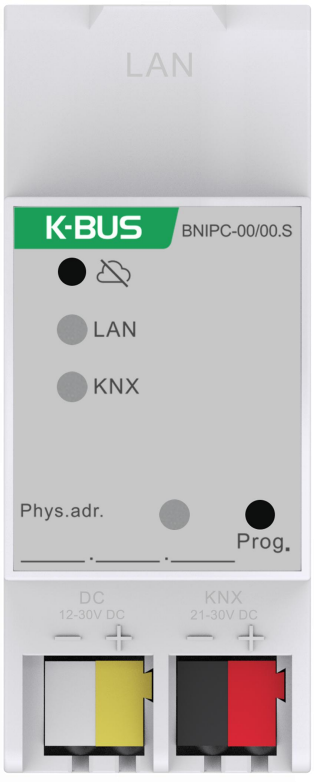
User Manual

K-BUS® IP Interface with Secure and Cloud_V1.0

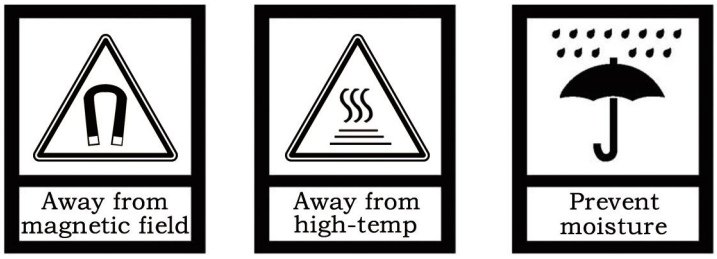
BNIPC-00/00.S



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 and Cloud 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.

For operation an additional 12~30V DC supply is necessary. The bus connection and auxiliary power supply connection are 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 3.3.

This product is not only supported to the basic functions, but also remote debug function, which is related to a website access via “KNX Engineering Assistant Management Platform” and connection management via KNX project assistant software. KNX Engineering Assistant Management Platform is a Web configuration and is used for enterprise management, engineer management and device management. KNX Project Assistant is a PC configuration and is used for remotely connecting and debugging projects.

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 the operation and usage of KNX Engineering Assistant

Management Platform and KNX Project Assistant, and explains how to use the interface device by the application examples.

Note: The device does not support programming itself using an IP tunneling connection, but it can be programmed via a broadcast connection (Realtek PCIe GBE Family Controller).

The device also does not support bus monitoring.

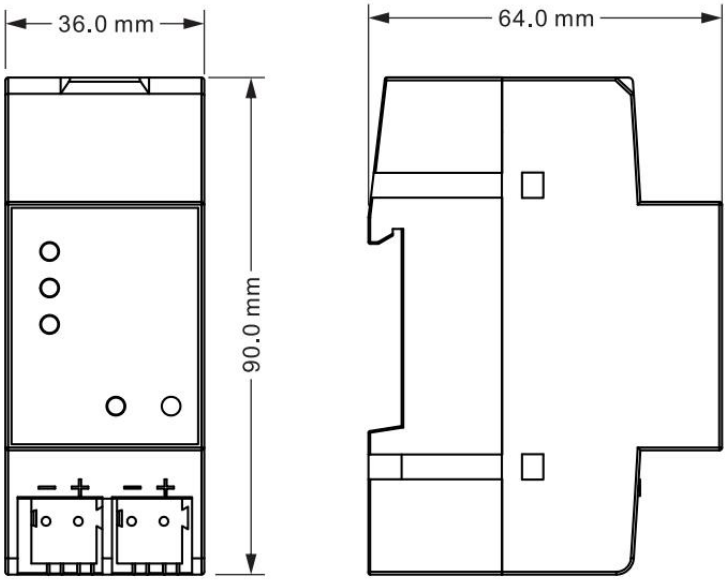
Chapter 2 Technical Data

Power supply	Operation voltage	21-30V DC, via the KNX bus
	Current consumption	<5mA, 24V; <4mA, 30V
	Power consumption	<120mW
	Auxiliary voltage	12-30V DC
	Auxiliary current	<60mA, 24V; <50mA, 30V
	Auxiliary power consumption	<1.5W
Connections	KNX	Via bus connection terminal (red/black)
	Auxiliary supply	Via bus connection terminal (yellow/white)
	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
	Cloud button	Press to disable/Enable ETS commissioning via cloud
	LAN LED	Always ON: enable ETS commissioning via cloud Single flashing: disable ETS commissioning via cloud Double flashing: abnormal connection to cloud OFF: unconnected or abnormal Network
	KNX LED	Flashing: the application layer running normally OFF: the application layer running abnormal
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	Plastic housing, Beige	

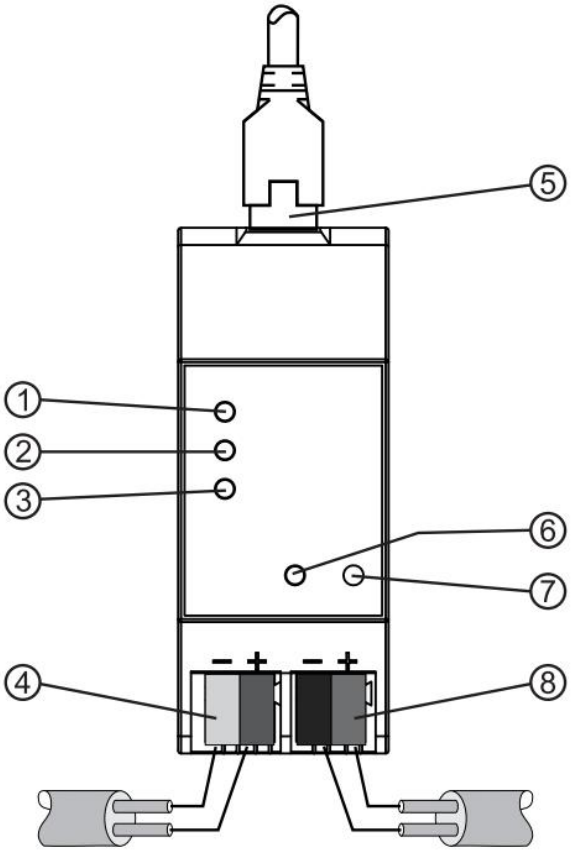
Application program	Max. number of communication objects	Max. number of group address	Max. number of associations
IP Interface with Secure	0	0	0

Chapter 3 Dimension and Connection Diagram

3.1. Dimension diagram



3.2. Connection diagram



① Cloud button: Press to disable/Enable ETS commissioning via cloud

② LAN LED:

Always ON-enable ETS commissioning via cloud

Single flashing-disable ETS commissioning via cloud

Double flashing-abnormal connection to cloud

OFF-unconnected or abnormal Network

③ KNX LED:

Flashing-the application layer running normally

OFF-the application layer running abnormal

④ Auxiliary power supply connection

⑤ LAN connection

⑥ Programming LED, red LED ON for assignment of physical address

⑦ Programming 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

⑧ KNX 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.

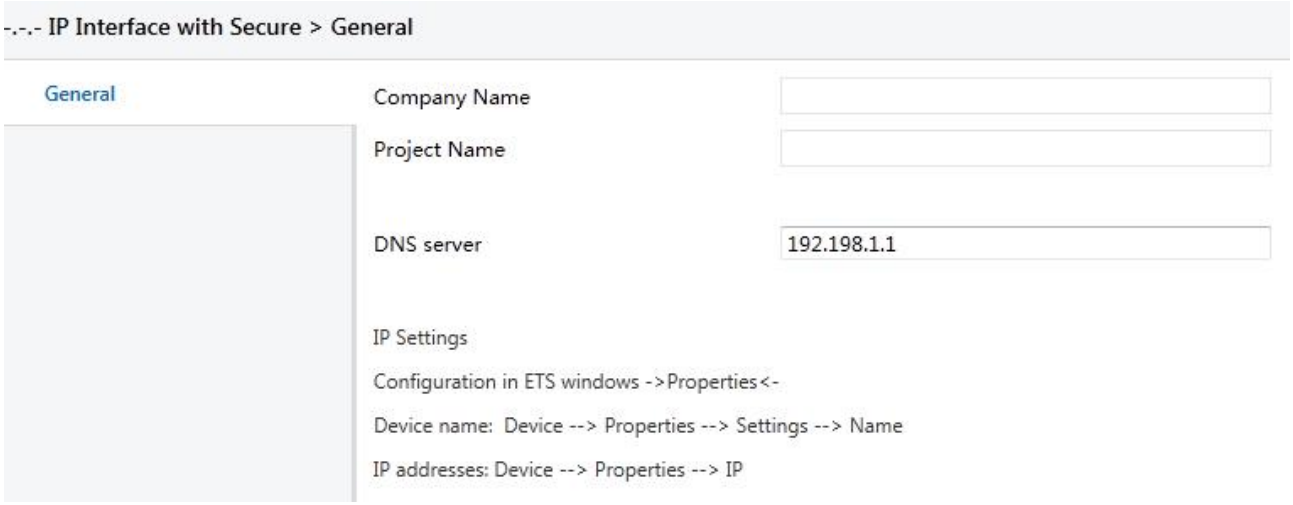


Fig 4.1.1 “General” parameter window

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.

Note: the project name needs to be consistent with the enterprise name in KNX Engineering Assistant Management Platform, for device to be automatically associated with this project. You can find this device from bound devices of this project in KNX Engineering Assistant Management Platform.

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.

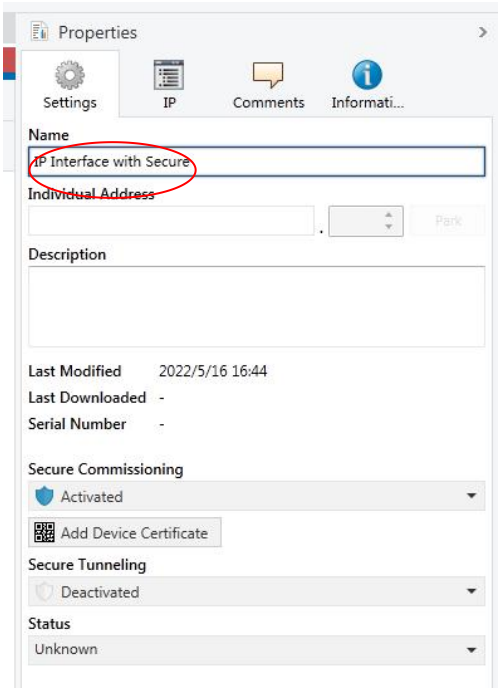


Fig. 4.1.2 Settings

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

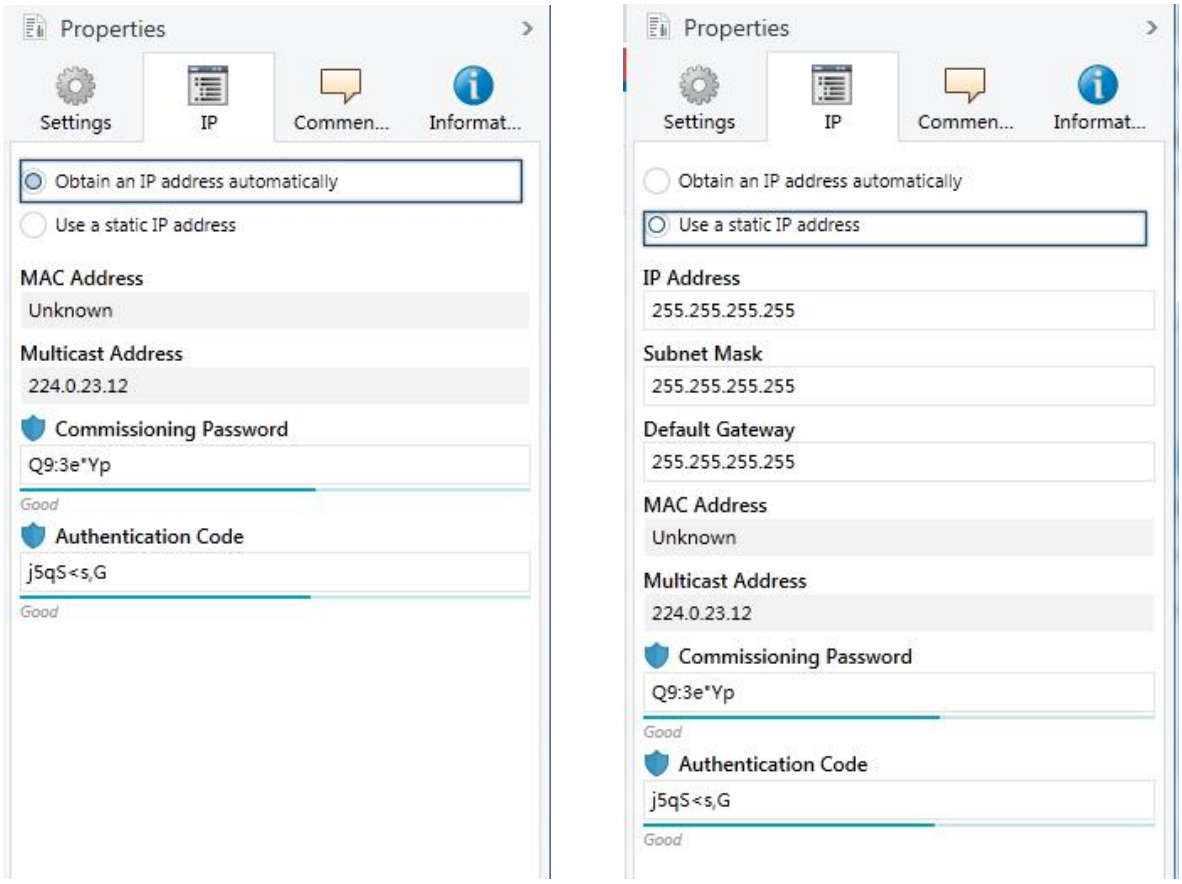


Fig. 4.1.3 IP

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.

