IN00S01RIP	**KNX IP Router Secure**



USER MANUAL

Translation of the original instructions

Version: **1.0**

Date: **08/10/26**

Index

01. Application 4
02. KNX Security 4
03. Coupler function (KNXnet/IP Routing) 5
04. Bus access function (KNXnet/IP Tunneling) 6
05. Installation and Connection 6
06. Factory default settings 6
07. Interface settings with ETS 7
08. ETS database 7
09. ETS parameter dialogue 9
10. Programming 11
11. Open Source Licenses 11

VERSION	DATE	CHANGES
1.0	08/10/26	-

Any information in this manual is subject to change without notice.

This handbook can be downloaded freely from the website:
www.eelectron.com

Exclusion of liability:
Despite checking that the contents of this document match the hardware and software, deviations cannot be completely excluded. We therefore cannot accept any liability for this.
Any necessary corrections will be incorporated into newer versions of this manual.

Symbol for relevant information

Symbol for warning

DISPOSAL : The crossed-out bin symbol on the equipment or packaging means the product must not be included with other general waste at the end of its working life. The user must take the worn product to a sorted waste centre, or return it to the retailer when purchasing a new one. An efficient sorted waste collection for the environmentally friendly disposal of the used device, or its subsequent recycling, helps avoid the potential negative effects on the environment and people's health, and encourages the reuse and/or recycling of the construction materials.

Eelectron S.p.A.
Via Claudio Monteverdi 6,
I-20025 Legnano (MI), Italia
Tel +39 0331.500802 info@eelectron.com

IN00S01RIP secure

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



IN00S01RIP *secure*

01. Application

The compact IN00S01RIP *secure* 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). For access via KNXnet/IP Tunneling max. 8 simultaneous connections are possible.

The device supports KNX Security. 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 Security 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 IN00S01RIP *secure* has an extended filter table for main groups 0..31 and can buffer up to 150 telegrams. Power is supplied via the KNX bus.

02. KNX Security

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

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

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

KNX IP Security for the router function

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

Routing communication is encrypted with KNX IP Security. 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 Security is used for routing, all connected KNX IP devices must support security and be configured accordingly.

KNX IP Security for the interface function

When using a KNX IP router as an interface to the bus, access to the installation is possible without security for all devices that have access to the IP network. With KNX Security 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 Security for the device

The IN00S01RIP *secure* also supports KNX Data Security 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 Security 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 security properties are checked by the respective recipient.

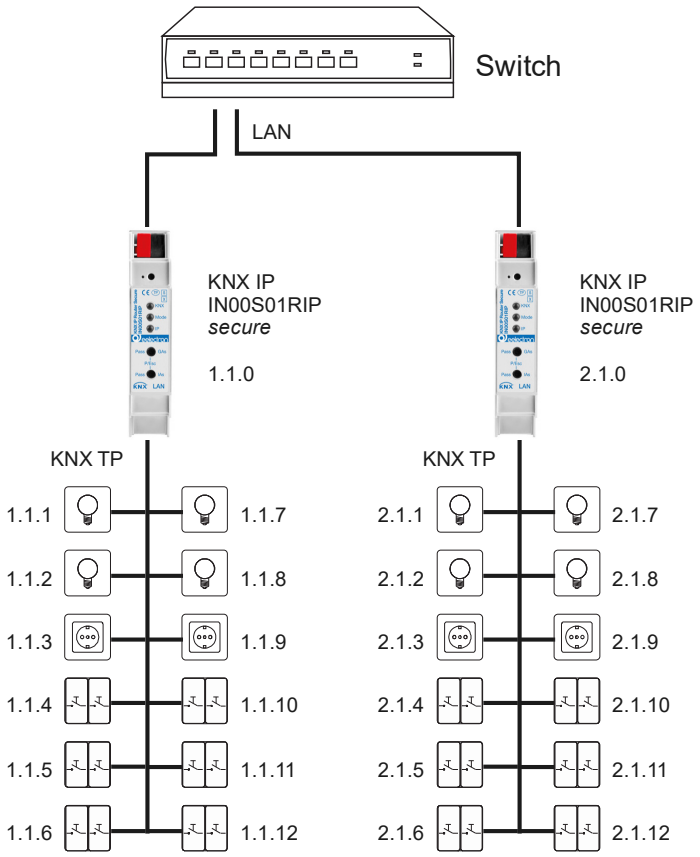
KNX Data Security and KNX IP Security can be used in parallel. In this case, for example, a KNX sensor would send a group telegram encrypted with KNX Data Security to the bus. When forwarding via KNX IP with KNX IP Security, the encrypted telegram would be encrypted again just like unencrypted ones.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

