Application manual

KNX-IP Interface secure
EK-IE1-SEC-TP

KNX-IP Router secure
EK-IF1-SEC-TP

Contents

Revision	Changes	Date	Written by	Verified by
1.0	First release	07/10/2022	G. Schiochet	C. Baldini

1. Document

This application manual refers to the release A1.0 of the ekinex® KNX-IP interface EK-IE1-SEC-TP and KNX-IP Router secure EK-IF1-SEC-TP.
Application manual and application program for ETS® are available for download at www.ekinex.com.

Object	Filename	Device release	Update
Application Manual	MAEKIE1IF1SECTP_EN.pdf	A1.0	10 / 2022
Application program KNX-IP interface secure	APEKIE1SECTP01.knxproj		
Application program KNX-IP router secure	APEKIF1SECTP01.knxproj		

Other technical information on the device is available on the datasheet STEKIE1IF1SECTP_EN.pdf.

2. Product description

The ekinex® KNX IP Interface EK-IE1-SEC-TP secure is a compact bus powered interface between LAN/Ethernet and KNX bus. With its compact design has a width of only 1 module (18 mm) and is powered by the KNX bus. The device is an interface between IP and KNX and can be used as programming interface for ETS® Software. You can access the KNX Bus from every point of your LAN. Furthermore, the KNX IP Interface EK-IE1-SEC-TP secure allows you to program the KNX bus over the Internet.
The device supports KNX Security which can be enabled in ETS®. With its interface functionality (tunneling) KNX security prevents from unauthorized access.
The buttons and LEDs on the device allow a local diagnosis including the operating status and communication errors.
The ekinex® KNX IP Router EK-IF1-SEC-TP secure allows forwarding of telegrams between different lines through a LAN (IP) as a fast backbone. In addition this device is suited to connect a PC to the KNX network e.g. for ETS® programming.
The device supports KNX Security which can be enabled in ETS®. As secure router the device allows coupling of not secured communication on KNX TP to a secured IP backbone. Also for the interface functionality (tunneling) KNX security prevents from unauthorized access.
The IP address can be obtained by a DHCP server or by manual configuration (ETS®) respectively. This device works according to the KNXnet/IP specification using the core, the device management, the tunneling and the routing part.
The KNX IP Router EK-IF1-SEC-TP secure has an extended filter table for main group 0 ... 31 and is able to buffer up to 150 telegrams. Power is supplied via the KNX bus.

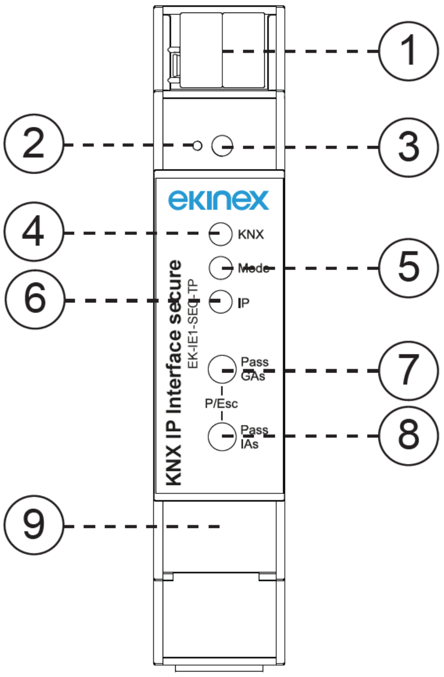
Following are the main features of the devices:

- Programming button and LED on the front
- LED for status and data traffic signaling on bus line and Ethernet network
- Buttons for activating connection functions
- Bus line connection via KNX terminal
- Connection to Ethernet network via RJ45 connector
- Ethernet 100BaseT (100MBit/s)
- Supported internet protocols ARP, ICMP, IGMP, UDP/IP, TCP/IP, DHCP and Auto IP
- Support for KNX secure technology, which can be activated via ETS®

- Up to 8 KNXnet/IP Tunneling connections simultaneously
- Max. APDU length: 55
- KNXnet/IP Security (AES-128)
- KNX Line / Area coupler functionality (EK-IF1-SEC-TP only)
- Extended filter table for main group 0 ... 31 (EK-IF1-SEC-TP only)

3. Switching, display and connection elements

The devices are equipped with a programming pushbutton and a programming LED, two operating buttons, three LEDs for status indication, terminals for connecting the KNX bus line and the Ethernet/LAN.



1. KNX Bus connector
2. LED for Programming Mode (red)
3. Programming Mode button
4. KNX LED (multicolor)
5. Mode LED (multicolor)
6. IP LED (multicolor)
7. Connection Up button
8. Connection Down button
9. Ethernet/LAN connector

Figure 1 - EK-IE1-SEC-TP elements

1.1 Switching elements

- Pushbutton ❸ for switching between the normal and programming operating mode. This operation can be done by simultaneously pressing the pushbuttons ❼ and ❽ as well;
- Pushbuttons ❼ and ❽ to perform the following operation:
  - for EK-IE1-SEC-TP, they allow to choose each single connection. ***Conn Up*** counts the connection numbers up and ***Conn Dn*** down. The actually selected connection number is indicated by flashing (1x…5x times) of the Mode LED ❺;
  - for EK-IF1-SEC-TP, with the button ***Pass GAs*** the forwarding of Group Addressed telegrams can be activated, while the button ***Pass IAs*** activates the forwarding of Individually Addressed telegrams.

3.2 Display and connection elements

- Red LED ❷ for displaying the active operating mode of the device (on = programming, off = normal operation).
- Multicolor KNX LED ❹, that lights up green if the device is successfully powered by the KNX bus. The LED indicates telegrams on the KNX bus by flickering. Communication failures (e.g. repetitions of telegram or telegram fragments) are indicated by a short change of the LED color to red.

