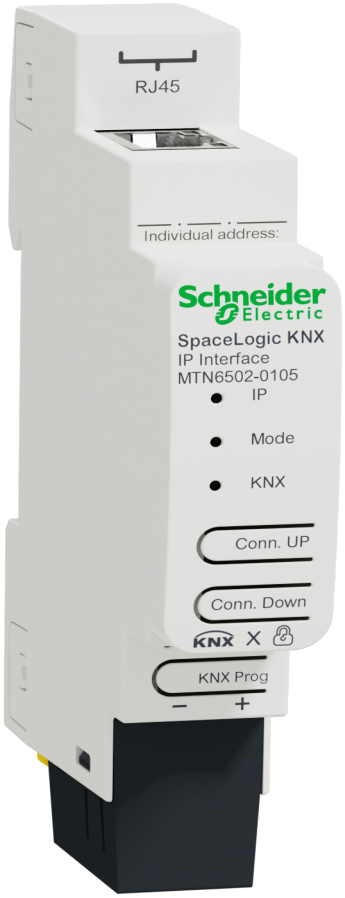
SpaceLogic KNX IP Interface DIN Rail

Product information and Application description

This document gives you product information about the SpaceLogic KNX IP Interface DIN Rail, MTN6502-0105 and describes the ETS application KNX IP Interface secure 7133/1.0

MTN6502-0105
12/2019



Legal Information

Table of Contents

Safety information

Important information

Read these instructions carefully and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this manual or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of either symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that accompany this symbol to avoid possible injury or death.

⚠⚠DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

Failure to follow these instructions will result in death or serious injury.

⚠WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result in** minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

For your safety

⚠⚠DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

Safe electrical installation must be carried out only by qualified electrical personnel. Qualified electrical personnel must prove profound knowledge in the following areas:

- Connecting to installation networks
- Connecting several electrical devices
- Laying electric cables
- Connecting and establishing KNX networks
- Connecting and establishing LAN networks
- Safety standards, local wiring rules and regulations

Failure to follow these instructions will result in death or serious injury.

Product information

The SpaceLogic KNX IP Interface serves as an universal interface for PC or Laptop to the KNX bus. The KNX bus can be accessed from any point on the LAN. The SpaceLogic KNX IP Interface can be used as a programming interface for ETS. For access via KNXnet/IP Tunneling max. 8 simultaneous connections are possible.

The device optionally supports KNX Security, which can be activated in the ETS. As a secure interface, the device prevents unauthorized access to the system.

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 and tunneling.

Power is supplied via the KNX bus.

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 (twisted pair) 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 KNX bus are also encrypted.

KNX IP Security for the interface function

When using the device 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 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.

KNX Data Security for the device

The KNX IP Interface also supports KNX Data Security to protect the device from unauthorized access from the KNX bus. If the KNX IP Interface is programmed via the KNX bus, this is done with encrypted telegrams.

> **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 (for example, USB) and any intermediate line couplers support the so-called KNX long frames.

The secured device configuration is also contained in KNX data security.

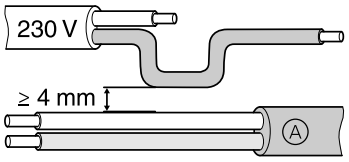
Installation and connection

The device is designed for installation on a DIN rail with a width of 1 unit (18 mm).

⚠⚠DANGER

HAZARD OF ELECTRIC SHOCK AND DEVICE DAMAGE

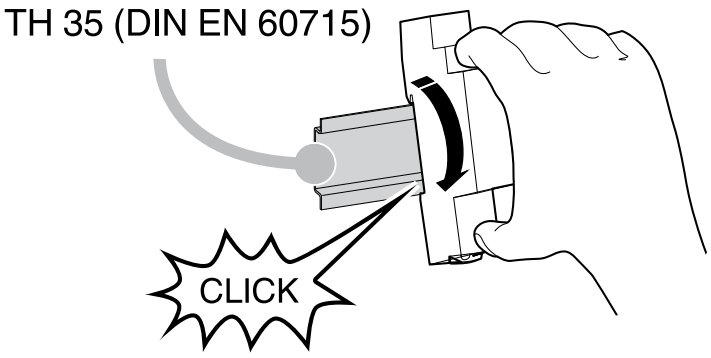
- Ensure a safety clearance of minimum 4 mm between the individual cores of the 230 V supply cable and the KNX line Ⓐ, in accordance with IEC 60664-1.



