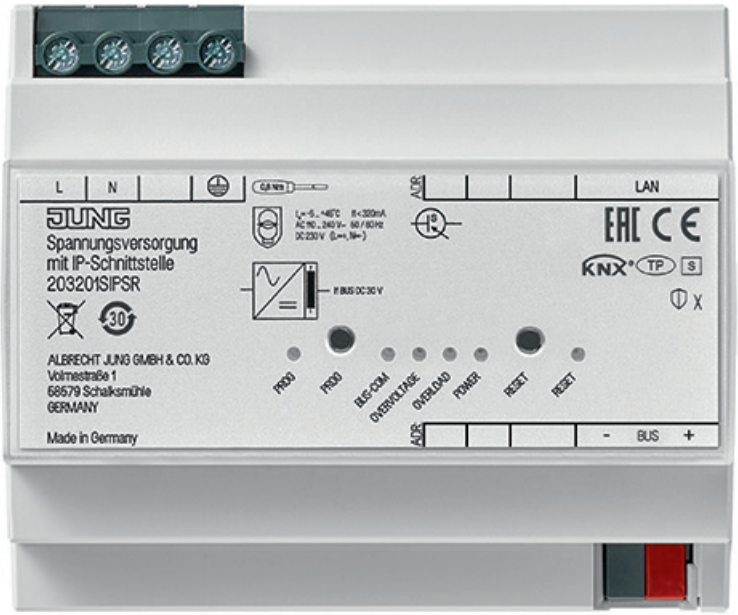
Product documentation



Power supply with IP interface

Ref.-no.: 20320 1S IPS R

ALBRECHT JUNG GMBH & CO. KG
Volmestraße 1
58579 Schalksmühle
GERMANY
Tel. +49 2355 806-0
Fax +49 2355 806-204
kundencenter@jung.de
www.jung.de

12/2020

Table of Contents

1 Safety instructions and device components

1.1 Safety instructions

Electrical equipment may only be fitted and connected by electrically skilled persons.

Serious injuries, fire or property damage possible. Please read and follow manual fully.

Danger of electric shock. During installation and cable routing, comply with the regulations and standards which apply for SELV circuits.

These instructions are an integral part of the product and must remain with the end customer.

1.2 Device components

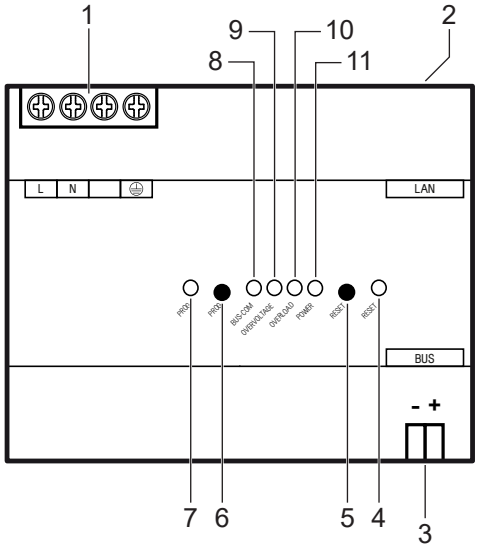


Fig. 1: Device components

1	Mains connection	5	RESET button	9	OVERVOLTAGE LED
2	LAN connection	6	PROG button	10	OVERLOAD LED
3	KNX connection	7	PROG LED	11	POWER LED
4	RESET LED	8	BUS-COM LED		

2 Function

2.1 System information

The device can be updated. Firmware can be easily updated.

The device is KNX Data Secure capable. KNX Data Secure offers protection against manipulation in building automation and can be configured in the ETS project. Detailed specialist knowledge is required. A device certificate, which is attached to the device, is required for safe commissioning. During mounting, the certificate must be removed from the device and stored securely.

Planning, installation and commissioning of the device are carried out with the aid of the ETS, version 5.7 and above.

2.2 Intended use

- Supplying KNX devices with bus voltage
- Connection between KNX devices and PC or other data processing devices via IP
- Operation as data interface
- Mounting on DIN rail according to EN 60715 in distribution boxes

2.3 Product characteristics

- Output with integrated choke for supplying KNX bus lines
- Reset of KNX lines via reset button or communication object
- Short-circuit proof
- Overvoltage proof
- No-load protection
- Support of KNX Data Secure from ETS version 5.7 upwards
- Support of KNX IP Secure from ETS version 5.7 upwards
- LED display for KNX communication, Ethernet communication and programming mode
- Configuration via ETS
- SNTP server
- Max. 8 connections to IP terminal devices, e.g. for simultaneous visualisation and configuration
- Electrical isolation between KNX and IP network

2.3.1 Application program A

ⓘ Only one application program per device can be used.

The additional functions of this application program are already provided with the delivery state of the device.

- Presence control: with key card holder or presence detector
- Welcome/Goodbye scenes

2.3.2 Application program B

ⓘ Only one application program per device can be used.

The additional functions of this alternative application program are only available after a firmware update of the device.

Requirement:
Remote access licence (ref.-no.: IPS-L)

- Encrypted access to KNX devices for configuration and maintenance outside the local network
- Enabling access via communication objects
- Feedback on access and programming processes via communication objects

3 Information for electrically skilled persons

3.1 Installation and electrical connection

DANGER
Electrical shock on contact with live parts in the installation environment.
Electrical shocks can be fatal.
Before working on the device, disconnect the power and cover live parts in the area!

3.2 Mounting

Observe ambient temperature. Ensure sufficient cooling.

- Mount device on DIN rail.

3.3 Connection

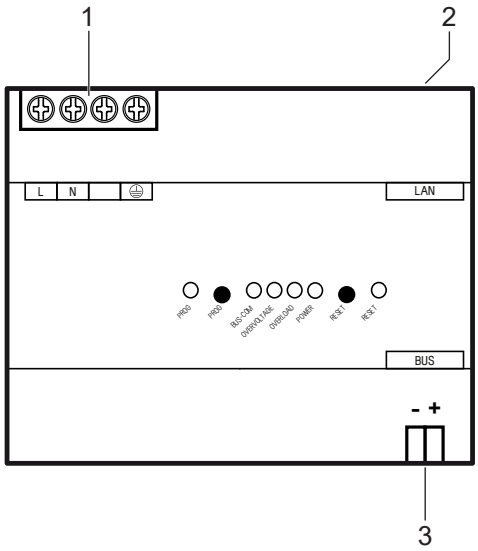


Fig. 2: Connection

1 Mains connection
2 KNX connection
3 LAN connection

Requirements:

- Ethernet connection with 10/100 Mbit
- KNX/EIB bus connection
- Power supply via a suitable circuit breaker

- Connect protective conductor and mains voltage.
- Connect LAN and KNX.

i The bus load must not exceed the output current.

i Do not connect any other products to the bus output. The bus communication could be affected by this.

4 Commissioning

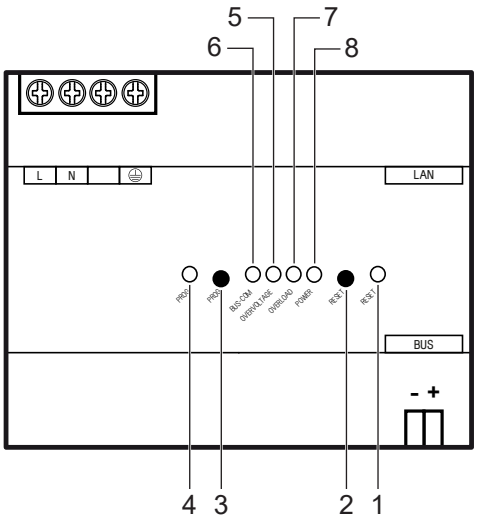


Fig. 3: Commissioning

1	RESET LED	5	BUS-COM LED
2	RESET button	6	OVERVOLTAGE LED
3	PROG button	7	OVERLOAD LED
4	PROG LED	8	POWER LED

4.1 Switching on

After connecting, the device is switched on automatically.

4.2 Boot procedure

The automatic boot procedure starts after switching on. The six LEDs flash on the front of the device as a running light during the boot procedure.

The duration of the boot procedure is prolonged if the IP address is assigned to the device via DHCP. DHCP is specified by the factory settings. The green POWER LED flashes during the assignment of the IP address.

At the end of the booting procedure, the green POWER LED lights up.

5 Operation

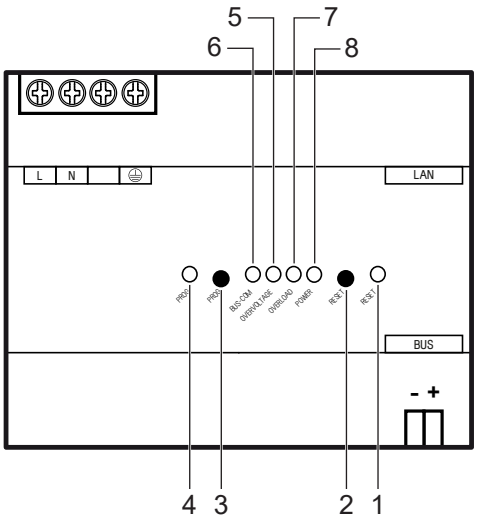


Fig. 4: Operation

1	RESET LED	5	BUS-COM LED
2	RESET button	6	OVERVOLTAGE LED
3	PROG button	7	OVERLOAD LED
4	PROG LED	8	POWER LED

5.1 LED displays

There are six LEDs on the front of the device. The LEDs indicate the following device statuses during operation:

- PROG LED lights up/flashes red:
  Programming mode is activated.
- BUS-COM LED lights up/flashes yellow:
  Lights up: Voltage on the device bus is normal.
  Flashes: Device bus is active.
- OVERVOLTAGE LED lights up yellow:
  Voltage on the device bus is too high.
- OVERVOLTAGE LED lights up red:
  Overload on the device bus
- POWER LED lights up/flashes green:
  Lights up: Device is ready for operation.
  Flashes: Overload or excessive voltage
- RESET LED lights up red:
  Device bus is reset.

5.2 Programming mode

Program interface:

• Press PROG button.
  PROG LED lights up red.

Program product application:

• Press the PROG button again.
  PROG LED flashes red.

Terminate programming mode:

• Press the PROG button again.

5.3 Diagnostic messages

Acknowledge diagnostic messages:

- Press RESET button briefly.

5.4 Reset

Reset device bus for 20 seconds:

- Press RESET button for 2 ... 4 seconds.
  RESET LED lights up red.
  Power supply on the device bus is interrupted and the device bus is short-circuited.
  Power is switched on again.

5.5 Master reset

- Ensure that the device is switched off (disconnect bus voltage and power supply).
- Press PROG button, hold it and connect device.
  Device switches on.
- Hold PROG button until PROG LED flashes slowly (approx. 1 Hz).
- Release PROG button.
- Press PROG button again and hold it until PROG LED flashes fast (approx. 4 Hz).
  The master reset starts.
- Release PROG button.

6 Configuration

Up to firmware version 1.050 (e.g. 1.006) the device consists of a combination of the following devices:

- Power supply with IP interface
- Power supply with IP interface - Additional functions

The additional functions can be used for hotel room management for example.

From firmware version 1.050 (e.g. 1.056) the device alternatively can consist of a combination of the following devices:

- Power supply with IP interface
- KNX IP interface - Additional functions

The configuration of both devices can be made in ETS 5.

For using all functions, product applications are necessary for both devices.

Both devices need a unique physical address in the ETS.

6.1 Topology

To insert the power supply into an ETS project, a TP line must exist which has the power supply and the additional functions inserted.

6.2 Device properties

6.2.1 General

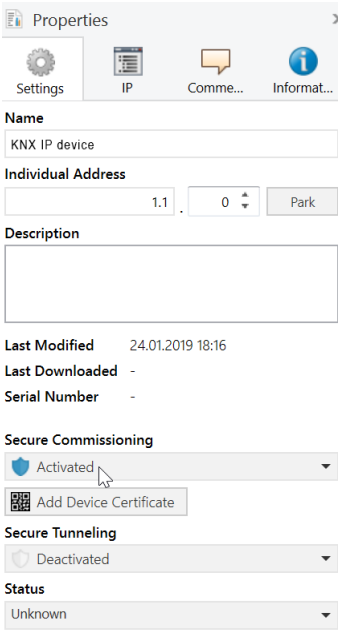


Fig. 5: Properties of the device

Function	Description
Name	Any name can be assigned, max. 50 characters.
Secure Commissioning	If activated, the encryption is active for commissioning: all parameters are then transmitted in encrypted form, although e.g. Tunnel connections are still unencrypted.
Secure Tunneling	If activated, the tunnel connections can only be established via KNX Secure Tunneling.

6.2.2 IP properties

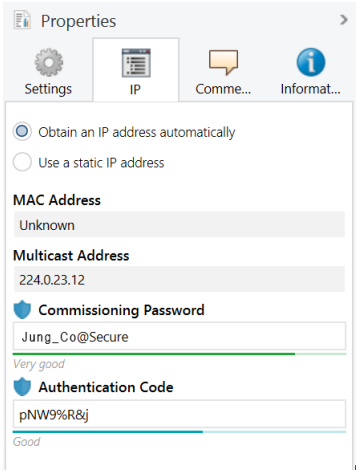


Fig. 6: IP Properties of the device

Function	Description
Obtain an IP address automatically	The IP address is assigned by a DHCP server in the network. If a DHCP server doesn't exist in the network or if it doesn't assigns the IP address within one minute, the device gets an IP address via AutoIP function. This for example allows to build up an IP connection via direct connection (without DHCP server) between PC and IP interface.
Use a static IP address	The user specifies the IP settings.
Commissioning Password	A password from which the ETS generates a key. This is the key to secure commissioning (see above).
Authentication Code	With the authentication password, the user proves that he has access to the project.
MAC Address	Is a device property.
Multicast Address	Is given by the backbone configuration. Can be changed in the topology view of the ETS.

6.2.3 KNX IP Secure

For an error-free operation of the devices in secure mode the ETS 5.7.4 or higher is required.

Requirements:

- Safe commissioning activated
- FDSK entered/scanned or device certificate added

Configuration of KNX IP Secure:

- Activate secure tunnelling.
- Define a password for each tunnel (max. 8 tunnels).
- Define a password for commissioning and authentication code.

i Document all passwords and store them securely.

6.2.4 Additional functions

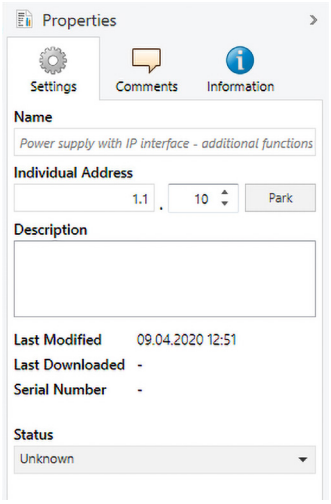


Fig. 7: Additional functions of the device

Function	Description
Name	Any name can be assigned, max. 50 characters.

6.2.5 KNX Data Secure

KNX Data Secure signs and encrypts the communication in KNX networks and provides a secured data transmission of telegrams.

The communication at commissioning processes with the ETS and the runtime communication between devices and visualisations is protected by KNX Data Secure. This ensures all KNX telegrams or just selected KNX telegrams to be authentificated and encrypted independent from the medium. The communication between transmitter and receiver can neither be interpreted nor manipulated.

Requirements:

- ETS 5.7.4 or higher
- FDSK entered/scanned or device certificate added

Symbols

Symbol	Meaning	KNX Data Secure	Secure Commissioning
	device safety is not activated	device is compatible	deactivated
	device safety is activated	device is compatible	activated
	no device safety available	device is not compatible	not possible
	device with activated device safety in application	device is compatible	activated

The ETS marks compatible devices for KNX Data Secure with a “secure shield” symbol. The symbol will be displayed in the list view of devices and in the tree structure of an opened ETS project. It doesn’t refer directly to the device but to the used application program.

When a symbol is displayed in the column “security” in the list view, the application program is compatible with KNX Data Secure. The colour of the symbol indicates an application program with activated device safety (blue) or not activated device safety (grey) for the used application.

Application programs without displayed symbol are principally not compatible with KNX Data Secure. In the tree view devices – corresponding to the used application – will also be marked with a “secure shield” symbol.

Group addresses

Devices which should safely communicate during runtime must be secure commissioned by the ETS. Group addresses will be created by the user of the ETS and receive a special safety attribute which can be edited afterwards.

Group addresses can be marked with the following safety attributes:

- unsecure – communication is conventional
- secure – communication is always safe
- automatic secure or unsecure – communication is depending on the links to objects

Only safe group addresses have an encryption during runtime. Compatible devices for KNX Data Secure which were secure commissioned and are interchanging secured data via communication objects with other devices for KNX Data Secure during runtime can principally also communicate conventional (unsecure) via selected group addresses. A combined operation of secure and conventional communication is possible at a sensor or actuator via different communication objects. But the communication via Secure and Unsecure with one and the same group address and therefore the same object is not possible.

