SpaceLogic KNX IP Router DIN Rail

Product information and Application description

This document gives you product information about the SpaceLogic KNX IP Router DIN Rail, MTN6500-0103 and describes the ETS application KNX IP Router secure 7127 /1.2

MTN6500-0103
12/2019

Schneider Electric
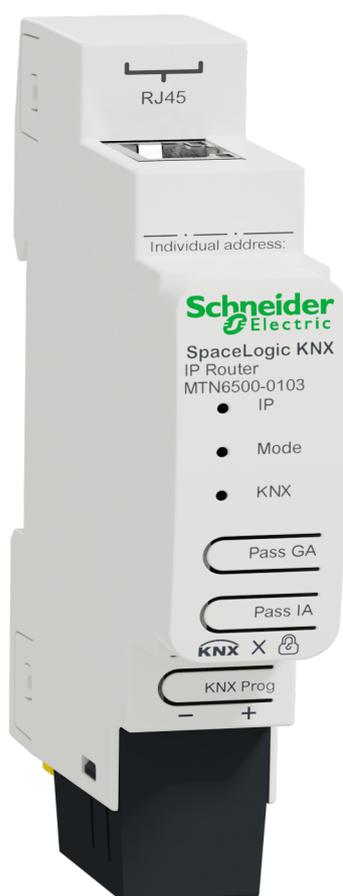
Legal Information

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this guide are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owners.

This guide and its content are protected under applicable copyright laws and furnished for informational use only. No part of this guide may be reproduced or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), for any purpose, without the prior written permission of Schneider Electric.

Schneider Electric does not grant any right or license for commercial use of the guide or its content, except for a non-exclusive and personal license to consult it on an "as is" basis. Schneider Electric products and equipment should be installed, operated, serviced, and maintained only by qualified personnel.

As standards, specifications, and designs change from time to time, information contained in this guide may be subject to change without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this material or consequences arising out of or resulting from the use of the information contained herein.

Table of Contents

Safety information

Important information

Read these instructions carefully and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this manual or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of either symbol to a "Danger" or "Warning" safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that accompany this symbol to avoid possible injury or death.

⚡⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

Failure to follow these instructions will result in death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result in** minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

For your safety

⚡⚠ DANGER
HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH
Safe electrical installation must be carried out only by qualified electrical personnel. Qualified electrical personnel must prove profound knowledge in the following areas:
• Connecting to installation networks
• Connecting several electrical devices
• Laying electric cables
• Connecting and establishing KNX networks
• Connecting and establishing LAN networks
• Safety standards, local wiring rules and regulations
Failure to follow these instructions will result in death or serious injury.

Product information

The compact SpaceLogic KNX IP Router (referred to below as **KNX IP Router**) 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 (For example, for ETS programming.)

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 unauthorized 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 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 Security

The KNX standard was extended by KNX Security to protect KNX installations from unauthorized 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 (twisted pair) 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 KNX bus are also encrypted.

KNX IP Security 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 Security. This means that only IP devices that know the key can decrypt the communication and send valid telegrams. If there is an existing installation with an old IP router that does not support IP Security, the whole installation can only work as non-secure. 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 the device 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.

In both modes, the interface forwards both encrypted and unencrypted KNX telegrams. The security properties are checked by the respective receiver or tool.

KNX Data Security for the device

The KNX IP Router also supports KNX Data Security to protect the device from unauthorized access from the KNX bus. If the KNX IP Router is programmed via the KNX bus, this is done with encrypted telegrams.

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

The secured device configuration is also contained in KNX data security.

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 Router 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.

Installation and connection

The device is designed for installation on a DIN rail with a width of 1 unit (18 mm).

⚠⚠ **DANGER**
HAZARD OF ELECTRIC SHOCK AND DEVICE DAMAGE
• Ensure a safety clearance of minimum 4 mm between the individual cores of the 230 V supply cable and the KNX line Ⓐ, in accordance with IEC 60664-1.
• Ensure that the installed devices have minimum basic insulation next to the device.
Failure to follow these instructions will result in death or serious injury.
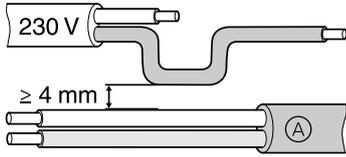
Installing

TH 35 (DIN EN 60715)

