

Bedienungs- und Montageanleitung

KNX IP Router IPR500 KNX-S

(Art. # 095956)

Kompakter busversorgter Router zwischen LAN/Ethernet und KNX-Bus mit KNX Secure



KNX IP Router IPR500 KNX-S

Anwendung

Der kompakte KNX IP Router IPR500 KNX-S 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 Secure. 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 Secure 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 IPR500 KNX-S besitzt eine erweiterte Filtertabelle für Hauptgruppe 0..31 und kann bis zu 150 Telegramme zwischenspeichern. Die Spannungsversorgung erfolgt über den KNX Bus.

KNX Secure

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

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

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

KNX IP Secure 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 Secure erfolgt die Routing-Kommunikation ver-

schlüsselt. 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 Secure für Routing verwendet wird, müssen alle angeschlossenen KNX IP Geräte Secure unterstützen und entsprechend konfiguriert sein.

KNX IP Secure für die Interface Funktion

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

KNX Data Secure für das Gerät

Der KNX IP Router IPR500 KNX-S unterstützt auch KNX Data Secure, 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.

KNX Data Secure 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 Secure-Eigenschaften werden vom jeweiligen Empfänger geprüft.

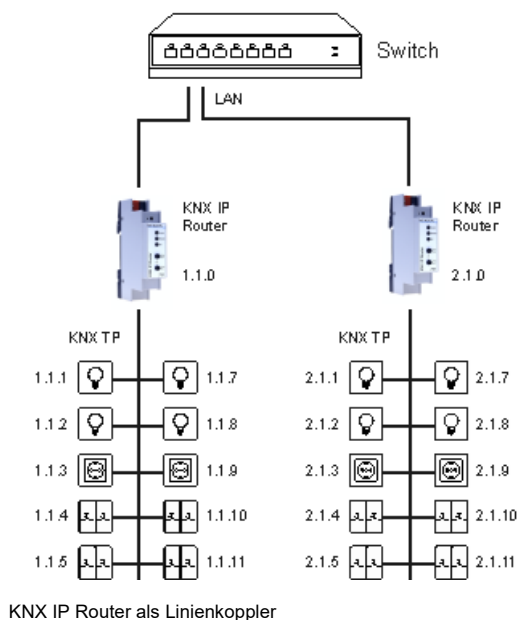
KNX Data Secure und KNX IP Secure können parallel eingesetzt werden. In diesem Fall würde zum Beispiel ein KNX Sensor ein mit KNX Data Secure verschlüsseltes Gruppentelegramm auf den Bus senden. Bei der Weiterleitung über KNX IP mit KNX IP Secure würde das verschlüsselte Telegramm so wie unverschlüsselte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

Koppler-Funktion (KNXnet/IP Routing)

Der KNX IP Router IPR500 KNX-S kann als Linien- bzw. Bereichskoppler arbeiten. In beiden Fällen wird das LAN (IP) als Backbone verwendet.

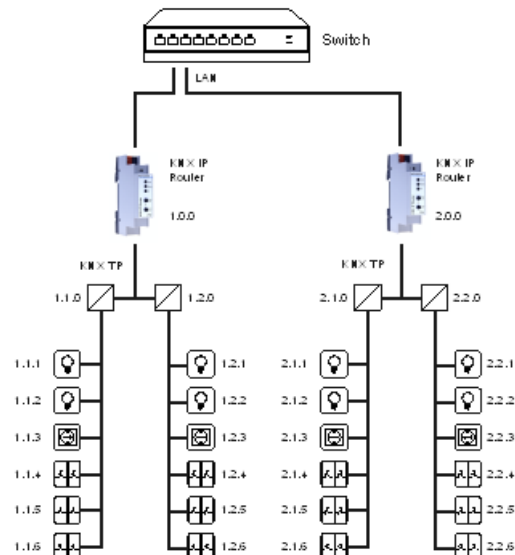
Die Einsatzmöglichkeiten des KNX IP Routers im Vergleich zur klassischen Topologie zeigt folgende Tabelle:

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



KNX IP Router als Linienkoppler

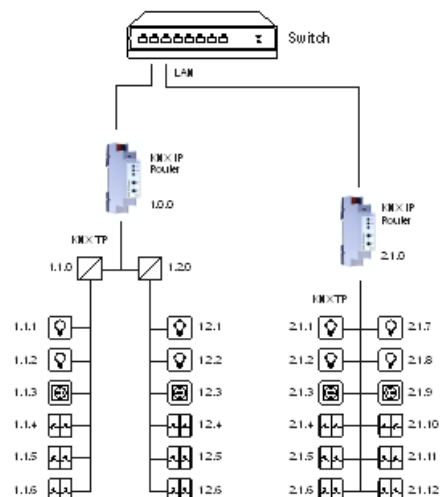
Die Vergabe der physikalischen Adresse des KNX IP Router IPR500 KNX-S entscheidet, ob das Gerät als Linien- oder als Bereichskoppler arbeitet. Entspricht die physikalische Adresse der Form x.y.0 (x, y: 1..15), funktioniert der Router als Linienkoppler. Hat die physikalische Adresse die Form x.0.0 (x: 1..15), handelt es sich um einen Bereichskoppler.



KNX IP Router als Bereichskoppler

i Wird der KNX IP Router IPR500 KNX-S 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 IPR500 KNX-S 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.



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

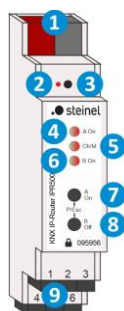
diese im Router zwischengespeichert werden, um Telegrammverluste zu vermeiden. Hierzu besitzt der KNX IP Router IPR500 KNX-S Speicherplatz für 150 Telegramme (von IP nach KNX).

Funktion als Buszugriff (KNXnet/IP Tunneling)

Der KNX IP Router IPR500 KNX-S 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.

