

Product Manual

KNX IP Router Secure

OPT-IPR-121



Table of Contents

1 Product Description	4
1.1 Application	4
1.2 KNX Security.....	4
1.3 KNX IP Security For The Router Function.....	4
1.4 KNX IP Security For The Interface Function.....	4
1.5 KNX Data Security For The Device.....	5
1.6 KNX Data Security For Group Telgrafs.....	5
1.7 Coupler Function (KNXnet/IP Routing)	5
1.8 KNX IP Router Secure As Line Coupler.....	6
1.9 KNX IP Router Secure As Area Coupler	6
1.10 Bus Access Function (KNXnet/IP Tunneling)	6
1.11 Installation and Connection.....	6
1.12 KNX Programming Mode	7
1.13 Status Display	7
2 Interface Settings With ETS.....	9
2.1 ETS Database.....	10
2.2 IP Address.....	14
2.3 Subnet Mask.....	14
2.4 Default Gateway	14
2.5 Routing Multicast Address	15
2.6 Remote Access.....	16
2.7 ETS Parameter Dialogue.....	16
2.8 General Settings.....	16

About this document

This document provides detailed technical information on the function, installation and programming of the OPT-IPR-121 device.

Legal disclaimer

OPTIMUS SOLUTION reserves the right to make changes to the product or change the content of this document without prior notice.

The agreed specifications are final for all orders placed. OPTIMUS SOLUTION accepts no liability in anyway for possible errors or possible deficiencies in this document. OPTIMUS SOLUTION reserves all rights in this document and in the subjects and drawings contained here in. Any reproduction, transfer or processing of the content - including parts thereof - to third parties without the prior written permission of OPTIMUS SOLUTION is prohibited.

Copyright 2024 OPTIMUS SOLUTION
All Rights Reserved

Disposing of packaging

The packaging protects the device from damage during transmission. All materials used are environmentally safe and recyclable. Please help us by disposing of the packaging in an environmentally responsible manner.

Discarding the old device

Please dispose of the old device at the designated collection point for electrical and electronic equipment in accordance with local regulations. If you have any questions, please contact the competent authority.

optimus ✓

1 Product Description

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

1.1 Application

The compact KNX IP Router Secure enables the forwarding of telgrafs between different lines via a LAN (IP) as a fast backbone. The device also serves as a programming interface between a PC and the KNX bus (e.g. for ETS programming).

The device supports KNX Security. The option can be activated in the ETS. As a secure router, the device enables the coupling of unsecured communication on a KNX TP line with a secure IP backbone.

KNX Security also prevents unauthorised access to the interface function (tunneling).

The IP address can be assigned via DHCP or via the ETS configuration. The device operates according to the KNXnet/IP specification using core, device management, tunneling and routing.

The KNX IP Router Secure has an extended filter table for main groups 0..31 and can buffer up to 150 telgrafs. Power is supplied via the KNX bus.

1.2 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 telgraf level. This means that the telgrafs on the twisted pair bus are also encrypted.

1.3 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 telgrafs. A time stamp in the routing telgraf ensures that no previously recorded telgrafs 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.

1.4 KNX IP Security For The Interface Function

When using a KNX IP router as an interface to the bus, access to the installation is possible without security for all devices that have access to the IP network. With KNX Security a password is required. A secure connection is already established for the transmission of the password. All communication via IP is en-cripted and secured.

1.5 KNX Data Security For The Device

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

Encrypted telgrafs 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.

1.6 KNX Data Security For Group Telgrafs

Telgrafs from the bus that do not address the 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 telgrafs 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 telgraf encrypted with KNX Data Security to the bus. When forwarding via KNX IP with KNX IP Security, the encrypted telgraf 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 telgraf 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 telgraf.

1.7 Coupler Function (KNXnet/IP Routing)

The KNX IP 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 Secure 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 Secure (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 Secure (max. 225 Pcs..)
Line	TP	TP	TP

1.8 KNX IP Router Secure As Line Coupler

The individual address assigned to The KNX IP Router 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.

If The KNX IP Router Secure is used as a line coupler ($x.y.0$), there must not be a KNX IP Router Secure in the topology above it. For example, if a KNX IP Router Secure has the individual address 1.1.0, there must be no KNX IP Router Secure with the address 1.0.0.

