blumotix
TOUCH YOUR WORLD

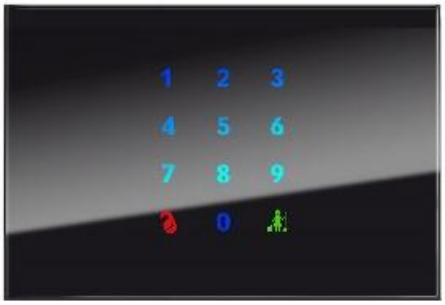
BX-E-R12SRFxx

BX-E-R12Sxx

BX-E-RSRFxx

Doory KNX Secure

Numeric keypad and RFID for access control



User manual

Rev.	Date	Description	Editor
01	15/01/2026	1ª Issue.	F. Melandri
02	24/04/2026	GO 50 data format sample	F. Melandri
03	11/05/2026	Inserted product BX-E-RSRFCHxx	E. Lumini
04	04/06/2026	Merge of BX-E-RSRFCHxx and BX-E-RSRFxx products	E. Lumini

Table of contents

Glossary

- CO: communication object
- Datapoint, DPT, dpt: type of data, data format; see KNX standard documentation
- LED: light emitting diode

1 Introduction

BX-E-R12SRFxx, BX-E-R12Sxx and BX-E-RSRFxx are KNX Secure devices designed by Blumotix and dedicated to access control applications.

Devices belonging to this product range share the same design concept and provide common aesthetic and functional characteristics. Differences between models may concern both the available functionalities and the elements present on the front surface, such as the pattern printed on the glass cover or the presence of specific components, depending on the model.
Throughout this manual, the term “device” is used in a general sense; however, it should be noted that some of the functions described are not available on all models listed below. The main features of the three models are summarised as follows.

BX-E-R12SRFxx – This is the most complete model, as it is equipped with both a capacitive numeric keypad and RFID card/tag management for access control. This model requires an auxiliary power supply for correct operation. In this manual, it is used as the reference model to describe all available behaviours and functions.

BX-E-R12Sxx - This model is equipped with a capacitive numeric keypad and supports access control via numeric codes.

BX-E-RSRFxx- Device for the management of RFID transponders used for access control applications. Through ETS configuration, it can operate either as an RFID Reader or as an RFID Card Holder for card presence detection. An auxiliary power supply is required for proper operation.

The device body is designed for installation in standard rectangular flush-mounted boxes (type 503), as well as in round (Ø 60 mm) or square (type 502) boxes.
Since the front panel of the keypad is rectangular, two versions are available: horizontal orientation and vertical orientation. The desired orientation must be selected at the time of ordering. The pocket device is available only in the horizontal orientation version.

The keypad features a glass front panel with 13 capacitive keys. The thirteenth key (optional) can be assigned to an additional command or to doorbell activation. The device is equipped with a proximity sensor, two independent base illumination zones (top–bottom and left–right), and independent backlighting for the 12 numeric and symbolic keys.
The glass front panel can be customised in terms of colour, text and graphics, including customer-specific designs.
From a functional and configuration point of view, the keypad implements a complete access control logic, including local storage of numeric access codes and all related information directly within the device.
Standard hotel functions are supported, together with a dedicated room energy management logic.
These features make the device particularly suitable for hospitality, tourism and hotel facilities.
Base illumination, proximity sensor, numeric keys, dedicated function keys and their associated LEDs can be configured and managed in various operating modes, depending on the required application.

2 General Information

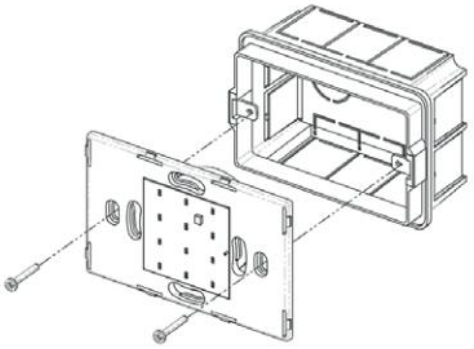
2.1 Wall mounting

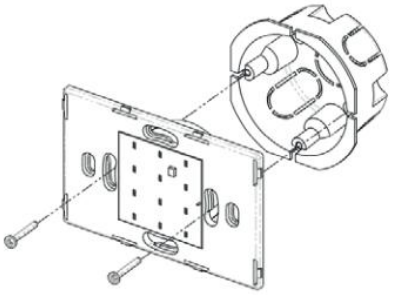
As mentioned above, the device can be installed in standard rectangular flush-mounted boxes, as well as in round or square boxes.
If the vertical version is selected and installed in a type 503 flush-mounted box, the box must be embedded in the wall in a vertical orientation.
Installation of the device is carried out by removing the glass front panel and fixing the device body to the slots of the flush-mounted box using suitable screws (self-tapping screws, pan head, 3.5 × 25 mm, DIN7981 UNI6954).

For models equipped with RFID card and tag reading, an auxiliary power supply must also be provided (refer to the technical datasheet), in addition to the KNX bus connection.

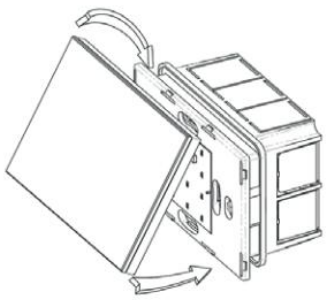
2.2 First activation

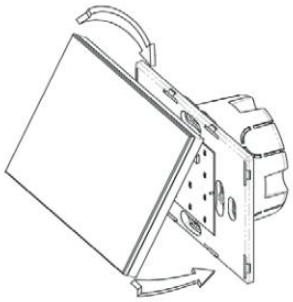
Once the keypad body has been fixed to the flush-mounted box and the device has been powered, the KNX individual address can be programmed using ETS software. The KNX programming button is located on the front of the device. Activation of KNX programming mode is indicated by a red LED visible on the rear cover of the device and the simultaneous illumination of the four corner led keys on the front panel.





Once the programming of the KNX individual address is ready, it is possible to mount the glass front of the keypad. Any changes to the device configuration parameters will also be possible without removing the cover.

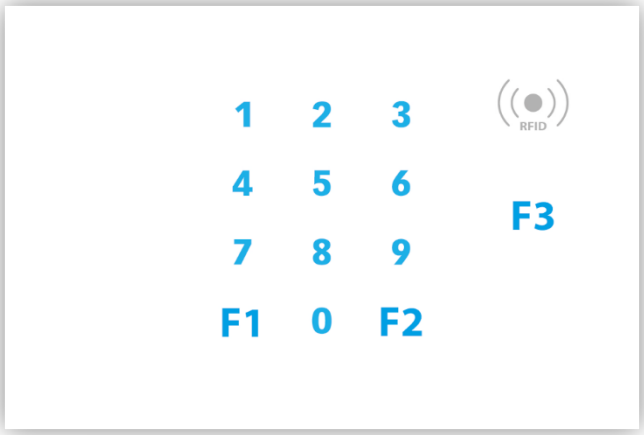


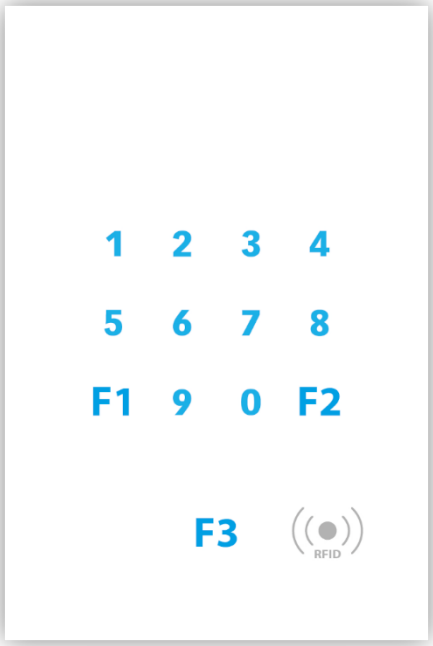


2.3 Keys layout

For BX-E-R12SRFxx and BX-E-R12Sxx devices, the figures below show the button layout in both the horizontal and vertical versions. The devices feature numeric buttons (0–9) dedicated to user code entry, function buttons identified as F1 and F2,

and, optionally, a thirteenth button identified as F3.

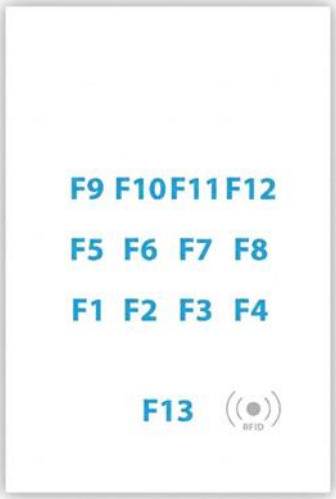




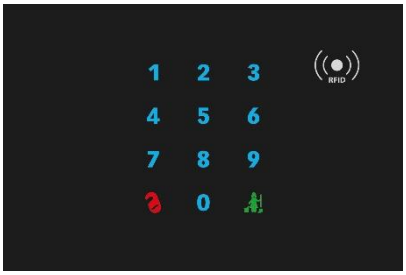
For the BX-E-RSRFxx device, the available functionalities depend on the operating mode configured through ETS:

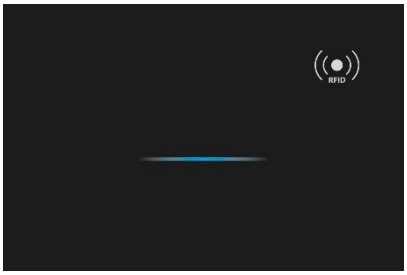
- In RFID Reader mode, all twelve front buttons and the optional thirteenth button can be independently configured as function buttons.
- In RFID Card Holder mode, the presence of the card holder limits the number of available function buttons. Only buttons F1, F4, F7, and F10 (in the horizontal version) are available and can be configured as function buttons through ETS.

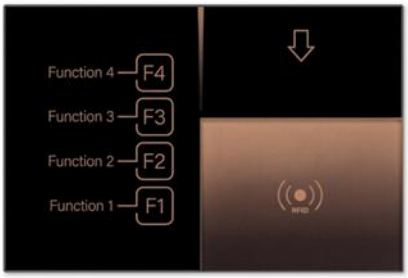
The figures below show the button layout in the horizontal and vertical versions of the BX-E-RSRFxx device when configured in RFID Reader mode.

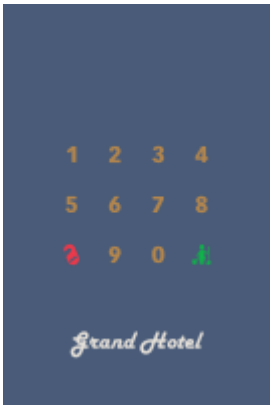


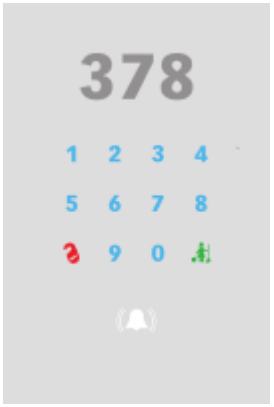
Some examples of customised horizontal and vertical layouts are shown, including numeric keys, function keys, logos and additional graphic elements.











3 Configuration

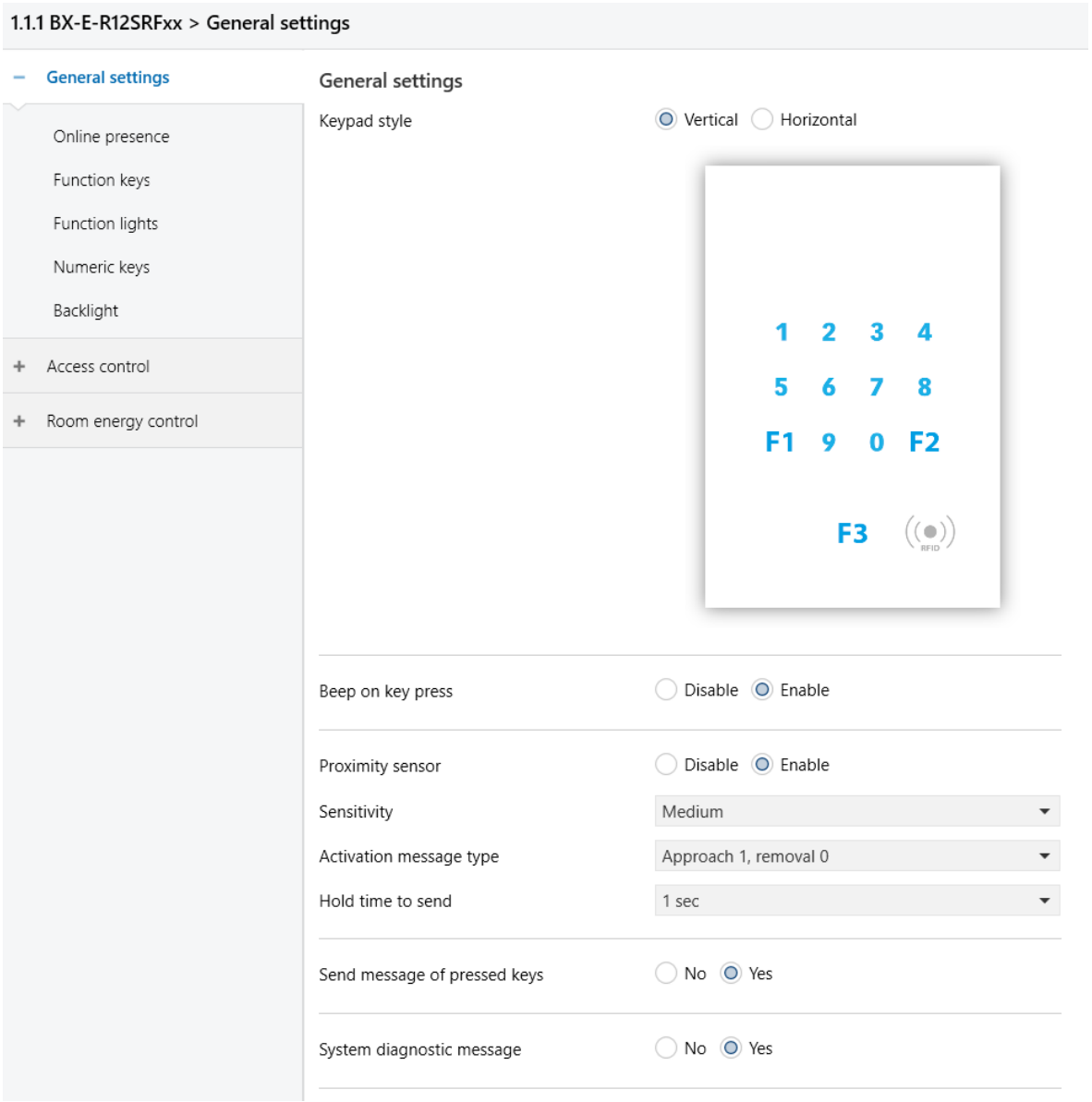
The ETS database supplied with the BX-E-R12SRFxx keypad allows full configuration of all available functions through parameter settings and the associated communication objects.

3.1 General settings

The first configuration section available in ETS is named “General settings”.

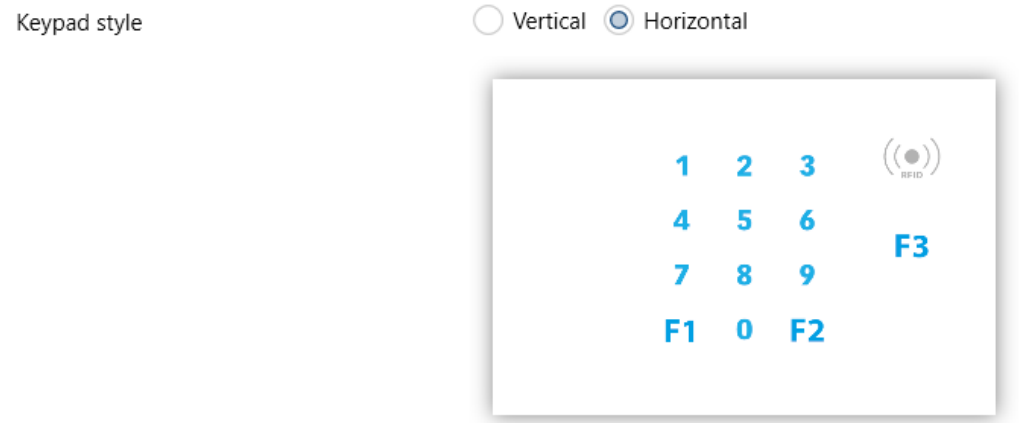
3.1.1 BX-E-R12SRFxx and BX-E-R12Sxx

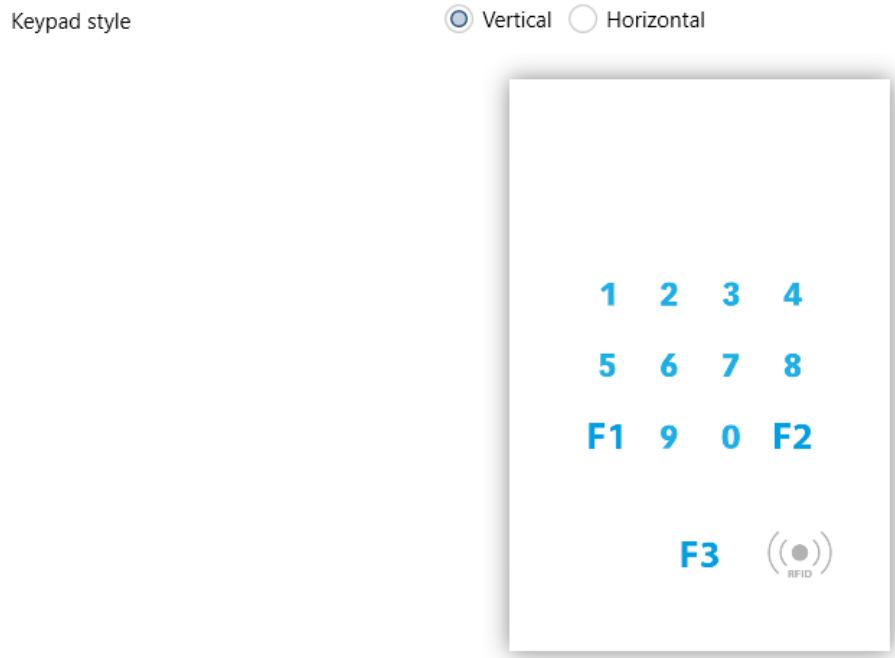
The following section describes the parameters and functions available for BX-E-R12SRFxx and BX-E-R12Sxx devices.



3.1.1.1 Keypad style

This parameter allows to choose the orientation of the device. It must reflect the device that has to be installed. The possible choices are horizontal or vertical.





3.1.1.2 Beep on key press

This parameter enables or disables the audible feedback generated when a key on the keypad is pressed.

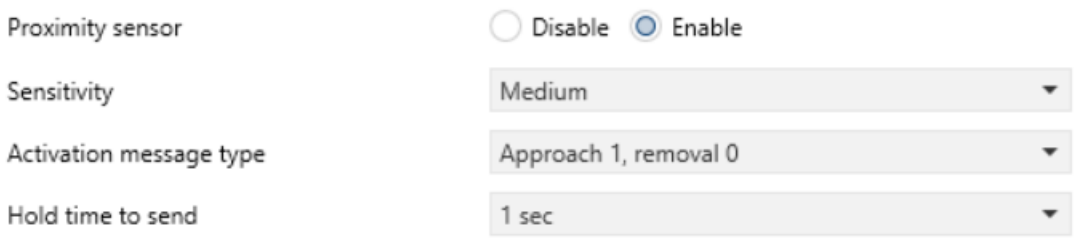
The mode defined by this parameter can be changed by writing the corresponding CO 2; the new value will be returned by the status CO 3.

- CO value = 1: sound enabled
- CO value = 0: sound disabled

2	Keypad	Enable/disable beep on touch	1 bit	C	-	W	-	-	1-bit, switch
3	Keypad	Enable beep on touch status	1 bit	C	R	-	T	-	1-bit, switch

3.1.1.3 Proximity sensor

The keypad is equipped with a proximity sensor that detects the approach of a hand to the front panel. Detection of proximity can be used to activate several functions, such as automatic switching on of key illumination or base backlighting. In addition, a dedicated KNX message can be transmitted when the sensor is activated. The parameters related to the proximity sensor are described below.



Besides enabling or disabling the sensor, it is possible to set the detection sensitivity, which typically ranges between approximately 5 cm and 10 cm (5 cm = low sensitivity, 10 cm = high sensitivity).
The “Activation message type” parameter allows the transmission of a dedicated communication object when the proximity sensor remains active for at least the time defined by the “Hold time to send” parameter.

1	Keypad	Proximity sensor	1 bit	C	R	-	T	-	1-bit, switch

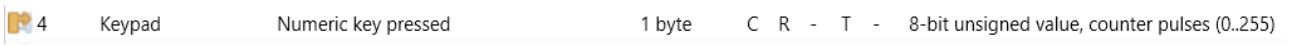
The value of the sent message can be:

- "Disable": no message is sent (CO not visible).
- "Approach 0, removal 1": with sensor occupied for hold time, message 0 is sent; with not occupied sensor, message 1 is sent.
- "Approach 1, removal 0": as described above, but with message values reversed.

- “Toggle approaching”: it alternatively sends 1 and 0 when the sensor is occupied for at least the set time.

3.1.1.4 Send message of pressed keys

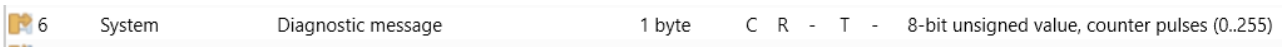
If this parameter is set to “Yes”, a message is transmitted on the KNX bus every time a numeric key is pressed. The value of the transmitted communication object corresponds to the numeric value of the pressed key (0–9).



If, in the “Function keys” section, key F2 is configured as a confirmation key for validating an entered access code, an additional communication object becomes available. This CO transmits value 1 when the key is pressed (see section 3.3).

3.1.1.5 System diagnostic message

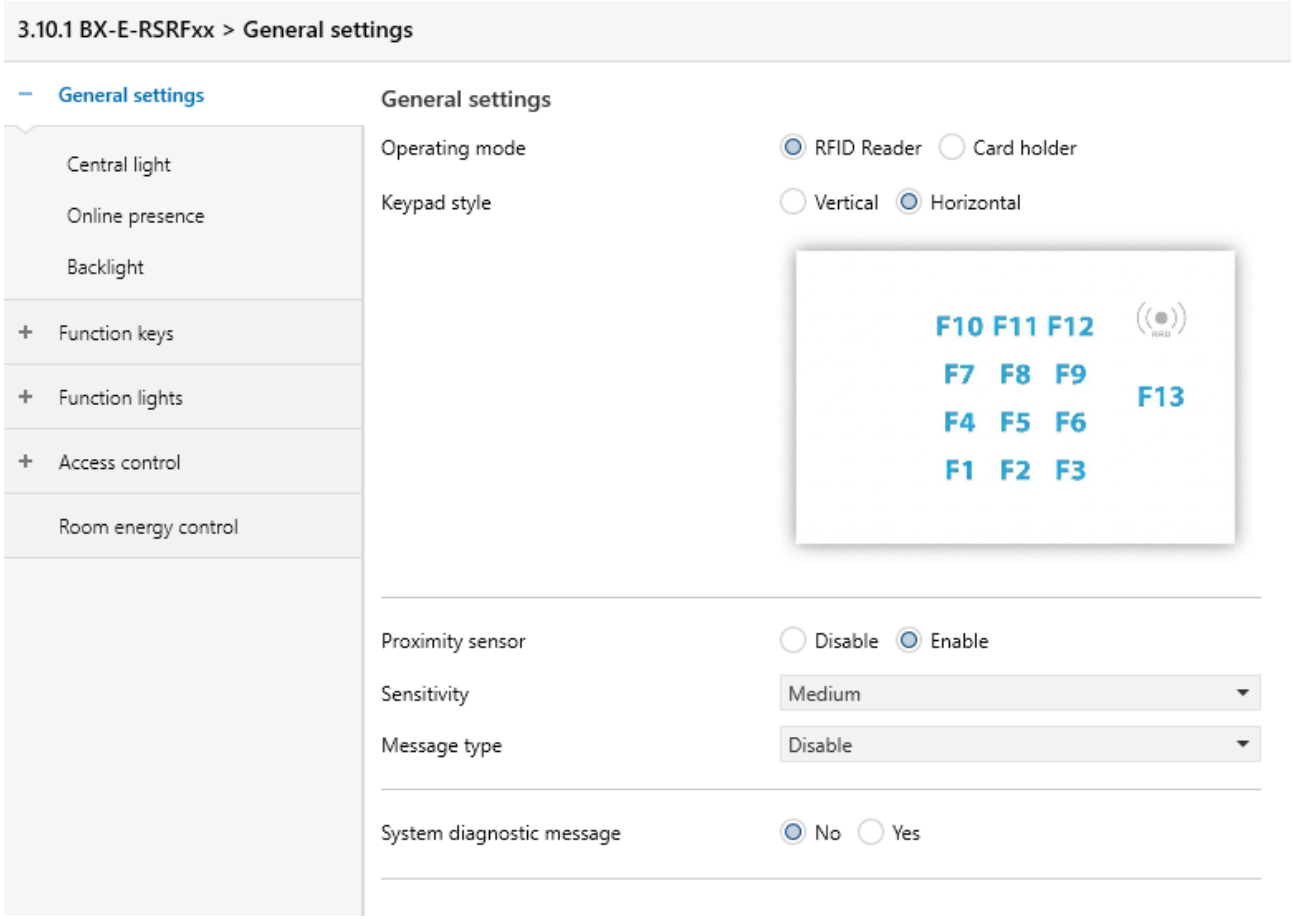
This parameter enables a KNX non-standard communication object.
The value of this CO represents a numeric error code in the range 0–255.



Refer to **Appendix A** for the detailed description of the DPT used and the list of diagnostic error codes.

3.1.2 BX-E-RSRFxx

The following section describes the parameters and functions available for the BX-E-RSRFxx device.



3.1.2.1 Operating mode

Allows the operating mode of the device to be selected. The available options are "RFID Reader" and "RFID Card Holder", as shown in the figure below.

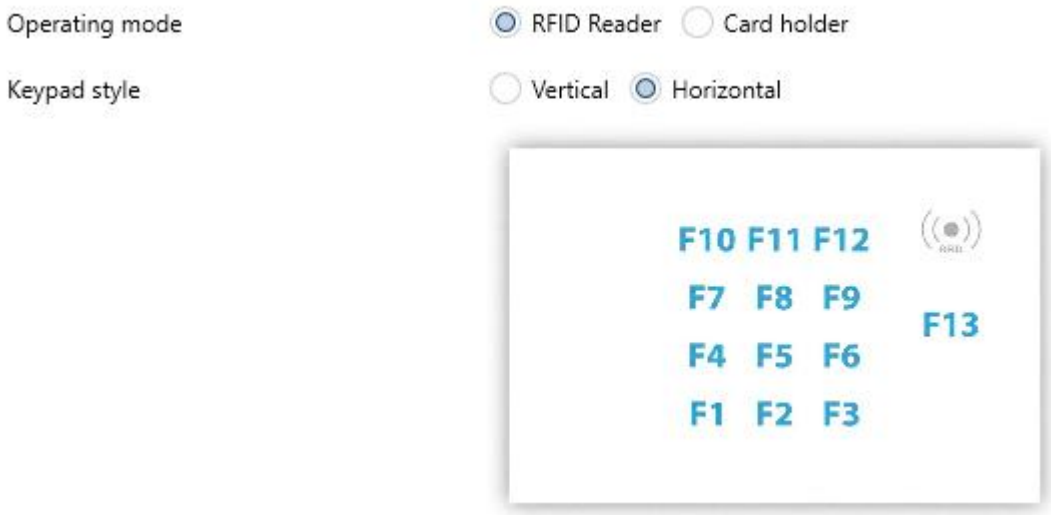
When "RFID Reader" mode is selected, the device operates as a standard RFID reader for transponder identification. When "RFID Card Holder" mode is selected, the device detects the presence of a card inserted into the dedicated slot.

