ABB Access Control

MiniMAC

System management and configuration software

1 Software installation

1.1 Minimum system requirements

Operating system:	Windows XP, Windows 7, Windows 8.1, Windows 10
Memory:	1 GByte
Fixed disk capacity:	150 GBytes available.

1.2 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:

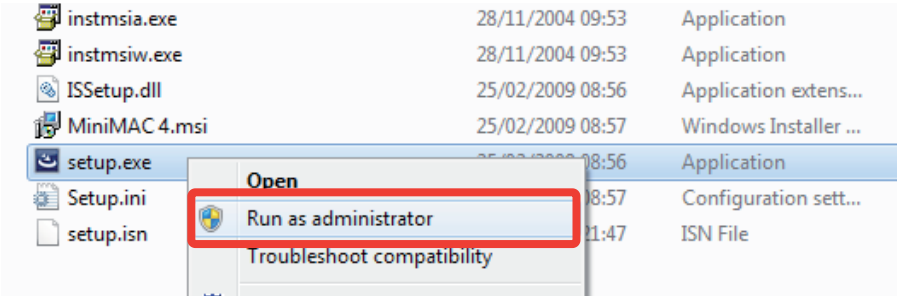
- 6501/TCP
- 6543/TCP
- 8100/TCP
- 9000/TCP

1.3 MiniMAC Installation procedure

1. Close all running programs
2. Search for the 'ABB Installation/MiniMAC'
3. Search for the setup.exe file

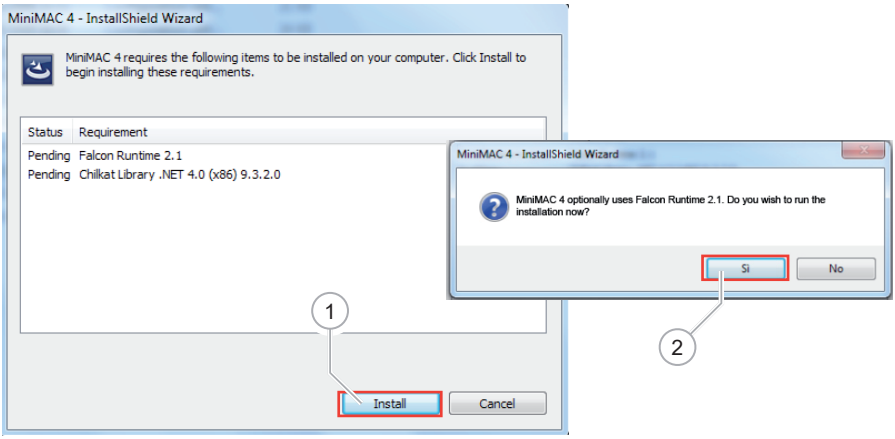
Warning
Make sure that you have Administrator credentials since software installation cannot be performed by a normal user. If you do not have Administrator rights, run the set-up via the option **Run as Administrator**. Right click with the mouse on the file called '**setup.exe**'.

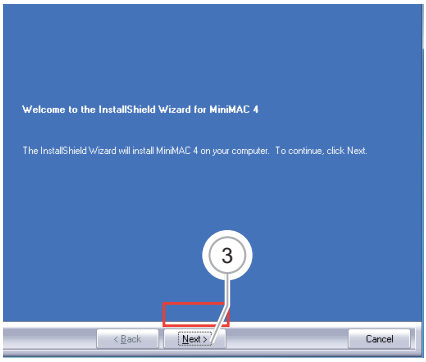
If the icon for confirmation is displayed, choose the option "Allow, I trust this program".

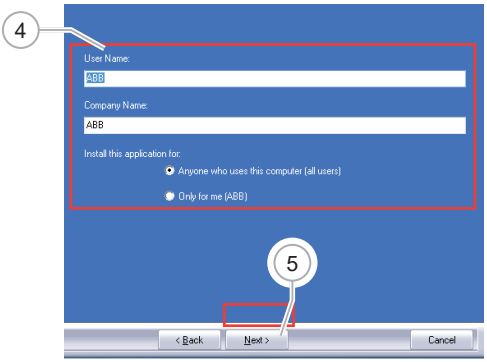


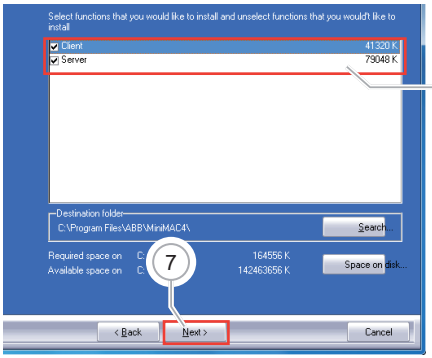
Proceed accepting the installation of Falcon library.
Select the technology (**8**) for the connection to the bus.

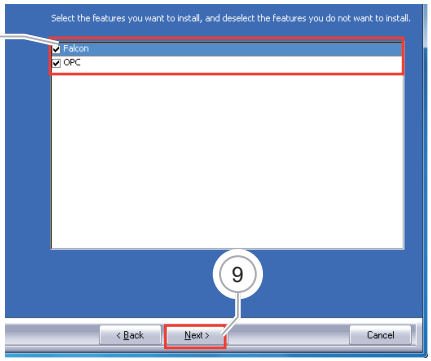
- If you choose the connection to MiniMAC bus via an OPC server, an OPC Server together with a valid licence must be installed.
- If you choose the connection to MiniMAC bus via Falcon libraries (reccomended) no additional software is required, but it's recommended to install Falcon Runtime if not yet installed (2).









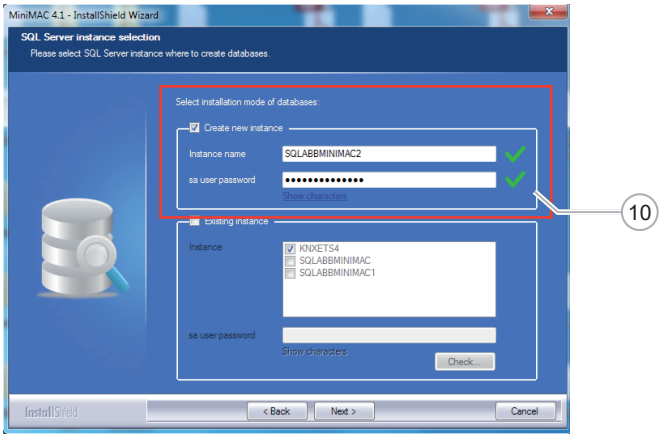


The MiniMAC installation wizard proceeds with the installation of the Microsoft SQL 2014 database.
If Microsoft SQL Server 2014 had been previously installed on the PC, the MiniMAC database will be installed using the Microsoft SQL Server 2014 that is already present: MiniMAC Database is created using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

- username = minimac
- password = ABB029034sace#

It is recommended to create a new instance of database (**10**). 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 two MiniMAC tools: MACWizardServer and MacWizardClient

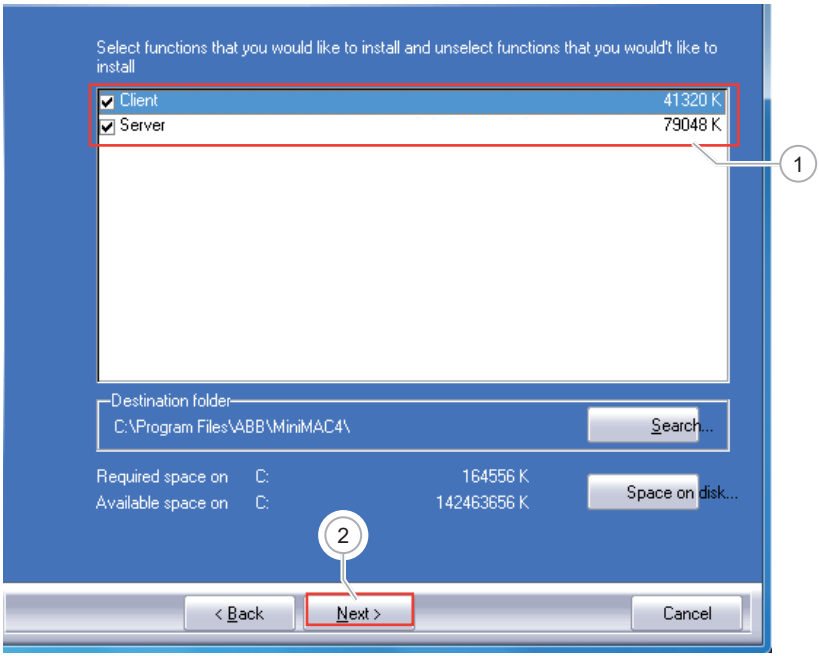


1.4 Client-server architecture

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

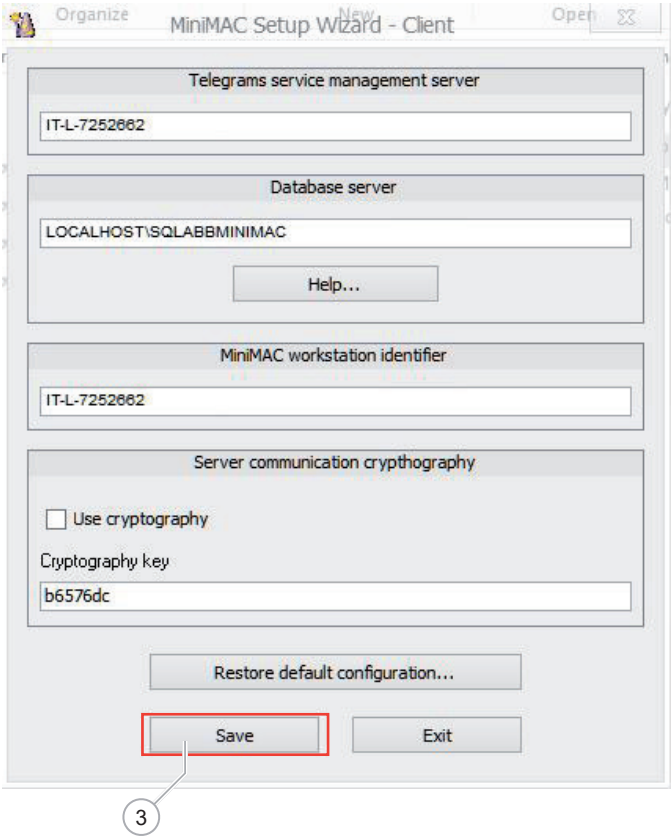
- Install both the MiniMAC client and server on the same PC
- Install only a MiniMAC server installation on one PC and several client installations on one or more separate PCs.
- Install a MiniMAC server+client installation on one PC and several client installations on one or more separate PCs.

