

EAE KNX IP Router Secure

Product Manual IPR200S



Contents

1. General.....	3
1.1. Technical Data.....	3
1.2. Installation and Connection	4
2. KNX Programming Mode.....	4
3. Status display	4
4. Factory default settings	6
5. Reset to factory device settings.....	6
6. Interface settings with ETS.....	6
7. Coupler function (KNXnet/IP Routing)	8
8. ETS Database.....	11
8.1. IP Address	13
8.2. Subnet Mask	13
8.3. Default Gateway	13
8.4. Routing Multicast Address	13
8.5. Example of assigning IP addresses	13
8.6. Multicast Address Change.....	13
9. ETS parameter dialogue	14
9.1. General settings	14
9.2. Programming mode on device front	14
9.3. Manual operation on device	14
9.4. Routing (KNX -> IP).....	14
9.5. Routing (IP -> KNX).....	16
Repetition of group telegrams	17
Repetition of individually addressed telegrams	17
Repetition of broadcast telegrams.....	17
10. Programming	17
10.1. Via KNX Bus	17
10.2. Via KNXnet/IP Tunneling	18
10.3. Via KNXnet/IP Routing	18
10.4. Via direct IP connection	18

1. General Description

The compact KNX IP Router Secure enables the forwarding of telegrams between different lines via a LAN (IP) as a fast backbone. The device also serves as a programming interface between a PC and the KNX bus (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 unauthorized access to the interface function (tunneling).

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

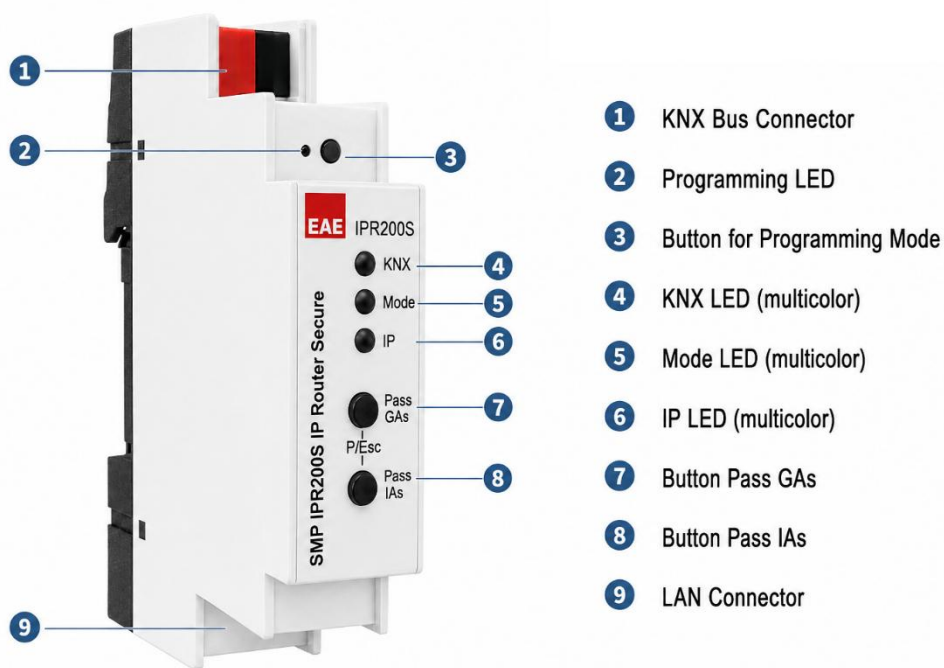
The KNX IP Router Secure has an extended filter table for main groups 0..31 and can buffer up to 150 telegrams. Power is supplied via the KNX bus.