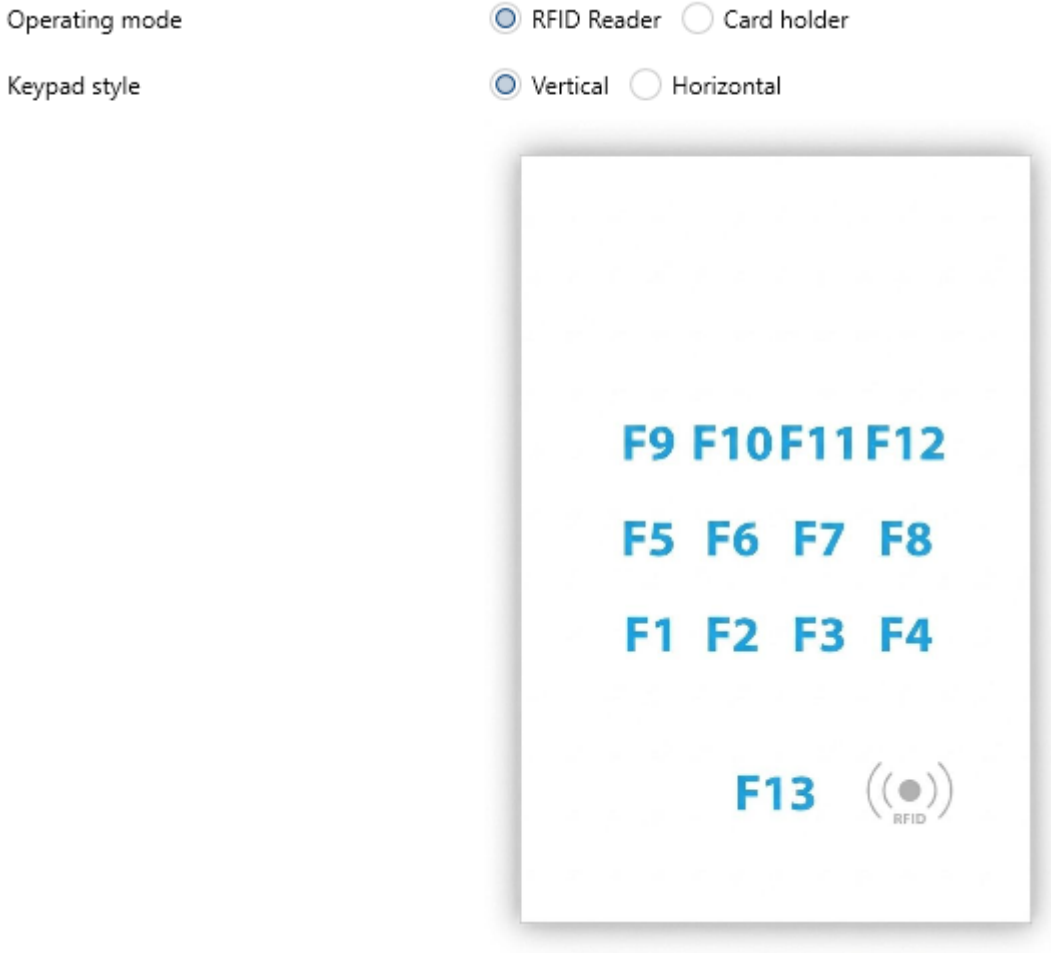
To use the "RFID Card Holder" mode, the device must be equipped with a front cover featuring the appropriate slot for card insertion.

3.1.2.2 Keypad style

This parameter allows the orientation of the device to be selected. The selected orientation must match the physical orientation of the installed device. The available options are Horizontal and Vertical.

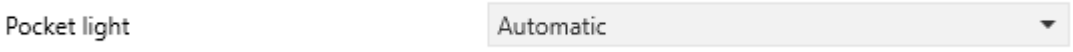
This parameter is available only when the device is configured in "RFID Reader" mode. When "RFID Card Holder" mode is selected, the orientation cannot be configured and the corresponding parameter is not displayed.





3.1.2.3 Pocket light

Allows the behavior of the RFID card holder illumination to be configured. This parameter is visible and configurable only when the device is set to "RFID Card Holder" mode.



In "Automatic" mode, the illumination is switched on when no RFID card is inserted and switched off when a valid RFID card is detected in the holder. The other available options are "Always On" and "Always Off", whose behavior is self-explanatory.

3.1.2.4 Proximity sensor

The "Proximity Sensor" section provides the same functionalities and parameters as those available for the BX-E-R12SRFxx and BX-E-R12Sxx devices. For detailed information, please refer to the corresponding section.

3.1.2.5 System diagnostic message

The "System Diagnostics Message" section provides the same functionalities and parameters as those available for the BX-E-R12SRFxx and BX-E-R12Sxx devices. For detailed information, please refer to the corresponding section.

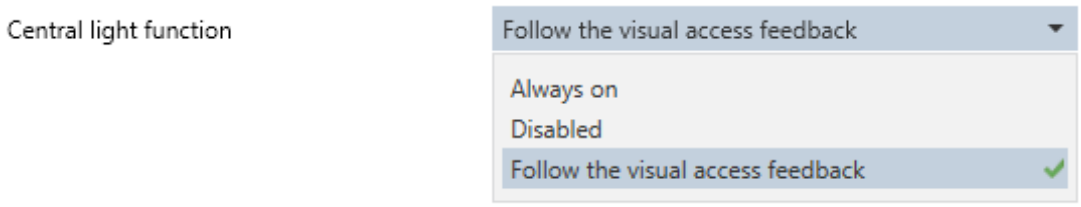
3.2 Central light (only BX-E-RSRFxx)

When the device is configured in RFID Reader mode, the Central Light function can be enabled. This function uses some of the LEDs normally associated with the function buttons: in the vertical version, the LEDs of buttons F5, F6, F7, and F8 are used, while in the horizontal version, the LEDs of buttons F4, F5, and F6 are used.

When the Central Light function is enabled, the affected LEDs cannot be configured in the "Function Lights" section. For this reason, an information message is displayed at the top of the page indicating which LEDs are temporarily unavailable. When the Central Light function is disabled, the corresponding LEDs become configurable again.

The following operating modes are available:

- Always On
- Disabled
- Follow Access Visual Feedback

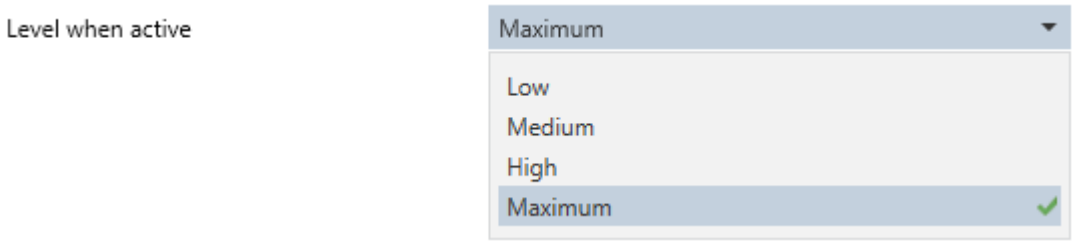


With the "Disabled" mode, the Central Light is disabled and all affected LEDs can be configured in the "Function Lights" section.

With the "Always On" mode, the Central Light remains permanently illuminated.

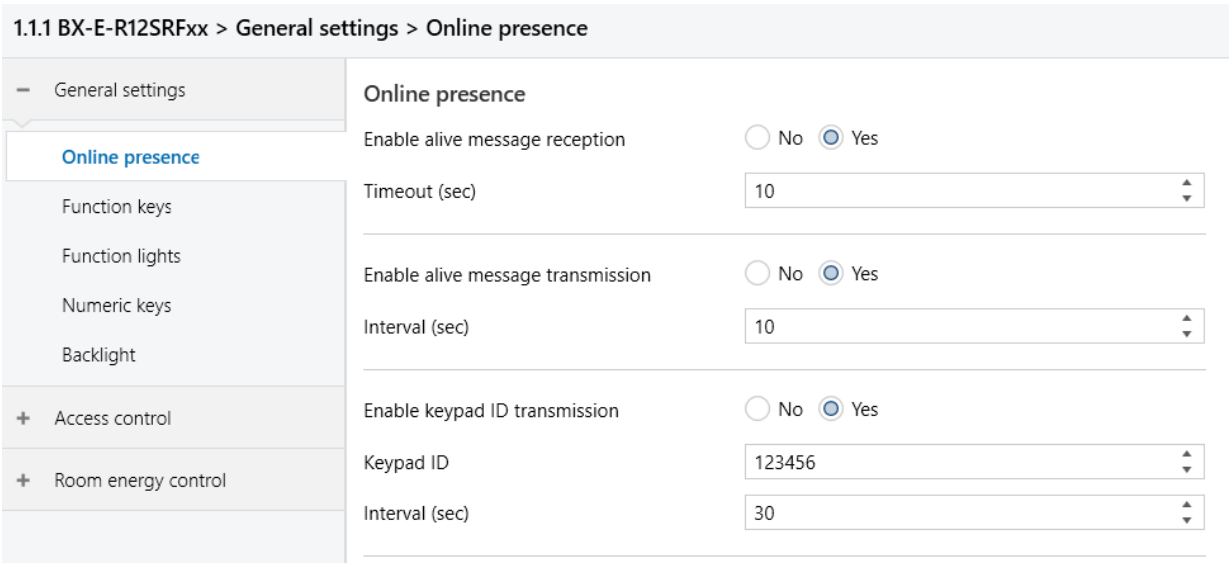
With the "Follow Access Visual Feedback" mode, the Central Light follows the device's access visual feedback, behaving in the same way as the backlight when the latter is enabled.

For the modes in which the Central Light is active, its brightness level can also be configured.



3.3 Online Presence

This section contains parameters that allow a supervisory system to monitor the correct operation of the device.
As the keypad is dedicated to access control applications, continuous monitoring of its availability and correct functioning on KNX bus, may be required.
The parameters managed in this section are described below.



3.3.1 Enable alive message reception

This parameter enables the keypad to receive a specific online presence message from a supervisory device within a defined time interval.
In practice, the keypad expects to receive periodically, from the KNX bus, a message with value 1 on the “Remote request” communication object (CO 8). The interval between successive receptions must not exceed the value defined by the “Timeout” parameter.

If the supervisory device cyclically sends value 1 within the configured timeout, the keypad responds by setting the “Remote request reply” communication object (CO 9) to value 0, indicating correct operation.
If the supervisory device stops sending the message, or if the timeout interval is exceeded, the keypad signals an error condition by transmitting value 1 on the “Remote request reply” communication object.

8	Online	Remote request	1 bit	C	R	W	-	-	1-bit, boolean
9	Online	Remote request reply	1 bit	C	R	-	T	-	1-bit, boolean

3.3.2 Enable alive message transmission

This parameter enables cyclic transmission by the keypad of a presence message with value 1 on the KNX bus. The transmission interval is defined by the “Interval” parameter.
This function can be used by a supervisory system to verify the correct operation of the keypad and its connection to the KNX bus.

10	Online	Transmit presence	1 bit	C	R	-	T	-	1-bit, boolean

3.3.3 Enable keypad ID transmission

This parameter enables cyclic transmission by the keypad of a numeric identifier.
The identifier consists of six digits (0–999999) and is configured using the “Keypad ID” parameter.
The transmission interval is defined by the “Interval” parameter.
This feature allows unambiguous identification of the device by a supervisory system.

11	Online	Transmit ID	4 bytes	C	R	-	T	-	4-byte unsigned value, counter pulses (unsigned)

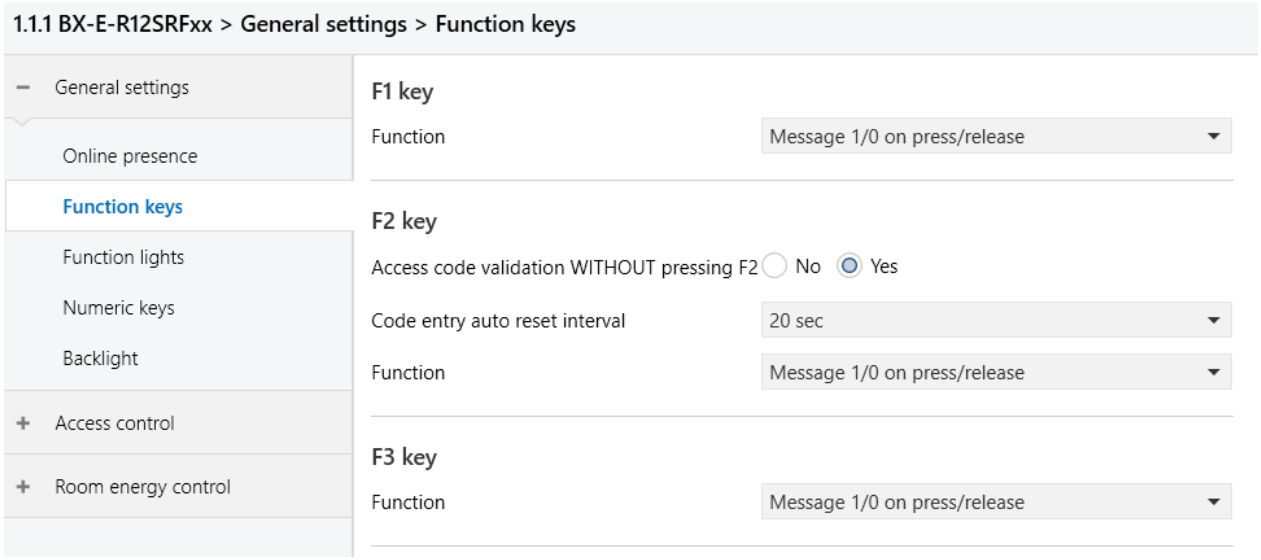
3.4 Function keys

These parameters determine the behavior of the function keys. For the BX-E-R12SRFxx and BX-E-R12Sxx devices, the function keys are named F1, F2, and F3.

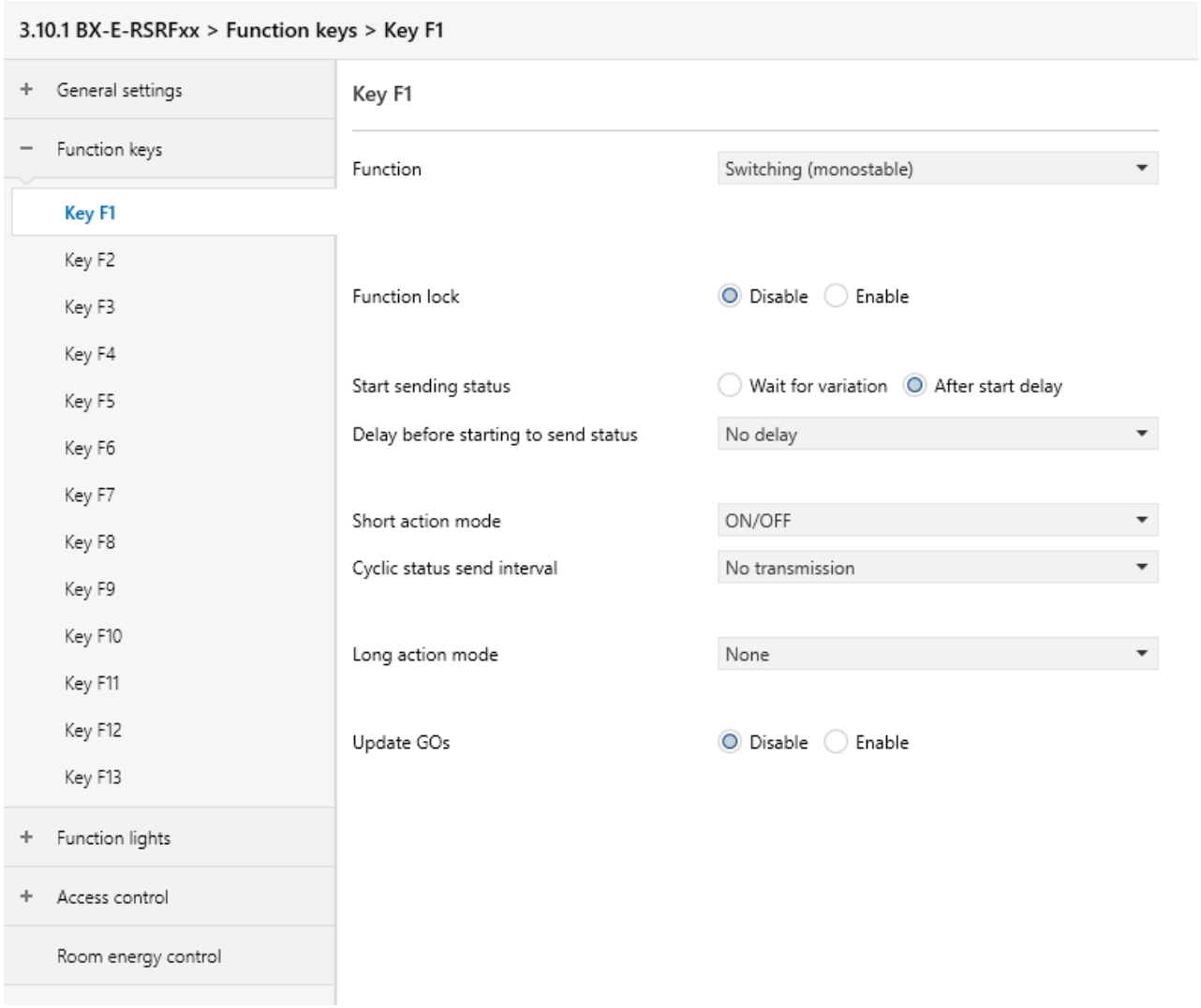
For the BX-E-RSRFxx device, the number of available function keys depends on the operating mode configured via ETS:

- In RFID Reader mode, all twelve front keys and the optional thirteenth key can be independently configured as function keys.
- In Card Holder Pocket mode, only the function keys not occupied by the RFID pocket are available, namely F1, F4, F7, and F10.

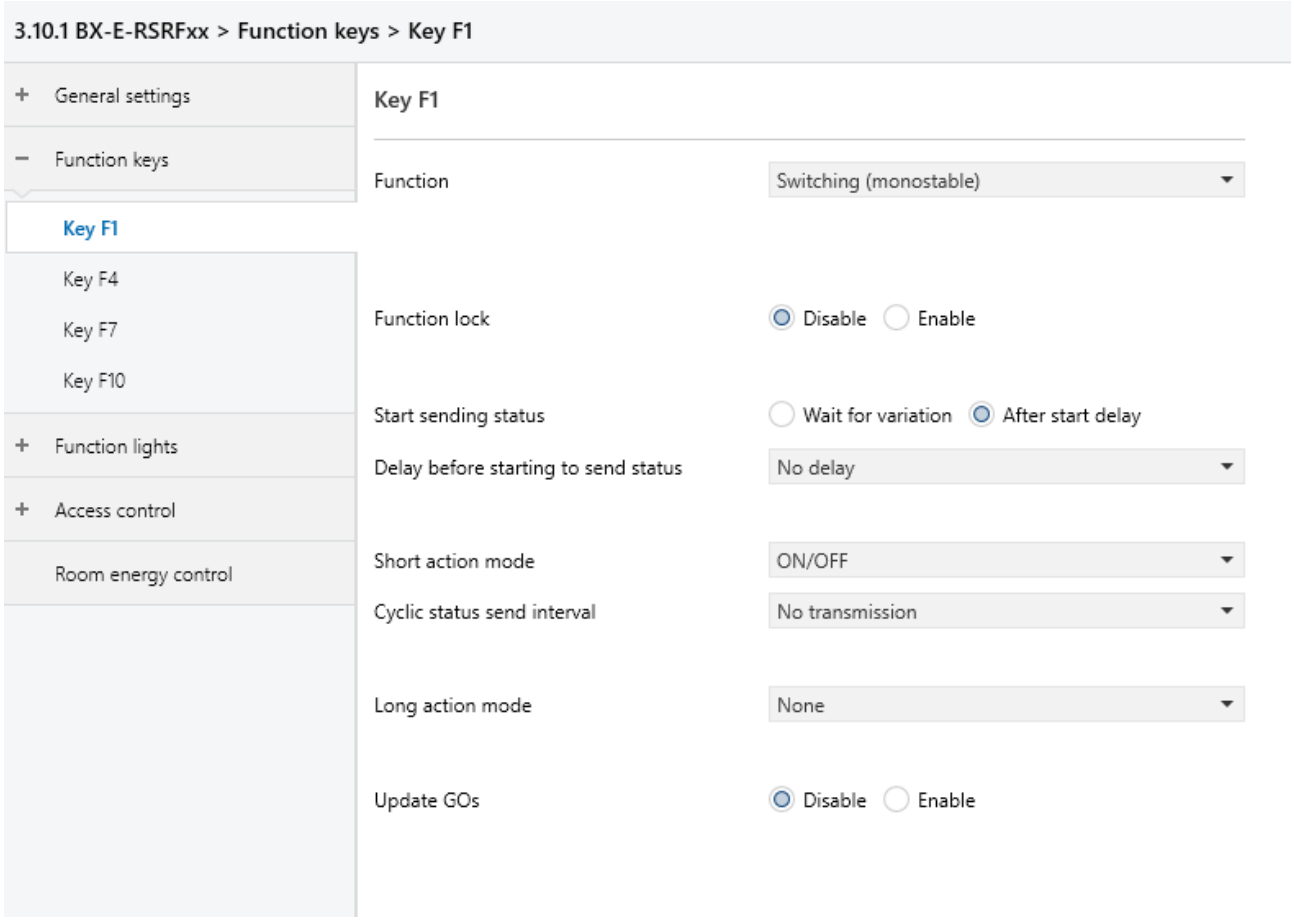
The functions associated with the keys of the BX-E-RSRFxx device differ from those available on the BX-E-R12SRFxx and BX-E-R12Sxx devices.



Function keys for BX-E-R12SRFxx and BX-E-R12Sxx



Function keys for BX-E-RSRFxx product configured in RFID Reader mode



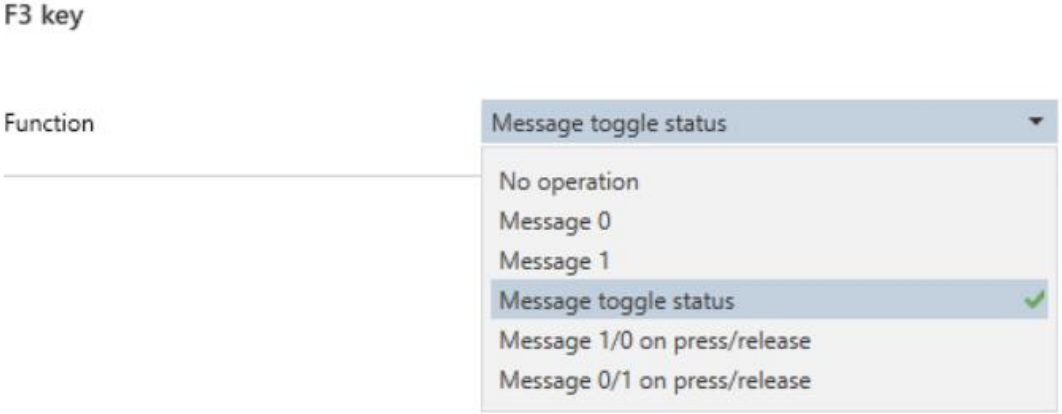
Function keys for BX-E-RSRFxx product configured in Card holder mode

3.4.1 BX-E-R12SRFxx and BX-E-R12Sxx

The BX-E-R12SRFxx and BX-E-R12Sxx devices support three function keys. Their functions are described below.

3.4.1.1 F1/F3 Key

Keys F1 and F3 can be used to transmit generic-purpose commands on the KNX bus. The value transmitted on the command communication object when the key is pressed is defined by the “Function” parameter.



If the option “Toggle based on status” is selected, an additional status communication object is enabled. In this case, the current value of the status object is read, inverted and then transmitted on the CO.

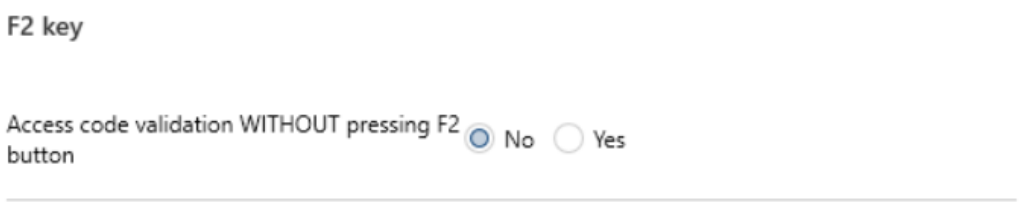
35	Key F3	Command	1 bit	C	R	-	T	-	1-bit, switch
36	Key F3	Status	1 bit	C	-	W	-	-	1-bit, switch

Important note. For correct operation of key F3 (if present on the glass front panel), the proximity sensor must be enabled (see section 3.1.3).

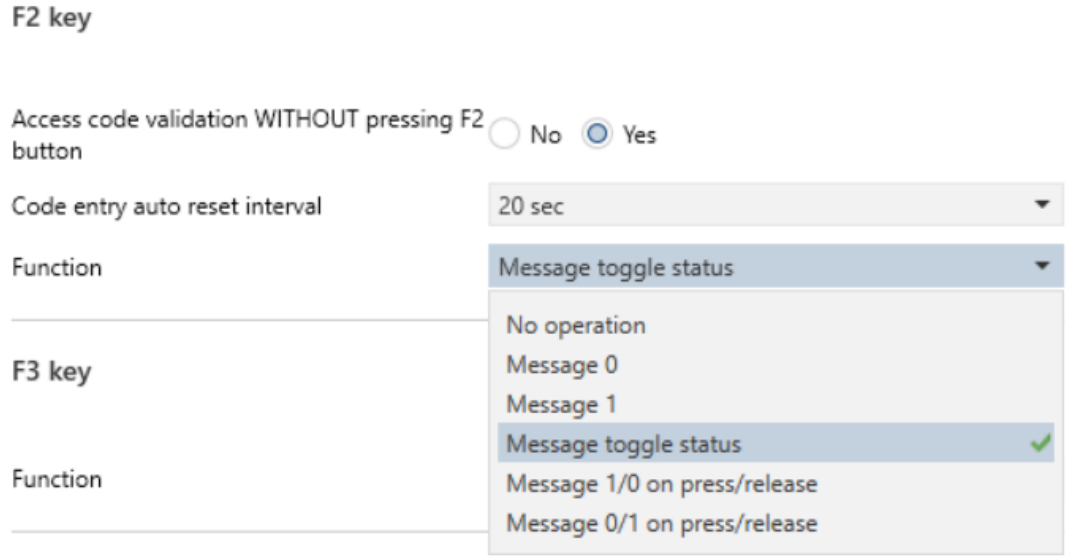
3.4.1.2 F2 Key

The F2 key can operate in two different modes.

- If confirmation of the entered numeric access code is required, F2 can be configured as a confirmation key. In this case, the access code is validated only when the F2 key is pressed.



- If access code validation is intended to be automatic (without pressing a confirmation key), F2 can be configured for generic-purpose use, in the same way as keys F1 and F3 (see section 3.3.1).



The use of F2 in general mode (command and status CO) also makes the parameter "Code entry auto reset interval" available.

Since automatic validation occurs as soon as the configured number of digits has been entered (see section 3.7.2), this parameter acts as a safety function.
If no further input occurs within the configured time, the digits temporarily stored in the keypad memory are cleared and the device returns to the initial state, ready to accept a new code.
This prevents a situation in which one user partially enters a code and leaves, allowing another user to unintentionally continue code entry.

3.4.2 BX-E-RSRFxx

The BX-E-RSRFxx device supports up to 13 function keys, which can be configured independently. Refer to **Appendix F** for a description of the available functions.

