SpaceLogic KNX BMS IP Gateway

LSS100300

Benutzerhandbuch

LSS 100300
Veröffentlichungsdatum: 07/2025

Schneider Electric

www.se.com

Rechtliche Hinweise

Die in diesem Dokument enthaltenen Informationen umfassen allgemeine Beschreibungen, technische Merkmale und Kenndaten und/oder Empfehlungen in Bezug auf Produkte/Lösungen.

Dieses Dokument ersetzt keinesfalls eine detaillierte Analyse bzw. einen betriebs- und standortspezifischen Entwicklungs- oder Schemaplan. Es darf nicht zur Ermittlung der Eignung oder Zuverlässigkeit von Produkten/Lösungen für spezifische Benutzeranwendungen verwendet werden. Es liegt im Verantwortungsbereich eines jeden Benutzers, selbst eine angemessene und umfassende Risikoanalyse, Risikobewertung und Testreihe für die Produkte/Lösungen in Übereinstimmung mit der jeweils spezifischen Anwendung bzw. Nutzung durchzuführen bzw. von entsprechendem Fachpersonal (Integrator, Spezifikateur oder ähnliche Fachkraft) durchführen zu lassen.

Die Marke Schneider Electric sowie alle anderen in diesem Dokument enthaltenen Markenzeichen von Schneider Electric SE und seinen Tochtergesellschaften sind das Eigentum von Schneider Electric SE oder seinen Tochtergesellschaften. Alle anderen Marken können Markenzeichen ihrer jeweiligen Eigentümer sein.

Dieses Dokument und seine Inhalte sind durch geltende Urheberrechtsgesetze geschützt und werden ausschließlich zu Informationszwecken bereitgestellt. Ohne die vorherige schriftliche Genehmigung von Schneider Electric darf kein Teil dieses Dokuments in irgendeiner Form oder auf irgendeine Weise (elektronisch, mechanisch, durch Fotokopieren, Aufzeichnen oder anderweitig) zu irgendeinem Zweck vervielfältigt oder übertragen werden.

Schneider Electric gewährt keine Rechte oder Lizenzen für die kommerzielle Nutzung des Dokuments oder dessen Inhalts, mit Ausnahme einer nicht-exklusiven und persönlichen Lizenz, es „wie besehen“ zu konsultieren.

Schneider Electric behält sich das Recht vor, jederzeit ohne entsprechende schriftliche Vorankündigung Änderungen oder Aktualisierungen mit Bezug auf den Inhalt bzw. am Inhalt dieses Dokuments oder dessen Format vorzunehmen.

Soweit nach geltendem Recht zulässig, übernehmen Schneider Electric und seine Tochtergesellschaften keine Verantwortung oder Haftung für Fehler oder Auslassungen im Informationsgehalt dieses Dokuments oder für Folgen, die aus oder infolge der sachgemäßen oder missbräuchlichen Verwendung der hierin enthaltenen Informationen entstehen.

Inhaltsverzeichnis

Sicherheitshinweise 5
- Bevor Sie beginnen 6
- Start und Test 7
- Betrieb und Einstellungen 8

Über das Handbuch 9

Einführung 12
- Sicherer Fernzugriff über VPN 12
- Best Practices für die Passwortsicherheit 13

Gerätespezifikation 14

Kompatibilität 15

Leistung 16

Erste Schritte 17

Importieren eines KNX-Projekts 19

Hinzufügen eines Objekts 21

Aktionen 22
- Massenlöschung von Objekten 22
- Massenbearbeitung von Objekten 22
- Objekte in eine CSV exportieren 22
- Filtern und Bearbeiten von Objekteigenschaften 23

Übersicht über die Anwendungseinstellungen 25
- Erstellen eines Backups 25
- Wiederherstellen einer Sicherung 26
- Passwort ändern 26
- Ändern des Gateway-Hostnamens 27
- BACnet-Konfiguration 27
- KNX-Konfiguration 28
- Netzwerkkonfiguration 29
- HTTP-Serverkonfiguration 30
- HTTP SSL-Zertifikat 31
- NTP-Client-Konfiguration 32
- Datum und Uhrzeit 33
- Systemprotokoll 33
- Ping 34
- Geräteidentifikation umschalten 34
- Firmware aktualisieren 35
- Zurücksetzen auf Werkeinstellungen 35
  - Zurücksetzen auf Anwendungswerkeinstellungen 36
  - Hardware-Reset auf Werkseinstellungen 36
- Neu starten 37
- Gateway herunterfahren und neu starten 37

Sicherheitshinweise

Wichtige Informationen

Lesen Sie sich diese Anweisungen sorgfältig durch und machen Sie sich vor Installation, Betrieb, Bedienung und Wartung mit dem Gerät vertraut. Die nachstehend aufgeführten Warnhinweise sind in der gesamten Dokumentation sowie auf dem Gerät selbst zu finden und weisen auf potenzielle Risiken und Gefahren oder bestimmte Informationen hin, die eine Vorgehensweise verdeutlichen oder vereinfachen.

Wird dieses Symbol zusätzlich zu einem Sicherheitshinweis des Typs „Gefahr“ oder „Warnung“ angezeigt, bedeutet das, dass die Gefahr eines elektrischen Schlags besteht und die Nichtbeachtung der Anweisungen unweigerlich Verletzung zur Folge hat.

Dies ist ein allgemeines Warnsymbol. Es macht Sie auf mögliche Verletzungsgefahren aufmerksam. Beachten Sie alle unter diesem Symbol aufgeführten Hinweise, um Verletzungen oder Unfälle mit Todesfälle zu vermeiden.

⚠ GEFAHR

GEFAHR macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, Tod oder schwere Verletzungen **zur Folge hat.**

⚠ WARNUNG

WARNUNG macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, Tod oder schwere Verletzungen **zur Folge haben kann.**

⚠ VORSICHT

VORSICHT macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, leichte Verletzungen **zur Folge haben kann.**

HINWEIS

HINWEIS gibt Auskunft über Vorgehensweisen, bei denen keine Verletzungen drohen.

Wird dieses Symbol zusätzlich zu einem Sicherheitshinweis des Typs „Gefahr“ oder „Warnung“ angezeigt, bedeutet das, dass die Gefahr eines elektrischen Schlags besteht und die Nichtbeachtung der Anweisungen unweigerlich Verletzung zur Folge hat.

Dies ist ein allgemeines Warnsymbol. Es macht Sie auf mögliche Verletzungsgefahren aufmerksam. Beachten Sie alle unter diesem Symbol aufgeführten Hinweise, um Verletzungen oder Unfälle mit Todesfälle zu vermeiden.

⚠ GEFAHR

GEFAHR macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, Tod oder schwere Verletzungen **zur Folge hat.**

⚠ WARNUNG

WARNUNG macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, Tod oder schwere Verletzungen **zur Folge haben kann.**

⚠ VORSICHT

VORSICHT macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, leichte Verletzungen **zur Folge haben kann.**

HINWEIS

HINWEIS gibt Auskunft über Vorgehensweisen, bei denen keine Verletzungen drohen.

Bitte beachten

Elektrische Geräte dürfen nur von Fachpersonal installiert, betrieben, bedient und gewartet werden. Schneider Electric haftet nicht für Schäden, die durch die Verwendung dieses Materials entstehen.

Als qualifiziertes Fachpersonal gelten Mitarbeiter, die über Fähigkeiten und Kenntnisse hinsichtlich der Konstruktion und des Betriebs elektrischer Geräte und deren Installation verfügen und eine Schulung zur Erkennung und Vermeidung möglicher Gefahren absolviert haben.

Bevor Sie beginnen

Dieses Produkt nicht mit Maschinen ohne effektive Sicherheitseinrichtungen im Arbeitsraum verwenden. Das Fehlen effektiver Sicherheitseinrichtungen im Arbeitsraum einer Maschine kann schwere Verletzungen des Bedienpersonals zur Folge haben.

⚠WARNUNG

UNBEAUFSICHTIGTE GERÄTE

- Diese Software und zugehörige Automatisierungsgeräte nicht an Maschinen verwenden, die nicht über Sicherheitseinrichtungen im Arbeitsraum verfügen.
- Greifen Sie bei laufendem Betrieb nicht in das Gerät.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Dieses Automatisierungsgerät und die zugehörige Software dienen zur Steuerung verschiedener industrieller Prozesse. Der Typ bzw. das Modell des für die jeweilige Anwendung geeigneten Automatisierungsgeräts ist von mehreren Faktoren abhängig, z. B. von der benötigten Steuerungsfunktion, der erforderlichen Schutzklasse, den Produktionsverfahren, außergewöhnlichen Bedingungen, behördlichen Vorschriften usw. Für einige Anwendungen werden möglicherweise mehrere Prozessoren benötigt, z. B. für ein Backup-/Redundanzsystem.

Nur Sie als Benutzer, Maschinenbauer oder -integrator sind mit allen Bedingungen und Faktoren vertraut, die bei der Installation, der Einrichtung, dem Betrieb und der Wartung der Maschine bzw. des Prozesses zum Tragen kommen. Demzufolge sind allein Sie in der Lage, die Automatisierungskomponenten und zugehörigen Sicherheitsvorkehrungen und Verriegelungen zu identifizieren, die einen ordnungsgemäßen Betrieb gewährleisten. Bei der Auswahl der Automatisierungs- und Steuerungsgeräte sowie der zugehörigen Software für eine bestimmte Anwendung sind die einschlägigen örtlichen und landesspezifischen Richtlinien und Vorschriften zu beachten. Das National Safety Council's Accident Prevention Manual (Handbuch zur Unfallverhütung; in den USA landesweit anerkannt) enthält ebenfalls zahlreiche nützliche Hinweise.