1.1. Technical Data

Protection Type	IP 20	IEC 60 529
Safety Class	III	IEC 61140
Power Supply	Voltage	21...30V DC, SELV
	Current Consumption	< 20 mA
Connections	KNX Line	Bus connection terminal
	IP Line	RJ45
Operating Elements	2 buttons and 3 LEDs (multicolor) KNX programming button with LED (red)	
Ethernet	100BaseT (100Mbit/s) Supported internet protocols ARP, ICMP, IGMP, UDP/IP, TCP/IP DHCP and Auto IP	
KNX	Medium IP/TP Max APDU length: 55 Simultaneous Connections: Up to 8 KNXnet/IP Tunneling Extended filter table for main group 0..31 KNXnet/IP Security (AES-128) Incl. Tunneling V2, Core V2	
Installation	1 unit (18 mm) DIN rail mount	
Temperature Range	Operation	-5° C + 45° C
	Storage	-25° C + 70° C
Humidity	%5 to 93 % non-condensing	
Dimensions	-H x W x D	90 mm x 18 mm x 60 mm
	Width W in mm	18 mm (1 module)
		Mounting depth 58 mm
Weight	40 g	
Box	Plastic (PC)	
CE	in accordance with:	
	• EMC directive 2014 / 30 / EU • RoHS directive 2011 / 65 / EU • EN 63044-3: 2018, • EN 63044-5-1: 2019 • EN 63044-5-2: 2019,	• EN 63044-5-3: 2019 • EN 61000-6-2: 2019 • EN 61000-6-3: 2021 • EN 63000: 2018

1.2. 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.

i The device is not working without KNX bus power.

2. 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**.

3. Status Display

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

Communication failures (e.g. repetitions of telegrams or telegram 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	Telegram traffic on the KNX bus
LED shortly red	Communication failures on the KNX bus

The IP LED ⑥ lights up when an Ethernet link is active. This LED is green if the device has valid IP settings (IP address, Subnet 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.

This LED indicates IP telegram traffic by flickering.

Overview of the different indications of the IP LED ⑥:

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

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

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

With the button Pass IAs ⑧ the forwarding of individually addressed telegrams 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.

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

Overview of the different indications of the Mode LED:

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.

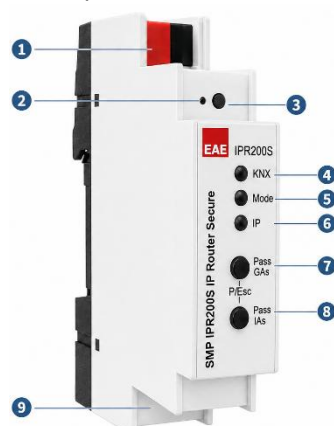
4. Factory Default Settings

The following configuration is set by factory default:

Factory default configuration	
Individual device address	15.15.0
Number of configured KNXnet/IP tunneling configuration	1
Individual address of tunneling configuration	15.15.240
IP address assignment	DHCP
Initial KEY (FDSK)	Active
Security Modus	Not active

5. Reset to Factory Device Settings

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



Disconnect the KNX Bus connector ① from device
Press the KNX programming button ③ and keep it pressed
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.

6. 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 Routers even without a database entry. If the setup of the KNX IP Router does not comply with the conditions of the KNX installation it must be configured via an ETS project. See the ETS 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 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 via the bus.

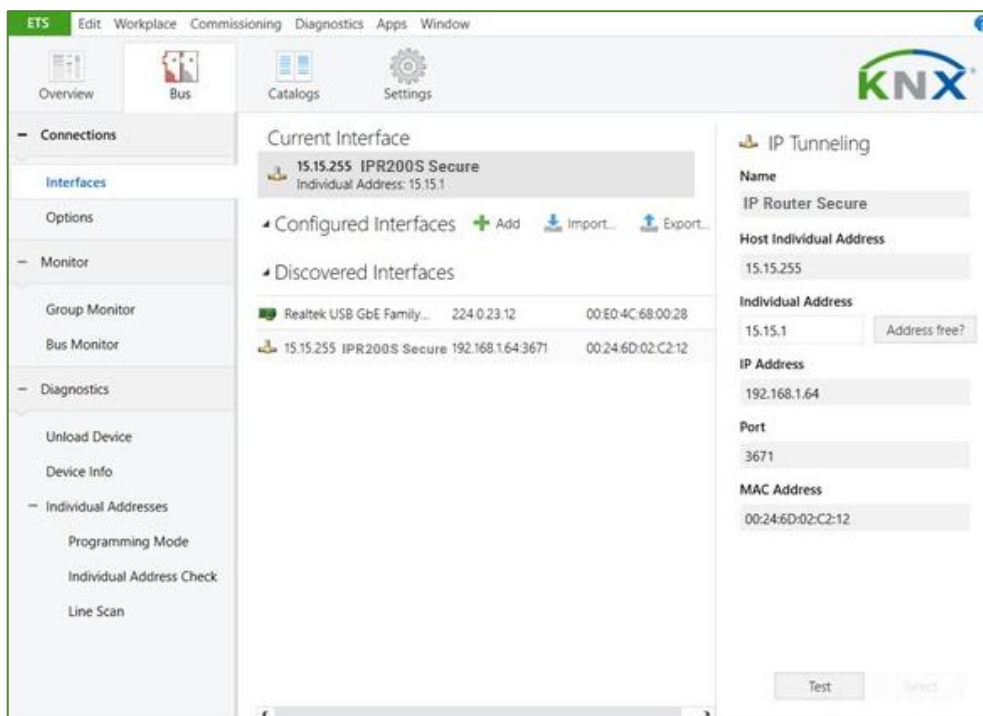
For the interface function the device contains additional individual addresses that can be set in the ETS. When a client (e.g. ETS) sends via the KNX IP Router telegrams to the bus, they contain a sender address as one from the additional addresses. Each address is associated with a connection. Thus,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

