Organeez : ACCESS CONTROL

With integrated wander management

User Guide

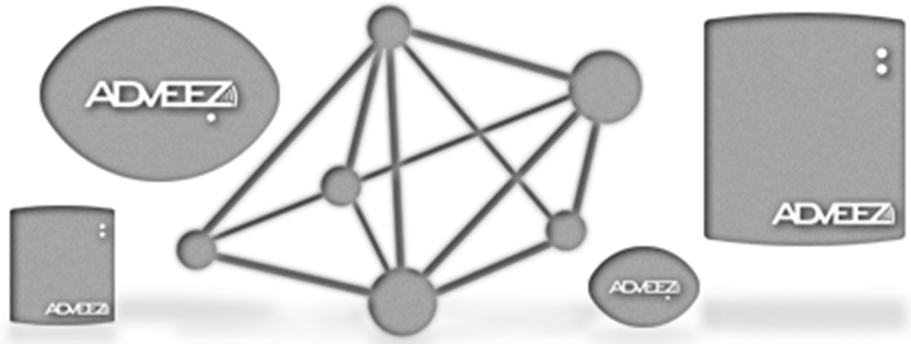


TABLE OF CONTENTS

ACCESS CONTROL MANAGEMENT OVERVIEW 4

AUTOREEZ 5

AREAS & GROUPS 6

QUICK START 7

CREATING A DATABASE 8

BUILDING A NEW ACCESS CONTROL NETWORK 10

Overview of the « area » tab 10

To add an area 11

To remove an area 12

To add a controller into an area 12

To remove a controller or an UTL from an AREA 13

CONFIGURING UTL AND READERS 14

To configure the Wiegand frame/ UTL Automations 15

CONFIGURING CONTROLLERS 17

Activate Anti-Passback 18

MANAGING USER GROUPS/ CALENDAR/ TIME SLOTS 20

Overview of the time slots tab 20

How to configure/ delete time slots 21

To edit a timeslot 22

Overview of the non working days tab 23

To add a non working days group 23

To delete/ edit a non-working days group 24

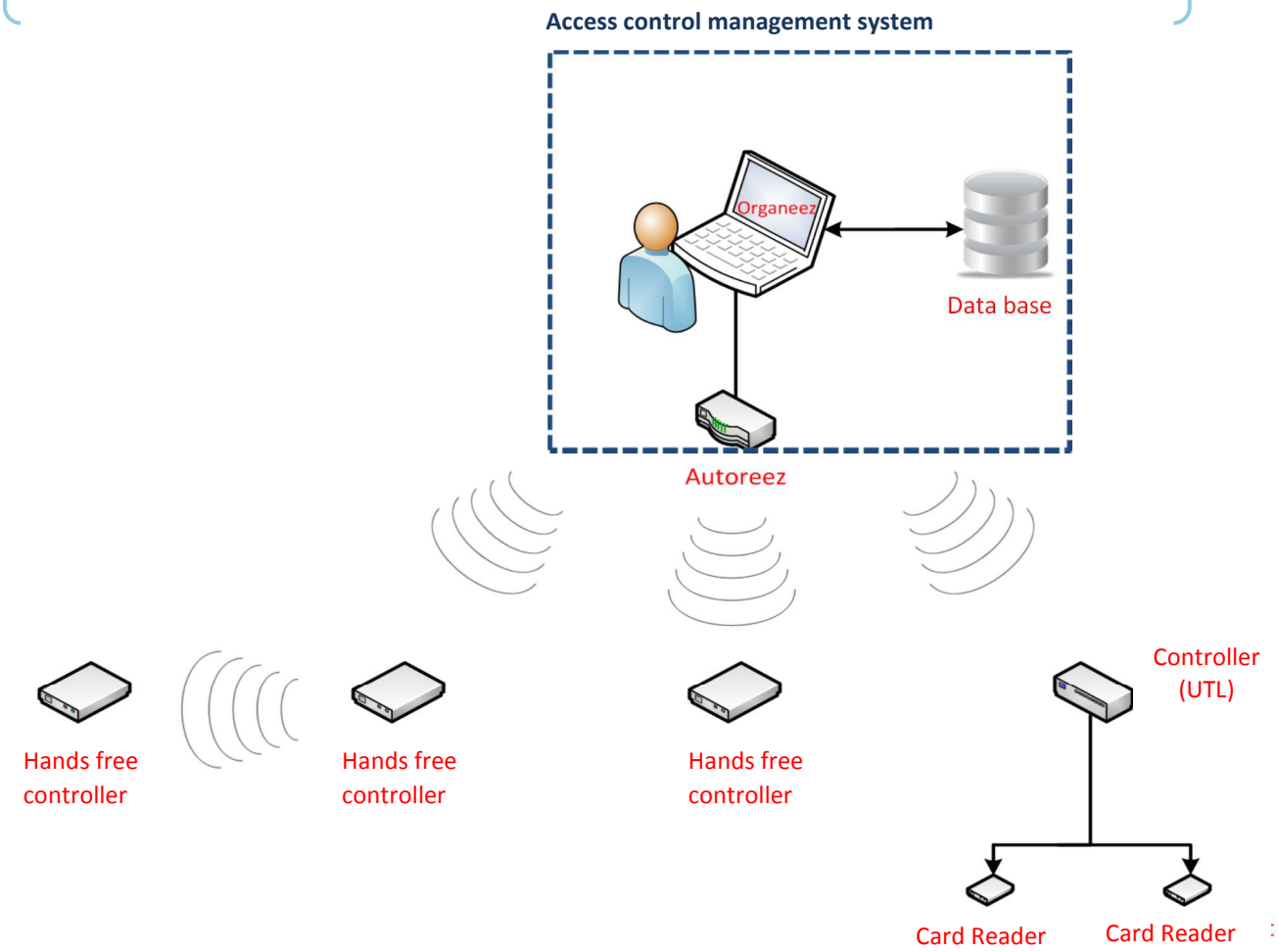
MANAGING USER LIST 25

Overview of the « groups » tab 25

How to add a user group 25
To delete/ edit users group 26
Overview of the users tab 27
To add user 27
To delete user 28
Editing user rights/ info 29
To add and edit user profile 30
EVENT HISTORY/ REPORTS 31
Exporting/ editing events 31
To associate/ delete report 32
MAPS 33
Overview of the maps tab 33
To build a map 33
To remote opening/ closure 34
INSTALLING UTL 35
CONNECTION BY TYPE OF NETWORK 37
CONFIGURING WANDER MANAGEMENT CONTROLLERS 38
General parameters 38
Nuisance Mode 39
Inhibition 40
CONFIGURING WANDER MANAGEMENT USERS/ PATIENTS 41
How to add a care person 41
How to add a disoriented patient 42
CONFIGURING WANDER MANAGEMENT ALARMS 43
ESPA or POCSAG OUTPUT 43

ORGANEEZ: ACCESS CONTROL MANAGEMENT OVERVIEW

The ADVEEZ access control management system is composed of several components:
- The User Interface software ("ORGANEEZ"), various databases including all information related to each site, and the access control system gateway ("AUTOREEZ"). All are installed/connected into a single PC.
-Various hardware devices enabling controlling doors and user access, generally located close to access points to be controlled.



Database	Stores all of the information which is related to a given site (controller list, list of users, time zones...)
Organeez	Access control management software provides interface for managing user rights, controller & reader configurations…
Autoreez	Access control gateway connected to the PC, in some version, this device is integrated into door controller
Controllers	Single access point controllers with integrated hands free/long range reading capabilities (access control: PE3LR-C / Wander management: AD-CARE)
AD-UTL-XX	This hardware controls door locking devices (magnet locks, strikes) & readers, it is located close to doors to be controlled.
Reader	Card reader proximity credentials (Mifare and Marin 125 kHz)

AUTOREEZ (FCC ID : R8T-AUTOREEZ)

The access control central PE3IR-NT (AUTOREEZ) can provide a full centralized management of Hands Free tag, EM card (125Khz) and Mifare. The central can manage until 128 doors by radio, or 512 doors by wired network. It works by radio, RS485 or IP. With the radio, each controllers PE3LR-C-NT becomes an access network. In this mode, the central can supervise each controllers on the network and can manage in real time every updates. It also download and save every events from controllers in the database. The central can include a reader to enroll tags. The computer is plugged to the central by a USB cable or IP.

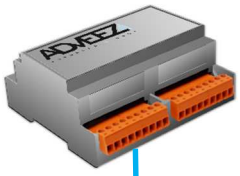
The ADVEEZ access control central can be in two different forms:

The office version

The connection to the supervisor PC is made via USB port

Connecting controllers to the central access control can be done via radio.

The rail DIN version



The connection to the supervisor PC is made via IP.

Connecting controllers to the central access control can be done via IP, RS485 or radio.

OPTION: It's possible to integrate a « Healthcare » system by RS 232 connection to add a nurse call system.

This device (FCC ID: R8T-AUTOREEZ) complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation"

The users manual or instruction manual for an intentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. In cases where the manual is provided only in a from other than paper, such as on a computer disk or over the Internet, the information required by this section may be included in the manual in that alternative form, provided the user can reasonably be expected to have the capability to access information in that form.

1. **USER MANUAL:** Please add the following warning statements to the User Manual (a. is for the ZigBee module, and b. is for the computer peripheral):

a. This equipment complies with the FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and any part of your body.

B. NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
-Consult the dealer or an experienced radio/TV technician for help.

Area

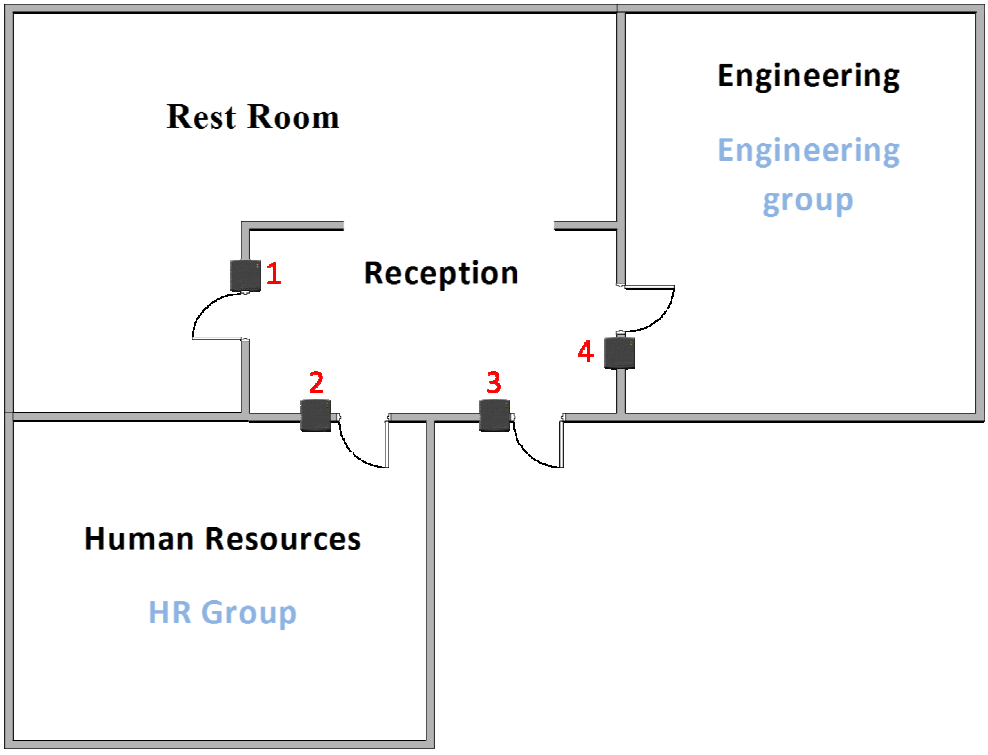
A set of readers which is assigned to a group, users belonging to that group will have access to readers included in the defined area.

Group

A group can be associated with one or more readers.

Example: Here's the plan of company X with four Readers numbered 1 to 4.

If the desk, engineering department and human resource office need to be locked with different people being authorized to access to them; then areas and their corresponding groups need to be created:



The solution is to create three zones and two different groups:

Area Name	Readers in the area	Groups associated to this area
Area "ENGINEERING"	N°4	ENGINEERING Group
Area "HR"	N°2	HR Group
Area "Common"	N°1 & N°3	ENGINEERING Group & HR Group

QUICK START

1

The network discovery identifies all the controllers that are present near the Autoreez.

Regrouping the controllers in an area allow you a comprehensive and effective management of all controllers with identical functionalities.

2

The creation of a time slot allows control the access of users with different time zones.

We can associate seven time slots per day.

3

A group of non-working days aims to deny access to users during the closing days.

A group of non-working days is constituted by 18 months.

4

Create a group simplifies the management of multiple users who have the same rights.

A group can be extended to several areas, but it accepts a time slots and one group of non-working days.

5

The user is associated with one or more groups according to these access rights.

He can have several tags.

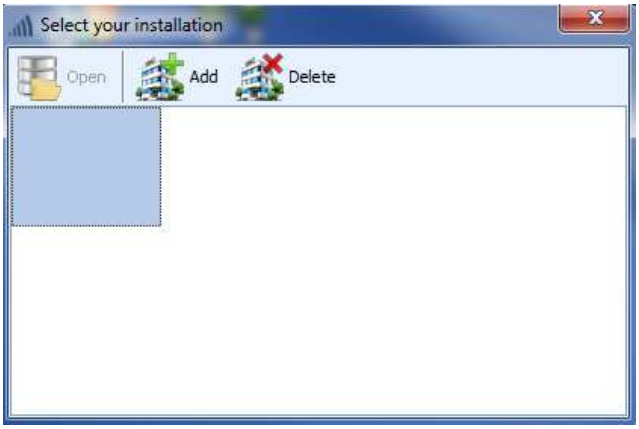
The information like "Name", "Company" or picture can be stored in the database.

CREATING A DATABASE

Double clicking on the Organeez shortcut launches the ADVEEZ access management software: Installation main window opens.
First step consists in creating a database which will include all access control details related to the given site.

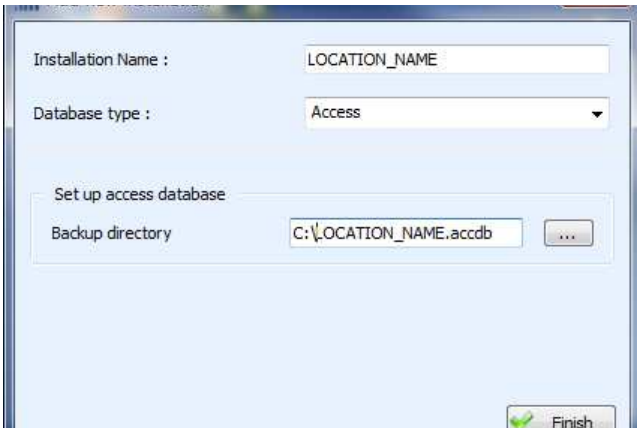
How to create a Database:

1. Click on 'Add' to display the 'Add new installation' dialog box



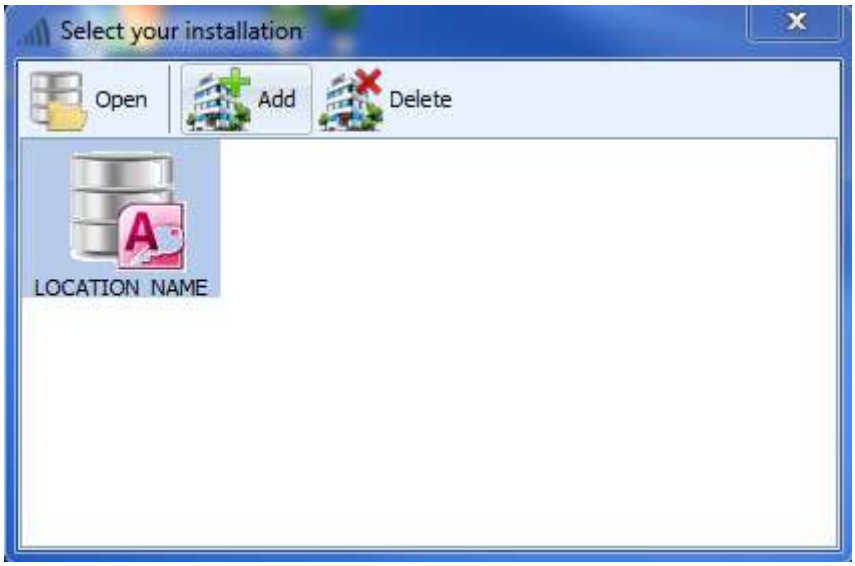
2. Fill-in the installation name
3. Select your database type (access or SQL)
4. Select or enter the database file path
5. Click on 'Finish'

—> Your database is now created



To open your Database and start configuring/using access management:

Click on the related icon
Click on 'Open'



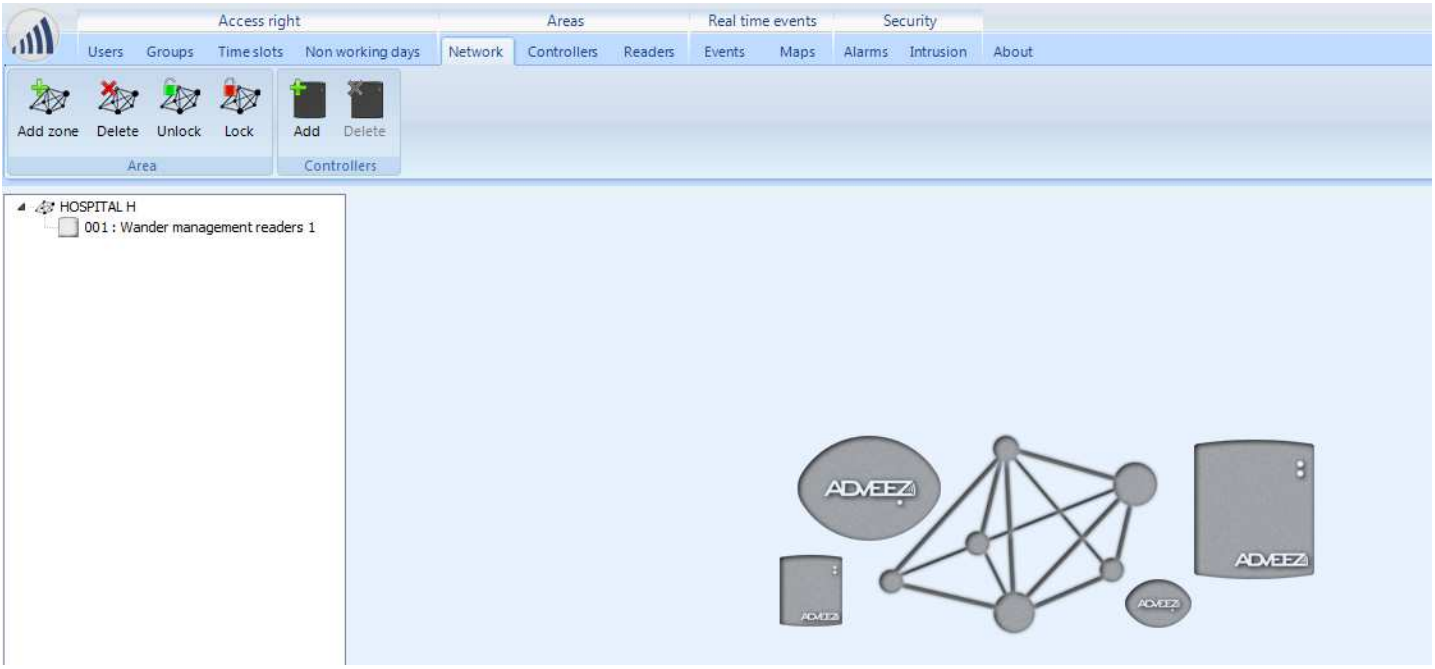
You can now enter your user name and password. Confirm your password.

