FERMAX

CAC SERVER

INSTALLER'S MANUAL

ENGLISH

CAC Server Manual
Cod.97307I V06_14

ENGLISH

CE

INDEX

CAC system ARCHITECTURE

Installation of access control of CAC is composed of hardware on the one hand: CAC central units, readers, decoders etc.. and on the other, of software that allows configuration and management of the installation

With respect to the software management side of the installation, CAC has various applications which will permit configuration and management of the different options and possibilities it offers.

These applications are grouped under «Server Application» and «Client Application»:

- ***Server Application***:

  · **CAC Server**: this is the application in which the installer defines the hardware elements of the installation, and which, in turn, acts as the server for the CAC architecture´s client application and as communications server with the CAC installation.

  The PC in which the CAC server is installed should be connected directly to the installation through an adequate interface (see section Connections PC-Central).

  This application also manages the data base where all information pertaining to the installation is stored (users, incidents etc..) , which supplies the rest of the user applications and the CAC Server itself.

  The whole CAC system must have a single CAC Server application.

- ***Client Application***: this is the application developed for the user which allows maximum use of the functions offered by the CAC system, through a simple, highly intuitive graphical interface, allowing you to act on the installation, search and view information relevant to the installation (events, users etc..), all in online/offline mode via the server applications.

  Furthermore, thanks to the architecture employed in CAC, the client application may be installed in one or various computers on the same network, being multi-station applications.

Important observations regarding CAC system architecture!!!!!

The following instructions must be kept in mind when using either server or client software:

• Whenever system management tasks are carried out using the CAC Server application (adding a new system, exploring systems, modifying systems..) contradictory processes may arise in the CAC Access client application; where both are open at the same time. ***It is recommended that all client applications are closed before making any modifications on the server.***

• A similar situation may arise when 2 CAC Access sessions are executed simultaneously under the same profile (administrator, profile, operator). The easiest option is to open each session under a different user profile.

Configuration and Topology of the CAC system

The use of the CAC applications server permits a client-server architecture with the following advantages:

- The possibility of managing the installation from any PC connected to the same computer network as the server.
- The server may be installed in a secure area so as to protect access and guarantee security for the same.
- Simultaneous handling from various PCs (the same user application installed in various machines).

- Different applications may be started on the same computer or from different computers.

The computer that acts as server must be connected to the access control installation by means of one of the supported media: local serial connection (RS-232 / RS-485) or remote connection (IP).

In the event of having client applications installed in different computers, other than that which is installed in the Server, the latter must continue to work without interruption, for which it is recommended that it is protected by UPS and installed in a restricted area.

The installation database (CAC Server) stores the information of the installed equipment, user access and generated incidents.

In the following diagrams you can view the different installation options:

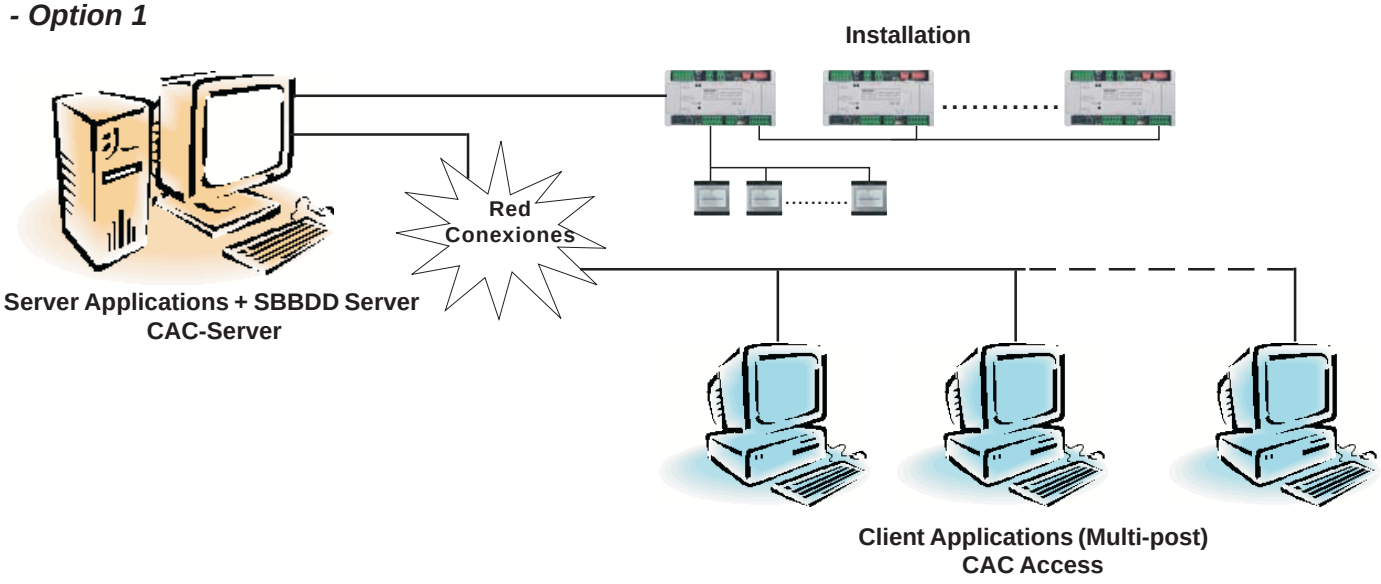
- Option 1. The computer acting as server holds the database and the user applications are controlled from other computers.
- Option 2. All the applications, server and database are supported on the same computer.

  This is the simplest method, in which a local network is not necessary. This occurs when there is only one operator.

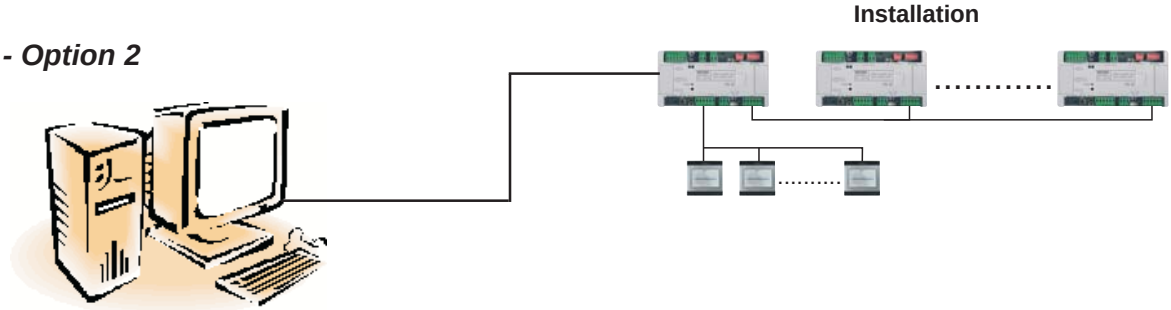
At the end of the manual an Annex is attached, where there are detailed diagrams of network connections between central units (FXL Network) and the connection between the PC and the installation.

System installation option

- Option 1



- Option 2



Characteristics of the CAC system

- 2046 user access control
- Management of up to 64 central units and 32 doors per centre unit, with the possibility of grouping them into 4 different sections (see section on sections).
- Management of user logins for access to Server and Client applications.
- Test of installed devices (central units, readers).
- Special treatment for vehicle doors. Car parks.
- 64 groups of users (profiles). Each one defines the restrictions that are applied to the group over the assignment of up to 3 Areas and 3 Timetables.
- 4 special profiles without restrictions.
- 32 Areas. Define the doors through which access is permitted.
- 32 Timetables Define the periods of time in which access is permitted to users.
- Holidays (20 days' holiday and 3 holiday periods). Affects all profiles except the special profiles.
- Register of the last 3000 incidents (entrances, exits, accesses denied, alarms etc..) in each central unit. When the Server is on there is no restriction.
- 1000 intercommunication panels / 1000 sensors / 1000 relays per central unit.
- 32 weekly device activation plans (sensors and relays).
- Restriction on the number of people in certain rooms or areas.
- Temporary blocking of individual users or groups. They are not permitted access until they are unblocked.
- Automatic changes to winter and summer time.
- Global antipassback function.
- Activation of devices associated with each user, on presenting thier identifier in a reader.
- Activation of relays from a reader with keypad and proximity card. Connection and disconnection of alarms.
- Continuous test of devices.
- Interaction of PC software with the installation: door openings, blocking/unblocking of doors, blocking of users etc..

Recommended requirements

In order to launch the application the following requirements are recommended:

-Processor: 1Ghz processor, 32 or 64 bits
- Operating System: Windows 7
- RAM: 1Gb RAM (32 bits) 2Gb RAM (64 bits)
- Port: 1 RS-232 series or USB port
- Hard Drive: 256 Mb

DEFINITION OF ITEMS

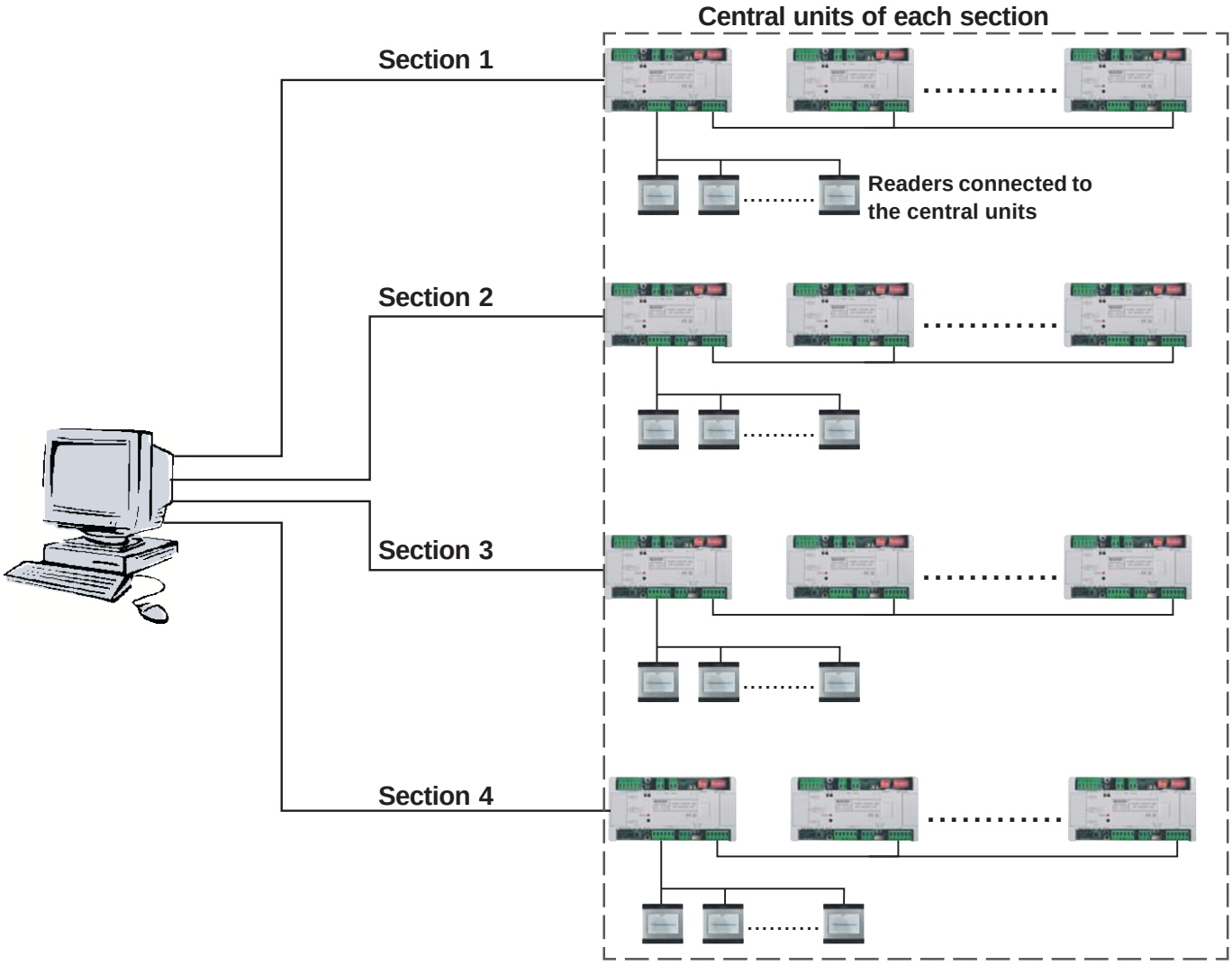
**** Sections***

The CAC Control Server application, allows the installation to be organised into Sections (up to 4 different sections).

In installations with an elevated number of central units or central units very distant from each other, the creation of sections allows management of all the central units from the same PC, without any need to join all the central units to each other through the FXL Network, and so creating a single installation.

In order to do this, it is only necessary to join the central units through the FXL Network that belong to the same section and connect each section to the PC through the corresponding PC-Central interface (2338, 2466, 24661, 1086 Remote Terminal Management IP, etc).

In this way the PC becomes the hub of the central units, allowing all the central units to have a connection between them::



Important:

- The whole CAC installation will consist of at least one section.
- The maximum number of central units is 64, regardless of the number of existing sections.
- Connection between central units of the same section is carried out through the FXL Network.
- Each Section is physically connected to the ports of the computer where the CAC Server is installed. The connection can be made through:

  Ports series RS232: required interfaces RS232-485, Ref.2338 or 2466.
  Local Network: required interface Remote Management Terminal IP, Ref.1087 + Ref.2466
  USB Port: interface RS485 needed, Ref. 24661.

**** CAC Central units.***

An installation of CAC access control will use from 1 to 64 CAC central units.

Each central unit is inserted into the CAC Control Server application, into its corresponding section and it is assigned a description and central unit number.

This central unit number must coincide with the number assigned to the central unit through dip-switches 1 to 5 of microswitch SW2.

**** Doors.***

A door corresponds to each one of the readers or door controllers (DC) of the installation. Each DC may manage up to 2 readers (Entrance/Exit) from the same door.

In accordance with access permission, defined later within the CAC Access user application, the users will have access through some doors and others.

In the CAC Control Server application, for each central unit, as many doors as readers or DCs are added which can be connected to the the central units in the installation (from 1 to 32 readers or door controllers per central unit).

For each door it is necessary to configure diverse parameters according to the type of door (reader or door controller) and its function within the installation, it being essential to assign them a description and an access number.

This access number should coincide with the number assigned to the reader or door controller by means of the dip-switches of the reader or door controller configuration.

**** Areas.***

It is only necessary to define areas in cases when this is required ***capacity restriction*** (capacity control).

In order to set up this function it will be necessary to define in each door:

- the area which is accessed (to enter) and the area which is vacated (to exit) through the door.
- and in order to restrict capacity, indicate if the door influences capacity of the area.

Up to 32 different areas may be created and each one has its own independent counter. The information on capacity is stored in non-volatile memory, in such a way that if a reset is made or a power outage occurs in the central unit, information will not be lost.

Restricted capacity: For the restricted capacity to function, the maximum capacity of users in the area should be defined and the relay should be activated in the event of reaching this capacity (optional).

The CAC system carries out capacity control, increasing the area capacity counter by 1 when a user accesses an area through a door defined as an access to this area, decreasing by 1 when the user leaves the area by an access defined as an exit from the area (these parameters are defined at each door).

When maximum capacity has been reached no access is permitted to any other users (although they may wait for access permission), until one of the users leaves the area.

It is possible to carry out a reset of the capacity of the area, that is to say, reset the capacity counter of the area to zero, resetting the access door in the area, a defined proximity card (through the CAC Access application) as "capacity reset". In this way, apart from the users already in the area, access is allowed to the area for new users, until the maximum capacity is reached again.

Also, capacity can be reset from the CAC Access application.

Also, a capacity of "0" may be defined; in this case the number of users in the area is not restricted, the selected relay activating itself while there is a user in the area.

**** Antipassback.***

The antipassback function restricts a user who has accessed the installation, through an entrance door, the installation may be re-entered (through any other entrance door), unless they have previously exited the installation by an exit door.

In this way various people are prevented from accessing the installation with the same user device, in the same way that various cars are prevented from accessing the carparks with the same identifier, so providing better security to the installation.

The CAC system permits the anti-passback function to be carried out in a very simple way and at a global level for the whole installation. In order to do this it is only necessary to define the perimeter of the installation where the antipassback function is required to be introduced.

The perimeter of the installation is defined by the doors of the installation, configured thus ***entrance to the perimeter*** or ***exit from the perimeter*** from the installation.

Therefore, in order to set up the antipassback function, for each door to form part of the perimeter, it is necessary to indicate if they are doors which permit ***entry*** o ***exit*** from the same.

Two levels of antipassback: pedestrian and vehicle pedestrian and vehiclar

In order to increase security, the CAC system incorporates two levels of antipassback, one pedestrian and the other vehicular, which apply automatically in accordance with the type of door through which the perimeter of the installation is accessed.

Access through a pedestrian door:

When a user enters into the perimeter (by a pedestrian door marked as 'entrance' to the same) remains marked as 'within' the installation since passage is not permitted through any entrance door to the perimeter, whether a pedestrian or vehicular door.

Of course the passage through exit doors or doors that do not belong to the perimeter is permitted.

When going through an 'exit' door from the perimeter, you are marked as 'outside the installation', being able to access the installation again through any entrance door to the perimeter.

Access through a vehicular door:

If, on the other hand, the user accesses the perimeter by a vehicular door, the system marks the user and their vehicle as inside the installation, so entering again through a vehicular entrance will not be possible unless previously exited by a vehicle exit access.

Of course, exit doors or those that do not belong to the perimeter are allowed.

In the event of passing through a door of *pedestrian exit* from the perimeter, the user will be able to access the perimeter again only by pedestrian entrances, and not vehicular ones, given that the vehicle is still within the installation.

**** Sensor groups - Individual sensors***

It is only necessary to define sensor groups or individual sensors when there are sensor decoders in the installation and some of the following functions associated with activation of one or more sensor inputs:

- Activation of a device (by means of relay decoder or relays of the door controller).
- Despatch of message to guard unit.
- Identification of the activated sensor in the Incident Register.
- Use of sensors in the planner.

**** Relay groups - Individual relays***

It will only be necessary to define groups of relays or individual relays, in the event that there are relay decoders in the installation and one of the following functions is required:

- Activation of lock-release by means of relay decoder (in order to provide better security for the installation).
- Associated with a sensor: Activation of a device following detection by a sensor.
- Activation of a user device.
- Activation of devices from keypad readers connected to the door controller.
- Activation of relay for restricting capacity in the area.
- Use of relays in the planner..

**** Planner***

Allows definition of up to 32 automation plans for control of devices.

In each plan the following parameters are defined:

- Initial and final timetable of the plan (initial and final timetable of activity of a device)
- Days of the week that the plan is executed.
- It must be carried out during days of official holiday.
- It should be sinchronized after a reset of the central unit..
- Select the operation to be carried out:

  activation/deactivation of the auxiliary door relay from a door controller.

  activation/ deactivation of decoder relay.

  enabling/disabling of decoder sensor.

**** Sabotage control***

Permits activation of the detection of sabotage function of the decoders busbar (where the relay decoders are connected, sensor decoders or panel decoders for intercommunication).

In order to do this the type of decoder installed must be indicated on the end part of the busbar and the given address on one of its outputs.

If during the verification process of the state of the decoder buses, that is carried out by the central unit every 60 seconds, the central unit does not detect the address of the indicated output, the central unit generates a sabotage incident that will be stored in the incident register and a sabotage message will be sent to the guard unit (if it exists).

STEPS FOR INITIATING CAC INSTALLATION

The configuration and initiating steps for a CAC access control installation are the following:

1º. Installing, wiring and configurating the hardware equipment:

- **CAC Central units.** Configuring the address of each central unit
- **Readers.** Configuring the address of the readers (door controller or controller with integrated reader) by means of the microswitches located in each one of them.
- **Sensor decoders, relays and panels (if they exist).** Programming the addresses of the exits/entrances of the decoders and the rest of the parameters by means of the Decowin application (supplied with the CAC central unit).
- **Guard unit (if it exists).** The guard unit occupies the address 0 of the reader's busbar.

2º. Install the "CAC Control Server» server program on the PC.

See section: **"Installation of CAC Control Server application"**.

3º. Execute and configure the server application.

See section: **"Installation of CAC Control Server application"**.

From the CAC Control Server application:

4º. Create the installation

4.1. Create the sections of the installation

4.2. Add the CAC Central Units that comprise each section.

4.3. For each central unit, configuring the elements that form:

4.3.1. Doors (readers)

4.3.2. Areas

4.3.3. Groups of sensors - individual sensors

4.3.4. Relay groups - individual relays

4.3.5. Planner

4.3.6. Sabotage control

The following sections of the manual show how to configure each one of the elements of the installation.

5º. Updaing Date and Time of the central units and Daylight Saving Time. (See section **"Control Panel "**).

8º. Updating the central units. (See section **"Updating of the information in the central units"**).

9º. Start up of services. (See section **"Start services"**).

INSTALLATION of the CAC Server application

As detailed above, the CAC system requires a server application (CAC Server) for its configuration and for the correct operation of the client application.

This application should always be running so that the client application (CAC Access) can work in online mode (online, in real time) with the installation. Otherwise the client application will work in offline mode and the changes or actions carried out on the system will not have any effect until the server applications are initiated.

The system installer will run on the CAC Server application, through which the installation´s hardware elements are configured, and its services should be running in order for the CAC system to operate correctly.

Installation and initial configuration of the server application

The CAC Server application is installed from the CD supplied with the CAC central unit.

Below are the steps for installing the server application correctly for the first time:

1. Install the server application

Install the Server application on the computer that will carry out the communications server functions and configuration of the CAC installation, along with the database server functions for the CAC installation.

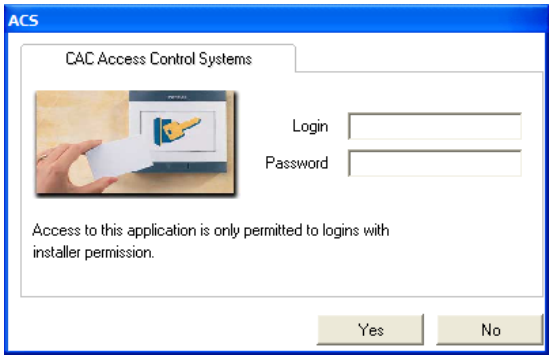
Upon installing the application a direct access icon to each application in the computer´s directory appears:

CAC Server: 

2º. Start the server application

1.1. Launch the Server application:
Double click on the direct access icon on the desktop or go to Start menu >> Programs >>Fermax >> CAC Server.

A screen appears, asking for the username and password:

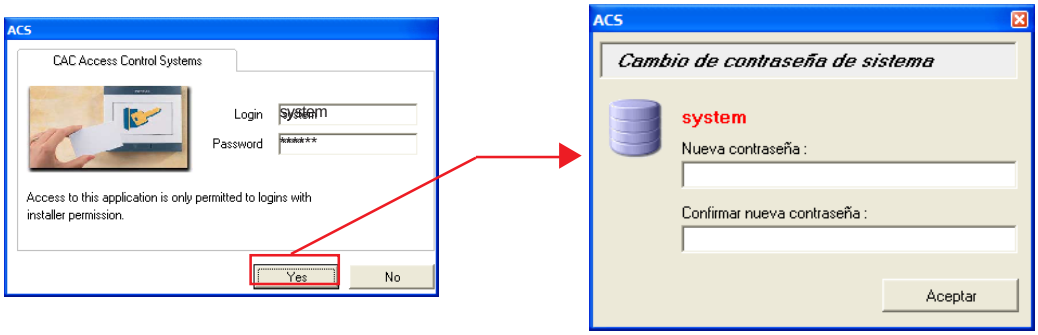


3º. Enter Login and Password

Enter the installer login and password to access the Server application and begin configuration of the CAC installation.

Login: system
Password: fermax

immediately after it will ask for a new password. Enter the new access password:

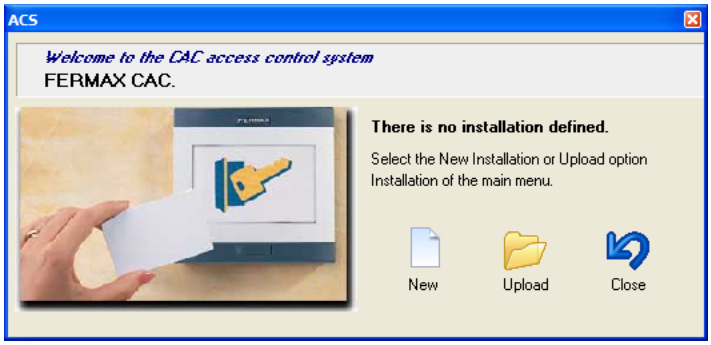


From now access to the application as installer will be carried out with the login ***"system"*** and the new password entered.

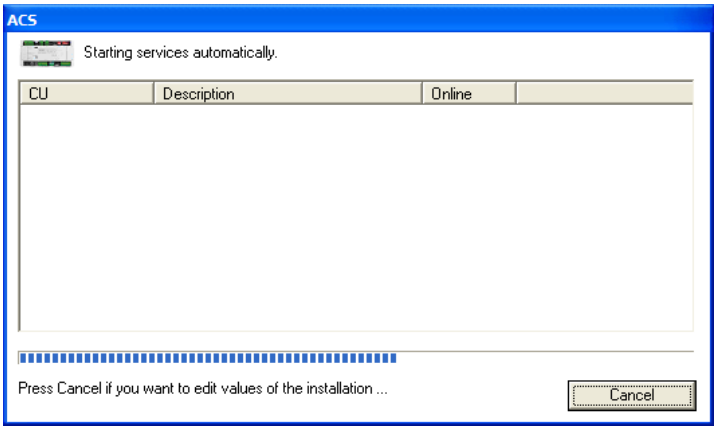
If, with the new password, the password "fermax" is repeated every time it accesses the application it will ask for a new password until it is modified.

