SpaceLogic KNX

BMS-IP-Gateway

LSS100300

Benutzeranleitung

10/22 – SpaceLogic KNX BMS-IP-Gateway

www.se.com

Schneider Electric

Rechtliche Hinweise

Die Marke Schneider Electric sowie alle Markenzeichen von Schneider Electric SE und seiner Niederlassungen, auf die in diesem Handbuch Bezug genommen wird, sind Eigentum von Schneider Electric SE oder seiner Niederlassungen. Alle anderen Marken sind Marken ihrer jeweiligen Inhaber.

Diese Anleitung und ihr Inhalt sind durch geltende Urheberrechtsgesetze geschützt und nur zu Informationszwecken zur Verfügung gestellt. Kein Teil dieses Handbuchs darf ohne vorherige schriftliche Genehmigung von Schneider Electric in irgendeiner Form oder mit irgendwelchen Mitteln (elektronisch, mechanisch, durch Fotokopie, Aufzeichnung oder auf andere Weise) zu irgendeinem Zweck vervielfältigt oder übertragen werden.

Schneider Electric gewährt weder Recht noch Erlaubnis zum gewerblichen Gebrauch des Handbuchs oder seines Inhalts, mit Ausnahme eines nicht exklusiven und persönlichen Einsichtsrechts bei aktuellem Stand. Die Produkte und Geräte von Schneider Electric sind nur durch qualifiziertes Personal zu installieren, zu bedienen, zu warten und instandzuhalten.

Da sich Normen, Spezifikationen und Bauformen von Zeit zu Zeit ändern, können sich die in diesem Handbuch enthaltenen Informationen jederzeit ohne Vorankündigung ändern.

Soweit dies gesetzlich zulässig ist, übernehmen Schneider Electric und seine Tochtergesellschaften keine Verantwortung oder Haftung für Fehler oder Auslassungen des Informationsinhalts dieses Materials oder für Folgen, die sich aus der Verwendung der hierin enthaltenen Informationen ergeben oder daraus resultieren.

Markennamen

Andere Marken und eingetragene Markennamen gehören den jeweiligen Eigentümern.

Warnhinweise

Lesen Sie die folgenden Anweisungen sorgfältig durch und machen Sie sich mit dem Hybrid-Modul vertraut, bevor Sie ihn installieren, bedienen und warten. Die nachstehend aufgeführten Warnhinweise sind in der gesamten Dokumentation zu finden und weisen auf mögliche Risiken und Gefahren oder auf spezifische Informationen hin, die ein Verfahren verdeutlichen oder vereinfachen.

Die Ergänzung eines Sicherheitshinweises („Gefahr“ bzw. „Warnung“) um ein Symbol weist auf eine elektrische Gefahr hin, die bei Missachtung der jeweiligen Anweisungen zu schweren Verletzungen führen kann.

Dieses Symbol steht für eine Sicherheitswarnung. Es weist auf die mögliche Gefahr von Personenschäden hin. Befolgen Sie alle Sicherheitshinweise mit diesem Symbol, um schwere oder gar tödliche Verletzungen zu vermeiden.

GEFAHR

GEFAHR weist auf eine unmittelbare Gefahrensituation hin, die bei Nichtbeachtung des Hinweises unweigerlich zu schweren oder tödlichen Verletzungen führt**.**

WARNUNG

WARNUNG weist auf eine mögliche Gefahr hin, die zum Tod oder zu schweren Verletzungen führen kann, wenn sie nicht vermieden wird.

ACHTUNG

ACHTUNG weist auf eine mögliche Gefahr hin, die zu leichten Verletzungen führen kann, wenn sie nicht vermieden wird.

HINWEIS

HINWEIS informiert über Verfahren, bei denen keine Verletzungsgefahr besteht.

Symbole

Zusätzliche Angaben

Die Angaben müssen unbedingt beachtet werden, da es sonst zu Programm- oder Datenfehlern kommen kann.

Inhaltsverzeichnis

1 Zu Ihrer Sicherheit

WARNUNG

GEFAHR DURCH ELEKTRISCHEN SCHLAG ODER LICHTBOGEN.

Eine sichere Elektroinstallation muss von qualifizierten Fachkräften ausgeführt werden. Qualifizierte Fachkräfte müssen fundierte Kenntnisse in folgenden Bereichen nachweisen:

- Anschluss an Installationsnetze
- Verbindung mehrerer elektrischer Geräte
- Verlegung von Elektroleitungen
- Anschluss und Errichtung von KNX-Netzwerken
- Sicherheitsnormen, örtliche Anschlussregeln und Vorschriften

Die Nichtbeachtung dieser Anweisung kann zum Tod oder schweren Verletzungen führen.

WARNUNG

GEFAHR VON FALSCHINFORMATIONEN

- Konfigurieren Sie die Software nicht falsch, da dies zu falschen Reports und/oder Datenergebnissen führen kann.
- Richten Sie Ihre Wartungs- und Instandhaltungsmaßnahmen nicht ausschließlich nach den von der Software angezeigten Meldungen und Informationen.
- Verlassen Sie sich nicht allein auf Softwaremeldungen und Reports, um festzustellen, ob das System korrekt funktioniert oder alle geltenden Normen und Anforderungen erfüllt.
- Berücksichtigen Sie die Auswirkungen von unvorhergesehenen Übertragungsverzögerungen oder Ausfällen von Kommunikationsverbindungen.

Bei Nichtbefolgung dieser Anweisungen besteht Lebensgefahr bzw. die Gefahr schwerwiegender Verletzungen sowie einer Beschädigung von Geräten.

Qualifiziertes Personal

Dieses Dokument richtet sich an das Personal, das für die Einrichtung, Installation, Inbetriebnahme und den Betrieb des Gerätes und des Systems, in dem es installiert ist, verantwortlich ist.

Detaillierte Kenntnisse, die durch eine Schulung im KNX-System erworben werden, sind Voraussetzung.

2 Einführung

SpaceLogic KNX BMS-IP-Gateway (nachfolgend **Gateway** genannt) ist ein Multifunktionsgerät, mit dem Sie KNX-Anlagen in Geräte der Gebäudeautomation integrieren können.

Die Hauptkommunikationsschnittstelle ist KNX TP und IP, die das BACnet-Protokoll unterstützt.

In einem Gerät sind drei Komponenten kombiniert:

- KNX IP-Router (max. 500 Objekte)
- KNX IP-Schnittstelle
- DPSU-Drossel

Das Gateway ermöglicht es professionellen Installateuren, KNX-Installationen dank einer Kombination von Funktionen kosten- und zeiteffizienter zu installieren.

Die Architektur ist einfacher, da die Verwendung von KNX-Routern und KNX-Spannungsversorgungen in Bezug auf bestimmte Parameter nicht mehr erforderlich ist.

Das Gateway ist für gewerbliche Anlagen bestimmt.

In dieser Dokumentation werden die Gateway-Anwendungssoftware, die Gerätefunktionen und die Benutzeroberfläche beschrieben.

2.1 Sicherheitsempfehlung

- Die Netzwerksicherheit muss auf der entsprechenden Ebene festgelegt werden. Das Gateway sollte Teil eines sicheren Netzwerks mit eingeschränktem Zugriff sein. Bei einer Internetverbindung wird die Verwendung eines VPN- oder HTTPS-Kanals dringend empfohlen.
- Verwenden Sie den Sicherheitsprotokollzugang HTTPS://IP:Port.
- Die Sicherheitsmethode wird durch die Fähigkeit anderer Netzwerkelemente bestimmt (Firewall, Schutz vor Viren und Malware-Bedrohungen).
- Es wird dringend empfohlen, die Dateien mit den Sicherungskopien an einem sicheren Ort aufzubewahren, zu dem Unbefugte keinen Zugang haben.
- Stellen Sie sicher, dass Ihr Gateway über keine öffentlich zugängliche IP-Adresse verfügt.
- Verwenden Sie keine Portweiterleitung, um über das öffentliche Internet auf Ihr Gateway zuzugreifen.
- Das Gateway sollte sich in seinem eigenen Netzwerksegment befinden.
- Wenn Ihr Router ein Gastnetzwerk oder VLAN unterstützt, ist es besser, Ihr Gateway dort unterzubringen.

