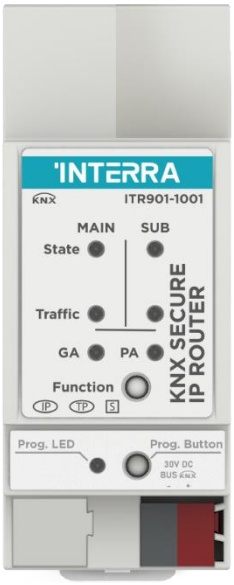
INTERRA

Developer of Uniqueness

KNX Secure IP Router

System Device

Product Manual



PM2405200219AEN

Contents

1. Content of The Document 6

2. Product Description 7

2.1. Technical Information 8
2.2. Connection Features 9
2.3. Device Commissioning 11
2.4. Secure Commissioning 12
2.5. Dimensions 13
2.6. Functionality 14
2.7. KNXNET/ IP 15
2.7.1. IP Secure Tunnelling 15
2.7.2. IP Secure Routing 15
2.7.3. IP Firmware Update 15
2.9. Operational Description 17
2.9.1. IP Secure Router Application 17
2.9.2. IP Network 17
2.9.3. KNX Network Installation: 18
2.9.4. Adding Device Certificate 19
2.9.5. Programming 20
2.9.5.1. Physical Address Assignment 20
2.9.5.2. IP Configuration 21
2.9.6. Special Functions 22
2.9.6.1. Manual Function 22
2.9.6.2. Restore Factory Settings 23
2.9.6.3. IP Firmware Update Request 23
2.9.6.4. Led Status Display 24

3. ETS Parameters & Descriptions 26

3.1. General Page 27
3.1.1. Parameters List 27
3.2. IP Configuration 28
3.2.1. Parameters List 28
3.3. KNX Multicast Address 29
3.3.1. Parameters List 29
3.4. Main Line (IP) 30

3.4.1. Parameters List 30
3.5. Subline (KNX TP) 31
3.5.1. Parameters List 32
4. WEB FRONT-END 33
4.2. Accessing the Device Web Front-End 34
4.2.1. Access via Windows Network UPnP 34
4.2.2. Access via IP Address 34
4.2.3. Access via MAC Address 35
4.3. Device Info 36
4.4. KNX 37
4.5. Firmware Update & Boot Mode 38
4.6. IP Tunnelling Address Assignment 40

Information in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets your specifications.

INTERRA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR NONSTATUTORY, RELA-TED TO THE INFORMATION INCLUDING BUT NOT LIMITED TO ITS CONDITION, QUALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR PURPOSE.

Interra disclaims all liability arising from this information and its use. Use of Interra devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Interra from any damages, claims, suits, or expenses resulting from such use. No licenses are implicitly or otherwise conveyed under any Interra intellectual rights.

Trademarks

The Interra name, logo and the Interra ITR901-1001 KNX Secure IP Router device are registered trademarks of Interra Technology in Turkey and other countries.

All other trademarks mentioned herein are property of Interra Technology.

Printed on recycled paper.

TS EN ISO 9001:2008

TO OUR CUSTOMERS

One of our most important aims is to provide you with the best documentation possible to use successfully your Interra products. Focusing on this, we will keep on improving our documentation to better suit your needs. Our publications will be updated as new volumes as soon as changes are introduced.

If you have any questions or comments regarding this publication, do not hesitate to contact us:

E-Mail: info@interratechnology.com

Tel: +90 (216) 326 26 40 Fax: +90 (216) 324 25 03

Most Current Product Manual

To obtain the most up-to-date version of this product manual, please visit our Web site at:

http://www.interratechnology.com

You can determine the version of an Interra document by examining its literature number found on the bottom right corner of any page.

The first two letters of the literature are the type of document. The following numbers are the document's creation date and the last letter is the version (e.g., PM181017001A is version A of a product manual created on 17/10/18).

1. Content of The Document

This document contains Interra ITR901-1001 KNX Secure IP Router electronic and all essential feature information for programming the products. In each subtitle is explained the characteristics of the device. Modifications of the product and special change requests are only allowed in coordination with product management.

This manual provides detailed technical information concerning ITR901-1001 KNX Secure IP Router. All the models have the same software functionality so, the features described in this document apply to all versions.

This user manual is intended for use by KNX installers and describes the functions and parameters of the ITR901-1001 KNX Secure IP Router devices and how it is possible to change the settings and configurations using the ETS software tool. This document also describes the installation, programming, commissioning and use of the devices with detailed information.

2. Product Description

ITR901-1001 is a KNXnet/IP routing & tunnelling secure device and works as KNX IP line/area coupler. An external power supply is not necessary. The ability to address all bus devices in the KNX bus system makes network operations less time-consuming. Operational and filtering states, malfunction and faulty communication are indicated by LEDs. UPnP is available and the firmware can be updated by a comfortable Web front-end. Long messages with up to 240 bytes APDU length are supported. For IP Secure Tunnelling, four (password-protected) Tunnelling channels are available.

ITR901-0001 connects the two communication media Ethernet/KNX IP and KNX TP to feature (for all bus devices connected):

- Secure commissioning
- Addressing
- Setting Parameters
- Secure tunnelling
- Protocol
- Diagnostic operations

ITR901-1001 is able to filter the traffic according to the installation place in the bus system hierarchy and according to the built-in filter tables for group oriented communication. Con- figuring from the subline can be blocked. Message filtering can be temporarily deactivated by a single button press. The time period to automatically switch back to normal operation is ETS-configurable. To ease commissioning, temporary access to other lines is possible also without download from the ETS.

2.1. Technical Information

The following table shows the technical information of the ITR901-1001 KNX Secure IP Router.

Product Code	ITR901-1001
Power Supply	21-30 V DC, KNX Bus Voltage
Current Consumption	< 20 mA
Connection	RJ45 Ethernet Connector KNX Connector
Maximum APDU	240 Byte
Push Buttons	1 x Programming Button 1 x Function Button
LED Indicators	1 x Programming LED 6 x Operate LEDs
Type of Protection	IP 20
Temperature Range	Operation (-5°C...45°C) Storage (-20°C...60°C)
Maximum Air Humidity	< 93 RH
Colour	Light Grey
Mounting Type	On 35 mm DIN-Rail
Dimensions	90 x 36 x 71 mm (H x W x D)
Certification	KNX Certified
Configuration	Configuration with ETS

2.2. Connection Features

The figure below shows the KNX Secure IP Router. All of the ITR901-1001 models have the same connection layout.

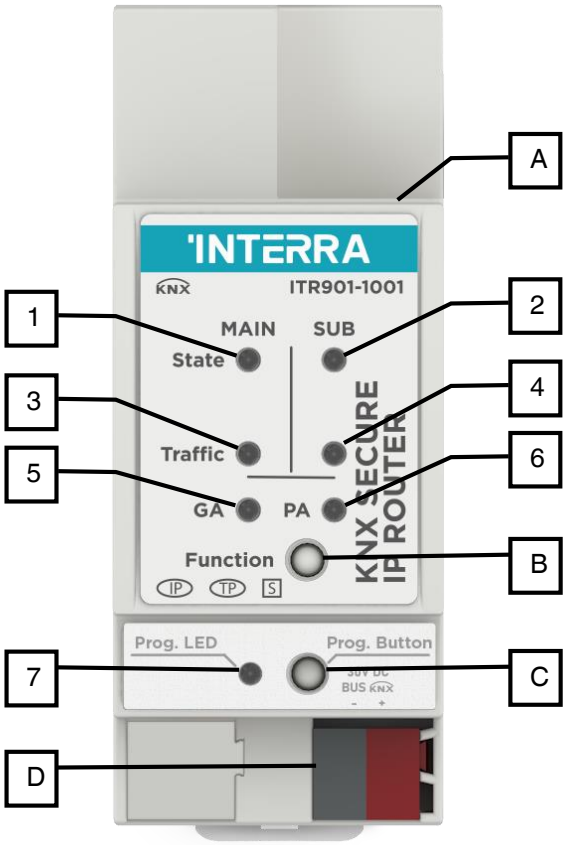


Fig. 1: Connection Features of KNX Secure IP Router

	LED		BUTTON / CONNECTOR
1	State IP (Main Line)	A	Ethernet Connector
2	Bus State KNX TP (Sub line)	B	Function Button
3	Telegram Traffic IP (Main Line)	C	Program Button
4	Telegram Traffic KNX TP (Sub line)	D	KNX TP Connector
5	Group Address(GA) Routing (0....13)		
6	Physical Address (PA) Routing		
7	Programming		

Table 1: LEDs and Buttons Definitions

Letter	Feature	Description
1	State IP (Main Line)	Green: IP line OK. Red: Manual Function active. Off: No IP connection
2	Bus State KNX TP (Subline)	Green: Subline OK. Off: Subline not connected
3	Telegram Traffic IP (Main Line)	Blinking Green: Telegram traffic extent indicated by blinking (Speed up to 10 Mbit/s). Off: No telegram traffic.
4	Telegram Traffic KNX TP (Subline)	Blinking Green: Telegram traffic extent indicated by blinking. Blinking Red: Transmission error. Off: No telegram traffic.
5	Group Address Routing	Green: Filter table active. Orange: Route all. Red: Block all. Off: Routing of Group Telegrams is different on main line and subline.
6	Physical Address Routing	Green: Filtering active. Orange: Route all. Red: Block all. Off: Routing of Physical Telegrams is different on main line and subline.
7	Programming	Red: Program Mode/ Boot Mode active. Blinking Red: No IP connection. Off: Program Mode/Boot Mode not active.

