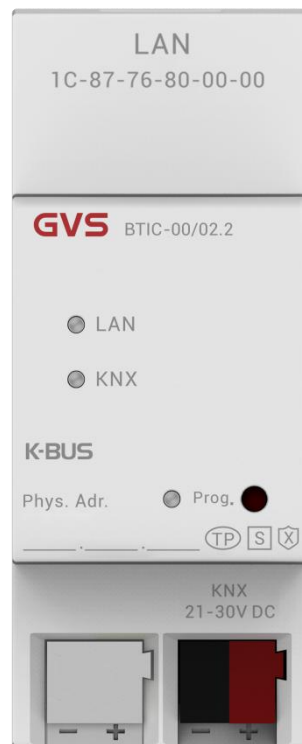


User Manual

K-BUS KNX-BACnet Gateway Server_V1.0

BTIC-00/02.2



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	1
Chapter 2 Technical Data	2
Chapter 3 Dimension and Structural Diagram	3
3.1. Dimension Diagram	3
3.2. Structural Diagram	3
Chapter 4 Project Design and Programming	4
Chapter 5 Parameter setting description in the ETS	5
5.1. Parameter window "General"	5
5.2. Parameter window "Templates"	7
5.3. Parameter window "Object"	8
5.4. Using the Integrated Tunneling Server	12
5.5. KNX Secure	14
5.6. Removing the Device	20
Chapter 6 Description of Communication Object	21
6.1. "Object x" Communication Object	21
Chapter 7 Factory settings	23

Chapter 1 Summary

The KNX-BACnet Gateway Server is mainly used in intelligent control systems. Deployed between the KNX bus and the BACnet/IP network, it enables bidirectional data exchange between the two systems, allowing BACnet central control systems, building automation systems (BAS), and third-party BACnet clients to seamlessly access sensors, actuators, and function modules on the KNX bus, thereby enabling centralized monitoring and cross-system coordination of subsystems such as lighting, HVAC, and security.

This manual provides detailed technical information about KNX-BACnet Gateway Server for users as well as assembly and programming details, and explains how to use the device by the application examples.

KNX-BACnet Gateway Server is powered from KNX bus. It is available to assign the physical address and configure the parameters by engineering design tools ETS with .knxprod (support edition ETS5.7 or higher).

The functions are summarized as follows:

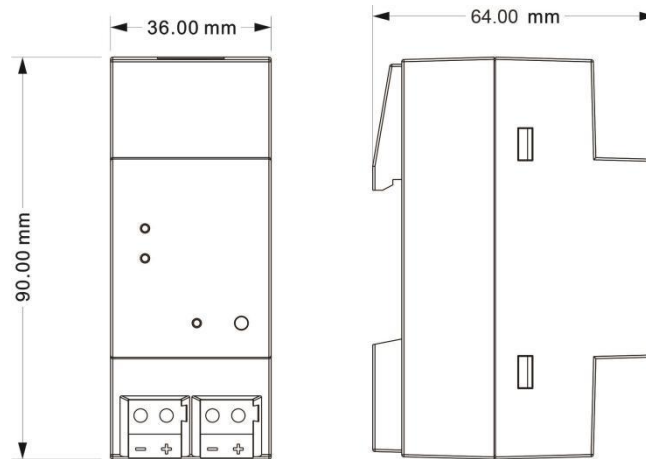
- Supports custom BACnet gateway names, BACnet device instance numbers, and DCC mode access password for BACnet gateway configuration
- Provides 8 selectable templates when the object type is MultiState
- Supports configuration of up to 512 objects. The type, transmission direction, and datatype (1bit/1byte/2byte/4byte) of each object can be configured independently
- Support up to 5 KNXnet/IP connections at the same time
- Support the KNX Data Secure and KNXnet/IP Secure

Chapter 2 Technical Data

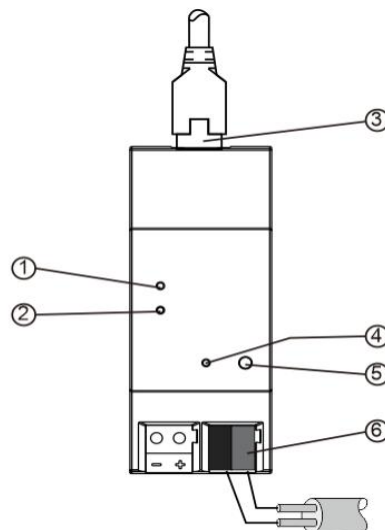
Power supply	Bus voltage	21-30V DC, via KNX bus
	Bus current	19.5mA/24V; 15.5mA/30V
	Bus consumption	470mW
Connections	KNX	Bus connection terminal (red/black)
	LAN	RJ45 socket for 10/100 Base-T
Operation and display	LAN LED	On: That network connect normally Flashing: The telegram traffic between device and network
	KNX LED	On: The KNX bus connect normally Flashing: The telegram traffic between KNX bus and device
	Programming button and LED	For assigning the physical address
Temperature	Operation	– 5 °C ... 45 °C
	Storage	– 25 °C ... 55 °C
	Transportation	– 25 °C ... 70 °C
Ambient	Humidity	<93%, except dewing
Design	Protocol stack	BACnet Stack at SourceForge
	Installation	Standard 35mm DIN rail installation
Dimension/Weight	36 × 90 × 64mm/0.1kg	