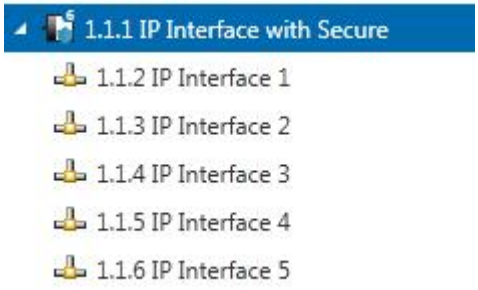


Fig.4.2.1 Tunneling

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)

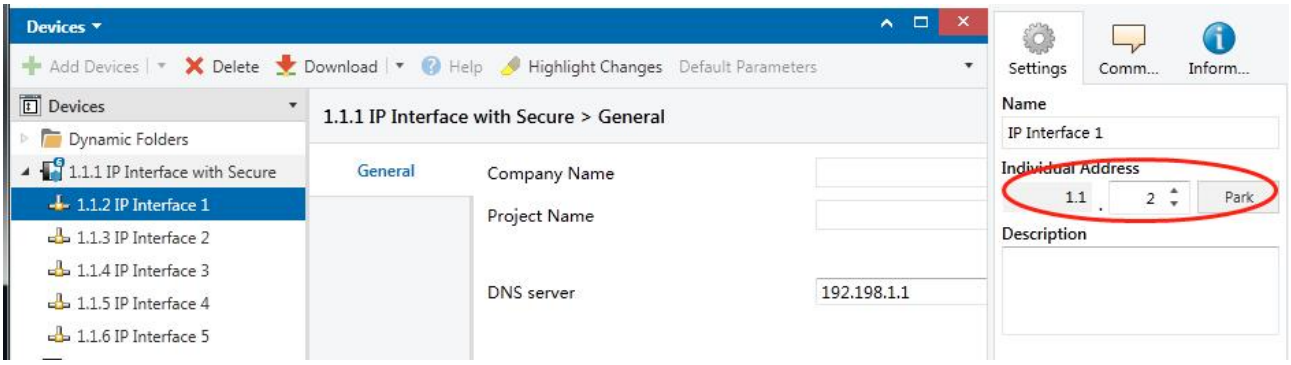


Fig.4.2.2 Setting - Park

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.

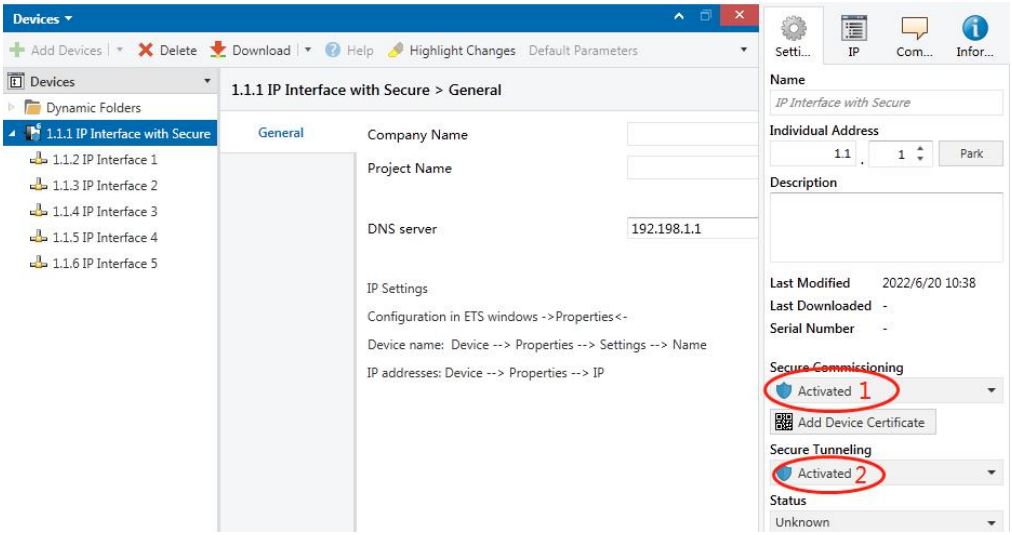


Fig.4.2.3 Setting - Secure activated

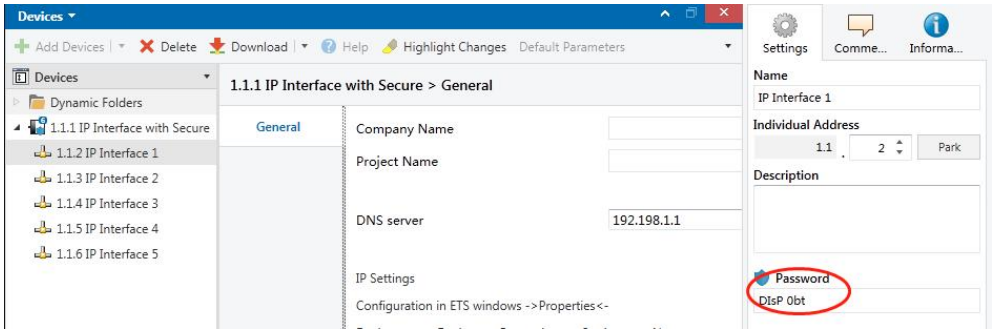


Fig.4.2.4 Setting - tunneling password

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).

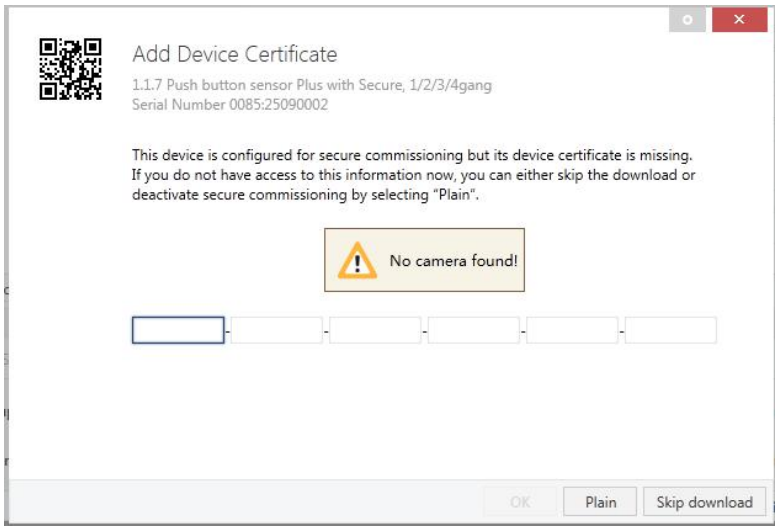


Fig.4.3.1 Add Device Certificate window

✧ 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.

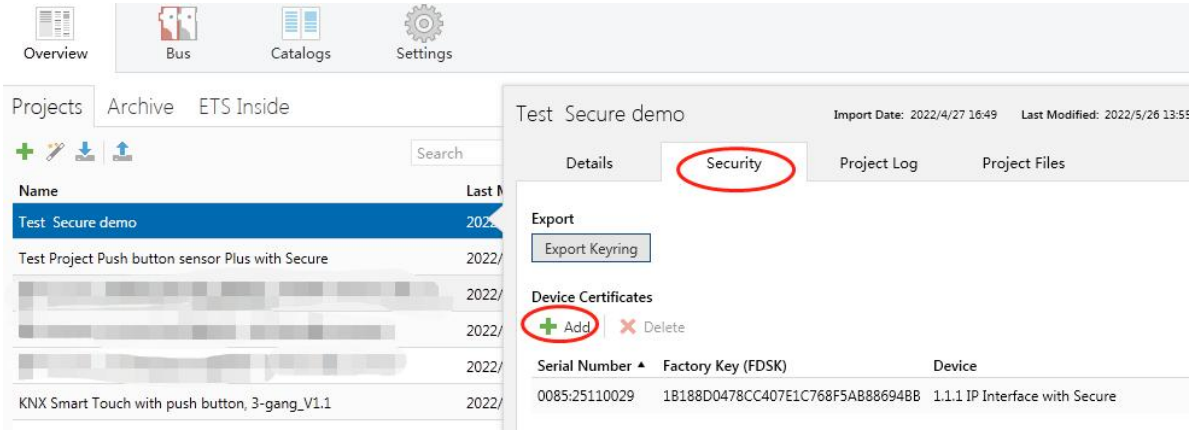


Fig. 4.3.2 Add Device Certificate in overview

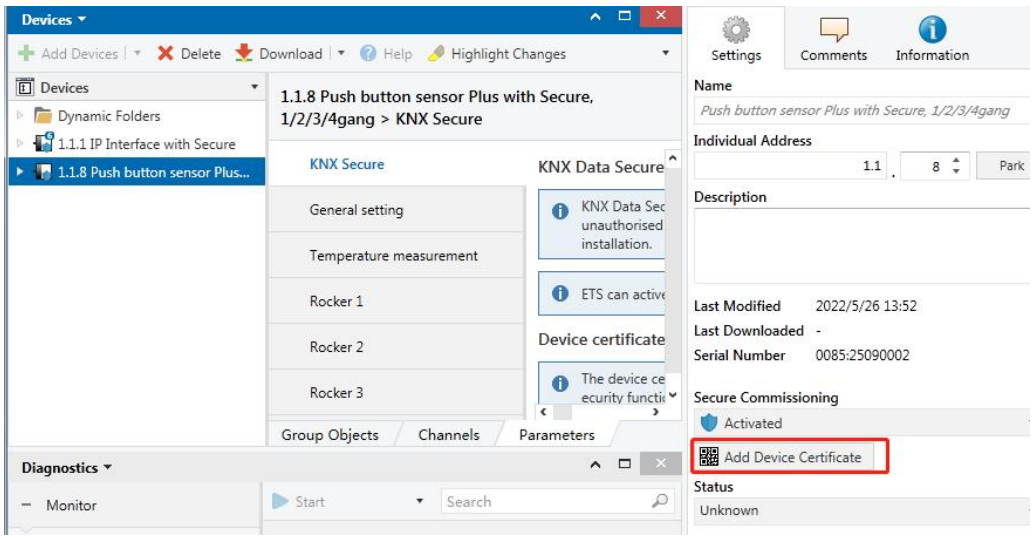


Fig. 4.3.3 Add Device Certificate in project

✧ A FDSK sticker is applied 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.

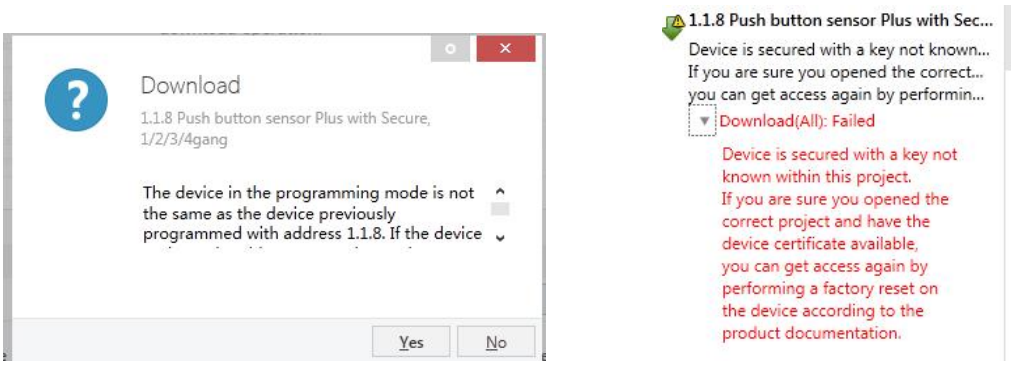


Fig. 4.3.5 Example

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.

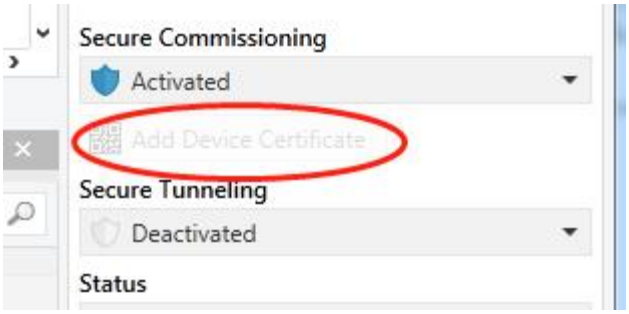


Fig. 4.3.6

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.

