag) nutzt einen eindeutigen Tag (die VLAN-ID) im MAC-Header, um die VLAN-Zugehörigkeit eines Frames unabhängig von den „Bridges“ zu identifizieren, ganz gleich, auf welchem Switch der Tag erzeugt wurde. VLANs können statisch (manuell durch Benutzer) oder dynamisch über das GVRP („GARP VLAN Registration Protocol“) eingerichtet werden. Die VLAN-ID ordnet ein Frame einem bestimmten VLAN zu und stellt die Informationen bereit, die Switches zur Verarbeitung des Frames innerhalb des Netzwerks benötigen. Ein Frame mit Tag ist vier Byte länger als ein Frame ohne Tag und enthält zwei Byte für den TPID (den „Tag Protocol Identifier“, der sich im Feld Typ/Länge des „ETHERNET Frames“ befindet) und zwei Byte für die TCI (die „**T**ag **C**ontrol **I**nformation“, die nach dem Quelladressfeld des „ETHERNET Frames“ beginnt).

Weitergeleitete Frames mit und ohne Tag

Jeder Port des Switches kann Frames mit und ohne Tags weiterleiten. Bei der Weiterleitung eines Frames von einem 802.1Q-VLAN-unterstützenden Switch zu einem ohne diese Unterstützung, muss der Switch zuerst entscheiden, wohin er den Frame weiterleitet und dann den VLAN-Tag entfernen. Im umgekehrten Fall muss der Switch zuerst entscheiden, wohin er den Frame weiterleitet und dann den VLAN-Tag hinzufügen, der der Default-VID des Eingangsports entspricht. Die Default-PVID für alle Ports ist „VLAN 1“, was aber geändert werden kann.

Ein Broadcast-Frame (oder ein Multicast-Frame für eine Multicast-Gruppe, die dem System bekannt ist) wird nur für Ports dupliziert, die Teilnehmer der VID sind (außer dem Eingangsport selbst) und somit auf eine spezifische Domäne begrenzt.

Portbasiertes 802.1Q-VLAN

Als Teilnehmer eines portbasierten VLANs wird der Port einem spezifischen VLAN zugewiesen, unabhängig davon, welcher Benutzer oder welches Gerät mit dem Port verbunden ist. Das bedeutet, dass alle mit diesem Port verbundenen Benutzer Teilnehmer desselben VLANs sind. Normalerweise nimmt der Netzwerkadministrator die VLAN-Zuordnung vor. Die Port-Konfiguration ist statisch und kann nicht automatisch in ein anderes VLAN verändert werden, ohne dass eine manuelle Neukonfiguration durchgeführt wird.

In einem portbasierten VLAN können einem Port zwei Rollen zugewiesen werden:

- Access-Port: Dieser Port überträgt nur Daten von bzw. zu dem spezifischen VLAN, dem er zugeordnet ist.
- Trunk-Port: Dieser Port kann Daten von bzw. zu einem oder zu allen VLANs übertragen, zu denen ein spezifischer Switch Zugang hat.

Wie auch bei anderen VLAN-Verfahren können die mit dieser Methode weitergeleiteten Pakete nicht in andere VLAN-Domänen oder Netzwerke übertragen werden. Nachdem ein Port einem VLAN zugewiesen wurde, kann er ohne Einsatz eines Layer-3-Gerätes keine Daten von Geräten eines anderen VLANs empfangen oder an sie senden.

Das an den Port angeschlossene Gerät kann nicht erkennen, dass ein VLAN vorhanden ist. Das Gerät erkennt lediglich, dass es Teil eines Subnetzes ist und mit allen anderen Netzteilnehmern kommunizieren kann, indem es einfach Informationen über die Kabelverbindung sendet. Der Switch ist dafür verantwortlich zu erkennen, dass Informationen aus einem spezifischen VLAN stammen, und er muss sicherstellen, dass diese Informationen zu allen Teilnehmern des VLANs übertragen werden. Außerdem muss der Switch sicherstellen, dass diese Informationen nicht von Ports aus einem anderen VLAN empfangen werden können.

Dieser Ansatz ist simpel, schnell und einfach zu verwalten, weil er keine komplexen Zuordnungstabellen für die VLAN-Segmentierung benötigt. Wenn die „Port-to-VLAN“-Verbindung mit einer anwendungsspezifischen integrierten Schaltung (ASIC, einem „**A**pplication-**s**pecific **i**ntegrated **c**ircuit“) ausgeführt wird, bringt dies große Leistungsvorteile. Ein ASIC ermöglicht eine „Port-to-VLAN“-Zuordnung auf Hardwareebene.

ⓘ Hinweis

Erstellung von VLANs

Es können bis zu 128 VLANs eingerichtet werden. Es wird empfohlen, einen Trunk-Port mit Tag zu konfigurieren und alle Ports in das VLAN aufzunehmen.

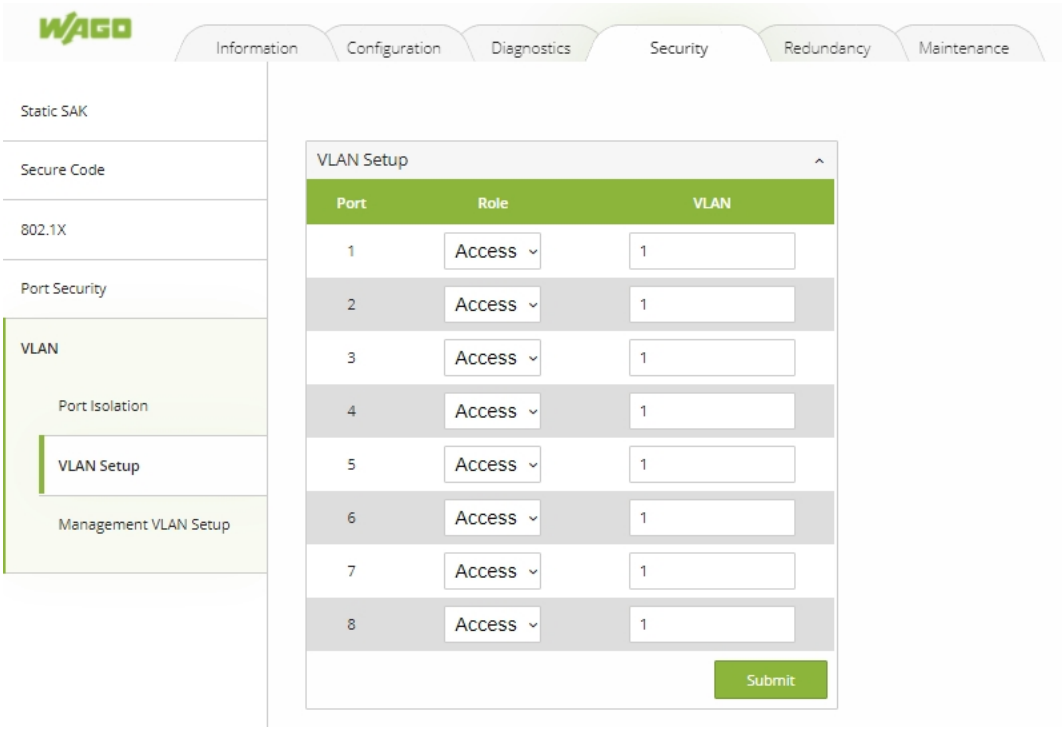

Abbildung 53: WBM-Seite „Security“ – Registerseite „VLAN-Einrichtung“

Tabelle 38: WBM-Seite „Security“ – Registerseite „VLAN-Einrichtung“

Parameter	Beschreibung
Role (Rolle)	Wählen Sie aus, ob dieser Port die Rolle als Access-Port oder als Trunk-Port zugewiesen werden soll.
VLAN	Wählen Sie das VLAN aus, das dem Port zugewiesen werden soll (für Trunk z. B.: 1,3,6,19)

10.6.5.3 Management-VLAN

Es muss immer ein Port im Management-VLAN sein. Andernfalls kann der Switch nicht konfiguriert werden.

ⓘ Hinweis

Erhalt der Management-VLAN-Informationen

Fehlen die Informationen für das Management-VLAN, können Sie sie über das LLDP erhalten.

- Schritt 1: Verbinden Sie Port 1 mit Ihrem Laptop oder PC.

- Schritt 2: Port 1 wird die Informationen für die Konfiguration des Management-VLANs drei Mal über das LLDP DA senden, wenn das System neu gestartet wird (mit einem Intervall von 5 Sekunden).

