



# Access control software **SENATORFX**

*Quick start guide*

---



## CONTENTS

CONTENTS .....	2
INFORMATION .....	3
1) PC specifications .....	3
2) RS485 bus connections .....	4
3) Ethernet network connections .....	5
4) Software installation .....	6
SETTING UP THE SITE .....	7
1) Launching the software .....	7
2) Setting up the control unit network .....	8
3) Setting up the control units .....	9
4) Setting up the readers .....	10
5) Using biometry .....	11
6) Setting up access groups with time zones .....	15
7) Setting up badges and users .....	17
8) Setting up the software operators .....	18
9) Setting up the data stream log .....	19
10) Managing the system history .....	20
MULTI-WORKSTATION SYSTEM .....	21
NOTES .....	22



## INFORMATION

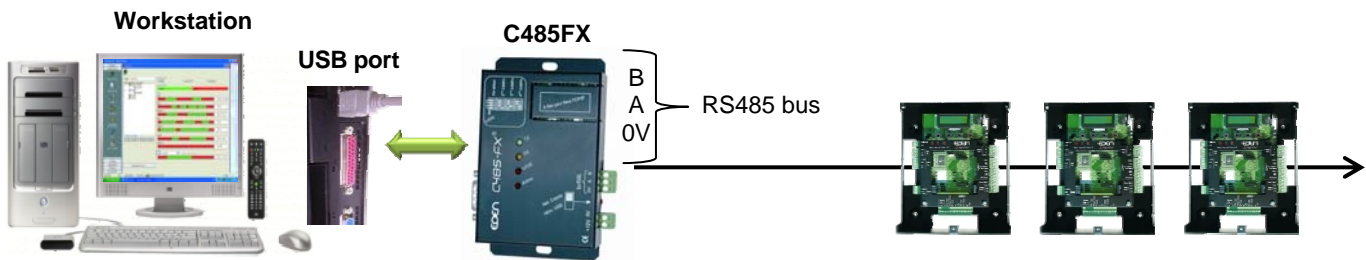
### **1) PC specifications**

- o Windows® 2000, XP and VISTA™ compatible.
- o 1 GHz processor with a minimum of 1 GB RAM.
- o Minimum disk space of 2 GB.
- o 2 available USB ports.
- o CD-ROM drive.
- o Sound card.



## 2) RS485 bus connections

- o Connect the **C485Fx** interface to your PC as well as to your network of control units



If you intend to connect several interfaces to the PC, you need to configure the addressing switches. (See Technical Information).

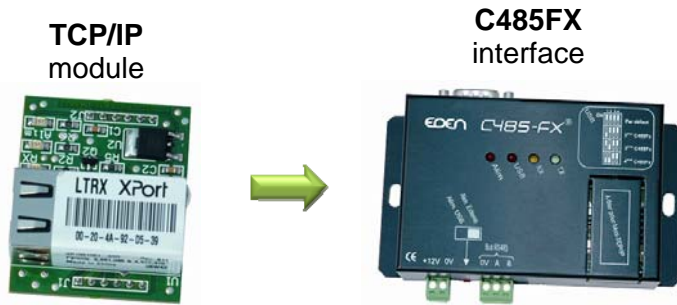
A dangle (protection key) must be installed on one of your system's control units. (See Technical Information)

- o This interface does not need a driver or an external power supply. However, you must ensure that the power supply switch is set to "**Alim USB**".
- o If the workstation does not have an available USB port, refer to the installation instructions supplied with the C485Fx interface for connection to an RS232 port.

### 3) Ethernet network connections

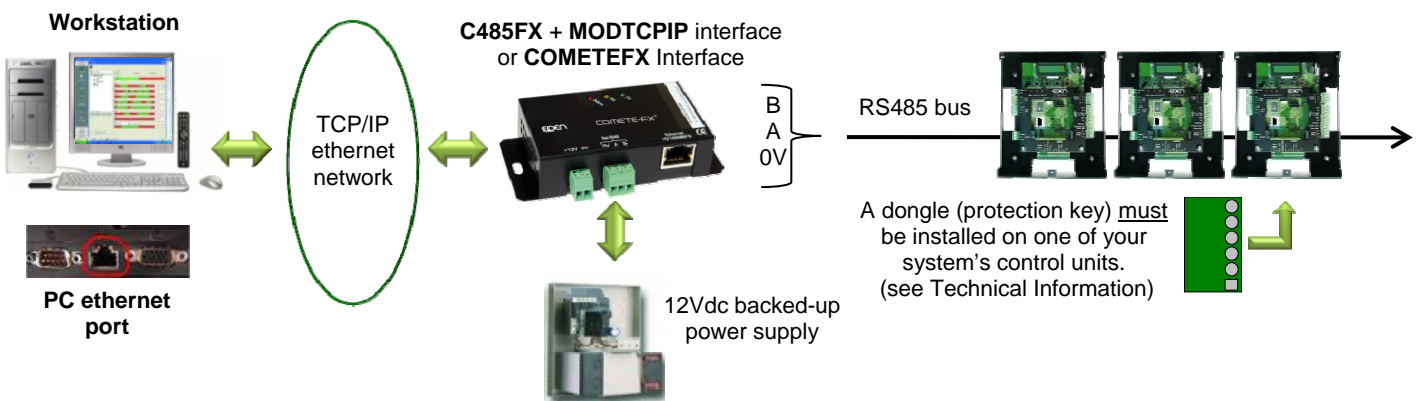
#### Integration of the MODTCP/IP module in the housing for the C485FX interface supplied with SENATORFX:

Remove the 2 mounting screws from the cover of the C485FX then insert the module as follows:

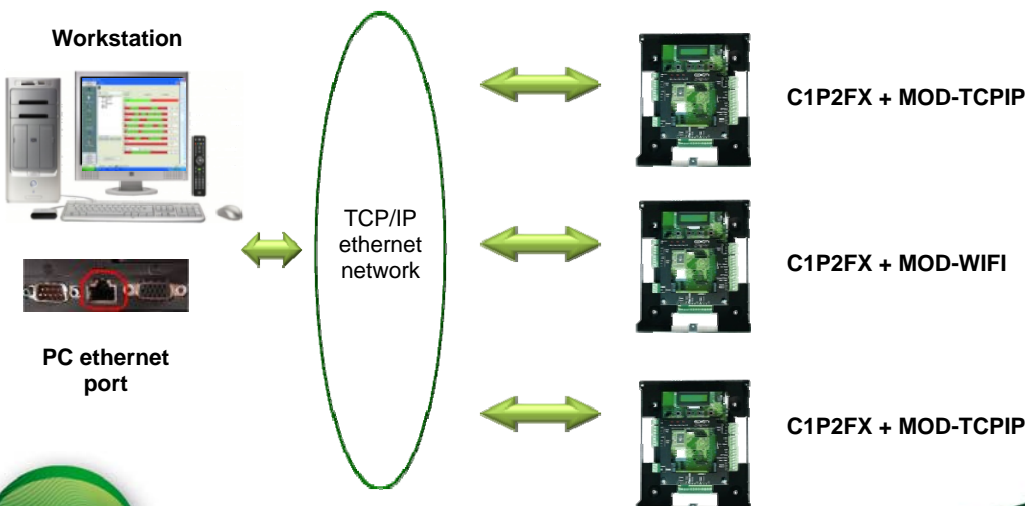


Replace the cover and secure it using the 2 screws

When using a module, you will need to connect a 12 V DC external power supply to the interface. You should also ensure that the power supply switch is set to “Alim. Externe”.



#### Using the MOD-TCPIP and MOD-WIFI communication modules:



### 4) Software installation

Insert the **SENATOR® FX** CD-ROM in your drive and wait for automatic installation to begin. Then, follow the instructions that appear on your screen.



Select the installation language



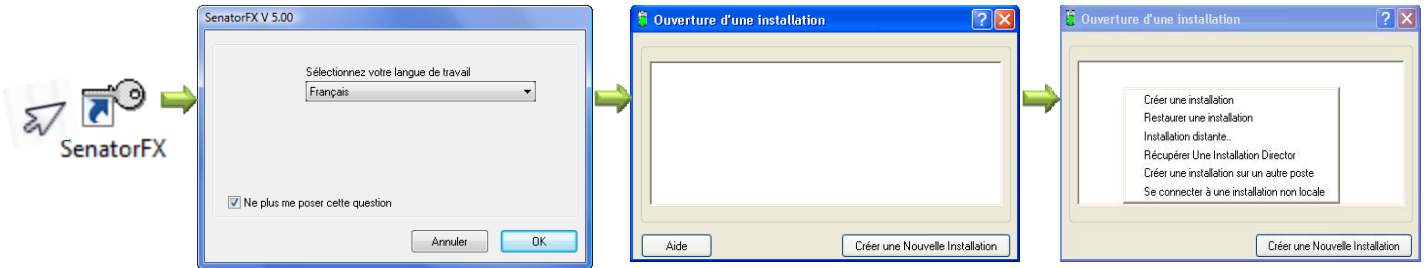
4 possible options:  
**Install** the software  
**Modify** the existing installation.  
**Repair** the existing installation.  
**Remove** the existing installation

Follow the options on your screen



## SETTING UP THE SITE

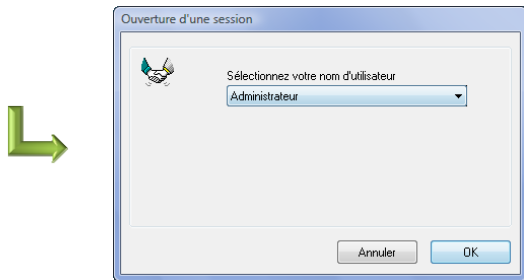
### 1) *Launching the software*



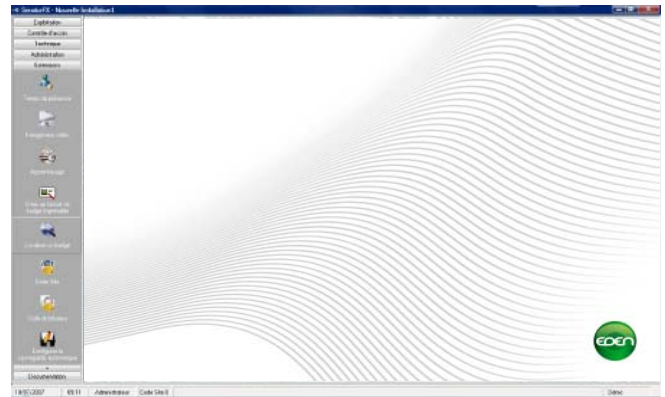
Select the required language then tick the “Do not remind me again” box.

This window appears, click with the right mouse button.

To create a new installation, select “Create an installation” then enter the name of the new installation.



Click on OK.  
We recommend that you subsequently create a password to access the software.