BUILDING A NEW ACCESS CONTROL NETWORK

Once wiring all controllers and connecting them to the Autoreez Gateway is done (if wireless communication is not used), a network discovery must be performed in order to connect all access points to the access control management.

Overview of the “area” tab

1. Managing Network
2. Managing controllers
3. Managing reader configuration
4. Area tree window
5. Controllers

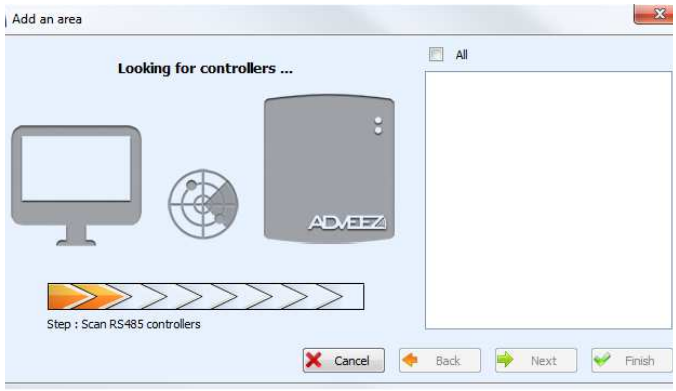


To add an area:

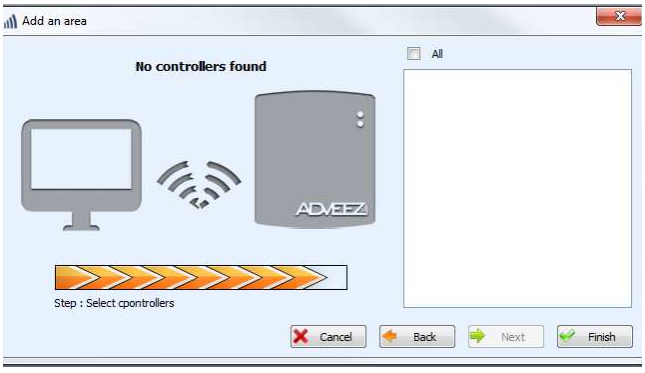
1 In the subset managing areas, click on ‘Add Zone’ (Or just Add to Add just a new controller)

2 Fill-in the area name, select controller interface type to be connecter (RS485, IP or Wireless) and click on ‘Next‘

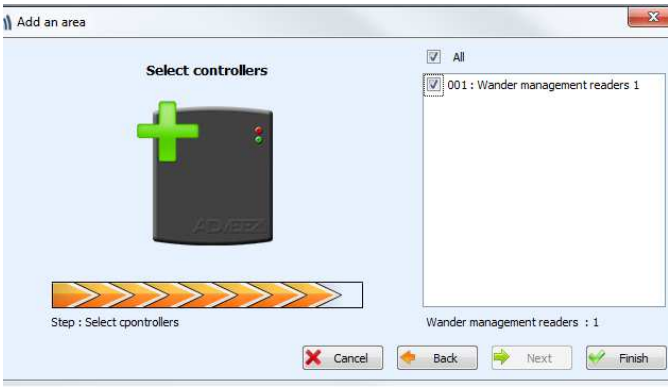
—> The searching process is then started.



3. If no controller is detected, cick on ‘Skip‘



If one or several controllers are detected, select the controllers which need to be added into the area and click on ‘Finished’



—>The ‘area tree’ is now updated

To remove an area:

1. From the area tree window, select the area which has to be removed

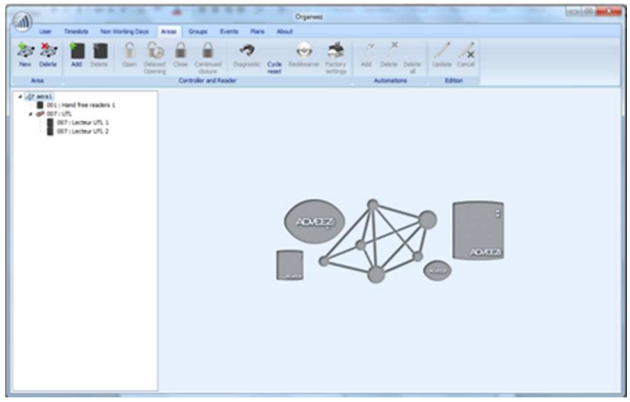
2. In the subset managing areas, click on ‘Delete’

3. Confirm the deletion to remove the area

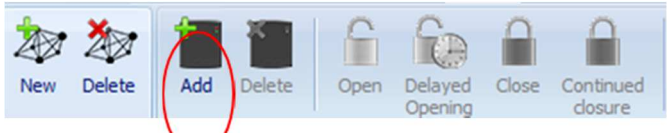
—> The tree area is updated (subset 4)

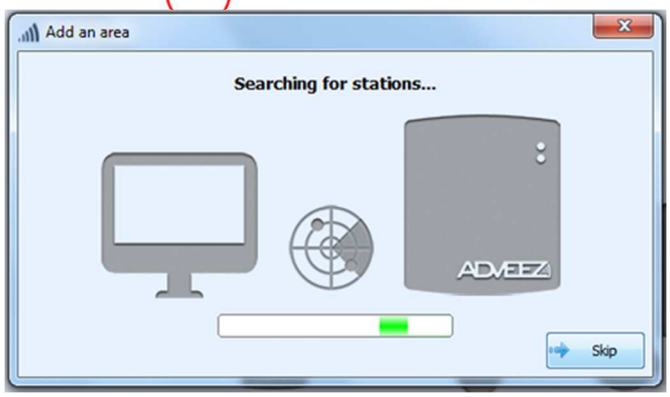
To add a controller into an area:

1.From the area tree window, select the area which need to be modified



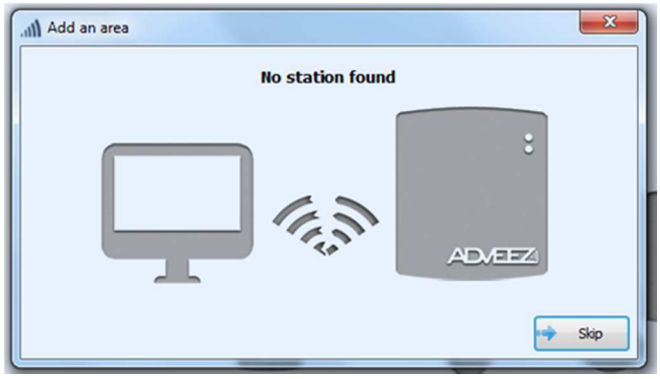
2.In the subset managing controllers, click on ‘Add’



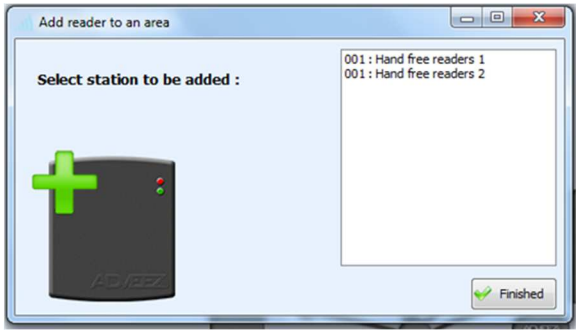


—> The Network discovery is started

3. If no controller is detected, click on ‘Skip’



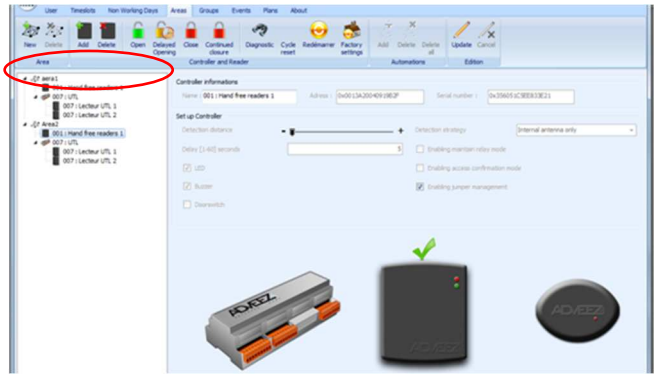
If one or several controllers are detected, select the controllers on the area and click on ‘Finished’



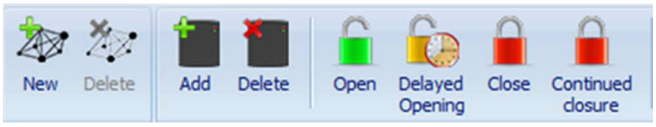
—> The area tree is then updated (subset 4)

To remove a controller or an UTL from an AREA:

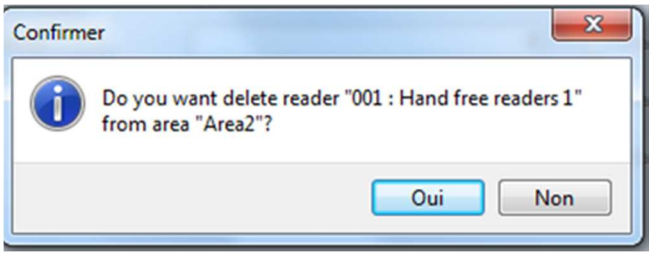
1. In the area tree window, select a controller/UTL



2. In the subset managing controllers, click on ‘Delete’



3. Confirm the deletion to remove the controller



—> The tree area is updated (subset 4)

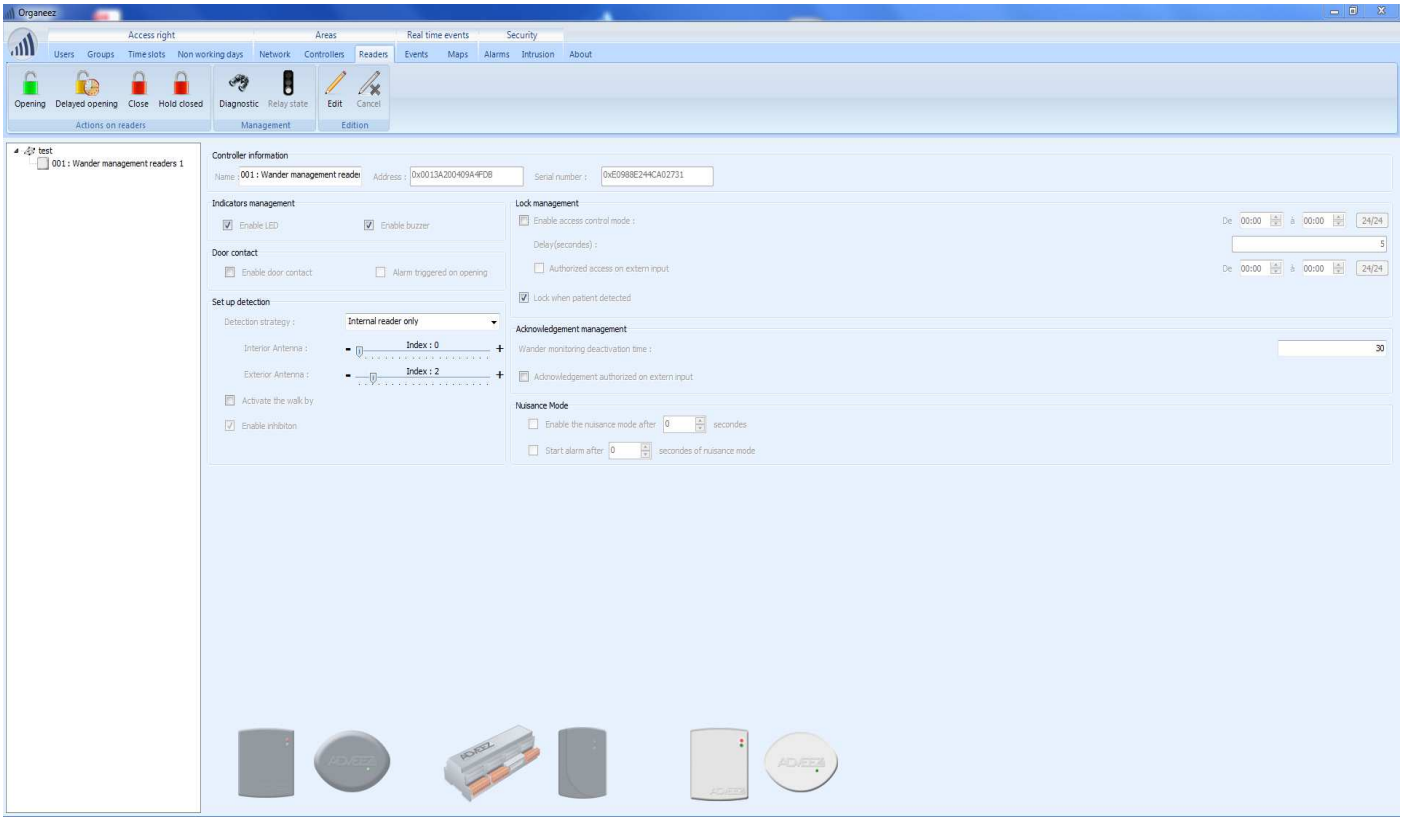
CONFIGURING UTL AND READERS

Once access control network is created, each door controller (AD-UTL-XX) needs to be configured. Following parameters: reader, locks, inputs such as door contact, motion detectors…

Reader configuration items is located in the “Reader set up” main window (which is activated by clicking on readers in the area tree window) and it consists on:

- Enabling the LEDs according to the relay state or the state of the door.
- Enabling the buzzer & adjusting the buzzer duration.
- Enabling relay mode: the door is unlocked while detecting an authorized credential, then stays open until a second credential is detected.
- Enabling escort which consists on preventing a given credential to unlock the door until a second accompanying credential is detected.
- Ticking the ‘Enabling counter’ which counts the numbers of allowed runs.
- Configuring the door lock:
  - NC: to control a magnetic lock
  - NO: to control an electric strike

Select the UTL and readers you want to set up

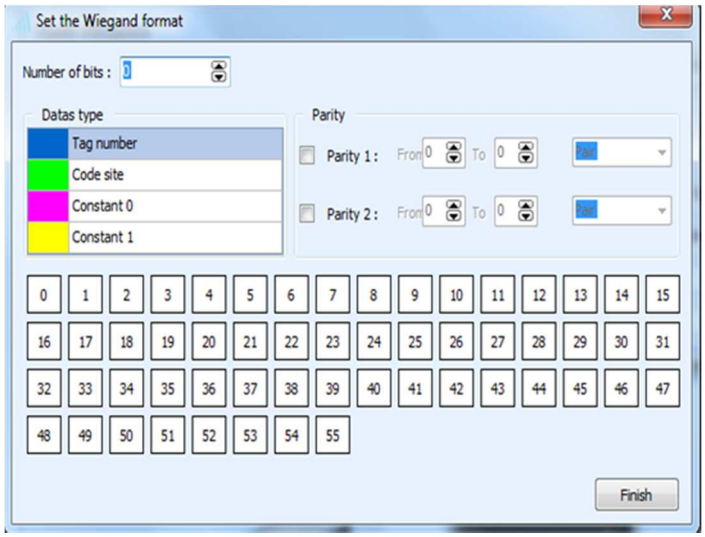


To configure the Wiegand frame:

1.In the form ‘Set the Wiegand format’, select the composition of your frame by.

