User Manual

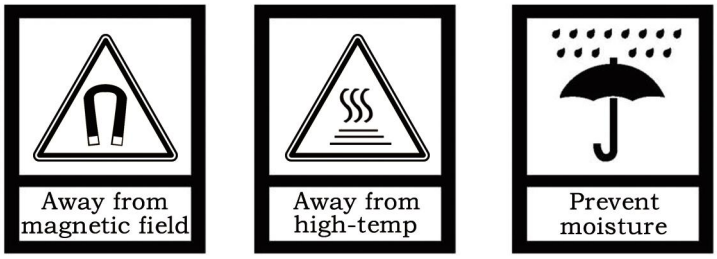
K-BUS IP Interface with Secure_V1.5

BNIP-00/00.S

KNX/EIB Home and Building Control System

Attentions

1. **Please keep devices away from strong magnetic field, high temperature, wet environment;**



2. **Please do not fall the device to the ground or make them get hard impact;**

3. **Please do not use wet cloth or volatile reagent to wipe the device;**

4. **Please do not disassemble the devices.**

Contents

Chapter 1 Summary

The IP Interface with Secure is designed for an intelligent building control system, which is used for facilitating communication between the Ethernet network and the KNX system. KNX telegram can be sent to or received from other devices via the network.

The device supports the KNX Secure protocol (KNXnet/IP Security).

The device serves as an interface between KNX installations and IP networks, and can configure, parameterize and commission the KNX installation as well as group monitoring via the LAN using the ETS software.

The bus connection is carried out via using KNX bus connection terminals.

The device adopts an Ethernet RJ45 interface to connect with LAN network. The network interface can be operated with a transmission speed of 10/100Mbit/s Auto Sensing.

The IP address of the device can be fixed or can be received from a DHCP server. If you need to remain the IP address static or here no DHCP server on the network, you can assign a fixed IP address to the device via ETS.

It can support the UDP/TCP telegram and the port number 3671，and support up to 5 KNX IP client connections，please refer to chapter 4.2. Supports extended frames telegrams, with an APDU length of 55 bytes

It is able to use the Engineering Tool Software ETS (ETS5 or later) with a .knxprod file to allocate the physical address and set the parameter.

It is a modular installation device. It can be installed in the distribution board on 35mm mounting rails according to EN 60 715.

This manual provides detail technical information on the function as well as assembly and programming of the device for users, and explains how to use the interface device by the application examples.

Note: The device can not be programmed via a broadcast connection (Realtek PCIe GBE Family Controller).

The device also does not support bus monitoring.

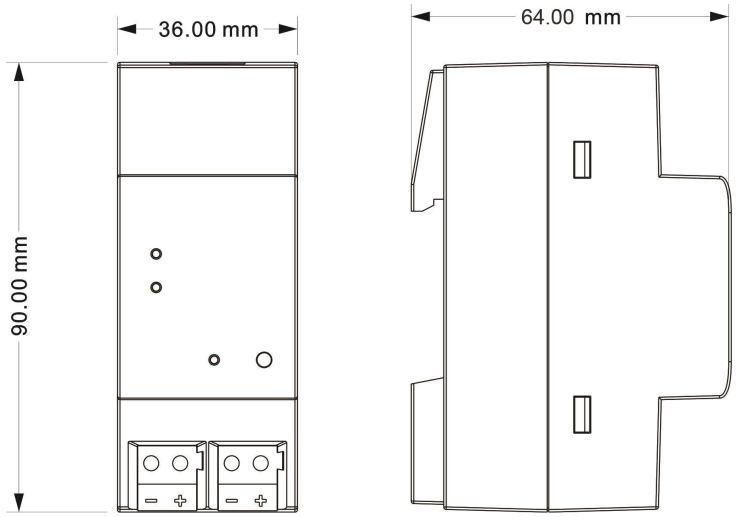
Chapter 2 Technical Data

Power supply	Operation voltage	21-30V DC, via the KNX bus
	Current consumption	<19.5mA, 24V; <15.5mA, 30V
	Power consumption	<470mW
Connections	KNX	Via bus connection terminal (red/black)
	LAN	RJ45 socket for10/100Base-T, IEEE 802.3 network, Auto Sensing
Operating and display	Programming LED and button	For assignment of the physical address
	LAN LED ON	Network connection indicator
	LAN LED flashing	Telegram traffic between the device and network
	KNX LED ON	KNX bus connection indicator
	KNX LED flashing	Telegram traffic between the device and KNX bus
Temperature	Operation	–5 °C ... + 45 °C
	Storage	–25 °C ... + 55 °C
	Transport	– 25 °C ... + 70 °C
Ambient	Humidity	<93%, except condensation
Design	Modular installation device, on 35mm mounting rail	
Dimensions	36 mm×90 mm×64mm	
Weight	0.1KG	
Housing, colour	Plastic housing, Beige	

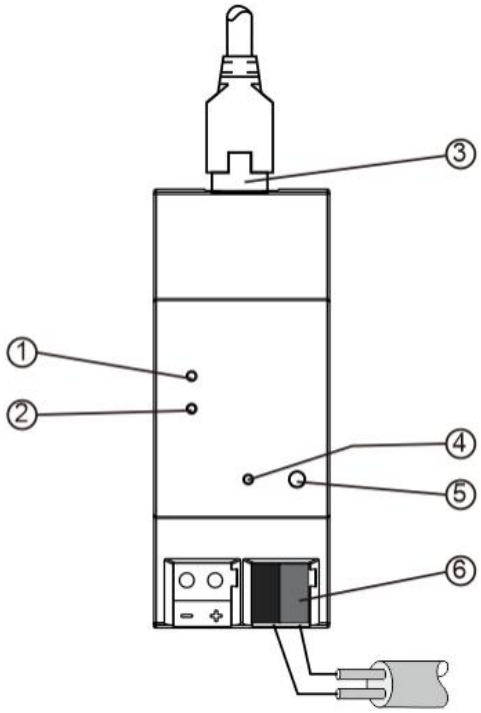
Application program	Max. number of communication objects	Max. number of group address	Max. number of associations
IP Interface with Secure	0	0	0

