KNX SECURITY IN BUILDINGS

Working with KNX Secure

Contents

1. Purpose of the Document

This guide provides essential information on effectively utilizing KNX Secure within the ETS (Engineering Tool Software). It covers key topics such as generating ETS reports, understanding the general principles of secure communication, and ensuring the coexistence of KNX plain and secure devices. By following this guide, users will enhance their knowledge and implementation of KNX Secure, contributing to a more robust and secure building automation environment.

2. Working with KNX Secure

When working with KNX Secure, several key points must be considered to ensure a smooth and secure implementation.

1. Understand the two variants:

- KNX IP Secure: Secures communication over IP networks.
- KNX Data Secure: Secures telegrams on twisted pair (TP) networks.

Choose the appropriate variant based on your network type and security needs.

2. Device compatibility:

Mixed systems (secure and non-secure devices) are possible but require careful planning to avoid security gaps. An overview of which devices support KNX Secure should be obtained as early as possible in the planning process.

3. Secure Key Management:

Use a strong and unique ETS password. Store and manage keys securely—never share them openly or store them in unsecured locations.

4. ETS requirements:

ABB recommends using ETS 6.x or higher to configure KNX Secure devices. Ensure the project file is protected with a password and backed up securely.

3. KNX Secure in the ETS

The Engineering Tool Software (ETS) is central to the implementation of KNX Secure, as it manages all key security functions within the system:

- **Device Management:** Standard device management operations are protected through symmetric encryption using the tool key.
- **Group Communication Encryption:** Each group address is assigned a unique encryption key to secure group telegrams.
- **Point-to-Point Communication Encryption**: For direct communication (e.g., property access), each device pair uses a dedicated symmetric key.

The overall security of the KNX system, including devices, communication, and configuration, is primarily defined by the settings applied within ETS.

a) ETS Compatibility with KNX Secure

KNX Data Secure is supported starting from **ETS version 5.5.0**. However, for optimal performance and reliability, it is strongly recommended to use **ETS version 6.x or higher**.

Using versions before ETS 6.x may result in issues during commissioning, particularly when replacing devices or making configuration changes, due to limited support for newer security features.

b) KNX Infrastructure must Support Extended Frames

To enable routing or forwarding of KNX Data Secure communication, including the communication with the commissioning tool ETS, KNX infrastructure components must be capable of processing extended frames—telegrams with a maximum length of 263 bytes. This requirement ensures compatibility with the larger payloads used in KNX Data Secure messages.

Compatible ABB Devices
The following ABB components meet this requirement and can support KNX Data Secure communication, even if they are not KNX Secure devices themselves:

- USB/S 1.2 USB Interface (2CDG110243R0011) – Product details
- IPS/S 3.1.1 IP Interface (2CDG110177R0011) – Product details
- IPS/S 3.5.1 IP Interface Secure (2CDG110204R0011) – Product details
- IPR/S 3.1.1 IP Router (2CDG110175R0011) – Product details
- IPR/S 3.5.1 IP Router Secure (2CDG110176R0011) – Product details
- LK/S 4.3 Line Coupler Secure (2CDG110310R0011) – Product details

The devices are capable of handling extended APDU lengths and can therefore be used in secure KNX installations to facilitate communication.

c) Routing Requirements and Topology Awareness in KNX Secure Systems

KNX couplers and routers support the routing of unicast and system broadcast telegrams, which are essential for device commissioning and configuration via ETS.

Addressing requirements for this routing to function correctly:

- The interfaces used during commissioning and configuration must have a physical KNX individual address.
- This address must accurately reflect the interface's position within the KNX topology.

This requirement has always been part of the KNX system design, but it becomes especially critical in KNX Secure environments, where secure communication depends on precise addressing and topology alignment.

d) Use of Mobile (Roaming) KNX Interfaces in Secure Installations

When using a mobile KNX interface, also referred to as a roaming interface, it is essential to ensure that the local physical interface address is correctly configured in ETS.

ETS Support for Roaming Interfaces:

- ETS is capable of managing roaming interfaces effectively.
- It can configure the Secure Proxy of a segment coupler to ensure that all communication required for commissioning and configuration is routed correctly, even when the interface is not fixed to a specific location in the topology.

Third-Party Tools:

For KNX configuration tools outside of ETS (e.g., ABB i-bus® Tool), this automatic handling may not be supported. In such cases, it is advisable to connect to the system via a KNX interface located either on the Main Line or Area Line.

e) ETS Project Password

When a KNX Secure device is added to a project, ETS prompts the user to set a project password. This password is essential for protecting the project against unauthorized access.

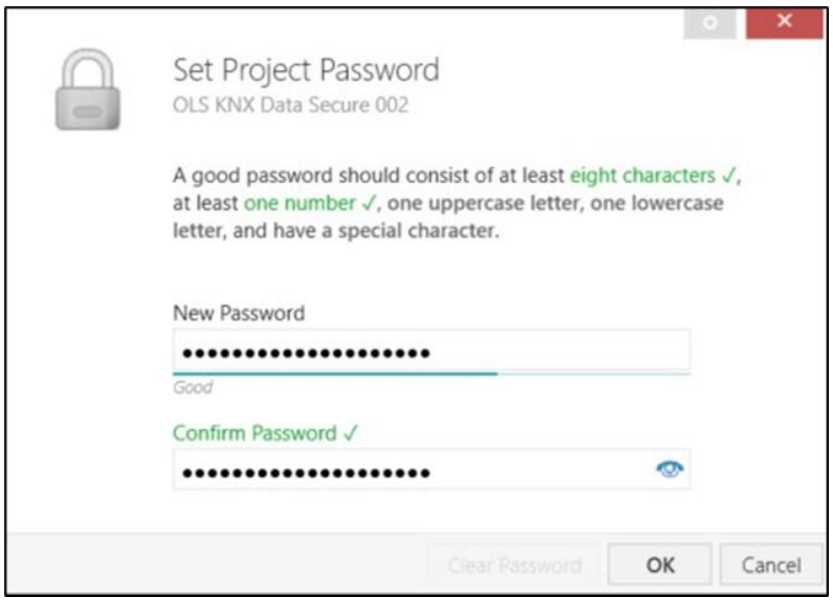


Image 1: Set project password in the ETS

If no ETS password is defined:

- KNX devices cannot be configured as Secure devices.
- All communication remains unencrypted (plain), leaving the system vulnerable.

Setting a strong project password is therefore a critical step in enabling and maintaining KNX Secure functionality.

Important: The ETS project password must be stored securely, as it is the only means of accessing encrypted project files. Once a project is encrypted:

- It cannot be opened without the correct password.
- Neither the KNX Association nor KNX device manufacturers can
    - Open encrypted ETS projects,
    - Reset forgotten passwords,
    - Or retrieve any data from encrypted files.

This makes secure password management essential for maintaining access to your KNX Secure projects.

f) Initial Commissioning

Each KNX Secure device comes with a device certificate, typically located on a removable label attached to the device (required for the first commissioning of the device). This certificate should be stored securely after installation to prevent unauthorized access to the Factory Default Setup Key (FDSK).

The device certificate provides the following information:

- The Factory Default Setup Key (FDSK)
- The corresponding serial number

Image 2: Example of device certificate on ABB devices

During the initial device setup, ETS will prompt you to enter the device certificate. It is also available as a QR code, which can be scanned using a QR scanner or entered manually.

