MEET

INSTRUCTION AND INSTALLATION MANUAL FOR MEET MANAGEMENT SOFTWARE V 1.0.6

FERMAX

MEET MANAGEMENT SOFTWARE MANUAL

CONGRATULATIONS FOR BUYING A QUALITY PRODUCT!

Fermax Electrónica develops and manufactures premium equipment that meets the highest design and technology standards. We hope you will enjoy all its features.

Technical publication for information purposes edited by FERMAX ELECTRÓNICA S.A.U.

FERMAX ELECTRÓNICA applies a continuous improvement policy, therefore it reserves the right to modify the contents of this document, as well as the product features hereof at any time and without prior notice. Any modification will be reflected in subsequent editions of this document.

Code 970138Ic/V02_21

CONTENTS

1 INTRODUCTION

MEET Management Software (MMS) is a computer application that allows you to perform various tasks related to an installation with MEET products, regardless of the size of the installation.

It has 2 main functions:

- **A tool to be used by the installer**, for registering/unregistering proximity cards and facial recognition users.
- **Management point for the administrator or manager of the installation**, with functions such as receiving alarms from apartments and access points, generating messages to indoor monitors (individually or grouped), and controlling the use of IDs by users.

The application (in its latest version) can be downloaded from the Fermax website www.fermax.com or from the download section of the specific Meet website, http://meet.fermax.com. However, it does require a **SECURITY ENCRYPTED KEY (DONGLE) Ref. 9540,** which must be plugged into a USB port in order to start the application, and left plugged in for the entire time it is being used.

1.1 User profiles

MMS is a security system that uses access credentials, so that, when a user attempts to operate it, it will ask for their credentials in order to establish permissions and the associated functions.

MMS has 3 user different profiles, which can be assigned to the various users who will be operating it:

- **Installer:**
    - Users with this profile can access all the available features, including those related to installing and configuring the software.
    - There can only be one user with the Installer profile.
    - The Installer can create new users, although only those with different profiles (Admin or Concierge), and can also delete them.
    - The Installer can modify the access data (credentials) of any user, including their own.
    - The Installer is the only one who can create groups.
- **Admin:**
    - Users with this profile can access all the functionalities designed for managing the system, such as registering/unregistering cards or facial recognition, but the installation and configuration functionalities are blocked, to avoid possible errors due to accidental configuration errors.
    - An **Admin** user can create new users with the **Guard** profile, as well as delete them (regardless of who created them).
    - An **Admin** user can modify their own credentials and those of any user with a Concierge profile, regardless of who created them.

- **Concierge:**
  - They can only use the software's everyday functionalities, such as sending messages to monitors and viewing alarm and access events and logs.
  - A user with a **Concierge** profile cannot create or delete any other user.
  - A user with a **Concierge** profile can only modify their own credentials.

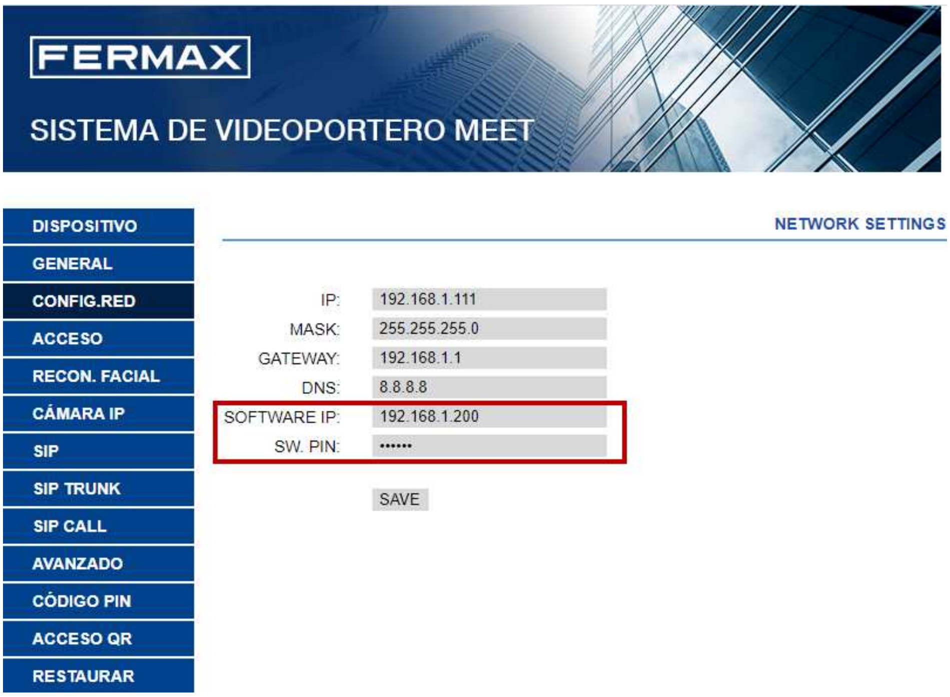
The management software does not offer any kind of options related to any MEET installation audio or video communication functions.

You can use one computer for managing multiple MEET installations, using the same DONGLE, but it is only possible to have one instance of the Management Software running, so you can only control one MEET installation at a time.

The DONGLE Ref. 9540 only needs to be inserted in the PC when you are operating the Management Software. It is not necessary for general use of the MEET installation as an audio/video intercom system, nor for operating the monitors as an alarm system, relay control, IP camera view, etc.

The computer must be assigned a fixed IP ADDRESS within the same Ethernet network as the MEET devices being controlled. This IP address must be entered for the programming of all devices in the SOFTWARE IP field.

You should also note down the SOFTWARE PIN assigned to each device in the installation, as you will need to use it to register them in MMS. If the installer finds it convenient, they may use the same SOFTWARE PIN for all devices.



IP: 192.168.1.111
MASK: 255.255.255.0
GATEWAY: 192.168.1.1
DNS: 8.8.8.8
SOFTWARE IP: 192.168.1.200
SW. PIN: ••••••

1.2 Minimum system requirements

- Windows 7 (32 bits) operating system. Preferably Windows 10.
- CPU: 2.5GHz Dual-Core Processor
- Hard drive: HDD SATA 160 GB
- 2 USB ports
- Gigabit Ethernet port, 100/1000Mbps (Fast-Ethernet).
- The computer IP address must be fixed and in the same range as all the devices in the installation. .
- A computer capable of playing audio and video.

The MEET MANAGEMENT SOFTWARE is distributed with an individual licence for one device (computer) by means of a SECURITY ENCRYPTED KEY (DONGLE), which is protected against unauthorised copying.

The DONGLE can be used on more than one computer, but the SOFTWARE will only work while the DONGLE is plugged into the computer USB port.

.

2 DOWNLOADING MMS

MMS consists of a structured set of folders, executable files, libraries and data bases, which all interact with each other. All these elements must be contained in one single global folder located on the computer.

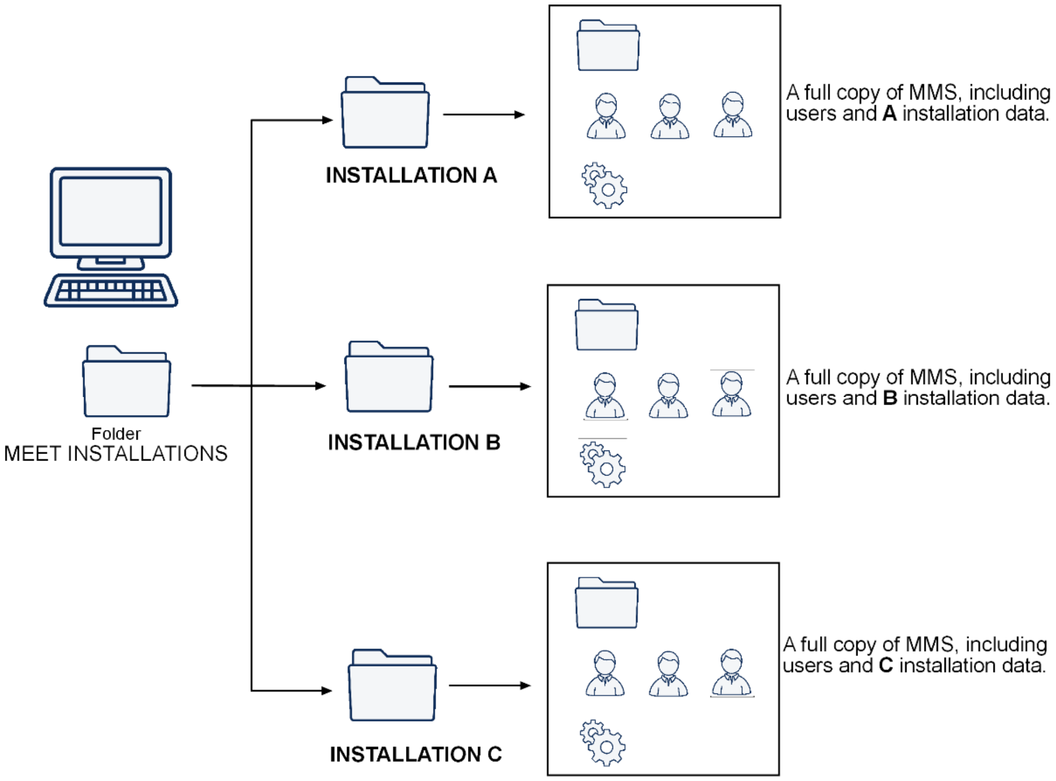
It also includes the **MEET MANAGEMENT SOFTWARE.EXE** file for starting the application.

It can be downloaded from the SOFTWARE section on the Fermax website, under the name **MEET Management Software V1.06.** It is provided as an *.rar file to make it easier to download.
It is also available in the download section at http://meet.fermax.com.

The steps for downloading and using MMS are as follows:

1. Download the **MEET Management Software V1.6.rar** from any of the above locations.
2. Unzip the file, which will contain a MEET MANAGEMENT SOFTWARE folder.
3. Rename this folder using whatever name you like (e.g. VILLAS SYSTEM), and place it in the desired location on the computer.

It is possible to manage multiple MEET installations from one computer, as long as there is a full copy of MMS in a separate folder for each installation:


Folder
MEET INSTALLATIONS
INSTALLATION A
A full copy of MMS, including users and **A** installation data.
INSTALLATION B
A full copy of MMS, including users and **B** installation data.
INSTALLATION C
A full copy of MMS, including users and **C** installation data.

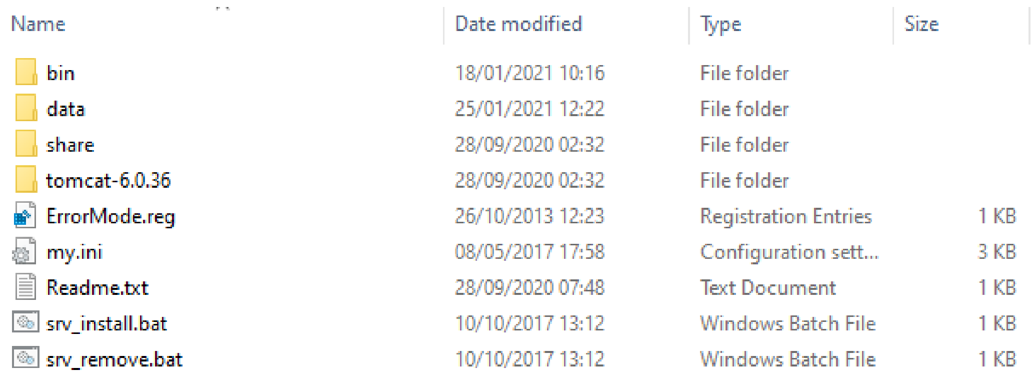
- **However, it is only possible to run one instance of MMS at a time.**
- **Restart the computer to switch from managing one installation to another.**

3 STARTING THE APPLICATION

You need to use the SECURITY KEY (DONGLE) Ref. 9540 to operate MMS.
The key must be inserted in one of the computer's USB ports when you start the application.

Once you have inserted the DONGLE, follow the steps below to start MMS**:**

1. Open the MEET MANAGEMENT SOFTWARE folder that you downloaded:



Name	Date modified	Type	Size
bin	18/01/2021 10:16	File folder	
data	25/01/2021 12:22	File folder	
share	28/09/2020 02:32	File folder	
tomcat-6.0.36	28/09/2020 02:32	File folder	
ErrorMode.reg	26/10/2013 12:23	Registration Entries	1 KB
my.ini	08/05/2017 17:58	Configuration sett...	3 KB
Readme.txt	28/09/2020 07:48	Text Document	1 KB
srv_install.bat	10/10/2017 13:12	Windows Batch File	1 KB
srv_remove.bat	10/10/2017 13:12	Windows Batch File	1 KB

2. Open the **bin** folder and locate the file watchdog.exe

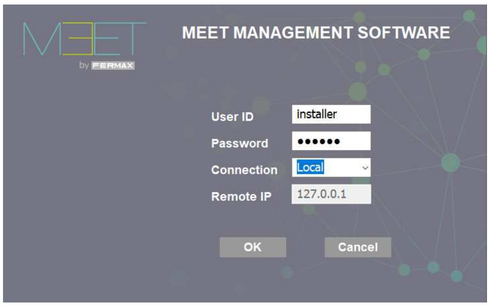
3. **Run watchdog.exe**
   This executable file launches the data bases and services necessary for operating the application.

   You should see the following icon appear in the task bar:

4. Locate the file: MEET MANAGEMENT SOFTWARE.exe

5. **Open the MEET MANAGEMENT SOFTWARE file**.

6. Identify yourself with the corresponding credentials and access level.



MEET MANAGEMENT SOFTWARE

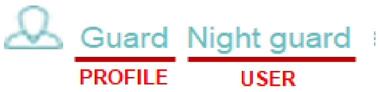
User ID: installer
Password: ••••••
Connection: Local
Remote IP: 127.0.0.1

- Each software user registered in the installation will have a USER ID.
- When the application is started for the first time, only the **Installer** user profile will be available, and they will be able to create new users with different profiles (see. Section 4.4.1 SYSTEM:USER)
- The default password for the **Installer** user is: **123456**
- Since MMS is stored locally on your own computer, use the local and remote IP connection: 127.0.0.1.