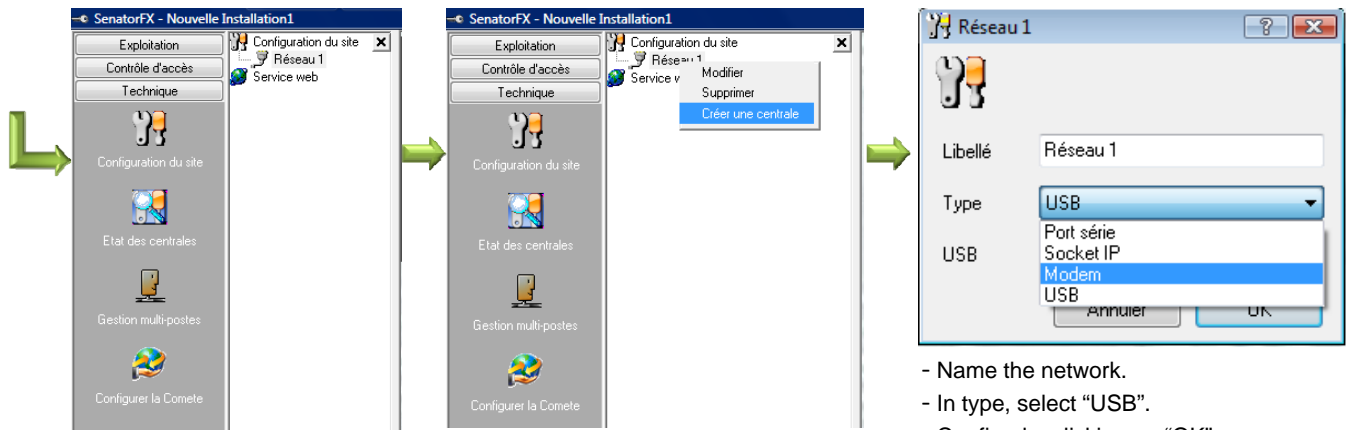


The main page of the SENATORFX software is opened



## 2) Setting up the control unit network

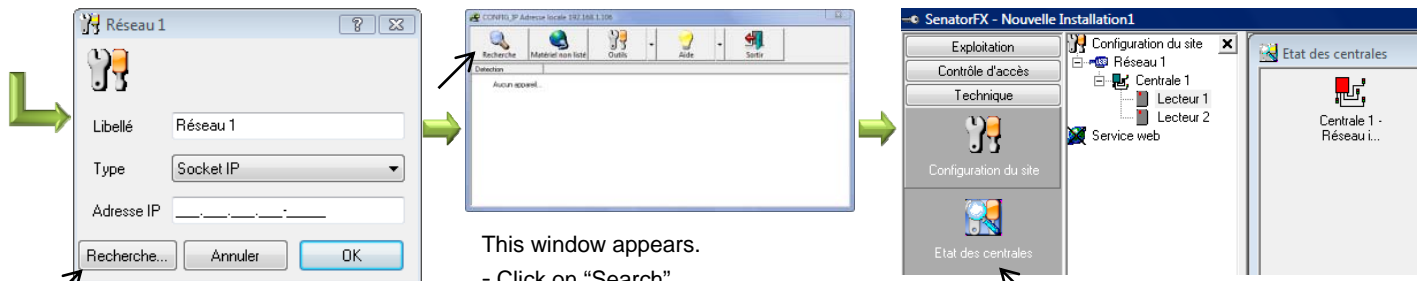
Select the technical tab from the vertical menu.



Click on "network" and select "modify".

- Name the network.
- In type, select "USB".
- Confirm by clicking on "OK".

For other connection templates, see the instructions or press the F1 key.



This window appears.

- Click on "Search".
- Modify the auto-detected IP address.
- Drag the IP address to the previous window.
- Confirm by clicking on "Exit".

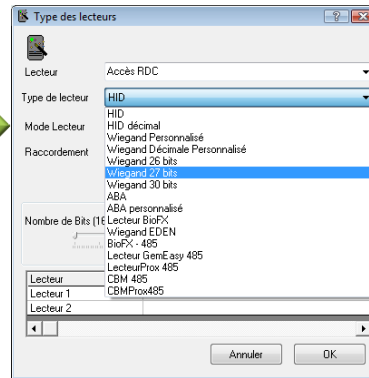
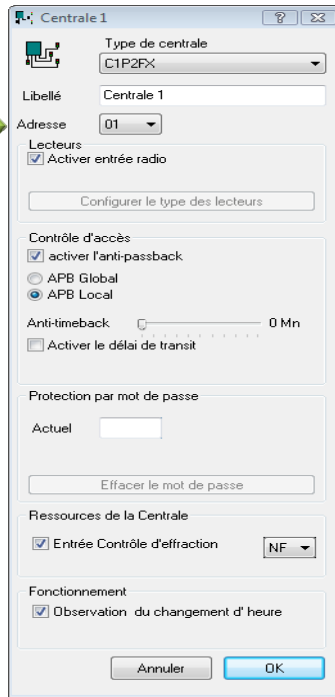
- Click on control unit status.

If the network is connected the control unit icons will change to green otherwise they will be red. See the instructions or press the F1 key.



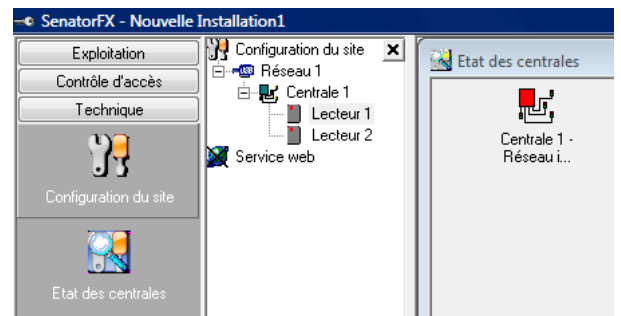
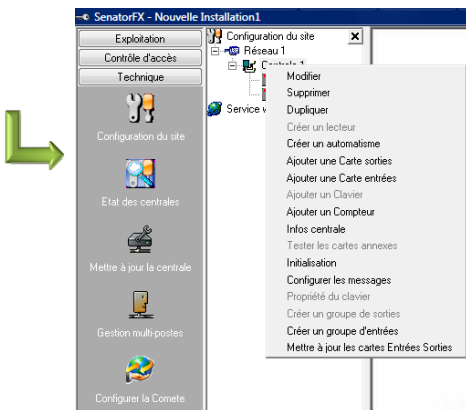
### 3) Setting up the control units

Click on “network” and then on “create control unit”.



- This window appears.
- Select the format depending on the readers/badges(cards) on the site.
- See the instructions or press the F1 key.
- Confirm by clicking on “OK”.