A. Determining the bit number in your frame.
B. Defining the parity type
C. Defining the state of each bits:
   -Credential ID/number
   -Site code
   -Constant 0
   -Constant 1

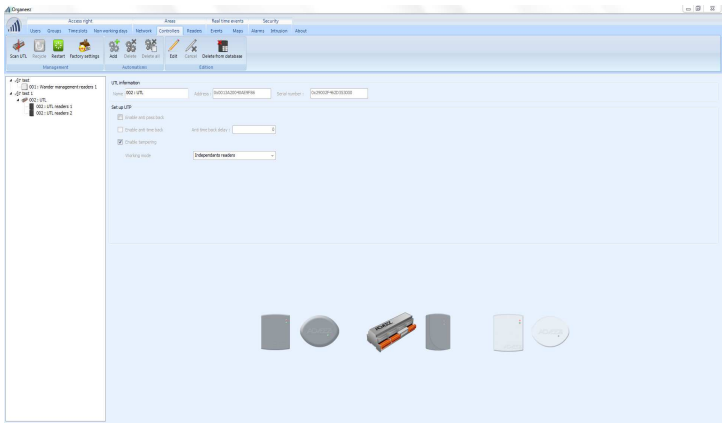
The credential ID bits must be entered consecutively.

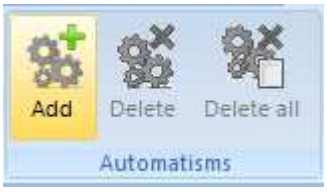


2. Click on finish once your frame is done.

To configure the UTL Automations:

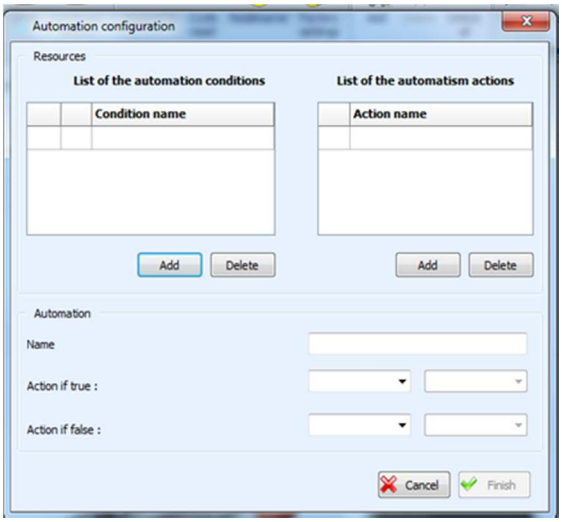
In the “Automation tool bar subset”, automations can be created and updated based on the access control system inputs (credential events, fixed dates…).

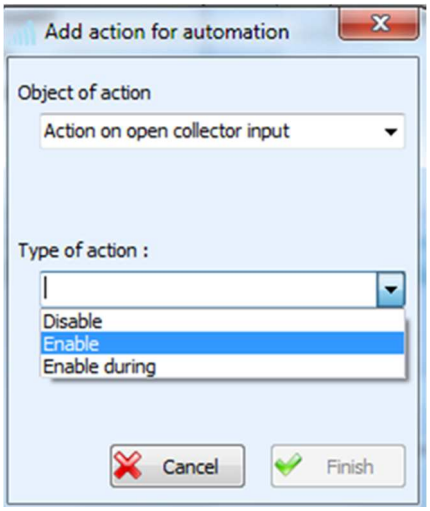


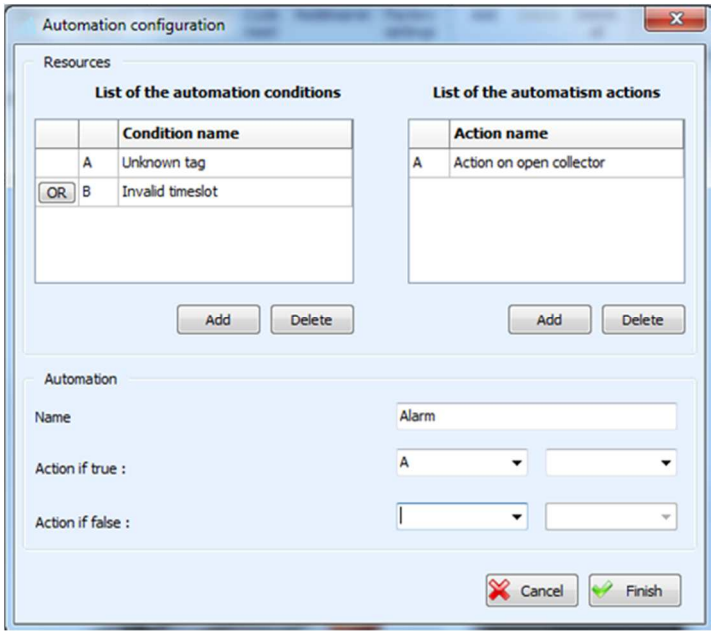


Conditions

1. Select the Input conditions (e.g. “unknown tag” or “invalid timeslot”) by clicking on the Boolean function in grey: “OR” or “AND” can be chosen.
2. Define the action by clicking on “Add”. Here on “open collector input” and define the type of action (“enable”).
3. Click on finish.



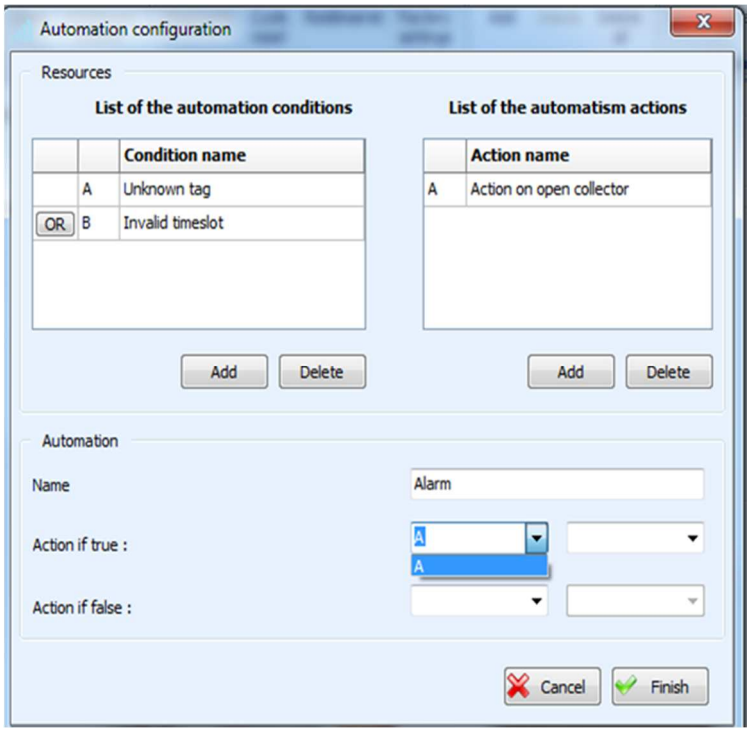




Action

4. If the « A » or « B » condition is true (if an unknown tag is presented or if a tag is presented on an in-valid timeslot) then open collector “action A” will be activated..
5. Click on finish to add the new automation.

Condition or action can be deleted by selecting them and clicking on “Delete”



CONFIGURING CONTROLLERS

Once access control network is created, each controller needs to be configured depending on the door configuration it controls and depending on the hands free configuration which is required: detection distance, reader position, lock delay, inputs such as door contact, motion detectors…

Controllers are adjusted as following:

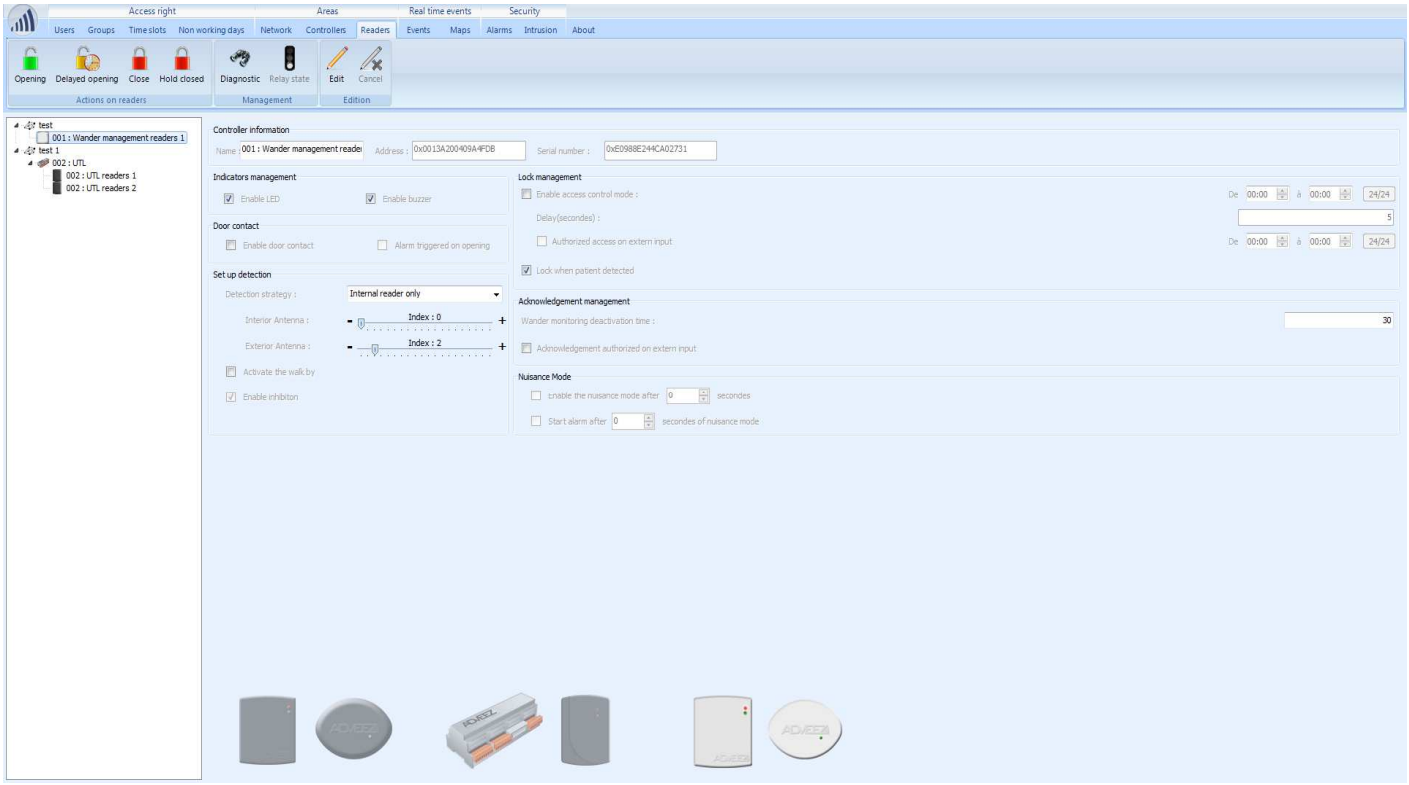
- The detection distance can be adjusted by moving the cursor thanks to the mouse

- Drop-down menu on the right enables: -

-choosing the reader function external reader (Stand alone, antenna ext), internal reader (Standalone antenna int), both external & internal reader (Two way circulation) or specific mode (Distinction int/ext)

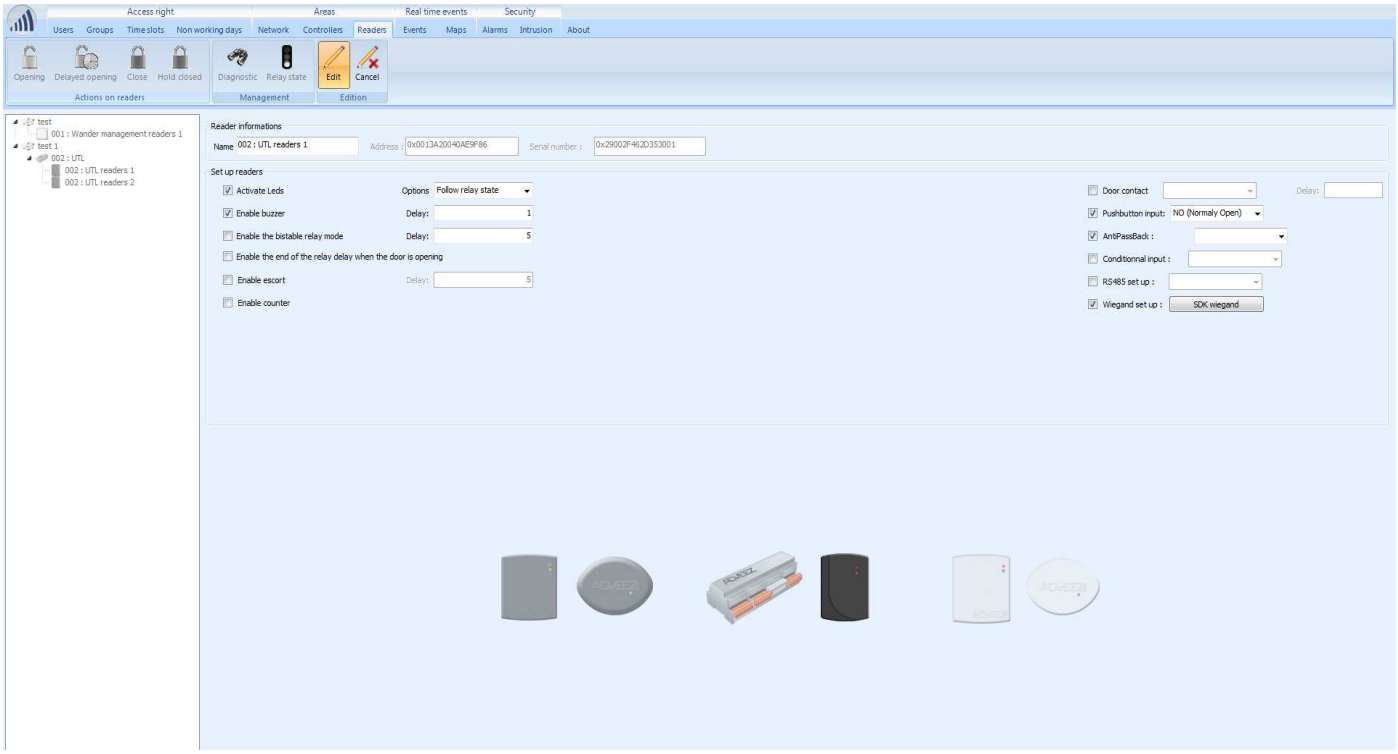
1. In area tab, select the area you want to set and click 'Edit' in the tool bar.
2. Select the activation time of the relay (between 1 and 60 seconds)
3. Tick the boxes of the item you want to activate: LED, buzzer, door switch
4. In order to avoid unwanted detections while hands free tags passing by in front of the reader with no intention of accessing the given door: The controller can check hands free credential 3 times in a row 3 times before granting access to allow the opening of the door. Simply tick "access confirmation" box.

