

KNX SECURE

ETS USER MANUAL

CONTENTS

1 KNX SECURITY 3
2 SECURITY ON THE KNX BUS 4
2.1 SECURE COMMISSIONING 5
2.1.1 PROJECT PASSWORD 6
2.1.2 DEVICE CERTIFICATE 7
2.2 SECURE GROUP COMMUNICATION 8
3 KNX IP SECURE 9
3.1 SECURE COMMISSIONING AND TUNNELLING 10
3.2 CREDENTIALS AND INTERFACE CONNECTION 11
3.3 ROUTING AND EXTERNAL CLIENTS 12
4 FACTORY RESET 13
5 NOTES 14

1 KNX SECURITY

This manual describes how to commission DINUY devices that support KNX Secure and protect their communications. Prepare the project, enable secure commissioning, add the certificates and download the configuration. For IP Secure devices, also configure access and, where applicable, routing security.

Before starting, check the Secure functions supported by the DINUY product and its application program. Import the correct product file and use a compatible version of ETS. The screenshots show ETS 6.3 in English; the layout and some labels may vary between versions.

Which security to configure

- **KNX Data Secure:** protects group data between compatible devices, including across different KNX media. It is configured through secure commissioning of the device and the security of the group addresses linked to its objects.
- **KNX IP Secure:** protects tunnelling access or routing communication on the IP segment. It does not automatically enable Data Secure on TP lines. Both mechanisms can be used together.

Workflow

1. **Prepare the device:** add it to the project, check the product and assign a unique individual address.

2. **Enable secure commissioning:** select the setting in the device properties.

3. **Set the project password:** complete the ETS prompt and keep the password safe.

4. **Add the certificate:** scan the QR code or enter the code supplied with that device.

5. **Configure the groups:** link the objects and select the security of each group address.

6. **Download and test:** download the affected devices and test the configured functions.

Secure commissioning protects programming access from ETS. Security during operation is configured separately: on group addresses for Data Secure and on the tunnel or IP medium for IP Secure. Enabling a single setting does not complete the whole configuration.

2 SECURITY ON THE KNX BUS

Figure 1 shows a protected function between two KNX Data Secure devices. All participants must be compatible. The programming interface and the couplers along the path must support the extended frames required both during download and during operation.

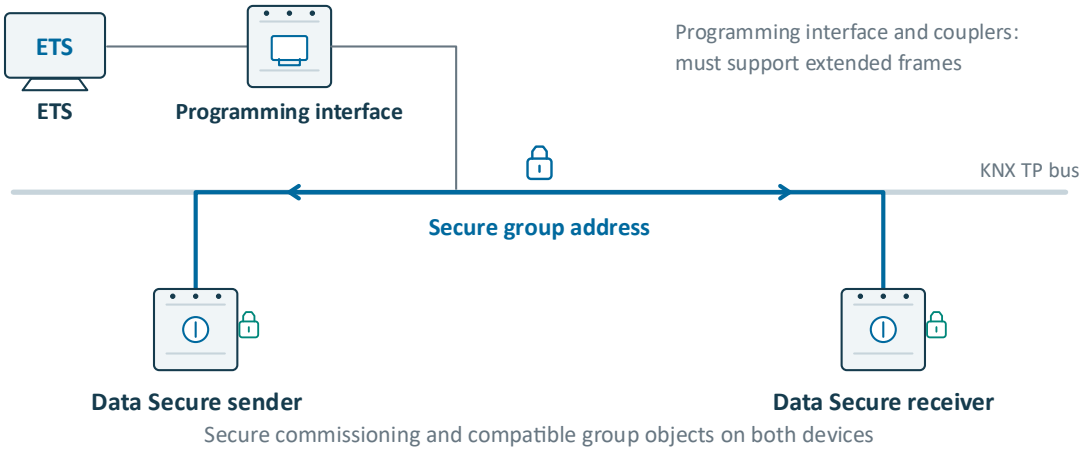


Figure 1. Installation diagram with KNX Data Secure devices

Preparing the project

1. **Add the DINUY devices** from the catalogue and identify their location and product reference.