03. Coupler function (KNXnet/IP Routing)

The IN00S01RIP *secure* operates as a line or backbone coupler. In both cases, the LAN (IP) is used as a backbone.

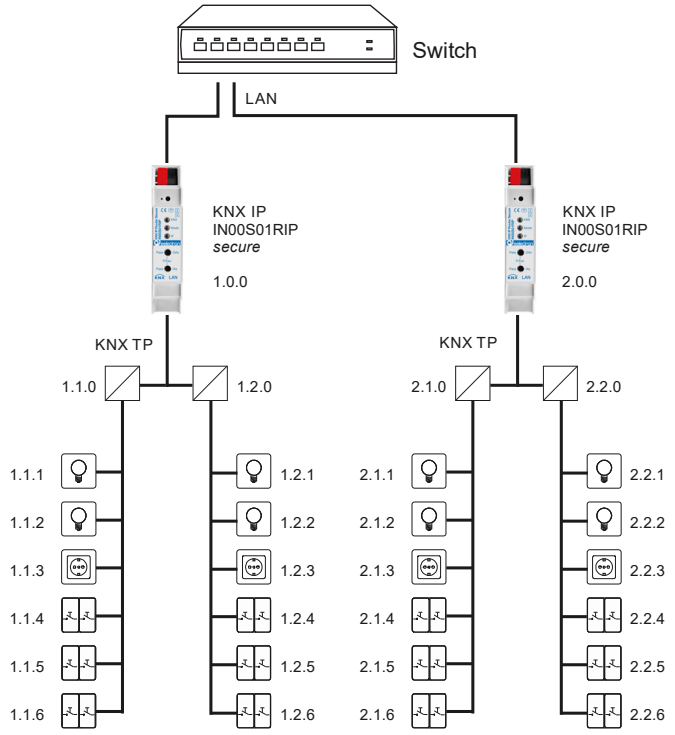
The following table shows the application possibilities of the KNX IP Router compared to the classic topology:

	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 Units)	KNX IP Router (max. 15 Units)	Directly via LAN Switch
Main line	TP	TP	IP
Coupling	KNX Line Coupler (max. 15x15 Units)	KNX Line Coupler (max. 15x15 Units)	KNX IP Router (max. 225 units)
Line	TP	TP	TP



KNX IP Router as line coupler

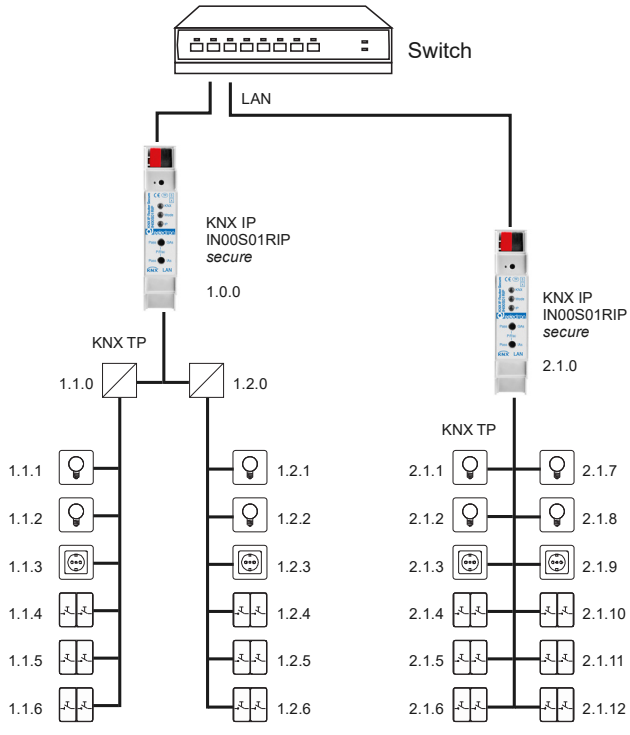
The individual address assigned to the IN00S01RIP secure determines whether the device operates as a line or area coupler. If the individual address is in the form of x.y.0 (x, y: 1..15), the router operates as a line coupler. If it is in the form of x.0.0 (x: 1..15), the router acts as a backbone coupler.



