DE

LEDIMAX®

Bedienungs- und Montageanleitung

LEDIMAX KNX IP Schnittstelle MIT KNX SECURITY

(Art. LX-6095-KX)

Kompakte busversorgte Schnittstelle zwischen LAN/Ethernet und KNX-Bus mit KNX Security

LEDIMAX KNX IP Schnittstelle

Anwendung

Das LEDIMAX KNX IP SCHNITTSTELLE MIT KNX SECURITY dient als Schnittstelle für PC oder Laptop zum KNX Bus. Von jedem Punkt im LAN kann auf den KNX Bus zugegriffen werden. Das LEDIMAX KNX IP SCHNITTSTELLE MIT KNX SECURITY kann als Programmierschnittstelle für die ETS® verwendet werden. Beim Zugriff über KNXnet/IP Tunneling sind max. 8 Verbindungen gleichzeitig möglich.

Das Gerät unterstützt KNX Security. Die Option kann in der ETS aktiviert werden. Als Secure Interface verhindert das Gerät den unberechtigten Zugriff auf das System.

Die IP-Adresse kann über DHCP oder durch die ETS Konfiguration zugewiesen werden. Das Gerät arbeitet nach der KNXnet/IP-Spezifikation unter Verwendung von Core, Device Management und Tunneling.

Die Spannungsversorgung erfolgt über den KNX Bus.

KNX Security

Der KNX Standard wurde um KNX Security erweitert, um KNX Installationen vor unerlaubten Zugriffen zu schützen. KNX Security verhindert zuverlässig sowohl das Mithören der Kommunikation als auch die Manipulation der Anlage.

Die Spezifikation für KNX Security unterscheidet zwischen KNX IP Security und KNX Data Security. KNX IP Security schützt die Kommunikation über IP während auf KNX TP die Kommunikation unverschlüsselt bleibt. Somit kann KNX IP Security auch in bestehenden KNX Anlagen und mit nicht-secure KNX TP Geräten eingesetzt werden.

KNX Data Security beschreibt die Verschlüsselung auf Telegrammebene. Das heißt, dass auch die Telegramme auf dem Twisted Pair Bus verschlüsselt werden.

KNX IP Security für die Interface Funktion

Bei der Verwendung eines KNX IP Interfaces zum Bus ist ohne Security der Zugriff auf die Installation für alle Geräte möglich, die Zugang zum IP Netzwerk haben. Mit KNX Security ist ein Passwort erforderlich. Bereits für die Übertragung des Passwortes wird eine sichere Verbindung aufgebaut. Die gesamte Kommunikation über IP ist verschlüsselt und abgesichert.

In beiden Modi leitet das Interface sowohl verschlüsselte als auch unverschlüsselte KNX Telegramme weiter. Die Security-Eigenschaften werden vom jeweiligen Empfänger bzw. Tool geprüft.

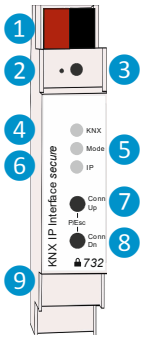
KNX Data Security für das Gerät

Das LEDIMAX KNX IP SCHNITTSTELLE MIT KNX SECURITY unterstützt auch KNX Data Security, um das Gerät vor unerlaubten Zugriffen aus dem KNX Bus zu schützen. Wird das LEDIMAX KNX IP über den KNX Bus programmiert, erfolgt dies mit verschlüsselten Telegrammen.

Verschlüsselte Telegramme sind länger als die bisher verwendeten unverschlüsselten. Deshalb ist es für die sichere Programmierung über den Bus erforderlich, dass das verwendete Interface (z.B. USB) und ggf. dazwischenliegende Linienkoppler die sogenannten KNX Long-Frames unterstützten.

Installation und Inbetriebnahme

Das *LEDIMAX KNX IP* wird auf einer Hutschiene montiert und hat einen Platzbedarf von 1 TE (18 mm). Es besitzt folgende Bedienelemente und Anzeigen:



1 *KNX Bus Anschluss*
2 *Programmier-LED (rot)*
3 *Taster f. Programmiermodus*
4 *KNX LED (mehrfarbig)*
5 *Mode LED (mehrfarbig)*
6 *IP LED (mehrfarbig)*
7 *Taster Connection up*
8 *Taster Connection down*
9 *LAN Buchse*

Das LEDIMAX KNX IP SCHNITTSTELLE MIT KNX SECURITY wird aus dem KNX Bus versorgt. Der Anschluss einer externen Versorgungsspannung ist nicht erforderlich.

