FERMAX

FINGERPRINT READER SOFTWARE
Singular Key

INSTALLATION MANUAL

en.

SINGULAR KEY SOFTWARE

Code 97668I V07_19

INDEX

Introduction

The Fingerprint Reader is a biometric entrance control system that recognises fingerprints.

Add a Proximity Reader as an alternative and/or complementary method for access via proximity cards. The proximity reader may be configured in different modes.

Operating Modes

- Identification only by fingerprint:
  - The option of operating with 1 or 2 fingerprints per user.
- Identification only by Card:
  - It is estimated that 1% of the population lacks the necessary information for biometric recognition. In these cases a proximity card may be used as an alternative method.
- Security Mode with Fingerprint + Card.
- Security Mode with Fingerprint + Code:
  - This requires a keypad module connected to the reader.
- Identification only by Code:
  - This requires a keypad module connected to the reader.

Installation of a Fingerprint Reader. Configuration of the autonomous or centralised mode.

The reader´s configuration in autonomous or centralised mode is done via a dipswitch that is located in the back of the reader. Autonomous mode is configured by turning the reader´s dipswitch 8 to ON and centralised mode is configured by turning the dipswitch 8 to OFF.

There are 2 operating modes on the reader, which allow two methods for managing users with the software:

- **AUTONOMOUS**.
  The reader acts as a controller, granting and denying access based on whether the user has been set up on the system. The reader's users are managed manually, (or alternatively via the software).
- **CENTRALISED.**
  The reader delegates the lock-release to the centralised controller ref. 4420.

  In both operating modes, autonomous and centralised, the installation´s users **are synchronised** with the aim of ensuring that each user has the same identifying number on each of the readers.

Within each project, we can simultaneously manage different types of readers, the application will assume responsibility for managing the users correctly in each case.

"Singular Key SW" management software.

The software for managing the Fingerprint Reader with a proximity reader allows you to organise and administrate the data these devices generate, without having to register each one of the readers on the installation.

The available actions in the program depend on the type of installation to manage, determined by project level (fingerprint or fingerprint+proximity/code), and the mode in which the reader is configured (Autonomous - Centralised).

Ports and Connections.

For connections with readers you can use:

- USB Converter to RS485 Ref. 24661
- RS232-485 Adaptor Ref. 2466
- IP Management Model Ref. 1087

Note: see the corresponding installation manual. AUTONOMOUS Fingerprint installation manual, cod. 97666 or CENTRALISED Fingerprint installation manual, cod. 97667.

Features of the AUTONOMOUS fingerprint reader

The Fingerprint Reader is an autonomous reader with an integrated controller.

This is a biometric recognition system based on the users' fingerprints, which allows a greater level of security than that offered by other systems which use different types of identifiers. Integrate a "proximity reader."

Some people's fingerprints do not have the information required to register them in a biometric system. An estimated 1% of the population. In these cases we use the built-in Proximity reader.

Specifications:
Fingerprint reader with a thermal sensor and capacity to store up to 4500 fingerprints.

- Number of users:
  * 4500 in 1 fingerprint per person mode.
  * 2970 in 2 fingerprints per person mode.

  The use of one of these fingerprints (if registered on the system) will result in the activation of a relay which activates the lock-release or another device. To do this, just steadily run your finger along the reader sensor.
- Reader with 2 status leds and a 4 digit, 7 segment display.
- Infrared Keypad for Programming. The system is programmed with the Master fingerprint/card and a remote infrared keypad.
- Lock-Release Activation Relay
- Auxiliary Relay for other Functions.
- Auxiliary Input for Exit Button.
- Input for Open Door Sensor.

Features of the CENTRALISED Fingerprint Reader

The Fingerprint reader is designed as a universal reader with a wiegand-26 or data-clock output, for "Centralised Access Control." Requires a door controller for its connection to the central unit

This is a biometric recognition system based on the users' fingerprints, which allows a greater level of security than that offered by other systems which use different types of identifiers. Integrate a "proximity reader."

Some people's fingerprints do not have the information required to register them in a biometric system. An estimated 1% of the population.

Similar to the Autonomous reader with the exception that the lock-release and relay activation mechanisms are maintained by the door controller. The user must register users both on the (fingerprint) reader and on the central guard unit (identifier number).

Characteristics:
Fingerprint reader with a capacitive sensor and capacity to store 1 or 2 fingerprints per user:

- Number of users:
  - o Central units with capacity for up to:
  - **1020 users** with the UC MDS (ref. 2405). 2405).
  - **2046 users** with the UC AC Plus (ref. 4410).

  Note: *the fingerprints are registered in the reader and then sent to the exchange.*

  The use of one of these fingerprints (if registered on the system) will result in the activation of a relay which activates the lock-release or another device. To do this, just steadily run your finger along the reader sensor.
- Reader with 2 status leds and a 4 digit, 7 segment display.
- Via the Door Controller:
  * Lock-Release Activation Relay
  * Auxiliary Relay for other Functions.
  * Auxiliary Input for Exit Button.
  * Input for Open Door Sensor.

Important note:

the reader will not work if the master finger/card is not entered.

See the corresponding installation manual. AUTONOMOUS Fingerprint installation manual, cod. 97666 or CENTRALISED Fingerprint installation manual, cod. 97667.

Rapid Configuration Guide

Below are details of the steps to follow to configure the fingerprint reader systems (projects) and their respective users:

1) Create a New Project.

A project is a collection of files, configurations and databases which represent each of the systems in place. Within the application we can define which projects we need, group them into categories, and open and close them as needed. For each system we will create a project.

Each of these projects is independent in terms of the users it has defined and the type of readers it manages.

1.1.- **Establish as "Main Project"**(various projects may exist).

2) Create Sections.

A section is each of the buses connected via ref. 2466, ref. 24661 and/or ref. 1087 to some of the ports RS-232, USB or IP to the PC. You can assign a different name to each of the sections for it to be more descriptive (perimeter section, administrative zone, general access area...).

In order to define a new section, use the context button in the "Readers network" or with the direct button: "Add section."

3) Add the connectors to use to communicate with the readers.

- **Serial Ports:** connectors via a real serial port (or virtual, USB, Tibbo, etc).

Once we have defined the section, we must assign one of the system´s available serial ports to make the communication. This is done by dragging the serial port used (COM1,COM2…) over the corresponding section node.

Important notes:

for the **Tibbo (ref. 1087)** *to operate correctly with the fingerprint reader systems, the following parameters should be configured as detailed below:*

- **Speed (Baud Rate)**: 115200.
- **Parity:** without parity.

4) Fingerprint Reader Detection.

During the start-up of the installation each of the connected readers in each section must be registered . The fastest way to do this is by detecting them.

To ensure that the readers network operates correctly the readers should:

- Have an "Identifier" assigned. See *AUTONOMOUS Fingerprint installation manual, cod. 97666 or CENTRALISED Fingerprint installation manual, cod. 97667.*
- Don't have repeated identifier numbers.
- The version shown on the module's rear screen print should be V2.x or above.

Every time you delete or add a reader to the installation you must repeat this operation.

Once the fingerprint reader is detected, relative to the class of reader (Autonomous or Centralised, via the reader´s dipswitch 8), the available actions and properties are different. It is important that you identify the type of AUTONOMOUS or CENTRALISED reader to correctly register the users (fingerprints) on the readers. There are some exclusive AUTONOMOUS reader fingerprints.

Important notes:

- The reader will not work if the master finger/card is not entered.

- If the users were added to the reader directly (manual) with the control, you must perform a ***synchronisation****, in order to avoid losing users. This way the users are included in the project. This can be detected by looking at the colour (red) of the system´s reader´s. Whenever this situation occurs, we must use the Synchronisation iconlocated in the tool menu, (independently of autonomous or centralised readers).*

5) Select the auxiliary reader for registrations

Once the readers are detected in the installation as explained in the corresponding section, we must select the reader and use it to register the new users, *(Tools> Options> Fingerprint Reader).*

6) Create Users.

Each fingerprint reader can store the following number of users depending on the mode selected.
Each AUTONOMOUS fingerprint reader can store the following number of users depending on the mode selected.

- Number of users:
  - **4500 users** in 1 fingerprint per person mode.
  - **2970 users** in 2 fingerprints per person mode.

Each CENTRALISED fingerprint reader has the capacity to store 1 or 2 fingerprints per user:

- Number of users.
  - o Central units with capacity for up to:
  - **1020 users** with the UC MDS (ref. 2405).
  - **2046 users** with the UC AC Plus (ref. 4410).

6.1.- **Selecting Fingerprints**.

Within *Tools > Options* there are settings where we can configure the number of fingerprints to save for each user. When we are using mixed reader configuration; where 1 fingerprint and 2 fingerprint readers are used in conjunction, we must select the 2nd here, although only the appropriate fingerprints will be sent to each reader.

6.2.- **Copy Users on the Reader:**

In both operating modes, autonomous and centralised, the installation´s users **are synchronised** with the aim of ensuring that each user has the same identifying number on each of the readers.

6.2.1. *With an AUTONOMOUS Reader.*

Once we have the users defined for our project, we can select those we need and drag them to the reader where we want them copied, this way they are **associated** (linked) to the reader. Then they must be **synchronised**.

The **Synchronise** option is to ensure that the same information is copied on each of the readers within the system and for those users to remain in the reader.

Select the **Synchronise** option and apply.

6.2.2. *If it is a CENTRALISED Reader.*

Once we have the users defined for our project, we can select those we need and drag them to the reader where we want them copied, this way they are **associated** (linked) to the reader. Then they must be **synchronised**.

The **Synchronise** option is to ensure that the same information is copied on each of the readers within the system and for those users to remain in the reader.

Select the **Synchronise** option and apply.

6.2.2.1 *Export Users.*

Once the users are set up on the CENTRALISED Readers, they should be updated on the centralised software application being used (Wincom +, AC Plus Access).

To this end, there is an option to export these users from the project into an excel table (XLS) if you are using the Wincom application and then import the table from the centralised software application. If a AC Plus, it allows you to send the users directly to the software, as long as the program is open on the PC.

Important notes:

- Fingerprint Selection for Readers:

- **Normal User**: *user fingerprint for AUTONOMOUS - CENTRALISED readers.*
- **Master 1 / Master 2 / Free access / Unlock:** *types of special fingerprints for AUTONOMOUS readers.*

*- System users must ASSOCIATE=LINK the reader/s and then SYNCHRONISE = INCLUDE into the readers. Since the **associate** process is almost instantaneous and the **synchronisation** takes more time, we recommend associating the users to the readers and then perform their synchronisation.*

*- Users with **Proximity Card**or **Keypad code.***

- o *If we have the incidents activated, we can pass the card over the reader in order for this field to fill-in automatically with the card´s code.*
- o *For the keypad´s code, keep in mind the configured length for each reader (4 or 6). This requires a keypad module connected to the reader.*

7) OPTIONAL: If groups have been created.

Using groups is a dynamic way of assigning which readers a user will have access to.

A group is a collection of readers. There is no limitation for this, so you can define groups with repeated readers, with the list of readers for a specific user as the sum of all the different readers.

In order to add a group, just drag it over the desired group node.

Minimum PC requirements for Singular key SW software

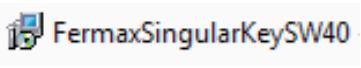
In order to launch the application the following requirements must be fulfilled:

	Minimum Requirements	Recommended
Operating System	Microsoft Windows XP Professional SP3 (32-bit) Vista SP1 Windows 7 Professional (32 or 64-bit)	Microsoft Windows XP Professional SP3 (32-bit) Vista SP1 Windows 7 Professional (32 or 64-bit)
Processor	800Mhz Intel Pentium III or equivalent	2.6Ghz Intel Pentium IV or equivalent
RAM Memory	1GB	2GB
Disk space	750 Mb of free space	1Gb of free space

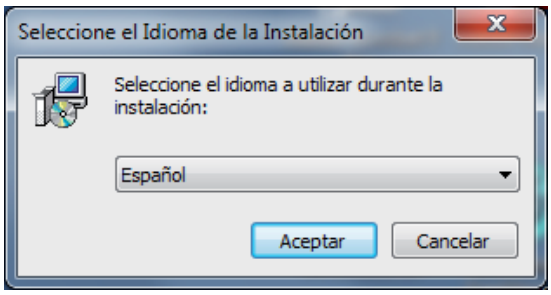
Note: Singular Key 4.0 version is required to install on windows 10 64 bits.

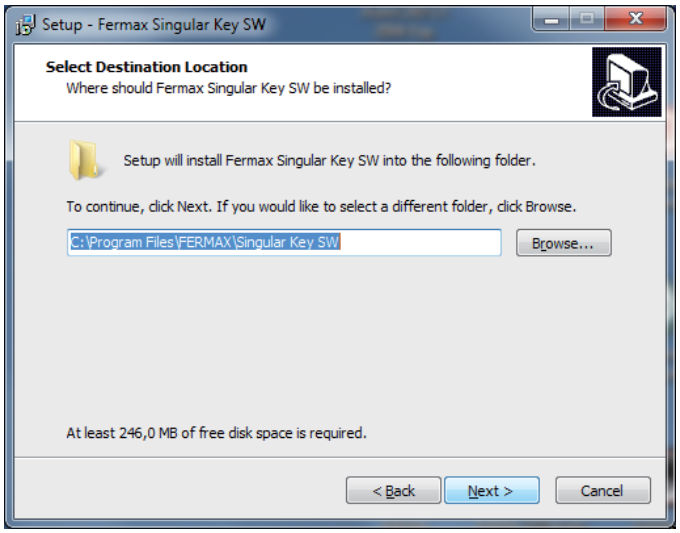
Installation of the "Singular Key SW" fingerprint reader software

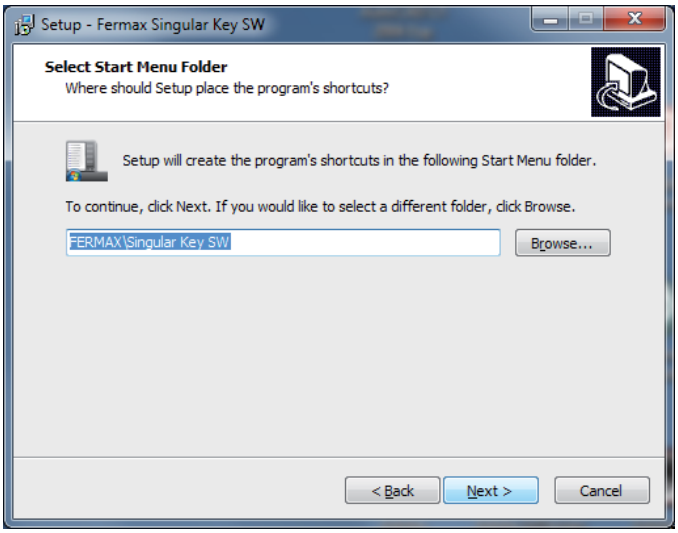
Install the Fingerprint reader software "Singular Key SW". It can be downloaded at www.fermax.com.

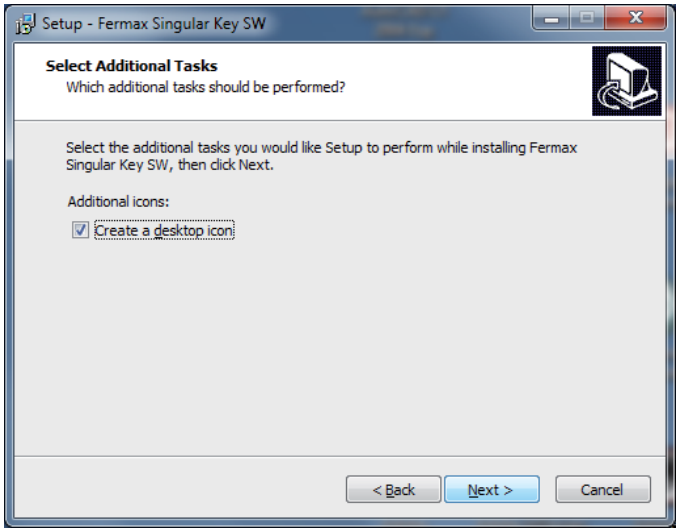


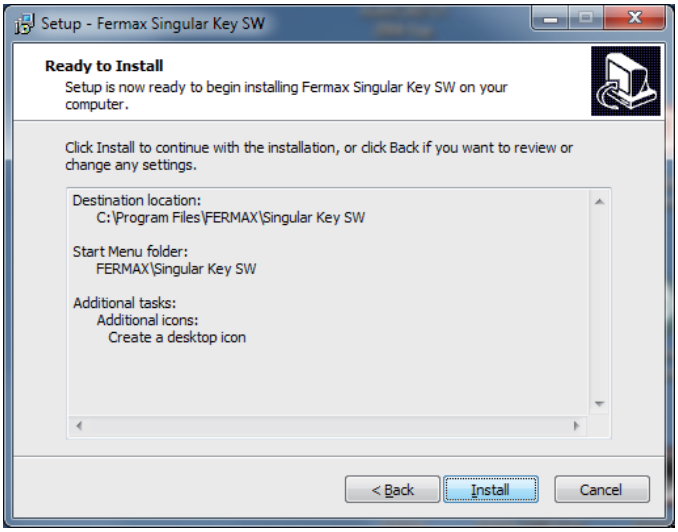
Select Language The language selected on the installer will be the software´s initial language. You can select the installation´s file location, otherwise the default location is C:/Program files/FERMAX

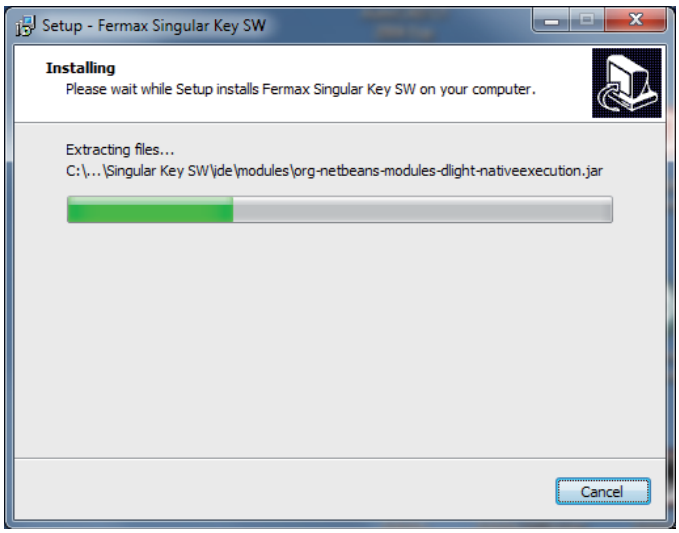


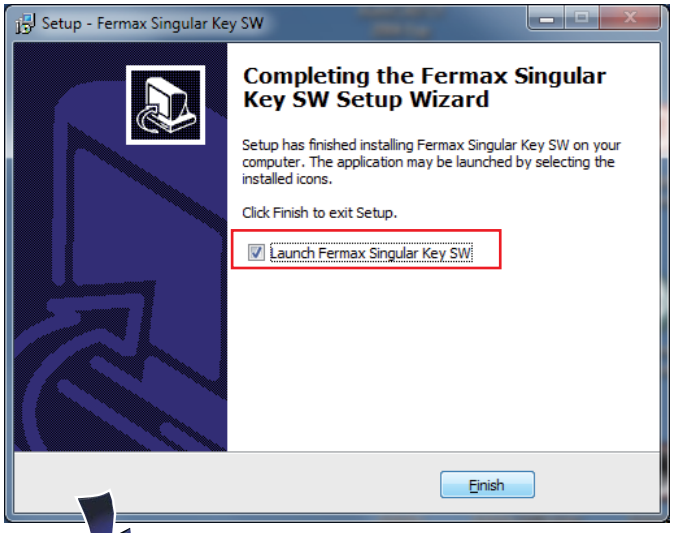




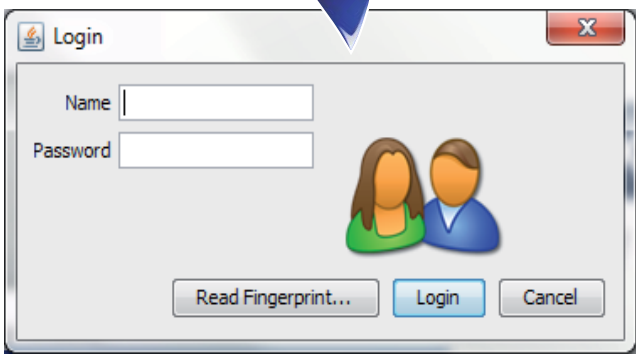


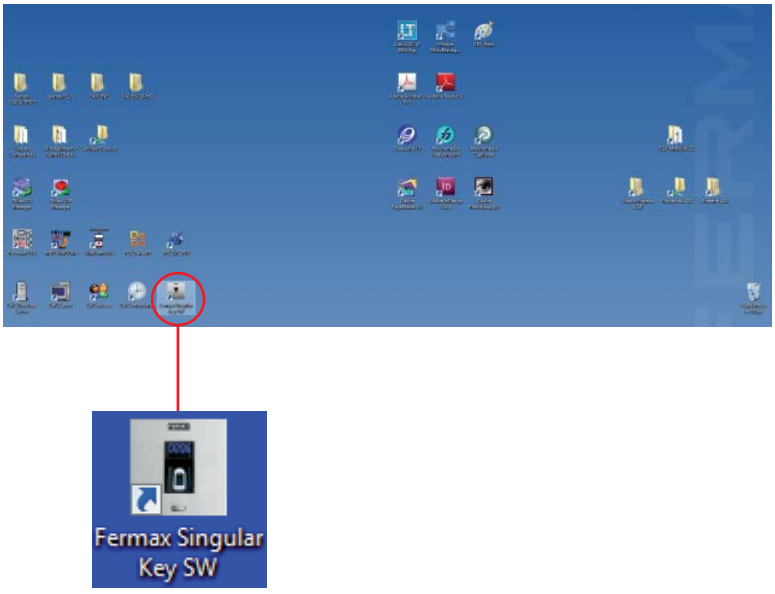



Setup - Fermax Singular Key SW
Installing
Please wait while Setup installs Fermax Singular Key SW on your computer.
Extracting files...
C:\...\Singular Key SW\jde\modules\org-netbeans-modules-dlight-nativeexecution.jar
Cancel


Setup - Fermax Singular Key SW
Completing the Fermax Singular Key SW Setup Wizard
Setup has finished installing Fermax Singular Key SW on your computer. The application may be launched by selecting the installed icons.
Click Finish to exit Setup.
Launch Fermax Singular Key SW
Finish

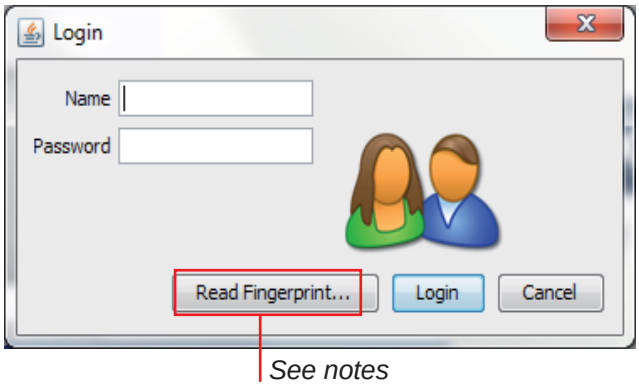

FERMAX
Singular Key SW
Turning on modules...


Login
Name
Password
Read Fingerprint...
Login
Cancel


Fermax Singular Key SW

START - Login and Password Request Screen

Run the Singular Key SW software:



See notes

To access the Singular Key SW application you must enter a name (login) and an access password, which are set to default as:

Name: **system**
Password: **fermax**

Notes:

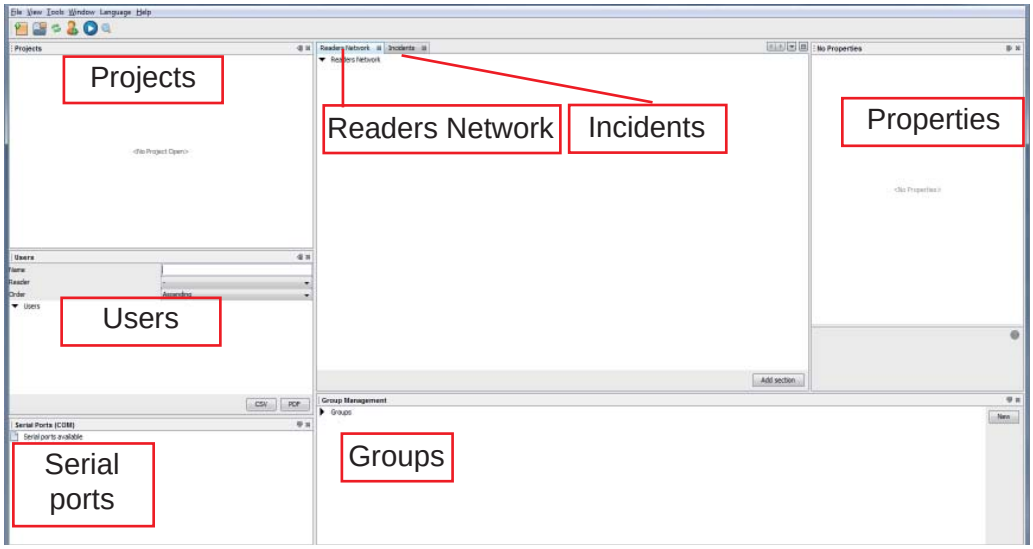
- *The first time accessing must be with a Login and Password. Then the Login and Password give way to the fingerprint saved by the reader configured during registration.*
- *This fingerprint may coincide with another identical fingerprint stored by another reader in the system, since the identification is done in the PC.*
- *If the login is entered incorrectly or the fingerprint is not recognised, the screen reappears for you to re-enter the information or fingerprint.*

MAIN SCREEN of the Singular Key SW application

Once the access password has been entered, the application starts up and opens the main screen.

The application comes programmed with the following structure, which is flexible and can be adapted according to the user's preferences. The application is divided into the following areas:

- **Projects**: allows you to check the open projects, change the main project, rename, delete and close a project.
- **Readers' network** this allows us a schematic vision of the physical installation.
- **Properties:** relative to the selected element, this shows us each of their properties.
- **Users**: list of users in the project, which allows you to filter per reader in which the user is included.
- **Incidents**: it contains both the actions performed by the software users and the incidents received from the readers.
- **Communication ports**: list of serial ports via which communication is made with the readers.
- **Groups**: this allows you to define lists of readers to facilitate assigning and managing users in different readers within the system.



PROJECTS

Description

A project is a collection of files, configurations and databases which represent each of the systems in place. Within the application we can define as many projects as we need, opening and closing them as needed.

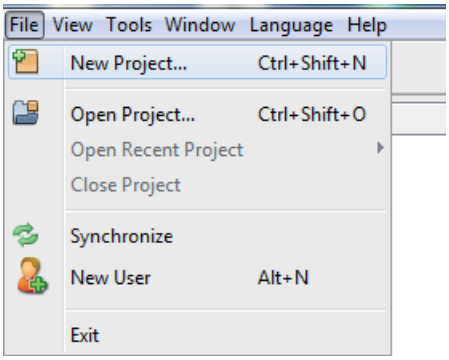
Each of these projects is independent in terms of the users it has defined and the type of readers it manages.

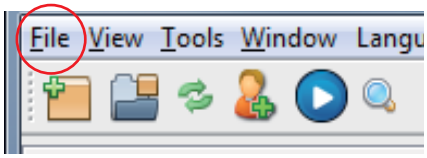
This area lists the open fingerprint projects. You can change the active project (only once) via the context "load project data," rename project, delete disk or simply close it (without removing the project from our file system).

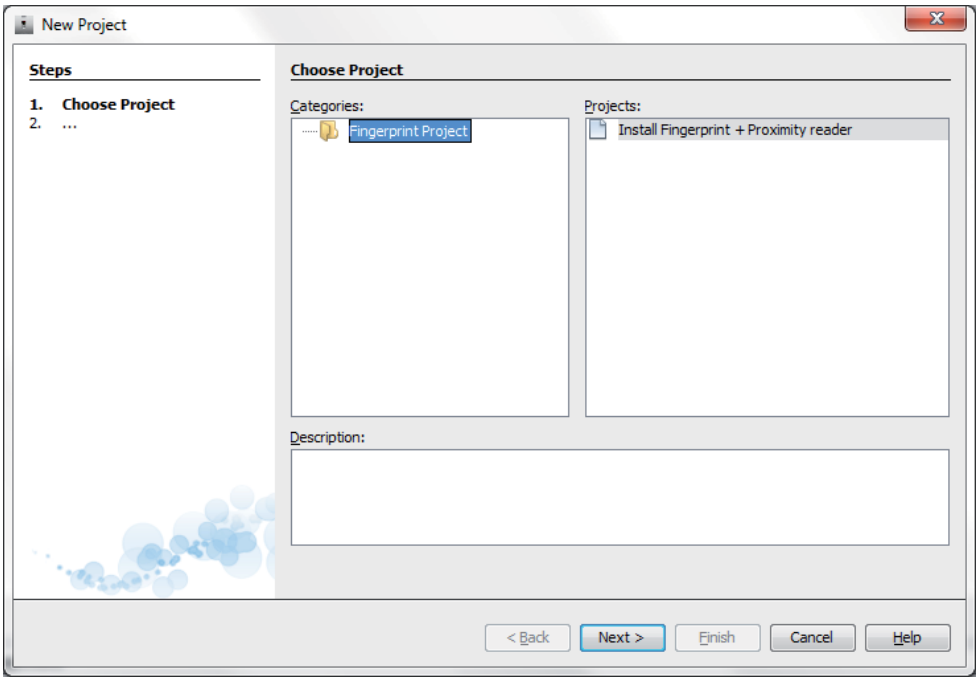
Project types:
The software Singular Key SW, allows us to manage only the fingerprint users, and the fingerprint and proximity/code.

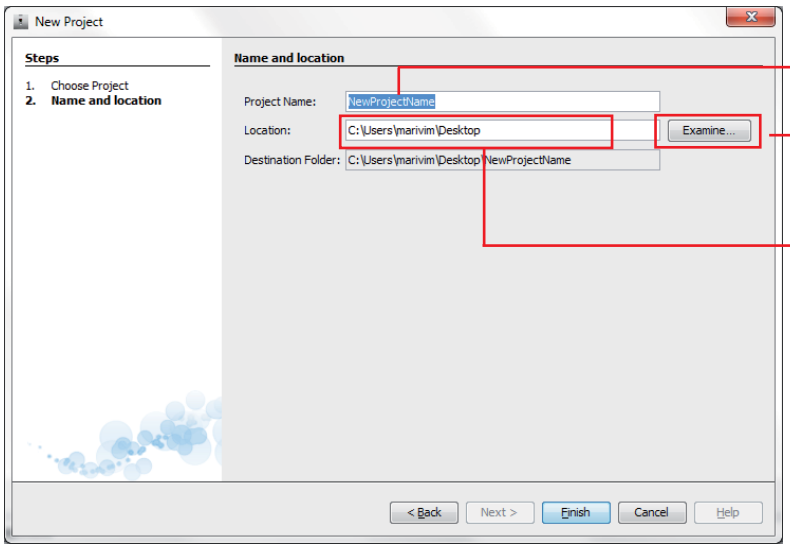
Create a New Project

Via this context menu you can also create a new project, open a recent one, or create project groups if necessary.
You can create a new project using:
- File / New project (tool bar).
- The corresponding rapid access buttons.





