

SMARTPHONE M2000BT APPLICATION USER GUIDE



INDEX

I : INTRODUCTION	4
1 / Conditional Input	4
3 / First Person In	4
4 / Schedule	5
5 / Antipassback	6
5 / Antipassback Case Exemple	7
II : INITIALIZATION	8
1 / Home	8
2 / Login	9
3 / General configuration	11
4 / Time table configuration	12
5 / Relay configuration	14
6 / Group configuration	15
7 / User management	16
8 / Add user	17
III : SETTINGS	18
1 / Relay commands	18
2 / User management	19
3 / Backup	22
4 / Group settings	25
5 / History	29
6 / Schedule	32
7 / Central setting	41
8 / Relay Configuration	42
9 / Session management	43
10 / Help	44

I : INTRODUCTION

The M2000-BT is an access control who may need some special vocabulary. This guide aim to explain in a ludic way the specific terms you may incounter while using the product.

1/Conditional Input

The **conditional input** consists in adding an extra action **B** necessary to validate relay activation:

Credential validation **A** + Extra action **B** = Relay activation 

This operating mode can be used when you want a vehicle to be present to allow relay's activation. In this case, the **conditional input B** would be a car loop detector connected to the M2000BT. The reading of a badge **A** by a pedestrian cannot therefore be accepted.

2/Bypass conditional entry

The **bypass conditional entry** allows the credential to be authorized without fulfilling conditional input (**B**).

For example, a pedestrian credential with «**bypass conditional entry**» can open the gates without having a vehicle present on a site with car detection loop and conditional entry activated.

3/First Person In

The **first person in** feature set the activation of a pre-planned schedule when the first authorized credential is used.

This feature will protect your premise by keeping the doors locked until an authorized employee presents his/her credential to unlock the building.

4/Schedule

Schedule planification allow you to configure your access control for the upcoming years , setting opening for work hour, closure time for bank holiday and special event opening hour such as a reception.

In the following paragraph see the schedule planification's logic it's powerful capabilities.

Create a time slot to set work hour opening for a portal during intensive passage time:

From Monday to Thursday: OPEN at the following
[8h30 ➡ 9h30] ; [11h30 ➡ 12h30]
[13h45 ➡ 14h15] ; [16h30 ➡ 17h10]

On Friday : OPEN at the following
[8h30 ➡ 9h30] ; [11h30 ➡ 12h30]
[13h45 ➡ 14h15] ; [15h30 ➡ 16h30]

On Saturday : OPEN at the following
[8h30 ➡ 9h30]

On Sunday : CLOSE

On holiday : OPEN at the following
[8h30 ➡ 11h30]

On special day = once in a year : OPEN at the following
[19h00 ➡ 23h30]

5/Antipassback

The **antipassback** feature prevents credential misuse, by putting certain restrictions on the use of their cards. When activated, users must present their credentials to enter  and exit  all zones.

Antipassback prevents a user from using his or her credential twice at the same access point.

It can be used to maximize security, prevent fraudulent use of credential and maintain accurate recording of the number of people who are currently in an area .

6/Antipassback Status

There are 3 **antipassback status** for every users.

-  **Entering** : the user can only be accepted on an "**Exiting**" reader.
-  **Exiting** : the user can only be accepted on an "**Entering**" reader.
-  **Unkown**: the user can be accepted indifferently on an **Entering** or **Exiting** reader.

❗ When you create a credential: its first **antipassback status** is «unknown»: it can be accepted indifferently the first time on. As soon as it is accepted on a reader it loses its "unknown" state and enters the cycle of antipassback.

When powering up the M2000BT, all users systematically switch to an "unknown" state of antipassback.

7/Bypass Antipassback

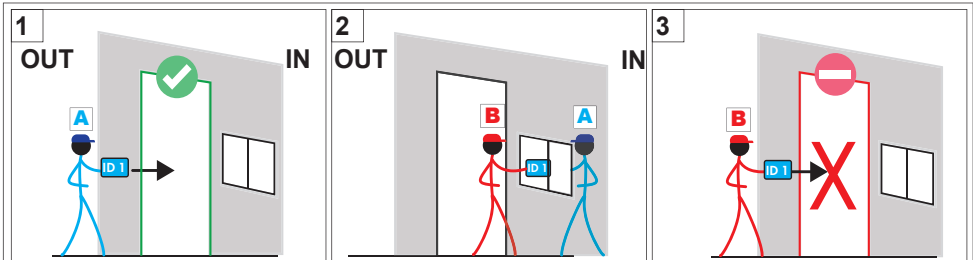
The **bypass antipassback** feature allows users to use his/her credentials on every reader whitout having fulfill antipassback requirement.

It allows the user not to worry about the antipassback status to open doors.

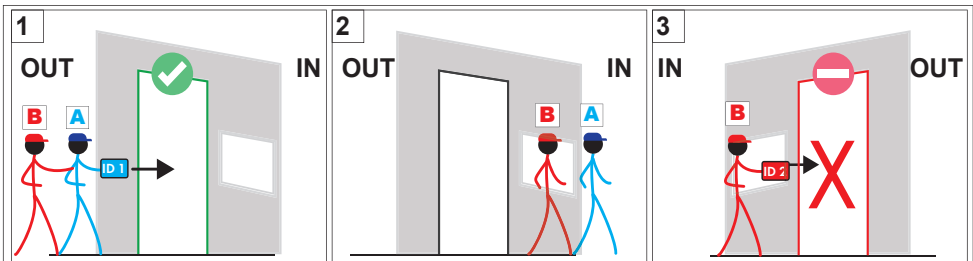
5/Antipassback Case Example

See below few example of antipassback feature abilities:

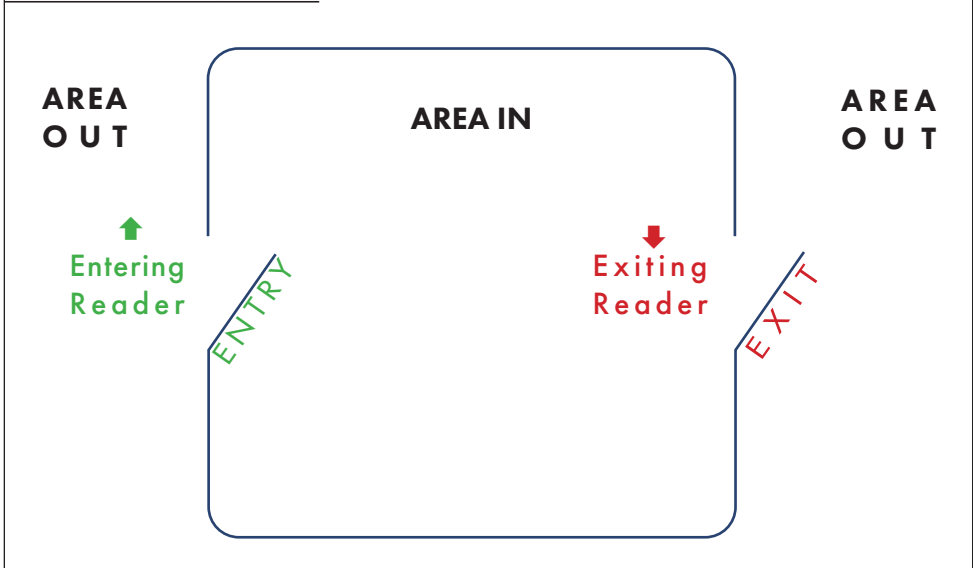
Case 1:



Case 2:



Case 3 : PARKING LOTS



This drawing represent an antipassback secured installation:

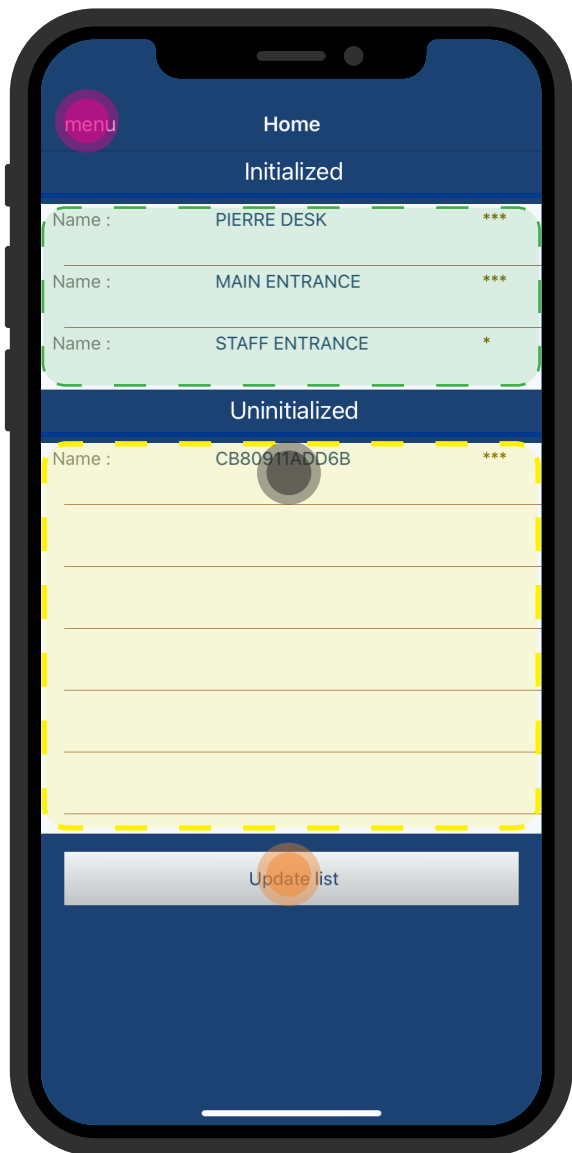
- there are 2 areas: inside [IN] and outside [OUT] the secured zone.
- there are 2 doors/gates controlled by readers:
ENTRY controlled by Entering Reader and EXIT controlled by Exiting Reader.

II : INITIALIZATION

1/Home

Caution: DO NOT FORGET to activate the BT on your smartphone.

When the M2000-BT application is started, the Home window is accessed and after an automatic search, the list of available control units is displayed.