Chapter 3 Dimension and Connection Diagram

3.1. Dimension diagram



3.2. Connection diagram



①LAN LED ON, indicate that network connect normally
LAN LED flashing, indicate that telegram traffic between device and network

②KNX LED ON, indicate that KNX bus connect normally
KNX LED flashing, indicate that telegram traffic between KNX bus and device

③LAN connection

④Programming LED, red LED ON for assignment of physical address

⑤Programming button, to enter or exit the physical address programming mode

Reset the device to the factory configuration: press the programming button and hold for 4 seconds then release, repeat the operation for 4 times, and the interval between each operation is less than 3 seconds

⑥KNX bus connection terminal

Chapter 4 Parameter setting description in the ETS

4.1. Parameter window “General”

Parameter window “General” is shown in fig. 4.1.1. The device information,including company name, project name,DNS server can be set here.

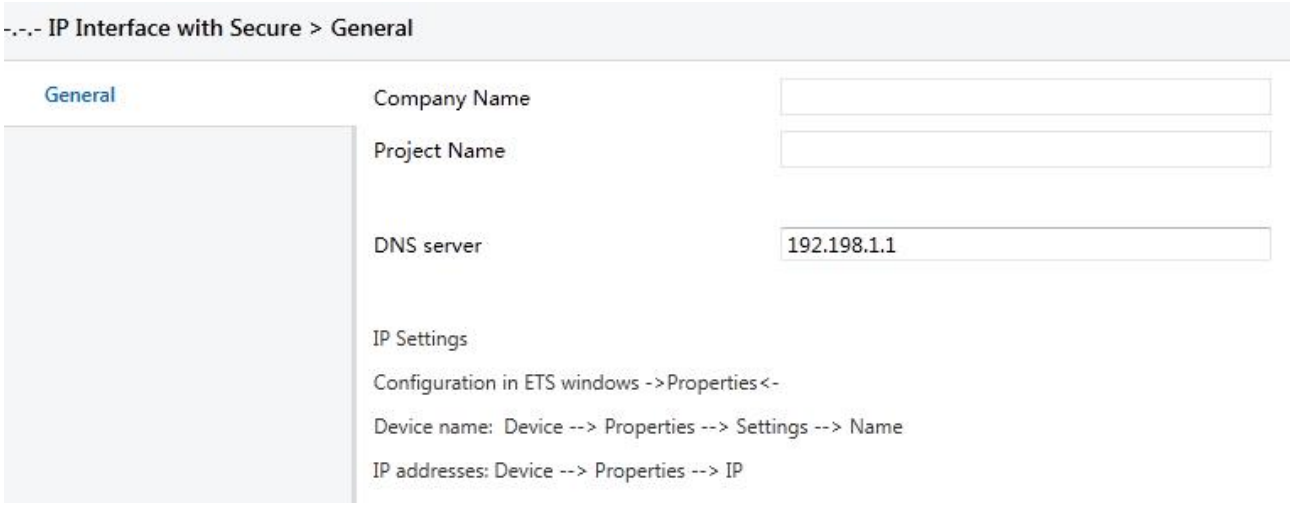


Fig 4.1.1 “General” parameter window

Parameter "Company Name (30 char.)"

This parameter is used to set the company name the device belongs to. Maximum 30 characters can be input.

Parameter "Project Name (30 char.)"

This parameter is used to set the project name the device belongs to. Maximum 30 characters can be input.

Parameter "DNS server"

This parameter is used to set the DNS server address.

Parameter "IP settings..."

Configuration in ETS windows-->Properties

Configure the IP parameters of the IP device in the properties window of ETS.

Device name: Device-->Properties-->Settings-->Name

The device name can be entered in the Settings Properties window. The device name loaded into the device can be changed in the Name field, as shown in Figure 4.1.2 below.

The device name is used for identification of the device on the LAN. For example, the installation location can be identified by the names assigned to the devices, e.g. IP interface, hall, etc

Note: Only the first 30 characters of the device name are loaded into the device; the rest is truncated.

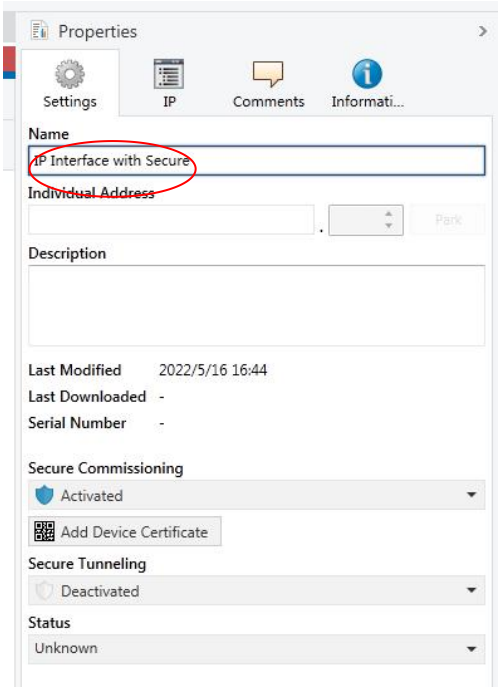


Fig. 4.1.2 Settings

IP addresses: Device-->Properties-->IP

The IP address can be defined in the IP Properties window, as shown in Figure 4.1.3 below.

