

KNX power supply 640 mA with KNX IP router

KNX IP LineMaster 762.1 *secure*

Operation and installation manual



(Art. # 5465)

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 (device display).....	4
3	Reset to factory default settings.....	12
3.1	Factory default settings	12
4	Wiring scheme	13
4.1	Function as coupler (KNXnet/IP routing)	13
4.2	Function as bus access (KNXnet/IP tunneling).....	16
5	KNX Security	16
6	Interface settings in the ETS	17
6.1	ETS 5.....	17
6.2	ETS 6.....	18
6.3	Common	19
7	Programming.....	20
7.1	Via KNX bus	20
7.2	Via KNXnet/IP tunneling.....	20
7.3	Via KNXnet/IP routing	20
7.4	Via direct IP connection	20
8	ETS database	22
8.1	Secure commissioning	22
8.2	Secure group communication.....	24
8.3	Additional individual addresses	26
8.4	IP settings	27
8.5	Description.....	30
8.6	General settings.....	30
8.7	Routing (KNX -> IP)	31
8.8	Routing (IP -> KNX)	34
8.9	Filter Table.....	36
9	Open source licenses	37

1 Application

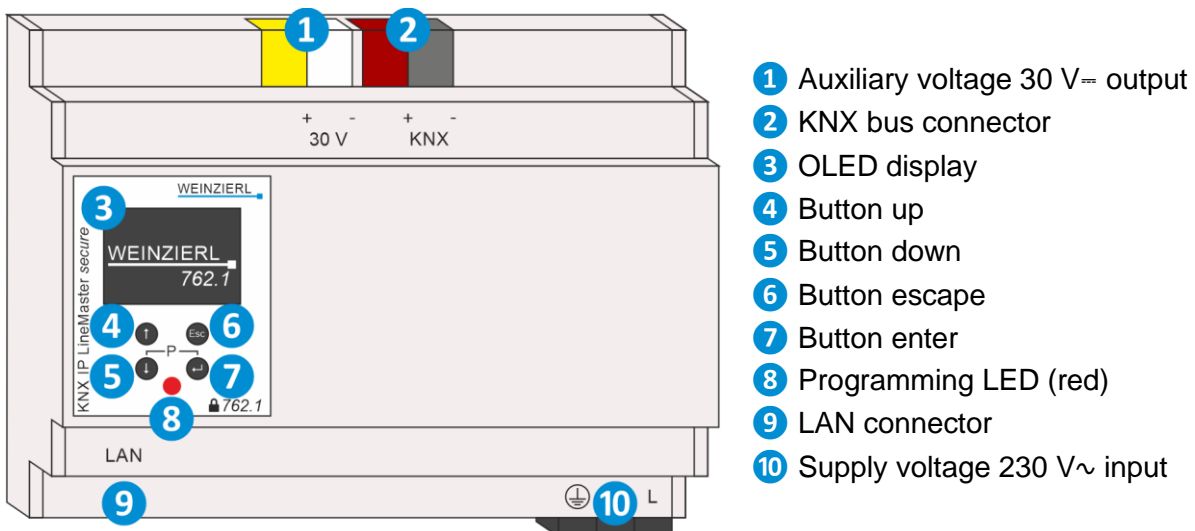
The KNX LineMaster 762.1 *secure* combines the essential functions of a KNX bus line: KNX power supply with choke, KNX IP router and KNX IP interface. In addition to the bus voltage the power supply offers an auxiliary voltage.

The KNX IP router in the KNX IP LineMaster 762.1 *secure* allows forwarding of telegrams between different lines through a LAN (IP) as a fast backbone. Using the embedded KNX IP interface, the KNX line can be connected directly to a PC (e.g. by ETS). The device supports KNX Security which can be enabled in ETS. As secure router the device allows coupling of not secured communication on KNX TP to a secured IP backbone. Also for the interface functionality (tunneling) KNX security prevents from unauthorized access. The IP address can be obtained by a DHCP server or by manual configuration (ETS) respectively.

This device works according to the KNXnet/IP specification using the core, the device management, the tunneling and the routing part. The KNX IP LineMaster 762.1 *secure* has an extended filter table for main groups 0 to 31 and is able to buffer up to 150 telegrams.

2 Installation and connection

The KNX IP LineMaster 762.1 *secure* is designed for installation on a DIN rail (35 mm) with a width of 6 units (108 mm). It features the following controls and displays:



The device configuration can be done as follows:

- Via the device display (partially).
- With the ETS (version 5.7 or newer)

2.1 KNX programming mode

The KNX programming mode is activated/deactivated either by simultaneously pressing the buttons (P) 5 and 7.

When the programming mode is active, the programming LED 8 lights up red.

2.2 Manual operation and status display (device display)

The red LED 8 on the front of the device is used to indicate KNX programming mode and errors.

Summary of the states of the programming LED 8:

LED Status	Meaning
LED lights red	The programming mode is active. Errors are not shown by the LED, but can be read in the display.
LED flashes red	Error conditions: <ul style="list-style-type: none"> Overload (sum of current from auxiliary and bus voltage output). The device is not loaded correctly e.g. after aborting a download. The programming mode is not active.
LED is off	The device operates in normal operating mode. No error condition is active. The programming mode is not active.

2.2.1 Startup and idle display

```

✓ WEINZIERL
15.15.0 Running
192.168. 1. 31
KNX IP LineMaster

```

During startup of the device, the individual address and the state of the application is displayed. The device name “KNX IP LineMaster” can be changed within ETS parameter settings.

The state can take one of the following values:

- Running:** The application is loaded and running.
- Stopped:** The application is stopped (programming LED 8 flashes)
- Unloaded:** The application is not loaded (programming LED 8 flashes)
- Loading:** The application is being loaded by the ETS
- Overload:** The output current exceeds the overload threshold 900 mA (programming LED 8 flashes)

- **Manual:** Parameterized coupler settings were overwritten manually via manual operation in the device display (filter, retransmit and acknowledge). A long press on button enter **7** restores the normal operating mode as parameterized.

The power supply function (KNX – and auxiliary voltage) is independent of the state of the application.



After 10 minutes of no activity, the device switches to the screen saver (blank screen with a jumping dot) to increase the lifetime of the display. Pressing any key turns the display back on.

2.2.2 Main menu

```
^ KNX IP LineMaster
v
*-----*
* Router      *
*-----*
Powersupply *
```

Pressing the button down **5** calls up the main menu of the device. By pressing button enter **7** you call up the submenus. Within the menus, use buttons up **4** and down **5** to navigate, the button enter **7** to confirm and the button escape **6** to go back or up one level.

The main menu offers the following menu items for selection:

- Router
- Powersupply
- System Info
- Dev Reset
- Contrast

2.2.3 “Router” menu item

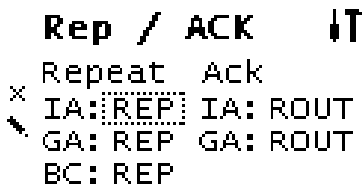
The Router menu item offers the following submenus for selection:

- IP Config
- IP Tunnel
- Filter
- Operation
- Transit
- Bus Errors



Settings that deviate from the parameterization are marked with a square bracket. The parameterized setting can be restored with a long button press on button enter **7**.

