



## Applikationsbeschreibung

### KNX/IP Router Secure

*Elektrische / mechanische Eigenschaften: siehe Produktbeschreibungen*

- ▲ Hersteller
- ▲ Hager Electro
- ▲ Systemgeräte
  - IP/KNX Router

	Bestellnummer	Produktbezeichnung	Ref. Anwendungssoftware	TP-Produkt Funk Produkte
	TYFS121	KNX / IP Router Secure	STYFS121	

## Inhaltsverzeichnis

<b>1. Anwendung</b> .....	<b>3</b>
<b>2. KNX Security</b> .....	<b>3</b>
2.1. KNX IP Security für die Router-Funktion.....	3
2.2. KNX IP Security für die Interface Funktion.....	3
2.3. KNX Data Security für das Gerät .....	3
2.4. KNX Data Security für Gruppentelegramme .....	4
<b>3. Koppler-Funktion (KNXnet/IP Routing)</b> .....	<b>5</b>
<b>4. Funktion als Buszugriff (KNXnet/IP Tunneling)</b> .....	<b>7</b>
<b>5. Installation und Inbetriebnahme</b> .....	<b>7</b>
5.1. KNX Programmiermodus .....	7
5.2. Handbedienung und Statusanzeige .....	7
<b>6. Werkseinstellungen</b> .....	<b>9</b>
<b>7. Schnittstelleneinstellungen in der ETS</b> .....	<b>10</b>
<b>8. ETS Datenbank</b> .....	<b>12</b>
<b>9. ETS Parameterdialog</b> .....	<b>16</b>
9.1. Allgemeine Einstellungen .....	16
9.2. Routing (KNX -> IP).....	16
9.3. Routing (IP -> KNX).....	17
<b>10. Programmierung</b> .....	<b>19</b>
10.1. Über den KNX Bus .....	19
10.2. Über KNXnet/IP Tunneling .....	19
10.3. Über KNXnet/IP Routing .....	19
10.4. Über direkte IP Verbindung .....	19
<b>11. Fernzugriff</b> .....	<b>20</b>
11.1. Network Address Translation NAT .....	20
11.2. Fernzugriff über ein VPN.....	20
11.3. Fernzugriff und KNX secure .....	21
<b>12. Open Source Lizenzen</b> .....	<b>22</b>

## 1. Anwendung

Der kompakte KNX IP Router secure ermöglicht die Weiterleitung von Telegrammen zwischen verschiedenen Linien über ein LAN (IP) als schnellen Backbone. Das Gerät dient zudem als Programmierschnittstelle zwischen einem PC und dem KNX Bus (z.B. für ETS-Programmierung).

Das Gerät unterstützt KNX Security. Die Option kann in der ETS aktiviert werden. Als Secure Router ermöglicht das Gerät die Kopplung nicht gesicherter Kommunikation auf einer KNX TP Linie mit einem sicheren IP-Backbone.

Auch bei der Schnittstellenfunktion (Tunneling) verhindert KNX Security den unbefugten 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, Tunneling und Routing.

Der KNX IP Router secure besitzt eine erweiterte Filtertabelle für Hauptgruppe 0..31 und kann bis zu 150 Telegramme zwischenspeichern. Die Spannungsversorgung erfolgt über den KNX Bus..

## 2. 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..

### 2.1. KNX IP Security für die Router-Funktion

Die Kopplung einzelner KNX TP Linien über IP wird als KNX IP Routing bezeichnet. Die Kommunikation zwischen allen angeschlossenen KNX IP Router erfolgt über UDP Multicast.

Mit KNX IP Security erfolgt die Routing-Kommunikation verschlüsselt. Das heißt nur IP Geräte, die den Schlüssel kennen, können die Kommunikation entschlüsseln und gültige Telegramme senden. Ein Zeitstempel im Routing-Telegramm sorgt dafür, dass keine vorher aufgezeichneten Telegramme eingespielt werden können. Somit wird der sogenannte Replay-Attack verhindert.

Der Schlüssel für die Routing-Kommunikation wird von der ETS für jede Installation neu vergeben. Wenn KNX IP Security für Routing verwendet wird, müssen alle angeschlossenen KNX IP Geräte Security unterstützen und entsprechend konfiguriert sein.

### 2.2. KNX IP Security für die Interface Funktion

Bei der Verwendung eines KNX IP Routers als Interface 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..

### 2.3. KNX Data Security für das Gerät

Der KNX IP Router secure unterstützt auch KNX Data Security, um das Gerät vor unerlaubten Zugriffen aus dem KNX Bus zu schützen. Wird der KNX IP Router 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 unterstützen.

## **2.4. KNX Data Security für Gruppentelegramme**

Telegramme vom Bus, die nicht den KNX IP Router als Gerät adressieren werden entsprechend der Filtereinstellungen (Parameter und Filtertabelle) weitergeleitet bzw. blockiert. Hierbei spielt es keine Rolle, ob es sich um unverschlüsselte oder verschlüsselte Telegramme handelt. Das Weiterleiten erfolgt ausschließlich anhand der Zieladresse. Die Security-Eigenschaften werden vom jeweiligen Empfänger geprüft.

KNX Data Security und KNX IP Security können parallel eingesetzt werden. In diesem Fall würde zum Beispiel ein KNX Sensor ein mit KNX Data Security verschlüsseltes Gruppentelegramm auf den Bus senden. Bei der Weiterleitung über KNX IP mit KNX IP Security würde das verschlüsselte Telegramm so wie unverschlüsselte noch einmal verschlüsselt. Alle Teilnehmer auf der KNX IP Ebene, die KNX IP Security unterstützen, können zwar die IP Verschlüsselung decodieren, nicht aber die Data Security. Somit wird das Telegramm von den anderen KNX IP Router wieder mit KNX Data Security in die Ziellinie(n) übertragen. Nur Geräte, die den Schlüssel kennen, der für Data Security verwendet wurde, können das Telegramm interpretieren.