6.3 Device-specific parameters

6.3.1 General settings

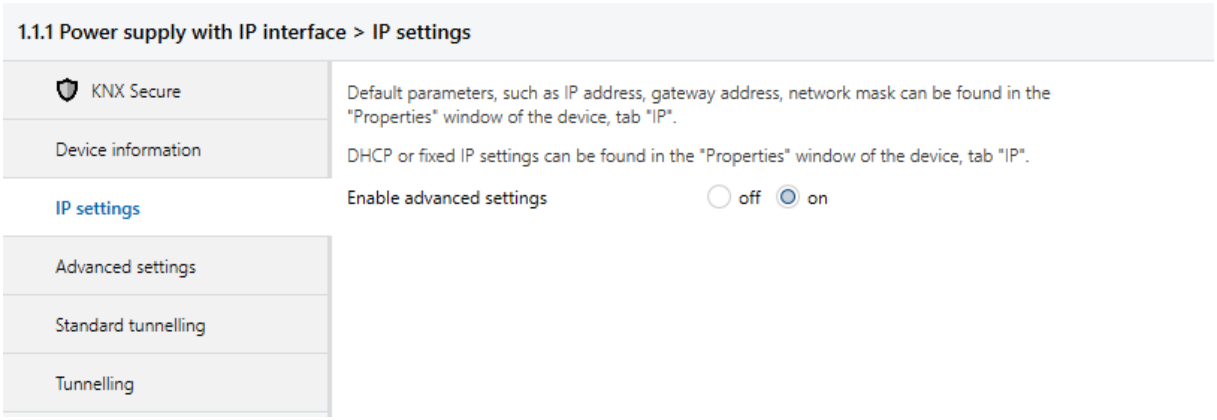


Fig. 8: General settings of the device

Function	Options	Description
(Text)		The ETS has manufacturer-independent uniform parameter descriptions for various settings. To simplify the application, a note text is displayed here.
Enable advanced settings	off/on	Advanced functions to ensure a maximum of flexibility.

6.3.2 Advanced settings

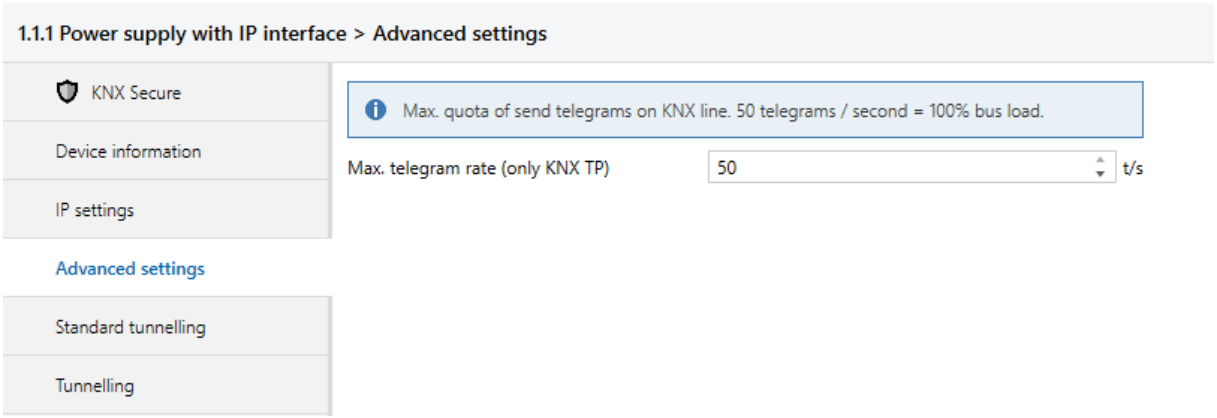


Fig. 9: Advanced settings of the device

Function	Options	Description
Max. number of telegrams to KNX TP	5 .. 50	See parameter description

Advanced settings standard tunnel preferred IP

For standard tunnel connections (before 2019) it is possible to assign each of these tunnel connections to an IP address. In the analysis of group telegrams, this makes it easier to assign the telegrams to the sender which „sits“ behind the tunnel, as e.g. Visualizations or smartphone apps.

i This assignment can be resolved at any time by the ETS or a new so-called extended tunnel connection (as of 2019).

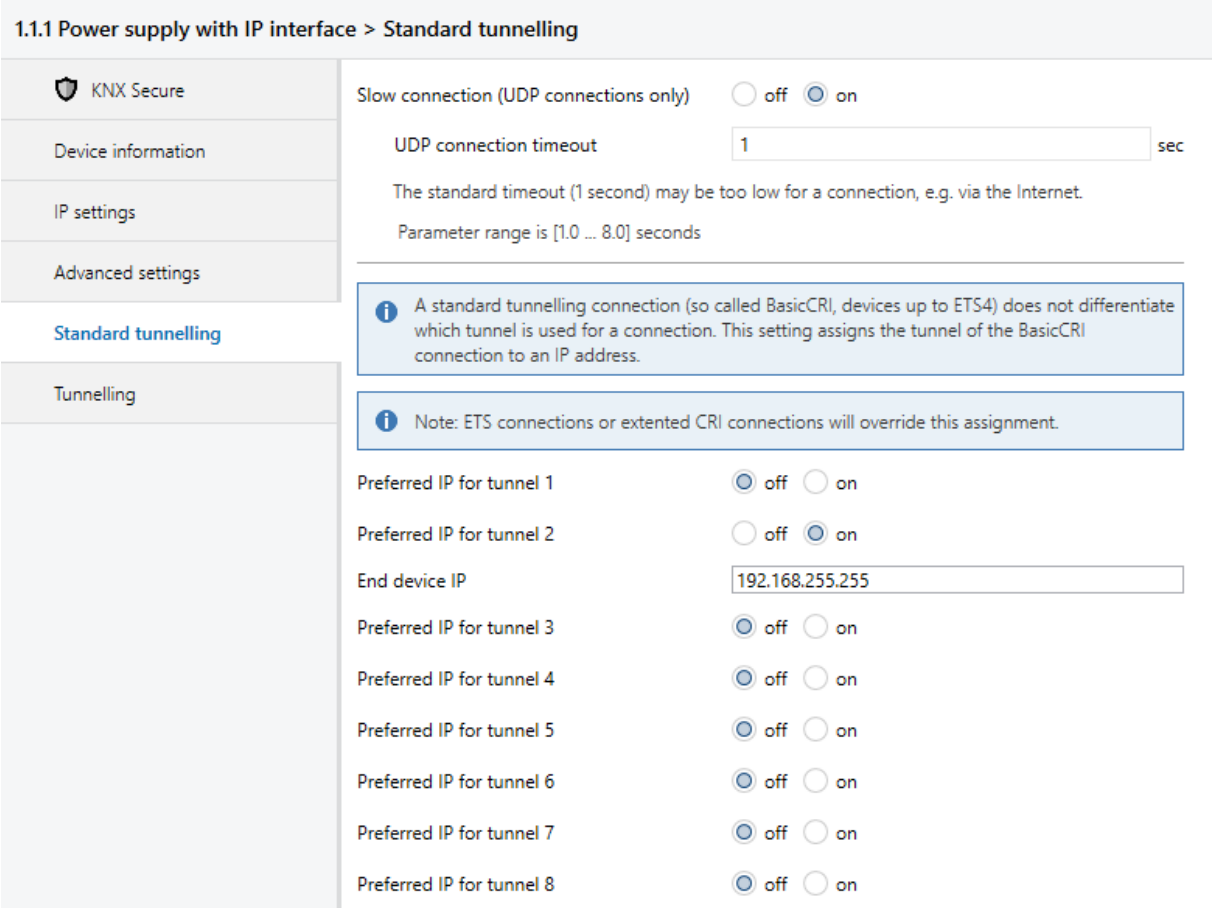


Fig. 10: Preferred IP for Tunnelling

Function	Options	Description
Slow connection	off/on	The tunnel connections over UDP are controlled by default with a connection timeout of 1 second. This may be too short for connections over the Internet.
UDP connection timeout	1.0 ... 8.0 sec	Setting of timeout for tunnel connection over UDP
Preferred IP for tunnel X	off/on	Tunnel X should preferably be used for communication with the parametrized IP address.
End device IP	(IP-V4 address)	IP address of end device

6.4 General settings

6.4.1 Application program A

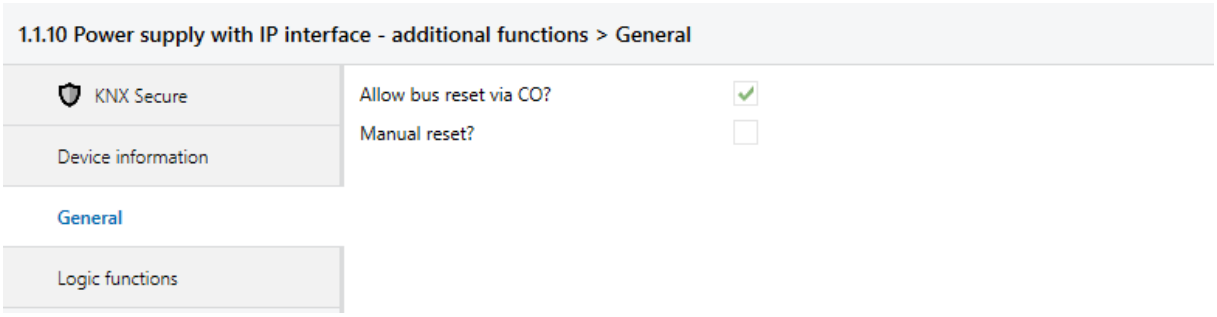


Fig. 11: General settings of the device

Function	Options	Description
Allow bus reset via CO?	active/inactive	Releases a communication object to trigger a bus reset.
Manual reset?	active/inactive	When active, the reset can be triggered via reset button at the device. When inactive, the function of the reset button is locked. In this case the reset of error states (overvoltage and overload) via reset button is not possible anymore.

Logic functions

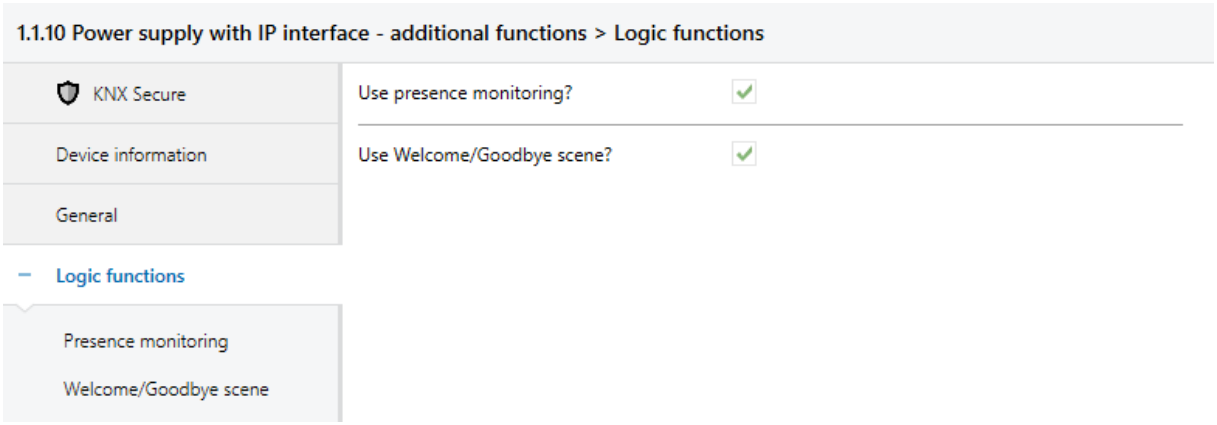


Fig. 12: Logic functions

Function	Options	Description
Use presence monitoring?	active/inactive	When active, the area for presence monitoring will be unlocked. In this area the presence monitoring (with key card holder or with presence detector) can be configured and the triggers for Welcome/Goodbye scenes can be configured.
Use Welcome/Goodbye scene?	active/inactive	When active, the area for Welcome/Goodbye scenes will be unlocked. In this area the triggers for Welcome/Goodbye scenes can be configured and the Welcome/Goodbye scenes can be configured.

Presence monitoring

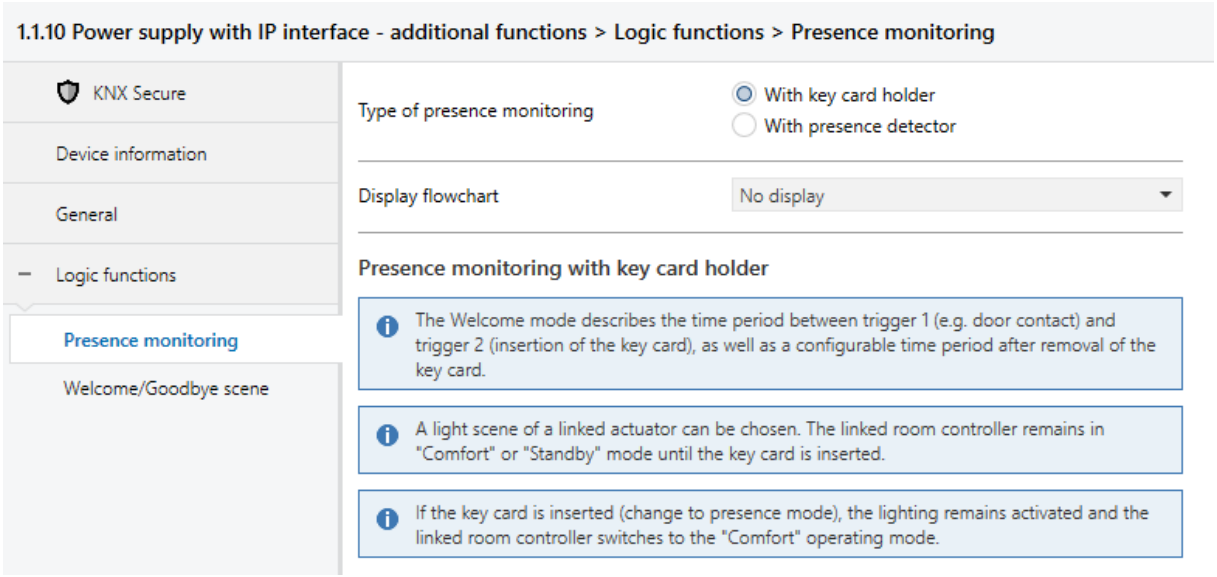


Fig. 13: Presence monitoring

Function	Options	Description
Type of presence monitoring	With key card holder/ With presence detector	When active, the area for presence monitoring will be unlocked. In this area the presence monitoring (with key card holder or with presence detector) can be configured and the triggers for Welcome/Goodbye scenes can be configured.

Presence monitoring key card holder

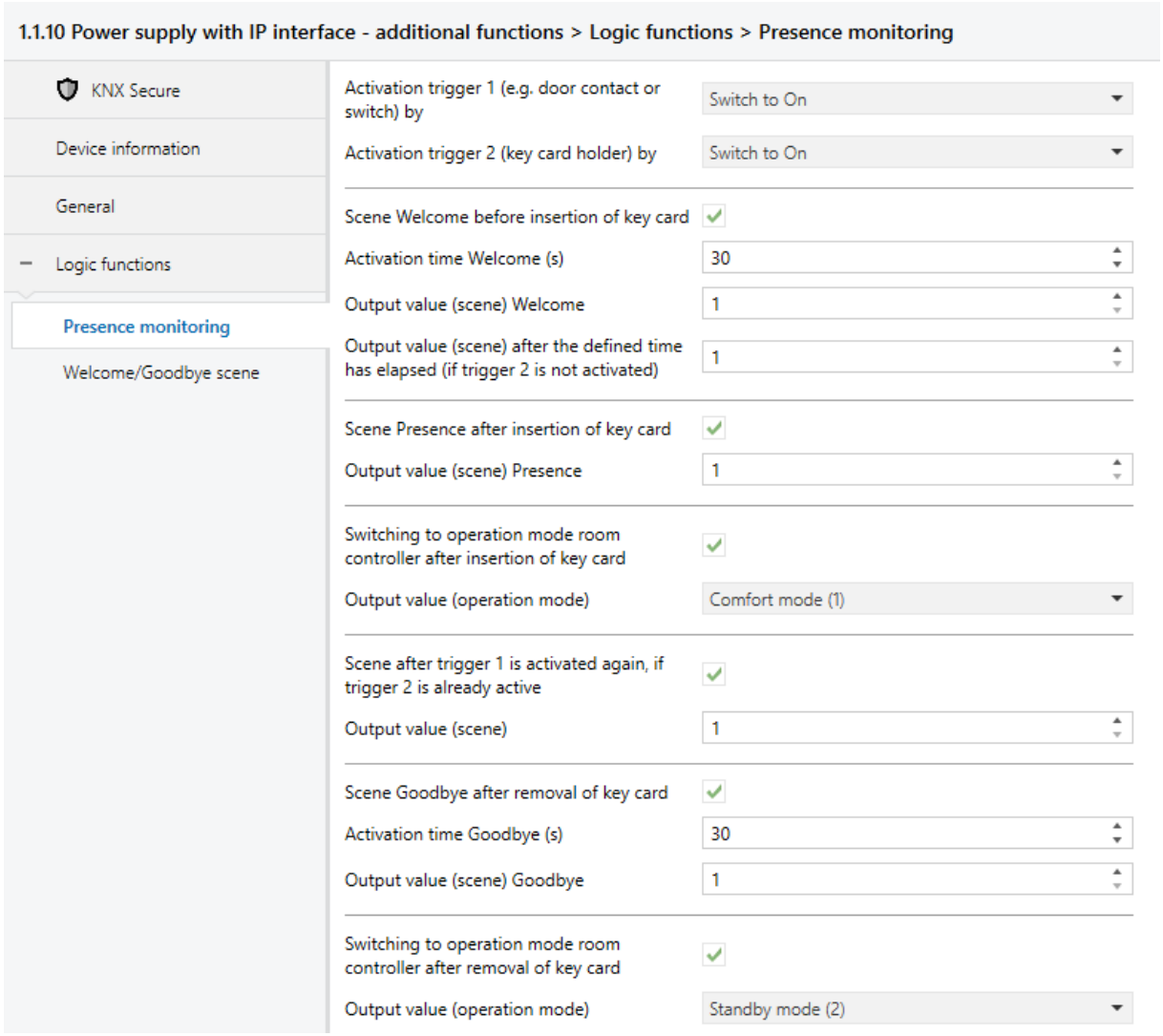


Fig. 14: Presence monitoring key card holder

Function	Options	Description
Activation trigger 1 (e.g. door contact or switch) by	Switch to On/ Switch to Off/ Switch-over	The activation of trigger 1 can be selected. By selecting “Switch-over“ the trigger is activated by switching to On or switching to Off.
Activation trigger 2 (e.g. key card holder) by	Switch to On/ Switch to Off/ Switch-over	The activation of trigger 2 can be selected. By selecting “Switch-over“ the trigger is activated by switching to On or switching to Off.