Falls Sie Cybersicherheitsvorfälle oder Schwachstellen feststellen, kontaktieren Sie uns bitte über diese Seite:
https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp.
Weitere Informationen zur Systemhärtung finden Sie hier:
https://www.se.com/ww/en/download/document/AN002_107/.

HINWEIS

MATERIALSCHÄDEN DURCH UNBERECHTIGTEN ZUGRIFF AUF DIE KNX-ANLAGE

Sobald Sie über das Internet auf die KNX-Anlage zugreifen, kann der Datenverkehr von Dritten gelesen werden.

- Verwenden Sie für diese Verbindung nur einen VPN-Zugriff mit einer sicheren Verschlüsselung für alle Datenpakete.
- Die erforderliche Hardware (VPN-Router) und die Funktionen der Mobilfunkanbieter unterscheiden sich je nach Land bzw. Region erheblich in Bezug auf die Einstellungen und technischen Möglichkeiten.
- Lassen Sie den VPN-Zugriff immer von einem spezialisierten VPN-Dienstanbieter einrichten und in Betrieb nehmen. Der VPN-Dienstanbieter wählt einen geeigneten Mobilfunkanbieter und geeignete Hardware für den VPN-Zugriff aus und stellt sicher, dass das VPN von einem qualifizierten Fachmann eingerichtet wird.

Schneider Electric kann nicht für Leistungsprobleme und Inkompatibilitäten verantwortlich gemacht werden, die durch Anwendungen, Dienste oder Geräte von Drittanbietern verursacht werden. Schneider Electric bietet bei der Einrichtung eines VPN-Zugriffs keinen technischen Support.

Bei Missachtung dieser Anweisungen besteht Beschädigungsgefahr.

Der VPN-Zugang (VPN = Virtual Private Network) erlaubt dem tragbaren Gerät, über das Internet auf das lokale Netzwerk und damit auch auf die KNX-Anlage zuzugreifen.

Vorteile von VPN:

- Nur autorisierte Benutzer haben Zugriff auf das lokale Netzwerk.
- Alle Daten werden verschlüsselt.
- Die Daten werden während der Übertragung nicht geändert, aufgezeichnet oder umgeleitet. Dies wird oft als VPN-Tunnel bezeichnet.

Voraussetzungen für die Einrichtung einer VPN-Verbindung:

- Internetverbindung.
- Das tragbare Gerät und der Router sind für eine VPN-Verbindung aktiviert (VPN-Client installiert).
- Das Gateway sollte sich in seinem eigenen Netzwerksegment befinden.
- Wenn Ihr Router ein Gastnetzwerk oder VLAN unterstützt, ist es besser, Ihr Gateway dort unterzubringen.

2.2 Sicheres Kennwort erstellen

- Bei Ihrem Kennwort kann es sich um eine beliebige Kombination aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen handeln.
- Verwenden Sie mindestens 8 Zeichen.
- Erstellen Sie Ihr Passwort so, dass es schwer zu erraten oder in den Wörterbüchern von Cyberkriminellen zu finden ist.
- Bevorzugen Sie Sätze.
- Ändern Sie Ihr Kennwort regelmäßig, mindestens einmal im Jahr.
- Ändern Sie das Standard-Administratorkennwort sofort nach Erhalt und nach einer Rücksetzung auf die Werkseinstellungen.
- Verwenden Sie niemals Ihre Kennwörter erneut.

3 Gerätespezifikation

Spezifikation	Beschreibung	Hinweis
Klemmen, Schnittstelle	1 x RJ45 – Ethernet 10BaseT/100BaseTx 1 x KNX TP 1 x Reset-Drucktaster	
Konnektivität	IP LAN-Anschluss 10/100 Mbit KNX / EIB TP-Bus	
LED-Anzeigen	2 x LED, CPU, (Betrieb + Reset)	
KNX IP-Routing	500 Objekte (automatisch deaktiviert, wenn dieser Grenzwert überschritten wird)	Sie können bis zu 4000 BACnet-Punkte verwenden. Siehe Leistung → 10.
KNX IP-Tunneling	Für die Inbetriebnahme von KNX-Geräten über ETS	
KNX TP-Begrenzung	Die Bandbreitenbegrenzung des KNX TP-Mediums ist auf 9,6 kBit/s begrenzt. Auf jeder einzelnen KNX TP-Linie können zwischen 20 und 40 Telegramme pro Sekunde übertragen werden.	
BS (Firmware)	Flashsys	
Anwendungen	Integrierte Konfigurationsanwendung mit Webserver.	
IP-Schnittstelleneinstellung	Standardmäßig – statische IP 192.168.0.10/255.255.255.0	
BACnet-Protokollversion	22	
BACnet-Geräteprofil	B – ASC, B – GW	

4 Kompatibilität

Das Gateway entspricht folgenden Normen:

- KNX/EIB TP
- KNXnet/IP
- BACnet IP

5 Leistung

Parameter	Hinweis	
Anzahl der BACnet-Objekte	4000	Die maximale Anzahl an Punkten, die in dem virtuellen BACnet-Gerät im Gateway definiert werden können. Objekte, deren Grenzwert überschritten wird, werden stillschweigend verworfen.
Anzahl der BACnet-Abonnement (COV)-Anfragen	4000 (1500*)	Max. Anzahl der vom Gateway akzeptierten BACnet-Abonnement (COV)-Anfragen.
KNX-Kommunikationsobjekte	4000	Max. Anzahl verschiedener KNX-Gruppenadressen, die importiert/definiert werden können.

*Die Unterstützung von BACnet COV ermöglicht eine schnelle Datenkommunikation bei gleichzeitiger Reduzierung des BACnet-Netzwerkverkehrs.

*1500 für SXWAUTSVR10001 - Automatisierungsserver von Schneider Electric.

6 Erste Schritte

Stellen Sie vor dem Start sicher, dass das Gateway ordnungsgemäß entsprechend den Installationsanweisungen verbunden ist.

Sie benötigen einen Standard-Webbrowser, um mit der Anwendung zu arbeiten und das Gateway einzurichten. Wir empfehlen den Webbrowser Google Chrome oder Mozilla Firefox.

Beim ersten Zugriff:

Standard-IP-Adresse

1. Geben Sie die Standard-IP-Adresse 192.168.0.10 in die Adressleiste Ihres Webbrowsers ein und klicken Sie auf *Eingabe*.

Das Gateway verwendet ein selbstsigniertes Zertifikat, und es erscheint die folgende Meldung:

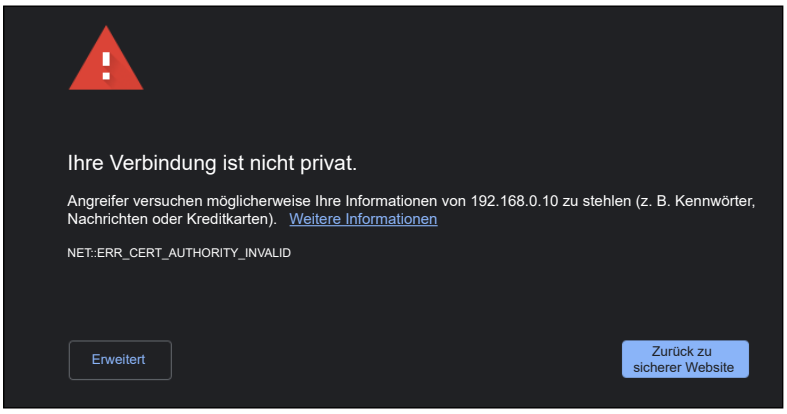

Abb. 1 Achtung: Ihre Verbindung ist nicht privat.