The device certificate is required only once, during the initial encryption and authentication process between ETS and the KNX Data Secure device. Once the certificate is read, ETS extracts its key components: the serial number and the Factory Default Setup Key (FDSK).

ETS then generates and assigns a Toolkey to the device, which replaces the original certificate for runtime authentication and the continued commissioning process.

Only after this step the device can be configured as a KNX Secure device within ETS.

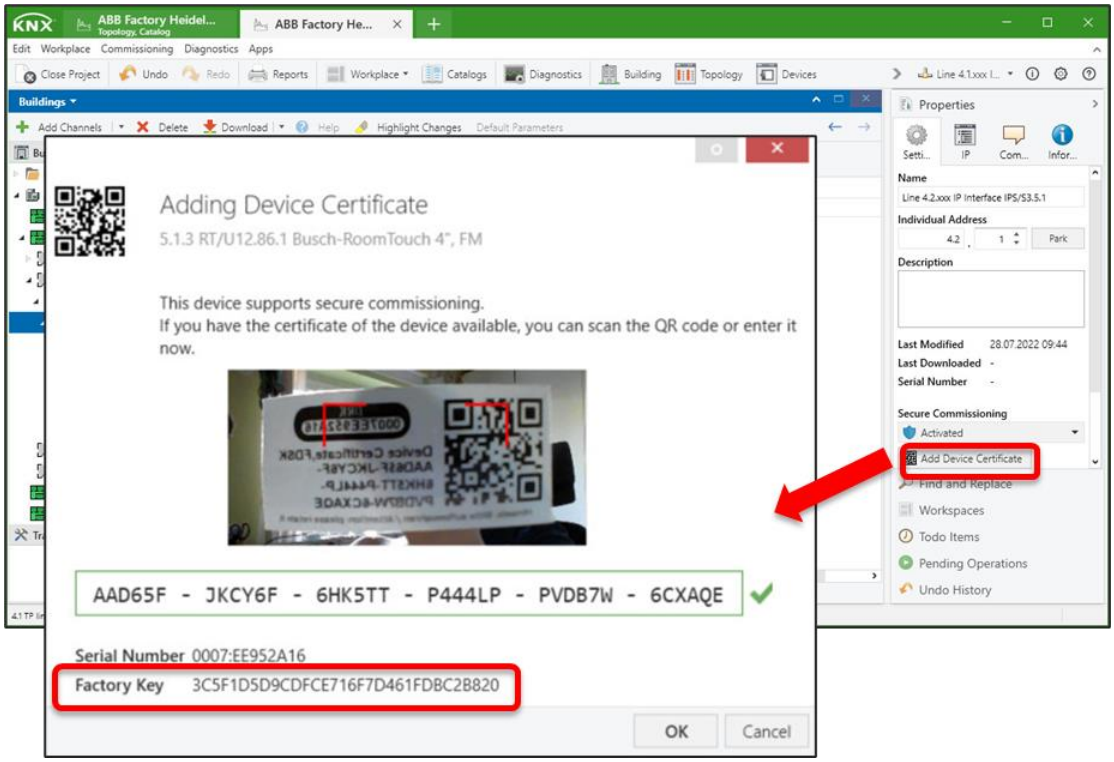


Image 3: Adding a device certificate to the ETS

Since the device certificate contains both the FDSK and the serial number, ETS can automatically match and assign the correct certificate to each device during initial commissioning. This streamlines the setup process, ensuring that each KNX Secure device is securely and correctly integrated into the project.

g) Offline Certificate Entry in ETS

You can conveniently scan or manually enter all device certificates for your KNX products into ETS in a single step, even without a live connection to the devices.

During initial commissioning, ETS automatically assigns each certificate to the correct device using the serial number, which is included in both the device's readable product data and its certificate.

As soon as a project is created, it appears in the ETS overview under "Local projects". When you click on a project tile, the "Details" option appears.

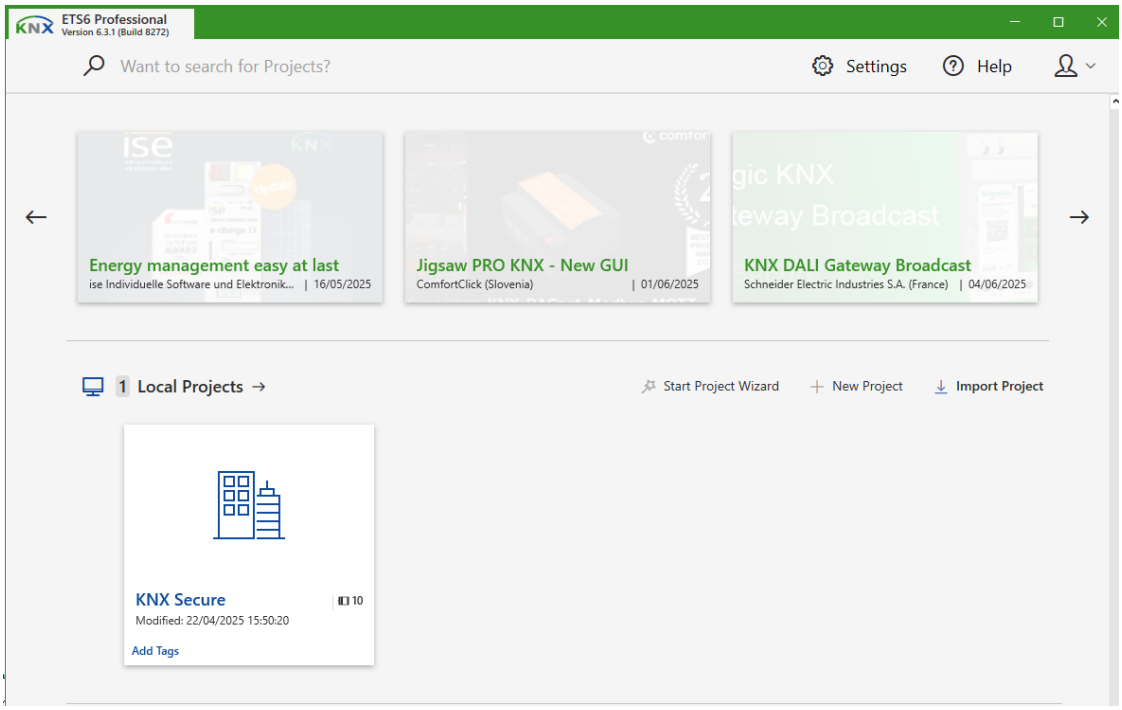


Image 4: ETS starting page with local projects view

By clicking on the “Security” tile in an ETS project, you can view all device serial numbers and FDSK keys, which are both part of the device certificate. This section also allows you to add new device certificates, making it easy to manage and update your KNX Secure setup directly within the ETS interface.