Back to **General Menu**

List of «**Initialized**» control units
(already configured)

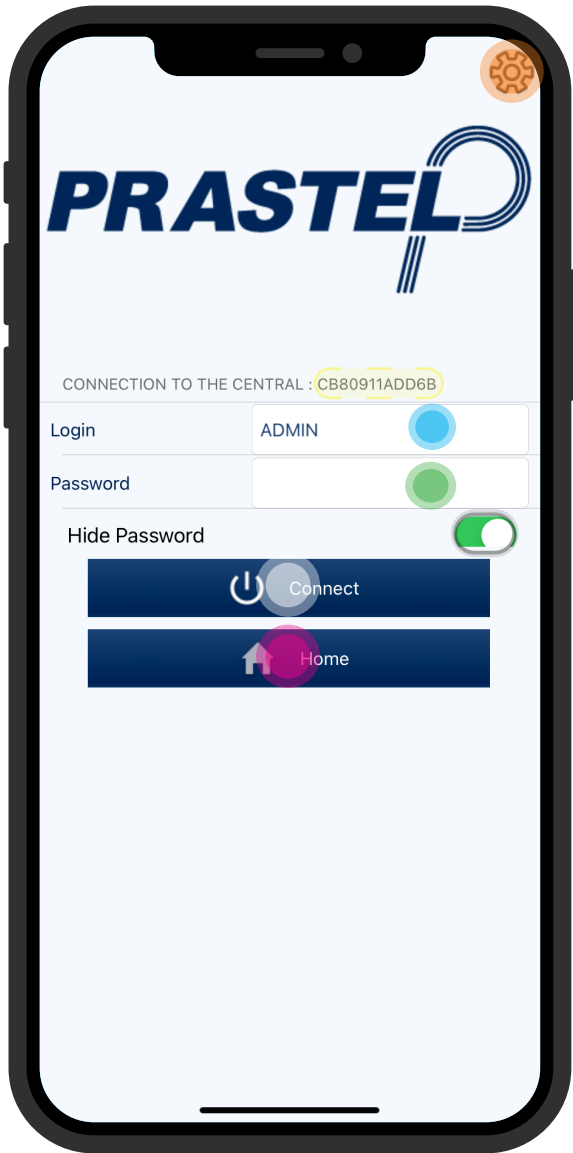
List of «**Uninitialized**» control units
(without login and password)

Start a control units search
and update the list.

Select your new control unit from the uninitialized list, , to go to the next step.

2/Login

Click the  **Connect** button to go to the next step.



Reset
(Contact **Prastel France**)

① MAC adress.

 Enter login
(ADMIN by default).

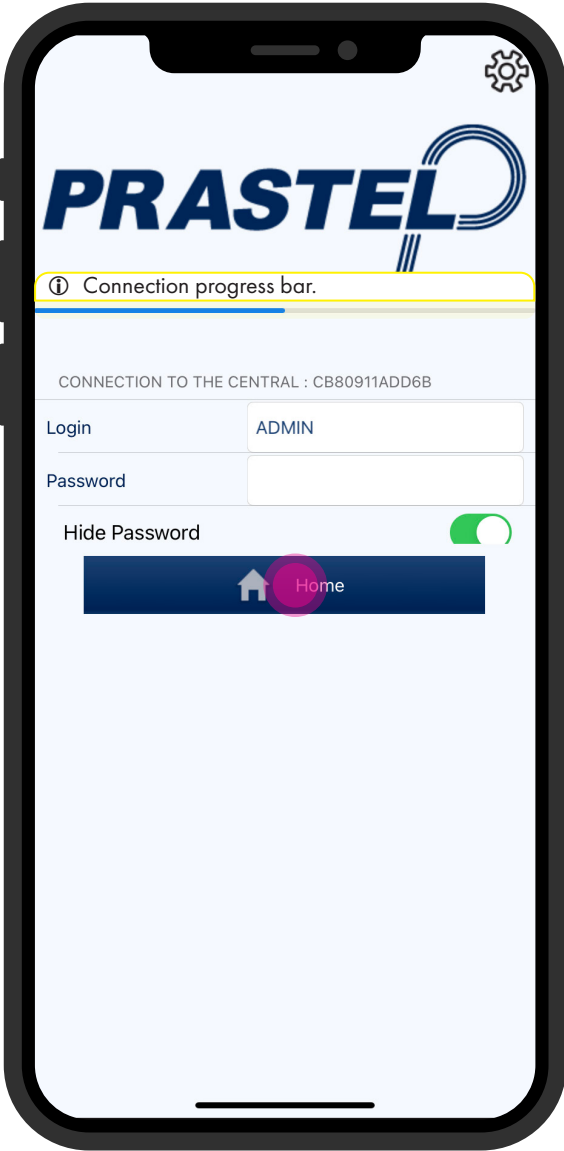
 Enter password.

View password.
 hidden  visible

Connection to the control
unit.

Back to **Home**

The application connects to the selected control unit, please wait.



Back to Home

3/General configuration

The image shows a smartphone screen with the 'General Configuration' app. At the top, there's a blue header with the title 'General Configuration'. Below it, a yellow-bordered box contains an information icon and the text 'Our advices for the first installation'. This box also includes instructions about the default configuration of the M2000BT unit, recommendations for naming the unit and changing login/password, and a 'Next' button. The main configuration area is divided into two sections: 'GENERAL CONFIGURATION' and 'ADMINISTRATOR CONFIGURATION'. The first section has fields for 'Equipment name' (set to 'NORTH ENTRANCE') and 'MAC address' (set to 'CB80911ADD6B'). It also features five toggle switches: 'Anti-passback' (green, on), 'Only encrypted remote controls' (green, on), 'Summer/Winter Europe' (green, on), 'Summer/Winter USA/Canada' (orange, off), and 'Facility Code Management' (pink, off). The second section has fields for 'Login' (set to 'ADMIN') and 'Password' (empty). At the bottom, there is a 'Next' button with a checkmark icon.

General Configuration

① Our advices for the first installation

See below the default configuration of M2000BT unit.

Recommendation :

- Choose the unit name (ex: NORTH ENTRANCE, DOOR BUILDING A) for next use of the standalone unit.
- Change your login and administrator password to secure your unit.

To validate the information please click on the button "Next".

GENERAL CONFIGURATION

Equipment name: NORTH ENTRANCE

MAC address : CB80911ADD6B

Anti-passback: ☒

Only encrypted remote controls: ☒

Summer/Winter Europe: ☒

Summer/Winter USA/Canada: ☐

Facility Code Management: ☐

ADMINISTRATOR CONFIGURATION

Login: ADMIN

Password:

Next ✓

Antipassback: in a 2-door system, an entry activated by reader 1 authorises the exit on reader 2 (see p.42)

Enable compatibility with our encrypted remotes only.

Ex: SLIM+, SLIM2E+

Activate the automatic time change according to the selected geographical area..

Activate facility code management for DATA inputs, e.g. for proximity readers such as the MPROXMINI.

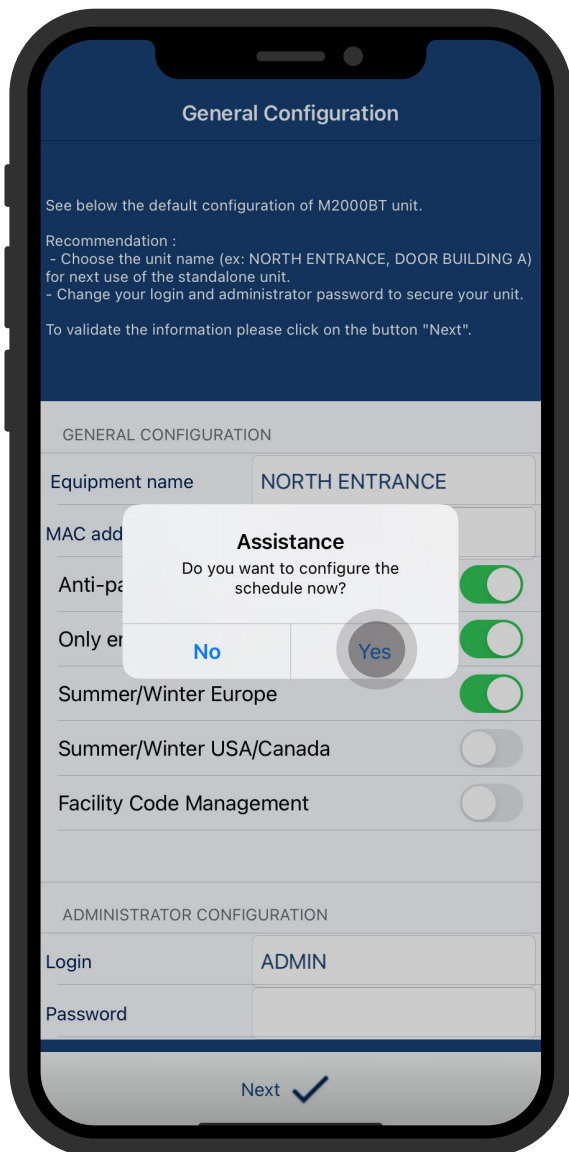
Click the  button to go to the next step.

4/Time table configuration

By clicking on the **Next**  button, the installation wizard offers you to configure time slots. They can be used to define access authorisations for groups and/or relay.

It also include an automatic positive opening operation mode.

You need to define public holidays, special day and exception in order to set reading authorization and or opening/closure time slot..



General Configuration

See below the default configuration of M2000BT unit.

Recommendation :

- Choose the unit name (ex: NORTH ENTRANCE, DOOR BUILDING A) for next use of the standalone unit.
- Change your login and administrator password to secure your unit.

To validate the information please click on the button "Next".

GENERAL CONFIGURATION

Equipment name **NORTH ENTRANCE**

MAC address

Anti-passback ☒

Only entrance ☒

Summer/Winter Europe ☒

Summer/Winter USA/Canada ☐

Facility Code Management ☐

ADMINISTRATOR CONFIGURATION

Login **ADMIN**

Password

Assistance

Do you want to configure the schedule now?

No **Yes**

Next 

Validate ✓

[← Back](#)
[Time table configuration](#)

See below the schedule configuration by default:
It is valid from 8:00 to 12:00 and from 14:00 to 18:00 from Monday to Friday.
Access is restricted on weekends, on special days and on holidays.
To change the information, please click the button "Validate".