1.9 KNX IP Router Secure As Area Coupler

The KNX IP Router Secure 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 telgrafs can be transmitted on IP. If several consecutive telgrafs are transmitted for the same line, they must be buffered in the router to avoid telgraf loss. The KNX IP Router Secure has a memory for 150 telgrafs (from IP to KNX).

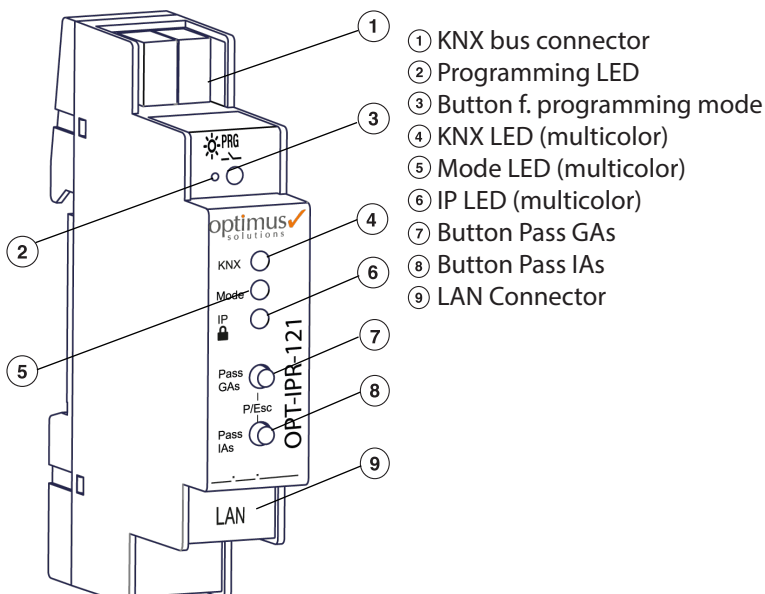
If The KNX IP Router Secure is used as a area coupler ($x.0.0$), there must not be a KNX IP Router Secure in the topology beneath it. For example, if a KNX IP Router Secure has the individual address 1.0.0, there must be no KNX IP Router Secure with the address 1.1.0.

1.10 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 the following sections.

1.11 Installation and Connection

The KNX IP Router Secure is designed for installation on a DIN rail with a width of 1 unit (18mm). It features the following controls and displays:



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

NOTE:

The device is not working without bus power.

1.12 KNX Programming Mode

The KNX programming mode is activated/deactivated either by pressing the flushed KNX programming button ③ or by simultaneously pressing the buttons ⑦ and ⑧

1.13 Status Display

The KNX LED ④, lights up green if the device is successfully powered by the KNX bus. This LED indicates telgraf traffic on the KNX bus by flickering.

Communication failures (e.g. repetitions of telgrafs or telgraf fragments) are indicated by a short change of the LED color to red.

Overview of the different indications of the KNX LED ④:

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

Overview of the different indications of the Mode LED ⑤:

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 telgraf traffic

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

With the button "Pass GAs" ⑦ the forwarding of group addressed telgrafs can be activated.

With the button "Pass IAs" ⑧ the forwarding of individually addressed telgrafs can be activated.

This is visualized with a single flash of the Mode LED ⑤ (orange). If both modes are activated the Mode LED ⑤ flashes two times.

Pressing button "Pass GAs" ⑦ or button "Pass IAs" ⑧ again these settings can be selected and deselected on demand. Via the Escape function (Esc) the manual operation can be stopped by simultaneously pressing the buttons "Pass GAs" ⑦ and "Pass IAs" ⑧.

Overview of the different indications of the Mode LED ⑤:

If neither programming mode nor manual mode are active the LED ⑤ can visualize configuration errors.

LED Status	Meaning
LED lights green	Device is working in standard operation mode.
LED light 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.

The following configuration is set by factory default:

Individual device address:	15.15.0
Number of configured KNXnet/IP tunneling con.:	1
Individual address of tunneling con.:	15.15.240
IP address assignment:	DHCP
Initial Key (FDSK)	active
Security Modus	not active

Reset to factory device settings:

Disconnect the KNX Bus connector ① from device.

Press the KNX programming button ③ and keep it pressed down.

Reconnect the KNX Bus connector ① of device.

Keep the KNX programming button ③ pressed for at least another 6 seconds.

A short flashing of all LEDs (②,④,⑤,⑥) visualizes the successful reset of the device to factory default settings.