The following options are available for setting the IP address:

Options:

Obtain an IP address automatically

Use a static IP address

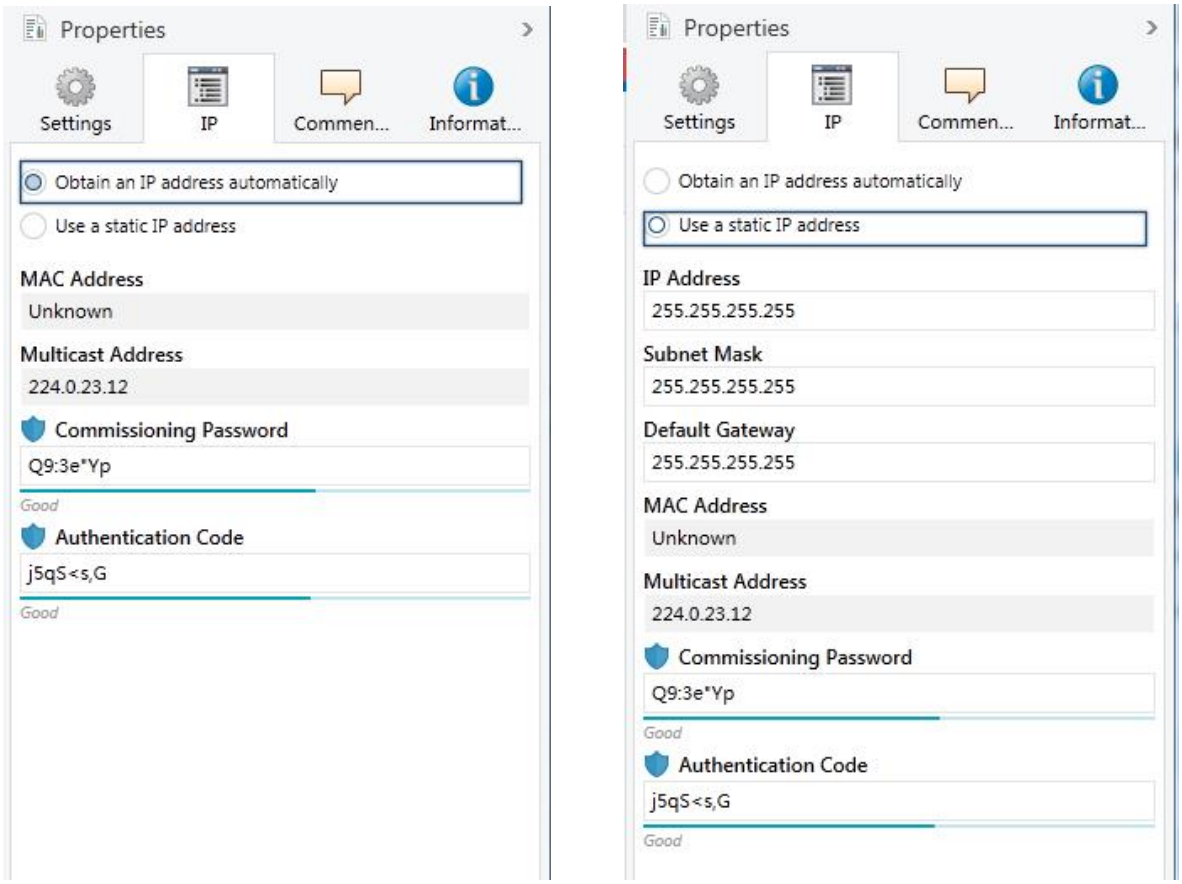


Fig. 4.1.3 IP

Obtain an IP address automatically：In the default setting the IP Interface with Secure expects the assignment of an IP address by a DHCP (dynamic host configuration protocol) server. This server responds to a request by assigning a free IP address to the device. If a DHCP server is not available in the network, the device will be inaccessible.

Use a static IP address：If no DHCP server is installed on the network or if the IP address should remain the same, it can be assigned as static. When assigning static IP addresses, ensure that each device receives a different IP address, and also configure the matching subnet mask and default gateway.

The MAC address is read from the device after a download

The multicast address is only displayed here, 224.0.23.12, it can not be changed.

The commissioning password and the authentication code are only visible when KNX Secure is activated, and are required for IP tunneling connections.

4.2. Use of the integrated tunneling servers

The IP Interface with Secure offers 5 additional physical addresses, which can be used for a tunneling connection, shown in fig. 4.2.1. These so-called tunneling servers can be used with the ETS as a programming interface or with another visual display client, with smartphone, with tablet, with bus tool etc.

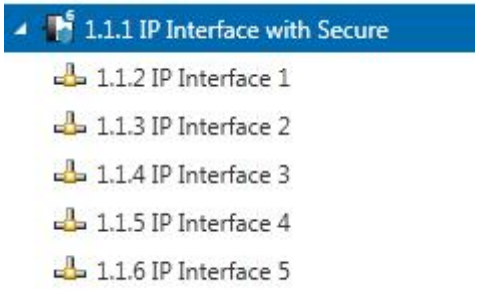


Fig.4.2.1 Tunneling

The physical address of each tunneling connection can be changed in the setting property window, and their physical addresses must fit the topology.

In ETS, the first five free addresses in the line are assigned automatically after the device has been inserted into a line. This is a property of the ETS and cannot be changed.

The addresses will be available in the device after the first download.

If this is not desired, the setting can be changed manually in the Properties window via activated the Park, shown in fig. 4.2.2. This tunnel will receive the address 15.15.255 after download. If the option Park is selected for all tunneling servers, all tunneling servers will be assigned the address 15.15.255. (15.15.255 is the default address for devices with no physical address assigned)