  Overview of the different indications of the KNX LED ❹:

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

- Multicolor Mode LED ❺:
  For testing purposes (for example, during commissioning) the configured routing settings (filter or block) can be by-passed via manual operation.
  - for EK-IE1-SEC-TP, The Mode LED ❺ can visualize the status of each KNXnet/IP tunneling connection. With the buttons Conn Up/Dn ❼ ❽ you can chose each single connection. Conn Up ❼ counts the connection numbers up and Conn Dn ❽ down. The actually selected connection number is indicated by flashing (1x…5x) of the Mode LED ❺. An available KNXnet/IP Tunneling connection is indicated by a green LED and a used tunneling connection is indicated by an orange LED.
    Via the Escape function (Esc) this indication can be ended by simultaneously pressing the buttons Conn Up/Dn ❼ ❽.
    If neither programming mode nor manual operation are active the Mode LED ❺ can visualize configuration errors.
    Overview of the different indications of the Mode LED ❺ for EK-IE1-TP-SEC-TP:

LED Status	Meaning
LED lights green	Device is working in standard operation mode.
LED lights red	Programming mode is active
LED flashes green 1x..5x	Programming mode is not active. Manual operation is active. The selected tunnel (1-5) is not used and free
LED flashes orange 1x…5x	Programming mode is not active. Manual operation is active. The selected tunnel (1-5) is used
LED flashes red	Programming mode is not active. Manual operation is not active. The device is not properly loaded e.g. after an interrupted download.

  - for EK-IF1-SEC-TP, Mode LED ❺ shows the forwarding of Individual and/or Group Adressed telegrams.

With the button Pass GAs ❼ the forwarding of group addressed telegrams can be activated.
With the button Pass IAs ❽ the forwarding of individually addressed telegrams can be activated.
This is visualized with a single flash of the Mode LED ❺ (orange). If both modes are activated the Mode LED ❺ flashes two times.
Pressing button Pass GAs ❼ or button Pass IAs ❽ again these settings can be selected and deselected on demand. Via the Escape function (Esc) the manual operation can be stopped by simultaneously pressing the buttons Pass GAs ❼ and Pass IAs ❽.
If neither programming mode nor manual mode are active the LED ❺ can visualize configuration errors.
Overview of the different indications of the Mode LED ❺:

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

- Multicolor IP LED ❻ lights up when an Ethernet link is active. This LED is green if the device has valid IP settings (IP address, Sub net and Gateway). With invalid or nonexistent IP settings the LED is red. This is also the case if e.g. the device has not yet received the IP settings by a DHCP server. The LED indicates IP telegrams traffic by flickering.
  Overview of the different indications of the IP LED ❻:

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

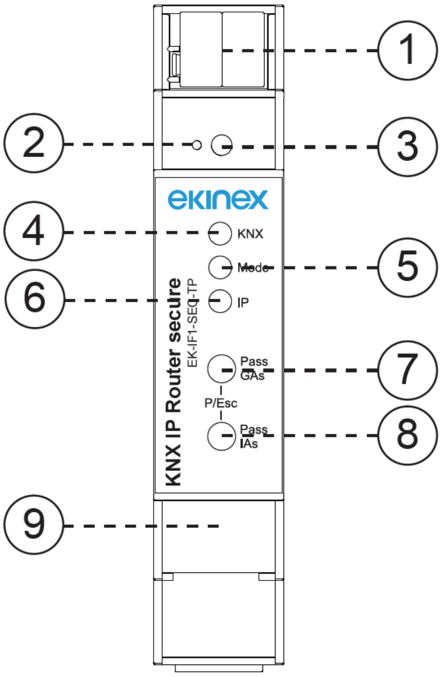


Figure 2 - EK-IF1-SEC-TP elements

1. KNX Bus connector
2. LED for Programming Mode (red)
3. Programming Mode button
4. KNX LED (multicolor)
5. Mode LED (multicolor)
6. IP LED (multicolor)
7. Pass GAs (Group Addresses) button
8. Pass IAs (Individual Addresses) button
9. Ethernet/LAN connector

3.3 Factory default settings

Factory default configuration:

- Individual device address:
  - EK-IE1-SEC-TP: 15.15.255
  - EK-IF1-SEC-TP: 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

3.4 Reset to factory device settings (Master-Reset)

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

- Separate the KNX Bus connector ❶ from device;
- Press the KNX programming button ❸ and keep it pressed down;
- Reconnect the KNX Bus connector ❶ of device;
- Keep the KNX programming button ❸ pressed for at least another 6 seconds;
- A short flashing of all LEDs (❷❹❺❻) visualizes the successful reset of the device to factory default settings.

4. 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 the communication remains unencrypted. Thus KNX IP Security can also be used in existing KNX systems and with non-secure KNX TP devices.

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

4.1 KNX IP Security for the Interface function

When using a KNX IP 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 transfer 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.

4.2 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. 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.

4.3 KNX IP Security for the devices

Both EK-IE1-SEC-TP Interface secure and EK-IF1-SEC-TP Router secure also support KNX Data Security to protect the device from unauthorised access from the KNX bus. If the KNX IP device is programmed via the KNX bus, this is done with encrypted telegrams.

> i **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 (e.g. USB) and any intermediate line couplers support the so-called KNX long frames.*

4.4 KNX Data Security for group telegrams (EK-IF1-SEC-TP only)

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

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

5. Coupler function (EK-IF1-SEC-TP only)

The KNX IP EK-IF1-SEC-TP Router *secure* operates as a line or backbone coupler. In both cases, the LAN (IP) is used as a backbone. The following table shows the application possibilities of the KNX IP Router compared to the classic topology:

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

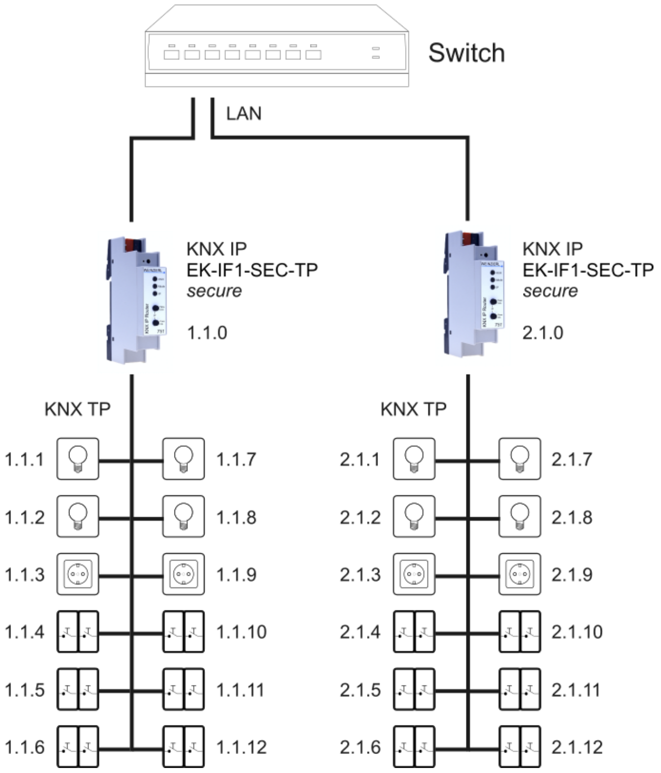


Figure 3 - KNX IP Router as line coupler

i **Note:** *if the KNX IP Router secure is used as a line coupler (x.y.0), there must not be a KNX IP Router in the topology above it. For example, if a KNX IP Router has the individual address 1.1.0, there must be no KNX IP Router with the address 1.0.0.*

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

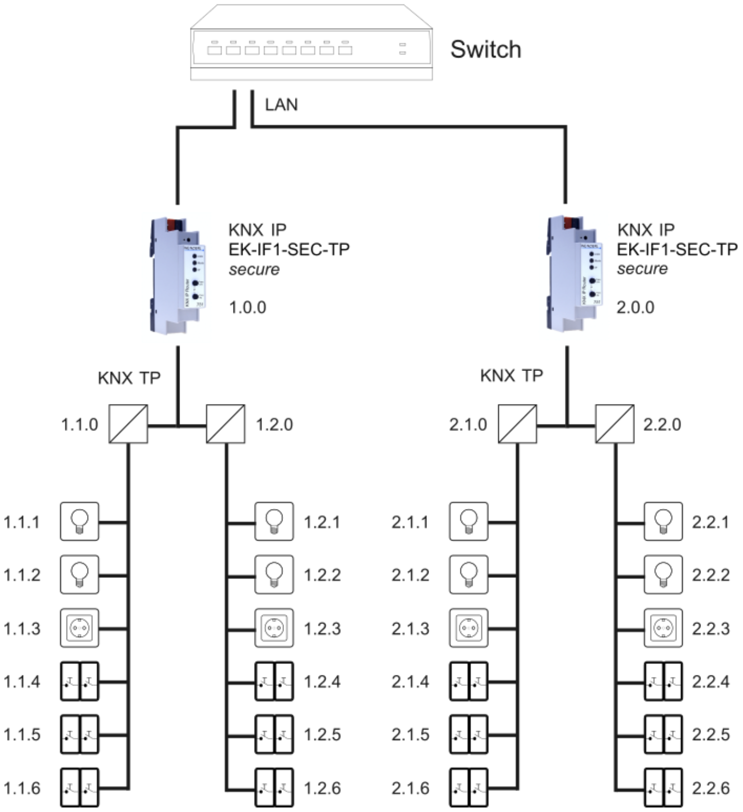


Figure 4 - KNX IP Router as area coupler

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

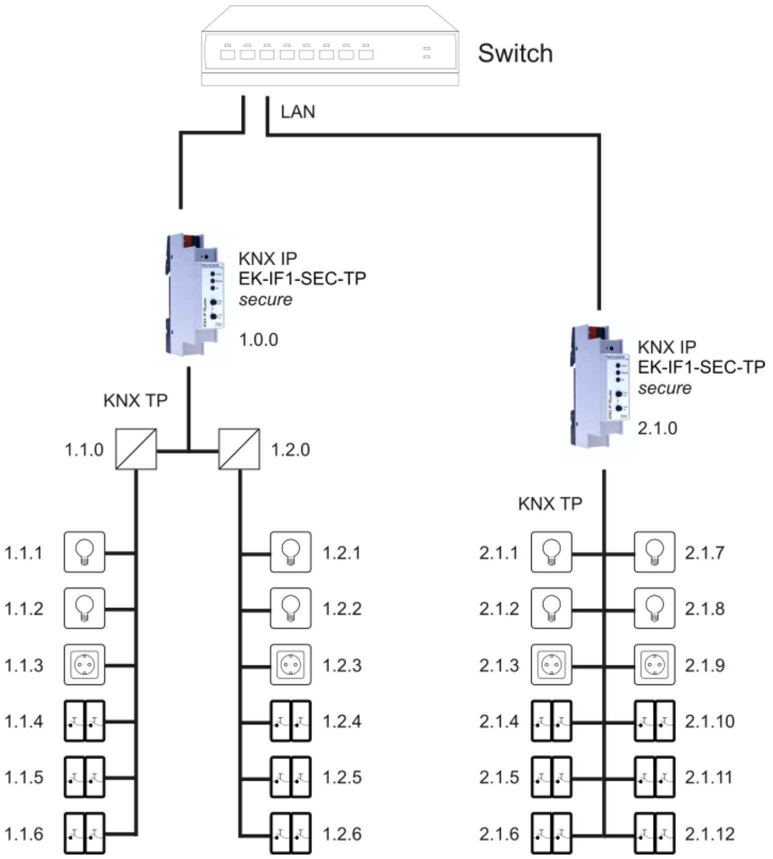


Figure 5 - KNX IP Router as area and line coupler

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

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

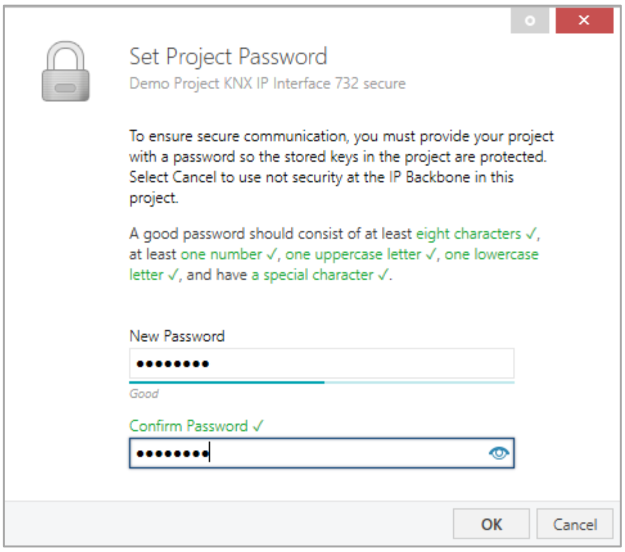
5.1 Bus access function (KNXnet/IP Tunneling)

The KNX IP Router secure can be used as an interface to KNX. The KNX bus can be accessed from any point in the LAN. For this purpose, an additional individual address must be assigned. This is described in chapter 6.