2 Interface Settings With ETS

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

The ETS can access configured KNX IP Router Secures even without a database entry. If the setup of the KNX IP Router Secure does not comply with the conditions of the KNX installation it must be configured via an ETS project. See the ETS database section for more information.

As factory default the assignment of the IP address is set to "automatically via DHCP" and thus no further settings are necessary. To use this feature a DHCP server on the LAN must exist (e.g. many DSL routers have an integrated DHCP server).

After connecting the KNX IP Router Secure to the LAN and the KNX bus, it should automatically appear in the ETS within the menu "Bus" under "Discovered interfaces".

By clicking on the discovered interface it is selected as the current interface. On the right side of the ETS window all specific information and options of the connection appear.

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



Like all programmable KNX devices The KNX IP Router Secure has an individual address which can be used to access the device. This is used, for example, of the ETS when downloading to the KNX IP Router Secure via the bus. For the interface function the device contains additional individual addresses that can be set in the ETS. When a client (e.g. ETS) sends via the KNX IP Router Secure telgrafs to the bus, they contain a sender address as one from the additional addresses. Each address is associated with a connection. Thus response telgrafs can be clearly transmitted to the respective client.

The additional individual addresses must be selected from the address range of the bus line in which the interface is installed and may not be used by another device.

Example:

Device address	1.1.0	(address within ETS topology)
Connection 1	1.1.240	(1. additional address)
Connection 2	1.1.241	(2. additional address)
Connection 3	1.1.242	(3. additional address)
Connection 4	1.1.243	(4. additional address)
Connection 5	1.1.244	(5. additional address)
Connection 6	1.1.245	(6. additional address)
Connection 7	1.1.246	(7. additional address)
Connection 8	1.1.247	(8. additional address)

The section "Individual Address" enables you to select the individual KNX address of the currently used KNXnet/IP Tunneling connection.

