KNX SECURE GUIDE

Table of Contents

1. Introduction

Until now, the data transmitted in a KNX automation installation was open and could be read or manipulated by anyone with sufficient knowledge and access to the KNX medium. Security therefore relied solely on preventing physical access to the KNX bus and to the devices. The new KNX Secure protocols add an additional layer of protection to the communication within a KNX installation in order to prevent such attacks.

Devices that support KNX Secure are able to communicate securely with ETS and with any other secure device, as they incorporate mechanisms for authentication and encryption of the transmitted information.

There are two types of KNX security, which can be implemented simultaneously within the same installation:

- **KNX Data Secure:** secures the communication within a KNX installation.
- **KNX IP Secure:** secures communication via the IP network in KNX installations that use IP communication.

A secure KNX device is a device that provides the basic capability for secure communication, although enabling this capability is not mandatory. An unsecured communication on a secure KNX device behaves the same as communication between devices without KNX Secure support.

The use of security depends on two key settings in the ETS project:

- **Commissioning Security:** Defines whether the communication with ETS shall be secured during commissioning, and enables the activation of runtime security.
- **Runtime Security:** Defines whether communication between devices shall be secured during runtime; in other words, it determines which group addresses are to be secured. To activate runtime security, commissioning security must be enabled beforehand.

The activation of security on KNX Secure devices is optional. When enabled, it is configured individually for each group address, allowing either all or only a subset of the objects to be secured while the remaining ones continue to operate normally with non-secured devices. This means that devices with and without KNX Secure support can coexist within the same installation.

1.1. KNX Data Secure

Its implementation secures the communication between end devices, as KNX Secure devices exchange encrypted telegrams with other devices that also support KNX Secure. Whether the communication is secured or not can be defined individually for each group address.

1.2.KNX IP Secure

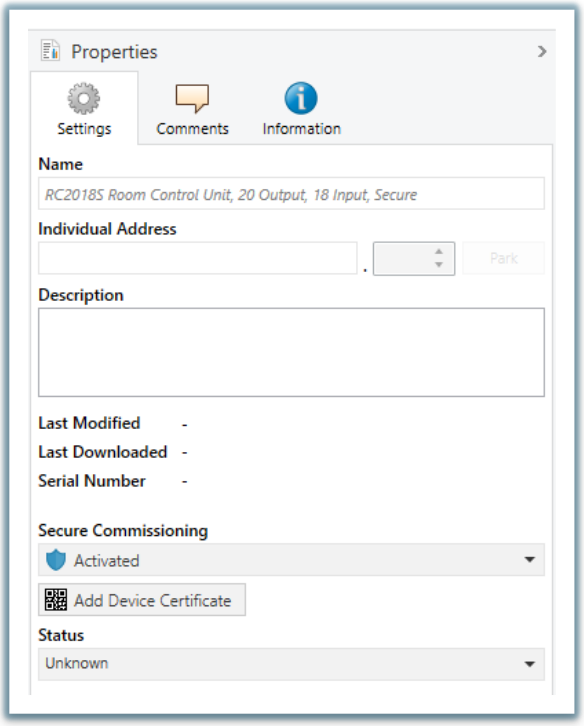
KNX IP Secure is designed for KNX installations that use IP communication. Its implementation ensures the secure exchange of KNX data between systems through secure KNX devices with an IP connection.

This type of security is applied at the bus interfaces and only on the IP medium; that is, secure telegrams are transmitted between secure KNX IP couplers, devices and interfaces. In order to also secure the transmission of telegrams on a main line or sub-line, security must additionally be activated on the KNX bus.