6. KNX-IP ETS parameters

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

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



Set Project Password
Demo Project KNX IP Interface 732 secure

To ensure secure communication, you must provide your project with a password so the stored keys in the project are protected. Select Cancel to use not security at the IP Backbone in this project.

A good password should consist of at least eight characters ✓, at least one number ✓, one uppercase letter ✓, one lowercase letter ✓, and have a special character ✓.

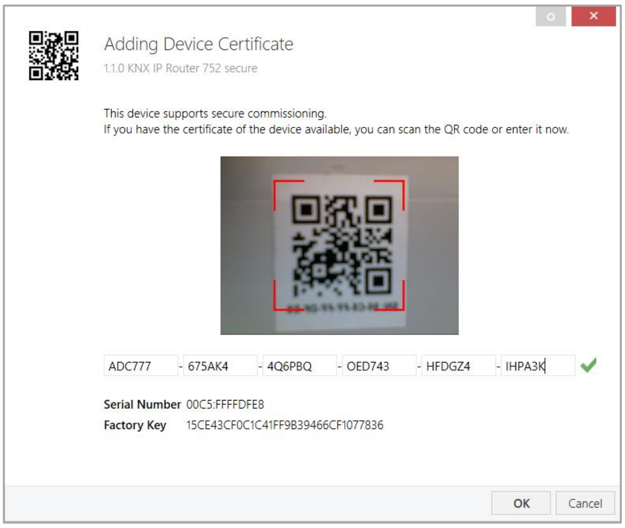
New Password: ••••••••
Good

Confirm Password ✓: ••••••••

Figure 6 - Project password settings

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 by-passed 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).



Adding Device Certificate
1.1.0 KNX IP Router 752 secure

This device supports secure commissioning.
If you have the certificate of the device available, you can scan the QR code or enter it now.

ADC777 - 675AK4 - 4Q6PBQ - OED743 - HFDGZ4 - IHPA3K ✓

Serial Number 00C5:FFFFDFE8
Factory Key 15CE43CF0C1C41FF9B39466CF1077836

Figure 7 - Adding device certificate

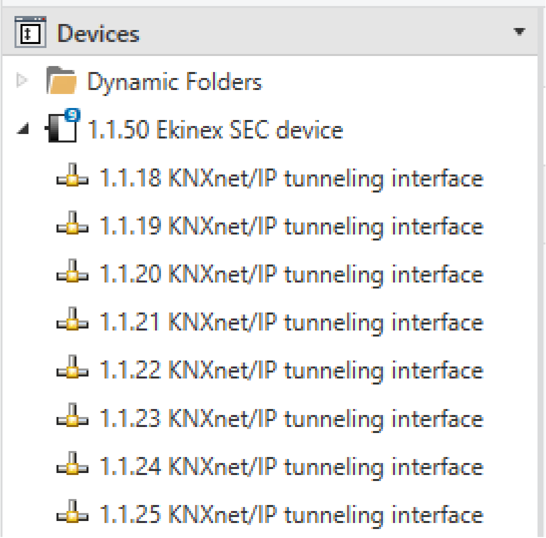
The certificate is printed as text on the device. It can also be conveniently scanned from the printed QR code via a webcam.

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

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

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

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



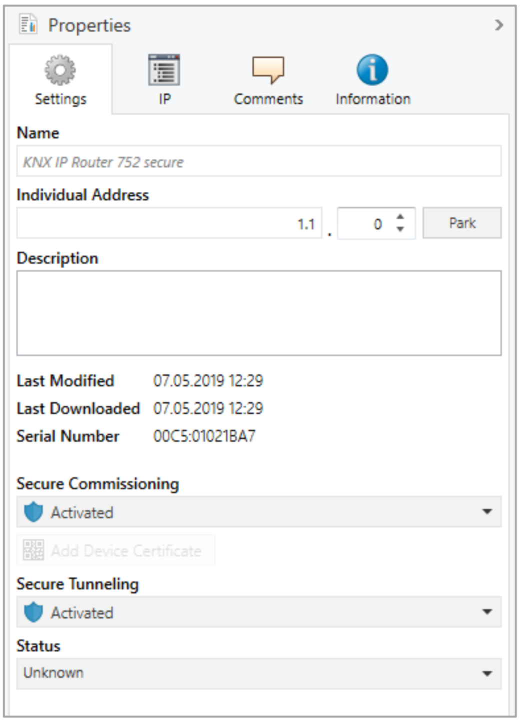
Devices
Dynamic Folders
1.1.50 Ekinex SEC device
1.1.18 KNXnet/IP tunneling interface
1.1.19 KNXnet/IP tunneling interface
1.1.20 KNXnet/IP tunneling interface
1.1.21 KNXnet/IP tunneling interface
1.1.22 KNXnet/IP tunneling interface
1.1.23 KNXnet/IP tunneling interface
1.1.24 KNXnet/IP tunneling interface
1.1.25 KNXnet/IP tunneling interface

Figure 8 - Additional addresses

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 the ETS project.

Note: *Make sure that none of the addresses above is already in use within the KNX installation.*

By clicking on the KNX IP Interface or Router secure device entry within the 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.