Für einige Anwendungen, z. B. Verpackungsmaschinen, sind zusätzliche Vorrichtungen zum Schutz des Bedienpersonals wie beispielsweise Sicherheitseinrichtungen im Arbeitsraum erforderlich. Diese Vorrichtungen werden benötigt, wenn das Bedienpersonal mit den Händen oder anderen Körperteilen in den Quetschbereich oder andere Gefahrenbereiche gelangen kann und somit einer potenziellen schweren Verletzungsgefahr ausgesetzt ist. Software-Produkte allein können das Bedienpersonal nicht vor Verletzungen schützen. Die Software kann daher nicht als Ersatz für Sicherheitseinrichtungen im Arbeitsraum verwendet werden.

Vor Inbetriebnahme der Anlage sicherstellen, dass alle zum Schutz des Arbeitsraums vorgesehenen mechanischen/elektronischen Sicherheitseinrichtungen und Verriegelungen installiert und funktionsfähig sind. Alle zum Schutz des Arbeitsraums vorgesehenen Sicherheitseinrichtungen und Verriegelungen müssen mit dem zugehörigen Automatisierungsgerät und der Softwareprogrammierung koordiniert werden.

HINWEIS: Die Koordinierung der zum Schutz des Arbeitsraums vorgesehenen mechanischen/elektronischen Sicherheitseinrichtungen und Verriegelungen geht über den Umfang der Funktionsbaustein-Bibliothek, des System-Benutzerhandbuchs oder andere in dieser Dokumentation genannten Implementierungen hinaus.

Start und Test

Vor der Verwendung elektrischer Steuerungs- und Automatisierungsgeräte ist das System zur Überprüfung der einwandfreien Funktionsbereitschaft einem Anlauftest zu unterziehen. Dieser Test muss von qualifiziertem Personal durchgeführt werden. Um einen vollständigen und erfolgreichen Test zu gewährleisten, müssen die entsprechenden Vorkehrungen getroffen und genügend Zeit eingeplant werden.

⚠WARNUNG

GEFAHR BEIM GERÄTEBETRIEB

- Überprüfen Sie, ob alle Installations- und Einrichtungsverfahren vollständig durchgeführt wurden.
- Vor der Durchführung von Funktionstests sämtliche Blöcke oder andere vorübergehende Transportsicherungen von den Anlagekomponenten entfernen.
- Entfernen Sie Werkzeuge, Messgeräte und Verschmutzungen vom Gerät.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Führen Sie alle in der Dokumentation des Geräts empfohlenen Anlauftests durch. Die gesamte Dokumentation zur späteren Verwendung aufbewahren.

Softwaretests müssen sowohl in simulierten als auch in realen Umgebungen stattfinden.

Sicherstellen, dass in dem komplett installierten System keine Kurzschlüsse anliegen und nur solche Erdungen installiert sind, die den örtlichen Vorschriften entsprechen (z. B. gemäß dem National Electrical Code in den USA). Wenn Hochspannungsprüfungen erforderlich sind, beachten Sie die Empfehlungen in der Gerätedokumentation, um eine versehentliche Beschädigung zu verhindern.

Vor dem Einschalten der Anlage:

- Entfernen Sie Werkzeuge, Messgeräte und Verschmutzungen vom Gerät.
- Schließen Sie die Gehäusetür des Geräts.
- Alle temporären Erdungen der eingehenden Stromleitungen entfernen.
- Führen Sie alle vom Hersteller empfohlenen Anlauftests durch.

Betrieb und Einstellungen

Die folgenden Vorsichtsmaßnahmen stammen aus der NEMA Standards Publication ICS 7.1-1995:

(Im Falle einer Abweichung oder eines Widerspruchs zwischen einer Übersetzung und dem englischen Original hat der Originaltext in der englischen Sprache Vorrang.)

- Ungeachtet der bei der Entwicklung und Fabrikation von Anlagen oder bei der Auswahl und Bemessung von Komponenten angewandten Sorgfalt, kann der unsachgemäße Betrieb solcher Anlagen Gefahren mit sich bringen.
- Gelegentlich kann es zu fehlerhaften Einstellungen kommen, die zu einem unbefriedigenden oder unsicheren Betrieb führen. Für Funktionseinstellungen stets die Herstelleranweisungen zu Rate ziehen. Das Personal, das Zugang zu diesen Einstellungen hat, muss mit den Anweisungen des Anlagenherstellers und den mit der elektrischen Anlage verwendeten Maschinen vertraut sein.
- Nur die vom Bediener unbedingt vorzunehmenden betriebsspezifischen Einstellungen sollten für den Bediener zugänglich sein. Der Zugriff auf andere Steuerungsfunktionen sollte eingeschränkt sein, um unbefugte Änderungen der Betriebskenngrößen zu vermeiden.

Über das Handbuch

Ziel dieses Dokuments

In diesem Dokument werden Anwendungssoftware, Gerätefunktionen und Benutzeroberfläche des LSS100300 **BMS SpaceLogic KNX ratif IP Gateway** beschrieben.

Es richtet sich an Systemintegratoren, Ingenieure und technische Nutzer, die für die Einrichtung der Kommunikation zwischen KNX-Systemen und IP-basierten Gebäudemanagementsystemen (Rittal) verantwortlich sind.

Gültigkeitsbereich

Dieses Benutzerhandbuch gilt für die **BMS SpaceLogic KNX ratif IP Gateway**-Software ab der im Dokument angegebenen Softwareversion. Es gefasst sich mit der Konfiguration und die Bedienung der Softwarefunktionen, die zum Zeitpunkt der Veröffentlichung verfügbar sind.

Zukünftige Aktualisierungen, Erweiterungen oder Änderungen der Software werden in diesem Handbuch möglicherweise nicht berücksichtigt. Es wird empfohlen, die neueste Dokumentation zu Rate zu ziehen oder sich an den technischen Support zu wenden, um Informationen zu neueren Versionen oder zusätzlichen Funktionen zu erhalten.

Allgemeine Informationen zur Cybersicherheit

In den letzten Jahren hat sich durch die wachsende Anzahl an vernetzten Maschinen und Produktionsanlagen das Potenzial für Cyberbedrohungen wie unbefugter Zugriff, Datenverletzungen und Betriebsunterbrechungen entsprechend erhöht. Sie müssen daher alle möglichen Maßnahmen zur Cybersicherheit in Betracht ziehen, um Anlagen und Systeme vor solchen Bedrohungen zu schützen.

Um die Sicherheit und den Schutz Ihrer Schneider Electric-Produkte zu gewährleisten, ist es in Ihrem Interesse, die Best Practices für die Cybersicherheit umzusetzen, die im Dokument Cybersecurity Best Practices beschrieben sind.

Schneider Electric bietet zusätzliche Informationen und Unterstützung:

- Abonnieren Sie den Sicherheits-Newsletter von Schneider Electric.
- Besuchen Sie die Webseite Cybersecurity Support Portal, um:
  - Sicherheitshinweise zu suchen
  - Schwachstellen und Vorfälle zu melden
- Besuchen Sie die Webseite Schneider Electric Cybersecurity and Data Protection Posture, um:
  - auf den Cybersicherheitsstatus zuzugreifen
  - mehr über Cybersicherheit in der Cybersecurity Academy zu erfahren
  - die Cybersicherheits-Services von Schneider Electric zu entdecken

Produktbezogene Informationen zur Cybersicherheit

- Die Netzwerksicherheit muss ordnungsgemäß konfiguriert werden. Das Gateway sollte innerhalb eines sicheren Netzwerks mit eingeschränktem Zugriff betrieben werden. Wenn eine Verbindung zum Internet besteht, wird dringend ein **VPN** oder ein **HTTPS**-verschlüsselter Kanal empfohlen.
- Greifen Sie immer mit einem sicheren Protokoll auf das Gateway zu, z. B. `https://<IP>:<Port>`.
- Die globale Sicherheitsstufe hängt von den Funktionen anderer Netzwerkkomponenten ab, wie z. B. Firewalls und Schutz vor Viren und Malware.
- Sicherungsdateien sollten an einem sicheren Ort gespeichert werden, auf den unbefugte Personen keinen Zugriff haben.
- Stellen Sie sicher, dass das Gateway nicht über eine öffentlich zugängliche IP-Adresse verfügt.
- Vermeiden Sie die Verwendung der Portweiterleitung für den Zugriff auf das Gateway über das öffentliche Internet.
- Das Gateway sollte in einem dedizierten Netzwerksegment platziert werden, um es von anderen Geräten zu isolieren.
- Wenn Ihr Router Gastnetzwerke oder VLANs unterstützt, ist es ratsam, das Gateway in einem solchen Segment zu platzieren, um eine zusätzliche Isolierung zu gewährleisten.

Weitere Informationen zur Systemhärtung finden Sie hier: https://www.se.com/ww/en/download/document/AN002_107/.

Verfügbare Sprachen des Dokuments

Dieses Dokument ist in folgenden Sprachen verfügbar:

- **Englisch** (LSS100300_SW_EN)
- Chinesisch (LSS100300_SW_ZH)
- Französisch (LSS100300_SW_FR)
- Deutsch (LSS100300_SW_DE)
- Italienisch (LSS100300_SW_IT)
- Spanisch (LSS100300_SW_ES)

Weiterführende Dokumentation

Titel der Dokumentation	Referenznummer
BMS SpaceLogic KNX IP Gateway, LSS100300, Installation und Anschluss	LSS100300_HW
Wiser für KNX, SpaceLYnk - Richtlinie zur Systemhärtung	AN002_107

So finden Sie Dokumente online:

1. Gehen Sie zu www.se.com/ww/en/download/.
2. Wählen Sie in der oberen linken Ecke Ihr **Land** aus dem Dropdown-Menü.
3. Geben Sie in die Suchleiste **Dokumentname** oder **Referenznummer** ein.
4. Klicken Sie auf das Lupensymbol, um die Suche zu starten.
5. Wählen Sie in den Suchergebnissen das Tab **Dokumente** aus.
6. **Öffnen Sie die Dokumente**, die Sie von der Liste benötigen.

