2CSN600047D0201 | 30.03.2020

ABB solutions for access control
Installation and use of configuration and management software MiniMAC

1 General information

1.1 Use

MiniMAC software is a tool for the planning, configuration and management of an access control system consisting of products from the ABB range.

1.2 Main functions

- system creation and configuration;
- customer check in/check out, with automated procedure to:
  - enter customer data;
  - assign a room;
  - assign access rights;
  - create or delete a TAG;
- management of customers and staff personal data;
- history and access statistics;
- customer status;
- room status;
- generation of Tag Master for stand-alone systems;
- air conditioning management in single rooms;
- alarm control (for example alarm in the bathroom, technical alarm, fire alarm, etc.);
- load control (for example lighting of common areas, electrical devices, etc.).

1.3 Supported devices

MiniMAC software supports the management of systems consisting of access control devices of they are building automation devices for the integration into a KNX system.

MiniMAC software, as already summarized in previous paragraph, is needed for configuring devices belonging to ABB Access control range. It's important to underline that ABB range includes different devices and solutions with different characteristics and functionalities. In particular, different ABB access control systems can be configured using MiniMAC software:

- ABB access control solution based on 125 KHz contactless technology (available for Chiara, Elos, Mylos wiring accessories range)
- ABB access control solution based on Mifare (13,56 MHz) technology (available for Millenium and Chiara wiring accessories range)
- ABB access control solution based on Mifare (13,56 MHz) technology (available for capacitive sensors range, Tacteo)

These three access control system are all part of ABB range but cannot be included together in the same installation.
They require specific transponder cards (CH/T for 125 KHz devices, TS/T for Millenium devices, TS/T for Tacteo devices) and specific programming device (PRT/U for 125 KHz devices, TR/U configured as programmer for Millenium, TP/T 1 for Tacteo).

The following table lists all ABB devices supported by MiniMAC:

Technology	**125 KHz**				**Mifare (13,56 MHz)**
ABB range	**Elos**	**Chiara**	**Mylos, white**	**Mylos, black**	**Millenium, Chiara**
Transponder reader	LT/U 1.1	LT/U 1.1.CH	LT/U 1.1.MC	LT/U 1.1.MS	TR/U 1.1, TR/U 1.1.CH
Transponder holder	PTI/U 1.1	PTI/U 1.1.CH	PTI/U 1.1.MC	PTI/U 1.1.MS	TH/U 1.1, TH/U 1.1.CH
Transponder programming device	PRT/U 1.1	PRT/U 1.1.CH	PRT/U 1.1.MC	PRT/U 1.1.MS	TR/U 1.1, TR/U 1.1.CH
Transponder reader with POS function	LTP/U 1.1	LTP/U 1.1.CH	LTP/U 1.1.MC	LTP/U 1.1.MS	-

Technology	Mifare (13,56 MHz)
ABB range	**Tacteo**
Card holder conventional	TKK/U.X.X-CG
Card holder universal	TKM/U.X.X-CG
Room outside sensor with card reader	TLM/U.X.X-CG
Room outside sensor with room number and card reader	TSM/U.X.X-CG
USB MIFARE Programmer	TP/T 1

As you can see from the, identification types of the devices following 125 KHz techology are indicated as follows:
- LT/U 1.1.XX for the transponder reader;
- PTI/U 1.1.XX for the transponder holder;
- PRT/U 1.1.XX for the transponder programming device;
- LTP/U 1.1.XX for the transponder reader with POS function.
- TR/U 1.1 Mifare transponder reader (for Millenium range)
- TH/U 1.1 Mifare transponder holder (for Millenium range)
- TR/U 1.1.CH Mifare transponder reader (for Chiara range)
- TH/U 1.1.CH Mifare transponder holder (for Chiara range)

The XX suffix changes according to the type of ABB wiring accessories series associated with the access control device:
- CH = Chiara;
- MC = Mylos, white;
- MS = Mylos, black;
- No suffix = Elos.

The devices will be discussed later with a general reference to the versions without suffix: the descriptions of functionality and configuration obviously apply to all devices in the range, as summarised in the table above.

In the second table there is the list of Tacteo access control devices, based like Millenium on MIFARE (13,56 MHz) technology, but not compatible with Millenium.
In the list of devices there is the generic name with suffix X.X that change according to the specific dimension of device.

1.3.1 Transponders and Transponder reader with POS function (Chiara-Mylos-Elos: 125 KHz)

Transponders (LT/U and LTP/U) are devices to be flush-mounted in 3-module rectangular boxes and are specifically designed for access control installation systems. In addition to this type of application, it provides input and output functions that can be managed via bus and programmed via ETS, which allow you to implement additional automation functions with respect to access control.

The transponder reader allows the user to access a room (or environment or entrance) thanks to a transponder TAG which, once approached to the reader (no need to get in contact with it, in contactless mode), is able to send the authentication data to the transponder reader. The transponder reader is able to decide whether or not to grant the passage (or, more generally, the provision of a service) in a completely autonomous way.
Access Control functions can be adapted to system characteristics and use and can therefore comply with Access Control needs not only of hotel applications but also, for example, of communities, car parks, harbours, offices and plants, fitness and wellness centres, resorts, farmhouses and Bed&Breakfasts.

Authorisation modes
Transponders can be programmed for working in four modes: two "local" and two "central" modes.
1. A "local" authorisation mode means that the reader autonomously decides about authentication,
2. while a "central" authorisation mode means that the decision is taken by a supervisor.

- Authorisation modes are: Local and Central "White list" mode: only users programmed in the individual transponders can be authorised. It is ideal for installations where there are many entrances/environments in which a few users get access (example: hotel rooms).
- Local and Central "Black list" mode: registered users in the single transponders are not authorised. It is designed for installations where there are a few entrances/environments, each of them has to control many users access (example: entrance to a common area such as a parking lot).

Another mode (No TAG) can be defined. It expects that each transponder reader can authorise access only if it receives ON messages coming from the KNX bus on the specific communication object made available by the reader, or if it detects a special TAG (MASTER TAG).

"White" and "Black" lists of the transponder reader in local authorisation mode include:
- up to 65,535 TAG codes (transponder TAG of the CH/T1 type);
- moreover, each TAG is also identified by a "system code" that can have up to 16 millions of different values.

In this way the numerical combinations, which uniquely identify the TAGs that can be generated in an access control system managed by MiniMAC, are virtually countless. Furthermore, up to 128 system codes can be recorded in each transponder reader, which is able to handle up to 8 millions different TAGs (65,535 TAG codes X 128 system codes). In a central authorisation mode, the number of TAG codes and system codes is much higher: in this case, the system controller (MiniMAC software) decides whether to validate a transponder TAG for the access to an entrance/environment and so the number of manageable TAGs becomes equal to the theoretical maximum (2^{40}).

Notification modes
Transponders notify events associated to each transponder card (TAG) in three different ways. Notification means that the reader, after the authorisation of a transponder TAG (customer access to the entrance), sends this information to the system controller (MiniMAC software). Each notification mode is designed in order to enhance performance depending on the installation typology. In particular, they are:

- Spontaneous Emission: The transponder immediately notifies the system controller (MiniMAC) of the authorised operation by sending, through the bus, a telegram containing:
  - moment of authorisation: Year, Month, Hour, Minutes, Seconds;
  - code of authorisation object TAG
  - authorisation result: access granted/denied
- Spontaneous Emission with handshake: similar to the previous one, but MiniMAC sends an "acknowledgement" telegram to the reader.
- Polling: Notifications are stored inside each reader and are not transmitted until MiniMAC requires them.

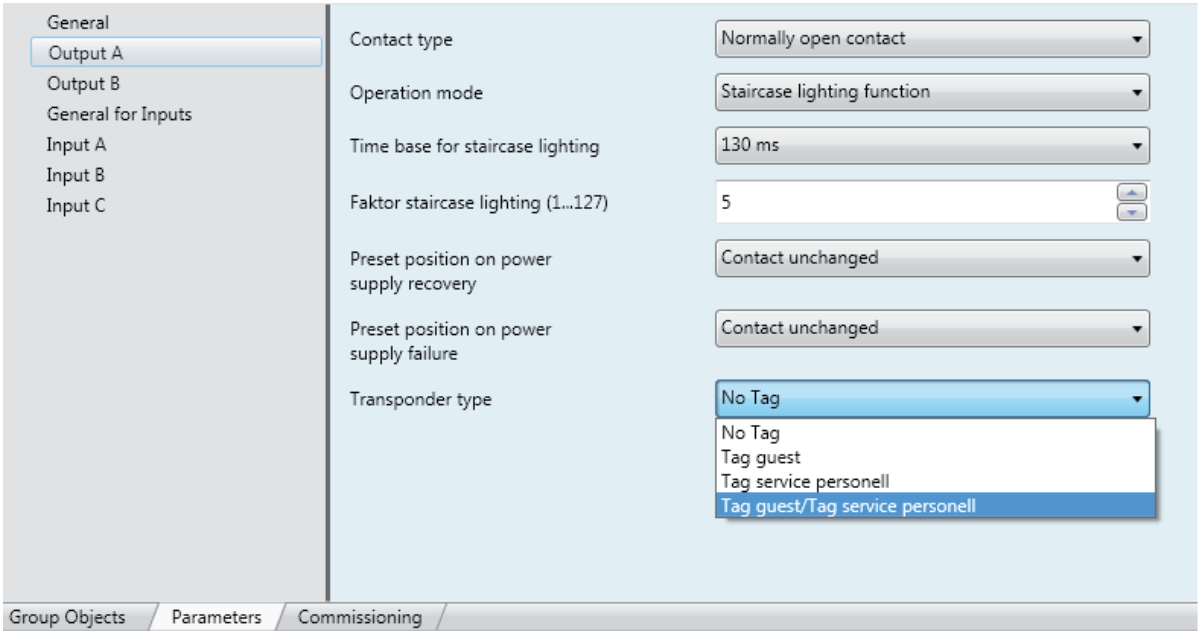
Timeslots and TAG codes expiration time
Transponders are equipped with a clock programmable via bus, so they can work differently in different time slots and handle TAG codes expiration time.
Up to 256 different timeslots can be managed; each of them is derived by 12 elementary timeslots. Timeslots can be set with a precision of one minute and the indication of the day of the week. In any case, the transponders refuse the authorisation of expired TAGs.
Transponder TAGs that are recognised by a reader contain information about System code, TAG type, TAG Serial Number and Expiration Date.

Main features

Transponders accept three types of TAG codes: Customer, Service and Master. Master TAGs allow programming and normal use of the device even if there is no bus communication, thanks to the "Stand-Alone" mode which is made possible by the fact that the reader requires a separate, external power supply (10-32 VDC, 12-24 VAC) in addition to bus power supply. The additional supply is also useful for systems that use bus communication, since it allows the operation of devices even in case of a voltage drop on the KNX bus.

The reader has two 8A latching relay outputs working at 250V AC. One of the two relays is usually programmed via ETS for the automatic door opening control (or, more generally, the provision of a service), depending on the authorisation of the user transponder TAG.

However, it is possible to program the reader via ETS so that one or both outputs are not associated with the authorisation of the TAG (customer or service).



The transponders are also provided with three not opto-isolated, voltage-free inputs, whose scanning voltage is supplied directly by the terminals of the device itself.

4 LEDs on the front panel allow you to monitor device operation and send visual signals to the user over the bus.

Transponder reader with POS function

The ABB device range for access control also comprises transponders with POS function, which are the extension of the basic transponder: actually, they also perform POS functions with electronic wallet mode (prepaid card) or credit card. The Transponder reader with POS function authorises or denies customer access to a payment entrance/environment (i.e. swimming pool, car park, wellness centre, etc.) depending on the credit associated with the customer transponder TAG. In particular, the Transponder reader with POS function recognises up to 4 types of TAGs and applies a customised rate to each TAG. All the rates declared by MiniMAC can be customised for each POS reader.

1.3.2 Transponder holder (Chiara-Mylos-Elos: 125 KHz)

The transponder holder shares all the characteristics of the input-output and bus communication structure with the transponder reader described in the previous section.
The main function of the transponder holder is to manage and control user presence in a certain environment (typically hotel rooms).

In particular:

- Inserting a valid TAG into the reader, the system controller (MiniMAC software) is informed that the customer is inside the room and could use electrical devices. Note that customers are not able to use any electrical device until a valid and not expired transponder TAG is recognised by the transponder holder.
- Removing the TAG previously inserted, the system controller (MiniMAC software) is informed that the customer is leaving the room and that electrical devices are deactivated.
- Inserting specific master TAGs available to service staff into the transponder holder, it is possible to automatically send details on room status to the system controller (MiniMAC software): cleaning, Minibar supply, room status and request for maintenance. This information is useful, for example, to the staff at the reception.

1.3.3 Transponder programming device (Chiara-Mylos-Elos: 125 KHz)

The transponder programming device shares all the characteristics of the input-output and bus communication structure with the transponder reader described in section ***"1.3.1 Transponders and Transponder reader with POS function (Chiara-Mylos-Elos: 125 KHz)"***.
The main function of a transponder programming device concerns its ability to interface, via the KNX bus, the supervision program (MiniMAC) to create and delete Tags (for example, during customer check-in and check-out operations). Both the client and master tag.

1.3.4 Transponder reader (Chiara and Millenium: MIFARE)

The “transponder reader” is a flush-mounting device for British Standard wall boxes, designed to realize access control systems with a communication support based on KNX bus.
It is equipped with:

- one relay (4A @24V AC/DC)
- one input to be used for connecting external conventional card-holder (e.g. Chiara and Millenium wiring accessories card-holder)

The output can be programmed in three different ways:

- “Linked to access control”, receiving in this case switching commands from the device itself (according to transponder card validation). It’s moreover possible to switch the relay according to a standard KNX telegram received from the bus by a KNX device
- Being a standard KNX Switch actuator output, able to be controlled by every KNX-standard devices
- “Linked to card-holder”, that means that the relay is switched according to closing/opening internal input contact available on transponder reader and connected to a conventional card-holder

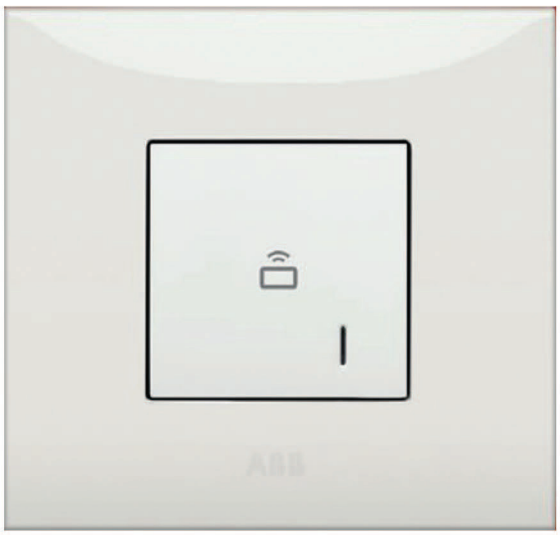
The bicolor (red-green) LED placed on the front of the device allow you to monitor device operation (for example GREEN = card validation ongoing, RED = card not authorized). The LED can be also switched ON/OFF in the proper color according to KNX telegram (for example for DND/MUR purposes).

The transponder reader requires an external power supply enabling its operation even without bus. The transponder reader is available for ABB Millenium and Chiara wiring accessories range.

The following functions are available for the relay output:

- Normal switching
- Staircase lighting function with programmable delay (in “Linked to access Control” and “Actuator” modality)
- delayed OFF with programmable delay (in “Linked to card holder” modality)

The available input can be connected to a conventional card-holder in order to make the transponder reader aware about guest presence/absence in the room, and consequently performing some actions (for example sending 1bit or 1byte notification scenario on the KNX bus) or switching internal relay (this only when the output relay is configured as “Linked to card holder”.



1.3.5 Transponder holder (Chiara and Millenium: MIFARE)

The “transponder holder ” is a flush-mounting device for wall boxes, designed to realize access control systems with a communication support based on KNX bus. It is equipped with:

- one relay (4A @24V AC/DC)
- one input to be used for connecting external conventional devices (such as push-button, door/window contact, ...)

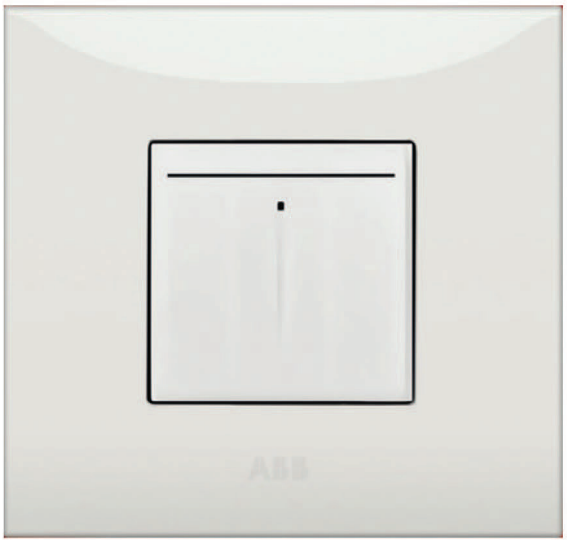
The output can be programmed in two different ways:

- “Linked to access control cards”, receiving in this case switching commands from the device itself (according to valid transponder card inserted/removed into/from the card holder)
- “Being a standard KNX Switch actuator output”, able to be controlled by every KNX-standard devices

The white LED on the front is blinking when the card is not inserted, while is OFF when the card is inserted. In the ETS file is available a communication objects for switching controlling LED behaviour (blinking, fixed ON).

The transponder holder requires an external power supply enabling its operation even without bus. The transponder holder is available for ABB Millenium and Chiara wiring accessories range.

The available input can be used to connect conventional push-button or for example door/window contact. The input can be configured as Switch sensor, Dimmer sensor, Shutter sensor.



1.3.6 Room outdoor sensor with card reader (Tacteo - MIFARE)

The devices are available in the dimensions 86 mm x 86 mm, 86 mm x 115 and 115 mm x 86, they are KNX certified and are provided with:

- 1 output channel with 4A@24V relay.
- 1 “touch” push-button for controlling external door-bell which will be rung by touching the relative icon on the glass panel.
- 3 Illuminable icons on the glass (a make-up-room icon, a do-not-disturb icon, a bell icon) which can be configured via ETS (e.g. bell can be omitted)
- 1 icon with signaling related to card validation: access allowed/denied
- All push-button follow the same common application program of the other Tacteo devices
- All push-button (including the hidden one in the middle) can be configured with Configuration Tool (type of icon, color)

1.3.7 Card holder (Tacteo - MIFARE)

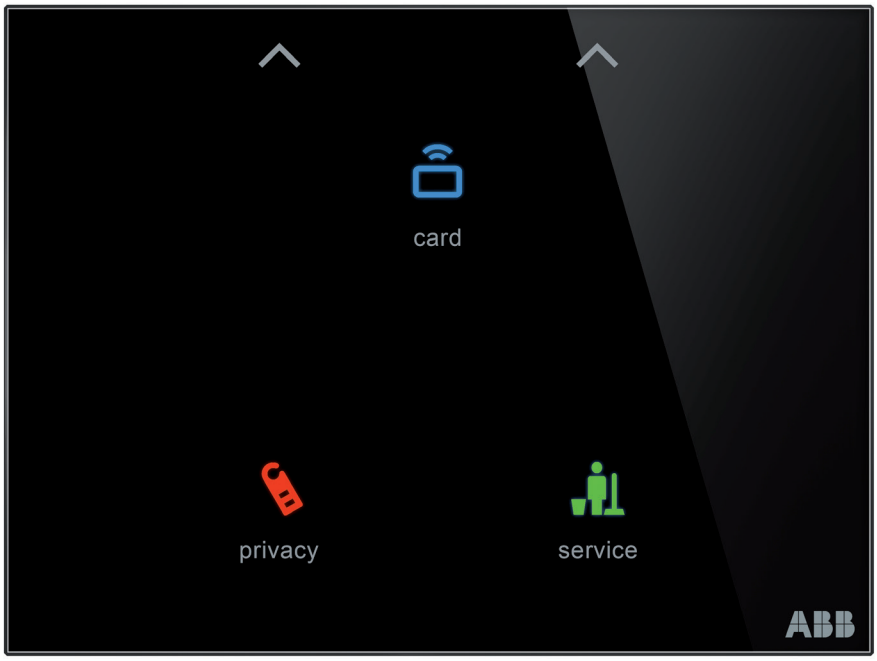
The devices are available in the dimensions 86 mm x 86 mm and 115 mm x 86 mm, they are KNX certified and are provided with:

- 1 output channel with 4A@24V relay.
- 2 push-buttons on the front (corresponding to “make-up room” and “do not disturb” icons), which can be configured through ETS in order to send (with the proper communication objects) a 1-bit KNX telegram, for controlling associated illuminable icons on the glass transponder reader outside the room.
- In the middle there is a third (hidden) push button available.
- All push-button follow the same common application program of the other Tacteo devices
- All push-button (including the hidden one in the middle) can be configured with Configuration Tool (type of icon, color).
- icon with signaling related to card validation: card valid/not valid

On glass panel will be available a card-holder for card insertion, and an illuminable status icon (with signalling related to card validation).

The device can be supplied in two different versions: universal and conventional.

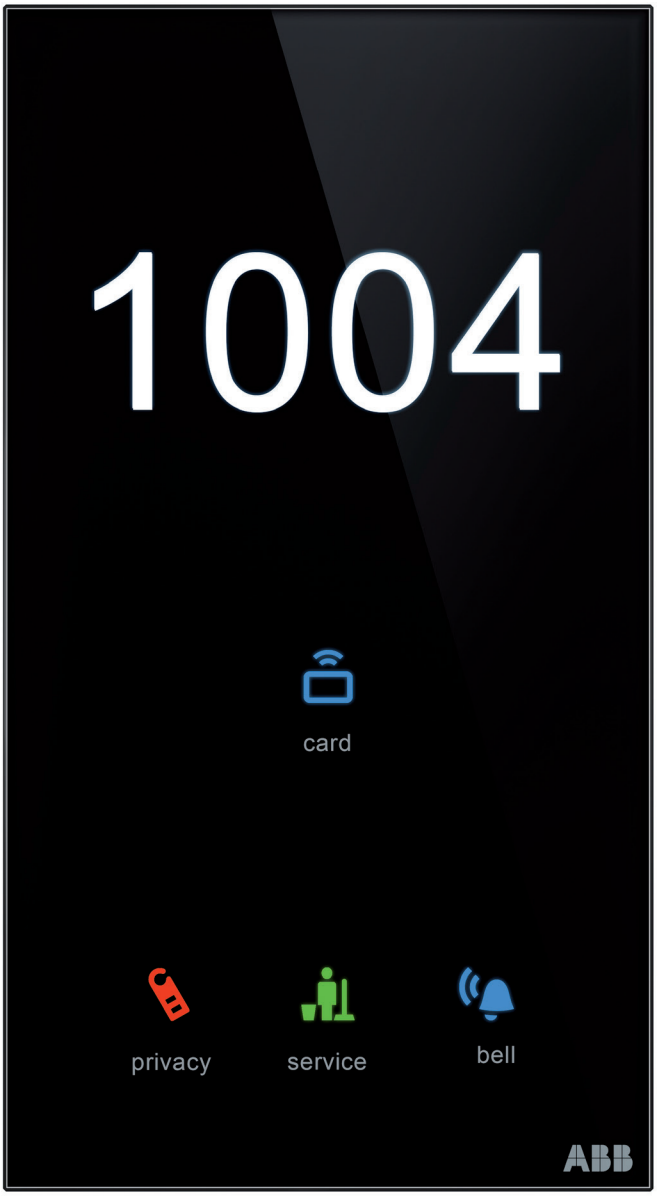
- The universal card holder includes MIFARE antenna and access control capabilities. It works according to valid cards with access control configuration software.
- The conventional card holder includes MIFARE antenna but without access control capabilities (card validation). This means that every MIFARE cards (also not programmed) is able to enable the relay of the output channel included in the device.



1.3.8 Room outdoor sensor with card reader and room number

The device is available in the dimension 86 mm x 157 mm, it is a KNX certified device and it is provided with:

- 1 “touch” push-button for controlling external door-bell which will be rung by touching the relative icon on the glass panel.
- 1 output channel with 4A@24V relay
- Illuminable icons on the glass (a make-up-room icon, a do-not-disturb icon, a bell icon with touch capabilities) which can be configured via ETS (e.g. bell can be omitted).
- icon with signaling related to card validation: access allowed/denied
- The indication of the room number on the display (the room number indication will be ON/OFF switched by a KNX communication).
- All push-button follow the same common application program of the other Tacteo devices
- All push-button (including the hidden one in the middle) can be configured with Configuration Tool (type of icon, color)



1.3.9 USB Programmer – MIFARE

For Tacteo Access Control range it is needed a USB Programmer (TP/T 1) for programing (writing/deleting) cards used in the installation. The USB programmer connects directly to the PC using the USB cable.

1.3.10 Room thermostat

In an access control system based on bus communication, the traditional devices described in the previous sections (reader, transponder and programming device) can be integrated with other devices in order to implement a complete building automation system, also controlling other functions such as lighting, shutters, temperature regulation, etc.
In particular, a room thermostat is foreseen for hotel applications to allow the user to adjust the temperature (setting of the desired setpoint). As explained in section ***"4.7 Heating and Cooling Supervision"***, MiniMAC interfaces with the thermostats so that room temperature regulation can be managed from the reception. The ABB range offers different thermostats for room temperature regulation that can be controlled by MiniMAC in an access control system:

- Mylos KNX thermostat;
- Generic ABB KNX thermostat.

1.4 Installation

Access Control devices are able to provide its services only if connected to the communication bus.
“Stand-Alone” operation is possible, but only manual programming through Master cards is possible. In this mode, the only operations that can be performed are card validation and door relay control.
In “Stand-Alone” operation date and time cannot be set and the access control device does not handle timeslots and TAGs expiration. TAGs programming with a far expiration time is a good practice in order to avoid a rejection during the authorisation process: initially every device has the programmed date January 1st 2000, which is updated during device operation.
Installing a system without a Bus requires the devices to be connected to the electrical system, as described in the previous sections. Furthermore, the devices can be “locally” programmed by MASTER TAGs that are created by MiniMAC with the procedure described in the specific section ***“7.6 Master TAG management”***.

2 Configuration of the access control system

2.1 Filters

ABB access control can work in two different modes:
1. Stand-alone;
2. Using bus communication.

In access control systems integrated in a KNX bus installation, Access control generates telegrams notifying each transit during its operation. Generated traffic on the bus cannot be predicted a priori and depends on factors that vary from installation to installation. These factors are:
- Number of transponders in the system
- Use of the system by customers: Number of transit telegrams generated.

Since the system's quality of service and supervision is lower when the generated bus traffic increases, **much attention must be paid in order to limit data traffic on the KNX installation main line**. To this end, the use of filters associated to line couplers is recommended in order to block messages sent to the main line and unimportant for the devices not connected to the local line. A good design practice foresees the assignment of the same address group to all the devices that have to be connected to the same line. Messages related to the devices connected to the same line are blocked and do not reach the main line.

2.2 Access Strategy

The Access Strategy sets the rules to be followed for granting or denying the access to a TAG that requested the access to a transponder reader. Two main access Access Strategy can be chosen.

2.2.1 Localized access strategy

It's the device itself that decided to allow access to the gate/room controlled by transponder reader.

2.2.1.1 Local White List

How it works

Each device set up in White list has a list of TAG serial numbers. The transponder grants access **only** to TAGs whose serial number is in the White list.
Use of a White List means **denying access to everyone.** Entering a TAG in the White List represents an exception. It can be done only when authorised customers are considered an "exception" to the total of customers to whom a TAG is assigned.

When to use it

White List use is recommended when there are **many transponders** in the installation and a few customers (TAGs) are authorised.
Using White Lists, the system can control those who have the access right: only those customers having a TAG in the White list can get access.
Example: in a hotel installation, in customers' rooms. Only those customers having a valid TAG, who checked-in for a certain room, have the right to enter that room.

2.2.1.2 Local Black List

How it works

Each device set up in Black List has a list of TAG serial numbers. The transponder **grants** access **only** to those TAGs which **do not** have a serial number in its Black List.
Use of a Black List means **granting access to everyone.** Entering a TAG in the Black List represents an exception.
It can be done only when unauthorised customers are considered an "exception" to the total of customers to whom a TAG is assigned.

When to use it

Black List use is recommended when most of the customers (TAGs) are authorised by transponders in the installation.
Example: in a hotel installation, customers and staff with a valid TAG (valid system code, non-expired TAG, etc.) must be authorised to access **common areas and main entrances**.

2.2.1.3 No tag

Authorisation mode available only in transponder holder. It is a simplified system for TAG validation. Its operation assumes that:

- the transponder holder is inside a hotel room
- Room accesses are controlled by a transponder

Therefore, a customer wishing to validate a TAG inside the transponder holder has already been controlled by the transponder reader outside the room. However it does not happen that with NO TAG access strategy configuration any type of card activate the electrical loads connected to the transponder holder: transponder holder controls/checks System code and expiration date on the card/TAG, and only cards for which there is valid match with System Code and Expiration date activate the electrical loads. The transponder holder can be configured with a Black List if a more accurate control is required. However, this does not allow activation of the White List or central modes (see next section).

2.2.2 Centralized access strategy

With the centralized operation, the result of the application of authorizations is submitted to the supervision software (MiniMAC).
White list/black list available, as for localized access strategy.

Warning
Pay attention: if MiniMAC/KNX bus is not available, the decision cannot be taken and opening the door is not possible

2.2.3 Access Strategy Selection

Local White List	To be used for entrances where transit is allowed only to a few customers. Example: all restricted areas. Hotel rooms. Areas reserved to the staff and not for hotel customers. All areas requiring strict control of those who have an access right. The White List shows all those who use a transponder to gain access. Therefore, it is easy to keep under control who gains access and who does not.
Local Black List	To be used for entrances where transit is allowed to most customers. Example: all common areas of an installation. Main entrance/exit of the building. All customers, regardless of their specifications, access main entrances indistinctly. Parking lots.
Central (White List or Black List)	To be preferred when: Authorisation to access an entrance is limited to the presence of the supervisor (PC with MiniMAC), which must be running and connected to the installation. Fast programming and database update are required.
NO TAG	Only for transponder holder

2.3 Notification mode selection

Every time the transponder is activated for validation of a TAG, it records the event and transfers it to MiniMAC supervisor software.

Notification mode regulates information exchange from transponders to the supervisor (MiniMAC) following up an access request. Thus the supervisor records such information in the Data Base, which can be consulted by MiniMAC users (e.g. reception clerk).

Note
Notification mode can be selected only when the transponder is connected to the bus. A system in stand-alone mode does not provide any notification mode because the transponder does not communicate with the supervisor (MiniMAC).

How to choose the notification mode:
1. Need of controlling/limiting data traffic coming from transit notifications.
2. Speed with which transits information is updated inside the data base.

The choice of the notification mode directly affects the type of authorisation that can be set up in transponders.
ABB access control provides four notification modes, three for the local access strategy and one notification mode for central access strategy:

Access strategy	Notification mode
Local	Spontaneous Emission
	Spontaneous Emission with handshake
	Polling
Central	Central

2.3.1 Spontaneous Emission

Note
The transponder sends to the supervisor (MiniMAC) a KNX telegram as soon as TAG validation is terminated.

Information in the telegram sent by the transponder to the MiniMAC is:
- TAG number;
- Date/hour/minutes/seconds (with a 10 seconds accuracy);
- Authorisation result = granted/denied

MiniMAC receives the telegram and updates the Data Base with the information received, so the access history can be consulted.

Warning
When the transponder is not able to send the telegram to destination due to collisions on the bus/unavailability of communication with MiniMAC, information is recorded in the internal memory and is not lost.
(The transponder can record up to 255 transits on 125 KHz range, 64 transits on MIFARE range. When the memory is full, the oldest memory record is replaced with the new one).

2.3.2 Spontaneous Emission with handshake

This notification mode is similar to the previous one but it is designed to quickly unload transits memory inside transponders; it ensures telegrams recording inside the database.

Note
In this notification mode, the telegrams management service (integrated in MiniMAC) sends an acknowledgement telegram to the transponders that have sent a notification telegram.

When the transponder transits memory is not empty:

- The acknowledgement telegram is used by the device as confirmation to download other transits that might have accumulated inside the transits memory.
- Upon the reception of a notification telegram, the telegrams management service sends a new acknowledgement telegram to the transponder which can keep sending telegrams until the memory is empty or a confirmation telegram gets lost.

2.3.3 Polling

Note
This notification mode has been designed to rigorously regulate the number of telegrams that are exchanged on the bus.

In this mode, transponders do not immediately send notification telegrams on the bus. All transits are registered inside the transponders' internal memory, which can record up to 255 transits on Chiara-Mylos-Elos range, 64 tranansits on Millenium and Tacteo range.
MiniMAC, by means of its Telegrams management service (ACC), requests individual transponders transits information. The protocol is:

- Scan of the list containing the devices working in polling mode.
- For each device, MiniMAC requires the number of registered transits.
- If this number is higher than a certain threshold (parameter set in MiniMAC), MiniMAC requests transponders to communicate a limited number of transits, whose amount is programmed in MiniMAC.
- If the number of registered transits is lower than the programmed threshold, transits request is ignored. When the number of ignored requests is higher than a programmed value and the transponder has some registered transits, MiniMAC requests the transponder to communicate all its transits.
- If the transponder memory is 75% or 100% (only these two thresholds can be programmed), the device sends a warning telegram to ACC, which stops devices scanning and requests the transponder to communicate its transits.

The frequency with which a transponder sends telegrams on the bus is limited to 3 telegrams per second. Therefore, the maximum Bus activity required by polling is 3 telegrams/sec. Furthermore, all parameters previously described can be set in order to reduce the **average** throughput required by the polling to very low values.

2.3.4 Central Notification Mode

In central mode, TAG validation is not performed by transponders but directly by the MiniMAC. Indeed the transponder sends a telegram with the required information to validate or not the TAG to MiniMAC, which decides whether to grant or deny the access.
This way, there is no delay from the authorisation to the event registration in the database. Therefore, central mode ensures that all transits are certainly registered.
However, to end validation, if access is authorised, the MiniMAC must send a telegram to the transponder to confirm the opening. In short, to have a door opening, two telegrams must be exchanged: request (from transponder to MiniMAC) and access confirmation (from MiniMAC to transponder). If MiniMAC does not authorise the opening, it does not send any telegram and the transponder denies the access after a 5 seconds timeout, waiting for the next TAG reading.

2.4 Access strategy and Notification mode

Note
MiniMAC makes available a number of different combination for Access strategy and Notification mode
In most of the applications it's recommended to don't touch these configuration and use the default value

- Access strategy = localized (White List or Black list)
- Notification mode = Spontaneous Emission

Default values grant good performances in every kind of application

2.5 System codes

System codes are essential elements for proper TAG authentication and validation.
A system code is a number ranging from **1 (One)** to **16,777,215**.
Note that **0 (Null) is NOT A VALID system code.**
Each transponder can record up to 128 different system codes in its internal list (with MiniMAC if the system is set up with KNX bus communication, via Master TAG in case of a stand-alone system).
In order for a TAG to be recognized by a transponder and start validation, the TAG to use for door opening must have a system code which is present in the transponder list of system codes.

2.5.1 How to and why use system codes

- System codes help to create a first TAG discrimination factor during validation. System codes may be used to create different TAGs' logic groups in the same installation. Since the number of possible system codes' combinations is really high, a TAG created for an ABB Access Control System customer 'x' cannot be recognized by an ABB Access Control System of customer 'y'.
- System codes may be created to create different TAGs' logic GROUPS in the same installation. To these logic groups can correspond different cases, as for example:
  - A complex of several buildings, where users of a building have no right to access other buildings.
  - Several sectors in a building, where users of a sector have no right to access other sectors.
  - NOTE: each transponder can recognize up to 128 system codes. Therefore, two parts of the same installation having different system codes can always be merged. Merging is achieved entering more system codes in the transponders' list.
- An example of code merging could be a big company having several offices in different sites. It is logical to assume that each office has a different System code to differentiate its TAGs. On the other hand, it is also expected that, for example, employees of office A can access offices C and F but not other ones. In order to make it possible, transponders in offices A, C and F must be set up to recognize system codes assigned to A, C and F, but must not able to recognize system codes assigned to other offices.
- TAGs sharing the same system code can be simply, instantaneously and simultaneously disabled by removing their system code from the transponders' lists.
- A specific system code must be assigned to Master TAGs to differentiate them from others. The illicit use of a stolen or lost Master TAG can be prevented quickly and effortlessly by removing Master TAGs' system code from the system. Other TAGs (customers and service) will still be working without any problem.

2.5.2 Operation suggestions

1. Values to be assigned to system codes should be RANDOMLY chosen from the large range of available values (1 to 16 millions).

Warning
A progressive assignment starting from 1 must be avoided: two access control systems could likely share the same system codes. Such a situation does not cause any system malfunctioning but reduces the security level of your access control system.

2. Reserve a particular system code to Master TAGs. Better would be a different system code for each Master TAG.
3. Reserve a system code for customers' TAGs.
4. Reserve a system code for staff TAGs.

2.6 Programming procedure through Master TAGs

Warning
In order to understand the installation procedure here described, the reader should be aware of the following concepts:
Authorisation policies or TAGs validation
Use of system codes
TAG generation mode using MiniMAC
Reading of the chapters dealing with these subjects is recommended before reading this section.

Warning
Please remember that Programming procedure through MASTER TAGs is supported only by Chiara, Elos, Mylos range. Millenium adn Tacteo range does not support this procedure and therefore creation of MASTER TAGs related to programming in the specific menu (see ***"7.6 Master TAG management"***), although available, is not working.

Procedure description:

1. Using the "Insert System code" TAG, enter the first system code.
   A. If the system codes list is empty, the system code of the "Insert System Code" TAG will be entered.
      - Using the "Insert System Code" to add system codes will be successful if the "Insert System Code" TAG has a system code in the list.

   B. LED no. 2 remains lit up orange until the "Insert System Code" TAG is reinserted a second time or 5 seconds have elapsed.
   C. Entering a system code is necessary because the device does not recognize TAGs with a system code not present in its list. Warning: each Master and not Master TAG needs a system code in the transponder list in order to be used for the following operations.
2. Enter any further system codes using any type of TAG as long as it contains the system code you want to set.
3. Optional: Remove one or more system codes from the device: you can use the "Remove system code" master TAG. After doing this, the LED 2 turns orange, then use any type of TAG containing the system code you want to remove from the transponder. LED no. 2 remains lit up orange until the "Remove System Code" TAG is reinserted a second time or 5 seconds have elapsed. There is also the "Reset system codes list" TAG which resets the list immediately. Use it carefully.
4. Enable the device through the "Enable MAC" TAG. Access control devices are factory-set as "Disabled".
5. Set the local authorisation mode: white list or black list (central mode is not available in a "Stand-Alone" system).
   A. Use the "set white list mode" master TAG or
   B. Use the "set black list mode"master TAG
6. Enter the TAGs you wish to create in the White or Black list.
   A. The White list must contain customer/service TAGs with the rights to access the service:
      - There is a specific Master TAG ("**Insert in White list**") to add the TAG numbers which will be subsequently inserted in the transponder white list.
      - Insertion Mode stays active (orange LED 2 on) until the "Insert in White List" TAG is inserted a second time or a few seconds have elapsed.

A. The Black list must contain customer/service TAGs without the rights to access the service:
   - There is a specific Master TAG ("**Insert in Black list**") to add the TAG numbers which will be subsequently inserted in the transponder black list.
   - Insertion Mode stays active (orange LED 2 on) until the "**Insert in Black List**" TAG is inserted a second time or a few seconds have elapsed.

7. **Optional:** White or black list items removal
   A. The White list must remove the customer/service TAGs which no longer have the rights to access the service.
      - There is a specific Master TAG ("**Remove from White list**") to remove the TAG numbers which will be subsequently inserted in the transponder **White list**.

- Removal Mode stays active (orange LED 2 on) until the “Remove from White List” TAG is inserted a second time or a few seconds have elapsed.
- The “Reset White List” master TAG can be used to delete all elements in the white list. “**Reset White List**” master TAG - This operation must be performed carefully.

B. The Black list must contain customer/service TAGs with the rights to access the service.

- There is a specific Master TAG (“**Remove from Black list**”) to remove the TAG numbers which will be subsequently inserted in the transponder **Black list**.
- Removal Mode stays active (orange LED 2 on) until the “Remove from Black List” TAG is inserted a second time or a few seconds have elapsed.
- The “Reset Black List” master TAG can be used to delete all black list elements. **“Reset Black List”** master TAG - This operation must be performed carefully.

Note 1
Customer/Service TAGs to be inserted in the transponder lists have to be created before entering them into transponder White or Black lists.

Note 2
Master TAGs called “Unconditional Opening” and able to access everywhere can be programmed by MiniMAC. They make the transponder open the door and they only have a valid system code (in the transponder list). These TAGs never expire and do not need to be entered in White lists (or not entered in Black Lists) and to be associated to time slots.

Note 3
The set of available Master TAGs includes more MASTER TAGs than those used so far. In any case MASTER TAGs commonly used are those just described:
Open! - “Unconditional Opening”
“Insert System code”
“Remove System code”
“Reset System code List”
“Set White List Mode”
“Set Black List Mode”
“Insert in White List”
“Insert in Black List”
“Remove from White List”
“Remove from Black List”
“Reset White List”
“Reset Black List”

Warning
Good practice is to save a specific and reserved system code only for MASTER TAGs and adopt other system codes for all other TAGs (system codes used for customer/service TAGs).

This expedient allows solving unpleasant events such as

- Theft
- Loss
- Improper use of Master TAGs.

Indeed, in case of a Master TAG theft or loss, its system code can be disabled in order to avoid fraudulent use of the missing TAG.
All Master TAGs with the same system code cannot be used any more (therefore, fraudulent use of a lost or stolen Master TAG can be avoided). At the same time all customer/service TAGs in the system transponders can still be used. In order to end the emergency procedure, the Master TAGs need to be re-programmed with a new system code and this code (if not already present) has to be entered inside the system transponders. The customer/service TAGs already in the transponder lists will be preserved by these operations and do not require interventions.

Warning
Programming of a device through Master TAGs is possible also when the transponders are connected to the KNX bus:
The use of master TAGs in a system where the bus connects all devices must be avoided.

This is suggested because each operation made through a Master TAG is not under MiniMAC supervision, which consequently **cannot keep track of each operations performed by means of a Master TAG.** This way, MiniMAC cannot get a correct vision of the real system situation and the quality of service cannot be guaranteed putting at risk fundamental Access Control functions.

Note
Always use MiniMAC to configure the system once connected to the bus and use Master TAGs for the “Stand-Alone” operation.

.

3 Software installation

3.1 Minimum system requirements

We recommend to check your system compliance with MiniMAC installation requirements.

Operating system:	Windows XP, Windows 7, Windows 10
Memory:	1 Gbyte
Fixed disk capacity:	150 GBytes available.

However, it is recommended to give MiniMAC the exclusive use of PC resources: the full effectiveness of the program is not guaranteed (and the warranty is no longer valid) if there are additional programs on the computer where the installation of MiniMAC resides.

3.2 Network configuration

In order to enable more security of the system, MiniMAC software should be installed on a PC not connected to external network (Internet/web). It is in general responsibility of the system integrator guarantying the right configuration of protection tools for the PC (firewall, antivirus, ...).
When protection tools such as firewall or antivirus are installed, it is important to configure correctly the right exceptions in order to make possible for MiniMAC working correctly. In particular remember to add the following exceptions in firewall/antivirus:

- ABB_ACC_Service.exe
- MiniMAC41.exe

These executables are usually installed in the following folder (C:\Program Files (x86)\ABB\MiniMAC4).
Networks ports used by MiniMAC software are the following ones, that need to be opened in the firewall configuration:

- 6501/TCP
- 6543/TCP
- 8100/TCP
- 9000/TCP

3.3 Cyber Security Statement

MiniMAC software is designed to be connected to and to communicate information and data via a network interface, which should be connected to a secure network. It is your sole responsibility to provide and continuously ensure a secure connection between the product and your network or any other network (as the case may be). You shall establish and maintain any appropriate measures (such as but not limited to the installation of firewalls, application of authentication measures, encryption of data, installation of anti-virus programs, etc.) to protect the product, the network, its system and the interface against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB Ltd and its entities are not liable for damages and/or losses related to such security breaches, any unauthorized access, interference, intrusion, leakage and/or theft of data or information.

3.4 Additional software required

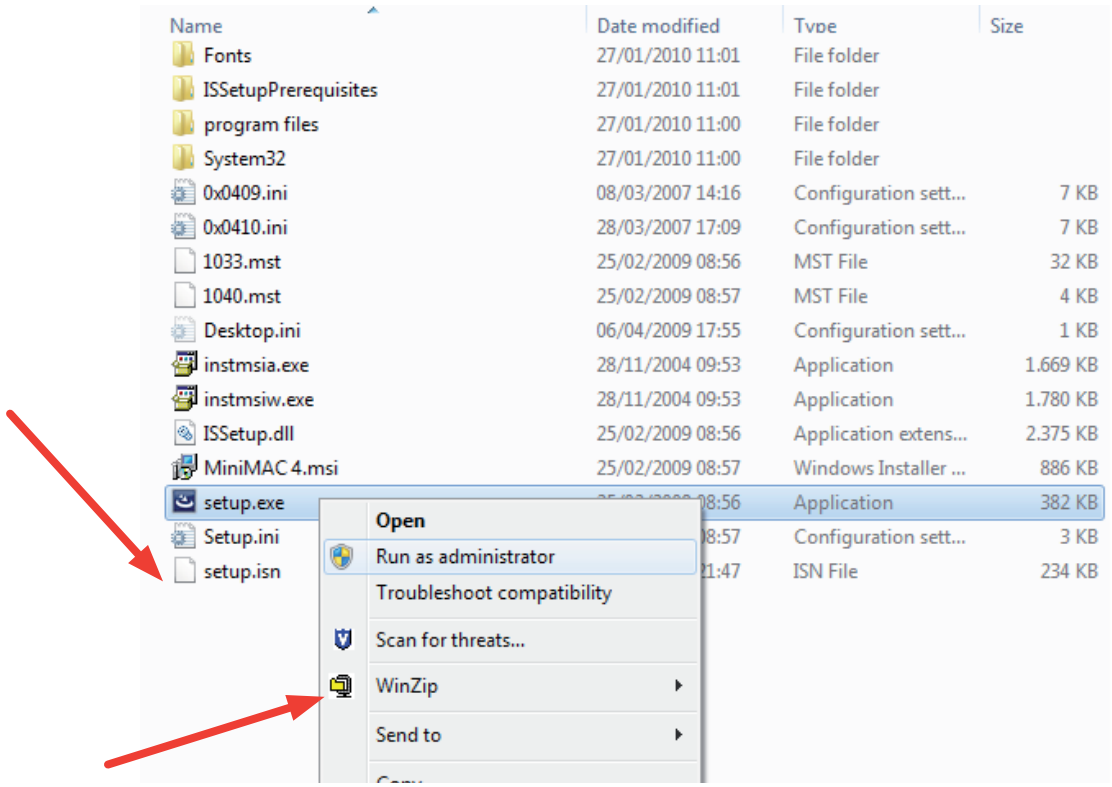
MiniMAC will install automatically during the installation phase, the following software components required if not yet installed on the PC:

- Microsoft .NET Framework 1.1
- Microsoft .NET Framework 2.2 SP2
- Microsoft .NET Framework 4.0
- Microsoft SQL CLR Types 2008 R2 e 2014 x86
- Microsoft SQL Management Objects 2008 R2 e 2014 x86
- Microsoft SQL Native Client 10.5 x86 e x64
- Microsoft Visual C++ 2010 SP1 x86
- Microsoft SQL Server Express 2014

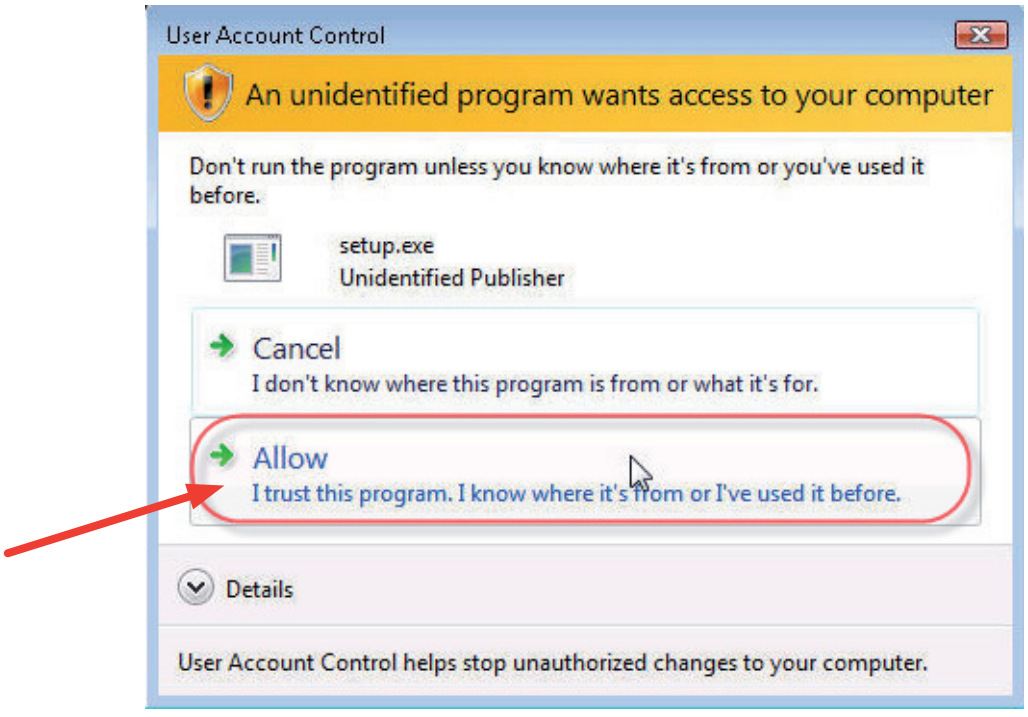
3.5 Installation procedure

Before proceeding with MiniMAC installation, close all running programs and search the CD ROM for the ‘ABB Installation/MiniMAC4.1.x.x’ folder (where *4.1.x.x* indicates the version) and search for the "setup.exe" file.

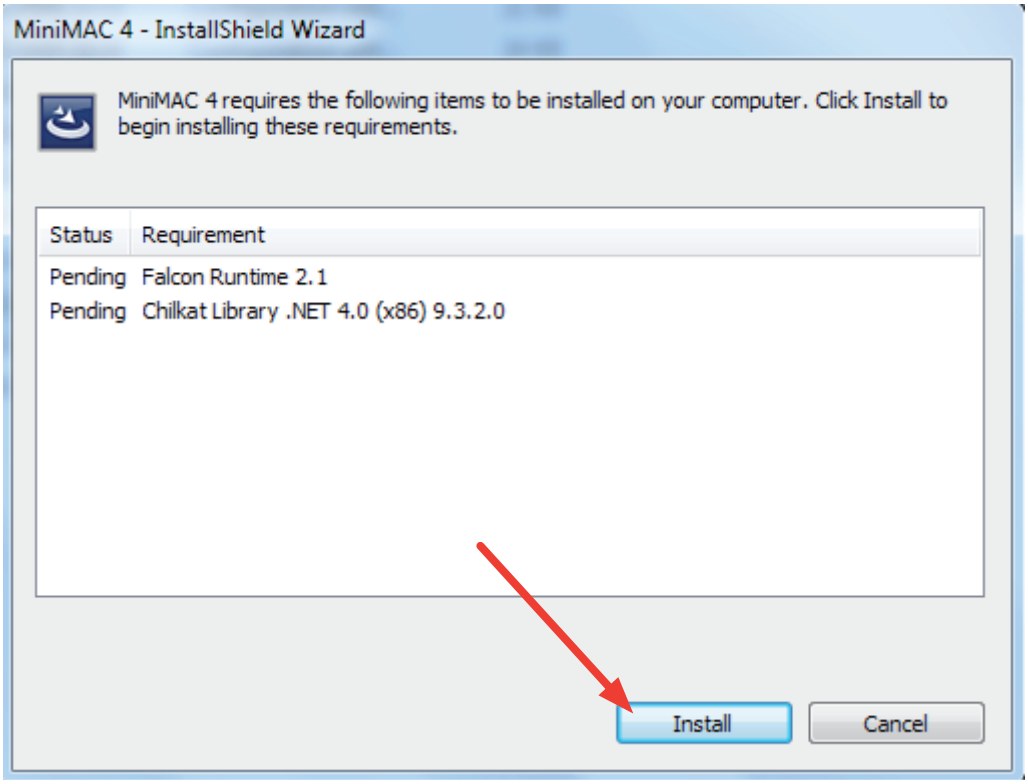
Make sure that you have Administrator credentials since software installation cannot be performed by a normal user. If you do not have Administrator rights, it is possible to run the set-up via the option **Run as Administrator**. Right click with the mouse on the file called '**setup.exe**'.

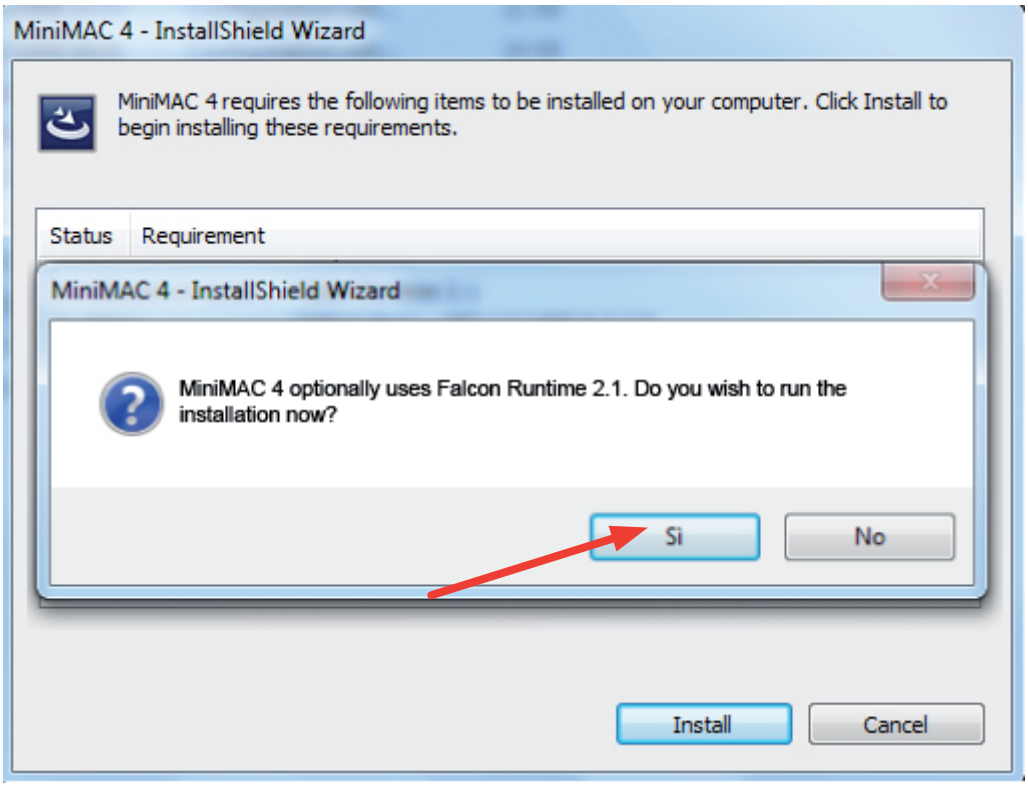


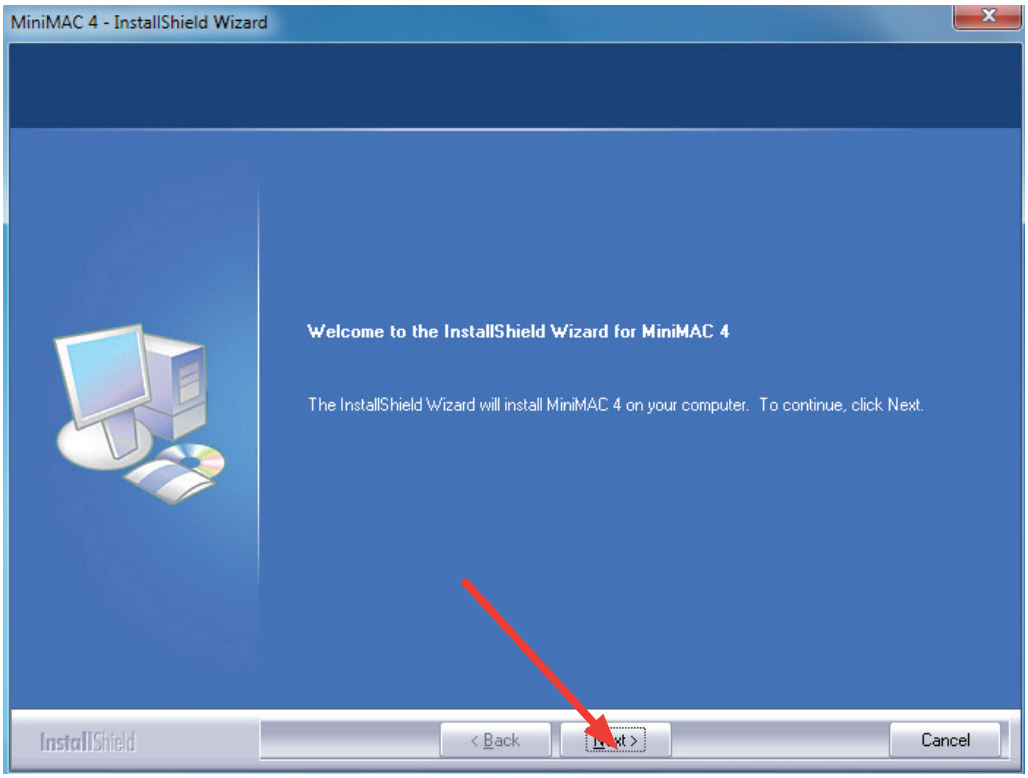
If the icon for confirmation is displayed, choose the option "Allow, I trust this program".

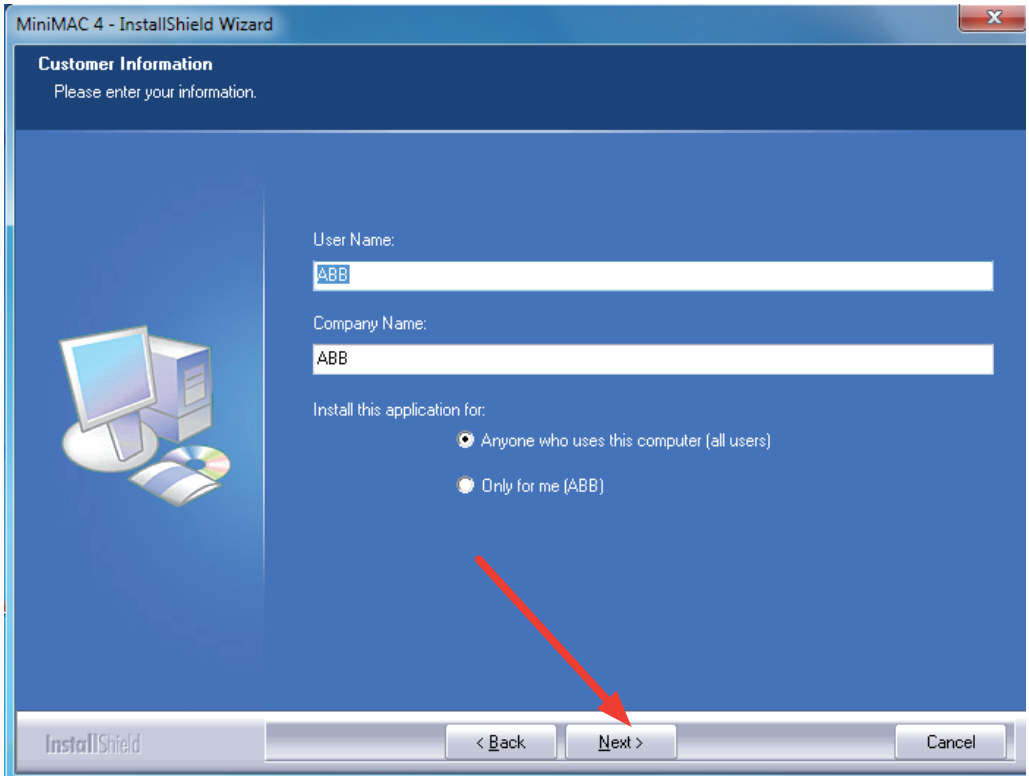


Proceed with the installation following the wizard.
Proceed accepting the installation of Falcon library.

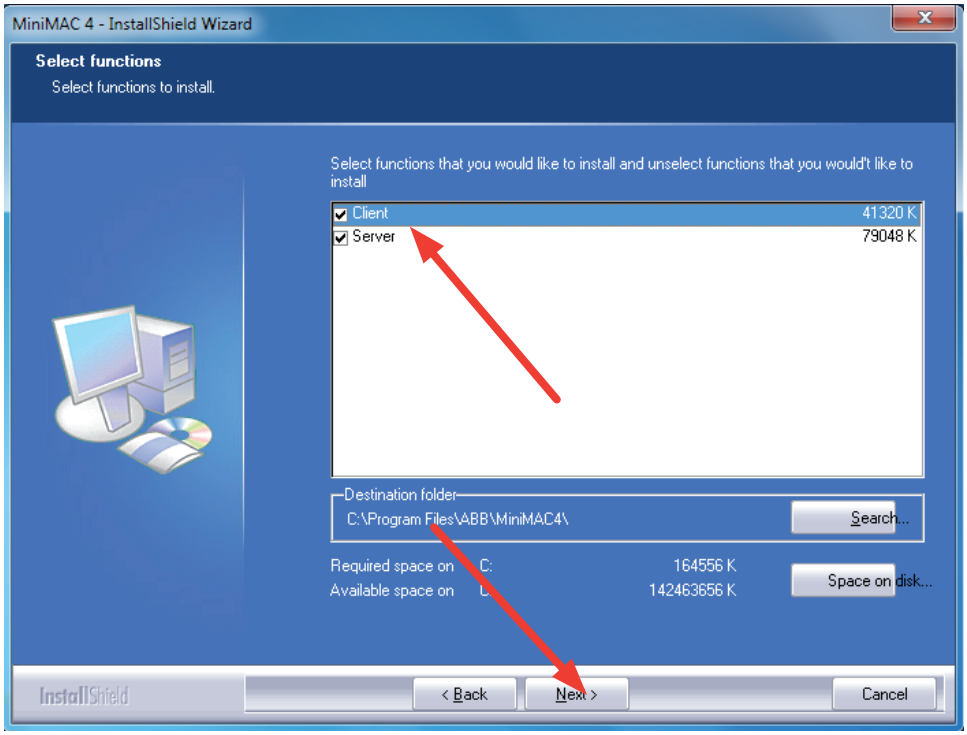





MiniMAC 4 - InstallShield Wizard
Welcome to the InstallShield Wizard for MiniMAC 4
The InstallShield Wizard will install MiniMAC 4 on your computer. To continue, click Next.
InstallShield
< Back
Next >
Cancel

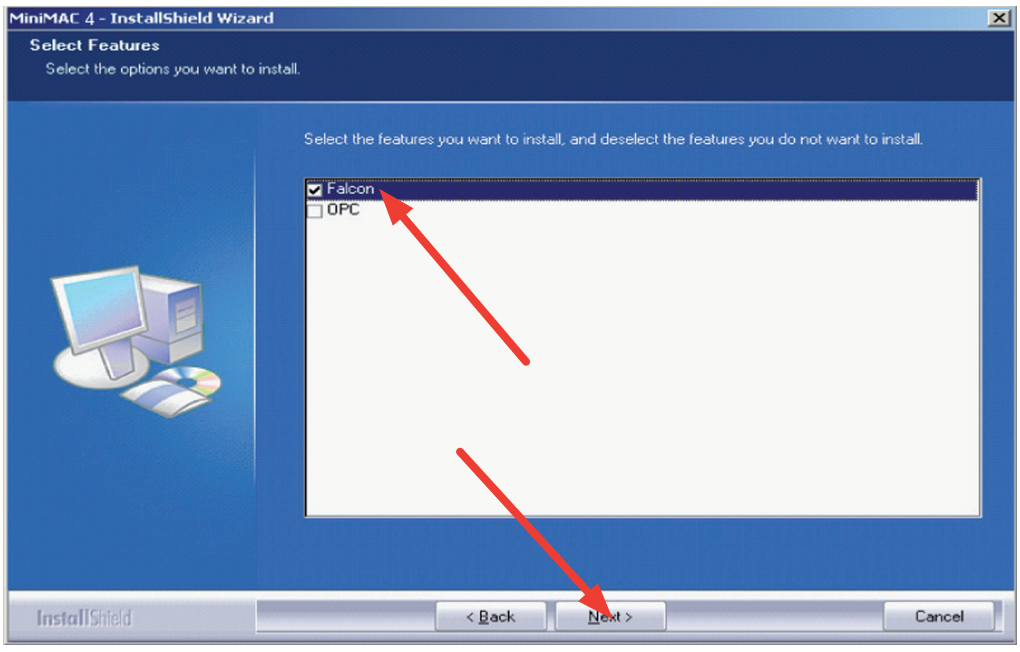

MiniMAC 4 - InstallShield Wizard
Customer Information
Please enter your information.
User Name:
ABB
Company Name:
ABB
Install this application for:
Anyone who uses this computer (all users)
Only for me (ABB)
InstallShield
< Back
Next >
Cancel

Select the type of installation (client, server, client+server).



Select the technology for the connection to the bus.

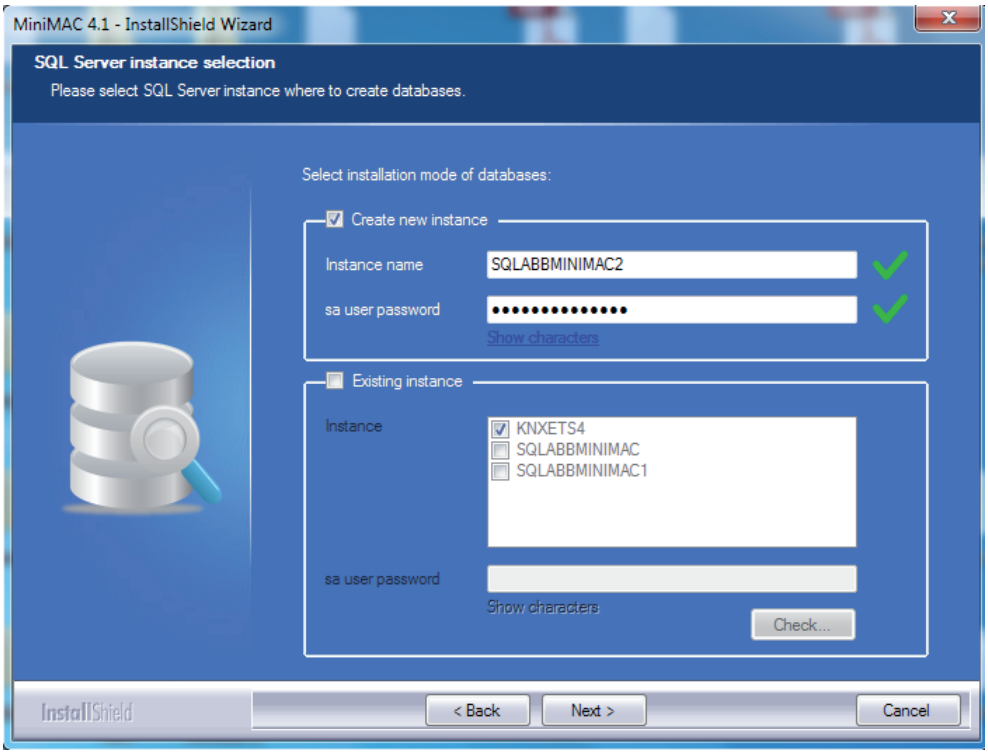
- If you choose the connection to MiniMAC bus via an OPC server, an OPC Server together with a valid licence must be installed.
- If you choose the connection to MiniMAC bus via Falcon libraries no additional software is required.