The controller configuration can be done by using the jumpers, software configuration is then deactivated, check "Enabling jumper management"

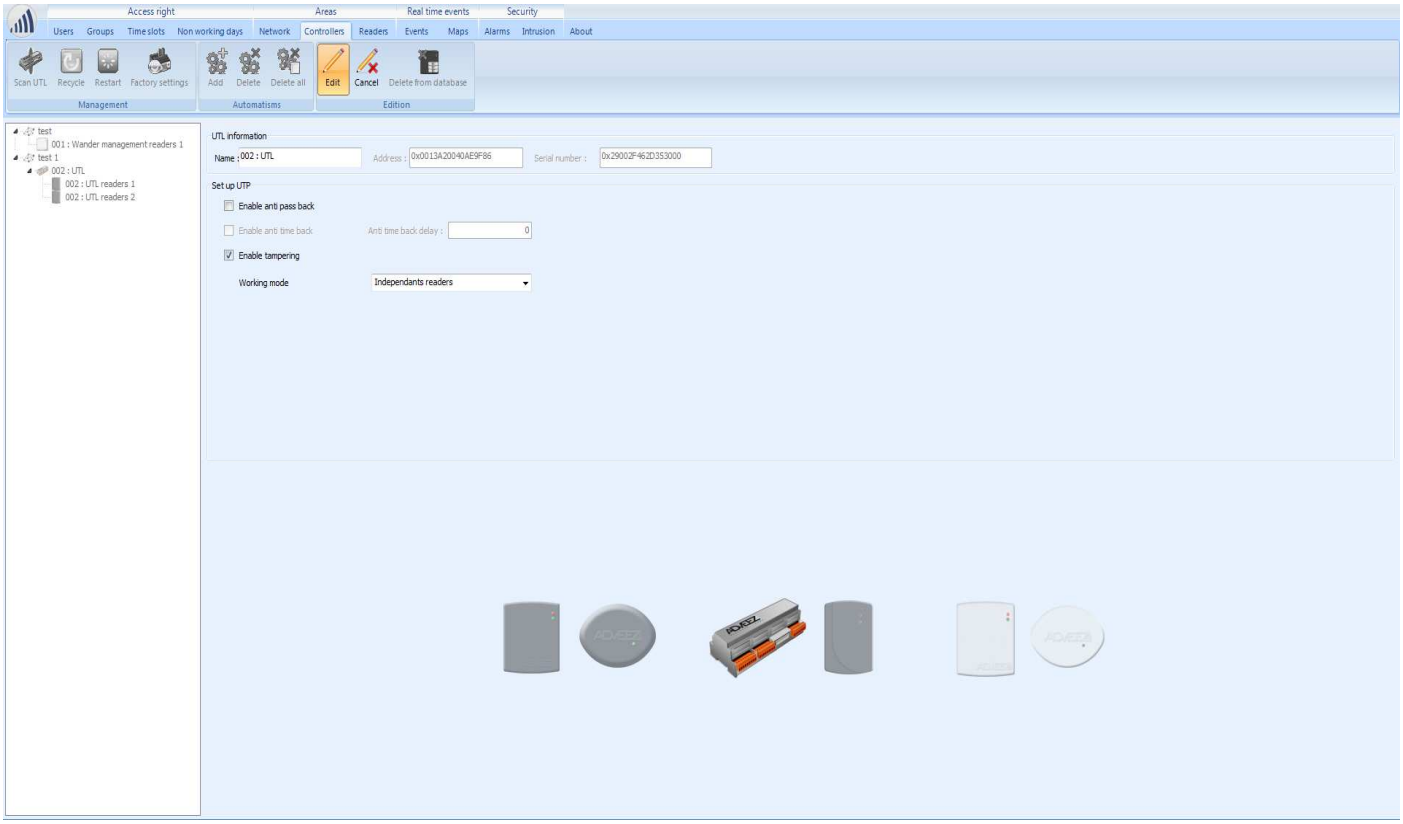


Activate anti-passback

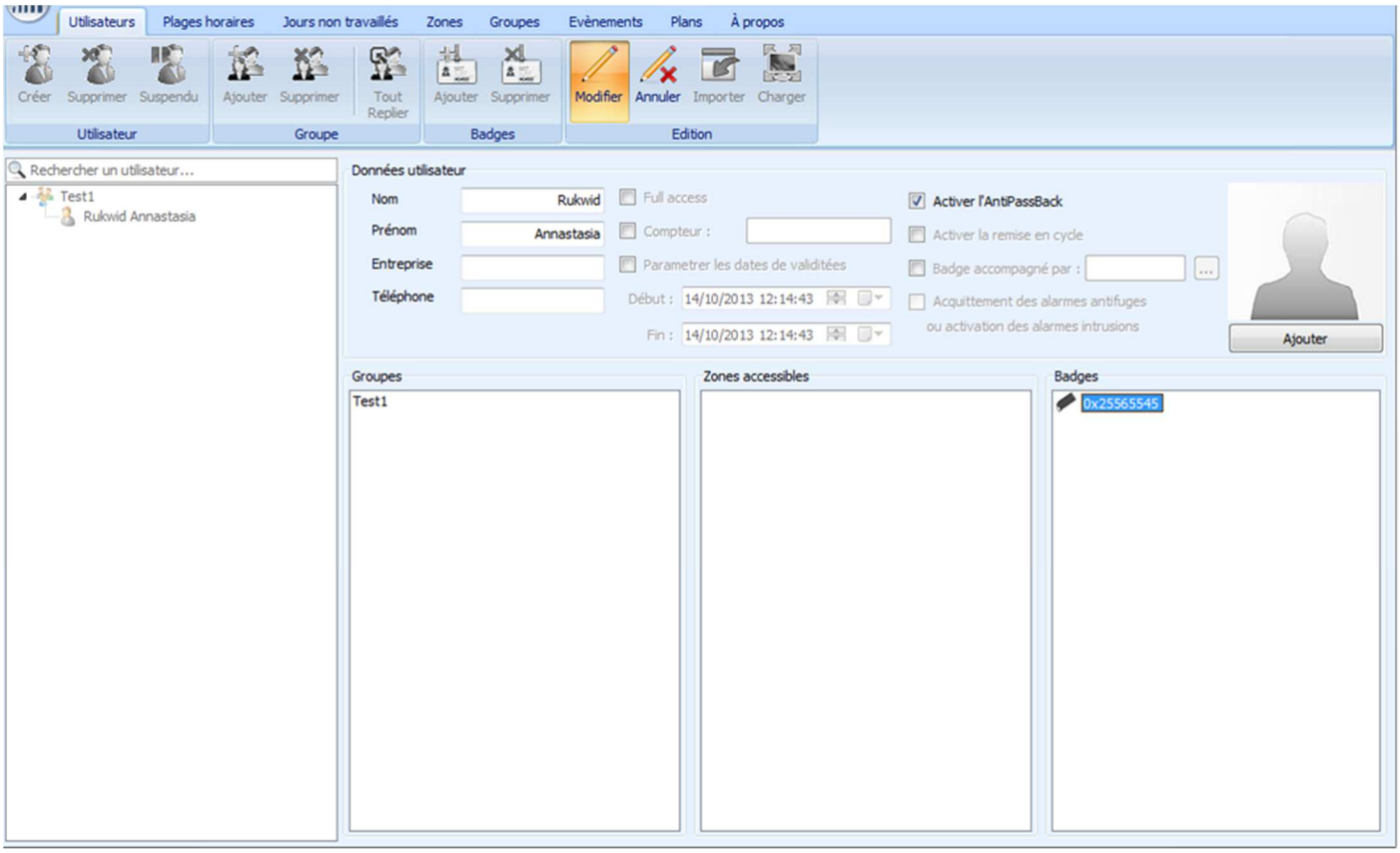
Select the "Zones" tab, select your drive and select the Anti-passback



Select the "Zones" tab, select your UTL and select the Anti-passback



Select the "Users" tab, select your user and activate the Anti-passback

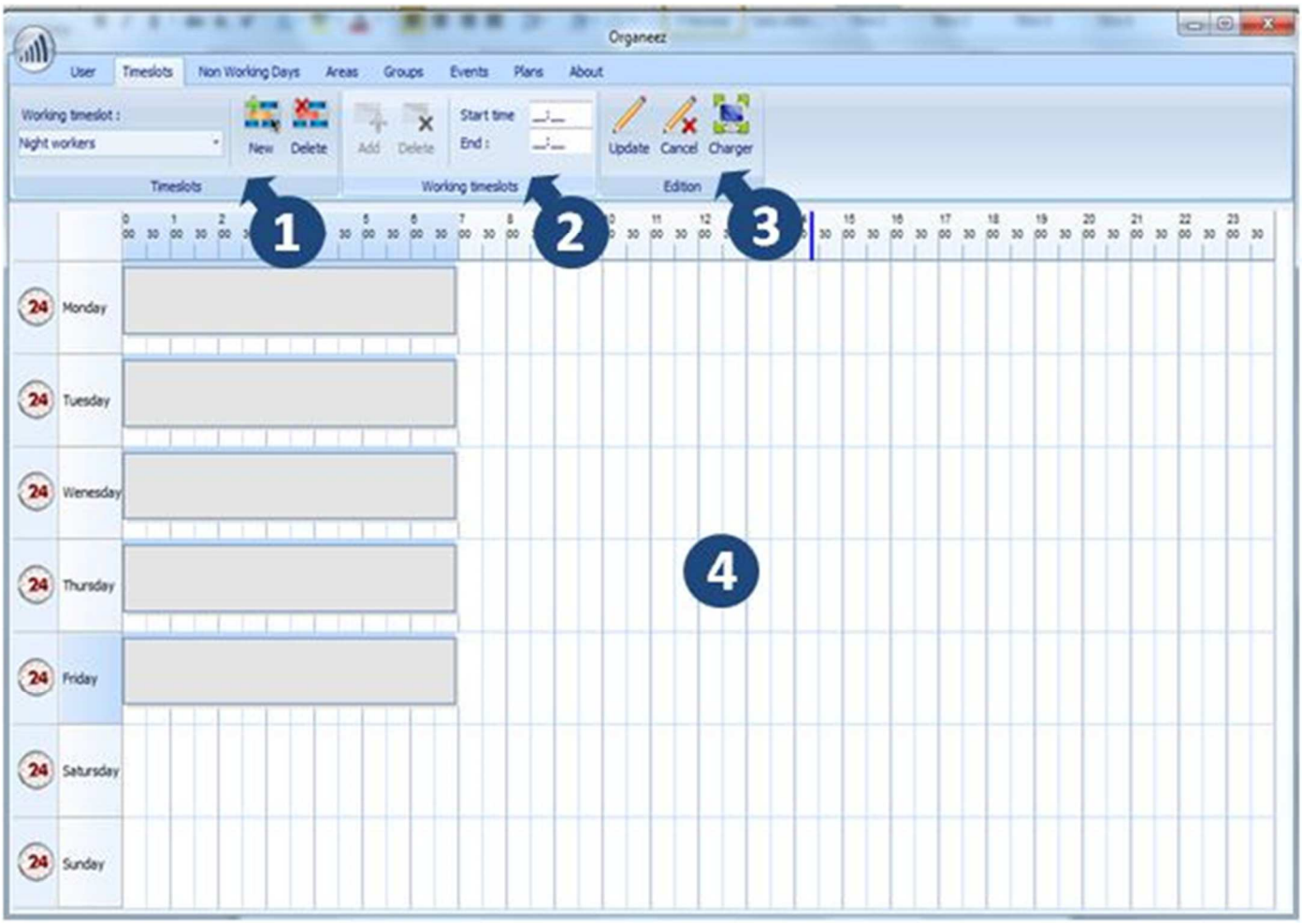


MANAGING USER GROUPS / CALENDAR / TIME SLOTS

This section details the process to set a cgroupwhich is a combination of a time slot and a group of non-working day. Maximum number of time slots per day: 7. A group of non-working days lasts over eighteen months. A group can be created directly by clicking on "Add group" in subset "Groups".

Overview of the time slots tab

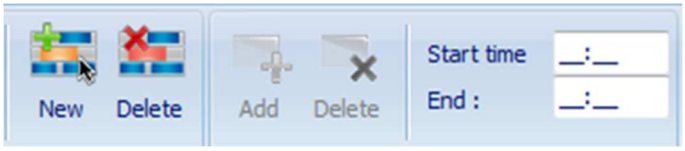
1. Managing time slots
2. Tools
3. Edition of the time slots
4. Overview of the time slots



How to configure time slots

1. In the subset ‘managing time slots’,

click on ‘New’

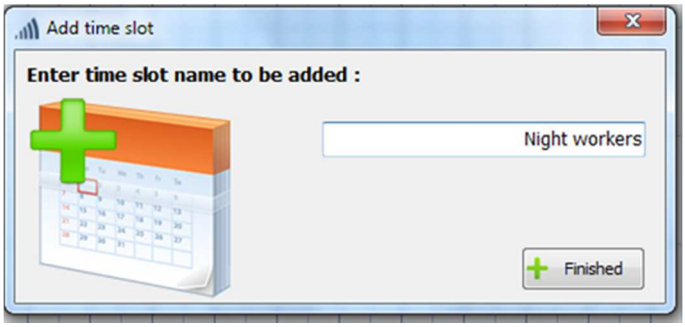


2. In dialog box ‘Add time slot’, give a

name to the time slot

3. Click on ‘Finished’

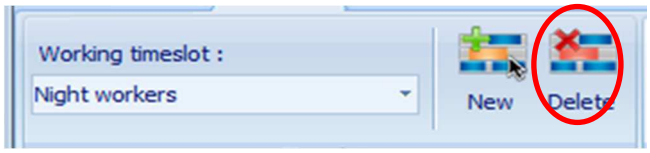
—> The time slot is added to the database



The time slot is created but is not associated to any group. It must then be assigned to a group, so that users can be entered into this group, and their access rights can be managed. This is done in tab 'groups'.

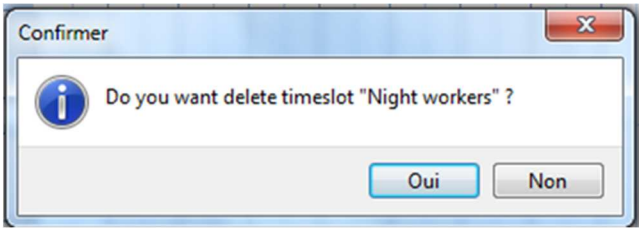
To delete a time slot:

1. In the subset ‘managing time slots’,
select a time slot in the drop down menu



2. Click on ‘Delete’

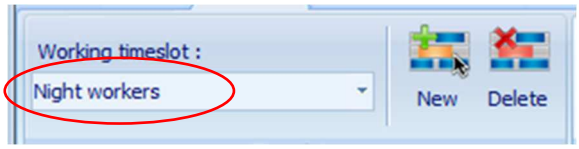
3. Confirm the removal in the dialog box
‘Confirmer’



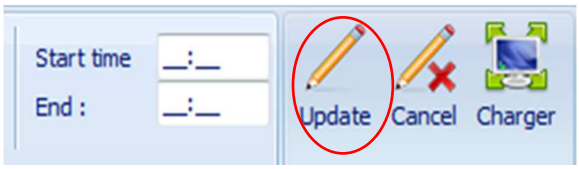
—> The time slot is removed from the database

To edit a time slot:

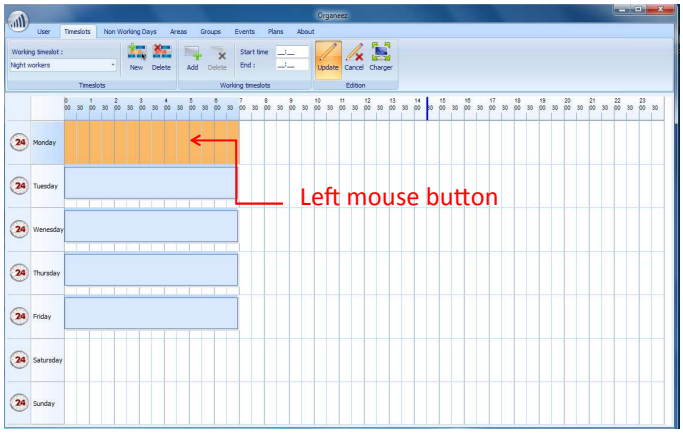
1. In the subset ‘managing time slots’,
select a time slot in the drop down menu



2. In the subset ‘Edit’, click on update



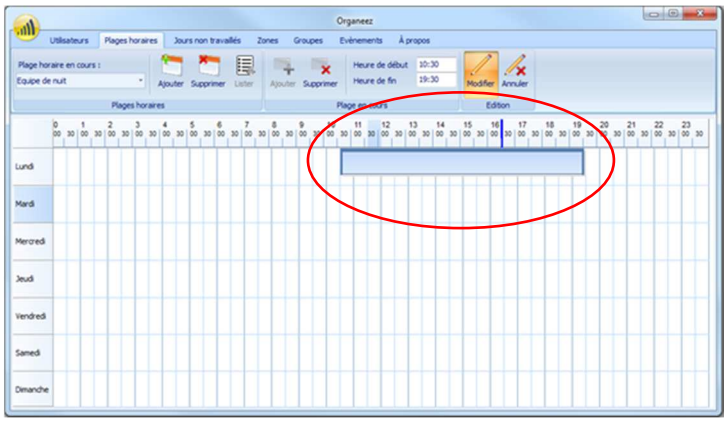
3. In the subset time slot, select a range



3.1To add a time range, click on add

in the subset tools

—> The time range is validated and turns blue



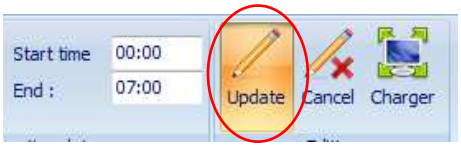
Repeat the process as many times as necessary to complete your time slots

3.2 To delete a time range, click on delete
3.3 In the subset tools

In the edition subset :

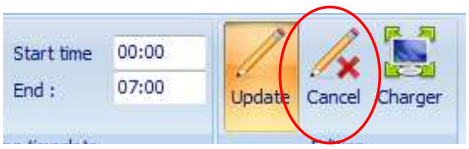
Validate

Click on ‘Update’