- Select the type of control unit.
- Name the control unit.
- Select the control unit’s address.
- Activate APB or not.
- Activate latency or not.
- Activate break-in control or not.
- Activate “summer/winter” clock change.
- Confirm by clicking on “OK”.



For several control units repeat the process.

There are several possible options:

- Modify the control unit.
- Remove the control unit.
- Duplicate the control unit.

For other parameters see the instructions or press the F1 key.

Then click on the “control unit status” icon.

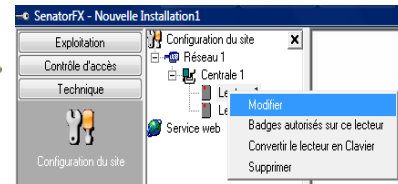
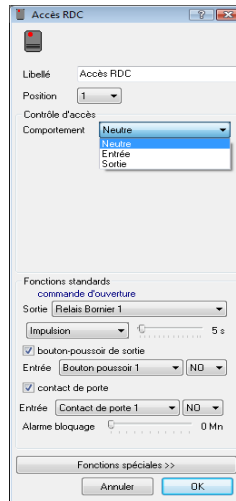
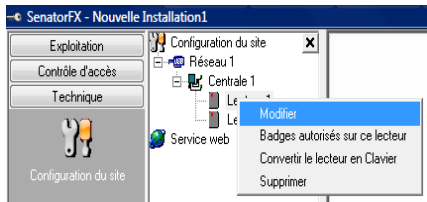
If the control unit network is connected, the icons will change to green, otherwise they will be red.

See the instructions or press the F1 key.



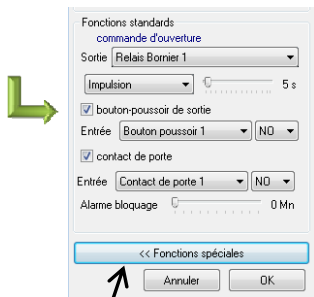
## 4) Setting up the readers

Click on reader and select “modify”.

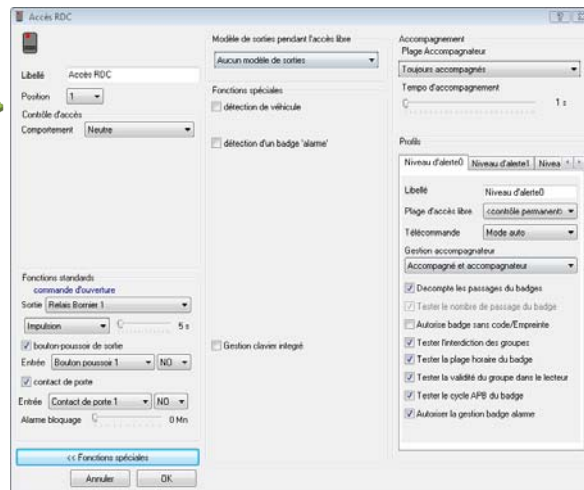


Repeat the process for each of the readers on the site

- Name the reader.
  - Select the reader's mode for APB:
    - Entry, Exit or Neutral.
  - Select the door relay and its mode.
  - Activate the door exit PB or not and its status "NO or NF".
  - Activate the door contact or not and its status "NO or NF".
  - Confirm by clicking on "OK".
- For more detailed setup see the instructions or press the F1 key.



Click on “special functions”, if necessary



Various additional options:

- Activate “vehicle detection” or not and its status “NO or NF”.
- Activate the “badge alarm” function or not.
- Activate “integrated keypad” management or not.
- Activate the “visitor's badge” function or not.
- Parameterise the emergency profiles or not.

For more detailed setup see the instructions or press the F1 key.

## 5) Using biometry

SenatorFX offers the option of making use of biometry on your system by using C1P2FX control units and CBMPROX485 (optical sensors) or BIOFX485 (capacitive sensors) readers.

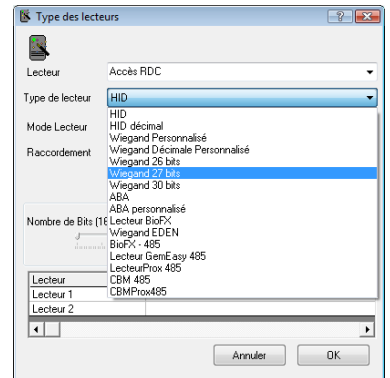
**Note:** the two sensor technologies (optical and capacitive) are not mutually compatible on the same system.

### 1. Setting up the control units

Proceed as described in the chapter entitled “Setting up the control units” to register your C1P2FXs to your system.

### 2. Setting up the readers

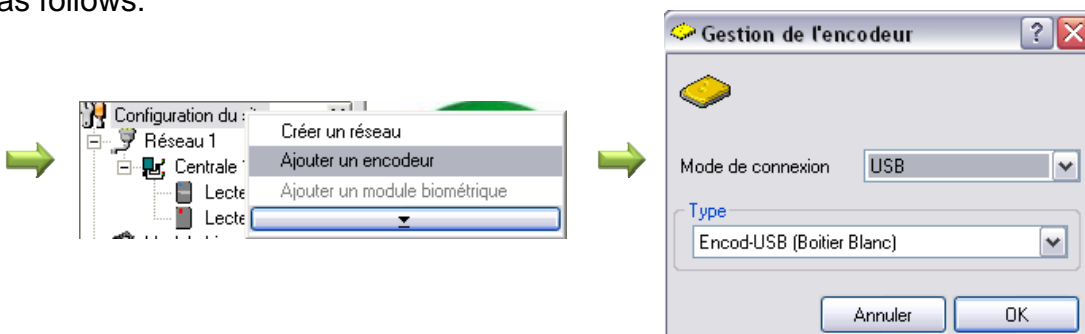
In the “Reader types” window, select the type of reader you are going to install (CBMPROX485 or BIOFX485). Next, enter the reader’s identifier (you will find this on a label attached to the reader itself or to its Technical Information sheet). Then click on OK.



