LINE/FIELD COUPLING KNX SECURE - IP20 - 1 MODULE - DIN RAIL MOUNTING

GW A9708

Technical Manual

Contents

1 Introduction

The KNX Line Coupler secure is a KNX line coupler in a compact design.

It connects two KNX bus segments (for example, a KNX line with a KNX area).

The device has an extended filter table for main group 0…31 and ensures a galvanic isolation between the lines. The coupler supports KNX Data Security and KNX Long Frames.

It is compatible with the ETS® software ETS 5 or higher. The functionality of Security Proxy and Segment Coupler is only supported with the ETS 6 database.

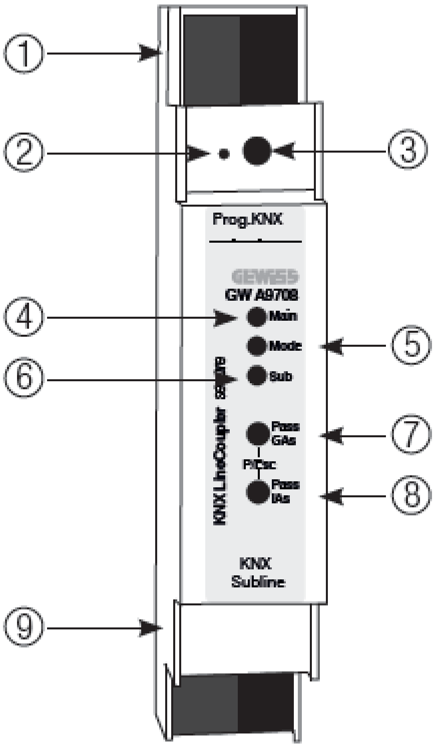
The buttons on the front panel allow disabling the telegram filter for testing purposes.

The LEDs indicate operating conditions as well as communication errors on the KNX bus.

The power is supplied via the KNX bus (main line).

2 Installation

The Device is designed for installation on a DIN rail with a width of 1 unit (18mm). It features the following controls and displays:



1. KNX bus connector (main line)
2. Programming LED (red)
3. Button for programming mode
4. LED Main (multicolor)
5. LED Mode (multicolor)
6. LED Sub (multicolor)
7. Button Pass GAs
8. Button Pass IAs
9. KNX bus connector (sub line)

If the bus voltage is missing, the device is without function.

2.1 KNX programming mode

The KNX programming mode is activated/deactivated either by pressing the recessed KNX programming button ❸ or by simultaneously pressing the buttons (P/Esc) ❼ and ❽.

When the programming mode is active, the programming LED ❷ and the LED Mode ❺ light up red.

The operation/visualization of the programming mode on the front can be activated/deactivated in the ETS® on page general settings.

2.2 Manual operation and status display

The LED Main ❹ lights up green if the device is successfully powered by the KNX bus. This LED indicates telegram traffic on the KNX bus by flickering.

Communication failures (e.g. repetitions of telegrams or telegram fragments) are indicated by a short change of the LED color to red.

Overview of the different indications of LED Main ❹:

LED Status	Meaning
LED lights green	KNX bus power active (main line)
LED flashes green	Telegram traffic on the KNX bus (main line)
LED briefly red	Communication error on the KNX bus (main line)

The LED Sub ❻ lights up green when the device is ready for operation (supplied by the main line) and the KNX bus voltage is present on the sub line. If the LED is flickering, telegram traffic takes place on the sub line.

Errors in the communication (such as telegram repeats or telegram fragments) are indicated by a short-time color change to red.

Overview of the different indications of LED Sub ❻:

LED Status	Meaning
LED lights green	KNX bus power active (sub line)
LED flashes green	Telegram traffic on the KNX bus (sub line)
LED briefly red	Communication error on the KNX bus (sub line)

For testing purposes (for example, during commissioning) the configured routing settings (filter or block) can be bypassed via manual operation.

With the button Pass GAs ❼ the forwarding of group addressed telegrams can be activated.

With the button Pass IAs ❽ the forwarding of individually addressed telegrams can be activated.

This is visualized with a single flash of the LED Mode ❺ (orange). If both modes are activated the LED Mode ❺ flashes two times.

Pressing button Pass GAs ❼ or button Pass IAs ❽ again these settings can be selected and deselected on demand. Via the Escape function (Esc) the manual opera-tion can be stopped by simultaneously pressing the button Pass GAs ❼ and button Pass IAs ❽.

If neither programming mode nor manual mode are active the LED Mode ❺ can visualize configuration errors (for details see table below).

Overview of the different indications of the LED Mode ❺:

LED Status	**Meaning**
LED lights green	Device is working in standard operation mode.
LED light red	Programming mode is active.
LED flashes 1x orange	Programming mode is not active. Manual operation is active: Forwarding IA or GA.
LED flashes 2x orange	Programming mode is not active. Manual operation is active: Forwarding IA and GA.
LED flashes red	Programming mode is not active. Manual operation is not active. The device is not loaded correctly, e.g. after aborting a download.
LED flashes green	The device is currently loaded by the ETS.

3 Reset to factory default settings

It is possible to reset the device to its factory default settings.

- Disconnect the KNX bus connector (main line) ❶ from the device.
- Press the KNX programming button ❸ and keep it pressed down.
- Reconnect the KNX bus connector (main line) ❶ to the device.
- Keep the KNX programming button ❸ pressed for at least another 6 seconds.
- A short flashing of all LEDs (❷❹❺❻) visualizes the successful reset of the device to factory default settings.