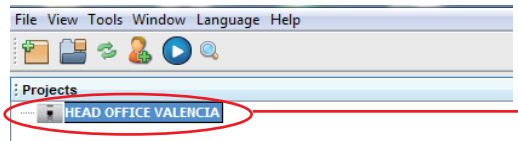




Project Name: *for example, HEAD OFFICE VALENCIA*

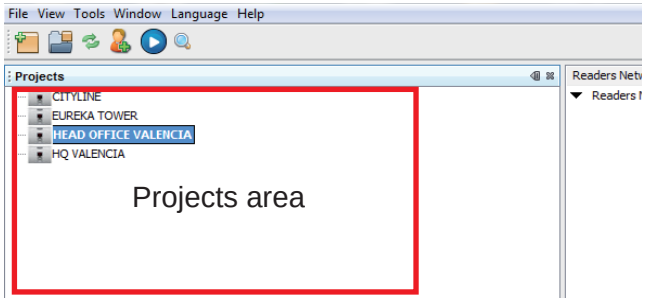
Selecting "Browse," we can choose the location where we want to save the "New Project."

If not the default location is that indicated.



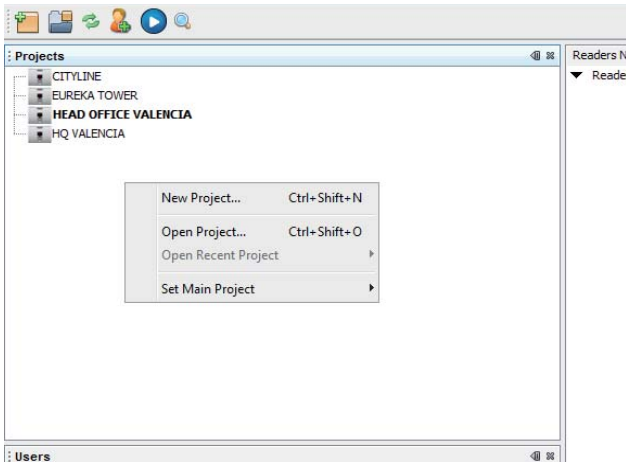
Managing Various Projects

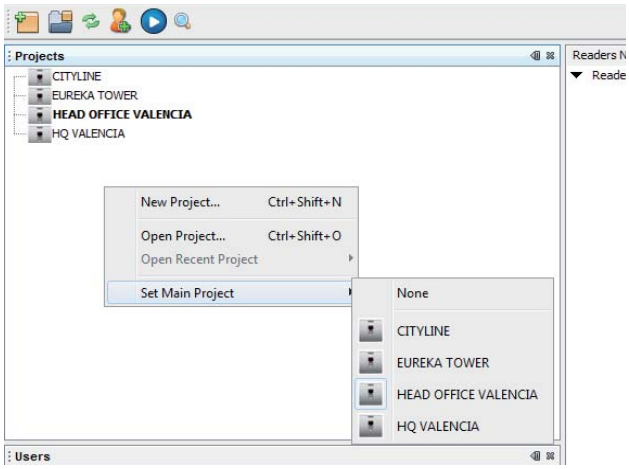
More than 1 project can be managed. To do this it is important to establish which is the "Main Project".



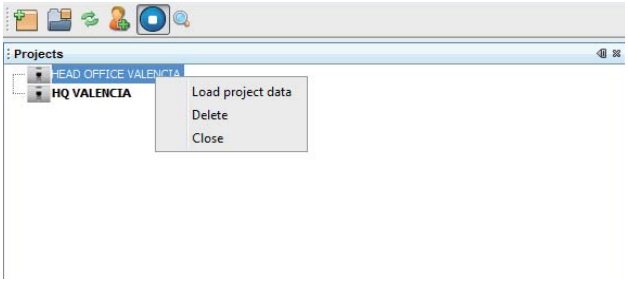
There are two ways to establish a project as a "Main Project."

a) Right-click on the mouse within the "Projects" area and a new window is opened, here select "Establish as Main Project" and choose the project. This menu option gives us the chance of changing the active project to another one loaded on the screen at that time.

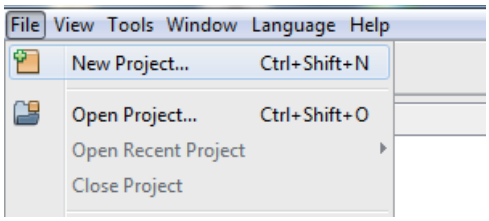




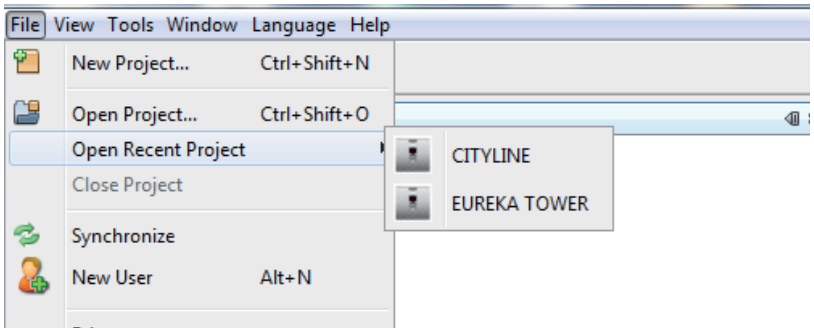
b) Select the project you want to establish as the Main Project and right-click on the mouse; a window opens, and from here select "Load project data." This menu option deactivates the active project and activates the selected one and loads its data.



Other options for projects



- **Open Project**: from this option you open a previously saved project.
- **Close Project**: this option closes the project that is currently open in the application.
- **Open Recent Project**: this option shows a list of projects that have previously been open in the software. By selecting one from the list it automatically opens. While the project is loading a screen appears indicating the project is loading.



COMMUNICATION PORTS

Description

In the Serial Ports (COM) area there is a list of serial ports that communicate with the readers (detected by the application).

- **Serial Ports:** connectors via a real or virtual serial port (USB, Tibbo, etc).

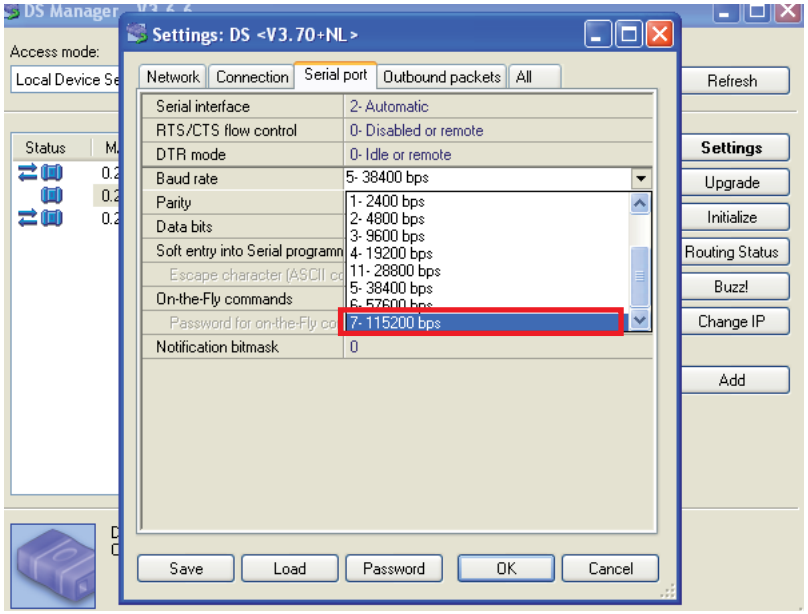
Prior considerations for serial ports

Important note
*for the**Tibbo** to work right with fingerprint readers systems, when installed, the following parameters must be installed:*

- **Speed (Baud Rate)**: 115200.
- **Parity:** without parity.

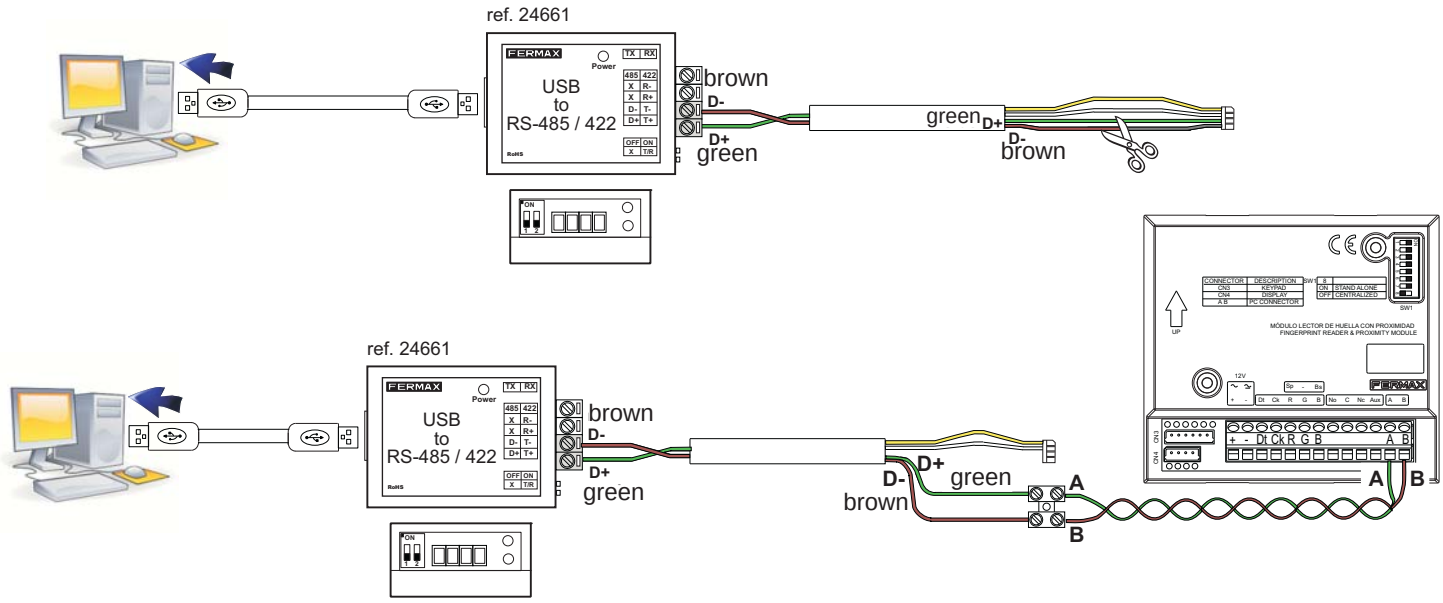
See the Tibbo Manual cod. 94571. **** See Details.***

**** Details: TIBBO: DS Manager-> Settings / Serial Port***

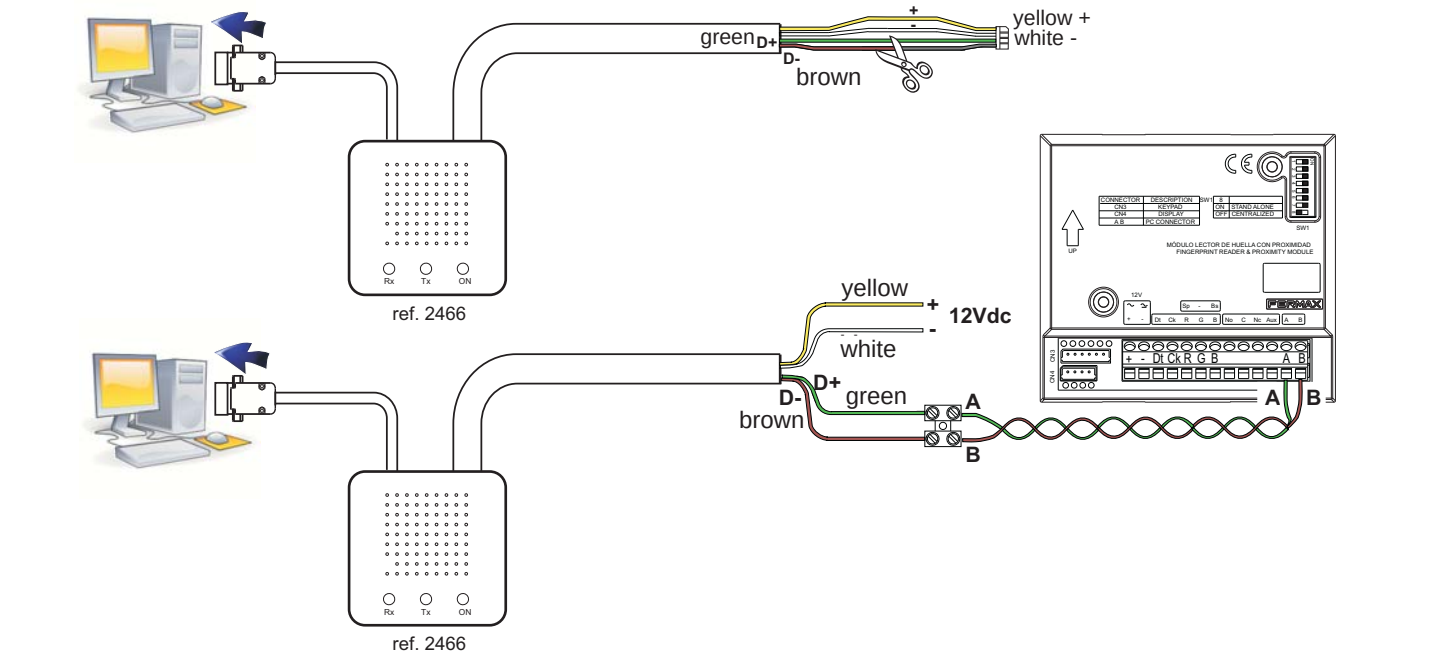


PC connection ports (PC interface)

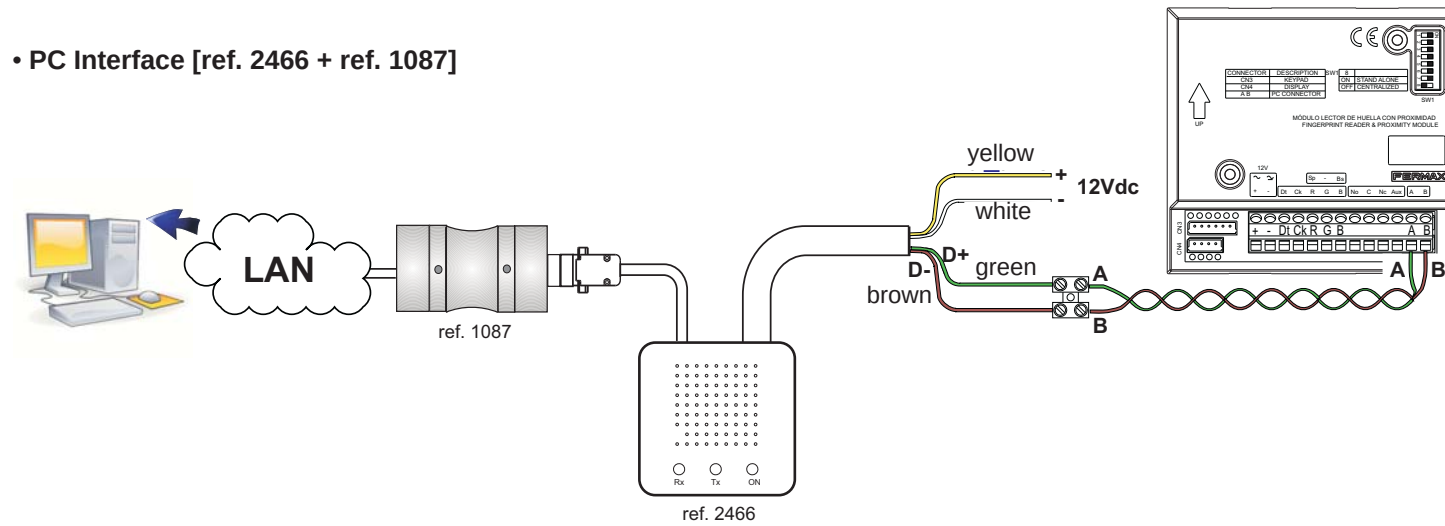
• PC Interface ref. 24661



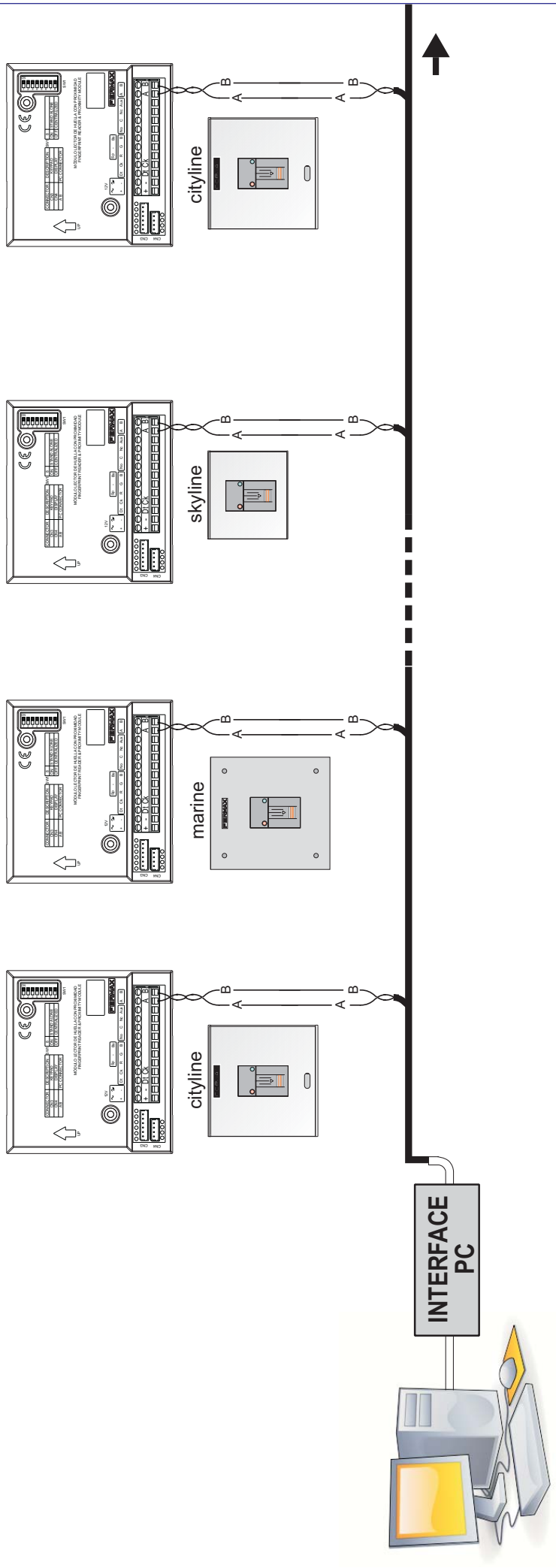
• PC Interface ref. 2466



• PC Interface [ref. 2466 + ref. 1087]



- **General installation**



READERS´ NETWORK

Description

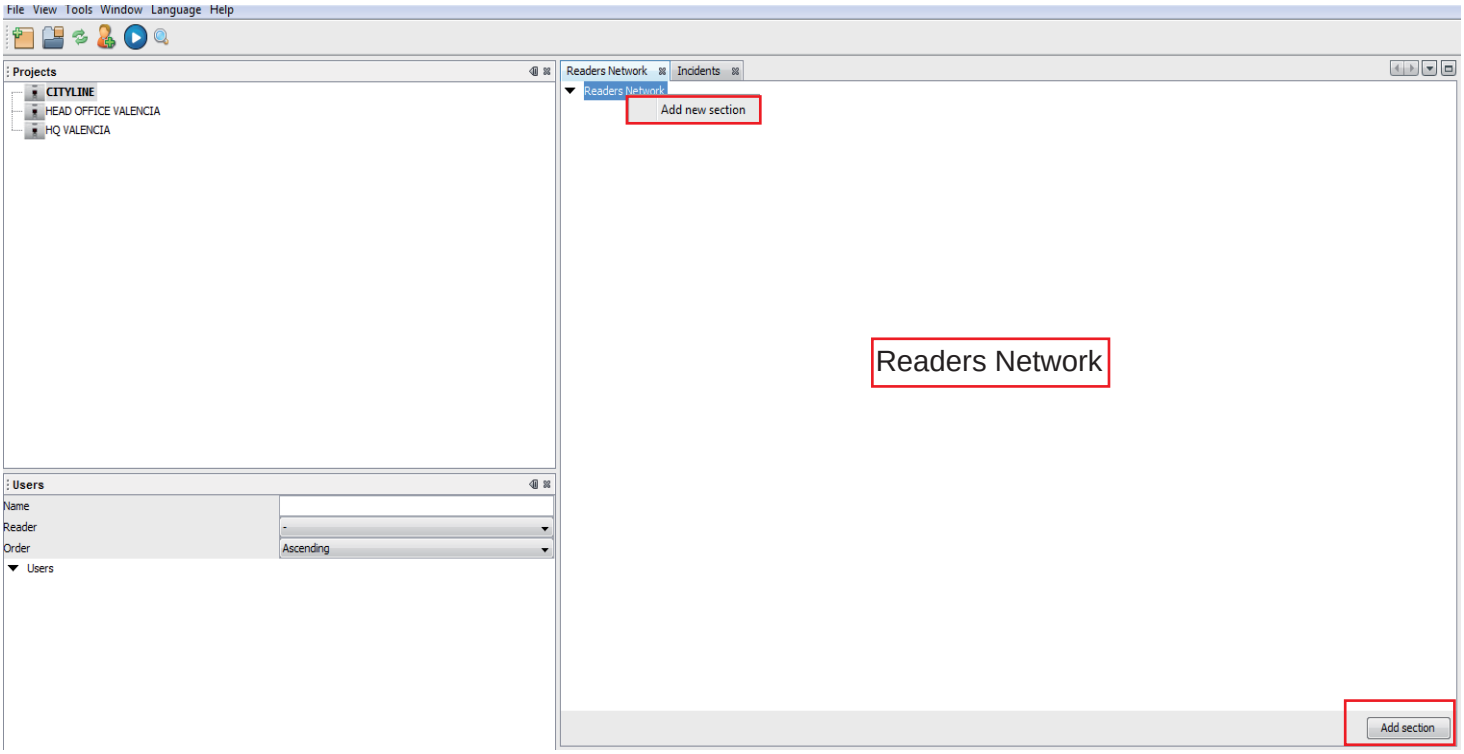
Accessible from the Reader´s network window. From here we can manage the different sections in our software and the readers connected to it each one. This allows us a schematic image of the installation.

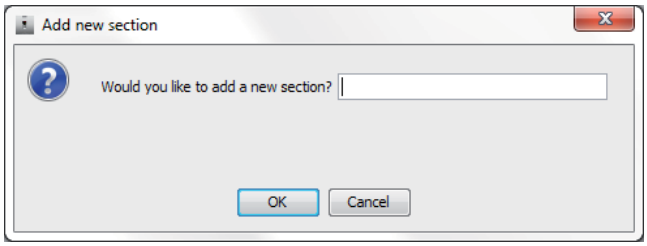
Sections

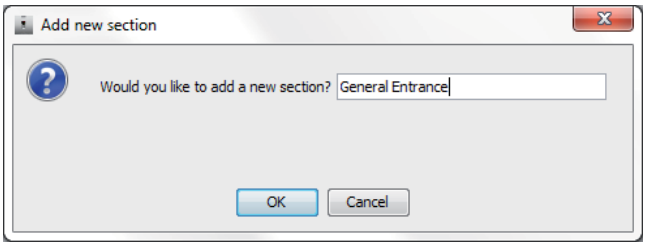
A section is each of the buses connected via ref. 2466, ref. 24661 and/or ref. 1087 to some of the ports RS-232, USB or IP to the PC. You can assign a different name to each of the sections for it to be more descriptive (perimeter section, administrative zone, general access area...).

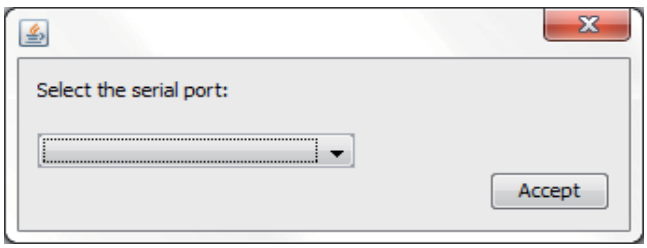
In order to define a new section, use the context button in the "Readers network" or with the direct button: "Add section." Once we have defined the section, we must assign one of the system´s available serial ports to make the communication. This is done by dragging the serial port used (COM1,COM2…) over the corresponding section node.

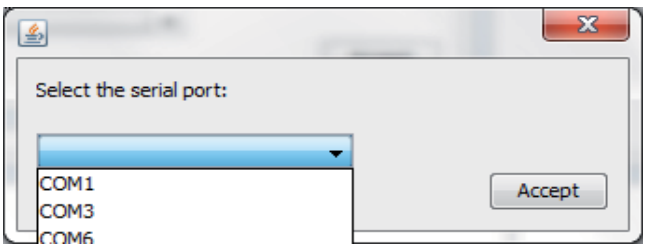
We can check the selected port for each of the sections in the properties window.

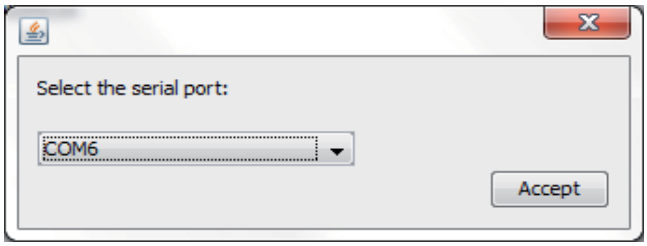


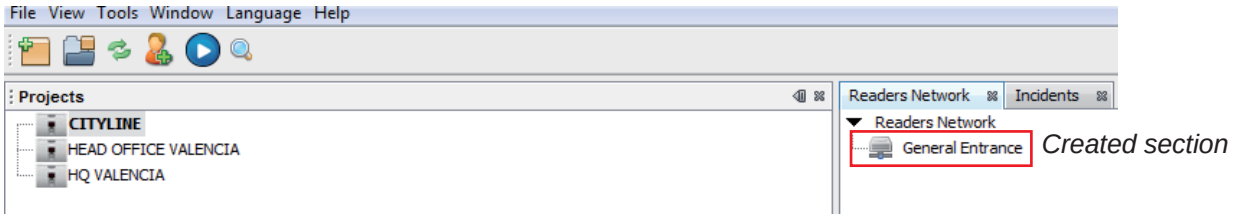




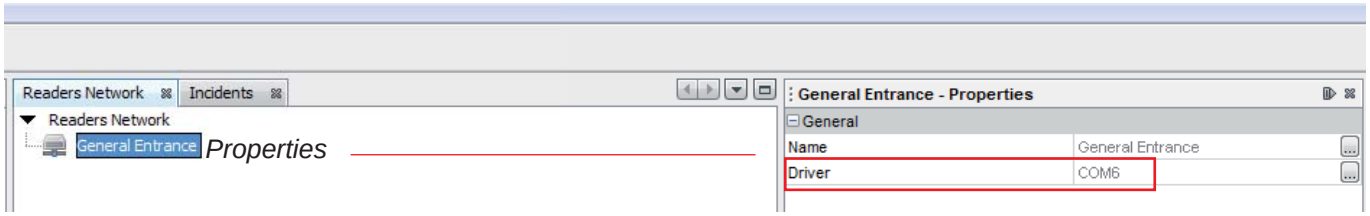






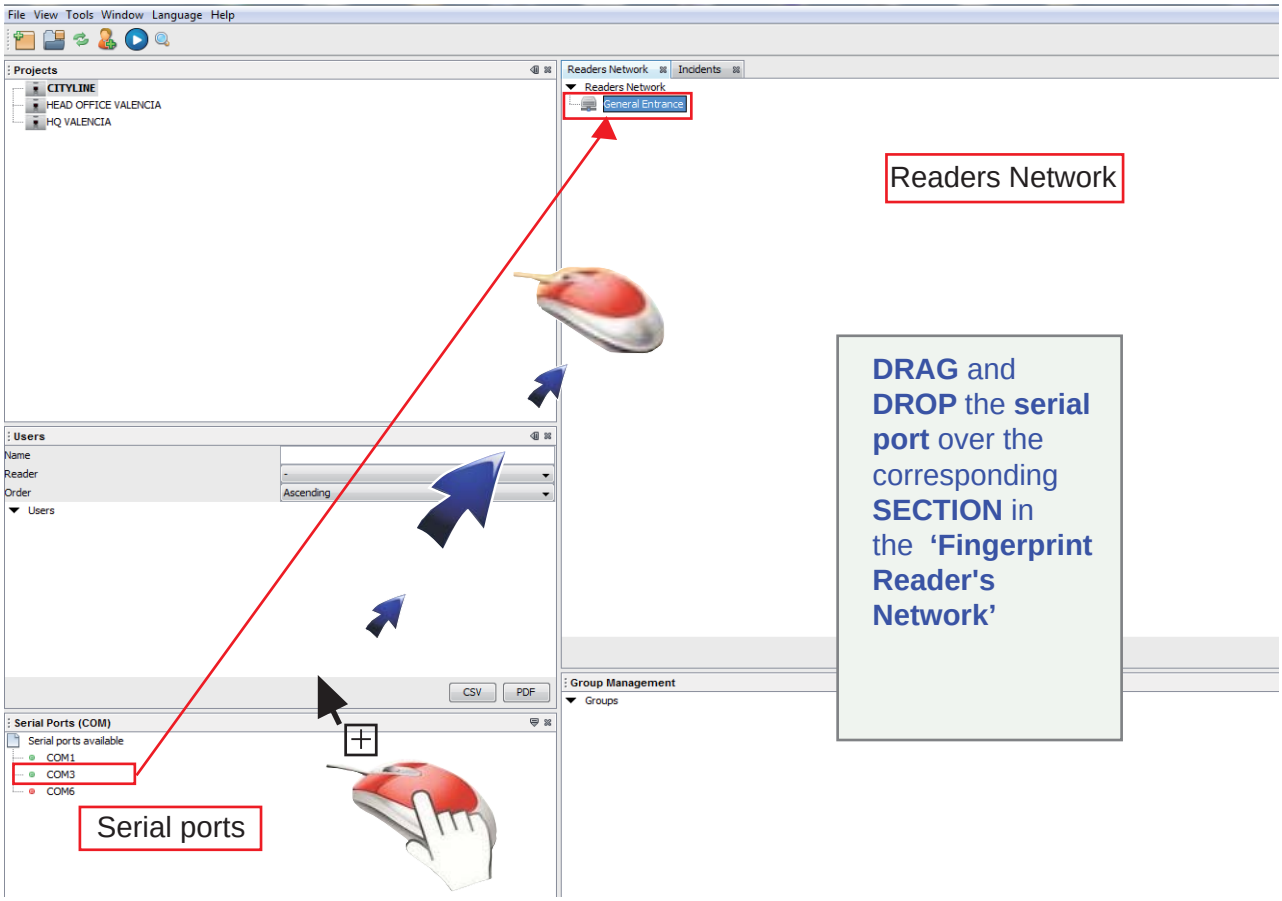


You can check the port by rolling over the **section**.