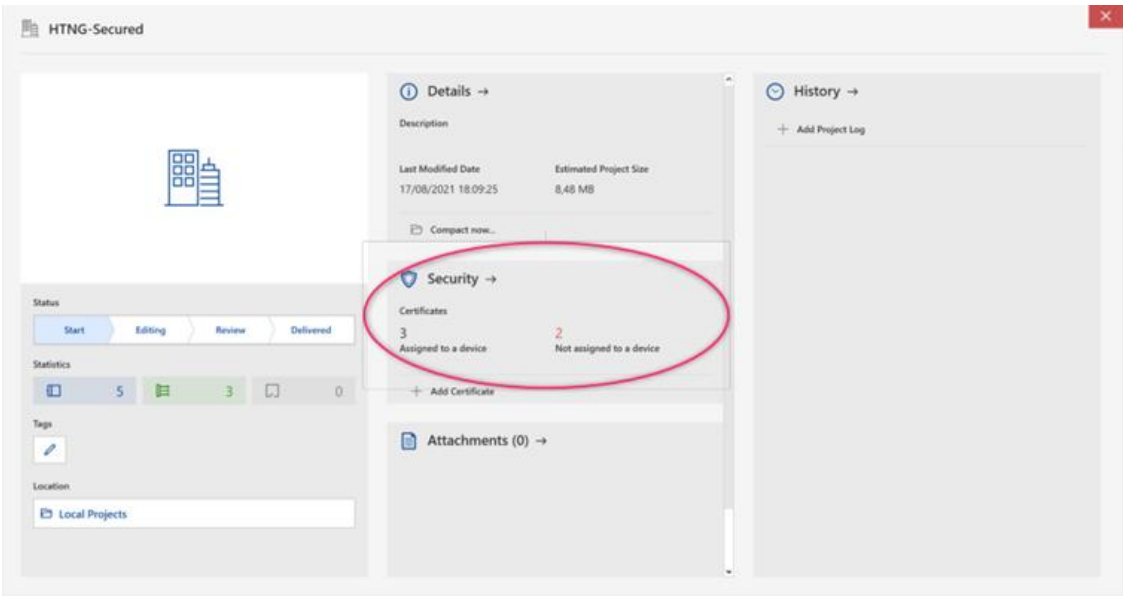


Image 5: Security view in the ETS project information

As soon as it is confirmed that a device will be part of the project, its certificate can be imported into ETS—even before the device is created in the software, installed on-site, or delivered to the construction location. This proactive step helps streamline the commissioning process and ensures that all necessary security credentials are already in place when the device is eventually integrated.

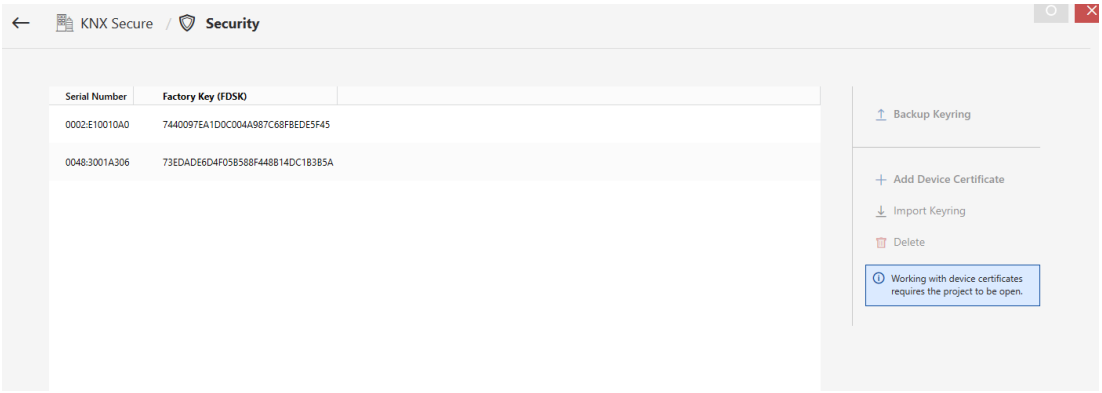


Image 6: Overview device certificates

This procedure is suitable for devices that are easily accessible and for which the individual KNX address can be easily set by pressing the programming button.

h) Online Commissioning using Device Certificates

Alternatively, you can select a specific device within ETS and manually link it to the appropriate device certificate. This allows ETS to identify the device and begin commissioning based on its **serial number**. This method is particularly beneficial when **physical access to the device is limited**, as it removes the need to press the programming button during setup.

A frequent challenge when commissioning **hard-to-reach KNX devices** is accessing the programming button. In such cases, assigning the **individual device address** using the serial number from the device certificate is a practical and efficient solution that eliminates the need for direct interaction with the device.

ABB KNX devices are supplied with two device certificate stickers. It is recommended that a sticker be removed and attached to the project documentation, stating which product it is and where it is installed. If the device certificate can be assigned to a device, programming can be carried out via the serial number without using the programming button.

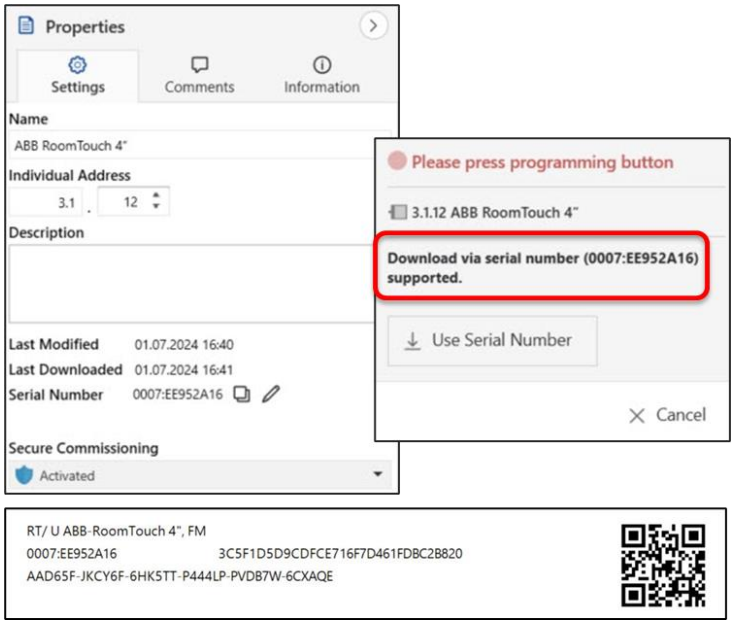
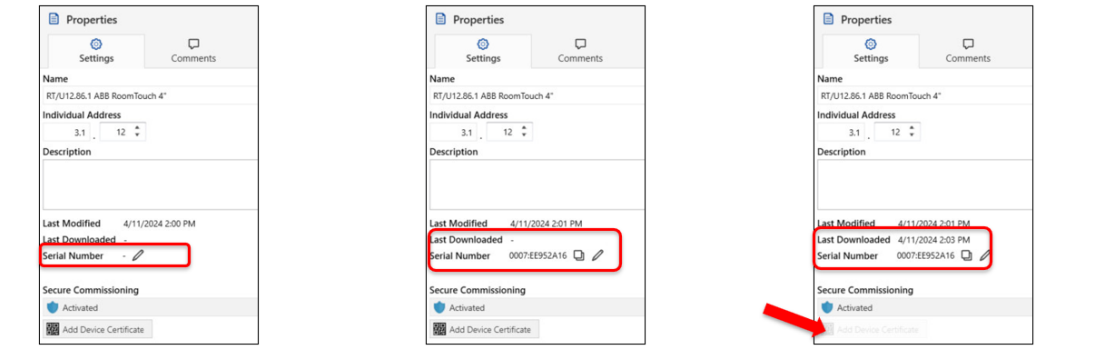


Image 7: Download via serial number in the ETS

The ETS tile on the right, under “Properties”, indicates whether a device certificate has been assigned to the device. The device is registered as a KNX product and is given a unique KNX address. Additionally, the tile shows whether the device currently supports KNX Data Secure based on its configuration.