Note: If the device is used as IP Router without physical address x.y.0, the "physical address routing" named LED 6 (PA) works not like described at Table 1.

2.3. Device Commissioning

The default settings of the device are:

- All telegrams are blocked due to the filter table is not defined.
- The Manual Function switch-off time is 120 min.
- Physical address is “15.15.0”.
- Never connect the device to 230 V.

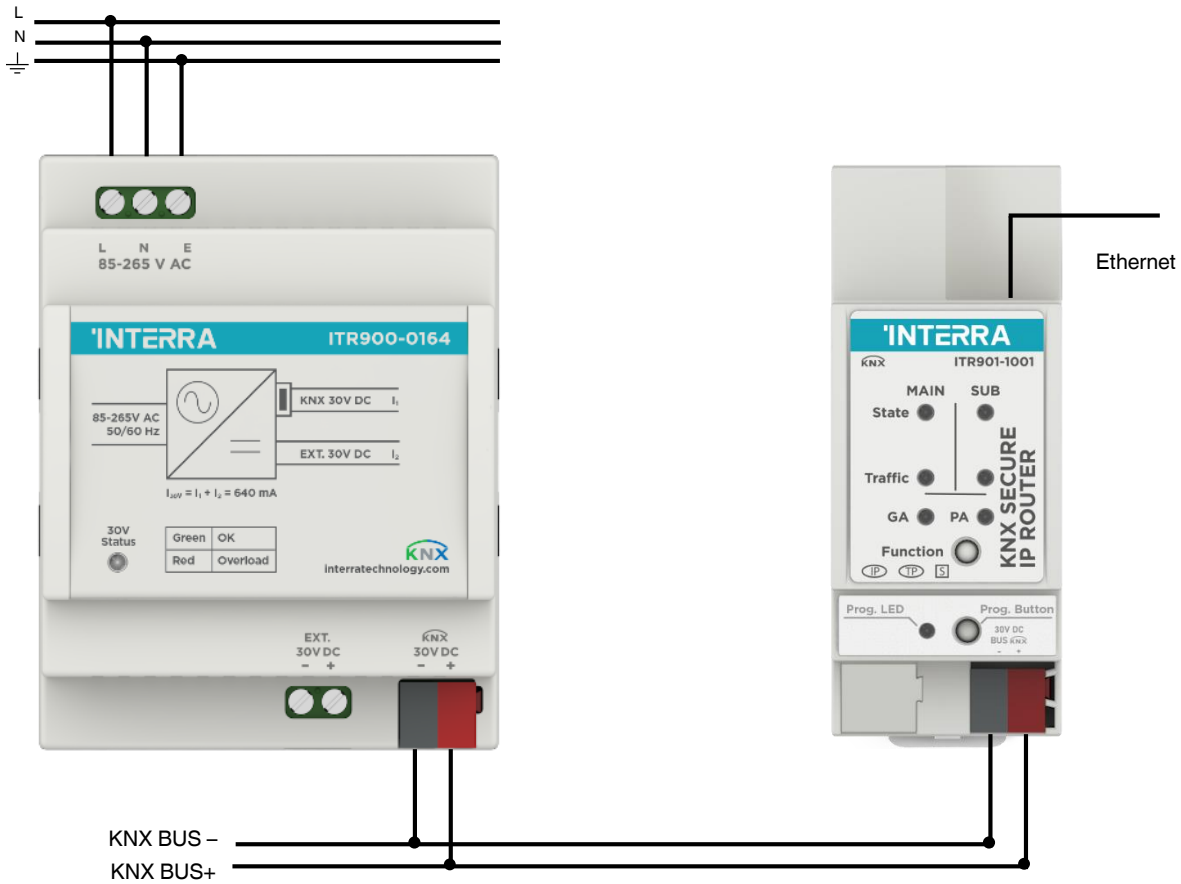


Fig. 2: Connection Scheme

2.4. Secure Commissioning

Before the secured download of a configuration setting and/or the Individual Address can start, the individual Device Certificate of KNX Secure IP Router must have been added to the ETS project. To be able to add it, the ETS project must be password-protected.

- A secured download is only possible after activation of Secure Commissioning.
- Activation of Secure Commissioning demands the individual Device Certificate.
- Device Certificates can only be added to a password-protected ETS project.

When no project password is set, Secure Commissioning cannot be activated. ETS projects with having Secure Commissioning and/or IP Security set to active always require pre-setting a project password. Having no project password set on activation, the ETS then asks to type it in.

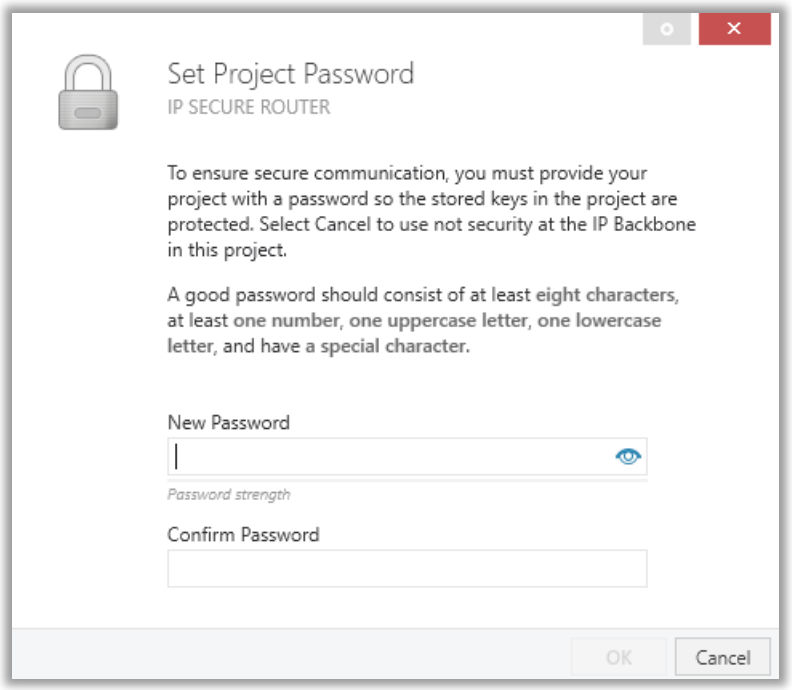


Fig. 3: Password Window

The individual Device Certificate always is enclosed with a KNX Secure product. To keep the product fully configurable by the user, it is important to make sure the Device Certificate cannot be lost.

2.5. Dimensions

All values given in the device dimensions are millimetres.