The MiniMAC installation wizard proceeds with the installation of the Microsoft SQL 2014 database.
If Microsoft SQL Server 2014 had been previously installed on the PC, the MiniMAC database will be installed using the Microsoft SQL Server 2014 that is already present: MiniMAC Database is created using the following credentials:

- username = minimac
- password = ABB029034sace#

It is recommended to create a new instance of database. In case of older instances are already installed, if possible remove them using “Control Panel” utility of Windows.
The password of MiniMAC database can be changed during installation phase or later using SQL Server Managment Studio (following the instructions of the tool). Once/if you change password of the database, it is necessary to update the credentials configured into the 2 MiniMAC tools: MACWizardServer and MacWizardClient.



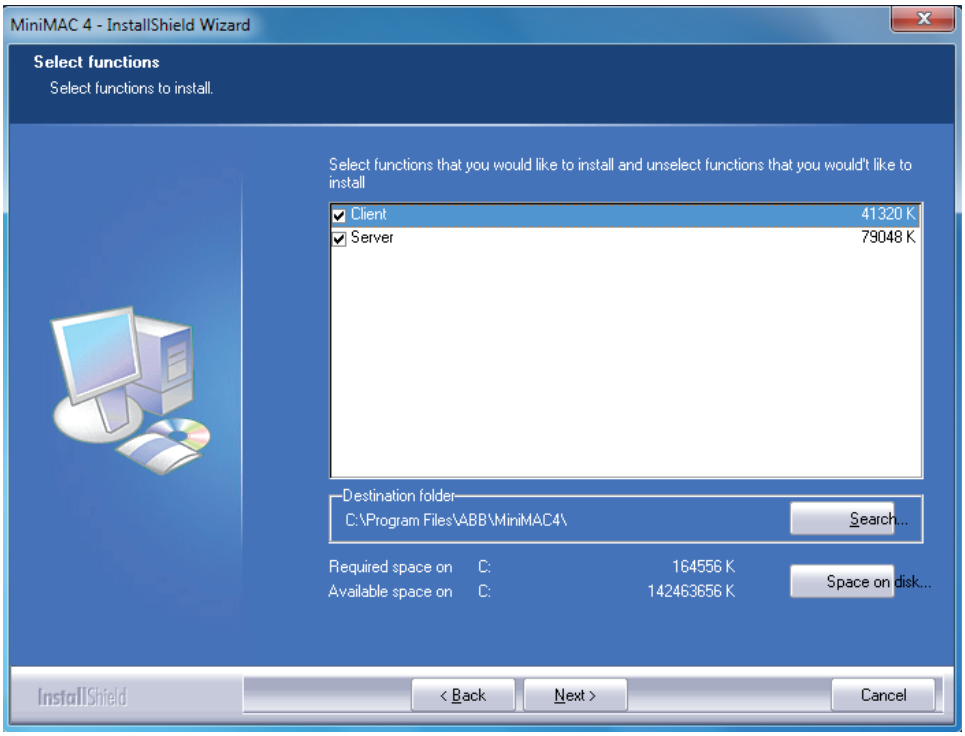
The installation is complete: **Restart the computer in order for the changes to be made permanent**. After restart, if you already have a connection to the bus and the devices are ready for programming or use, it is necessary to perform the configuration of the PC-BUS interface.

3.6 Client-server architecture

MiniMAC is based on a client-server architecture. Therefore, there are different possibilities:

- Install both the MiniMAC client and server on the same PC
- Install only a MiniMAC server installation on one PC and several client installations on one or more separate PCs.
- Install a MiniMAC server+client installation on one PC and several client installations on one or more separate PCs.

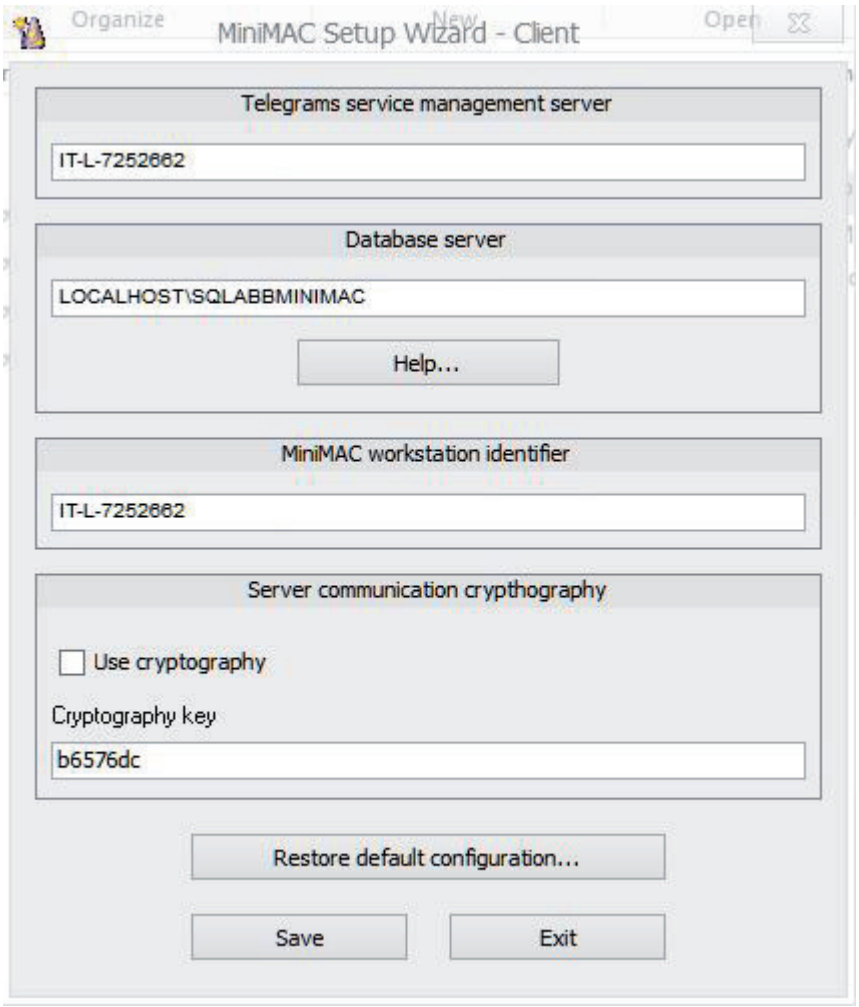
The type of installation (client, server, client+server) can be selected when installing MiniMAC.
The client-server architecture gives you the possibility (especially, but not only, useful for large applications) to have access to the information on access control system management and its remote control (i.e.



heating and cooling supervision, events management, loads management, etc.) on different positions, also far from the system itself and the PC on which the MiniMAC server version is installed.

To set the connection of client installations to the corresponding server installation, you need to run the MACWizard Client and enter the values of the PC on which the server version is installed in the first two boxes: these values are obtained running the MACWizard Server on the server machine.

In case of client-server installations, it is possible to encrypt the communication between client and server. In order to configure the encryption, it is necessary to select the box “Use cryptography” and insert in the box “Cryptography key” the same key inserted in the correspondent box of MACWizardServer on the server PC.
For security reason the chosen key can’t be exchanged/sent via mail/web.

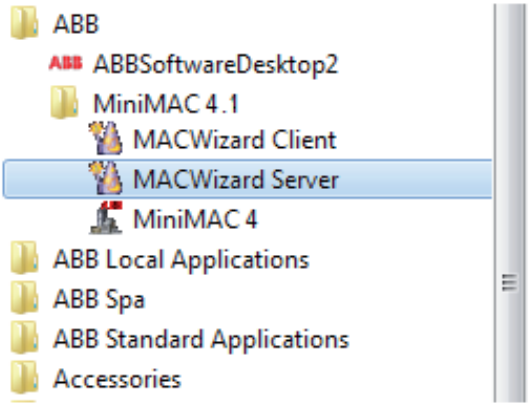


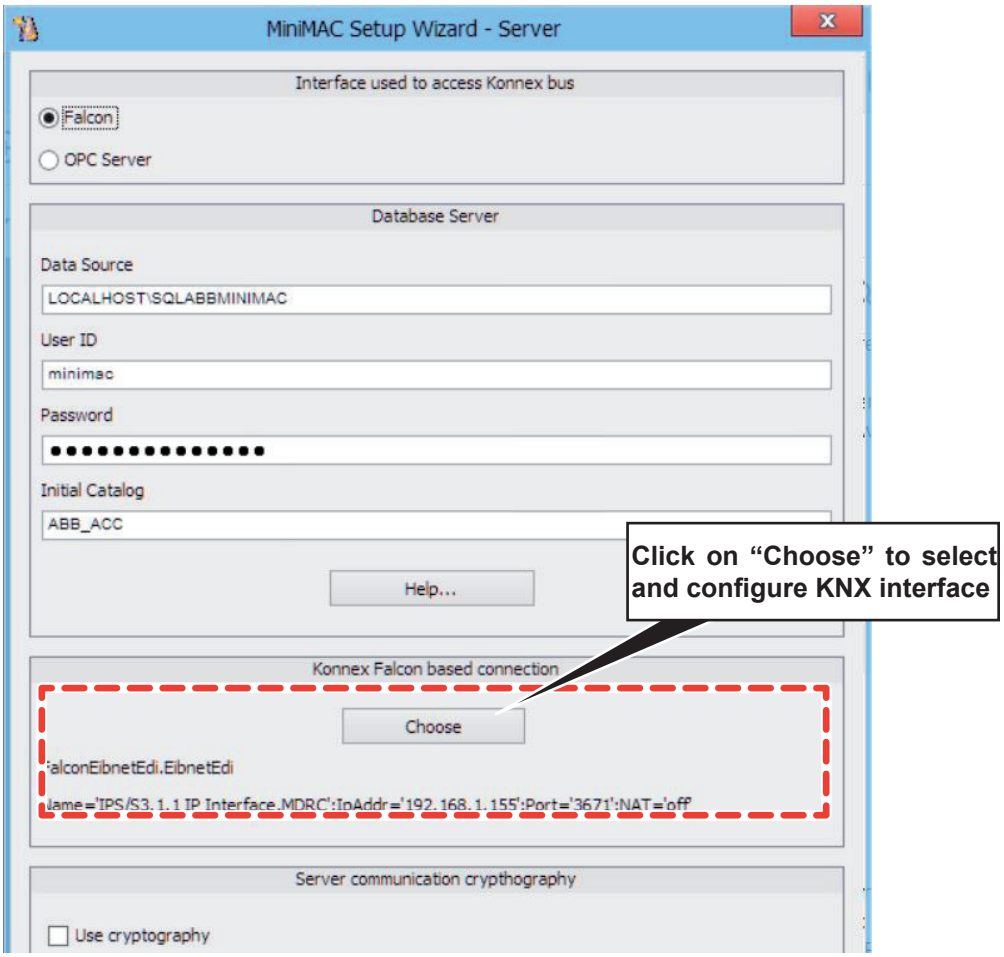
3.7 Configuration of the KNX bus interface

For connecting MiniMAC 4.1 with KNX bus a KNX interface is required. Due to Falcon libraries compatibility issues on some PCs with new operative systems (Windows 8, Windows 10), for connecting MiniMAC 4.1 with KNX bus an IP interface has to be used (ABB IPS/S 3.1), since connection with the bus using USB/S 1.1 is not granted in every environment.

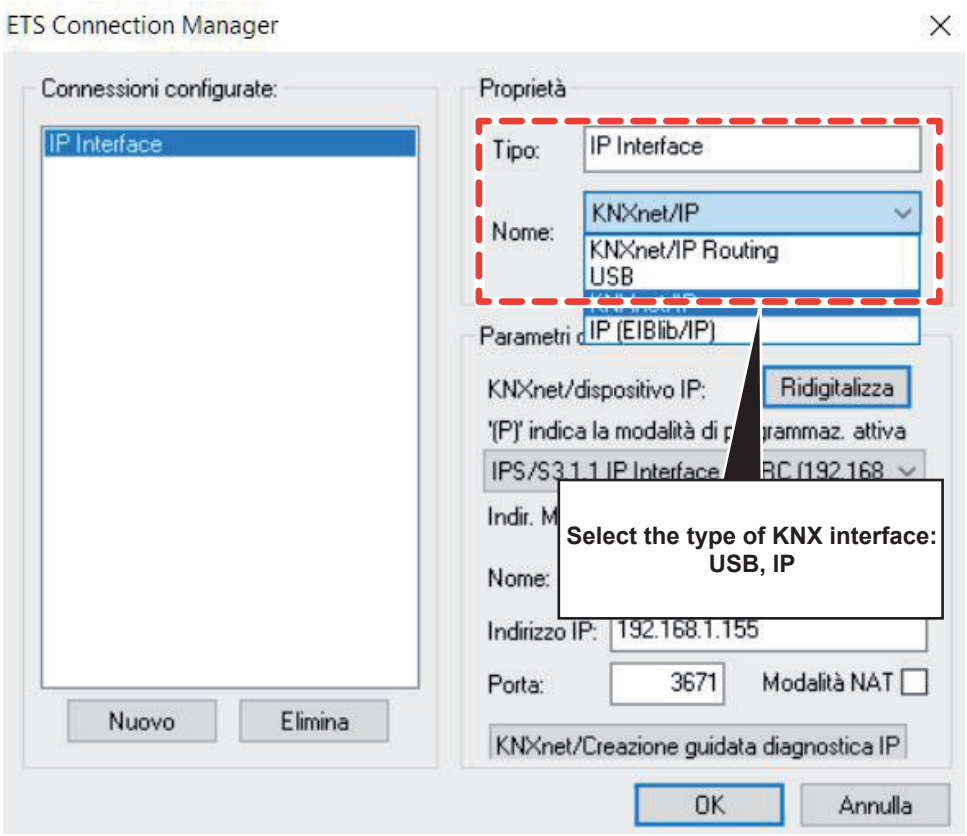
Warning
We recommend to us only IP interface for connecting MiniMAC PC to the KNX bus. USB interface it is not supported by MiniMAC software for connection to the KNX bus

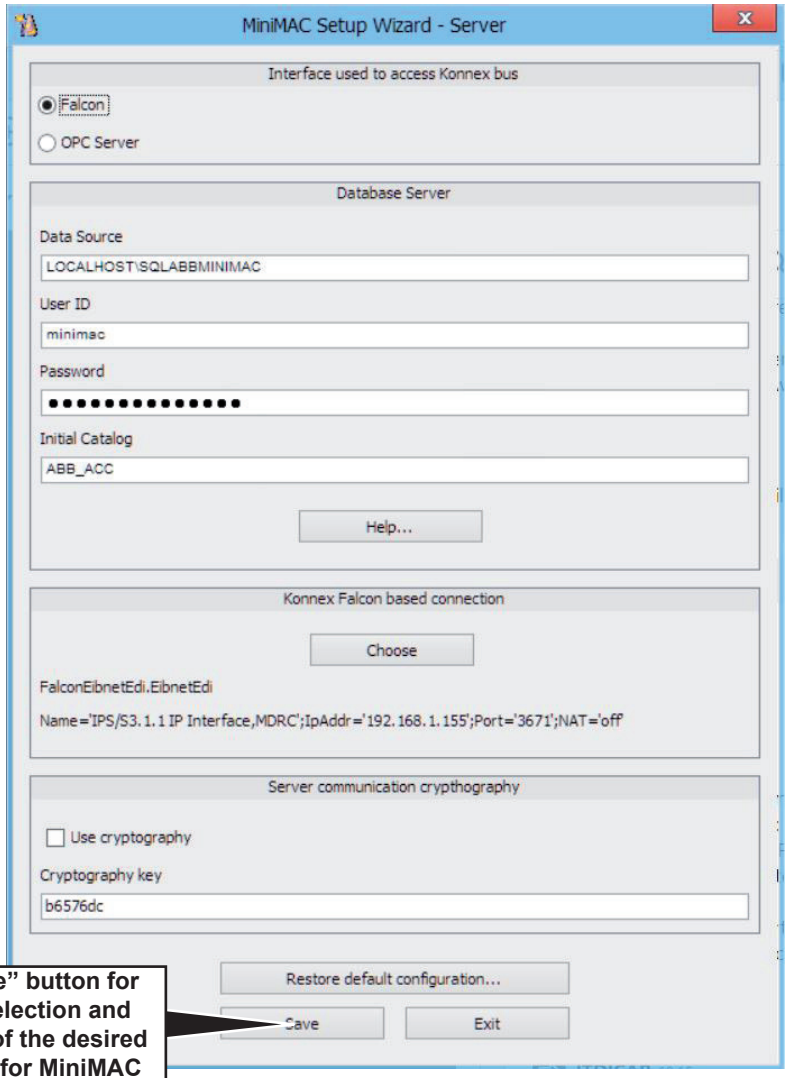
For configuring MiniMAC interface with KNX bus, run MACWizard Server program from the Programs-ABB-MiniMAC 4.1 folder.





It is now possible to select the desired KNX connection (USB interface, IP interface), through standard ETS connection manager window. Remember to use an IP interface (USB interface is not supported).



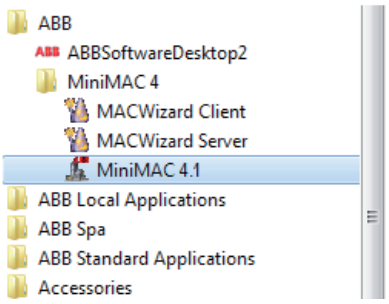


Click on "Save" button for confirming selection and configuration of the desired KNX interface for MiniMAC (USB, IP)

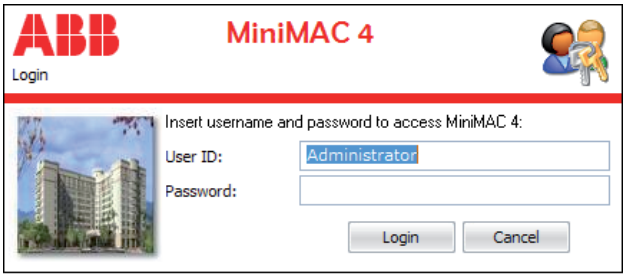
Remember that in case of client-server installations, it is possible to encrypt the communication between client and server. In order to configure the encryption, it is necessary to select the box "Use cryptography" and insert in the box "Cryptography key" the same key inserted in the correspondent box of MACWizardClient in all the clients PCs.
For security reason the chosen key can't be exchanged/sent via mail/web.

4 System configuration

The program runs through the link on the desktop or the PROGRAMS-ABB-MINIMAC-MiniMAC.exe menu:



The first login to the program is possible entering the following access data:
User ID: Administrator
Password: Administrator

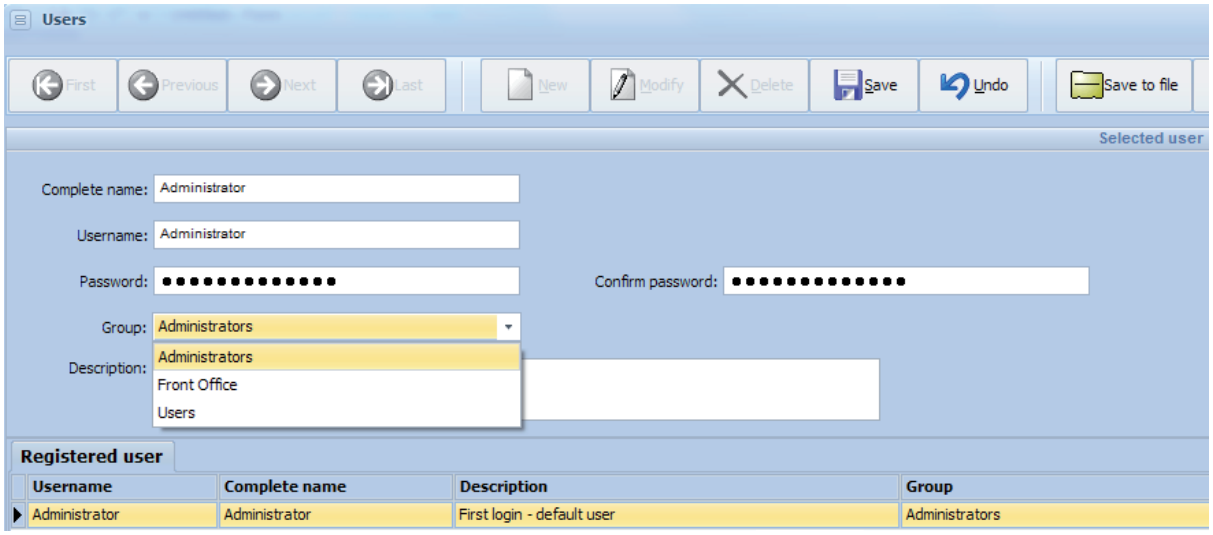


The main menu is displayed, from which you can recall all program functions.
First of all, the access control system must be configured.

4.1 User accounts definition

In order to create a system, you first need to create the user accounts that belong to the system. From the menu "Customers and staff", click on "Users" and create the different necessary user accounts (typically one for each member of the staff that uses the software). Administrator is reserved to the first login and must be removed as soon as possible. This is a good practice since MiniMAC keeps track of all operations performed on the system (see the following section Event History Menu).

This way each event and programming action is registered and associated to the person who made it. In order to grant transparency, each MiniMAC user must access the program with a personal username and password. If Administrator is not removed from the system, everyone could use it (simply by reading this manual) and operate anonymously on the system. Therefore, Administrator must be deleted as soon as possible: in this way the event history will show the precise indication of the responsible user. This is a very important safety and transparency function that cannot be waived.
Creation of a new user is easy: click on NEW, insert the required data and save.



The software allows you to manage two different User categories:

- Administrators
- Front Office
- Users

The Administrator can use all MiniMAC functions, whereas the User and Front Office is subject to some restrictions.
It is important that the administrators are not created indiscriminately. For security and stability issues of system programming, administrator privileges must be assigned only to expert and/or responsible staff, for example the person responsible for the planning and programming of the access control system.

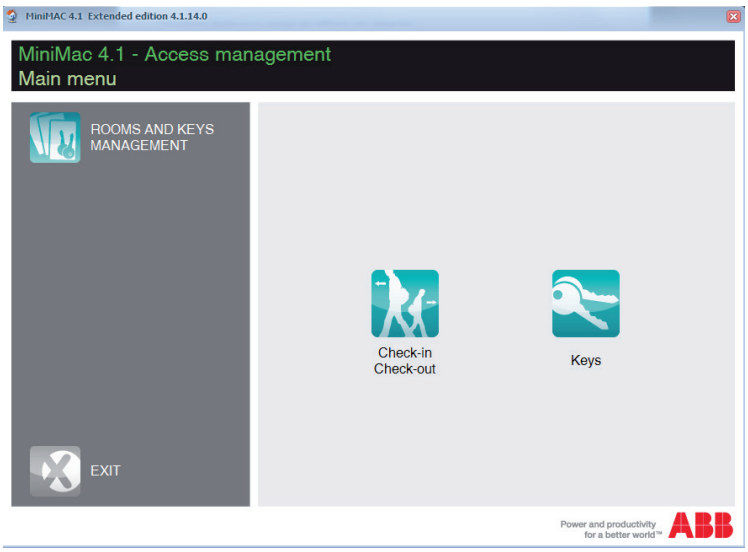
“Front Office” and “Users” cannot operate on the system configuration.

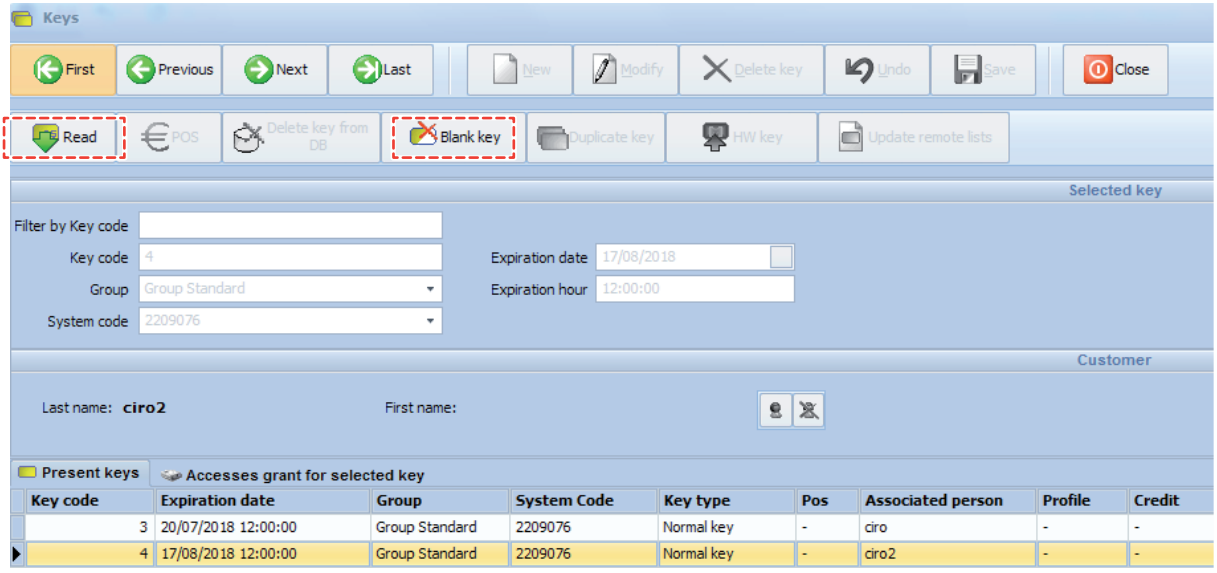
Front Office

“Front Office” has minimal rights: they have only the possibility to access the “Room and keys management” menu, in particular:

- Check-in/check-out operation
- Keys operation: it is possible only to BLANK key and READ key

“Front office” is the typical user created for hotel staff at reception, whose main task is check-in/check-out guests.



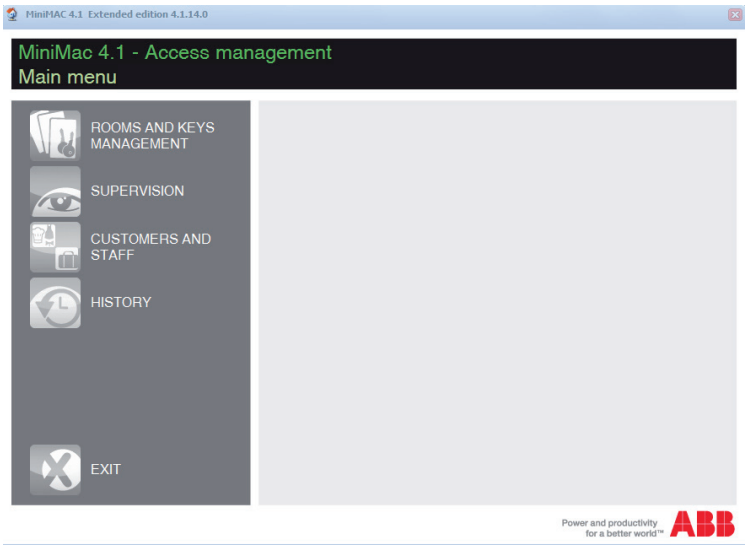


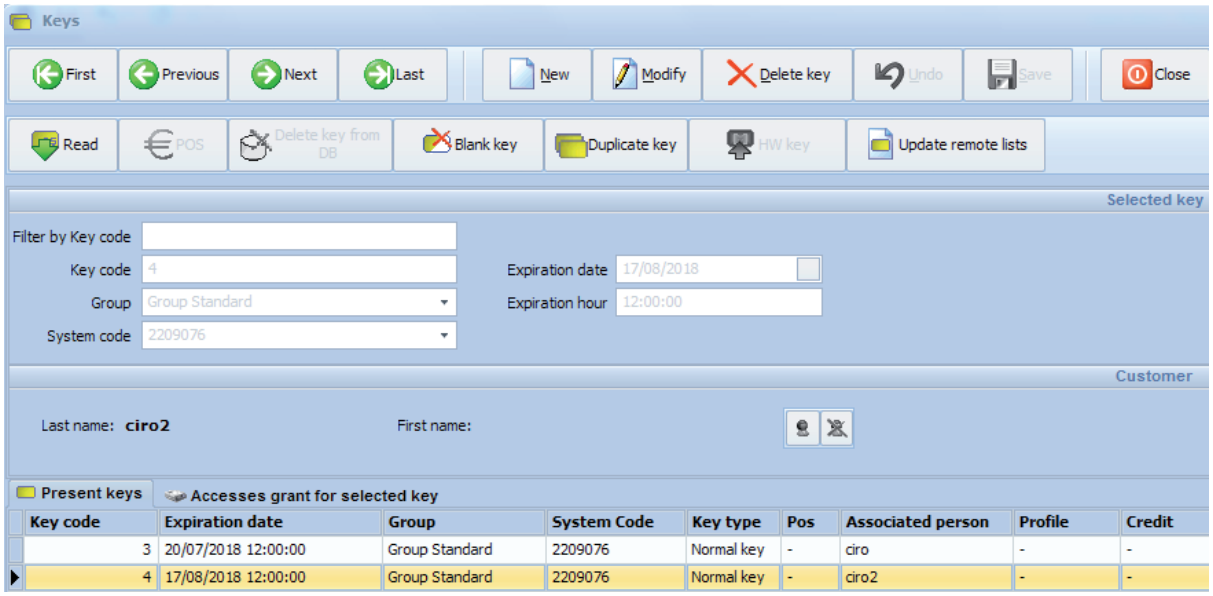
Users

“Users” have intermediate rights: they can access the following menu:

- “Room and keys management” (every operation is possible, except creation of “Hardware keys” and delete cards from Database)
- “Supervision” (only visualization, no configuration)
- “Customer and Staff” (without possibility to create new users in the “Users” menu)
- “History”

“Users” is the typical user created for hotel staff experienced in IT/software, who could be involved for advanced tasks by staff at reception.



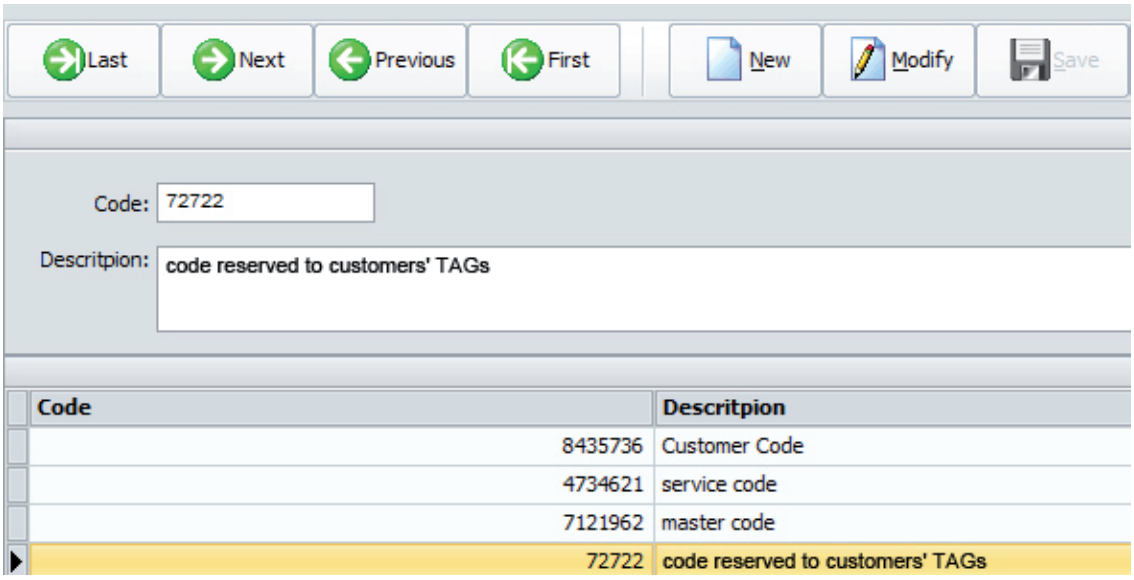


4.2 Creation of system codes

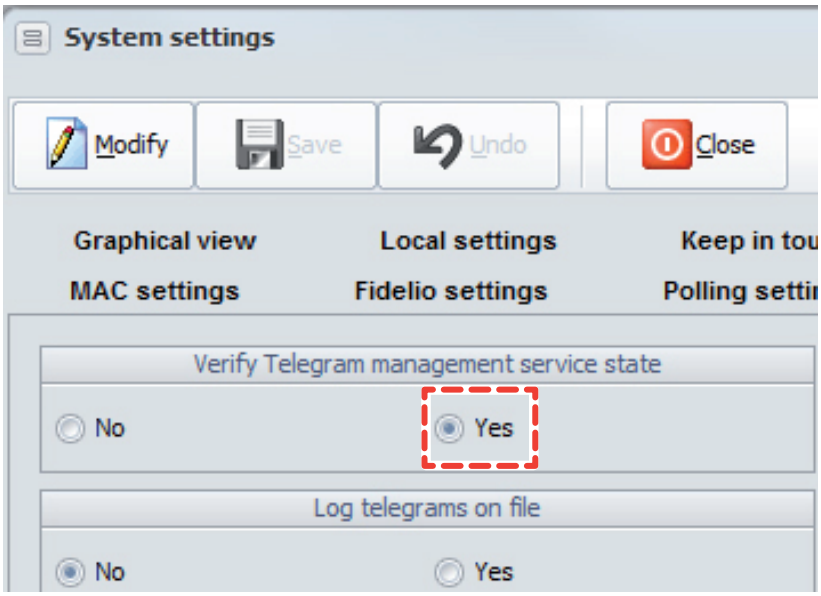
The second step for the creation of a system is the definition of system codes. Click on System Codes button in the “Plant management” menu and declare the system codes to be used in the installation.

It is easy to create system codes: click on NEW, insert data and description and finally Save.
For security, usability and flexibility reasons, we suggest (but it is not mandatory) the creation of at least THREE types of system codes:

- a code reserved to master TAGs
- a code reserved to service TAGs
- a code reserved to customers TAGs.



Remember that this monitoring option must be enabled when you are working on the system:

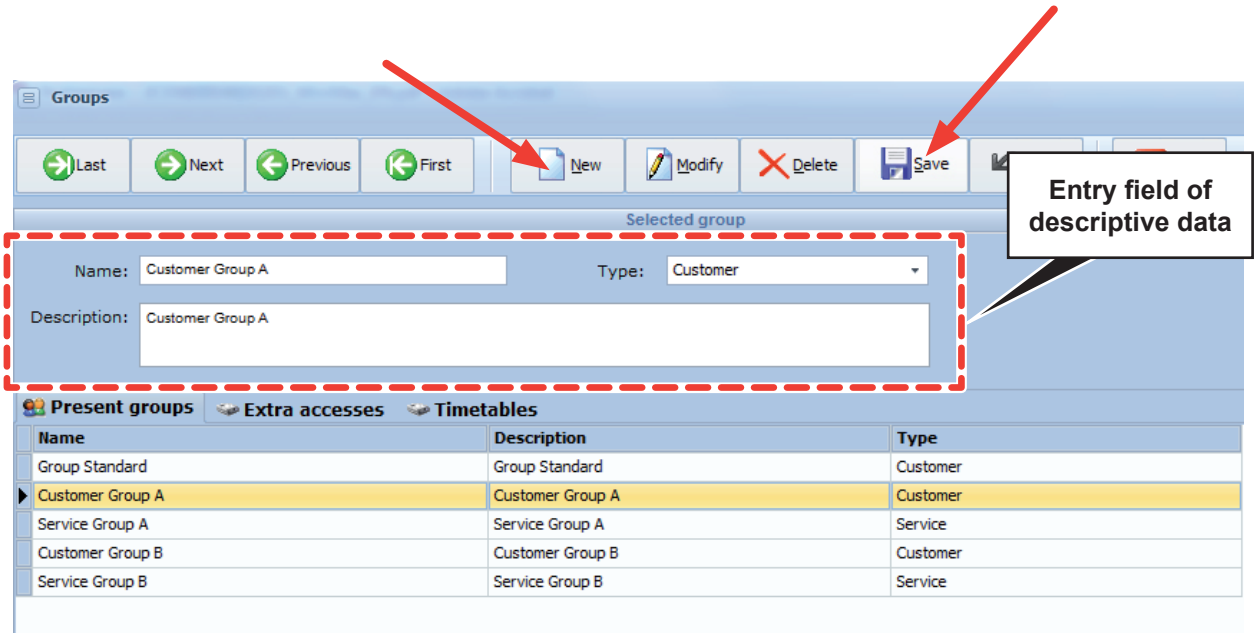


4.3 Creating groups

The function of groups is to: assign elementary timeslots to a certain homogeneous set of system users and then create a common temporal access profile for each group.
When a TAG is created, you must declare which group it belongs to. Each transponder TAG gets access by transponder with active timeslots, according to the temporal profile of its group.

Note
Group creation is essential: a TAG cannot be created if a group is not defined!

If you do not wish to use timeslots, simply leave the group with no timeslot. However timeslots must not be activated in the devices: a group without timeslots is a group without authorisation.
Groups have a further role: apart from timeslots, they also collect data structures called "areas". The use of areas is a MiniMAC function that makes the check-in wizard operations easier in extended installations, as explained in the section.
Groups creation is easy:
1. click on ‘New’;
2. enter the descriptive data (Name, Type, Description) in the specific area;
3. click on ‘Save’ button to confirm.



4.3.1 Timetables

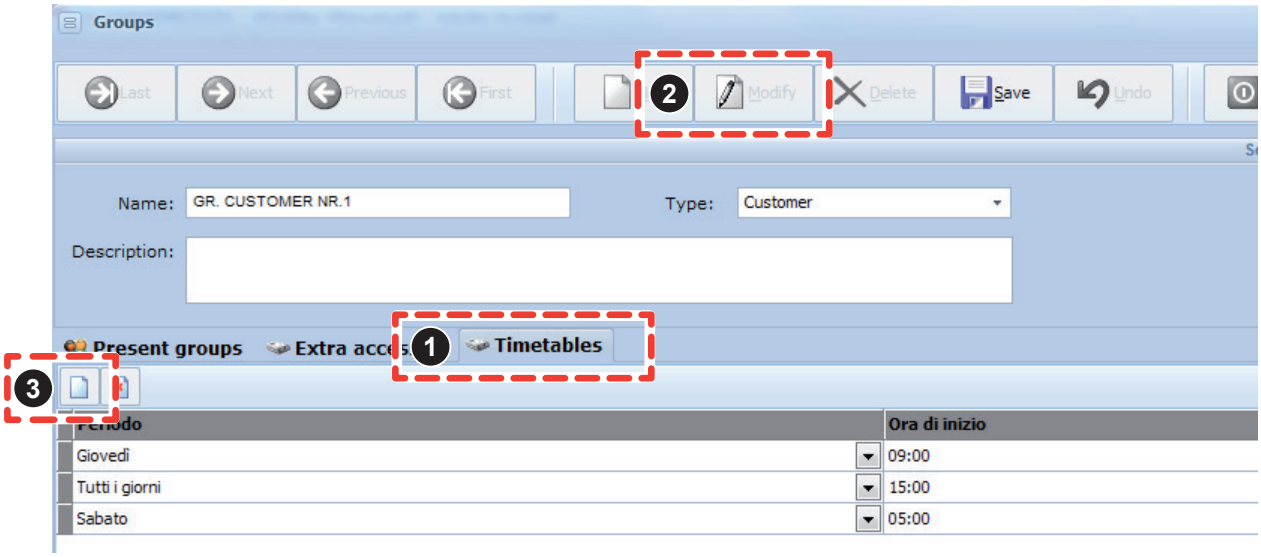
Once useful groups have been created in the system, it is necessary to enter appropriate timeslots for each group, in order to create an overall temporal profile associated with that group.
With the timeslots you can indicate a time interval during which the passage/access to an entrance/ room is allowed.
Elementary timeslots may be defined on a WEEKLY base and can be created without any limit.
Inside a specific group, up to 12 timeslots can be overlapped and up to 255 groups can be defined. Timeslots combinations are then unlimited.

If timeslots are not useful, you can go directly to the next step: groups are not required to include timeslots (but remember: if timeslots are activated, a group without timeslots will never get access).
To assign timeslots to a created group, you have to:

1. Select a group;
2. Click on Timetables TAB (**1**);
3. Activate Edit mode (**2**);
4. Click on New Element (**3**) and define a new timetable for the group.

Timeslots definition is easy and intuitive. The required data are:

- Start and end time
- The day of the timeslot or the possibility to use it every day

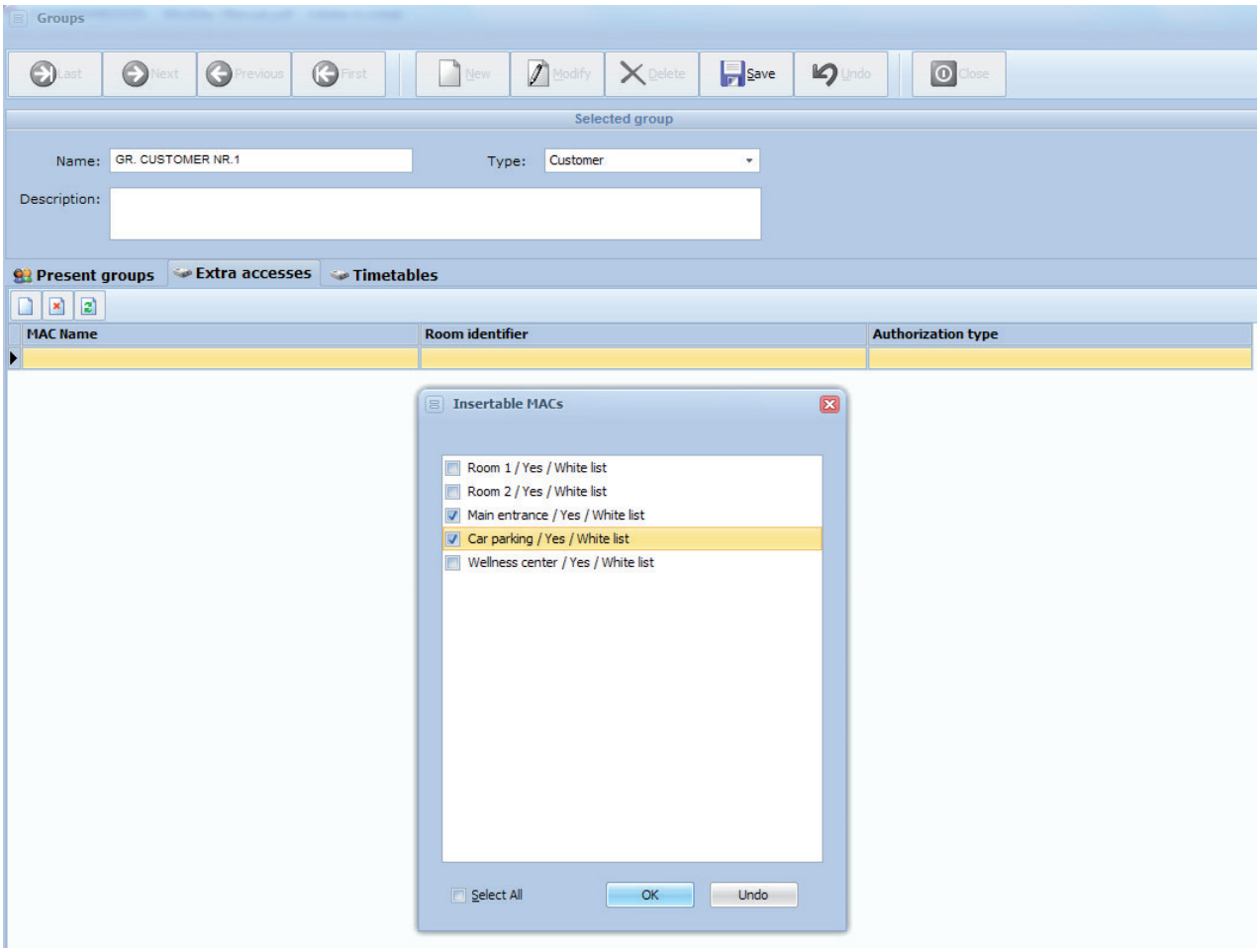


4.3.2 Extra accesses

The concept of “Extra accesses” bases on the fact that a hotel has several rooms and common areas. When creating a TAG for a customer or a staff member (for further details see section ***“7.2 Check-in”***, section ***“7.4 Check-out”***), assignment of the access rights can be challenging in case of an extended system with a lot of common transits.
“Extra accesses” definition can solve this problem with an automation of the operations that would be unnecessarily repetitive. Assuming that there is a group of customers who need to have the right to enter “Main entrance”, “Car parking” and “Wellness center”, with “Extra accesses” it’s possible to have automatically one/more groups of customer right to access these gates.

Configuration of “Extra accesses” is simple:
1. Select the specific Group for which you need configuration of “Extra accesses”
2. From “Extra accesses” TAB insert the access control devices you want to associate with present groups.

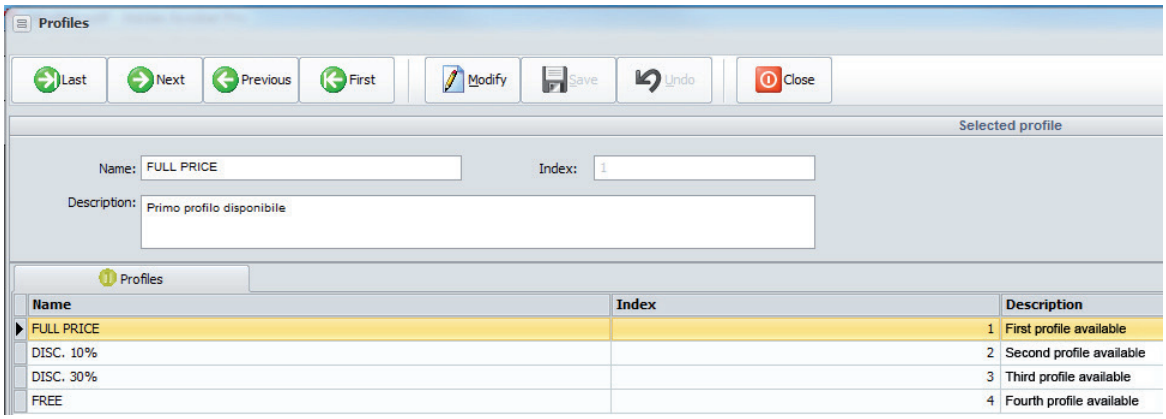
By selecting some access control device, you grant automatically access at these gates to all users belonging to these groups.



4.4 Rate profiles definition

This step applies only to those systems where transponder readers with POS function (electronic money) are installed. Otherwise, this step can be ignored and you can go directly to step 7 (see section *"4.6 System Design"*).

This menu allows you to assign a name to the four rate profiles that are handled by each reader device with POS function. Such operation is not necessary because the 4 profiles are automatically named by MiniMAC, but the assignment of a custom name to the rate profiles is useful during TAG creations and can help avoiding errors.
Creation of customised profiles is very easy.

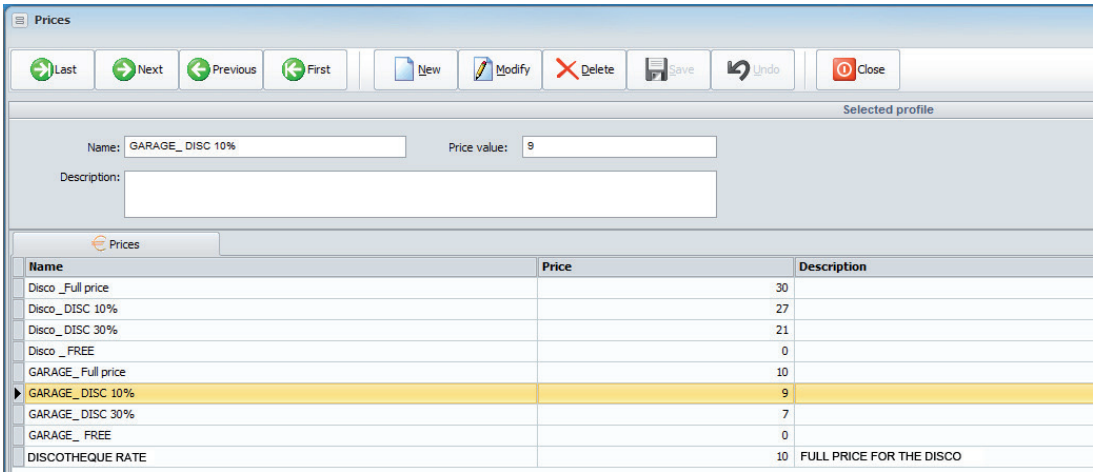


During the creation of a TAG, a rate profile is assigned to the TAG (1 of the 4 available rate profiles). The profile identifies in the system the rate to be applied each time a customer makes a payment. The rate can change from access point to access point and system administrators have to make the rates congruent with profile.
As an example, if a TAG belongs to the profile TOURIST DISCOUNT 10%, to each payment in the system must be applied a rate with a 10% discount. This has to be taken into account in order to guarantee transparency to customers.
Even if 4 profiles are available, not all of them have to be used. The differentiation of profiles makes it possible to have 4 different rates for the same access, depending on customer type. It is possible to have only one rate for all customers, but you can also configure 2 or 3 different rates.

4.5 Rates creation

Rates are managed in this menu. It is possible to create, edit and delete rates. Generated rates are available for a following insertion in transponder reader with POS functions that are present in the system.

The procedure for rates creation is easy and similar to the other procedures described in the previous sections.
Click on New Rate button, enter the required data including the amount (Default 0 means that the rate is free).
As an example, assume that there are two payment points: sauna-fitness and discotheque.
According to the selected profiles, rates must be properly created keeping attention on discounts.



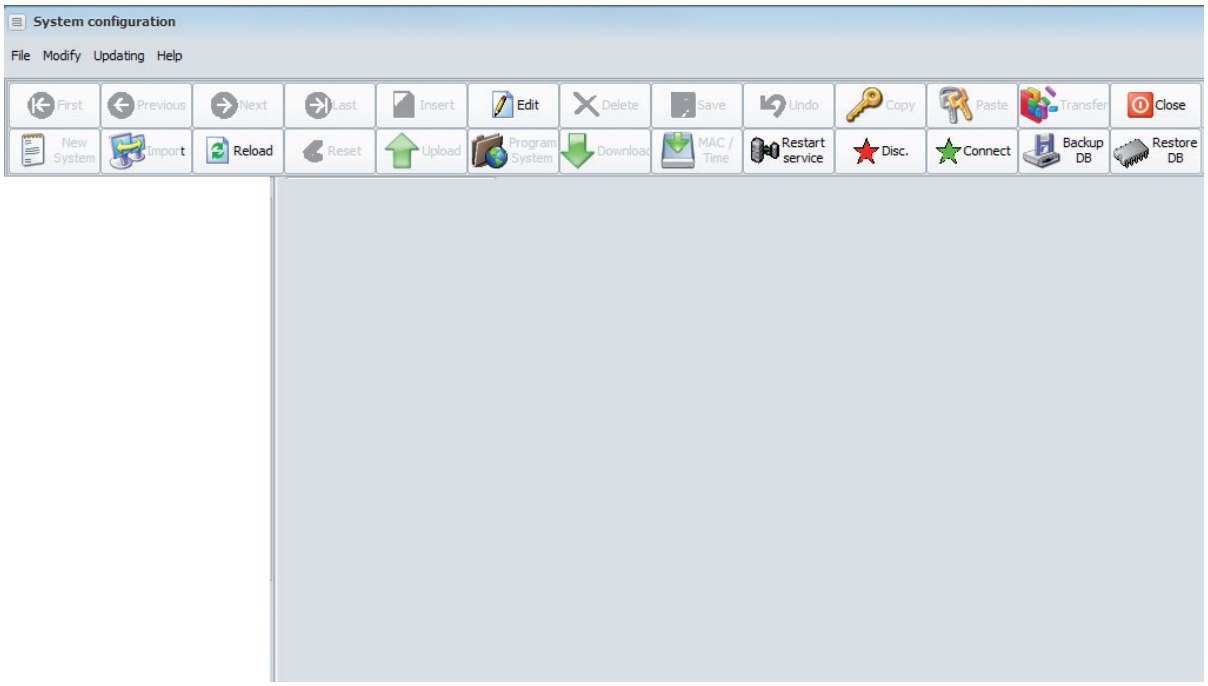
Name	Price	Description
Disco _Full price	30	
Disco_ DISC 10%	27	
Disco_ DISC 30%	21	
Disco _ FREE	0	
GARAGE_ Full price	10	
GARAGE_ DISC 10%	9	
GARAGE_ DISC 30%	7	
GARAGE_ FREE	0	
DISCOTHEQUE RATE	10	FULL PRICE FOR THE DISCO

The previous table shows two payment points, 4 profiles available for each point. In this case up to 8 (=4x2) rates can be generated.
In our example we defined a VIP profile with a 0 € rate, so creation of two rates FREE SAUNA and FREE DISCO is not necessary and a single FREE RATE can be defined.

4.6 System Design

A series of important operations have been described in the previous sections and they are the starting point for system creation, which is configured using the PLANT submenu, in the System Management menu.

Assuming, for example, a very small basic system consisting of a room, some common areas and 2 payment areas (SAUNA and DISCO). Step-by-step system design is described below. Consider that system dimensions do not change the design procedure: when learned how to create a room you know how to create 3,000 rooms, the only difference lies in the time spent to enter the information necessary to complete the project.
At the first startup it is necessary to enter the information concerning the various devices in the database (the system is actually empty).



4.6.1 Comunication between MiniMAC and access control devices

The room, called 101, is accessible through a transponder. A transponder holder checks physical presence in the room.
These values must correspond to the group addresses configured in the ETS project on the related device (see figure below).

For every access control devices belonging to the installation, it's necessary to configure the communication with MiniMAC software.
Configure devices using ETS file according to desired behavior Pay attention to ABB communication objects:

- On Millenium and Chiara-Mylos devices ACC1 and ACC14 objects have to be linked into MiniMAC device configuration menu related to specific device: every device has to be configured with a couple of group addresses for ACC1 and ACC14, different from those chosen for other devices
- On Tacteo devices "Access Data" object have to be linked into MiniMAC device configuration menu related to specific device: every device has to be configured with a group address for "Access Data", different from that chosen for other devices
- For all devices (Millenium, Chiara-Mylos, Tacteo) Date and Time have to be linked later on into MiniMAC Setting page (in the "Timing" TAB): every device share the same couple of group addresses for Date and Time, since the all receive them from MiniMAC

Number	Name	Object Function	Description	Group Address	Length	C	R	W	T	U	Data Type	Priority
0	Switch	Switch			1 bit	C	-	W	-	-		Low
1	Scene	Scene			1 byte	C	-	W	-	-		Low
2	Status Switch	Status Switch			1 bit	C	R	-	T	-		Low
3	Guest in the room	Guest in the room			1 bit	C	R	-	T	-		Low
4	Acc1 Command	Acc1 Command	ACC1	1/1/0	1 byte	C	R	W	T	U		Low
5	Acc14 Command	Acc14 Command	ACC14	1/1/1	14 bytes	C	R	W	T	U		Low
6	Date	Date	Date	0/0/1	3 bytes	C	-	W	-	-		Low
7	Time	Time	Time	0/0/2	3 bytes	C	-	W	-	-		Low
9	Guest card acknowledgment scene	Guest card ack scene			1 byte	C	-	-	T	-		Low
10	Services card acknowledgment scene	Services card ack sce...			1 byte	C	-	-	T	-		Low
11	Guest card acknowledgment	Guest card acknowle...			1 bit	C	-	-	T	-		Low
12	Services card acknowledgment	Services card acknow...			1 bit	C	-	-	T	-		Low
13	Card insertion scene	Card insertion scene			1 byte	C	-	-	T	-		Low
14	Card removal scene	Card removal scene			1 byte	C	-	-	T	-		Low
15	Green Led	Green Led			1 bit	C	-	W	-	-		Low
16	Red Led	Red Led			1 bit	C	-	W	-	-		Low

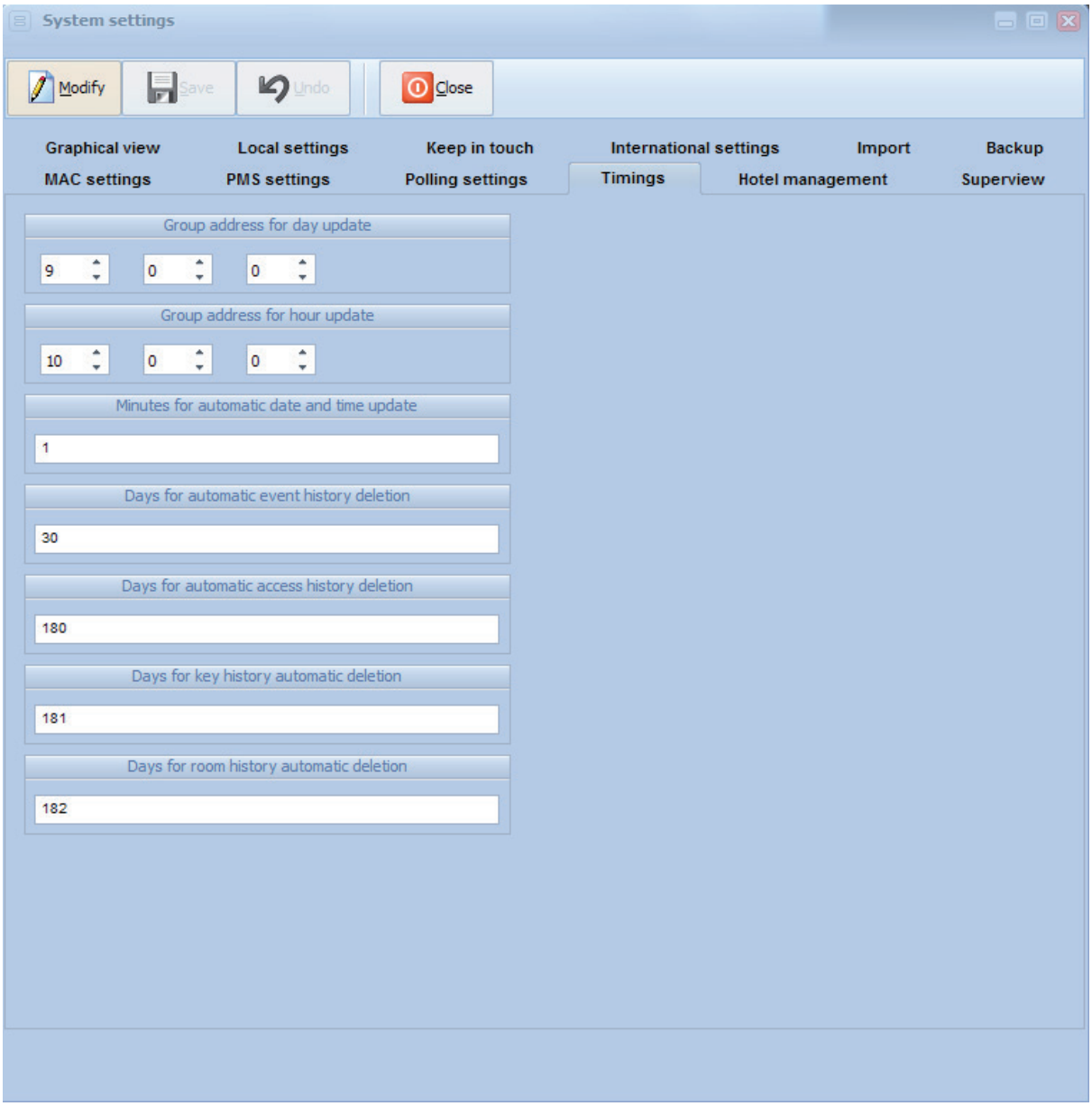
ETS communication object (Chiara, Elos, Mylos devices)

Number	Name	Object Function	Description	Group Address	Length	C	R	W	T	U	Data Type	Priority
0	Output A	Switch			1 bit	C	-	W	T	-		Low
1	Output B	Switch			1 bit	C	-	W	T	-		Low
2	Input A / B short	Telegr. Move up/down			1 bit	C	R	W	T	-		Low
3	Input A / B long	Telegr. Move up/down			1 bit	C	R	W	T	-		Low
4	Input C	Telegr. Switch			1 bit	C	R	W	T	-		Low
5	Output A	Telegr. Status			1 bit	C	R	-	T	-		Low
6	Output B	Telegr. Status			1 bit	C	R	-	T	-		Low
7	ACC1	ACC1 Management	ACC1	1/1/0	1 byte	C	R	W	T	-		Low
8	ACC 14 byte	ACC14 Management	ACC14	1/1/1	14 bytes	C	R	W	T	-		Low
9	Date	Date Telegr.	Data	0/0/1	3 bytes	C	-	W	T	-		Low
10	Time	Time Telegr.	Ora	0/0/2	3 bytes	C	-	W	T	-		Low
11	Yellow LED 3 bi - ON/OFF	Yellow LED 3 bi - ON/OFF			1 bit	C	-	W	T	-		Low
12	Red LED 3 bi - ON/OFF	Red LED 3 bi - ON/OFF			1 bit	C	-	W	T	-		Low
13	Red LED 4 bi - ON/OFF	Red LED 4 bi - ON/OFF			1 bit	C	-	W	T	-		Low
14	Green LED 4 bi - ON/OFF	Green LED 4 bi - ON/OFF			1 bit	C	-	W	T	-		Low

ETS communication object (Millenium devices)

Number	Name	Object Function	Description	Group Addres	Length	C	R	W	T	U	Data Type	Priority
15	S1: Switching	Input/Output			1 bit	C	-	W	T	U	switch	Low
23	S2: Switching	Input/Output			1 bit	C	-	W	T	U	switch	Low
31	S3: Switching	Input/Output			1 bit	C	-	W	T	U	switch	Low
39	RL: Switch object	Input			1 bit	C	-	W	-	-	switch	Low
41	CR: Card Valid	Output			1 bit	C	R	-	T	U	switch	Low
42	CR: Date	Input	Date	0/0/1	3 bytes	C	-	W	-	U	date	Low
43	CR: Time of the day	Input	Time	0/0/2	3 bytes	C	-	W	-	U	time of day	Low
44	CR: Access data	Output	Access Data	1/1/0	4 bytes	C	R	-	T	U	counter pulses (unsigned)	Low
45	CR: Customer card valid	Output			1 bit	C	R	-	T	U	switch	Low
46	CR: Service card valid	Output			1 bit	C	R	-	T	U	switch	Low

ETS communication object (Tacteo)


System settings
Modify
Save
Undo
Close
Graphical view
Local settings
Keep in touch
International settings
Import
Backup
MAC settings
PMS settings
Polling settings
Timings
Hotel management
Superview
Group address for day update
9
0
0
Group address for hour update
10
0
0
Minutes for automatic date and time update
1
Days for automatic event history deletion
30
Days for automatic access history deletion
180
Days for key history automatic deletion
181
Days for room history automatic deletion
182

4.6.2 Room configuration

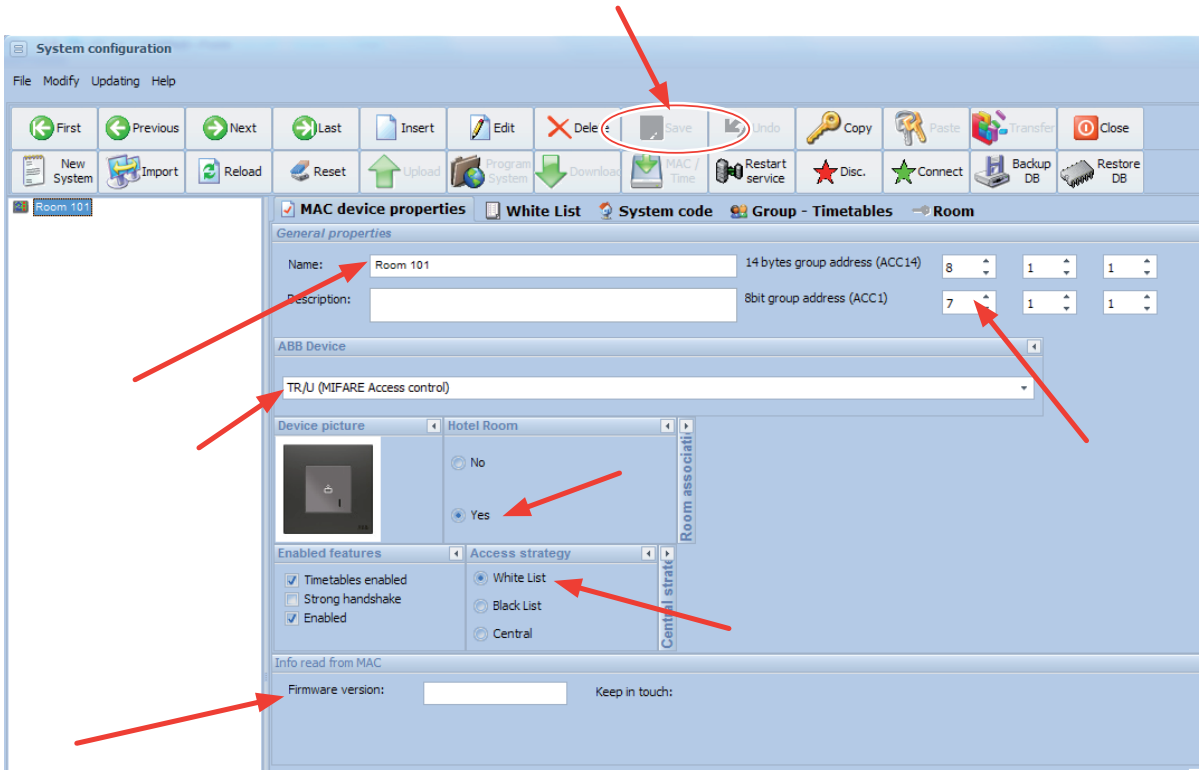
For configuring a Room you need to follow two steps:

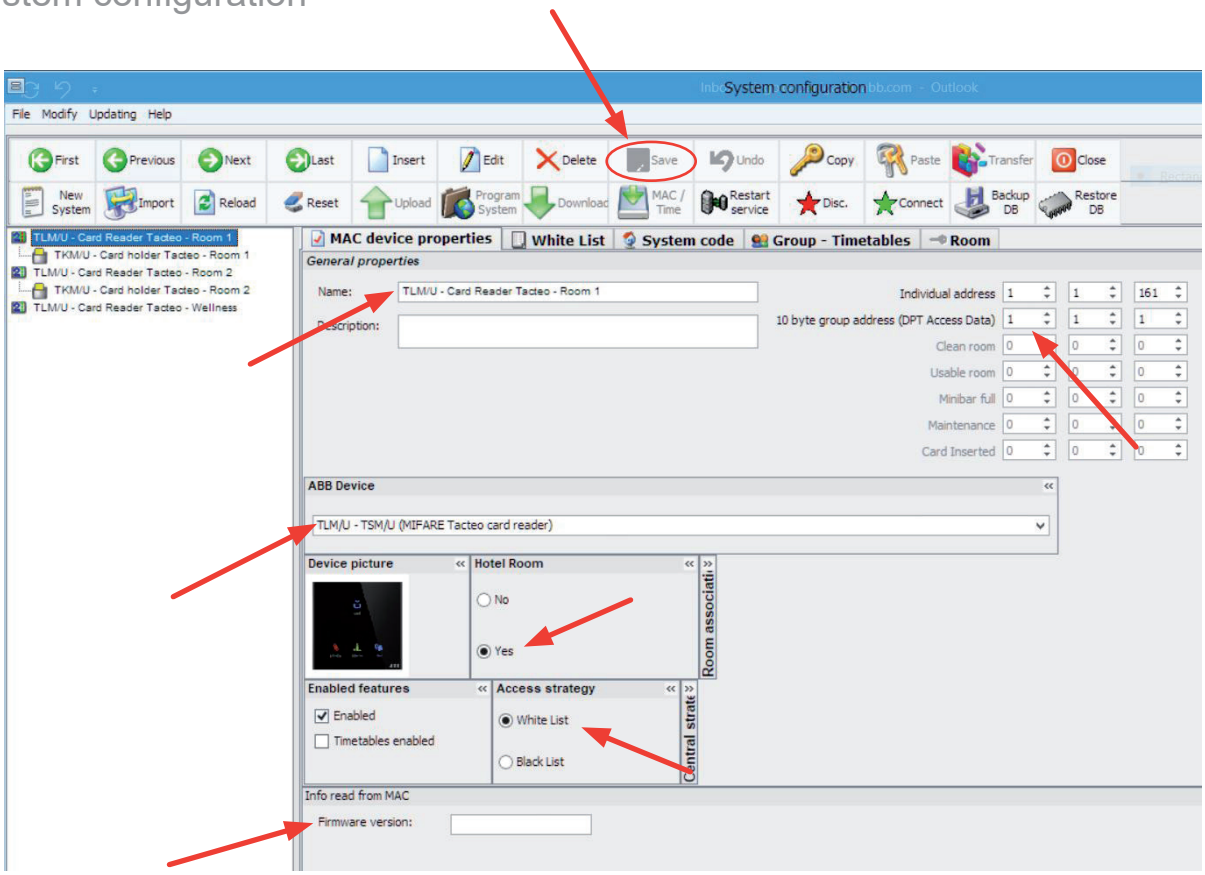
- configuration of transponder reader installed outside the Room (mandatory)
- configuration of transponder holder installed inside the Room (optional)

This means that every Room must have a transponder reader associated to it, while you could have installations where rooms have not card holder installed inside.