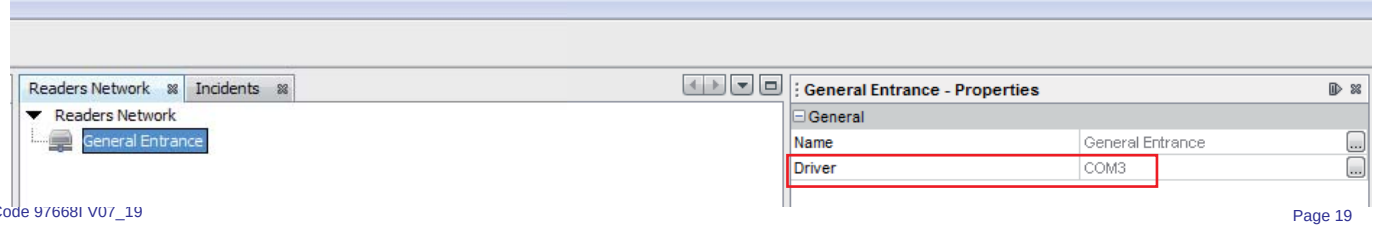


Edit the port over the section

To edit the port in said section just drag and drop the serial port in the 'Fingerprint Readers Network´**over the corresponding section**.



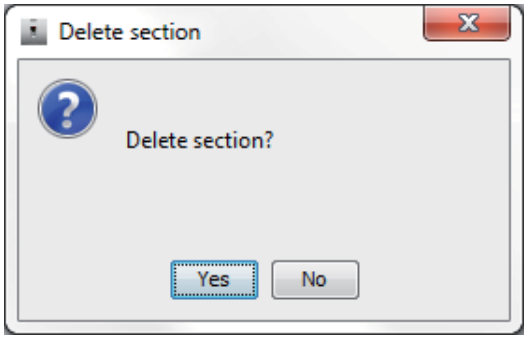
You can check the port by rolling over the **section**.



Section options. Available actions:

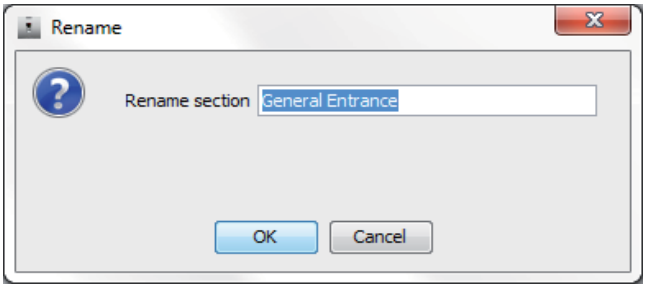
Delete section

This menu option deletes the selected section and all of its associated readers.



Rename section

This menu option changes the section name, opening a window to change the name in.



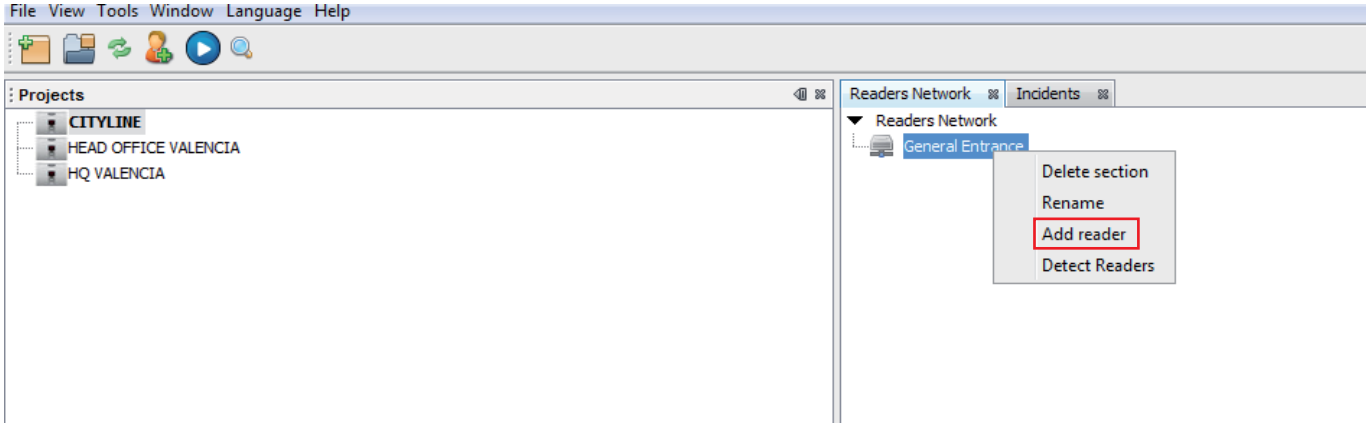
Add reader (manually insert readers)

In cases in which there is no reader system available **but there is at least one reader,** in order to register the first users, we may want to manage, create groups and define which readers a user is linked to without having connected the readers yet.

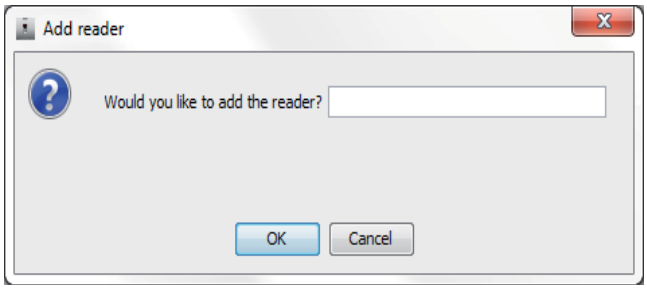
Then, once we have connected it to the network and have configured these readers we can transfer the users to those readers assigned during the start-up.

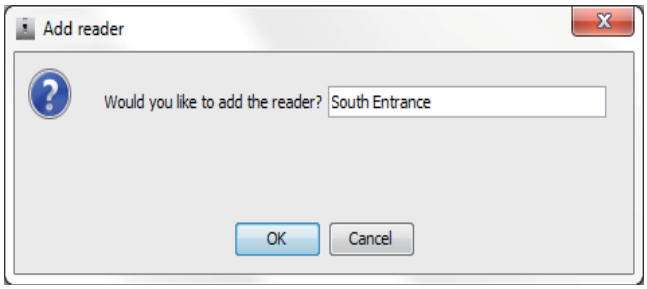
Within the contextual menu of each section via the "Add Reader" option we register a reader by giving it a name and assigning it a code via the properties window.

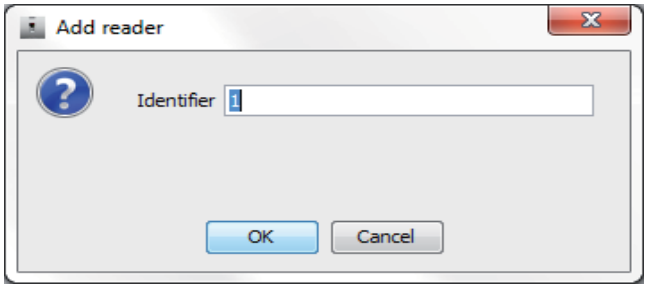
From this moment on, the reader may be used as if they were real readers in order to link them to groups and users.

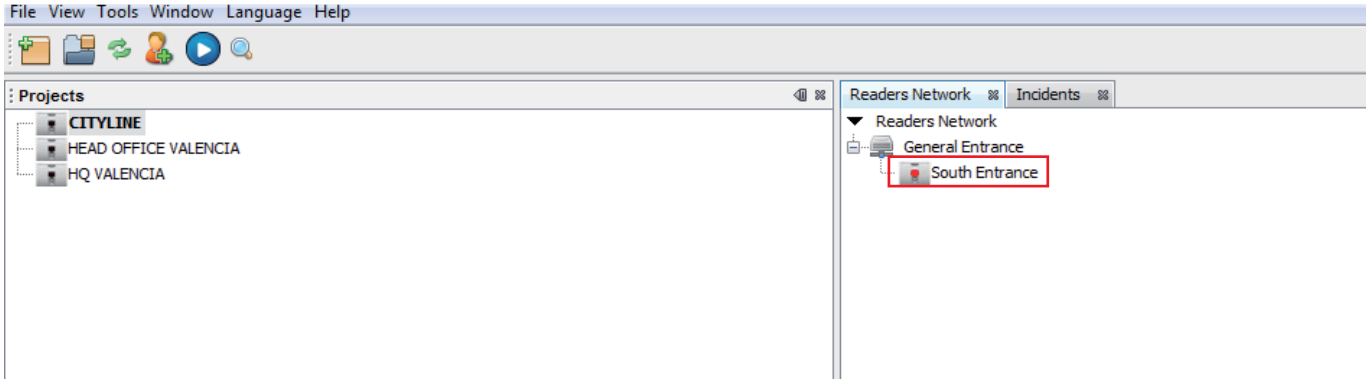


This menu option creates a reader and adds it to the section. For this it opens a window to ask for the name and then asks us to give it an identifier for this section.







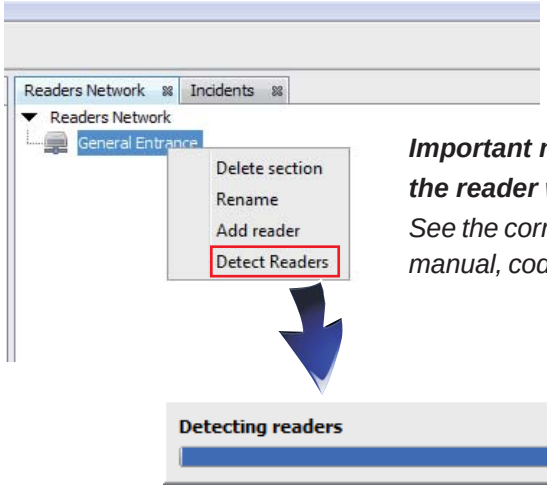


Reader detection

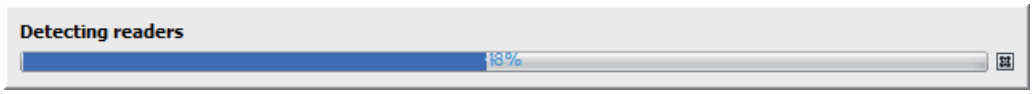
During the start-up of the installation each of the connected readers in each section must be registered . The fastest way to do this is by detecting them.

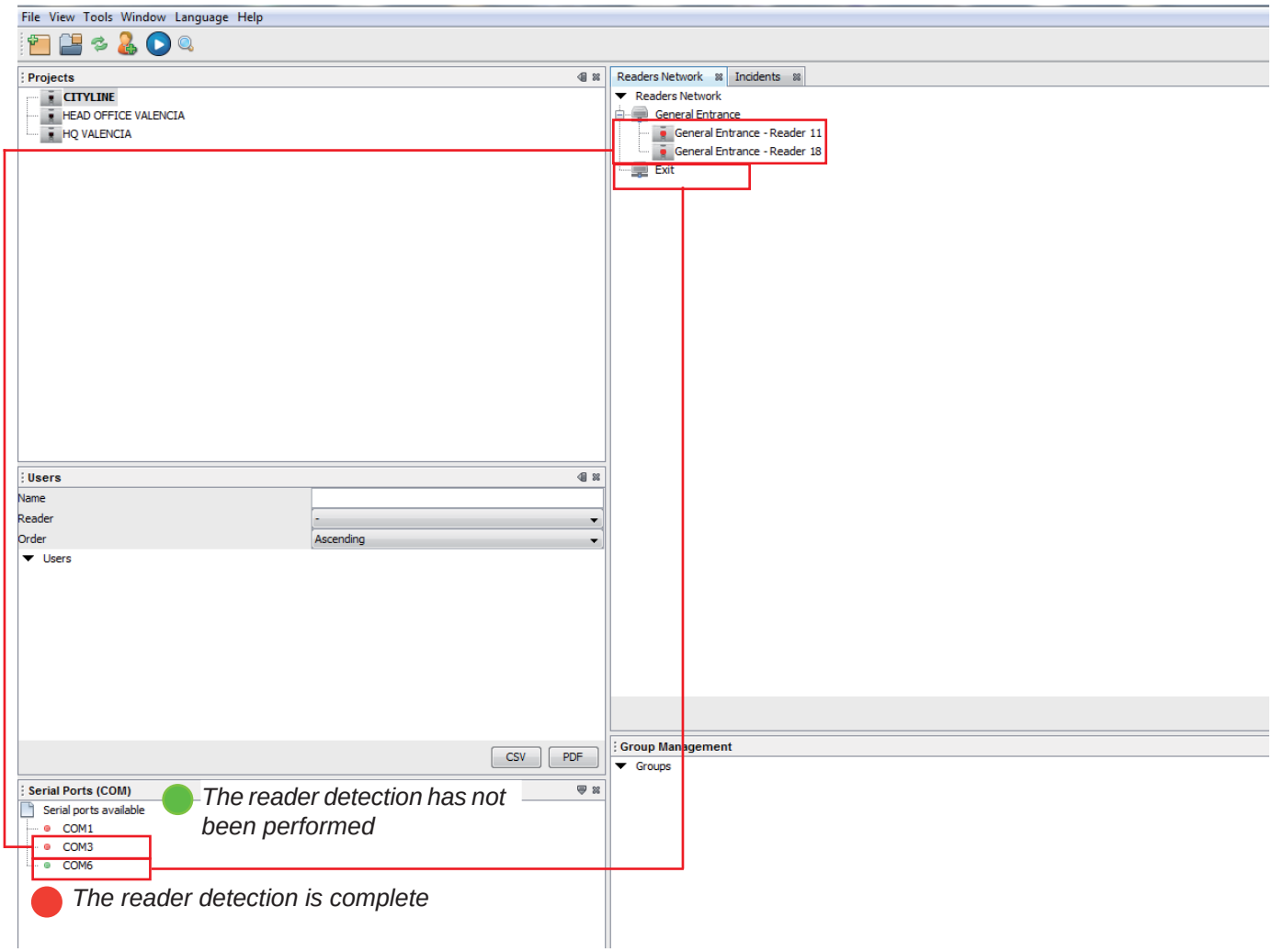
This operation performs an individual test for each of the 127 possible readers that we can have connected, from the codes 1 to 127. This takes a little less than 30" per section, depending on the no. of connected readers.
You can cancel this operation by pressing on the icon on the right of the progress bar.

Note: every time you delete or add a reader to the system you must repeat this operation.

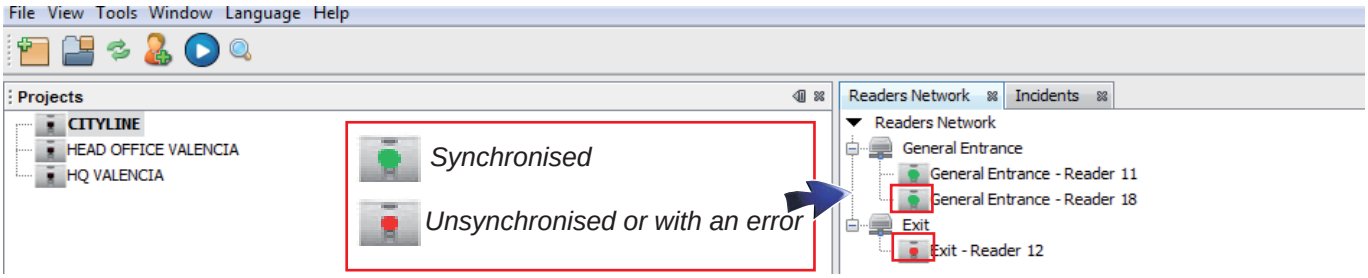


Important note:
the reader will not work if the master finger/card is not entered.
See the corresponding installation manual. AUTONOMOUS Fingerprint installation manual, cod. 97666 or CENTRALISED Fingerprint installation manual, cod. 97667.



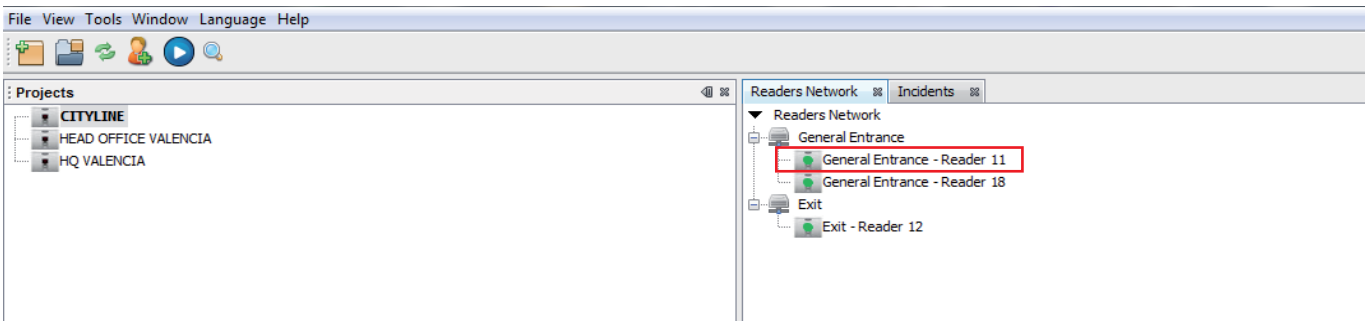


This screen has all of the readers and sections to which each one belongs to.
Depending on if the readers are synchronised or not, their icon would change:



The readers detected in the application get the section´s description along with the reader´s own encoding.
Example:

- Section: **General Entrance**
- Reader Encoding: **11, 12** and **18**.
- So the **description of reader 11** would be: **General Entrance - Reader 11**



Configuration and management of readers

Once the fingerprint reader is detected, relative to the class of reader (Autonomous or Centralised, via the reader´s dipswitch 8), the available actions and properties are different.

Considerations prior to detecting readers:
To ensure that the readers network properly performs the detection, the readers should:

- have a network Identifier* assigned.
- don't have repeated identifier numbers.
- if fingerprint readers with keypads are used, check/assign the keypad´s code length* (4 or 6 dígits).
- only in the Centralised, door controller encoding (wiegand-26 / data-clock) and relative to the selected encoding of the same communication protocol*.
- only in the Centralised, door controller encoding * .

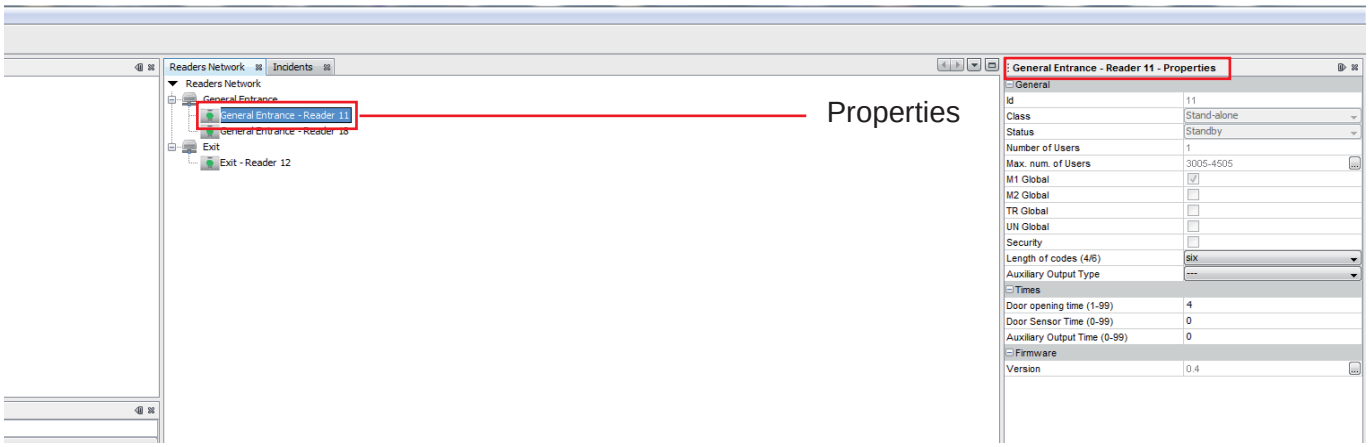
Note: see the corresponding installation manual. AUTONOMOUS Installation manual, cod. 97666 or CENTRALISED Fingerprint installation manual, cod. 97667.*

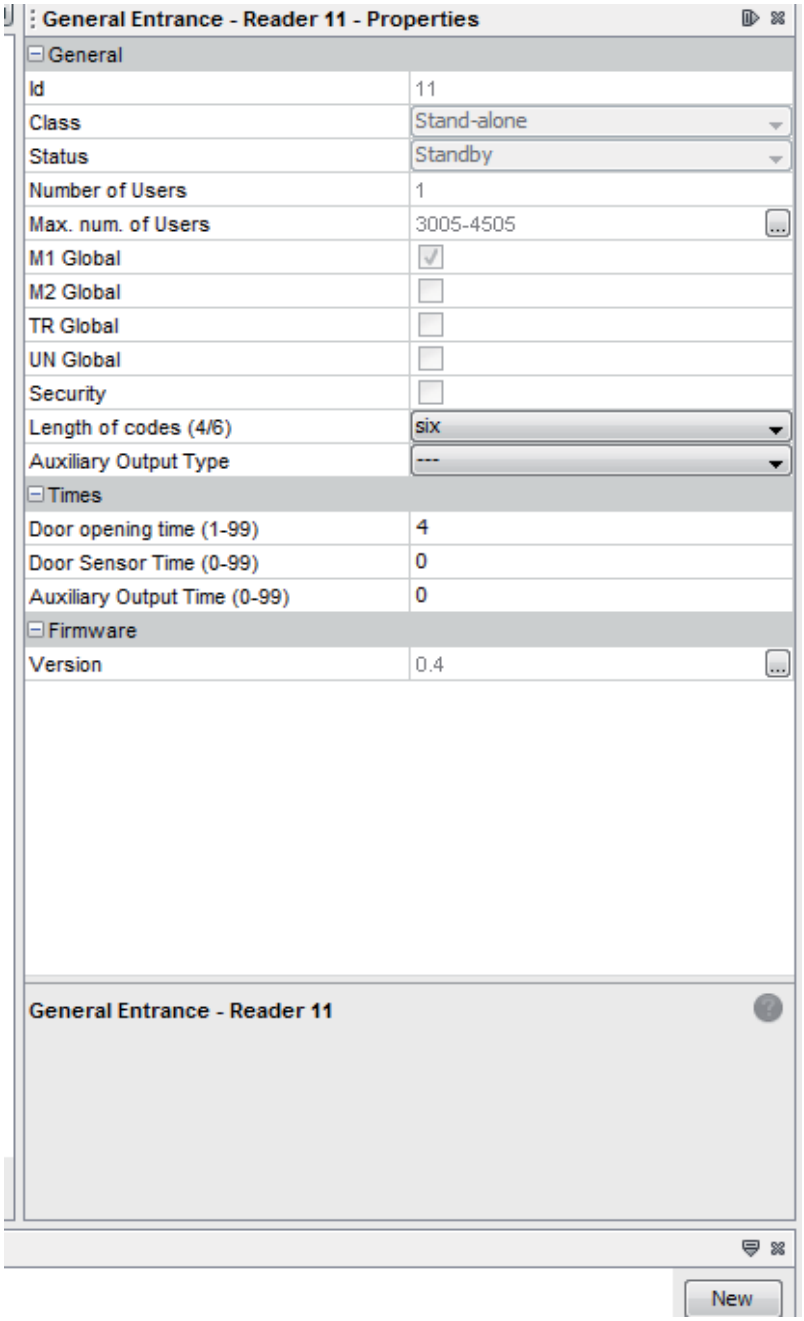
AUTONOMOUS Fingerprint Reader

This configuration in autonomous mode allows for the reader to decide to give access to a user or not.

Properties:

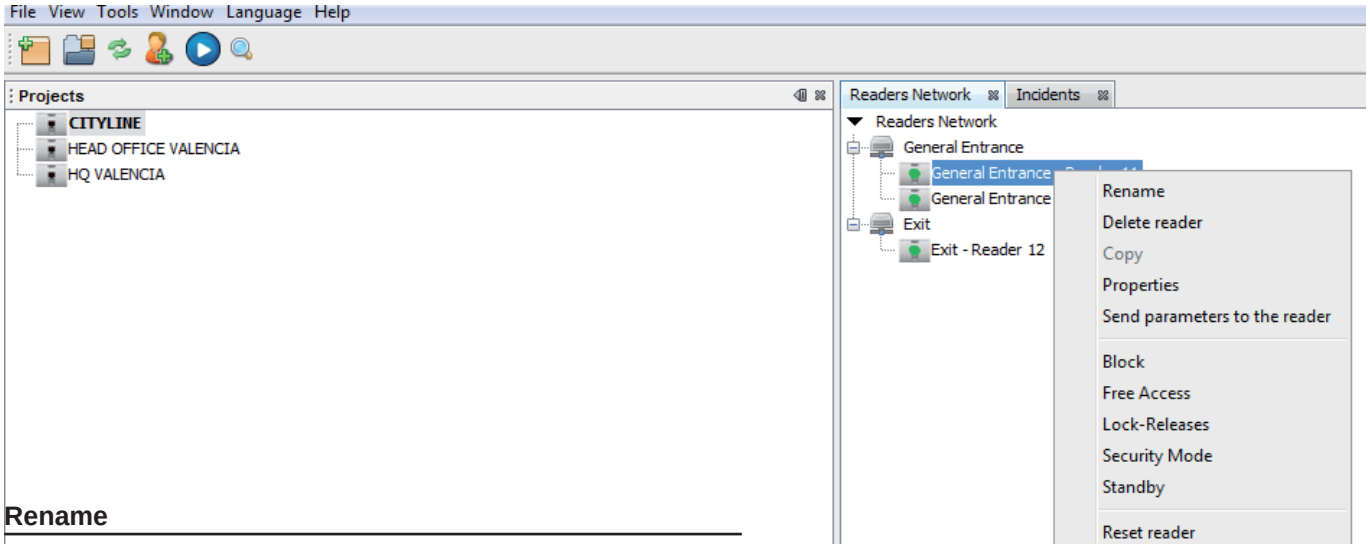
- **Id**: reader identifier (configured via the dip-switch).
- **Class**: autonomous (configured via dip-switch)
- **Status**: report of the current status in which the reader is configured (standby, blocked, security mode, unblocked, trades...)
- **No. of Users**: informs us of the no. of users that are currently occupying the reader´s memory.
- • **Max. no. of Users**: maximum capacity, which depends on the no. of fingerprints stored in each user. A maximum of 4500 for one fingerprint per user, and a maximum of 2970 if using 2 fingerprints per user.
- **M1, M2, TR, Un, Security**: indicates the presence of special users, Master, Free access (**Tr**ade), Unblock and Security.
  - o **M1 Global:** master Fingerprint/card 1. The master fingerprint/card is necessary to enter in programming mode.
  - o **M2 Global:** master Fingerprint/card 2. To register a second master fingerprint and allow the operation of the second fingerprint where there is a problem with the first one (short-circuit, fire damage..etc). or register a second master card.
  - o **TR Global:** free access fingerprint/card(**TR: Tr**ades). **TR Global**The trades option is a special "free access" function, which is activated from the reader by entering a registered fingerprint/card.
  - o **UN Global:** free access fingerprint/card(**UN: Un**block). The **UN Global** option is a special function to block/unblock access.
  - o **Security:** finger/Card security, you can add a user (finger or card security), that allows for a change in the way the reader operates.
- **Code lengths (4/6):** keypad codes permitted lengths (4 and 6 digits).
- **Auxiliary Output Type:** this activates the auxiliary output.
  - o - - -: none.
  - o Door alarm: activation by open/forced door alarm .
  - o Invalid user: activation with unrecognised fingerprint.
- **Door opening time (1-99)**: time the door's lock-release relay remains active.
- **Door sensor time (0-99)**: Maximum time the door can be open before an alarm goes off, (0: deactivated).
- **Auxiliary Output Time (0-99)**: time the auxiliary alarm remains active, (0: deactivated).
- **Server version:** reader's firmware version.





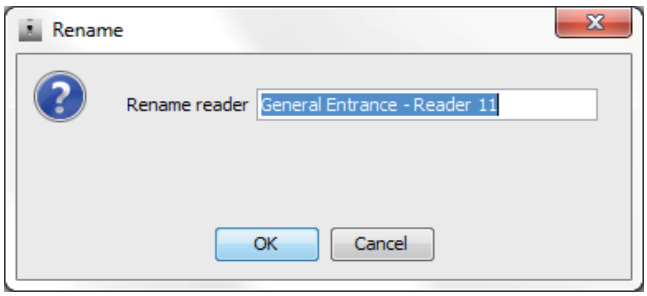
Note: *if a property changes from the screen, you must select "Send parameters to the reader." For this right-click over the reader.*

Options for autonomous readers. Available actions:



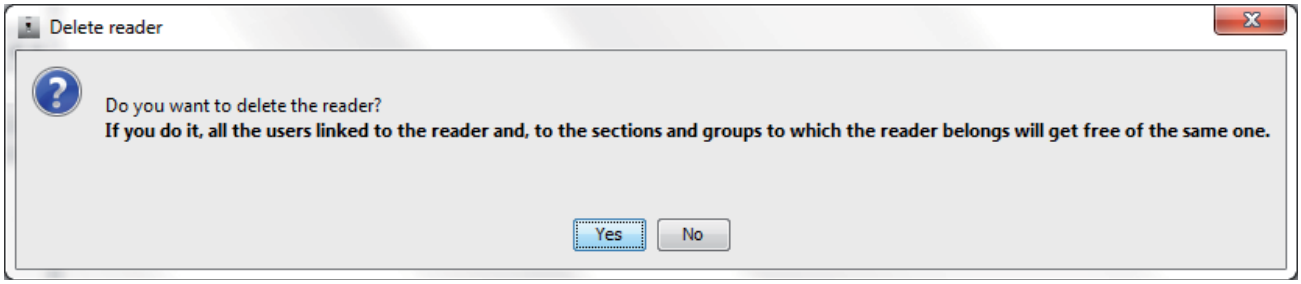
Rename

The readers can receive a name relative to the door it belongs to with the "rename" option. We can change the reader´s default name to a more descriptive one.
This menu option allows us to change the reader´s name, opening the following change of name screen.



Delete reader

This menu option deletes a reader. But first it asks for confirmation. It is not available until it has been detected.

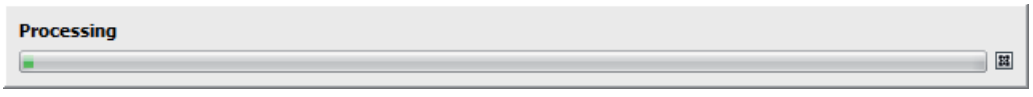


Properties

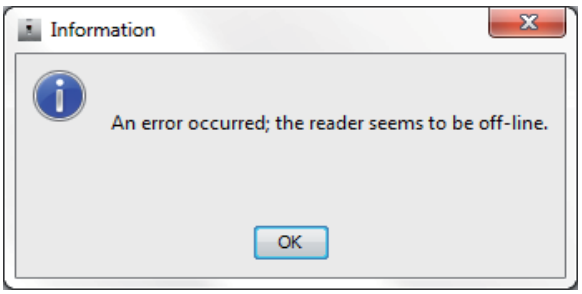
Open the properties window of said reader. See the screen on the previous page.