## Koppler-Funktion (KNXnet/IP Routing)

### 3. Koppler-Funktion (KNXnet/IP Routing)

Der KNX IP Router secure kann als Linien- bzw. Bereichskoppler arbeiten. In beiden Fällen wird das LAN (IP) als Backbone verwendet.

Die Einsatzmöglichkeiten des KNX IP Routers im Vergleich zur klassischen Topologie zeigt folgende Tabelle:

	Klassische Topologie (ohne IP)	IP Kopplung der Bereiche (IP Bereichskop.)	IP Kopplung der Linien (IP Linienkoppler)
<b>Bereichsline (Backbone)</b>	TP	IP	IP
<b>Kopplung</b>	KNX Linienkoppler (max. 15 St.)	KNX IP Router (max. 15 St.)	direkt über LAN Switch
<b>Hauptlinie</b>	TP	TP	IP
<b>Kopplung</b>	KNX Linienkoppler (max. 15x15 St.)	KNX Linienkoppler (max. 15x15 St.)	KNX IP Router (max. 225 St.)
<b>Linie</b>	TP	TP	TP

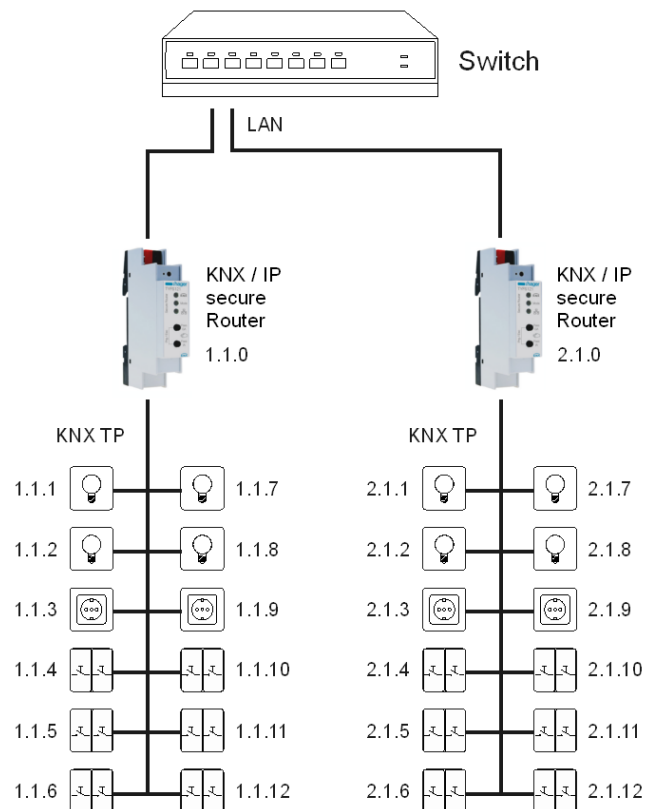


Figure 1 – KNX IP Router als Linienkoppler

Die Vergabe der physikalischen Adresse des KNX IP Router secure entscheidet, ob das Gerät als Linien- oder als Bereichskoppler arbeitet. Entspricht die physikalische Adresse der Form  $x.y.0$  ( $x, y: 1..15$ ), funktioniert der Router als Linienkoppler. Hat die physikalische Adresse die Form  $x.0.0$  ( $x: 1..15$ ), handelt es sich um einen Bereichskoppler..

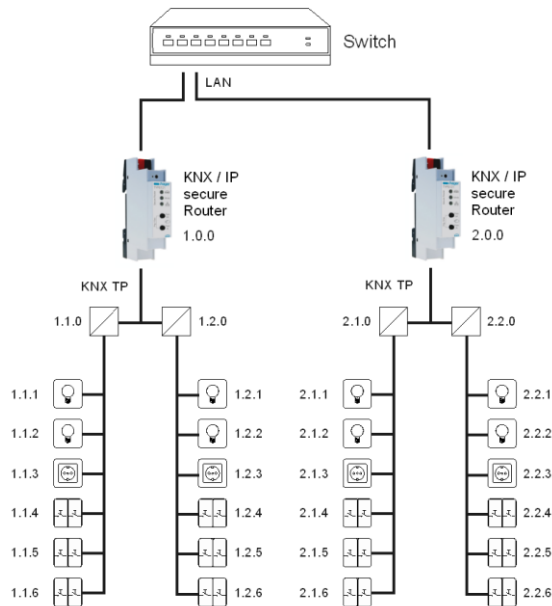


Figure 2 – KNX IP Router als Bereichskoppler

- i** Wird der KNX IP Router secure als Bereichskoppler (x.0.0) genutzt, darf sich kein KNX IP Router topologisch unterhalb befinden. Hat z.B. ein KNX IP Router die physikalische Adresse 1.0.0, so darf es keinen KNX IP Router mit der Adresse 1.1.0 geben..
- i** Wird der KNX IP Router secure als Linienkoppler (x.y.0) genutzt, darf sich kein KNX IP Router topologisch darüber befinden. Hat z.B. ein KNX IP Router die physikalische Adresse 1.1.0, so darf es keinen KNX IP Router mit der Adresse 1.0.0 geben..

