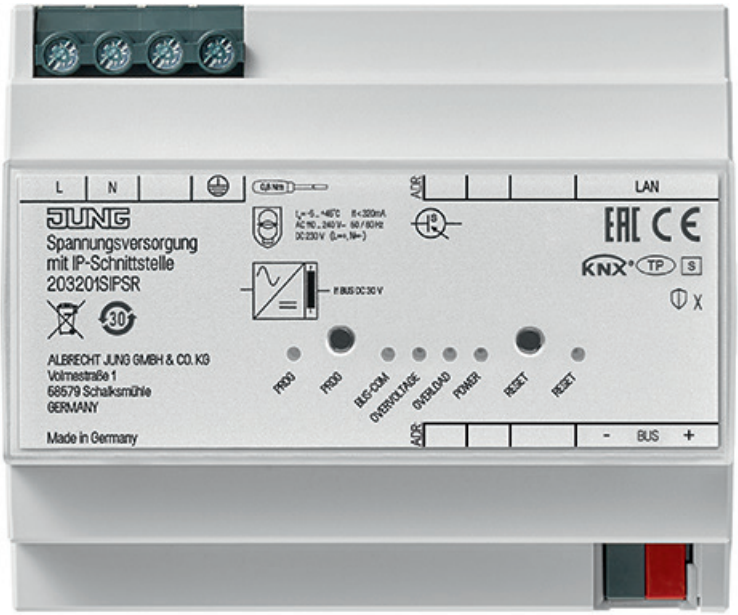
Produktdokumentation



KNX Spannungsversorgung mit IP-Schnittstelle

Art.-Nr.:500.500.336

ALBRECHT JUNG GMBH & CO. KG
Volmestraße 1
58579 Schalksmühle
GERMANY
Tel. +49 2355 806-0
Fax +49 2355 806-204
kundencenter@jung.de
www.jung.de

04/2022

Inhaltsverzeichnis

1 Sicherheitshinweise und Geräteaufbau 4
1.1 Sicherheitshinweise 4
1.2 Geräteaufbau 4
2 Funktion 4
2.1 Systeminformation 4
2.2 Bestimmungsgemäßer Gebrauch 5
2.3 Produkteigenschaften 5
2.3.1 Applikationsprogramm A 5
2.3.2 Applikationsprogramm B 5
3 Montage und elektrischer Anschluss 6
3.1 Information für Elektrofachkräfte 6
3.2 Montage 6
3.3 Anschluss 6
4 Inbetriebnahme 7
4.1 Einschalten 7
4.2 Bootvorgang 7
5 Bedienung 8
5.1 LED-Anzeigen 8
5.2 Programmiermodus 9
5.3 Diagnosemeldungen 9
5.4 Reset 10
5.5 Master-Reset 10
6 Konfiguration 11
6.1 Topologie 11
6.2 Geräteeigenschaften 11
6.2.1 Allgemein 11
6.2.2 IP-Einstellungen 12
6.2.3 KNX IP Secure 12
6.2.4 Zusatzfunktionen 13
6.2.5 KNX Data Secure 14
6.3 Gerätespezifische Parameter 15
6.3.1 Allgemeine Einstellungen 15
6.3.2 Erweiterte Einstellungen 15
6.4 Allgemeine Einstellungen 17
6.4.1 Applikationsprogramm A 17
6.4.2 Applikationsprogramm B 30
6.5 Kommunikationsobjekte 36
6.5.1 Applikationsprogramm A 36
6.5.2 Applikationsprogramm B 38
7 Erweiterte Konfiguration 41
7.1 Konfigurationstool 41
7.1.1 Geräteverbindung 41
7.1.2 Gerätekonfiguration 42
7.2 Telnet-Interface 43

8 Anwendungsfälle 47
8.1 Applikationsprogramm A – Logikfunktionen 47
8.1.1 Anwesenheitsüberwachung mit Hotelcardschalter 47
8.1.2 Anwesenheitsüberwachung mit Präsenzmelder 51
8.2 Applikationsprogramm B – KNX IP-Schnittstelle 55
8.2.1 Mapper 55
8.2.2 Fernwartung 55
9 Firmware-Update 55
9.1 Firmware-Version anzeigen 55
9.2 Firmware-Update vorbereiten 55
9.2.1 Sichere Inbetriebnahme deaktivieren 55
9.2.2 Gerät neuprogrammieren 55
9.3 Firmware-Update durchführen 56
10 FAQ 56
11 Begriffe 57
12 Technische Daten 58
13 Gewährleistung 58
14 Open Source Software 59
14.1 LWIP 59

1 Sicherheitshinweise und Geräteaufbau

1.1 Sicherheitshinweise

Montage und Anschluss elektrischer Geräte dürfen nur durch Elektrofachkräfte erfolgen.

Schwere Verletzungen, Brand oder Sachschäden möglich. Anleitung vollständig lesen und beachten.

Gefahr durch elektrischen Schlag. Bei Installation und Leitungsverlegung die für SELV-Stromkreise geltenden Vorschriften und Normen einhalten.

Diese Anleitung ist Bestandteil des Produktes und muss beim Endkunden verbleiben.

1.2 Geräteaufbau

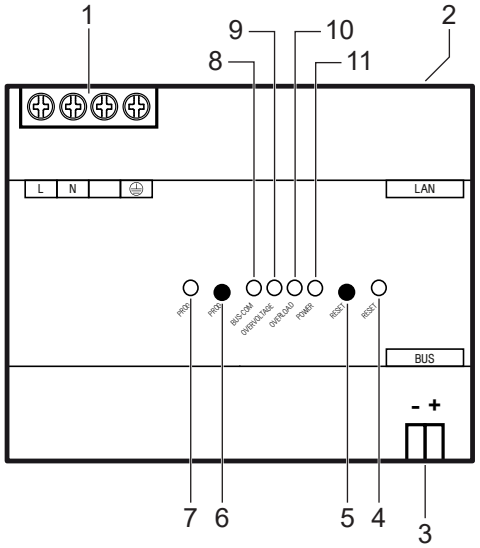


Abb. 1: Geräteaufbau

1	Anschluss Netz	5	Taste RESET	9	LED OVERVOLTAGE
2	Anschluss LAN	6	Taste PROG	10	LED OVERLOAD
3	Anschluss KNX	7	LED PROG	11	LED POWER
4	LED RESET	8	LED BUS-COM		

2 Funktion

2.1 Systeminformation

Das Gerät ist updatefähig. Firmware-Updates können komfortabel durchgeführt werden.

Das Gerät ist KNX Data Secure fähig. KNX Data Secure bietet Schutz vor Manipulation in der Gebäudeautomation und kann im ETS-Projekt konfiguriert werden. Detaillierte Fachkenntnisse werden vorausgesetzt. Zur sicheren Inbetriebnahme ist ein Gerätezertifikat erforderlich, das auf dem Gerät angebracht ist. Im Zuge der Montage ist das Gerätezertifikat vom Gerät zu entfernen und sicher aufzubewahren.

Planung, Installation und Inbetriebnahme des Gerätes erfolgen mit Hilfe der ETS ab Version 5.7.

2.2 Bestimmungsgemäßer Gebrauch

- Versorgung von KNX-Geräten mit Busspannung
- Verbindung von KNX-Geräten mit PC oder anderen Datenverarbeitungsgeräten via IP
- Betrieb als Datenschnittstelle
- Montage auf Hutschiene gemäß DIN EN 60715 in Unterverteiler

2.3 Produkteigenschaften

- Ausgang mit integrierter Drossel zur Versorgung von KNX-Buslinien
- Zurücksetzen von KNX-Buslinien über Reset-Taste oder Kommunikationsobjekt
- Kurzschlussfest
- Überspannungsfest
- Leerlaufsicher
- Unterstützung von KNX Data Secure ab ETS Version 5.7
- Unterstützung von KNX IP Secure ab ETS Version 5.7
- LED-Anzeige für KNX-Kommunikation, Ethernet-Kommunikation und Programmiermodus
- Konfiguration über ETS
- SNTP-Server
- Max. 8 Verbindungen zu IP-Endgeräten, z.B. zum gleichzeitigen Visualisieren und Konfigurieren
- Galvanische Trennung zwischen KNX und IP-Netzwerk

2.3.1 Applikationsprogramm A

i Es kann nur ein Applikationsprogramm pro Gerät genutzt werden.

Die Zusatzfunktionen dieses Applikationsprogramms werden bereits mit dem Auslieferungszustand des Geräts bereitgestellt.

- Präsenzüberwachung: Durch Hotelcard-Schalter bzw. Präsenzmelder
- Welcome-/Goodbye-Szenen

2.3.2 Applikationsprogramm B

i Es kann nur ein Applikationsprogramm pro Gerät genutzt werden.

Die Zusatzfunktionen dieses alternativen Applikationsprogramms sind erst nach einem Firmwareupdate des Geräts verfügbar.

Voraussetzung:
Fernzugrifflizenz (Art.-Nr.: IPS-L)

- Verschlüsselter Zugriff auf KNX-Geräte zur Konfiguration und Wartung außerhalb des lokalen Netzwerkes
- Freigabe des Zugriffs über Kommunikationsobjekte
- Rückmeldung über Zugriff und Programmiervorgänge über Kommunikationsobjekte

3 Montage und elektrischer Anschluss

3.1 Information für Elektrofachkräfte

GEFAHR
Elektrischer Schlag bei Berühren spannungsführender Teile in der Einbauumgebung.
Elektrischer Schlag kann zum Tod führen.
Vor Arbeiten am Gerät freischalten und spannungsführende Teile in der Umgebung abdecken!

3.2 Montage

Umgebungstemperatur beachten. Für ausreichend Kühlung sorgen.

- Gerät auf Hutschiene montieren.

3.3 Anschluss

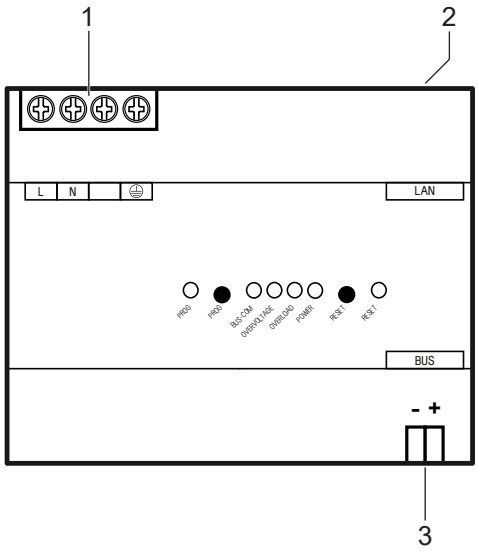


Abb. 2: Anschluss

1 Anschluss Netz
2 Anschluss KNX
3 Anschluss LAN

Voraussetzungen:

- Ethernetverbindung mit 10/100 Mbit
- KNX/EIB-Busverbindung
- Stromversorgung über einen geeigneten Leitungsschutzschalter

- Schutzleiter und Netzspannung anschließen.
- LAN und KNX anschließen.

i Die Buslast darf den Ausgangsstrom nicht überschreiten.

i An den Busausgang keine anderen Produkte anschließen. Die Buskommunikation kann hierdurch beeinflusst werden.

4 Inbetriebnahme

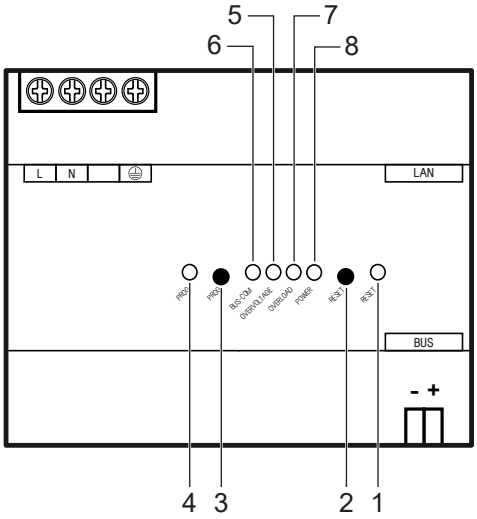


Abb. 3: Inbetriebnahme

1	LED RESET	5	LED BUS-COM
2	Taste RESET	6	LED OVERVOLTAGE
3	Taste PROG	7	LED OVERLOAD
4	LED PROG	8	LED POWER

4.1 Einschalten

Nach dem Anschließen wird das Gerät automatisch eingeschaltet.

4.2 Bootvorgang

Nach dem Einschalten startet der automatische Bootvorgang. Während des Bootvorgangs blinken die sechs LEDs auf der Frontseite des Geräts als Lauflicht.

Die Dauer des Bootvorgangs verlängert sich, wenn dem Gerät die IP-Adresse per DHCP zugewiesen wird. DHCP wird durch die Werkseinstellungen vorgegeben. Während der Zuweisung der IP-Adresse blinkt die grüne LED POWER.

Am Ende des Bootvorgangs leuchtet die grüne LED POWER.

5 Bedienung

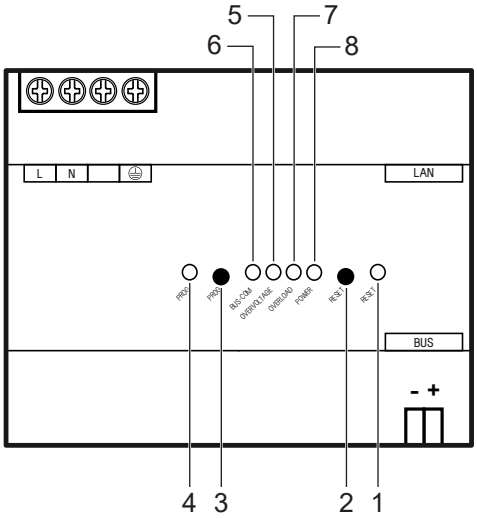


Abb. 4: Bedienung

1	LED RESET	5	LED BUS-COM
2	Taste RESET	6	LED OVERVOLTAGE
3	Taste PROG	7	LED OVERLOAD
4	LED PROG	8	LED POWER

5.1 LED-Anzeigen

Auf der Frontseite des Gerätes befinden sich sechs LEDs. Die LEDs signalisieren während des Betriebs folgende Gerätezustände:

- LED PROG leuchtet/blinkt rot:
  Programmiermodus ist aktiviert.
- LED BUS-COM leuchtet/blinkt gelb:
  Leuchtet: Spannung am Gerätebus ist normal.
  Blinkt: Gerätebus ist aktiv.
- LED OVERVOLTAGE leuchtet gelb:
  Spannung am Gerätebus ist zu hoch.
- LED OVERLOAD leuchtet rot:
  Überlast am Gerätebus
- LED POWER leuchtet/blinkt grün:
  Leuchtet: Gerät ist betriebsbereit.
  Blinkt: Überlast oder zu hohe Spannung
- LED RESET leuchtet rot:
  Gerätebus wird zurückgesetzt.

5.2 Programmiermodus

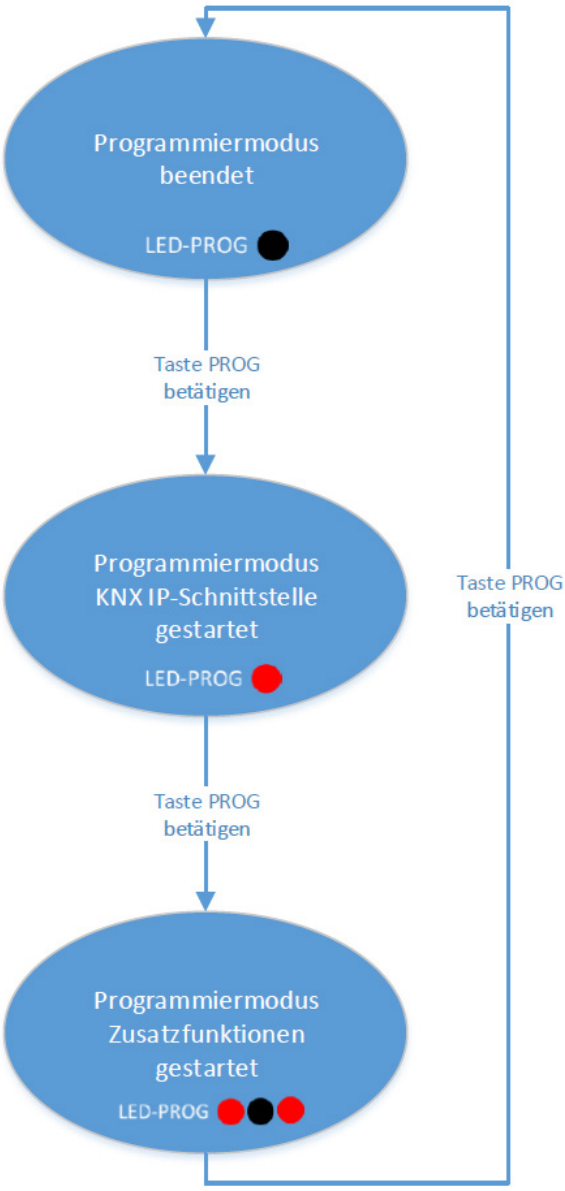


Abb. 5: Programmiermodus

Schnittstelle programmieren:

- Taste PROG betätigen.
  LED PROG leuchtet rot.

Zusatzfunktionen programmieren:

- Taste PROG erneut betätigen.
  LED PROG blinkt rot.

Programmiermodus beenden:

- Taste PROG erneut betätigen.

5.3 Diagnosemeldungen

Diagnosemeldungen quittieren:

- Taste RESET kurz betätigen.

5.4 Reset

Gerätebus für 20 Sekunden zurücksetzen:

- Taste RESET für 2 ... 4 Sekunden betätigen.
  LED RESET leuchtet rot.
  Spannungsversorgung am Gerätebus wird unterbrochen und Gerätebus wird kurzgeschlossen.
  Spannung wird wieder eingeschaltet.

5.5 Master-Reset

- Sicherstellen, dass das Gerät ausgeschaltet ist (Versorgungsspannung trennen).
- Taste PROG drücken, gedrückt halten und Versorgungsspannung anschließen.
  Das Gerät wird eingeschaltet.
- Taste PROG gedrückt halten bis die LED PROG langsam blinkt (ca. 1 Hz).
- Taste PROG loslassen.
- Taste PROG erneut drücken und gedrückt halten bis die LED PROG schnell blinkt (ca. 4 Hz).
  Der Master-Reset wird durchgeführt.
- Taste PROG kann nun losgelassen werden.

6 Konfiguration

Bis Firmware-Version 1.050 (z. B. 1.006) besteht das Gerät aus einer Kombination von folgenden Geräten:

- Spannungsversorgung mit IP-Schnittstelle
- Spannungsversorgung mit IP-Schnittstelle - Zusatzfunktionen

Die Zusatzfunktionen können beispielsweise für eine Hotelzimmersteuerung genutzt werden.

Alternativ kann das Gerät ab Firmware-Version 1.050 (z. B. 1.056) aus einer Kombination von folgenden Geräten bestehen:

- Spannungsversorgung mit IP-Schnittstelle
- KNX IP-Schnittstelle - Zusatzfunktionen

Die Konfiguration der beiden Geräte erfolgt über die ETS 5.

Um die volle Funktionalität nutzen zu können, sind für beide Geräte Produktapplikationen notwendig.

Beide Geräte benötigen eine eindeutige physikalische Adresse in der ETS.

6.1 Topologie

Um die Spannungsversorgung mit IP-Schnittstelle in ein ETS-Projekt einzufügen, muss dieses eine TP-Line besitzen, in welche die Spannungsversorgung und die Zusatzfunktionen als Geräte eingefügt werden.

6.2 Geräteeigenschaften

6.2.1 Allgemein

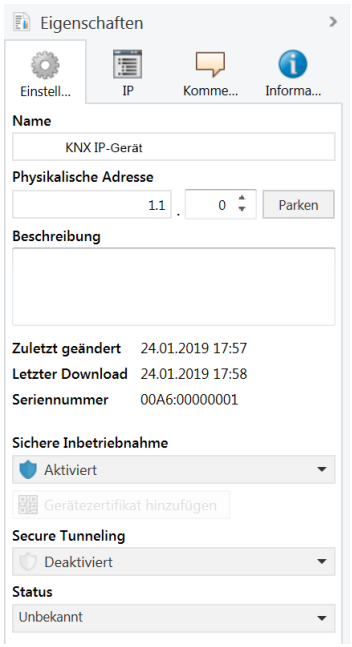


Abb. 6: Eigenschaften des Geräts

Funktion	Beschreibung
Name	Es kann ein beliebiger Name vergeben werden, max. 50 Zeichen.
Sichere Inbetriebnahme	Wenn aktiviert, ist die Verschlüsselung für die Inbetriebnahme aktiv: Es werden dann alle Parameter bereits verschlüsselt übertragen, wenngleich z. B. Tunnelverbindungen noch unverschlüsselt genutzt werden.
Secure Tunneling	Wenn aktiviert, können die Tunnelverbindungen nur über KNX Secure Tunneling aufgebaut werden.

6.2.2 IP-Einstellungen

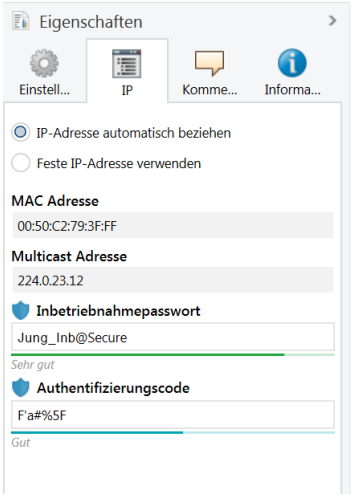


Abb. 7: IP-Einstellungen des Geräts

Funktion	Beschreibung
IP-Adresse automatisch beziehen	Die Zuteilung der IP-Adresse erfolgt mittels eines DHCP-Servers im Netzwerk. Falls kein DHCP-Server im Netzwerk existiert bzw. falls dieser keine IP-Adresse innerhalb einer Minute zuweist, dann weist sich das Gerät mittels AutoIP-Funktion selbst eine IP-Adresse zu. Dadurch ist es bspw. möglich, per Direktverbindung (ohne einen DHCP-Server) eine IP-Verbindung zwischen PC und IP-Schnittstelle aufzubauen.
Feste IP-Adresse verwenden	Der Anwender gibt die IP-Einstellungen selbst vor.
Inbetriebnahmepasswort	Ein Passwort, aus welchem die ETS einen Schlüssel generiert. Dieser ist der Schlüssel für die Sichere Inbetriebnahme (s. o.).
Authentifizierungscode	Mit dem Authentifizierungspasswort beweist der Anwender, dass er Zugriff auf das Projekt hat.
MAC-Adresse	Wird vom Gerät vorgegeben.
Multicast-Adresse	Wird vom Backbone vorgegeben. Kann in der Topologieansicht der ETS geändert werden.