3.1 Factory default settings

In the factory default settings, the device has the physical address 15.15.0.

Also, KNX Data Security is disabled and the initial key (FDSK) must be used for secure commissioning.

Routing (Sub -> Main)

Group telegrams: Lock
Individual addressed telegrams: Filter

Routing (Main -> Sub)

Group telegrams: Lock
Individual addressed telegrams: Filter

4 Function as line or area coupler

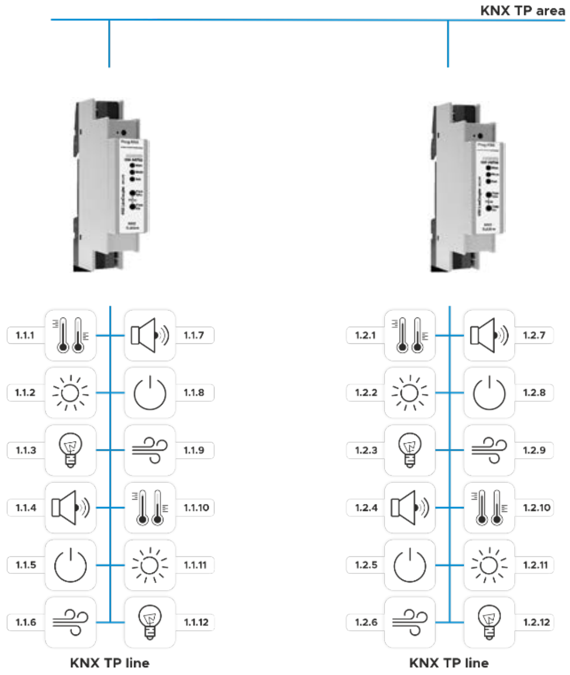
The device can work as line or area coupler.

The following table shows the possible applications of the device compared to IP based topology:

	Classic topology (without IP)	IP coupling of the areas (IP area coupler)	IP coupling of the lines (IP line coupler)
Backbone	TP	IP	IP
Coupling	KNX TP line coupler (max. 15 couplers)	KNX IP router (max. 15 routers)	Directly via LAN with switch
Area	TP	TP	IP
Coupling	KNX TP line coupler (max. 15x15 couplers)	KNX TP line coupler (max. 15x15 couplers)	KNX IP router (max. 225 routers)
Line	TP	TP	TP

The device has a filter table and therefore helps to reduce the bus load. The filter table supports the extended group address range (main groups 0 … 31) and is automatically generated by the ETS.

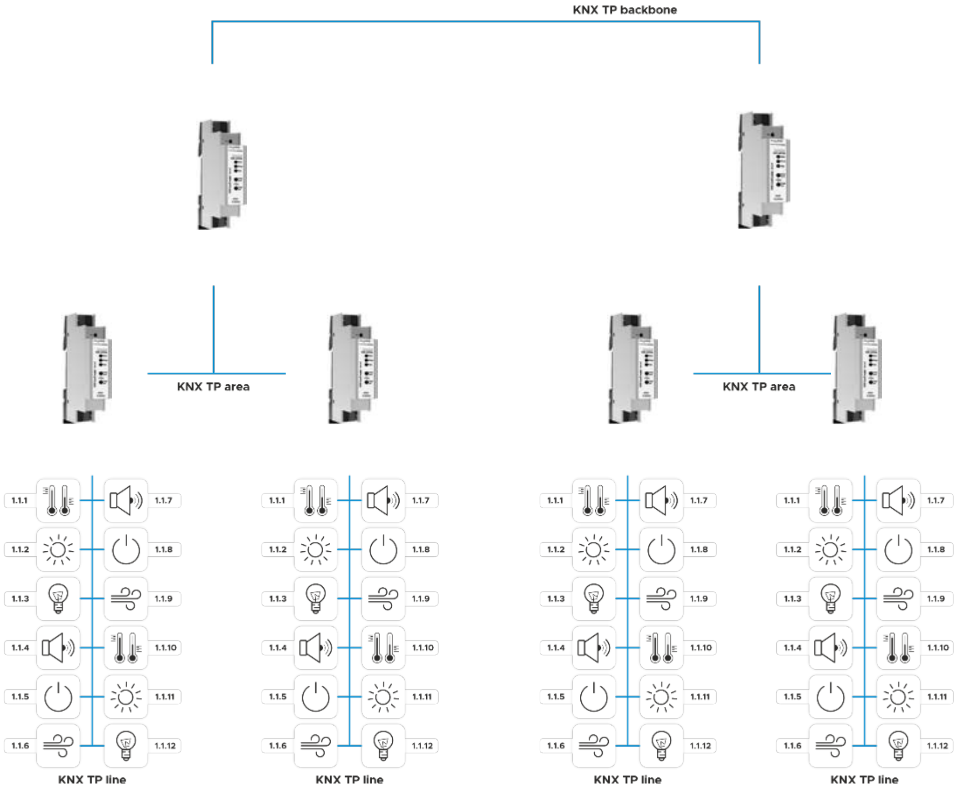
4.1 Line coupler



The individual address of the Device corresponds to the form x.y.0 (x, y: 1 … 15).

