

Compact KNX RF/TP coupler with support of
KNX Data Security, Security Proxy and Segment Coupler

KNX RF/TP Coupler 673.1 *secure*

Operation and installation manual



(Art. # 5474)

WEINZIERL ENGINEERING GmbH
Achatz 3-4
84508 Burgkirchen an der Alz
GERMANY

Tel.: +49 8677 / 916 36 – 0
E-Mail: info@weinzierl.de
Web: www.weinzierl.de

Content

1	Application	3
2	Installation and connection	3
2.1	KNX programming mode.....	4
2.2	Manual operation and status display	4
3	Reset to factory default settings.....	6
3.1	Factory default settings	6
4	Wiring scheme	6
4.1	Line Coupler	7
4.2	Segment Coupler	9
5	KNX Security	10
5.1	Security Proxy.....	10
6	ETS database	11
6.1	ETS 5.....	11
6.2	ETS 6.....	11
6.3	Secure commissioning.....	11
6.4	Secure group communication.....	14
6.5	Description.....	16
6.6	General settings.....	16
6.7	Routing TP->RF	17
6.8	Routing RF->TP.....	19
6.9	Filter Table / Security Proxy Tables.....	21

1 Application

The KNX RF/TP Coupler 673.1 secure is a compact KNX radio coupler. It connects KNX RF devices of a radio line with the KNX Bus Twisted Pair.

The device has an extended filter table for main group 0 ... 31. The coupler supports KNX Long Frames and is compatible with the ETS® software ETS 5 or higher.

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.

The device supports KNX Data Security. The functionality of Security Proxy and Segment Coupler is only supported with the ETS 6 database.

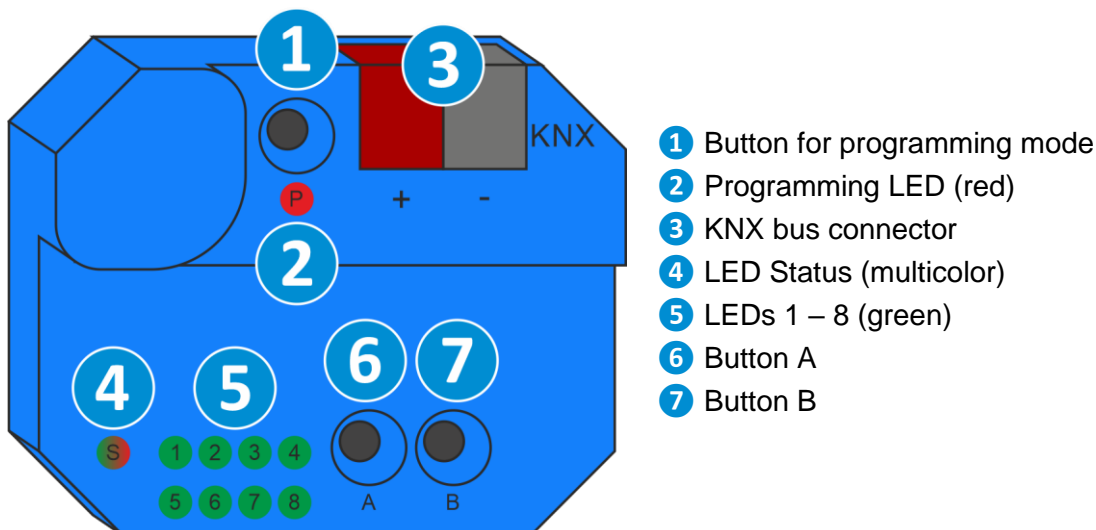
2 Installation and connection

Mounting can be recessed in the wall and thus almost “invisible”, because the housing has the right size for mounting in a standard flush-mounted box.

When selecting the mounting location, the range of the radio devices to be connected to the device must be taken into account. Shielding objects (e.g. metal cabinets) or interfering transmitters (e.g. computers, electronic transformers, ballasts) near the gateway should be avoided.

The device is connected to the KNX bus using a bus terminal. The correct polarity of the terminal according to the marking on the device must be observed.

The KNX RF/TP Coupler 673.1 *secure* has the following operating elements and displays:



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 ①.