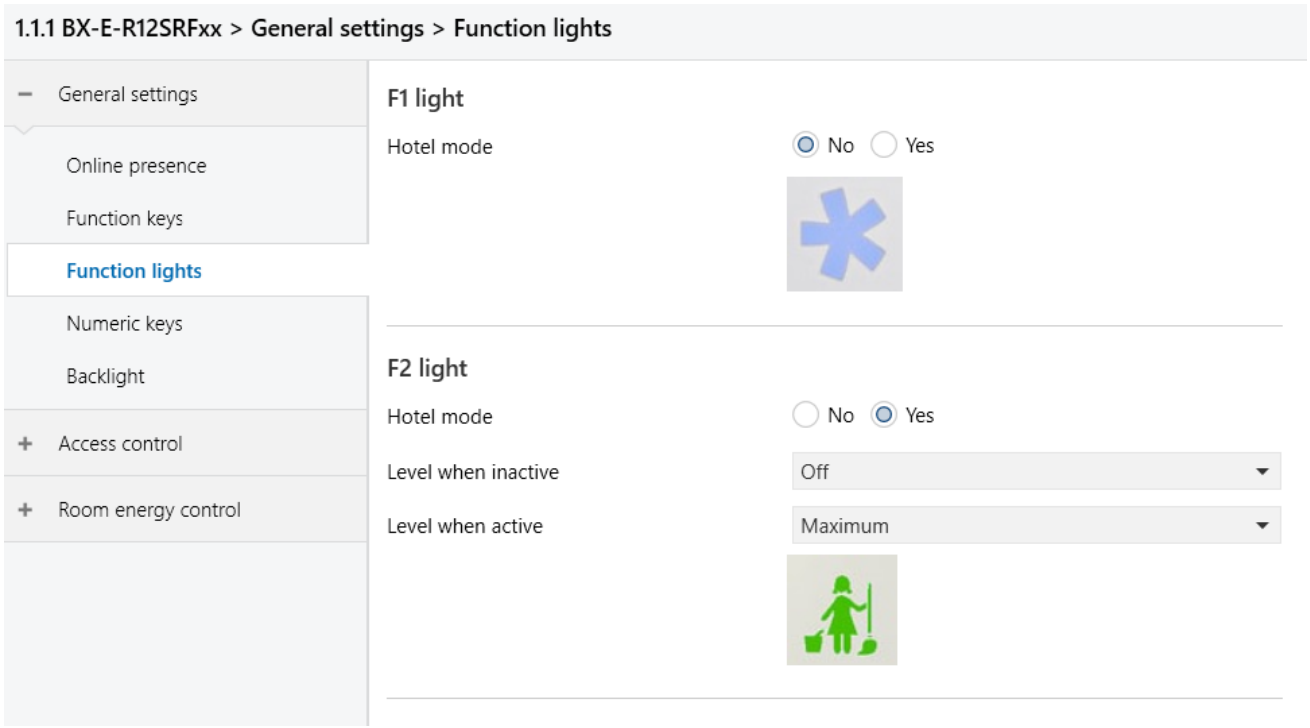
3.5 Function lights

These parameters determine the behavior of the LEDs associated with the function keys.

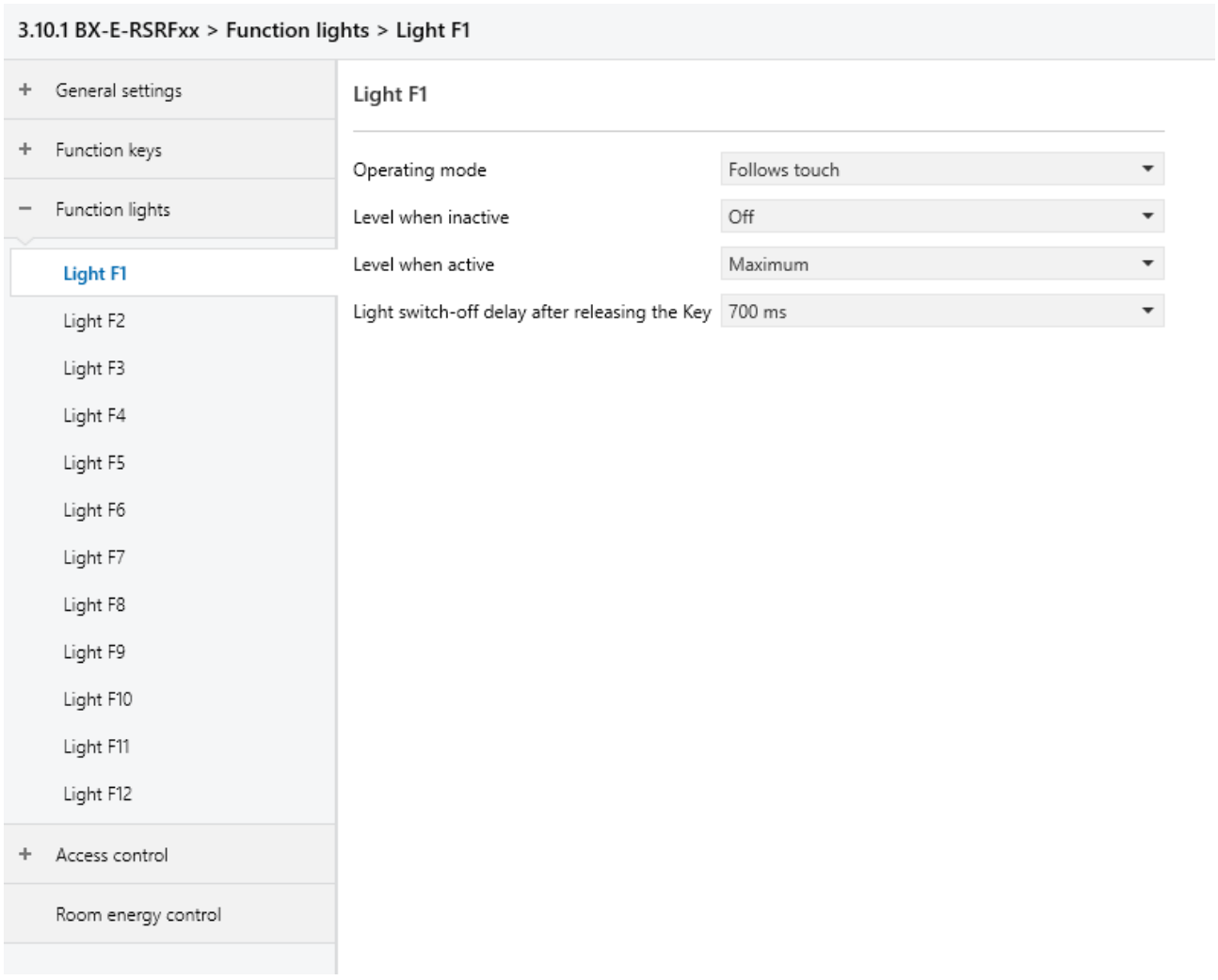
For the BX-E-R12SRFxx and BX-E-R12Sxx devices, the illuminated keys are F1 and F2, while key F3 does not provide any illumination.

For the BX-E-RSRFxx device, up to 12 keys can be illuminated. The actual number of illuminable keys depends on the device configuration and the enabled functions. In particular, the maximum of 12 illuminated keys is available when the device is configured in RFID Reader mode and the central light is disabled. The optional thirteenth key does not provide any illumination.

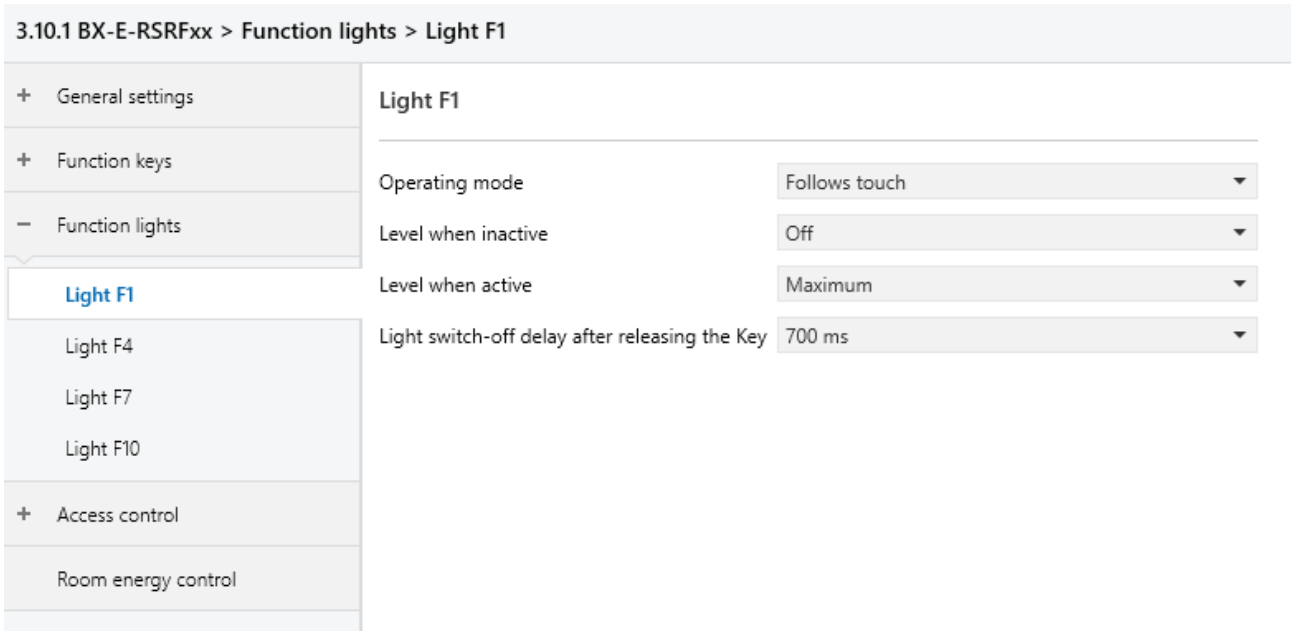
The available LED functions for the function keys of the BX-E-RSRFxx device differ from those provided for the BX-E-R12SRFxx and BX-E-R12Sxx devices; the related parameters are described in the following sections.



Function lights for BX-E-R12SRFxx and BX-E-R12Sxx products



Function lights for BX-E-RSRFxx product configured in RFID Reader mode



Function lights for BX-E-RSRFxx product configured in Card holder mode

3.5.1 BX-E-R12SRFxx and BX-E-R12Sxx

For the BX-E-R12SRFxx and BX-E-R12Sxx devices, the light indicators include the "Hotel function" enable parameter. The behavior varies depending on the selected mode.

3.5.1.1 Hotel mode/Function light disabled

By selecting "No", the light of the function key will be managed in the same way as the numeric key lights (section 3.5).

3.5.1.2 Hotel mode/Function light enabled

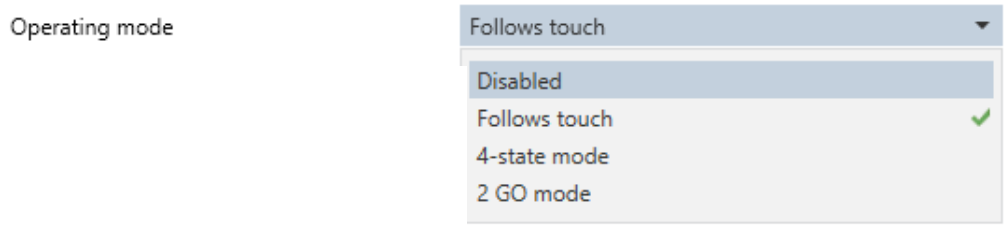
By selecting "Yes", the light of the function key is controlled by the dedicated communication object; the keypad will return the status controlled on another specific CO.

41	Light F2	Set	1 bit	C	-	W	-	-	1-bit, switch
42	Light F2	Status	1 bit	C	R	-	T	-	1-bit, switch

In this last case, the parameters "Level when inactive" and "Level when active" are available and allow to specify the brightness level of the LED to be set when the command CO is written respectively with the values 0 and 1.

3.5.2 BX-E-RSRFxx

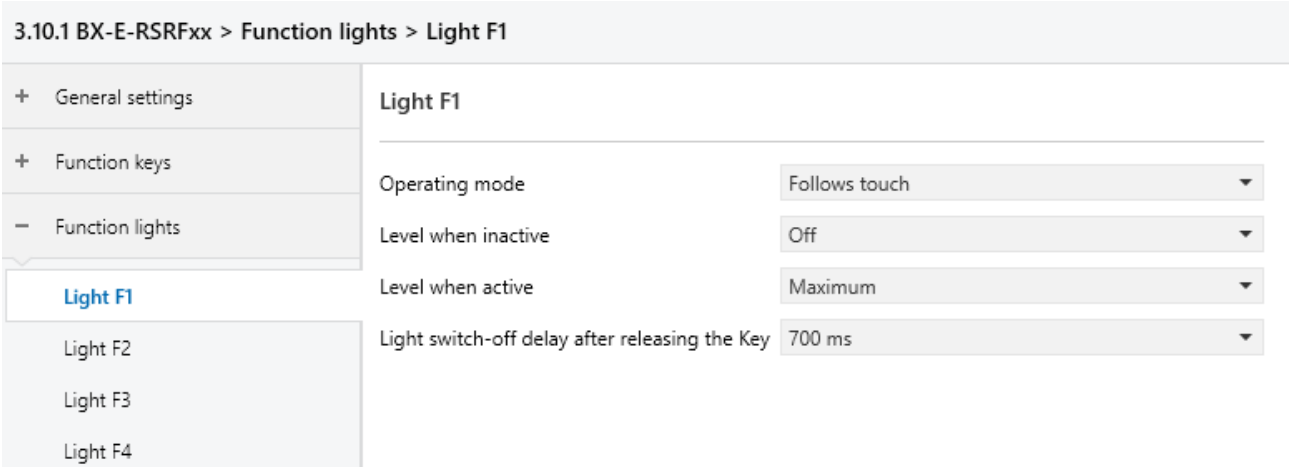
For the BX-E-RSRFxx device, the behavior of the function key light indicators is determined by the “Operating mode” parameter. In particular, one of the following modes can be selected: Disabled, Follows touch, 4-state mode, and 2 GO mode.



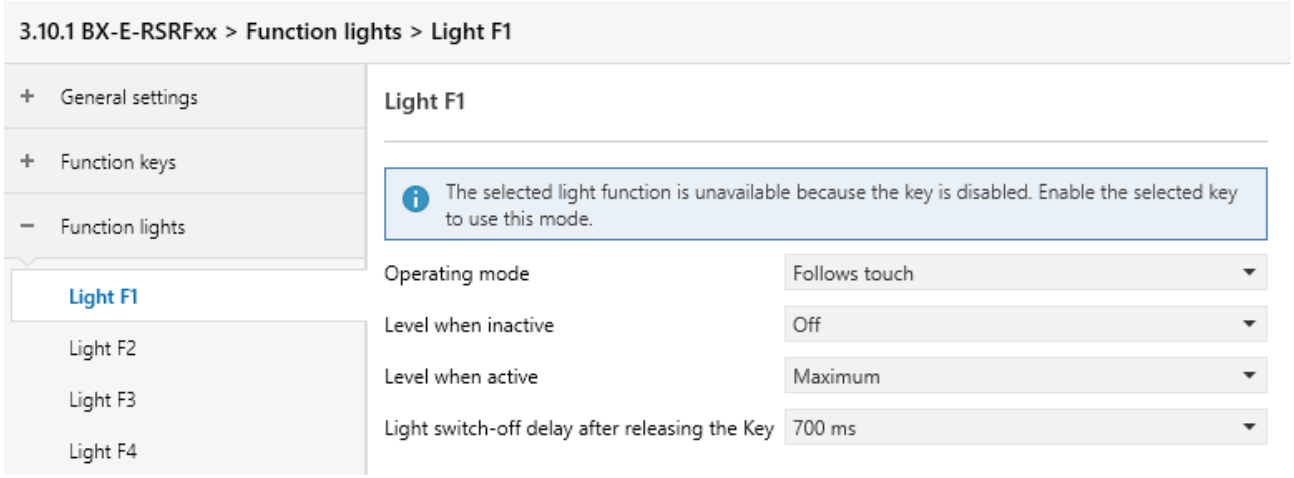
The available functions and the related configuration parameters vary depending on the selected mode, as described in the following sections.

3.5.2.1 Follows touch

It represents an operating mode in which the LED associated with the function key automatically follows the key press state. The switching on, switching off, and the corresponding brightness levels are therefore managed according to the user’s interaction with the key.



For this mode to operate, the key associated with the LED must be enabled. If the key is disabled, the LED will not follow the key press and release events. In this case, a warning message will be displayed, as shown in the following figure.

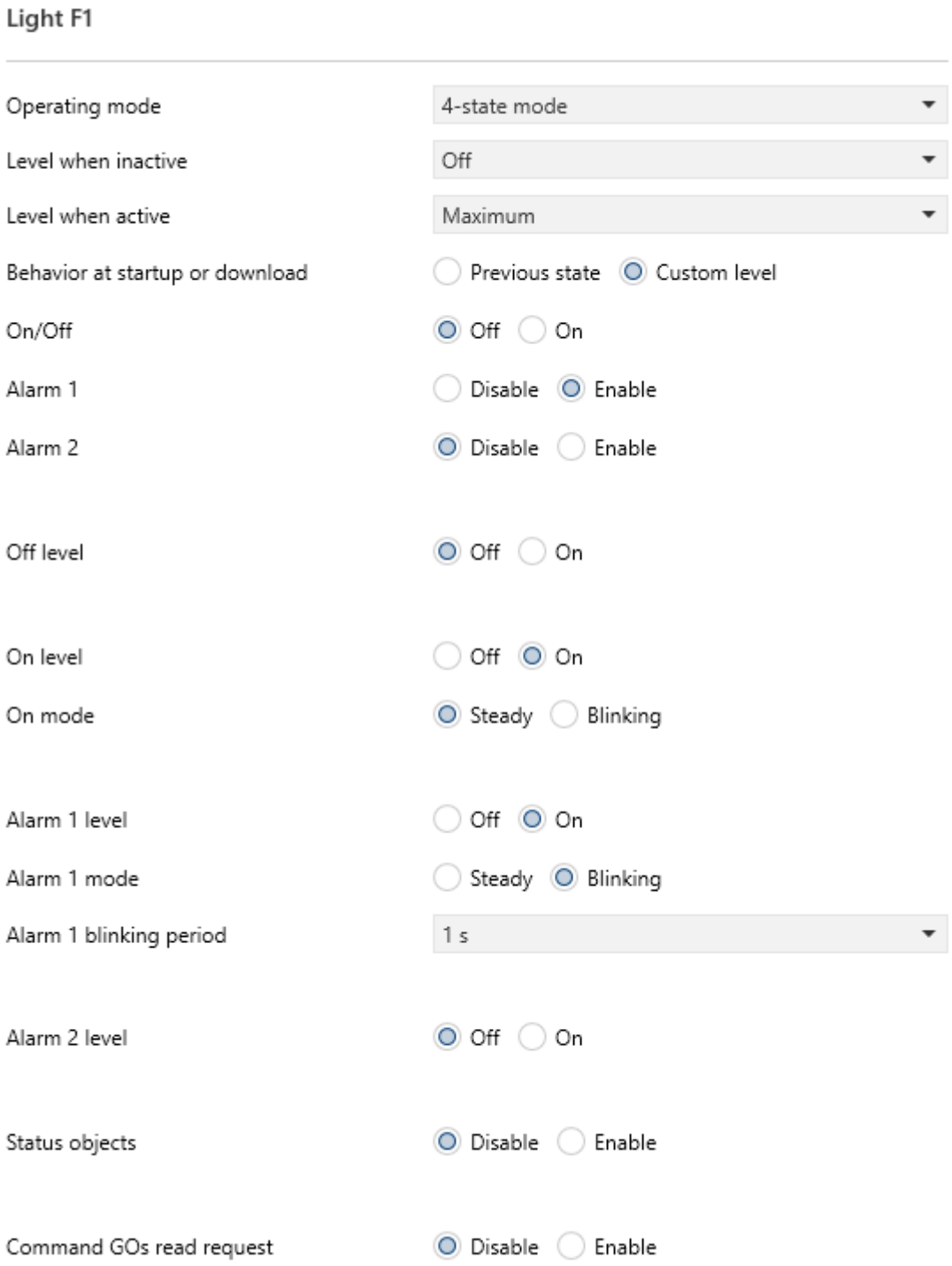


"Inactive level" sets the LED brightness level when the key is not pressed.
"Active level" sets the LED brightness level when the key is pressed.

When the key transitions from the pressed state to the released state, the "Key release light switch-off delay" parameter defines the delay for transitioning from the "Active level" intensity to the "Inactive level" intensity of the associated LED.

3.5.2.2 4-state mode

In 4-state mode, it is possible to associate a different LED behavior with four distinct states. Consequently, the corresponding dedicated communication objects will be made available.



The states that the LED channel can assume are:

- ON
- OFF
- Alarm 1
- Alarm 2

The LED brightness levels are defined by the “Level when inactive” and “Level when active” parameters, as described above.

For each state, the following parameters can be configured:

- LED state (on or off);
- LED operating mode (steady or blinking);
- Blinking period, if blinking mode is selected.

The communication objects for setting the LED state and, if enabled via the “Status objects” parameter, the corresponding status objects are illustrated below.

626	Light F1	On/Off setting	1 bit	C	-	W	T	U	1-bit, switch
627	Light F1	On/Off status	1 bit	C	R	-	T	-	1-bit, switch
628	Light F1	Alarm 1 setting	1 bit	C	-	W	T	U	1-bit, alarm
629	Light F1	Alarm 1 status	1 bit	C	R	-	T	-	1-bit, switch
630	Light F1	Alarm 2 setting	1 bit	C	-	W	T	U	1-bit, alarm
631	Light F1	Alarm 2 status	1 bit	C	R	-	T	-	1-bit, switch

The LEDs can also be used to signal system operating states or alarm conditions. A different display mode can be associated with each state, allowing the user to quickly identify the active condition.

The alarm states (Alarm 1 and Alarm 2) have priority over the normal ON and OFF states. In particular, Alarm 2 has priority over Alarm 1, which in turn has priority over the ON and OFF states.

If Alarm 2 is activated (by writing the value 1 to the “Alarm 2 setting” GO), the LED assumes the behavior configured in the “Alarm 2” section. Any writes to the “On/Off setting” or “Alarm 1 setting” objects will have no visible effect due to the lower priority of these states.

Only when Alarm 2 is deactivated (by writing the value 0 to the “Alarm 2 setting” GO) does the LED return to displaying the active state with the immediately lower priority.

The “Behavior at startup or download” parameter defines the LED state at device power-on or after ETS configuration download. It is possible to choose whether to restore the previous state or apply a configurable default state.

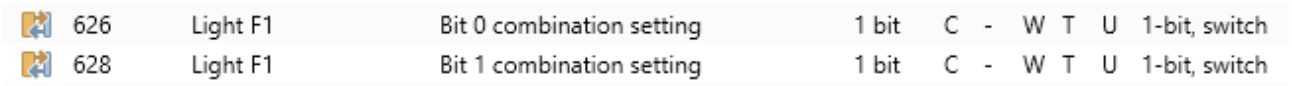
The “Status objects” parameter enables the LED state communication objects. These states can be sent on the KNX bus once after startup and subsequently at periodic intervals, according to the configured parameters.

The “Command GOs read request” parameter enables a KNX bus read request for the command objects associated with the LED channel, facilitating synchronization between the device and any supervision systems.

The read request is performed once after device startup and can be repeated periodically depending on the configured settings.

3.5.2.3 2 GO mode

This LED management mode allows selecting one of the four available states by writing two 1-bit communication objects associated with the LED channel.



626	Light F1	Bit 0 combination setting	1 bit	C	-	W	T	U	1-bit, switch
628	Light F1	Bit 1 combination setting	1 bit	C	-	W	T	U	1-bit, switch

The parameters related to LED behavior remain unchanged compared to the 4-state mode (see previous section).

In particular, for each combination it is possible to configure:

- the LED state (on or off);
- the LED operating mode (steady or blinking);
- the blinking period, if blinking mode is selected.

Unlike 4-state mode, the states are not named ON, OFF, Alarm 1, and Alarm 2, but Combination 1, Combination 2, Combination 3, and Combination 4.

The active combination is determined by the value assumed by the two command communication objects, as shown in the following table.

Combination	1	2	3	4
Set combination bit 0	0	1	0	1
Set combination bit 1	0	0	1	1

The meaning and behavior of the other parameters, including “Behavior at startup or download”, “Status objects”, and “Command GOs read request”, remain unchanged compared to the 4-state mode described in the previous section.

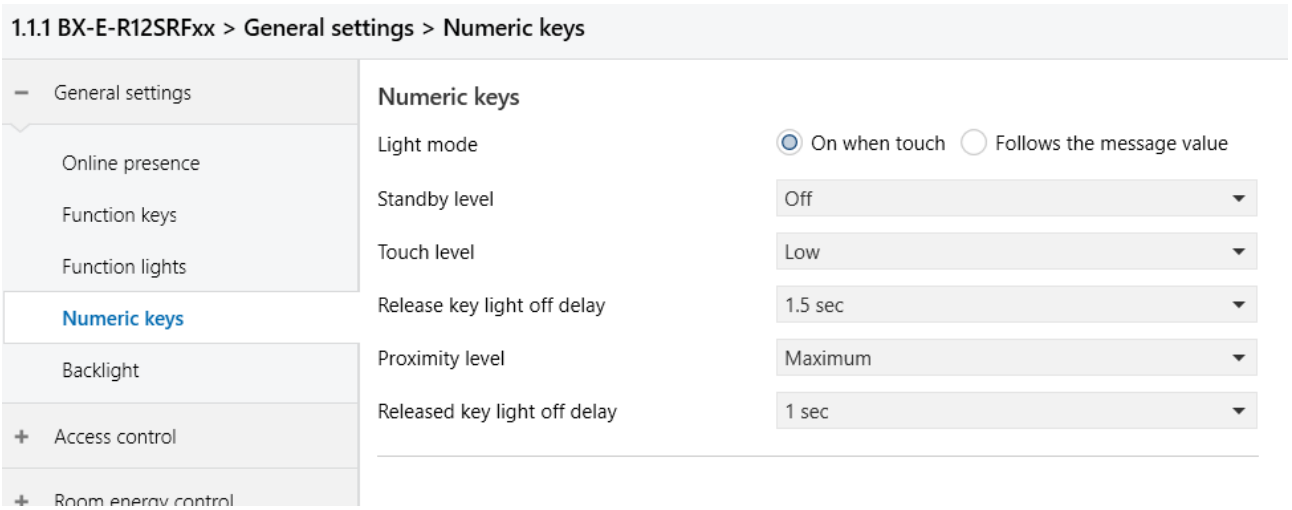
3.6 Numeric keys (only BX-E-R12SRFxx e BX-E-R12Sxx)

This section, available exclusively for the BX-E-R12SRFxx and BX-E-R12Sxx devices, allows configuring the illumination mode of the numeric keys through the parameters available in the corresponding ETS library page.

The available operating modes are “On on touch” and “Follows the message value”.

3.6.1 On when touch

This mode provides automatic control of numeric key illumination. Switch-on, switch-off and brightness levels are managed using the proximity sensor. For this mode to operate correctly, the proximity sensor must be enabled (see section 3.1.3).



"Standby level" sets the light intensity level of the numeric keys when none of them is pressed and when the proximity sensor is not occupied.

"Proximity level" is the light intensity when no button is pressed but the proximity sensor is occupied; for example, a hand is present in the sensor’s range of action.