2. **Assign individual addresses** according to the installation topology.

3. **Locate each device certificate** before downloading. Keep a record linking the label, serial number and installed device.

Keep the certificates safe: record the serial number and location of each device. Do not publish QR codes or factory keys in drawings available to general users.

4. **Select the ETS connection** that reaches the line. Check that the interface and every intermediate coupler support extended frames; support for Secure in the end devices alone is not enough.

Continue by enabling secure commissioning in the device properties.

2.1 SECURE COMMISSIONING

1. **Select the DINUY device** in the project.

2. Open the "**Properties**" panel and the "**Settings**" tab.

3. Open the "**Secure Commissioning**" list and select "**Activated**". Figure 2 shows the setting to select; the change still needs to be downloaded to the device.

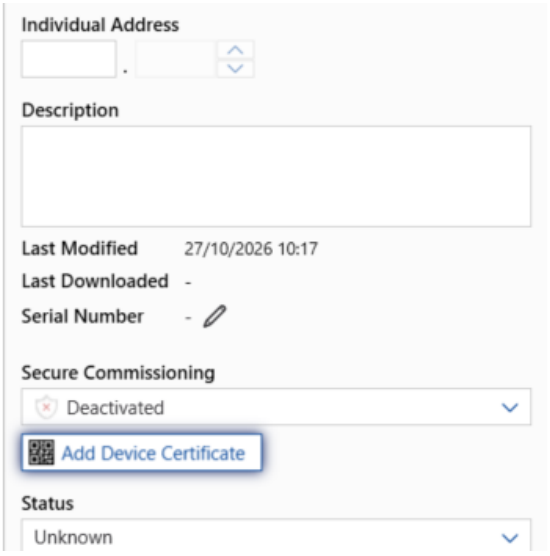


Figure 2. Selecting secure commissioning in the device properties

4. If ETS prompts you to protect the project, set its password as explained in section 2.1.1. A password is required to add certificates and use KNX Secure.

5. Click "**Add Device Certificate**" and add the certificate for that device, as described in section 2.1.2.

Expected result: secure commissioning is enabled in the project and the device has its certificate assigned. The configuration must be downloaded to the device to complete commissioning.

If the setting is not displayed, check that the correct device is selected and its application supports KNX Secure. If a product allows unsecured operation and "**Deactivated**" is selected, that configuration cannot participate in protected group communication requiring Data Secure.

2.1.1 PROJECT PASSWORD

When ETS displays the window in Figure 3, enter a project password in "**New Password**" and enter it again in the confirmation field. Follow the requirements shown in the window and confirm.

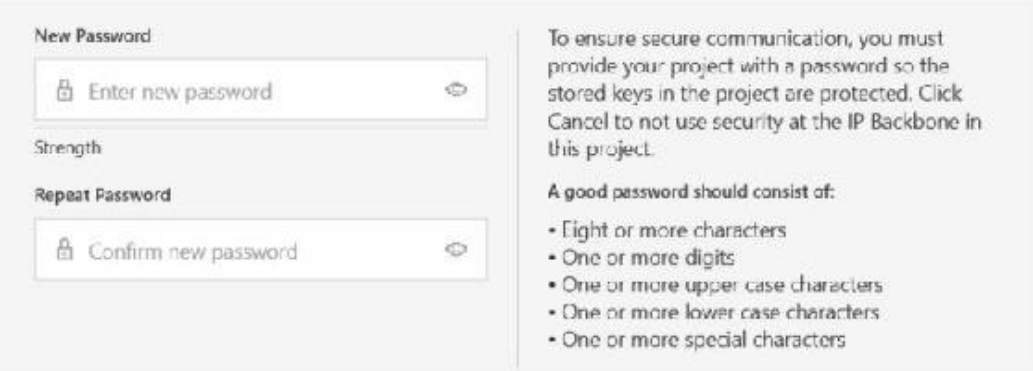


Figure 3. Prompt to set the project password

Alternative route: open the project details from the overview. Under "**Details**", use the password option. Figure 4 identifies the entry point to that section; the password is set on the next screen.