Send parameters to the reader

This menu option sends the reader parameters as configured from the reader´s software.
During the process the following progress bar is displayed.

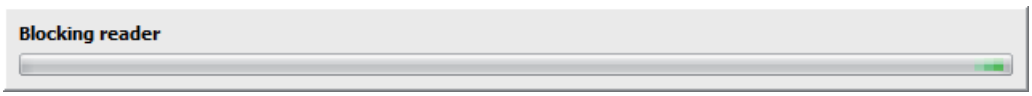


If there is an error, the following screen appears.

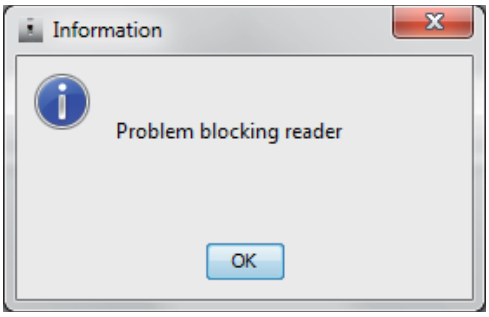


Block

Leave the reader in a status so no user has access, until it returns to standby.
This menu option opens the block reader command.
During the process the following progress bar is displayed.

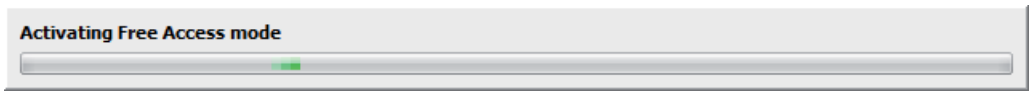


If there is an error, the following screen appears.



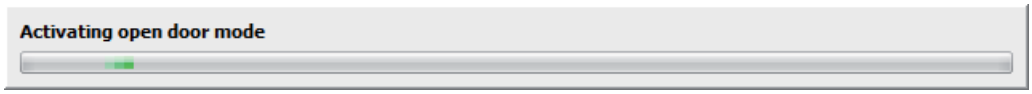
Free Access

This allows any card or fingerprint to activate the lock release. During the process the following progress bar is displayed.



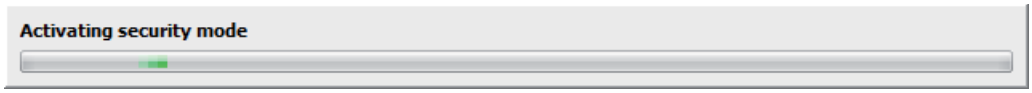
Lock-Releases

The lock release relay remains active continuously. You don´t have to pass the fingerprint or a card to open the door.
During the process the following progress bar is displayed.



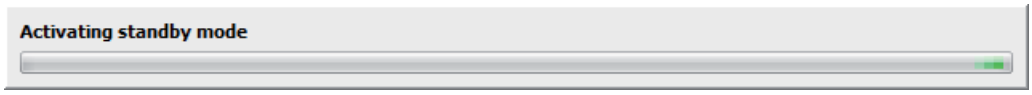
Security Mode

Enable the security mode, requiring the keypad code or card along with the fingerprint. During the process the following progress bar is displayed.



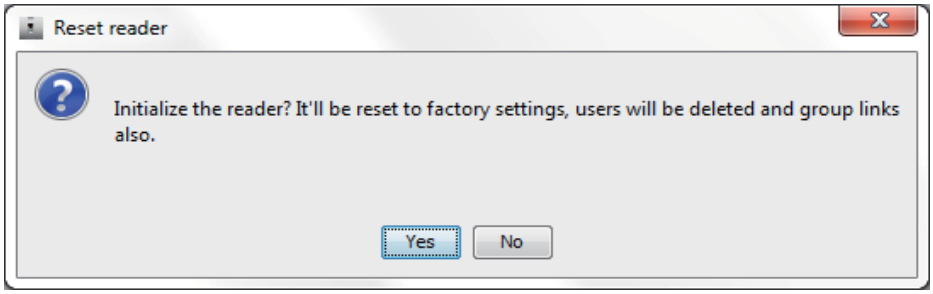
Standby Mode

Return the reader to standby, all other statuses are deactivated. During the process the following progress bar is displayed.



Start reader

This menu option opens the start reader command. This deletes all reader users included in Master 1, leaving the reader with default values.
Before launching the command, it warns us that this will delete all users from that reader and the software will remove the link between the reader and all users and groups. The confirmation screen is the following:

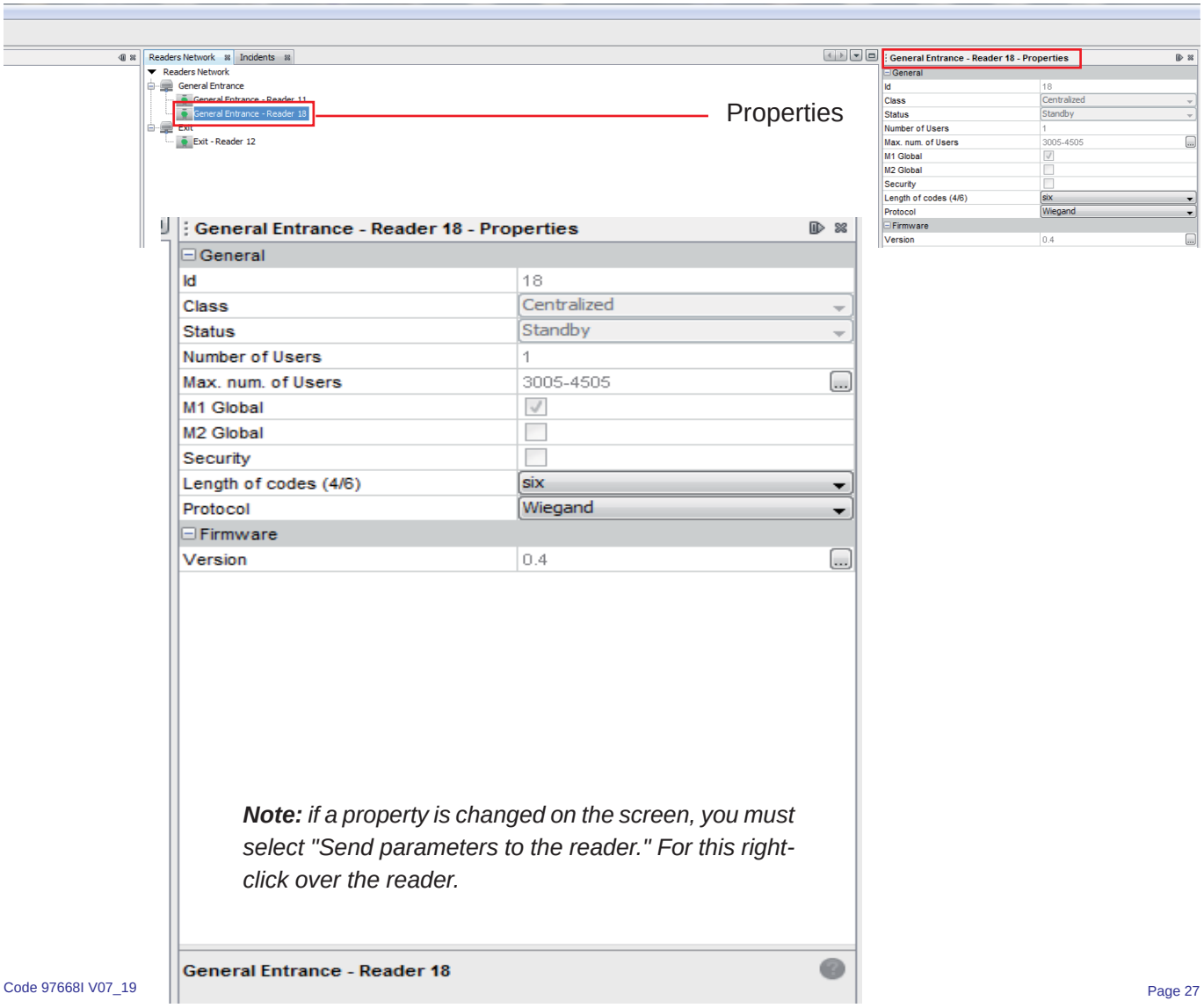


CENTRALISED Fingerprint Reader

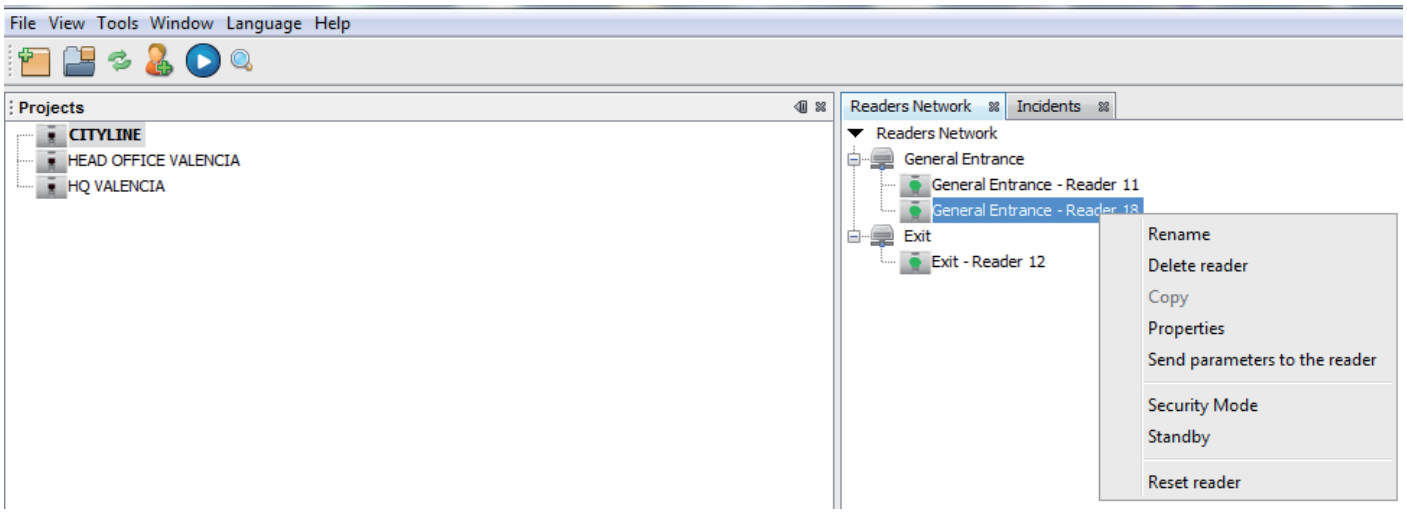
In this configuration the reader behaves as a generator of codes that are transmitted to a door controller ref. 4420. It is this controller´s responsibility to limit the access by schedule, code, etc...

Properties:

- **Id**: reader identifier (configurable via the door controller).
- **Class**: centralised (configured via dip-switch)
- **No. of Users**: informs us of the no. of users that are currently occupying the reader´s memory.
- **Max. no. of Users**: capacity of storing in 1 or 2 fingerprints per user:
  - Central units with capacity for up to:
    - **1020 users** with the UC MDS (ref. 2405).
    - **2046 users** with the UC AC Plus (ref. 4410).
- **M1, M2**: indicates the presence of special Master and Security users.
  - **M1 Global:** master Fingerprint/card 1. The master fingerprint/card is necessary to enter in programming mode.
  - **M2 Global:** master Fingerprint/card 2. To register a second master fingerprint and allow the operation of the second fingerprint when there is a problem with the first one (short-circuit, fire damage..etc). or register a second master card.
  - **Security:** finger security, you can add a user (finger or card security), that allows for a change in the way the reader operates.
- **Code lengths (4/6):** keypad codes permitted lengths (4 and 6 digits).
- **Protocol**: encoding format with which the generated code is transmitted to the door controller.
  - **Wiegand**
  - **Dataclock**
- **Server version:** reader's firmware version.
- **Door Sensor Timing**: Maximum time the door can be open before an alarm goes off, (via the door controller).
- **Auxiliary Output Time**: time the auxiliary alarm remains active, (via the door controller).



Options for centralised readers. Available actions:



The available actions, since the workload is done by the door controller, are:

- **Rename**: we can change the reader´s default name to a more descriptive one.
- **Delete reader**: delete the installation´s reader. It is not available until it has been detected.
- **Properties**: open the properties window of said reader (previous page).
- **Send parameters to the reader**: send the the changed reader´s configuration.
- **Security Mode:** enable the security mode, requiring the keypad or card code along with the fingerprint.
- **Standby Mode:** return the reader to standby, all other statuses are deactivated.
- **Start reader**: this menu option opens the start reader command. This deletes all reader users included in Master 1, leaving the reader with default values.

Note: *these actions are described in more detail with their corresponding screen shots in: "Options for autonomous readers" (previous pages).*

USERS

Description

A user is each one of the different accesses a person may have, whether it is with their fingerprint, proximity card or a keypad code.

Each AUTONOMOUS fingerprint reader can store the following number of users depending on the mode selected.

- Number of users:
  - 4500 in 1 fingerprint per person mode.
  - 2970 in 2 fingerprint per person mode.

Each CENTRALISED fingerprint reader has the capacity to store 1 or 2 fingerprints per user:

- Number of users.
  - o Central units with capacity for up to:
  - **1020 users** with the UC MDS (ref. 2405).
  - **2046 users** with the UC AC Plus (ref. 4410).

ADJUSTMENTS prior to registering Users.

Before describing the management of users, first check some of the software´s adjustments.

a) Auxiliary Reader for registrations: once the readers on the system are detected, as explained in the previous section, we must select the reader to use to provide the new user registrations.

b) Number of fingerprints per user: if we are going to use users with double fingerprints in our system (for security or double function) we must activate the "Main + secondary fingerprint" mode.

Possible functions in "Main + secondary fingerprint":

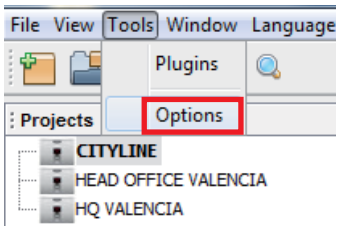
- 2 fingerprint identifications per user.
- Security mode: 2 Fingerprints + Card.
- Security mode: 2 fingerprints + code. *Note: this requires a keypad module connected to the reader.*

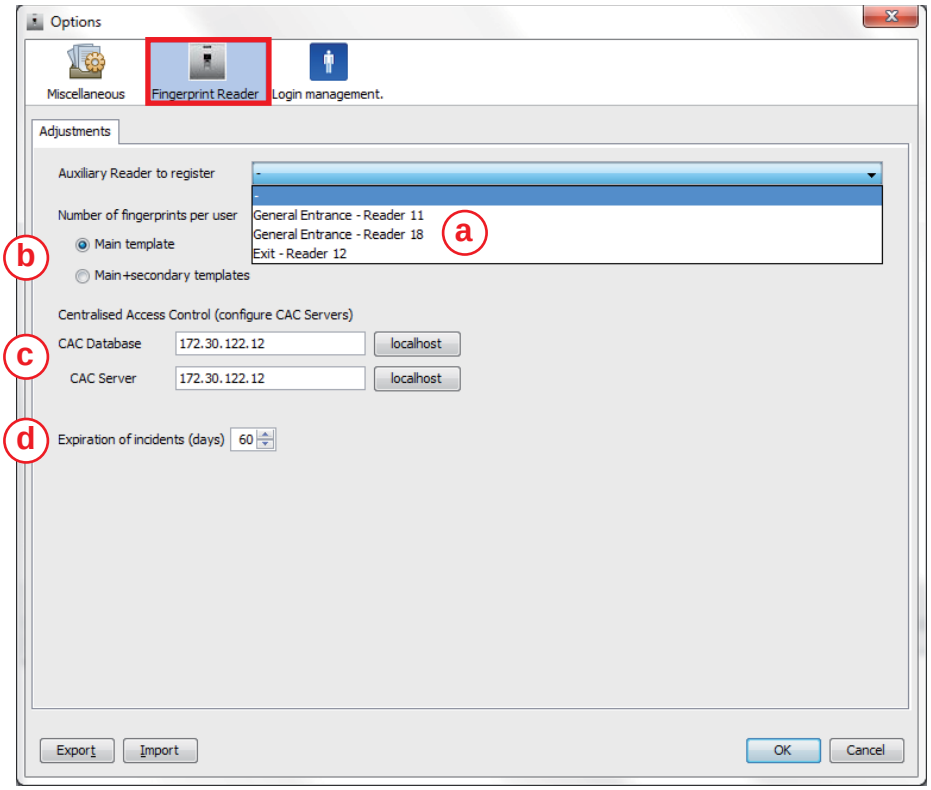
Possible functions in "Main fingerprint" mode:

- 1 fingerprint identifications per user.
- Security mode: fingerprint + card.
- Security mode: fingerprint + code. *Note: this requires a keypad module connected to the reader.*

c) Centralised Access Control: if we have a Centralised Access Control system and want to synchronise the users in this system with the fingerprint, here we must indicate the IP addresses of both servers.

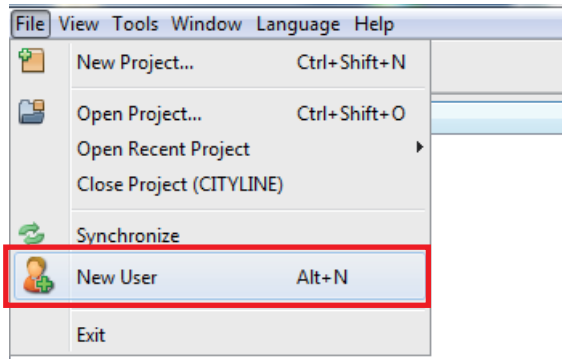
d) Incident expiration: the number of days the incidents will be saved. 0 indicates no expiration.

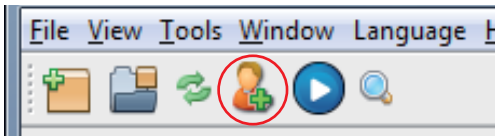




Description Register user / Change user

Register new users by pressing on the corresponding icon of the tool bar or from the File-New User menu.

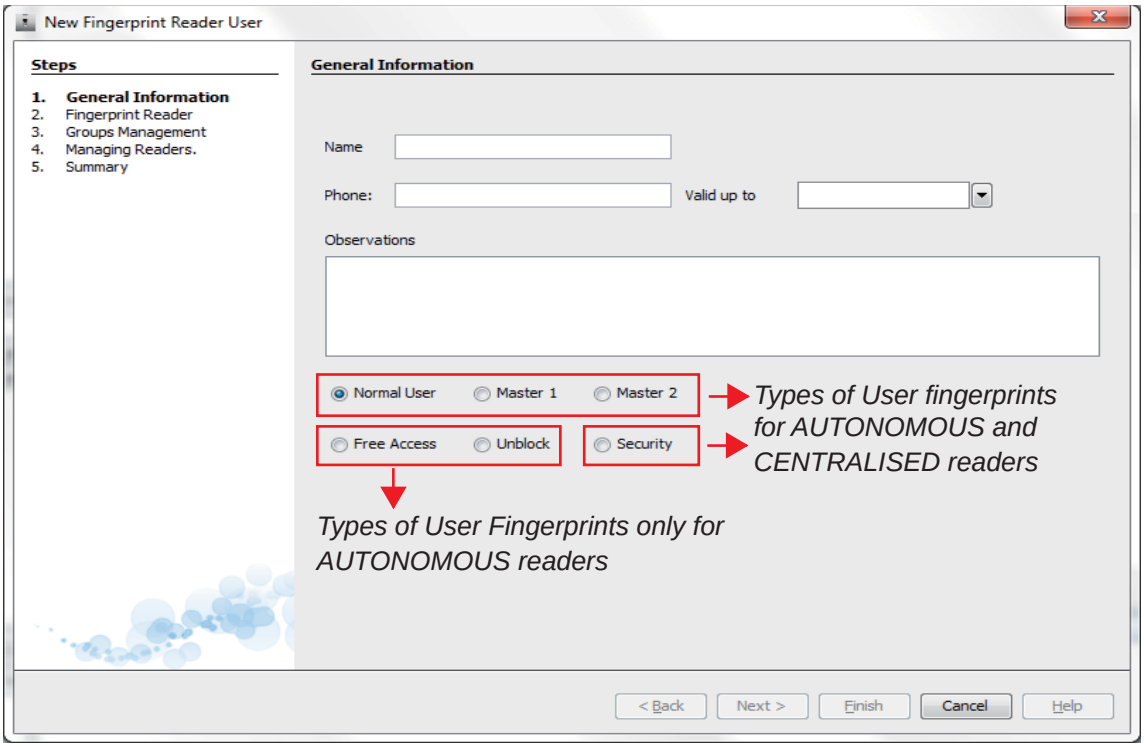




This assistant helps to **create** users to assign to readers. You can also **modify** the users.

The assistant takes 5 steps:

1. General information.
2. Fingerprint reading.
3. Manage Groups, **this is only shown if groups have been registered in the application.**
4. Manage Readers, **this is only shown if readers have been registered in the application.**
5. Summary - Enable/Disable direct user insertion.



1. General user information:

- **Name**: alpha-numerical descriptive identifier of the user.
- **ID**: this is the internal code used by the reader if communicating with a door controller in CENTRALISED mode. The application provides a open code, even though you can modify it at will. This is the code shown on the display.
- **Tel**: person´s telephone
- **Valid up to (optional):** we can create temporary users that automatically expire and are deleted from the system after a specific date[1] . Expired users are marked with an asterisk, and those expired for more than a day are marked in red, see the chapter "Graphic view of the types of Users."
  Note[1]: The application must remain open for it to be deleted, or run periodically. The process is run at midnight and each time the application is run and has a project open, or every time a project is loaded.
- **Observations:** we can include any information that can be of interest to identify this user. A classic example is the indication of the finger used for identification.
- **Type of user:**
  - o **Normal:** regular user of an access control system. It does not have any type of privilege.
  - o **Master 1, Master 2**: allows you to access the reader´s local configuration menu.
  - o **Free Access (Trade):** allows for the activation/deactivation of 'Free Access' (just the AUTONOMOUS reader).
  - o **Unblock:** allows for unlocking/blocking (standby) the lock-release indefinitely (just the AUTONOMOUS reader).
  - o **Security:** allows for enabling/disabling the security mode, which requires the card or keypad code besides the fingerprint (AUTONOMOUS and CENTRALISED readers).

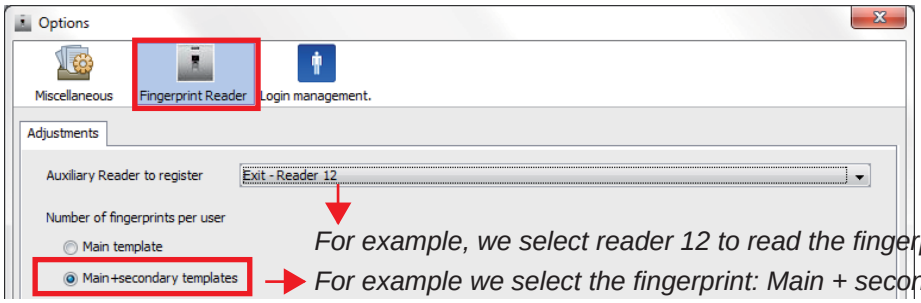
2. Fingerprint Reader

In this section you can assign the biometric, keypad or proximity card information you want the user to have. Remember that the reader on which the fingerprint reading should be done is the one selected in: "ADJUSTMENTS prior to registering Users." The reading will only be requested from this reader.

1. **Main Fingerprint.**
   The first of these tabs is used to register the main fingerprint. This fingerprint requires a double reading, as it requests. Each time you have 8 seconds to pass the fingerprint on each sensor.

   We must also select the output this access should activate (open door relay, auxiliary or both).

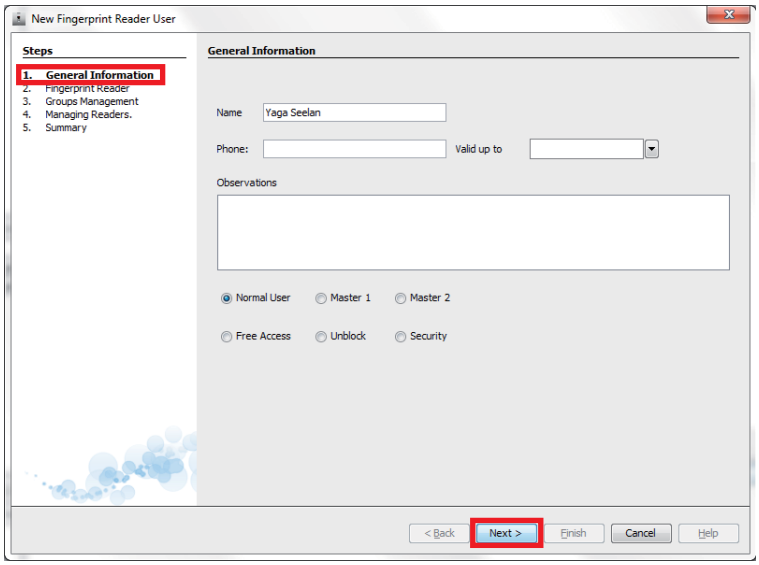
If we define the user data and press next, the **Main fingerprint template screen** or the **Main + secondary fingerprint template screen** appears. The selection of these profiles is done via: *Tools / Options:*



For example, we select reader 12 to read the fingerprint

For example we select the fingerprint: Main + secondary fingerprint

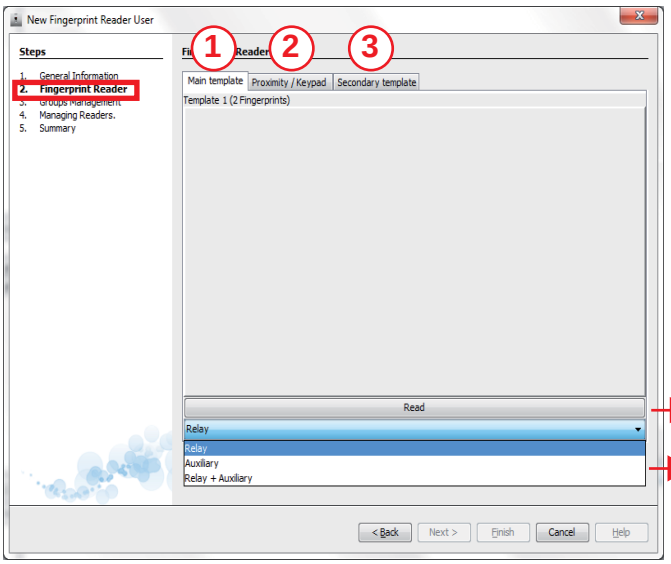
The sequence to CREATE a user with a Main + secondary fingerprint template:



1. Main fingerprint

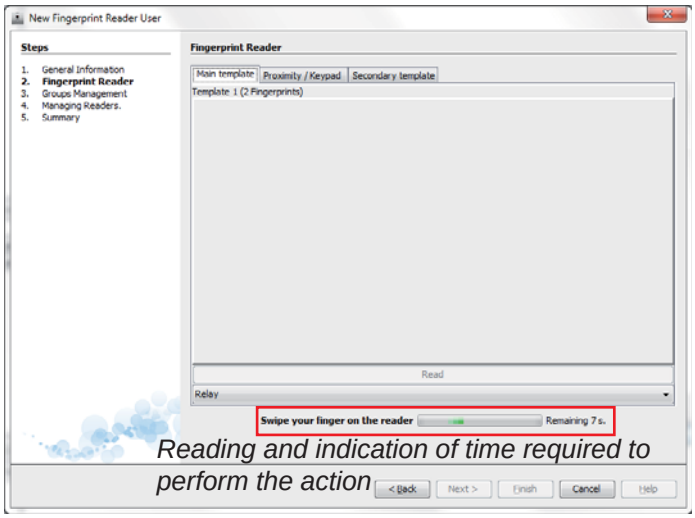
The first of these tabs (tab 1) is used to register the main fingerprint. This fingerprint requires a double reading, as it requests. Each time you have 8 seconds to pass the fingerprint on each sensor.

We must also select the output this access should activate (open door relay, auxiliary or both).

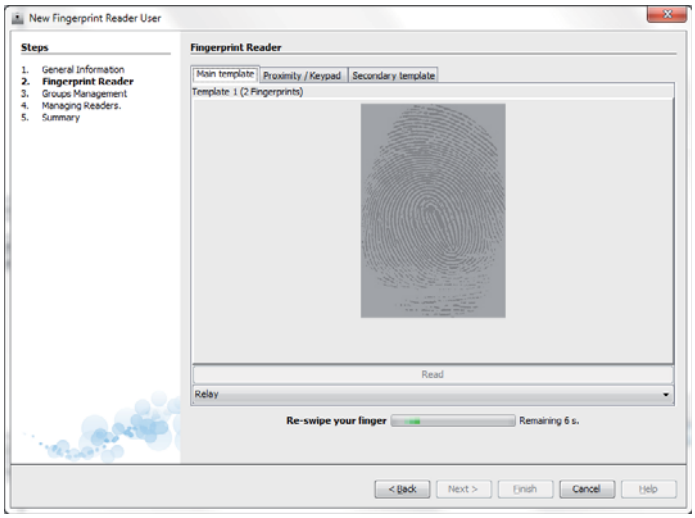


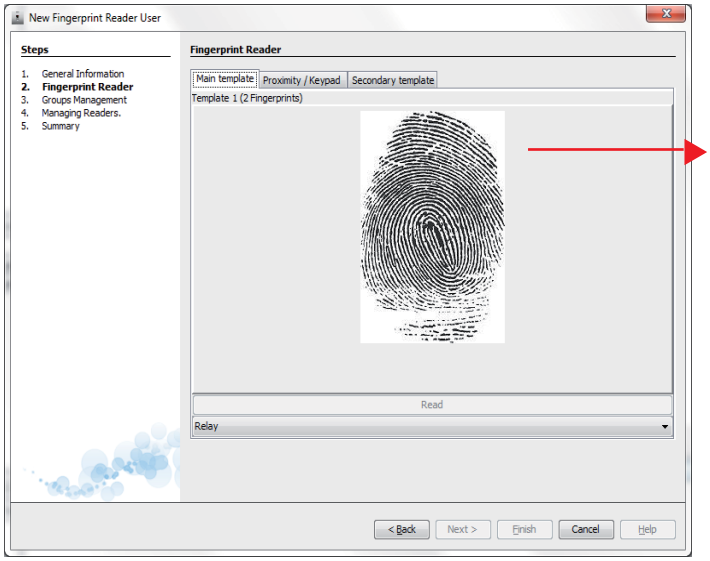
Press here to start reading.

Also select the output this access should activate (open door relay, auxiliary or both).



Reading and indication of time required to perform the action





Note:
the fingerprint image does not correspond to that of the user for security and data protection purposes.