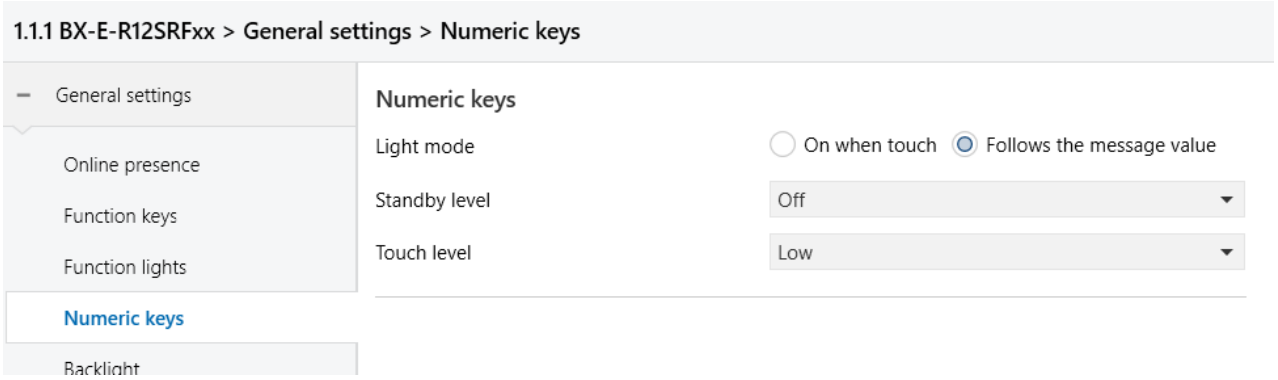
When the proximity sensor switches from occupied to not occupied (released), the parameter "Released proximity light off delay" represents the delay in the transition from light level "Proximity level" to "Standby level" of the numeric keys LEDs.
"Touch level" sets the light intensity level of the pressed numeric key.
When the key switches from pressed to released, the parameter "Released key light off delay" represents the delay in the passage from intensity "Touch level" to intensity "Proximity level" of the numeric key LED.

3.6.2 Follows the message value

In this operating mode, the illumination of the numeric keys is not linked to the proximity sensor, but is controlled exclusively via KNX communication objects.
A dedicated communication object is available for each numeric key, allowing its illumination to be switched on or off individually.

17	Key light 1	On/off	1 bit	C - W - -	1-bit, switch
18	Key light 2	On/off	1 bit	C - W - -	1-bit, switch
19	Key light 3	On/off	1 bit	C - W - -	1-bit, switch
20	Key light 4	On/off	1 bit	C - W - -	1-bit, switch
21	Key light 5	On/off	1 bit	C - W - -	1-bit, switch
22	Key light 6	On/off	1 bit	C - W - -	1-bit, switch
23	Key light 7	On/off	1 bit	C - W - -	1-bit, switch
24	Key light 8	On/off	1 bit	C - W - -	1-bit, switch
25	Key light 9	On/off	1 bit	C - W - -	1-bit, switch
26	Key light F1	On/off	1 bit	C - W - -	1-bit, switch
27	Key light 0	On/off	1 bit	C - W - -	1-bit, switch

The parameters "Standby level" and "Touch level" define the brightness applied when the associated CO assumes values 0 (off) and 1 (on), respectively.

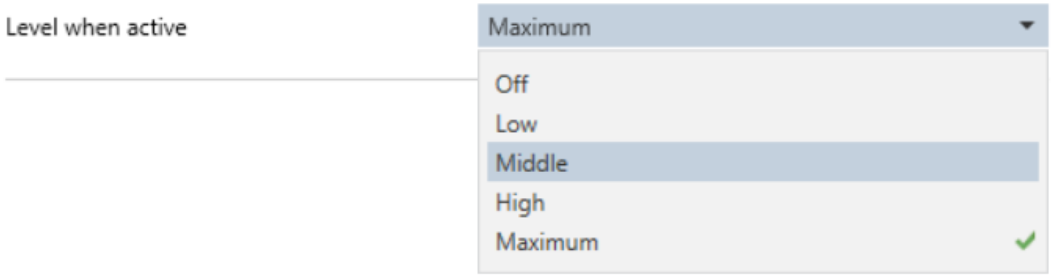


3.7 Backlight

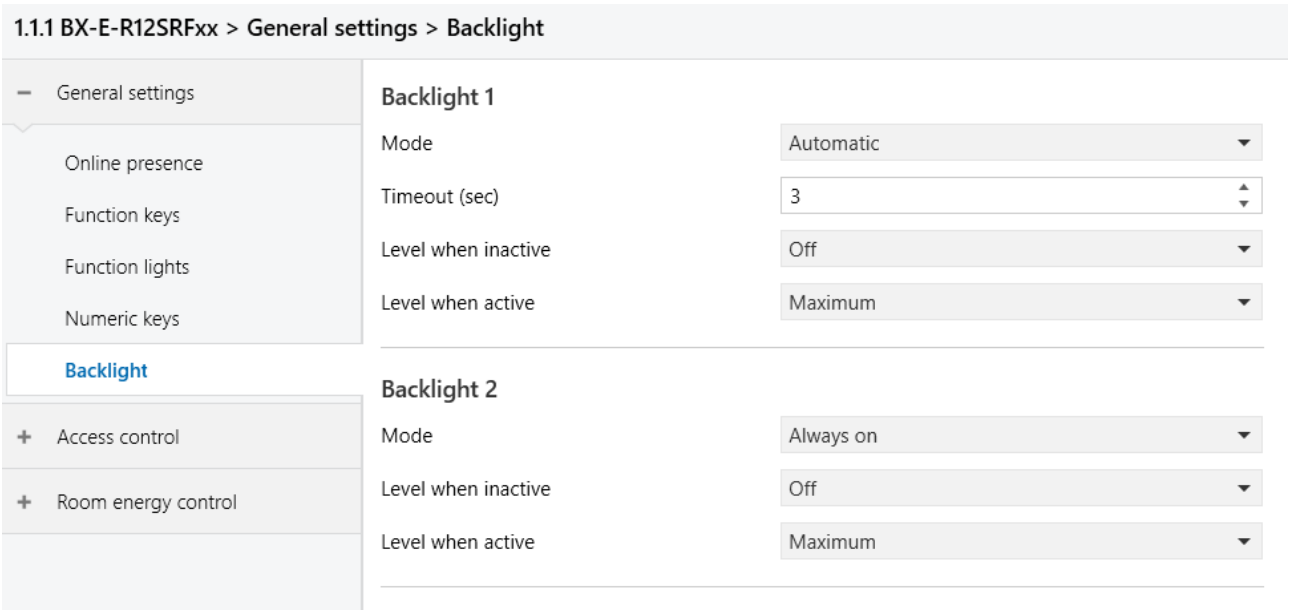
The backlight of the keypad allows to spread a light through the transparent plastic base of the device.

BX-E-R12SRFxx differentiates the backlight, its parameters and communication objects into two groups: "Backlight 1" and "Backlight 2". In fact, it is possible to manage the light of the top/bottom and left/right sides separately; both offer the same control options.

All the 3 modes provide the setting of the brightness levels corresponding to the inactive state and the active state of the backlight (1 and 2); see the parameters "Level when inactive" and "Level when active".



Similarly, all the 3 modes allow to control the backlight also through a communication object that override the default behaviour set in the parameter "Mode".



3.7.1 Mode: Always off

The lighting is normally inactive. It is possible to still control it using the CO shown above.

3.7.2 Mode: Always on

Lighting is normally on. It is possible still control it using the CO shown above.

3.7.3 Mode: Automatic

Represents the automatic operation of the backlight. In this case, lighting occurs when the proximity sensor is occupied. The shutdown will occur automatically after the proximity sensor has been released and kept free for the time indicated by the parameter "Timeout".
This mode of operation requires the proximity sensor to be enabled (section 3.1.3).

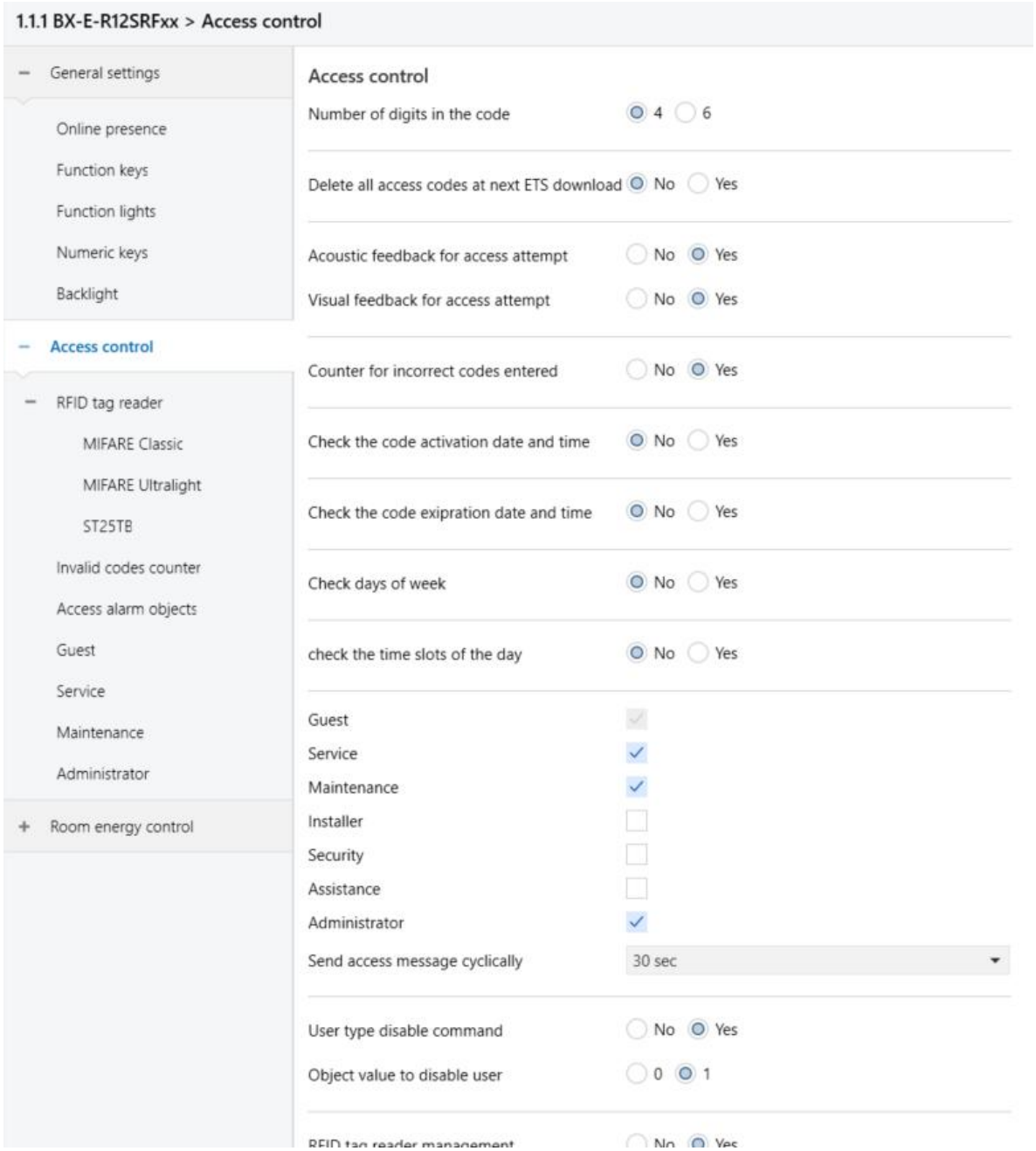
3.8 Access control

The keypad supports access control via:

- numeric access codes (4 or 6 digits), and
- RFID cards or tags (not supported in BX-E-R12Sxx)

Access validation is performed locally by the keypad, without the need of external controllers.

The device is capable of storing internally up to approximately 1000 numeric access codes and all associated information required for access management.



3.8.1 System date and time

Access control management implies that the system is informed of the current date and time.

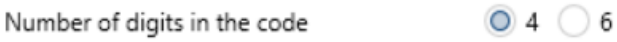
This information must be provided to the keypad via KNX bus by writing CO 46 at all start-ups and after downloading the ETS application.
The date-time captured by the device is returned to CO 47.

46	System	Set current date and time	8 bytes	C	-	W	-	-	Date Time, date time
47	System	Current date and time status	8 bytes	C	R	-	T	-	Date Time, date time

If the CO 46 is not written with the current date and time value, the keypad will not be able to perform the required checks. In this case, a special error code will be emitted on the diagnostic CO when the access is attempted (see section 3.1.5).

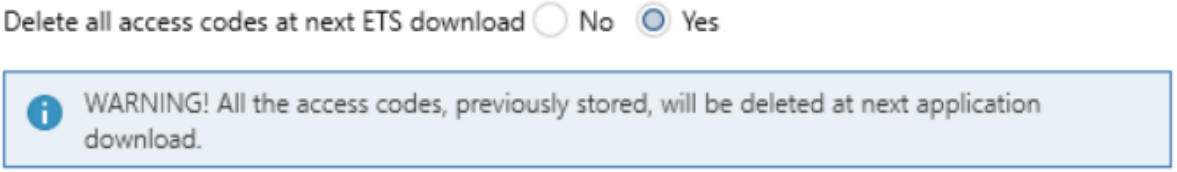
3.8.2 Number of digits in the code

It sets the number of digits that form the numeric access codes.



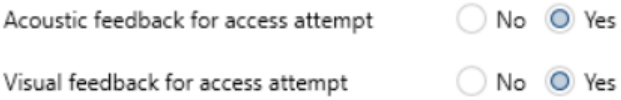
3.8.3 Delete all access codes at next ETS download

The keypad keeps all codes information saved in its internal memory. This parameter allows to set the download behaviour of the ETS application program; it is possible to keep the previously stored information or delete them. In case of deletion, a warning message pops up to warn of the danger of the operation.



3.8.4 Acoustic/Visual feedback for access attempt

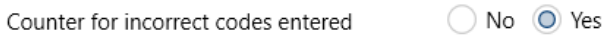
When the user enters a numeric code or approaches an RFID tag, the success of the access attempt can be signaled by the device with a sound (acoustic feedback) and with a flashing of the backlight (visual return) of the device base. With these parameters you can choose whether or not to enable the signals.



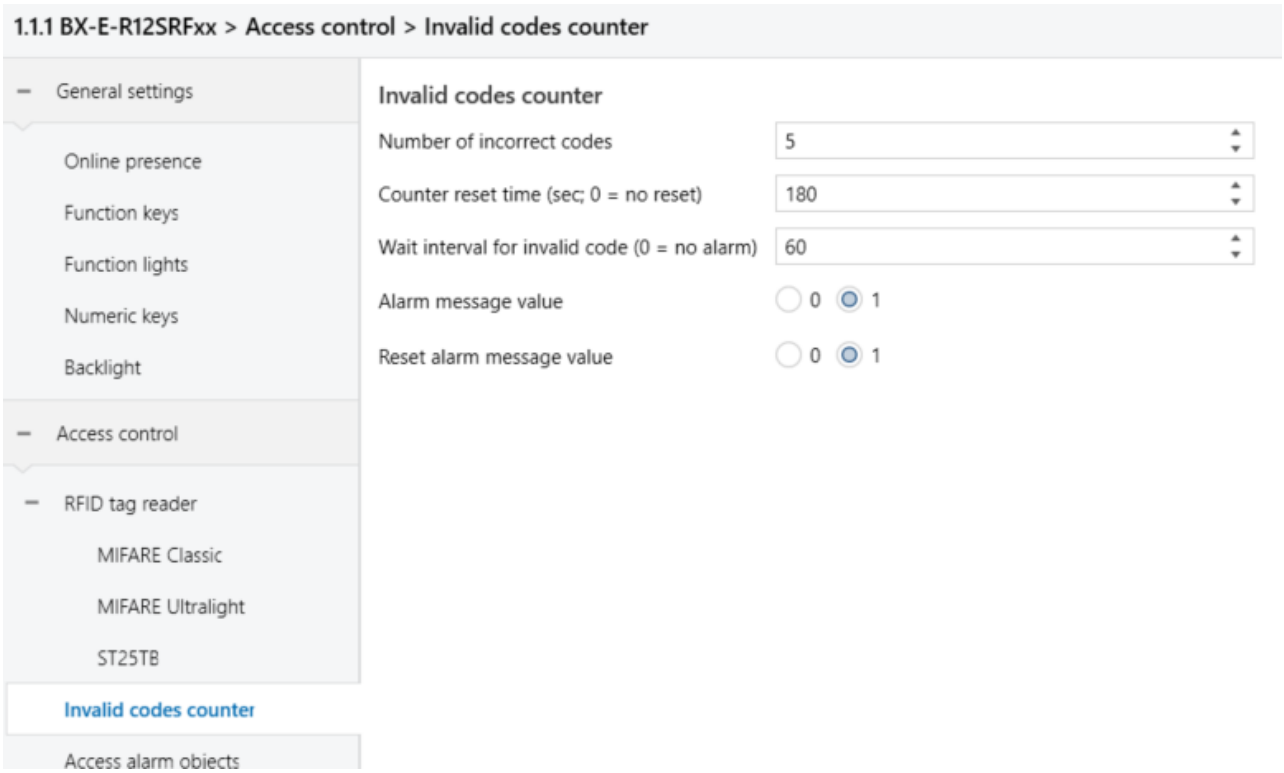
The sound and flashing are different depending on the outcome of the access.
With access denied, three short and rapid sounds and flashes are generated (0.2 sec).
With access allowed, a single sound and long interval flashing (1.5 sec) is generated.

3.8.5 Counter for incorrect codes entered

This function enhances security by limiting the number of incorrect access attempts.



This measure prevents the user from continuing to enter invalid access codes, hoping to find a valid one sooner or later. An alarm is reported through a communication object if the conditions defined by the parameters described below occur. The alarm can be cancelled with another communication object.
When enabled, additional configuration parameters and communication objects become available.



"Number of incorrect codes" is the number of invalid access attempts (by keypad or RFID tag) allowed before the alarm is reported. The device maintains an internal counter of the incorrect attempts made by the user.

"Counter reset time": after this specific interval of time (time starts from the last invalid attempt), the internal counter of the attempts is reset. This function prevents the alarm from being issued when attempts are made at a distance of time from each other. With the values of the parameters, indicated in figure, if the wrong attempt is performed at intervals of 4 minutes, the alarm will never be issued because the counter is reset every 3 minutes (180 sec).

If this parameter is set to zero, the counter is never reset. If only one incorrect code per day is entered, the alarm will be issued on the fifth day.

"Wait interval for valid code" from the insertion of the first incorrect code, the system waits for this specific time interval before triggering the alarm. Only the insertion of a correct code, within this time, avoids the emission of the alarm.
If this parameter is set to zero, the described control is not performed.

"Alarm message value" defines the CO value transmitted on the KNX bus to signal the alarm condition.
"Reset alarm message value" specifies the CO value required to cancel the alarm condition.

70	Codes	Alarm for incorrect codes entered	1 bit	C	R	W	T	-	1-bit, alarm
71	Codes	Reset incorrect codes alarm	1 bit	C	-	W	-	-	1-bit, reset

3.8.6 Access information description

Access management is based on a series of checks that the device operates before issuing the appropriate KNX messages enabling or denying the access. The information to be checked must be stored in advance in the device with the help of software tools that facilitate the sending and formatting of data. Supervision software running on a PC connected to the bus or smartphone application can take care of managing (saving, removing) the "blocks" of information relating to the codes.

Only if all the required checks are successful, access will be allowed by issuing appropriate messages on the bus. If the check fails, a different set of messages will be sent; in addition, a special error code will be issued on the diagnostic CO (see section 3.1.5) describing the reason for the failure to authenticate.

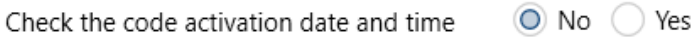
The access checks are performed on the following information

3.8.6.1 Access code value

The value entered via the keypad or read from an RFID tag must be present in the internal memory of the keypad. The length of the access code (4 or 6 digits) is checked: if the code length is set to 4 digits (see section 3.7.2), 6-digit codes are not validated, even if the first 4 digits match those of a stored code.

3.8.6.2 Code activation date and time

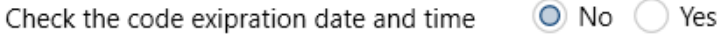
This check is performed only if enabled by the corresponding parameter.



The check is successful if the activation date and time associated with the entered code is earlier than the current date and time.

3.8.6.3 Code expiry date and time

This check is performed only if enabled by the corresponding parameter.



The check is successful if the expiry date and time associated with the entered code is later than the current date and time.

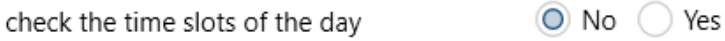
3.8.6.4 Days of the week

This check is performed only if enabled by the corresponding parameter.

The check is successful if the code is enabled for the day of the week on which the access attempt is made.

3.8.6.5 Time slots

This check is performed only if enabled by the corresponding parameter.

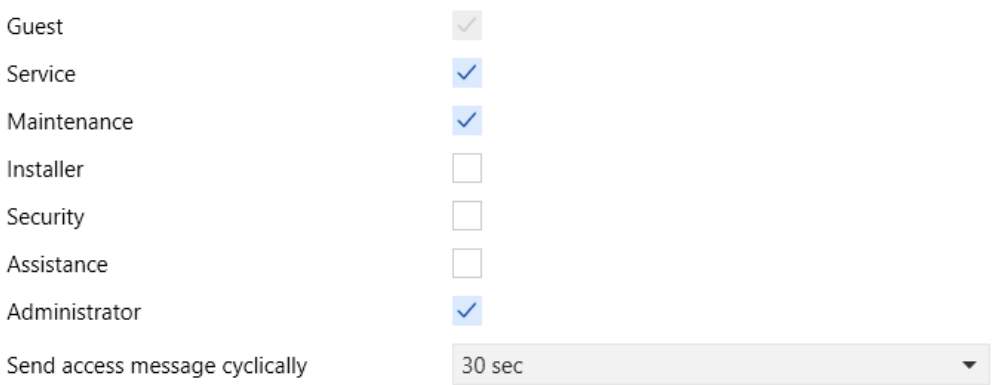


It is possible to specify the time ranges during the day for which an access code is valid or invalid.

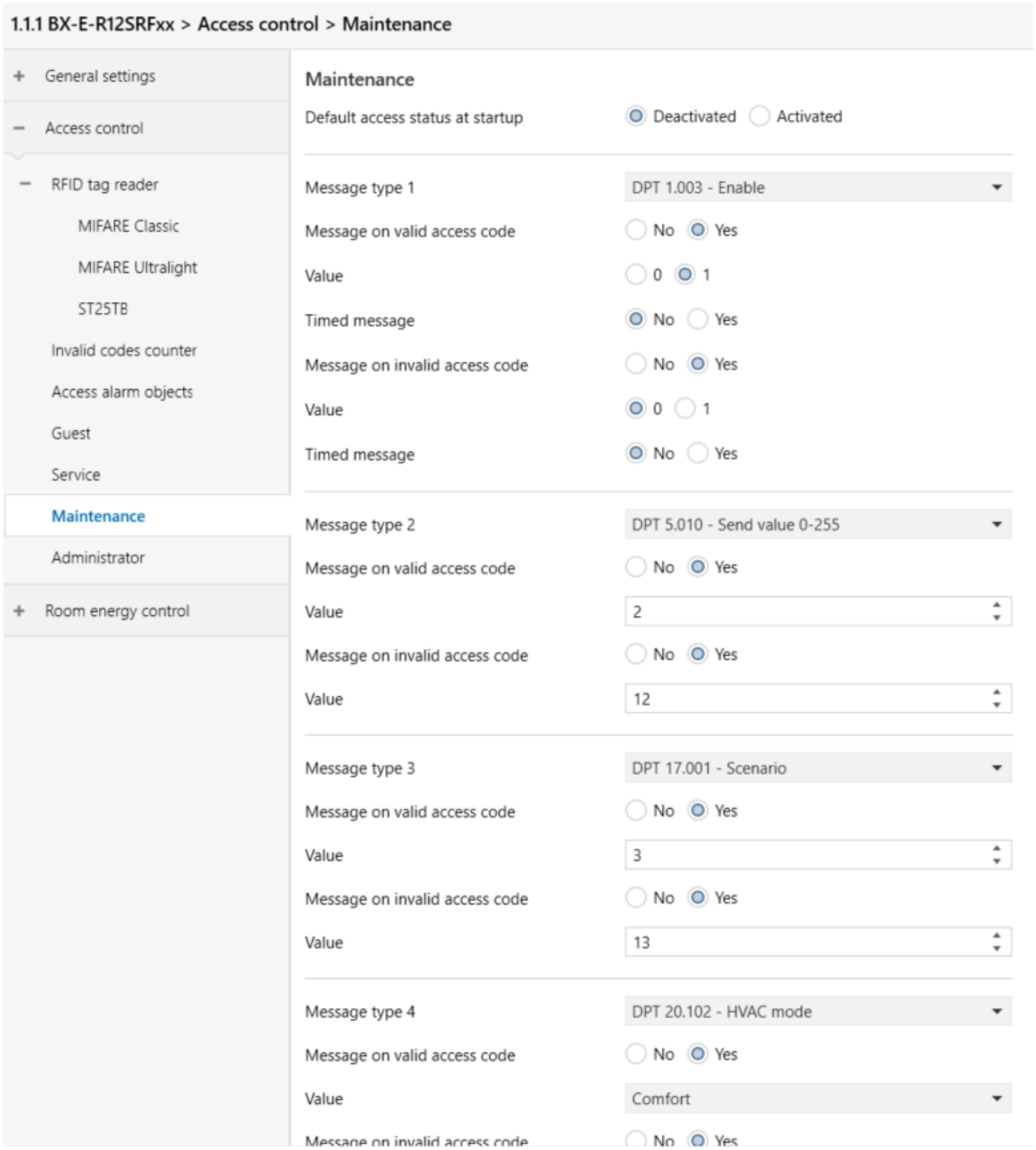
3.8.6.6 User type

The access code information block also contains the user type associated with the code. There are 7 user types, of which 6 are optional. The “Guest” user type is always present.

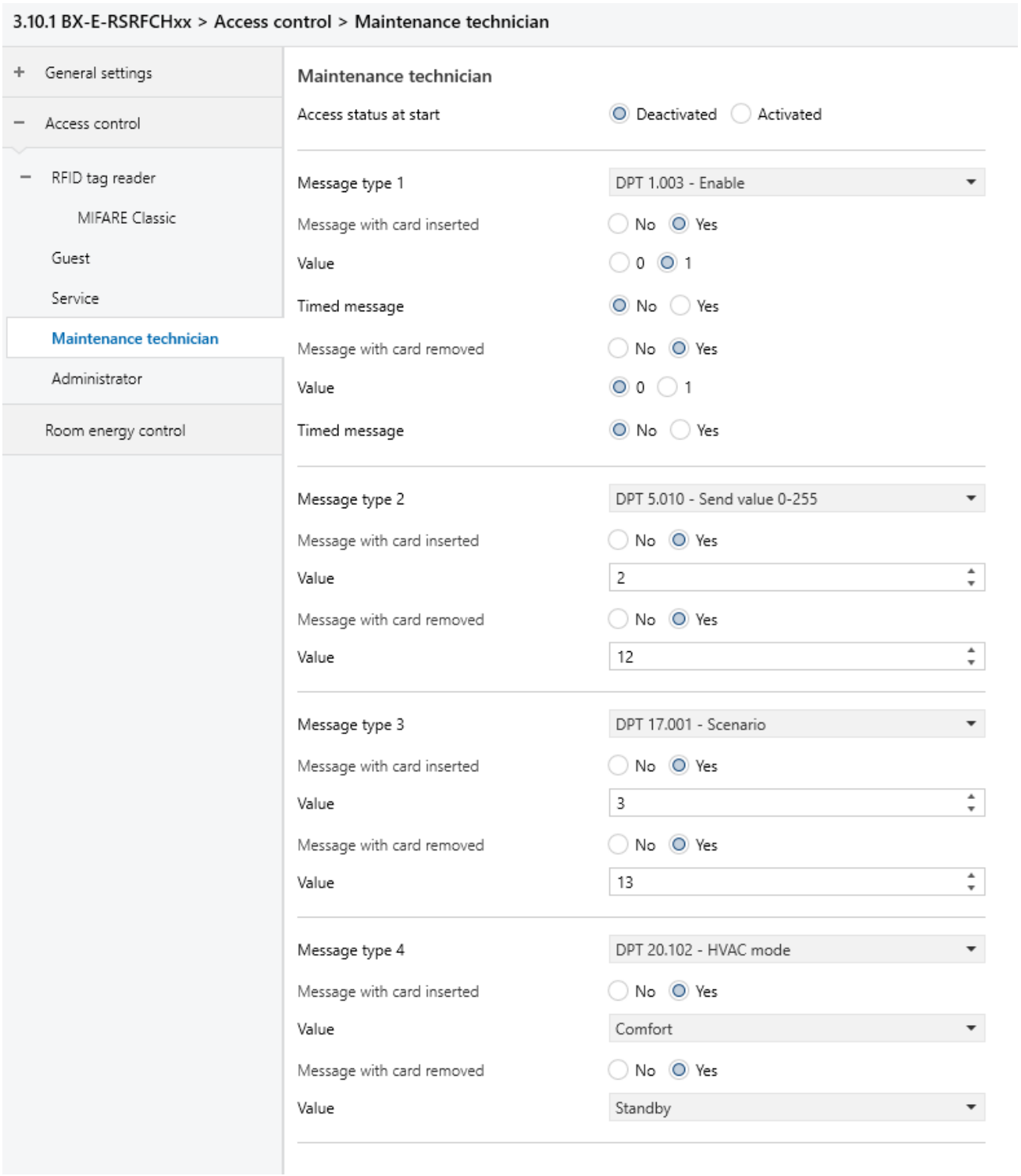
Different user types performing an access attempt, correspond to different sets of KNX messages transmitted on the bus when access is granted.