4.6.2.1 Transponder Reader

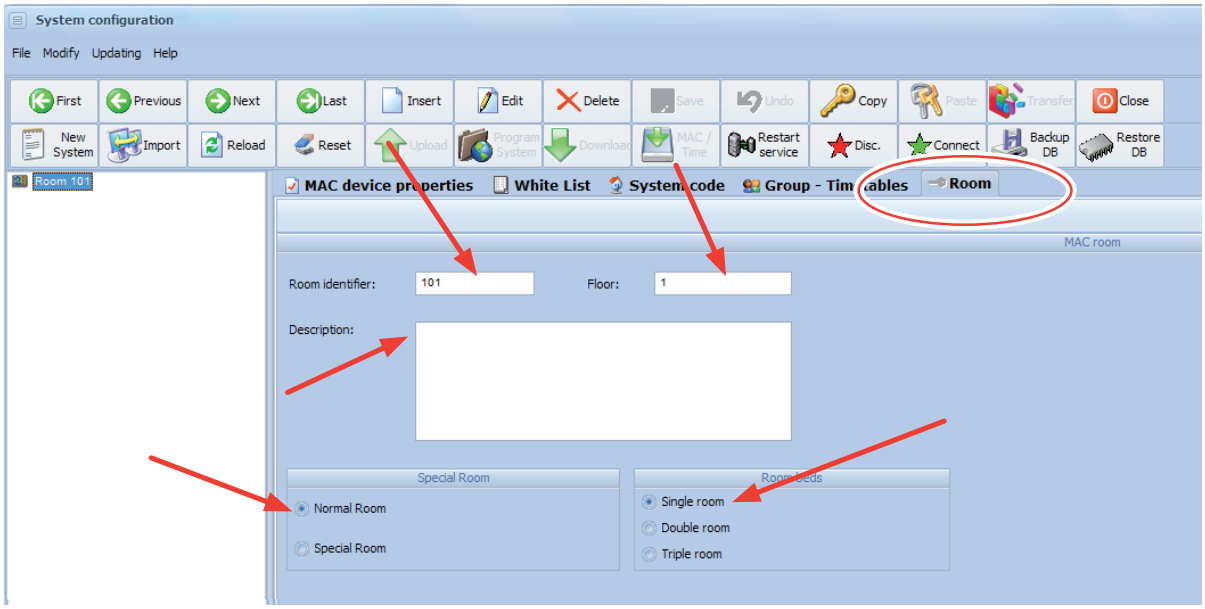
1. Select by the menu drop-down the type of transponder reader:
   - TR/U for Millenium
   - LT/U for Chiara-Mylos-Elos
   - TLM/U - TSM/U for Tacteo
2. Configure the communication between MiniMAC and device specifying group address “ACC1, ACC14” for Chiara-Mylos and Millenium devices, “Access Data” for Tacteo devices
   - Only for Tacteo devices configure the KNX physical address (Individual address) as already configured in the ETS project for this specific device
3. insert Name (and Descriprion, optional) of device
4. specify Hotel Room = Yes
5. configure Access Strategy: the recommendation for transponder reader related to Hotel Room is White List
6. configure the device as “Enabled”
7. Enable Timetables if requested. If you enable Timetables please be sure to configure Timetables for every Group. A user belonging to a Group without Timetables configured, by default has no right to access a transponder reader with Timetables enabled



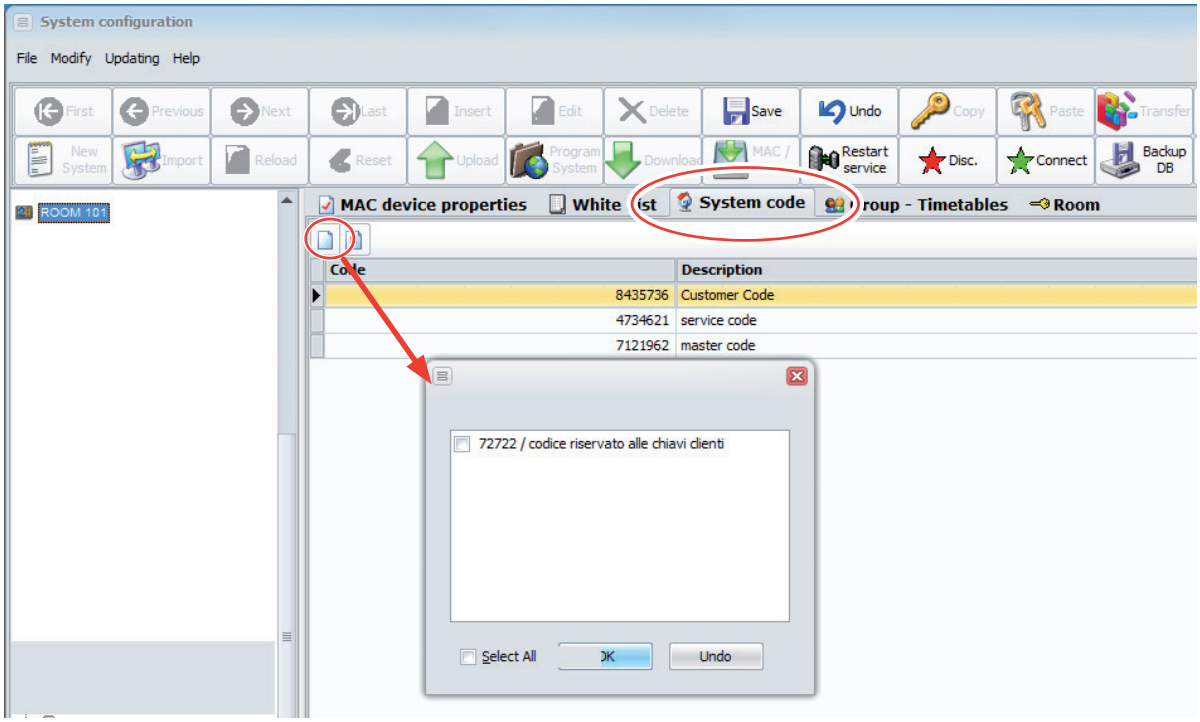


Click on the ROOM TAB and then EDIT to enter further information that are necessary for the hotel management:

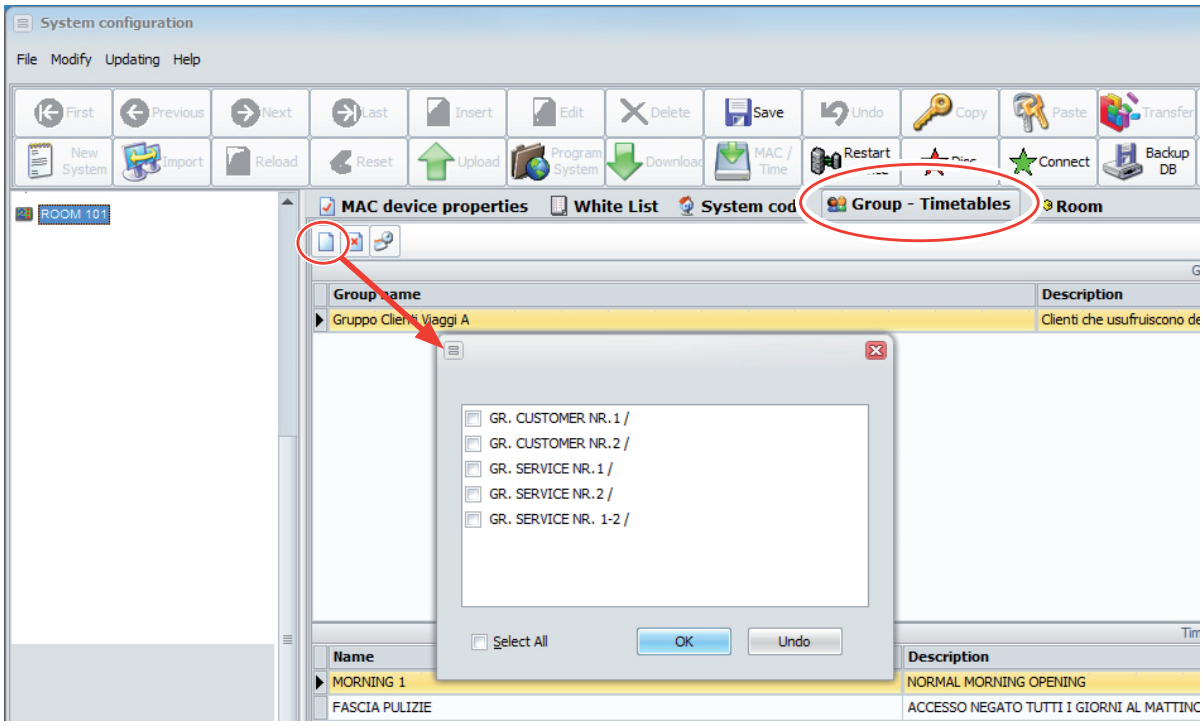
- room number
- floor
- type of room



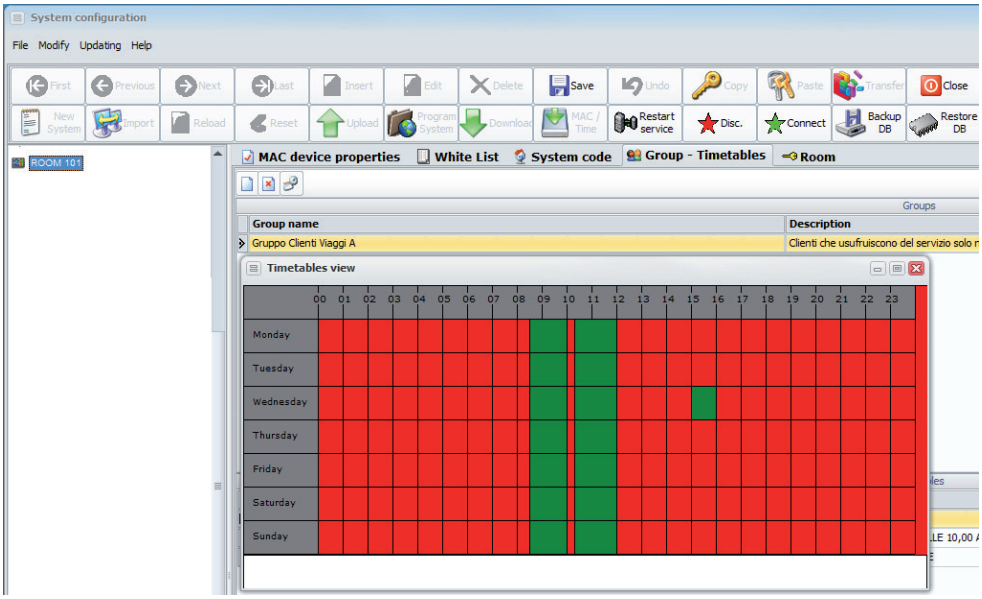
After the requested information is entered, system CODES must be associated with the device. Remember that the device will grant the passage only to the TAGs with one of the system codes contained in the list that is filled in in the "System code" TAB.



Click on "Groups-Timeslots" TAB and, in EDIT mode, you can enter the groups associated with the device/room.



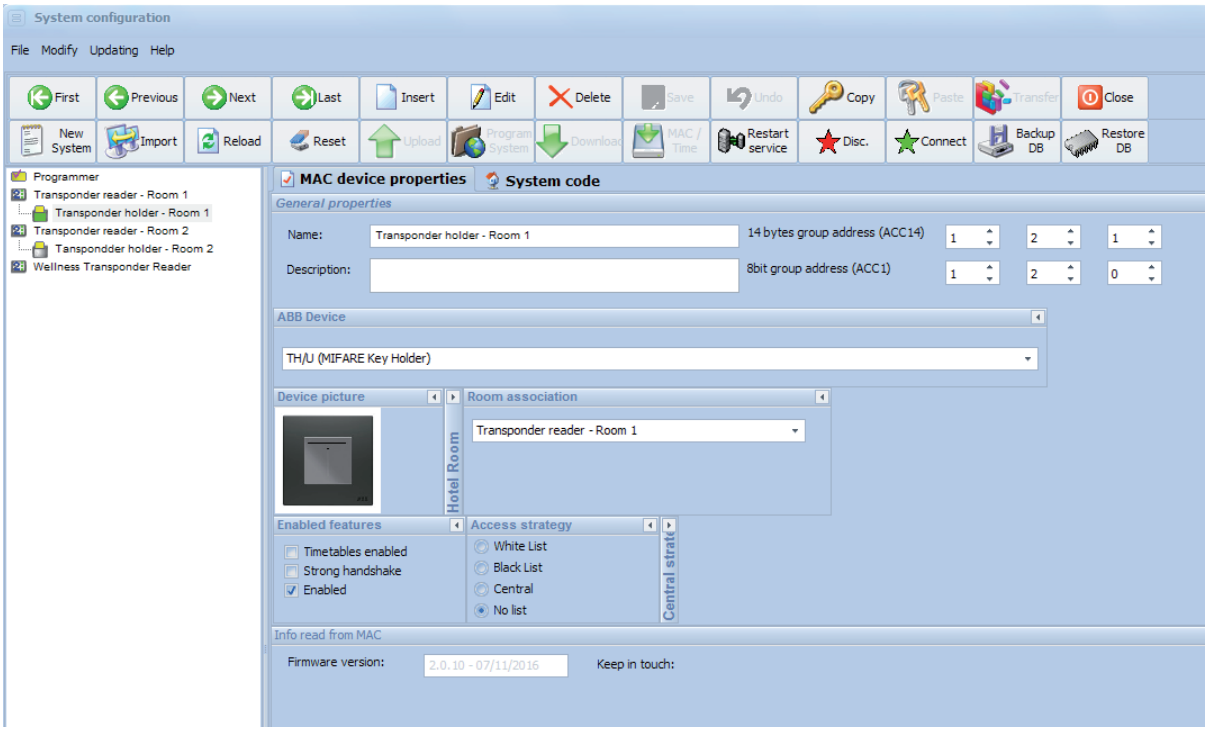
If you click on the dedicated button (“View Timetables”) you see for every group the timetables configured, if configured. In the example below As you can see, the green area is reserved to the room cleaning service staff which has a set of TAGs part of this group and can enter the room only in that timeslot.

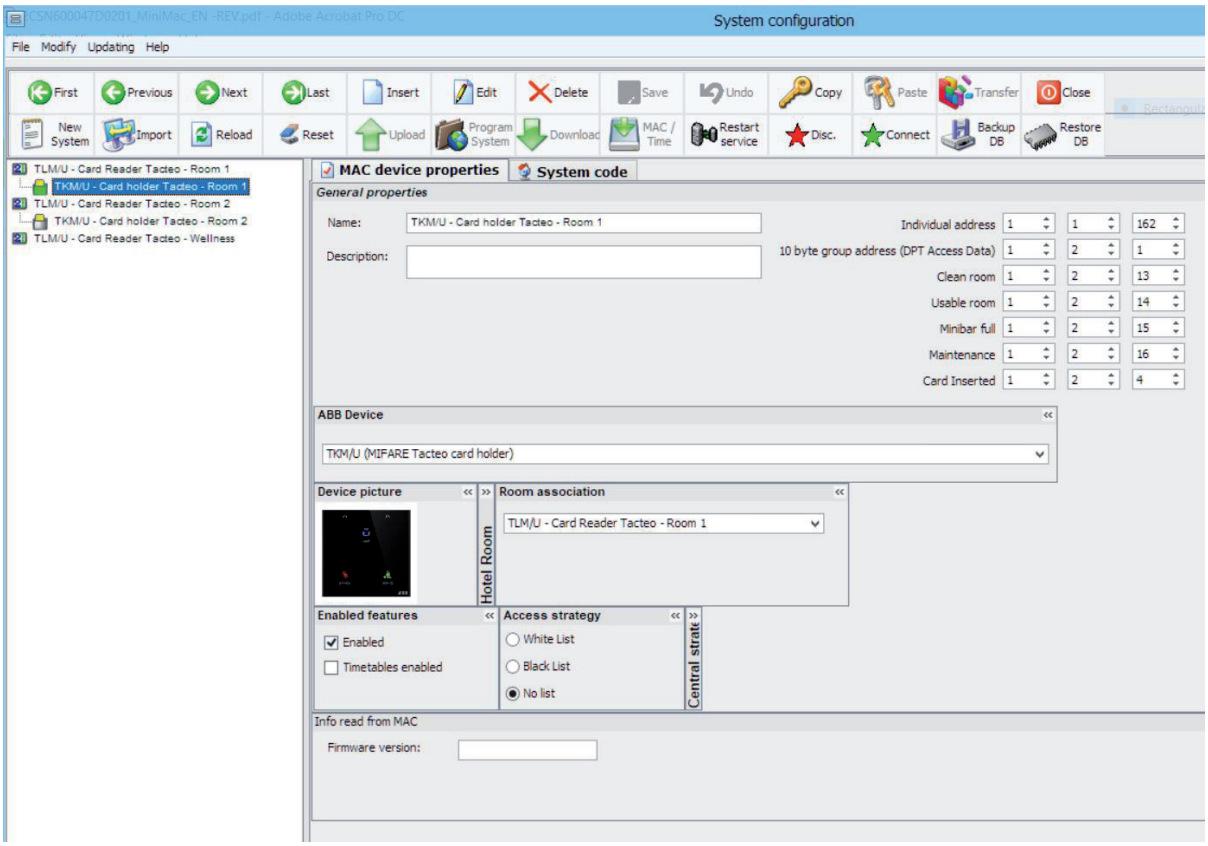


4.6.2.2 Transponder Holder

If in the installation there are transponder holders, it is necessary to add them in the “Plant” view and configure.

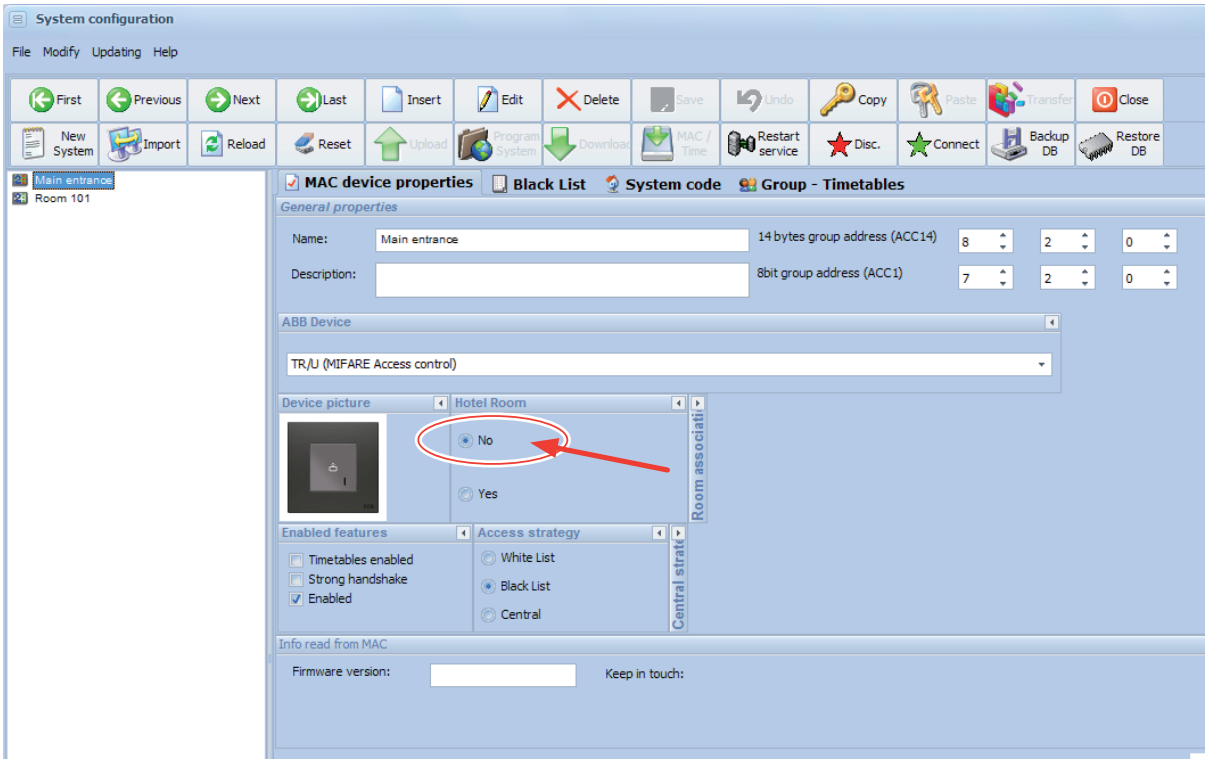
1. Select by the menu drop-down the type of transponder holder:
   - TH/U for Millenium
   - PTI/U for Chiara-Mylos-Elos
   - TKM/U for Tacteo
2. Configure the communication between MiniMAC and device specifying group address “ACC1, ACC14” for Chiara-Mylos and Millenium devices, “Access Data” for Tacteo devices Only for Tacteo devices:
   - configure the KNX physical address (Individual address) as already configured in the ETS project for this specific device
   - configure the group address related to MASTER TAG with special functionalities (Clean Room, Usable Room. Minibar full, Maintenance, Card Inserted), as already configured in the ETS project for this specific device
3. insert Name (and Descriprion, optional) of device
4. configure Access Strategy: for Transponder Holder devices, also if in the menu it’s possible to select other possibilities, the only acceptable methods are “No List” and “Black list”. The recommendation is configuring Access Strategy for Transponder Holder as “No List”. This means that the device accepts every valid (not expired) transponder cards with a system code correspondent to one of the system codes configured in the device
5. configure the device as “Enabled”
6. link the transponder holder to the related transponder reader using the menu “Room Association”. A room is composed by a transponder reader and (when present in the installation) a transponder holder
7. insert configured system codes using the menu in the tab “System code”. This operation is similar to that carried out for the transponder reader


System configuration
File Modify Updating Help
First Previous Next Last Insert Edit Delete Save Undo Copy Paste Transfer Close
New System Import Reload Reset Upload Program System Download MAC / Time Restart service Disc. Connect Backup DB Restore DB
Programmer
Transponder reader - Room 1
Transponder holder - Room 1
Transponder reader - Room 2
Tansponder holder - Room 2
Wellness Transponder Reader
MAC device properties
System code
General properties
Name:
Transponder holder - Room 1
Description:
14 bytes group address (ACC14)
8bit group address (ACC1)
ABB Device
TH/U (MIFARE Key Holder)
Device picture
Room association
Transponder reader - Room 1
Hotel Room
Enabled features
Timetables enabled
Strong handshake
Enabled
Access strategy
White List
Black List
Central
No list
Central strat
Info read from MAC
Firmware version:
2.0.10 - 07/11/2016
Keep in touch:


System configuration
File Modify Updating Help
First Previous Next Last Insert Edit Delete Save Undo Copy Paste Transfer Close
New System Import Reload Reset Upload Program System Download MAC / Time Restart service Disc. Connect Backup DB Restore DB
TLM/U - Card Reader Tacteo - Room 1
TKM/U - Card holder Tacteo - Room 1
TLM/U - Card Reader Tacteo - Room 2
TKM/U - Card holder Tacteo - Room 2
TLM/U - Card Reader Tacteo - Wellness
MAC device properties
System code
General properties
Name:
TKM/U - Card holder Tacteo - Room 1
Description:
Individual address
10 byte group address (DPT Access Data)
Clean room
Usable room
Minibar full
Maintenance
Card Inserted
ABB Device
TKM/U (MIFARE Tacteo card holder)
Device picture
Room association
TLM/U - Card Reader Tacteo - Room 1
Hotel Room
Enabled features
Enabled
Timetables enabled
Access strategy
White List
Black List
No list
Central strat
Info read from MAC
Firmware version:

4.6.3 Configuration of common areas and entrances

In a hotel installation there are not only rooms but also common areas as main entrance, wellness area, swimming pool, car parking, to add new devices to the system, from System menu click on NEW to insert new transponder readers required. These are transponders not associated with a hotel room and the flag "NO" has to be set in the "Hotel room" setting.



In the example, the device has been configured in the Black list, since usually for main entrance and common areas it is necessary that access is granted to every person owning a valid TAG. Every created TAG is automatically accepted by the device, only the exceptions decided by the system administrator do not get access. Such exception must be inserted in the device Black list.
Obviously it is also possible to configure the devices in White List, and simplifying configuration of accesses granted for these common areas using the “Extra Access” tab in the Group menu (see paragraph ***“4.3.2 Extra accesses”***)
After the device is created, it must be programmed with the system codes. The procedure is the same as previously described: SYSTEM CODES TAB, EDIT and clicking on the appropriate button in the minitoolbar, system codes can be added to the list.

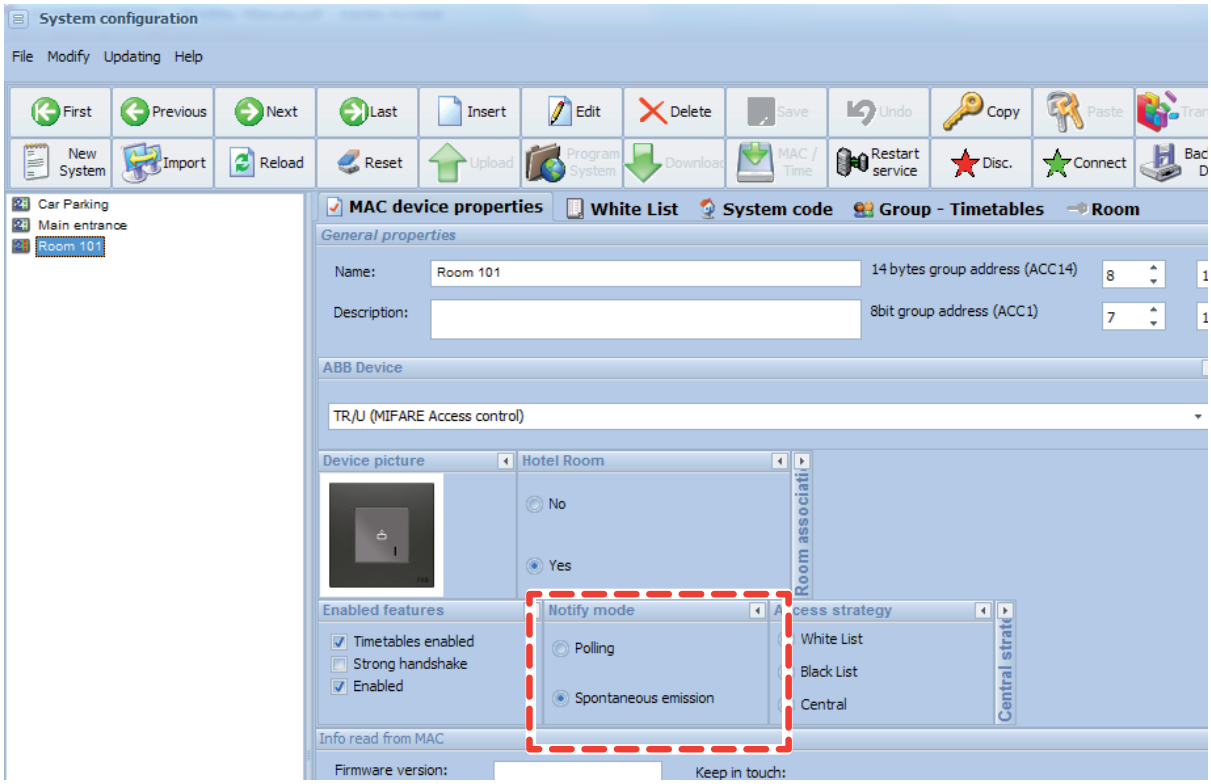
Note
System codes insertion is mandatory: a device without system codes does not let pass anybody.

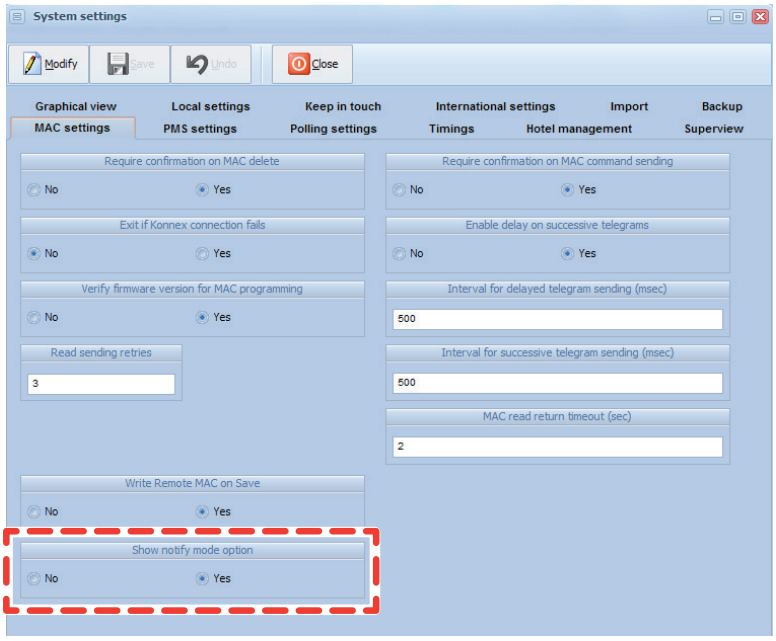
Finally, consider the groups: each device can contain any number of groups, even none. In this case, no group is defined because there is no need to set timeslots for this access. Apart from the fact that groups are not defined, timeslots are disabled in the device properties.

4.6.4 Configuration of notify mode

Note

Please pay attention that “Notify mode” menu is by default hidden in the “MAC device properties”, and therefore the Notification mode is automatically set as “Spontaneous emission”, which is the mode suitable for all the installation, granting good performances. When and if required, it’s possible to show the menu “Notify mode”, enabling it in the “Settings” menu, under “MAC settings” TAB, the “Show notify mode option”.

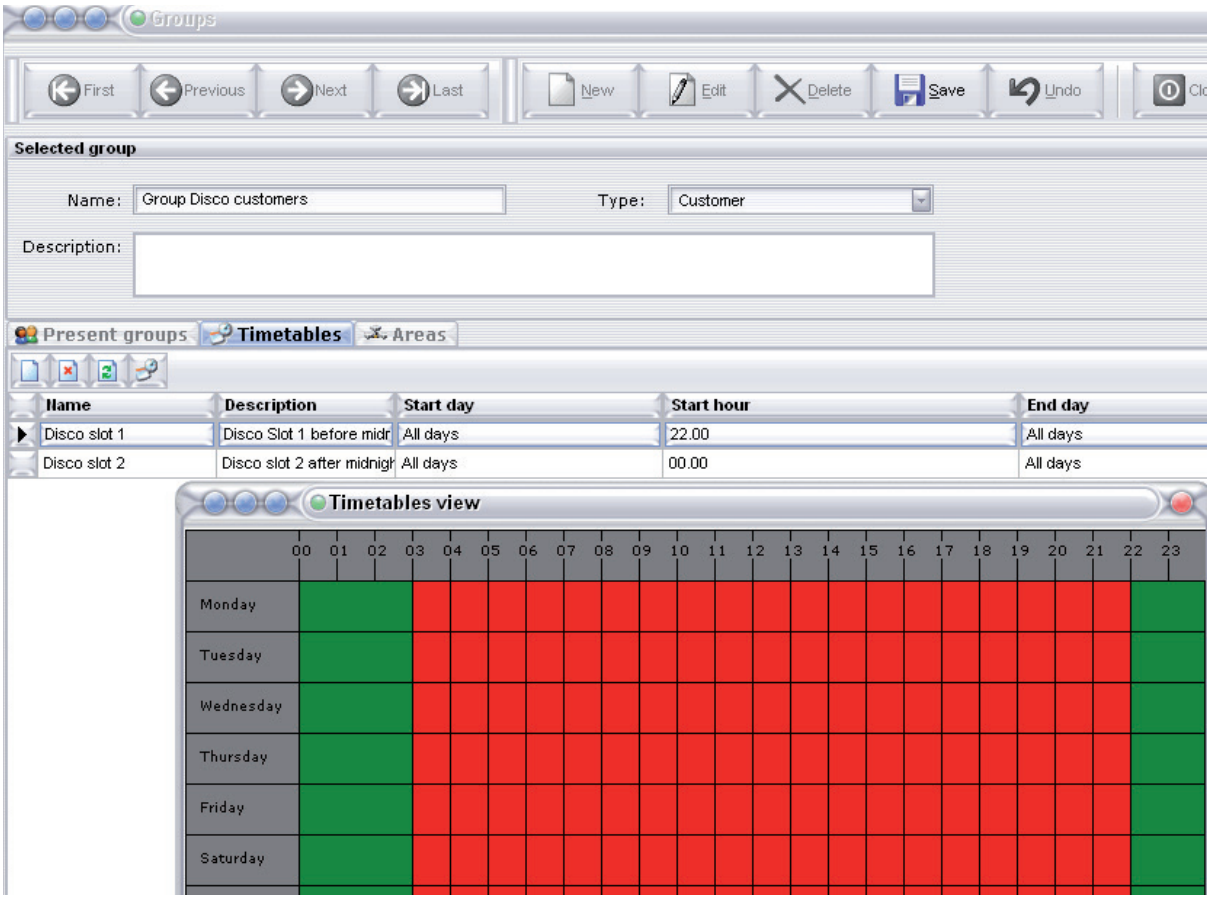




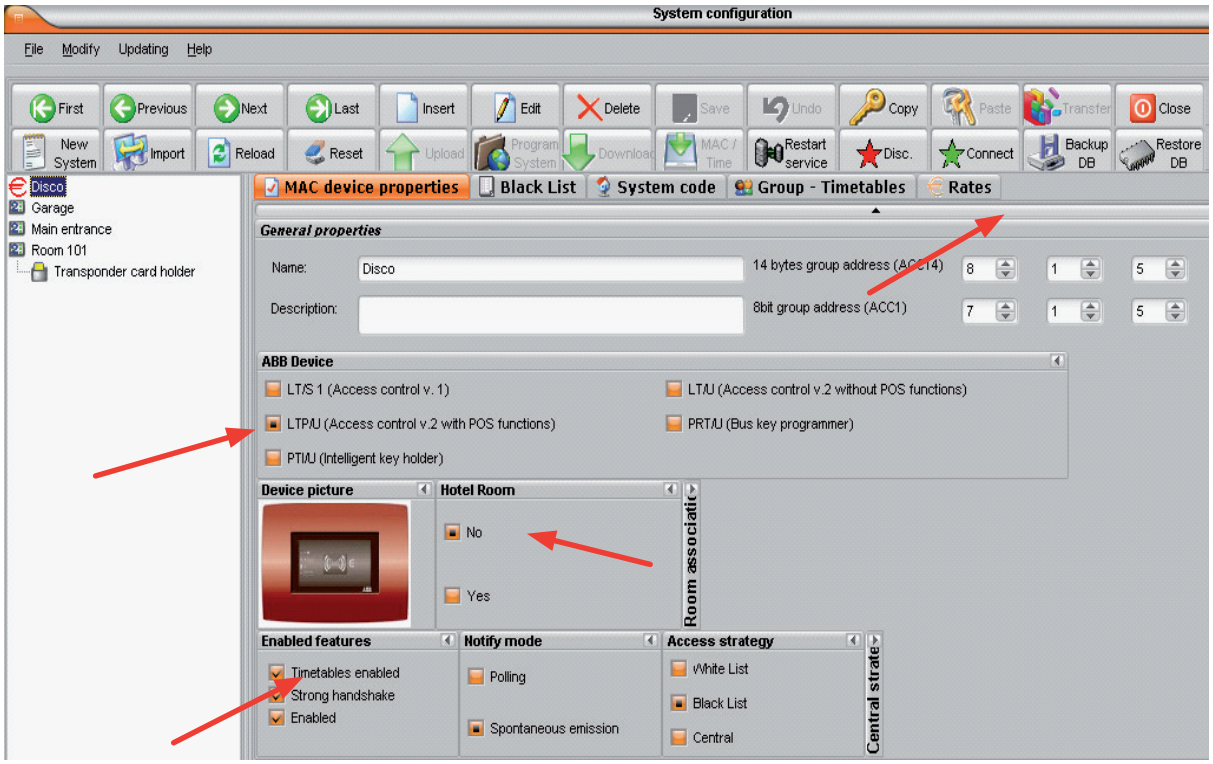
4.6.5 Configuration of payment entrances

Note
Management of payment services with access control system is available only using Chiara, Elos and Mylos range, where you can find transponder reader with “virtual money” functionality.

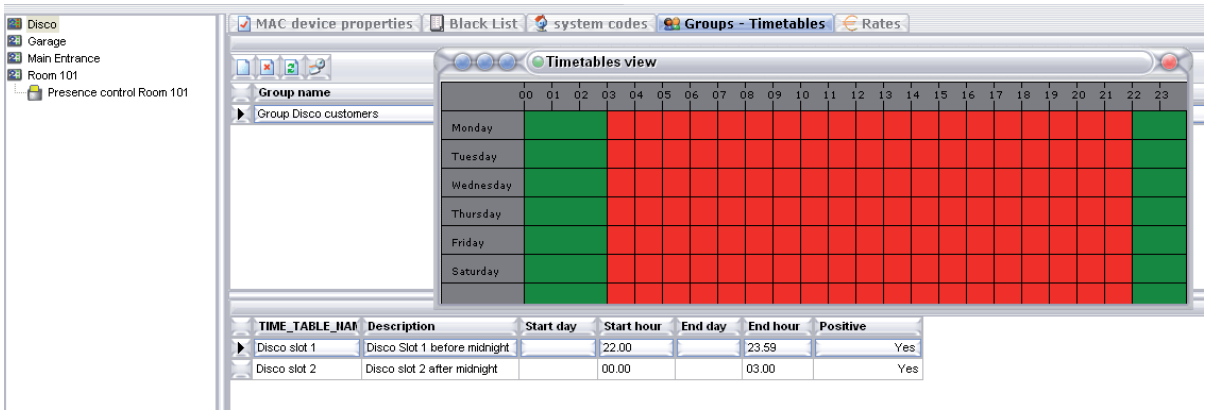
It is possible to manage the access to payment entrances (i.e. wellness centres, discotheques, car parks, etc.). In these cases, it is necessary to use transponder readers with POS function (LTP/U). A LTP/U is not very different from a normal transponder (LT/U): it is perfectly identical, apart from the fact that it contains information about rates management that needs to be entered for the access to the entrance. To insert the device, click NEW from the system menu and insert, for example, a device for the disco access control. You can configure it in the Black list and timeslots will be activated: for example, for client access only from 22 to 3.00. For this purpose, a timeslot beginning on the evening of a certain day and ending the following day is created. Therefore two slots must be defined: the first from 23:00:00 to 23:59:59 and the second from 00:00:00 to 03:00:00. The group must contain both timeslots:



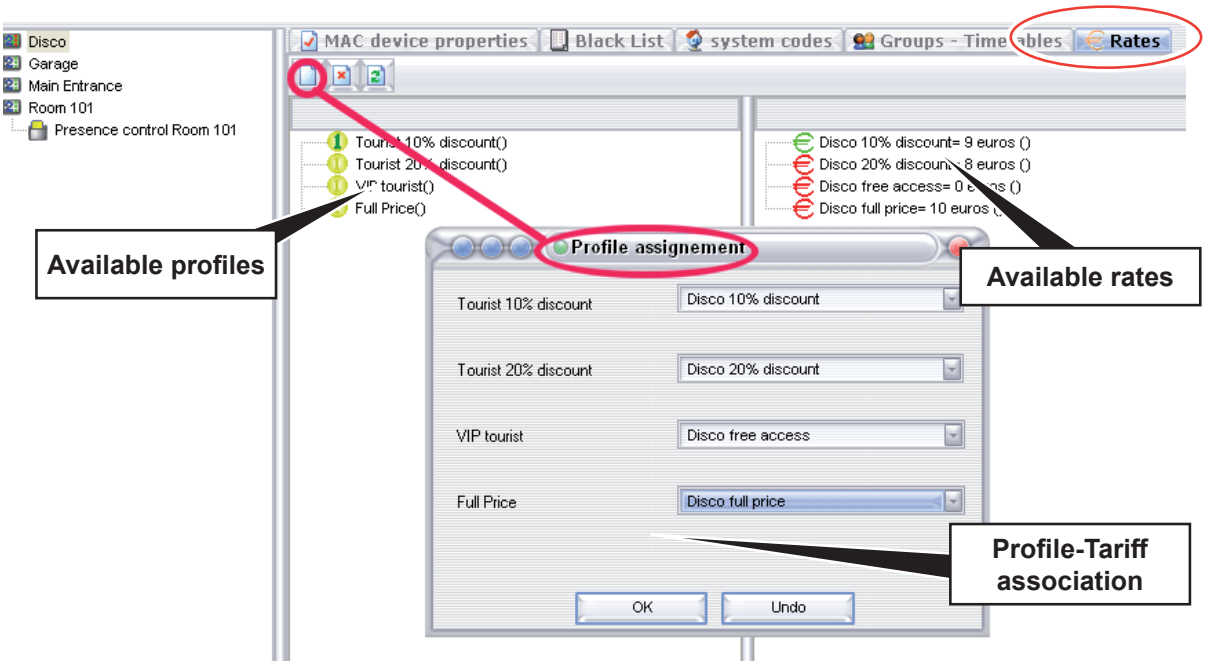
Create discotheque access control in the usual way:



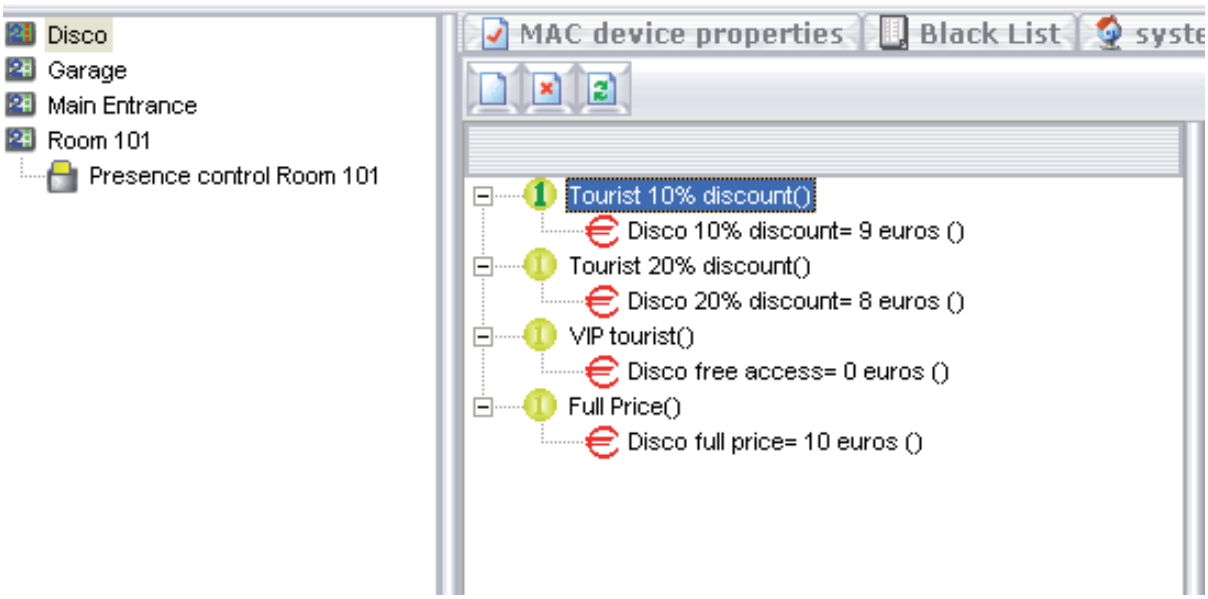
Also in this case (as for traditional transponders) remember to set system codes and groups:



Click on Rates TAB, a window shows up to insert the suitable rate for each one of the 4 profiles we previously defined:



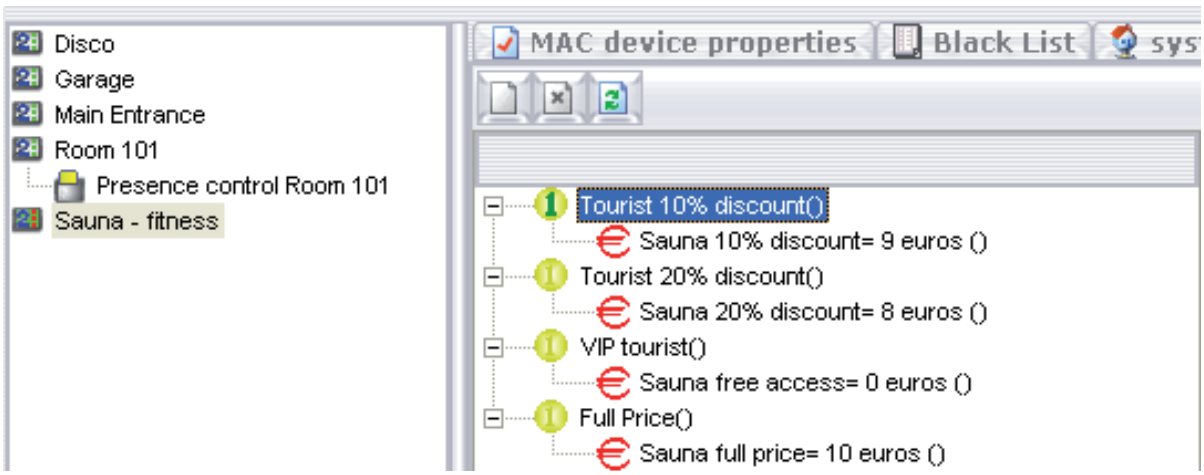
Assigning the rates to the profiles, we get for example:



At the same time you can proceed, as in the example, with the transponder reader with POS function associated with the SAUNA: the procedure is the same as those previously described.

To sum up, in order to configure payment entrances in the system, you have to:

- Create all rates for payment entrances (wellness centre, discotheque, car park, etc.) both at full price and discounted (section ***"4.5 Rates creation"***).
- Rename the default profiles available in MiniMAC, based on manager needs, so that they clearly refer to a specific customer type: i.e. regular customer, holiday packages, etc. (section ***"4.4 Rate profiles definition"***)
- Associate one of the 4 available profiles, or more, with each POS reader (see above).
- When creating transponder TAGs (i.e. for the check-in to a hotel), program the TAGs associating each customer with the profile that corresponds to the appropriate rate type (section ***"7.2 Check-in"***).

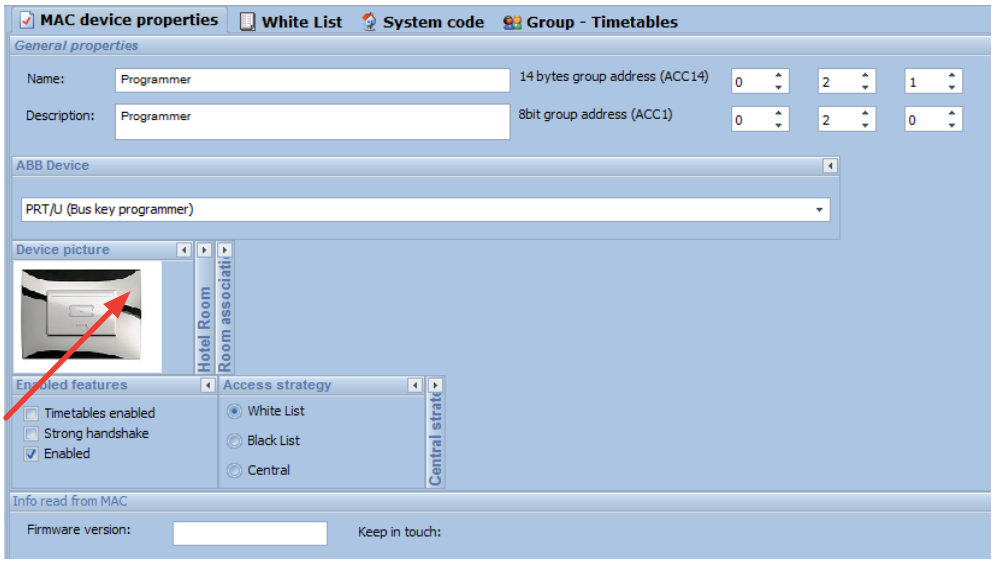


4.6.6 Transponder programming device

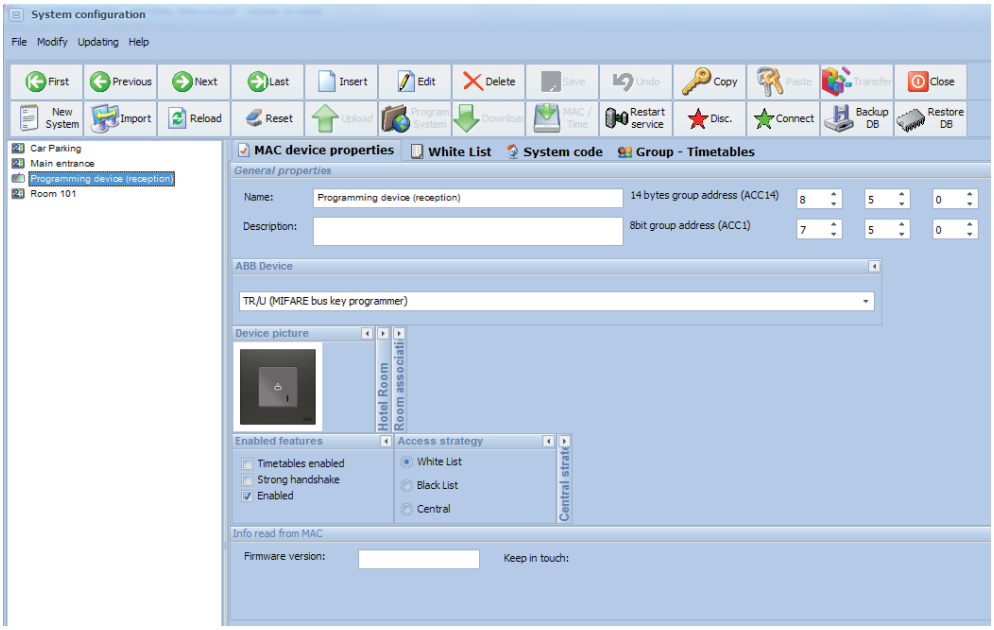
To complete the system, the last device to be set is the TAG programmer (transponder cards, TAGs). The programming device is used to program transponder TAGs to be used in the system for the access to the various entrances. The programming device is used together with the MiniMAC software (section ***"7.2 Check-in"***, section ***"7.4 Check-out"***).
The transponder programming device interfaces with the KNX bus like all other devices, therefore it must be inserted in the system.

There are three types of transponder programming devices to be used, according to type of access control system chosen:

- For Chiara, Elos, Mylos system use as programming device PRT/U
- For Millenium and Chiara MIFARE (MIFARE) system use as programming device TR/U, configure its behavior in the "Plant" menu, under "MAC device properties" of the specific device
- For Tacteo (MIFARE) system use a USB programming device. This USB programmer has not be to be added in the Plant menu, as on the contrary is required for PRT/U and TR/U

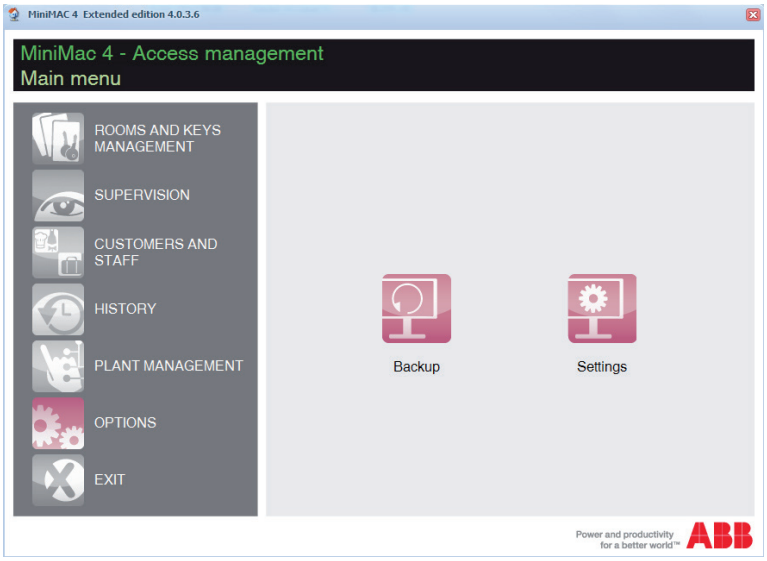


Chiara, Elos, Mylos programming device (PRT/U)

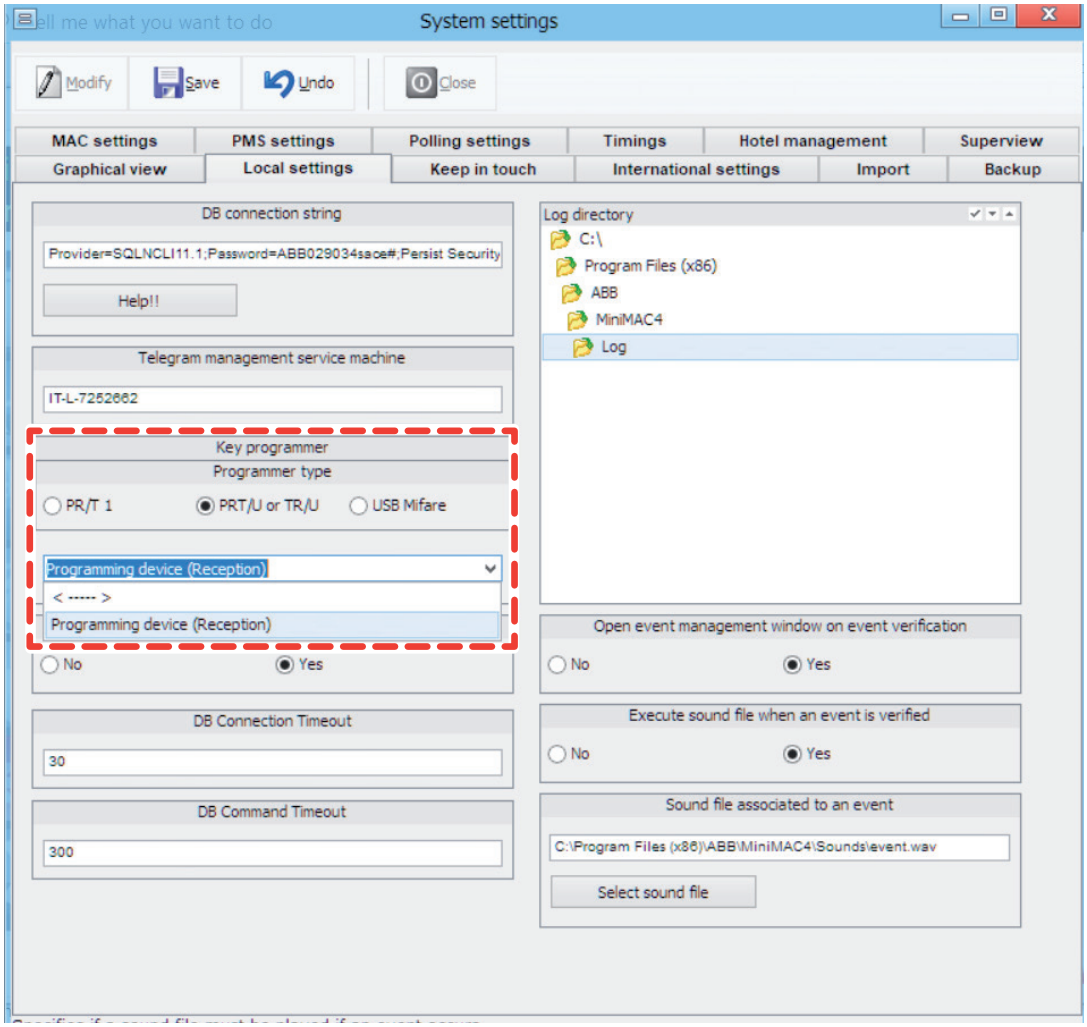


Millenium programming device (TR/U)

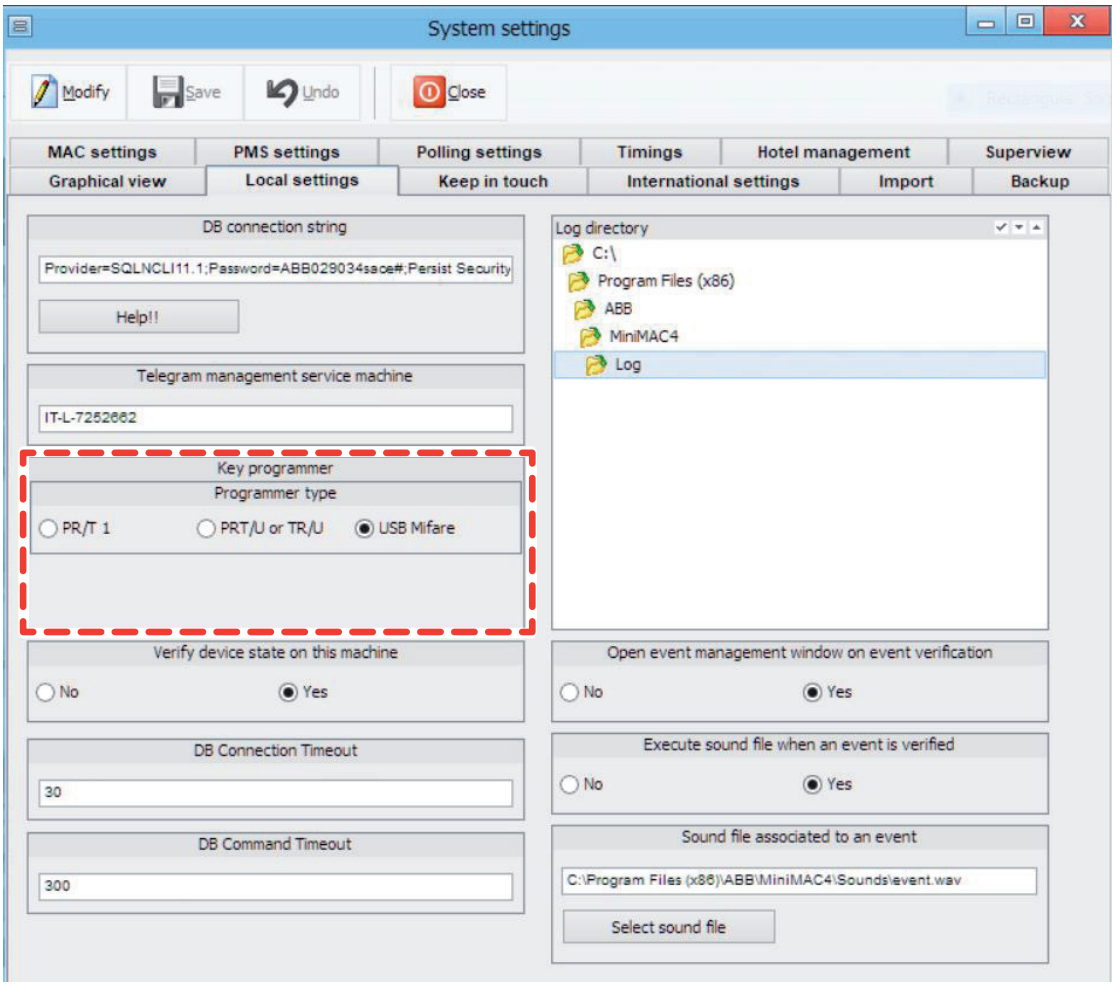
Since in a system there are as much clients as TAG programmers, the device to be used must be specified in the program. In our example we have just one device; however, the type of programmer must be specified in the setting menu.



For Chiara-Mylos programmer (PRT/U) and Millenium programmer (TR/U) you need to select which device using, since more than one programmer (client) you can have in one installation

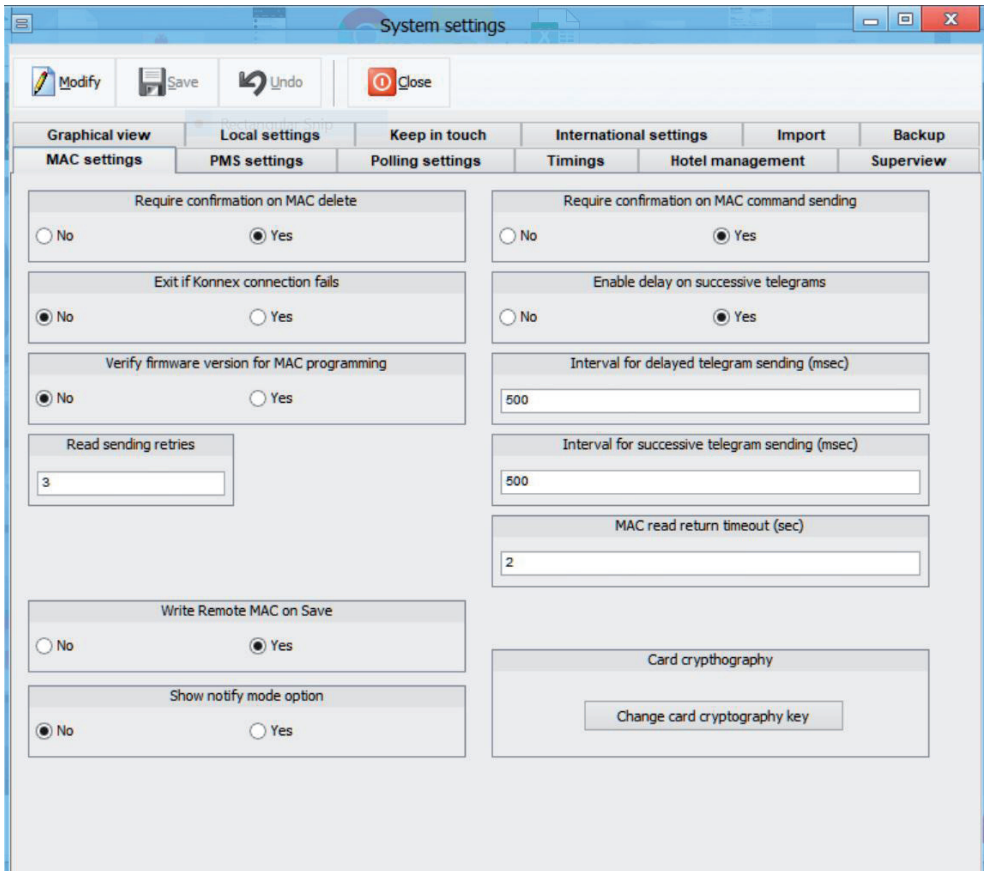


For Tacteo range USB Programmer is not a device belonging to the system and therefore you need only to select the type of programmer (USB Mifare)



4.7 Access Control keys encryption (only for Tacteo range)

In order to grant an higher level of security, contents of access control keys/TAGS writen by MiniMAC software is encrypted. The encryption key is automatically and randomly generated at every MiniMAC installation. During programming phase (when MiniMAC software write/download the access control configuration into the memory of the devices), this encryption key is saved into the devices. It is therefore recommended to perform the first download of MiniMAC configuration on the devices in a protected environment in order to avoid that someone try to read this encryption key on the KNX bus. Once the encryption key is saved onto the Access Control devices, no other encryption keys can be downloaded overwriting the previous one. In order to reset the encryption key of the devices and downloading a new one, it is possible to press 5 times consecutively the KNX programming button, taking care that the LED of the push-buttons on the front of the device turn to “blue” color: when this happens it is necessary to press the KNX programming button one last time. The device is now ready to receive from MiniMAC software a new encryption key.
As an alternative it is possible to create a new encryption key in an existing installation/plant, using the menu Options > Setttings. In the tab “MAC settings” it is possible to create a new encryption key clicking on the button “Change card Cripthography Key”. It is asked confirmation 3 times in order to complete this procedure.



Warning
With the change of encryption key the installation/plant is no more usable: all the keys/ TAGS previously created, and all the access control have stored internally the previous encryption key, and therefore the access control devices do not work with the old keys/ TAG created. In order to download the new encryption key, follow the above procedure.

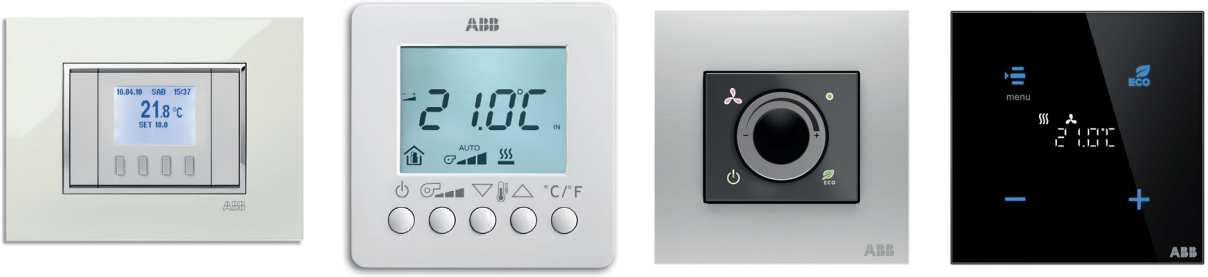
Warning
With a firmware update of the device, for security reason the encryption key is reset. In this case, after a firmware update, it is enough go to the “Plant” menu of MiniMAC and pressing “Download” / “Program system” button: with this operation the new encryption key is downloaded into the Access Control devices that have update the firmware, without need of additional operation on the devices.

4.8 Heating and Cooling Supervision

MiniMAC allows you to manage room Heating and Cooling.
MiniMAC allows you to manage KNX thermostat, especially three different thermostat types, as you will see later:

- TUX/U thermostat of the access control range (discontinued product)
- Generic ABB KNX thermostat (i.e. Mylos KNX thermostat, or thermostats of the Busch Jaeger range)
- Generic KNX thermostat

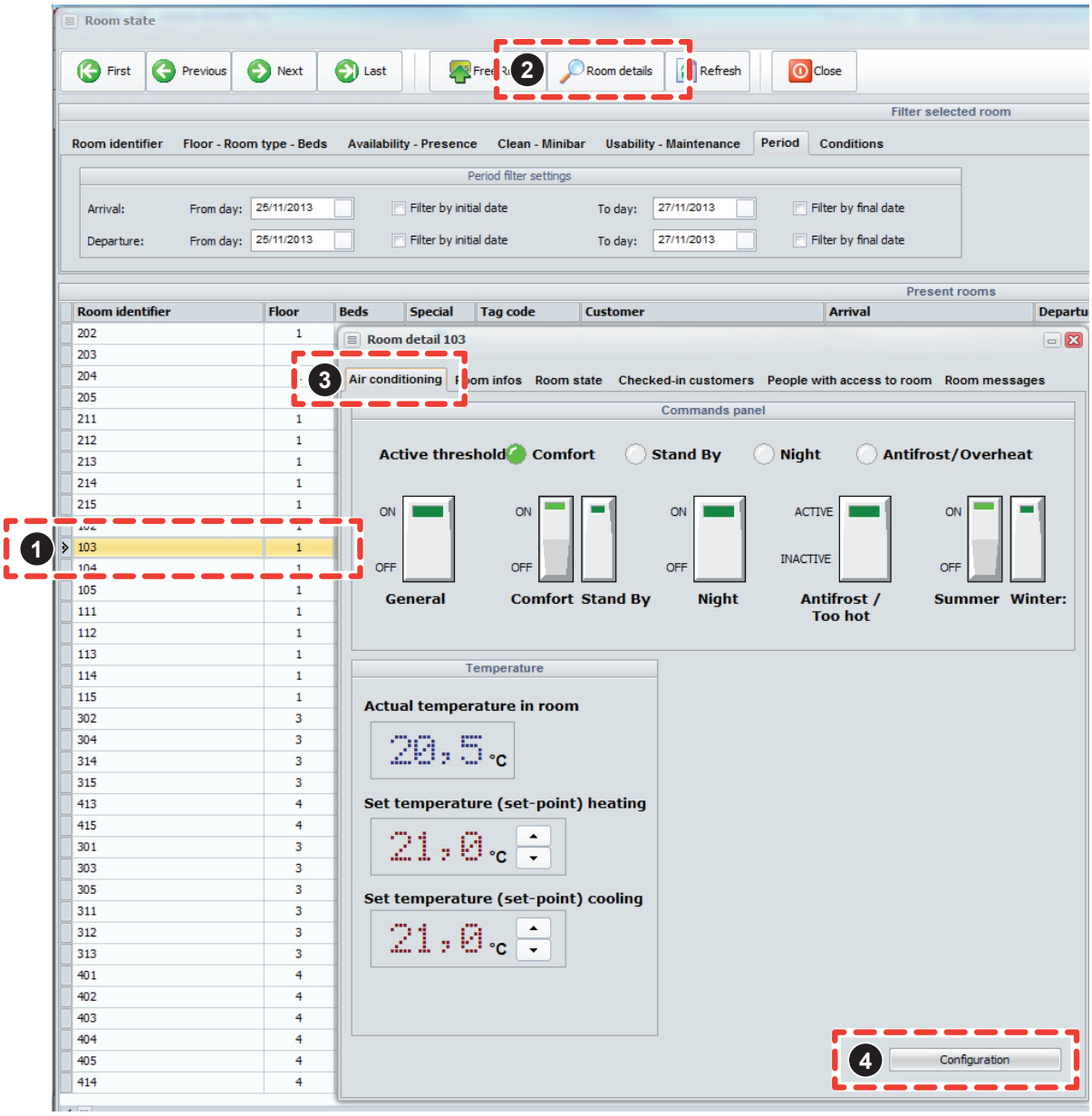
The supervision operations that can be performed by MiniMAC from the reception are summarised below:



- set summer-winter season
- set the set-point between day and night
- set anti-frost or overheat function
- set the setpoint (stand-by/comfort)
- adjust room temperature set-point in real time
- display current room temperature

It is worth remembering that MiniMAC allows you to manage generic KNX thermostats, not necessarily belonging to the ABB range.
In this case, the supervision function is still available with limitations depending on the model used.
In any case, all KNX thermostats offer more or less the same communication objects and most of them allow you to monitor the main functions (for example, setting the room setpoint temperature, display of the current temperature and summer/winter selection).