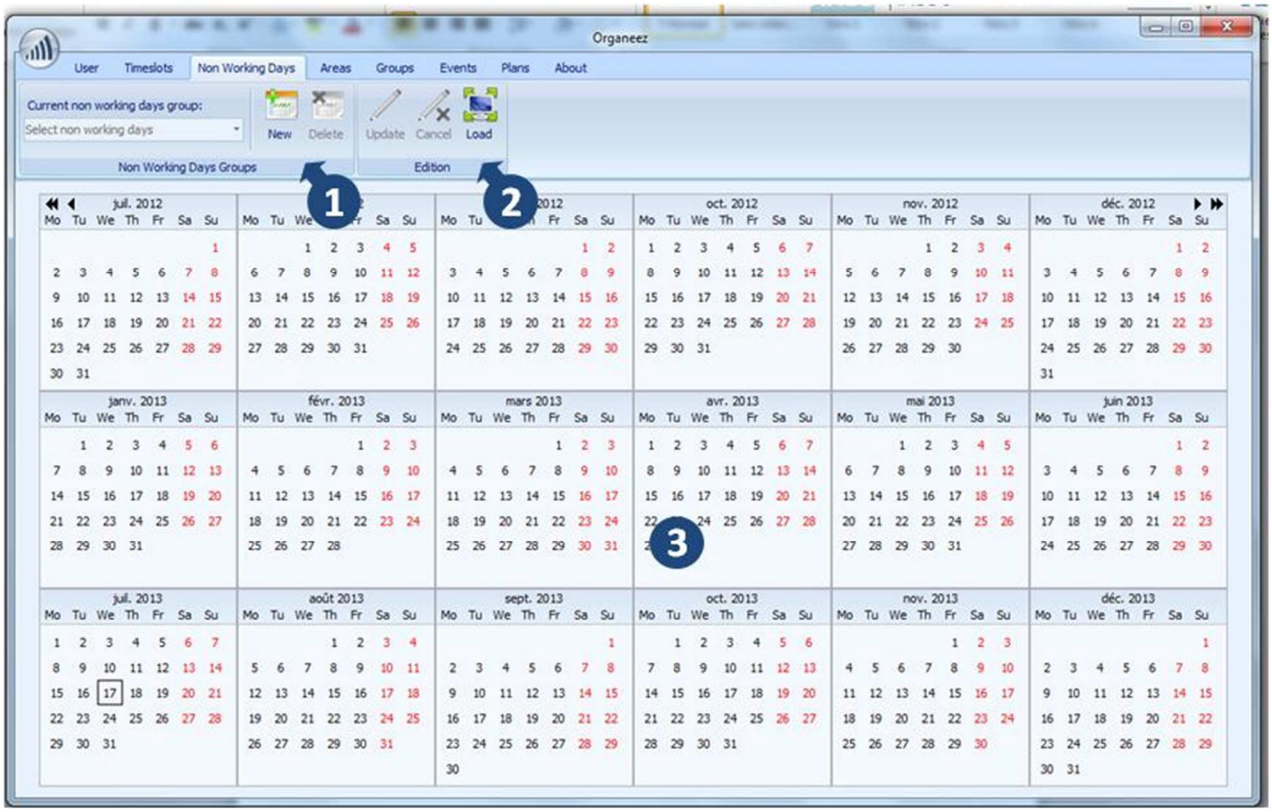
Cancel

Click on ‘Cancel’



Overview of the non working days tab

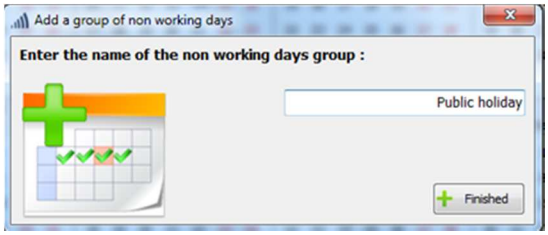
1. Managing non-working days groups
2. Edit non-working days groups
3. Overview of a non-working days group



To add a non working days group:

1. In the subset Managing non-working days groups, click on new

2. In the Dialog Box that appears, give a name to the non-working days group
3. Click on 'Finish'

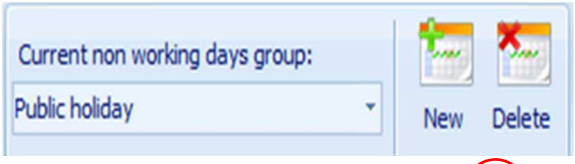


—> The non-working days group is updated in the database

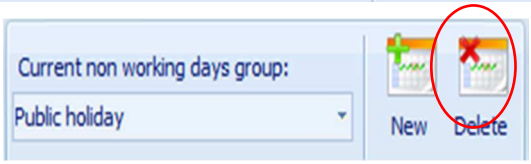
The group of non-working days is created but is n but is not associated to any group. It must then be assigned to a group, so that users can be entered into this group, and their access rights can be managed. This is done in tab 'groups'

To delete a non-working days group:

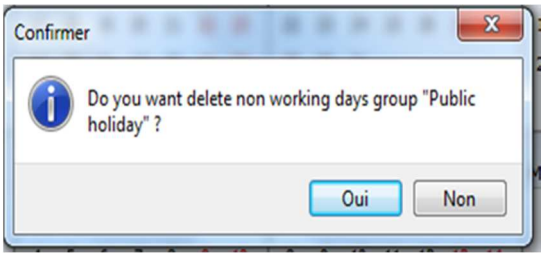
1. In the subset managing non-working days, select a non-working days group in the drop-down



In the subset managing non-working days**, c**lick on delete



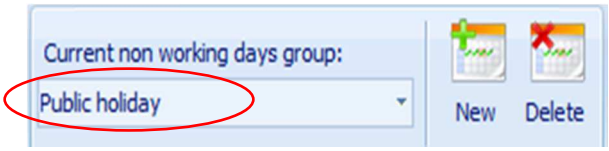
In the dialog box, confirm the removal



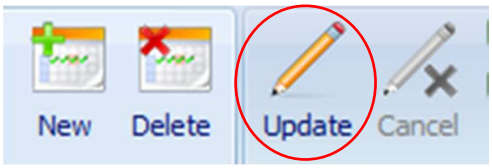
—> The non-working days group is deleted from the database.

To edit a non-working days group:

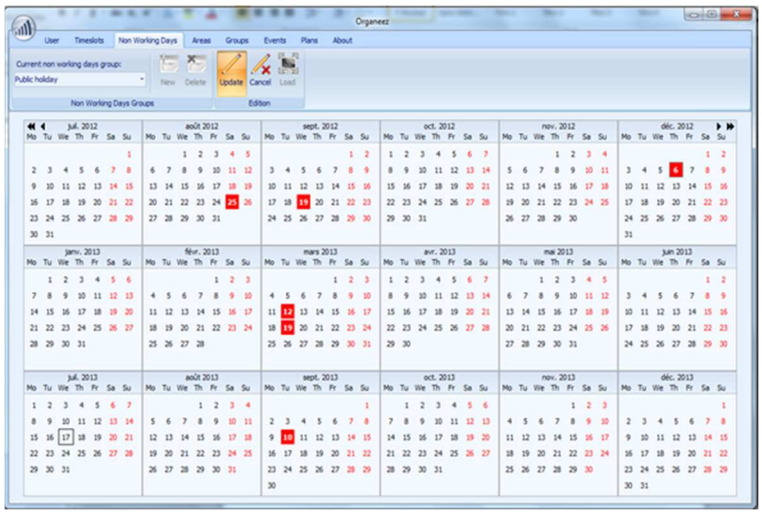
1. In the subset managing non-working days, select a non-working



2. In the edition subset, click on update



3. In the subset overview of a non-working days group:

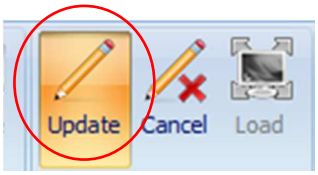


3.1 To add a non-working day, choose the non-working days by clicking

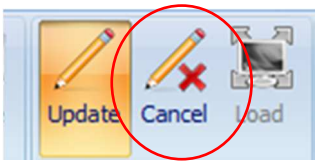
3.2 To delete a non-working day, click again on the day

In the edition subset :

To validate the creation of a non-working days group, click on update



To cancel the creation of a non-working days group, click on cancel

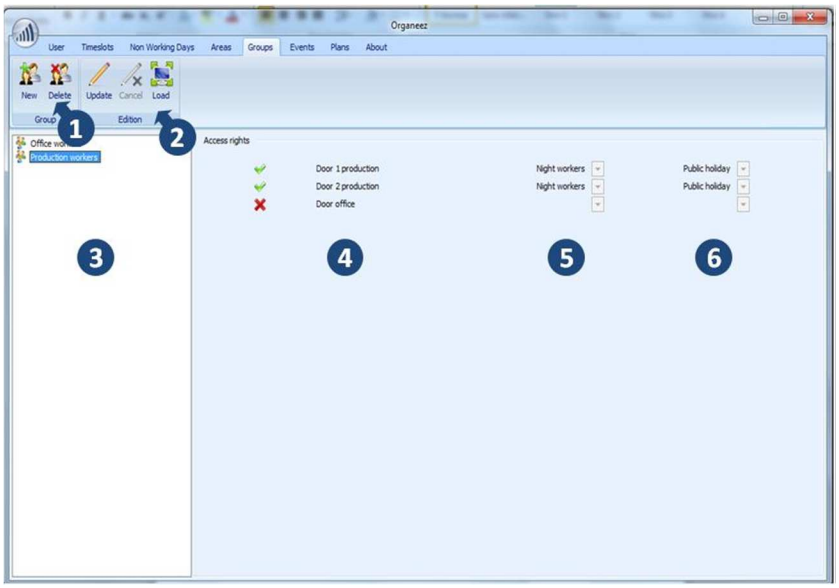


MANAGING USER LIST

In this section you will learn how to create and edit a list of users. You can associate multiple users with each other through groups. A group must specify the area of application and schedule applicable.

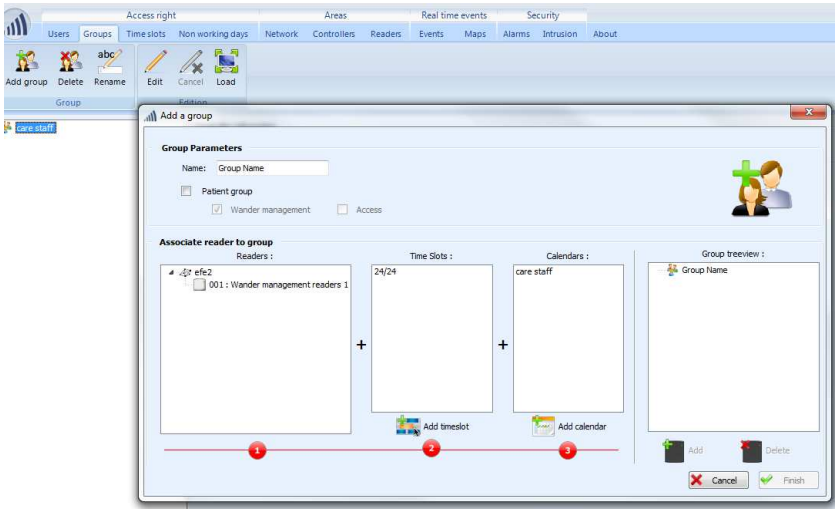
Overview of the "groups" tab

1. Managing groups
2. Editing group
3. Group list
4. Area list
5. Time slot list
6. Non-working days list



How to add a user group

1. In the subset managing groups, click on 'Add group', *A group can be created directly by clicking on "Add group" in subset "Groups".*
A dialog box "Add a group" appears:



Readers :

Select area

Time slots :

Select a time slot

Add a time slot if necessary

Calendars :

Select a non-working days group

Add a non-working day if necessary

Group name :

Give a name to your group

Click on finish

Controllers of related area will be updated with info:

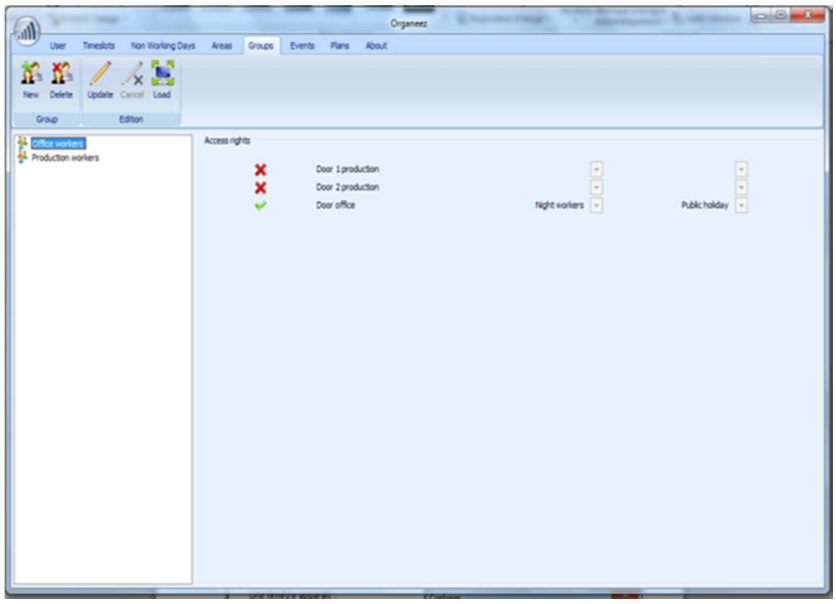
Time slot is created or modified

The non-working days group is created or modified

The group is created

—> Database is updated.

To delete users group

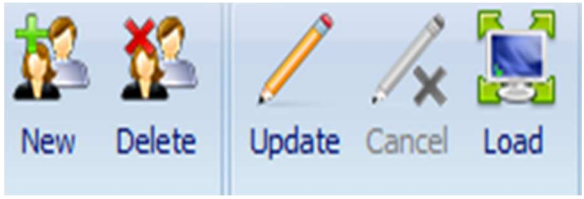


1. In the subset groups list,

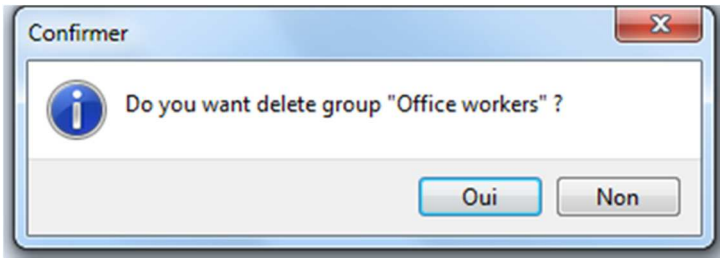
select a group

2. In the subset managing groups,

click on ‘Delete’

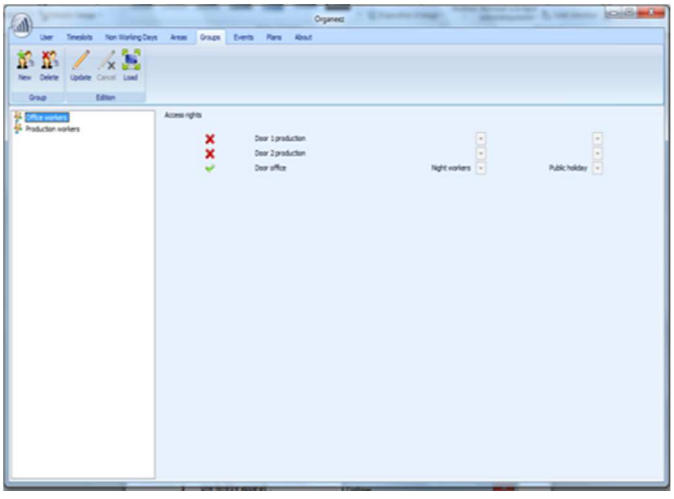


3. Confirm the removal in the dialog box



—> The non-working days group is deleted from the database and the stations of the area.