Name

STANDARD

Schedule Enable

ALL

Monday	T1	T2	T3	T4
Start	08h00	14h00	---	---
End	12h00	18h00	---	---
Tuesday	T1	T2	T3	T4
Start	08h00	14h00	---	---
End	12h00	18h00	---	---
Wednesday	T1	T2	T3	T4
Start	08h00	14h00	---	---
End	12h00	18h00	---	---
Thursday	T1	T2	T3	T4
Start	08h00	14h00	---	---
End	12h00	18h00	---	---
Friday	T1	T2	T3	T4

Validate ✓

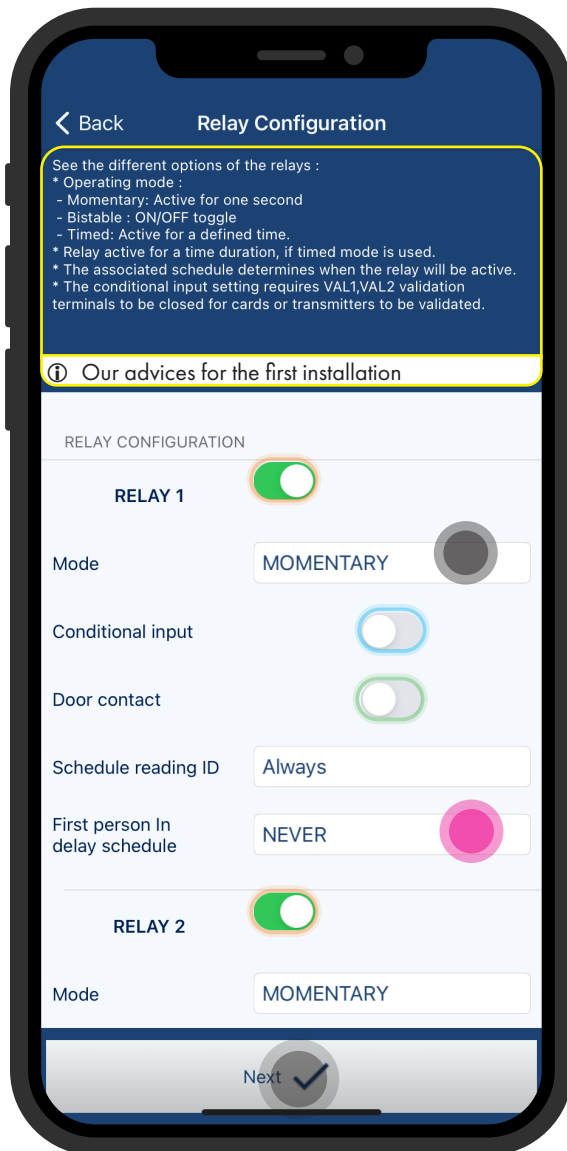
 **STANDARD** = 8h-12h/14h-18h
from M to F except public holidays
and exception (set by default /
editable).

✅ ALWAYS = 24h/24h

➡ **NEVER**= No time slots (no passage allowed).

5/Relay configuration

Select the desired relay configuration and then click the **Validate**  button to proceed to the next step.



Relay Configuration

See the different options of the relays :

- * Operating mode :
 - Momentary: Active for one second
 - Bistable : ON/OFF toggle
 - Timed: Active for a defined time.
- * Relay active for a time duration, if timed mode is used.
- * The associated schedule determines when the relay will be active.
- * The conditional input setting requires VAL1,VAL2 validation terminals to be closed for cards or transmitters to be validated.

Our advices for the first installation

RELAY CONFIGURATION

RELAY 1

Mode: **MOMENTARY**

Conditional input: ☐

Door contact: ☐

Schedule reading ID: **Always**

First person In delay schedule: **NEVER**

RELAY 2

Mode: **MOMENTARY**

Next 

Enable or disable relays.

Conditional input : adds an extra action to the validate the credential.
e.g. a magnetic loop contact that adds the condition of vehicle presence to activate the input.
(see p.41)

Activation of schedule for access authorization or positive opening operation on the relay.

6/Group configuration

The group settings (e.g. schedule) will apply to the users linked to it.

< Back Group configuration

i Our advices for the first installation

All added users must be registered to a group.
For each group, there are 3 sub-groups to choose from; Card, transmitter, or Card/Transmitter.
Below, the predefined group which can be modified.

To save and validate the information, click on the "Validate" button.

GROUPS SETTINGS

Group Enable ☒

Name STANDARD

Type Badge/Transmitter

Schedule Always

RELAY 1 B1 C1

RELAY 2 B2 C2

Bypass Conditional entry ☐

Bypass Anti-passback ☐

Validate ✓

Enable or disable the group

Define the group name.

Type of support for your identifiers

Activate an access authorisation schedule for this group.

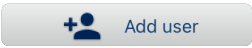
Define the association of a radio channel and/or a reader with the relays for this group

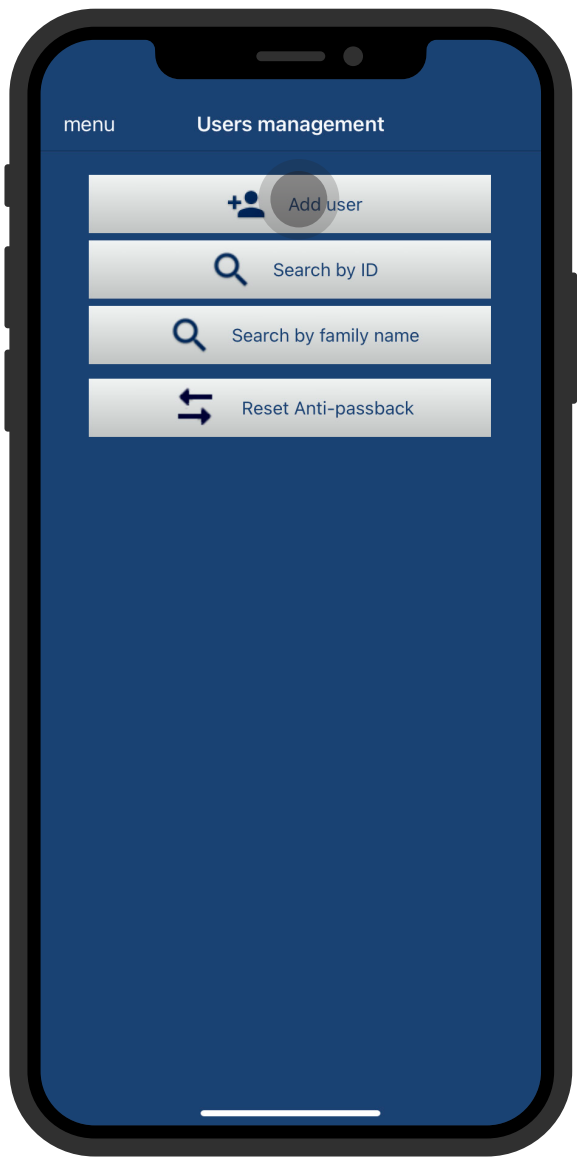
Bypass functions:

In the case of an installation with activated access conditions such as conditional entry or antipassback (see p.42), when the override is activated, the users of this group are no longer obliged to comply with the activated conditions.

Once the group has been configured, click on the button to proceed to the next step.

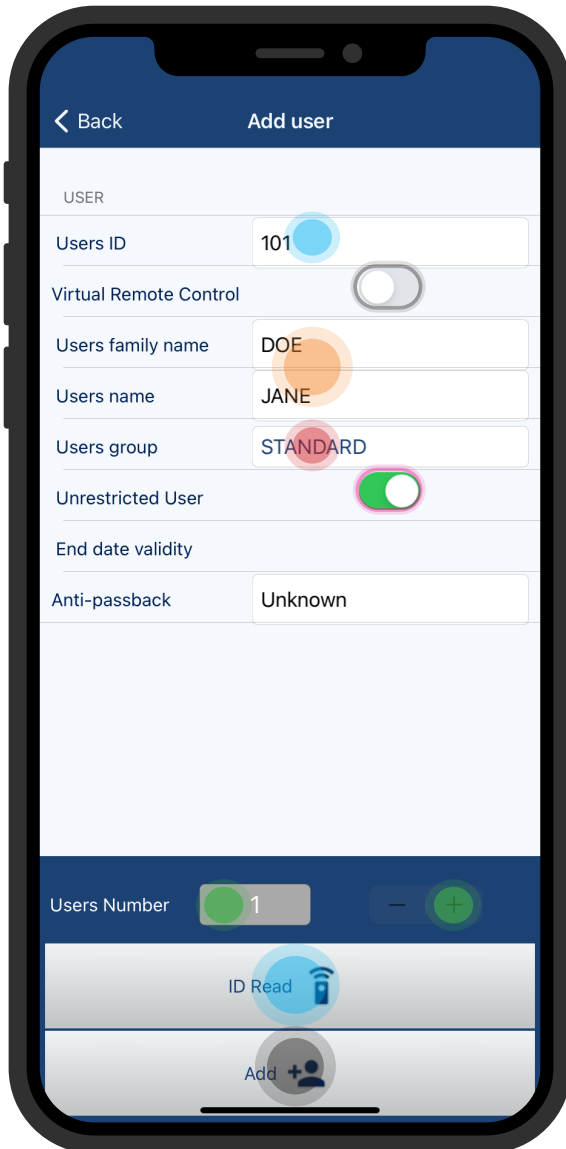
7/User management

Click on the  button to go to the next step.



8/Add user

Set up the user file then click on the  button to validate.



USER

Users ID: 101

Virtual Remote Control: ☐

Users family name: DOE

Users name: JANE

Users group: STANDARD

Unrestricted User: ☒

End date validity:

Anti-passback: Unknown

Users Number: 1

ID Read

Add 

 Enter the user ID or press the **ID Read** button and then activate the user ID.