Bei fehlender Busspannung ist das Gerät ohne Funktion.

KNX Programmiermodus

Der KNX Programmiermodus wird über den versenkten KNX-Programmiertaster 3 oder über gleichzeitigen Druck der Tasten 7 und 8 ein- bzw. ausgeschaltet.

Statusanzeige

Die KNX LED 4 leuchtet grün bei vorhandener KNX Busspannung. Bei Flackern dieser LED findet Telegrammverkehr auf dem KNX Bus statt.

Fehler in der Kommunikation (z.B. Telegrammwiederholungen oder Telegrammfragmente) werden durch einen kurzzeitigen Farbwechsel zu rot angezeigt.

Zusammenfassung der Zustände der *KNX LED* 4:

LED Verhalten	Bedeutung
LED leuchtet grün	KNX Busspannung vorhanden.
LED flackert grün	Telegrammverkehr auf dem KNX Bus.
LED kurzzeitig rot	Fehler in der Kommunikation auf dem KNX Bus.

Die IP LED 6 leuchtet bei einem aktiven Ethernet-Link. Diese LED ist grün, wenn das Gerät gültige IP Einstellungen (IP Adresse, Subnetz und Gateway) hat. Bei ungültigen bzw. nicht vorhandenen IP Einstellungen ist diese LED rot. Dies ist z.B. auch der Fall, wenn das Gerät die IP Einstellungen vom DHCP Server noch nicht erhalten hat. Bei Flackern dieser LED findet IP Telegrammverkehr statt.

Zusammenfassung der Zustände der *IP LED* 6:

LED Verhalten	Bedeutung
LED leuchtet grün	Das Gerät hat einen aktiven Ethernet-Link und gültige IP Einstellungen.
LED leuchtet rot	Das Gerät hat einen aktiven Ethernet-Link und ungültige IP Einstellungen oder noch keine IP Einstellungen vom DHCP Server erhalten.
LED flackert grün	IP-Telegrammverkehr

Mit der Mode LED 5 kann der Status jeder KNXnet/IP Tunneling Verbindung angezeigt werden.

Dazu kann mit den Tastern Conn Up/Dn 7 8 die jeweilige Verbindung ausgewählt werden. Conn Up 7 zählt die Verbindungsnummer hoch, Conn Dn 8 herunter. Die aktuelle Verbindungsnummer wird durch 1 bis 5-faches Blitzen der Mode LED 5 angezeigt. Eine verfügbare KNXnet/IP Tunneling Verbindung wird grün angezeigt, eine belegte KNXnet/IP Tunneling Verbindung orange.

Über die Escape-Funktion (Esc) kann durch gleichzeitiges Betätigen der Taster Conn Up/Dn 7 8 diese Anzeige beendet werden.

Sind weder Programmiermodus noch Handbedienung aktiv, kann die Mode LED 5 Konfigurationsfehler anzeigen.

Zusammenfassung der Zustände der *Mode LED* 5:

LED Verhalten	Bedeutung
LED leuchtet grün	Das Gerät arbeitet im normalen Betriebsmodus.
LED leuchtet rot	Der Programmiermodus ist aktiv.
LED blitzt 1x..5x grün	Der Programmiermodus ist nicht aktiv. Handbedienung (Statusanzeige) aktiv: Der angewählte Tunnel (1..5) ist frei.
LED blitzt 1x…5x orange	Der Programmiermodus ist nicht aktiv. Handbedienung (Statusanzeige) aktiv: Der angewählte Tunnel (1..5) ist belegt.
LED blinkt rot	Der Programmiermodus ist nicht aktiv. Der Handbedienung ist nicht aktiv. Das Gerät ist nicht korrekt geladen. z.B. nach Abbruch eines Downloads.