From the Server application new logins and passwords may be created, with different access levels to the server and client applications. This point is explained in the section "Management of logins and authorisations"

Once the new password is entered the Server application main screen will be displayed along with the assistant for creating an installation:

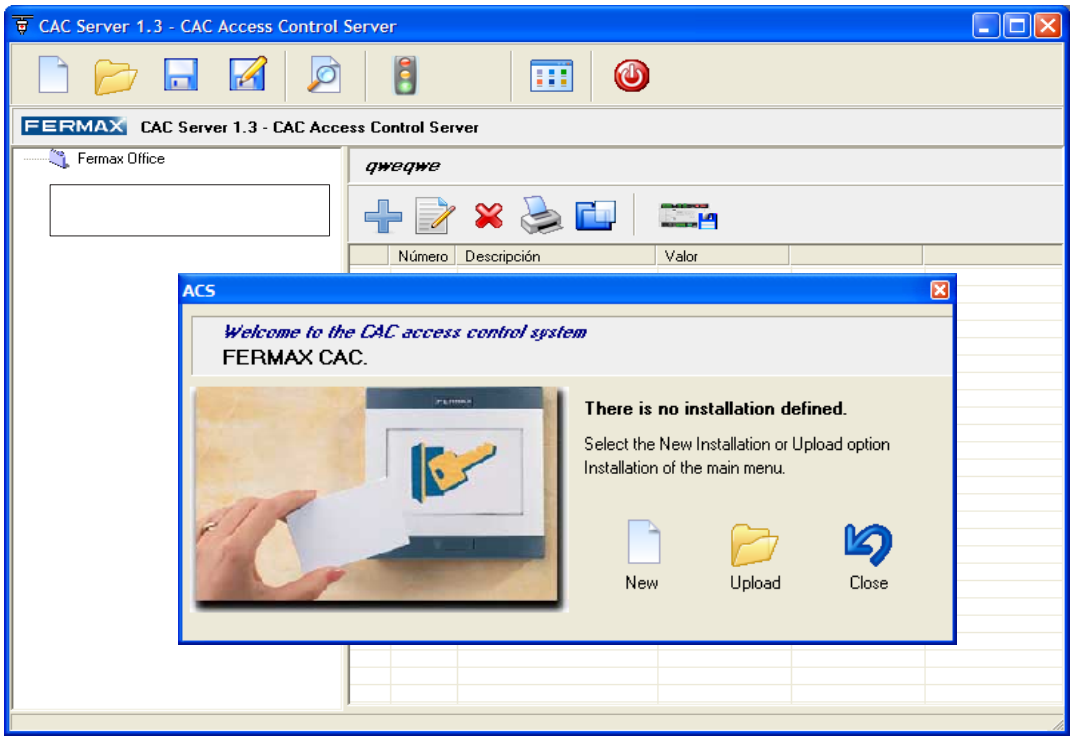


Subsequently, when an an installation already exists, and the application Server is accessed, an information screen is automatically displayed showing startup of services necessary for the correct running of the client applications (for more information consult the section "Startup services"):



CREATE AN INSTALLATION

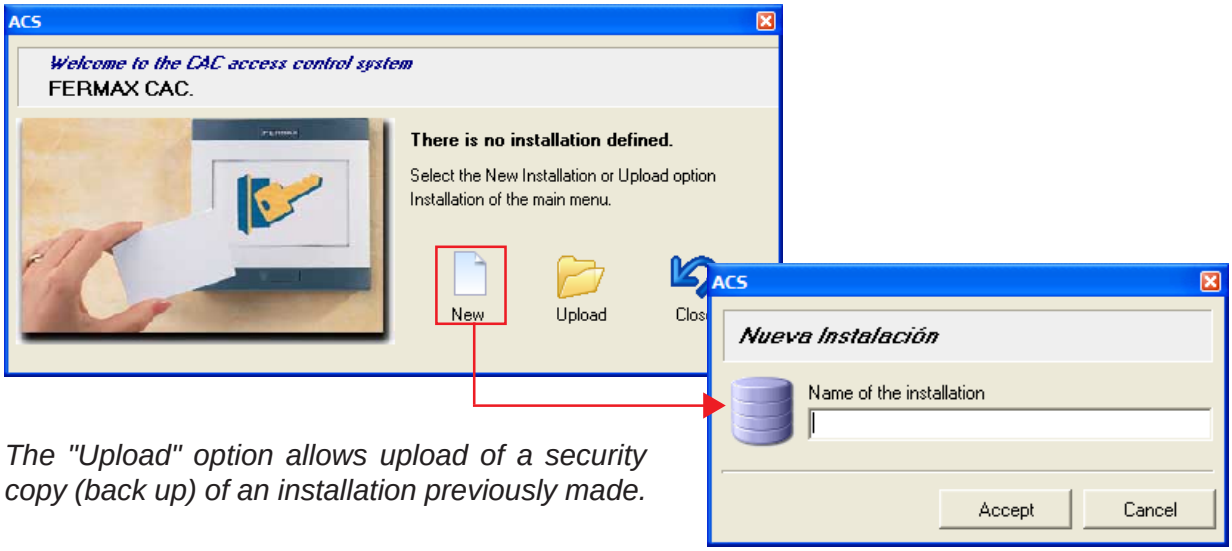
The first time that the CAC Server application is accessed (or if the application is accessed and there is no previously created installation), the main Server application screen and the assistant for creating an installation will appear.



In a CAC installation, a minimum of one section, its central unit or units and the readers (doors) connected to each central unit must be defined.

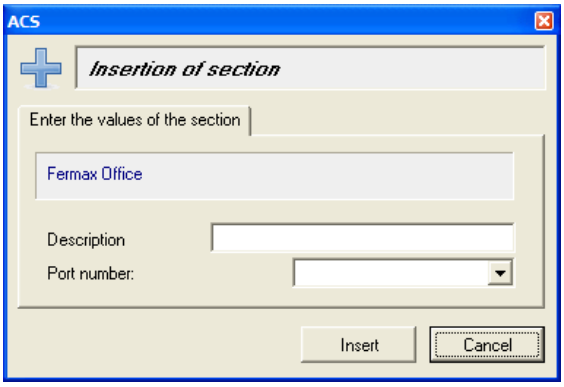
Creating an installation and its Sections

Press the "New" button and enter a name for the intstallation



The "Upload" option allows upload of a security copy (back up) of an installation previously made.

On pressing "Accept" the following screen appears which allows creation of the section or sections which the CAC installation consists of:



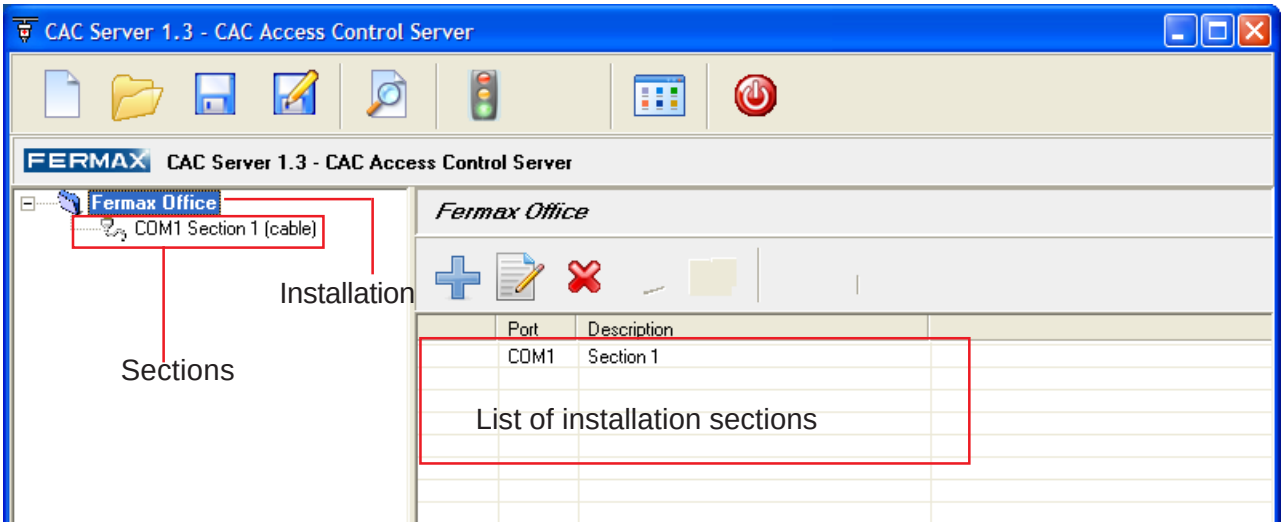
Enter a description for the Section and select the connections port (COM) that will be used to connect the installation Section with the computer.

The physical connection between the computer, where the Server is installed, and the CAC central units of the section is made using the PC-Central interface (See section "Connection between PC-Central")

Press "Insert" in order to create the section (the edition boxes will show empty in order to continue creating sections, up to a maximum of 4).

Press "Cancel" in order to finalize the insertion of sections and display the main Server application screen, where the installation and the created sections are shown:

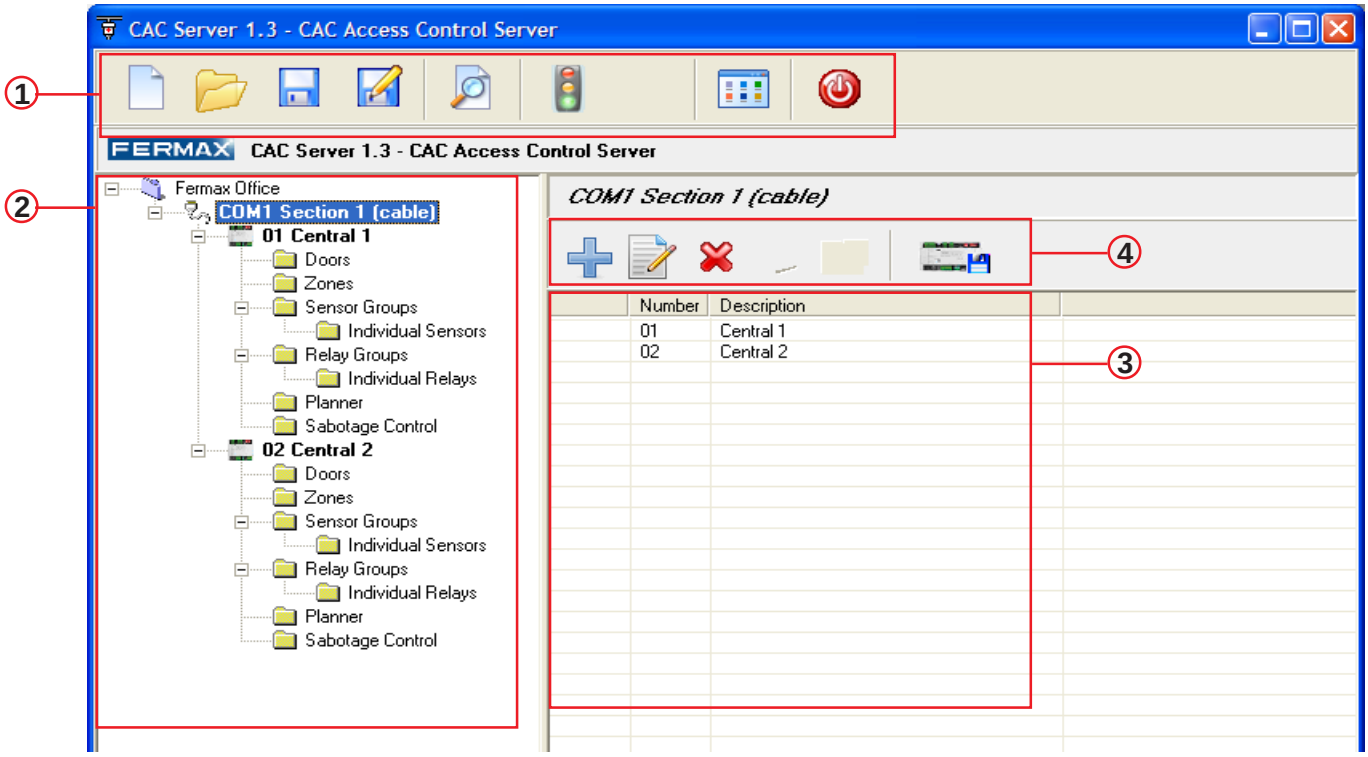
Later it will be possible to delete or create new sections in the installation (See section "Insert/Delete elements of an installation").



Once created, the installation and sections will proceed to define and configure the different elements that make up the installation: central units, doors, decoders etc..

Before continuing to define and configure the rest of the components that make up the CAC installation, the main screen of the installation will be explained, and how to insert, edit and delete elements of an installation (the process will be the same for any of the elements that comprise it).

MAIN DISPLAY FOR THE CAC Server APPLICATION Server



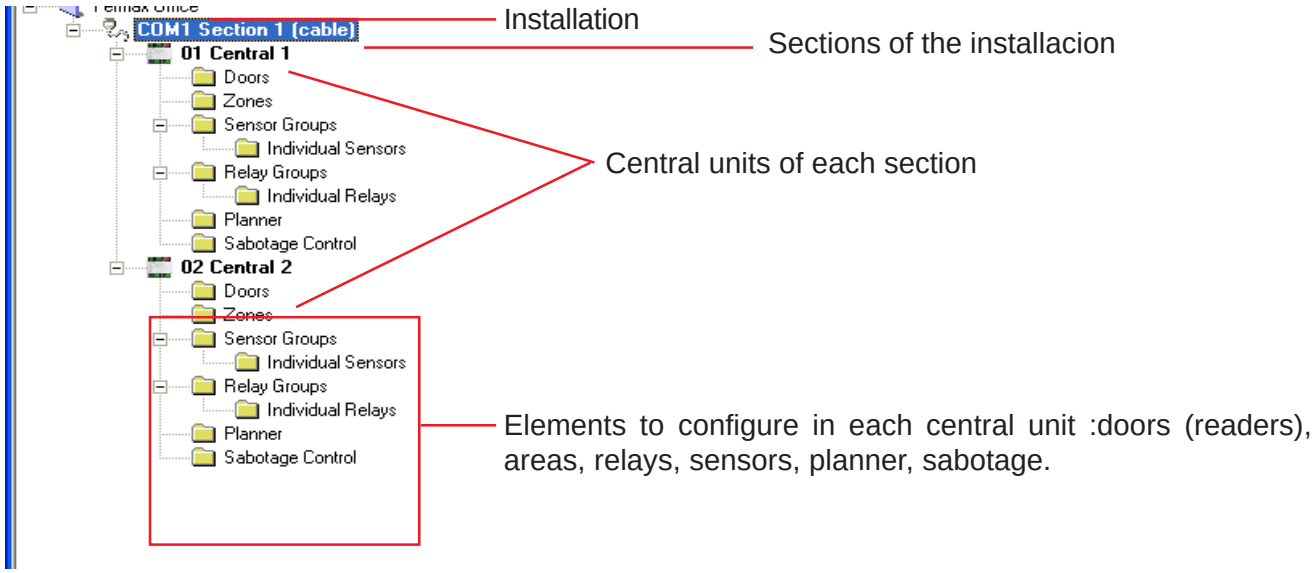
① Buttons for general use

	Creates a new installation. *This action overwrites the actual installation.* *It is recommended to make a Backup of the actual installation before creating a new installation.*
	Opens/Loads the security copy (backup) of a saved installation. *This action overwrites the actual installation.*
	Creates a security copy (backup) of the actual installation.
	Changes the name of the installation
	Carries out a test of the installation.
	Starts services of the server for the correct running of the client applications.
	Halts services that have been launched. In order to modify the installation it is necessary to ensure that the services are NOT activated
	Displays the screen "Control Panel"
	Closes the application and finalizes services The client applications will not function.

② List of components of the installation

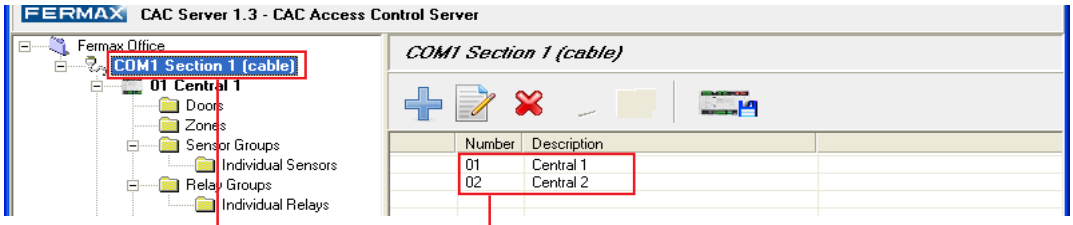
Shows a list of all the components entered for the installer, which form part of the access control for the installation.

On selecting one of the components of the installation, the information referring to the component is shown on the right of display nº 3.



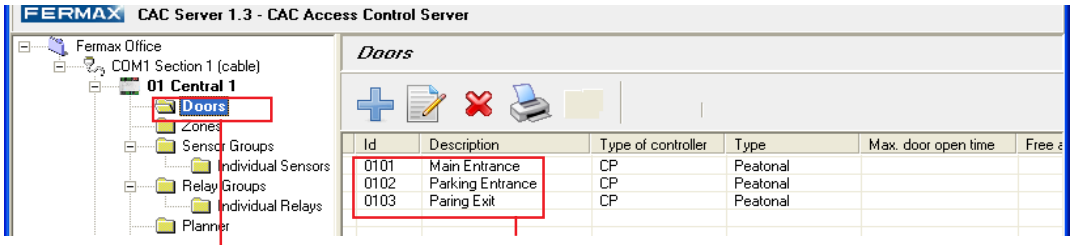
③ List of information of the selected component: elements that comprise it.

Displays information on the selected component from the "list of components":



Selected component: Section 1

Elements that make up "Section 1": Central units 1 yl 2



Selected component: Doors

Elementos que componen "Puertas": Puerta Entrada oficinas, Entrada Parking, Salida Parking, etc..

④ Component edition buttons

Permits action over the selected component and/or over the elements that contain:

	Adds a new element to the selected component.
	Edits the selected element on information display nº 3.
	Deletes the selected element on information display nº 3.
	Prints the list of elements of the selected component.
	Manages relays (see section on relays).
	Upgrades all the information in the CAC central units of the installation.

Note: *Depending on the selected component, some of these buttons may be disabled.*

INSERT, EDIT AND DELETE ELEMENTS OF AN INSTALLATION

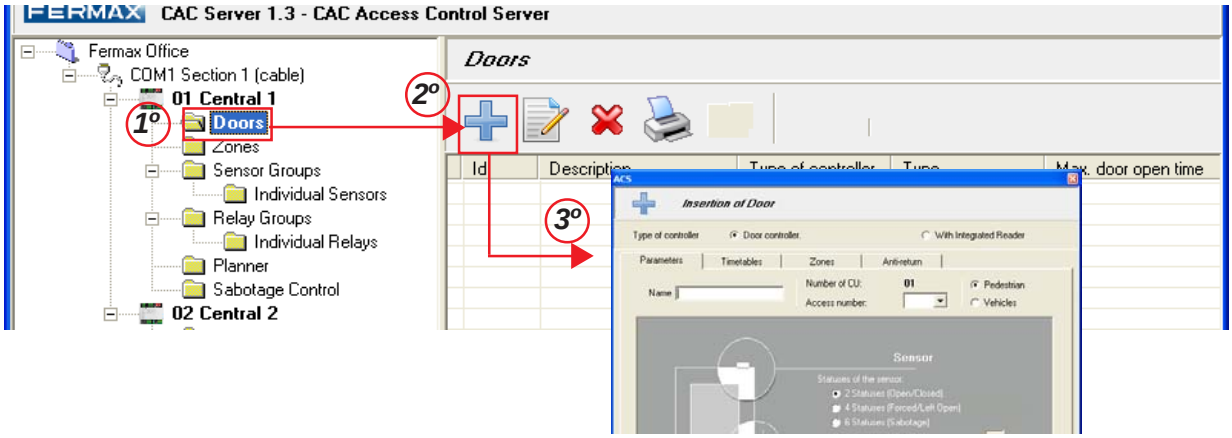
Once the installation is created, the following step for configuring the installation is to insert all the elements that it is comprised of at a physical or hardware level (central units, doors, decoders etc..) and at a functional level (sections, areas, planner etc..) so as to later on configure the corresponding parameters to each element.

As well as inserting the elements into the installation, it may be necessary at any time, to delete or modify (edit) any of the elements already inserted.

In order to insert, edit or eliminate any element of the installation, the steps to be taken are the same. Following on, steps to follow are shown for each one of these actions.

Inserts elements

1. ***Select the element to be inserted.***
2. ***Press the button*** 
3. ***Configure the corresponding parameters to each element.***
   The parameters configurable for each element and their operation is explained in the same sections for each element.



Note: In order to insert Sections or Central units, the element immediately higher that contains them should be selected:

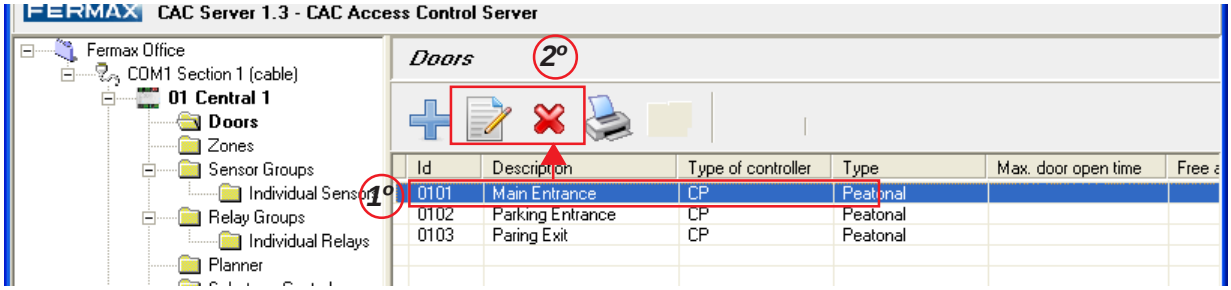
- Sections: select the installation (in the example: Fermax Office) and press "+"
- Central units: select the corresponding section (in the example: COM1 Sección 1) and press "+"

Delete or Edit elements

1. ***Select the element to be deleted from the "list of elements" (right side of the screen).***
2. ***Carry out the action:***

   - In order to delete the selected element:***Press the button*** 

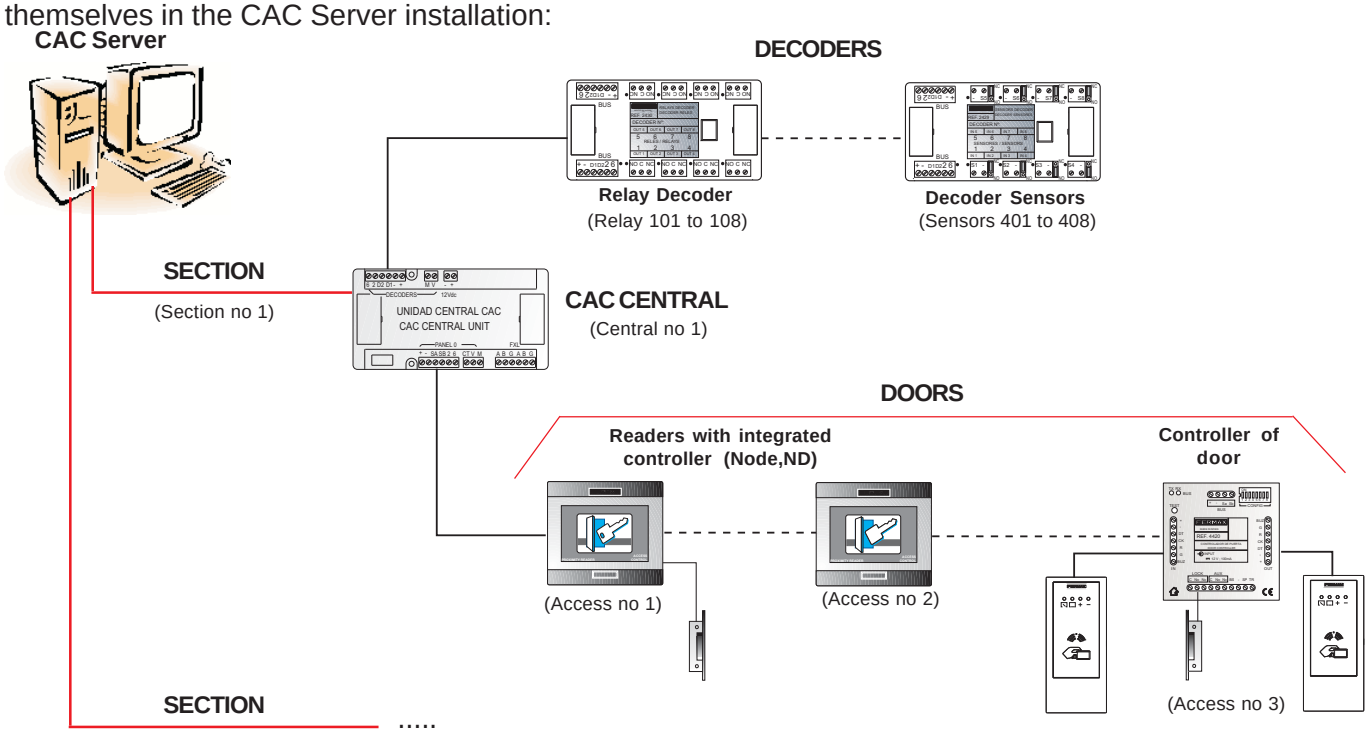
   - In order to edit the selected element: ***Press the button*** 



CONFIGURING THE ELEMENTS OF THE INSTALLATION

The following sections show the parameters to configure for each element, after their insertion into the installation. According to their function within the installation some parameters and others will configure themselves.

In the following diagram all the devices (hardware elements) are represented that can configure themselves in the CAC Server installation:



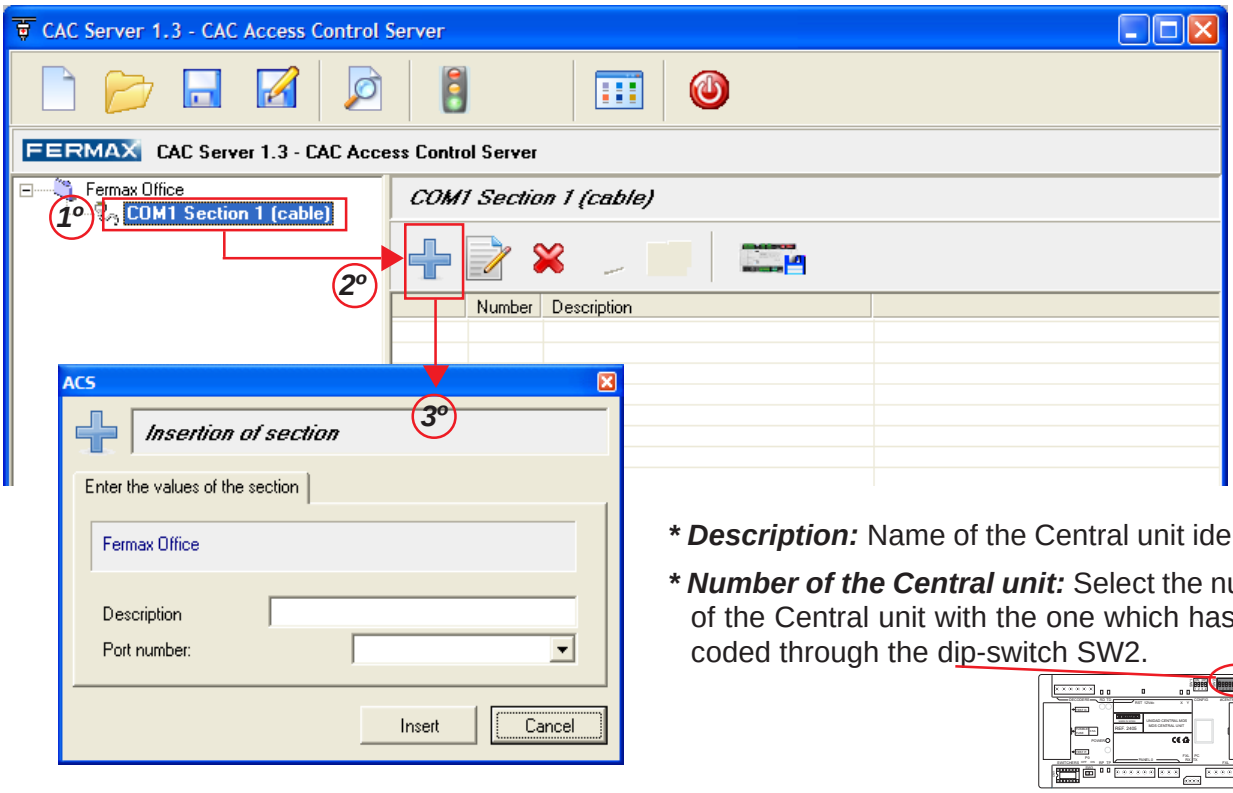
As well as the devices shown here, it is also necessary to define, according to the installation, the Area, Planner and Sabotage control elements.