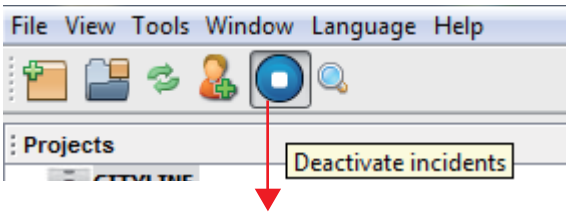
Note: you will be notified if you enter a fingerprint that has already been used or that has high level of similarity with another fingerprint.

2. Keypad / Proximity.

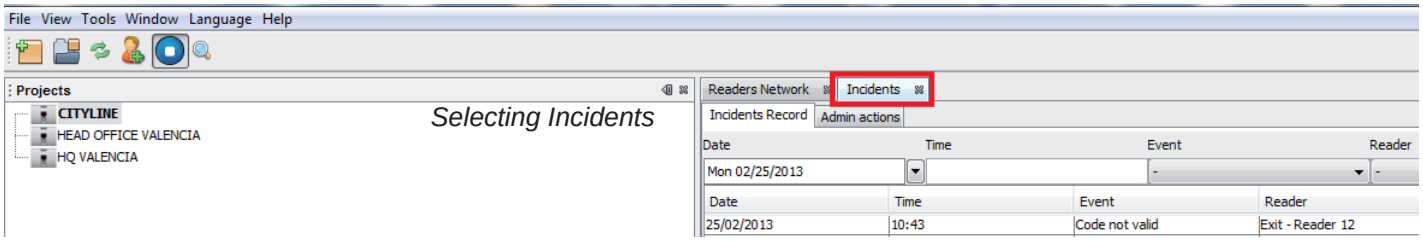
In the second tab (tab 2), you configure the proximity card code or keypad code. If we have the incidents activated, we can pass the card over the reader in order for this field to fill-in automatically with the card´s code.

For the keypad´s code, the configured length for each reader is (4 or 6). *Note: this requires a keypad module connected to the reader.*

Press to activate incidents



Press to deactivate incidents



Selecting Incidents

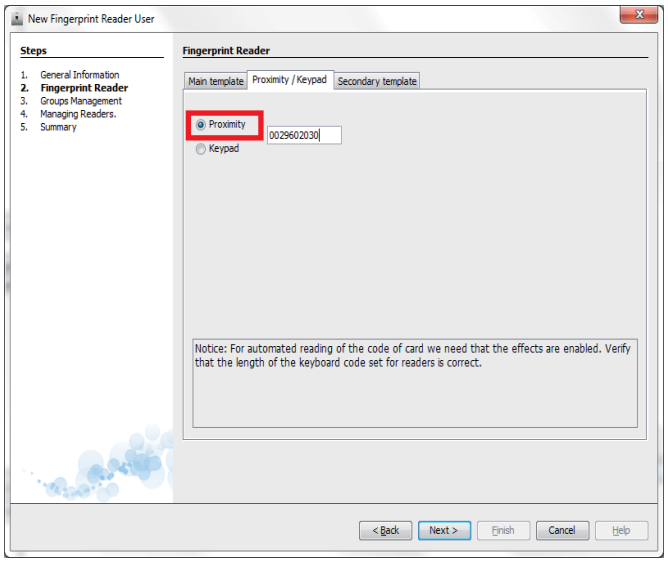
Previous considerations.

For the user to be registered properly on the reader:

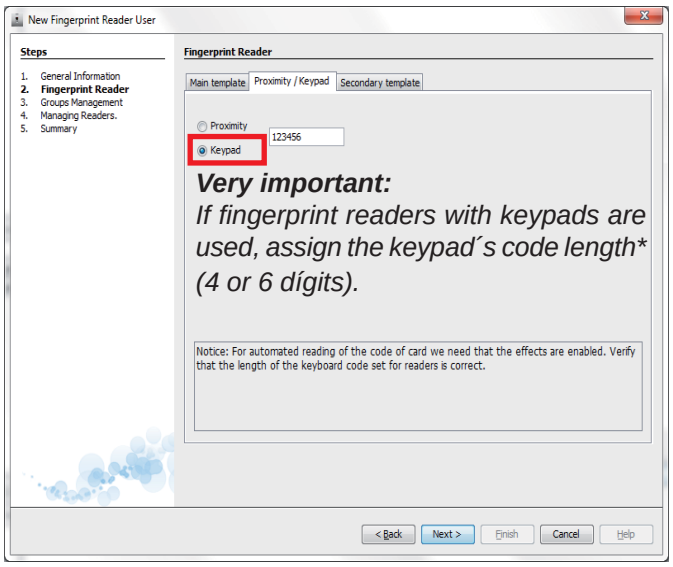
- if fingerprint readers with keypads are used, check/assign the keypad´s code length* (4 or 6 dígits).
- in order to recognise the card or keypad code, assign the Security mode on the reader.
- only in the Centralised, door controller encoding (wiegand-26 / data-clock) and relative to the selected encoding of the same communication protocol*.
- only in the Centralised, door controller encoding * .

Note: see the corresponding installation manual. AUTONOMOUS Installation manual, cod. 97666 or CENTRALISED Fingerprint installation manual, cod. 97667.*

If you choose **Proximity**



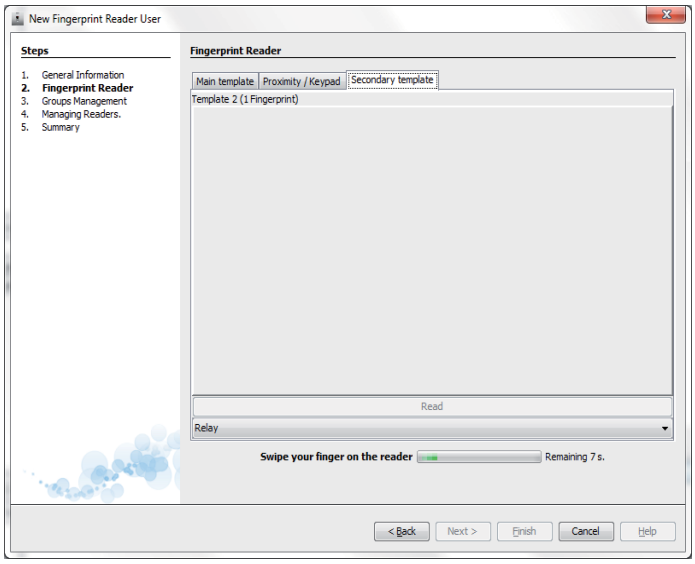
If you choose **Keypad**

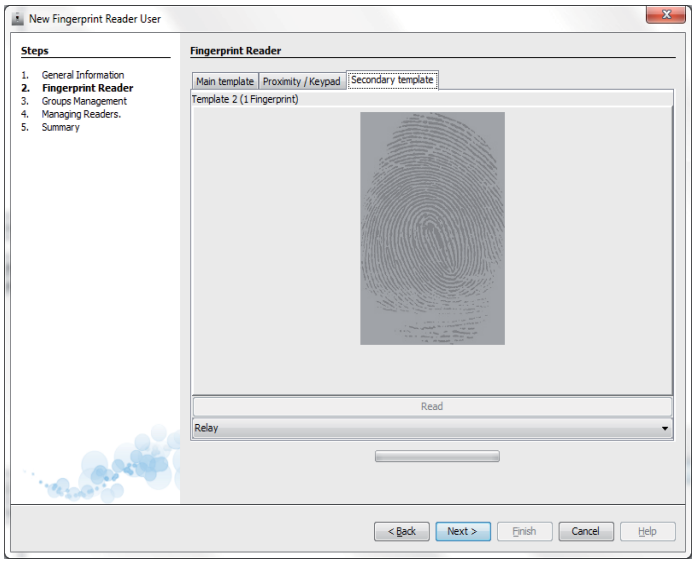


3. Secondary Fingerprint.

The third tab (tab 3), is to register a second fingerprint. It works identically as the main fingerprint, with the only difference being that it only does one reading of it.

We must also select the output this access should activate (open door relay, auxiliary or both). You can assign an output different from the main one.



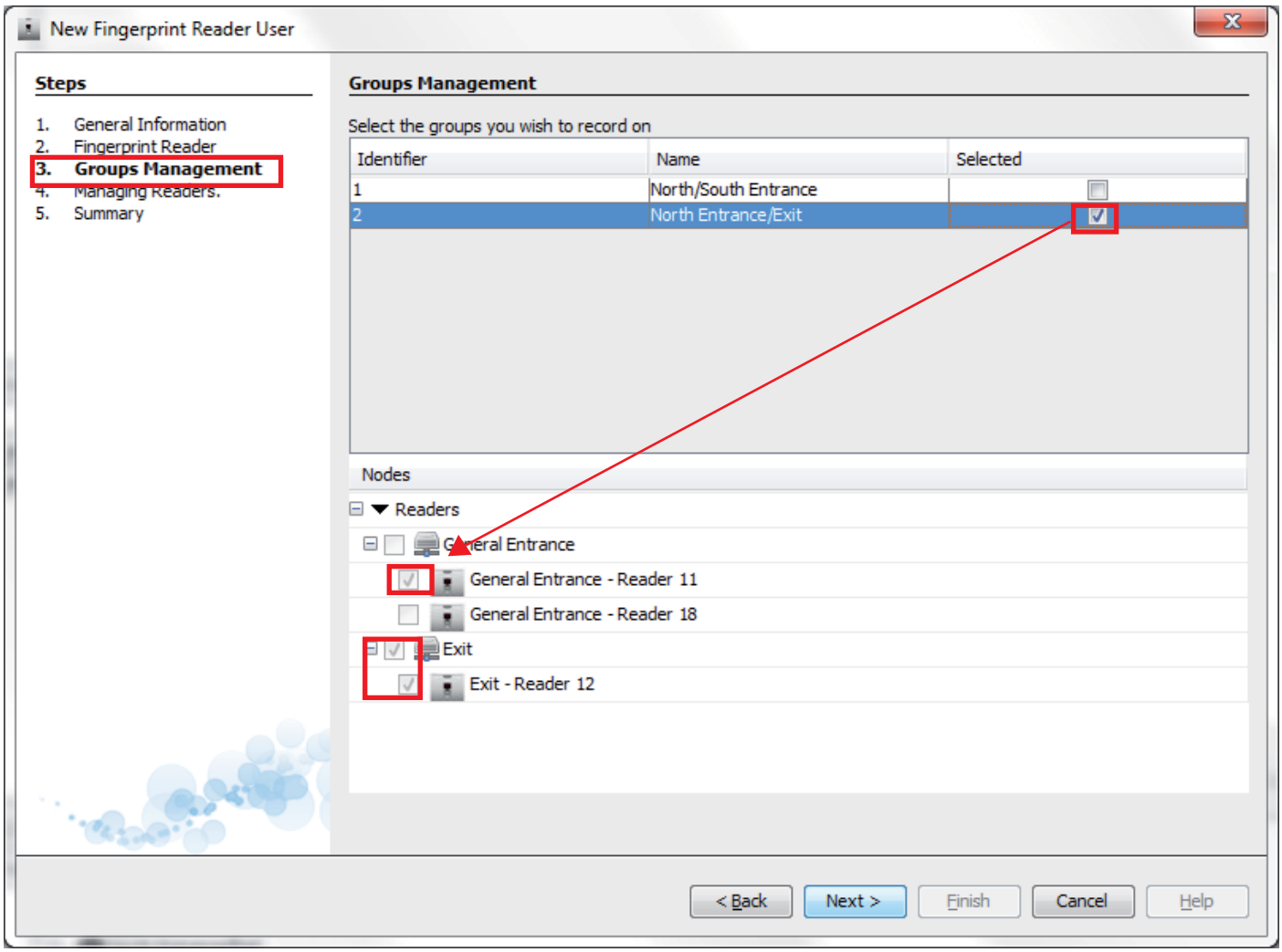


***Note:** upon having selectedthe template: "Main + secondary fingerprint", you must register the secondary fingerprint.*

3. Manage Groups - assign users

Using groups is a dynamic way of assigning which readers a user will have access to. On this screen the user can be assigned to groups. See chapter "Groups" for more information.

On this screen you must select the groups to which you want to assign the user. Each group selected in the previous part, the change is shown on the reader´s view so that you know which readers are assigned to the user upon being assigned to a group.



Note: the screen Manage Groups, ***is only shown if groups have been registered in the application.*** *See chapter "Groups" for more information.*

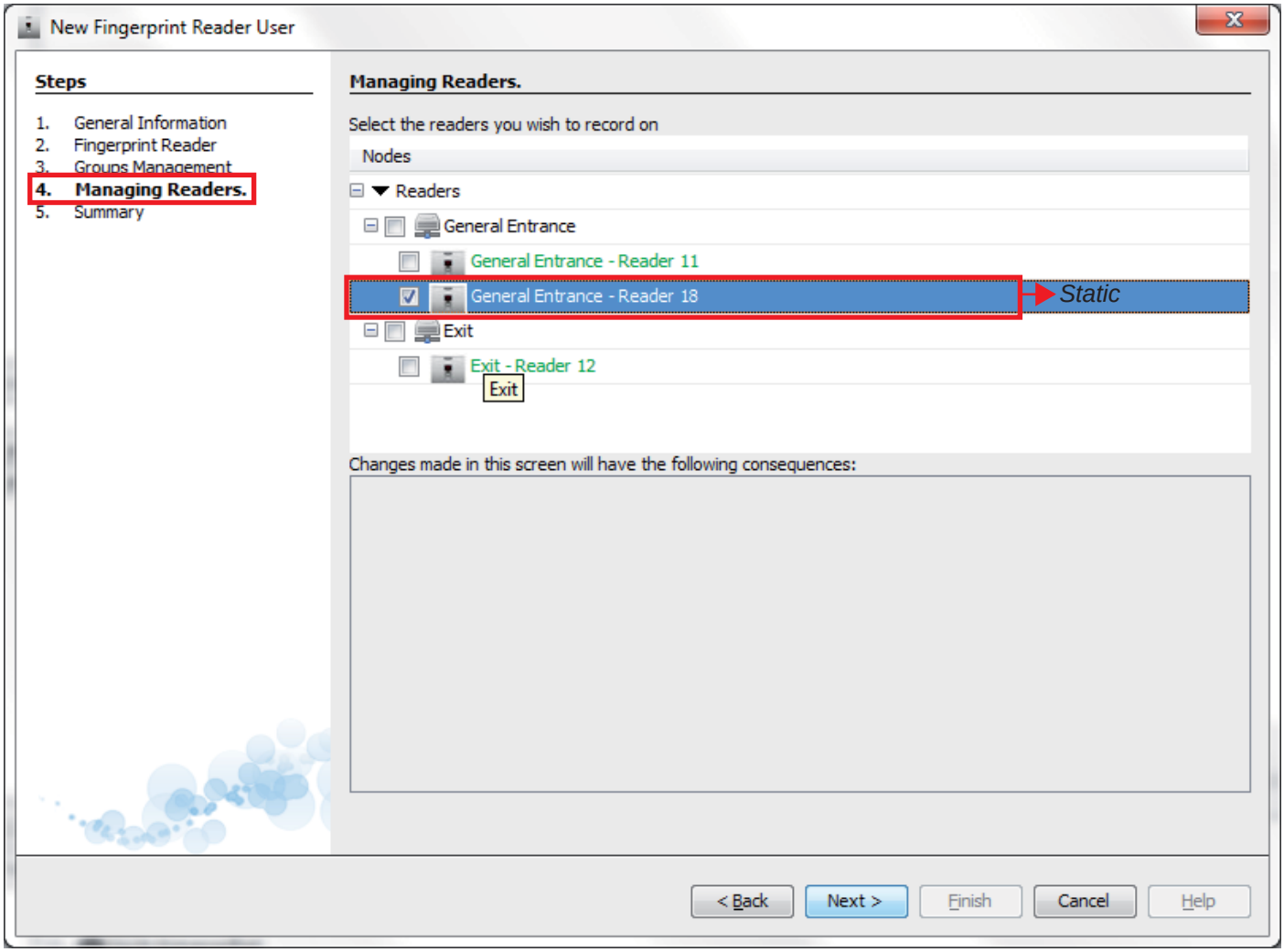
4. Manage Readers - assign users

On this screen you make the direct assignments (without groups), amongst users and readers.
The readers **in green** are readers in which **the user is already assigned via a group.**
Those in**black**, are those **not assigned to a reader via groups**.
You can have a user assigned to a reader via a group and then make a direct assignment.

Therefore, once we have assigned the user´s biometric information or proximity card, we must select the readers we want the user to have access to. This can be assigned in two ways:

- **static:** assigning each of the installation´s readers, **(4. Manage readers)**.
  or
- **dynamic:** assigning the user to a group through a "profile," which can be modified later on if the system´s access policies change or the readers to be accessed by a type of users change **(3. Manage groups,** previous page**)**.

Note: the screen Manage Readers, ***is only shown if groups have been registered in the application.*** *See chapters "Add reader" and "Detecting readers" for more information.*



5. Summary - Enable/Disable direct entering of a user

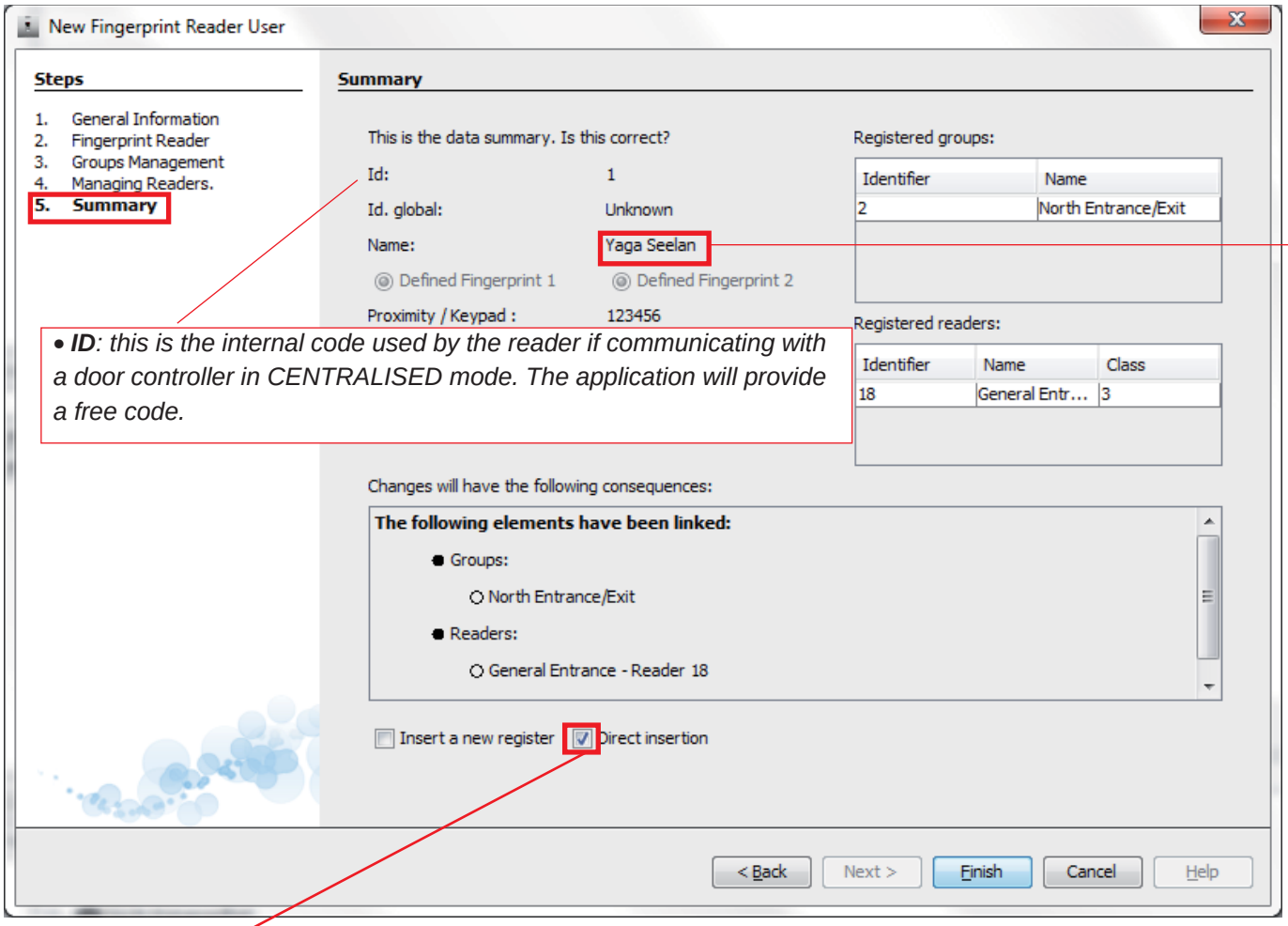
On this screen you can see the changes made to user links and unlinks to groups and readers. We get a summary before trying to save them to the user´s database.

Depending on if **registering or changing a user**, this screen displays some of **the selected fields**. As options we can enable the direct insertion of the user in the selected readers, or continue performing user registrations and delay this insertion in the readers until later on.

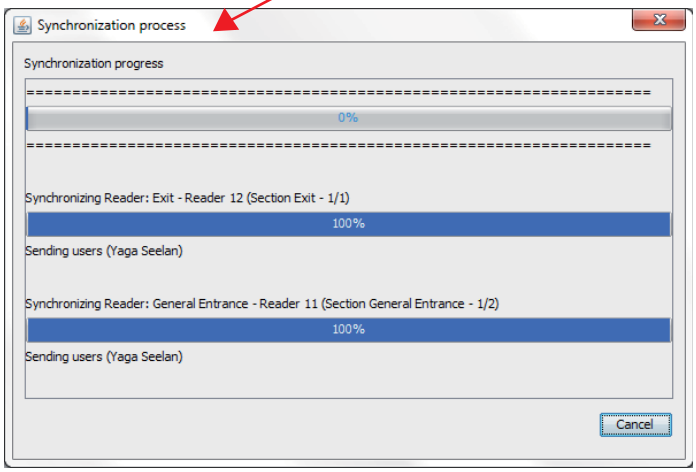
- **Insert a new register:** When the assistant finishes inserting the user, it restarts in order to register another user.
- **Direct insertion:** When the assistant finishes, the synchronisation process starts to apply the changes to the readers and users.

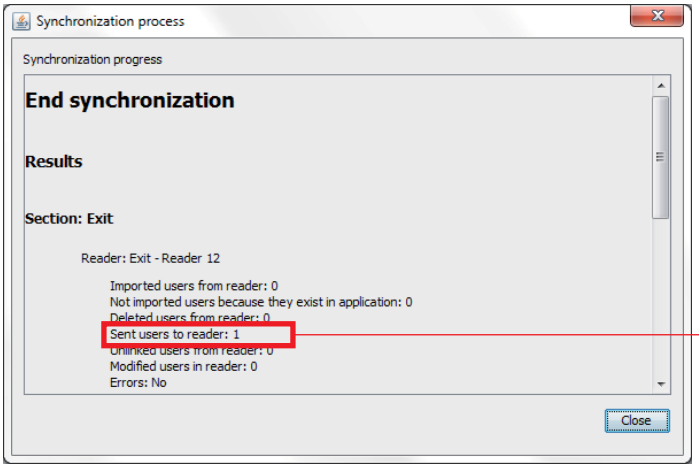
Note: we must keep in mind that the insertion operation may be slow if there are many assigned readers.

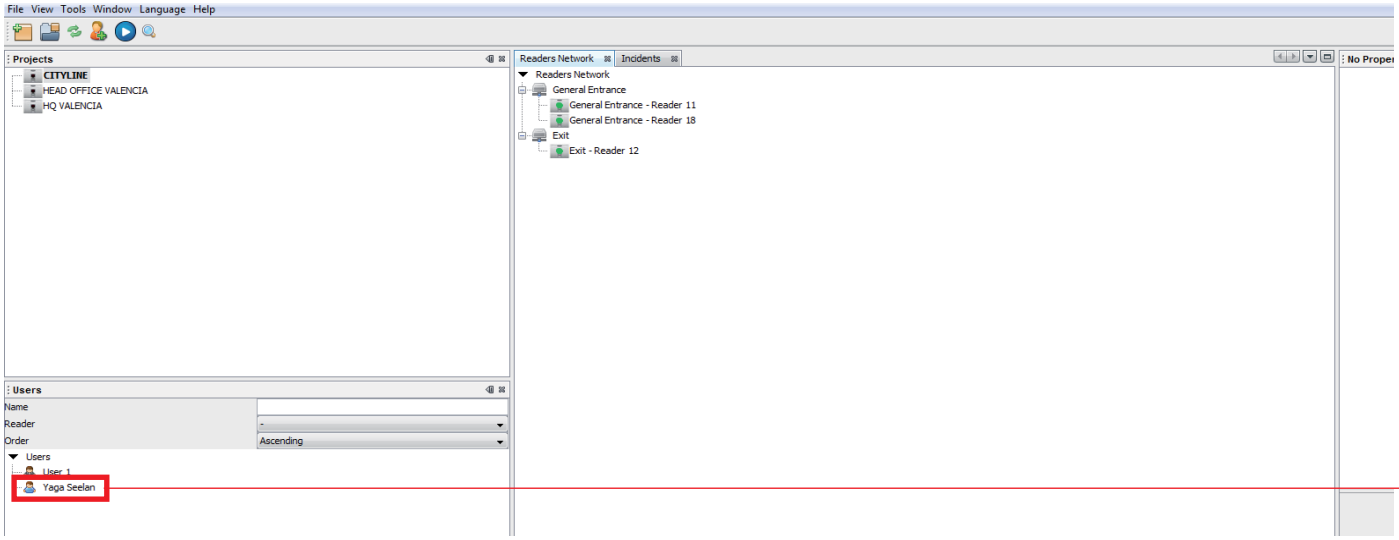
Summary of **Insertion**



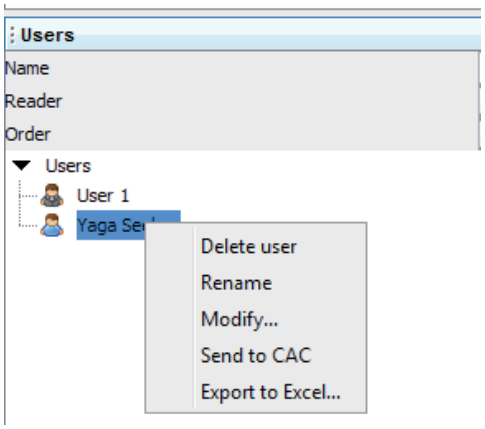
• ***ID***: *this is the internal code used by the reader if communicating with a door controller in CENTRALISED mode. The application will provide a free code.*

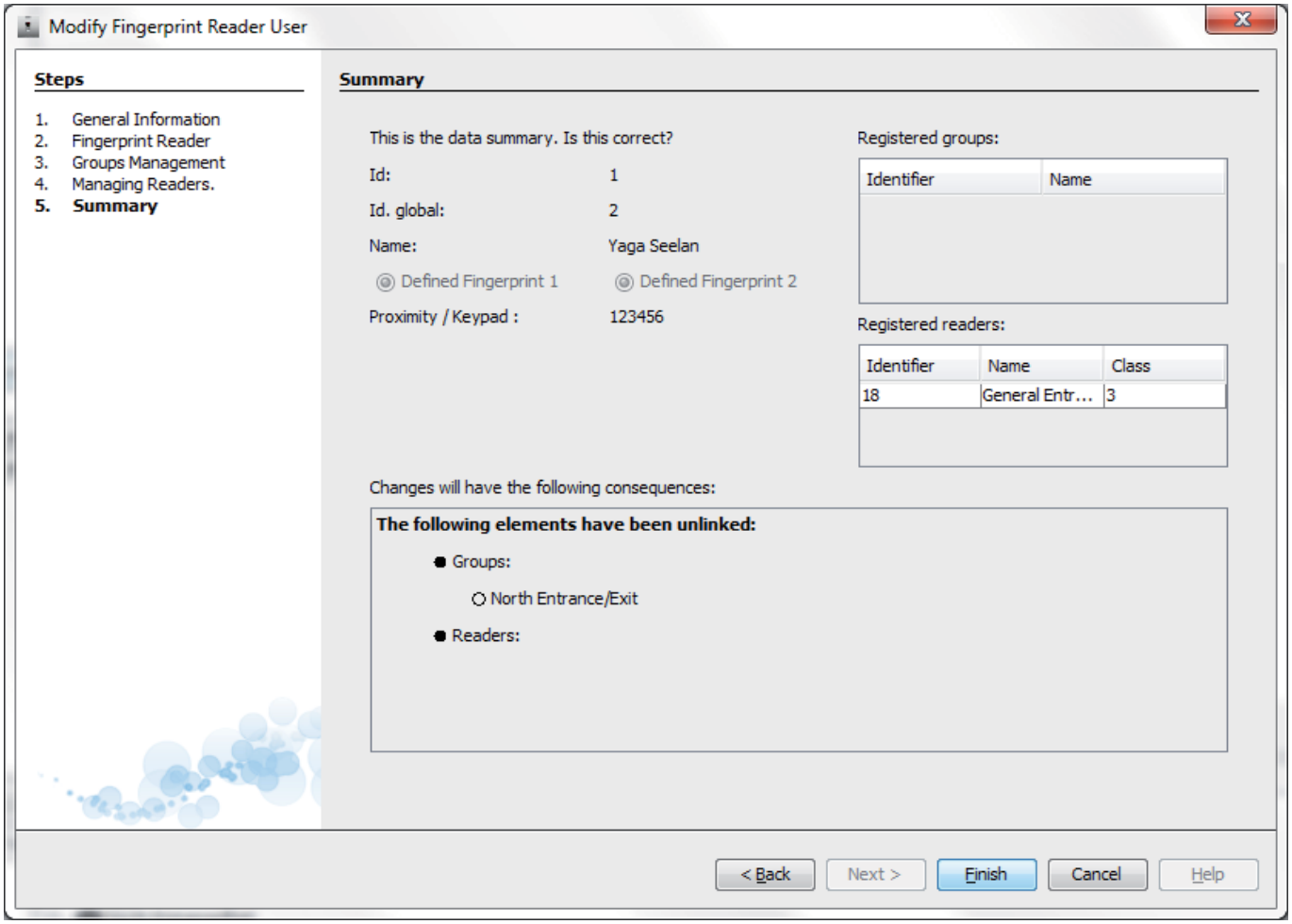






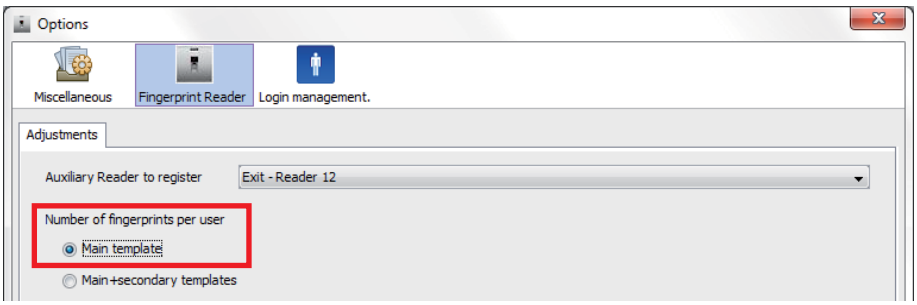
Summary of **Modifications**



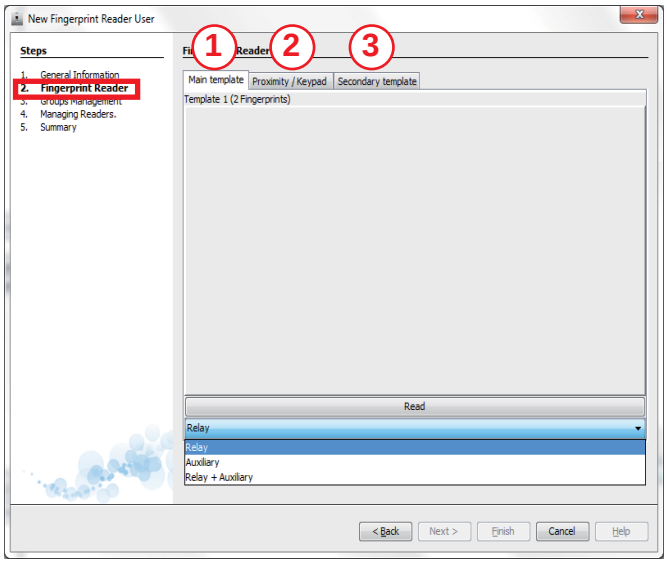


*Note: depending on if **registering or changing a user**, this screen displays the "Summary" of some of **the selected fields**.*

