ENGLISH

INKNXRTR008000 User Manual

Intesis KNX IP Router Secure
Router between KNX TP and KNX IP
Interface for connection to KNX TP via IP

USER MANUAL
Version 1.0.0
Publication date 2026-06-25

Disclaimer

The information in this document is for informational purposes only. Please inform HMS Networks of any inaccuracies or omissions found in this document. HMS Networks disclaims any responsibility or liability for any errors that may appear in this document.

HMS Networks reserves the right to modify its products in line with its policy of continuous product development. The information in this document shall therefore not be construed as a commitment on the part of HMS Networks and is subject to change without notice. HMS Networks makes no commitment to update or keep current the information in this document.

The data, examples and illustrations found in this document are included for illustrative purposes and are only intended to help improve understanding of the functionality and handling of the product. In view of the wide range of possible applications of the product, and because of the many variables and requirements associated with any particular implementation, HMS Networks cannot assume responsibility or liability for actual use based on the data, examples or illustrations included in this document nor for any damages incurred during installation of the product. Those responsible for the use of the product must acquire sufficient knowledge in order to ensure that the product is used correctly in their specific application and that the application meets all performance and safety requirements including any applicable laws, regulations, codes and standards. Further, HMS Networks will under no circumstances assume liability or responsibility for any problems that may arise as a result from the use of undocumented features or functional side effects found outside the documented scope of the product. The effects caused by any direct or indirect use of such aspects of the product are undefined and may include e.g. compatibility issues and stability issues.

Contents

1 Order Code and Description

ORDER CODE
INKNXRTR0080000

DESCRIPTION
Intesis KNX IP Router Secure.

This device works as a router between KNX TP and KNX IP, and as an interface for accessing the KNX TP installation via KNX IP through up to eight IP tunneling connections, even remotely.

2 General Information

2.1 Intended Use of the User Manual

This manual contains the main features of the *Intesis KNX IP Router Secure* and the instructions for its appropriate installation, configuration, and operation.

Any person who installs, configures, or operates the *Intesis KNX IP Router Secure* or any associated equipment should be aware of this manual's contents.

Keep this manual for future reference during the installation, configuration, and operation.

2.2 General Safety Information

⚠ Follow these instructions carefully. Improper work may seriously harm your health and damage the *Intesis KNX IP Router Secure* and/or any other equipment connected to it.

Only technical personnel, following these instructions and the country legislation for installing electrical equipment, can install and manipulate the *Intesis KNX IP Router Secure*.

Install the *Intesis KNX IP Router Secure* indoors, in a restricted access location, avoiding exposure to direct solar radiation, water, high relative humidity, or dust.

Mount the *Intesis KNX IP Router Secure* on a DIN rail inside a grounded metallic cabinet, following the instructions in this manual.

Connect the *Intesis KNX IP Router Secure* only to networks without routing to the outside plant. All communication ports are considered for indoor use and must only be connected to SELV circuits.

Disconnect all systems from power before manipulating and connecting them to the *Intesis KNX IP Router Secure*.

Respect the expected polarity of communication cables when connecting them to the *Intesis KNX IP Router Secure*.

Take the necessary antistatic precautions before manipulating the *Intesis KNX IP Router Secure* to avoid electrostatic discharges.

3 Factory Default Settings

The following configuration is set by factory default:

- Individual device address: 15.15.0
- Number of configured KNXnet/IP tunneling connections: 1
- Individual address of tunneling connections: 15.15.240
- IP address assignment: DHCP
- Initial Key (FDSK): Active
- Security Modus: Not active

To reset the *Intesis KNX IP Router Secure* to its factory default settings, see Reset to Factory Settings.

4 About KNX Secure

This is a KNX Secure device.

The specification for KNX Secure distinguishes between KNX IP Secure and KNX Data Secure.

- KNX IP Secure protects 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.

4.1 KNX IP Secure for the Router Function

Routing communication is encrypted with KNX IP Secure. This means that only IP devices that know the key can decrypt 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 also support KNX IP Secure and be configured accordingly.

4.2 KNX IP Secure for the Interface Function

When using the *Intesis KNX IP Router Secure* 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 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.

4.3 KNX Data Secure for the Device

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

Encrypted telegrams use longer frames (up to 63 bytes of payload) than the standard KNX ones (up to 23 bytes of payload). For secure programming via the bus, every device in the communication path must support long frames.