- Schritt 3: Verwenden Sie das Tool zur Netzwerküberwachung, um die LLDP-Pakete zu überwachen und das Management-VLAN zu finden. Im Beispiel unten hat das Management-VLAN die ID 1. Die Ports 1, 3, 5 und 7 wurden für das VLAN 1 eingerichtet.

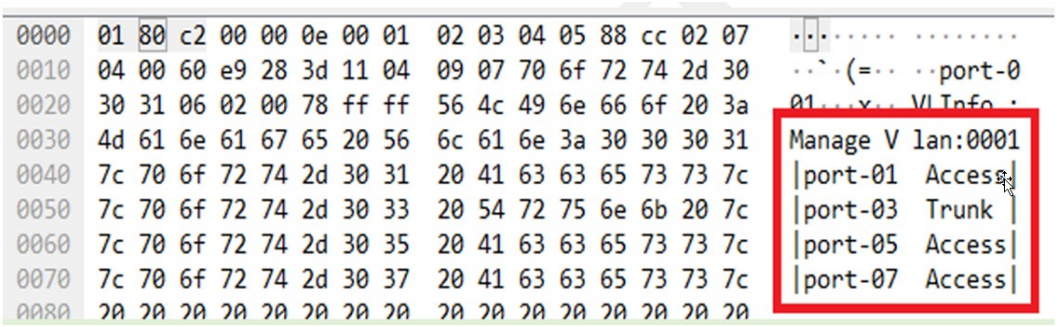

Abbildung 54: Management –VLAN - Beispiel

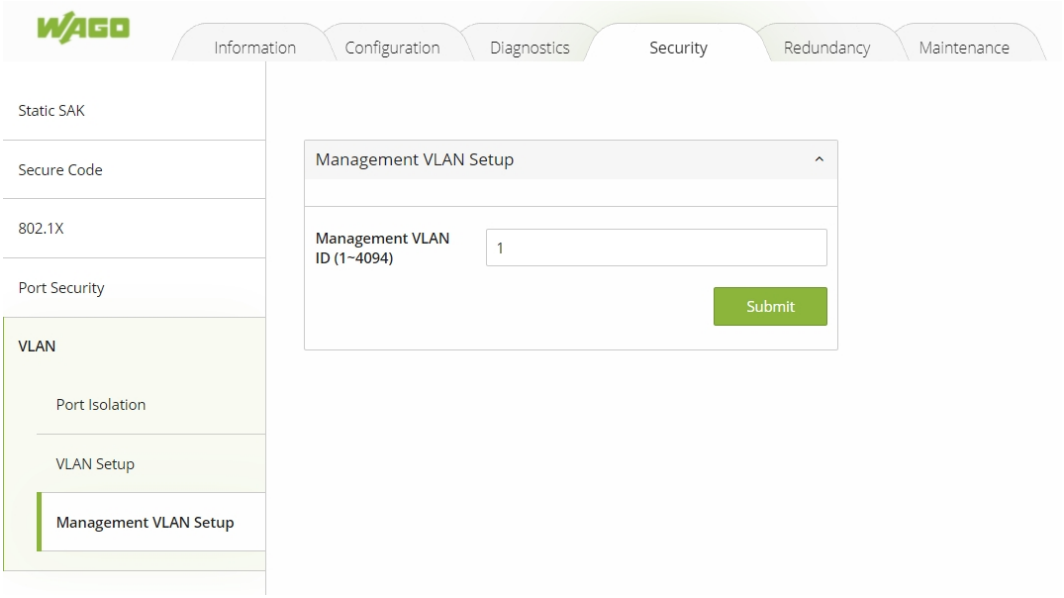

Abbildung 55: WBM-Seite „Security“ – Registerseite „Management VLAN-Einrichtung“

Tabelle 39: WBM-Seite „Security“ – Registerseite „Management VLAN-Einrichtung“

Parameter	Beschreibung
Management-VLAN	Wählen Sie die VLAN-ID für das Management-VLAN aus.

ⓘ Hinweis

Wird das Management-VLAN nicht als Access-Port auf dem Switch konfiguriert, muss über den Trunk-Port auf die Konfiguration zugegriffen werden. In diesem Fall muss die Konfiguration über einen Access-Port auf einem zweiten Switch erfolgen, der sich im selben Management-VLAN befindet.

10.7 Redundancy (Redundanz)

10.7.1 RSTP

10.7.1.1 Allgemeine Informationen

Das „**R**apid **S**panning **T**ree **P**rotocol“ (RSTP) ist eine Weiterentwicklung des „**S**panning **T**ree **P**rotocol“ (STP). Beide Protokolle wurden von der IEEE in den folgenden Standards definiert:

- IEEE 802.1D: Spanning Tree Protocol
- IEEE 802.1w: Rapid Spanning Tree Protocol

Das RSTP kann Netzwerkschleifen erkennen und aufbrechen sowie „Backup Links“ (Ersatzverbindungen) zwischen Switches, Bridges oder Routern bereitstellen. Durch den regulären Austausch von „Bridge Protocol Data Units“ (BDPUs) kann ein Switch mit anderen RSTP-fähigen Switches im Netzwerk interagieren, um sicherzustellen, dass zwischen zwei gegebenen Stationen im Netzwerk zu jeder Zeit immer nur eine Verbindung besteht.

Im Vergleich zum STP ermöglicht das RSTP eine schnellere Adaptation des „Spanning Tree“. Außerdem ist es abwärtskompatibel mit ausschließlich STP-fähigen Bridges. Mit dem RSTP werden Informationen über Topologieänderungen direkt von dem Gerät durch

das Netzwerk übertragen, das eine Topologieänderung verursacht hat. Beim STP gibt es größere Verzögerungen, weil das Gerät, das eine Topologieänderung verursacht, zuerst die „Root Bridge“ benachrichtigt und diese dann den Rest des Netzwerks. Sowohl das RSTP als auch das STP entfernen ungewollt erlernte Adressen aus der Filterdatenbank.

Zur Erstellung des „Spanning Tree“ muss zuerst eine „Root Bridge“ gewählt werden. Die „Root Bridge“ ist der Startpunkt eines „Spanning Tree“. Beginnend mit der „Root Bridge“ erfolgt die Definition aller Pfade darüber, welche anderen

Bridges im Netzwerk erreichbar sind. Die Auswahl der „Root Bridge“ erfolgt nach einem definierten Verfahren. Zu diesem Zweck tauschen die Switches ihre Bridge-IDs (BID – bestehend aus Priorität, System-ID und MAC-Adresse) über Multicast-Nachrichten aus und wählen den Switch mit der niedrigsten Priorität als „Root Bridge“ für den „Spanning Tree“ aus. Wurde die niedrigste Priorität mehr als einem Switch zugewiesen, sind andere Kriterien entscheidend, wie etwa die MAC-Adresse.

Nach der Auswahl der „Root Bridge“ werden die Pfade definiert, über die die anderen Bridges im Netzwerk erreichbar sind. Dafür wiederum werden zunächst alle Pfade bestimmt, über die andere Switches erreichbar sind. Werden mehrere Pfade erkannt, über die ein Switch erreichbar ist, werden die Pfade mit den ungünstigsten Pfadkosten blockiert. Die Pfadkosten („Path Cost“) sind die Kosten für die Übertragung eines Frames durch den Port in das LAN. Der IEEE-Standard definiert die Pfadkosten, erlaubt jedoch auch eine manuelle Einstellung. Dabei sollte dieser Wert an die Übertragungsgeschwindigkeit angepasst werden. Der gültige Bereich liegt bei 1 bis 200000000. Es ist wahrscheinlicher, dass ein Pfad mit höheren Kosten vom STP blockiert wird, wenn eine Netzwerkschleife erkannt wird.

Wenn sich in einem per Bridge gekoppelten LAN die Topologie ändert, wird ein neuer Baum aufgespannt. Sobald eine stabile Netzwerktopologie eingerichtet ist, warten alle Bridges auf „Hello BPDUs“, die von der „Root Bridge“ übertragen werden. Wenn eine Bridge nach einem zuvor definierten Intervall („Max Age“) keine „Hello BPDUs“ empfängt, geht die Bridge davon aus, dass die Verbindung zur „Root Bridge“ unterbrochen ist. Daraufhin beginnt die Bridge Negotiationen mit anderen Bridges, um das Netzwerk neu zu konfigurieren und wieder eine gültige Netzwerktopologie einzurichten.