Steps for configuring the installation are the following:

1. **Add the CAC Central Units that comprise each section.**
2. **For each central unit, configuring the elements that form:**
   - **2.1. Doors (readers). Insert and configure the parameters of each reader present in the installation, indicating, among other characteristics, the type of reader: door controller or reader with integrated controller.**
   - **2.2. Areas:** it will be necessary to define and configure areas if the installation will require restrictions of numbers of people in any area of installation. For every area created, it will be defined that the readers permit entry or exit to or from the area.
   - **2.3. Sensor groups - individual sensors:** it will be necessary to define and configure the sensor decoders present in the installation, indicating, among other parameters, the programmed address in each sensor (of individual or group type) and assign them their corresponding function.
   - **2.4. Relay groups - individual relays:** it will be necessary to define and configure the relay decoders present in the installation, indicating, among other parameters, the programmed address in each relay (of individual or group type) and assign them their corresponding function.
   - **2.5. Planner:** it will be necessary to define and configure plans, if some type of automation is required in the installation.
   - **2.6. Sabotage control:** if the installation has some kind of decoder and is configured for this option, the Server application checks if there are any communication problems with the decoder buses.

CENTRAL UNITES

The CAC system allows installation and management of up to 64 central units, regardless of the number of sections that exist (1 to 4).

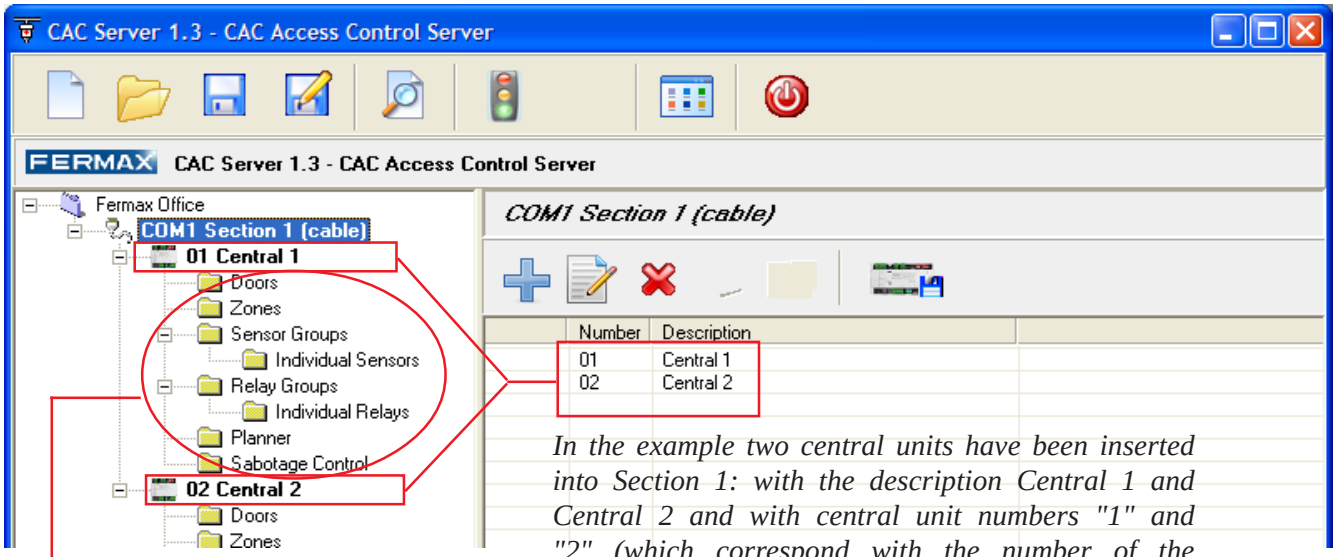


* ***Description:*** Name of the Central unit identifier

* ***Number of the Central unit:*** Select the number of the Central unit with the one which has been coded through the dip-switch SW2.

Press "Insert" to create the Central unit (the edition boxes will show empty in order to continue creating central units, up to a maximum of 64).

Press "Cancel" to finalize insertion of the central units:



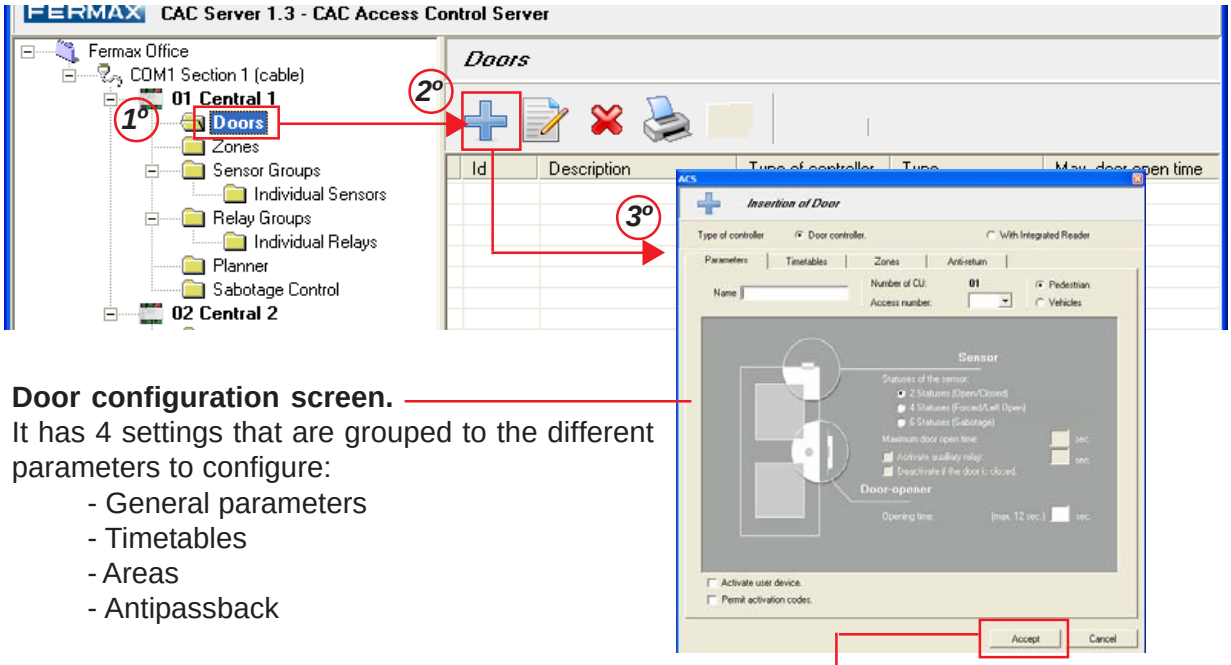
In the example two central units have been inserted into Section 1: with the description Central 1 and Central 2 and with central unit numbers "1" and "2" (which correspond with the number of the central unit coded in the microswitches).

Elements to be defined and configured for Central unit 1 according to the type of installation.

DOORS

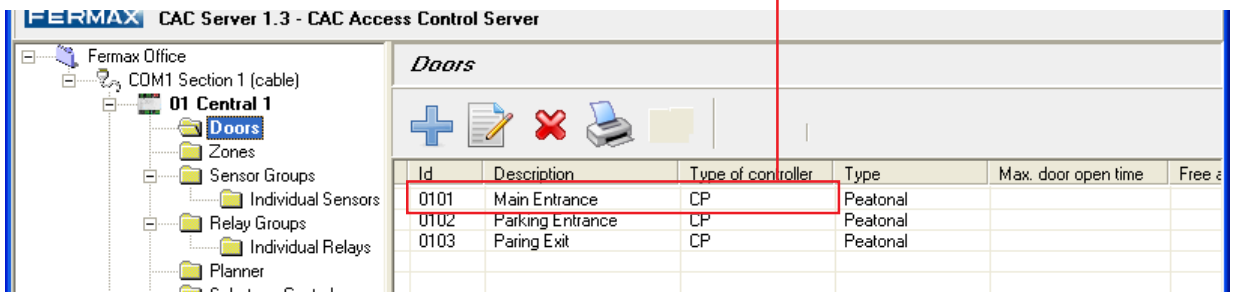
Through each central unit, the CAC system allows installation and management of up to 32 accesses with their corresponding door conrollers or readers with integrated controller.

Each door controller or reader equates to a door of the installation, restricting access through the same.



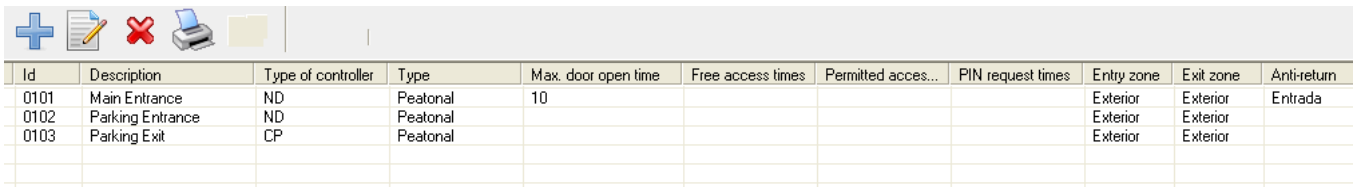
Door configuration screen.
It has 4 settings that are grouped to the different parameters to configure:

- General parameters
- Timetables
- Areas
- Antipassback



In the example 3 doors have been inserted into Central unit 1.

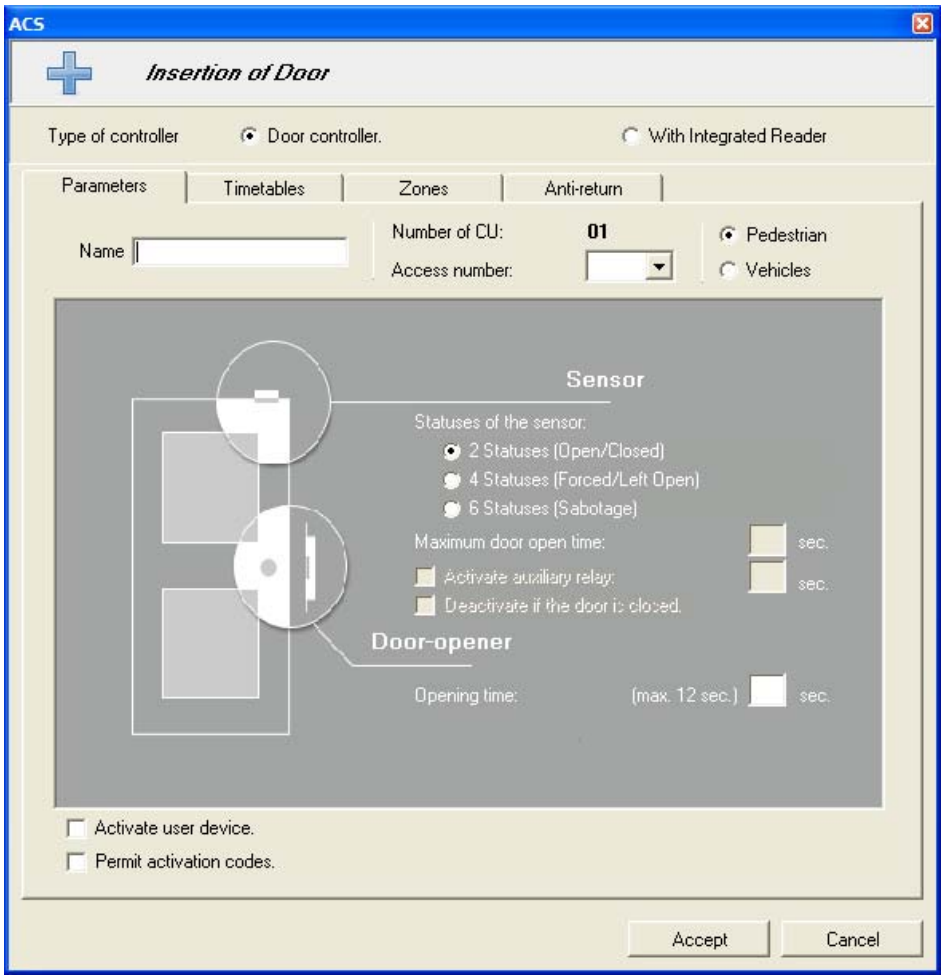
The main screen shows the doors of each central unit and information for the configuration of each door:



Id	Description	Type of controller	Type	Max. door open time	Free access times	Permitted acces...	PIN request times	Entry zone	Exit zone	Anti-return
0101	Main Entrance	ND	Peatonal	10				Exterior	Exterior	Entrada
0102	Parking Entrance	ND	Peatonal					Exterior	Exterior	
0103	Parking Exit	CP	Peatonal					Exterior	Exterior	

Then each one of the configurable parameters for the element "Doors" are shown.

General parameters



* ***Type of Controller :*** is the first parameter that should be configured for a door.
Every door should indicate the type of controller installed for that door (each door is associated with an installation controller).

Two types of controller exist:
- Door controller (DC) = the reader is separated.
- Controller with integrated reader = the reader is connected to the bus readers.

Depending on the type of controller selected, some parameters and others configure themselves (the non-configurable parameters for each type of reader are shown as disabled and in the colour grey).

* ***Name:*** ame assigned to the door (the name of a door may not be repeated).
This name will identify the door in the server and client applications of the installation.

* ***Access number:*** Each controller of the installation has an access number assigned (understood to be between 0 and 31), coded through the configuration dip-switches present in each controller, which identifies it within the central unit and the installation.

In the field "*Access number*" the access number should be selected (that is to say, the controller) that is required to associate to the door to insert.

The access numbers already used do not appear on the pop-up menu in future door insertions of the same central unit.

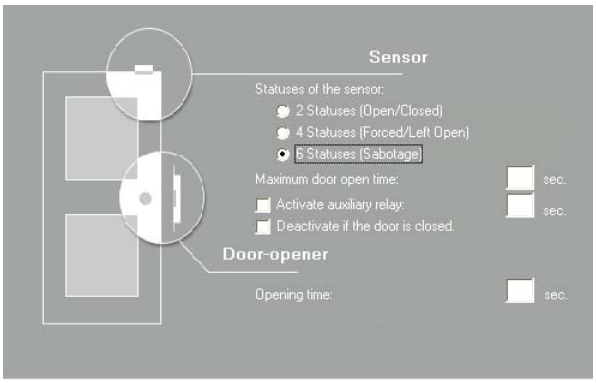
Now shown are the "*General parameters*" for configuration according to the type of controller selected:

Door controller

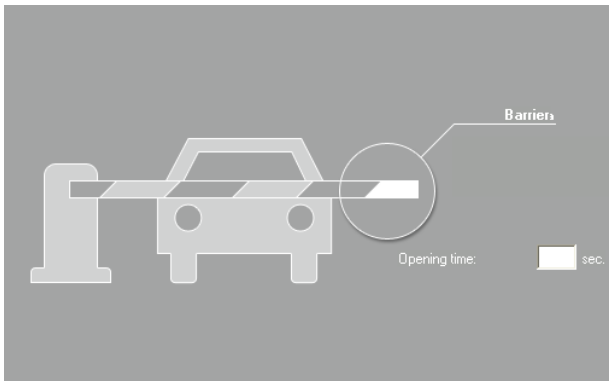
* **Operation of the door controller in vehicle mode:** In this case 2 vehicle presence detectors are needed. One connected to BS to detect the presence at reader level and the other at the height of the barrier, connected to SP. The first one allows the identifier to be read and the second one counts the vehicle (capacity) and confirms the anti-passback. For more details see the installation manual Controller of Door cod. 97033, given that in the case of vehicular access the controller should be installed according to the vehicular configuration.

  In accordance with the selected option the parameters to configure, shown in the colour grey, vary:

Pedestrian:



Vehicles:



* ***Sensor (pedestrian access)***

  Allows working configuration of the door sensor (if one exists) connected to the Door Controller:

  - 2 Sates (Open/Closed): Informs of the change of state of the door (open or closed).

  - **4 States (Open/Closed/Forced/Left Open):**
    - Informs of any change of state of the door (open or closed).
    - Informs if the door has been ***Forced***, that is, if the door has been opened without the controller previously receiving the order to "open door" from the central unit (after identification of a valid user, through door opening time from a client application etc..)

      The incident of a Forced Door supercedes that of an Open Door
    - Reports if the door has been ***Left Open***, that is, if after a valid door opening time, the door has not been closed before the time indicated on the box "Maximum door open time".

  - 6 States (Open/Closed/Forced/Left Open/Sabotaged):

  As well as the 4 states previously described (open/closed/forced/left open), informs if there has been a sabotage of the door sensor

  this type of sensor detects two types of sabotage:

  - Sabotage by shortcircuit: when the two sensor cables join (shortcircuit) in order to simulate that the sensor is on standby.

  Sabotage through open circuit: when one of the sensor cables is severed.

  In order to be able to detect the sabotage of the sensor, it should have been installed according to the configuration of the 6 states (see manual Door Controller cod.) 97033).

  According to the state and the configuration of the sensor, the door controller sends a report to the central unit indicating actual state of the door in conjunction with the state of the sensor (door open, forced..). The incident is stored in the incident register of the central unit, being able to be consulted and seen in real time through the client applications.

  - **Maximum time of door open**: is the maximum time that the door may remain open (after a valid opening) before generating a "Door left open" alarm.

  - Activate auxiliary relay: If this box activates when a "Door left open" event is produced, the auxiliary relay of the door controller is activated, during the time indicated in the box "seg". After this time the relay deactivates iself. If the programmed time is equal to 255 seconds, the relay remains locked following its activation.

  The auxiliary relay also activates if a "Forced" door event is produced or a "Sabotage of sensor". In thse cases the relay remains locked until it is deactivated from a combined reader (keypad+proximity).

  - Deactivates if the door is closed: Deactivates the auxiliary relay of the Door Controller, activated after an event of "Door left open" on closing of the door, regardless of the time of activation programmed for the relay.

* ***Door opener*** **(pedestrian and vehicular access)**

  - ***Time of opening:*** Time of activation of the ***relay of door opener*** of the Door Controller, after correct identification of the user (vehicle or pedestrian according to the type of access).

* ***Activates user device***: using the CAC Access client application a device can be associated to each user so that if the corresponding door has this function active, on presenting of user identifier. If it has no restrictions, as well as opening the door it switches the state of the associated device: if it is a sensor (decoder) it activates or deactivates, according to its previous state. If it is a relay, it activates or deactivates. This function is available for any identifier (proximity, keypad,...)

  This operation is for use when activation of the courtesy light is required, or when activating/deactivating a detector individually for each user, activating access for a second individual etc...

* ***Permits activation codes:*** from the combined readers of proximity and keypad connected to a **DC,** if the corresponding door has this function, it is possible to activate or deactivate a large number of devices.

  For this to happen, from the combined reader, the following sequence should be followed:

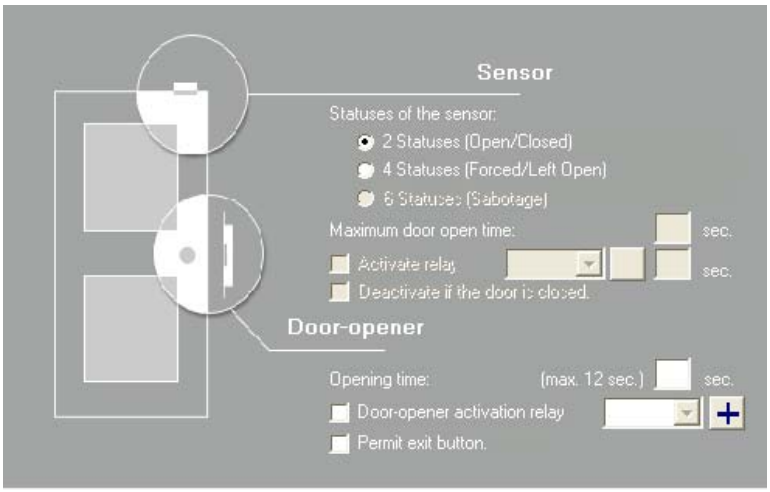
  1. Enter, using the keypad, the code for the action to be carried out, followed by the device code that will carry out the action.
  2. Present a valid identifier (proximity card) into the reader.

  The actions and devices are the following:

Code of keypad	Function
0	deactivates the door sensor of the door controller. (Permits the door to be left open indefinitely).
0X sensors	deactivates the group X of the sensor decoders (100 at a time). Ej: 02+tarjeta: deactivates the 200 to 299.
0XYZ	deactivates the sensor XYZ (decoder). When required to deactivate the alarm in an area before entering it.
1	activation door sensor of the door controller. (Reactivation of sensor in the programmed time).
1X	activation of group X of the sensor decoders (100 at a time).
1XYZ	activation of the sensor XYZ (decoder).
2	deactivation auxiliary relay of the DC.
2X	deactivation of group X of relay decoders. (100 at a time).
2XYZ	deactivation relay XYZ. (1).
3	activation auxiliary relay of the DC.
3X	activation of group X of relay decoders. (100 at a time).
3XYZ	activation relay XYZ. (1). Ej: 3010+card: activates relay 10.

With integrated reader

The controllers with integrated reader are used for pedestrian access.



* ***Sensor***

The operation of the door reader sensor is the same as that described previously for the door controller with the only difference being that it soes not have configuration for 6 states, nor does it have the auxiliary relay, nor vehiclar door.

And now the specific parameters of the reader that are different to those of the door controller (previously described) will now be described:

- **Maximum door open time:** is the maximum time that the door may remain open (after a valid opening) before generating a "Door left open" alarm.
- Activate relay: If this box activates, in the event of a "Door left open" the relay activates (an output of a relay decoder) selected from the box display, during the time indicated on the box "sec".

  The display box shows the list of relays defined in the installation (see section "Relay groups and individual relays"). From this screen, it is also possible to define relay outputs, pushing the button "**+**".
- **Deactivates if the door is closed:** - Deactivates if the door closes: Deactivates the relay (previously selected), activated after a "Door left open" event, on the door closing itself, regardless of the time of activation programmed for the relay.

* ***Door opener***

- ***Time of opening:*** Time of activation of the ***door opener relay*** of the reader, after correct identification of the user. The maximum time of activation of this relay is 12 seconds
- ***Door opener relay activation:*** Activate this box, in the event of needing to activate the door opener by means of a relay from a relay decoder (in order to provide better security in the installation) or requiring activation of an additional device (by means of a relay decoder) in the moment of carrying out a door opening, and selecting from the display box the relay to be activated during the time indicated on the box "sec".
- ***Exit permit button:*** Enables the opening of the door from the exit button connected to the reader (if it exists).

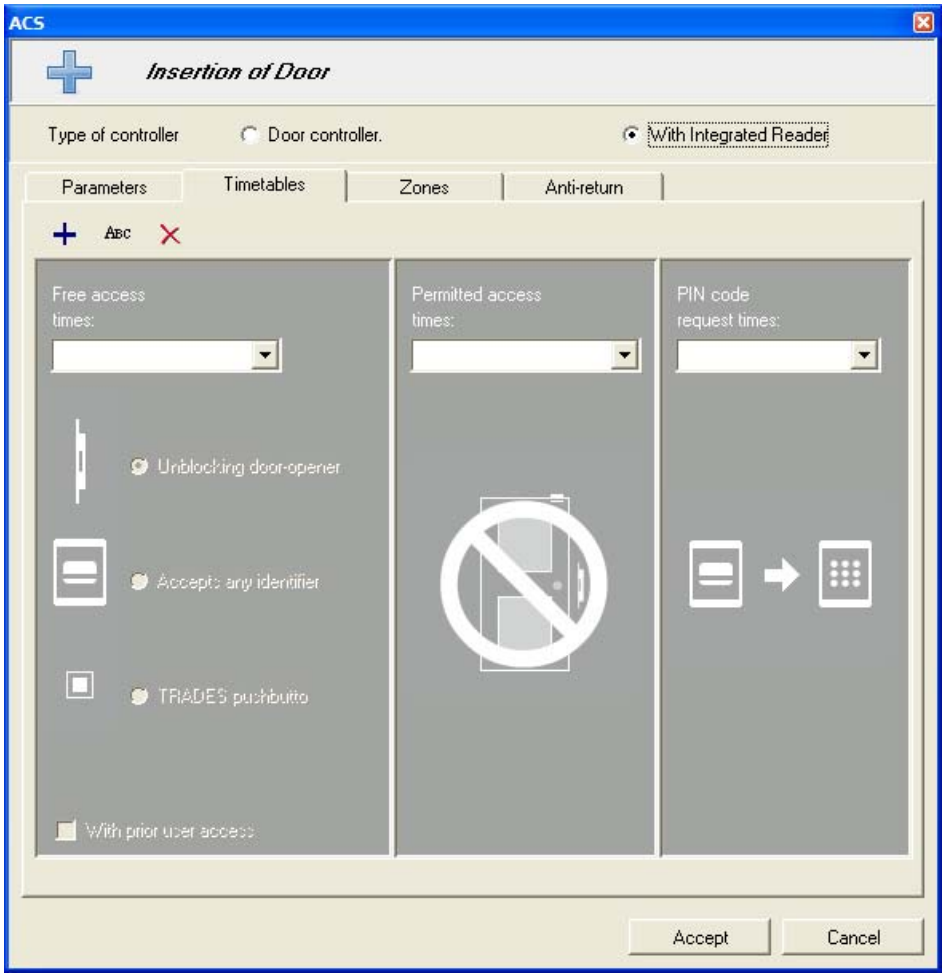
  The exit button may also be activated by means of a central unit from the guard unit connected to the installation.

  In the case of needing to enable the exit button, it will be necessary to disable this option from the Server application (deactivate the box and update the CAC central unit) and disable the option from the guard unit if this option has also been enabled from the guard unit.

  In the event that in one of the two elements of the installation (Server or guard unit), this option is activated, the exit button will carry out the opening of the door after pressing the button.

Timetables

For each door three modes of alternative operation can be configured. These modes of operation cannot be simultaneous, as they must not be defined in non-matching timetables.



* * ***Free access:*** During the times of free access selected, access is permitted through the door to any person.

  The access mode is chosen from the following:

  - ***Unblocking door opener:*** The door opener remains activated during the chosen times.
  - ***Any identifier:*** Access is permitted (door opener is activated) on introducing any user identifier, valid or not, into the reader.
  - ***TRADES pushbutton (entrance button):*** Only available with door controller.
    If a TRADES button is there and connected to the door controller, the door opener will be activated on pressing it during the chosen times.
  - ***With previous user access:*** Allows conditional mode of operation of "Free Access" in the presence of an authorised person inside the installation, that is, the "free access" mode selected will not be active until an authorised user enters a valid identifier, for that particular door, within the chosen timetable of free access.

* ***Access permitted:*** Permits assignment of a timetable of access to the door, to restrict access outside of that timetable to all users, except those users with special permission. (super-users or non-restricted users). In this way access can be restricted to all personnel without need to create or assign access levels (profiles) to users.

The access levels for each user (profiles) are created and assigned through the CAC Access application.

* ***PIN number request:*** During this time a personal code of 4 digits (PIN) is requested, as well as the user identifier.

If the code belongs to the user that introduces the identifier, access will be permitted. In this way if a user loses their identifier, the person finding it will be prevented from accessing the installation, on non-recognition of PIN.

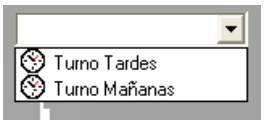
The PIN code is assigned to the user by means of the CAC Access application in the user's file.