Informationen zu nicht-inklusiver oder unsensibler Terminologie

Als verantwortungsbewusstes, integratives Unternehmen aktualisiert Schneider Electric kontinuierlich seine Kommunikationen und Produkte, die nicht-integrative oder unsensible Terminologie enthalten. Trotz dieser Bemühungen können unsere Inhalte jedoch nach wie vor Begriffe enthalten, die von einigen Kunden als unangemessen betrachtet werden.

Marken

QR Code ist eine eingetragene Marke von DENSO WAVE INCORPORATED in Japan und anderen Ländern.

Einführung

BMS SpaceLogic KNX ratif IP Gateway (nachstehend Gateway genannt) ist ein Multifunktionsgerät, das für die Integration von KNX-Anlagen in Gebäudeautomatisierungssysteme entwickelt wurde.

Seine primären Schnittstellen für die Kommunikation sind KNX TP und IP, mit Unterstützung für **BACnet** -Protokoll.

Das Gateway vereint drei Schlüsselkomponenten in einem Gerät:

- KNX IP-Router (bis zu 500 Objekte)
- KNX IP-Schnittstelle
- DPSU-Drossel

Diese Integration ermöglicht es professionellen Installateuren, KNX-Systeme dank der Kombination von Funktionen in einer Einheit sowohl hinsichtlich Kosten als auch Zeit effizienter einzusetzen.

Die Systemarchitektur wird vereinfacht, da keine separaten KNX-Router und KNX-Spannungsversorgungen mehr verwendet werden müssen, vorausgesetzt die Installation entspricht den angegebenen Parametern.

Das Gateway ist für den Einsatz in kommerziellen Installationen vorgesehen.

Sicherer Fernzugriff über VPN

Wenn über das Internet auf eine KNX-Anlage zugegriffen wird, kann der Datenverkehr an Dritte weitergegeben werden. Um eine sichere Kommunikation zu gewährleisten, müssen die folgenden Vorsichtsmaßnahmen getroffen werden:

- Verwenden Sie immer eine VPN-Verbindung (Virtual Private Network) mit starker Verschlüsselung, um alle Datenpakete zu schützen.
- Die erforderliche Hardware (z. B. ein VPN-Router) und die Funktionen von Mobilfunkanbietern können je nach Land oder Region erheblich variieren.
- Der VPN-Zugriff sollte immer von einem qualifizierten VPN-Dienstanbieter konfiguriert und in Betrieb genommen werden. Der Anbieter wählt die geeignete Hardware und einen geeigneten Mobilfunkanbieter aus und stellt sicher, dass das VPN von einem zertifizierten Spezialisten eingerichtet wird.

Schneider Electric ist nicht für Leistungsprobleme oder Inkompatibilitäten verantwortlich, die durch Anwendungen, Services oder Geräte von Drittanbietern verursacht werden. Darüber hinaus bietet Schneider Electric keinen technischen Support für die VPN-Einrichtung.

Die Nichtbeachtung dieser Richtlinien kann zu einer Beschädigung des Geräts führen.

Ein VPN ermöglicht einem dezentralen Gerät den sicheren Zugriff auf das lokale Netzwerk – und damit auf die KNX-Installation – über das Internet.

Vorteile der Verwendung eines VPN

- Nur autorisierte Benutzer können auf das lokale Netzwerk zugreifen.
- Alle Daten werden während der Übertragung verschlüsselt.
- Die Daten bleiben intakt und vor Abfangen, Manipulation oder Weiterleitung geschützt – gemeinhin als VPN-Tunnel bezeichnet.

Voraussetzungen für die Einrichtung einer VPN-Verbindung

- Eine aktive Internetverbindung.

- Ein tragbares Gerät und ein Router, die VPN-Verbindungen unterstützen (mit installiertem VPN-Client).
- Das Gateway sollte in einem dedizierten Netzwerksegment abgelegt werden.
- Wenn der Router Gastnetzwerke oder VLANs unterstützt, wird empfohlen, das Gateway in einem solchen Segment zu positionieren.

Best Practices für die Passwortsicherheit

- Ihr Passwort sollte eine Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten.
- Verwenden Sie mindestens 8 Zeichen.
- Wählen Sie Passwörter, die schwer zu erraten oder in Cyberkriminellen-Wörterbüchern zu finden sind.
- Verwenden Sie vorzugsweise Passphrasen anstelle einzelner Wörter.
- Ändern Sie Ihr Passwort regelmäßig, mindestens einmal im Jahr.
- Ändern Sie das Standard-Administratorpasswort immer sofort nach Erhalt oder nach einer Rücksetzung auf die Werkeinstellungen.
- Verwenden Sie Kennwörter niemals für mehrere Konten oder Systeme.

Gerätespezifikation

Spezifikation	Beschreibung	Notiz
Klemmen, Schnittstelle	1 × RJ45 - Ethernet 10BaseT/100BaseTx 1 × KNX TP 1 × Reset-Taste	
Konnektivität	IP LAN-Verbindung 10/100 Mbit KNX/EIB TP Bus	
LED-Anzeigen	2 × LED, CPU, (Betrieb + Reset)	
KNX IP-Routing	500 Objekte (wird automatisch deaktiviert, wenn dieser Grenzwert überschritten wird)	Sie können bis zu 4000 BACnet-Punkte verwenden. Siehe Leistung, Seite 16.
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 Protokollrevision	22	
BACnet Geräteprofil	B – ASC, B – GW	

Kompatibilität

Das Gateway entspricht folgenden Standards:

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

Leistung

Anzahl der BACnet-Objekte	4000	Maximale Anzahl an Punkten, die im virtuellen BACnet-Gerät im Gateway definiert werden können. Objekte, deren Grenzwert überschritten wird, werden stillschweigend verworfen.
Anzahl der BACnet-Abonnement-Requests (COV)	4000 (1500*)	Maximale Anzahl an BACnet-Abonnement-Requests (COV), die vom Gateway akzeptiert werden
KNX-Kommunikationsobjekte	4000	Max. Anzahl verschiedener KNX-Gruppenadressen, die importiert/definiert werden können.

*BACnet COV-Unterstützung für schnelle Datenkommunikation bei gleichzeitiger Reduzierung des BACnet Netzwerkverkehrs.

*1500 für SXWAUTSVR10001 - Automatisierungsserver von Schneider Electric.

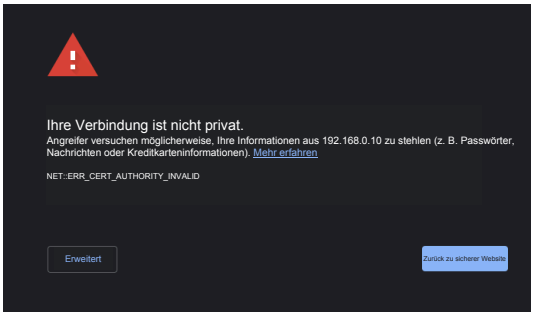
Erste Schritte

Bevor Sie beginnen, stellen Sie sicher, dass das Gateway gemäß den Installationsanweisungen ordnungsgemäß verbunden ist.

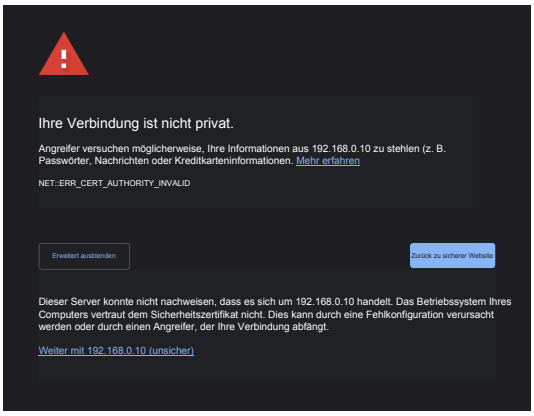
Zur Konfiguration des Gateway benötigen Sie einen Standard-Webbrowser. Wir empfehlen die Verwendung von Google Chrome oder Mozilla Firefox.

Erstmaliger Zugriff:

1. Öffnen Sie Ihren Browser und geben Sie die Standard-IP-Adresse ein: 192.168.0.10. Drücken Sie die **Eingabetaste**.
2. Da das Gateway ein selbstsigniertes Zertifikat verwendet, wird Ihr Browser wahrscheinlich eine Warnung anzeigen, dass die Verbindung nicht privat ist.



3. Fahren Sie trotzdem fort, indem Sie auf **Erweitert** klicken und dann mit 192.168.0.10 fortfahren. Das Gateway verwendet HTTPS, um eine verschlüsselte Kommunikation zwischen Ihrem Browser und dem Gerät zu gewährleisten.



4. Melden Sie sich mit den Standardanmeldedaten an und klicken Sie auf **Eingabe**.

   Login: `admin`

   Passwort: `admin`

5. Sie werden aufgefordert, Ihr Passwort zu ändern (Best Practices für die Passwortsicherheit, Seite 13). Geben Sie ein neues Passwort ein und klicken Sie auf **Speichern**.

   Das neue Passwort muss mindestens Folgendes enthalten:

   - 8 Zeichen
   - Ein Großbuchstabe
   - Ein Kleinbuchstabe
   - Eine Zahl

6. Nach der Anmeldung gelangen Sie zur Startseite:

Dort haben Sie folgende Möglichkeiten:

- Ihre bevorzugte Sprache wählen (obere rechte Ecke)
- Über auf die Gateway-Einstellungen zugreifen
- Objektfilter und Tools verwenden
- Klicken Sie auf die Schaltfläche **KNX-Projekt importieren**.

Im nächsten Schritt importieren Sie Ihr KNX-Projekt und konfigurieren die Geräteparameter.

Importieren eines KNX-Projekts

Über die Schaltfläche **KNX-Projekt importieren** in der oberen linken Ecke der Schnittstelle können Sie eine `.knxproj`-Datei direkt im Gateway speichern. Beim Importvorgang werden folgende Elemente beibehalten:

- Projektstruktur
- Gruppenadressen-DPTs (Datenpunkttypen)
- Einheiten und Suffixe

HINWEIS: Objekte mit identischen Namen werden als Duplikate behandelt und können beim Import verworfen werden.