To edit users group



1. In the subset groups list, select a group

2. In the subset editing groups, **c**lick on ‘Update’

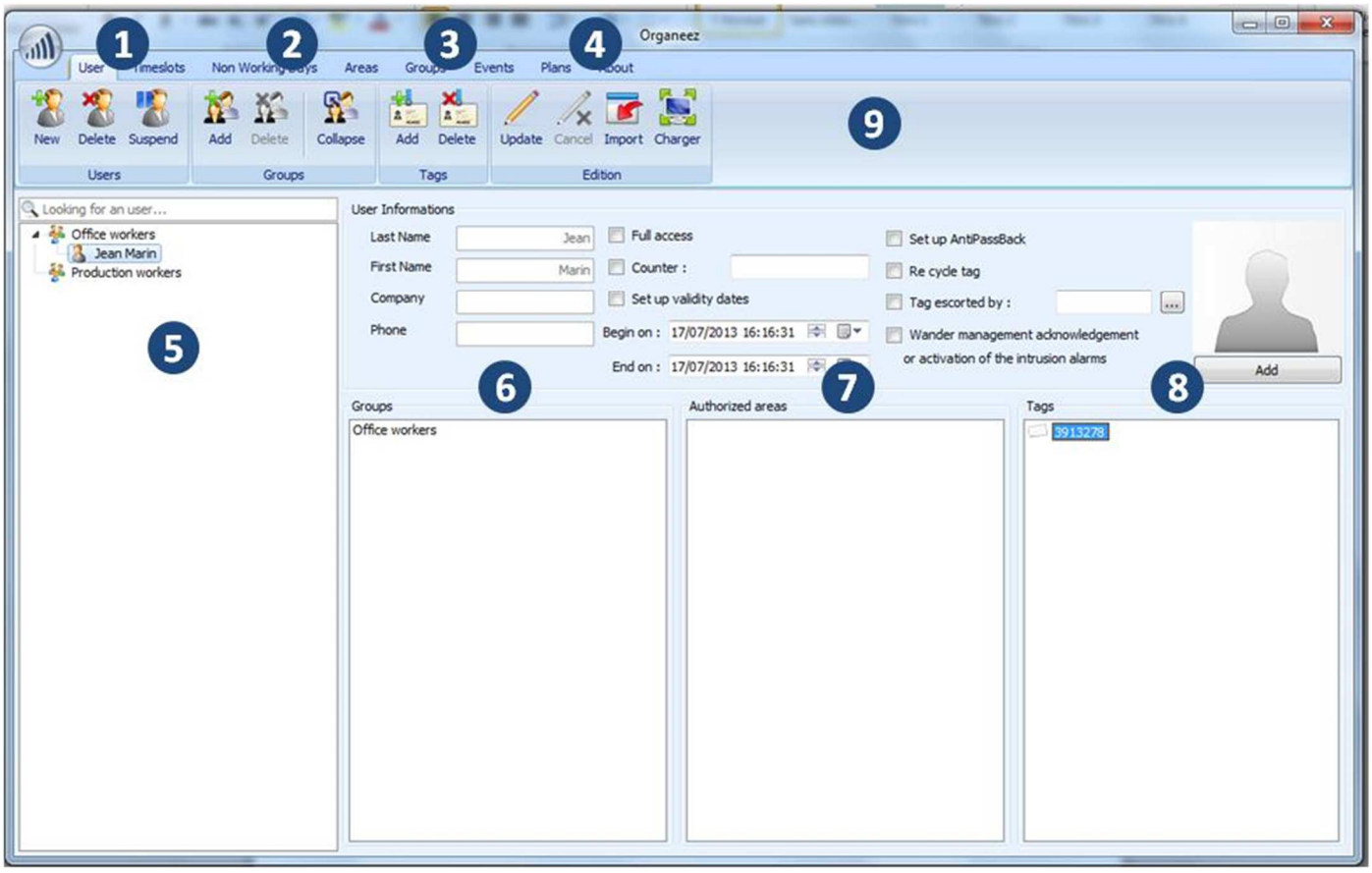
3. To change the settings of a group
   3.1 In the subset areas list:
   Select or unselect areas
   3.2 In the subset time slots list:
   Modify time slot
   3.3 In the subset the non-working days groups list :
   Modify the non-working days group

4. To validate group modifications In the subset edition, Click ‘Update’

5. To cancel group modifications, click on cancel

Overview of the users tab

1. Managing users
2. Managing groups
3. Managing tags
4. Edit users
5. Tree users
6. User groups list
7. Area list accessible to the user
8. User list tags
9. Overview of the user information



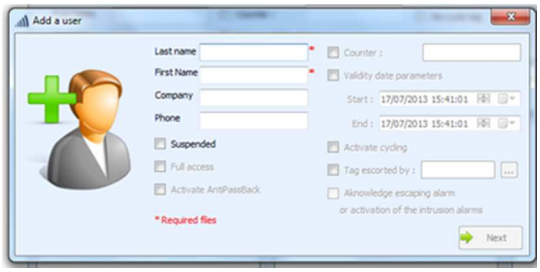
To add user

1. In the subset managing users **:**

   Click on new

2. A dialog box appears :

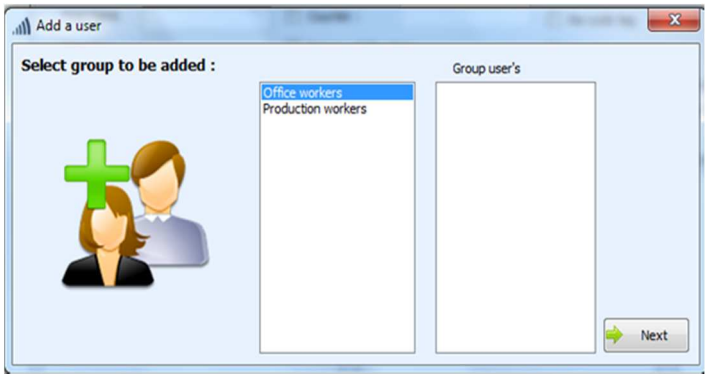
   Fill in fields
   Click on next



3. On the next window :

Select the groups to which the user must be added

Click on next



4. On the next window :

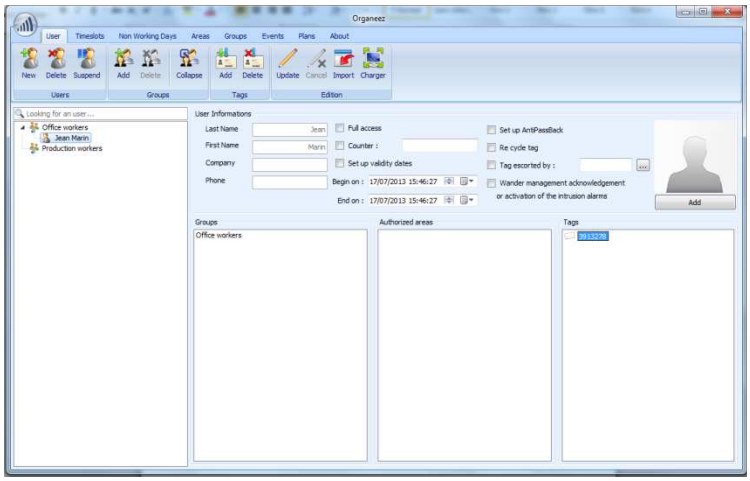
Scan the badge on the dedicated slot on the autoreez

5. On the next window :

Click on finished to create new user

6. The tree users is updated

To delete user



1. In the tree users:

Select user

2. In the subset managing users :

Click on delete

3. A window appears :

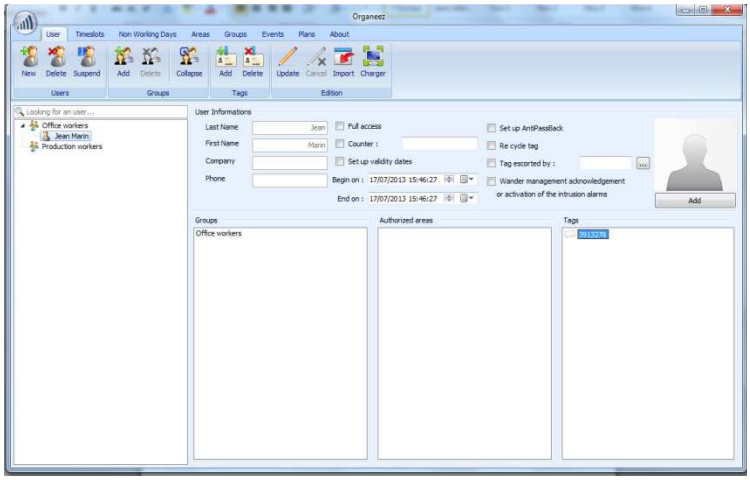
Confirm removal

User is deleted from the database and the stations of the area

Editing user rights/info

1. In the “user” tree:

Select a given user

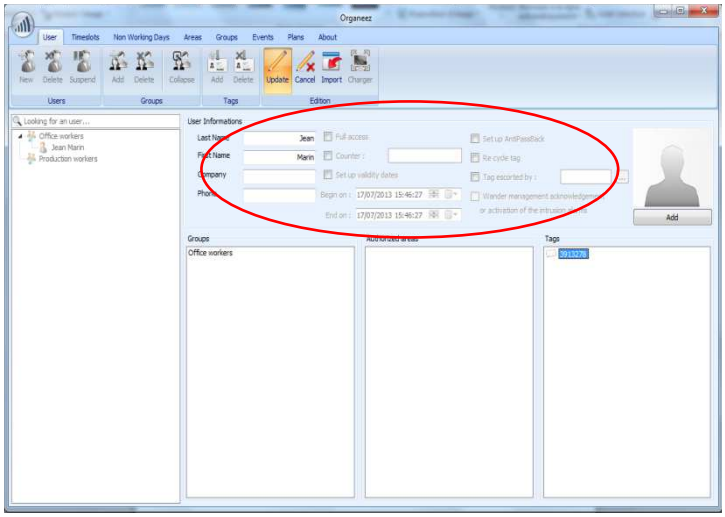


2. In the subset edit users:

Click on update

3. In the subset overview of the user information:

Modify the related fields



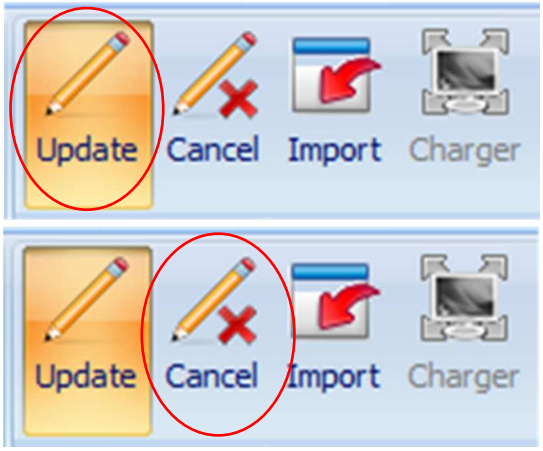
4. Edit user information :

+ Valid group modifications

Click on update

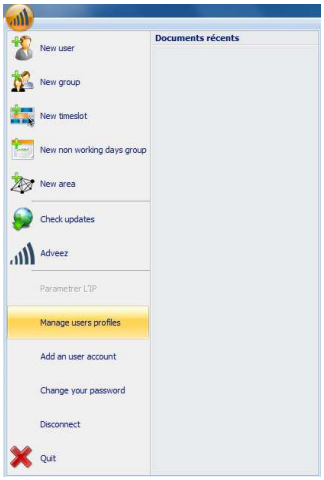
+Cancel modification group:

Click on cancel

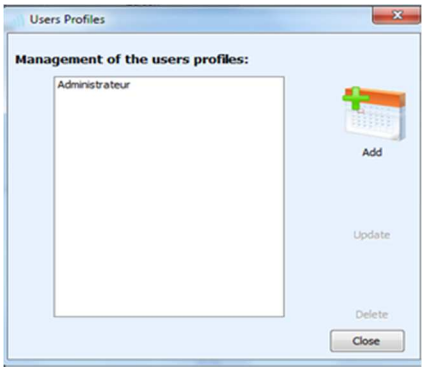


To add and edit user profile

After clicking on the logo Adveez I click on "manage user profiles"



P to add a user profile, I click on "add"



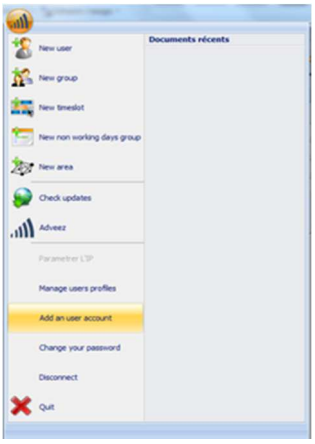
In the window that just appeared I give a name to my new user profile.

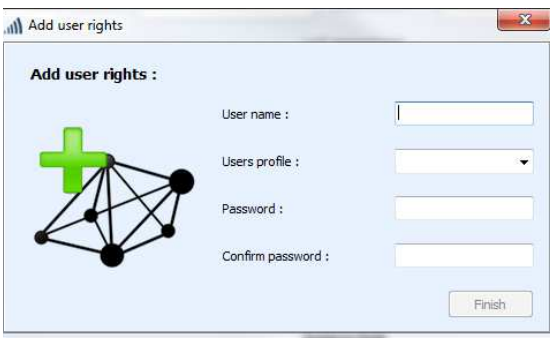
Then I can tick a list of actions that my profile may or may not do (here he can add and delete users).

Then I click "Finish".

I can now assign my user profile to the desired person.

I click "add a user account." I fill the cells of the window that appears and click finish. The user receptionist can now add and delete users.

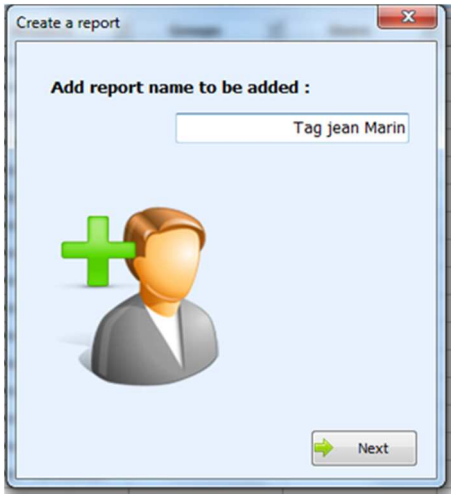




EVENT HISTORY/ REPORTS

This section how to view event history, sort events, export event lists, delete or sort events.

Exporting events



1 In the subset manage reports, click on export

2 A window appears:

- Save in the folder dedicated

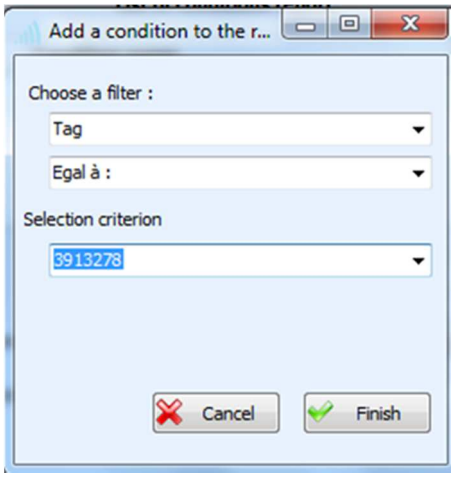
To edit events

1 In the subset manage reports:

Click on edit

2 Browse the folder where event history file has to be stored in the dialog box:

Give a name at the report to be added
Click on next



3 A new window appears:

Click Add
Choose a filter
Give a criterion of selection
After give all necessary data, click on Finish

4 To finalize editing reports:

Enter the name of the created condition in “association of the conditions”
You can enter many conditions and associate them with operators like “AND”, “OR”, “(“, “)”.

—> Click on Finish

To associate report

In the subset manage reports:

In associate a report, click on the drop down arrow
Choose your report

To delete report

In the subset manage reports:

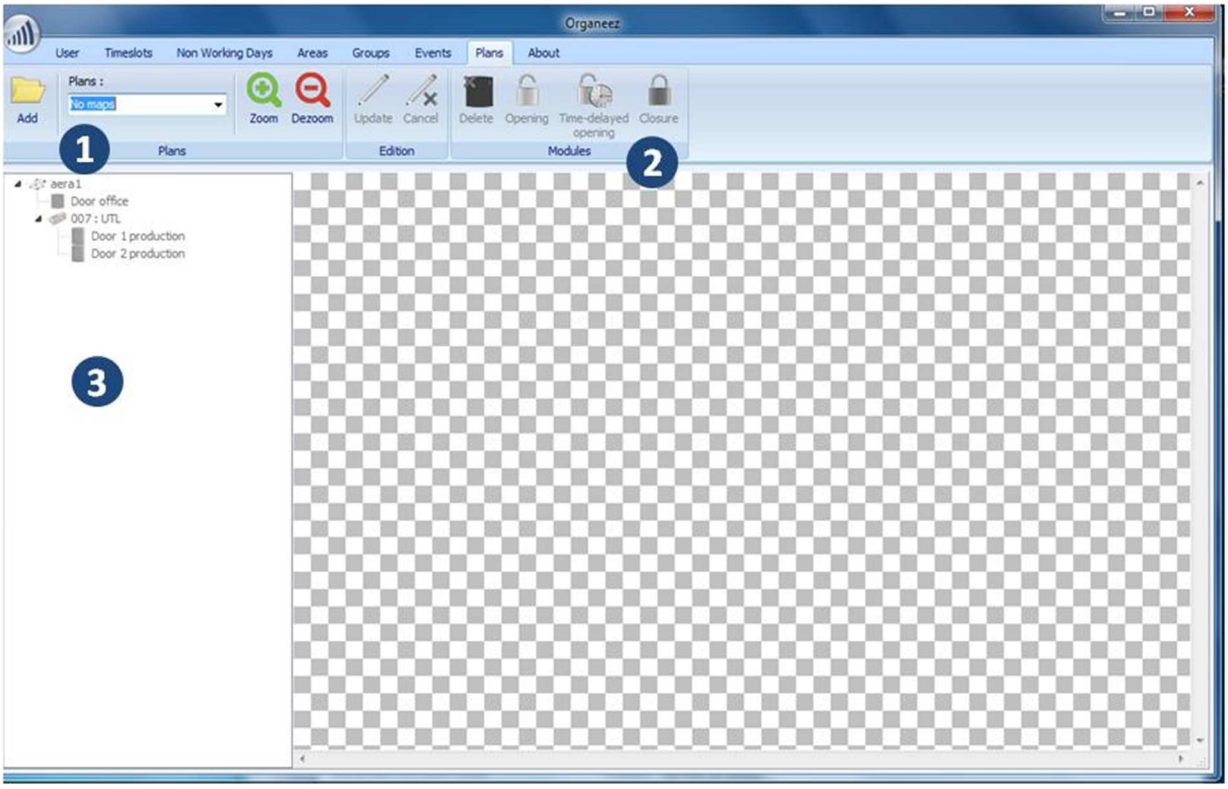
In associate a report, click on the drop down arrow. Choose the report you want to delete
Click on delete.

MAPS

The "map" functionality gives a clear site overview by displaying readers on a site map picture file. This map enables controlling the reader remotely and gives access to each reader's event log.