Name
KNX IP Router 752 secure

Individual Address
1.1 . 0 Park

Description

Last Modified 07.05.2019 12:29
Last Downloaded 07.05.2019 12:29
Serial Number 00C5:01021BA7

Secure Commissioning
Activated

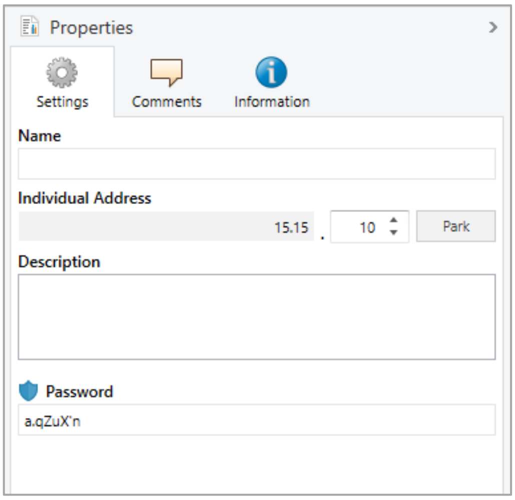
Add Device Certificate

Secure Tunneling
Activated

Status
Unknown

Figure 9 - Device Properties - Settings

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.



Name

Individual Address
15.15 . 10 Park

Description

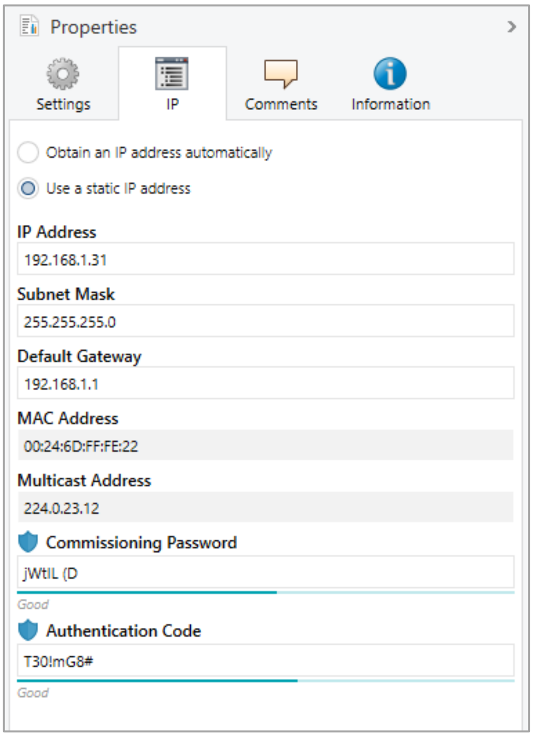
Password
a.qZuX'n

Figure 10 - Password for secure tunneling

Within the “IP” overview, the IP network specific options of the KNX IP Interface or Router secure can be changed.

By changing "obtain an IP address automatically" (via DHCP) to “Use a 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.*



○ Obtain an IP address automatically
● Use a static IP address

IP Address
192.168.1.31

Subnet Mask
255.255.255.0

Default Gateway
192.168.1.1

MAC Address
00:24:6D:FF:FE:22

Multicast Address
224.0.23.12

Commissioning Password
jWtIL (D
Good

Authentication Code
T30!mG8#
Good

Figure 11 – static IP address setting

6.1 IP address

Here the IP address of the KNX IP Interface or Router secure device 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.

6.2 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.

6.3 Default gateway

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

6.4 Example of assigning IP addresses

A PC is used to access the KNX IP Interface or Router secure:

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

The KNX IP Interface or Router secure is located in the same local 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 IP interface or 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 in use). It must be ensured that no numbers are assigned twice.

- IP address of the IP Interface/Router: 192.168.1.31
- Subnet of the IP Interface/Router: 255.255.255.0

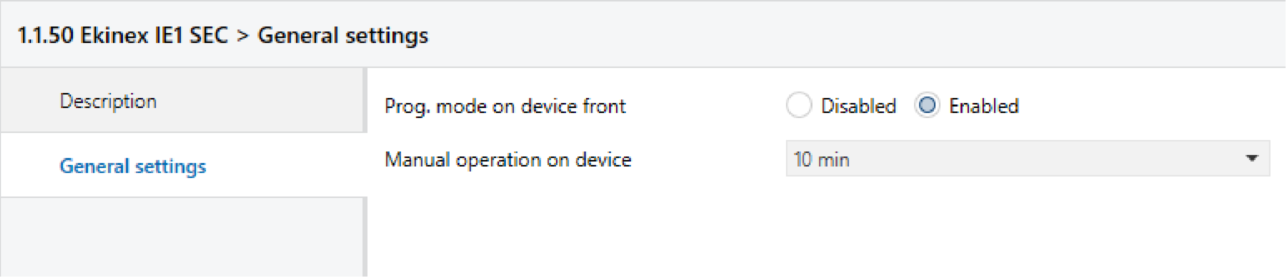
6.5 Remote access

Remote access via the Internet is possible via the KNX IP Interface or Router secure.

7. ETS parameter dialogue

The following parameters can be set using the ETS.