KNX IP Router as area coupler

If the IN00S01RIP secure is used as an 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 IN00S01RIP secure 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 IN00S01RIP *secure* has a memory for 150 telegrams (from IP to KNX).

04. Bus access function (KNXnet/IP Tunneling)

The IN00S01RIP *secure* 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.

05. Installation and Connection

The IN00S01RIP *secure* 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 IN00S01RIP *secure* is powered by the KNX bus. An external power supply is not necessary.

The device does not operate without KNX 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 lights 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.

06. 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**
Security Mode	**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 to the 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.

07. 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 IN00S01RIP *secure* 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.

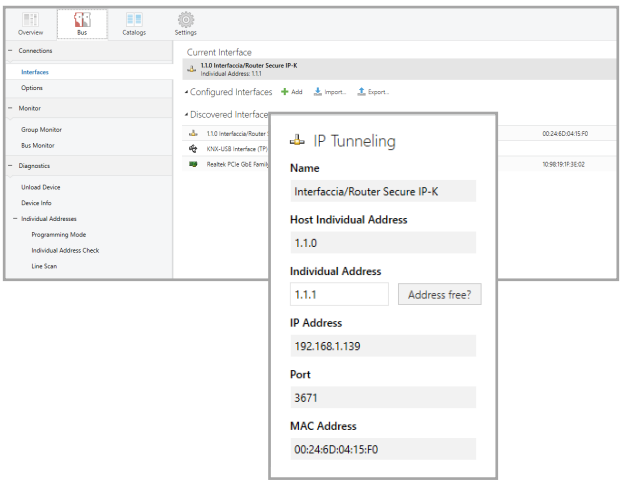
For the interface function the device contains additional individual addresses that can be set in the ETS. When a client (e.g. ETS) sends via the KNX IP Router telegrams to the bus, they contain a sender address as one from the additional addresses. Each address is associated with a connection. Thus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

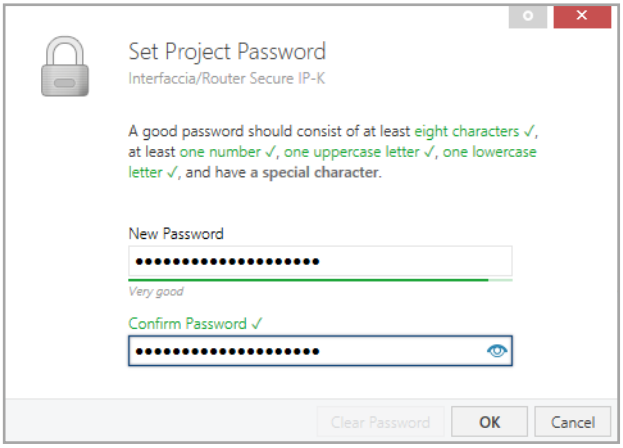


The individual KNX device address and the individual KNX addresses for additional tunneling connections can be changed within the ETS project, after the device has been added to the project.