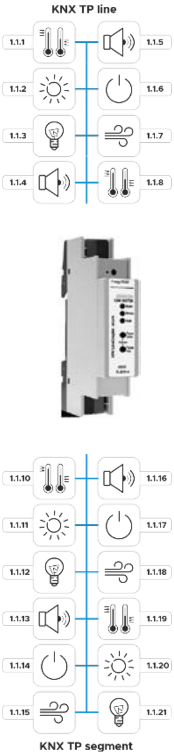
Thus the device functions as line coupler.

4.2 Area coupler



The individual address of the Device corresponds to the form x.0.0
(x: 1 … 15). Thus the device functions as area coupler.

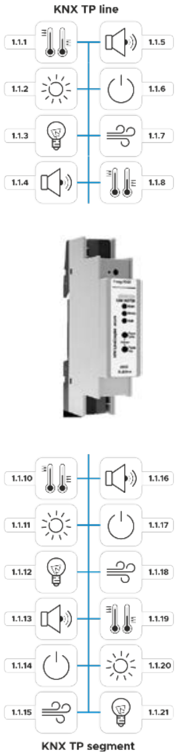
4.3 Function as segment coupler



The individual address of the Device corresponds to the form x.y.z
(x, y: 1 … 15, z: 1 … 255). Thus the device functions as segment coupler.

If the segment is extended with a new device, the segment coupler must be downloaded again before a download can be performed on the new device.

4.4 Function as repeater (only with ETS5)



The individual address of the Device corresponds to the form x.y.z
(x, y: 1 … 15, z: 1 … 255). Thus the device functions as repeater.

The filter settings in the parameter dialog of the ETS are ineffective in repeater mode.

5 KNX Security

The KNX standard was extended by KNX Security to protect KNX installations from unauthorized access.

KNX Security reliably prevents the monitoring of communication as well as the manipulation of the system.

The specification for KNX Security distinguishes between KNX IP Security and KNX Data Security. KNX IP Security protects the communication over IP while on KNX TP the communication remains unencrypted.

Thus, KNX IP Security can also be used in existing KNX systems and with non-secure KNX TP devices.

KNX Data Security describes the encryption on telegram level. This means that the telegrams on the twisted pair bus or via RF (radio frequency) are also encrypted.

Encrypted telegrams are longer than the previously used unencrypted ones. For secure programming via the bus, it is therefore necessary that the interface used (e.g. USB) and any intermediate line couplers support the so called KNX Long Frames.

5.1 Security Proxy

A Security Proxy translates secure group communication from one side (e.g. secured KNX TP line) into unsecured group communication on the other side (e.g. unsecured KNX TP area) and vice versa.

6 ETS database

The device supports KNX Data Security to protect the device against unauthorized access from the KNX bus.

If the device is programmed via the KNX bus, this is done with encrypted telegrams.

6.1 ETS 5

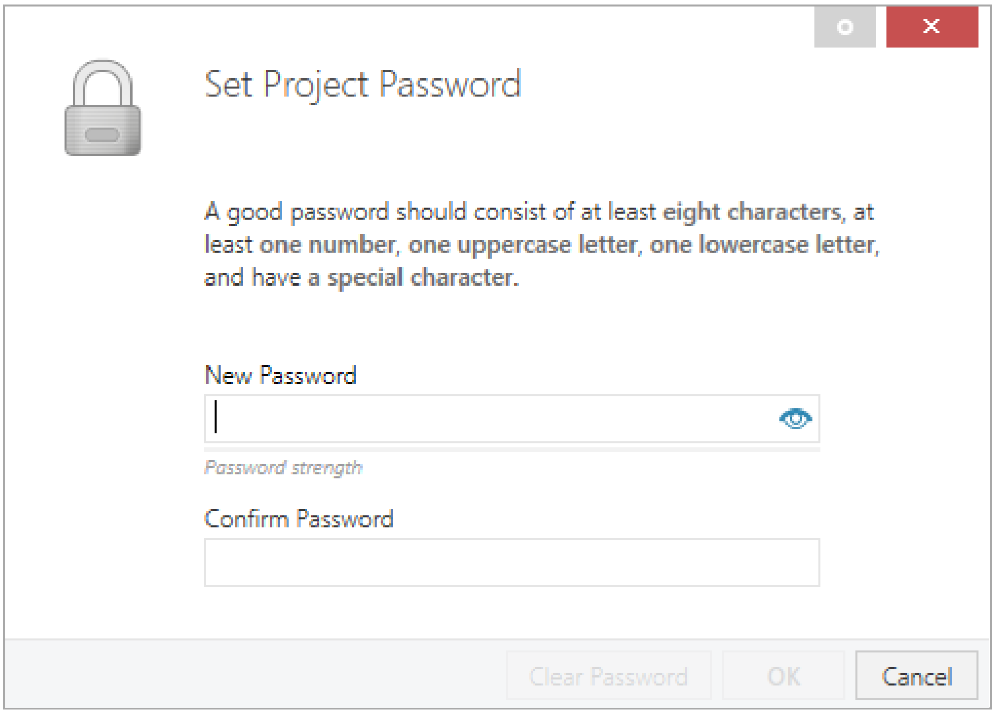
The ETS 5 database supports only KNX Data Security. The functionality of Security Proxy and Segment Coupler is not supported.

6.2 ETS 6

The ETS 6 database supports KNX Data Security as well as the functionality of Security Proxy and Segment Coupler.

