First Access Cloud

QUICKSTART GUIDE

September 2024

Cansec Systems Ltd.

Cutting edge simplicity

Table of Contents

Step 1. Software Installation **3**

Step 2. Software Configuration **3**

Step 3. Panel and Reader Definition **4**

- Add Panel 4
- Add Reader 5

Step 4. Schedules, Profiles, Users and Operators **7**

- Access Schedules 7
- Unlock Schedules 8
- User Profiles 8
- Add Cardholders 10
- Search, Edit and Delete Cardholder 12
- Operator Profiles 14

Cardholder and Credential Report **16**

Audit History **17**

Elevator **18**

- Floor Groups, Access Groups and Floor-Unlock Schedule 18
- Add Elevator Panel 21
- Manage Elevator Floors 22

Software Update **24**

Cansec MSM App **25**

Troubleshooting **35**

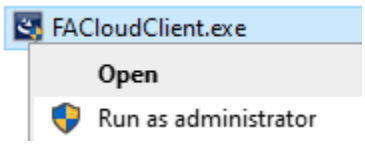
CAUTION: EMERGENCY LOCKDOWN

Emergency lockdown functions must operate totally independent of the access control system and must not rely on operation of card readers, access control panels, communications networks, communications devices or host software. Cansec accepts no responsibility for direct or consequential damages resulting from the failure of emergency lockdown functions which are dependant in any way on the operation of card readers, access control panels, communications networks, communications devices or host software.

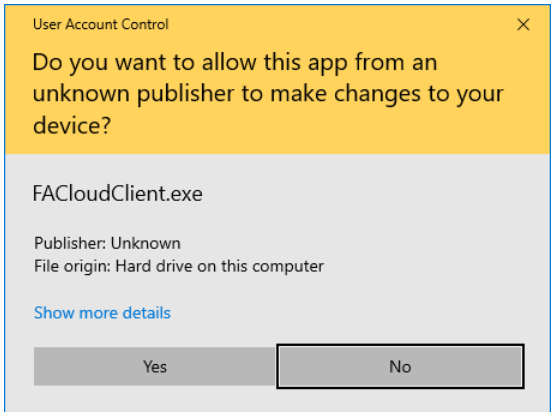
Copyright © 2024 Cansec Systems, Ltd.

Step 1. Software Installation

1. Log on to the computer with an administrative account.
2. Download **First Access Cloud Client** software from www.cansec.com/downloads.
3. Unzip and open the folder First Access.
4. Right click on FACloudClient.exe and select Run as administrator.



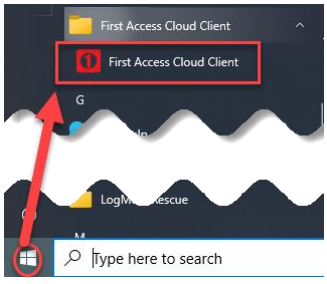
5. When prompted, select **Yes** to continue.

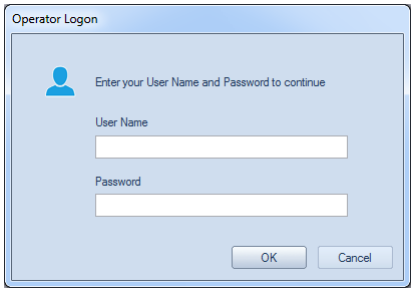


6. Read and accept the terms of the license agreement then follow the on-screen instructions to finish the installation.

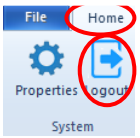
Step 2. Software Configuration

1. Launch First Access Cloud Client from the Start menu of Windows.





Manual logout can be done by clicking on logout button

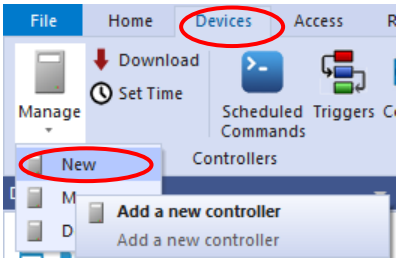


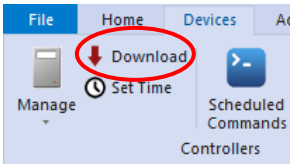
2. Use your login credential to log on.

Step 3. Panel and Reader Definition

ADD PANEL

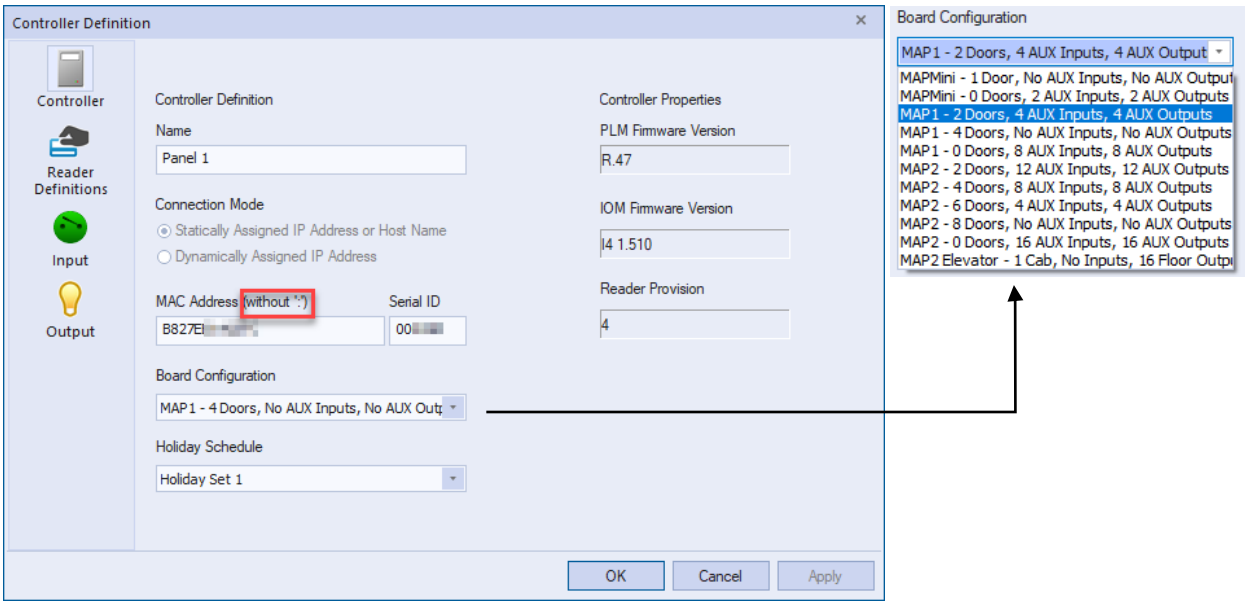
1. Select **Devices->Manage->New.**





Perform download whenever a new panel is added or whenever necessary

2. Enter a name for the panel, e.g. *Panel 1*. Select board configuration. The factory default configuration is 2 Doors.



3. Enter the MAC address, without colons :, and SID of the panel or controller then select an appropriate board configuration

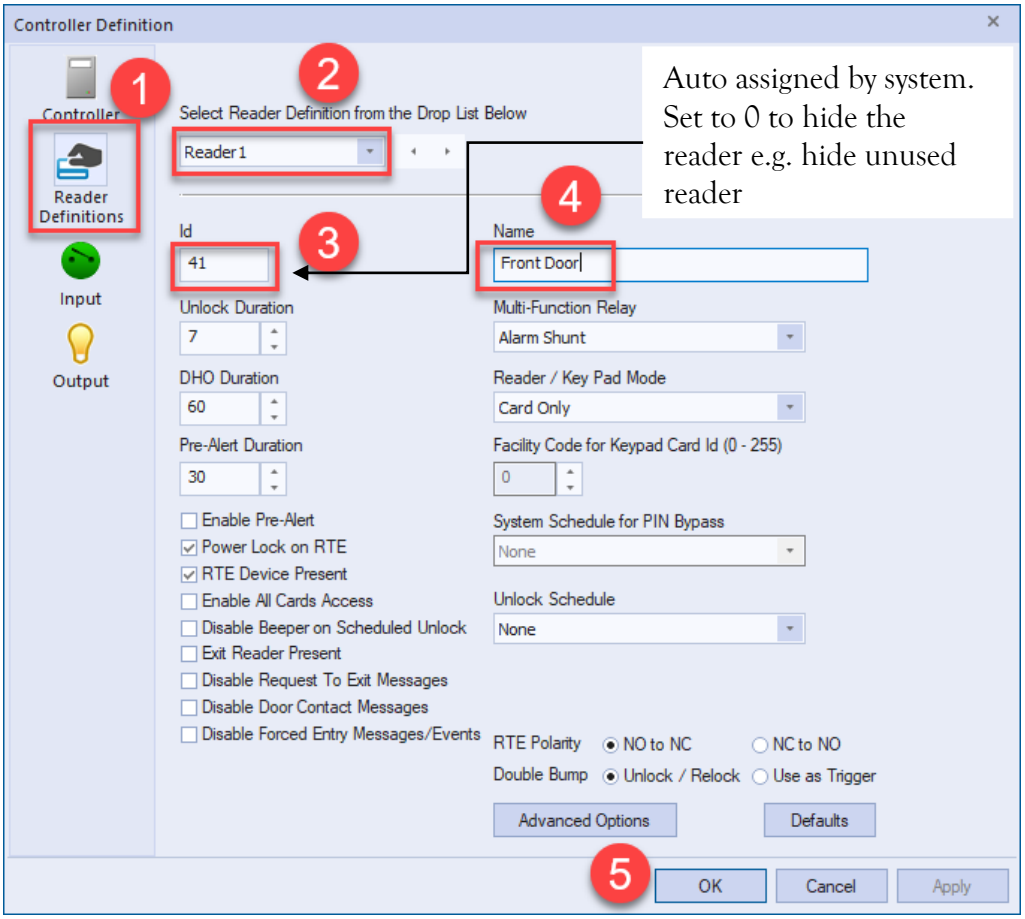
Aux Inputs/Outputs: Applicable to all controllers but MAP1 is used as an example below.

MAP1 handles 2 or 4 doors. If you purchase 2-door MAP1 then only 2 doors are enabled along with their dedicated inputs (REX & Door Contact) and dedicated outputs (MF outputs and lock outputs). The remaining inputs/outputs of the 2 unused doors can be used as auxiliary inputs/outputs. If you purchase 4-door MAP1 then no inputs/outputs left that can be used as auxiliary input/outputs.

MAP2 Elevator: Supports 1 elevator cab. No inputs are supported. All outputs are reserved for managing elevator floors. Additional hardware can be added to control more than 16 floors, up to 64 floors.

ADD READER

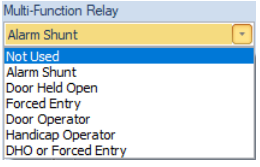
1. Select ***Reader Definitions***. Reader Id is auto-generated by selecting it. **Note**: *Reader with Id 0 is an undefined reader*. Each reader has its own unique Id. Use the drop-down arrow or the left and right arrows to select the desired reader.



2. Select an unlock duration, in seconds (60 seconds max.), for the door when a valid credential is presented or when an exit button is pressed.

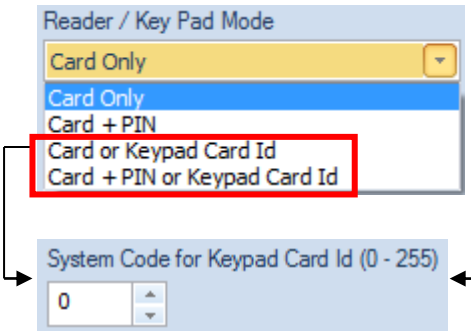
3. Select a **DHO** (Door Held Open) time (300 seconds max.) for the panel to wait before activating the multi-function relay when the door is left open for too long. This requires the door to have a door contact installed and the multi-function relay configured as **Door Held Open** relay.

4. Select the desired function to assign to the multi-function relay.

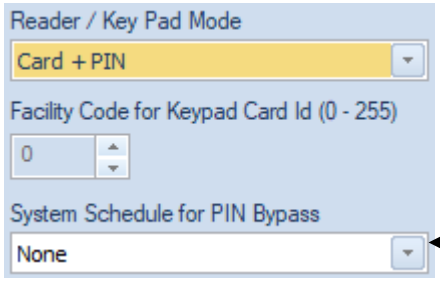


5. Select an optional unlock schedule. There are 255 available unlock schedules. The unlock schedule, when defined and used, allows the door to automatically unlock and relock at pre-defined times. If not used, select **None**.

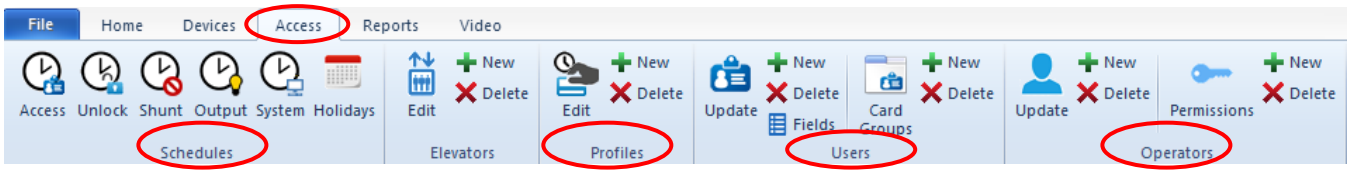
6. If using keypad select one of the available modes below.



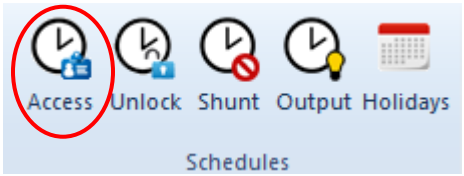
System/Facility Code (between 0 and 255 inclusive) must be entered whenever *Keypad Card Id* is involved. Not required for **Card Only** mode or **Card + PIN** mode.