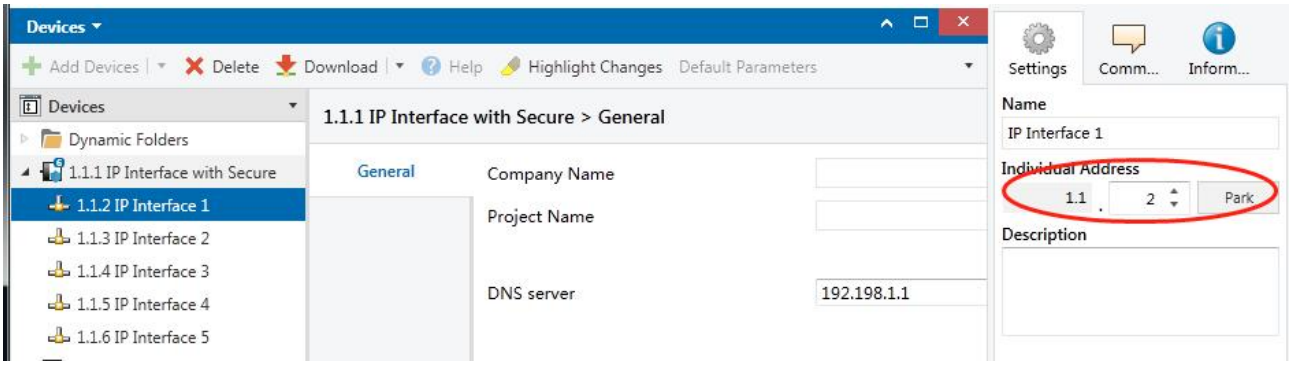


Fig.4.2.2 Setting - Park

In addition, the tunneling servers can also be encrypted with KNX Secure. First activate Secure Commissioning, and then activate Secure Tunneling, as shown in Figure 4.2.3. After activating Secure Tunneling, the password for each Tunneling connection can be set in ETS, as shown in Figure 4.2.4, and users can change this password as needed.

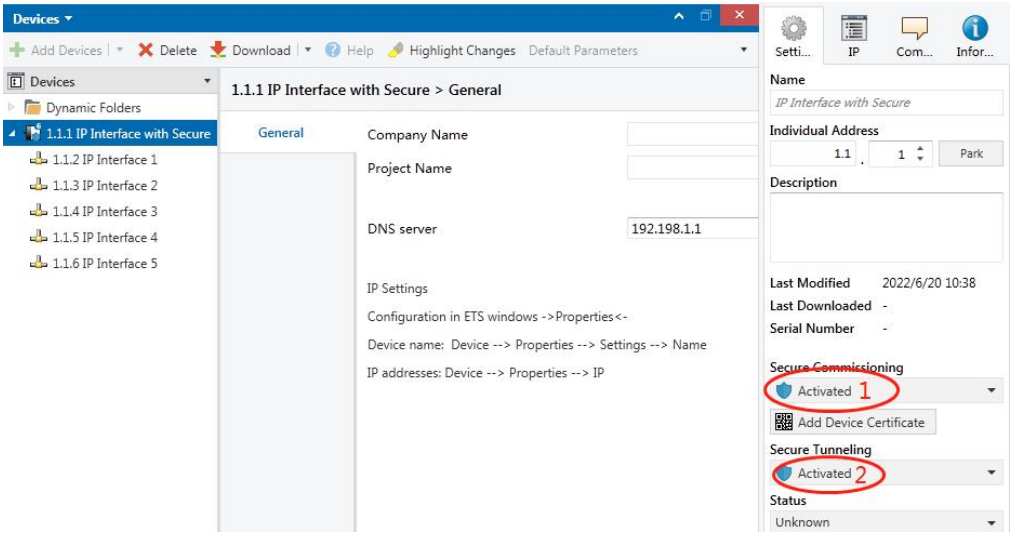


Fig.4.2.3 Setting - Secure activated

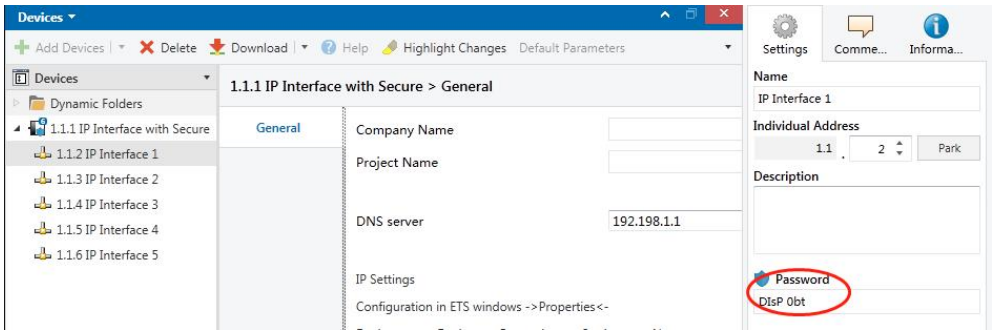


Fig.4.2.4 Setting - tunneling password

If a project password is not assigned to the project, ETS will prompt to assign a project password when activate Secure Commissioning , as shown in Figure 4.2.5 below. In other words, you must set a project password for the project, otherwise the Secure Commissioning cannot be activated.

Fig.4.2.5 Set project password

4.3. KNX Secure

The IP Interface with Secure is a KNX device according to the KNX Secure standard. In other words, the device can run in secure mode, and the tunneling connection are encrypted.

Therefore, the following information must be taken into account during device commissioning:

❖ It is essential to assign a project password as soon as a KNX Secure device is imported into a project. This will protect the project against unauthorized access.

The password must be kept in a safe place – access to the project is not possible without it (not even the KNX Association or device manufacturer will be able to access it)!

Without the project password, the commissioning key will not be able to be imported.

❖ A commissioning key is required when commissioning a KNX Secure device (first download). This key (FDSK = Factory Default Setup Key) is included on a sticker on the side of the device, and it must be imported into the ETS prior to the first download.

✧ On the first download of the device, a window pops up in the ETS to prompt the user to enter the key, as shown in Figure 4.3.1 below. The certificate can also be read from the device using a QR scanner (recommended).