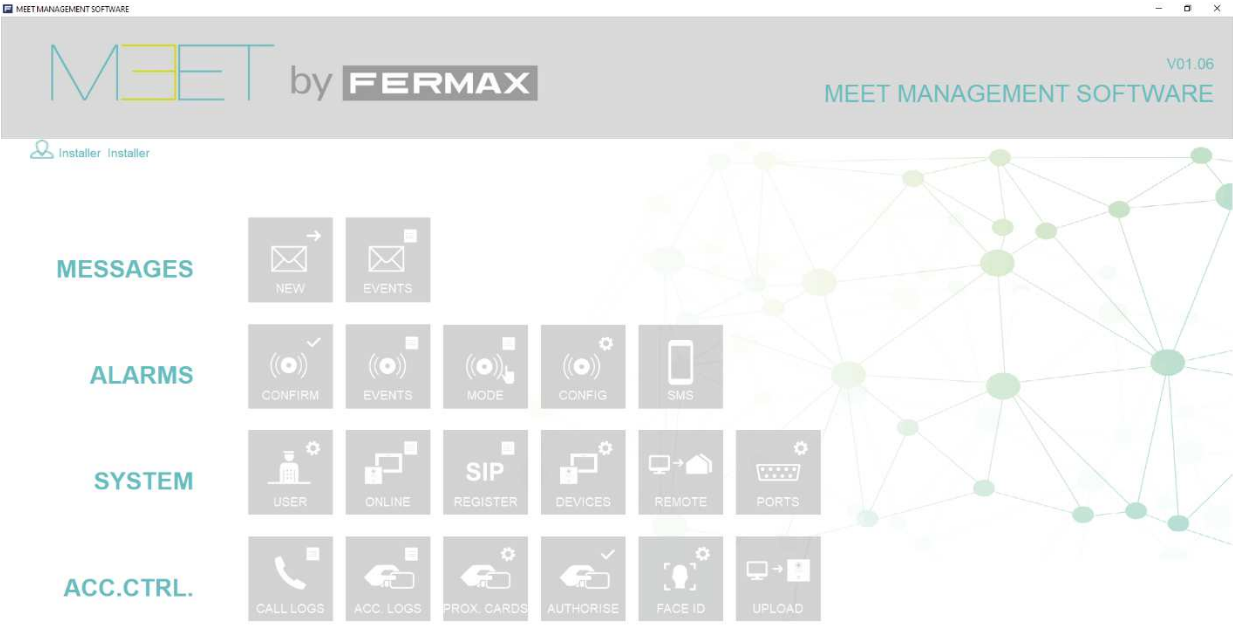
4 OPERATING THE APPLICATION

Once the application has been started, the OPTIONS MENU will appear, and the content available will depend on the profile of the user.

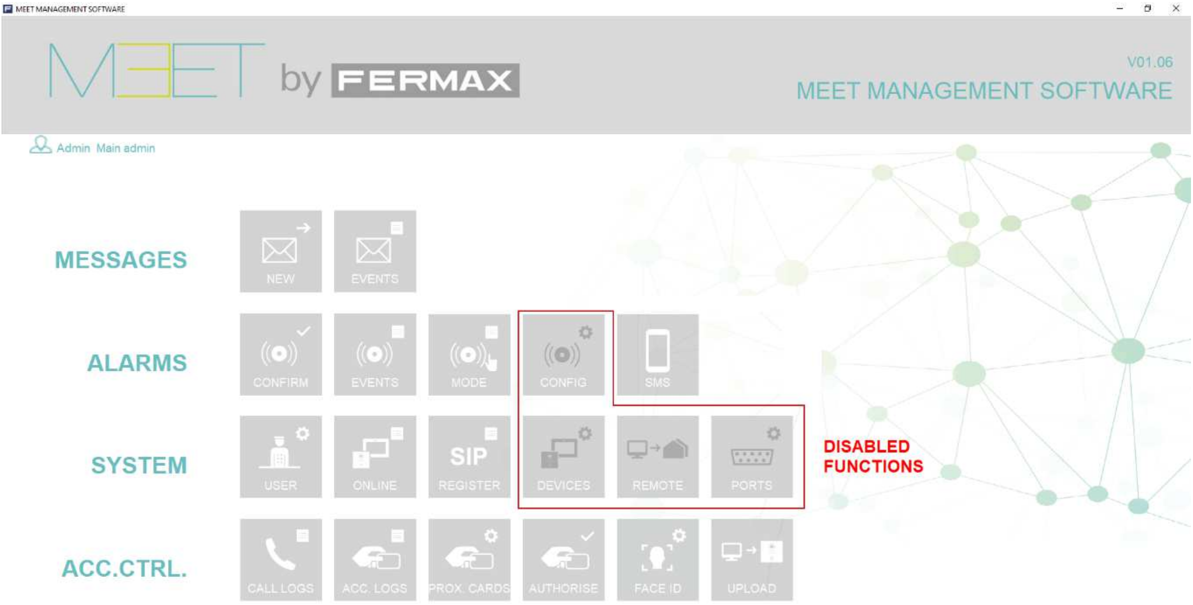
The profile and user type will be shown at the top left of the screen



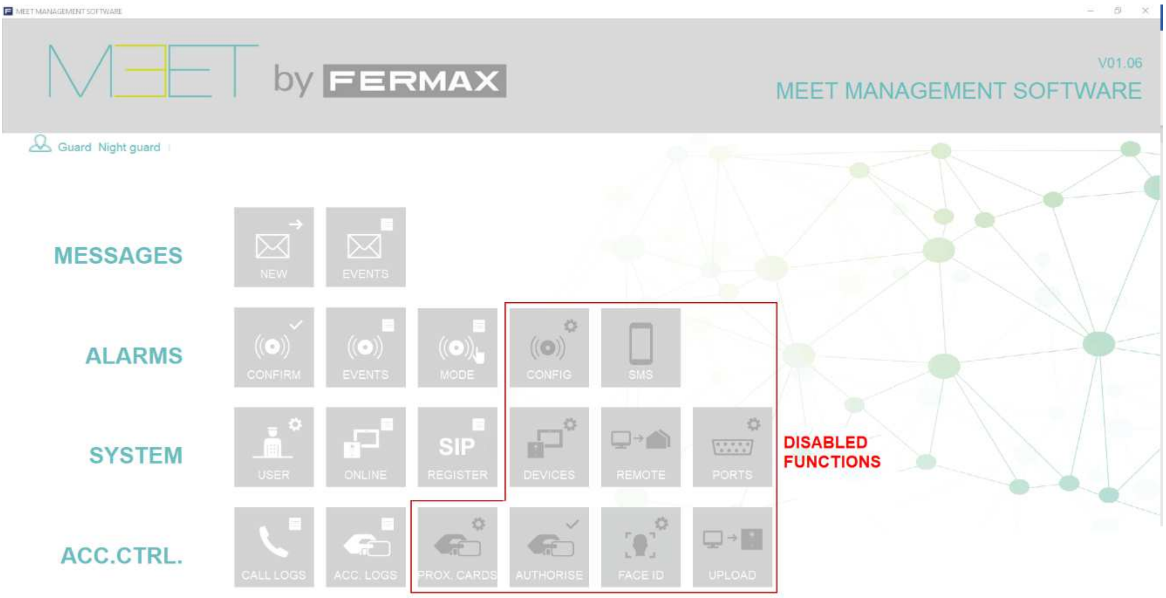
User with Installer profile (default profile)



Users with Admin profile



Users with Concierge profile



This main screen shows a series of icons, grouped into 4 sections (MESSAGES, ALARMS, SYSTEM and MANAGEMENT), which allow the user to access the corresponding function, as explained in the following sections of this manual.

- **MESSAGE Section**
  Allows you to use the functions related to sending text messages to a monitor or a group of monitors, as well as viewing the record of sent messages.

- **ALARM Section**
  Functions related to the alarm events generated in the various installation monitors, in addition to MMS configurations related to these alarms.

- **SYSTEM Section**
  Functions for configuring MMS according to the respective MEET installation. These configurations include the registration of different devices (panels, monitors, etc.), as well as the management of different users of the software.

- **ACCESS CONTROL Section**
  Allows the user to register/unregister proximity cards and facial recognition of authorised users in the installation and to view records generated by the corresponding events related to these users.

4.1 Basic initial configuration of MMS

MMS is an application for managing alarms and events related to the different devices of a specific installation (outdoor panels, monitors and guard units), as well as for access control for the different users of the installation (access control by card and/or facial recognition).
MMS will therefore need to be configured initially so it can communicate with all these devices, as follows:

1. **Registering devices. See section 4. 4 4 SYSTEM: DEVICES**
   Follow the indicated procedure to register all the devices in the installation, and define their groups (if required).
   You can also assign software users (administrators and/or concierges).

2. **Check devices online. See section 4.4.2 ONLINE SYSTEM**
   Once you've registered all the devices, check that they have been correctly registered and are controlled properly by MMS.

3. **Registering proximity cards. See section 4.5.3 ACCESS CONTROL: CARDS**
   Follow these instructions to register proximity cards to be assigned to users of the installation.

4. **Programming facial recognition. See section 4.5.4 ACCESS CONTROL: FACIAL ID**
   Follow these instructions to define the users authorised to open the access doors using facial recognition.

5. **Loading authorised cards onto panels. See section 4.5.6 ACCESS CONTROL: LOAD ID**
   Follow these instructions to load the data of the authorised cards onto the corresponding panels, in addition to the facial recognition data.

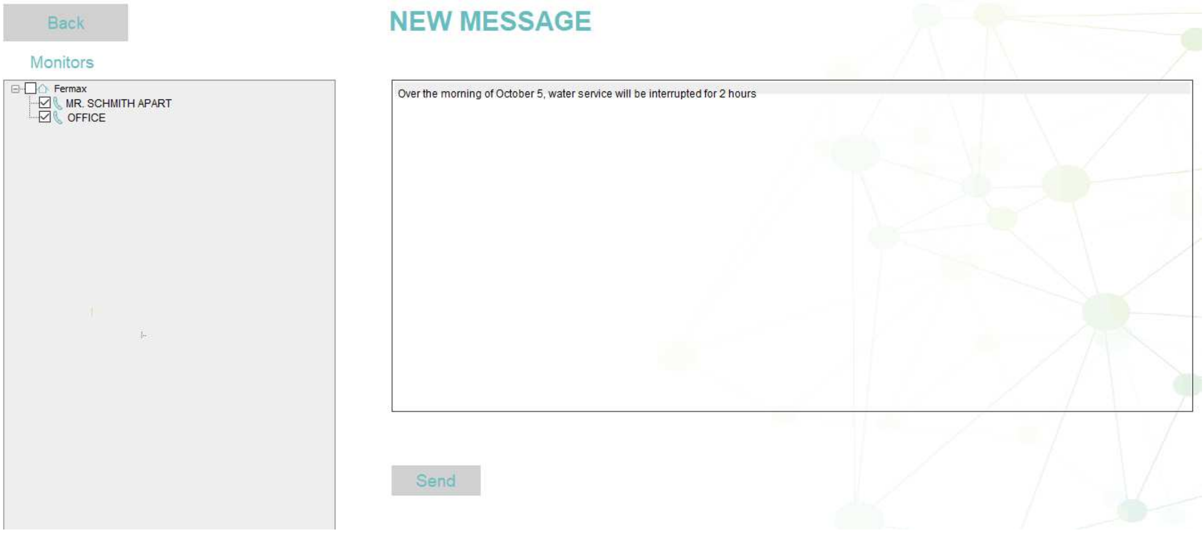
4.2 MESSAGE Section

Allows you to use the functions related to sending text messages to a monitor or a group of monitors, as well as viewing the record of sent messages.

There are 2 options in this section:

4.2.1 MESSAGES: NEW MESSAGE

Use this feature to send text messages to the desired monitors or groups of monitors. Message length is limited to 254 characters, including spaces.



Over the morning of October 5, water service will be interrupted for 2 hours

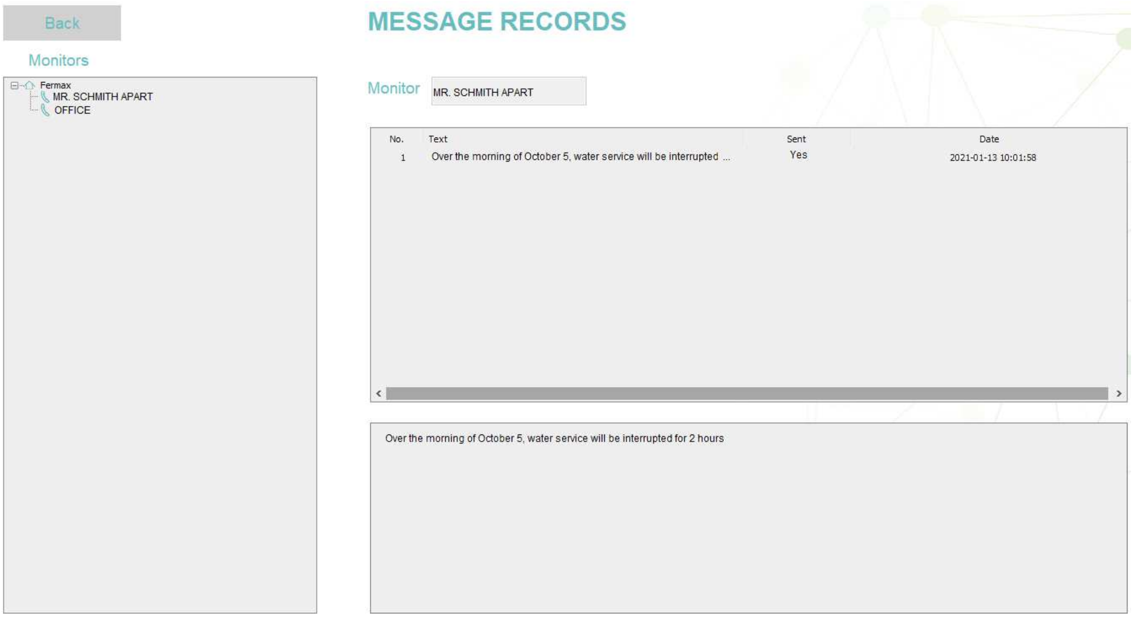
- Select the monitors or groups that you want to message from the column on the left.
- Enter the message text and select **Send**.

You will be asked for confirmation and then receive a notification that the message has been successfully sent to the selected recipients -

- When finished, select **Back**.

