blumotix
TOUCH YOUR WORLD

BX-E-AK12

IP65 outdoor Doory

Numeric keypad for access control

Rev.	Data	Descrizione	Redazione
01	28/11/2023	1st Release	F. Melandri P. Zambelli

Table of contents

Glossary

- CO: communication object
- Datapoint: type of data; see KNX standard documentation
- LED: light emitting diode
- LG: yellow led on the front panel, near key 3
- LR: red led on the front panel, near key 2
- LV: green led on the front panel, near key 1
- A, B: function keys A and B

1 Introduction

BX-E-AK12 (Doory) is KNX Blumotix keypad dedicated to access control, specifically designed for outdoor use.
In fact, the container is IP65 certified: it can resist water and dust and is designed to avoid any attempts of tampering or vandalism.

The operation is based on the standard KNX protocol; it has 12 backlit mechanical keys of which 10 numeric (0-9) and 2 generic keys (A, B) configurable to perform different functions; 3 light signals are also available (red, yellow, green LEDs).

With regard to functionality and parameterization, the keypad manages an access control logic with memorization of numeric codes directly on the device. A smartphone app is available for storing and erasing codes.
All the standard functions typical of hotel services can be managed by this keypad and there is also a logic of room energy management.
These functions are particularly suitable in accommodation, tourist and hotel facilities.
The lighting, the numeric keys, the keys dedicated to specific functions, the 3 colored signals, are all configurable and manageable in various modes depending on the type of application required.

2 General information

2.1 Wall mounting

The device is mounted to the wall by fixing the plastic base provided and by using the seal that guarantees its tightness. No need to use recessed boxes. Rear access to the device is necessary to only allow the passage of the KNX bus cable, that provides power and data communication. No other electrical connections are required.

See data sheet for more details about mounting process.

2.2 First activation

Pass the bus cable through the base and connect the KNX to the device. It is advisable to check the correct functioning of the device by powering the bus and programming the physical address KNX with the ETS software. If the programming of the physical address is successful, you can complete the assembly by fixing the base to the wall, placing the seal and proceed with the fixing of the keyboard body on the base.

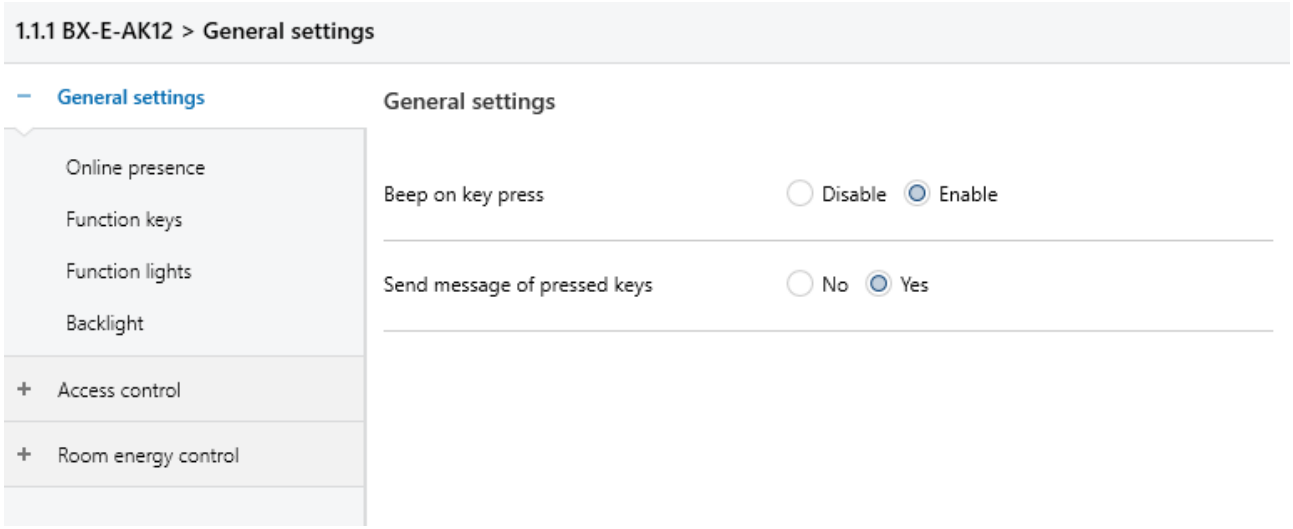
The KNX programming mode can be activated either by the button inside the device (accessible when not fixed to the base) or by pressing the buttons 1, 5, 9 from the front.
The KNX programming status is indicated by the internal red LED on the keyboard and also by the LR on the front.

3 Setup

The ETS database supplied with BX-E-AK12 keypad allows the complete configuration of all the available functions through the modification of the parameters and the use of the offered communication objects.

3.1 General settings

The first section is called "General settings". Below is an analysis of the parameters and functions described in this section.

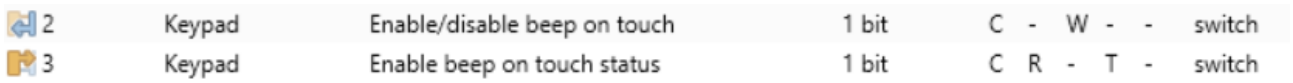


3.1.1 Beep on key press

It enables or disables sound generation at the touch of a key on the keypad.

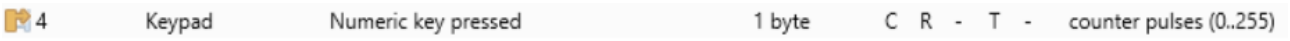
The mode set by this parameter can be changed by writing the corresponding CO 2 setting; the new value will be returned by the status CO 3.

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



3.1.2 Send message of pressed keys

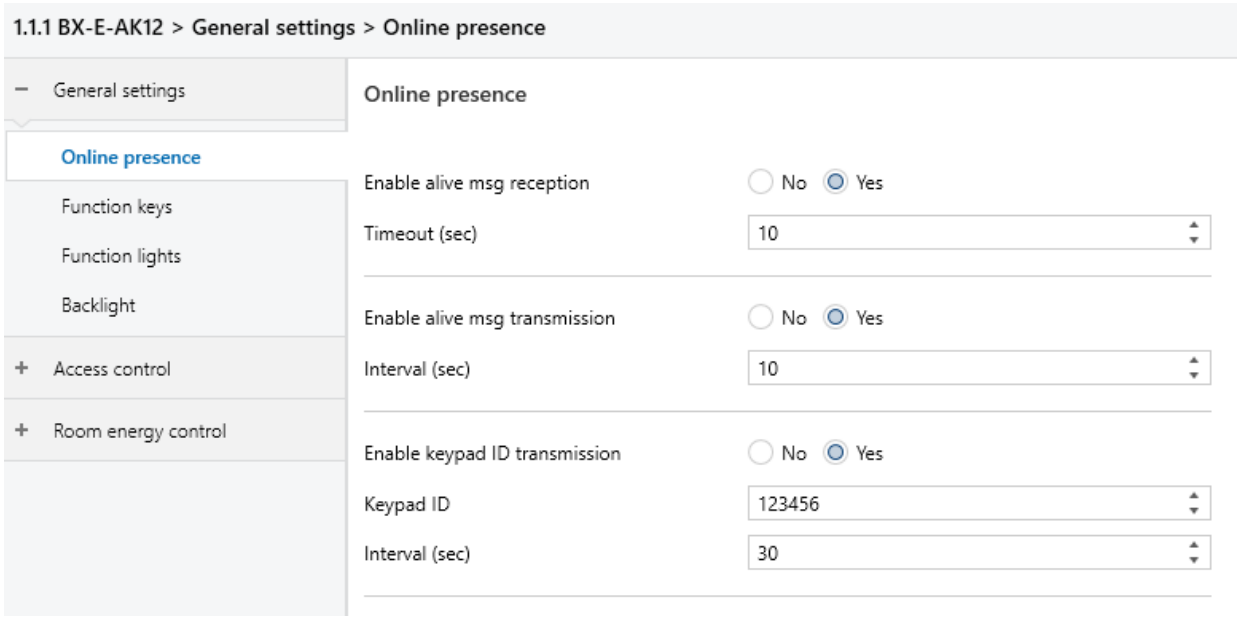
If set to "Yes", it enables the ability to send a message on the bus with each numeric key pressed. The value of the CO corresponds to the numerical value of the button (0-9).