CLICK
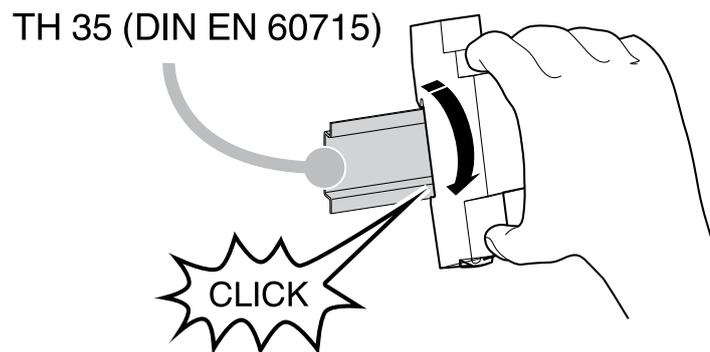
Removing

Connecting

max. 9 mm 5 mm
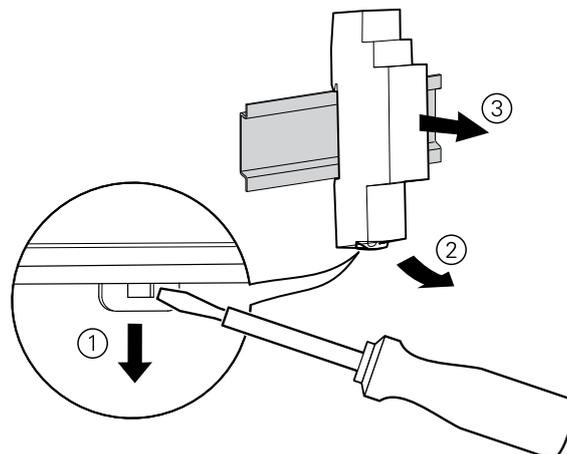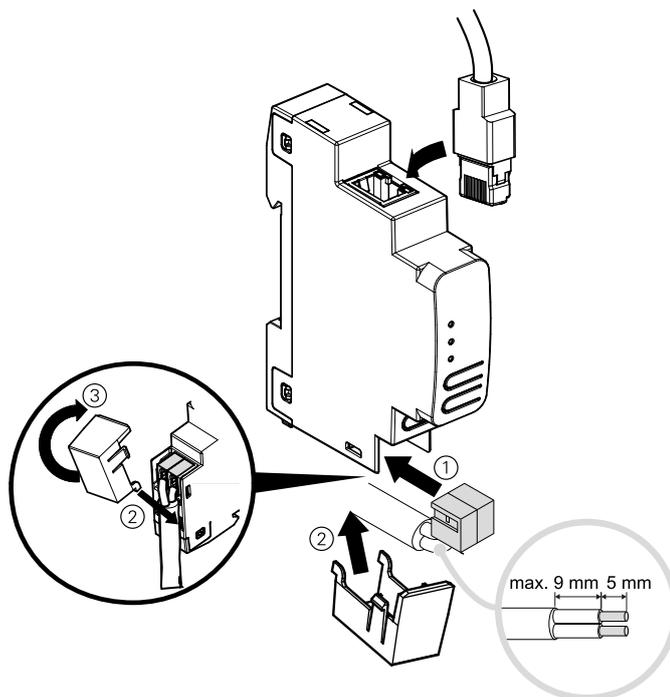
NOTICE

EQUIPMENT DAMAGE AND LOSS OF COMMUNICATION

Installation of communication cabling for information technology must be guaranteed in accordance with DIN EN 50174.

Failure to follow these instructions can result in equipment damage.

Technical data

Power supply	via KNX bus, <20mA

Connection	
LAN	RJ45 Connector
KNX	Bus connecting terminal

Dimension (LxWxD)	100x18x86 mm
Device width	1 module = 18 mm

Coupler function (KNXnet/IP Routing and TP Routing)

The KNX IP Router 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 Spacelogic KNX Coupler compared to the IP based topology:

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

KNX IP Router as line coupler

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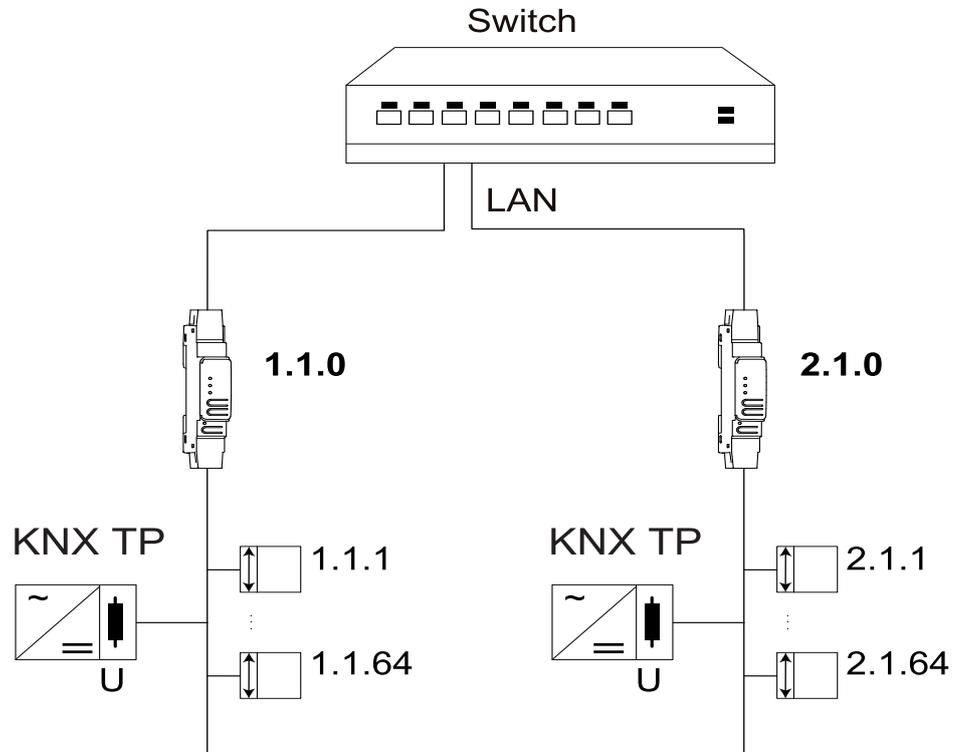
If the individual address is in the form of x.y.0 (x, y: 1…15), the router operates as a line coupler. If it is in the form of x.0.0 (x: 1…15), the router acts as a backbone coupler.