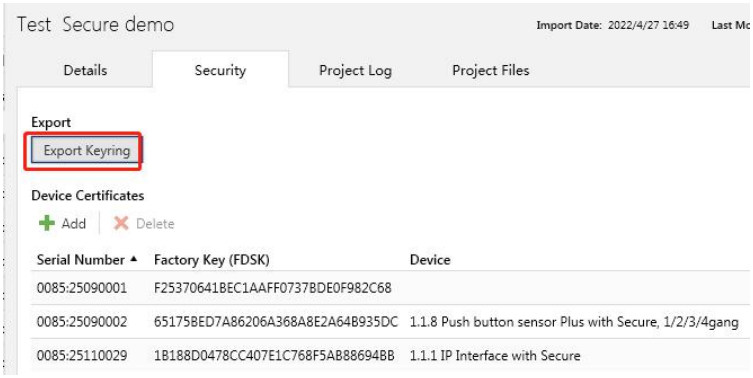


Fig. 4.3.7

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.

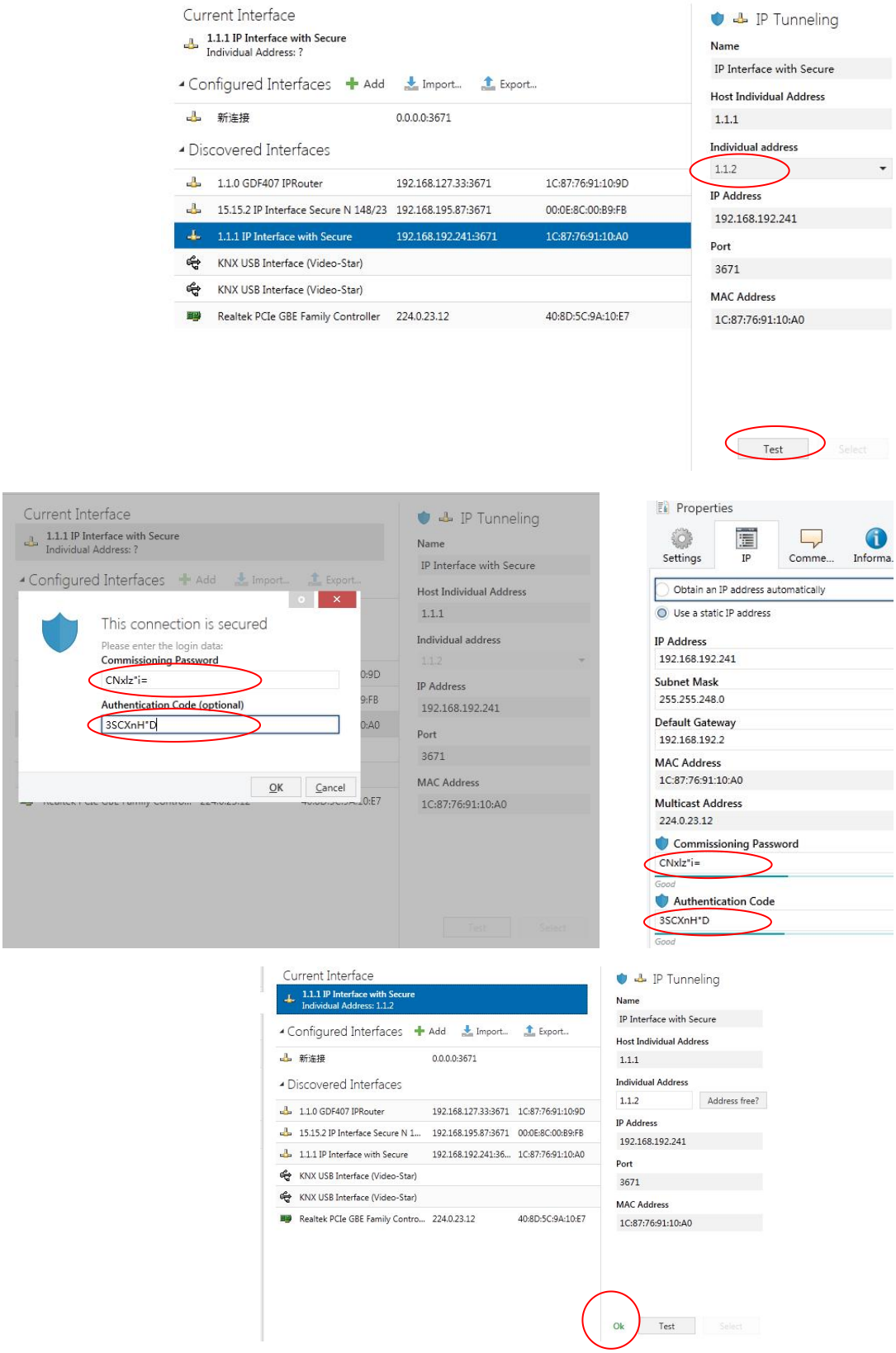


Fig. 4.3.8 IP tunneling connection

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 KNX indicators is off and programming LED indicator is flashing, and the device enters the restart, and after the KNX return to normal instructions, and 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 description, and upgrade devices. **Note: If KNX security is enabled, device description and 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.

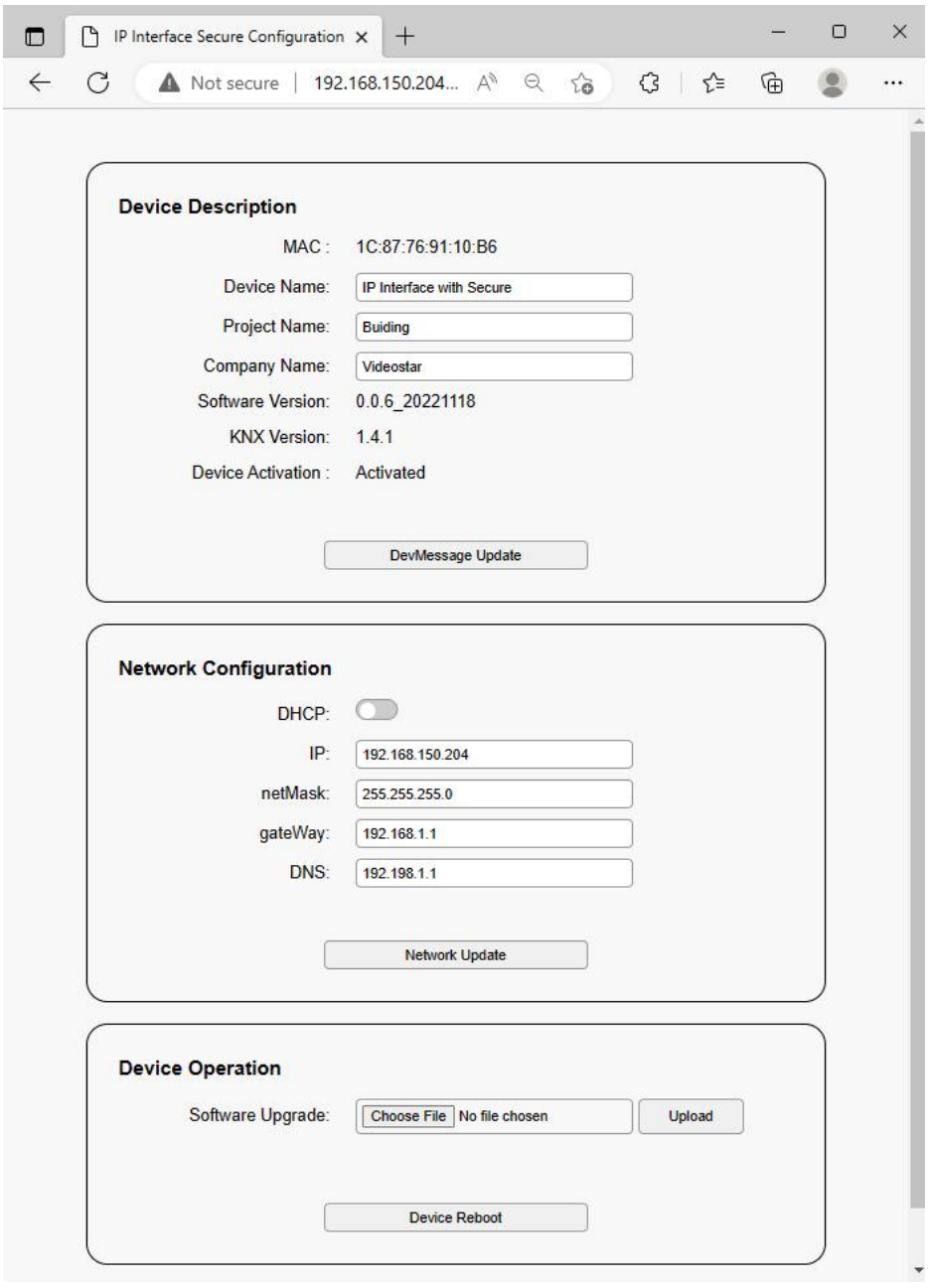


Fig.6.1 IP Interface web configuration window

Device Description:

① **MAC Addr.:** Display the MAC address.

② **Device Name:** Display or set the device name.

③**Project Name:** Display or set the project name.

④**Company Name:** Display or set the company name.

⑤**Software Version:** Display the firmware (linux software.fwp) version and date.

⑥**KNX Version:** Display the firmware (KNX software.bin) version.

⑦【**DevMessage Update**】 Click this button to save after setting changes are completed. Pop up following window after the update is successful.

Network Configuration:

Firmware Date: Display the date of the device firmware.

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

② **IP:** Display or set the IP address.

③ **netMask:** Display or set the subnet mask.

④ **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.

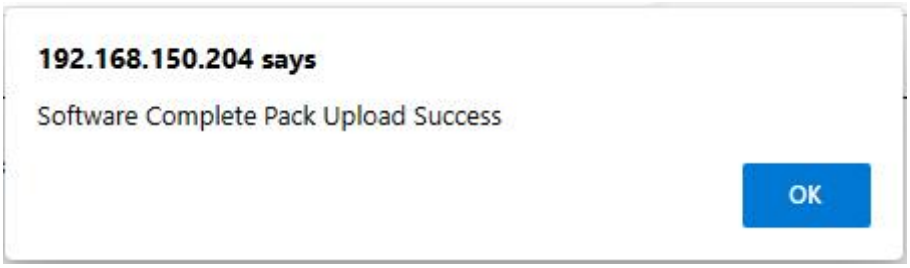
⑤ **DNS:** Display and set DNS.

⑥【**Network Update**】**:** Click this button to save after finishing configuration. Pop up following window after the update is successful. If change IP address, you should input new IP address to re-enter the configuration interface, check the latest information.

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.

Device Operation:

① **Software Upgrade:** It is used to upgrade the firmware of the device. Click the button [Choose File] to choose the firmware (.bin, .fwp) of the updated device, and then click the button [Upload] to update the device. Pop up following window after the update is successful. (After the firmware is uploaded successfully, around 30s, you can refresh the webpage to confirm whether the upgrade is successful when it is not busy.)



②【**Device Reboot**】**:** Press the button to restart device.

Chapter 7 KNX Engineering Assistant Management Platform

Login address of KNX Project Management Platform: https://assistant.gvs-icloud.com/, as shown as Fig.7.1.

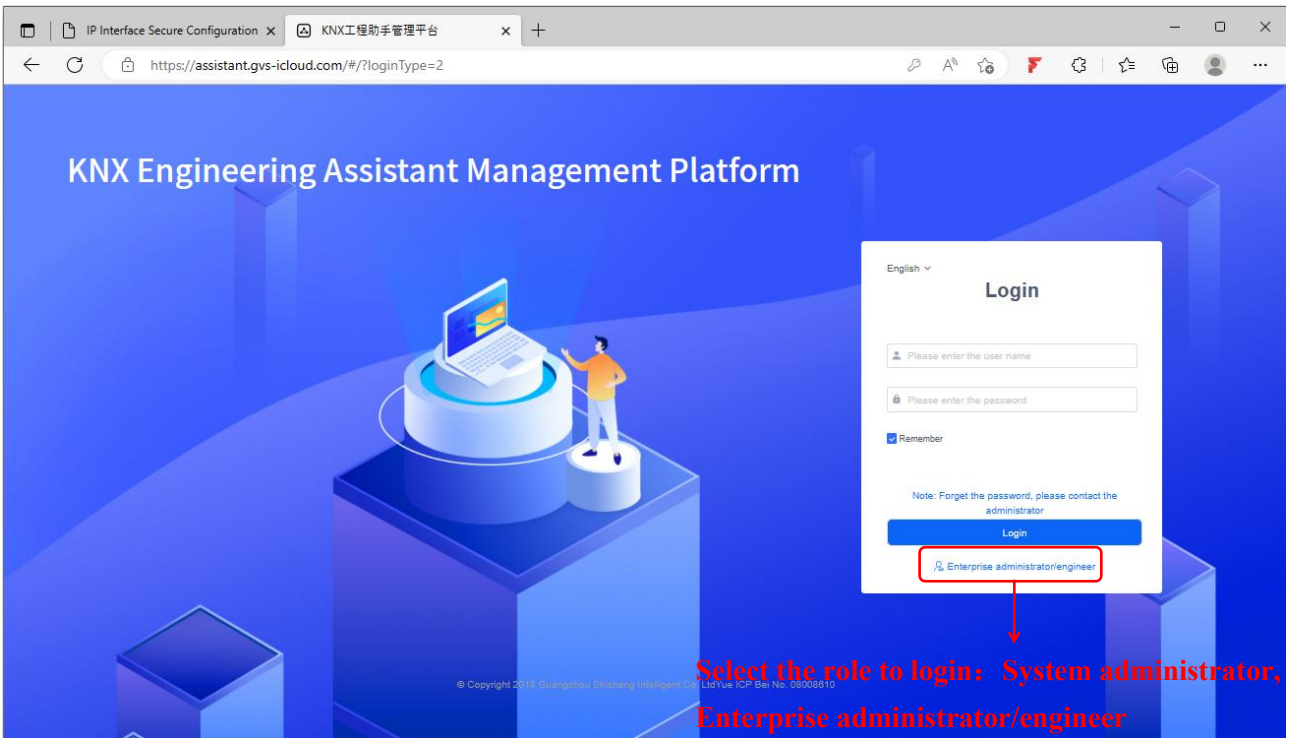


Fig.7.1 Login window

KNX Project Management Platform is used for assisting IP interface for remote debugging of KNX projects, including System client (login as System administrator), Enterprise client (login as Enterprise administrator / engineer).