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 distributed card programmer devices in the access control installation, and to have access to the information on access control system management and its control (i.e. heating and cooling supervision, events management, loads management, history, etc.) on different positions.



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.

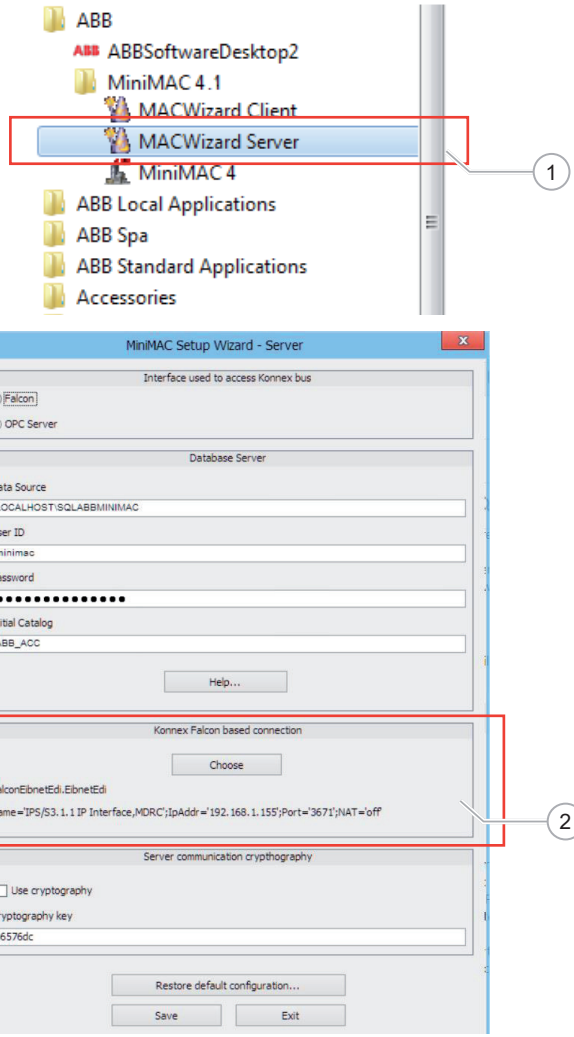


1.5 Configuration of the KNX bus interface

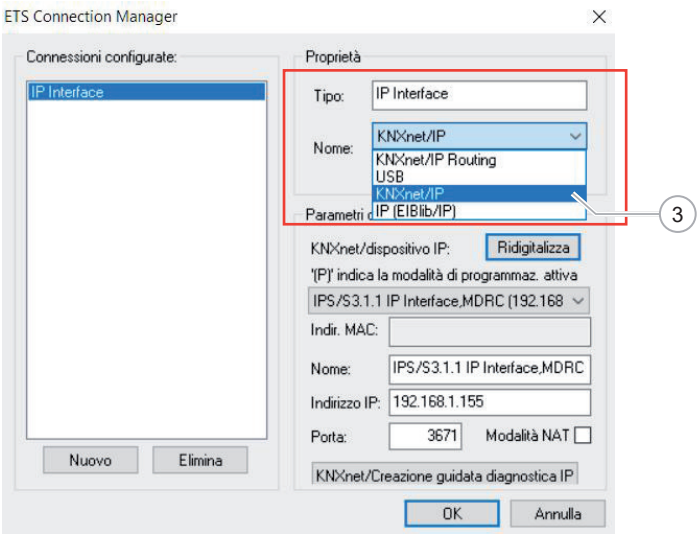
For connecting MiniMAC 4.1 with KNX bus a KNX interface is required.

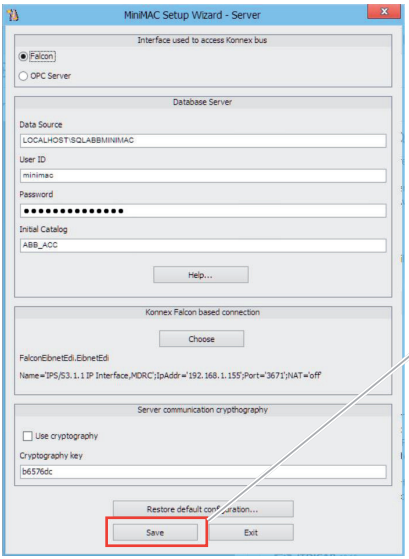
Warning
We recommend to us only IP interface for connecting MiniMAC PC to the KNX bus.
USB interface it is not supported by MiniMAC software for connection to the KNX bus.

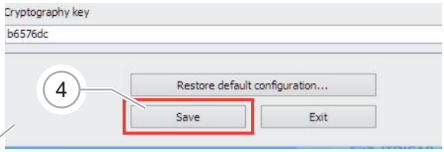
For configuring MiniMAC interface with KNX bus, run MACWizard Server program from the Programs-ABB-MiniMAC 4.1 folder.



It is now possible to select the desired KNX connection (IP interface is recommended), through standard ETS connection manager window (**3**) and then click the Save button (**4**).







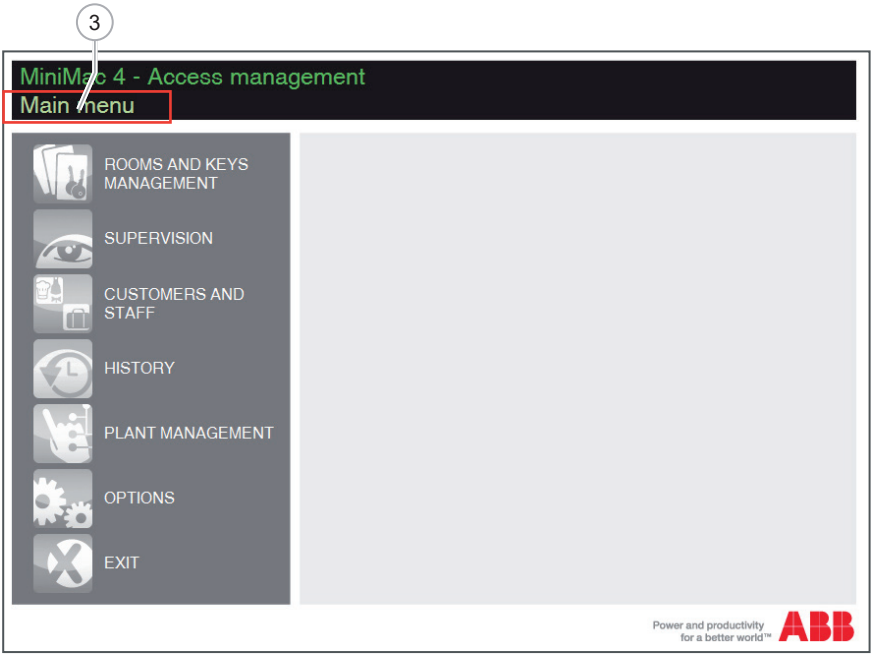
Remember that in case of client-server installations, it is possible to encrypt the communication between client and server. In order to configure the encryption, it is necessary to select the box “Use cryptography” and insert in the box “Cryptography key” the same key inserted in the correspondent box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

2 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.

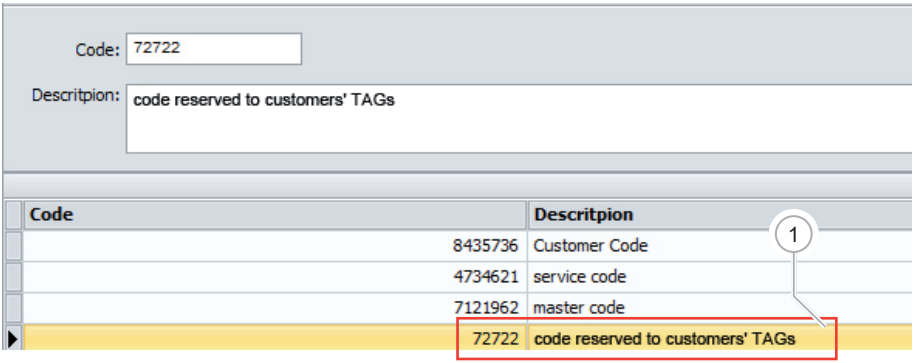


2.1 Creation of system codes

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 the creation of at least THREE types of system codes:

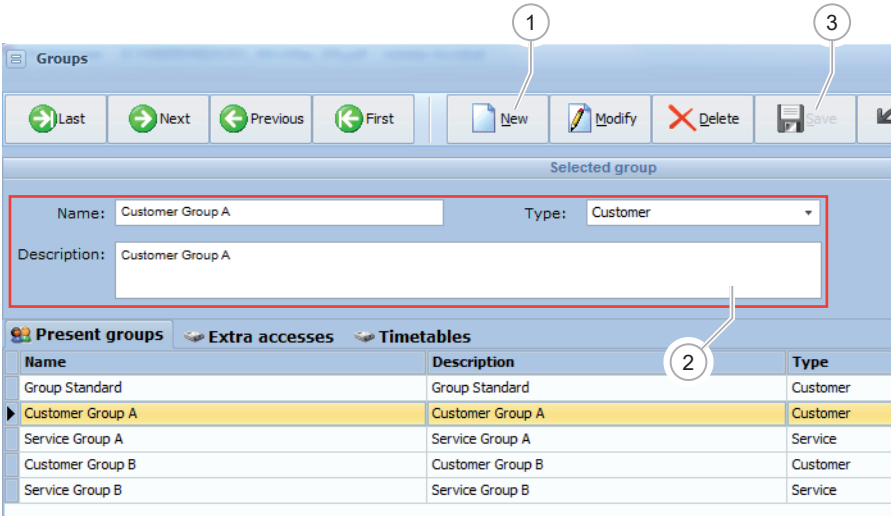
- A code reserved to master TAGs
- A code reserved to service TAGs
- A code reserved to customers TAGs



2.2 Creating groups

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

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

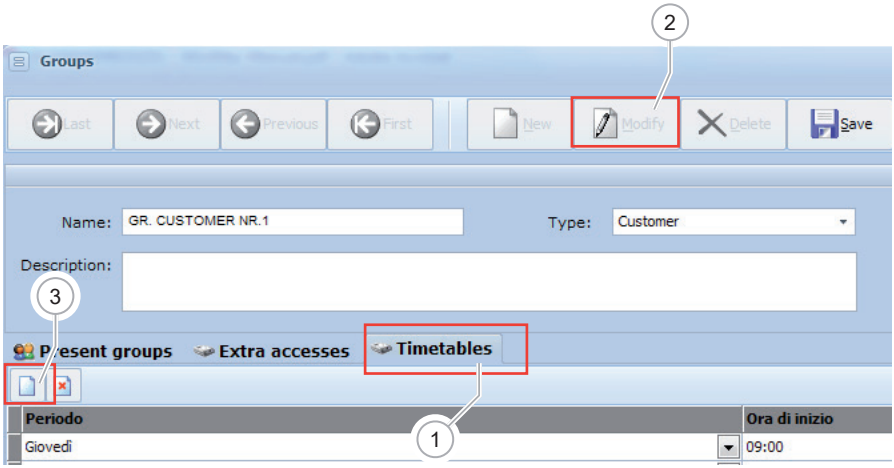


2.2.1 Timetables

If you do not wish to use timetables, simply leave the group with no timetables. However timetables must not be activated in the devices: a group without timetables is a group without authorization for the device in which timetables are enabled.