6.3 Secure commissioning

If the first product is inserted into a project with KNX Security, the ETS prompts you to enter a project password.



Set Project Password

A good password should consist of at least eight characters, at least one number, one uppercase letter, one lowercase letter, and have a special character.

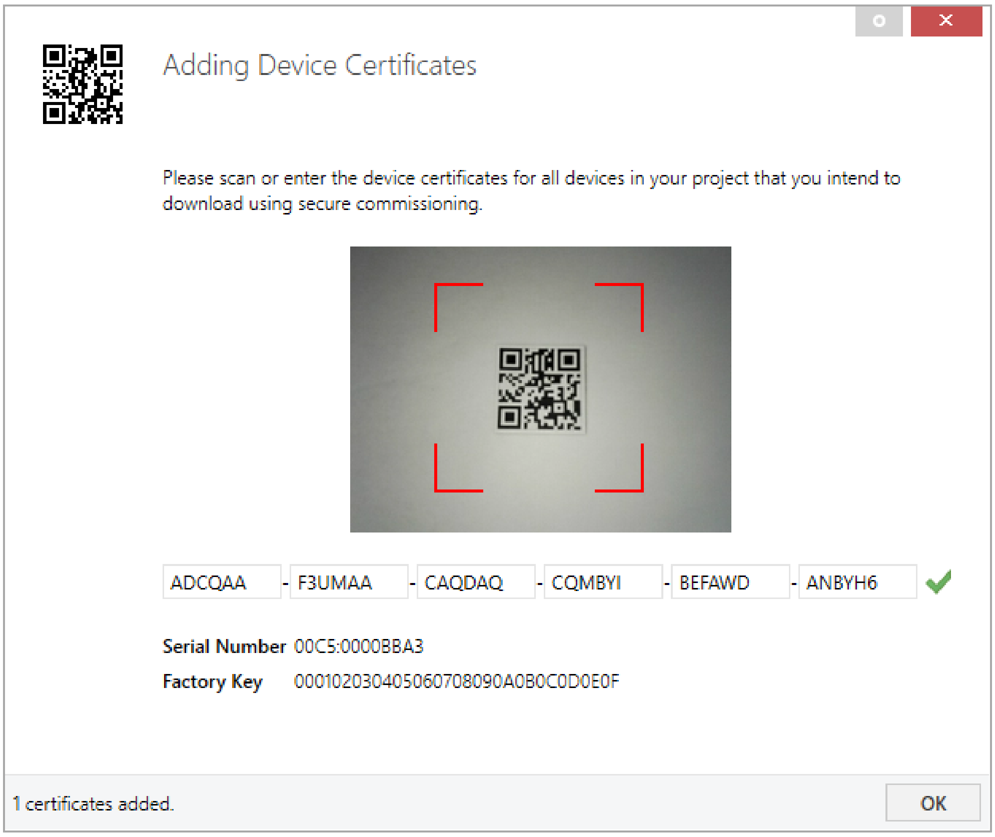
New Password

Password strength

Confirm Password

This password protects the ETS project from unauthorized access. This password is not a key that is used for KNX communication. The entry of the password can be bypassed with "Cancel", but this is not recommended for security reasons.

ETS requires a device certificate for each device with KNX Security that is created in the ETS. This certificate contains the serial number of the device as well as an initial key (FDSK = Factory Default Setup Key).



Adding Device Certificates

Please scan or enter the device certificates for all devices in your project that you intend to download using secure commissioning.

ADCQAA - F3UMAA - CAQDAQ - CQMBYI - BEFAWD - ANBYH6 ✓

Serial Number 00C5:0000BBA3

Factory Key 000102030405060708090A0B0C0D0E0F

1 certificates added.

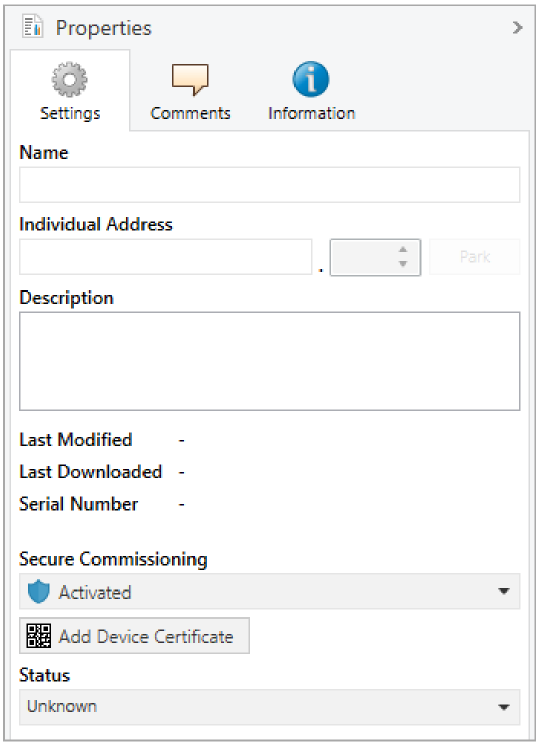
The certificate is printed as text on the device. It can also be scanned from the printed QR code via a webcam.

The list of all device certificates can be managed in the ETS panel Reports – Project Security.

This initial key is required to safely put a device into operation from the start. Even if the ETS download is recorded by a third party, the third party has no access to the secured devices afterwards. During the first secure download, the initial key is replaced by the ETS with a new key that is generated individually for each device. This prevents persons or devices who may know the initial key from accessing the device. The initial key is reactivated after a reset to factory default settings.