Port-Zustände bei RSTP-Switches

- **Discarding**
  Wenn ein Port einen „Switching Loop“ (eine Schleifenverbindung zwischen zwei Ports) erzeugt, können keine Benutzerdaten mehr gesendet oder empfangen werden. Der Port kann aber in den Zustand „Forwarding“ (Weiterleitungsmodus) übergehen, sofern die anderen aktiven Verbindungen ausfallen und der Algorithmus des „Spanning Tree“ bestimmt, dass der Port in diesen Modus übergehen darf. BPDU-Daten (**B**ridge **P**rotocol **D**ata **U**nit, Konfigurationsnachricht) werden im Zustand „Discarding“ weiterhin empfangen und gesendet.
- **Learning**
  Auch wenn der Port noch keine Frames (Pakete) weitergeleitet hat, kann er Quell-Adressen von empfangenen Frames erlernen und sie der Filterdatenbank („Switching Database“) hinzufügen.
- **Forwarding**
  Der Port ist im normalen Betriebsmodus und empfängt und sendet Daten. Das RSTP überwacht eingehende BPDUs daraufhin, ob sie anzeigen, dass der Port in den Zustand „Blocking“ übergehen soll, um eine Schleife zu verhindern.

Port-Rollen bei RSTP-Bridges

- **Root**
  Der „Root Port“ ist ein weiterleitender Port, der Daten von der „Non-Root Bridge“ zur „Root Bridge“ am besten übertragen kann.
- **Designated**
  Dies ist ein weiterleitender Port für jedes LAN-Segment.
- **Alternate**
  Dieser Port stellt einen alternativen Pfad zur „Root Bridge“ dar. Dieser Pfad unterscheidet sich jedoch vom Root-Port.
- **Backup**
  Dieser Port dient als Ersatz-/redundanter Pfad zu einem Segment, mit dem ein anderer „Bridge Port“ bereits verbunden ist.
- **Disabled**
  Dies ist eigentlich kein Teil des RSTP, da ein Netzwerkadministrator einen Port manuell deaktivieren kann.

Weitere wichtige Begriffe:

Tabelle 40: Weitere wichtige Begriffe

Begriff	Beschreibung
Forward Time	Die „Forward Time“ (Weiterleitungszeit) oder „Forward Delay“ (Weiterleitungsverzögerung) ist die maximale Zeit (in Sekunden), die der Switch wartet, bevor er Zustände ändert. Diese Verzögerung ist erforderlich, weil jeder Switch erst Informationen über Topologieänderungen empfangen muss, bevor er Frames weiterleitet. Außerdem benötigt jeder Port Zeit, um Informationen über Konflikte zu empfangen, die ihn zurück in den blockierten Zustand versetzen würden. Anderenfalls könnten vorübergehende Datenschleifen entstehen. Der gültige Bereich ist 4 bis 30 Sekunden.
Max Age	Das „Max Age“ (Maximales Alter) ist die maximale Zeit (in Sekunden), die der Switch ohne eine BPDU („Bridge Protocol Data Unit“, Konfigurationsnachricht) zu empfangen warten kann, bevor er versucht, mit der Rekonfiguration zu beginnen. Alle Switch-Ports (außer „Designated Ports“) empfangen in regelmäßigen Abständen BPDUs. Jeder Port, der RSTP-Informationen (aus der letzten BPDU) verlernt, wird zum „Designated Port“ für das angeschlossene LAN. Wenn dies ein „Root Port“ ist, wird aus den an das Netzwerk angeschlossenen Switch-Ports ein neuer „Root Port“ gewählt.
Hello Time	Die „Hello Time“ ist das Zeitintervall in Sekunden zwischen den vom Root-Switch versendeten BPDUs.
Edge Port	„Edge Ports“ sind mit einem LAN verbunden, an das keine anderen Bridges angeschlossen sind. Diese Ports können direkt in den Zustand „Forwarding“ übergehen. Das RSTP überwacht diese Ports dennoch auf Empfang von BPDUs, falls eine Bridge angeschlossen wird. Das RSTP kann auch so konfiguriert werden, dass es „Edge Ports“ automatisch erkennt. Sobald die Bridge erkennt, dass eine BPDU bei einem „Edge Port“ eingeht, verliert dieser seinen Status als „Edge Port“.
Transmission Limit	Mit dem „Transmission Limit“ (Übertragungsgrenze) wird das minimale Intervall zwischen der Übertragung aufeinanderfolgender RSTP-BPDUs konfiguriert. Diese Funktion kann nur im RSTP-Modus aktiviert werden. Der gültige Bereich liegt bei 1 bis 10 Sekunden.
Priority	Über die Priorität wird die Auswahl des Root-Switches, des Root-Ports und des „Designated Port“ bestimmt. Der Switch mit der höchsten Priorität (also dem niedrigsten numerischen Wert) wird zum RSTP-Root-Switch. Haben jedoch alle Switches die gleiche Priorität, wird der Switch mit der niedrigsten MAC-Adresse zum Root-Switch. Tragen Sie einen Wert von 0 bis 61440 ein. Je niedriger der von Ihnen zugewiesene numerische Wert ist, desto höher ist die Priorität dieser Bridge. Die Priorität bestimmt die „Root Bridge“, die im Gegenzug wiederum „Root Hello Time“, „Root Maximum Age“ und „Root Forwarding Delay“ bestimmt.

Begriff	Beschreibung
Convergence Time	Die „Convergence Time“ (Konvergenzzeit) ist die erforderliche Zeit zur Neuberechnung des „Spanning Tree“, wenn eine Verbindung ausfällt.
BPDU Guard	Diese Einstellung wird für jeden Port individuell konfiguriert. Wenn der Port im „BDU Guard“ aktiviert ist und eine BPDU empfängt, wird er in den Zustand „Disabled“ wechseln, um eine fehlerhafte Umgebung zu vermeiden. Der Benutzer muss den Port dann manuell aktivieren.
BPDU Filter	Mit dieser Funktion wird ein Filter für das Senden oder Empfangen von BPDUs in einem Switch-Port eingerichtet. Wenn ein Port BPDUs empfängt, werden diese verworfen. Bei gleichzeitiger Aktivierung von „BPDU Filter“ und „BPDU Guard“ hat ersterer die höhere Priorität.
Root Guard	Die Funktion „Root Guard“ zwingt eine Schnittstelle dazu, ein „Designated Port“ zu werden, um zu verhindern, dass benachbarte Switches zu einem Root-Switch werden. Diese Funktion bietet eine Möglichkeit, die Auswahl der „Root Bridge“ in einem Netzwerk festzulegen. Sie verhindert, dass ein „Designated Port“ zum „Root Port“ werden kann. Wenn ein Port mit der Funktion „Root Guard“ eine höherwertige BPDU empfängt, wird der Port in einen Root-inkonsistenten (praktisch dem Zustand „Listening“ gleichzusetzenden) Zustand versetzt, um so den Status der aktuellen „Root Bridge“ aufrechtzuerhalten. Der Port kann in den Zustand „Forwarding“ übergehen, wenn er über den Zeitraum von drei „Hello Times“ keine höherwertigen BPDUs mehr empfängt.

10.7.1.2 RSTP-Einrichtung

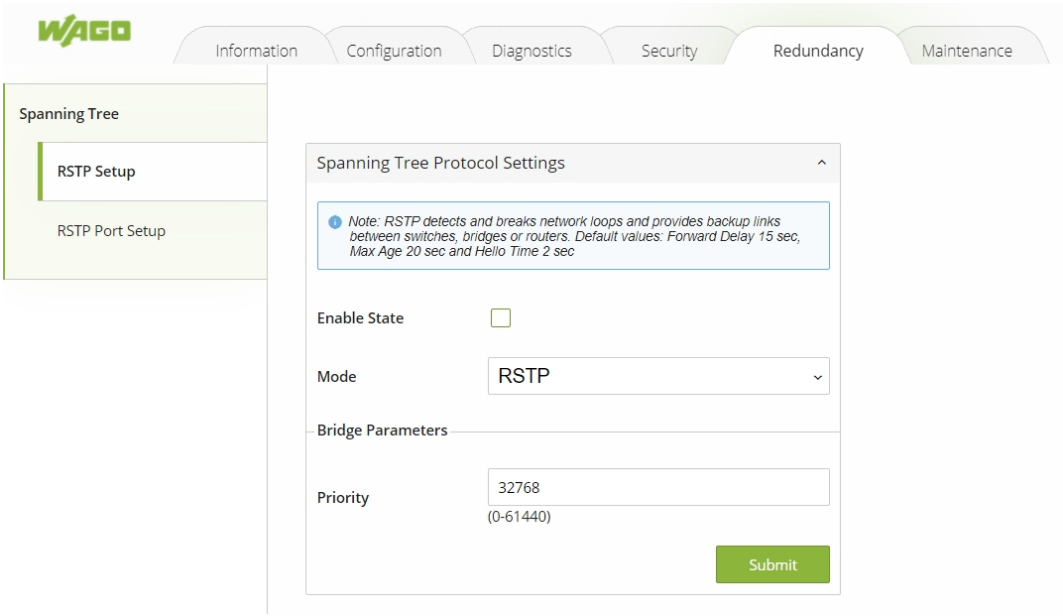

Abbildung 56: WBM-Seite „Redundanz“ – Registerseite „RSTP-Einrichtung"