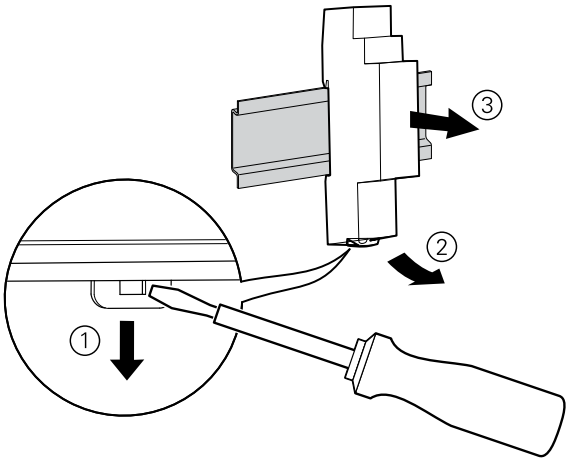
- Ensure that the installed devices have minimum basic insulation next to the device.

Failure to follow these instructions will result in death or serious injury.

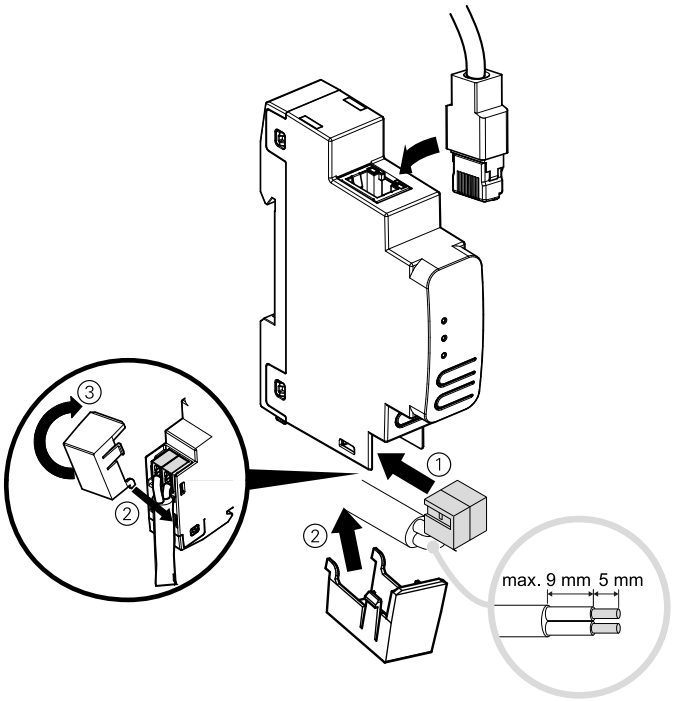
Installing



Removing



Connecting



NOTICE

EQUIPMENT DAMAGE AND LOSS OF COMMUNICATION

Installation of communication cabling for information technology must be guaranteed in accordance with DIN EN 50174.

Failure to follow these instructions can result in equipment damage.