If in the parameter section "Function keys", the B key has been chosen as confirmation to validate the access code entered, then an additional CO will be available that will be transmitted on the bus with value 1 at the press of the button (see paragraph 3.3 “Function keys”).

3.2 Online Presence

This section provides some useful parameters to control the smooth operation of the device by a supervisor. Since this device is dedicated to access control, it may be necessary to constantly monitor the operation of the keypad. The parameters managed are illustrated in the following figure.



3.2.1 Enable alive msg reception

This parameter enables the keypad to receive, within a certain time interval, a specific message of online presence of a supervisor device. Basically, the keypad claims to receive periodically, from the KNX bus, a message of value 1, on the CO 8 "Remote request". The time interval between one reception and the next should not exceed the value of the "Timeout" parameter.

If the supervisor cyclically sends the value 1, within the timeout, then the CO 9 "Remote request reply" will assume the value 0 of correct operation; if instead the supervisor stops sending or exceeds the timeout interval, the CO 9 "Remote request reply" will signal error by sending value 1 on the bus.

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

3.2.2 Enable alive msg transmission

This parameter enables the keypad to send a message of value 1 cyclically to the bus. The sending period is specified by the "Interval" parameter. This function can be used by a possible supervisor device to make sure that the Doory keypad and the data bus are working correctly.

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

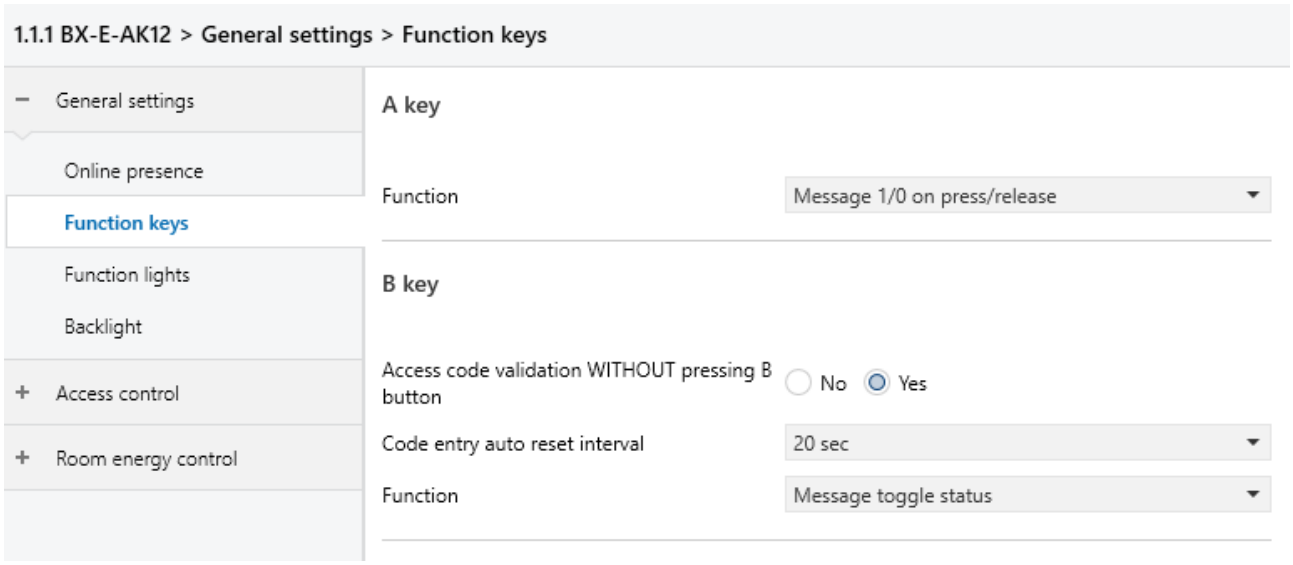
3.2.3 Enable keypad ID transmission

This parameter enables the keypad to cyclically send a message containing a 6-digit (0-999999) identification number to the bus, which the user can specify in the "Keypad ID" parameter. The sending period is set in the "Interval" parameter.

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

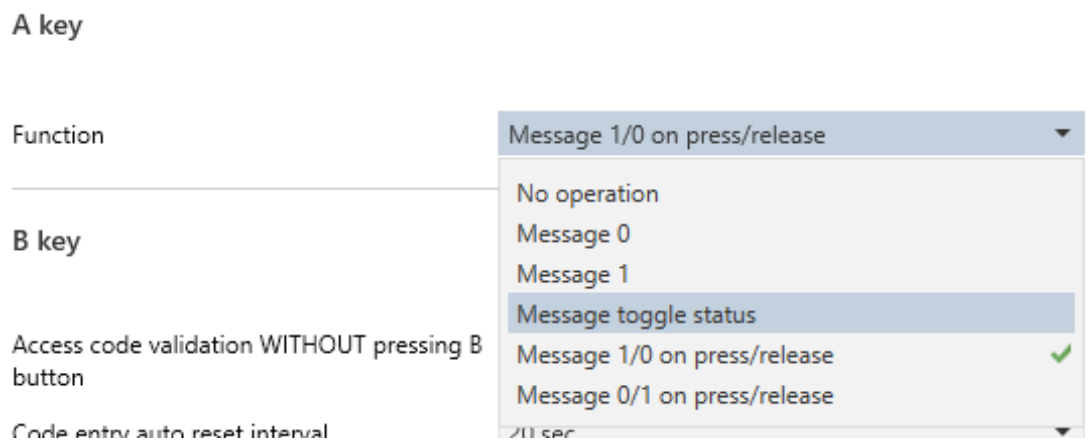
3.3 Function keys

These parameters affect the function keys named A and B.

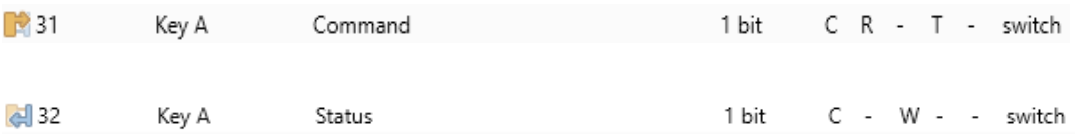


3.3.1 A Key

The A key can be used to send general messages on the bus. The value of the command CO that has to be sent when the button is pressed is configured by selecting an item of the parameter "Function".



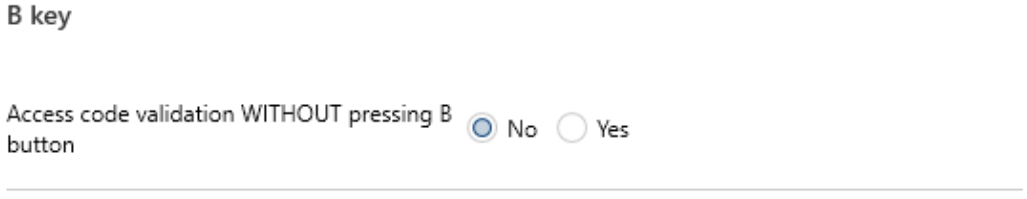
If "Message toggle status" is selected, an additional state CO is enabled whose value is first read, then reversed and finally sent to the command CO.