**Note:** if you are only connecting a single biometric reader to the same control unit, and the second control unit reader is not used, leave the type as HID for the second reader or remove it.

### 3. Setting up a USB encoder

In order to encrypt (MIFARE® type) badges that are compatible with the CBMPROX485, you need to have a USB encoder (reference ENCOD-USB, this encoder does not need a driver). To activate it in SenatorFX, click on the “Technical” tab then “Site configuration” and proceed as follows:



You can monitor the status of your encoder at the bottom of the main window of SenatorFX:



## 5) Using biometry (continued)

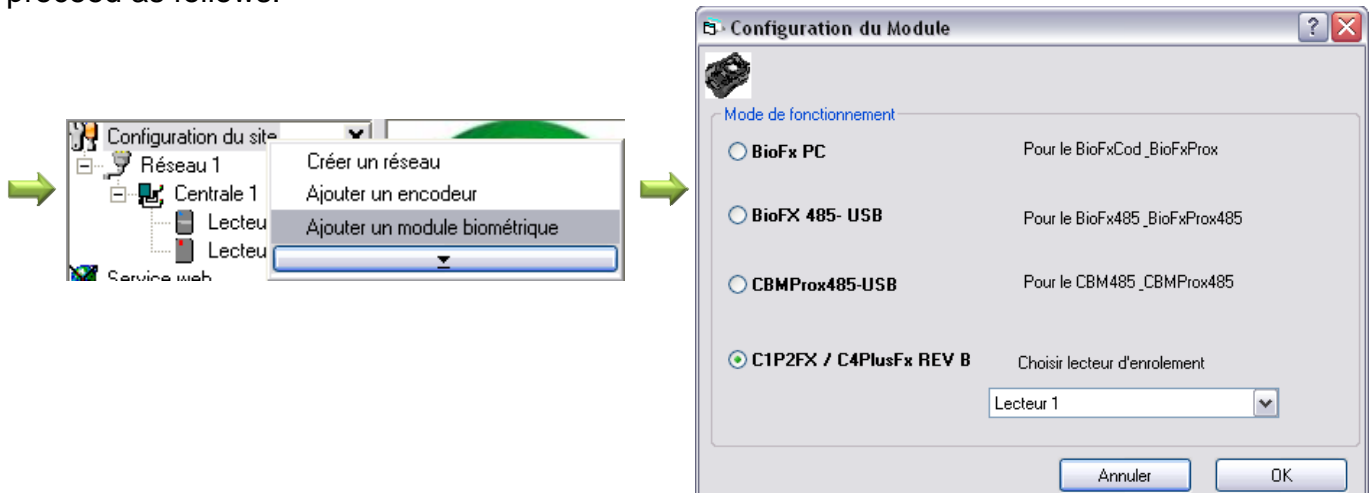
### 4. Setting up a biometric enroller

In order to create badges with fingerprints for your users, you need to have a biometric enroller. Compatibility between biometric enrollers and readers

<i>Readers used</i>	<i>Compatible enroller</i>
CBMPROX485	CBMPROX485-USB
BIOFX485	BIOFX485-USB

Before registering your enroller in SenatorFX, check that the latter is properly installed on your PC and that the drivers have also been properly installed. For more information on this configuration, refer to the relevant technical documentation.

To activate you enroller in SenatorFX, click on the “Technical” tab then “Site configuration” and proceed as follows:



Select the type of enroller depending on your equipment.

## 5) Using biometry (continued)

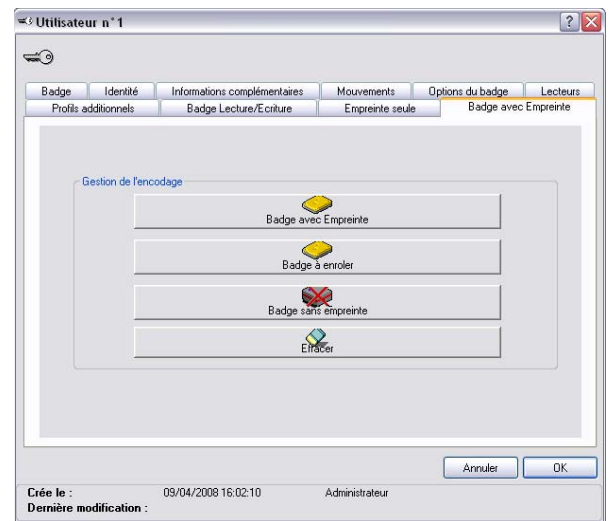
### 5. Encrypting badges

Before encrypting badges, create your access groups and your users. To do this, proceed as explained in the chapters entitled “Setting up access groups with time zones” and “Setting up badges and users”.

Next, open the file for one of the users, then select the “Badge with fingerprint” tab:

You can then:

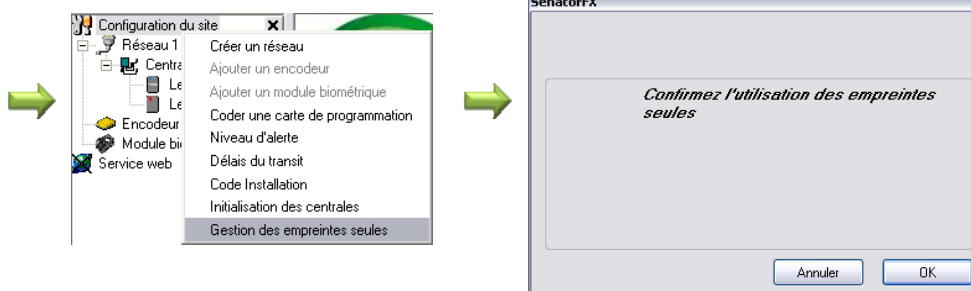
- Encrypt a badge with a fingerprint: SenatorFX will ask you to enrol one or two of the user’s fingers and to then encrypt his or her badge
- Encrypt a badge for enrolling: this button allows you to encrypt a badge to give to your user, who will enrol himself/herself at a CBMPROX485 reader when he uses one for the first time
- Encrypt a badge without a fingerprint: the user of this badge will not have to give a fingerprint reading when passing CBMPROX485 readers. To do this you can select, for each reader, whether it will accept this type of badge or not (Configuring readers, special functions in the “Technical” tab followed by “Site configuration”)
- Delete a badge: delete the entire configuration of a badge in order to re-issue it to another user



### 6. Using fingerprints only

**Important:** before using this function, ensure that you have authorisation to use fingerprints as the only means of identification in accordance with the applicable legislation in the country of installation.