Overview of the MAPs tab

1- Manage plans
2- Manage modules
3- Tree areas



To build a MAP:

1 In the subset "Maps", click on add to open the file

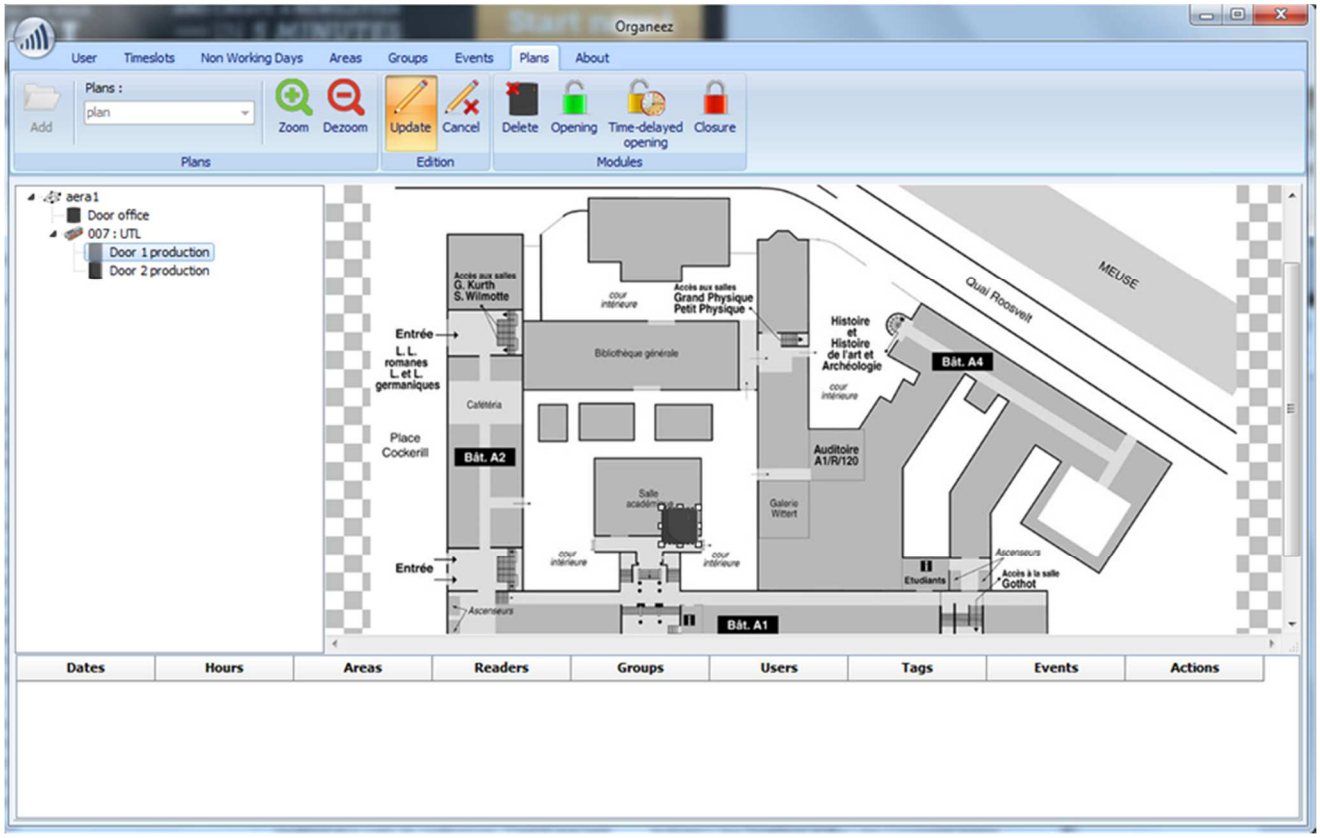
2 In the area tree

Choose a controller
Drag it & drop it on the map
Once reader is on the map, it can be moved, its size can be adjusted.
Event histories of each reader will be displayed in a window frame below site map by clicking on reader icon.

To remote opening/closure:

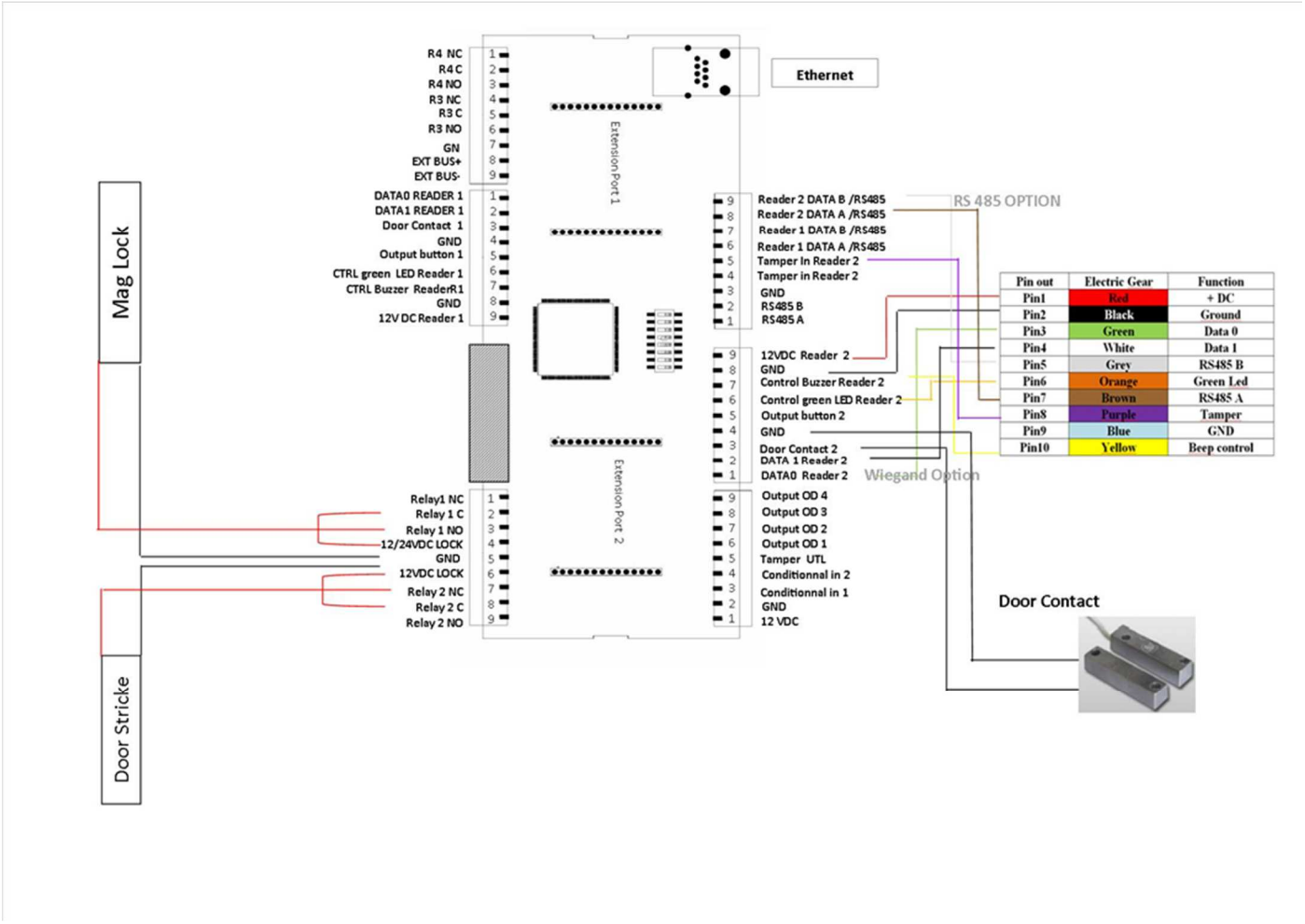
1 In the subset modules

Click on « opening », « time delayed opening » or « closure »



INSTALLING UTL

AD-UTL-XX type of controller must be installed on a DIN rail and supplied by 12V DC. Up to 2 readers and their electric strike or electromagnetic lock can be connected as shown in the wiring diagram below. As most of system installation troubles are caused by wiring issues, following wiring diagram must be carefully taken into account.



Connections to plug in advance to start on the software: **DESKTOP VERSION**

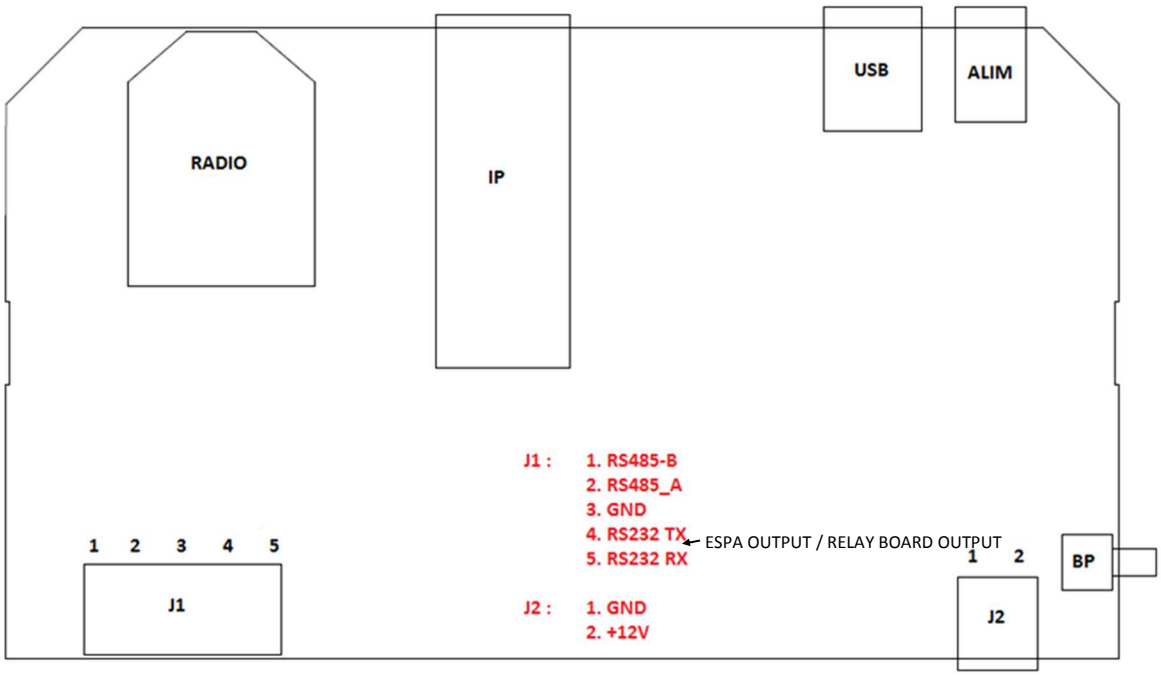
1. Power the desktop version by the Jack connector power supply.
2. Connect the USB cable to the PC

Connections to plug in advance to start on the software: **DIN Rail VERSION**

12V supply by terminal block J2.

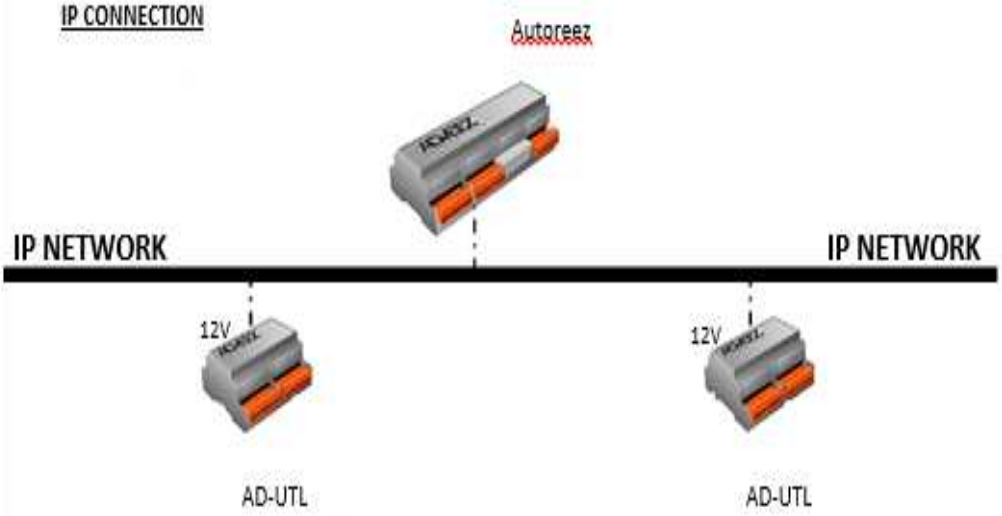
Connect the TCP / IP network cable to initiate the connection to the PC

Connect the RS485 BUS if needed (if UTL RS485 on the access control system)

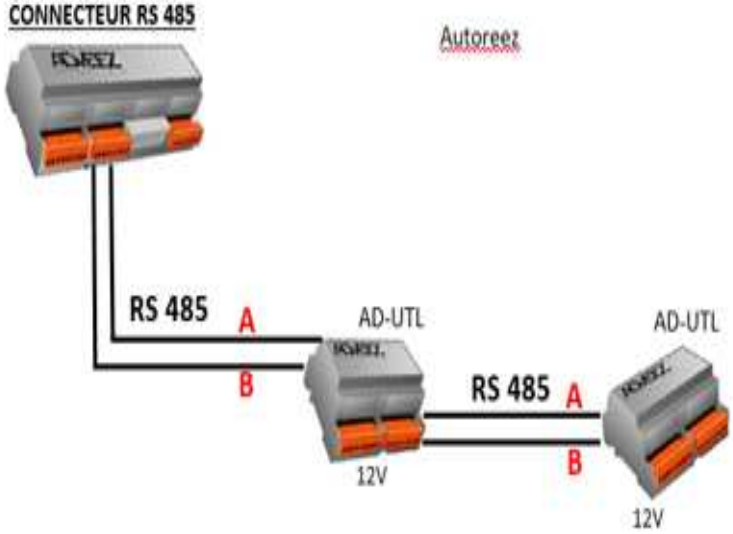


CONNECTION BY TYPE OF NETWORK

IP CONNECTION

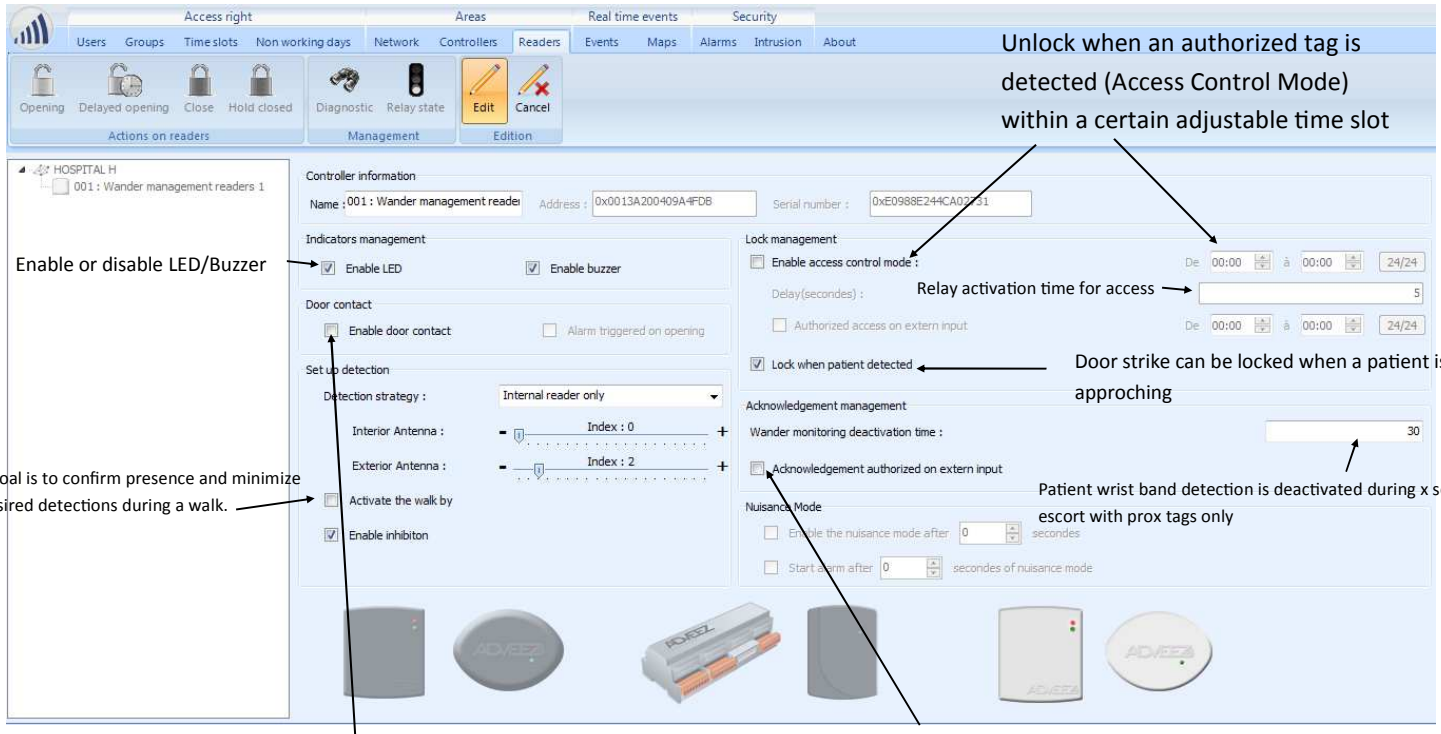


CONNECTEUR RS 485



WIRELESS CONNECTION

A) General parameters



.

When the door contact is activated and the option "alarm triggered on door opening" is not checked, the alarm is triggered as soon as a patient is detected.