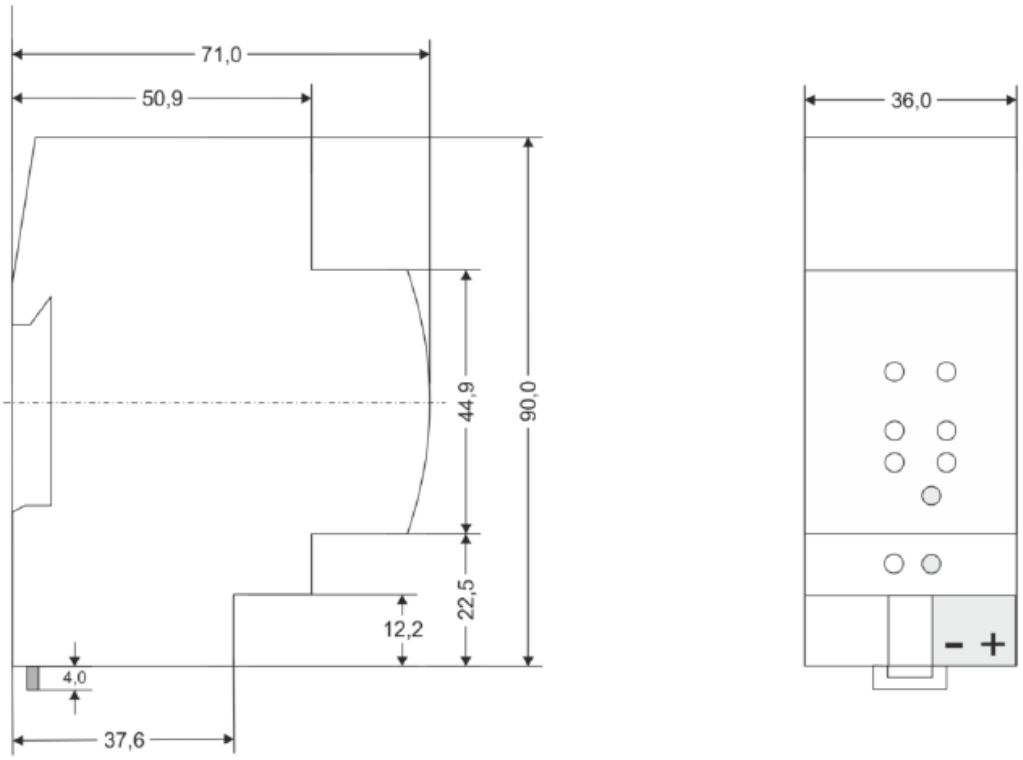


Fig. 4: Dimensions of KNX Secure IP Router

2.6. Functionality

- ITR901-1001 KNX IP Secure Router supports extended frames and long telegrams up to 240 bytes APDU length.
- When the ETS “Secure Commissioning” function is active, configuration data is downloaded only in encrypted KNX Data Secure format.
- Activation of “IP Backbone Security” for protection of IP routing.
- ITR901-1001, favourably replaces a common TP line/area coupler. The great advantage is using KNX IP as a fast KNX backbone medium (for sending telegrams between lines and areas).
- ITR901-1001 works without external power supply.
- On activation of Secure Tunnelling, the password protection becomes available. Four different tunnelling connections with a separate address for each can be realized in parallel.
- Settings to increase data throughput and decrease high bus traffic are featured.
- IACK sending on sent out messages is ETS configurable.
- When there is no IACK response on the subline the Interra KNX IP Secure Router is able to repeat messages up to three times. Repetitions can be configured for both Physical Telegrams and Group Telegrams via ETS (to ease troubleshooting). After an IACK response no repetition is following and the negative IACK/BUSY failure mechanism is maintained.
- Automatic function for switching back to run-time telegram filtering after configurable suspension period. This avoids forgetting the reactivation of filtering.
- For an ETS configurable time period, it is possible to switch off telegram filtering by only pressing a button on the device front panel. Without additional ETS download filtering is suspended. This is necessary for running fast diagnostics on site.
- Temporarily suspending telegram filtering eases commissioning and debugging. Without ETS download temporary access to other lines becomes possible.
- UPnP is available to discover the device within the IP network. This can only be realized by a proper network installation in terms of topology. With use of KNXnet/IP ETS is able to recognize the communication interface device.
- Updating the firmware can easily be accomplished by a Web browser. The available Web front-end provides informative settings and enables to switch the device into Program Mode without use of the Program Button.
- In networks with high busload the internal amount of communication buffers are capable of smoothing peeks in the communication load course.
- With the web front-end, a 60 min busload history diagram can be watched.
- For Security, the web front-end can fully be disabled or be set to display only status info.
- ITR901-1001 supports KNXnet / IP, ARP, ICMP, IGMP, HTTP, UPnP, UDP/IP, TCP/IP, DHCP and AutoIP.

2.7. KNXNET/ IP

ITR901-1001 is a KNX IP Secure Router and KNX IP Secure Routers are highly similar to TP line couplers. The only difference is that they use the IP communication medium as main line and the KNXnet/IP communication protocol. However, KNX end devices can be integrated directly via IP. This makes the Ethernet a real KNX medium.
As documented in the KNXnet/IP protocol specifications, KNX telegrams can also be transmitted encapsulated in IP telegrams. Ethernet networks as well as Internet can be used to route and tunnel KNX telegrams. In this way, IP interfaces and IP routers are an alternative to USB data interfaces and TP line/area/backbone couplers. In the latter case, the normal TP backbone is replaced by a fast Ethernet based line.

2.7.1. IP Secure Tunnelling

KNXnet/IP enables KNX connections via IP tunneling. These point-to-point IP Tunneling connections are typically used to connect clients such as ETS or supervision systems to the KNX installation. When "Secure Tunneling" is enabled, these connections, also known as IP Secure Tunneling, become secure. This means that each channel's data exchange is encrypted, and passwords can be used to protect individual channels.

2.7.2. IP Secure Routing

Regarding KNX topology, KNX TP lines and areas can be interconnected using an Ethernet/IP network, referred to as a KNX IP (backbone) line. KNX IP media couplers facilitate the transfer of KNX data between TP and IP, functioning as KNX IP routers for this purpose.
For data communication on KNX IP, specifically between KNX IP devices, the fundamental protocol used is KNXnet/IP for IP Routing. When IP Security is enabled, the standard IP Routing protocol is replaced by the IP Secure Routing protocol, ensuring that KNX IP communication is fully encrypted in accordance with the KNX Secure security framework. The aspect of KNX Secure relevant to IP is known as KNX IP Secure.

2.7.3. IP Firmware Update

To enable remote firmware updates via IP, the KNX Secure IP Router includes an integrated bootloader functionality. This feature, known as IP Firmware Update, can be executed through the web frontend. The download process for rewriting the program memory content operates independently from ETS, replacing both the communication stack and the application software.

2.8. KNX Secure

KNX devices that support KNX Secure utilize telegram encryption for enhanced protection. Access to these devices for configuration is restricted to users who possess the Device Certificate. This certificate is a unique protection code provided with the device upon delivery. To leverage KNX Secure protection, each KNX Secure device operates in a secure mode. When secure mode is activated, commissioning, configuration, and runtime communication are encrypted, safeguarding the device against unauthorized access and manipulation. Activation requires the Device Certificate (see chapter 2.4 Secure Commissioning).
In secure mode, the KNX Secure device can read and send encrypted telegrams. If secure mode is deactivated, the device functions like a standard KNX device without KNX Secure support (referred to as a plain KNX device). KNX Secure devices in secure mode and plain devices cannot be combined in the same group object. However, it is possible to have a mixed installation that includes both secured and plain devices.

Mixing unsecure and secure communication on the same group address is impossible. Additionally, a combination of KNX IP Secure couplers in secure mode and plain KNX IP Secure couplers cannot be configured when IP Backbone Security is enabled.

Encrypted KNX telegrams processed by secured devices can be distinguished between those intended for KNX IP Secure and those for KNX Data Secure:

- **KNX IP Secure** can only be applied to the KNX IP medium. KNX Secure telegrams are sent as encrypted IP Secure frames, regardless of whether KNX Data Secure is used or not.
- **KNX Data Secure** can be applied to any KNX communication medium. End-to-end communication, specifically group communication for one or more certain group objects, is encrypted. Due to an individual security key, only end devices with identical Group Addresses can encrypt and decrypt the telegrams within their secured group.

To program a KNX Secure device, ETS must know its FDSK (Factory Default Setup Key) and serial number. However, it is not necessary to manually enter the FDSK or serial number. ETS retrieves this information from the Device Certificate, a device-specific 36-character code containing both the serial number and the FDSK. These cannot be modified.

After adding a KNX Secure device and its Device Certificate to the ETS project, ETS automatically sets the project-specific Tool Key, which is then used for programming. This Tool Key cannot be modified and can only be deleted by performing a device reset (see chapter 2.9.6.2. Restore Factory Settings). After the reset, ETS uses the registered FDSK to access the device and program a new Tool Key.

2.9. Operational Description

In KNX network installations, the KNX Secure IP Router is used as a KNX IP line/area coupler to connect KNX IP and KNX TP (see also chapter 2.7.2. IP Secure Routing). It can operate in plain mode, without security activation, and in ETS projects where security is active.
After connecting to KNX TP, the KNX Secure IP Router operates with its default settings. For KNX IP routers, only Individual Addresses in the format x.y.0 can be set. Assigning the correct Individual Address is necessary for proper telegram transmission and functioning within the installation.

2.9.1. IP Secure Router Application

During normal operation, the KNX Secure IP Router operates according to its filter settings. When the router receives telegrams addressed to specific Individual Addresses (such as during commissioning), it compares the destination Individual Address with its own to determine whether it needs to route the telegrams. For telegrams addressed to group addresses, only those with group addresses listed in the filter table are routed.

If the KNX Secure IP Router forwards a telegram to the TP line without receiving an acknowledgement—due to a missing receiver or a transmission error—the telegram may be repeated up to three times, depending on the ETS configuration. This repetition behaviour can be configured for both types of telegrams using the "Repetitions if errors..." parameter, although it is recommended to use the default setting.

The KNX Secure IP Router application is designed for use in 10/100 BaseT networks compliant with IEEE802.3. The Autosensing feature automatically sets the baud rate to either 10 Mbit or 100 Mbit. The IP address can be obtained from a DHCP server by configuring the router in ETS to "obtain an IP address automatically." If no DHCP server is found, the router initiates an AutoIP procedure to assign an IP address automatically. For a fixed IP configuration (including IP address, subnet mask, and default gateway), these settings can also be specified through ETS.

2.9.2. IP Network

ITR901-1001 sends telegrams from/to the TP network to/from the IP network in accordance with the KNXnet/IP protocol specification. According to the default setting these telegrams are sent as multicast telegrams to the multicast IP address 224.0.23.12 port 3671. The multicast IP address 224.0.23.12 is the defined address for the KNXnet/IP by KNX Association in conjunction with the IANA. It is recommended to use this default address as defined. Only if it becomes necessary due to the existing network, the address can be changed as shown in chapter 3.3 KNX Multicast Address.

Key Notes:

- All KNX IP devices that are intended to communicate with each other via IP must have the same IP multicast address.
- Multicast IP address 224.0.23.12 may need to be changed in respect of the network type and of the network components´ settings.
- IGMP (Internet Group Management Protocol) is used for IP configuration to establish multicast group belonging.
- If the IP address is changed from the IP side it may happen that ETS does no longer recognize the device and connection cannot be maintained (tunnelling uses IP addresses).
- It is recommended to trigger a restart and to change IP addresses only from TP side.
- If problems occur for IP address assignment, please ask your network administrator.
- According to the topology, the Tunnelling addresses always have to be assigned in the range of subline addresses. For more information about additional physical addresses for tunnelling please check the section 4.5.
- Programming devices of another line different to which the device used for (re)programming is connected the use of a correct topology is mandatory.

2.9.3. KNX Network Installation:

For line coupler functionality in a KNX network the ITR901-1001 device has to use the correct physical address of a line coupler (X.Y.0, 1≤X & Y ≤15). In ETS up to 225 addresses can be defined (from 1.1.0 to 15.15.0). For area coupler functionality in a KNX network ITR901-001 has to use the correct physical address of an area coupler (X.0.0, 1≤X≤15). In ETS up to 15 areas can be defined.

If ITR901-1001 is used in a KNX system for both purposes, it is only necessary to ensure that the ITR901-1001 used as a line coupler has a line coupler address assigned from a free addressing area. Following figure illustrates the ITR901-1001 router topology for KNX lines and KNX areas.