Important:

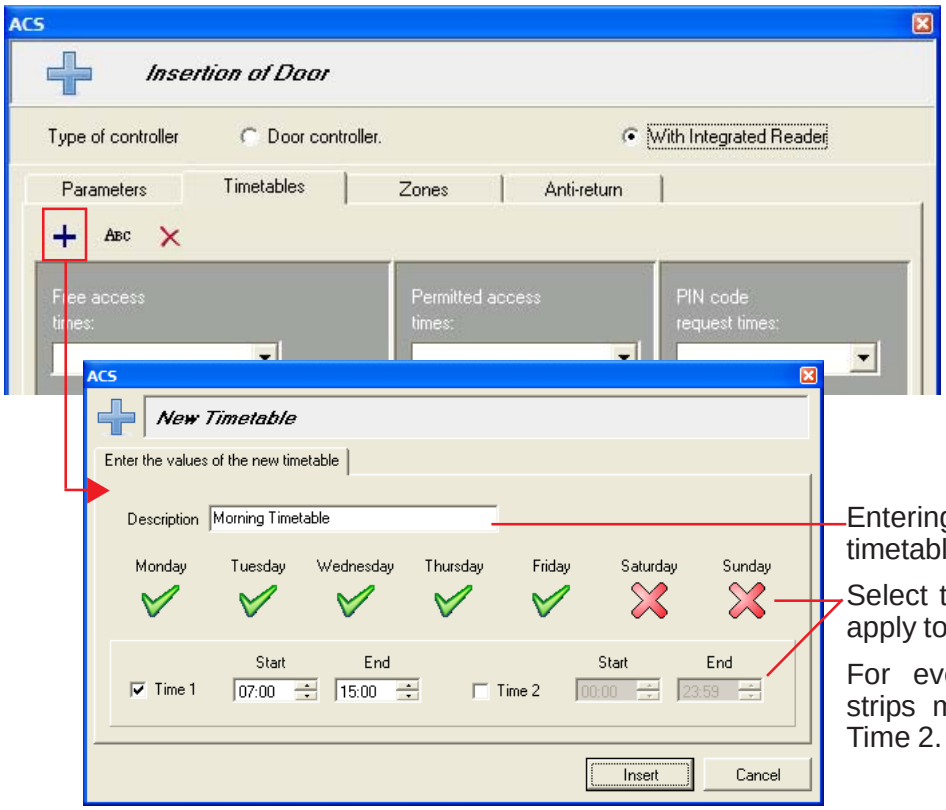
- The PIN code only works in combined readers with keypad AND proximity.

CREATE TIMETABLES

The assigned timetables to each fuctional mode are selected from the display menu available in each mode.



The selected timetables must be created in the following way (up to 32 timetables can be created):



Entering a description for each timetable

Select the days and hours which will apply to the timetable.

For every timetable two timetable strips may be defined: Time 1 and Time 2.

Abc Modify an existing timetable.

Delete an existing timetable.

Important

- In holidays (defined in the CAC Access application) these modes of operation are not applicable

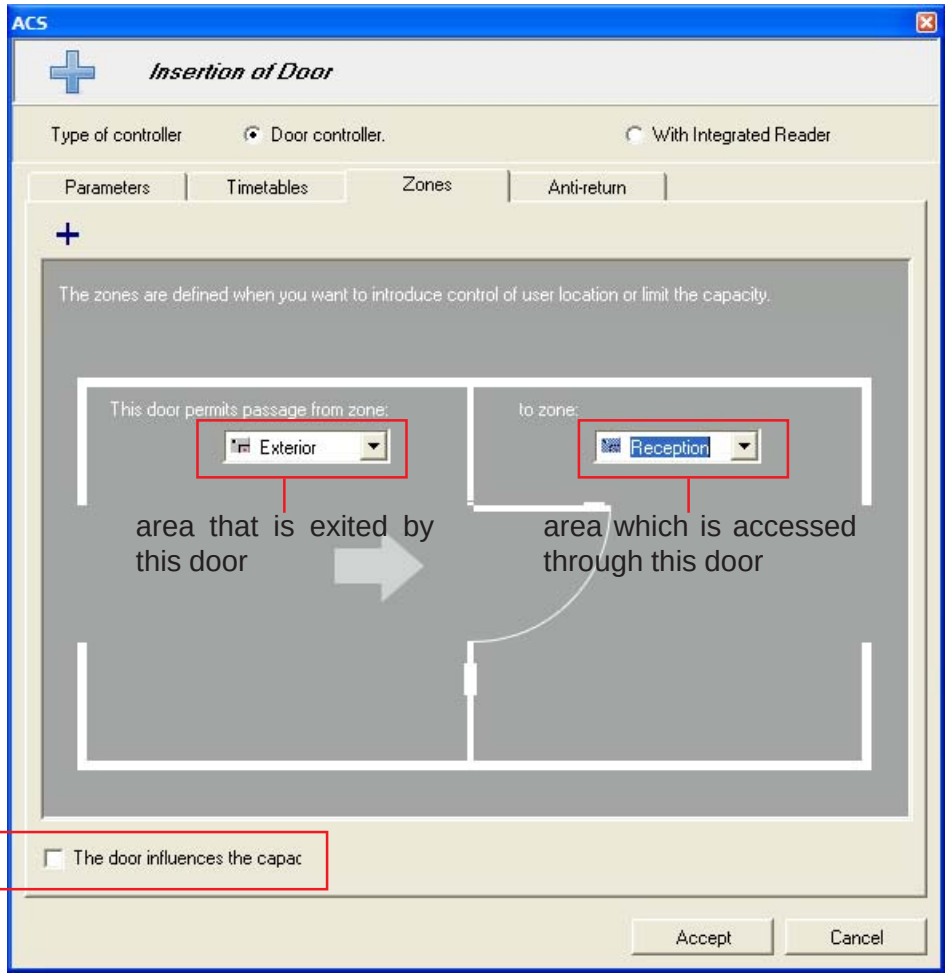
Areas

It is not compulsory to define them. This will only happen in the event requiring function **capacity restriction** (maximum capacity of users in an area).

In order to take advantage of these functions, it is necessary to indicate, on each door, if the door allows entry or exit from an area.

The areas of the installation must be created previously from the element "Areas" of each central unit. They can also be created directly from this screen pushing the button "+".

The steps for creating areas are explained in the section aimed at the element "Areas".



* ***The door influences capacity:*** If this option is enabled, it will be indicated that the door influences capacity of the area which is accessed or exited.

With the option "influences capacity" enabled:

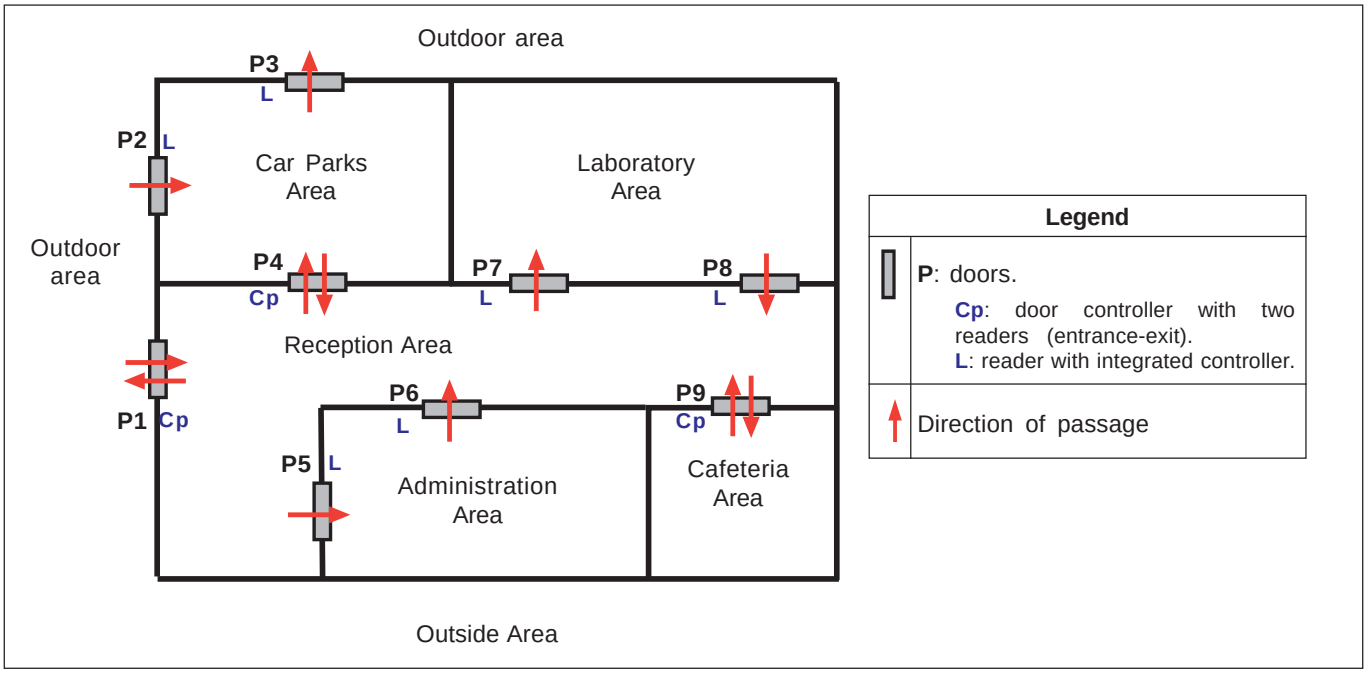
- *The capacity of the area,* indicated in the field "to area",*will be increased by 1*, when a user (after producing a valid identifier) accesses the area through this door.

- *The area capacity,* indicated in the field "This door allows passage from the area:", *is decreased by 1*, when a user (after producing a valid identifier) leaves the area through this door.

The capacity always increases or decreases when it has reached a maximum capacity for the area (see section Areas).

Example configuration of parameter Areas:

The following example shows how the installation doors are configured in the diagram when requiring the functions of capacity control:



For this installation 5 areas have been defined, as well as the "Outdoor" area (defined by default in the Server application):

- Reception Area
- Parking Area
- Administration Area
- Laboratory Area: with restricted capacity.

Cafeteria Area: with restricted capacity.

Configuration of the area parameter of the doors:

Door	This door allows passage from the area:	to the area:	Door influences capacity
P1	Outdoor Area	Reception Area	No
P2	Outdoor Area	Parking Area	No
P3	Parking Area	Outdoor Area	No
P4	Parking Area	Reception Area	No
P5	Reception Area	Administration Area	No
P6	Administration Area	Reception Area	No
P7	Reception Area	Laboratory area	Yes, door access area: increases capacity by 1
P8	Laboratory area	Reception Area	Yes, door exit area: decreases capacity by 1
P9	Reception Area	Cafeteria Area	Sí, (*)

(*) The doors that have provision of a door controller can be used as much for entry as for exit with a single controller (entrance and exit reader in the same door controller), which, depending on the direction of flow will take into account the exiting area and the area to which access is gained, increasing or decreasing the capacity counter of the corresponding area.

The entrance reader is situated in the indicated area with "This door allows access from the area" and the exit reader in the area is indicated with "to the area".

Anti-paspack

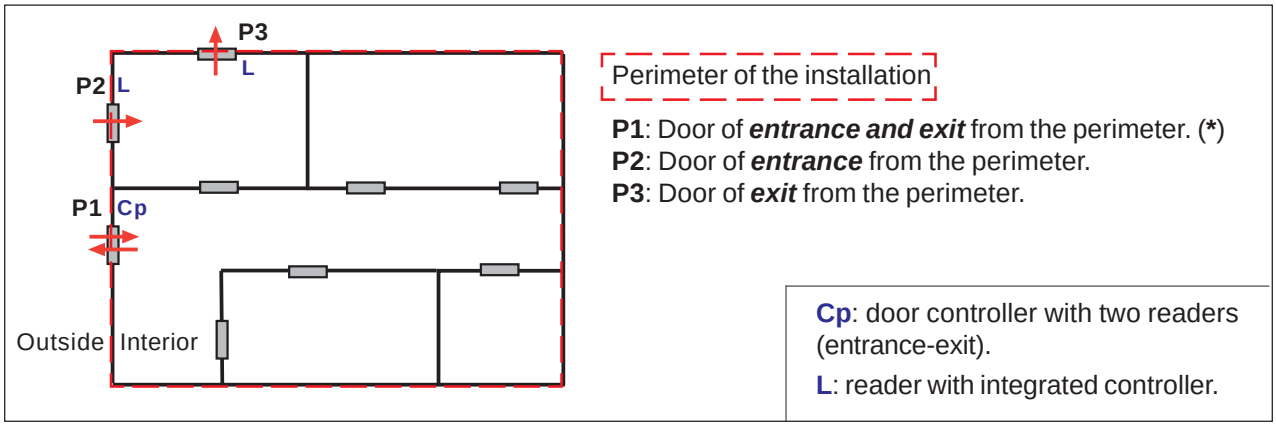
The anti-passpack function prevents a user who has accessed the installation, by means of an *entrance door*, the installation may be re-entered (through any other entrance door), unless they have previously exited the installation by an *exit door*.

In this way various people are prevented from accessing the installation with the same user device, in the same way that various cars are prevented from accessing the carparks with the same identifier, so providing better security to the installation.

The CAC system permits the anti-passback function to be carried out in a very simple way and at a global level for the whole installation. In order to do this it is only necessary to define the perimeter of the installation where the antipassback function is required to be introduced.

The perimeter of the installation is defined by the doors of the installation, configured thus ***entrance to the perimeter*** o ***exit from the perimeter*** from the installation.

Therefore, in order to set up the antipassback function, for each door to form part of the perimeter, it is necessary to indicate if they are doors which permit ***entry*** or ***exit*** from the same.



(*) Since the doors that have a door controller can be used for entry and exit with a single controller (entrance and exit reader in the same door controller), depending on the direction taken it will take into account if the user enters or exits the facilities (it thus appears in the option. **Entrance and Exit**).

Two levels of anti-passback: pedestrian and vehiclar

In order to increase security, the CAC system incorporates two levels of antipassback, one pedestrian and the other vehicular, which apply automatically in accordance with the type of door through which the perimeter of the installation is accessed..

Access through a pedestrian door:

When a user enters into the perimeter (by a pedestrian door marked as 'entrance' to the same) remains marked as 'within' the installation since passage is not permitted through any entrance door to the perimeter, whether a pedestrian or vehicular door.

Of course the passage through exit doors or doors that do not belong to the perimeter is permitted.

When going through an 'exit' door from the perimeter, you are marked as 'outside the installation', being able to access the installation again through any entrance door to the perimeter.

Access through a vehicular door:

If, on the other hand, the user accesses the perimeter by a vehicular door, the system ***marks the user and their vehicle as inside the installation***, so entering again through a vehicular entrance will not be possible unless previously exited by a vehicle exit access.

Of course, exit doors or those that do not belong to the perimeter are allowed.

In the event of passing through a door of *pedestrian exit* from the perimeter, the user will be able to access the perimeter again only by pedestrian entrances, and not vehicular ones, given that the vehicle is still within the installation.

Thanks to the two levels of antipassback the example in figure 1 may be solved in two different ways:

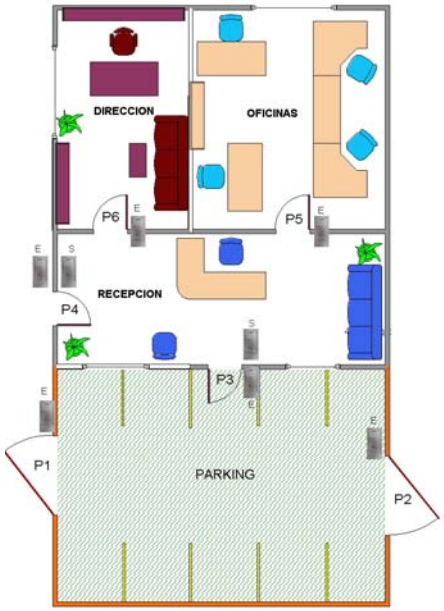
OPCIÓN A: Using a single level of antipassback

The access doors to the carpark are defined (P1 and P2) as belonging to the perimeter (P1 entrance y P2 exit) and the access doors P3 and P4 to a restricted area, therefore users without permission will not be allowed access to it. If a user uses his identifier for entry with their vehicle by P1, they will not be able to re-enter that door, but of course they will be able to re-enter through the rest of the doors of the installation (if their identifier allows it). When leaving the carpark with their vehicle by P2, access will again be possible through P1. In this case antipassback control will not be in reception.

OPTION B: Using two levels of antipassback

The access doors to the car park are defined as vehicular doors of access to the perimeter and door P4 as a pedestrian access to the perimeter. When a user accesses by a parking entrance (necessary to bring their car in order to do this) the user as much as the car are marked as within the installations. At this time they will be able to access only through P1 if they have exited previously through P2 or been excused by antipassback. Regardless as to whether they have exited through P2, the user will always be able to exit on foot through P4 and re-enter through the same door but never through the parking entrance P1. In the same way that, once inside the installation (through P1 or P4) the user will not be able to re-enter through any of the perimeter accesses.

Figure 1



In this example the capacity restriction function may be combined also to existing carpark spaces. In order for this to happen it should be indicated that door 1 permits passage from the 'Outside' area (defined as default) to the 'Parking' area and door 2 allows passage from the 'Car Park' area to the 'Outdoor' area.

Characteristics of the antipassback function

- In the event of having more than one central unit in the installation, this information is shared by all the central units that can be found on the same network, therefore it is possible to set up the antipassback function in a global manner in the whole installation.

  As an example, let's suppose we are a university campus that has 3 distant car parks, each one controlled by access of vehicles connected to different central units. When a user enters with their vehicle into one of the carparks through an entrance access, they will be marked as within the perimeter. If trying to enter their identifier to enter into another car park, they will not be able to given that all the central units have that information.

- All this information is stored in a non-volatile memory, in such a way that a power outage (or a failure of the *backup*) will not allow the users outside the installation.

- *Antipassback pardon*: In case of inappropriate use of the system on the part of the user, like the exiting of the installation without introducing the identifier or using the exit of another user, that user will not be granted access the next time they try to attain it, given that the system has marked that user as 'within the installation' (has not validated their exit by any exit reader).

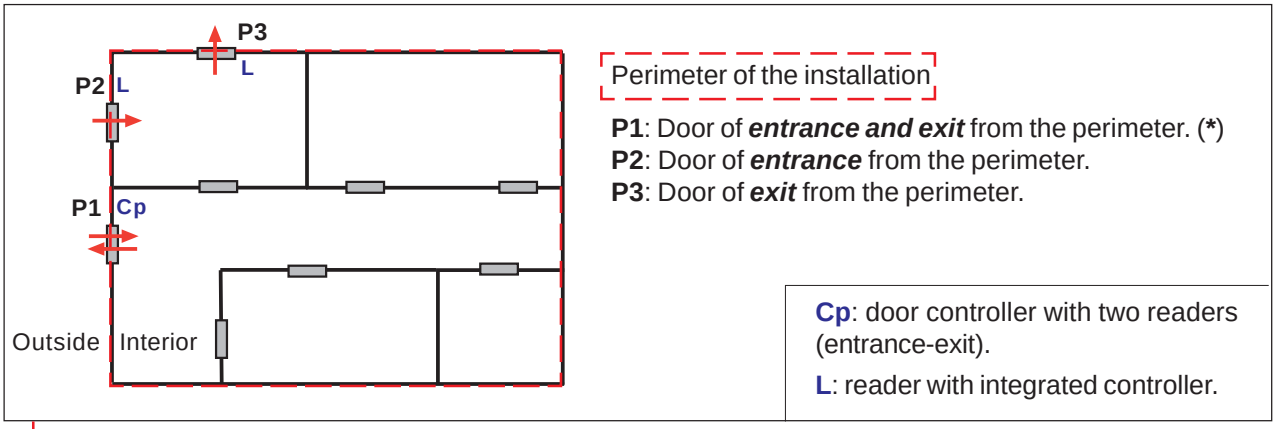
  In order to avoid these problems, it is possible, using the Server application, to determine a time of day (normally during the night) for placing all users automatically outside the perimeter (see section "Control Panel >> Antipassback pardon time").

- It is possible to determine the marking of the user as within the perimeter on the condition that the door is open, in such a way that if the door does not open, the user will not be considered as inside. In order to do this it is necessary to use the door sensor.

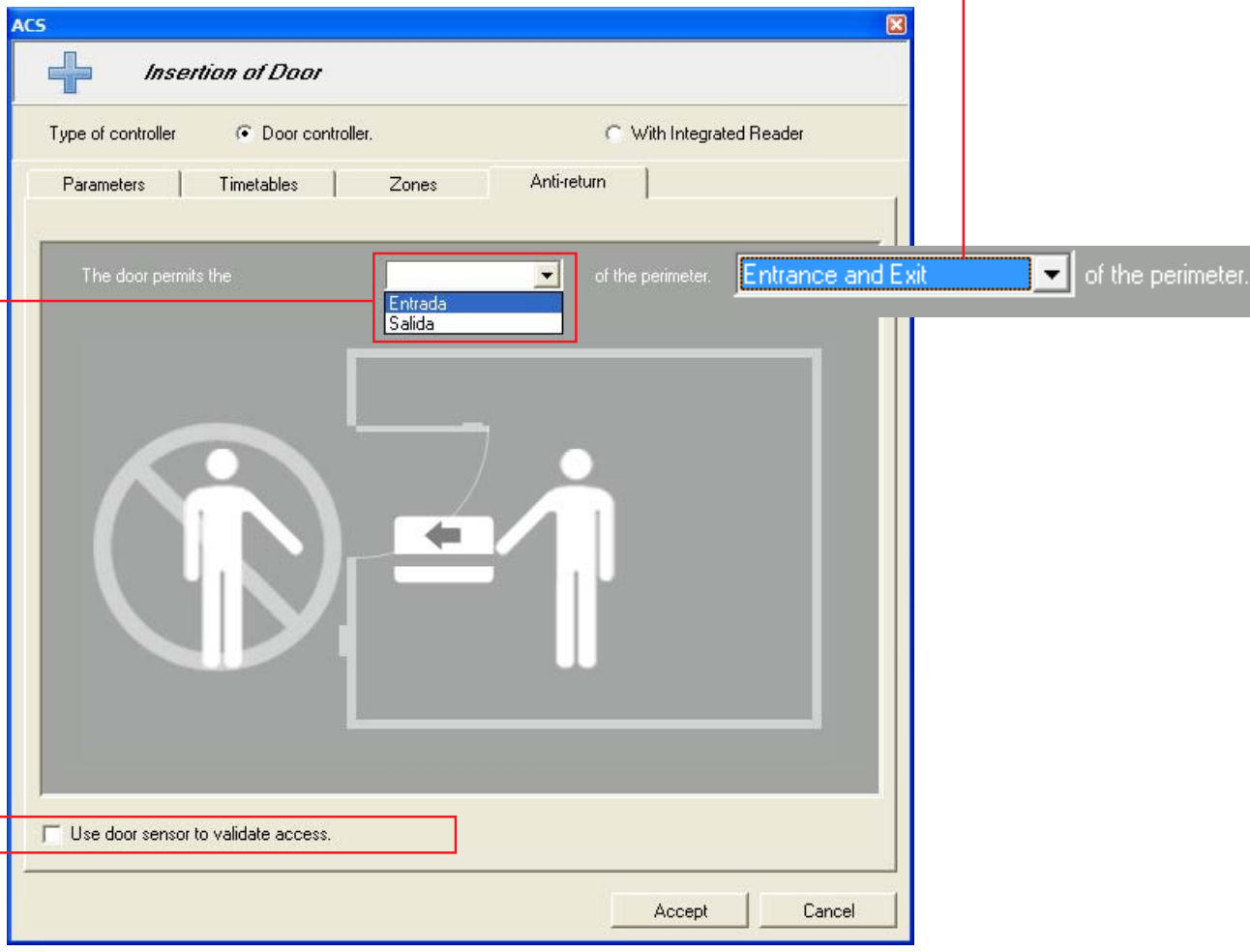
- The antipassback function is available to any identifier (proximity, keypad,..)

**** How to set up the antipassback function***

To carry out the antipassback function (at global installation level), it is necessary to define each door that forms part of the perimeter of the installation, if they are doors that permit ***entry*** or ***exit*** from the same.



(*) Since the doors that have a door controller can be used for entry and exit with a single controller (entrance and exit reader in the same door controller), depending on the direction taken it will take into account if the user enters or exits the facilities (it thus appears in the option. **Entrance and Exit**).



* ***Using the door sensor to validate access:*** If this option is enabled, the system will not consider the user to be inside the perimeter of the installation until the door opens. In this way the situation is prevented where a user - who may have entered a valid identifier into a perimeter door and for whatever reason decides not to enter it (i.e. not open the door) - remains registered within the installation and is not able to enter it later (antipassback).

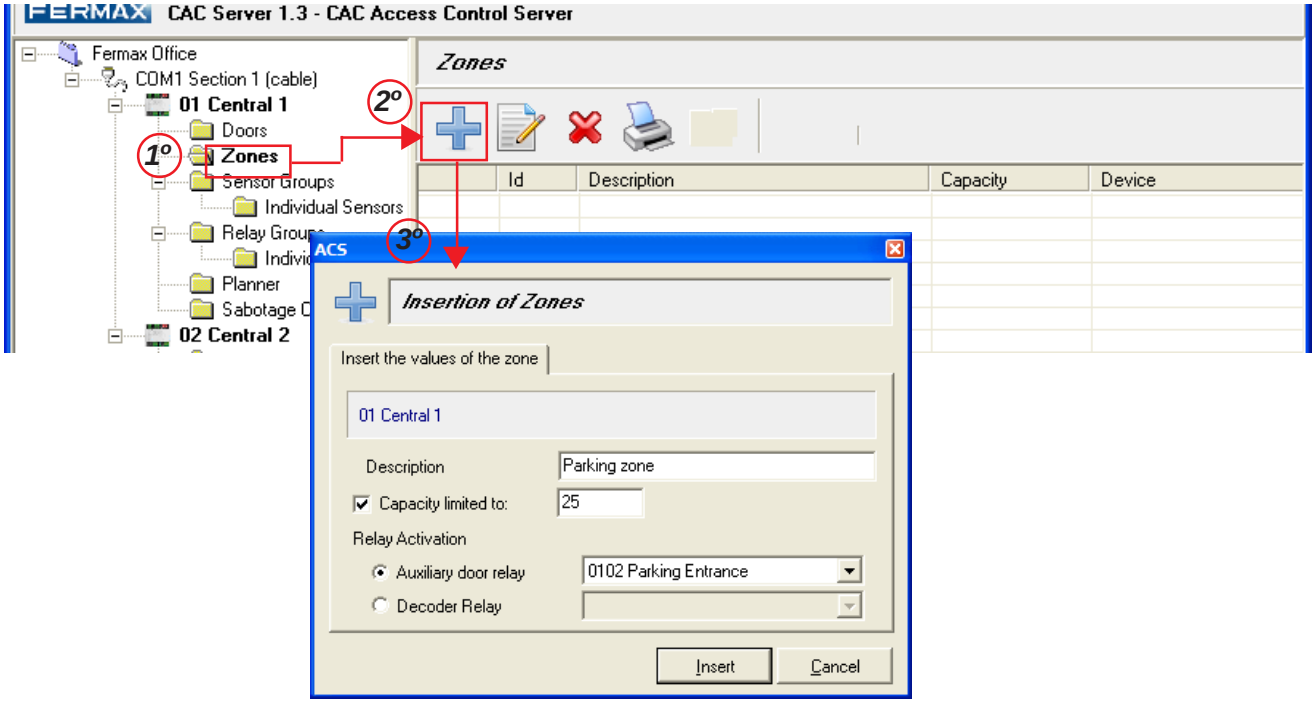
In order for this to happen, as well as enabling the option it is necessary to use the door sensor. In the case of vehicular access it is very interesting to apply it.

AREAS

It is not compulsory to define them. This will only be done in the event of requiring use of the function of **capacity restriction** (maximum capacity of users in an area).

In the information on Doors (described in the previous section), in the event of requiring use of these restriction of capacity functions or capacity control, each door should indicate the ***area*** to which access is permitted and the ***area*** that is vacated through this door. n order to select these areas in each door, it is necessary to create and configure previously, the areas of the installation. This section shows how.