Standardmäßig verwendet das Gateway einen HTTPS-Kommunikationsmodus. Aufgrund der verwendeten selbstsignierten Zertifizierung müssen Sie die Ausnahme bestätigen, um fortfahren zu können. HTTPS ermöglicht eine verschlüsselte Kommunikation zwischen dem Gateway und dem Client.

2. Klicken Sie auf *Erweitert* > *Weiter mit 192.168.0.10*.

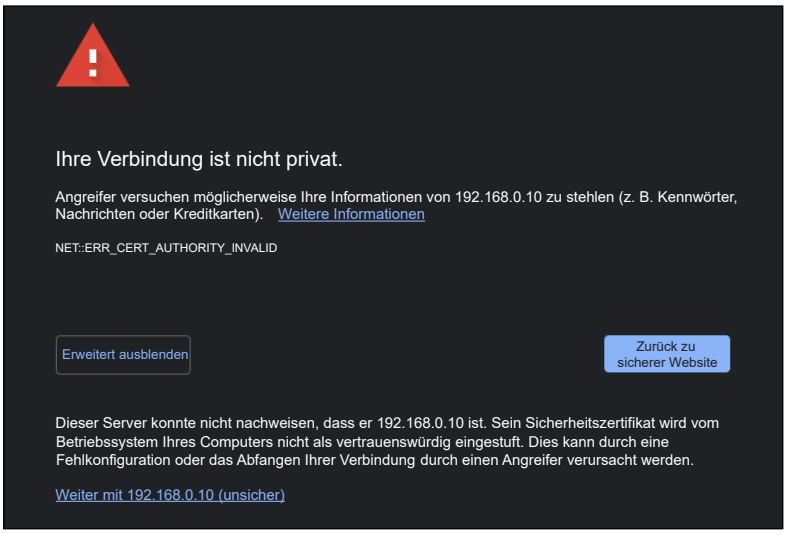

Abb. 2 Achtung: Weiter mit 192.168.0.10

Benutzername und Kennwort

3. Geben Sie die Standard-Anmeldedaten ein und klicken Sie auf *Eingabe*.

Benutzername: **admin**

Kennwort: **admin**

Aufforderung zur Kennwortänderung

4. Sie werden aufgefordert, Ihr Kennwort zu ändern. Geben Sie es ein und klicken Sie auf *Speichern*.

Das neue Kennwort muss mindestens 8 Zeichen lang sein und Folgendes beinhalten:

- einen Großbuchstaben
- einen Kleinbuchstaben
- eine Ziffer

Startseite

5. Als Nächstes gelangen Sie zur Startseite.

Abb. 3 Startseite

Sie finden dort:

- Spracheinstellungen
- Die Gateway-Einstellungen ( )
- Tool zum Filtern und Arbeiten mit Objekten
- Schaltfläche *KNX-Projekt importieren*

Spracheinstellungen

Wählen Sie zunächst im Dropdown-Menü die gewünschte Anwendungssprache aus.

Abb. 4 Wählen Sie Ihre Sprache aus

In den folgenden Schritten importieren Sie Ihr KNX-Projekt und stellen die Geräteparameter ein.

7 KNX-Projekt importieren

Über die Schaltfläche *KNX-Projekt importieren* rechts oben können Sie die Datei *.knxproj direkt in das Gateway importieren. Dabei wird die Struktur des Projekts und der DPTs der Gruppenadressen, einschließlich der automatischen Einheiten und Endungen, beibehalten.

Objekte mit demselben Namen werden als Duplikate betrachtet und möglicherweise nicht importiert und als verworfen markiert.

Sie können Objekte ohne definierte Datentypen hinzufügen und den Objekten auch Namen auf Strukturebene hinzufügen.

Kennwortgeschützte *.knxproj-Dateien erfordern ein in ETS festgelegtes Kennwort. Sie können das Projekt nicht importieren, ohne das richtige Kennwort zu kennen.

KNX-Projekt importieren

Gehen Sie vor wie folgt, um Ihr Projekt zu importieren:

1. Klicken Sie auf die Schaltfläche *KNX-Projekt importieren* und wählen Sie Ihre Datei aus.
2. Geben Sie ggf. das richtige Passwort ein.
3. Aktivieren Sie die Option *Pegelnamen zu Objekten hinzufügen*, wenn Sie auch Objektnamen und deren Strukturstandortbezeichnung importieren möchten.
4. Sie können das Kontrollkästchen *Bestehende Objekte überschreiben* aktivieren, wenn Sie bestehende Objekte überschreiben möchten.
5. Klicken Sie auf *Weiter*.

Die Filtertabellen werden automatisch entsprechend dem importierten KNX-Projekt ausgefüllt und können weiter bearbeitet werden.

Der Backbone-Schlüssel wird ebenfalls automatisch aus dem KNX-Projekt importiert.

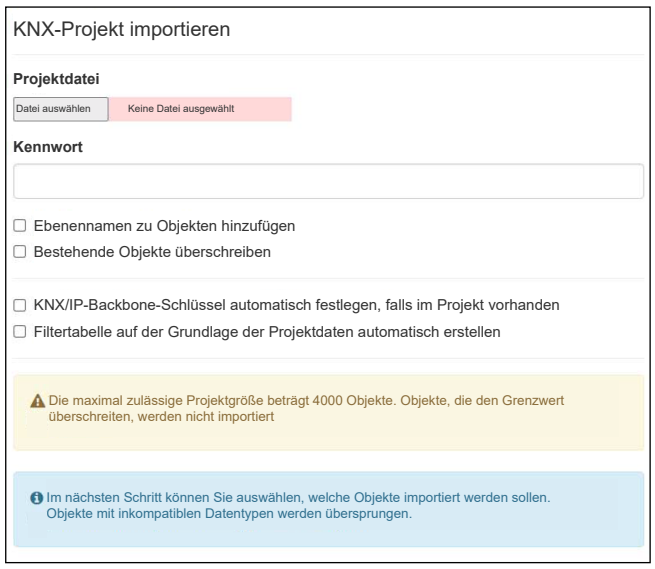

Abb. 5 Importieren Sie Ihr KNX-Projekt.

KNX-Routing kann für Projekte, die größer als 500 Objekte sind, nicht aktiviert werden.

Objekte auswählen, die importiert werden sollen

Im nächsten Schritt wählen Sie, welche Objekte Sie aus dem KNX-Projekt in BACnet exportieren möchten. Nur ausgewählte Objekte werden in die Gateway-Datenbank importiert.

Sie können Objekte nach Namen, Gruppenadresse oder Datentyp filtern, um das Auffinden Ihres Objekts zu erleichtern. Weitere Informationen hierzu finden Sie in Filtern und Ändern von Objekteigenschaften → 16.

Wählen Sie Ihre Objekte aus und klicken Sie auf *Weiter*.

Abb. 6 Objekte auswählen, die importiert werden sollen.

Importieren von Objekten abschließen

Es wird ein Popup-Fenster angezeigt, in dem Sie darüber informiert werden, wie viele Objekte importiert werden.

Abb. 7 Letztes Dialogfeld KNX-Projekt importieren.

Klicken Sie auf *OK*. Der Importvorgang ist abgeschlossen.

7.1 Objekt hinzufügen

Die Funktion *Objekt hinzufügen* ist nützlich, wenn Sie ein einzelnes Objekt zu einem späteren Zeitpunkt hinzufügen müssen und nicht die gesamte *.knxproj-Datei erneut importieren möchten.