Function	Options	Description
Scene Welcome before insertion of key card	active/inactive	When active, scene Welcome will be activated by trigger 1. But the scene will only be activated when trigger 2 is not active during activation of trigger 1, e.g. when door is opened but key card is not inserted.
Activation time Welcome (s)	1 .. 30 .. 120	Duration for activated scene Welcome. After this time the scene of the extension scene (KO16) changes from parameter “Output value Welcome“ to parameter “Output value after expiration of defined time“.
Output value (scene) Welcome	1 .. 64	Value which is sent to the extension scene (KO16) by activation of scene Welcome.
Output value (scene) after the defined time has elapsed (if trigger 2 is not activated)	1 .. 64	Value which is sent to the extension scene (KO16) after expiration of scene Welcome.
Scene Presence after insertion of key card	active/inactive	When active, scene Presence will be activated by activation of trigger 2. But the scene will not be activated when time delay for function Goodbye is activated. This avoids retriggering of scene Presence if the key card is inserted and removed multiple times.
Output value (scene) Presence	1 .. 64	Value which is sent to the extension scene (KO16) by activation of scene Presence.
Switching to operation mode room controller after insertion of key card	active/inactive	When active, operation mode of room controller will be sent by activation of trigger 2 according to parameter “Output value (operation mode)”.
Output value (operation mode)	Automatic (0)/ Comfort mode (1)/ Standby mode (2)/ Night mode (3)/ Frost/heat protection (4)	Value which is sent to operation mode of room controller (KO32) by activation of trigger 2.
Scene after trigger 1 is activated again, if trigger 2 is already active	active/inactive	Another scene can be activated here when trigger 1 is activated again and trigger 2 is already activated. This scene can be used e.g. for scenario “2nd person is entering room”.
Output value (scene)	1 .. 64	Value which is sent to the extension scene (KO16) by activation of trigger 1 when trigger 2 is already activated.

Function	Options	Description
Scene Goodbye after removal of key card	active/inactive	When active, scene Goodbye is activated with time delay after deactivation of trigger 2. The time delay is set with parameter “Activation time Goodbye (s)“.
Activation time Goodbye (s)	1 .. 30 .. 120	Time delay in seconds which activates scene Goodbye
Output value (scene) Goodbye	1 .. 64	Value which is sent to the extension scene (KO16) by activation of scene Goodbye.
Switching to operation mode room controller after removal of key card	active/inactive	When active, operation mode of room controller will be sent by deactivation of trigger 2 according to parameter “Output value (operation mode)”. This happens without time delay.
Output value (operation mode)	Automatic (0)/ Comfort mode (1)/ Standby mode (2)/ Night mode (3)/ Frost/heat protection (4)	Value which is sent to operation mode of room controller (KO32) by deactivation of trigger 2.

Presence monitoring presence detector

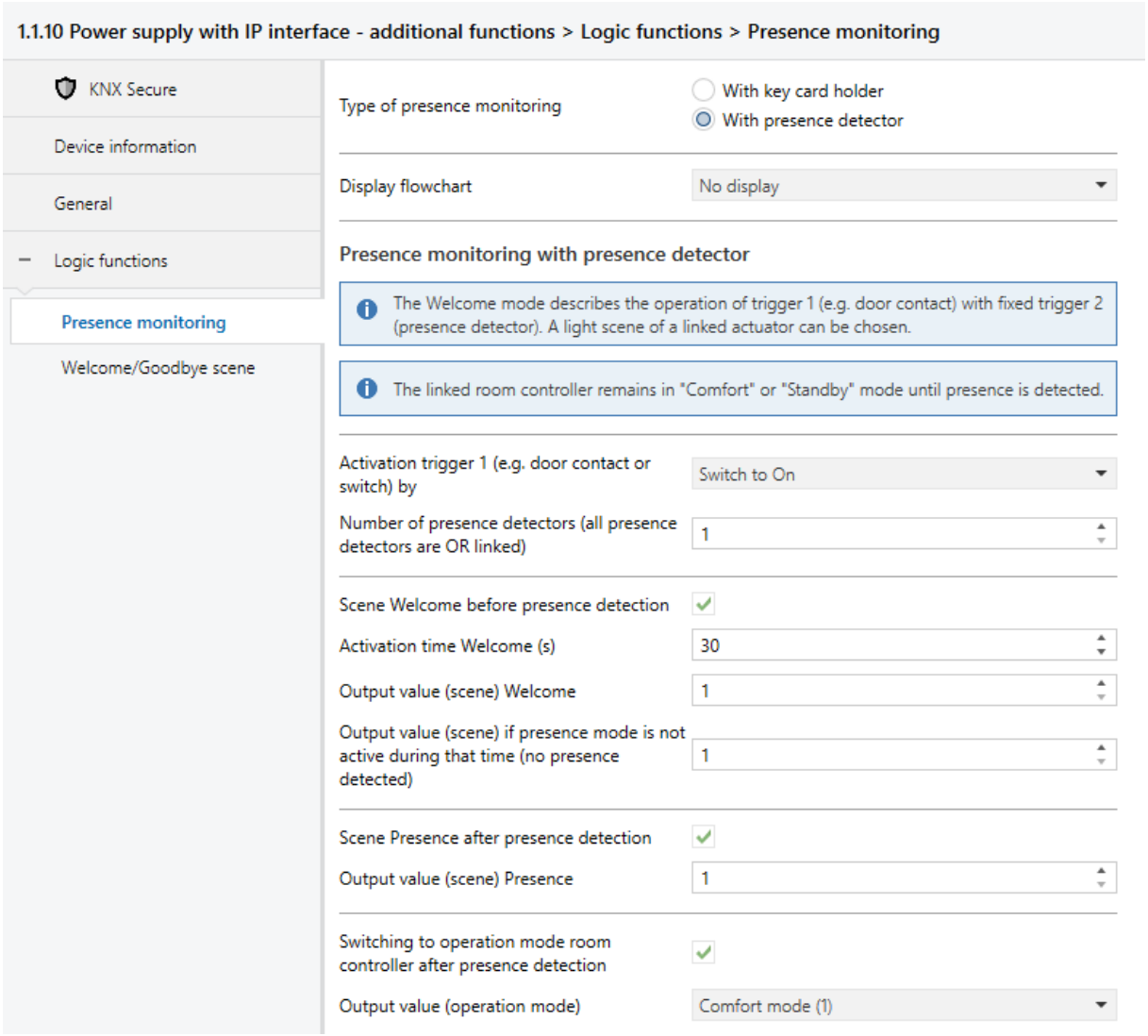


Fig. 15: Presence monitoring presence detector

Function	Options	Description
Activation trigger 1 (e.g. door contact or switch) by	Switch to On/ Switch to Off/ Switch-over	The activation of trigger 1 can be selected. By selecting “Switch-over“ the trigger is activated by switching to On or switching to Off.
Number of presence detectors (all presence detectors are OR linked)	1 .. 5	The number of used presence detectors can be selected. For every presence detector and its value one CO will be unlocked. For all functions the result of all presence detectors from the OR link will be used.

Function	Options	Description
Scene Welcome before presence detection	active/inactive	When active, scene Welcome will be activated by trigger 1. But the scene will only be activated when trigger 2 is not active during activation of trigger 1, e.g. when no presence is detected in the room until this moment.
Activation time Welcome (s)	1 .. 30 .. 120	Duration for activated scene Welcome. After this time the scene of the extension scene (KO16) changes from parameter “Output value Welcome“ to parameter “Output value if presence mode is not active during that time“.
Output value (scene) Welcome	1 .. 64	Value which is sent to the extension scene (KO16) by activation of scene Welcome.
Output value (scene) if presence mode is not active during that time (no presence detected)	1 .. 64	Value which is sent to the extension scene (KO16) after expiration of scene Welcome.
Scene Presence after presence detection	active/inactive	When active, scene Presence will be activated by activation of trigger 2. But the scene will only be activated once after trigger 1 was activated. This avoids retriggering of scene Presence if the presence detector changes his presence status multiple times.
Output value (scene) Presence	1 .. 64	Value which is sent to the extension scene (KO16) by activation of scene Presence.
Switching to operation mode room controller after presence detection	active/inactive	When active, operation mode of room controller will be sent by activation of trigger 2 according to parameter “Output value (operation mode)”.
Output value (operation mode)	Automatic (0)/ Comfort mode (1)/ Standby mode (2)/ Night mode (3)/ Frost/heat protection (4)	Value which is sent to operation mode of room controller (KO32) by activation of trigger 2.

Presence monitoring presence detector – Presence mode

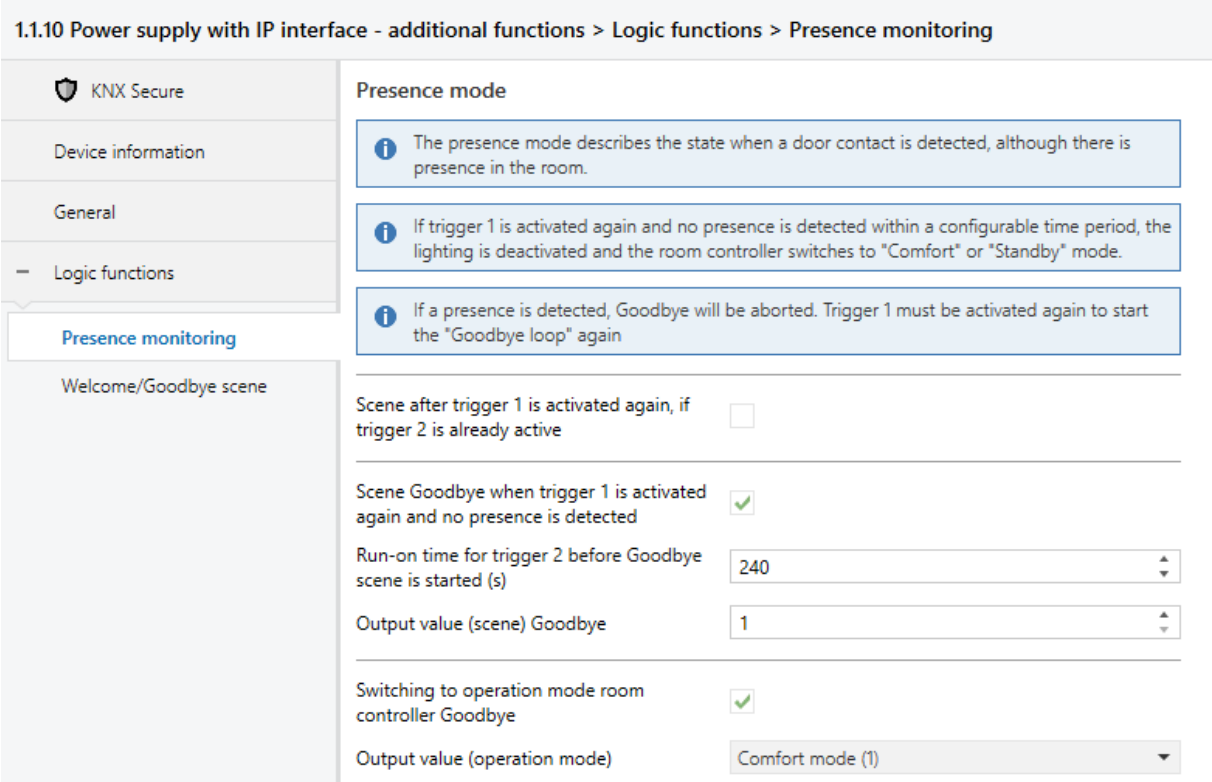


Fig. 16: Presence monitoring presence detector – Presence mode

Function	Options	Description
Scene after trigger 1 is activated again, if trigger 2 is already active	active/<u>inactive</u>	Another scene can be activated here when trigger 1 is activated again and trigger 2 is already activated. This scene can be used e.g. for scenario “2nd person is entering room”.
Scene Goodbye when trigger 1 is activated again and no presence is detected	<u>active</u>/inactive	Scene Goodbye can be activated here. Scene Goodbye is activated with time delay by activation of trigger 1. But it is only activated if trigger 2 is “OFF” or “not occupied” during activation of scene. The time delay is set with parameter “Run-on time for trigger 2 before Goodbye scene is started“.

Function	Options	Description
Run-on time for trigger 2 before Goodbye scene is started (s)	1 .. 30 .. 3600	Time delay in seconds which activates scene Goodbye after activation by trigger 1. Parameterization note: If scenes Goodbye and Welcome are used together, the time delay must be longer than activation time of scene Welcome. This avoids an accidental permanently lit of the room light after leaving the room.
Output value (scene) Goodbye	1 .. 64	Value which is sent to the extension scene (KO16) by activation of scene Goodbye.
Switching to operation mode room controller Goodbye	active/inactive	When active, operation mode of room controller will be sent by activation of scene Goodbye according to parameter “Output value (operation mode)”.
Output value (operation mode)	Automatic (0)/ Comfort mode (1)/ Standby mode (2)/ Night mode (3)/ Frost/heat protection (4)	Value which is sent to operation mode of room controller (KO32) by activation of scene Goodbye.

Welcome/Goodbye scene

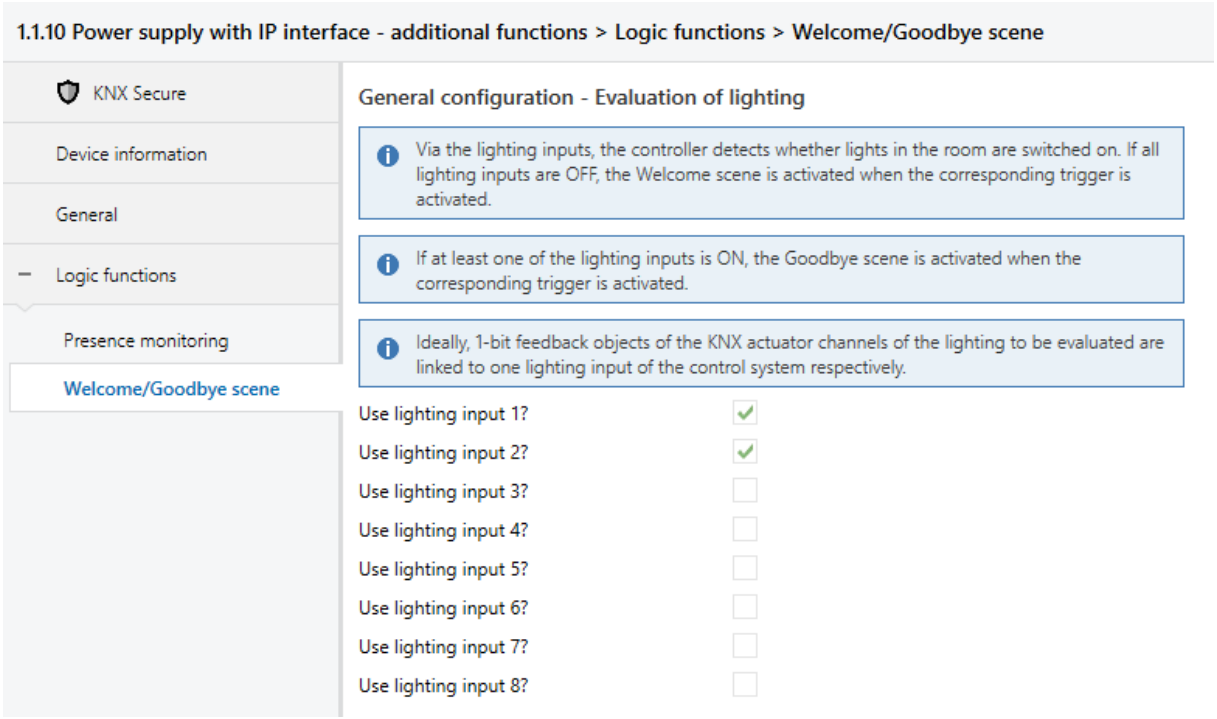


Fig. 17: Welcome/Goodbye scene

Function	Options	Description
Use lighting input 1?	active/inactive	When active, this input (KO55) is used as a criterion for activating the Welcome scene or the Goodbye scene by trigger 1. By activation the communication object 55 will be unlocked.
Use lighting input 2?	active/inactive	When active, this input (KO56) is used as a criterion for activating the Welcome scene or the Goodbye scene by trigger 1. By activation the communication object 56 will be unlocked.
Use lighting input 3 .. 8?	active/inactive	When active, this input (KO57 .. KO62) is used as a criterion for activating the Welcome scene or the Goodbye scene by trigger 1. By activation the communication object 57 .. 62 will be unlocked.