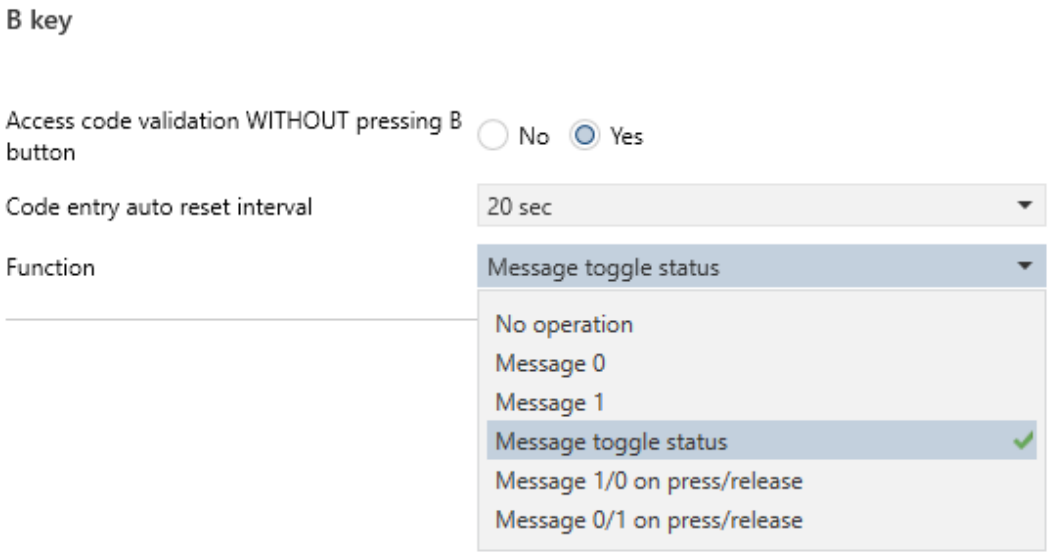
3.3.2 B Key

The B key can be used in two different ways.

- In order to use a confirmation key in the access code input procedure after the numeric keys, B key can be used for this purpose; the parameter must be set as below.



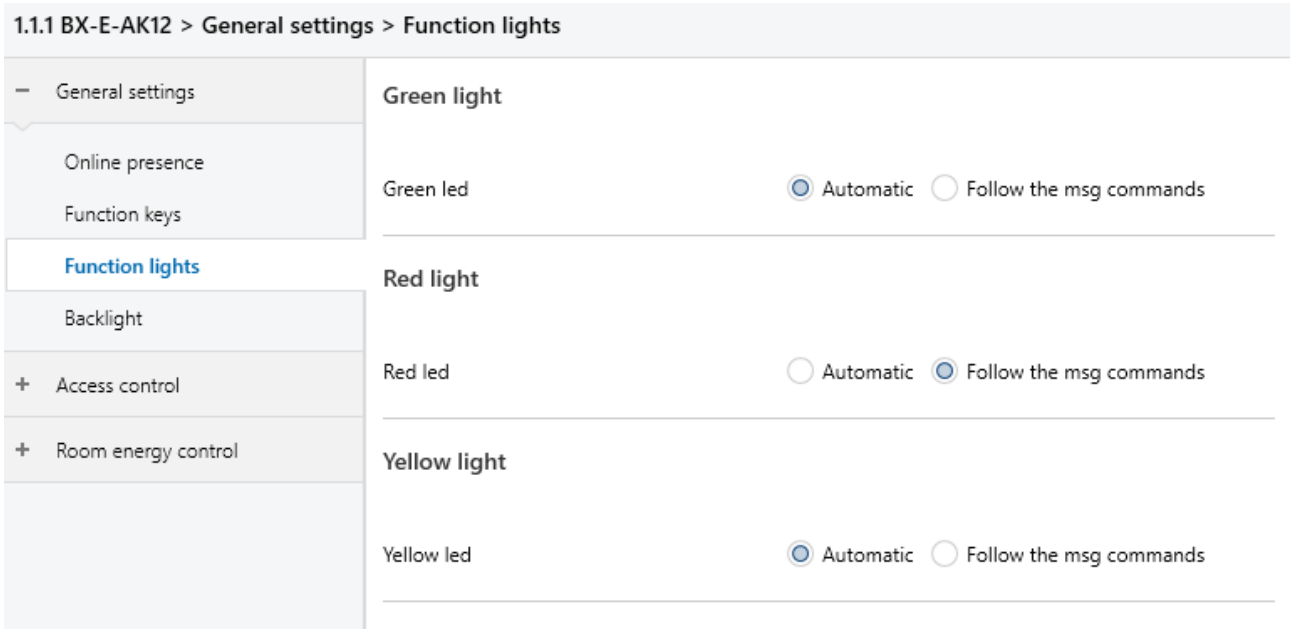
- In order to make the validation phase automatic (without pressing any confirmation button) in the access code input procedure, then B key can be used for general purpose as already shown for A (section 3.3.1).



The use of B button in general mode (command and status CO) also makes the parameter "Code entry auto reset interval" appear.
The validation of the inserted code will happen automatically when the number of digits selected for the length of the code are typed (paragraph 3.7.2), so the parameter "Code entry auto reset interval" represents a security: after this time interval, the digits typed and stored temporarily by the keypad are removed from the memory, so now the keypad is again waiting for the first digit of the code.
This prevents a user from entering a part of the code and leaving the operation pending; after some time, another user could continue the entry, ignoring that other digits had already been previously entered.

3.4 Function lights

These parameters affect the behaviour of the lights LV, LR, LG on the front of the keypad near the numeric keys 1, 2, 3.



All light indications have the selection parameter between "Automatic" and "Follow the msg commands"; based on the selected value, these are the possible behaviours.

3.4.1 “Automatic” mode

By selecting "Automatic", the LEDs LV, LR and LG will be governed by the access attempt; in particular, when a code on the keyboard is typed, the LEDs will signal the outcome of the access attempt with the following behaviours:

- LG is switched on when the button is pressed and turned off when the button is released.
- LR is turned on when the passcode entered is invalid and remains lit until the next operation.
- LV is turned on when the entered passcode is valid and remains lit until the next operation.

3.4.2 “Follow the msg commands”

By selecting "Follow the msg commands", the lighting of the LV, LR and LG LEDs will be delegated to the dedicated communication object; the keypad will return the status controlled on another specific CO.

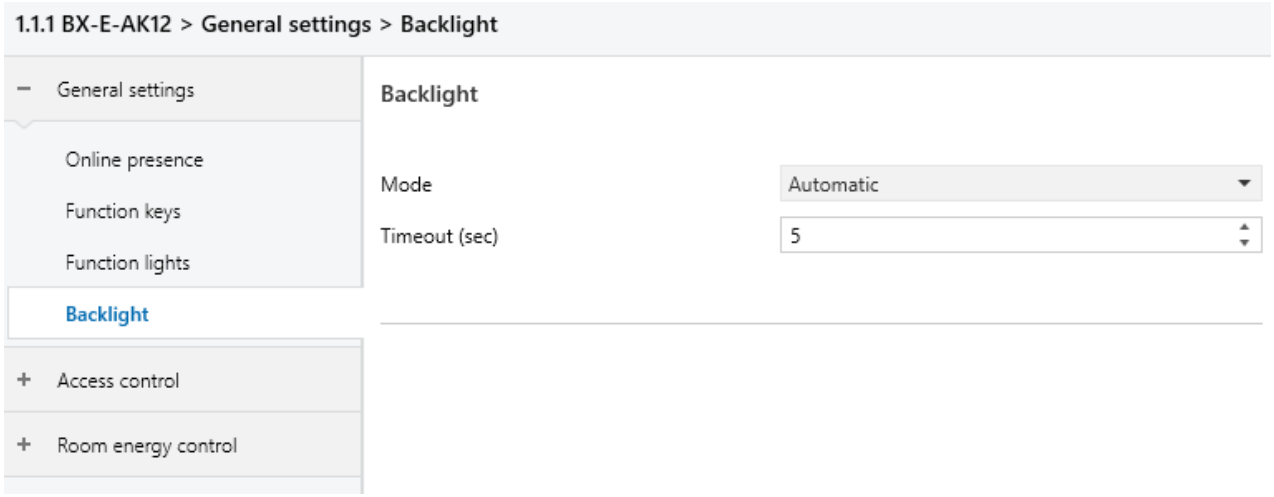
For each led will then be available a pair of CO of control and status.

41	Red led	Set	1 bit	C	-	W	-	-	switch
42	Red led	Status	1 bit	C	R	-	T	-	switch

3.5 Backlight

The keyboard backlight allows to spread a light through the contour of the keys on the front of the device.
There are 3 modes of backlight management and all also provide the possibility of command with a communication object that overrides the default behaviour set in the parameter "Mode".

