KNX Secure Guide

User manual edition: b

www.zennio.com

USER MANUAL

CONTENTS

DOCUMENT UPDATES

Version	Changes	Page(s)
b	Added instructions for performing a factory reset.	

1 INTRODUCTION

So far, the data transmitted in a KNX automation installation was open and could be read and manipulated by anyone with some knowledge with access to the KNX medium, so that security is guaranteed by preventing access to the KNX bus or to the devices. The new KNX Secure protocols add additional security to the communications in a KNX installation to prevent such kind of attacks.

Devices with KNX secure will be able to communicate securely with ETS and any other secure device, as they will incorporate system for authentication and encryption of the information.

There are two types of KNX security that can be implemented simultaneously in the same installation:

- **KNX Data Secure:** secures the communication within a KNX installation.
- **KNX IP Secure:** for KNX installations with IP communication, secures communication via IP network.

A secure KNX device refers to a device that has the basic capability to enable secure communication, although it is not always required to do so. An unsecured communication on secured KNX devices is equal to communication established between devices without KNX security.

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

- Commissioning security: sets whether, during the commissioning, the communication with ETS should be secure or not and opens up the possibility of activating the runtime security.
- Runtime security: sets whether during runtime, communication between devices should be secure or not. In other words, it determines which group addresses are to be secure. In order to activate the security during runtime, the commissioning security must be activated.

The activation of security on KNX Secure devices is optional. If it is activated, it is set individually in the group addresses, so that all or only a part of the objects can be secured, while the rest can function normally with non-secured devices. In other words, devices with and without KNX Secure can coexist in the same installation.

2 CONFIGURATION

From ETS version 5.7 onwards, the use of KNX security and all its functionalities to work with secure devices is enabled.

In this section a guide for the configuration of KNX secure in ETS projects is presented.

2.1 KNX DATA SECURE

Its implementation ensures communication between end devices. Secure KNX devices will transmit encrypted telegrams to other devices that also have KNX secure.

It will be possible to choose for each group address, whether the communication will be secure or not.

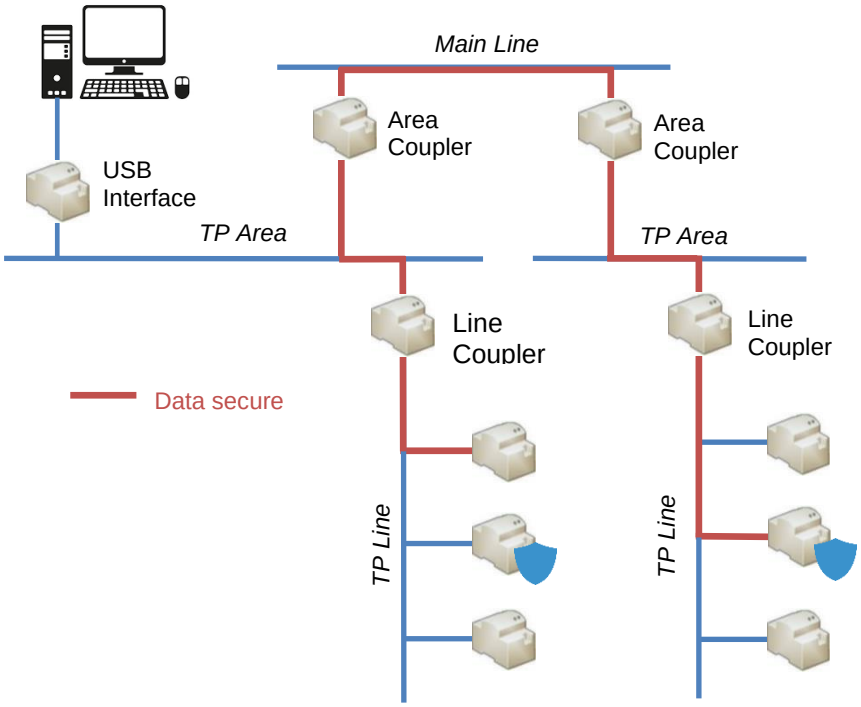

Figure 1. KNX data secure scheme.