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



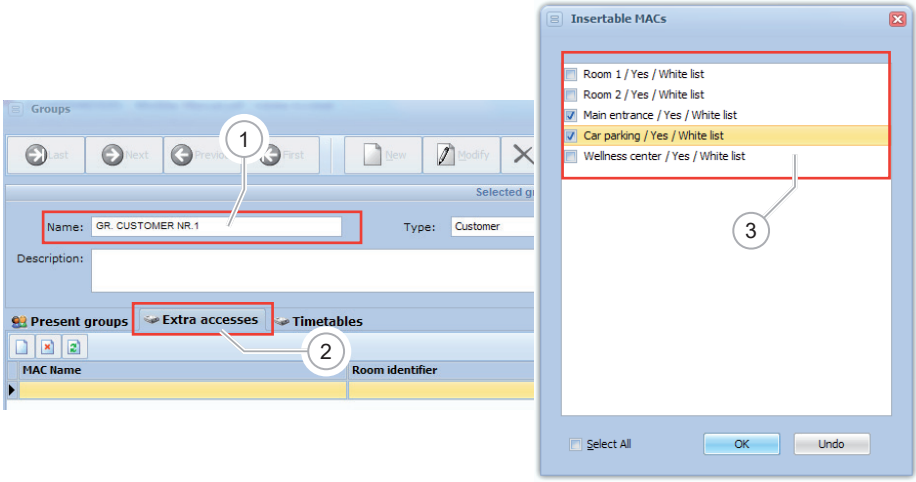
2.2.2 Extra accesses

The concept of “Extra accesses” bases on the fact that a hotel has several rooms and common areas.
Assuming for example 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 devices, when you create a card you grant automatically access at these gates to all users belonging to these groups.



2.3 System Design

Access Control system is created and configured using the PLANT submenu, in the System Management menu.

2.3.1 Comunication between MiniMAC and access control devices

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	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/dov			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

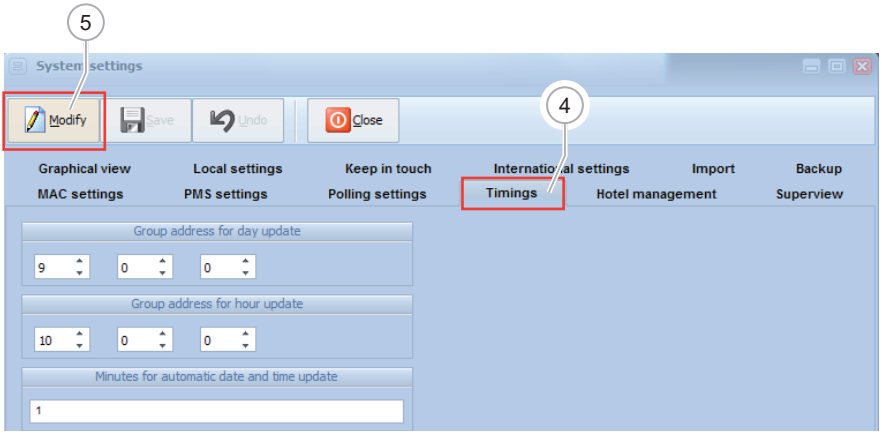
ETS communication objects (Chiara, Elos, Mylos devices)

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

ETS communication objects (Millenium devices)

Number	Name	Object Function	Description	Group Addres	Length	C	R	W	T	U	Data Type	Priority
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 devices)



2.3.2 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)

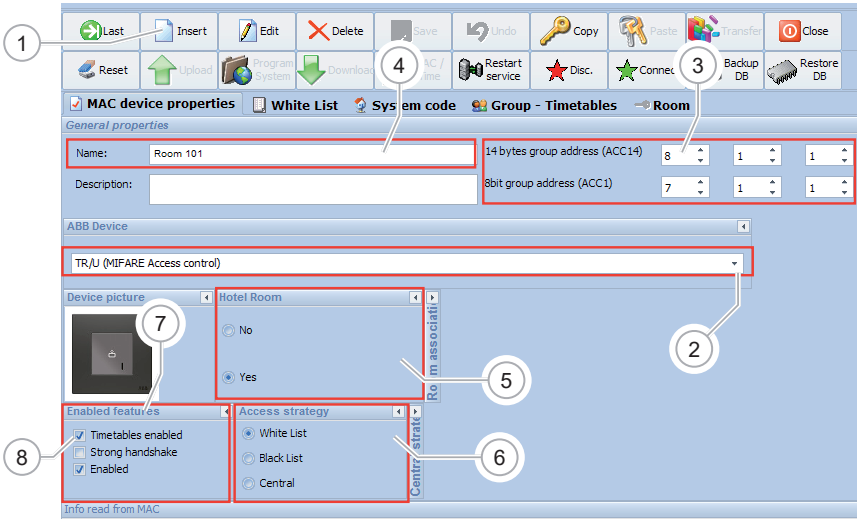
This means that every Room must have a transponder reader associated to it, while you could have installations where rooms have not card holder installed inside.

2.3.2.1 Transponder Reader

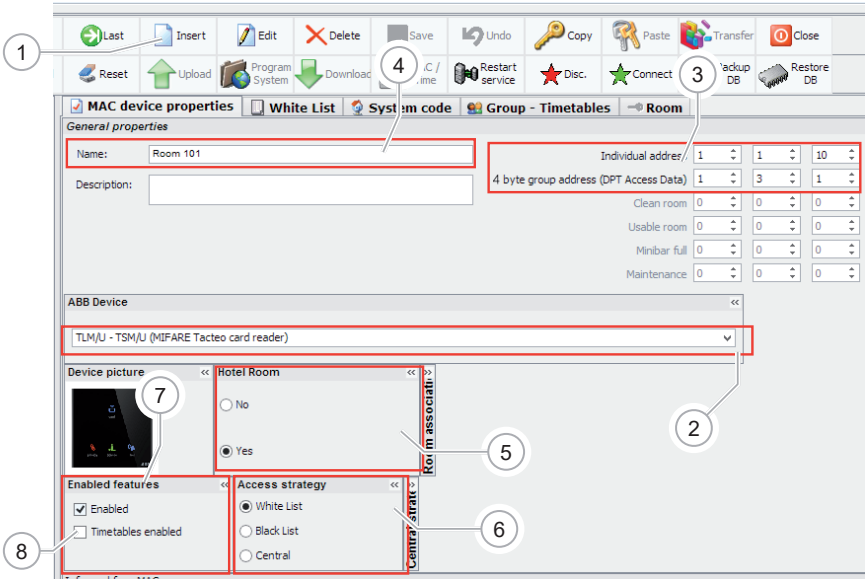
1. Click on INSERT from the main toolbar
2. Select by the menu drop-down the type of transponder reader:
   - TR/U for Millenium
   - LT/U for Chiara-Mylos-Elos
   - TLM/U - TSM/U for Tacteo
3. Configure the communication between MiniMAC and device specifying group address “ACC1, ACC14” for Chiara-Mylos 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
4. Insert Name (and Descriprion, optional) of device
5. Specify Hotel Room = Yes
6. Configure Access Strategy: the recommendation for transponder reader related to Hotel Room is White List
7. Configure the device as “Enabled”
8. Enable Timetables if requested.

Note

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.



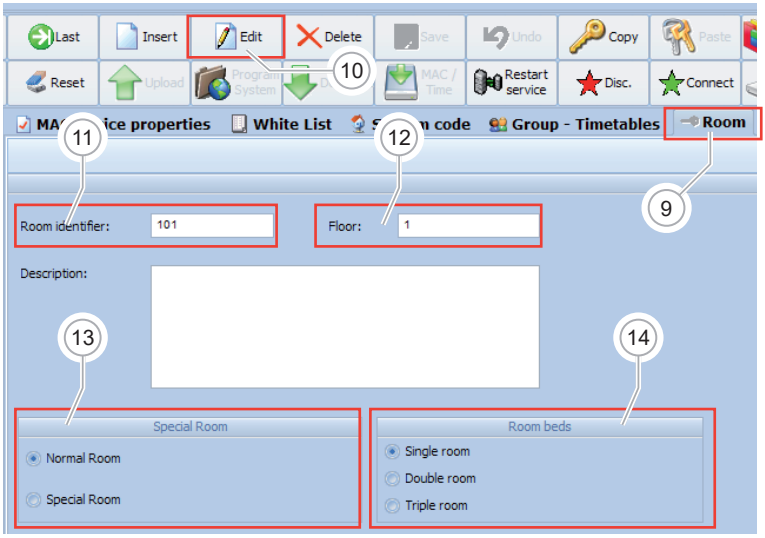
Device configuration (Chiara-Mylos and Millenium devices)



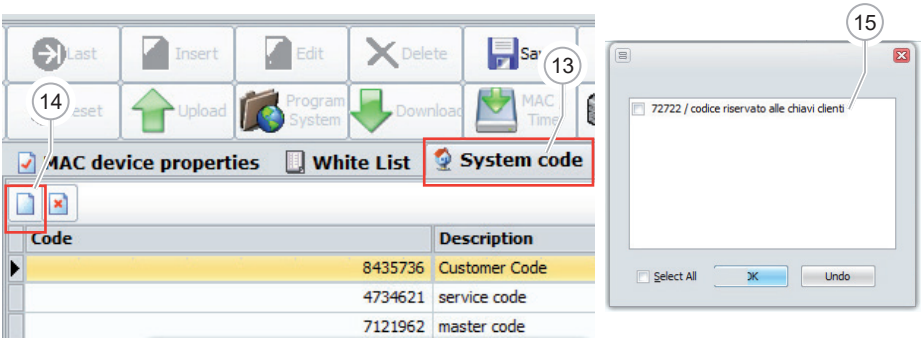
Device configuration (Tacteo devices)