The CAC system allows creation and management of up to 32 areas through each central unit:



*** * *Description:*** Name assigned to the area (the name of the area may not be repeated).
This description will identify the area in the server and client applications of the installation.

* ***Restricted capacity to:*** Activate this box if the function "restricted capacity" is required, that is to say, it assigns a maximum capacity of users to the area, and enters into the box the maximum capacity of the area

On reaching this maximum capacity, access for more area users is not permitted, until some of the users leave the area or a capacity reset is carried out.

A relay may be assigned to the area which will become activated whenever maximum capacity of the area is reached.

Also, a capacity of "0" may be defined; in this case the number of users in the area is not restricted, the selected relay activating itself while there is a user in the area.

* ***Relay activation:*** allows selection of the relay which will become active when maximum capacity of the area is reached.

- **Auxiliary door relay:** activate this option and select (from the list displayed) the door controller that will activate its relay after reaching maximum capacity for the area.
- **Relay decoder:** activate this option and select (from the list displayed) the relay output that will become active after reaching maximum capacity for the area.

  The displayed lists show the available relays. The relays and door controllers (auxiliary relay) should be defined previously in the Server application.

If the area does not have exit readers and this is carried out in a controlled way, the capacity counter will not decrease and should do this from the CAC Access application or through a profile identifier "capacity reset".

A user counted in the area may enter many times without increasing the capacity further.

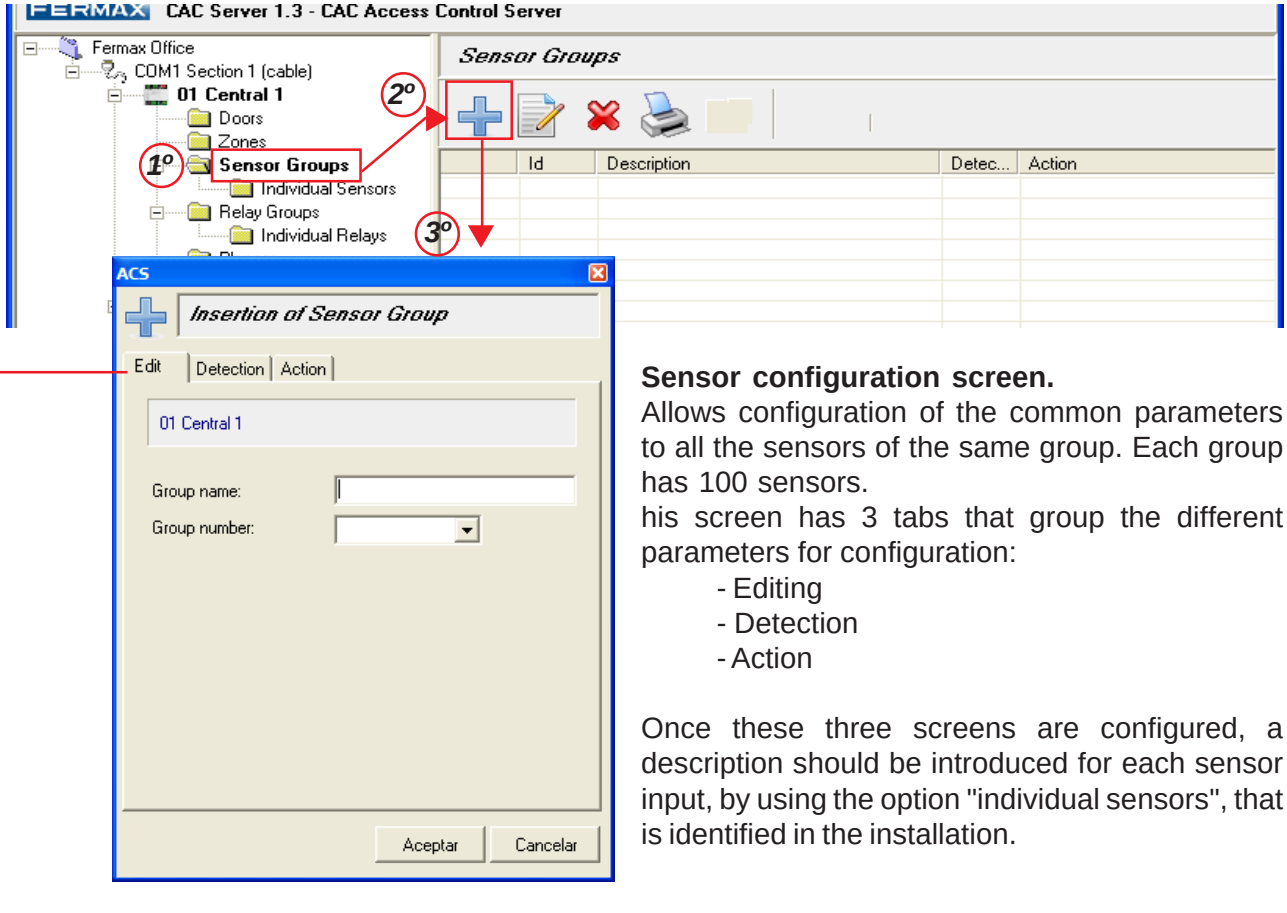
SENSOR GROUP

Permits definition of the sensor decoders of the installation and configuration for the operation of each one of them.

Previous to configuration of sensor decoders from the CAC Server, it is necessary to have programmed them by means of the Decowin application, supplied with the CAC central unit, (if not - provided from the guard unit):

- the addresses of each sensor input of each one of the decoders
- time of detection: instantaneous or timed.

Once the decoders are programmed, they are defined and configured in the Server application:



Sensor configuration screen.
Allows configuration of the common parameters to all the sensors of the same group. Each group has 100 sensors.
his screen has 3 tabs that group the different parameters for configuration:

- Editing
- Detection
- Action

Once these three screens are configured, a description should be introduced for each sensor input, by using the option "individual sensors", that is identified in the installation.

Edition

*** *Group name:*** Name assigned to the sensor groups (the name of a group may not be repeated). This description will identify the group in the server and client applications of the installation.

* ***Group number:*** Select the ***sensor group*** that is going to be used for a specific function (for example, activate a relay when a sensor becomes active, send messages to the guard unit etc.)

Sensor group: The sensor input of the decoder sensors are programmed (using the application Decowin) with addresses of three digits that range from 000 to 999.

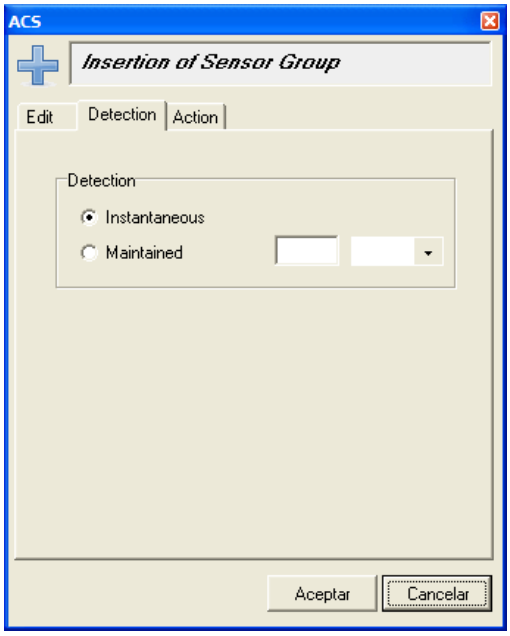
The sensor groups "0" correspond with the sensor inputs programmed 000 to 099: group "1" corresponds with the sensor inputs 100 to 199: and so on.

On defining the sensor group in the Server application, it indicates that decoders exist whose inputs are programmed with addresses belonging to each group. In this way the application knows of the existence of these decoders in the installation.

The parameters and configured functions in the following screens apply to all the sensor inputs belonging to the group.

Detection

In this screen the type of detection of the sensor input corresponding to the group is indicated, that is to say, the time that the sensor has to be activated (detecting) in order to generate an alarm or carry out the action configured for the sensor:



* ***Instantaneous:*** If the sensor input detects an activity in its input, it will communicate the aforementioned detection immediately to the CAC system (to the central unit to which it is connected), and it will carry out the action associated to the sensor groups.

* ***Maintained:*** The sensor should be activated continually during the time indicated on the box, in order to communicate such a detection to the CAC system and carry out the action associated to the sensor group.

  If detection ceases before completing the detection time indicated, the associated action will not be carried out.

  The maintained detection time, entered on the box, may be selected in seconds or minutes.

IMPORTANT NOTICE

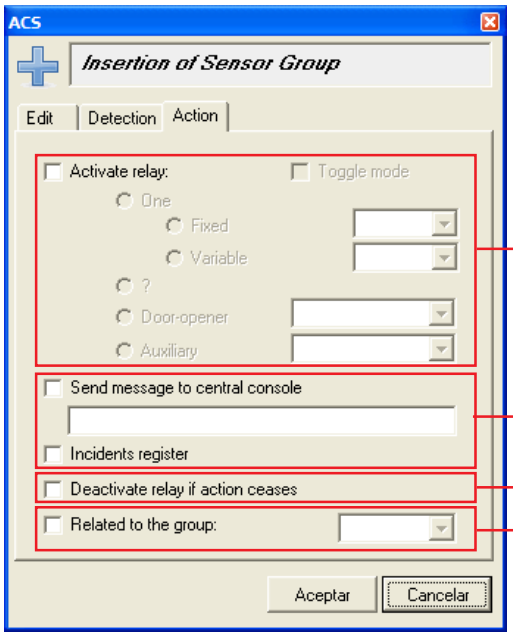
As can be observed, the parameters defined here, have already been programmed previously in the sensor decoders for each one of their inputs, using the Decowin application.

The type of "detection" selected on this screen should coincide with that programmed in the decoder using the Decowin application.

If the type of detection is modified on this screen, so that the sensor inputs of the correspoding decoders are updated, the central unit should be updated (see section "Updating data of the central unit") from the Server application, and subsequently from a guard unit connected to the installation, entering individual programming of decoders and confirming each one of the programmed outputs belonging to the group; or using the Decowin application reprogramming the corresponding decoders again.

Action

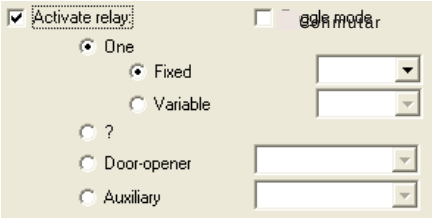
In this screen the action or actions are configured that the CAC system will carry out following a detection (instant or maintained) of one of the sensor inputs belonging to the defined sensor group.



Actions associated with sensor detection:

- Activate/switch relays
- Generate incidents and warnings
- Sinchronizing relay activation with sensor detection
- Double detection.

* ***Activate relay:*** If this box is enabled on carrying out a detection, it will be activated or it will switch in a relay, a group of relays or various relays according to the options selected:



- **One:** Indicates that on activating any sensor input or defined group, ***a single relay output will be activated*** from a relay decoder:

  · **Switching:** If this box is activated the action associated with the relay group is that of ***switching the state of the relay***, if it does not the associated action is that of activating the relay.

  Fijo: For each sensor activation, ***the same relay is always activated*** *(relay output)* selected from the list displayed (the displayed list shows all the *individual relays* defined in the application).

  Example: *- Defined sensor Groups: 1.*
  - Fixed Relay to activate/switch, selected from the displayed list: 105. ***(*)***
  - Functioning: If any sensor input of group 1 is activated (entrances programmed with an address between 100 and 199) it will always activate/switch relay 105.

  · **Variable:**For each activation of a sensor input, the relay output is activated from the relay group selected from the list, whose two last figures of address coincide with the two last figures of address of the activated sensor:

  Example: *- Defined sensor Groups: 1.*
  - Relay Group selected from the list: 4. **(*)**
  - Operation: If sensor 125 is activated the relay output 425 will be activated.
  If sensor 101 is activated relay output 401 will be activated.

  Notes
  (*) Each relay decoder of the installation must have its ouputs programmed (using the Decowin application) with 3 digit addresses (000 to 999) and the corresponding relay Groups and individual Relays defined on the Server application.
  The activation of the relay output will be carried out during the programmed time for each relay output decoder.
  In the case of switching relay, the activation time programmed for the decoder outputs of relays must be "0".

- **Various:** Indicates that on activation of any sensor input, ***all the relay outputs of the relay group will be activated***whose group number coincides with the defined sensor group.

  Example: *- Defined sensor Groups: 1.*
  - Operation: If any sensor input from group 1 is activated (for example: 108), all of the group of relay outputs of relay group 1 will become active, that is, all the relay outputs programmed in the relay decoders with address 1XX (during the time programmed for these relay outputs).

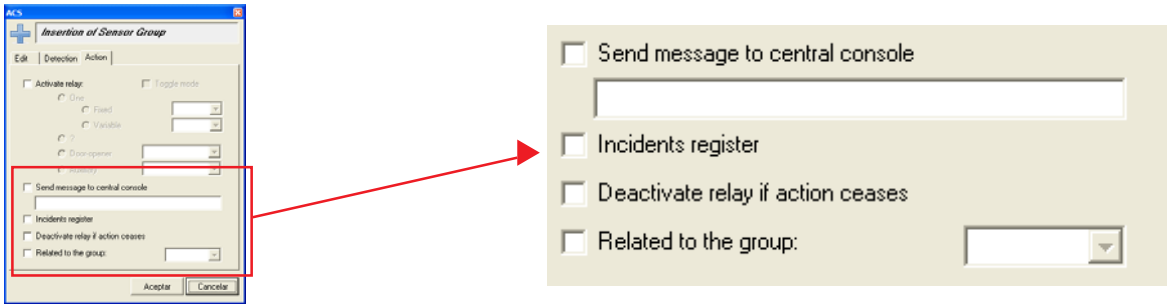
- **Door opener:** Indicates that on activation of any sensor input of the group of sensors, ***the door opening relay will activate, from the door*** selected from the displayed list (the list shows all the defined doors in the installation).

  Example: *- Defined sensor Groups: 1.*
  - Door opener, selected door: Company entrance.
  - Operation: If any sensor input of group 1 is activated (entrances programmed with an address between 100 and 199) the door opener relay of the door defined as "Company Entrance" will activate.

- **Auxiliary:** Indicates that on activation of any sensor input of the group of sensors, ***the auxiliary relay of the door*** selected from the displayed list will activate

  The list only shows doors which have the type of controller: ***door controller***.

  Example: *- Defined sensor Groups: 1.*
  - Auxiliary, Door selected: Car park Entrance.
  - Operation: If any sensor input of group 1 is activated (inputs programmed with an address of between 100 and 199) the auxiliary relay of the door defined as "Car park Entrance" will activate".



* ***Send message to the central console:*** If this box is enabled, on activating any sensor input of the sensor group, ***is sent*** the discreet message in the lower box to the reception area of the installation.

* ***Incident register:*** If this box is enabled, on activation of any sensor input of the sensor group, ***they are sent*** and registered, in the CAC central unit, the incidents of activation and deactivation of the corresponding sensor output..

The incidents registered by the central unit are seen from the client applications.

* ***Deactivation of relay if action ceases:*** If this box is enabled, the activation of the relay or group of relays associated to the sensor group, will be disactivated when detection of the sensor stops.

For this function, relays programmed with bi-stable function (time of activation "0" for the relay decoder or "255" for the auxiliary relay of the door controller), in such a way that the relay will only deactivate when detection of the sensor stops.

If the activation time programmed for the relay is less than the detection time of the sensor, the latter will deactivate before detection of the sensor stops.

* ***Related to the group:*** Permits linking of the actual sensor group with another group of sensors, selectable from the displayed list.

So that this option functions properly the link should be reciprocal, that is, if sensor group 1 is linked with sensor group 3, it is necessary to link group 3 with group 1.

Operation

The operation of linked sensors is the following (As an example sensor group 1 will be linked with sensor group 3 and viceversa):

Each sensor of a group will pair up (link) with the equivalent of the other group, for example sensor 125 will link with sensor 325, and 143 with 343 etc.

When the linked sensors are detected simulaneously, the action associated to the group of the last sensor acitvated will be carried out. ***This action is registered as an incident in the system.***

Example:
- Sensor 125 activates: nothing happens the incident will only be registered if the option is enabled).
- Sensor 325 activates (while sensor 125 is active): the action assigned to sensor group 3 will be carried out.

The actions that can be carried out on generating the simultaneous detection are:

- *Activation of the relay* or relay group assigned to the sensor group activated last of all.
- *Sending the message to the central console* assigned to the group of sensors activated last of all.
- *It is important that the relay that is defined is to the same one in the two groups.*

The rest of the actions available for each sensor group, are carried out individually at the moment of activation/deactivation of the corresponding sensor:

- *Register of the incidents*: if it is activated, the activation/deactivation of the corresponding sensor is registered.
- *Deactivates relay if action ceases* : if it is activated, on ceasing the detection of the sensor, the active relay assigned to the sensor will deactivate.

Individual Sensors

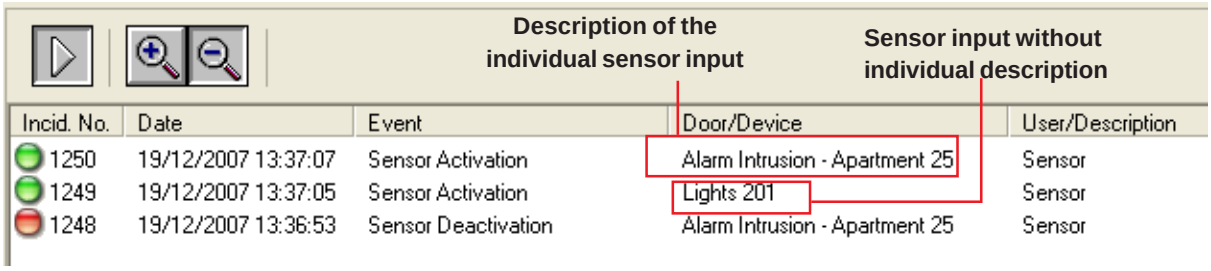
Permits individual description of each one of the sensor inputs of the sensor decoders of the installation.

* Why define individual sensors:

- to identify the sensor, which has started an event, in a much easier way.

  for each sensor input a description (name of sensor) is introduced that will identify it in the installation and in the different client applications.

  In this way, on producing an event in one of the individually defined sensor inputs, the registered incident will show the assigned description to the sensor, if not it will show only the address of the sensor:

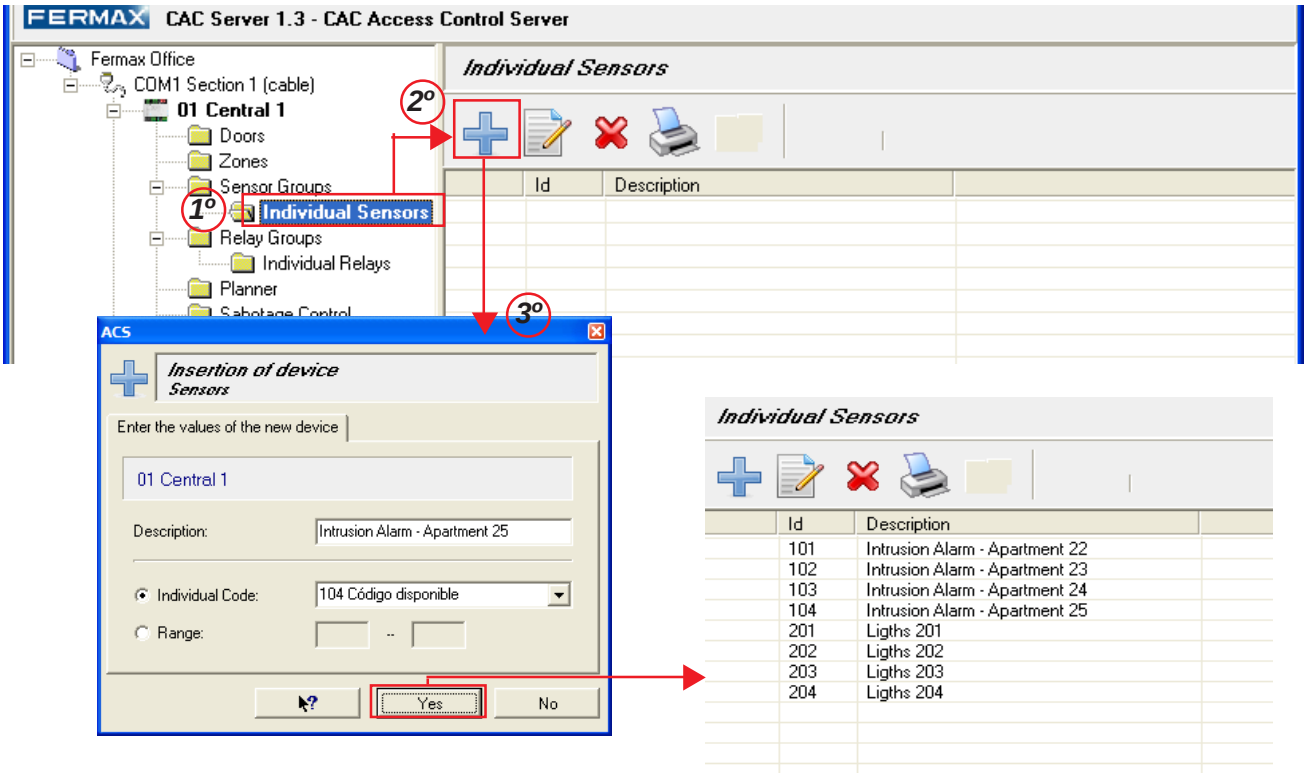


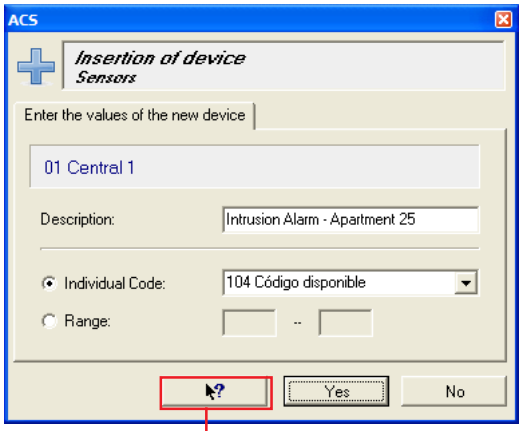
(display for register of incidents of the CAC Access application)

- Describing the sensor inputs individually, subsequently permits individual sensor inputs to be selected and assigned (in other options of the Server application, as in the case of the Planner) or in client applications (assigning a sensor to a user as activated/deactivated, control of sensors etc.)

* Mode of operation of the individual sensors:

The mode of operation of the individual sensors depends on the configuration made for the sensor group which contains it (see section Sensor Groups).



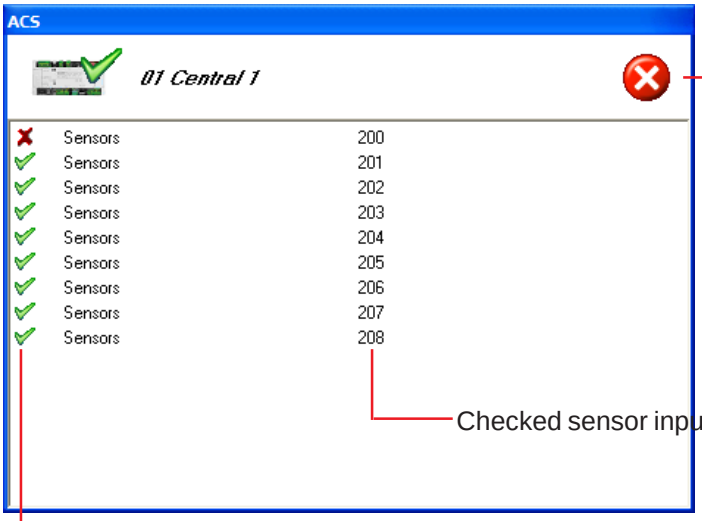


* ***Description:*** Description assigned to the sensor input or range of sensor inputs.
This description will identify the sensor input in all the server and client applications of the installation.

* ***Individual code:*** Allows selection of the sensor input to the one which is assigned the description. The list shows the addresses of all the selectable sensor inputs.

* ***Range:*** Permits the entering of a range of sensor inputs (initial address-final address) to those that are assigned the same description. For example, sensor inputs with addresses from 201 up to 205.

Carry out a test of the sensor input or selected range, by means of the decoder bus, in order to check that they exist in the installation:



Close test screen.

Checked sensor input addresses.

Test result:

Sensor input detected.

Sensor input not detected.

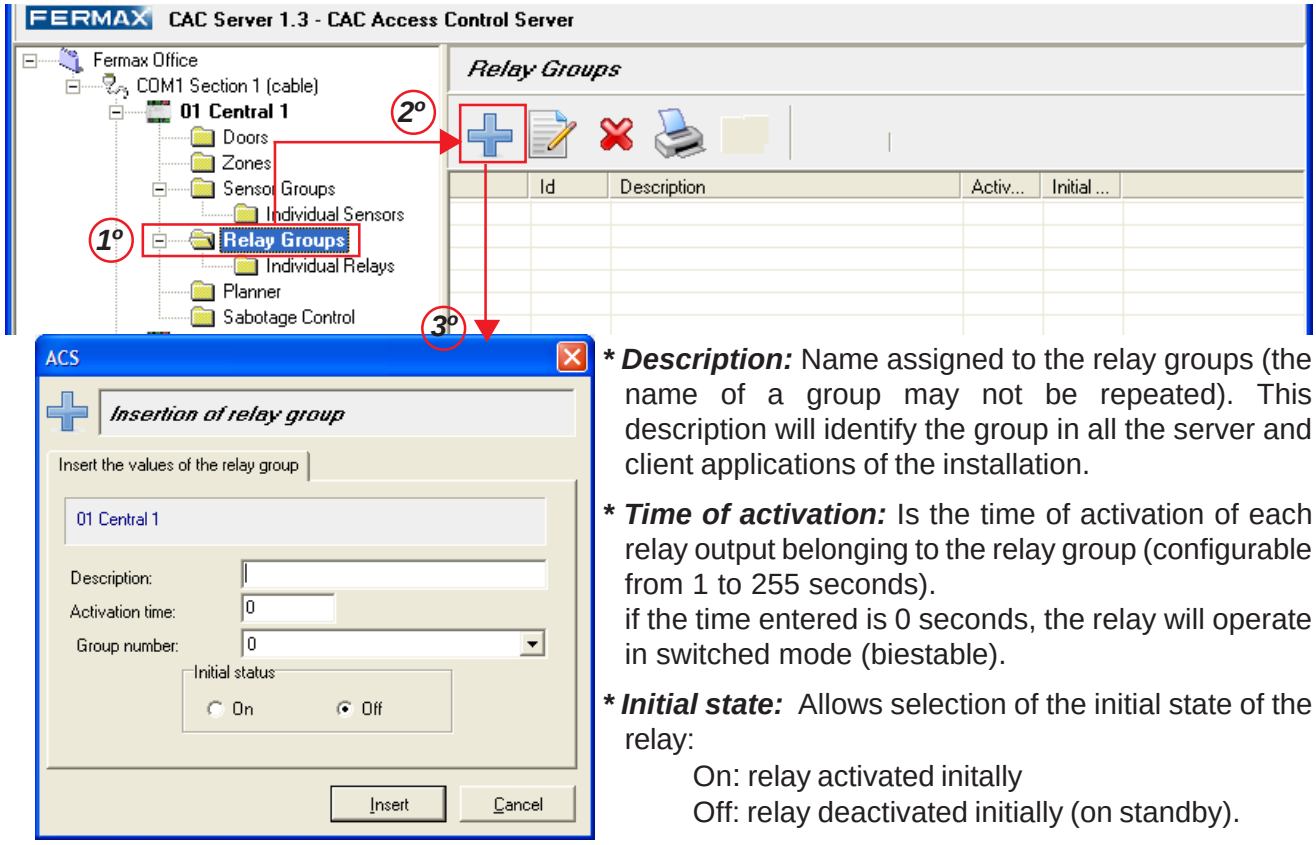
RELAY GROUP

Permits definition of the relay decoders of the installation and configuration of the operation of each one of them.