Activate if it is a virtual remote control (smartphone application)

 Enter the user's civil information

Define the group to which the user is linked

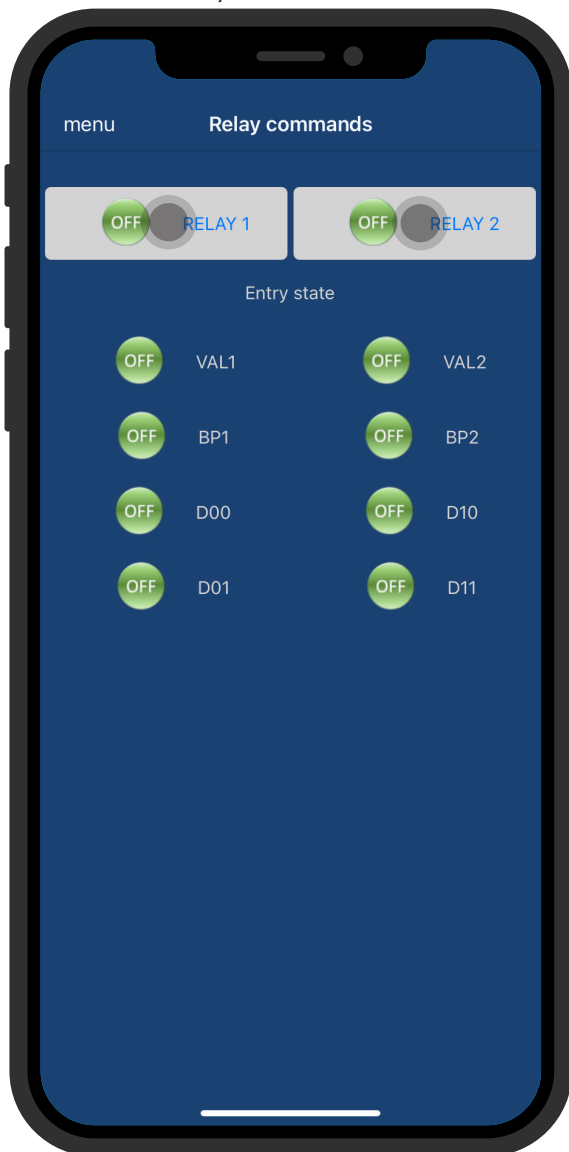
Define whether the user is permanent (no expiry date)

Creation of multiple users:
If your identifiers are a suite, (ex: 100 to 150)enter the number of users, the application will automatically insert the credentials to be registered.

III :SETTINGS

1 /Relay commands

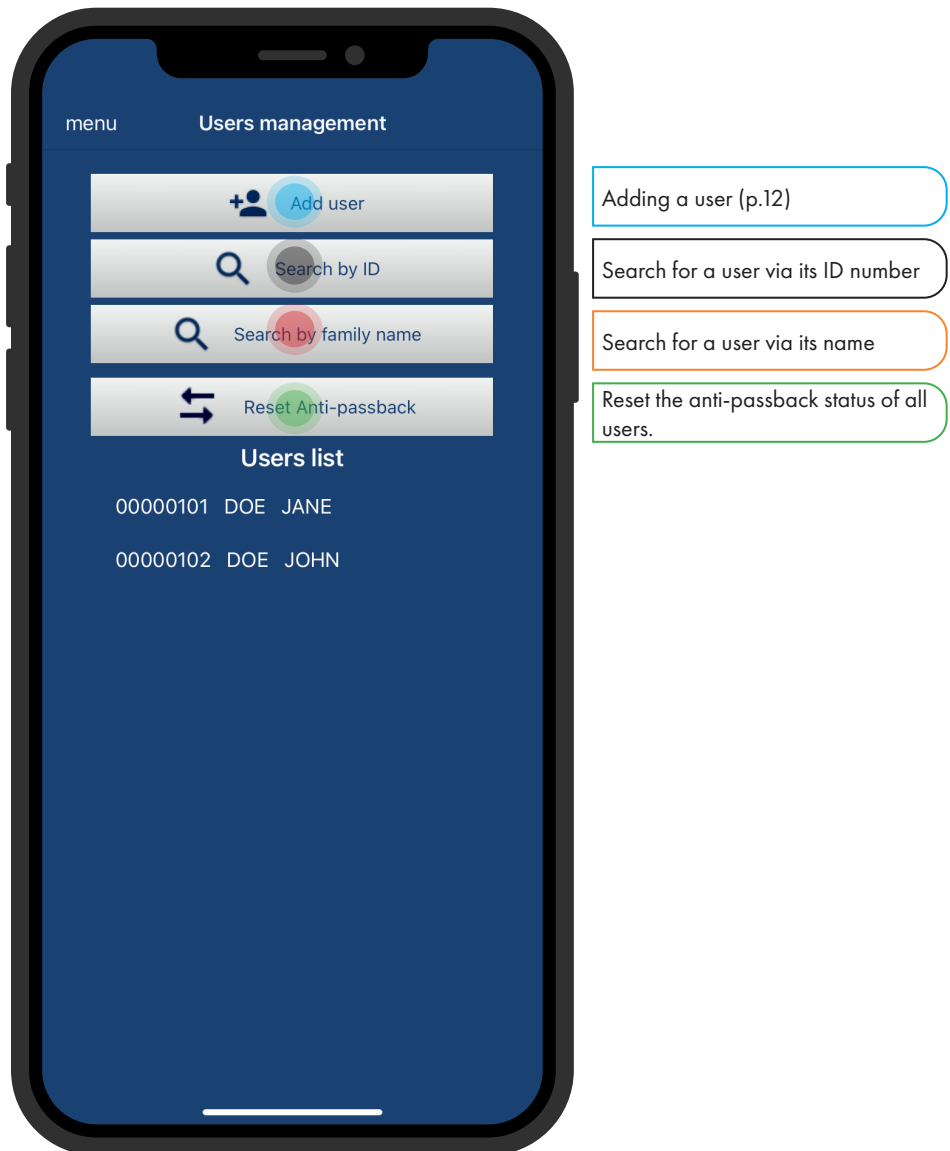
The relay control function allows the operation of the installation to be monitored via the various input status LEDs and relay activation buttons.



Changes relay status according to its configuration.

2/User management

The user management part allows you to add users (see I.8.Adding users on p.12) and manage registered users.



The search by ID number can be done by manual input or by reading an ID:

Back

Search by ID

Search

101

USER

Users ID

101

Virtual Remote Control

Users family name

DOE

Users name

JANE

Users group

STANDARD

Unrestricted User

End date validity

Anti-passback

Unknown

<

Previous

Next>

ID Read

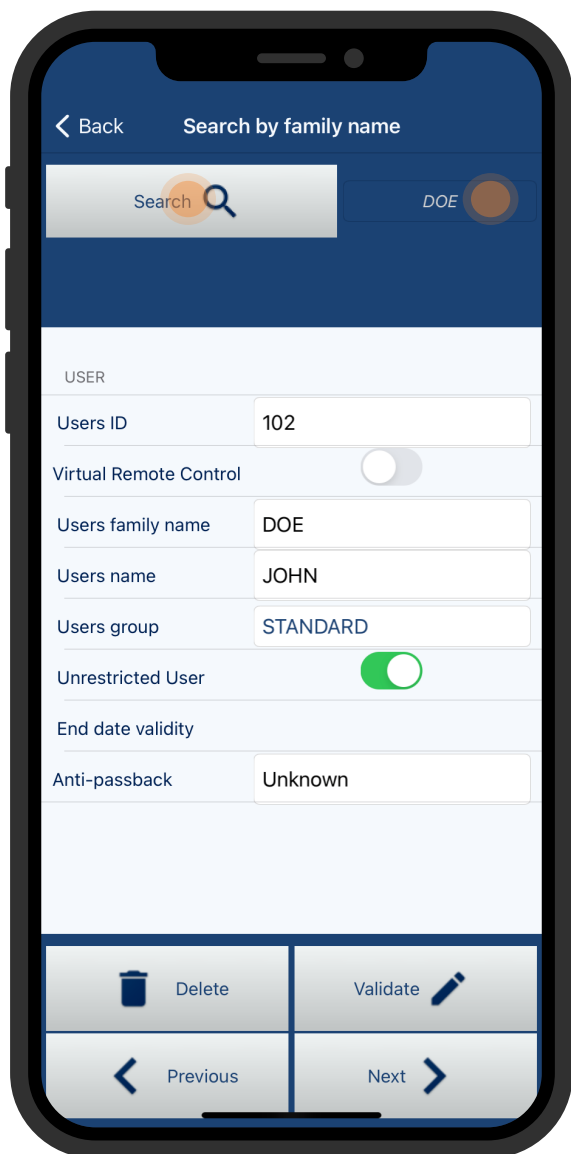
Delete

Validate

 Insert ID number and press 

 ID Read : activates the reading of ID number, badge or remote control.
After the remote control is sent or the badge is read, the ID number will appear automatically..

Searching by family name is done by manually entering the name to be searched for:

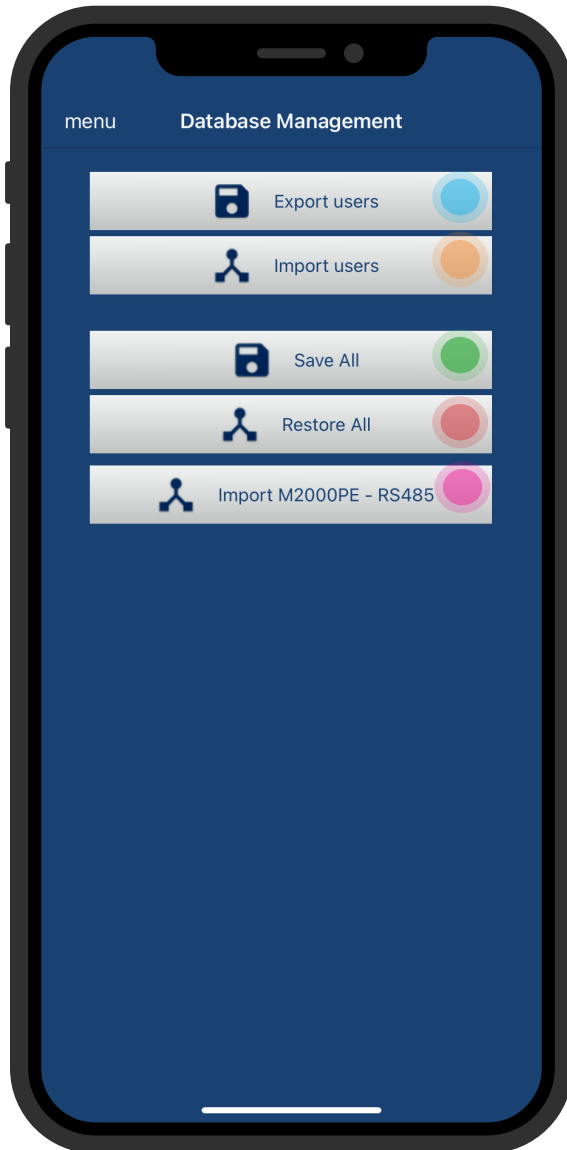


Insert the Name to be searched for, then press

3/Backup

The application allows 2 types of backups to be made: either the list of users only, or the complete installation (user list, time slot, relay configuration, etc.).