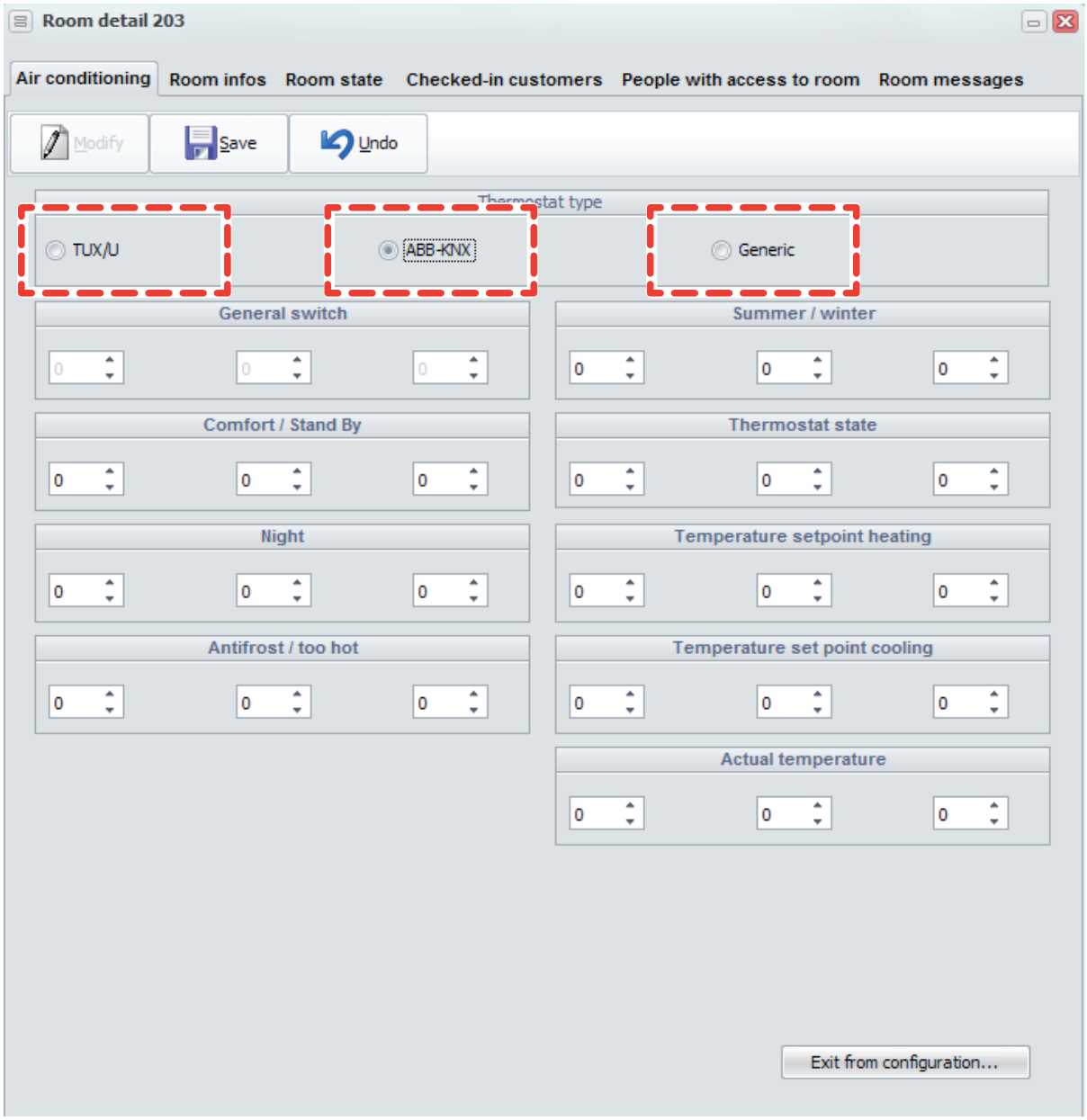
Configuring a KNX thermostat is easy.
Go to "Room Management" menu, select the room (**1**) that you wish to equip with a thermostat, then click on Room details (**2**):



Once you entered the "Room details" screen, click on Heating/Cooling (**3**) TAB to configure, using the "Configuration" button (**4**), Heating and Cooling supervision for the specific room.

It is necessary to:

- Choose the thermostat type: TUX/U, generic ABB KNX (i.e. Mylos KNX or any Busch Jaeger thermostat), generic KNX thermostat
- Connect thermostat group address to MiniMAC supervision.



The available group addresses will be connected based on the type of thermostat: if some addresses are not available (for example, on the generic thermostat) the associated function is not available.

As you can see from the figure, it is possible to set the heating and cooling setpoint from the room supervision. To manage room Heating and Cooling in this mode, it is necessary to configure the ABB KNX thermostat (Mylos KNX or Busch Jaeger thermostat) using individual set-points (and not dependent setpoints): in this case, specific setpoints are displayed (it is usually linked to comfort setpoint supervision); using dependent setpoints on the thermostat, it is not possible to manage Heating and Cooling supervision via MiniMAC.
To manage the cooling (summer) and heating (winter) setpoint, the thermostat will be configured as Summer-Winter, with the possibility to switch between summer and winter directly managed by the thermostat, or performed "manually" sending a communication object to the thermostat.

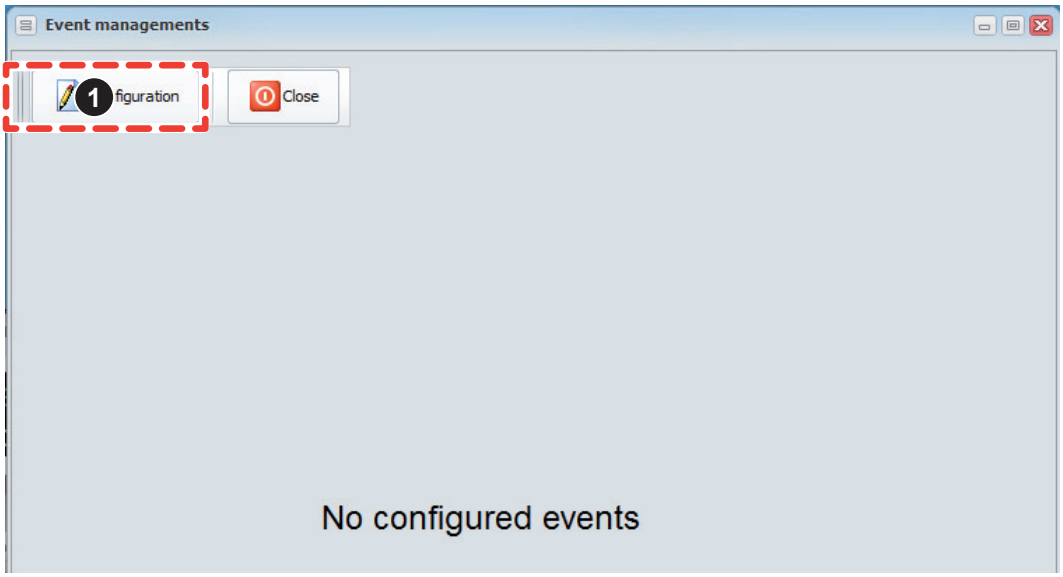
In case a NON ABB (GENERIC) thermostat is used, the supervision screen allows you to control the data indicated in the figure: as compared with the TUX/U thermostat, it does not show fan coils speed, thermostat status and other functions that depend on the thermostat characteristics.

Note
Please remember that for all kind of KNX thermostats managed by MiniMAC, the possibility of changing operating mode (comfort, standby, night, anti-frost/heat protection) is based only on three 1bit KNX communication object (using of 1byte object is not supported).

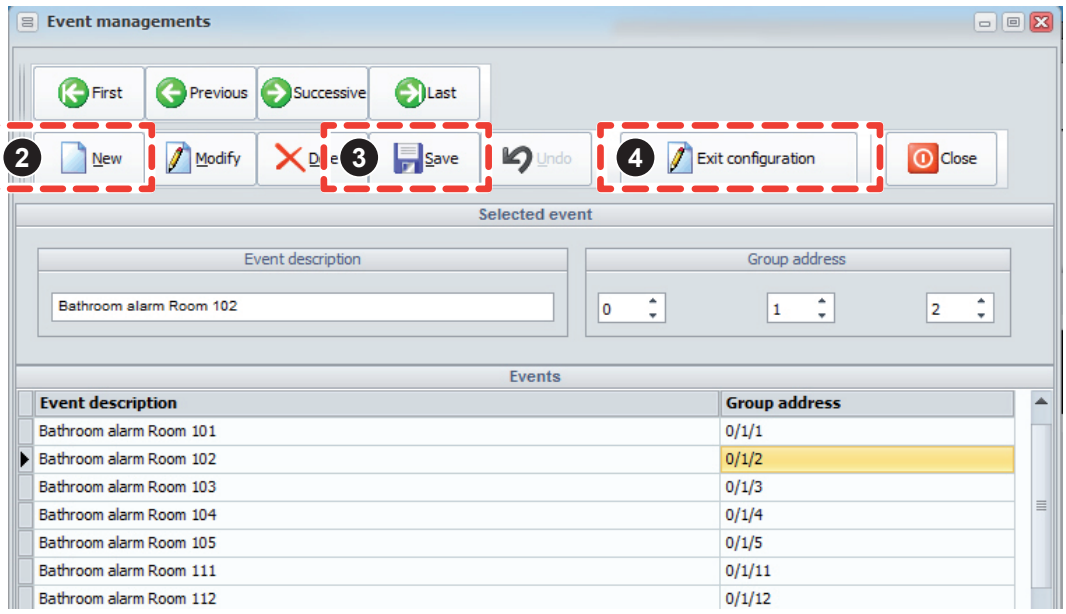
4.9 System Events Supervision

MiniMAC offers the chance to create a panel including indicators that can be associated with system events. Each event must be associated with group addresses.
In the case an event is detected, the panel shows up with the blinking indicator; an acoustic signal can also be emitted to draw operators attention.The acoustic signal is customisable adding a .wav or .mp3 file to the sounds folder as indicated in the Settings panel.

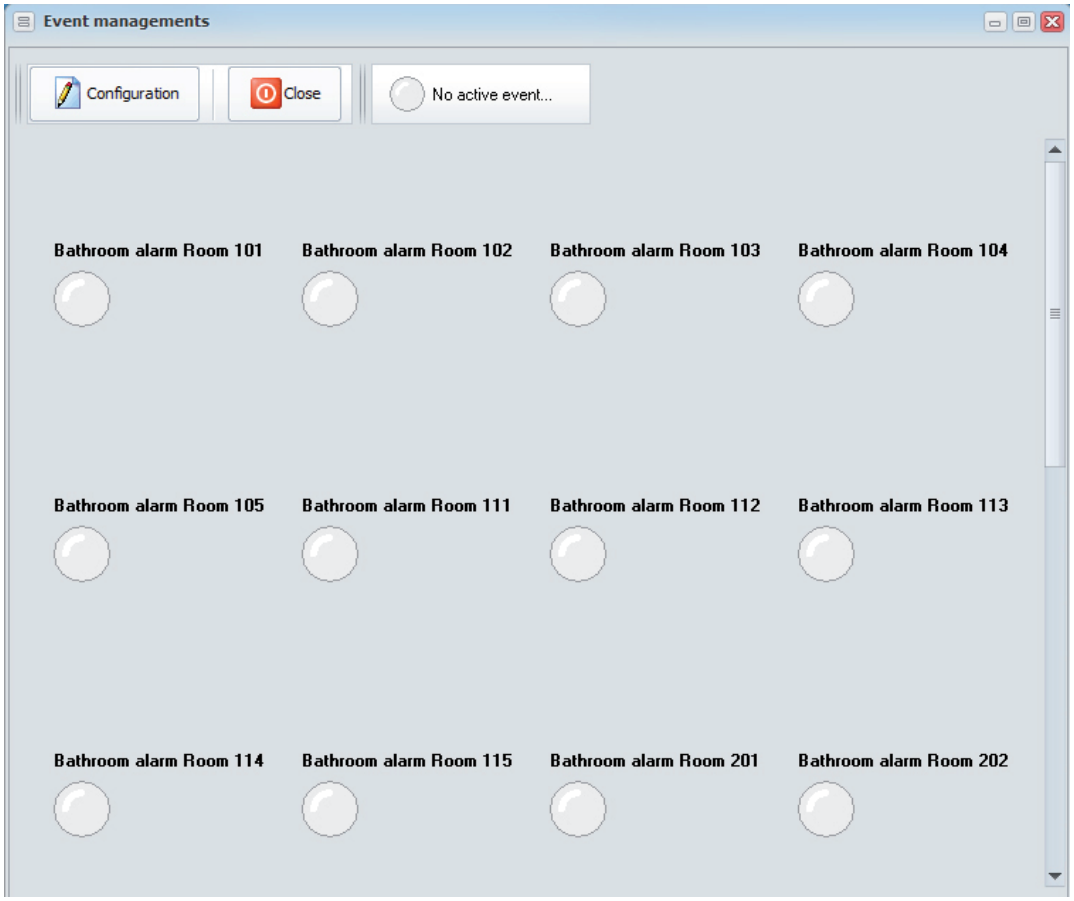
To create an event, click on CONFIGURATION (**1**)



and then on NEW (**2**). Insert a description and select the associated group address.
Then SAVE (**3**) and EXIT FROM CONFIGURATION (**4**).



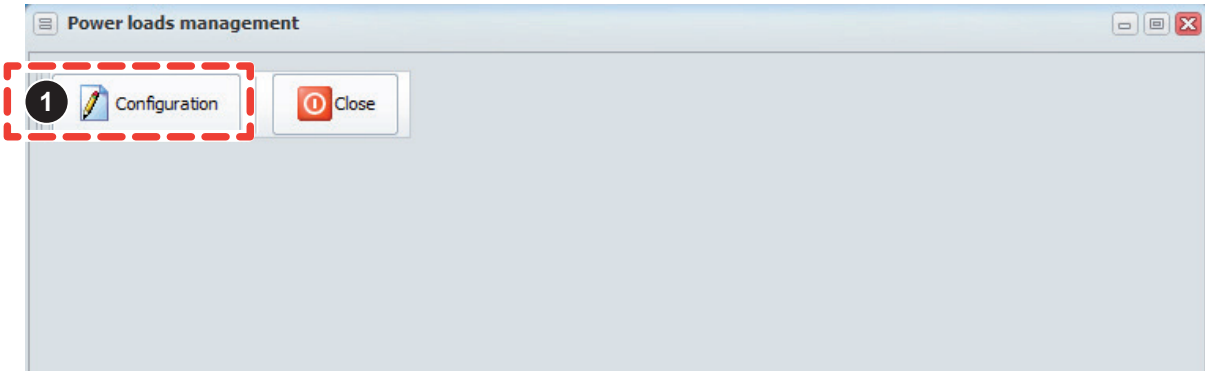
Note
If one of the configured events happens, associating them with the appropriate group addresses of the KNX building automation system, the panel with the blinking event shows up on all Customers connected to the LAN:



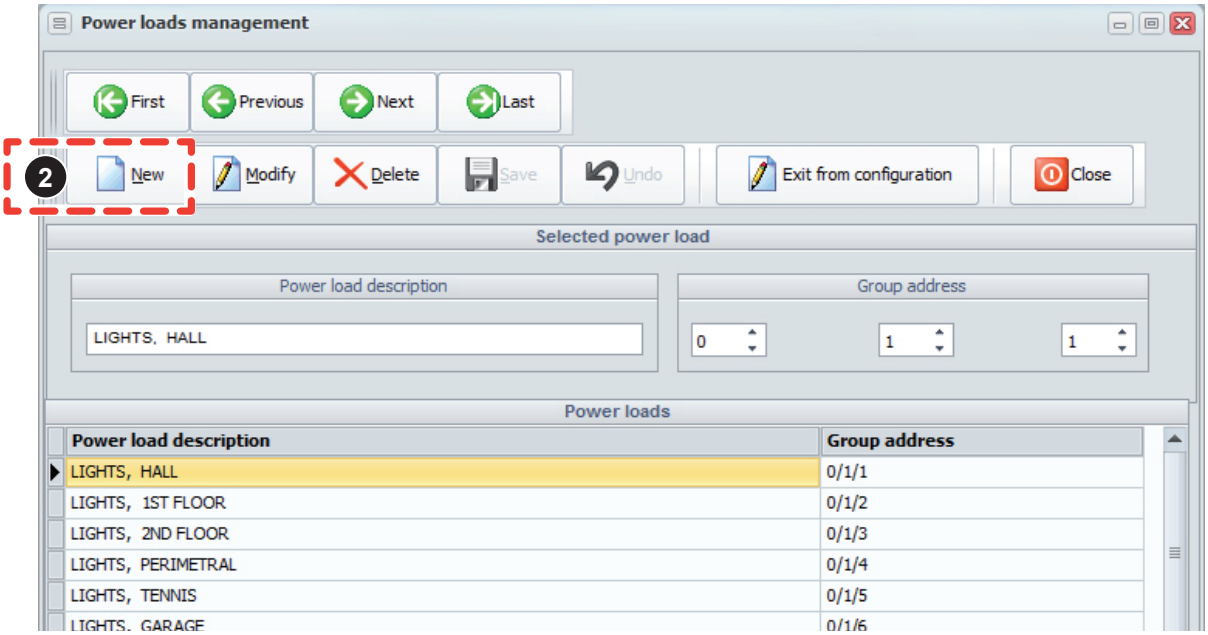
4.10 Loads Management

MiniMAC can create a control page including ON/OFF commands and red/green LEDs. Through this page, ON/OFF group addresses can be connected to actuators of the KNX system.

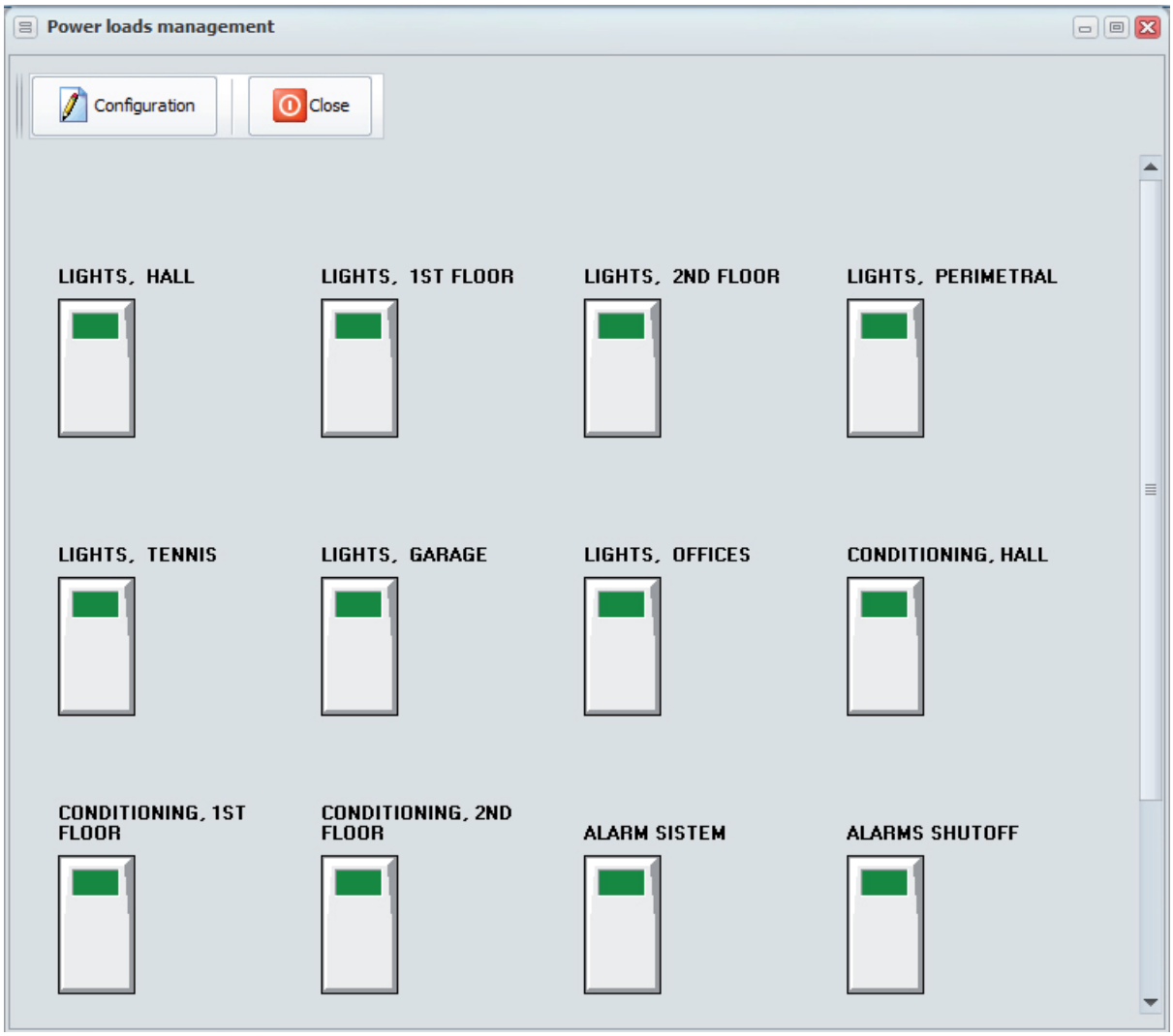
An ON/OFF command can be easily created: from Loads Management menu click on configuration (**1**).



Click on NEW (**2**) and insert a description with the associated group address:



Saving and exiting the configuration, you directly enter the control board where the corresponding red/ green indicators are already present.



4.11 Other installations

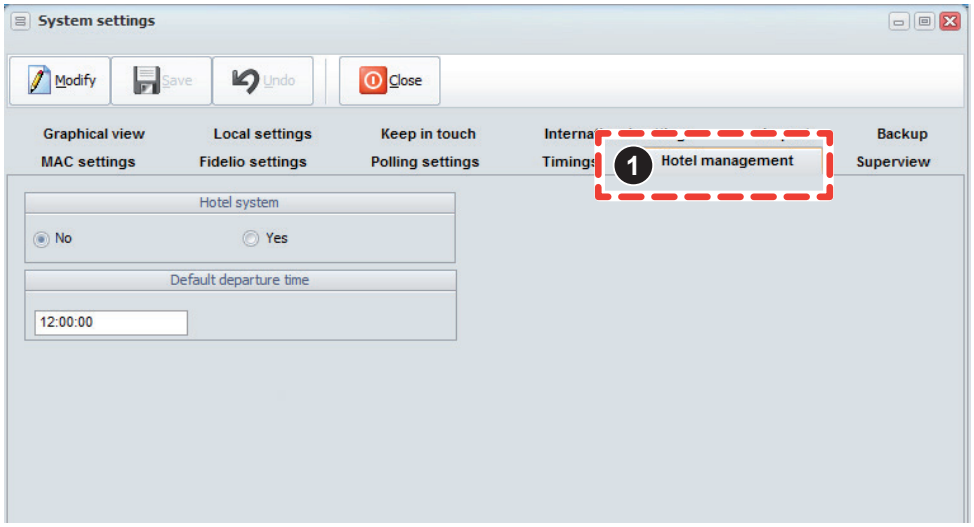
The ABB access control solution is particularly appropriate for hotel applications, where managers need every day to:

- Grant controlled access to hotel rooms to customers and authorised personnel
- Check the presence of customers in the rooms and automatically activate room loads only in the case of presence
- Have a complete supervision software allowing the management of the entire system from the reception and in particular also customer check-in/check-out and transponder TAGs.

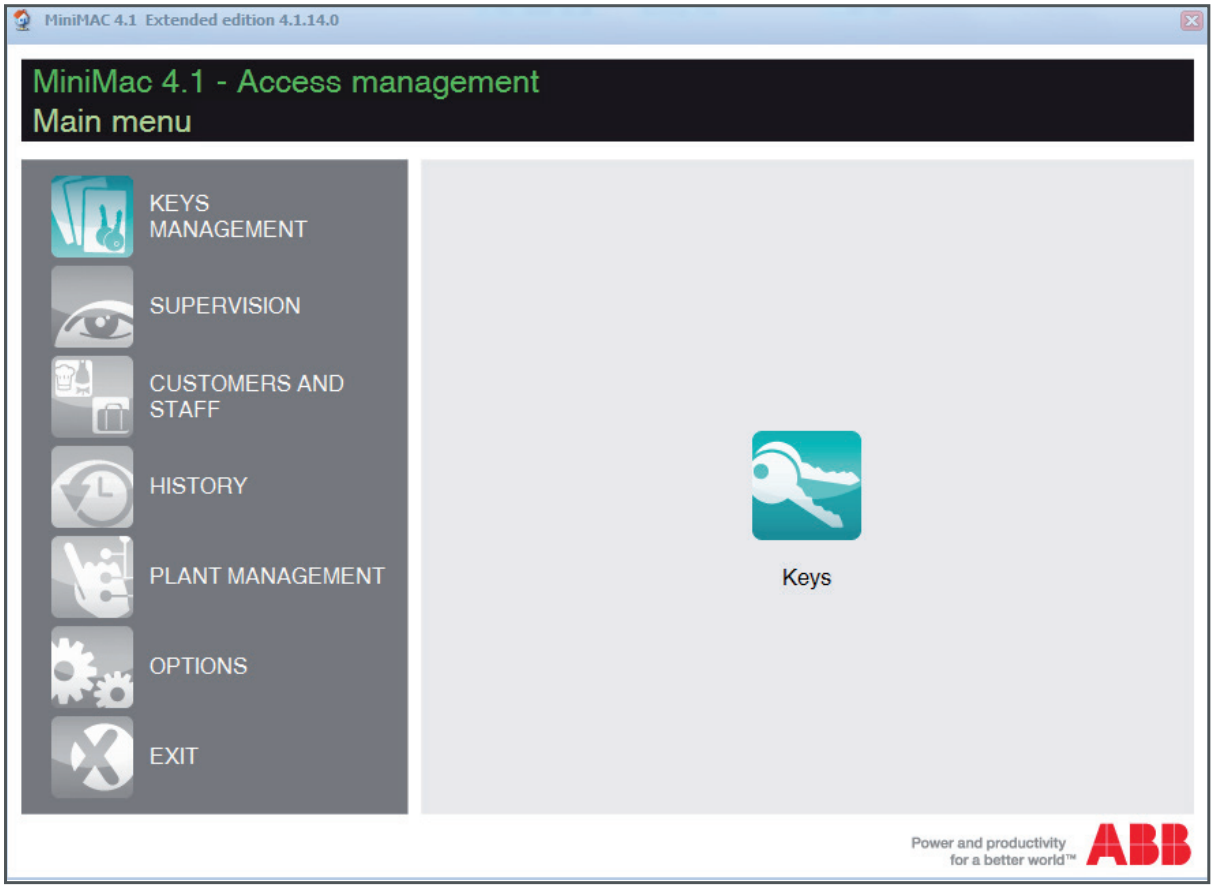
The ABB access control solution can be perfectly used also for other applications, where there is still the need to grant a controlled access to entrances/rooms/environment. For example:

- Wellness and fitness centres
- Paying car parks
- Offices
- Laboratories
- Common areas in apartment buildings

In all cases where ABB access control is used for other applications, MiniMAC software can be configured from the Settings menu, "Hotel management" TAB (**1**): set the "Hotel installation" flag to "No", which is set on "Yes" by default. In this way, MiniMAC is configured to manage other installations different from hotel installations.

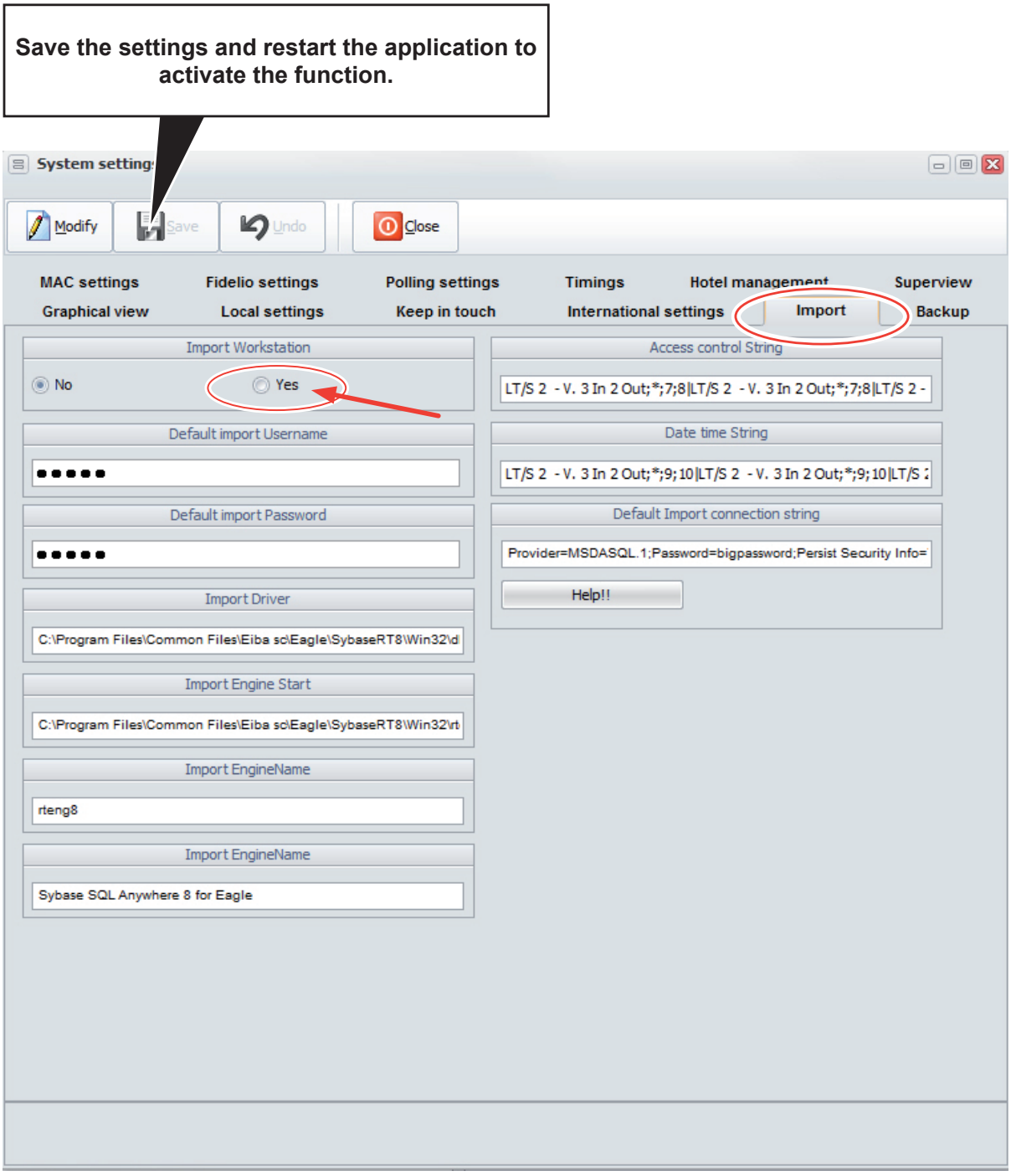


As you can see, the main menu changes accordingly (i.e. the menu "Rooms and cards management" becomes "Cards management"). All functions for room management will disappear from MiniMAC, since they are specific for hotel installations (i.e. check-in/check-out, Heating and Cooling supervision, room presence history, etc.).
The management of other installations is the same as that for hotel installation: the functions are exactly the same as those already described, expect for the ones that are specific for a hotel installation.



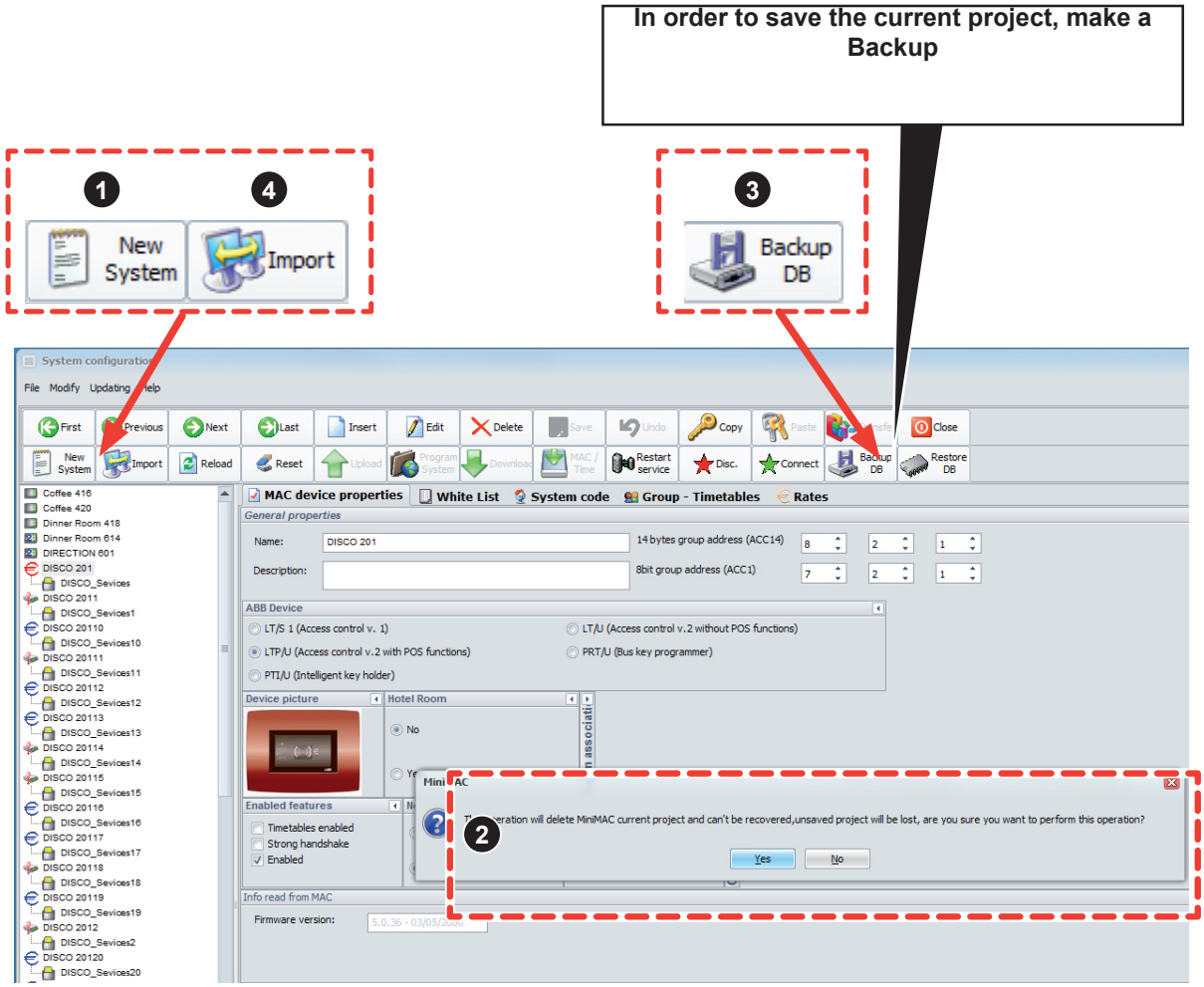
4.12 Importing a project via ETS

In order to use this function, you must activate it using the MiniMAC Settings icon shown below:



Going back to "System" menu, under "System management" you can import an ETS project.
The import process adds the devices present in the KNX project that you choose to your MiniMAC project.

If you wish to have, inside the system, only the devices of the KNX project to be imported, you need to start another project before performing the import process, clicking on "New system" (**1**):
Selecting YES (**2**), the current MiniMAC project will be deleted.
The project will be lost if it was not saved with the backup (**3**).
At this point, to start importing an ETS project in MiniMAC, you only need to select the IMPORT (**4**) icon in the System menu:



At this point, MiniMAC allows you to choose the type of KNX project to be imported:

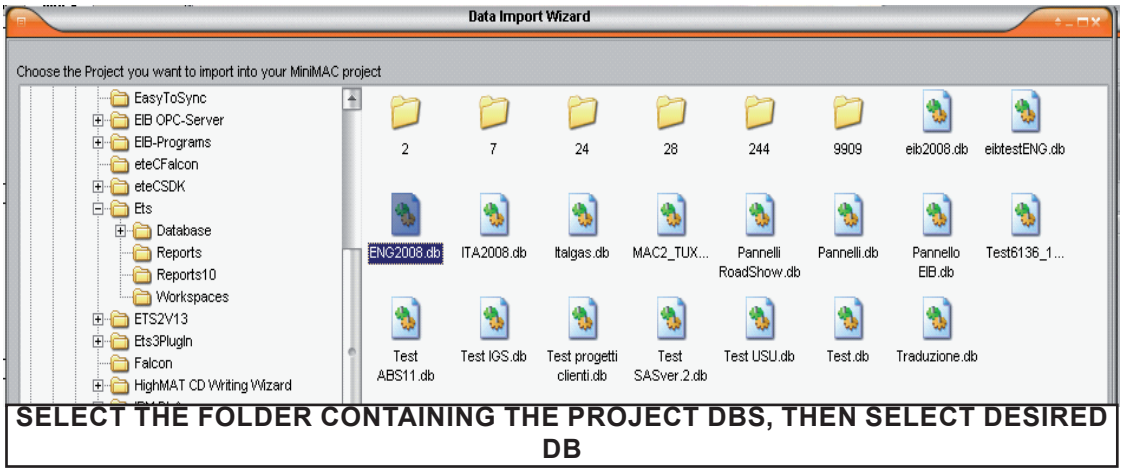
- ETS 3
- ETS 4

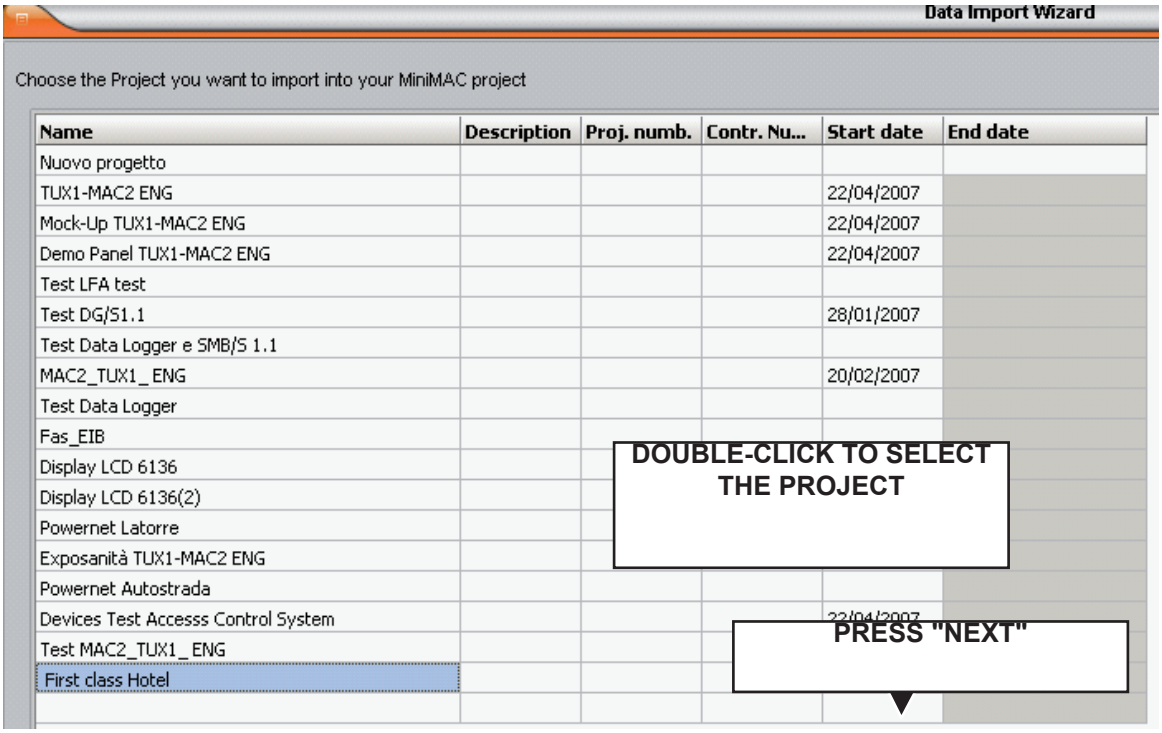
Clicking on the image ETS 3 or ETS 4 and then on "Next", you choose the type of ETS project to be imported.

4.12.1 Importing a project from ETS 3

When importing from ETS 3 you need to:

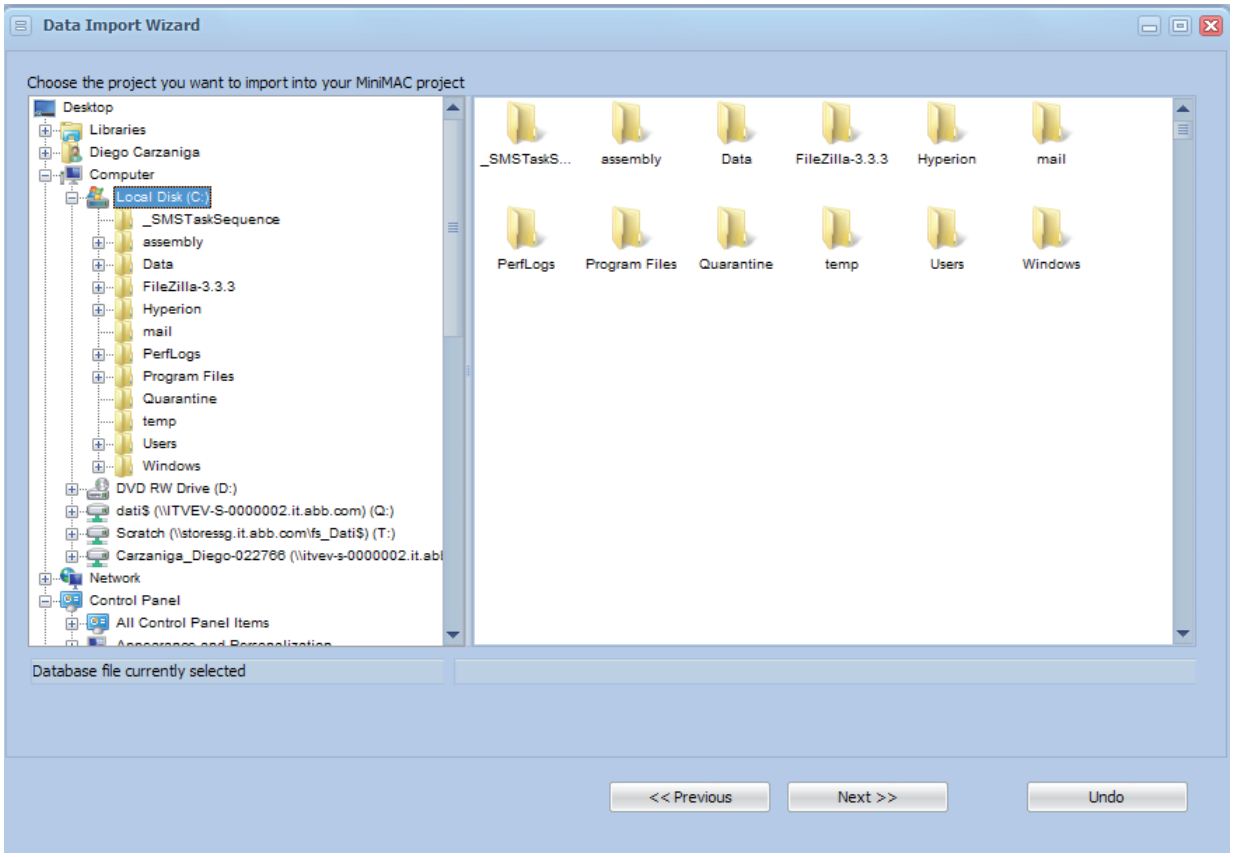
1. select the ETS 3 Database where the KNX project to be imported was saved.
2. after selecting the reference Database, the KNX project to be imported is selected from the list.



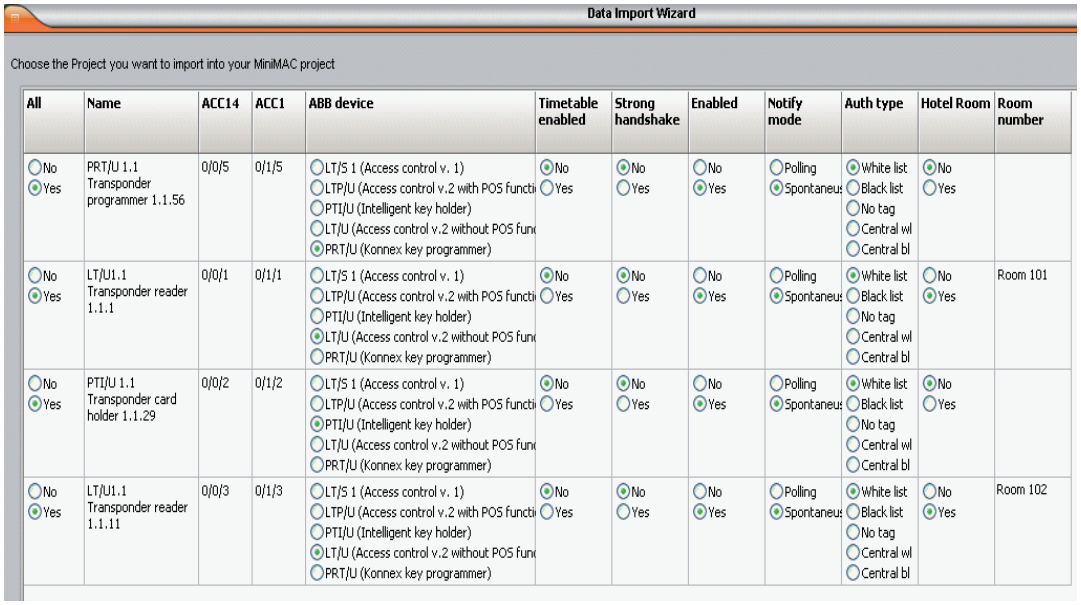


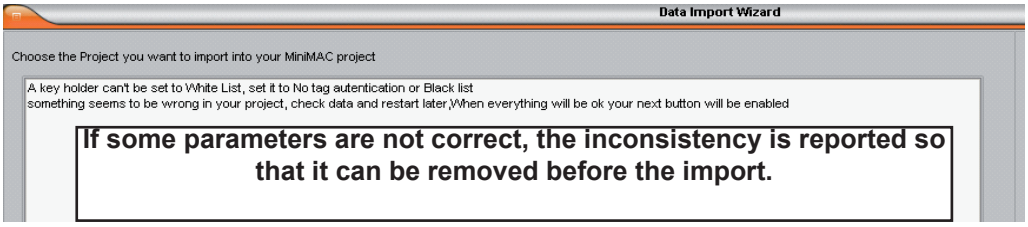
4.12.2 Importing a project from ETS 4/5

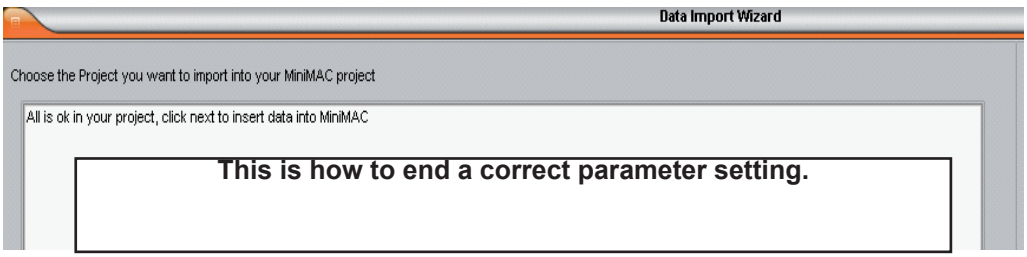
If importing from ETS 4/5, you are asked to directly select the ETS 4 project file (.knxproj format), previously got from ETS via the “Export” process.
Therefore it is not necessary to select the ETS Database, as for the import from ETS 3 and then choose the reference project: in the import from ETS 4/5 you directly select the .knxproj file of the project that you wish to import.



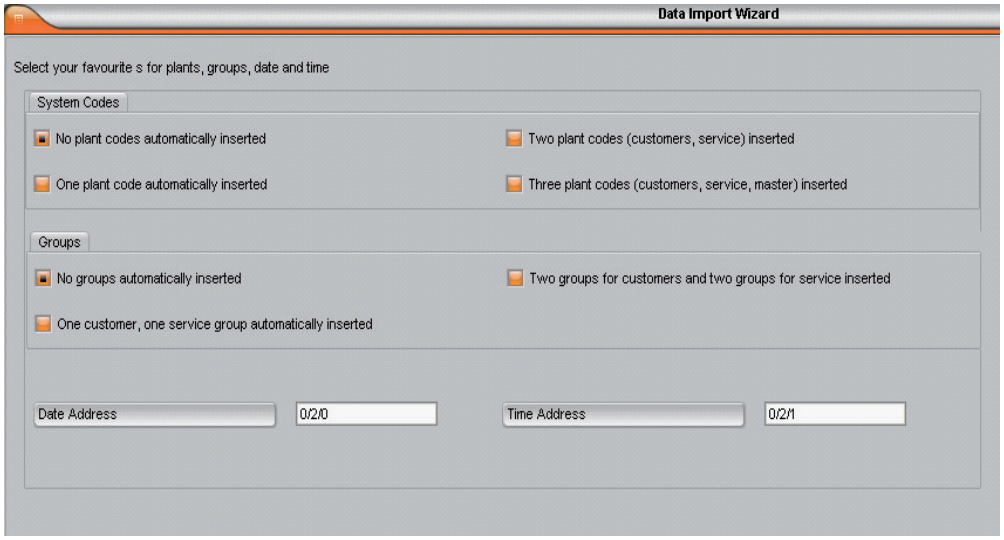
After selecting the project to be imported (or ETS 3 or ETS 4/5 based on the instructions given above in the two cases), the list of all access control devices present in the imported ETS project is displayed (transponder, transponder readers with POS functions, transponder holder, programming device). For each one of these devices, group addresses (ACC14, ACC1) and physical addresses are displayed and it is possible to select them and have an identical or customised programming for all devices.



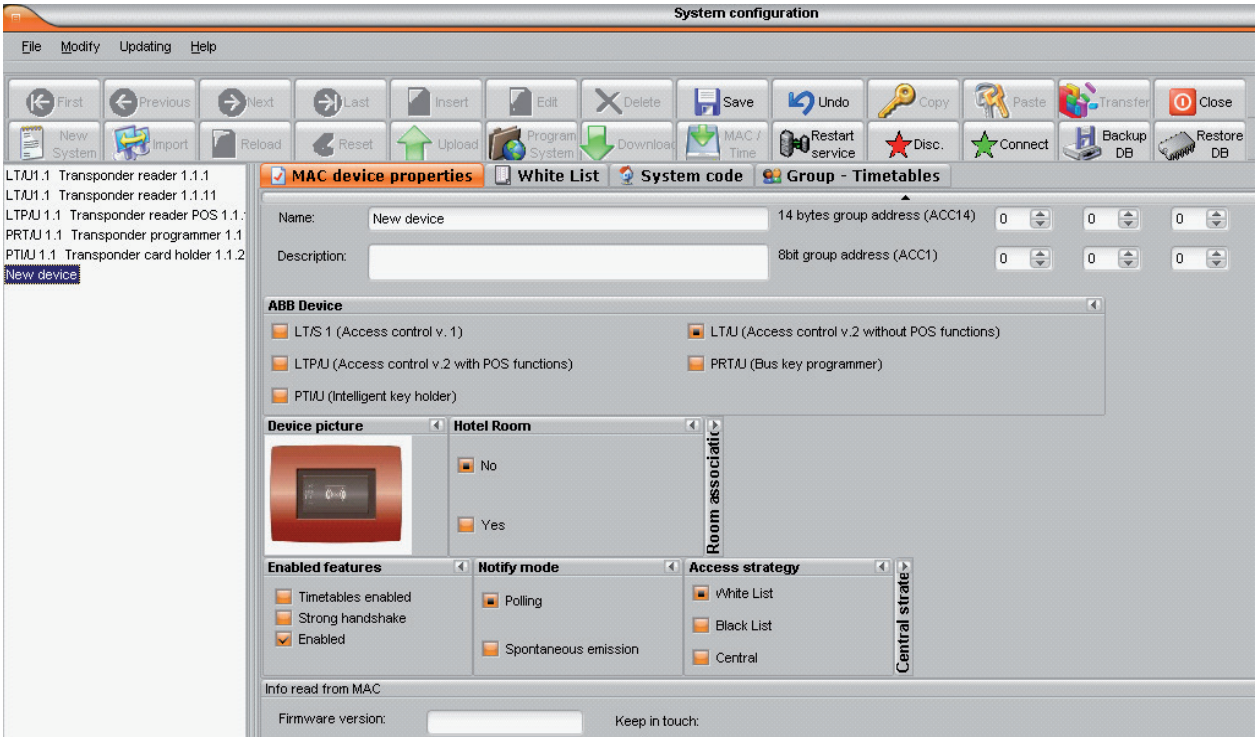




This final screen may be used to automatically create system codes and groups and insert them in the devices being imported. Choose the desired options and click on NEXT.



At the end of the import process, the next screen shows the imported system, with the previously selected options already active.

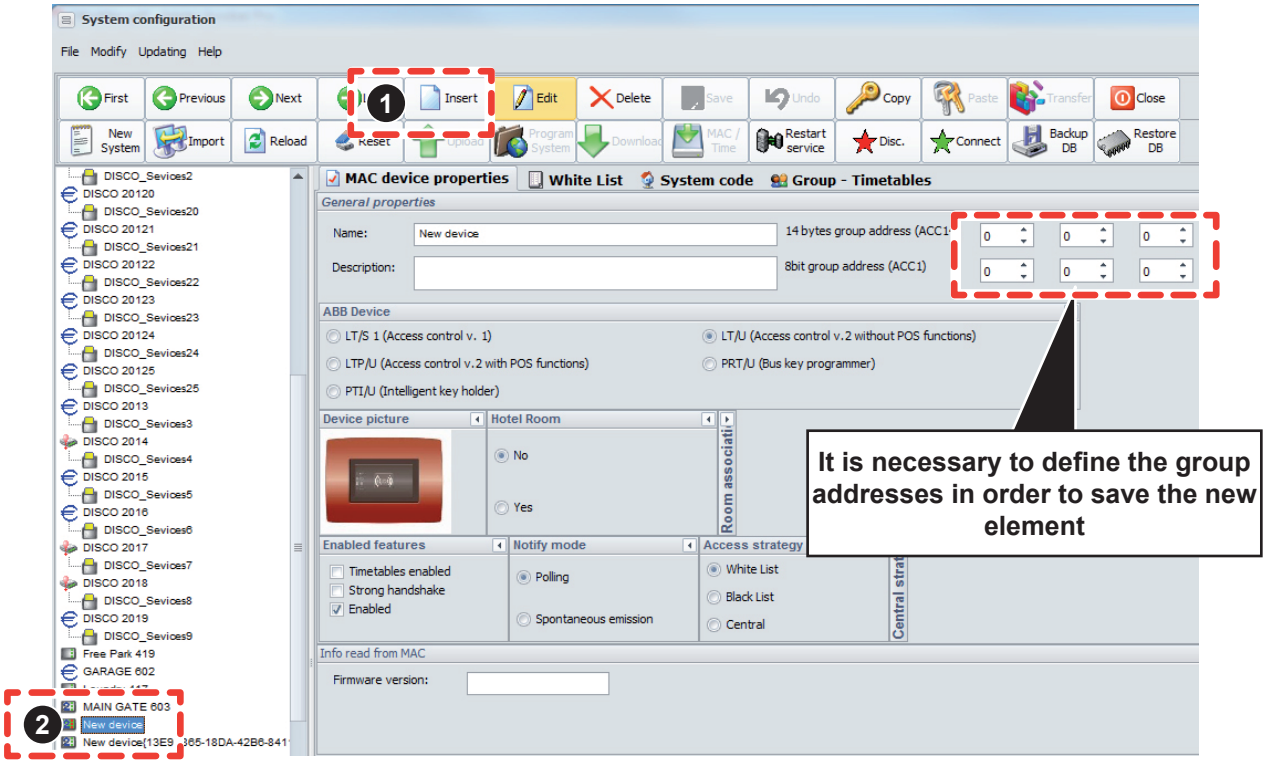


The system set up in this way can subsequently be expanded and/or modified as described in the chapters that follow.

5 Management of the project

5.1 Inserting a device

To insert a new device (**2**) in the project, go to SYSTEM menu and select INSERT (**1**) from the main toolbar:



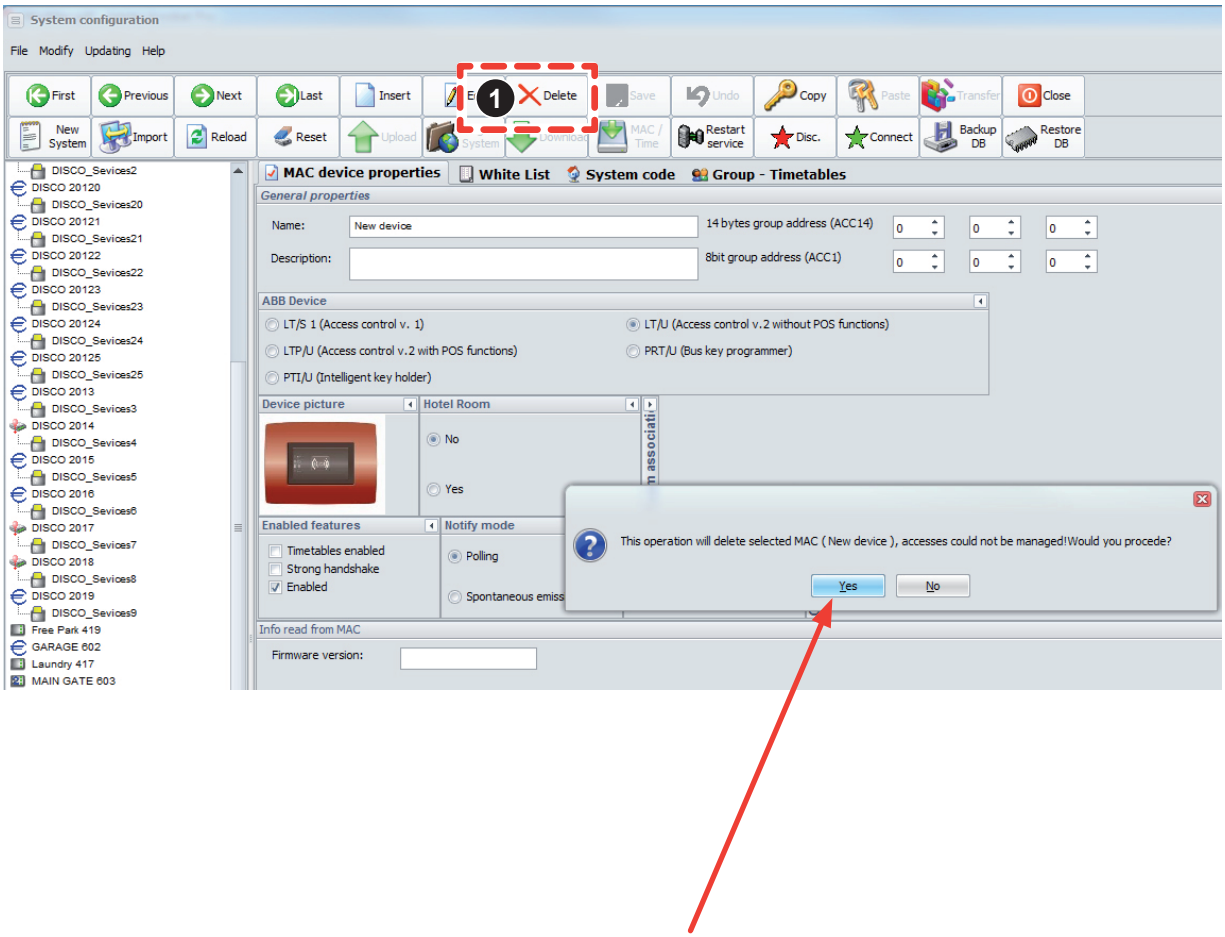
Note

To insert a device, it is necessary to define at least group addresses used by MiniMAC to communicate on the KNX bus with the devices (ACC1 and ACC14 for Chiara-Mylos and Millenium; Physical address and Access Data for Tacteo).
These group addresses must correspond to the values configured on the device via ETS.

The devices saved in the project, but still without group address, are displayed within the structure together with the following icon:

5.2 Deleting a device

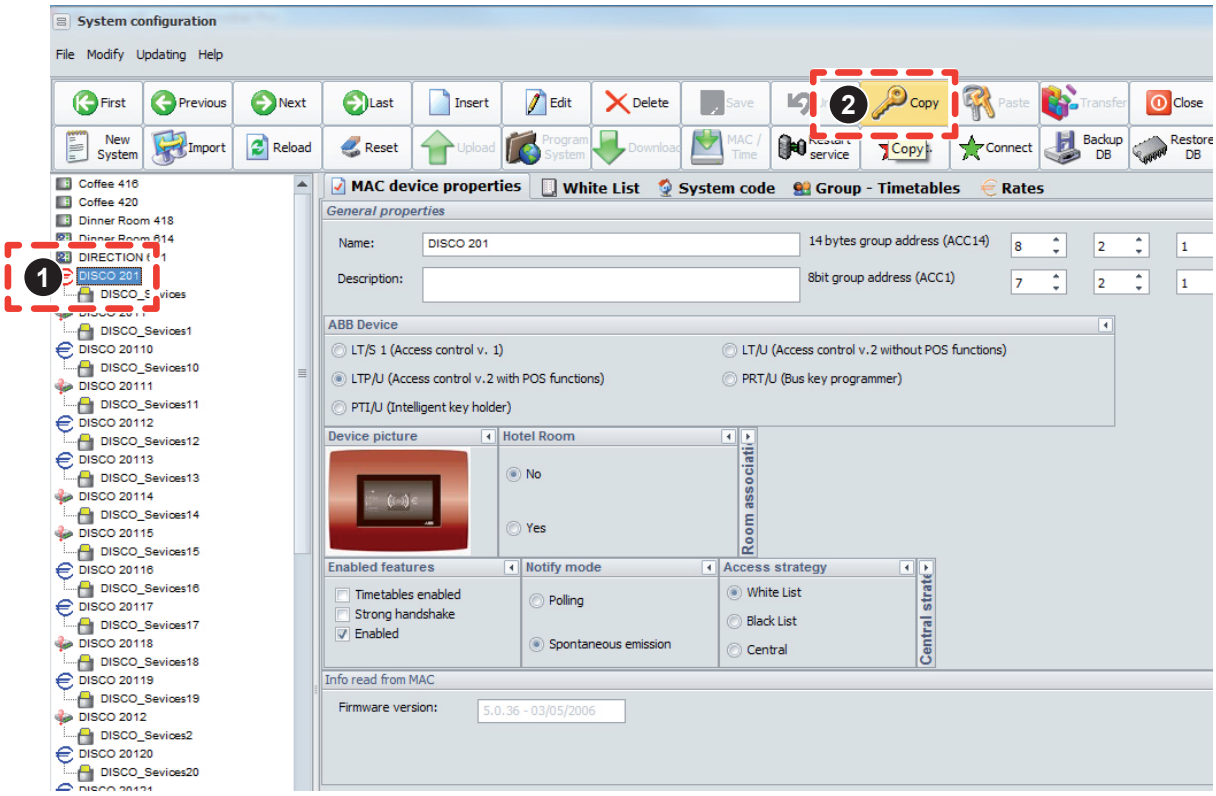
1. Select the device to be deleted;
2. press ‘Delete’ (**1**);
3. confirm the deletion.



5.3 Copy and paste

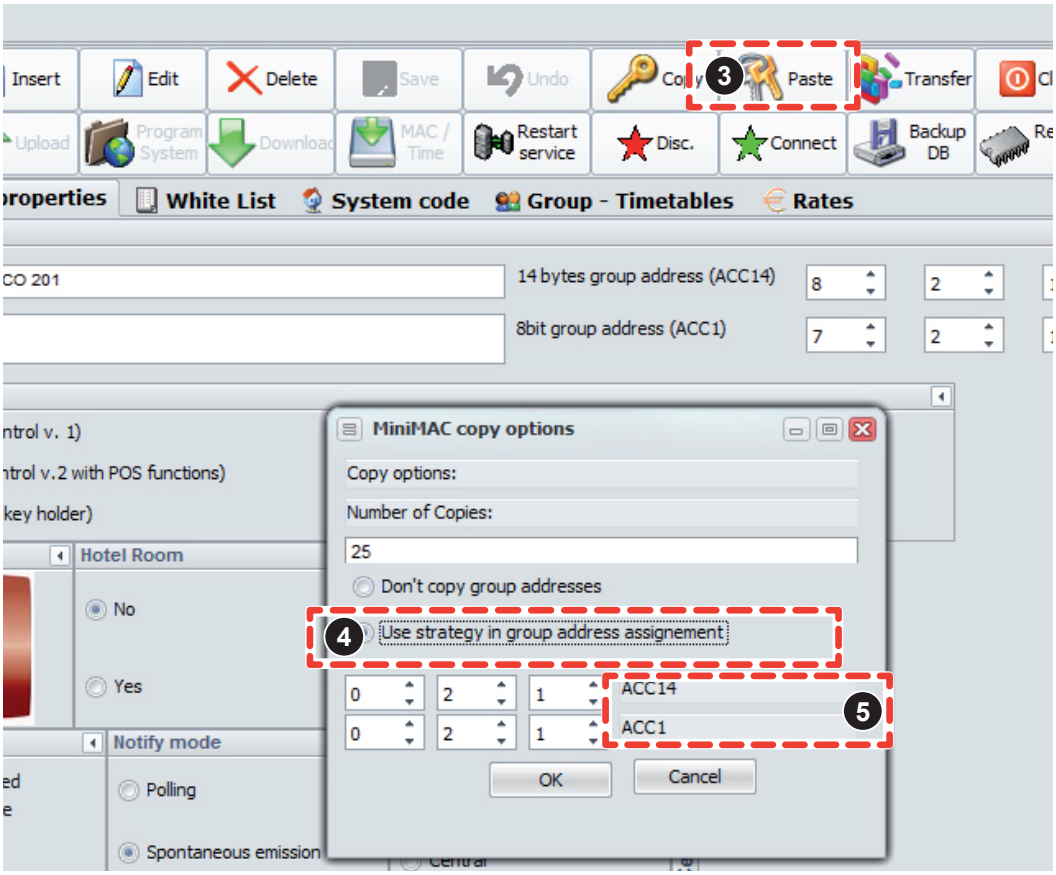
If a configured device is already available, you can make any number of copies using the copy/paste function:

1. Select the sample device (**1**);
2. Select Copy (**2**).

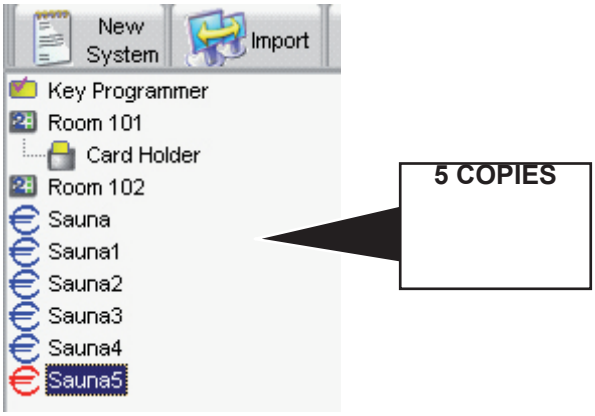


After having copied the sample device, you need to activate the Paste function from the main toolbar. All characteristics will be copied except the group addresses ACC1 and ACC14 and any TAG codes that could be present on the white or black lists.