Installation und Inbetriebnahme

Der KNX IP Router IPR500 KNX-S wird auf einer Hutschiene montiert und hat einen Platzbedarf von 1 TE (18 mm). Er besitzt folgende Bedienelemente und Anzeigen:



- 1 KNX Bus Anschluss
- 2 Programmier-LED
- 3 Taster f. Programmiermodus
- 4 KNX LED (mehrfarbig)
- 5 Mode LED (mehrfarbig)
- 6 IP LED (mehrfarbig)
- 7 Taster Pass GAs
- 8 Taster Pass IAs
- 9 LAN Buchse

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.

Handbedienung und 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

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 7 kann das Weiterleiten gruppen-adressierter Telegramme aktiviert werden.

Mit dem Taster Pass IAs 8 kann das Weiterleiten physikalisch adressierter Telegramme aktiviert werden.

Dies wird jeweils mit einfachem Blitzen der Mode LED 5 (orange) angezeigt. Werden beide Modi gleichzeitig ausgewählt, so blitzt die Mode LED 5 zweifach.

Durch erneutes Drücken der Taster Pass GAs 7 und Pass IAs 8 können diese Einstellungen beliebig an- und abgewählt werden. Über die Escape-Funktion (Esc) kann durch gleichzeitiges Betätigen der Taster Pass GAs 7 und Pass IAs 8 die Handbedienung 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 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.

Werkseinstellungen

Ab Werk ist folgende Konfiguration voreingestellt:

Physikalische Adresse des Gerätes:	15.15.0
Konfigurierte KNXnet/IP Tunneling Verbindung:	1
Physikalische Adr. der Tunneling Verbindung:	15.15.240
IP Adressen Vergabe:	DHCP
Initialer Schlüssel (FDSK)	aktiv
Secure Modus	nicht aktiv

Zurücksetzen auf Werkseinstellungen

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

- KNX Bus Anschluss ① vom Gerät trennen
- KNX Programmieraster ③ drücken und gedrückt halten
- KNX Bus Anschluss ① zum Gerät wieder herstellen
- Programmieraster ③ mindesten noch 6 Sekunden gedrückt halten
- Ein kurzes Aufblinker aller LEDs (②④⑤⑥) signalisiert die erfolgreiche Rücksetzung auf Werkseinstellung.

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

Der KNX IP Router IPR500 KNX-S 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 zusätzlichen Adressen. Jede Adresse ist einer Verbindung zugeordnet. Somit können Antworttelegramme eindeutig zum jeweiligen Client weitergeleitet werden.

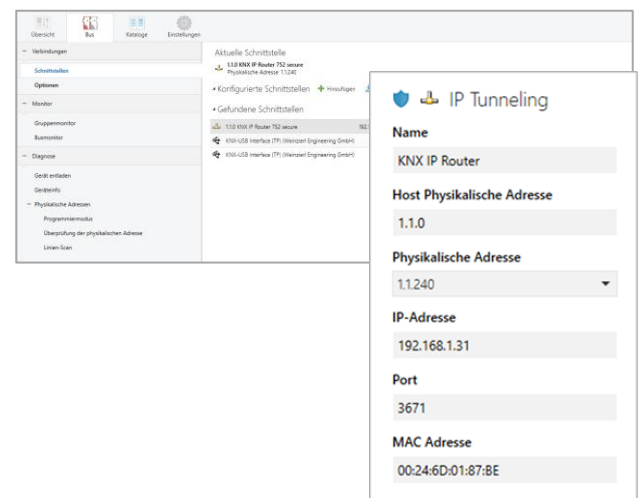
Die zusätzlichen physikalischen Adressen müssen aus dem Adressbereich der Bus-Linie sein, in der sich der KNX IP Router

befindet und dürfen nicht von einem anderen Gerät verwendet werden.

Beispiel:

Geräteadresse	1.1.0	(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.

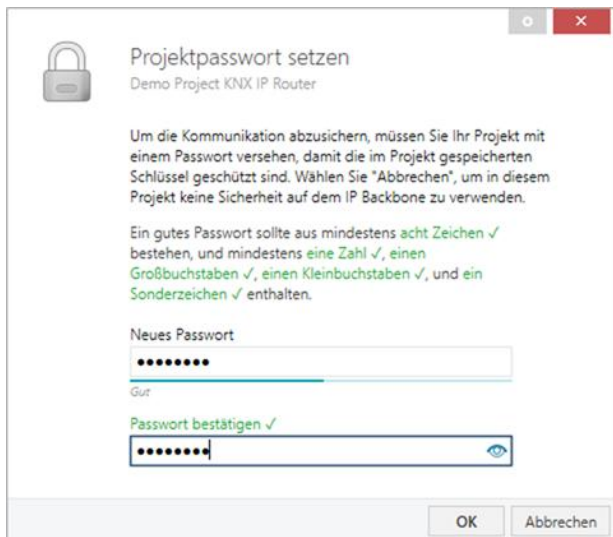


Die physikalische KNX Geräteadresse sowie die physikalischen KNX Adressen für die zusätzlichen Tunneling Verbindungen können innerhalb des ETS Projekts geändert werden, nachdem das Gerät dem Projekt hinzugefügt wurde.

ETS Datenbank

Die ETS Datenbank (ab ETS 5.7) kann auf der Produkt Website KNX IP Router IPR500 KNX-S (www.steinell.de) oder im KNX Online-Katalog der ETS heruntergeladen werden.

Wird das erste Produkt mit KNX Secure 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 Secure, 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).



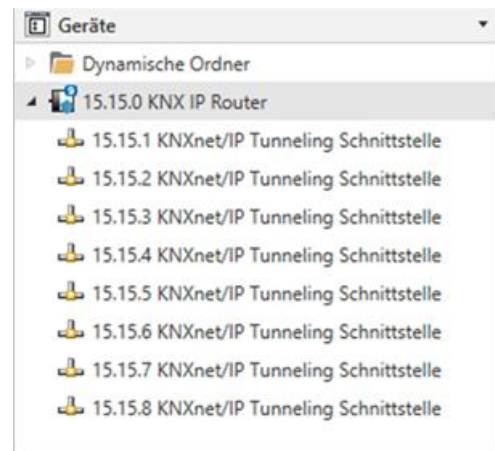
Das Zertifikat ist als Text auf dem Gerät aufgedruckt. Es kann auch bequem über eine Webcam vom aufgedruckten QR-Code abgescannt werden.