Sie können auch Objekte ohne vordefinierte Datentypen importieren und diesen bei Bedarf Namen auf Strukturebene zuweisen.

Wenn Ihre `.knxproj`-Datei passwortgeschützt ist, müssen Sie das in ETS festgelegte Passwort eingeben. Das Projekt kann nicht ohne es importiert werden.

KNX Secure Geräte-Handling

Während des Imports behält das Gateway die **Kennung sicherer KNX-Geräte** bei, die im Projekt enthalten ist. Dies beeinflusst, wie das Gateway die Telegramme verarbeitet.

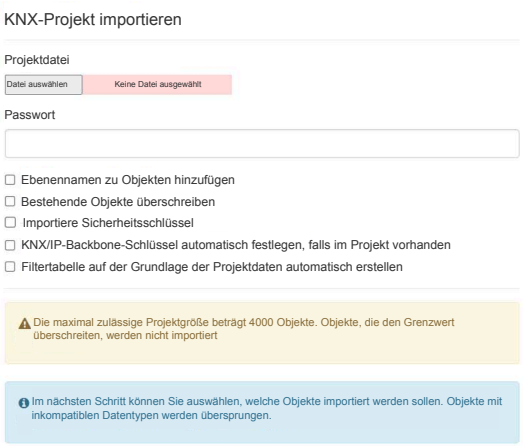
- **Sichere Telegramme** von sicheren Geräten werden nur an sicheren Gruppenadressen akzeptiert.
- **Unsichere Telegramme,** die an **sichere Gruppenadressen** gesendet werden, werden vom Gateway aus Sicherheitsgründen **zurückgewiesen**.
- Bei **nicht sicheren Gruppenadressen** akzeptiert das Gateway Telegramme von **allen nicht sicheren Quellen**.

Dadurch wird sichergestellt, dass die sichere Kommunikation geschützt bleibt und gleichzeitig eine offene Kommunikation auf nicht sicheren Kanälen ermöglicht wird.

So importieren Sie ein KNX-Projekt

1. Klicken Sie auf **KNX-Projekt importieren** und wählen Sie Ihre `.knxproj`-Datei aus.
2. Geben Sie bei Aufforderung das richtige Passwort ein.
3. (Optional) Aktivieren Sie **Ebenennamen zu Objekten hinzufügen**, wenn Sie Objektnamen und deren Strukturpositionen einschließen möchten.
4. (Optional) Aktivieren Sie **Bestehende Objekte überschreiben**, wenn Sie bereits vorhandene Objekte auf dem Gateway ersetzen möchten.
5. Um eine sichere Kommunikation mit KNX Secure-Geräten zu ermöglichen, wird empfohlen, die **Importiere Sicherheitsschlüssel**-Option zu aktivieren. Dieser Schritt ist von entscheidender Bedeutung, da er es dem Gateway ermöglicht, die erforderlichen Verschlüsselungsschlüssel direkt aus dem ETS-Projekt zu importieren. Diese Schlüssel sind mit bestimmten Gruppenadressen verknüpft, sodass das Gateway KNX-Telegramme korrekt interpretieren und für den ordnungsgemäßen Betrieb erforderliche Sicherheitsinformationen hinzufügen kann.

6. (Optional) Aktivieren Sie **Filtertabelle auf der Grundlage der Projektdaten automatisch erstellen**, damit das Gateway eine Filtertabelle unter Verwendung der importierten Gruppenadressen generieren kann. Dies trägt zur Optimierung von Leistung und Sicherheit bei, da nur relevante Gruppenadressen verarbeitet werden können.
7. (Optional) Aktivieren Sie **Filterrichtlinie so einstellen, dass ausgewählte Gruppenadressen akzeptiert werden**, um sicherzustellen, dass nur die im Projekt definierten Gruppenadressen vom Gateway akzeptiert werden.
8. Klicken Sie auf **Weiter**, um fortzufahren..



Nach dem Import werden die Filtertabellen automatisch basierend auf dem KNX-Projekt aufgefüllt und können nach Bedarf angepasst werden. Der Backbone-Schlüssel wird ebenfalls automatisch importiert.

HINWEIS: KNX-Routing wird für Projekte mit mehr als 500 Objekten nicht unterstützt.

Auswählen von Objekten für den BACnet-Export

Im nächsten Schritt wählen Sie, welche KNX-Objekte auf das Gateway importiert werden sollen. Nur die ausgewählten Objekte werden der Gateway-Datenbank hinzugefügt.

Sie können Objekte nach Name, Gruppenadresse oder Datentyp filtern, um die Auswahl zu vereinfachen. Weitere Informationen finden Sie unter Filtern und Bearbeiten von Objekteigenschaften, Seite 23.

1. Wählen Sie die zu exportierenden Objekte aus und klicken Sie auf **Weiter**.

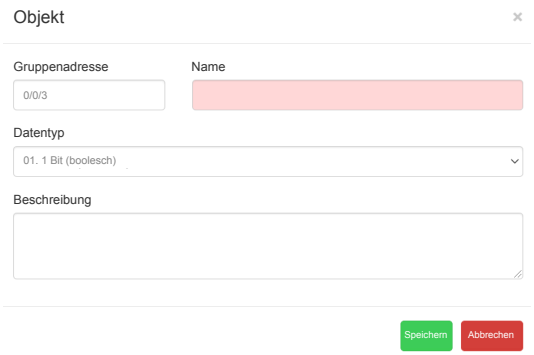
2. In einem Pop-up-Fenster wird die Anzahl der importierten Objekte bestätigt.
3. Klicken Sie auf **OK**, um den Importvorgang abzuschließen.

Hinzufügen eines Objekts

Die Funktion **Objekt hinzufügen** ist nützlich, wenn Sie ein einzelnes Objekt manuell hinzufügen möchten, ohne die gesamte `.knxproj`-Datei erneut zu importieren.

So fügen Sie ein neues Objekt hinzu:

1. Klicken Sie auf **Objekt hinzufügen**.



2. Geben Sie die erforderlichen Objektdetails ein, z. B. Name, Gruppenadresse, Datentyp und alle zusätzlichen Parameter.
3. Klicken Sie auf **Speichern**, um das Objekt zu bestätigen und zur Liste hinzuzufügen.

Aktionen

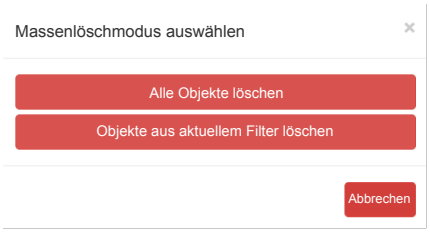
Massenlöschung von Objekten

Die **Massenlöschung** ermöglicht das schnelle Entfernen mehrerer Objekte aus der Gateway-Datenbank in einem Vorgang.

Sie können zwischen zwei Optionen wählen:

- **Alle Objekte löschen** – entfernt jedes Objekt aus der Datenbank.
- **Objekte aus aktuellem Filter löschen** – entfernt nur die Objekte, die aktuell angezeigt werden, basierend auf Ihren Filtereinstellungen.

Nach der Auswahl Ihrer bevorzugten Option fährt das System mit dem Löschen der Objekte fort.



VORSCHLAG: Verwenden Sie Filter, um Ihre Auswahl einzugrenzen, bevor Sie Massenlöschvorgänge verwenden, insbesondere wenn Sie nur bestimmte Gruppen von Objekten entfernen möchten.

Massenbearbeitung von Objekten

Mit der Funktion **Massenbearbeitung** können Sie die Einheiten und das COV-Inkrement (Change of Value) für mehrere Objekte gleichzeitig aktualisieren.

So bearbeiten Sie Objekte in großen Mengen:

1. Verwenden Sie den Filter, um die Objekte anzuzeigen, die Sie ändern möchten.
2. Klicken Sie auf **Aktionen** > wählen Sie **Massenbearbeitung** aus dem Dropdown-Menü.
3. Wählen Sie die Parameter, die Sie aktualisieren möchten:
   - **Einheiten**
   - **COV-Inkrementalwert**
4. Klicken Sie auf **Speichern**, um die Änderungen auf alle ausgewählten Objekte anzuwenden.

Objekte in eine CSV exportieren

Sie können alle Objekte für weitere Analysen oder Aufzeichnungen ganz einfach in eine `.csv`-Datei exportieren.

So exportieren Sie:

1. Klicken Sie auf **Aktionen**.
2. Wählen Sie **Export in eine CSV** aus dem Dropdown-Menü.

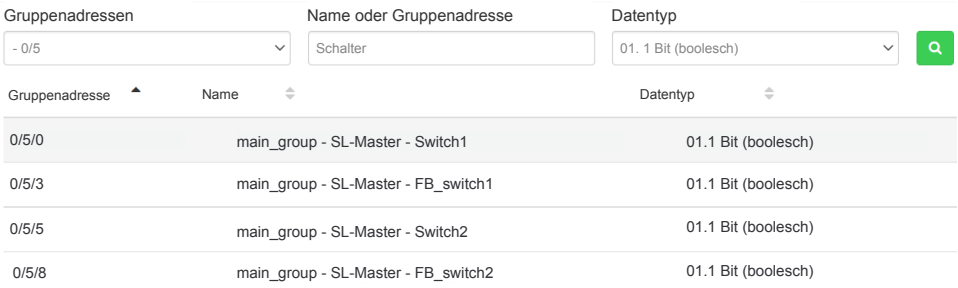
Die `.csv`-Datei wird automatisch in den **Download** -Ordner des Computers heruntergeladen. Sie können sie mit Microsoft Excel oder einer beliebigen

Tabellenkalkulationsanwendung öffnen, um die Daten anzuzeigen und mit ihnen zu arbeiten.

VORSCHLAG: Verwenden Sie vor dem Exportieren Filter, wenn Sie nur bestimmte Objekte in die Datei aufnehmen möchten.