Werkseinstellungen

Ab Werk ist folgende Konfiguration voreingestellt:

Physikalische Adresse des Gerätes:	**15.15.255**
Konfigurierte KNXnet/IP Tunneling Verbindung:	**1**
Physikalische Adr. der Tunneling Verbindung:	**15.15.240**
IP Adressen Vergabe:	**DHCP**
Initialer Schlüssel (FDSK)	**aktiv**
Security Modus	**nicht aktiv**

Zurücksetzen auf Werkseinstellungen (Master-Reset)

Es besteht die Möglichkeit, das Gerät auf diese Werkseinstellungen zurückzusetzen.

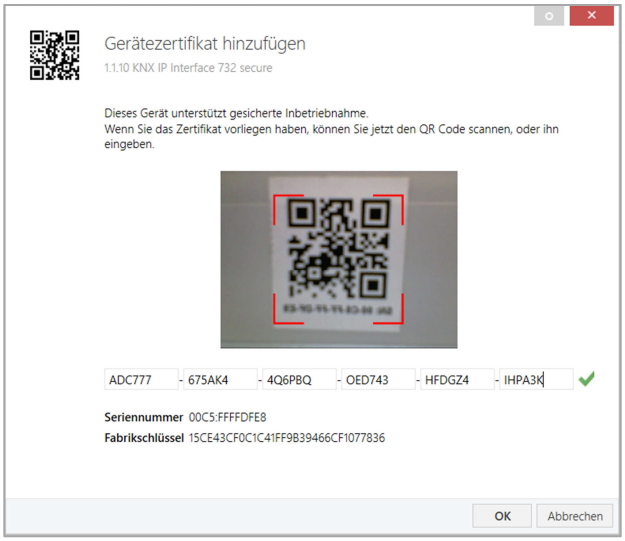
- KNX Bus Anschluss 1 vom Gerät trennen
- KNX Programmiertaster 3 drücken und gedrückt halten
- KNX Bus Anschluss 1 zum Gerät wieder herstellen
- Programmiertaster 3 mindesten noch 6 Sekunden gedrückt halten
- Ein kurzes Aufblinken aller LEDs (2 4 5 6) signalisiert die erfolgreiche Rücksetzung auf Werkseinstellung.

ETS Datenbank

Die ETS Datenbank (ab ETS 5.7) kann im KNX Online-Katalog der ETS heruntergeladen werden.
Wird das erste Produkt mit KNX Security in ein Projekt eingefügt, fordert die ETS dazu auf, ein Projektpasswort einzugeben.

Dieses Passwort schützt das ETS Projekt vor unberechtigtem Zugriff. Dieses Passwort ist kein Schlüssel, der für die KNX Kommunikation verwendet wird. Die Eingabe des Passwortes kann mit „Abbrechen“ umgangen werden, dies wird aus Sicherheitsgründen aber nicht empfohlen.

Für jedes Gerät mit KNX Security, das in der ETS angelegt wird, benötigt die ETS ein Gerätezertifikat. Dieses Zertifikat beinhaltet die Seriennummer des Gerätes sowie einen initialen Schlüssel (FDSK = Factory Default Setup Key).

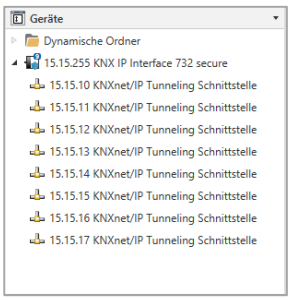


Das Zertifikat ist als Text auf dem Gerät aufgedruckt. Es kann auch bequem über eine Webcam vom aufgedruckten QR-Code abgescannt werden.

Die Liste aller Gerätezertifikate kann im ETS-Fenster Übersicht – Projekte – Sicherheit verwaltet werden.

Dieser initiale Schlüssel wird benötigt, um ein Gerät von Anfang an sicher in Betrieb zu nehmen. Selbst wenn der ETS-Download von einem Dritten mitgeschnitten wird, hat dieser anschließend keinen Zugriff auf die gesicherten Geräte. Während dem ersten sicheren Download wird der initiale Schlüssel von der ETS durch einen neuen Schlüssel ersetzt, der für jedes Gerät einzeln erzeugt wird. Somit wird verhindert, dass Personen oder Geräte, die den initialen Schlüssel eventuell kennen, Zugriff auf das Gerät haben. Der initiale Schlüssel wird erst bei einem Master-Reset wieder aktiviert.
Durch die Seriennummer im Zertifikat kann die ETS während eines Downloads den richtigen Schlüssel zu einem Gerät zuordnen.