Tabelle 41: WBM-Seite „Redundanz“ – Registerseite „RSTP -Einrichtung“

Parameter	Beschreibung
Enable State	Aktivieren Sie „Enable State“, um das RSTP im Switch zu aktivieren. Deaktivieren Sie „Enable State“, um das RSTP im Switch zu deaktivieren.
Mode	Es wird nur ein Modus (RSTP) unterstützt.
Bridge-Parameter	
Priority	Definieren Sie die Priorität des Switches, die zur Bestimmung des Root-Switches, des Root-Ports und der „Designated Ports“ verwendet wird.

ⓘ Hinweis

Maximale Switch-Anzahl im RSTP-Ring

Mit einem RSTP-Ring können maximal 20 Switches verbunden werden (Default-Werte: „Max Age“ = 20 Sek.).

10.7.1.3 RSTP-Port-Einrichtung

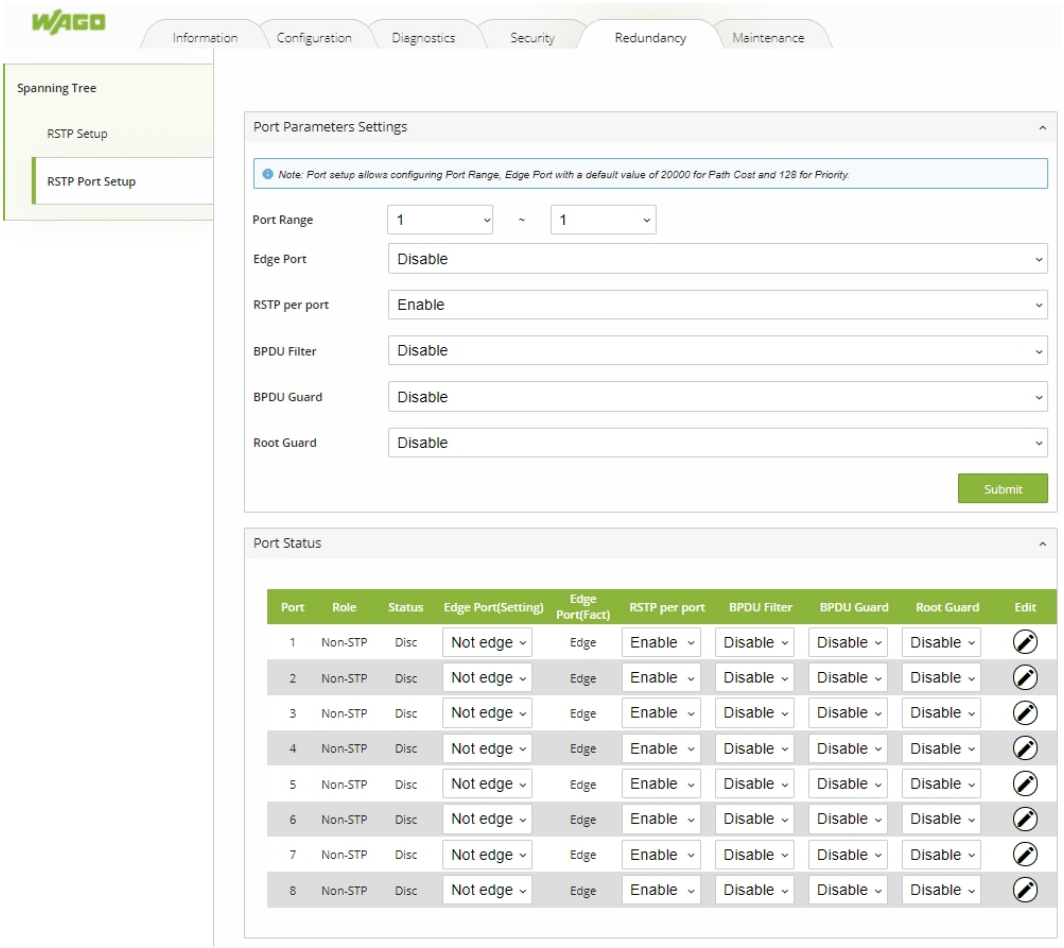

Abbildung 57: WBM-Seite „Redundanz“ – Registerseite „RSTP-Port-Einrichtung"

Tabelle 42: WBM-Seite „Redundanz“ – Registerseite „RSTP-Port-Einrichtung“

Parameter	Beschreibung
Port Range	Wählen Sie den Port-Bereich aus, auf den Sie die Port-Parametereinstellungen übertragen möchten.
Edge Port	Wählen Sie aus, ob die Edge-Port-Einstellung für den ausgewählten Port-Bereich aktiviert oder deaktiviert werden soll.
RSTP pro Port	Wählen Sie aus, ob das RSTP für den ausgewählten Port-Bereich aktiviert oder deaktiviert werden soll.
BDPU Filter	Wählen Sie aus, ob die BDPU-Filter-Einstellung für den ausgewählten Port-Bereich aktiviert oder deaktiviert werden soll.
BDPU Guard	Wählen Sie aus, ob die BDPU-Guard-Einstellung für den ausgewählten Port-Bereich aktiviert oder deaktiviert werden soll.
Root Guard	Wählen Sie aus, ob die Root-Guard-Einstellung für den ausgewählten Port-Bereich aktiviert oder deaktiviert werden soll.

10.7.1.4 RSTP-Failover und Recovery-Zeiten

Applikationen für die industrielle Automatisierung erfordern robuste Kommunikationsnetzwerke, die eine hohe Verfügbarkeit sicherstellen. Die Verfügbarkeit eines Ethernet-Netzwerks wird zu großen Teilen dadurch bestimmt, wie schnell ein Netzwerk den Ausfall eines Kabels oder eines Geräts ausgleichen kann.

Zur Gewährleistung der Verfügbarkeit gibt es mehrere Ansätze. Die ringbasierte Netzwerktopologie, ist der einfachste und am häufigsten verfolgte Ansatz. Aber nicht alle Lösungen erzielen die gleiche Systemverfügbarkeit und sind direkt abhängig von der Netzwerktopologie. Um Rückschlüsse auf die Leistung einer spezifischen industriellen Applikation ziehen zu können, sind unten die Ergebnisse der Messungen von „Failover“ und „Recovery Time“ des Netzwerks aufgeführt. Die getesteten Topologien entsprechen einem RSTP-Ring mit 10 und 20 Switches.

Kabelbruch (Failover) und neue Verbindung (Recovery)

	Bidirektionaler Datenverkehr (TCP)		Bidirektionaler Datenverkehr (UDP)	
Geräteanzahl im Ring (852-1322)	Durchschnittliche Failover-Zeit (ms)	Durchschnittliche Recovery-Zeit (ms)	Durchschnittliche Failover-Zeit (ms)	Durchschnittliche Recovery-Zeit (ms)
10	1210,7	127,0	1213,3	127,8
20	1238,8	528,7	1239,0	530,0

Netzabschaltung – Root (Failover)

	Bidirektionaler Datenverkehr (TCP)		Bidirektionaler Datenverkehr (UDP)	
Geräteanzahl im Ring (852-1322)	Durchschnittliche Failover-Zeit (ms)	Durchschnittliche Recovery-Zeit (ms)	Durchschnittliche Failover-Zeit (ms)	Durchschnittliche Recovery-Zeit (ms)
10	1064,9	k. A.	1064,5	k. A.
20	1233,6	k. A.	1232,6	k. A.

10.8 Maintenance (Wartung)

10.8.1 Firmware Upgrade (Firmware-Upgrade)

Benutzer können die Produkt-Firmware über das Web-Interface aktualisieren, wie in Abbildung „WBM-Seite „Maintenance“ – Registerseite „Firmware-Upgrade“ angezeigt.