The serial number in the certificate enables the ETS to assign the correct key to a device during a download.

In the ETS project in the properties of the device, secure commissioning can be activated and the device certificate can be added:



Name

Individual Address

Description

Last Modified -

Last Downloaded -

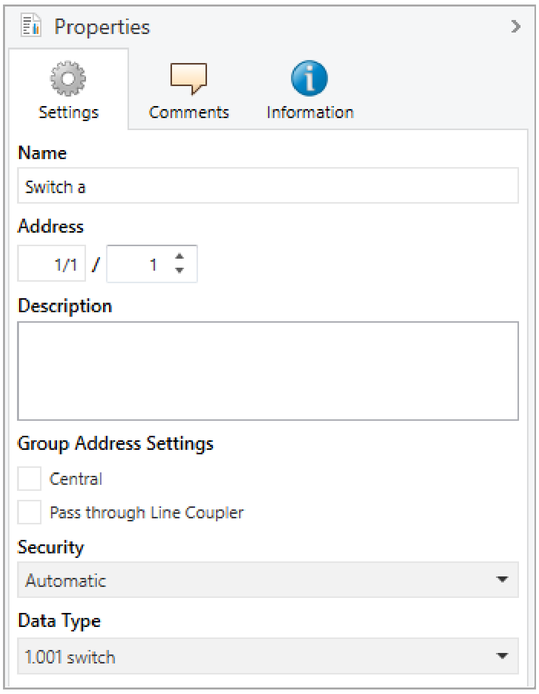
Serial Number -

Secure Commissioning: Activated

Status: Unknown

6.4 *Secure group communication*

Each object of the device can communicate either encrypted or unencrypted. The encryption is set under "Security" in the properties of the used group address:



Name: Switch a

Address: 1/1 / 1

Description

Group Address Settings

□ Central

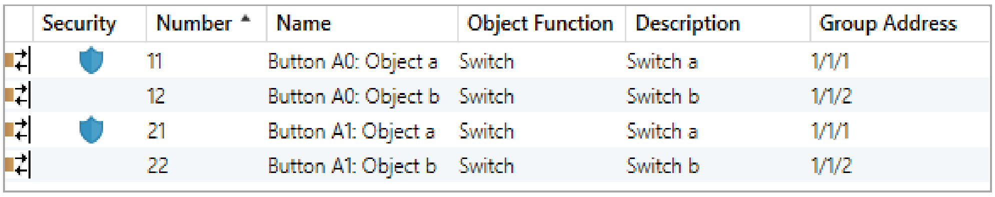
□ Pass through Line Coupler

Security: Automatic

Data Type: 1.001 switch

The setting "Automatic" activates encryption if both objects to be connected can communicate encrypted. Otherwise encrypted communication between the objects is not possible.

In the overview of communication objects in the ETS project, secured objects can be recognized by a shield symbol:

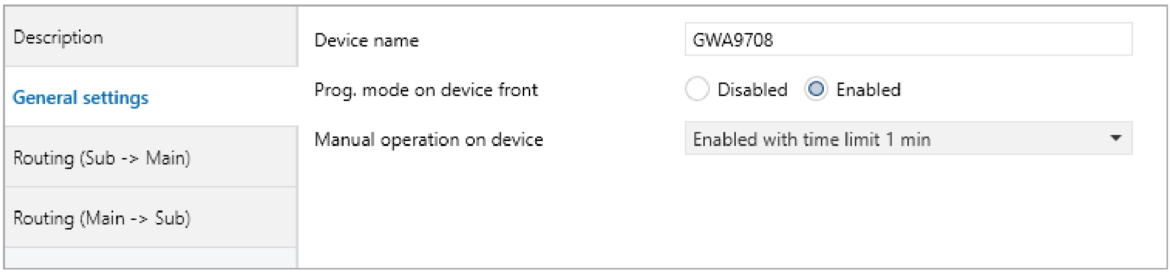


Security	Number ▲	Name	Object Function	Description	Group Address
🛡	11	Button A0: Object a	Switch	Switch a	1/1/1
	12	Button A0: Object b	Switch	Switch b	1/1/2
🛡	21	Button A1: Object a	Switch	Switch a	1/1/1
	22	Button A1: Object b	Switch	Switch b	1/1/2

A separate key is automatically generated by the ETS for each secured group address. These keys can also be checked in the ETS panel Reports – Project Security. To enable all devices to communicate with a secure group address, the keys must be known to all. Therefore a download must be made into all devices that use this group address when a key is created or changed. A key is changed by the ETS e.g. when the encryption of a group address is switched off and on again.

Telegrams from the bus that do not address the device as a device are forwarded or blocked according to the filter settings (parameters and filter table). It does not matter whether the telegrams are unencrypted or encrypted. The forwarding is done exclusively on the basis of the destination address. The security properties are checked by the respective recipient.

6.5 General settings



Description

General settings

Routing (Sub -> Main)

Routing (Main -> Sub)

Device name	GWA9708
Prog. mode on device front	○ Disabled ● Enabled
Manual operation on device	Enabled with time limit 1 min

Device name *(30 characters)*

Any name can be assigned.

The device name should be meaningful, e.g. “Living room EG”. This helps the clarity in the ETS project.