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

Example:

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

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



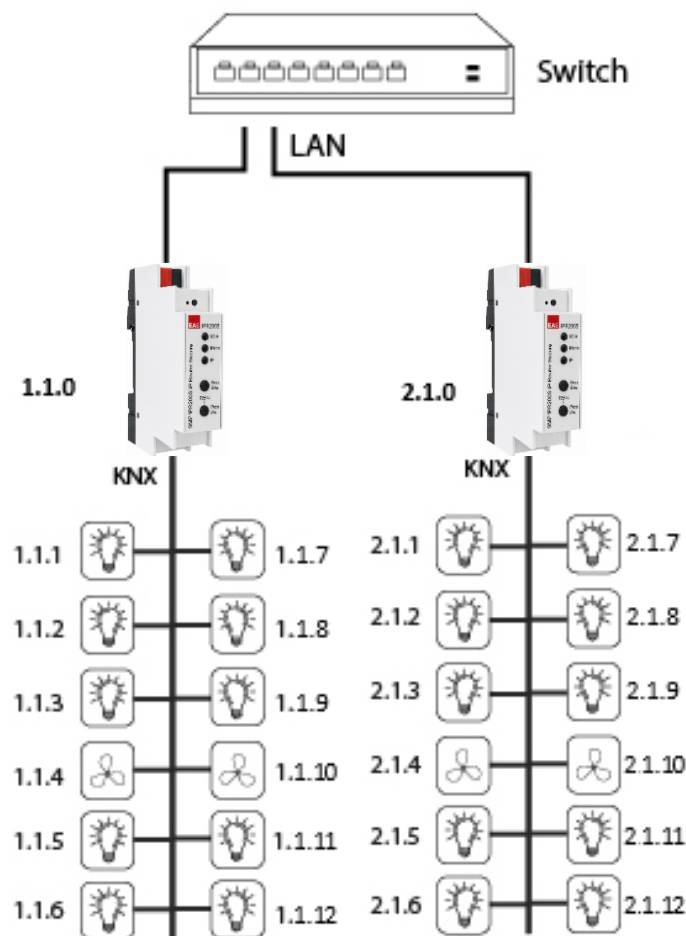
The individual KNX device address and the individual KNX addresses for additional tunneling connections can be changed within the ETS project, after the device has been added to the project.

7. Coupler Function (KNXnet/IP Routing)

The KNX IP Router Secure operates as a line or back-bone coupler. In both cases, the LAN (IP) is used as a backbone.