Chapter 3 Dimension and Structural Diagram

3.1. Dimension Diagram



3.2. Structural Diagram



① LAN LED

④ Programming LED

② KNX LED

⑤ Programming button

③ LAN connection

⑥ KNX bus connection terminal

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.

Chapter 4 Project Design and Programming

Application	Maximum of communication objects	Maximum number of group addresses	Maximum number of associations	Secure group addresses
KNX-BACnet IP Gateway Server/00F3 1.0	1034	1500	1500	800

Chapter 5 Parameter setting description in the ETS

5.1. Parameter window "General"

Device Name(max. 31 chars)	KNX-BACnet Gateway
Start Delay for read on init	10 s
Delay between read requests	200 ms
Device Instance(Must be unique)	0
Bacnet communication port	47808
KNX read failure max retry times	0
DCC Password *	12345
Device Location(max. 31 chars)	
Device Description(max. 31 chars)	

Fig.5.1 "General" Parameter window

Parameter "Device Name(max. 31 chars)"

This parameter is for setting the device name, up to input 31 characters.

Parameter "Start delay for read on init"

This parameter is for setting the time delay for sending status telegrams after the bus recovery reset. Options:

10s

20s

...

5min

Parameter "Delay between read requests"

This parameter is for setting the interval between read requests for the KNX device status.

Options: **200ms/500ms/1s/2s/5s**

Parameter "Device Instance(Must be unique)"

This parameter is for setting the unique device instance number of the BACnet device, it must not be duplicated within the same LAN. Options: **0...4194303**

Parameter "Bacnet communication port"

This parameter is for setting the BACnet protocol communication port of the gateway.

Options: **0...65535**

Parameter "KNX read failure max retry times"

This parameter is for setting the number of automatic retries after a point read fails.

Options:

0

1

2

3

Parameter "DCC password"

This parameter is for setting the DCC password.

Parameter "Device location(max.31 chars)"

This parameter is for setting the description of device location, up to input 31 characters.

Parameter "Device Description(max.31 chars)"

This parameter is for setting the description of device, up to input 31 characters.

5.2. Parameter window "Templates"



Number of Template	8
Template description	
State description count[value from 1..n]	2
State 1, description	
State 2, description	

Fig.5.2 "Templates" Parameter window

Parameter "Number of Template"

This parameter is for setting the number of template.

Options: **1...8**

Parameter "Template description"

This parameter is for setting the custom description of template, up to input 31 characters.

Parameter "State description count[value from 1..n]"

This parameter is for setting the number of device state descriptions.

Options: **2...16**

Parameter "State x(x=2~16) description"

This parameter is for setting the text description corresponding to each device state, up to input 31 characters.

5.3. Parameter window "Object"

Fig.5.3 "Object" Parameter window

Parameter "Number of object"

This parameter is for setting the number of bidirectional KNX-BACnet mapping points.

Options: **0...512**

Parameter "Object description"

This parameter is for setting the custom description of object, up to input 31 characters.

Parameter "Object type"

This parameter is for setting the object type.

Options:

Analog

Binary

MultiState

---Parameter "object datatype"

This parameter is visible when the previous parameter selects "Analog". Set the object datatype.

Options:

1bit value

1byte percentage value(5.001)

1byte unsigned value

1byte signed value

2byte unsigned value

2byte signed value(8.001)

2byte float value

4byte unsigned value(12.001)

4byte signed value

4byte float value

--Parameter "Datapoint type"

This parameter is visible when the previous parameter selects "1byte unsigned value\1byte signed value\2byte unsigned value\2byte float value\4byte signed value\4byte float value". The value range depends on the data type selected in the previous parameter.

--Parameter "select template"

This parameter is visible when "Multistate" is selected. It is used to select one of the previously created multistate templates.

Options:

Template1

...

Template8

Parameter "Transmission direction"

This parameter is for setting the transmission direction.

Options:

KNX<--BACnet(output)

KNX-->BACnet(input)

KNX<-->BACnet(value)

KNX<--BACnet(output): One-way downstream; only BACnet commands are sent to KNX. Local KNX status is not uploaded back to the upper-level BACnet.