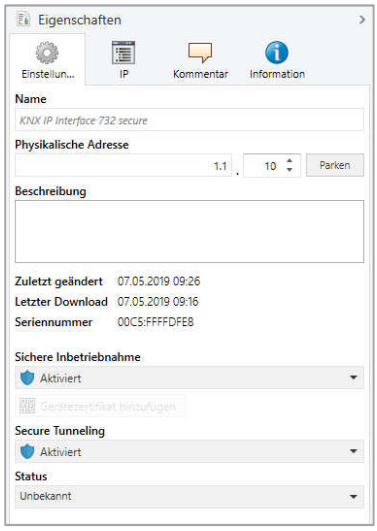
In der ETS werden einige Einstellungen zusätzlich zum Parameterdialog im Eigenschaftendialog (am Bildschirmrand) angezeigt. So können hier die IP-Einstellungen vorgenommen werden. Die zusätzlichen Adressen für die Schnittstellen-Verbindungen werden in der Topologie-Ansicht angezeigt.



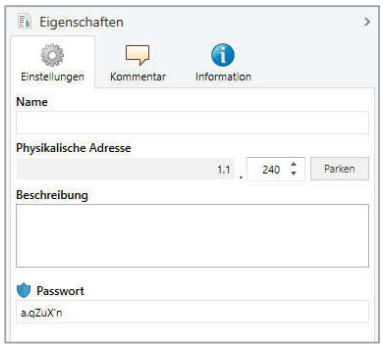
Um die einzelnen Adressen zu ändern, ist der entsprechende Eintrag in der Liste zu markieren und im Textfeld die gewünschte Adresse einzugeben. Sollte der Rahmen des Textfeldes, nach Eingabe, seine Farbe auf Rot wechseln weist dies darauf hin, dass die eingegebene Adresse bereits verwendet wird.

Stellen Sie sicher, dass keine der oben angegebenen Adressen bereits in Ihrer KNX Installation verwendet wird.

Durch Markieren des LEDIMAX KNX IP SCHNITTSTELLE MIT KNX SECURITY in der Baum-struktur der Topologie Ansicht des ETS Projekts, erscheint auf der rechten Seite des ETS Fensters die Übersicht „Eigenschaft"ten“. Unter Eigenschaften Menüpunkt „Einstellungen“ kann der Gerätename des LEDIMAX KNX IP SCHNITTSTELLE MIT KNX SECURITY geändert werden.



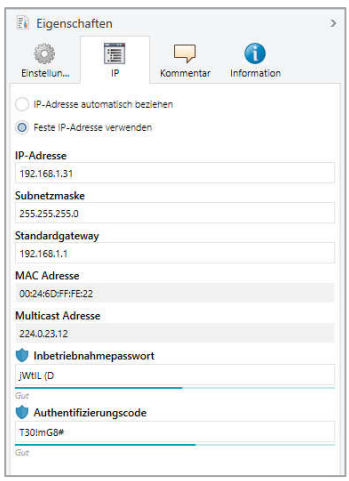
Wenn Secure Tunneling aktiviert ist, wird automatisch ein Passwort für jeden Tunnel vergeben. Dieses Passwort wird unter Menüpunkt „Einstellungen“ angezeigt, wenn ein Tunnel ausgewählt ist.



Unter Eigenschaften Menüpunkt „IP“ können die IP spezifischen Optionen des LEDIMAX KNX IP SCHNITTSTELLE MIT KNX SECURITY geändert werden.

Durch Umschalten von „IP-Adresse automatisch beziehen (über DHCP) auf „Folgende IP-Adresse verwenden“ (statische IP Adresse) kann die IP-Adresse, Subnetzmaske und das Standardgateway frei gewählt werden.