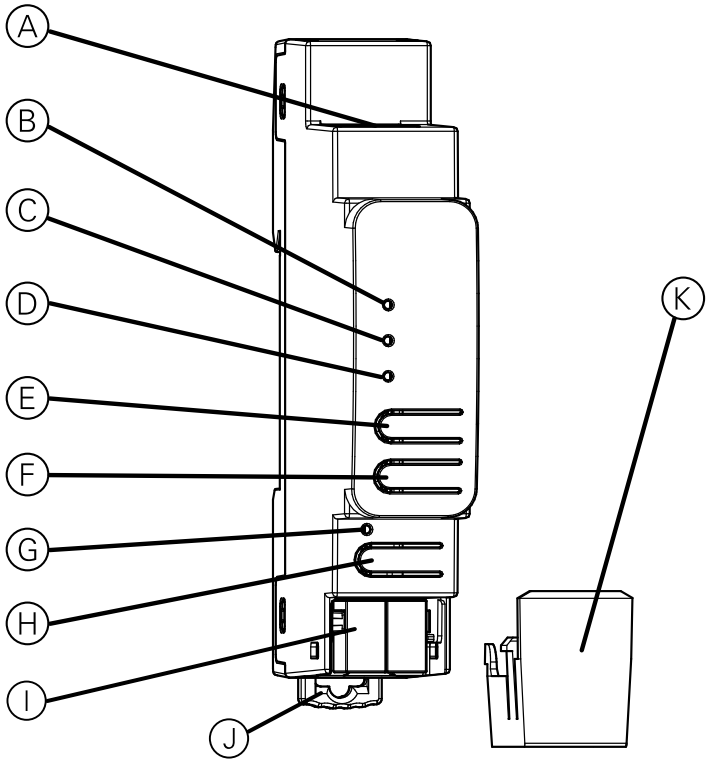
Technical data

Power supply	via KNX bus, <20mA

Connection	
LAN	RJ45 Connector
KNX	Bus connecting terminal

Dimension (LxWxD)	100x18x86 mm
Device width	1 module = 18 mm

Connections and operating elements



A	Ethernet/LAN Connector
B	IP LED (multicolor)
C	Mode LED (multicolor)
D	KNX LED (multicolor)
E	Button: Conn Up (Selection of the connection number upwards)
F	Button: Conn Down (Selection of the connection number downwards)
G	Programming LED (red)
H	Button for programming mode
I	KNX bus connector
J	Release lever for disassembly
K	Cable cover

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

NOTE: The device does not work without bus power.

KNX Programming mode

The KNX programming mode is activated/deactivated by pressing the flushed KNX programming button Ⓗ.

It is possible to write the programmed individual address on the labeling field with a non permanent marker or pencil. So it is possible to change it, if needed.

Status display

Overview of the different indications of the IP LED

IP LED Ⓑ Status	**Meaning**
LED lights green	The device has an active Ethernet link and valid IP settings (IP address, Subnet, and Gateway.)
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.

Overview of the different indications of the Mode LED

Mode LED Ⓒ Status	**Meaning**
LED lights green	Device is working in standard operation mode.
LED flashes green 1x..8x	Manual operation is active. The selected tunnel (1-8) is not used and free.
LED flashes orange 1x…8x	Manual operation is active. The selected tunnel (1-8) is used.
LED flashes red	Manual operation is not active. The device is not properly loaded. For example, after an interrupted download.

Overview of the different indications of the KNX LED

KNX LED Ⓓ Status	**Meaning**
LED lights green	Device is successfully powered by the KNX bus.
LED flickers green	Telegram traffic on the KNX bus.
LED shortly red	Communication failures on the KNX bus. For example, repetitions of telegrams or telegram fragments are indicated by a short change of the LED color to red.

Manual operation

The Mode LED Ⓒ can visualize the status of each KNXnet/IP tunneling connection.

With the buttons Conn Up/Dn Ⓔ Ⓕ, you can choose each single connection. Conn Up Ⓔ counts the connection numbers up and Conn Down Ⓕ down. The actually selected connection number is indicated by repeatedly flashing (1x…8x) of the Mode LED Ⓒ. An available KNXnet/IP Tunneling connection is indicated by a green LED and a used tunneling connection is indicated by an orange LED.

If neither programming mode nor manual operation are active, the Mode LED Ⓒ can visualize configuration errors.

Factory default settings

The following configuration is set by factory default:

Individual device address	**15.15.255**
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**

Reset to factory device settings (master reset)

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

1. Disconnect the KNX Bus connector Ⓘ from device.
2. Press the KNX programming button Ⓗ and keep it pressed down.
3. Reconnect the KNX Bus connector of device.
4. Keep the KNX programming button Ⓗ pressed for at least another 6 seconds.

A short flashing of all LEDs (Ⓖ, Ⓓ, Ⓒ, Ⓑ) visualizes the successful reset of the device to factory default settings.

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 Interface even without a database entry. If the setup of the KNX IP Interface does not comply with the conditions of the KNX installation it must be configured via an ETS project. See the *ETS project, page 18* 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. (For example, many DSL routers have an integrated DHCP server.)

If the KNX IP Interface has been connected to the LAN and has a valid IP address, it should automatically appear in the ETS within the menu **Bus** under **Discovered interfaces**.

By clicking **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 Interface 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 Interface via the bus.