No device certificate has been assigned yet (no serial number is displayed)

A device certificate has been assigned (the serial number is displayed)

The device was put into operation with the device certificate (“Add device certificate” button is grayed out)

Image 8: Device certificate assignment in the ETS “Properties” view

The ETS topology view offers a clear overview of which KNX devices have been securely commissioned. Devices that support KNX Secure are marked with a blue label in ETS.

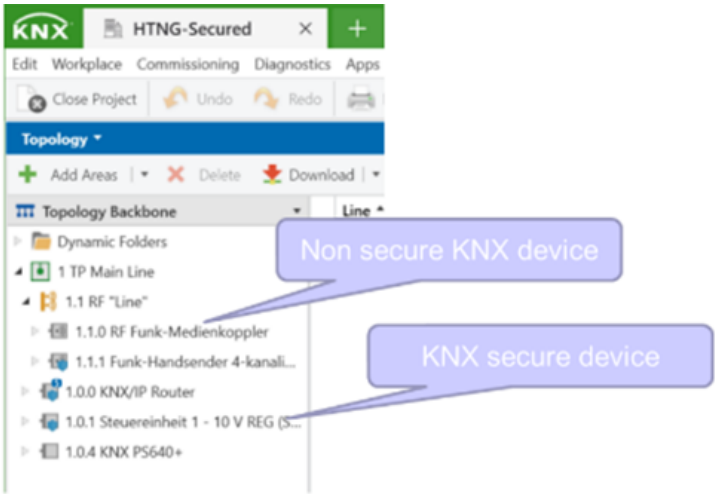


Image 9: Display of KNX Secure devices in the topology view in the ETS (blue shield)

i) KNX Device Security Settings

The security settings of a device can be modified. If the Secure commissioning option is set to "Deactivated", all group addresses linked to the device will switch to unencrypted communication (plain).

Important: Changing this setting triggers a master reset. All security keys will be erased, and the device must be fully recommissioned. Please note that this process may involve longer download times.

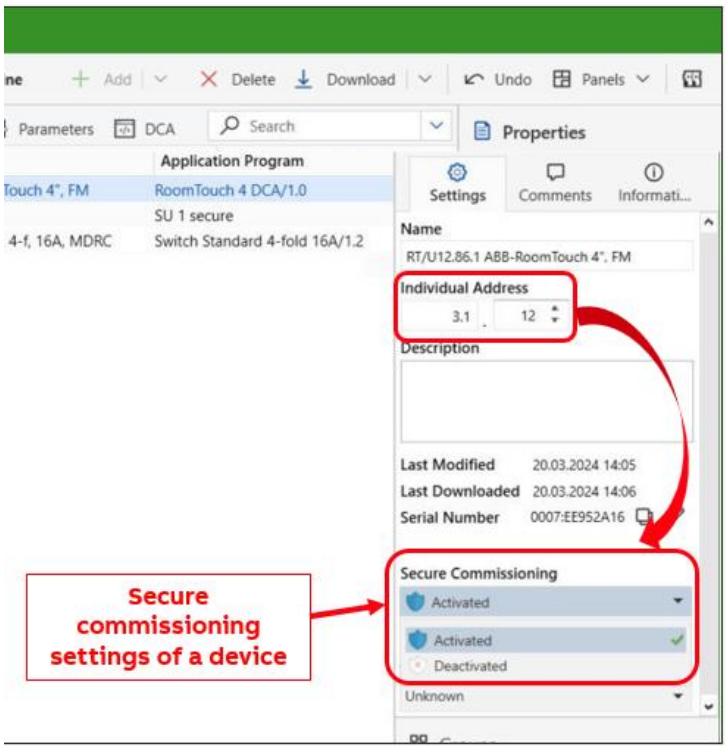


Image 10: Activate/Deactivate secure commissioning of a device in the ETS

When reactivating Secure Commissioning, a new Toolkey must be assigned. As a result, the security keys for all group addresses to which this KNX device sends data are also regenerated.

Note: Changing a device's security setting from Secure commissioning to Deactivated is rarely necessary and can lead to significant additional effort.

4. ETS Reports

ETS provides the ability to generate a variety of reports. In addition to general project reports, it also offers dedicated reports for KNX Secure, allowing for detailed documentation of security-related configurations.

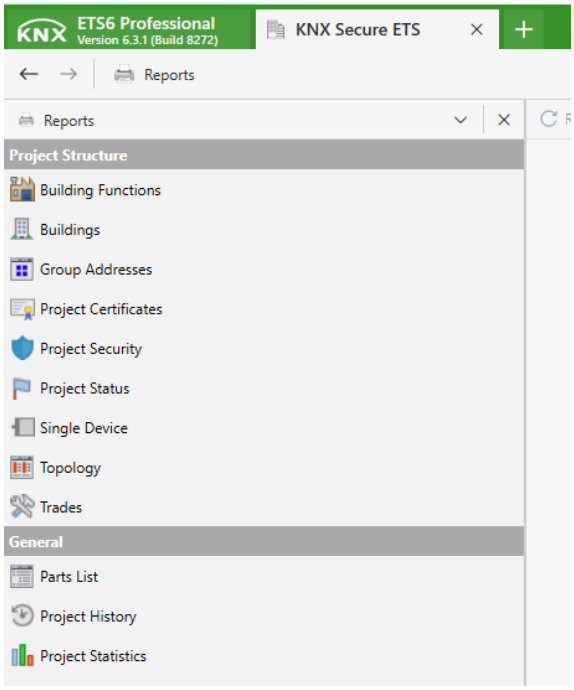


Image 11: ETS Reports overview

a) Project Security Report

The Project Security Report in ETS displays all keys and passwords generated during the configuration process. These include:

- Device Key
- Group Address Key
- KNXnet/IP Secure Backbone Key (used for Routing Services)
- Authentication Codes for KNXnet/IP Tunneling Interfaces

This report provides a comprehensive overview of the security credentials used within the project, supporting secure commissioning and communication.

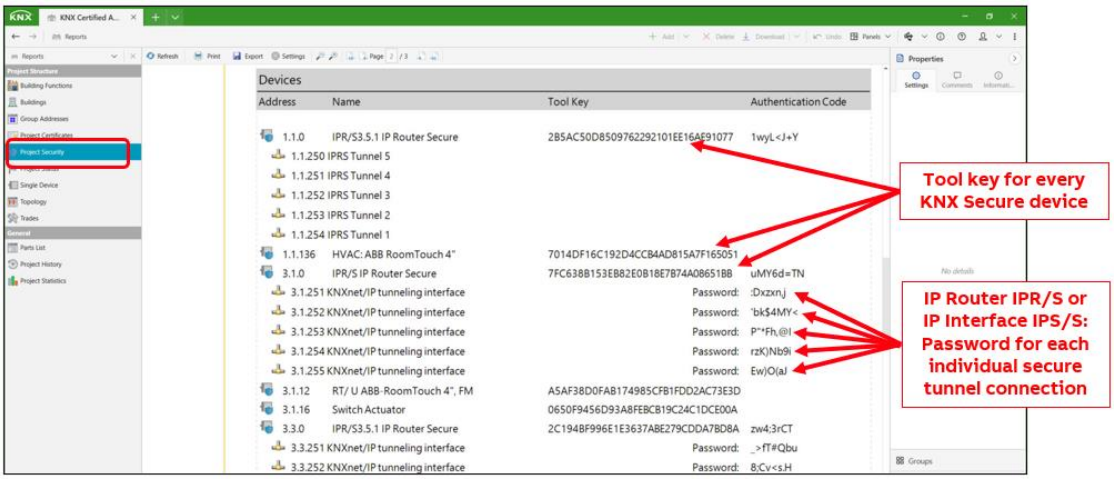


Image 12: Project Security Report example

The Project Security Report is primarily intended for documentation purposes. For further use, the data can be imported into external tools, or visualized using the Keyring Export function.