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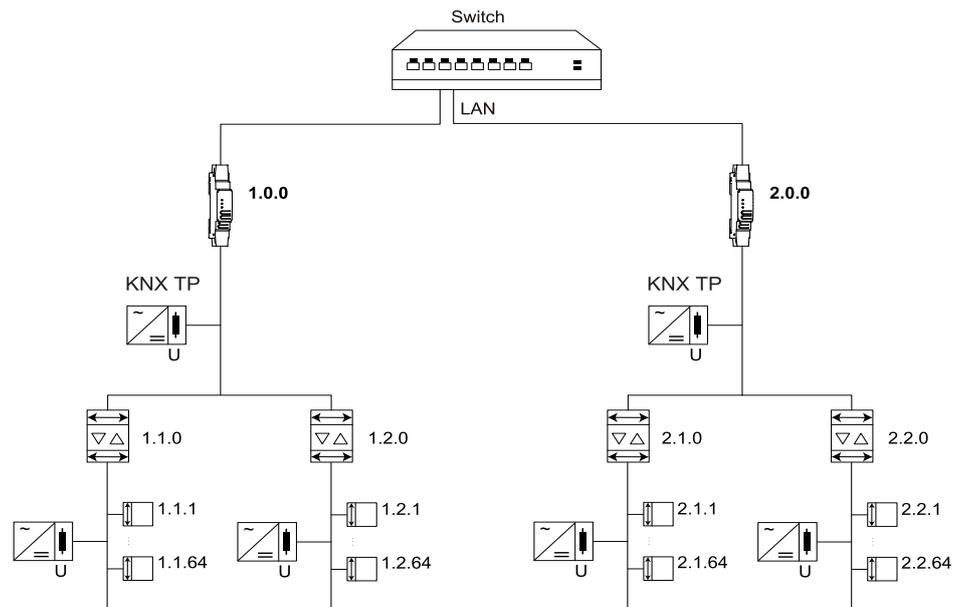
If the KNX IP Router is used as an area coupler (x.0.0), there must not be a KNX IP Router in the topology beneath it. For example, if a KNX IP Router has the individual address 1.0.0, there must be no KNX IP Router with the address 1.1.0.

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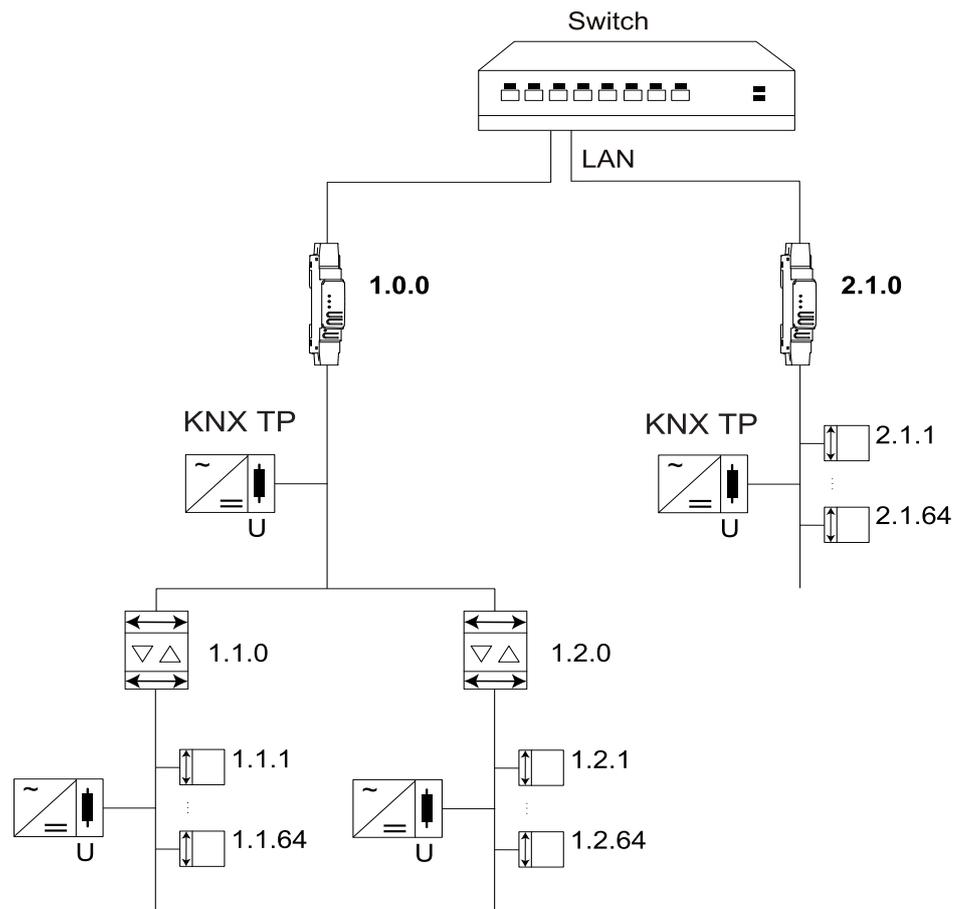
The KNX IP Router has a filter table and thus contributes to reducing the bus load. The filter table (8 kB) supports the extended group address range (main groups 0…31) and is automatically generated by the ETS.

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 has a memory for 150 telegrams (from IP to KNX).

Bus access function (KNXnet/IP Tunneling)

The KNX IP Router 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.