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.

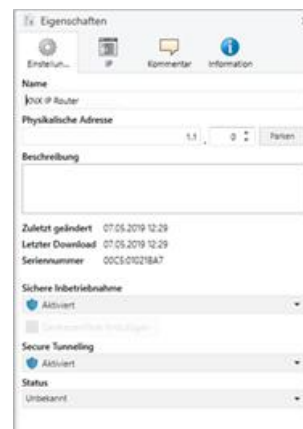


Um die einzelnen Adressen zu ändern, ist der entsprechende Eintrag in der Liste zu markieren und im Textfeld die gewünschte Adresse einzugeben. Sollte der Rahmen des Textfeldes, nach Eingabe, seine Farbe auf Rot wechseln, weist dies darauf hin, dass die eingegebene Adresse bereits verwendet wird.



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

Durch Markieren des KNX IP Router IPR500 KNX-S 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 IPR500 KNX-S 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“ spezifische Optionen des KNX IP Router IPR500 KNX-S 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 KNX IP Router IPR500 KNX-S 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 DSL-Router 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 IPR500 KNX-S zugegriffen werden.

IP-Adresse des PCs: 192.168.1.30

Subnetz des PCs: 255.255.255.0

Der KNX IP Router IPR500 KNX-S 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

Fernzugriff

Über den KNX IP Router IPR500 KNX-S ist ein Fernzugriff über das Internet möglich. Weitere Details befinden sich im Dokument „Fernzugriff mit der ETS“ auf www.steinle.de

ETS Parameterdialog

Mit der ETS können folgende Parameter gesetzt werden.

Allgemeine Einstellungen

Prog. Modus an Gerätefront

Zusätzlich zur normalen Programmieraste 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 Programmieraste ③ (neben der Programmier-LED ②) ist immer aktiviert und wird von diesem Parameter nicht beeinflusst.

Handbedienung am Gerät

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

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.

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.

Routing (IP -> KNX)

15.15.0 KNX IP Router		> Routing (IP -> KNX)	
Beschreibung	Gruppentelegramme (Hauptgruppen 0 bis 13)	Filtern	
Allgemeine Einstellungen	Gruppentelegramme (Hauptgruppen 14 bis 31)	Filtern	
Routing (KNX -> IP)	Physikalisch adressierte Telegramme	Filtern	
Routing (IP -> KNX)	Broadcast Telegramme	☐ Sperren ☒ Weiterleiten	
	Wiederholungssenden von Gruppentelegrammen	☐ Deaktiviert ☒ Aktiviert	
	Wiederholungssenden von physikalisch adressierten Telegrammen	☐ Deaktiviert ☒ Aktiviert	
	Wiederholungssenden von Broadcast-Telegrammen	☐ Deaktiviert ☒ Aktiviert	

Gruppentelegramme (Hauptgruppen 0 bis 13)

- Sperren:** 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)

- Sperren:** 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

- Sperren:** 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

- Sperren:** 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.

Programmierung

Der KNX IP Router IPR500 KNX-S 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 Tunneling

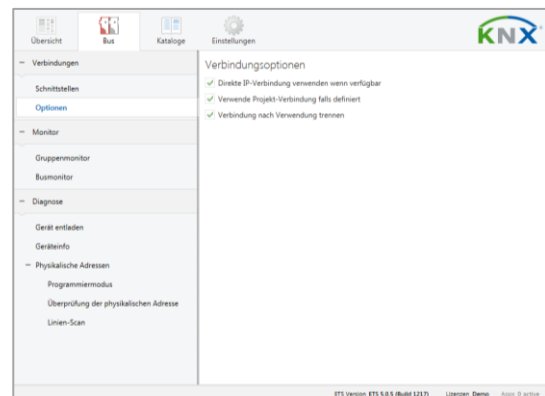
Hierbei ist keine zusätzliche Schnittstelle erforderlich. Die Programmierung über KNXnet/IP Tunneling ist möglich, wenn das Gerät bereits eine gültige IP Konfiguration besitzt (z.B. über DHCP). In diesem Fall wird das Gerät bei den Schnittstellen in der ETS angezeigt und muss ausgewählt werden. Der Download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

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.

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.



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

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.



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.



Steinel GmbH
Dieselstrasse 80-84
33442 Herzebrock-Clarholz
Deutschland
Tel: +49 5245 448 0
www.steinell.de
product@steinell.de

15.01.2026

Operation and installation manual

KNX IP Router IPR500 KNX-S

(Art. # 095956)

Compact bus powered Router between LAN/Ethernet and KNX bus with KNX secure



KNX IP Router IPR500 KNX-S

Application

The compact KNX IP Router IPR500 KNX-S enables the forwarding of telegrams between different lines via a LAN (IP) as a fast backbone. The device also serves as a programming interface between a PC and the KNX bus (e.g. for ETS programming).

The device supports KNX Secure. The option can be activated in the ETS. As a secure router, the device enables the coupling of unsecured communication on a KNX TP line with a secure IP backbone.

KNX Secure also prevents unauthorised access to the interface function (tunneling).

The IP address can be assigned via DHCP or via the ETS configuration. The device operates according to the KNXnet/IP specification using core, device management, tunneling and routing.

The KNX IP Router IPR500 KNX-S has an extended filter table for main groups 0..31 and can buffer up to 150 telegrams. Power is supplied via the KNX bus.

KNX Secure

The KNX standard was extended by KNX Secure to protect KNX installations from unauthorized access. KNX Secure reliably prevents the monitoring of communication as well as the manipulation of the system.

The specification for KNX Secure distinguishes between KNX IP Secure and KNX Data Secure. KNX IP Secure protects the communication over IP while on KNX TP the communication remains unencrypted. Thus KNX IP Secure can also be used in existing KNX systems and with non-secure KNX TP devices.