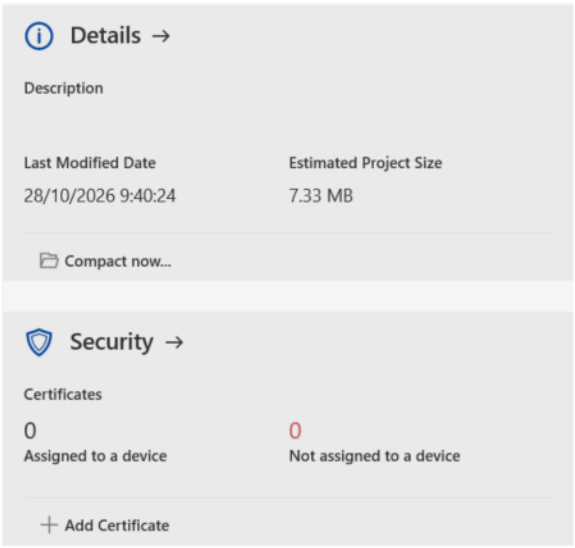


Figure 4. Accessing the project details from the overview

Expected result: the project is protected and ETS allows you to continue adding certificates and configuring Secure.

Keep the password with an unambiguous project identifier and provide it to the authorised person through a secure channel. This password opens the project; it is not the password of an IP interface or a tunnelling address.

2.1.2 DEVICE CERTIFICATE

1. In the device properties, click "**Add Device Certificate**".

2. **Using a QR code:** hold the label in front of the selected camera and position the code within the scanning area.

3. **Manual entry:** enter the certificate code in the six blocks of six characters. ETS uses 36 Base32 characters and does not accept the digits 0 and 1. Copy the complete code from the label; the serial number alone is not the certificate.

4. Check that ETS recognises the certificate and that its serial number matches the installed device. Confirm the addition.

If ETS rejects the code: check the transcription, the complete QR scan and the serial number. If the certificate is already assigned to another device, check that assignment before accepting a reassignment.