When the programming mode is active, the programming LED ② lights up red.

2.2 Manual operation and status display

The LED Status ④ lights up green when KNX bus voltage is present. This LED flashes red if the application is not running, e.g. after an aborted ETS download. If manual operation is active, this is indicated by the LED Status ④ lighting up orange.

Summary of the states of the LED Status ④:

LED Status	Meaning
LED lights green	The device operates in normal operating mode.
LED flashes red	The device is not loaded correctly e.g. after aborting a download.
LED lights orange	Manual operation is active.
LED briefly orange	RF telegrams from another domain received.

LEDs 1 – 4 ⑤ indicate TP telegram traffic.

LEDs 5 – 8 ⑤ indicate RF telegram traffic. If RF telegrams are received from another domain, the LED Status ④ flashes orange briefly in addition.

Summary of the states of the LEDs 1 – 8 ⑤:

LED Status	Meaning
LEDs 1 – 4 briefly green	Manual operation is not active. Telegram traffic via KNX TP.
LEDs 5 – 8 briefly green	Manual operation is not active. Telegram traffic via KNX RF.

2.2.1 Manual operation TP

Briefly pressing button A ⑥ activates manual operation for mode TP.

Pressing button A ⑥ briefly deactivates/activates the forwarding of the group telegrams. This is indicated by LEDs 1 and 2 ⑤.

Pressing button B ⑦ briefly deactivates/activates the forwarding of the physically addressed telegrams and the broadcast telegrams. This is indicated by LEDs 3 and 4 ⑤.

Pressing button A ⑥ or button B ⑦ for a long time exits manual operation.

Manual operation can be locked in the ETS database.

Summary of the states of the LEDs 1 – 4 **5**:

LED Status	Meaning
LEDs 1 and 2 light green	Manual operation is active. Forwarding of group telegrams via KNX TP is active.
LEDs 1 and 2 off	Manual operation is active. Forwarding of group telegrams via KNX TP is not active.
LEDs 3 and 4 light green	Manual operation is active. Forwarding of physically addressed telegrams and broadcast telegrams via KNX TP is active.
LEDs 3 and 4 off	Manual operation is active. Forwarding of physically addressed telegrams and broadcast telegrams via KNX TP is not active.

2.2.2 Manual operation RF

Briefly pressing button B **7** activates manual operation for mode RF.

Pressing button A **6** briefly deactivates/activates the forwarding of the group telegrams. This is indicated by LEDs 5 and 6 **5**.

Pressing button B **7** briefly deactivates/activates the forwarding of the physically addressed telegrams, the broadcast telegrams and the system broadcast telegrams. This is indicated by LEDs 7 and 8 **5**.

Pressing button A **6** or button B **7** for a long time exits manual operation.

Manual operation can be locked in the ETS database.

Summary of the states of the LEDs 5 – 8 **5**:

LED Status	Meaning
LEDs 5 and 6 light green	Manual operation is active. Forwarding of group telegrams via KNX RF is active.
LEDs 5 and 6 off	Manual operation is active. Forwarding of group telegrams via KNX RF is not active.
LEDs 7 and 8 light green	Manual operation is active. Forwarding of physically addressed telegrams, broadcast telegrams and system broadcast telegrams via KNX RF is active.
LEDs 7 and 8 off	Manual operation is active. Forwarding of physically addressed telegrams, broadcast telegrams and system broadcast telegrams via KNX RF is not active.

3 Reset to factory default settings

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

- Disconnect the KNX bus connector **3** from the device.
- Press the KNX programming button **1** and keep it pressed down.
- Reconnect the KNX bus connector **3** to the device.
- Keep the KNX programming button **1** pressed for at least another 6 seconds.
- A short flashing of all LEDs (**2 4 5**) 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 TP->RF