KNX-->BACnet(input): One-way upload; only KNX data is uploaded to BACnet. The upper-level BACnet cannot control KNX in reverse.

KNX<-->BACnet(value): Bidirectional; local KNX status is synchronized to the upper-level, and upper-level BACnet commands can be sent down to control KNX.

Parameters as follow are visible when “KNX-->BACnet(input)” or “KNX<-->BACnet(value)” is selected:

--Parameter “Transmission to BACnet”

This parameter is for setting the trigger condition for reporting point values to the BACnet gateway

Options:

On change

On all events

On change: data is uploaded to the higher-level BACnet gateway only when the point value changes.

On all events: each time KNX receives a corresponding telegram, it is reported to the BACnet gateway immediately in real time.

--Parameter “Enable read on init”

This parameter is for setting whether the KNX point values read automatically during power-on initialization are synchronized to the BACnet gateway.

Options:

No

Yes

--Parameter “Read request cyclically”

This parameter is for setting whether to enable the gateway to cyclically read KNX points.

Options:

No

2min

...

3h

--Parameter "Default value in faulty case[timeout=10s]"

This parameter is visible when "0" is not selected. Set the default interval at which the gateway reads KNX points.

Options:

0[invalue when multstate]

1

Max. Value [float Max. When analog]

Note: in case of not receiving any response the present-value can be defined by a default!



In case of not receiving any response the present-value can be defined by a default!

5.4. Using the Integrated Tunneling Server

The KNX-BACnet Gateway Server provides 5 additional physical addresses, as shown in Fig.5.4, for tunnel connections, such as: programming interface (ETS), or for connecting visualization clients, smartphone apps, tablets, bus tools, etc.



Fig.5.4

The physical address of each tunnel connection can be modified in the settings properties window, and their physical addresses must comply with the topology requirements and be located on the same line. In ETS5, when assigning physical addresses to the device, the first 5 free physical addresses on that line are automatically assigned to the individual tunnel connections.

If you do not want to assign a physical address to a tunnel, activate "Park" (as shown in Fig.5.4.2); after the download, this tunnel will receive address 15.15.255. If all tunnels are "Park", all tunnels will be assigned address 15.15.255. (15.15.255 is the default address of devices without an assigned physical address)

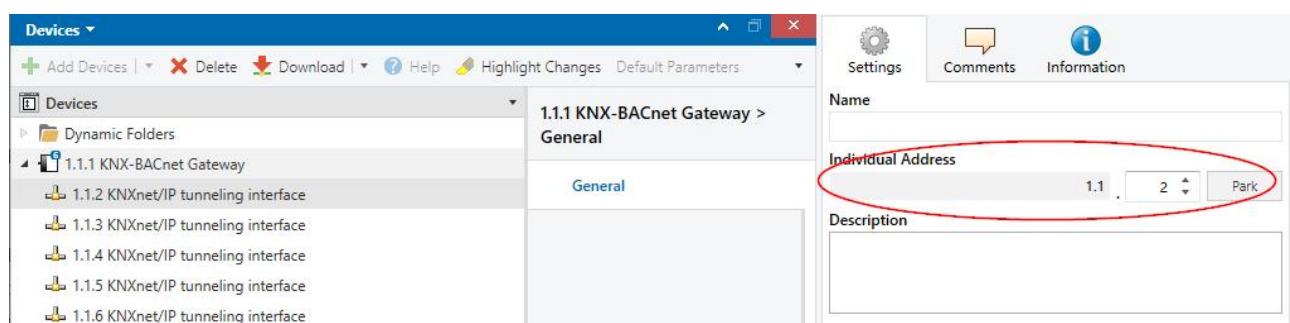


Fig.5.4.2

In addition, tunnel connections can also be encrypted using KNX Security. First activate "Secure Commissioning", then activate "Secure Tunneling", as shown in Fig.5.4.3 After activating "Secure Tunneling", the password of each tunnel connection can be set in ETS, as shown in Fig.5.4.4, users can change this password as required.