08. ETS database

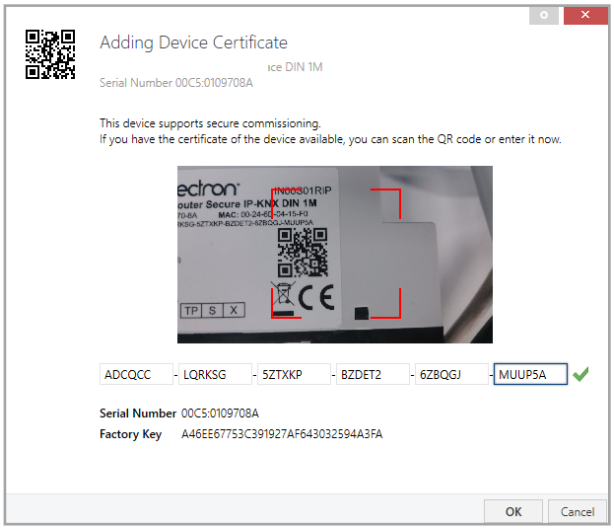
The ETS database (ETS 5.7 or higher) can be downloaded from the product website of the IN00S01RIP secure (www.eelectron.com) or via the KNX online catalogue.

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



This password protects the ETS project from unauthorised 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 security reasons.

ETS requires a device certificate for each device with KNX Security that is created in the ETS. This certificate contains the serial number of the device as well as a unique factory default setup key (FDSK = Factory Default Setup Key).



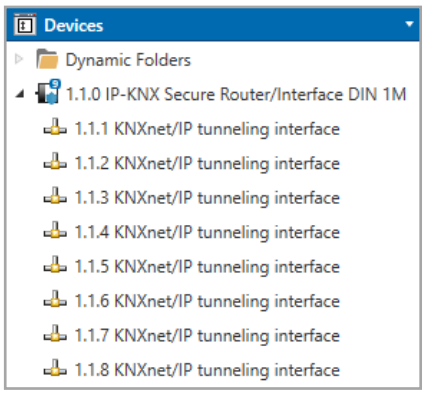
The certificate is printed as text on the device. It can also be conveniently scanned from the printed QR code via a webcam.

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

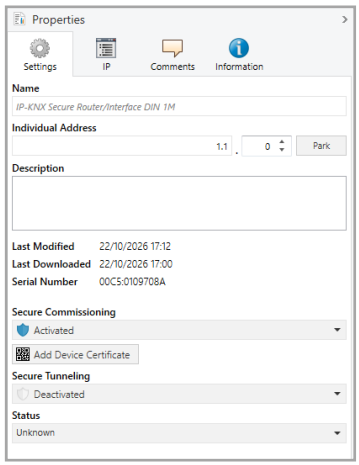
In the ETS, some settings are displayed in addition to the parameter dialog in the properties dialog (at the edge of the screen). The IP settings can be made here. The additional addresses for the interface connections are displayed in the topology view.



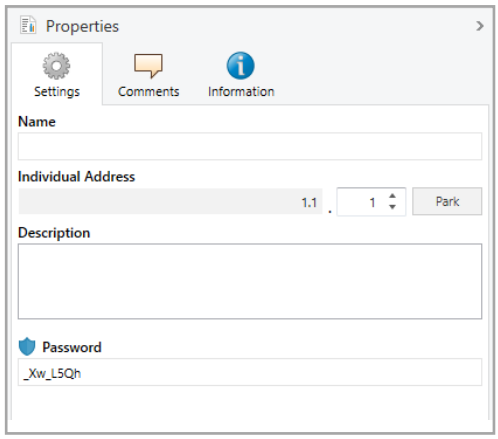
Each individual KNX address can be changed by clicking on the list entry and typing in the desired address into the “Individual Address” text-field. If the text-field frame switches to color red after entering the address, the address is already taken within your ETS project.

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

By clicking on the IN00S01RIP *secure* 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.