Group telegrams: Filter

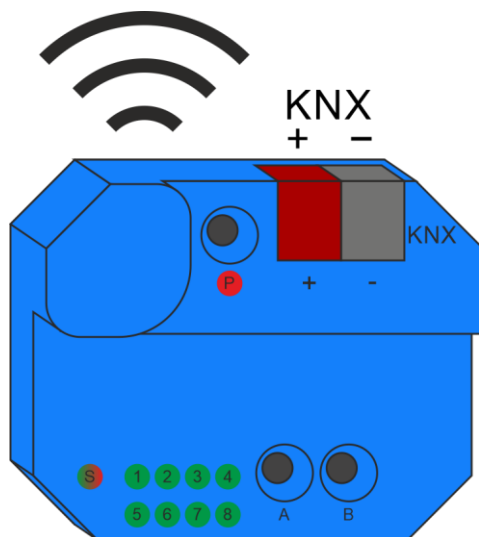
Individual addressed telegrams: Filter

Routing RF->TP

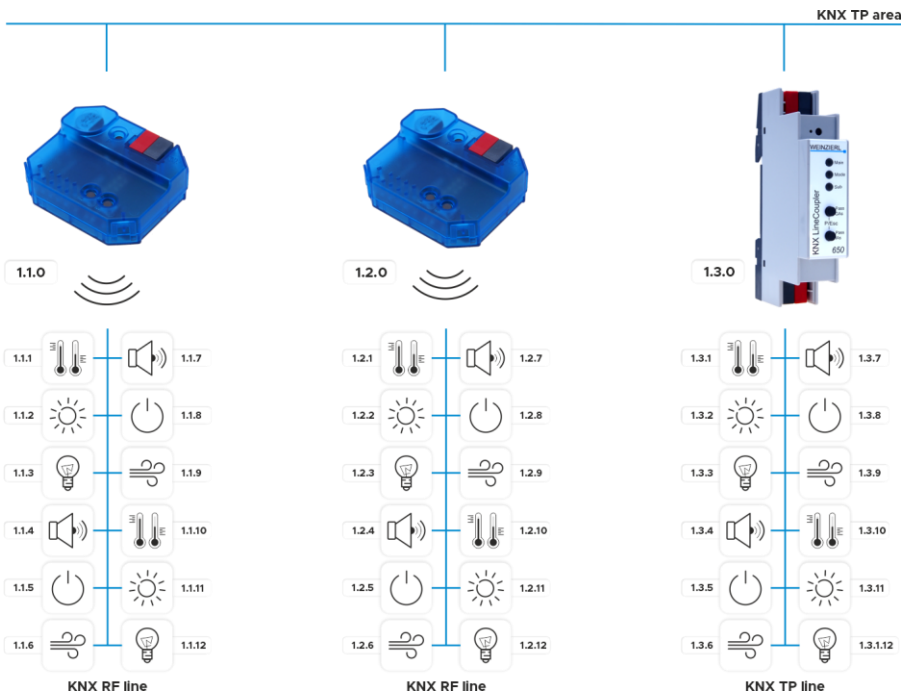
Group telegrams: Filter

Individual addressed telegrams: Filter

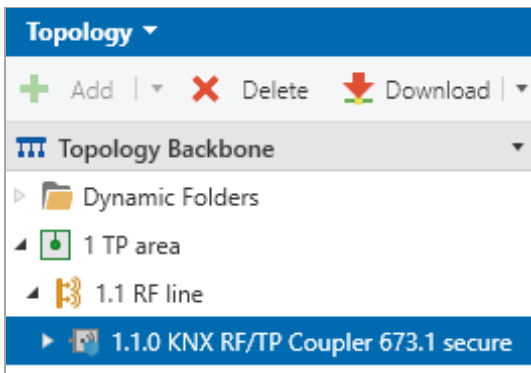
4 Wiring scheme



4.1 Line Coupler



The individual address of the KNX RF/TP Coupler 673.1 *secure* corresponds to the form x.y.0 (x, y: 1 ... 15). Thus the device functions as a line coupler.



The device functions as a line coupler only if its individual address has the form x.y.0.

The KNX RF/TP Coupler 673.1 *secure* 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.