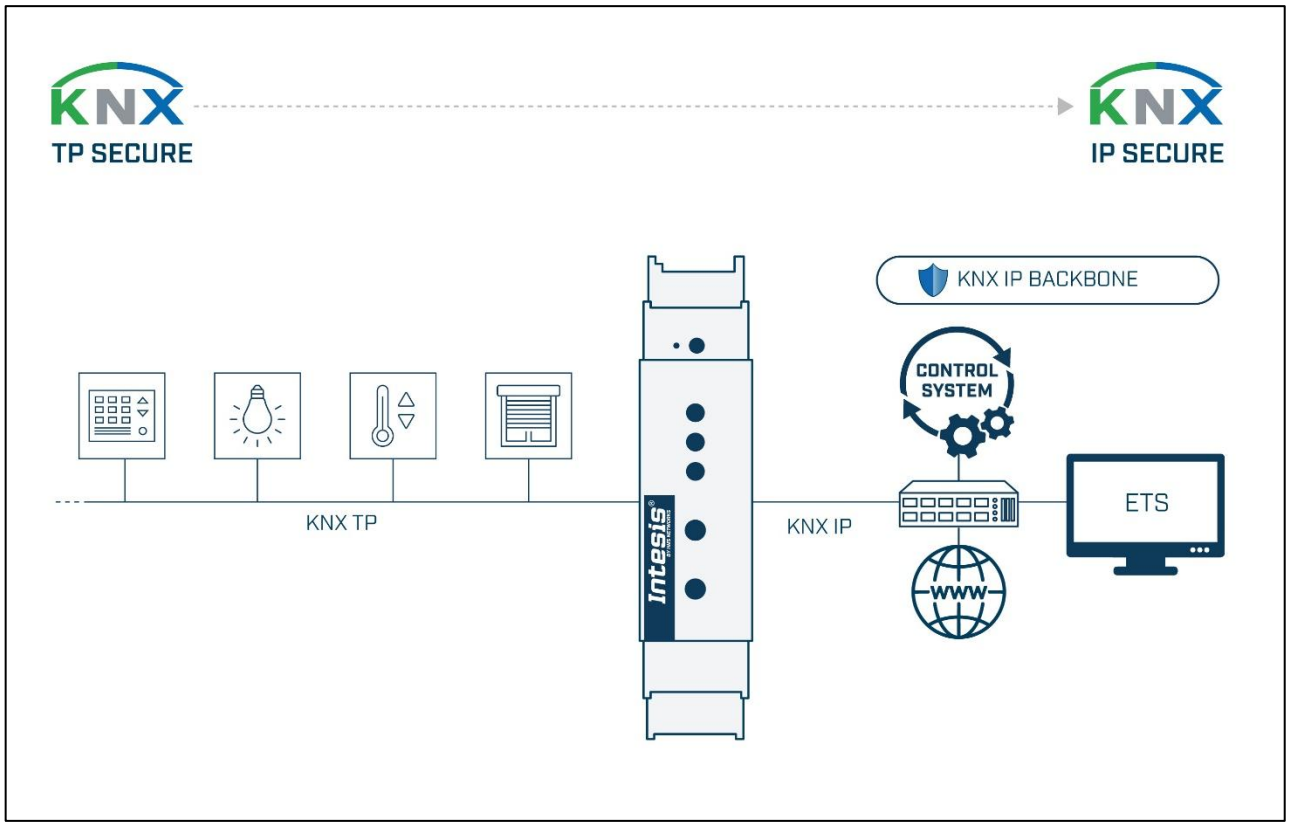
4.4 KNX Data Secure for Group Telegrams

Telegrams from the bus that do not address the *Intesis KNX IP Router Secure* 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 will 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 original encryption with KNX 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 KNX Data Secure can interpret the telegram.

5 Overview

Use case: *The Intesis KNX IP Router Secure as a router between KNX TP and KNX IP, and as an interface for accessing the KNX TP installation via KNX IP, even remotely.*



5.1 Main Features

- This is a KNX IP Secure and KNX Data Secure product.
- Double function: KNX IP router and KNX IP interface.
- As a KNX IP router, use it to forward telegrams between KNX TP and KNX IP devices, as a line coupler, and as an area coupler.
- As a KNX IP interface, it allows up to eight simultaneous IP tunneling connections.
- Manual mode: forwarding of grouped and/or individual addresses for testing and debugging purposes.
- Extended filter table for main groups 0 .. 31.
- Buffering capacity of up to 150 telegrams.

5.2 Capacity

As a KNX IP interface, the *Intesis KNX IP Router Secure* allows up to eight simultaneous IP tunneling connections.

5.3 General Functionality

The *Intesis KNX IP Router Secure* operates according to the KNXnet/IP specification using core, device management, tunneling and routing.

As a KNX IP router, the *Intesis KNX IP Router Secure* is used for routing and filtering telegrams between KNX TP and KNX IP segments.

As a KNX IP interface, the *Intesis KNX IP Router Secure* allows up to eight IP tunneling connections, i.e., point-to-point connections of client devices to the KNX TP installation via IP.

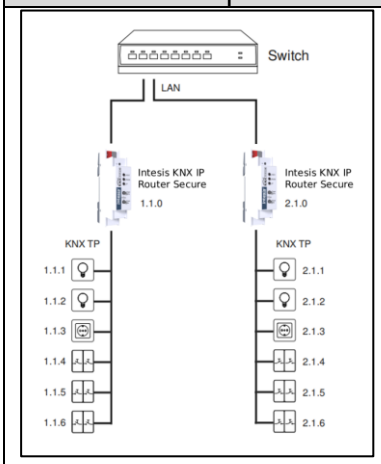
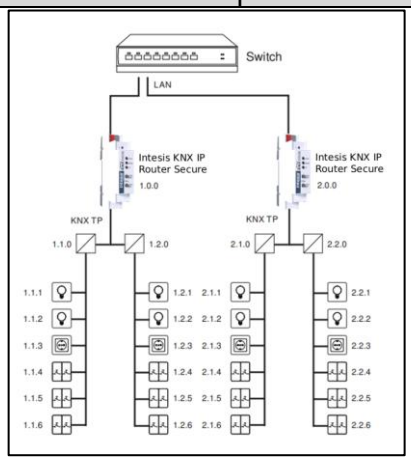
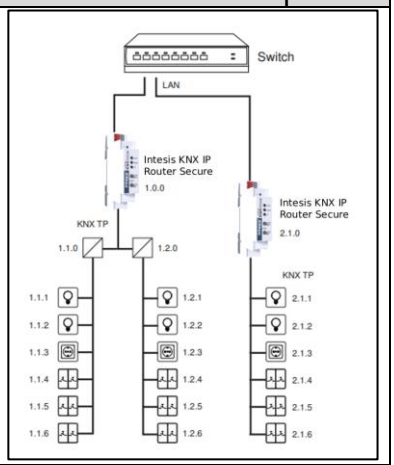
Examples of client devices include:

- A PC running ETS used for programming KNX TP devices over the IP network.
- A visualization server.