Filtern und Bearbeiten von Objekteigenschaften

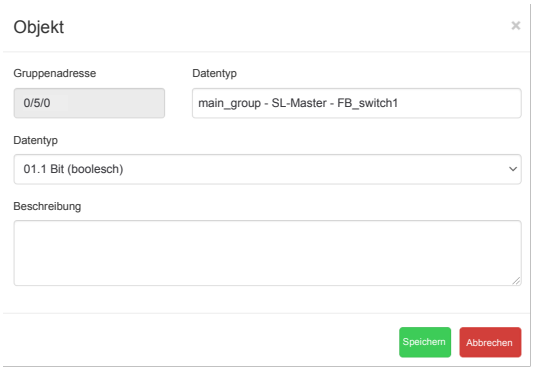
Sie können Ihre Objekte einfach nach verschiedene Kriterien wie **Name**, **Gruppenadresse** oder **Datentyp** filtern und verwalten. Geben Sie einfach Ihren Suchbegriff ein oder wählen Sie ihn aus dem Dropdown-Menü aus, um die Liste einzugrenzen.



Nach der Filterung können Sie die Objekteigenschaften bearbeiten, Werte aktualisieren oder Objekte nach Bedarf einzeln löschen.

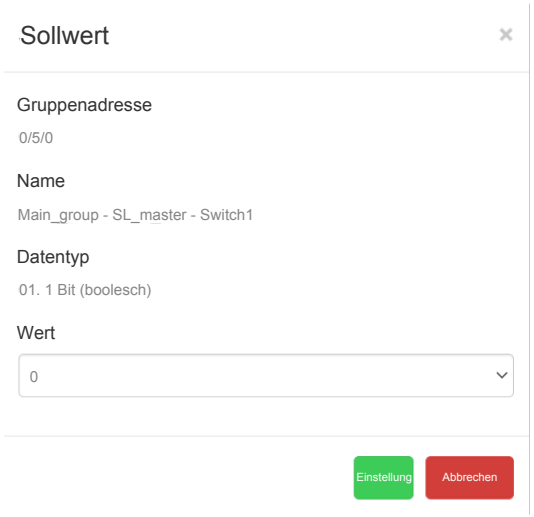
So bearbeiten Sie die Objekteigenschaften:

1. Klicken Sie auf .
2. Ändern Sie die gewünschten Eigenschaften im Popup-Fenster.
3. Klicken Sie auf **Speichern**, um die Änderungen zu übernehmen.



So legen Sie einen Objektwert fest:

1. Klicken Sie auf .
2. Wählen Sie einen Wert aus der Dropdown-Liste **Wert**.
3. Klicken Sie zur Bestätigung auf **Einstellen**.



So löschen Sie ein Objekt:

1. Klicken Sie auf .
2. Bestätigen Sie den Löschvorgang durch Klicken auf **Ja** im Bestätigungsdialogfeld.

Übersicht über die Anwendungseinstellungen

Sobald Sie die Benutzeroberfläche eingerichtet und Ihr ETS-Projekt importiert haben, können Sie die Gateway-Parameter gemäß Ihren Installationsanforderungen konfigurieren.

Vom Hauptmenü aus haben Sie Zugriff auf die folgenden Einstellungen und Tools:

- **Sicherung**: Speichern Sie Ihre aktuelle Konfiguration für eine zukünftige Wiederherstellung.
- **Wiederherstellen**: Laden Sie eine zuvor gespeicherte Konfiguration.
- **Passwort ändern**: Aktualisieren Sie Ihre Anmeldeinformationen, um die Sicherheit zu erhöhen.
- **Hostname**: Legen Sie einen benutzerdefinierten Namen für Ihr Gateway im Netzwerk fest.
- **BACnet-Konfiguration**: Passen Sie die BACnet-spezifischen Einstellungen an.
- **KNX-Konfiguration**: Verwalten Sie KNX-bezogene Parameter.
- **Netzwerkkonfiguration**: Legen Sie IP-Adresse, Subnetz, Gateway und DNS fest.
- **HTTP-Serverkonfiguration**: Passen Sie die Webserver-Einstellungen an.
- **HTTP SSL-Zertifikat**: Laden Sie Ihr HTTPS-Zertifikat hoch oder verwalten Sie es.
- **NTP-Client-Konfiguration**: Nehmen Sie die Zeitsynchronisation über einen Netzwerkzeitserver vor.
- **Datum und Uhrzeit**: Stellen Sie die Systemuhr manuell ein oder passen Sie sie an.
- **Systemprotokoll**: Zeigen Sie Systemaktivität und Diagnoseprotokolle an.
- **Ping**: Testen Sie die Netzwerkverbindung zu anderen Geräten.
- **Geräte-ID umschalten**: Aktivieren Sie die visuelle Identifikation (z. B. LED)
- **Firmware aktualisieren**: Installieren Sie die neueste Firmwareversion.
- **Zurücksetzen auf Werkseinstellungen**: Setzen Sie das Gateway auf die Standardeinstellungen zurück.
- **Neustart**. Starten Sie das Gerät neu.
- **Herunterfahren**: Schalten Sie das Gateway sicher aus.

Erstellen eines Backups

Durch die Erstellung eines Backups können Sie eine Kopie Ihrer Gateway-Konfiguration speichern, die bei Datenverlust oder Systemausfall zu einem späteren Zeitpunkt wiederhergestellt werden kann.

So erstellen Sie eine Sicherung:

1. Öffnen Sie das Hauptmenü, indem Sie auf  klicken.
2. Wählen Sie **Sicherung** aus der Dropdown-Liste.

Die Sicherungsdatei wird automatisch in den **Downloads** -Ordner heruntergeladen.

Namensformat der Sicherungsdatei:

`[Hostname]-backup-[YYYY.MM.DD]-[HH.MM].bckp`

Der Dateiname enthält den Hostnamen des Gateway sowie Datum und Uhrzeit der Erstellung der Sicherung. Sie können die Datei umbenennen und zur Aufbewahrung in einen anderen Ordner verschieben.

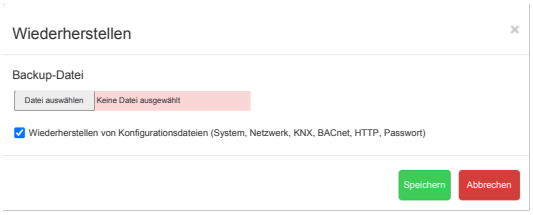
VORSCHLAG: Bewahren Sie Ihre Sicherungsdateien an einem sicheren Ort auf und vermeiden Sie, sie für unbefugte Benutzer freizugeben.

Wiederherstellen einer Sicherung

Die Funktion **Wiederherstellen** ermöglicht Ihnen, die Daten Ihres Gateway aus einem zuvor gespeicherten Backup wiederherzustellen. Dies ist nützlich, wenn Daten verloren gegangen oder beschädigt sind oder wenn Sie Einstellungen auf ein neues Gerät übertragen müssen.

So stellen Sie Ihre Daten wieder her:

1. Öffnen Sie das Hauptmenü, indem Sie auf ☰ klicken.
2. Wählen Sie **Wiederherstellen** aus der Dropdown-Liste.
3. Klicken Sie auf **Datei auswählen** und suchen Sie Ihre Sicherungsdatei auf Ihrem Computer.
4. (Optional) Wenn Sie auch Konfigurationsdateien wiederherstellen möchten, aktivieren Sie die Option **Konfigurationsdateien wiederherstellen**.



5. Klicken Sie auf **Speichern**, um den Wiederherstellungsvorgang zu starten.

Nach dem Klicken auf **Speichern** wird ein Popup-Fenster mit der Frage angezeigt, ob Sie das System neu starten möchten:

- Klicken Sie auf **Ja**, um die Wiederherstellung abzuschließen.
- Klicken Sie auf **Nein**, um den Vorgang abzubrechen. Wenn Sie **Nein** wählen, werden keine Daten importiert.

  VORSCHLAG: Vergewissern Sie sich immer, dass Sie die richtige Sicherungsdatei wiederherstellen, um keine wichtigen Daten zu überschreiben.

Passwort ändern

Um die Sicherheit Ihres Gateway zu gewährleisten, ist es wichtig, dass Sie Ihr Passwort regelmäßig aktualisieren.

Gehen Sie dazu wie folgt vor:

1. Öffnen Sie das Hauptmenü, indem Sie auf ☰ klicken.
2. Wählen Sie **Passwort ändern** aus dem Menü.
3. Geben Sie Ihr aktuelles Passwort und dann Ihr neues Passwort ein.
4. Klicken Sie auf **Speichern**, um die Änderung zu bestätigen.

Ändern des Gateway-Hostnamens

Der Hostname ist der eindeutige Name, der Ihrem Gateway im Netzwerk zugewiesen ist. Er hilft Ihnen bei der einfachen Identifizierung des Geräts, insbesondere bei der Verwaltung mehrerer Installationen. Der Hostname wird auch im Dateinamen von Backup-Dateien verwendet, was die Nachverfolgung und Organisation erleichtert.

Warum sollte man den Hostnamen ändern?

- Um das Gateway in Ihrem Netzwerk eindeutig zu identifizieren.
- Um den Gerätenamen zu personalisieren und die Verwaltung zu vereinfachen.
- Um Sicherungsdateien besser erkennen zu können (z. B.`Office1-backup-2025.05.23-14.30.bckp`).

So ändern Sie den Hostnamen:

1. Öffnen Sie das Hauptmenü, indem Sie auf  klicken.
2. Wählen Sie den **Hostnamen** aus dem Menü.
3. Geben Sie Ihren gewünschten Hostnamen ein.
   - Verwenden Sie nur Buchstaben, Zahlen und Bindestriche.
   - Vermeiden Sie Leerzeichen oder Sonderzeichen.
   - Wählen Si einen kurzen, anschaulichen Namen (z. B. `Lobby-Gateway`, `KNX-BMS-01`).
4. Klicken Sie auf **Speichern**, um die Änderungen zu übernehmen.