Zur Aktualisierung der Firmware müssen Benutzer eine neue Firmware von der Website von WAGO herunterladen und auf einem lokalen Computer speichern. Klicken Sie anschließend auf die Schaltfläche **[Browse…]** (Suchen) und wählen Sie die zuvor heruntergeladene Firmware aus. Die Dateiendung der Firmware für den Switch ist für gewöhnlich „.dld“ (z. B.: 0852-132x-V223.dld). Klicken Sie danach auf die Schaltfläche **[Update]** und warten Sie, bis die Aktualisierung abgeschlossen ist.

ⓘ Hinweis

Firmware-Upgrade

Stellen Sie sicher, dass für die gesamte Dauer des Firmware-Upgrades die Spannungsversorgung des Switches eingeschaltet ist.

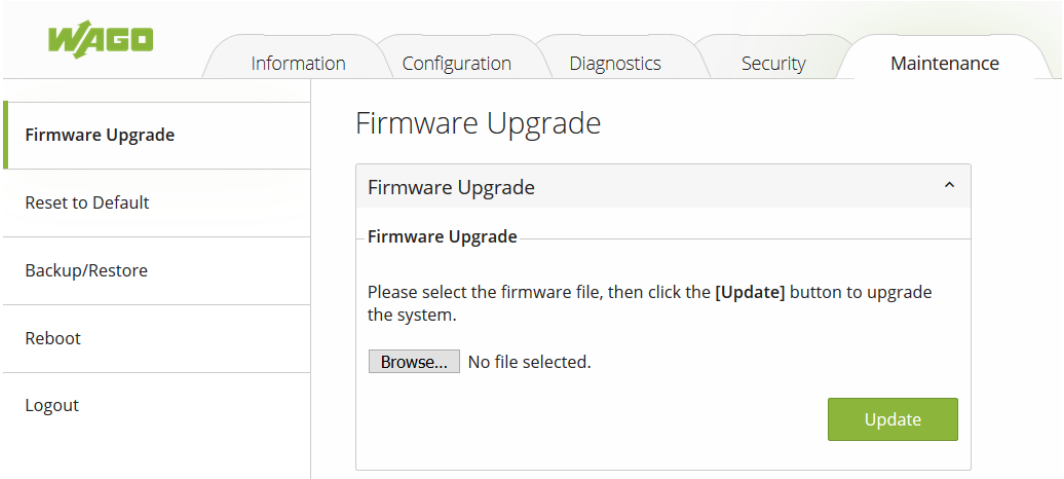

Abbildung 58: WBM-Seite "Maintenance" - Registerseite "Firmware-Upgrade"

10.8.2 Reset to Default (Rücksetzen auf Default-Werte)

Sollte der Switch nicht ordnungsgemäß funktionieren, können Benutzer ihn auf die originalen Werkseinstellungen zurücksetzen, indem sie auf die Schaltfläche **[Reset]** (Rücksetzen) klicken, wie in Abbildung „WBM-Seite „Wartung“ – Registerseite „Rücksetzen auf Default-Werte“ angezeigt. Beim Neustart des Switches wird der Webbrowser auf die Anmeldeseite umgeleitet, wie in Abbildung „Anmeldungsseite“ dargestellt. Bitte beachten Sie, dass es auf der Vorderseite des Gehäuses keine physische Taste für die Rücksetzung gibt. Deshalb müssen Benutzer die Schaltfläche **[Reset]** auf dieser Seite verwenden.

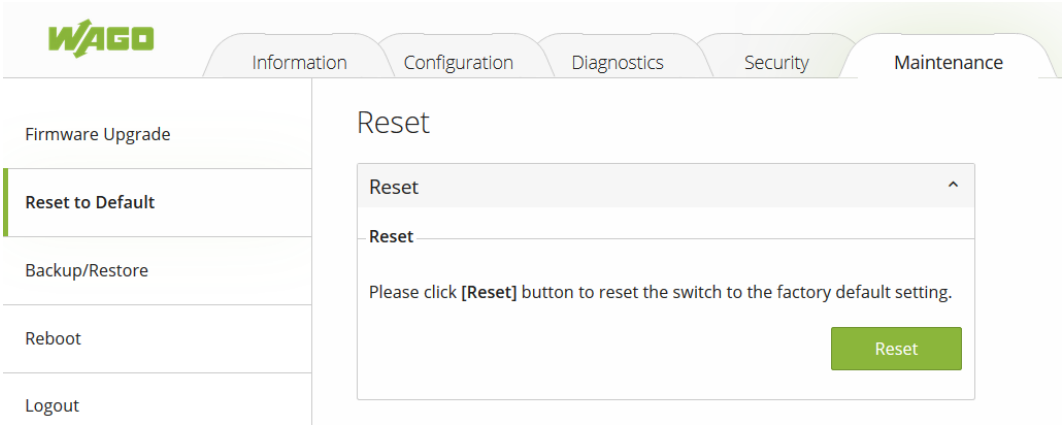

Abbildung 59: WBM-Seite „Wartung“ – Registerseite „Rücksetzen auf Default-Werte“

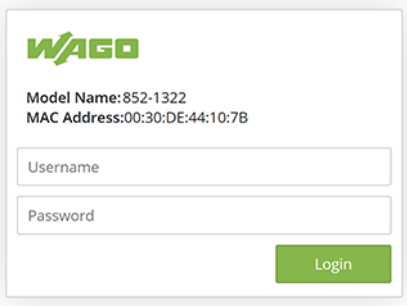

Abbildung 60: Anmeldungsseite (Beispiel)

10.8.3 Backup/Restore (Sichern/Wiederherstellen)

Auf der Registerseite „Sichern/Wiederherstellen“ können Benutzer die aktuelle Konfiguration des Switches in einer Datei speichern, die Konfigurationsdatei auf einem lokalen PC sichern oder eine neue Konfiguration aus einer zuvor gespeicherten Konfigurationsdatei hochladen. Die Abbildung „WBM-Seite „Wartung“ – Registerseite „Sichern/Wiederherstellen“ zeigt die Registerseite „Sichern/Wiederherstellen“, die in zwei Bereiche unterteilt werden kann: Sichern der Konfiguration und Wiederherstellen der Konfiguration.

Durch einen Klick auf die Schaltfläche **[Download]** (Herunterladen) im oberen Bereich der Seite (Feld „Backup the Configuration“) werden Benutzer durch den Webbrowser aufgefordert, die Datei „852-1322_XXX.XXX.XXX.XXX.ini“ zu speichern. Durch die Auswahl „Datei speichern“ wird die aktuelle Konfiguration des Switches auf dem Laufwerk des lokalen PCs gespeichert.