6.2.3 KNX IP Secure

Für einen fehlerfreien Betrieb der Geräte im abgesicherten Modus (Secure Mode) benötigt man die ETS 5.7.4 oder höher.

Voraussetzungen:

- Sichere Inbetriebnahme aktiviert
- FDSK eingegeben/eingescannt bzw. Gerätezertifikat hinzugefügt

Konfiguration von KNX IP Secure:

- Secure Tunneling aktivieren.
- Passwort für jeden Tunnel (max. 8 Tunnel) festlegen.
- Passwort für Inbetriebnahme und Authentifizierungscode festlegen.

ⓘ Alle Passwörter dokumentieren und sicher aufbewahren.

6.2.4 Zusatzfunktionen

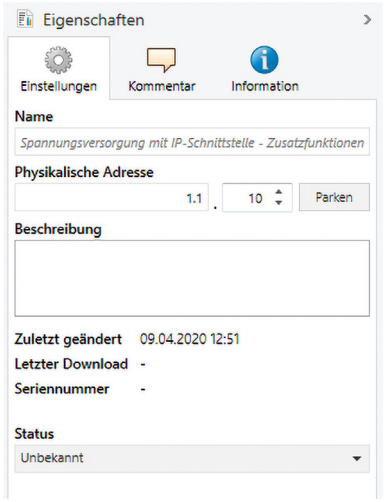


Abb. 8: Zusatzfunktionen Eigenschaften des Geräts

Funktion	Beschreibung
Name	Es kann ein beliebiger Name vergeben werden, max. 50 Zeichen.

6.2.5 KNX Data Secure

KNX Data Secure signiert und verschlüsselt die Kommunikation im KNX-Netzwerk und gewährleistet eine gesicherte Datenübertragung von Telegrammen.

Die Kommunikation bei Inbetriebnahmevorgängen mit der ETS und die Laufzeitkommunikation zwischen Geräten sowie zu Visualisierungen ist hierdurch gesichert. Somit wird gewährleistet, dass unabhängig vom Medium alle oder nur ausgewählte KNX-Telegramme authentifiziert und verschlüsselt werden. Die Kommunikation zwischen Sender und Empfänger ist weder interpretierbar noch manipulierbar.

Voraussetzungen:

- ETS 5.7.4 oder höher
- FDSK eingegeben/eingescannt bzw. Gerätezertifikat hinzugefügt

Symbole

Symbol	Bedeutung	KNX Data Secure	Sichere Inbetriebnahme
	Gerätesicherheit nicht aktiviert	Gerät ist kompatibel	deaktiviert
	Gerätesicherheit aktiviert	Gerät ist kompatibel	aktiviert
	keine Gerätesicherheit vorhanden	Gerät ist nicht kompatibel	nicht möglich
	Gerät mit aktivierter Gerätesicherheit in Applikation	Gerät ist kompatibel	aktiviert

Die ETS kennzeichnet kompatible Geräte für KNX Data Secure mit einem „Secure Shield“-Symbol. Das Symbol wird in der Listenansicht der Geräte und in der Baumstruktur eines geöffneten ETS-Projekts angezeigt. Es bezieht sich nicht direkt auf das Gerät, sondern auf das verwendete Applikationsprogramm.

Sobald in der Listenansicht in der Spalte „Sicherheit“ ein Symbol angezeigt wird, handelt es sich um ein Applikationsprogramm, das für KNX Data Secure geeignet ist. Die Farbe des Symbols weist darauf hin, dass es sich entweder um ein Applikationsprogramm mit aktivierter Gerätesicherheit (blau) handelt oder die Gerätesicherheit bei der verwendeten Applikation deaktiviert (grau) ist.

Applikationsprogramme, zu denen kein Symbol in der Listenansicht angezeigt wird, sind grundsätzlich nicht für Data Secure geeignet. In der Baumstruktur werden Geräte – entsprechend des verwendeten Applikationsprogramms – ebenso mit einem „Secure Shield“-Symbol kenntlich gemacht.

Gruppenadressen

Geräte, die zur Laufzeit über Gruppenadressen sicher kommunizieren sollen, müssen auch durch die ETS sicher in Betrieb genommen werden. Gruppenadressen werden vom Benutzer der ETS angelegt und erhalten dabei ein besonderes Sicherheitsattribut, das nachträglich editiert werden kann.

Gruppenadressen können mit folgenden Sicherheitsattributen gekennzeichnet werden:

- Unsecure – Kommunikation ist immer herkömmlich
- Secure – Kommunikation ist immer sicher
- Automatisch Unsecure oder Secure – Kommunikation ist abhängig von der Verknüpfung zu Objekten

Nur die sicheren Gruppenadressen besitzen eine Verschlüsselung zur Laufzeit. Kompatible Geräte für KNX Data Secure, die durch die ETS sicher in Betrieb genommen wurden und auch über Kommunikationsobjekte zur Laufzeit gesicherte Daten mit anderen Data Secure fähigen Geräten austauschen, können grundsätzlich über ausgewählte Gruppenadressen auch herkömmlich (Unsecure) kommunizieren. Ein kombinierter Betrieb von sicherer und herkömmlicher Kommunikation ist an einem Sensor oder Aktor über unterschiedliche Kommunikationsobjekte möglich. Allerdings ist das Kommunizieren per Secure und Unsecure über ein und dieselbe Gruppenadresse und folglich dasselbe Objekt nicht möglich!

6.3 Gerätespezifische Parameter

6.3.1 Allgemeine Einstellungen

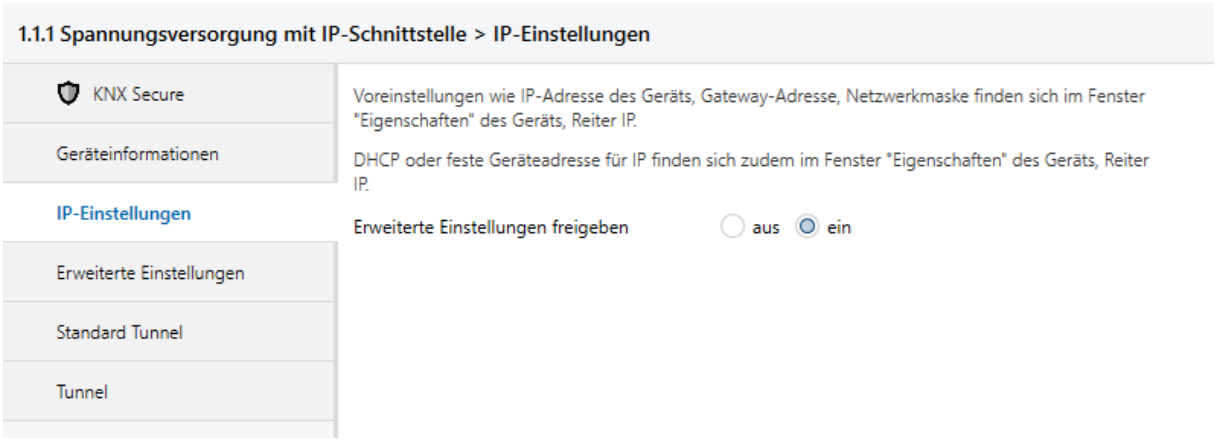


Abb. 9: Allgemeine Einstellungen des Geräts

Funktion	Auswahl	Beschreibung
(Erläuternder Text)		Die ETS hat herstellerunabhängig einheitliche Parameterbeschreibungen für verschiedene Einstellungen. Um die Anwendung zu vereinfachen, wird hier ein Hinweistext eingeblendet.
Erweiterte Einstellungen freigeben	aus/ein	Erweiterte Funktionen, um den Anwendern die max. Flexibilität zu gewährleisten.

6.3.2 Erweiterte Einstellungen

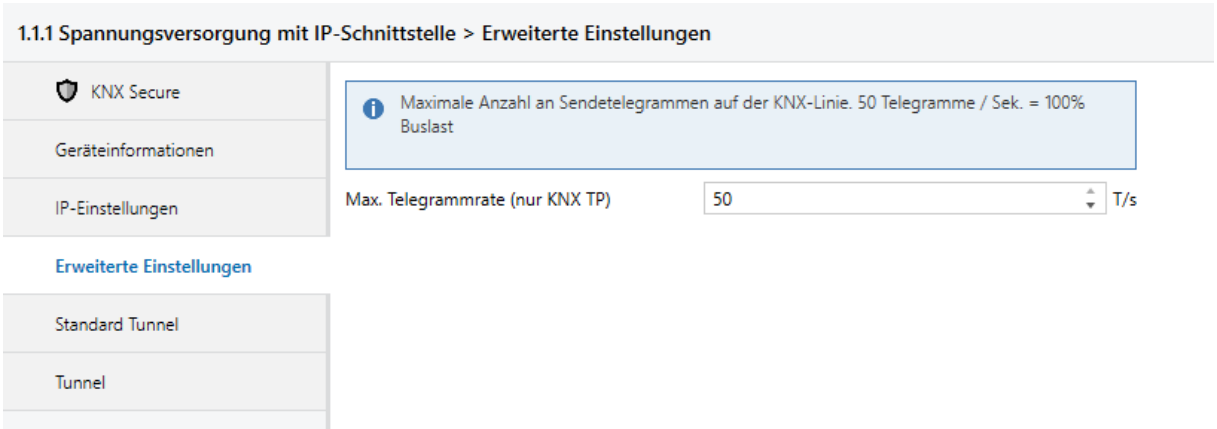


Abb. 10: Erweiterte Einstellungen des Geräts

Funktion	Auswahl	Beschreibung
Max. Telegrammrate	5 .. 50	Vgl. Parameterbeschreibung

Erweiterte Einstellungen Standard Tunnel bevorzugte IP

Die KNX IP-Schnittstellen bieten für Standard-Tunnelverbindungen (vor 2019) die Möglichkeit, jede dieser Tunnelverbindungen jeweils einer IP-Adresse zuzuordnen. Dies ermöglicht bei der Analyse von Gruppentelegrammen eine leichtere Zuordnung der Telegramme zum Sender, der hinter dem Tunnel „sitzt“, wie z. B. Visualisierungen oder Smartphone-Apps.

ⓘ Diese Zuordnung kann allerdings jederzeit durch die ETS oder eine neue sog. erweiterte Tunnelverbindung (Stand 2019) aufgelöst werden.

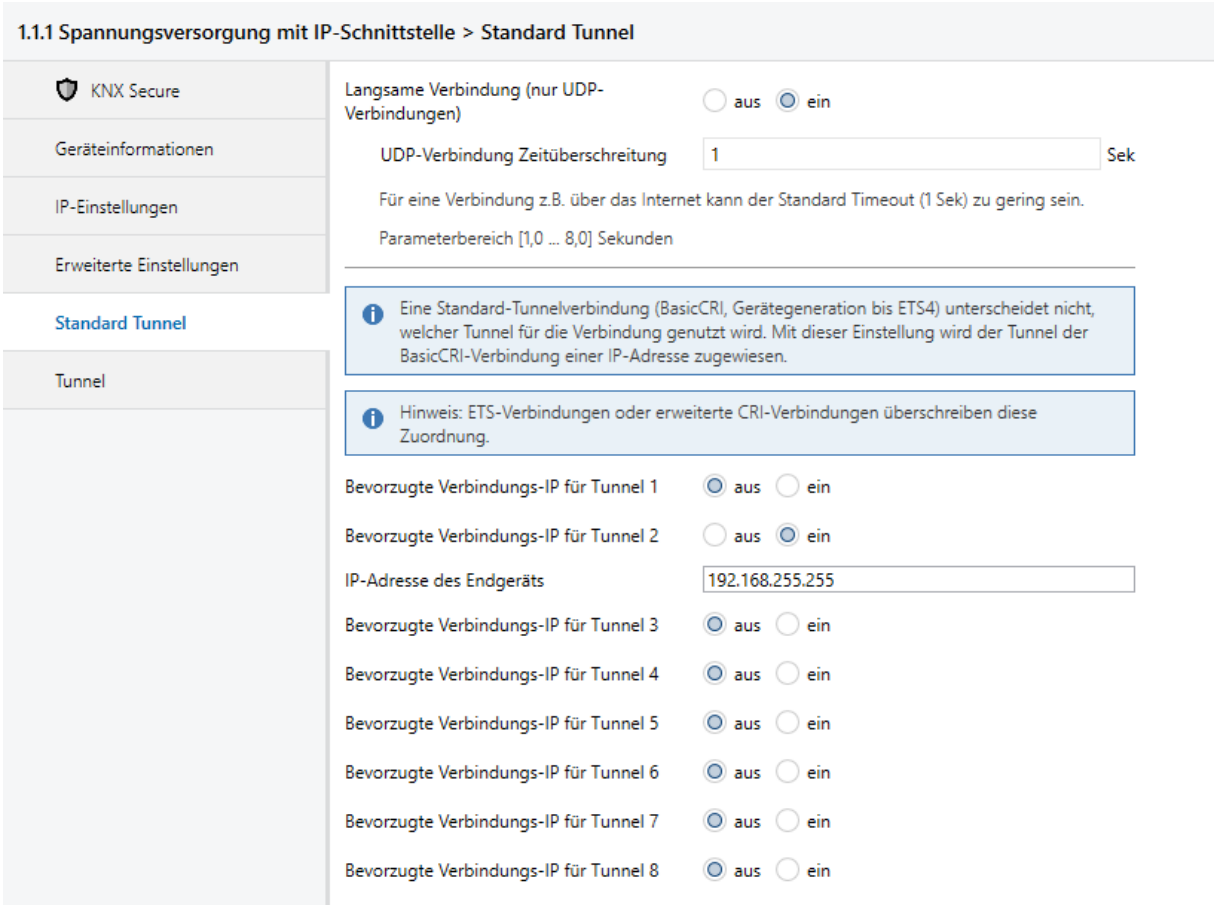


Abb. 11: Bevorzugte Verbindungs-IP für Tunneling

Funktion	Auswahl	Beschreibung
Langsame Verbindung	aus/ein	Die Tunnelverbindungen über UDP werden standardmäßig mit einem Verbindungstimeout von 1 Sekunde betrieben. Dies kann bei Verbindungen über das Internet zu kurz sein.
UDP-Verbindung Zeitüberschreitung	1,0 ... 8,0 sec	Einstellung des Timeouts für UDP-Tunnelverbindungen
Bevorzugte Verbindungs-IP für Tunnel X	aus/ein	Tunnel X soll bevorzugt für eine IP-Adresse verwendet werden.
IP-Adresse des Endgeräts	(IP-V4-Adresse)	IP-Adresse des Endgeräts

6.4 Allgemeine Einstellungen

6.4.1 Applikationsprogramm A

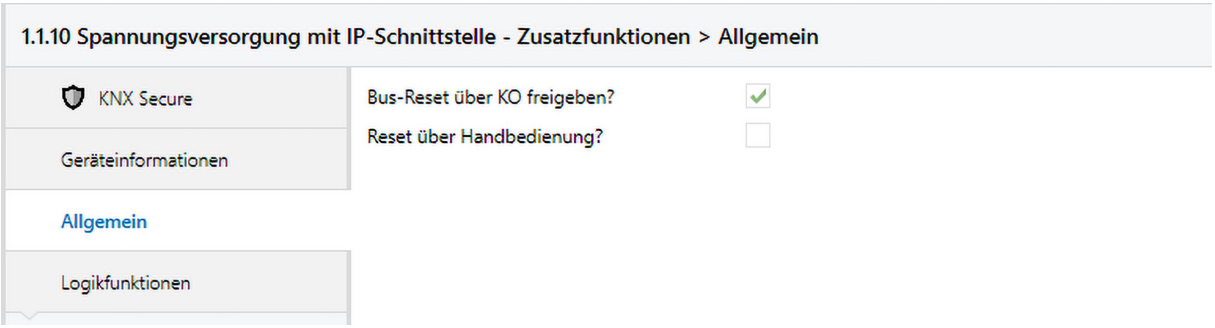


Abb. 12: Allgemeine Einstellungen des Geräts

Funktion	Auswahl	Beschreibung
Bus-Reset über KO freigeben?	aktiv/inaktiv	Gibt ein Kommunikationsobjekt frei, um einen Bus-Reset auszulösen.
Reset über Handbedienung?	aktiv/inaktiv	Wenn aktiviert, kann der Reset über den Reset-Taster am Gerät ausgelöst werden. Wenn inaktiv, dann ist die Funktion des Reset-Tasters gesperrt. In diesem Fall ist auch die Rückstellung der Fehlerzustände (Überspannung und Überlast) per Reset-Taster nicht mehr möglich.

Logikfunktionen

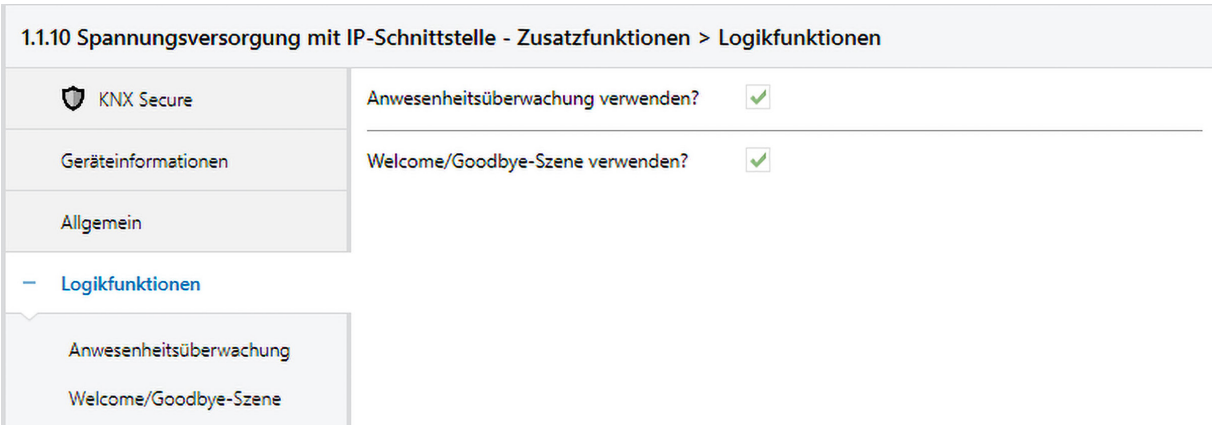


Abb. 13: Logikfunktionen

Funktion	Auswahl	Beschreibung
Anwesenheitsüberwachung verwenden?	aktiv/inaktiv	Wenn aktiviert, wird die Seite Anwesenheitsüberwachung freigegeben. Auf dieser Seite kann konfiguriert werden wie die Anwesenheit (Hotelcard-Schalter oder Präsenzmelder) überwacht wird und welche Szenen bei Erkennung von Anwesenheit und Abwesenheit ausgelöst werden.
Welcome/Goodbye-Szene verwenden?	aktiv/inaktiv	Wenn aktiviert, wird die Seite Welcome/Goodbye-Szene freigegeben. Auf dieser Seite kann konfiguriert werden unter welchen Bedingungen die Welcome- und Goodbye-Szene aktiviert werden und welche Szenen bei der Erkennung der Welcome- und Goodbye-Szene ausgelöst werden.

Anwesenheitsüberwachung

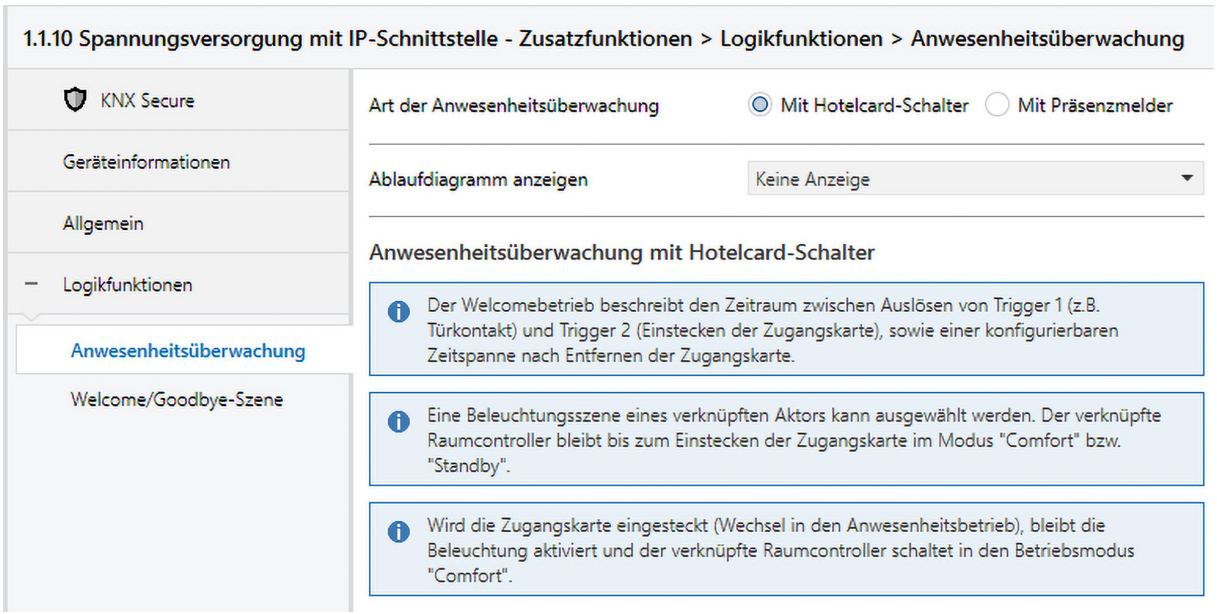


Abb. 14: Anwesenheitsüberwachung

Funktion	Auswahl	Beschreibung
Art der Anwesenheitsüberwachung	Mit Hotelcard-Schalter/ Mit Präsenzmelder	Wenn aktiviert, wird die Seite Anwesenheitsüberwachung freigegeben. Auf dieser Seite kann konfiguriert werden wie die Anwesenheit (Hotelcard-Schalter oder Präsenzmelder) überwacht wird und welche Szenen bei Erkennung von Anwesenheit und Abwesenheit ausgelöst werden.