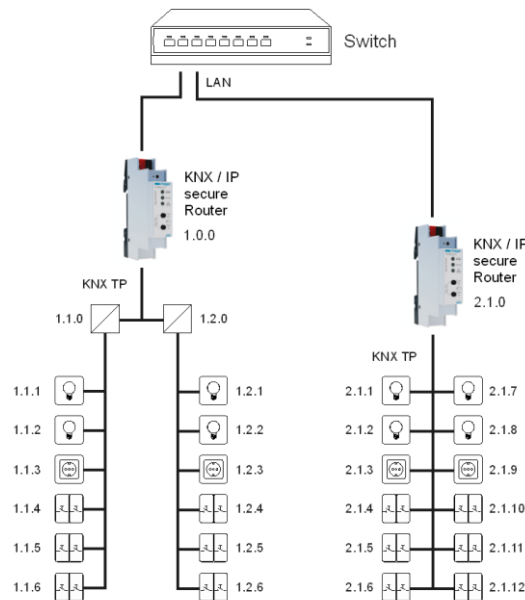


Figure 3 – KNX IP Router als Bereichs-und Linienkoppler

Der KNX IP Router besitzt eine Filtertabelle und trägt so zur Verringerung der Buslast bei. Die Filtertabelle (8kB) unterstützt den erweiterten Gruppenadressbereich (Hauptgruppen 0..31) und wird von der ETS automatisch erzeugt.

Aufgrund des Geschwindigkeitsunterschiedes zwischen Ethernet (10/100 MBit/s) und KNX TP (9,6 kBit/s) können auf IP wesentlich mehr Telegramme übertragen werden. Folgen mehrere Telegramme für die gleiche Linie kurz aufeinander, müssen diese im Router zwischengespeichert werden, um Telegrammverluste zu vermeiden. Hierzu besitzt der KNX IP Router secure Speicherplatz für 150 Telegramme (von IP nach KNX).

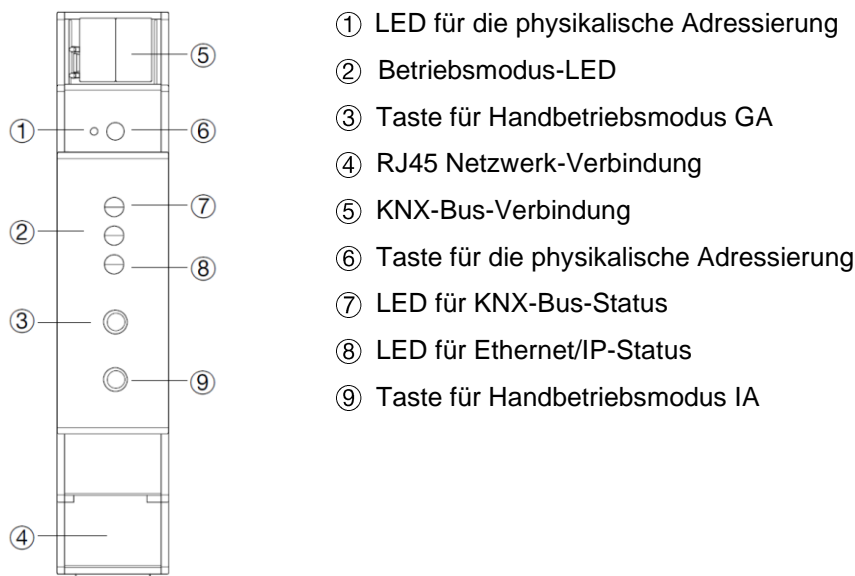
## Funktion als Buszugriff (KNXnet/IP Tunneling)

### 4. Funktion als Buszugriff (KNXnet/IP Tunneling)

Der KNX IP Router secure kann als Schnittstelle zum KNX genutzt werden. Es kann von jedem Punkt im LAN auf den KNX Bus zugegriffen werden. Dazu muss jeweils eine zusätzliche physikalische Adresse vergeben werden. Dies wird in den folgenden Kapiteln beschrieben.

### 5. Installation und Inbetriebnahme

Der KNX IP Router secure wird auf einer Hutschiene montiert und hat einen Platzbedarf von 1 TE (18 mm). Er besitzt folgende Bedienelemente und Anzeigen::



Der Anschluss einer externen Versorgungsspannung ist nicht erforderlich..

**i** Bei fehlender Busspannung ist das Gerät ohne Funktion.

#### 5.1. KNX Programmiermodus

Der KNX Programmiermodus wird über den versenkten KNX-Programmiertaster ⑥ oder über gleichzeitigen Druck der Tasten ③ und ⑨ ein- bzw. ausgeschaltet.

#### 5.2. Handbedienung und Statusanzeige

Die KNX LED ⑦ 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..

LED Verhalten ⑦	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.

Table 1 - Zusammenfassung der Zustände der KNX LED

Die IP LED ⑧ 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.

LED Verhalten ⑧	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

Table 2 - Zusammenfassung der Zustände der IP LED

Für Testzwecke (z.B. während der Inbetriebnahme) können die parametrisierten Routing-Einstellungen (filtern oder sperren) über die Handbedienung umgangen werden.

Mit dem Taster Pass Gas ③ kann das Weiterleiten gruppenadressierter Telegramme aktiviert werden..

Mit dem Taster Pass IAs ⑨ kann das Weiterleiten physikalisch adressierter Telegramme aktiviert werden. Dies wird jeweils mit einfachem Blitzen der Mode LED ② (orange) angezeigt. Werden beide Modi gleichzeitig ausgewählt, so blitzt die Mode LED.