System client is used to establish information about the enterprise to which the device belongs, such as enterprise code, enterprise name, legal person, enterprise administrator, enterprise account and etc. Enterprise account is used for enterprise administrator to login enterprise client. **The system administrator account is built into the system and cannot be changed, there is usually only one account, and it is usually the manufacturer or organization that acts as the system administrator.**

Enterprise client is used for enterprise-to-project (engineer / device) management. You can view the number of projects, engineers and IP devices on home page. Enterprise administrator can create project and engineer account from the platform, including user name, engineer name, device accredit and etc, also enable /disable engineer account. You can view device name, MAC address, device ID, project, online status and etc., as well as generate a device authorization code and its valid period. **Account and initial password of enterprise client are obtained from system administrator, that is created by system administrator.**

The following mainly describes the operation of the enterprise client, and the detail of system client is not described here.

7.1. Enterprise management

7.1.1. Login

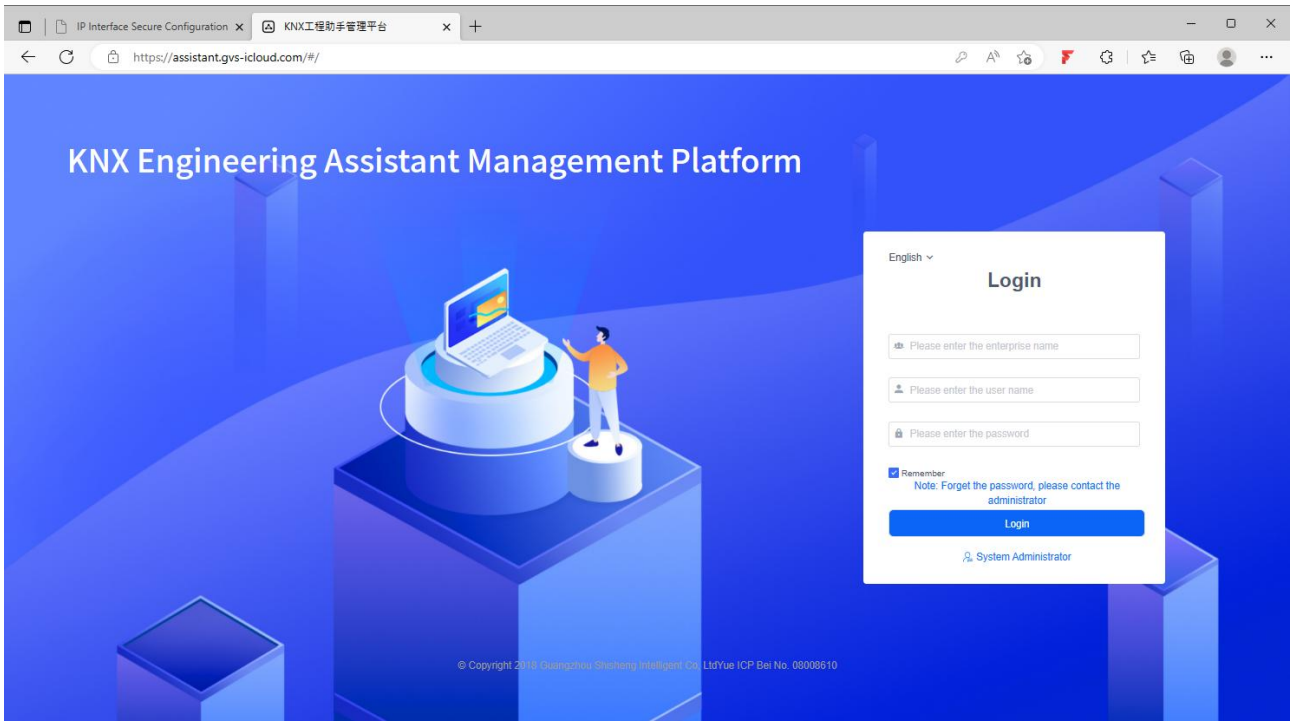


Fig.7.1.1.1 Login window

Please contact the manufacturer to obtain account and password of enterprise client, that is, contact the system administrator to provide it. Then input correct enterprise name, user name and password to login.

The enterprise name and the user name can only be created and modified by system administrator.

It will pop up a dialog box that prompts you to change your password when firstly login, as shown as following figure. In order to ensure the security of the account, it is mandatory to change the initial password, if cancel change and will return the login window. After successful login, initialize password again will not pop up this dialog box.

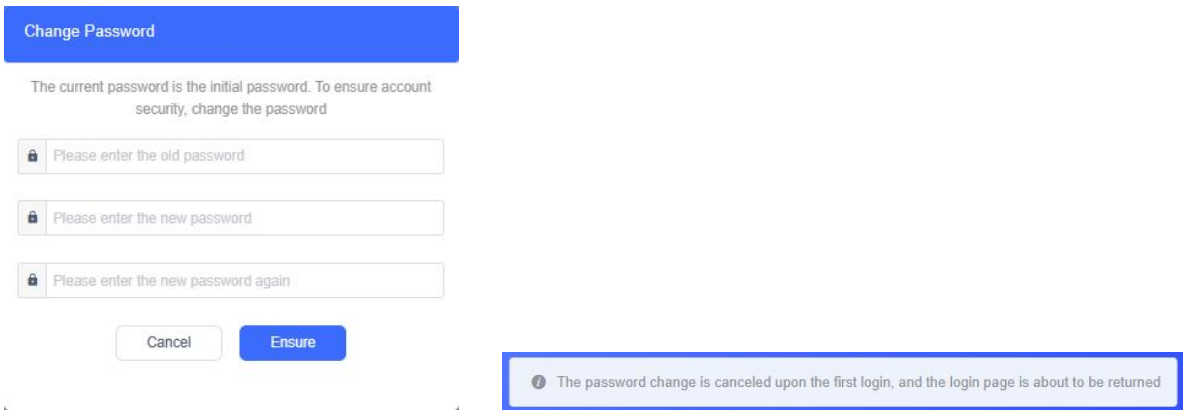


Fig.7.1.1.2 Password change

7.1.2. Home

Home page shows an overview, including number of projects, engineers and devices, enterprise name, enterprise code, account status and etc. It provides the password changing and logout in the upper right corner of the interface.

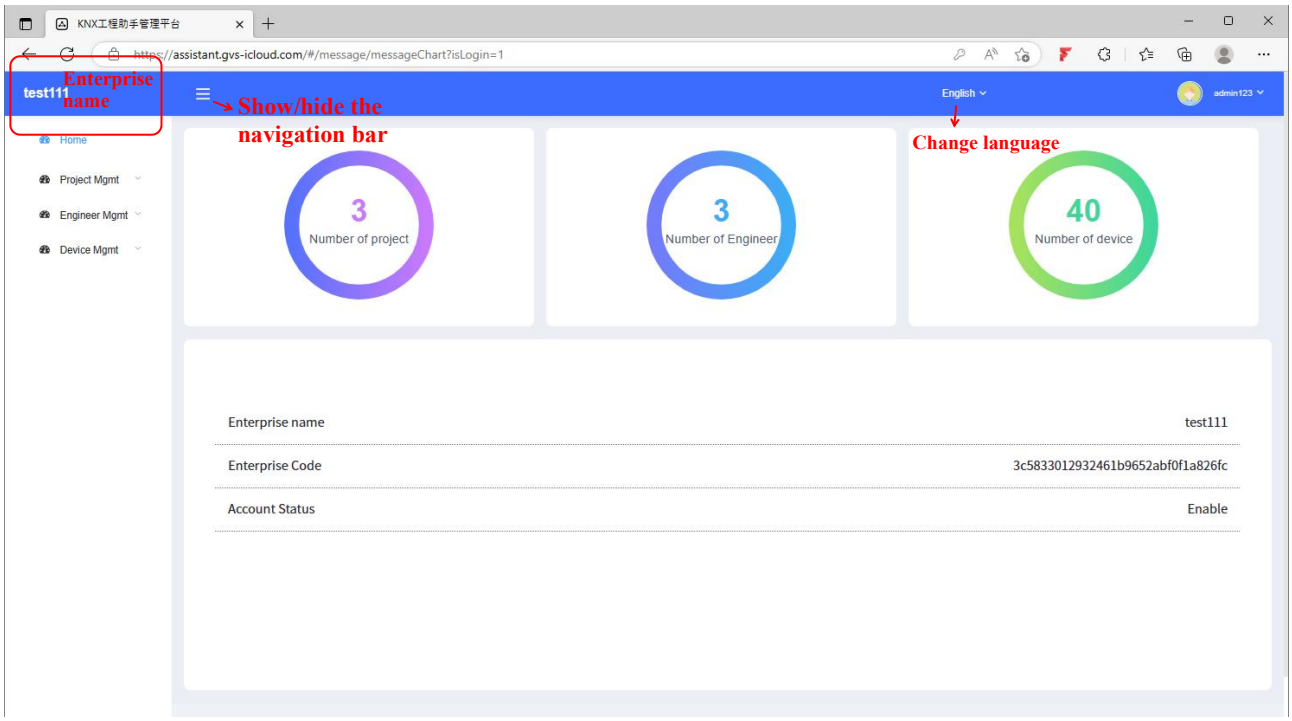


Fig.7.1.2 Home page of enterprise management

The navigation bar on the left of home page, Enterprise administrator can open the interfaces of project management, engineer management and device management to edit or view. Operation of each management interface is described in following chapters.

7.1.3. Project management

Interface of project management is shown as Fig.7.1.3.1, you can add, delete, view, search and sort the projects.

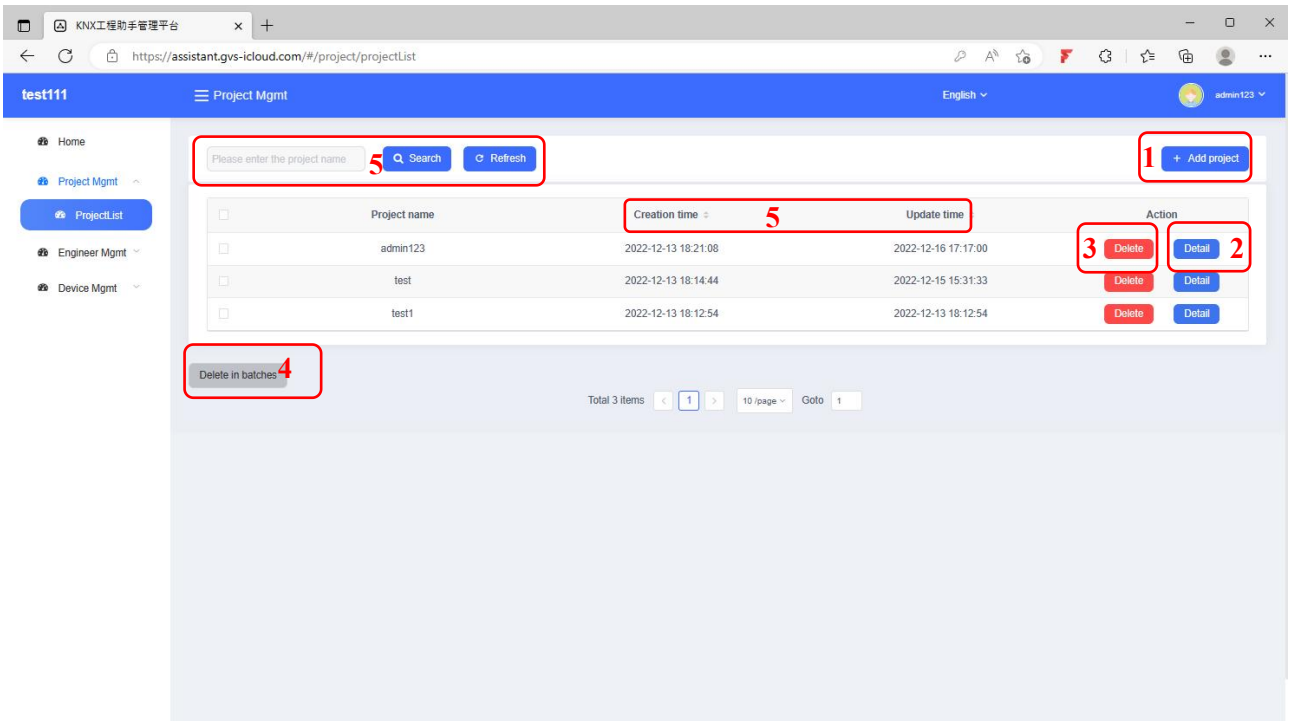


Fig.7.1.3.1 Project management

The instructions for the items in the figure are as follows:

(1) Add new project

Click "+ Add project" button, pop up a window as shown as Fig.7.1.3.2, enter project name in the window, and the operation is successful after clicking "Ensure", the newly created project is added to the project list.