Welcome/Goodbye scene – Scene Welcome

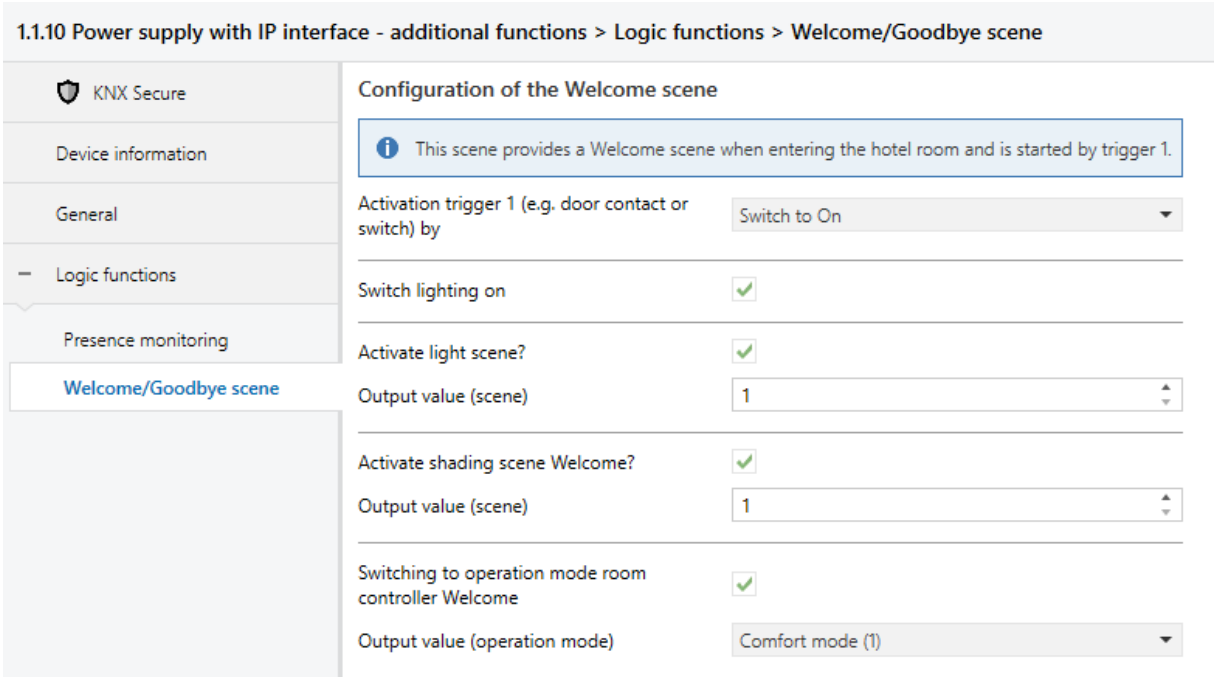


Fig. 18: Welcome/Goodbye scene – Scene Welcome

Function	Options	Description
Activation trigger 1 (e.g. door contact or switch) by	Switch to On/ Switch to Off/ Switch-over	The activation of trigger 1 can be selected. By selecting “Switch-over“ the trigger is activated by switching to On or switching to Off.
Switch lighting on	active/inactive	When active, the lighting will be switched on by activation of the Welcome scene and the value “ON” will be sent to communication object 165.
Activate light scene?	active/inactive	When active, the light scene will be activated by activation of the Welcome scene. The following value will be sent to the extension scene (KO194) by this.
Output value (scene)	1 .. 64	Value which is sent to the extension scene (KO194) by activation of the light scene.
Activate shading scene Welcome	active/inactive	When active, the shading scene will be activated by activation of the Welcome scene. The following value will be sent to the extension scene (KO214) by this.
Output value (scene)	1 .. 64	Value which is sent to the extension scene (KO214) by activation of the light scene.

Function	Options	Description
Switching to operation mode room controller Welcome	active/inactive	When active, operation mode of room controller will be sent by activation of scene Welcome according to parameter “Output value (operation mode)”.
Output value (operation mode)	Automatic (0)/ Comfort mode (1)/ Standby mode (2)/ Night mode (3)/ Frost/heat protection (4)	Value which is sent to operation mode of room controller (KO234) by activation of Welcome scene.

Welcome/Goodbye scene – Scene Goodbye

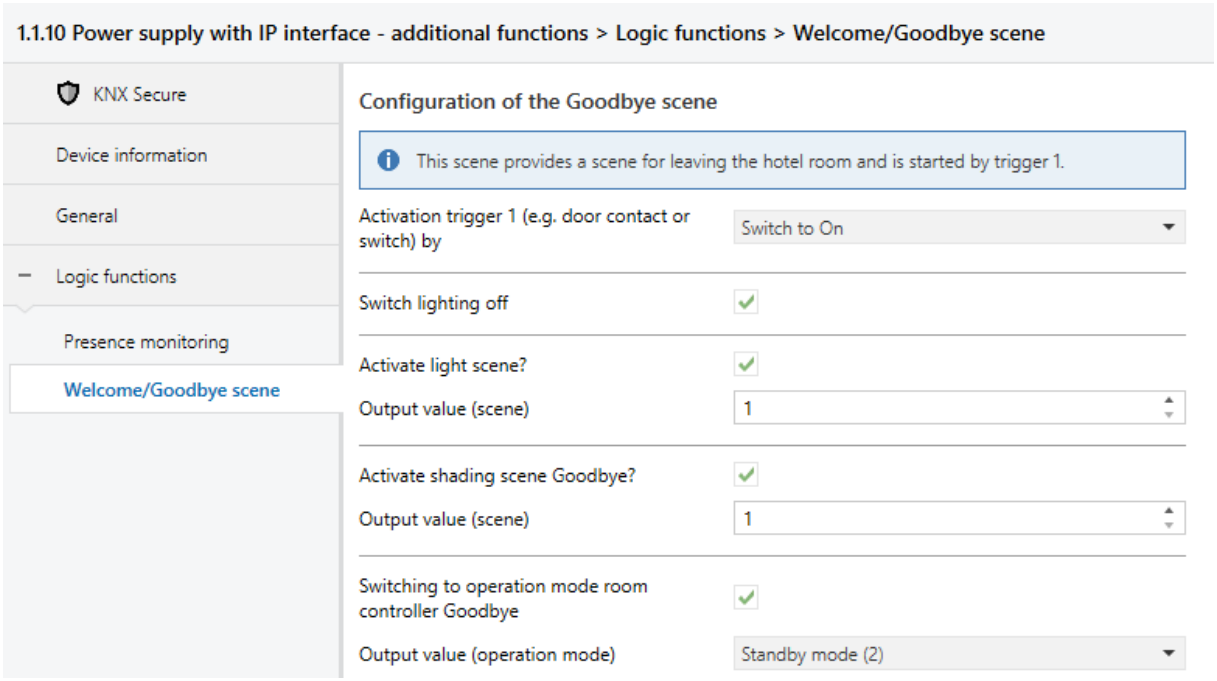


Fig. 19: Welcome/Goodbye scene – Scene Goodbye

Function	Options	Description
Activation trigger 1 (e.g. door contact or switch) by	Switch to On/ Switch to Off/ Switch-over	The activation of trigger 1 can be selected. By selecting “Switch-over“ the trigger is activated by switching to On or switching to Off.
Switch lighting off	active/inactive	When active, the lighting will be switched off by activation of the Goodbye scene and the value “OFF” will be sent to communication object 166.
Activate light scene?	active/inactive	When active, the light scene will be activated by activation of the Goodbye scene. The following value will be sent to the extension scene (KO195) by this.

Function	Options	Description
Output value (scene)	1 .. 64	Value which is sent to the extension scene (KO195) by activation of the light scene.
Activate shading scene Goodbye?	active/inactive	When active, the shading scene will be activated by activation of the Welcome scene. The following value will be sent to the extension scene (KO215) by this.
Output value (scene)	1 .. 64	Value which is sent to the extension scene (KO215) by activation of the light scene.
Switching to operation mode room controller Goodbye	active/inactive	When active, operation mode of room controller will be sent by activation of scene Welcome according to parameter “Output value (operation mode)”.
Output value (operation mode)	Automatic (0)/ Comfort mode (1)/ Standby mode (2)/ Night mode (3)/ Frost/heat protection (4)	Value which is sent to operation mode of room controller (KO234) by activation of Welcome scene.

6.4.2 Application program B

Further functionalities are provided by the additional application.

- Timer
- Remote maintenance
- Mapper

Timer

- External timer server (NTP) as the source of time synchronisation when commissioning
- External time server can be set to a static IP address or via pool.ntp.org
- Status for the availability of the external time server
- Status for the validity of the internal clock (e.g. after power failure)
- User-controlled synchronisation with external time server

The timer synchronises the time of the integrated real time clock via the internet with pool.ntp.org or with another local source. This time can be issued to the KNX bus as a time or date telegram. When power fails, the device will buffer the time for approx. 36 hours. Every 48 hours and when restarting, the time automatically synchronises with the NTP server. Via a communisation object (referred to as KO below), the synchronisation can be requested manually by the user.

The “validity” of the time is issued via a separate KO. As long as the real time clock is power supplied, the time is valid. If, e.g., in normal operation a synchronisation is not possible because the internet connection is interrupted, the internal time continues to be valid. The last synchronisation failure can be checked via a separate KO using a reading request. If the status changes, this change will be issued on the bus.

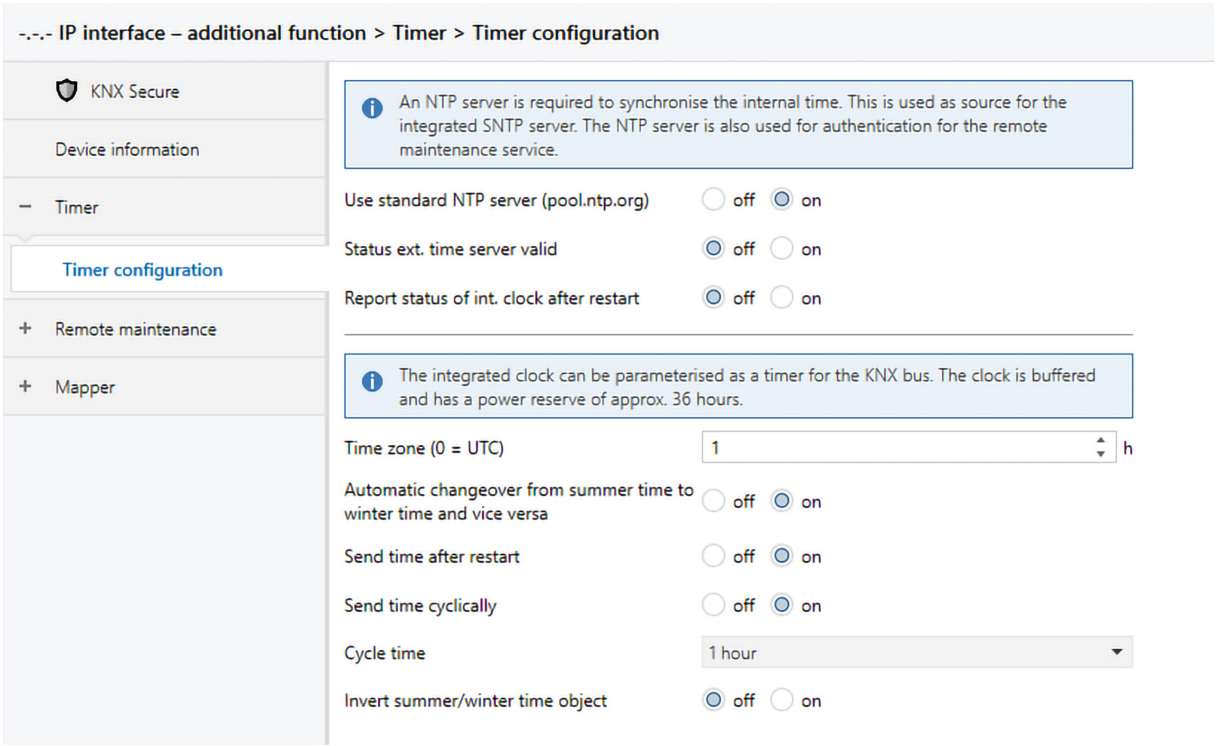


Fig. 20: Additional functions, Timer

Function	Options	Description
Use standard NTP server (pool.ntp.org)	off/<u>on</u>	See parameter dialogue If "off" is chosen here, an input field for the IP address of the own external time server is displayed.
Status ext. time server valid	<u>off</u>/on	Notification via KO1
Report status of int. clock after restart	<u>off</u>/on	Notification via KO2

Function	Options	Description
Time zone (0 = UTC)	-12 ... 1 ... +14	Time lapse between internal time to UTC
Automatic changeover from summer to winter time and vice versa	off/on	
Send time after restart	off/on	Display of time and date via KO3, KO4, KO5
Send time cyclically	off/on	
Cycle time	24 hours 12 hours 3 hours 1 hour 30 minutes 15 minutes	Cyclical display of time and date via KO3, KO4, KO5

When shipping the device, the internal clock is invalid. Therefore the communication object KO2 is false [0].

The internal clock becomes valid (value = true [1]) once the device can reach an external time server (NTP server).

This happens after every restart but at least once a week automatically. For this to work, the NTP server specified has to be available.

After a restart or an ETS programming operation of the device, the time continues to be valid.

Only it the power reserve of the internal clock is low because the power was off for more than 36 hours, the time will again become invalid.

The internal clock can deviate approx. 1 second per 2 days from real time.

Mapper

- Translation of secure to plain communication objects.
- Mapping of up to 20 communication objects.
- Size of every communication object configurable between 1 bit, 2 bit, 4 bit , 8 bit, 16 bit, 24 bit, 32 bit, 6 bytes, 8 bytes and 14 bytes.

The mapper serves to translate secure to plain communication objects. For this, the mapper provides 20 channels, which communicate bidirectionally. The user can configure the communication objects in such a way that the group addresses have different lengths (max. 14 bytes).

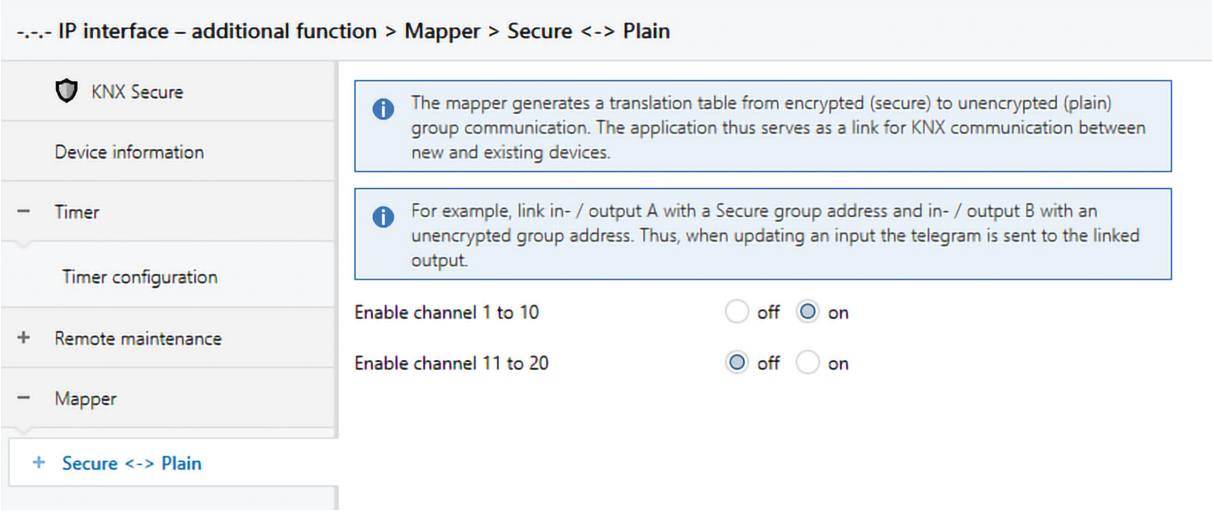


Fig. 21: Additional functions, Mapper

Function	Options	Description
Enable channel 1 to 10	off/<u>on</u>	see below
Enable channel 11 to 20	<u>off</u>/on	see below

The mapper serves to translate secure to plain communication objects. For this, the mapper provides 20 channels, which communicate bidirectionally. The user can configure the communication objects in such a way that the group addresses have different lengths (max. 14 bytes). The length can be configured between 1 bit, 2 bit, 4 bit , 8 bit, 16 bit, 24 bit, 32 bit, 6 bytes, 8 bytes and 14 bytes.