2.2.7 “Rep / ACK” submenu



In this submenu the settings for repeating telegrams on the subline (TP) can be changed. The settings for broadcast telegrams (BC), individual addressed telegrams (IA) and group telegrams (GA) can be changed separately.

The following selections are available:

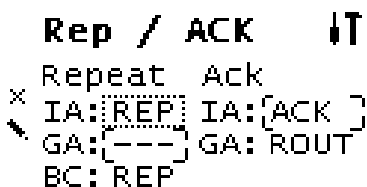
- No repetition: ---
- Up to 3 repetitions: **REP**

In addition, the settings for the telegram acknowledgement (acknowledge) on the subline (TP) can be changed:

- Confirm only when routing: **ROUT**
- Always confirm: **ACK**
- Negative confirmation: **NACK**

If the response is NACK, access to the device via KNX TP is no longer possible, see ETS parameter settings.


These settings are temporary.



Settings that deviate from the parameterization are marked with a square bracket. The parameterized setting can be restored with a long button press on button enter **7**.

2.2.8 “Tel Counter” submenu

```


Tel Counter 
  To Sub  To Main
× IA      0      0
↘ GA      0      0
  RESET COUNTERS

```


This submenu contains telegram counters. The number of forwarded telegrams can be read here separately according to direction (main line IP to subline TP and vice versa) and telegram type (individual addressed telegrams IA and group telegrams GA). The counters can be reset here.

2.2.9 “Bus Errors” submenu

```

Bus Errors 
Send :      0
× Rcv :      0
↘ Repeat:    0
  RESET COUNTERS

```

In this submenu errors during KNX communication are displayed. By pressing button enter  the error counters can be reset under the navigation item **RESET COUNTERS**.

The following errors are counted:

- Send (error while sending)
Send failed after last retry because ACK, NACK or BUSY responses are missing.
- Rcv (Error while receiving)
Deformed telegrams or telegram fragments received.
- Repeat
Number of repeatedly sent or repeatedly received telegrams.

2.2.10 “Powersupply” menu item

The Powersupply menu item offers the following submenus for selection:

- Diagnosis
- History
- Bus Reset
- Ev Counter

2.2.11 "Diagnosis" submenu

```

Diagnosis  -|/-
Busload:    50    %
× Voltage:   29    V
  Current:   11    mA
≡ Temp.    : 27    °C
  
```

This menu displays the current values of busload (%), voltage (V), current (mA) and temperature (°C).



The busload is a measure for the number of telegrams in a certain period of time. 100 % busload is reached at approx. 50 telegrams per second (Group Value Write telegrams with 1 byte). The voltage shows the current value of the bus voltage, the current the sum of bus and auxiliary current. The temperature is measured in the device.

2.2.12 "History" submenu

```

√ History 24h  |||||
Busload:  0..61  %
× Voltage:  6..29  V
  Current:  0..25  mA
≡ Temp.   : 8..27  °C
  
```

The history shows the value range (min. and max.) for busload (%), voltage (V), current (mA) and temperature (°C) of the last 24 hours.

```

^ Pk: 58%      0%
√
×
≡ Busload
  
```

Pressing button down **5** several times displays a graphical representation ("real time") for the following values: Busload, voltage, current and temperature. The time span of each graph is approx. 2 minutes.

To return to the main menu, press button escape button **6**.

2.2.13 "Bus Reset" submenu

```

Bus Reset
× Enter to reset
  ( ) 30
≡
  
```

In this submenu, the KNX line can be reset. By pressing button enter **7** the KNX bus voltage is switched off. The maximum reset time is 30 seconds. This time can be shortened by pressing button escape **6**.

2.2.14 “Ev Counter” submenu

```

√ Ev Counter  762
Op. time [h:m]
×           1:10
Run time [h:m]
           1:10

^ Ev Counter  762
Restarts [count]
×           1
Time [h:m] > 75 °C
           0:00

^ Ev Counter  762
Time [h:m] > 640 mA
×           0:00
Time [h:m] > 900 mA
           0:00

```

Various operating states are automatically logged in the device, which can be read in this submenu. All times are displayed in the format “hours:minutes”.

- Op. time [h:m]
Total summed up operating time of the device.
- Run time [h:m]
Time since the last device restart.
The time restarts when the operating voltage is applied.
- Restarts [count]
Number of device restarts.
The counter is incremented when the operating voltage is applied.
- Time [h:m] > 75 °C
Summed operating time during which the temperature in the device was above 75 °C.
- Time [h:m] > 640 mA
Summed operating time during which the current load was higher than 640 mA.
The current load of both outputs is recorded.
- Time [h:m] > 900 mA
Summed operating time during which the current load was higher than 900 mA.
The current load of both outputs is recorded.



In order to extend the life of the internal memory, the values of the counters are stored in the memory in a dynamic time span of up to 8 h. Thus, the values - if the power supply to the device was interrupted - can fall back somewhat.

2.2.15 “System Info” menu item

```

v System Info ⓘ
  SerNo: 00C500000000
x Info : 00C5.071B.10
  State: Running
  Vers.: 1.0.0
  MAC  : 0050C2554000
^
  [QR Code] ADCQAA
             AAAAAA
             CAQDAQ
             COMBYI
             BEFAWD
             ANBYHW
x
  
```

Information about the device is displayed here:

- SerNo: Serial number
- Info: ManufacturerID.AppID.AppVersion
- State: State of the application
- Vers.: Firmware version
- MAC: MAC address
- QR Code: KNX Security initial key (FDSK)

2.2.16 “Dev Reset” menu item

```

Dev Reset [Refresh]
x [Press Long ↵]
^ [RESTART DEVICE]
  [MASTER RESET]
  
```

In this menu, the device can be restarted with **RESTART DEVICE** or reset to factory settings with **MASTER RESET**. After selecting an option, button enter **7** must be held down until the animation has finished and the option is executed.



After a master reset a new ETS download is required.

2.2.17 “Contrast” menu item

```

^ Dev Reset [Refresh]
  [RESTART DEVICE]
x Contrast [Slider]
  
```

To adjust the contrast of the display, this menu item is selected in the main menu. By pressing button enter **7** several times, the contrast can be set to different levels.

3 Reset to factory default settings

It is possible to reset the device to its factory default settings (see “Dev Reset” menu item).

In the factory default settings, the device has the individual address 15.15.0 and no group addresses are connected. The IP address assignment is done via DHCP. Also, KNX Security is disabled and the initial key (FDSK) must be used for secure commissioning.

3.1 Factory default settings

Individual addresses, KNXnet/IP tunneling connections and IP address assignment

Individual address: 15.15.0

Active KNXnet/IP tunneling connections: 8

Individual address of tunneling connection 1: 15.15.240

Individual address of tunneling connection 2: 15.15.241

Individual address of tunneling connection 3: 15.15.242

Individual address of tunneling connection 4: 15.15.243

Individual address of tunneling connection 5: 15.15.244

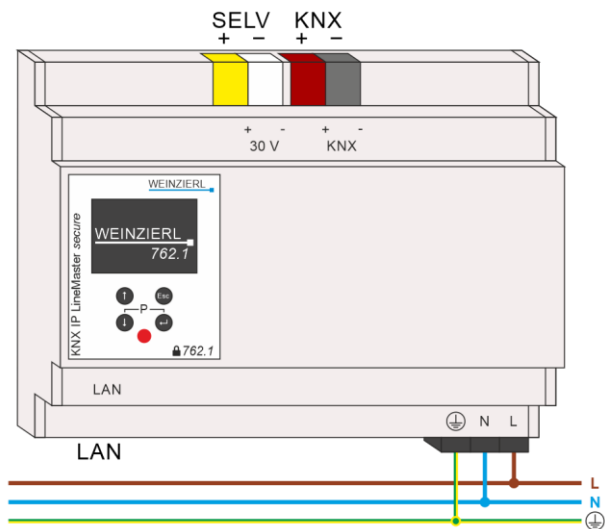
Individual address of tunneling connection 6: 15.15.245

Individual address of tunneling connection 7: 15.15.246

Individual address of tunneling connection 8: 15.15.247

IP address assignment: DHCP

4 Wiring scheme



4.1 Function as coupler (KNXnet/IP routing)

The KNX IP LineMaster 762.1 *secure* can work as line or area coupler. In both cases the LAN (IP) is used as backbone.