Durch erneutes Drücken der Taster Pass Gas ③ und Pass IAs ⑨ können diese Einstellungen beliebig an- und abgewählt werden. Über die Escape-Funktion (Esc) kann durch gleichzeitiges Betätigen der Taster Pass GAs③ und Pass IAs ⑨ die Handbedienung beendet werden.

Sind weder Programmiermodus noch Handbedienung aktiv, kann die Mode LED ② Konfigurationsfehler anzeigen.

LED Verhalten ②	Bedeutung
LED leuchtet grün	Das Gerät arbeitet im normalen Betriebsmodus.
LED leuchtet rot	Der Programmiermodus ist aktiv.
LED blitzt 1x orange	Der Programmiermodus ist nicht aktiv. Handbedienung aktiv: Durchleitung IA oder GA
LED blitzt 2x orange	Der Programmiermodus ist nicht aktiv. Handbedienung aktiv: Durchleitung IA und GA
LED blinkt rot	Der Programmiermodus ist nicht aktiv. Die Handbedienung ist nicht aktiv. Das Gerät ist nicht korrekt geladen, z.B. nach Abbruch eines Downloads.

Table 3 - Zusammenfassung der Zustände der Mode LED



### 6. Werkseinstellungen

Ab Werk ist folgende Konfiguration voreingestellt :

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

#### Zurücksetzen auf Werkseinstellungen (Master-Reset)

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

- KNX Bus Anschluss ⑤ vom Gerät trennen
- KNX Programmieraster ⑥ drücken und gedrückt halten
- KNX Bus Anschluss ⑤ zum Gerät wieder herstellen
- Programmieraster ⑥ mindesten noch 6 Sekunden gedrückt halten
- Ein kurzes Aufblinken aller LEDs (①②⑦⑧) signalisiert die erfolgreiche Rücksetzung auf Werkseinstellung.

### 7. Schnittstelleneinstellungen in der ETS

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

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

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).

Nachdem der KNX IP Router an das LAN und den KNX Bus angeschlossen wurde, 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 verbindungspezifische Informationen und Optionen.

Der angezeigte Geräte name und die „Host Physikalische Adresse“ (physikalische Adresse des Gerätes) kann anschließend innerhalb des ETS Projekts geändert werden.

Der KNX IP Router secure verfügt wie alle programmierbaren KNX Geräte über eine physikalische Adresse, mit der das Gerät angesprochen werden kann. Diese wird zum Beispiel von der ETS beim Download des KNX IP Routers 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 den KNX IP Router 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 der KNX IP Router befindet und dürfen nicht von einem anderen Gerät verwendet werden.

**Beispiel:**

Geräteadresse	1.1.10	(address within ETS topology)
Verbindung 1	11.1.240	(1. zusätzliche Adresse)
Verbindung 2	11.1.241	(2. zusätzliche Adresse)
Verbindung 3	11.1.242	(3. zusätzliche Adresse)
Verbindung 4	11.1.243	(4. zusätzliche Adresse)
Verbindung 5	11.1.244	(5. zusätzliche Adresse)
Verbindung 6	11.1.245	(6. zusätzliche Adresse)
Verbindung 7	11.1.246	(7. zusätzliche Adresse)
Verbindung 8	11.1.247	(8. zusätzliche Adresse)

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

## Schnittstelleneinstellungen in der ETS

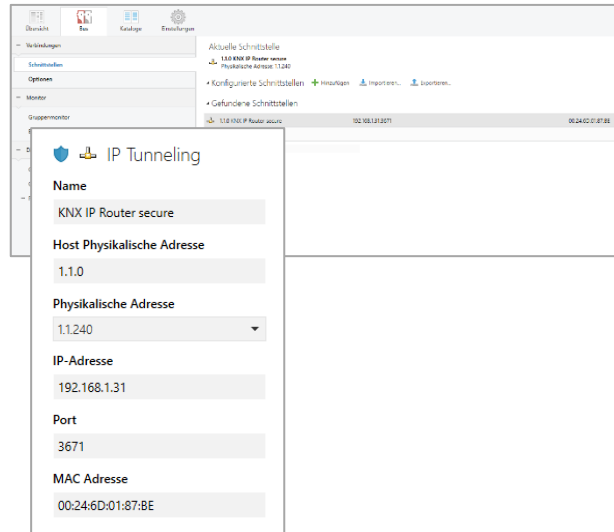


Figure 4 – IP Tunneling

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.