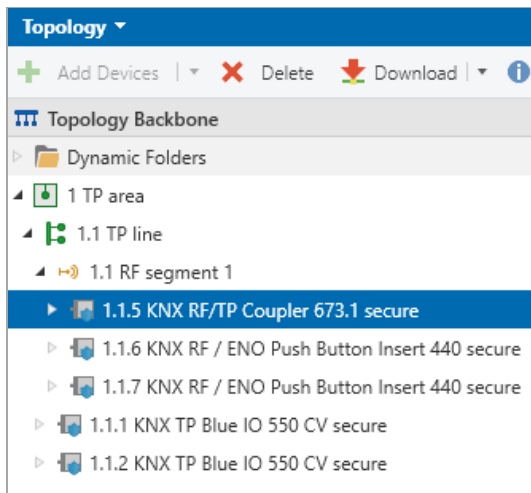
Wireless extension of a KNX line



4.2 Segment Coupler



The individual address of the KNX RF/TP Coupler 673.1 *secure* corresponds to the form x.y.z (x, y: 1 ... 15, z: 1 ... 255). Thus the device functions as a segment coupler.



The device functions as a segment coupler only if its individual address has the form x.y.z.

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 RF line) into unsecured group communication on the other side (e.g. unsecured KNX TP area) and vice versa.

6 ETS database

The ETS database (for ETS 5.7 or newer) can be downloaded from the product website of the KNX RF/TP Coupler 673.1 *secure* (www.weinzierl.de) or from the ETS online catalogue.

The KNX RF/TP Coupler 673.1 *secure* 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

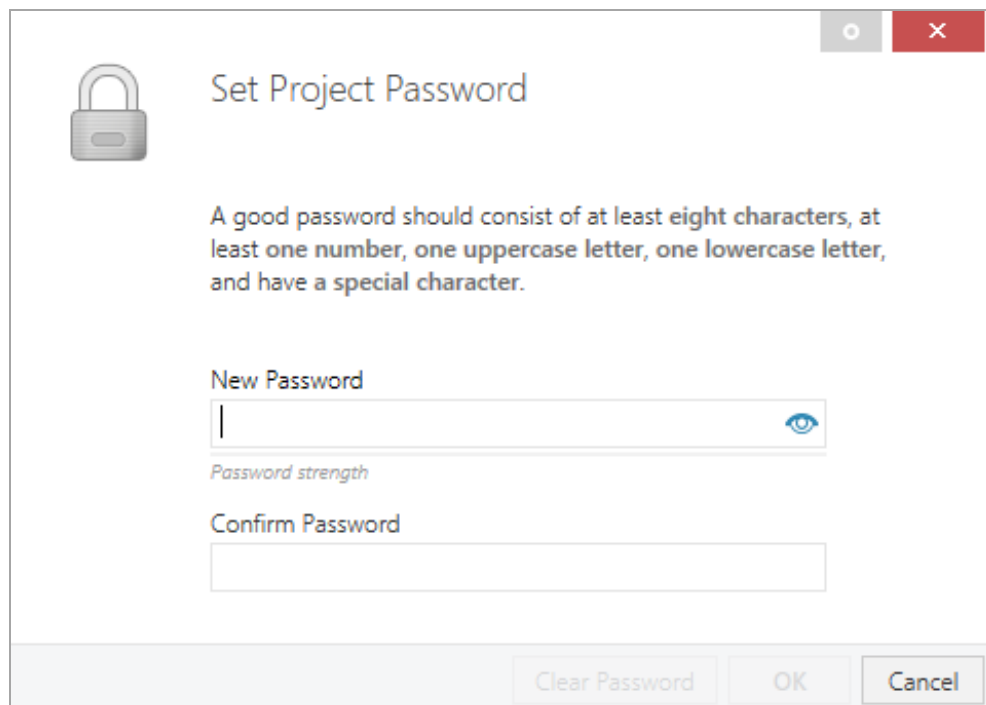
The ETS 5 database supports only KNX Data Security. The functionality of Security Proxy and Segment Coupler is not supported.

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**.