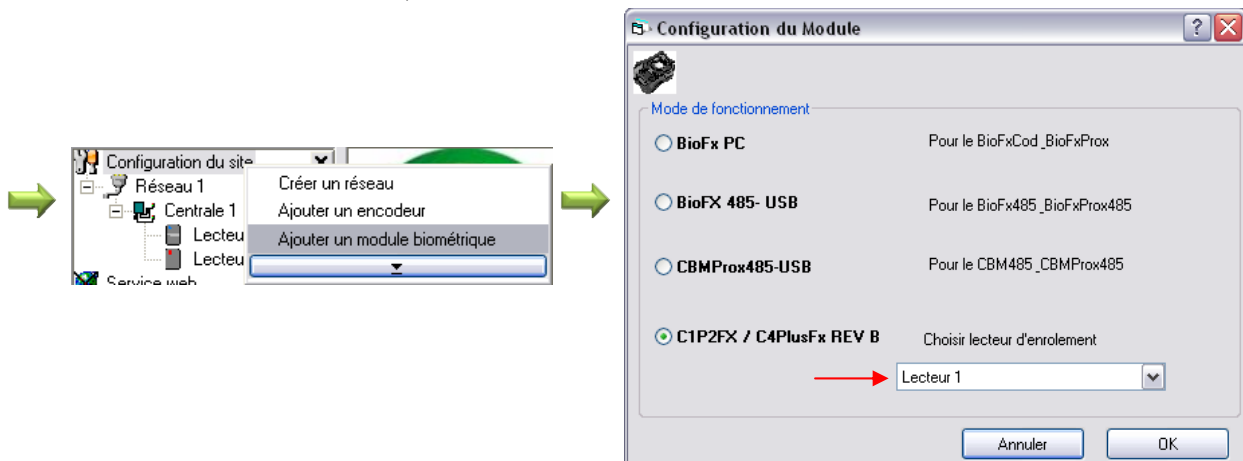
To activate the function, go to the “Technical” tab then “Site configuration” and click on “Management of fingerprints only”:



**Note:** to stop checking fingerprints only, proceed as above and confirm the stop.

### 5) Using biometry (continued)

You will then need a biometric enroller (see previous chapter). If this is not the case, you can use one of your system's readers. To do this, go to the "Add a biometric module" menu then select the reader to be used, as follows:



Before enrolment, create your access groups and your users. To do this, proceed as explained in the chapters entitled "Setting up access groups with time zones" and "Setting up badges and users".

Next, open the file for one of the users, then select the "Fingerprint only" tab: Click on the "Enrol" button to start enrolling a user. If the user is already enrolled, the "Delete" button will be accessible. Click on this button to delete the user's current fingerprint.



## 6) Setting up access groups with time zones

- o A group is made up of one or more of the system's readers. Once a group has been created, it can be assigned to a badge or a set of badges.
- o Click on the "access control" vertical menu.

Then click on the "access group" icon.

Click on access group and "create a group".

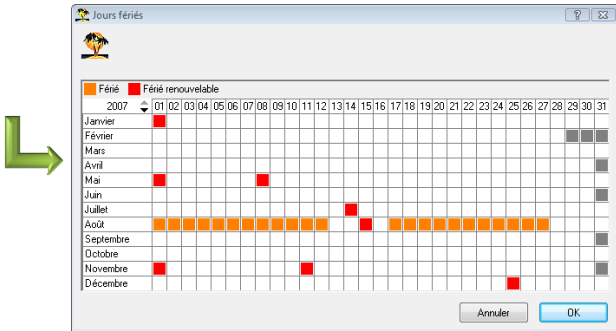
- Name the group.
- Tick the "authorised" readers.
- For each reader, select "permanent access" for a 24/24h authorisation or "Select a time slot" for a temporary authorisation.

- o The time slots can be configured at the same time.

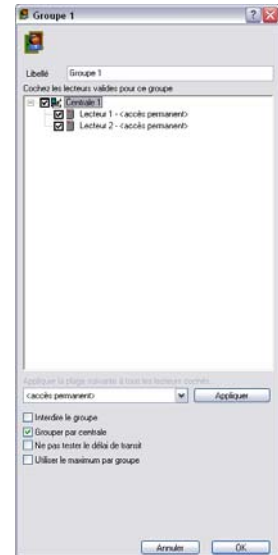
- Rename the time slot
- Select "detailed" for each day of the week, or "week/WE" for the week and week-end separately, or "daily" for every day of the week.
- Click on "authorised" then create the green authorisation time slots.
- 10 time slots are available per day .

## 6) Setting up access groups with time zones (continued)

o Click on “public holidays” in the current window



Confirm by clicking on “OK”.



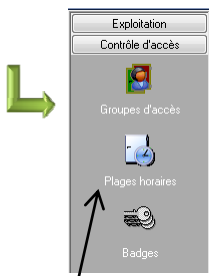
Return to the previous window then confirm by clicking on “OK”.

You can create 32 public holiday periods, which will be stored in the control units.