  IP Tunneling

Name
KNX IP Router 752 secure

Host Individual Address
1.1.0

Individual address
1.1.240 ▼

IP Address
192.168.1.31

Port
3671

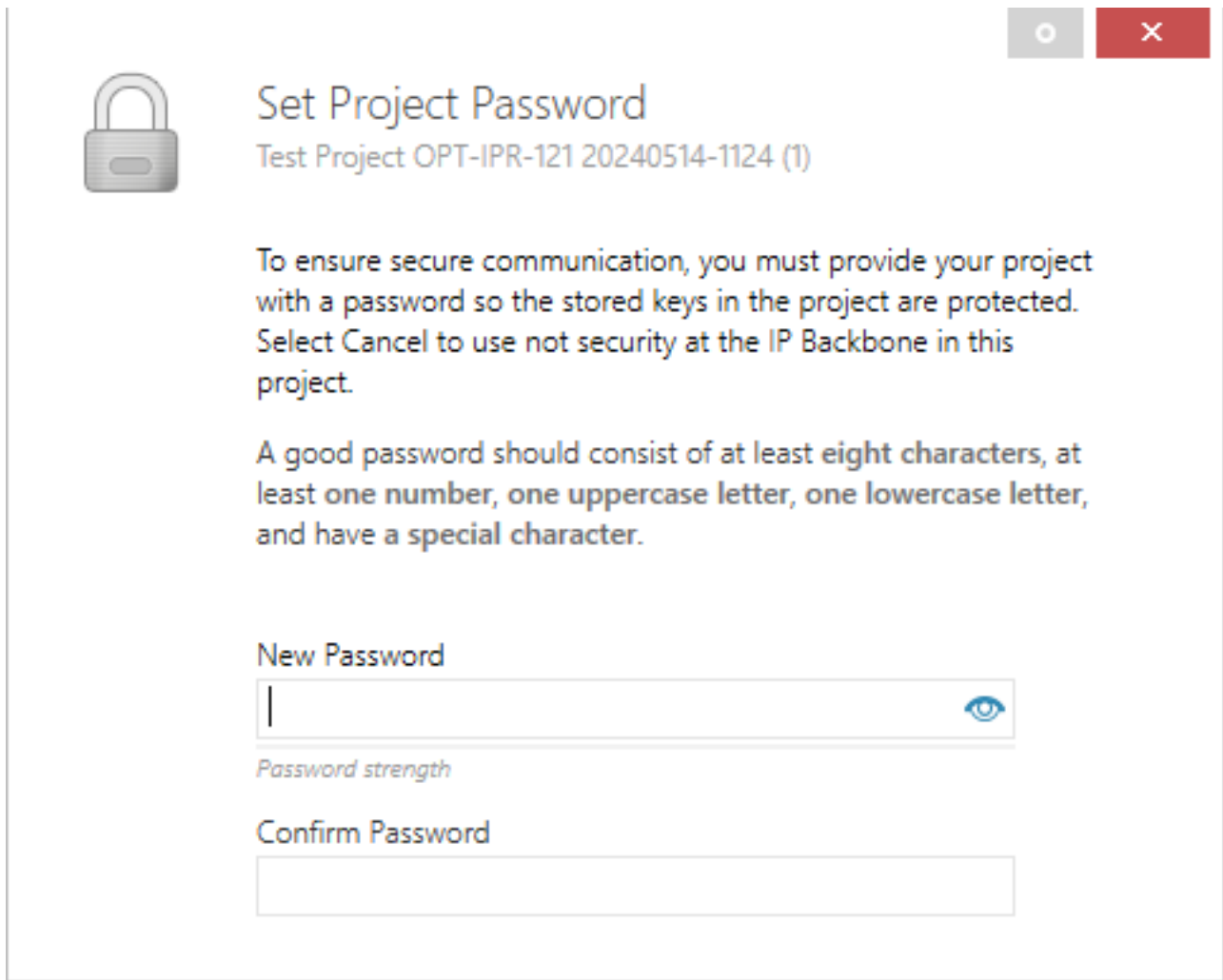
MAC Address
00:24:6D:01:87:BE

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

2.1 ETS Database

The ETS database (ETS 5.7 or higher) can be downloaded from the product website of The KNX IP Router Secure (www.optimusst.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
Test Project OPT-IPR-121 20240514-1124 (1)

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.