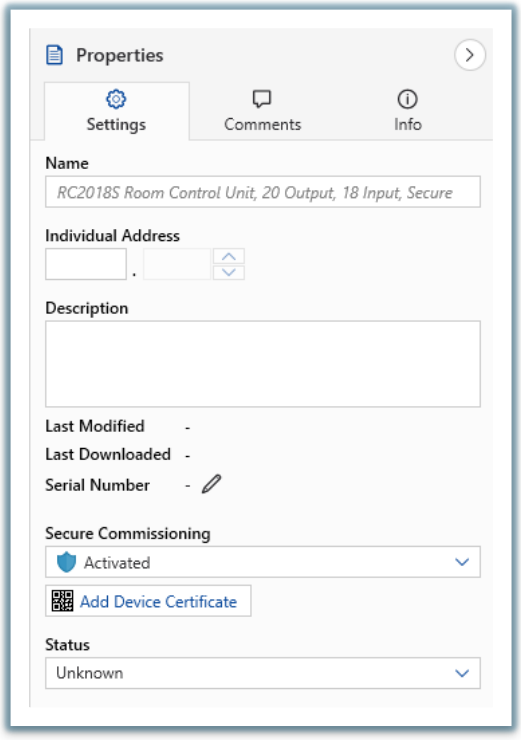
2. KNX Data Secure Configuration

2.1. Secure Commissioning

Secure commissioning can be “Activated/ Deactivated” by the commissioner in the device properties section.



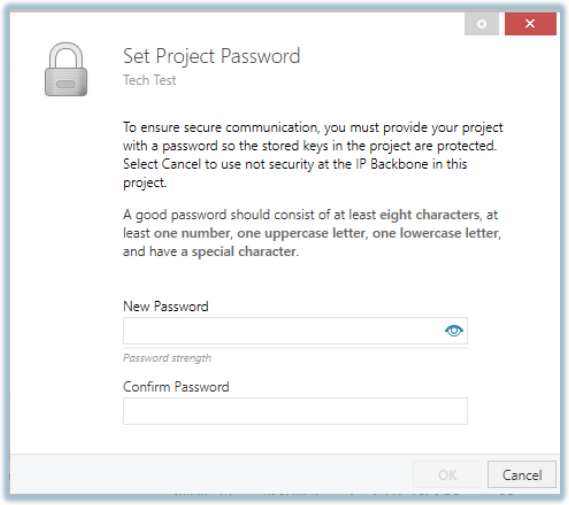
ETS5



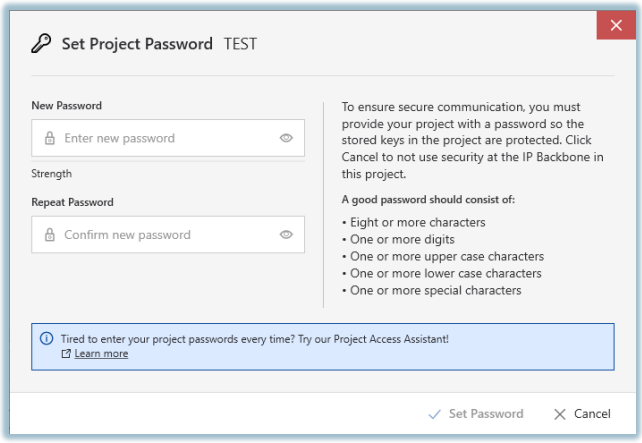
ETS6

2.2. Project Password

If the "*Activated*" option is selected, ETS strictly enforces project password protection as a prerequisite for managing and storing system-wide security keys.