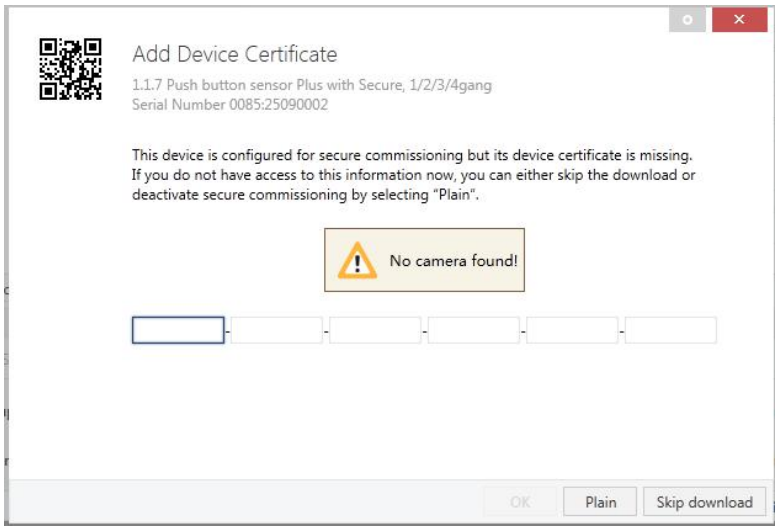


Fig.4.3.1 Add Device Certificate window

✧ Alternatively, the certificates of all Secure devices can be entered in the ETS beforehand. This is done on the "Security" tab on the project overview page, as shown in Figure 4.3.2 below.

The certificates can be also added to the selected device in the project, as shown in Figure 4.3.3.

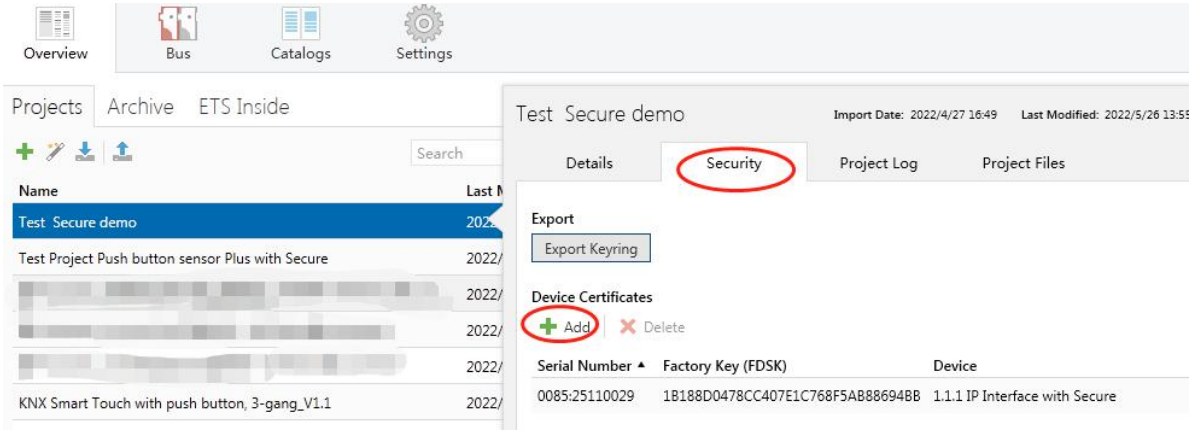


Fig. 4.3.2 Add Device Certificate in overview

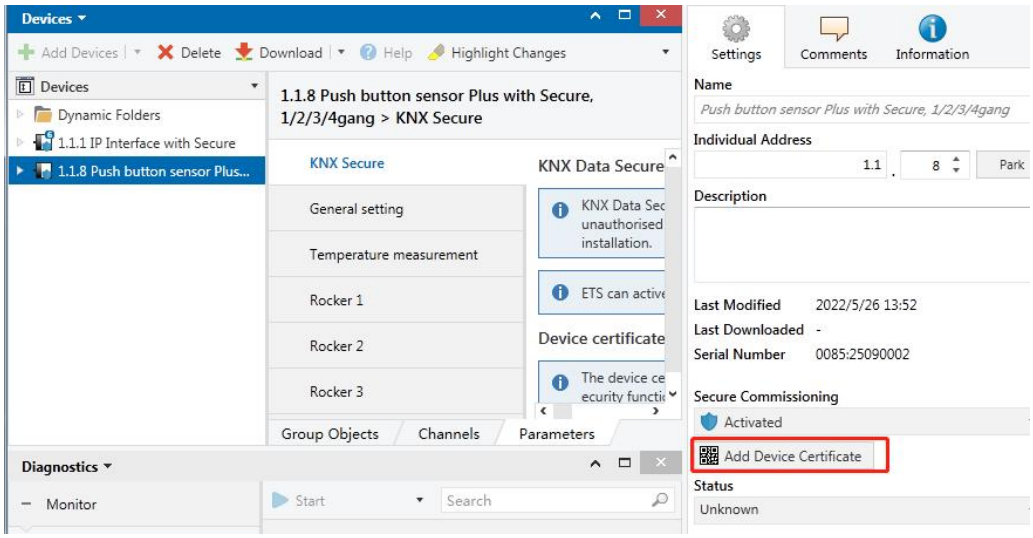


Fig. 4.3.3 Add Device Certificate in project

✧ Two FDSK stickers are applied on the device. One of them can be used for the project documentation, and the other one can remain on the device.

Without the FDSK, it will no longer be possible to operate the device in KNX Secure mode after a reset.

The FDSK is required only for initial commissioning. After entering the initial FDSK, the ETS will assign a new key, as shown in Figure 4.3.4 below.

The FDSK will be required again only if the device was reset to its factory settings (e.g. If the device is to be used in a different ETS project).

Fig. 4.3.4 Adding Device Certificate window

Example:

If this application in the project needs to be tried with another device, it is no longer the original device. When the application is downloaded to a new device, the following prompt will appear on the left of figure 4.3.5, click yes, the Add Device Certificate window will appear, then enter the initial FDSK of the new device, and you need to reset the device to the factory settings (it is not required if the device is still factory default; If it has been used, it will be required to reset, otherwise the following error message will appear on the right of figure 4.3.5), and then the device can be successfully downloaded again.