7.1 General settings



1.1.50 Ekinex IE1 SEC > General settings

Prog. mode on device front ○ Disabled ● Enabled

Manual operation on device 10 min

Figure 12 - General settings

7.2 Programming mode on device front

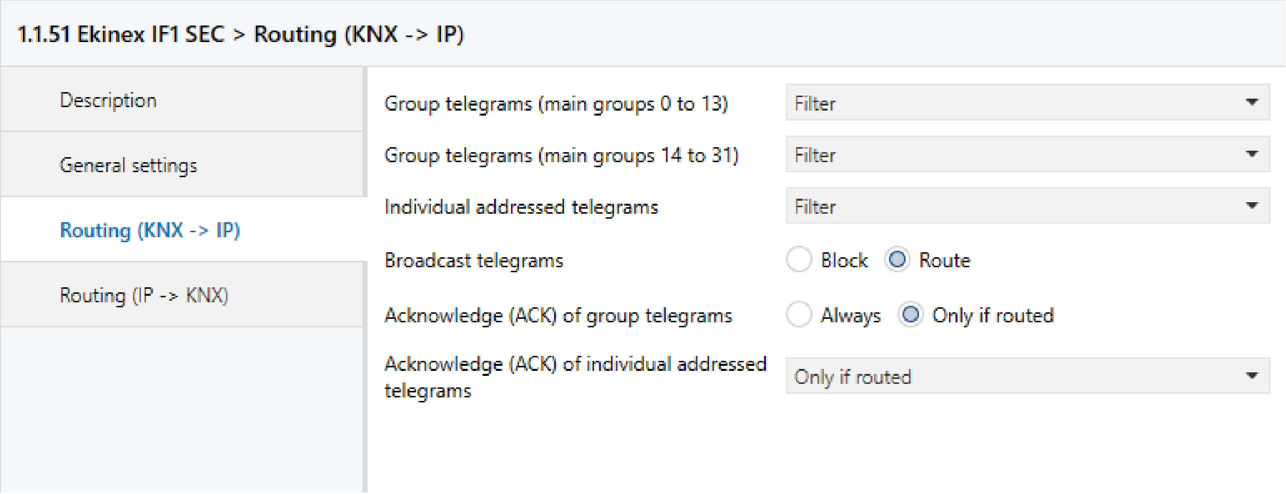
In addition to the normal programming button ❸ the device allows activating the programming mode on the device front without opening the switchboard cover. The programming mode can be activated and deactivated via pressing simultaneously both buttons ❼ and ❽.

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

7.3 Manual operation on device

The manual operation of the KNX IP Interface or Router secure contains the status display only. This parameter sets the duration of the manual mode. Upon completion the normal display mode is restored.

7.4 Routing (KNX -> IP) for EK-IF1-SEC-TP Router


1.1.51 Ekinex IF1 SEC > Routing (KNX -> IP)

Group telegrams (main groups 0 to 13): Filter
Group telegrams (main groups 14 to 31): Filter
Individual addressed telegrams: Filter
Broadcast telegrams: ○ Block ● Route
Acknowledge (ACK) of group telegrams: ○ Always ● Only if routed
Acknowledge (ACK) of individual addressed telegrams: Only if routed

Figure 13 - Routing KNX -> IP Tab

Group telegrams (main groups 0 to 13)

- Block: No group telegrams of the main groups 0 to 13 are routed to IP.
- Route: All group telegrams of the main groups 0 to 13 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 groups 14 to 31)

- Block: No group telegrams of main groups 14 to 31 are routed to IP.
- Route: All group telegrams of main groups 14 to 31 are routed to IP.
- Filter: The filter table is used to check whether or not the received group telegram should be routed to IP.

Individually addressed telegrams

- Block: No individually addressed telegrams are routed to IP.
- Route: All individually addressed telegrams are routed to IP.
- Filter: The individual address is used to check whether the received individually addressed telegram should be routed to IP.

Broadcast telegrams

- Block: No received broadcast telegrams are routed to IP.
- Route: All received broadcast telegrams are routed to IP.

Acknowledge (ACK) of group telegrams

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

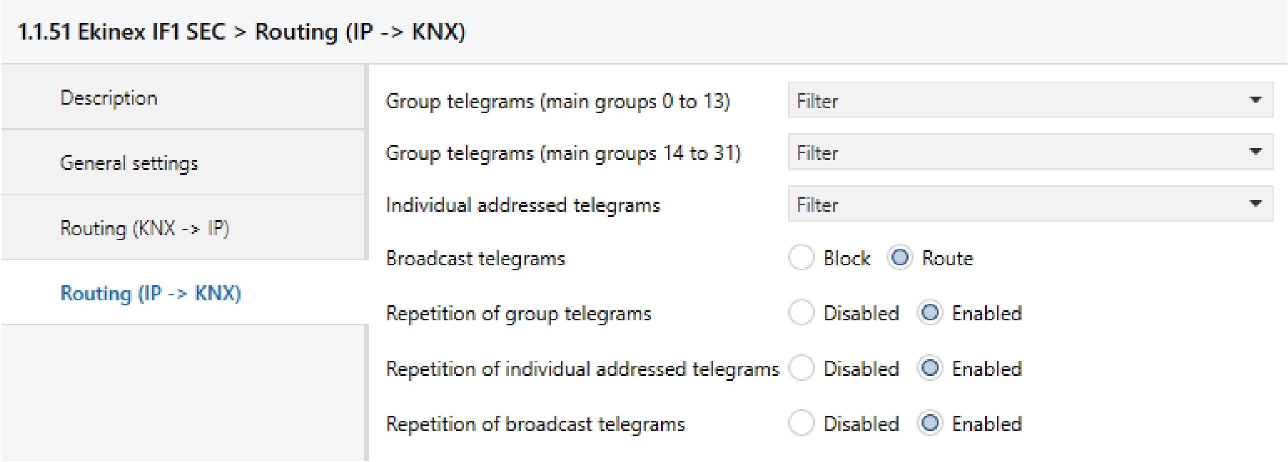
- Only if routed: A acknowledge is only generated for received group telegrams (from KNX) if they are routed to IP.

Acknowledge (ACK) of individually addressed telegrams

- Always: An acknowledge is generated for every received individual addressed telegram (from KNX).
- Only if routed: A acknowledge is only generated for received individually addressed group telegrams (from KNX) if they are routed to IP.
- Answer with NACK: Every received individually addressed telegram (from KNX) is responded to with NACK (Not acknowledge). This means that communication with individually addressed telegrams on the corresponding KNX line is not possible. Group communication (group telegrams) is not affected. This setting can be used to block attempts at manipulation.

> **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.*

7.5 Routing (IP -> KNX) for EK-IF1-SEC-TP Router



1.1.51 Ekinex IF1 SEC > Routing (IP -> KNX)

Group telegrams (main groups 0 to 13)	Filter
Group telegrams (main groups 14 to 31)	Filter
Individual addressed telegrams	Filter
Broadcast telegrams	○ Block ● Route
Repetition of group telegrams	○ Disabled ● Enabled
Repetition of individual addressed telegrams	○ Disabled ● Enabled
Repetition of broadcast telegrams	○ Disabled ● Enabled

Figure 14 - Routing IP -> KNX Tab

Group telegrams (main groups 0 to 13)

- Block: No group telegrams of the main groups 0 to 13 are routed to KNX.
- Route: All group telegrams of the main groups 0 to 13 are routed to KNX independently 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 groups 14 to 31)

- Block: No group telegrams of main groups 14 to 31 are routed to KNX.
- Route: All group telegrams of the main groups 14 to 31 are routed to KNX.