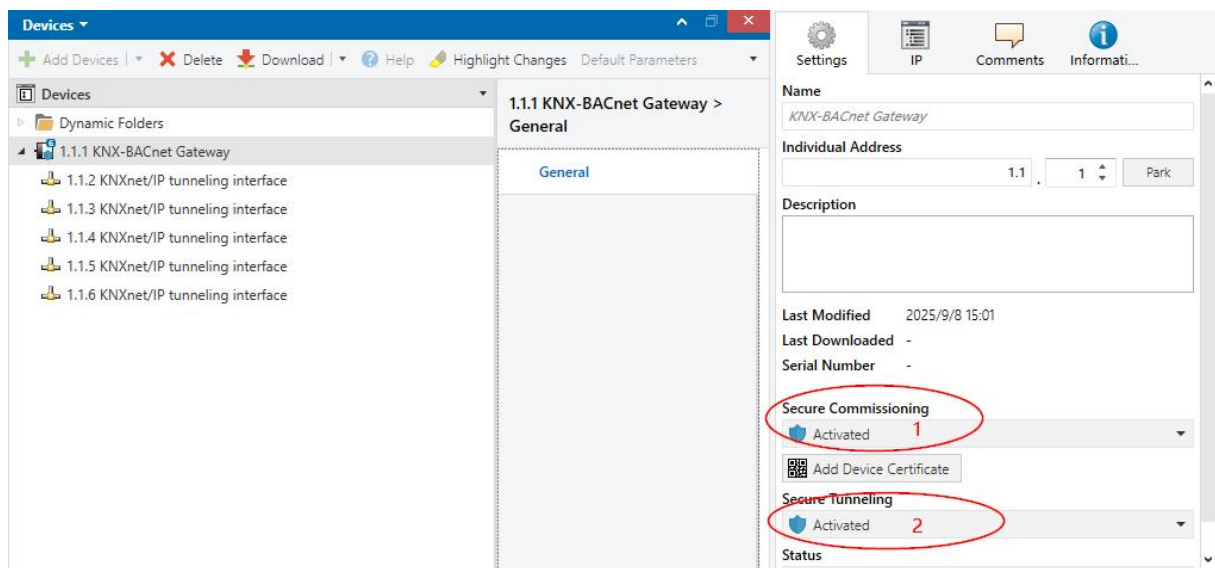


Fig.5.4.3

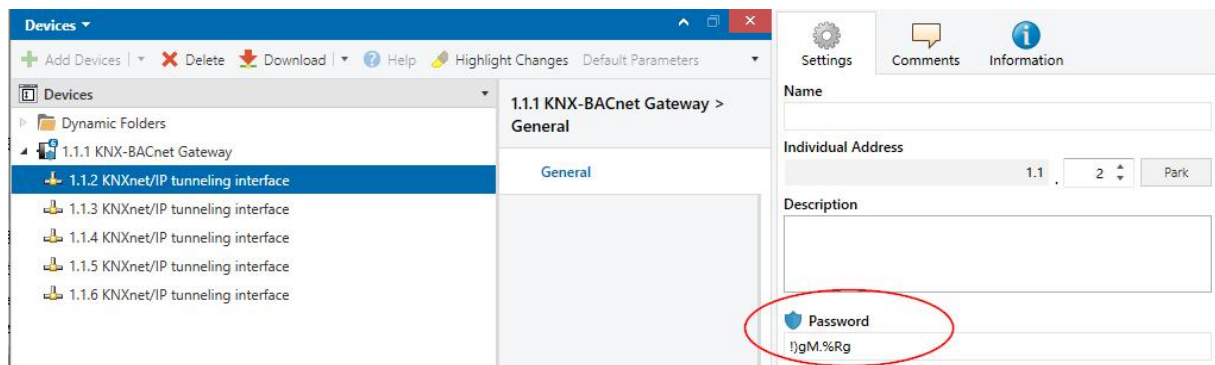


Fig.5.4.4

If the project has no password assigned, manually activating “Secure Commissioning” will prompt you to assign a project password, as shown in Fig.5.4.5 Without a project password, “Secure Commissioning” cannot be activated.

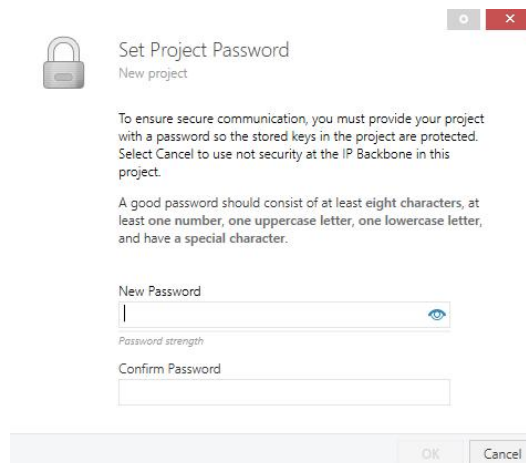


Fig.5.4.5

5.5. KNX Secure

KNX-BACnet Gateway Server is a KNX device that complies with the KNX secure standard. That is, you can run the device in safe way.

If secure commissioning is activated in ETS project, the following information must be considered during device debugging:



❖ 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 Fig.5.5.1 below.

The certificate can also be read from the device using a QR scanner (recommended).