The KNX ETS Keyring Export allows keys from an ETS project to be exported for archiving outside the project, or integration with other applications.

This is especially useful when managing KNX Secure devices with external tools like the i-bus Tool, since each device has a unique initial key.

Additionally, the Keyring Export is essential when a visualization system or a KNX client needs to connect to a KNX Secure installation.

b) Project Certificates

The ETS provides the capability to record device certificates that have been assigned to devices. This documentation should be stored securely. A copy should be provided to the customer upon project handover. Please be sure to inform the customer that the documentation contains sensitive security information and should be kept in a safe place.

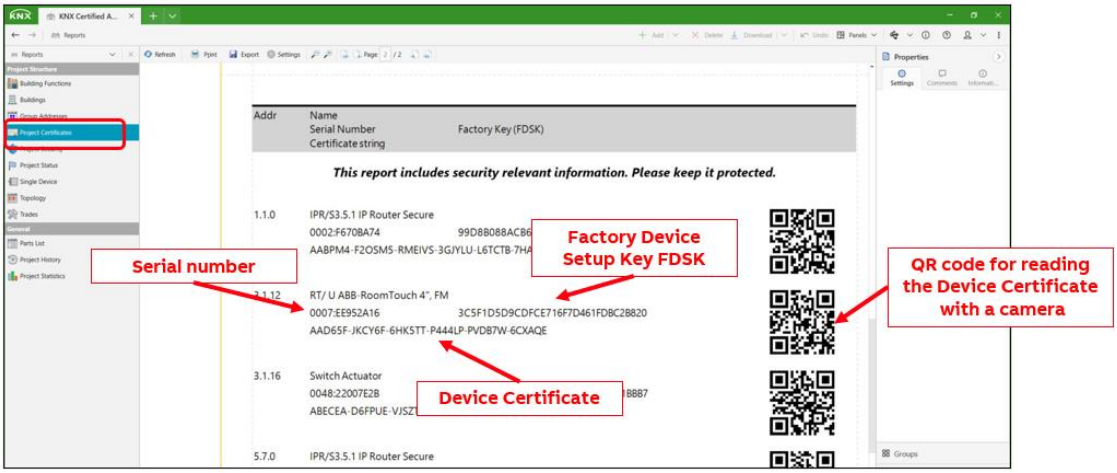


Image 13: Overview of project certificates in the ETS (recommended for customer documentation)

The documentation generated by the ETS includes a digital copy of the device certificate originally supplied with the product. This digital copy allows the device to be recommissioned as a KNX Secure product after a factory reset, in case the original certificate is no longer available.

5. General Principles of KNX Secure Communication

Dual Communication Capability

KNX Secure devices are capable of both secure and plain communication. They can even handle both modes simultaneously using different communication objects.

Communication Object Constraints

Each communication object can operate in either Secure or Plain mode, but not both.

All group addresses linked to a communication object must match its security mode.

Group Address Security Modes

Group addresses are classified as either Plain or Secure.

Exception: When a secure proxy is used, a group address in one KNX segment or line may be plain, but the proxy translates it into a secure group address in another segment or line.

Security Key Management

Every KNX Secure device uses a unique security key for each secure group address. These keys are generated by the ETS during commissioning. The keys are automatically loaded into the devices but are not visible in the ETS interface.

Whether ETS configures a group communication as secure or plain depends on multiple factors:

1. Commissioning / Device Security

Whether a KNX device is commissioned as a KNX Secure device using the Factory Default Setup Key (FDSK). Only devices recognized by ETS as Secure—indicated by a blue shield icon—can be assigned to Secure group addresses. If a device is not commissioned with the FDSK, it will not support secure communication, even if it technically supports KNX Secure.

2. Runtime / Group Address Security Properties

This setting allows the ETS user to define whether communication should be secured (forced on) or unsecured (forces off) during runtime. This can be configured individually per group address, offering flexibility in securing only the necessary parts of the KNX installation.

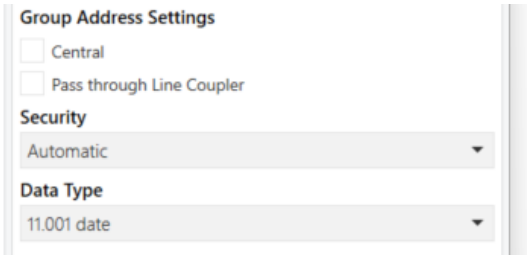


Image 14: Group address security properties

In ETS, the default setting for group address security properties is **“Automatic.”** The behavior of each setting is as follows:

Automatic
The group address adopts the highest level of security supported by all communication objects linked to it. If a group address connects both a KNX Secure device (with a secure communication object) and a KNX Plain device (with a plain communication object), the group address will default to KNX Plain, as secure communication cannot be guaranteed across all devices. If all connected devices support secure, the group address will default to secure.

Forced On
When this option is selected, the group address is explicitly set to **secure**. Only communication objects from KNX Secure devices can be linked to this group address. Any attempt to connect a plain (non-secure) device will be rejected.

Forced Off
This setting enforces **plain (unencrypted)** communication for the group address, regardless of whether the connected devices support KNX Data Secure. All communication over this group address will be unencrypted.

KNX Secure group addresses are marked with a blue or white label in the ETS.

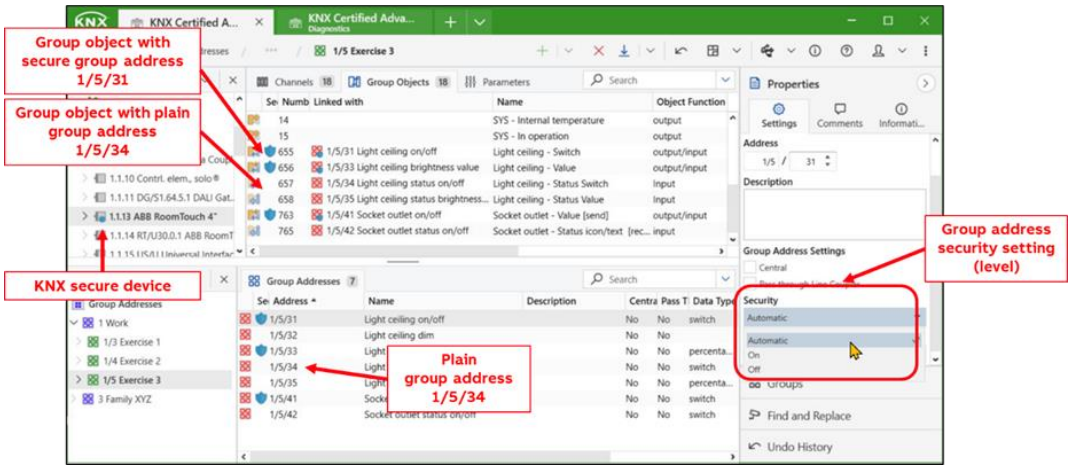


Image 15: Display of secure communication in the ETS (blue shield)

A blue indicator signifies that secure communication is continuously maintained from the sender to the receiver.