Prog. mode on device front

In addition to the normal programming button ❸ the device allows activating the programming mode on the device front without opening the switchboard cover. The programming mode can be activated and deactivated via pressing simultaneously both buttons ❼ and ❽.

This feature can be enabled and disabled via the parameter “Prog. mode on device front”. The recessed programming button ❸ (next to the Programming LED ❷) is always enabled and not influenced by this parameter.

Manual operation on device

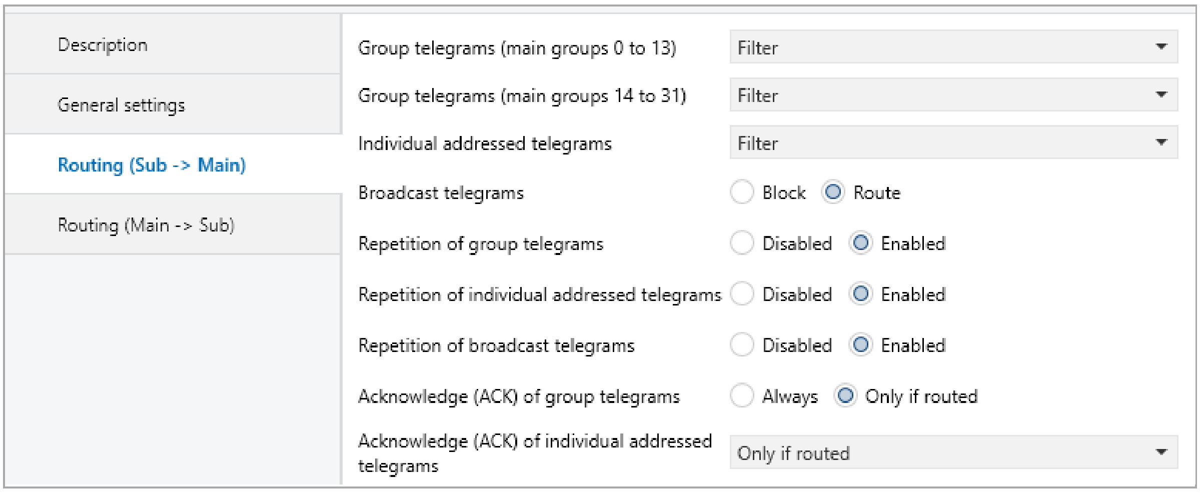
This parameter is used to configure manual operation on the device. The manual operation mode can be blocked or activated (with or without time limit). The time limit defines the duration until the automatic return from manual operation back to the normal operating mode.

The following configuration options are available:

- Disabled
- Enabled with time limit 1 min
- Enabled with time limit 10 min
- Enabled with time limit 30 min
- Enabled without time limit

The activated manual operation can reduce the security of the installation.

6.6 Routing (Sub -> Main)



Group telegrams (main groups 0 to 13)	Filter
Group telegrams (main groups 14 to 31)	Filter
Individual addressed telegrams	Filter
Broadcast telegrams	○ Block ● Route
Repetition of group telegrams	○ Disabled ● Enabled
Repetition of individual addressed telegrams	○ Disabled ● Enabled
Repetition of broadcast telegrams	○ Disabled ● Enabled
Acknowledge (ACK) of group telegrams	○ Always ● Only if routed
Acknowledge (ACK) of individual addressed telegrams	Only if routed

Group telegrams (main groups 0 to 13)

- Block
  No group telegrams of this main group are routed to the main line.
- Route
  All group telegrams of this main group are routed to the main line independent of the filter table.
- Filter
  The filter table is used to check whether or not the received group telegram should be routed to the main line.

The setting “Route” should only be used for test purposes.

Group telegrams (main groups 14 to 31)

- Block
  No group telegrams of main groups 14 to 31 are routed to the main line.
- Route
  All group telegrams of main groups 14 to 31 are routed to the main line.
- Filter
  The filter table is used to check whether or not the received group telegram should be routed to the main line.

The setting “Route” should only be used for test purposes.

Individually addressed telegrams

- Block
  No individually addressed telegrams are routed to the main line.
- Route
  All individually addressed telegrams are routed to the main line.
- Filter
  The individual address is used to check whether the received individually addressed telegram should be routed to the main line.

The setting “Route” should only be used for test purposes.

Broadcast telegrams

- Block
  No received broadcast telegrams are routed to the main line.
- Route
  All received broadcast telegrams are routed to the main line.

Repetition of group telegrams

- Disabled
  The received group telegram is not resent to the main line in case of a fault.
- Enabled
  The received group telegram is resent up to three times in case of a fault.

If repetitions are enabled, it is possible that the device suppresses the repetitions dynamically in order to limit a high bus load.

Repetition of individually addressed telegrams

- Disabled
  The received individually addressed telegram is not resent to the main line in case of a fault.
- Enabled
  The received individually addressed telegram is resent up to three times in case of a fault.

If repetitions are enabled, it is possible that the device suppresses the repetitions dynamically in order to limit a high bus load.

Repetition of broadcast telegrams

- Disabled
  The received broadcast telegram is not resent to the main line in case of a fault.
- Enabled
  The received broadcast telegram is resent up to three times in case of a fault.

If repetitions are enabled, it is possible that the device suppresses the repetitions dynamically in order to limit a high bus load.