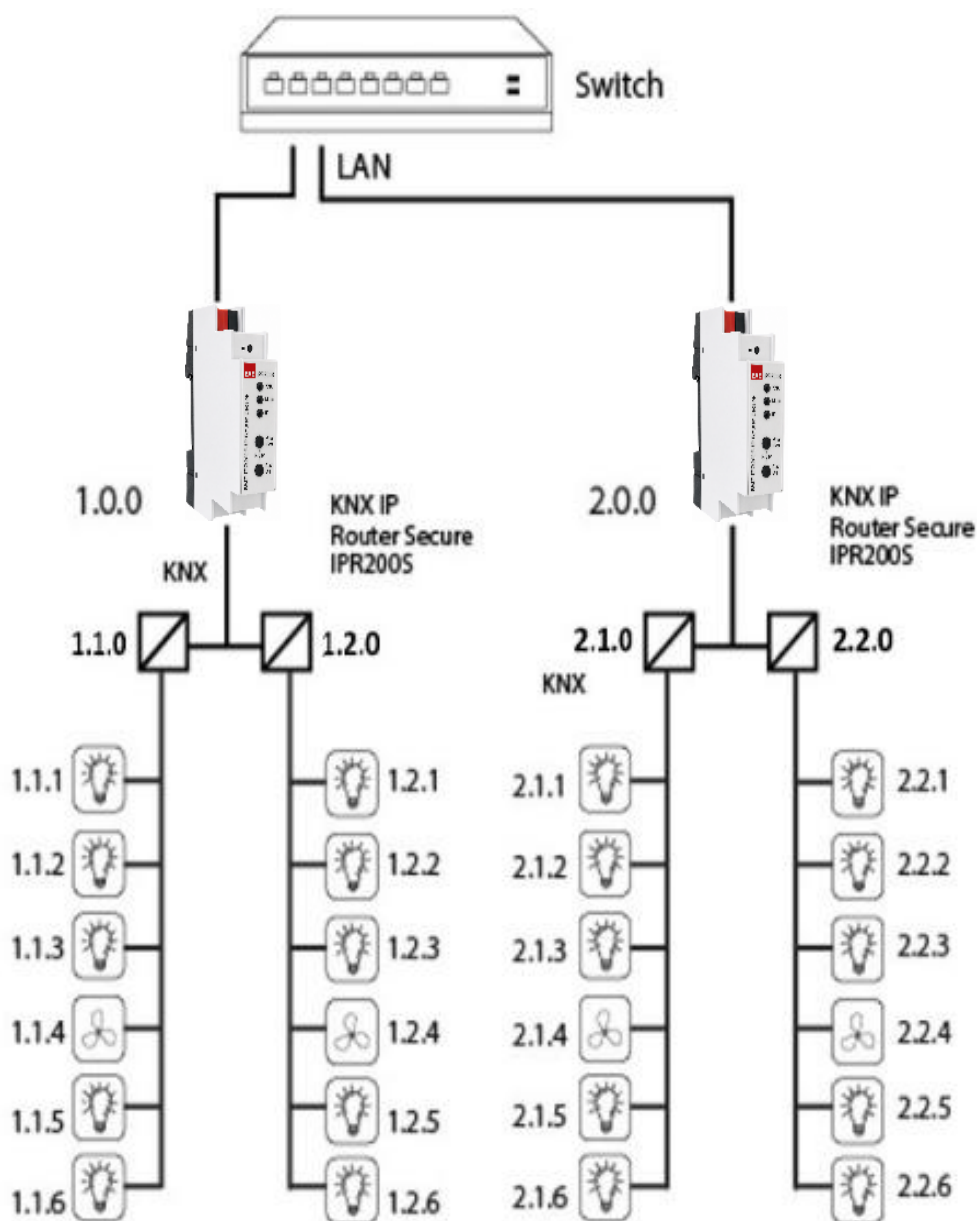
The following table shows the application possibilities of the KNX IP Router Secure compared to the classic topology:

	Classical Topology (without IP)	IP coupling of areas (IP area coupler)	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



KNX IP Router as line coupler

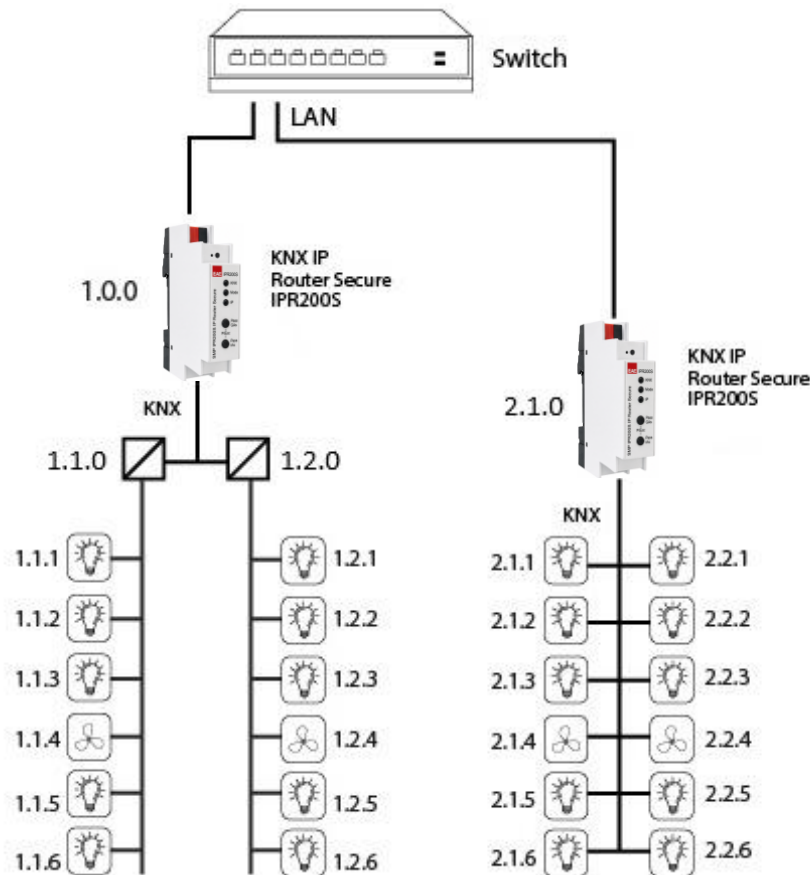
The individual address assigned to the KNX IP Router *Secure* determines whether the device operates as a line or area coupler. If the individual address is in the form of x.y.0 (x, y: 1..15), the router operates as a line coupler. If it is in the form of x.0.0 (x: 1..15), the router acts as a backbone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