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

Individually addressed telegrams

- Block: No individually addressed telegrams are routed to KNX.
- Route: All individually addressed telegrams are routed to KNX.
- Filter: The individual address is used to check whether the received individually addressed telegram should be routed to KNX.

Broadcast telegrams

- Block: No received broadcast telegrams are routed to KNX.
- Route: All received broadcast telegrams are routed to KNX.

Repetition of group telegrams

- Disabled: The received group telegram is not re-sent to KNX in case of a fault.
- Enabled: The received group telegram is re-sent up to three times in case of a fault.

Repetition of individually addressed telegrams

- Disabled: The received individually addressed telegram is not re-sent to KNX in case of a fault.
- Enabled: The received individually addressed telegram is re-sent up to three times in case of a fault.

Repetition of broadcast telegrams

- Disabled: The received broadcast telegram is not re-sent to KNX in case of a fault.
- Enabled: The received broadcast telegram is re-sent up to three times in case of a fault.

8. ETS Programming

The KNX IP Interface and Router secure devices can be programmed in different ways via the ETS:

8.1 Programming via the 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.

8.2 Programming via KNXnet/IP Tunneling

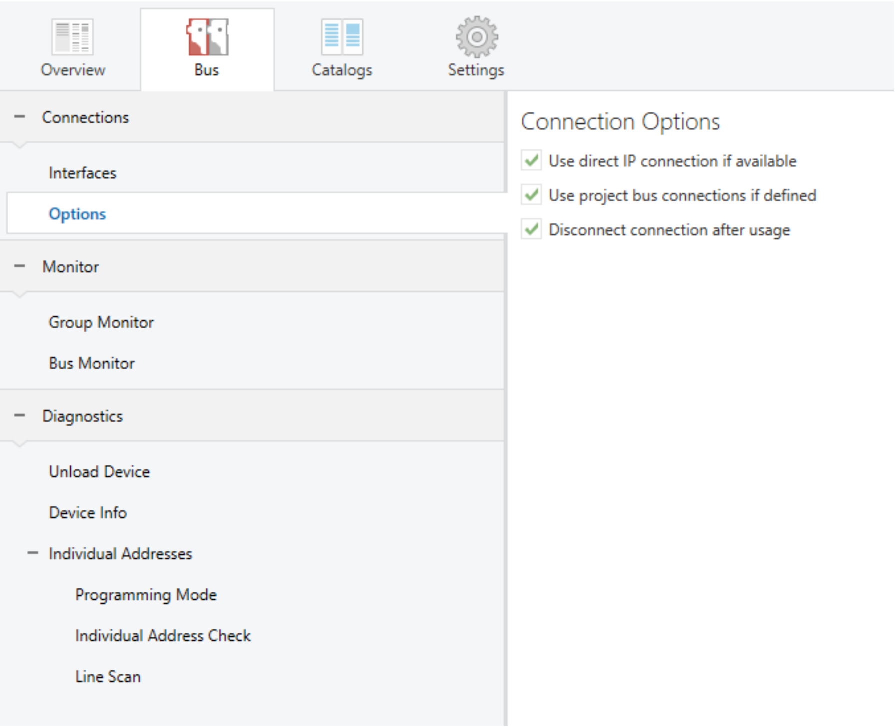
No additional interface is required. Programming via KNXnet/IP Tunneling is possible if the device already has a valid IP configuration (e.g. via DHCP). In this case the device is displayed in the interface configuration of the ETS and must be selected. The download is executed via the ETS project as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

8.3 Programming via direct IP connection

While KNXnet/IP tunneling is limited to the speed of KNX TP, the device can be loaded at high speed via a direct IP connection. The direct IP connection is possible if the device already has a valid IP configuration as well as a physical address. To do this, select "Use direct IP connection if possible" in the ETS menu under "Bus - Connections - Options". The download then takes place directly into the device and is not visible in the ETS group monitor.

8.4 Programming via KNXnet/IP Routing (EK-IF1-SEC-TP only)

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



Connection Options

☑ Use direct IP connection if available

☑ Use project bus connections if defined

☑ Disconnect connection after usage

Figure 15 - Connection options via ETS

Note: *due to the significantly shorter transmission times, it is recommended that downloads be carried out via IP.*

9. Interface settings with ETS

The KNX IP secure devices serve as programming interface. The ETS can use this function to establish a connection via IP to the respective TP line.

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

The ETS can access configured the KNX IP Interface and Router even without a database entry. If the setup of the KNX IP Interface or Router device does not comply with the conditions of the KNX installation it must be configured via an ETS project. Please see the ETS Programming section for more information.

If security mode is activated in the KNX IP Interface, 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 (e.g. many DSL routers have an integrated DHCP server).

If the KNX IP interface and/or Router device has been connected to the LAN and has a valid IP address, it should appear automatically in the menu item "Bus" under "Discovered interfaces".

By clicking on the discovered interface it is selected as the current interface. On the right side of the ETS window all specific information and options of the connection appear (name, individual address, etc.).

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

Like all programmable KNX devices the KNX IP secure Interfaces and Router have an individual address which can be used to access the device. This is used, for example, when downloading the ETS application to the KNX IP Interface and/or Router via the bus.