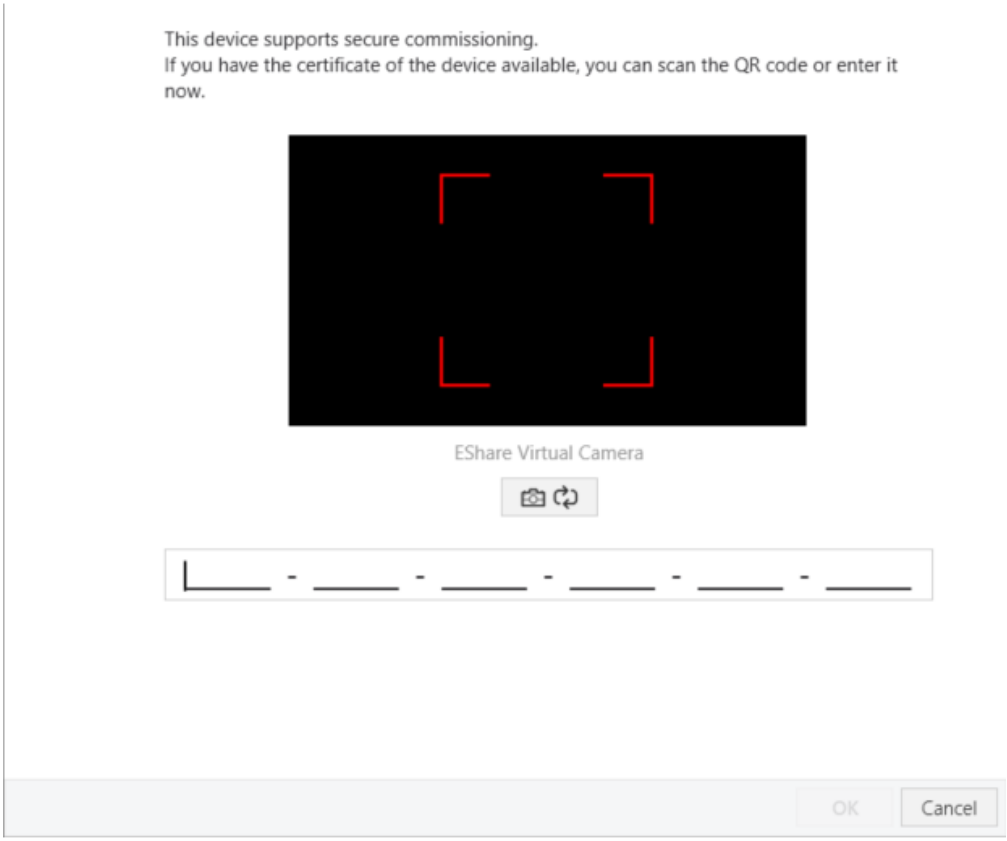


Figure 5. Scanning the QR code or entering the certificate

After the first secure download: ETS establishes the operational keys; in Data Secure, the programming key is called the Tool Key. The certificate contains the Factory Default Setup Key (FDSK), which must be kept for device recovery after a factory reset. The certificate does not replace the project with its current keys.

2.2 SECURE GROUP COMMUNICATION

1. Create or select the group address and link the objects involved in the function.

2. Select that address and open "**Properties**" > "**Settings**".

3. Locate "**Security**" and select the appropriate setting, as shown in Figure 6.

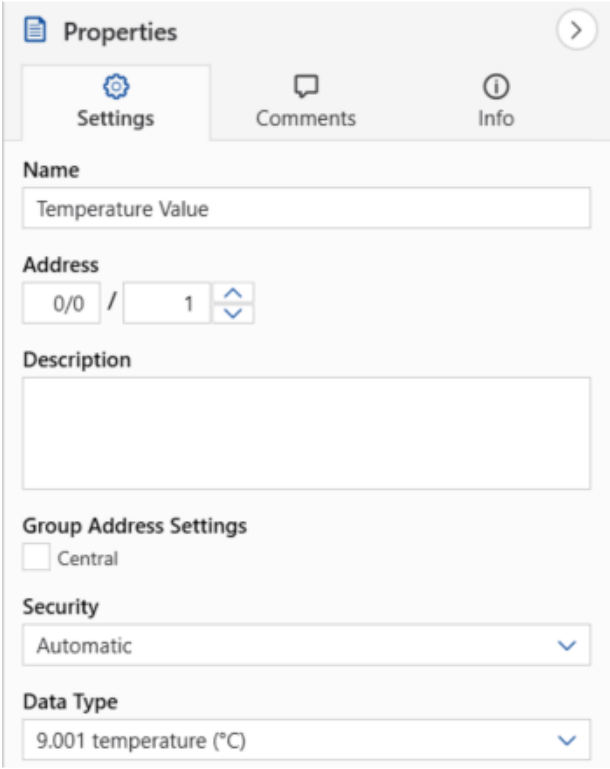


Figure 6. Security of a group address

- "**Automatic**": ETS determines the security from the linked objects. Check the effective state after adding or changing participants.
- "**On**" or "**Activated**", depending on the version: requests secure communication. All linked objects must support it and their devices must have secure commissioning enabled. Resolve any incompatibility reported by ETS before downloading.
- "**Off**" or "**Deactivated**": the address operates without Data Secure, where the application allows this option.

4. **Download the configuration:** select the devices and open "**Download**". During initial commissioning, download the individual address and application. Press the programming button only when ETS prompts you. Wait for completion and check the download flags; also update the affected participants and couplers.

5. **Test the command and its status** between the actual participants. A device may have secure and conventional functions on different objects. A single object cannot combine secure and unsecured group addresses: check all its associations, including receiving addresses.