If the parameter “Send access message cyclically” is set to a value other than “No”, the KNX messages of the last access attempt will be transmitted cyclically on the bus; all communication objects configured on the page of the user who attempted access will be periodically re-sent on the KNX bus.
For each user type enabled by the parameter, a dedicated configuration sub-page and a dedicated set of communication objects are available.
The access state at device start-up can be selected using the “Access state at start-up” parameter. At power-up, the device transmits the messages corresponding to the selected state.
For each user type, up to 4 communication objects can be configured, which may be sent with different values depending on whether access is enabled or inhibited. In case of an access attempt with an invalid code (i.e. not present in the device memory), the messages configured for the “Guest” user (always enabled) will be sent, using the values defined by the “Invalid access code message” parameters.
In the case of the BX-E-RSRFxx product, if configured as “Card holder”, this behaviour is different: no message equivalent to the one used in other products is generated for an invalid code, as the “Invalid access code message” is replaced by the “Card removed message”. The access error can still be detected via the group object related to the access attempt and/or via the system diagnostic message.
Messages can be of different types (“Message type X”); the 1-bit type (“DPT1.003 – Enable”) also supports timed message handling.
Output messages can be differentiated depending on whether the entered code is valid or not (“Valid / Invalid access code message”). In the case of the BX-E-RSRFxx product, , if configured as “Card holder”, this setting is renamed as “Card inserted / removed message”.



BX-E-R12SRFxx, BX-E-R12Sxx and BX-E-RSRFxx (RFID Reader mode)

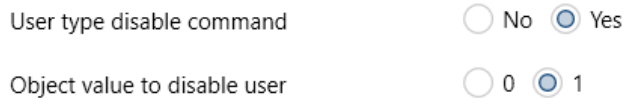


BX-E-RSRFxx (Card holder mode)

Below is an example of communication objects related to output commands for the “Maintenance” user type.

88	Maintenance	Out 1 - DPT 1.003 - Enable	1 bit	C	R	-	T	-	1-bit, enable
89	Maintenance	Out 2 - DPT 5.010 - Send value 0-255	1 byte	C	R	-	T	-	8-bit unsigned value, counter pulses (0..255)
90	Maintenance	Out 3 - DPT 17.001 - Scenario	1 byte	C	R	-	T	-	scene number, scene number
91	Maintenance	Out 4 - DPT 20.102 - HVAC Mode	1 byte	C	R	-	T	-	1-byte, HVAC mode

3.8.6.7 User type disable command



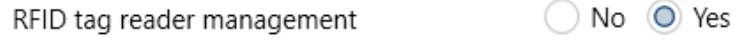
This parameter enables a pair of communication objects for each user type.
These communication objects allow the user to be enabled or disabled and return the corresponding status. The “Object value to disable user” parameter specifies the value to be written to the “Set…” communication object in order to disable the user.

108	Guest	Set disable user type	1 bit	C	-	W	-	-	1-bit, enable
109	Guest	User type disable status	1 bit	C	R	-	T	-	1-bit, enable
110	Service	Set disable user type	1 bit	C	-	W	-	-	1-bit, enable
111	Service	User type disable status	1 bit	C	R	-	T	-	1-bit, enable
112	Maintenance	Set disable user type	1 bit	C	-	W	-	-	1-bit, enable
113	Maintenance	User type disable status	1 bit	C	R	-	T	-	1-bit, enable
120	Administrator	Set disable user type	1 bit	C	-	W	-	-	1-bit, enable
121	Administrator	User type disable status	1 bit	C	R	-	T	-	1-bit, enable

If a valid code is entered but it belongs to a disabled user, the access attempt will fail.

3.8.6.8 RFID tag reader management

For device model BX-E-R12SRFxx, which supports code entry both via keypad and RFID tag, it is possible to disable the entire RFID section by setting this parameter to “No”.



Refer to section 3.7.8 for the description of the parameters related to the RFID reader function.

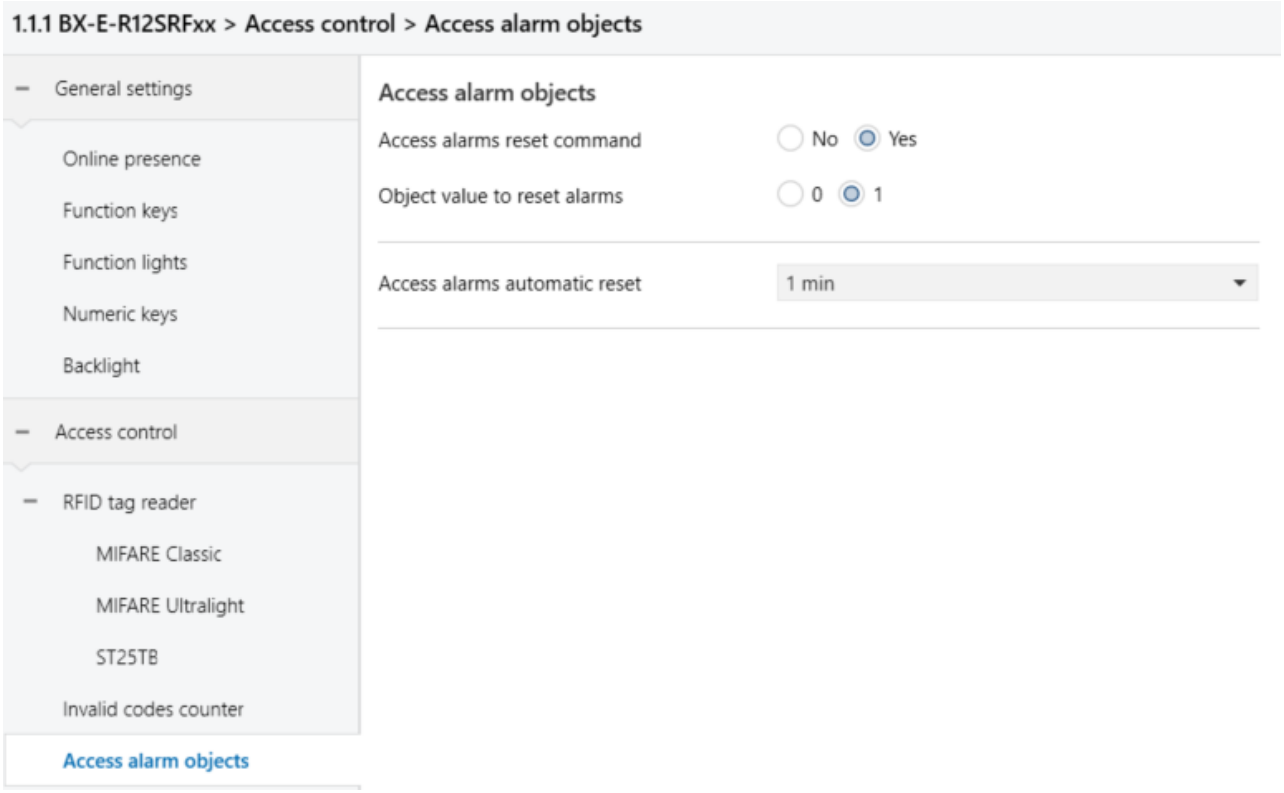
3.8.6.9 Code insertion origin check

If the RFID section is enabled (see section 3.7.6.8), it is also possible to enable separate management of access codes, distinguishing between codes that can be entered only via keypad and codes that are valid only via RFID tag.

If this parameter is set to “Yes”, some communication objects are duplicated to allow separate handling (CO 50–51, 58–59, 75–76, 77–78).

3.8.6.10 Oggetti di allarme per tentativo di accesso

This parameter enables a dedicated configuration sub-page and several 1-bit communication objects for managing error conditions that may occur during an access attempt.



150	Alarms	Reset all	1 bit	C	-	W	-	-	1-bit, reset
151	Alarms	System date and time not valid	1 bit	C	R	W	T	-	1-bit, alarm
152	Alarms	Invalid access code	1 bit	C	R	W	T	-	1-bit, alarm
157	Alarms	User type disabled	1 bit	C	R	W	T	-	1-bit, alarm
158	Alarms	Wrong plant identifier	1 bit	C	R	W	T	-	1-bit, alarm
159	Alarms	Card read error	1 bit	C	R	W	T	-	1-bit, alarm

By writing to CO 150 the value defined by the parameter “Object value to reset alarm”, it is possible to reset the alarm communication objects (CO 151, 152, …). Alarm messages are transmitted on the KNX bus with value 1 when active and value 0 when inactive.

3.8.7 Access control communication objects

In addition to the communication objects that depend on the configuration of the parameters described above, there are also CO that are always available for access control management.

3.8.7.1 Save/Delete access code information objects

The communication objects dedicated to saving and deleting access code data blocks are described below.

50	Codes	Store/delete request (keypad)	14 bytes	C	-	W	-	-	character string, Character String (ISO 8859-1)
51	Codes	Store/delete request (rfid)	14 bytes	C	-	W	-	-	character string, Character String (ISO 8859-1)
53	Codes	Delete request	14 bytes	C	-	W	-	-	character string, Character String (ISO 8859-1)
55	Codes	Delete request	4 bytes	C	-	W	-	-	entrance access, entrance access

Communication objects 50 and 51 (14-byte non-standard KNX format) are used both for saving and deleting access code information. If numeric codes entered via keypad and RFID tag codes needs to be managed separately, the parameter “Code insertion origin check” (see section 3.7.6.9) must be enabled. In this case, the save/delete objects (as well as other CO described later) are separated and identified by the text in brackets “keypad” or “rfid”.
Communication object 53 (14-byte non-standard KNX format) is dedicated exclusively to removing an access code data block from the internal memory of the keypad. To write this object, it is sufficient to fill in only the numeric code field, ignoring all other fields.
Communication object 55 is also dedicated to removing a code block, in this case it uses a standard KNX DPT (DPT 15.000).

Refer to **Appendix B** for the description and data format of the 14-byte non-standard DPTs.

3.8.7.2 Save/Delete request result objects

Writing to the communication objects described above generates a response from the device, allowing verification of the outcome of the requested operation.
This is particularly useful for supervisory software managing access code lists and handling the storage and deletion of codes within the keypad. These communication objects use DPT 15.000 format.

58	Codes	Store/delete request result (keypad)	4 bytes	C	R	-	T	-	entrance access, entrance access
59	Codes	Store/delete request result (rfid)	4 bytes	C	R	-	T	-	entrance access, entrance access

If access code information is differentiated between keypad and RFID (see section 3.7.6.9), the response objects are also differentiated; otherwise, only one response object is available (CO 58).

The response contains:

- in the first 3 bytes (2 bytes if a 4-digit code is used): the access code involved in the operation.

If a save operation is attempted:

- successful save → flags D = 1 and P = 1
- failed save → flag E = 1

If a delete operation is attempted:

- successful deletion → flag P = 1
- failed deletion → flag E = 1

Below is the description of DPT 15.000 as defined in the KNX standard documentation.

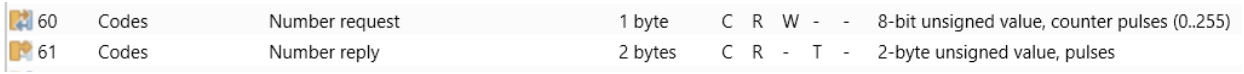
Format:	4 octets: $U_4U_4U_4U_4U_4U_4B_4N_4$
octet nr.	4 MSB | 3 | 2 | 1 LSB
field names	D_6 D_5 | D_4 D_3 | D_2 D_1 | E P D C Index
encoding	U U U U U U U U | U U U U U U U U | U U U U U U U U | b b b b N N N N
Encoding:	$D_6, D_5, D_4, D_3, D_2, D_1$: binary encoded value N: binary encoded value E, P, D, C: See below
Unit:	Not applicable.
Resol.:	Not applicable.
PDT:	PDT_GENERIC_04

Datapoint Types		
ID:	Name:	Use:
15.000	DPT_Access_Data	FB

Field	Description	Encoding	Range
$D_6, D_5, D_4, D_3, D_2, D_1$	digit x (1…6) of access identification code. Only a card or key number should be used. System number, version number, country code, etc are not necessary. Ciphered access information code should be possible in principle. If 24 bits are not necessary, the most significant positions shall be set to zero.	Values binary encoded.	[0 … 9]
E	Detection error	0 = no error 1 = reading of access information code was not successful).	{0,1}
P	Permission (informs about the access decision made by the controlling device)	0 = not accepted 1 = accepted	{0,1}
D	Read direction (e.g. of badge) If not used (e.g. electronic key) set to zero.	0 = left to right 1 = right to left	{0,1}
C	Encryption of access information.	0 = no 1 = yes	{0,1}
Index	Index of access identification code (future use)	Value binary encoded.	[0 … 15]

DPT 15.000 description

3.8.7.3 Number request/reply objects



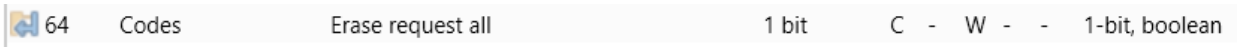
60	Codes	Number request	1 byte	C	R	W	-	-	8-bit unsigned value, counter pulses (0..255)
61	Codes	Number reply	2 bytes	C	R	-	T	-	2-byte unsigned value, pulses

CO 60 is a 1-byte KNX message used to request information regarding the number of managed access codes.
The device replies to this request on CO 61, which has a size of 2 bytes.
The supported write/read values are:

- CO 60 = 1 ⟷ CO 61 = number of access codes currently stored in memory
- CO 60 = 2 ⟷ CO 61 = number of access codes still available for storage
- CO 60 = 3 ⟷ CO 61 = total number of managed codes (approximately 1000)

3.8.7.4 Erase request all

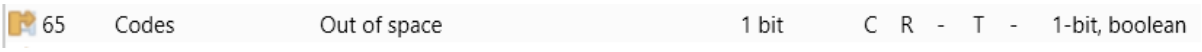
When written with value 1, this communication object forces the deletion of all access code data blocks stored in the keypad.



64	Codes	Erase request all	1 bit	C	-	W	-	-	1-bit, boolean

3.8.7.5 Out of space

This communication object signals the memory full status for access code information. If the device transmits value 1 on this object, no further access codes can be stored in internal memory.
This object may be transmitted as a result of save or delete commands and is always transmitted at device power-up and at the end of the ETS application download.



65	Codes	Out of space	1 bit	C	R	-	T	-	1-bit, boolean

After storing the last available access code information, value 1 is sent to indicate that no more memory is available.
As soon as one code or the entire memory is deleted, restoring a condition in which almost one code information can be stored, value 0 is transmitted on this object.

3.8.7.6 Request by index

CO 68 is a 2-byte message used to request information from the keypad regarding a specific memory position in the access code information list.
The value written to this object must be between 0 (index of the first valid position), and the maximum number of storable codes minus one.
The response is transmitted on CO 69.

68	Codes	Request by index	2 bytes	C	R	W	-	-	2-byte unsigned value, pulses

3.8.7.7 Reply by index

This communication object represents the response to CO 68, using DPT 15.000 format.
If an access code exists, at the requested memory location, the first 3 bytes (2 bytes if a 4-digit code is used) contain the code value and the flags D = 1 and P = 1 are set.
If no access code exists at that location the first 3 bytes are set to 0 and flag E = 1 is set.

69	Codes	Reply by index	4 bytes	C	R	-	T	-	entrance access, entrance access

3.8.7.8 Simulation (keypad, rfid)

75	Access	Simulation (keypad)	4 bytes	C	R	W	-	-	entrance access, entrance access
76	Access	Simulation (rfid)	4 bytes	C	R	W	-	-	entrance access, entrance access

These communication objects allow an access code to be sent from the KNX bus in order to simulate an access attempt.
Writing to these objects simulates the physical action of entering digits on the keypad or presenting an RFID tag near the device.

The data format is DPT 15.000:

- the first 3 bytes (2 bytes for 4-digit codes) contain the access code
- the fourth byte must have flag P = 1 set

The objects are differentiated for keypad and RFID if the parameter “Code insertion origin check” is set to “Yes”.

3.8.7.9 Access try result (keypad, rfid)

77	Access	Try result (keypad)	4 bytes	C	R	-	T	-	entrance access, entrance access
78	Access	Try result (rfid)	4 bytes	C	R	-	T	-	entrance access, entrance access

Whenever an access attempt is made by entering a code on the keypad or presenting an RFID tag (also by writing to CO 75 or CO 76), these communication objects will report the result of the operation.

The data format is DPT 15.000:

- the first 3 bytes contain the access code used for the attempt
- if access is successful, flag P = 1 is set
- if access fails, all flags are set to 0

3.8.8 RFID tag reader

On this page of the ETS library, the configuration of the RFID tag reading section is managed. Presenting a RFID tag near the device represents an alternative to typing the numeric code on the keyboard.

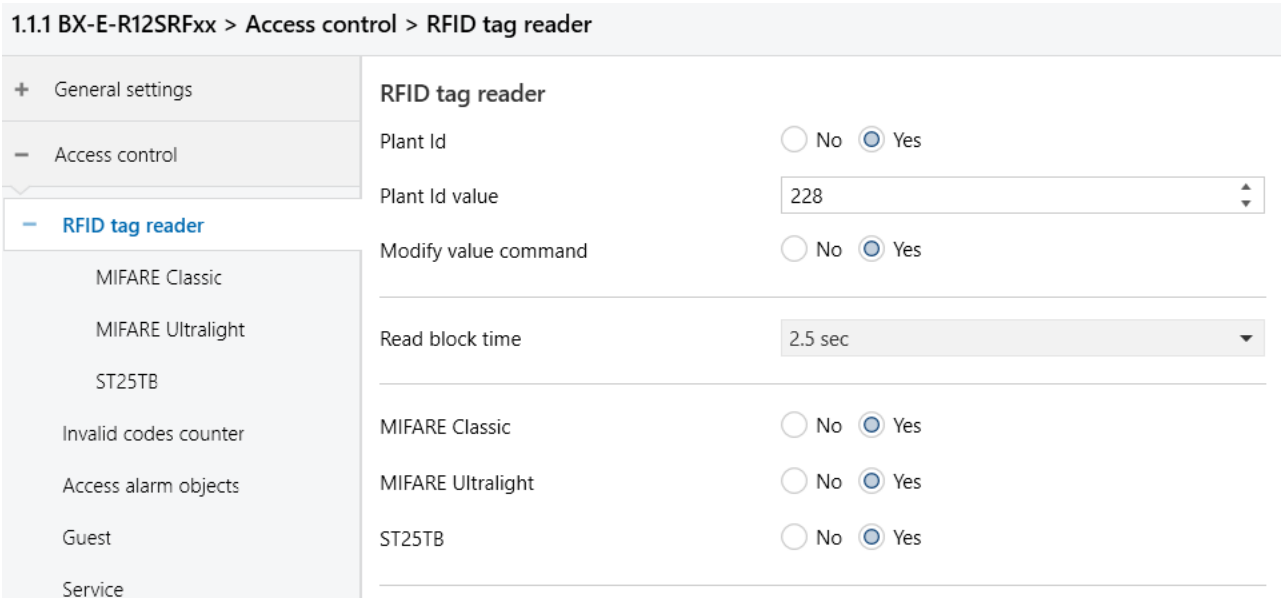
The RFID function is not present in BX-E-R12Sxx device model.

The RFID reader requires connection to an auxiliary power supply. See **Appendix E** for electrical specifications.

For this access method to work properly, it is important that the RFID tag is approached and physically placed on the "RFID" symbol printed on the keyboard cover.

RFID cards or tags must be programmed following a precise scheme; the data to be programmed in the tag memory are the numerical access code and possibly the "Plant ID". Please refer to **Appendix C** for RFID tag programming specifications.

Parameters of RFID tag reader section



3.8.8.1 Plant ID

The parameter enables the management of the plant identifier functionality.
The identifier has meaning only when access is made by RFID tag and represents a second level of security as both the numerical code and the plant id must be stored in the RFID support used for access. Only if both are correct the access can be granted.
In the "Plant Id value" parameter, a 2-byte numeric value (from 0 to 65535) is set to identify the system. If the rfid tag has a valid access code in memory but a different plant id from the one set in the "Plant Id value" parameter, then the access will be precluded.
With the parameter "Modify value command" set to "Yes", 2 communication objects are available with which it is possible to overwrite the value set in the parameter by dynamically changing the plant id (GO 161) and check that the change has been successfully made (GO162).

3.8.8.2 Read block time

This parameter defines the minimum time interval between two RFID tag readings.
After an access attempt by presenting an RFID card or tag to the keypad, it is necessary to wait at least this interval before attempting a new access by presenting the tag again. If this waiting time is not respected, the RFID tag is ignored.

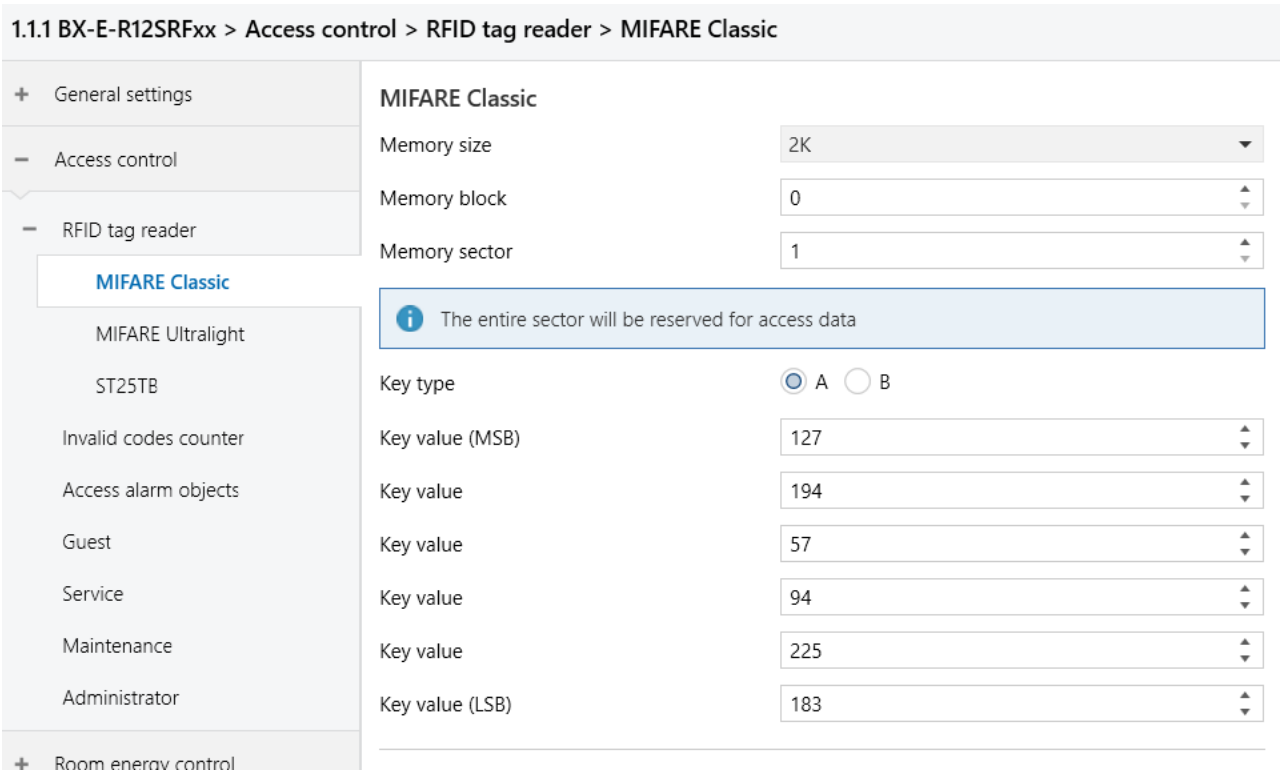
3.8.8.3 RFID tag type

With these parameters, the system is enabled to manage different types of RFID transponders. A specific parameter sub-page will be made available for each enabled type.

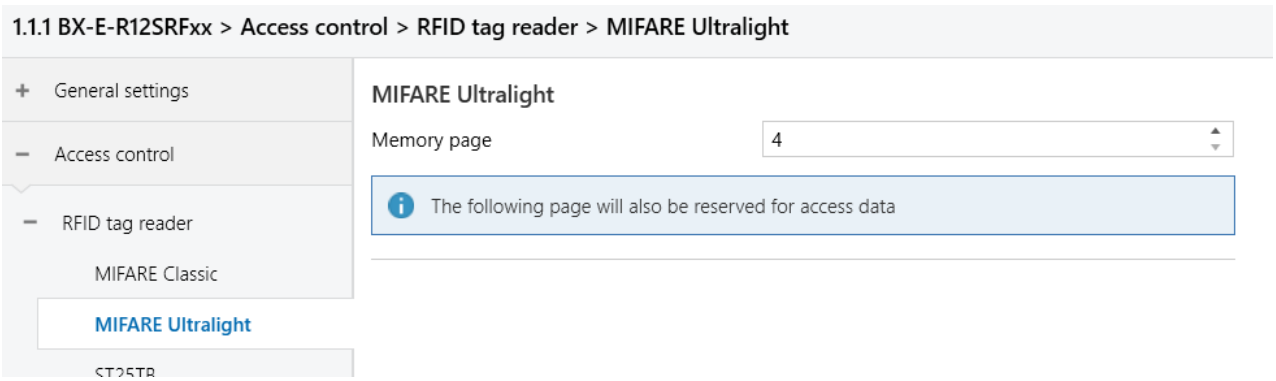
The supported RFID technologies are:

- MIFARE Classic
- MIFARE Ultralight
- ST25TB

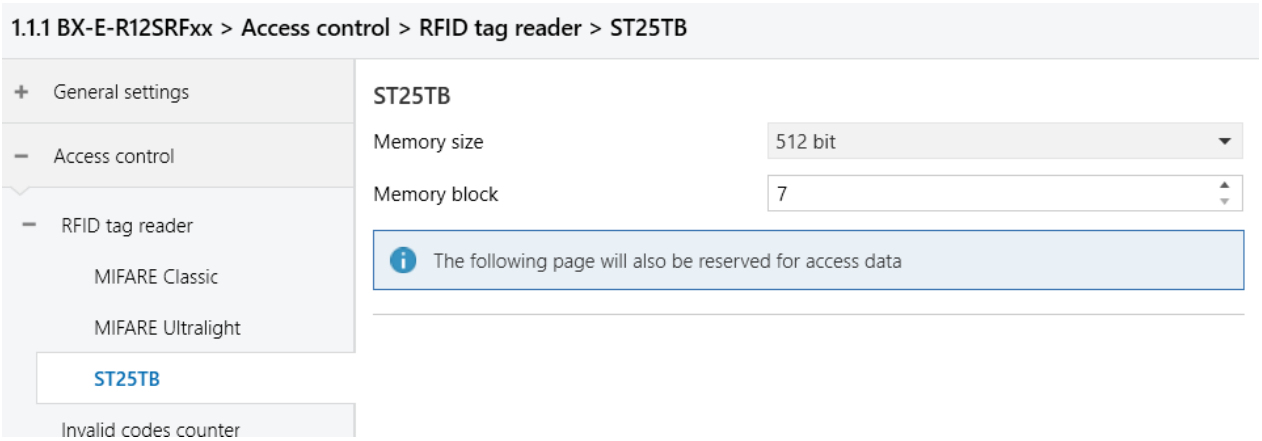
MIFARE Classic



MIFARE Ultralight



ST25TB



For each tag type, specific parameters are provided to adapt the system to the underlying tag technology. Depending on the internal structure of the tag, it is possible to:

- select the memory size
- define the portion of memory to be used for access control application data (the remaining memory areas will be available for other applications, i.e. payment systems)
- configure security key-based encoding, where supported by the selected technology

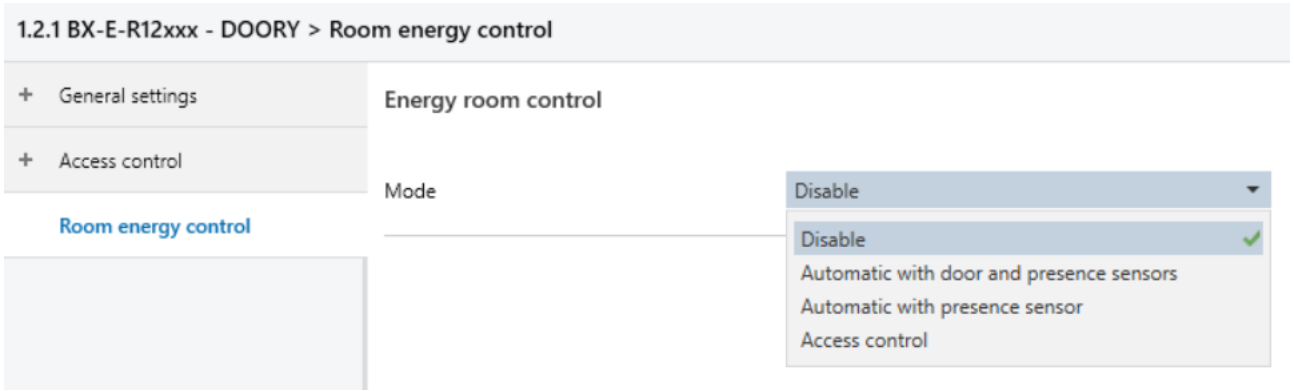
Refer to **Appendix C** for the technical specifications of the supported RFID tags.