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

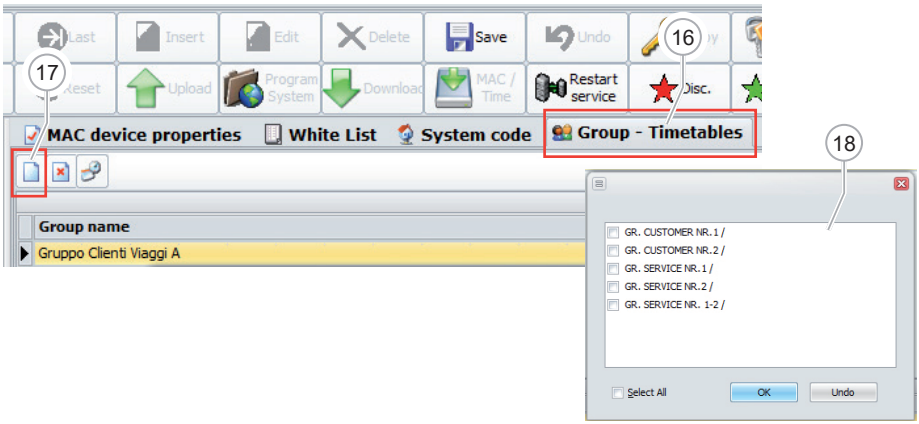
- room number
- floor
- type of room



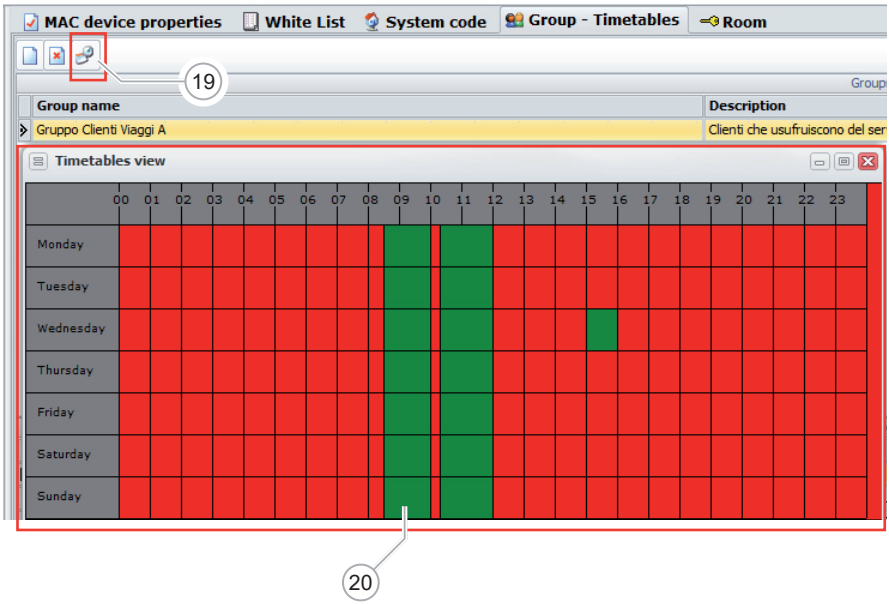
After the requested information is entered, system CODES must be associated with the device. The device will grant the passage only to the TAGs with one of the system codes contained in the list that is filled in in the "System code" TAB.



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



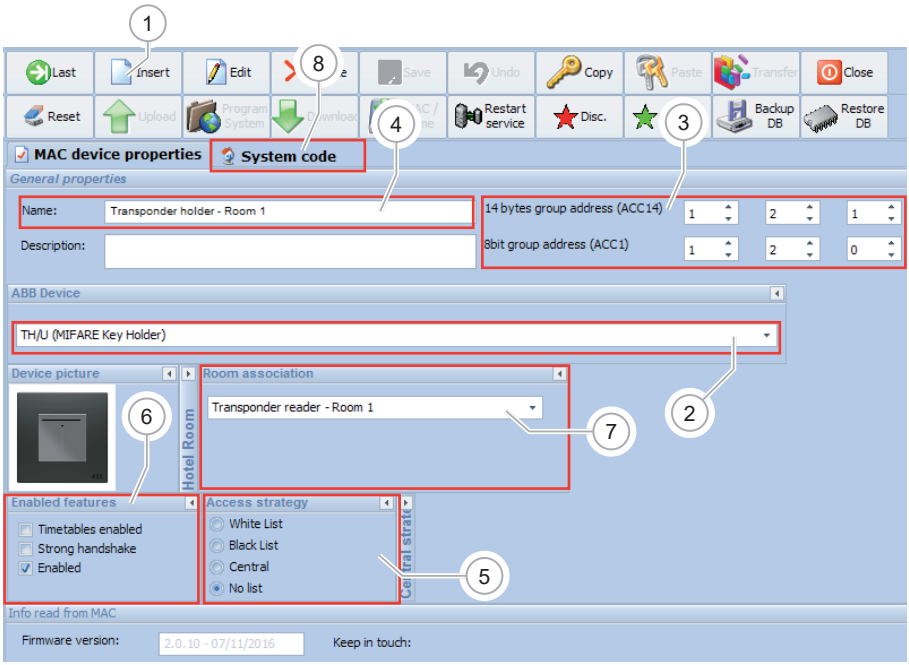
If you click on the dedicated button (“View Timetables”) you see for every group the timetables configured, if configured. In the example below As you can see, the green area is reserved to the room cleaning service staff which has a set of TAGs part of this group and can enter the room only in that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



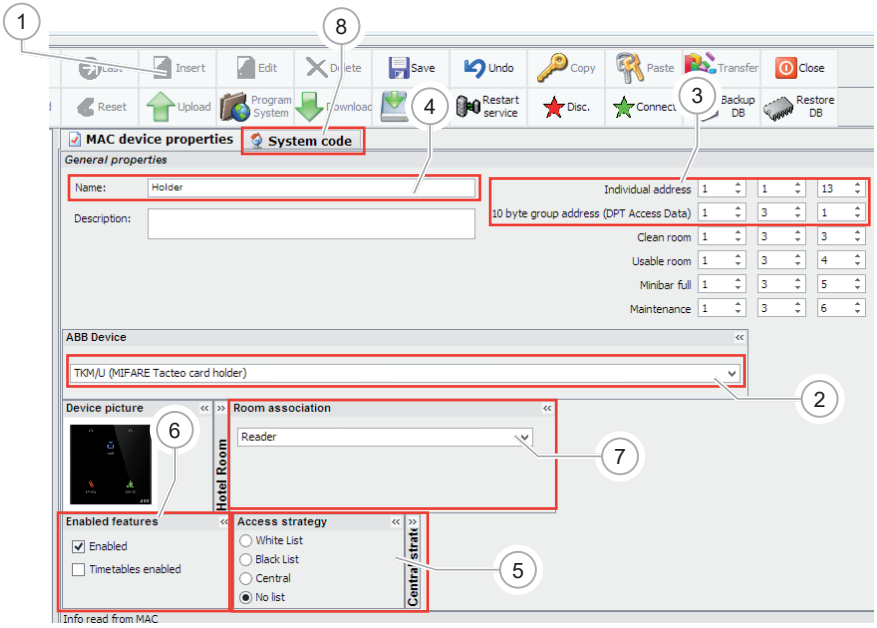
2.3.2.2 Transponder Holder

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

1. Click on INSERT from the main toolbar
2. 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
3. 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
4. Insert Name (and Descriprion, optional) of device
5. Configure Access Strategy: for Transponder Holder devices, the only acceptable methods are “No List” and “Black list”. The recommendation is configuring Access Strategy for Transponder Holder as “No List”.
6. Configure the device as “Enabled”
7. 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
8. Insert configured system codes using the menu in the tab “System code”



Device configuration (Chiara-Mylos and Millenium devices)

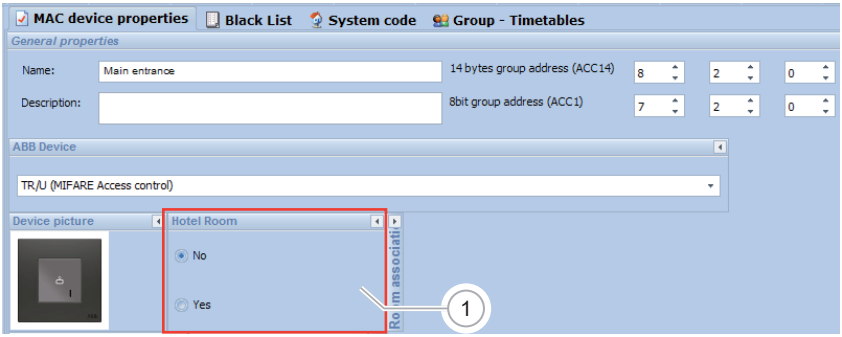


Device configuration (Tacteo devices)

2.3.3 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:

- From System menu click on NEW
- Insert new transponder readers
- Set the flag “NO” in the “Hotel room” setting

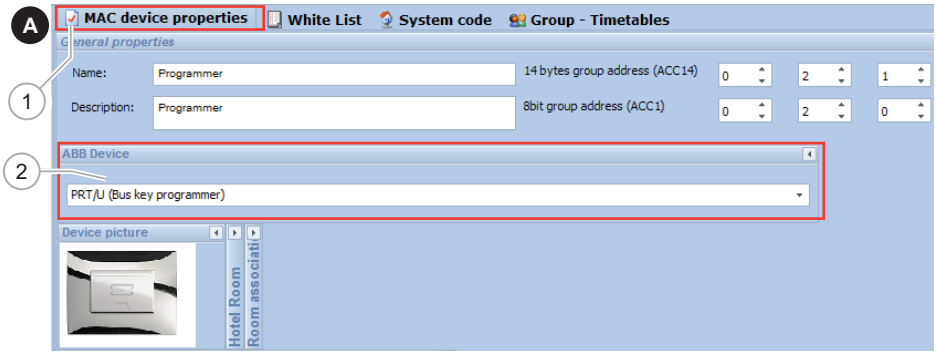


2.3.4 Transponder programming device

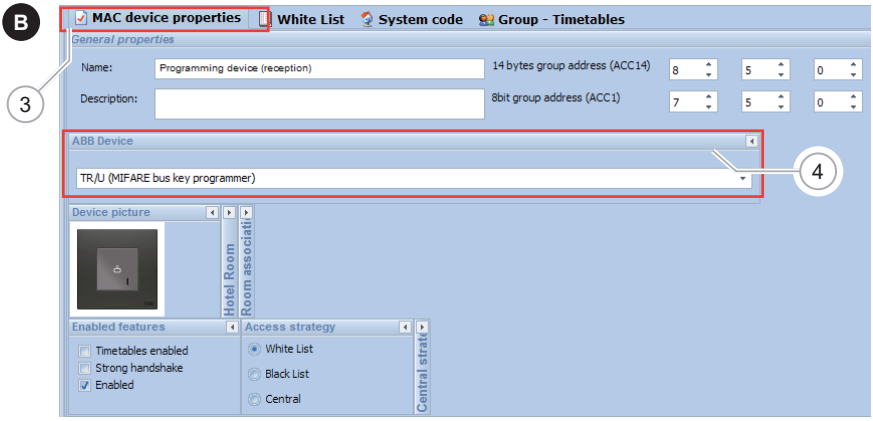
To complete the system, the last device to be set is the TAG programmer (transponder cards, TAGs).
The programming device is used to program transponder TAGs to be used in the system for the access to the various entrances.