4.2.2 MESSAGE: MESSAGE RECORDS

Allows you to check the status of sent messages, including message content, and date/time sent.



MESSAGE RECORDS

Monitor: MR. SCHMITH APART

No.	Text	Sent	Date
1	Over the morning of October 5, water service will be interrupted ...	Yes	2021-01-13 10:01:58

Over the morning of October 5, water service will be interrupted for 2 hours

- Select the monitor you want to check from the column on the left.
  In the central section you will see the header of the sent message, the reception status and the date/time when it was sent.

- Select the message to view the full contents.
  The full message text will appear in the section below.

- When finished, select **Back**.

4.3 ALARM Section

Functions related to the alarm events generated in the various installation monitors, in addition to MMS configurations related to these alarms.

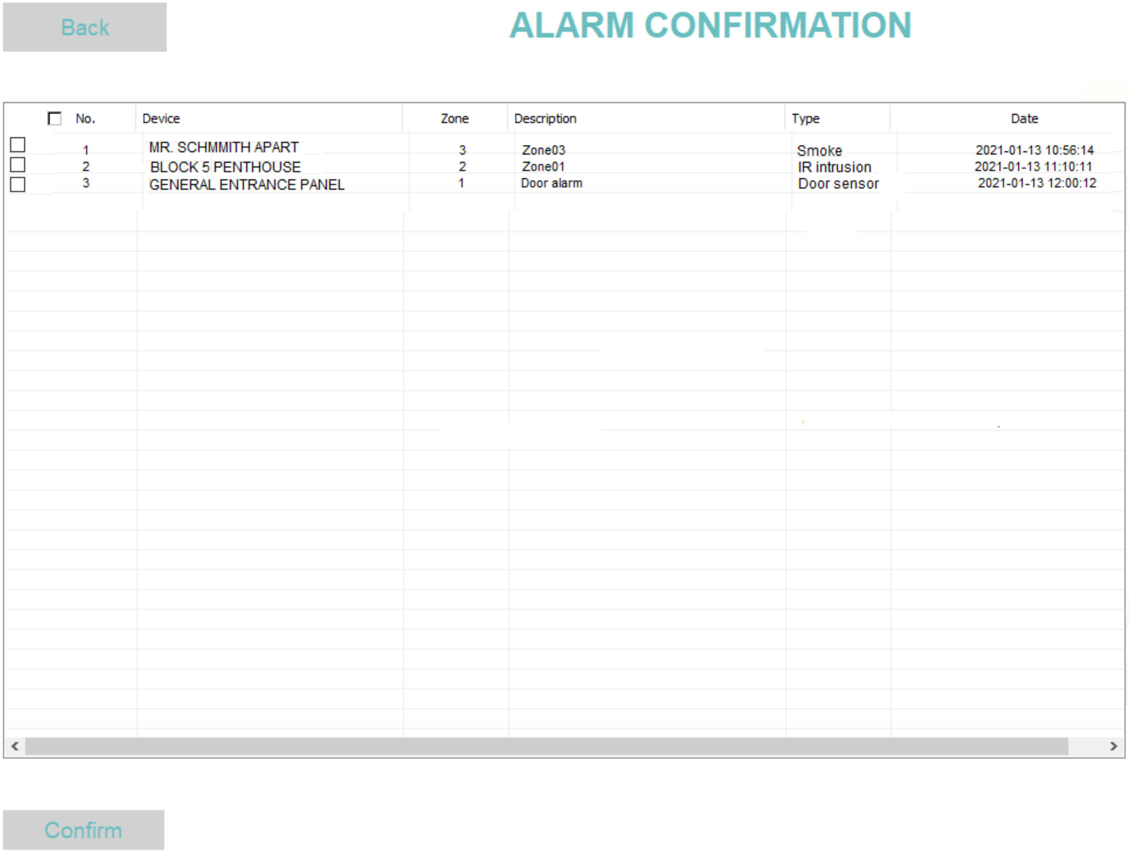
There are 5 options in this section:

4.3.1 ALARMS: CONFIRM

This section gives the user information about the alarms generated in the apartment monitors and in the outdoor panels, at the moment they occur.
If an alarm occurs, a list with information about the alarm or alarms that have just occurred will automatically appear on the computer screen.

The concierge can confirm that they have taken a note of them, and then remove them from the list. However, they will remain recorded in the alarm log (see next section).

The MMS station will continue sounding an alert as long as there are alarms in this list pending acknowledgement.



	☐ No.	Device	Zone	Description	Type	Date
☐	1	MR. SCHMMITH APART	3	Zone03	Smoke	2021-01-13 10:56:14
☐	2	BLOCK 5 PENTHOUSE	2	Zone01	IR intrusion	2021-01-13 11:10:11
☐	3	GENERAL ENTRANCE PANEL	1	Door alarm	Door sensor	2021-01-13 12:00:12

- **Device:** Monitor or panel where the alarm was generated.
- **Area:** No. of the alarm zone affected on the indicated device.
- **Description:** Description of the affected alarm area.
- **Type:** Additional information about the type of sensor installed in that zone.

- **Date:** The date and time when the alarm occurred.
- Check the box on the left corresponding to a certain event and select **OK** to confirm and delete an alarm event.

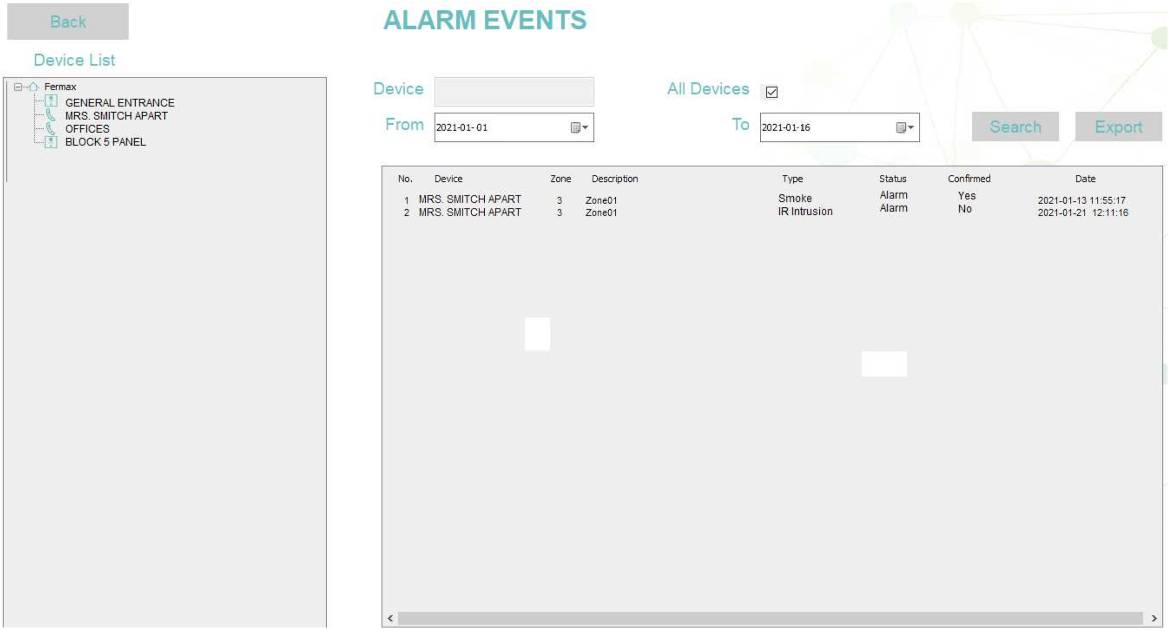
- **NOTES:**
  The alarm will remain active on the affected device (monitor or panel) regardless of whether it has been removed from this list.

  The alarm will be stored in the alarm log (see next section), even if the alarm has been acknowledged.

4.3.2 ALARMS: EVENTS

You can check which alarms have been generated on a particular monitor or panel (or on all of them) during a given period of time.

The displayed lists can also be exported to the computer in EXCEL format for further analysis.



Fermax
GENERAL ENTRANCE
MRS. SMITCH APART
OFFICES
BLOCK 5 PANEL

Device
All Devices ☑
From 2021-01- 01
To 2021-01-16

No.	Device	Zone	Description	Type	Status	Confirmed	Date
1	MRS. SMITCH APART	3	Zone01	Smoke	Alarm	Yes	2021-01-13 11:55:17
2	MRS. SMITCH APART	3	Zone01	IR Intrusion	Alarm	No	2021-01-21 12:11:16

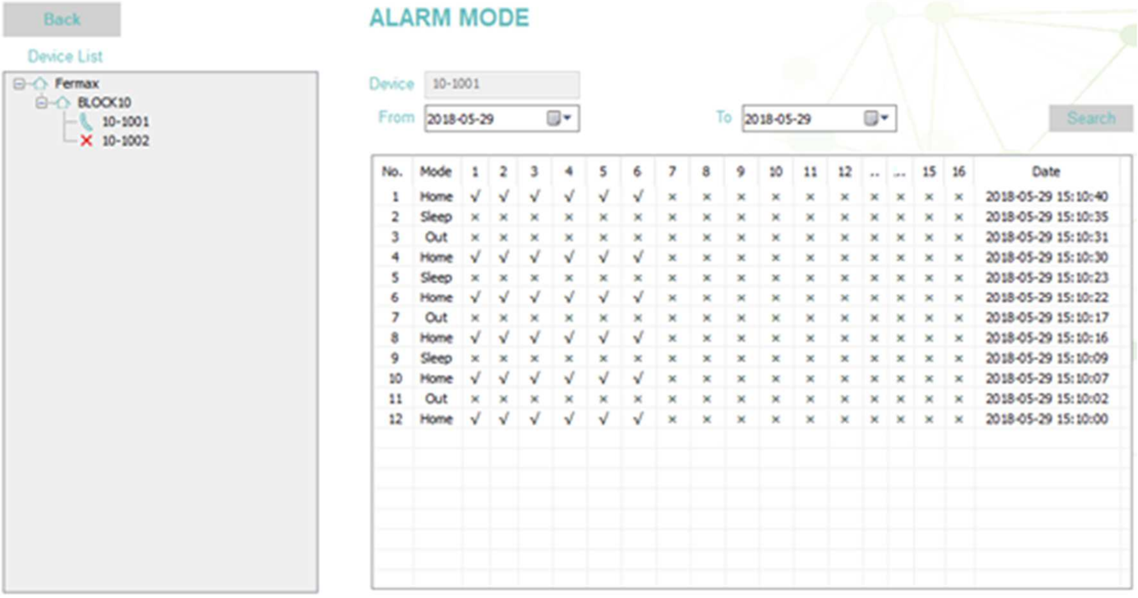
- Select the device with the alarm information that you want to view from the column on the left (or select the **All** check box **,** if you want information from all devices).
- Indicate the date range for the information you want to view.
- Select **Search**, to obtain the list, which will contain the information related to the indicated event or events. The Confirm column indicates whether the event has been confirmed for display (Yes) or if it is still pending (No).
- Select **Export** if you want to obtain an EXCEL spreadsheet containing the presented information.

NOTE:
Alarm information will remain in the log regardless of whether it has been viewed or exported.

4.3.3 ALARMS: MODE

This feature lets you see the status of the MEET alarm system for the monitor in a particular apartment, and it also keeps a record of changes of status (night, day, or house) over a certain period of time.

It also gives you an indication of the protected areas for each of the cases.



Device 10-1001

From 2018-05-29 To 2018-05-29

No.	Mode	1	2	3	4	5	6	7	8	9	10	11	12	..	...	15	16	Date
1	Home	√	√	√	√	√	√	×	×	×	×	×	×	×	×	×	×	2018-05-29 15:10:40
2	Sleep	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	2018-05-29 15:10:35
3	Out	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	2018-05-29 15:10:31
4	Home	√	√	√	√	√	√	×	×	×	×	×	×	×	×	×	×	2018-05-29 15:10:30
5	Sleep	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	2018-05-29 15:10:23
6	Home	√	√	√	√	√	√	×	×	×	×	×	×	×	×	×	×	2018-05-29 15:10:22
7	Out	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	2018-05-29 15:10:17
8	Home	√	√	√	√	√	√	×	×	×	×	×	×	×	×	×	×	2018-05-29 15:10:16
9	Sleep	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	2018-05-29 15:10:09
10	Home	√	√	√	√	√	√	×	×	×	×	×	×	×	×	×	×	2018-05-29 15:10:07
11	Out	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	2018-05-29 15:10:02
12	Home	√	√	√	√	√	√	×	×	×	×	×	×	×	×	×	×	2018-05-29 15:10:00

- Select the monitor with the ALARM MODE information you want to see from the column on the left.
- Indicate the date range for the information you want to view.
- Select **Search** to view the list.
  It will list the changes of alarm status in date order (Home, Out or Night) indicating which zones were active or not active in each case.