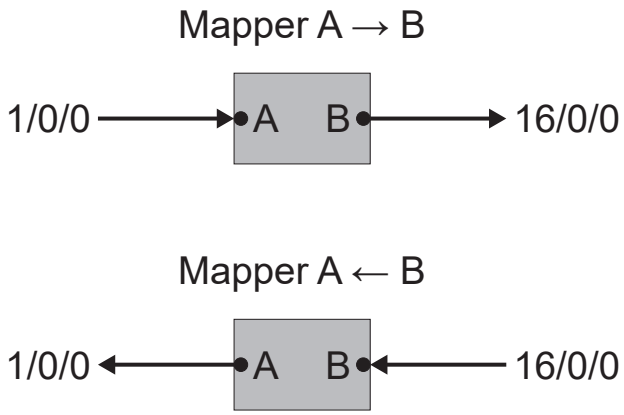


Fig. 22: Mapper writes on group addresses

Figure 22 shows the functionality described. Writing (or answering) to 1/0/0 (input/output A) triggers writing to 16/0/0 (input/output B). Therefore it is irrelevant whether 1/0/0 or 16/0/0 are encrypted or not. 1/0/0 could, for example, be an encrypted group address and 16/0/0 an unencrypted address. This way, one (or more) encrypted group addresses can be sent via an unencrypted one. The same is true the other way round. If several links according to the KNX regulation are used, it is important that a maximum of one group address is sending.

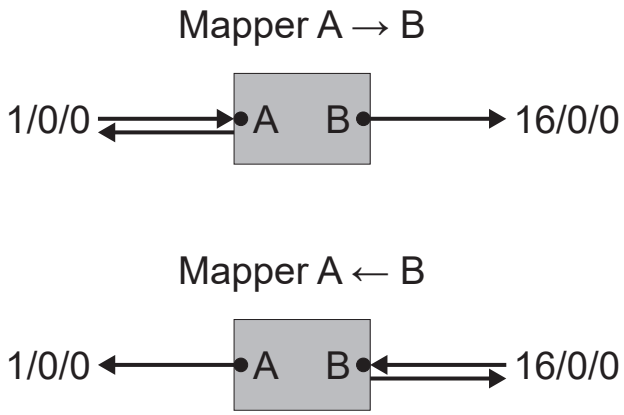


Fig. 23: Mapper reads on group addresses

Figure 23 shows the functionality described for reading. Reading via 1/0/0 (input/output A) triggers reading via 16/0/0 (input/output B). If the reading flag for input/output A is placed, the request of input/output A is answered with an answer telegram. If afterwards, the communication partners involved send an answer telegram, it will be treated as in figure 22. Therefore it is irrelevant whether 1/0/0 or 16/0/0 are encrypted or not. 1/0/0 could, for example, be an encrypted group address and 16/0/0 an unencrypted address. This way, a reading request of an encrypted group address can follow an unencrypted one. The same is true the other way round.

The application combines the mapper into the channels 1 to 10 and 11 to 20 for reasons of better overview. Every channel, containing both entries/exits A and B, can be configured to the length of choice.

i The mapper only works with group addresses which are connected to another device. Group addresses which are connected to own communication objects, e.g. KO1 to KO13 will not be treated by the mapper in the way described.

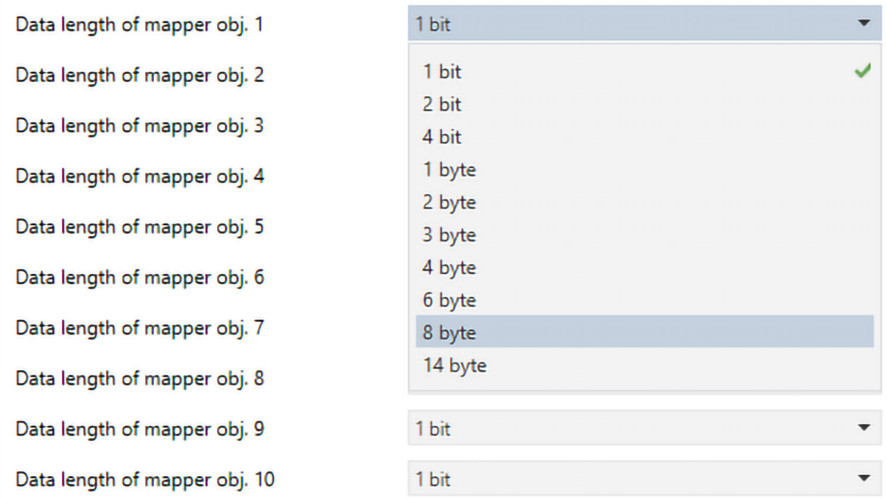


Fig. 24: Data length of mapper

Directions of communication:

Using the flags of the group addresses, directing group addresses through the mapper can be set to be dependant on the direction and on the kind of communication (reading or writing), The communication flags will have to be set as described in the table.

The communication flags for channel A are in column “Flags A” and for channel B in column “Flags B”. Flags not listed do not have to be set. The direction of the arrows show in which direction the communication (reading or writing) is possible. A → B: A to B is the mapper direction possible as described in the table. There is no mapping of group addresses from B to A.

The communication flags found in ETS are sketched in figure 25.

In the table, the letters describe the same flags as in the ETS. C for example, for communication, R for reading etc.

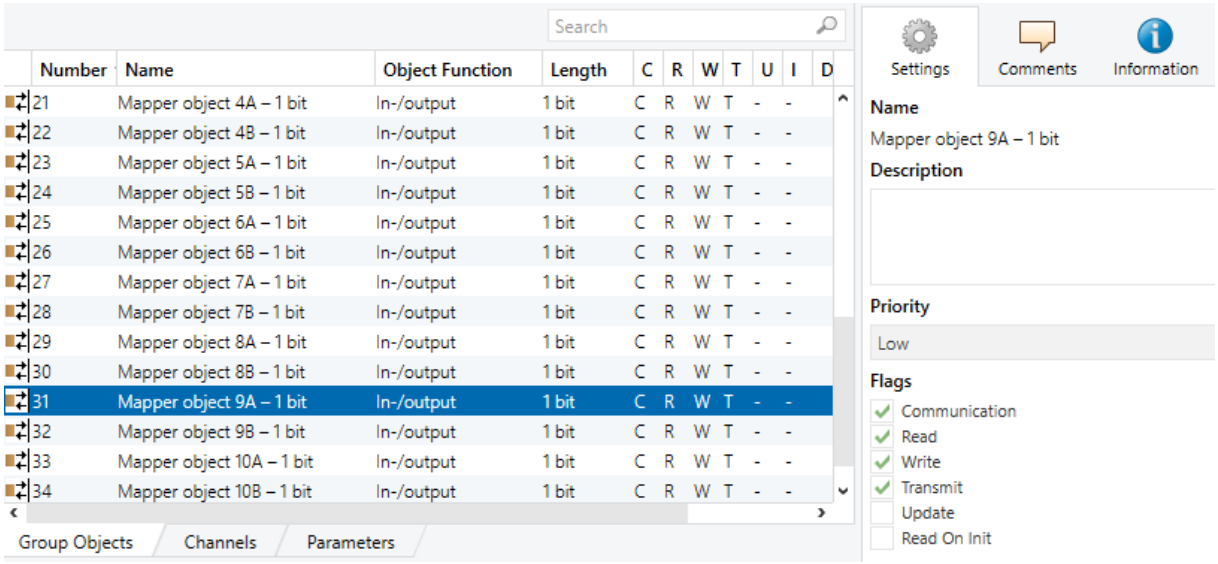


Fig. 25: Mapper flags

Directions	Reading	Writing	Flags A	Flags B
A ↔ B	yes	yes	CRWT--	CRWT--
A ↔ B	yes	–	CR-T--	CR-T--
A ↔ B	–	yes	C-WT--	C-WT--
A → B	yes	yes	CRW--	C-WT--
A → B	yes	–	CR----	C-WT--
A → B	–	yes	C-W---	C-WT--
A ← B	yes	yes	C-WT--	CRW---
A ← B	yes	–	C-WT--	CR----
A ← B	–	yes	C-WT--	C-W---

6.5 Object table

6.5.1 Application program A

ⓘ Depending on the parametrization some objects might not be available.

ID	Name	Object function	Length	Type	Flags
1	General	**Reset of bus voltage – Input**	1 bit	[1.009] DPT_Trigger	C-W---
Object for triggering a bus reset.					

6	Logic 1 - input - presence monitoring	**Trigger 1 (1 bit)**	1 bit	[1.009] DPT_OpenClose	C-WT--
Input object for the logic of presence detection. Can be linked e.g. with a door contact or with a switch.					

7	Logic 1 - input - key card holder	**Trigger 2 (1 bit)**	1 bit	[1.001] DPT_Switch	C-WT--
Input object for the logic of presence detection with key card holder.					

8	Logic 1 - input - presence detector 1	**Trigger 2 (1 bit)**	1 bit	[1.018] DPT_Occupancy	C-WT--
Input object for the logic of presence detection with presence detector.					

9	Logic 1 - input - presence detector 2	**Trigger 2 (1 bit)**	1 bit	[1.018] DPT_Occupancy	C-WT--
Input object for the logic of presence detection with presence detector.					

10	Logic 1 - input - presence detector 3	**Trigger 2 (1 bit)**	1 bit	[1.018] DPT_Occupancy	C-WT--
Input object for the logic of presence detection with presence detector.					

11	Logic 1 - input presence detector 4	**Trigger 2 (1 bit)**	1 bit	[1.018] DPT_Occupancy	C-WT--
Input object for the logic of presence detection with presence detector.					

12	Logic 1 - input presence detector 5	**Trigger 2 (1 bit)**	1 bit	[1.018] DPT_Occupancy	C-WT--
Input object for the logic of presence detection with presence detector.					

13	Logik 2 - input - Welcome/Goodbye	**Trigger 1 (1 bit)**	1 bit	[1.017] DPT_Trigger	C-WT--
Input object for the logic of the activation of a Welcome/Goodbye scene. Can be linked e.g. with a door contact or with a switch.					

ID	Name	Object function	Length	Type	Flags
16	Logic 1 - output - presence monitoring	**Scene extension (1 byte)**	1 byte	[17.001]	C-W---
Output object for the activation of scenes corresponding to presence monitoring of logic 1.					

32	Logic 1 - output - presence monitoring	**Room controller operation mode (1 byte)**	1 byte	[20.102] DPT_HVACM	C-T--
Output object for switch-over the operation mode of a room controller corresponding to presence monitoring of logic 1.					

55 - 65	Logic 2 - input - Welcome/Goodbye	**Switching input 1 – 8 (1 bit)**	1 bit	[1.002] DPT_Bool	C-WT--
Input object 1 - 8 for the logic of the activation of a Welcome/Goodbye scene. Can be linked e.g. with the status object of a lighting.					

165	Logic 2 - output - Welcome	**Switching (1 bit)**	1 bit	[1.001] DPT_Switch	C--T--
Output object for switching a lighting corresponding to the Welcome scene of logic 2.					

166	Logic 2 - output - Goodbye	**Switching (1 bit)**	1 bit	[1.001] DPT_Switch	C--T--
Output object for switching a lighting corresponding to the Goodbye scene of logic 2.					

194	Logic 2 - output - Welcome	**Scene extension lighting (1 byte)**	1 byte	[17.001] DPT_ SceneNumber	C--T--
Output object for triggering a lighting scene corresponding to the Welcome scene of logic 2.					

195	Logic 2 - output - Goodbye	**Scene extension lighting (1 byte)**	1 byte	[17.001] DPT_ SceneNumber	C--T--
Output object for triggering a lighting scene corresponding to the Goodbye scene of logic 2.					

214	Logic 2 - output - Welcome	**Scene extension blinds (1 byte)**	1 byte	[17.001] DPT_ SceneNumber	C--T--
Output object for triggering a blinds scene corresponding to the Welcome scene of logic 2.					

215	Logic 2 - output - Goodbye	**Scene extension blinds (1 byte)**	1 byte	[17.001] DPT_ SceneNumber	C--T--
Output object for triggering a blinds scene corresponding to the Goodbye scene of logic 2.					

ID	Name	Object function	Length	Type	Flags
234	Logic 2 - output - Welcome	**Room controller operation mode (1 byte)**	1 byte	[20.102] DPT_HVACM	C--T--
Output object for switch-over the operation mode of a room controller corresponding to the Welcome scene of logic 2.					

235	Logic 2 - output - Goodbye	**Room controller operation mode (1 byte)**	1 byte	[20.102] DPT_HVACM	C--T--
Output object for switch-over the operation mode of a room controller corresponding to the Goodbye scene of logic 2.					

6.5.2 Application program B

i Depending on the configuration, some object may not be available.

ID	Name	Object function	Length	Type	Flags
1	External time server valid – output	**Status**	1 bit	[1.2] DPT_Bool	CR-T--
Shows whether the external time server pool.ntp.org can be reached by the device. The DNS Server 9.9.9.9 is responsible for the name resolution. For more information, go to www.quad9.net. If using an own NTP time server, the IP address has to be known. In this case, the KO does not send. Every 2 days, the time is automatically synchronised with the external NTP server or when initiated by KO7. It the time server was not reachable during the last synchronisation, the status will be issued via this KO on the bus.					

2	Internal clock valid – output	**Status**	1 bit	[1.2] DPT_Bool	CR-T--
Shows whether the internal clock is valid. Value true [1] represents valid, value false [0] invalid. The communication object can be sent automatically after every restart via the configuration. When shipping the device, the communication object is false [0]. The clock becomes valid [value = true [1]) if the device can synchronise its time via an NTP server. After a restart or an ETS programming operation of the device, the value continues to be true [1]. Only if the internal buffer capacitor is too low on power because the power was off for several days, the time will again become invalid (value = false [0]).					

3	Time – output	**Time output**	3 bytes	[10.001] DPT_ TimeOf Day	CR-T--
Communication object for outputting the current time to the bus. The internal clock is buffered internally for approx. 1.5 days (via supercap capacitor). The internal clock can deviate approx. 1 second per 2 days from real time. A reading telegram always delivers the current time.					

4	Date – output	**Date output**	3 bytes	[11.001] DPT_Date	CR-T--
Communication object for issuing the calendar of the internal clock.					

ID	Name	Object function	Length	Type	Flags
5	Date and time – output	**Date and time output**	8 bytes	[19.001] DPT_ DateTime	CR-T--
Time and date for outputting the current time and date to the bus.					

6	Date/time – input	**Requesting**	1 bit	[1.017] DPT_ Trigger	C-WT--
Trigger for writing of KO3, KO4 and KO5. It triggers writing with 0 as well as 1.					

7	NTP server synch. – input	**Requesting**	1 bit	[1.017] DPT_ Trigger	C-WT--
Every 2 days, the internal clock is automatically synchronised with the external NTP server or when initiated by this KO. It triggers writing with 0 as well as 1.					

8	Summer / winter time - output	**Status**	1 bit	[1.xxx]	CR-T--
If summer time is active, this KO is set to 0, if winter time to 1. This KO is therefore directly usable for the change to winter configuration of heating systems.					

9	Enable remote maintenance – input	**Switching**	1 bit	[1.002] DPT_ Switch	CRWT--
Turning on remote maintenance (1) or stopping remote maintenance (0): When the user opens the remote maintenance access via this KO, Secure Tunnelling is enabled for this duration. The interface connects to the relay server. There is no decryption on the cloud. The customer's connection can be either IPv4 or IPv6.					

10	Activation code valid – output	**Status**	1 bit	[1.2] DPT_Bool	CR-T--
Shows true [1] if the device was fed with a valid activation code at least once and if remote maintenance is generally possible. Otherwise the value is false [0].					

11	Secure mode active – output	**Status**	1 bit	[1.2] DPT_Bool	CR-T--
Shows true [1] if the IP interface was commissioned securely and secure (encrypted) tunnelling in the interface application was activated. Otherwise the value is false [0].					

12	Server connection – output	**Status**	1 bit	[1.2] DPT_Bool	CR-T--
If the connection to the relay server is established, this KO turns true [1] otherwise false [0].					