Card Only	*Only cards or card numbers entered as a PIN.*
Card + PIN 4-bit bust programming card provided with Cansec P-620 or P-640 keypad	*Card presentation followed by PIN entered from keypad. Optionally, select a system schedule you have defined to bypass PIN requirement.* 
Card or Keypad Card Id (For P-620 or P-640 keypad, use provided 4-bit bust programming card to program the keypad. See keypad manual for more info)	*Card presentation or use keypad to enter card number e.g.* (asterisk) * **card number** # (pound)
Card + PIN or Keypad Card Id (For P-620 or P-640 keypad, use provided 4-bit bust programming card to program the keypad. See keypad manual for more info)	*Card presentation followed by PIN entered from keypad or use keypad to enter card number e.g.* (asterisk) * **card number** # (pound)

Step 4. Schedules, Profiles, Users and Operators

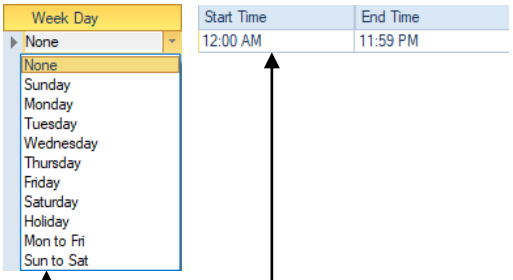


ACCESS SCHEDULES

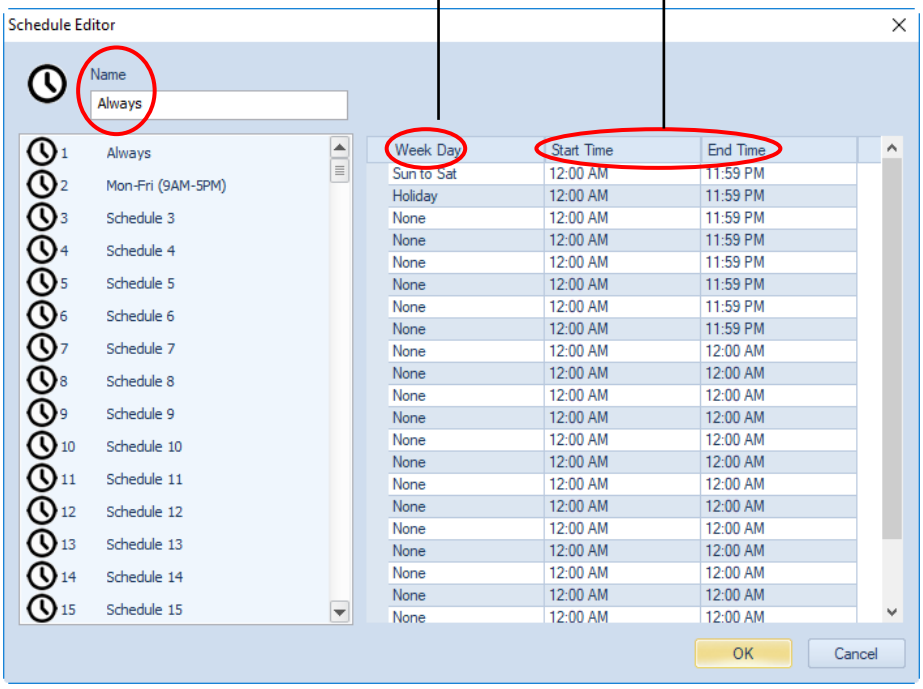


Note: *There are 24 available intervals shared between weekdays (7 days from Sunday to Saturday) and a holiday (1 day) for a total of 8 days. Several intervals can be defined within a day, e.g. Monday 9:00AM to12:59PM and Monday 1:00PM to 5:00PM. More than 3 intervals can be defined within a day as long as the number of intervals for the 8 days (Mon to Sun and Holiday) does not exceed 24.*

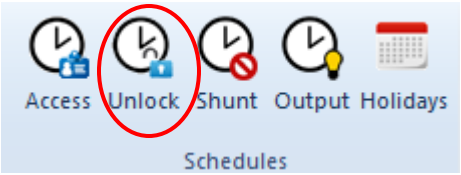
Access schedules specify when cardholders can use their credentials to access a door.



1. Click the **Access Schedule** icon.
2. Select one of the 255 available access schedules.
3. Enter a name for the access schedule, e.g. *24/7 or Always*.
4. Select an option for the Week Day. Double click on hour, minutes and period (AM or PM) to modify times accordingly. Click **OK** when done.

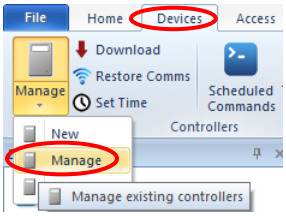


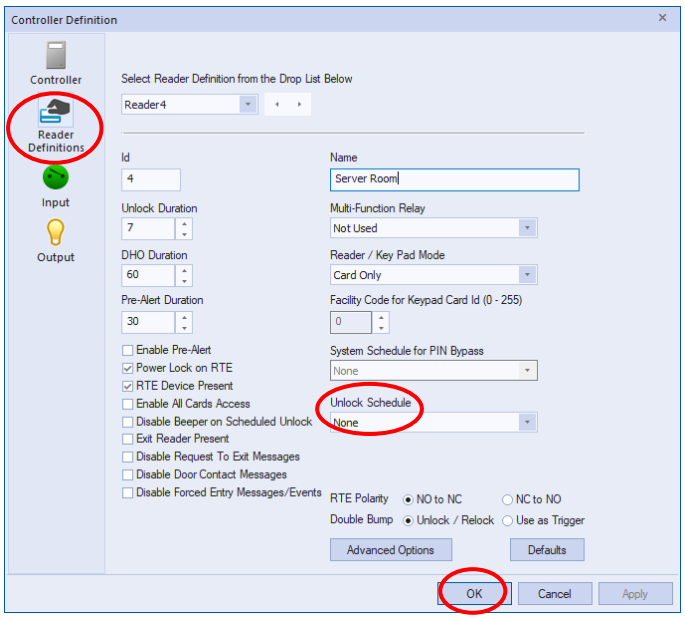
UNLOCK SCHEDULES



Unlock schedules are used to automatically unlock and relock a door at specified times.

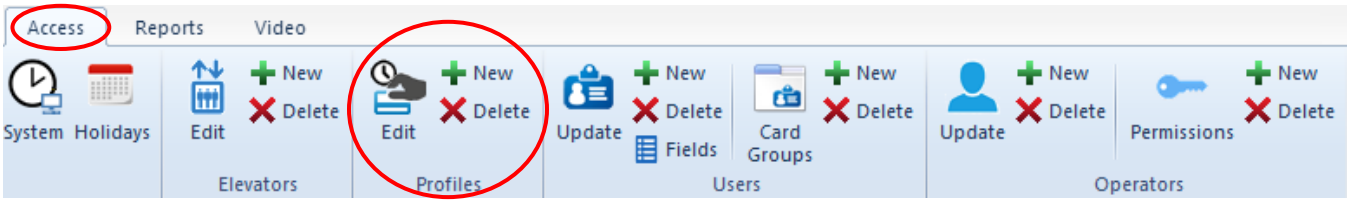
1. Click on the Unlock icon.
2. Select one of the 255 available unlock schedules.
3. Enter a name for the access schedule, e.g. *M-F 8AM-5PM.*
4. Select the day of the week. Double click on hour, minute and period (AM or PM) to modify times accordingly.
5. To assign an unlock schedule to a door, select **Devices->Manage** and select a desired panel. Select **Reader Definition** and select an unlock schedule to assign to that door.





6. Click **OK** when done.

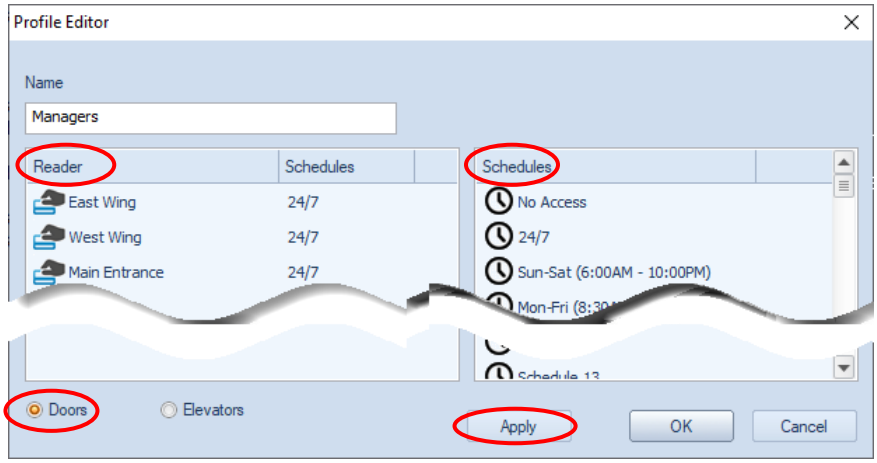
USER PROFILES



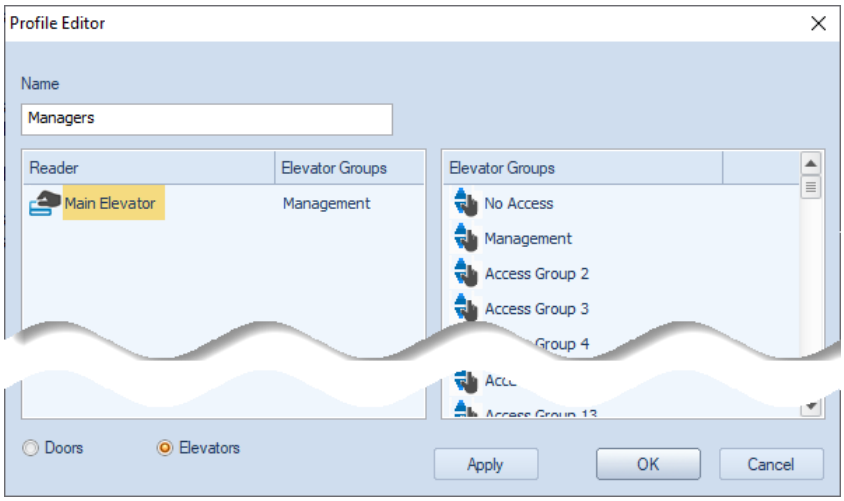
User profiles specify which doors a group of cardholders can access, and the time during which access will be granted at each door. To create a new user profile:

1. In **Profiles** section, click the **+New** icon.

2. Enter a name for the profile, e.g. Managers.

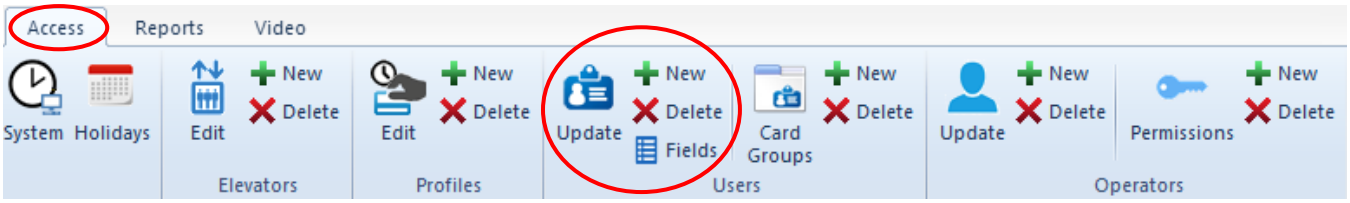


3. For **Doors**, select a reader on the left panel and select a schedule on the right panel to assign to the reader. Click **Apply**. Repeat the same step for other reader(s) if necessary. If there is no elevator then skip steps related to elevator and click **OK** to finish.
4. For **Elevators**, select the elevator on the left panel and select an elevator group on the right panel to assign to the elevator.



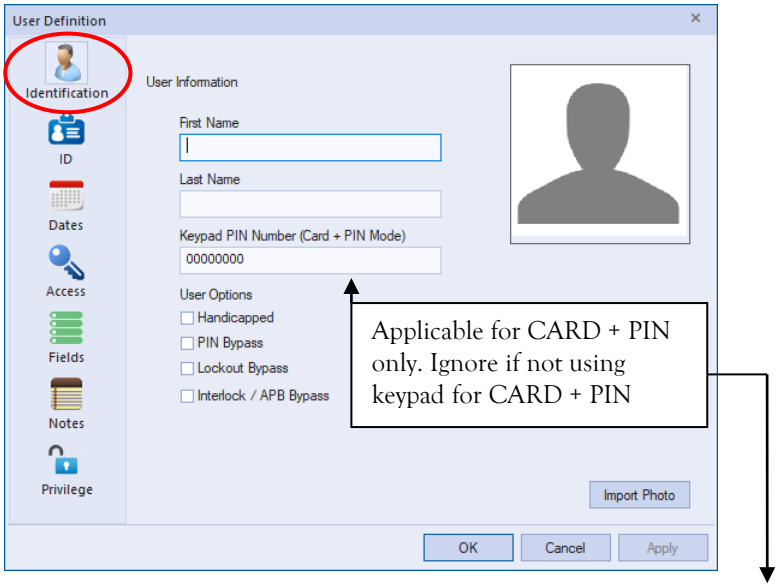
See Elevator section in this document for more information

5. Cardholders who belong to this profile will only be able to access the readers or doors during the times specified in the associated access schedule. Likewise, if elevator is assigned then cardholders in this profile can only access elevator floors specified in that elevator group e.g. *Management*. See **Elevator** section for more information about elevator group and how to define elevator groups.
6. Click **OK** when done.

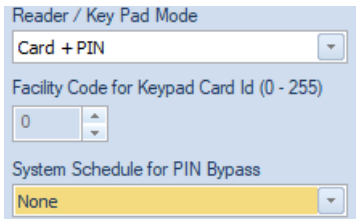


➢ Card Holders

1. In the **Users** section, click the **+New** icon. beside the update button.

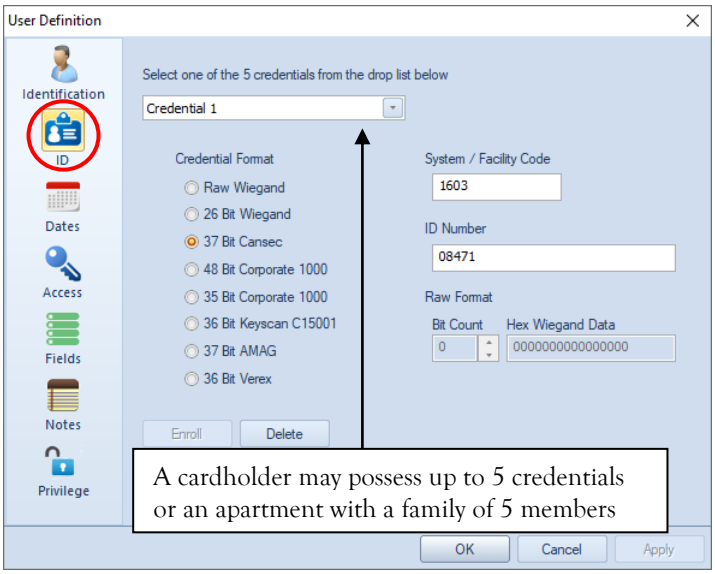


2. If Card + PIN is used, create/enter the PIN number for this card. To bypass PIN requirement for certain day and times, create and select a system bypass schedule. *In this mode, the card must be presented followed by the PIN number followed by #.*

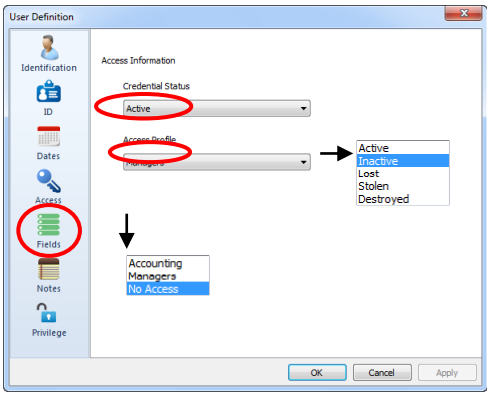


- Handicapped: *The door operator will be energized when this cardholder swipes his/her credential. Note: The door operator must be installed and hooked up to the MAP controller using the Multi-Function relay which must be set to Handicap Operator mode.*
- PIN Bypass: *This cardholder is exempted from entering the PIN when Card + PIN is required*
- Lockout Bypass: *This cardholder is granted access when reader is in lockout mode*
- Interlock/APB Bypass: *This cardholder is granted access when reader is in interlock or anti-passback mode*

3. In the **ID** tab, select a credential from the drop-down list. Select a credential format. For **Raw Wiegand** present the credential to the enroller (purchased separately) and click **Enroll**. For other Wiegand formats simply enter the system/facility code and the credential number in the field **System/Facility Code** and **ID Number** respectively.