13	Backlight	Set	1 bit	C	-	W	-	-	switch
15	Backlight	Status	1 bit	C	R	-	T	-	switch



3.5.1 Mode: Always off

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

3.5.2 Mode: Always on

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

3.5.3 Mode: Automatic

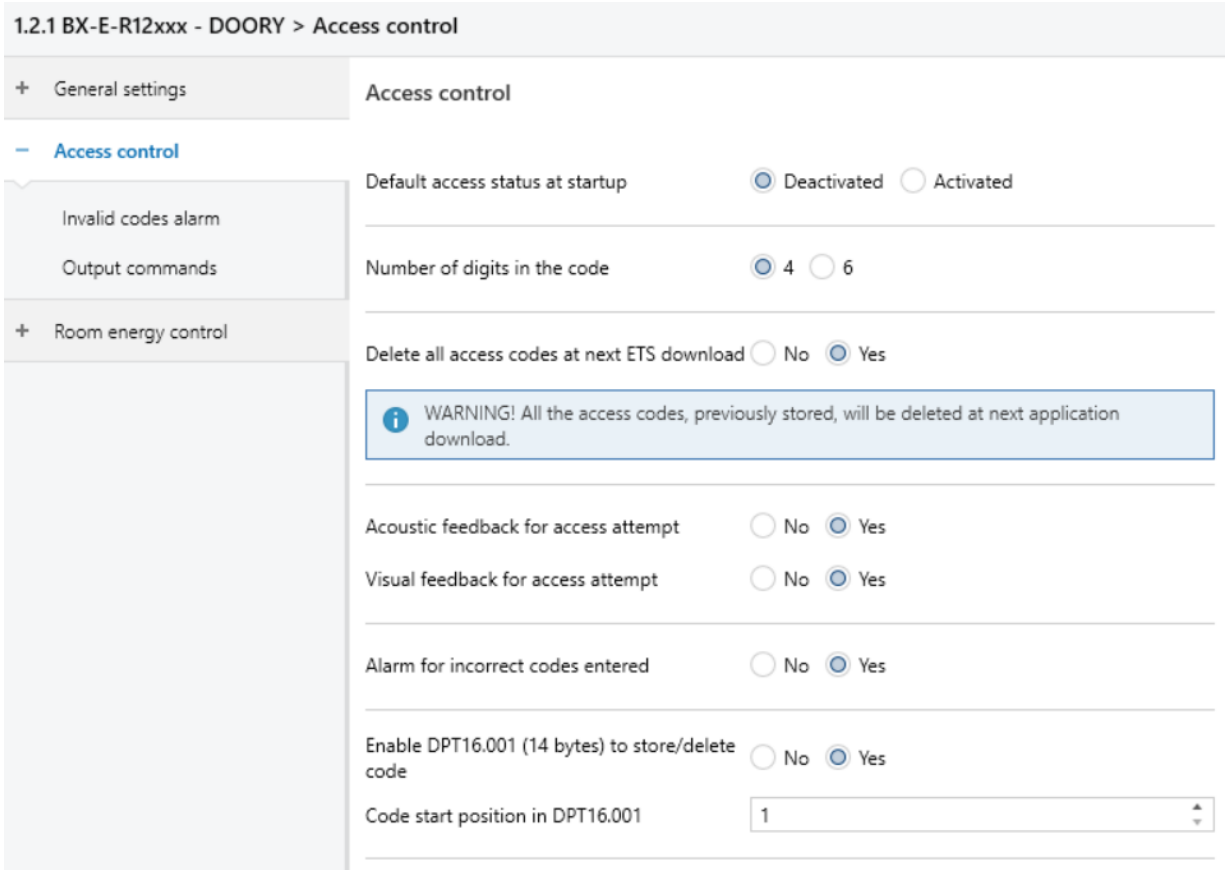
It represents the automatic operation of the backlight. In this case, the ignition occurs when a key is pressed. The shutdown will occur automatically after the time indicated by the parameter "Timeout" has elapsed.

3.6 Access control

The keypad provides access management through the user's insertion of a numeric code of 4 or 6 digits; it is not necessary to use other accessories such as keys or

magnetic cards. Note that the validation of the code is managed directly on the keypad, in fact the device is able to store up to 1000 numeric codes.
The access control system can be integrated with the BMS BX-NEMO software, interfaced with the main hotel management systems on the market, that allows the supervision and management of the accommodation facilities via smartphone, tablet or pc.

Doory and KRIM apps allow to manage the check-in and check-out operations from smartphone/tablet, renew and update the access codes when new guests arrive and whenever necessary.
It is also possible to force a door to open in case of loss of the code; the manager can do it from the phone by just pushing one button of the app.



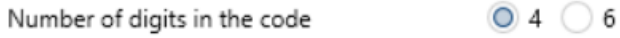
3.6.1 Default access status at startup

When switching on the device or at the end of a download of the ETS application program, the device outputs the KNX access messages enabled or disabled based on the setting of this parameter.

The number and value of output messages depends on the "Output commands" configuration (section 3.6.7).

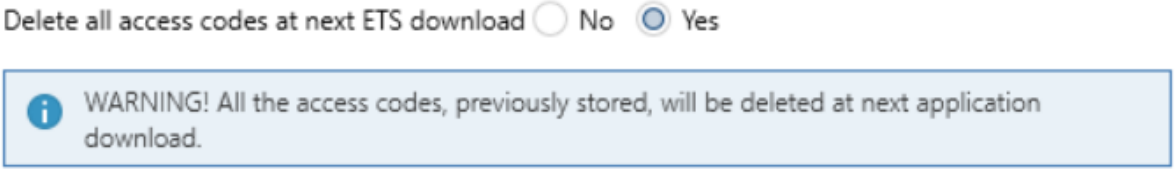
3.6.2 Number of digits in the code

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



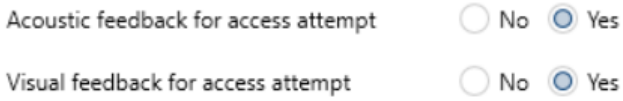
3.6.3 Delete all access codes at next ETS download

The keypad keeps all codes saved (up to 1000) 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 codes or delete them. In case of deletion, a warning message pops up to warn of the danger of the operation.



3.6.4 Acoustic/Visual feedback for access attempt

When the user enters a numeric access code, the outcome of the operation can be signaled by the device with a sound (acoustic return) and with a flashing of the backlight (visual return) of the keypad base. With this parameter, it is possible to choose whether or not to enable the two feedbacks.



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

3.6.5 Alarm for incorrect codes entered

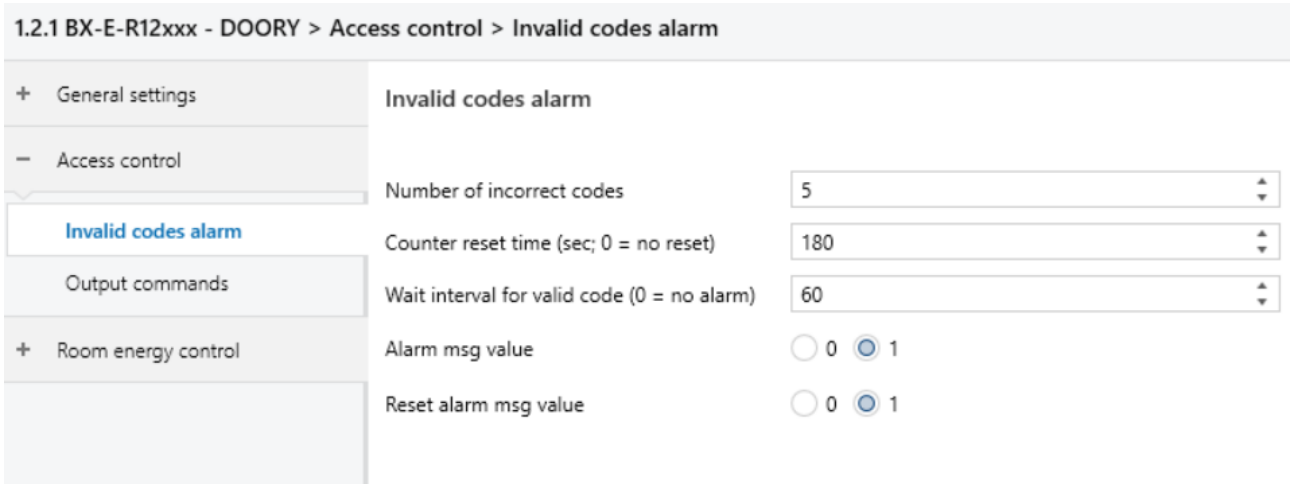
This is a security measure that limits the number of log in attempts with incorrect code.