KNX IP Router as area coupler

i 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.

i 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.



KNX IP Router as area and line coupler

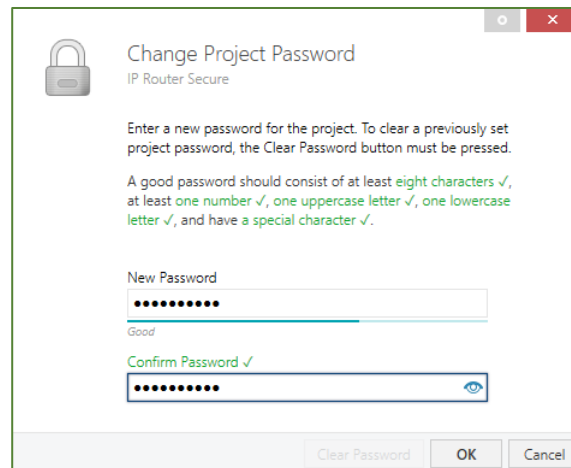
The KNX IP Router has a filter table and thus contributes to reducing the bus load. The filter table (8kB) supports the extended group address range (main groups 0..31) and is automatically generated by the ETS.

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).

8. ETS Database

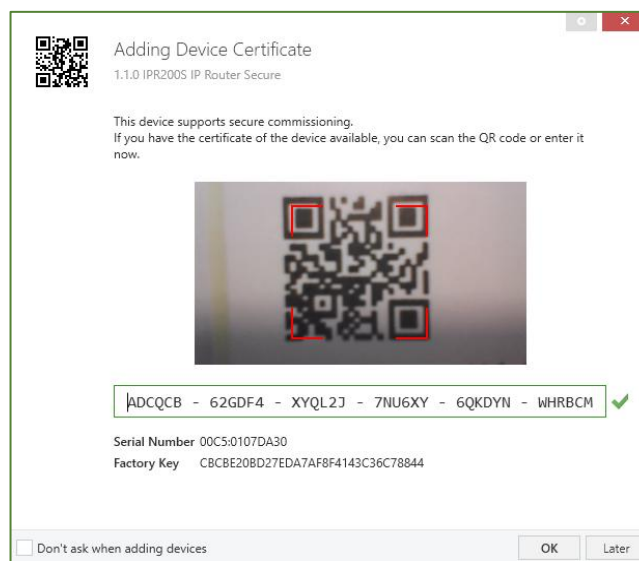
The ETS database (ETS 5.7 or higher) can be downloaded from the product website of the KNX IP Router Secure or via the KNX online catalogue.

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



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).