Anwesenheitsüberwachung Hotelcard-Schalter

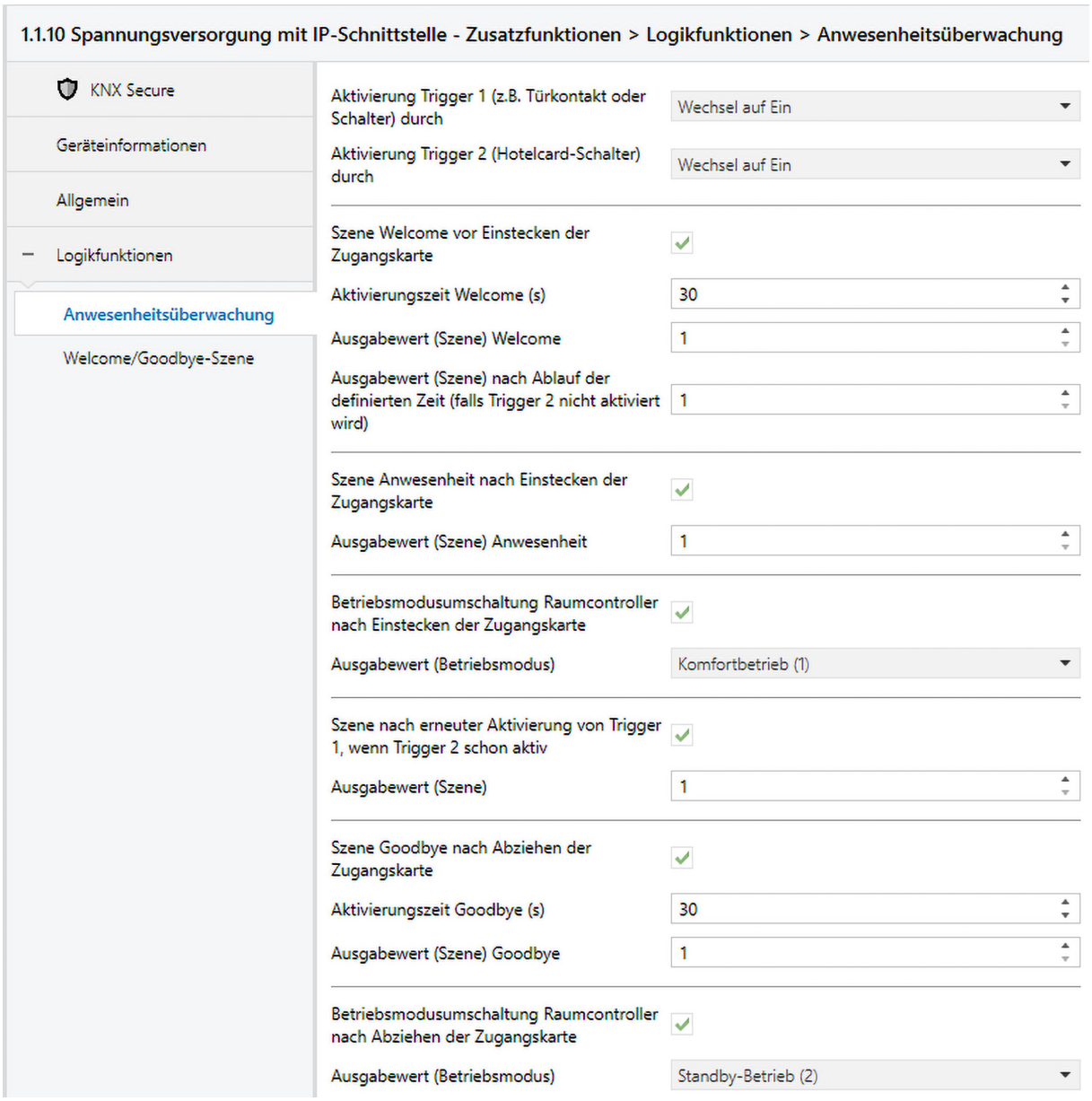


Abb. 15: Anwesenheitsüberwachung Hotelcard-Schalter

Funktion	Auswahl	Beschreibung
Aktivierung Trigger 1 (z. B. Türkontakt oder Schalter) durch	Wechsel auf Ein/ Wechsel auf Aus/ Umschalten	Es kann gewählt werden, wie der Trigger 1 aktiviert wird. Bei der Einstellung „Umschalten“ erfolgt die Aktivierung bei Wechsel auf Ein und Wechsel auf Aus.
Aktivierung Trigger 2 (Hotelcard-Schalter) durch	Wechsel auf Ein/ Wechsel auf Aus/ Umschalten	Es kann gewählt werden, wie der Trigger 2 aktiviert wird. Bei der Einstellung „Umschalten“ erfolgt die Aktivierung bei Wechsel auf Ein und Wechsel auf Aus.

Funktion	Auswahl	Beschreibung
Szene Welcome vor Einstecken der Zugangskarte	aktiv/inaktiv	Wenn aktiv, dann wird die Szene Welcome bei Aktivierung von Trigger 1 ausgelöst. Die Szene wird jedoch nur dann ausgelöst, wenn am Zeitpunkt der Aktivierung von Trigger 1 der Trigger 2 nicht aktiv ist, d. h. bspw. wenn die Tür öffnet aber noch keine Hotelcard gesteckt ist.
Aktivierungszeit Welcome (s)	1 .. 30 .. 120	Dauer, die die Szene Welcome aktiv ist. Nach dieser Zeit wechselt die Szene der Szenennebenstelle (KO16) vom Parameter „Ausgabewert Welcome“ zum Parameter „Ausgabewert nach Ablauf der definierten Zeit“.
Ausgabewert (Szene) Welcome	1 .. 64	Wert, der auf die Szenennebenstelle (KO16) bei Aktivierung der Szene Welcome gesendet wird.
Ausgabewert (Szene) nach Ablauf der definierten Zeit (falls Trigger 2 nicht aktiviert wird)	1 .. 64	Wert, der auf die Szenennebenstelle (KO16) nach Ablauf der Szene Welcome gesendet wird.
Szene Anwesenheit nach Einstecken der Zugangskarte	aktiv/inaktiv	Wenn aktiv, dann wird die Szene Anwesenheit bei Aktivierung von Trigger 2 ausgelöst. Die Aktivierung erfolgt jedoch nicht, falls aktuell der Zeitverzögerungs-Timer für die Goodbye-Funktion aktiv ist. Damit wird das Retriggern der Szene Anwesenheit vermieden, falls die Karte mehrmals hintereinander gesteckt und gezogen wird.
Ausgabewert (Szene) Anwesenheit	1 .. 64	Wert, der auf die Szenennebenstelle (KO16) bei Aktivierung der Szene Anwesenheit gesendet wird.
Betriebsmodusumschaltung Raumcontroller nach Einstecken der Zugangskarte	aktiv/inaktiv	Wenn aktiv, dann wird der Betriebsmodus des Raumcontrollers bei Aktivierung von Trigger 2 gemäß dem nachfolgenden Parameter "Ausgabewert (Betriebsmodus)" gesendet.
Ausgabewert (Betriebsmodus)	Automatik (0)/ Komfortbetrieb (1)/ Standby-Betrieb (2)/ Nachtbetrieb (3)/ Frost-/Hitzeschutz (4)	Wert, der auf den Betriebsmodus des Raumcontrollers (KO32) bei Aktivierung von Trigger 2 gesendet wird.
Szene nach erneuter Aktivierung von Trigger 1, wenn Trigger 2 schon aktiv	aktiv/inaktiv	Hier kann eine weitere Szene ausgelöst werden, wenn bei aktivem Trigger 2 der Trigger 1 erneut aktiviert wird. Die Szene kann bspw. das Szenario „2. Person betritt den Raum“ bedienen.
Ausgabewert (Szene)	1 .. 64	Wert, der auf die Szenennebenstelle (KO16) bei Aktivierung von Trigger 1 gesendet wird, wenn Trigger 2 aktiv ist.

Funktion	Auswahl	Beschreibung
Szene Goodbye nach Abziehen der Zugangskarte	aktiv/inaktiv	Wenn aktiv, dann wird bei Deaktivierung von Trigger 2 die Szene Goodbye mit einer Zeitverzögerung ausgelöst. Die Zeitverzögerung wird im Parameter „Aktivierungszeit Goodbye (s)" eingestellt.
Aktivierungszeit Goodbye (s)	1 .. 30 .. 120	Zeitverzögerung in Sekunden, mit der die Szene Goodbye ausgelöst wird.
Ausgabewert (Szene) Goodbye	1 .. 64	Wert, der auf die Szenennebenstelle (KO16) bei Aktivierung der Szene Goodbye gesendet wird.
Betriebsmodusumschaltung Raumcontroller nach Abziehen der Zugangskarte	aktiv/inaktiv	Wenn aktiv, dann wird bei Deaktivierung von Trigger 2 der Betriebsmodus des Raumcontrollers gemäß dem nachfolgenden Parameter „Ausgabewert (Betriebsmodus)“ gesendet. Dies geschieht ohne Zeitverzögerung.
Ausgabewert (Betriebsmodus)	Automatik (0)/ Komfortbetrieb (1)/ Standby-Betrieb (2)/ Nachtbetrieb (3)/ Frost-/Hitzeschutz (4)	Wert, der auf den Betriebsmodus des Raumcontrollers (KO32) bei Deaktivierung von Trigger 2 gesendet wird.

Anwesenheitsüberwachung Präsenzmelder

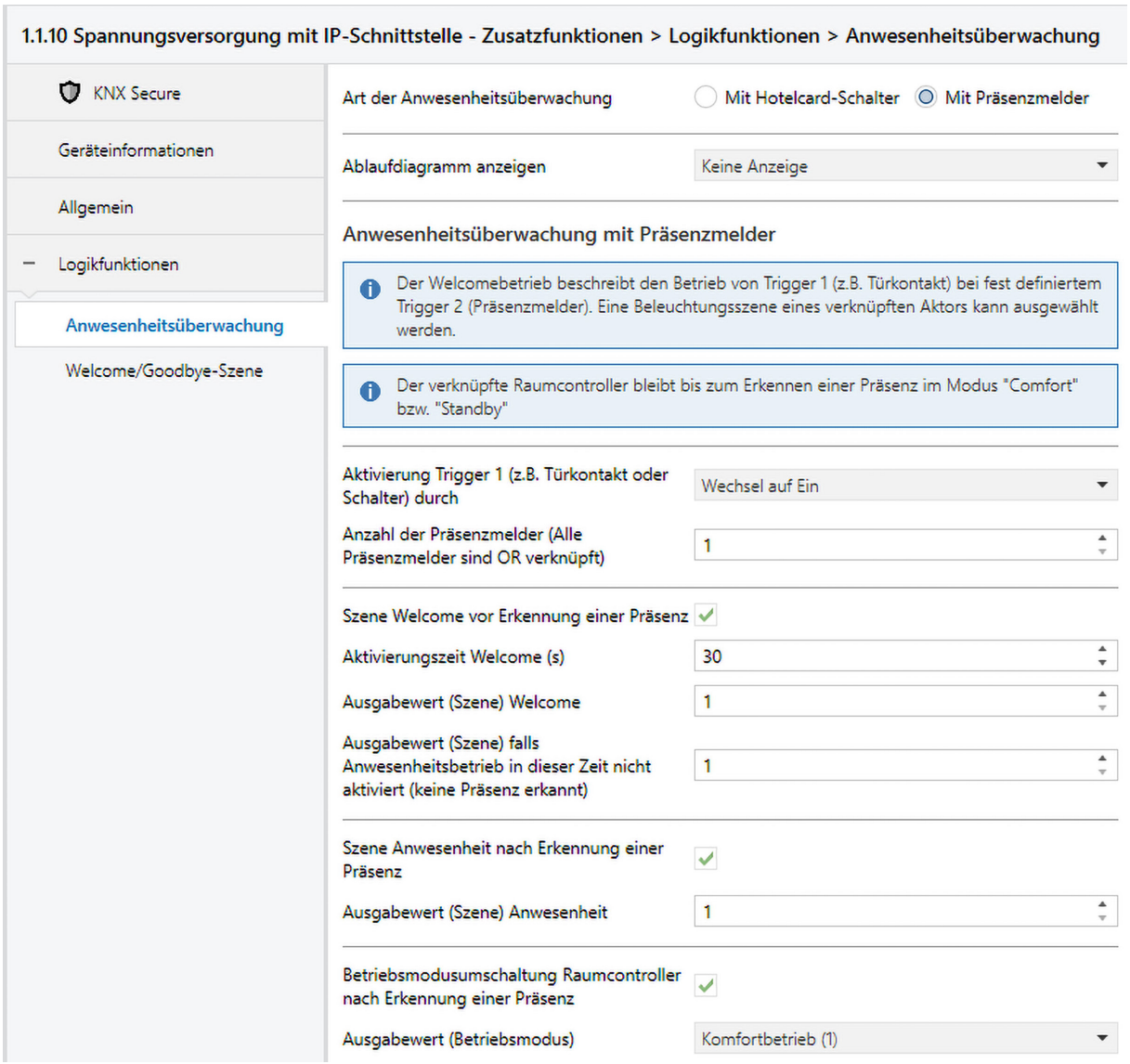


Abb. 16: Anwesenheitsüberwachung Präsenzmelder

Funktion	Auswahl	Beschreibung
Aktivierung Trigger 1 (z. B. Türkontakt oder Schalter) durch	Wechsel auf Ein/ Wechsel auf Aus/ Umschalten	Es kann gewählt werden, wie der Trigger 1 aktiviert wird. Bei der Einstellung „Umschalten“ erfolgt die Aktivierung bei Wechsel auf Ein und Wechsel auf Aus.
Anzahl der Präsenzmelder (Alle Präsenzmelder sind mit OR verknüpft)	1 .. 5	Es kann gewählt werden, wie viele Präsenzmelder genutzt werden. Pro gewählten Präsenzmelder wird ein KO für dessen Wert freigeschaltet. Für alle Funktionen wird immer das Ergebnis aus der OR-Verknüpfung aller Präsenzmelder verwendet.

Funktion	Auswahl	Beschreibung
Szene Welcome vor Erkennung einer Präsenz	aktiv/inaktiv	Wenn aktiv, dann wird die Szene Welcome bei Aktivierung von Trigger 1 ausgelöst. Die Szene wird jedoch nur dann ausgelöst, wenn zum Zeitpunkt der Aktivierung von Trigger 1 der Trigger 2 nicht aktiv ist, d.h. bspw. wenn zu diesem Zeitpunkt noch keine Präsenz im Raum erkannt wurde.
Aktivierungszeit Welcome (s)	1 .. 30 .. 120	Dauer, die die Szene Welcome aktiv ist. Nach dieser Zeit wechselt die Szene der Szenennebenstelle (KO16) vom Parameter „Ausgabewert Welcome“ zum Parameter „Ausgabewert falls Anwesenheit-Betrieb in dieser Zeit nicht aktiviert“.
Ausgabewert (Szene) Welcome	1 .. 64	Wert, der auf die Szenennebenstelle (KO16) bei Aktivierung der Szene Welcome gesendet wird.
Ausgabewert (Szene) falls Anwesenheitsetrieb in dieser Zeit nicht aktiviert (keine Präsenz erkannt)	1 .. 64	Wert, der auf die Szenennebenstelle (KO16) nach Ablauf der Szene Welcome gesendet wird.
Szene Anwesenheit nach Erkennung einer Präsenz	aktiv/inaktiv	Wenn aktiv, dann wird die Szene Anwesenheit bei Aktivierung von Trigger 2 ausgelöst. Die Aktivierung erfolgt jedoch nur einmalig, ab dem Zeitpunkt ab dem Trigger 1 aktiv wurde. Damit wird das Retriggern der Szene Anwesenheit vermieden, falls der Präsenzmelder mehrmals hintereinander seinen Präsenz-Status ändert.
Ausgabewert (Szene) Anwesenheit	1 .. 64	Wert, der auf die Szenennebenstelle (KO16) bei Aktivierung der Szene Anwesenheit gesendet wird.
Betriebsmodusumschaltung Raumcontroller nach Erkennung einer Präsenz	aktiv/inaktiv	Wenn aktiv, dann wird der Betriebsmodus des Raumcontrollers bei Aktivierung von Trigger 2 gemäß dem nachfolgenden Parameter „Ausgabewert (Betriebsmodus)“ gesendet.
Ausgabewert (Betriebsmodus)	Automatik (0)/ Komfortbetrieb (1)/ Standby-Betrieb (2)/ Nachtbetrieb (3)/ Frost-/Hitzeschutz (4)	Wert, der auf den Betriebsmodus des Raumcontrollers (KO32) bei Aktivierung von Trigger 2 gesendet wird.

Anwesenheitsüberwachung Präsenzmelder – Präsenzbetrieb

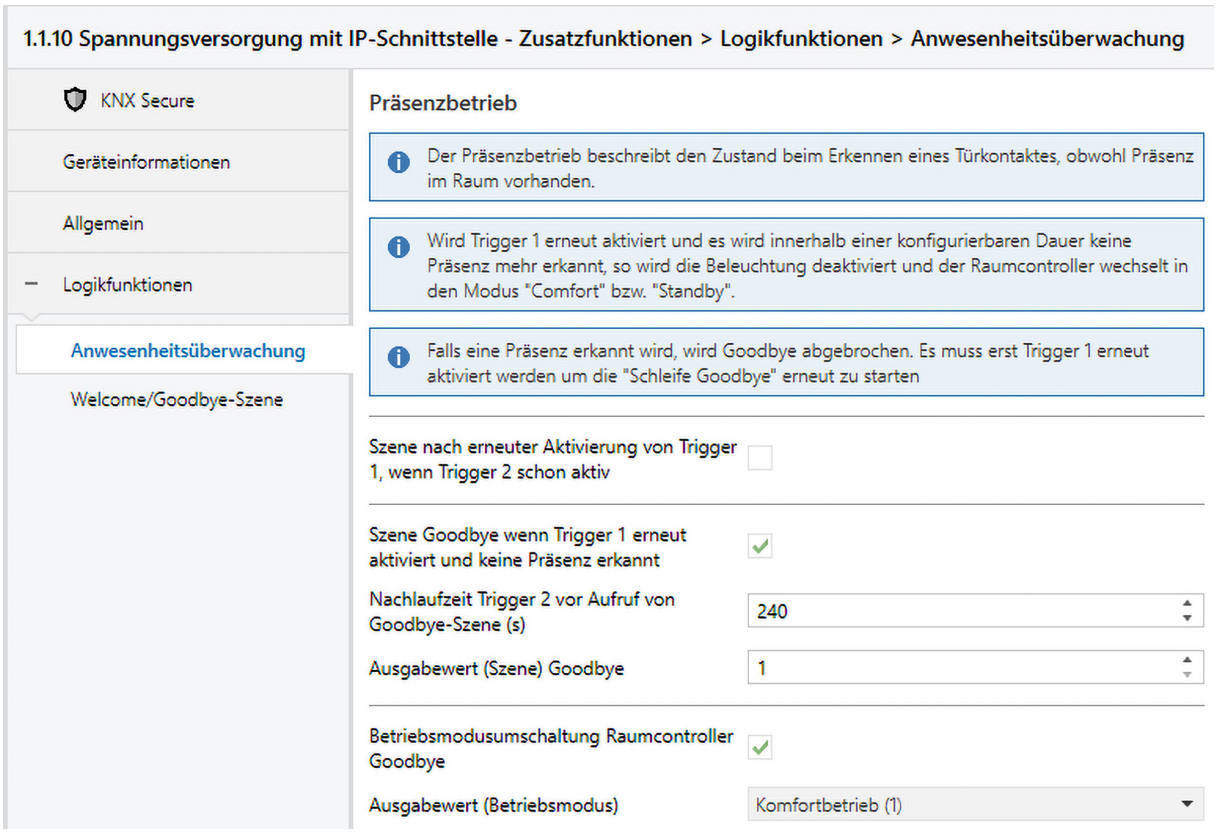


Abb. 17: Anwesenheitsüberwachung Präsenzmelder – Präsenzbetrieb

Funktion	Auswahl	Beschreibung
Szene nach erneuter Aktivierung von Trigger 1, wenn Trigger 2 schon aktiv	aktiv/<u>inaktiv</u>	Hier kann eine weitere Szene ausgelöst werden, wenn bei aktivem Trigger 2 der Trigger 1 erneut aktiviert wird. Die Szene kann bspw. das Szenario „2. Person betritt den Raum“ bedienen.
Szene Goodbye wenn Trigger 1 erneut aktiviert und keine Präsenz erkannt	<u>aktiv</u>/inaktiv	Hier kann die Szene Goodbye aktiviert werden. Die Szene Goodbye wird bei Aktivierung von Trigger 1 mit einer parametrierbaren Zeitverzögerung ausgelöst. Allerdings nur dann, wenn zum Zeitpunkt der etwaigen Szenenauslösung der Trigger 2 „AUS“ bzw. „not occupied“ ist. Die Zeitverzögerung wird im Parameter „Nachlaufzeit Trigger 2 vor Aufruf von Goodbye-Szene“ eingestellt.

Funktion	Auswahl	Beschreibung
Nachlaufzeit Trigger 2 vor Aufruf von Goodbye-Szene (s)	1 .. 30 .. 3600	Zeitverzögerung in Sekunden, mit der die Szene Goodbye nach Aktivierung durch Trigger 1 ausgelöst wird. Parametrierungshinweis: Wenn zusätzlich zur Szene Goodbye auch die Szene Welcome verwendet wird, dann sollte die Nachlaufzeit länger als die Aktivierungszeit der Szene Welcome gewählt werden. Dies verhindert ein unbeabsichtigtes dauerhaftes Leuchten der Zimmerbeleuchtung nach Verlassen des Zimmers.
Ausgabewert (Szene) Goodbye	1 .. 64	Wert, der auf die Szenennebenstelle (KO16) bei Aktivierung der Szene Goodbye gesendet wird.
Betriebsmodusumschaltung Raumcontroller Goodbye	aktiv/inaktiv	Wenn aktiv, dann wird bei Aktivierung der Szene Goodbye der Betriebsmodus des Raumcontrollers gemäß dem nachfolgenden Parameter „Ausgabewert (Betriebsmodus)“ gesendet.
Ausgabewert (Betriebsmodus)	Automatik (0)/ Komfortbetrieb (1)/ Standby-Betrieb (2)/ Nachtbetrieb (3)/ Frost-/Hitzeschutz (4)	Wert, der auf den Betriebsmodus des Raumcontrollers (KO32) bei Aktivierung der Szene Goodbye gesendet wird.