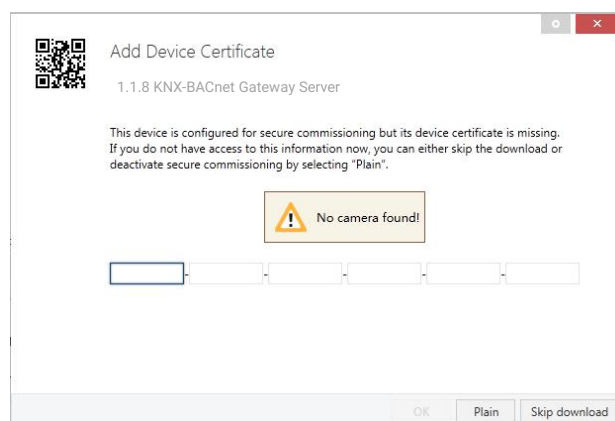


Fig.5.5.1 Add Device Certificate window

✧ 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 Fig.5.5.2 below.

The certificates can be also added to the selected device in the project, as shown in Fig.5.5.3.

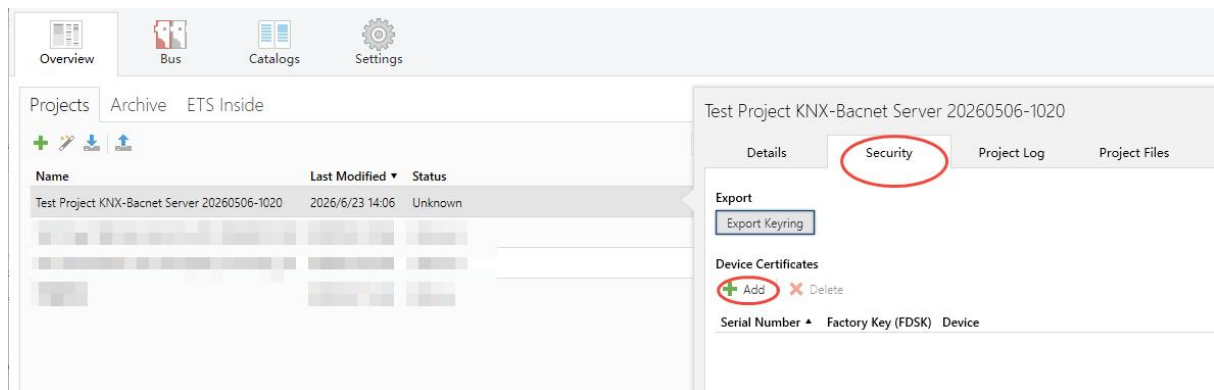


Fig.5.5.2 Add Device Certificate

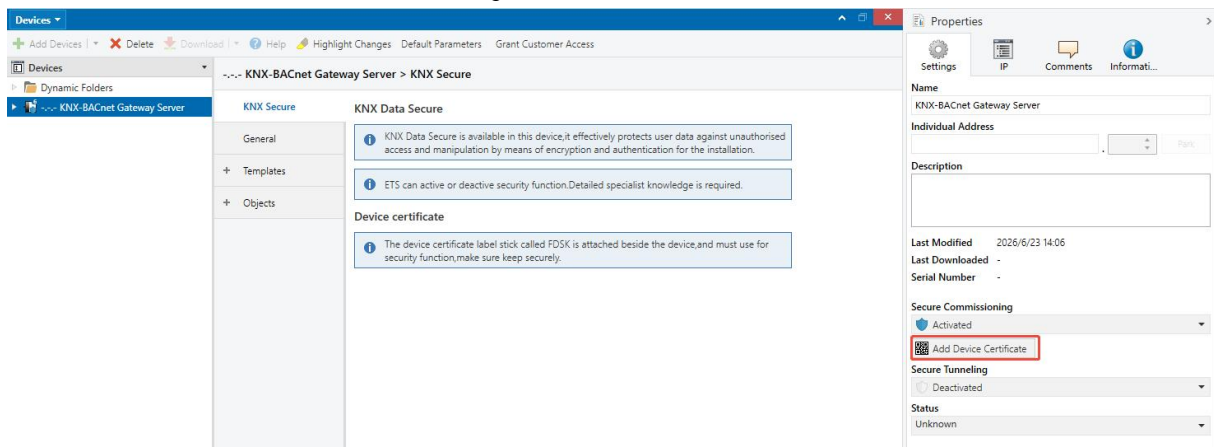


Fig.5.5.3 Add Device Certificate

✧ There is a FDSK sticker on the device, which is used for viewing FDSK number.

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 Fig.5.5.4 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).