Fig.7.1.3.2 Add new project

Project name: 1-30 characters, all blank strings are prohibited.

(2) Detail

Click “Detail” on interface of project management, you can view the detail information of project, as show as Fig.7.1.3.3.

View or edit project information, and view the device information and device status of the project, including device name, device ID, MAC address, online status.

Note: the association of device with the project needs to be configured in ETS, the enterprise name and project name configured for the device in ETS must be consistent with the enterprise name and project name of the management platform, to establish an association.

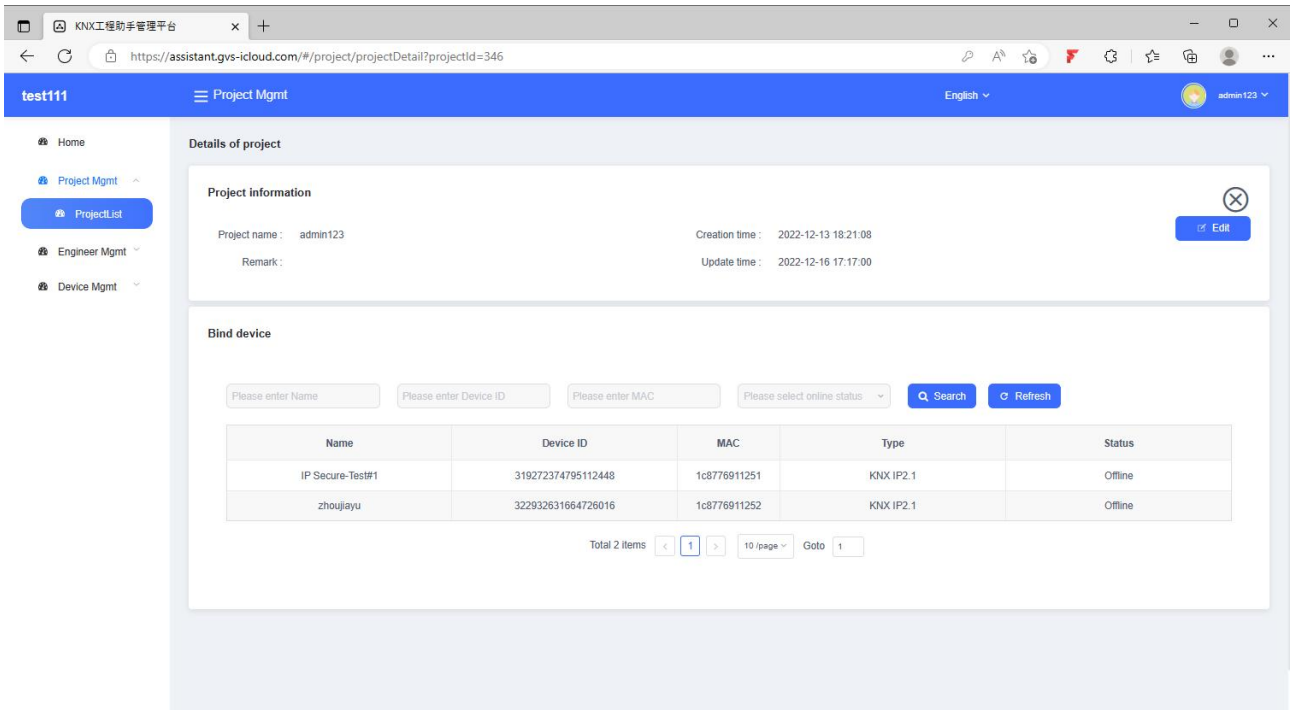
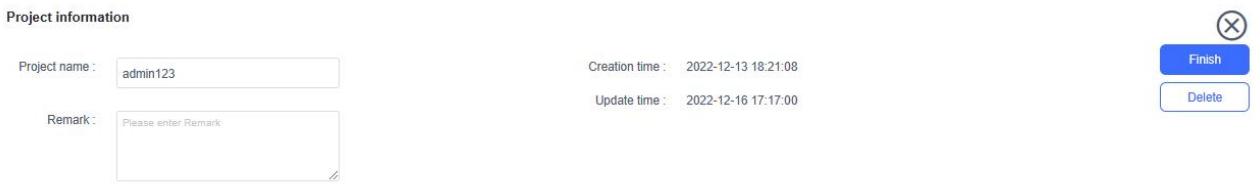


Fig.7.1.3.3 Project detail

Edit project information, you can modify project name and remark, as shown as following figure, click the “Finish” button when finished, delete this project is to click “Delete” button.



Edit project information

(3) Delete

Click “Delete” on interface of project management, pop up a window as following figure, click “Delete” button and the devices in this project are deleted synchronously. **When re-add a new project with the same information (the name of the enterprise and project coincide), the devices of original project will be associated automatically.**

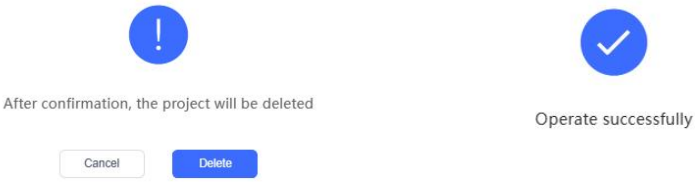


Fig.7.1.3.4 Delete project

(4) Delete in batches

Choose multiple projects and delete together.

(5) Search&Sort

①Search: support fuzzy search of keywords, such as project name.

②Refresh: refresh the interface display when there is update.

③Sort: sort with creation time or update time.

7.1.4. Engineer management

Interface of engineer management is shown as Fig.7.1.4.1, you can add, delete, view, search and sort engineer, as well as authorize device to engineers.

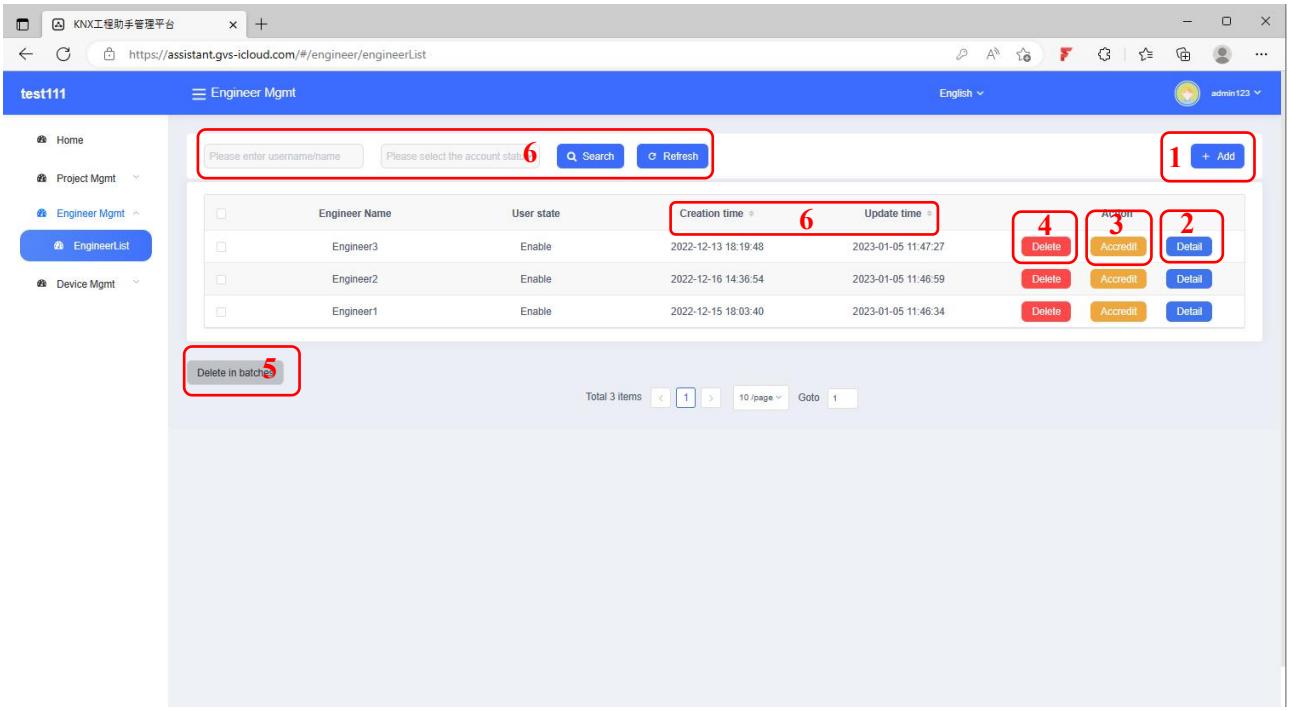


Fig.7.1.4.1 Engineer management

The instructions for the items in the figure are as follows:

(1) Add new engineer

Click "+ Add" button, pop up a window as shown as Fig.7.1.4.2, enter engineer user name and name of engineer in the window, as well as add remark, clicking "Ensure", then a pop-up window prompts you with a randomly generated initial password (allow copying of user name and password) for the engineer, the newly created engineer is added to the engineer list.

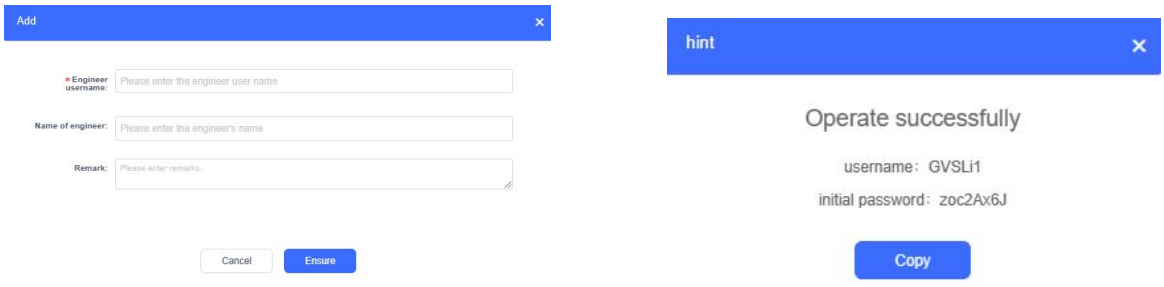


Fig.7.1.4.2 Add new engineer

Engineer user name: 6-50 characters in English or a combination of English and digit, - is allowed.

Name of engineer: 1-50 characters, all blank strings are prohibited.

Remark (optional): 0-200 characters, all blank strings are prohibited.

(2) Detail

Click “Detail” button on interface of engineer management, you can view the detail information of engineer, as show as Fig.7.1.4.3.

View or edit engineer information, and view / edit authorized devices.

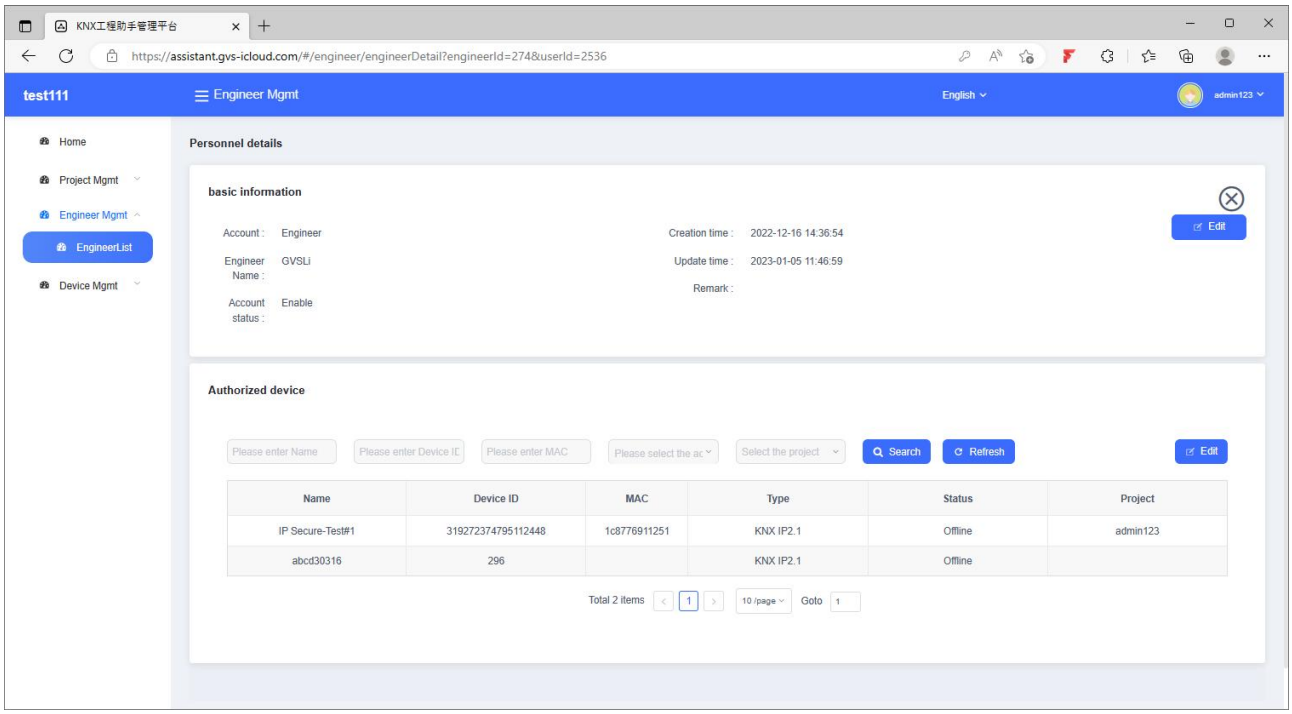
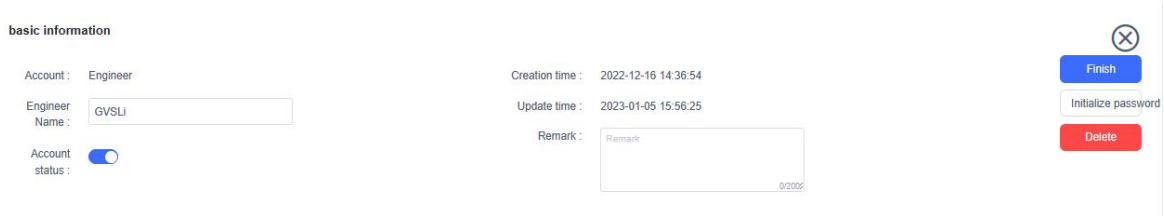