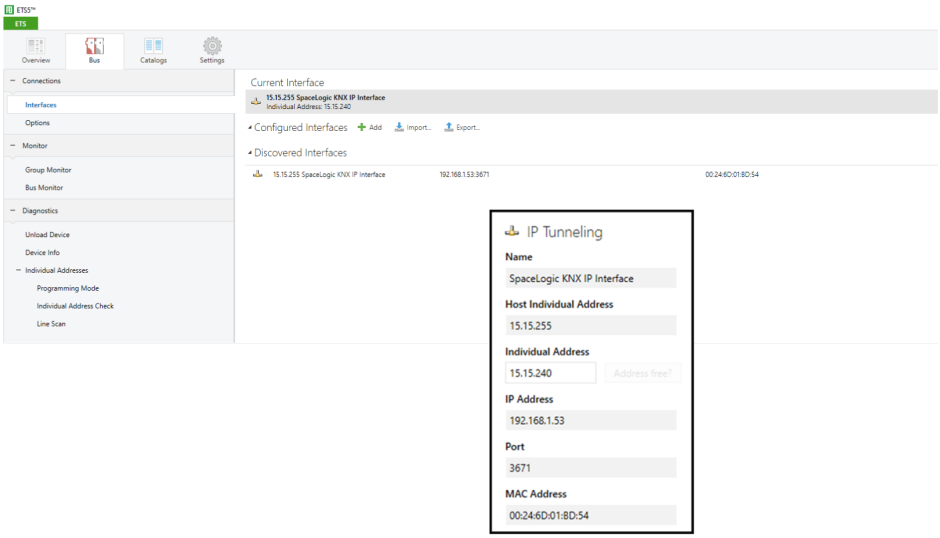
For the interface function, the device contains additional individual addresses that can be set in the ETS. When a client (for example, ETS) sends via the KNX IP Interface telegrams to the bus, they contain a sender address as one from the additional addresses. Each address is associated with a connection.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

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.

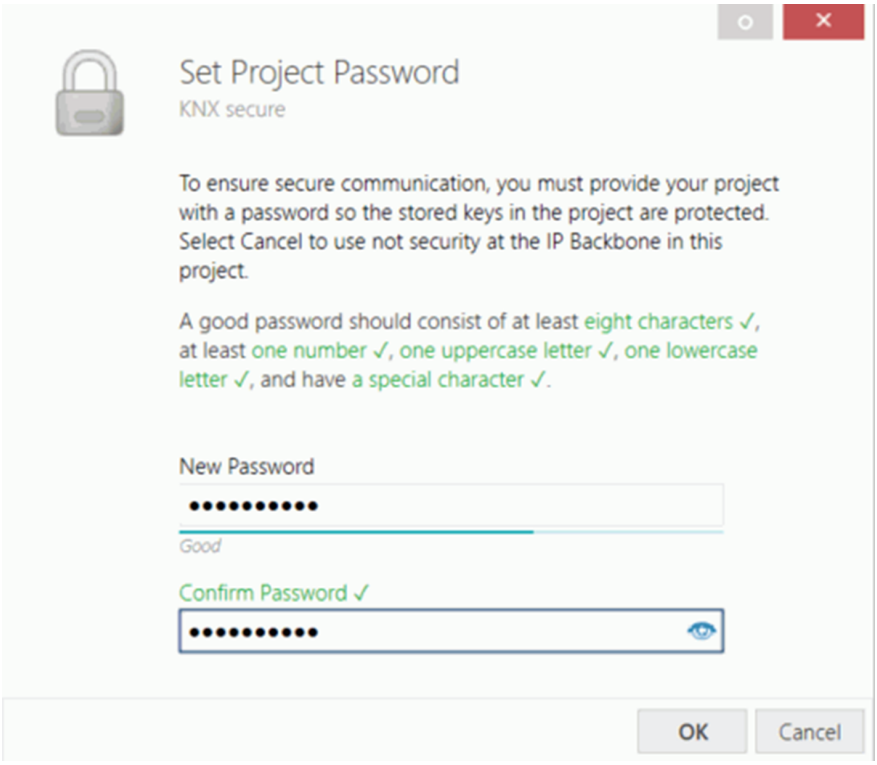
ETS application

The ETS database (ETS 5.7 or higher) can be downloaded from the product website of the KNX IP Interface (*www.schneider-electric.com*) or via the KNX online catalogue.