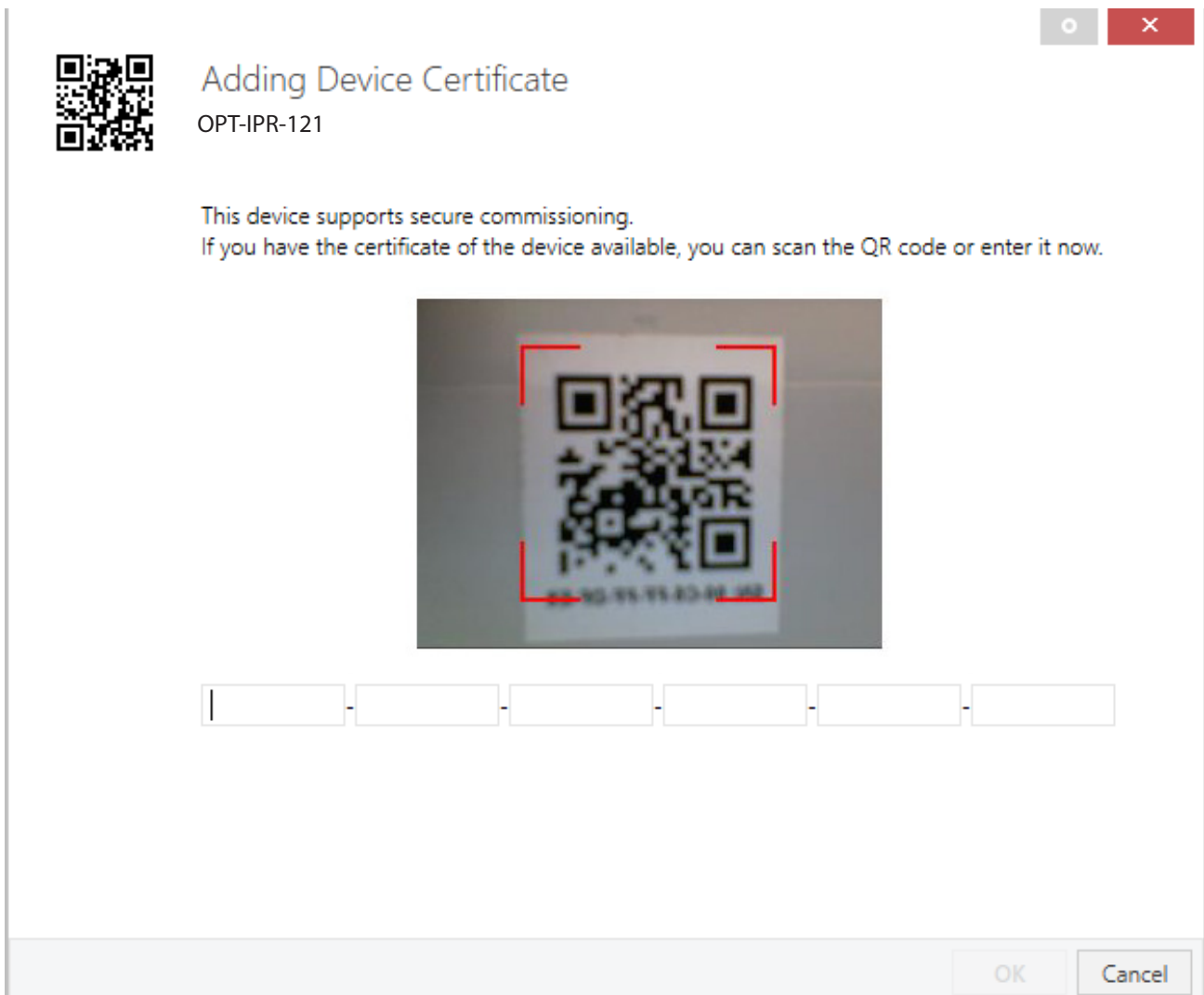
New Password

Password strength

Confirm Password

This password protects the ETS project from unauthorized access. This password is not a key that is used for KNX communication. The entry of the password can be bypassed with "Cancel", but this is not recommended for security reasons.

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

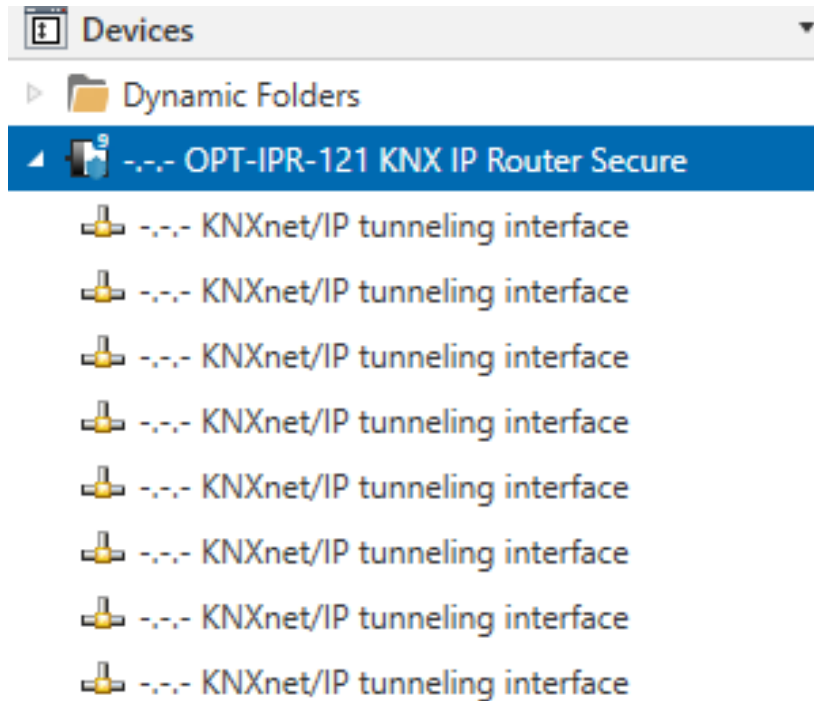


The certificate is printed as text on the device. It can also be conveniently scanned from the printed QR code via a webcam.

The list of all device certificates can be managed in the ETS Overview - Projects - Security window. This initial key is required to safely put a device into operation from the start. Even if the ETS download is recorded by a third party, the third party has no access to the secured devices afterwards. During the first secure download, the initial key is replaced by the ETS with a new key that is generated individually for each device. This prevents persons or devices who may know the initial key from accessing the device. The initial key is only reactivated after a master reset.

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

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

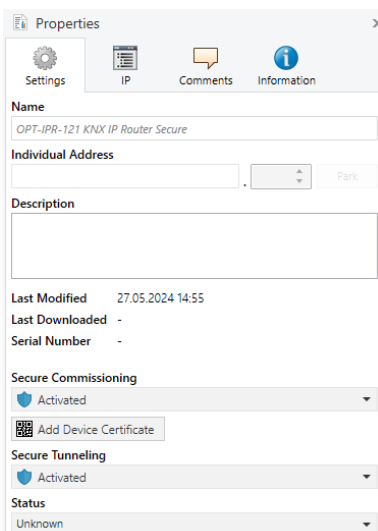


Each individual KNX address can be changed by clicking on the list entry and typing in the desired address into the "Individual Address" text-field. If the text-field frame switches to color red after entering the address, the address is already taken within your ETS project.