The following table shows the possible applications of the KNX IP LineMaster 762.1 *secure* compared to the classic topology:

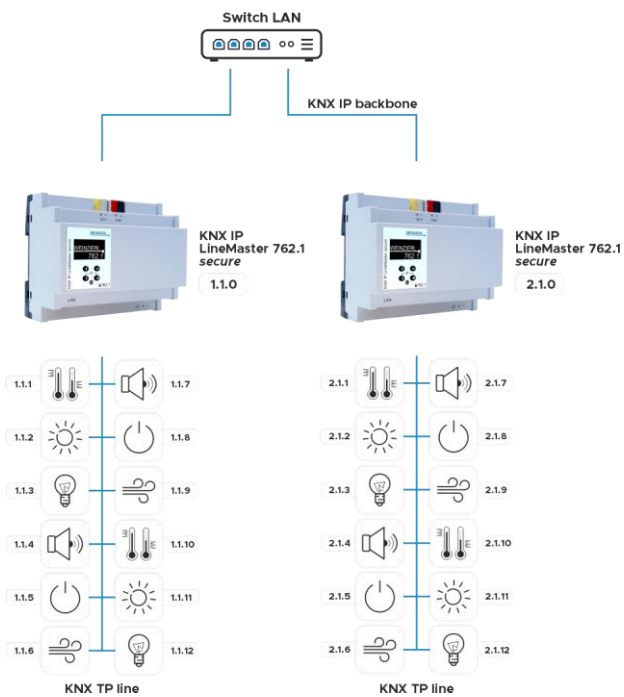
	Classic topology (without IP)	IP coupling of the areas (IP area coupler)	IP coupling of the lines (IP line coupler)
Backbone	TP	IP	IP
Coupling	KNX TP line coupler (max. 15 couplers)	KNX IP router (max. 15 routers)	Directly via LAN with switch
Area	TP	TP	IP
Coupling	KNX TP line coupler (max. 15x15 couplers)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

The KNX IP LineMaster 762.1 *secure* has a filter table and thus contributes to the reduction of the bus load. The extended filter table for main groups 0 ... 31 is automatically generated by the ETS.

Due to the difference in speed between Ethernet (100 Mbit/s) and KNX TP (9.6 kbit/s), considerably more telegrams can be transmitted on IP. If several telegrams for the same line follow each other shortly, they have to be buffered in the router to avoid telegram losses. For this purpose, the KNX IP LineMaster 762.1 *secure* has memory space for 150 telegrams (from IP to KNX TP).

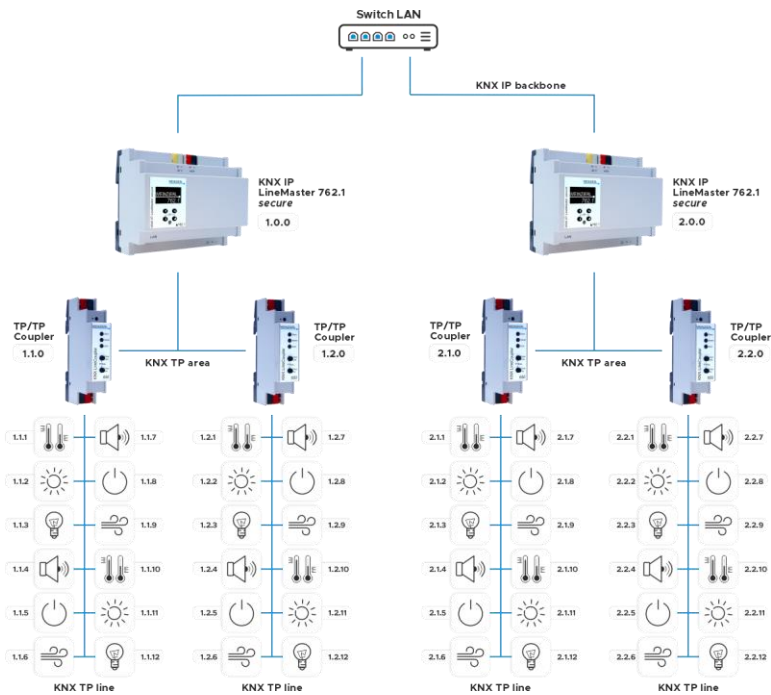
The assignment of the individual address of the KNX IP LineMaster 762.1 *secure* determines whether the device operates as a line or as an area coupler. If the individual address corresponds to the form x.y.0 (x, y: 1 ... 15), the KNX IP LineMaster 762.1 *secure* functions as a line coupler. If the individual address has the form x.0.0 (x: 1 ... 15), it is a area coupler.

4.1.1 IP line coupler



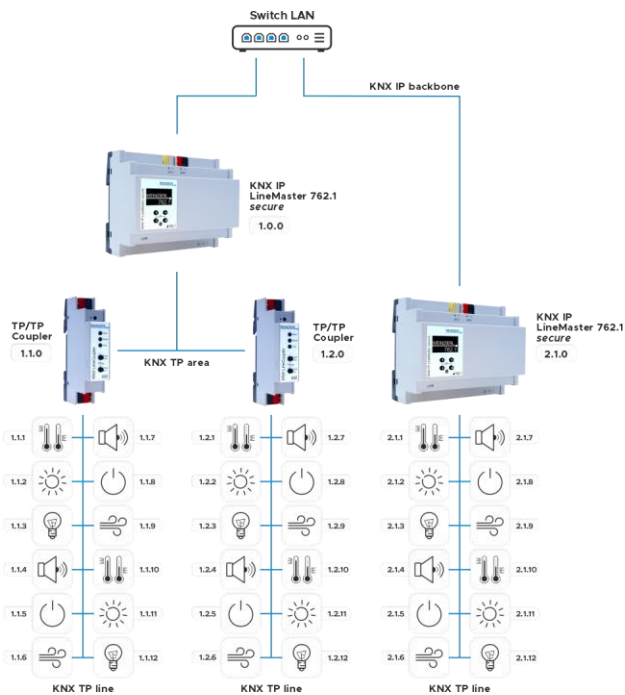
If the KNX IP LineMaster 762.1 secure is used as line coupler (x.y.0), no KNX IP router may be topologically above it. If, for example, a KNX IP router has the individual address 1.1.0, there must be no KNX IP router with the address 1.0.0.

4.1.2 IP area coupler



If the KNX IP LineMaster 762.1 secure is used as an area coupler (x.0.0), no KNX IP router may be located topologically below it. If, for example, a KNX IP router has the individual address 1.0.0, there must be no KNX IP router with the address 1.1.0.