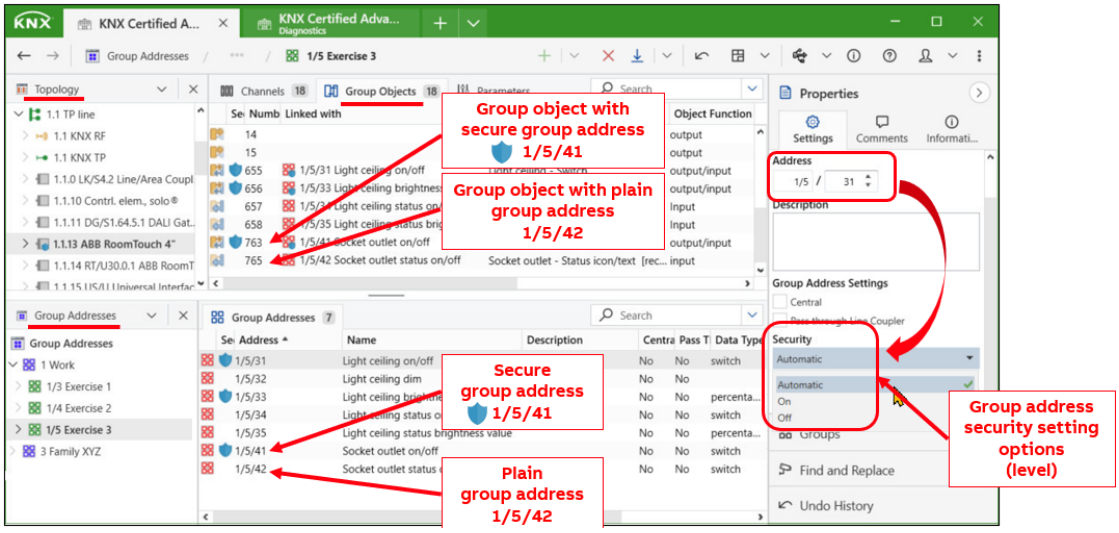


Image 16: Secure communication indicated by a blue shield next to the group address

Predefined Security Properties in KNX Devices

The security properties of a KNX device are predefined by the device manufacturer. For certain communication objects, the manufacturer may specify that secure communication is mandatory—this is typically the case when the function requires a high level of security (e.g., a door or window contact).

Attention: If secure communication is enforced by the manufacturer for a specific communication object, ETS will not allow that object to be connected to a KNX Plain group address. This restriction is intentional and ensures the integrity and security of critical functions.

6. External KNX Communication Devices

Building Management Systems (BMS), visualization systems, or other clients that are commissioned outside of ETS must have access to the group address key in order to decrypt secure group communication.

Devices that communicate with KNX but are not commissioned via ETS are considered external KNX communication devices.

These devices are not covered by the KNX standard and therefore are not KNX certified and are not registered with the KNX Association.

Even if such devices claim to support KNX Data Secure, this does not guarantee that the device itself is secure. Security assurance must be verified with the device manufacturer.

ETS Keyring Export

The ETS keyring export provides the necessary credentials for secure communication and includes:

- All group address runtime keys
- Tool Keys for each secure device
- Passwords for IP tunneling connections
- The exported file is saved with the extension: .knxkeys

Important Security Note:

The xxx .knxkeys file itself is not encrypted, but the keys inside are encrypted.

Password Protection

When creating a keyring export (also known as a backup keyring), the user is prompted to set a password. This password is required to decrypt and use the keys stored in the file.

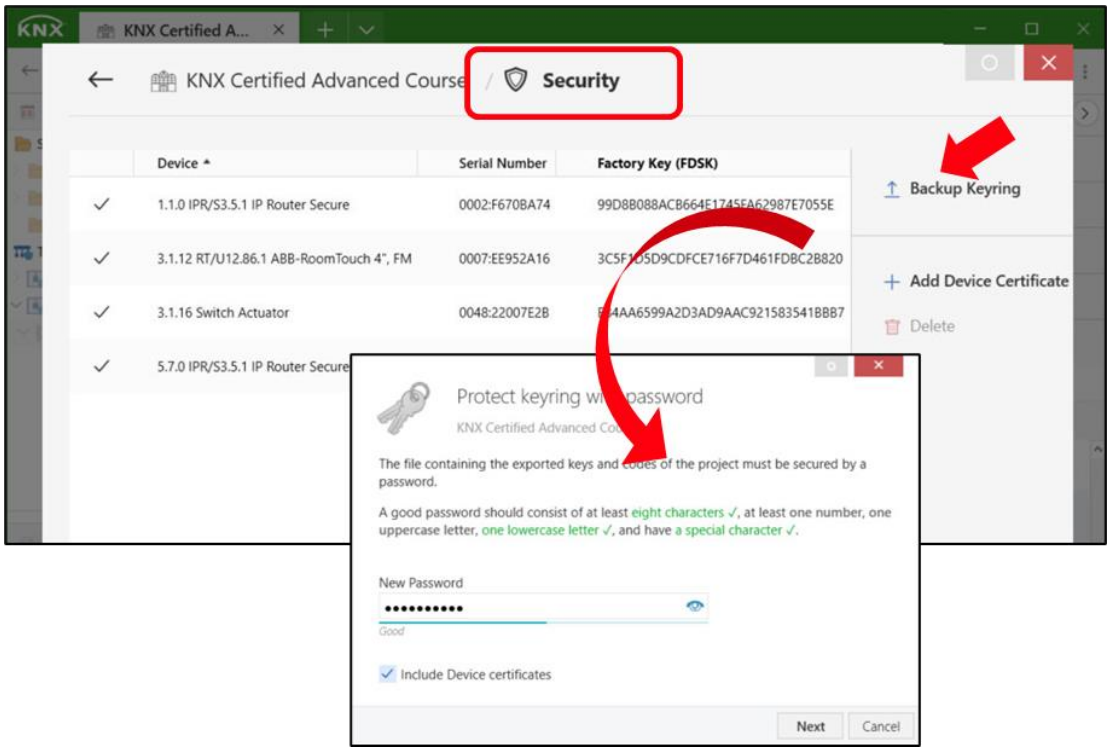


Image 17: Set password to protect keyring export

Important: Before exporting the keyring, ensure that the physical address of the external communication device (dummy) is created in the ETS project. This must be done prior to the export. The address can either be:

- The individual address of the KNXnet/IP tunnel interface, or

- The individual address of a dummy object created in ETS.

This address must exactly match the individual address configured as the "own address" in the external communication subscriber.