Objekte hinzufügen

Gehen Sie wie folgt vor, um ein neues Objekt hinzuzufügen:

1. Klicken Sie auf *Objekt hinzufügen*.
2. Füllen Sie die Objektdetails aus.
3. Klicken Sie auf *Speichern*.

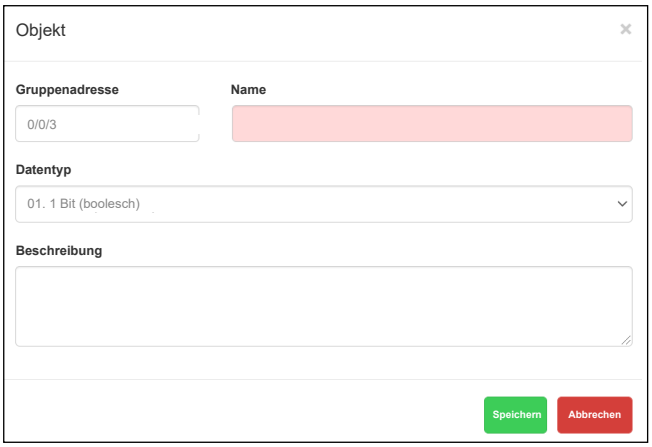

Abb. 8 Hinzufügen von Objekten.

7.2 Aktionen

Massenlöschung

Mit der Funktion *Massenlöschen* können Sie Objekte in großen Mengen löschen.

Sie haben zwei Optionen:

- *Alle Objekte löschen*
- *Objekte aus aktuellem Filter löschen*

Im nächsten Schritt werden die Objekte so gelöscht, wie Sie sie auswählen.

Abb. 9 Löschen von Objekten in großen Mengen

Mass edit (Massenbearbeitung)

Sie können Einheiten und COV-Inkremente Ihrer Objekte in großen Mengen bearbeiten.

1. Filtern Sie die Objekte, die Sie bearbeiten möchten.
2. Klicken Sie auf *Aktionen* > *Massenbearbeitung*.
3. Wählen Sie Parameter – Einheiten und/oder COV-Inkrementalwert aus und klicken Sie auf *Speichern*.

CSV exportieren

Sie können Objekte in eine .csv-Datei exportieren.

Klicken Sie auf *Aktionen* > *In CSV exportieren*.

Die .csv-Datei mit allen Objekten wird automatisch in Ihren lokalen *Downloads*-Ordner heruntergeladen, von wo aus Sie sie in MS Excel öffnen können.

7.3 Filtern und Ändern von Objekteigenschaften

Filtern von Objekten

Sie können Objekte nach Namen, Gruppenadresse oder Datentyp filtern. Sie können entweder im Dropdown-Menü auswählen oder eingeben, was Sie suchen.

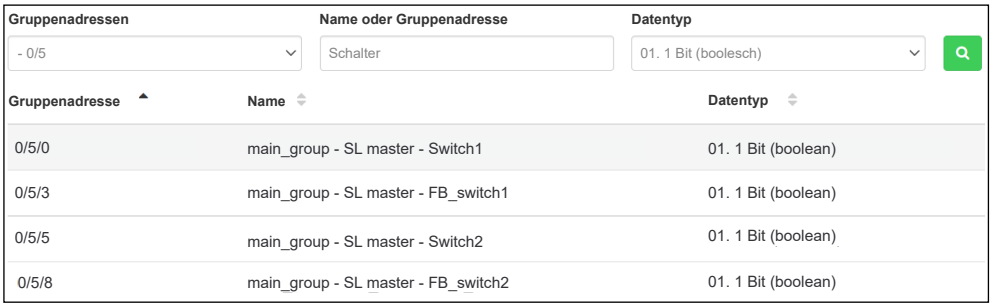

Abb. 10 Filtern von Objekten

Ändern der Objekteigenschaften

Sie können die Eigenschaften von Objekten und deren Werte später nach Bedarf bearbeiten. Oder Sie können sie einzeln löschen.

Gehen Sie wie folgt vor, um die Objekteigenschaften zu bearbeiten:

Bearbeiten der Objekteigenschaften

1. Klicken Sie auf .
2. Bearbeiten Sie die Objekteigenschaften.
3. Klicken Sie auf *Speichern*.

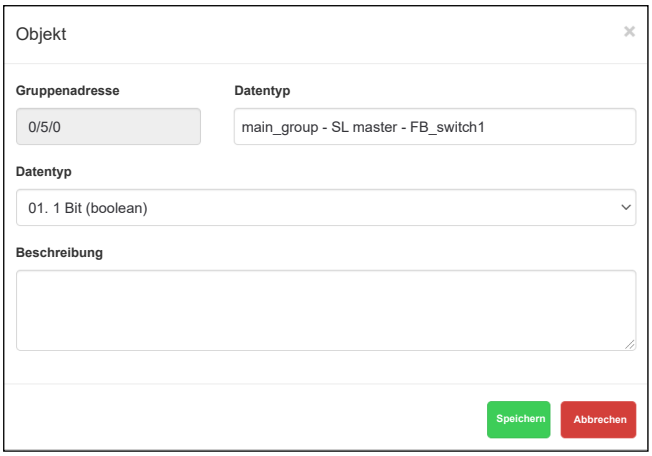

Abb. 11 Bearbeiten von Objekteigenschaften

Festlegen des Objektwerts

Sie können den Wert Ihres Objekts festlegen.

1. Klicken Sie auf .
2. Wählen Sie in der Dropdown-Liste *Wert* die Option aus.
3. Klicken Sie auf *Einstellung*.

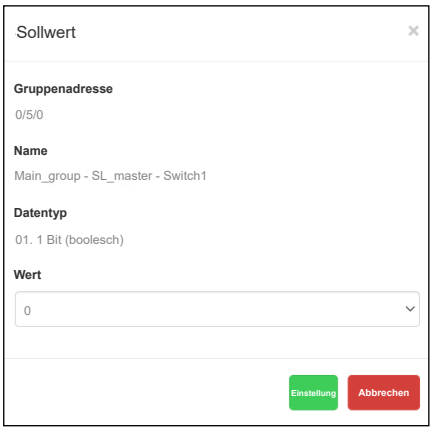

Abb. 12 Einstellen des Objektwerts

Löschen des Objekts

Wenn Sie ein Objekt löschen möchten, klicken Sie auf . Klicken Sie zur Bestätigung auf *Ja*.

Abb. 13 Löschen des Objekts

8 Anwendungseinstellungen

Nachdem Sie die Benutzeroberfläche der Anwendung eingerichtet und das ETS-Projekt importiert haben, können Sie die einzelnen Parameter Ihres Gateways festlegen.

Im Hauptmenü stehen folgende Optionen zur Auswahl:

- Sicherung
- Wiederherstellen
- Kennwort ändern
- Hostname
- BACnet-Konfiguration
- KNX-Konfiguration
- Netzwerkkonfiguration
- HTTP-Serverkonfiguration
- HTTP SSL-Zertifikat
- NTP-Clientkonfiguration
- Datum und Uhrzeit
- Systemprotokoll
- Ping
- Identifizierung der Schaltvorrichtung
- Firmware aktualisieren
- Zurücksetzen auf Werkseinstellungen
- Neustart
- Herunterfahren

8.1 Sicherung

Der Zweck des Backups ist die Erstellung einer Kopie der Daten, die bei einem primären Datenfehler wiederhergestellt werden können.

Um eine Backupdatei zu erstellen, gehen Sie zu  und wählen Sie im Drop-down-Menü die Option *Sicherung* aus.

Ihre Backupdatei wird sofort in den Ordner *Downloads* des Browsers heruntergeladen. Der Name der Backupdatei besteht aus den folgenden Daten:

Hostname-backup-jjjj.mm.tt-hh.mm.bckp

Die aktuelle Uhrzeit und das Datum des Gateways werden bei der Erstellung des Backups verwendet. Sie können die Datei später umbenennen und in einem anderen Ordner speichern.