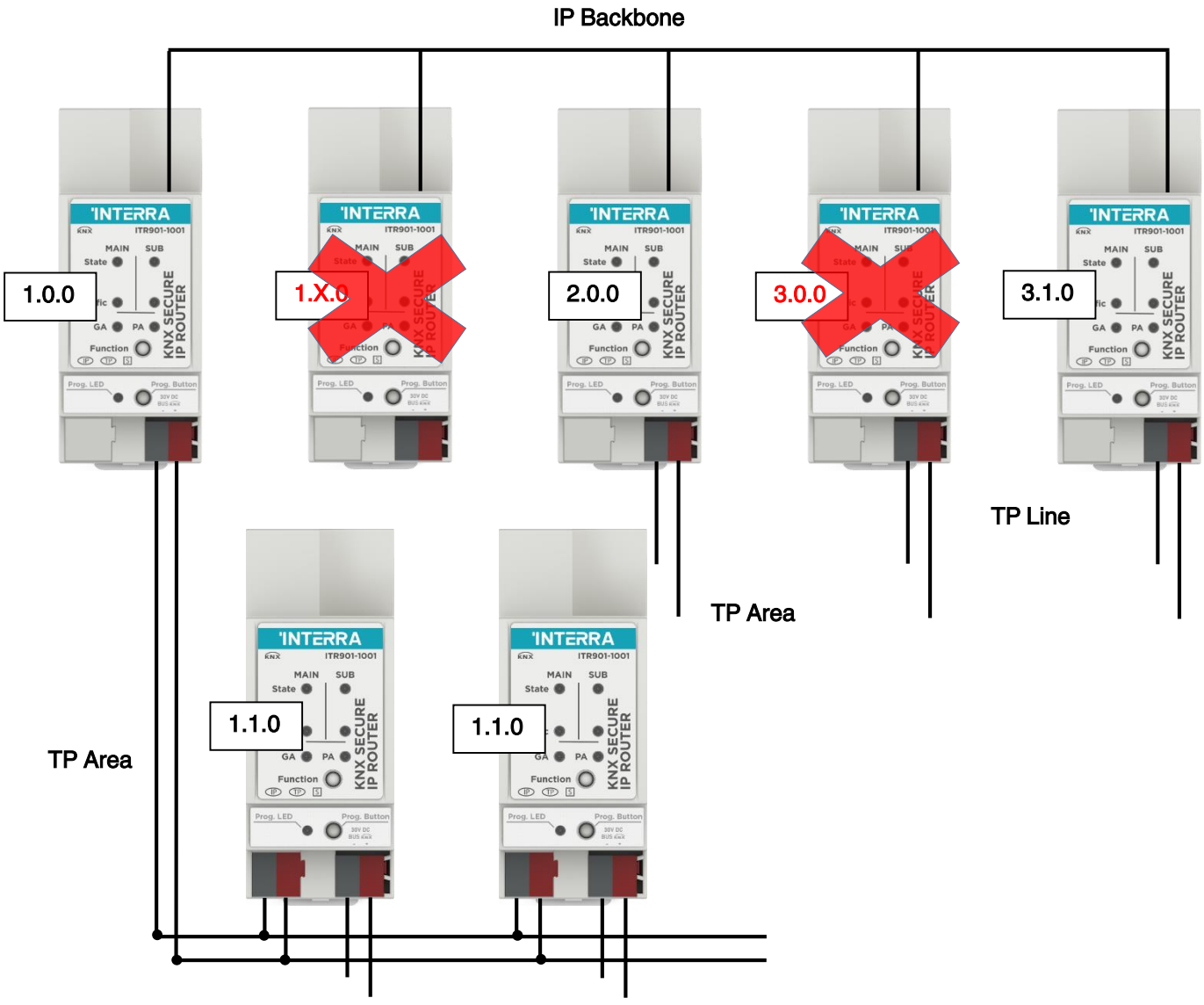


Fig. 5: Interra KNX Secure IP Router Network Topology

Example: If an IP router with address 1.0.0 already exists on the backbone no IP router with address 1.X.0, 1≤X≤15 can be added here. Even if no line coupler with address 1.1.0 exists on the subline of the 1.0.0 IP coupler. Vice versa, if a line coupler with address 1.1.0 already exists in the installation no IP router with address 1.0.0 can be added.

2.9.4. Adding Device Certificate

The Device Certificate, unique to each KNX Secure device, is typically printed on a side label on the device housing. It is essential to enter this Device Certificate into ETS before activating or utilizing any KNX Security functions.

The Device Certificate can be entered into the system manually or by scanning the QR code included on the tear-off part of the Device Certificate side label using a webcam.

Fig. 6: Interra KNX Secure IP Router Device Certificate Enable

After opening the project, the Device Certificate list can be edited. In the Security tab under Project Overview Device Certificates can be added and deleted.

When the Device Certificate list does not contain the Device Certificate of a specific secure device, the following window appears upon starting the secure download into this device. At this point, the QR code must be scanned, or alternatively, the 36-character code of the Device Certificate must be entered manually to proceed.

Fig. 7: Interra KNX Secure IP Router Adding Device Certificates

2.9.5. Programming

2.9.5.1. Physical Address Assignment

The Individual Address (IA) can be assigned to the KNX Secure IP Router by setting the desired address in the properties window of ETS. After downloading the IA into the device, the KNX Secure IP Router can be addressed and identified by its new Individual Address.

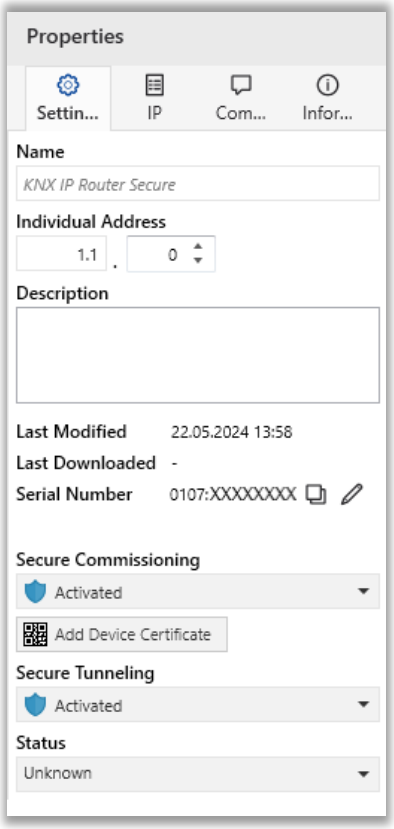


Fig. 8: ETS Properties Window

To download the Individual Address into the device, Programming Mode must be active. Successive pressing of the Programming Button toggles Programming Mode on and off. When LED 7 lights up red, it indicates that Programming Mode is on. Once the download is started in ETS, the Programming Button needs to be pressed. After that, the new Individual Address is stored in the device's memory.

To program devices on a different line than the one to which the ETS Current Interface device is connected, ensuring a correct topology is mandatory.

The device comes with the Individual Address 15.15.0 as the Factory Default Setting. It is advisable not to use this address for regular operation and instead assign a different address during commissioning.

A blinking red Programming LED indicates the Ethernet cable is not properly connected or no IP network connection is available.

2.9.5.2. IP Configuration

The IP configuration of the KNX Secure IP Router can be adjusted in the Properties window of the ETS. To activate DHCP/AutoIP, select the "Obtain an IP address automatically" option. For further guidance and details on configuring IP networks, it's recommended to consult your local network administrator.

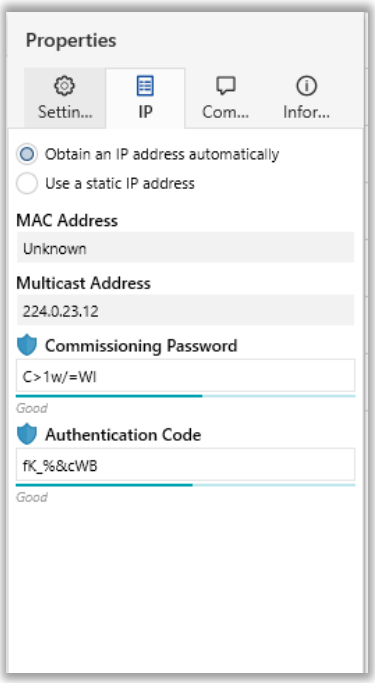


Fig. 9: Automatic IP Address Assignment

When the “Use a static IP address” option is chosen, IP address, Subnet Mask and Default Gateway can be set manually.

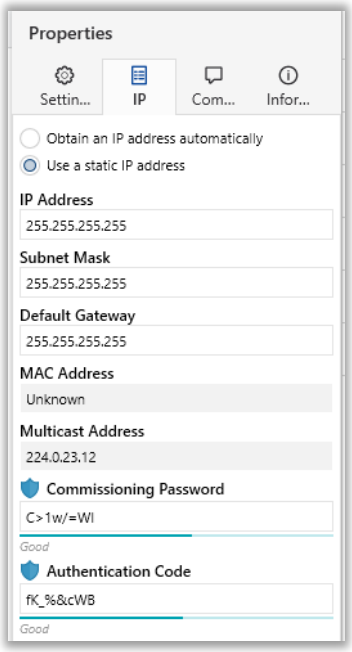


Fig. 10: Manual IP Address Assignment

KNX IP devices that aim to communicate via the IP (Secure) Routing protocol must be configured to use the same Multicast Address. Modification of the Multicast Address is achievable solely through the IP (configuration) tab located within the Backbone's Properties window, which becomes accessible upon selecting the blue Topology bar.
When KNX Secure IP Router is designated as the ETS Current Interface and its IP address undergoes a change through a configuration download, ETS attempts to sustain the connection to the Current Interface with the prior IP address. Specifically, the former IP address remains visible in the IP Tunneling window, and ETS indicates that the Current Interface is unreachable. The updated KNX Secure IP Router, with its new IP address, appears under Discovered Interfaces and must be selected to re-establish it as the Current Interface.