5.3.1 Router Function (KNXnet/IP Routing)

The *Intesis KNX IP Router Secure* operates as a coupler between KNX TP and KNX IP segments:

- Line coupler: It routes communication between a KNX TP line and a KNX IP area.
- Area coupler: It routes communication between a KNX TP area and the KNX IP backbone.

Line coupler	Area coupler	Line and area coupler
		

The individual address assigned to the *Intesis KNX IP Router Secure* determines whether it operates as a line or area coupler:

- If the individual address is in the form of x.y.0 (x, y: 1 .. 15), it operates as a line coupler.
- If the individual address is in the form of x.0.0 (x: 1 .. 15), it operates as an area coupler.

The *Intesis KNX IP Router Secure* can function either as a line coupler or as an area coupler. However, regardless of its role, the IP network is always treated as the KNX backbone.

When using an *Intesis KNX IP Router Secure*, there must not be another KNX IP router in the segment beneath or above it.

For example, if an *Intesis KNX IP Router Secure* is used as a line coupler with the address 1.x.0, there must not be another KNX IP router with the address 1.0.0. In the case of using an *Intesis KNX IP Router Secure* as an area coupler with the individual address 1.0.0, there must not be a KNX IP router with the address 1.x.0.

5.3.1.1 Filter Table

The *Intesis KNX IP Router Secure* features a filter table, contributing 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 to avoid telegram loss. The *Intesis KNX IP Router Secure* has a memory for 150 telegrams (from IP to KNX).

5.3.2 Interface Function (KNXnet/IP Tunneling)

The *Intesis KNX IP Router Secure* can be used as an interface to KNX. The KNX TP bus can be accessed via the IP network. For this purpose, additional individual addresses must be assigned, as described in Additional KNXnet/IP Tunneling Interfaces.

The access via the IP network can be performed either from the local area network (LAN) or remotely via a network address translation (NAT) or virtual private network (VPN) connection. To know more about remote access via NAT and VPN, see Remote Access.

6 Hardware

6.1 Layout

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

6.2 Mounting

The *Intesis KNX IP Router Secure* is designed for installation on a DIN rail with a width of 1 unit (18 mm).

6.3 Connections

- **Connection to the KNX TP bus**: Connect the *Intesis KNX IP Router Secure* to the KNX TP bus using its standard KNX connector 1.
- **Connection to the KNX IP backbone**: Connect the *Intesis KNX IP Router Secure* to the KNX IP backbone using its Ethernet connector 9.

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

6.4 Push Buttons

6.4.1 KNX Programming Mode Button

Use this button 3 to enable and disable the KNX programming mode.

TIP
You can also enable the KNX programing mode by pressing both Pass GAs 7 and Pass IAs 8 buttons simultaneously, provided the manual operation is not enabled in the router. See Manual Operation Mode with the Pass GAs and Pass IAs Buttons below.

This functionality can be enabled and disabled using ETS: From the **Parameters** tab select **General settings** and use the **Prog. mode on device front parameter** to select either:

- **Disabled**
- **Enabled** (default option)

When the KNX programming mode is enabled, both the programming LED 2 and the Mode LED 5 light up red.

6.4.2 Manual Operation Mode with the Pass GAs and Pass IAs Buttons

For testing and debugging purposes, the configured routing settings (filter or block) can be bypassed by enabling the manual operation mode.

- Short press (click) the **Pass GAs** button 7 to enable and disable the forwarding of grouped addressed telegrams.
- Short press (click) the **Pass IAs** button 8 to enable and disable the forwarding of individually addressed telegrams.

If one of these modes is enabled, the Mode LED 5 flashes orange once each second. If both modes are enabled, the Mode LED 5 flashes orange twice each second.

Instead of clicking again the button to exit the manual operation mode (**Esc**), you can click both **Pass GAs** 7 and **Pass IAs** 8 buttons simultaneously.

This functionality can be configured using ETS: From the **Parameters** tab select **General settings** and use the **Manual operation on device** parameter to select either:

- **Disabled**
- **Enabled with time limit 1 min**
- **Enabled with time limit 10 min**
- **Enabled with time limit 30 min**
- **Enabled without time limit** (default option).

6.5 LED Indicators

6.5.1 KNX LED

Overview of the different indications of the KNX LED 4:

Color	Pattern	Description
Green	Solid	The device is powered
	Flickering	Telegram traffic on the KNX bus
Red	Shortly	Communication failures

6.5.2 Mode LED

Overview of the different indications of the Mode LED 5:

Color	Pattern	Description
Green	Solid	Standard operation mode
Red	Solid	Programming mode is active
	Flashing	Loading error, e.g., after an interrupted download
Orange	Flash x1	• Manual operation is active • Forwarding IA **or** GA
	Flash x2	• Manual operation is active • Forwarding IA **and** GA

6.5.3 IP LED

Overview of the different indications of the IP LED 6:

Color	Pattern	Description
Green	Solid	• Active Ethernet link • Valid IP settings
	Flickering	IP telegram traffic
Red	Solid	• Active Ethernet link • Invalid IP settings or IP settings not received from DHCP server yet

7 Reset to Factory Settings

To reset the *Intesis KNX IP Router Secure* to its factory settings, follow this procedure:

1. Disconnect the KNX connector 1 from the device.
2. Press the KNX programming button 3 and keep it pressed down.
3. Reconnect the KNX connector 1 to the device.
4. Keep the KNX programming button 3 pressed for at least another six seconds.