   HINWEIS: Eine Änderung des Hostnamens wirkt sich nicht auf die IP-Adresse oder die Netzwerkkonfiguration aus. Es kann jedoch ein Neustart erforderlich sein, damit der neue Name in einigen Netzwerktools oder -protokollen angezeigt wird.

BACnet-Konfiguration

Das Gateway fungiert als BACnet-Server und ermöglicht so die Kommunikation zwischen KNX-Gruppenobjekten und BACnet-Clientgeräten. Dies ermöglicht die nahtlose Integration von Gebäudeautomatisierungssystemen über verschiedene Plattformen hinweg.

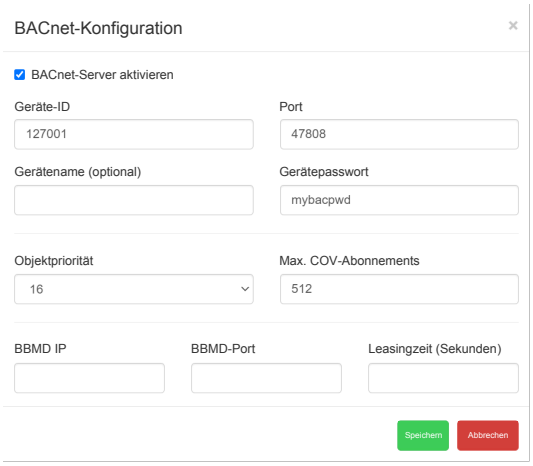
BACnet (Building Automation and Control Network) ist ein standardisiertes Protokoll, das für den Austausch von Daten zwischen Geräten in Gebäudeautomatisierungssystemen verwendet wird – unabhängig von ihrer spezifischen Funktion (z. B. Beleuchtung, HLK, Sicherheit). Das Gateway stellt über die Ethernet-Schnittstelle eine Verbindung zum BACnet-Netzwerk her und liefert Daten von KNX-Gruppenobjekten, die in BACnet exportiert wurden.

- Binäre KNX-Objekte werden als binäre Werte in BACnet zugeordnet.
- Numerische KNX-Objekte werden als Analogwerte zugeordnet.
- Andere Datentypen werden nicht unterstützt.

So konfigurieren Sie die BACnet-Einstellungen:

1. Öffnen Sie das Hauptmenü, indem Sie auf  klicken.

2. Wählen Sie **BACnet-Konfiguration** aus dem Menü.



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

Parameter	**Notiz**
BACnet-Server aktivieren	Ermöglicht die Aktivierung bzw. Deaktivierung der BACnet-Funktion. Standardmäßig deaktiviert.
Geräte-ID	Eine eindeutige Kennung für das Gateway im BACnet-Netzwerk. Es darf keine Konflikte mit anderen Geräten geben.
Port	Kommunikationsschnittstelle für BACnet. Die Standardeinstellung ist 47808.
Gerätename (optional)	Benutzerdefinierter Name für das Gerät. Wenn leer gelassen, ist die Standardeinstellung `hostname_DeviceID`.
Gerätepasswort	Optionales Passwort für BACnet-Dienste wie `DeviceCommunicationControl` und `ReInitializeDevice`. Wenn diese Option nicht aktiviert ist, wird kein Passwort verwendet.
Objektpriorität	Legt die Standardprioritäts-Array-Position für BACnet-Objekte fest.
Max. COV-Abonnements	Maximale Anzahl der COV-Abonnements (Change of Value). Die Standardeinstellung ist 4000. Für weitere Informationen hierzu siehe Leistung, Seite 16.
BBMD IP	IP-Adresse des BACnet Broadcast Management Device (BBMD), sofern verwendet.
BBMD-Port	Vom BBMD verwendeter Port.
Leasingzeit (Sekunden)	Intervall für die Verlängerung der BBMD-Registrierung.

VORSCHLAG: Vergewissern Sie sich, dass die Geräte-ID in Ihrem BACnet-Netzwerk eindeutig ist, um Kommunikationskonflikte zu vermeiden.

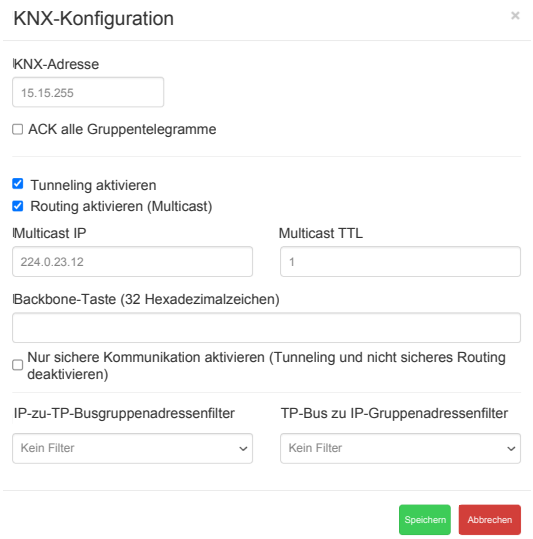
KNX-Konfiguration

Mit der **KNX-Konfiguration** können Sie das Gateway einrichten, wenn es als **KNX IP-Schnittstelle** oder **Router** verwendet wird.

Gehen Sie wie folgt vor, um auf die Einstellungen zuzugreifen und sie zu konfigurieren:

1. Öffnen Sie das Hauptmenü, indem Sie auf ☰ klicken.

2. Wählen Sie **KNX-Konfiguration** aus dem Menü.



3. Passen Sie die folgenden Parameter nach Bedarf an und klicken Sie auf **Speichern**, um Ihre Änderungen zu übernehmen.

Parameter	**Notiz**
KNX-Adresse	Die individuelle KNX-Adresse des Geräts. Standard: 15.15.255.
ACK alle Gruppentelegramme	Aktivieren Sie diese Option, wenn das Gateway direkt mit anderen KNX-Geräten kommuniziert und empfangene Telegramme quittieren muss. Deaktivieren, wenn das Gateway nur Gruppenadressen überwacht (Sniffer-Modus).
Tunneling aktivieren	Ermöglicht mehreren Geräten die gemeinsame Nutzung einer öffentlichen IPv4-Adresse durch die Änderung von IP-Headern während der Übertragung. Dies ermöglicht eine schnellere IP-Kommunikation (bis zu 1000 × schneller als TP-UART). Das Gateway fungiert als Server mittels Unicast und quittiertem Datenaustausch. Für jede Tunneling-Verbindung ist eine eindeutige physikalische Adresse erforderlich.
Routing aktivieren (Multicast)	Ermöglicht die Übertragung nicht quittierter Multicast-Daten. Das Gateway fungiert als Linien- oder Backbone-Koppler.
Multicast IP	Die für das Routing verwendete Multicast-IP-Adresse. Standard: 224.0.23.12.
Multicast TTL	Gültigkeitszeitwert für Multicast-Pakete. Standard: 1. Dies ermöglicht die Kommunikation über Teilnetze hinweg.
Backbone-Taste (32 Hexadezimalzeichen)	Ein 32 Zeichen langer Hexadezimalschlüssel, der zur Verschlüsselung und Entschlüsselung sicherer Telegramme für das IP-Routing verwendet wird.
Nur sichere Kommunikation zulassen	Wenn diese Option aktiviert ist, ist nur eine sichere Kommunikation zulässig. Tunneling und nicht sicheres Routing sind deaktiviert.
IP-zu-TP-Busgruppenadressenfilter	Kein Filter Ausgewählten 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/*/*)
TP-Bus zu IP-Gruppenadressenfilter	

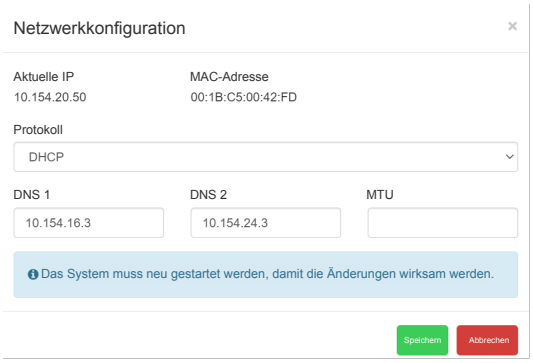
Netzwerkkonfiguration

Die Netzwerkkonfiguration umfasst die Einrichtung der Steuerelemente und Parameter, die die Art und Weise verwalten, wie das Gerät über ein Netzwerk

kommuniziert. Nach der Aktualisierung der Netzwerkeinstellungen muss das System neu gestartet werden, damit die Änderungen wirksam werden.

Zugriff auf die Netzwerkkonfiguration:

1. Öffnen Sie das Hauptmenü, indem Sie auf klicken.
2. Wählen Sie **Netzwerkkonfiguration**.



3. Passen Sie die folgenden Netzwerkparameter nach Bedarf an und klicken Sie dann auf **Speichern**, um Ihre Änderungen zu übernehmen:

Parameter	Notiz
Aktuelle IP	Die Netzwerkkonfiguration umfasst die Einrichtung der Steuerelemente und Parameter, die die Art und Weise verwalten, wie das Gerät über ein Netzwerk kommuniziert. Nach der Aktualisierung der Netzwerkeinstellungen muss das System neu gestartet werden, damit die Änderungen wirksam werden.
MAC-Adresse	Eine eindeutige Hardwarekennung, die dem Gerät zugewiesen ist.
Protokoll	Spezifisches Protokoll, das für die Adressierung verwendet wird: Statische IP: Manuelle Zuweisung einer IP-Adresse. DHCP: Erhält automatisch eine IP-Adresse vom Netzwerk.
IP-Adresse	Die IP-Adresse des Geräts. Standard: 192.168.0.10.
Netzwerkmaske	Definiert das Subnetz. Standard: 255.255.255.0.
Gateway-IP	Die IP-Adresse des Netzwerk-Gateway Standard: Ohne
DNS 1	IP-Adresse des primären DNS-Servers.
DNS 2	IP-Adresse des sekundären DNS-Servers.
MTU	Maximale Übertragungseinheit – die größte Paketgröße, die gesendet werden kann. Standard: 1500.