KNX Data Secure describes the encryption at telegram level. This means that the telegrams on the twisted pair bus are also encrypted.

KNX IP Secure for the router function

The coupling of individual KNX TP lines via IP is referred as KNX IP routing. Communication between all connected KNX IP routers takes place via UDP multicast.

Routing communication is encrypted with KNX IP Secure. This means that only IP devices that know the key can decrypt the communication and send valid telegrams. A time stamp in the routing telegram ensures that no previously recorded telegrams can be replayed. This prevents the so-called replay attack.

The key for the routing communication is reassigned by ETS for each installation. If KNX IP Secure is used for routing, all connected KNX IP devices must support secure and be configured accordingly.

KNX IP Secure for the interface function

When using a KNX IP router as an interface to the bus, access to the installation is possible without secure for all devices that have access to the IP network. With KNX Secure a password is required. A secure connection is already established for the transmission of the password. All communication via IP is encrypted and secured.

KNX Data Secure for the device

The KNX IP Router IPR500 KNX-S also supports KNX Data Secure to protect the device from unauthorised access from the KNX bus. If the KNX IP router is programmed via the KNX bus, this is done with encrypted telegrams.



Encrypted telegrams are longer than the previously used unencrypted ones. For secure programming via the bus, it is therefore necessary that the interface used (e.g. USB) and any intermediate line couplers support the so-called KNX long frames.

KNX Data Secure for group telegrams

Telegrams from the bus that do not address the KNX IP Router as a device are forwarded or blocked according to the filter settings (parameters and filter table). It does not matter whether the telegrams are unencrypted or encrypted. Forwarding takes place exclusively on the basis of the destination address. The secure properties are checked by the respective recipient.

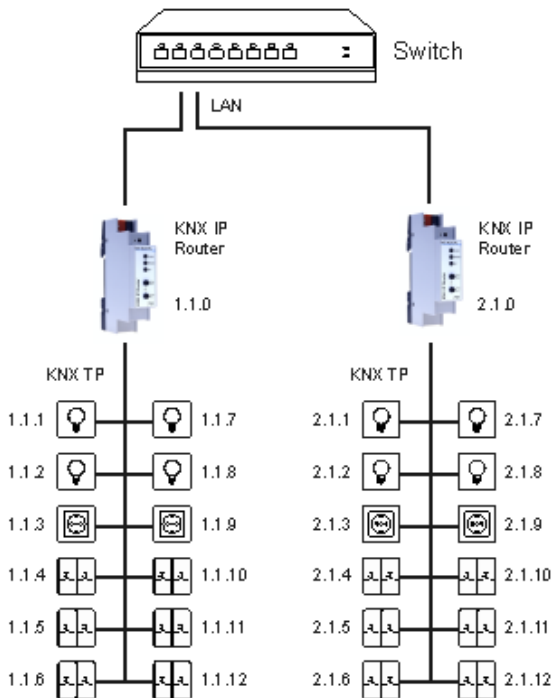
KNX Data Secure and KNX IP Secure can be used in parallel. In this case, for example, a KNX sensor would send a group telegram encrypted with KNX Data Secure to the bus. When forwarding via KNX IP with KNX IP Secure, the encrypted telegram would be encrypted again just like unencrypted ones. All participants on the KNX IP level that support KNX IP Secure can decode the IP encryption, but not the data secure. Thus the telegram from the other KNX IP routers is again transmitted to the target line(s) with KNX Data Secure. Only devices that know the key used for data secure can interpret the telegram.

Coupler function (KNXnet/IP Routing)

The KNX IP Router IPR500 KNX-S operates as a line or backbone coupler. In both cases, the LAN (IP) is used as a backbone.

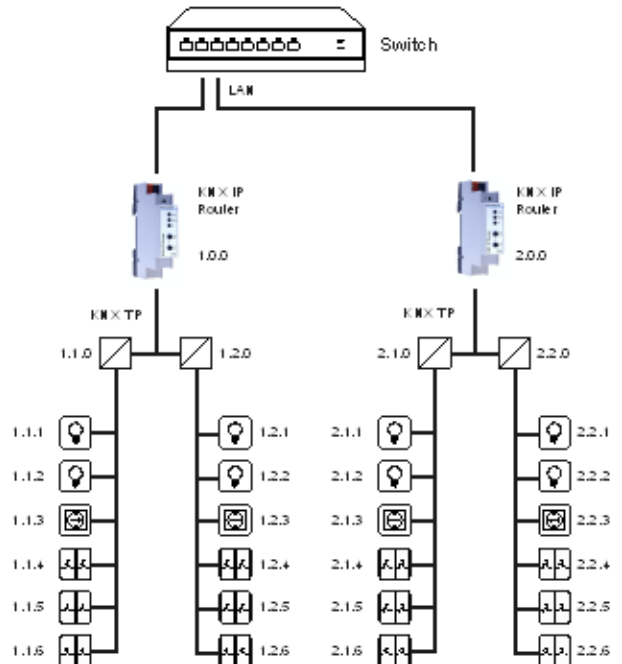
The following table shows the application possibilities of the KNX IP Router compared to the classic topology:

	Classical Topology (without IP)	IP coupling of areas (IP area coupl.)	IP coupling of lines (IP line coupler)
Area (Backbone)	TP	IP	IP
Coupling	KNX Line Coupler (max. 15 Pcs.)	KNX IP Router (max. 15 Pcs.)	Directly via LAN Switch
Main line	TP	TP	IP
Coupling	KNX Line Coupler (max. 15x15 Pcs.)	KNX Line Coupler (max. 15x15 Pcs.)	KNX IP Router (max. 225 Pcs..)
Line	TP	TP	TP



KNX IP Router as line coupler

The individual address assigned to the KNX IP Router IPR500 KNX-S determines whether the device operates as a line or area coupler. If the individual address is in the form of x.y.0 (x, y: 1..15), the router operates as a line coupler. If it is in the form of x.0.0 (x: 1..15), the router acts as a backbone coupler.