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 (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

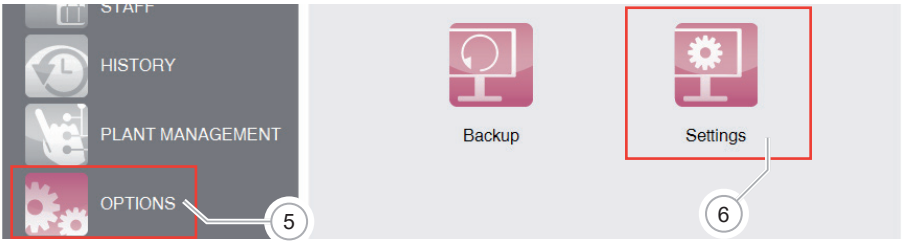


Chiara, Elos, Mylos programming device (PRT/U)

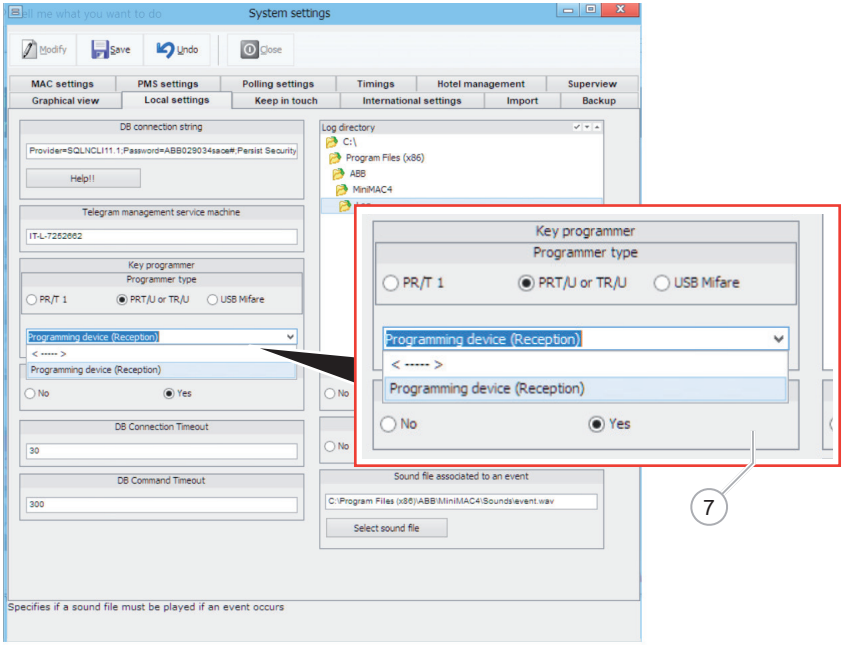


Millenium programming device (TR/U)

The type of programmer must be specified in the setting menu.

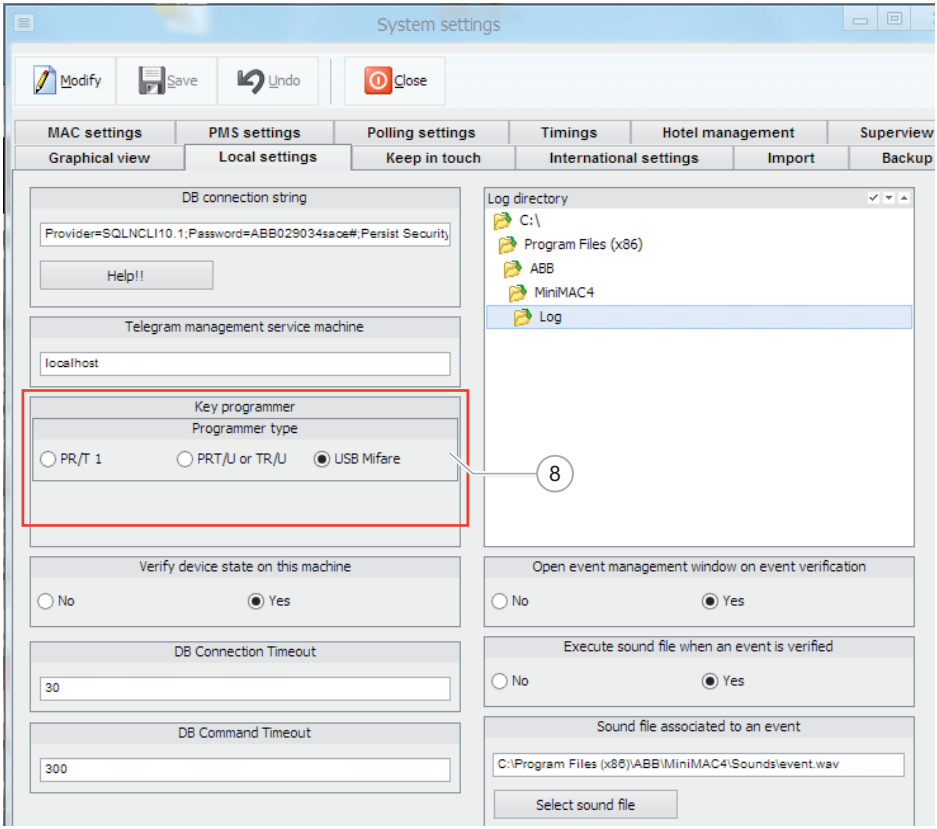


For Chiara-Mylos programmer (PRT/U) and Millenium programmer (TR/U) you need to select which device using, since more than one programmer (client) you can have in one installation (**7**).



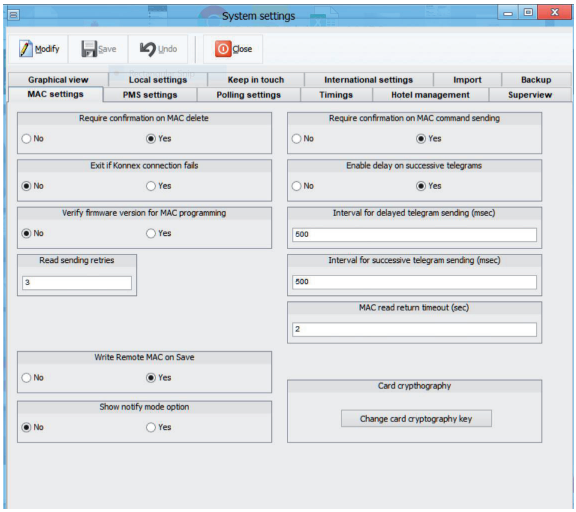
PRT/U - TR/U selection

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).



2.4 Access Control keys encryption (only for Tacteo range)

In order to grant an higher level of security, contents of access control keys/TAGS written by MiniMAC software is encrypted. The encryption key is automatically and randomly generated at every MiniMAC installation. During programming phase (when MiniMAC softare 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.

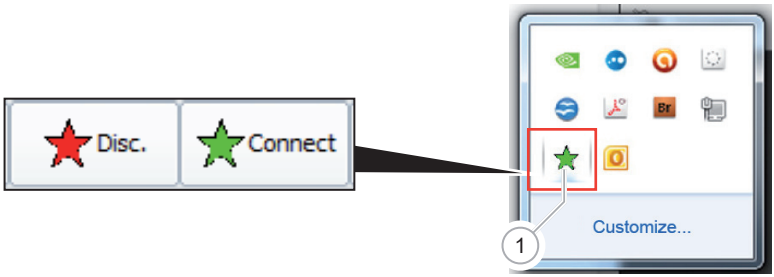


Warning
With the change of encryption key the installation/plant is no more usable: all the keys/TAGS previously created, and all the access control have stored internally the previous encryption key, and therefore the access control devices do not work with the old keys/TAG created. In order to download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

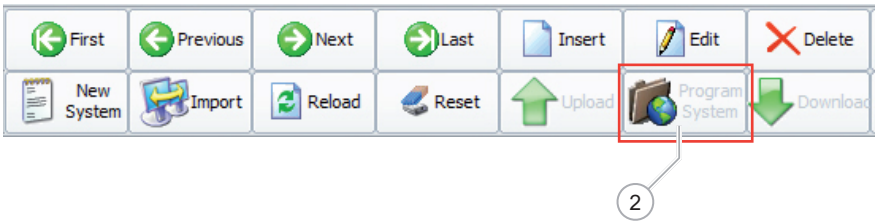
3 Download the configuration

MiniMAC allows you to work in off-line mode using a direct command (System menu/Disc. (off-line)/Connect (on-line).
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" (**2**) 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.

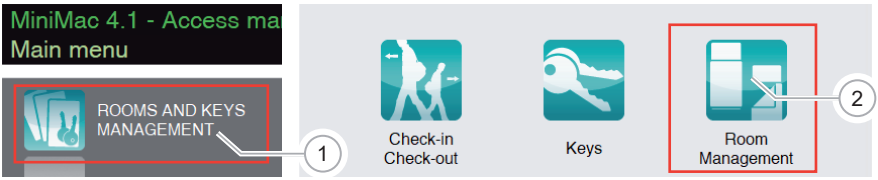
4 User manual

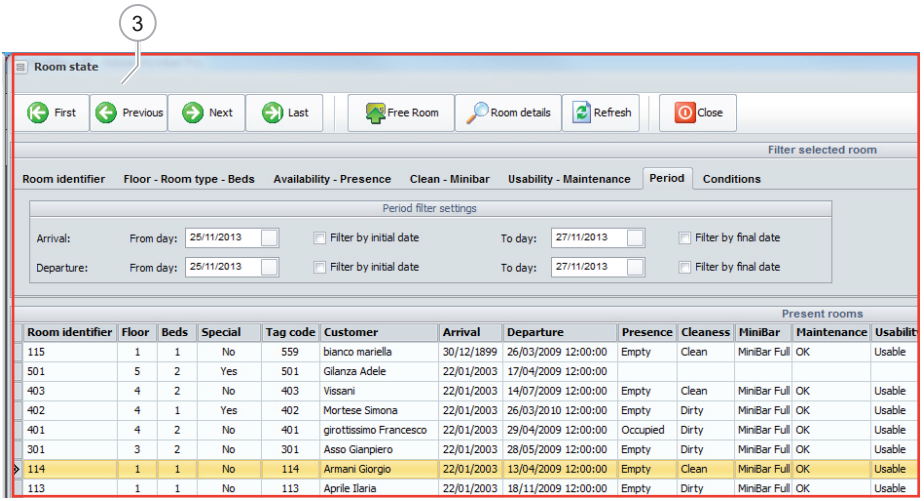
4.1 Room Management

MiniMAC 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

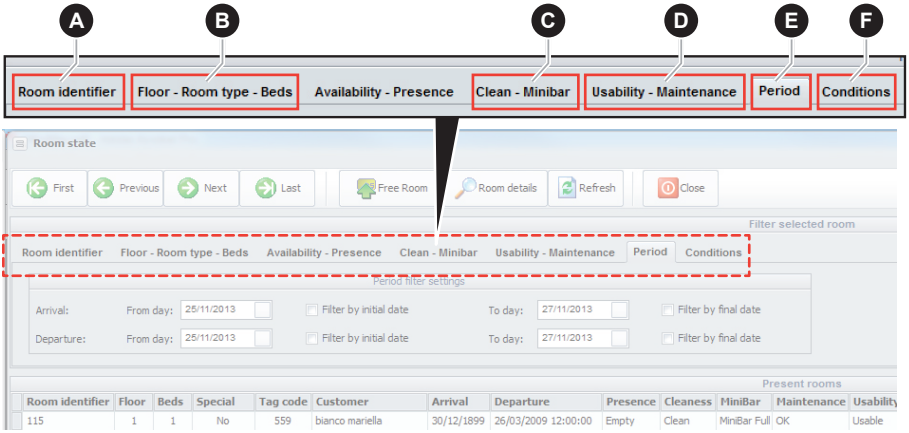
From the menu “Room Management” it is possible to have an exhaustive overview of the hotel:





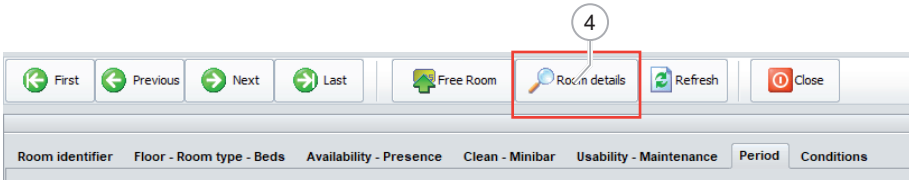
Room identifier	Floor	Beds	Special	Tag code	Customer	Arrival	Departure	Presence	Cleaness	MiniBar	Maintenance	Usabilit
115	1	1	No	559	bianco mariella	30/12/1899	26/03/2009 12:00:00	Empty	Clean	MiniBar Full	OK	Usable
501	5	2	Yes	501	Gilanza Adele	22/01/2003	17/04/2009 12:00:00					
403	4	2	No	403	Vissani	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

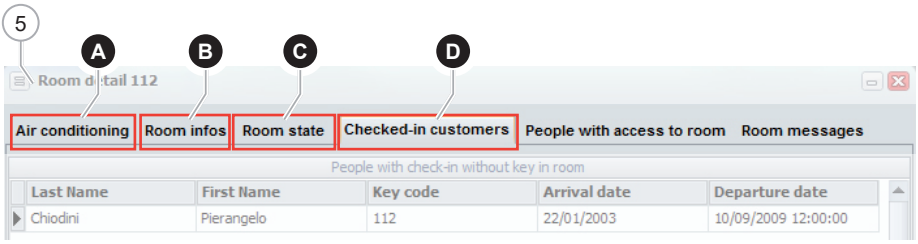
Room situation shows whether a room is available for a new customer to check-in. Furthermore, it shows when a room will be available in order to accept a reservation (check-in with check-in date in the future).
For each guest, room situation shows his/her assigned key code.
Furthermore, room type is 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.**



A	Search of a specific room.
B	View of room type and location.
C	View of Minibar status and room cleaning.
D	View whether the room can be used and technical maintenance status.
E	View of guest arrival and departure.
F	All conditions previously described can be made up.

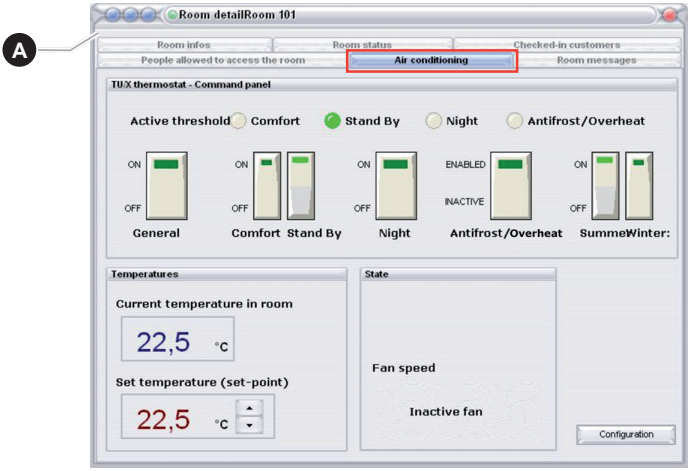
Selecting a room and clicking ROOM DETAILS, further information is shown.

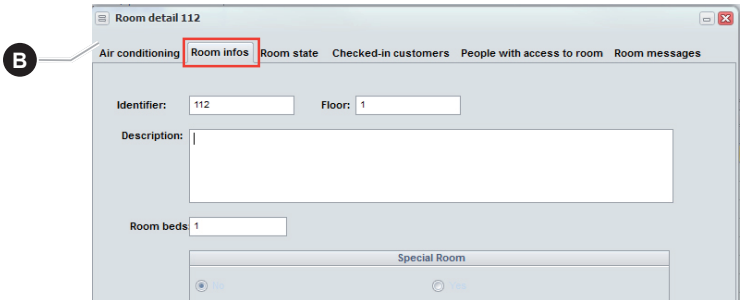


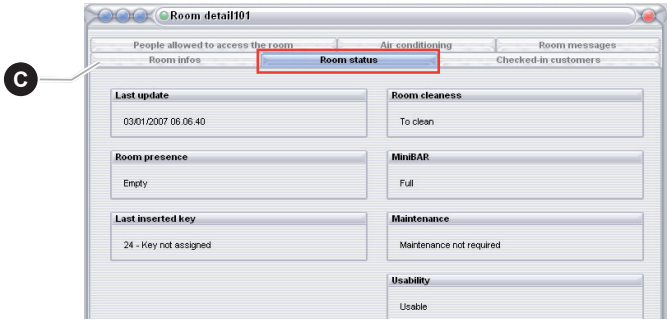


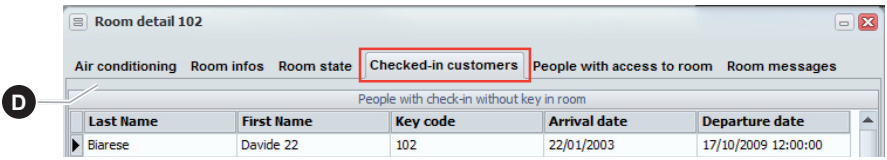
A	Heating and Cooling information.
B	Room type.
C	Room status.
D	List of persons who can access the room, apart from the guest.

"Air conditioning" menu shows relevant data if the communication with a KNX thermostat is previously properly configured





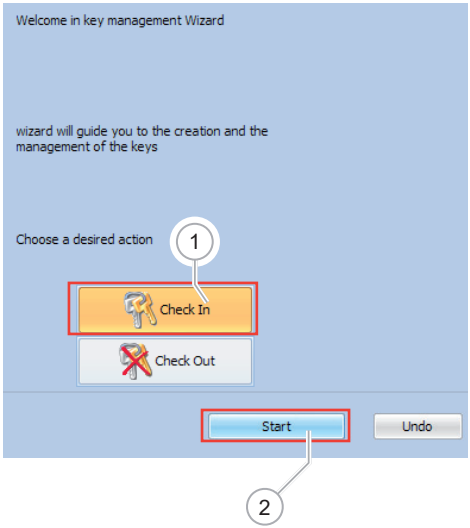


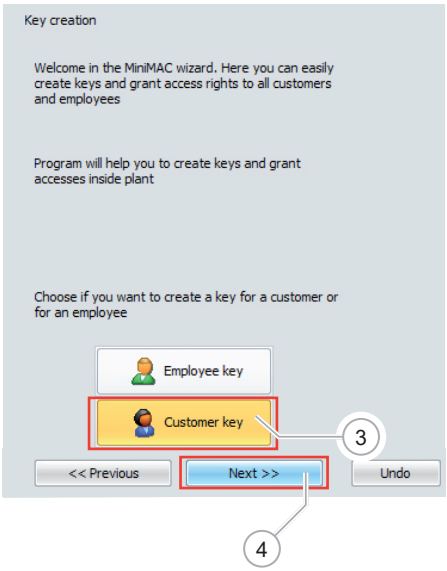


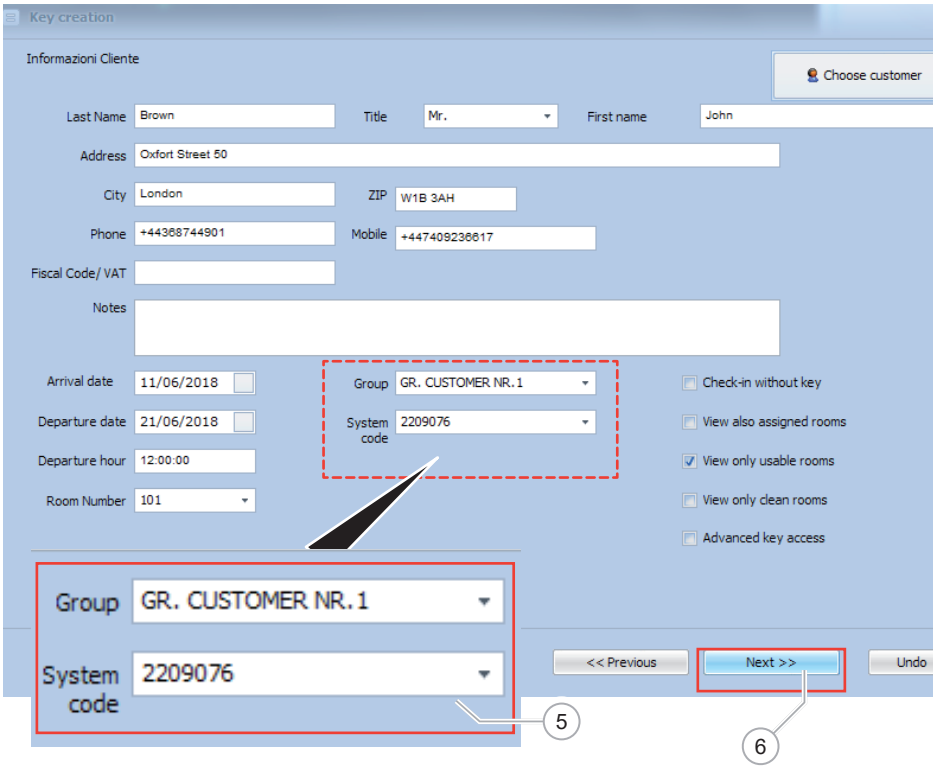
4.2 Check-in

During check-in, the system has to register the new guest, assign a room and generate the TAG for the access to his/her room and the common 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.