Die vorgenommenen Änderungen in den Eigenschaften Menüs werden erst nach einem Applikationsdownload wirksam.



IP-Adresse

Hier ist die IP-Adresse des *LEDIMAX KNX IP SCHNITTSTELLE MIT KNX SECURITY* einzutragen. Diese dient der Adressierung des Gerätes über das IP-Netzwerk (LAN). Die IP-Adressierung sollte mit dem Administra-tor des Netzwerks abgestimmt werden.

Subnetzmaske

Hier ist die Subnetz-Maske anzugeben. Diese Maske dient dem Gerät festzustellen, ob ein Kommunikationspartner sich im lokalen Netz befindet. Sollte sich ein Partner nicht im lokalen Netz befinden, sendet das Gerät die Telegramme nicht direkt an den Partner, sondern an das Gateway, das die Weiterleitung übernimmt.

Standardgateway

Hier ist die IP-Adresse des Gateways anzugeben, z.B. der DSL-Router der Installation.

Beispiel zur Vergabe von IP-Adressen:

Mit einem PC soll auf das LEDIMAX KNX IP SCHNITTSTELLE MIT KNX SECURITY zugegriffen werden.

IP-Adresse des PCs: 192.168.1.30

Subnetz des PCs: 255.255.255.0

Das LEDIMAX KNX IP SCHNITTSTELLE MIT KNX SECURITY befindet sich im selben lokalen LAN, d.h. er verwendet das gleiche Subnetz. Durch das Subnetz ist die Vergabe der IP-Adresse eingeschränkt, d.h. in diesem Beispiel muss die IP-Adresse des IP Interfaces 192.168.1.xx betragen, xx kann eine Zahl von 1 bis 254 sein (mit Ausnahme von 30, die schon verwendet wurde). Es ist darauf zu achten, keine Adressen doppelt zu vergeben.

IP-Adresse des IP Interface: 192.168.1.31

Subnetz des IP Interface: 255.255.255.0

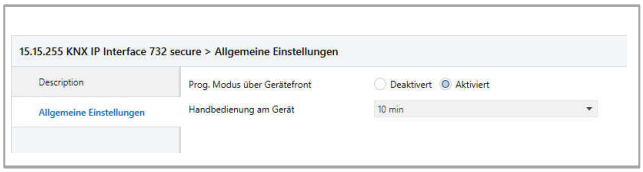
Fernzugriff

Über das *LEDIMAX KNX IP SCHNITTSTELLE MIT KNX SECURITY* ist ein Fernzugriff über das Internet möglich.

ETS Parameterdialog

Mit der ETS können folgende Parameter gesetzt werden

Allgemeine Einstellungen



Prog. Modus an Gerätefront

Zusätzlich zur normalen Programmiertaste 3 ermöglicht das Gerät die Aktivierung des Programmiermodus an der Gerätefront, ohne die Schalttafelabdeckung zu öffnen. Der Programmiermodus kann durch gleichzeitiges Drücken der Tasten 7 und 8 aktiviert und deaktiviert werden.

Diese Funktion kann über den Parameter „Prog. Modus an Gerätefront“ ein- und ausgeschaltet werden. Die vertiefte Programmiertaste 3 (neben der Programmier-LED 2) ist immer aktiviert und wird von diesem Parameter nicht beeinflusst.

Handbedienung am Gerät

Die Handbedienung des LEDIMAX KNX IP SCHNITTSTELLE MIT KNX SECURITY beinhaltet nur die Statusanzeige. Dieser Parameter stellt die Dauer des Handbedienungsmodus ein. Bei Beendigung wird der normale Anzeigemodus wiederhergestellt.