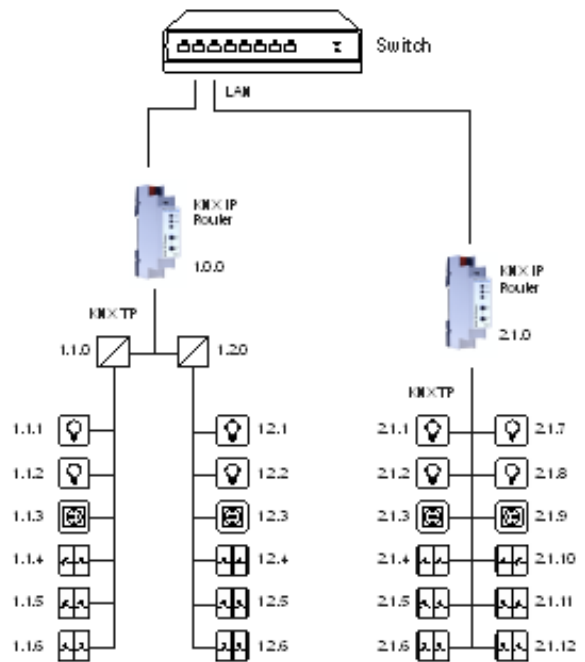
KNX IP Router as area coupler



If the KNX IP Router IPR500 KNX-S is used as a area coupler (x.0.0), there must not be a KNX IP Router in the topology beneath it. For example, if a KNX IP Router has the individual address 1.0.0, there must be no KNX IP Router with the address 1.1.0.



If the KNX IP Router IPR500 KNX-S is used as a line coupler (x.y.0), there must not be a KNX IP Router in the topology above it. For example, if a KNX IP Router has the individual address 1.1.0, there must be no KNX IP Router with the address 1.0.0.



KNX IP Router as area and line coupler

The KNX IP Router has a filter table and thus contributes to reducing the bus load. The filter table (8kB) supports the extended group address range (main groups 0..31) and is automatically generated by the ETS.

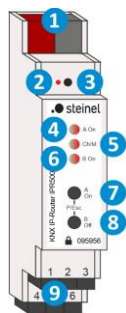
Because of the speed difference between the Ethernet (10/100 MBit/s) and KNX TP (9.6 kBit/s), a far greater number of telegrams can be transmitted on IP. If several consecutive telegrams are transmitted for the same line, they must be buffered in the router to avoid telegram loss. The KNX IP Router IPR500 KNX-S has a memory for 150 telegrams (from IP to KNX).

Bus access function (KNXnet/IP Tunneling)

The KNX IP Router IPR500 KNX-S can be used as an interface to KNX. The KNX bus can be accessed from any point in the LAN. For this purpose, an additional individual address must be assigned. This is described in the following sections.

Installation and Connection

The KNX IP Router IPR500 KNX-S is designed for installation on a DIN rail with a width of 1 unit (18mm). It features the following controls and displays:



- 1 KNX bus connector
- 2 Programming LED
- 3 Button f. programming mode
- 4 KNX LED (multicolor)
- 5 Mode LED (multicolor)
- 6 IP LED (multicolor)
- 7 Button Pass GAs
- 8 Button Pass IAs
- 9 LAN Connector

The KNX IP Router IPR500 KNX-S is powered by the KNX bus. An external power supply is not necessary.

i The device is not working without bus power.

KNX Programming mode

The KNX programming mode is activated/deactivated either by pressing the flushed KNX programming button 3 or by simultaneously pressing the buttons 7 and 8.

Status display

The KNX LED 4 lights up green if the device is successfully powered by the KNX bus. This LED indicates telegram traffic on the KNX bus by flickering.

Communication failures (e.g. repetitions of telegrams or telegram fragments) are indicated by a short change of the LED color to red.

Overview of the different indications of the KNX LED 4:

LED Status	Meaning
LED lights green	KNX bus voltage available.
LED flickers green	Telegram traffic on the KNX bus
LED shortly red	Communication failures on the KNX bus

The IP LED 6 lights up when an Ethernet link is active. This LED is green if the device has valid IP settings (IP address, Sub net and Gateway). With invalid or nonexistent IP settings the LED is red. This is also the case if e.g. the device has not yet received the IP settings by a DHCP server.

This LED indicates IP telegram traffic by flickering.

Overview of the different indications of the IP LED 6:

LED Status	Meaning
LED lights green	The device has an active Ethernet link and valid IP settings.
LED lights red	The device has an active Ethernet link and invalid IP settings or not yet received the IP settings by a DHCP server.
LED flickers green	IP telegram traffic

For testing purposes (for example, during commissioning) the configured routing settings (filter or block) can be bypassed via manual operation.

With the button Pass GAs 7 the forwarding of group addressed telegrams can be activated.

With the button Pass IAs 8 the forwarding of individually addressed telegrams can be activated.

This is visualized with a single flash of the Mode LED 5 (orange). If both modes are activated the Mode LED 5 flashes two times.

Pressing button Pass GAs 7 or button Pass IAs 8 again these settings can be selected and deselected on demand. Via the Escape function (Esc) the manual operation can be stopped by simultaneously pressing the buttons Pass GAs 7 and Pass IAs 8.

If neither programming mode nor manual mode are active the LED 5 can visualize configuration errors.

Overview of the different indications of the Mode LED 5:

LED Status	Meaning
LED lights green	Device is working in standard operation mode.
LED light red	Programming mode is active
LED flashes 1x orange	Programming mode is not active. Manual operation is active. Forwarding IA or GA
LED flashes 2x orange	Programming mode is not active. Manual operation is active. Forwarding IA and GA
LED flashes red	Programming mode is not active. Manual operation is not active. The device is not properly loaded e.g. after an interrupted download.