2.9.6. Special Functions

The Function Button on the KNX Secure IP Router device enables the activation of its special functions: Manual Function and Factory Reset. The Manual Function configures the device to a specific filter setting, while the Factory Reset reverts KNX Secure IP Router to its original factory settings. The Function Button must also be pressed during the Firmware Update procedure. The status of these active special functions is displayed via the LED indicators.

2.9.6.1. Manual Function

During normal operation, a brief press (approximately 3 seconds) activates or deactivates the Manual Function. LED 1 indicates whether the function is active, while LEDs 5 and 6 display the current filtering states. When the Manual Function is engaged, KNX Secure IP Router allows either all Physical Telegrams, all Group Telegrams, or both to pass through without filtering. Once the predefined switch-off time has elapsed, KNX Secure IP Router reverts to normal operation automatically. The Manual Function and switch-off time can be configured via the General parameter tab, as detailed in chapter 3.1. General. Upon returning from Manual Function to normal operation, the most recent filter parameter settings and filter table entries are reactivated.

Step	Manual Function
1	Hold Function button for 3 seconds.
2	LED 1 now is orange indicating Manual Function is on.
3	After switch-off, normal operation is indicated by LED 1 lighting green.

Table 2: Activation of Manual Functions

2.9.6.2. Restore Factory Settings

To perform a Factory Reset, a long press (approximately 15 seconds) of the Function Button, immediately followed by a short press (approximately 3 seconds), is required. Upon the initial press, the LED display will illuminate as specified in Table 5: LED Status Display for Factory Reset after First Function Button Press. Following the second press, all parameters, including the Individual Address, will revert to factory defaults. Any set Tool Key will be deleted, and the FDSK will become the key used for reconfiguration. Thereafter, the LEDs will revert to displaying the normal operation status.

Step	Factory Reset
1	Hold Function button for 15 seconds
2	LEDs 1/2 now are orange
3	Hold Function button for 3 seconds
4	Device restarts

Table 3: Activation of Factory Reset

2.9.6.3. IP Firmware Update Request

To start the Firmware Update download process, a short press on the Function Button is necessary during Programming Mode is active. After a click on the “request update” button in the web front-end, KNX Secure IP Router switches to its boot mode and ‘Status: update authorized’ is indicated.

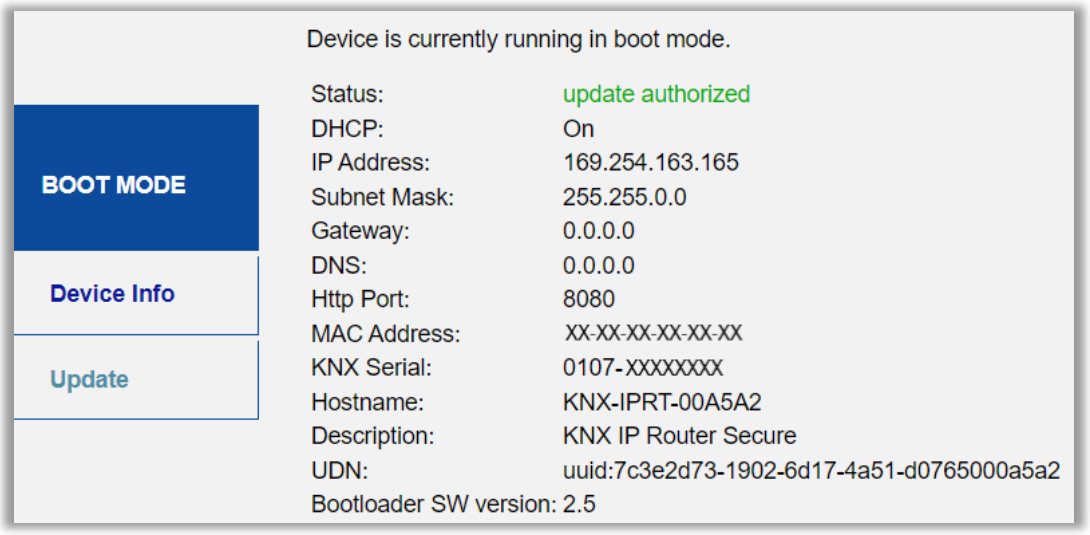


Fig. 11: Authorized Update Request

Step	Firmware Update
1	Short press on Program button
2	Short press on Function button
3	Click on “request update” in the web front-end
4	LED2 is blinking green
5	Firmware file can be selected
6	Device restarts

Table 4: Activation of Firmware Update

2.9.6.4. Led Status Display

NUMBER	LED	COLOUR	DESCRIPTION
1	State IP	Orange	Lights red if not connected.
2	Bus State KNX TP	Green	
5	Group Address Routing	Green Orange Red	Filter Route All Block All
6	Individual Address Routing	Green Orange Red	Filter Route All Block All

Table 5: LED Status Display for Manual Function

NUMBER	LED	COLOUR	DESCRIPTION
1	State IP	Orange	Lights red if not connected.
2	Bus State KNX TP	Orange	
5	Group Address Routing	Green Orange Red	Filter Route All Block All
6	Individual Address Routing	Green Orange Red	Filter Route All Block All

Table 6: LED Status Display for Factory Reset After First Button Press

NUMBER	LED	COLOUR	DESCRIPTION
1	State IP (Main Line)	Green	blinking, then lighting
2	Bus State KNX TP (Subline)	Blinking Green	
3	Telegram Traffic IP (Main Line)	Green	
7	Programming LED	Red	

Table 7: LED Status Display for Firmware Update

3. ETS Parameters & Descriptions

In this chapter, the ETS parameters of ITR901-1001-KNX IP Secure Router devices are described using the parameter pages and options. The parameter page features are dynamic structures which means further parameters and parameter pages are enabled depending on the configuration.

In the ETS parameter configuration pages, each of the parameters has got a default parameter value. These default values are written in bold.

- E.g.: Enable in operation ●**no** yes

3.1. General Page

If the host name is changed by a download in ETS4, a manual device restart (bus disconnection, reset of the line etc.) is recommended to take over this change.

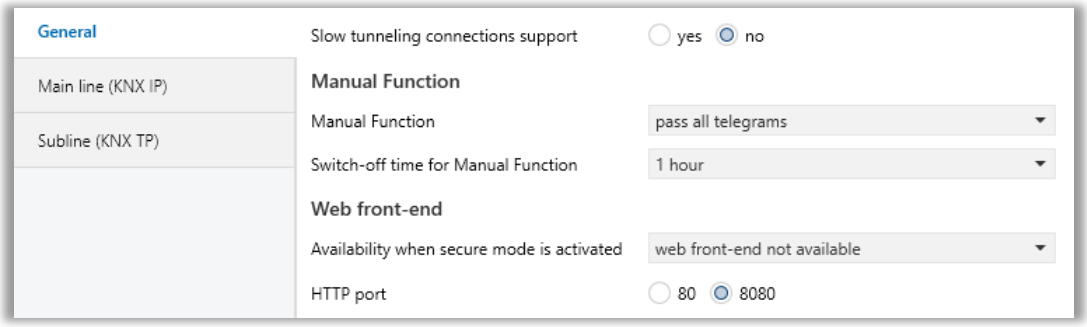


Fig. 12: General Tab Parameters

3.1.1. Parameters List

PARAMETER	DESCRIPTION	VALUES
Host name	Field to enter the device name providing an easy search of the device by ETS, by Windows Network and by KNXnet/IP visualisation systems.	30 Characters allowed (**KNX IP Secure Router**)
Slow tunnelling connections support	Enable to support slow tunnelling connections.	yes **no**
Switch-off time for Manual Function	After expiry of this time period the Manual Function is switched off automatically.	10 mins, **1 hour**, 4 hours, 8 hours
Manual Function		
Manual Function	Configuration setting for telegram routing when the Manual Function is active.	disabled **pass all telegrams** pass all Physical telegrams pass all Group telegrams **pass all telegrams**
Switch-off time for Manual Function	After expiry of this time period the Manual Function is switched off automatically.	10 min, **1 hour**, 4 hours, 8 hours
Web front-end		
Availability when secure mode is activated	When Security is switched on, the web front-end can be set to fully available (read/write), to available with limited usage (only readout) or be deactivated.	available having full functionality only status info display **web front-end not available**
HTTP port	Select the HTTP port.	80 **8080**

3.2. IP Configuration

After an ETS download IP addresses are not updated. It is essential to execute a manual device restart (bus disconnection, reset of the line) to get IP configuration data updated.

Fig. 13: IP Configuration Tab Parameters

3.2.1. Parameters List

PARAMETER	DESCRIPTION	VALUES
HTTP Port	Select one of the two official system ports.	80 **8080**
DHCP	If DHCP is used, no further IP parameters have to be set.	do not use **use**
IP address*1	Due to each part is 1 byte, the values should be adjusted by entering between 0 and 255.	0-255.0-255.0-255.0-255 **[0.0.0.0]**
Subnet mask*1	Due to each part is 1 byte, the values should be adjusted by entering between 0 and 255.	0-255.0-255.0-255.0-255 **[0.0.0.0]**
Default gateway*1	Due to each part is 1 byte, the values should be adjusted by entering between 0 and 255.	0-255.0-255.0-255.0-255 **[0.0.0.0]**
DNS server*1	Due to each part is 1 byte, the values should be adjusted by entering between 0 and 255.	0-255.0-255.0-255.0-255 **[0.0.0.0]**

*1This parameter, is only visible when the “DHCP” parameter is set to “do not use”.