2.1.1 SECURE COMMISSIONING

When a device has a secure commissioning, the communication between ETS and the device will be carried out in safe mode.

A device should have a secure commissioning configured whenever there is runtime security, i.e. one of its objects is associated to a safe group address (see section 2.1.2).

Note: *Please note that the presence of a secure device within an ETS project, implies the protection of the project itself with a password.*

ETS PARAMETERISATION

The secure commissioning can be set from the "Configuration" tab in the "Properties" window of the device.

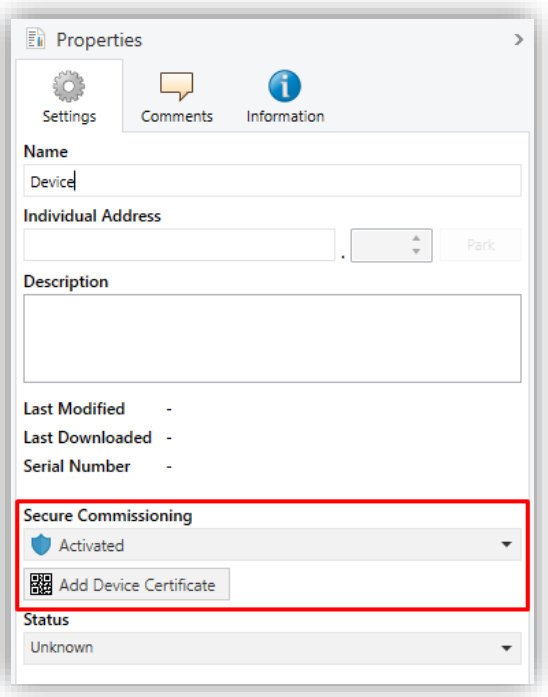

Figure 2. KNX Data Secure – Secure Commissioning.

- **Secure Commissioning** [*Activated / Deactivated*]: enables to choose whether ETS should communicate with the device in safe mode or not, i.e. to enable or disable KNX secure on the device.

  If the "*Activated*" option is selected, it will be mandatory to have a **password for the project**.

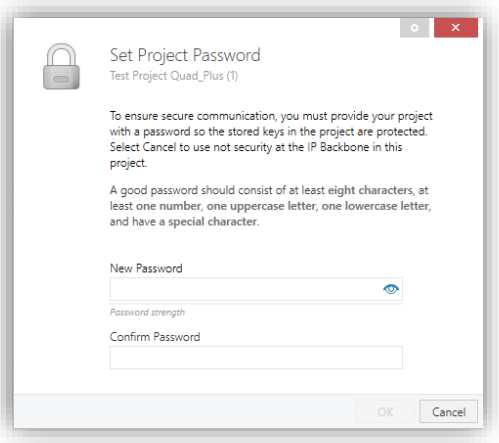

Figure 3. Project – Set Password.

An additional way to set a password on a project is through the main window ("Overview") of ETS. When selecting the project, a section will be displayed on the right side where, under "Details", the desired password can be entered.

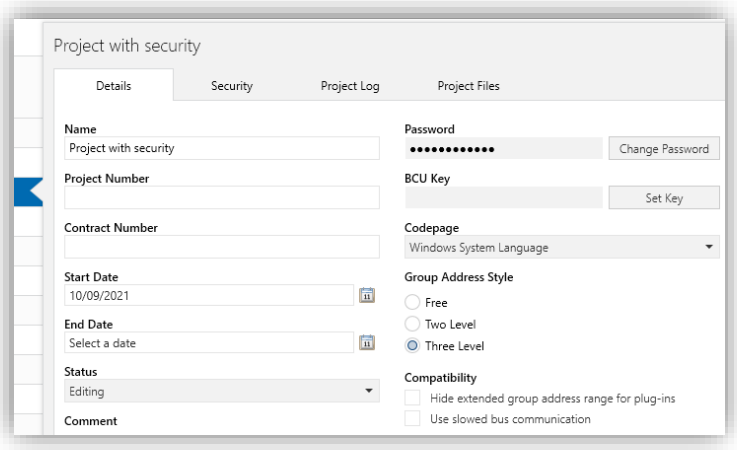

Figure 4. ETS - Device password.