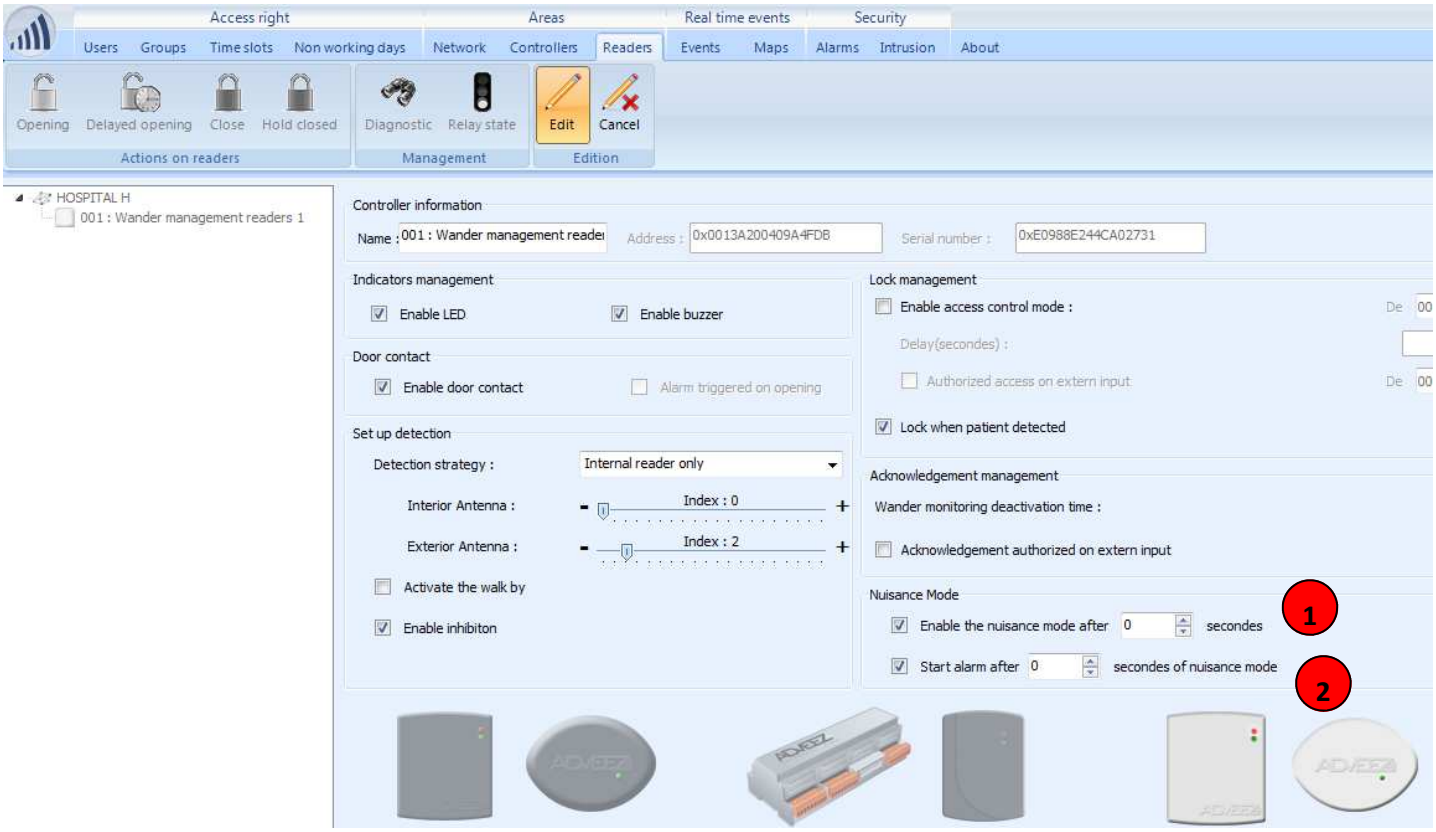
If not the alarm is triggered when a patient is detected + door opening.

B) Nuisance Mode

Door contact must be connected and activated in order to enable this feature:

① When a wristband is detected a beep is activated after x seconds to urge the patient to move away from the door. Once patients left detection zone then controller stops beeping.

② Nuisance mode is activated: If patient stays inside the detecting area for more than (y seconds) an alarm is triggered.

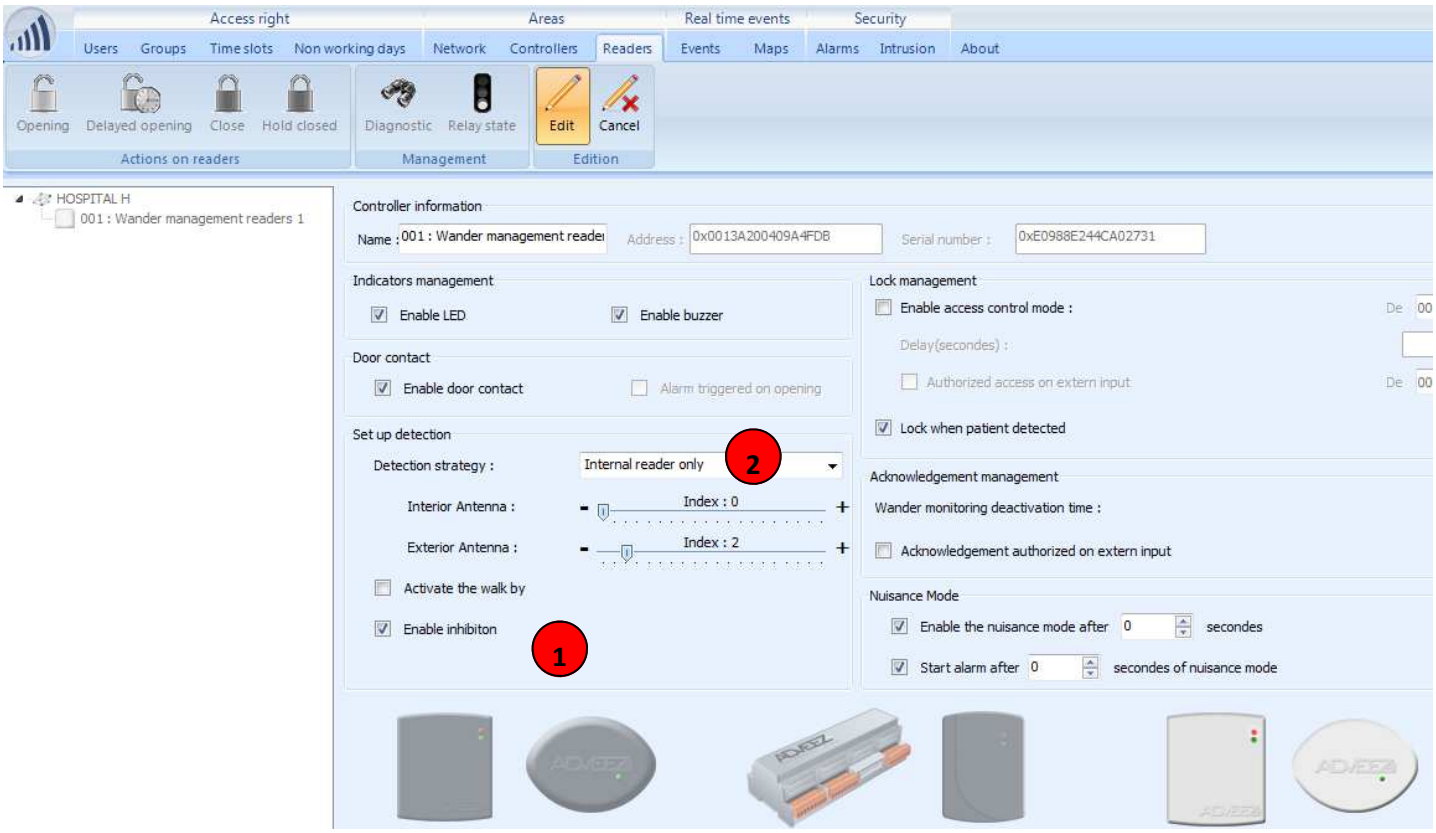


C) Inhibition

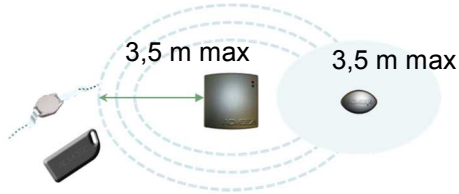
Non-desired detection can occur in certain areas since controller detection zone is a sphere and detects through brick, wood…. Then, using a controller + external antenna, one detection zone can be used in order to mask a portion of the other, where no detection should be performed.

① Select inhibition option

② Select component which should perform detection. If internal reader is chosen, then controller will detect wander monitoring tags and external antenna will inhibit (=mask) tag detection.



Hereafter typical case of deactivation (in blue) via external antenna on controller detection zone.

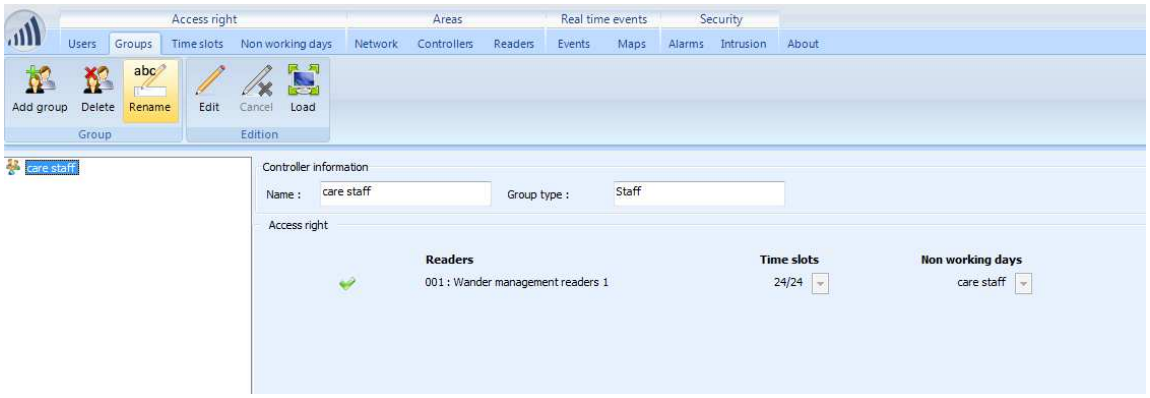


CONFIGURING WANDER MANAGEMENT USERS/PATIENTS

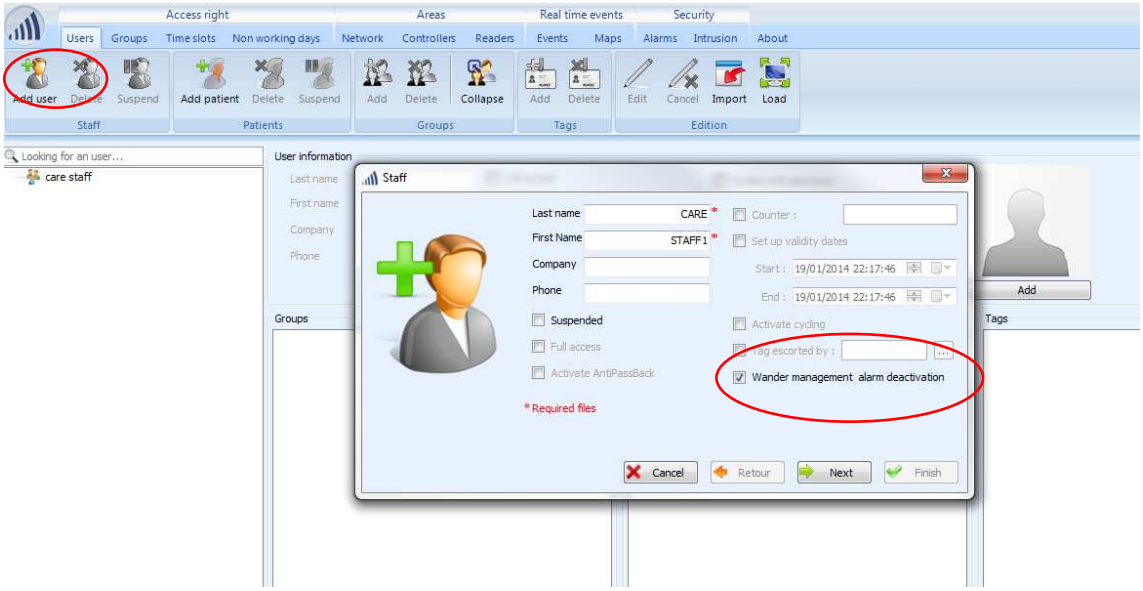
This section how to assign rights to deactivate wander monitoring alarms generated by AD-CARE-C wander management controllers and wrist band watch tags for disoriented patients. It also describes how to enroll patients in the database (= how to assign wander management wrist band tags to patients).

How to add a care person:

1 A group is first created, which is supposed to care for disoriented patients.



2 A user must be added to which “Wander alarm management alarm deactivation” right will be assigned by ticking the related box in the dialog window.



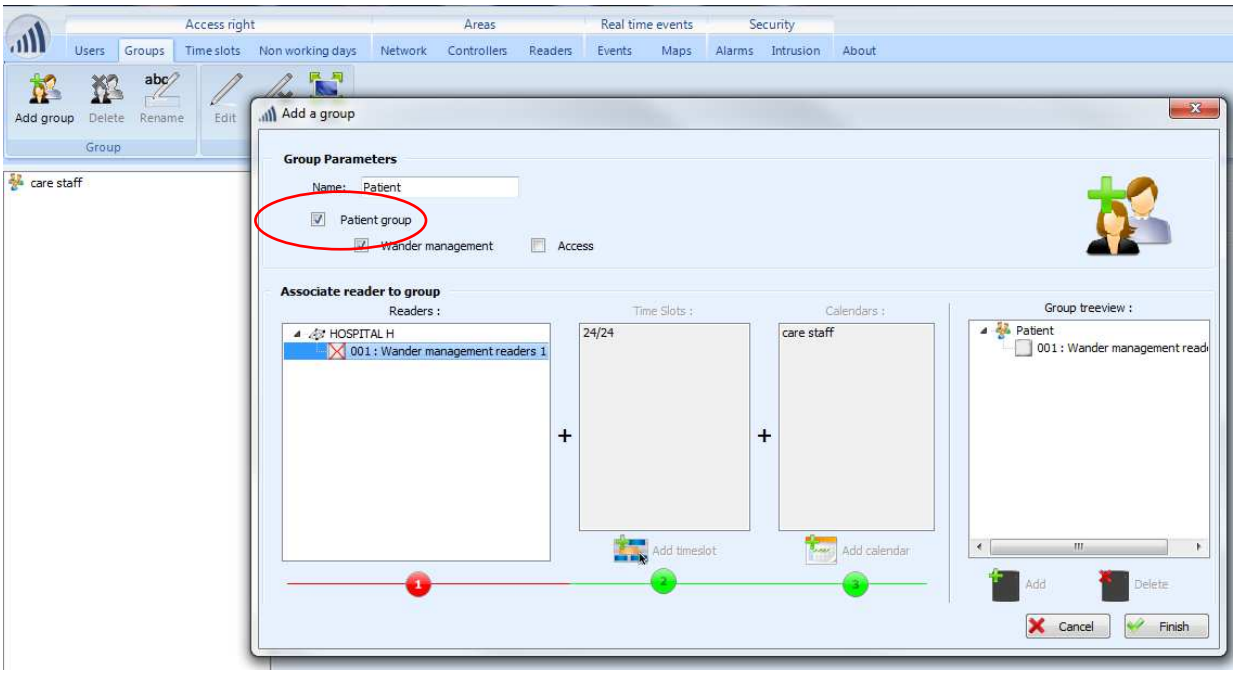
3 People having hands free tags will be able to escort disoriented people with no specific action, while people with prox tags will have to put their tag close to the controller in order to deactivate wander monitoring.

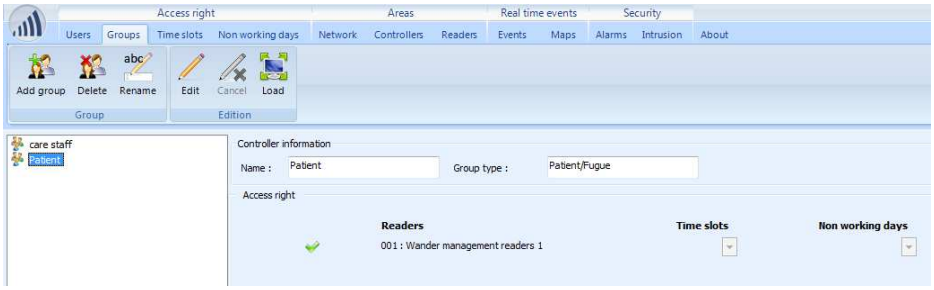
How to add a disoriented patient:

1 A group is first created, which will contain only disoriented patients. “Patient group” tick box must be activated.

2 Controller which will monitor this patient (on the given location) must be added to the group.

3 Neither any time slot, nor any calendar is required. Click on finish, then Patient group has been created.





A) ESPA or POCSAG OUTPUT

Patient name and access name (controller label) can be sent to an external messaging device via ES-PA4.4.4 or POCSAG by configuring alarm outputs of network manager AUTOREEZ (RS232 output)

① Click on « Autoreez set-up »

② Configure baudrate, ESPA adresses….

③ Configure call mode by clicking on « add »