Below is an example of how this setting appears in the EisBaer software. ABB provides this software, developed by Alexander Maier GmbH, in two versions:

- **EisBaer SCADA3** – for standard applications
- **EisBaer 4.0** – for advanced solutions, including full historical data recording and storage

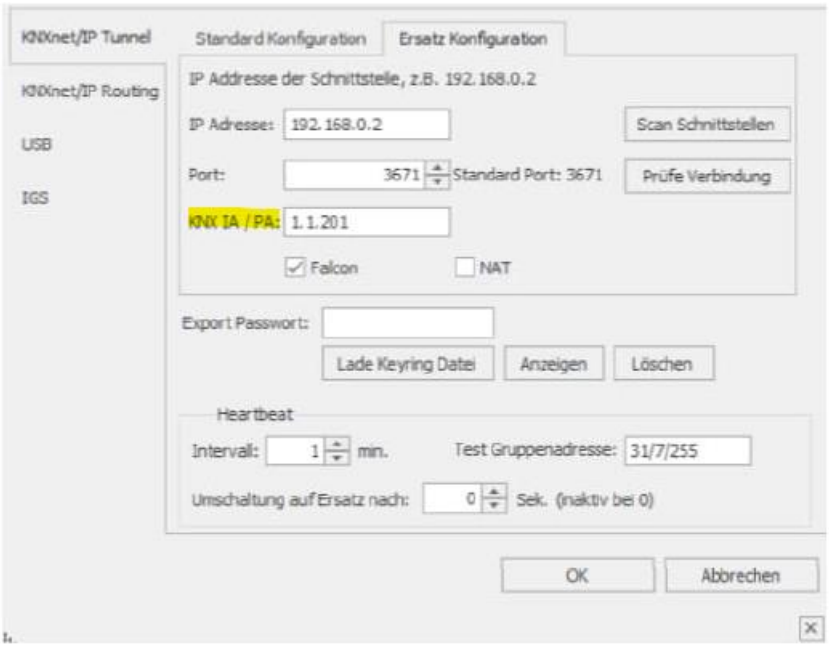


Image 18: Physical address of external communication device in the EisBaer software

Safety Note:

The security characteristics of KNX Secure communication devices that are not KNX-certified—whether they support KNXnet/IP Secure, KNX Data Secure, or both—are only partially governed by the KNX standard. As a result, their security properties may vary and cannot be fully guaranteed by the standard alone.

a) KNX Data Secure and External Communication Participants

With KNX Data Secure, each telegram is protected using two security keys:

- Sender Authentication Key – to verify the identity of the sender.
- Group Address Encryption Key – to secure the communication on the group address level.

These keys are essential for secure communication and are included in the ETS keyring export (also known as the backup keyring). In addition to the keys, each telegram is also protected by a sequence counter and the source address, which are evaluated during communication.

Unlike unencrypted KNX communication, KNX Secure requires every participant in group communication to have a unique individual address. This address must be:

- Created in the ETS project, and
- Used consistently by the external communication device.

For devices not managed directly in ETS, it is still mandatory that they:

- Receive an individual address defined in the KNX project, and
- Send and receive telegrams using this address.

This can be achieved by:

- Assigning group addresses to a secure dummy object, or
- Using a tunneling interface with assigned group addresses.

The dummy object must be secure and topologically located above the physical bus interface to ensure proper communication flow.

b) Group Addresses are Connected to a KNXnet/IP Tunnel

KNX IP routers and IP interfaces with an > 5.0 ETS database entry (support the linking of group addresses to a KNXnet/IP tunneling connection). In this configuration, communication is tunneled through the individual address of the KNXnet/IP tunnel interface.

This setup enables secure and structured communication, particularly in KNX Secure environments, by ensuring that each tunneling connection is uniquely identifiable and properly integrated into the ETS project.

Backbone

Key CCDDB77A89FF77B57DBA61C56CD8A5DE

Devices

Address	Name	Tool Key	Authentication Code
1.1.0	IPR/S3.5.1 IP Router Secure	9208D477B123531F33F6306502E1D266	f3eYFIS<
1.1.251	KNXnet/IP tunneling interface	Password:	#kfBb"/9
1.1.252	KNXnet/IP tunneling interface	Password:	mq!,C5T<
1.1.253	KNXnet/IP tunneling interface	Password:	MmC7_;h4
1.1.254	KNXnet/IP tunneling interface	Password:	,pZkUP$d
1.1.255	KNXnet/IP tunneling interface	Password:	G?8XZewW
1.1.1	US/U4.3 Universal Interface, 4-fold, FM	38675C8794E2E2645FB5A94166B70D21	
1.1.2	JRA/S4.24.5.2 Blind/Shutter Actuator, travel detection, manual operation, 4-fold, 24 V DC	F48063CE4E5D9514831E8FE76F0684A2	

Image 19: KNXnet/IP tunneling connections

However, the KNXnet/IP interface only provides an interface, or in other words a communication tunnel. All KNX Data Secure processes must be supported by external communication participants.

In addition to the IP address, the individual KNX address of the KNXnet/IP tunneling interface must also be correctly configured in the external communication device.

If the configuration in the external communication participant does not exactly match the data defined in the ETS project, KNX Data Secure communication will fail.

c) ETS Dummy Application

For systems using USB interfaces or IP interfaces not supported in ETS versions earlier than 5, an alternative method for integrating external communication participants is available: Creating Secure KNX Dummy Objects in the ETS project.

What is a Dummy Object?

A dummy object is a virtual KNX device entry in ETS that does not correspond to a physical device. It serves several important purposes:

- Topological Placement: It allows external devices to be logically positioned within the ETS project structure.
- Filter Table Configuration: It enables the editing of filter tables in KNX routers and couplers, ensuring proper routing of group telegrams.

Although the dummy application cannot be downloaded into a physical device, it influences the behavior of the network by modifying the filter tables. These changes must be downloaded to the routers and couplers to take effect.

Implementation Notes:

Since a dummy object is purely a virtual database entry, any dummy object available in the ETS online catalog can be used for this purpose.

The dummy object must be configured as Secure and placed topologically correctly to represent the physical bus interface to ensure proper communication flow and security compliance.