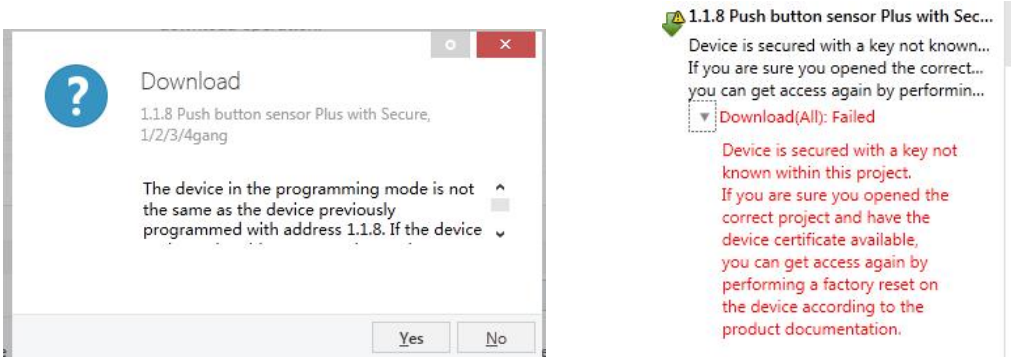


Fig. 4.3.5 Example

Whether the device is replaced in the same project, or the device is replaced in a different project, the processing is similar: **Reset the device to the factory settings, then reassign the FDSK.**

After the device is downloaded successfully, the label Add Device Certificate turns gray, indicating that the key for this device has been assigned successfully, as shown in Figure 4.3.6 below.

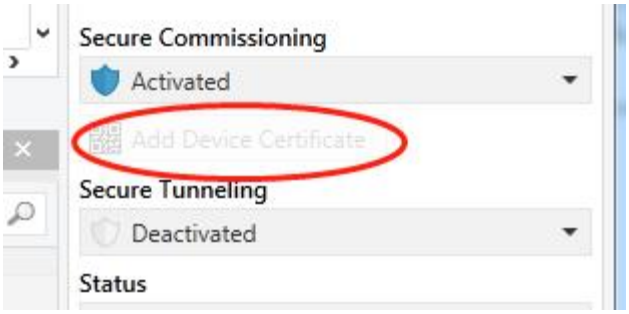


Fig. 4.3.6

ETS generates and manages keys:

Keys and passwords can be exported as needed to the use of security keys outside of the associated ETS projects, e.g. if a client would like to access one of the tunnels. As shown in Figure 4.3.7 below, the file extension is .knxkeys.

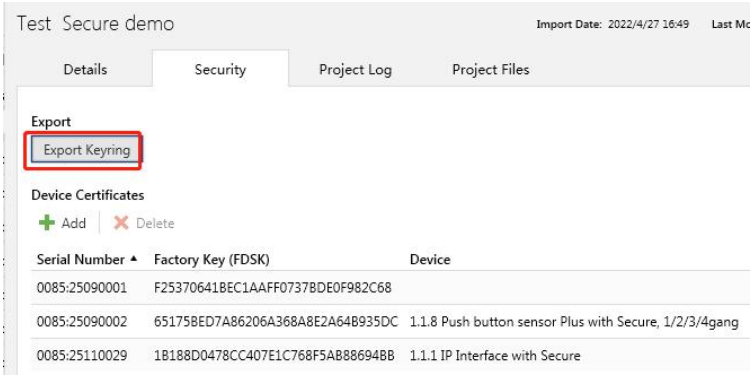


Fig. 4.3.7

ETS with IP connection example:

The whole process is shown in Figure 4.3.8 below. Select the IP Interface device, select one of the Tunneling (such as physical address 1.1.2), click “Test”, the commissioning password and authentication code input window will pop up (the password and authentication code can be viewed in the device property window in the project), enter the password and authentication code. After click “OK”, the word Ok will appear next to the “Test” button, and then click “Select” to connect.