The database management part also allows the import of backups saved on the smartphone used..



Save the user list.

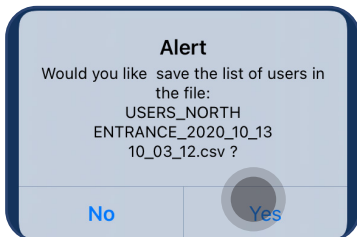
Restore the list of users saved.

Save the complete configuration.

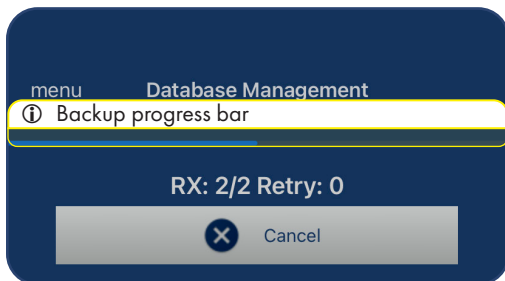
Restore the complete saved configuration.

Import the configuration of a M2000PE -RS485 control unit

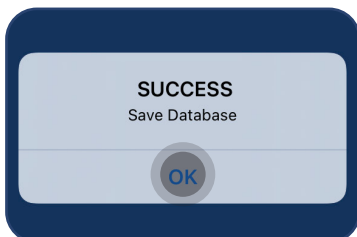
Save/Export :



Confirm the saving of the backup
(user list or full configuration)

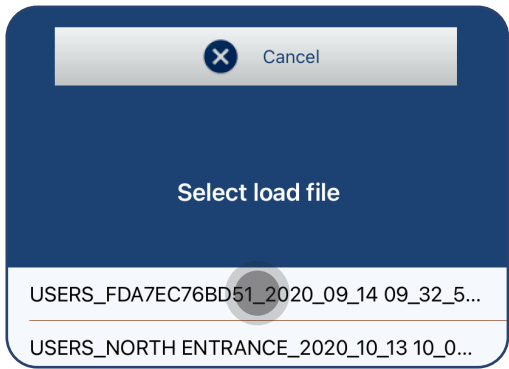


Wait for the end of the backup.



Validate the message of success

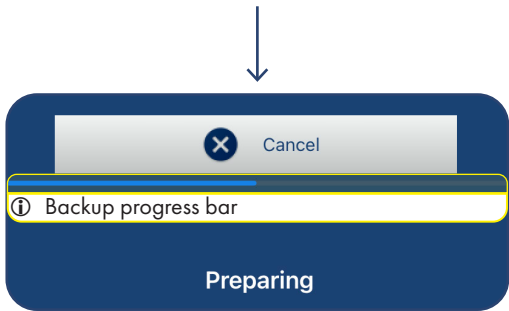
Import/ Restore :



Select the backup file.



Validate the import of the backup (user list or full configuration)



Wait for the end of the backup.

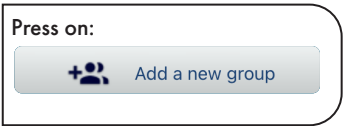
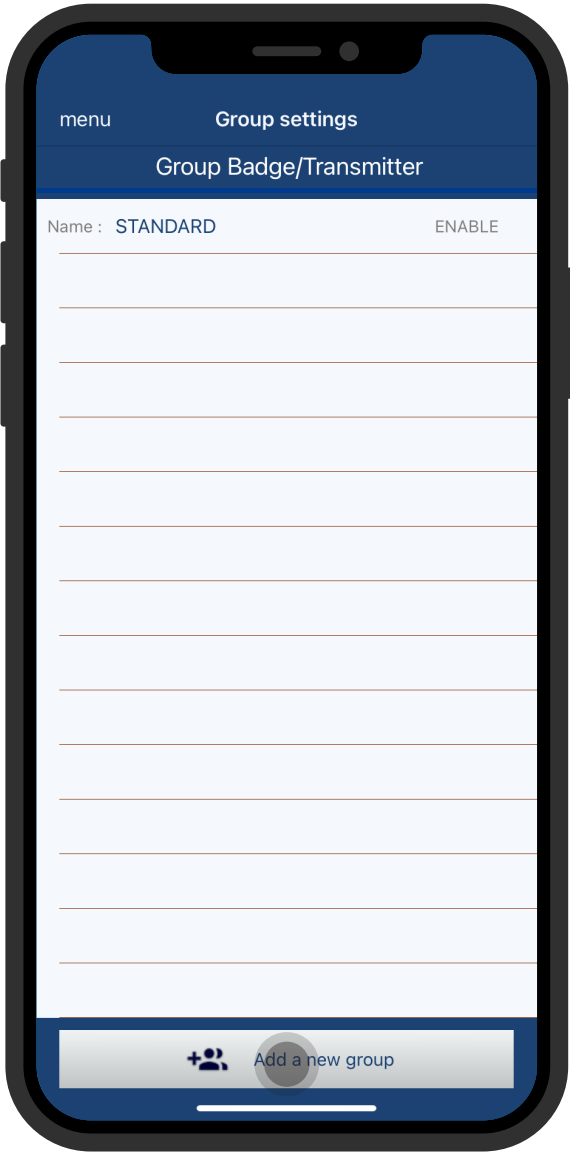


Validate the message of success

4/Group settings

The group management function allows you to control the operation of the installation according to the parameters of the group(s).

The group is used to apply a specific configuration to several users.



In this case we add the GRP 1 group which will be authorised according to the ALWAYS schedule with 2 types of identifiers accepted for RELAY 1 (badges and remote controls) without the bypass function activated.

Groups settings

GROUPS SETTINGS

Group Enable ☒

Name GRP 1

Type Badge/Transmitter

Schedule Always

RELAY 1

RELAY 2

Bypass Conditional entry ☐

Bypass Anti-passback ☐

Validate

Enable or disable the group

Define the group name.

Type of support for your identifiers

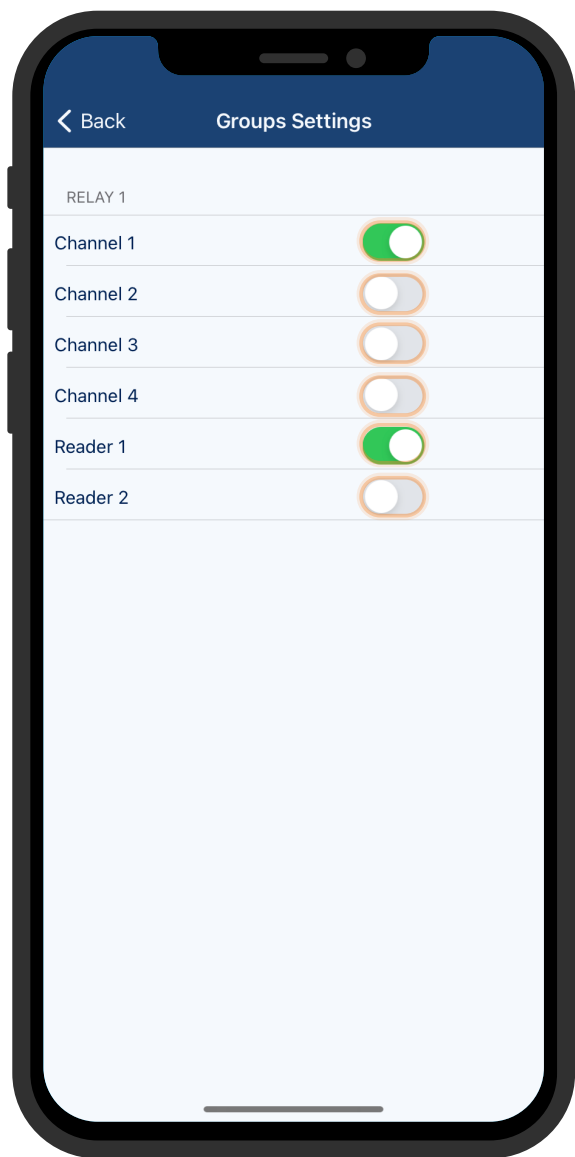
Activate an access authorisation schedule for this group.

Define the association of a radio channel and/or a reader with the relays for this group

Bypass functions:

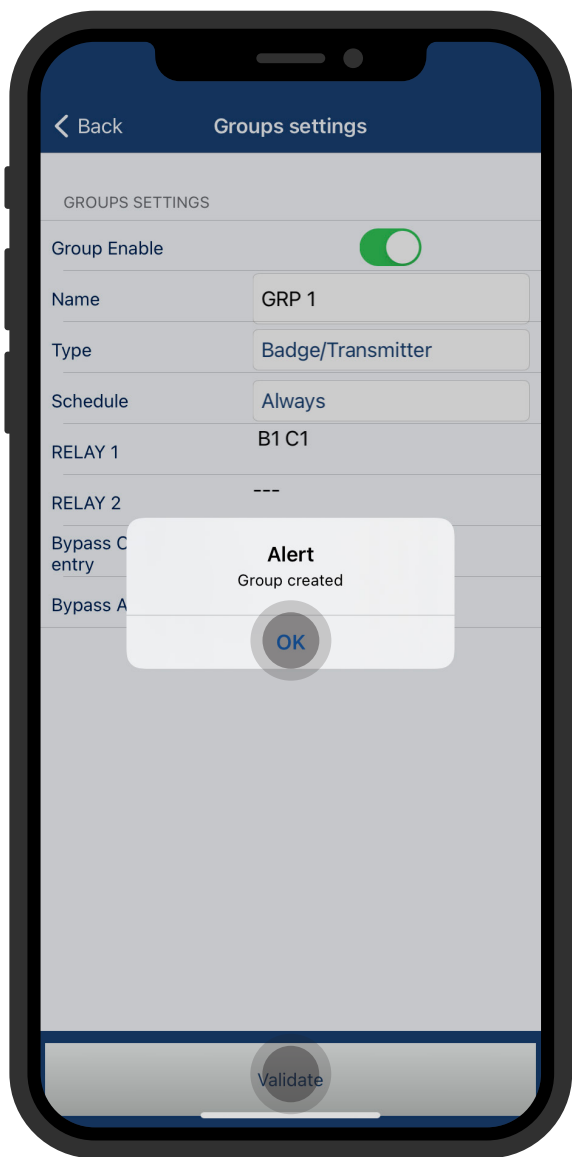
In the case of an installation with activated access conditions such as conditional entry or antipassback (see p.42), when the override is activated, the users of this group are no longer obliged to comply with the activated conditions.