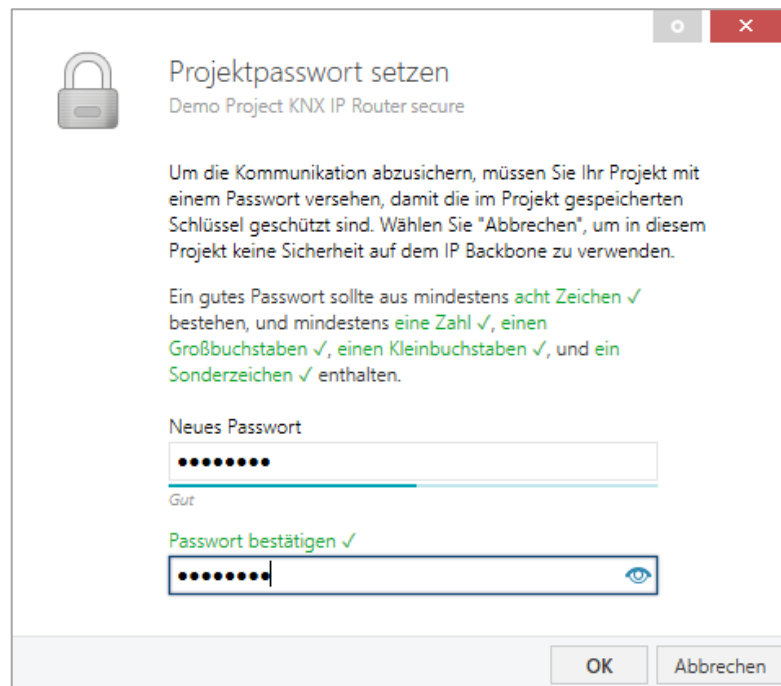
## 8. ETS Datenbank

Die ETS Datenbank (ab ETS 5.7) kann auf der Produkt Website KNX IP Interface secure oder im KNX Online-Katalog der ETS heruntergeladen werden.

Wenn Sie nicht an der KNX IP Secure Funktion Interesse haben, haben Sie immer noch die Möglichkeit, eine non-Secure Version der Applikation zu verwenden, um Ihr Gerät zu konfigurieren.

Wenn Sie die Secure Version der Applikation verwenden, müssen die folgenden Schritte durchgeführt werden.

Wird das erste Produkt mit KNX Security in ein Projekt eingefügt, fordert die ETS dazu auf, ein Projektpasswort einzugeben.




**Projektpasswort setzen**  
Demo Project KNX IP Router secure

Um die Kommunikation abzusichern, müssen Sie Ihr Projekt mit einem Passwort versehen, damit die im Projekt gespeicherten Schlüssel geschützt sind. Wählen Sie "Abbrechen", um in diesem Projekt keine Sicherheit auf dem IP Backbone zu verwenden.

Ein gutes Passwort sollte aus mindestens **acht Zeichen** ✓ bestehen, und mindestens **eine Zahl** ✓, **einen Großbuchstaben** ✓, **einen Kleinbuchstaben** ✓, und **ein Sonderzeichen** ✓ enthalten.

Neues Passwort  
  
 Gut

Passwort bestätigen ✓  
 

OK Abbrechen

Figure 5 – Projektpasswort ändern

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).



Figure 6 – Geräte-zertifikat hinzufügen

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 Geräte-zertifikate 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.

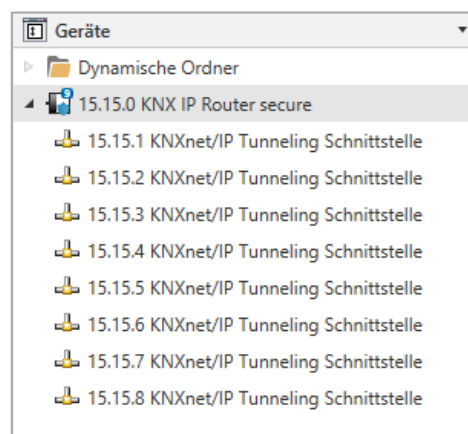



Figure 7 – Geräte

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 KNX IP Router 752 secure in der Baumstruktur der Topologie Ansicht des ETS Projekts, erscheint auf der rechten Seite des ETS Fensters die Übersicht „Eigenschaften“. Unter Eigenschaften Menüpunkt „Einstellungen“ kann der Gerätenamen des KNX IP Routers 752 secure geändert werden.

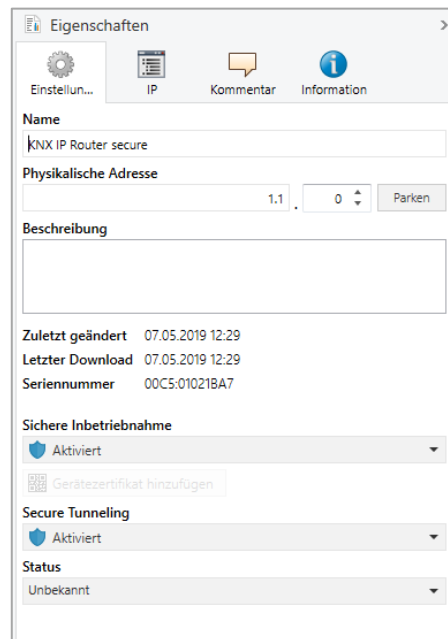


Figure 8 – Eigenschaften

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.

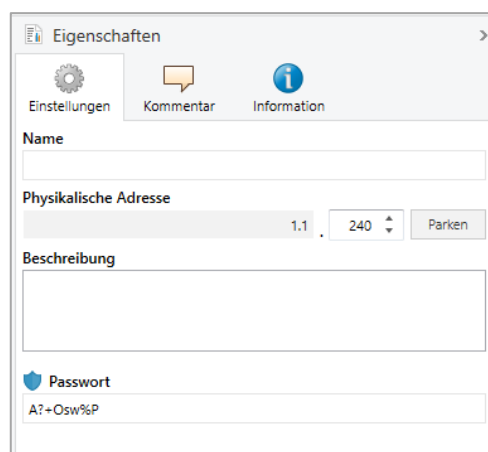



Figure 9 – Eigenschaften

Unter Eigenschaften Menüpunkt „IP“ spezifische Optionen des KNX IP Router secure 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.