Programmierung

Das *LEDIMAX KNX IP SCHNITTSTELLE MIT KNX SECURITY* kann über verschiedene Wege von der ETS programmiert werden:

Über den KNX Bus

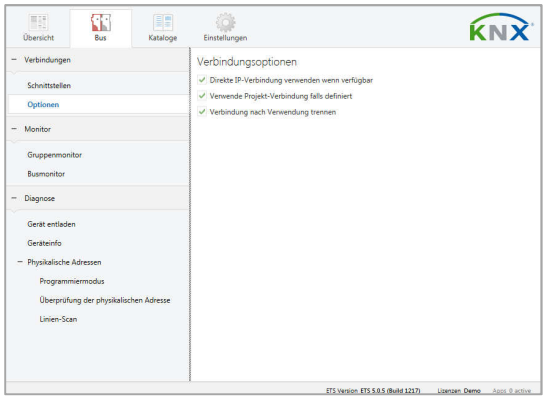
Dazu muss das Gerät nur mit dem Bus verbunden sein. Die ETS benötigt eine zusätzliche Schnittstelle (z.B. USB) zum Bus. Über diesen Weg kann sowohl die physikalische Adresse als auch die gesamte Applikation inklusive IP Konfiguration programmiert werden. Die Programmierung über den Bus wird empfohlen, wenn keine IP Verbindung hergestellt werden kann.

Über KNXnet/IP Tunnelling

Hierbei ist keine zusätzliche Schnittstelle erforderlich. Die Programmierung über KNXnet/IP Tunnelling ist möglich, wenn das Gerät bereits eine gültige IP Konfiguration besitzt (z.B. über DHCP). In diesem Fall wird das Gerät bei den Schnittstellen in der ETS angezeigt und muss ausgewählt werden. Der Download erfolgt aus dem ETS Projekt heraus wie bei anderen Geräten auch.

Über direkte IP Verbindung

Während KNXnet/IP Tunneling auf die Geschwindigkeit von KNX TP begrenzt sind, kann über eine direkte IP Verbindung das Gerät mit hoher Geschwindigkeit geladen werden. Die direkte IP Verbindung ist möglich, wenn das Gerät bereits sowohl eine gültige IP Konfiguration als auch eine physikalische Adresse besitzt. Dazu muss im ETS Menü bei „Bus - Verbindungen – Optionen“ die Auswahl „Direkte IP-Verbindung verwenden wenn möglich“ angewählt werden. Der Download erfolgt dann direkt in das Gerät und ist nicht im ETS Gruppenmonitor sichtbar.



Aufgrund der deutlich kürzeren Übertragungszeiten wird empfohlen, Downloads über IP durchzuführen.

Schnittstelleneinstellungen in der ETS

Das LEDIMAX KNX IP SCHNITTSTELLE MIT KNX SECURITY dient als Programmierschnitt-stelle. Die ETS kann mit dieser Funktion über IP eine Verbin-dung in die jeweilige TP Linie aufbauen.

In der ETS können Schnittstellen über das ETS Menü „Bus - Schnittstellen“ ausgewählt und konfiguriert werden.

Die ETS kann auf konfigurierte IP Schnittstellen auch ohne Datenbankeintrag zugreifen. Entspricht die Konfiguration nicht den Gegebenheiten der Installation, muss diese über das ETS Projekt konfiguriert werden. Siehe dazu den Abschnitt ETS Datenbank.

Ist im LEDIMAX KNX IP SCHNITTSTELLE MIT KNX SECURITY der Security-Modus aktiviert, ist ein Passwort erforderlich, um eine Verbindung herzustellen.

Im Auslieferungszustand erfolgt die Zuweisung der IP-Adresse automatisch über DHCP, d.h. es sind keine weiteren Einstellungen dafür notwendig. Um diese Funktion nutzen zu können, muss sich ein DHCP-Server im LAN befinden (z.B. haben viele DSL-Router einen DHCP-Server integriert).

Wenn das LEDIMAX KNX IP SCHNITTSTELLE MIT KNX SECURITY HUTSCHIENE an das LAN angeschlossen wurde und eine gültige IP Adresse hat, sollte es von der ETS automatisch im Menüpunkt „Bus“ unter „gefundene Schnittstellen“ erscheinen.

Durch Anklicken der gefundenen Schnittstelle wird diese als aktuelle Schnittstelle ausgewählt. Auf der rechten Seite des ETS Fensters erscheinen dann verbindungsspezifische Informationen und Optionen.

Der angezeigte Gerätename und die „Host Physikalische Adresse“ (physikalische Adresse des Gerätes) kann nur innerhalb Ihres ETS Projekts geändert werden.