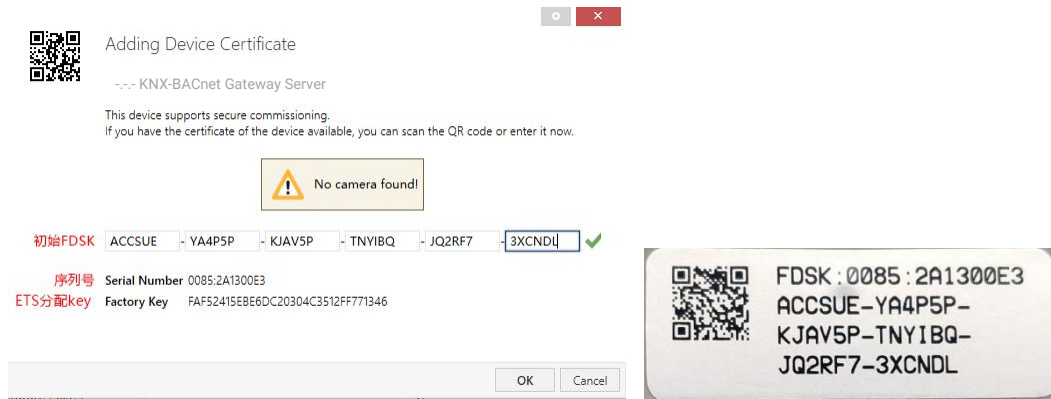


Fig.5.5.4

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 Fig.5.5.5, 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 Fig.5.5.5 and then the device can be successfully downloaded again.

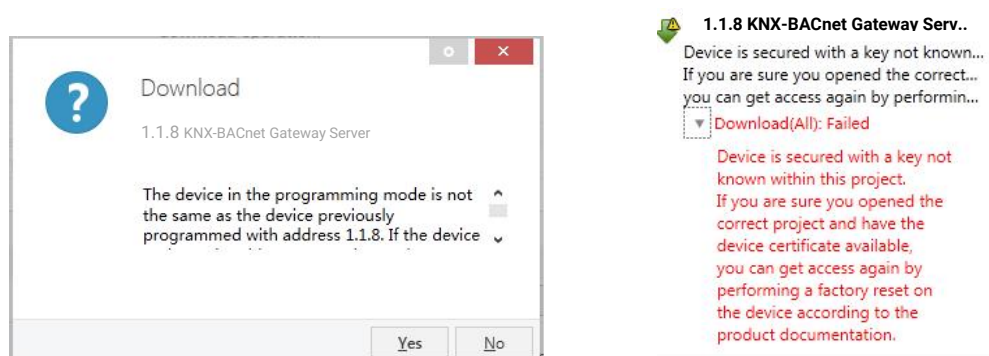


Fig.5.5.5 Example

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 Fig.5.5.6 below.



Fig.5.5.6

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. As shown in Fig.5.5.7 below, the file extension is .knxkeys.

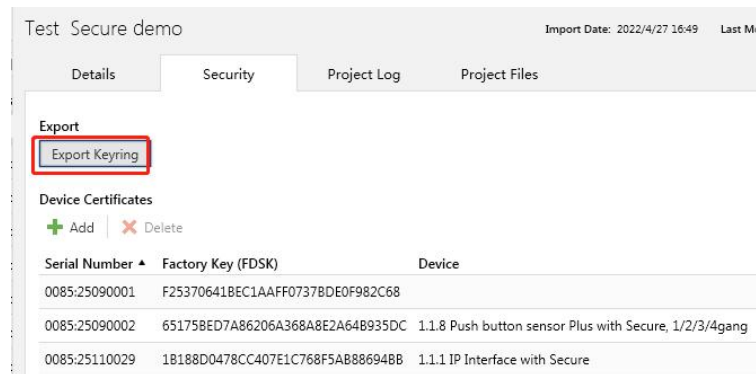


Fig.5.5.7

Example of ETS connecting via an IP tunnel:

Select the IP device, select one of the tunnels (e.g. physical address 1.1.2), and click Test. A dialog for entering the password and authentication code appears (the password and authentication code can be viewed in the properties of the IP device in the project). Enter the password and authentication code and click OK; the word "Ok" appears next to the Test button. Click Select to connect. The whole process is shown in Fig.5.5.8.