The Paste function (**3**) provides two options: with or without automatic group address assignment.
If you select the automatic group address assignment option (**4**), you must define the strategy by which the addresses are to be assigned. In the ACC1 and ACC14 (**5**) boxes, you must indicate the increments to be attributed to each address field starting from the original group address.
In the example shown in the figure below, it can be seen that for the ACC1 and ACC14 the first field will not be incremented, while the first and second will be incremented by 2 and 1, respectively.



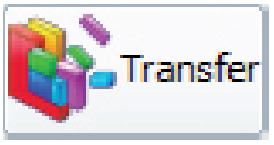
The copied devices will have a default name that is similar to that of the original plus a progressive number appended to this name.



5.4 Transferring parameters

You can change the characteristics of a device present in your project to make them correspond to those of a sample device using the COPY/TRANSFER PARAMETERS function.
Select a sample device:

Select a device to which the sample characteristics are to be transferred:



In this way, all the sample characteristics will be transferred to the target device.

Obviously, the operation can be repeated on all desired devices, but remember that you must copy the parameters from the sample before transferring them. In fact, the TRANSFER PARAMETERS icon is disabled if the COPY key has not been pressed first.

The "copy format" function includes the following parameters:
- Type of device
- Notification method
- Validation method
- Time bands enabled or disabled
- Mac enabled or disabled
- MAC Room or not

If Mac room, copy also:
- Type of room.
- Number of beds.
- Floor.

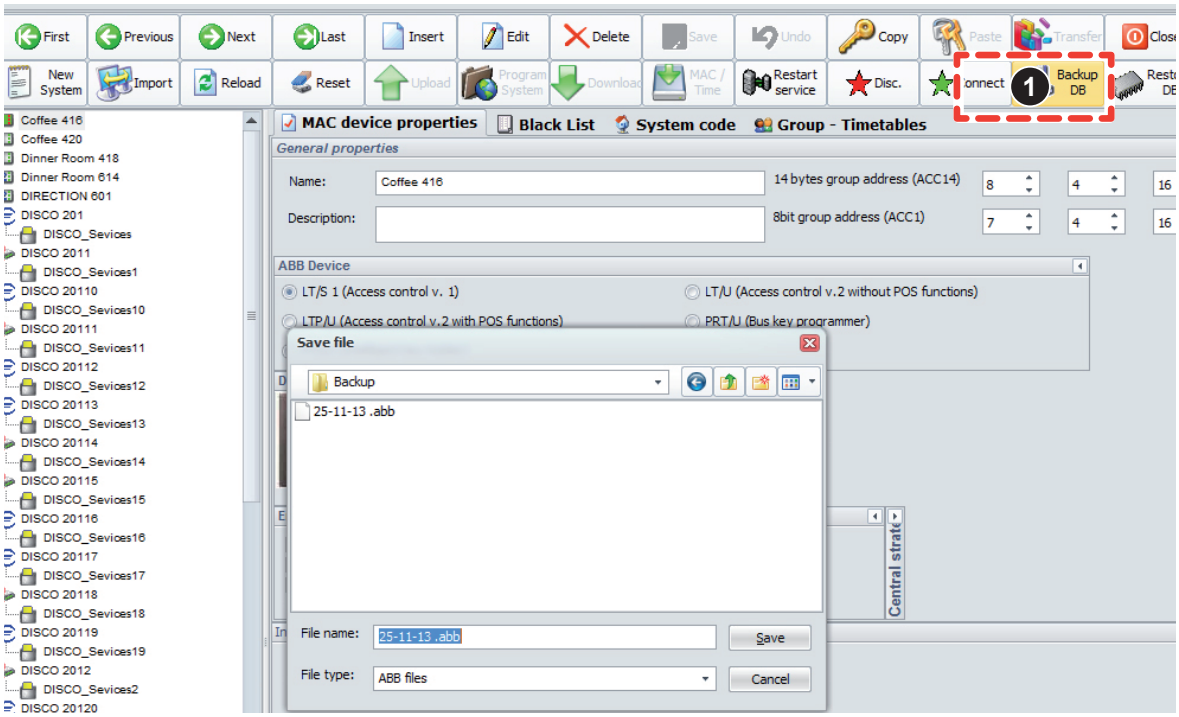
- System codes
- Groups-Timeslots
- Profile-Tariff association

5.5 Backing up and restoring a project

MiniMAC enables you to back up and restore projects. In this way, an installation engineer can have several projects on the PC, loading each time the required project. This function also enables the end user to backup his data regularly and keep the database in efficient order.
The tool for backing up and restoring the database is provided on the MiniMAC CD Rom. You will only need it if you want to import the MiniMAC database into the MiniMAC environment. Reference should be made to the specific manual for details on how to import MiniMAC projects with MiniMAC.

5.5.1 Backing up or saving the project

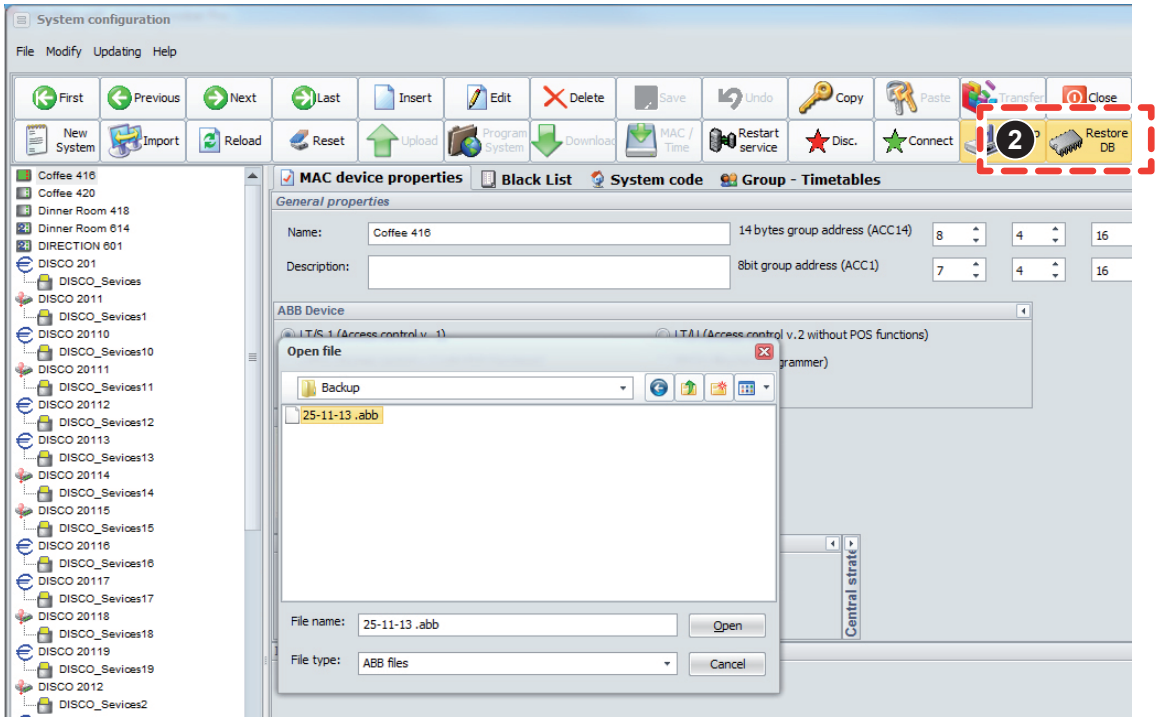
To make a backup of a MiniMAC project, you simply need to click on the "Backup DB" (**1**) icon:



You will be prompted to select the folder and the file name to be assigned to the saved project.
The extension of the file must be ".ABB", as suggested by the dialog box: Do NOT change it, otherwise you will not be able to restore it. It may take several minutes to save the project, according to the size of the system and the amount of information present. Do NOT stop the operation once started, do not start or use programs in the background during the saving operation.

5.5.2 Restoring the project

To recover a MiniMAC project, you simply need to click on the "Restore DB" (**2**) icon:

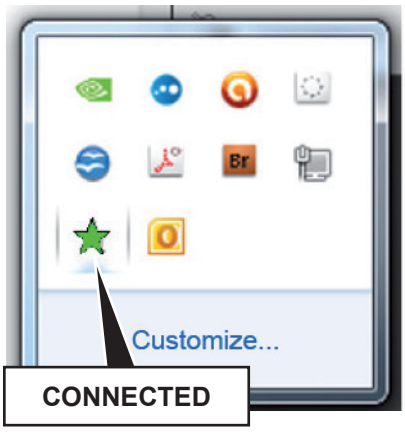


You will be prompted to specify the folder and the name of the .abb file containing the project that you wish to restore/load.

5.6 On-line and off-line mode

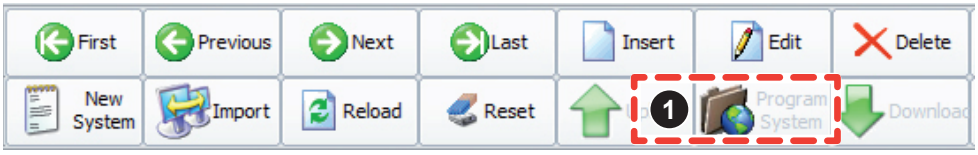
MiniMAC allows you to work in off-line mode using a direct command (System menu/Disc.(off-line)/ Connect (on-line), which can also be used by the installation engineer to avoid having to access the bus repeatedly while programming the system. This will speed up system maintenance operations.
At the login MiniMAC by default tries to start working in connected mode (Online). If no connection to the bus is available, MiniMAC starts in Disconnected mode (Offline). In the “Plant” menu it’s possible to switch from/to Connected/Disconnected mode with specific buttons.

An Icon on the Windows Icon Tray displays the current status of MiniMAC (Connected to or Disconnected from the Bus):



The configuration of the whole system (room definition and insertion of devices, configuration of lists, notification modes, timeslots, rates, areas, groups, etc.) is usually performed with the MiniMAC software working in disconnected mode.
It is then possible to download the programming to the various devices of the access control system, proceeding as follows:

- passage from disconnected to connected mode (MiniMAC is then connected to the KNX-bus)
- click on "System programming" (**1**) to start transferring the programming to all devices of the access control system:



Once you have executed the system programming command, you must wait for it to end before carrying out any other activities with MiniMAC. System programming may take several minutes, depending on the size of the system.

6 MiniMAC interfacing with hotel management software (PMS)

MiniMAC allows integration with hotel management software applications, usually called PMS (Property Management System).
If a hotel is equipped with PMS software and MiniMAC monitoring and configuration software for access control, the two applications can communicate with each other, each performing its own specific function.
MiniMAC by default offer two plug-in available for granting interfacing with two important PMS software:

- Micros Fidelio
- Protel

Other PMS software can be interfaced developing the related plug-in. System integrators/software house interested in developing a dedicated plug-in for a a specific PMS software, can contact ABB sales team for more information.

- PMS software allows the proprietor and reception staff to manage all the information concerning booking, customer records, billing, management of room and services fees, etc.
- MiniMAC software for the configuration of the access control system (TAG programming, definition of access to rooms and readers, load management, climate control from the reception, display of alarms from the reception, ...)

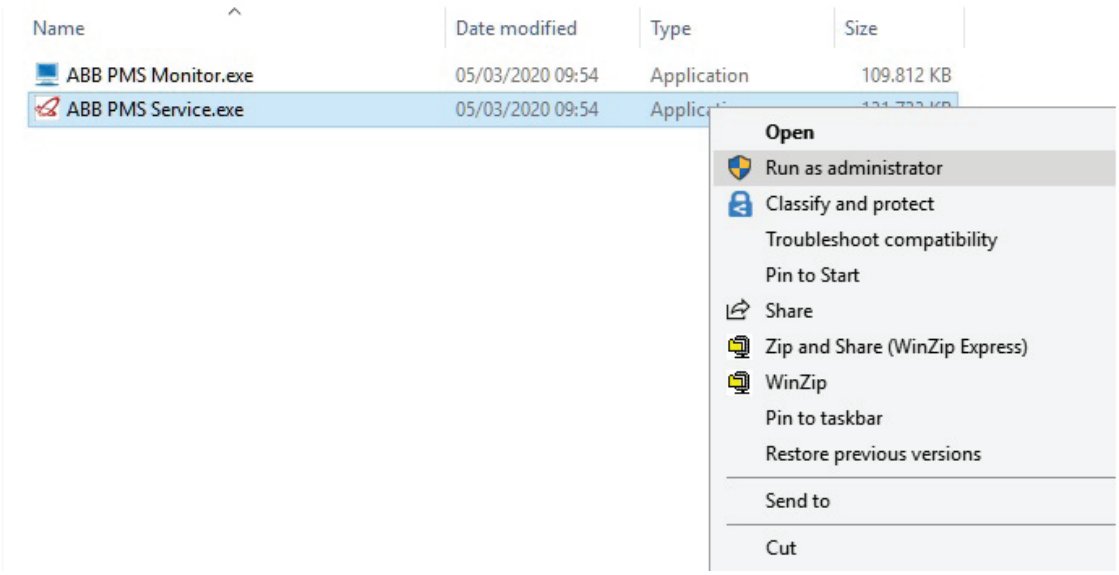
The interfacing between the two systems allows you to enter the customer in the database from PMS software, which will recall the necessary check-in/check-out and transponder TAG programming operations on MiniMAC software.

6.1 Installation of PMS-MiniMAC interface

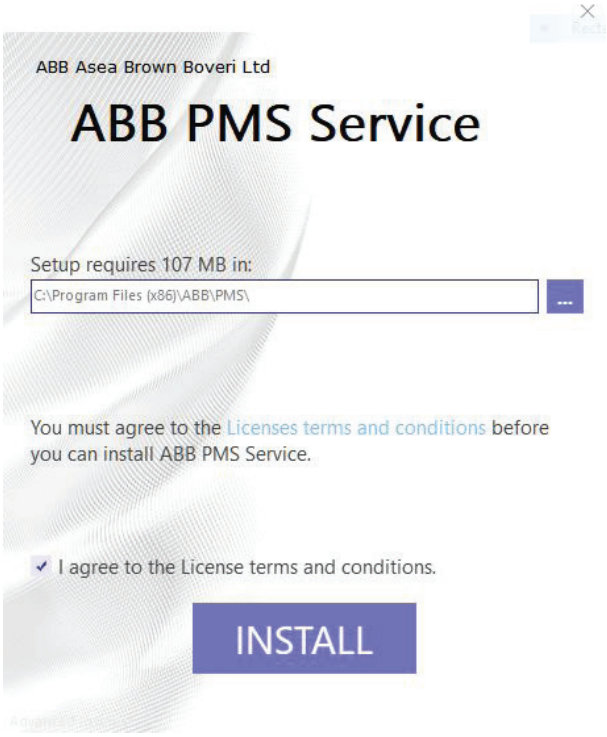
To interface PMS and MiniMAC, it is necessary to install the following ABB PMS software.

6.1.1 ABB PMS Service and ABB PMS Wizard

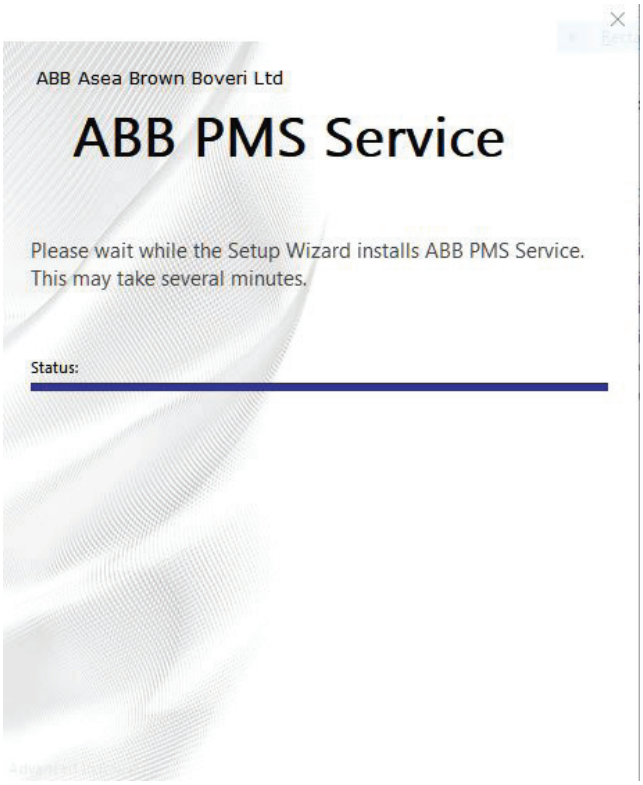
Close all running programs, search in the USB stick for the ‘PMS ABB (Fidelio-Protel)’ folder and launch the ABB PMS Service.exe as administrator.

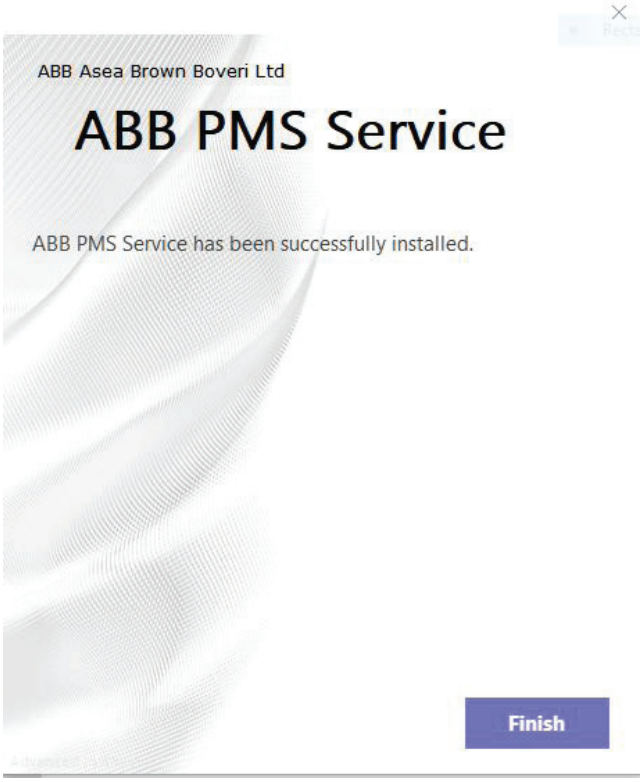


For the installation of PMS Service it is required Microsoft .NET Framework 4.8 software, that it will be installed automatically if not already installed on the PC.
You have to read Licence and terms conditions, and tick the box. Click then on Next button.



If there are some software to be installed as ABB PMS Service prerequisite, please confirm the installation.
The installation will proceed: wait the completion of the installation.





At the end of the installation, 3 software have been installed on the PC:

1) **ABB PMS Service**
   This service is responsible of management of the communication between PMS (Fidelio, Protel) and MiniMAC

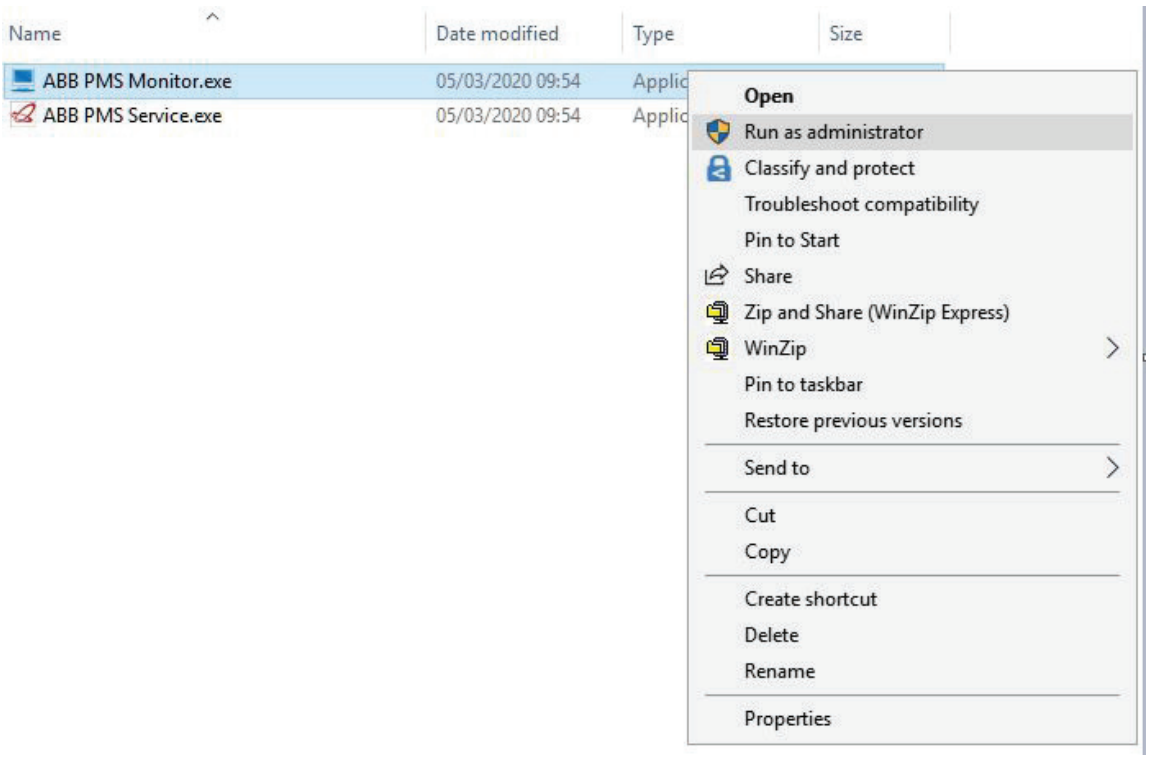
2) **PMS Wizard**
   This application allow configuration of “ABB PMS Service”

3) **Log Viewer**
   This application allows reading of log files related to ABB PMS Service

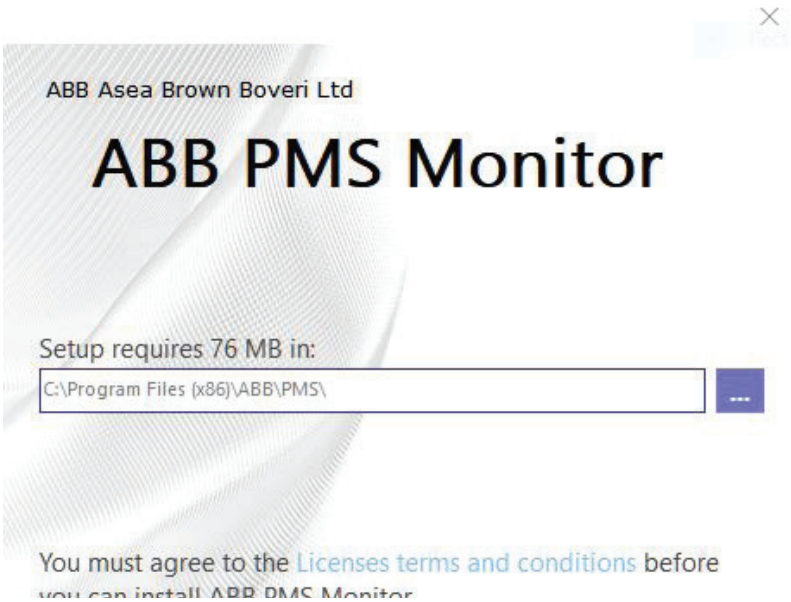
6.1.2 ABB PMS Monitor

PMS monitor allow monitoring of the PMS-MiniMAC interfacing.
It is an optional tool that helps in the diagnostic of the communication between PMS and MiniMAC.

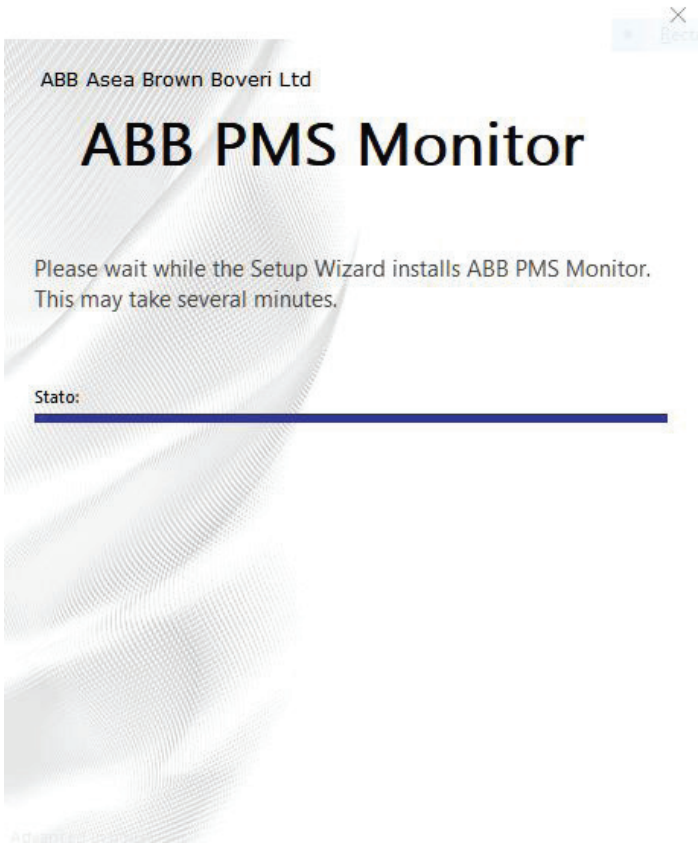
Close all running programs, search in the USB stick for the ‘PMS ABB (Fidelio-Protel)’ folder and launch the ABB PMS Monitor.exe as administrator.

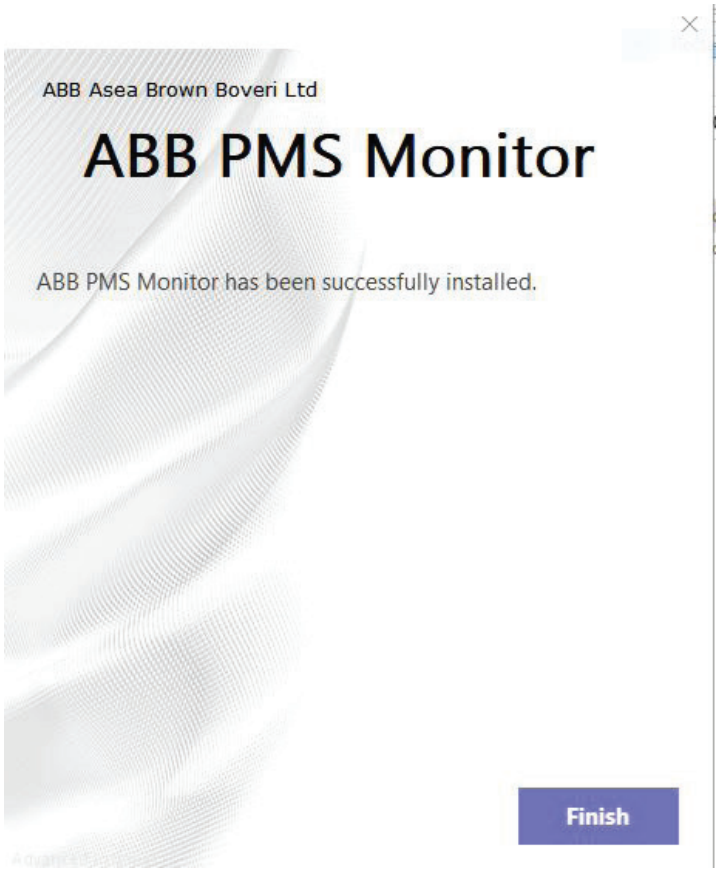


You have to read Licence and terms conditions, and tick the box. Click then on Next button.



If there are some software to be installed as ABB PMS Service prerequisite, please confirm the installation. The installation will proceed: wait the completion of the installation.





6.2 PMS Service configuration

After having installed the ABB PMS Service, it is possible to configure it using the ABB PMS Wizard. You can launch it from the Windows search bar, or directly from the installation folder, or alternative using the icon added by the setup in the Windows taskbar.

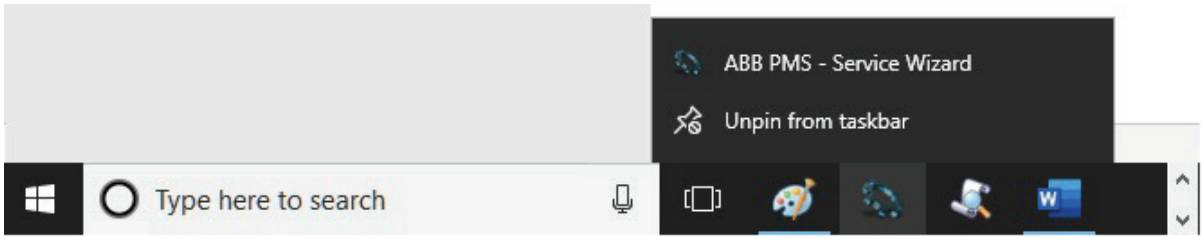


ABB PMS Wizard is the application which allows configuration of ABB PMS Service.
You have to click on MODIFY button on the top and perform the following steps for the configuration.

6.2.1 PMS Protocol

In the TAB “PMS protocol” it is possible to configure the type of PMS software used, and the characteristics of the interfacing with ABB MiniMAC.

1. Plug-in List: you can select which PMS you have to interface with MiniMAC software. There are two PMS that MiniMAC is able to interface, both based on FIAS protocol:
   - Opera/Fidelio (in this case select from the menu “ABBMMC_FIDELIO”)
   - Protel (in this case select from the menu “ABBMMC_PROTEL”)

2. The below parameters are specifically related to the PMS protocol and it is not needed to change them. Please keep the default values, and change it only if suggested by ABB customer support:
   - Waiting for connection
   - Waiting for link-alive
   - Link-alive failure management
   - Enable link-end command

3. Welcome message: this is the welcome message sent by ABB PMS Service to PMS Software (Fidelio/ Protel) in order to declare which commands is able to execute, and synchronize correctly with it. Also this parameter is not necessary to be changed

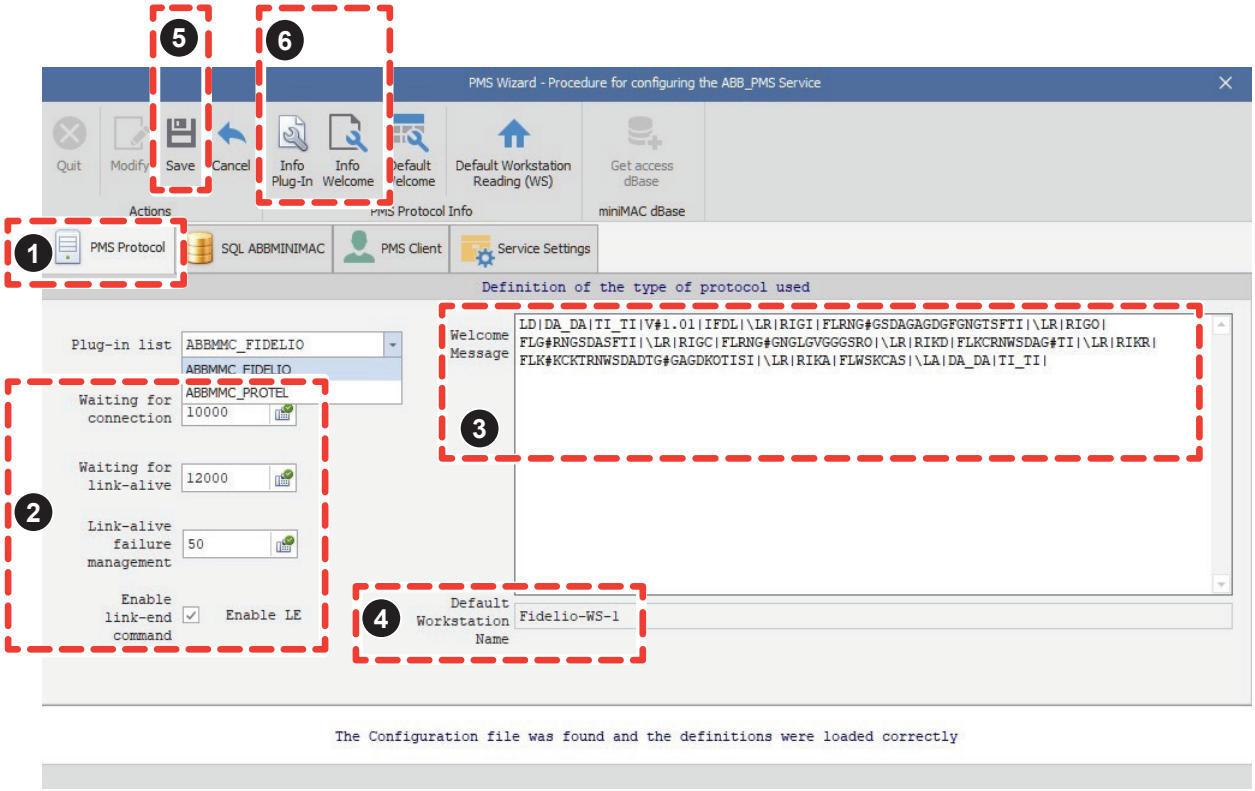
4. Default Workstation Name: it is the default name that ABB PMS Service insert in the message received from PMS software if PMS software does not send it. You can insert the name that you prefer, or configure the value using the Default Workstation Reading button (5), that allows reading the configuration of the association between PMS Workstation and MiniMAC client done in MiniMAC “Settings” menu (see paragraph 6.4 MiniMAC-PMS workstation association). It is possible to choose from this menu one of the PMS workstations correctly associated in MiniMAC “Settings”

Click on SAVE button when you've done the configuration and wait until it is completed the ABB PMS Service restart (automatically done).

Looking at the other buttons in the top part of the window:

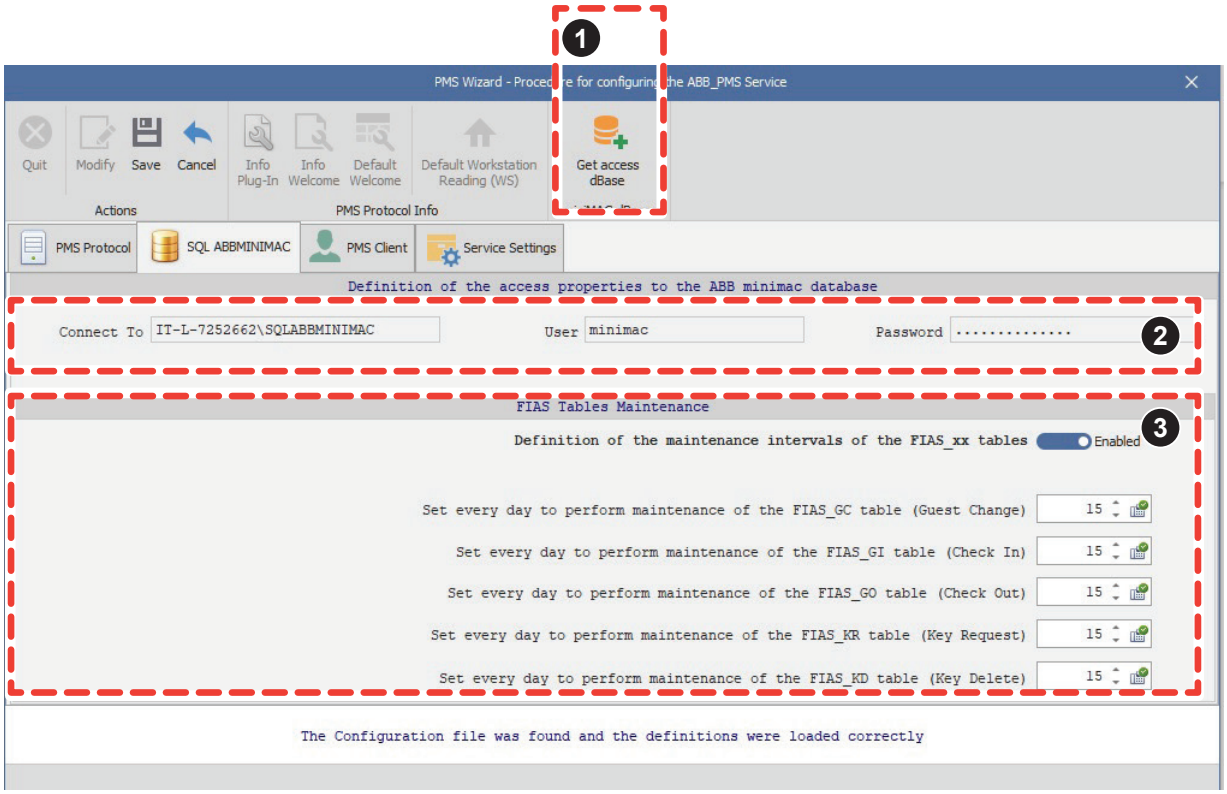
a) Info Pugin: give information about the version of ABB PMS plugin

b) Info Welcome: give information on how it is possible to change Welcome message (typically it has not to be changed, the default is ok), and open the FIAS protocol help



6.2.2 SQL ABBMINIMAC

In the TAB “SQL ABBMINIMAC” it is possible to configure the connection to MiniMAC database and the management of database table of MiniMAC used for interfacing with PMS.



1. Click on the button “GetAccess dBase”, and it will open the window for configuring the connection with MiniMAC database

   A. Server Name: it is the name of MiniMAC database, as you can see in the “MACWizard Server” tool. The default is <hostname>/SQLABBMINIMAC, where <hostname> is the hostname of the PC on which server instance of MiniMAC (and therefore MiniMAC database instance) is installed

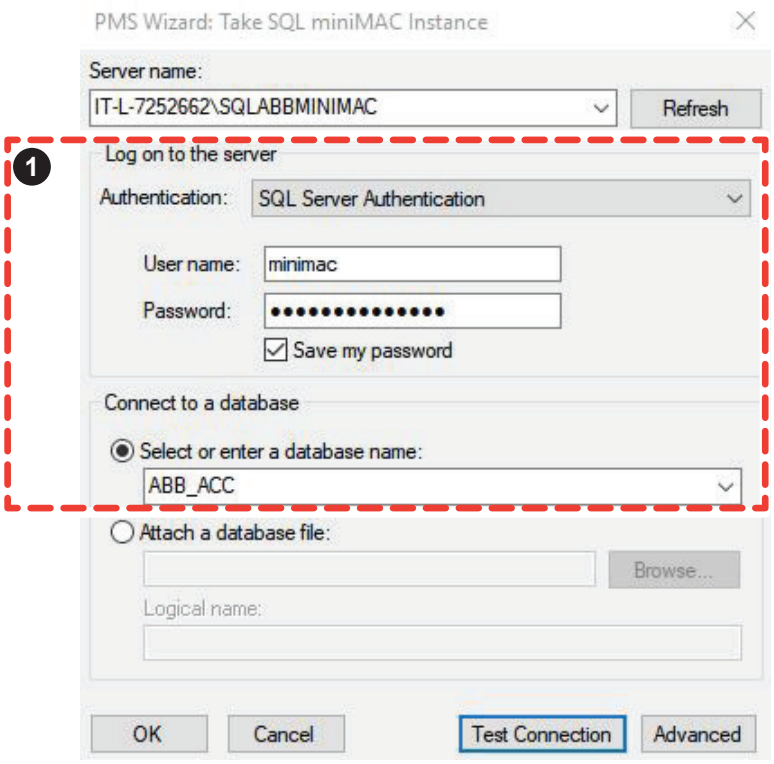
   B. Authentication: SQL Server Authentication

   C. User Name: the default value is minimac. If you have changed username of the MiniMAC database with Microsft SQL Studio, insert here the new username

   D. Password: the default value is ABB029034sace#. If you have changed password of the MiniMAC database with Microsft SQL Studio, insert here the new username (click on “Save my password”)

   E. Select or enter a database name: ABB_ACC

   F. Click on the button “Test Connection” to check the successfully connection with the Database



2. Now in the section “Definition of the access properties to the ABB MiniMAC database”, you will find parameters (login, password, database name) configured at step 1)

3. The values under “FIAS table maintenance” are the parameters related to deletion of FIAS table used by MiniMAC for managing the interfacing with PMS. Please keep the default values, and change it only if suggested by ABB customer support.

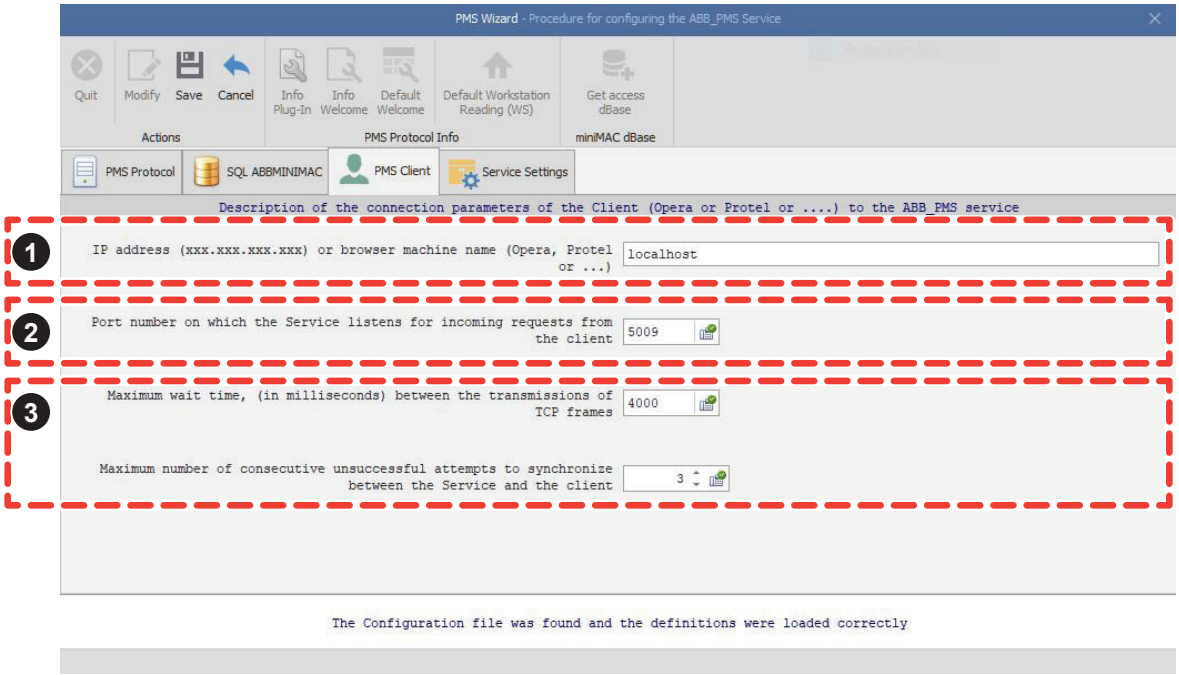
6.2.3 PMS Client

In the tab “PMS Client” it is possible to configure the parameters related to the PMS client that connects to the ABB PMS Service.

1. IP Address: IP address or hostname of the PMS machine/client that send (FIAS) telegrams o ABB PMS service. This value has to be communicated by PMS Software provider (Fidelio/Oracle or Protel)

2. Port: Port number on which PMS ABB Service listen/wait for FIAS telegrams sent by PMS client. Please don’t change the default value, unless PMS Software provider (Fidelio/Oracle or Protel) communicate to use another port number

3. “Maximum wait time …” and “Maximum number of consecutive unsuccessful attempts …” are parameters specifically related to the PMS protocol and it is not needed to change them. Please keep the default values, and change it only if suggested by ABB customer support.



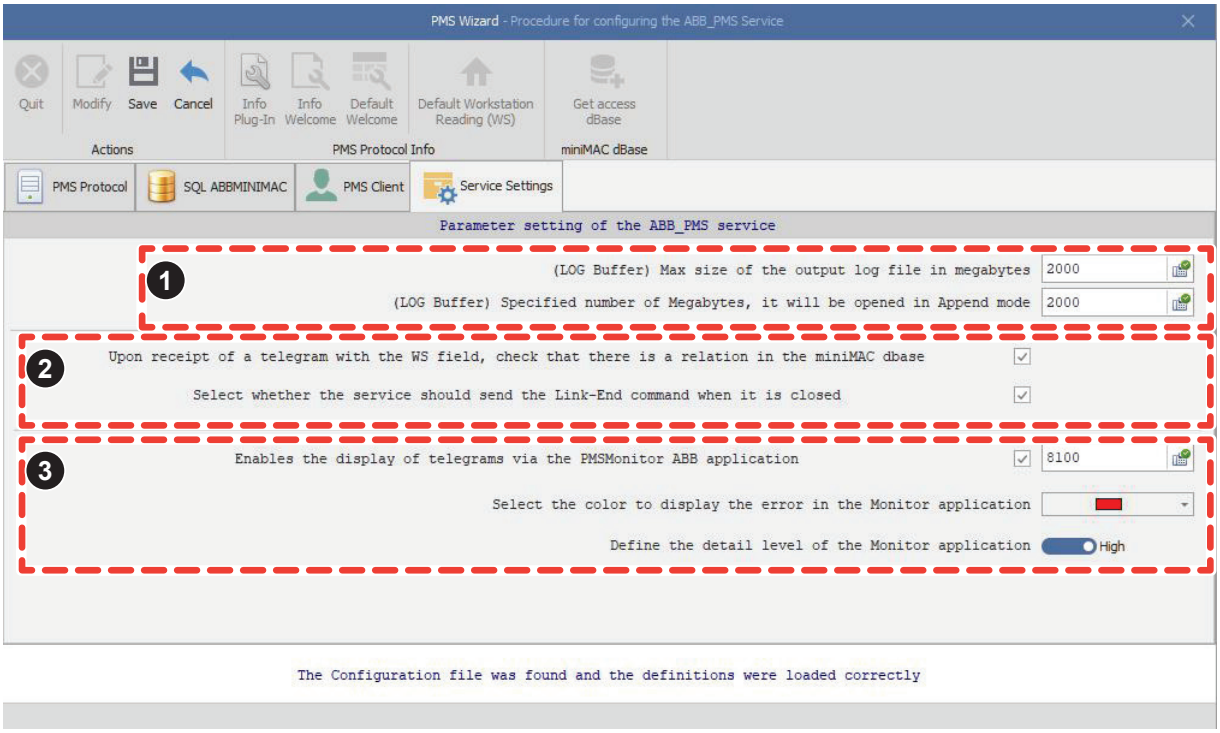
6.2.4 Service Settings

In this tab it is possible to configure diagnostic/maintenance tools available for ABB PMS Service

1. In the first section it is possible to configure the dimension of the log file of ABB PMS Service. Log file can be read with “TracerX Log Viewer” (see paragraph 6.3 TracerX Log Viewer) that is installed together with ABB PMS Service

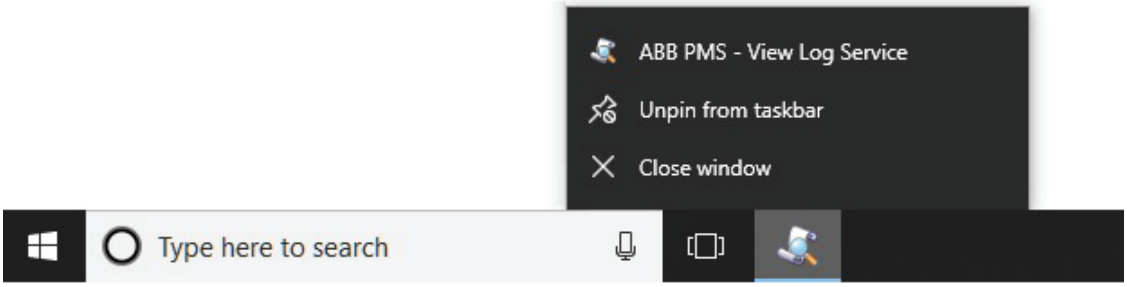
2. In the second section there parameters specifically related to the PMS protocol and it is not needed to change them. Please keep the default values, and change it only if suggested by ABB customer support.

3. In the last section you can decide to enable/disable the ABB diagnostic tool (ABB PMS Monitor, see paragraph “6.6 PMS Monitor”) and on which port ABB PMS Service send telegrams to ABB PMS Monitor. It is moreover possible to choose the level of details of the logging in the PMS Monitor and the color for signaling errors

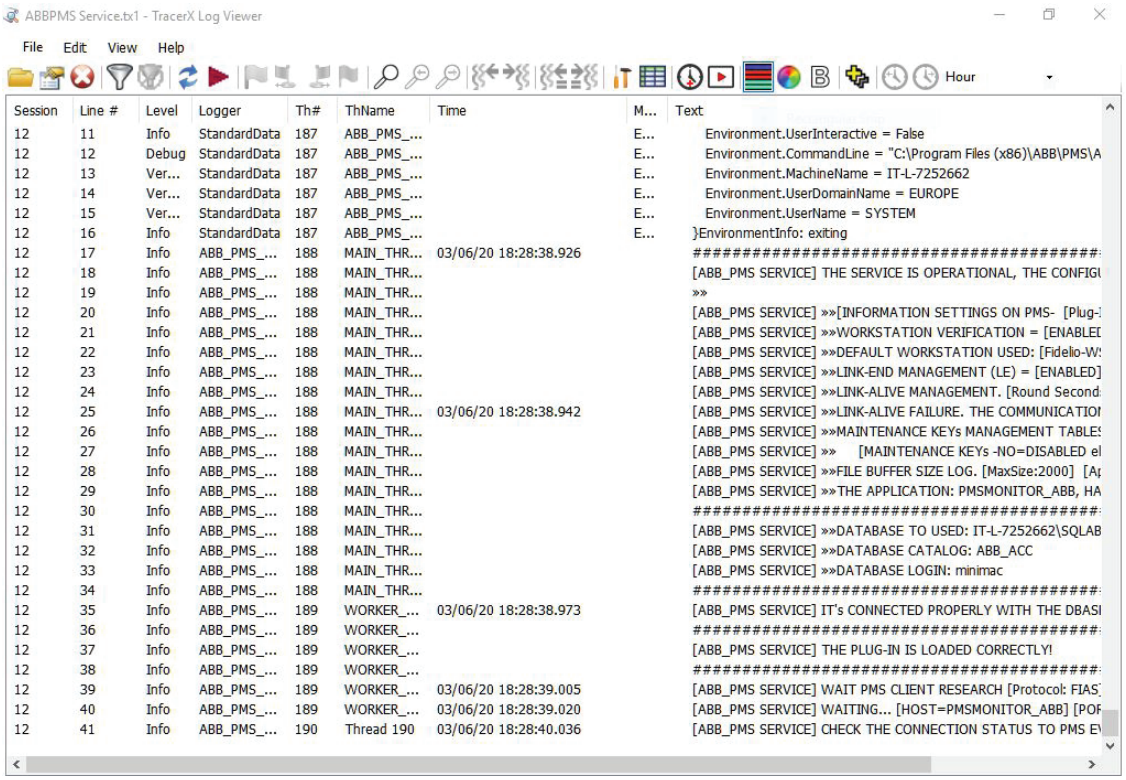


6.3 TracerX Log Viewer

After having installed the ABB PMS Service, and having configured it using the ABB PMS Wizard, it is possible to look at the Log file created by the ABB PMS Service, when necessary.
You can launch it from the Windows search bar, or directly from the installation folder, or alternative using the icon added by the setup in the Windows taskbar.



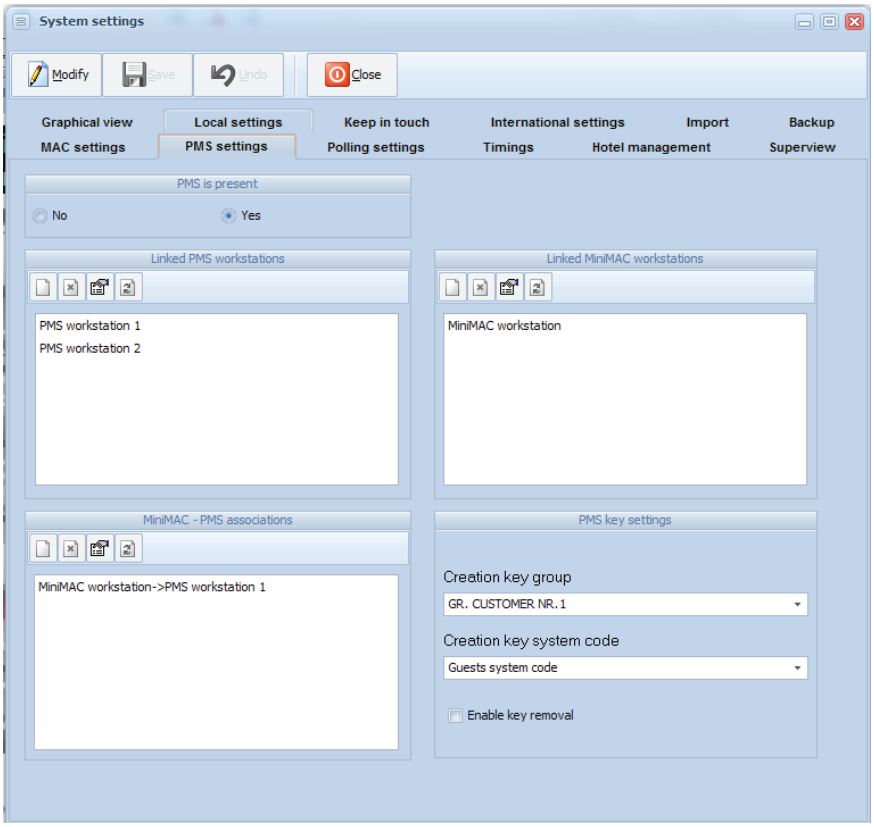
Once launched, you can double click on one specific log file (the most recent one is always at the top) and then see the contents of the ABB PMS Service log file.



Session	Line #	Level	Logger	Th#	ThName	Time	M...	Text
12	11	Info	StandardData	187	ABB_PMS_...		E...	Environment.UserInteractive = False
12	12	Debug	StandardData	187	ABB_PMS_...		E...	Environment.CommandLine = "C:\Program Files (x86)\ABB\PMS\A
12	13	Ver...	StandardData	187	ABB_PMS_...		E...	Environment.MachineName = IT-L-7252662
12	14	Ver...	StandardData	187	ABB_PMS_...		E...	Environment.UserDomainName = EUROPE
12	15	Ver...	StandardData	187	ABB_PMS_...		E...	Environment.UserName = SYSTEM
12	16	Info	StandardData	187	ABB_PMS_...		E...	}EnvironmentInfo: exiting
12	17	Info	ABB_PMS_...	188	MAIN_THR...	03/06/20 18:28:38.926		##########
12	18	Info	ABB_PMS_...	188	MAIN_THR...			[ABB_PMS SERVICE] THE SERVICE IS OPERATIONAL, THE CONFIGU
12	19	Info	ABB_PMS_...	188	MAIN_THR...			»»
12	20	Info	ABB_PMS_...	188	MAIN_THR...			[ABB_PMS SERVICE] »»[INFORMATION SETTINGS ON PMS- [Plug-I
12	21	Info	ABB_PMS_...	188	MAIN_THR...			[ABB_PMS SERVICE] »»WORKSTATION VERIFICATION = [ENABLED
12	22	Info	ABB_PMS_...	188	MAIN_THR...			[ABB_PMS SERVICE] »»DEFAULT WORKSTATION USED: [Fidelio-W
12	23	Info	ABB_PMS_...	188	MAIN_THR...			[ABB_PMS SERVICE] »»LINK-END MANAGEMENT (LE) = [ENABLED]
12	24	Info	ABB_PMS_...	188	MAIN_THR...			[ABB_PMS SERVICE] »»LINK-ALIVE MANAGEMENT. [Round Second
12	25	Info	ABB_PMS_...	188	MAIN_THR...	03/06/20 18:28:38.942		[ABB_PMS SERVICE] »»LINK-ALIVE FAILURE. THE COMMUNICATIO
12	26	Info	ABB_PMS_...	188	MAIN_THR...			[ABB_PMS SERVICE] »»MAINTENANCE KEYs MANAGEMENT TABLES
12	27	Info	ABB_PMS_...	188	MAIN_THR...			[ABB_PMS SERVICE] »» [MAINTENANCE KEYs -NO=DISABLED el
12	28	Info	ABB_PMS_...	188	MAIN_THR...			[ABB_PMS SERVICE] »»FILE BUFFER SIZE LOG. [MaxSize:2000] [A
12	29	Info	ABB_PMS_...	188	MAIN_THR...			[ABB_PMS SERVICE] »»THE APPLICATION: PMSMONITOR_ABB, HA
12	30	Info	ABB_PMS_...	188	MAIN_THR...			##########
12	31	Info	ABB_PMS_...	188	MAIN_THR...			[ABB_PMS SERVICE] »»DATABASE TO USED: IT-L-7252662\SQLAB
12	32	Info	ABB_PMS_...	188	MAIN_THR...			[ABB_PMS SERVICE] »»DATABASE CATALOG: ABB_ACC
12	33	Info	ABB_PMS_...	188	MAIN_THR...			[ABB_PMS SERVICE] »»DATABASE LOGIN: minimac
12	34	Info	ABB_PMS_...	188	MAIN_THR...			##########
12	35	Info	ABB_PMS_...	189	WORKER_...	03/06/20 18:28:38.973		[ABB_PMS SERVICE] IT's CONNECTED PROPERLY WITH THE DBASI
12	36	Info	ABB_PMS_...	189	WORKER_...			##########
12	37	Info	ABB_PMS_...	189	WORKER_...			[ABB_PMS SERVICE] THE PLUG-IN IS LOADED CORRECTLY!
12	38	Info	ABB_PMS_...	189	WORKER_...			##########
12	39	Info	ABB_PMS_...	189	WORKER_...	03/06/20 18:28:39.005		[ABB_PMS SERVICE] WAIT PMS CLIENT RESEARCH [Protocol: FIAS
12	40	Info	ABB_PMS_...	189	WORKER_...	03/06/20 18:28:39.020		[ABB_PMS SERVICE] WAITING... [HOST=PMSMONITOR_ABB] [POR
12	41	Info	ABB_PMS_...	190	Thread 190	03/06/20 18:28:40.036		[ABB_PMS SERVICE] CHECK THE CONNECTION STATUS TO PMS EV

6.4 MiniMAC-PMS workstation association

It is important to complete also the configuration of MiniMAC-PMS workstation association. Go in the menu Options-->Settings, and then click on the tab “PMS settings”.
As first thing you have to select “PMS is present = Yes”



In the Settings menu ("PMS Settings" tab) three windows must be configured:

- **Connected PMS workstations**
  To enter the name of all workstations where there is a PMS client.
- **Connected MiniMAC workstations**
  To enter the name of all workstations where there is a MiniMAC client installation.
- **MiniMAC – PMS association**
  To enter the associations between workstations (PMS and MiniMAC) for which the interfacing should be operating.

Moreover some specific menus are available in the “PMS key settings” located in the bottom part of the page, on the right:

- Creation key group: you can choose the group of MiniMAC customer in which guest are inserted when check-in/card creation is triggered by PMS
- Creation key system code: you can choose the MiniMAC system code assigned to the card when check-in/card creation is triggered by PMS
- Enable key removal: if this option is flagged, on card creation via PMS for a specific room/transponder reader, all the cards already inserted in the white list of this transponder reader are deleted

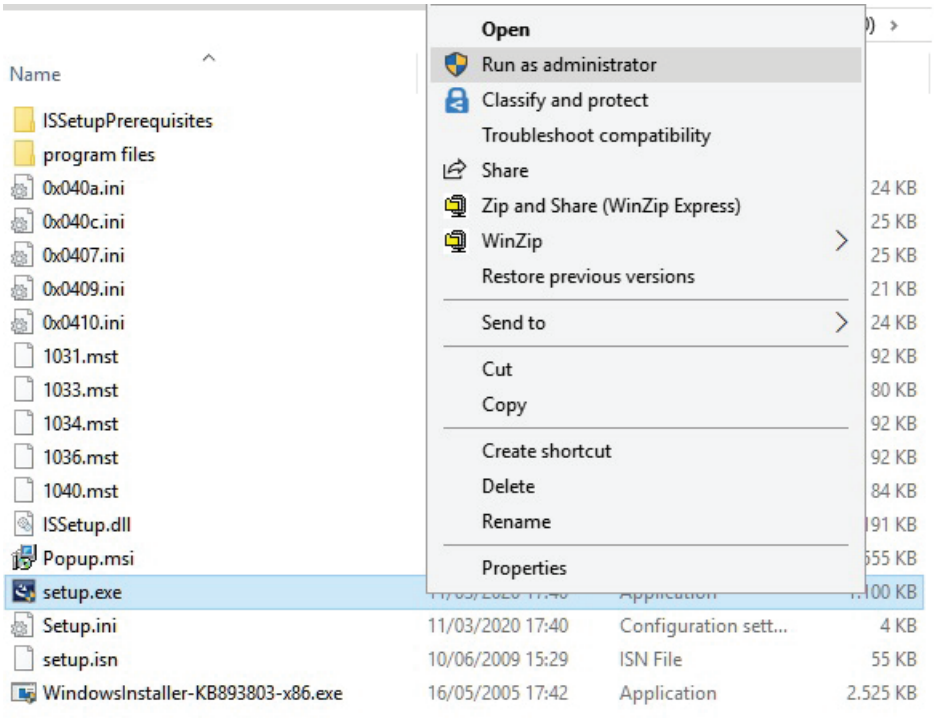
Note
The interfacing between two workstations (PMS and MiniMAC) is not operating (even after the installation is complete, as described in section 6.1) until you enter the names of these two workstations in the window "MiniMAC - PMS associations".

Warning
Configuration of parameters under “PMS setting” tab has to be performed on PC where MiniMAC client is installed. Remember that it could be possible having several MiniMAC client workstations and several PMS client workstations. In the “MiniMAC - PMS associations” you are configuring which MiniMAC client is used by a specific PMS client for check-in/card creation operations.

6.5 ABB Popup

ABB Popup is a software that can be combined with PMS service and allows the creation of TAGs without using MiniMAC software.

Close all running programs, search in the USB stick for the ‘PMS ABB (Fidelio-Protel)’ folder: inside the ‘ABB Popup’ folder launch the setup.exe as administrator.



The set-up checks the presence of MiniMAC software: if the software is not present, installation will not be possible.

In the absence of ABBPopup, MiniMAC and PMS software communicate with each other, but MiniMAC must be used in order to create a customer TAG. The reception staff will then use two software applications: MiniMAC to create TAGs, PMS software for the management of customer records, reservations and more.

With the installation of ABB Popup, reception staff can create TAGs without using MiniMAC software.

Warning
Remember that ABBPopup has to be installed on a PC where a MiniMAC client instance is installed.

Warning
ABB Popup is an application that allows creating keys without using MiniMAC. It obviously requires presence of a PMS software installed (i.e Fidelio, Protel). Without a PMS installed, ABB Popup is useless.

ABB Popup is a Windows application that is positioned in the tray-icon (at the bottom right of the display) and that is able to write the TAG according to the indications of the service, after the confirmation by the operator.
The TAGs to be created must have the following characteristics: they must be "white" or expired (in this last case they will be automatically overwritten).
In all other cases, a writing error is displayed.

The Client is activated with the right button of the mouse and will be as follows:

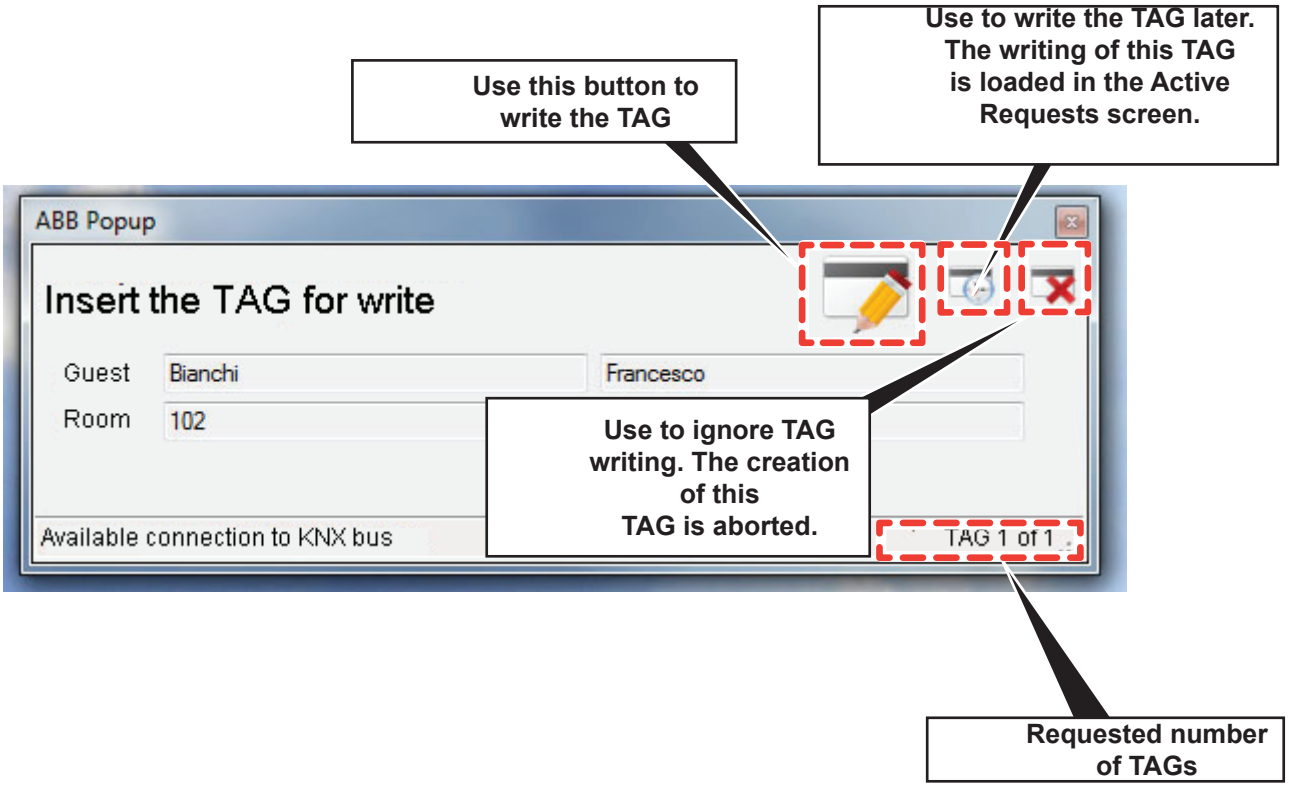
Available connection to KNX bus
- Green icon: it indicates that the connection to the ServicePopup is up and running
- Yellow icon: it indicates a connection problem towards both the service and the KNX bus
- Red icon: it indicates a failure to connect to the service

Active requests
selecting this menu you access a window containing all the requests that are not processed and still hanging, from which the user can select the TAG(s) to be created.

Information
Information about version and use of the ABB software.