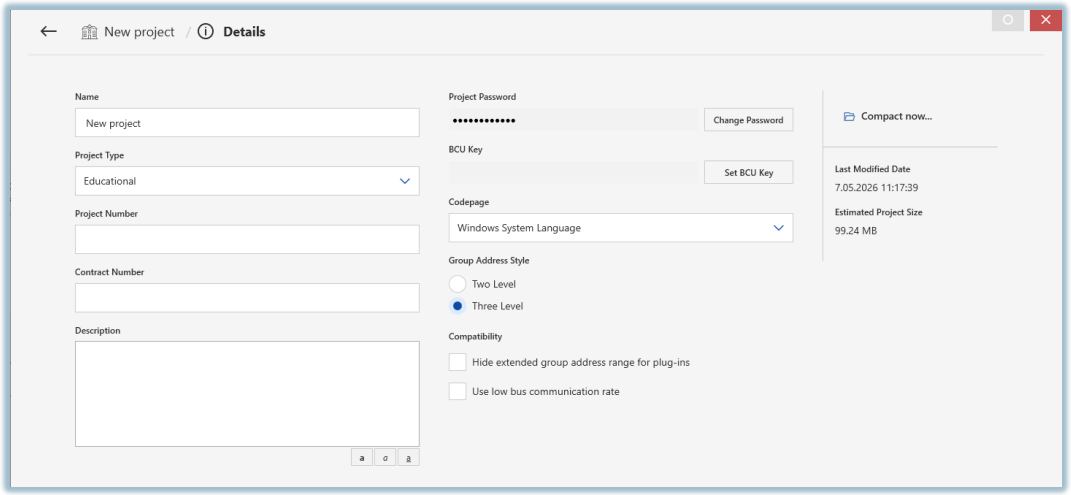


ETS5



ETS6

Alternatively, a project password can be set via the Project Details section on the ETS main dashboard.



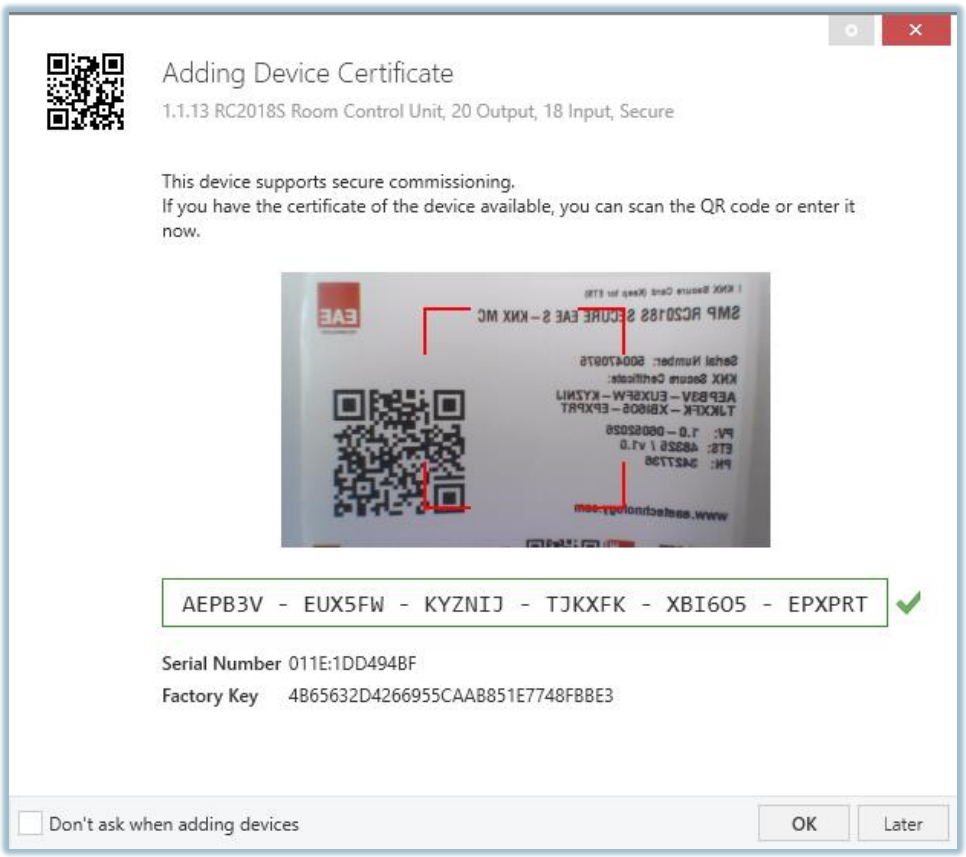
2.3. Device Certificate

When the KNX Secure feature is Active, ETS prompts for a unique device certificate to authorize programming.