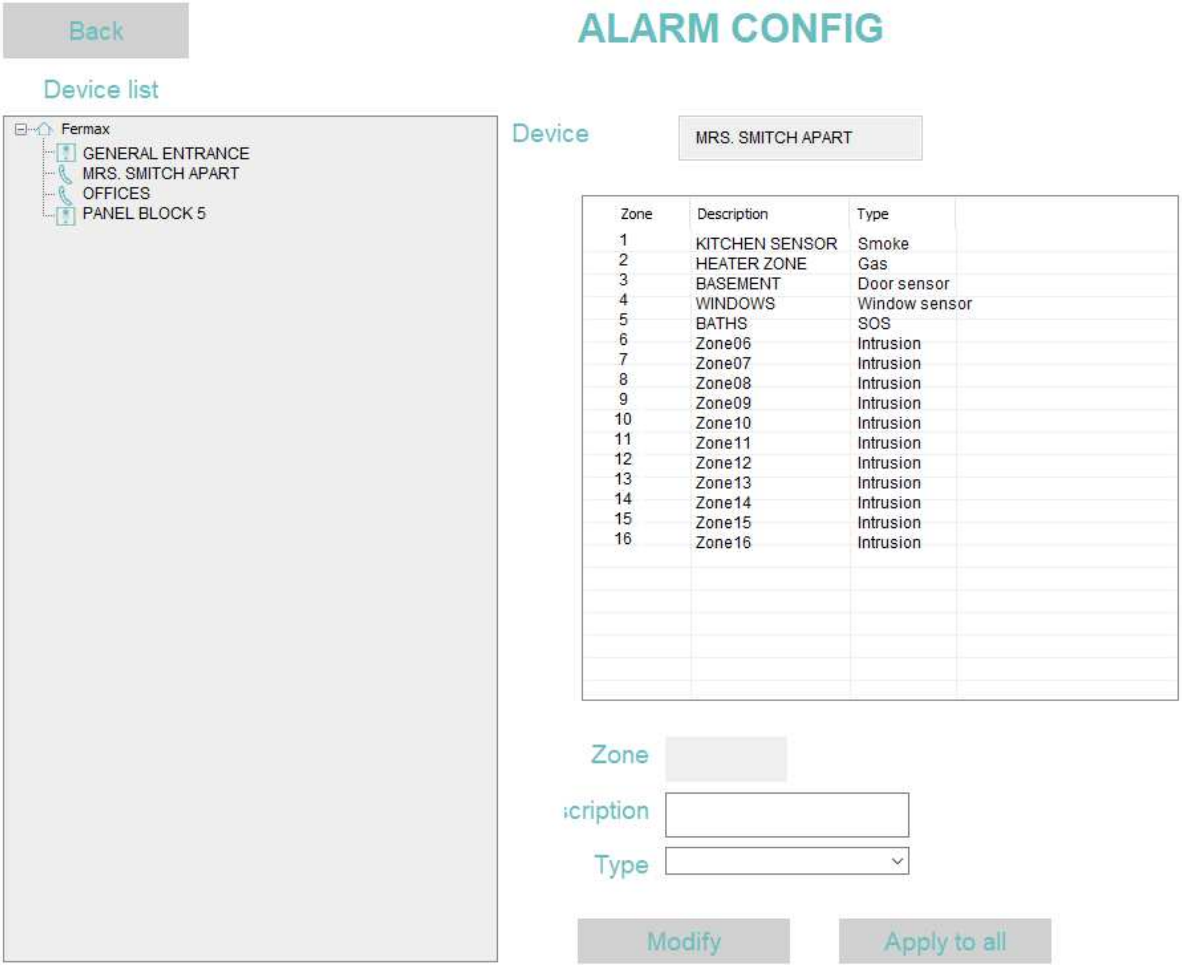
4.3.4 ALARMS: CONFIG

This feature allows you to change the text information provided by MMS when an alarm is generated in an apartment or a panel, replacing it with text that is more intuitive and understandable for MMS users.

For example, if an alarm is triggered from the zone 1 monitor, the alarm log entry will show Zone01 in the description field.

You can use this feature to replace this text with something more descriptive, such as KITCHEN SENSOR.

These changes can be made independently for each device in the installation.



Fermax
- GENERAL ENTRANCE
- MRS. SMITCH APART
- OFFICES
- PANEL BLOCK 5

Device: MRS. SMITCH APART

Zone	Description	Type
1	KITCHEN SENSOR	Smoke
2	HEATER ZONE	Gas
3	BASEMENT	Door sensor
4	WINDOWS	Window sensor
5	BATHS	SOS
6	Zone06	Intrusion
7	Zone07	Intrusion
8	Zone08	Intrusion
9	Zone09	Intrusion
10	Zone10	Intrusion
11	Zone11	Intrusion
12	Zone12	Intrusion
13	Zone13	Intrusion
14	Zone14	Intrusion
15	Zone15	Intrusion
16	Zone16	Intrusion

- Select the device with the alarm information record text that you want to change from the column on the left.
  Information on all the alarm entries from that device will be displayed in the central box.
- Select the entry with the text that you want to change.
- Enter the descriptive text you want for this entry in the **Description** field.
- Select the associated sensor type from the **Type** box.
- Select **Modify** to apply the changes.

- Select **Apply to all** if you want the change you made to be applied to all entries on the device.

  NOTES:
  The new alarm events that occur will be described and identified using the new text.

  These changes will not affect alarm events already in the logs.

4.3.5 ALARMS: SMS

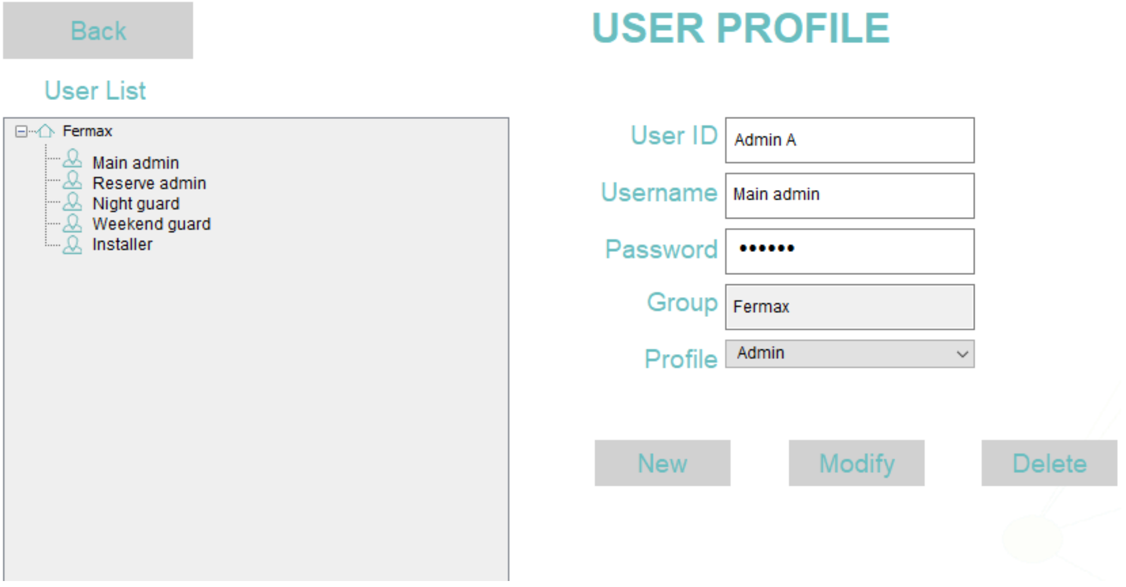
This function cannot be used with this version of the Software.

4.4 SYSTEM Section

This section offers configuration functions for adapting MMS to the corresponding MEET installation. These configurations include the registration of different devices (panels, monitors, etc.), as well as the management of different users of the software.

4.4.1 SYSTEM: USER

You can use this section to register users of MMS software, and also to assign the profile for each of them.



USER PROFILE

Fermax
- Main admin
- Reserve admin
- Night guard
- Weekend guard
- Installer

User ID: Admin A
Username: Main admin
Password: ••••••
Group: Fermax
Profile: Admin

- **User ID**: A unique ID to identify each of the MMS users. It is very important that users do not forget their ID, as they will need it to identify themselves when using MMS.
  The default ID (when no other users have been assigned yet) is **Installer**.

- **Username**: The name assigned to the corresponding user.

- **Password**: Assign the password thatthe corresponding user will need to use for accessing MMS. The default password for the **Installer** user ID is **123456**.
  A.

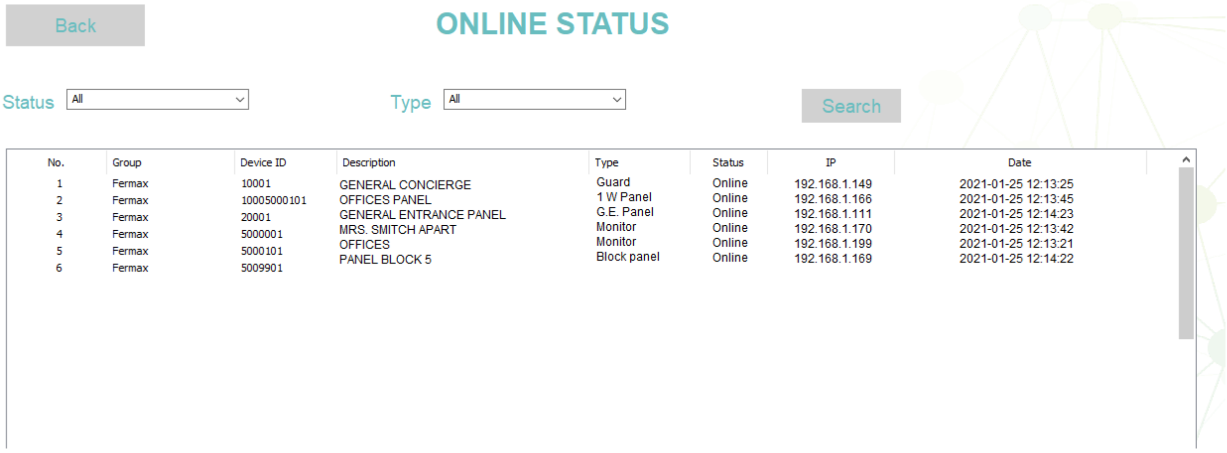
- **Group:** Choose the group that you want to assign this user to. The groups need to be set up beforehand. See section 4.4.4. SYSTEM: DEVICES -> Groups.
  If a group has not already been set up, choose **Fermax**.

- **Profile:** Select the profile you want to assign to this user. See the profile hierarchy in section **1.1. User profiles**.

- Enter **New** to save the data, **Modify** if you want to amend the previous data, or **Delete** if you want to delete the indicated user record.

4.4.2 SYSTEM: ONLINE

This section allows you to check if all the devices in the installation are connected to the system properly. It shows the ID for each device, a description, the type of device, its IP address and the last date when it was detected by MMS, as well as its status: Online.



Status: All

Type: All

No.	Group	Device ID	Description	Type	Status	IP	Date
1	Fermax	10001	GENERAL CONCIERGE	Guard	Online	192.168.1.149	2021-01-25 12:13:25
2	Fermax	10005000101	OFFICES PANEL	1 W Panel	Online	192.168.1.166	2021-01-25 12:13:45
3	Fermax	20001	GENERAL ENTRANCE PANEL	G.E. Panel	Online	192.168.1.111	2021-01-25 12:14:23
4	Fermax	5000001	MRS. SMITCH APART	Monitor	Online	192.168.1.170	2021-01-25 12:13:42
5	Fermax	5000101	OFFICES	Monitor	Online	192.168.1.199	2021-01-25 12:13:21
6	Fermax	5009901	PANEL BLOCK 5	Block panel	Online	192.168.1.169	2021-01-25 12:14:22

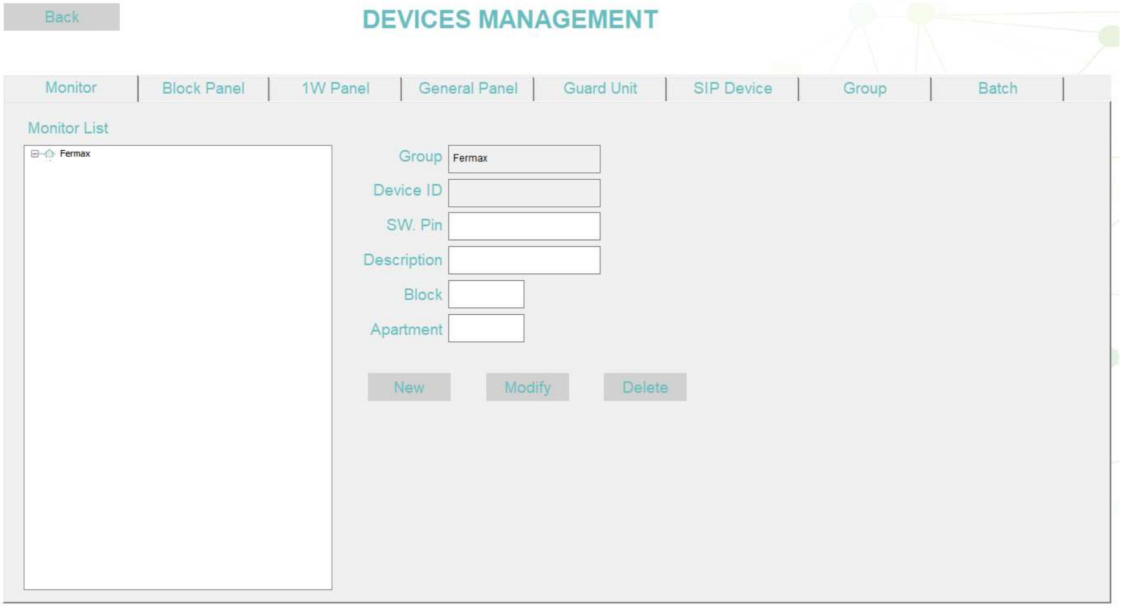
If a device is in the offline status, this means that it is not properly connected to MMS, so you won't be able to interact with it (send messages, receive alarms, etc.).
You should resolve the issue as soon as possible (device switched off, offline, etc.).

4.4.3 SYSTEM: SIP RECORD

This function cannot be used with this version of the software.

4.4.4 SYSTEM: DEVICES

Use this section to register the MEET devices in the installation that you want to control with MMS.



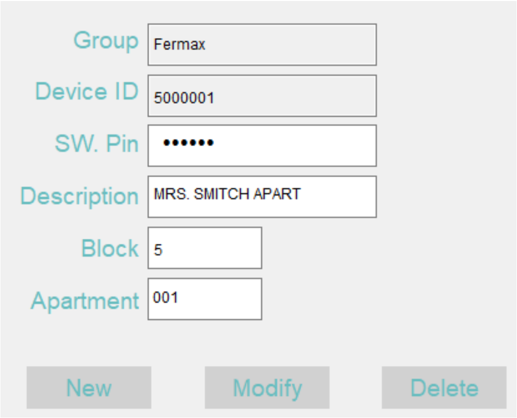
Fermax

Group: Fermax
Device ID:
SW. Pin:
Description:
Block:
Apartment:

Select the tab corresponding to the type of device you want to register and enter the required information.

Monitor

Use this form to enter data for all the monitors in the installation.



Group: Fermax
Device ID: 5000001
SW. Pin: ••••••
Description: MRS. SMITCH APART
Block: 5
Apartment: 001

- **Group:** Choose the group. If no group has been created, choose Fermax.
- **Device ID:** Automatically assigned by MMS.
- **SW PIN:** A password that must match the NETWORK -> SW PIN field programmed in the monitor itself.
- **Description**: Enter a description for this device. You can use letters, numbers and special characters.
- **Block**: Enter the block number for the monitor.
- **Apartment:** Enter the apartment number for the monitor.