Previous to the configuration of the relay decoders from the CAC Server application, it is necessary to have programmed them using the Decowin application (supplied from the CAC central unit):

- the addresses of each relay output of each one of the decoders
- the time of activation.
- and its initial state: On (activated), Off (deactivated).

Once the decoders are programmed, they are defined and configured in the Server application:



* ***Description:*** Name assigned to the relay groups (the name of a group may not be repeated). This description will identify the group in all the server and client applications of the installation.

* ***Time of activation:*** Is the time of activation of each relay output belonging to the relay group (configurable from 1 to 255 seconds).
if the time entered is 0 seconds, the relay will operate in switched mode (biestable).

* ***Initial state:*** Allows selection of the initial state of the relay:
On: relay activated initally
Off: relay deactivated initially (on standby).

* ***Group number:*** Select the ***relay group*** that will be used for a specific function (for example: activation of lights, activation of the siren alarm, maximum capacity warning etc.). A group consisting of 100 relays.

Relay group: The relay outputs of the relay decoders are programmed (using the Decowin application) with addresses of three digits that range from 000 to 999.

The relay group "0" corresponds with the relay inputs programmed as 000 to 099; group "1" corresponds with the relay inputs 100 to 199; and so on successively.

On defining the relay group, in the Server application, it is indicating that decoders exist whose outputs are programmed with addresses belonging to this group. In this way the application knows of the existence of these decoders in the installation.

IMPORTANT NOTICE

As can be seen, some of the parameters defined here have already been programmed previously in the relay decoders for each one of their outputs, using the Decowin application.

The values entered into the fields "Time of activation" and "initial state" of this screen should coincide with those programmed in the decoder using the Decowin application.

If these parameters are modified on this screen, so that the relay outputs of the corresponding decoders are updated, the central unit should be updated (see section "Updating data of the central unit") from the Server application, and subsequently from a central unit of the guard unit/reception area connected to the installation, entering individual programming of decoders and confirming each one of the programmed outputs belonging to the group; or using the Decowin application to reprogram the corresponding decoders again.

Individual Relays

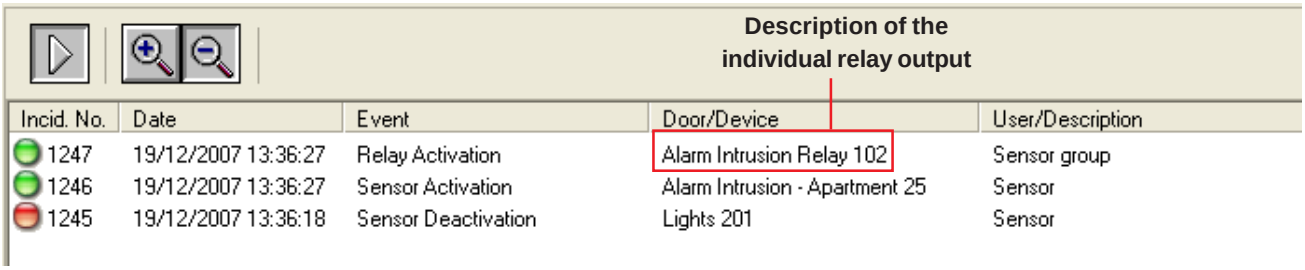
Allows individual description of each one of the relay outputs of the relay decoders of the installation.

* Why describe individual relays:

- In order to identify the relay that has originated an event (activated/deactivated) much more easily.

  For every relay output a description (name of the relay) is entered that will identify it in the installation and in the different client applications.

  In this way, on activation/deactivation of one of the individually defined relay outputs, the registered incident will show the description assigned to the relay, if not, it will only show the relay address:

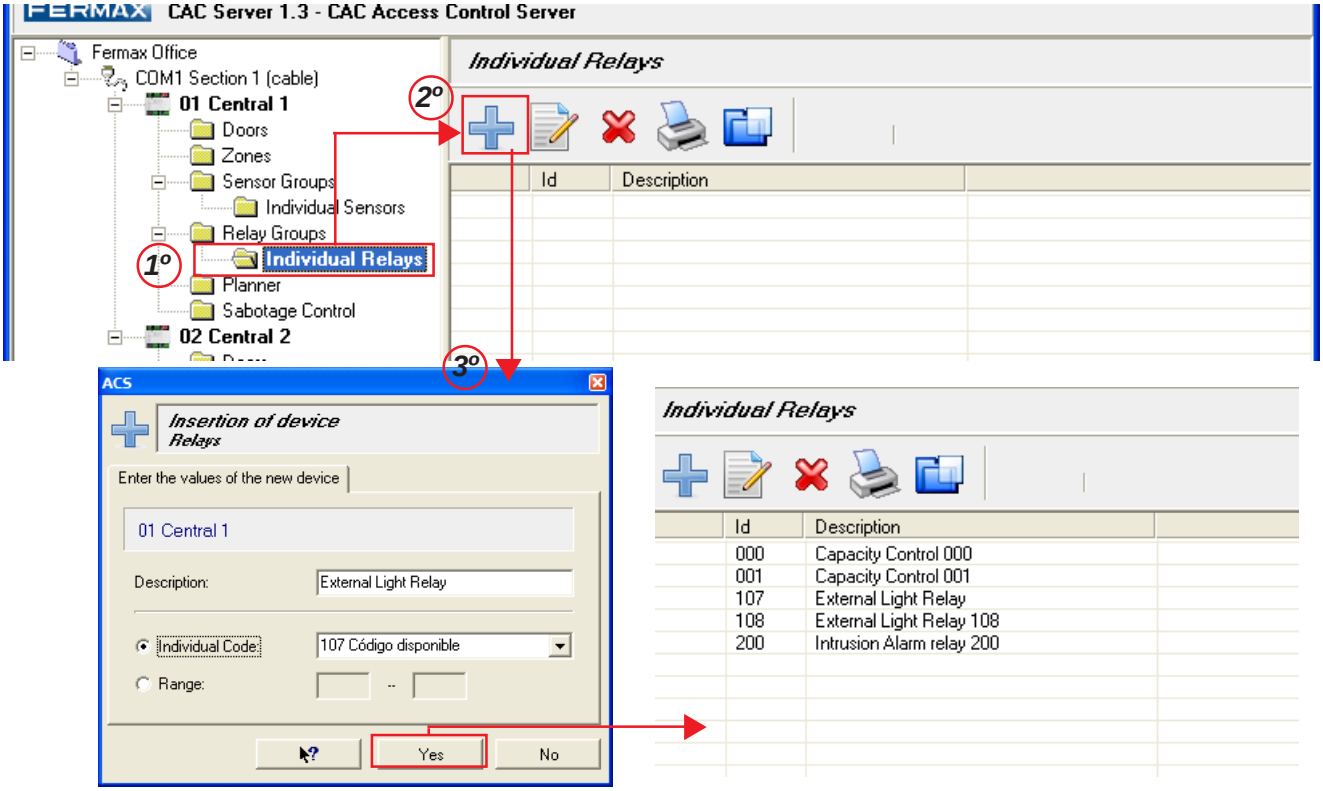


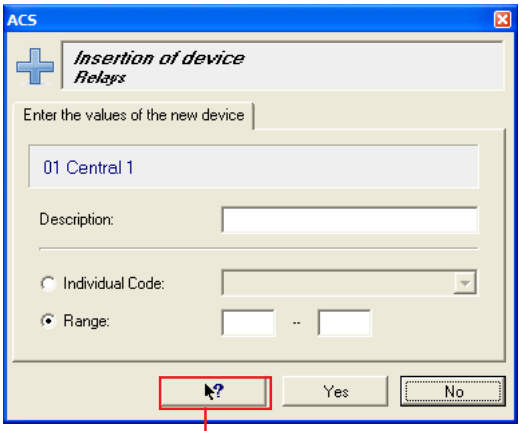
(display for the incident register of the CAC Access application)

- Describing the relay outputs individually, subsequently allows, in other options of the Server application (as is the case with the Planner, Doors, Sensors, etc.) or in client applications (activation of relay by user, control of relays etc.) individual relay outputs to be selected..

* Mode of operation of the individual relays:

The mode of operation of the individual relays depends on the configuration used for the relay group that contains it (see section Relay Groups).



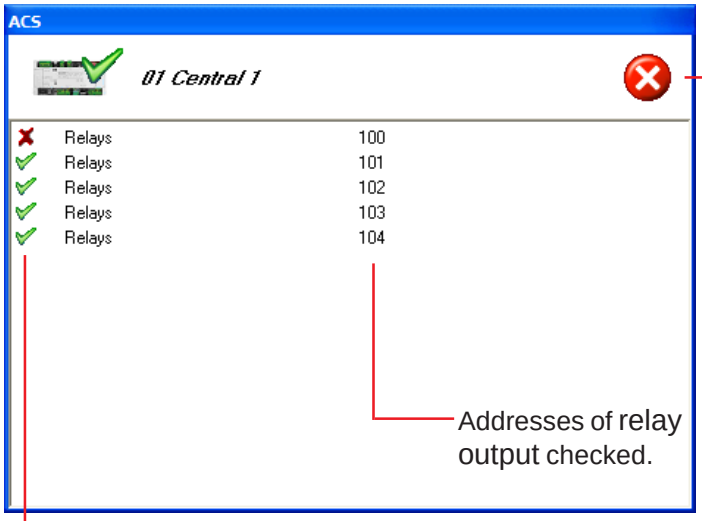


* ***Description:*** Description assigned to the relay output or range of relay outputs.
  This description will identify each relay output in the server and client applications of the installation.

* ***Individual code:*** Permits selection of the relay output to which the description is assigned. The list shows the addresses of all the selected relay outputs.

* ***Range:*** Allows entry of a range of relay outputs (initial address-final address) to which the same description is assigned. For example relay outputs with addresses from 201 up to 205.

Carry out a test of the relay output or selected range, through the decoder bus, in order to check that they exist in the installation:



Close test screen.

Addresses of relay output checked.

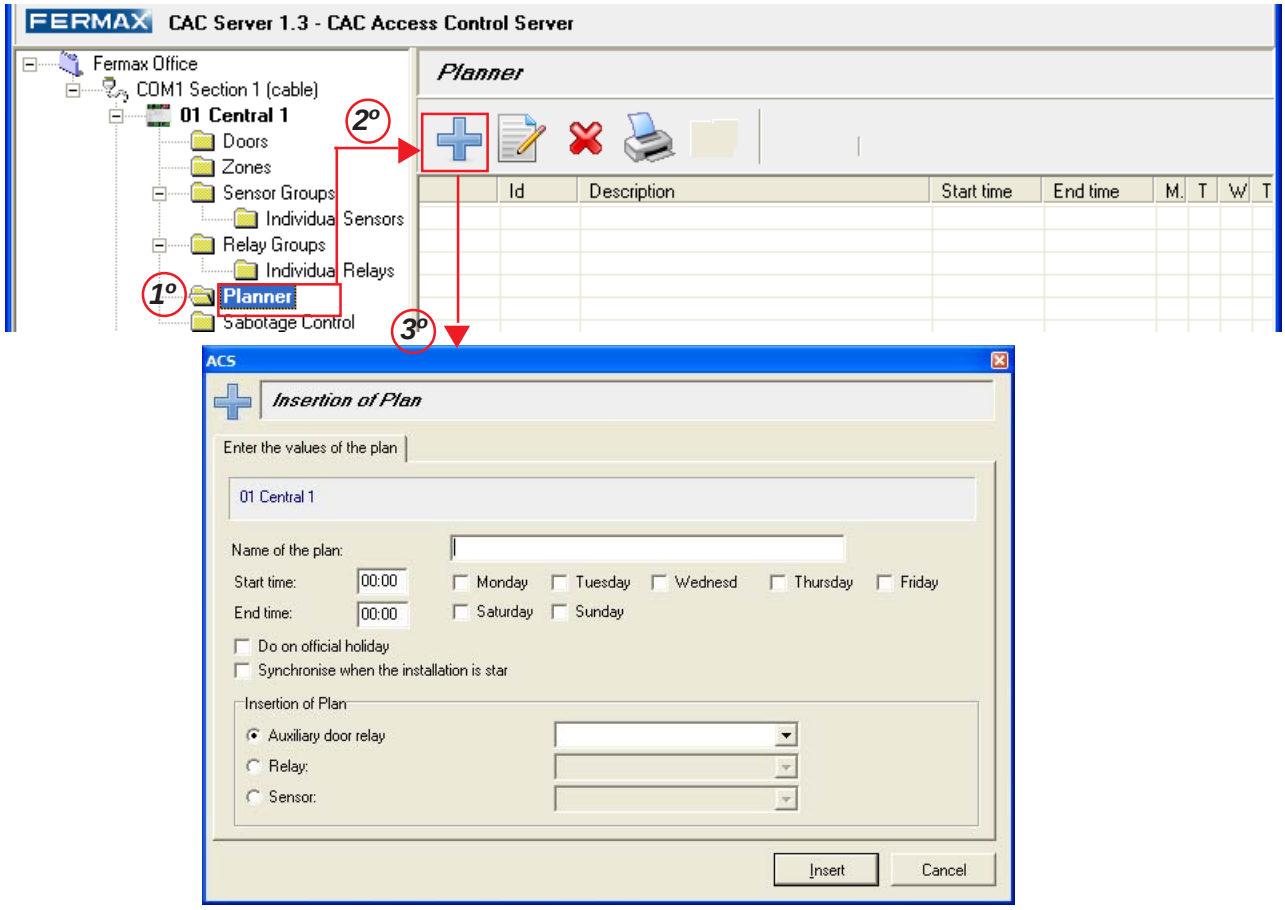
Test result:

Relay output detected.

Relay output not detected.

PLANNER

The CAC system allows up to 32 automation plans to be carried out (through the central unit) for the control of devices.



In every plan the following parameters are defined:

*** *Name of the plan:*** Name assigned to the plan (the name of a plan may not be repeated). This description will identify the automation plan in the server and client applications of the installation.

* ***Initial time:*** Time of initiation of the plan to which a determined action is established. The action to be carried out depends on the element selected in the field "Insertion of Plan":

- *Sensor*: the selected sensor is **disabled**.
- *Relay*: the action depends on its initial state:

Initial state:	Action
Deactivated	Activate relay
Activated	Deactivate relay

* ***End time:*** End time of plan to which a determined action is produced. The action to be carried out depends on the element selected in the field "Insertion of Plan":

- *Sensor*: the selected sensor is **enabled**.
- *Relay*: the action depends on its initial state:

Initial state:	Action
Deactivated	Activate relay
Activated	Deactivate relay

*** *Days of the week:*** Mark those days of the week during which the automation plan will be carried out, at the times indicated.

* ***Carry out on official holiday:*** If this box is activated it will indicate that the automation plan will also be carried out on the official days of holiday programmed using the CAC Access client application, if not the plan will not be carried out on the holidays.

* ***Synchronise on starting up the installation:*** If this box is activated, in the event of a system reset from the CAC central unit (due to a power outage etc.) the plan that should have been carried out during the period in which the central unit stopped operating, will be carried out on restart of the operation of the central unit.

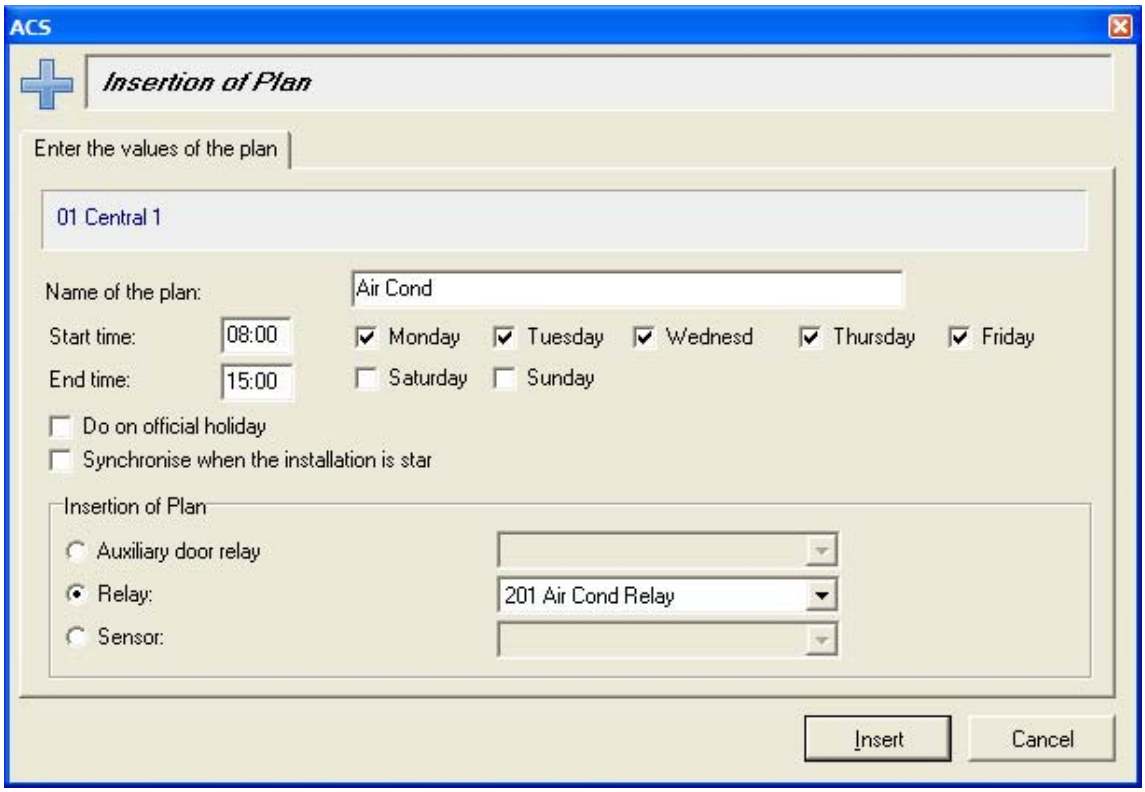
* ***Insertion Plan:*** allows selection of the element that is required to be automated:
  - **Auxiliary door relay:** Permits selection of the door controller that will activate/deactivate its auxiliary relay when the automation plan is initiated or finalized.
  - **Relay:** Allows selection of the relay output of the decoder that will be activated/deactivated when the automation plan is initiated or finalized.
  - **Sensor:** Permits selection of the sensor input of the decoder that will be disabled/enabled when the automation plan is initiated or finalized.

    The displayed lists show the available relays and sensors that have been previously defined in the Server application as: door controllers, individual relays or sensors.

Example: Air Conditioning Plan.

The air conditioning system is required to be connected automatically from Monday to Friday between 08:00 and 15:00.

In order to activate the system the relay output of the decoder, programmed with address 201 will be used:

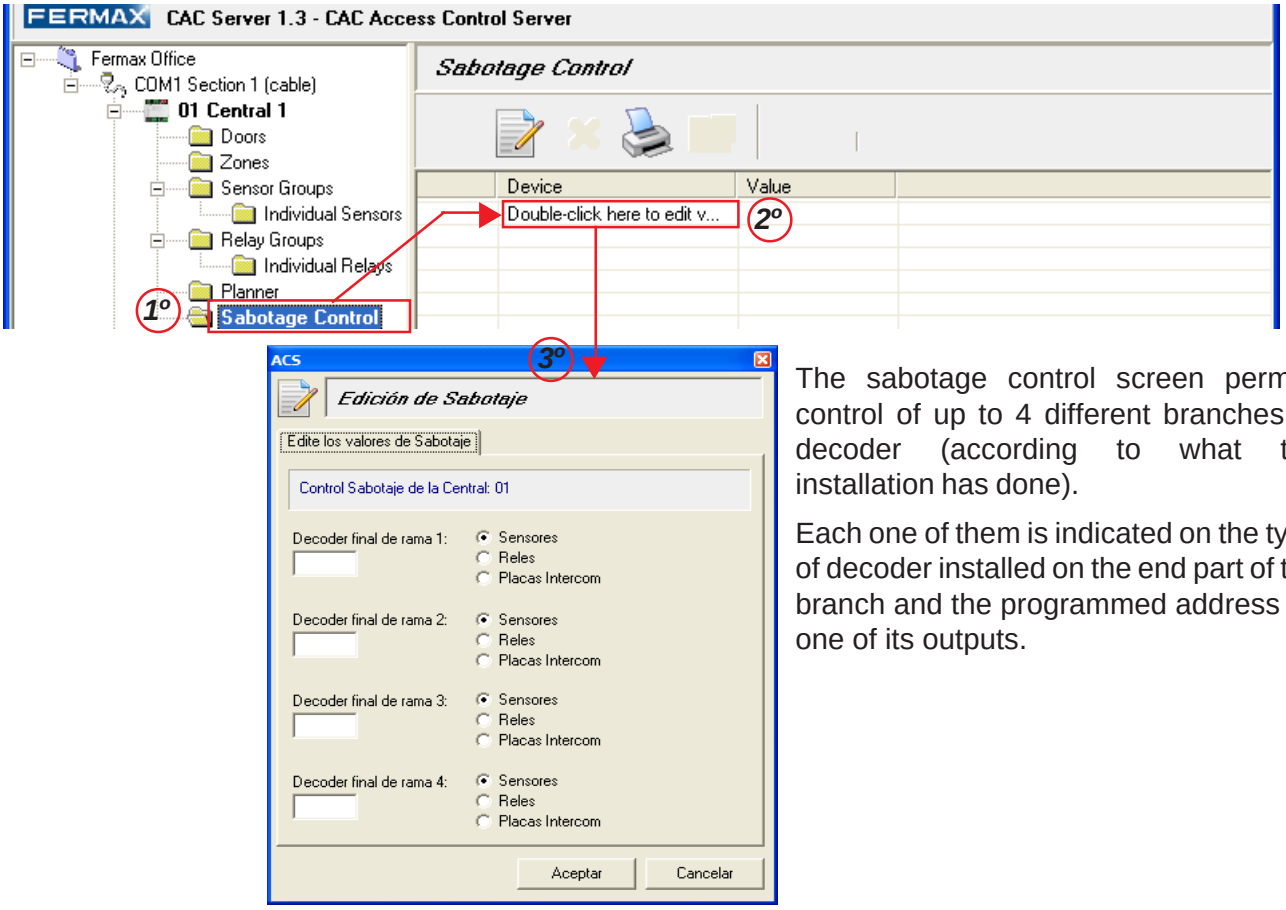


SABOTAGE CONTROL

Permits activation of the sabotage detection function from the decoder bus (where the decoder relays are connected, sensor decoders or panel decoders for intercommunication).

For this to happen the type of decoder installed should be indicated on the back of the bus and the programmed address on one of its outputs.

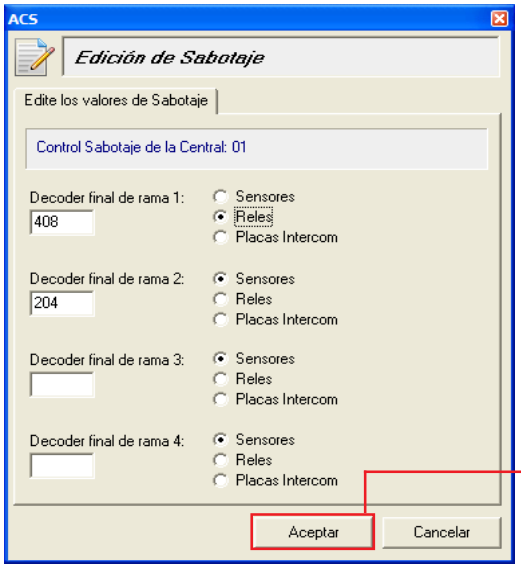
If, during the verification process of the sate of the decoder buses, which the central unit carries out every 60 seconds, the central unit does not detect the address of the indicated output, the central unit will generate an incident of sabotage which will be stored in the incident register and will send a sabotage message to the guard unit/reception area (if it exists).



The sabotage control screen permits control of up to 4 different branches of decoder (according to what the installation has done).

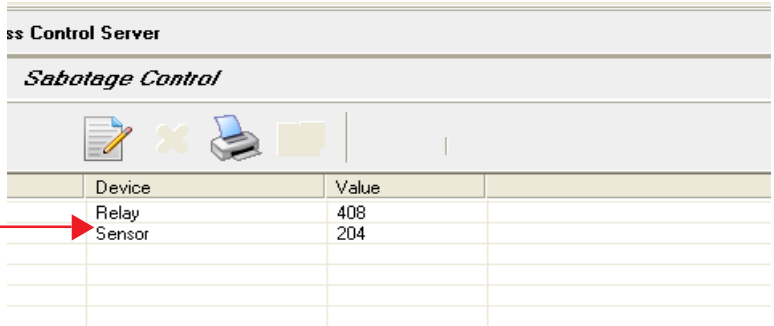
Each one of them is indicated on the type of decoder installed on the end part of the branch and the programmed address on one of its outputs.

Example: Control is required of the sabotage of the decoder bus, composed of two branches: branch 1 and branch 2.



The last decoder of branch 1 is a relay decoder with one of its outputs programmed with address 408.

The last decoder of branch 2 is a decoder of sensors with one of its inputs programmed with address 204.

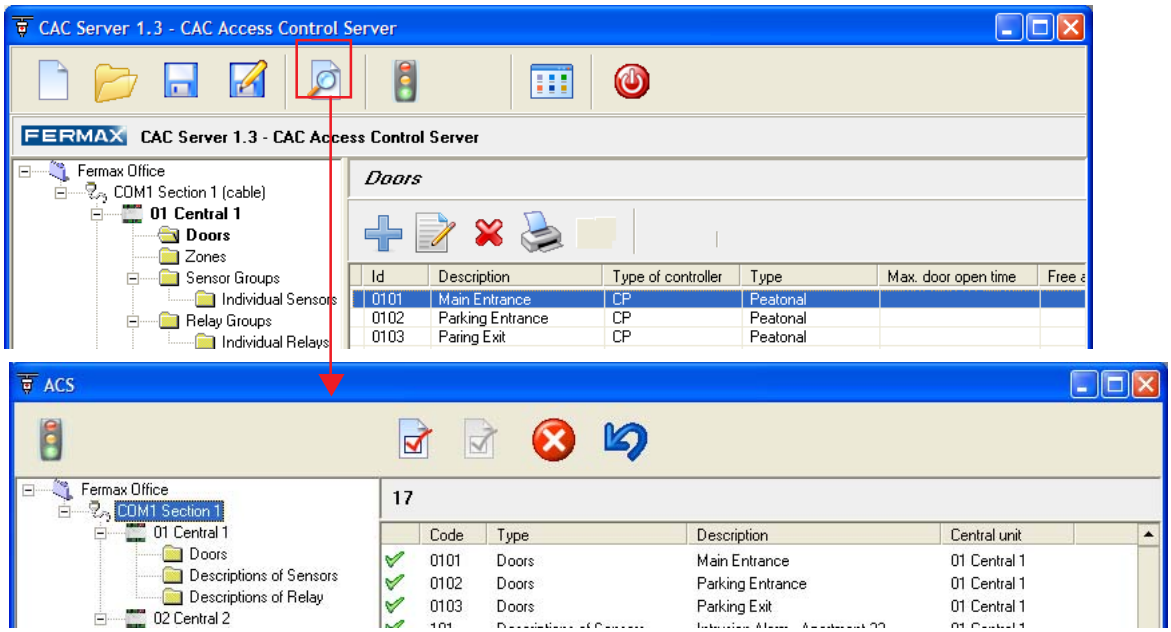


TEST OF INSTALLATION

The Server application allows a test to be carried out of the elements installed and defined in the installation.