KNX Secure devices have secure icons on ETS software's product database, also the devices have label on it. You can check our KNX Secure devices on our website. (www.eaetechnology.com)

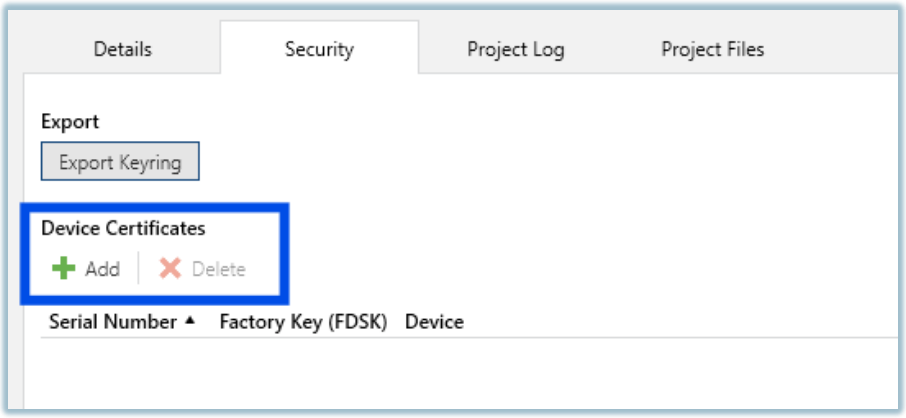
Each device includes a unique **36-character certificate** based on its serial number and FDSK. This authentication data is also formatted as a **QR code** to facilitate rapid scanning and error-free entry.

Serial Code Format : " XXXXXX- XXXXXX- XXXXXX- XXXXXX- XXXXXX- XXXXXX **"**

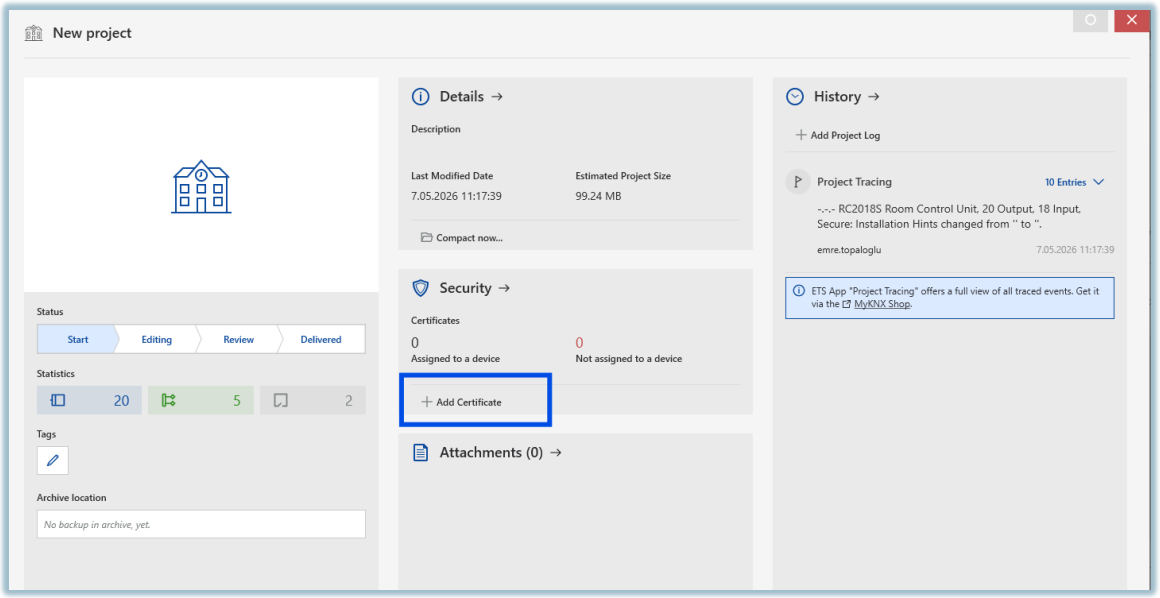


ETS5/ETS6

Alternatively, device certificates can be added via the Project Security section on the ETS main dashboard.