Welcome/Goodbye-Szene

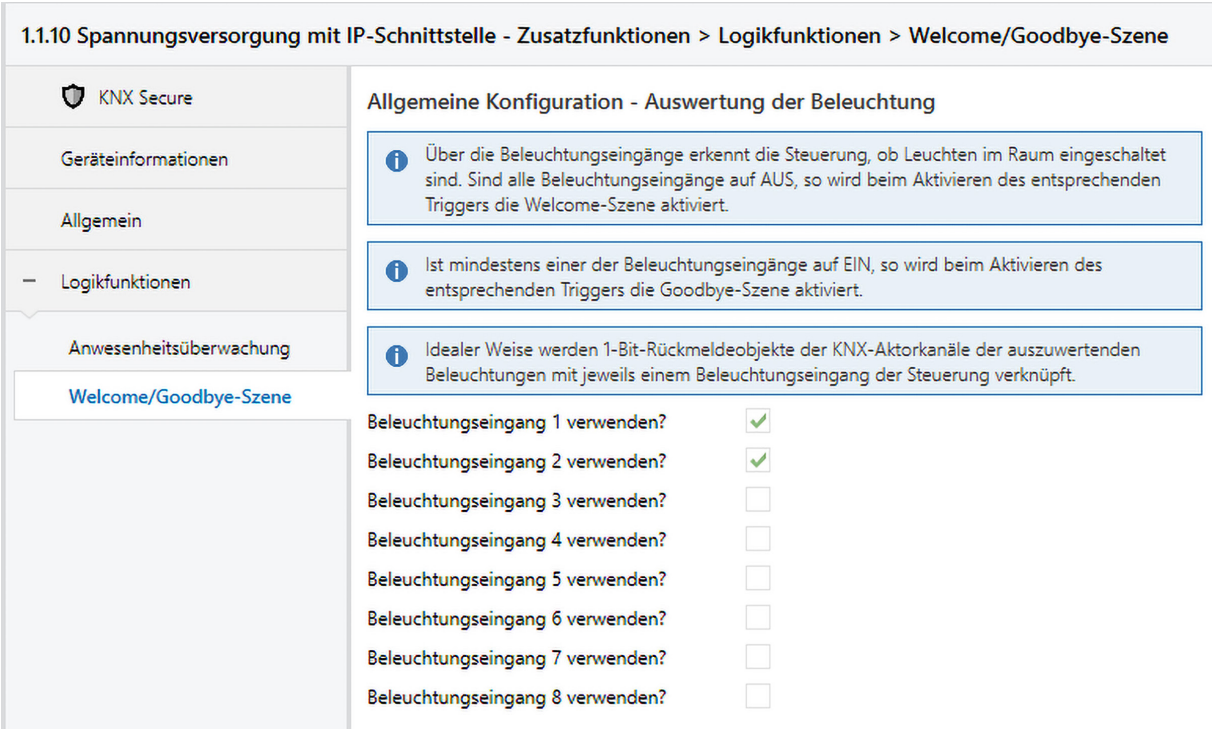


Abb. 18: Welcome/Goodbye-Szene

Funktion	Auswahl	Beschreibung
Beleuchtungseingang 1 verwenden?	aktiv/inaktiv	Wenn aktiviert, dann wird dieser Eingang (d. h. KO55) als Kriterium genutzt, ob bei Aktivierung von Trigger 1 die Welcome-Szene oder die Goodbye-Szene ausgelöst wird. Durch die Aktivierung wird das Kommunikationsobjekt 55 freigeschaltet.
Beleuchtungseingang 2 verwenden?	aktiv/inaktiv	Wenn aktiviert, dann wird dieser Eingang (d. h. KO56) als Kriterium genutzt, ob bei Aktivierung von Trigger 1 die Welcome-Szene oder die Goodbye-Szene ausgelöst wird. Durch die Aktivierung wird das Kommunikationsobjekt 56 freigeschaltet.
Beleuchtungseingang 3 .. 8 verwenden?	aktiv/inaktiv	Wenn aktiviert, dann wird dieser Eingang (d. h. KO57 .. KO62) als Kriterium genutzt, ob bei Aktivierung von Trigger 1 die Welcome-Szene oder die Goodbye-Szene ausgelöst wird. Durch die Aktivierung wird das Kommunikationsobjekt 57 .. 62 freigeschaltet.

Welcome/Goodbye-Szene – Szene Welcome

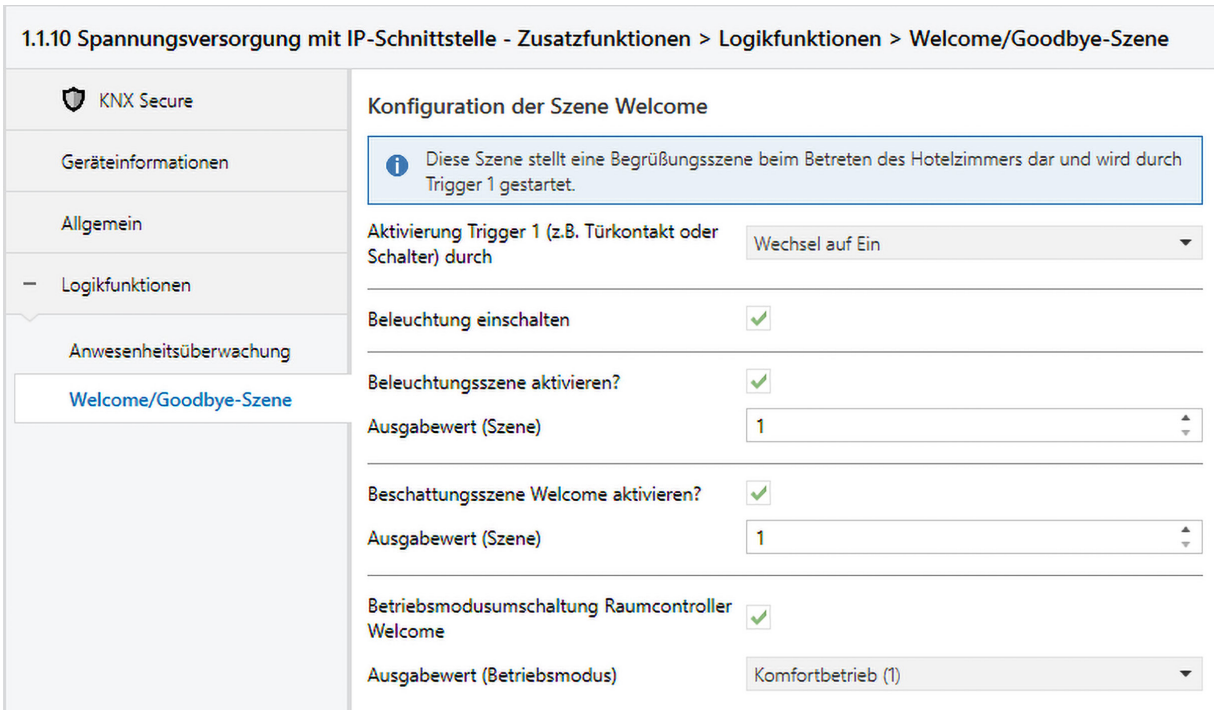


Abb. 19: Welcome/Goodbye-Szene – Szene Welcome

Funktion	Auswahl	Beschreibung
Aktivierung Trigger 1 (z. B. Türkontakt oder Schalter) durch	Wechsel auf Ein/ Wechsel auf Aus/ Umschalten	Es kann gewählt werden, wie der Trigger 1 aktiviert wird. Bei der Einstellung „Umschalten“ erfolgt die Aktivierung bei Wechsel auf Ein und Wechsel auf Aus.
Beleuchtung einschalten	aktiv/inaktiv	Wenn aktiv, dann wird bei Aktivierung der Welcome-Szene die Beleuchtung eingeschaltet, indem der Wert „EIN“ auf das Kommunikationsobjekt 165 gesendet wird.
Beleuchtungsszene aktivieren?	aktiv/inaktiv	Wenn aktiv, dann wird die Beleuchtungsszene bei Aktivierung der Welcome-Szene ausgelöst. Dadurch wird auf die Szenennebenstelle (KO194) der nachfolgend parametrierte Wert gesendet.
Ausgabewert (Szene)	1 .. 64	Wert, der auf die Szenennebenstelle (KO194) bei Aktivierung der Beleuchtungsszene gesendet wird.
Beschattungsszene Welcome aktivieren?	aktiv/inaktiv	Wenn aktiv, dann wird die Beschattungsszene bei Aktivierung der Welcome-Szene ausgelöst. Dadurch wird auf die Szenennebenstelle (KO214) der nachfolgend parametrierte Wert gesendet.
Ausgabewert (Szene)	1 .. 64	Wert, der auf die Szenennebenstelle (KO214) bei Aktivierung der Beschattungsszene gesendet wird.

Funktion	Auswahl	Beschreibung
Betriebsmodusumschaltung Raumcontroller Welcome	aktiv/inaktiv	Wenn aktiv, dann wird bei Aktivierung der Welcome-Szene der Betriebsmodus des Raumcontrollers gemäß dem nachfolgenden Parameter „Ausgabewert (Betriebsmodus)“ gesendet.
Ausgabewert (Betriebsmodus)	Automatik (0)/ Komfortbetrieb (1)/ Standby-Betrieb (2)/ Nachtbetrieb (3)/ Frost-/Hitzeschutz (4)	Wert, der auf den Betriebsmodus des Raumcontrollers (KO234) bei Aktivierung der Welcome-Szene gesendet wird.

Welcome/Goodbye-Szene – Szene Goodbye

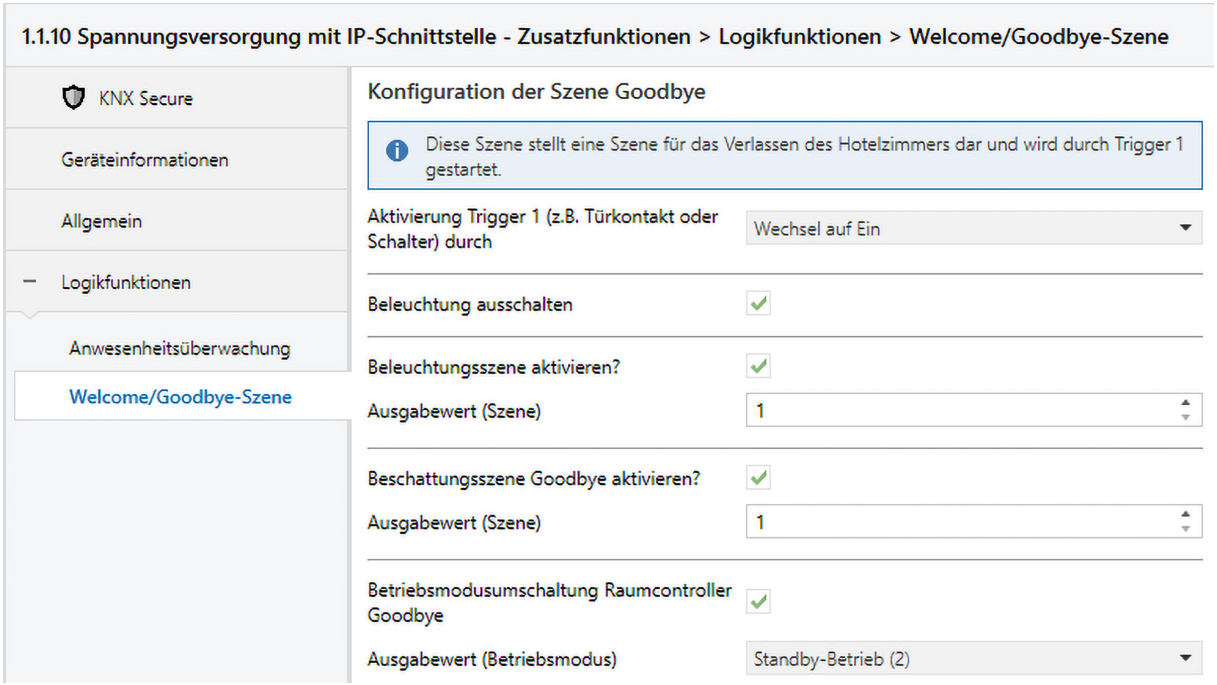


Abb. 20: Welcome/Goodbye-Szene – Szene Goodbye

Funktion	Auswahl	Beschreibung
Aktivierung Trigger 1 (z. B. Türkontakt oder Schalter) durch	Wechsel auf Ein/ Wechsel auf Aus/ Umschalten	Es kann gewählt werden, wie der Trigger 1 aktiviert wird. Bei der Einstellung „Umschalten“ erfolgt die Aktivierung bei Wechsel auf Ein und Wechsel auf Aus.
Beleuchtung ausschalten	aktiv/inaktiv	Wenn aktiv, dann wird bei Aktivierung der Goodbye-Szene die Beleuchtung ausgeschaltet, indem der Wert „OFF“ auf das Kommunikationsobjekt 166 gesendet wird.
Beleuchtungsszene aktivieren?	aktiv/inaktiv	Wenn aktiv, dann wird die Beleuchtungsszene bei Aktivierung der Goodbye-Szene ausgelöst. Dadurch wird auf die Szenennebenstelle (KO195) der nachfolgend parametrierte Wert gesendet.

Funktion	Auswahl	Beschreibung
Ausgabewert (Szene)	1 .. 64	Wert, der auf die Szenennebenstelle (KO195) bei Aktivierung der Beleuchtungsszene gesendet wird.
Beschattungsszene Goodbye aktivieren?	aktiv/inaktiv	Wenn aktiv, dann wird die Beschattungsszene bei Aktivierung der Goodbye-Szene ausgelöst. Dadurch wird auf die Szenennebenstelle (KO215) der nachfolgend parametrierte Wert gesendet.
Ausgabewert (Szene)	1 .. 64	Wert, der auf die Szenennebenstelle (KO215) bei Aktivierung der Beschattungsszene gesendet wird.
Betriebsmodusumschaltung Raumcontroller Goodbye	aktiv/inaktiv	Wenn aktiv, dann wird bei Aktivierung der Goodbye-Szene der Betriebsmodus des Raumcontrollers gemäß dem nachfolgenden Parameter „Ausgabewert (Betriebsmodus)“ gesendet.
Ausgabewert (Betriebsmodus)	Automatik (0)/ Komfortbetrieb (1)/ Standby-Betrieb (2)/ Nachtbetrieb (3)/ Frost-/Hitzeschutz (4)	Wert, der auf den Betriebsmodus des Raumcontrollers (KO234) bei Aktivierung der Goodbye-Szene gesendet wird.

6.4.2 Applikationsprogramm B

Die Zusatzapplikation stellt folgende weitere Funktionalitäten zur Verfügung:

- Zeitgeber
- Fernwartung
- Mapper

Zeitgeber

- Externer Zeitserver (NTP) als Quelle der Zeitsynchronisierung bei Inbetriebnahme
- Externer Zeitserver einstellbar auf feste IP-Adresse oder über pool.ntp.org
- Status für die Erreichbarkeit des externen Zeitservers
- Status für die Gültigkeit der internen Uhr (z. B. nach Spannungsausfall)
- Benutzergesteuerte Synchronisierung mit externem Zeitserver

Der Zeitgeber synchronisiert die Uhrzeit der eingebauten Echtzeituhr über das Internet mit pool.ntp.org oder mit einer anderen lokalen Quelle. Diese Uhrzeit kann als Zeit- bzw. Datumstelegramm auf den KNX-Bus ausgegeben werden. Bei Spannungsunterbrechung puffert das Gerät ca. 36 Stunden die Uhrzeit. Die Uhrzeit wird automatisch alle 48 Stunden und beim Neustart mit dem NTP-Server synchronisiert. Der Anwender kann über ein Kommunikationsobjekt (nachfolgend KO genannt) die Synchronisierung manuell anfordern.

Die „Gültigkeit“ der Uhrzeit wird über ein separates KO ausgegeben. Solange die eingebaute Echtzeituhr versorgt wird, ist die Uhrzeit gültig. Wenn im Normalbetrieb beispielsweise die Synchronisation nicht möglich ist, weil die Internetverbindung unterbrochen ist, so bleibt die interne Uhrzeit dennoch gültig. Die Nichterreichbarkeit des letzten Synchronisationsversuchs ist über ein getrenntes KO per Leseanforderung abzufragen. Wenn sich der Zustand ändert, wird dieser per KO auf den Bus ausgegeben.

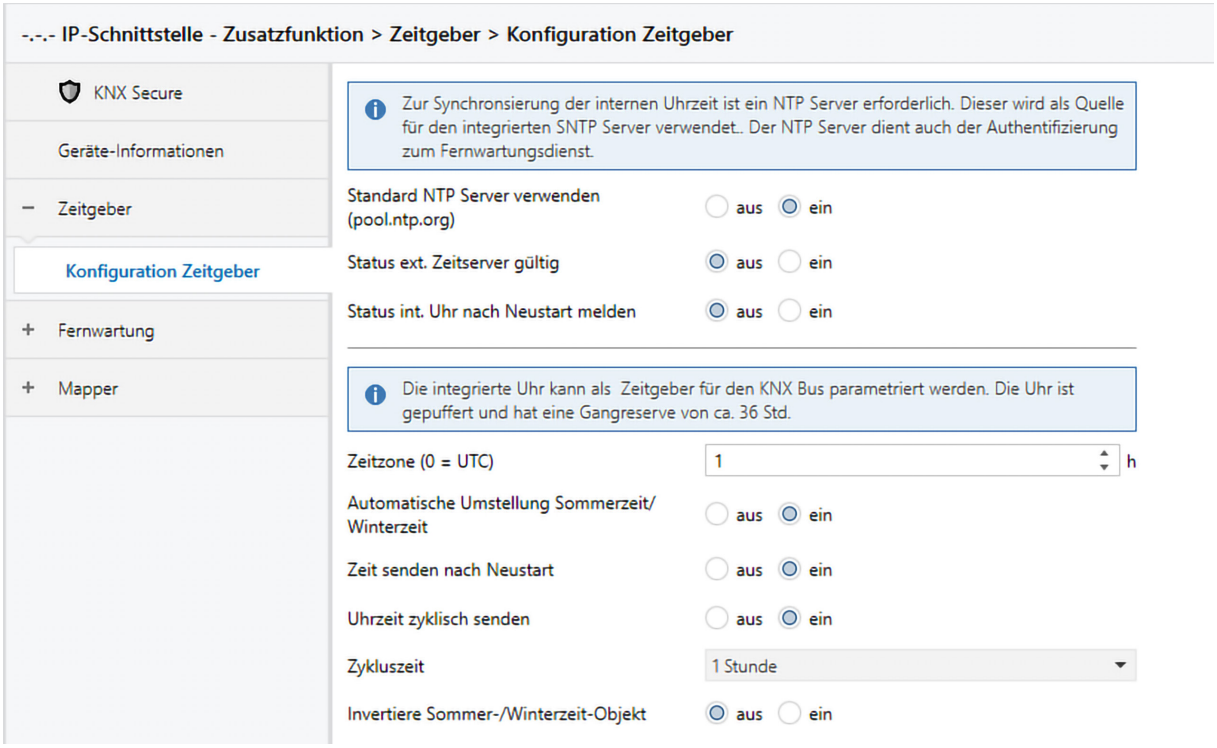


Abb. 21: Zusatzfunktionen Zeitgeber

Funktion	Auswahl	Beschreibung
Standard NTP-Server verwenden (pool.ntp.org)	aus/<u>ein</u>	Vgl. Parameterdialog Falls hier „aus“ gewählt wird, erscheint ein Eingabefeld für die IP-Adresse des eigenen externen Zeitservers
Status ext. Zeitserver gültig	<u>aus</u>/ein	Meldung über KO1

Funktion	Auswahl	Beschreibung
Status int. Uhr nach Neustart melden	aus/ein	Meldung über KO2
Zeitzone (0 = UTC)	-12 ... 1 ... +14	Stundenversatz der internen Uhr zu UTC
Automatische Umstellung Sommerzeit/Winterzeit	aus/ein	
Zeit senden nach Neustart	aus/ein	Ausgabe von Zeit und Datum auf KO3, KO4, KO5
Uhrzeit zyklisch senden	aus/ein	
Zykluszeit	24 Stunden, 12 Stunden, 3 Stunden, 1 Stunde, 30 Minuten, 15 Minuten	Zyklische Ausgabe von Zeit und Datum auf KO3, KO4, KO5

Bei Auslieferung des Geräts ist die interne Uhr ungültig, das Kommunikationsobjekt KO2 ist daher false [0].

Die interne Uhr wird gültig (Wert = wahr [1]), wenn das Gerät einen externen Zeitserver (NTP-Server) erreichen kann.

Dies erfolgt nach jedem Neustart bzw. jede Woche einmal automatisch. Hierzu muss der angegebene NTP-Server erreichbar sein.

Nach einem Neustart bzw. einer ETS-Programmierung des Geräts bleibt die Uhrzeit weiterhin gültig.

Nur im Fall, dass die Gangreserve der internen Uhr aufgrund eines mehr als 36-stündigen Stromausfalls zu stark entladen wurde, wird die Uhr wieder ungültig.

Die interne Uhr kann pro 2 Tage um ca. 1 Sekunde von der realen Zeit abweichen.

Mapper

- Übersetzung von verschlüsselte (secure) auf unverschlüsselte (plain) Kommunikationsobjekte
- Mapping von bis zu 20 Kommunikationsobjekten
- Größe jedes Kommunikationsobjekts parametrierbar zwischen 1 Bit, 2 Bit, 4 Bit , 8 Bit, 16 Bit, 24 Bit, 32 Bit, 6 Bytes, 8 Bytes und 14 Bytes

Der Mapper dient der Übersetzung von verschlüsselten (secure) auf unverschlüsselte (plain) Kommunikationsobjekte. Dazu stellt der Mapper 20 Kanäle zur Verfügung, die bidirektional die Kommunikation herstellen. Der Anwender kann die Kommunikationsobjekte so konfigurieren, dass die Gruppenadressen unterschiedliche Längen (max. 14 Byte) aufweisen.