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.

"Number of incorrect codes" is the number of incorrect code entries allowed before the alarm is reported. The device maintains an internal counter of the number of incorrect attempts made by the user.

"Counter reset time": after this specific interval of time (time starts since the last insertion of incorrect code), 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 attempts are performed at intervals of 4 minutes from each other, the alarm will never be issued because the counter resets every 3 minutes (180 sec).
If this parameter is set to zero, the counter never resets. 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 executed.



"Alarm msg value" specifies the value of the CO transmitted on the KNX bus to signal the alarm for incorrect codes.

70	Codes	Alarm for incorrect codes entered	1 bit	C R - T - alarm

"Reset alarm msg value" specifies the CO value required to cancel the alarm condition.

71	Codes	Reset incorrect codes alarm	1 bit	C - W - - reset

3.6.6 Enable DPT16.001 (14 bytes) to store/delete code

The communication objects enabled by this parameter are used to save and delete access codes in the internal memory of the keypad.

52	Codes	Store request	14 bytes	C - W - -	Character String (ISO 8859-1)
53	Codes	Delete request	14 bytes	C - W - -	Character String (ISO 8859-1)

The value of these objects is string type with a maximum extension of 14 bytes: these messages can be written at most with 14 numeric characters.
Since the access codes are 4 or 6 digits format, it is possible to specify from which position of the 14 bytes string the code to be saved or deleted starts; for this it is possible to use the parameter "Code start position in DPT16.001".

For example, having set the 6-digit code length (paragraph 3.6.2) and the position in that parameter to 5, the values in CO 52 and 53 must have the following format:

"xxxx123456xxxx"

Where "123456" represents the numeric code, while the characters "x" are not significant and are therefore ignored by the system.

Another example, with the 4-digit code length and the position in the above parameter at 1, the values in CO 52 and 53 must have the following format:

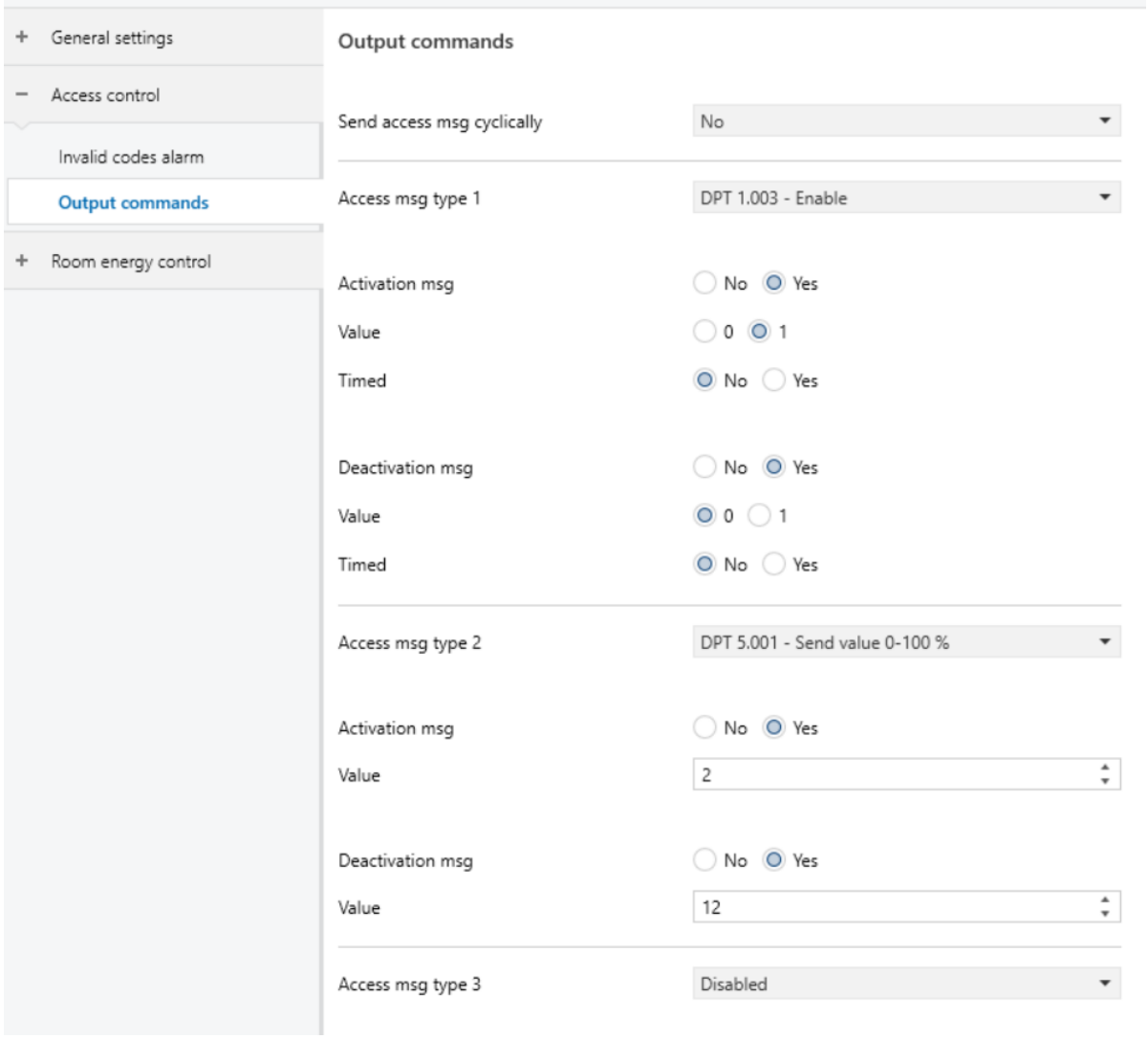
"1234xxxxxxxxxx"

Writing CO 52 stores the code in the memory, unless it is already present. Writing CO 53 erases the code from memory, only if it is present.
As a result of writing CO 52 or 53, there will always be a keypad response on CO 58 (paragraph 3.6.8).

The user can use either these COs or others, with different format (datapoint) that perform the same function (paragraph 3.6.8); the choice depends only on the type of need of the user and the final application.

3.6.7 Output commands

This page defines messages and communication objects to the KNX bus related to access control management. The typing of access codes by the user and the consequent validity check of the same are translated by the device into KNX messages.



Each access attempt by the user can trigger the sending of up to 4 messages on the bus simultaneously.
Messages can be of different types ("Access msg type X"); the 1-bit type ("DPT1.003 - Enable") also allows time management of the message.
The output messages are differentiable depending on whether the code entered is valid or not ("Activation msg", "Deactivation msg").
By setting "Send access msg cyclically", it is possible to periodically send on the bus the result of the last access attempt.

Here is an example of CO for the 4 output commands:

80	Access	Out 1 - DPT 1.003 - Enable	1 bit	C	R	-	T	-	enable
85	Access	Out 2 - DPT 5.001 - Send value 0-100 %	1 byte	C	R	-	T	-	percentage (0..100%)
86	Access	Out 3 - DPT 17.001 - Scenario	1 byte	C	R	-	T	-	scene number
87	Access	Out 4 - DPT 20.102 - HVAC Mode	1 byte	C	R	-	T	-	HVAC mode

3.6.8 Communication objects for access codes management

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

54	Codes	Store request	4 bytes	C	-	W	-	-	entrance access
55	Codes	Delete request	4 bytes	C	-	W	-	-	entrance access
58	Codes	Store/delete request result	4 bytes	C	R	-	T	-	entrance access
60	Codes	Number request	1 byte	C	R	W	-	-	counter pulses (0..255)
61	Codes	Number reply	2 bytes	C	R	-	T	-	pulses
64	Codes	Erase request all	1 bit	C	R	W	-	-	boolean
65	Codes	Out of space	1 bit	C	R	-	T	-	boolean
68	Codes	Request by index	2 bytes	C	R	W	-	-	pulses
69	Codes	Reply by index	4 bytes	C	R	-	T	-	entrance access
76	Access	Simulation	4 bytes	C	R	W	-	-	entrance access
78	Access	Try result	4 bytes	C	R	-	T	-	entrance access

CO 54 e 55 – Store/Delete request

They are used to save and delete access codes in the internal memory of the keypad (same function as CO 52 and 53, paragraph 3.6.6).
The 4 bytes format is type DPT15.000 "entrance access"; the values to be written are in hexadecimal format; example of values to be attributed to these CO:

0x12, 0x34, 0x56, 0x00

Length 6 digits, code 123456, the last byte is not significant.