When you've finished, select **New**.

- Select **Modify** if you want to change any of the parameters you've entered, or **Delete** if you want to delete the entire record.

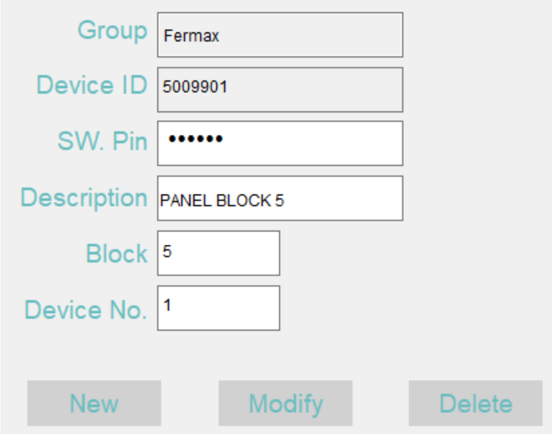
The devices being added will appear in the left column, along with their status:

☎ **MRS. GARCIA APARTMENT**: The monitor has been successfully registered.
It may take a few seconds for this icon to appear.

✗ **MRS. GARCIA APARTMENT:** The monitor has not been registered correctly.
If this icon does not change after a few seconds, check the information entered.

Block panel

Use this form to enter the information for all the block panels in the installation.



Group	Fermax
Device ID	5009901
SW. Pin	••••••
Description	PANEL BLOCK 5
Block	5
Device No.	1

- **Group:** Choose the group. If no group has been created, choose Fermax.
- **Device ID:** Automatically assigned by MMS.
- **SW PIN**: A password that must match the NETWORK -> SW PIN field programmed in the panel itself.
- **Description:** Enter a description for this device. You can use letters, numbers and special characters.
- **Block**: Enter the block number for the panel.
- **Apartment:** Enter the apartment number for the monitor.

When you've finished, select **New**.

Select **Modify** if you want to change any of the parameters you've entered, or **Delete** if you want to delete the entire record.

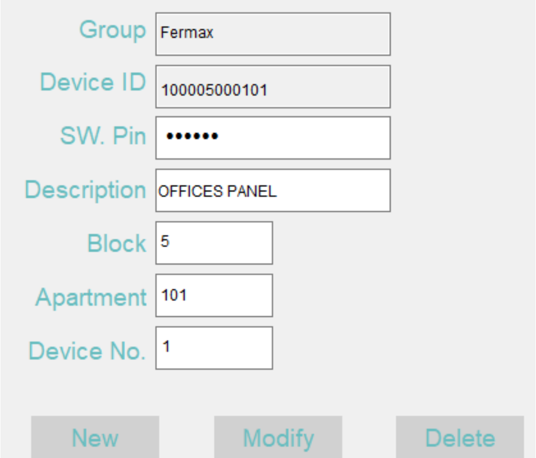
The devices being added will appear in the left column, along with their status:

▣ **BLOCK 5 PANEL**: The panel has been successfully registered.
It may take a few seconds for this icon to appear.

✗ **BLOCK 5 PANEL:** The panel has not been registered correctly.
If this image does not change after a few seconds, check the information entered.

Panel 1 pushbutton

Use this form to enter the information for all the 1-pushbutton panels in the installation.



Group	Fermax
Device ID	100005000101
SW. Pin	••••••
Description	OFFICES PANEL
Block	5
Apartment	101
Device No.	1

- **Group:** Choose the group. If no group has been created, choose Fermax.
- **Device ID:** Automatically assigned by MMS.

- **SW PIN:** A password that must match the NETWORK -> SW PIN field programmed in the panel itself.
- **Description:** Enter a description for this device. You can use letters, numbers and special characters.
- **Block**: Enter the block number for the panel.
- **Apartment**: Enter the apartment number associated with the pushbutton on the panel.
- **Device No:** Enter the same panel number that was used when it was programmed.

When you've finished, select **New**.

Select **Modify** if you want to change any of the parameters you've entered, or **Delete** if you want to delete the entire record.

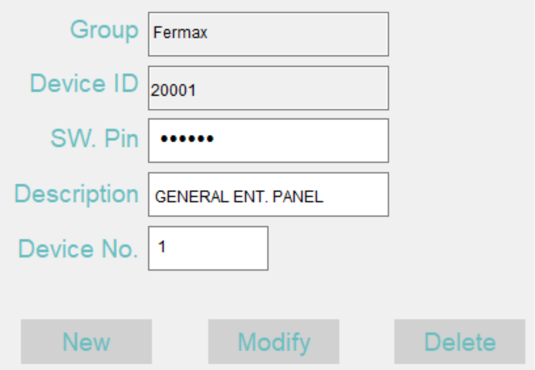
The devices being added will appear in the left column, along with their status:

OFFICE PANEL: The panel has been successfully registered.
It may take a few seconds for this icon to appear.

✗ **OFFICE PANEL:** The panel has not been registered correctly.
If this image does not change after a few seconds, check the information entered.

General panel

Use this form to enter the data for all general entry panels in the system



Group	Fermax
Device ID	20001
SW. Pin	••••••
Description	GENERAL ENT. PANEL
Device No.	1

- **Group:** Choose the group. If no group has been created, choose Fermax.
- **Device ID:** Automatically assigned by MMS.
- **SW PIN**: A password that must match the NETWORK -> SW PIN field programmed in the panel itself.
- **Description:** Enter a description for this device. You can use letters, numbers and special characters.
- **Device No:** Enter the same panel number that was used when it was programmed.

When you've finished, select **New**.

Select **Modify** if you want to change any of the parameters you've entered, or **Delete** if you want to delete the entire record.

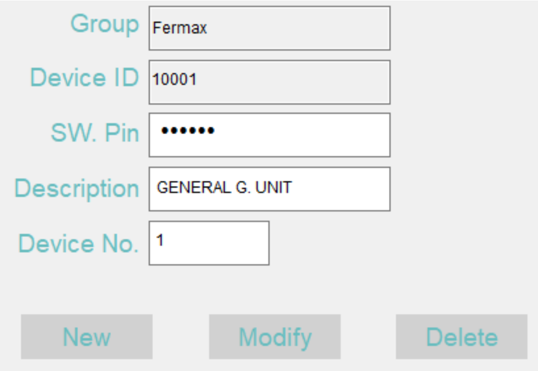
The devices being added will appear in the left column, along with their status:

BLOCK 5 PANEL: The panel has been successfully registered.
It may take a few seconds for this icon to appear.

✗ **BLOCK 5 PANEL:** The panel has not been registered correctly.
If this image does not change after a few seconds, check the information entered.

Guard unit

Use this form to enter the information for all the guard units in the installation.



Group	Fermax
Device ID	10001
SW. Pin	••••••
Description	GENERAL G. UNIT
Device No.	1

- **Group:** Choose the group. If no group has been created, choose Fermax.
- **Device ID:** Automatically assigned by MMS.
- **SW PIN**: A password that must match the NETWORK -> SW PIN field programmed in the panel itself.
- **Description:** Enter a description for this device. You can use letters, numbers and special characters.
- **Device No:** Enter the same guard unit number that was used when it was programmed.

When you've finished, select **New**.

Select **Modify** if you want to change any of the parameters you've entered, or **Delete** if you want to delete the entire record.

The devices being added will appear in the left column, along with their status:

GENERAL GUARD UNIT: The guard unit has been successfully registered..
It may take a few seconds for this icon to appear.

✗ **GENERAL GUARD UNIT:** The guard unit has not been registered correctly.
If this image does not change after a few seconds, check the information entered.

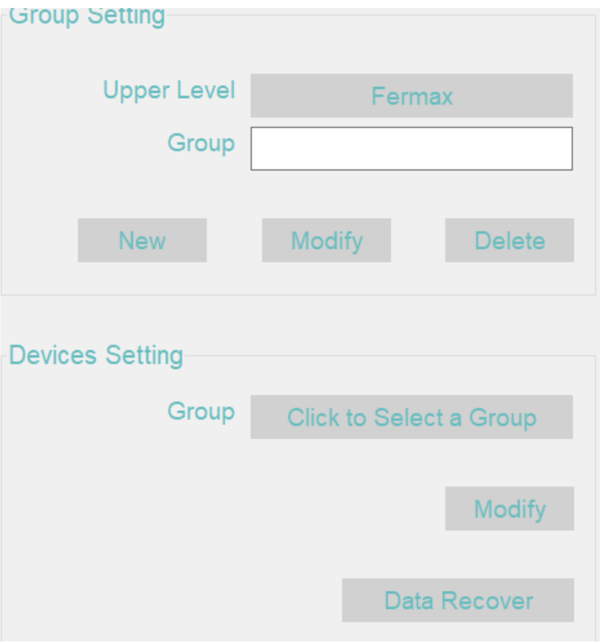
SIP device

This function cannot be used with this version of the software.

Group

This feature allows you to group the registered devices into a tree structure. *For example, you can group together all devices (monitors and panels) in a certain block or section of a condominium*.
Grouping the devices like this makes it easier to manage other software functions, such as sending general text messages or registering proximity cards.

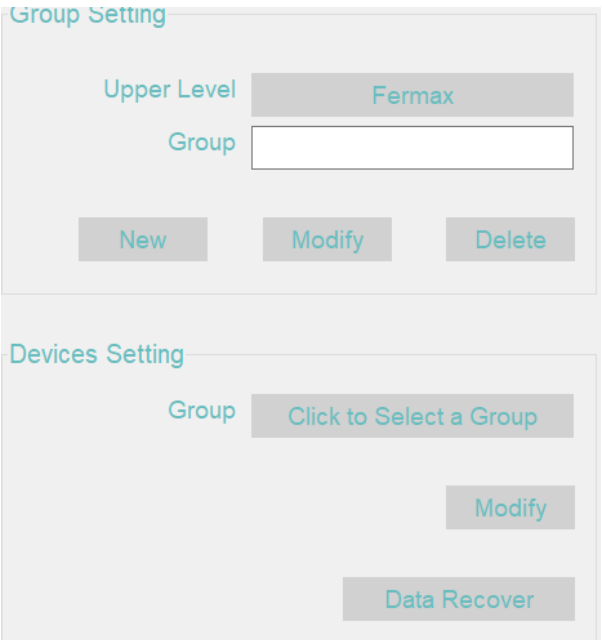
Use this form for creating groups and assigning the corresponding devices or elements to the blocks created.



Upper Level: Fermax

Group configuration

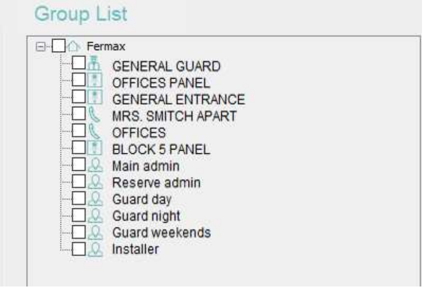
- **Upper level:** From the group list, select the group above the one that you are creating.
  If no group has been created yet, choose Fermax**.**
- **Group:** Enter the name for the new group you are creating.
- **New:** Click to create the new group. *It will appear in the group list on the left*.
- **Modify:** Select the group you want to modify (rename), and click on this button.
- **Delete:** Select the group you want to delete, and click on this button The elements of this group will move to the upper level group.



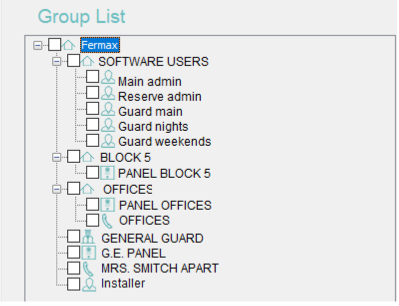
Device Setting

- **Group:** From the group list, select the group that you want to assign devices to.
- **Modify:** Indicate the elements to be assigned to the marked group and click on this button.
- **Data recovery**: Allows you to recover any data lost when modifying groups.

What the group list looks like before and after creating and configuring the SOFTWARE USERS, BLOCK 5, and OFFICE groups. The groups can be collapsed, to make it easier to find them in the list.


Group List

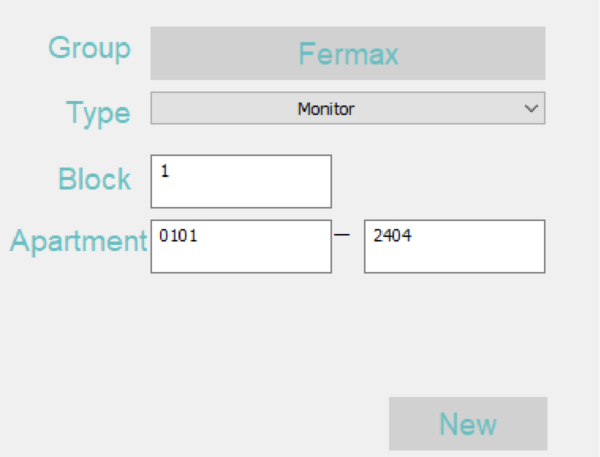
- □ Fermax
  - □ GENERAL GUARD
  - □ OFFICES PANEL
  - □ GENERAL ENTRANCE
  - □ MRS. SMITCH APART
  - □ OFFICES
  - □ BLOCK 5 PANEL
  - □ Main admin
  - □ Reserve admin
  - □ Guard day
  - □ Guard night
  - □ Guard weekends
  - □ Installer


Group List

- □ Fermax
  - □ SOFTWARE USERS
    - □ Main admin
    - □ Reserve admin
    - □ Guard main
    - □ Guard nights
    - □ Guard weekends
  - □ BLOCK 5
    - □ PANEL BLOCK 5
  - □ OFFICES
    - □ PANEL OFFICES
    - □ OFFICES
  - □ GENERAL GUARD
  - □ G.E. PANEL
  - □ MRS. SMITCH APART
  - □ Installer

Batch

Once the groups have been created, this feature allows you to save a set of monitors or 1-pushbutton panels (batch) to a certain group at the same time.


Group: Fermax

Type: Monitor

Block: 1

Apartment: 0101 — 2404

- **Group:** From the group list, select the group that you want to save devices to.
- **Type:** Select whether the devices will be monitors or 1L panels.
- **Block:** Enter the block number for the devices.
- **Apartment:** Define the addressing range for the devices (see **NOTE**).
- **New:** Click to generate the batch.