Product family	1.3 Interfaces/Gateways
Product type	1.3.14 IP devices
Manufacturer	Schneider Electric Industries SAS
Name	Spacelogic KNX USB Interface DIN Rail
Order number	MTN6502-0101

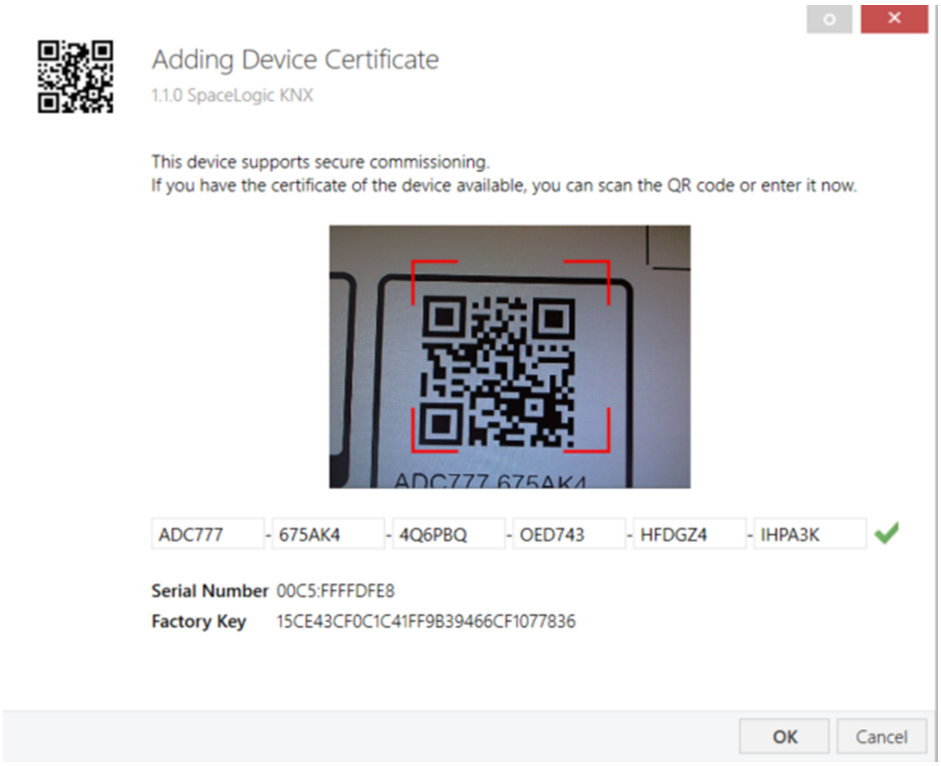
ETS project

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



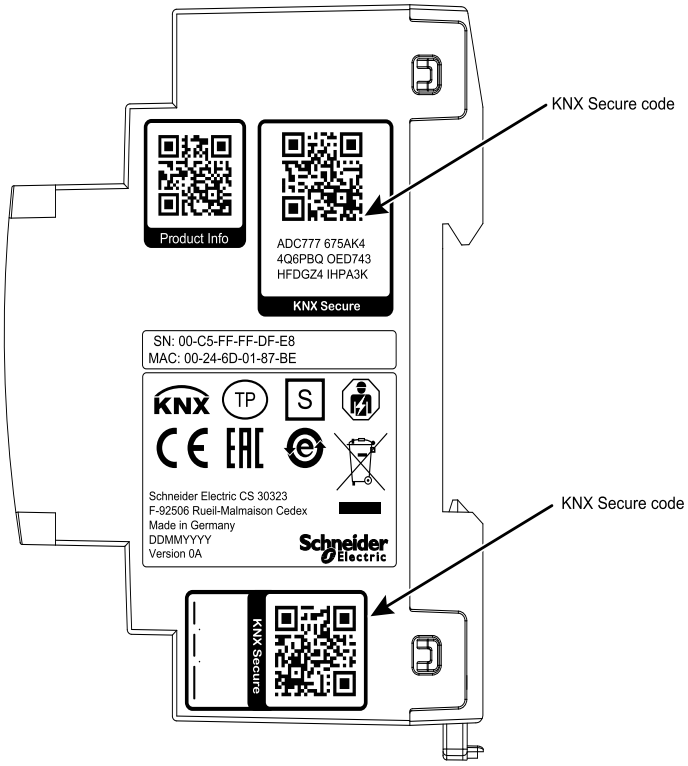
This password protects the ETS project from unauthorized access. This password is not a key that is used for KNX communication. The entry of the password can be bypassed with **Cancel**, but this is not recommended for security reasons.

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 camera connected to the PC that runs the ETS.

The KNX Secure code can be found on the right side of the device. The small KNX Secure code sticker with labeling field at the bottom of the device can be removed for documentation purpose.