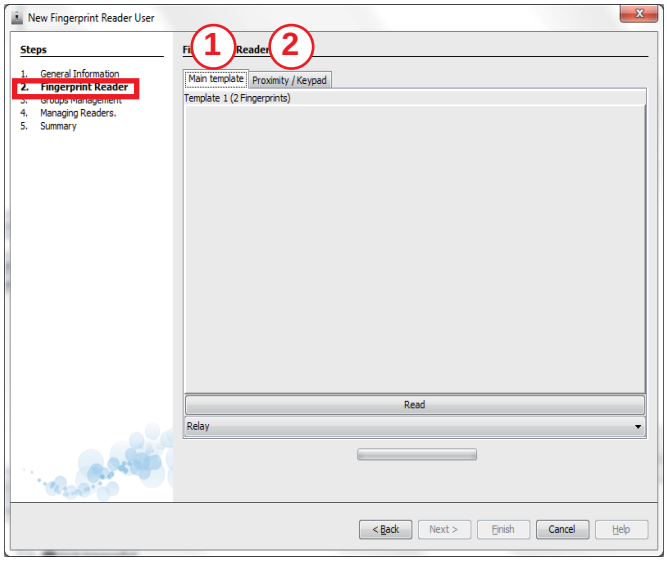
The sequence to CREATE a user with a Main fingerprint template:



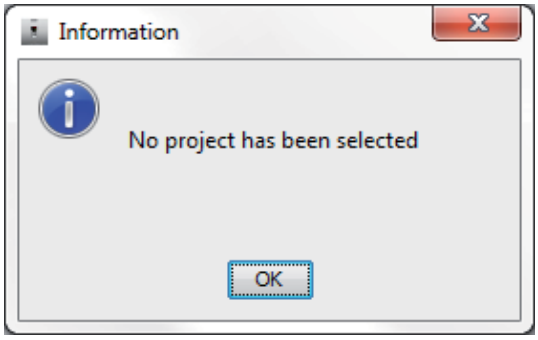
Once having selected the **main fingerprint** from: *Tools/Options,* the steps to take are the same as explained in the template example for **the Main + secondary template.** The only difference is that**the secondary fingerprint tab does not appear (3).**



Screen with the **main fingerprint** tab

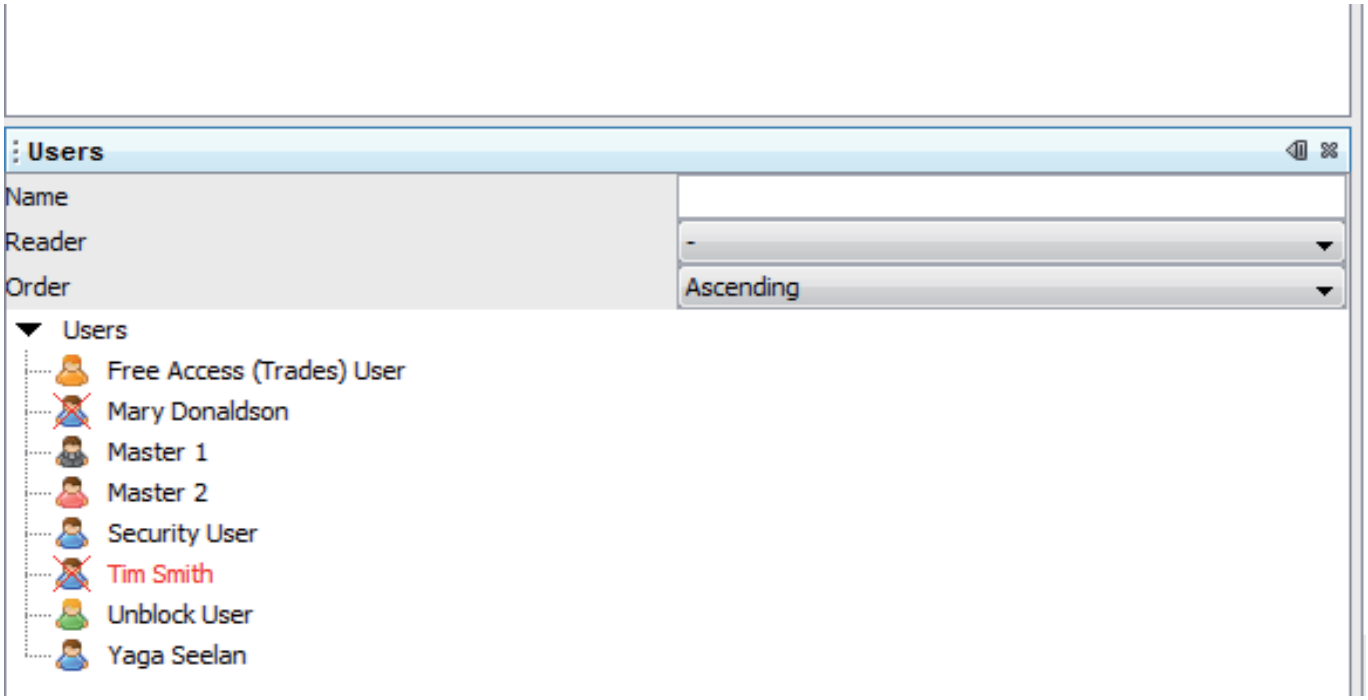


Note: from the New User Option you can create a user within the project that is opened as explained in this chapter, but if there is no open project a warning screen appears indicating that there is no project open.



User area in the main screen

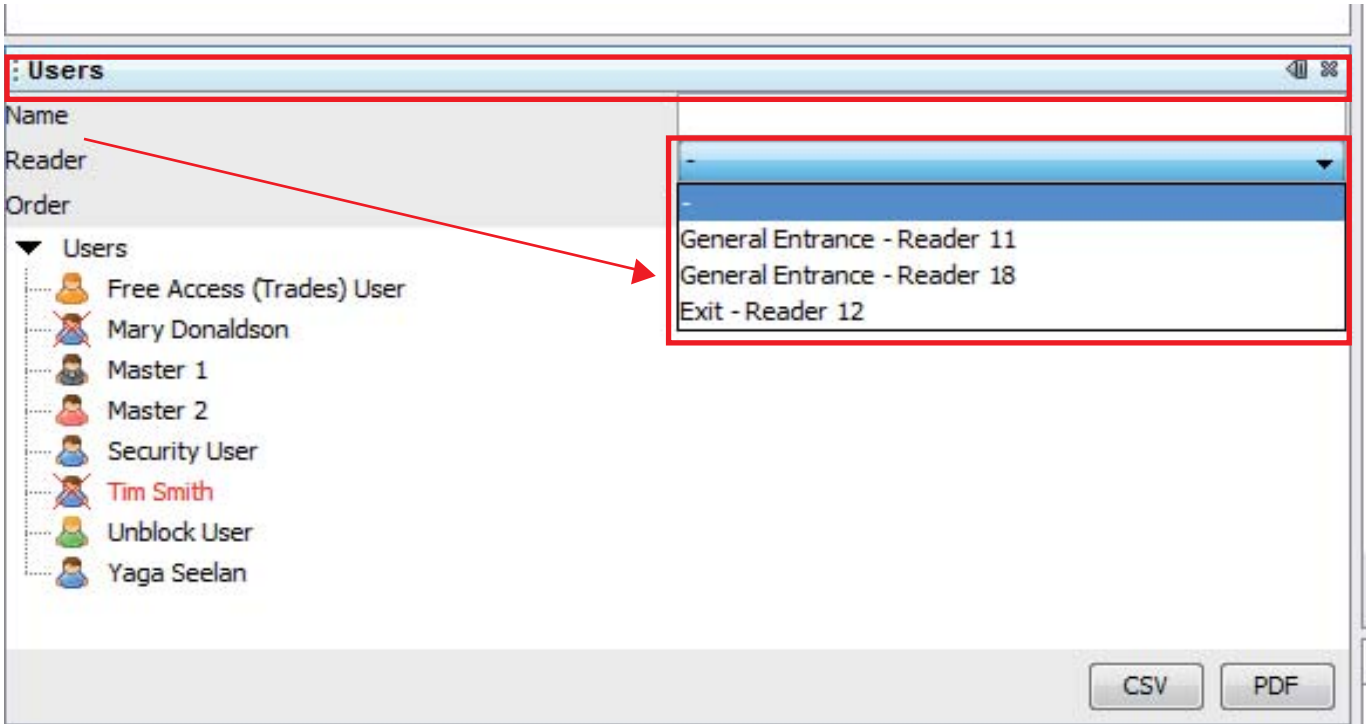
This one has the users assigned to the readers. The users may be registered from the application or from the readers upon synchronisation, (see the corresponding chapters).

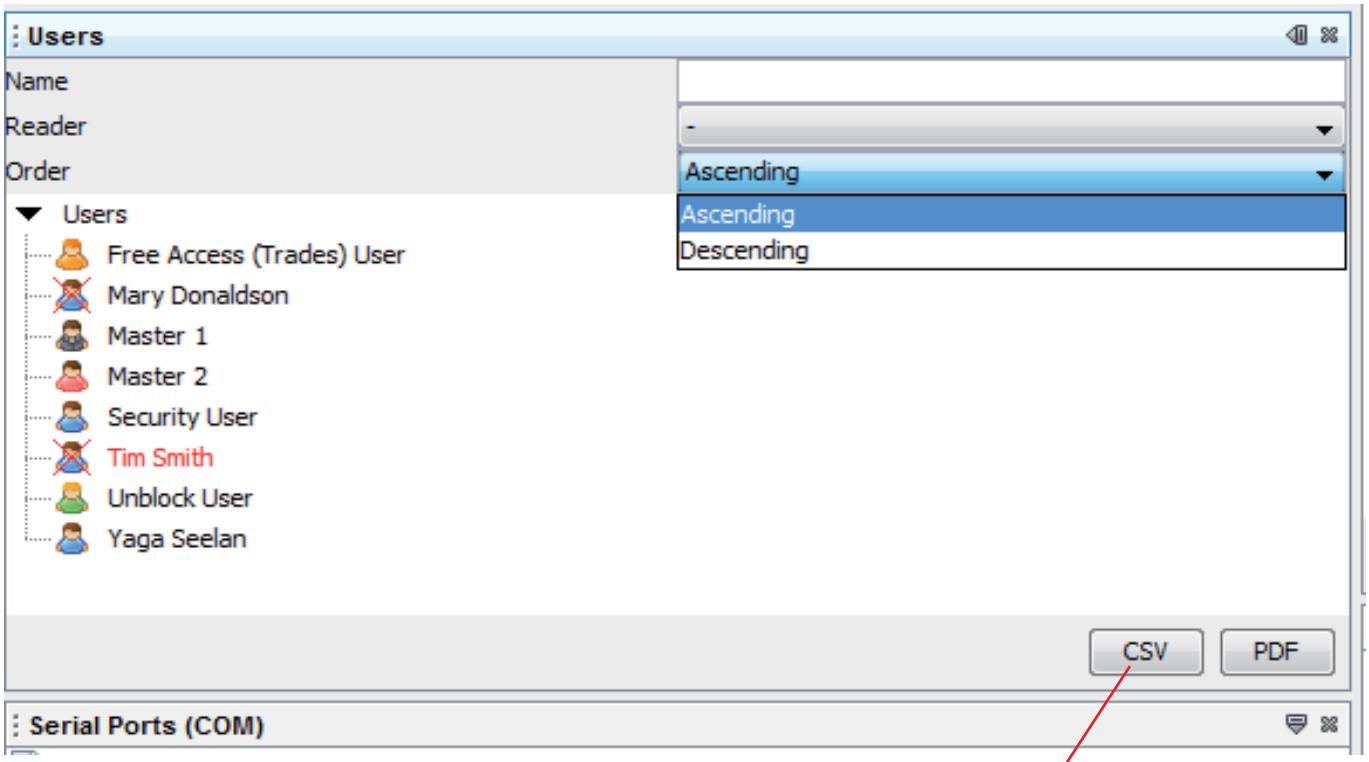


From this area we can filter the users to view here.
The users can be filtered by:

- Name
- Reader
- Both

And they can be sorted by name in ascending or descending order.





Send to Wincom (WC+)

This option allows us to generate a CSV file compatible with WC+ to be imported.

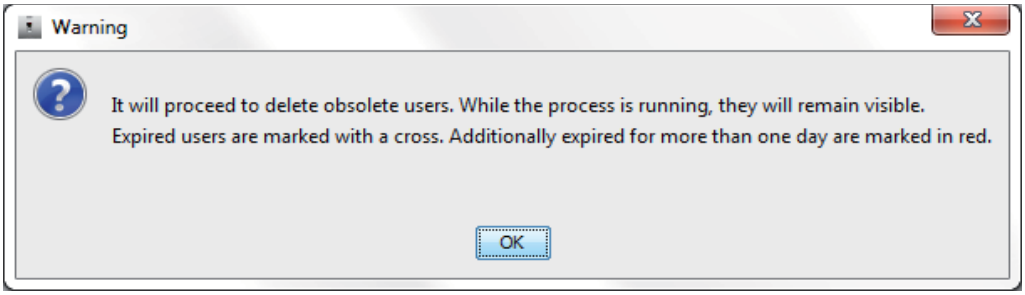
Graphic view of the types of Users

Depending on the type of user, this is represented differently:

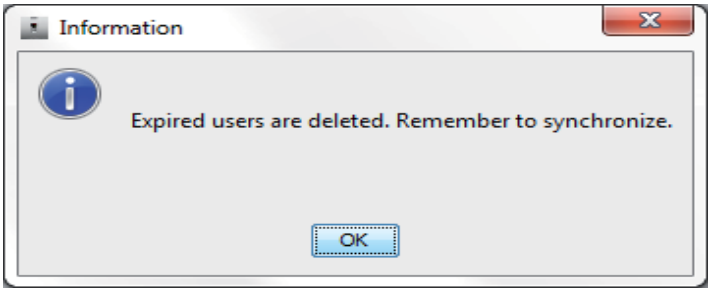
Representation	Type of user
	Free Access
	Expires today
	Unblock
	Expires in more than 1 day
	Master 1
	Master 2
	Security
	Normal User

Notes:

- every time you start the application and have a project open, or every time the project is loaded, if there are expired users or users about to expire, the following screen indicates it.



- Once the application has deleted the expired users, the following screen appears to remind them to synchronise.

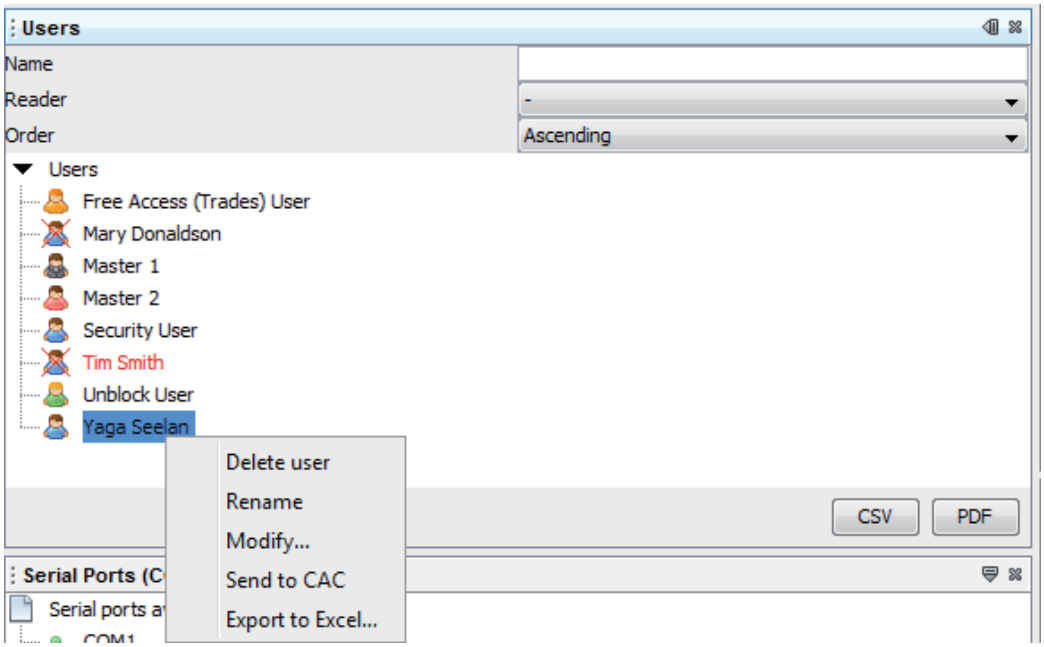


User Management

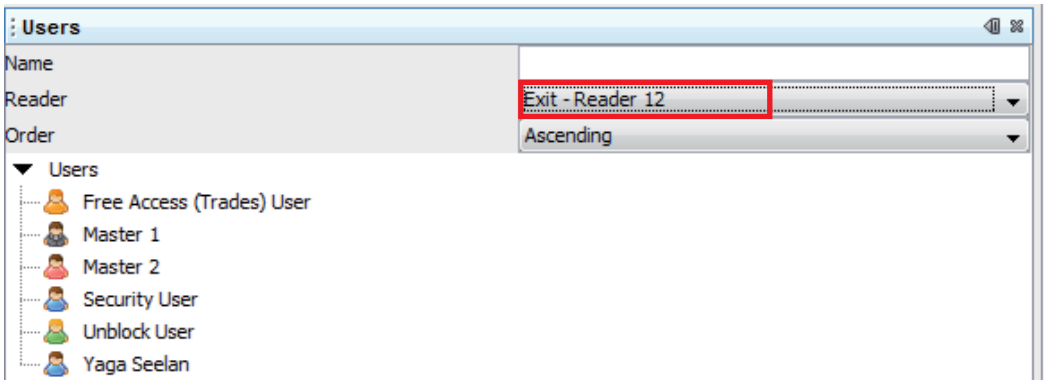
The panel of Users allows us to locate and consult the users we have registered in our project that are or are not saved in the readers.

Via contextual actions you can delete, rename or open user files to edit any other parameter.

- **Delete users**: action to delete user/users.
- **Rename**: we can change the user name.
- **Change**: to edit user parameters.
- **Send to CAC (AC Plus)**: send the selected users to the AC Plus system.
- **Export to Excel**: sending the selected users to a CSV file compatible with WC+ to be imported.

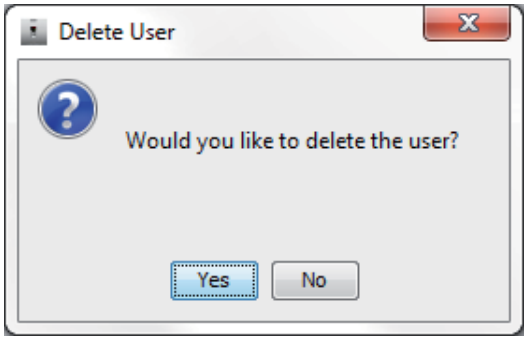


Selecting a reader, you can check which users are registered.



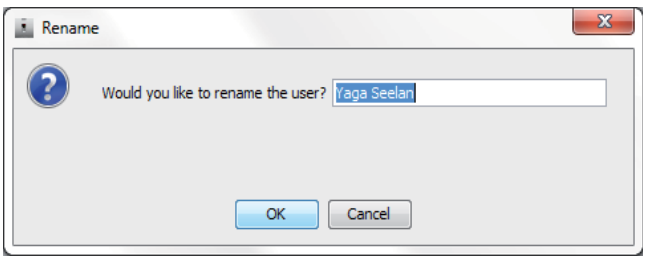
Delete

This option allows us to delete the user, for this it launches the following screen to delete users.



Rename

This option allows us to change the user´s name, for this it launches the following screen to rename users.



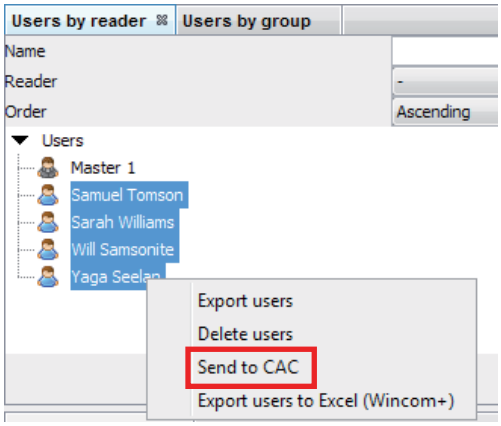
Modify

This option allowsyou to edit user parameters. See the chapter "Description Register user / Change user."

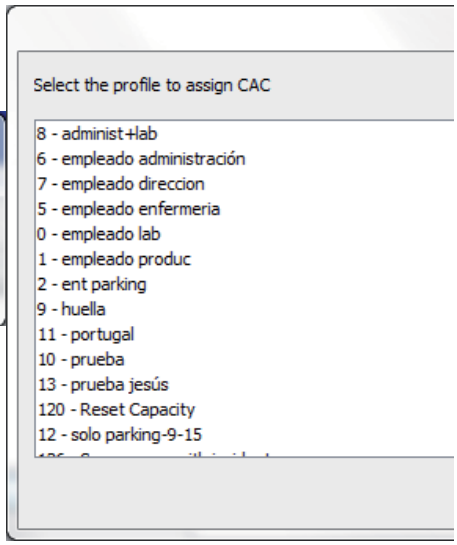
Send to AC Plus

Having properly configured the AC Plus server adjustments, this action allows us to send the selected users to the AC Plus system. We will be asked for the existing profile to assign. First you must select the available AC Plus version in the computer: V1.x or V2.x or greater, on the indicated screen.

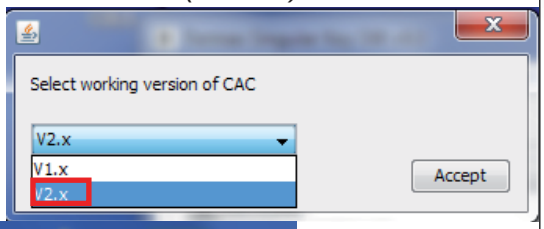
Once the users are set up on the CENTRALISED Readers, they should be updated on the centralised AC Plus Access software. The AC Plus application must be run.



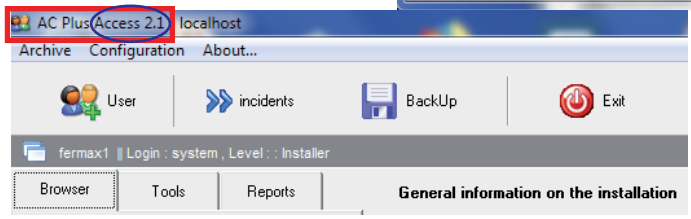
Screen to select the existing profile to assign.



Screen for selecting the available CAC (AC Plus) version.



The AC Plus version may be viewed in the program bar.



Export to excel

This option allows us to generate an excel file compatible with WC+ to be imported.

Link users to the reader

In order to register Users in the Readers, just perform a simple drag and drop on the readers you wish to register. This way users are associated to the reader (linked).

Note:

- *see chapters GROUPS and SYNCHRONISATION as alternative options.*
- *We must keep in mind that the insertion operation may be slow if there is a high number of assigned readers.*

GROUPS

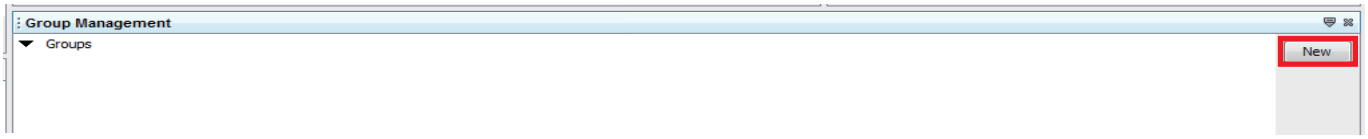
Description

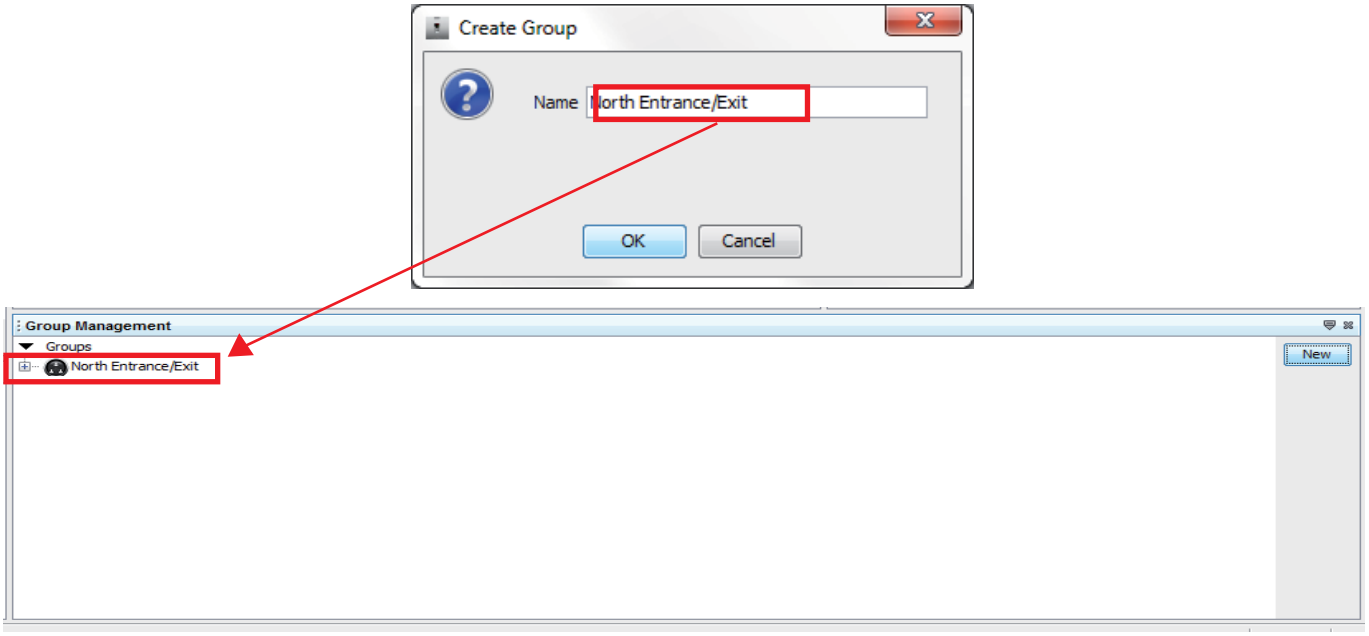
Using groups is a dynamic way of assigning which readers a user will have access to.

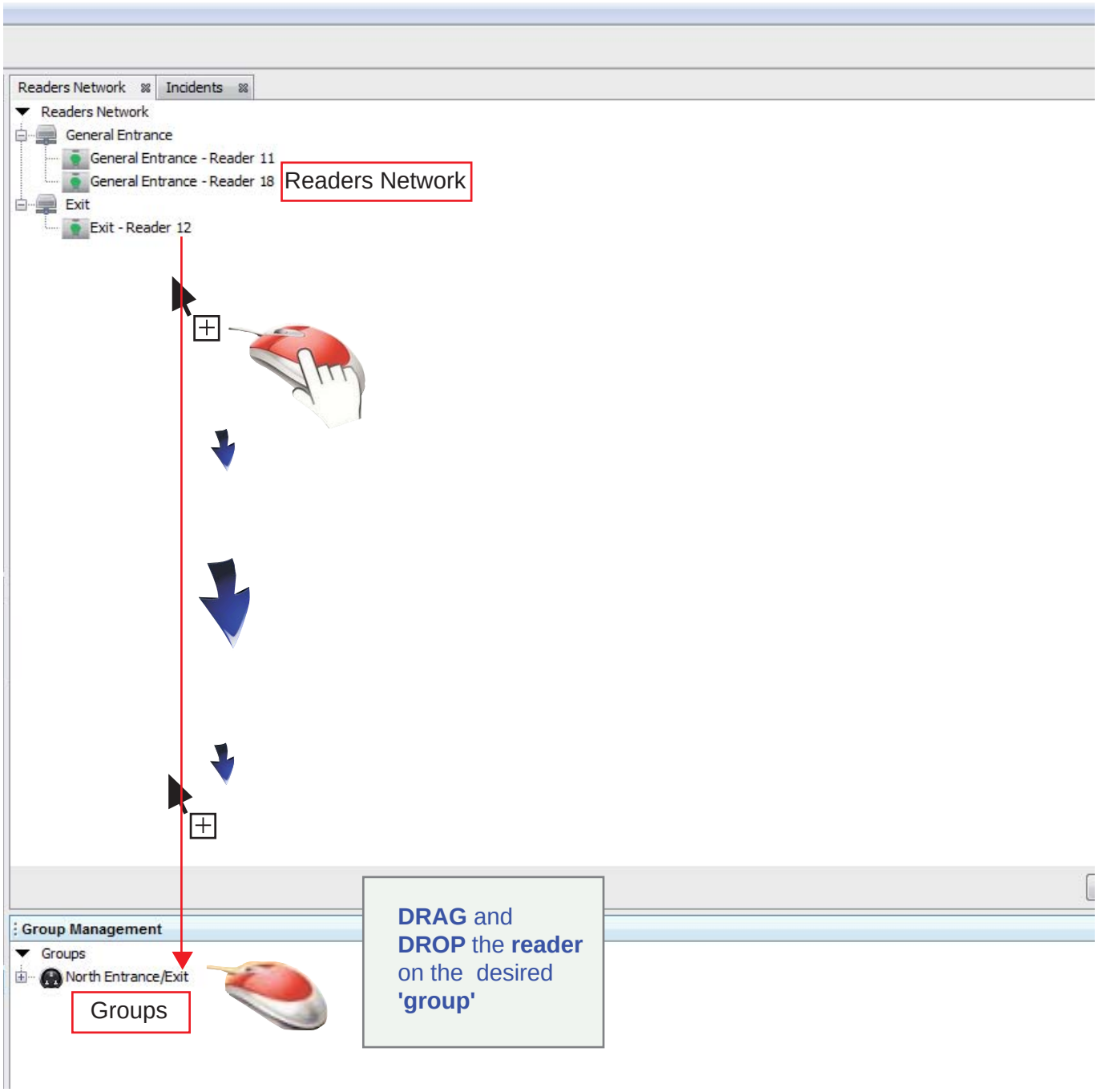
A group is a collection of readers. There is no limitation for this, so you can define groups with repeated readers, with the list of readers for a specific user as the sum of all the different readers.