13	Secure tunnelling active – output	**Status**	1 byte	[5.1] DPT_Scaling	CR-T--
Status of Secure Tunnellings: false [0] = inactive, true [1] = active Inactive means that the unencrypted tunnelling connection can be established.					

ID	Name	Object function	Length	Type	Flags
14	Programming of remote maintenance active – output	**Status**	1 bit	[1.2] DPT_Bool	C--T--
If remote maintenance is established to the IP interface from the computer of the installer (ETS), this is true [1], otherwise false [0]. In general, it takes approx. 10 seconds for the connection to the device to be completely closed. Normally, a time lapse can be observed between the output of the KOs and the display in the group monitor.					

15	MapperObjekt channel A - Field length	**In-/output**	1 bit to 14 bytes	n/a	CRWT--
When writing or answering on this KO, the value will be written on the KO of channel B on the bus. Here, the encryption of the individual channels is taken into consideration. When reading is requested, the request will be answered. At the same time a reading request is issued to channel B.					

16	MapperObjekt channel B - Field length	**In-/output**	1 bit to 14 bytes	n/a	CRWT--
When writing or answering on this KO, the value will be written on the KO of channel A on the bus. Here, the encryption of the individual channels is taken into consideration. When reading is requested, the request will be answered. At the same time a reading request is issued to channel B.					

7 Advanced configuration

7.1 Configuration tool

This software simplifies the configuration of the device and provides detailed information about the device for error analysis.

If the device is in secure mode, the configuration tool can not connect to the device.

7.1.1 Device connection

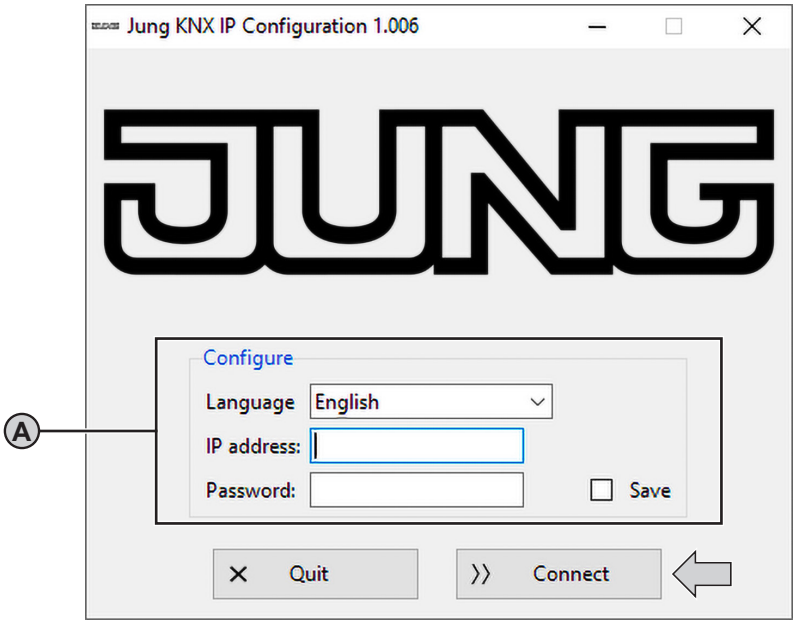


Fig. 26: Device connection

Requirements:

- device connected and booted
- configuration tool started

Configure (A)

Changing language:

- Select language.
  Configuration tool is shown in selected language.

Connecting device for device configuration:

- Enter IP address of device.
  The IP address can be located as follows:
  Static IP address: see ETS
  Dynamic IP address: see DHCP server
- Enter password.
  The default password is “knxsecure“.
  The entered password can be saved, so it must not be entered again after the next start of the configuration tool.
- Select “Connect“.
  Device is connecting.
  Device configuration is shown.

7.1.2 Device configuration

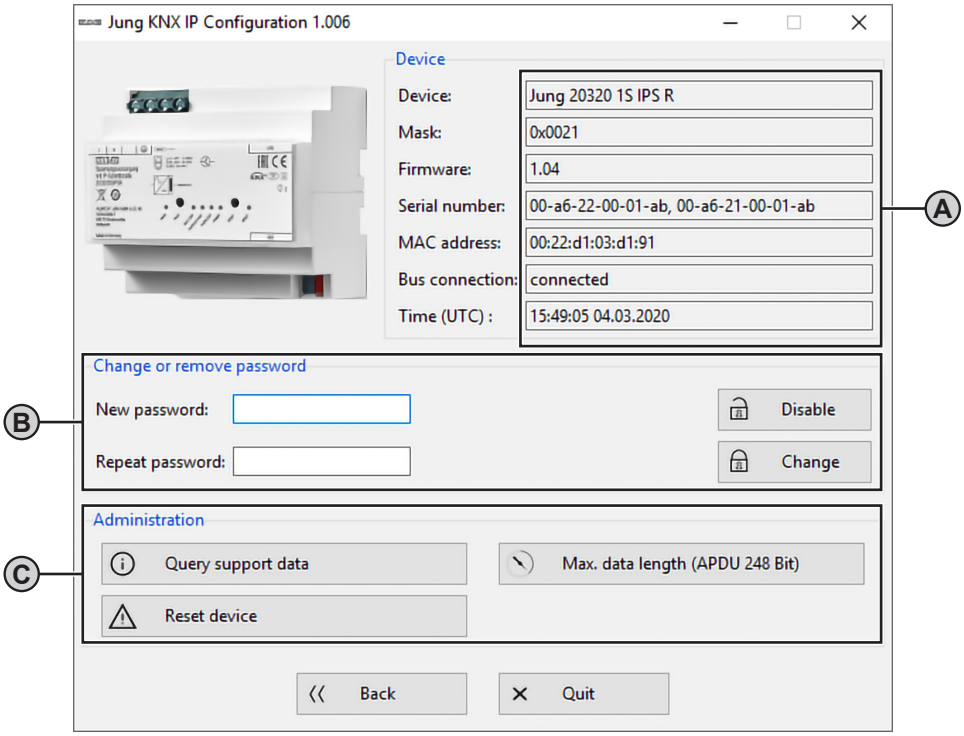


Fig. 27: Device configuration

Requirement:

- device connected

Device (A)

Shows current properties of the device.

Change or remove password (B)

Changing password:

- Enter new password and repeat input.
- Confirm new password with “Change”.
  Password is changed.

Removing password:

- Select “Disable”.
  Password is removed.

Administration (C)

Saving device information for error correction:

- Select “Query support data“.
  A text file with device information is saved in the main folder of the software.
  Example path: C:\Programs\ConfigTool\

Performing master reset for restoring of default settings:

- Select “Reset device”.
  Master reset is performed.
  Configuration tool is restarting.

Selecting min. / max. length of telegrams for error correction of third party products:

- Select “Max. data length (APDU 248 Bit)“ or “Min. data length (APDU 55 Bit)“.
  Telegram length is adjusted.

7.2 Telnet interface

Telnet is a common network protocol based on a TCP connection between a Telnet server (the device in this case) and a client (the commissioning PC in this case).

For communication to be possible, it is necessary for the device to be administered in the network and to be reached by the commissioning PC via IP. Settings can then be made on the device (particularly status information) via Telnet as well as status information viewed without there being a connection to the ETS.

Telnet can either be activated as a function of the Windows operating system or used via a third party program, e.g. PuTTY.

Telnet access is factory-protected with the password “knxsecure”.

Once the device is in secure mode, the telnet interface is disabled.

Telnet input	Description
`help`	Displays all available commands

`ifconfig`	Displays network parameters
	
	`IP mode.....: DHCP`
	`IP.....: 192.168.33.142`
	`Subnet mask...: 255.255.0.0`
	`Gateway.....: 192.168.33.1`
	`NTP server....: 192.53.103.108`
	`Hardware addr.: 00:50:c2:79:3f:ff`

`ifconfig [help|dhcp|ip |mask]`	Set network parameters via the telnet interface.
	Expamples:
	
	Setting IP Addresse with DHCP:
	`ifconfig dhcp`
	Statically set the IP address to 192.168.1.2 (in this case, the gateway and mask should also be adapted, see below)
	`ifconfig ip 192.168.1.2`
	Set the gateway to 192.168.1.1:
	`ifconfig gw 192.168.1.1`
	Set the mask to 255.255.255.0:
	`ifconfig mask 255.255.255.0`

`tpconfig`	Shows KNX parameters
	
	`KNX bus state.: up`
	`KNX address...: 15.15.000`
	`Serial number.: 00-a6-00-00-00-01`

`tpconfig [help|set]`	Set KNX parameters via the telnet interface. Set the TP address to 1.1.0: `tpconfig set 1.1.0`
`progmode [0|1]`	Query or change programming mode (0 = off, 1 = on)

`apdu [55..248]`	Read or configure the maximum length of the KNX TP telegrams. This may be necessary if there is an incorrect implementation of a TP stack. In that case the ETS may try to use telegrams with 248 bytes payload, but the TP device can not process (e.g. Zennio Z35i). Default is 248 and should only be changed if necessary.
	
	`# apdu`
	`maximal len of a KNX telegram 248.`
	`Usage: apdu [55 .. 248]`

`tpratemax [5..50]`	Read or configure maximum telegram rate (IP => TP); 50 T / s corresponds to 100 % bus load.
	
	`# tpratemax`
	`no limit, sending with maximum performance to TP.`
	`Usage: tpratemax [5 .. 50]`

Telnet input	Description
stats	Shows various statistics on device and bus status **uptime: 114 days, 2:19** **KNX communication statistics:** **TX to IP (all)..: 333729 (ca. 233 t/m)** **TX to KNX.....: 23244 (ca. 16 t/m)** **RX from KNX.....: 94559 (ca. 66 t/m)** **Overflow to IP..: 0** **Overflow to KNX.: 0** **TX tunnel re-req: 260** **TP bus voltage..: 28.95 V** **TX TP rate.....: 50 T/s (= 100 %)** Uptime: Runtime of the interface since last restart TX to IP (all): Number of all telegrams sent on IP TX to KNX: Number of all telegrams sent on KNX RX from KNX: number of telegrams received from the KNX bus Overflow to IP: Number of telegrams that could not be sent to IP Overflow to KNX: Number of telegrams that could not be sent to the KNX bus TX tunnel re-req: Number of telegrams that had to be repeated in the tunnel connections TP bus voltage: Current bus voltage (at the time of calling stats) TX TP rate: maximum telegram rate (TP)
free [clear]	Shows statistics about the memory usage **Used stack memory...: 14 %** **Allocated memory....: 64 %** **Unused memory.....: 35 %** **TP-Tx buffer.....: 0 %** **TP-Tx buffer max....: 0 %** **TP-Rx buffer max....: 0 %** **Tunnel-T8 buffer max: 92 %** Used stack memory: Function stack utilization Allocated memory: Allocated device memory Unused memory: Unused device memory TP-Tx buffer: Currently used TP send buffer TP-Tx buffer max:Max. Utilization of TP send buffer (IP => TP) since system startup TP-Rx buffer max:Max. Utilization TP receive buffer (IP <= TP) since system startup Tunnel-XX (XX = 1..8) buffer max:Max. Utilization of the tunneling buffer. Only tunnels whose buffer was used at all will be displayed Clear the buffer statistics: **free clear**

Telnet input	Description
tunnel [1..8]	Shows active tunnel connections (without argument) or detailed information about the specified tunnel connection (with argument 1..8) **# tunnel** **Tunnels open: 1/8** **1: 00.02.246, closed** **2: 00.02.247, open (CCID: 82)** **3: 00.02.248, closed** **4: 00.02.249, closed** **5: 00.02.250, closed** **6: 00.02.251, closed** **7: 00.02.252, closed** **8: 00.02.253, closed** **# tunnel 2** **Tunnel 2.....: open (CCID 82)** **KNX address.....: 00.02.247** **HPAI control.....: 192.168.22.252:4808** **HPAI data.....: 192.168.22.252:4808** **Connect. type.....: TUNNEL_CONNECTION** **Communication.....: UDP CONNECTION** **TX tun req.....: 23169** **TX tun re-req.....: 0** **RX tun req.....: 821** **RX tun re-req (identified): 0** **RX tun req (wrong seq.)...: 0** **Current tunnel buffer.....: 0 %** **Connected since (UTC).....: 16:26:16 29-01-2019** CCID: Connection ID of the tunnel connection KNX address: Tunneling address HPAI control: Control endpoint of the connection partner HPAI data: Data endpoint of the connection partner Connect. Type:Connection type tunnel or management connection Communication: UDP or TCP Connection TX tun req: Number of telegrams sent to the tunnel connection TX tun re-req: Number of telegrams that had to be repeated in the tunnel connections RX tun req: Number of telegrams received from the tunnel connections RX tun re-req: Number of telegrams received twice by the tunnel connections RX tun req (wrong seq.):number of frames received from the tunnel connections with wrong sequence number Current tunnel buffer: Utilization currently of the IP buffer of the tunnel Connected since (UTC): Time since the tunnel connection has been established.
version	Firmware version
mask	Mask version
tunaddr 1..8 address **tunaddr reset** **tunaddr setall** **tunaddr help**	KNX address of a tunnel read (**tunaddr**) or change, e.g. **tunaddr 1 15.15.240,** set all tunnel addresses consecutively from a certain start address (**tunaddr setall 15.15.15**), or reset the KNX addresses of all tunnels to factory settings (tunaddr reset) **# tunaddr** **1: KNX address: 15.15.010** **2: KNX address: 15.15.011** **3: KNX address: 15.15.012** **4: KNX address: 15.15.013** **5: KNX address: 15.15.014** **6: KNX address: 15.15.015** **7: KNX address: 15.15.016** **8: KNX address: 15.15.017**
tunmode [std/tpblk]	Read tunnel mode (without parameters) or set (**tp** or **tpblk**); **tunmode tpblock**: IP => KNX If same backbone forward to line frame KNX => IP If same sub line send to backbone

Telnet input	Description
`Tunneltime [1.0..8.0]`	Query or change timeout for tunnel connection (1.0 to 8.0). Setting is identical to "slow connection", figure 14
`tunudp`	Query or change the type of tunnel connection for the ETS (0 = default, 1 = UDP only).
`date`	Show date and time
`busload`	Shows the busload of the last minute / last 5 minutes / last 15 minutes / since start and also the maximum load with date and time
`sntp [query|server IP]`	Send request to the NTP server (sntp query) or set the IP of the NTP server (`sntp server 1.2.3.4`)
`logmem`	Event memory in the device. Suitable for the development of clients. Read out for support requests.

`passwd oldpw newpw`
`passwd oldpw`
`passwd newpw`
	Changes the current Telnet password (passwd), deletes the current password (old passwd) or sets a new password if none is currently set (new passwd)

`factory_reset`	Reset to factory settings and reboot
`reboot`	Reboot
`logout`	End Telnet session

8 Use cases

8.1 Application program A – Logic functions

For every device the integrated logic can be configured for the presence monitoring. The presence monitoring can be selected with a key card switch or up to five presence detectors.

8.1.1 Presence monitoring with key card switch

Via key card switch and door contact a predefined logic for presence monitoring can be parameterized. The following figure shows the modes of operation and the possibilities for individualization. Some examples for parameterizations are shown as well.