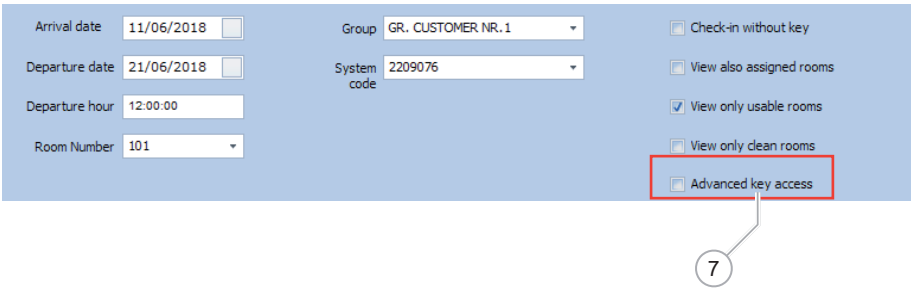




- Insert personal data and assign a room
- Define the System code to be written in the TAG
- Define the Group to which the TAG will belon to

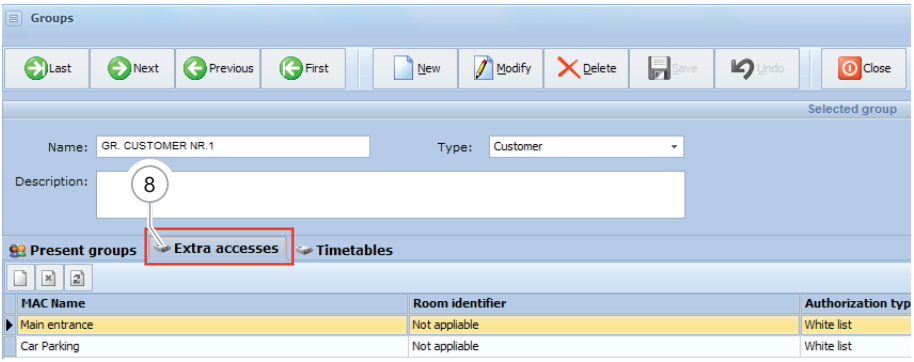
Note that GR. CUSTOMER NR.1 has been selected for the customer. This means that, for devices with active timeslots, the allowed time profile will be that defined for group GR. CUSTOMER NR.1.

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.

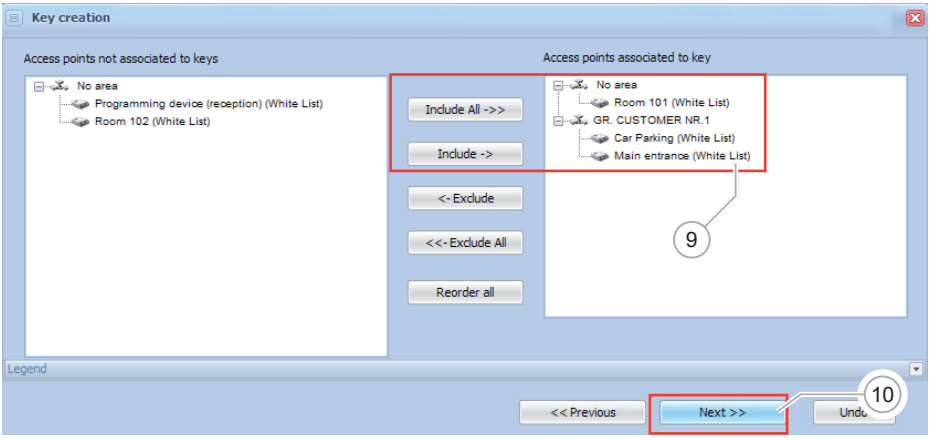


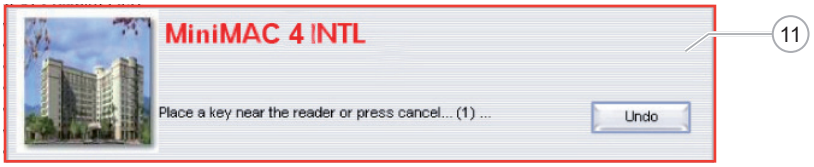
Otherwise, if “Advanced key access” option is enabled, the check-in procedure does not terminate immediately with card writing, but it’s possible to choose the entrances to which this customer (and therefore his/her card) has access.
In the figure below transits assigned to the TAG are shown.
A TAG assigned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

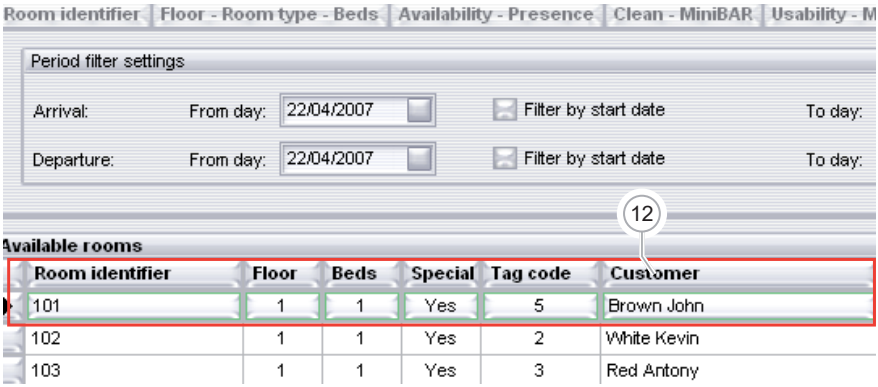


It's obviously possible to select other entrances to give access.
Variations to authorization rights can be performed by moving devices icons from the right to the left window, and vice versa.





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



4.3 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

4.3.1 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**.

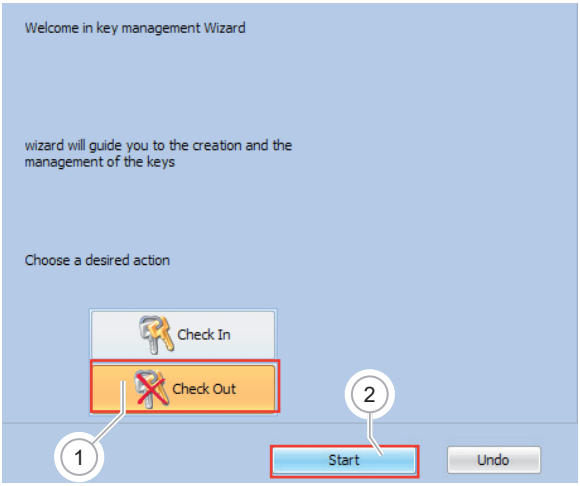
4.3.2 Check-out without TAG

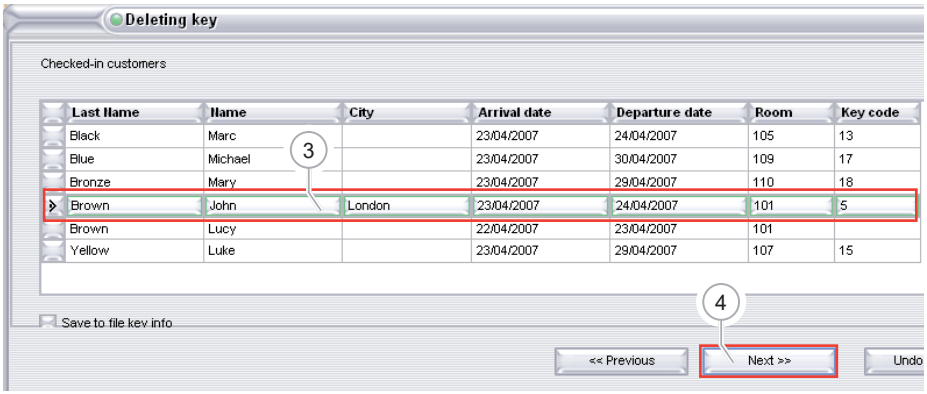
In a check-out without TAG, the TAG is removed from the system (as in the previous case) but it should not be returned (therefore it is not formatted). The reasons for such a check-out are several: the guest decides to keep the TAG, or s/he lost it, or the administrator decides to leave it to the customer.

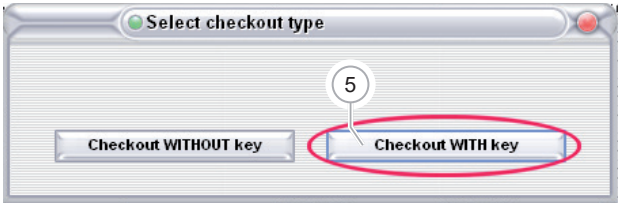
Note
Note that the TAG was removed from White lists, so it cannot get access to those transits. However, the TAG is not automatically inserted in Black lists, typical of common areas, so it keeps getting access to transponders working in Black list (at least as far as the TAG expires, usually the check-out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





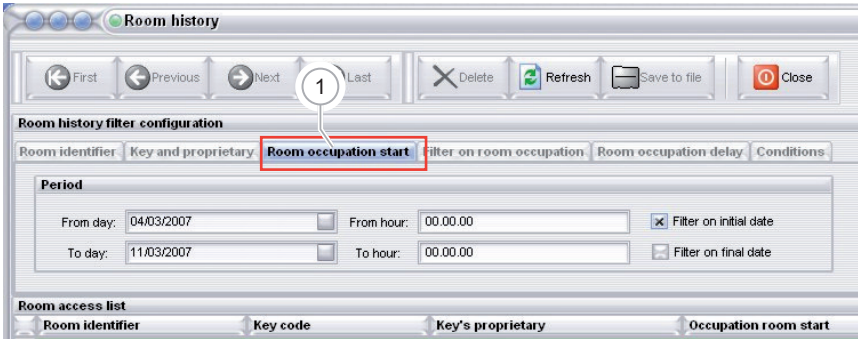


4.4 History management

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.

4.4.1 Presence history / room history

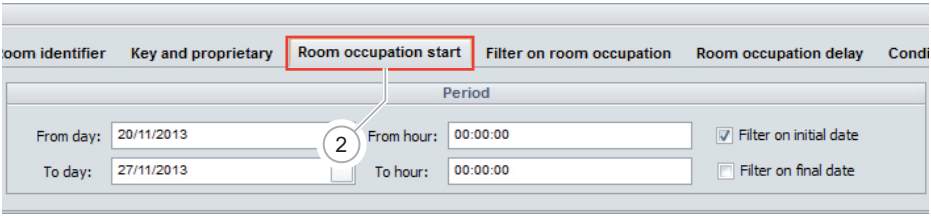
Thanks to this function you are able to view, for each room, time of entrance/exit, duration of stay and guest ID. Such function is available only if a transponder holder is installed in hotel rooms.