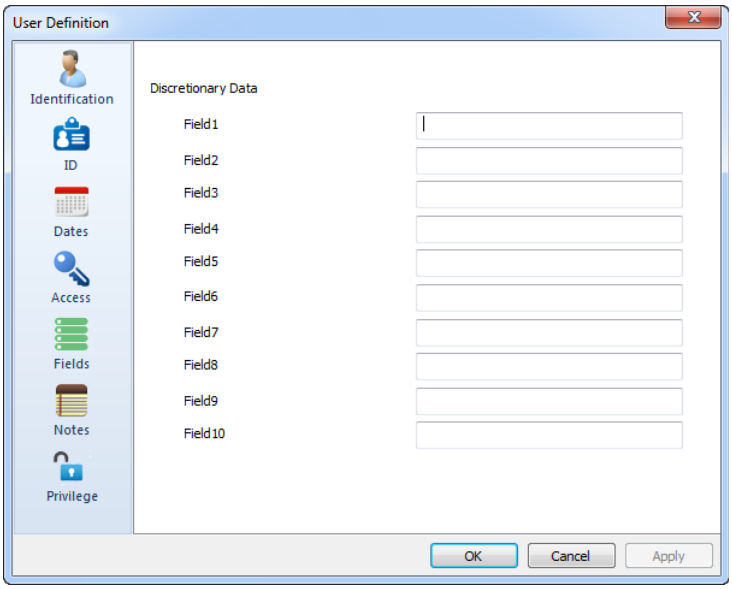


4. In the **Dates** tab, select the dates and times for the credential to be automatically validated and automatically expired.

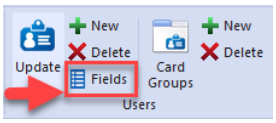


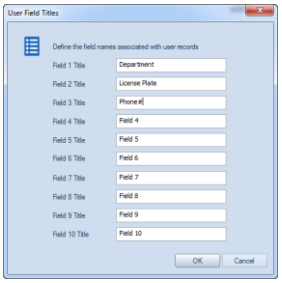
5. In the **Access** tab, select a **Credential Status** and select an **Access Profile** previously created. For new credentials, set the credential status to **Active.**

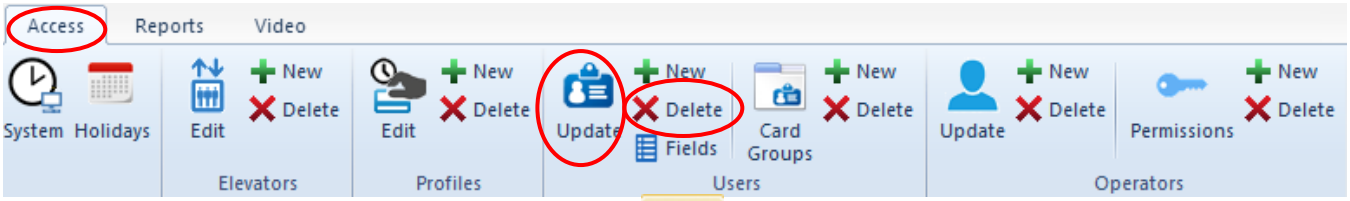
6. In the **Fields** tab, enter optional information in the 10 available fields, e.g. *Phone #*, *Parking lot #*, *Car license plate*, etc.



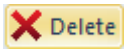
*The field titles e.g. Field1, Field2 etc... can be renamed as desired by selecting **Fields** from the **Users** menu and modify the titles accordingly.*



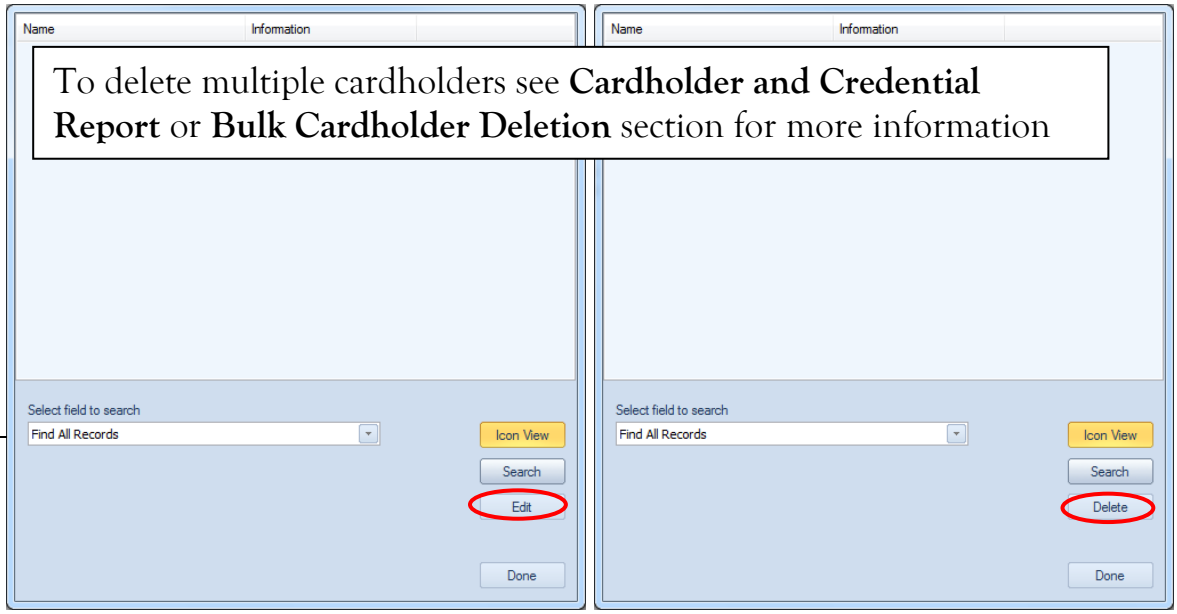




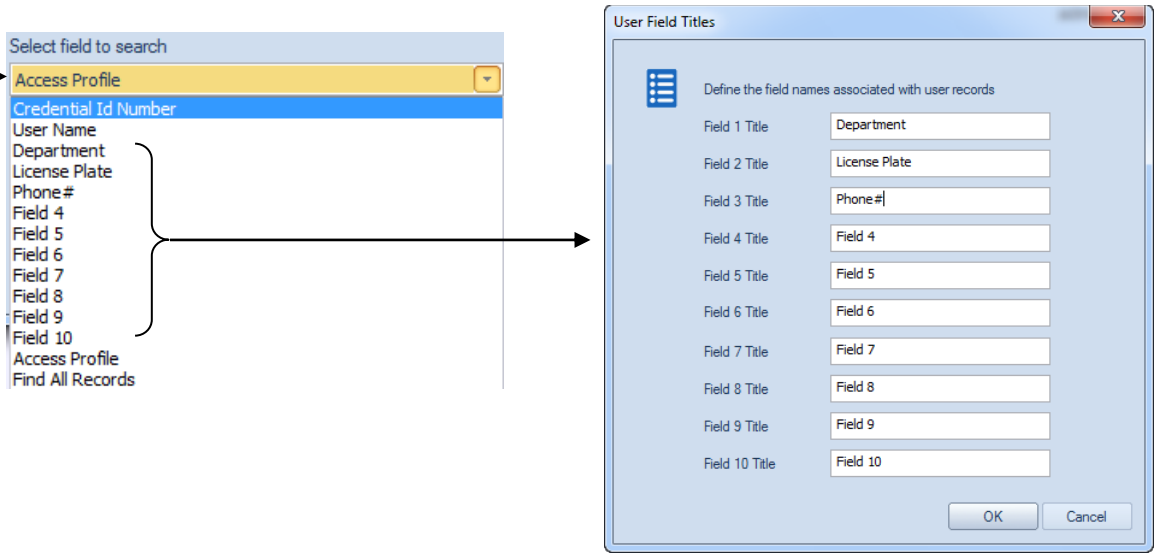
1. To edit or delete a cardholder, click the

or 

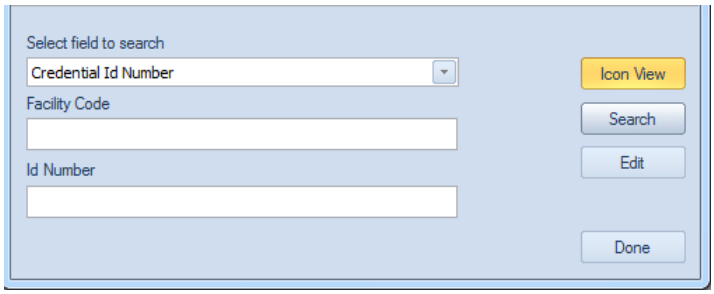
button respectively.



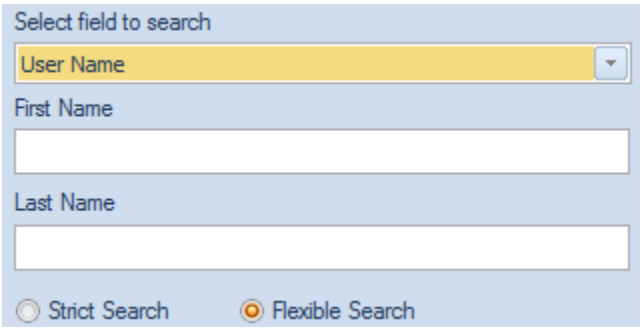
2. Select a desired option to search for e.g. *All Records*, *User Name* etc....



3. To search records by Credential ID select **Credential Id Number**. If only *Facility Code* is entered then the result will be all credentials having that facility code. Similarly, if only *Id Number* is entered then the result will be all credentials having that *Id Number*. However, if both *Facility Code* and *Id Number* are entered then the result will just be one unique credential having that *Facility Code* and *Id Number*



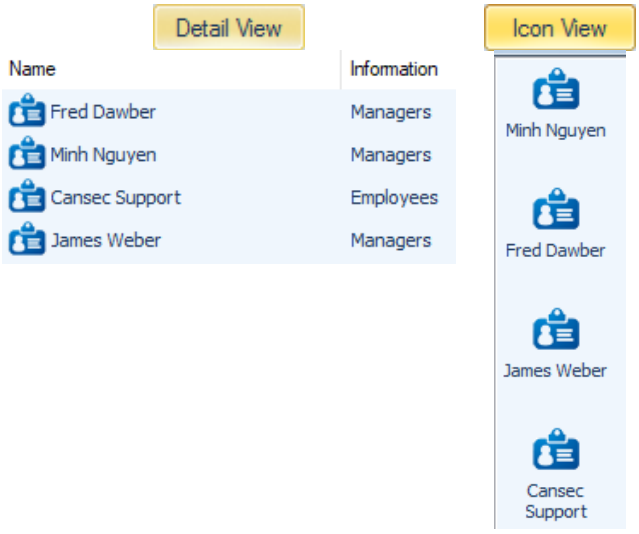
4. To search records by user name select **User Name** and enter either First Name or Last Name or both to search.



Strict Search: *Requires full or complete information to be entered e.g. John not Jo will search for all first names having John. Option applies to both First and Last Name.*

Flexible Search: *Allows partial information to be entered e.g. Jo instead of John will search for all first names having Jo as the first 2 characters (John, Joe etc…). Option applies to both First and Last Name.*

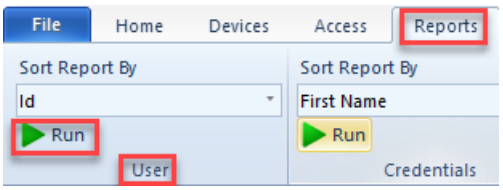
5. Results can be viewed in either detailed mode Detail View or icon mode Icon View



6. To edit a record, select it and click button Edit

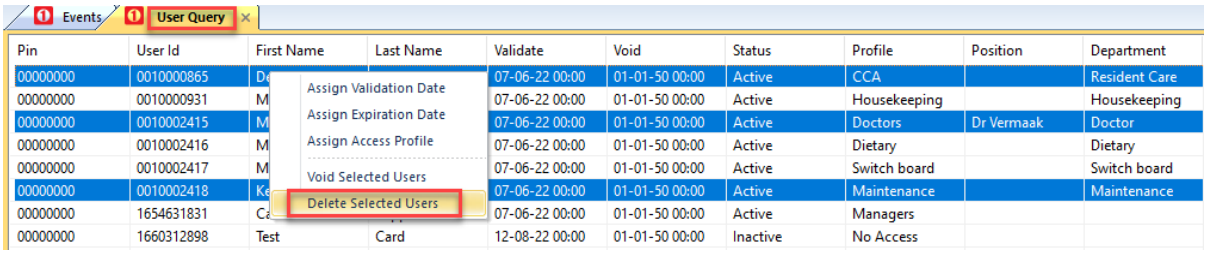
➢ Bulk Cardholder Deletion

To delete multiple cardholders select Report, under User section select Run

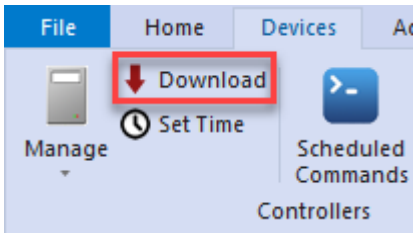


See **Cardholder and Credential Report** section for more information

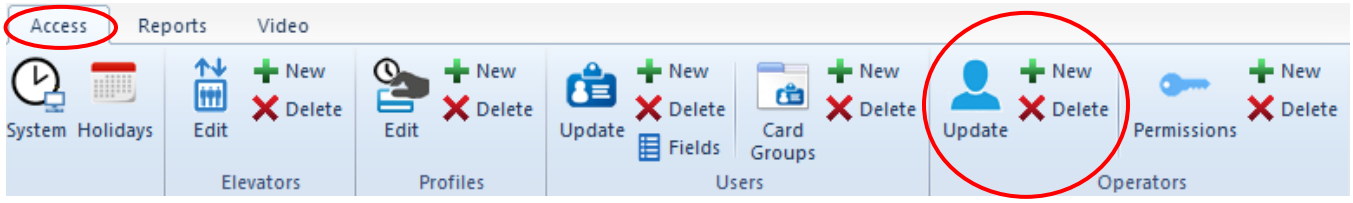
Select all or desired records then right click to display a pop-up menu. Select "Delete Selected Users".



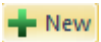
Note: *Communication must be established between the software and controller for the modified or deleted user record to be updated from the controller. If there is no communication when the modification or deletion is performed, the user record will remain in the database. When communication is resumed, a manual download from the software is required to update the controller.*

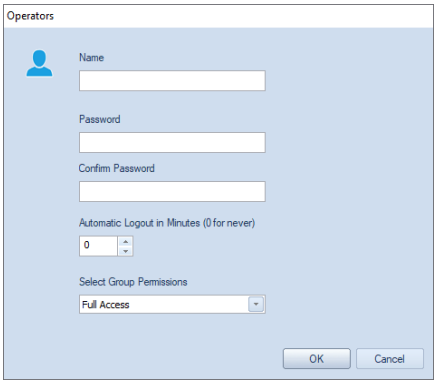


OPERATOR PROFILES



Operators are personnel who are authorized to login and manage the software and controllers or panels.

1. In the **Operators** section, click the **+New** icon  to create new operator.

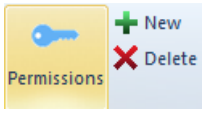


2. Enter a short operator name e.g. Cansec.
3. Enter the password and enter it again on the next line to confirm.
4. Enter the idle time out in minutes to automatically log the operator out of the software. Enter 0 for the software not to log out at all.
5. Select an appropriate group to assign to the operator. *See Operator Group Permission section.*

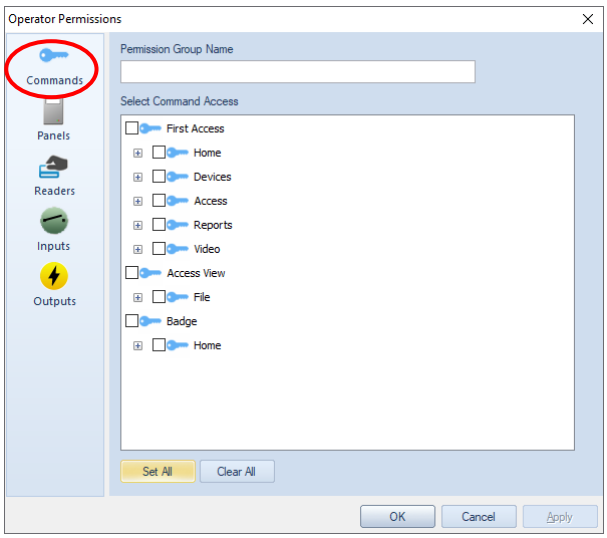
❖ Operator Group Permission

Operator group permissions provide options to create different operator groups with individual permissions for devices and commands. There default operator group has full permissions assigned.