- **Add Device Certificate:** If **secure commissioning** is "*Activated*", ETS will, in addition to the password, request a unique certificate for the device.

  The **certificate** to be added [*xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx*] consists of 36 alphanumeric characters generated from the serial number and the FDSK (*Factory Default Setup Key*) of the device. It is included with the device and contains the corresponding QR code for easy scanning.

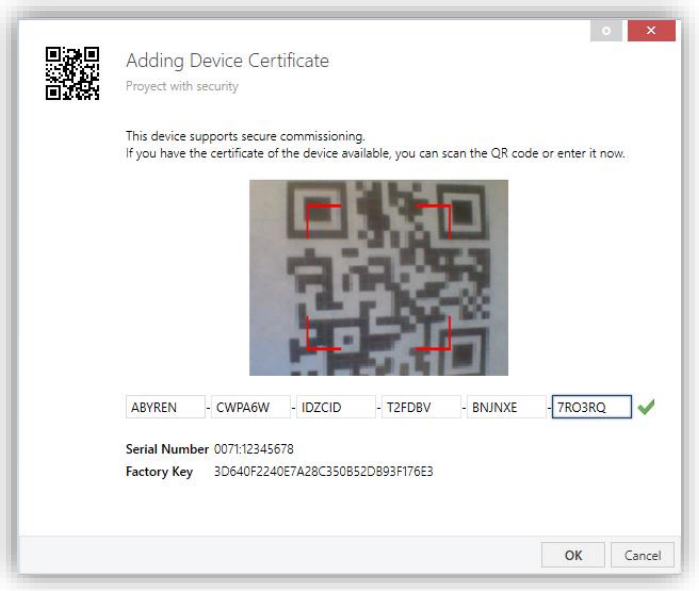

Figure 5. Project – Add Device Certificate.

Device certificate can also be added from the main ETS window ("Overview"), by accessing the "Security" section of the new window displayed on the right side when selecting the project.

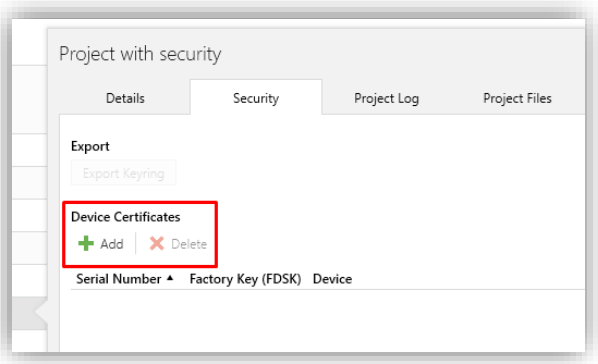

Figure 6. ETS – Add device certificate.

During the first secure commissioning, ETS replaces the FDSK of the device with a new key (*Tool Key*) that is generated individually for each device.

If the project is lost, all tool keys will be lost with it, therefore, the devices cannot be reprogrammed. In order to be able to recover them, the FDSK must be reset.

The FDSK can be restored in two ways: after an unloading, provided that it is performed from the project in which the first commissioning was carried out, or after a manual factory reset (see section 3).

2.1.2 SECURE GROUP COMMUNICATION

Each object of a secure device can transmit its information in encrypted form, thus establishing security in communication or operation.

For an object to have KNX security, it has to be configured from the group address itself, i.e. the address to which the object will be associated.

ETS PARAMETERISATION

The communication security settings are defined from the "Configuration" sub-tab in the "Properties" window of the group address.