Fig.7.1.4.3 Engineer detail

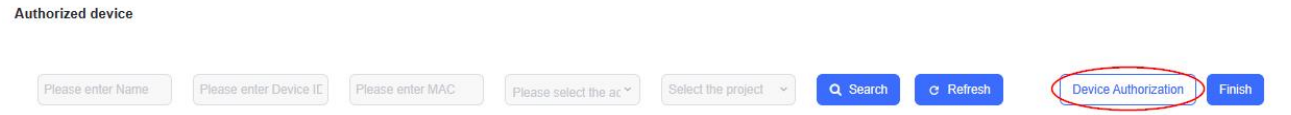
①Edit basic information, as following figure:



Edit basic information of engineer

- Engineer Name: you can modify the engineer name.
- Account status: Enable / Disable.
- Remark: you can add a remark.
- Delete: delete this engineer. Jump to the interface of engineer management after successful delete, and corresponding engineer in the list is also deleted.
- Initialize password: enterprise administrator can initialize the login password of engineer.

②Edit authorized devices, as following figure:



Click “Device Authorization”, enter the interface of device authorization:

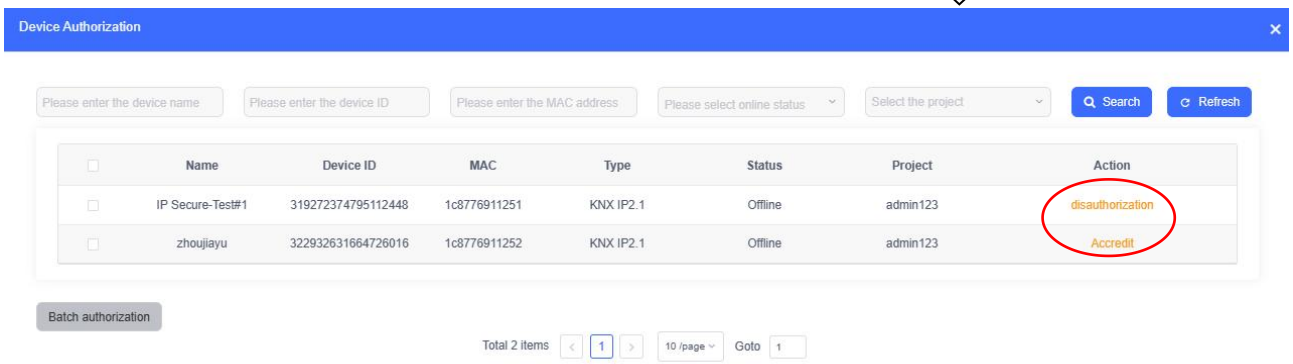


Fig.7.1.4.4 Device authorization

- ❖ Support precise search of device name, device ID, and MAC address;
- ❖ Support the filter of the device online / offline status and the project to which it belongs;
- ❖ Accredit / Disauthorization: click “Accredit” button, if the operation is successful, the authorization is successful, conversely, the same action can be disauthorized. After confirmation, engineer will not be able to remotely debug the equipment through KNX Assistant, please exercise caution!
- ❖ Batch authorization / disauthorization: choose multiple devices and accredit / disauthorize together.

(3) Accredit

Click “Accredit” on interface of engineer management, enter the interface of device authorization, as show as Fig.7.1.4.4, enterprise administrator authorizes the device for engineers, or cancel the authorization. When authorize the devices to one, then he can operate remote project debugging with KNX Project Assistant.

(4) Delete

Click “Delete” on interface of engineer management, pop up a window as following figure, click “Delete” button and remove the authorization between devices and engineer, and the personnel will not be able to use KNX Project Assistant to remotely debug the device.

Fig.7.1.4.5 Delete engineer

(5) Delete in batches

Choose multiple engineers and delete together.

(6) Search&Sort&Refresh

①Search: support fuzzy search of keywords, such as user name, name, phone number or email address.

②Select the account status (Enable / Disable).

③Refresh: refresh the interface display when there is update.

④Sort: sort with creation time or update time.

7.1.5. Device management

Device management interface is shown as Fig.7.1.5.1, you can search device information (device name, device ID, MAC address, online status and project), as well as manage authorization code of IP device in the project.

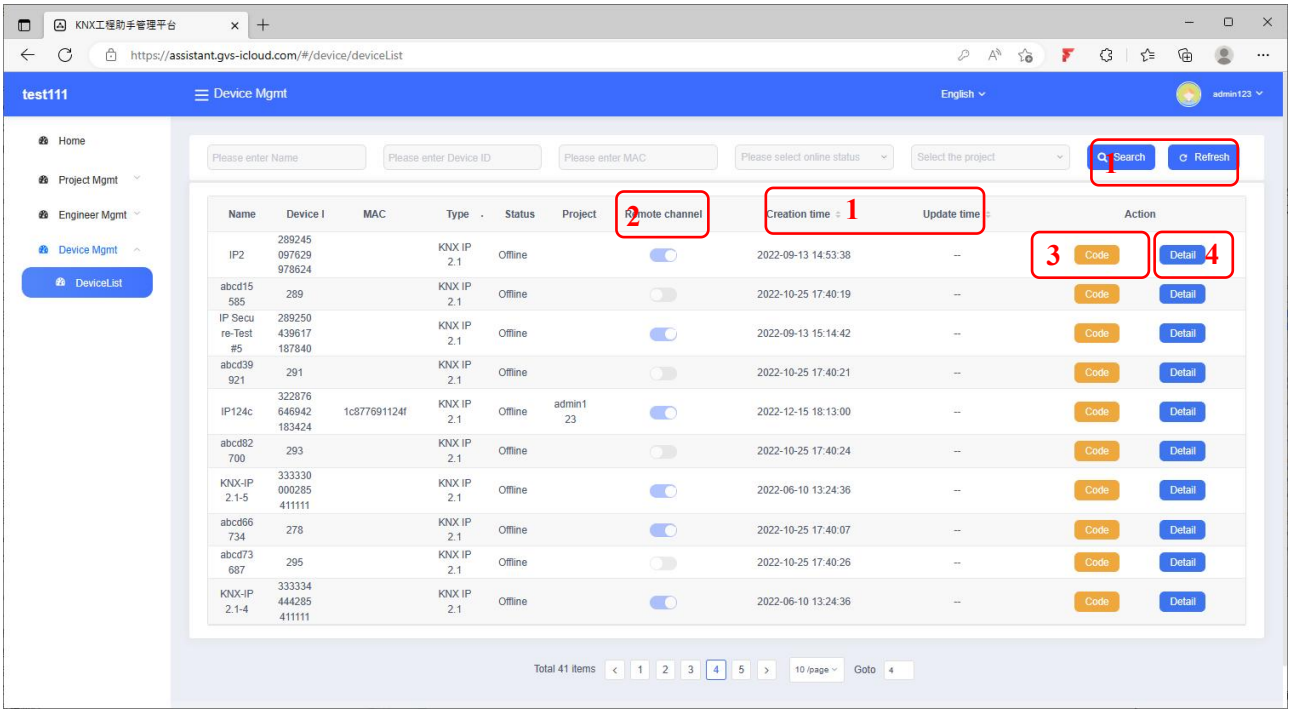


Fig.7.1.5.1 Device management

The instructions for the items in the figure are as follows:

(1) Search&Sort&Refresh

①Search: support search of keywords, such as device name, device ID, MAC address.

②Select the device online status (Online / Offline) and the project belonged to.

③Refresh: refresh the interface display when there is update.

④Sort: sort with creation time or update time.

(2) Remote channel status

Enable or disable remote debug channel via the Cloud button on the device. When it is enabled, you can remotely connect the device to debug project, if disabled, you can not connect the device remotely.

(3) Generate authorization code

Click “Code” on interface of device management, pop up the window for authorization code, as show as Fig.7.1.5.2. Each device only has a authorization code, if it already has a authorization code, the original code will be replaced by the new one. There are a valid period for authorization code, when generate a new code, you can set a period of time which is specific to hour:minute. Operation is as shown as following figure:

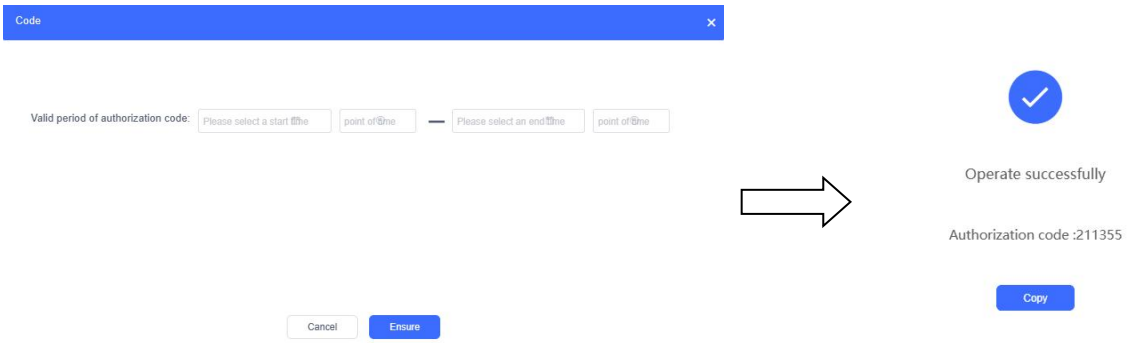


Fig.7.1.5.2 Generate authorization code

(4) Detail

Click “Detail” on interface of device management, enter the interface of device details, you can view the device information, authorization code and its status (Ineffective, In use, Lost effectiveness), the valid period of authorization code, creation time and so on. And you can generate or cancel an authorization code.

Authorization code is 6 digits, and used in KNX Project Assistant when engineers need to assist with debugging remotely.

- ❖ Ineffective: already has an authorization code but not reach the valid period.
- ❖ In use: the authorization code is in the valid period.
- ❖ Lost effectiveness: the authorization code is already out off the valid period.