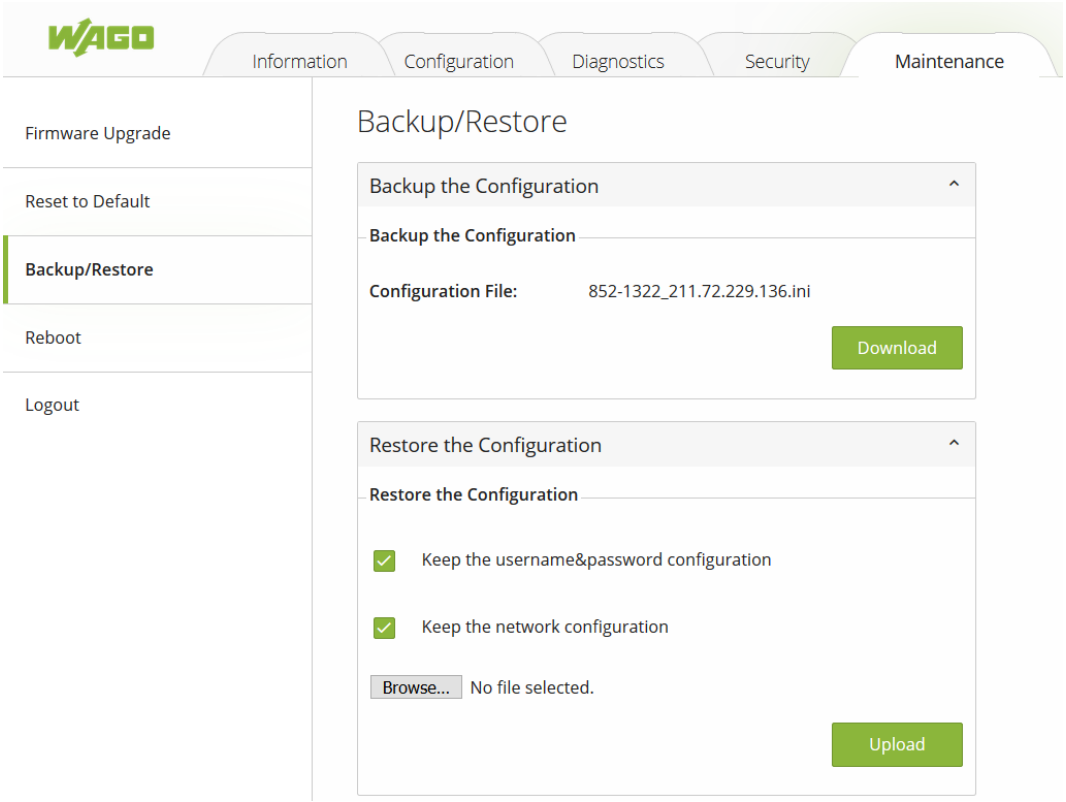

Abbildung 61: WBM-Seite „Wartung“ – Registerseite „Sichern/Wiederherstellen“

Zur Wiederherstellung einer Konfiguration auf dem Switch klicken Sie auf die Schaltfläche **[Browse…]** und wählen eine Konfigurationsdatei vom Laufwerk Ihres lokalen PCs aus. Vor dem Klick auf die Schaltfläche **[Upload]** (Hochladen) können Sie prüfen, ob Sie eine der Optionen über dem Dateinamen auswählen möchten. Dazu gehören „Keep the username & password configuration“ (Konfiguration von Benutzername und Passwort beibehalten) und „Keep the network configuration“ (Netzwerkkonfiguration beibehalten). Diese beiden Optionen helfen dabei, die unnötige Anmeldung im Switch nach der Widerherstellung der Einstellungen mit zuvor gespeichertem Benutzernamen, Passwort und/oder Netzwerkkonfiguration zu vermeiden.

10.8.4 Reboot (Neustart)

Auf dieser Registerseite gibt es eine einfache Reboot-Funktion, für die ein einzelner Klick auf die Schaltfläche **[Reboot]** genügt, wie in Abbildung „WBM-Seite „Wartung“ – Registerseite „Rebooten““ angezeigt.

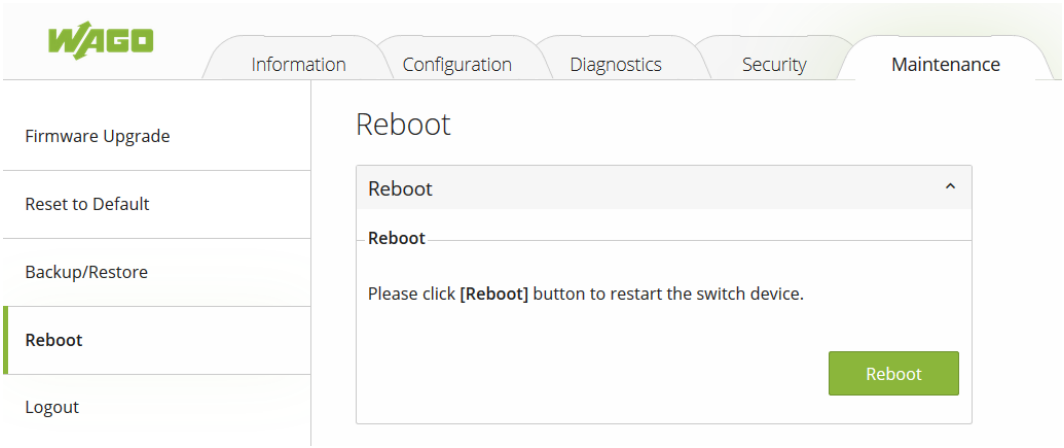

Abbildung 62: WBM-Seite „Wartung“ – Registerseite „Rebooten“

10.8.5 Logout (Abmelden)

Hinsichtlich der Security ist es eine bewährte Vorgehensweise, wenn sich Benutzer vom Produkt abmelden, wenn sie Änderungen an der Systemkonfiguration abgeschlossen haben. Die Abmeldung wird dringend empfohlen, um zu verhindern, dass Benutzereinstellungen unbeabsichtigt oder durch nicht autorisierte Benutzer verändert werden. Die Abmeldung kann entweder durch Aufrufen der Abmeldeseite und einen Klick auf die Schaltfläche **[Logout]** (Abmelden) oder durch einen Klick auf die Schnellabmelde-Schaltfläche oben rechts auf der Seite erfolgen, wie in Abbildung „WBM-Seite „Wartung“ – Registerseite „Abmelden“ bzw. Abbildung „Schnellabmelde-Schaltfläche oben rechts auf der Seite“ angezeigt.

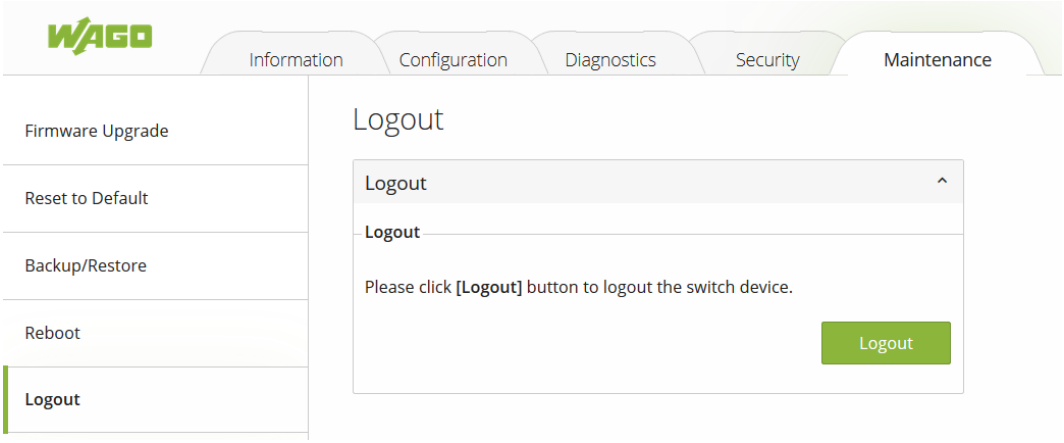

Abbildung 63: WBM-Seite "Maintenance" - Registerseite "Abmelden"

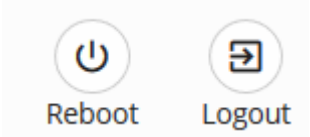

Abbildung 64: Schnellabmelde-Schaltfläche oben rechts auf der Seite

In Betrieb nehmen

Hinweis

Wichtige und nützliche Hinweise zur Inbetriebnahme finden Sie zu folgenden Themen, siehe die Kapitel:

- Systemeinstellungen: **System Settings (Systemeinstellungen) [▶ 36]**
- Netzwerkeinstellungen: **Network Settings (Netzwerkeinstellungen) [▶ 42]**
- Port-Einstellungen: **Setting (Einstellung) [▶ 43]**
- Passwort-Einstellungen: **Password (Passwort) [▶ 46]**
- Uhr-Einstellung: **SNTP-Einrichtung [▶ 39]**

Diagnose

ⓘ Hinweis

Zur Diagnose und Fehlerbehebung können folgende Themen nützlich sein, zu denen die folgenden Kapitel angegeben werden:

Diagnose über LED-Anzeigen:

- Diagnose mithilfe Produkt-LEDs: **Produkt-LEDs [▶ 18]**
- Diagnose mithilfe Anschluss-LEDs: **Anschluss-LEDs [▶ 19]**

Diagnose über WBM:

- Diagnose mithilfe des Netzwerkmanagements SNMP: **SNMP [▶ 47]**
- Diagnose im System Log: **System-Log (System-Log) [▶ 57]**
- Überwachung der Ports: **Port Monitor (Port-Überwachung) [▶ 60]**

Service

Hinweis

Zur Wartung können folgende Themen nützlich sein, zu denen die Kapitel in der Beschreibung der WBM angegeben werden:

- ein Upgrade der Firmware vornehmen: **Firmware Upgrade (Firmware-Upgrade) [▶ 79]**
- auf Werkseinstellungen zurücksetzen: **Reset to Default (Rücksetzen auf Default-Werte) [▶ 80]**
- Sichern und Wiederherstellen: **Backup/Restore (Sichern/Wiederherstellen) [▶ 81]**
- Rebooten: **Reboot (Neustart) [▶ 82]**
- Abmelden: **Logout (Abmelden) [▶ 82]**

Außer Betrieb nehmen

14.1 Entsorgung und Recycling

- Beachten Sie die nationalen und örtlichen Vorschriften für die Entsorgung von Batterien, Verpackungen und Elektro- und Elektronikgeräten.
- Löschen Sie im Elektro- und Elektronikgerät gespeicherte Daten.
- Entnehmen Sie im Elektro- und Elektronikgerät hinzugefügte Batterie, Akku oder Speicherkarte.
- Entsorgen Sie Verpackungen aller Art so, dass ein hohes Maß an Rückgewinnung, Wiederverwendung und Recycling möglich ist.
- Lassen Sie die Elektro- und Elektronikgeräte Ihrer örtlichen Sammelstelle zukommen.
- Europaweit gelten die Richtlinien 2006/66/EG, die PPWD 2018/852/EU und die WEEE 2012/19/EU. National können abweichende Richtlinien und Gesetze gelten.