4.1.3 IP area and line coupler



4.2 Function as bus access (KNXnet/IP tunneling)

The KNX IP LineMaster 762.1 *secure* can be used as an interface to the KNX. The KNX bus can be accessed from any point in the LAN. The device supports up to 8 simultaneous tunneling connections. An additional individual address must be assigned for each connection. A more detailed description can be found in the section “Interface settings in the ETS”.

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.

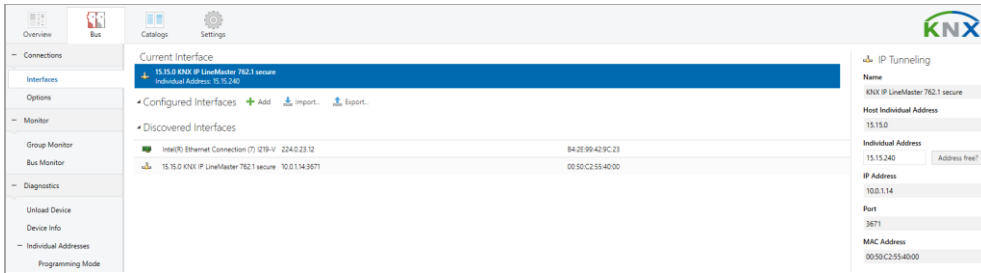


Encrypted telegrams are longer than the previously used unencrypted ones. For secure programming via the bus, it is therefore necessary that the interface used (e.g. USB) and any intermediate line couplers support the so called KNX Long Frames.

6 Interface settings in the ETS

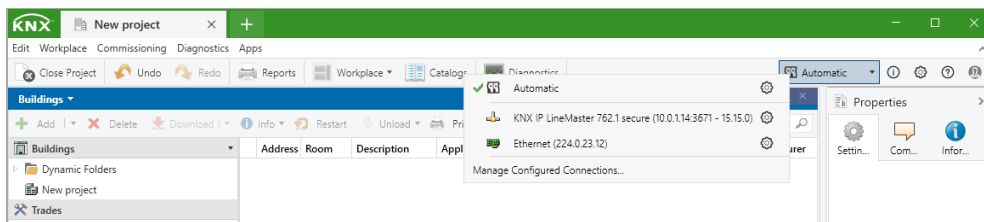
6.1 ETS 5

In ETS 5, interfaces can be selected and configured via the ETS menu “Bus – Interfaces”. All available connections are listed under “Discovered interfaces”. After clicking on the desired connection, connection specific information and options appear on the right side of the ETS window. Via the “Select” button, the marked connection can be selected as “Current interface”.



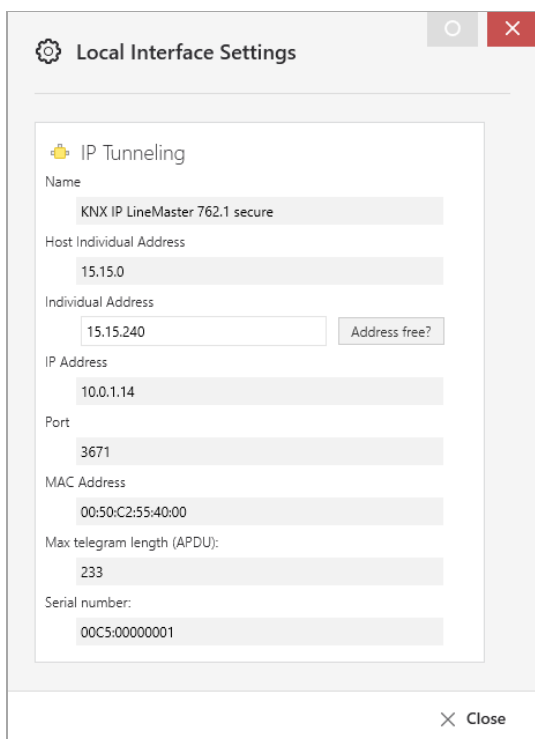
6.2 ETS 6

In ETS 6, interfaces can be selected and configured in the ETS project via the “Interface” button. All available connections are listed here.



By clicking on a connection, this is selected as the desired interface.

By clicking the gear next to the desired connection, the connection specific information and options appear.



6.3 Common

The displayed device name and the “Host Individual Address” (individual address of the device) can be changed via the database entry within your ETS project.

In the “Individual address” input field, the individual KNX address of the currently used KNXnet/IP tunneling connection can be changed. To check if the desired individual address is not already available in your KNX installation, the button “Address free?” can be pressed.

The KNX IP LineMaster 762.1 *secure* supports up to 8 connections simultaneously. A separate individual address is used for each connection.

The ETS can access configured IP interfaces even without a database entry. If the configuration does not correspond to the conditions of the installation, it must be adapted via the database entry in the ETS project.

The individual KNX device address as well as the individual KNX addresses for the additional tunneling connections can be changed via the database entry within the ETS project after the device has been added to the project. See section “ETS database - Additional individual addresses”.

The KNX IP LineMaster 762.1 *secure* has, like all programmable KNX devices, an individual address with which the device can be addressed. This is used, for example, by the ETS when downloading the interface via the KNX bus.

For the interface function, the device uses additional individual addresses that can be set in the ETS (for ETS 5.7 or newer). If a client (e.g. ETS) sends secure telegrams to the KNX bus via the KNX IP LineMaster 762.1 *secure*, these contain one of the additional addresses as the sender address. Each address is assigned to a connection. Thus, response telegrams can be forwarded definitely to the respective client.

The additional individual addresses must be from the address range of the bus line in which the interface is located and must not be used by another device.

Example:

<i>Individual address:</i>	<i>1.1.0 (device address in the topology)</i>
<i>KNXnet/IP tunneling connection 1:</i>	<i>1.1.240 (1. additional individual address)</i>
<i>KNXnet/IP tunneling connection 2:</i>	<i>1.1.241 (2. additional individual address)</i>
<i>KNXnet/IP tunneling connection 3:</i>	<i>1.1.242 (3. additional individual address)</i>
<i>KNXnet/IP tunneling connection 4:</i>	<i>1.1.243 (4. additional individual address)</i>
<i>KNXnet/IP tunneling connection 5:</i>	<i>1.1.244 (5. additional individual address)</i>
<i>KNXnet/IP tunneling connection 6:</i>	<i>1.1.245 (6. additional individual address)</i>
<i>KNXnet/IP tunneling connection 7:</i>	<i>1.1.246 (7. additional individual address)</i>
<i>KNXnet/IP tunneling connection 8:</i>	<i>1.1.247 (8. additional individual address)</i>

7 Programming

The KNX IP LineMaster 762.1 *secure* can be programmed by the ETS via different ways.

7.1 Via KNX bus

For this purpose, the device must only be connected to the KNX bus. The ETS requires an additional interface (e.g. USB) to the KNX bus. Via this way, both the individual address and the entire application including IP configuration can be programmed. Programming via the KNX bus is recommended if no IP connection can be established.

7.2 Via KNXnet/IP tunneling

No additional interface is required here. Programming via KNXnet/IP tunneling is possible if the device already has a valid IP configuration (e.g. via DHCP or Auto IP). In this case, the device is displayed in the interfaces in the ETS and must be selected. The download takes place from the ETS project, as with other devices.