8.2 Wiederherstellen

Es wird eine Wiederherstellung durchgeführt, um verlorene, gestohlene oder beschädigte Daten in den ursprünglichen Zustand zurückzuversetzen oder Daten an einen neuen Ort zu verschieben. Verwenden Sie Backupdateien, um die Gateway-Daten zu einem früheren Zeitpunkt wiederherzustellen.

Datenwiederherstellung

Gehen Sie wie folgt vor, um Ihre Daten wiederherzustellen:

1. Gehen Sie zu .
2. Klicken Sie auf *Wiederherstellen*.
3. Klicken Sie auf *Datei auswählen* und suchen Sie die Backupdatei.

Wenn Sie auch die Konfigurationsdateien wiederherstellen möchten, aktivieren Sie die Option *Konfigurationsdateien wiederherstellen*.

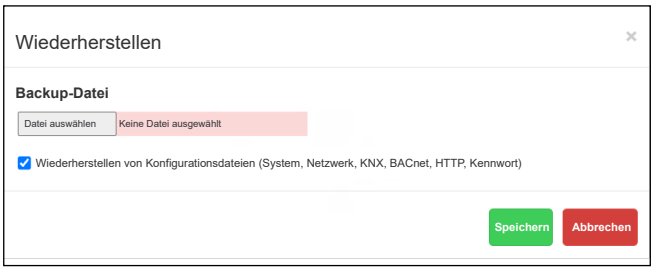

Abb. 14 Wiederherstellen der Anwendungskonfiguration

Nachdem Sie auf *Speichern* geklickt haben, wird ein Popup-Fenster mit der Frage angezeigt, ob Sie das System neu starten möchten. Wählen Sie *Ja* oder *Nein*. Wenn Sie *Nein* wählen, wird nichts importiert.

Abb. 15 Neustart des Systems

8.3 Kennwort ändern

Gehen Sie wie folgt vor, um Ihr Kennwort zu ändern:

1. Gehen Sie zu .
2. Klicken Sie auf *Kennwort ändern*.
3. Geben Sie Ihr aktuelles Kennwort und das neue Kennwort ein.
4. Klicken Sie auf *Speichern*.

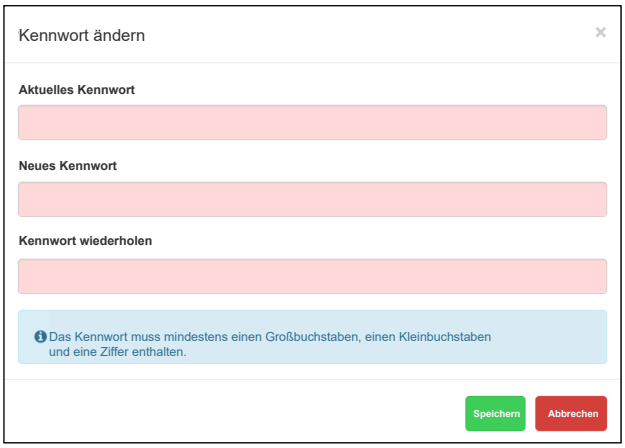

Abb. 16 Ändern des Kennworts

8.4 Hostname

Sie können den Hostnamen Ihres Gateways für eine einfache Identifizierung ändern. Er wird unter dem Namen der Sicherungsdatei angezeigt.

Gehen Sie wie folgt vor, um den Hostnamen zu ändern:

Hostnamen ändern

1. Gehen Sie zu .
2. Wählen Sie *Hostname* aus.
3. Geben Sie Ihren Hostnamen ein.
4. Klicken Sie auf *Speichern*.

8.5 BACnet-Konfiguration

BACnet-Server

Das Gateway fungiert als BACnet-Server. Es dient zur Datenlesbarkeit für BACnet-Client-Geräte, und BACnet-Client-Geräte können Daten auf den Server schreiben.

Das BACnet-Protokoll ermöglicht den Austausch von Informationen zwischen Geräten der Gebäudeautomation, unabhängig von der jeweiligen Gebäudedienstleistung, die sie erbringen.

Die Geräte werden über die Ethernet-Bitübertragungsschicht verbunden.

Die Verbindung zum BACnet-Netzwerk erfolgt über KNX-Gruppenobjekte, die nach BACnet exportiert werden.

Binäre Objekte erscheinen als binäre Werte, numerische Werte erscheinen als analoge Werte. Andere Datentypen werden nicht unterstützt.

BACnet-Konfiguration

1. Gehen Sie zu .
2. Wählen Sie *BACnet-Konfiguration* aus.

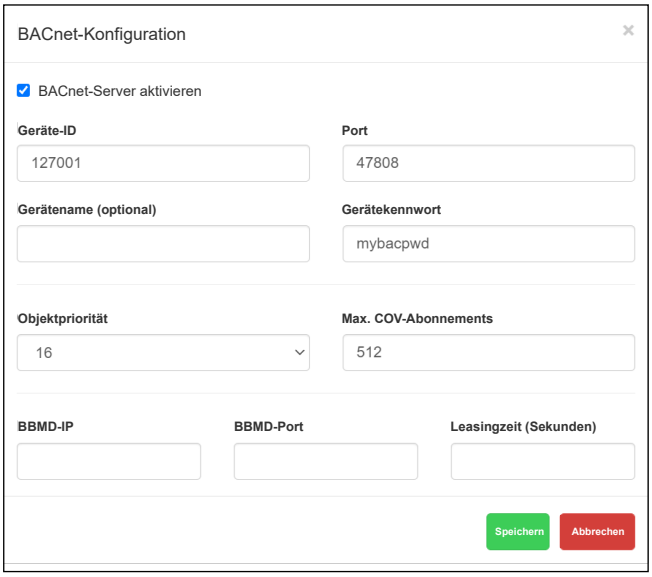

Abb. 17 BACnet-Konfiguration

3. Konfigurieren Sie die folgenden BACnet-Parameter und klicken Sie auf *Speichern*.

Parameter	Hinweis
BACnet-Server aktivieren	Standardmäßig deaktiviert
Geräte-ID	Eindeutige Netzwerk-ID auswählen
Port	BACnet-Port, standardmäßig 47808
Gerätename (optional)	Standardmäßig Hostname des Hubs_Geräte-ID Wenn Sie hier den Gerätenamen eingeben, ist BACnet-Name = Gerätename.
Gerätekennwort	BACnet-Kennwort Das Kennwort wird für BACnet-Dienste verwendet (z. B. "DeviceCommunicationControl"und "ReInitializeDevice" – Reinitialisierung des Geräts). Wenn kein Kennwort definiert ist, wird es nicht an das BACnet-Gerät gesendet.
Objektpriorität	Standardpriorität der Arrayposition
Max. COV-Abonnements	4000 (Siehe Leistung → 10).
BBMD-IP	BACnet-Router-IP
BBMD-Port	BACnet-Routerport
Leasingzeit (Sekunden)	BBMD-Registrierungs-Neusendungsintervall

8.6 KNX-Konfiguration

Im Menü *KNX-Konfiguration* können Sie die Detaileinstellung von KNX konfigurieren, wenn das Gateway in einer Rolle der KNX IP-Schnittstelle oder des Routers verwendet wird.