1. Select

from 

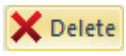
to create a new group.

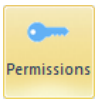


Select commands alone do not allow commands to apply to anything. Devices must also be selected for the commands to be applied to

Video and Badge are add-on software which must be purchased separately. Video deals with local NVR integration and Badge deals with photo badge.

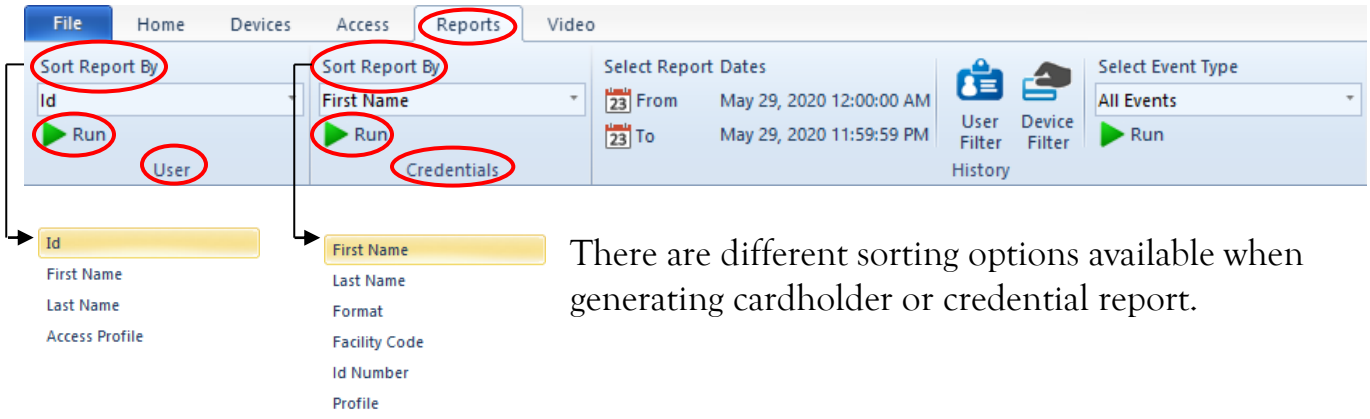
2. Enter a name for the group e.g. Restricted or HR or Security Guard etc...

3. Select desired commands and panels, readers, inputs and outputs points that you would like operators to have access to.
4. Click **OK** to save. If necessary, follow the same steps above to create multiple groups with different permissions.
5. To delete a group, select 

then select a desired group to delete.
6. To modify permissions for a group select 

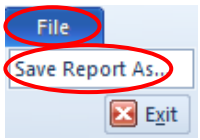
then select a desired group to modify permissions.

Cardholder and Credential Report

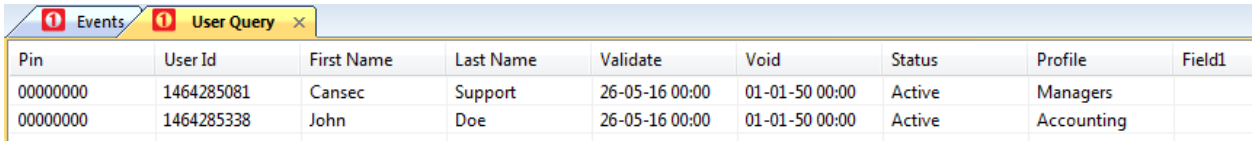


There are different sorting options available when generating cardholder or credential report.

➢ **User Report** – display all the users

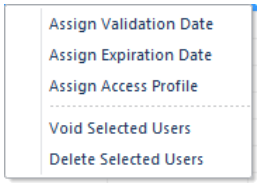


1. Pick the **User** then select a desired sorting option.
2. Click **Run**. Save report in csv format if necessary.



Pin	User Id	First Name	Last Name	Validate	Void	Status	Profile	Field1
00000000	1464285081	Cansec	Support	26-05-16 00:00	01-01-50 00:00	Active	Managers	
00000000	1464285338	John	Doe	26-05-16 00:00	01-01-50 00:00	Active	Accounting	

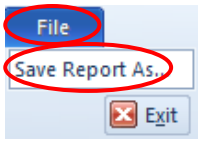
Optionally, select a cardholder or select multiple cardholders and right click to display a pop-up menu from which quick commands can be performed. This can be used to assign multiple cardholders to a common validation date, expiration date or to a common access profile. Multiple cardholders can also be:



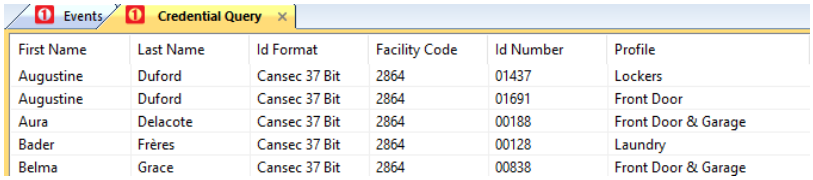
- Voided – *Credentials' status are set to* **Inactive**. *Access is not granted at any door. However, the records are kept in the database for the purpose of potential re-activation.*

- Deleted – *The records are permanently deleted from the database and from the controllers. Access is not granted at any door.*

➢ **Credential Report** – display all the credentials of the users



3. Pick the **Credentials** then select a desired sorting option.
4. Click **Run**. Save report in csv format if necessary

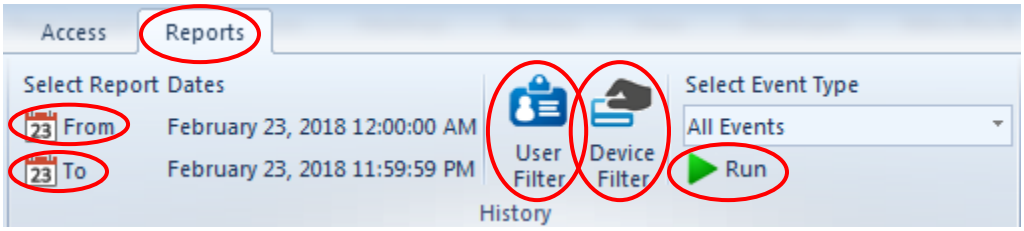


First Name	Last Name	Id Format	Facility Code	Id Number	Profile
Augustine	Duford	Cansec 37 Bit	2864	01437	Lockers
Augustine	Duford	Cansec 37 Bit	2864	01691	Front Door
Aura	Delacote	Cansec 37 Bit	2864	00188	Front Door & Garage
Bader	Frères	Cansec 37 Bit	2864	00128	Laundry
Belma	Grace	Cansec 37 Bit	2864	00838	Front Door & Garage

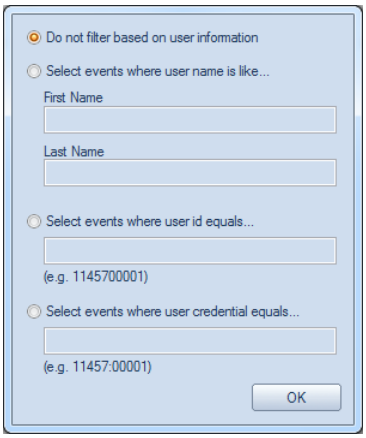
Audit History

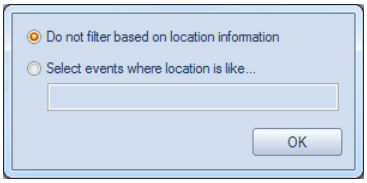
To view all audit history events stored in the database:

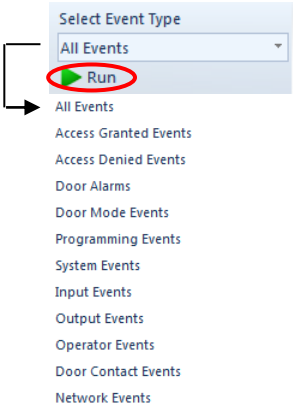
1. Select **Report** from the top main menu.



2. Select Month, Day and Year for **From** date.
3. Select Month, Day and Year for **To** date**.**
4. Optionally select **User Filter** and/or Device Filter to generate a report for a particular user.
5. Select a filter for the **Event Type**.
6. Click the **Run** button.





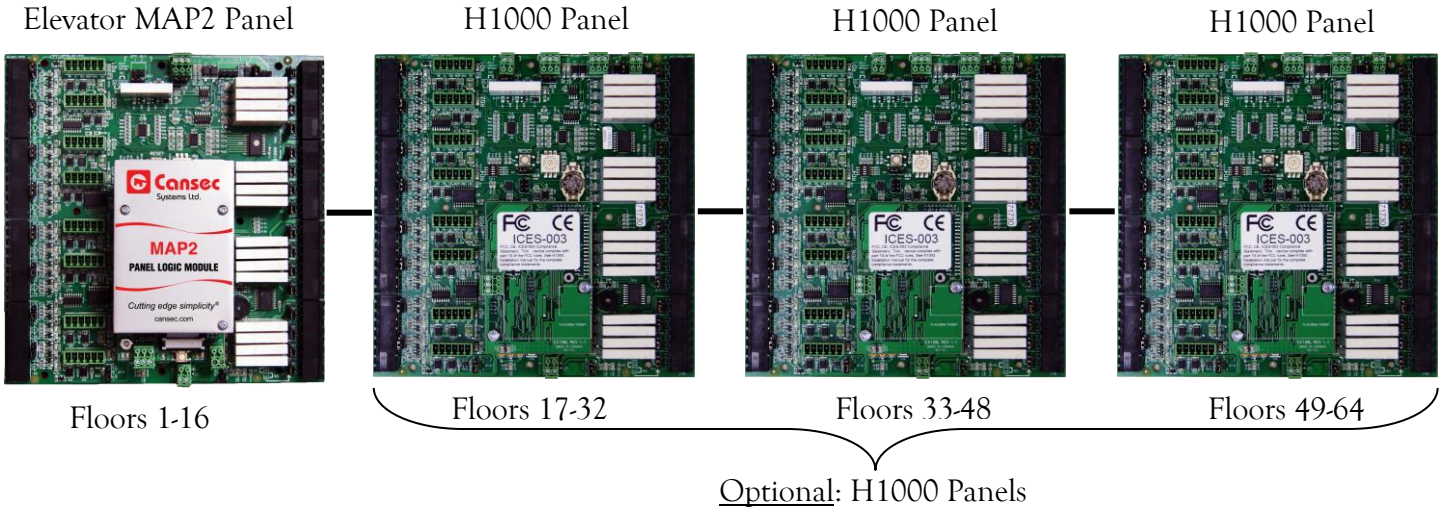


Elevator

The **First Access Cloud** supports MAP2 panel provisioned for elevator mode. The MAPmini and MAP1 panel does not support elevator mode.

The elevator MAP2 panel alone supports up to 16 floors. However, with the optional add-on dedicated H1000 panels, the MAP2 panel supports up to a maximum of 64 floors.

Elevator MAP2 Panel must be provisioned by Cansec each time an additional add-on H1000 panel is added

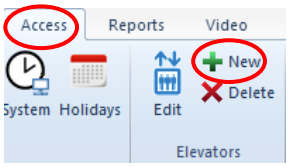


FLOOR GROUPS, ACCESS GROUPS AND FLOOR-UNLOCK SCHEDULE

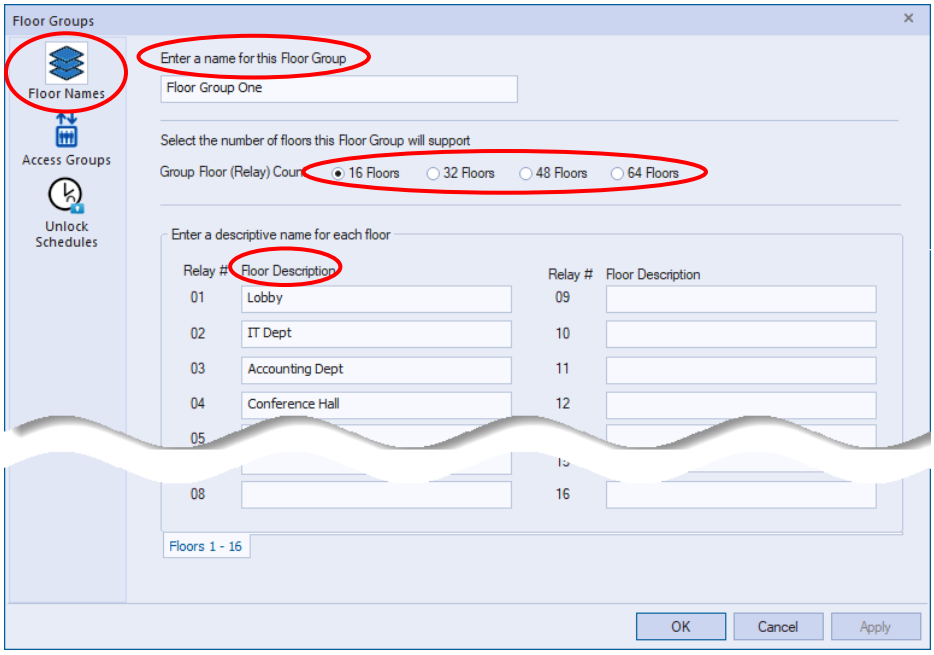
The elevator floor group defines a set of floors that an elevator handles. The access group defines who may access those floors. The optional floor-unlock schedule defines when selected floors may be freely accessible to everyone.

Typically, there is just one floor group and one elevator, but there are cases where multiple elevators are used to serve different floor sets e.g. elevator one serves floors 1 to 32 while elevator two serves floors 33 to 64.

1. If not already created then create a new elevator floor group from the top menu **Access** under the **Elevators** sections

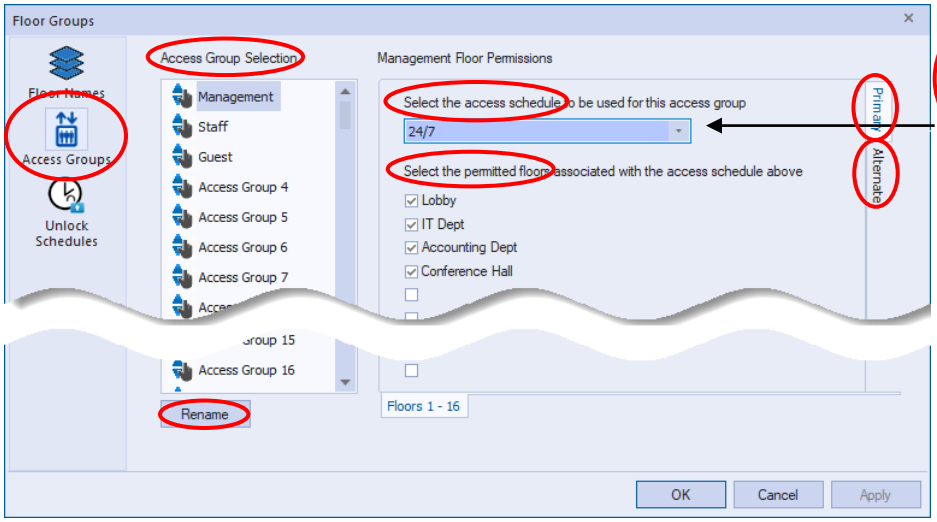


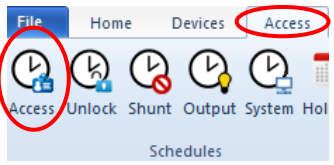
2. Enter a name for the floor group e.g. *Floor Group One*



3. Select the desired number of floors (16, 32, 48 or 64) that this elevator group will support and name each floor accordingly.