7.3 Via KNXnet/IP routing

Programming via KNXnet/IP routing is possible if the device already has a valid IP configuration (e.g. via DHCP or Auto IP). The routing interface appears in the ETS if at least one device is visible in the network that supports routing. The name of the network interface in the PC appears as the designation. If routing is selected as interface, the programming is done from the ETS project as for other devices. In this case the LAN is used as KNX medium similar to TP. No additional interface device is required.

7.4 Via direct IP connection

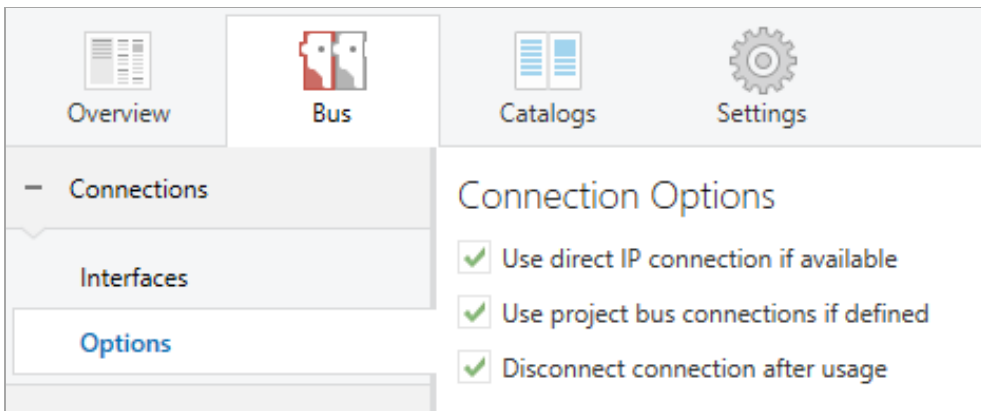
While both KNXnet/IP tunneling and KNXnet/IP routing are limited to the speed of KNX TP, a direct IP connection allows the device to be loaded at high speed. The direct IP connection is possible if the device already has both a valid IP configuration and an individual address.



Due to the significantly shorter transmission times, it is recommended to perform downloads via IP.

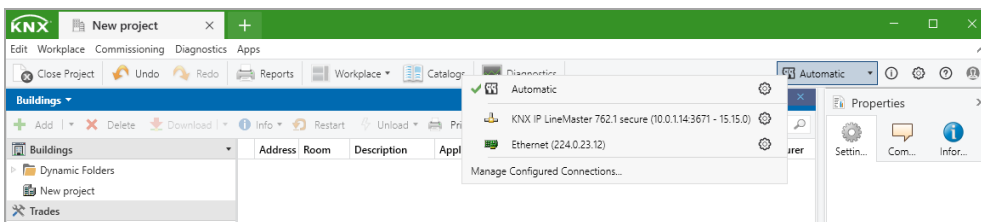
ETS 5

In ETS 5, the selection “Use direct IP connection if available” can be selected in the menu under “Bus – Connections – Options”. The download then takes place directly in the device and is not visible in the ETS group monitor.



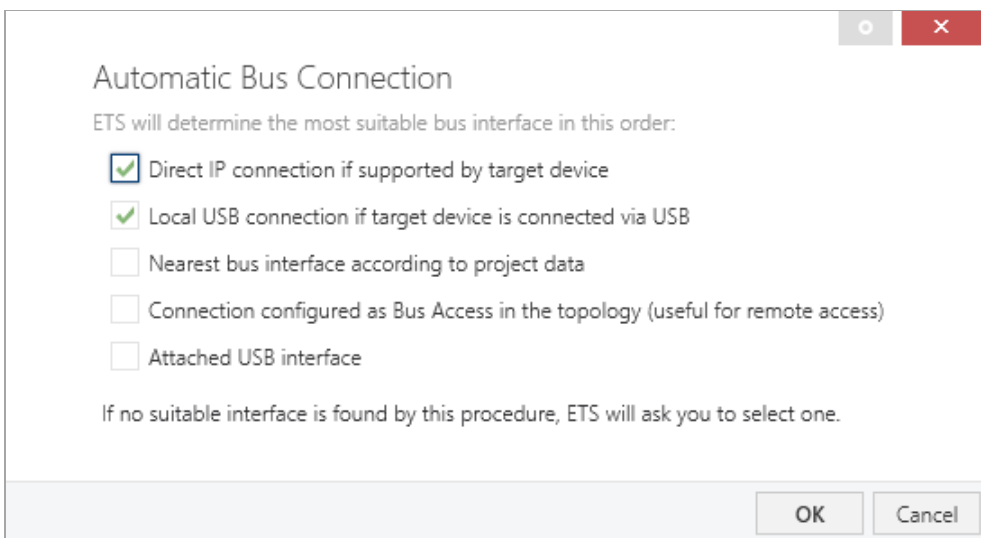
ETS 6

In ETS 6, interfaces can be selected and configured in the ETS project via the “Interface” button. All available connections are listed here.



By clicking on “Automatic” selects the “Automatic Bus Connection”.

By clicking the gear next to “Automatic” the specific options appear.



Here, the selection “Direct IP connection if supported by target device” can be selected. The download then takes place directly in the device and is not visible in the ETS group monitor.

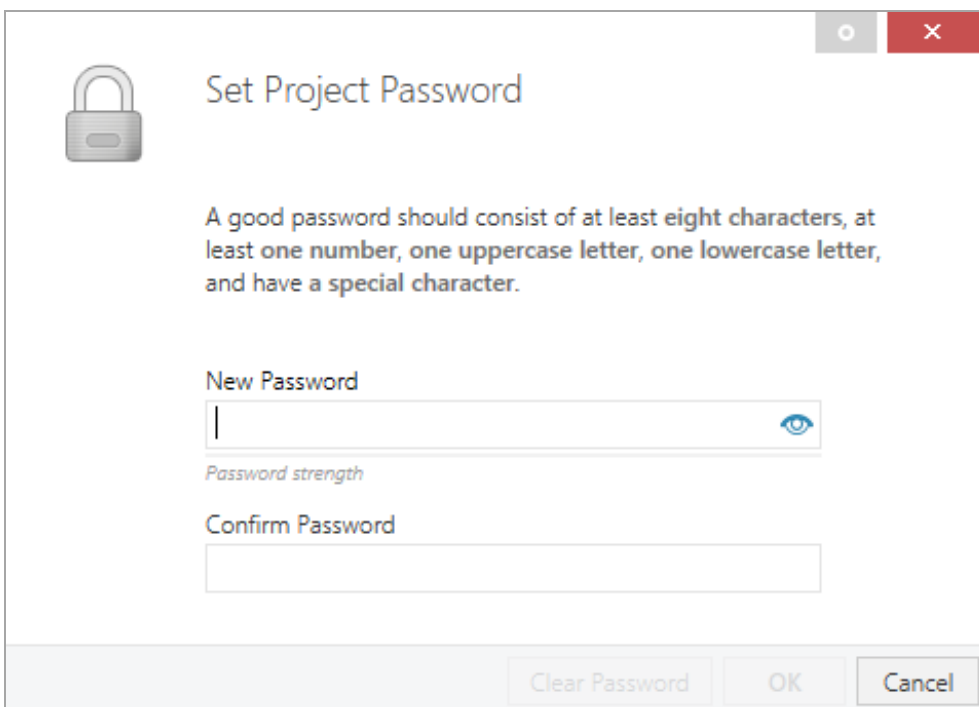
8 ETS database

The ETS 5 database (for ETS 5.7 or newer) can be downloaded from the product website of the KNX IP LineMaster 762.1 *secure* (www.weinzierl.de) or from the ETS online catalogue.