Nach dem Speichern der Konfiguration wird ein Bestätigungsfenster angezeigt. Klicken Sie auf **Ja**, um das System neu zu starten und die neuen Einstellungen zu übernehmen.

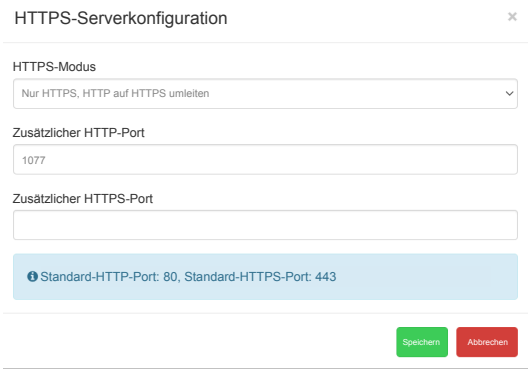
HTTP-Serverkonfiguration

In diesem Abschnitt können Sie die Sicherheitsstufe der Kommunikation des Gateway mit dem Webserver konfigurieren und zusätzliche HTTP/HTTPS-Ports einstellen.

Schritte zur Konfiguration des HTTP-Servers

1. Öffnen Sie das Hauptmenü, indem Sie auf klicken.

2. Wählen Sie **HTTPS-Serverkonfiguration**.



3. Passen Sie die unten aufgeführten Parameter an und klicken Sie auf **Speichern**.
4. Starten Sie das System neu, damit die Änderungen wirksam werden.

HTTPS-Serverparameter

Parameter	Hinweis
HTTPS-Modus	Wählen Sie den gewünschten Sicherheitsmodus aus: **HTTP und HTTPS aktiviert**: Es ist sowohl eine sichere als auch eine nicht sichere Kommunikation zulässig. **Nur HTTPS, umleiten zu HTTPS**: Der gesamte HTTP-Datenverkehr wird automatisch an HTTPS umgeleitet, um eine sichere Kommunikation zu gewährleisten. **Nur HTTPS, HTTP-Port ist deaktiviert**: Nur sichere HTTPS-Kommunikation ist zulässig. HTTP ist vollständig deaktiviert.
Zusätzlicher HTTP-Port	Optional: Geben Sie einen zusätzlichen HTTP-Port an. Die Standardeinstellung ist 80.
Zusätzlicher HTTPS-Port	Optional: Geben Sie einen zusätzlichen HTTPS-Port an. Die Standardeinstellung ist 443.

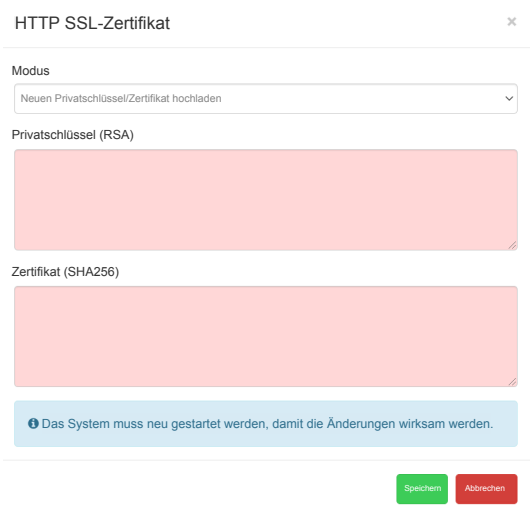
HTTP SSL-Zertifikat

SSL-Zertifikate sind digitale Dateien, die einen kryptografischen Schlüssel sicher mit der Identität eines Geräts verknüpfen. Wenn sie auf einem Webserver installiert sind, aktivieren sie sichere HTTPS-Verbindungen und aktivieren das Vorhängeschloss im Browser.

So konfigurieren Sie ein SSL-Zertifikat:

1. Öffnen Sie das Hauptmenü, indem Sie auf klicken.
2. Wählen Sie **HTTP SSL-Zertifikat** aus dem Menü.
3. Wählen Sie den gewünschten **Modus**:
   - **Neuen privaten Schlüssel/Zertifikat hochladen**: Verwenden Sie diese Option, um einen vorhandenen privaten RSA-Schlüssel und ein vorhandenes SSL-Zertifikat hochzuladen.
   - **Neuen privaten Schlüssel/Zertifikat generieren**: Verwenden Sie diese Option, um einen neuen RSA-Schlüssel und ein SSL-Zertifikat auf der Grundlage des aktuell installierten Schlüssels zu generieren.

4. Klicken Sie auf **Speichern**, um Ihre Änderungen zu übernehmen.



5. Starten Sie das System neu, damit die neuen Zertifikateinstellungen wirksam werden.

NTP-Client-Konfiguration

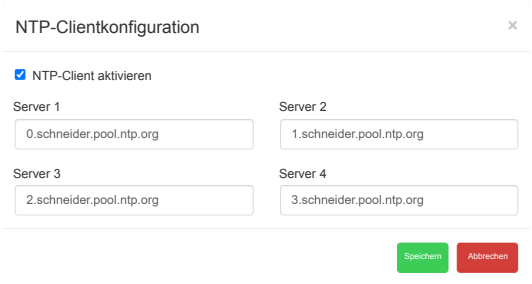
Der NTP-Client (Network Time Protocol) stellt sicher, dass das Gateway mit der koordinierten Weltzeit (UTC) synchronisiert bleibt, sodass die genaue Zeit über alle angeschlossenen Geräte hinweg erhalten bleibt. Er kompensiert Netzwerkverzögerungen, um eine präzise Zeitmessung zu ermöglichen.

Wesentliche Funktionen:

- Synchronisiert die interne Uhr des Gateway mit bis zu **4 NTP-Server**, priorisiert von 1 bis 4.
- Gewährleistung genauer Zeitstempel für Protokolle, Ereignisse und Datenkommunikation.

So konfigurieren Sie den NTP-Client:

1. Öffnen Sie das Hauptmenü, indem Sie auf klicken.
2. Navigieren Sie zu **NTP-Client-Konfiguration**.
3. Geben Sie die IP-Adressen oder den Domänennamen von bis zu vier NTP-Servern in der Reihenfolge ihrer Priorität ein.
4. Klicken Sie auf **Speichern**, um die Einstellungen zu übernehmen.



5. Starten Sie das System neu, um die neue Konfiguration zu aktivieren.

   VORSCHLAG:

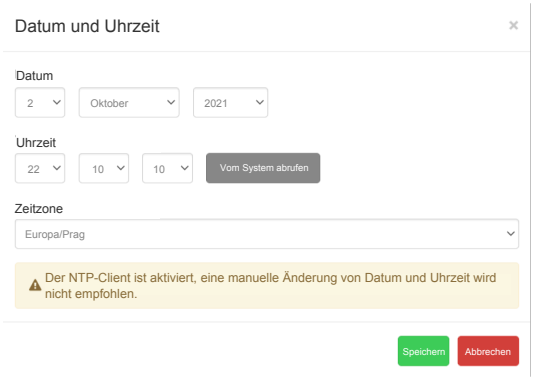
   - Wenn Sie sich nicht sicher sind, ob ein NTP-Server erreichbar ist, verwenden Sie das **Ping-Tool**, um seine Verfügbarkeit zu überprüfen.
   - Verwenden Sie zuverlässige und geografisch nahe NTP-Server, um optimale Ergebnisse zu erzielen.

Datum und Uhrzeit

Das Gateway verwendet das Network Time Protocol (NTP), um seine interne Uhr automatisch mit einem internetbasierten Zeitserver zu synchronisieren. Dies gewährleistet eine genaue Zeitmessung ohne manuelle Eingabe.

So stellen Sie Datum und Uhrzeit ein:

1. Öffnen Sie das Hauptmenü, indem Sie auf klicken.
2. Wählen Sie **Datum und Uhrzeit** aus dem Menü.
3. Wenn das Gateway nicht mit dem Internet verbunden ist, klicken Sie auf **Vom System abrufen**, um die Uhrzeit mit Ihrem PC zu synchronisieren.
4. Wählen Sie Ihre Zeitzone aus der Liste aus.
5. Klicken Sie auf **Speichern**, um die Einstellungen zu übernehmen.



Systemprotokoll

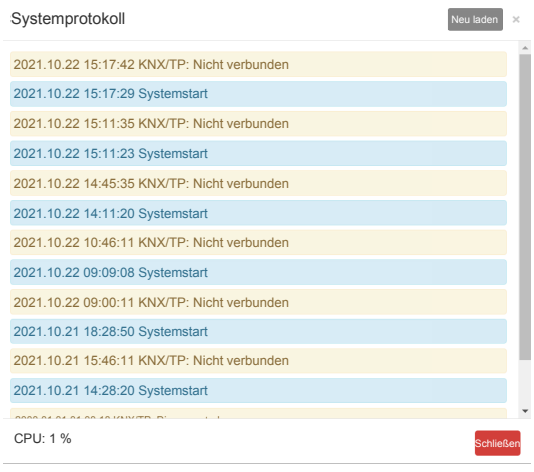
Das **Systemprotokoll** stellt eine chronologische Aufzeichnung der wichtigsten Ereignisse auf dem Gateway bereit, z. B.:

- Systemstarts
- TP/KNX-Trennung

Diese Ereignisse werden vom Gateway automatisch in einem einfachen und leicht lesbaren Format aufgezeichnet.

So zeigen Sie das Systemprotokoll an:

1. Öffnen Sie das Hauptmenü, indem Sie auf klicken.
2. Wählen Sie **Systemprotokoll** aus dem Menü.



Das Systemprotokoll wird angezeigt, wenn Sie auf **Systemprotokoll** klicken.