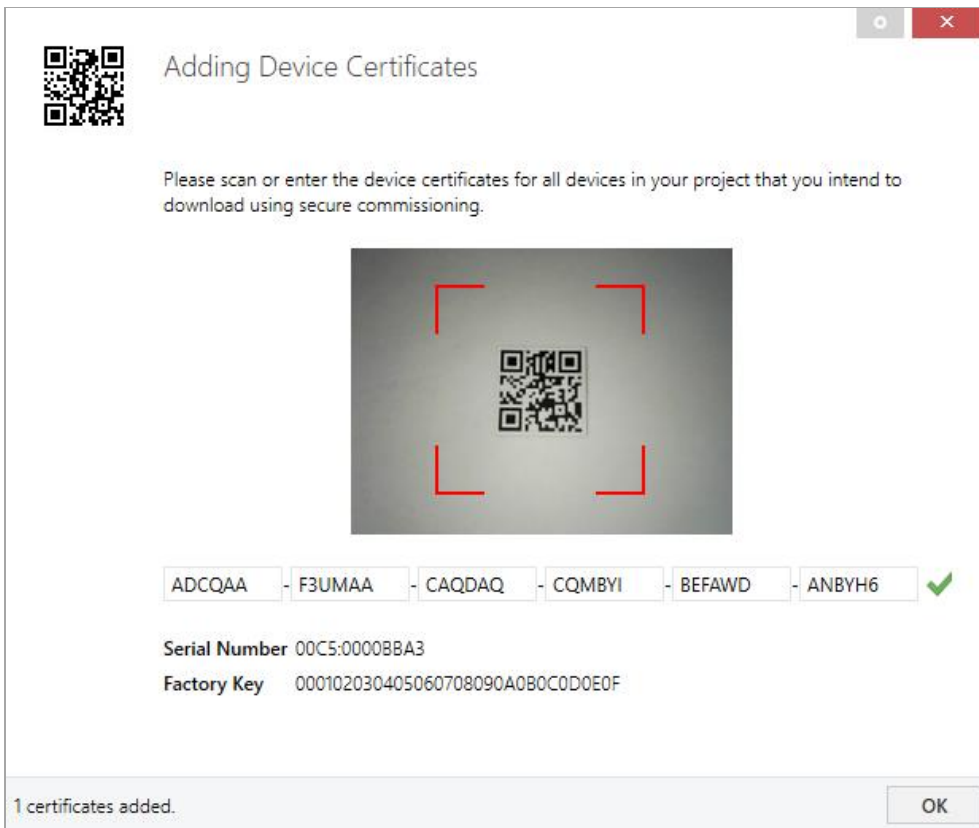
New Password

Confirm Password

Clear Password OK Cancel

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).



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.

By marking the RF line in the tree structure of the topology view of the ETS project, the overview “Properties” appears on the right side of the ETS window. Under Properties menu item “Settings” the domain address of the line can be changed.

The screenshot shows the 'Properties' dialog box with the 'Settings' tab selected. The fields are as follows:

- Name:** RF line
- Address:** 1 . 2
- Description:** (Empty text area)
- Status:** Unknown
- Medium:** RF
- Domain Address:** 00FA:A4083A1C (with a 'Generate new' button)

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:

The screenshot shows the 'Properties' dialog box with the 'Settings' tab selected. The fields are as follows:

- Name:** Switch a
- Address:** 1/1 / 1
- Description:** (Empty text area)
- 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 KNX RF/TP Coupler 673.1 secure 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 Description

--- KNX RF/TP Coupler 673.1 secure > Description

Description	KNX RF/TP Coupler 673.1 secure	
General settings	Compact KNX RF/TP coupler with support of KNX Data Security, Security Proxy and Segment Coupler	WEINZIERL
Routing TP->RF		
Routing RF->TP		

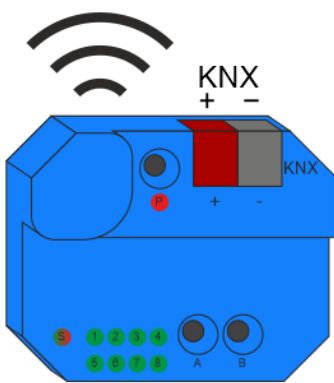
The KNX RF/TP Coupler 673.1 secure is a compact KNX radio coupler. It connects KNX RF devices of a radio line with the KNX Bus Twisted Pair.

The device has an extended filter table for main group 0 ... 31. The coupler supports long frames and is compatible with the ETS® software ETS 5 or higher.

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.