Factory default settings

The following configuration is set by factory default:

Individual device address:	15.15.0
Number of configured KNXnet/IP tunneling con.:	1
Individual address of tunneling con.:	15.15.240
IP address assignment:	DHCP
Initial Key (FDSK)	active
Secure Modus	not active

Reset to factory device settings

It is possible to reset the device to its factory settings:

- Disconnect the KNX Bus connector ① from device
- Press the KNX programming button ③ and keep it pressed down
- Reconnect the KNX Bus connector ① of device
- Keep the KNX programming button ③ pressed for at least another 6 seconds
- A short flashing of all LEDs (② ④ ⑤ ⑥) visualizes the successful reset of the device to factory default settings.

Interface settings with ETS

Within the ETS KNX interfaces can be selected and set up via the ETS menu "Bus Interfaces".

The ETS can access configured KNX IP Routers even without a database entry. If the setup of the KNX IP Router does not comply with the conditions of the KNX installation it must be configured via an ETS project. See the ETS database section for more information.

As factory default the assignment of the IP address is set to "automatically via DHCP" and thus no further settings are necessary. To use this feature a DHCP server on the LAN must exist (e.g. many DSL routers have an integrated DHCP server).

After connecting the KNX IP Router to the LAN and the KNX bus, it should automatically appear in the ETS within the menu "Bus" under "Discovered interfaces".

By clicking on the discovered interface it is selected as the current interface. On the right side of the ETS window all specific information and options of the connection appear.

The indicated device name and the "Host Individual Address" (individual address of the device) can be changed within your ETS project then.

Like all programmable KNX devices the KNX IP Router IPR500 KNX-S has an individual address which can be used to access the device. This is used, for example, of the ETS when downloading to the KNX IP Router via the bus.

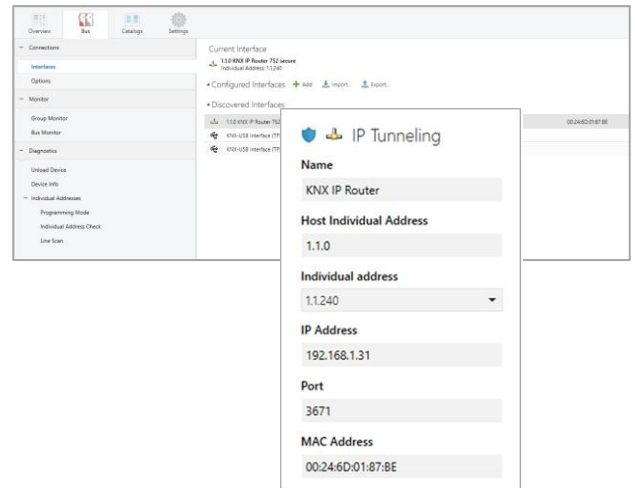
For the interface function the device contains additional individual addresses that can be set in the ETS. When a client (e.g. ETS) sends via the KNX IP Router telegrams to the bus, they contain a sender address as one from the additional addresses. Each address is associated with a connection. Thus response telegrams can be clearly transmitted to the respective client.

The additional individual addresses must be selected from the address range of the bus line in which the interface is installed and may not be used by another device.

Example:

Device address	1.1.0	(address within ETS topology)
Connection 1	1.1.240	(1. additional address)
Connection 2	1.1.241	(2. additional address)
Connection 3	1.1.242	(3. additional address)
Connection 4	1.1.243	(4. additional address)
Connection 5	1.1.244	(5. additional address)
Connection 6	1.1.245	(6. additional address)
Connection 7	1.1.246	(7. additional address)
Connection 8	1.1.247	(8. additional address)

The section "Individual Address" enables you to select the individual KNX address of the currently used KNXnet/IP Tunneling connection.

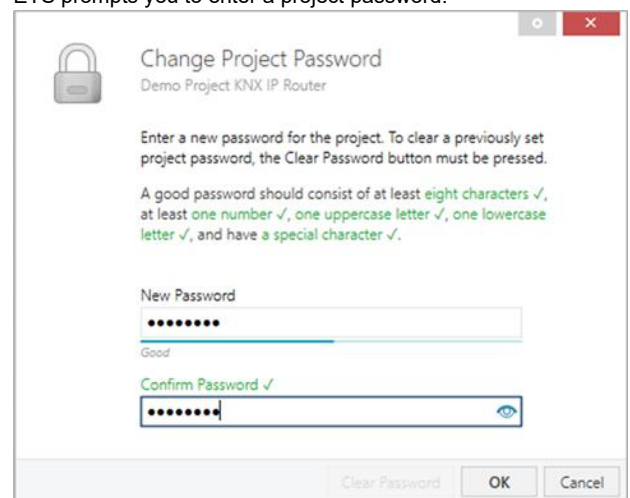


The individual KNX device address and the individual KNX addresses for additional tunneling connections can be changed within the ETS project, after the device has been added to the project.

ETS database

The ETS database (ETS 5.7 or higher) can be downloaded from the product website of the KNX IP Router IPR500 KNX-S (www.steinell.de) or via the KNX online catalogue.

If the first product is inserted into a project with KNX Secure, the ETS prompts you to enter a project password.



This password protects the ETS project from unauthorized access. This password is not a key that is used for KNX communication. The entry of the password can be bypassed with "Cancel", but this is not recommended for secure reasons.

ETS requires a device certificate for each device with KNX Secure that is created in the ETS. This certificate contains the serial number of the device as well as an intangible key (FDSK = Factory Default Setup Key).



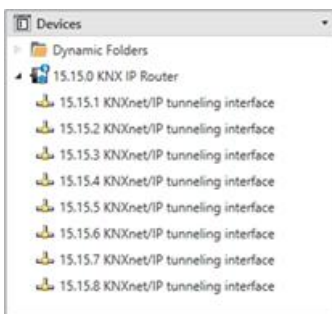
The certificate is printed as text on the device. It can also be conveniently scanned from the printed QR code via a webcam.

The list of all device certificates can be managed in the ETS Overview - Projects - Secure window.

This initial key is required to safely put a device into operation from the start. Even if the ETS download is recorded by a third party, the third party has no access to the secured devices afterwards. During the first secure download, the initial key is replaced by the ETS with a new key that is generated individually for each device. This prevents persons or devices who may know the initial key from accessing the device. The initial key is only reactivated after a master reset.