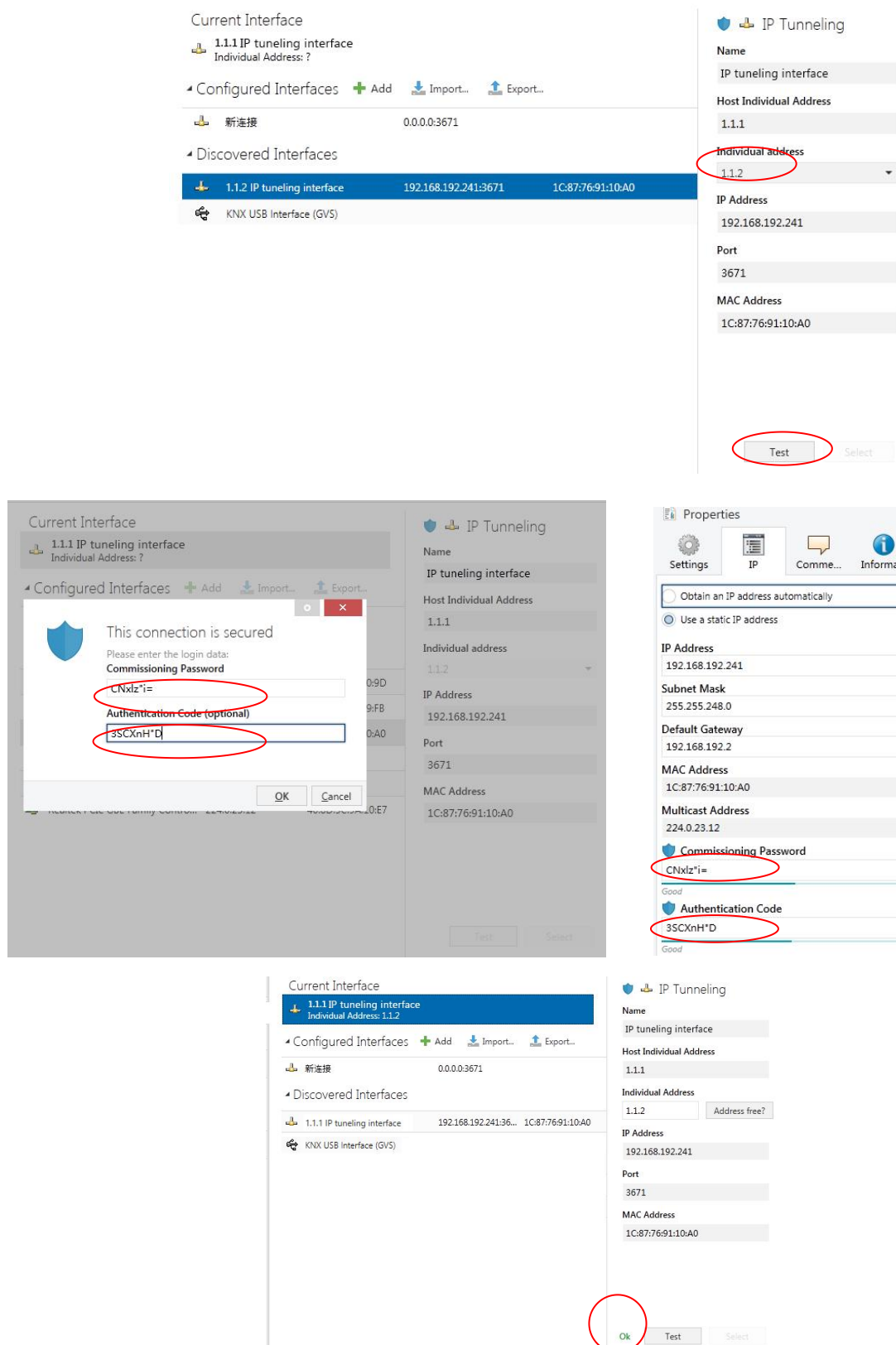


Fig.5.5.8 Example of an IP tunnel connection

In Fig.5.5.8, if "Secure Tunneling" is not activated, no commissioning password or authentication code is required when connecting as an interface. If "Secure Tunneling" is activated, ETS will prompt for

the commissioning password and authentication code when connecting.

If necessary, the KNX-BACnet Gateway Server can be reset to factory settings; please refer to [Chapter 7](#).

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 in Fig.5.5.9.

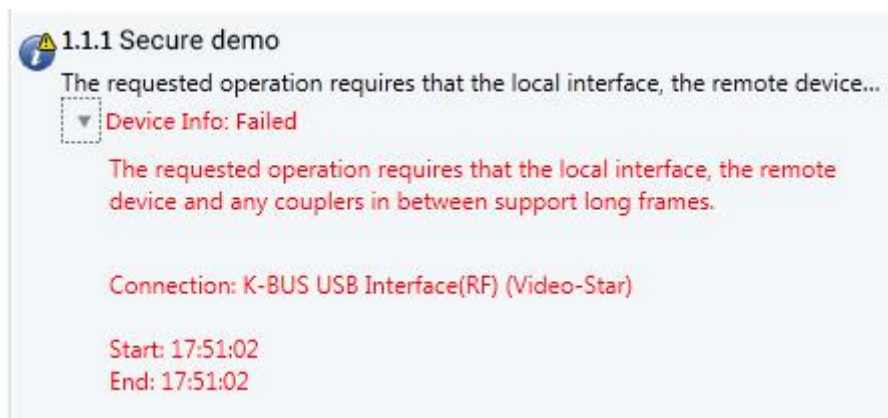


Fig.5.5.9

5.6. Removing the Device

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

When the device is operated in KNX Secure mode, it can only be reset via ETS when ETS uses the project in which this device is parameterized or when the project provides its commissioning key.