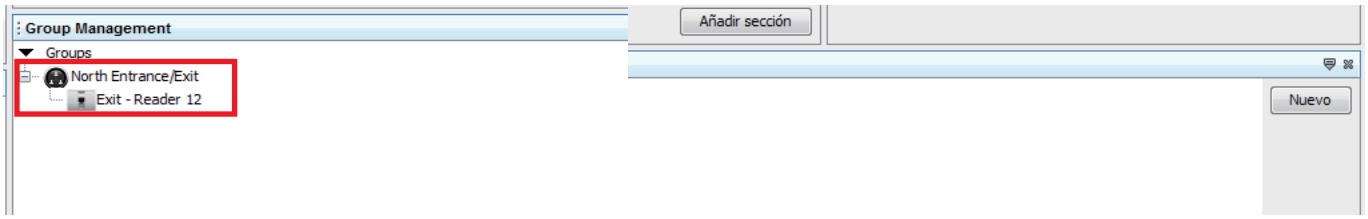
In order to add a group, just drag it over the desired group node. Deleting a reader from a group is done in the contextual action "delete from the group."

This screen is in charge of creating, changing and managing groups.

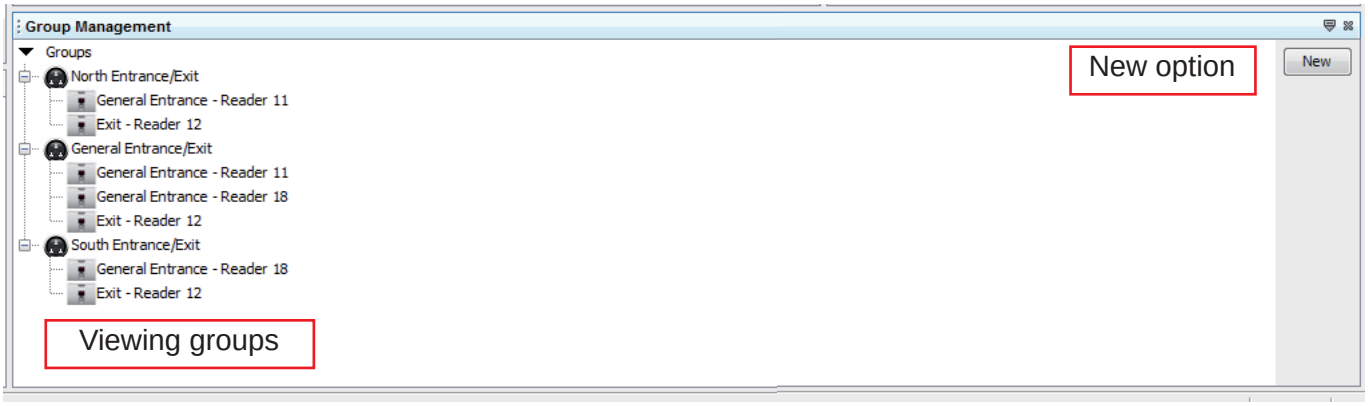



Create Group
Name
North Entrance/Exit
OK
Cancel
Group Management
Groups
North Entrance/Exit
New


Readers Network
Incidents
Readers Network
General Entrance
General Entrance - Reader 11
General Entrance - Reader 18
Exit
Exit - Reader 12
Readers Network
Group Management
Groups
North Entrance/Exit
Groups
DRAG and DROP the reader on the desired 'group'



The groups screen is divided into zones:



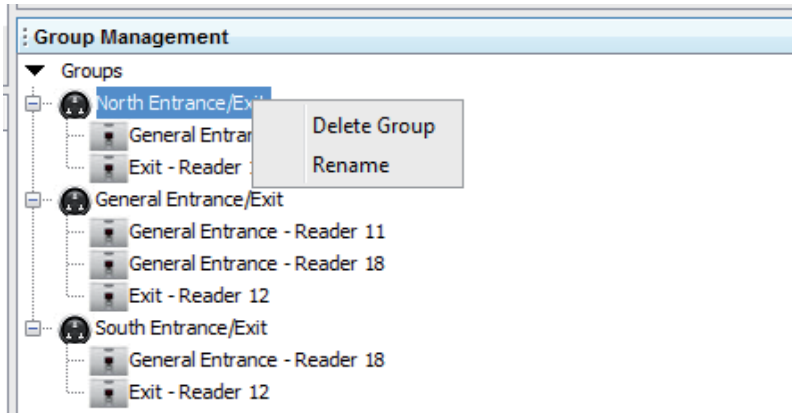
Viewing Groups

From this zone we can view and manage groups.

New Option

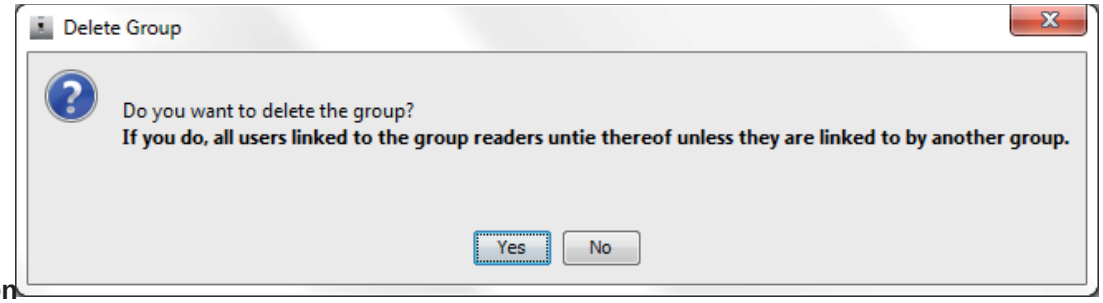
From this option we can create new groups, just as is explained in the previous page.

Group options. Available actions:



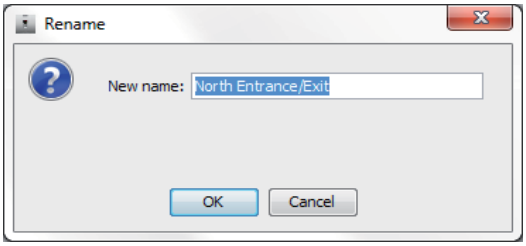
Delete Group

This option deletes the group from the application.

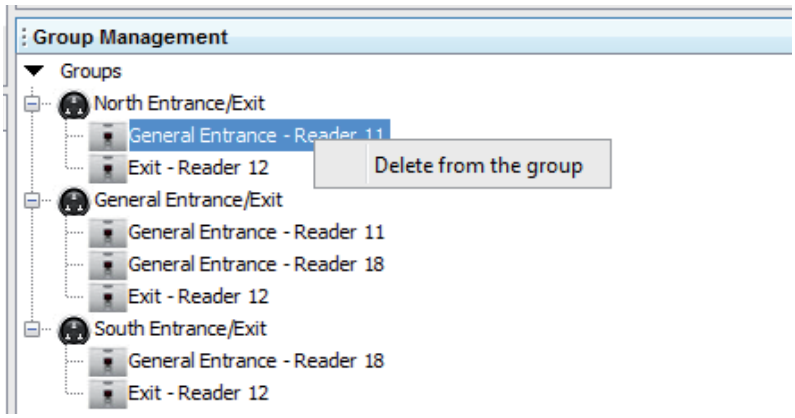


New Option

This option changes the group name. For this a dialogue box appears to be able to change the name.

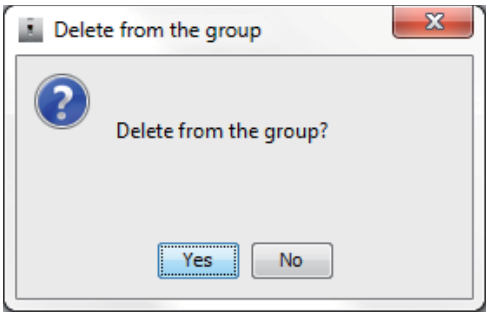


Options on an element in the group. Available actions:



Delete from the group

This option unlinks the selected reader from the group it belongs to. Before performing the action is shows us a confirmation screen.



SYNCHRONISATION

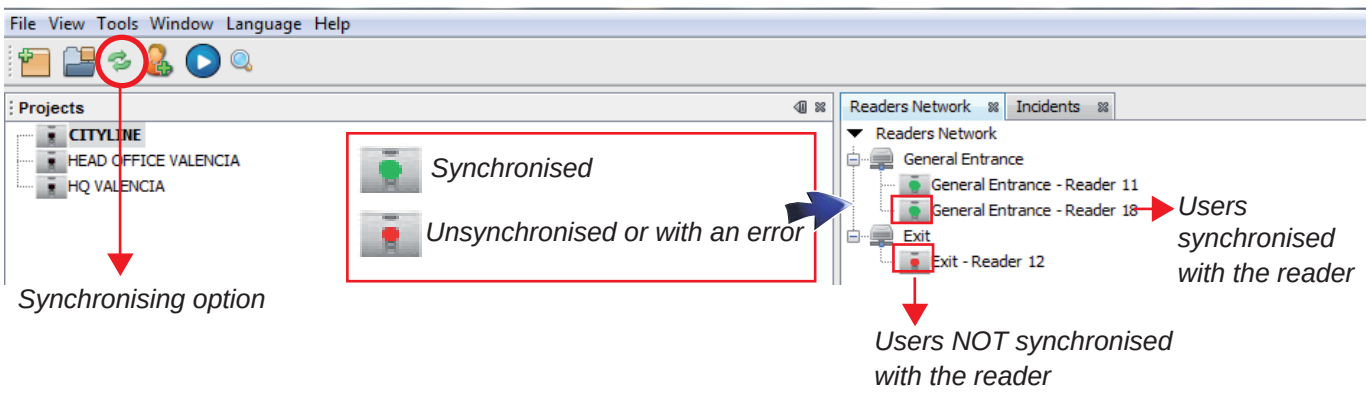
Description

You must synchronise since the following situations may occur, or the direct entering of users has been done correctly, or that changes have been made (deletions, new registrations, etc..) both in readers and the PC´s software, and it is also possible that some changes had been made and the readers were not physically connected at that time. In order to resolve all these situation, you must synchronise.

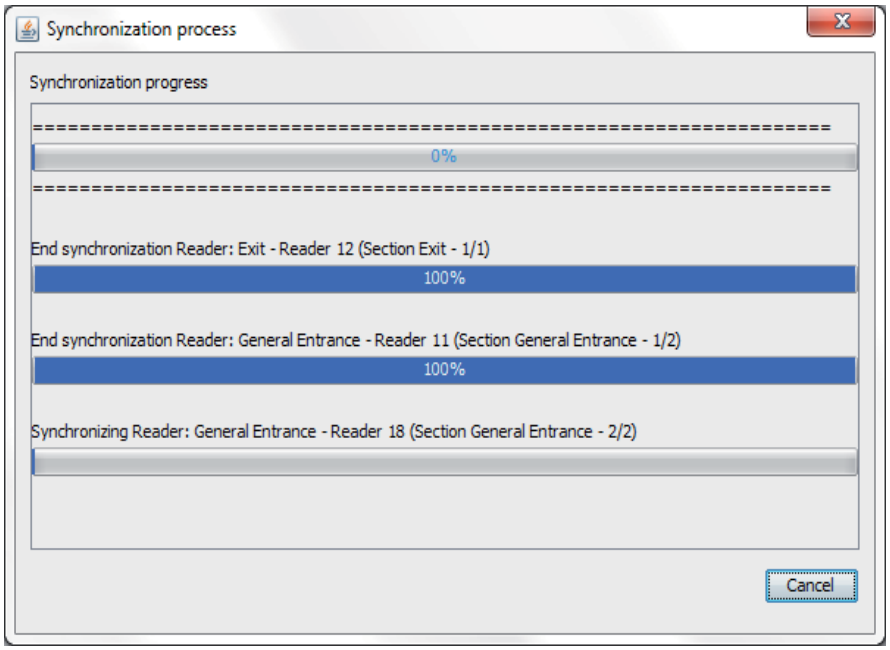
During the synchronisation various operations are performed:

- importing local users that have been registered manually to the readers (via the control pad).
- Global deletion of users in the readers that no longer figure in the software´s project, either from being deleted or because they have been disassociated to said readers.
- Entering global users in the project that must still be entered into the readers.

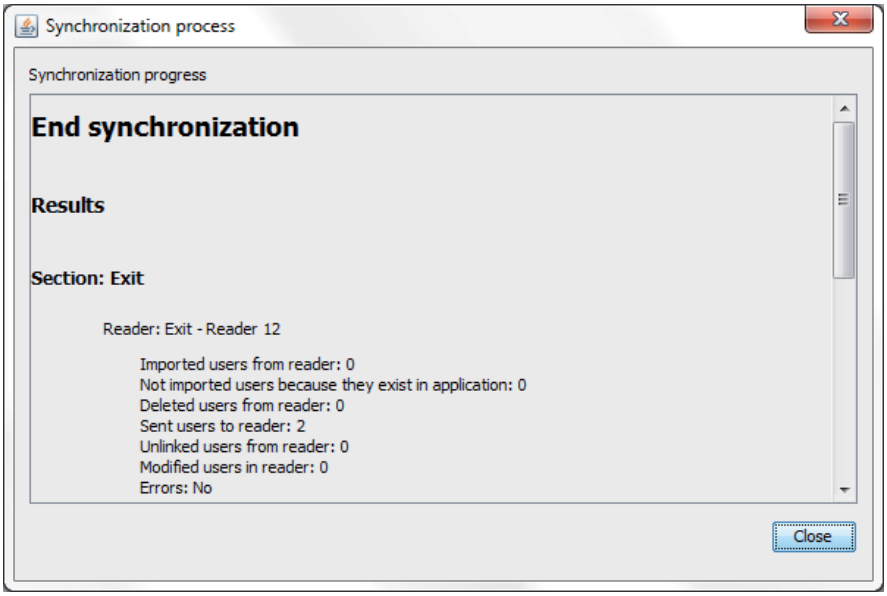
This can be detected by looking at the colour (red) in which the system´s reader´s appear. Whenever this situation occurs, we must use the Synchronisation iconlocated in the tool menu, (independently of autonomous or centralised readers).

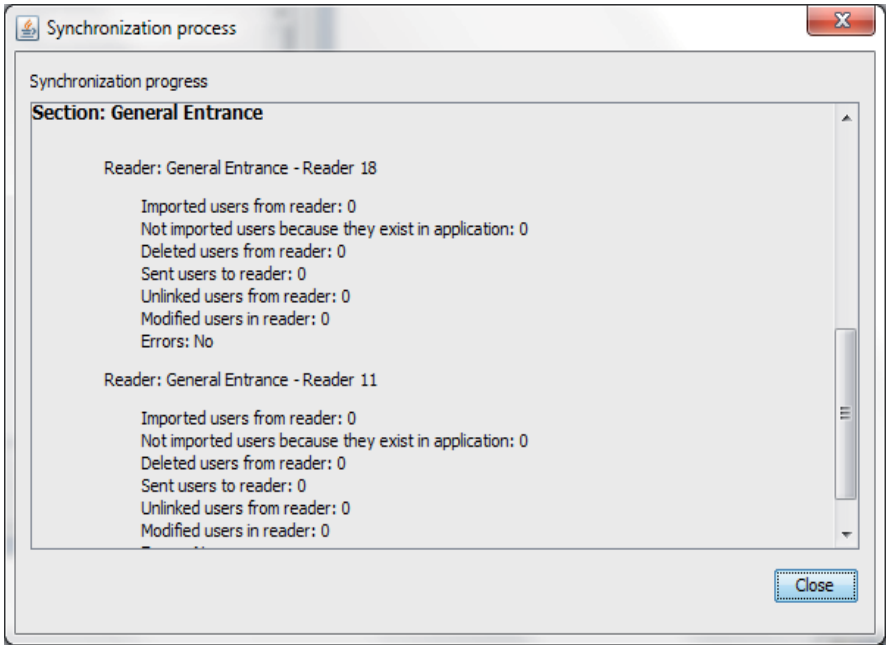


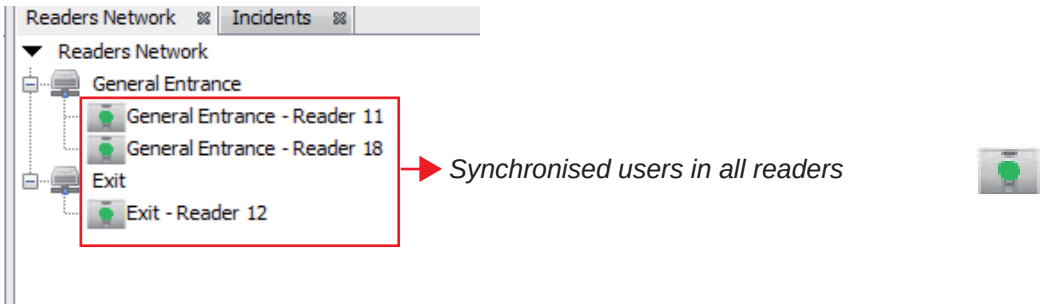
During this synchronisation process this screen appears, which indicates the reader being synchronised and the operation being performed.



Upon completing the synchronisation process, whether because it has finished or you have pressed *Cancel*, a summary of the synchronisation is displayed.







INCIDENTS

Description

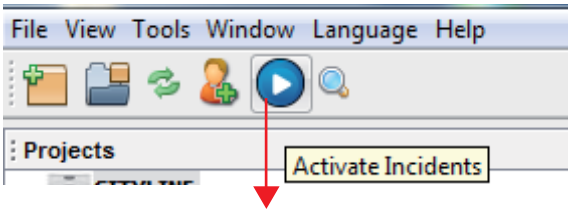
All information on the events produced in the readers configured as AUTONOMOUS can be recorded.

The activation/deactivation in all readers with this capacity is done via the icon on the tool bar.

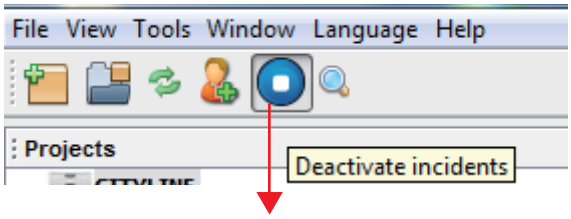
The user must have the permission to access this feature. See the corresponding chapter on: "Managing Logins" (permissions).

Incidents are shown in descending order from the time they were generated. You can filter incidents shown by type, origin, user and/or code that has generated them by using the components located on the upper part of the list.

Note: there is also the option of exporting or printing these incidents to other formats.

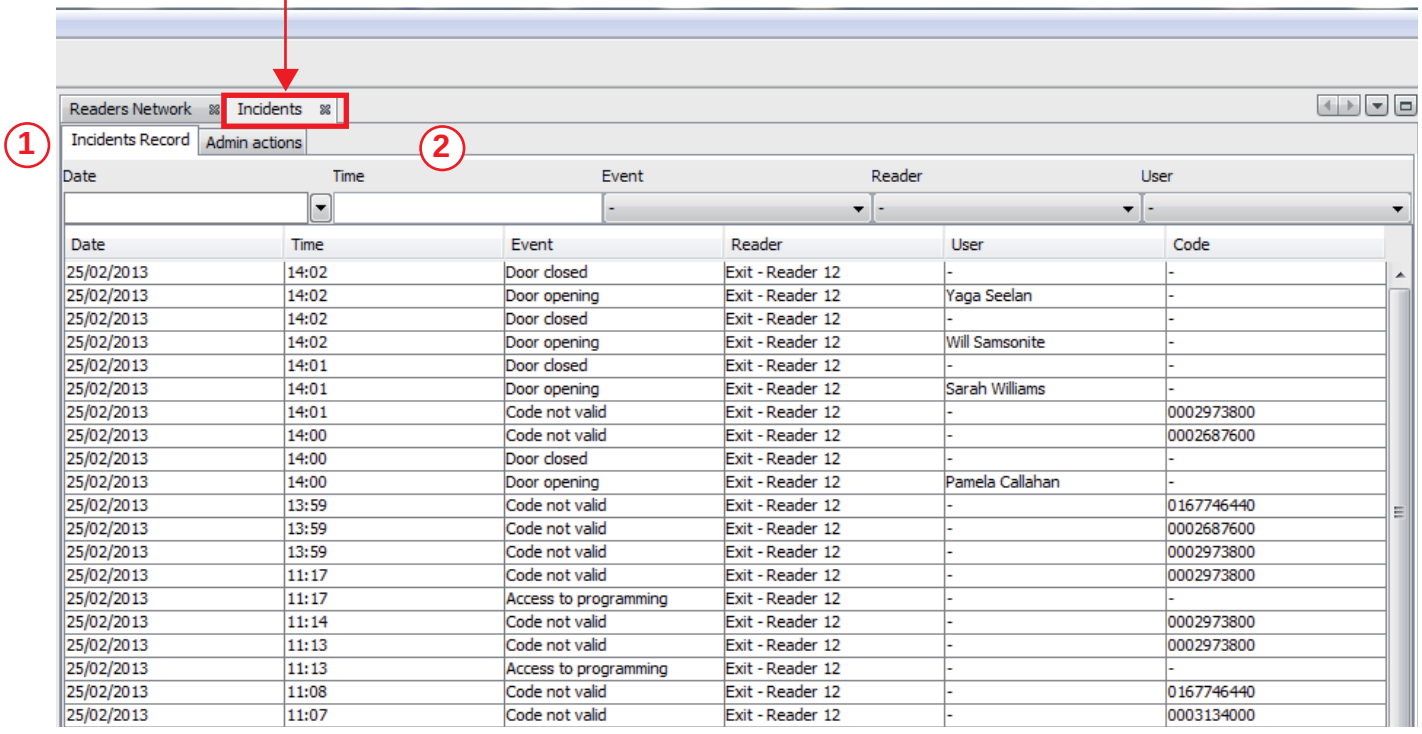


Press to activate incidents



Press to deactivate incidents

Selecting Incidents

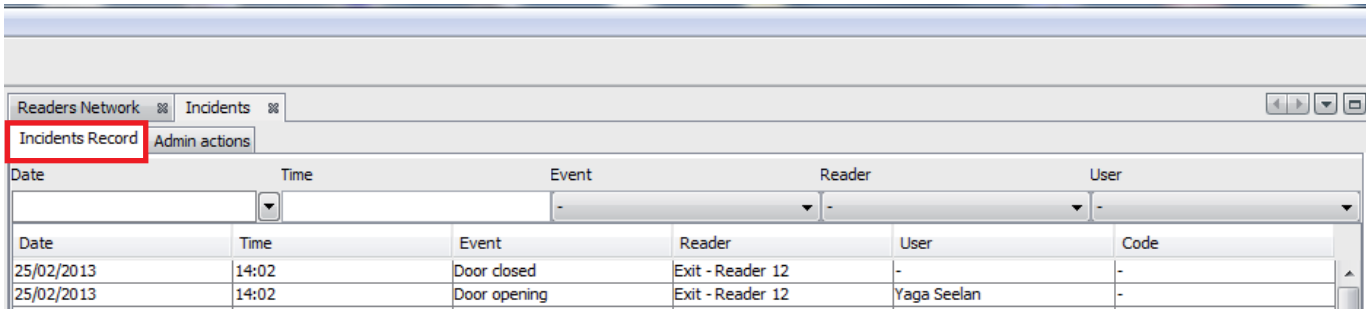


Date	Time	Event	Reader	User	Code
25/02/2013	14:02	Door closed	Exit - Reader 12	-	-
25/02/2013	14:02	Door opening	Exit - Reader 12	Yaga Seelan	-
25/02/2013	14:02	Door closed	Exit - Reader 12	-	-
25/02/2013	14:02	Door opening	Exit - Reader 12	Will Samsonite	-
25/02/2013	14:01	Door closed	Exit - Reader 12	-	-
25/02/2013	14:01	Door opening	Exit - Reader 12	Sarah Williams	-
25/02/2013	14:01	Code not valid	Exit - Reader 12	-	0002973800
25/02/2013	14:00	Code not valid	Exit - Reader 12	-	0002687600
25/02/2013	14:00	Door closed	Exit - Reader 12	-	-
25/02/2013	14:00	Door opening	Exit - Reader 12	Pamela Callahan	-
25/02/2013	13:59	Code not valid	Exit - Reader 12	-	0167746440
25/02/2013	13:59	Code not valid	Exit - Reader 12	-	0002687600
25/02/2013	13:59	Code not valid	Exit - Reader 12	-	0002973800
25/02/2013	11:17	Code not valid	Exit - Reader 12	-	0002973800
25/02/2013	11:17	Access to programming	Exit - Reader 12	-	-
25/02/2013	11:14	Code not valid	Exit - Reader 12	-	0002973800
25/02/2013	11:13	Code not valid	Exit - Reader 12	-	0002973800
25/02/2013	11:13	Access to programming	Exit - Reader 12	-	-
25/02/2013	11:08	Code not valid	Exit - Reader 12	-	0167746440
25/02/2013	11:07	Code not valid	Exit - Reader 12	-	0003134000

This screen shows the incidents sent by the readers (1) and the actions performed by the administrators (2), there is a tab for each of these two options.

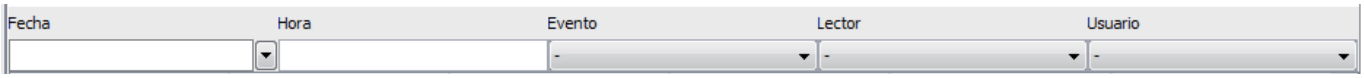
1. Incident record.

This screen contains the incidents reported by the readers to the application. The screen is divided in 3 zones:



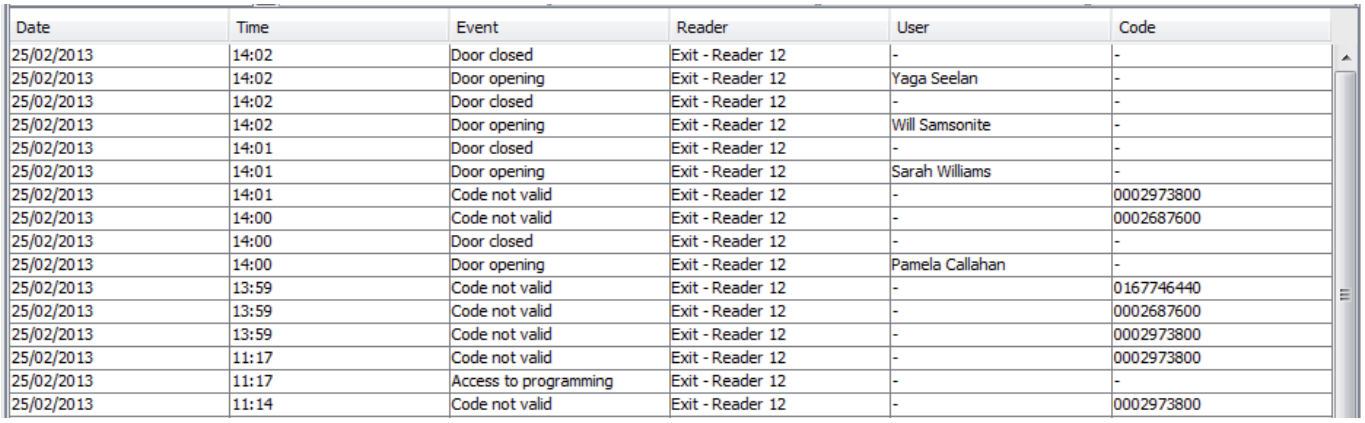
Filter

In this zone you can filter the data to view.



View information

In this one you can view the incidents reported by the readers.

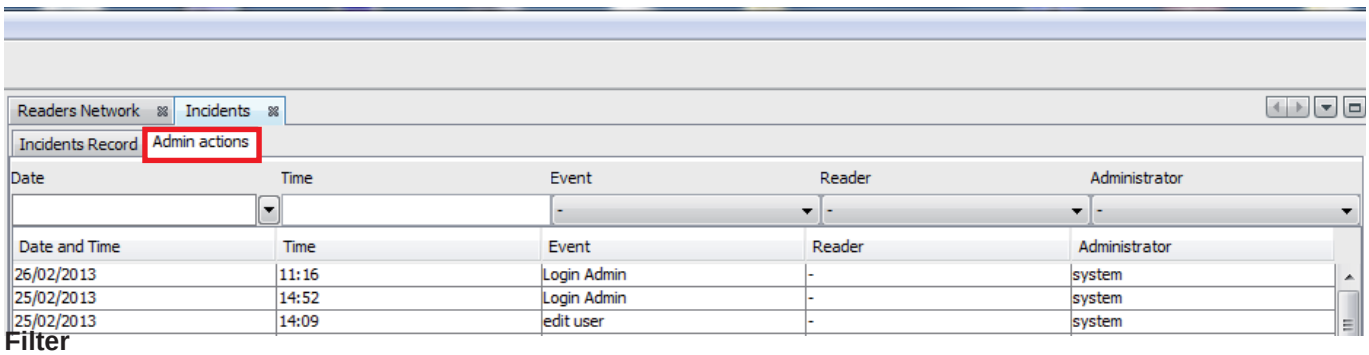


Exports

In this zone, depending on the button you press to export the data from the view zone to the desired format, from the possible ones on the software.

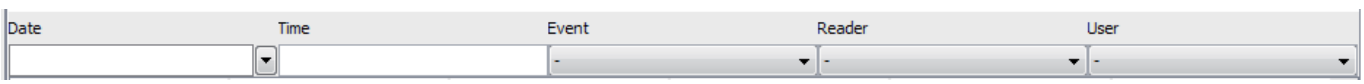
2. Administrative Actions.

This screen has the actions performed by the administrators (users that manage the application). Just like on the previous tab, the screen is divided into 3 zones:



Filter

In this zone you can filter the data to view.



View information

In this one you can view the actions performed by the administrators.

Date and Time	Time	Event	Reader	Administrator
26/02/2013	11:16	Login Admin	-	system
25/02/2013	14:52	Login Admin	-	system
25/02/2013	14:09	edit user	-	system
25/02/2013	14:09	edit user	-	system
25/02/2013	14:09	edit user	-	system
25/02/2013	14:09	edit user	-	system
25/02/2013	14:09	edit user	-	system
25/02/2013	14:09	edit user	-	system
25/02/2013	13:55	delete user	-	system
25/02/2013	13:51	edit user	-	system
25/02/2013	13:51	edit user	-	system
25/02/2013	13:51	edit user	-	system
25/02/2013	13:51	edit user	-	system
25/02/2013	13:51	edit user	-	system
25/02/2013	13:51	edit user	-	system
25/02/2013	13:51	edit user	-	system
25/02/2013	13:51	edit user	-	system
25/02/2013	13:51	create user	-	system
25/02/2013	13:50	create user	-	system

Exports

In this zone, depending on the button you press to export the data from the view zone to the desired format, from the possible ones on the software.