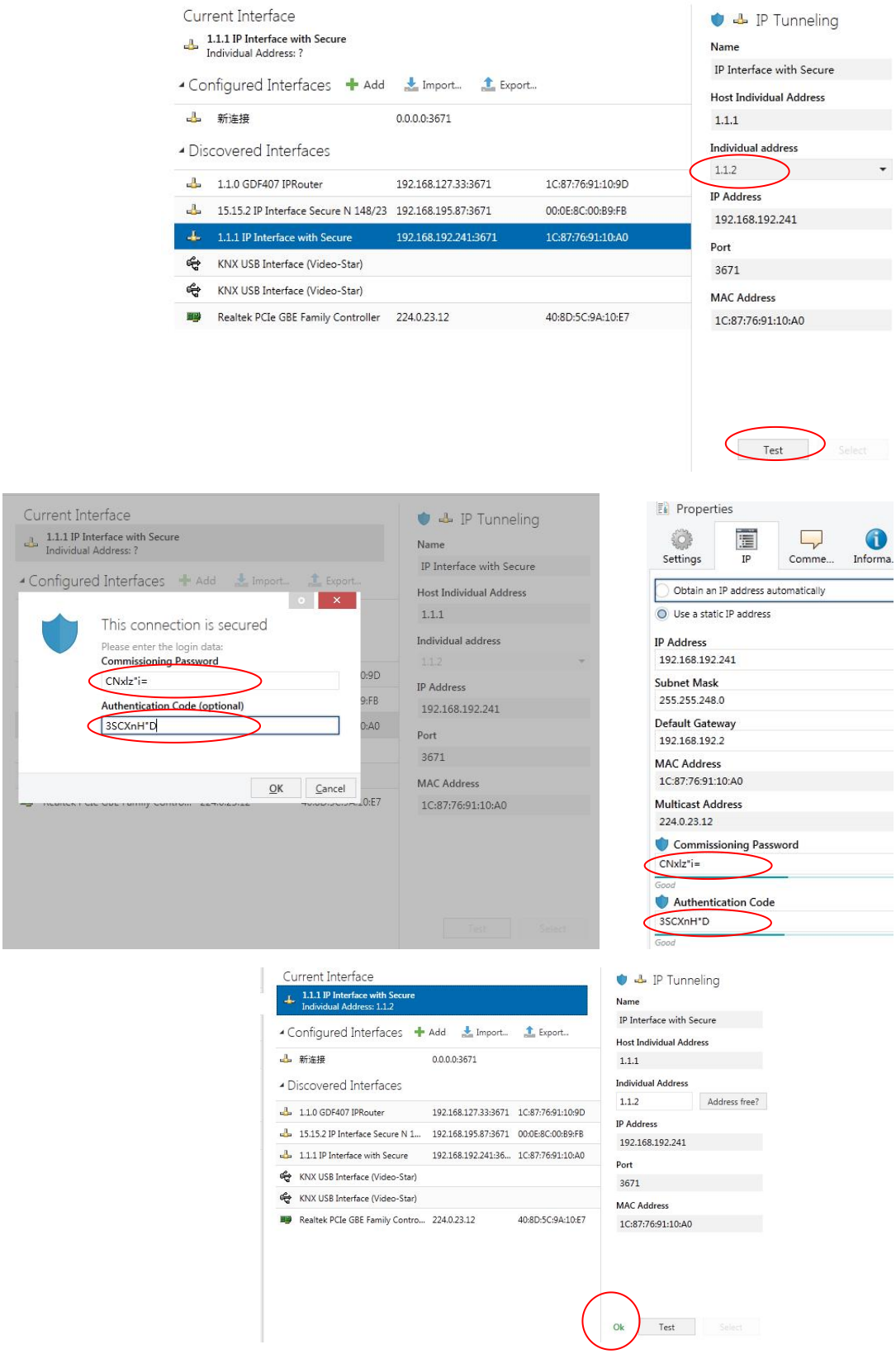


Fig. 4.3.8 IP tunneling connection

In Figure 4.3.8, if Secure Tunneling is not activated, , the commissioning password and authentication code are not required when the device is connected as an interface; if Secure Tunneling is activated, ETS will prompt you to enter the commissioning password and authentication code when connecting.

The IP Interface can be reset to its factory settings if necessary, see chapter 5, Factory setting

Note: Any USB interface used for programming a KNX Secure device must support “long frames”. Otherwise ETS will report a download failure information, as shown below.

Fig. 4.3.9

4.4. Unloading the device

The device can be reset to the factory settings. This is a secure device, so the following information must be observed:

When the device is operated in KNX Secure mode, it can be reset via the ETS only if the ETS uses the project with which the device was parameterized or if the commissioning key is available in the project.

The device can be unloaded by right-clicking it in the ETS.

Unloading the application:

- The IP address and IP configuration will be retained
- The passwords of the tunneling servers will be deleted. There will not be required to enter the commissioning password and authentication code when connecting (if there is the pop-up window,it is empty)
- The key assigned by the ETS will be retained. In other words, the FDSK will not be needed for reprogramming
- The physical address will be retained

Unloading the physical address and the application

- The device will be reset to the factory state
- The FDSK will be required for re-commissioning unless it is still available in the ETS project from the original commissioning process

4.5. Read device information

Reading device information can only be done in the project of the device, via select the device-->right-click-->info-->device info, as shown fig.4.5 below.

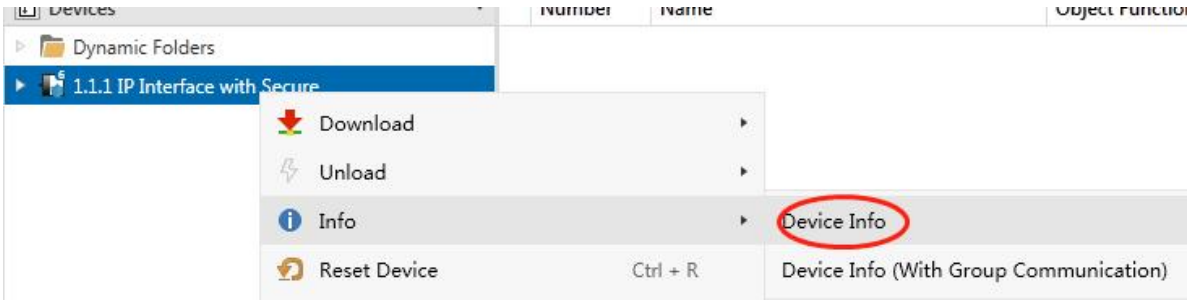


Fig. 4.5 Read device information

Chapter 5 Factory setting

The IP Interface is delivered with the following default factory settings:

Physical address	15.15.254
Tunneling Addresses	15.15.241 15.15.242 15.15.243 15.15.244 15.15.245
IP configuration	
IP address	192.168.2.200
Subnet mask	255.255.255.0
Default gateway	192.168.2.1

The reset to factory settings can also be performed directly on the device. The specific operation as follows:

Press the programming button and hold for 4 seconds then release, repeat the operation for 4 times, and the interval between each operation is less than 3 seconds, after that, the LAN, KNX and programming LED indicators are all off, and then the LAN and KNX return to normal instructions, and the device enters the restart, and after the restart is completed, it can be restored to the factory settings.

For more information about the FDSK (Factory Default Setup Key). See chapter 4.3, KNX Secure.

Chapter 6 Web Configuration

Web configuration is typically used to modify IP addresses and device names, and upgrade devices. **Note: If KNX security is enabled, network configuration cannot be modified via the web configuration.**

Enter the IP address of the device in the web browser to enter the web configuration interface of the IP Interface, as shown in Fig.6.1 below.