3 KNX IP SECURE

Use this procedure when the DINUY device supports KNX IP Secure. Distinguish the functions: tunnelling connects ETS or a client to an interface; routing connects lines through routers. A tunnelling interface cannot act as a router unless it includes that function.

Figure 7 distinguishes the two paths. Blue represents IP Secure protection; grey identifies the TP line, where group security is configured separately using Data Secure. For routing and external clients, also complete section 3.3.

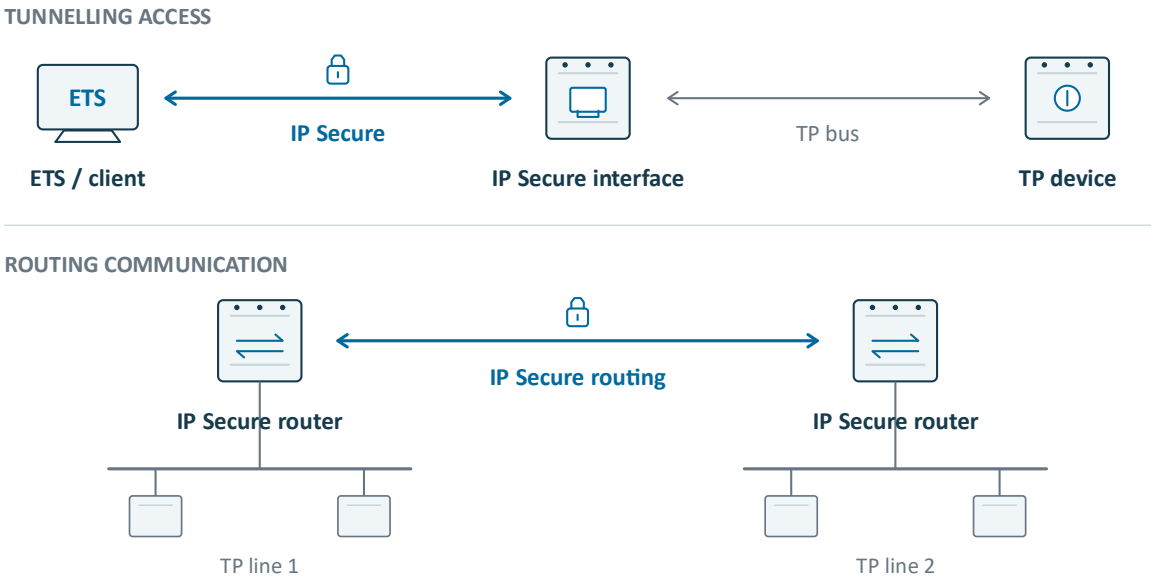


Figure 7. Scope of KNX IP Secure protection in tunnelling and routing

Preparing the interface

1. Add the correct IP product to the project and assign its individual address.

2. Configure IP addressing for the installation network. Check that ETS can reach the device and that there are no duplicate IP or individual addresses.

3. Enable secure commissioning and add the device certificate, following the same procedure as for bus devices.

4. Configure secure tunnelling and its slots, as explained in section 3.1.

3.1 SECURE COMMISSIONING AND TUNNELLING

1. Select the IP Secure interface or device and open "**Properties**" > "**Settings**".

2. Set "**Secure Commissioning**" to "**Activated**" and add its certificate.

3. If the device provides "**Secure Tunneling**", select "**Activated**". Figure 8 shows both settings. The configuration only takes effect in the interface after it has been downloaded.