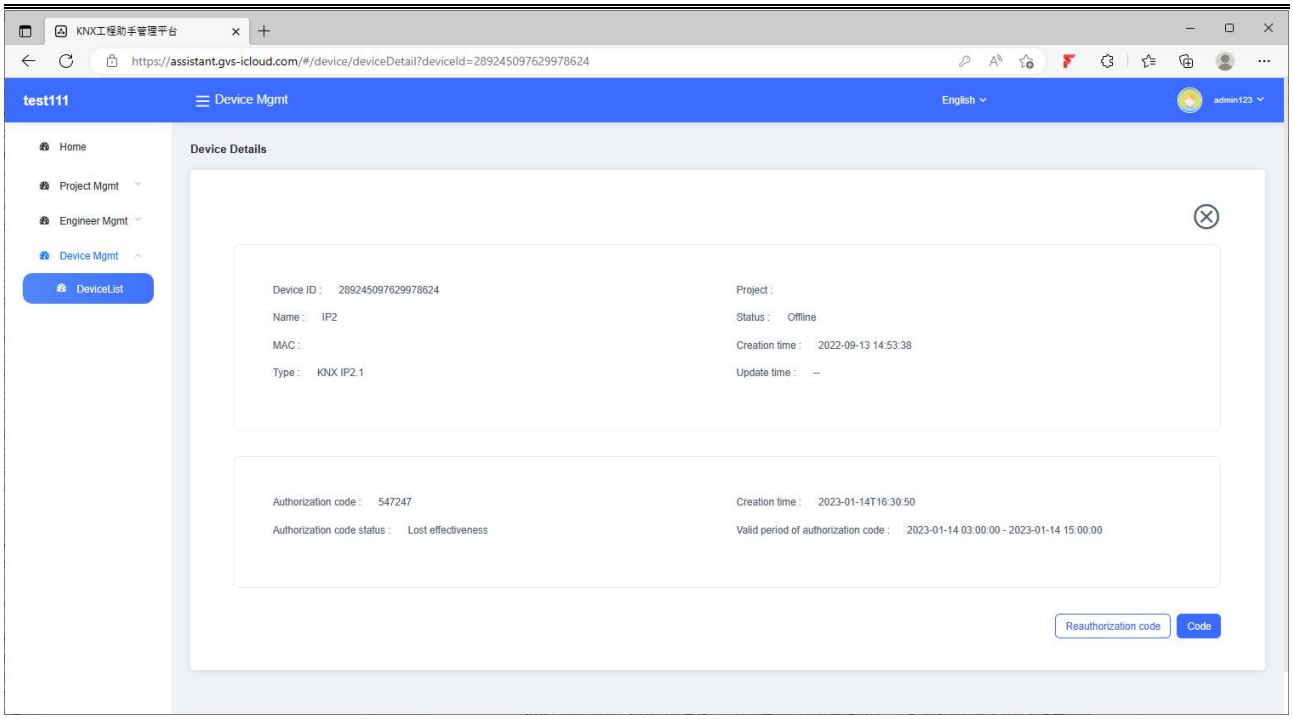


Fig.7.1.5.3 Device details

7.1.6. Additional Instructions

Enterprise administrator create account for engineers, and engineers also can login KNX Engineering Assistant Management Platform with created user name and initial password. The interface as shown as Fig.7.1.6 after login. It is different to enterprise administrators is that engineers can only view two interfaces: project management and device management.

Project management: only have permission to view project information, but not edit it.

Device management: same as enterprise administrator.

Engineer also can change password in the interface.

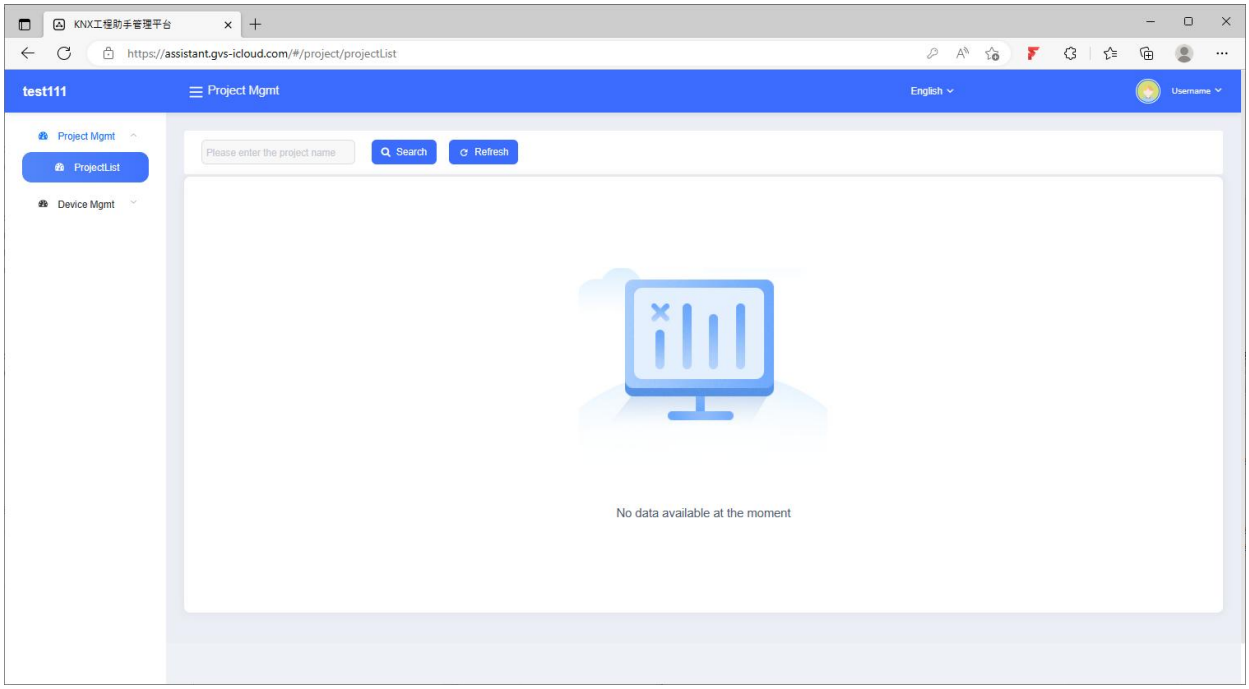


Fig.7.1.6 window after logging

Chapter 8 KNX Project Assistant

KNX Project Assistant is a tool for assisting IP interface to debug KNX program remotely. Connect IP device remotely via local PC, then you can operate a remote debugging and no need to go to the scene.

8.1. Installation

1. **Operation system:** Win7 and above systems;
2. **Operation environment:** Microsoft.NET Framework 4.6.1 and above version are installed on PC.

8.2. Login

Double click [KNX Project Assistant] on desktop or click in turn [Start]->[All programs]->[KNX Project Assistant], then launch the software, enter the login interface as shown as Fig.7.2.

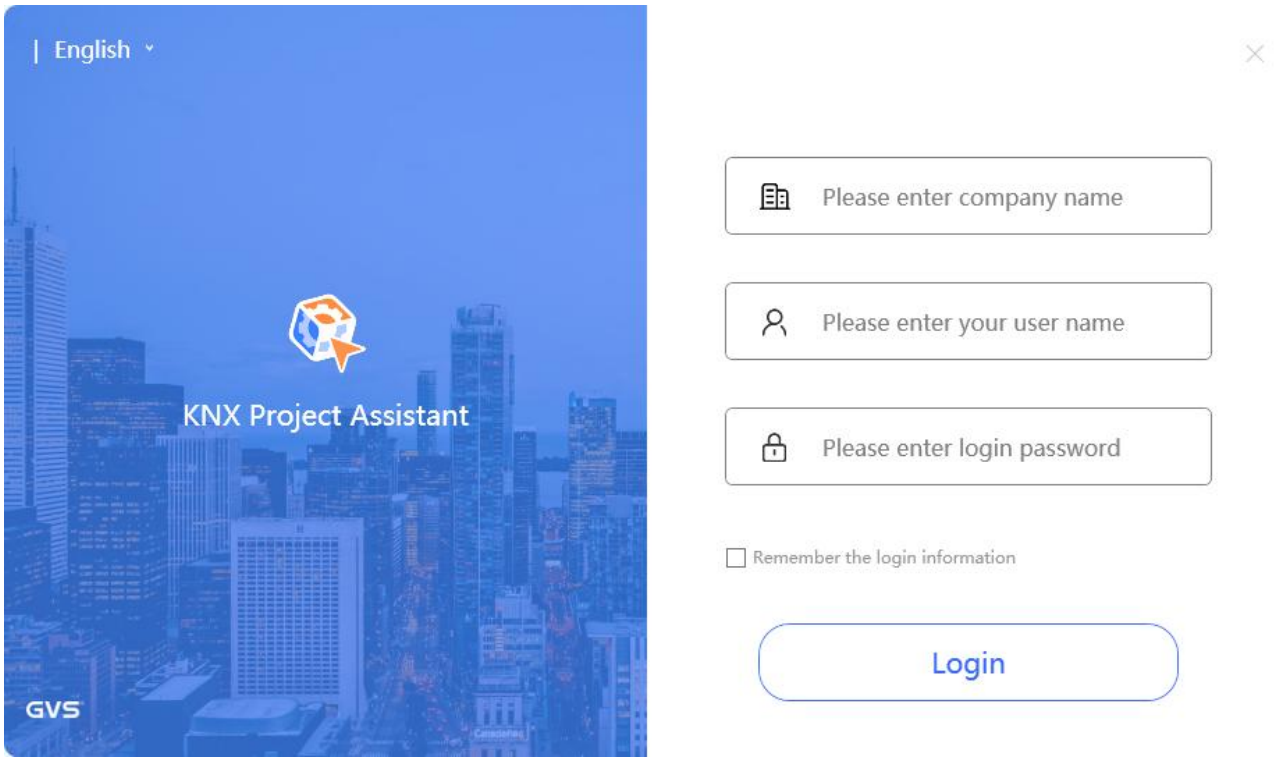


Fig.7.2 Login interface of KNX Project Assistant

Engineer in the enterprise input company name, user name and password to login.

After login successfully, you can operate IP device, such as connect IP device remotely, test the response time and so on.

8.3. Device connection

The interface of device connection as shown as Fig.7.3.1, you can view the online status of all IP device, the connection status and so on.

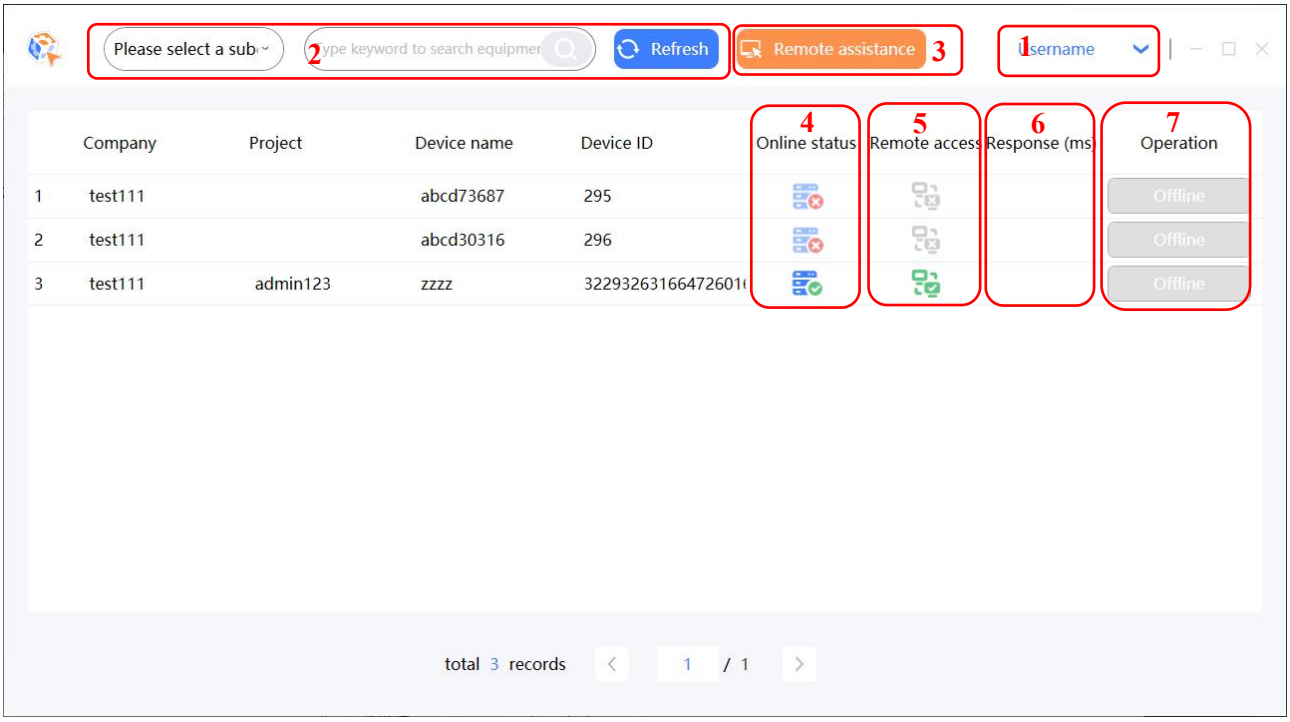


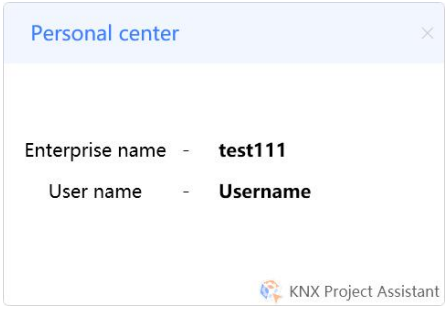
Fig.7.3.1 The interface of device connection

The instructions for the items in the figure are as follows:

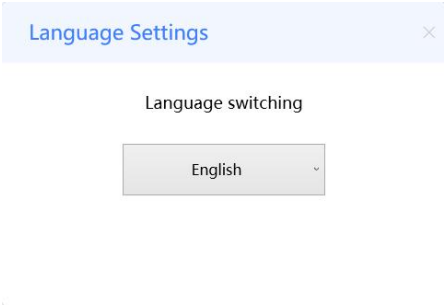
(1) Account information

Click the dropdown menu, you can view / change account information, including personal center, language, about, log out.