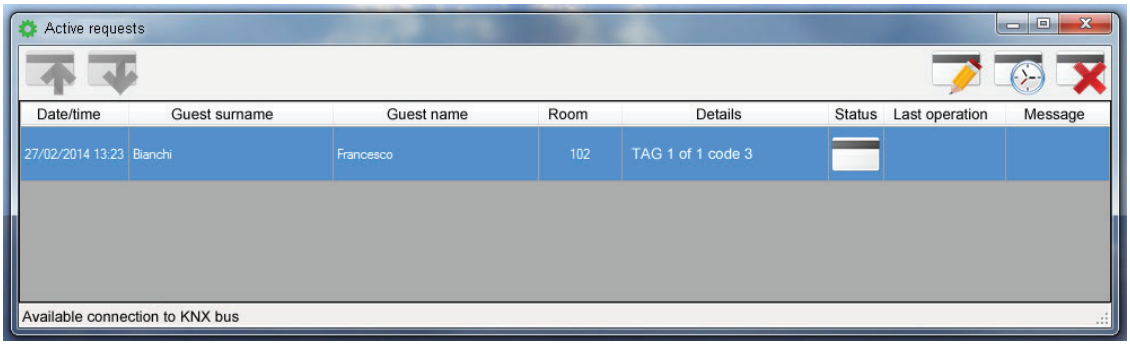
The EXIT button is not present to prevent accidental closure of the program.

The client is usually activated automatically by the service as soon as it detects one or more TAGs to be created.
This screen is only triggered by the service and cannot be recalled at user level. An example of customer TAG creation request is shown below.

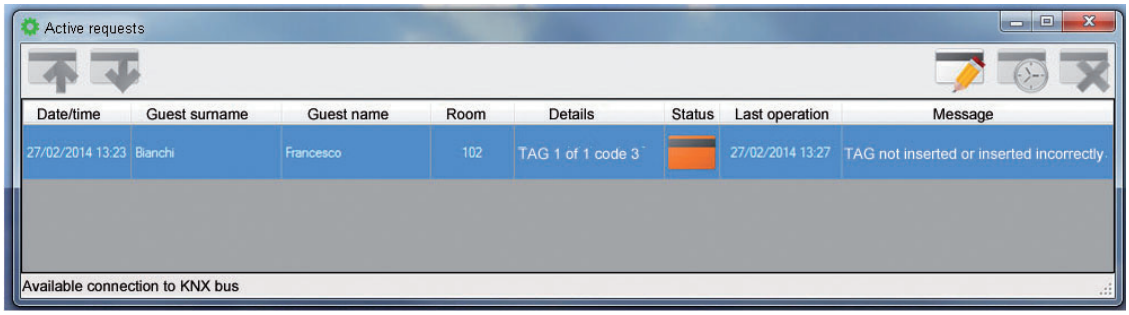


Screen with active requests and reports.

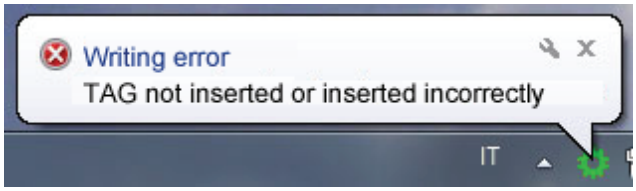
- TAG not yet written



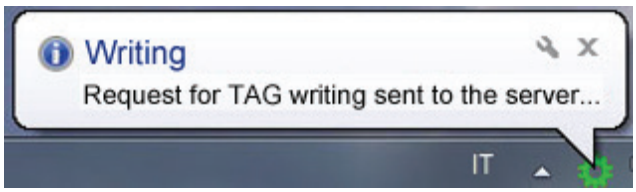
- TAG not written due to problems



- Writing error

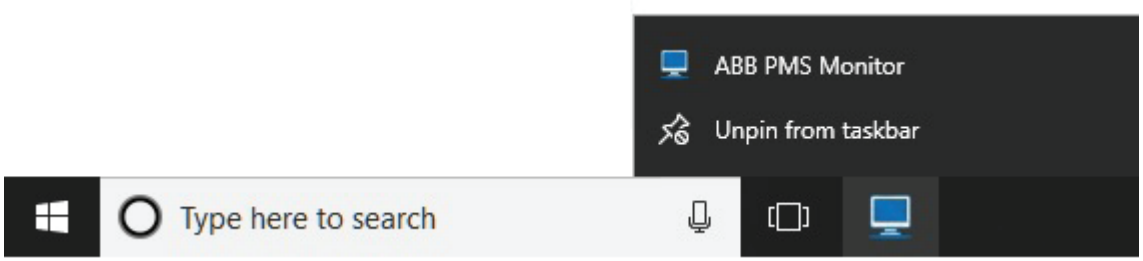


- Writing



6.6 PMS Monitor

ABB PMS monitor allow monitoring of the PMS-MiniMAC interfacing.
It is an optional tool that helps in the diagnostic of the communication between PMS and MiniMAC: it is in particular possible to display the FIAS telegram received by ABB PMS Service.
You can launch ABB PMS Monitor from the Windows search bar, or directly from the installation folder, or alternative using the icon added by the setup in the Windows taskbar.



You can configure the connection of ABB PMS Monitor to ABB PMS Services, clicking on the button “Preferences” and filling the following parameters:

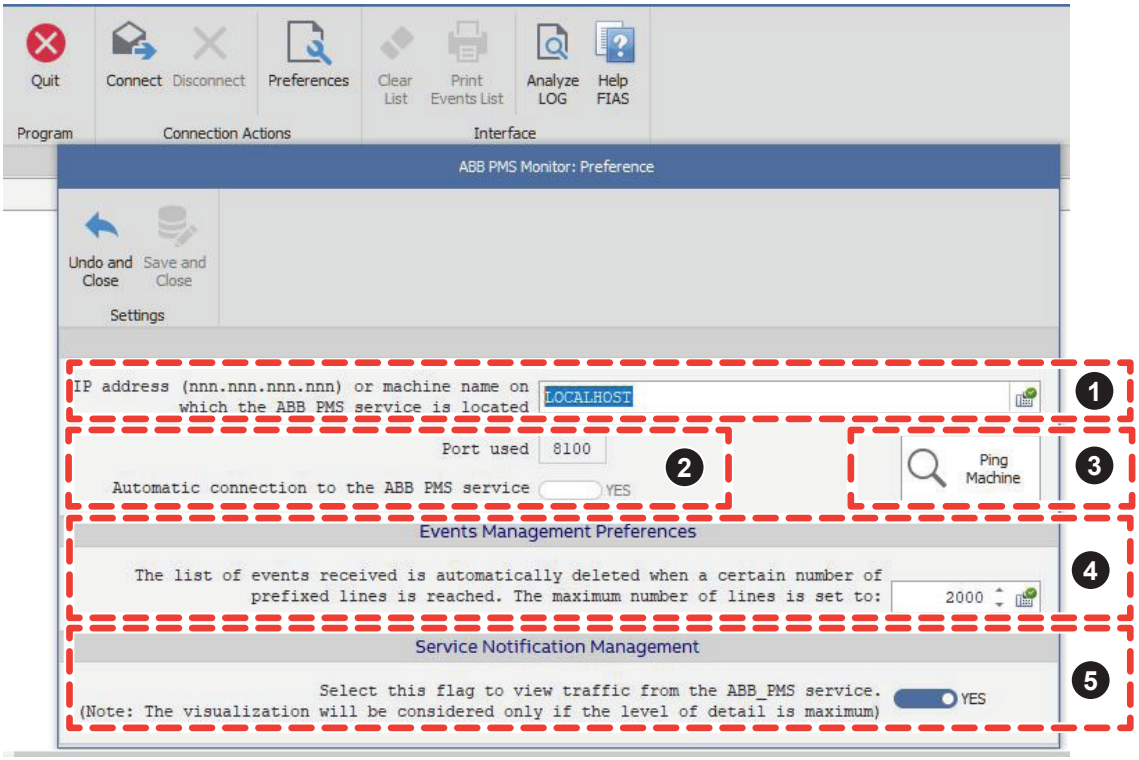
1. IP Address: it is the IP Address of the machine where ABB PMS Service has been installed

2. Port: it is the port number used by ABB PMS Monitor to receive telegrams by ABB PMS Service. The default value is 8100. If you change this value, please remember to use the same port number configured for the ABB PMS Service with ABB PMS Wizard (see paragraph “6.2.4 Service Settings”)

3. Ping Machine: click on this button in order to check if ABB PMS Service machine (IP Address and port number configured at step 1 and 2) is reachable

4. Event Management Preferences: list of events saved by the ABB PMS monitor (default is 2000 events)

5. Service Notification Management: flag YES in order to receive telegram by ABB PMS Service



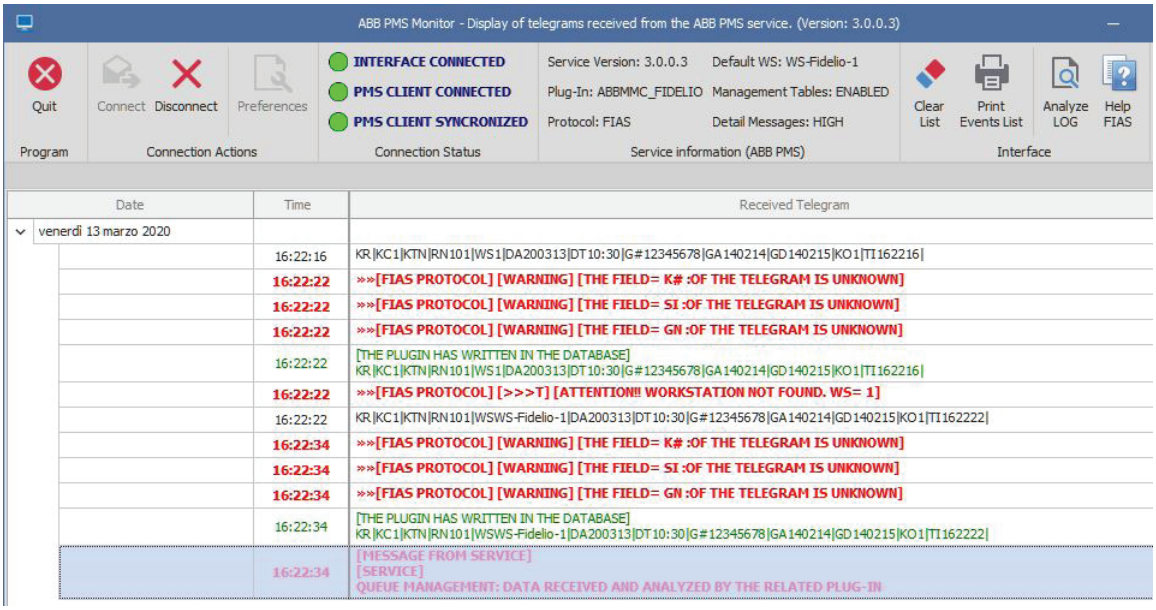
Once configured, it is possible to connect PMS Monitor to ABB PMS Service, clicking on the button "Connect".
The 3 status icons on the top must be all green:

A. INTERFACE CONNECTED: if it is red, ABB PMS Service could be down or not correctly configured with ABB PMS Wizard (see paragraph 6.2 PMS Service configuration)
B. PMS CLIENT CONNECTED: if it is red, no PMS client is connected or correctly configured. Check in this case the configuration of PMS client with ABB PMS Wizard (see paragraph 6.2 PMS Service configuration) and/or parameters/configuration of PMS itself (Fidelio/Protel)
C. PMS Client Synchronized: if it is red, the PMS Client (Fidelio/Protel) has not yet exchanged with ABB PMS Service the synchronization message

The PMS Monitor shows the list of FIAS Telegrams sent by PMS (Fidelio/Protel) to ABB PMS Service. In the example below two telegrams are listed:

- One telegram where Workstation name (the value after field "WS") is 1, not recognized by ABB PMS Service as one of the Workstation listed in the MiniMAC association table between PMS Workstation and MiniMAC workstation
- The other telegram has Workstation field which is "WS-Fidelio-1" and it is recognized as one of the Workstation listed in the MiniMAC association table between PMS Workstation and MiniMAC workstation. Therefore the telegram is received and processed by MiniMAC plugin

Clicking on the button “FIAS Help” it is possible also to have a look at the FIAS protocol help, containing the description of FIAS protocol and usage, and the list of telegrams and commands with their syntax. If you want to disconnect from ABB PMS Service, click on “Disconnect” button.



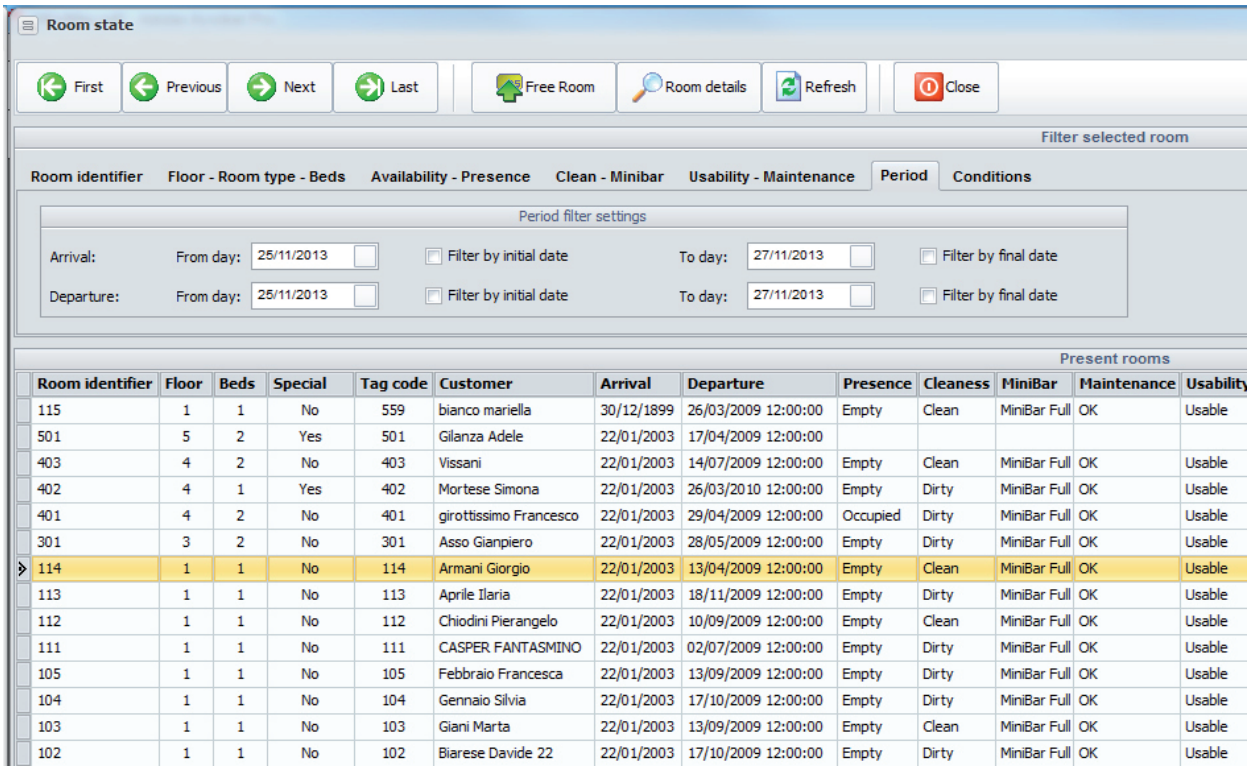
7 Users manual

7.1 Room Management

MiniMAC gives you the possibility to use the functions of the intelligent tag holder (PTI/U) in the best way: this device allows you to manage the hotel, to monitor presence and stay in the room as well as:

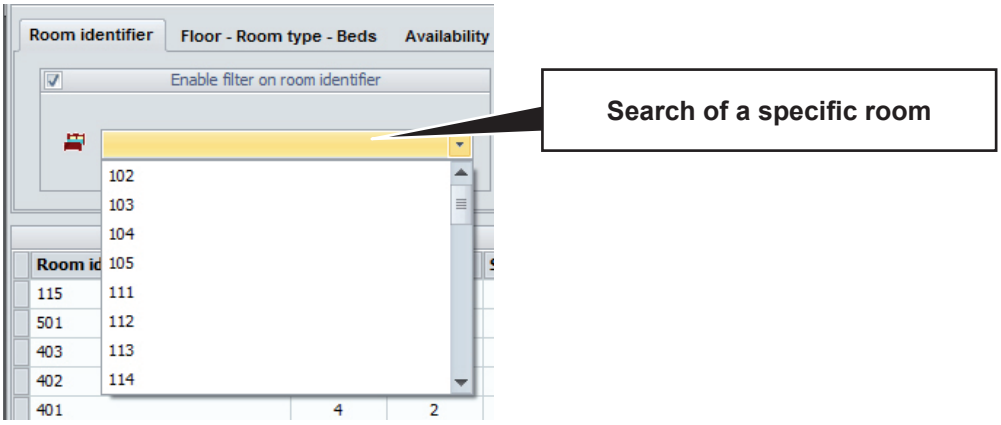
- Room cleaning
- Minibar status check
- Maintenance required
- Room usability

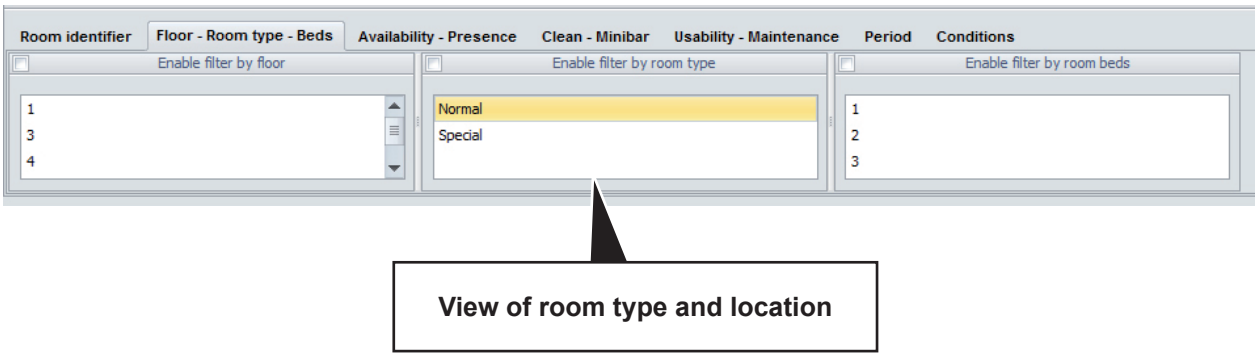
From the menu “Room Management” it is possible to have an exhaustive overview of the hotel:

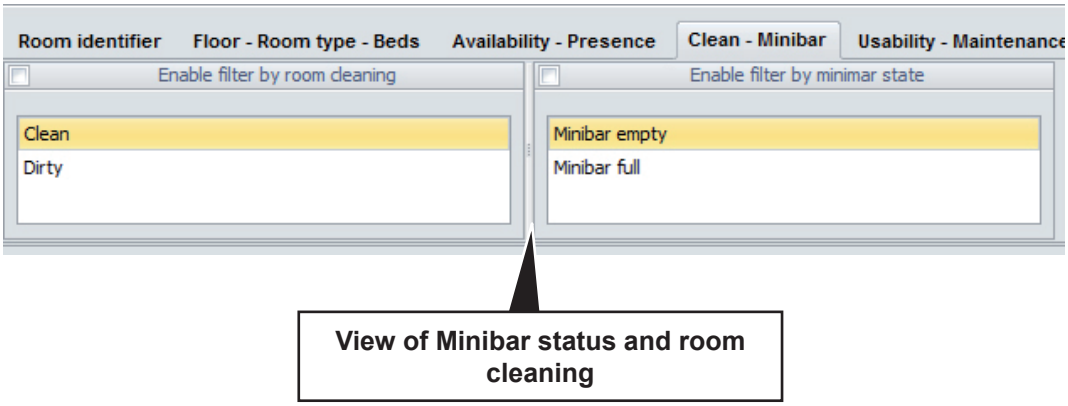


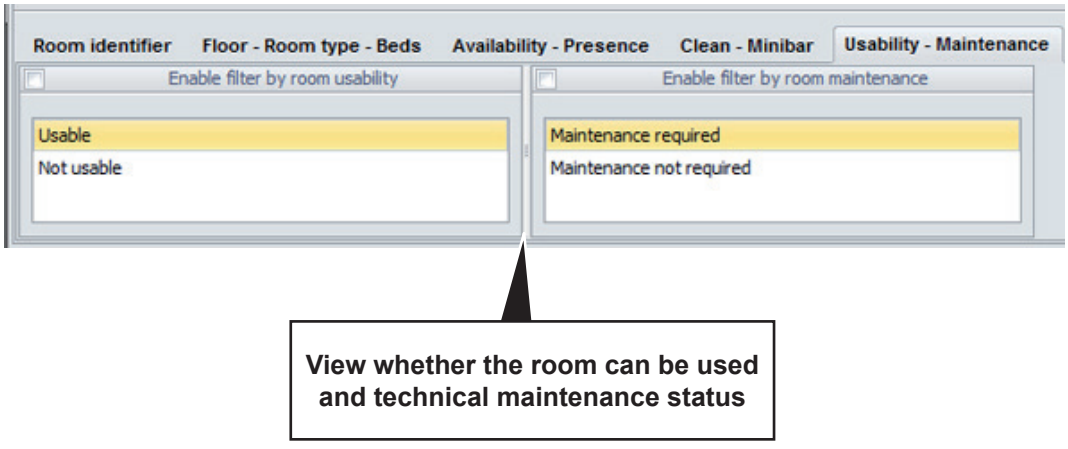
Room identifier	Floor	Beds	Special	Tag code	Customer	Arrival	Departure	Presence	Cleaness	MiniBar	Maintenance	Usability
115	1	1	No	559	bianco mariella	30/12/1899	26/03/2009 12:00:00	Empty	Clean	MiniBar Full	OK	Usable
501	5	2	Yes	501	Gilanza Adele	22/01/2003	17/04/2009 12:00:00					
403	4	2	No	403	Vissani	22/01/2003	14/07/2009 12:00:00	Empty	Clean	MiniBar Full	OK	Usable
402	4	1	Yes	402	Mortese Simona	22/01/2003	26/03/2010 12:00:00	Empty	Dirty	MiniBar Full	OK	Usable
401	4	2	No	401	girottissimo Francesco	22/01/2003	29/04/2009 12:00:00	Occupied	Dirty	MiniBar Full	OK	Usable
301	3	2	No	301	Asso Gianpiero	22/01/2003	28/05/2009 12:00:00	Empty	Dirty	MiniBar Full	OK	Usable
114	1	1	No	114	Armani Giorgio	22/01/2003	13/04/2009 12:00:00	Empty	Clean	MiniBar Full	OK	Usable
113	1	1	No	113	Aprile Ilaria	22/01/2003	18/11/2009 12:00:00	Empty	Dirty	MiniBar Full	OK	Usable
112	1	1	No	112	Chiodini Pierangelo	22/01/2003	10/09/2009 12:00:00	Empty	Clean	MiniBar Full	OK	Usable
111	1	1	No	111	CASPER FANTASMINO	22/01/2003	02/07/2009 12:00:00	Empty	Dirty	MiniBar Full	OK	Usable
105	1	1	No	105	Febbraio Francesca	22/01/2003	13/09/2009 12:00:00	Empty	Dirty	MiniBar Full	OK	Usable
104	1	1	No	104	Gennaio Silvia	22/01/2003	17/10/2009 12:00:00	Empty	Dirty	MiniBar Full	OK	Usable
103	1	1	No	103	Giani Marta	22/01/2003	13/09/2009 12:00:00	Empty	Clean	MiniBar Full	OK	Usable
102	1	1	No	102	Biarese Davide 22	22/01/2003	17/10/2009 12:00:00	Empty	Dirty	MiniBar Full	OK	Usable

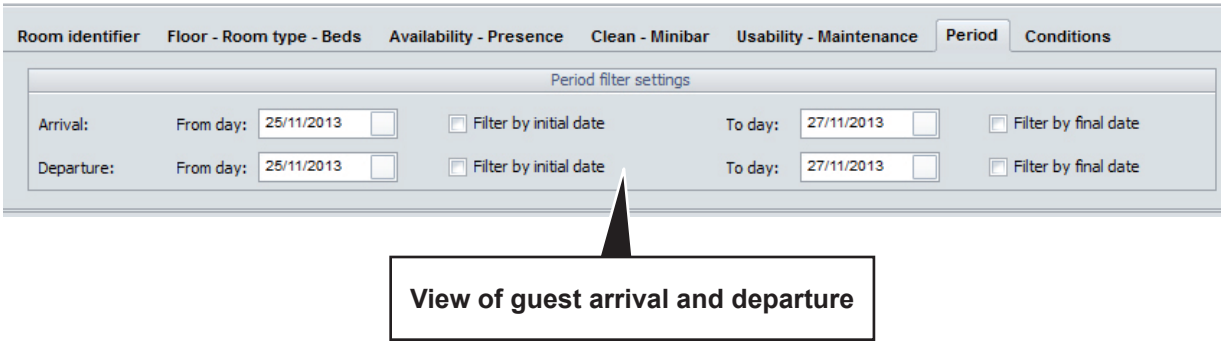
Room situation shows whether a room is available for a new customer to check-in. Furthermore, it shows when a room will be available in order to accept a reservation (check-in with check-in date in the future). For each guest, room situation shows his/her assigned key code.
Furthermore, room type is also shown and it is possible to **search a room that satisfies customer preferences.**
You can click the column header at the top of any column to **sort the list in ascending or descending order.**


Room identifier
Floor - Room type - Beds
Availability
Enable filter on room identifier
102
103
104
105
111
112
113
114
Room id
115
501
403
402
401
4
2
Search of a specific room


Room identifier
Floor - Room type - Beds
Availability - Presence
Clean - Minibar
Usability - Maintenance
Period
Conditions
Enable filter by floor
Enable filter by room type
Enable filter by room beds
1
3
4
Normal
Special
1
2
3
View of room type and location


Room identifier
Floor - Room type - Beds
Availability - Presence
Clean - Minibar
Usability - Maintenance
Enable filter by room cleaning
Enable filter by minimar state
Clean
Dirty
Minibar empty
Minibar full
View of Minibar status and room cleaning

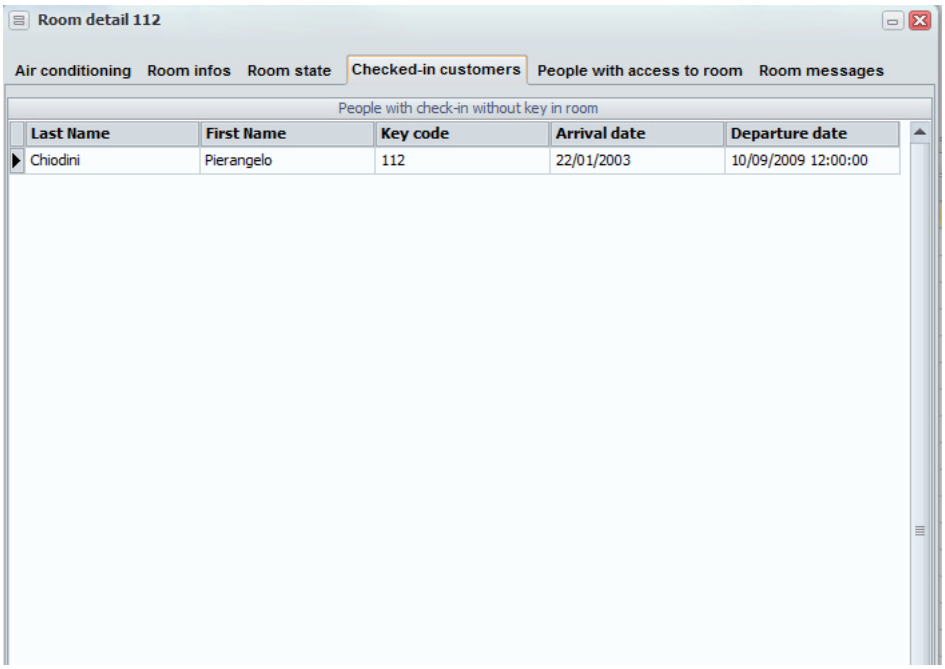

Room identifier
Floor - Room type - Beds
Availability - Presence
Clean - Minibar
Usability - Maintenance
Enable filter by room usability
Enable filter by room maintenance
Usable
Not usable
Maintenance required
Maintenance not required
View whether the room can be used and technical maintenance status



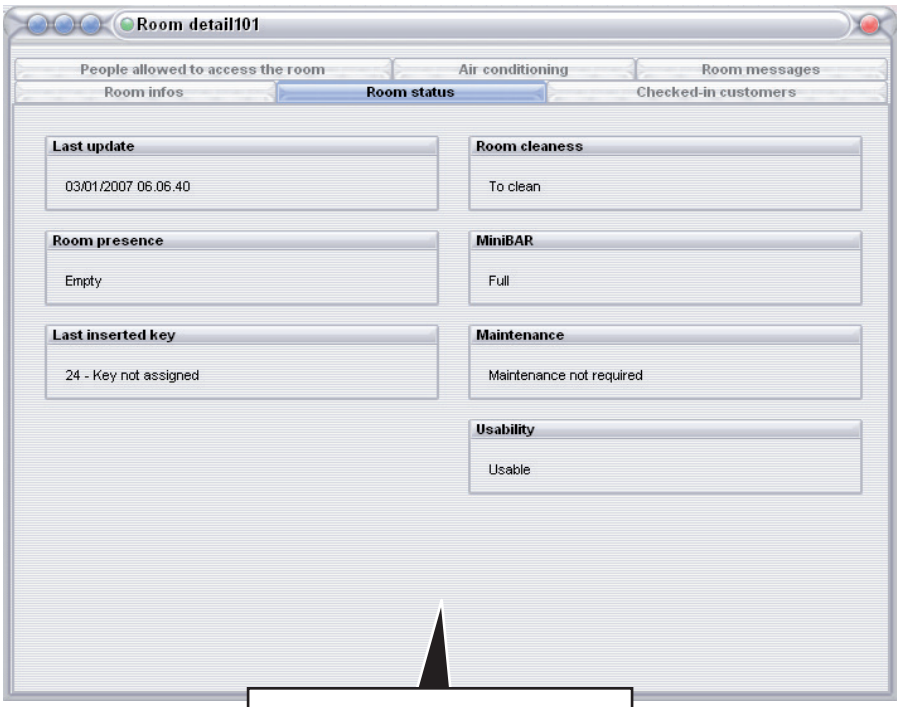
View of guest arrival and departure

All conditions previously described can be made up

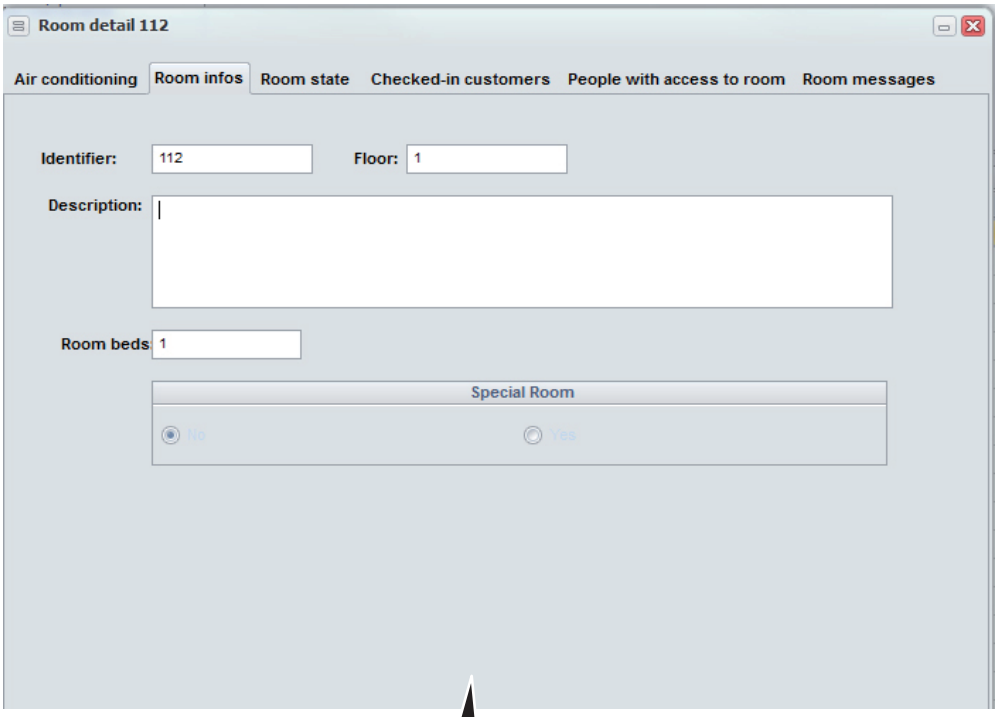
Selecting a room and clicking ROOM DETAILS, further information is shown.



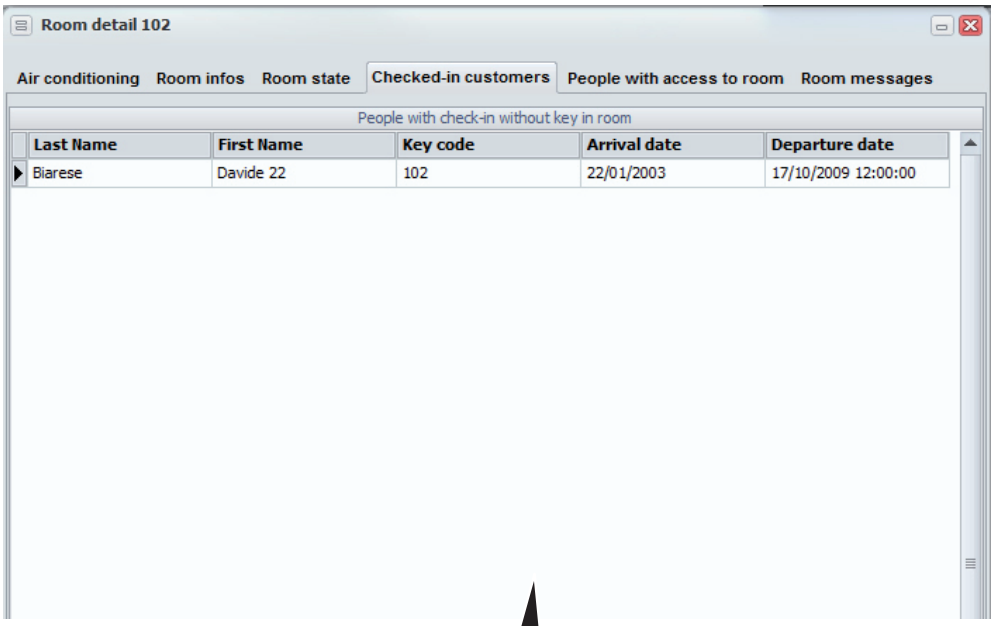
List of guests who were checked-in in the room



Room status



Room type



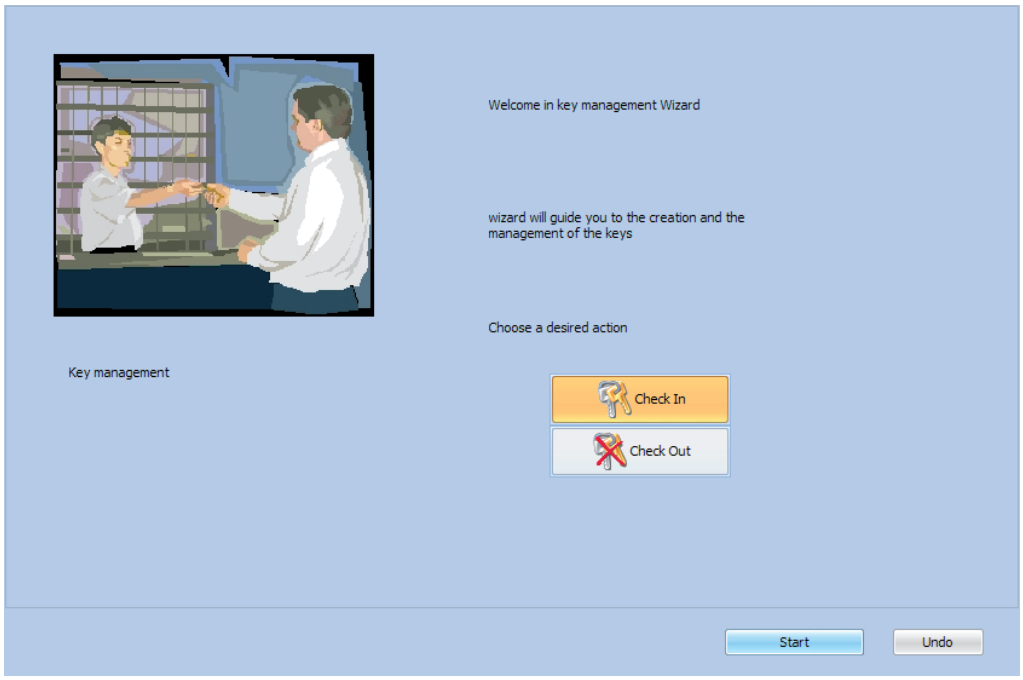
List of persons who can access the room, apart from the guest

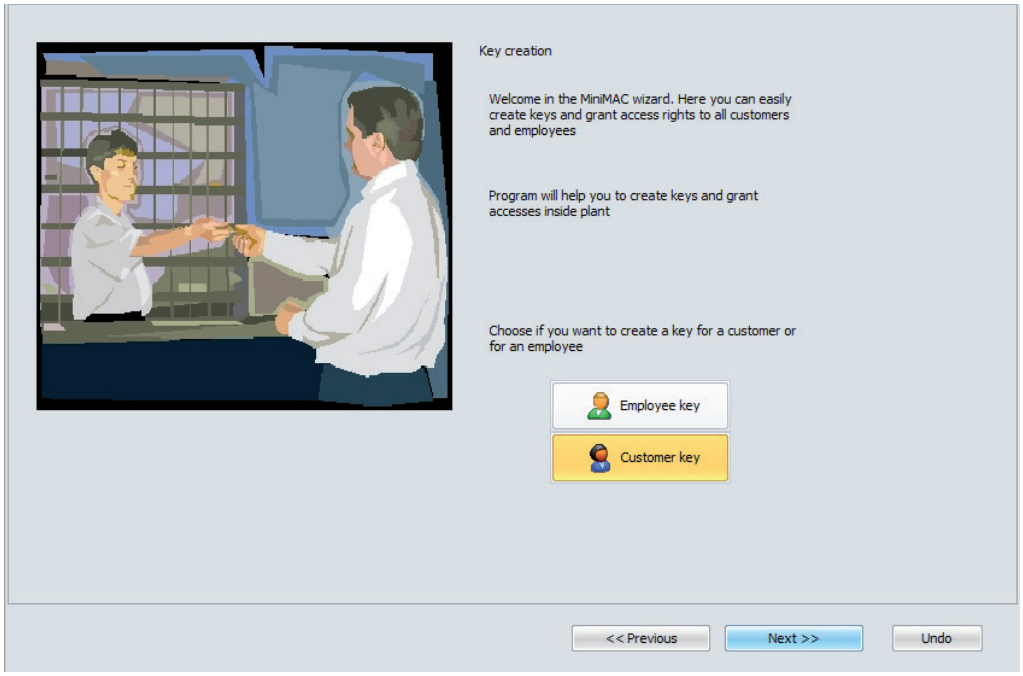
Heating adn Cooling information

7.2 Check-in

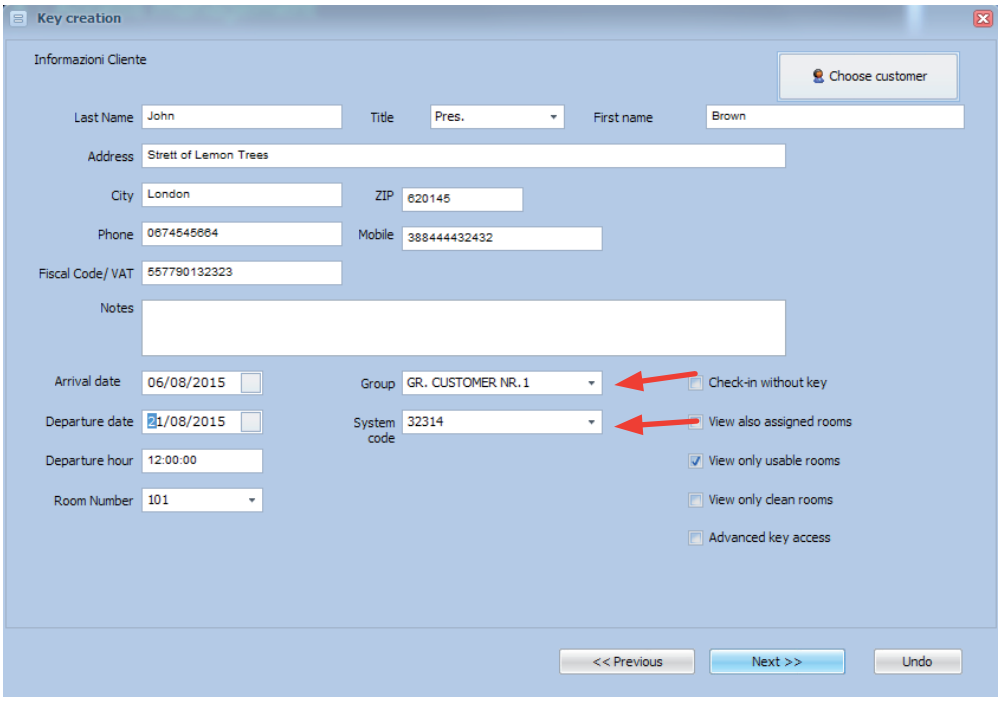
CHECK-IN WIZARD makes check-in operations very easy. During check-in, the system has to register the new guest, assign a room and generate for him/her and his/her fellows the TAGs for the access to the reserved areas.
The CHECK-IN procedure is supported by CHECK-OUT, whose function is to manage and automate the operations that are necessary to free the room and remove the TAGs (physically/logically) from the system.

Consider a check-in example. Mr. Brown and his wife will be guests of the hotel. Only a TAG will be generated and assigned to Mr. Brown.



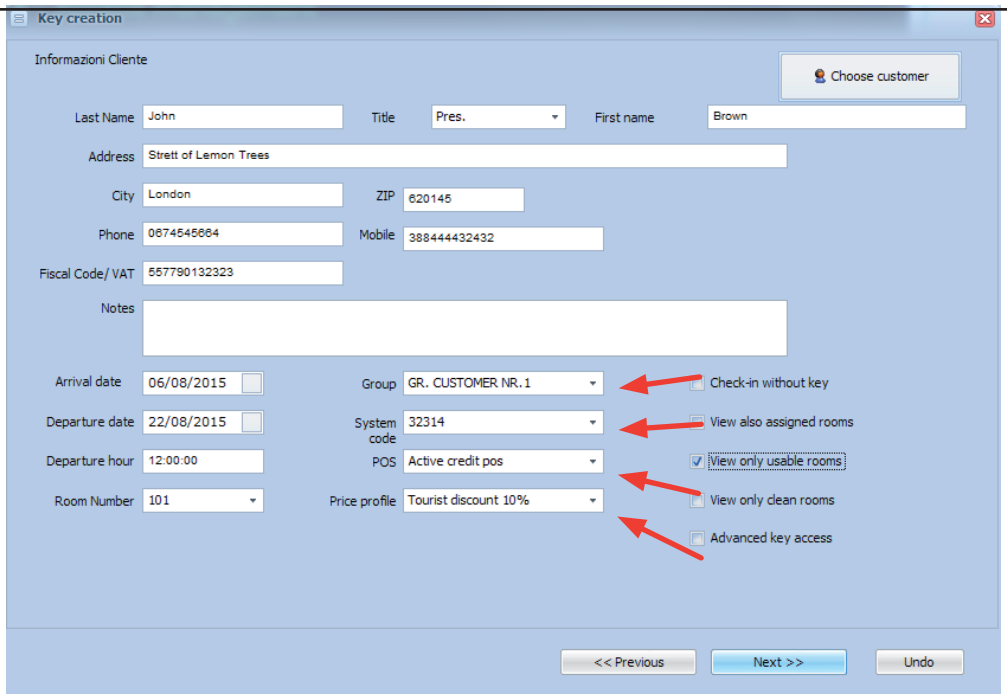


In a installation where there aren't devices with virtual money function (i.e. LTP/U, transponder reader with POS function), window to be filled with check-in data does not include automatically POS parameters.



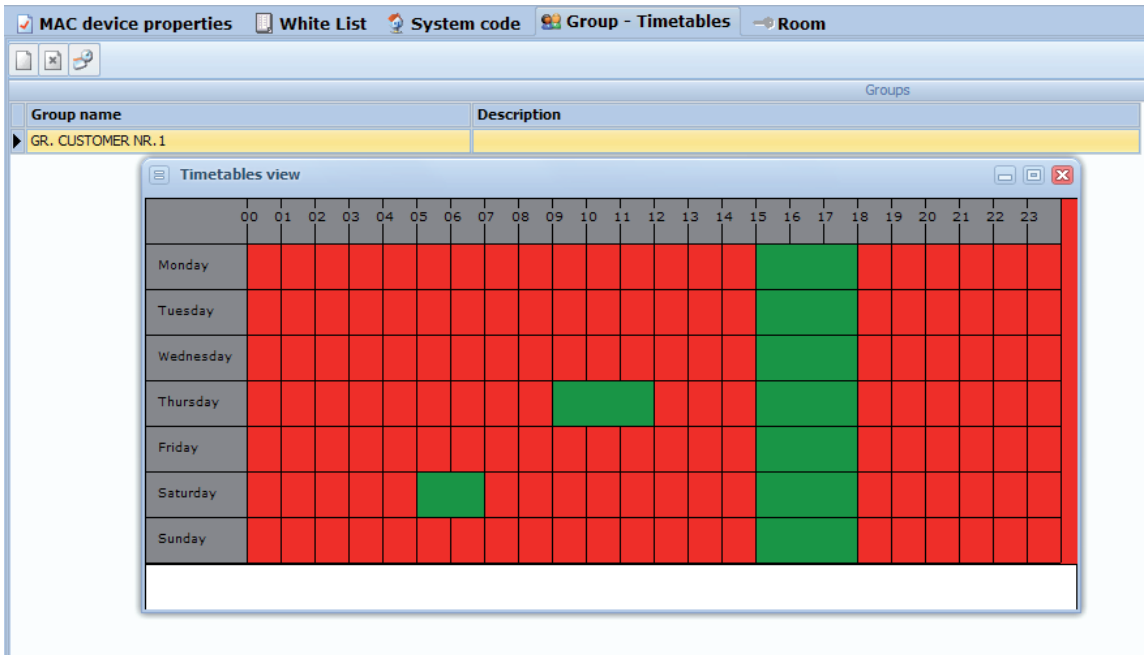
Create a TAG for the customer

In a installation where there are devices with virtual money function window to be filled with check-in data automatically include POS parameters.



Insert personal data and assign a room. Define the type of TAG. Decide whether the generated TAG can use POS services or not. Choose for example a POS-Credit card TAG.
Note that GR. CUSTOMER NR.1 has been selected for the customer. This means that, for devices with active timeslots, the allowed time profile will be that defined in GR. CUSTOMER NR.1.

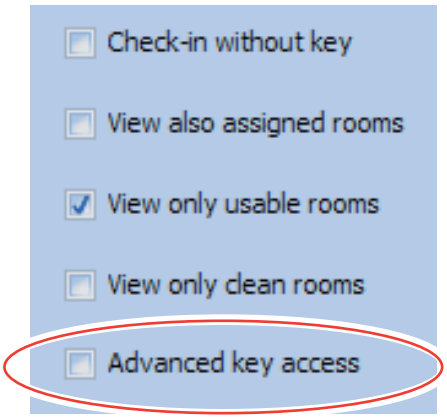
GR. CUSTOMER NR.1 definition:



Warning
In an installation where there aren't devices with virtual money function (i.e. LTP/U, transponder reader with POS function), on card creation memory reserved on the card for storing data about credit, is instead used for saving data about number of floor of the room associate to the card/guest. This data could be useful for integration of access control system with elevator systems.

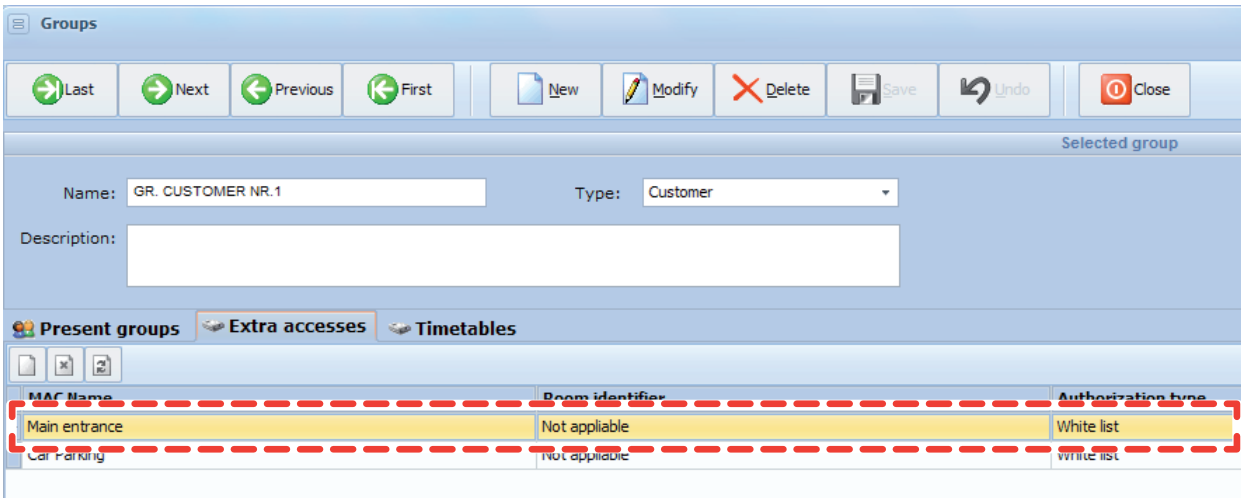
Please notice that functionalities of ABB access control system does not include integration with elevator system. When and if required, this integration has to be realized by system integrator, for example using data about number of floor stored on the transponder card.

In the check-in window by default the "Advanced key access" option (see figure below) at the bottom is not enabled. This means that after clicking on "Next" the check-in immediately ends writing the card inserted in the programming device. It's like a "fast" check-in.

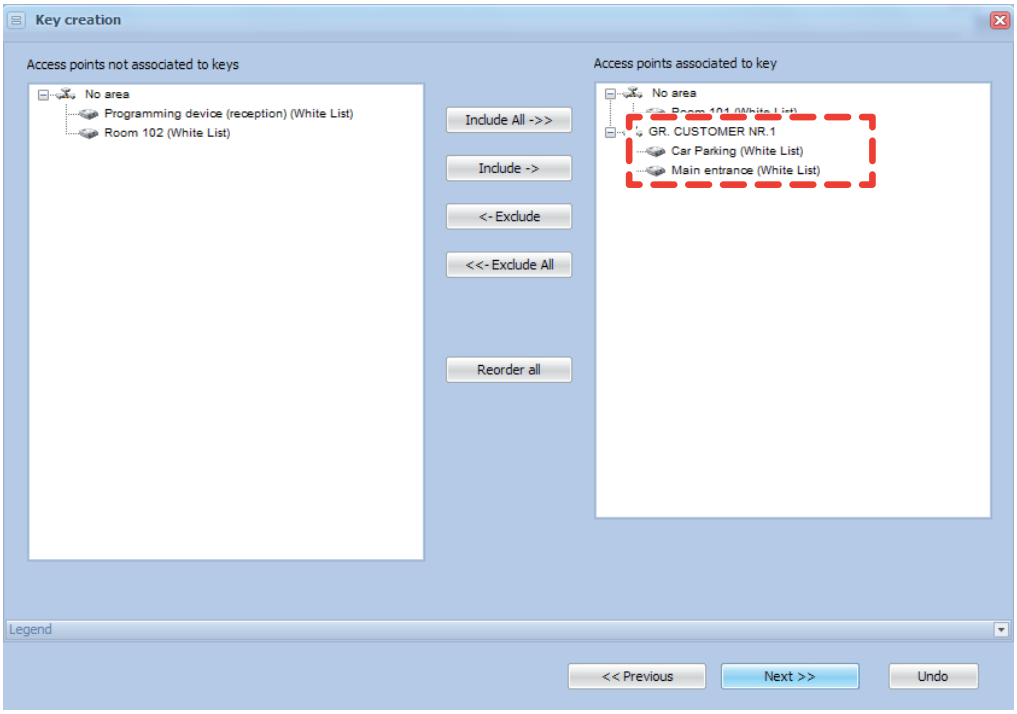


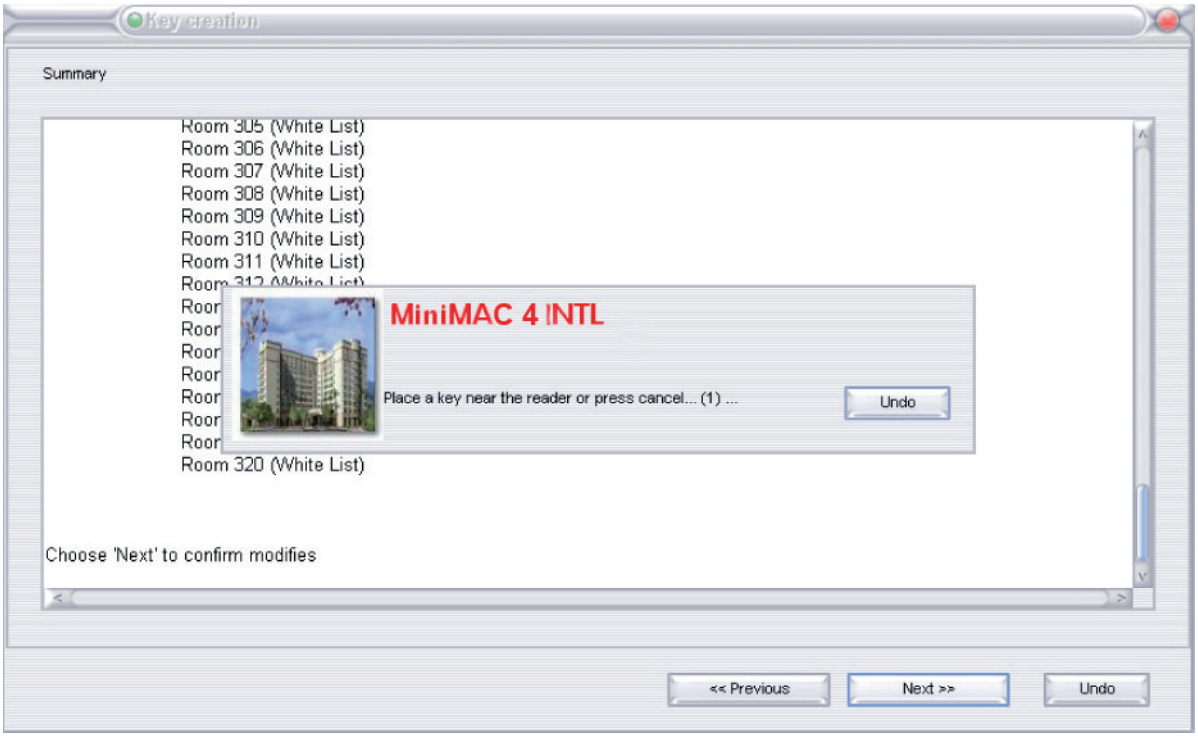
Otherwise, if “Advanced key access” option is enabled, the check-in procedure does not terminate immediately with card writing, but it’s possible to choose the entrances to which this customer (and therefore his/her card) has access.
In the figure below transits assigned to the TAG are shown.
A TAG assigned to a White list device means the TAG can access; a TAG assigned to a Black list device means the TAG cannot access.

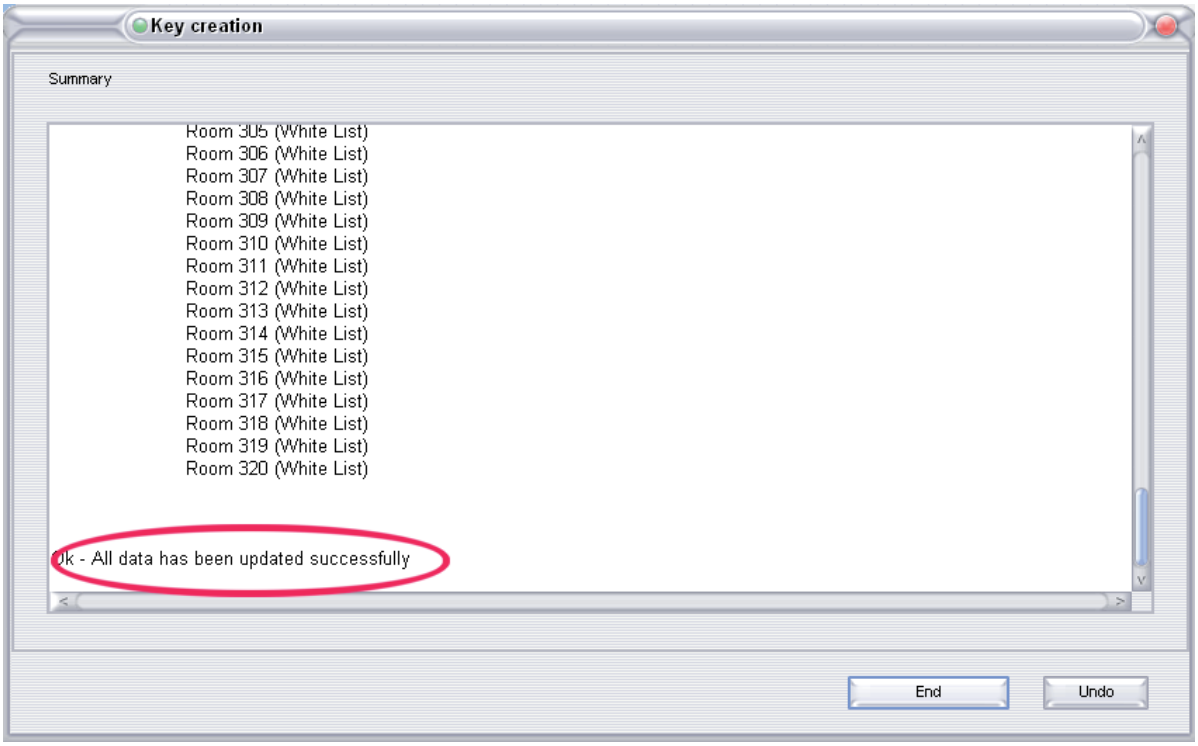
The guest has automatically access to assigned room (Room 101), and to entrances assigned to GR. CUSTOMER NR.1 in “Extra accesses” tab.



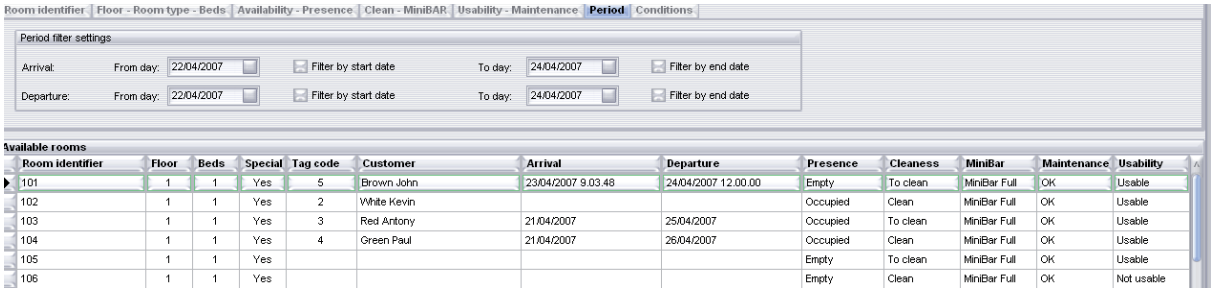
It’s obviously possible to select other entrances to give access.
Variations to authorization rights can be performed by moving devices icons from the right to the left window, and vice versa.

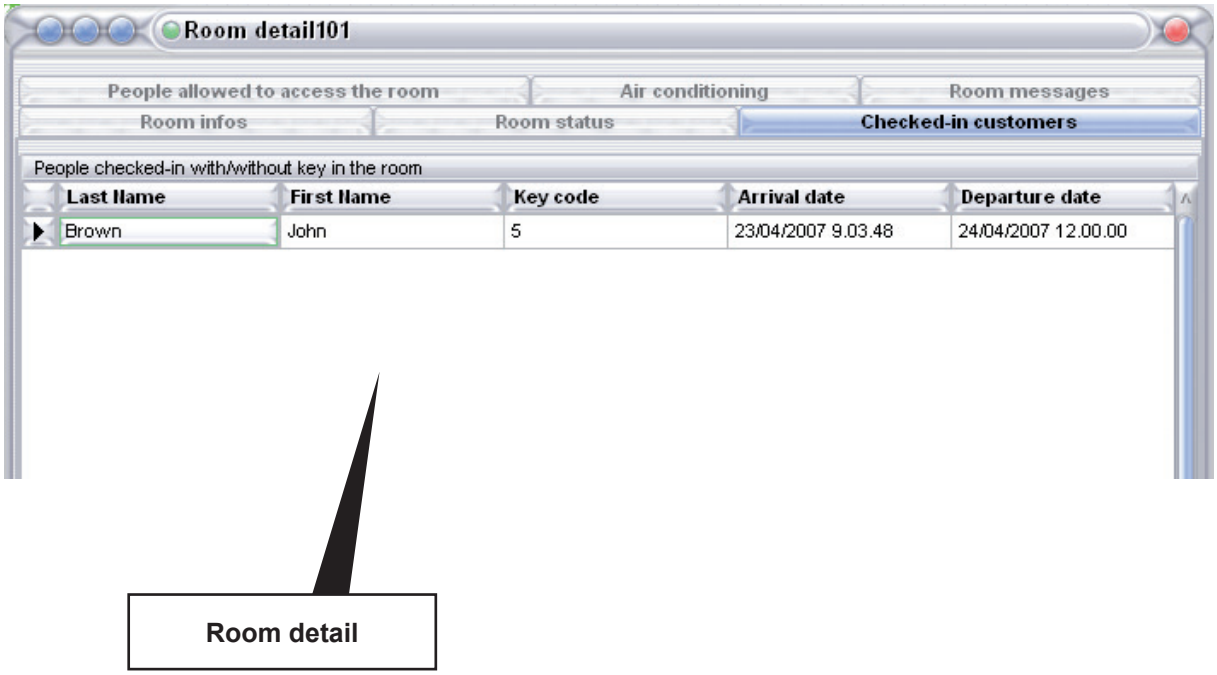



Key creation
Summary
Room 305 (White List)
Room 306 (White List)
Room 307 (White List)
Room 308 (White List)
Room 309 (White List)
Room 310 (White List)
Room 311 (White List)
Room 320 (White List)
MiniMAC 4 INTL
Place a key near the reader or press cancel... (1) ...
Undo
Choose 'Next' to confirm modifies
<< Previous
Next >>
Undo

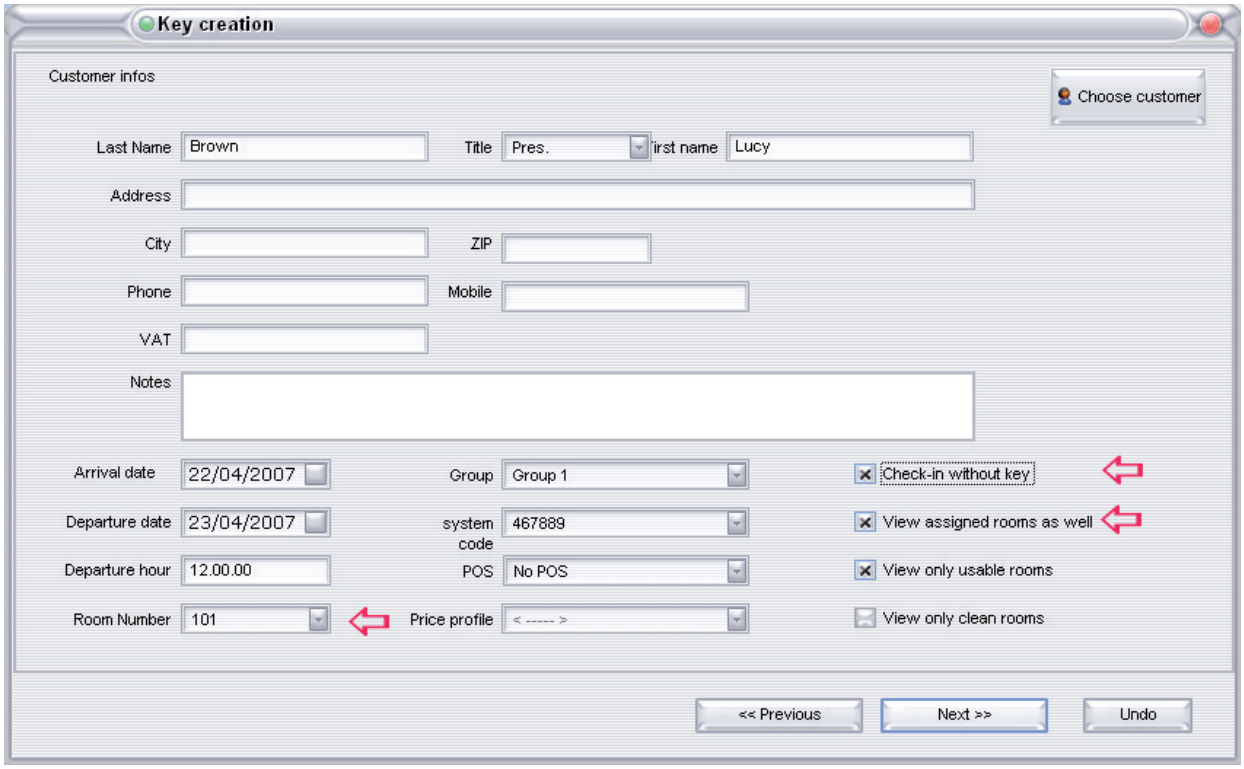

Key creation
Summary
Room 305 (White List)
Room 306 (White List)
Room 307 (White List)
Room 308 (White List)
Room 309 (White List)
Room 310 (White List)
Room 311 (White List)
Room 312 (White List)
Room 313 (White List)
Room 314 (White List)
Room 315 (White List)
Room 316 (White List)
Room 317 (White List)
Room 318 (White List)
Room 319 (White List)
Room 320 (White List)
Ok - All data has been updated successfully
End
Undo

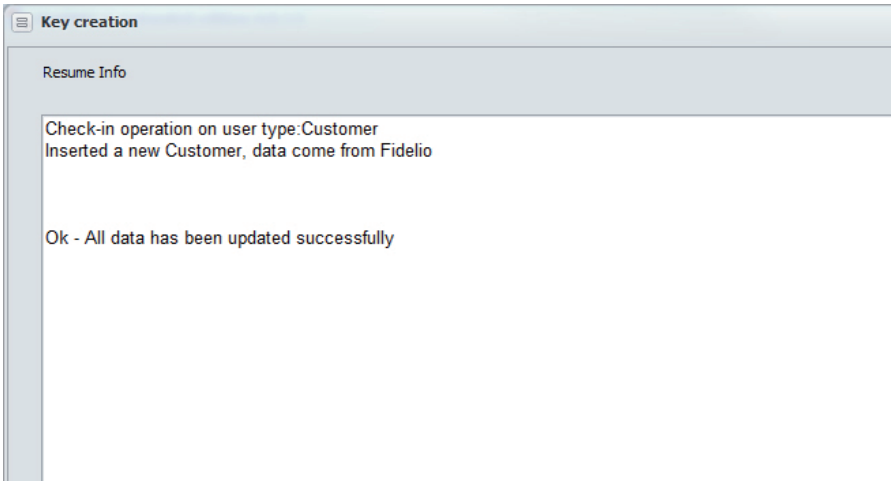
Check-in is completed and the TAG can be handed to the guest.
Room status shows room 101 assigned to Mr Brown.