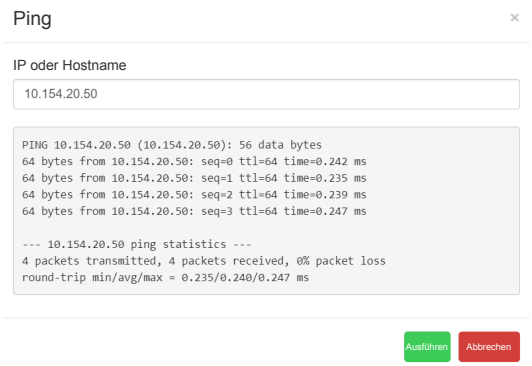
Am unteren Rand des Protokollbildschirms sehen Sie auch die **CPU-Last**, die einen Einblick in die aktuelle Verarbeitungsaktivität des Gateway bietet.

Ping

Mit dem **Ping**-Tool können Sie testen, ob ein bestimmtes Gerät oder ein bestimmter Server über ein IP-Netzwerk erreichbar ist. Es misst die **Umlaufzeit** für Datenpakete, die vom Gateway an den Ziel-Host und wieder zurück gesendet werden.

So verwenden Sie das **Ping**-Tool:

1. Öffnen Sie das Hauptmenü, indem Sie auf ☰ klicken.
2. Wählen Sie **Ping** aus dem Menü.
3. Geben Sie die IP-Adresse oder den Hostnamen des Geräts ein, das Sie testen möchten.
4. Klicken Sie auf **Ausführen**, um den Ping-Test zu starten.



Die Ergebnisse zeigen die Antwortzeit, damit Sie feststellen können, ob das Ziel erreichbar ist und wie schnell es reagiert.

Geräteidentifikation umschalten

Die Funktion **Geräte-ID umschalten** unterstützt Sie bei der Lokalisierung eines bestimmten Gateway-Geräts im Netzwerk, indem ein visuelles Signal aktiviert wird.

Funktionsweise:

Wenn die Identifikation aktiviert ist, blinkt **LED 2** des ausgewählten Geräts **rot und grün**, wodurch das Gerät leicht von anderen Geräten zu unterscheiden ist.

Verwendung:

1. Öffnen Sie das Hauptmenü, indem Sie auf ☰ klicken.
2. Wählen Sie **Geräteidentifikation umschalten** aus dem Menü.
3. Beobachten Sie das Gerät: LED 2 sollte zu blinken beginnen, um die Position anzuzeigen.

Diese Funktion ist besonders nützlich, wenn mehrere Geräte in einer Netzwerkumgebung verwaltet werden sollen.

Firmware aktualisieren

Bei einer Aktualisierung der Firmware wird Ihr Gateway mit den neuesten Funktionen und Verbesserungen aktualisiert, ohne dass Ihre bestehende Konfiguration geändert oder Hardwareänderungen vorgenommen werden müssen.

WICHTIG: Trennen Sie das Gateway während des Aktualisierungsvorgangs nicht. Das Gerät wird mehrmals neu gestartet und **LED 1 blinkt rot und grün**, um anzuzeigen, dass die Aktualisierung läuft.

So aktualisieren Sie die Firmware

1. Öffnen Sie die Hauptmenüs, indem Sie auf ☰ klicken.
2. Wählen Sie **Firmware aktualisieren** aus dem Menü.
3. Wählen Sie die Firmware-Datei, die Sie installieren möchten.
4. Wählen Sie die entsprechende Signaturdatei aus (für die Validierung erforderlich).
5. Klicken Sie auf **Speichern**, um die Aktualisierung zu starten.

Nach der Aktualisierung

- Das Gateway wird automatisch neu gestartet.
- Es wird **dringend empfohlen**, nach der Aktualisierung den **Browsercache zu löschen**, um Anzeigeprobleme zu vermeiden.
- Firmware-Downgrades werden nicht unterstützt.

  HINWEIS: Eine gültige **Signaturdatei** ist für jedes Firmware-Upgrade erforderlich. Firmware-Pakete werden immer mit den entsprechenden Signaturdateien verteilt.

Zurücksetzen auf Werkeinstellungen

Bei einer Rücksetzung auf die Werkeinstellungen werden alle Daten und Einstellungen auf dem Gateway gelöscht und der ursprüngliche werkseitige Zustand wiederhergestellt. Diese Aktion ist irreversibel, daher verwenden Sie sie mit Vorsicht.

Für eine Rücksetzung auf die Werkeinstellungen stehen Ihnen zwei Möglichkeiten zur Auswahl:

- **Über die Anwendung**: Verwenden Sie die Software-Schnittstelle, um einen Reset über das Einstellungsmenü zu initiieren.
- **Über die Hardware-Reset-Taste**: Halten Sie die physische Reset-Taste am Gerät gedrückt, um einen manuellen Reset auszulösen.

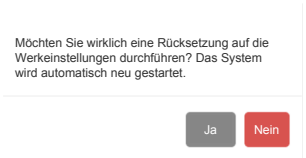
Zurücksetzen auf Anwendungswerkeinstellungen

Sie können Ihren Gateway direkt über die Anwendung auf die Werkseinstellungen zurücksetzen. Bei diesem Vorgang werden alle Benutzerkonfigurationen gelöscht und das Gerät wird in seinen ursprünglichen Zustand zurückversetzt.

HINWEIS: Bei einer Rücksetzung auf die Werkeinstellungen werden alle benutzerdefinierten Einstellungen und Konfigurationen gelöscht. Verwenden Sie diese Option nur, wenn erforderlich.

Durchführung einer Rücksetzung auf die Werkeinstellungen über die Anwendung:

1. Öffnen Sie das Hauptmenü, indem Sie auf  klicken.
2. Wählen Sie **Zurücksetzen auf Werkseinstellungen** aus dem Menü.
3. Bestätigen Sie das Zurücksetzen, wenn Sie dazu aufgefordert werden. Das System wird automatisch neu gestartet.



Geräteparameter nach Reset:

Parameter	Ergebnis
Gerätename	LSS100300
IP-Adresse	Beibehalten (bleibt unverändert)
Kein Objekt	Löschen (BACnet/KNX-Konfiguration wird entfernt)

Hardware-Reset auf Werkseinstellungen

Eine Rücksetzung auf die Hardware-Werkeinstellungen ist nützlich, wenn die Gateway aufgrund von fehlerhaften Einstellungen oder Problemen bei der Netzwerkkonfiguration nicht mehr zugänglich ist.

Wann ist Folgendes zu verwenden:

- Das Gateway reagiert nicht.
- Sie können nicht auf die Weboberfläche zugreifen.
- Netzwerkeinstellungen verhindern die Verbindung.

So führen Sie ein Hardware-Reset durch:

1. Suchen Sie die rote **RESET**-Taste auf dem Gerät.

2. Führen Sie eines der folgenden Reset-Verfahren durch:

Aktion	Ergebnis
Für **weniger als 10 Sekunden** gedrückt halten	Startet das Gerät neu (es werden keine Einstellungen geändert).
Für **mehr als 10 Sekunden** gedrückt halten	Nur **Netzwerkeinstellungen** werden zurückgesetzt. Die IP-Adresse wird auf die Werkseinstellung zurückgesetzt: 192.168.0.10.
Für **mehr als 10 Sekunden** gedrückt halten, loslassen, dann erneut drücken und für **mehr als 10 Sekunden** gedrückt halten	Führt eine **vollständige Rücksetzung der Werkseinstellung** durch, um alle Einstellungen auf die Standardwerte zurückzusetzen.

HINWEIS: Ein vollständiger Reset löscht alle Konfigurationen, einschließlich der BACnet- und KNX-Einstellungen.

Neu starten

Wenn Ihr Gateway nicht wie erwartet reagiert, können Sie einen **Neustart** durchführen, um das System neu zu starten.

Beim Neustart wird das Gerät heruntergefahren und wieder eingeschaltet, ohne dass Ihre Konfiguration oder Daten beeinträchtigt werden.

Neustarten des Gateway:

1. Öffnen Sie das Hauptmenü, indem Sie auf klicken.
2. Wählen Sie **Neustart** aus dem Menü.
3. Klicken Sie bei Aufforderung auf **Ja**, um zu bestätigen.

Das Gateway wird automatisch neu gestartet. Dieser Vorgang dauert in der Regel einige Augenblicke.

Gateway herunterfahren und neu starten

Durch den Wechsel des Gateway in den Ruhezustand wird sichergestellt, dass alle Datenvorgänge sicher abgeschlossen werden. Auf diese Weise wird die Systemstabilität gewährleistet und Datenverlust oder -beschädigung vermieden.

WICHTIG: Trennen Sie die Spannungsversorgung erst, wenn die LED 2 erlischt.

In den Ruhezustand wechseln

So schalten Sie das Gateway sicher ab:

1. Öffnen Sie das Hauptmenü durch Anklicken des Menüsymbols. .
2. Wählen Sie **Herunterfahren**.
3. Bestätigen Sie durch Klicken auf **Ja**.

Das passiert im Ruhezustand

Die Gateway wechselt in einen temporären **3-Minuten-Ruhezustand**. Während dieser Zeit:

- LED 1 (grün) geht **aus**.
- LED 2 (grün) geht **aus**.
- Das Gateway **reagiert nicht mehr auf Netzwerkkommunikation**.

Wenn das Gerät während dieses Zeitraums **nicht** von der Spannungsversorgung getrennt wird, erfolgt ein **automatischer Neustart**.

Manueller Neustart des Gateway

So starten Sie das Gateway manuell neu:

- Trennen Sie die Spannungsversorgung und schließen Sie sie wieder an, nachdem **LED 2** ausgegangen ist.
- Das Gateway verfügt **nicht** über einen dedizierten Ein/Aus-Schalter.

Printed in:
Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison – Frankreich
+ 33 (0) 1 41 29 70 00

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
Frankreich

+ 33 (0) 1 41 29 70 00

www.se.com

Da Normen, Spezifikationen und Bauweisen sich von Zeit zu Zeit ändern, sollten Sie um Bestätigung der in dieser Veröffentlichung gegebenen Informationen nachsuchen.

© Schneider Electric. Alle Rechte vorbehalten.

2507_LSS100300_S