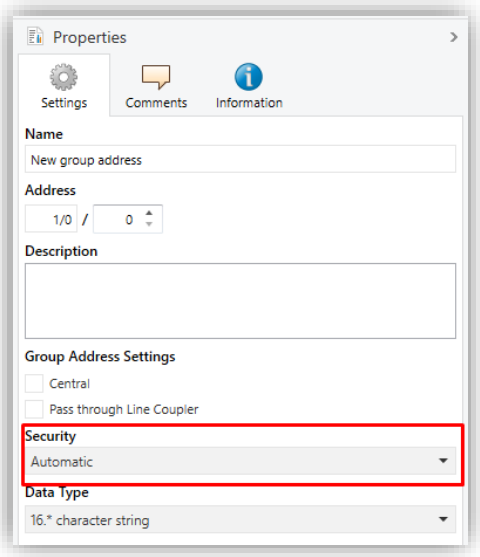

Figure 7. KNX Data Secure – Group Address Security.

- **Security** [*Automatic / On / Off*]: in "Automatic" setting, ETS decides whether encryption is activated if the two linked objects can communicate securely.

  Notes:

  - *All object linked to a **secure group address** shall be **secure objects**.*
  - *Same device can have both secure and non-secure group address.*

Secure Objects can be identified with a "blue shield".

Security	Number	Name	Object Function	Description	Group Address	Length	C	R	W	T	U	Data Type	Priority
	2	[Access] Open Door	1 = Open Door	[Access] Open Door	0/0/4	1 bit	C	-	W	-	-	acknowledge	Low
	4	[Access] Lock Serial Channel	0 = Unlock; 1 = Lock	[Access] Lock Serial Channel	0/0/5	1 bit	C	-	W	-	-	enable	Low
	5	[Access] Lock Opening Object	0 = Unlock; 1 = Lock	[Access] Lock Opening Object	0/0/6	1 bit	C	-	W	-	-	enable	Low

Figure 8. Secure Object.

2.2 KNX IP SECURE

KNX IP security is designed for KNX installations with IP communication. Its implementation ensures the secure exchange of KNX data between systems via secure KNX devices with IP connection.

This type of security is applied on bus interfaces and only in the IP medium, i.e. secure telegrams are transmitted between secure KNX IP couplers, devices and interfaces.

In order for the transmission of telegrams on a main line or sub-line to also be secure, security must be activated on the KNX bus (see section 2.1).

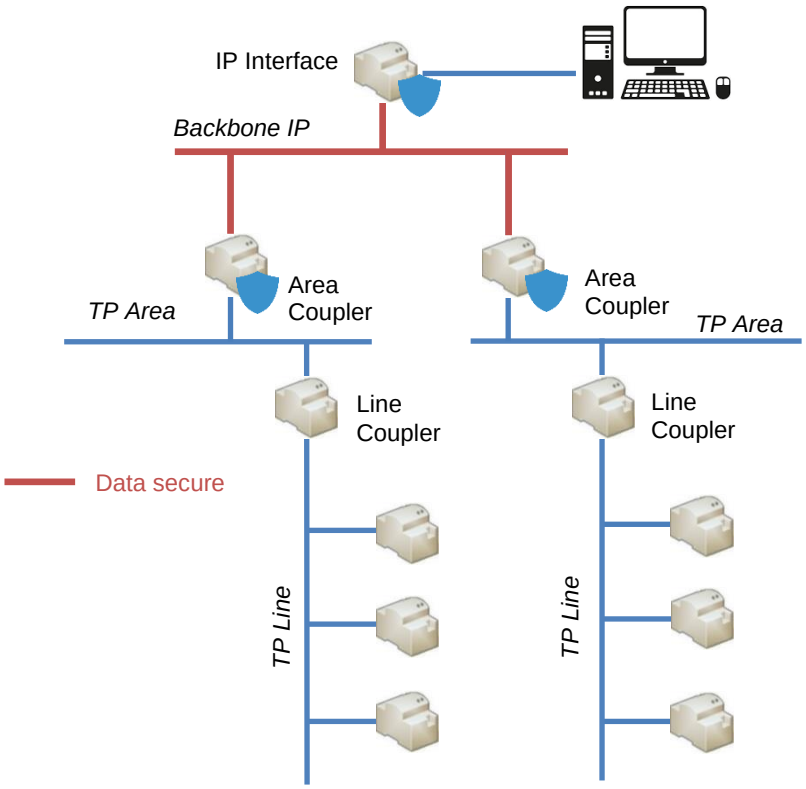

Figure 9. KNX IP Secure scheme

2.2.1 SECURE COMMISSIONING

In this type of security, in addition to secure commissioning in section 1.1.1, "Secure Tunneling" can also be activated. This parameter can be found in the "Settings" tab of the device properties window on the right-hand side of the ETS screen.