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

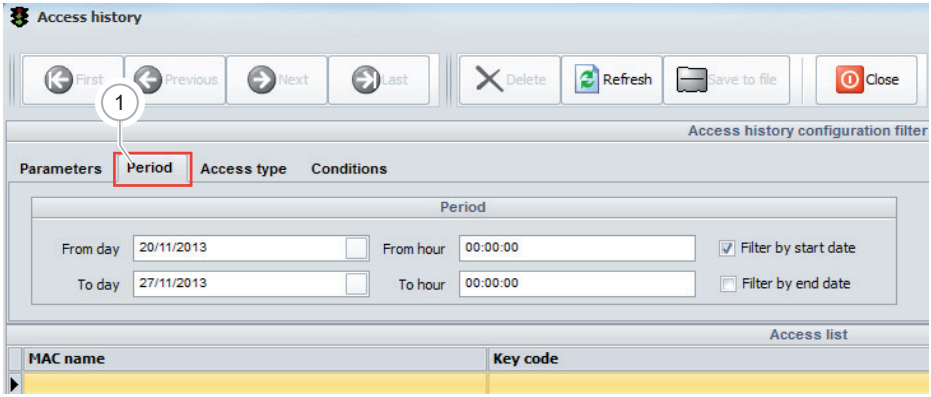
Note
The filer and save option described above can be used for all History tabs that follow.

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



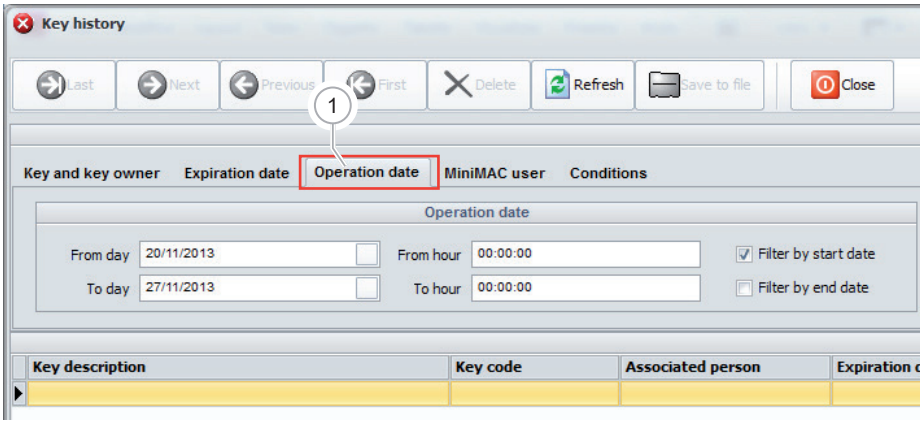
4.4.2 Access History

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



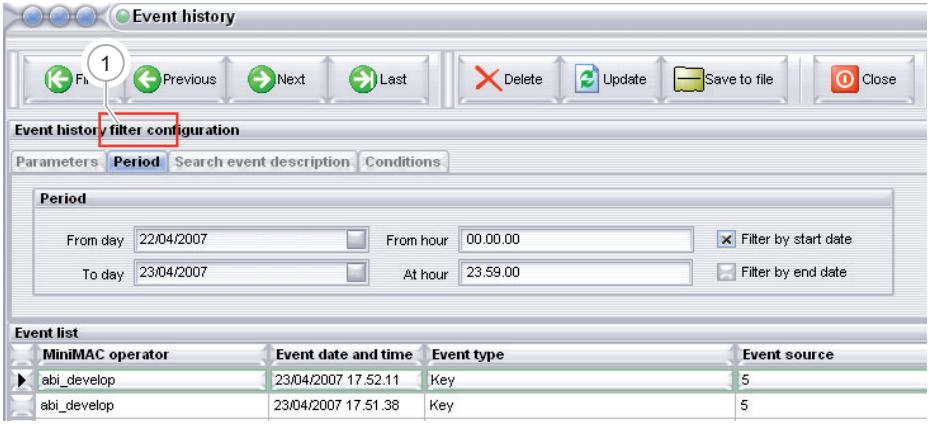
4.4.3 Key History

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.



4.4.4 Event History

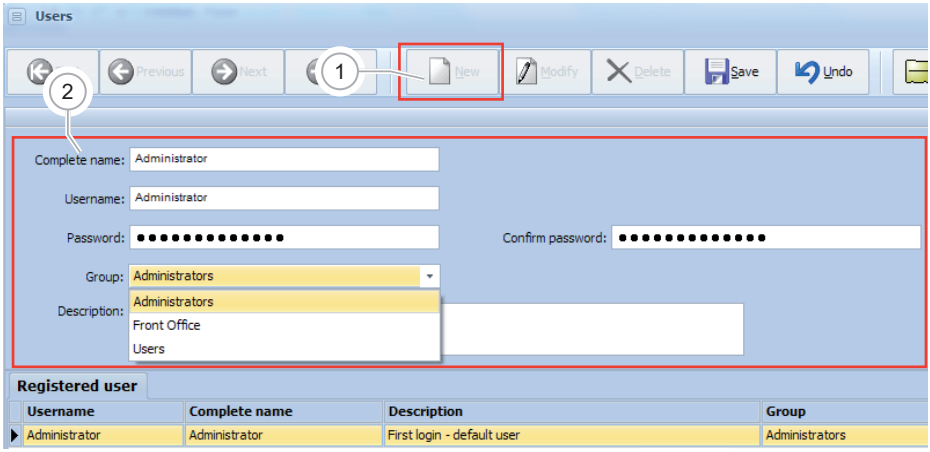
ALL operations performed on the system are stored in this history list.
In case of need, the administrator can check/view:
operations made by MiniMAC operators
events captured by MiniMAC telegrams management service



4.5 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 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 and operate anonymously on the system. Therefore, Administrator must be deleted as soon as possible.
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.
Administrator privileges must be assigned only to expert and/or responsible staff.

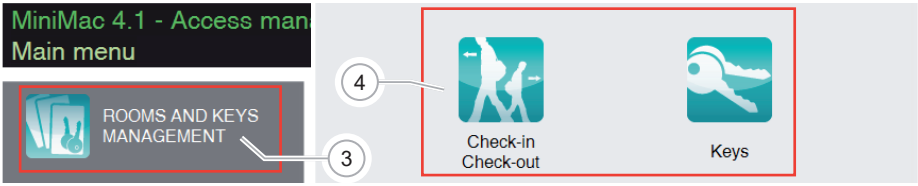
“Front Office” and “Users” cannot operate on the system configuration.

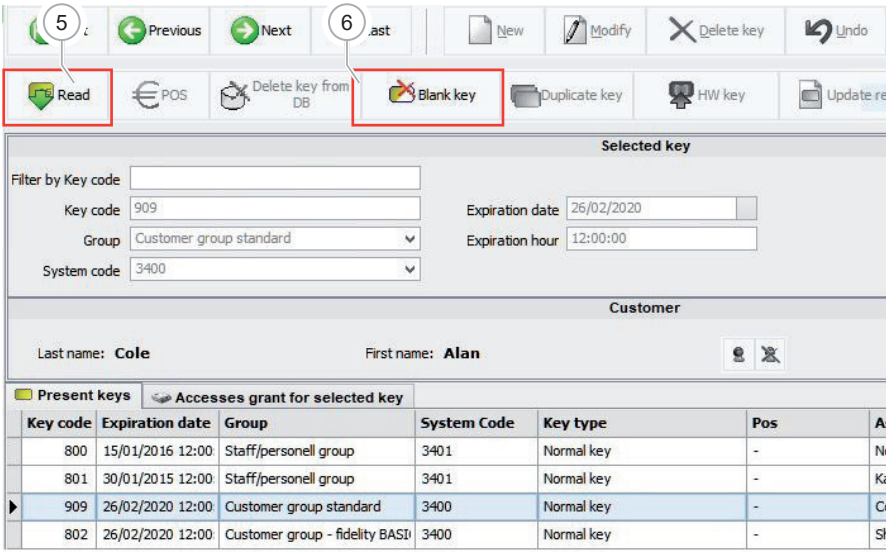
Front Office

“Front Office” has 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.



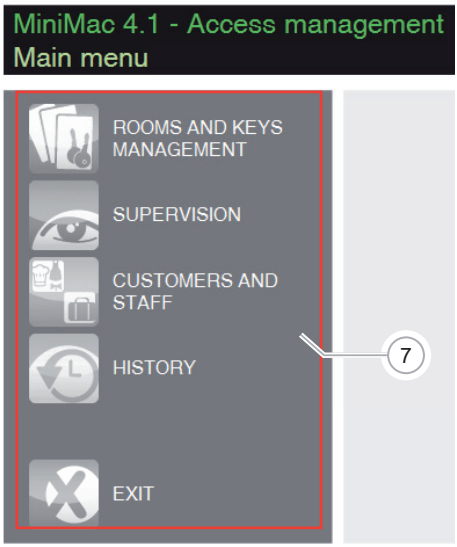


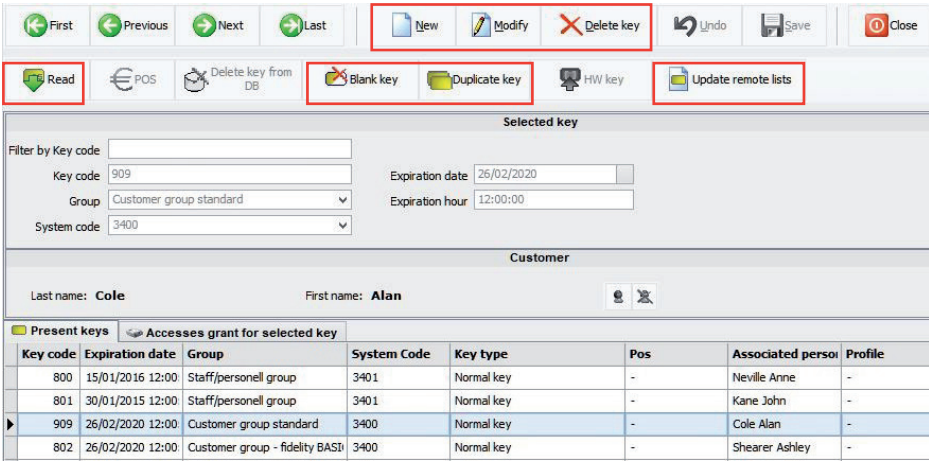
Users

"Users" 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.





Notes

Notes

—

ABB S.p.A.
Viale dell'Industria, 18
20010 Vittuone (MI),
Italy

www.abb.com/knx