0x12, 0x34, 0x00, 0x00

Length 4 digits, code 1234, the last byte is not significant.

By writing CO 54, the code will be stored, unless it is already present.
By writing CO 55, the code will be erased from memory only if it is present.
As a result of writing CO 54 or 55, there will always be response from the keypad on the CO 58.

In the first 3 bytes, the answer contains (2 bytes if 4-digit code) the code that is the object of the command. Then, in case of trying a storage:

- if the storage is successful, the response contains flags D=1 and P=1
- if the storage fails, the answer contains the flag E=1

In case of attempting a cancellation:

- if the cancellation is successful, the answer contains the flag P=1
- if the cancellation is unsuccessful, the answer contains the flag E=1

Below, the description of the DPT15.000 directly from the documentation of the KNX standard.

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	UUUUUUUU | UUUUUUUU | UUUUUUUU | bbbbNNNN
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

CO 58 – Store/delete request result

It represents the message emitted by the keypad as a result of writing or deleting an access code using the communication objects described above (CO 52, 53, 54, 55). It is useful for any supervision software that manage the list of access codes and take care of storing and deleting these codes in the keypad. This CO is in DPT15.000 format.

CO 60 e 61 – Number request/reply

CO 60 is a 1-byte message that asks the keypad for information about the amount of managed codes.

The answer from the device to the interrogation happens on the CO 61, that has dimension 2 bytes.

The values expected in writing/reading are:

- CO60 = 1 <-> CO61 = number of access codes currently stored in memory
- CO60 = 2 <-> CO61 = number of codes available for storage
- CO60 = 3 <-> CO61 = total number of codes managed by the device (1000)

CO 64 – Erase request all

If written with value 1, it requires the deletion of all access codes stored in the keypad.

CO 65 – Out of space

It reports the out of memory space for access codes. If the device emits the value 1 on this CO, it means that no other codes can be stored.
It can be issued as a result of storage or cancellation commands and is always issued when the device is switched on and at the end of the ETS application download.
After storing the last available code, this object is notified with a value of 1 to indicate that there is no more memory available.
On this object the value 0 is notified when a code or all the memory is deleted and it is possible again to store new codes.

CO 68 – Request by index

CO 68 is a 2 bytes message that asks the keypad for information about a specific code memory location. The value written in this CO must be between 0 (index of the first valid position) and the maximum number of codes that can be stored, minus 1 (999). The answer to writing will be on CO 69.

CO 69 – Reply by index

It represents the response to CO 68 in DPT15.000 format.
If a code exists in that location, then it will be returned in the first 3 bytes (2 bytes if 4-digit code) and the flags D=1 and P=1 will be set.
Conversely, if in that location there is no code, the first 3 bytes will be set to 0 and the flag E=1 will be set.

CO 76 – Simulation

This communication object allows to send an access code from the bus to attempt access. It is like simulating the user entering the code digits on the keypad.
The data structure is always DPT15.000, where in the first 3 bytes (2 bytes if 4-digit code) the access code must be inserted and in the fourth byte the flag P=1 must be set.

CO 78 – Try result

Every time someone tries to access by entering a code in the keypad (even writing on CO 76), this communication object will notify the result of the operation; the data format is DPT15.000: in the first 3 bytes will be transcribed the code that is being used

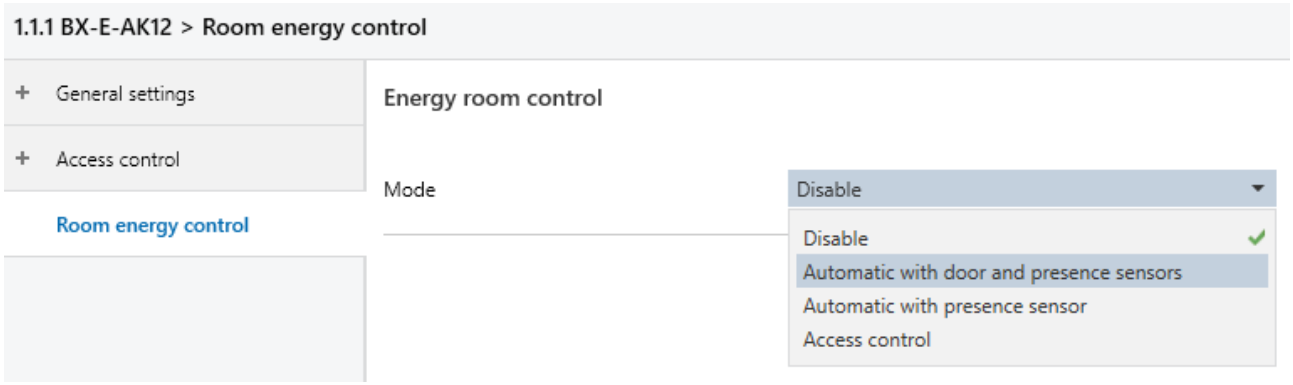
to try to access. If access is successful, the P flag will be set to 1. If access fails, all flags will be 0.

3.7 Room energy control

The keypad includes the management of the automatic detachment/connection of the energy of the room; this functionality is normally used in hotel rooms and accommodation facilities.
The function is configurable in different modes depending on the installation needs. The result of signal processing and integration with other configuration parameters allow to control an actuator (typically relay) that interrupts/connects the energy of the room automatically. With this same logic, it is possible to send other commands to enable/disable room utilities, scenario selection, HVAC mode, thermoregulation.