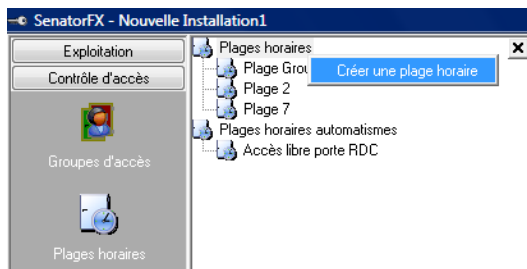
- 1 click for a public holiday.
- 2 clicks for a repeatable public holiday.
- 3 clicks to delete the public holiday.

To create a period, move the cursor over the calendar with your mouse.

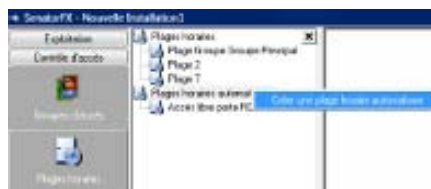
o You can also create time slots using the “time slots” menu.



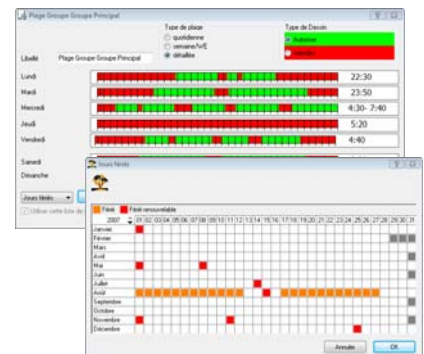
Click on the “Time slots” icon.



Click on “Time slots” then on “create a time slot”.



Click on “automation time slots” in order to create a free access time zone to give free access to an entry point.



For time slots and public holidays, follow the procedure on the previous page.



## 7) Setting up badges and users

Click on the badges icon on the “access control” vertical menu.

Click on the “Badges” icon.

Click on “badges” then on “create a set”.

The badge set you have created appears

- Enter the number of the 1<sup>st</sup> badge.
- Enter the number of badges.
- Select the status of the set: “In service or Suspended”.
- Select the access group.
- Option to see the group.
- If there is a reader + keypad on the site select badge with code.
- Confirm by clicking on “OK”».

Click on a badge then on “modify”.

Modification of the access group, status, access time slot, date/time of the beginning/end of validity, visitor's badge or not and PIN code entry if necessary.

Click on the “identity” tab.

Proceed in the same way for each user.

- Enter the surname and first name.
- Take a photo with the webcam or import one.
- Confirm by clicking on “OK”.

## 8) Setting up the software operators

- o The number of profiles and software operators is unlimited.
- o Select the “administration” tab then click on the “operator profiles” icon.

Creation of “operator” profiles.

Click on “operator profiles” then on “create an operator profile”.

- Enter the name of the profile.
- Tick the access rights.
- Confirm by clicking on “OK”

Repeat the process for each operator profile.

Creation of “operators”.

Click on the new operator then on “modify”.

- Edit the surname and the first name.
- Select an operator profile.
- Edit the password.
- Confirm by clicking on “OK”

Repeat the process for each operator.  
**We strongly recommend assigning a secure password to the basic “Administrator” profile.**

## 9) Setting up the data stream log

- o The data stream log provides “real time” monitoring of events arising during operation.

Click on “list of events”.

When you select a line, the photo of the user in question and his/her identity appears on the right hand side of the screen.

If you click twice on an event line, the file for the user in question appears on the screen.

If you click on “modify badge”, the file for the user in question also appears.

Date	Heure	Badge	Noms	Lecteur	Evènement
03/07/03	15:20:18	000037	FELIX	Lecteur 50	Badge accepté
03/07/03	15:20:14	000037	FELIX	Lecteur 50	Badge accepté
03/07/03	15:20:13	000037			
03/07/03	15:20:13	000037			
03/07/03	15:20:10	000036			
03/07/03	15:19:05	000037			
03/07/03	15:19:02	000036			
03/07/03	15:19:00	000037			
03/07/03	15:18:57	000036			
03/07/03	15:18:56	000036			
03/07/03	15:18:56	000036			
03/07/03	11:53:43	000039			
03/07/03	11:52:38	000036			
03/07/03	11:52:34	000037			
03/07/03	10:30:21	000036			
03/07/03	10:30:19	000037			
03/07/03	10:30:10	000037			
03/07/03	10:30:00	000036			
03/07/03	10:28:27	000036			

- o The log setup can be configured. Select the “access control” tab.

Click on “events setup”.

-Select a type of event from the list on the left hand side of the window.  
 Several possible options:

- A colour for this event.
- A sound template or not.
- Display in the log or not.
- Display in monitoring or not.
- Display with an “information bubble”.
- Acknowledgement and instructions required.
- Automatic purge of the database.

## 10) Managing the system history

Select the “operation” tab then click on the “History” icon.

Click on “analysis tool”.

Save the request template.

Print the request.

Export the request as a .txt file

Copy the request to the clipboard.

Click on the column for “ascending or descending” order.

You can drag and drop the columns between themselves

Click twice on a line in the log and the file for the user in question will appear on the screen.

Click on “badge file” and the file for the user in question will also be displayed.

- Tick the required search criteria:  
 Surname, first name, start/end date and time, control unit, reader, status, specific nature of the badge, event type, accepted or refused, etc.  
 - Then start the search.