KNX-Konfiguration

1. Gehen Sie zu .
2. Klicken Sie auf *KNX-Konfiguration*.

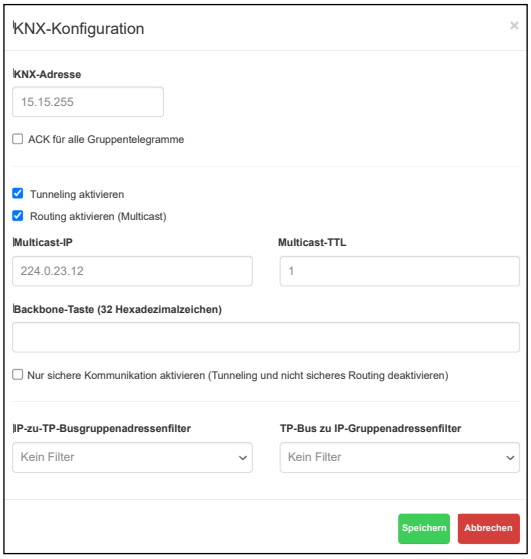

Abb. 18 KNX-Konfiguration

3. Konfigurieren Sie die folgenden BACnet-Parameter und klicken Sie auf *Speichern*.

Parameter	Hinweis
KNX-Adresse	KNX-Einzeladresse des Geräts. Standardmäßig 15.15.255.
ACK für alle Gruppentelegramme	Wenn das Gateway direkt mit einem anderen KNX-Gerät kommuniziert, muss es empfangene Telegramme quittieren. Deaktivieren Sie diese Option, wenn das Gateway nur als Sniffer von Gruppenadressen arbeitet.
Tunneling aktivieren	Ermöglicht mehreren Geräten den Anschluss an das öffentliche Netzwerk über dieselbe öffentliche IPv4-Adresse. Er ändert die IP-Adressinformationen in den IPv4-Headern während der Übermittlung durch ein Traffic-Routing-Gerät. IP-Anschluss, ist 1000-mal schneller als TP-UART. Das Gateway als Server. Unicast, quittierter Datenaustausch, zusätzliche Einzeladresse pro Tunneling-Verbindung.
Routing aktivieren (Multicast)	Multicast, nicht quittierte Datenübertragung. Das Gateway als Linien- oder Backbone-Koppler.
Multicast-IP	Multicast-IP-Adresse, standardmäßig 224.0.23.12.
Multicast-TTL	Der Standardwert ist 1; er ermöglicht die Kommunikation zwischen verschiedenen Subnetzen.
Backbone-Taste (32 Hexadezimalzeichen)	Backbone-Schlüssel zum Verschlüsseln und Entschlüsseln gesicherter Telegramme für IP-Routing.
Nur sichere Kommunikation zulassen -	Tunneling und ungesichertes Routing sind deaktiviert.

Parameter	Hinweis
IP-zu-TP-Busgruppenadressen-filter	Kein Filter
TP-Bus zu IP-Gruppenadres-senfilter	Ausgewählte Gruppenadressen akzeptieren Ausgewählte Gruppenadressen löschen Beispiele für Filtereinträge: - Einfache Adresse (1/1/1) - Bereich (1/1/1-1/1/100) - Platzhalter (1/1/* oder 1/*/*)

8.7 Netzwerkkonfiguration

Bei der Netzwerkkonfiguration werden die Steuerungen, der Fluss und der Betrieb eines Netzwerks festgelegt, um die Netzwerkkommunikation zu unterstützen. Nach der Einstellung der Netzwerkparameter muss das System neu gestartet werden, damit die Änderungen wirksam werden.

Netzwerkkonfiguration

1. Gehen Sie zu ☰.
2. Klicken Sie auf *Netzwerkkonfiguration*.

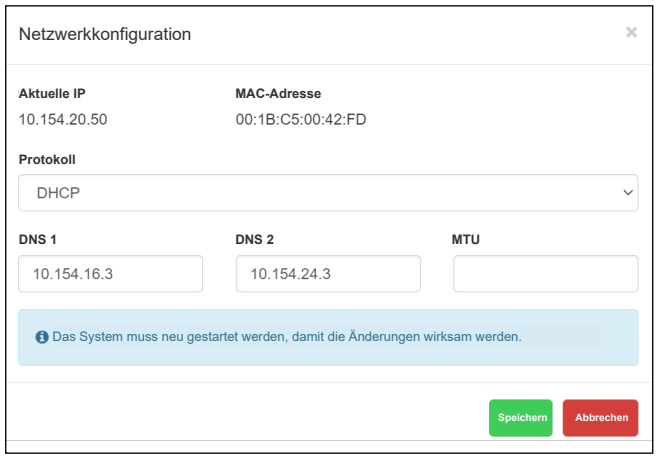

Abb. 19 Netzwerkkonfiguration

3. Konfigurieren Sie die folgenden Netzwerkparameter und klicken Sie auf *Speichern*.

Parameter	Hinweis
Aktuelle IP	Die vom DHCP-Server angegebene IP-Adresse oder die statische IP-Adresse. Dieses Feld erscheint nur, wenn die IP-Adresse angegeben ist, andernfalls wird es ausgeblendet.
MAC-Adresse	Jedes Gerät hat seine eigene eindeutige MAC-Adresse.
Protokoll	Spezifisches Protokoll, das für die Adressierung verwendet wird: Statische IP DHCP
IP-Adresse	Standardmäßig 192.168.0.10
Netzwerkmaske	Standardmäßig 255.255.255.0
Gateway-IP	Standardmäßig keine
DNS 1	IP-Adresse des primären DNS-Servers.

Parameter	Hinweis
DNS 2	IP-Adresse des sekundären DNS-Servers.
MTU	Maximale Übertragungseinheit, die größte Größe des Pakets, das im Kommunikationsprotokoll übergeben werden kann. (Standardmäßig 1500).

Klicken Sie im Popup-Fenster auf *Ja*, und bestätigen Sie den Neustart des Systems, damit die Änderungen wirksam werden.

Abb. 20 Neustart des Systems

8.8 HTTP-Serverkonfiguration

In diesem Abschnitt legen Sie die Sicherheitsstufe für die Kommunikation des Gateways mit dem Webserver und zusätzliche HTTP/S-Ports fest.

HTTP-Serverkonfiguration

1. Gehen Sie zu .
2. Wählen Sie *HTTPS-Serverkonfiguration* aus.

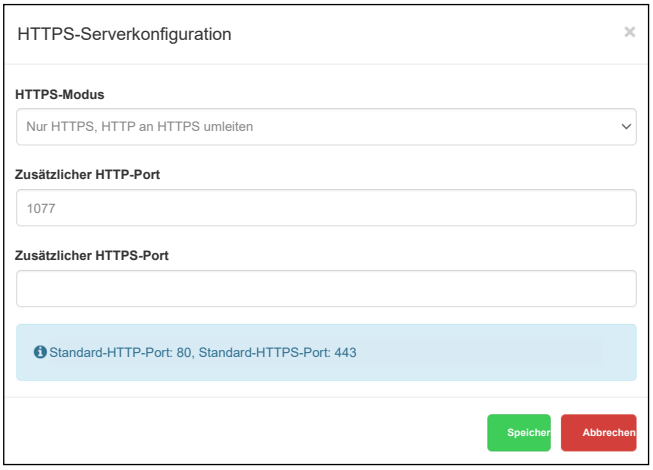

Abb. 21 Konfiguration des HTTP-Servers

3. Konfigurieren Sie die folgenden HTTPS-Serverparameter, und klicken Sie auf *Speichern*.
4. Neustart, damit die Änderungen wirksam werden.

Parameter	Hinweis
HTTPS-Modus	HTTP und HTTPS aktiviert Nur HTTPS, zu HTTPS umleiten Nur HTTPS, HTTP-Port ist deaktiviert
Zusätzlicher HTTP-Port	Wählen Sie die Nummer aus. (Standardmäßiger HTTP Port: 80.)
Zusätzlicher HTTPS-Port	Wählen Sie die Nummer aus. Standardmäßiger HTTPS Port: 443.

HTTPS-Modi:

- **HTTP und HTTPS aktiviert** – sowohl HTTP- als auch HTTPS-Kommunikation ist zulässig
- **Nur HTTPS, HTTP zu HTTPS umleiten** – die gesamte Kommunikation über HTTP-Ports wird zu HTTPS umgeleitet
- **Nur HTTPS, HTTP-Port ist deaktiviert** – nur gesicherte Kommunikation ist aktiviert

Aus Sicherheitsgründen wird der HTTPS-Kommunikationsmodus empfohlen.