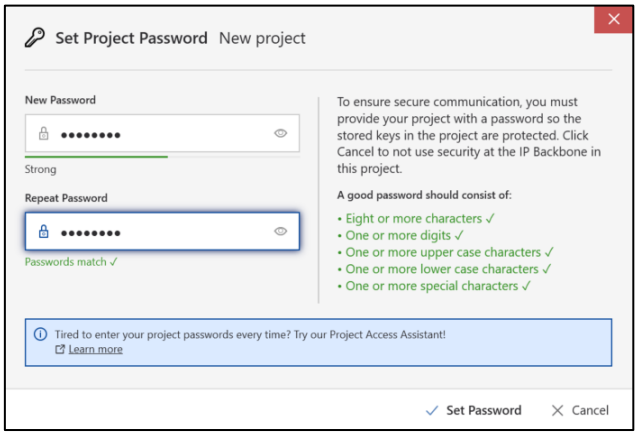
A short orange flash of all LEDs (2 4 5 6) indicates a successful reset of the *Intesis KNX IP Router Secure* to its factory default settings.

8 Configuration with ETS

8.1 ETS database

The ETS database (ETS 5.7 or higher) can be downloaded from the product page, via the KNX online catalogue, or by clicking here.

When importing the *Intesis KNX IP Router Secure* to your project, ETS will prompt you to set a project password.



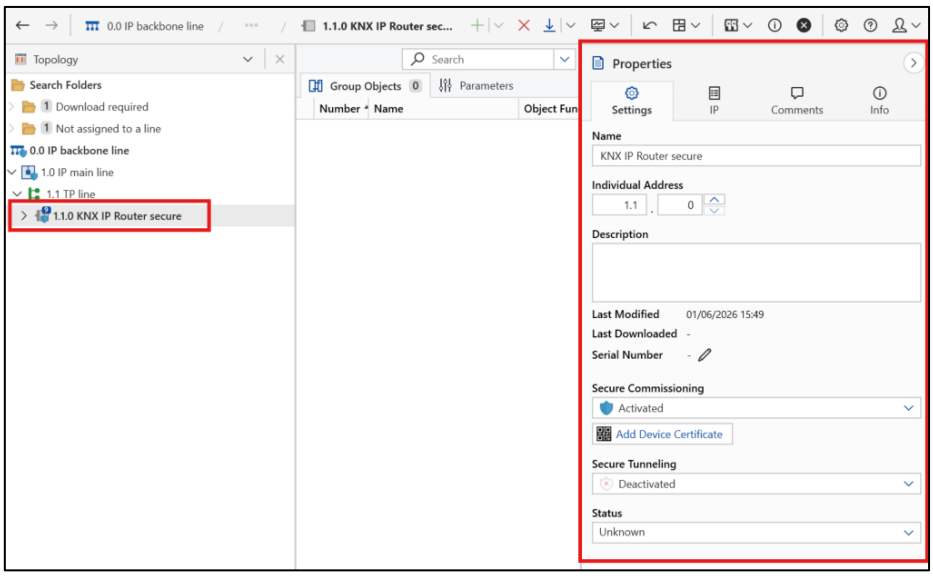
Enter the password and click **Set Password**.

A new dialog will ask if you also want to secure the tunneling interfaces.

You can set the password and activate the security for the tunneling interfaces later from the **Properties** -> **Settings** menu.

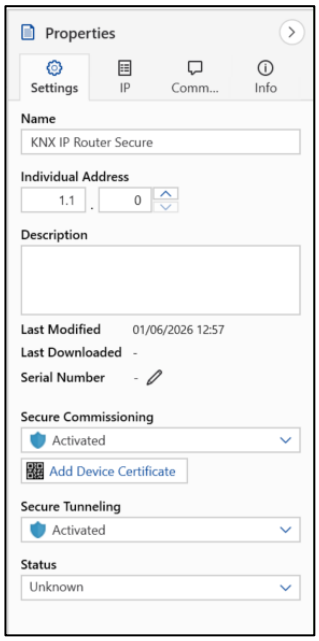
8.2 Properties Menu

Select the *Intesis KNX IP Router Secure* from the **Topology** panel to habilitate its **Properties** menu.



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

8.2.1 Settings Tab



Name: Type a name.

Individual Address: Type the individual address.

The individual address assigned to the *Intesis KNX IP Router Secure* determines whether it operates as a line or area coupler:

- If the individual address is in the form of x.y.0 (x, y: 1 .. 15), it operates as a line coupler.
- If the individual address is in the form of x.0.0 (x: 1 .. 15), it operates as an area coupler.

Description: Type a description.

Secure Commissioning: Use this option to set a project password, if you haven't yet. When this option is activated, two new options appear in the **IP** tab, showing a commissioning password and an authentication code. See IP Tab.

Add Device Certificate: This certificate contains the serial number and the factory default setup key (FDSK) of the *Intesis KNX IP Router Secure*.

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

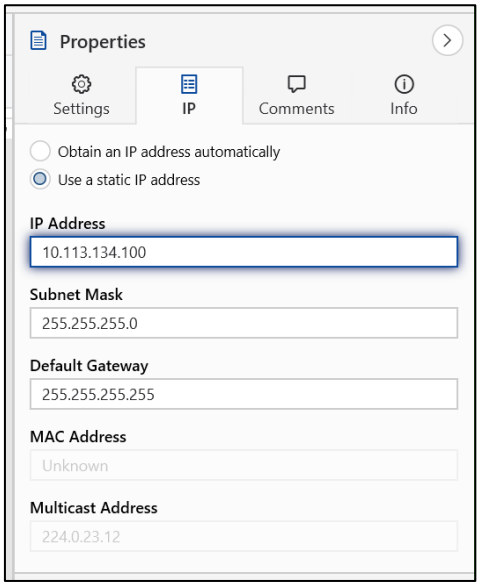
The device certificate is just an initial key required to safely put a device into operation from the start. During the first secure download, the initial key is replaced by ETS with a new key that is generated individually for each device.