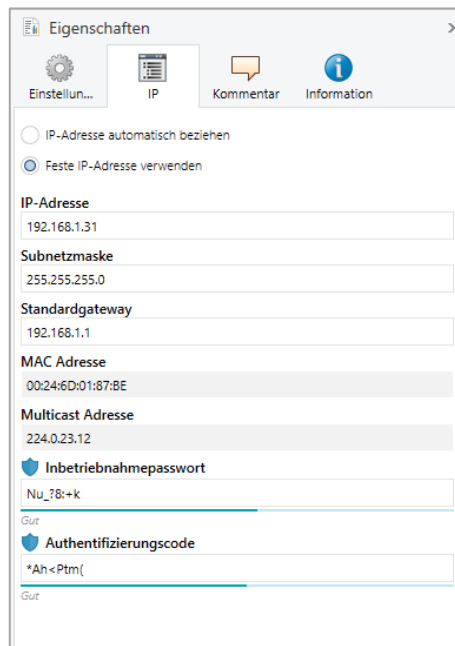


Figure 10 – Eigenschaften

#### ■ IP-Adresse

Hier ist die IP-Adresse des KNX IP Router secure einzutragen. Diese dient der Adressierung des Gerätes über das IP-Netzwerk (LAN). Die IP-Adressierung sollte mit dem Administrator 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 DSLRouter der Installation.

#### ■ Routing Multicast Adresse

Diese Adresse wird für das Routing von Telegrammen auf IP verwendet. Die Multicast-IP-Adresse 224.0.23.12 wurde für diesen Zweck (KNXnet/IP) von der IANA (Internet Assigned Numbers Authority) reserviert. Sollte eine andere Multicast-IP-Adresse gewünscht sein, muss diese aus dem Bereich 239.0.0.0 bis 239.255.255.255 sein.

#### ■ Beispiel zur Vergabe von IP-Adressen:

Mit einem PC soll auf das KNX IP Router secure zugegriffen werden :

IP-Adresse des PCs : 192.168.1.30

Subnetz des PCs : 255.255.255.0

Der KNX IP Router secure 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 Routers 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 Router : 192.168.1.31

Subnetz des IP Router : 255.255.255.0

### 9. ETS Parameterdialog

Mit der ETS können folgende Parameter gesetzt werden.

#### 9.1. Allgemeine Einstellungen

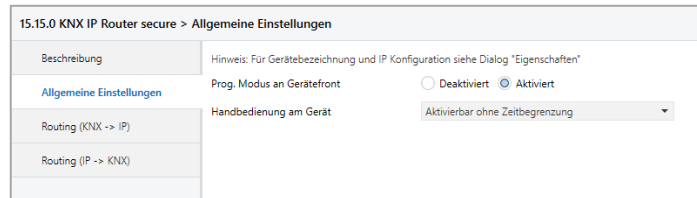


Figure 11 – Allgemeine Einstellungen

**i** Bei den beiden folgenden Parametern sind die Applikation und die partielle Programmierung nicht funktionsfähig, wenn die Option "Direkte IP-Verbindung verwenden, wenn möglich" aktiviert ist. Wenn die Option aktiviert ist, muss das Produkt neu gestartet werden, damit die Parameter berücksichtigt werden können.

##### 9.1.1. Prog. Modus an Gerätefront

Zusätzlich zur normalen Programmierertaste ⑥ ermöglicht das Gerät die Aktivierung des Programmiermodus an der Gerätefront, ohne die Schalttafelabdeckung zu öffnen. Der Programmiermodus kann durch gleichzeitiges Drücken der Tasten ③ und ⑨ aktiviert und deaktiviert werden.

Diese Funktion kann über den Parameter „Prog. Modus an Gerätefront“ ein- und ausgeschaltet werden. Die vertiefte Programmierertaste ⑥ (neben der Programmier-LED ①) ist immer aktiviert und wird von diesem Parameter nicht beeinflusst.

##### 9.1.2. Handbedienung am Gerät

Hierbei wird die Dauer des Handbedienungsmodus eingestellt. Bei Beendigung wird automatisch wieder der normale Betriebszustand ausgeführt.

#### 9.2. Routing (KNX -> IP)

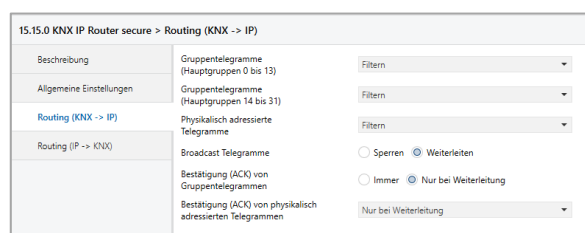


Figure 12 – Routing (KNX -> IP)

##### ■ Gruppentelegramme (Hauptgruppen 0 bis 13)

**Sperren:** Kein Gruppentelegramm dieser Hauptgruppen wird nach IP weitergeleitet.

**Weiterleiten:** Alle Gruppentelegramme dieser Hauptgruppen werden unabhängig von der Filtertabelle nach IP weitergeleitet. Diese Einstellung sollte nur zu Testzwecken dienen.

**Filtern:** Hier wird anhand der Filtertabelle geprüft, ob das empfangene Gruppentelegramm nach IP weitergeleitet wird.



## ETS Parameterdialog

### ■ Gruppentelegramme (Hauptgruppen 14 bis 31)

- Sperren:* Kein Gruppentelegramm der Hauptgruppen 14 bis 31 wird nach IP weitergeleitet.
- Weiterleiten:* Alle Gruppentelegramme der Hauptgruppen 14 bis 31 werden nach IP weitergeleitet.
- Filtern:* Hier wird anhand der Filtertabelle geprüft, ob das empfangene Gruppentelegramm nach IP weitergeleitet wird.