4. Select an **Access Group** then select a desired primary and optional alternate access schedule and floors that this access group is permitted to access. Rename the group as desired e.g. *Management*, *IT Department*, *Guest etc…*



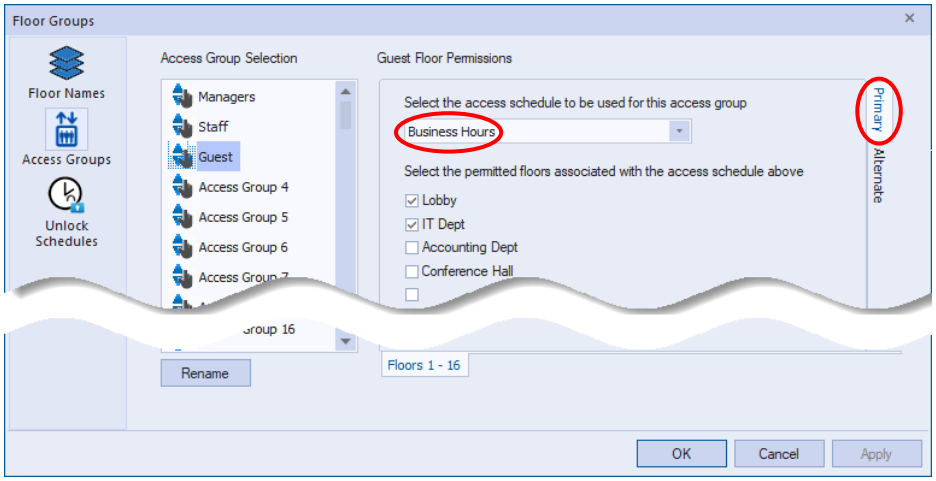


Access schedule define day and time that access is granted to the selected floors

➢ **Primary Schedule**

Primary schedule is used to specify floors that are permitted during certain days and times.

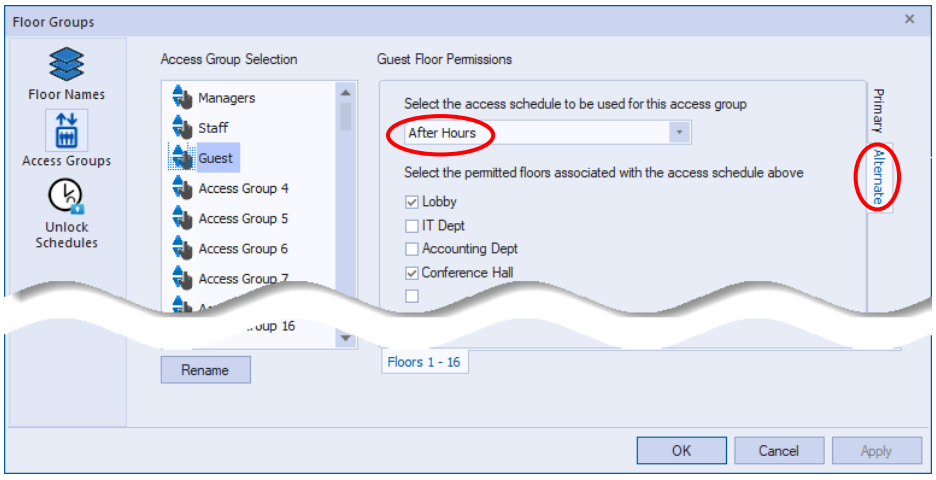
This example shows that the Guest group has access only to Lobby floor and IT Dept floor during business hours.



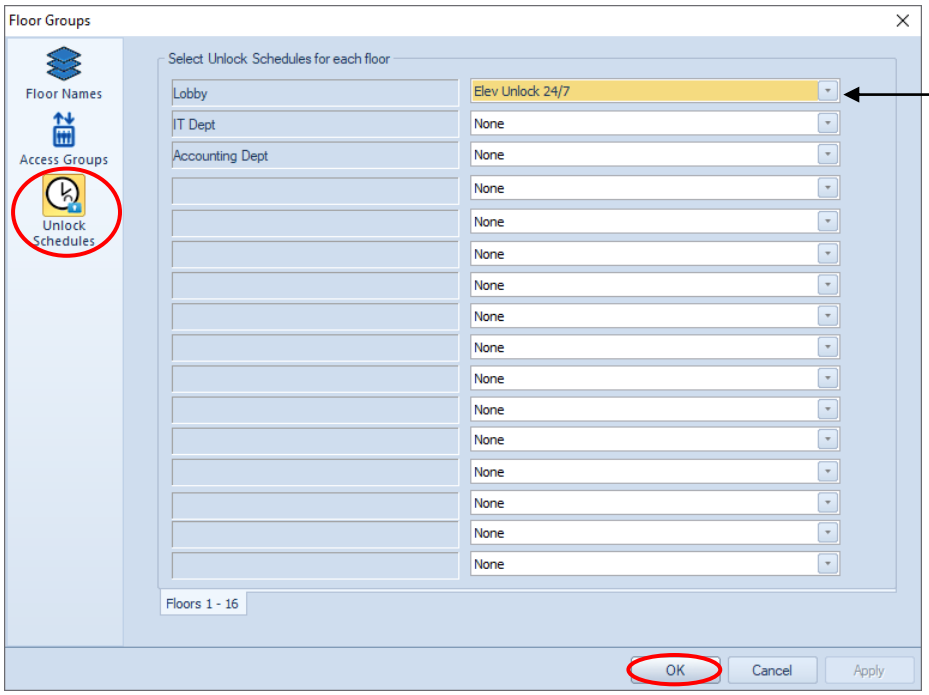
➢ **Alternate Schedule**

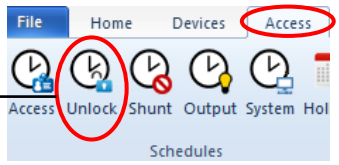
Alternate schedule is used to specify floors that are permitted outside of the primary schedule.

Continuing with the above example, we can now use the alternate schedule to select only Lobby and Conference Hall floors are permitted for the Guest group after hours.



5. If a floor is required to unlock for the purpose of free access then select **Unlock Schedules**. Next, select a desired floor and choose an unlock schedule to assign to it. If necessary, repeat similar steps for other floors.





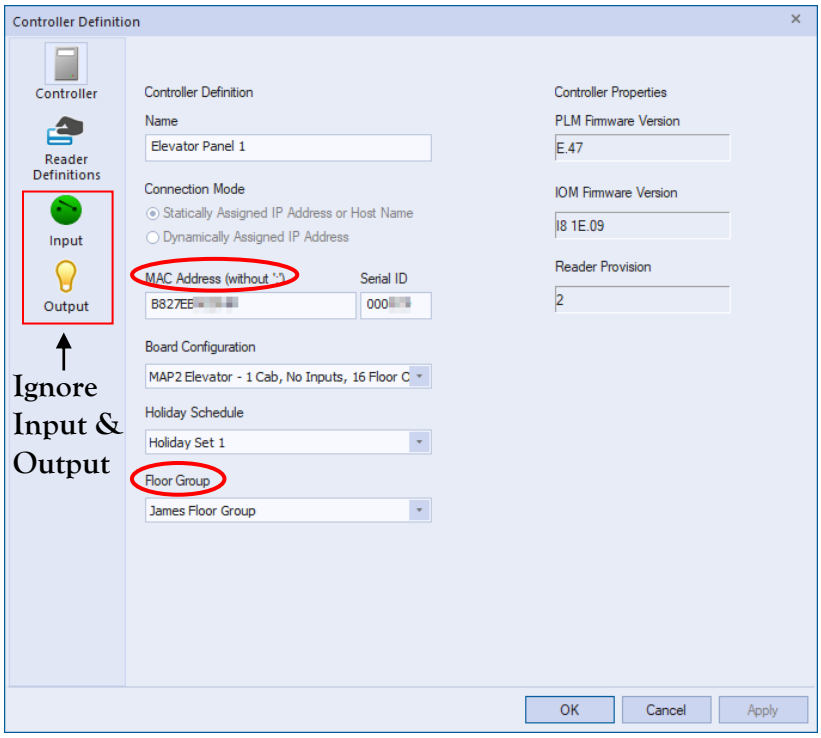
Unlock schedule define day and time that the selected floors is freely accessible

ADD ELEVATOR PANEL

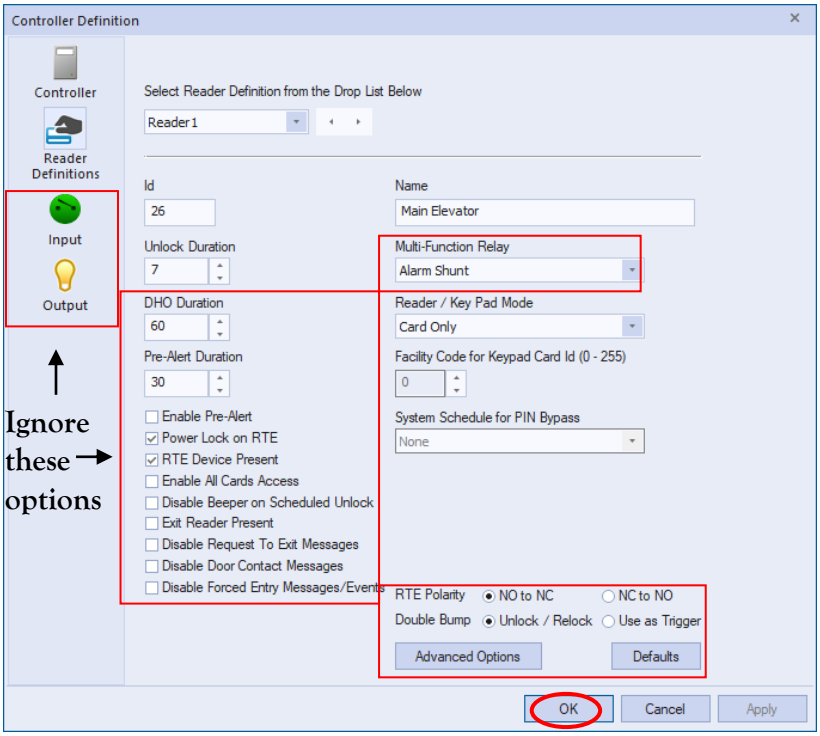
1. Select **Devices -> Managed -> New** from the top menu

2. Name the panel e.g. *Elevator Panel 1* etc...

3. Select *MAP2 Elevator* for board configuration and assign it a floor group that it will handle.

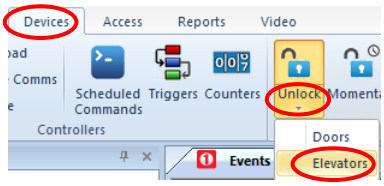


4. Enter a name for the reader e.g. *Main Elevator*. Ignore options that are related to doors e.g. Multi-Function Relay, DHO duration etc... Click **OK** when done.



MANAGE ELEVATOR FLOORS

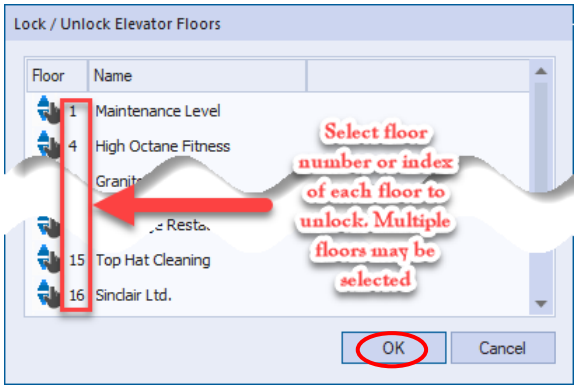
➢ Floor Unlock



1. Select **Devices** and select the down arrow of the **Unlock** button then select **Elevators**. Select a desired elevator.

2. Select floors to be unlocked.

3. Click **OK** when done.

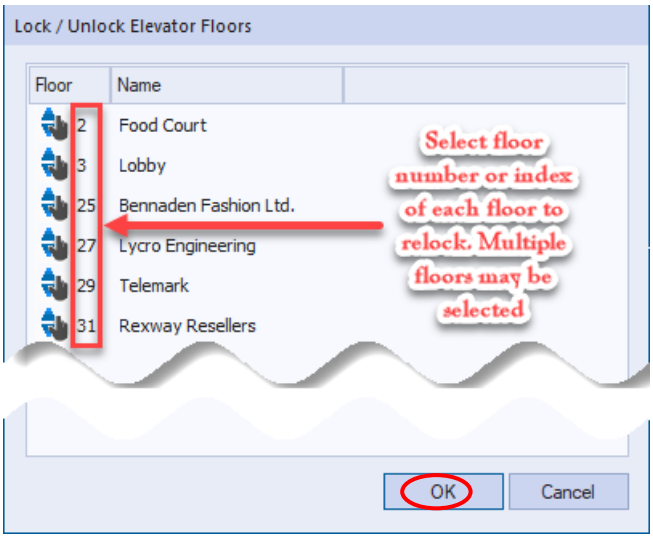


➢ Floor Relock

1. Select **Devices** and select the down arrow of the **Relock** button then select **Elevators**.

2. Select a desired elevator.

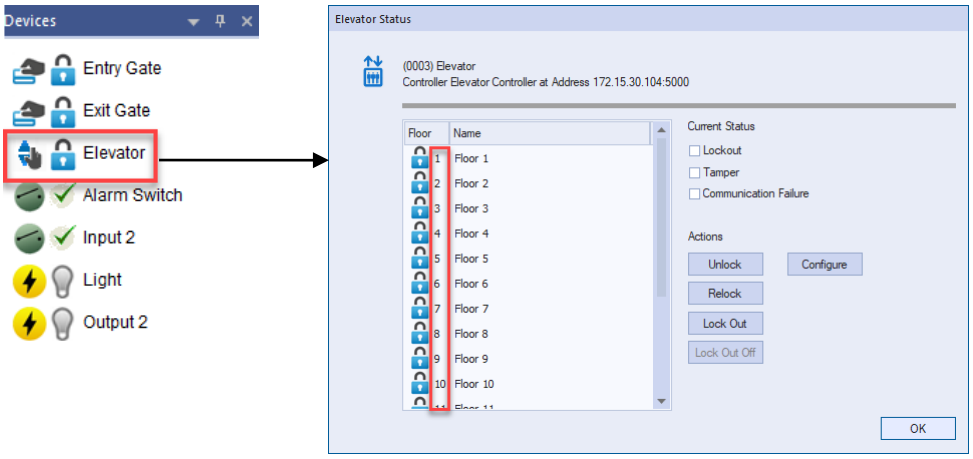
3. Select currently unlocked floors to relock them.



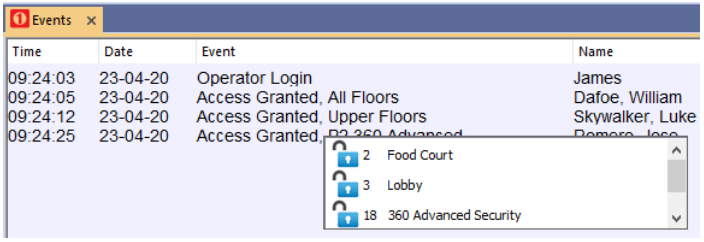
4. Click **OK** when done.