Acknowledge (ACK) of group telegrams

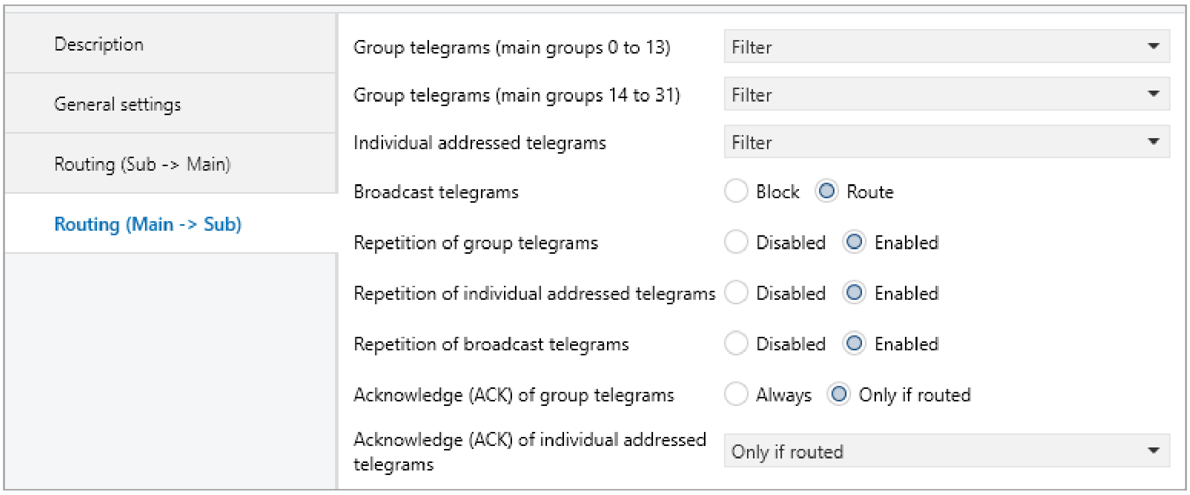
- Always
  A acknowledge is generated for every received group telegram (from the sub line).
- Only if routed
  A acknowledge is only generated for received group telegrams (from the sub line) if they are routed to the main line.

Acknowledge (ACK) of individually addressed telegrams

- Always
  A acknowledge is generated for every received individual addressed telegram
  (from the sub line).
- Only if routed
  A acknowledge is only generated for received individually addressed group telegrams
  (from the sub line) if they are routed to the main line.
- Answer with NACK
  Every received individually addressed telegram (from the sub line) is responded to with NACK (Not acknowledge). This means that communication with individually addressed telegrams on the corresponding KNX line is not possible. Group communication (group telegrams) is not affected. This setting can be used to block attempts at manipulation.

ℹ *When using "Answer with NACK" an access to the device via the KNX sub line is no longer possible. The configuration must be performed via the main line.*

6.7 Routing (Main -> Sub)



Description

General settings

Routing (Sub -> Main)

Routing (Main -> Sub)

Group telegrams (main groups 0 to 13)	Filter
Group telegrams (main groups 14 to 31)	Filter
Individual addressed telegrams	Filter
Broadcast telegrams	○ Block ● Route
Repetition of group telegrams	○ Disabled ● Enabled
Repetition of individual addressed telegrams	○ Disabled ● Enabled
Repetition of broadcast telegrams	○ Disabled ● Enabled
Acknowledge (ACK) of group telegrams	○ Always ● Only if routed
Acknowledge (ACK) of individual addressed telegrams	Only if routed

Group telegrams (main groups 0 to 13)

- Block
  No group telegrams of this main group are routed to the sub line.
- Route
  All group telegrams of this main group are routed to the sub line independent of the filter table.
- Filter
  The filter table is used to check whether or not the received group telegram should be routed to the sub line.

The setting "Route" should only be used for test purposes.

Group telegrams (main groups 14 to 31)

- Block
  No group telegrams of main groups 14 to 31 are routed to the sub line.
- Route
  All group telegrams of main groups 14 to 31 are routed to the sub line.
- Filter
  The filter table is used to check whether or not the received group telegram should be routed to the sub line.

The setting "Route" should only be used for test purposes.

Individually addressed telegrams

- Block
  No individually addressed telegrams are routed to the sub line.
- Route
  All individually addressed telegrams are routed to the sub line.
- Filter
  The individual address is used to check whether the received individually addressed telegram should be routed to the sub line.

ℹ *The setting “Route” should only be used for test purposes.*

Broadcast telegrams

- Block
  No received broadcast telegrams are routed to the sub line.
- Route
  All received broadcast telegrams are routed to the sub line.

Repetition of group telegrams

- Disabled
  The received group telegram is not re-sent to the sub line in case of a fault.
- Enabled
  The received group telegram is resent up to three times in case of a fault.

ℹ *If repetitions are enabled, it is possible that the device suppresses the repetitions dynamically in order to limit a high bus load.*

Repetition of individually addressed telegrams

- Disabled
  The received individually addressed telegram is not resent to the sub line in case of a fault.
- Enabled
  The received individually addressed telegram is resent up to three times in case of a fault.

ℹ *If repetitions are enabled, it is possible that the device suppresses the repetitions dynamically in order to limit a high bus load.*

Repetition of broadcast telegrams

- Disabled
  The received broadcast telegram is not resent to the sub line in case of a fault.
- Enabled
  The received broadcast telegram is re-sent up to three times in case of a fault.