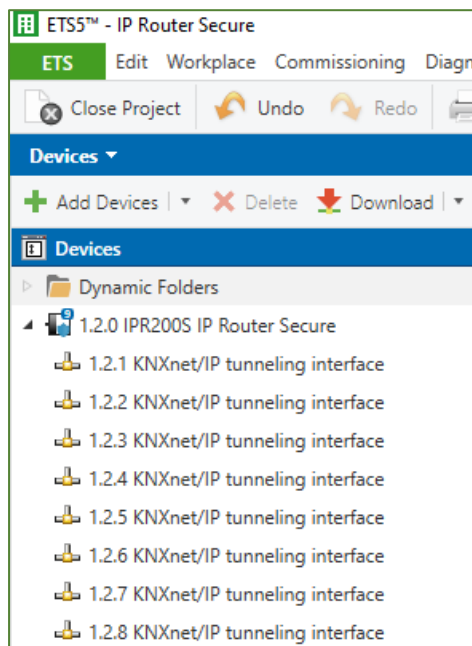


The certificate is printed as text on the device. It can also be conveniently scanned from the printed QR code via a webcam. The list of all device certificates can be managed in the ETS Overview - Projects - Security window.

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.

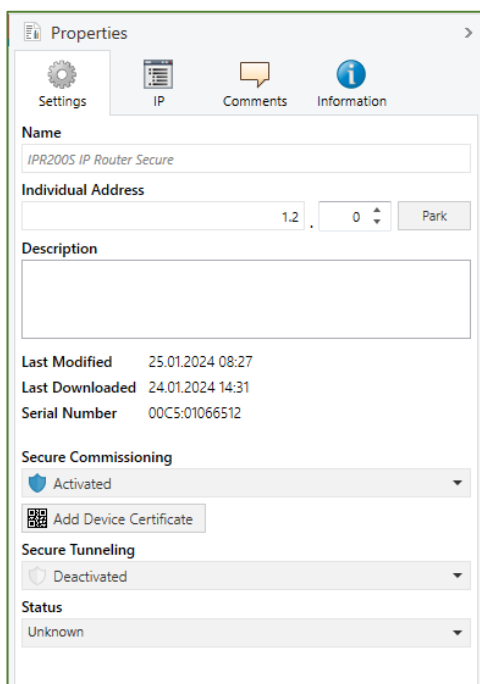
In the ETS, some settings are displayed in addition to the parameter dialog in the properties dialog (at the edge of the screen). The IP settings can be made here. The additional addresses for the interface connections are displayed in the topology view.



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.



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.



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

8.1. 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.

8.2. 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.

8.3. Default Gateway

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

8.4. Routing Multicast Address

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

8.5. Example of Assigning IP Address

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 <i>Secure</i> is located in the same LAN, i.e. it uses the same subnet. The subnet constrains the IP addresses that can be assigned. In this example, the IP address of the KNX IP Router must be 192.168.1.xx, where xx can be a number from 1 to 254 (with the exception of 30, which is already taken by the client PC). It must be ensured that no IP addresses are assigned twice.	
IP address of the IP Router:	192.168.1.31
Subnet of the IP Router:	255.255.255.0

8.6. Multicast Address Change

Multicast address assignment can be configured.

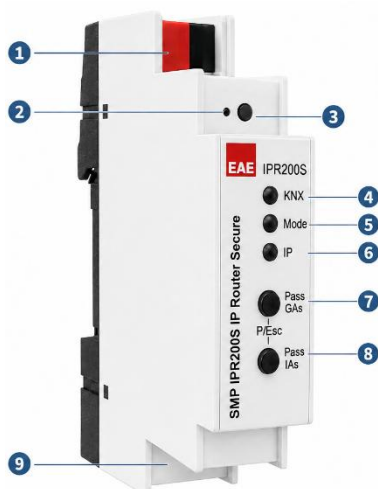
9. ETS Parameter Dialogue

The following parameters can be set using the ETS.

9.1. General Settings

1.2.0 IPR200S IP Router Secure > General settings	
Description	Note: For device name and IP settings see dialog "Properties"
General settings	Prog. mode on device front: ☐ Disabled ☒ Enabled Manual operation on device: Enabled without time limit
Routing (KNX -> IP)	
Routing (IP -> KNX)	

9.2. Programming Mode on Device Front



In addition to the normal programming button **3** 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 **2** (next to the Programming LED **2**) is always enabled and not influenced by this parameter.

9.3. Manual operation on device

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

9.4. Routing (KNX -> IP)

1.2.0 IPR200S IP Router Secure > Routing (KNX -> IP)	
Description	Group telegrams (main groups 0 to 13): Route
General settings	Group telegrams (main groups 14 to 31): Route
Routing (KNX -> IP)	Individual addressed telegrams: Route
Routing (IP -> KNX)	Broadcast telegrams: ☐ Block ☒ Route Acknowledge (ACK) of group telegrams: ☐ Always ☒ Only if routed Acknowledge (ACK) of individual addressed telegrams: Only if routed

Group Telegrams

- **Block** → No group telegrams of this main group are routed to the IP.
- **Routing** → All group telegrams of this main group are routed to the main line independent of the filter table.
- **Filter** → The filter table is used to check whether or not the received group telegram should be routed to the main line.