➢ Floor Unlock & Relock

Alternatively, select the elevator in the device view to launch the Elevator Status screen. Select desired floors using the floor number and unlock or relock accordingly. Single or multiple floors may be selected.



➢ Access Granted Event



When an access-granted event for the elevator is displayed in the **First Access** software, click on that event to display the pop-up box which shows the floors that were unlocked. Click on the pop-up box to dismiss it.

Software Update

➢ Software Update

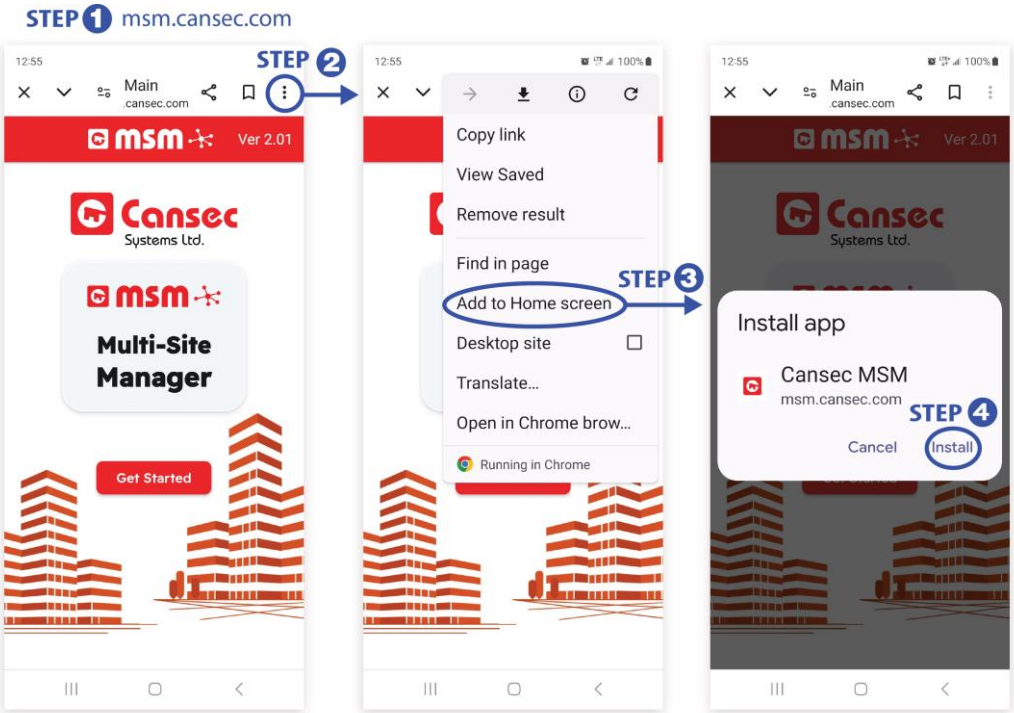
- Download the latest version of the First Access Cloud Client software from https://www.cansec.com/downloads.html. Unzip and launch the installation package. Follow on-screen instructions to complete the update.

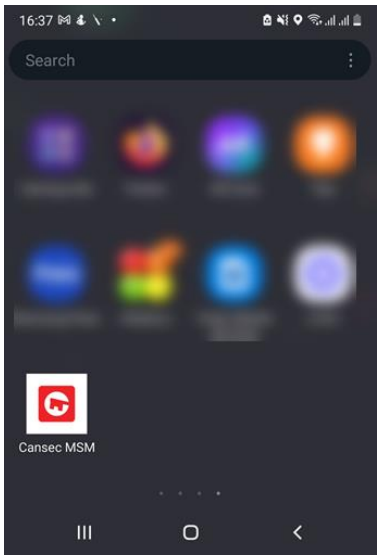
Cansec MSM App

How to download and install Cansec MSM app (iOS or Android app) to your phone.

Android phone:

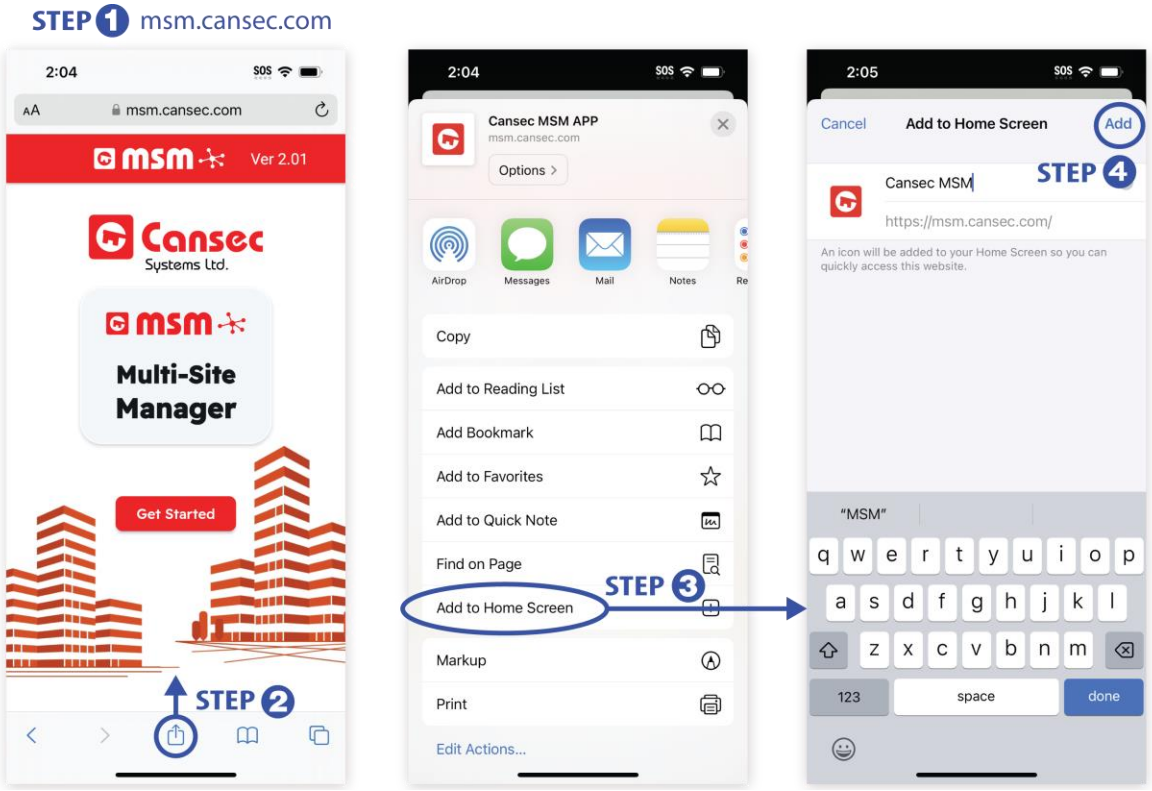
Step 1: Launch a Web browser, visit “https://msm.cansec.com”
Step 2: Select the three vertical dots at the top right corner.
Step 3: Select “Add to Home screen”.
Step 4: When prompted, select “Install”.

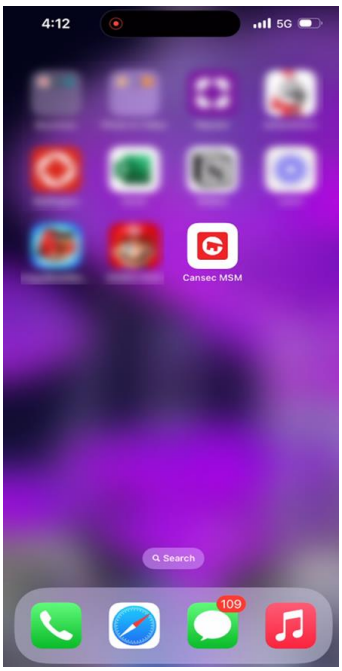




iOS phone:

Step 1: Launch a Web browser and visit “https://msm.cansec.com”
Step 2: Select “Share” button as shown in the image below.
Step 3: Select “Add to Home screen”.
Step 4: Select “Add” at the top right corner.

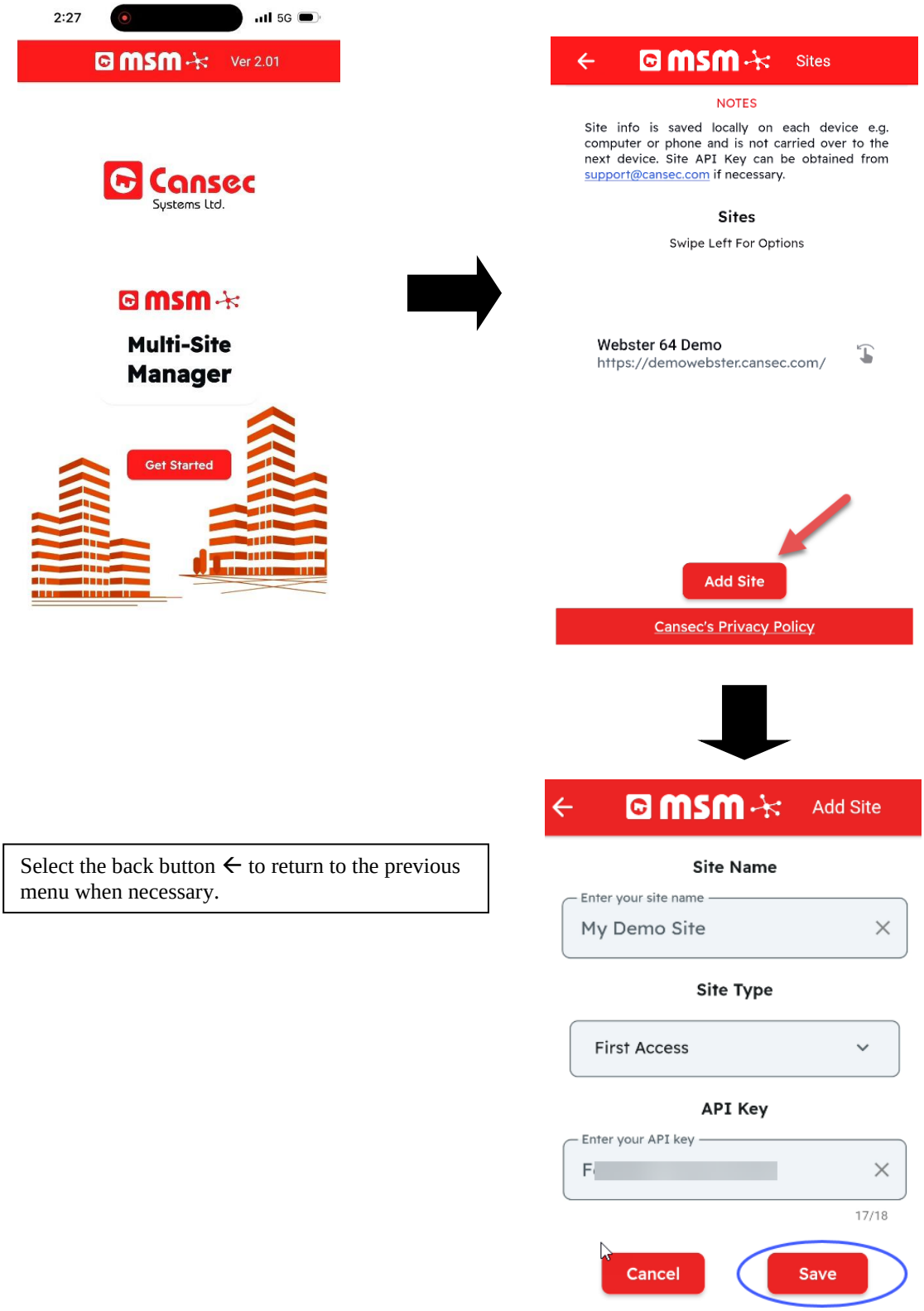




Desktop PC:

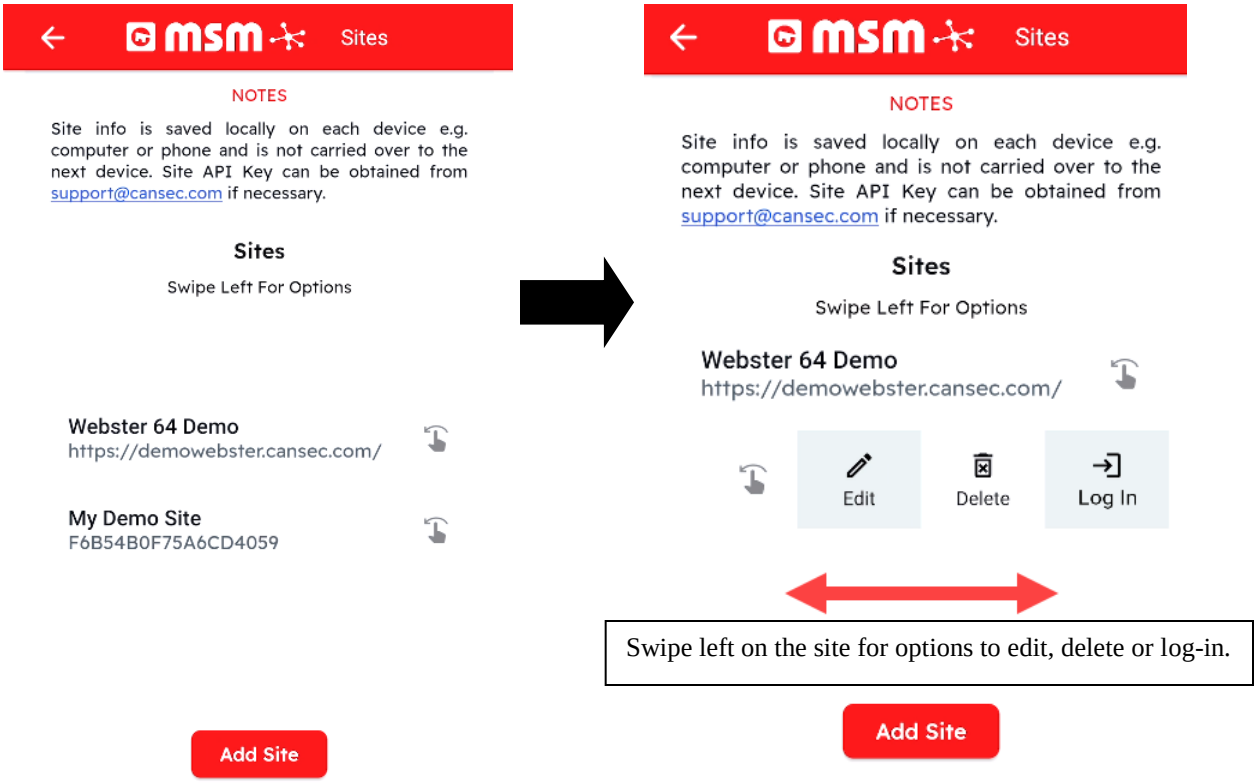
Step 1: Launch a Web browser and visit “https://msm.cansec.com”
Step 2: Select the install app button highlighted in the below image.
Step 3: Select “Install” when prompted.

1. Launch the app and select “Get Started”. Select “Add Site”. Enter site name e.g. My Demo Site. Select First Access. Enter the API key you have been issued, and select “Save”.