3.3. KNX Multicast Address

For KNXnet/IP the multicast address “224.0.23.12” is the defined address from KNX Association in conjunction with IANA. Change this address only if it becomes necessary due to the existing network.
Make sure that during commissioning all KNX IP devices intended to communicate with each other via IP use the same multicast address. After downloading a new multicast address a manual restart has to be executed.

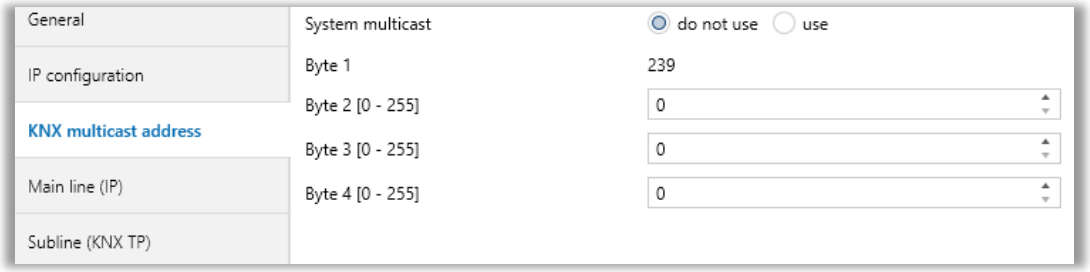


Fig. 14: KNX Multicast Address Parameter Page

3.3.1. Parameters List

PARAMETER	DESCRIPTION	VALUES
System multicast	System default multicast address is “224.0.23.12”. If system multicast is not used the multicast address has to be defined manually.	do not use **use**
Byte 1*[1]	If system multicast address is used “**224”** is set permanently. Otherwise “**239”** is set permanently.	224(System) **239**
Byte 2*[1]	Set manually if system multicast address is not used.	**0** (0-255)
Byte 3*[1]	Set manually if system multicast address is not used.	**0** (0-255)
Byte 4*[1]	Set manually if system multicast address is not used.	**0** (0-255)

*[1]This parameter, is only visible when the “System multicast” parameter is set to “do not use”.

3.4. Main Line (IP)

For Group Telegrams and Physical Telegrams the setting “transmit all” is intended only for testing purposes. Please do not use for normal operation.

Fig. 15: Main Line (IP) Parameter Page

3.4.1. Parameters List

PARAMETER	DESCRIPTION	VALUES
Telegram routing	Routing of Physical Telegrams and Group Telegrams can be set to ‘block’ (no routing), ‘filter’ (telegrams are routed according to filtering) and ‘route’ (all telegrams are transmitted). To set telegram routing different as available here, use ‘configure’.	Group: filter, Physical: block Group and Physical: filter **Group: route, Physical: filter** Group and Physical: route configure
Group telegrams : Main group 0...13*1	Filtering of Group telegrams (with main groups 0…13) can be configured to route all telegrams, no telegrams, or only telegrams entered in the filter table.	transmit all (not recommended) block **filter**
Group telegrams : Main group 14...31*1	Filtering of Group telegrams (with main groups 14…31) can be configured to route all telegrams, no telegrams, or only telegrams entered in the filter table.	transmit all (not recommended) block **filter**
Physical telegrams	Filtering of Physical telegrams can be configured to route all telegrams, no telegrams, or only telegrams according to their Individual Address.	transmit all (not recommended) block **filter**

*1This parameter, is only visible when the “Telegram routing” parameter is set to “configure”.

3.5. Subline (KNX TP)

For Group Telegrams and Physical Telegrams the setting “transmit all” is intended only for testing purposes. Please do not use for normal operation.

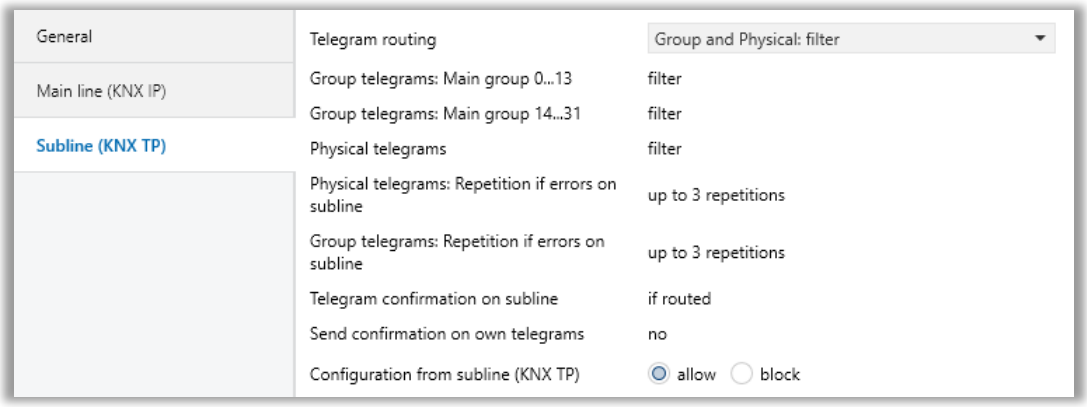


Fig. 16: Subline (KNX TP) Tab Parameters

3.5.1. Parameters List

PARAMETERS	DESCRIPTION	VALUES
Telegram routing	Routing of Physical Telegrams and Group Telegrams can be set to 'block' (no routing), 'filter' (telegrams are routed according to filtering) and 'route' (all telegrams are transmitted). To set telegram routing different as available here, use 'configure'.	Group: filter, Physical: block Group and Physical: filter **Group: route, Physical: filter** Group and Physical: route configure
Group telegrams: Main group 0...13*[1]	Filtering of Group telegrams (with main groups 0…13) can be configured to route all telegrams, no telegrams, or only telegrams entered in the filter table.	transmit all (not recommended) block **filter**
Group telegrams: Main group 14...31*[1]	Filtering of Group telegrams (with main groups 14…31) can be configured to route all telegrams, no telegrams, or only telegrams entered in the filter table.	transmit all (not recommended) block **filter**
Physical telegrams	Filtering of Physical telegrams can be configured to route all telegrams, no telegrams, or only telegrams according to their Individual Address.	transmit all (not recommended) block **filter**
Physical telegrams: Repetition if errors on subline	After subline transmission error (e.g. due to missing receiver), Physical telegrams can be not repeated, be repeated only once, or be repeated for max. 3 times.	no **up to 3 repetitions** one repetition
Group telegrams: Repetition if errors on subline	After subline transmission error (e.g. due to missing receiver), Group telegrams can be not repeated, be repeated only once, or be repeated for max. 3 times.	no **up to 3 repetitions** one repetition
Telegram confirmation on subline	Either only routed telegrams to IP main line are confirmed by an ACK on the subline or each telegram on the subline is confirmed by an ACK.	**if routed** always
Send confirmation on own telegrams	Telegrams sent out to the subline can be confirmed by an added ACK.	yes **no**
Configuration from subline (KNX TP)	'Block' means KNX Secure IP Router can only be configured from its main line side and configuring devices on main line (and behind) from the subline side is blocked.	**allow** block

*[1]This parameter, is only visible when the "Telegram routing" parameter is set to "configure".

4. WEB FRONT-END

The web front-end can be used to read out KNX Secure IP Router´s actual device settings (HTTP port, IP address, MAC address, …), to update the firmware and to set (additional) Individual Addresses for Tunneling. For identifying a certain KNX Secure IP Router in a KNX network, Programming Mode can be remotely switched on and off without having to press the on-device Programming Button.
To switch back from boot mode to normal operation it is necessary to run the firmware update procedure, then press abort, or wait for the 10 min timeout.

4.1. Protection of the KNX Secure IP Router Web Front-end

The web front-end can be used for remotely carrying out firmware updates, control functions and readout device settings. To raise protection for an installation, the web front-end availability is configurable. The highest degree is reached, when “not available” is set for normal runtime operation.
To use the remote functions of the web front-end, also when Security is active, it must be set to “available having full functionality”.

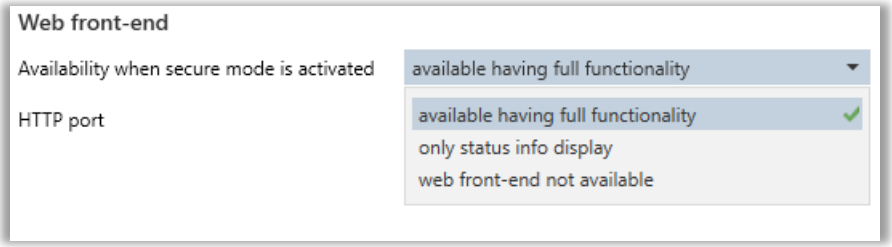


Fig. 17: ETS Parameter for Web Front-End Availability

When the web front-end is set to “only status info display”, remote control functions (Programming Mode activation, Set Tunneling) and the update function are off. Changing settings or parameters via IP is not possible, and only the informational readout is available.
To ensure full protection of a secured installation, the web front-end availability must be set to “web front-end not available” (default value).

For reasons of efficient protection, it is strictly recommended not to use the “available having full functionality” option on a permanent basis.

4.2. Accessing the Device Web Front-End

There are three ways to access the Interra KNX Secure IP Router. It can be accessed like a Microsoft Windows UPnP network device (Windows7 or later) and by a web browser. For access by a web browser either the IP address or the MAC address, together with the HTTP port, have to be known. How to use IP address and MAC address with the browser´s URL bar is described in the following.

Note1: For access via web browser the HTTP port that is set by ETS (or the factory default parameter value) has to be used.

Note 2: ITR901-001 is able to use both official HTTP system ports (80 and 8080).