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

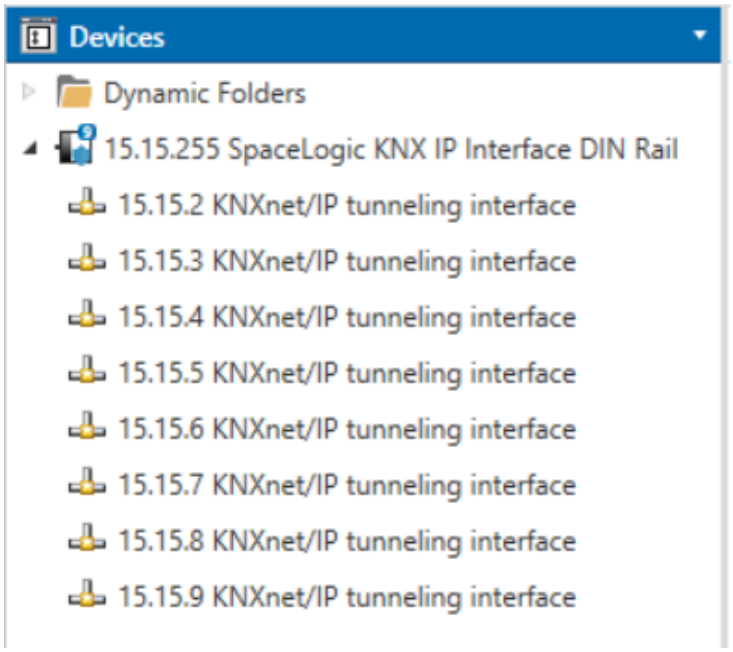
This initial key is required to safely put a device into operation from the start. Even if the ETS download is recorded by a third party, the third party has no access to

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.

Additional parameters

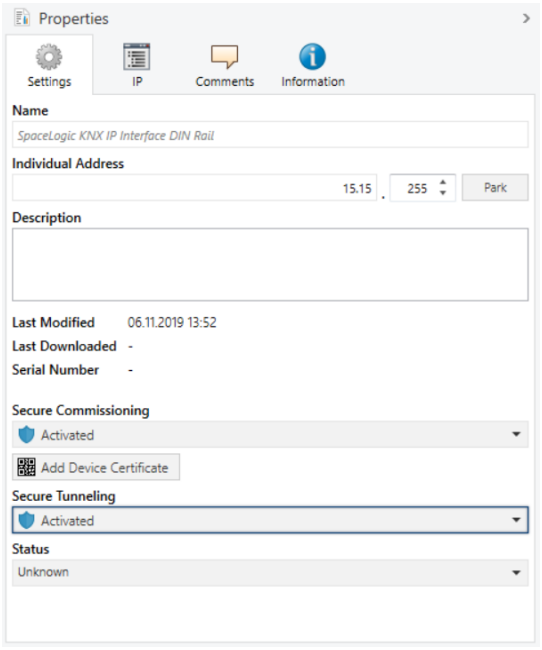
In the ETS, some settings are displayed in addition to the parameter dialog in the properties dialog (at the edge of the screen). The IP settings can be made here. The additional addresses for the interface connections are displayed in the topology view.



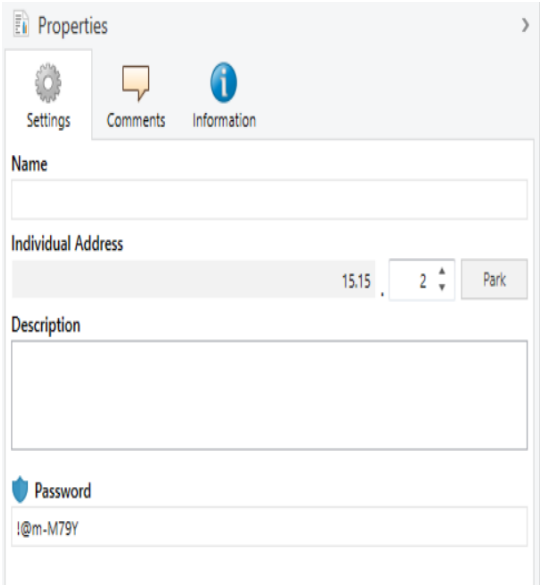
Each individual KNX address can be changed by clicking on the list entry and typing in the desired address into the **Individual Address** text-field. If the text-field frame switches to color red after entering the address, the address is already taken within your ETS project.

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

By clicking on the KNX IP Interface 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.