The serial number in the certificate enables the ETS to assign the correct key to a device during a download.

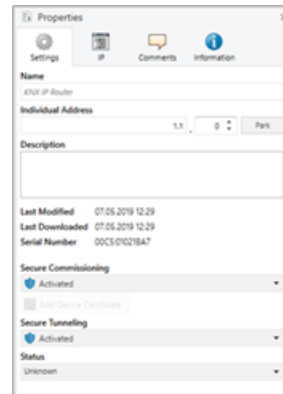
In the ETS, some settings are displayed in addition to the parameter dialog in the properties dialog (at the edge of the screen). The IP settings can be made here. The additional addresses for the interface connections are displayed in the topology view.



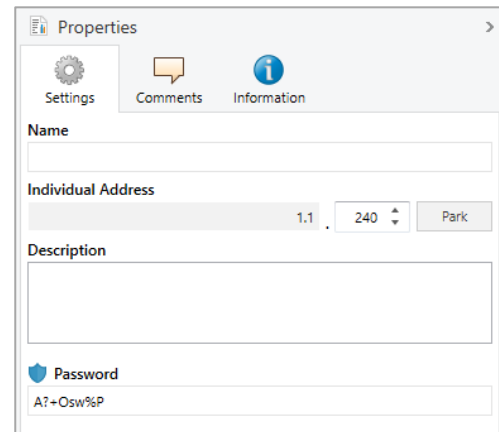
Each individual KNX address can be changed by clicking on the list entry and typing in the desired address into the "Individual Address" text-field. If the text-field frame switches to color red after entering the address, the address is already taken within your ETS project.

i Make sure that none of the addresses above are already present in your KNX installation.

By clicking on the KNX IP Router IPR500 KNX-S device entry within your ETS projects topology view, an information column 'Properties' will appear on the right side of the ETS window. Within the 'Settings' overview, you can change the name of the device.



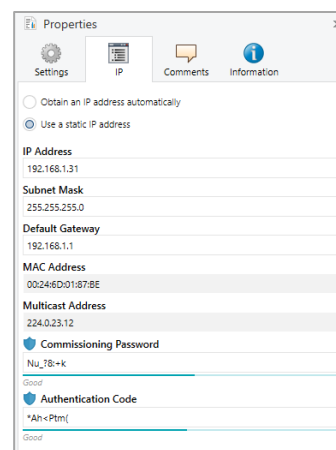
If secure tunneling is activated, a unique password will be created automatically for each tunnel. These passwords can be displayed under the 'Settings' overview, when a tunnel is selected.



Within the "IP" overview the IP network specific options of the KNX IP Router IPR500 KNX-S can be changed.

By changing "obtain an IP address automatically (via DHCP)" to "Use a static IP address" (static IP address) the IP address, subnet mask, and default gateway can be set freely.

i All changes in the properties menu become effective only after a successful application download.



IP address

Here the IP address of the KNX IP Router IPR500 KNX-S can be entered. This is used to address the device via the IP network (LAN). The IP addressing should be coordinated with the administrator of the network.

Subnet mask

Enter the subnet mask here. The device uses the values entered in this mask to determine whether there is a communication partner in the local network. If there is no partner in the local network, the device will not send the telegrams directly to the partner but to the gateway that routes the telegram.

Default gateway

Enter the IP address of the gateway here, e.g. the DSL router of the installation.

Routing Multicast Address

This address is used for routing telegrams on IP. The multicast IP address 224.0.23.12 was reserved (KNXnet/IP) at the IANA (Internet Assigned Numbers Authority) for this purpose. If a different multicast IP address is required, it must be within the range of 239.0.0.0 to 239.255.255.255.

Example of assigning IP addresses

A PC is to be used to access the KNX IP Router 752 *secure*.

IP address of the PC: 192.168.1.30

Subnet of the PC: 255.255.255.0

The KNX IP Router IPR500 KNX-S is located in the same LAN, i.e. it uses the same subnet. The subnet constrains the IP addresses that can be assigned. In this example, the IP address of the KNX IP Router must be 192.168.1.xx, where xx can be a number from 1 to 254 (with the exception of 30, which is already taken by the client PC). It must be ensured that no IP addresses are assigned twice.

IP address of the KNX IP Router 192.168.1.31

Subnet of the KNX IP Router: 255.255.255.0

Remote access

Remote access via Internet is possible with the KNX IP Router 752 *secure*. More details can be found in the document "Remote access with the ETS" at www.weinzierl.de

ETS parameter dialogue

The following parameters can be set using the ETS.

General settings

15.15.0 KNX IP Router > General settings	
Description	Note: For device name and IP settings see dialog "Properties"
General settings	Prog. mode on device front ☐ Disabled ☒ Enabled
Routing (KNX -> IP)	Manual operation on device Enabled without time limit
Routing (IP -> KNX)	

Prog. mode on device front

In addition to the normal programming button ③ the device allows activating the programming mode on the device front without opening the switchboard cover. The programming mode

can be activated and deactivated via pressing simultaneously both buttons ⑦ and ⑧.

This feature can be enabled and disabled via the parameter "Prog. mode on device front". The recessed programming button ③ (next to the Programming LED ②) is always enabled and not influenced by this parameter.

Manual operation on device

This parameter sets the duration of the manual mode. Upon completion the normal display mode is restored.

Routing (KNX -> IP)

15.15.0 KNX IP Router > Routing (KNX -> IP)	
Description	Group telegrams (main groups 0 to 13) Filter
General settings	Group telegrams (main groups 14 to 31) Filter
Routing (KNX -> IP)	Individual addressed telegrams Filter
Routing (IP -> KNX)	Broadcast telegrams ☐ Block ☒ Route
	Acknowledge (ACK) of group telegrams ☐ Always ☒ Only if routed
	Acknowledge (ACK) of individual addressed telegrams Only if routed

Group telegrams (main group 0 to 13)

Block: No group telegrams of this main group are routed to IP.