The device can be removed by right-clicking the device in its project in ETS.

Removing the application program:

- The IP address and IP configuration will be retained
- The password for the Tunneling server will be deleted, the commissioning password and authentication code will not be required when connecting (leave the dialog empty if it appears)
- The key assigned by ETS will be retained, no FDSK is required for reprogramming
- The physical address will be retained

Removing the physical address and application program:

- The device will be reset to the factory state
- Recommissioning will require the FDSK, unless the device is in its original commissioning project and its FDSK is still present in the project; then the interface can be reprogrammed directly.

Chapter 6 Description of Communication Object

The communication object is the medium to communicate other device on the bus, namely only the communication object can communicate with the bus.

NOTE: “C” in “Flag” column in the below table means enable the communication function of the object; “W” means value of object can be written from the bus; “R” means the value of the object can be read by the other devices; “T” means the object has the transmission function; “U” means the value of the object can be updated.

6.1. “Object x” Communication Object

序号 ^	名称	对象功能	描述	群组地址	长度	C	R	W	T	U	数据类型	优先级
11	Object 1 - ...	1bit value	1bit value		1 bit	C	-	W	T	U	switch	低
11	Object 1 - ...	1byte percentage value	1byte percentage value(5.001)		1 byte	C	-	W	T	U	percentage (0..100%)	低
11	Object 1 - ...	1byte unsigned value	1byte unsigned value		1 byte	C	-	W	T	U	counter pulses (0..255)	低
11	Object 1 - ...	1byte signed value	1byte signed value(...)		1 byte	C	-	W	T	U	counter pulses (-128..127)	低
11	Object 1 - ...	2byte unsigned value	2byte unsigned value(...)		2 bytes	C	-	W	T	U	pulses	低
11	Object 1 - ...	2byte signed value	2byte signed value(8.001)		2 bytes	C	-	W	T	U	pulses difference	低
11	Object 1 - ...	Pressure (Pa)	2byte float value(...)		2 bytes	C	-	W	T	U	pressure (Pa)	低
11	Object 1 - ...	4byte unsigned value	4byte unsigned value(12.001)		4 bytes	C	-	W	T	U	counter pulses (unsigned)	低
11	Object 1 - ...	4byte signed value	4byte signed value(...)		4 bytes	C	-	W	T	U	counter pulses (signed)	低
11	Object 1 - ...	4byte float value	4byte float value(...)		4 bytes	C	-	W	T	U	4-byte float value	低

Fig.6.1 “Object x”communication object

NO.	Object Function	Name	Data Type	Flag	DPT
11	1bit value 1byte percentage value 1byte unsigned value 1byte signed value(...) 2byte unsigned value(...) 2byte signed value(8.001) 2byte float value(...) 4byte unsigned value(12.001) 4byte signed value(...) 4byte float value(...)	Object x - {}	1bit 1byte 1byte 1byte 2byte 2byte 4byte 4byte 4byte 4byte	C,W,T,U	1.001 switch 5.001 percentage (0...100%) 5.010 counter pulses(0...255) /5.004 percentage (0...255%) /17.001 scene number /18.001 scene control 6.010 counter pulses (-128...127) /6.001 percentage (-128...127%) 7.001 pulses /7.013 brightness (lux) 8.001 pulses difference 9.*2-byte float value 12.001 counter pulses (unsigned) 13.001 counter pulses(signed)/ 13.002 flow rate(m³/h)/ 13.010 active energy (Wh)/ 13.013 active energy (kWh) 14.*4-byte float value

This communication object is used to receive the control commands issued by the BA system from the KNX bus.

The data point type depends on the parameter settings.

The name in parentheses changes with the parameter "Object description". If description is empty, display "Object x -" by default.

Table 6.1 "Object x" communication object

Chapter 7 Factory settings

The default parameter settings of the KNX-BACnet Gateway Server at delivery are as follows:

Physical address	15.15.254
Physical address of the IP tunneling connection	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

When the IP address needs to be reset, the device can be reset to the factory configuration.

The procedure to reset the device to the factory configuration is 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. The LAN, KNX, and programming LED will turn off, and then the LAN and KNX LED will return to normal status and the device restarts. After the restart is completed, the device is restored to the factory settings.

For more information about the FDSK (Factory Default Setting Key), please refer to [Chapter 5.5](#).