Now, check-in Mrs. Brown Lucy, Mr. Brown's wife. Obviously, she will be checked-in to the same room. **She will be registered in same room 101. She has not requested a TAG so no TAG will be generated.**

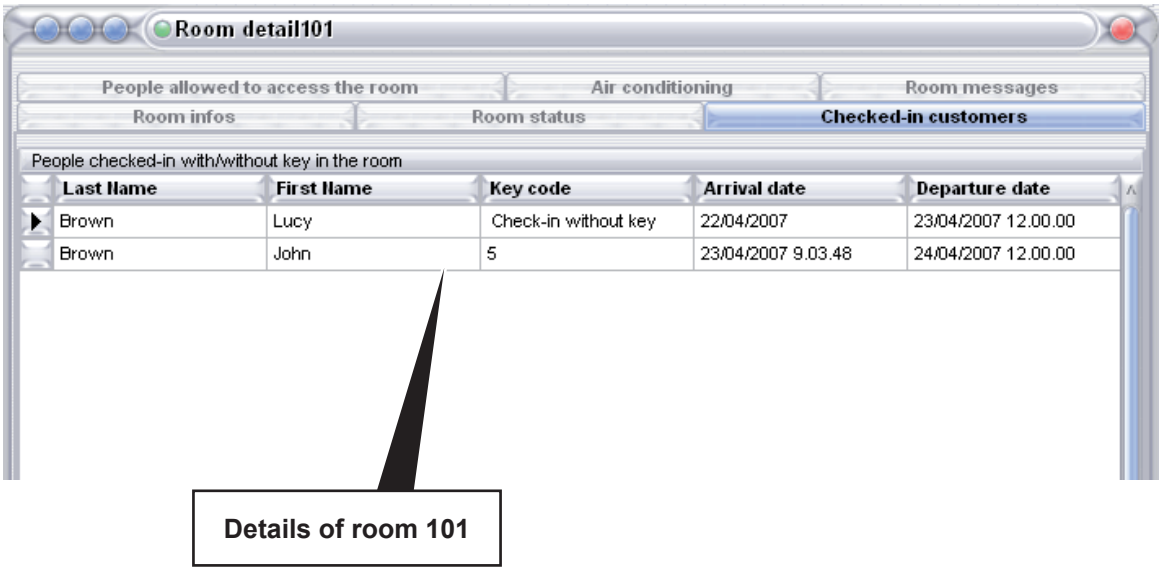




Available rooms

Room identifier	Floor	Beds	Special	Tag code	Customer	Arrival	Departure	Presence	Cleaness	MiniBar	Maintenance	Usability
101	1	1	Yes		Brown Lucy	22/04/2007 21.51.24	23/04/2007 12.00.00	Empty	To clean	MiniBar Full	OK	Usable
101	1	1	Yes	5	Brown John	22/04/2007 21.40.20	27/04/2007 12.00.00	Empty	To clean	MiniBar Full	OK	Usable
102	1	1	Yes	2	White Kevin			Occupied	Clean	MiniBar Full	OK	Usable
103	1	1	Yes	3	Red Antony	21/04/2007	25/04/2007	Occupied	To clean	MiniBar Full	OK	Usable
104	1	1	Yes	4	Green Paul	21/04/2007	26/04/2007	Occupied	Clean	MiniBar Full	OK	Usable
105	1	1	Yes					Empty	To clean	MiniBar Full	OK	Usable
106	1	1	Yes					Empty	Clean	MiniBar Full	OK	Not usable
107	1	1	Yes					Empty	To clean	Empty	Maintenance re	Usable

Room status shows that Mrs. Brown is a guest of room 101.



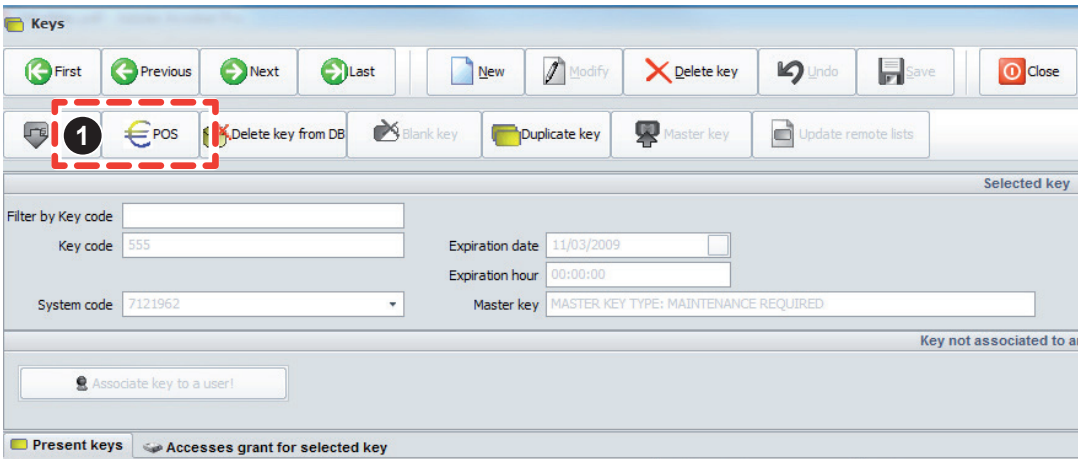
7.3 Customer TAG management

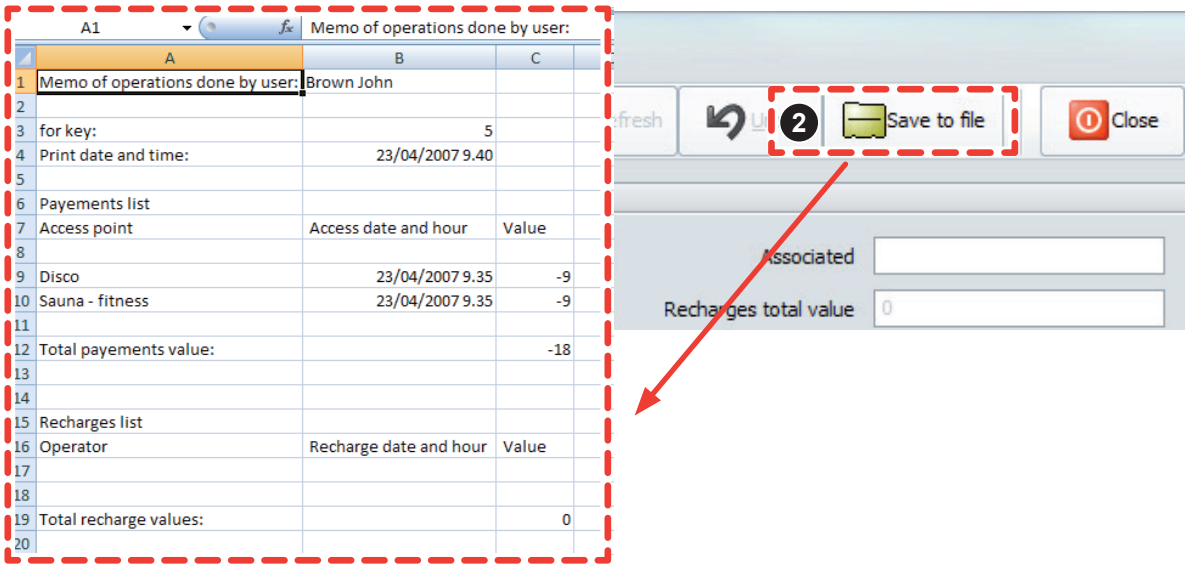
The guest can use the TAG to access his/her room and a defined number of entrances. The collection of accessible entrances is defined during Check-In.

In the example shown in the previous section, the TAG was enabled to POS functions with Credit Card: this means the card can access to POS transits an unlimited number of times. Only a final statement will show the expenses total amount.
In TAGS menu, clicking on POS (**1**) button, a report of POS transits shows up.
The report lists the payments made with the POS TAG:

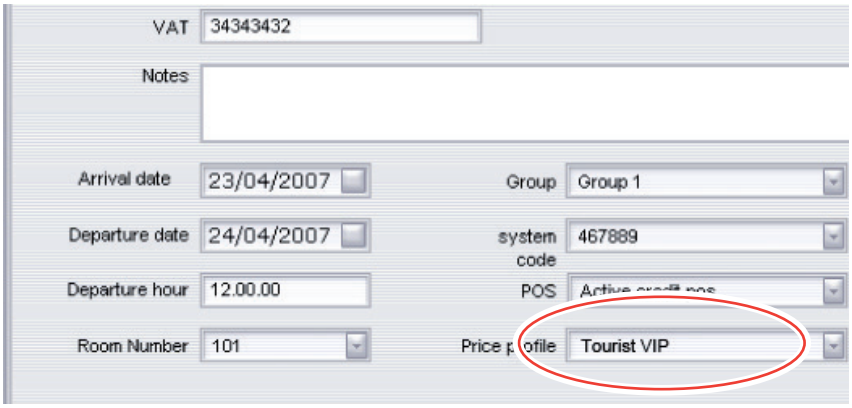
- date and time of the event
- location of POS entrance
- applied rate.

It is possible to save the report as an EXCEL file and then print it. It is not a fiscal receipt, but it is an "expenses summary" to be used at the administrator's discretion.
In the example of Mr. Brown, we simulated two accesses: one to the fitness room and the other to the discotheque.

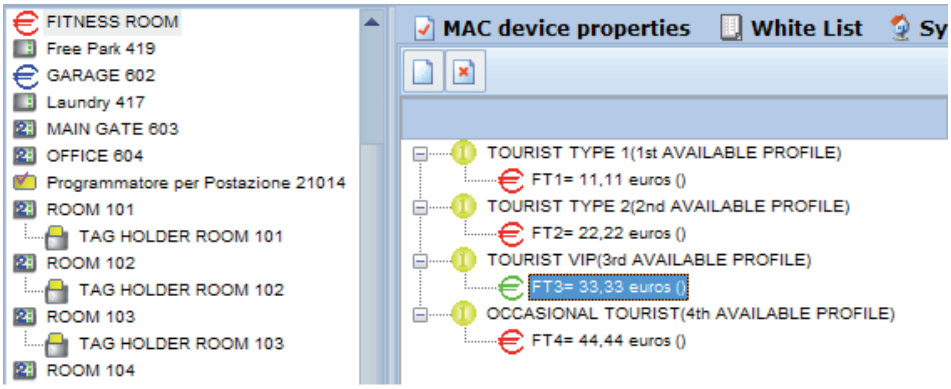




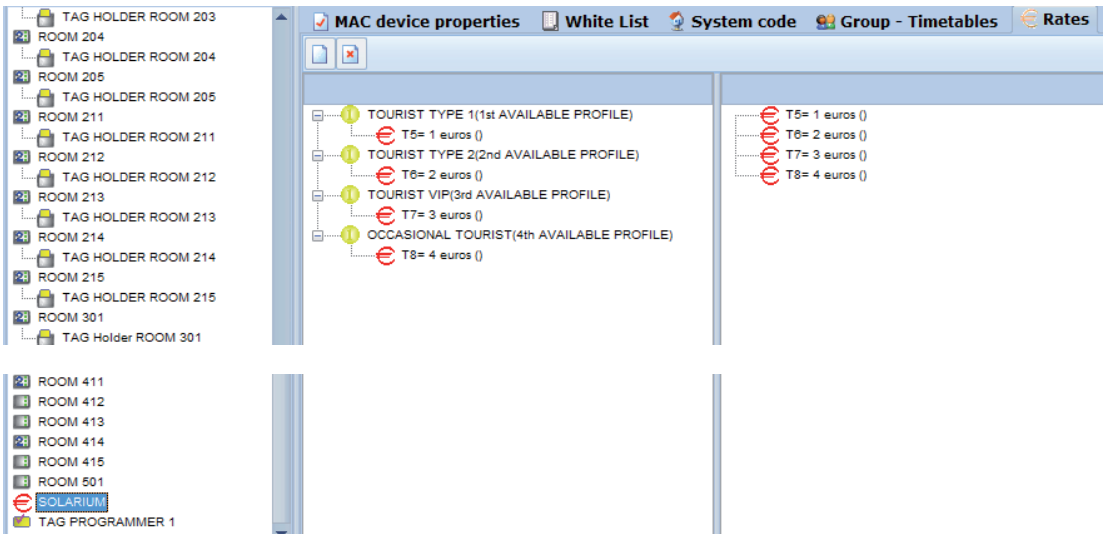
Remember that the rates paid by the customer depend on the Rate Profile assigned to Mr. Brown's TAG during check-in. In this example, a VIP profile was assigned to Mr. Brown's TAG.



It is possible to check which rate is associated with this profile in the two payment accesses under examination, using the System menu and clicking the "Rates" Tab corresponding to the payment entrance in question ("Fitness room" in this case).



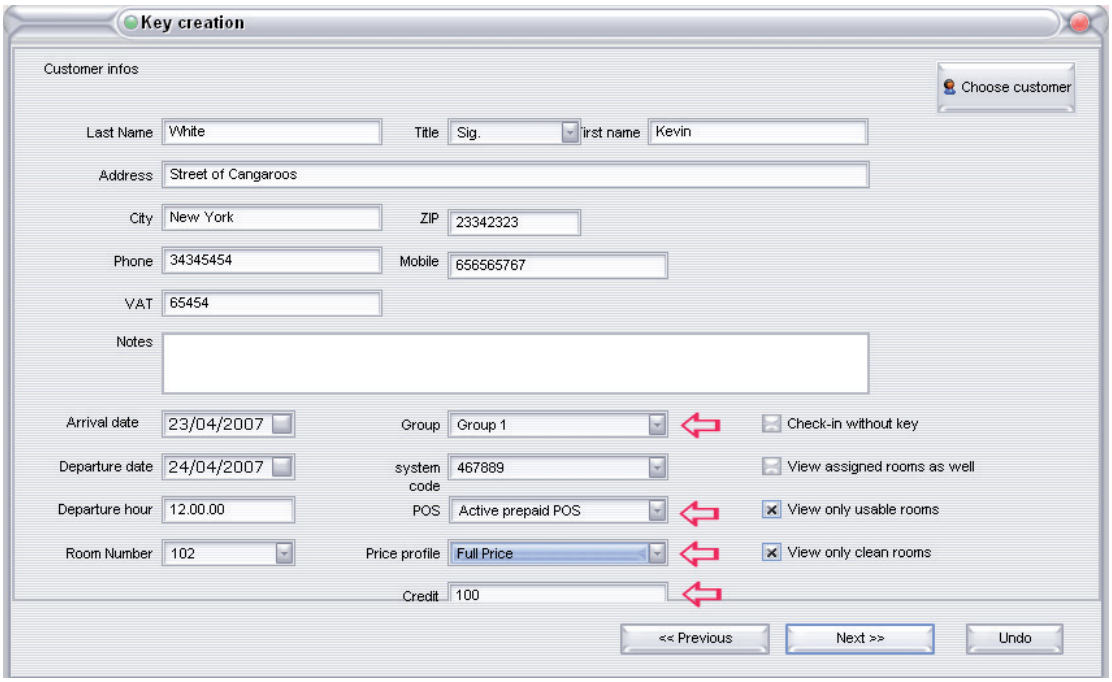
In this case, you can see that the "Fitness room" rate: for Tourist VIP profile = 33,33 €.



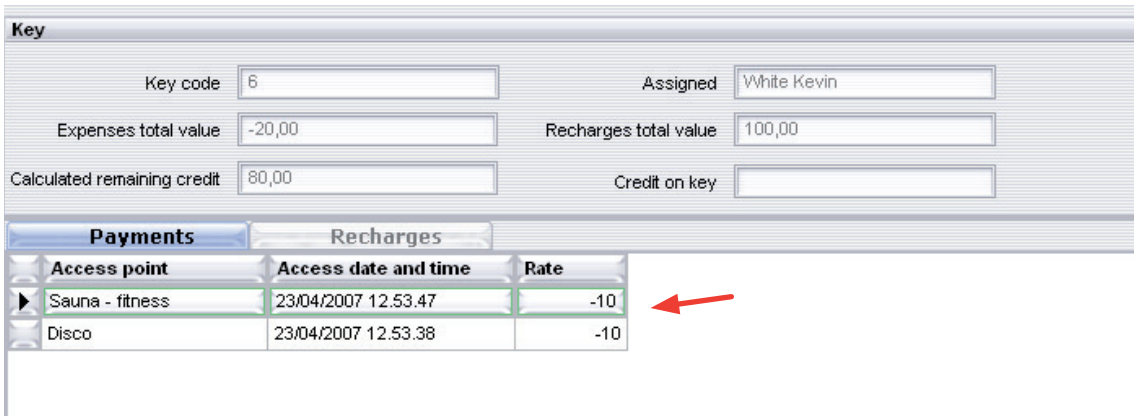
SOLARIUM rate: for Tourist profile VIP = 3 €

Note that customers with different profiles have to pay different rates (obviously this is an example: you can decide to have only one rate for all customers).

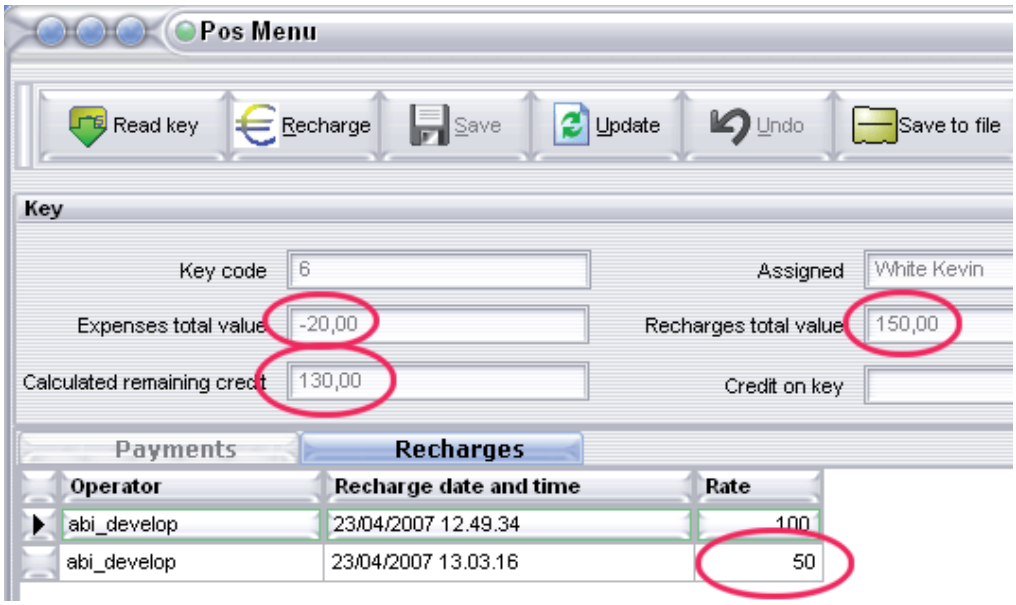
A POS TAG can also be created with a prepaid amount. During check-in this type of TAG can be chosen and the administrator decides the amount to be charged on the TAG. During the entire stay, guest can recharge his/her card an unlimited number of times (TAGS menu, POS and RECHARGES). Otherwise when the residual amount in the TAG is not high enough to pay the rate applied by a POS device, **transit is not authorised**.



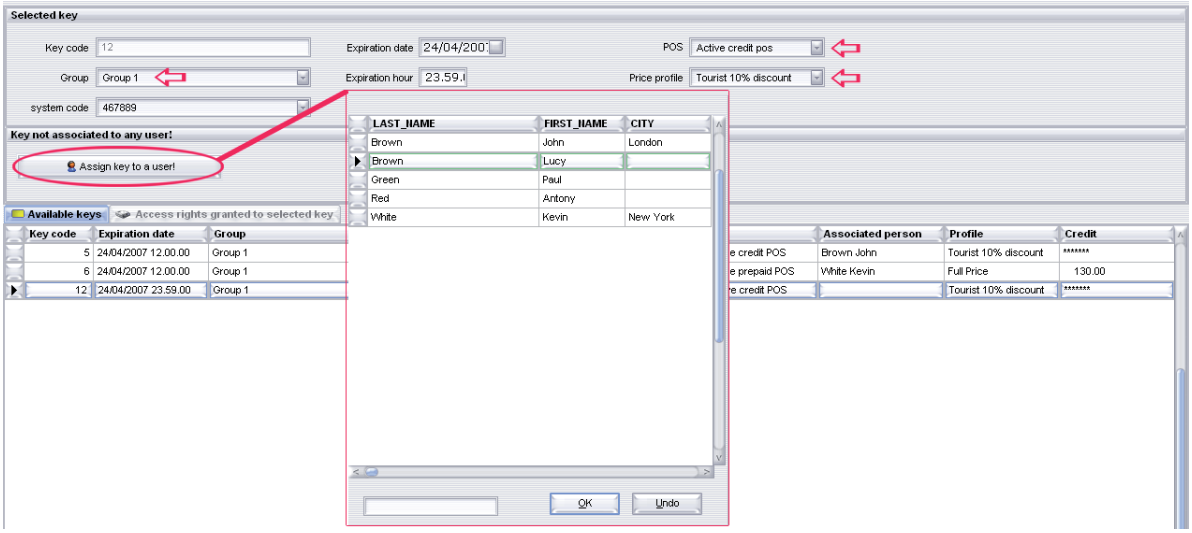
In this example, a prepaid POS TAG is created for the customer. Note that Mr. White has a profile “Full price”: if he goes to the fitness room, he pays a rate in accordance to his profile which is different from Mr. Brown’s one.



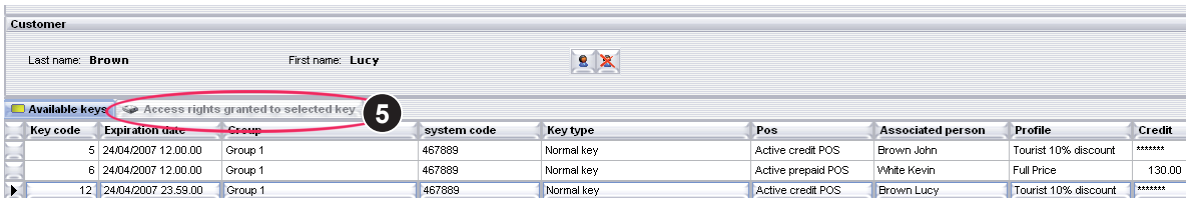
Mr. White can recharge the prepaid POS TAG:



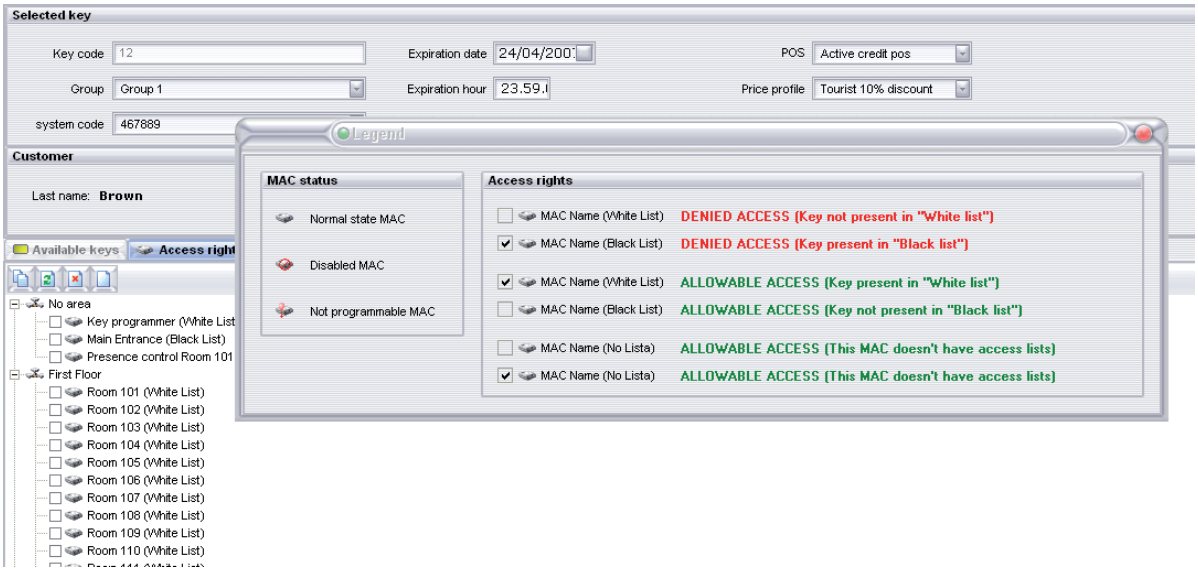
Now consider Mrs. Brown wishes to get a personal TAG. She checked-in before, so a new TAG can be generated in TAGS menu.
Since her personal data have already been recorded during check-in (for further details see previous section), click to associate the new TAG with the customer already present in the database, then save and assign access rights.



With respect to the check-in procedure, where access rights to the room and various entrances are automatically set when creating the TAG, during the 'manual' procedure you have to pay particular attention since access rights must be set manually.
After saving, the situation is:



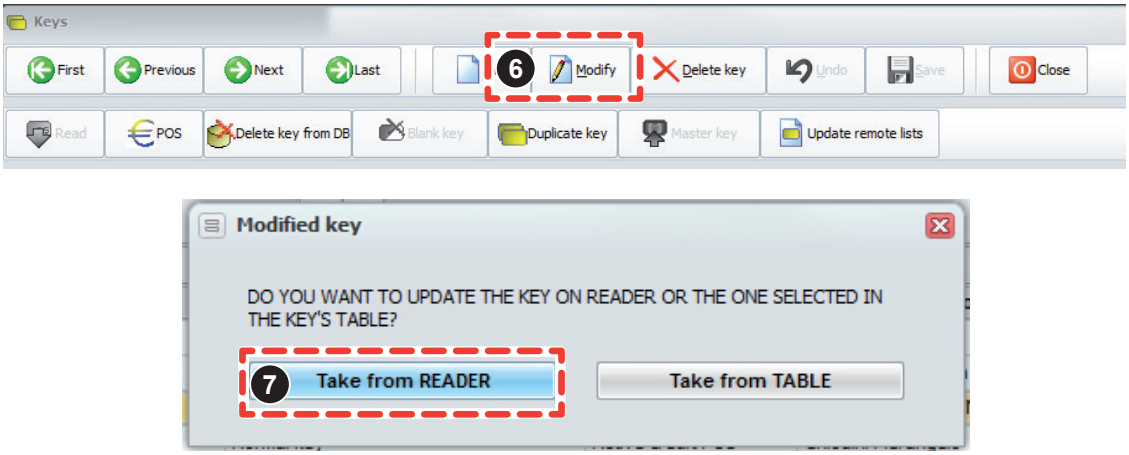
For the assignment of transit rights, click “ACCESS RIGHTS FOR THE SELECTED TAG” TAB (**5**):

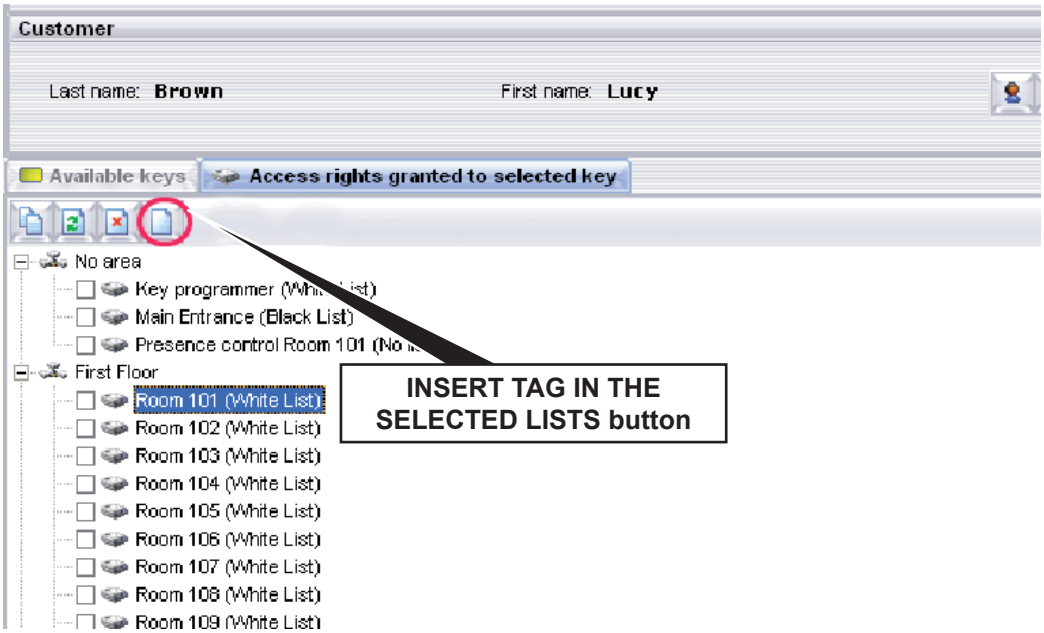


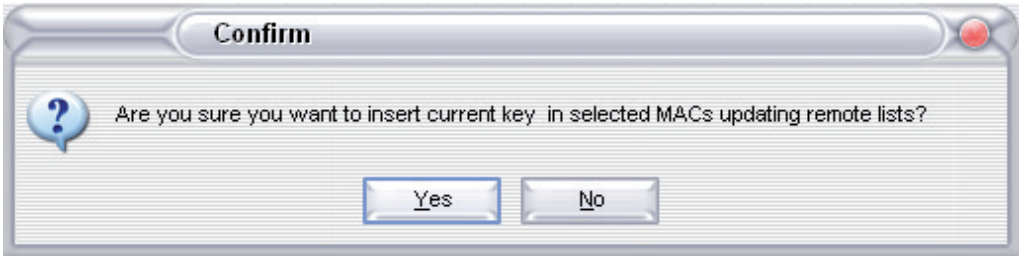
The current view shows the collection of all system devices. A legend explains that access is possible when the TAG is in a White list, while it is denied when the TAG is in a Black list.
Assuming that Mrs. Brown needs the same access rights given to her husband, room (101) and POS area are assigned.
TAG insertion in the devices lists is easy:

- Select EDIT in the Toolbar (**6**);
- MiniMAC asks you whether the TAG to be modified is the one inserted in the programming device (PRT/U) or it has to be chosen from the TAGs list. In our case, the TAG is taken from the reader (**7**);

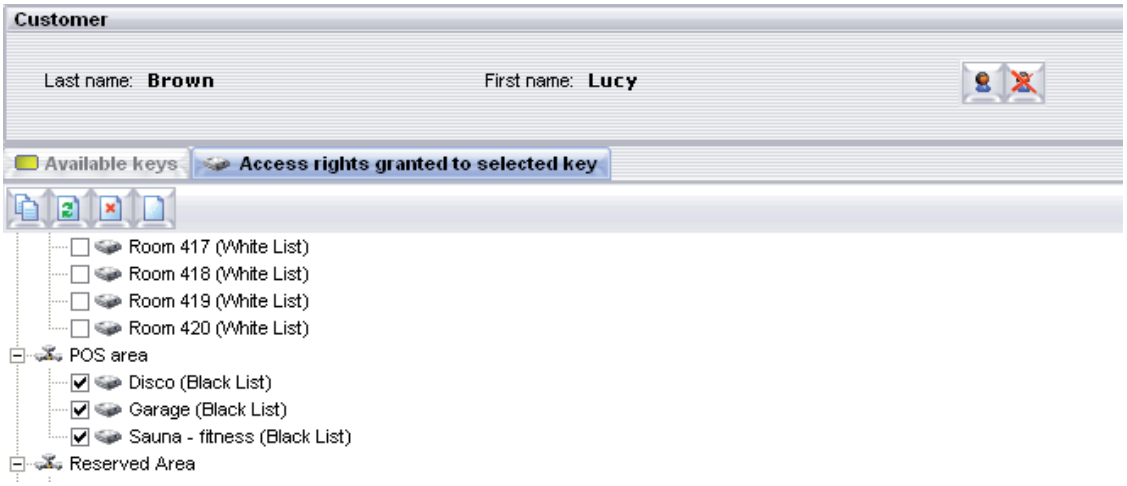
- Select the devices (multiple selections allowed: SHIFT+LEFT CLICK) and click "Insert" in the minitoolbar.



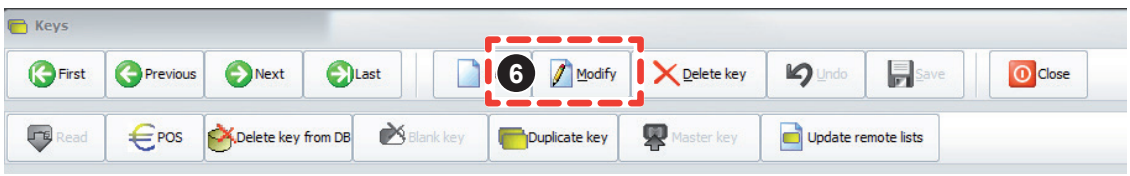


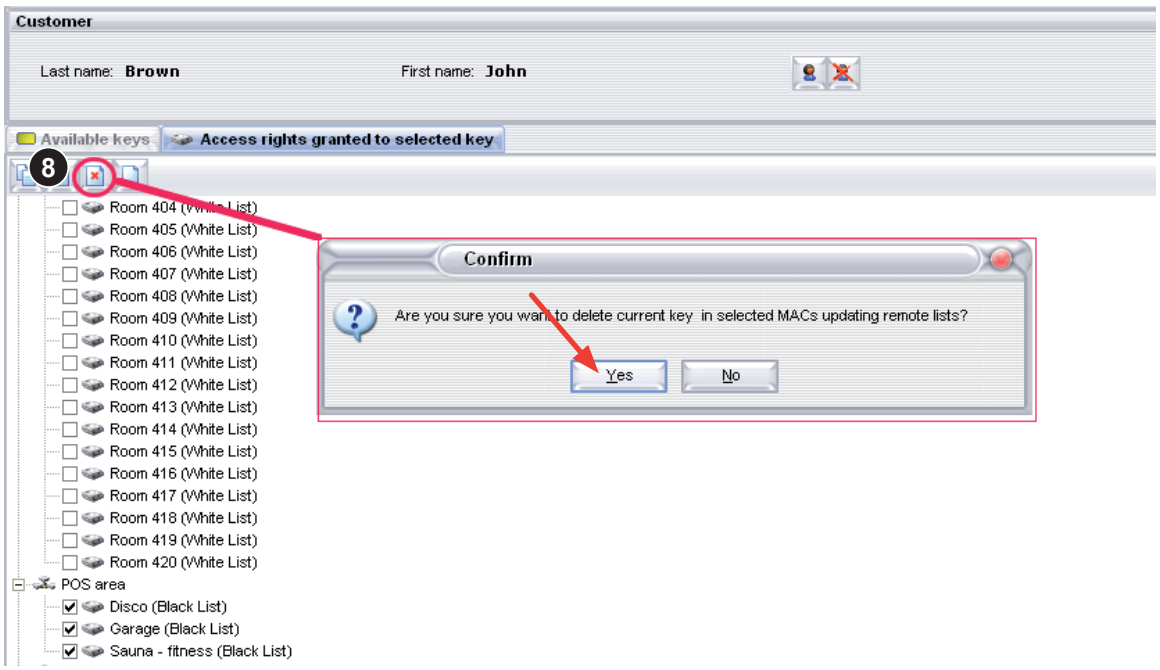


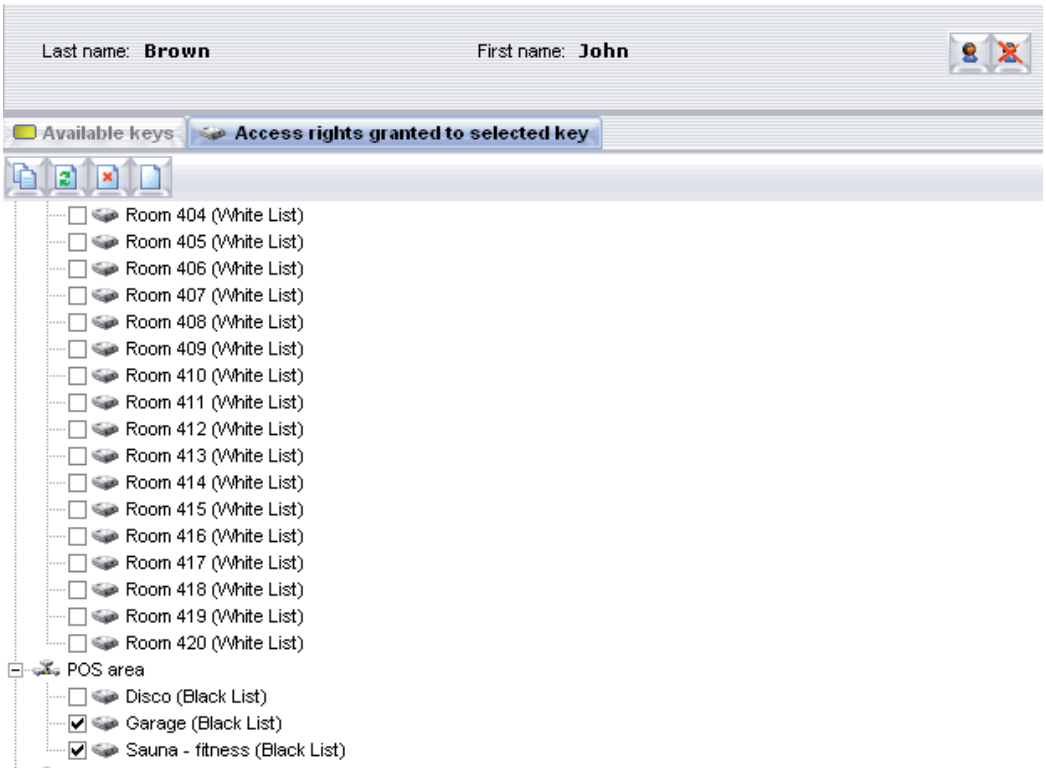
After confirmation, the TAG is inserted in the devices that have been selected.



Now consider that Mr. Brown wants to renounce the right to access the DISCOTHEQUE.
The procedure to remove an access right is: in TAGs menu, select Mr. Brown's TAG and click Edit (**6**). Click "Transits Right" TAB, select the device in which the TAG has to be removed and then click Delete (**8**) in the minitoolbar.







After this modification, Mr. Brown will no longer be able to access the discotheque.

7.4 Check-out

When the guests' stay is completed, their room must be vacated so that other customers can use it. Furthermore we have to decide what to do with the TAGs. There are two possibilities:

1. Check-out with TAG
2. Check-out without TAG

Note
During check-out, remember to calculate the final balance of POS TAG-credit card. Decide whether the residual amount in a prepaid POS TAG has to be refunded or not.

7.4.1 Check-out with TAG

In a Check-out with TAG, the guest returns his/her TAG. The procedure removes the TAG from all devices where it was declared valid and the TAG is **formatted/deleted and available for a new programming**.

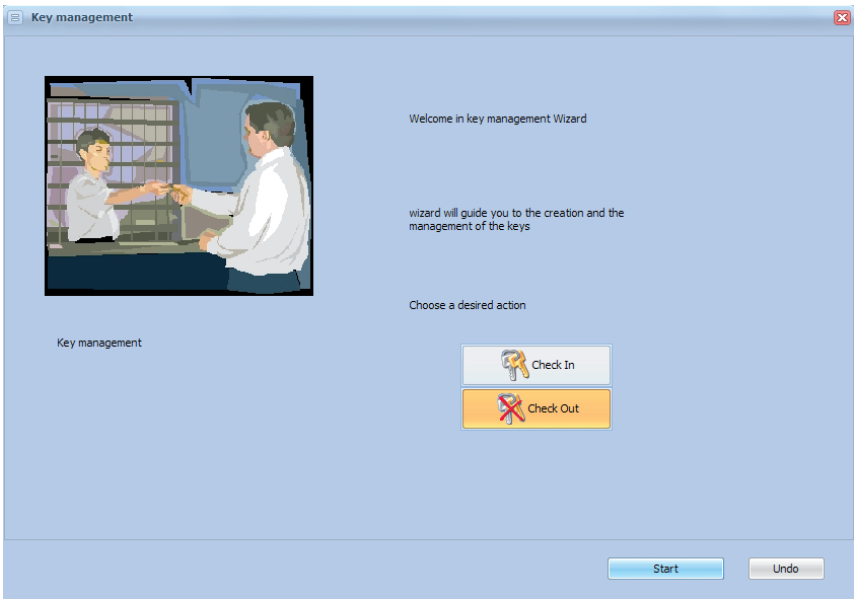
7.4.2 Check-out without TAG

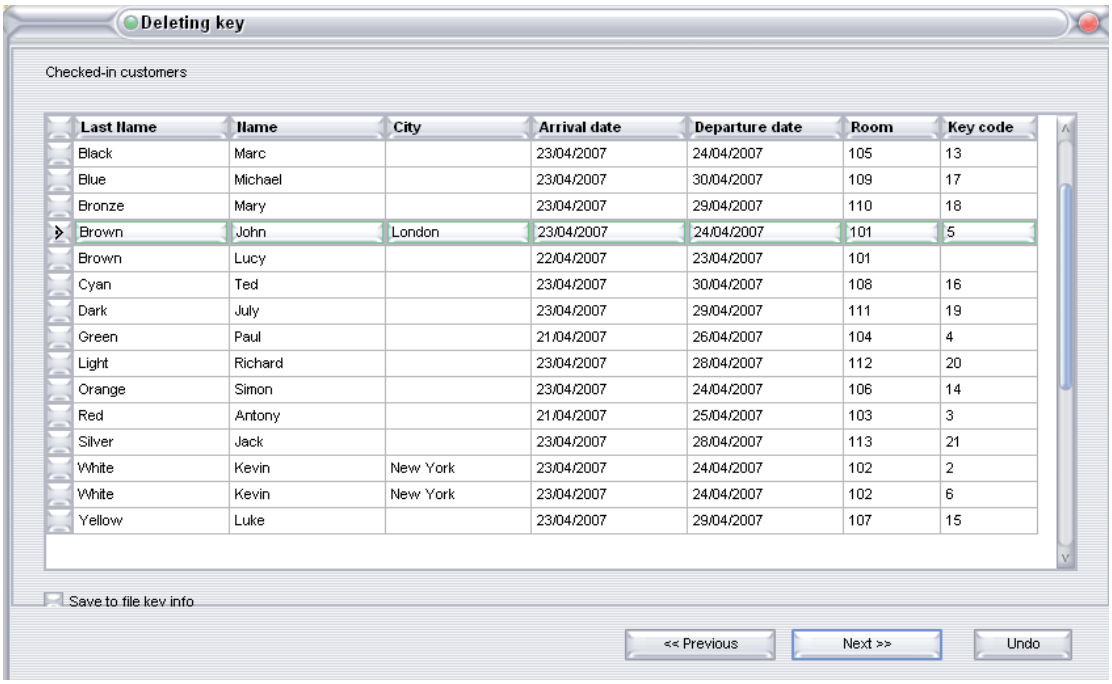
In a check-out without TAG, the TAG is removed from the system (as in the previous case) but it should not be returned (therefore it is not formatted). The reasons for such a check-out are several: the guest decides to keep the TAG, or s/he lost it, or the administrator decides to leave it to the customer.

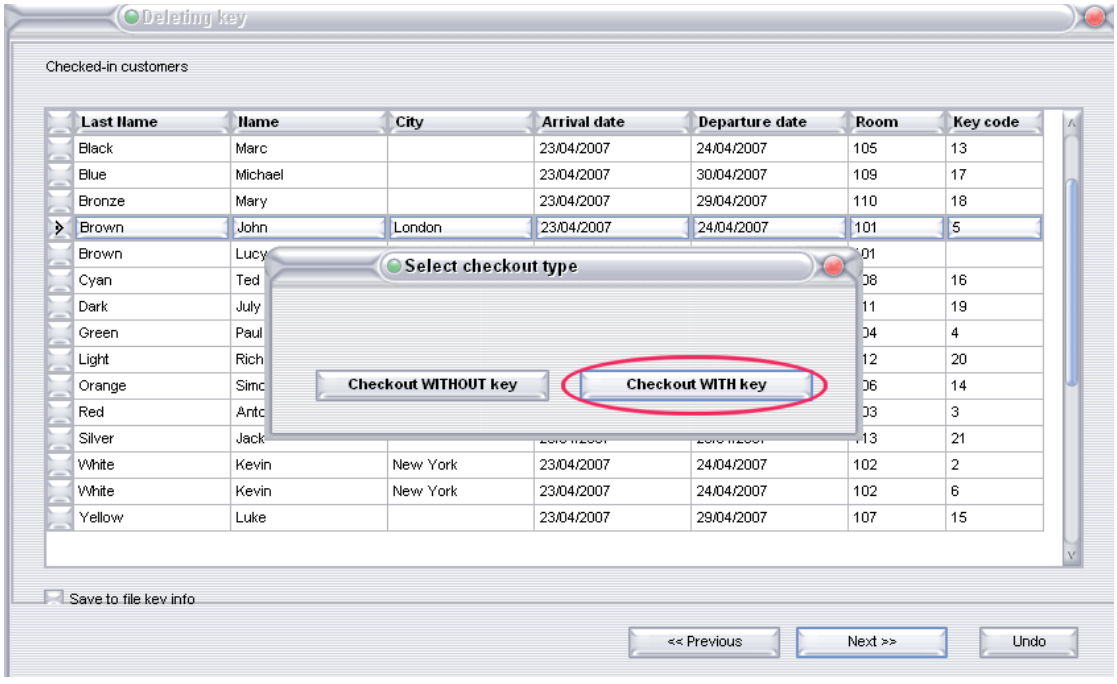
Note
Note that the TAG was removed from White lists, so it cannot get access to those transits. However, the TAG is not automatically inserted in Black lists, typical of common areas, so it keeps getting access to transponders working in Black list (at least as far as the TAG expires, usually the check-out day).

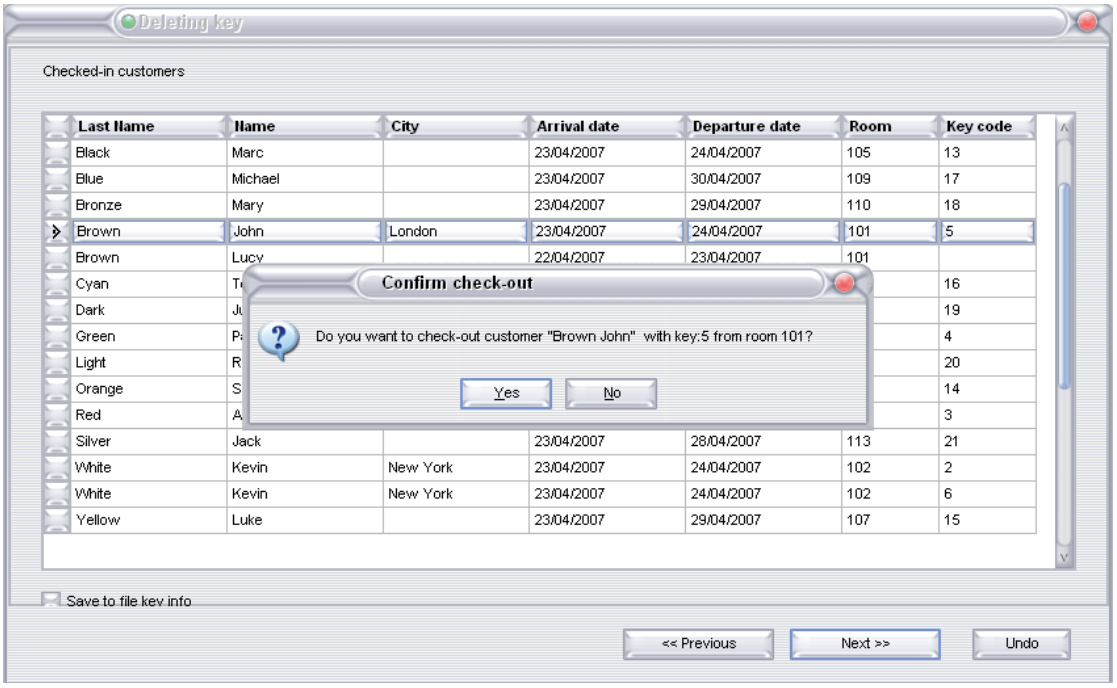
This choice is due to the fact that customers may need their TAG after check-out as well.
For example, if the garage and the external entrances where inserted in the Black list, the customer can use his/her TAG to exit the building without any assistance. If you are not interested in this last option: after check-out without TAG, the administrator can insert the TAG in all Black lists and it will stop working.

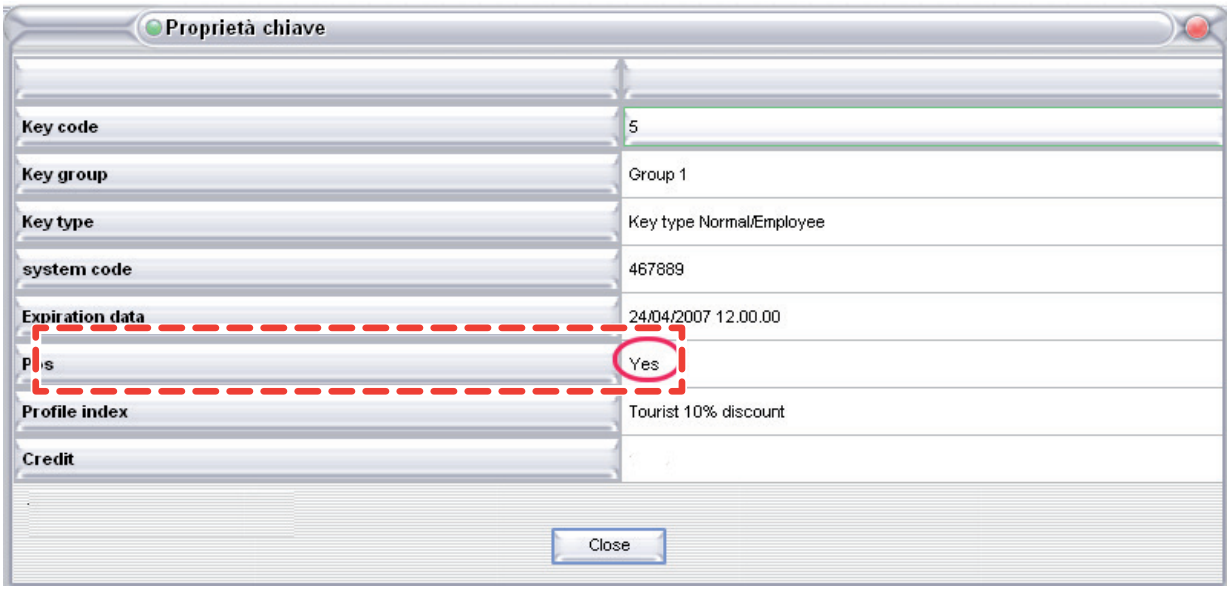
In this example, Mr. Brown's check-out is with TAG whereas Mrs. Brown's check-out will be without TAG.



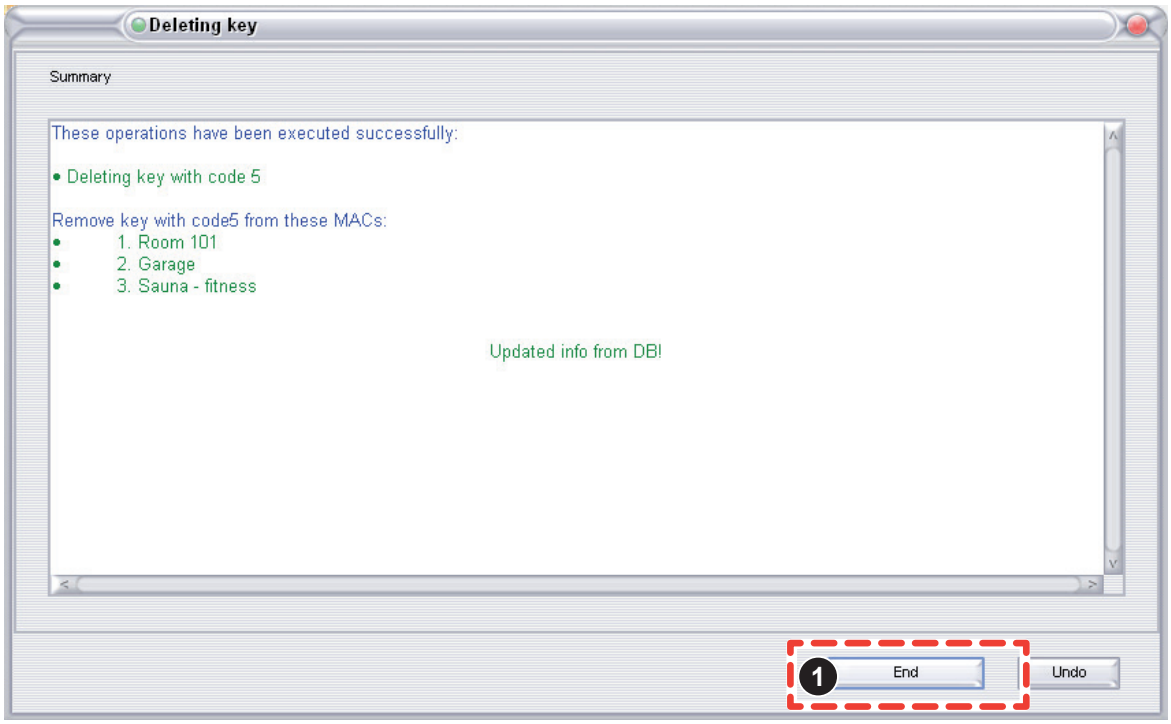

Deleting key
Checked-in customers
Last Name | Name | City | Arrival date | Departure date | Room | Key code
Black | Marc | | 23/04/2007 | 24/04/2007 | 105 | 13
Blue | Michael | | 23/04/2007 | 30/04/2007 | 109 | 17
Bronze | Mary | | 23/04/2007 | 29/04/2007 | 110 | 18
Brown | John | London | 23/04/2007 | 24/04/2007 | 101 | 5
Brown | Lucy | | 22/04/2007 | 23/04/2007 | 101 |
Cyan | Ted | | 23/04/2007 | 30/04/2007 | 108 | 16
Dark | July | | 23/04/2007 | 29/04/2007 | 111 | 19
Green | Paul | | 21/04/2007 | 26/04/2007 | 104 | 4
Light | Richard | | 23/04/2007 | 28/04/2007 | 112 | 20
Orange | Simon | | 23/04/2007 | 24/04/2007 | 106 | 14
Red | Antony | | 21/04/2007 | 25/04/2007 | 103 | 3
Silver | Jack | | 23/04/2007 | 28/04/2007 | 113 | 21
White | Kevin | New York | 23/04/2007 | 24/04/2007 | 102 | 2
White | Kevin | New York | 23/04/2007 | 24/04/2007 | 102 | 6
Yellow | Luke | | 23/04/2007 | 29/04/2007 | 107 | 15
Save to file key info
<< Previous
Next >>
Undo


Deleting key
Checked-in customers
Last Name | Name | City | Arrival date | Departure date | Room | Key code
Black | Marc | | 23/04/2007 | 24/04/2007 | 105 | 13
Blue | Michael | | 23/04/2007 | 30/04/2007 | 109 | 17
Bronze | Mary | | 23/04/2007 | 29/04/2007 | 110 | 18
Brown | John | London | 23/04/2007 | 24/04/2007 | 101 | 5
Select checkout type
Checkout WITHOUT key
Checkout WITH key
White | Kevin | New York | 23/04/2007 | 24/04/2007 | 102 | 2
White | Kevin | New York | 23/04/2007 | 24/04/2007 | 102 | 6
Yellow | Luke | | 23/04/2007 | 29/04/2007 | 107 | 15
Save to file key info
<< Previous
Next >>
Undo

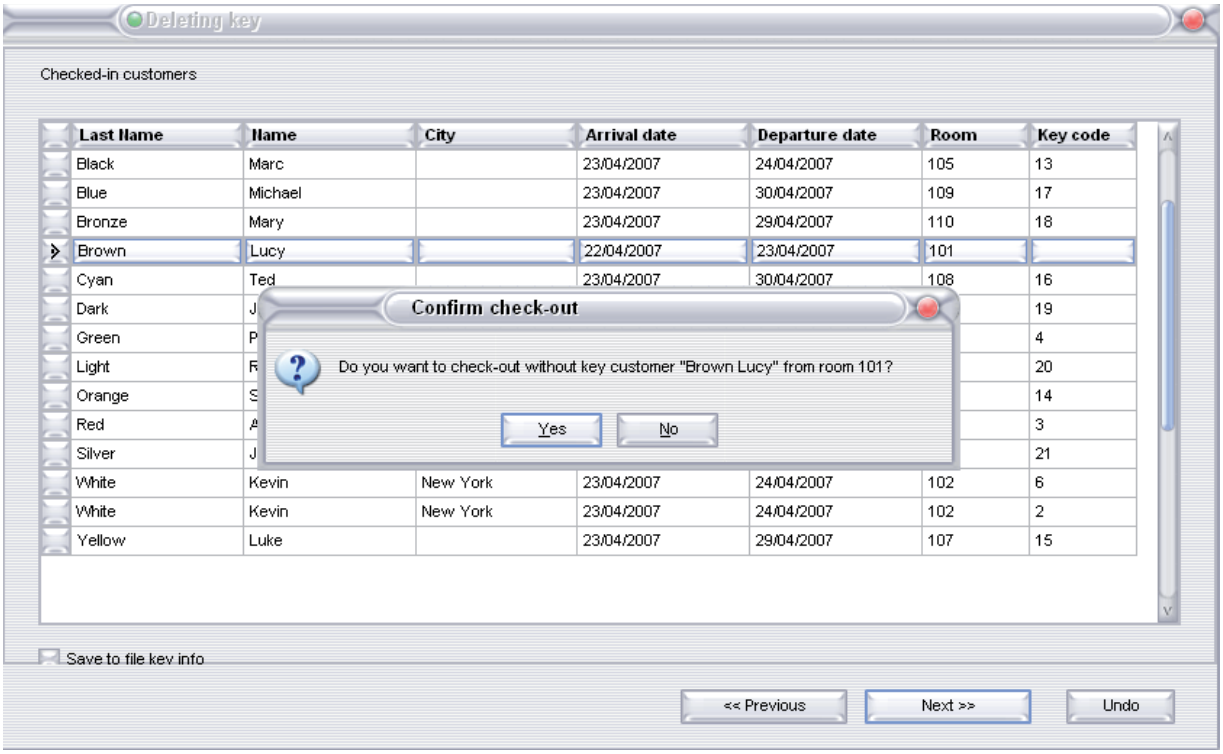




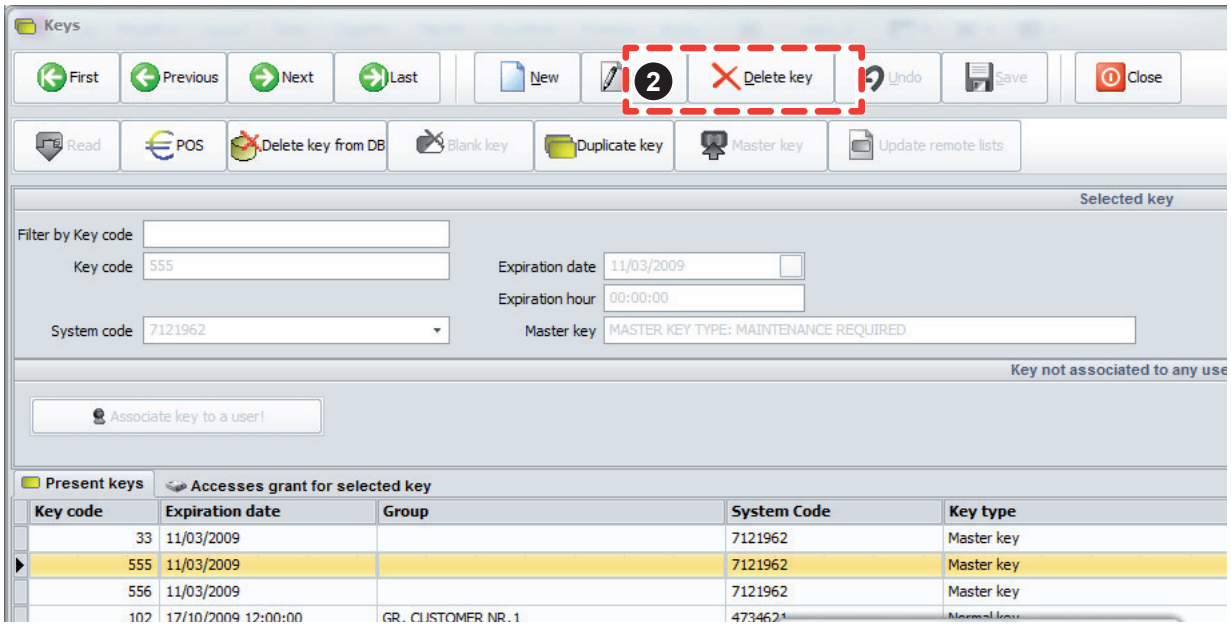
Note
This panel reminds you that TAG type is POS-credit card and final balance must be calculated before deleting the TAG.
If you have not calculated the final balance yet, stop checking out and in TAGs-POS menu display the final balance of the TAG.



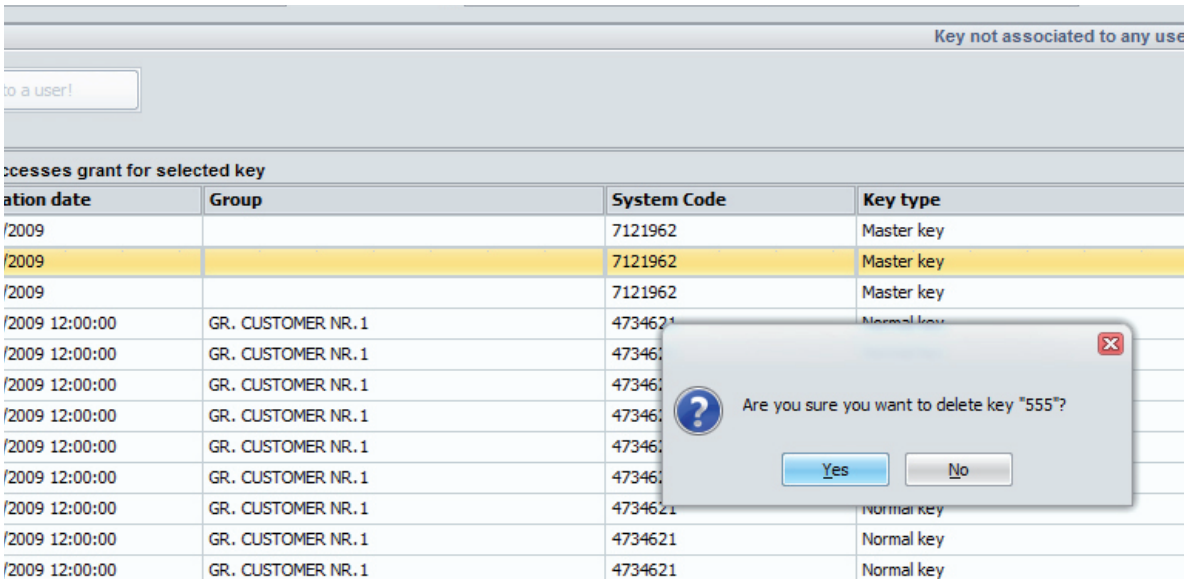
Click Next (**1**) and the operation is completed.
The differences in case Mrs. Brown is checked-out without TAG are shown below.



The only possible choice for Mrs. Brown is check-out without TAG. A check-out without TAG has to be chosen because no TAG was generated during check-in. The TAG created after checking in must be removed from TAGs menu.

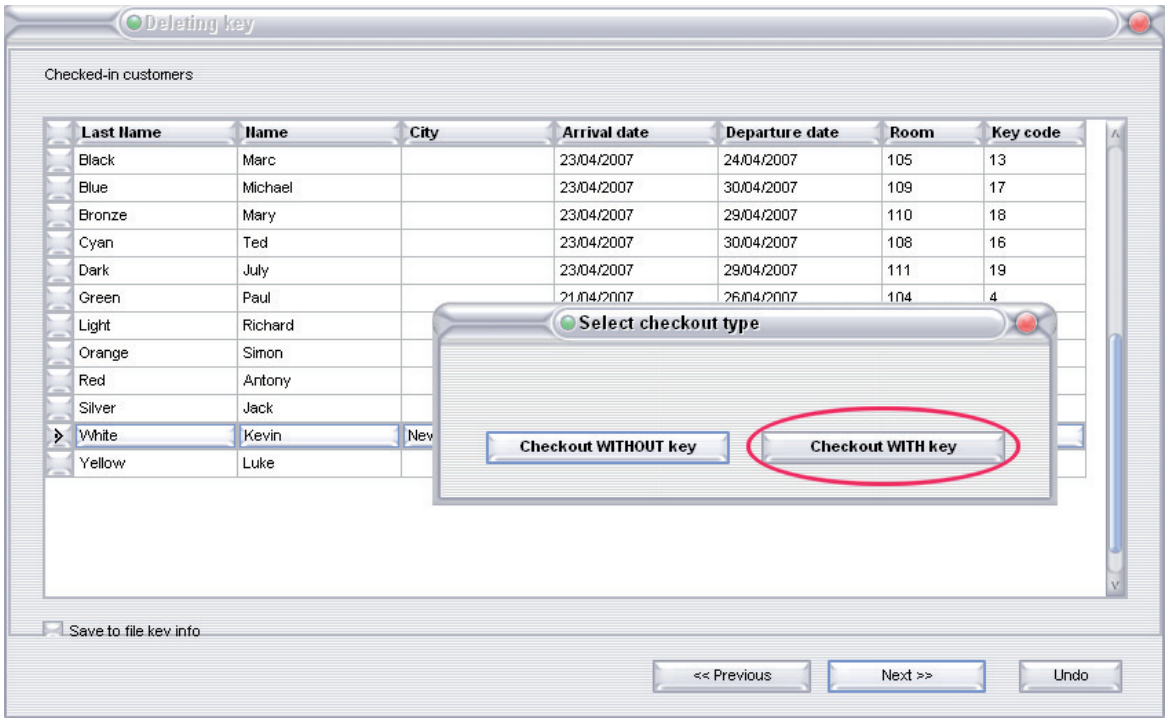


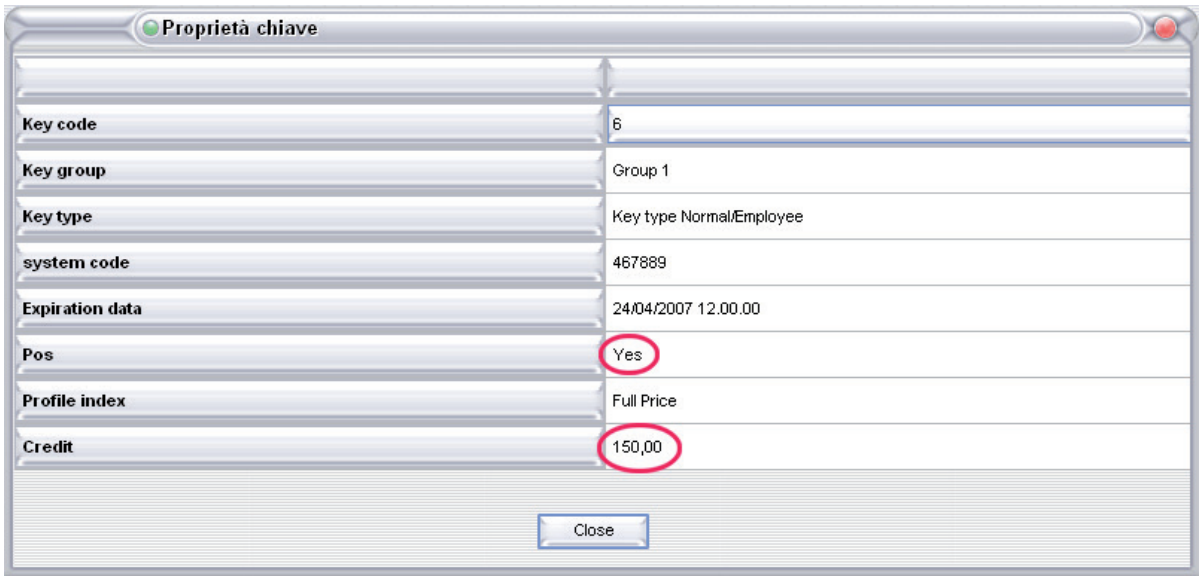
Mrs. Brown's TAG could be definitively removed by pressing Delete button (**2**):



Answer NO because we want to leave the TAG to the couple.They will use the TAG to leave the hotel through Black list transits (for example, the garage).