ETS5



ETS6

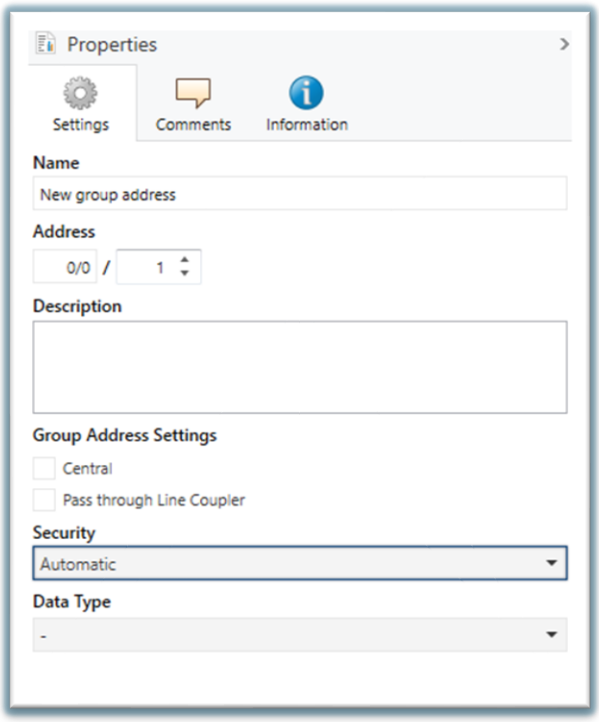
NOTE : During the initial secure commissioning, ETS automatically replaces the Factory Default Setup Key (FDSK) with a unique, randomly generated Tool Key. This "Tool Key" is used for all encrypted communication and configuration updates between the device and ETS and prevents the device from being used in another ETS project.

The “Tool Key” loaded onto the device can be viewed in ETS5/6 under ‘Reports’ -> “Project Certificates.”

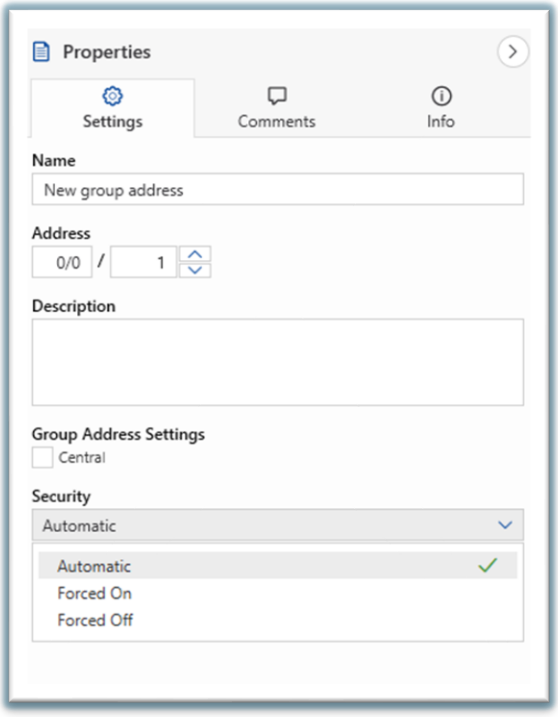
If security mode is enabled for a KNX Secure product and there is no "Tool Key" on the ETS project, the device must be reset to factory settings. A device that has been reset to factory settings must be put back into commission using a QR code or manual code.

2.4. Secure Label Example

2.5. Secure Communication



ETS5



ETS6

- Automatic : ETS enables encryption only if all linked objects are secure-capable. If a non-secure object is added, the GA reverts to "non-secure" mode to ensure compatibility.

- On : Strictly enforces encryption. All linked objects must support KNX Secure. ETS will block any unsecure devices from linking this GA to maintain system integrity.

- Off : Security is disabled. All telegrams are transmitted as unencrypted, even if the linked devices support encryption. This is mainly used for legacy integration.

2.6. Device Security Status In ETS

	Security	Address	Room	Description	Product	Adr Prg Par Grp Cfg	Manufacturer
		2.1.1	2		RC2018S Room Control Unit, 20 Output, 18 Input, Secure	- - - - -	EAE
		2.1.2	2		RC2018S Room Control Unit, 20 Output, 18 Input, Secure	- - - - -	EAE
		2.1.3	2		RC2018 Room Control Unit, 20 Output, 18 Input/2.0	- - - - -	EAE