Tabelle 43: WEEE-Kennzeichnung

Logo	Beschreibung
	Elektro- und Elektronikgeräte dürfen nicht über den Hausmüll entsorgt werden. Dies gilt auch für Produkte ohne diese Kennzeichnung.

Elektro- und Elektronikgeräte enthalten Materialien, Stoffe und Substanzen, die umwelt- und gesundheitsschädlich sein können. Elektro- und Elektronikgeräte müssen nach Nutzungsbeendigung ordnungsgemäß entsorgt werden. Eine umweltverträgliche Entsorgung dient der Gesundheit, schützt die Umwelt vor schädlichen Substanzen aus Elektro- und Elektronikgeräten und ermöglicht einen nachhaltigen und effizienten Umgang mit Ressourcen.

Anhang

15.1 MODBUS/TCP-Tabellen

15.1.1 Modbus-Register

Tabelle 44: Modbus-Register

Addresse	Data Type	Read/Write Lesen/ Schreiben	Beschreibung
Systeminformation			
0x0020 (32)	1 word	R	Firmwareversion =
			Bsp: Version = 1.02
			Word 0 Hi byte = 0x01
			Word 0 Lo byte = 0x02
0x0021 (33)	3 words	R	ETHERNET-MAC-Adresse
			Bsp: MAC = 00-01-02-03-04-05
			Word 0 Hi byte = 0x00
			Word 0 Lo byte = 0x01
			Word 1 Hi byte = 0x02
			Word 1 Lo byte = 0x03
			Word 2 Hi byte = 0x04
			Word 2 Lo byte = 0x05
0x0024 (36)	1 word	R	Kernel-Version
			Bsp: Version = 1.03
			Word 0 Hi byte = 0x01
			Word 0 Lo byte = 0x03
IP-Information			
0x0050 (80)	1 word	R	DHCP-Status
			0x0000: Disabled
			0x0001: Enabled
0x0051 (81)	2 words	R	IP Adresse des Switches
			Bsp: IP = 192.168.1.1
			Word 0 Hi byte = 0xC0
			Word 0 Lo byte = 0xA8
			Word 1 Hi byte = 0x01
			Word 1 Lo byte = 0x01
0x0053 (83)	2 words	R	Subnetzmaske des Switches
			Bsp: IP = 255.255.255.0
			Word 0 Hi byte = 0xFF
			Word 0 Lo byte = 0xFF
			Word 1 Hi byte = 0xFF
			Word 1 Lo byte = 0x00
0x0055 (85)	2 words	R	Gateway-Adresse des Switches
			Bsp: IP = 192.168.1.254
			Word 0 Hi byte = 0xC0
			Word 0 Lo byte = 0xA8
			Word 1 Hi byte = 0x01

Addresse	Data Type	Read/Write Lesen/ Schreiben	Beschreibung
			Word 1 Lo byte = 0xFE
Port Status			
0x1000 (4096)	5 words	R	Port-Status
			0x0000: Disabled
			0x0001: Enabled
			Word 0 Hi byte = Port 1 Status
			Word 0 Lo byte = Port 2 Status
			Word 1 Hi byte = Port 3 Status
			Word 1 Lo byte = Port 4 Status
			Word 2 Hi byte = Port 5 Status
			Word 2 Lo byte = Port 6 Status
			Word 3 Hi byte = Port 7 Status
			Word 3 Lo byte = Port 8 Status
			Word 4 Hi byte = Port 9 Status
			Word 4 Lo byte = Port 10 Status
0x1040 (4160)	5 words	R	Port-Geschwindigkeit
			Status, 10M = 0x01
			Status, 100M = 0x02
			Status, 1000M = 0x03
			Word 0 Hi byte = Port 1 Status
			Word 0 Lo byte = Port 2 Status
			Word 1 Hi byte = Port 3 Status
			Word 1 Lo byte = Port 4 Status
			Word 2 Hi byte = Port 5 Status
			Word 2 Lo byte = Port 6 Status
			Word 3 Hi byte = Port 7 Status
			Word 3 Lo byte = Port 8 Status
			Word 4 Hi byte = Port 9 Status
			Word 4 Lo byte = Port 10 Status
0x10A0 (4256)	5 words	R	Port-Link-Status
			Status, down = 0x00
			Status, up = 0x01
			Word 0 Hi byte = Port 1 Status
			Word 0 Lo byte = Port 2 Status
			Word 1 Hi byte = Port 3 Status
			Word 1 Lo byte = Port 4 Status
			Word 2 Hi byte = Port 5 Status
			Word 2 Lo byte = Port 6 Status
			Word 3 Hi byte = Port 7 Status
			Word 3 Lo byte = Port 8 Status
			Word 4 Hi byte = Port 9 Status
			Word 4 Lo byte = Port 10 Status

Tabellenverzeichnis

Tabelle 1 Legende zur Abbildung "Frontansicht des Industrial-Managed-Switches" 15
Tabelle 2 Legende zur Abbildung "Draufsicht des Industrial-Managed-Switches" 15
Tabelle 3 Legende zur Abbildung „Etikett“ 16
Tabelle 4 Legende zur Abbildung "Spannungsversorgungsanschluss" 17
Tabelle 5 Legende zur Abbildung "Netzwerkanschlüsse" 17
Tabelle 6 Legende zur Abbildung „Produkt-LEDs“ 18
Tabelle 7 Legende zur Abbildung „Anschluss-LEDs“ 19
Tabelle 8 Technische Daten – Produkt 19
Tabelle 9 Technische Daten – Systemdaten 19
Tabelle 10 Technische Daten – Spannungsversorgung 19
Tabelle 11 Technische Daten – Kommunikation 19
Tabelle 12 Technische Daten – Umgebungsanforderungen 20
Tabelle 13 Übersicht – Navigationslinks und WBM-Seiten 31
Tabelle 14 WBM-Seite „Informationen“ – Registerseite „Systeminformation“ 35
Tabelle 15 WBM-Seite „Konfiguration“ – Registerseite „Systemeinstellungen“ 37
Tabelle 16 WBM-Seite „Konfiguration“ – Registerseite „LLDP-Einstellungen“ 38
Tabelle 17 WBM-Seite „Konfiguration“ – Registerseite „SNTP“ 39
Tabelle 18 WBM-Seite „Konfiguration“ – Registerseite „SNTP“ 41
Tabelle 19 WBM- Seite „Konfiguration“ – Registerseite „Netzwerkeinstellungen“ 43
Tabelle 20 WBM- Seite „Konfiguration“ – Registerseite „Port-Einstellungen“ 44
Tabelle 21 WBM-Seite „Konfiguration“ – Registerseite „Mirror“ 45
Tabelle 22 WBM- Seite „Konfiguration“ – Registerseite „Passwort“ 46
Tabelle 23 WBM-Seite „Diagnose“ – Registerseite „Einstellungen für den SNMP-Agent“ 51
Tabelle 24 WBM-Seite „Diagnose“ – Registerseite „Einstellung für die SNMPv1/v2c Community“ 52
Tabelle 25 WBM-Seite „Diagnose“ – Registerseite „SNMP“, Abschnitt „SNMP Trap“ 53
Tabelle 26 WBM-Seite „Diagnose“ – Registerseite „SNMP“, Abschnitt „SNMP V3 Auth.“ 55
Tabelle 27 WBM-Seite „Diagnose“ – Registerseite „Modbus TCP“ 56
Tabelle 28 WBM-Seite „Diagnose“ – Registerseite „System Log“ – Abschnitt „Setting“ 57
Tabelle 29 WBM-Seite „Diagnose“ – Registerseite „System Log“ – Abschnitt „Log“ 59
Tabelle 30 Beschreibung der Log-Ereignisse 60
Tabelle 31 WBM-Seite „Diagnose“ – Registerseite „Port Monitor“ 61
Tabelle 32 WBM-Seite „Security“ – Registerseite „Static SAK“ 62
Tabelle 33 WBM-Seite „Security“ – Registerseite „802.1X“ – Abschnitt „Einstellungen“ 65
Tabelle 34 WBM-Seite „Security“ – Registerseite „802.1X“ – Abschnitt „802.1X – Parametereinstellungen“ 66
Tabelle 35 WBM-Seite „Security“ – Registerseite „802.1X“ – Abschnitt „802.1X – Port-Einstellungen“ 67