If a customer has a prepaid POS TAG, MiniMAC warns you that during check out with TAG the residual credit will be lost. The following example explains Mr. White's check out:

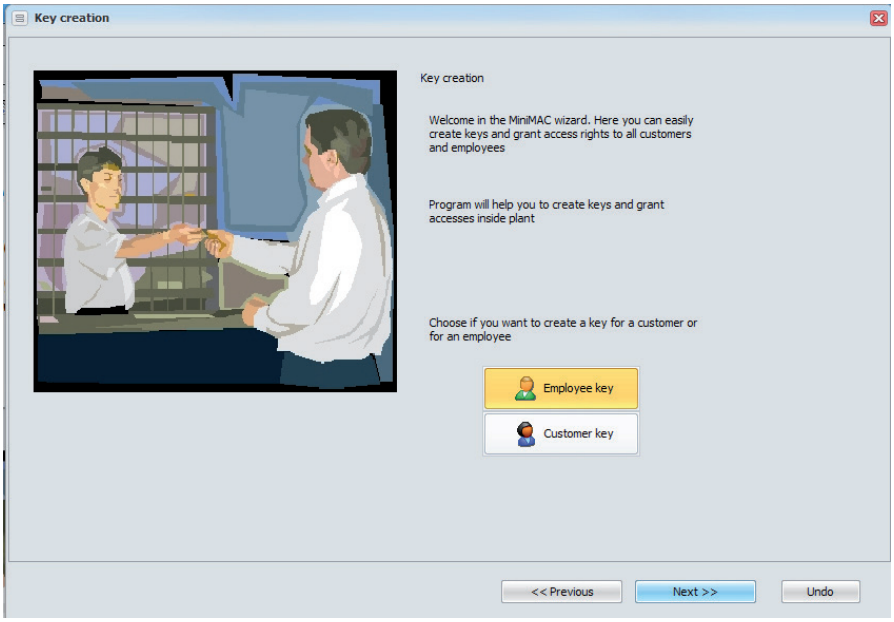




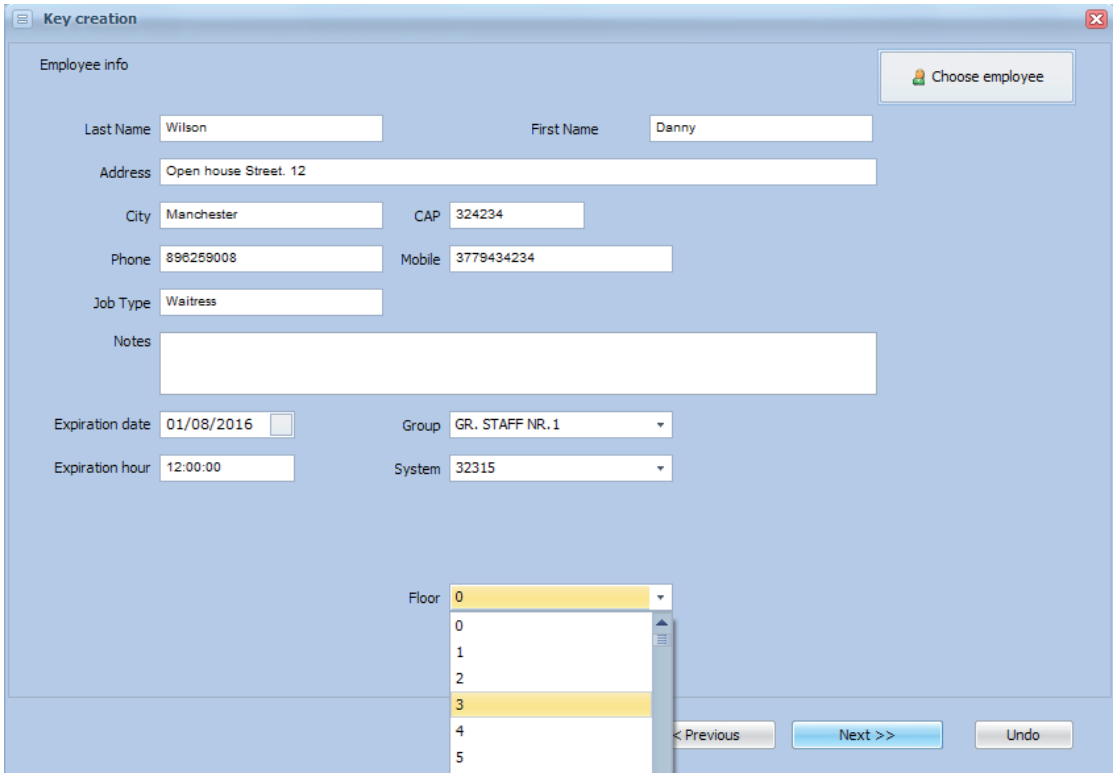
Last panel shows the residual credit in the TAG. According to the hotel administrator choice, it is possible to define the amount to be returned to the customer.

7.5 Service TAG management

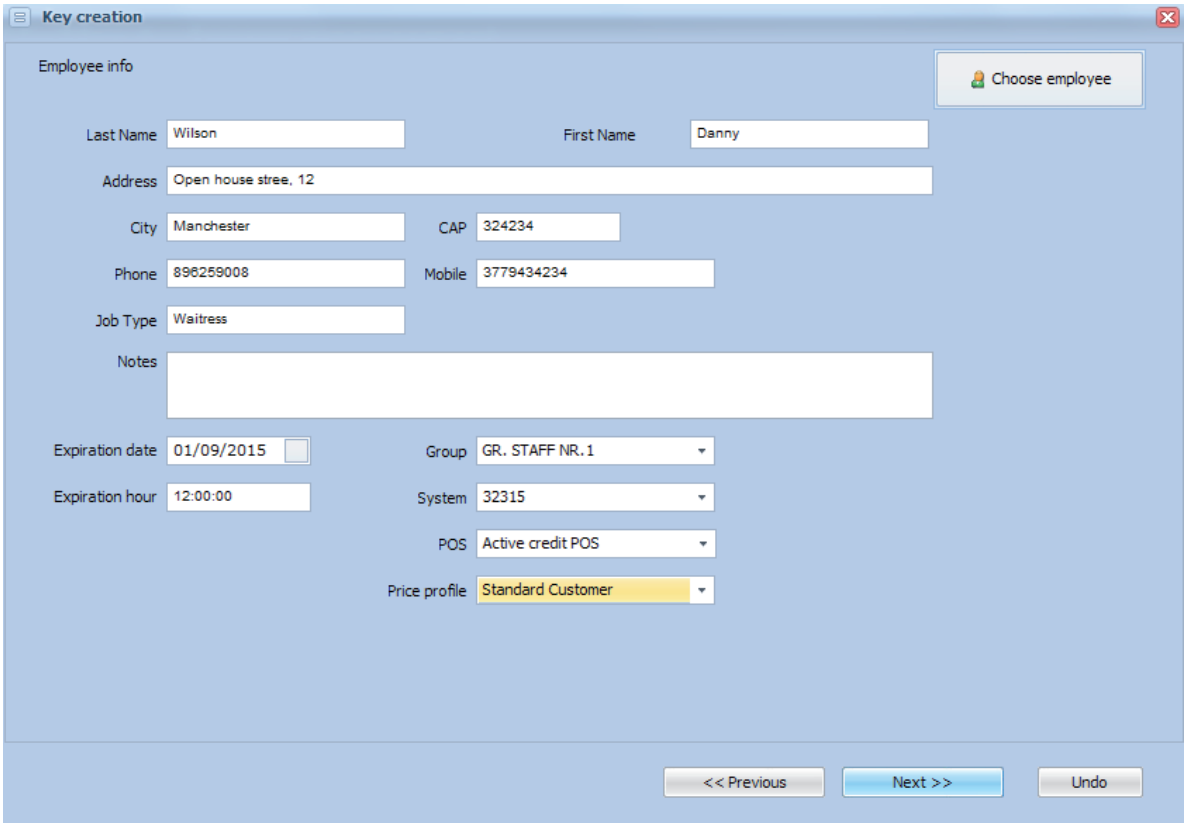
During check-in, and in general during the creation of TAGs, service personnel are usually provided with TAGs that are different from those handed over to guests.
To create a service TAG, click on "Staff TAG" button in the Check-in wizard.



In a installation where there aren't devices with virtual money function (i.e. LTP/U, transponder reader with POS function), window to be filled with check-in data does not include automatically POS parameters. It's possible to select the number of floor associated to the employee to store on the card (for example for hotel owners who want that every waitress is able to access with the elevator only one specific floor, the floor where he/she works).



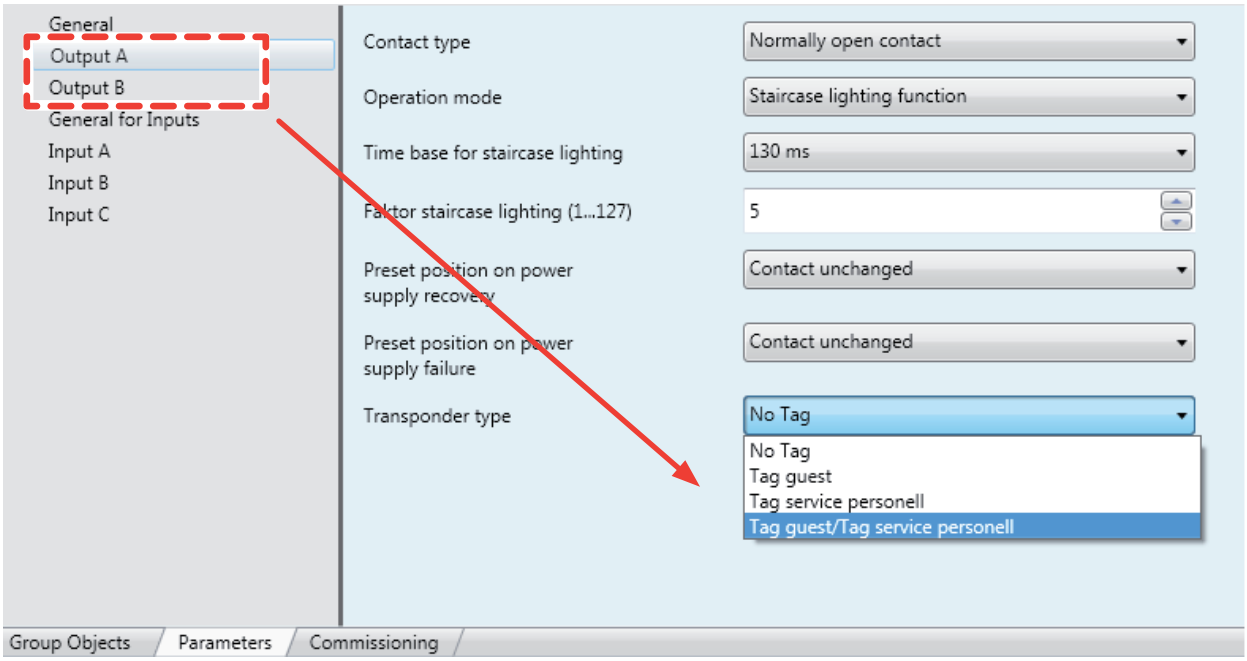
In a installation where there are devices with virtual money function window to be filled with check-in data automatically include POS parameters.



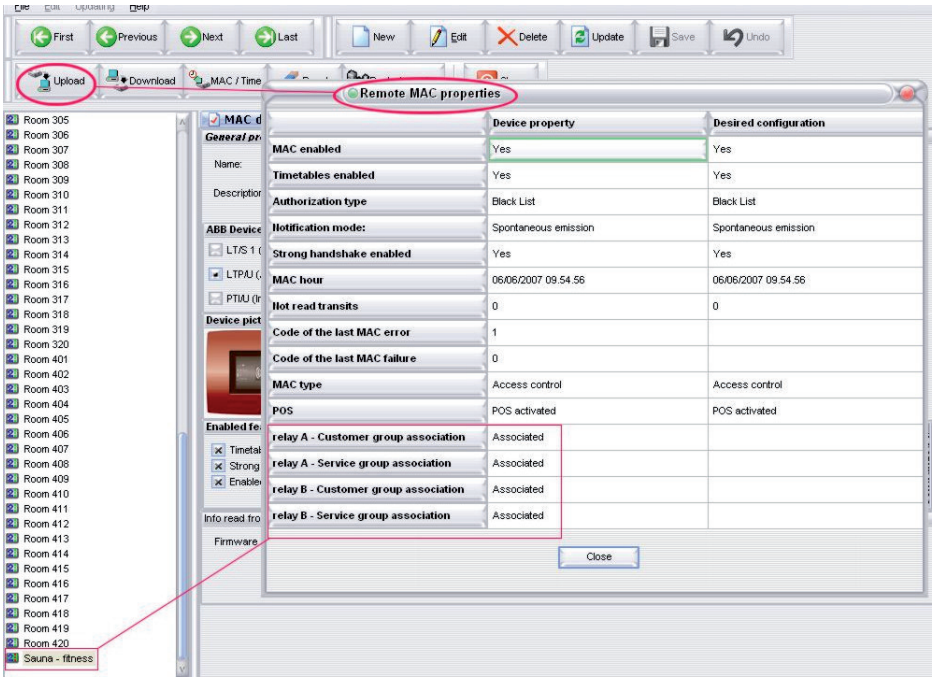
Warning
In an installation where there aren't devices with virtual money function (i.e. LTP/U, transponder reader with POS function), on card creation memory reserved on the card for storing data about credit, is instead used for saving data about number of floor associate to employee, as chosen in the check-in window. This data could be useful for integration of access control system with elevator systems.

Please notice that functionalities of ABB access control system does not include integration with elevator system. When and if required, this integration has to be realized by system integrator, for example using data about number of floor stored on the transponder card.

The difference of employee check-in operation compared with guest, is set during check-in or TAGs generation. Panel for service TAGs creation do not request the assignment of a room. Furthermore the box for the group assignment allows choosing between groups reserved to staff. Access rights can be assigned in the same way as customer TAGs.
Service TAGs (similarly to customer TAGs) can control one or both relays of transponders (or even none). Relays are assigned to TAG types by the system integrator, according to customer request, during the system configuration with KNX programming tool (see below ETS file for Chiara-Elos-Mylos devices).
Please notice that on Millenium and Tacteo transponder reader there is no differentiation between Service and Guest TAG: via ETS it's possible to define if the output channel (relay) is controlled according to TAG validation, no distinction between Service and Guest TAG.



For further information consult the device manuals.
MiniMAC gives you the possibility to check (not to edit) relays assignment performed via ETS from the SYSTEM menu. The association can only be displayed: modifications can be made only via ETS.
In System menu, select a device in the system and click UPLOAD:

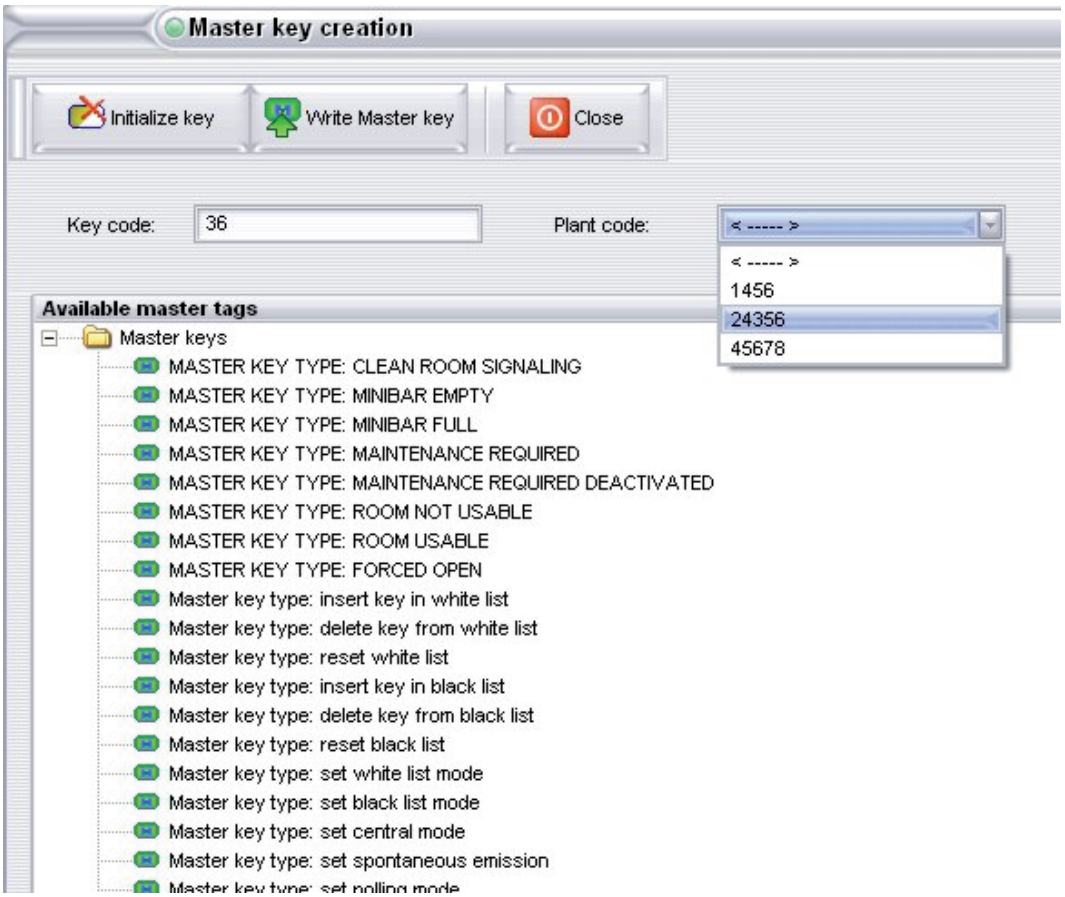


7.6 Master TAG management

MiniMAC can generate special TAGs called MASTER TAGs.
In an access control system for hotel applications, over the KNX bus, such TAGs are:

- **OPEN! Unconditioned**: such TAG does not ever expire and can get access everywhere as long as the system code in the TAG is recognised by the device.
- **Cleaned room**: special card that is used by service personnel to notify the direction that the room has been cleaned. Note: room status becomes 'dirty' when a CUSTOMER TAG is inserted in the transponder holder (PTI/U). Service TAGs (the TAGs that are handed over to service personnel) do not change room status.
- **Maintenance required/not required**: signals the need to fix problems in the room.
- **Minibar Empty/Full**: keeps track of minibar filling.
- **Usable/not usable room**: set room status as available/unavailable

For MASTER TAGS creation press MASTER TAG button in TAGS menu:

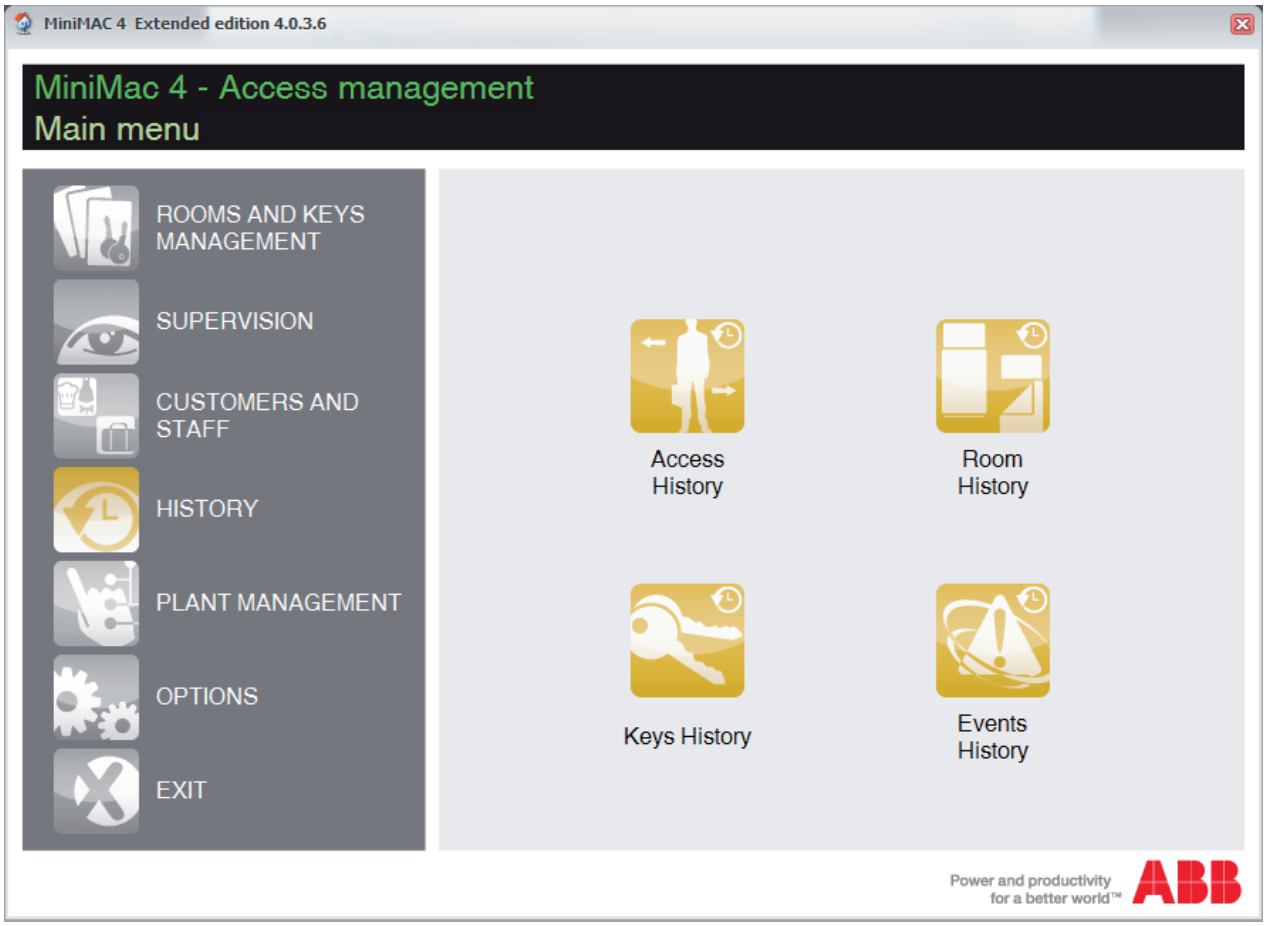


MASTER TAGS have to be used in the following way:
Insert the TAG in a transponder holder (PTI/U) or place it near the transponder as long as the second LED turns on in yellow.

Master TAGs are much more than those listed before. Other master TAGs are used for devices programming in a stand-alone mode. This last kind of operation is not recommended in a system based on KNX bus. See the procedure for system programming in stand-alone mode with master TAGs (***"2.7 Programming procedure through Master TAGs"***).

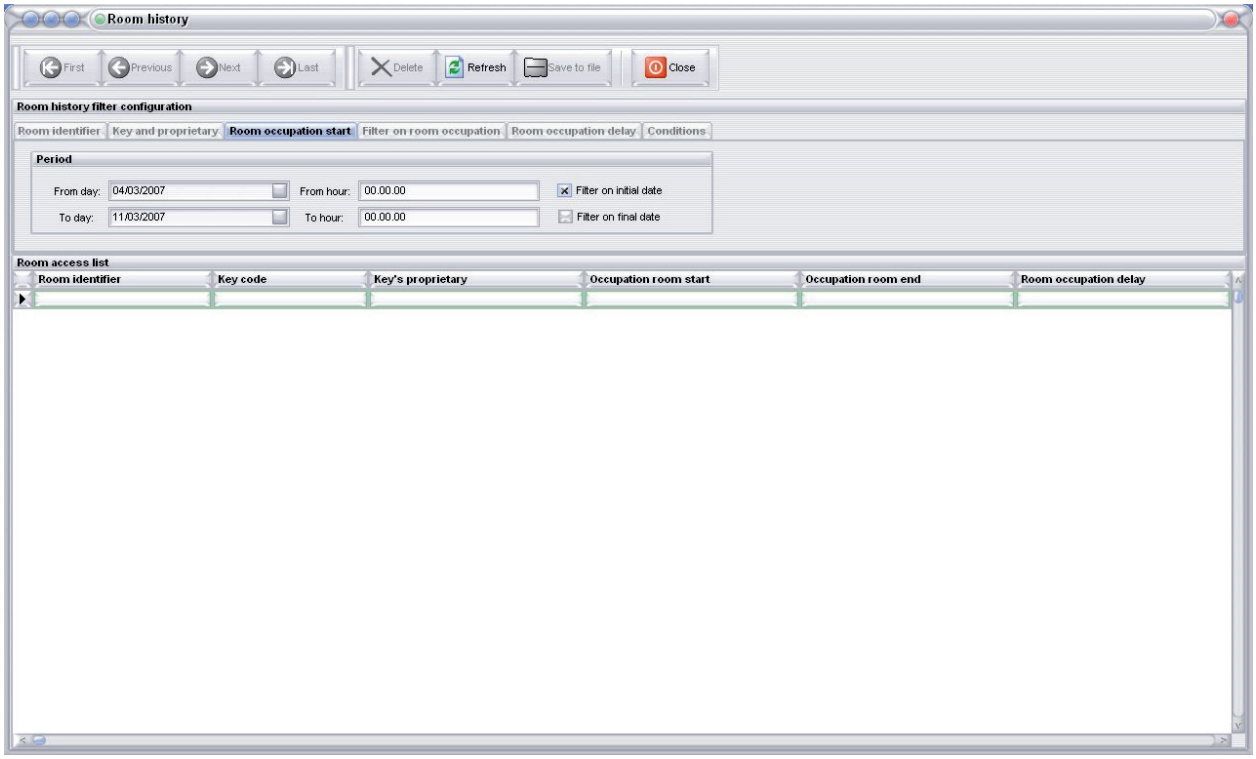
7.7 History management

MiniMAC offers you a powerful tool to control the use of the access control system, with an access history available for entrances, room presence, cards and events.

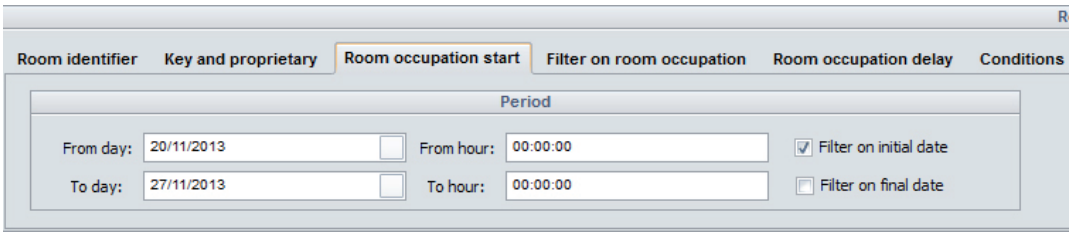


7.7.1 Presence history / room history

Thanks to this function you are able to view, for each room, time of entrance/exit, duration of stay and guest ID. Such function is available only if a PTI/U device (transponder holder) is installed in hotel rooms.



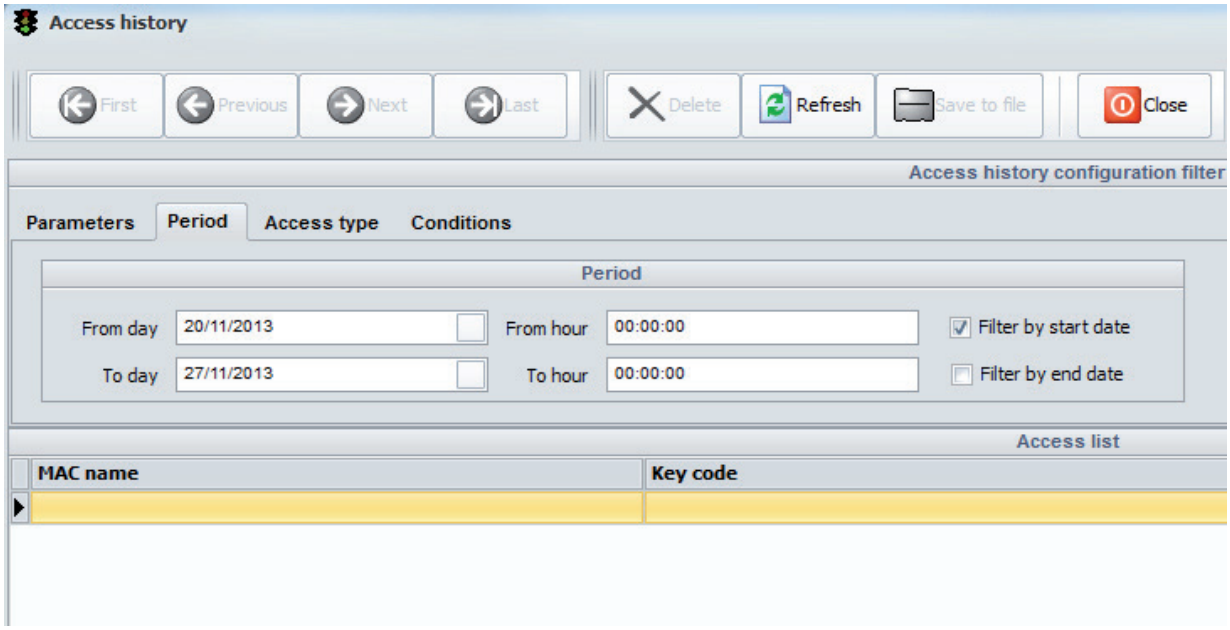
MiniMAC allows you to sort the data in the display list: click the header in bold at the top of the column that should be used as sorting criterion.
Furthermore, the available information may be filtered (so that it is possible to show only part of the information) setting the most suitable criterion for the search you wish to perform. Filters are listed and can be configured in the upper part of the table:



Also in this case data can be saved as an Excel file.

7.7.2 Access History

Since an access control system does not only consist of rooms, a transit history is available for all system devices. This way you can monitor when someone accessed a certain entrance.



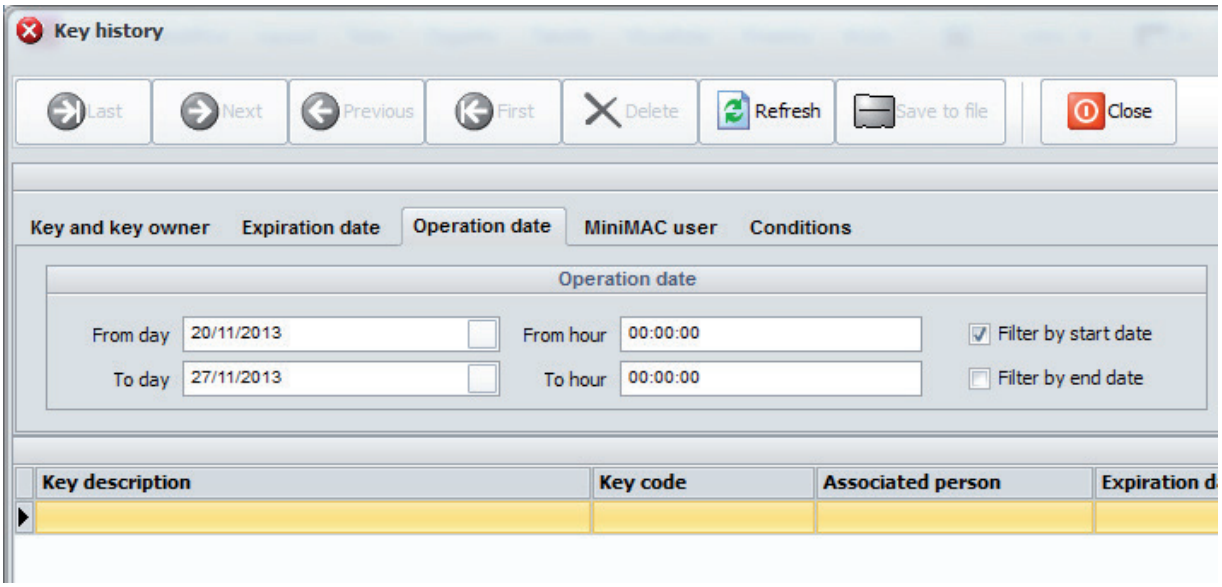
Also in this case it is possible to:

- Click the header at the top of any column to quickly sort the viewed list by that column (in ascending or descending order).
- Filter data to display a specific set.
- Data can be saved as Excel file for separate filing or printing.

7.7.3 TAGs History

For the system administrator it may be useful to know the details about creation and deletion of TAGs.
Many frauds/swindles by unfaithful staff assume the ability to hide the operations related to the assignment of TAGs and, consequently, of rooms.
MiniMAC keeps track of every operation on the TAGs in a history list.

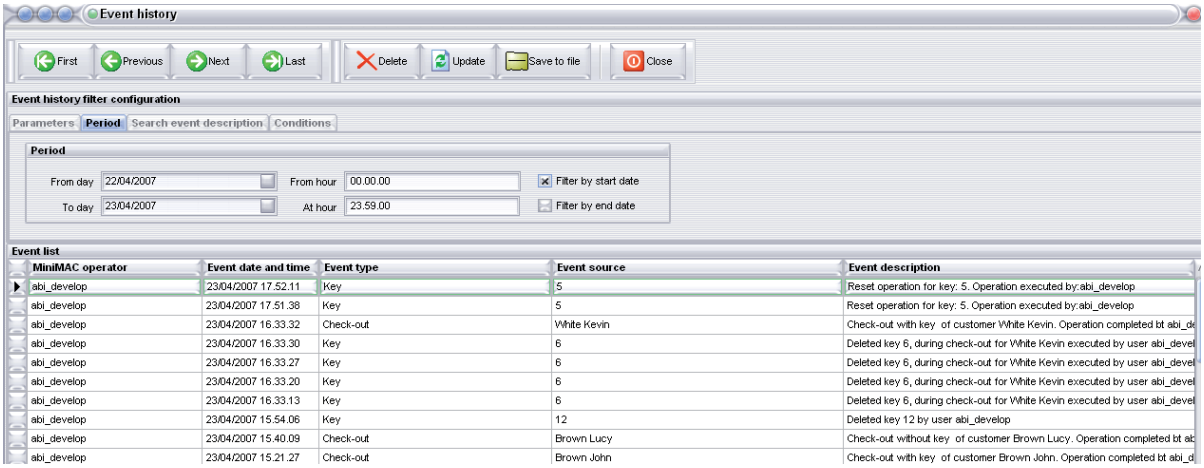
Also in this case it is possible to:



- Click the header at the top of any column to quickly sort the viewed list by that column (in ascending or descending order).
- Filter data to display a specific set.
- Data can be saved as Excel file for separate archiving or printing.

7.7.4 Event History

MiniMAC keeps track of every operation on the TAGs in the event history list. ALL operations performed on the system are stored in this history list. In case of need, the administrator can go back to:
operations made by MiniMAC operators
events captured by MiniMAC telegrams management service

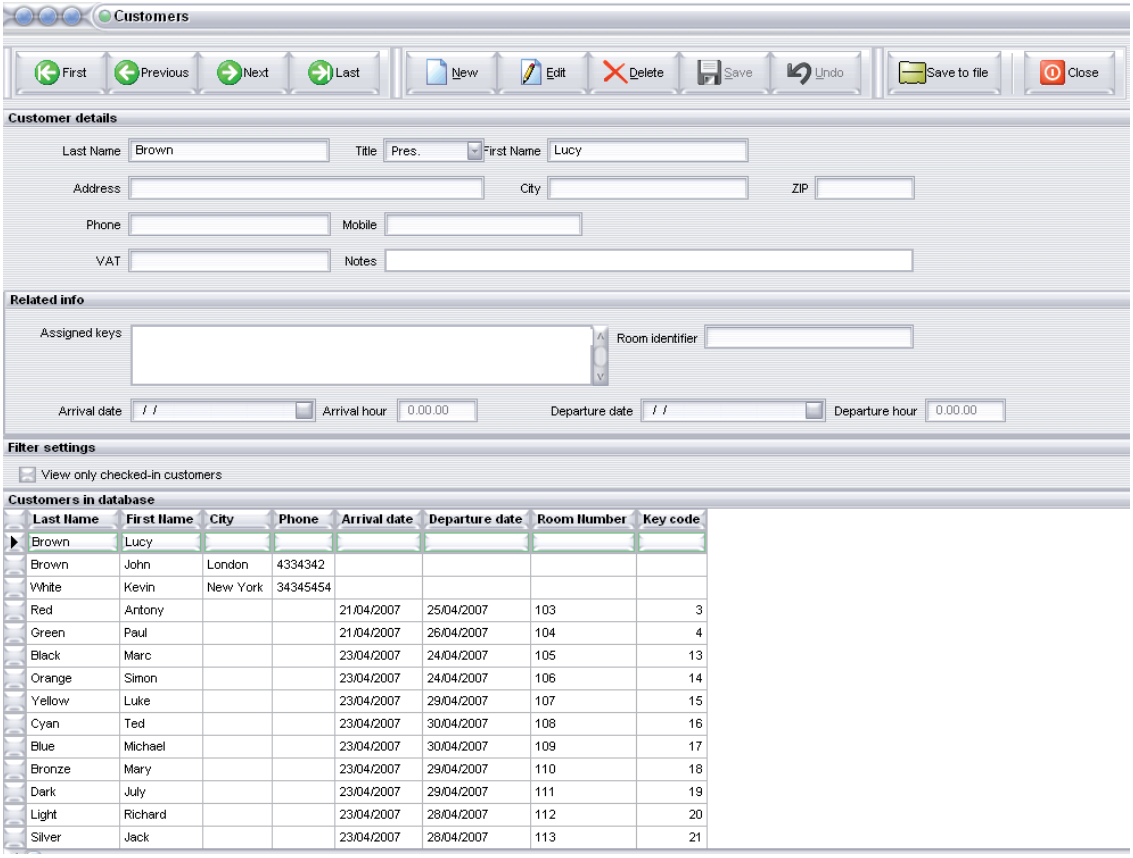


Also in this case it is possible to:

- Click the header at the top of any column to quickly sort the viewed list by that column (in ascending or descending order).
- Filter data to display a specific set.
- Data can be saved as Excel file for separate archiving or printing.

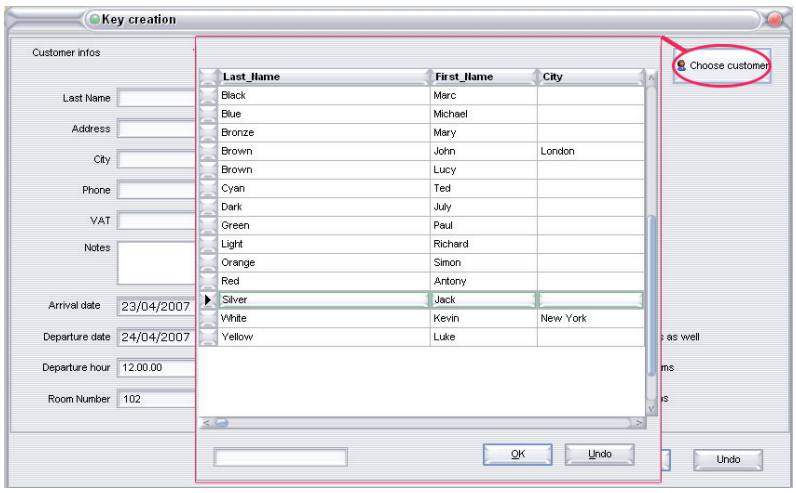
7.7.5 Customer personal data

MiniMAC records customers' personal data that can be used during their stay in the hotel and in the future as well.
Once inserted, such data are available any time they have to be consulted. If data are not useful, they can be removed from the list exporting them to an EXCEL file.

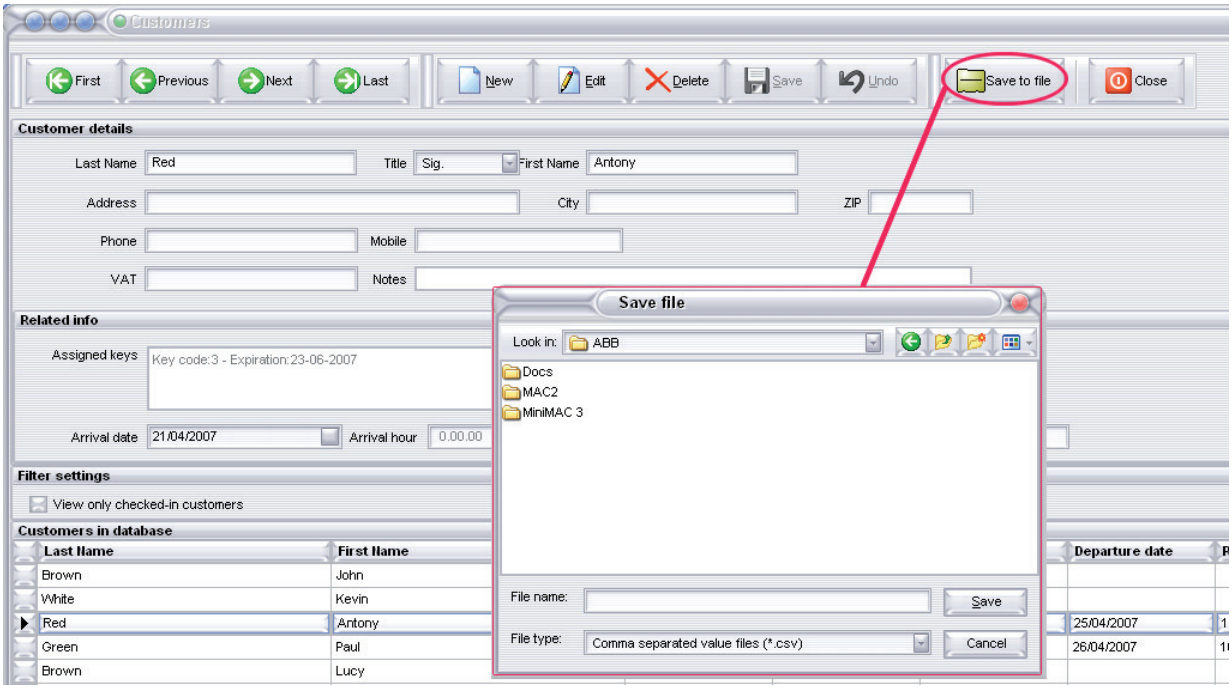


Last Name	First Name	City	Phone	Arrival date	Departure date	Room Number	Key code
Brown	Lucy						
Brown	John	London	4334342				
White	Kevin	New York	34345454				
Red	Antony			21/04/2007	25/04/2007	103	3
Green	Paul			21/04/2007	26/04/2007	104	4
Black	Marc			23/04/2007	24/04/2007	105	13
Orange	Simon			23/04/2007	24/04/2007	106	14
Yellow	Luke			23/04/2007	29/04/2007	107	15
Cyan	Ted			23/04/2007	30/04/2007	108	16
Blue	Michael			23/04/2007	30/04/2007	109	17
Bronze	Mary			23/04/2007	29/04/2007	110	18
Dark	July			23/04/2007	29/04/2007	111	19
Light	Richard			23/04/2007	28/04/2007	112	20
Silver	Jack			23/04/2007	28/04/2007	113	21

Personal data previously inserted in the database can be recalled during check-in so customer information is automatically filled in.



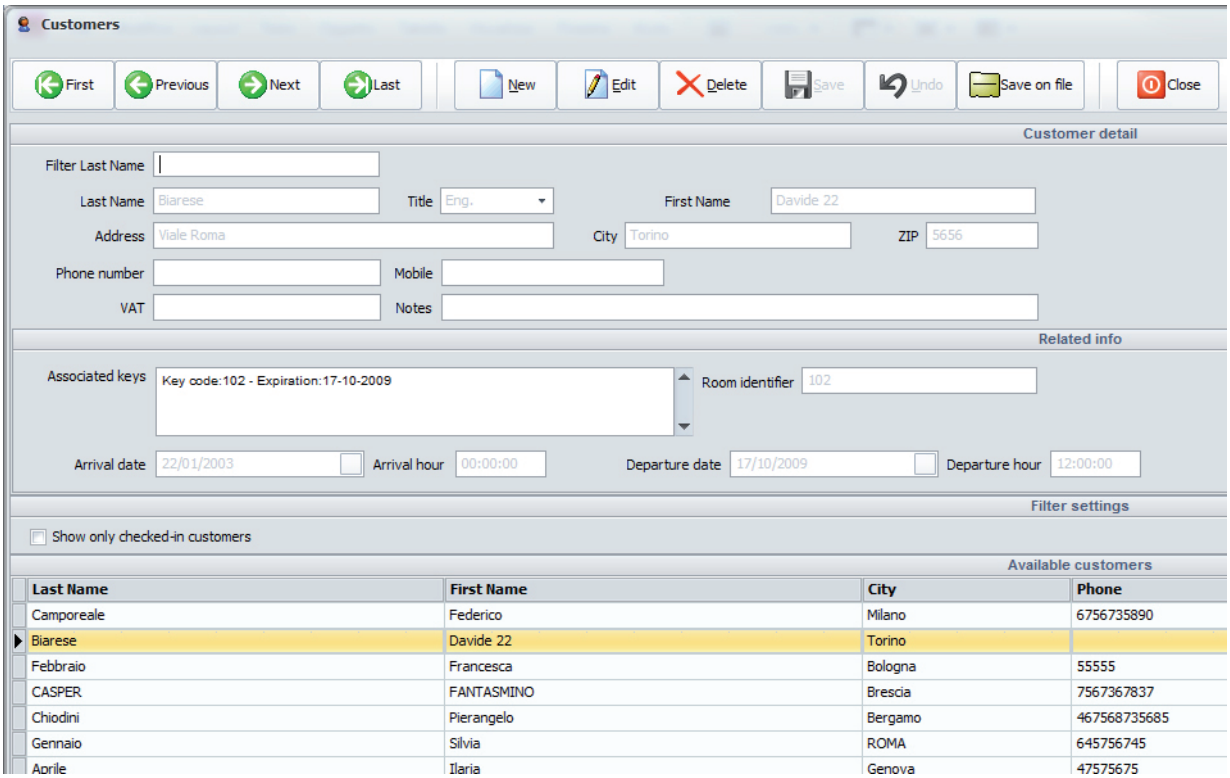
Personal data is kept stored even after customer check-out. Personal data can be saved in an EXCEL file and removed from the MiniMAC database.



A1 | Last Name

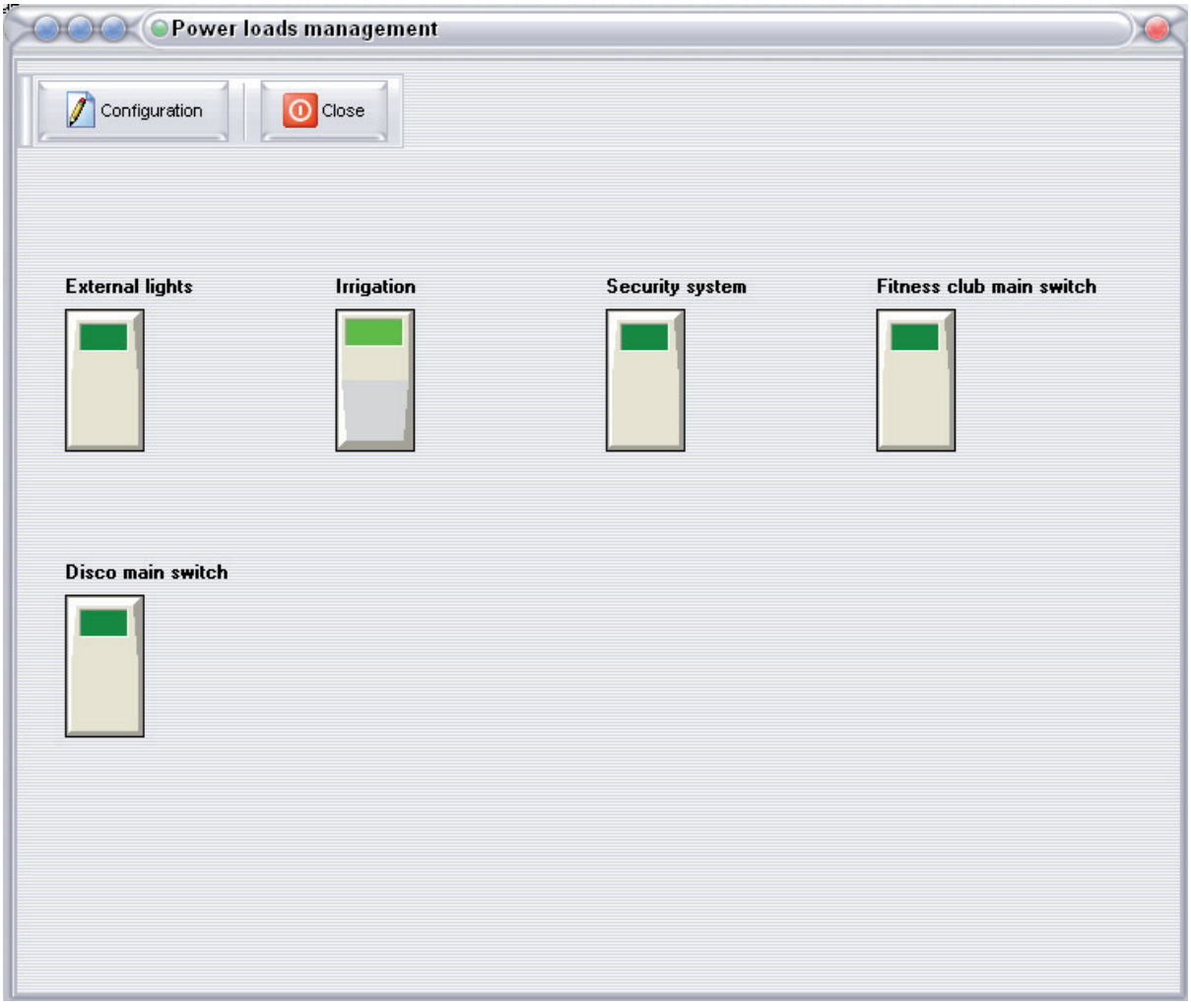
	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Last Name	First Name	Address	City	CAP	Phone	Mobile	VAT	Notes	Arrival Date	Departure Date	Room	Key code
2	Brown	John	Street of Lemon Trees	London	124343	4334342	343434	34343432					
3	White	Kevin	Street of Cangaroos	New York	23342323	34345454	6,57E+08	65454					
4	Red	Antony								21/04/2007	25/04/2007	103	3
5	Green	Paul								21/04/2007	26/04/2007	104	4
6	Brown	Lucy											
7	Black	Marc								23/04/2007	24/04/2007	105	13
8	Orange	Simon								23/04/2007	24/04/2007	106	14
9	Yellow	Luke								23/04/2007	29/04/2007	107	15
10	Cyan	Ted								23/04/2007	30/04/2007	108	16
11	Blue	Michael								23/04/2007	30/04/2007	109	17
12	Bronze	Mary								23/04/2007	29/04/2007	110	18
13	Dark	July								23/04/2007	29/04/2007	111	19
14	Light	Richard								23/04/2007	28/04/2007	112	20
15	Silver	Jack								23/04/2007	28/04/2007	113	21
16													

Management of service staff personal data is identical to that of customers.



7.8 Loads management

MiniMAC has a panel that allows you to control the electrical devices present inside the system.
By means of the light buttons present on the Loads Management MiniMAC screen, it is possible to activate/deactivate the loads previously configured by the installer while performing software configuration.

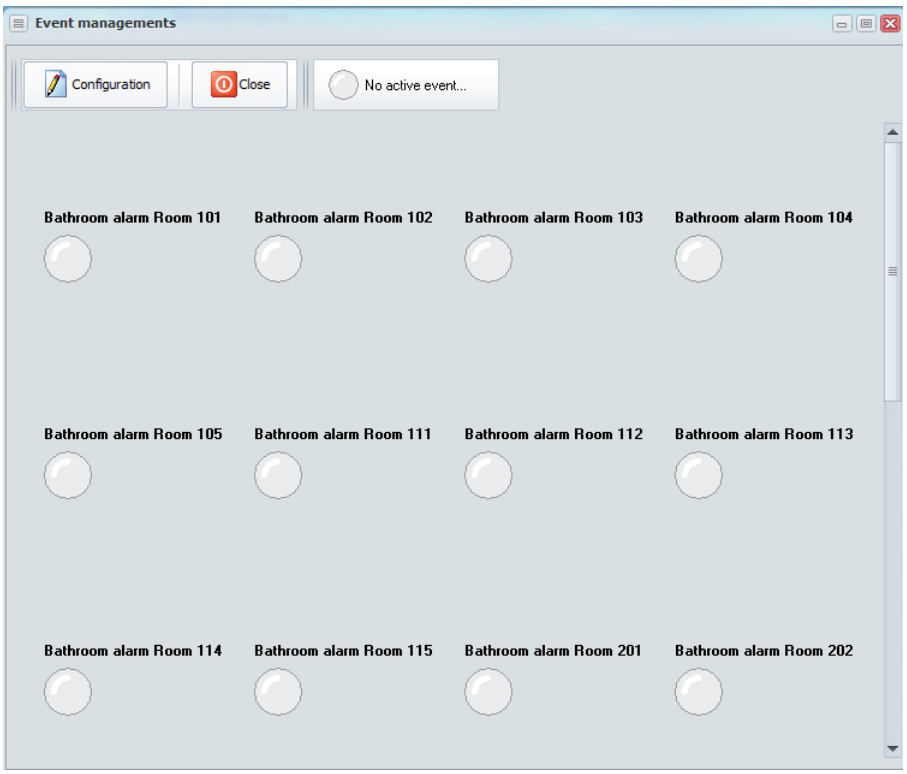


7.9 System Events Management

MiniMAC gives you the possibility of associating light indicators with the system events that need to be monitored. Each indicator is assigned to a particular event detected through KNX bus.

We remind you that the association of an indicator with an event that concerns the health and safety of a person **requires careful evaluation**, since the type of communication via bus, although highly reliable, cannot ensure the total absence of errors or delay in signalling.
You are therefore recommended to make redundant the possible connections of the type described above using specific Hardware signalling devices.

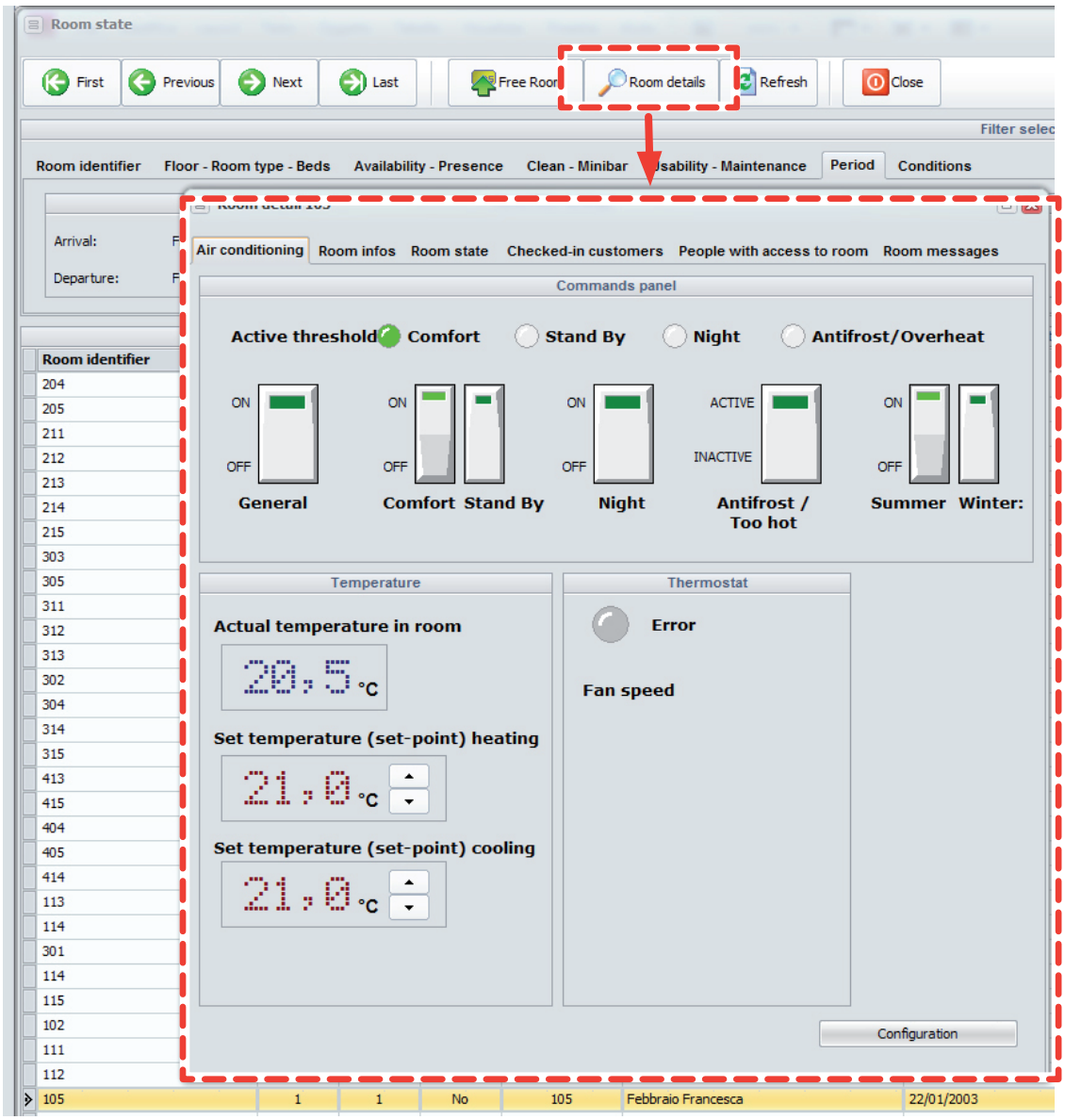
Warning
ABB cannot be responsible for any harm to people or damage to properties caused by an improper use of the bus event signalling.



The activation of an indicator can be accompanied by an acoustic signal and by the automatic opening of the panel above each window that could be open on the user computer monitor at that moment.

7.10 Heating and Cooling management

MiniMAC can control heating and cooling devices installed in the rooms.



From the room Heating and Cooling control panel it is possible to display the room status and edit air-conditioning parameters.

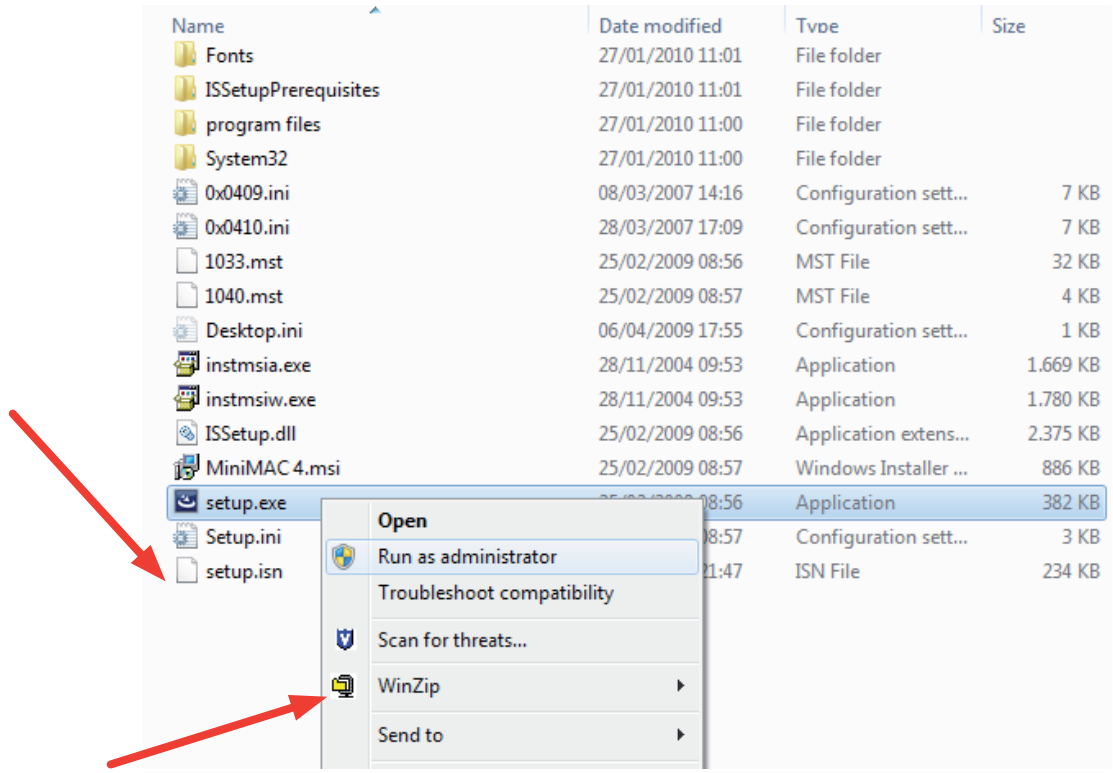
7.11 Other installations

In all cases where ABB access control is used for other applications (car parks, wellness and fitness centres, offices, laboratories, etc.), the MiniMAC software can be duly configured to work in this type of contexts. The management of other installations is the same as that for hotel installation: the functions are exactly the same as those already described, expect for the ones that are specific for a hotel installation, which will not be present (check-in/check-out, room management, etc.).

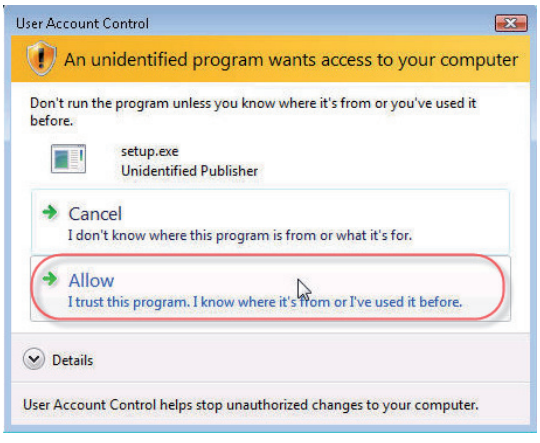
8 Uninstalling

8.1 Uninstalling the software from the PC

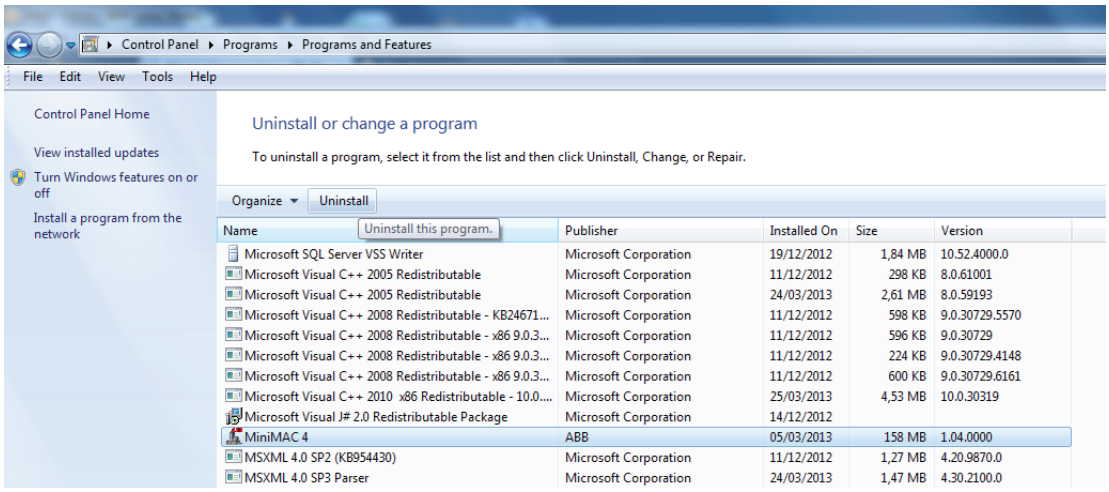
Look in the MiniMAC CD ROM for the ‘ABB Installation/MiniMAC4.1.x.x’ folder (where x.x indicates the version).
Start the set-up launching the “Run-as-administration” option. Right click with the mouse on setup.exe:

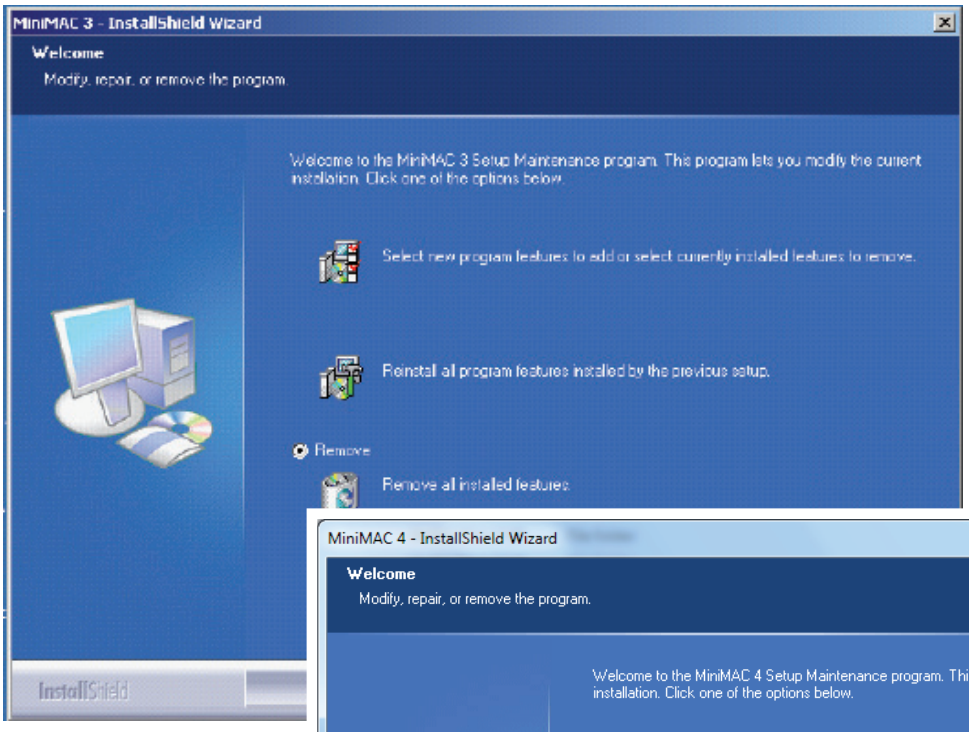


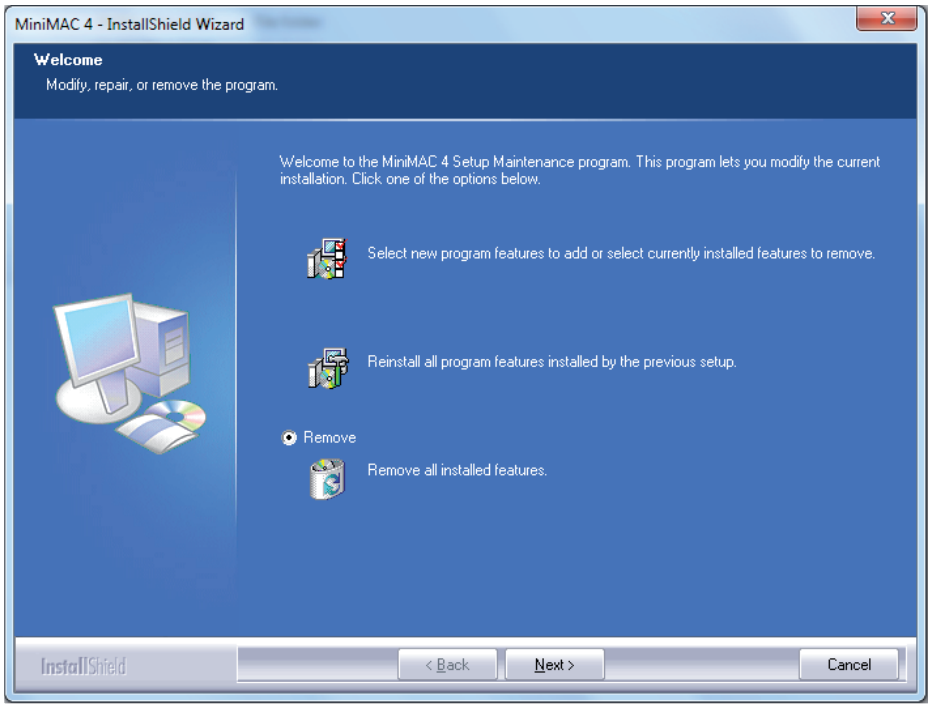
Some operating systems (in particular Windows Vista, for example) could have a confirmation panel: to proceed with uninstalling, choose the option to run the program (“Allow”).



Alternatively, you can uninstall the MiniMAC software from the Windows Control Panel.







Notes

Notes

ABB SACE
A division of ABB S.p.A.
Wiring accessories, Home & Building automation
Viale dell'Industria, 18
20010 Vittuone (MI), Italy
Tel.: +39 02 9034 1
Fax: +39 02 9034 7609

www.abb.com/knx
ABB Access Control solution
ABB offer for Hotels

User manual 2CSN600047D0201 | 30.03.2020