The KNX IP LineMaster 762.1 *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.

8.1 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

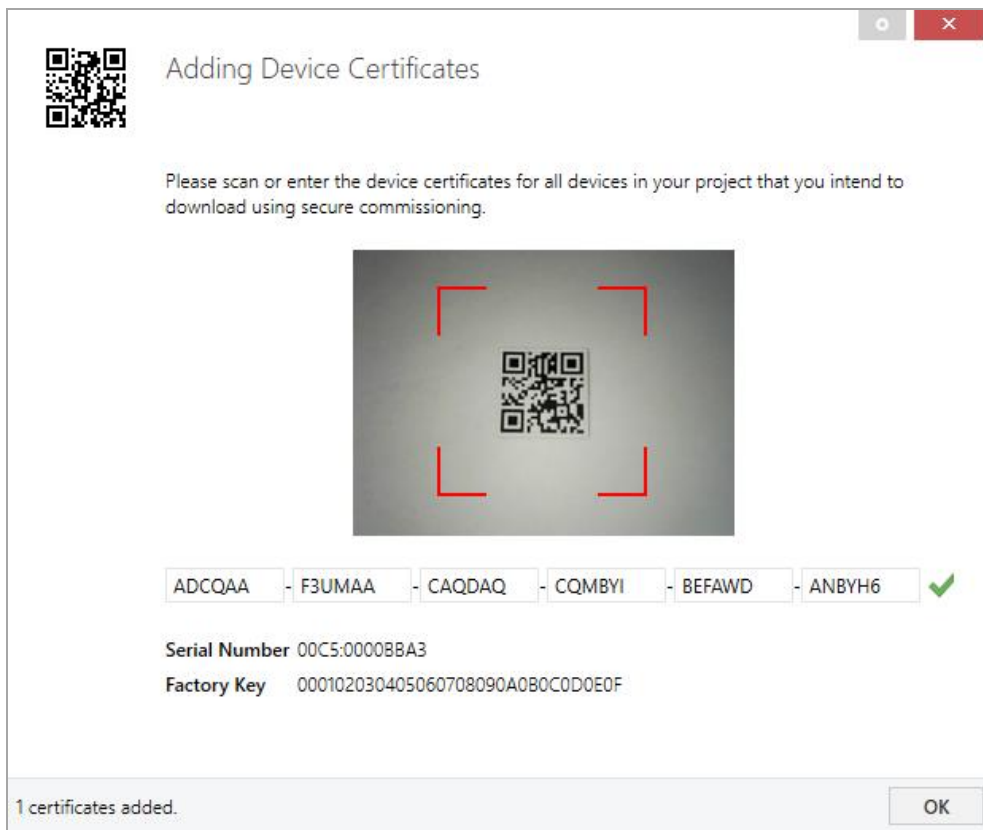
Password strength

Confirm Password

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).



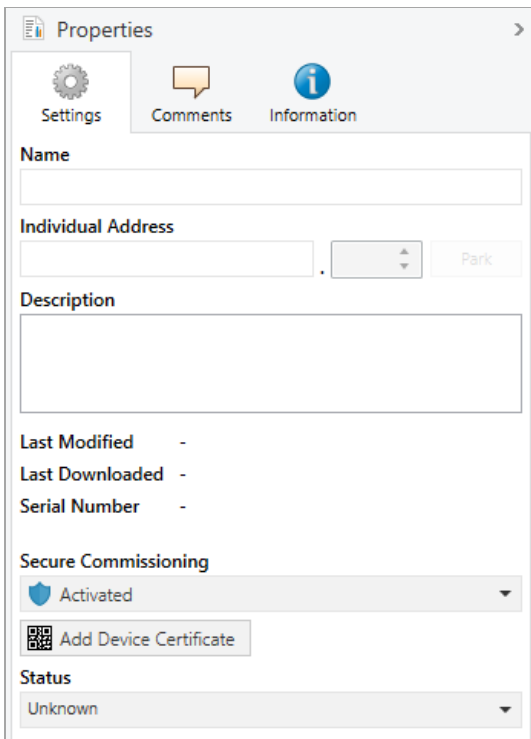
The certificate is printed as text on the device. It can also be scanned from the printed QR code via a webcam.

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.

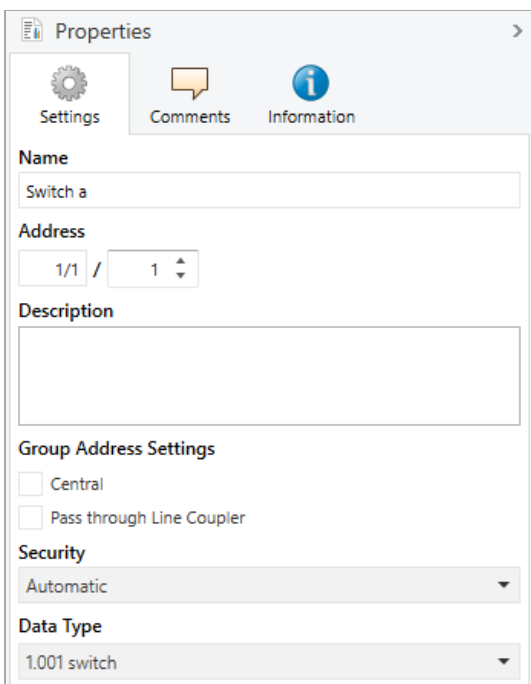
The serial number in the certificate enables the ETS to assign the correct key to a device during a download.

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









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

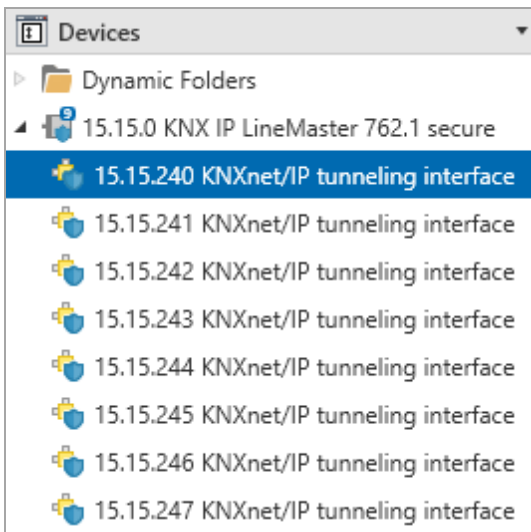
In the overview of communication objects in the ETS project, secured objects can be recognized by a shield symbol:

	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

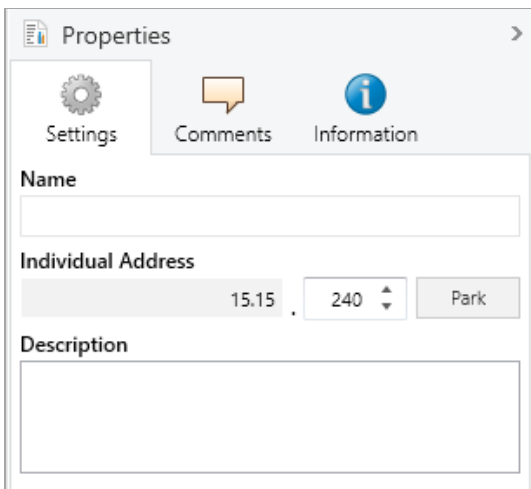
A separate key is automatically generated by the ETS for each secured group address. These keys can also be checked in the ETS panel Reports – Project Security. To enable all devices to communicate with a secure group address, the keys must be known to all. Therefore a download must be made into all 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.