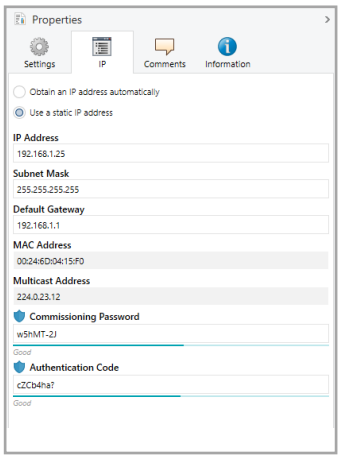
If secure tunneling is activated, a unique password will be created automatically for each tunnel. These passwords can be displayed under the ‘Settings’ overview, when a tunnel is selected.



Within the “IP” overview the IP network specific options of the IN00S01RIP *secure* 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.

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



IP address

Here the IP address of the IN00S01RIP *secure* 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 IN00S01RIP *secure*.

IP address of the PC:	192.168.1.30
Subnet of the PC:	255.255.255.0

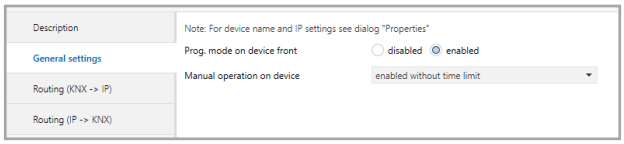
The IN00S01RIP *secure* is located in the same LAN, i.e. it uses the same subnet. The subnet constrains the IP addresses that can be assigned. In this example, the IP address of the KNX IP Router must be 192.168.1.xx, where xx can be a number from 1 to 254 (with the exception of 30, which is already 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

09. ETS parameter dialogue

The following parameters can be set using the ETS.

General settings



Prog. mode on device front

In addition to the normal programming button 3 the device allows activating the programming mode on the device front

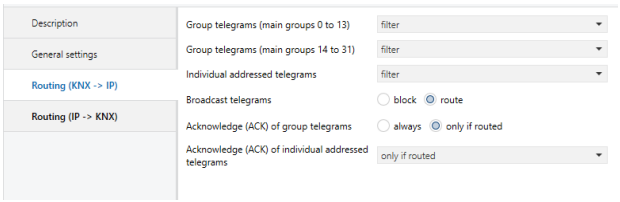
without opening the switchboard cover. The programming mode can be activated and deactivated via pressing simultaneously both buttons 7 and 8.

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)



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: An acknowledgement is generated for every received group telegram (from KNX).

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

Acknowledge (ACK) of individually addressed telegrams

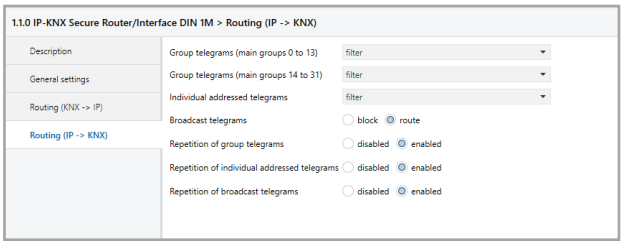
Always: An acknowledge is generated for every received individual addressed telegram (from KNX).

Only if routed: An acknowledge is only generated for received individually addressed 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 KNX 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.

10. Programming

The IN00S01RIP *secure* 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. In 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

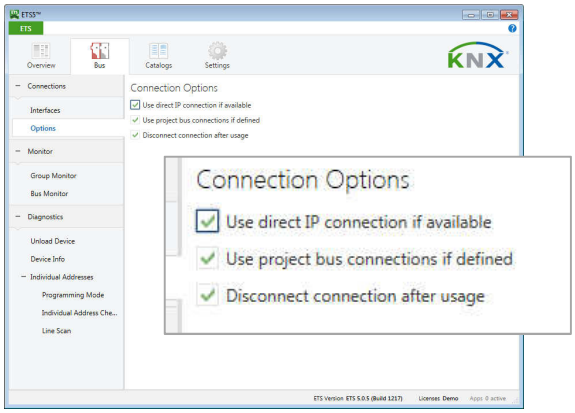
No additional interface is required. Programming via KNXnet/IP Tunneling is possible if the device already has a valid IP configuration (e.g. via DHCP). In this case the device is displayed in the interface configuration of the ETS and must be selected. The download is executed via the ETS project as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

11. 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.