### ■ Physikalisch adressierte Telegramme

- Sperren:* Kein physikalisch adressiertes Telegramm wird nach IP weitergeleitet.
- Weiterleiten:* Alle physikalisch adressierten Telegramme werden nach IP weitergeleitet.
- Filtern:* Anhand der physikalischen Adresse wird geprüft, ob das empfangene physikalisch adressierte Telegramm nach IP weitergeleitet wird.

### ■ Broadcast Telegramme

- Sperren:* Kein empfangenes Broadcast Telegramm wird nach IP weitergeleitet.
- Weiterleiten:* Alle empfangenen Broadcast Telegramme werden nach IP weitergeleitet.

### ■ Bestätigung (ACK) von Gruppentelegrammen

- Immer:* Bei empfangenen Gruppentelegrammen (von KNX) wird immer ein Acknowledge erzeugt.
- Nur bei Weiterleitung:* Bei empfangenen Gruppentelegrammen (von KNX) wird ein Acknowledge nur bei Weiterleitung nach IP erzeugt.

### ■ Bestätigung (ACK) von physikalisch adressierten Telegrammen

- Immer:* Bei empfangenen physikalisch adressierten Telegrammen (von KNX) wird immer ein Acknowledge erzeugt.
- Nur bei Weiterleitung:* Bei empfangenen physikalisch adressierten Telegrammen (von KNX) wird ein Acknowledge nur bei Weiterleitung nach IP erzeugt..
- Antwort mit NACK::* Jedes empfangene physikalisch adressierte Telegramm (von KNX) wird mit NACK (Not Acknowledge) beantwortet d.h. es ist keine Kommunikation mit physikalisch adressierten Telegrammen auf der entsprechenden KNX Linie mehr möglich. Die Gruppen- Kommunikation (Gruppentelegramme) ist davon nicht betroffen. Diese Einstellung kann verwendet werden um Manipulationsversuchen vorzubeugen.

Bei Antwort mit NACK ist ein Zugriff auf das Gerät über KNX TP nicht mehr möglich. Die Parametrierung muss über IP erfolgen.

## 9.3. Routing (IP -> KNX)

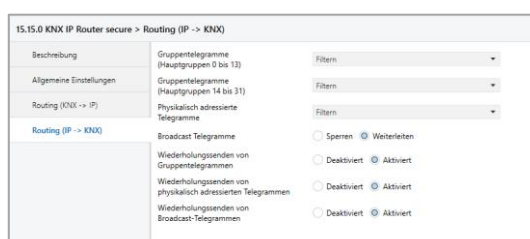


Figure 13 – Routing (IP -> KNX)

### ■ Gruppentelegramme (Hauptgruppen 0 bis 13)

- Sperrern:* Kein Gruppentelegramm dieser Hauptgruppen wird nach KNX weitergeleitet.
- Weiterleiten:* Alle Gruppentelegramme dieser Hauptgruppen werden unabhängig von der Filtertabelle nach KNX weitergeleitet. Diese Einstellung sollte nur zu Testzwecken dienen.
- Filtern:* Hier wird anhand der Filtertabelle geprüft, ob das empfangene Gruppentelegramm nach KNX weitergeleitet wird.

### ■ Gruppentelegramme (Hauptgruppen 14 bis 31)

- Sperrern:* Kein Gruppentelegramm der Hauptgruppen 14 bis 31 wird nach KNX weitergeleitet.
- Weiterleiten:* Alle Gruppentelegramme der Hauptgruppen 14 bis 31 werden nach KNX weitergeleitet.
- Filtern:* Hier wird anhand der Filtertabelle geprüft, ob das empfangene Gruppentelegramm nach IP weitergeleitet wird.

### ■ Physikalisch adressierte Telegramme

- Sperrern:* Kein physikalisch adressiertes Telegramm wird nach KNX weitergeleitet.
- Weiterleiten:* Alle physikalisch adressierten Telegramme werden nach KNX weitergeleitet.
- Filtern:* Anhand der physikalischen Adresse wird geprüft, ob das empfangene physikalisch adressierte Telegramm nach KNX weitergeleitet wird.

### ■ Broadcast Telegramme

- Sperrern:* Kein empfangenes Broadcast Telegramm wird nach KNX weitergeleitet.
- Weiterleiten:* Alle empfangenen Broadcast Telegramme werden nach KNX weitergeleitet.

### ■ Wiederholungssenden von Gruppentelegrammen

- Deaktiviert:* Das empfangene Gruppentelegramm wird im Fehlerfall nicht wiederholt auf den KNX Bus gesendet.
- Aktiviert:* Das empfangene Gruppentelegramm wird im Fehlerfall bis zu dreimal wiederholt.

### ■ Wiederholungssenden von physikalisch adressierten Telegrammen

- Deaktiviert:* Das empfangene physikalisch adressierte Telegramm wird im Fehlerfall nicht wiederholt auf den KNX Bus gesendet.
- Aktiviert:* Das empfangene physikalisch adressierte Telegramm wird im Fehlerfall bis zu dreimal wiederholt.

### ■ Wiederholungssenden von Broadcast Telegrammen

- Deaktiviert:* Das empfangene Broadcast Telegramm wird im Fehlerfall nicht wiederholt auf den KNX Bus gesendet.
- Aktiviert:* Das empfangene Broadcast Telegramm wird im Fehlerfall bis zu dreimal wiederholt.

## 10. Programmierung

Der KNX IP Router secure kann über verschiedene Wege von der ETS programmiert werden:

### 10.1. 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.

### 10.2. Über KNXnet/IP Tunneling

Hierbei ist keine zusätzliche Schnittstelle erforderlich. Die Programmierung über KNXnet/IP Tunneling 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.