Route: All group telegrams of this main group are routed to IP independent of the filter table. This setting is for test purposes only.

Filter: The filter table is used to check whether or not the received group telegram should be routed to IP.

Group telegrams (main group 14 to 31)

Block: No group telegrams of main groups 14 to 31 are routed to IP.

Route: All group telegrams of main groups 14 to 31 are routed to IP.

Filter: The filter table is used to check whether or not the received group telegram should be routed to IP.

Individually addressed telegrams

Block: No individually addressed telegrams are routed to IP.

Route: All individually addressed telegrams are routed to IP.

Filter: The individual address is used to check whether the received individually addressed telegram should be routed to IP.

Broadcast telegrams

Block: No received broadcast telegrams are routed to IP.

Route: All received broadcast telegrams are routed to IP.

Acknowledge (ACK) of group telegrams

Always: A acknowledge is generated for every received group telegram (from KNX).

Only if routed: A acknowledge is only generated for received group telegrams (from KNX) if they are routed to IP.

Acknowledge (ACK) of individually addressed telegrams

Always: A acknowledge is generated for every received individual addressed telegram (from KNX).

Only if routed: A acknowledge is only generated for received individually addressed group telegrams (from KNX) if they are routed to IP.

Answer with NACK: Every received individually addressed telegram (from KNX) is responded to with NACK (Not acknowledge). This means that communication with individually addressed telegrams on the corresponding KNX line is not possible. Group communication (group telegrams) is not affected. This setting can be used to block attempts at manipulation.



When using "Answer with NACK" an access to the device via KNX TP is no longer possible. The configuration must be performed via IP.

Routing (IP -> KNX)

Group telegrams (main group 0 to 13)

Block: No group telegrams of these main groups are routed to KNX.

Route: All group telegrams of this main group are routed to KNXG independent of the filter table. This setting is used for testing purposes only.

Filter: The filter table is used to check whether the received group telegram should be routed to KNX.

Group telegrams (main group 14 to 31)

Block: No group telegrams of main groups 14 to 31 are routed to KNX.

Route: All group telegrams of the main groups 14 to 31 are routed to KNX.

Filter: The filter table is used to check whether the received group telegram should be routed to KNX.

Individually addressed telegrams

Block: No individually addressed telegrams are routed to KNX.

Route: All individually addressed telegrams are routed to KNX.

Filter: The individual address is used to check whether the received individually addressed telegram should be routed to KNX.

Broadcast telegrams

Block: No received broadcast telegrams are routed to KNX.

Route: All received broadcast telegrams are routed to KNX.

Repetition of group telegrams

Disabled: The received group telegram is not resent to KNX in case of a fault.

Enabled: The received group telegram is resent up to three times in case of a fault.

Repetition of individually addressed telegrams

Disabled: The received individually addressed telegram is not resent to KNX in case of a fault.

Enabled: The received individually addressed telegram is resent up to three times in case of a fault.

Repetition of broadcast telegrams

Disabled: The received broadcast telegram is not resent to KNX in case of a fault.

Enabled: The received broadcast telegram is resent up to three times in case of a fault.

Programming

The KNX IP Router IPR500 KNX-S can be programmed in different ways by the ETS:

Via KNX Bus

The device only needs to be connected to the KNX bus. The ETS requires an additional interface (for example, USB) to have access to the bus. Via this way both the individual address and the entire application including IP configuration can be programmed. Programming via the bus is recommended if no IP connection can be established.

Via KNXnet/IP Tunneling

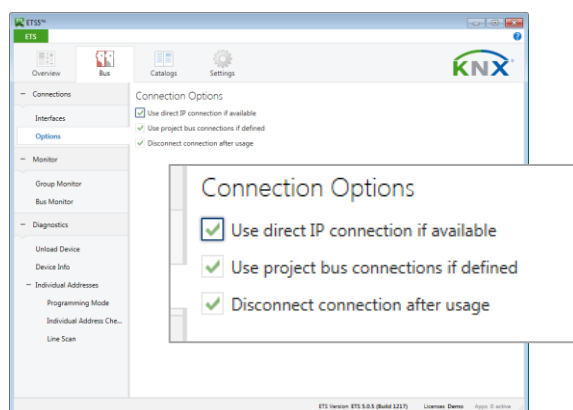
No additional interface is required. Programming via KNXnet/IP Tunneling is possible if the device already has a valid IP configuration (e.g. via DHCP). In this case the device is displayed in the interface configuration of the ETS and must be selected. The download is executed via the ETS project as with many other devices.

Via KNXnet/IP Routing

Programming via KNXnet/IP Routing is possible if the device already has a valid IP configuration (e.g. by using DHCP or Auto IP). In the ETS, the routing interface appears if at least one device on the network which supports routing is available. The name of the network interface appears in the PC as description. If routing is selected as interface, the programming done from the ETS project as like with other devices. In this case LAN is used as a KNX medium like TP. There is no additional interface device required.

Via direct IP connection

While KNXnet/IP Tunneling and KNXnet/IP Routing is limited to the speed of KNX TP the device can be loaded via a direct IP connection at high speed. The direct IP connection is possible if the device already has a valid IP configuration as well as an individual address. To do this select "Use direct IP connection if available" in the ETS menu "Bus – Connections - Options". The download is then directly performed in the device and is not visible in the ETS group monitor.



Due to the significantly shorter transmission times it is recommended to perform downloads via IP.

Open Source Licenses

This product contains open source software license:
curve25519-donna: Curve25519 elliptic curve, public key function

Source: <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

- The device must be mounted and commissioned by an authorized electrician.
- The prevailing safety rules must be heeded.
- The device must not be opened.
- For planning and construction of electric installations, the relevant guidelines, regulations and standards of the respective country are to be considered.



Steinel GmbH
Dieselstrasse 80-84
33442 Herzebrock-Clarholz
Deutschland
Tel: +49 5245 448 0
www.steinel.de
product@steinel.de