3.7.1 Mode

Parameterization is different depending on the selected operation mode

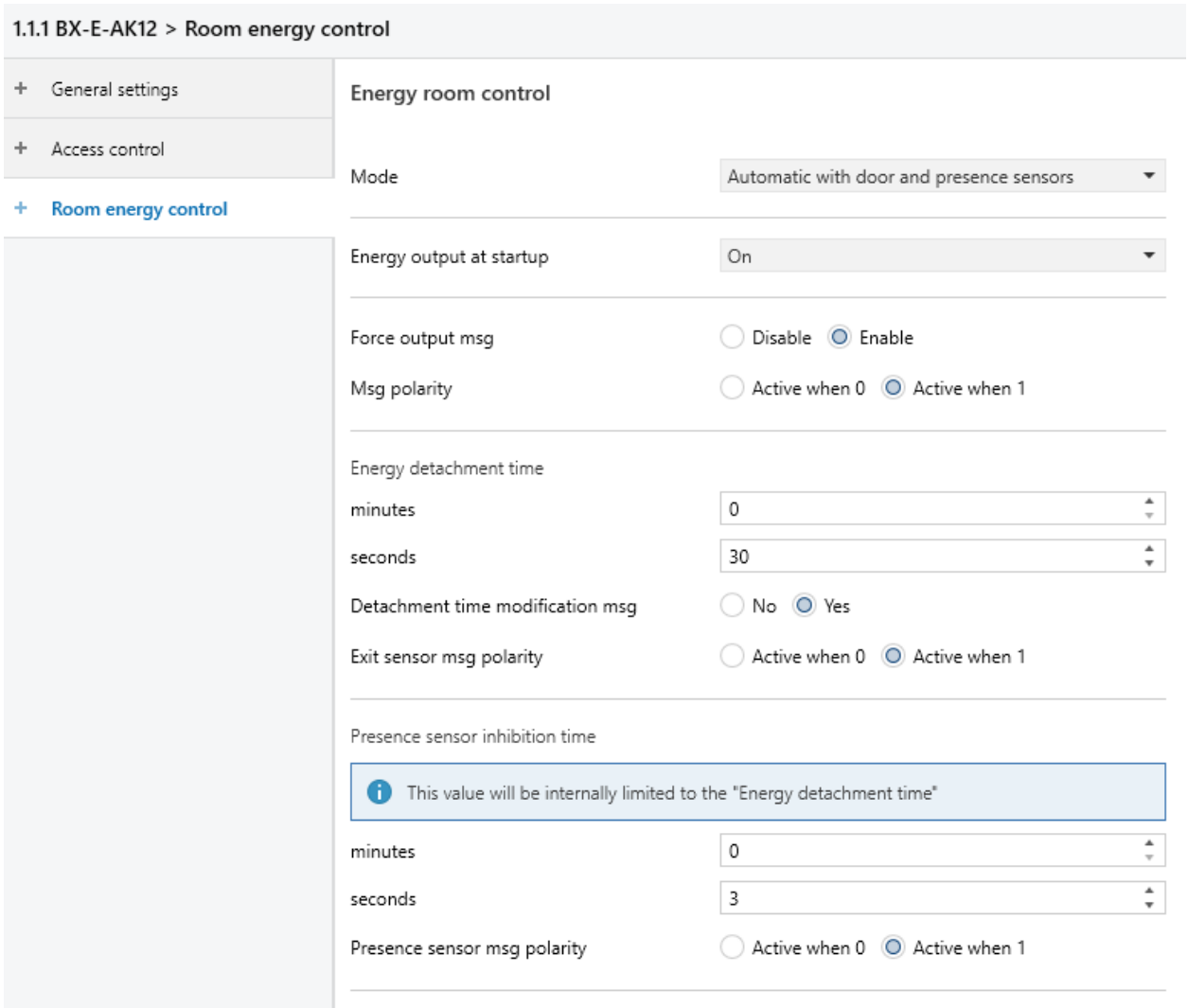


The three possibilities are:
1 – “Automatic with door and presence sensors”
2 – “Automatic with presence sensor”
3 – “Access control”

Mode 1 – “Automatic with door and presence sensors”

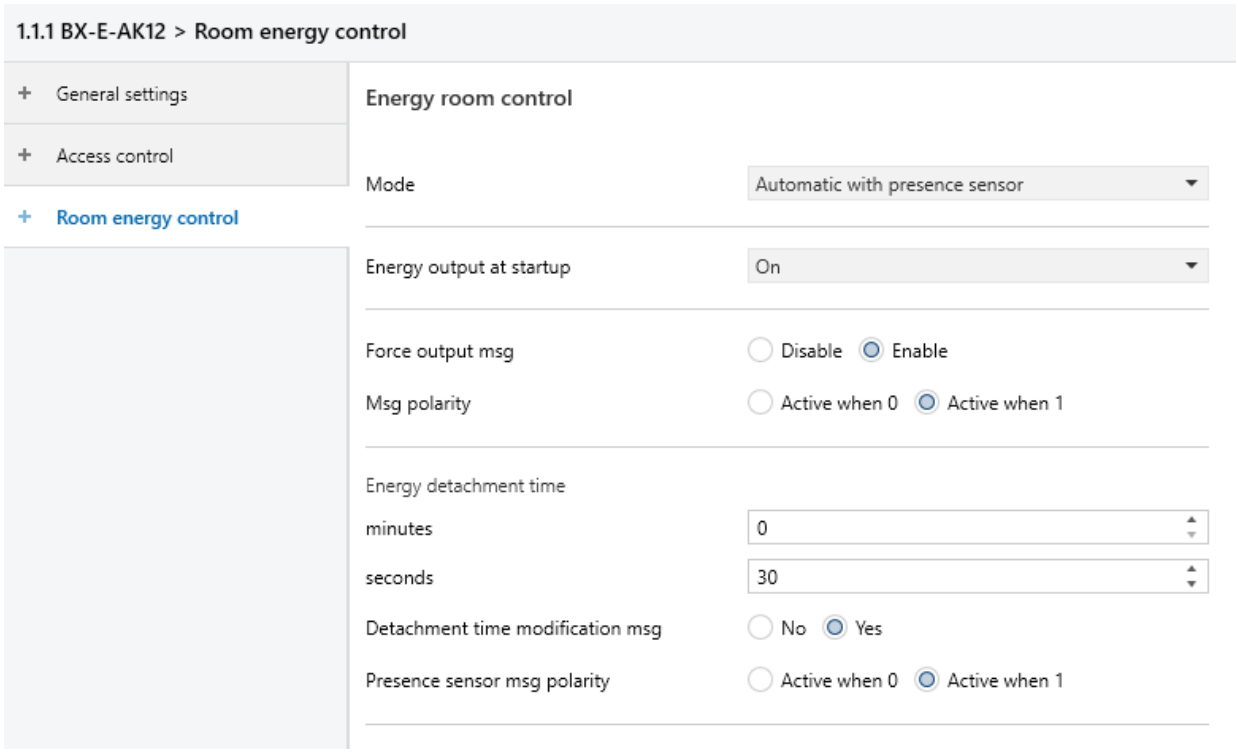
It involves the use of a sensor or microswitch that signals the closing of the door of the room (signals the guest’s exit from the room) and a PIR sensor that detects the actual presence of people in the room (the guest enters or is present in the room).

When the system detects the guest's exit from the room and does not detect any presence in it, it triggers 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 management works by considering the signal fronts 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"

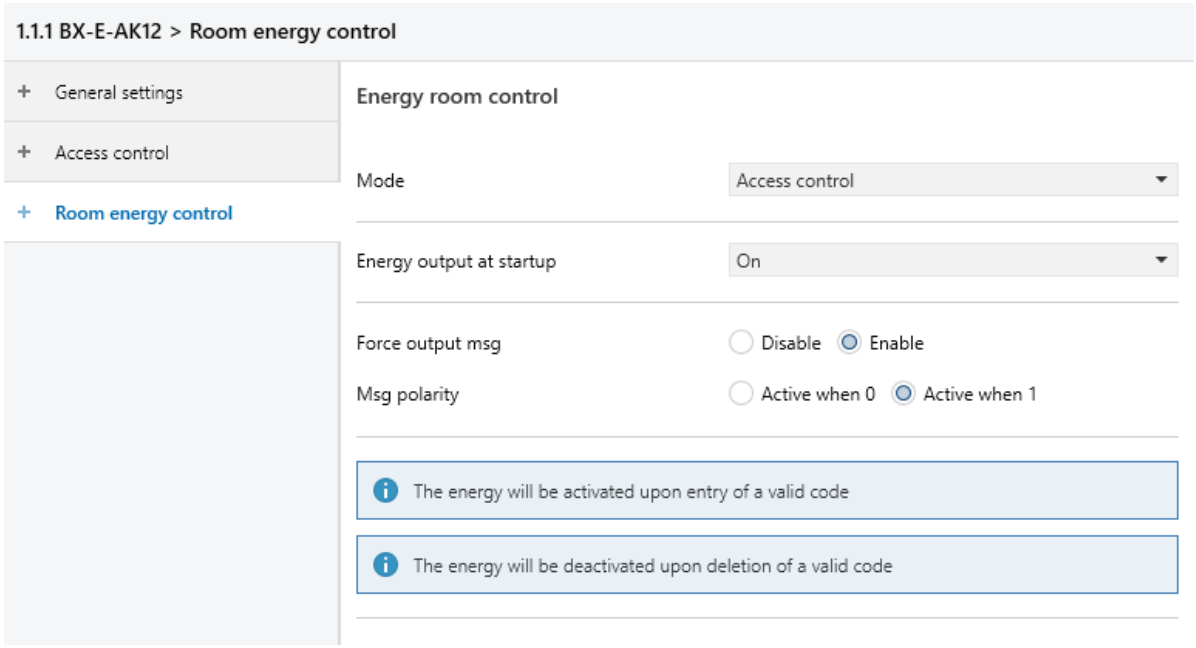
It involves the use of a single PIR sensor that detects the presence of people in the room. When it fails to detect a presence in the room, it starts a timing at the end of which the device will send the disconnection command energy.
If a presence is detected in the room during the timing, the process 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 management works by considering the PIR sensor signal fronts; 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 provide signals from external sensors but the activation/deactivation of the energy of the room depends on the management of the access codes; in particular, we will have the following two conditions:

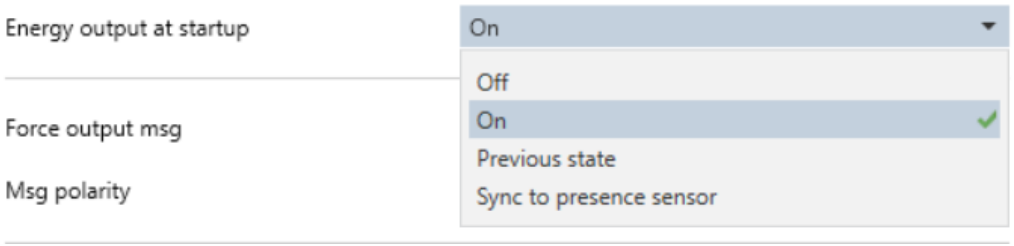
- Input of a valid access code by the user = power on
- Erasing valid access code from memory = power off



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

3.7.2 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 decided by this parameter:



- "Off": power off, sending deactivation messages.
- "On": power on, 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.