3.9 Room energy control

The keypad provides the management of the automatic detachment or connection of the room energy (mains supply).
This functionality is normally used in hotel rooms and accommodation facilities. The function can be configured in different modes, depending on the installation needs. The result of signal processing and the integration with other configuration parameters allows you to control an actuator (typically relay) that automatically breaks/connects the energy. Further, it is possible to send other commands for activating/deactivating room utilities, scenario selection, HVAC mode, temperature control.

3.9.1 Mode

Parameterization depends on the selected operating mode

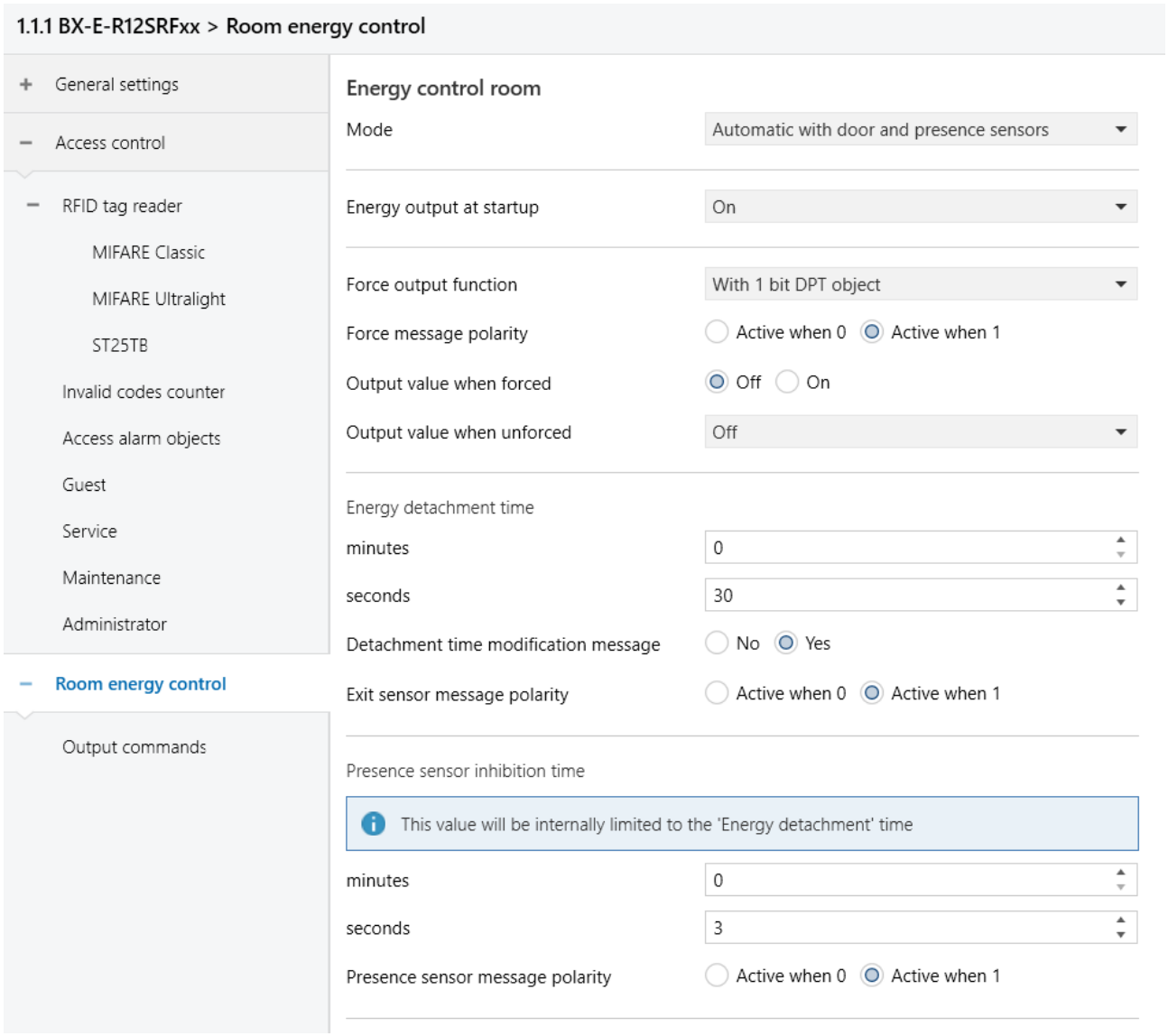


The three possibilities are:
1 – Automatic with door and presence sensors
2 – Automatic with presence sensor
3 – Access control

Mode 1 – Automatic with door and presence sensors

It involves the use of a sensor or microswitch that signals the closing of the room door (i.e. the guest's exit from the room) and a PIR sensor that detects the actual presence of people in the room (the guest enters or is present in the room).
When the system detects the guest's exit from the room and does not detect any presence in it, it starts a timer at the end of which it will disconnect the energy.
If a presence is detected in the room, during the timing, the process is interrupted and the energy will be maintained.
With energy already detached, detection of a presence will trigger an energy hang-up command.
Note that the function logic works by considering the signal edges of the door and PIR sensors; the messages related to the output sensor and the presence sensor must first

be activated and then return to the resting state to obtain a proper functioning of the logic.



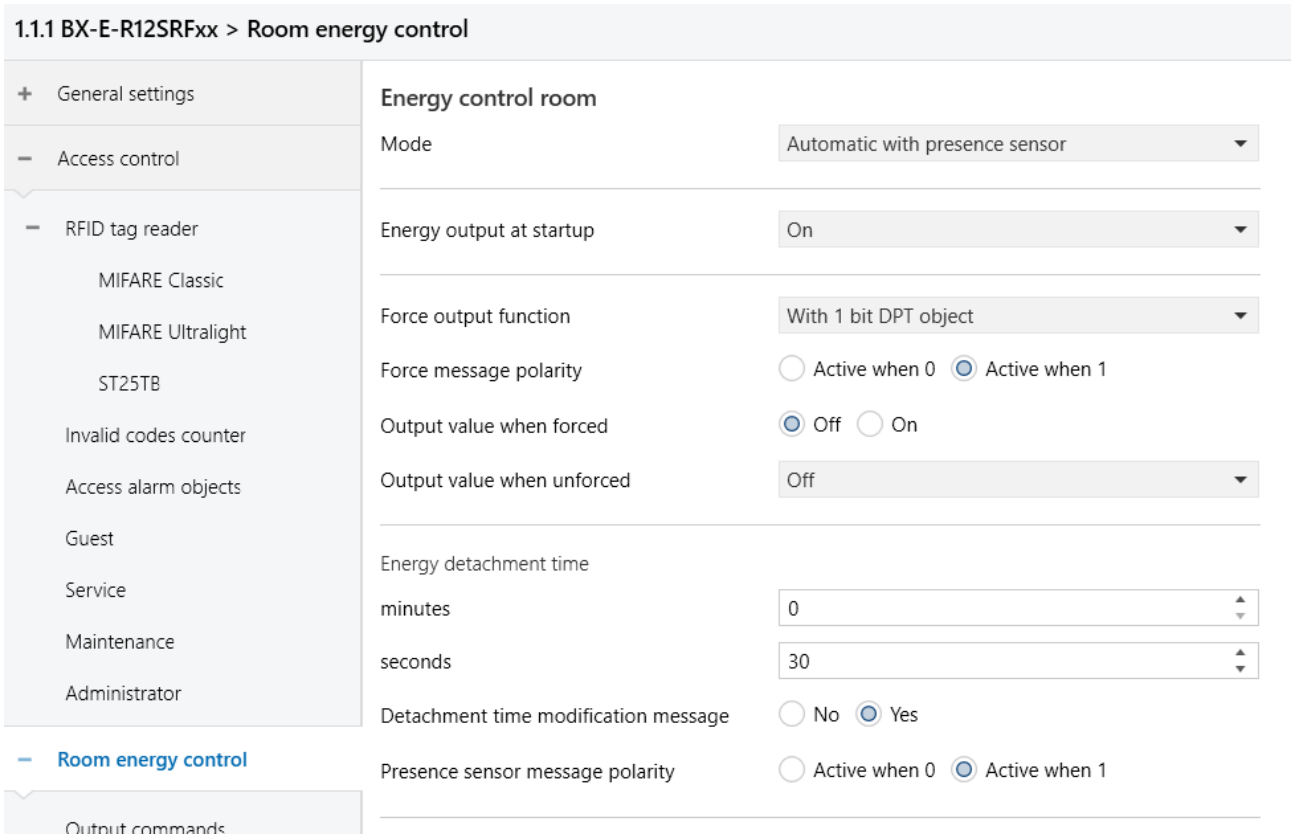
Mode 2 – Automatic with presence sensor

It involves the use of a PIR sensor that detects the presence of people in the room. When it doesn't detect a presence in the room, it starts a timer at the end of which the device will send the mains supply disconnection command.

If a presence is detected in the room, during the timing, the process is interrupted and the energy will be maintained.

With energy already detached, detection of a presence will trigger an energy hang-up command.

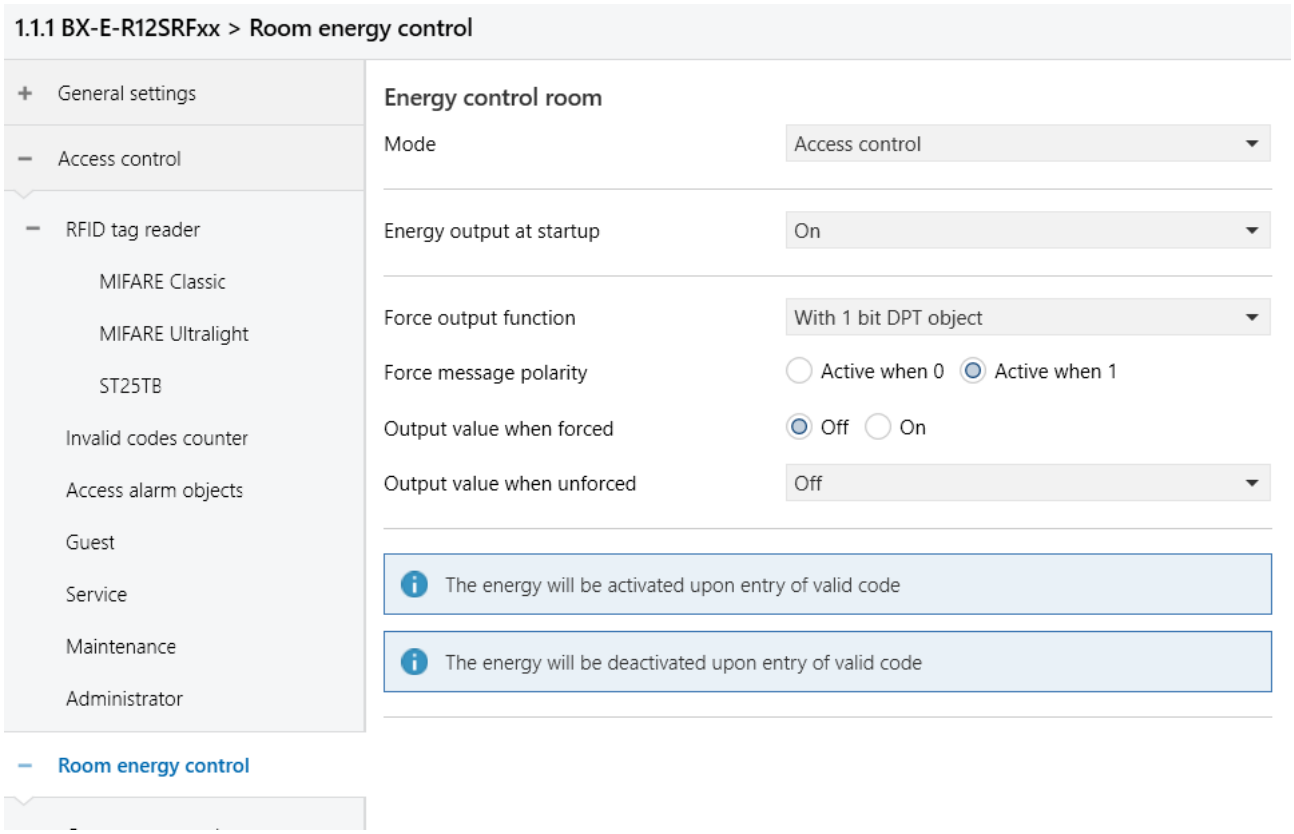
Note that the management works by considering the PIR sensor signal edge; the sensor-related messages must first be activated and then return to a resting state to achieve proper logic operation.



Mode 3 – Access control

It does not need signals from external sensors but the release/connect of the room mains supply depends on the access codes management; specifically there are the following two conditions:

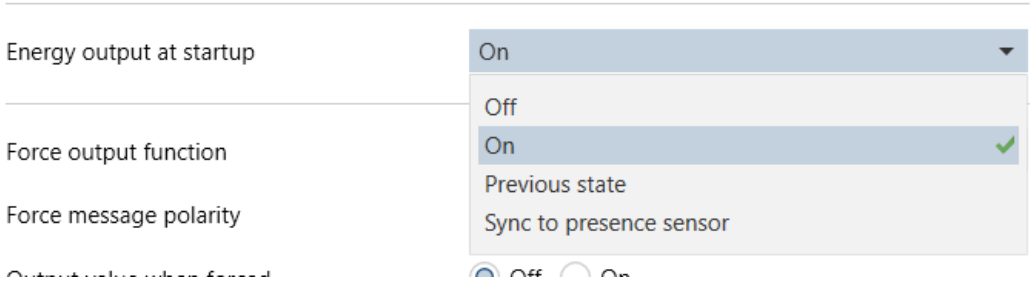
- Input of a valid access code by the user = power activation
- Erasing valid access code from memory = power off



Below the description of the parameters, some will not be significant in certain modes.

3.9.2 Energy output at startup

When the device is switched on or the application is downloaded from the ETS software, the energy status is defined by sending messages configured on the "Output commands" page to the KNX bus. The state of the energy can be selected by this parameter:



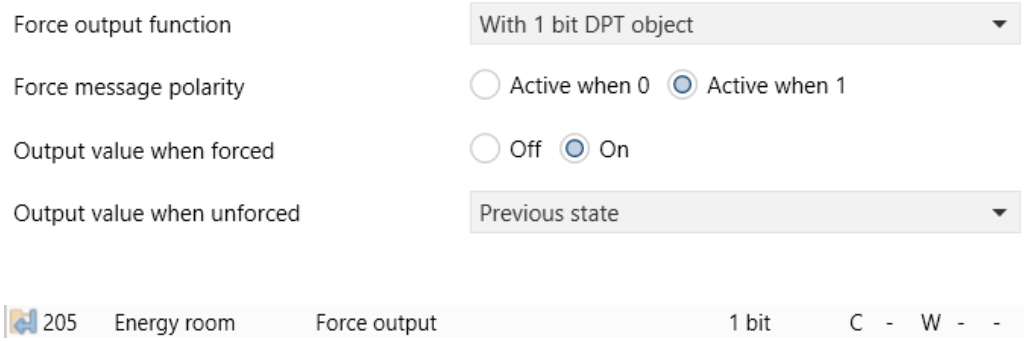
- "Off": power off, sending deactivation messages.
- "On": active energy, sending activation messages.
- "Previous state": energy as before shutdown or ETS download.

- "Sync to presence sensor": the bus requires to read the PIR sensor status; the energy is set according to this. This option is not provided in the "Access control" mode.

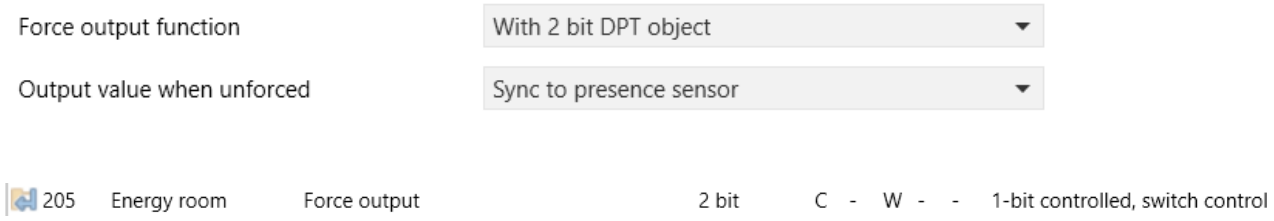
3.9.3 Force output function

This parameter enables the availability of a communication object that allows the energy state to be forced on or off, overriding the normal logic and sensor inputs; the datapoint type of the forcing object can be 1-bit, or 2-bit.
The available parameters adapt automatically depending on the selected datapoint type.

1-bit

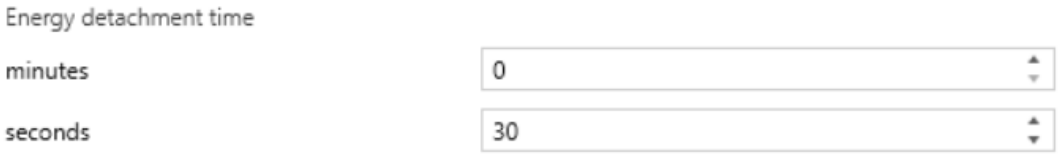


2-bit



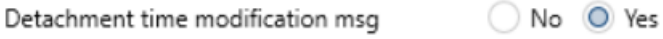
3.9.4 Energy detachment time

In mode 1 - Automatic with door and presence sensors, it represents the time interval between the user's exit (door-switch event) and the energy detachment command.
In mode 2 - Automatic with presence sensor, it represents the interval of time of waiting between the detection of the absence of the guest (PIR not engaged) and the energy detachment command.



3.9.5 Detachment time modification message

It enables the presence of modification and feedback communication objects to manage and override the “Energy detachment time” value.



Two CO will be available if the parameter is set to “Yes”

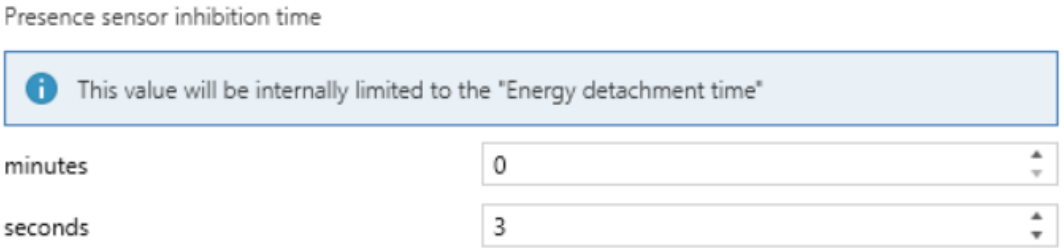
206	Energy room	Set detachment time	2 bytes	C	-	W	-	-	2-byte unsigned value, time (s)
207	Energy room	Detachment time status	2 bytes	C	R	-	T	-	2-byte unsigned value, time (s)

3.9.6 Exit sensor message polarity

Only available in mode 1 - Automatic with door and presence sensors, it defines the active edge of the sensor signal that detects the opening and closing of the room door.

3.9.7 Presence sensor inhibition time

Only available in mode 1 - Automatic with door and presence sensors. The time interval in which the system ignores the possible activation of the presence sensor.



When the guest leaves the room, it starts the timer for the energy detachment; also the time inhibition is counted starting from the user’s exit event.
During this interval, any activation of the PIR presence sensor will not be considered and then the process will proceed by detaching the energy at the end of the disconnect timer.
The PIR activations that will ensure that the energy is not detached are the ones that occur after the inhibition interval and before the disconnection timer expires.

3.9.8 Presence sensor message polarity

Available in mode 1 and 2, it defines the active edge of the PIR sensor signal that detects the presence of a guest in the room.

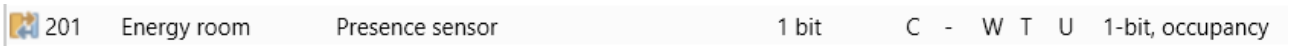
3.9.9 Sensor communication objects

Depending on the mode of operation, it may be present or not.

The CO “Exit sensor”, an input available only in mode 1, must be written with the status of the sensor that detects the opening and closing of the room door.

200	Energy room	Exit sensor	1 bit	C	-	W	-	-	1-bit, window/door

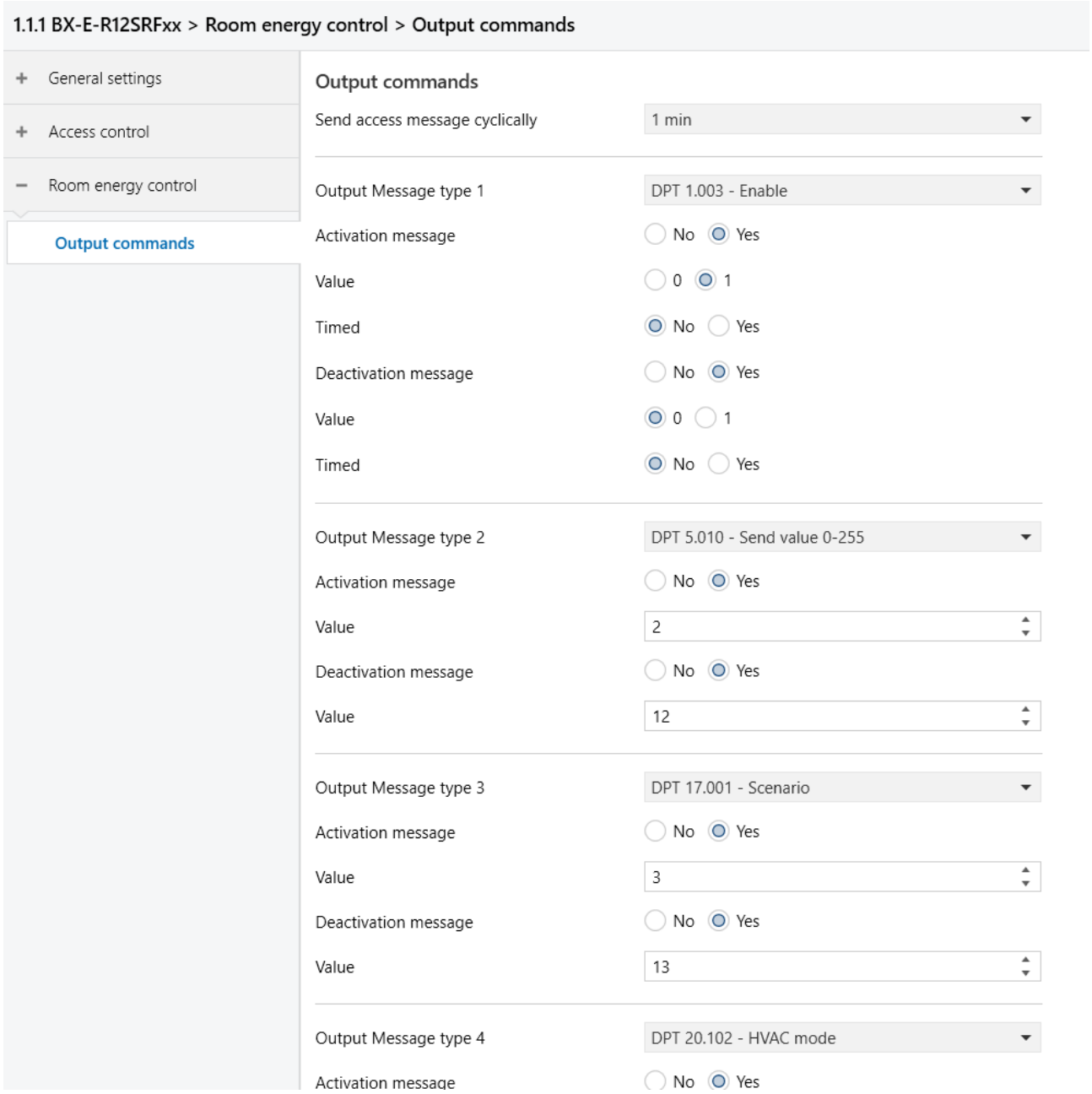
The CO “Presence sensor”, an input available only in mode 1 and 2, must be written with the status of the sensor that detects the presence of people in the room.



201	Energy room	Presence sensor	1 bit	C	-	W	T	U	1-bit, occupancy

3.9.10 Output commands

All power management modes have a parameter page that defines messages and communication objects. The processing of the events and signals described for the three modes are translated by the device into KNX bus messages that will control the energy through actuator devices.



Each power activation and deactivation event can trigger up to 4 messages on the bus simultaneously.
Messages can be of different types ("Output message type X"); the datapoint 1 bit ("DPT1.003 - Enable") also provides time management of the message.
The output messages are differentiated depending on whether the energy is connected or detached ("Activation message", "Deactivation message").
By setting "Send access message cyclically", it is possible to periodically send the result of the last result of the management logic on the KNX bus.