Note 3: Factory default HTTP port is 8080.

4.2.1. Access via Windows Network UPnP

When the UPnP network function is enabled, ITR901-1001 Interra KNX Secure IP Router appears in the Windows Network. A click on the ITR901-1001 network device opens the Web front-end with the standard web browser. If Interra KNX Secure IP Router is not visible as an UPnP network device a manual restart is recommended. After that, the device becomes visible in the list of network devices.

4.2.2. Access via IP Address

When IP address and HTTP port (80 or 8080) are known, this information is sufficient to access the ITR901-1001 Web front-end by a web browser. The actual IP address is shown in the ETS list of Discovered Interfaces.

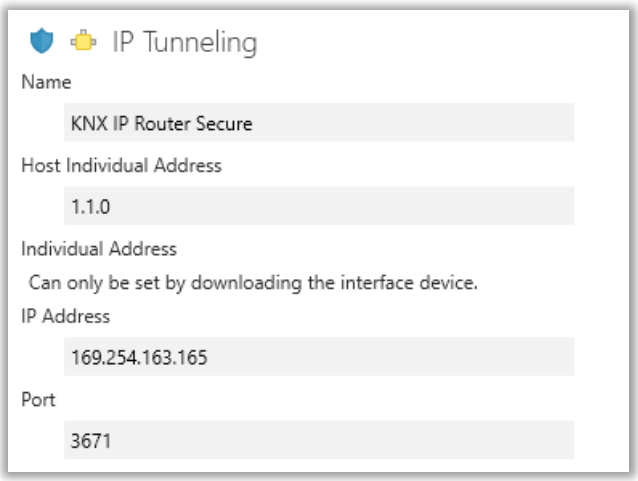


Fig. 18: Identifying KNX Secure IP Router IP address with ETS

According to KNX Secure IP Router pre-set IP configuration (HTTP port, IP address and DHCP), in the URL bar has to be entered (without brackets):

http://[IP address]:[HTTP port]/

The above box shows how to enter the IP address and HTTP port in the URL bar.

Ex 1: DHCP is not used. With the latest ETS download the IP address was set to 192.168.1.32 and HTTP port was set to 80. In the browser´s URL bar has to be entered “http://192.168.1.32:80/”.

Ex 2: With the latest ETS download HTTP port was set to 8080 and DHCP was activated. The DHCP server assigned a free IP address to KNX Secure IP Router and ETS shows this IP address to be 192.168.1.201. In the browser´s URL bar has to be entered “http://192.168.1.201:8080/”.

4.2.3. Access via MAC Address

When NetBIOS is installed (by default on Windows systems and Linux systems containing SAMBA) the MAC address that is printed on a label on the side of the ITR901-1001 housing can be used. Due to name resolution is mandatory to establish communication by Host name, activation of NetBIOS is necessary.

Use the MAC address in the form of AA-BB-CC-XX-YY-ZZ and the pre-set HTTP port to be entered in the browser´s URL bar as described here (without brackets):

http://knx-iprt-[XXYYZZ]:[HTTP port]/

Ex: On the housing side ITR901-1001 is labelled with MAC address D0-72-59-55-44-66 and the pre-set HTTP port is 8080. Then, in the web browser´s URL bar has to be entered “http://knx-iprt-554466:8080/”.
Note: The values to be entered in the browser bar are the values inside the quotation mark.

4.3. Device Info

After accessing the Web front-end the Device Info tab is shown. All general information about the current device settings is visible.

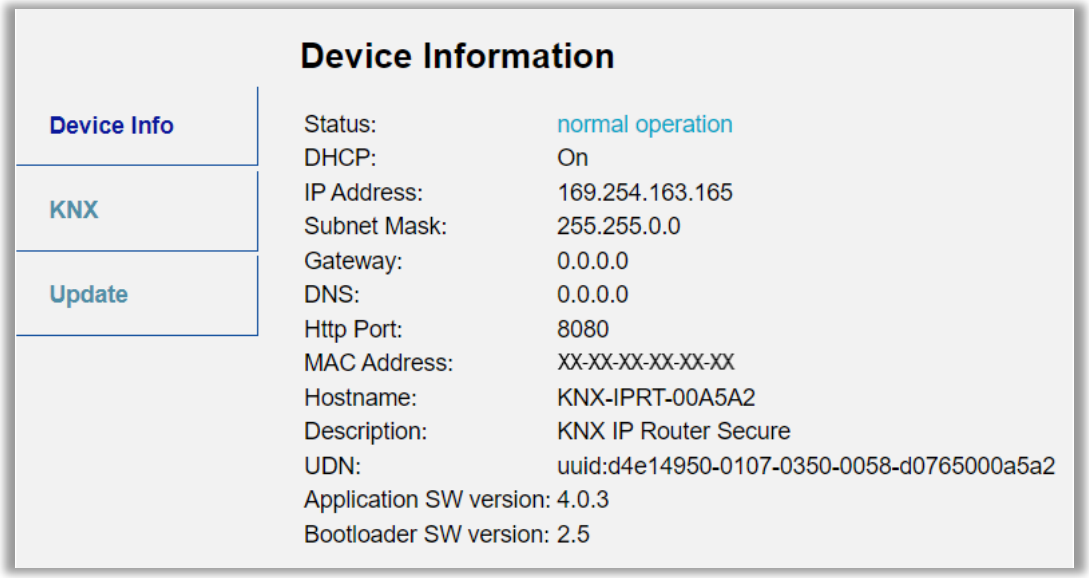


Fig. 19: Device Info Tab

4.4. KNX

With a simple click on “On” or “Off” Program Mode can be switched on/off. This function is equivalent to a Program Button press. Together with the Device Info tab it is easy to distinguish the regarded device (with a certain IP address or MAC address or serial number) from other similar devices in the same IP network. Also, setting changes can easily be checked.

Four tunnelling addresses can be set. ETS sets the first tunnelling address. With a click on “Set” the remaining ones are set. Moreover, routing multicast address, serial number of the device and a last-60-minutes KNX busload diagram are visible. The red curve shows the maximum busload history and the green one shows the average busload history both of the TP side.

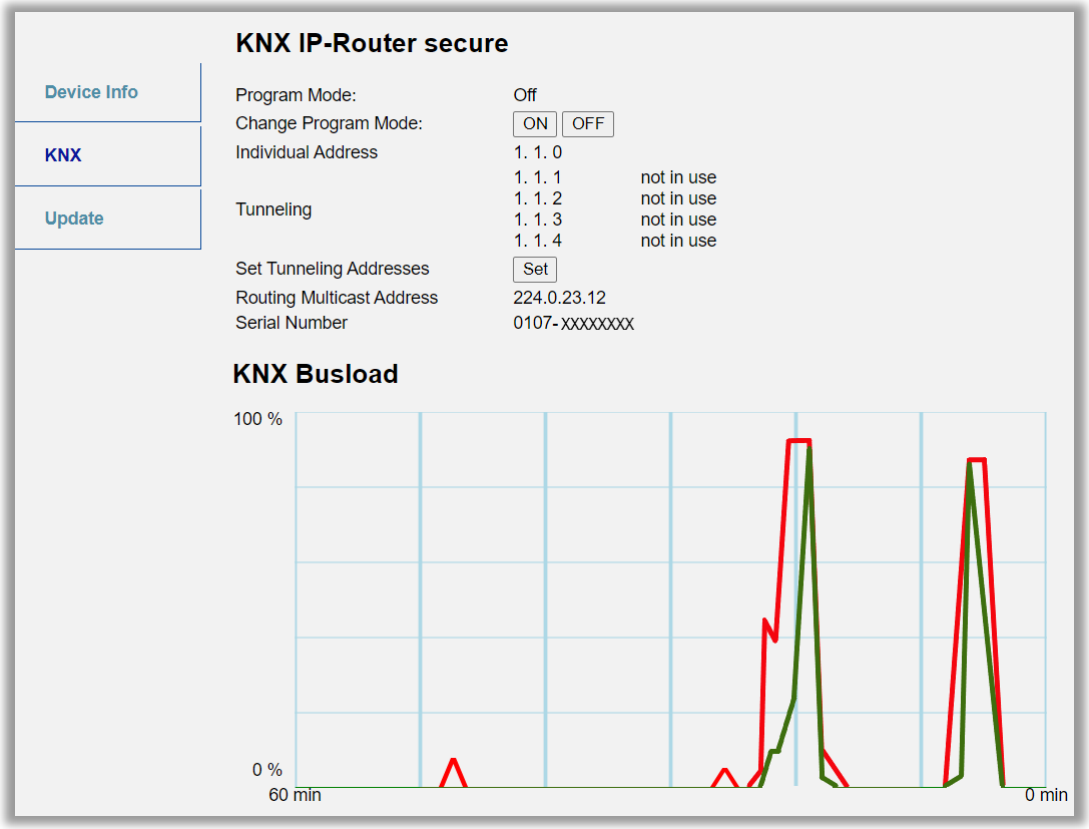


Fig. 20: KNX Tab

Note: The web browser used has to support SVG graphics.

4.5. Firmware Update & Boot Mode

Under the Update tab the ITR901-1001 firmware can be updated like described in following steps 1 to 5. During the firmware update process KNX Secure IP Router enters Boot Mode. Then LEDs 1, 2, 3, and 7 have states as described in Table 4.

Note 1: If Boot Mode is already active only the Web front-end instructions from step 3 to step 5 must be followed (refresh, request update).

Note 2: Boot Mode is still active after device reset and after factory reset.

To exit Boot Mode, it is necessary to enter the Update tab of the Web front-end. Then either the firmware update has to be completed (if a new firmware is available) or the firmware update process has to be stopped by a click on the “Abort” button. After that the device restarts and continues with normal operation.