8.3 Additional individual addresses

The additional individual addresses appear in the topology view.



To change the individual addresses, select the corresponding entry in the list and enter the desired address in the text field under “Properties – Settings”. If the frame of the text field changes its colour to red after entry, this indicates that the address entered is already being used. The changes are only applied in the device after download.



Make sure that none of the specified addresses are already used in your KNX installation.

8.4 IP settings

By marking the KNX IP LineMaster 762.1 *secure* in the tree structure of the topology view of the ETS project, the overview “Properties” appears on the right side of the ETS window.

8.4.1 Device name (user friendly name)

Under Properties menu item “Settings”, the device name (user friendly name) of the KNX IP LineMaster 762.1 *secure* can be changed. The first 30 characters are used.

Properties

Settings IP Comments Informati...

Name
KNX IP LineMaster 762.1 secure

Individual Address
15.15 . 0 Park

Description

Last Modified -
Last Downloaded -
Serial Number -

Secure Commissioning
Activated

Add Device Certificate

Secure Tunneling
Activated

Status
Unknown



The change made will only take effect after an ETS download.

8.4.2 IP configuration

Under Properties menu item “IP”, the IP specific options of the KNX IP LineMaster 762.1 *secure* can be changed.

Properties

Settings IP Comments Informati...

Obtain an IP address automatically

Use a static IP address

IP Address
255.255.255.255

Subnet Mask
255.255.255.255

Default Gateway
255.255.255.255

MAC Address
Unknown

Multicast Address
224.0.23.12

Commissioning Password
g<QtLI2m
Good

Authentication Code
D91q@M-O
Good



The change made will only take effect after an ETS download.

By switching from “Obtain an IP address automatically” (via DHCP) to “Use a static IP address” (static IP address), the IP address, subnet mask and standard gateway can be freely selected.

IP Address

The IP address of the KNX IP LineMaster 762.1 *secure* must be entered here. This is used to address the device via the IP network (Wi-Fi). The IP addressing should be coordinated with the administrator of the network.

Subnet Mask

The subnet mask must be entered here. This mask is used by the device to determine whether a communication partner is located in the local network. If a partner is not in the local network, the device does not send the telegrams directly to the partner, but to the standard gateway, which takes over the forwarding.

Default Gateway

Enter the IP address of the gateway here, e.g. the access point of the installation.

Multicast address

This address is used for routing telegrams to IP. The multicast IP address 224.0.23.12 has been reserved for this purpose (KNXnet/IP) by the IANA (Internet Assigned Numbers Authority). If another multicast IP address is required, it must be from the range 239.0.0.0 to 239.255.255.255.

Example for the assignment of IP addresses

The KNX IP LineMaster 762.1 *secure* is to be accessed with a PC.

IP address of PC: 192.168.1.30

Subnet mask of PC: 255.255.255.0

The KNX IP LineMaster 762.1 *secure* is located in the same local network, i.e. it uses the same subnet. The assignment of the IP address is restricted by the subnet, i.e. in this example the IP address of the IP interface must be 192.168.1.xx, xx can be a number from 1 to 254 (with the exception of 30, which has already been used). Care must be taken not to assign addresses twice.

IP address of KNX IP LineMaster 762.1 *secure*: 192.168.1.31

Subnet mask of KNX IP LineMaster 762.1 *secure*: 255.255.255.0

Remote access

Via the KNX IP LineMaster 762.1 *secure* remote access via the internet is possible. Further details can be found in the document "Remote access with ETS" on www.weinzierl.de.

8.5 Description

--- KNX IP LineMaster 762.1 secure > Description	
<p>Description</p>	
General settings	KNX IP LineMaster 762.1 secure KNX power supply 640 mA with KNX IP router WEINZIERL
Routing (KNX -> IP)	
Routing (IP -> KNX)	
	<p>The KNX LineMaster 762.1 secure combines the essential functions of a KNX bus line: KNX power supply with choke, KNX IP router and KNX IP interface.</p> <p>In addition to the bus voltage the power supply offers an auxiliary voltage.</p> <p>The KNX IP router in the KNX IP LineMaster 762.1 secure allows forwarding of telegrams between different lines through a LAN (IP) as a fast backbone.</p> <p>Using the embedded KNX IP interface, the KNX line can be connected directly to a PC (e.g. by ETS).</p> <p>The device supports KNX Security which can be enabled in ETS. As secure router the device allows coupling of not secured communication on KNX TP to a secured IP backbone.</p> <p>Also for the interface functionality (tunneling) KNX security prevents from unauthorized access. The IP address can be obtained by a DHCP server or by manual configuration (ETS) respectively.</p> <p>This device works according to the KNXnet/IP specification using the core, the device management, the tunneling and the routing part.</p> <p>The KNX IP LineMaster 762.1 secure has an extended filter table for main groups 0 to 31 and is able to buffer up to 150 telegrams.</p>
	<p>Wiring scheme:</p>
	<p>Please consult device data sheet and manual for further information.</p>
	<p>Contact:</p> <p>WEINZIERL ENGINEERING GmbH Achatz 3-4 84508 Burgkirchen an der Alz GERMANY www.weinzierl.de info@weinzierl.de</p>

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

8.6 General settings

--- KNX IP LineMaster 762.1 secure > General settings	
Description	<p>i For device name and IP settings see dialog "Properties"</p>
General settings	<p>Local settings via menu <input type="radio"/> Disabled <input checked="" type="radio"/> Enabled</p>
Routing (KNX -> IP)	<p>Manual operation on device <input type="text" value="Enabled without time limit"/></p>
Routing (IP -> KNX)	

Local settings via the menu

By deactivating this option, it is no longer possible to make settings via the device menu. This concerns the setting of the IP configuration, the resetting of the counters, the device reset, the bus reset and the temporary changing of the filter settings.

Manual operation on device

The duration of the manual operation mode is set here. For commissioning or test purposes, the filter table can be temporarily bypassed. This can be set under the "Filter" menu item. When terminated, the normal operating mode, as programmed, is automatically executed again.

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

8.7 Routing (KNX -> IP)

--- KNX IP LineMaster 762.1 secure > Routing (KNX -> IP)		
Description	Group telegrams (main groups 0 to 13)	Filter
General settings	Group telegrams (main groups 14 to 31)	Filter
Routing (KNX -> IP)	Individual addressed telegrams	Filter
Routing (IP -> KNX)	Broadcast telegrams	<input type="radio"/> Block <input checked="" type="radio"/> Route
	Acknowledge (ACK) of group telegrams	<input type="radio"/> Always <input checked="" type="radio"/> Only if routed
	Acknowledge (ACK) of individual addressed telegrams	Only if routed

Group telegrams (main groups 0 to 13)

The main groups 0 to 13 form the standard group address range of the ETS.