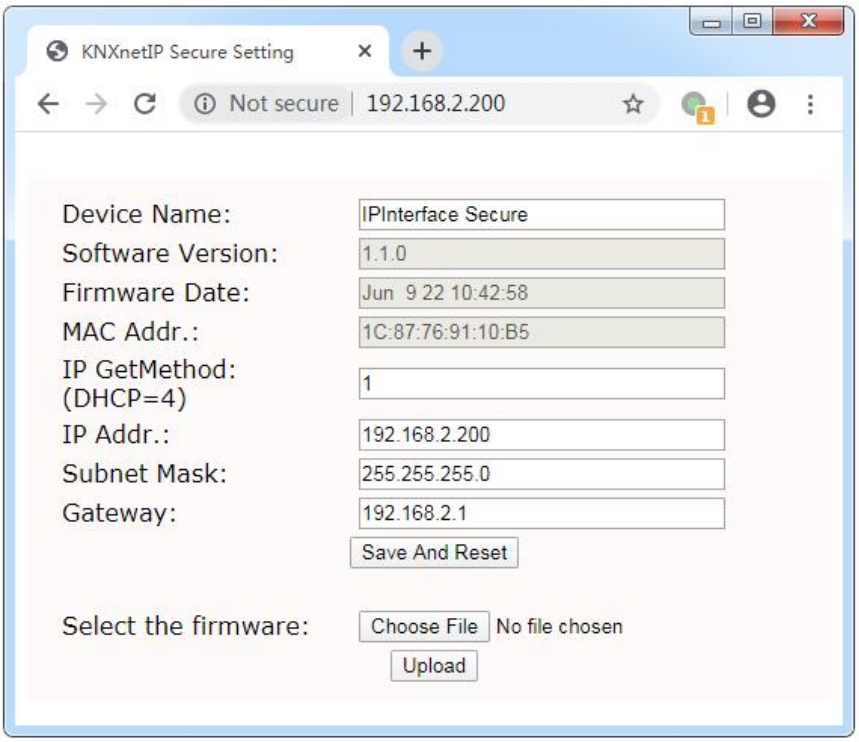


Fig.6.1 IP Interface web configuration window

① **Device Name:** Display or set the device name.

② **Software Version:** Display the firmware (software) version.

③ **Firmware Date:** Display the date of the device firmware.

④ **MAC Addr.:** Display the MAC address.

⑤ **IP GetMethod:** The method to get IP address. When the value is set to 1, it represents the fixed IP address. The custom IP address, subnet mask and default gateway can be entered below. When the value is set to 4, IP address is automatically assigned via the DHCP server.

⑥ **IP Addr.:** Display or set the IP address.

⑦ **Subnet Mask:** Display or set the subnet mask.

⑧ **Gateway:** Display or set the gateway.

Note: When using a fixed IP address setting, please ensure that each device receives a different IP address, and configure an appropriate subnet mask and default gateway, otherwise the web configuration interface cannot be opened even if the IP address is entered.

⑨【**Save And Reset**】**:** Click this button to save and reset after setting changes are completed. At this time, the page will jump to the window as shown in Fig.6.2, indicating that the device is restarting. After restarting, the page will automatically return to the configuration window.

If the IP address is changed, you need to enter the new IP address to enter the configuration interface again.

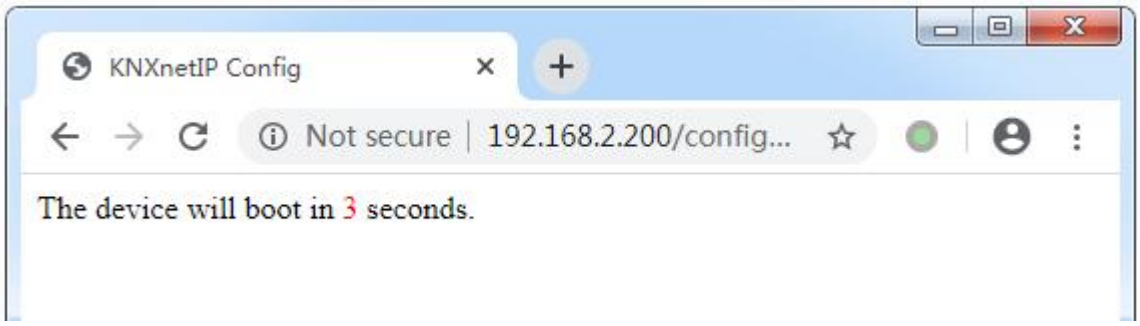


Fig. 6.2

⑩ **Select the firmware:** It is used to upgrade the firmware of the device. Click the button [Choose File] to choose the firmware (.bin) of the updated device, and then click the button [Upload] to update the device. Figure 6.3 shows the firmware upgrade successful .

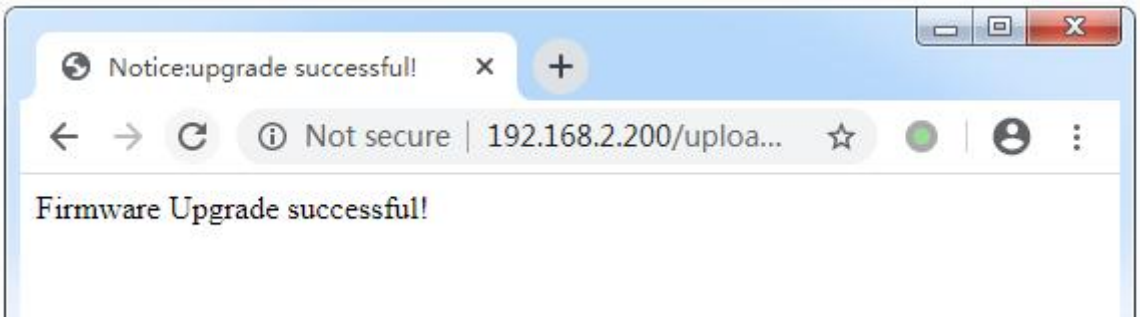


Fig. 6.3

Note: If the user does not know or forget the IP address, reset the IP address of the device to the default address of 192.168.2.200 via restore factory setting (See Chapter 5 for details), and then enter this IP address in the browser to enter the web configuration window of the device and change the IP settings and then save.