Connections and operating elements
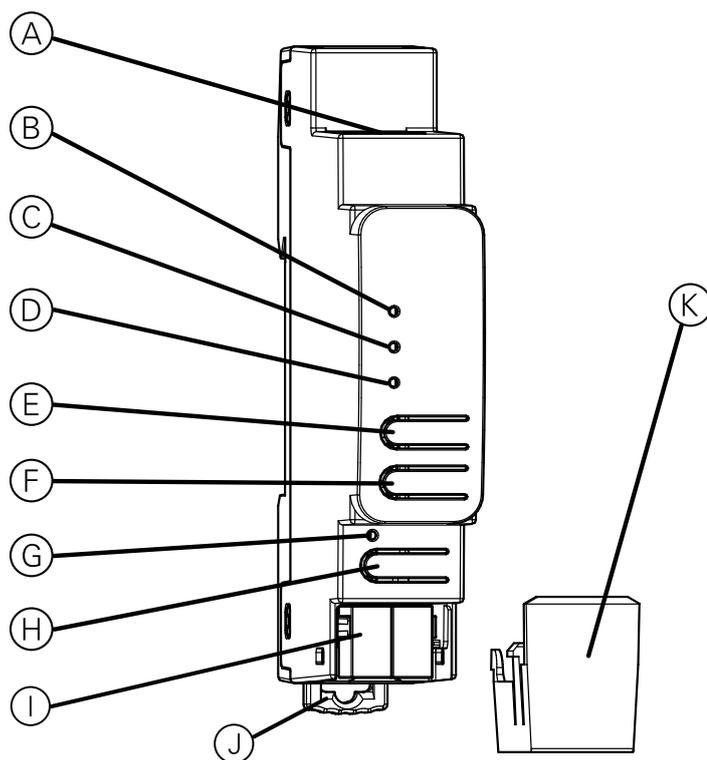
Ⓐ	Ethernet/LAN Connector
Ⓑ	IP LED (multicolor)
Ⓒ	Mode LED (multicolor)
Ⓓ	KNX LED (multicolor)
Ⓔ	Button: Pass GA (Forwarding of group addressed telegrams)
Ⓕ	Button: Pass IA (Forwarding of individually addressed telegrams)
Ⓖ	Programming LED (red)
Ⓗ	Button for programming mode
Ⓘ	KNX bus connector
Ⓙ	Release lever for disassembly
Ⓚ	Cable cover

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

   NOTE: The device does not work without bus power.

KNX Programming mode

The KNX programming mode is activated/deactivated by pressing the flushed KNX programming button ⊕.

It is possible to write the programmed individual address on the labeling field with a non permanent marker or pencil. So it is possible to change it, if needed.
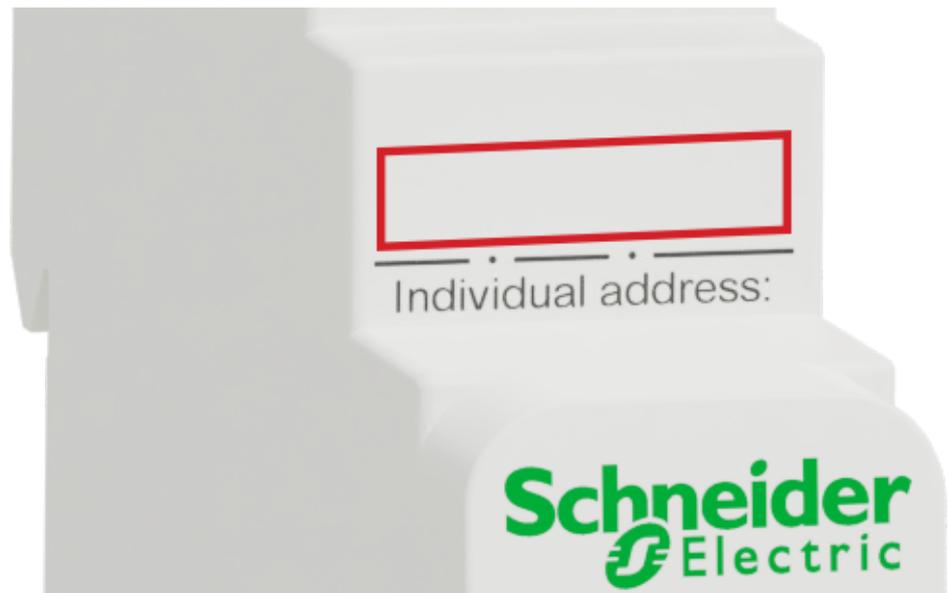
Status display

Overview of the different indications of the IP LED

IP LED Ⓑ Status	Meaning
LED lights green	The device has an active Ethernet link and valid IP settings (IP address, Subnet, and Gateway.)
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.

Overview of the different indications of the Mode LED

Mode LED Ⓒ Status	Meaning
LED lights green	Device is working in standard operation mode.
LED flashes 1x/s orange	Manual operation is active. Forwarding IA **or** GA.
LED flashes 2x/s orange	Manual operation is active. Forwarding IA **and** GA.
LED flashes red	Manual operation is not active. The device is not properly loaded. For example, after an interrupted download.

Overview of the different indications of the KNX LED

KNX LED Ⓓ Status	Meaning
LED lights green	Device is successfully powered by the KNX bus.
LED flickers green	Telegram traffic on the KNX bus.
LED shortly red	Communication failures on the KNX bus. For example, repetitions of telegrams or telegram fragments are indicated by a short change of the LED color to red.

Manual operation

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

With the button Pass GA Ⓔ the forwarding of all group addressed telegrams can be activated.

With the button Pass IA Ⓕ the forwarding of all individually addressed telegrams can be activated.

This is visualized by flashing of the Mode LED Ⓒ 1x/s (orange). If both modes are activated the Mode LED Ⓒ flashes 2x/s.

Pressing button Pass GA Ⓔ or button Pass IA Ⓕ again these settings can be selected and deselected on demand.