The initial key is only reactivated after a master reset.

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

Secure Tunneling: Use this option to secure IP tunneling connections, if you haven't yet. If activated, a password is assigned to each additional KNXnet/IP tunneling interface. See Additional KNXnet/IP Tunneling Interfaces.

8.2.2 IP Tab



Obtain an IP address automatically (default option): The DHCP server on the IP network will automatically assign an IP address to the *Intesis KNX IP Router Secure.*

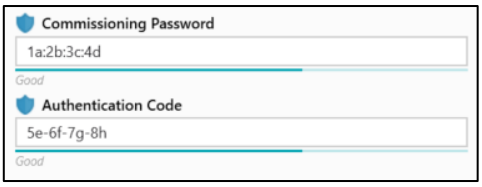
To use the automatic IP address assignment, a DHCP server must be present on the LAN.

Use a static IP address: Select this option to assign an IP address manually.

IP Address: Type an IP address for the *Intesis KNX IP Router Secure.*

Subnet Mask: Type the subnet mask according to the IP address.

Default Gateway: If needed, type the IP address of the gateway (e.g., the DSL router connected to the KNX installation).

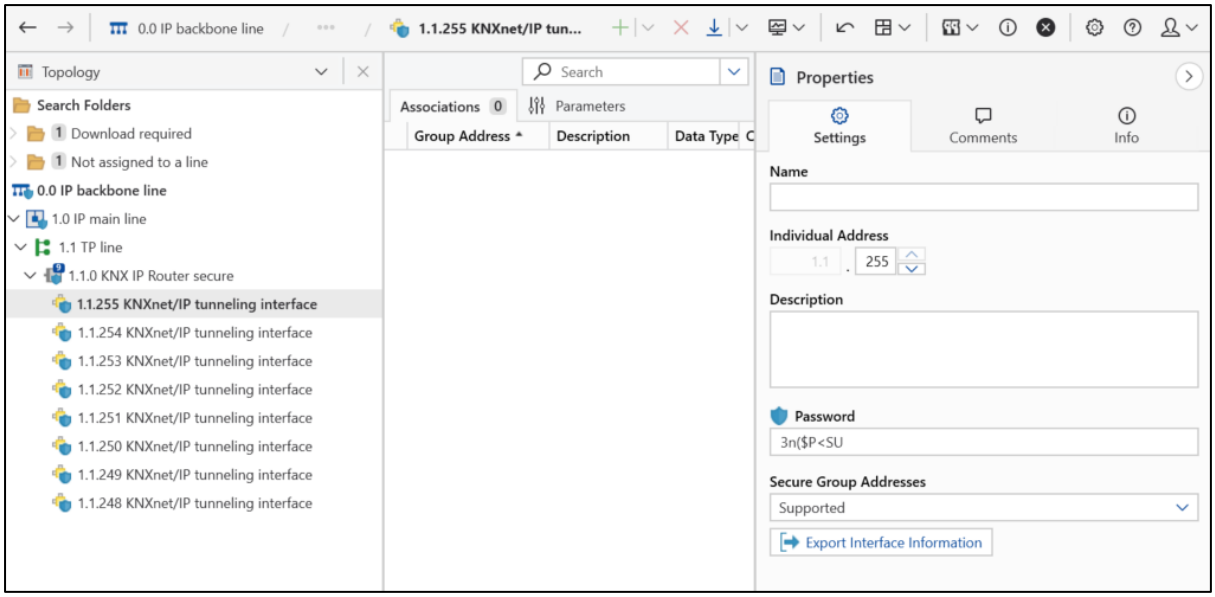


If the **Secure Commissioning** and **Secure Tunneling** options are activated in the **Settings** tab, two more options appear here:

The **Commissioning Password** and the **Authentication Code** are used for a secure connection to the *Intesis KNX IP Router Secure* from ETS.

8.2.3 Additional KNXnet/IP Tunneling Interfaces

For the interface function, the *Intesis KNX IP Router Secure* implements eight additional KNXnet/IP tunneling interfaces that are visible when expanding the device element in the **Topology** view.



KNXnet/IP tunneling interfaces are used by client devices (e.g., a PC running ETS, a visualization server, etc.) for connecting to the KNX installation via the IP network.

Select the desired **KNXnet/IP tunneling interface** to open its **Properties** menu.

Name: Type a name.

Individual Address: Type the individual address.

Set an individual address within the address range of the bus line in which the *Intesis KNX IP Router Secure* is installed.

The individual address cannot be used by any other device.

Each individual address is associated with a connection. Thus, when a client (e.g. ETS) sends telegrams to the bus through the *Intesis KNX IP Router Secure*, it is identified with the assigned additional address. In the same way, response telegrams can be clearly transmitted to the respective client.

Description: Type a description.