ℹ *If repetitions are enabled, it is possible that the device suppresses the repetitions dynamically in order to limit a high bus load.*

Acknowledge (ACK) of group telegrams

- Always
  A acknowledge is generated for every received group telegram (from the main line).
- Only if routed
  A acknowledge is only generated for received group telegrams (from the main line) if they are routed to the sub line.

Acknowledge (ACK) of individually addressed telegrams

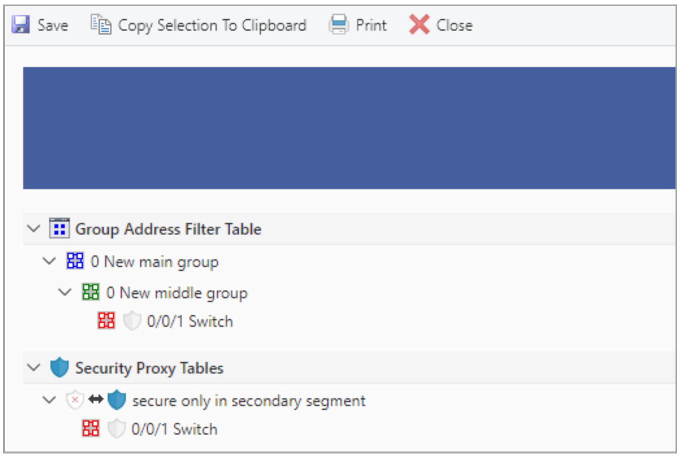
- Always
  A acknowledge is generated for every received individual addressed telegram (from the main line).
- Only if routed
  A acknowledge is only generated for received individually addressed group telegrams (from the main line) if they are routed to the sub line.
- Answer with NACK
  Every received individually addressed telegram (from the main line) is responded to with NACK (Not acknowledge). This means that communication with individually addressed telegrams on the corresponding KNX line is not possible. Group communication (group telegrams) is not affected. This setting can be used to block attempts at manipulation.

ℹ *When using “Answer with NACK” an access to the device via the KNX main line is no longer possible. The configuration must be performed via the sub line.*

6.8 *Filter Table / Security Proxy Tables*

The filter table is created automatically by the ETS. The group addresses of the telegrams that are to be forwarded via the coupler are included in the filter table for this purpose. The content of the filter table can be displayed via the preview.

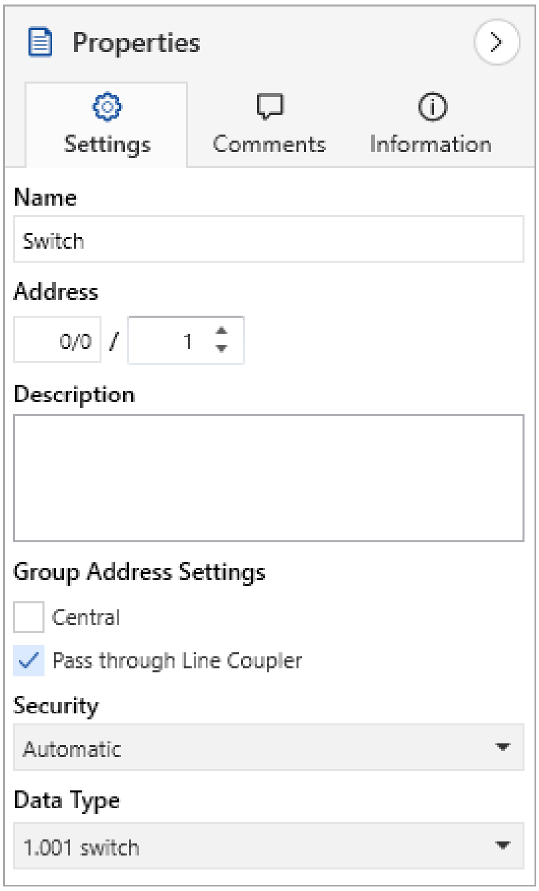
Also the security proxy tables are displayed here.



Group Address Filter Table
- 0 New main group
  - 0 New middle group
    - 0/0/1 Switch

Security Proxy Tables
- secure only in secondary segment
  - 0/0/1 Switch

The filter table can be extended by manually adding group addresses. For this purpose, “Pass through Line Coupler” must be activated in the properties window of the corresponding group address.



Name: Switch

Address: 0/0 / 1

Description:

Group Address Settings

☐ Central

☑ Pass through Line Coupler

Security: Automatic

Data Type: 1.001 switch

code 70207071

LAST REVISION 01/2026

Punto di contatto indicato in adempimento ai fini delle direttive e regolamenti UE applicabili:
Contact details according to the relevant European Directives and Regulations:
GEWISS S.p.A. Via D.Bosatelli, 1 IT-24069 Cenate Sotto (BG) Italy tel: +39 035 946 111 E-mail: qualitymarks@gewiss.com

According to applicable UK regulations, the company responsible for placing the goods in UK market is:
**GEWISS UK LTD - Unity House, Compass Point Business Park, 9 Stocks Bridge Way, ST IVES
Cambridgeshire, PE27 5JL, United Kingdom tel: +44 1954 712757 E-mail: gewiss-uk@gewiss.com**

☎ **+39 035 946 111**
8:30 - 12:30 / 14:00 - 18:00
lunedì - venerdì / monday - friday

www.gewiss.com