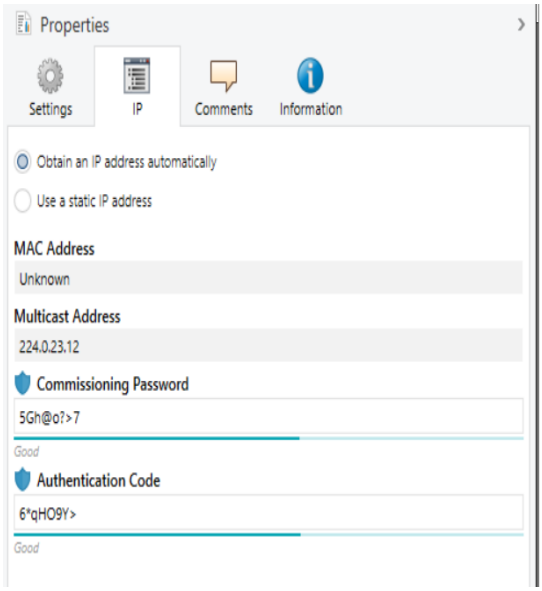
If secure tunneling is activated, a unique password will be created automatically for each tunnel. These passwords can be displayed under the **Settings** overview, when a tunnel is selected.



Within the **IP** overview, the IP network specific options of the KNX IP Interface 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.



IP address

Here the IP address of the KNX IP Interface 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.

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.

Default gateway

Enter the IP address of the gateway here, for example, the DSL router of the installation.

Example of assigning IP addresses

A PC is to be used to access the KNX IP Interface.

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

The KNX IP Interface 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 Interface 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 Interface	**192.168.1.31**
Subnet of the KNX IP Interface	**255.255.255.0**

Remote access

Remote access via Internet is possible with the KNX IP Interface.

NOTICE

MATERIAL DAMAGE THROUGH UNAUTHORIZED ACCESS TO THE KNX INSTALLATION

As soon as you access the KNX installation via the Internet, the data traffic can be read by third parties.

- Only use a VPN access for this connection with a secure encryption for all data packages.
- The required hardware (VPN router) and the features offered by mobile service providers differ significantly with regard to the settings and technical possibilities depending on the country or region.
- Always have the VPN access set up and commissioned by a specialist VPN service provider. The VPN service provider selects a suitable mobile service provider and suitable hardware for the VPN access and ensures that the VPN is set up by a qualified specialist.

Schneider Electric cannot be held responsible for performance problems and incompatibilities caused by applications, services or devices from third-party providers. Schneider Electric offers no technical support when setting up a VPN access.

Failure to follow these instructions can result in equipment damage.

VPN access

The VPN access (VPN = Virtual Private Network) authorises the portable device to access the local network, and therefore also the KNX installation, via the Internet.

Benefits of VPN:

- Only authorised users have access to the local network.
- All data is encrypted.
- The data is not changed, recorded or diverted during the transfer. This is often referred to as a VPN tunnel.

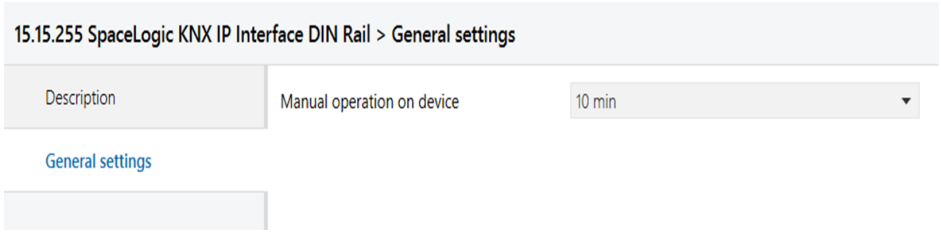
Requirements for setting up a VPN connection:

- Internet connection.
- The portable device and the router are enabled for a VPN connection (VPN client installed).

ETS parameter dialogue

The following parameters can be set using the ETS.