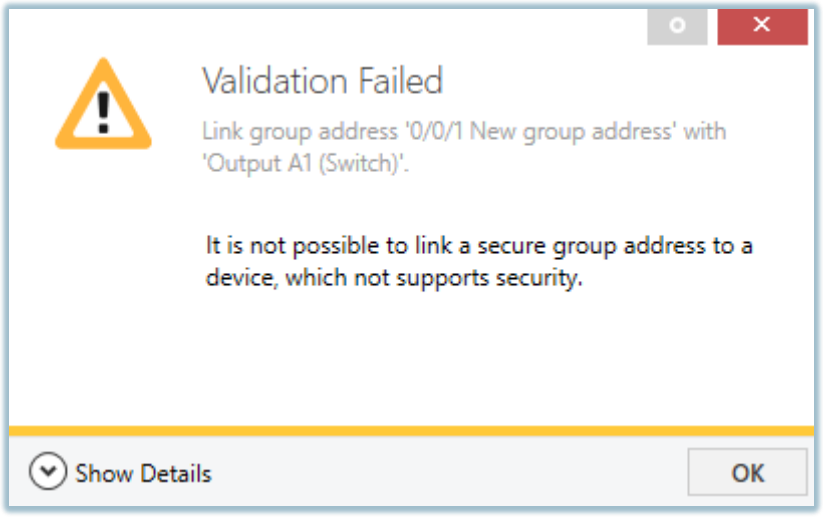
Secure Active (Blue Shield): The device supports KNX Secure and the secure commissioning feature is currently **enabled**.

Secure Inactive (Grey Shield): The device is secure-capable, but the secure commissioning feature is currently **disabled**.

Non-Secure (Empty): The hardware does not support KNX Secure standards. It can only communicate via standard, unencrypted telegrams.

	Security	Address	Name	Description	Central	Pass Throug	Data Type	Length	No. of Associations	Last Value
		0/0/1	New group address		No	No			0	
		0/0/2	New group address		No	No			0	
		0/0/3	New group address		No	No			0	

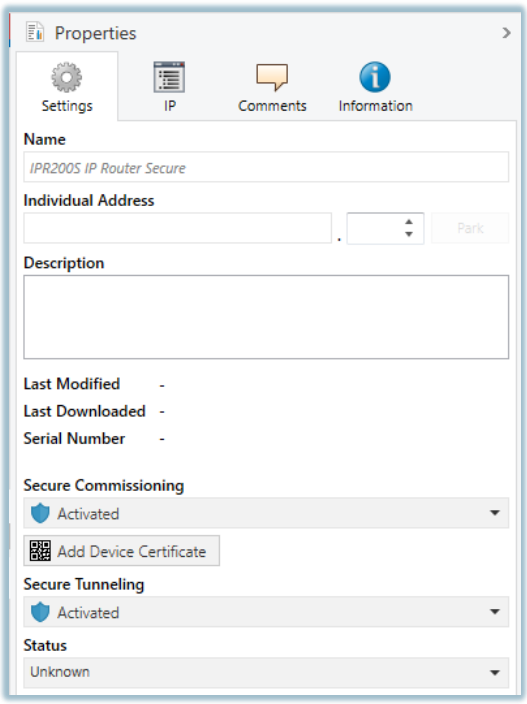
NOTE : To preserve KNX Secure communication, all objects assigned to a Secure Group Address shall only belong to KNX Secure compliant devices.



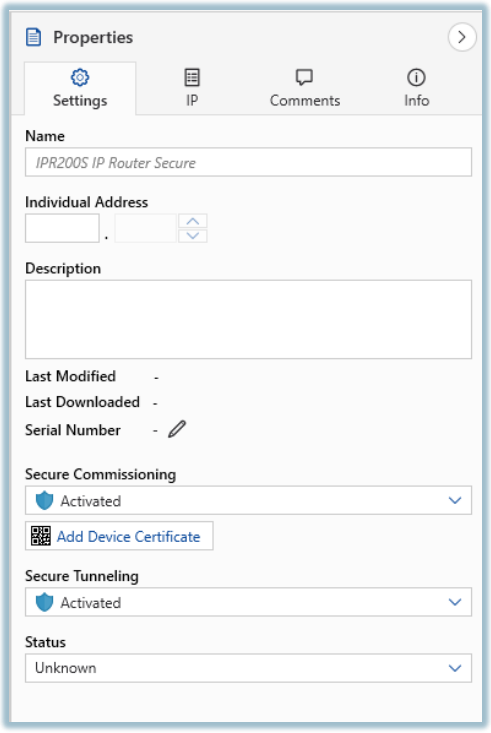
3. KNX IP Secure Configuration

3.1. Secure Commissioning

Secure commissioning can be “Activated/ Deactivated” by the commissioner in the device properties section