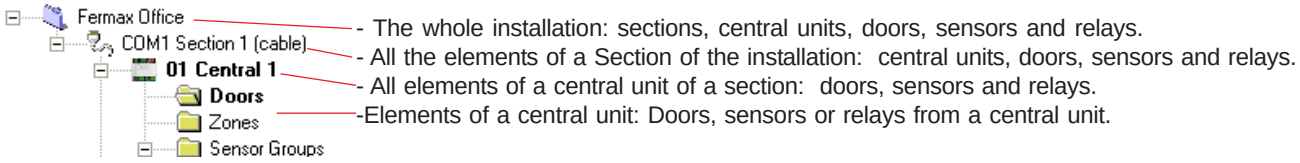
On carrying out the test, the Server application checks that the elements defined in it, exist in the installation and have communications between devices and the central unit.

In order to access the Test screen press the icon of the main screen of the application:



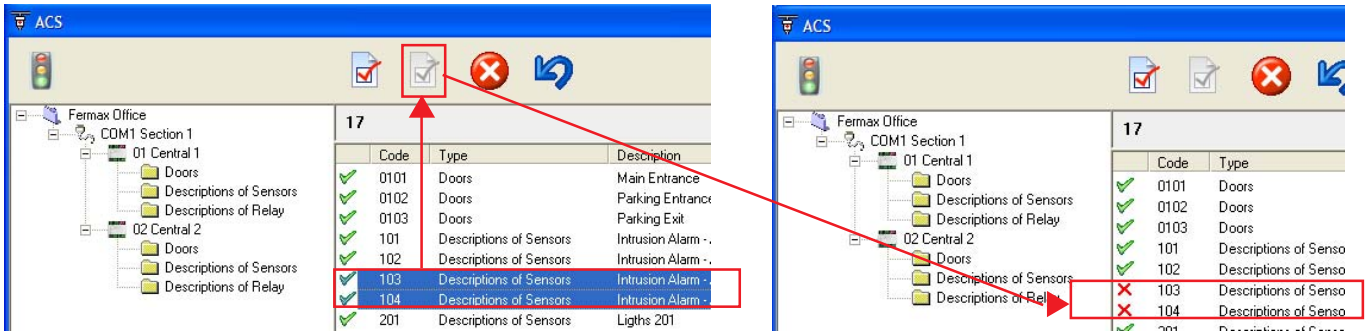
Carry out the Test

1º. Select the group of elements which the test will be carried out on:



In the upper right part of the screen a list with all the elements for testing is shown.

2º. If not wishing to carry out the test on one of the elements shown on the list, select the element from the list (or elements) and press the button :

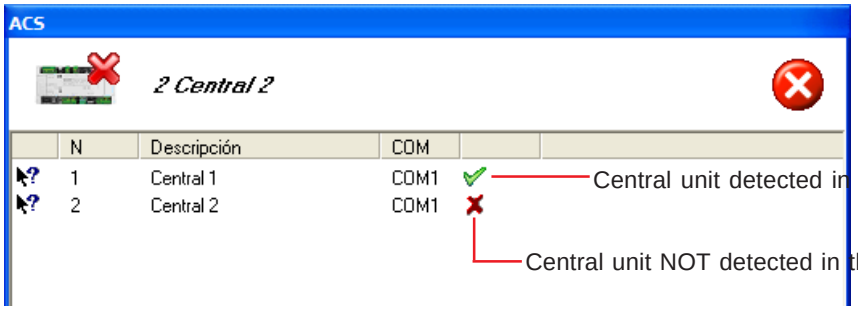


✕ indicates that the test of the element will not be carried out.
✓ indicates that the test of the element will be carried out.

In order to do the test again, select the element and press the button .

3º. Initiate the test: Press the button 

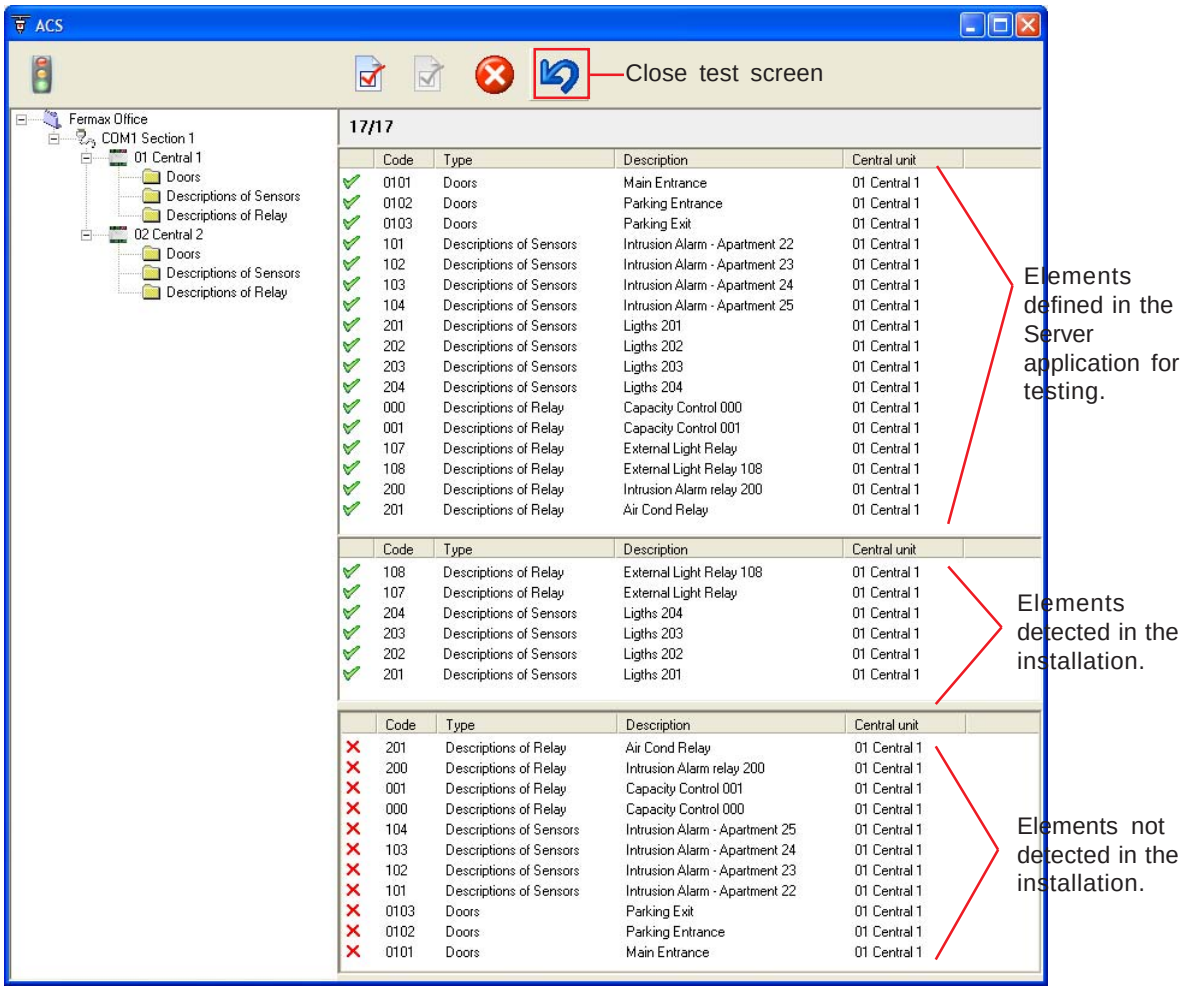
Firstly, a test will be carried out of the existing central units, the following screen showing the result of the test:



If one central unit is not detected, the Server application will not be able to carry out a test of the defined elements for that central unit.

To continue with the test press the button  .

Then, the result of the test of the selected elements is shown:



UPGRADE OF DATA IN THE CAC CENTRAL UNITS

Once all the elements of the installation are defined and their parameters configured in the Server application, it is necessary to activate the central units, that is, to send to each central unit of the installation the programmed configuraion.

It is very important to update the information of the different central units of the installation for correct operation of the CAC system.

Update central units

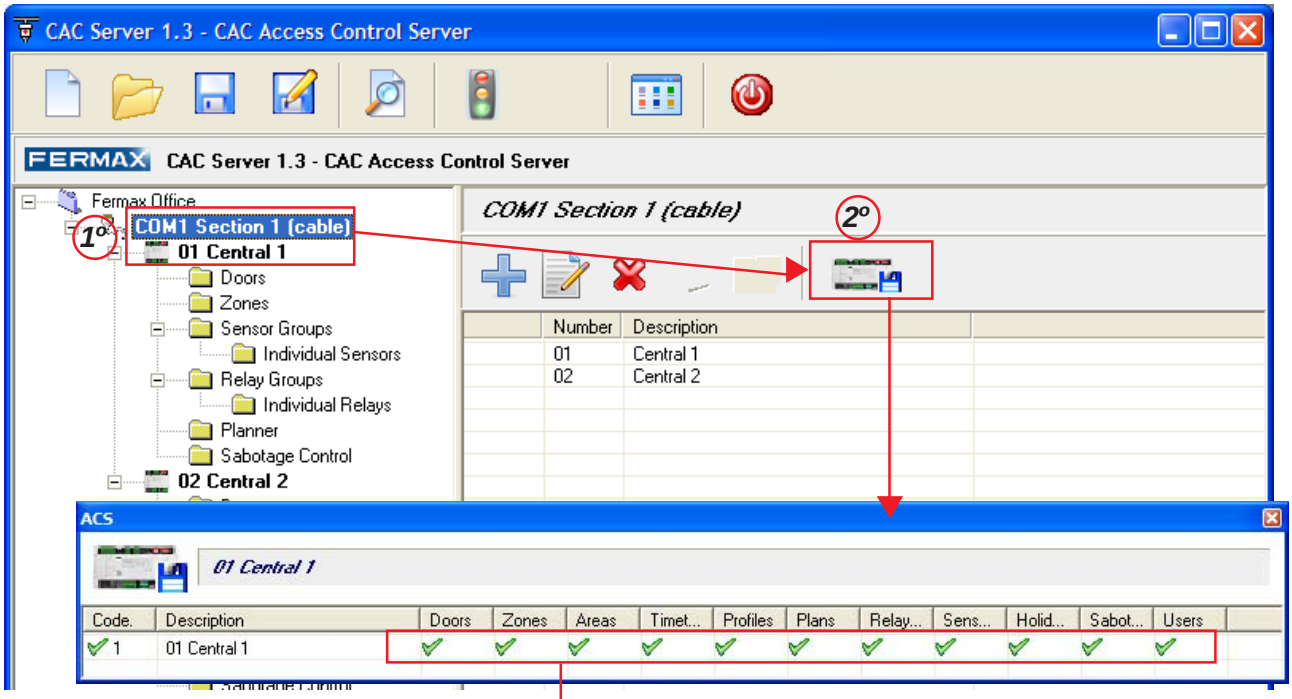
Each central unit may be updated individually or all the central units of the same section at the same time.

Every time a parameter is modified, it will be necessary to update the corresponding central unit.

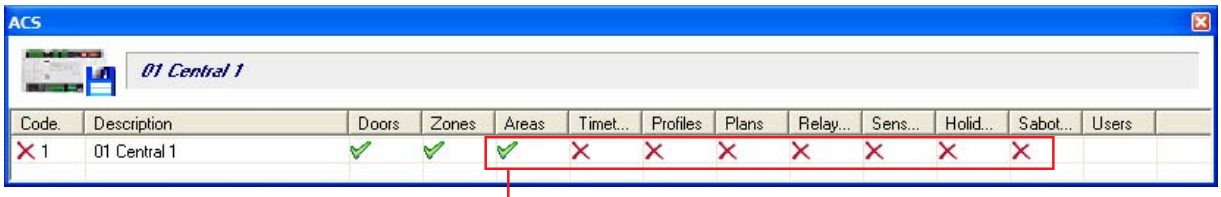
The steps to update the central units are the following:

1º- Select the central unit or the section to be updated: >If a section is selected all the central units of the section will be updated.

2º- Press the button  ***to initiate the upgrade***: A screen will be displayed which informs of the actual process and the final result of the update.



Elements of the central unit (Central unit 1) updated correctly.



Elements of the central unit not updated, (it is necessary to updated the central unit again).

Now the central units are working autonomously, managing the decoders, planner, incident register, etc. but it needs the information of the users, which should be shown through the client applications.

Having updated the data on the CAC Server's Central Unit, it is recommended that you wait a reasonable period (5-20 seconds) before activating the services based on the number of central units and devices in the system, to ensure that all data in all devices is fully updated.

START SERVICES

Once the installation in the central units is created, configured and updated, the final step, in order for the CAC system and client and server applications to start to work is "**start up services**".

On starting the services, the server application establishes communications with the installation, so everything that happens in the installation remains registered on the servers, as well as enabling access to the client application servers, which will use the information stored and configured in them (the client application stores its own information on the database server).

If the services are not initiated, the CAC installation operates correctly and autonomously, registering in each central unit the events occurring in the installation, with the disadvantage that the data will not be stored in the servers until the services are started.

Once the services are started the information stored in the central units is sent to the servers.

Equally, if the services are not started, the client applications will not interact with the installation, working off-line until services are initiated.

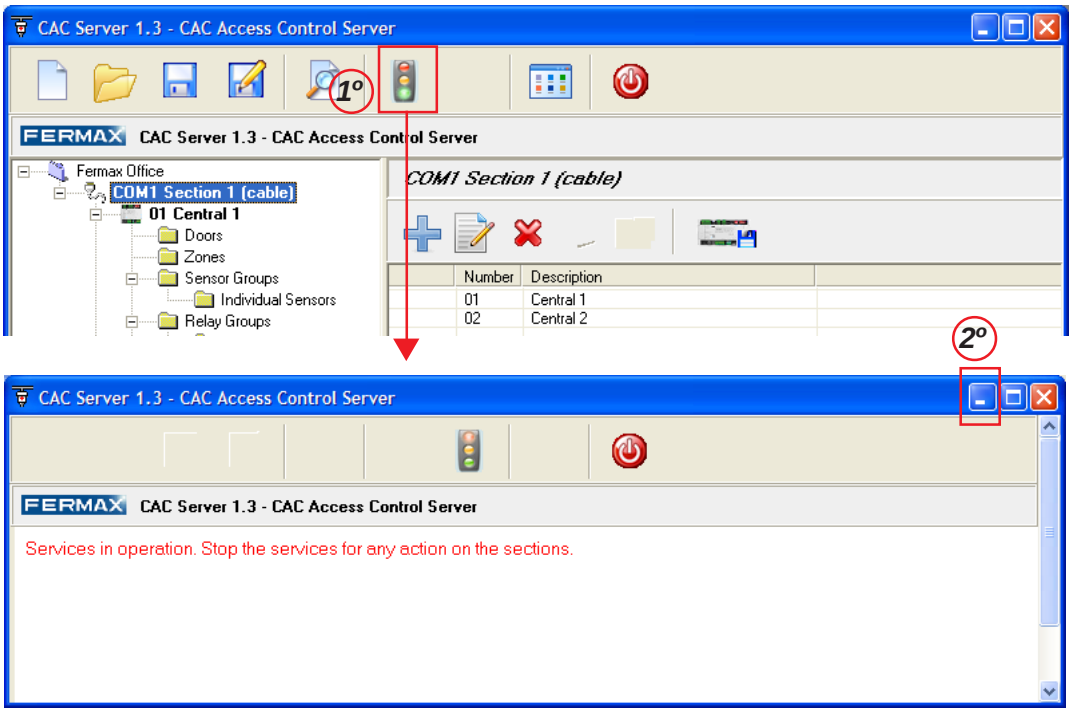
The client applications detect if the services are initiated or not, informing of this using alert messages.

In order to initiate services the following steps should be carried out:

1- ***Press the button***  : The services are started and it is now impossible to modify the configuration of the installation while they remain active. It is only permitted to carry out a test of the installation.

2- ***Minimize the server screen***: Services started, the screen should be minimized so that it is not accessible to non-permitted users. On minimizing the application, it remains password protected.

In order to minimize it press the icon  located in the extreme upper left of the screen, in this instant an icon will be created on the start menu of the PC (), that informs that the application is active and allows maximization of the application again.

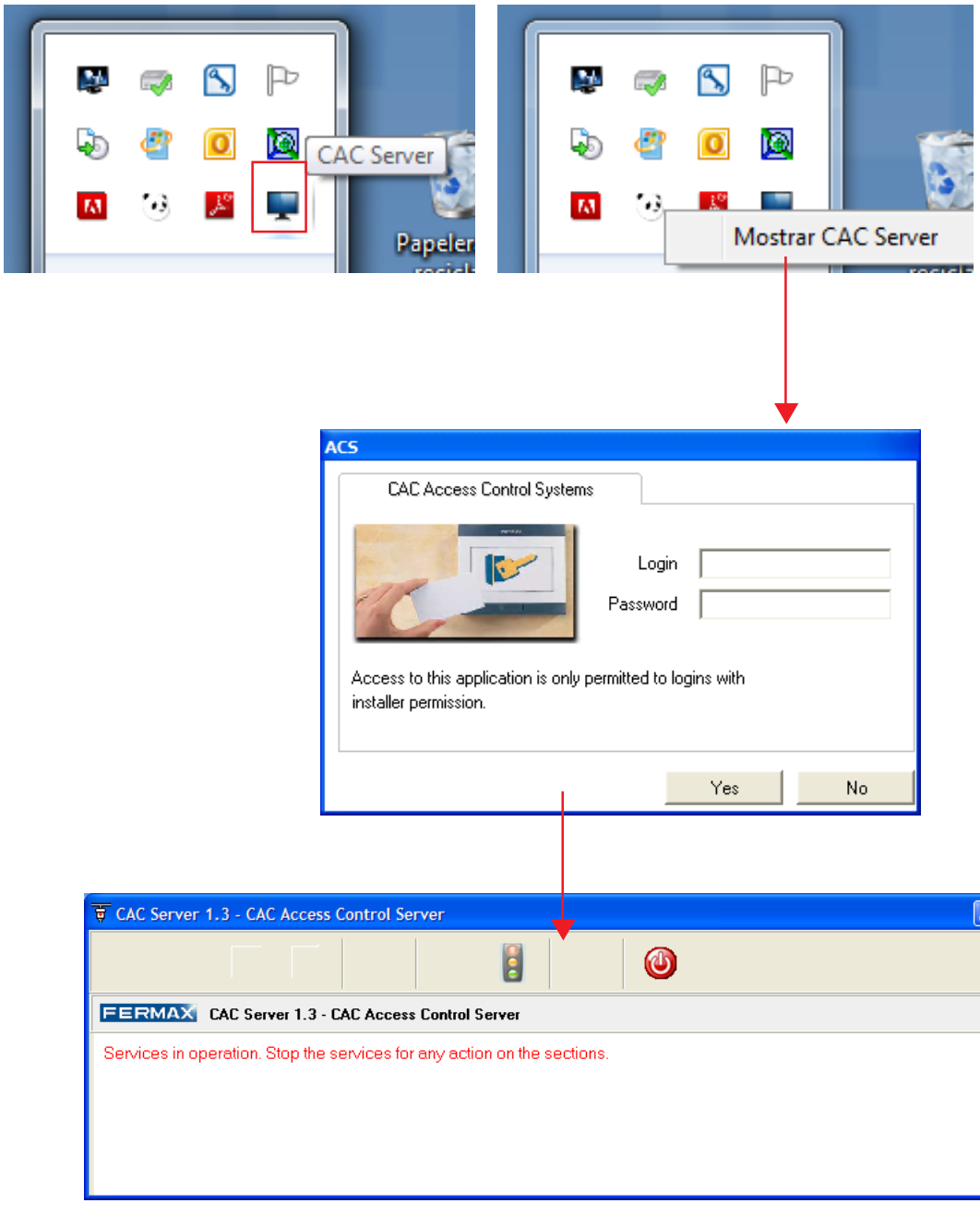


Maximize the Server screen

In order to maximize the Server screen, place the mouse over the icon , located on the start up screen, and click the right-hand button.

In the emerging menu select "Show CAC Server", the Login-Password screen for controlling access to the application will appear.

Enter the login and password requested in order to be able to access the server.



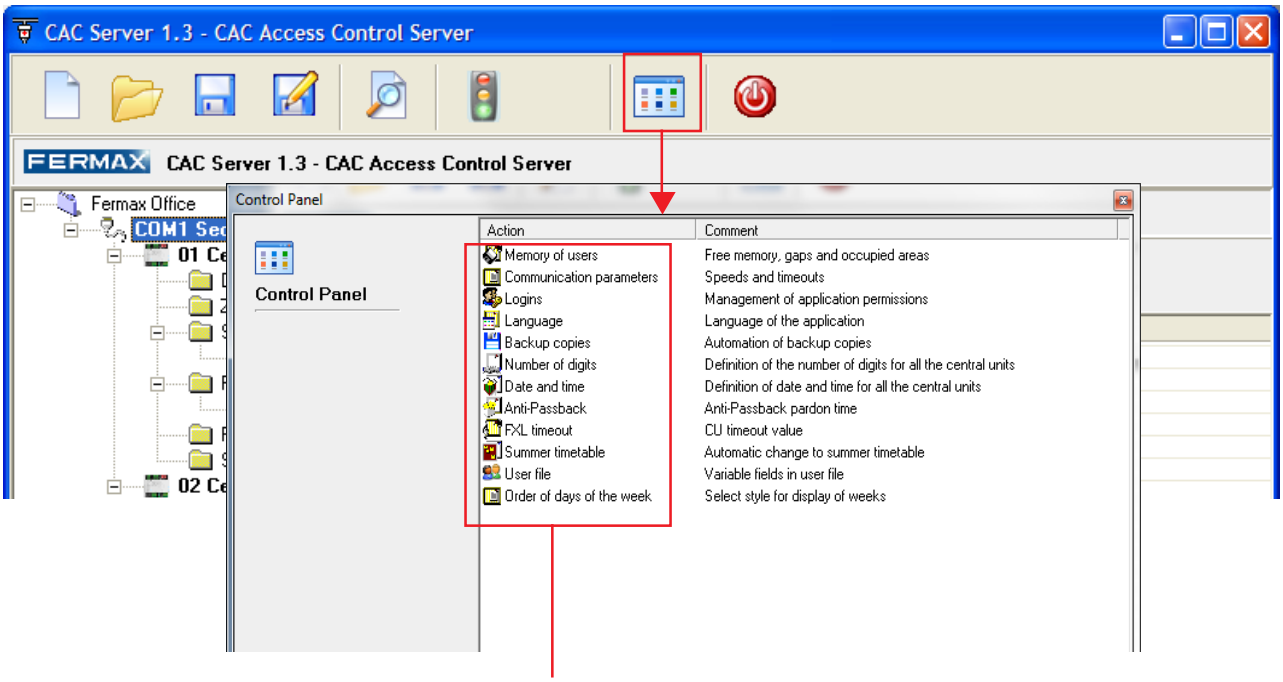
Halt services

In order to be able to modify the configuration of the installation using the Server application, the services should be disabled.

In order to disable the services press the button .

CONTROL PANEL

The control panel is a group of options and parameters for general configuration, as much for the central units of the installation as for the CAC Control Server.

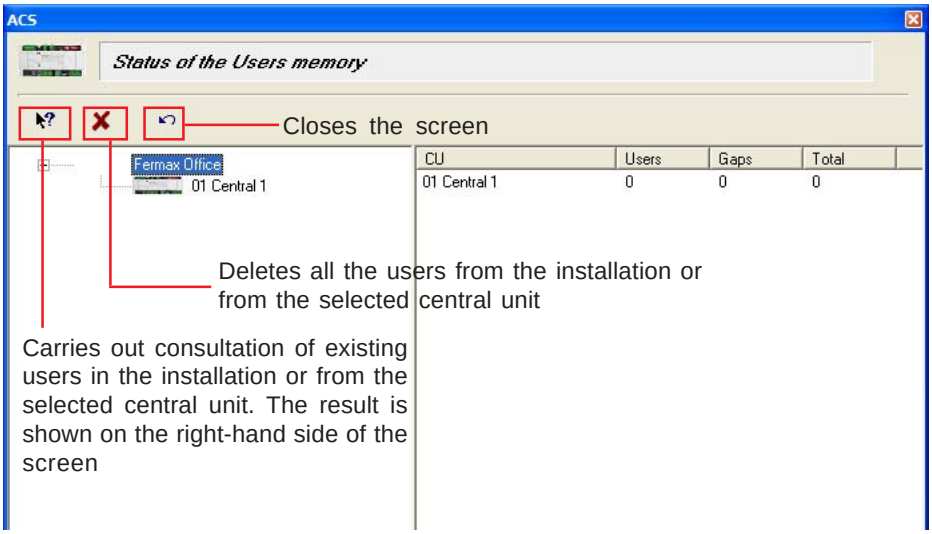


Double clicking on each one of the options will display the corresponding screen:

Memory of users

Shows information referring to the state of usage of the memory of users from the central units of the installation:

- Users: quantity of existing users in the central unit.
- Holes: a hole is a position of memory initially occupied by a user that has been deleted and that remains available for use on the insertion of a new user.



Communication parameters

Allows configuration of the speed of communication between central units and other communication parameters.

Do not modify the values indicated on this screen.

Logins

When any software application of the CAC system is initiated (server application or client application) a login and password for access is requested. Depending on the login with which the user gains access, the user will have more or less functions activated in order to manage and control the installation from the corresponding application.

There are four login levels, applicable to all the server and client applications of the CAC system: Installer, Administrator, Operator and Reports.