The device supports KNX Data Security, Security Proxy and Segment Coupler functionality.



Wiring scheme:

Please consult device data sheet and manual for further information.

Contact:

WEINZIERL ENGINEERING GmbH
 Achatz 3-4
 84508 Burgkirchen an der Alz
 GERMANY
www.weinzierl.de
info@weinzierl.de

This page shows the device description and the corresponding connection diagram.

6.6 General settings

--- KNX RF/TP Coupler 673.1 secure > General settings

Description	Device name	<input type="text" value="KNX RF/TP Coupler 673.1 secure"/>
General settings	Manual operation on device	<input type="text" value="Enabled with time limit 1 min"/>
Routing TP->RF		
Routing RF->TP		

Device name (30 characters)

Any name can be assigned to the KNX RF/TP Coupler 673.1 *secure*. The device name should be meaningful, e.g. "Living room EG". This helps the clarity in the ETS project.

Manual control on the 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.

6.7 Routing TP->RF

--- KNX RF/TP Coupler 673.1 secure > Routing TP->RF		
Description	Group telegrams	Filter
General settings	Individual addressed telegrams	Filter
Routing TP->RF	System broadcast telegrams	<input type="radio"/> Block <input checked="" type="radio"/> Route
Routing RF->TP	Broadcast telegrams	<input type="radio"/> Block <input checked="" type="radio"/> Route
	Acknowledge (ACK) of group telegrams	<input type="radio"/> Always <input checked="" type="radio"/> If routed

Group telegrams

The following settings are possible:

- Block
No group telegram is forwarded to the RF line.
- Route
All group telegrams are forwarded to the RF line regardless of the filter table.
- Filter
The filter table is used to decide whether the received group telegram is to be forwarded to the RF line.



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

Individual addressed telegrams

The following settings are possible:

- Block
No individual addressed telegram is forwarded to the RF line.
- Route
All individual addressed telegrams are forwarded to the RF line.
- Filter
The destination address is used to check whether the received individual addressed telegram is forwarded to the RF line.



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

System broadcast telegrams

The following settings are possible:

- Block
No received system broadcast telegram is forwarded to the RF line.
- Route
All received system broadcast telegrams are forwarded to the RF line.

Broadcast telegrams

The following settings are possible:

- Block
No received broadcast telegram is forwarded to the RF line.
- Route
All received broadcast telegrams are forwarded to the RF line.

Acknowledge (ACK) of group telegrams

The following settings are possible:

- Always
For received group telegrams (from the TP line) always send an acknowledge.
- If routed
For received group telegrams (from the TP line) an acknowledge is sent only when telegram is forwarded to the RF line.

6.8 Routing RF->TP

--- KNX RF/TP Coupler 673.1 secure > Routing RF->TP		
Description	Group telegrams	Filter
General settings	Individual addressed telegrams	Filter
Routing TP->RF	System broadcast telegrams	<input type="radio"/> Block <input checked="" type="radio"/> Route
Routing RF->TP	Broadcast telegrams	<input type="radio"/> Block <input checked="" type="radio"/> Route
	Repetition of group telegrams	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
	Repetition of individual addressed telegrams	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
	Repetition of broadcast telegrams	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled

Group telegrams

The following settings are possible:

- Block
No group telegram is forwarded to the TP line.
- Route
All group telegrams are forwarded to the TP line regardless of the filter table.
- Filter
The filter table is used to decide whether the received group telegram is forwarded to the TP line.



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

Individual addressed telegrams

The following settings are possible:

- Block
No individual addressed telegram is forwarded to the TP line.
- Route
All individual addressed telegrams are forwarded to the TP line.
- Filter
The destination address is used to check whether the received individual addressed telegram is forwarded to the TP line.



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

System broadcast telegrams

The following settings are possible:

- Block
No received system broadcast telegram is forwarded to the TP line.
- Route
All received system broadcast telegrams are forwarded to the TP line.

Broadcast telegrams

The following settings are possible:

- Block
No received broadcast telegram is forwarded to the TP line.
- Route
All received broadcast telegrams are forwarded to the TP line.