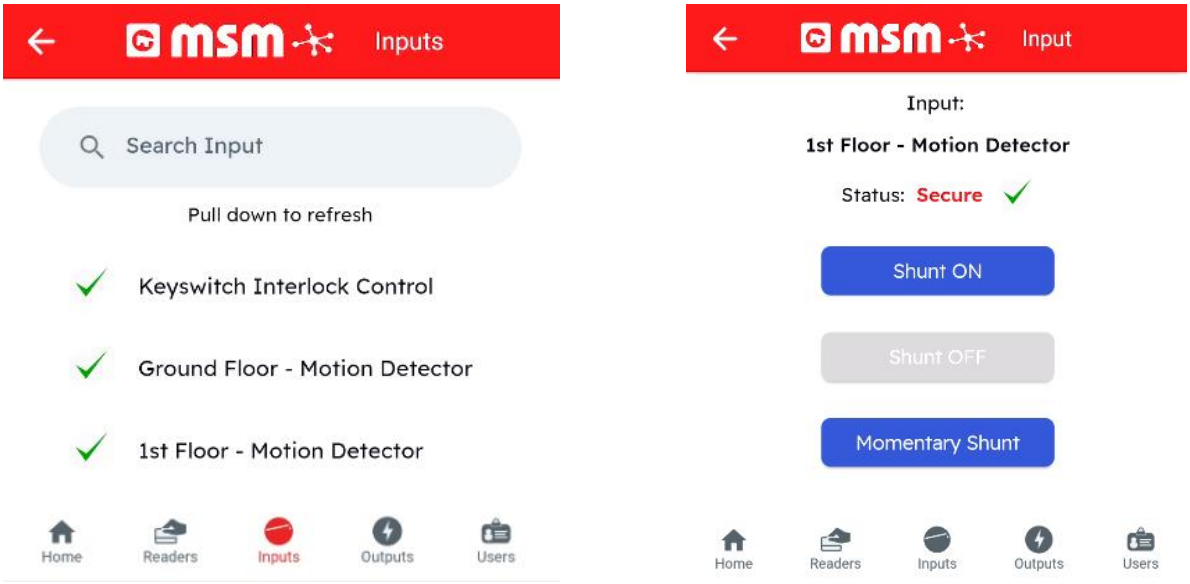


Select the back button ← to return to the previous menu when necessary.

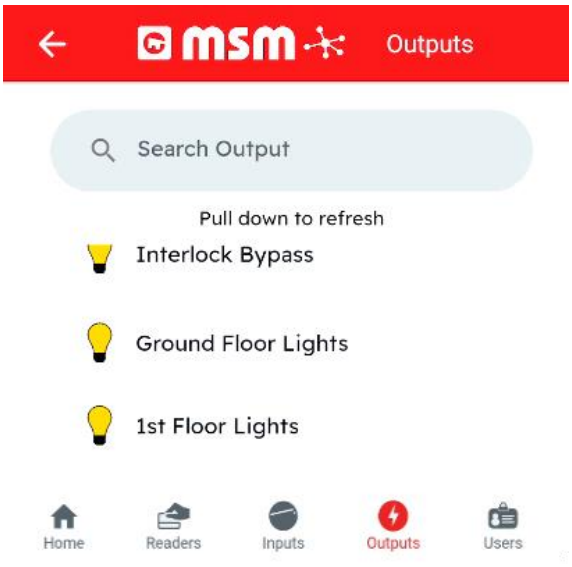
2. Swipe left on the site for options to edit, delete or log-in

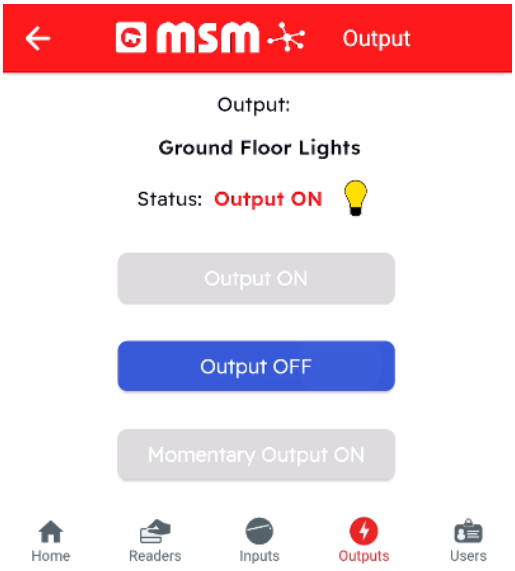


❖ <u>Input Commands</u>: Shunt On, Shunt Off, Momentary Shunt

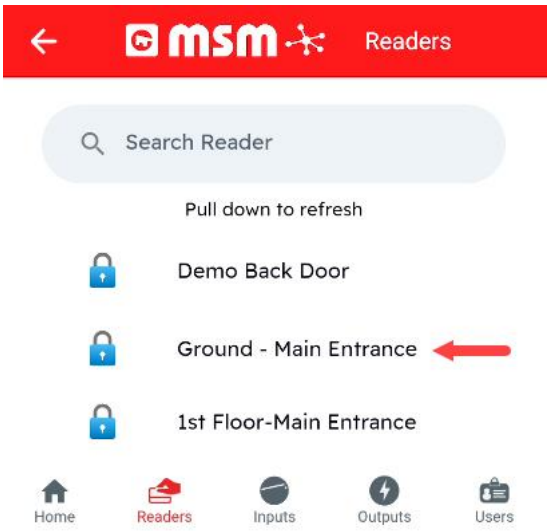


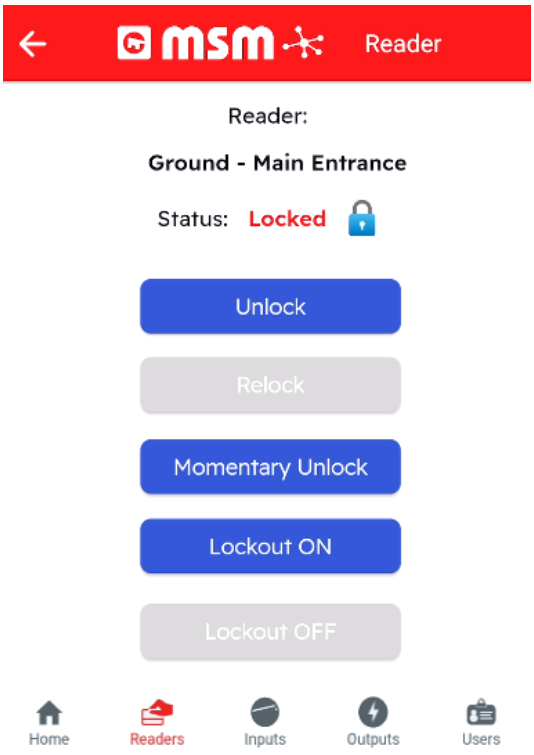
❖ **Output Commands**: Output On, Output Off, Momentary Output On





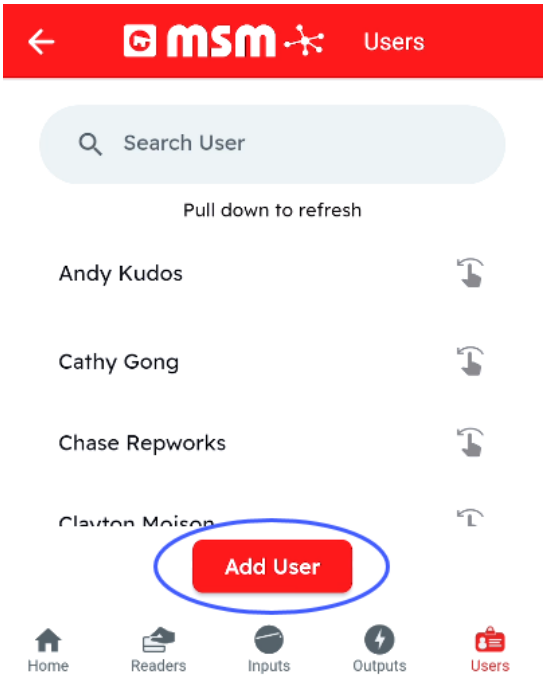
❖ **Reader Commands**: Unlock, Relock, Momentary Unlock, Lockout On, Lockout Off



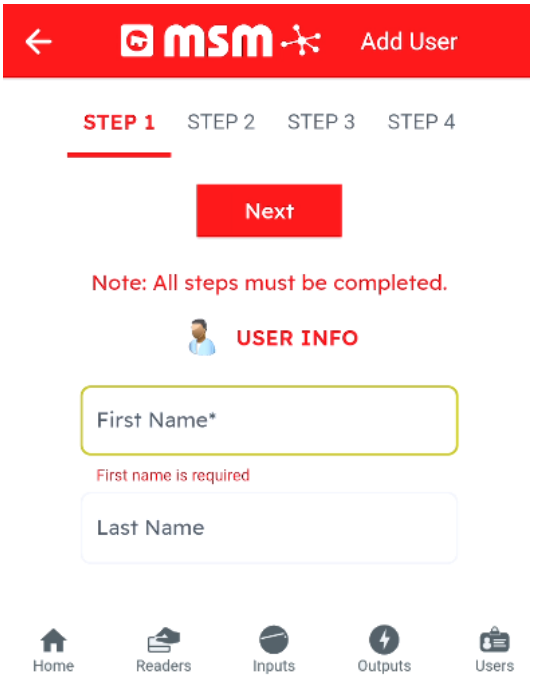


❖ **User Command**: Add User

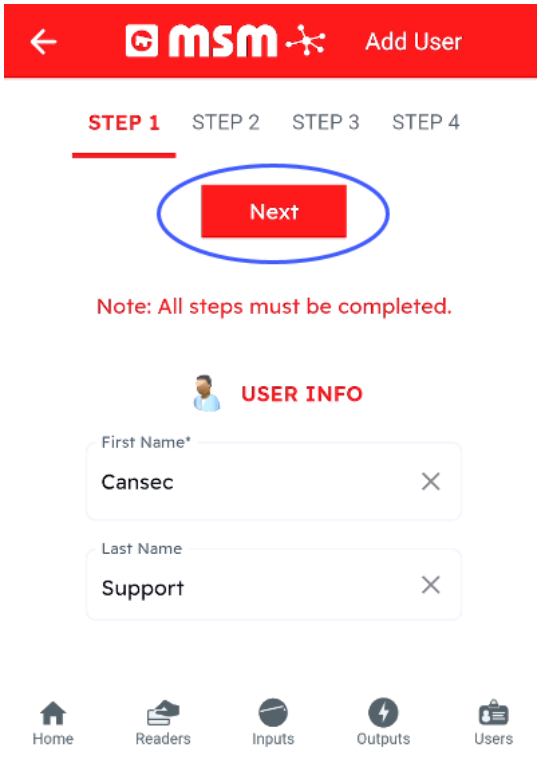
Step 1: Select Add User.



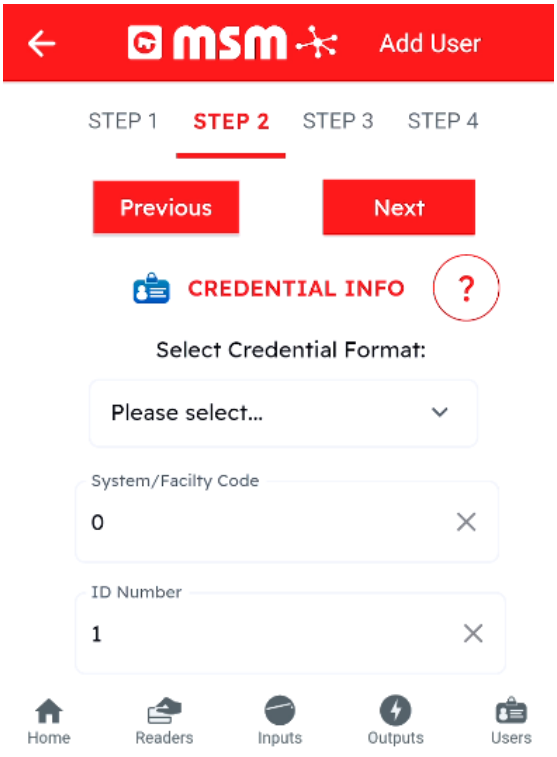
Step 2: Enter First & Last Name of the User.



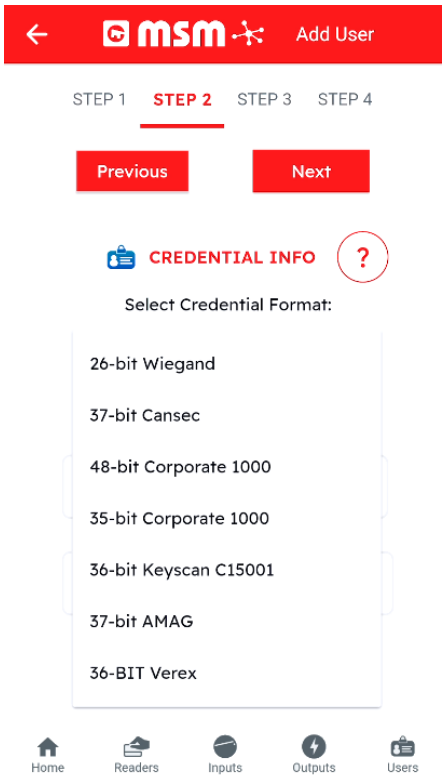
Step 3: Select "Next" after each step.



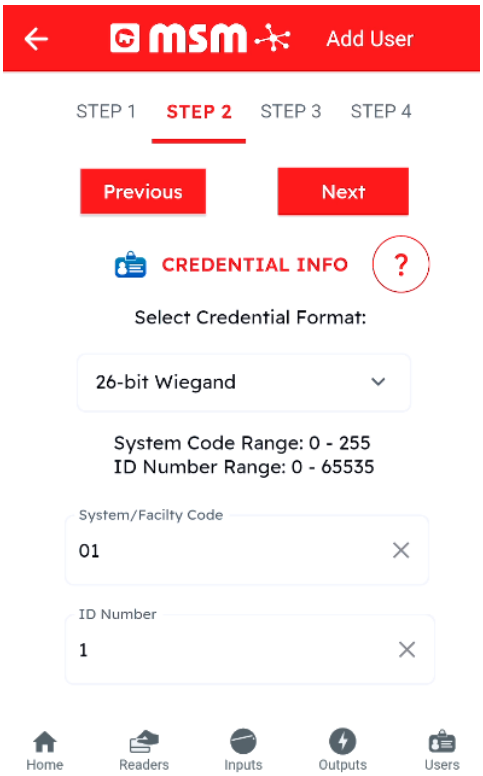
Select the Credential Format and enter the Facility Code, ID number.



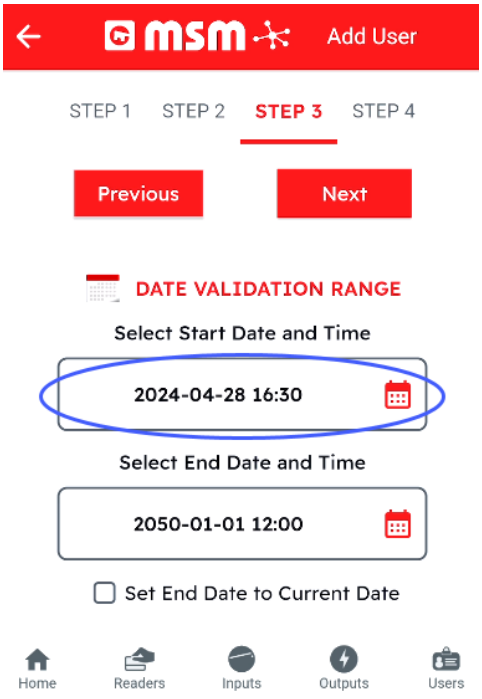
Step 4: Select Credential Format.