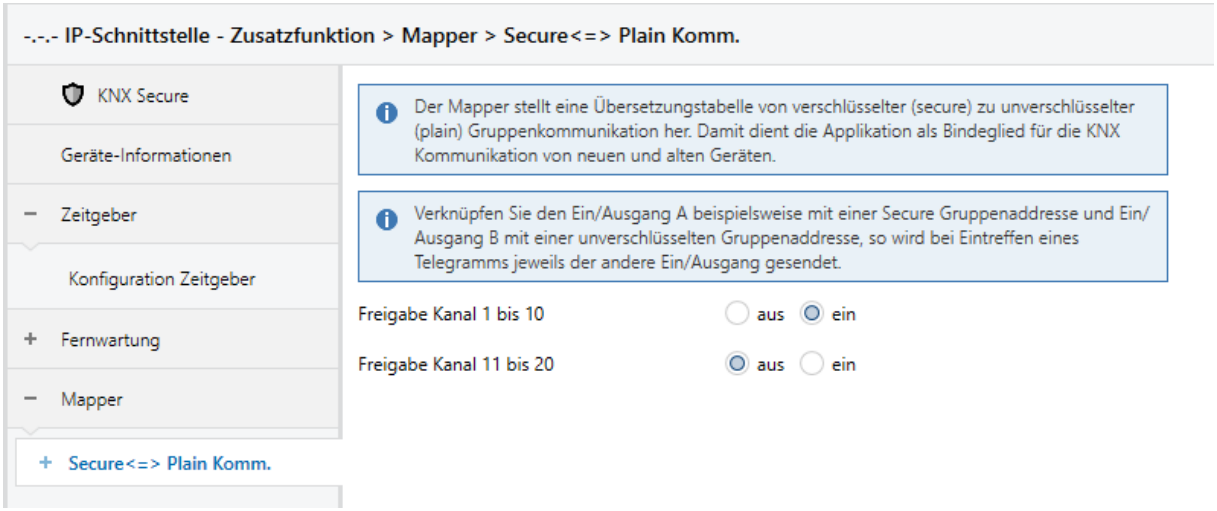


Abb. 22: Zusatzfunktionen Mapper

Funktion	Auswahl	Beschreibung
Freigabe Kanal 1 bis 10	aus/<u>ein</u>	s. u.
Freigabe Kanal 11 bis 20	<u>aus</u>/ein	s. u.

Der Mapper dient der Übersetzung von verschlüsselten (secure) auf unverschlüsselte (plain) Kommunikationsobjekte. Dazu stellt der Mapper 20 Kanäle zur Verfügung, die bidirektional die Kommunikation herstellen. Der Anwender kann die Kommunikationsobjekte so konfigurieren, dass die Gruppenadressen unterschiedliche Längen (max. 14 Byte) aufweisen. Die Länge kann parametriert werden zwischen 1 Bit, 2 Bit, 4 Bit , 8 Bit, 16 Bit, 24 Bit, 32 Bit, 6 Bytes, 8 Bytes und 14 Bytes.

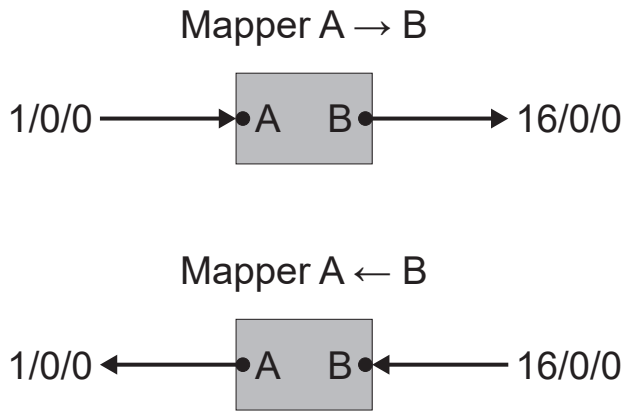


Abb. 23: Mapper Schreiben auf Gruppenadressen

Abbildung 22 zeigt die beschriebene Funktionsweise: Ein Schreiben (oder Antworten) auf 1/0/0 (Ein-/Ausgang A) löst ein Schreiben auf 16/0/0 (Ein-/Ausgang B) aus. Dabei spielt es keine Rolle ob, 1/0/0 oder 16/0/0 jeweils verschlüsselt sind oder nicht. Es kann z. B. 1/0/0 eine verschlüsselte Gruppenadresse darstellen und 16/0/0 eine unverschlüsselte. Auf diese Weise werden daher eine (oder mehrere) verschlüsselte Gruppenadressen auf eine unverschlüsselte gesendet. Das gleiche gilt sinngemäß in umgekehrter Richtung. Dabei ist im Falle von mehreren Verknüpfungen gemäß KNX-Vorgaben zu beachten, dass maximal nur eine Gruppenadresse sendend ist.

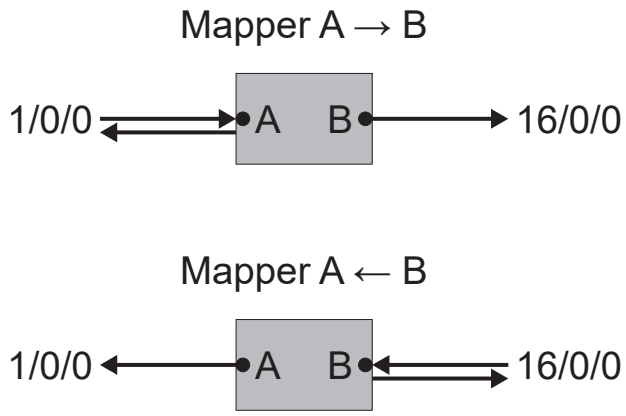


Abb. 24: Mapper Lesen auf Gruppenadressen

Abbildung 23 zeigt die beschriebene Funktionsweise für Leseanfragen: Ein Lesen auf 1/0/0 (Ein-/Ausgang A) löst ein Lesen auf 16/0/0 (Ein-/Ausgang B) aus. Wenn das Leseflag für Ein-/Ausgang A gesetzt ist, wird die Anfrage vom Ein-/Ausgang A mit einem Antworttelegramm beantwortet. Wenn danach die beteiligten Kommunikationspartner ein Antworttelegramm senden, so wird dieses behandelt wie in Abbildung 22. Dabei spielt es keine Rolle ob, 1/0/0 oder 16/0/0 jeweils verschlüsselt sind oder nicht. Es kann z. B. 1/0/0 eine verschlüsselte GA sein und 16/0/0 unverschlüsselt. Auf diese Weise kann daher eine Leseanfrage einer verschlüsselten Gruppenadresse auf eine unverschlüsselte erfolgen. Das gleiche gilt sinngemäß in umgekehrter Richtung.

Die Applikation paart der Übersichtlichkeit halber die Mapper in die Kanäle 1 bis 10 und 11 bis 20. Jeder Kanal, bestehend aus den beiden Ein-/Ausgängen A und B, ist auf die gewünschte Länge einstellbar.

i Der Mapper arbeitet nur mit Gruppenadressen, die mit einem anderen Gerät verbunden sind. Gruppenadressen, die mit den eigenen Kommunikationsobjekten, z. B. KO1 bis KO13 verknüpft sind, werden vom Mapper nicht in der beschriebenen Art und Weise behandelt.

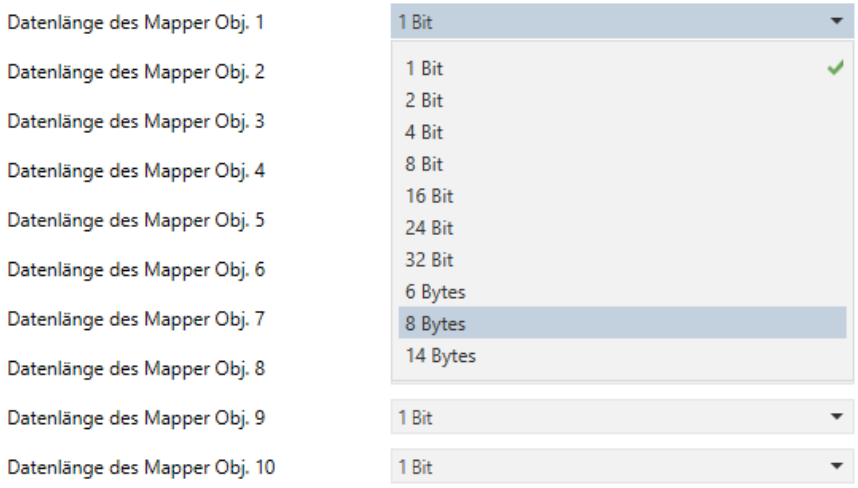


Abb. 25: Mapper Datenlänge

Kommunikationsrichtungen:

Mit Hilfe der Flags der Gruppenadressen kann das „Durchleiten“ von Gruppenadressen durch den Mapper richtungsabhängig und abhängig von der Art der Kommunikation (Lesen oder Schreiben) eingestellt werden. Dazu müssen die Kommunikationsflags wie in der Tabelle gesetzt werden.

Dort sind die Kommunikationsflags für Kanal A in der Spalte „Flags A“ und für B in Spalte „Flags B“ eingetragen. Jeweils nicht aufgeführte Flags sind nicht einzustellen. Die Pfeilrichtung gibt an, in welche Richtung die Kommunikation Lesen oder Schreiben möglich ist. A → B bedeutet, von A nach B ist die Mapper-Richtung wie in der Tabelle angegeben möglich, von B nach A erfolgt kein Mapping der Gruppenadresse.

Die Kommunikationsflags findet man in der ETS wie in Abbildung 25 angedeutet.

In der Tabelle bezeichnen die Buchstaben die gleichen Flags wie in der ETS, also z. B. K für Kommunikation, L für Lesen usw.

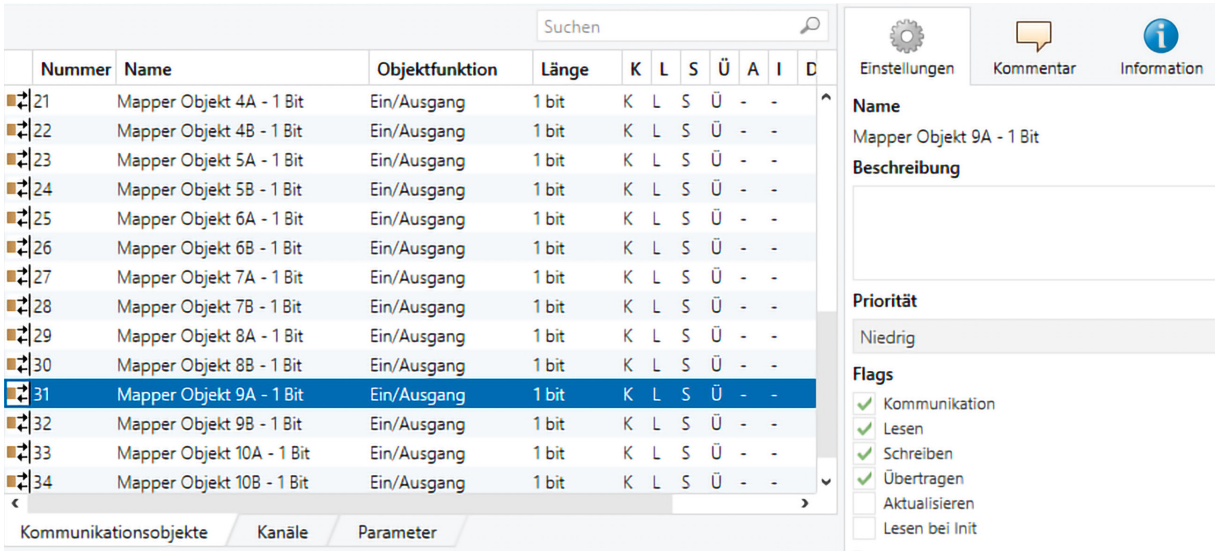


Abb. 26: Mapper Flags

Richtungen	Lesen	Schreiben	Flags A	Flags B
A ↔ B	ja	ja	KLSÜ--	KLSÜ--
A ↔ B	ja	–	KL-Ü--	KL-Ü--
A ↔ B	–	ja	K-SÜ--	K-SÜ--
A → B	ja	ja	KLS---	K-SÜ--
A → B	ja	–	KL----	K-SÜ--
A → B	–	ja	K-S---	K-SÜ--
A ← B	ja	ja	K-SÜ--	KLS---
A ← B	ja	–	K-SÜ--	KL----
A ← B	–	ja	K-SÜ--	K-S---

6.5 Kommunikationsobjekte

6.5.1 Applikationsprogramm A

ⓘ Abhängig von der Parametrierung können einige Objekte nicht verfügbar sein.

ID	Name	Objektfunktion	Länge	Typ	Flags
1	Allgemein	**Reset der Busspannung – Eingang**	1 Bit	[1.009] DPT_Trigger	K-S---
Objekt zum Auslösen eines Bus-Reset.					

6	Logik 1 - Eingang - Anwesenheitsüber-wachung	**Trigger 1 (1 Bit)**	1 Bit	[1.009] DPT_OpenClose	K-SÜ--
Eingangsobjekt für die Logik zur Anwesenheitserkennung. Kann z. B. mit einem Türkontakt oder einem Schalter verknüpft werden.					

7	Logik 1 - Eingang - Hotelcard-Schalter	**Trigger 2 (1 Bit)**	1 Bit	[1.001] DPT_Switch	K-SÜ--
Eingangsobjekt für die Logik zur Anwesenheitserkennung mit Hotelcard-Schalter.					

8	Logik 1 - Eingang - Präsenzmelder 1	**Trigger 2 (1 Bit)**	1 Bit	[1.018] DPT_Occupancy	K-SÜ--
Eingangsobjekt für die Logik zur Anwesenheitserkennung mit Präsenzmelder.					

9	Logik 1 - Eingang - Präsenzmelder 2	**Trigger 2 (1 Bit)**	1 Bit	[1.018] DPT_Occupancy	K-SÜ--
Eingangsobjekt für die Logik zur Anwesenheitserkennung mit Präsenzmelder.					

10	Logik 1 - Eingang - Präsenzmelder 3	**Trigger 2 (1 Bit)**	1 Bit	[1.018] DPT_Occupancy	K-SÜ--
Eingangsobjekt für die Logik zur Anwesenheitserkennung mit Präsenzmelder.					

11	Logik 1 - Eingang - Präsenzmelder 4	**Trigger 2 (1 Bit)**	1 Bit	[1.018] DPT_Occupancy	K-SÜ--
Eingangsobjekt für die Logik zur Anwesenheitserkennung mit Präsenzmelder.					

12	Logik 1 - Eingang - Präsenzmelder 5	**Trigger 2 (1 Bit)**	1 Bit	[1.018] DPT_Occupancy	K-SÜ--
Eingangsobjekt für die Logik zur Anwesenheitserkennung mit Präsenzmelder.					

13	Logik 2 - Eingang - Welcome/Goodbye	**Trigger 1 (1 Bit)**	1 Bit	[1.017] DPT_Trigger	K-SÜ--
Eingangsobjekt für die Logik zur Aktivierung der Welcome/Goodbye-Szene. Kann z. B. mit einem Türkontakt oder einem Schalter verknüpft werden.					

ID	Name	Objektfunktion	Länge	Typ	Flags
16	Logik 1 - Ausgang - Anwesenheitsüber-wachung	**Szenennebenstelle (1 Byte)**	1 Byte	[17.001]	K-S---
Ausgangsobjekt zum Auslösen von Szenen entsprechend der Anwesenheitserkennung von Logik 1.					

32	Logik 1 - Ausgang - Anwesenheitsüber-wachung	**Raumcontroller Betriebsmodus (1 Byte)**	1 Byte	[20.102] DPT_HVACM	K--Ü--
Ausgangsobjekt zum Umschalten des Betriebsmodus eines Raumcontrollers entsprechend der An-wesenheitserkennung von Logik 1.					

55 - 65	Logik 2 - Eingang - Welcome/Goodbye	**Schalteingang 1 – 8 (1 Bit)**	1 Bit	[1.002] DPT_Bool	K-SÜ--
Eingangsobjekt 1 - 8 für die Logik zur Aktivierung der Welcome/Goodbye-Szene. Kann z. B. mit dem Statusobjekt einer Beleuchtung verknüpft werden.					

165	Logik 2 - Ausgang - Welcome	**Schalten (1 Bit)**	1 Bit	[1.001] DPT_Switch	K--Ü--
Ausgangsobjekt zum Schalten einer Beleuchtung entsprechend der Welcome-Szene von Logik 2.					

166	Logik 2 - Ausgang - Goodbye	**Schalten (1 Bit)**	1 Bit	[1.001] DPT_Switch	K--Ü--
Ausgangsobjekt zum Schalten einer Beleuchtung entsprechend der Goodbye-Szene von Logik 2.					

194	Logik 2 - Ausgang - Welcome	**Szenennebenstelle Beleuchtung (1 Byte)**	1 Byte	[17.001] DPT_Scene-Number	K--Ü--
Ausgangsobjekt zum Auslösen einer Beleuchtungsszene entsprechend der Welcome-Szene von Logik 2.					

195	Logik 2 - Ausgang - Goodbye	**Szenennebenstelle Beleuchtung (1 Byte)**	1 Byte	[17.001] DPT_Scene-Number	K--Ü--
Ausgangsobjekt zum Auslösen einer Beleuchtungsszene entsprechend der Goodbye-Szene von Logik 2.					

214	Logik 2 - Ausgang - Welcome	**Szenennebenstelle Beschattung (1 Byte)**	1 Byte	[17.001] DPT_Scene-Number	K--Ü--
Ausgangsobjekt zum Auslösen einer Beschattung entsprechend der Welcome-Szene von Logik 2.					

215	Logik 2 - Ausgang - Goodbye	**Szenennebenstelle Beschattung (1 Byte)**	1 Byte	[17.001] DPT_Scene-Number	K--Ü--
Ausgangsobjekt zum Auslösen einer Beschattung entsprechend der Goodbye-Szene von Logik 2.					

ID	Name	Objektfunktion	Länge	Typ	Flags
234	Logik 2 - Ausgang - Welcome	**Raumcontroller Betriebsmodus (1 Byte)**	1 Byte	[20.102] DPT_HVACM	K--Ü--
Ausgangsobjekt zum Umschalten des Betriebsmodus eines Raumcontrollers entsprechend der Welcome-Szene von Logik 2.					

235	Logik 2 - Ausgang - Goodbye	**Raumcontroller Betriebsmodus (1 Byte)**	1 Byte	[20.102] DPT_HVACM	K--Ü--
Ausgangsobjekt zum Umschalten des Betriebsmodus eines Raumcontrollers entsprechend der Goodbye-Szene von Logik 2.					

6.5.2 Applikationsprogramm B

ⓘ Abhängig von der Parametrierung können einige Objekte nicht verfügbar sein.

ID	Name	Objektfunktion	Länge	Typ	Flags
1	Externer Zeitserver gültig - Ausgang	**Status**	1 Bit	[1.2] DPT_Bool	KL-Ü--
Gibt an, ob der externe Zeitserver pool.ntp.org vom Gerät erreichbar ist. Die Namensauflösung erfolgt über den DNS Server 9.9.9.9. Infos hierzu unter www.quad9.net. Wenn ein eigener NTP-Zeitserver eingestellt werden soll, muss dessen IP-Adresse bekannt sein. In diesem Fall sendet das KO nichts. Die Uhrzeit synchronisiert sich automatisch alle 2 Tage neu mit dem externen NTP-Server bzw. falls dies mit KO7 initiiert wird. Wenn der Zeitserver bei der zuletzt ausgeführten Synchronisation nicht erreichbar war, wird der Zustand über dieses KO auf den Bus ausgegeben.					

2	Interne Uhr gültig - Ausgang	**Status**	1 Bit	[1.2] DPT_Bool	KL-Ü--
Gibt an, ob die interne Uhr gültig ist. Wert wahr [1] steht für gültig, Wert falsch [0] für ungültig. Über die Parametrierung kann das Kommunikationsobjekt nach jedem Neustart automatisch gesendet werden. Bei Auslieferung des Geräts ist das Kommunikationsobjekt gleich falsch [0]. Die Uhr wird dann gültig (Wert = wahr [1]), wenn das Gerät sich über einen NTP-Server auf dessen Uhrzeit eichen kann. Nach einem Neustart bzw. einer ETS-Programmierung des Geräts bleibt der Wert weiterhin wahr [1]. Nur in dem Fall, falls der interne Pufferkondensator aufgrund eines mehrtägigen Stromausfalls zu stark entladen wurde, wird die Uhr wieder ungültig (Wert = falsch [0]).					

3	Uhrzeit - Ausgang	**Zeitausgabe**	3 Byte	[10.001] DPT_TimeOf Day	KL-Ü--
Kommunikationsobjekt zur Ausgabe der aktuellen Uhrzeit auf den Bus. Die interne Uhr ist für ca. 1,5 Tage intern (per Supercap-Kondensator) gepuffert. Die interne Uhr kann pro 2 Tage um ca. 1 Sekunde von der realen Zeit abweichen. Ein Lesetelegramm liefert stets die aktuelle Zeit.					

4	Datum - Ausgang	**Datumsausgabe**	3 Byte	[11.001] DPT_Date	KL-Ü--
Kommunikationsobjekt zur Ausgabe des Kalenders der internen Uhr.					

ID	Name	Objektfunktion	Länge	Typ	Flags
5	Uhrzeit und Datum - Ausgang	**Zeit- und Datumsausgabe**	8 Byte	[19.001] DPT_Date-Time	KL-Ü--
Uhrzeit und Datum zur Ausgabe der aktuellen Uhrzeit und Datums auf den Bus.					

6	Datum/Uhrzeit - Eingang	**Anfordern**	1 Bit	[1.017] DPT_Trigger	K-SÜ--
Trigger zum Schreiben von KO3, KO4 und KO5. Es triggert sowohl ein Schreiben mit 0 als auch 1.					

7	NTP Server Synch. - Eingang	**Anfordern**	1 Bit	[1.017] DPT_Trigger	K-SÜ--
Die interne Uhr synchronisiert sich automatisch alle 2 Tage neu mit den externen NTP-Server bzw. falls dieses KO geschrieben wird. Es triggert sowohl ein Schreiben mit 0 als auch 1.					