Below is the RELAY 1 setting: here RELAY 1 will be activated when Channel 1 of a registered transmitter is activated or when a registered badge is read by Reader 1.



Define the association of each radio channel and/or readers with the selected relay (here RELAY 1)

When the group is fully set up, press **Validate** and confirm the group creation warning.



5/History

The history function allows access to the database of events such as opening by remote control, smartphone, badge reading or reception of an unknown ID etc...

It is possible to export the list of events in CSV format.

The screenshot shows a mobile application interface for 'Event Management'. At the top, there is a dark blue header with a 'menu' button on the left and the title 'Event Management' in the center. Below the header is a large white area with horizontal lines, intended for a list of events. At the bottom of the screen, there is a dark blue footer containing three controls: a 'Start date' label next to a date input field showing '13/10/2020', a 'Number of days' label next to a numeric input field showing '1' with minus and plus buttons, and an 'Events' button with a circular arrow icon.

 Enter the start date of the history

Select the number of days to be displayed.

Refresh the history according to the parameters defined previously.

menu

Event Management

13/10/2020

10:04:44	37698	Channel 1
Transmitter refused		
10:04:40	17166	Channel 1
Transmitter refused		
10:04:39	17960	Channel 1
Transmitter refused		
10:04:38	17961	Channel 1
Transmitter refused		
10:04:37	17965	Channel 1
Transmitter refused		
09:54:49		
Smartphone connection		
ADMIN		
09:54:39	262200	Channel 1
Transmitter refused		
09:54:36	33	Channel 2
Transmitter refused		
09:47:17	4	
M2000BT restart		

Start date

13/10/2020

Number of days

1

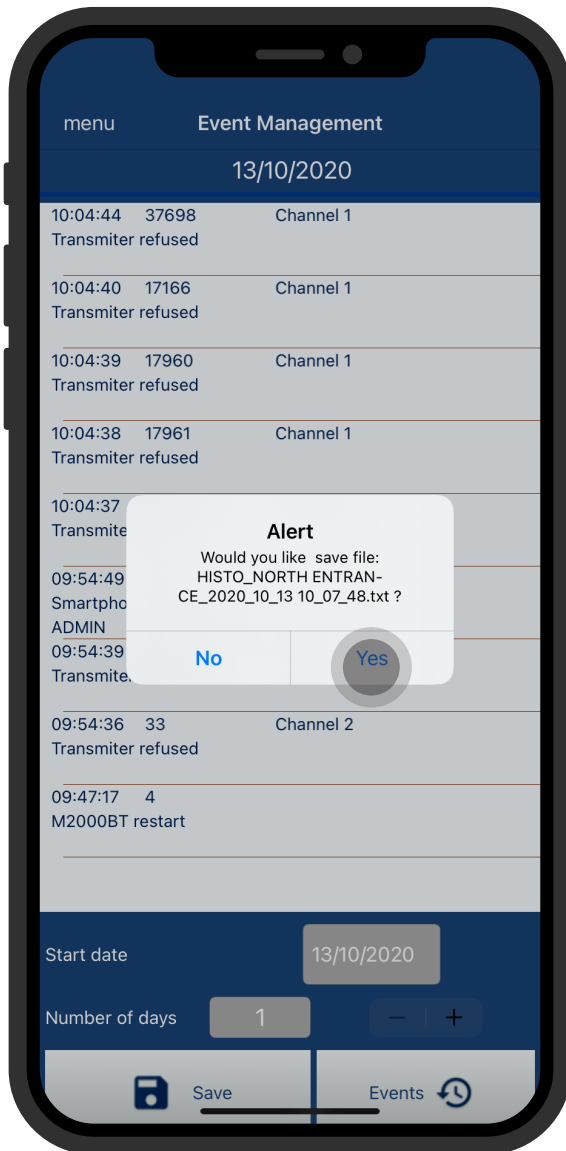
-

+

Save

Events

Press Save to export the resulting history.

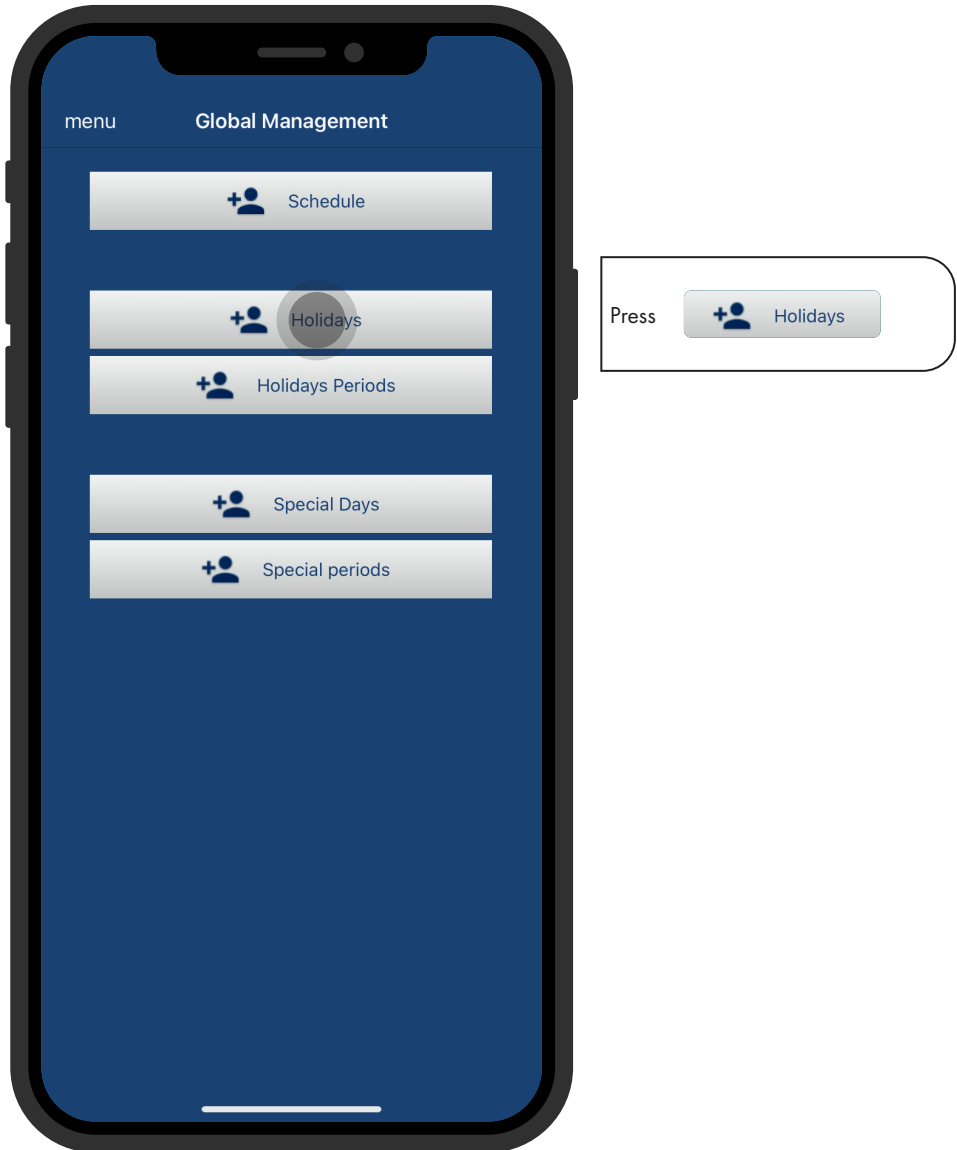


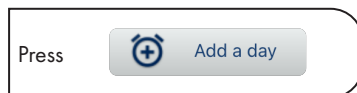
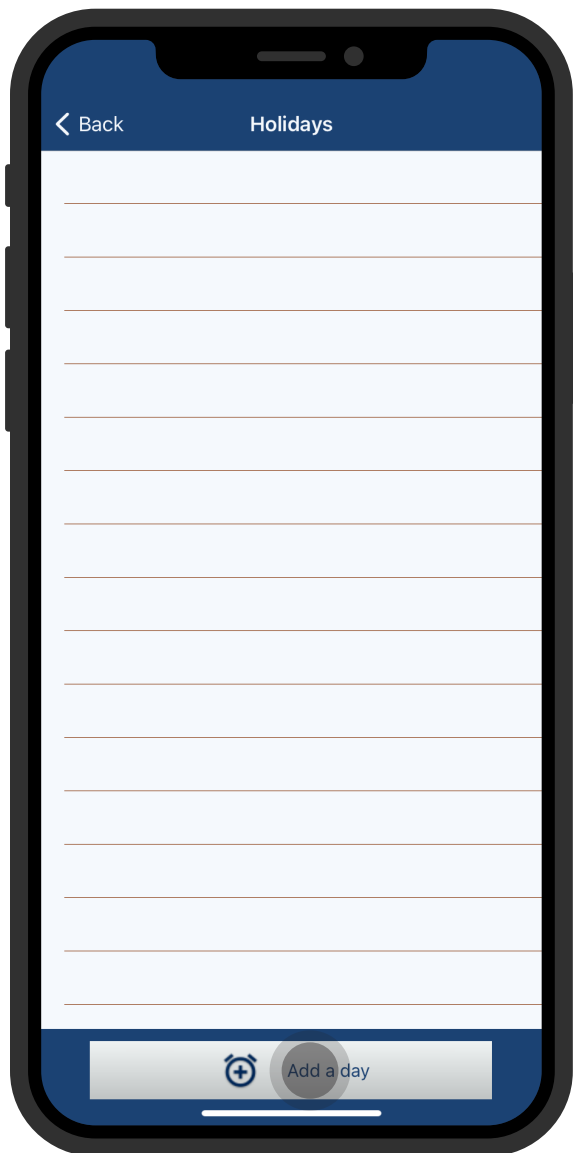
Confirm the export of the history obtained.