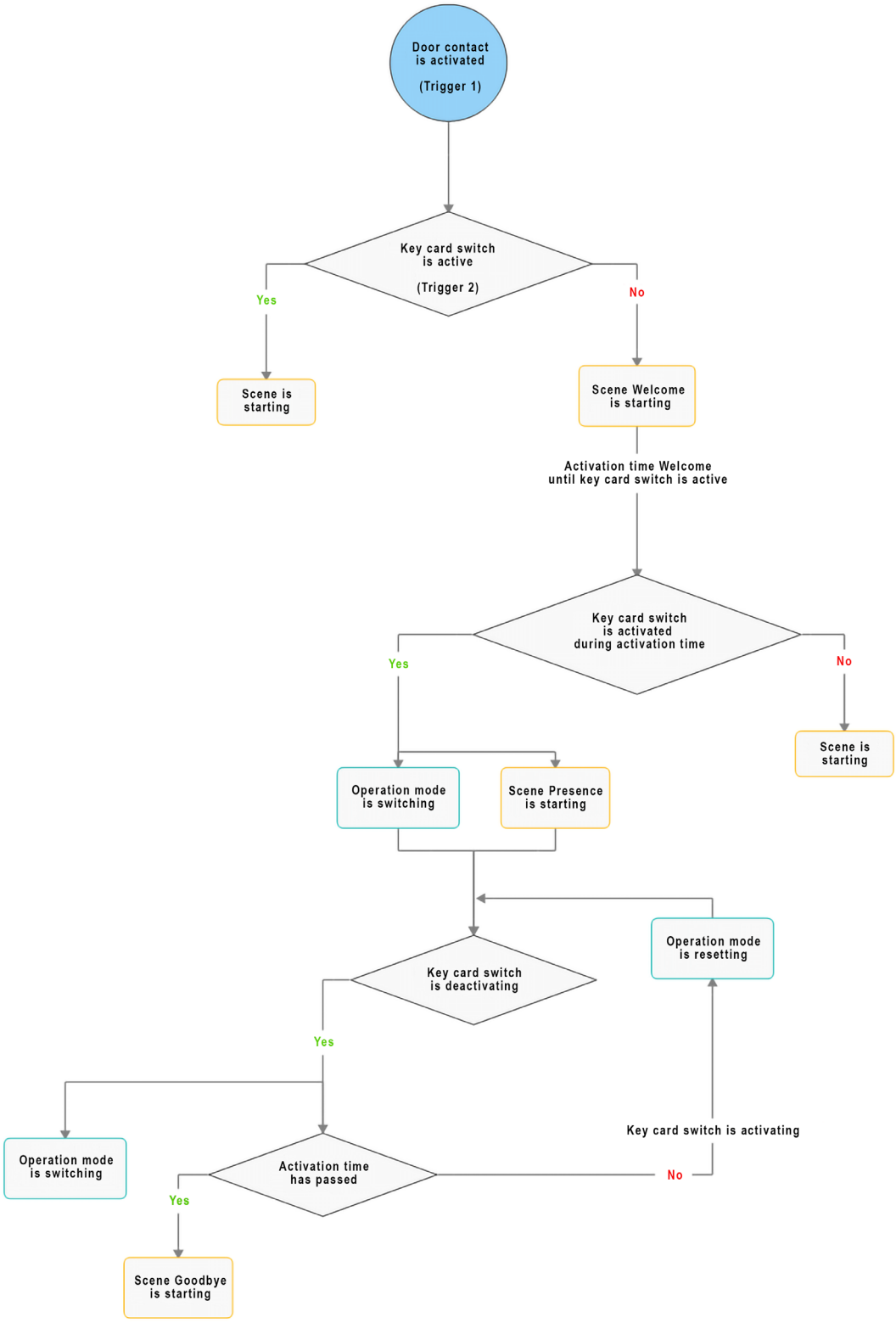


Fig. 28: Presence monitoring with key card switch

Presence monitoring with key card switch – Easy

The parameterization shows a simple use case for presence monitoring.

- One person is entering the room (door contact is activated)
  - A Welcome scene is triggered
    The lighting can be switched on dimmed for example
- One person inserts the key card during activation time in the key card switch
  - An operation mode is sent
    The operation mode “Comfort” can be activated for example
- One person doesn’t insert the key card during activation time
  - A scene is triggered
    The lighting can be switched off for example
- One person removes the key card and leaves the room
  - An operation mode is sent
    The operation mode “Standby” can be activated for example
  - After the activation time a Goodbye scene is triggered
    The lighting can be switched off for example

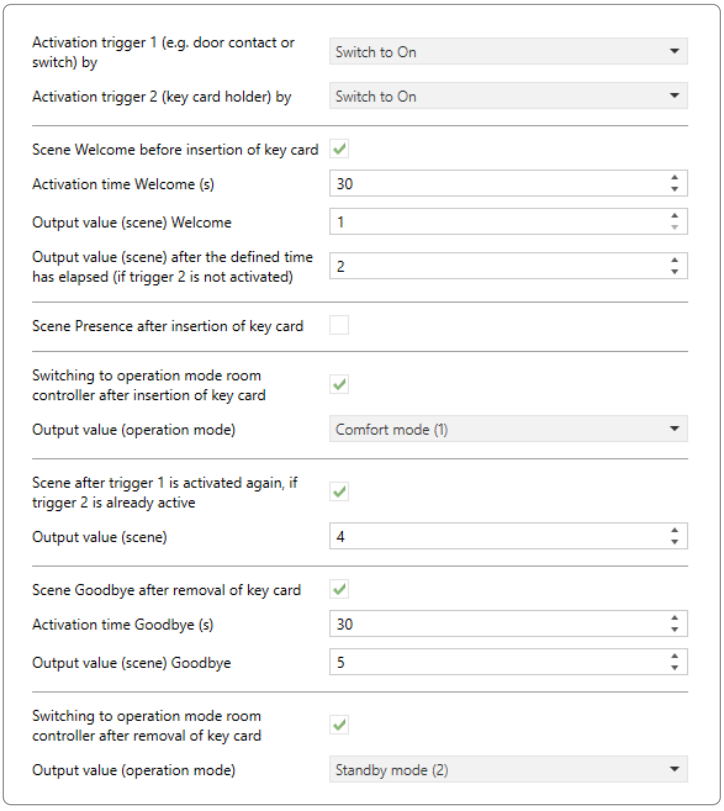


Fig. 29: Presence monitoring with key card switch – Easy

Presence monitoring with key card switch – Standard

The parameterization shows a standard use case for presence monitoring.

- One person is entering the room (door contact is activated)
  - A Welcome scene is triggered
    The lighting can be switched on dimmed for example
- One person inserts the key card during activation time in the key card switch
  - An operation mode and a presence scene are sent
    The operation mode “Comfort” can be activated, the blinds can be moved to the upper end position and an additional lighting can switched on dimmed for example
- One person doesn’t insert the key card during activation time
  - A scene is triggered
    The lighting can be switched off for example
- One person removes the key card and leaves the room
  - An operation mode is sent
    The operation mode “Standby” can be activated for example
  - After the activation time a Goodbye scene is triggered
    The lighting can be switched off for example

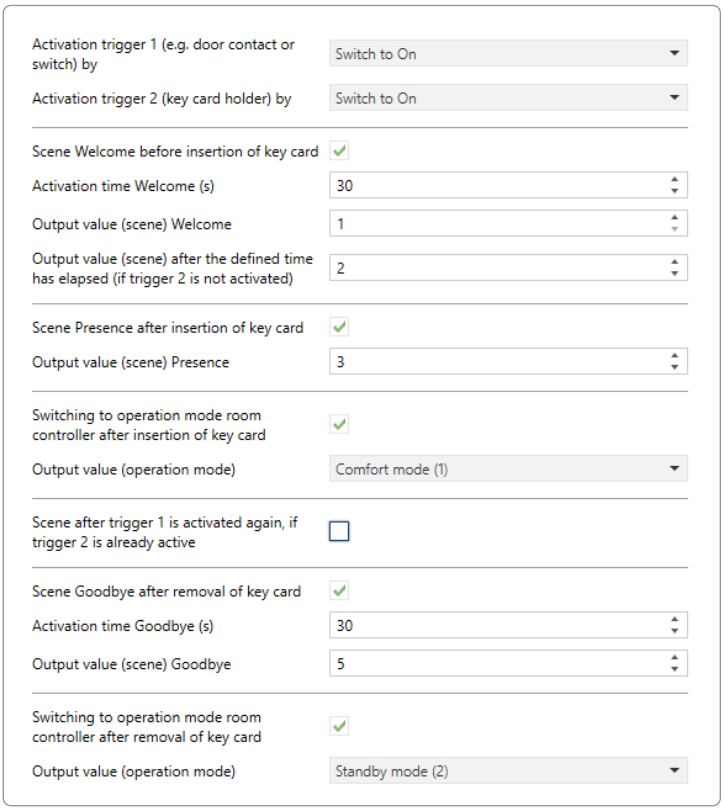


Fig. 30: Presence monitoring with key card switch – Standard

Presence monitoring with key card switch – Luxury

The parameterization shows a extensive use case for presence monitoring.

- One person is entering the room (door contact is activated) for the first time (first entry)
  - A Welcome scene is triggered
    The lighting can be switched on dimmed for example
- One person inserts the key card during activation time in the key card switch
  - An operation mode and a presence scene are sent
    The operation mode “Comfort” can be activated, the blinds can be moved to the upper end position and an additional lighting can switched on dimmed for example
- One person doesn’t insert the key card during activation time
  - A scene is triggered
    The lighting can be switched off for example
- Another person is entering the room (door contact is activated)
  - A nightlight scene is triggered
    The entrance lighting can be dimmed to minimum brightness for example
- One person removes the key card and leaves the room
  - An operation mode is sent
    The operation mode “Standby” can be activated for example
  - After the activation time a Goodbye scene is triggered
    The lighting can be switched off for example

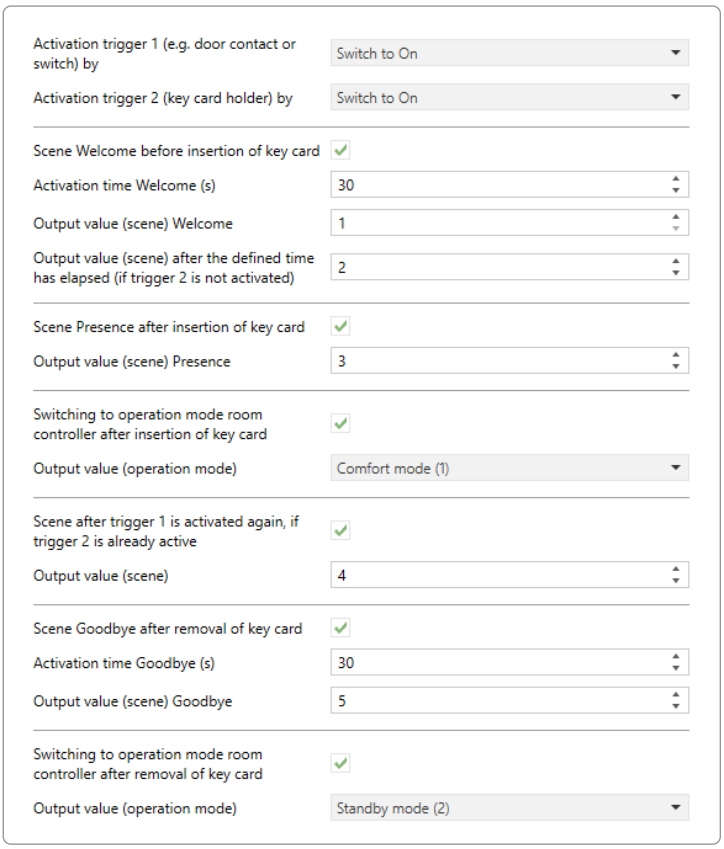


Fig. 31: Presence monitoring with key card switch – Luxury

8.1.2 Presence monitoring with presence detector

With up to 5 presence detectors and door contact a predefined logic for presence monitoring can be parameterized. The following figure shows the modes of operation and the possibilities for individualization. Some examples for parameterizations are shown as well.

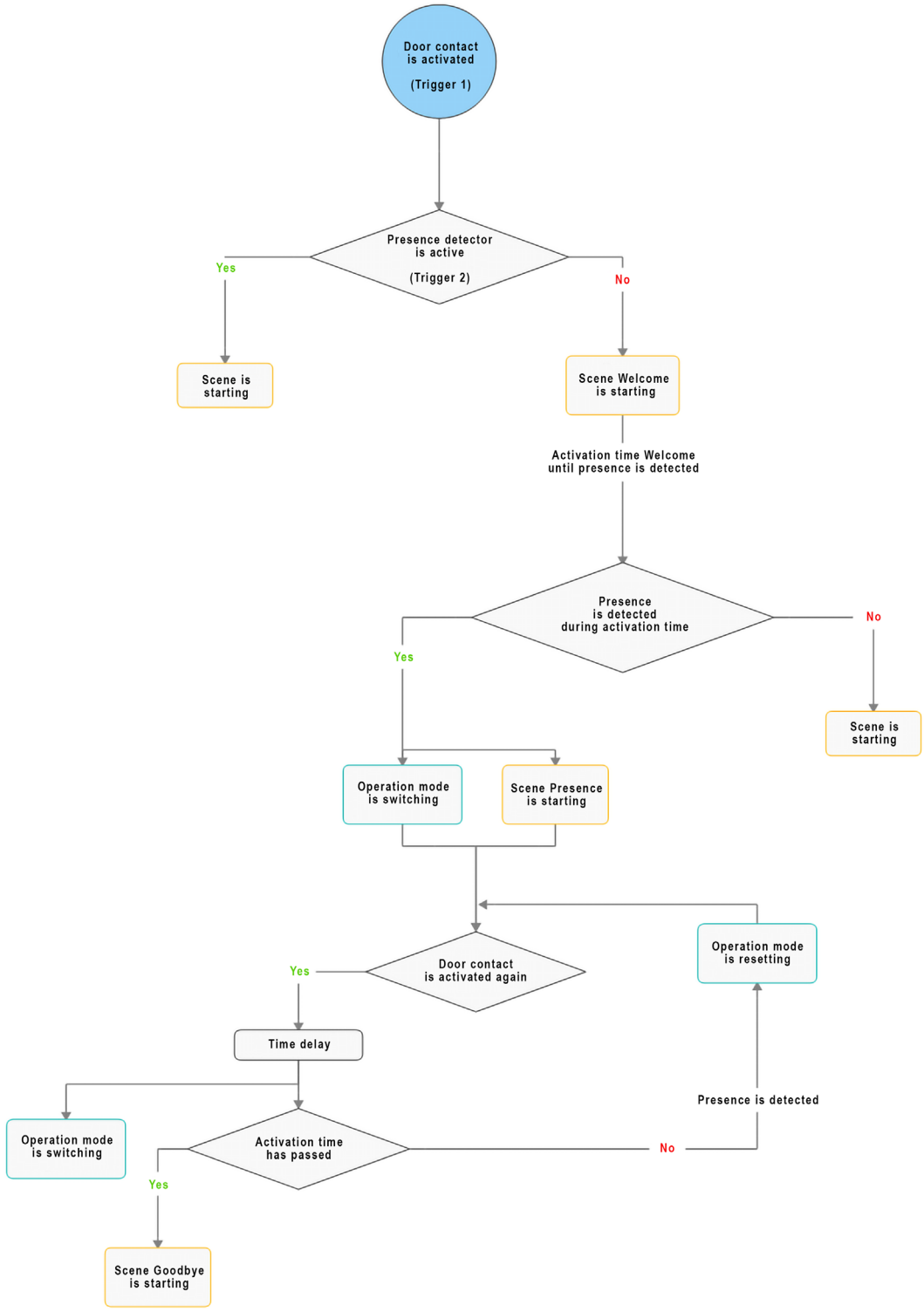


Fig. 32: Presence monitoring with presence detector

Presence monitoring with presence detector – Easy

The parameterization shows a simple use case for presence monitoring.

- One person is entering the room (door contact is activated)
  - A Welcome scene is triggered
    The lighting can be switched on dimmed for example
- A presence detector detects a presence during activation time
  - An operation mode is sent
    The operation mode “Comfort” can be activated for example
- A presence detector doesn’t detect a presence during activation time
  - A scene is triggered
    The lighting can be switched off for example
- One person leaves the room and no presence is detected after time delay
  - An operation mode is sent
    The operation mode “Standby” can be activated for example
  - After the activation time a Goodbye scene is triggered
    The lighting can be switched off for example

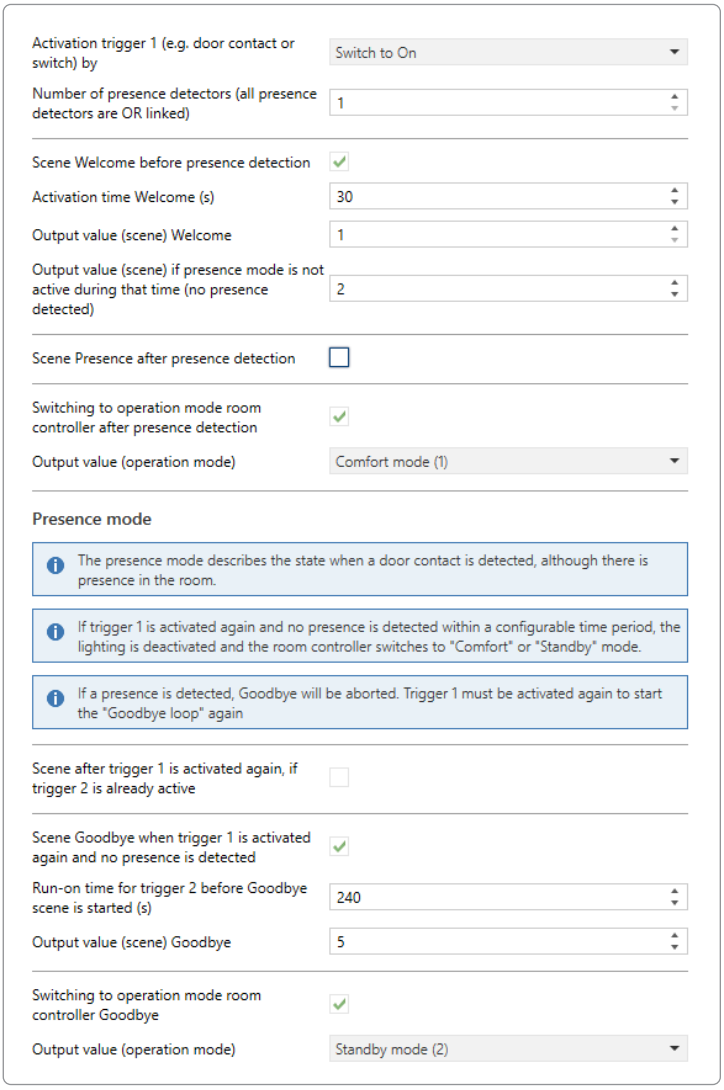


Fig. 33: Presence monitoring with presence detector – Easy

Presence monitoring with presence detector – Standard

The parameterization shows a standard use case for presence monitoring.