NOTE:

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

By clicking on The KNX IP Router Secure device entry within your ETS projects topology view, an information column 'Properties' will appear on the right side of the ETS window. Within the 'Settings' overview, you can change the name of the device.



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

Within the "IP" overview the IP network specific options of The KNX IP Router Secure can be changed.

By changing "obtain an IP address automatically (via DHCP)" to "Use a static IP address" (static IP address) the IP address, subnet mask, and default gateway can be set freely.

NOTE:

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

The screenshot shows a 'Properties' dialog box with four tabs: Settings, IP, Comments, and Information. The 'IP' tab is active. It contains the following elements:

- Two radio buttons: 'Obtain an IP address automatically' (unselected) and 'Use a static IP address' (selected).
- Text input fields for 'IP Address', 'Subnet Mask', and 'Default Gateway', all containing the value '255.255.255.255'.
- A text input field for 'MAC Address' containing 'Unknown'.
- A text input field for 'Multicast Address' containing '224.0.23.12'.
- A text input field for 'Commissioning Password' containing 'o(*F#U7<'. Below it is a progress bar labeled 'Good'.
- A text input field for 'Authentication Code' containing 'c, n+Jcu'. Below it is a progress bar labeled 'Good'.

2.2 IP Address

Here the IP address of The KNX IP Router Secure can be entered. This is used to address the device via the IP network (LAN). The IP addressing should be coordinated with the administrator of the network.

2.3 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 telgrafs directly to the partner but to the gateway that routes the telgraf.

2.4 Default Gateway

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

2.5 Routing Multicast Address

This address is used for routing telgrams on IP. The multicast IP address 224.0.23.12 was reserved (KNXnet/IP) at the IANA (Internet Assigned Numbers Authority) for this purpose. If a different multicast IP address is required, it must be within the range of 239.0.0.0 to 239.255.255.255.

Example of assigning IP addresses

A PC is to be used to access The KNX IP Router Secure.

IP address of the PC: 192.168.1.30

Subnet of the PC: 255.255.255.0

The KNX IP Router Secure is located in the same LAN, i.e. it uses the same subnet. The subnet constrains the IP addresses that can be assigned. In this example, the IP address of the KNX IP Router Secure must be 192.168.1.xx, where xx can be a number from 1 to 254 (with the exception of 30, which is already taken by the client PC). It must be ensured that no IP addresses are assigned twice.

IP address of the KNX IP Router Secure: 192.168.1.31

Subnet of the KNX IP Router Secure: 255.255.255.0

2.6 Remote Access

Remote access via Internet is possible with The KNX IP Router Secure. More details can be found in the document "Remote access with the ETS" at www.optimusst.com.

2.7 ETS Parameter Dialogue

The following parameters can be set using the ETS.

2.8 General Settings

--- OPT-IPR-121 KNX IP Router Secure > General

Description	Note: For device name and IP settings see dialog "Properties"	
General	Programming Mode on Device Front	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Routing (KNX -> IP)	Manual Operation	without Time Limit
Routing (IP -> KNX)		

Prog. Mode On Device Front

In addition to the normal programming button ④ the device allows activating the programming mode on the device front without opening the switchboard cover. The programming mode can be activated and deactivated via pressing simultaneously both buttons ⑦ and ⑧.

This feature can be enabled and disabled via the parameter "Prog. mode on device front". The recessed programming button ③ (next to the Programming LED ②) is always enabled and not influenced by this parameter.

Manual operation on device

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

Routing (KNX -> IP)

--- OPT-IPR-121 KNX IP Router Secure > Routing (KNX -> IP)

Description	Group Telegrams (Main Groups 0 to 13)	Filter
General	Group Telegrams (Main Groups 14 to 31)	Filter
Routing (KNX -> IP)	Individual Addressed Telegrams	Filter
Routing (IP -> KNX)	Broadcast Telegrams	<input type="radio"/> Block <input checked="" type="radio"/> Route
	Acknowledge (ACK) of Group Telegrams	<input type="radio"/> Always <input checked="" type="radio"/> Only if routed
	Acknowledge (ACK) of Individual Addressed Telegrams	Only if routed

Group telgrafs (main group 0 to 13)

- Block : No group telgrafs of this main group are routed to IP.
- Route : All group telgrafs of this main group are routed to IP independent of the filter table. This setting is for test purposes only.
- Filter : The filter table is used to check whether or not the received group telgraf should be routed to IP.