NOTE:

The apartment range consists of 4 digits. The first two define the floor and the second two define the number of apartments on that floor

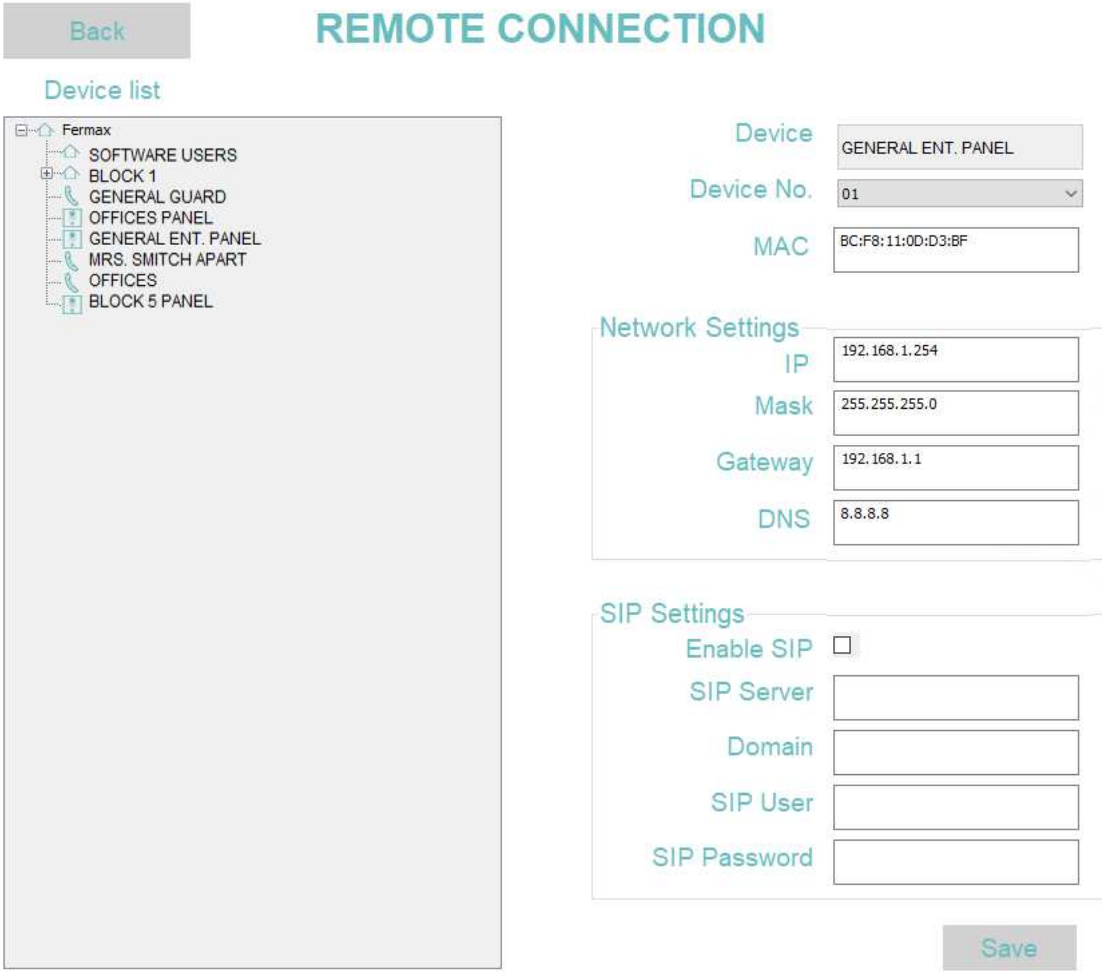
For example, for a 5-storey building, with 7 apartments per floor, the range would be set as 0101-0507, creating the following addresses:

0101	**0102**	**0103**	**0104**	**0105**	**0106**	**0107**
0201	**0202**	**0203**	**0204**	**0205**	**0206**	**0207**
0301	**0302**	**0303**	**0304**	**0305**	**0306**	**0307**
0401	**0402**	**0403**	**0404**	**0405**	**0406**	**0407**
0501	**0502**	**0503**	**0504**	**0505**	**0506**	**0507**

4.4.5 SYSTEM: REMOTE

Allows you to remotely modify configuration settings for the installation's devices, such as the IP address or SIP configuration.

The device being modified must be configured and accessible by MMS, and you will need to know its MAC.



REMOTE CONNECTION

Device list

- Fermax
  - SOFTWARE USERS
  - BLOCK 1
  - GENERAL GUARD
  - OFFICES PANEL
  - GENERAL ENT. PANEL
  - MRS. SMITCH APART
  - OFFICES
  - BLOCK 5 PANEL

Device: GENERAL ENT. PANEL

Device No.: 01

MAC: BC:F8:11:0D:D3:BF

Network Settings

IP: 192.168.1.254

Mask: 255.255.255.0

Gateway: 192.168.1.1

DNS: 8.8.8.8

SIP Settings

Enable SIP ☐

SIP Server

Domain

SIP User

SIP Password

- Select the device with the configuration you want to change from the Device list.
- Enter the MAC for the device.
- Enter the new Network Configuration or Remote Configuration details. *You must enter all the details, even those that you are not changing*.
- The new configuration will take effect after about 3 minutes**.**

NOTE:

For this operation, the computer should only be connected to the LAN network of the devices, even if it is capable of controlling several.

4.4.6 SYSTEM: PORTS

Allows you to configure the UART for connecting and configuring the COMPUTER CARD READER Ref. 9438. See Annex for more details.

It also allows NAT redirection, when the CARD READER is on a remote computer.

4.5 CONTROL ACCESS Section

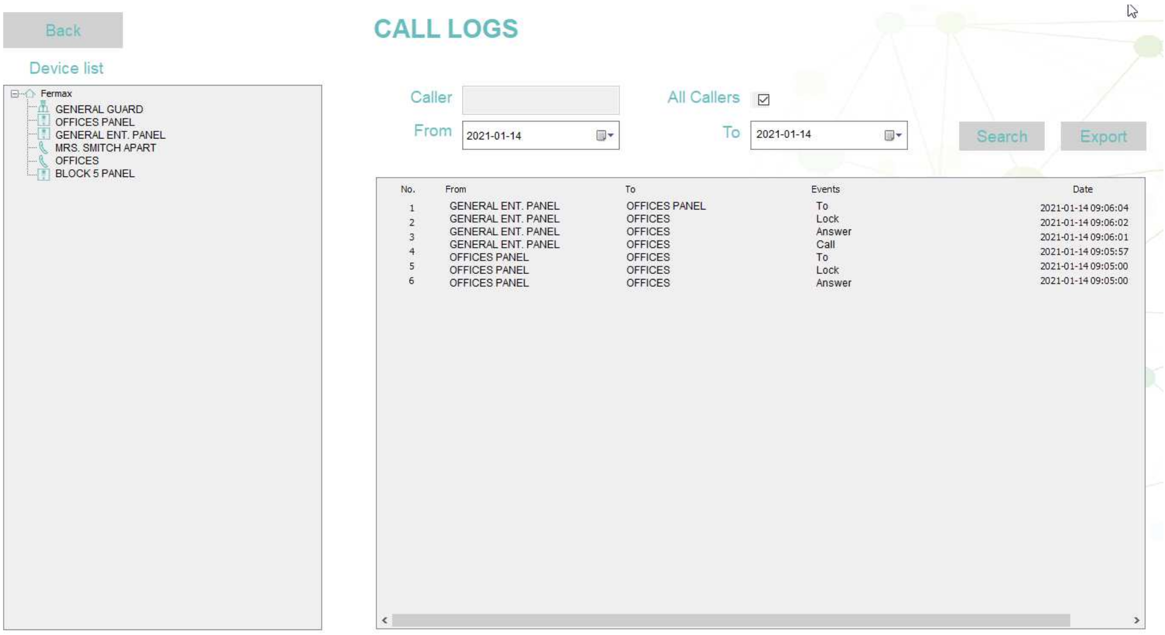
Allows you to manage proximity card registrations/cancellations and facial recognition of authorised users in the installation, and also to view records generated by the corresponding events related to these users.

4.5.1 CONTROL ACCESS: CALL LOGS

You have the option to view all call activity on a particular monitor, panel or guard unit (or on all the devices) over a certain period of time.
This includes calls made, calls received, calls answered, calls ended and door releases.

If the event is a call from a outdoor panel, it is also possible to obtain the image captured by the outdoor panelcamera when the call was made.

The displayed lists can also be exported to the computer in EXCEL format for further analysis.



Fermax
- GENERAL GUARD
- OFFICES PANEL
- GENERAL ENT. PANEL
- MRS. SMITCH APART
- OFFICES
- BLOCK 5 PANEL

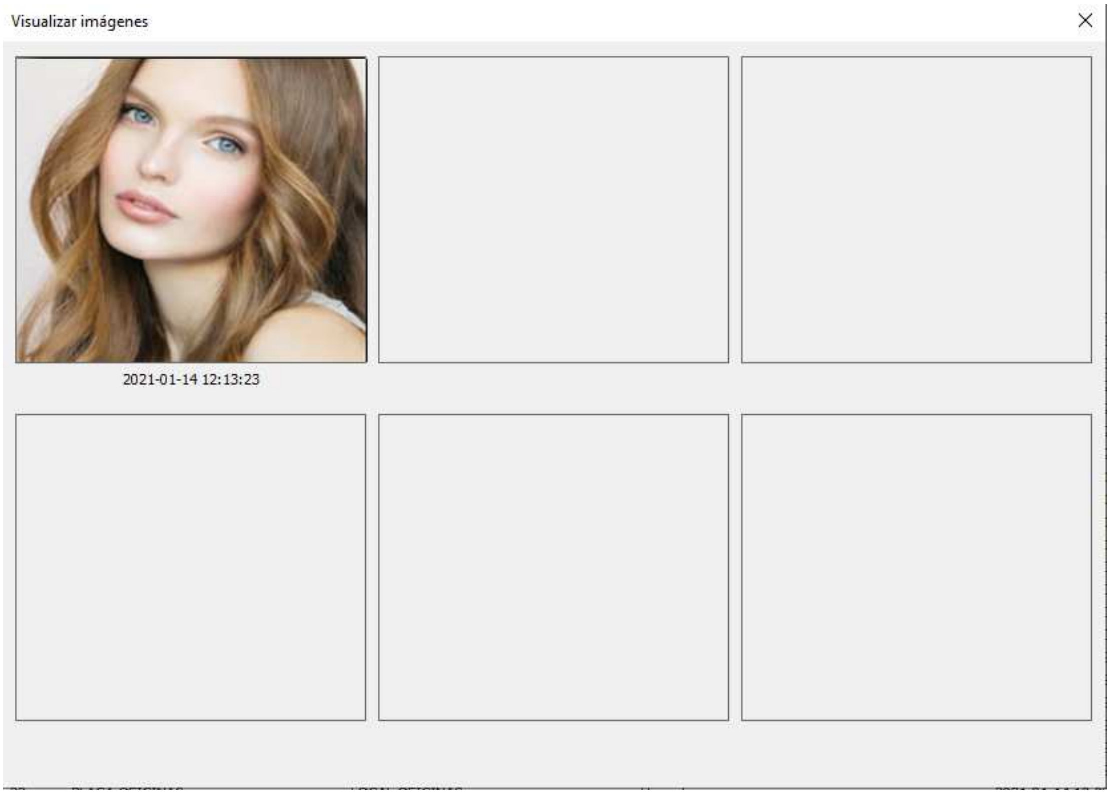
Caller

All Callers ☑

From 2021-01-14 To 2021-01-14

No.	From	To	Events	Date
1	GENERAL ENT. PANEL	OFFICES PANEL	To	2021-01-14 09:06:04
2	GENERAL ENT. PANEL	OFFICES	Lock	2021-01-14 09:06:02
3	GENERAL ENT. PANEL	OFFICES	Answer	2021-01-14 09:06:01
4	GENERAL ENT. PANEL	OFFICES	Call	2021-01-14 09:05:57
5	OFFICES PANEL	OFFICES	To	2021-01-14 09:05:00
6	OFFICES PANEL	OFFICES	Lock	2021-01-14 09:05:00
	OFFICES PANEL	OFFICES	Answer	

- Select the device with the call information that you want to view from the column on the left (or select the **All** checkbox **,** if you want information from all devices).
- Indicate the date range for the information you want to view.
- Select **Search**, to obtain the list, which will contain the information related to the indicated event or events. As well as the exact date and time of the event.
- Select **Export** if you want to obtain an EXCEL spreadsheet containing the presented information.
- If the indicated record relates to a call from the outdoor panel, double click on the **Caller**box to obtain the image captured by the camera at the time of the call and each time the door lock is activated from the apartment(up to a total of 6 images).

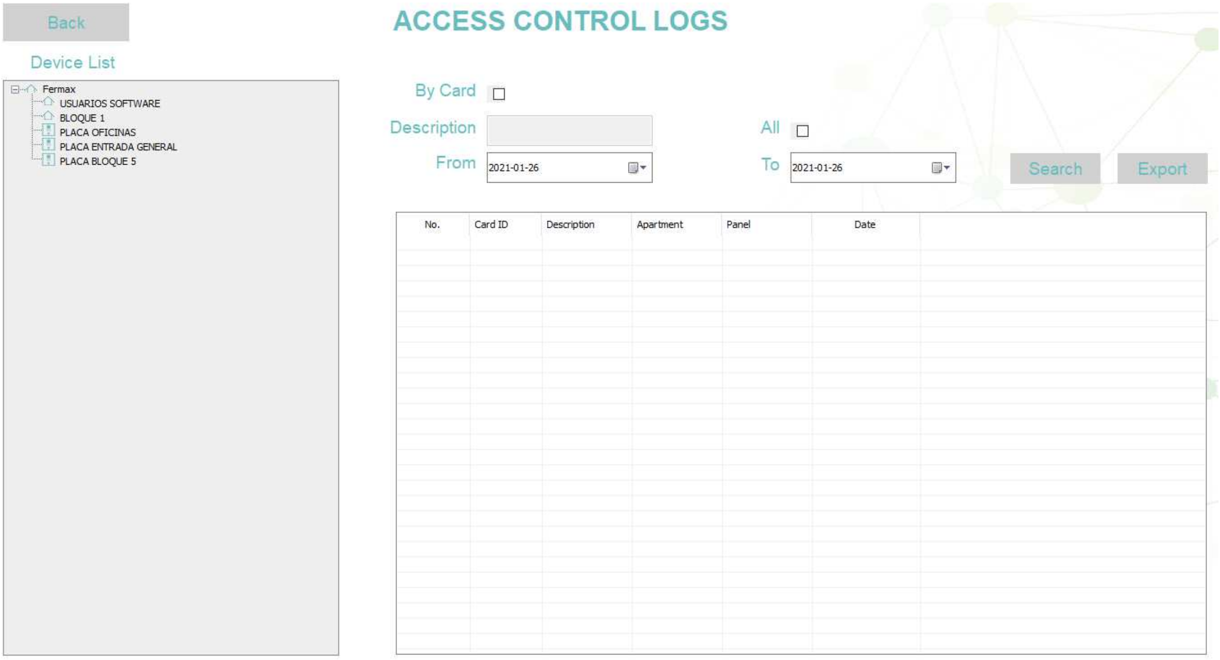


NOTE:

Call records will remain in the log regardless of whether they have been viewed or exported.