Numero de badge	Nom du porteur	Prénom du porteur	Statut	Groupe	Présence	Date Contrôle	Nombre
123456	DUPONT	Fabrice	En service	Groupe Principal	Implémenté	15/07/2007 15:28:59	100
123457	TEARROULE	Carole	En service	Groupe Principal	Implémenté	15/07/2007 15:28:59	100
123458	OSQF	Christophe	En service	Groupe Principal	Implémenté	15/07/2007 15:28:59	100
123459	OSQFOSQF	Christophe	En service	Groupe Principal	Implémenté	15/07/2007 15:28:59	100
123460	OSQFOSQF	Christophe	En service	Groupe Principal	Implémenté	15/07/2007 15:28:59	100
123461	OSQFOSQF	Christophe	En service	Groupe Principal	Implémenté	15/07/2007 15:28:59	100
123462	OSQFOSQF	Christophe	En service	Groupe Principal	Implémenté	15/07/2007 15:28:59	100
123463	OSQFOSQF	Christophe	En service	Groupe Principal	Implémenté	15/07/2007 15:28:59	100
123464	OSQFOSQF	Christophe	En service	Groupe Principal	Implémenté	15/07/2007 15:28:59	100
123465	OSQFOSQF	Christophe	En service	Groupe Principal	Implémenté	15/07/2007 15:28:59	100
123466	OSQFOSQF	Christophe	En service	Groupe Principal	Implémenté	15/07/2007 15:28:59	100
123467	OSQFOSQF	Christophe	En service	Groupe Principal	Implémenté	15/07/2007 15:28:59	100
123468	OSQFOSQF	Christophe	En service	Groupe Principal	Implémenté	15/07/2007 15:28:59	100
123469	OSQFOSQF	Christophe	En service	Groupe Principal	Implémenté	15/07/2007 15:28:59	100
123470	OSQFOSQF	Christophe	En service	Groupe Principal	Implémenté	15/07/2007 15:28:59	100



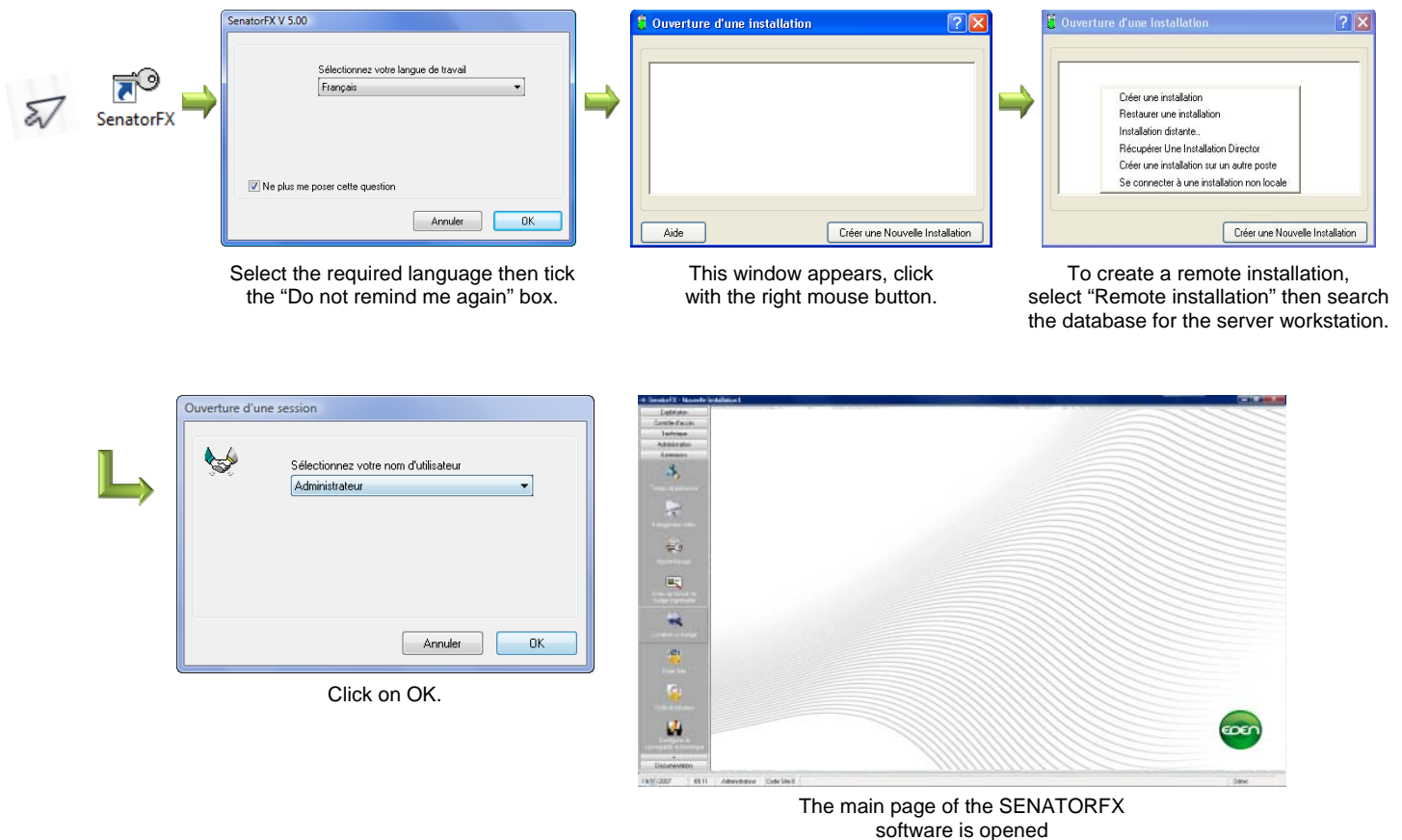
## MULTI-WORKSTATION SYSTEM

SenatorFX enables several PCs (up to 5 client workstations) on the same network to manage the same system (**no need for an additional dongle**).

Before installing client workstations, it is essential that the directory containing the installation details for your site (usually, *c:\program files\eden\Senatorfx\Installations\NomDeVotreInstallation\*) is shared in both **Read** and **Write** mode on the server workstation, in order for the client workstations to be able to access the database. To do this, you need to have sufficient administrator rights to perform this operation. Ask the network administrator on your site about this.

Install SenatorFX on all the client workstations as explained in the chapter entitled “Software installation”.

When you start the client workstation for the first time, proceed as follows:



**Note:** if you are unable to get to the session opening window, check that the installation directory on the server workstation is shared in **write** mode. If it is not, SenatorFX will not be able to open your installation.



NOTES

Dotted lines for notes.