Step 1: Open the Update tab of the Web front-end.

Fig. 21: Update Tab

Step 2: Activate Program Mode (at the KNX tab or by Program Button Press).

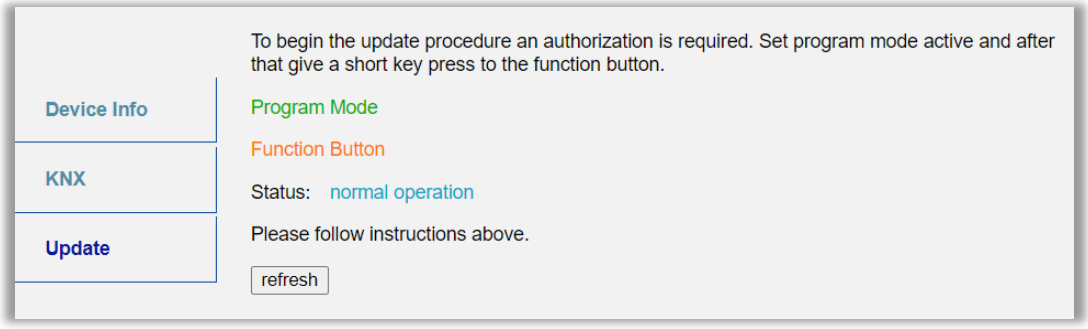


Fig. 22: Update Tab and activated Program Mode

Step 3: After Program Mode activation give a short press to the Function Button. Then click on the “refresh” button (alternatively, refresh the browser).

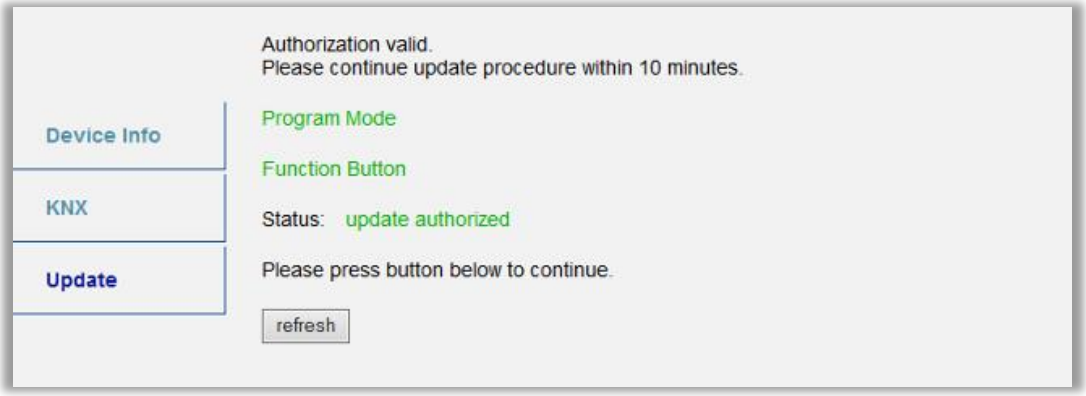


Fig. 23: Update Authorized

Step 4: When the “request update” button appears, it has to be pressed to select the update file and enter “Boot Mode”.

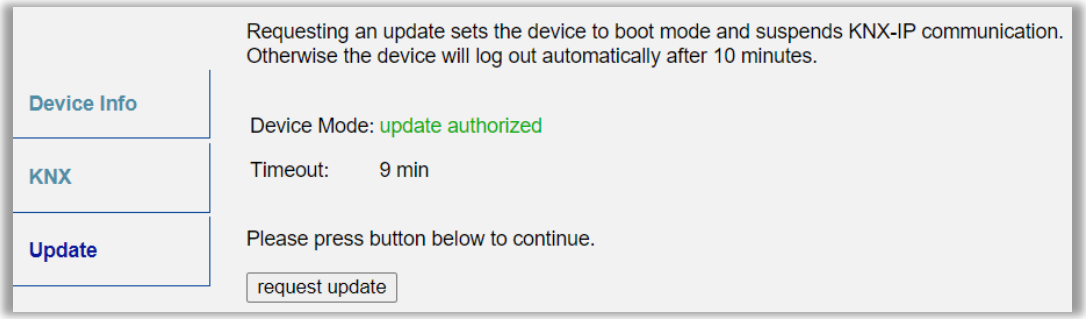


Fig. 24: Request Update

Step 5: The update file can be selected and be uploaded by a click on „Upload”. After that, the device exits boot mode and restarts. Clicking on the “Abort” button cancels the firmware update procedure and the device exits boot mode.

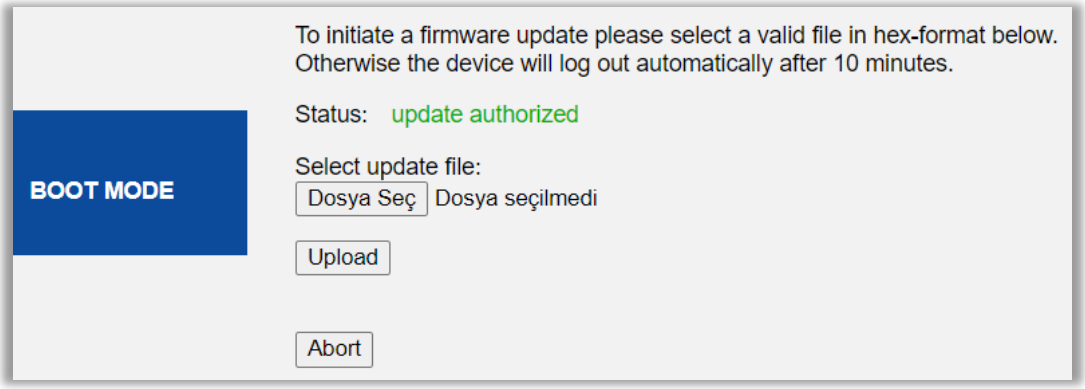


Fig. 25: Select Update File

4.6. IP Tunnelling Address Assignment

KNX Secure IP Router supports four channels for connections using IP (Secure) Tunnelling. To establish an IP Tunnelling connection, each Tunnelling Channel must be assigned a unique Individual Address. This assignment is performed through the Topology window. By selecting the Tunnelling Channel, its Properties window will open, allowing for configuration. Up to four Individual Addresses from the subline can be configured in this manner.

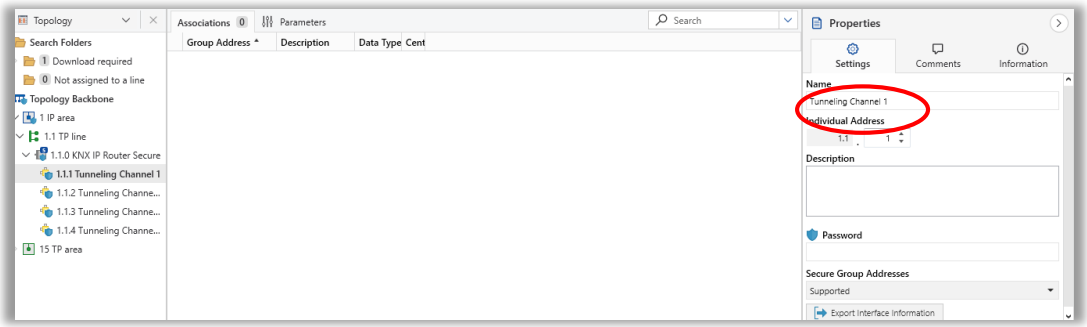


Fig. 26: Configuring of IP (Secure) Tunneling Cannels

To use IP Secure Tunneling both Secure Commissioning and Secure Tunneling must be activated in the Properties window of KNX Secure IP Router. After that, the passwords for protection of each Tunneling Channel can be entered (or changed).

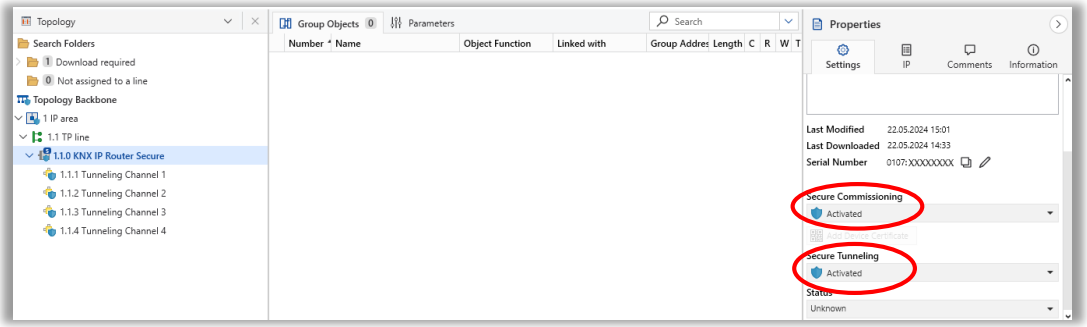


Fig. 27: Activation of Secure Tunneling

THE INTERRA WEBSITE

Interra provides documentation support via our website www.interratechnology.com. This website is used as a means to make files and information easily available to customers. Accessible by using your favourite Internet browser, the website contains the following information:

- Information about our products and projects.
- Overview of Interra Company and values.
- Product Support: Datasheets, product manuals, application descriptions, latest software releases, ETS databases and archived software.

EUROPE, Turkey

Interra
Cumhuriyet Mah. Kartal Cad. Interra R&D Centre No:95/1 Kartal/İstanbul
Tel: +90 (216) 326 26 40 Fax: +90 (216) 324 25 03
Web address: http://www.interratechnology.com