8.9 HTTP SSL-Zertifikat

SSL-Zertifikate sind Datendateien, die einen kryptografischen Schlüssel digital mit den Daten eines Geräts verbinden. Wenn es auf einem Webserver installiert ist, aktiviert es das Vorhängeschloss und das HTTPS-Protokoll und ermöglicht sichere Verbindungen von einem Webserver zu einem Browser.

HTTP SSL-Zertifikatseinstellungen

1. Gehen Sie zu .
2. Klicken Sie auf *HTTP SSL-Zertifikat*.
3. Wählen Sie Ihren *Modus*:
   - *Neuen Privatschlüssel/Zertifikat hochladen*: Vorhandenen RSA-Schlüssel/SSL-Zertifikat hochladen
   - *Neuen Privatschlüssel/Zertifikat generieren*: RSA-Schlüssel/SSL-Zertifikat von einem bereits installierten generieren
4. Klicken Sie auf *Speichern*, und starten Sie neu, damit die Änderungen wirksam werden.

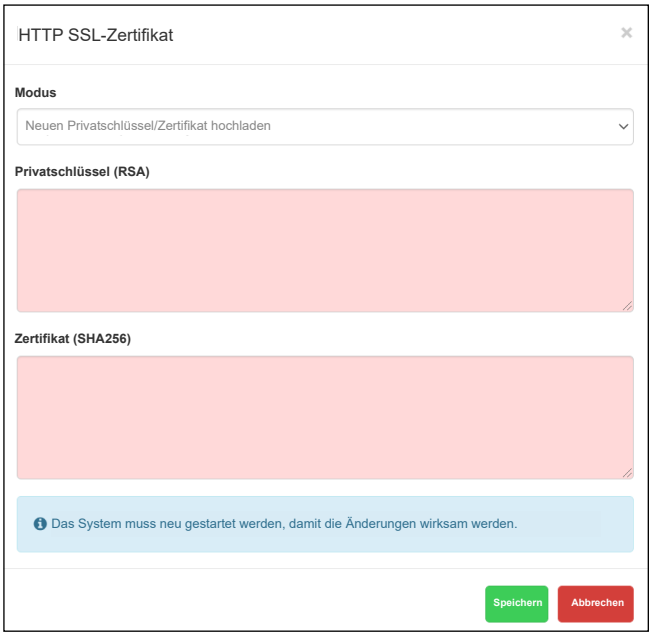

Abb. 22 HTTP SSL-Zertifikat

8.10 NTP-Clientkonfiguration

NTP (Network Time Protocol) dient der Synchronisierung aller teilnehmenden Geräte auf wenige Millisekunden genau mit der koordinierten Weltzeit (UTC). Es wurde entwickelt, um die Auswirkungen der variablen Netzwerklatenz zu minimieren.

Wenn der NTP-Client aktiviert ist, kann das Gateway Daten von bis zu 4 ausgewählten Servern erfassen (Priorität 1 bis 4 in einer Reihe).

Definieren Sie den Server, von dem Datum und Uhrzeit bezogen werden.

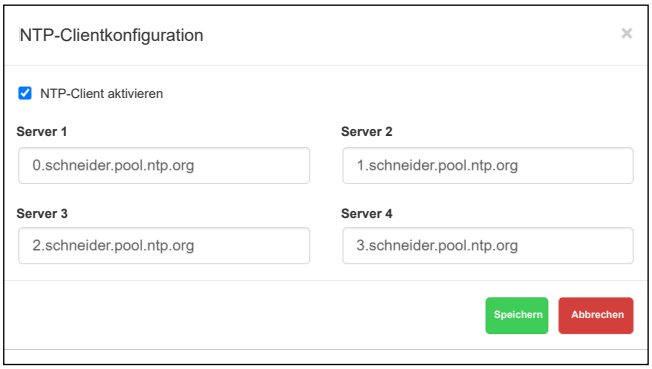

Abb. 23 NTP-Clientkonfiguration

Sie müssen nach der NTP-Clientkonfiguration einen Neustart durchführen.
Prüfen Sie bei Bedarf die Verfügbarkeit des NTP-Servers mit dem Ping-Tool.

8.11 Datum und Uhrzeit

Das Network Time Protocol (NTP) ist implementiert. Zusammen mit der Internetverbindung aktualisiert das Gateway automatisch die Zeit von einem NTP-Server.

Einstellung von Datum und Uhrzeit

1. Gehen Sie zu ☰.
2. Klicken Sie auf *Datum und Uhrzeit*.
3. Wenn keine Internetverbindung besteht, klicken Sie auf *Vom System übernehmen*, um die Zeit von Ihrem PC aus zu übernehmen.
4. Wählen Sie Ihre Zeitzone aus und klicken Sie auf *Speichern*.

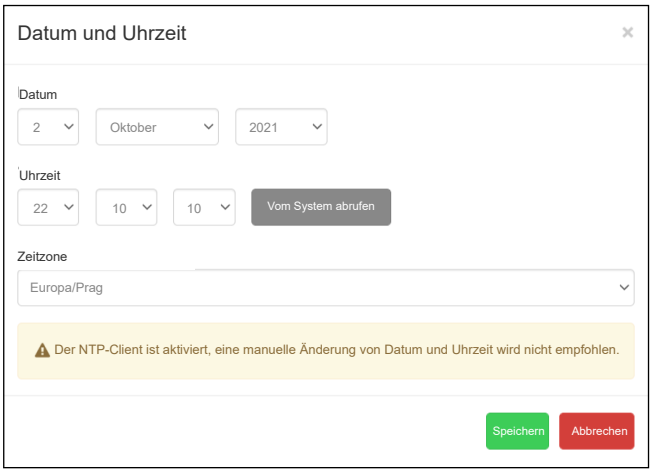

Abb. 24 Einstellung von Datum und Uhrzeit

8.12 Systemprotokoll

Das Gateway zeichnet jeden Systemstart und jede Trennung der TP/KNX-Verbindung auf. Transaktionen werden chronologisch in einer einfachen Protokolldatei aufgezeichnet. Die Protokolldatei wird automatisch vom Gateway erstellt und verwaltet.

Das Systemprotokoll wird angezeigt, wenn Sie zu wechseln und auf das *Systemprotokoll* klicken.

Unten sehen Sie die CPU-Lastinformationen.

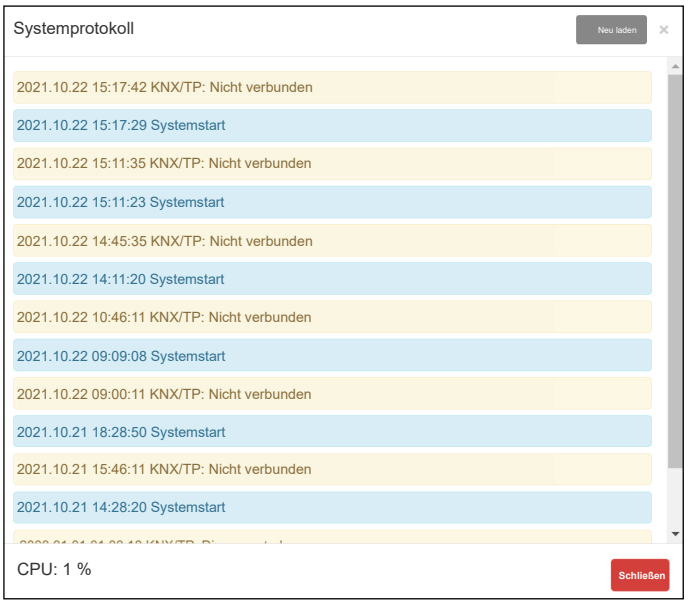

Abb. 25 Protokolldatei

8.13 Ping

Ping ist ein Tool zum Testen der Erreichbarkeit eines Hosts in einem IP-Netzwerk (Internet Protocol). Ping misst die Laufzeit (Pfad) für Pakete, die vom Ursprungshost an ein Ziel gesendet werden und an die Quelle zurückgesendet werden.