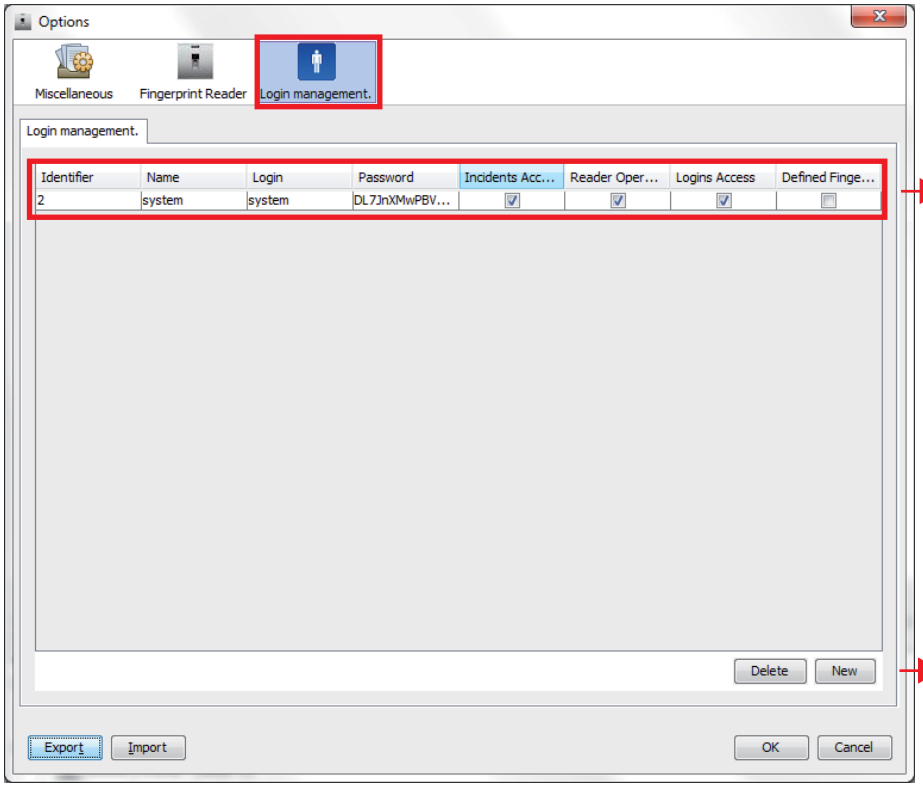
SECURITY

Description

From Tools-Options-Manage Logins you can define different types of logins (operators that use the application) with different types of permissions/roles:

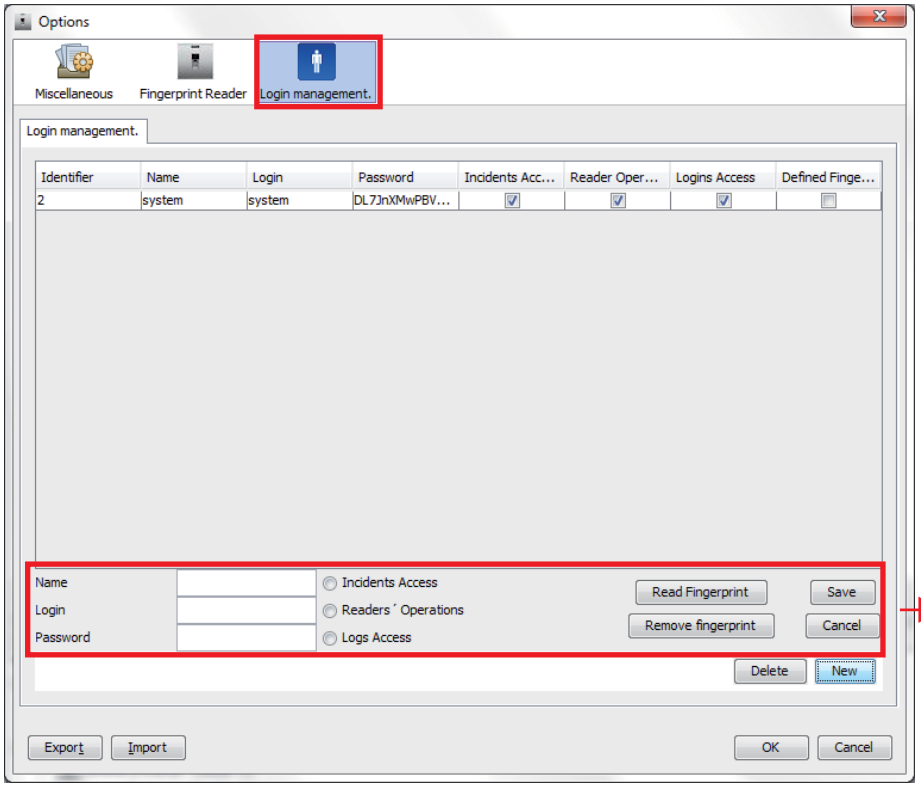
- **Access incidents**: this allows you to activate/deactivate the record and access the panel of incidents generated by the readers.
- **Reader Operations**: allows you to manage the readers, acting on the statuses, etc...
- **Logins Access**: this allows you to manage this panel

Without permission a user can NOT access the application.



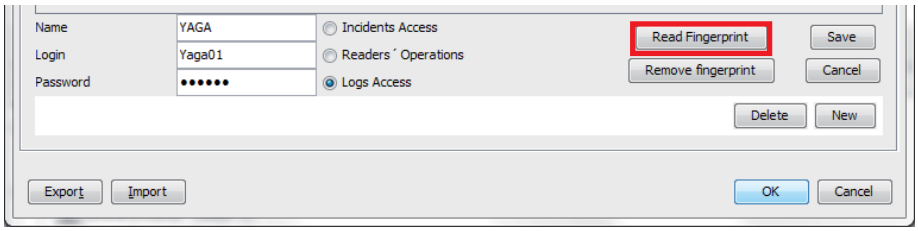
Default

Upon pressing "New" a zone on the screen appears to generate new logins

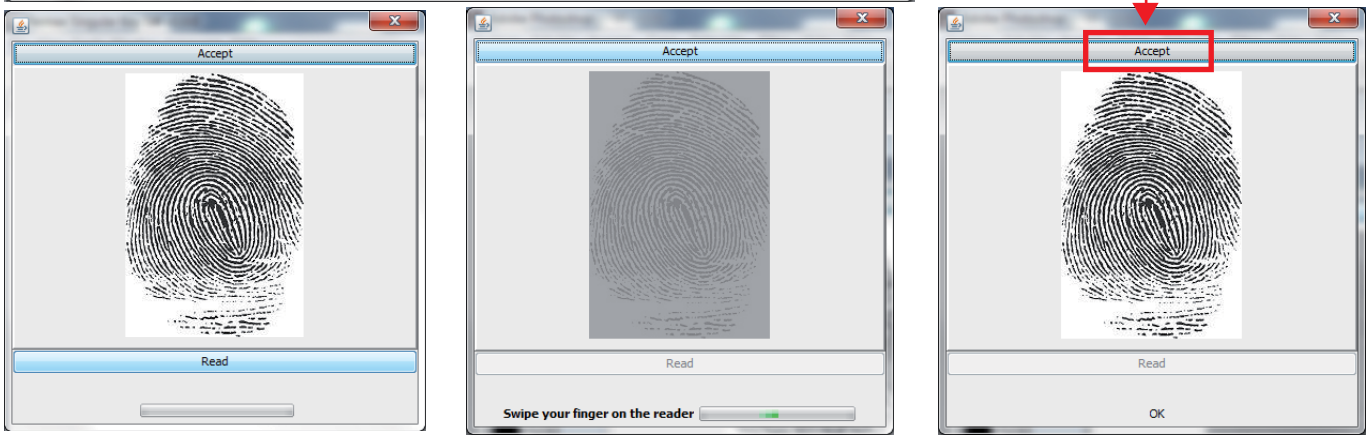


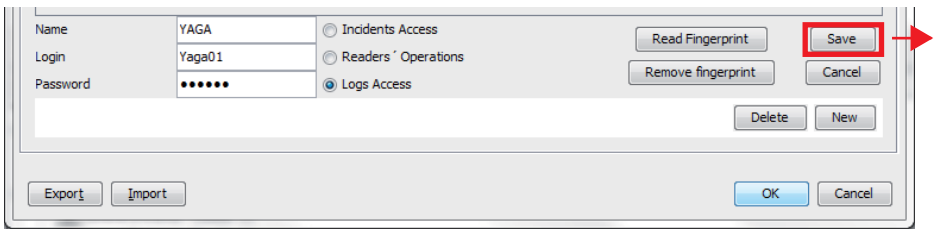
Data to fill-in to generate new logins

Note: we can use the operator´s fingerprint as an "alternative identifier." Then in the login form you don´t need to use the user and password, giving way to the fingerprint saved by the reader configured during registration. This fingerprint may coincide with another identical fingerprint stored by another reader in the system, since the identification is done in the PC.

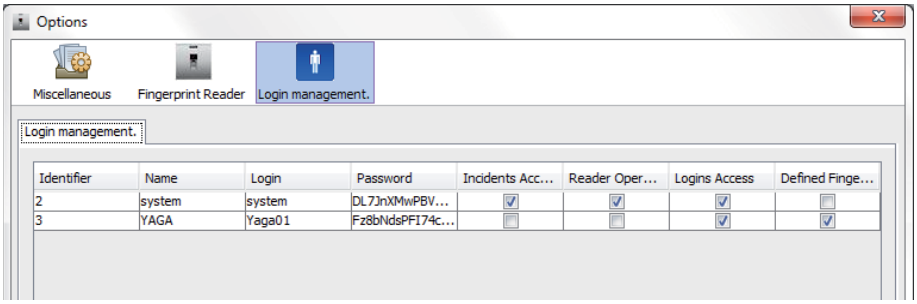


Press "Accept"





Press "Save"

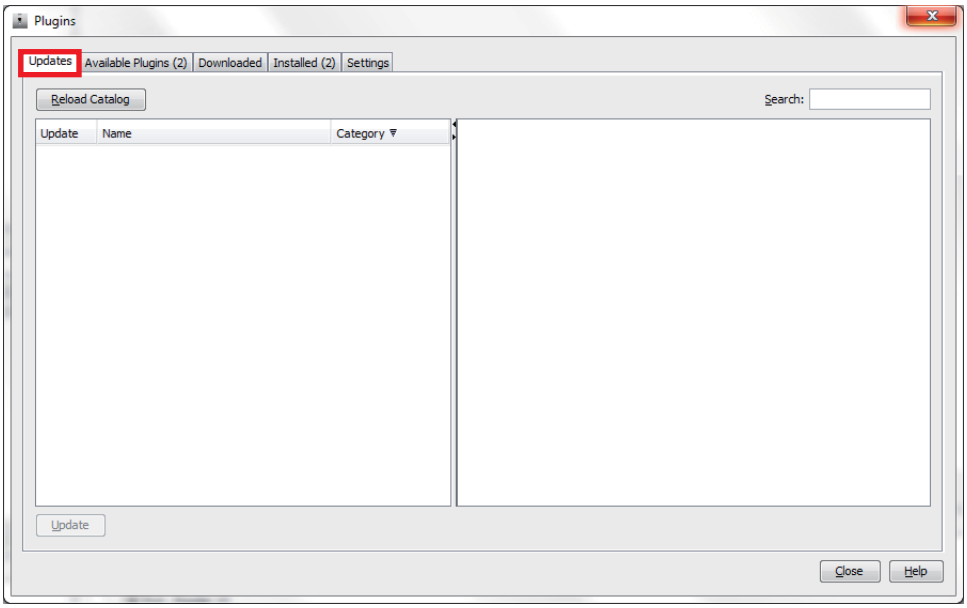


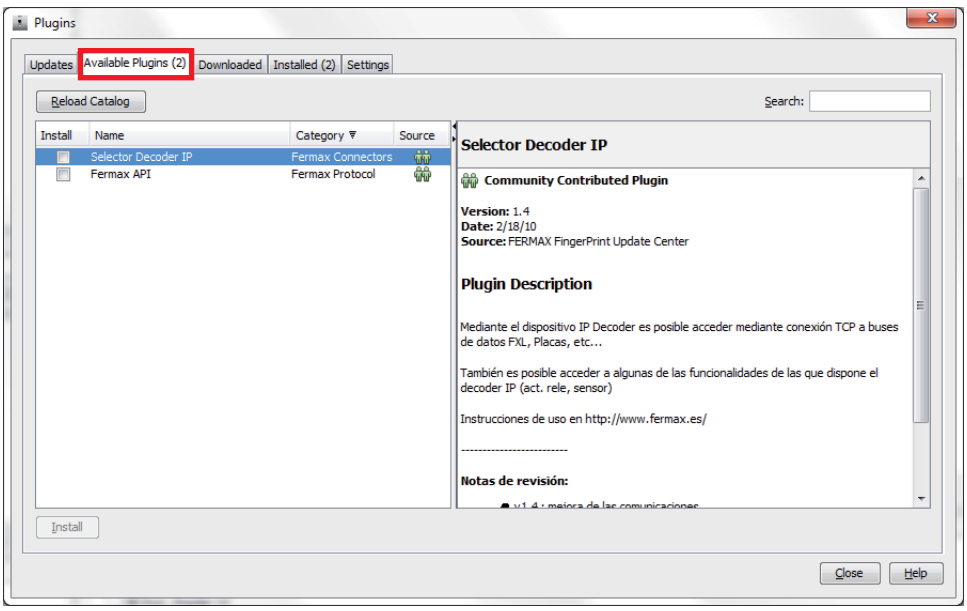
UPDATES

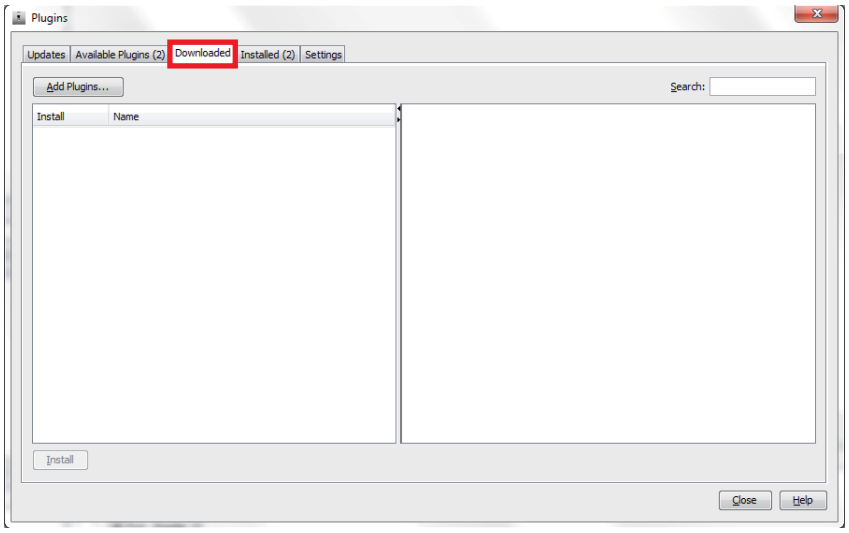
Description

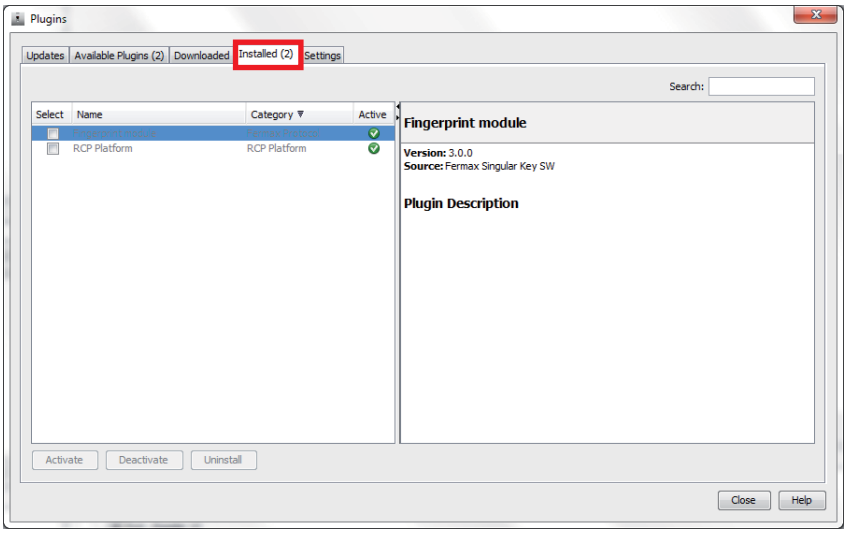
In Tools-Complements we can check for new program updates that can appear as they are distributed by our updates server. This control centre can also be used to distribute new modules or complements no included in the program´s initial version. You can also configure the frequency of checking for new updates, or deactivate their installations. Different screens:

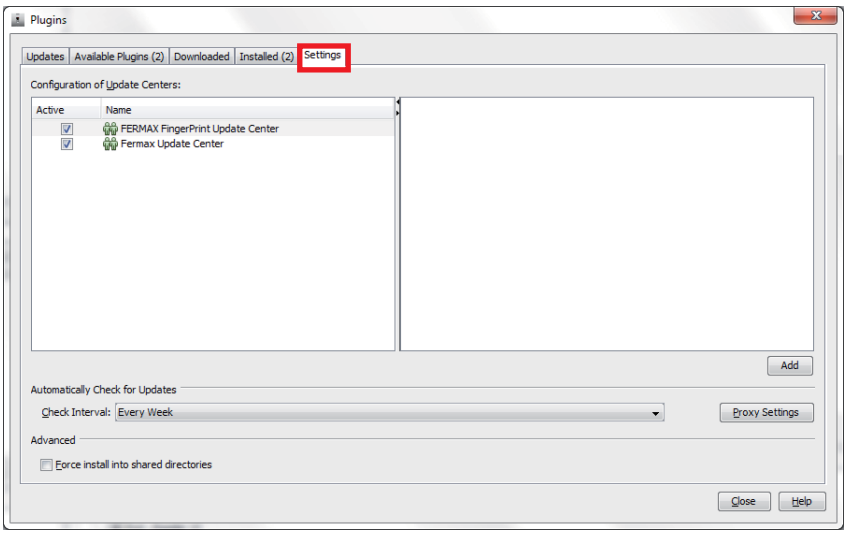
- **updates**
- **available complements**
- **downloaded**
- **installed**
- **configuration**





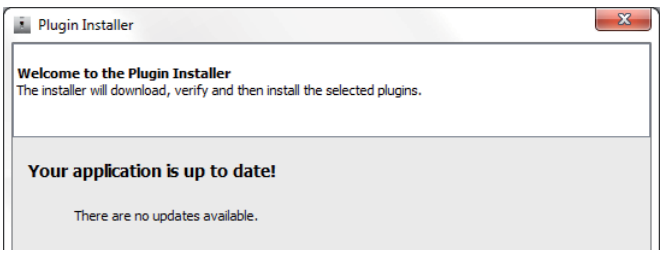






Check for updates

In Help-Check for updates, this screen appears which checks for new versions of complements, and if found are in charge of automatically installing them.

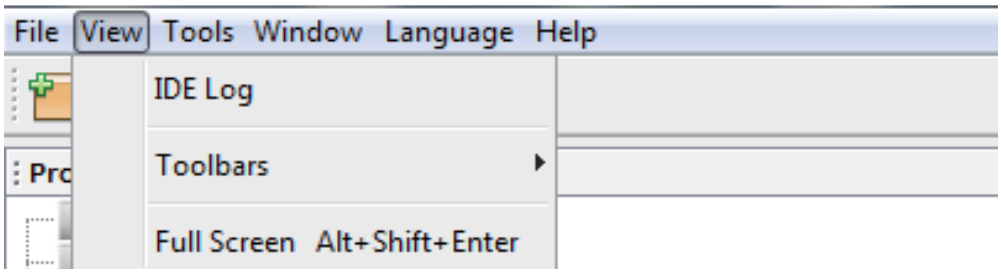


GENERAL BUTTONS (MENU BAR)

At this point you will see where the options appear from the menu bar, which has yet to be mentioned. The majority have been described and explained previously in the manual.

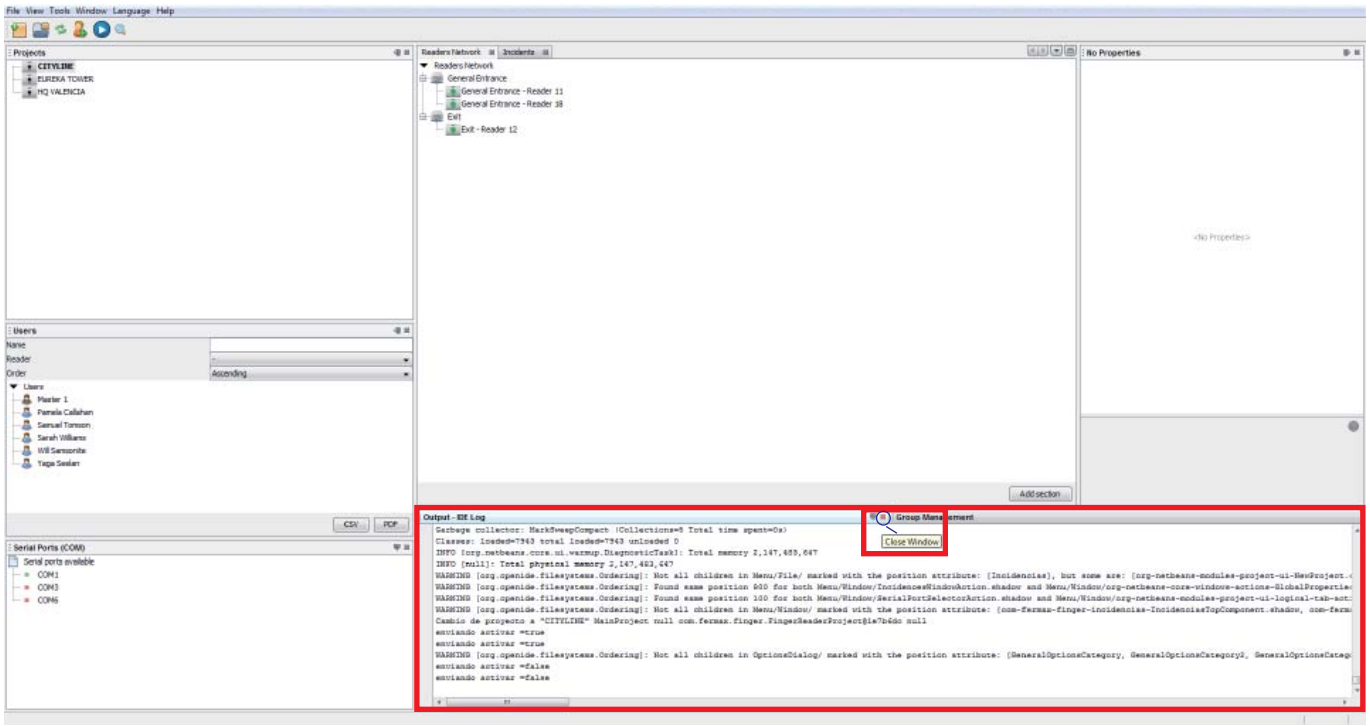
VIEW

Windows available within the application.

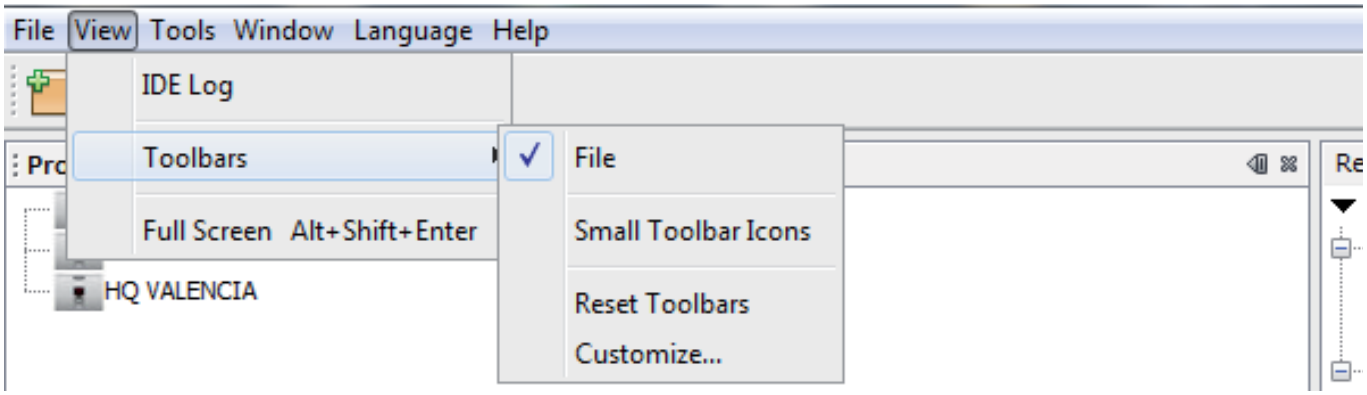


Program registration file

This option opens the program registration screen. This screen has the outputs per screen that have been indicated in the program´s code. This shares the part of the main screen where the Groups are. It can be closed as indicated on the screen.



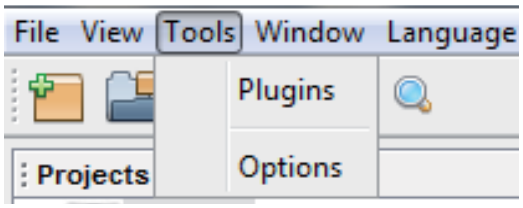
Tool bar



Full screen

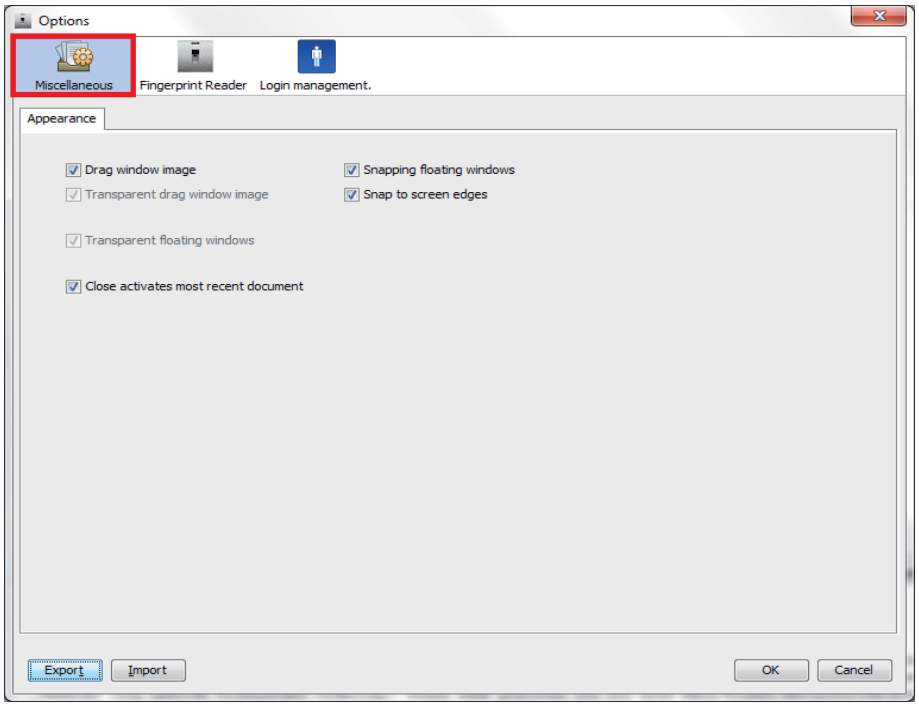
TOOLS

The other available options have already been described and explained previously in this manual.



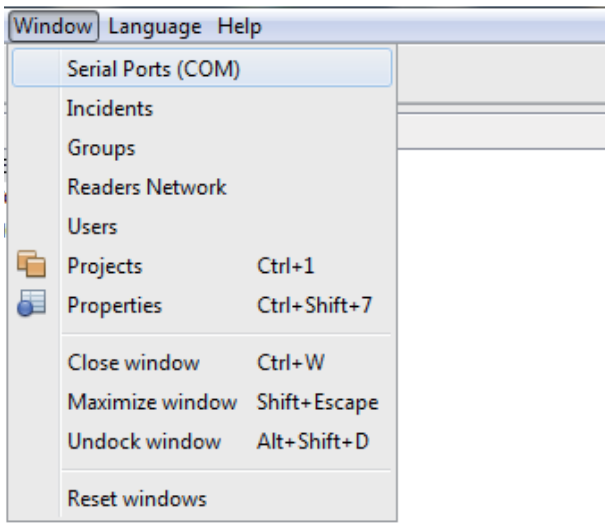
Options

The other available screens have already been described and explained previously in this manual.



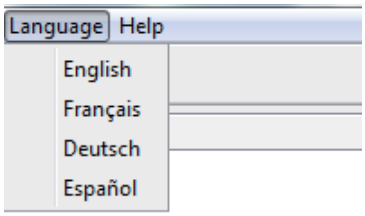
WINDOW

Windows available within the application.



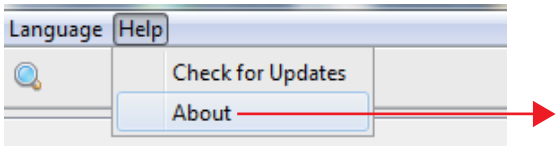
LANGUAGE

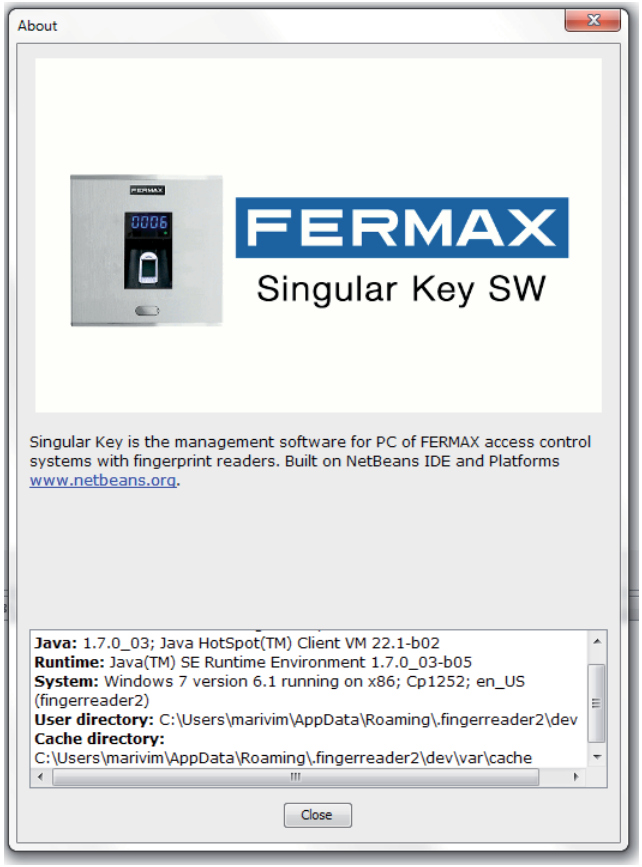
Languages available



HELP

Help





UNINSTALL THE SINGULAR KEY SW SOFTWARE

To uninstall the Program go to: Start > All Programs > Fermax > Fingerprint Reader > Uninstall Singular Key SW

FERMAX
Avd. Tres Cruces, 133
46017 Valencia
Spain