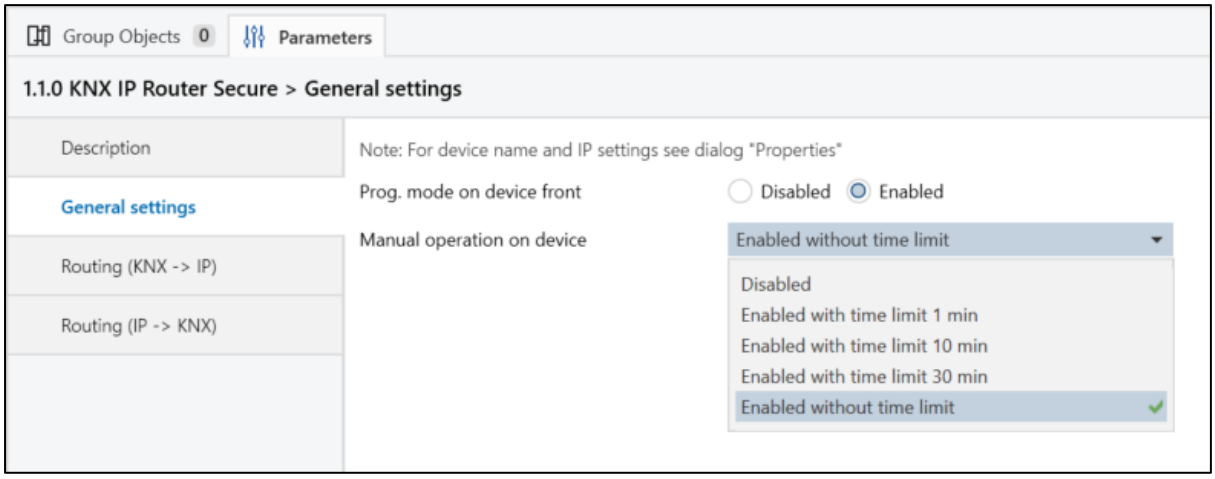
Password: If **Secure Tunneling** is activated in the **Settings** tab, a unique password will be created automatically for each tunnel.

Secure Group Addresses: Select whether the secure group addresses function is **Supported** or **Not Supported**.

Export Interface Information: Generate a KNX keyring file (*.knxkeys) containing the group address information assigned to the tunnel.

8.3 Parameters

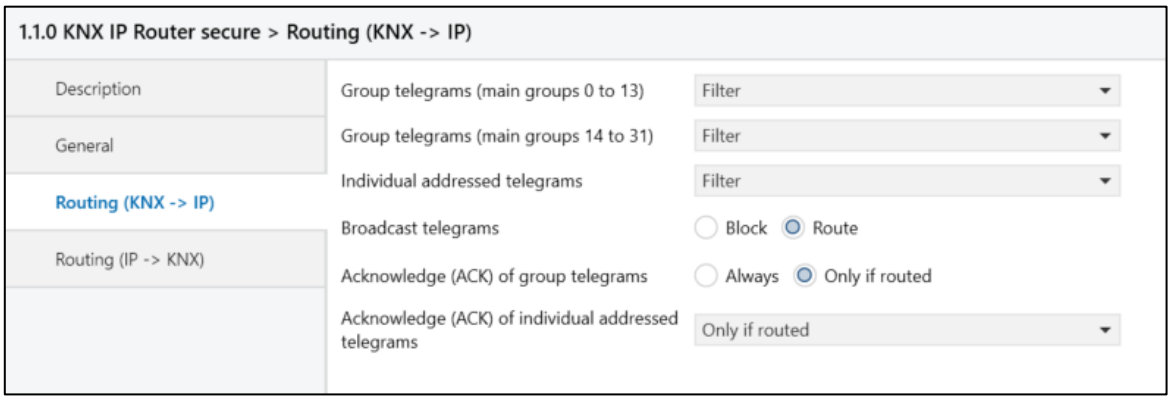
8.3.1 General settings



Prog. mode on device front: When enabled, in addition to the normal programming button, the *Intesis KNX IP Router Secure* allows activating and deactivating the programming mode by pressing simultaneously both **Pass GAs** 7 and **Pass IAs** 8 buttons.

Manual operation on device: This parameter sets the duration of the manual mode. Upon completion the normal display mode is restored.

8.3.2 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** (default option): The filter table is used to check whether the received group telegram should be routed to IP or not.

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** (default option): The filter table is used to check whether the received group telegram should be routed to IP or not.

Individually addressed telegrams:

- **Block**: No individually addressed telegrams are routed to IP.
- **Route**: All individually addressed telegrams are routed to IP.
- **Filter** (default option): 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** (default option): All received broadcast telegrams are routed to IP.

Acknowledge (ACK) of group telegrams:

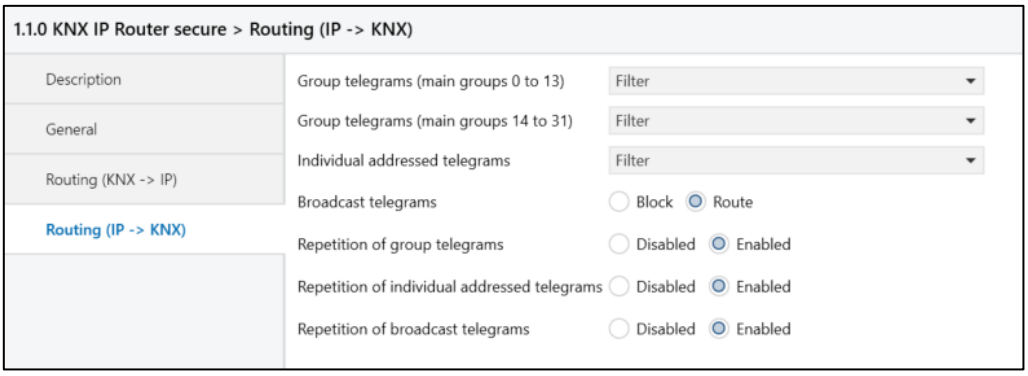
- **Always**: An acknowledge is generated for every received group telegram (from KNX).
- **Only if routed** (default option): An acknowledge is only generated for received group telegrams (from KNX) if they are routed to IP.

Acknowledge (ACK) of individually addressed telegrams:

- **Always**: An acknowledge is generated for every received individual addressed telegram (from KNX).
- **Only if routed** (default option): 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.

When using **Answer with NACK,** accessing the device via KNX TP is no longer possible. The configuration must be performed via IP.