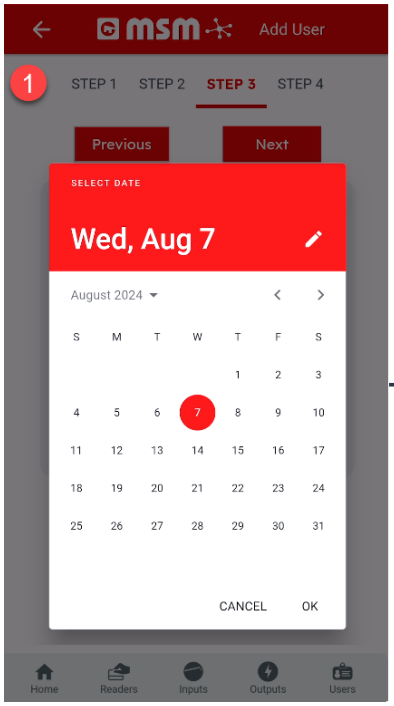
Step 5: Enter Facility Code, ID.

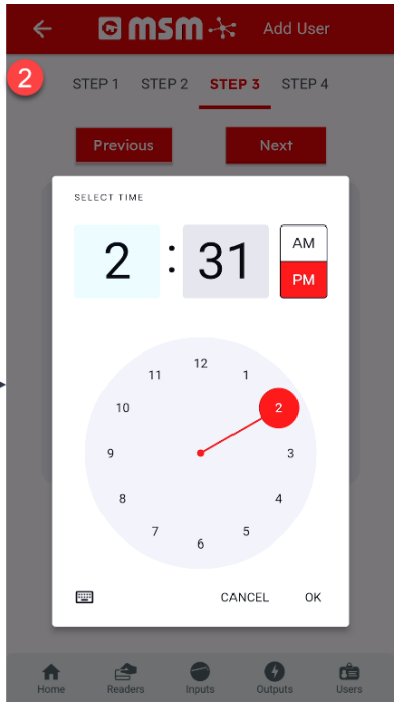


Step 6: Validate the credential by selecting Start Date, Start Time and End Date, End Time.



Select start date & time.





Set the time by rotating the clock hand.

Optional: Select the keyboard icon seen in figure 1 to enable digital input. To switch back to analog interface, select the clock icon seen in Figure 2.

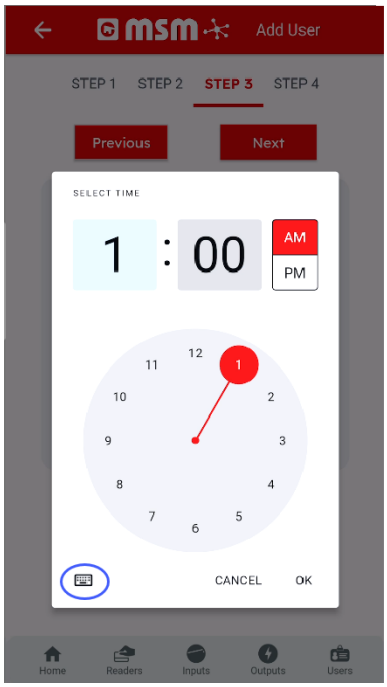


Figure 1

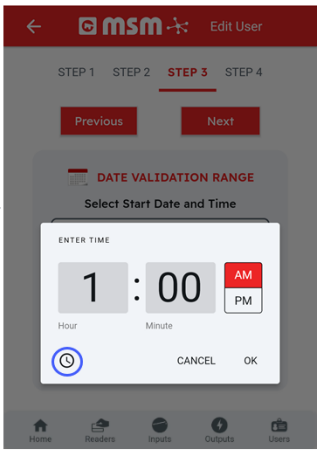
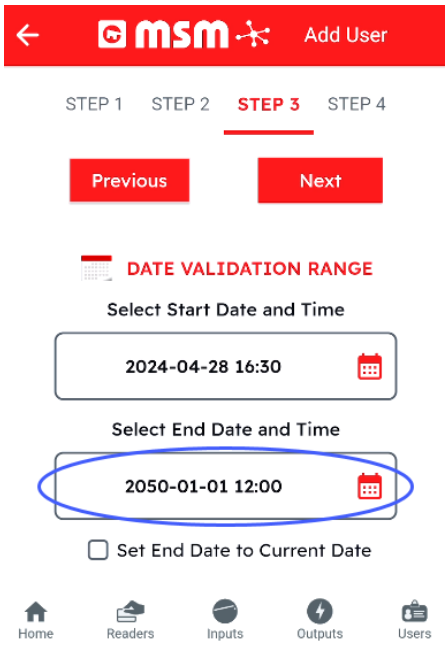
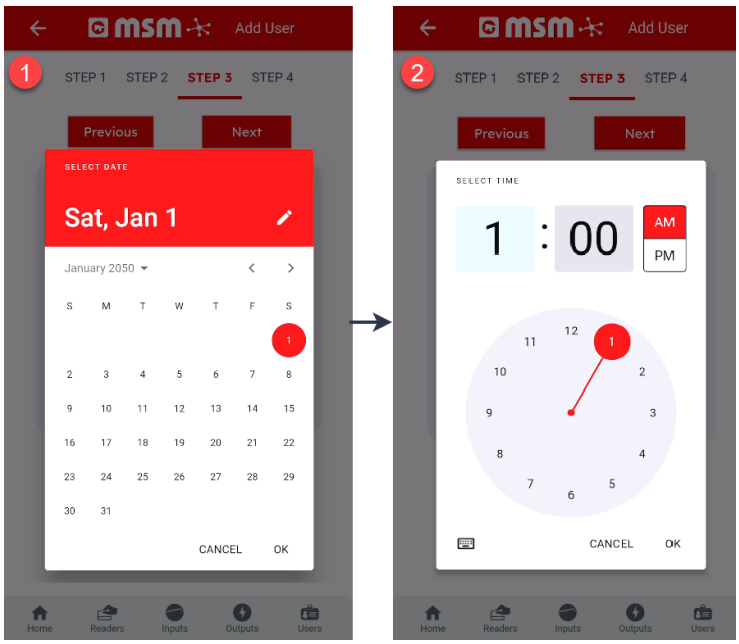


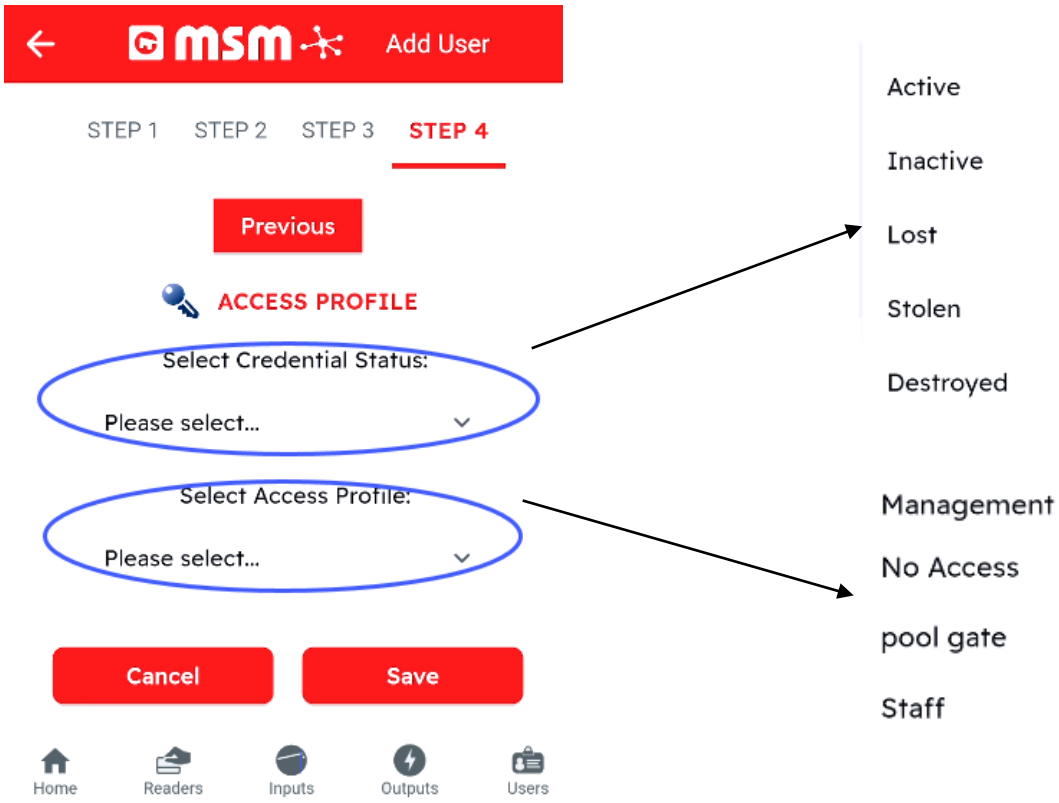
Figure 2



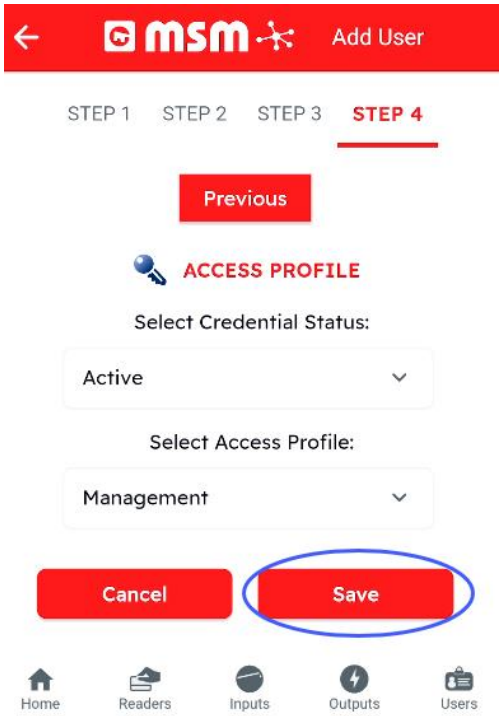


Set End Date & Time.

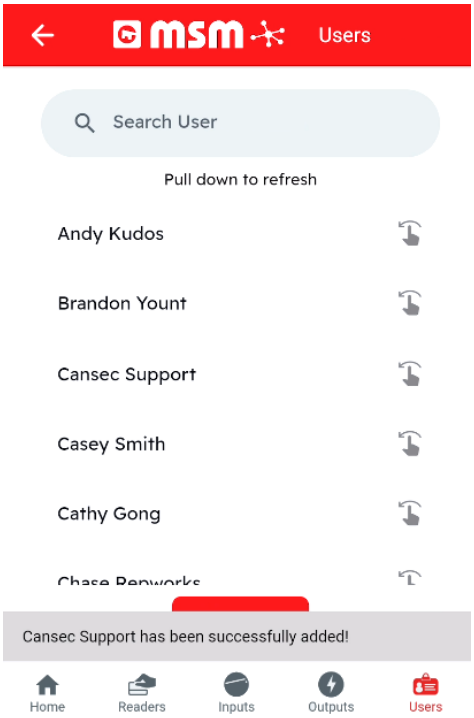
Step 7: Set status to “Active” and select the appropriate access profile.



Step 8: Select “Save”.

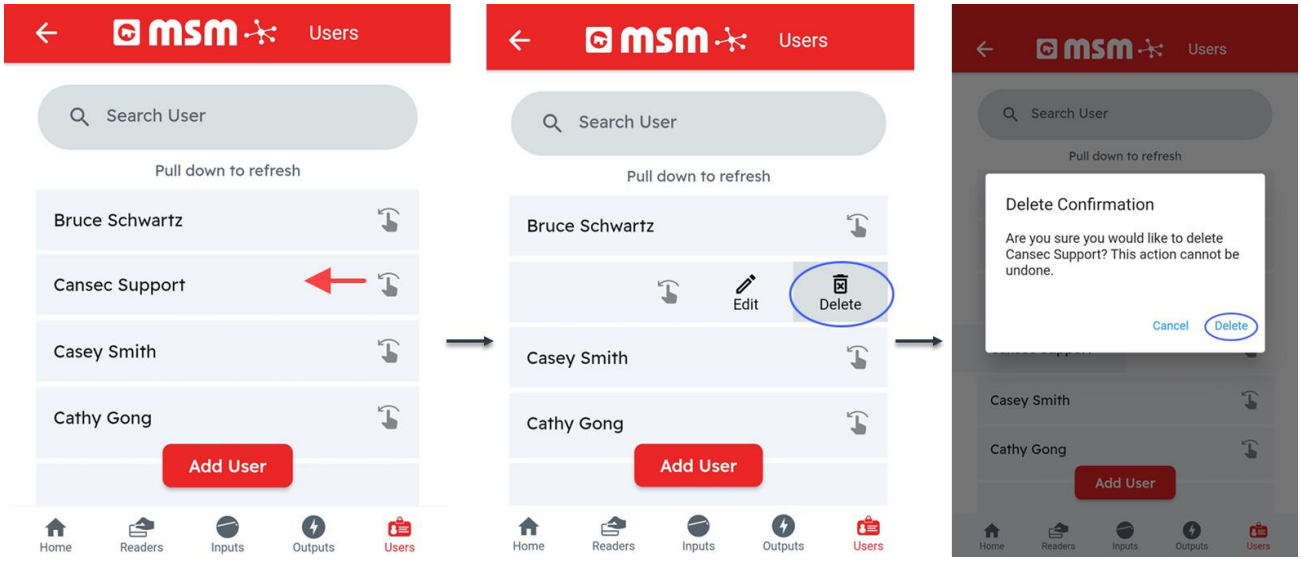


A new User record is added.



❖ **User Commands:** Delete User

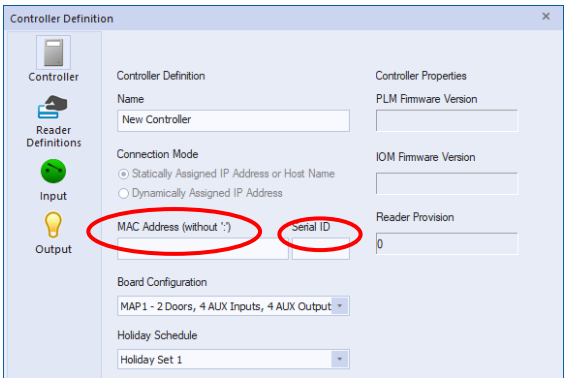
Locate the user and swipe left and tap on Delete.



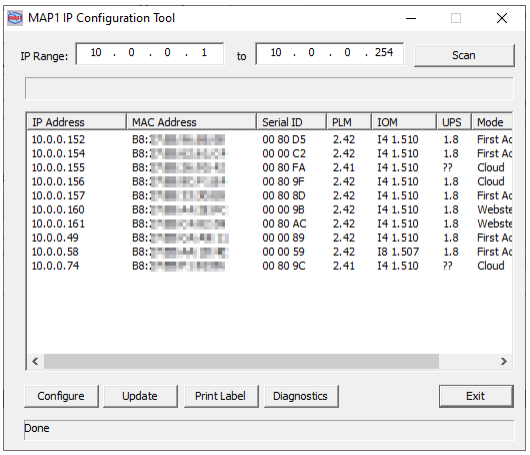
Troubleshooting

➢ Offline controller

- Ensure that the controller has internet access and that the controller's MAC address is correctly entered along with its SID.



- Use the MAP1 IP Configuration Tool to scan for all controllers to ensure that they are at least detected by this standalone tool downloadable from here: https://cansec.com/downloads/category/232-software.html



® First Access Cloud is a registered trademark of Cansec Systems Ltd.
® Windows is a registered trademark of Microsoft Corporation in the United States and/or other countries.