4.5.2 CONTROL ACCESS: ACCESS LOGS

This allows you to monitor access activity from users in the installation, whether it be for a specific access point, a group of access points or even to find out which access points a user has passed through with a certain card.



- Fermax
  - USUARIOS SOFTWARE
  - BLOQUE 1
  - PLACA OFICINAS
  - PLACA ENTRADA GENERAL
  - PLACA BLOQUE 5

By Card □

Description

All □

From 2021-01-26

To 2021-01-26

No.	Card ID	Description	Apartment	Panel	Date

- From the **Device List** column, select the access point where you want to see all the users who have passed through over a certain period of time.
- Select **All**, if you want to check all the access points.
- Indicate the date range for the information you want to view.
- Select **By card** if you want to see all the points accessed by a particular user. You can find all the cards in the Device List. Choose the one that you're interested in.
- Select **Search**, to obtain the list, which will contain the information related to the indicated event or events. As well as the exact date and time of the event.
- Select **Export** if you want to obtain an EXCEL spreadsheet containing the presented information.

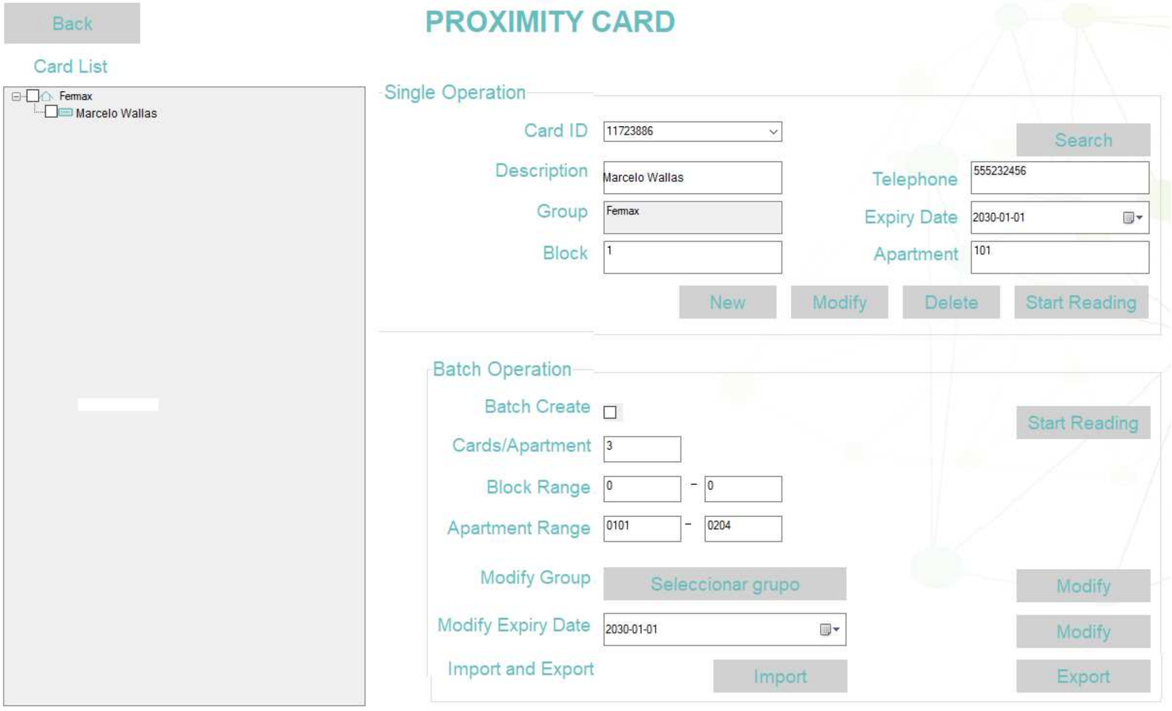
4.5.3 ACCESS CONTROL: PROXIMITY CARDS

MMS allows you to manage the access of system users through the entrances for which they have authorisation, which they can enter by presenting their personal proximity card to the reader on the corresponding access panel.
The CARD MANAGEMENT functionality is used for registering the corresponding proximity cards and assigning them authorisation for the assigned panel(s).

When registering a card, you will need to enter the BLOCK and APARTMENT details for the corresponding card user.

It is possible to register cards directly if you know the WIEGAND serial number for the cards. If not, you will need a COMPUTER PROXIMITY CARD READER Ref. 9438, which must be plugged into the computer's USB port. In this case you will need to have the specific card with you.
See the ANNEX of this document to find out how to install and configure the COMPUTER PROXIMITY CARD READER before using it.

You could also use an Excel spreadsheet containing the data of a batch of cards, if you want to register them all at the same time.



PROXIMITY CARD

Card List
- Fermax
  - Marcelo Wallas

Single Operation

Card ID	11723886		
Description	Marcelo Wallas	Telephone	555232456
Group	Fermax	Expiry Date	2030-01-01
Block	1	Apartment	101

Batch Operation

Batch Create	□
Cards/Apartment	3
Block Range	0 – 0
Apartment Range	0101 – 0204
Modify Group	Seleccionar grupo
Modify Expiry Date	2030-01-01
Import and Export	

You will need to enter the following details:

Individual Management (registering one card at a time)

- **Card ID:** You can use the WIEGAND serial number of the card, if you know it, or use the **Read Card** procedure below.
- **Description:** Enter a description for the card user (name or details of the apartment).
- **Telephone:** Enter the user's telephone number (optional).
- **Group:** Indicate the group, if it has been created. Otherwise indicate Fermax.

- **Expiry date:** If you want the card to expire on a certain date, you can enter that here.
- **Block:** Enter the block corresponding to the user's apartment (according to the name used when the system was programmed).
- **Apartment:** Enter the user's apartment number (according to the name used when the system was programmed).
- **New:** Confirm the details you've entered. The user description for the registered card will appear on the **Card List**.
- **Modify:** Select a user from the Card List and then click this button to make changes to the registered details.
- **Delete:** Select a user record from the Card List and then click this button to delete it. The associated card can be registered to be used again.
- **Start Reading:** Click on this button and then scan the card with the COMPUTER PROXIMITY CARD READER . The serial number for the card will appear in the **Card ID box**.

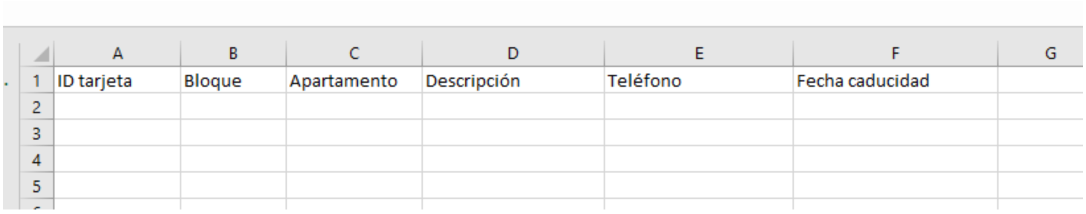
Batch management (register several cards sequentially or via an Excel spreadeheet)

- **Batch Create:** Tick this box first
- **Apt. cards**: Enter the number of cards to be registered
- **Block range**: Enter the block range containing the apartment of the users who will receive the cards once programmed.
- **Apartment range**: Indicate the range of user apartments where the cards will be delivered once programmed.
- **Start Reading**: Once the above details have been entered, click on this button and then scan all the cards in the batch sequentially with the COMPUTER PROXIMITY CARD READER.
  The cards will be assigned the APARTMENT and BLOCK as per the ranges entered, starting with the lowest values.
  For example, if you have 100 cards and the ranges indicated are block range: 4 and apartment Range 25, the programming sequence will be:

  Card 1: Apartment 1-Block 1
  Card 2: Apartment 2-Block 1
  Card 3: Apartment 3-Block 1
  …
  Card 25: Apartment 25-Block 1
  Card 26: Apartment 1-Block 2
  ….
  Card 75: Apartment 25-Block 3
  Card 76: Apartment 1-Block 4
  ….
  Card 100: Apartment 25-Block 4

- **Modify group**: Click here if you want to put the cards into a different group other than the current one.

- **Modify expiry date:** Enter an expiry date for all the cards in the batch, if applicable.
- **Import:** Click here if you would like to take the batch data from an Excel spreadsheet created expressly for this purpose.
  The spreadsheet must be in the following format:



	A	B	C	D	E	F	G
1	ID tarjeta	Bloque	Apartamento	Descripción	Teléfono	Fecha caducidad	
2							
3							
4							
5							

- **Export:** Click here if you want to export the entered data to an Excel spreadsheet to expand or modify it.
  It will be exported with the name ***Card_date-creation_time-creation.xls.***

NOTE:

Once the cards have been registered, the authorised accesses must be assigned to them and then the data must be loaded onto the corresponding panels (See section 4.5.5 MANAGEMENT: AUTHORISE)

4.5.4 ACCESS CONTROL: FACE ID

This function allows you to configure the MEET facial recognition system, which enables users (residents or condominium employees) to be recognised by the camera on the outdoor panels of the blocks and the general entrances, to open the corresponding door if the user is authorised.

MMS version V1.0.6 is compatible with the MEET panel firmware version V3.0. For panels with older versions, use MMS V1.0.5. See the panel installation manual for more details.

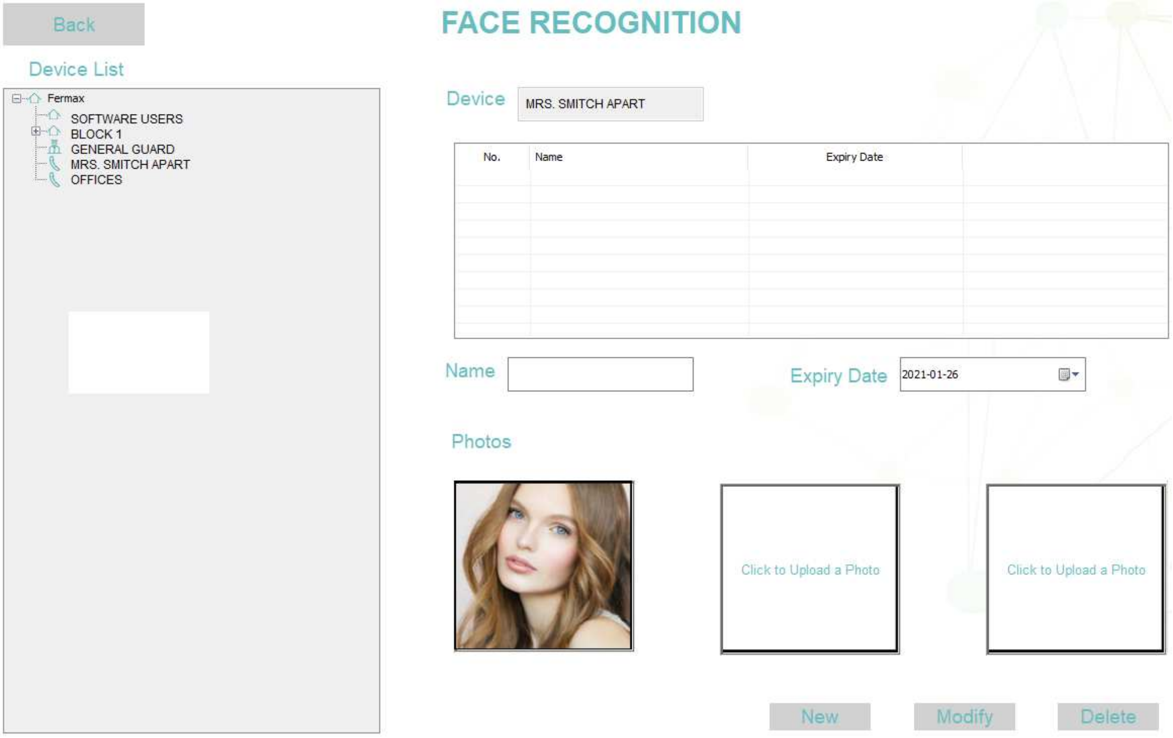
To register a user in the facial recognition system, they will need to be associated with the monitor corresponding to their apartment, in the case of a residents, or with the guard unit, in the case of condominium employees.

To register a user in the facial recognition system, you will need a photograph of their face, in JPG or MPG format.

To make the system more versatile, it is possible to use 2 or 3 different photos for each user, but this will reduce the system capacity from 6000 users to 3000 (if 2 photos are used for each user) or 2000 (if 3 photos are used for each user).

It is possible to assign an expiration date for each user, after which the access authorisation will no longer be effective.

The procedure for registering users is as follows:



FACE RECOGNITION

Device: MRS. SMITCH APART

No.	Name	Expiry Date

Name:

Expiry Date: 2021-01-26

- Select the user apartment to be registered from the Device List. In the case of a condominium employee, select the guard unit.
- Click on **New**.
  An empty user details (New Resident) will appear in the central box, along with a symbolic expiration date (01-01-2050).

- Select this "new resident" and enter the name or reference in the **Name** box**.**
- Change the expiry date, if necessary**.**
- Click on the **Upload a Photo** box on the left. Find the corresponding photo on your computer and upload it. If you require more versatility, repeat this operation with the following box(es).
- To finish, click on **Modify**. A confirmation message will appear.