ETS5

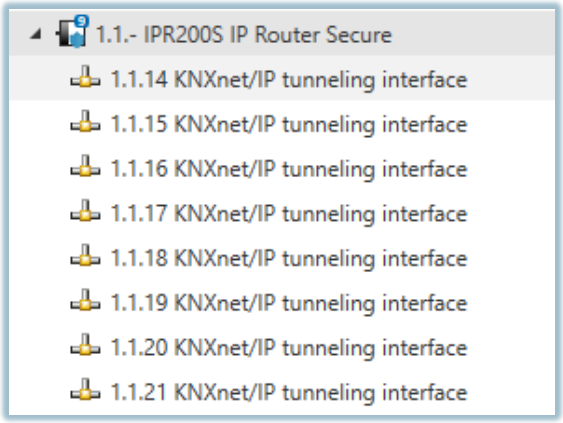


ETS6

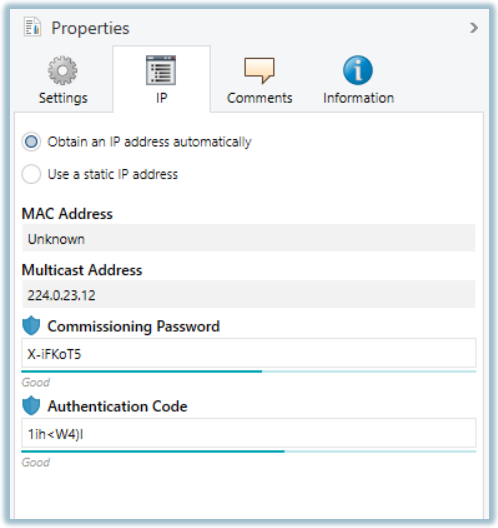
Secure Commissioning : Protects the device configuration process. When active, ETS requires a project password and device certificate to download or modify internal parameters, preventing unauthorized access over the IP network.

Secure Tunneling/Routing : Protects KNX IP tunneling communication. When active, ETS establishes an authenticated and encrypted connection with the device to prevent unauthorized access over the IP network.

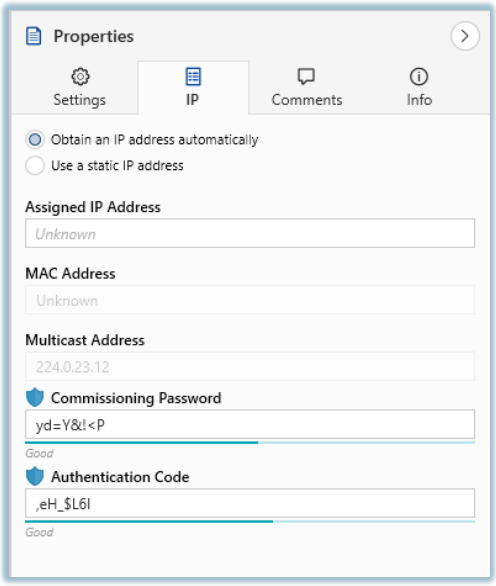
3.2. Commissioning Password and Authentication Code



"The KNX Secure device shown as an example"