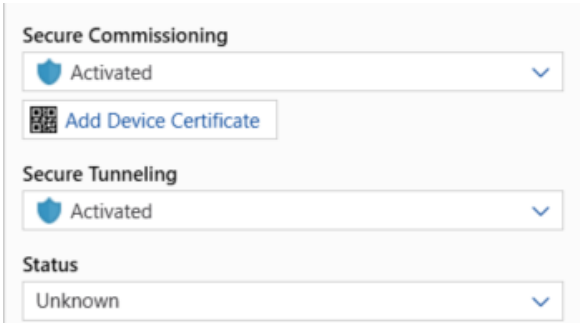


Figure 8. Enabling secure commissioning and secure tunnelling

4. Expand the device slots or tunnelling addresses and select the one the client will use.

5. In its properties, locate the password for that tunnelling slot, as shown in Figure 9. Assign an available slot to each client and check how many simultaneous connections the interface supports.

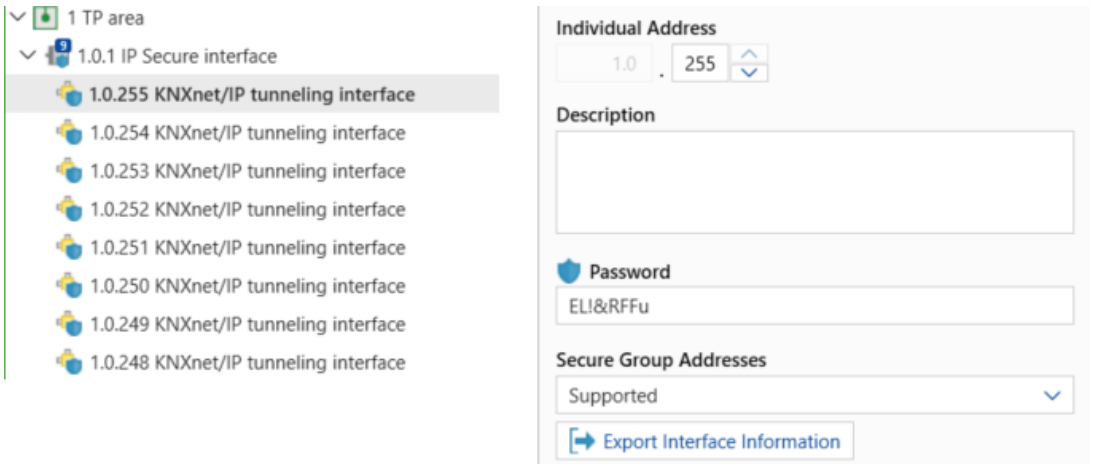


Figure 9. Password of the tunnelling slot

Check: each slot must have an individual address that is free on its line. The tunnel password is for the client using that slot; the commissioning password provides management access for ETS. Do not use the project password instead.

Continue with the commissioning credentials on the "**IP**" tab and select the interface in ETS.

3.2 CREDENTIALS AND INTERFACE CONNECTION

1. With the IP device selected, open the "**IP**" tab in its properties.

2. Locate "**Commissioning Password**" and "**Authentication Code**", shown in Figure 10. These are device credentials. Keep the values generated for each device and avoid reusing them. The values in the screenshots are from an example configuration.

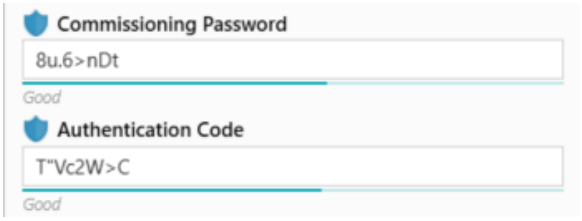


Figure 10. Device IP credentials

3. **Download the interface** with its network and security settings. First check the manufacturer's commissioning procedure and the available connection; the project credentials are not applied to the device until the download completes successfully.

4. Open the ETS connections and select the IP Secure interface. If prompted to log in, enter its commissioning password and authentication code where required. If ETS already has the correct credentials, it may use them without displaying a prompt.

5. Confirm the connection and test access to a device on the intended line. Then check the group functions that the client will use and their responses.

If the connection fails: check the selected interface, its IP and individual addresses, the downloaded configuration and the device credentials. Also check that a tunnel remains available. Do not disable security to resolve an authentication error.