Tabelle 36 WBM-Seite „Security“ – Registerseite „Port-Security – Einstellungen“ 69
Tabelle 37 WBM-Seite „Security“ – Registerseite „Port-Isolation – Einstellungen 70
Tabelle 38 WBM-Seite „Security“ – Registerseite „VLAN-Einrichtung“ 73
Tabelle 39 WBM-Seite „Security“ – Registerseite „Management VLAN-Einrichtung“ 74
Tabelle 40 Weitere wichtige Begriffe 76
Tabelle 41 WBM-Seite „Redundanz“ – Registerseite „RSTP -Einrichtung“ 77
Tabelle 42 WBM-Seite „Redundanz“ – Registerseite „RSTP-Port-Einrichtung“ 78
Tabelle 43 WEEE-Kennzeichnung 86
Tabelle 44 Modbus-Register 87

Abbildungsverzeichnis

Abbildung 1 Frontansicht des Industrial-Managed-Switches ... 14
Abbildung 2 Draufsicht des Industrial-Managed-Switches ... 15
Abbildung 3 Etikett ... 16
Abbildung 4 Erdungsschraube ... 16
Abbildung 5 Spannungsversorgungsanschluss ... 17
Abbildung 6 Netzwerkanschlüsse ... 17
Abbildung 7 Produkt-LEDs ... 18
Abbildung 8 Anschluss-LEDs ... 19
Abbildung 9 RADIUS-Authentifizierungssequenz ... 23
Abbildung 10 Beispiel mit der Sniffer-Software Wireshark zur Anzeige der IP-Adresse eines Switches ... 29
Abbildung 11 Seite mit Sicherheitswarnung ... 30
Abbildung 12 WAGO-Anmeldeseite ... 30
Abbildung 13 Startseite des WBM ... 30
Abbildung 14 Pop-up-Warnung zum Default-Passwort auf der Passwort-Website ... 31
Abbildung 15 Anmeldefehlerdialog ... 32
Abbildung 16 Anmeldefehlerdialog mit Schaltfläche [Forget it] ... 33
Abbildung 17 Dialogbeispiel nach einem Klick auf die Schaltfläche [Forget it] ... 33
Abbildung 18 Beispiel einer Sicherheitskarte ... 33
Abbildung 19 Weiterleitung zur Registerseite für die Passwortänderung ... 34
Abbildung 20 WAGO-Anmeldedialog nach Passworterneuerung ... 34
Abbildung 21 WBM-Seite „Informationen“ – „Systeminformation“ ... 35
Abbildung 22 WBM-Seite „Informationen“ – „Rechtliche Information“ – Registerseite „WAGO-Lizenzen“ ... 36
Abbildung 23 WBM-Seite „Informationen“ – „Rechtliche Information“ – Registerseite „Open-Source-Lizenzen“ ... 36
Abbildung 24 Seite "Konfiguration" - Registerkarte "Systemeinsetllungen" ... 37
Abbildung 25 WBM-Seite „Konfiguration“ – Registerseite „LLDP Einstellungen“ ... 38
Abbildung 26 WBM-Seite „Konfiguration“ – Registerseite „SNTP“ ... 39
Abbildung 27 WBM-Seite „Konfiguration“ – Registerseite „SNTP“ ... 41
Abbildung 28 WBM-Seite „Konfiguration“ – Registerseite „Netzwerkeinstellungen“ ... 42
Abbildung 29 WBM-Seite „Konfiguration“ – Registerseite „Port-Einstellungen“ ... 44
Abbildung 30 WBM-Seite „Konfiguration“ – Registerseite „Mirror“ ... 45
Abbildung 31 WBM-Seite „Konfiguration“ – Registerseite „Passwort“ ... 46
Abbildung 32 WBM-Seite „Diagnose“ – Registerseite „SNMP Setting Teil 1“ ... 48
Abbildung 33 WBM-Seite „Diagnose“ – Registerseite „SNMP Setting Teil 2“ ... 49
Abbildung 34 WBM-Seite „Diagnose“ – Registerseite „SNMP Setting Teil 3“ ... 50

Abbildung 35 Einstellungen für den SNMP-Agent 51
Abbildung 36 Einstellung für die „SNMPv1/v2c Community“ 52
Abbildung 37 WBM-Seite „Diagnose“ – Registerseite „SNMP“, Abschnitt „SNMP Trap“ 53
Abbildung 38 WBM-Seite „Diagnose“ – Registerseite „SNMP“, Abschnitt „SNMP V3 Auth.“ 54
Abbildung 39 WBM-Seite „Diagnose“ – Registerseite „Modbus TCP“ 56
Abbildung 40 WBM-Seite „Diagnose“ – Registerseite „System Log“ – Abschnitt „Setting“ 57
Abbildung 41 WBM-Seite „Diagnose“ – Registerseite „System Log“ – Abschnitt „Log“ 58
Abbildung 42 Die Schaltfläche [Start] ist sichtbar, wenn das Kontrollkästchen bei „Automatic refresh cycle“ aktiviert ist. 59
Abbildung 43 WBM-Seite „Diagnose“ – Registerseite „Port Monitor“ 61
Abbildung 44 WBM-Seite „Security“ – Registerseite „Static SAK“ 62
Abbildung 45 Beispiel für Sicherheitscodes 63
Abbildung 46 WBM-Seite „Security“ – Registerseite „Sicherheitscode“ 63
Abbildung 47 WBM-Seite „Security“ – Registerseite „802.1X“ 64
Abbildung 48 WBM-Seite „Security“ – Registerseite „802.1X“ – Abschnitt „Einstellungen“ 65
Abbildung 49 WBM-Seite „Security“ – Registerseite „802.1X“ – Abschnitt „802.1X – Parametereinstellungen“ 66
Abbildung 50 WBM-Seite „Security“ – Registerseite „802.1X“ – Abschnitt „802.1X – Port-Einstellungen“ 67
Abbildung 51 WBM-Seite „Security“ – Registerseite „Port-Security“ 69
Abbildung 52 WBM-Seite „Security“ – Registerseite „Port-Isolation – Einstellung“ 70
Abbildung 53 WBM-Seite „Security“ – Registerseite „VLAN-Einrichtung“ 72
Abbildung 54 Management –VLAN - Beispiel 73
Abbildung 55 WBM-Seite „Security“ – Registerseite „Management VLAN-Einrichtung“ 74
Abbildung 56 WBM-Seite „Redundanz“ – Registerseite „RSTP-Einrichtung" 77
Abbildung 57 WBM-Seite „Redundanz“ – Registerseite „RSTP-Port-Einrichtung" 78
Abbildung 58 WBM-Seite "Maintenance" - Registerseite "Firmware-Upgrade" 80
Abbildung 59 WBM-Seite „Wartung“ – Registerseite „Rücksetzen auf Default-Werte“ 80
Abbildung 60 Anmeldungsseite (Beispiel) 80
Abbildung 61 WBM-Seite „Wartung“ – Registerseite „Sichern/Wiederherstellen“ 81
Abbildung 62 WBM-Seite „Wartung“ – Registerseite „Rebooten“ 82
Abbildung 63 WBM-Seite "Maintenance" - Registerseite "Abmelden" 82
Abbildung 64 Schnellabmelde-Schaltfläche oben rechts auf der Seite 82

WAGO Kontakttechnik GmbH & Co. KG
Postfach 2880 · 32385 Minden
Hansastraße 27 · D-32423 Minden
✉ **info@wago.com**
www.wago.com

Zentrale	+49 (0) 571/887 – 0
Vertrieb	+49 (0) 571/887 – 44 222
Auftragsservice	+49 (0) 571/887 – 44 333
Fax	+49 (0) 571/887 – 844 169