8	Sommer- / Winterzeit - Ausgang	**Status**	1 Bit	[1.xxx]	KL-Ü--
Wenn Sommerzeit aktiv ist, wird dieses KO 0, während der Winterzeit 1. Dieses KO ist daher für die Winterumschaltung von Heizungen direkt nutzbar.					

9	Fernwartung aktivieren - Eingang	**Schalten**	1 Bit	[1.002] DPT_Switch	KLSÜ--
Einschalten der Fernwartung (1) bzw. stoppen der Fernwartung (0): Wenn der Anwender über dieses KO den Fernwartungszugang öffnet, wird sicheres Tunnelling während dieser Zeit aktiviert. Die Schnittstelle verbindet sich dann zum Relaisserver. Eine Entschlüsselung in der Cloud erfolgt nicht. Der kundenseitige Anschluss kann dabei vom Typ IPv4 oder IPv6 sein.					

10	Freischaltcode gültig - Ausgang	**Status**	1 Bit	[1.2] DPT_Bool	KL-Ü--
Zeigt wahr [1], wenn das Gerät mindestens einmal mit einem gültigen Freischaltcode geladen wurde und die Fernwartung grundsätzlich möglich ist. Ansonsten ist der Wert falsch [0].					

11	Abgesicherter Modus aktiv - Ausgang	**Status**	1 Bit	[1.2] DPT_Bool	KL-Ü--
Zeigt wahr [1], wenn die Schnittstelle sicher in Betrieb genommen und das sichere (=verschlüsselte) Tunnelling in der Schnittstellenapplikation aktiviert wurde. Ansonsten ist der Wert falsch [0].					

12	Serververbindung - Ausgang	**Status**	1 Bit	[1.2] DPT_Bool	KL-Ü--
Wenn die Verbindung zum Relaisserver steht, so wird dieses KO wahr [1], sonst falsch [0].					

13	Secure Tunnelling aktiv - Ausgang	**Status**	1 Byte	[5.1] DPT_Scaling	KL-Ü--
Status des Secure Tunnellings: falsch [0] = inaktiv, wahr [1] = aktiv. Inaktiv bedeutet, dass unverschlüsselte Tunnelverbindungen aufgebaut werden können.					

ID	Name	Objektfunktion	Länge	Typ	Flags
14	Programmierung der Fernwartung aktiv - Ausgang	**Status**	1 Bit	[1.2] DPT_Bool	K--Ü--
Wenn eine Fernwartung vom Rechner des Installateurs (ETS) zur Schnittstelle aufgebaut wird, ist dies wahr [1], sonst falsch [0]. Da generell eine Verbindung zum Gerät erst nach ca. 10 Sekunden komplett geschlossen wird, wird in der Regel ein zeitlicher Versatz zwischen der Ausgabe des KOs und beispielsweise der Anzeige im Gruppenmonitor beobachtbar.					

15	MapperObjekt Kanal A - Feldlänge	**Ein/Ausgang**	1 Bit bis 14 Byte	n.a.	KLSÜ--
Bei Schreiben oder Antworten auf dieses KO wird der Wert auf das KO des Kanal B auf den Bus geschrieben. Dabei wird die Verschlüsselung der einzelnen Kanäle berücksichtigt. Bei einer Leseanforderung wird diese beantwortet und gleichzeitig eine Leseanforderung auf Kanal B ausgegeben.					

16	MapperObjekt Kanal B - Feldlänge	**Ein/Ausgang**	1 Bit bis 14 Byte	n.a.	KLSÜ--
Bei Schreiben oder Antworten auf dieses KO wird der Wert auf das KO des Kanal A auf den Bus geschrieben. Dabei wird die Verschlüsselung der einzelnen Kanäle berücksichtigt. Bei einer Leseanforderung wird diese beantwortet und gleichzeitig eine Leseanforderung auf Kanal B ausgegeben.					

7 Erweiterte Konfiguration

7.1 Konfigurationstool

Die Software vereinfacht die Konfiguration des Geräts und stellt detaillierte Informationen zur Fehleranalyse zur Verfügung.

Wenn das Gerät im Secure-Modus betrieben wird, kann das Konfigurationstool keine Verbindung zum Gerät herstellen.

7.1.1 Geräteverbindung

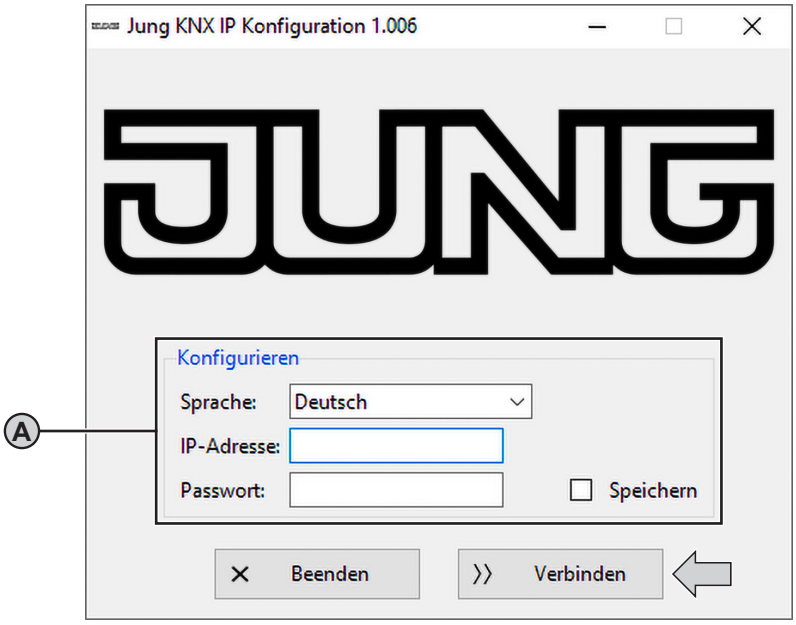


Abb. 27: Geräteverbindung

Voraussetzungen:

- Gerät angeschlossen und gebootet
- Konfigurationstool gestartet

Konfigurieren (A)

Sprache ändern:

- Sprache auswählen.
  Konfigurationstool wird in der ausgewählten Sprache angezeigt.

Gerät verbinden zur Gerätekonfiguration:

- IP-Adresse des Geräts eingeben.
  Die IP-Adresse kann wie folgt ermittelt werden:
  Feste IP-Adresse: siehe ETS
  Dynamische IP-Adresse: siehe DHCP-Server
- Passwort eingeben.
  Das voreingestellte Passwort ist „knxsecure“.
  Das eingegebene Passwort kann gespeichert werden, damit es nach dem nächsten Start des Konfigurationstools nicht erneut eingegeben werden muss.
- „Verbinden“ auswählen.
  Gerät wird verbunden.
  Gerätekonfiguration wird angezeigt.

7.1.2 Gerätekonfiguration

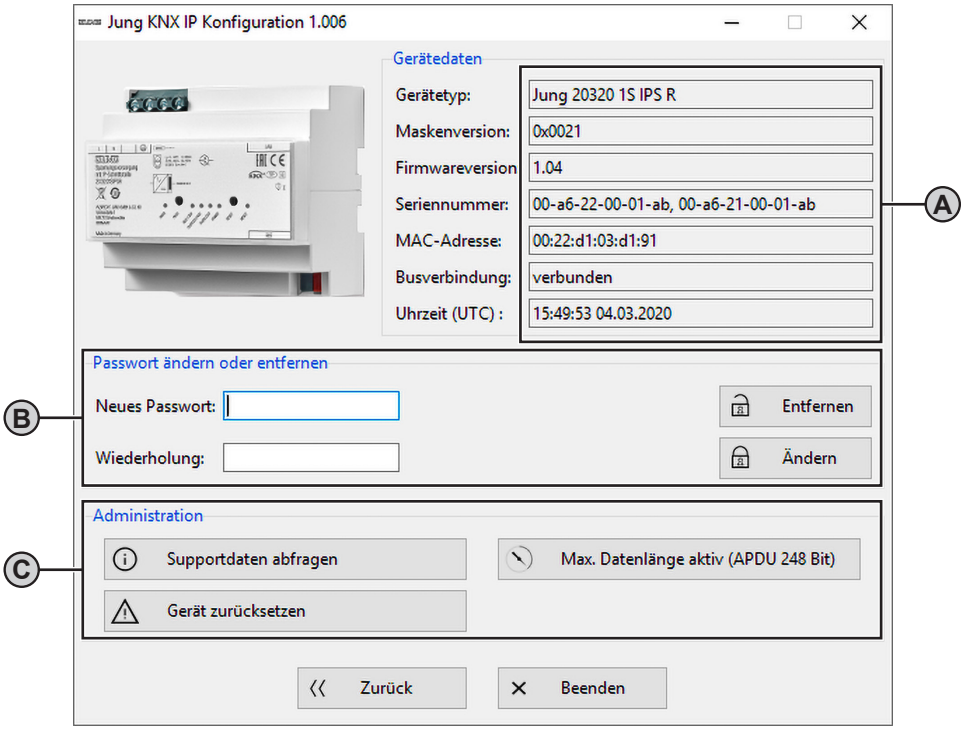


Abb. 28: Gerätekonfiguration

Voraussetzung:

- Geräteverbindung hergestellt

Gerätedaten (A)

Zeigt aktuelle Eigenschaften des Geräts an.

Passwort ändern oder entfernen (B)

Passwort ändern:

- Neues Passwort eingeben und Eingabe wiederholen.
- Neues Passwort mit „Ändern“ bestätigen.
  Passwort ist geändert.

Passwort entfernen:

- „Entfernen“ auswählen.
  Passwort wird entfernt.

Administration (C)

Geräteinformationen abspeichern zur Fehlerbehebung:

- „Supportdaten abfragen“ auswählen.
  Eine Textdatei mit Geräteinformationen wird im Hauptverzeichnis der Software abgespeichert.
  Beispielpfad: C:\Programme\KonfigTool\

Master-Reset durchführen zur Wiederherstellung von Werkseinstellungen:

- „Gerät zurücksetzen“ auswählen.
  Master-Reset wird durchgeführt.
  Konfigurationstool wird neugestartet.

Min. / max. Länge der Telegramme auswählen zur Fehlerbehebung durch Drittanbieterprodukte:

- „Maximale Datenrate aktiv (APDU 248 Bit)“ bzw. „Minimale Datenrate aktiv (APDU 55 Bit)“ auswählen.
  Telegrammlänge wird angepasst.

7.2 Telnet-Interface

Telnet ist ein weit verbreitetes Netzwerkprotokoll auf Basis einer TCP-Verbindung zwischen einem Telnet-Server und einem Client.

Voraussetzung für die Kommunikation ist, dass das Gerät im Netzwerk administriert ist und vom Inbetriebnahme-PC über IP erreicht wird. Über Telnet können dann Einstellungen vorgenommen, sowie Statusinformationen eingesehen werden, ohne dass eine Verbindung zur ETS besteht.

Telnet kann entweder als Funktion des Betriebssystems Windows aktiviert werden oder über ein Drittprogramm, wie z. B. PuTTY, genutzt werden.

Der Telnet-Zugang ist ab Werk mit dem Passwort „knxsecure“ geschützt.

Sobald das Gerät im Secure-Modus betrieben wird, ist das Telnet-Interface deaktiviert.

Telnet-Eingabe	Beschreibung
`help`	Zeigt alle verfügbaren Kommandos an

`ifconfig`	Zeigt Netzwerkparameter an
	
	`IP mode.......: DHCP`
	`IP............: 192.168.33.142`
	`Subnet mask...: 255.255.0.0`
	`Gateway.......: 192.168.33.1`
	`NTP server....: 192.53.103.108`
	`Hardware addr.: 00:50:c2:79:3f:ff`

`ifconfig [help|dhcp|ip |mask]`	Netzwerkparameter über das Telnet-Interface einstellen.
	Beispiele:
	
	Die IP-Adresse per DHCP vergeben:
	`ifconfig dhcp`
	Die IP-Adresse statisch auf 192.168.1.2 setzen (in diesem Fall sollte auch Gate-way und Maske angepasst werden, s. u.)
	`ifconfig ip 192.168.1.2`
	Das Gateway auf 192.168.1.1 setzen:
	`ifconfig gw 192.168.1.1`
	Die Maske auf 255.255.255.0 setzen:
	`ifconfig mask 255.255.255.0`

`tpconfig`	Zeigt KNX-Parameter an
	
	`KNX bus state.: up`
	`KNX address...: 15.15.000`
	`Serial number.: 00-a6-00-00-00-01`

`tpconfig [help|set]`	KNX-Parameter über das Telnet-Interface einstellen. Die TP-Adresse auf 1.1.0 setzen: `tpconfig set 1.1.0`
`progmode [0|1]`	Programmiermodus abfragen oder ändern (0 = aus, 1 = ein)

`apdu [55..248]`	Die maximale Länge der KNX-TP-Telegramme lesen oder konfigurieren. Dies kann notwendig werden, wenn eine fehlerhafte Implementierung eines TP-Stacks vorliegt, sodass die ETS eine Programmierung mit Telegrammen mit 248 Nutzbytes vornimmt, die das TP-Gerät aber nicht verarbeiten kann (z. B. Zennio Z35i). Default ist 248 und sollte nur bei Bedarf verändert werden.
	
	`# apdu`
	`maximal len of a KNX telegram 248.`
	`Usage: apdu [55 .. 248]`

`tpratemax [5..50]`	Maximale Telegrammrate (IP => TP) lesen oder konfigurieren; 50 T/s entsprechen 100 % Buslast.
	
	`# tpratemax`
	`no limit, sending with maximum performance to TP.`
	`Usage: tpratemax [5 .. 50]`

Telnet-Eingabe	Beschreibung
stats	Zeigt diverse Statistiken zu Geräte- und Busstatus **uptime: 114 days, 2:19** **KNX communication statistics:** **TX to IP (all)..: 333729 (ca. 233 t/m)** **TX to KNX.....: 23244 (ca. 16 t/m)** **RX from KNX.....: 94559 (ca. 66 t/m)** **Overflow to IP..: 0** **Overflow to KNX.: 0** **TX tunnel re-req: 260** **TP bus voltage..: 28.95 V** **TX TP rate.....: 50 T/s (= 100 %)** Uptime: Laufzeit der Schnittstelle seit letztem Neustart TX to IP (all): Anzahl aller auf IP verschickten Telegramme TX to KNX: Anzahl der auf den KNX-Bus geschickten Telegramme RX from KNX: Anzahl der vom KNX-Bus empfangenen Telegramme Overflow to IP: Anzahl der Telegramme, die nicht auf IP geschickt werden konnten Overflow to KNX: Anzahl der Telegramme, die nicht auf den KNX-Bus geschickt werden konnten TX tunnel re-req: Anzahl der Telegramme, die in den Tunnelverbindungen wiederholt werden mussten TP bus voltage: Aktuelle Busspannung (zum Zeitpunkt des Aufruf von stats) TX TP rate: maximale Telegrammrate (TP)
free [clear]	Zeigt Statistiken über die Speicherauslastung **Used stack memory...: 14 %** **Allocated memory....: 64 %** **Unused memory.....: 35 %** **TP-Tx buffer.....: 0 %** **TP-Tx buffer max....: 0 %** **TP-Rx buffer max....: 0 %** **Tunnel-T8 buffer max: 92 %** Used stack memory: Funktionsstapelauslastung Allocated memory: Allokierter Gerätespeicher Unused memory: Nicht genutzter Gerätespeicher TP-Tx buffer: Derzeit genutzter TP-Sendepuffer TP-Tx buffer max: Max. Auslastung TP-Sendepuffer (IP => TP) seit Systemstart TP-Rx buffer max: Max. Auslastung TP-Empfangspuffer (IP <= TP) seit Systemstart Tunnel-XX (XX = 1..8) buffer max: Max. Auslastung des Tunneling Buffers. Es werden nur Tunnel angezeigt, deren Puffer überhaupt benutzt wurde. Löschen der Pufferstatistik: **free clear**

Telnet-Eingabe	Beschreibung
tunnel [1..8]	Zeigt aktive Tunnelverbindungen (ohne Argument), bzw. detaillierte Informationen zur angegebenen Tunnelverbindung an (mit Argument 1..8) **# tunnel** **Tunnels open: 1/8** **1: 00.02.246, closed** **2: 00.02.247, open (CCID: 82)** **3: 00.02.248, closed** **4: 00.02.249, closed** **5: 00.02.250, closed** **6: 00.02.251, closed** **7: 00.02.252, closed** **8: 00.02.253, closed** **# tunnel 2** **Tunnel 2.....: open (CCID 82)** **KNX address.....: 00.02.247** **HPAI control.....: 192.168.22.252:4808** **HPAI data.....: 192.168.22.252:4808** **Connect. type.....: TUNNEL_CONNECTION** **Communication.....: UDP CONNECTION** **TX tun req.....: 23169** **TX tun re-req.....: 0** **RX tun req.....: 821** **RX tun re-req (identified): 0** **RX tun req (wrong seq.)...: 0** **Current tunnel buffer.....: 0 %** **Connected since (UTC).....: 16:26:16 29-01-2019** CCID: Verbindungs-ID der Tunnelverbindung KNX address: Tunneladresse HPAI control: Kontrollendpunkt des Verbindungspartners HPAI data: Datenendpunkt des Verbindungspartners Connect. Type: Verbindungstyp Tunnel oder Management-Verbindung Communication: UDP- oder TCP-Verbindung TX tun req: Anzahl der Telegramme, die in die Tunnelverbindungen geschickt wurden TX tun re-req: Anzahl der Telegramme, die in den Tunnelverbindungen wiederholt werden mussten RX tun req: Anzahl der Telegramme, die von der Tunnelverbindungen empfangen wurden RX tun re-req: Anzahl der Telegramme, die von der Tunnelverbindungen doppelt empfangen wurden RX tun req (wrong seq.): Anzahl der Telegramme, die von der Tunnelverbindun-gen mit falscher Sequenznummer empfangen wurden Current tunnel buffer: Auslastung aktuell des IP-Puffers des Tunnels Connected since (UTC): Uhrzeit, seitdem die Tunnelverbindung besteht
version	Firmware-Version abfragen
mask	Masken-Version abfragen
tunaddr 1..8 address **tunaddr reset** **tunaddr setall** **tunaddr help**	KNX-Adresse eines Tunnels lesen (**tunaddr**) oder ändern, z. B. **tunaddr 1 15.15.240**, alle Tunneladressen fortlaufend ab einer bestimmten Startadresse vergeben (**tunaddr setall 15.15.15**), oder die KNX-Adressen aller Tunnel auf Werkseinstellung zurücksetzen (**tunaddr reset**) **# tunaddr** **1: KNX address: 15.15.010** **2: KNX address: 15.15.011** **3: KNX address: 15.15.012** **4: KNX address: 15.15.013** **5: KNX address: 15.15.014** **6: KNX address: 15.15.015** **7: KNX address: 15.15.016** **8: KNX address: 15.15.017**
tunmode [std/tpblk]	Tunnelmodus lesen (ohne Parameter) oder setzen (**tp** bzw. **tpblk**); **tunmode tpblock**: IP => KNX bei gleicher Backbone Line Frame an TP weiterleiten KNX => IP bei gleicher Sub Line Frame an TP weiterleiten

Telnet-Eingabe	Beschreibung
Tunneltime [1.0..8.0]	Timeout für Tunnelverbindung abfragen oder ändern (1.0 bis 8.0). Einstellung ist identisch zu „Langsame Verbindung“, Abbildung 11
tunudp	Typ der Tunnelverbindung für die ETS abfragen oder ändern (0 = Standard, 1 = Nur UDP).
date	Datum und Uhrzeit anzeigen
busload	Zeigt die Buslast der letzten Minute / letzten 5 Minuten / letzten 15 Minuten / seit Start an sowie die höchste Busbelastung mit Datum und Uhrzeit
sntp [query|server IP]	Anfrage an den NTP-Server schicken (**sntp query**) oder IP des NTP-Servers einstellen (**sntp server 1.2.3.4**)
logmem	Ereignisspeicher im Gerät. Geeignet für die Entwicklung von Clients. Bei Supportanfragen auslesen.
passwd oldpw newpw **passwd oldpw** **passwd newpw**	Ändert das aktuelle Telnet-Passwort (passwd alt neu), löscht das aktuelle Passwort (passwd alt) oder setzt ein neues Passwort, falls momentan keines gesetzt ist (passwd neu).
factory_reset	Auf Werkseinstellungen zurücksetzen und neustarten
reboot	Neustart
logout	Telnet-Session beenden

8 Anwendungsfälle

8.1 Applikationsprogramm A – Logikfunktionen

Je Gerät kann die integrierte Logik zur Anwesenheitsüberwachung konfiguriert werden. Die Anwesenheitsüberwachung ist wahlweise mithilfe eines Hotelcardschalters oder mit bis zu fünf Präsenzmeldern auswählbar.

8.1.1 Anwesenheitsüberwachung mit Hotelcardschalter

Mittels Hotelcard-Schalter und einem Türkontakt kann eine vordefinierte Logik der Anwesenheitsüberwachung parametriert werden. Die nachfolgende Abbildung zeigt die die Wirkweise und die Möglichkeiten zu Individualisierung. Nachfolgend sind Beispiele zur Parametrierung aufgezeigt.