Pingen des Hosts

Gehen Sie wie folgt vor, um den Host zu pingen:

1. Gehen Sie zu .
2. Wählen Sie *Ping*.
3. Geben Sie die IP-Adresse oder den Hostnamen ein.
4. Klicken Sie auf *Ausführen*.

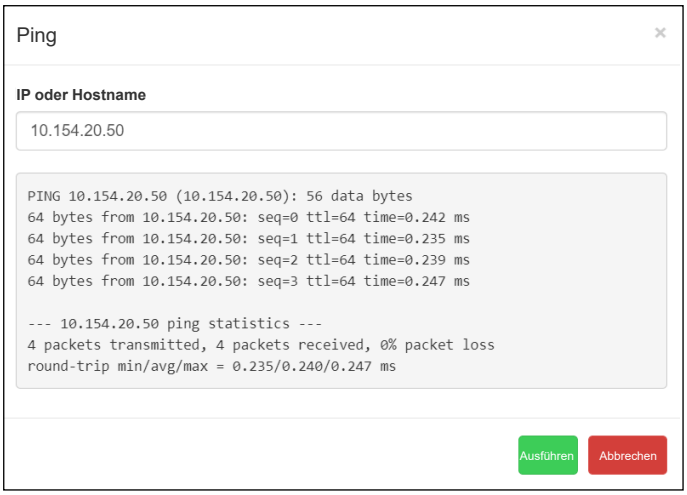

Abb. 26 Ping-Statistik.

8.14 Identifizierung der Schaltvorrichtung

Identifizierung der Schaltvorrichtung dient der Suche nach den einzelnen Gateway-Geräten in einem Netzwerk. Durch Einschalten der Identifizierung blinkt die LED 2 (rot/grün) am jeweiligen Gerät.

Identifizierung der Schaltvorrichtung

Gehen Sie zu ☰, klicken Sie auf *Identifizierung der Schaltvorrichtung*. Überprüfen Sie die Gerätesignalisierung.

8.15 Firmware aktualisieren

Bei einem Firmware-Upgrade wird das Gateway mit erweiterten Betriebsanweisungen aktualisiert, ohne dass eine Aktualisierung der Hardware erforderlich ist. Durch das Upgrade wird die Gateway-Konfiguration nicht geändert.

Während des Firmware-Upgrades reagiert das Gerät nicht und es startet mehrmals neu.

LED1 blinkt während des Upgrades rot/grün. Trennen Sie das Gateway nicht, während LED1 blinkt.

Firmware-Upgrade

1. Gehen Sie zu ☰.
2. Klicken Sie auf *Firmware aktualisieren*.
3. Wählen Sie Ihre Firmware-Datei aus.
4. Wählen Sie Ihre Signaturdatei aus.
5. Klicken Sie auf *Speichern*.

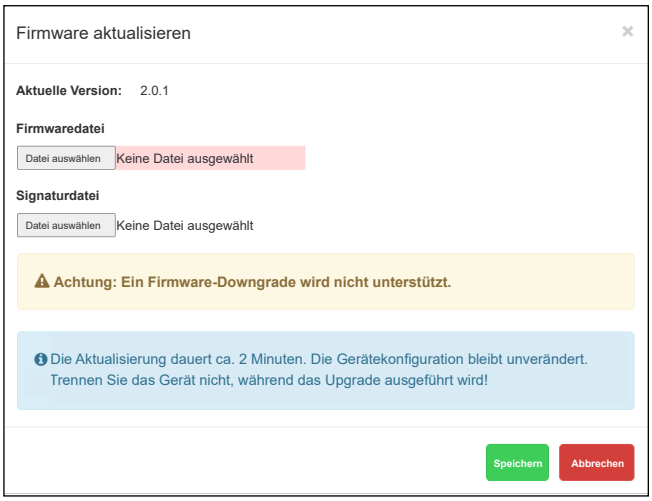

Abb. 27 Firmware wird aktualisiert.

Nach jeder Aktualisierung wird dringend empfohlen, den Browser-Cache zu leeren.

Ein Downgrade des Gateways mit Firmware wird nicht unterstützt.

Ohne Signaturdatei kann kein Upgrade durchgeführt werden. Die Firmware wird immer mit der entsprechenden Signaturdatei ausgeliefert.

8.16 Zurücksetzen auf Werkseinstellungen

Durch einen werkseitigen Reset werden alle Informationen auf dem Gateway gelöscht und die Software wird in ihren ursprünglichen Zustand zurückversetzt.

Es gibt zwei Möglichkeiten, das Gateway werkseitig zurückzusetzen:

- In der Anwendung
- Mit der Hardware-Reset-Taste

Anwendung Werkseinstellung

Um Ihr Gerät über die Anwendung zurückzusetzen, gehen Sie zu ☰, klicken Sie auf *Zurücksetzen auf Werkseinstellungen* und bestätigen Sie. Das System wird automatisch neu gestartet.

Abb. 28 Anwendung Werkseinstellung.

Die Geräteparameter nach einer Rücksetzung auf die Werkseinstellungen:

Parameter	Ergebnis
Gerätename	LSS100300
IP-Adresse	IP bleibt nach dem Zurücksetzen auf die Werkseinstellungen erhalten
Kein Objekt	Konfiguration als BACnet, KNX

Hardware-Werksreset

Zurücksetzten der Hardware auf Werkseinstellung eignet sich für Situationen, in denen das Gateway aufgrund fehlerhafter Einstellungen nicht verfügbar ist.

Drücken Sie die rote RESET-Taste an der Vorderseite lange (10 s). Lassen Sie die Taste los und drücken Sie sie erneut 10 Sekunden lang.

Die IP-Adresse nach einem Zurücksetzten der HW auf Werkseinstellung mit der Hardware-Taste ist immer 192.168.0.10.

3 HW-Tastertypen

Für <10 Sekunden gedrückt halten – Gerät neu starten

Für >10 Sekunden gedrückt halten – Netzwerk mit IP auf Werkseinstellung zurücksetzen

Für >10 Sekunden gedrückt halten und nochmals für >10 Sekunden gedrückt halten – vollständige Rücksetzung der Konfiguration auf die Werkseinstellungen

8.17 Neustart

Sie können das Gateway neu starten, wenn das Gerät nicht erwartungsgemäß funktioniert. Bei einem Neustart handelt es sich um einen einzigen Schritt, bei dem sowohl das Herunterfahren als auch das anschließende Einschalten durchgeführt wird.

Gateway neu starten

Um das Gerät neu zu starten, gehen Sie zu ☰, wählen Sie *Neustart* aus und klicken Sie auf *Ja*.

Abb. 29 Neustart des Gateways.

8.18 Herunterfahren

Beim *Herunterfahren* wird das Gateway so ausgeschaltet, dass kein Datenverlust entsteht und das System nicht beschädigt wird. Alle Einstellungen werden gespeichert.

Herunterfahren

Um Ihr Gerät ordnungsgemäß herunterzufahren, gehen Sie zu ☰ und wählen Sie *Herunterfahren* aus. Klicken Sie zur Bestätigung auf *Ja*.

Trennen Sie die Stromversorgung erst, wenn LED 1 (grün) aufhört zu blinken! Andernfalls kann es sein, dass die Datenbank nicht sicher gespeichert wird.

Die einzige Möglichkeit, das Gateway wieder einzuschalten, besteht darin, die Stromversorgung zu trennen und wieder anzuschließen.

Schneider Electric SA
35 rue Joseph Monier
92500 Rueil Malmaison - Frankreich
Telefon: +33 (0) 1 41 29 70 00
Fax: +33 (0) 1 41 29 71 00

Bei technischen Fragen wenden Sie sich bitte an das Customer Care Center in Ihrem Land.
schneider-electric.com/contact

LSS100300_SW_DE 10/22