ETS PARAMETERISATION

The commissioning and tunneling security settings are defined from the "Configuration" tab in the "Properties" window of the device.

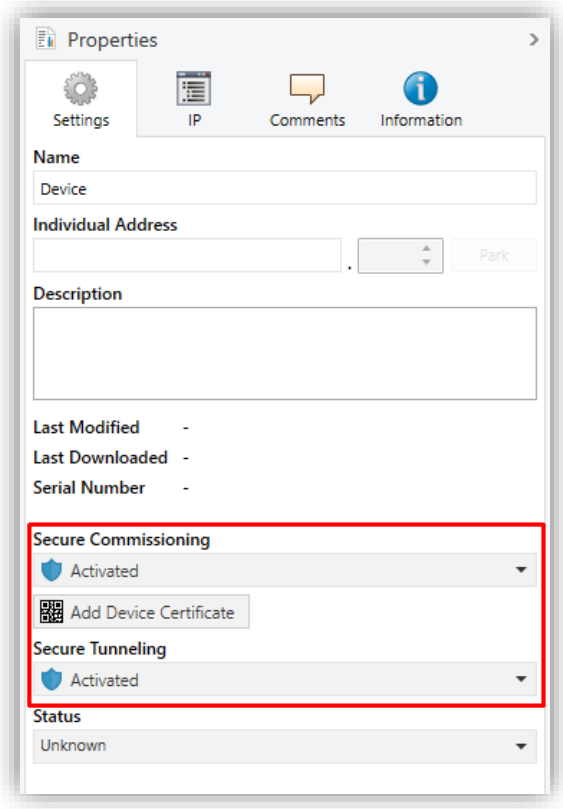

Figure 10. KNX IP Secure - Secure Commissioning and Tunneling.

In addition to **Secure Commissioning** and the button **Add Device Certificate**, previously explained on section 2.1.1, will also appear:

- **Secure Tunneling** [*Enabled / Disabled*]: parameter only available if secure commissioning is enabled. If this property is "Enabled", the data transmitted through the tunnel connections will be secure, i.e. the information will be encrypted through the IP medium. Each tunnel address will have its own password.

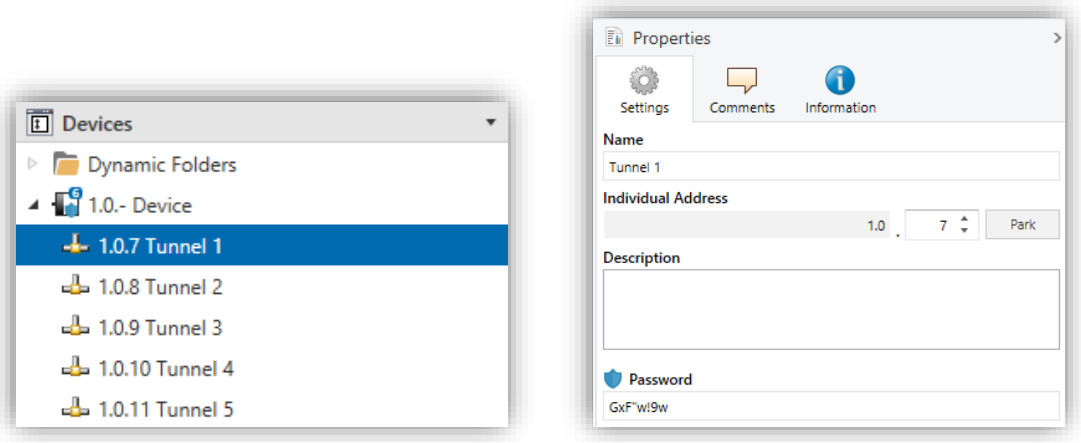

Figure 11. Tunneling Address Password.