- One person is entering the room (door contact is activated)
  - A Welcome scene is triggered
    The lighting can be switched on dimmed for example
- A presence detector detects a presence during activation time
  - An operation mode and a presence scene are sent
    The operation mode “Comfort” can be activated, the blinds can be moved to the upper end position and an additional lighting can switched on dimmed for example
- A presence detector doesn’t detect a presence during activation time
  - A scene is triggered
    The lighting can be switched off for example
- One person leaves the room and no presence is detected after time delay
  - An operation mode is sent
    The operation mode “Standby” can be activated for example
  - After the activation time a Goodbye scene is triggered
    The lighting can be switched off for example

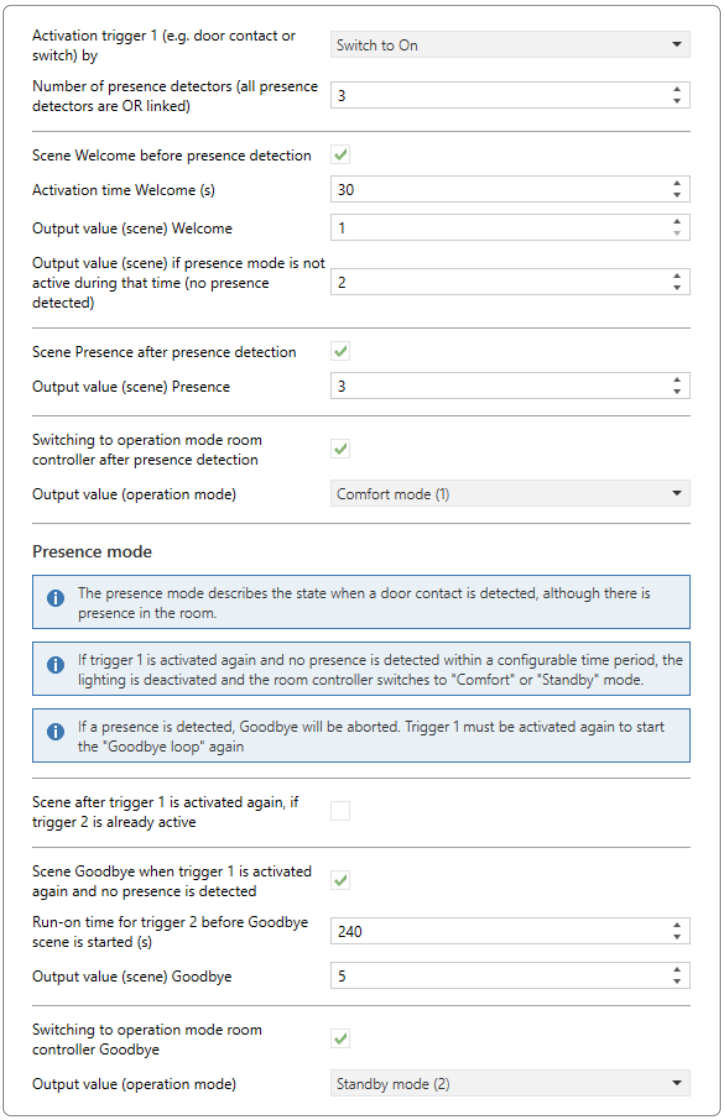


Fig. 34: Presence monitoring with presence detector – Standard

Presence monitoring with presence detector – Luxury

The parameterization shows a extensive use case for presence monitoring.

- One person is entering the room (door contact is activated) for the first time (first entry)
  - A Welcome scene is triggered
    The lighting can be switched on dimmed for example
- A presence detector detects a presence during activation time
  - An operation mode and a presence scene are sent
    The operation mode “Comfort” can be activated, the blinds can be moved to the upper end position and an additional lighting can switched on dimmed for example
- A presence detector doesn’t detect a presence during activation time
  - A scene is triggered
    The lighting can be switched off for example
- Another person is entering the room (door contact is activated)
  - A nightlight scene is triggered
    The entrance lighting can be dimmed to minimum brightness for example
- One person leaves the room and no presence is detected after time delay
  - An operation mode is sent
    The operation mode “Standby” can be activated for example
  - After the activation time a Goodbye scene is triggered
    The lighting can be switched off for example

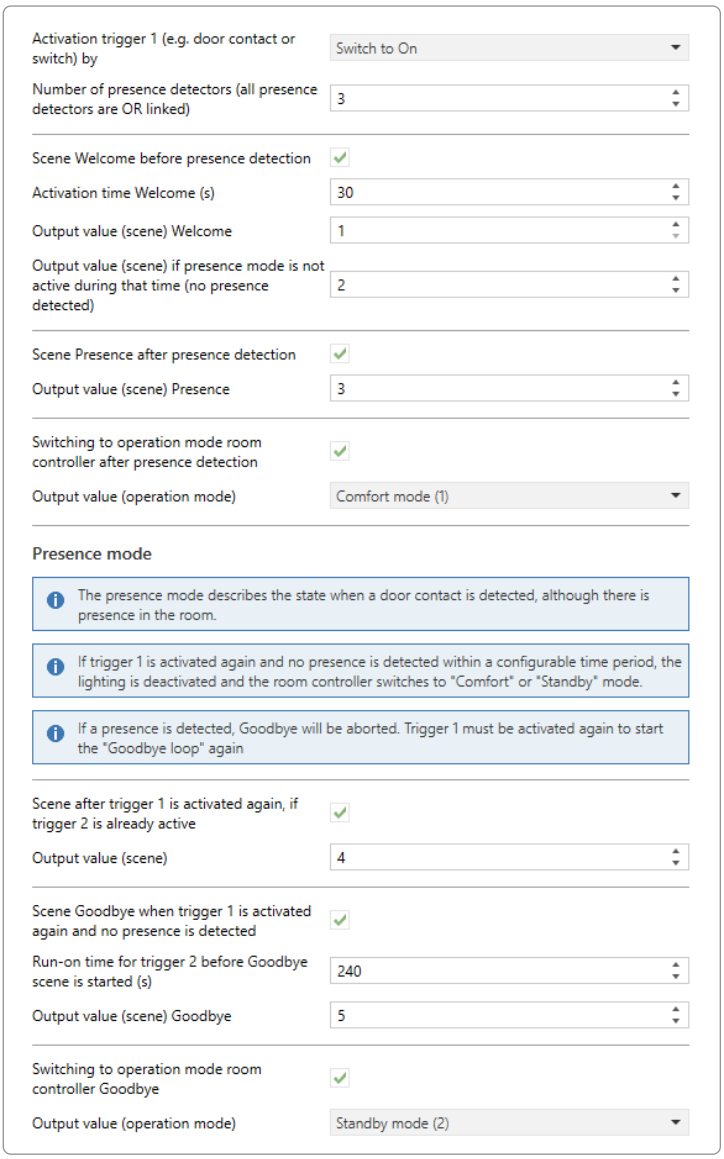


Fig. 35: Presence monitoring with presence detector – Luxury

8.2 Application program B – IP interface

8.2.1 Mapper

The practical use of the mapper is outlined in the following scenario:

A system comprises an inner and outer line. To increase the security of the system, it was decided to convert the outer line to Secure. Opening or closing a garage door, for example, is done via KNX and secure communication. In this example the group addresses 17/2/1, 17/2/2 und 17/2/3 are used. These are inserted into the inner line via two routers. The devices are these functions in the group communication 1/2/1, 1/2/2 und 1/2/3. The inner line, however, only has unencrypted actuators and sensors. The mapper maps the group addresses 17/2/1 to 1/2/1, 17/2/2 to 1/2/2 and 17/2/3 to 1/2/3. For this reason, only the devices on the inner line can only communicate with the outer line. Routing the main group 17 but main group 2 is blocked can be set via the routing. In this way, the security of the outer line can be combined with the inner line easily.

8.2.2 Remote maintenance

An encrypted or normal access via the tunnelling connection can be ensured setting the parameters “Secure Tunnelling after device restart” or “Secure Tunnelling after remote maintenance”. The visualisation has be activated consciously and has to support all attributes of the encrypted tunnelling connection.

For the usual access (e.g. Smart Visu Server) both parameters have to be set to “off”.

For encrypted access (e.g. JUNG Visu Pro), both parameters have to be set to “on”.

9 Firmware update

The device consists of a combination of the following devices:

- Power supply with IP interface
- Power supply with IP interface - Additional functions

There is only one combined update file for both devices with the ending “b03”.

The firmware update for both devices has to be imported via the physical address of the device “Power supply with IP interface”.

9.1 Displaying firmware version

The current version of the firmware can only be displayed via the device “Power supply with IP interface - Additional functions”.

- Perform right click on the device in the ETS.
- Select “Info > Device Info”.
  Firmware version is displayed behind the square brackets.
  Example: ... [...] 1.3

9.2 Preparing firmware update

Requirements:

- The firmware update can only be performed by the owner of the ETS licence and the ETS project.
- The device should not be protected by a password.

9.2.1 Deactivating secure commissioning

The device “Power supply with IP interface” has to be in unsecure commissioning mode before performing the update.

- Deactivate “Secure Commissioning” in device properties, see figure 5.

9.2.2 Downloading application program

The application program for the device “Power supply with IP interface” has to be downloaded before performing the update.

- Perform right click on the device in the ETS.
- Select “Download > Download Application”.
  Application program is downloading automatically.

9.3 Performing firmware update

The update has to be performed with the JUNG firmware update tool.

The JUNG firmware update tool can be downloaded from our website.

Detailed information about the JUNG firmware update tool can be found in the corresponding manual.

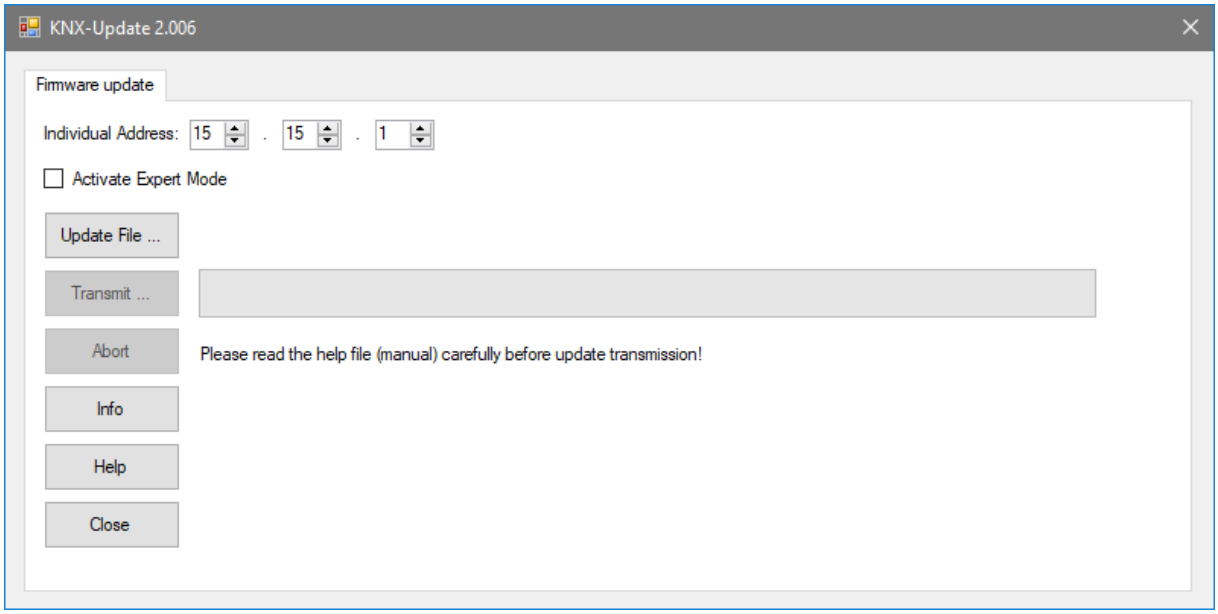


Fig. 36: Firmware update tool

- Start JUNG firmware update.
- Enter physical address of device “Power supply with IP interface”.
- Select update file with button “Update File”.
- Start update with button “Transmit”.
  Update for both devices is performing automatically.
  The update restores the default settings of both devices.
- After the update assign physical address for both devices in device properties, see figure 5 and figure 7.
- Download application program for both devices via “Download > Download Application”.
- Activate “Secure Commissioning” in device properties of the device “Power supply with IP interface”.

10 FAQ

Problem:
Power supply with IP interface - Additional functions:
Application download is canceled after timeout

Possible reason:
Physical address can’t be assigned at downloading.

Explanation:
The device has been inserted in the ETS project via copy and paste.
No addresses were assigned automatically.
All 8 tunnel addresses are in parking mode and invalid.

Solution:
Insert the device via drag and drop from the catalogue to the project.
The 8 tunnel addresses are assigned automatically by the ETS.

Problem:
Power supply with IP interface:
Application download is canceled after timeout

Possible reason:
Used system components (e.g. area / line coupler) are incompatible to KNX Data Secure.

Explanation:
KNX Data Secure uses a longer telegram format (extended frames). Only devices with KNX Data Secure can communicate safely in a line or in a line segment and can be secure commissioned in the ETS.

Solution:
Old or incompatible system components has to be replaced by newer system components.

11 Terms

Term	Description
Backbone	For IP routers and IP interfaces, this is always the IP network.
Encryption, encrypted	If devices send data information via the TP bus or IP network, they are generally readable by third parties. These only require access to the TP bus or IP network for reading. Encryption of the data in this context means that the contents of the telegrams are no longer to be interpreted if the encryption parameters (for example passwords) are unknown.
Key, Key Parameter	A series of numbers known only to the ETS project. These numbers are used to transform the data in both directions: encryption and decryption.
FDSK (Factory Default Setup Key)	The initial factory key. This key is used when commissioning the initial programming. A new key is loaded into the device, whereby this process is encrypted with the FDSK. The FDSK key is then no longer valid. It is reactivated only when resetting to factory settings.
Tunneling	A KNX point-to-point connection on the TCP / IP network, which is established with UDP or TCP protocol. Tunneling communication is reliable and has incorporated a link layer for that purpose. Therefore independent of the Ethernet connection, e.g. Cable or WLAN, and regardless of the TCP / IP protocol (UDP or TCP), no data is lost. With UDP, however, the restriction is that the data link layer works with a one-second timeout. This timeout can be adjusted in the advanced setup.
Telnet	A simple TCP server on port 23 that enables direct text-based communication with the IP device. Telnet is a de facto standard used at the window level, e.g. with “PuTTY” is addressed.
Abgesicherter Modus, Secure Mode	If the device is parameterized via the ETS so that the communication is only encrypted, this is referred to as secure mode.
Nicht abgesicherter Modus, Plain Mode	If the device is parameterized via the ETS so that the communication is only unencrypted, this is called unsecured mode.

12 Technical data

Symbols	 Must not be disposed of with household waste.
Rated voltage	AC 110 ... 240 V (± 10 %)
Mains frequency	50/60 Hz
Power loss (max. load of all outputs)	max. 1.4 W
Efficiency	approx. 88 %
Rated voltage	DC 230 V (± 10 %)
Rated output	12 W
KNX **KNX medium** **Bus output voltage** **Output current** **Short-circuit current** **Parallel operation with identical power supply** **KNX connection**	 TP 256 DC 28 ... 31 V SELV 320 mA max. 1 A no Connection terminal
IP communication	Ethernet 10/100 BaseT (10/100 Mbit/s)
IP connection	1 x RJ45
Ambient temperature	−5 ... +45 °C
Storage/transport temperature	−25 ... +75 °C
Relative humidity	max. 93 % (no moisture condensation)
Installation width	108 mm (6 rail units)
Connection mode:	Screw terminals
single wire	1 ... 4 mm²
stranded without ferrule	1 ... 4 mm²
stranded with ferrule	1 ... 2.5 mm²

13 Warranty

The warranty follows about the specialty store in between the legal framework as provided for by law.

14 Open Source Software

This product uses third-party software from the following authors:

Adam Dunkels adam@sics.se
Marc Boucher <marc@mbsi.ca> and David Haas dhaas@alum.rpi.edu
Guy Lancaster <lancasterg@acm.org>, Global Election Systems Inc.
Martin Husemann <martin@NetBSD.org>
Van Jacobson (van@helios.ee.lbl.gov)
Paul Mackerras, paulus@cs.anu.edu.au,
Christiaan Simons christiaan.simons@axon.tv
Jani Monoses jani@iv.ro
Leon Woestenberg <leon.woestenberg@gmx.net>

14.1 LWIP

Source: https://savannah.nongnu.org/projects/lwip/

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. The name of the author may not be used to endorse or promote products
derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ‘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 AUTHOR 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.}