General settings



Manual operation on device

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

Programming

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

Via KNX Bus

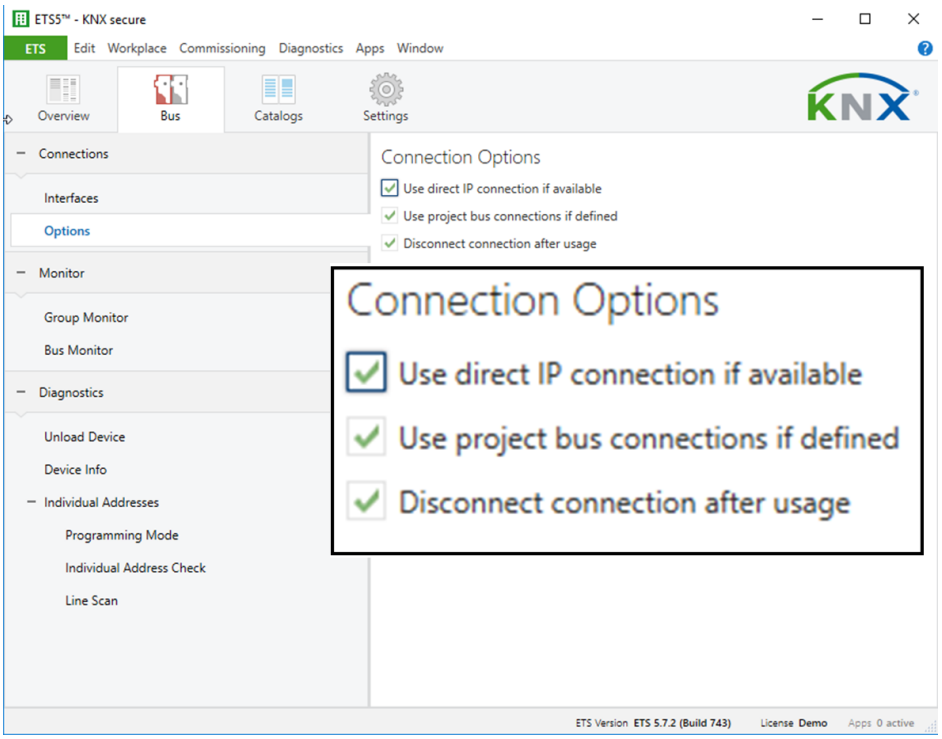
The device only needs to be connected to the KNX bus. The ETS requires an additional interface (for example, USB) to have access to the bus. Via this way both the individual address and the entire application including IP configuration can be programmed. Programming via the bus is recommended if no IP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

Open Source Software used in the product

The product contains, among other things, Open Source Software files, as specified below, developed by third parties and licensed under an Open Source Software license. These Open Source Software files are protected by copyright. Your right to use the Open Source Software is governed by the relevant applicable Open Source Software license conditions.

Your compliance with those license conditions will entitle you to use the Open Source Software as foreseen in the relevant license. In the event of conflicts between other Schneider Electric license conditions applicable to the product and the Open Source Software license conditions, the Open Source Software conditions shall prevail. The Open Source Software is provided royalty-free (i.e. no fees are charged for exercising the licensed rights). The list of Open Source Software contained in this product and the respective applicable Open Source Software terms and conditions are listed hereunder:

List of Open Source Software Files	Applicable Licenses
curve25519–donna	See *https://github.com/agl/curve25519-donna*

If Open Source Software contained in this product is licensed under GNU General Public License (GPL), GNU Lesser General Public License (LGPL), Mozilla Public License (MPL) or any other Open Source Software license, which requires that source code is to be made available, you can download the corresponding source code of the Open Source Software from the following link:

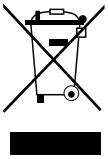
List of Open Source Software Files	Access to Open Source Software files
curve25519–donna	See *https://github.com/agl/curve25519-donna*

Warranty regarding further use of the Open Source Software

Schneider Electric SE and all of its subsidiaries (“Schneider Electric Group”) provide no warranty for the Open Source Software contained in this product, if such Open Source Software is used in any manner other than intended by Schneider Electric Group. The licenses listed above define the warranty, if any, from the authors or licensors of the Open Source Software. Schneider Electric Group specifically disclaims any warranty for defects caused by altering any Open Source Software or the product's configuration. Any warranty claims against Schneider Electric Group in the event that the Open Source Software contained in this product infringes the intellectual property rights of a third party are excluded.

Technical support, if any, will only be provided for unmodified software.

WEEE directive



Dispose of the device separately from household waste at an official collection point.

Professional recycling protects people and the environment against potential negative effects.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

If you have any technical questions, please contact the Customer Care Centre in your country.
www.schneider-electric.com/contact

www.schneider-electric.com

As standards, specifications, and design change from time to time, please ask for confirmation of the information given in this publication.

MTN6502-0105_SW_EN