Here is an example of CO for 4 output commands:

210	Energy room	Out 1 - DPT 1.003 - Enable	1 bit	C	R	-	T	-	1-bit, enable
215	Energy room	Out 2 - DPT 5.010 - Send value 0-255	1 byte	C	R	-	T	-	8-bit unsigned value, counter pulses (0..255)
216	Energy room	Out 3 - DPT 17.001 - Scenario	1 byte	C	R	-	T	-	scene number, scene number
217	Energy room	Out 4 - DPT 20.102 - HVAC Mode	1 byte	C	R	-	T	-	1-byte, HVAC mode

Appendix A

Non-standard communication object 1 byte

Non-standard communication object format and description for diagnostic message (CO 6, 1 byte)

Error code list

Error code	Description
0x00	**No error** No error occured.
0x01	**System datetime read error** An error occured while reading the system date and time.
0x02	**Time conversion error** Failed to convert the system date/time to the internal format.
0x03	**Invalid user type** The detected or provided user type is not recognized or not allowed.
0x04	**External EEPROM Access Error** An error occured while reading from or writing to the external EEPROM memory.
0x05	**RFID tag read error** Failure during the reading of the RFID tag.
0x06	**RFID tag data error** Error while reading data stored on the RFID tag.
0x07	**RFID authentication error** The RFID tag failed authentication or security verification.
0x08	**RFID Power Failure** The auxiliary power has been interrupted or is missing.
0x09	**Date/time not updated** The system clock is not synchronized or has invalid date/time information.
0x0A	**Invalid code** The access code is not valid or not present in memory.
0x0B	**Activation time not reached** The access code is not yet active (start date/time not reached).
0x0C	**Expiration time exceeded** The access code is expired (end date/time passed).
0x0D	**Day not enabled** Access attempted on a day of the week that is not authorized.
0x0E	**Hour not enabled** Access attempted outside the allowed time slots.
0x0F	**User type disabled** The user type associated with the code is currently disabled.
0x10	**Invalid plant code** The access code belongs to a different or incorrect plant/facility.
0x11	**Card read error** General error while reading the access RFID tag.

Ced Non-Standard Dpt Export

1. Definition

1.0. State for which product you are intending to have this non-standard DPT approved

Product name	KNX secure access control capacitive keypad
Order number	BX-E-R12Sxx
Application program name	BX-E-R12Sxx - Access control keypad
Application program version	1.0

1.1. Identification of the non-standard DPT

Name	Diagnostic message
Description	Indicates the current diagnostic message code

1.2. Definition of the fields

Field name	Description	Encoding	Unit	Size/bits	Range from	Range to	Resolution
Diagnostic code	Indicates the current diagnostic message code	N	none	8	0	255	1

Key	Value
0	No error - No error occured.
1	System datetime read error - An error occured while reading the system date and time.
2	Time conversion error - Failed to convert the system date/time to the internal format.
3	Invalid user type - The detected or provided user type is not recognized or not allowed.
4	External EEPROM Access Error - An error occured while reading from or writing to the external EEPROM memory.
5	RFID tag read error - Failure during the reading of the RFID tag.
6	RFID tag data error - Error while reading data stored on the RFID tag.
7	RFID authentication error - The RFID tag failed authentication or security verification.
8	RFID Power Failure - The auxiliary power has been interrupted or is missing.
9	Date/time not updated - The system clock is not synchronized or has invalid date/time information.
10	Invalid code - The access code is not valid or not present in memory.
11	Activation time not reached - The access code is not yet active (start date/time not reached).
12	Expiration time exceeded - The access code is expired (end date/time passed).
13	Day not enabled - Access attempted on a day of the week that is not authorized.
14	Hour not enabled - Access attempted outside the allowed time slots.
15	User type disabled - The user type associated with the code is currently disabled.
16	Invalid plant code - The access code belongs to a different or incorrect plant/facility.
17	Card read error - General error while reading the access RFID tag.
18	Available for future use.
19	Available for future use.
20	Available for future use.
21	Available for future use.
22	Available for future use.
23	Available for future use.
24	Available for future use.
25	Available for future use.
26	Available for future use.
27	Available for future use.
28	Available for future use.
29	Available for future use.
30	Available for future use.
31	Available for future use.
32	Available for future use.
33	Available for future use.
34	Available for future use.
35	Available for future use.
36	Available for future use.
37	Available for future use.

38	Available for future use.
39	Available for future use.
40	Available for future use.
41	Available for future use.
42	Available for future use.
43	Available for future use.
44	Available for future use.
45	Available for future use.
46	Available for future use.
47	Available for future use.
48	Available for future use.
49	Available for future use.
50	Available for future use.
51 ... 255	

1.3. Provide additional encoding information in clear text

Additional encoding information	Error_code Description 0x00 No error - No error occured. 0x01 System datetime read error - An error occured while reading the system date and time. 0x02 Time conversion error - Failed to convert the system date/time to the internal time_t format. 0x03 Invalid user type - The detected or provided user type is not recognized or not allowed. 0x04 External EEPROM Access Error - An error occured while reading from or writing to the external EEPROM memory. 0x05 RFID tag read error - Failure during the reading of the RFID tag. 0x06 RFID tag data error - Error while reading data stored on the RFID tag. 0x07 RFID authentication error - The RFID tag failed authentication or security verification. 0x08 RFID Power Failure - Power to the RFID chip was interrupted during operation. 0x09 Date/time not updated - The system clock is not synchronized or has invalid date/time information. 0x0A Invalid code - The access code is not valid or not present in memory. 0x0B Activation time not reached - The access code is not yet active (start date/time not reached). 0x0C Expiration time exceeded - The access code is expired (end date/time passed). 0x0D Day not enabled - Access attempted on a day of the week that is not authorized. 0x0E Hour not enabled - Access attempted outside the allowed time slots. 0x0F User type disabled - The user type associated with the code is currently disabled. 0x10 Invalid plant code - The access code belongs to a different or incorrect plant/facility. 0x11 Card read error - General error while reading the access card.

2. Communication

2.1. Access Type

Input				
N » this	1 » this			
Spontaneous	Cyclically	Time-out		
Request	Polling	Period		
Output				
this » M	1 » this			
Spontaneous	COV	Delta value	Min repetition time	
	Cyclic	Period		
Request				
Status information				
Diagnostic information				
Parameter				

3. Compatibility and compliance

3.1 Is this non-standard DPT a reuse of an already accepted non-standard DPT ?

Reused

3.2. Is the information, communicated via this non-standard DPT, in part or in total also available in other DPs that use standard DPTs in the same application program ?

Reference

3.3. Motivation

Motivation	It's suitable to be used by a system supervisor/server to inform about the device status or operation errors.

Approve / Reject

Status	Approved
When	n/a
Reason	This non-standard DPT is accepted for use in this application version. The data is very implementation specific, for diagnostic purposes, and there is thus no standard DPT with the same information. The format is properly designed (enum, starting with 0, no gaps, 0 is the default value). Steven De Bruyne System Architect - KNX Association

Appendix B

Non-standard communication object 14 bytes

Non-standard communication object format for saving and deleting access code information (14 bytes).
KNX registration of the datapoint.

Ced Non-Standard Dpt Export

1. Definition

1.0. State for which product you are intending to have this non-standard DPT approved

Product name	KNX secure access control capacitive keypad
Order number	BX-E-R12Sxx
Application program name	BX-E-R12Sxx - Access control keypad
Application program version	1.0

1.1. Identification of the non-standard DPT

Name	Access code data 14Byte
Description	Access code and all related information data (14Byte)

1.2. Definition of the fields

Field name	Description	Encoding	Unit	Size/bits	Range from	Range to	Resolution
P	Password	U	none	24	0	16777200	1

Field name	Description	Encoding	Unit	Size/bits	Range from	Range to	Resolution
S	Access Start	U	none	24	0	16777200	0

Field name	Description	Encoding	Unit	Size/bits	Range from	Range to	Resolution
D	Access Duration	U	none	24	0	16777200	0

Field name	Description	Encoding	Unit	Size/bits	Range from	Range to	Resolution
T	Grant Hour Access	U	none	24	0	0	0

Field name	Description	Encoding	Unit	Size/bits	Range from	Range to	Resolution
W	Day of week grant Access	U	none	8	0	0	0

Field name	Description	Encoding	Unit	Size/bits	Range from	Range to	Resolution
A	Access Type	U	none	8	0	10	1

1.3. Provide additional encoding information in clear text

Additional encoding information	S: counter for access start (5 minutes resolution) from 01/01/2020 D: counter for access duration (5 minutes resolution) T: 24 bit to grant access in 24 hours of day (1 bit per 1 hour) W: 8 bit to enable access in 7 days of week + 1 bit to enable/clear access code A: access or user type identifier

2. Communication

2.1. Access Type

v	**Input**						
	N » this	1 » this	v				
	Spontaneous	Cyclically		Time-out			
	Request	Polling		Period			
	Output						
	this » M	1 » this					
	Spontaneous	COV		Delta value		Min repetition time	
		Cyclic		Period			
	Request						
v	**Status information**						
	Diagnostic information						
	Parameter						

3. Compatibility and compliance

3.1 Is this non-standard DPT a reuse of an already accepted non-standard DPT ?

Reused	value="1429 - Password Data 14Byte"

3.2. Is the information, communicated via this non-standard DPT, in part or in total also available in other DPs that use standard DPTs in the same application program ?

Reference	

3.3. Motivation

Motivation	Non standard DPT to set access code and other information related to the code such as start validity date-time, duration interval, hour slot, day of week validity, access type. As discussed via e-mail in date 05/06/2025

Approve / Reject

Status	Approved
When	n/a
Reason	This non-standard DPT is accepted for use in this application version. This is a renewed use of an existing approved non-standard DPT. Steven De Bruyne System Architect - KNX Association

Formattazione dei dati

Payload 14 bytes payload data sample to save access code (GO 50); non-standard DPT.

Hexadecimal value:

1234FF90210AEC0700FFFFFF7F00

Access code: 1234
Code validity start date-time: 24/04/2026 – 09:21
Code validity end date-time: 01/05/2026 – 10:21
Validity: all hours of the day
Validity: all days of the week
User type: 0 (guest)

It CANNOT be sent with the ETS monitor because it does not handle non-standard DPTs. An external/custom application is required.

Appendix C

RFID tag

Information regarding the data format in internal memory and RFID tags types supported.

Summary of the main information for each card

For each card you have to write **8 bytes**, of which:

1. **Access code:** 6 bytes, each byte represents a digit in the range 0x00–0x09
2. **Plant Id:** 2 bytes, values in `the range 0x00-0xFF` (decimal: 0–65535)

Both codes are stored in **little endian** order: the first byte is the **LSB** and the last byte is the **MSB**.

Example

Access code: `123456` → stored as `0x010203040506` (LSB=0x01, MSB=0x06)
Plant Id: 43707→ stored as `0xAABB` (LSB = 0xAA, MSB = 0xBB)

Total bytes to write (hexadecimal): 010203040506AABB

Parameters and ranges for different card types

Card type	Parameters	Details / Range
Mifare Ultralight	Page Number	[4-14] - each page 4 bytes, then 2 contiguous pages
Mifare Classic 1K	Sector / Block	Sector [1-15], block [0-2] - each block 16 bytes, first 8 bytes used for data
Mifare Classic 2K	Sector / Block	Sector [1-15], block [0-2] - each block 16 bytes, first 8 bytes used for data
Mifare Classic 4K	Sector / Block	Sector [1-31], block [0-2] - each block 16 bytes, first 8 bytes used for data
ST25TB 512	Block number	[7-14] - 4-byte block, 2 contiguous blocks used
ST25TB 2K	Block number	[7-62] - 4-byte block, 2 contiguous blocks used
ST25TB 4K	Block number	[7-126] - 4-byte block, 2 contiguous blocks used

The system is designed to allow the simultaneous use of different types of cards.

Appendix E

Electrical specifications

KNX bus:

- voltage 21-32 V dc
- maximum current ≤ 20 mA

Auxiliary power supply:

- voltage 12-30 V dc
- maximum current ≤ 500 mA

Appendix F

Generic function key parameters and functions

For each key, it is possible to lock the configured function by enabling the “Function lock” parameter.

Enabling this parameter makes a dedicated communication object available, through which execution of the function can be inhibited.

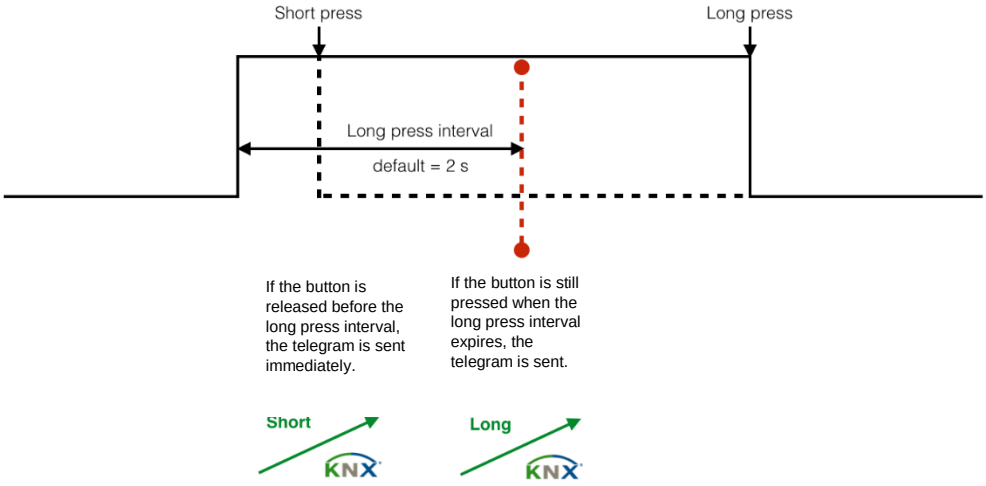
309	Button 1	Enable function lock	1 bit	C	-	W	-	-	1-bit, enable	Basso
310	Key 1	Function lock enable status	1 bit	C	R	-	T	-	1-bit, state	Basso

Communication objects for Key 1 with “Function lock” enabled

Warning

All modes, except the edge-triggered mode, allow enabling a second command associated with a long press.

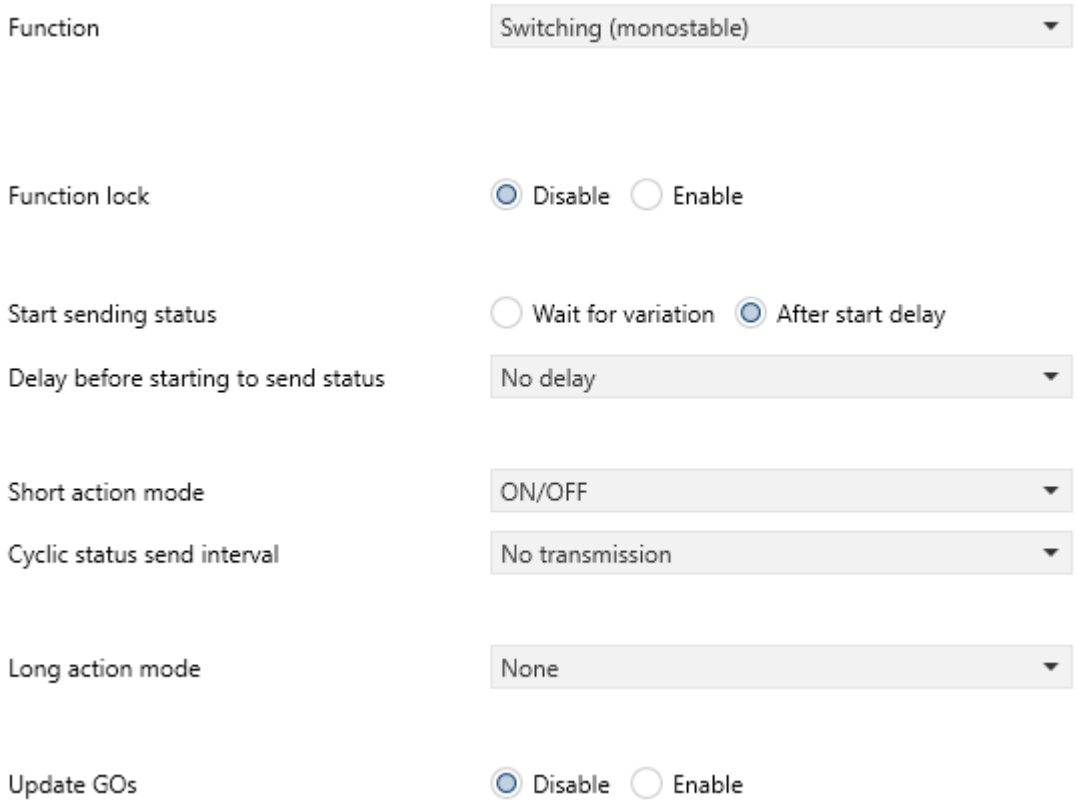
If this function is not active, the KNX telegram is sent immediately when the button is pressed (rising edge). If the long-press function is enabled, the interface waits to determine whether the command is short or long, introducing a small **latency**. This delay may be perceived as reduced command responsiveness.



The user should be aware that this is a normal consequence of the need to wait for the button release (falling edge) in order to determine whether the command to be executed is a long or short press.

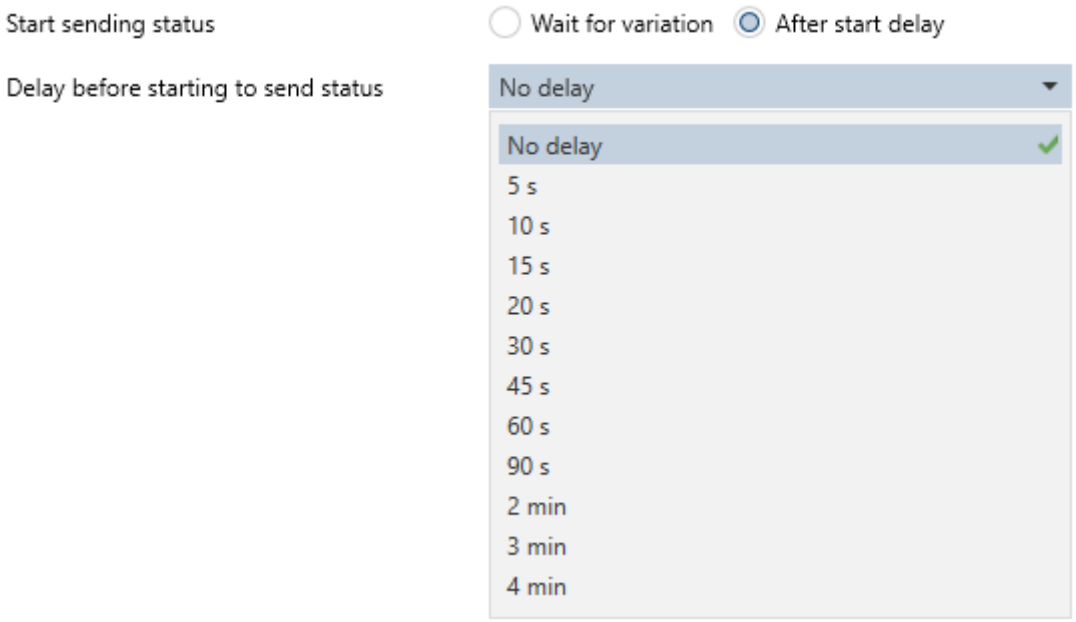
1. Switching (monostable)

The “Switching (monostable)” function allows a load to be switched on and off by pressing a push button.

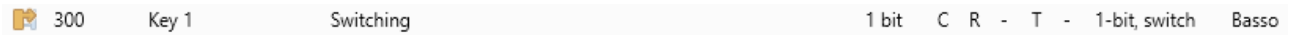


The “Start sending status” parameter allows defining when the first status telegram is sent: on the first change, by selecting “Wait for variation”, or at device startup, by selecting “After start delay”.

The “Delay before starting to send status” parameter allows setting the transmission delay time, applicable in both cases, from 0 up to 4 minutes.

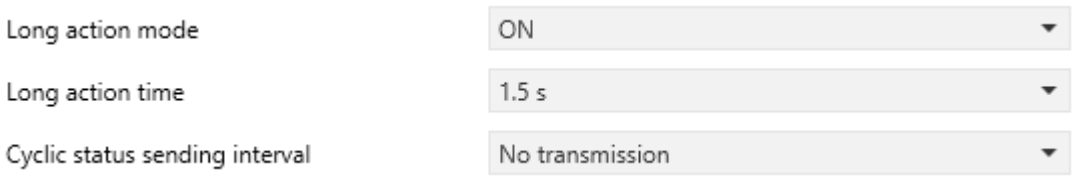


The “Short action mode” parameter allows defining the behavior of the command when the button is pressed. The “ON/OFF” value enables a toggle behavior, alternating ON and OFF data. The “ON” and “OFF” values disable the toggle mode, specifying whether the output data will always be ON or always OFF. The available DPTs are shown below.



The “Cyclic status send interval” parameter allows enabling the periodic sending of the key status, defining an interval of up to a maximum of 12 hours.

The “Long action mode” parameter allows enabling a second command, which will only be triggered when the button is held for a time longer than the value defined by the “Long action time” parameter.

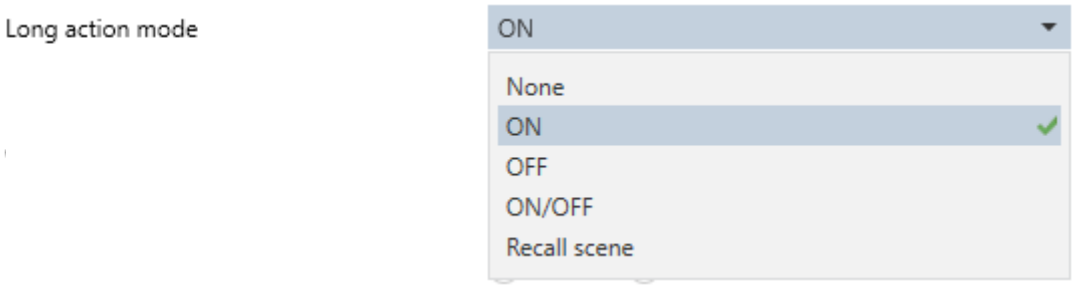


Enabling the long command makes an additional communication object available, whose name includes the suffix “(long action)”.

Configuration with ON enabled on long press.

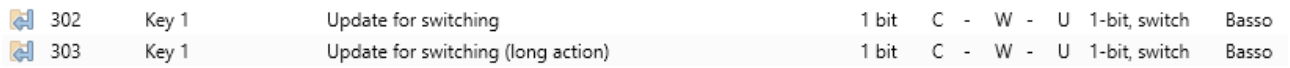
As in the case of short press, it is also possible to enable periodic status transmission of the key via the “Cyclic status sending interval” parameter.

The long press can trigger an ON/OFF toggle command, a fixed ON command, a fixed OFF command, or the execution of a scene.



When scene recall is enabled, it is possible to configure the scene number via the “Scene number” parameter.

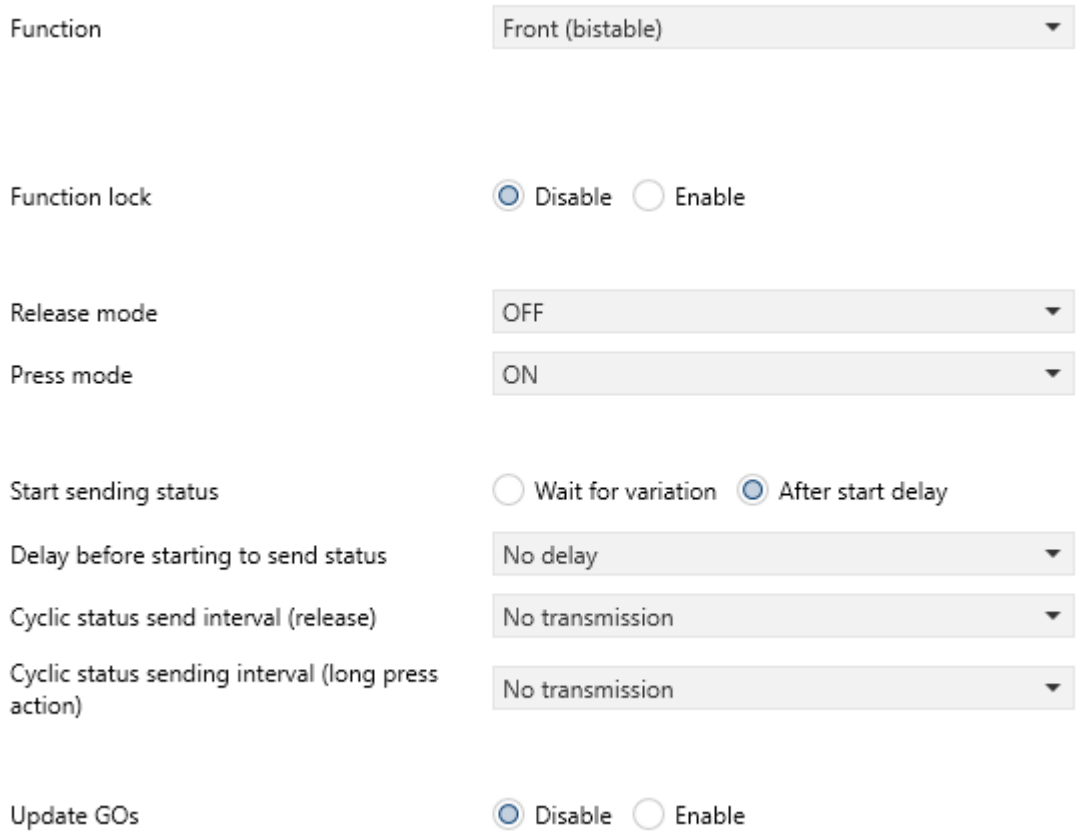
The “Update GOs” parameter makes available one object for the short function and, if enabled, one object for the long function, in order to synchronize the button state with an external status feedback.



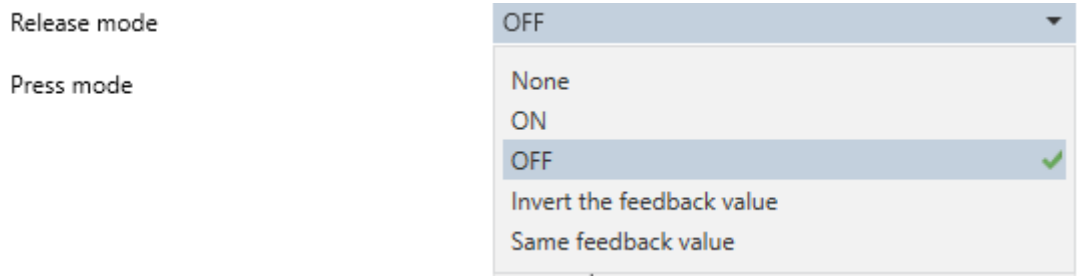
It is also possible to configure the automatic readout of the update communication objects (read request), by defining a delay for the first request, from 0 to 4 minutes, and a periodic request interval, from 0 to 12 hours.

2. Edges (bistable)

The “Edges (bistable)” function exhibits a behavior very similar to the “Switching (monostable)” function.



In this mode, short and long press actions are not available; instead, actions on button press and button release are handled.



All other parameters behave in the same way as defined for the “Switching (monostable)” function.

3. Dimming

The “Dimming” function allows switching a lamp on and off and adjusting its brightness.

Function	Dimming
Function lock	Disable / Enable
Start sending status	Wait for variation / After start delay
Delay before starting to send status	No delay
Cyclic status send interval (short action)	No transmission
Cyclic status sending interval (long action)	No transmission
Long action mode	Increase/Decrease
Long action time	1.5 s
Dimmer increment	100%
Send stop on release	Disable / Enable
Short action mode	ON/OFF
Update GOs	Disable / Enable

The need to manage two commands automatically enables the “Long action mode” function for dimming the light source, while the “Short action mode” function is reserved for switching the load on and off.

The switching behavior on short press operates exactly as described in the previous “Switching” function. What changes is the addition of brightness control on long press.

The available DPTs are shown below.

304	Key 1	Dimming	4 bit	C	R	-	T	-	3-bit controlle...	Basso

In KNX, the adjustment of a lighting source is performed via a specific 4-bit telegram.

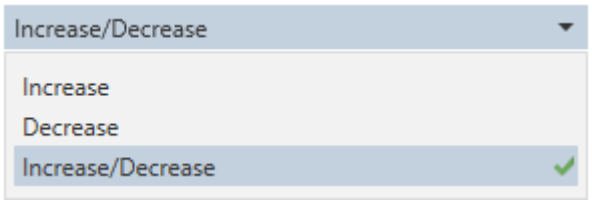
Brightness regulation is achieved by initiating a continuous change and letting it run until the desired level is reached. This command therefore consists of a START action that begins the dimming process and a STOP action that ends it.