3.7.3 Force output msg

It enables the presence of CO 95: by writing it, it is possible to force the state of the energy on or off without considering the logic and the sensors.

In the parameter "Msg polarity" it is possible to specify the activation and deactivation value to be assigned to the CO.

3.7.4 Energy detachment time

In mode 1 - "Automatic with door and presence sensors", it represents the time interval between the user's output (micro-door event) and the actual energy deactivation.
In mode 2 - "Automatic with presence sensor", it represents the interval of time of waiting between the detection of the absence of the guest (free PIR) and the effective deactivation of the energy.

3.7.5 Detachment time modification msg

It enables the presence of CO 96 and 97 modification and feedback of the time of deactivation of the energy.

The value of the parameter "Energy detachment time" can be overwritten with CO 96; the new value is returned on CO 97.

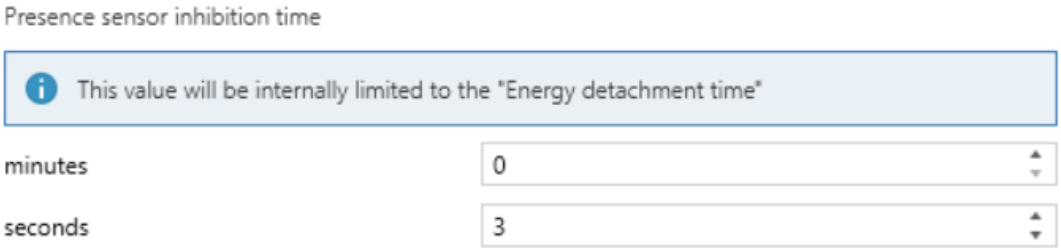
96	Energy room	Set detachment time	2 bytes	C	-	W	-	-	time (s)
97	Energy room	Detachment time status	2 bytes	C	R	-	T	-	time (s)

3.7.6 Exit sensor msg polarity

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

3.7.7 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 deactivation; also the time inhibition is counted starting from the event exit.
During this interval, any activation of the PIR presence sensor will not be considered and then the process will proceed by deactivating the energy at the end of the disconnect timer.
The PIR activations that will ensure that the energy is not deactivated are the ones that occur after the inhibition interval and before the disconnection timer expires.

3.7.8 Presence sensor msg polarity

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

3.7.9 Sensor communication objects

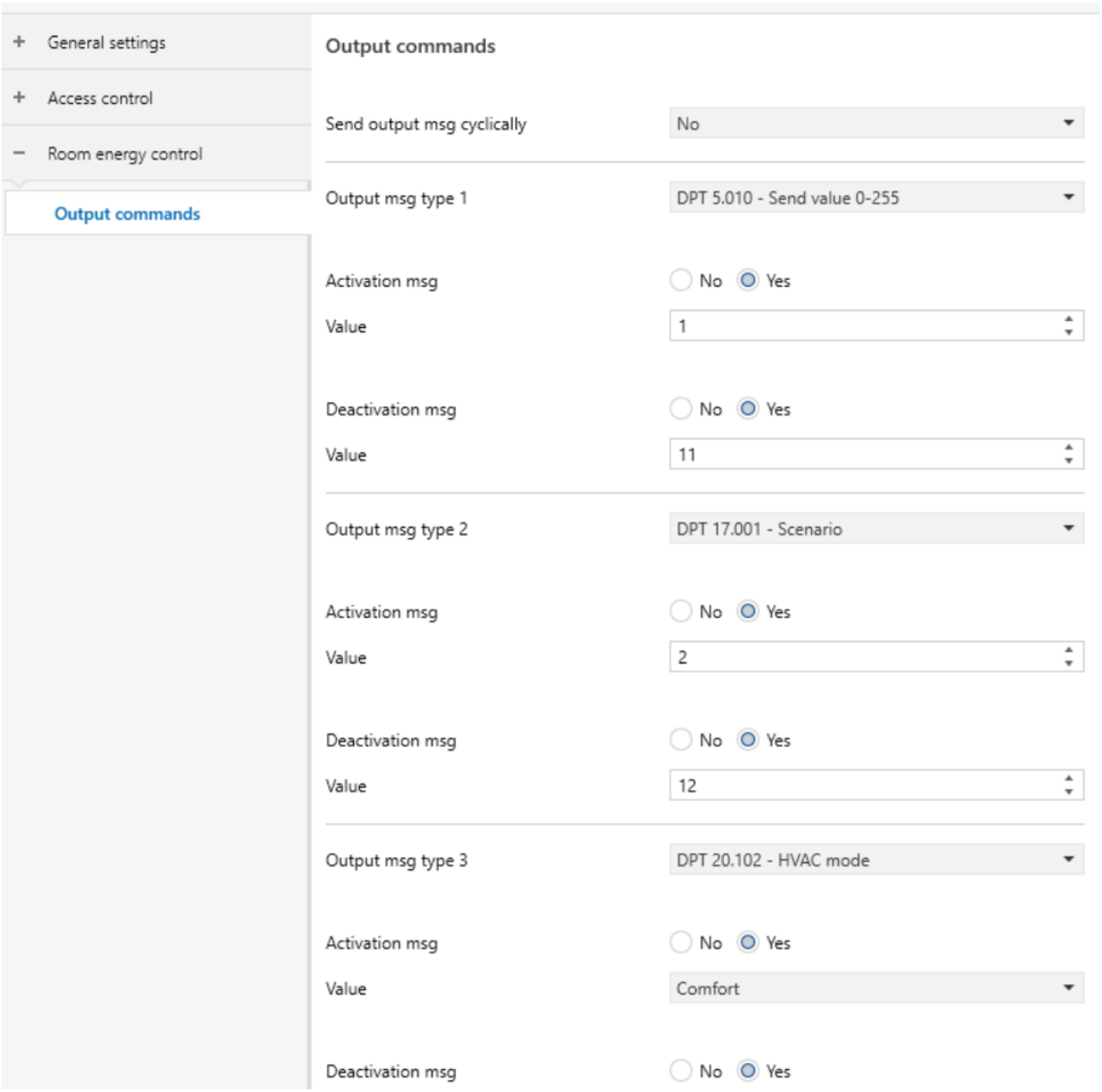
Depending on the mode of operation, it may be present or absent.

The CO 90, a keypad 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.

The CO 91, a keypad 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.

3.7.10 Output commands

All power management modes have a parameter page that defines messages and communication objects to the KNX bus. The processing of the events and signals described for the three modes are translated by the device into KNX 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 msg type X"); the type datapoint 1 bit ("DPT1.003 - Enable") also provides time management of the message.
The output messages are differentiated depending on whether the energy is switched on or off ("Activation msg", "Deactivation msg").
By setting "Send output msg cyclically", it is possible to periodically send the result of the last event on the bus.

Here is an example of CO for 4 output commands:

104	Energy room	Out 1 - DPT 5.010 - Send value 0-255	1 byte	C	R	-	T	-	counter pulses (0..255)
105	Energy room	Out 2 - DPT 17.001 - Scenario	1 byte	C	R	-	T	-	scene number
106	Energy room	Out 3 - DPT 20.102 - HVAC Mode	1 byte	C	R	-	T	-	HVAC mode
107	Energy room	Out 4 - DPT 5.001 - Send value 0-100 %	1 byte	C	R	-	T	-	percentage (0..100%)