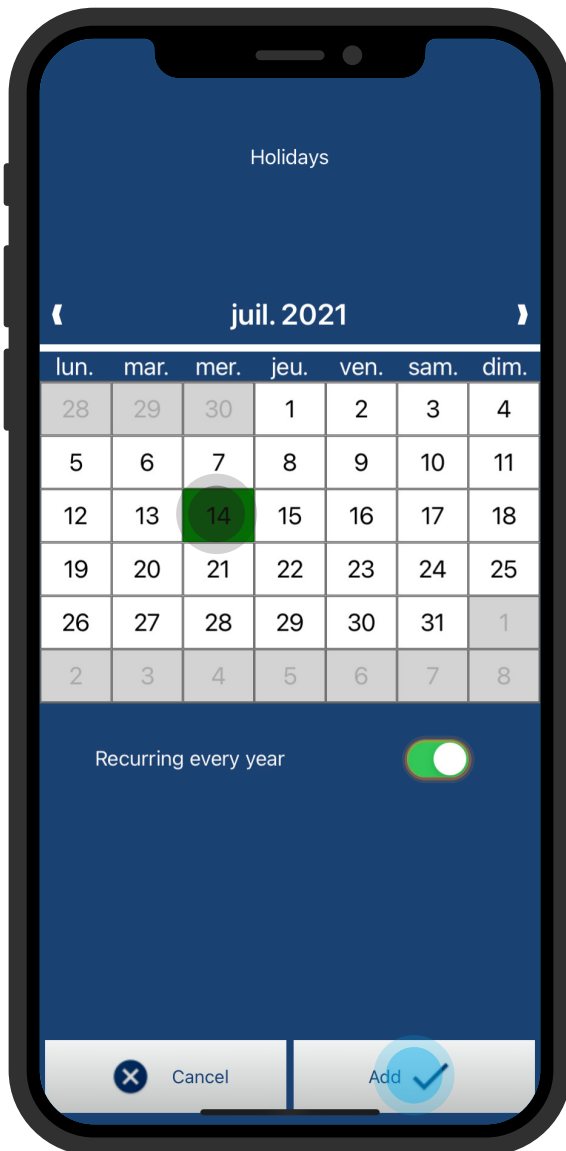
6/Schedule

The time slot function allows you to manage time slots and to add public holidays or special days or periods (e.g. public holiday, open day, etc.).

The following example shows how to add the 14th of July as a recurring holiday every year.





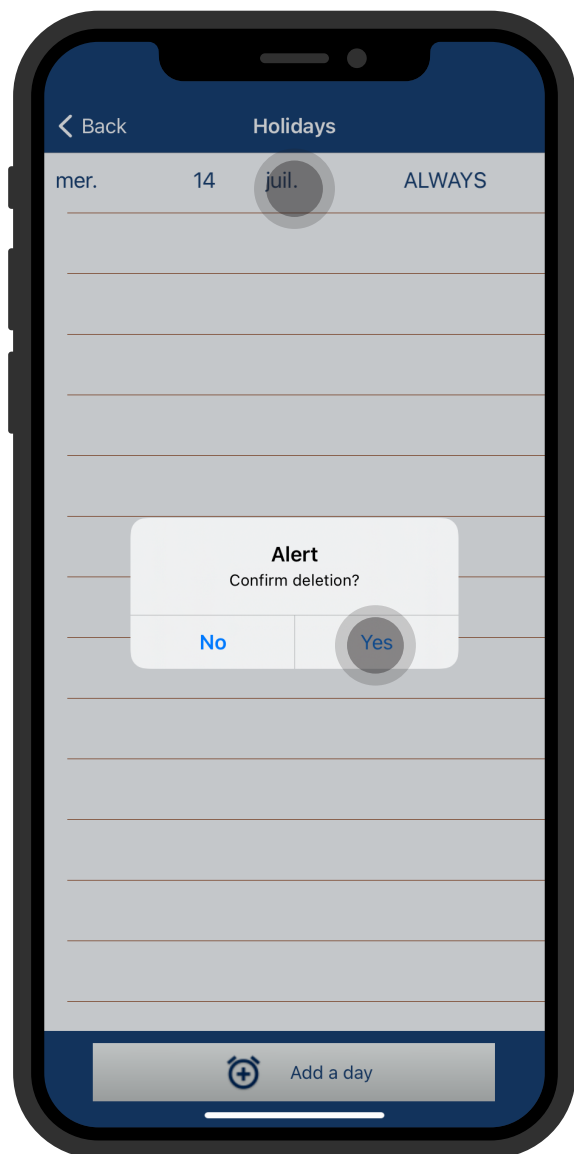


Select the holiday in the calendar (example: 14 July).

Activate the annual recurrence of the holiday.

Press **Add** to confirm the addition.

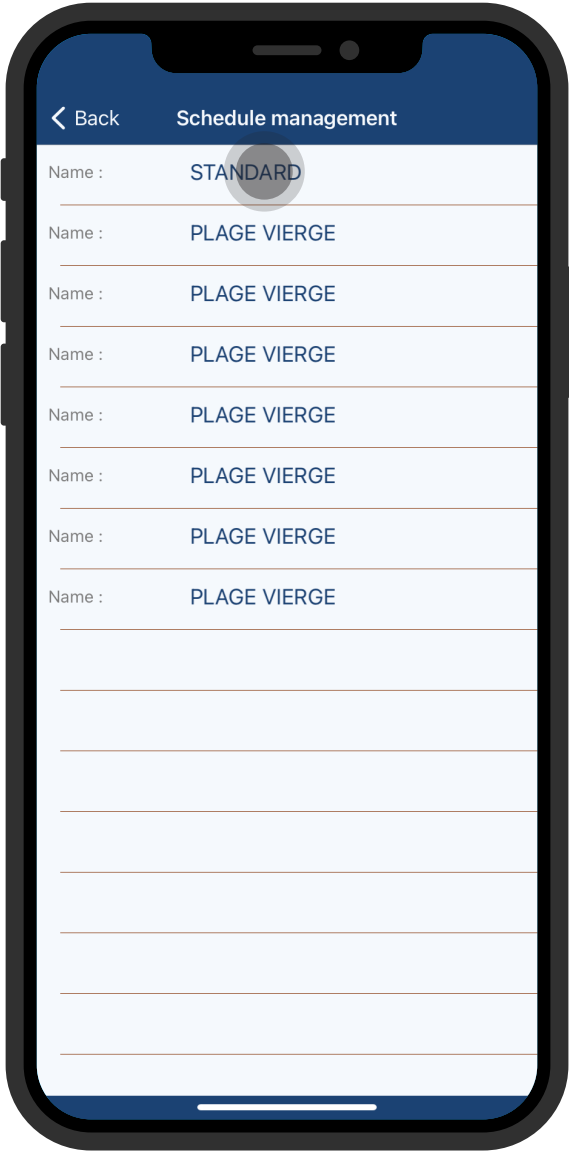
The registered day/period can be deleted by following the instructions below:



Press the day/period to be deleted.

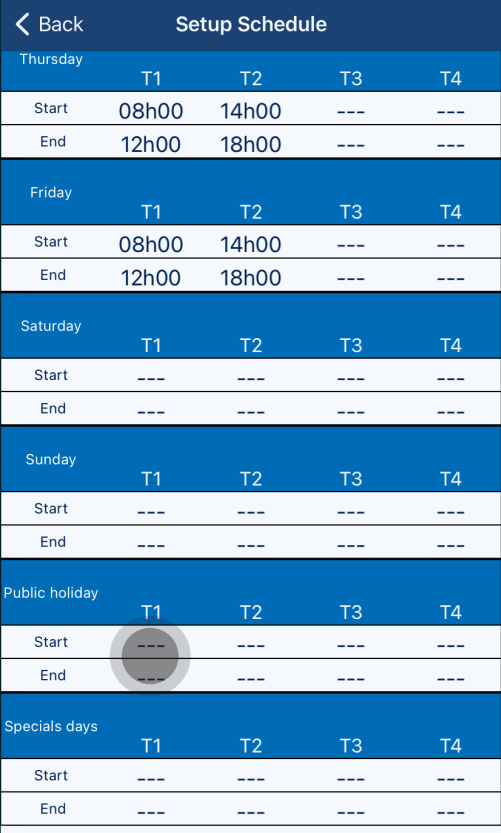
Confirm the deletion message

Select the time slot to be modified: Here we will modify the STANDARD time slot to add a specific time slot for public holidays.
In our example, it will apply to the 14th of July, previously defined as a public holiday.