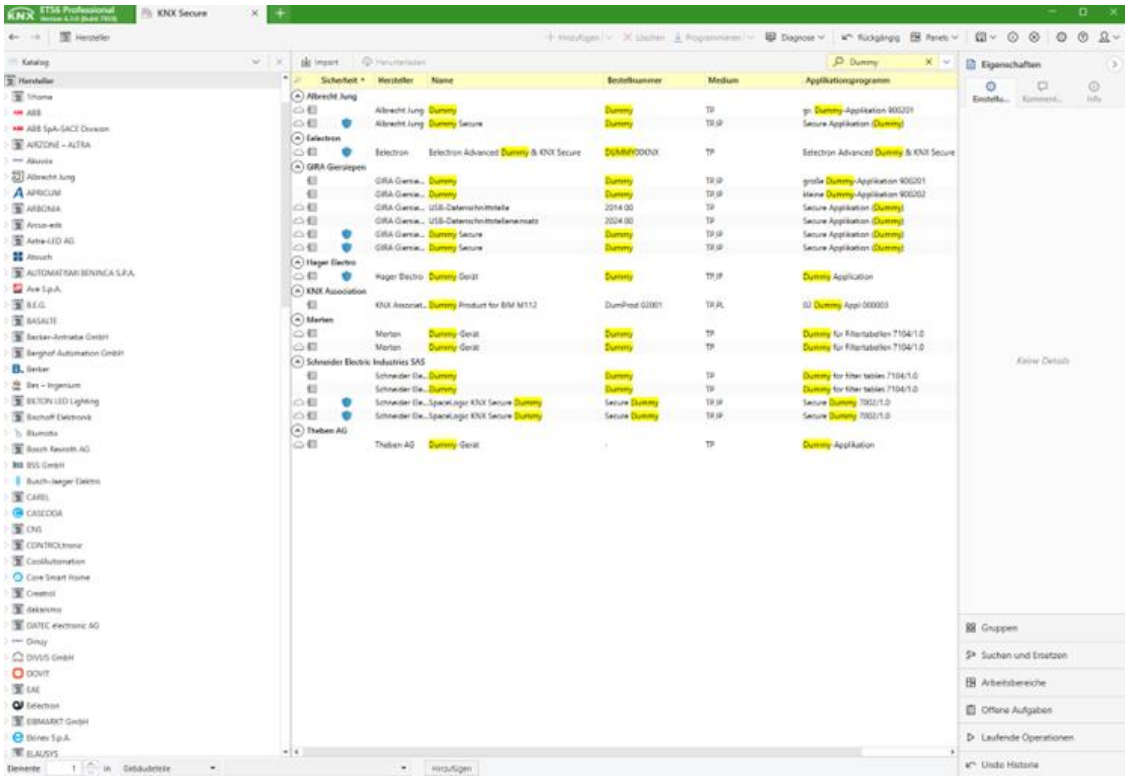


Image 20: ETS dummy application examples

When using dummy objects to integrate external communication devices into a KNX Secure setup, it is essential to select the correct type of dummy object from the ETS Online Catalog.

Secure dummy objects are clearly marked with a “Secure” symbol in the catalog.

If a “Plain” (non-secure) dummy object is used instead, ETS will automatically downgrade the communication to KNX Plain, effectively disabling KNX Data Secure for that communication path. This makes it critical to ensure that only Secure-designated dummy objects are used when configuring secure communication participants.

d) Maintenance of a KNX Secure Project

Access and Security of ETS Projects in KNX Secure Systems

To maintain or troubleshoot a KNX Secure system, access to the ETS project is essential. This is because all secure communication parameters, including keys and device configurations, are managed within the ETS project.

Password Protection

- Every ETS project is protected by a password.
- Access is impossible without the correct password—even for minor maintenance tasks.
- There is no password reset or recovery option. If the password is lost, the project becomes permanently inaccessible.

Password Management and Project Sharing

Changing the ETS project password:

- Does not affect ToolKeys or MaC Keys.
- Does not require recommissioning of the KNX Secure system.

However, password changes only apply to the local instance of the project.

- If the project has been shared (e.g., with installers or system integrators), those individuals can still access their local copies using the original password.
- With access to their copy, they can send, receive, decrypt telegrams, and make changes to the system.

Security Implications

For this reason, strict control over the distribution of ETS projects is critical.

Unauthorized access to a project file—even without the current password—can compromise the integrity and confidentiality of the KNX Secure system if the original password is still valid on other copies.

7. Coexistence of KNX Plain and KNX Secure Devices

KNX installations can include both KNX Plain and KNX Secure devices operating on the same physical medium (e.g., TP, IP). This flexibility allows for gradual upgrades and mixed-security environments.

Full-Security Installations

If all devices in the system—from sensors to actuators—are KNX Data Secure-capable, the entire installation can be secured end-to-end using KNX Data Secure. This ensures encrypted and authenticated communication across all group addresses.

Current Market Reality

However, KNX Data Secure is still relatively new, and not all device types or applications currently have Secure-capable options available. This limits the ability to implement full-system security in some scenarios.

Role of KNX Secure Proxy

A KNX Secure Proxy plays a crucial role in enabling interoperability between conventional KNX (Plain) and KNX Secure devices, while preserving the highest possible level of security within the system.

Key Functions:

Bridges Secure and Non-Secure Segments: It allows secure and non-secure devices to coexist in the same installation by isolating communication domains (coupler functionality) and at the same time translating between encrypted und non-encrypted communication.

Creates Security Sub-Networks: A coupler or router with proxy can be used to define secure zones within a larger KNX installation, ensuring that sensitive communication remains protected.

Provide Best Possible Security: Even when integrating legacy devices, the proxy ensures that an optimal level of secure communication is maintained

Implementation:

The KNX Secure Proxy is not a standalone device but a functional capability that can be implemented in various types of KNX couplers, including Segment Couplers, Line Couplers, Area (Backbone) Couplers.

These couplers, when equipped with Secure Proxy functionality, act as gateways between secure and non-secure segments, enforcing encryption and authentication rules where applicable.

Limitations and Configuration of KNX Secure Proxy:

A KNX Secure Proxy does not support the translation of unicast (point-to-point) communication or system broadcasts between secured and unsecured domains. This limitation is intentional and serves a critical security purpose: only ETS instances with valid security keys are permitted to program KNX devices that use KNX Data Secure.

Implementation Constraints:

The Secure Proxy function can only be implemented in couplers. Segment couplers cannot be cascaded; that is, they must not be used on the secondary side of another segment coupler.

Configuration Dependencies:

Several dependencies exist between the coupler and the Secure Proxy functionality. The availability of the Secure Proxy feature depends on how the coupler is configured in ETS 6:

- If the coupler is set up as a KNX Secure device, the Secure Proxy function is automatically enabled.
- If configured as a KNX Plain device, the Secure Proxy function is not available.

Once enabled, the Secure Proxy settings are managed entirely by ETS, based on the project configuration.

8. KNX Project Handover

a) Effects of the EU Cyber Resilience Act (CRA)

The EU Cyber Resilience Act (CRA) introduces mandatory cybersecurity requirements for all products with digital elements, including KNX systems. A key principle of the CRA is that customers must be able to assume that a product is secure by default. Any limitations to this security—whether technical or economic—must be clearly communicated to the customer.

When handing over a KNX project, it is essential to:

- Transfer all security-relevant data alongside the general project data.
- Provide the customer with a clear explanation of the system's security features, including any known or unavoidable risks.
- Document this information and include it in the technical handover package to avoid future liability.

b) ETS Reports, Security Certificates and Password Management

1. ETS Reports

ETS generates two key reports that contain essential security information:

- Project Security Report
- Project Certificates Report

These reports should be:

- Prepared and reviewed with the customer.
- Included in the project handover documentation.

2. Customer Awareness and Access

Customers—especially those without ETS access—must be informed about:

- The central role of the ETS project in maintaining KNX Secure systems.
- The need for ongoing collaboration with the system integrator to keep the project secure and up to date.

3. Password Management

The ETS project is protected by a password, which is required for planning and maintenance. If the customer has an ETS license, they may assign a new local password, but:

- This change only affects their local copy.
- It does not affect ToolKeys, MaC Keys, or group keys.
- If the system integrator retains a copy of the project, they can still access and modify the system.

It is recommended to:

- Agree on a clear policy for managing ETS project copies and passwords.
- Maintain a list of individuals who have access to the ETS project.

4. Device Certificates

For reusing KNX Secure devices after a master reset or in a new project, the device certificate is required. The method of certificate storage and retrieval varies by manufacturer and product. It is crucial to establish a process for recording, managing, and transferring these certificates between the system integrator and the customer.

9. Further Information

- KNX Cybersecurity Hardening Guide
- KNX Cybersecurity Hardening Checklist
- KNX Secure Technical Details
- KNX Data Secure training presentation