The setting “Route” should only be used for test purposes.

Group telegrams (main group 14 to 31)	
Block:	No group telegrams of main groups 14 to 31 are routed to IP.
Route:	All group telegrams of main groups 14 to 31 are routed to IP.
Filter:	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:	Acknowledge is generated for every received group telegram (from KNX).
Only if routed:	Acknowledge is only generated for received group telegrams (from KNX) if they are routed to IP.

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



When using “Answer with NACK” an access to the device via KNX TP is no longer possible. The configuration must be performed via IP.

9.5. Routing (IP -> KNX)

1.2.0 IPR200S IP Router Secure > Routing (IP -> KNX)

Description	Group telegrams (main groups 0 to 13)	Route
General settings	Group telegrams (main groups 14 to 31)	Route
Routing (KNX -> IP)	Individual addressed telegrams	Route
Routing (IP -> KNX)	Broadcast telegrams	☐ Block ☒ Route
	Repetition of group telegrams	☐ Disabled ☒ Enabled
	Repetition of individual addressed telegrams	☐ Disabled ☒ Enabled
	Repetition of broadcast telegrams	☐ Disabled ☒ Enabled

Group telegrams (main group 0 to 13)	
Block:	No group telegrams of these main groups are routed to KNX.
Route:	All group telegrams of this main group are routed to KNXG independent of the filter table. This setting is used for testing purposes only.
Filter:	The filter table is used to check whether the received group telegram should be routed to KNX.

Group telegrams (main group 14 to 31)	
Block:	No group telegrams of main groups 14 to 31 are routed to KNX.
Route:	All group telegrams of the main groups 14 to 31 are routed to KNX.
Filter:	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 resent to KNX in case of a fault.
Enabled:	The received group telegram is resent up to three times in case of a fault.

Repetition of individually addressed telegrams	
Disabled:	The received individually addressed telegram is not resent to KNX in case of a fault.
Enabled:	The received individually addressed telegram is resent up to three times in case of a fault.

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

10. Programming

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

10.1. 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.

10.2. Via KNXnet/IP Tunneling

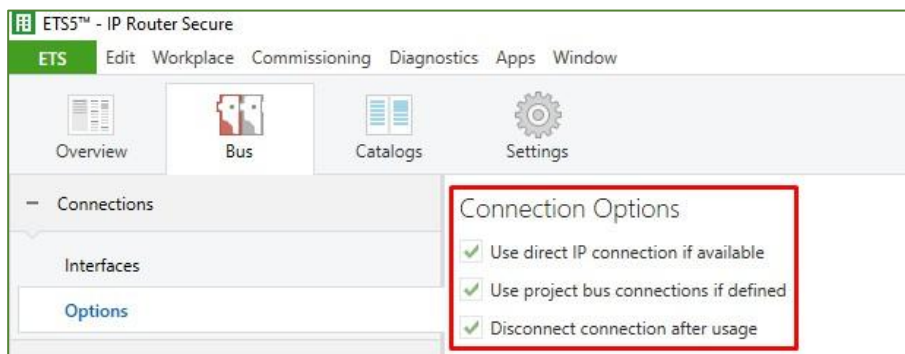
No additional interface is required. Programming via KNXnet/IP Tunneling is possible if the device already has a valid IP configuration (e.g. via DHCP). In this case the device is displayed in the interface configuration of the ETS and must be selected. The download is executed via the ETS project as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

10.3. 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.

10.4. 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.



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

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/>

Copyright 2008, Google Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in

the documentation and/or other materials provided with the distribution.

Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this

software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Commissioning

Determination of the physical address and setting of parameters are actualized with Engineering Tool Software (version 5.7 or higher). ".knxprod" file must be imported to the ETS.



Installation and commissioning of device may only be implemented by trained electricians. The relevant standards, directives, regulations and instructions must be observed when planning and implementing the electrical installation.

- When connecting the device make sure that the device can be isolated!
- Protect the device against moisture, dirt and damage during transport, storage and operation!
- Do not operate the device out of the specified technical data which is stated.
- The device may only be operated in closed enclosures (Distribution boards)