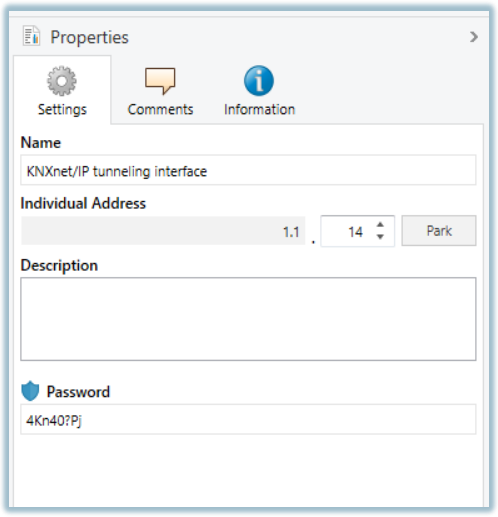
ETS5



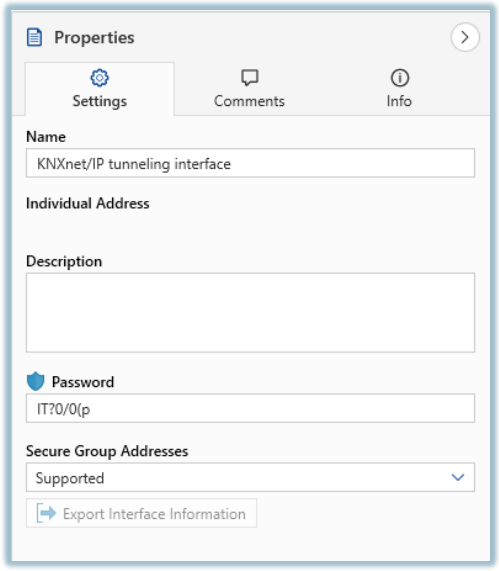
ETS6

The IP tab of the product contains the **Commissioning Password** and **Authentication Code**, which are mandatory for establishing a secure connection. These parameters ensure that only authorized ETS users can access or modify the device over the IP network.

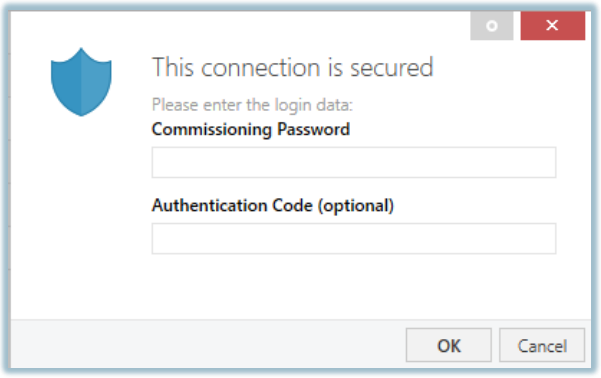
Note: It is recommended that each device uses a unique authentication code, preferably the default code assigned in ETS.



ETS5



ETS6



Commissioning Password

4. Factory Reset

1. Disconnect the “**KNX Bus Connector”** from the device.
2. Press and hold the “**Programming Button”** while the device is still unpowered.
3. **While holding** the” Programming Button”, **reconnect** the KNX bus power to the device.
4. **Continue holding the "Programming Button",** once the “Programming LED” turn on, hold the "Programming Button" for about “5 seconds” until it turns off. The “Programming LED” will turn off after 5 seconds and then turn on again.
5. Release the “Programming Button”, factory reset was performed.

NOTE : The device enters a "Security Disabled" and "Unloaded" state. Since the "Tool Key" is deleted, the device must be commissioned via ETS with the FDSK (Factory Default Setup Key).

5. Observations

1. **Individual Address Modification:** In a secure installation, security keys are uniquely linked to the device's **Individual Address**. Changing the address of a programmed secure device invalidates the existing security link. Consequently, it is mandatory to re-program not only the modified device but also all other secure devices that share group addresses with it to re-establish synchronized encryption keys.
2. **Reprogramming a Reset Device:** When attempting to commission a device following a factory reset, ETS will identify the use of the **FDSK** (Factory Default Setup Key). The software will then prompt for user confirmation to generate a new **Tool Key** required for the reprogramming process.
3. **Unauthorized Project Access Protection**: A device that has been securely commissioned within a project cannot be downloaded to or accessed from a different ETS project. To reuse such a device in another project, the original ETS project file must be available, or a manual factory reset must be performed in order to clear the existing security certificates.
4. **BCU Key :** This key is lost either by manual factory reset or by unloading.