### 10.3. Über KNXnet/IP Routing

Die Programmierung über KNXnet/IP Routing ist möglich, wenn das Gerät bereits eine gültige IP Konfiguration besitzt (z.B. über DHCP oder Auto IP). In der ETS erscheint die Routing Schnittstelle, wenn mindestens ein Gerät im Netzwerk sichtbar ist, das Routing unterstützt. Als Bezeichnung erscheint der Name der Netzwerkschnittstelle im PC. Wird Routing als Schnittstelle ausgewählt, erfolgt die Programmierung aus dem ETS Projekt heraus wie bei anderen Geräten auch. Das LAN wird in diesem Fall als KNX Medium ähnlich wie TP verwendet. Es ist kein zusätzliches Schnittstellengerät erforderlich.

### 10.4. Über direkte IP Verbindung

Während sowohl KNXnet/IP Tunneling als auch KNXnet/IP Routing 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.

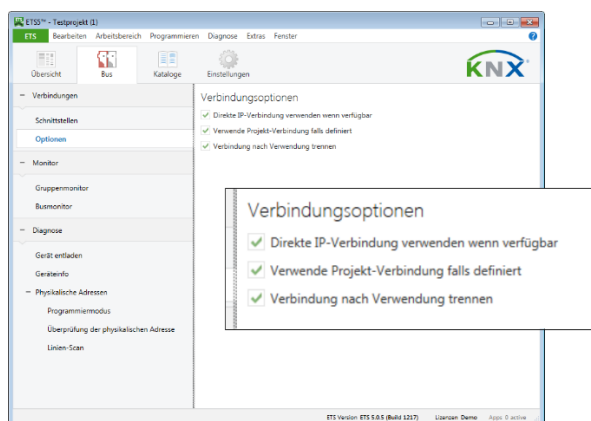


Figure 14 – Verbindungsoptionen



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

### 11. Fernzugriff

#### 11.1. Network Address Translation NAT

NAT (Network Address Translation) ist ein Verfahren, um externe IP-Adressen auf interne umzusetzen. Dies wird vor allem in Routern (z.B. DSL-Routern) verwendet.



##### WARNING

Bitte beachten Sie, dass der Fernzugriff über NAT ohne weitere Schutzmaßnahmen erhebliche Gefahren birgt. Durch die ungeschützte Portfreigabe wird ein allgemeiner Zugang in Ihr lokales IP Netzwerk und in Ihr KNX System möglich.

Jeder Internetnutzer weltweit kann den freigegebenen Port an Ihrer festen, öffentlichen IP Adresse finden und damit z.B. über die ETS Software auf Ihr KNX Netzwerk zugreifen. Wir raten dringend, den Zugang über NAT nur temporär zu Test- oder Diagnosezwecken zu öffnen und anschließend den Port umgehend wieder zu schließen, um Missbrauch zu verhindern.

Sollte der Fernzugriff über NAT realisiert werden, raten wir Ihnen dringend, nicht den Standard-Port 3671 in Richtung Internet anzugeben. Da es sich bei Port 3671 um den offiziellen Port für efcP – eFieldControl(EIBnet) der KNX Association handelt, kann dieser leichter von Unbefugten ermittelt werden. Bitte verwenden Sie einen Port aus dem nicht reservierten Bereich zwischen Port 50000 und Port 60000.

**Ein dauerhafter Fernzugriff sollte nur geschützt eingerichtet werden! Dazu empfehlen wir den Fernzugriff über VPN (Virtual Private Network). Die VPN Funktion ist in vielen DSL Routern bereits integriert.**

#### 11.2. Fernzugriff über ein VPN

Ein VPN ist eine Erweiterung privater Netzwerke. Über ein VPN lassen sich Fernzugriff (Site-To-End) und Kopplung privater Netzwerke (Site-To-Site) über das Internet realisieren.

##### Site-to-end

Mit einem Site-To-End VPN kann ein Zugriff auf ein internes Netz aufgebaut werden. Beispielsweise können sich so Mitarbeiter von außerhalb in das Netz ihrer Firma einwählen.

##### Site-to-site

Mit einem Site-To-Site VPN können private Netze untereinander gekoppelt werden. Beispielsweise erlaubt ein Site-To-Site VPN die Kopplung zweier entfernter Firmennetze.

Die IP-Schnittstelle wird nicht automatisch gefunden. Sie muss manuell konfiguriert werden.



Der Haken „Verbinden im NAT-Modus“ ist zwingend zu setzen. Die Verbindung wird dennoch nicht im NAT-Modus aufgebaut. Durch diese Aktivierung wird eine wichtige Initialisierung durchgeführt, die bedingt durch den IP-Aufsatz nötig ist.

### 11.3. Fernzugriff und KNX secure

Aus den verschiedenen Arten auf das Gerät zuzugreifen und der Möglichkeit KNX secure oder KNX unsecure zu benutzen, ergeben sich folgende Möglichkeiten.

	NAT	VPN
KNX unsecure	Warnung! ungeschützt	OK
KNX secure	OK	optimaler Schutz

Ein Fernzugriff über NAT und KNX unsecure ist vollkommen ungeschützt und sollte auf keinen Fall verwendet werden. Ein optimaler Schutz ergibt sich aus der gleichzeitigen Verwendung von KNX Security und VPN..

### 12. 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/>

Copyright 2008, Google Inc. All rights reserved.

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.



#### **WARNING**

- 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.



**Hager Electro SAS**  
132 Boulevard d'Europe  
BP3  
67210 OBERNAI CEDEX  
**[hager.com](http://hager.com)**