The following settings are possible:

- Block
No group telegram of the main groups 0 to 13 is forwarded to IP.
- Route
All group telegrams of the main groups 0 to 13 are forwarded to IP regardless of the filter table.
- Filter
Here it is checked by means of the filter table whether the received group telegram is forwarded to IP.



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

Group telegrams (main groups 14 to 31)

The main groups 14 to 31 form the extended group address range of the ETS.

The following settings are possible:

- Block
No group telegram of the main groups 14 to 31 is forwarded to IP.
- Route
All group telegrams of the main groups 14 to 31 are forwarded to IP regardless of the filter table.
- Filter
Here it is checked by means of the filter table whether the received group telegram is forwarded to IP.



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

Individual addressed telegrams

Individual addressed telegrams are used when downloading devices.

The following settings are possible:

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



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

Broadcast telegrams

Broadcast telegrams are used when assigning individual addresses.

The following settings are possible:

- Block
No received broadcast telegram is forwarded to IP.
- Route
All received broadcast telegrams are forwarded to IP.

Acknowledgement (ACK) of group telegrams

The following settings are possible:

- Always
An acknowledge is always generated for received group telegrams (from KNX).
- Only if routed
For received group telegrams (from KNX), an acknowledge is only generated when forwarding to IP.

Acknowledgement (ACK) of individual addressed telegrams

The following settings are possible:

- Always
An acknowledge is always generated for received individual addressed telegrams (from KNX).
- Only if routed
For received individual addressed telegrams (from KNX), an acknowledge is only generated when forwarding to IP.
- Answer with NACK
Each received individual addressed telegram (from KNX) is answered with NACK (Not Acknowledge), i.e. communication with individual addressed telegrams on the corresponding KNX line is no longer possible. Group communication (group telegrams) is not affected by this. This setting can be used to prevent manipulation attempts.



If the response is NACK, access to the device via KNX is no longer possible. The parameterization must be done via IP.

8.8 Routing (IP -> KNX)

--.- KNX IP LineMaster 762.1 secure > Routing (IP -> KNX)		
Description	Group telegrams (main groups 0 to 13)	Filter <input type="text"/>
General settings	Group telegrams (main groups 14 to 31)	Filter <input type="text"/>
Routing (KNX -> IP)	Individual addressed telegrams	Filter <input type="text"/>
Routing (IP -> KNX)	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 (main groups 0 to 13)

The main groups 0 to 13 form the standard group address range of the ETS.
The following settings are possible:

- **Block**
No group telegram of the main groups 0 to 13 is forwarded to KNX.
- **Route**
All group telegrams of the main groups 0 to 13 are forwarded to KNX regardless of the filter table.
- **Filter**
Here it is checked by means of the filter table whether the received group telegram is forwarded to KNX.



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

Group telegrams (main groups 14 to 31)

The main groups 14 to 31 form the extended group address range of the ETS.
The following settings are possible:

- **Block**
No group telegram of the main groups 14 to 31 is forwarded to KNX.
- **Route**
All group telegrams of the main groups 14 to 31 are forwarded to KNX regardless of the filter table.
- **Filter**
Here it is checked by means of the filter table whether the received group telegram is forwarded to KNX.



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

Individual addressed telegrams

Individual addressed telegrams are used when downloading devices.

The following settings are possible:

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



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

Broadcast telegrams

Broadcast telegrams are used when assigning individual addresses.

The following settings are possible:

- Block
No received broadcast telegram is forwarded to KNX.
- Route
All received broadcast telegrams are forwarded to KNX.

Repetition of group telegrams

The following settings are possible:

- Disabled
The received group telegram is not repeated on KNX in case of error.
- Enabled
The received group telegram is repeated up to three times in case of error.

Repetition of individual addressed telegrams

The following settings are possible:

- Disabled
The received individual addressed telegram is not repeated on KNX in case of error.
- Enabled
The received individual addressed telegram is repeated up to three times in case of error.

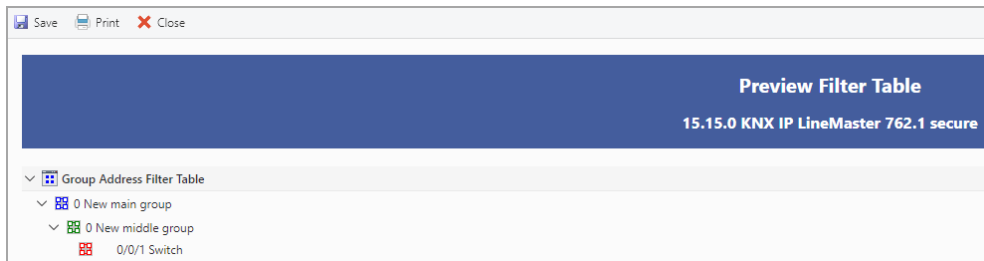
Repetition of broadcast telegrams

The following settings are possible:

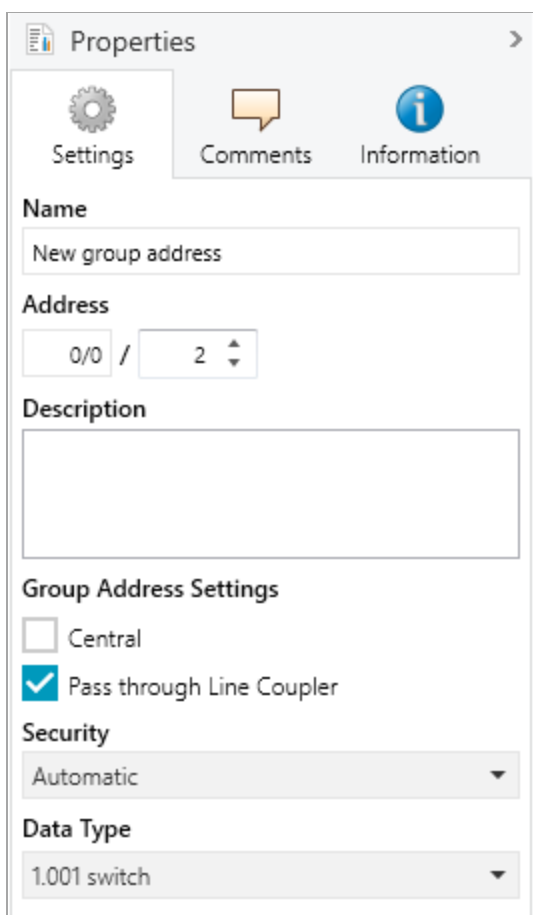
- Disabled
The received broadcast telegram is not repeated on KNX in case of error.
- Enabled
The received broadcast telegram is repeated up to three times in case of error.

8.9 Filter Table

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.



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.



9 Open source licenses

The firmware used in this product uses the following open source software package:

- curve25519-donna (<http://code.google.com/p/curve25519-donna/>)
Curve25519 elliptic curve, public key function

Copyright 2008, Google Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.



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.
- The device is a permanently connected equipment: A readily accessible disconnect device shall be incorporated external to the equipment.
- The installation requires a 16 A fuse for external overcurrent protection.
- The power rating is indicated on the side of the product.



Product database for ETS 5/6

www.weinzierl.de/en/products/762.1/ets6

Data sheet

www.weinzierl.de/en/products/762.1/datasheet

CE Declaration

www.weinzierl.de/en/products/762.1/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

2022-12-14