Group telgrafs (main group 14 to 31)

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

Individually addressed telgrafs

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

Broadcast Telgrafs

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

Acknowledge (ACK) Of Group Telgrafs

Always	:	A acknowledge is generated for every received group telgraf (from KNX).
Only if routed	:	A acknowledge is only generated for received group telgrafs (from KNX) if they are routed to IP.

Acknowledge (ACK) Of Individually Addressed Telgrafs

Always	:	A acknowledge is generated for every received individual addressed telgraf (from KNX).
Only if routed	:	A acknowledge is only generated for received individually addressed group tele-grams (from KNX) if they are routed to IP.
Answer with NACK	:	Every received individually addressed telgraf (from KNX) is responded to with NACK (Not acknowledge). This means that communication with individually addressed telgrafs on the corresponding KNX line is not possible. Group communication (group telgrafs) 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.

Routing (IP -> KNX)

--- OPT-IPR-121 KNX IP Router Secure > Routing (IP -> KNX)

Description	Group Telegrams (Main Groups 0 to 13)	Filter
General	Group Telegrams (Main Groups 14 to 31)	Filter
Routing (KNX -> IP)	Individual Addressed Telegrams	Filter
Routing (IP -> KNX)	Broadcast Telegrams	<input type="radio"/> Block <input checked="" type="radio"/> Route
	Repetition of Group Telegrams	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
	Repetition of Individual Addressed Telegrams	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
	Repetition of Broadcast Telegrams	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled

Group telgrafs (main group 0 to 13)

- Block : No group telgrafs of these main groups are routed to KNX
 Route : All group telgrafs of this main group are routed to KNXG independent of the filter table. This setting is used for testing purposes only.
 Filter : The filter table is used to check whether the received group telgraf should be routed to KNX.

Group telgrafs (main group 14 to 31)

- Block : No group telgrafs of main groups 14 to 31 are routed to KNX.
 Route : All group telgrafs of the main groups 14 to 31 are routed to KNX.
 Filter : The filter table is used to check whether the received group telgraf should be routed to KNX.

Individually addressed telgrafs

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

Broadcast Telgrafs

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

Repetition Of Group Telgrafs

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

Repetition Of Individually Addressed Telgrafs

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

Repetition of broadcast telgrafs

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

Programming

The KNX IP Router Secure can be programmed in different ways by the ETS:

Via KNX Bus

The device only needs to be connected to the KNX bus. The ETS requires an additional interface (for example, USB) to have access to the bus. Via this way both the individual address and the entire application including IP configuration can be programmed. Programming via the bus is recommended if no IP connection can be established.