8.3.3 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** (default option): 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** (default option): 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** (default option): 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** (default option): 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** (default option): 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** (default option): 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** (default option): The received broadcast telegram is resent up to three times in case of a fault.

8.4 Programming

The *Intesis KNX IP Router Secure* can be programmed in different ways from ETS:

8.4.1 Programming Through the KNX Bus

For this method, an additional interface (e.g., a USB interface) is required to allow ETS access to the KNX bus.

You just need to connect the *Intesis KNX IP Router Secure* to the KNX bus. The individual address and the entire application, including the IP configuration, can be programmed.

Programming via the bus is recommended if no IP connection can be established.

8.4.2 Programming Through KNXnet/IP Tunneling

No additional interface is required.

Programming via KNXnet/IP Tunneling is possible if the *Intesis KNX IP Router Secure* already has a valid IP configuration.

In this case the *Intesis KNX IP Router Secure* is displayed in the ETS menu used to manage connections, whose location varies depending on the ETS version.

8.4.3 Programming Through KNXnet/IP Routing

No additional interface is required.

Programming via KNXnet/IP Routing is possible if the *Intesis KNX IP Router Secure* already has a valid IP configuration.

In this case, ETS uses the PC's network interface as the communication endpoint. Therefore, ETS displays the available network adapters of the PC rather than the *Intesis KNX IP Router Secure* itself.

ETS menu for managing connections will list all the network interfaces available on the PC. Ensure you select the correct one.

TIP
The correct PC network interface will be on the same IP network as the *Intesis KNX IP Router Secure.* You can use the ipconfig command on Windows to check the IP address of each network adapter.

8.4.4 Programming Through Direct IP Connection

This method is recommended, since the *Intesis KNX IP Router Secure* configuration can be loaded at a high speed.

No additional interface is required.

Programming via direct IP connection is possible if the *Intesis KNX IP Router Secure* already has a valid IP configuration as well as an individual address.

8.5 Remote Access

Remote access to the KNX TP installation via Internet is possible with the *Intesis KNX IP Router Secure*.

Remote access can either be carried out using Network Address Translation (NAT) or Virtual Private Network (VPN). In addition to selecting the type of access, it is also possible to secure the KNX network using KNX Security.

8.5.1 Remote access with NAT

Remote access via NAT, without further safety measures, poses significant dangers. Port forwarding provides universal access to your local IP network and your KNX system. Any Internet user can discover the open port on your static public IP address and can, for example, access your KNX network via the ETS software.

We strongly advise using NAT only temporarily for testing or diagnostic purposes. After that, close the port again to prevent abuse.

If remote access is realized through NAT, do NOT use port 3671 as the external port (the port towards the Internet). 3671 is the official port for eFieldControl(EIBnet) registered by

KNX Association and can be easily determined by unauthorized persons. Please use a port in the non-reserved range between port 50000 and port 60000.

In the following sections, the generic term **network gateway** is used instead of *router* or *modem* to refer to the device connected to the KNX installation that provides Internet access. This distinction helps differentiate it from the *Intesis KNX IP Router Secure* and avoids potential confusion.

8.5.1.1 Necessary Settings in the Network Gateway

1. Open the configuration interface of the network gateway connected to the KNX installation.

2. Enter the section to allow external access.

This section is often called Port Forwarding, NAT, Permit Access, or similar.

Set the parameters as needed.

- **External port**: Use a port in the non-reserved range between port 50000 and port 60000.

- **Internal IP address**: Set the IP address of the *Intesis KNX IP Router Secure*.

- **Internal port**: Set the port of the *Intesis KNX IP Router Secure*.

Apply the changes to save the port forwarding in the network gateway.

8.5.1.2 IP Configuration of the Intesis KNX IP Router Secure

If you haven't already assigned a valid IP address to the *Intesis KNX IP Router Secure*, do so now as explained in **IP** Tab.

Use the **Default Gateway** parameter in the **IP** tab to set the IP address of the network gateway.

8.5.1.3 Establishing an IP Tunneling Connection with ETS

This process varies depending on your version of ETS.

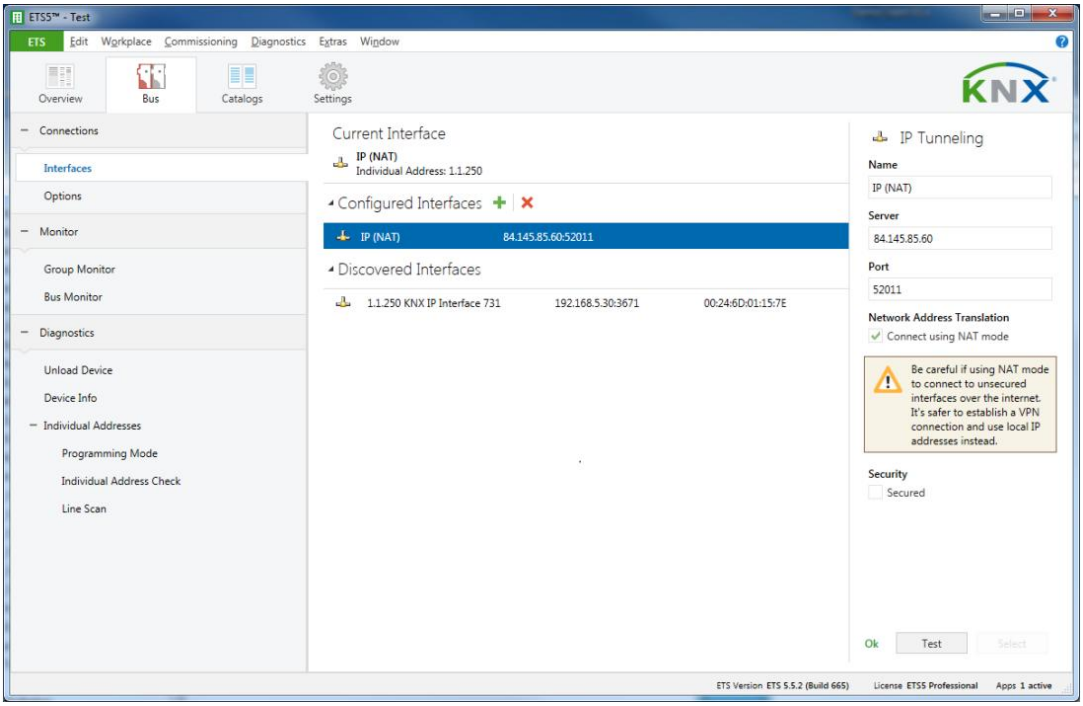
In ETS5, the menu to manage connections is located in **Bus -> Connections -> Interfaces**.