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

Factory default settings

The following configuration is set by factory default:

Individual device address	**15.15.0**
Number of configured KNXnet/IP tunneling configuration	**8**
Individual address of tunneling configuration	**15.15.240**
IP address assignment	**DHCP**
Initial Key (FDSK)	**active**
Security Modus	**not active**

Reset to factory device settings (master reset)

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

1. Disconnect the KNX Bus connector ⓘ from device.

2. Press the KNX programming button ⊕ and keep it pressed down.

3. Reconnect the KNX Bus connector ⓘ of device.

4. Keep the KNX programming button ⊕ pressed for at least another 6 seconds.

A short flashing of all LEDs (ⓖ, ⓓ, ⓒ, ⓑ) 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 Router 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 project, page 23* section for more information.

If security mode is activated in the KNX IP Router, a password is required to establish a connection.

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. (For example, many DSL routers have an integrated DHCP server.)

If the KNX IP Router has been connected to the LAN and has a valid IP address, it should automatically appear in the ETS within the menu **Bus** under **Discovered interfaces**.

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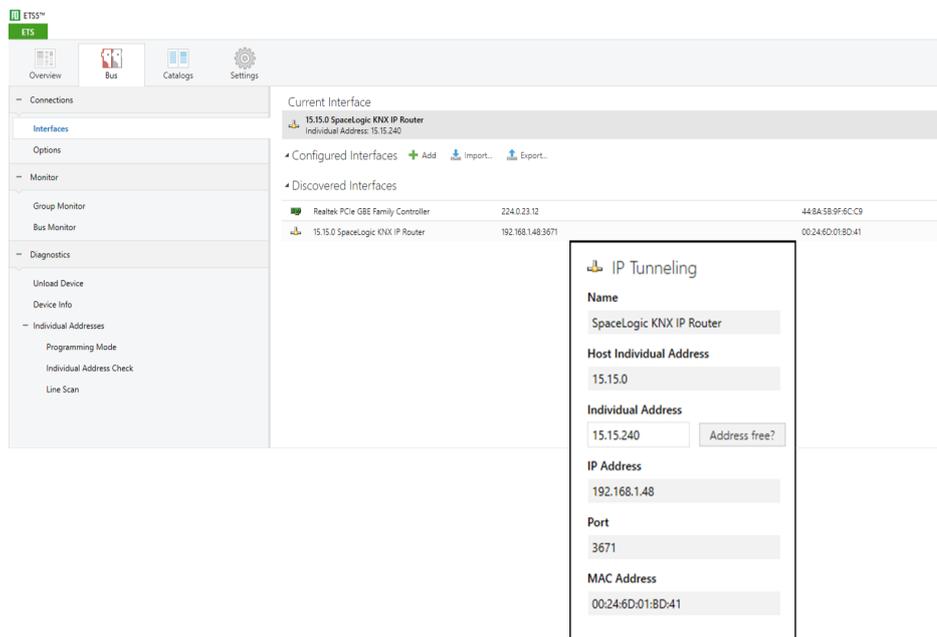
The individual KNX device address and the individual KNX addresses for additional tunneling connections can be changed within the ETS project, after the device has been added to the project.

ETS application

The ETS database (ETS 5.7.3 or higher) can be downloaded from the product website of the KNX IP Router (*www.schneider-electric.com*) or via the KNX online catalogue.

Product family	1.3 Interfaces/Gateways
Product type	1.3.14 IP devices
Manufacturer	Schneider Electric Industries SAS
Name	SpaceLogic KNX IP Router DIN Rail
Order number	MTN6500–0103

ETS project

If the first product is inserted into a project with KNX Security, the ETS prompts you to enter a project password.
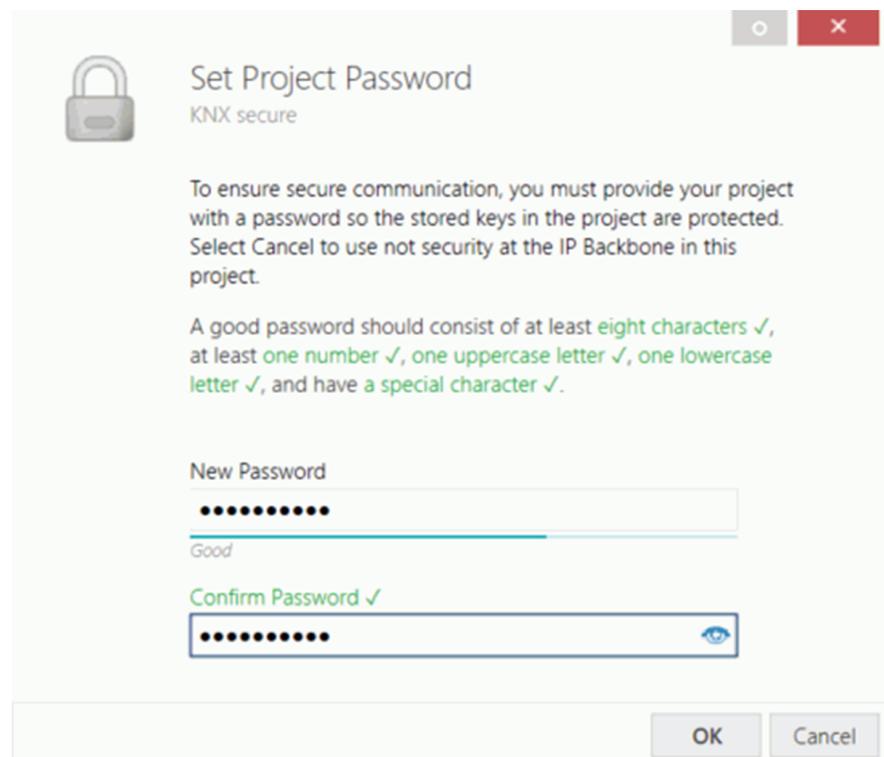
This password protects the ETS project from unauthorized access. This password is not a key that is used for KNX communication. The entry of the password can be bypassed with **Cancel**, but this is not recommended for security reasons.