The IP tab of the product also contains the **Commissioning Password** and the **Authentication Code**, which are required to make any secure connection to the device.

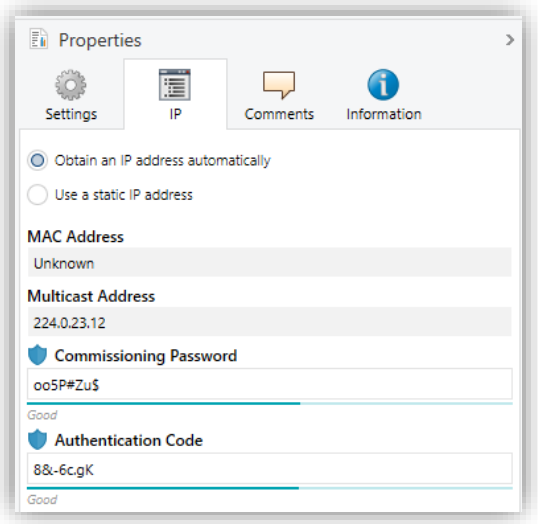

Figure 12. Commissioning Password and Authentication Code.

Note: *It is recommended that the authentication code for each device be individual (and preferably the default set in ETS)*.

The commissioning password will be requested when the IP Interface is selected in ETS to connect to it (the authentication code is optional):

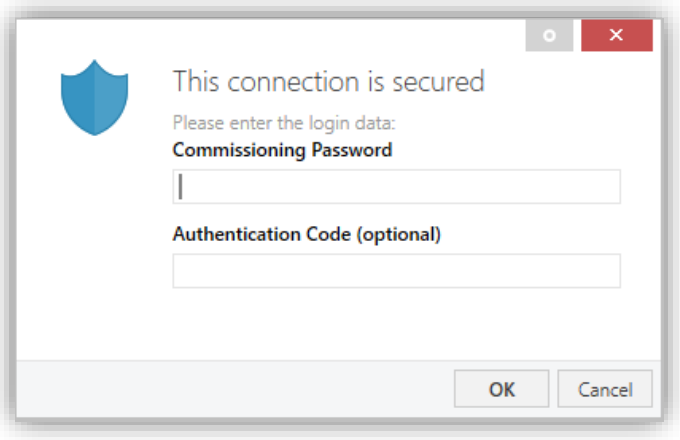

Figure 13. Request for Commissioning Password when selecting a secure IP Interface.

3 FACTORY RESET

To prevent a device from becoming unusable in the event of losing the project and/or the Tool Key with which it is programmed, it is possible to return it to the factory state restoring the FDSK by following the steps below:

1. Put the device in safe mode. This is achieved by powering it up with the programming button pressed until the programming LED flashes.
2. Release the programming button. It keeps flashing.
3. Press the programming button for 10 seconds. While pressing the button, it lights in red. The reset occurs when the LED turns off momentarily.

This process, apart from the Tool Key, also deletes the BCU password and resets the individual address to the value 15.15.255.

An unload of the application program also deletes the Tool Key and the BCU password, although in this case the ETS project with which it was programmed is required.

4 OBSERVATIONS

Some considerations for the use of KNX security:

- **Individual address change:** in a project with several already programmed secure devices that share group addresses between them, changing the individual address in one of them makes it necessary to program the rest of the devices that share group addresses with it.

- **Programming a reset device:** when trying to program a factory reset device, ETS detects that the *FDSK* is being used and asks for confirmation to generate a new *Tool Key* in order to reprogram the device.

- **Device programmed in another project:** if you try to download a device (safely or not) that has already been safely programmed in another project, you will not be able to download it. You will have to recover the original project or perform a factory reset.

- **BCU key:** this password is lost either by manual factory reset or by unloading.

Join and send us your inquiries about Zennio devices:

https://support.zennio.com

Zennio Avance y Tecnología S.L.
C/ Río Jarama, 132. Nave P-8.11
45007 Toledo. Spain

Tel. +34 925 232 002

www.zennio.com
info@zennio.com