In ETS6, this menu is located in **Bus -> Manage Configured Connections**.

1. Enter the connections manager.
2. Add a new interface.
3. Set the needed parameters:

- **Name**: Type a name.
- **Server**: Set the public IP address of the network gateway.
- **Port**: Set the port specified as the external port in the network gateway's settings.

4. Ensure that the **Connect using NAT mode** option is checked.



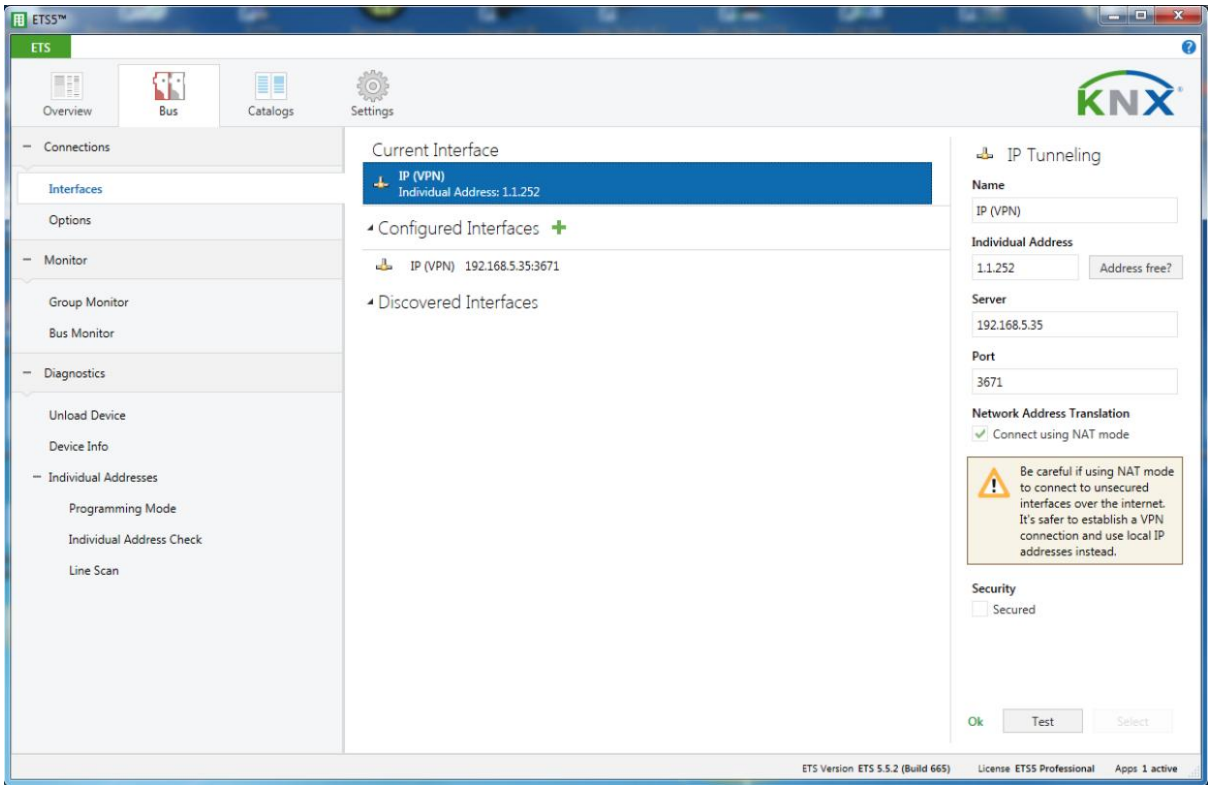
8.5.2 Remote Access with Virtual Private Network (VPN)

To establish a VPN tunnel, the VPN server functionality must be configured on the network gateway connected to the KNX installation. Additionally, a VPN client must be configured on the PC used to access the installation.

The procedure for setting up the VPN server on the network gateway and the VPN client on the PC requires vendor-specific configuration software and is not covered in this manual. Refer to the network gateway documentation for all the information required to complete the procedure.

8.5.2.1 Accessing the Intesis KNX IP Router Secure Remotely with the ETS

Once you have added the VPN connection to the network gateway, configured the VPN client on the PC, and established the connection between them, you must establish an ETS connection via the VPN connection.



It is not possible for ETS to identify the interface automatically via the Internet, so you must set the needed parameters manually.

1. Enter the **Bus** menu.
2. In the **Connections** parameter, select **Interfaces**.
3. Create a new interface.
4. Set the needed parameters manually:

- **Server**: Set the static IP address of the Intesis KNX IP Router Secure.
- **Port**: Set the Intesis KNX IP Router Secure port.

5. Ensure that the **Connect using NAT mode** option is checked.

Although the connection is not established in NAT mode, this option enables certain initializations that are necessary for a KNXnet/IP connection.