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 an intangible key (FDSK = Factory Default Setup Key).
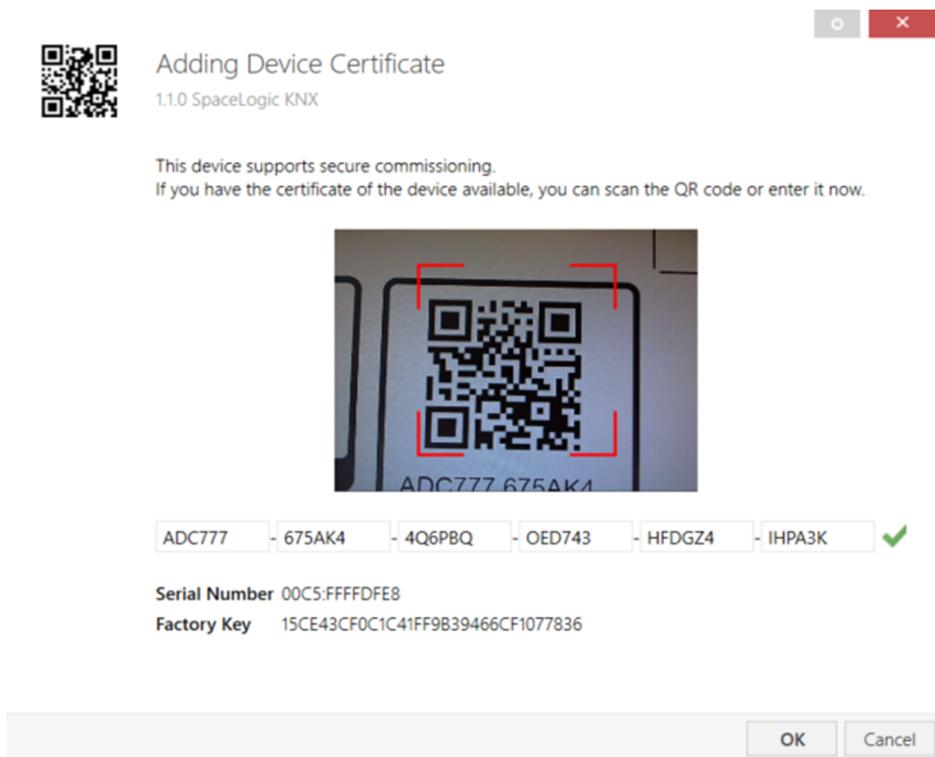
The certificate is printed as text on the device. It can also be conveniently scanned from the printed QR code via a camera connected to the PC that runs the ETS.

The KNX Secure code can be found on the right side of the device. The small KNX Secure code sticker with labeling field at the bottom of the device can be removed for documentation purpose.
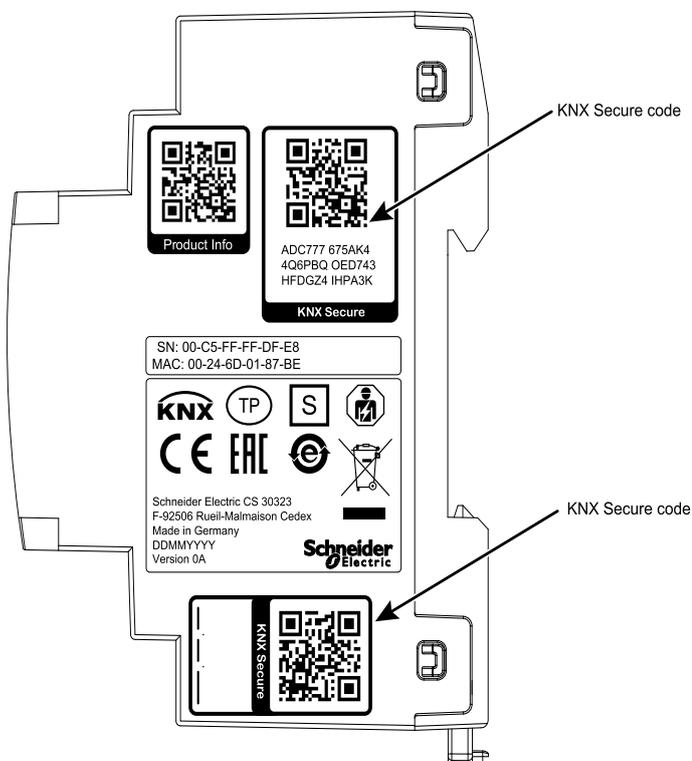
The list of all device certificates can be managed in the ETS **Overview > Projects > Security** window.

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.

Additional parameters

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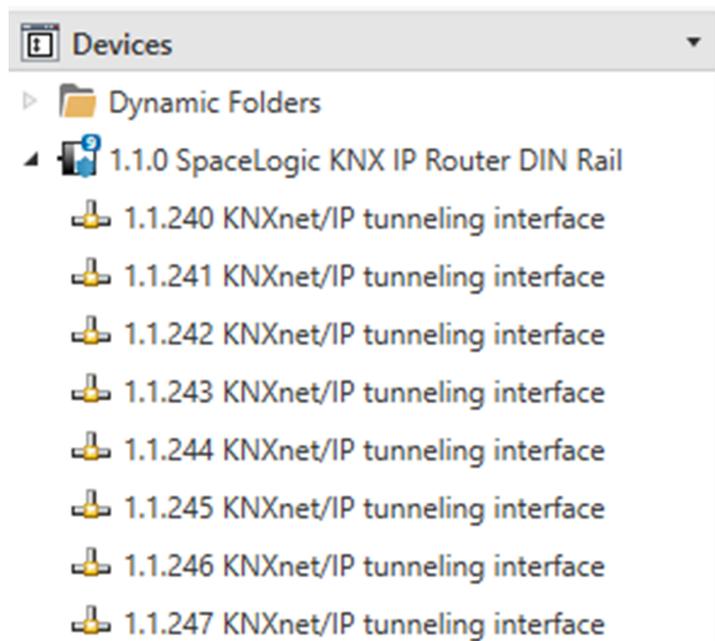
Each individual KNX address can be changed by clicking on the list entry and typing in the desired address into the **Individual Address** text-field. If the text-field frame switches to color red after entering the address, the address is already taken within your ETS project.