Das LEDIMAX KNX IP SCHNITTSTELLE MIT KNX SECURITY verfügt wie alle programmier-baren KNX Geräte über eine physikalische Adresse, mit der das Gerät angesprochen werden kann. Diese wird zum Beispiel von der ETS beim Download des Interfaces über den Bus verwendet.

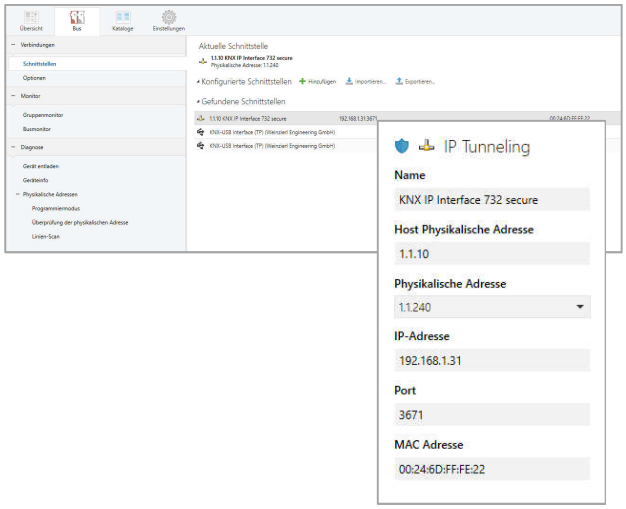
Für die Interface-Funktion verwendet das Gerät zusätzliche physikalische Adressen, die in der ETS eingestellt werden können. Sendet ein Client (z.B. ETS) über das KNX IP Interface Telegramme auf den Bus, so enthalten diese als Absende-Adresse eine der zusätzliche Adressen. Jede Adresse ist einer Verbindung zugeordnet. Somit können Antworttelegramme eindeutig zum jeweiligen Client weitergeleitet werden.

Die zusätzlichen physikalischen Adressen müssen aus dem Adressbereich der Bus-Linie sein, in der sich das Interface befindet und dürfen nicht von einem anderen Gerät verwendet werden.

Beispiel:

Geräteadresse	1.1.10	(Geräteadresse in der Topologie)
Verbindung 1	1.1.240	(1. zusätzliche Adresse)
Verbindung 2	1.1.241	(2. zusätzliche Adresse)
Verbindung 3	1.1.242	(3. zusätzliche Adresse)
Verbindung 4	1.1.243	(4. zusätzliche Adresse)
Verbindung 5	1.1.244	(5. zusätzliche Adresse)
Verbindung 6	1.1.245	(6. zusätzliche Adresse)
Verbindung 7	1.1.246	(7. zusätzliche Adresse)
Verbindung 8	1.1.247	(8. zusätzliche Adresse)

Im Abschnitt “Physikalische Adresse” kann die physikalische KNX Adresse der aktuell verwendeten KNXnet/IP Tunneling Verbindung ausgewählt werden.



Die physikalische KNX Geräteadresse sowie die physikalischen KNX Adressen für die zusätzlichen Tunneling Verbindungen können innerhalb des ETS Projekts geändert werden, nachdem das Gerät dem Projekt hinzugefügt wurde.

Open Source Lizenzen

Die in diesem Produkt eingesetzte Firmware basiert auf folgendem Open-Source Softwarepaket:
curve25519-donna: Curve25519 elliptic curve, public key function
Quelle: http://code.google.com/p/curve25519-donna/

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

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
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.
Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "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 COPYRIGHT OWNER OR CONTRIBUTORS 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.

WARNUNG

- Das Gerät darf nur von einer zugelassenen Elektrofachkraft installiert und in Betrieb genommen werden.
- Die geltenden Sicherheits- und Unfallverhütungsvorschriften sind zu beachten.
- Das Gerät darf nicht geöffnet werden.
- Bei der Planung und Errichtung von elektrischen Anlagen sind die einschlägigen Richtlinien, Vorschriften und Bestimmungen des jeweiligen Landes zu beachten.

IMPOLUX GmbH
D-56288 Kastellaun / Südstraße 4
Deutschland
Tel.: +49 (6762) 9699100
E-Mail: info@impolux.de
Web: www.Impolux.de