3.3 ROUTING AND EXTERNAL CLIENTS

IP Secure routing

1. Check that the routers along the path support KNX IP Secure. In "**Topology**", select the IP line or backbone and check its "**Security**" property. Select "**On**" or "**Activated**", depending on the version, and resolve any participant incompatibilities.

2. Configure a common multicast address for the routers that need to communicate. Check that multicast traffic can pass through the network. ETS manages the shared backbone key; this is not the password of a tunnelling slot.

3. Download the routers and any other devices marked as affected by ETS. Test a function between lines and its response. An unsecured router cannot exchange secure routing telegrams with protected participants.

Preparing the network

Keep KNX on a controlled network and restrict access through the installation's network segmentation and firewall. Do not expose KNX ports directly to the Internet; use a VPN for remote access. Coordinate addressing and multicast with the network administrator.

External clients and key export

1. Check which mechanism the client supports: IP Secure tunnelling, IP Secure routing or Data Secure group addresses. Configure the required access and addresses in the project.

2. If the client uses a key file, open the project, go to its "**Security**" section and export the keyring. Protect the .knxkeys file with the password requested by ETS and import it according to the client instructions. If individual credentials are used, provide those for the assigned slot.

3. Give authorised personnel only the data they need; the keyring may contain keys for more devices and groups than the client uses. Test the client and create an updated export if keys or slots change. A client using Data Secure groups also needs the keys for those groups.

4 FACTORY RESET

If the project that programmed the device or its operational keys have been lost, first try to recover a valid backup. The original certificate alone does not provide access to a device that is already using other keys. If the keys cannot be recovered, consult the factory reset procedure for that product.

Procedure for a DINUY device

1. **Identify the exact product** and consult its instructions for use. Locate the factory reset procedure, power supply conditions and LED indications.

2. **Have the original certificate ready** for that device and the project you will use to program it again.

3. **Follow the sequence specified for that product.** Observe its button press times and confirmation signals. There is no single sequence that applies to all DINUY devices.

4. **Add or check the certificate in ETS** and enable secure commissioning in the destination project.

5. **Download the individual address and application again.** Check the groups, keys and operation of the affected participants.

Before intervening: a reset may erase configuration and keys and interrupt the controlled function. Confirm its effects in the product instructions, keep the certificate and coordinate the service interruption before carrying it out.

If the original project is available: you can use the unload operations supported by ETS and the device. Before using them, check the product documentation for their effects on the application, individual address, keys and BCU password.

A power interruption or a restart does not necessarily perform a factory reset.

5 NOTES

Changing an individual address

If you change the address of a device already participating in secure communications, check the devices sharing those functions. Download the participants and couplers marked as affected by ETS and test the commands and statuses again.

Reprogramming after a factory reset

Confirm that the device has returned to the factory state specified by the manufacturer. Add its certificate to the destination project, check the serial number and repeat secure commissioning. The new configuration must also be downloaded to the affected participants.

Device programmed using another project

A different project may not have the keys needed to access a device that has already been securely commissioned. Recover the project used to program it. If this is not possible, follow the product's factory reset procedure and add it again using its certificate.

Replacing a device

First export a project backup. The replacement device has its own serial number and certificate: do not reuse those of the removed device. Configure the compatible application, address and intended groups; add the new certificate and perform the secure download. Update any other participants marked as affected by ETS, test the functions and keep a new project backup.

BCU password

Where supported by the device, the BCU password controls programming access through a mechanism separate from KNX Secure. Consult the DINUY instructions before unloading or resetting: do not assume that removing one key also removes the other.

Keeping the project safe

After commissioning or modifying the installation, export the project as a protected .knxproj file and keep a backup away from the commissioning computer. Store the original certificates, passwords and, where used, the updated .knxkeys file separately. The keyring does not replace the ETS project.

Identify the date and version handed over. Check that the exported backup opens correctly and provide the maintenance manager with the instructions and credentials through a secure channel. Do not provide passwords in screenshots or publicly accessible documentation.