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

By clicking on the KNX IP Router 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.
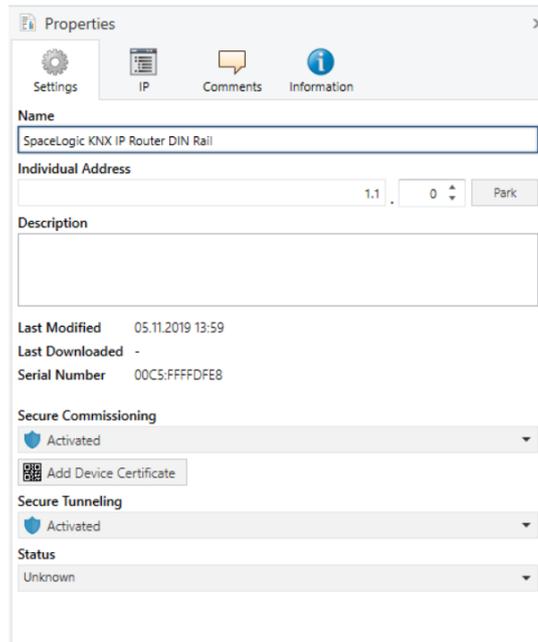
If secure tunneling is activated, a unique password will be created automatically for each tunnel. These passwords can be displayed under the **Settings** overview, when a tunnel is selected.
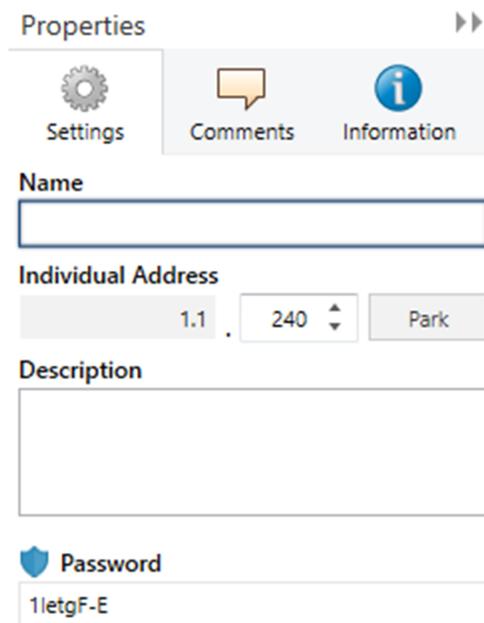
Within the **IP** overview, the IP network specific options of the KNX IP Router can be changed.

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.

> **NOTE:** All changes in the **Properties** menu become effective only after a successful application download.
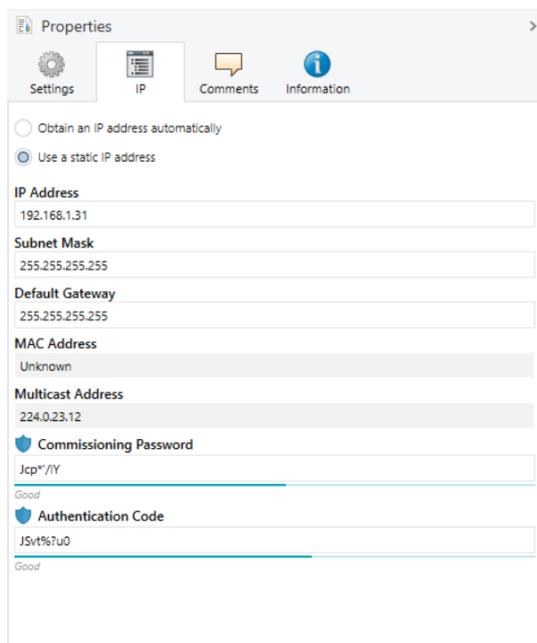
IP address

Here the IP address of the KNX IP Router 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, for example, 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.

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

The KNX IP Router 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.

NOTICE

MATERIAL DAMAGE THROUGH UNAUTHORIZED ACCESS TO THE KNX INSTALLATION

As soon as you access the KNX installation via the Internet, the data traffic can be read by third parties.

- Only use a VPN access for this connection with a secure encryption for all data packages.

- The required hardware (VPN router) and the features offered by mobile service providers differ significantly with regard to the settings and technical possibilities depending on the country or region.

- Always have the VPN access set up and commissioned by a specialist VPN service provider. The VPN service provider selects a suitable mobile service provider and suitable hardware for the VPN access and ensures that the VPN is set up by a qualified specialist.

Schneider Electric cannot be held responsible for performance problems and incompatibilities caused by applications, services or devices from third-party providers. Schneider Electric offers no technical support when setting up a VPN access.

Failure to follow these instructions can result in equipment damage.

VPN access

The VPN access (VPN = Virtual Private Network) authorises the portable device to access the local network, and therefore also the KNX installation, via the Internet.