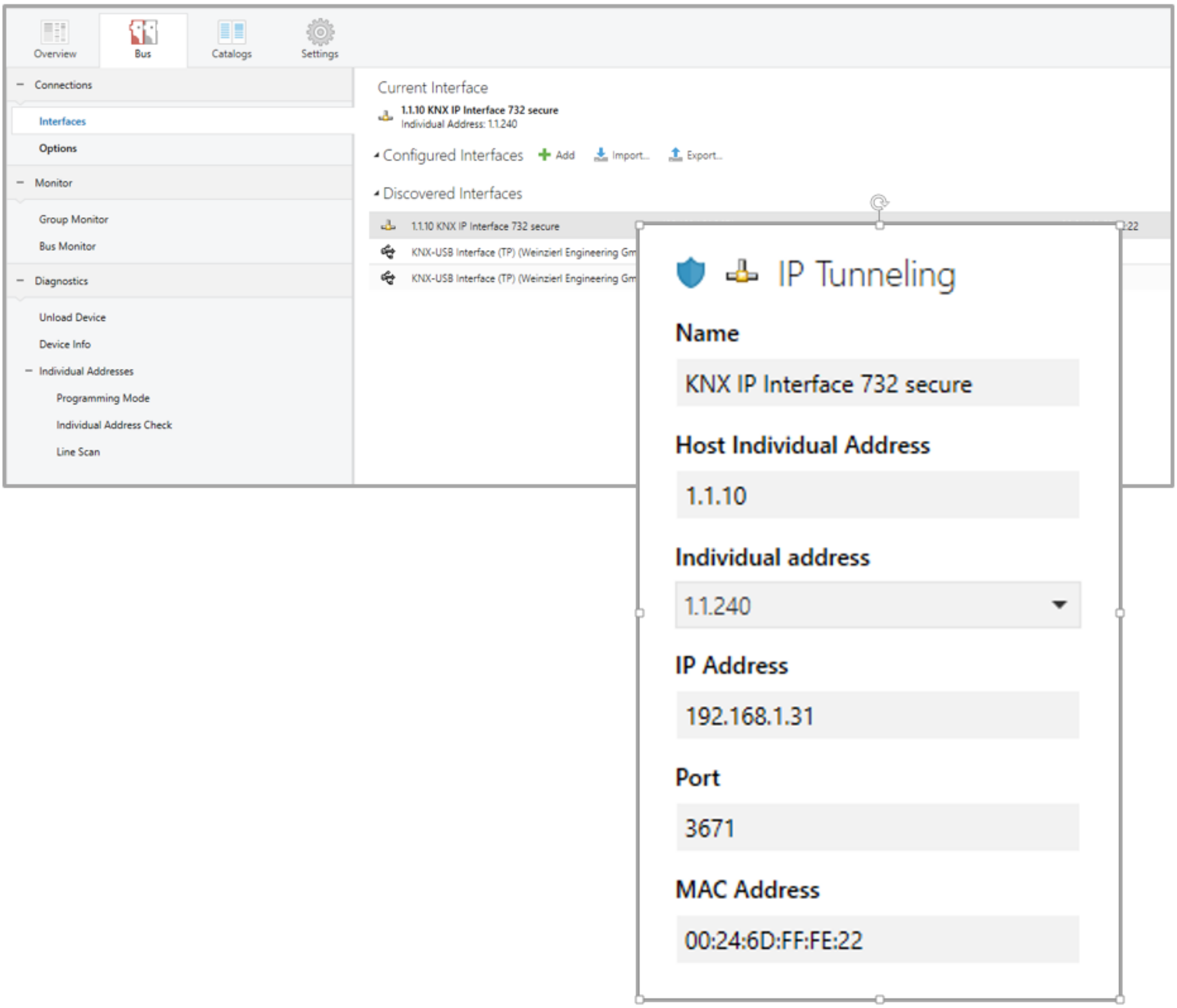
For the interface function the device contains additional individual addresses that can be set in the ETS. When a client (e.g. ETS) sends telegrams to the bus via the KNX IP secure devices, they contain a sender address as one from the additional addresses. Each address is associated with a connection. 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	1.1.10	(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)

Section “Individual Address” enables you to select the individual KNX address of the currently used KNXnet/IP Tunneling connection.



Current Interface
1.1.10 KNX IP Interface 732 secure
Individual Address: 1.1.240

1.1.10 KNX IP Interface 732 secure
KNX-USB Interface (TP) (Weinzierl Engineering Gm
KNX-USB Interface (TP) (Weinzierl Engineering Gm

IP Tunneling

Name: KNX IP Interface 732 secure

Host Individual Address: 1.1.10

Individual address: 1.1.240

IP Address: 192.168.1.31

Port: 3671

MAC Address: 00:24:6D:FF:FE:22

Figure 16 - Interface IP tunneling

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

10. Open Source Licenses

This product contains open source software license:

curve25519-donna: Curve25519 elliptic curve, public key function

Source: http://code.google.com/p/curve25519-donna/

11. Appendix

WARNINGS:

- ***Installation, electrical connection, configuration and commissioning of the device can only be carried out by qualified personnel.***
- ***The prevailing safety rules must be heeded.***
- ***The device must not be opened. Opening the housing of the device causes the immediate end of the warranty period.***
- ***For planning and construction of electric in-stallations, the relevant guidelines, regula-tions and standards of the respective country are to be considered.***

11.1 Return of defective products

Defective ekinex® KNX devices can be returned for repair / replacement following the procedure detailed below.

11.2 Devices purchased directly from ekinex®

Request an RMA number by sending an E-Mail to the address support@ekinex.com with following mandatory information:

- Exact device model
- Device serial number (can be found on the product label)
- Date of purchase / Order reference
- Detailed description of the fault or issue

The technical assistance team will contact you as quickly as possible to either investigate the problem further, suggest possible solutions or authorize the return of the device for replacement or repair.

If the device should be returned, it should be shipped to the following address:

EKINEX S.p.A. - Via Novara, 37 / SP229 - I-28010 Vaprio d'Agogna (NO) - Italy.

Further arrangements will be made with the technical support team, according to the type of issue and device.

11.3 Devices purchased through ekinex® resellers

If the device has been purchased through a reseller, please refer to the reseller's technical support contact. Depending on the issue and other factors, at the decision of ekinex® and after agreement with the reseller, the customer might be instructed to contact ekinex® directly according to the procedure above.

11.4 Other information

This application manual is aimed at installers, system integrators and planners.

For further information on the product, please contact the ekinex® technical support at the e-mail address: **support@ekinex.com** or visit the website http://www.ekinex.com