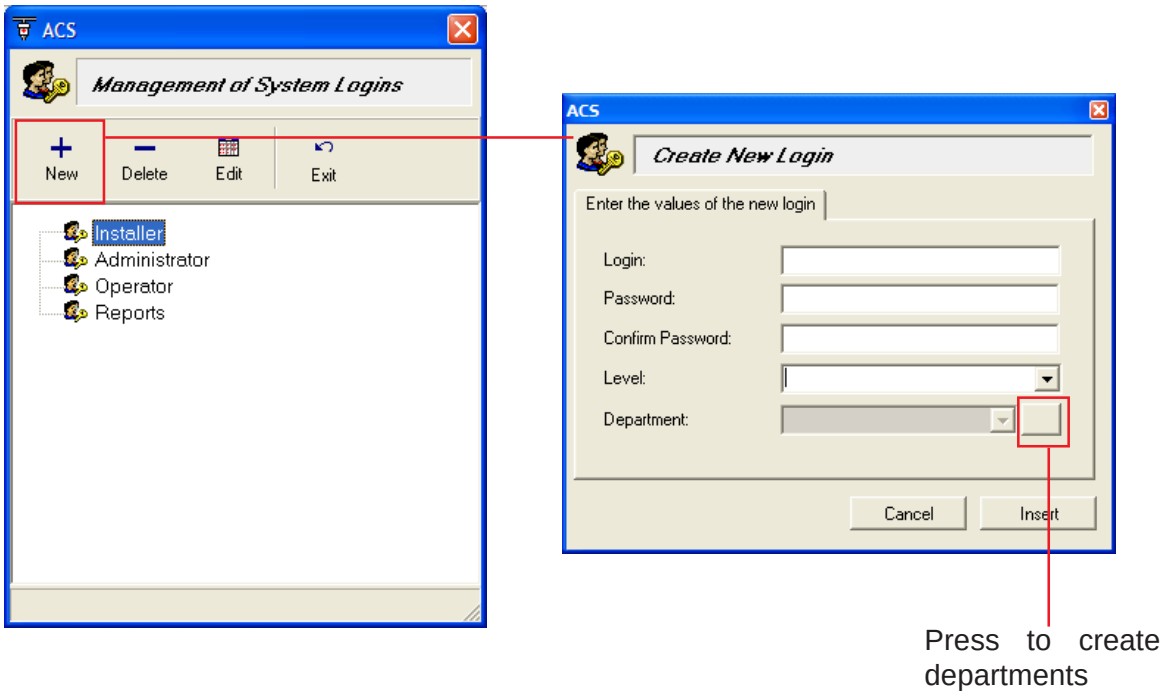
The following table specifies which functions a user can perform according to the assigned login:

Login	Server Applications	Client Applications
Installer	Total Control	Total Control
Administrator	Start applications - Start services	Total Control
Operator	None	activating/deactivating users (*)
Reports	None	Generating reports

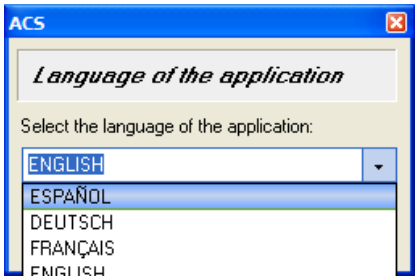
Important:

Access to the CAC Server is possible using logins at Installer and Administrator level. At Installer level all the options of the application can be started, and at Administrator level only services can be started.

(*) On defining a login at Operator level it is possible to associate it with a department. This option is useful for the CAC Access application, in such a way that the operators with this option will only see users who also belong to the same department. If this is not defined, the login will be able to be seen / edited by all the users, regardless of whether or not they have an associated department.



Language

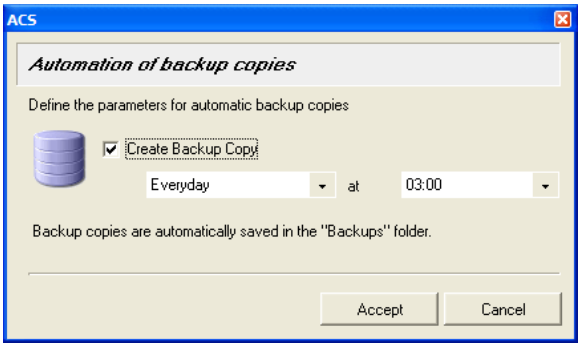


Permits selection of the language of the application.

The list of languages to select is obtained directly from the language file of the application (CAC_Server_lang.INI).

It is necessary to restart the server application so that the language change is implemented.

Security copies

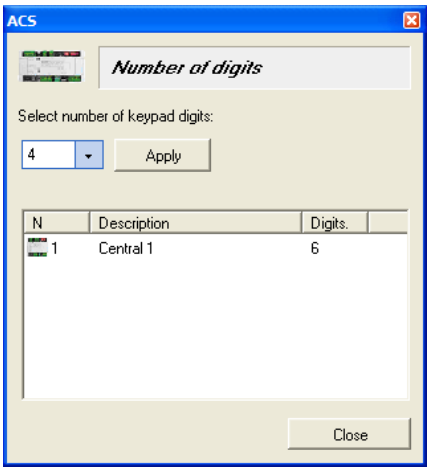


Activates the box and selects which days and at which times the server will make a security copy of the installation.

The security copies are stored in the file "Backups" located in the installation directory of the CAC Server application.

Subsequently, these security copies will be able to be uploaded from the option "Open" on the main application screen.

Number of digits

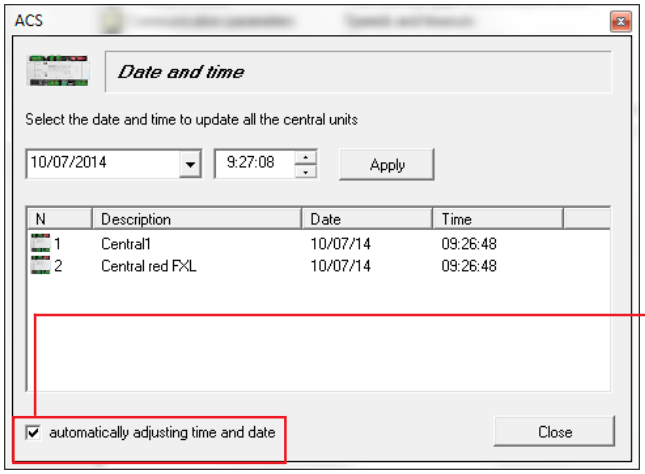


This screen allows selection of the number of digits that are necessary to enter into the readers and panels with keypads.

On accessing this screen the number of digits that each central unit has configured will be shown automatically (in the event of non-detection the symbol "?" will be displayed).

In order to change the number of digits, select the required value from the list displayed (4, 5 or 6) and press "Apply".

Date and Time



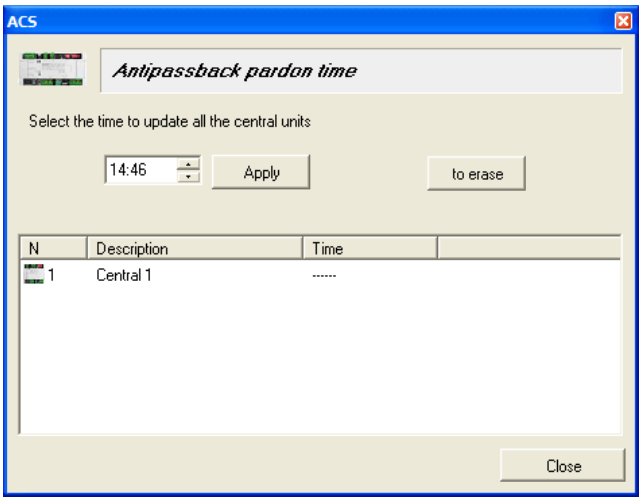
This screen allows update of the date and time for all the central units defined in the installation.

On accessing this screen the date and time of the central units will be displayed automatically (in the event of a non-detection the symbol "?" will be shown).

In order to update the date and time, enter the correct date and time and press "Apply".

Set date and time Due to environmental conditions, the central unit´s time may be lost. We recommend activating this option for the PC to maintain the proper time.

Antipassback pardon time



In case of inappropriate use of the system on the part of the user, such as exiting the installation without introducing the identifier, using the exit of another user, access will not be granted the next time access is attempted, given that the system considers the user as already inside.

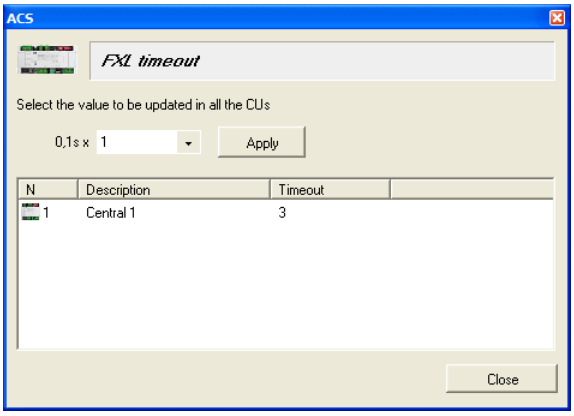
In order to avoid these problems, it is possible to define on this screen, an antipassback pardon time. In this way, at the time indicated (normally during the night) the system, automatically puts all users as outside the installation perimeter, allowing fresh access to the installation of all users who would have been left inside.

On accessing this screen the antipassback pardon time of the central units is shown automatically (in the case of being deactivated this option will be shown in the field time: "——").

In order to activate this function, enable the box "Activate", enter the antipassback pardon time and press "Apply".

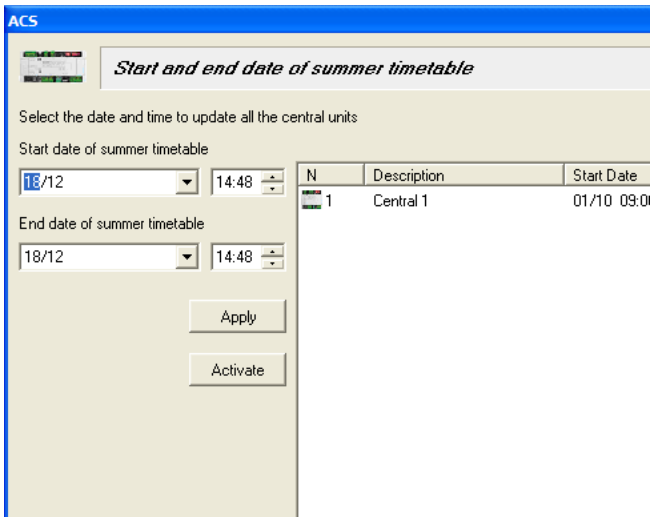
In order to deactivate it with the box "Activate" deactivated press "Apply".

Timeout FXL



Configuration parameters of the system. Do not change the values indicated on this screen.

Summer Timetable



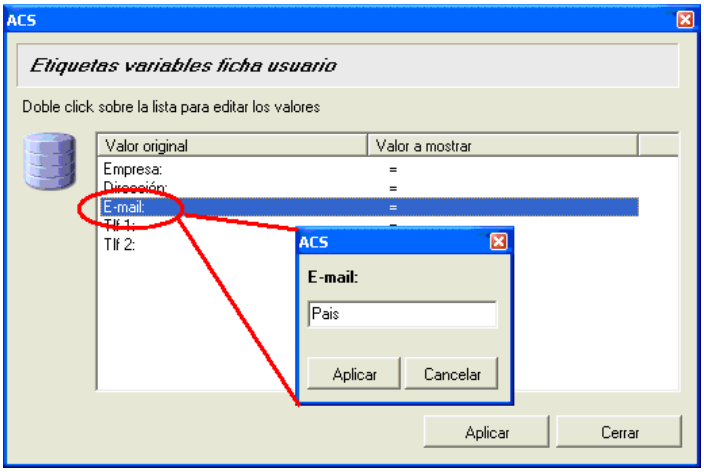
This screen allows the central units of the installation to carry out automatic changes to the timetable from summer to winter on the dates and times indicated as being the start and end of the summer timetable.

On accessing this screen, if this option is enabled, the start and end date of the summer timetable, programmed in the central units, will display automatically.

In order to activate this option, enable the box "Activate", entering the date and time of the start and end of the summer timetable and press "Apply". In order to deactivate it with the box "Activate" deactivated, press "Apply".

Each year it will be necessary to update the Summer Timetable.

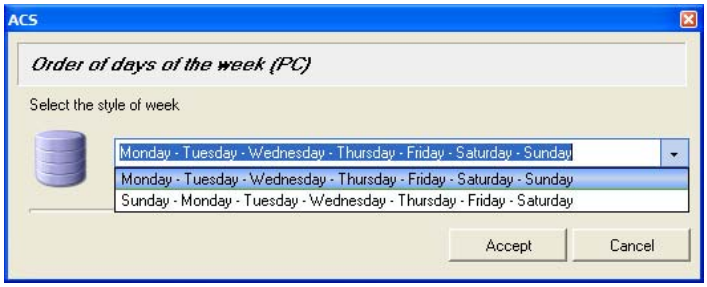
User file



On this screen the variable labels in each user file are defined, that will be shown on the client application "CAC Access". These values are for generic use, that is, it is not information that is saved in the central units, but may be useful for the user of the application.

In order to edit the value, double click on the label to be modified. When the value on the list is "=", it means that the label in the CAC Access application will show that it is defined in the language file of CAC Access. In this example the value 'Country' is defined instead of E-mail.

Day week order

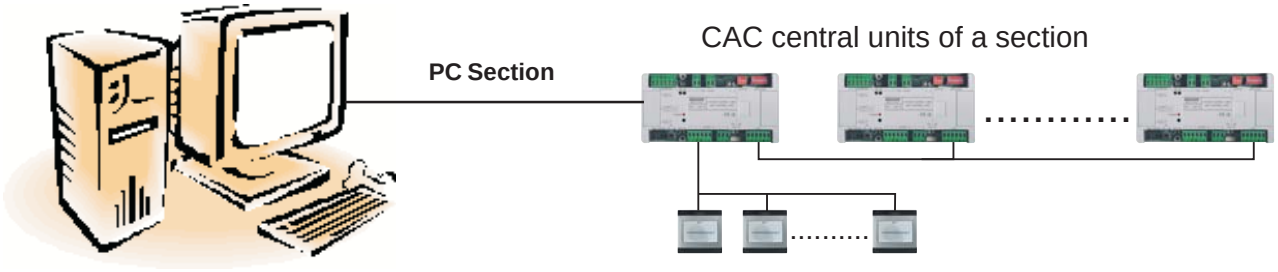


On this screen the order is established for showing the days of the week ("Monday to Sunday" or "Sunday to Saturday") on the different screens where timetables are seen and configured, in client applications and server applications.

APPENDIX

CONNECTION BETWEEN THE INSTALLATION AND THE PC (SERVER)

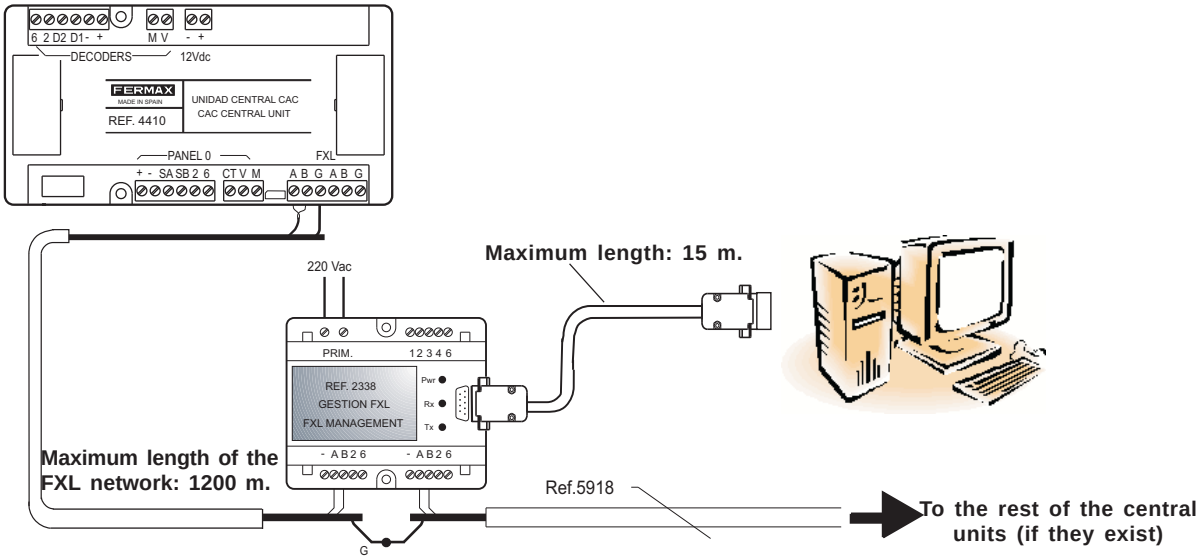
The installation should connect to the computer where the "CAC control Server" application is installed.



CAC control Server

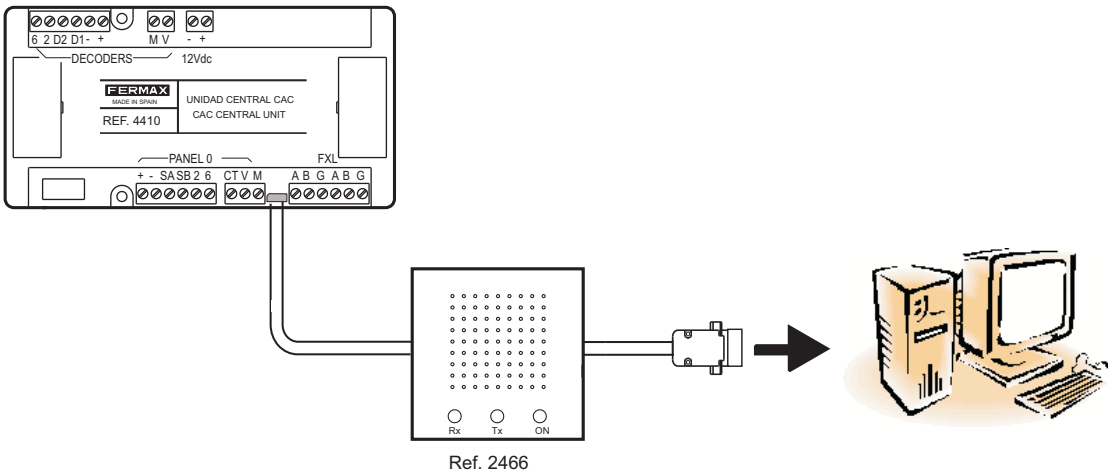
For each section it is necessary to have a connection between a central unit of the section and the PC.

Connection using interface 2338 - Port RS232 of the PC



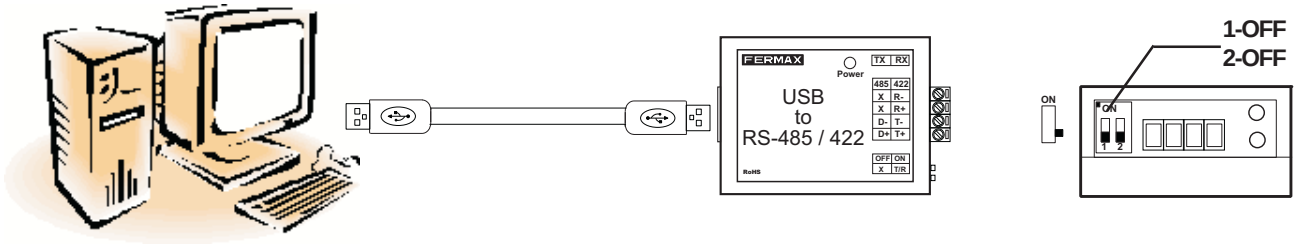
For more information consult "Interface Manual 2338" code 94098.

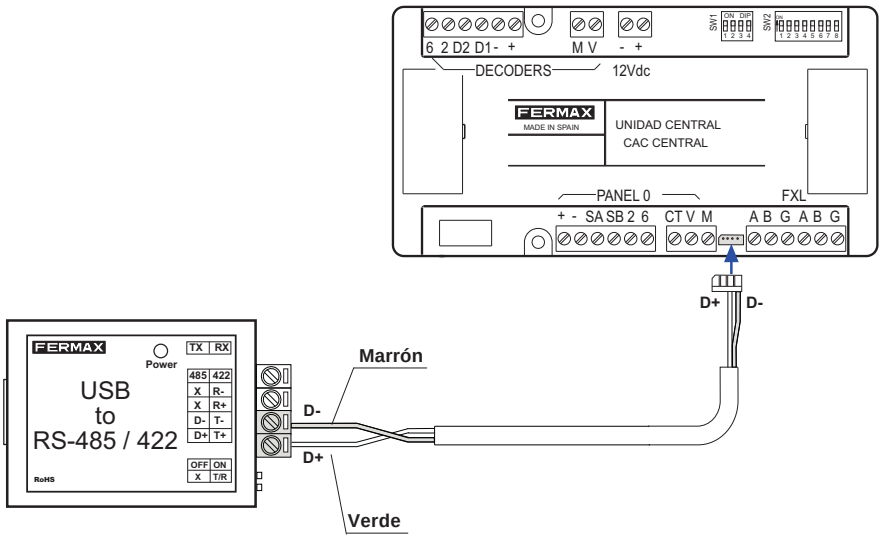
Interface 2446 - Port RS232 PC

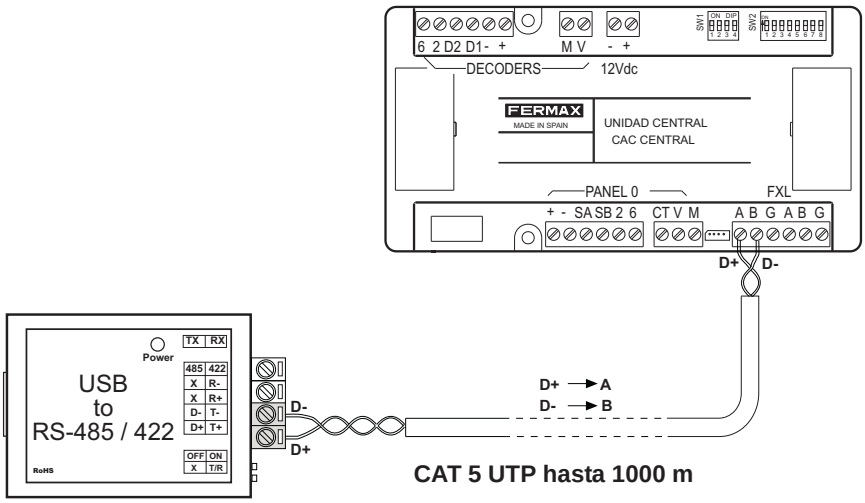


Ref. 2466

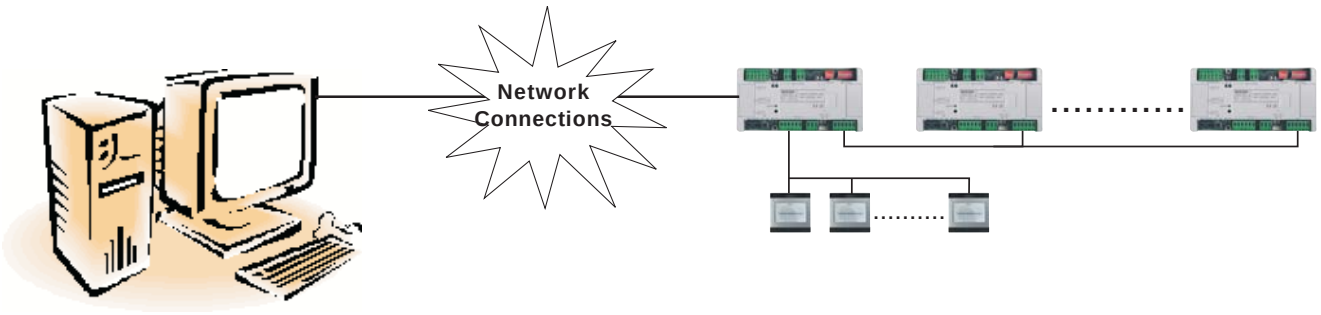
Interface 24661 - Port USB PC







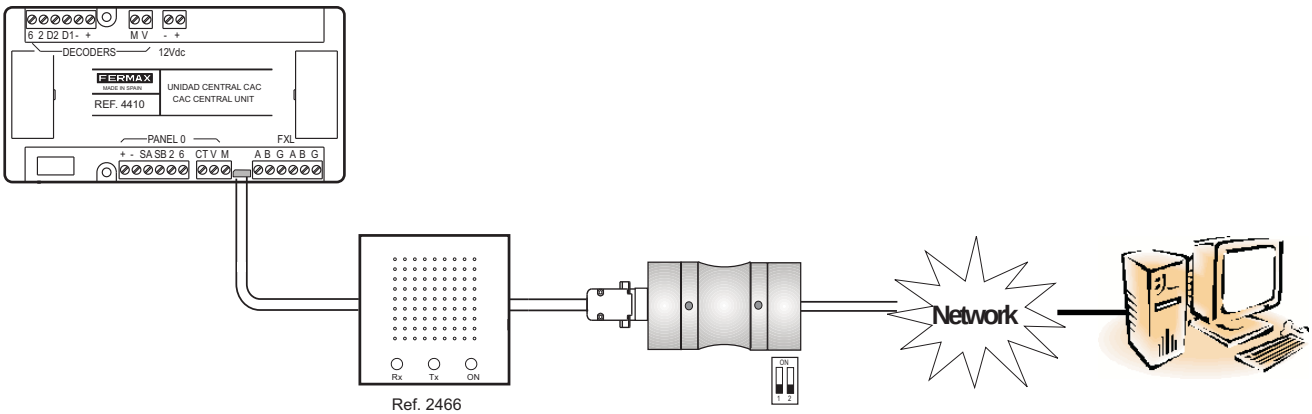
CONNECTION THROUGH LOCAL NETWORK



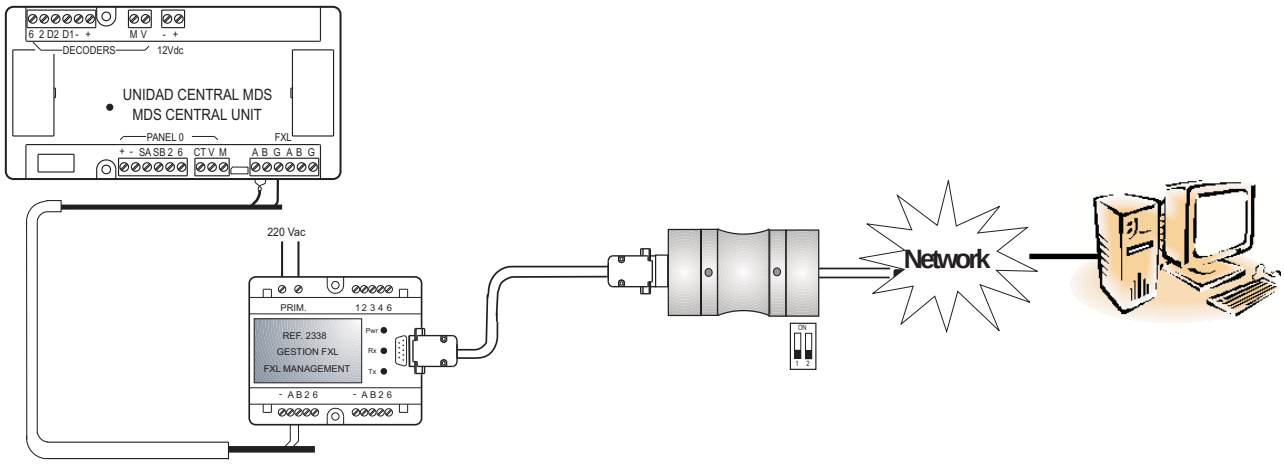
Connection using "Remote mangement terminal Ref. 1087"

Interface 1087 permits connection of the CAC installation and the PC server across a local or Internet network.
For more information consult the technical information code 94571, referring to the product.

Connection using Interface Ref. 2466 + Remote Management Terminal Ref. 1087



Connection using Interface Ref. 2338 + Remote Management Terminal Ref. 1087



PROBLEM RESOLUTION IN MULTI-HOMED ENVIRONMENTS (more than one active network connection)

In situations where we have more than one network connection configured and active at the same time, this may result in problems correctly establishing a connection between the CAC Access software and the CAC Server.

CAC Server uses software based on Borland® VisiBroker® 4.5 to detail its availability by way of a «broadcast», however this only applies in the case of network interfaces. The correct interface must be assigned by way of a configuration file (this information should be provided by your network administrator).

The steps are as follows:

1. Define the environment variable **OSAGENT_LOCAL_FILE** using the file's location values, this is where the configuration information will be stored (e.g. c:\windows\visibroker.cfg)

2. Format the file defined above using the following content and format:
    1. #IP subnet_mask broadcast_address
    2. 172.20.80.16 255.255.0.0 172.20.255.255

3. The above example requires that all input and output connections from the CAC Server are by way of an interface with the following address IP 172.30.80.16 (e.g. our IP and internal LAN).

For more information:
http://support.borland.com/kbshow.php?q=24886