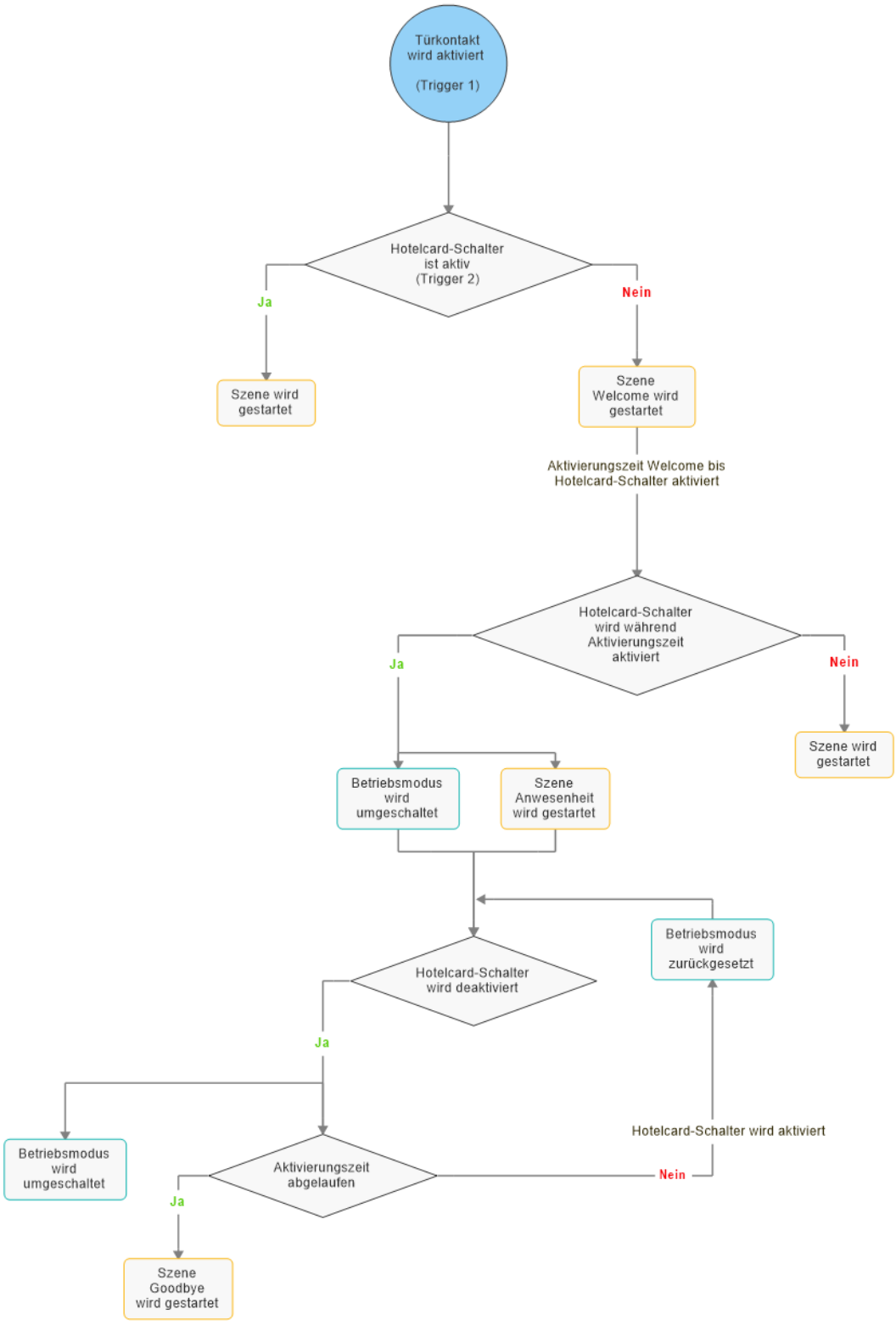


Abb. 29: Anwesenheitsüberwachung mit Hotelcardschalter

Anwesenheitsüberwachung mit Hotelcardschalter – Easy

Die aufzeigte Paramatrierung stellt eine einfache Anwendung der Präsenzerkennung dar.

- Eine Person betritt den Raum (Türkontakt wird aktiviert)
  - Eine Willkommensszene wird ausgelöst
    Hier kann beispielsweise die Beleuchtung gedimmt eingeschaltet werden
- Eine Person steckt die Zugangskarte innerhalb der Aktivierungszeit in den Hotelcard-Schalter
  - Ein Betriebsmodus wird gesendet
    Hier kann beispielsweise der Betriebsmodus „Komfort“ aktiviert werden
- Eine Person steckt die Zugangskarte innerhalb der Aktivierungszeit nicht
  - Eine Szene wird ausgelöst
    Hier kann beispielsweise die Beleuchtung ausgeschaltet werden
- Eine Person zieht die Zugangskarte heraus verlässt den Raum
  - Ein Betriebsmodus wird gesendet
    Hier kann beispielsweise der Betriebsmodus „Standby“ aktiviert werden
  - Nach der Aktivierungszeit wird eine Goodbye Szene ausgelöst
    Hier kann beispielsweise die Beleuchtung ausgeschaltet werden

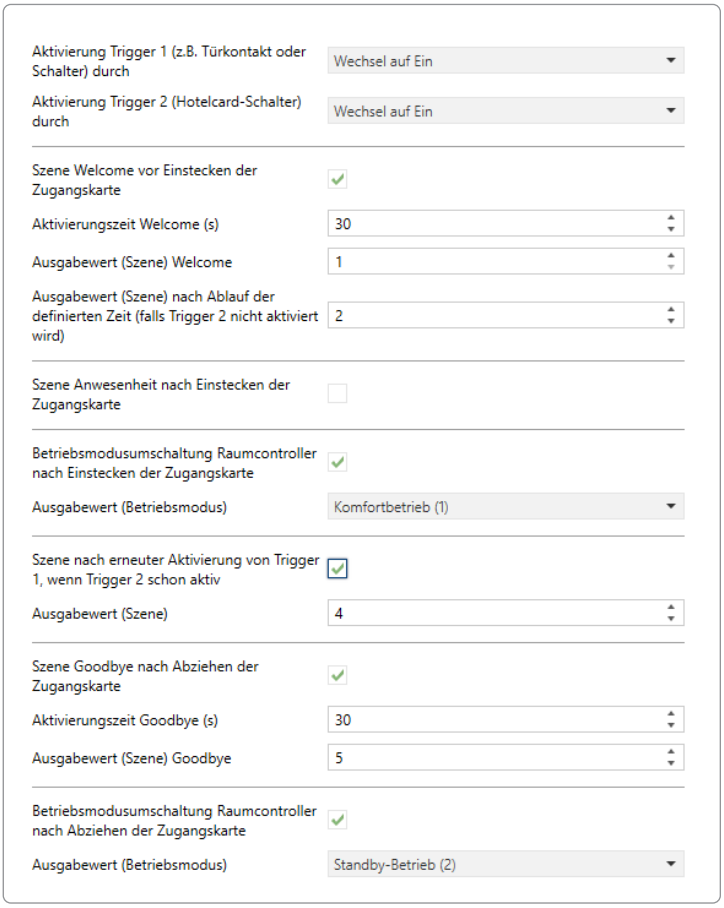


Abb. 30: Anwesenheitsüberwachung mit Hotelcardschalter – Easy

Anwesenheitsüberwachung mit Hotelcardschalter – Standard

Die aufzeigte Paramatrierung stellt eine Standard Anwendung der Präsenzerkennung dar.

- Eine Person betritt den Raum (Türkontakt wird aktiviert)
  - Eine Willkommensszene wird ausgelöst
    Hier kann beispielsweise die Beleuchtung gedimmt eingeschaltet werden
- Eine Person steckt die Zugangskarte innerhalb der Aktivierungszeit in den Hotelcard-Schalter
  - Ein Betriebsmodus und eine Anwesenheitsszene wird gesendet
    Hier kann beispielsweise der Betriebsmodus „Komfort“ aktiviert, die Jalousie in die obere Endlage gefahren und eine zusätzliche Beleuchtung gedimmt eingeschaltet werden
- Eine Person steckt die Zugangskarte innerhalb der Aktivierungszeit nicht
  - Eine Szene wird ausgelöst
    Hier kann beispielsweise die Beleuchtung ausgeschaltet werden
- Eine Person zieht die Zugangskarte heraus verlässt den Raum
  - Ein Betriebsmodus wird gesendet
    Hier kann beispielsweise der Betriebsmodus „Standby“ aktiviert werden
  - Nach der Aktivierungszeit wird eine Goodbye Szene ausgelöst
    Hier kann beispielsweise die Beleuchtung ausgeschaltet werden

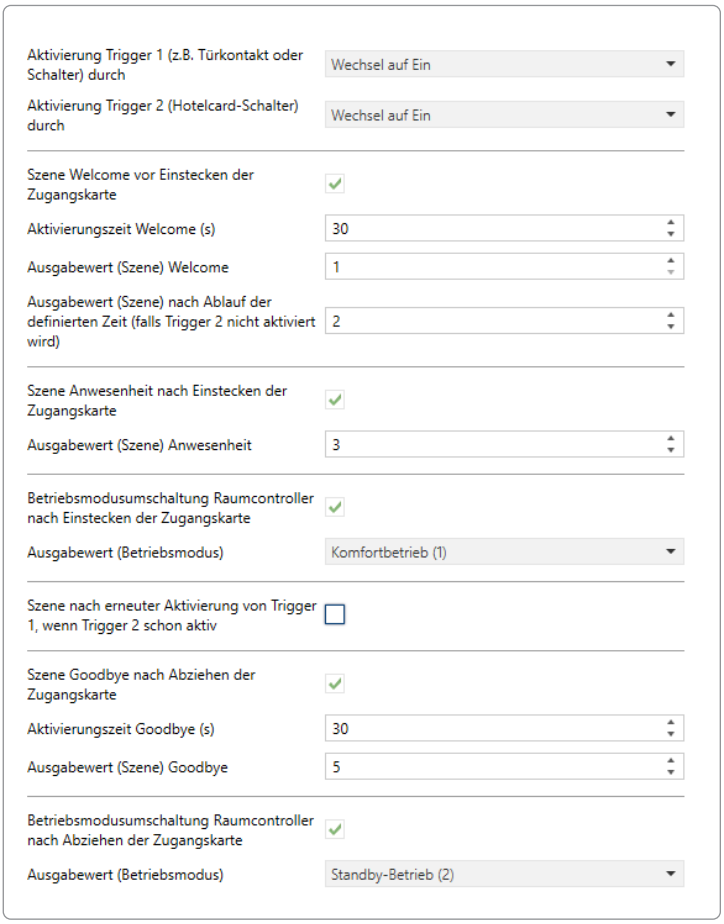


Abb. 31: Anwesenheitsüberwachung mit Hotelcardschalter – Standard

Anwesenheitsüberwachung mit Hotelcardschalter – Luxury

Die aufzeigte Paramatrierung stellt eine umfassende Anwendung der Präsenzerkennung dar.

- Eine Person betritt erstmalig (First Entry) den Raum (Türkontakt wird aktiviert)
  - Eine Willkommensszene wird ausgelöst
    Hier kann beispielsweise die Beleuchtung gedimmt eingeschaltet werden
- Eine Person steckt die Zugangskarte innerhalb der Aktivierungszeit in den Hotelcard-Schalter
  - Ein Betriebsmodus und eine Anwesenheitsszene wird gesendet
    Hier kann beispielsweise der Betriebsmodus „Komfort“ aktiviert, die Jalousie in die obere Endlage gefahren und eine zusätzliche Beleuchtung gedimmt werden
- Eine Person steckt die Zugangskarte innerhalb der Aktivierungszeit nicht
  - Eine Szene wird ausgelöst
    Hier kann beispielsweise die Beleuchtung ausgeschaltet werden
- Eine weitere Person betritt den Raum (Türkontakt wird aktiviert)
  - Eine Nighlightszene wird ausgelöst
    Hier kann beispielsweise die Eingangsbeleuchtung auf Minimalhelligkeit gedimmt werden
- Eine Person zieht die Zugangskarte heraus verlässt den Raum
  - Ein Betriebsmodus wird gesendet
    Hier kann beispielsweise der Betriebsmodus „Standby“ aktiviert werden
  - Nach der Aktivierungszeit wird eine Goodbye Szene ausgelöst
    Hier kann beispielsweise die Beleuchtung ausgeschaltet werden

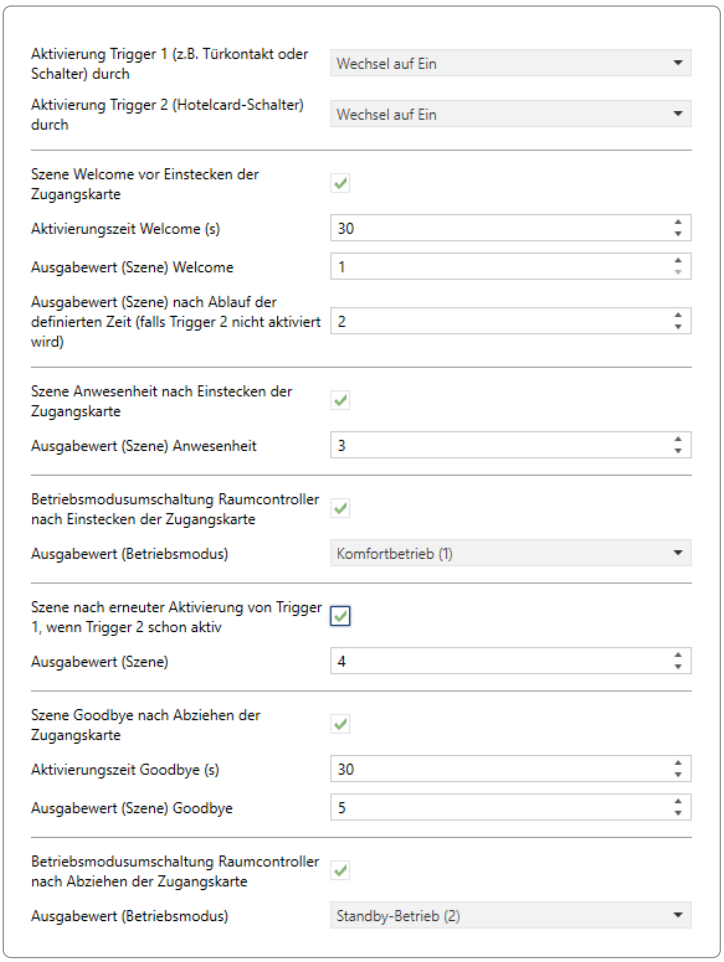


Abb. 32: Anwesenheitsüberwachung mit Hotelcardschalter – Luxury

8.1.2 Anwesenheitsüberwachung mit Präsenzmelder

Mit bis zu 5 Präsenzmeldern und einem Türkontakt kann eine vordefinierte Logik der Anwesenheitsüberwachung parametriert werden. Die nachfolgende Abbildung zeigt die die Wirkweise und die Möglichkeiten zu Individualisierung. Nachfolgend sind Beispiele zur Parametrierung aufgezeigt.

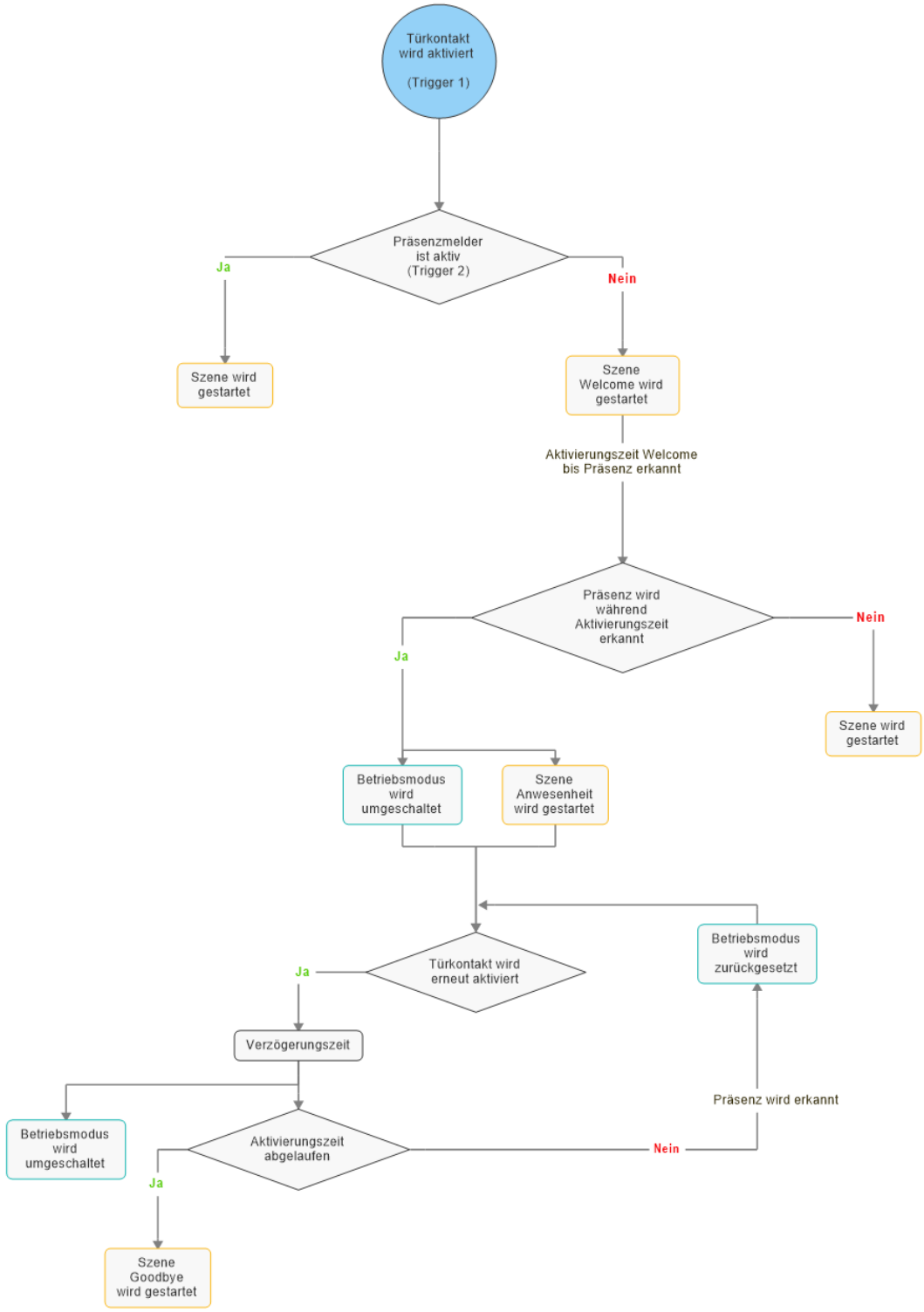


Abb. 33: Anwesenheitsüberwachung mit Präsenzmelder

Anwesenheitsüberwachung mit Präsenzmelder – Easy

Die aufzeigte Paramatrierung stellt eine einfache Anwendung der Präsenzerkennung dar.

- Eine Person betritt den Raum (Türkontakt wird aktiviert)
  - Eine Willkommensszene wird ausgelöst
    Hier kann beispielsweise die Beleuchtung gedimmt eingeschaltet werden
- Ein Präsenzmelder erkennt innerhalb der Aktivierungszeit Präsenz
  - Ein Betriebsmodus wird gesendet
    Hier kann beispielsweise der Betriebsmodus „Komfort“ aktiviert werden
- Ein Präsenzmelder erkennt innerhalb der Aktivierungszeit keine Präsenz
  - Eine Szene wird ausgelöst
    Hier kann beispielsweise die Beleuchtung ausgeschaltet werden
- Eine Person verlässt den Raum und es wird nach einer Verzögerungzeit keine Präsenz erkannt
  - Ein Betriebsmodus wird gesendet
    Hier kann beispielsweise der Betriebsmodus „Standby“ aktiviert werden
  - Nach der Aktivierungszeit wird eine Goodbye Szene ausgelöst
    Hier kann beispielsweise die Beleuchtung ausgeschaltet werden

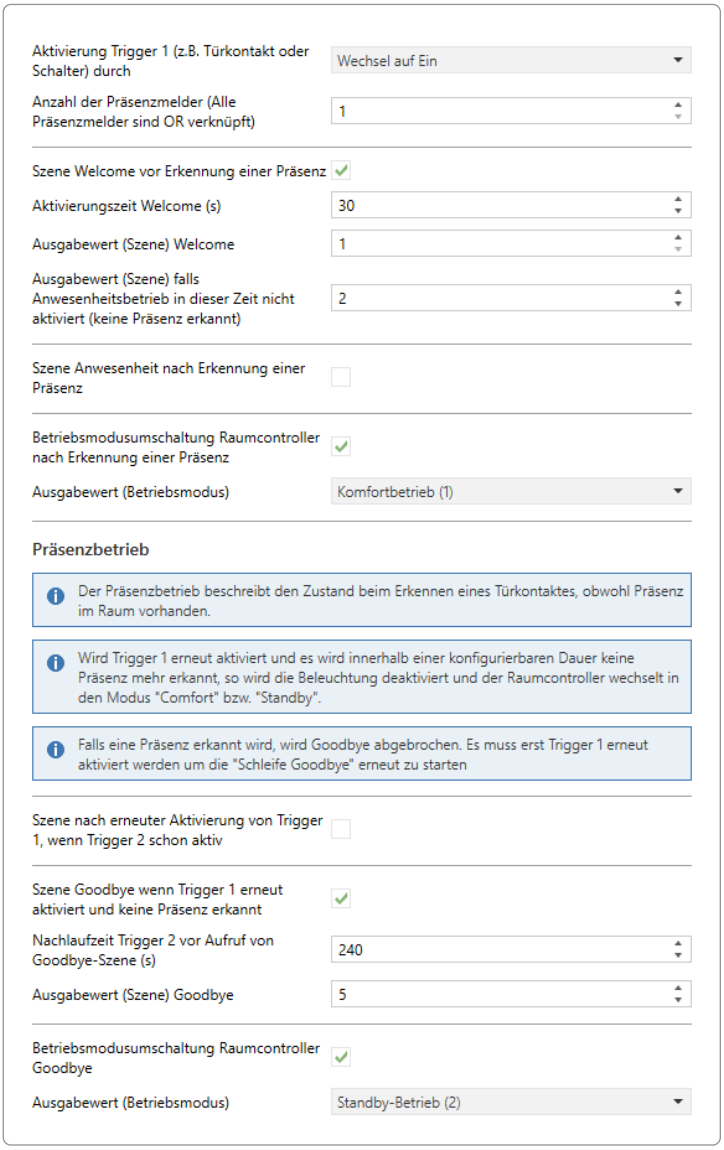


Abb. 34: Anwesenheitsüberwachung mit Präsenzmelder – Easy

Anwesenheitsüberwachung mit Präsenzmelder – Standard

Die aufzeigte Paramatrierung stellt eine Standard Anwendung der Präsenzerkennung dar.