Benefits of VPN:

- Only authorised users have access to the local network.
- All data is encrypted.
- The data is not changed, recorded or diverted during the transfer. This is often referred to as a VPN tunnel.

Requirements for setting up a VPN connection:

- Internet connection.
- The portable device and the router are enabled for a VPN connection (VPN client installed).

ETS parameter dialogue

The following parameters can be set using the ETS.

General settings

Manual operation on device

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

Routing (KNX → IP)

Group telegrams (main group 0 to 13)

Block	No group telegrams of these main groups are routed to IP.
Route	All group telegrams of these main groups 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 these main groups are routed to IP.
Route	All group telegrams of these main groups 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.

Individual 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 acknowledge is generated for every received group telegram (from KNX).
Only if routed	An acknowledge is only generated for received group telegrams (from KNX) if they are routed to IP.

Acknowledge (ACK) of individual 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 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.

NOTE: When using **Answer with NACK**, an access to the device via KNX TP is no longer possible. The configuration must be performed via IP. This can be used to make an installation more secure.

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 these main groups 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 these main groups are routed to KNX.
Route	All group telegrams of these main groups 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.

Individual 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 individual 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 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 (for example, 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 (For example, 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 (this can also be the default 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.
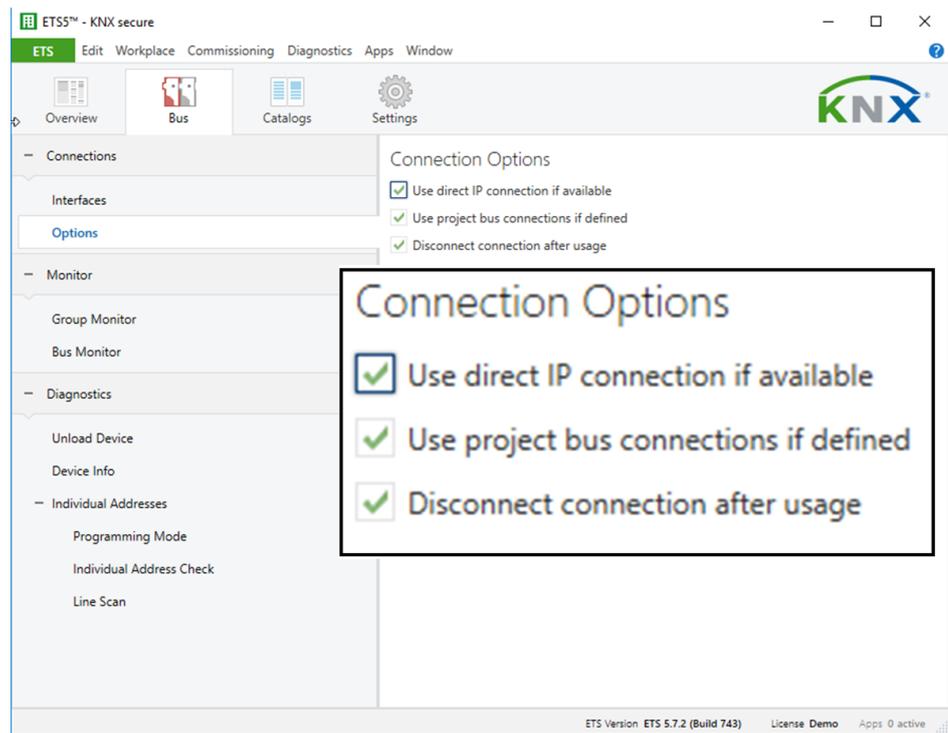
NOTE: Due to the significantly shorter transmission times it is recommended to perform downloads via IP.

Open Source Software used in the product

The product contains, among other things, Open Source Software files, as specified below, developed by third parties and licensed under an Open Source Software license. These Open Source Software files are protected by copyright. Your right to use the Open Source Software is governed by the relevant applicable Open Source Software license conditions.

Your compliance with those license conditions will entitle you to use the Open Source Software as foreseen in the relevant license. In the event of conflicts between other Schneider Electric license conditions applicable to the product and the Open Source Software license conditions, the Open Source Software conditions shall prevail. The Open Source Software is provided royalty-free (i.e. no fees are charged for exercising the licensed rights). The list of Open Source Software contained in this product and the respective applicable Open Source Software terms and conditions are listed hereunder:

List of Open Source Software Files	Applicable Licenses
curve25519–donna	See *https://github.com/agl/curve25519-donna*

If Open Source Software contained in this product is licensed under GNU General Public License (GPL), GNU Lesser General Public License (LGPL), Mozilla Public License (MPL) or any other Open Source Software license, which requires that source code is to be made available, you can download the corresponding source code of the Open Source Software from the following link:

List of Open Source Software Files	Access to Open Source Software files
curve25519–donna	See *https://github.com/agl/curve25519-donna*

Warranty regarding further use of the Open Source Software

Schneider Electric SE and all of its subsidiaries ("Schneider Electric Group") provide no warranty for the Open Source Software contained in this product, if such Open Source Software is used in any manner other than intended by Schneider Electric Group. The licenses listed above define the warranty, if any, from the authors or licensors of the Open Source Software. Schneider Electric Group specifically disclaims any warranty for defects caused by altering any Open Source Software or the product's configuration. Any warranty claims against Schneider Electric Group in the event that the Open Source Software contained in this product infringes the intellectual property rights of a third party are excluded.

Technical support, if any, will only be provided for unmodified software.

WEEE directive
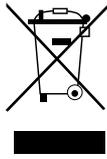
Dispose of the device separately from household waste at an official collection point.

Professional recycling protects people and the environment against potential negative effects.

MTN6500-0103_SW_EN