Via KNXnet/IP Tunneling

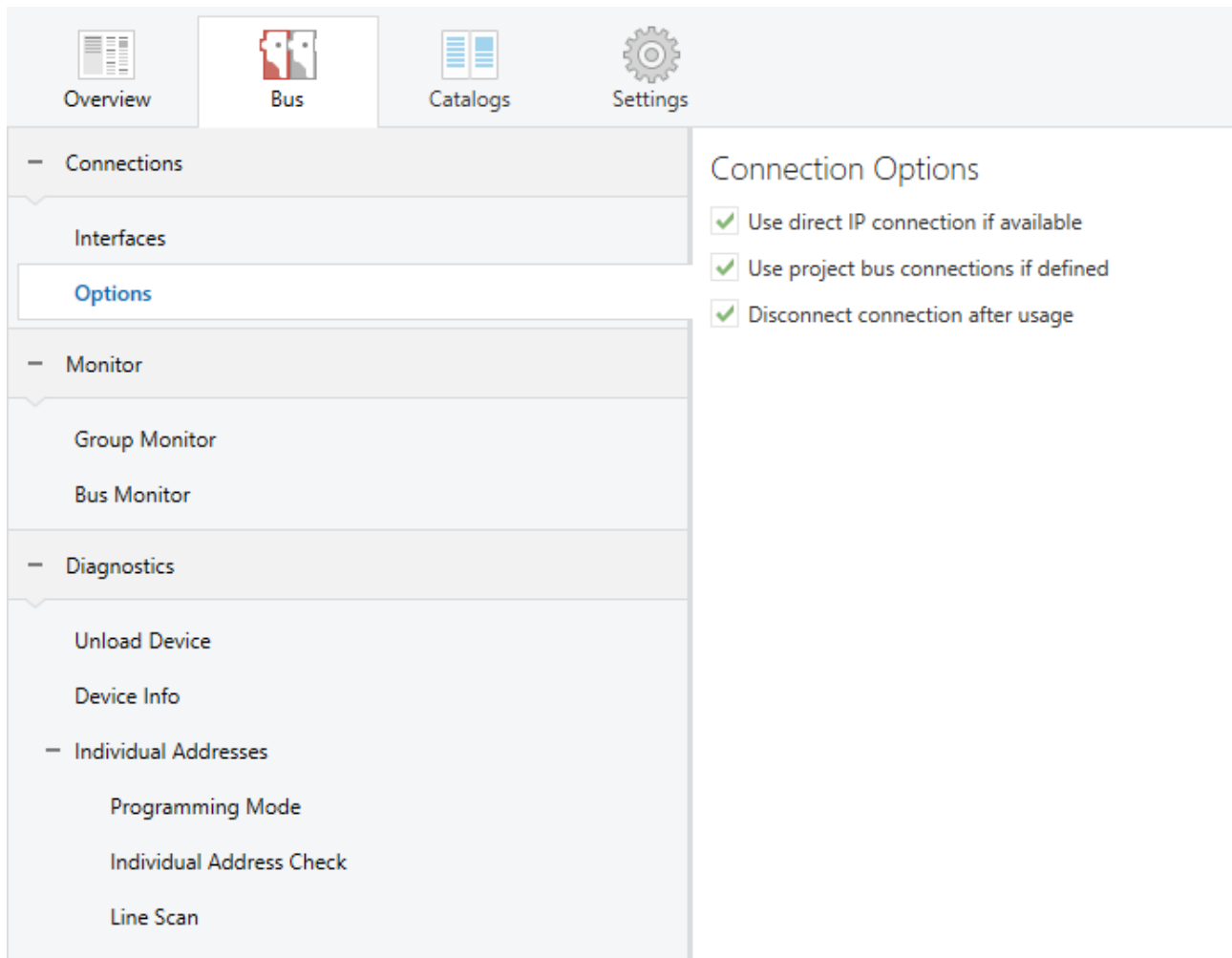
No additional interface is required. Programming via KNXnet/IP Tunneling is possible if the device already has a valid IP configuration (e.g. via DHCP). In this case the device is displayed in the interface configuration of the ETS and must be selected. The download is executed via the ETS project as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

Via KNXnet/IP Routing

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

Via direct IP Connection

While KNXnet/IP Tunneling and KNXnet/IP Routing is limited to the speed of KNX TP the device can be loaded via a direct IP connection at high speed. The direct IP connection is possible if the device already has a valid IP configuration as well as an individual address. To do this select "Use direct IP connection if available" in the ETS menu "Bus – Connections - Options". The download is then directly performed in the device and is not visible in the ETS group monitor.

**NOTE:**

Due to the significantly shorter transmission times it is recommended to perform downloads via IP.



—
OPTIMUS SOLUTION Teknoloji
Üretim Sanayi Ticaret A.Ş.
Emek Mh. Ordu Cd.
No: 4 34785 Sancaktepe
İstanbul / Türkiye
Tel.: +90 216 487 33 46
Fax: +90 216 487 33 48
Email: info@optimusst.com

Copyright 2022 OPTIMUS SOLUTIONS. Önceden haber vermeksizin teknik değişiklikler yapma veya bu belgenin içeriğini değiştirme hakkımız saklıdır. Mutabık kalınan özellikler verilen tüm siparişler için kesindir. OPTIMUS SOLUTIONS, bu belgedeki olası hatalar veya olası bilgi eksiklikleri için hiçbir şekilde sorumluluk kabul etmez. Bu belgedeki ve burada yer alan konu ve resimlerdeki tüm hakları saklı tutarız. OPTIMUS SOLUTIONS'in önceden yazılı izni olmaksızın, içeriğin - bunların bölümleri de dahil olmak üzere - çoğaltılması, üçüncü şahıslara aktarılması veya işlenmesine izin verilmez.