- Eine Person betritt den Raum (Türkontakt wird aktiviert)
  - Eine Willkommensszene wird ausgelöst
    Hier kann beispielsweise die Beleuchtung gedimmt eingeschaltet werden
- Ein Präsenzmelder erkennt innerhalb der Aktivierungszeit Präsenz
  - Ein Betriebsmodus und eine Anwesenheitsszene wird gesendet
    Hier kann beispielsweise der Betriebsmodus „Komfort“ aktiviert, die Jalousie in die obere Endlage gefahren und eine zusätzliche Beleuchtung gedimmt eingeschaltet werden
- Ein Präsenzmelder erkennt innerhalb der Aktivierungszeit keine Präsenz
  - Eine Szene wird ausgelöst
    Hier kann beispielsweise die Beleuchtung ausgeschaltet werden
- Eine Person verlässt den Raum und es wird nach einer Verzögerungzeit keine Präsenz erkannt
  - Ein Betriebsmodus wird gesendet
    Hier kann beispielsweise der Betriebsmodus „Standby“ aktiviert werden
  - Nach der Aktivierungszeit wird eine Goodbye Szene ausgelöst
    Hier kann beispielsweise die Beleuchtung ausgeschaltet werden

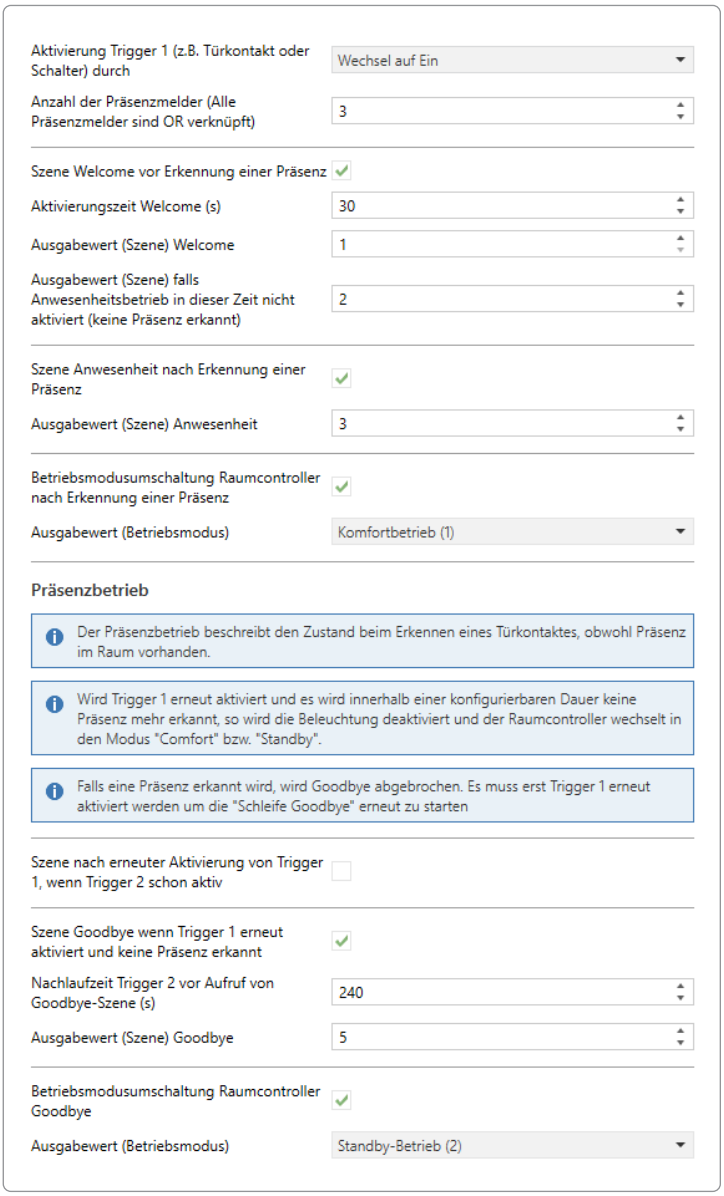


Abb. 35: Anwesenheitsüberwachung mit Präsenzmelder – Standard

Anwesenheitsüberwachung mit Präsenzmelder – Luxury

Die aufzeigte Paramatrierung stellt eine umfassende Anwendung der Präsenzerkennung dar.

- Eine Person betritt erstmalig (First Entry) den Raum (Türkontakt wird aktiviert)
  - Eine Willkommensszene wird ausgelöst
    Hier kann beispielsweise die Beleuchtung gedimmt eingeschaltet werden
- Ein Präsenzmelder erkennt innerhalb der Aktivierungszeit Präsenz
  - Ein Betriebsmodus und eine Anwesenheitsszene wird gesendet
    Hier kann beispielsweise der Betriebsmodus „Komfort“ aktiviert, die Jalousie in die obere Endlage gefahren und eine zusätzliche Beleuchtung gedimmt werden
- Ein Präsenzmelder erkennt innerhalb der Aktivierungszeit keine Präsenz
  - Eine Szene wird ausgelöst
    Hier kann beispielsweise die Beleuchtung ausgeschaltet werden
- Eine weitere Person betritt den Raum (Türkontakt wird aktiviert)
  - Eine Nighlightszene wird ausgelöst
    Hier kann beispielsweise die Eingangsbeleuchtung auf Minimalhelligkeit gedimmt werden
- Eine Person verlässt den Raum und es wird nach einer Verzögerungzeit keine Präsenz erkannt
  - Ein Betriebsmodus wird gesendet
    Hier kann beispielsweise der Betriebsmodus „Standby“ aktiviert werden
  - Nach der Aktivierungszeit wird eine Goodbye Szene ausgelöst
    Hier kann beispielsweise die Beleuchtung ausgeschaltet werden

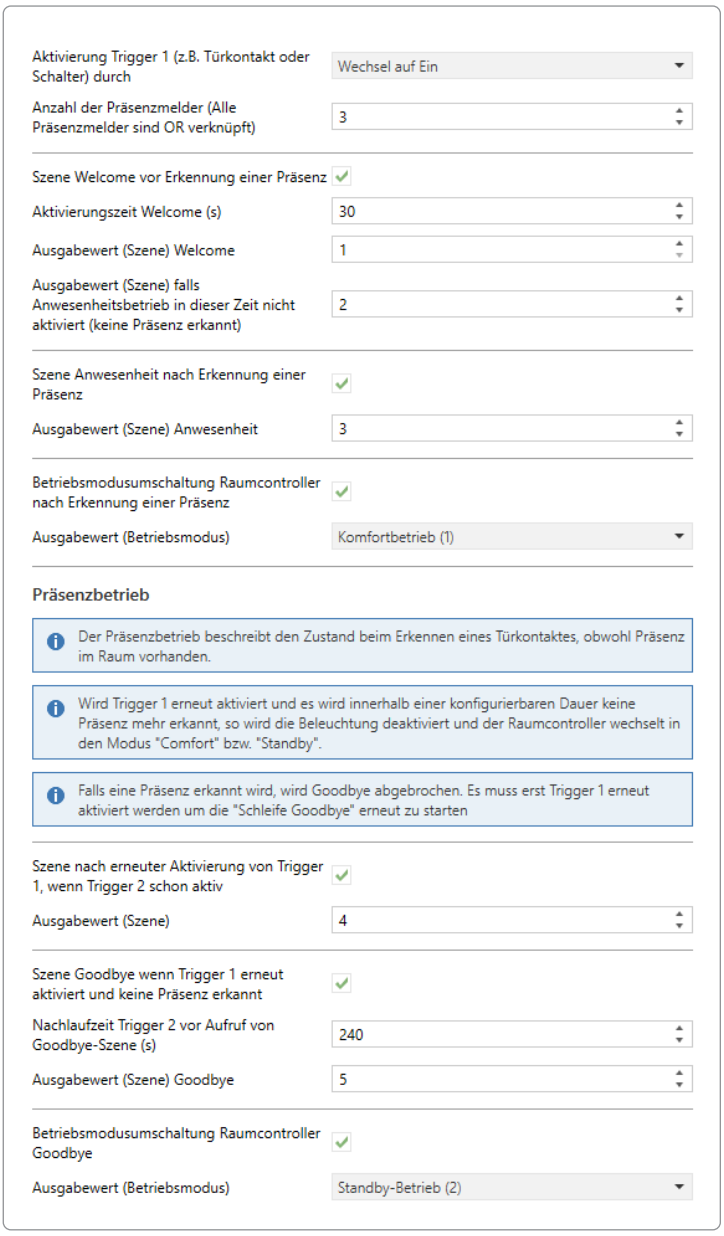


Abb. 36: Anwesenheitsüberwachung mit Präsenzmelder – Luxury

8.2 Applikationsprogramm B – KNX IP-Schnittstelle

8.2.1 Mapper

Der praktische Nutzen des Mappers wird im folgenden Szenario erläutert:

Eine Anlage besteht aus einer Innen- und Außenlinie. Um die Sicherheit der Anlage zu erhöhen, wird beschlossen, die Außenlinie Secure umzurüsten. Z. B. die Öffnung des Garagentors bzw. die Schließung erfolgt über KNX und Secure-Kommunikation. Im Beispiel seien das die Gruppenadressen 17/2/1, 17/2/2 und 17/2/3. Diese werden über zwei Router in die Innenlinie geführt. Die Geräte dort realisieren diese Funktionen in der Gruppenkommunikation 1/2/1, 1/2/2 und 1/2/3. Die Innenlinie verfügt aber nur über unverschlüsselte Aktorik und Sensorik. Über den Mapper werden nun die GAs 17/2/1 auf 1/2/1, 17/2/2 auf 1/2/2, 17/2/3 auf 1/2/3 gemappt. Daher können nun die Geräte auf der Innenlinie mit der Außenlinie kommunizieren. Über das Routing kann nun festgelegt werden, dass die Hauptgruppe 17 geroutet wird, aber die Hauptgruppe 2 blockiert wird. Damit kann nun die Sicherheit auf der Außenlinie problemlos mit der Innenlinie kombiniert werden.

8.2.2 Fernwartung

Über die einstellbaren Parameter „Secure Tunnelling nach Geräteneustart“ bzw. „Secure Tunnelling nach Fernwartung“ kann ein verschlüsselter oder ein herkömmlicher Zugriff über die Tunnelverbindungen gewährleistet werden. Die zugreifende Visualisierung muss alle Eigenschaften der verschlüsselten Tunnelverbindung unterstützen und bewusst aktiviert werden.

Für den herkömmlichen Zugriff (z. B. Smart Visu Server) sind beide Parameter auf „Aus“ einzustellen.

Für den verschlüsselten Zugriff (z. B. JUNG Visu Pro) sind beide Parameter auf „An“ einzustellen.

9 Firmware-Update

Das Gerät besteht aus einer Kombination von folgenden Geräten:

- Spannungsversorgung mit IP-Schnittstelle
- Spannungsversorgung mit IP-Schnittstelle - Zusatzfunktionen

Für beide Geräte gibt es nur eine kombinierte Update-Datei mit der Endung „b03“.

Das Firmware-Update für beide Geräte wird über die physikalische Adresse des Geräts „Spannungsversorgung mit IP-Schnittstelle“ eingespielt.

9.1 Firmware-Version anzeigen

Die aktuelle Version der Firmware kann nur beim Gerät „Spannungsversorgung mit IP-Schnittstelle - Zusatzfunktionen“ angezeigt werden.

- Rechtsklick auf das Gerät in der ETS ausführen.
- „Info > Geräteinfo“ auswählen.
  Firmware-Version wird hinter den eckigen Klammern angezeigt.
  Beispiel: ... [...] 1.3

9.2 Firmware-Update vorbereiten

Voraussetzungen:

- Nur der Besitzer der ETS-Softwarelizenz und des ETS-Projekts darf das Firmware-Update durchführen.
- Das Gerät darf nicht durch ein Passwort geschützt sein.

9.2.1 Sichere Inbetriebnahme deaktivieren

Das Gerät „Spannungsversorgung mit IP-Schnittstelle“ muss sich vor der Durchführung des Updates im unsicheren Modus befinden.

- In den Geräteeigenschaften „Sichere Inbetriebnahme“ des Geräts deaktivieren, siehe Abbildung 5.

9.2.2 Gerät neuprogrammieren

Das Gerät „Spannungsversorgung mit IP-Schnittstelle“ muss vor der Durchführung des Updates neuprogrammiert werden.

- Rechtsklick auf das Gerät in der ETS ausführen.
- „Programmieren > Applikationsprogramm“ auswählen.
  Neuprogrammierung wird automatisch durchgeführt.

9.3 Firmware-Update durchführen

Das Update muss mit dem JUNG Firmwareupdate-Tool durchgeführt werden.

Das JUNG Firmwareupdate-Tool steht auf unserer Website zum Download zur Verfügung.

Detaillierte Informationen zum JUNG Firmwareupdate-Tool finden Sie in der dazugehörigen Anleitung.

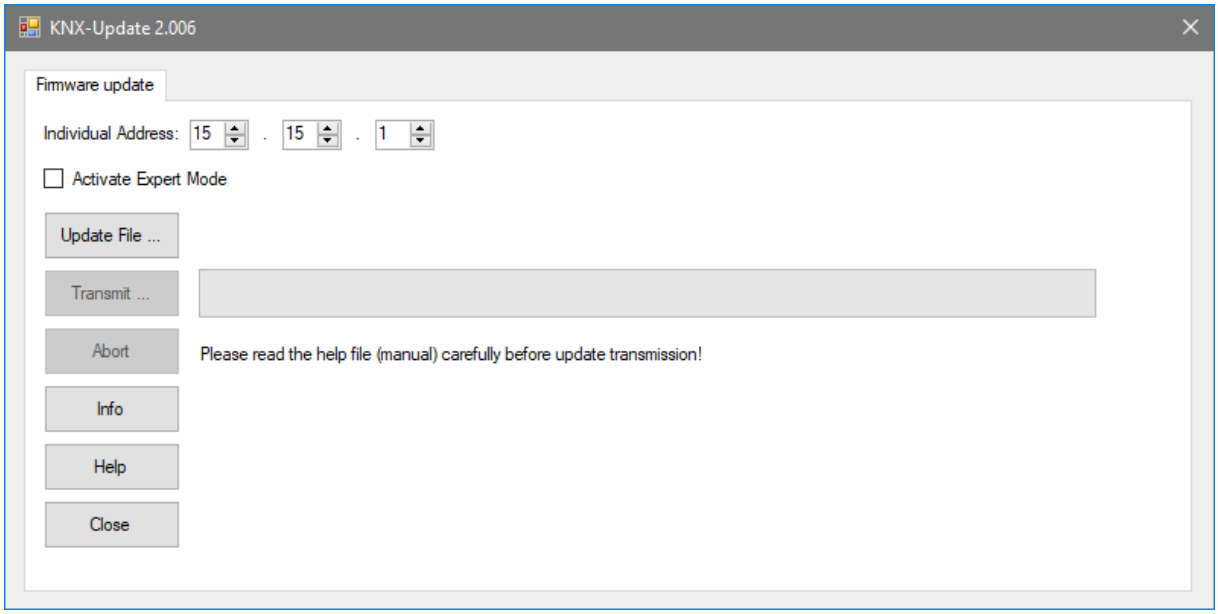


Abb. 37: Firmwareupdate-Tool

- JUNG Firmwareupdate-Tool starten.
- Physikalische Adresse des Geräts „Spannungsversorgung mit IP-Schnittstelle“ eingeben.
- Update-Datei auswählen mit Schaltfläche „Update File“.
- Update starten mit Schaltfläche „Transmit“.
  Update wird automatisch für beide Geräte durchgeführt.
  Beide Geräte werden durch das Update auf Werkseinstellungen zurückgesetzt.
- Nach dem Update in den Geräteeigenschaften physikalische Adresse für beide Geräte vergeben, s. Abbildung 5 und Abbildung 7.
- Beide Geräte neuprogrammieren über „Programmieren > Applikationsprogramm“.
- Ggf. „Sichere Inbetriebnahme“ des Geräts „Spannungsversorgung mit IP-Schnittstelle“ wieder aktivieren.

10 FAQ

Problem:
Spannungsversorgung mit IP-Schnittstelle - Zusatzfunktionen:
Programmierung wird nach Timeout abgebrochen

Mögliche Ursache:
Die Physikalische Adresse kann bei der Programmierung nicht vergeben werden.

Erläuterung:
Das Gerät wurde über Copy-and-paste in das ETS-Projekt aufgenommen.
Es wurden keine automatischen Adressen vergeben.
Alle 8 Tunneladressen sind im Parkmodus und ungültig.

Lösung:
Das Gerät per Drag-and-drop aus dem Katalog in das Projekt aufnehmen.
Die 8 Tunneladressen werden von der ETS automatisch vergeben.

Problem:
Spannungsversorgung mit IP-Schnittstelle:
Programmierung wird nach Timeout abgebrochen

Mögliche Ursache:
Eingesetzte Systemkomponenten (z. B. Bereichs-/Linienkoppler) sind inkompatibel mit KNX Data Secure.

Erläuterung:
KNX Data Secure verwendet ein längeres Telegrammformat (Extended Frames). Nur Geräte mit KNX Data Secure können innerhalb einer Linie oder eines Liniensegments stets sicher miteinander kommunizieren und auch sicher mit der ETS in Betrieb genommen werden.

Lösung:
Alte bzw. inkompatible Systemkomponenten müssen durch neue Systemkomponenten ersetzt werden.

11 Begriffe

Begriff	Beschreibung
Backbone	Bei IP-Routern und IP-Schnittstellen ist dies immer das IP-Netzwerk.
Verschlüsselung, Verschlüsselt	Wenn Geräte Dateninformationen in Form von Telegrammen über den TP-Bus oder IP-Netzwerk schicken, so sind diese grundsätzlich von Dritten lesbar. Diese benötigen hierzu lediglich Zugang zum TP-Bus oder IP-Netzwerk. Verschlüsselung der Daten soll in diesem Zusammenhang bedeuten, dass die Inhalte der Telegramme nicht mehr zu deuten sind, wenn die Verschlüsselungsparameter (z. B. Kennwörter) nicht bekannt sind.
Schlüssel, Verschlüsselungsparameter	Eine Folge von Zahlen, die nur dem ETS-Projekt bekannt sind. Diese Zahlen dienen zur Umformung der Daten in beide Richtungen: Ver- und Entschlüsseln.
FDSK (Factory Default Setup Key)	Der initiale Fabrikschlüssel. Dieser Schlüssel dient bei der Inbetriebnahme der initialen Programmierung. Dabei wird ein neuer Schlüssel in das Gerät geladen, wobei dieser Vorgang mit dem FDSK verschlüsselt wird. Der FDSK-Schlüssel ist danach nicht mehr gültig. Erst beim Zurücksetzen auf den Werkszustand (Factory Reset) wird er wieder aktiviert.
Tunneling	Eine KNX-Punkt-zu-Punkt-Verbindung auf dem TCP/IP Netzwerk, die entweder per UDP oder TCP-Protokoll aufgebaut wird. Tunneling hat immer eine Sicherungsschicht eingebaut, d. h. unabhängig von der Ethernetverbindung, z. B. Kabel oder WLAN, und unabhängig vom TCP/IP-Protokoll (UDP oder TCP) gehen keine Daten verloren. Bei UDP gilt allerdings die Einschränkung, dass die Sicherungsschicht mit einem 1-Sekunden-Timeout arbeitet. Dieser Timeout kann im erweiterten Setup angepasst werden.
Telnet	Ein einfacher TCP-Server auf Port 23, der direkte textbasierte Kommunikation mit dem IP-Gerät ermöglicht. Telnet ist ein de facto Standard, der auf der Windowsebene z. B. mit „PuTTY“ angesprochen wird.
Abgesicherter Modus, Secure Mode	Wenn das Gerät über die ETS so parametriert wird, dass die Kommunikation nur verschlüsselt erfolgt, spricht man vom abgesicherten Modus oder engl. Secure Mode.
Nicht abgesicherter Modus, Plain Mode	Wenn das Gerät über die ETS so parametriert wird, dass die Kommunikation nur unverschlüsselt erfolgt, spricht man vom nicht abgesicherten Modus oder engl. Plain Mode.

12 Technische Daten

Symbole	 Darf nicht über den Hausmüll entsorgt werden.
Nennspannung	AC 110 ... 240 V (± 10 %)
Netzfrequenz	50/60 Hz
Verlustleistung (max. Belastung aller Ausgänge)	max. 1,4 W
Wirkungsgrad	ca. 88 %
Nennspannung	DC 230 V (± 10 %)
Nennleistung	12 W
KNX **KNX Medium** **Ausgangsspannung Bus** **Ausgangsstrom** **Kurzschlussstrom** **Parallelbetrieb mit identischer Spannungsversorgung** **Anschluss KNX**	 TP 256 DC 28 ... 31 V SELV 320 mA max. 1 A nein Anschlussklemme
IP-Kommunikation	Ethernet 10/100 BaseT (10/100 Mbit/s)
Anschluss IP	1 x RJ45
Umgebungstemperatur	−5 ... +45 °C
Lager-/Transporttemperatur	−25 ... +75 °C
Relative Feuchte	max. 93 % (keine Betauung)
Einbaubreite	108 mm (6 TE)
Anschlussart	Schraubklemmen
eindrähtig	1 ... 4 mm²
feindrähtig ohne Aderendhülse	1 ... 4 mm²
feindrähtig mit Aderendhülse	1 ... 2,5 mm²

13 Gewährleistung

Die Gewährleistung erfolgt im Rahmen der gesetzlichen Bestimmungen über den Fachhandel.

14 Open Source Software

Dieses Produkt verwendet Software aus dritten Quellen folgender Autoren:

Adam Dunkels adam@sics.se
Marc Boucher <marc@mbsi.ca> and David Haas dhaas@alum.rpi.edu
Guy Lancaster <lancasterg@acm.org>, Global Election Systems Inc.
Martin Husemann <martin@NetBSD.org>
Van Jacobson (van@helios.ee.lbl.gov)
Paul Mackerras, paulus@cs.anu.edu.au,
Christiaan Simons christiaan.simons@axon.tv
Jani Monoses jani@iv.ro
Leon Woestenberg <leon.woestenberg@gmx.net>

14.1 LWIP

Quelle: https://savannah.nongnu.org/projects/lwip/

Copyright (c) 2001-2004 Swedish Institute of Computer Science.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification,
are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice,
this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice,
this list of conditions and the following disclaimer in the documentation
and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products
derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ‘AS IS‘ AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.}

ZidaTech
Innovation + Systeme

ZidaTech AG
Fabrikstrasse 9
CH-4614 Hägendorf

Telefon: 062 209 60 30
E-Mail: info@zidatech.ch
www.zidatech.ch