Repetition of group telegrams

The following settings are possible:

- Disabled
The forwarded group telegram will be not repeated in case of an error in the TP line.
- Enabled
The forwarded group telegram will be repeated up to three times in case of an error.

Repetition of individual addressed telegrams

The following settings are possible:

- Disabled
The forwarded individual addressed telegram will be not repeated in the TP line in case of an error.
- Enabled
The forwarded individual addressed telegram will be repeated up to three times in case of an error.

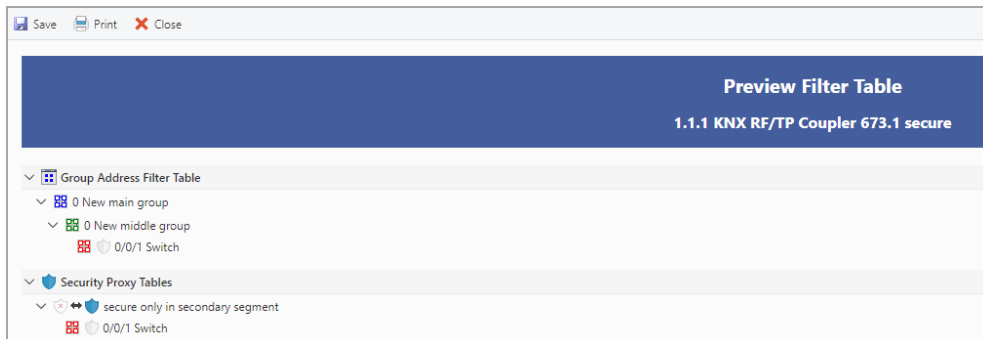
Repetition of broadcast telegrams

The following settings are possible:

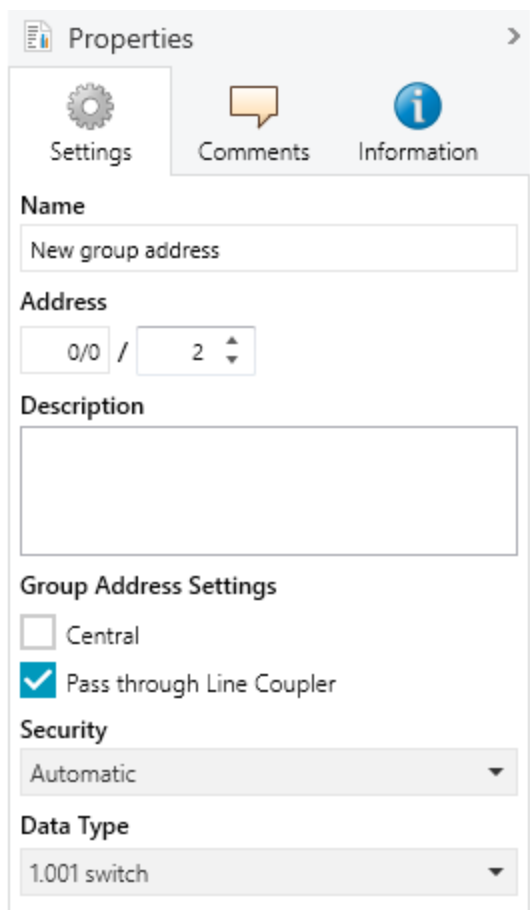
- Disabled
The forwarded broadcast telegram will be not repeated in the TP line in case of an error.
- Enabled
The forwarded broadcast telegram will be repeated up to three times in case of an error.

6.9 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.



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.





WARNING

- The device must be mounted and commissioned by an authorized electrician.
- The prevailing safety rules must be heeded.
- The device must not be opened.
- For planning and construction of electric installations, the relevant guidelines, regulations and standards of the respective country are to be considered.



Product database for ETS 6

www.weinzierl.de/en/products/673.1/ets6

Data sheet

www.weinzierl.de/en/products/673.1/datasheet

CE Declaration

www.weinzierl.de/en/products/673.1/ce-declaration

WEINZIERL ENGINEERING GmbH

Achatz 3-4
84508 Burgkirchen an der Alz
GERMANY

Tel.: +49 8677 / 916 36 – 0

E-Mail: info@weinzierl.de

Web: www.weinzierl.de

2022-10-25