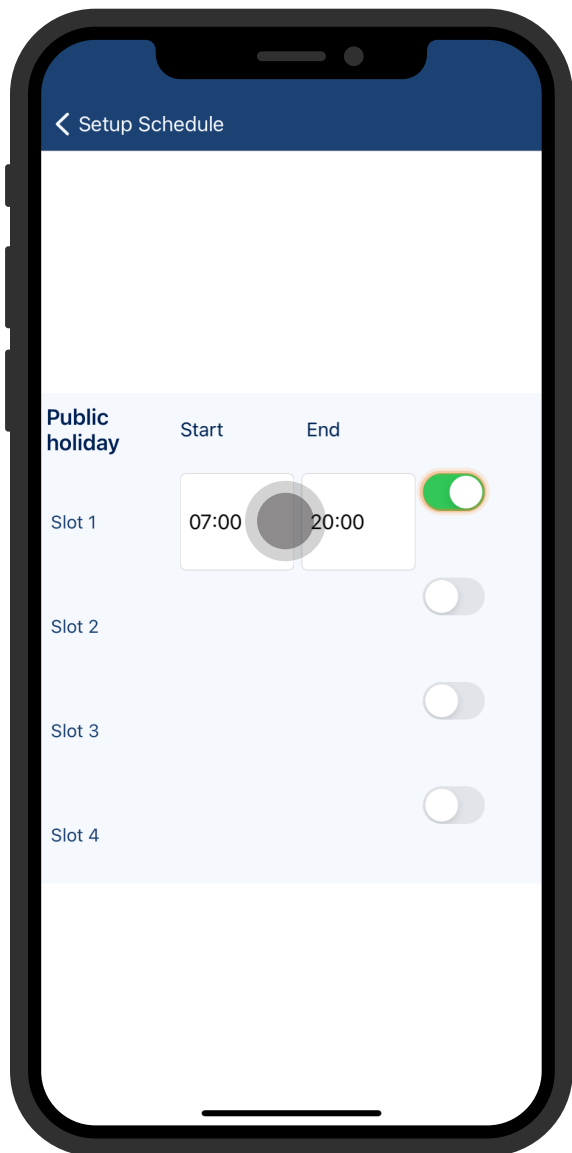


Press the schedule to be changed





Press Public Holiday



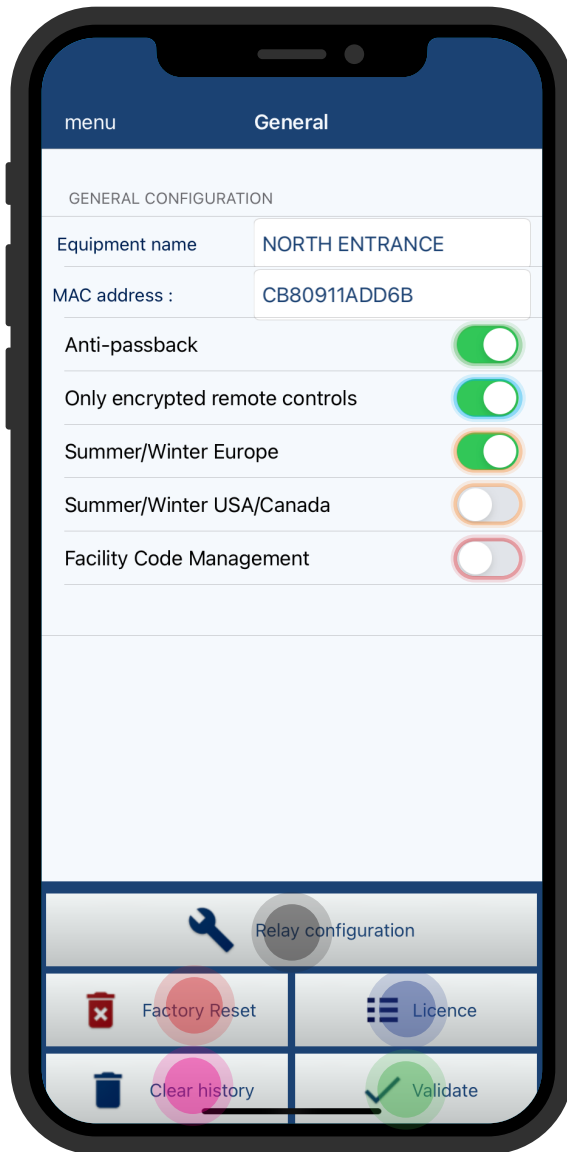
Enable slot 1.

Enter the start and end time of the time slot.



7/Central setting

The following parameters can be managed using the Control unit configuration function:



Activate the Anti-passback function (see p.42).

Enable compatibility with our encrypted remotes only.
Ex: SLIM+, SLIM2E+

Activate the automatic time change according to the selected geographical area.

Activate the management of the site code for DATA entries.
For example for proximity readers such as the MPROXMINI.

 Change the administrator login.
(ADMIN by default).

 Change the password.

 **Relay configuration** : open the relay settings window.

 **Licence** : manage virtual remote control licenses.

 **Validate** : save changes to the control panel and/or administrator login information.

 **Factory Reset** : Reset the control unit to factory settings.

 **Clear history** : delete all events stored in memory.

8/Relay Configuration

The image shows a smartphone screen with the 'Relay' configuration page. At the top, there's a navigation bar with a back arrow and the word 'General', and the title 'Relay'. Below this is a section titled 'RELAY CONFIGURATION'. It contains two identical blocks for 'RELAY 1' and 'RELAY 2'. Each block has a toggle switch at the top (currently turned on, indicated by a green circle). Below the toggle, there are settings for 'Mode' (a dropdown menu set to 'MOMENTARY'), 'Conditional input' (a toggle switch, currently off), 'Door contact' (a toggle switch, currently off), 'Schedule reading ID' (a dropdown menu set to 'Always'), and 'First person In delay schedule' (a dropdown menu set to 'NEVER'). At the bottom of the screen, there is a 'Validate' button with a checkmark icon.

Enable or disable relays.

Relay operating modes:

- MOMENTARY: active for a short time.
- BISTABLE: changes state with each valid order.
- TIMED: active for a defined period of time.

Adds an extra validation act to the activated badge or remote control. For example, activate it when you a magnetic loop contact will allow the presence of a vehicle to be added to activate the conditional entry. (see p.41).

Activate if you need to use the relay as an alarm.

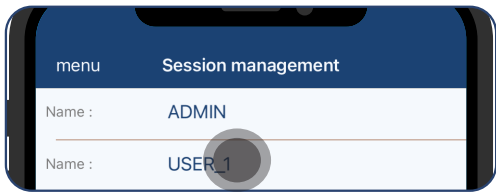
Activation of a schedule for reading IDs.

Activation of schedule for passage authorisation or forced opening on the relay.

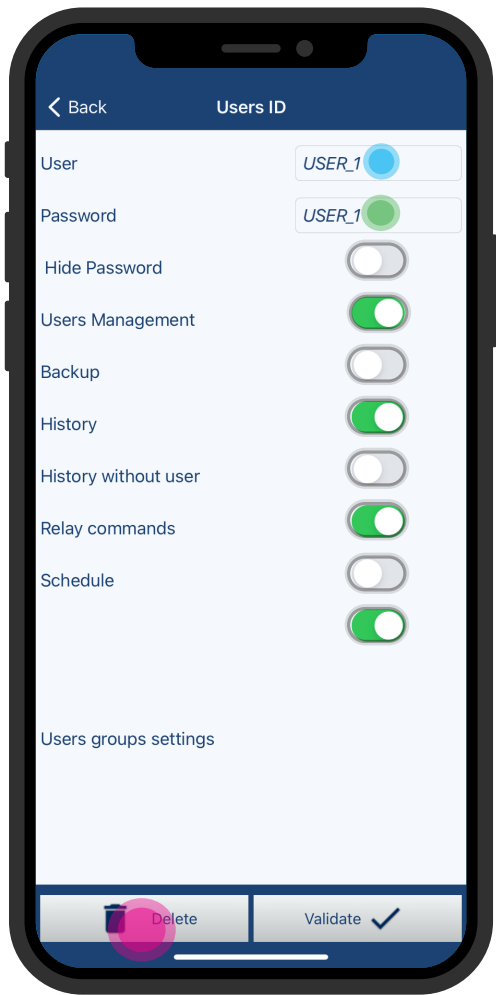
The first person in feature set the activation of a pre-planned schedule when the first authorized credential is used.

9/Session management

The Session Management function allows you to add and manage user sessions with the selected rights.



Press USER_1



Change the user's login.

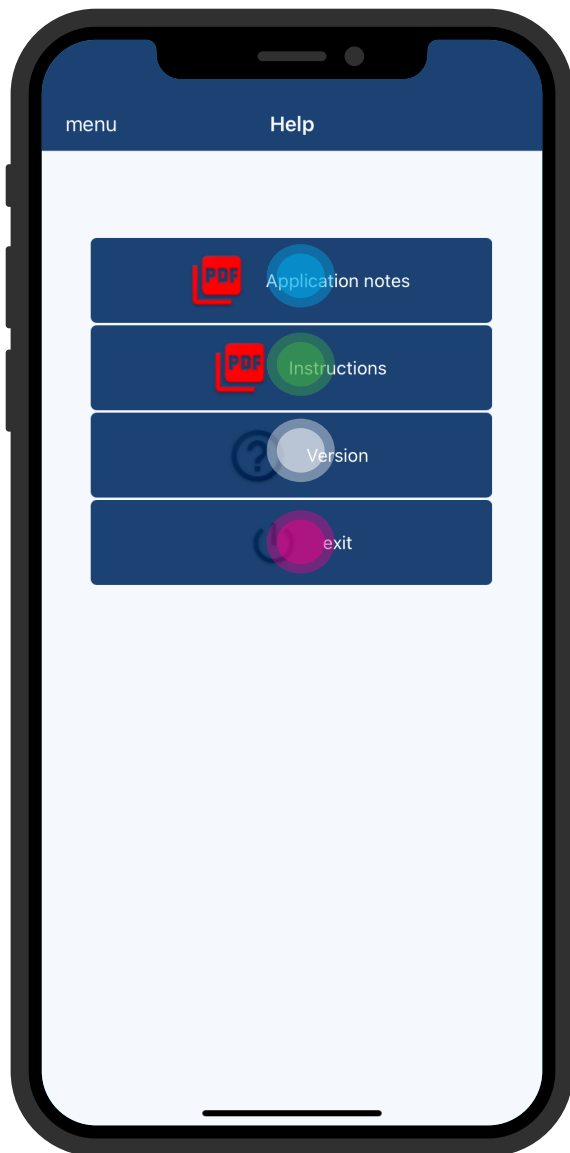
Change the user's password.

Change the user's access rights to the functions of the application.
For example, a user may be allowed to access the history only.

Delete user.

10/Help

The Help function provides access to information useful for the correct installation of the control unit.



Link to the latest version of this guide.

Link to the technical instructions for the installation of the control unit.

Displays the version of the control unit and the application.

Quit the application.

11 / Language

The Language function allows you to change the language of the application.