①Click “Personal center”, view the enterprise name and user name. As following figure:

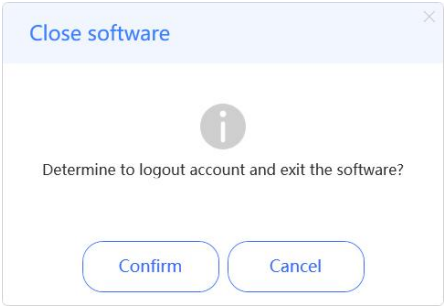


②Click “Language”, change software language. As following figure:



③Click “About”, display manufacturer logo, software version, date and etc., as shown as following figure. Click “Enter page of official website” and then it will jump to GVS official website automatically.

④ Click “Log out”, pop-up a window to confirm again, click “Confirm” and then return to login interface. And also you can click icon × on top right corner to log out. **If the account is login in remotely, and it will be log out in local.**



(2) Search&Sort&Refresh

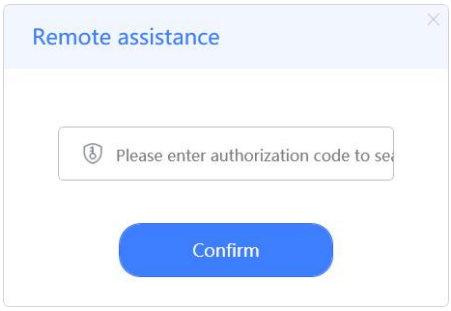
①Search: support search of keywords, such as company name, device name, device ID (complete).

②Select the project to which device belongs.

③Refresh: refresh the interface display when there is update.

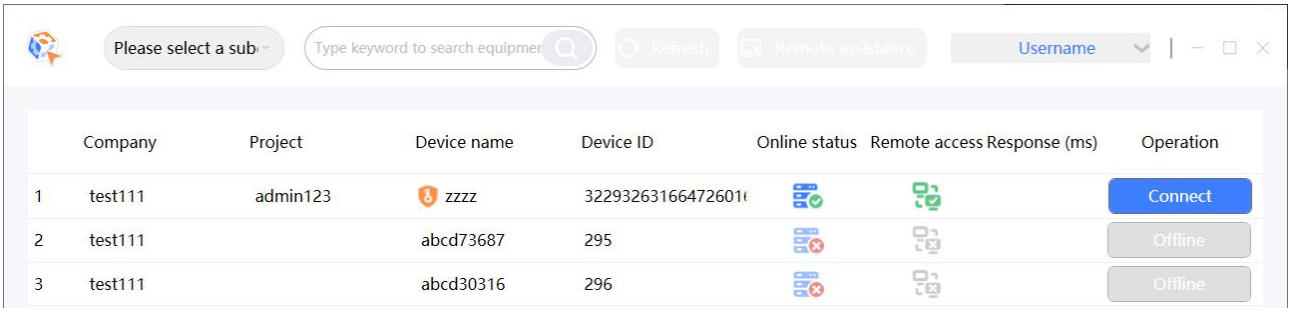
(3) Remote assistance

When other engineers need you to assist with debugging remotely, please click “Remote assistance”, then pop-up a dialog box as following, input authorization code of remote IP device.



Input correct code and confirm, then remote device will be added to list automatically. The left of authorized device name has a icon , the mouse hovers over the icon and display the valid period. When reauthorize code in Device management, current authorized device will be canceled the connection with engineer immediately, not displayed in the list.

The authorized device is a device that other projects or enterprises authorize current engineer to debug via the authorization code. Non-authorized device is belonged to current engineer to debug.



(4) Online status

Device is online or offline status is that device whether connect network normally.

(5) Remote access

Display the remote access status (enable / disable). When it is enabled, you can connect a remote device to debug project remotely; when it is disabled, you can not connect the remote device. **The remote access is enabled by factory default, the access disable can only be done by pressing Cloud button of device, once it has disabled, you can press the button to enable again.**

(6) Response time (ms)

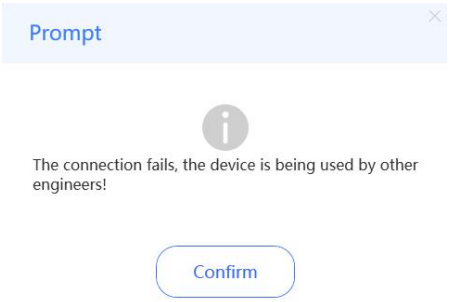
When device is already connected, this row displays delay time between the current and device, as shown as following figure, unit: ms. When below 1000ms, it is green, while 1000ms or above displays red.

(7) Operation

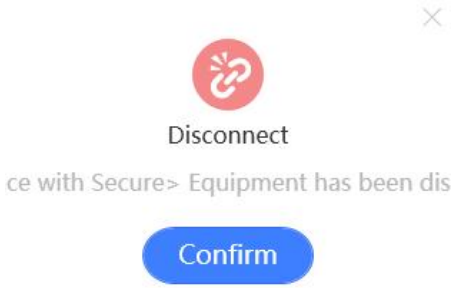
Click “Connect device”, then device is in connecting, display “Disconnect” after device is connected. If device is offline, “Connect device” is gray and can not be operated.

Click “Disconnect”, then disconnect the connection with the device. **If the device is not operated for a long time, it will be disconnected automatically.**

The same device can only be connected by one engineer, the other engineers request a connection will be prompted the device is being used by engineer. As shown as following figure.



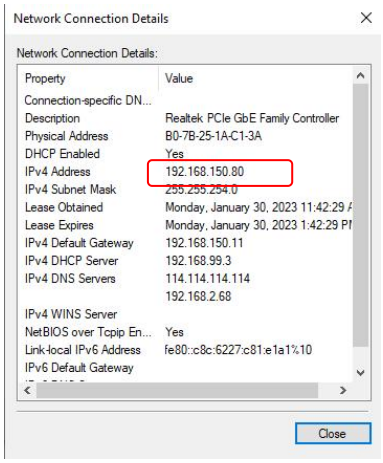
If connection fails, such as network abnormality, connection timeout and etc., it will pop-up following window, now you can not connect the remote devices.

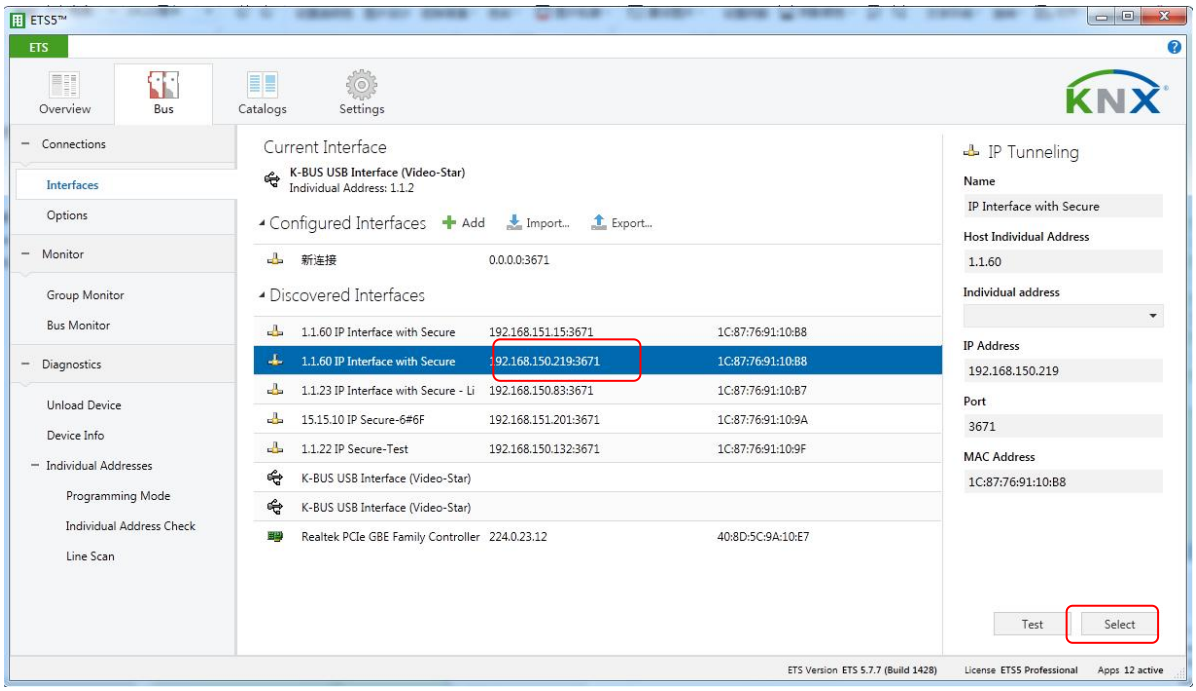


In the same engineer's account, only one device can be connected at anytime, and only the connected device is operable. If you want to change other devices, please disconnect the connected device at first, then connect the required device.

Confirm KNX Project Assistant has been already connected to remote IP device, select IP interface on the ETS5 BUS configuration window. **Note: IP address of remote IP interface will be mapped to IP address of local PC, so when there are multiple IP interfaces on ETS5, you can confirm the connection of remote IP interface by IP address of local PC**, as shown as Fig.7.3.2, after confirming the IP interface, select to connect, then you can debug project remotely via ETS software. **The prerequisite for remote debugging of the device is the physical addresses of the devices in the project are assigned.**

Note: remote debugging interface is built by KNX Project Assistant, therefore, please ensure the software must remain in connecting during remote debugging, that is do not close the software after the connection is established.





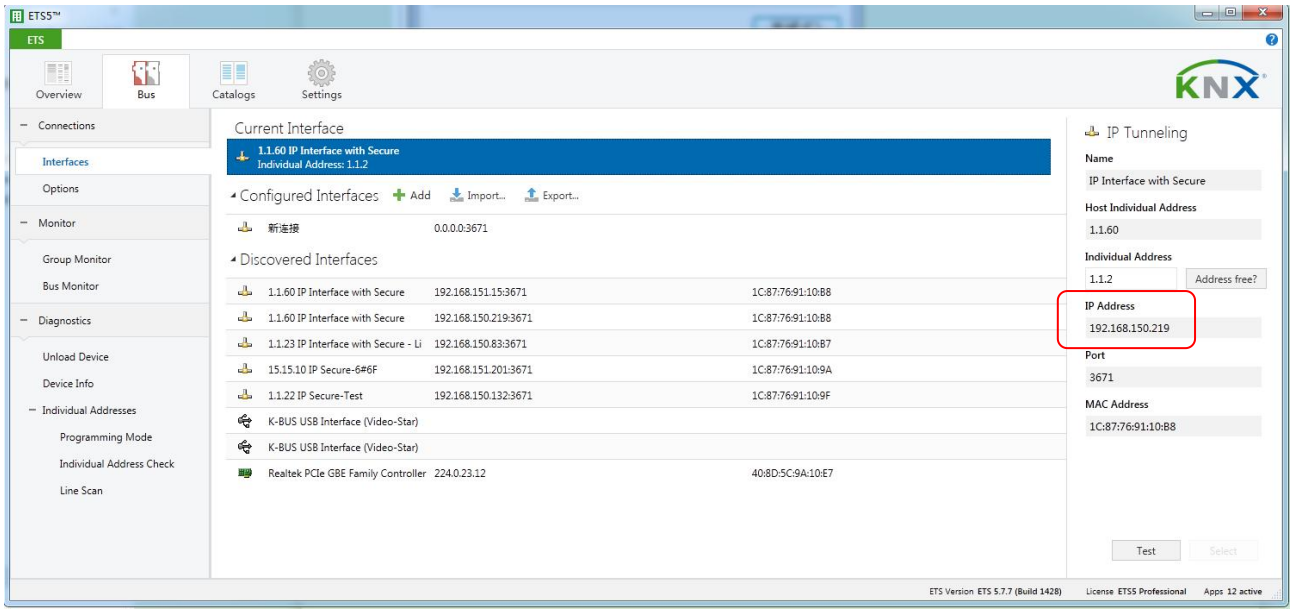


Fig.7.3.2 Remote connection building

Chapter 9 Remote Commissioning Steps

1. After obtaining the product from the manufacturer, check the product for abnormalities.

2. Connect to KNX system, auxiliary supply and network, then check the LED display, confirm power supply, KNX and network are already connected.

3. Configure IP interface via ETS and connect it to the internet, or configure IP address by web configuration, then save and restart the device (ETS configuration details please refer to chapter 3; Web configuration refer to chapter 5, and only KNX secure function is disabled can you configure on website). **Note: IP interface must be accessed to wide area network before remote debugging can be performed, if it is accessed to local area network, only support to local debugging. After accessing to wide area network, enable remote debugging, LAN LED is always ON, if remote connection is abnormal and the LED is double flashing. If remote connection is disable, but only local area network, the LAN LED is single flashing.**

4. Enterprise administrator obtain account from system administrator, please provide related information for system administrator before obtaining an account to build an enterprise administrator account. **System administrator is always a manufacture or organization.**

5. After obtaining the account, login KNX Engineering Assistant Management Platform, build the belonged relationship among project, engineer and device. (Detail please refer to chapter 7). **Note: the company name and project name should be same as the platform, if different, please re-configure.**

6. Engineer obtain account from enterprise administrator, you can login KNX Engineering Assistant Management Platform to manage IP devices of personal project, and also can login KNX Project Assistant to connect IP device, only connect the IP device can you debug remotely (Detail please refer to chapter 8).

7. Open ETS, select a remote debugging interface on the BUS window of ETS.

8. Open ETS project, then you can debug remotely now.