The START dimming command is executed as soon as the long press time has elapsed.

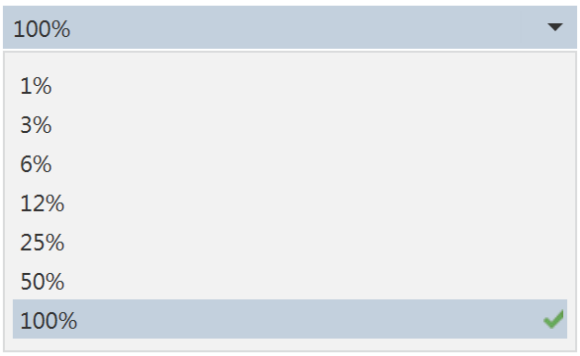
The STOP dimming command is executed when the button is released.

Following the START and STOP commands, the dimming actuator will adjust the light intensity more or less quickly, depending on its internal configuration. In particular, it is possible to set the time required to change brightness from 0% to 100%, thereby defining the speed at which the lamp changes intensity.

The long command can be configured to alternately perform an increase and a decrease, or it can be set to always perform an increase or always perform a decrease.



Finally, the maximum increment associated with a START+STOP action can be configured. Setting 25% means that the maximum increase/decrease that can be performed with a START+STOP action will be 25%.



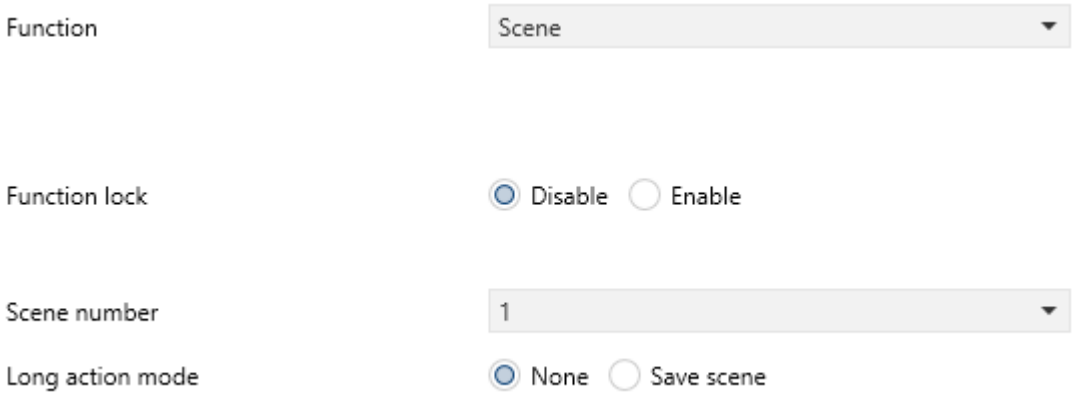
What is this for?
In general, if manual adjustment is required in order to fine-tune brightness as needed, this value should always be set to 100%, allowing the full possible range to be covered in a single operation.
A different case is when brightness is adjusted automatically in discrete steps. In this scenario, it is first recommended to configure the dimming actuator so that the transition time is set to zero, ensuring that each brightness step is immediate.
In this case, the maximum increment configuration effectively becomes the step size. Setting 25% means that each step will change brightness by 25%, resulting in 5 discrete levels: 0%, 25%, 50%, 75%, and 100%.
In conclusion, this function can only be properly used when commands are configured as “increment only” or “decrement only”, otherwise there is a risk of continuously toggling back and forth between adjacent steps.

This configuration requires a dual-command setup: one command dedicated to increasing and another dedicated to decreasing.
This application is particularly suitable for meeting rooms.

All remaining parameters for status transmission and update communication objects behave exactly as described for the previous functions.

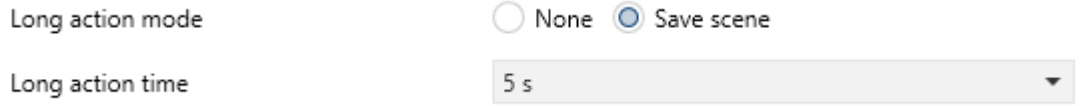
4. Scene

This function allows a specific KNX scene to be recalled via a command. It is possible to configure which scene is recalled by defining the “Scene number” according to the KNX numbering range from 1 to 64.

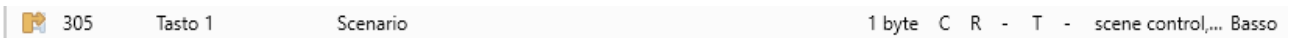


The “Scene” function not only allows recalling the desired configuration, but also enables saving the state of devices to create a new command.

In line with the typical behavior of car radios, the save command can be triggered by a long press of the button. The “Long action mode” parameter allows enabling or disabling this option.



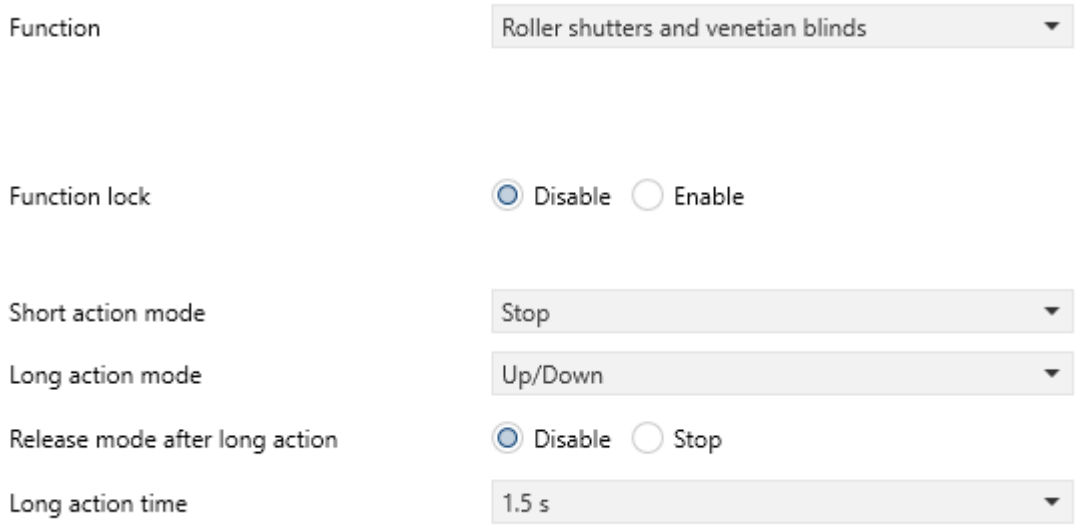
When this parameter is enabled, “Long action time” defines how many seconds the button must be held down to trigger saving. The available DPTs are shown below.



Both the “Recall scene” and “Store scene” commands use the same 1-byte communication object and typically act on the same communication object in the actuators. Therefore, a single group address is sufficient to program both functions.

5. Blinds and shutters

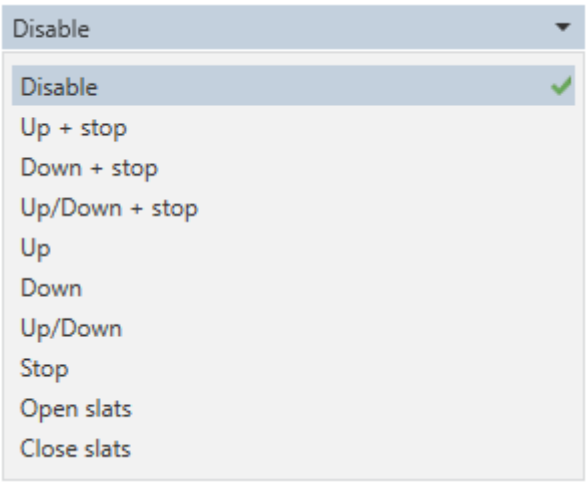
This function provides commands for moving blinds and shutters as well as for stopping their movement, allowing a wide range of flexible control solutions.



The image above shows the typical KNX configuration, where movement is triggered by a long press and stopping is triggered by a short press.

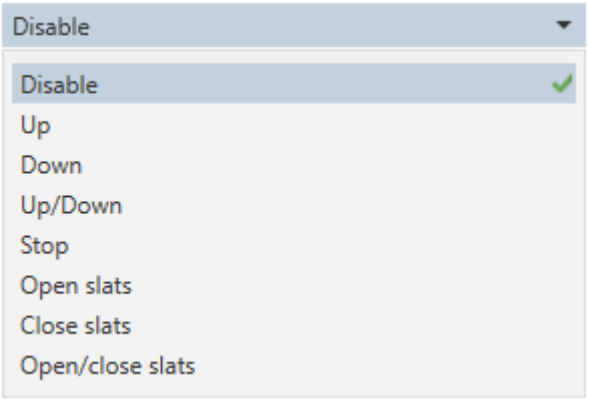
In reality, both short and long presses can be configured in many different ways to achieve various operating behaviors according to customer requirements.

Up + Stop is a cyclic command that alternates between upward movement and stopping.
Down + Stop is a cyclic command that alternates between downward movement and stopping.
Up/Down + Stop is a cyclic command that alternates between movement and stopping. The movement itself is also cyclic, alternating between upward and downward directions.
Up is the command that triggers upward movement.



Short action mode

Down is the command that triggers downward movement.
Up/Down is a cyclic command that alternates between upward and downward movement.
Stop is the command that stops movement.
Slat opening is the command that performs a short opening movement to adjust the slats.
In KNX terminology, slat opening corresponds to sending the value 0 to the STOP communication object.



Long action mode

Slat closing is the command that performs a short closing movement to adjust the slats. In KNX terminology, slat closing corresponds to sending the value 1 to the STOP communication object.

When the “Long action mode” is enabled, it is also possible to choose whether to send a STOP command upon button release.

If this option is enabled, the button can be used as a classic manual control, allowing the shutter to move as long as the button is held down.

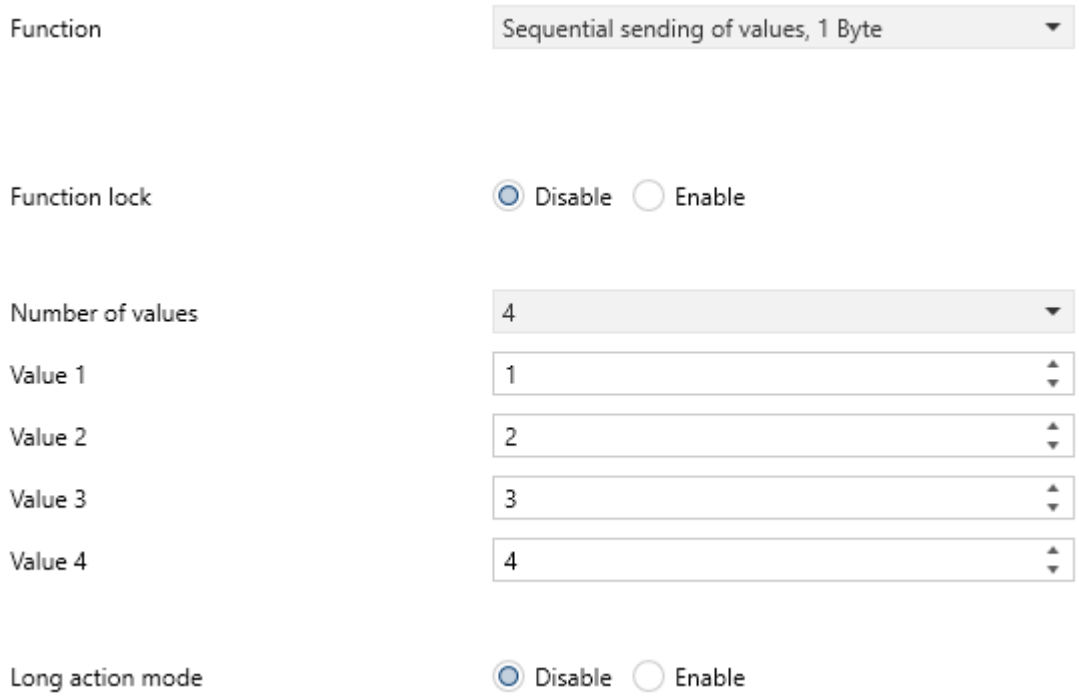
In KNX systems, MOVEMENT and STOP notifications to the actuator are transmitted via two separate communication objects. The available DPTs are shown below.

300	Key 1	Stop blind/shutter	1 bit	C	-	-	T	-	1-bit, step	Basso
301	Key 1	Blind/shutter movement	1 bit	C	-	-	T	-	1-bit, up/down	Basso

The STOP communication object stops the motor if it is currently in motion.
Conversely, if the motor is stationary, a STOP command may generate a short movement called STEP.
The STEP will open if the transmitted value is 0, and will close if the transmitted value is 1.
STEP is typically used to adjust the slats of venetian blinds.
To adjust the slats, a STEP in the opposite direction of the last performed movement must always be generated.

6. Sequential sending of values, 1 byte

This is a standard cyclic command that sends a different 1-byte value on each pulse, according to the programmed sequence.



The “Number of values” parameter allows selecting how many values the sequence will contain. A number between 1 and 4 can be selected.

ETS will display as many fields as the number of values defined in the sequence. These fields can be filled with values from 0 to 255 (byte).

This function also allows enabling the long press, providing the possibility to use a second sequence controlled by this command. In this case as well, the sequence can be defined by specifying the number of values and the data associated with each value.

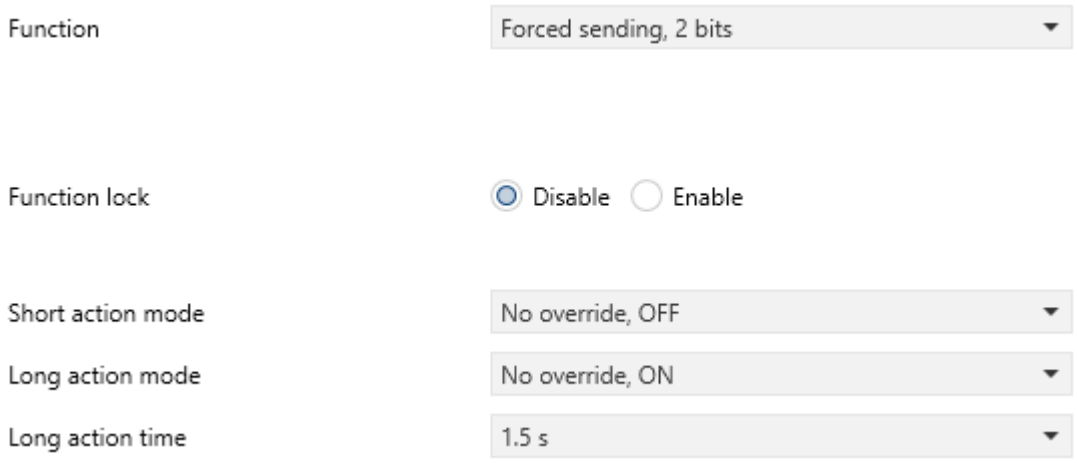
The available DPTs are shown below.

306	Key 1	Send sequential values	1 byte	C	-	-	T	-	8-bit unsigned...	Basso
307	Key 1	Send sequential values (long action)	1 byte	C	-	-	T	-	8-bit unsigned...	Basso

The sequential transmission of 1-byte values is carried out on the same communication object, one for the short press and one for the long press.

7. Forced sending, 2 bit

The “Forced sending” command forces the actuator to remain locked in the desired state.



A 2-bit value can assume four different states on a scale from 0 to 3:

- 0 corresponds to releasing the actuator from the OFF override
- 1 corresponds to releasing the actuator from the ON override
- 2 corresponds to forcing the actuator to the OFF state
- 3 corresponds to forcing the actuator to the ON state

In binary terms, a 2-bit value consists of two digits:

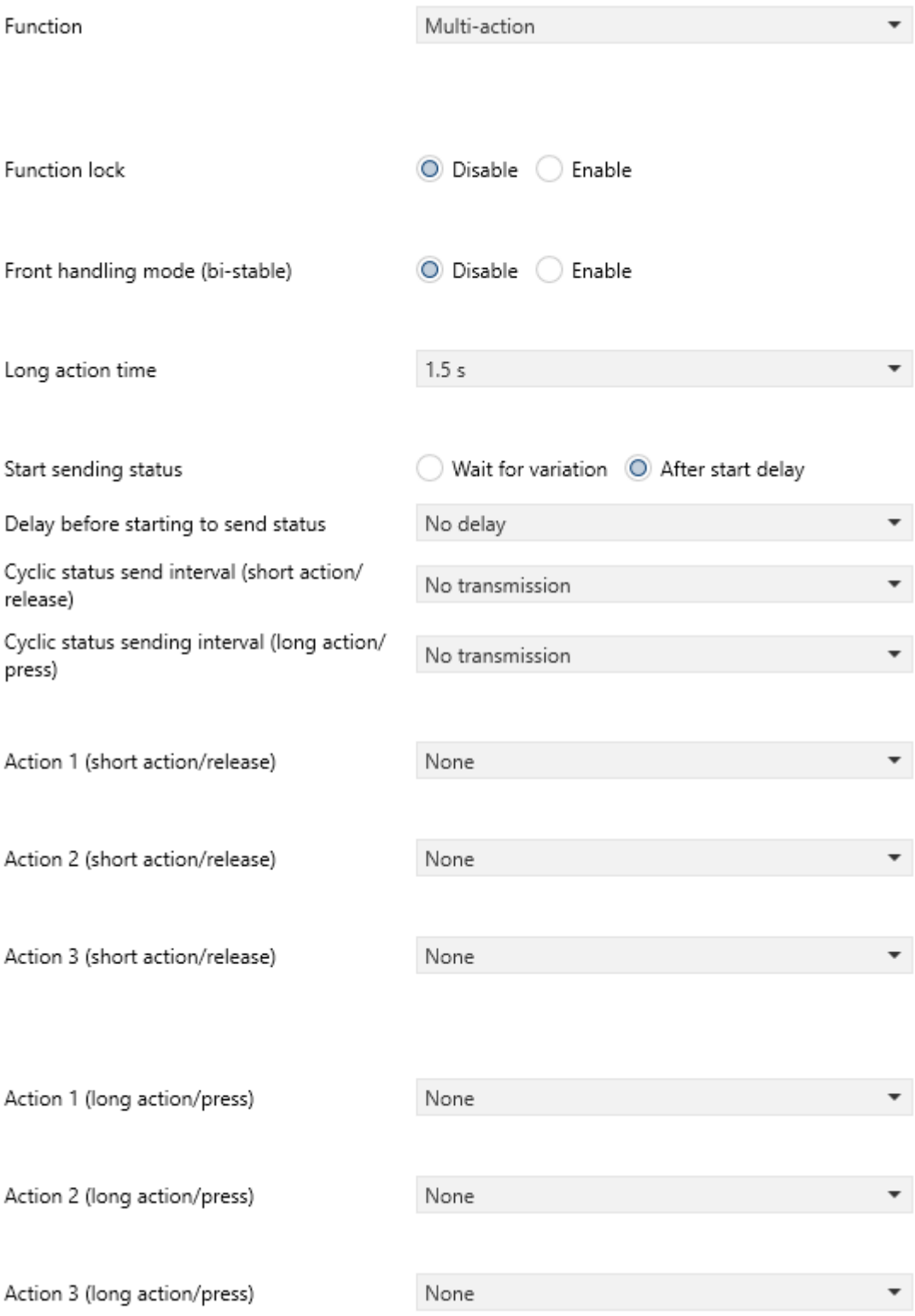
- The least significant bit indicates the OFF or ON position
- The most significant bit indicates whether override is disabled (0) or enabled (1)

The available DPT is shown below.

308	Key 1	Forced	2 bit	C	-	W	T	-	1-bit controlle...	Basso

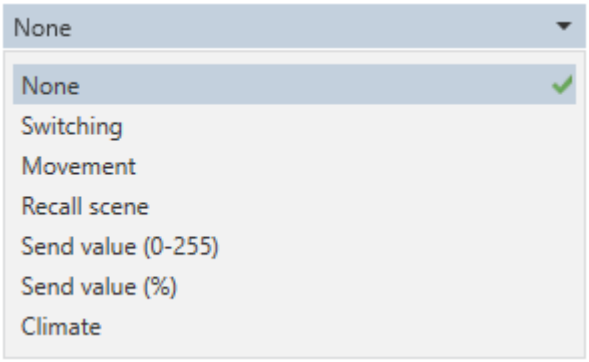
8. Multi-action

The “Multi-action” function allows associating a button press with the simultaneous transmission of a sequence of telegrams, which can be configured to perform different actions according to the programmer’s requirements.



The “Front handling mode (bi-stable)” parameter, when enabled, allows actions to be executed on both button press and button release. When disabled, the button operates in monostable mode and actions are executed on short press and/or long press.

The maximum number of configurable actions is 3 for the short command and 3 for the long command.

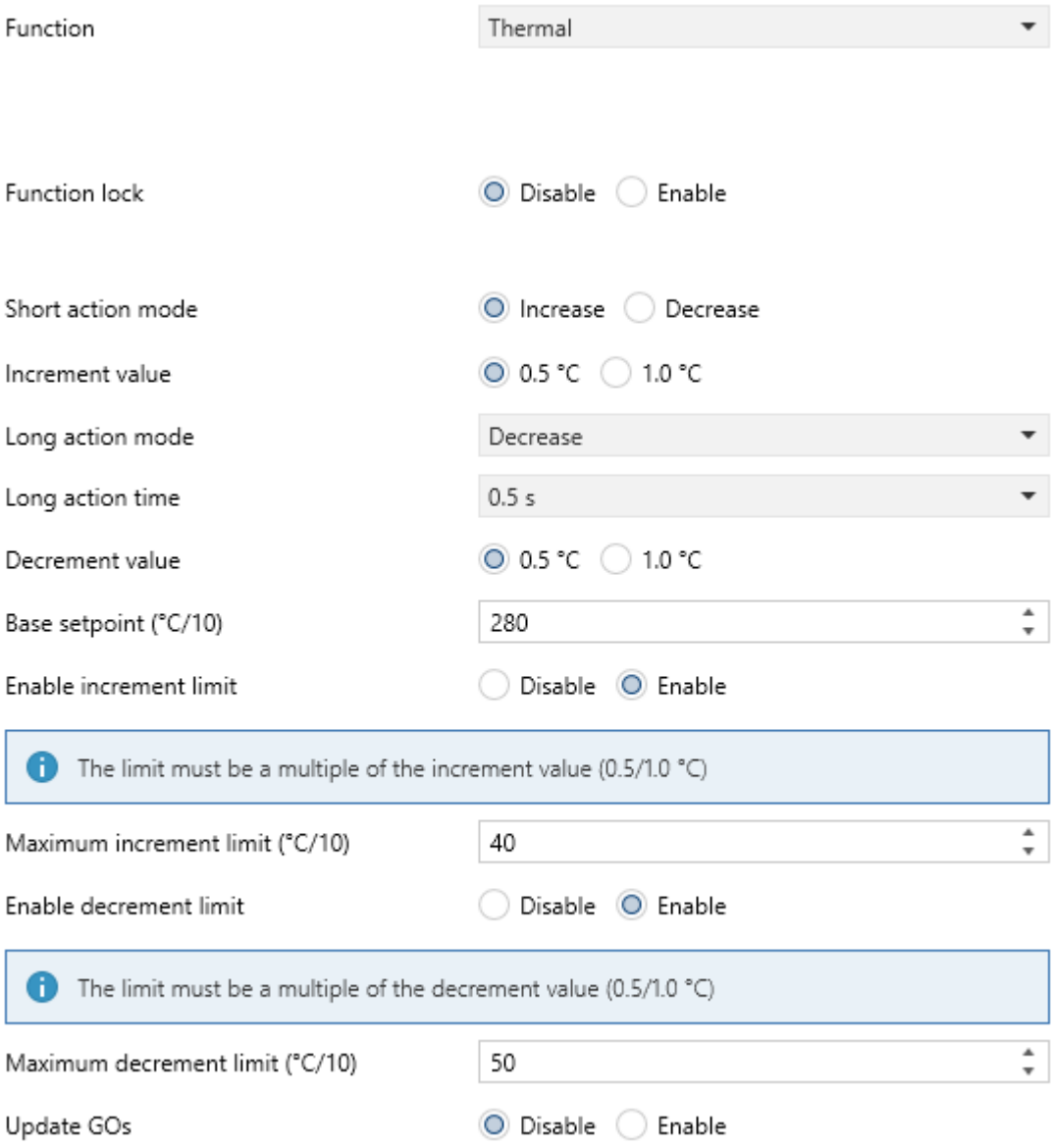


The available actions that can be selected are 6.
Switching allows turning a load on and off.
Shutter control allows opening or closing a blind.
Scene recall allows recalling the desired KNX scene.
Send value (0–255) allows transmitting the desired byte value on the bus.
Send value (%) allows adjusting brightness, position, or any percentage-based value.
HVAC allows selecting the desired HVAC mode: OFF, Comfort, Standby, Night, and Protection.

The parameters related to status transmission at startup and cyclic transmission behave in the same way as described for the previous modes.

9. Thermal

The “Thermal” mode allows increasing and/or decreasing a base setpoint by a predefined temperature value, within configurable minimum and maximum limits.



Short and long press actions can be configured independently: for each one, it is possible to set either an increase or a decrease of the setpoint. The long press action can also be disabled.

The increment and decrement values can be selected between 0.5 °C and 1.0 °C, and are also independently configurable for each action.

The “Base setpoint” parameter defines the reference temperature value on which increments and/or decrements are applied. The value is expressed in tenths of a degree (e.g. 28 °C = 280) and can also be set via a communication object (GO), using the appropriate DPTs.

317	Key 1	Set base setpoint (°C)	2 bytes	C	-	W	-	U	2-byte float va...	Basso
318	Key 1	Status base setpoint (°C)	2 bytes	C	R	-	T	-	2-byte float va...	Basso

For both increase and decrease actions, it is possible to define minimum and maximum limits relative to the base setpoint. In this case as well, values are expressed in tenths of a degree (e.g. 4 °C = 40). The limit parameters are made available only if the corresponding action is configured on at least one of the two commands. Both limits can also be set via communication object (GO), using the appropriate DPTs.

320	Key 1	Set maximum increment limit (°C)	2 bytes	C	-	W	-	U	2-byte float va...	Basso
321	Key 1	Status maximum increment limit (°C)	2 bytes	C	R	-	T	-	2-byte float va...	Basso
322	Key 1	Set maximum decrement limit (°C)	2 bytes	C	-	W	-	U	2-byte float va...	Basso
323	Key 1	Status maximum decrement limit (°C)	2 bytes	C	R	-	T	-	2-byte float va...	Basso

The result of the increase/decrease operation is output via the corresponding DPT.

319	Key 1	Status processed setpoint (°C)	2 bytes	C	R	W	T	-	2-byte float va...	Basso

The “Update GOs” parameter behaves as described in the previous modes.

Function example

Taking the configuration shown in the first image as an example:

- Base setpoint 28 °C (280)
- Increment limit 4 °C (40)
- Decrement limit 5 °C (50)
- Increment/decrement step value 0.5 °C

The maximum achievable setpoint will be 32 °C, while the minimum value will be 23 °C. In total, there will be 8 intermediate steps in the upward direction (28 °C → 28.5 °C → 29 °C → …) and 10 intermediate steps in the downward direction (… ← 27 °C ← 27.5 °C ← 28 °C).

Warning

Increment and decrement limits must be multiples of the configured step value in order to ensure consistency of operations. If this condition is not met, when a limit is reached the value is saturated at that limit.

In this condition, the opposite action (increase or decrease) may generate values that are not aligned with the configured step, resulting in a sequence that is inconsistent with the expected increment/decrement grid.

Example

Assume a base setpoint of 28 °C, an increment step of 1 °C, and a maximum limit set to 29.5 °C.
After the first increment, the value becomes 29 °C. A further increment would lead to 30 °C, but the limit forces saturation at 29.5 °C.
At this point, only decrements are possible: the first decrement brings the value to 28.5 °C and the next to 27.5 °C, highlighting a discontinuity with the initially configured 1 °C step.