NOTES:

The panels must have the FACIAL RECOGNITION function enabled.

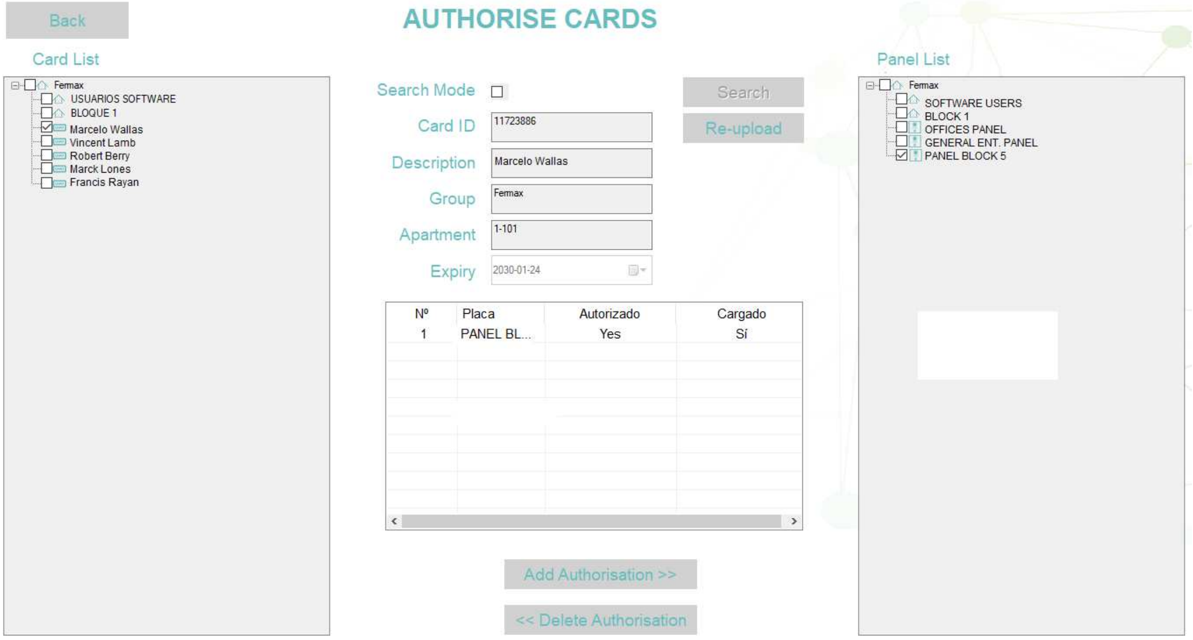
The MEET facial recognition system is based on a two-dimensional identification process, so it may reject flat images from printed photos, smartphone screens, etc.

The MEET facial recognition system is designed to enable users to open the entrance door easily, without the need to use keys or make a call. It is not a security system, so it is not possible to guarantee 100% reliability.

Once you have configured the facial identification, this information will need to be uploaded to the MEET system. See section 4.5.6 ACCESS CONTROL: UPLOAD.

4.5.5 ACCESS CONTROL: AUTHORISE

Once a proximity card has been registered (Section 4.5.3 ACCESS CONTROL: PROX CARDS) you will need to tell the system which installation access point(s) the card user is authorised to use.



AUTHORISE CARDS

Back

Card List

- ⊟ □ Fermax
  - □ USUARIOS SOFTWARE
  - □ BLOQUE 1
  - ☑ Marcelo Wallas
  - □ Vincent Lamb
  - □ Robert Berry
  - □ Marck Lones
  - □ Francis Rayan

Search Mode □

Card ID: 11723886

Description: Marcelo Wallas

Group: Fermax

Apartment: 1-101

Expiry: 2030-01-24

Nº	Placa	Autorizado	Cargado
1	PANEL BL...	Yes	Sí

Panel List

- ⊟ □ Fermax
  - □ SOFTWARE USERS
  - □ BLOCK 1
  - □ OFFICES PANEL
  - □ GENERAL ENT. PANEL
  - ☑ PANEL BLOCK 5

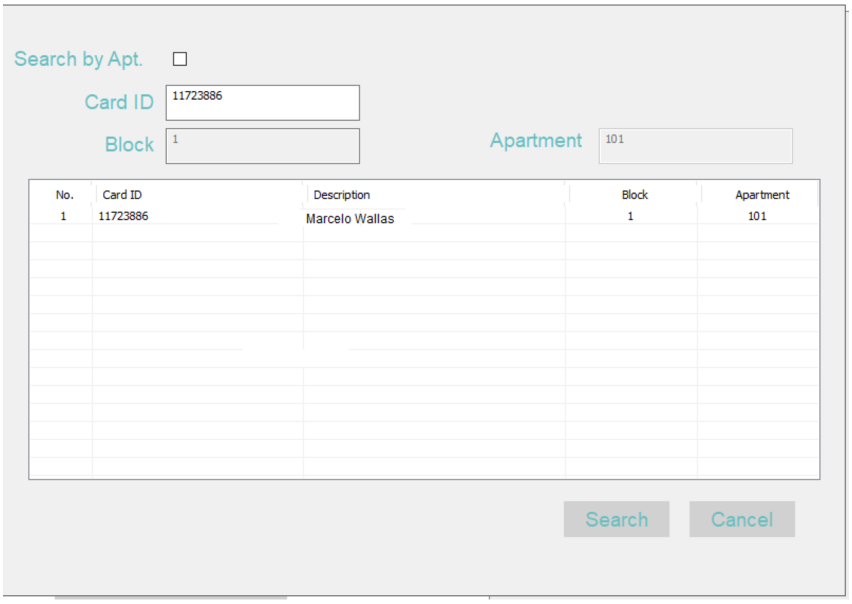
You can assign card authorisations as follows:

- Select the card to be authorised from the Card List.
  In the boxes below you will see the details of the corresponding card user.
- Select the panel(s) authorised to the associated user from the Panel List.

- Click the **Add Authorisation** button.
- If you wish to cancel a card authorisation, select it then click the **Delete authorisation** button.

There is a procedure for locating a specific card to make the work easier in cases where many cards have already been registered. This search can be done using the card's Wiegand number or the block number and associated apartment:

- Select the **Search Mode** box. The **Search** button will then be enabled.
- Click on **Search**. A new form will appear:



Search by Apt. □

Card ID: 11723886

Block: 1

Apartment: 101

No.	Card ID	Description	Block	Apartment
1	11723886	Marcelo Wallas	1	101

- Enter the Wiegand no. for the card. The card details will then appear.

It is also possible to locate all the cards assigned to users of a certain apartment. To do this:

- Select the **Search by Apt** box. The **Block** and **Apartment** boxes will then be enabled.
- Enter the corresponding block and apartment number. The details of the cards associated with the apartment will appear.

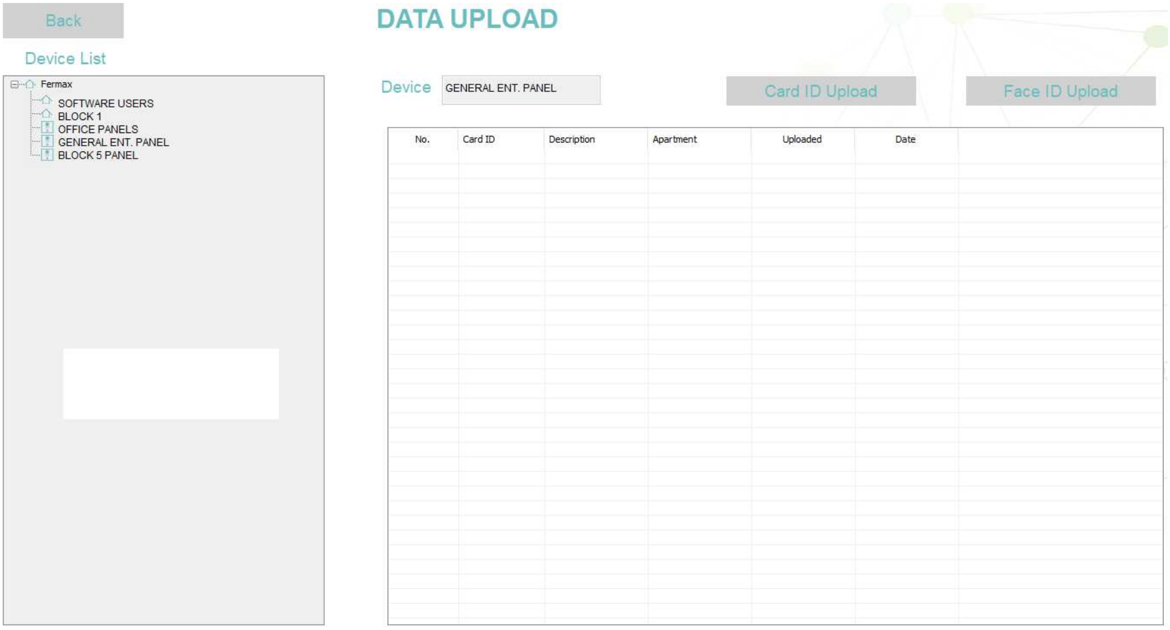
NOTE:

Once you've configured the card permissions for the different access points, this information will need to be loaded onto the corresponding panels - see following section.

4.5.6 ACCESS CONTROL: UPLOAD

Once you've configured MMS with the authorised access points for each card, this information will need to be loaded onto the corresponding panels in the installation.

Facial ID configuration information will also need to be uploaded to all building panels in the installation.



Device GENERAL ENT. PANEL

No.	Card ID	Description	Apartment	Uploaded	Date

Select the panel where you would like to send the updated information from the Device List.

- Click on **Card ID Upload**
- Repeat these steps when updating any other panel.
- If you have configured or modified the facial ID, click on **Face ID Upload**

NOTE:

You will need to perform these steps each time you make a change (add, delete, or modify) to MMS card settings or the face ID settings.

The facial ID will be uploaded to all the digital panels in the installation.

5 ANNEX

5.1 Configuration for remote use

The MEET system can be remotely managed over the internet, so the control station can be located in a different place from the installation.

This is very useful as it allows you to remotely manage various installations in different locations from the same place, or even several different places.

There will need to be a computer running constantly at the installation site.

MMS will need to be configured locally on this computer (registration of devices, cards and facial recognition). Once these steps have been completed, basic management tasks for the installation can be performed from the remote computer (alarm control, sending messages, etc.).

However, proximity cards and facial recognition can only be registered/unregistered locally.

The SECURITY ENCRYPTED KEY (DONGLE) Ref. 9540 can only be installed on the remote computer.

Bear in mind the following:

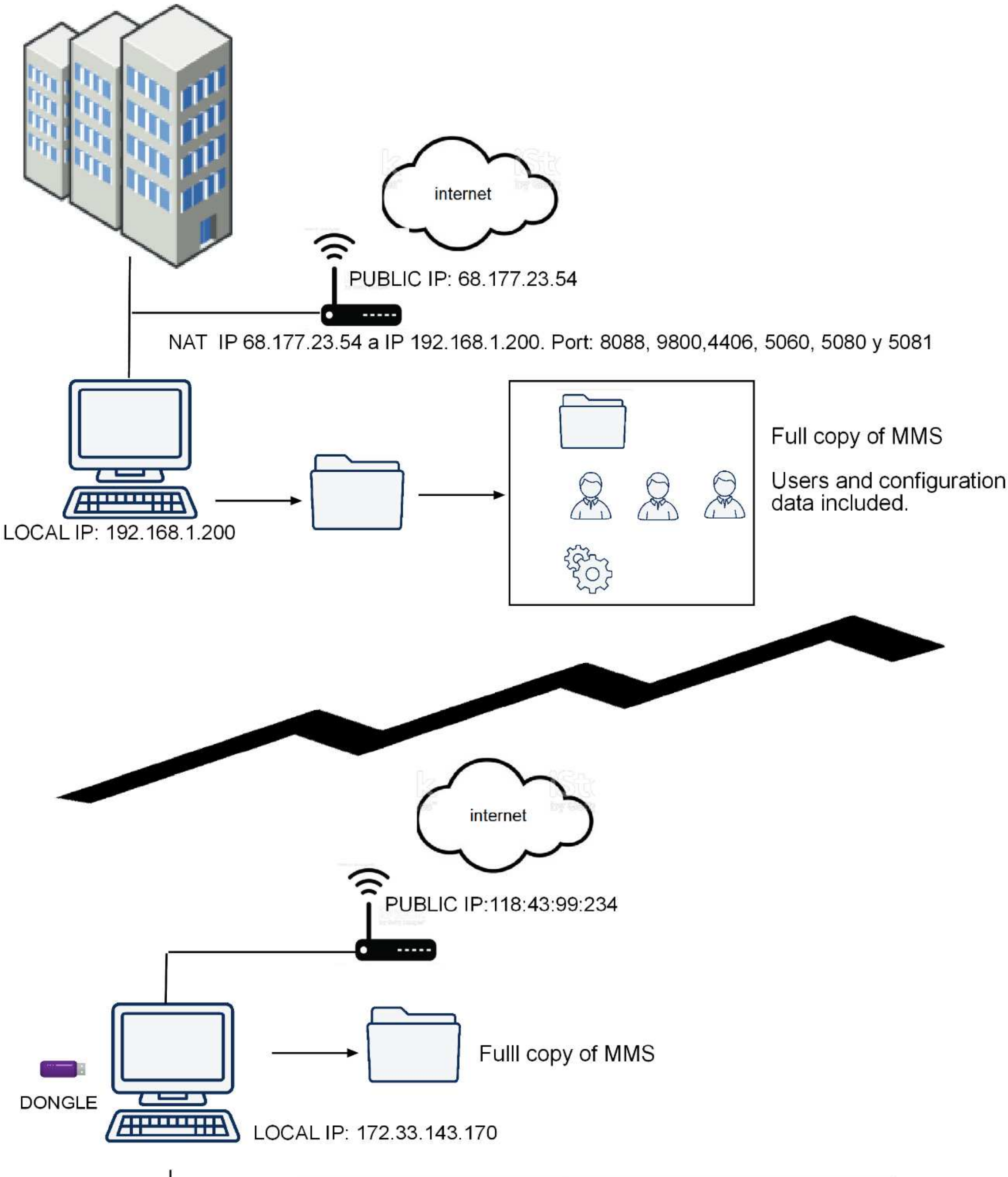
On the installation side:

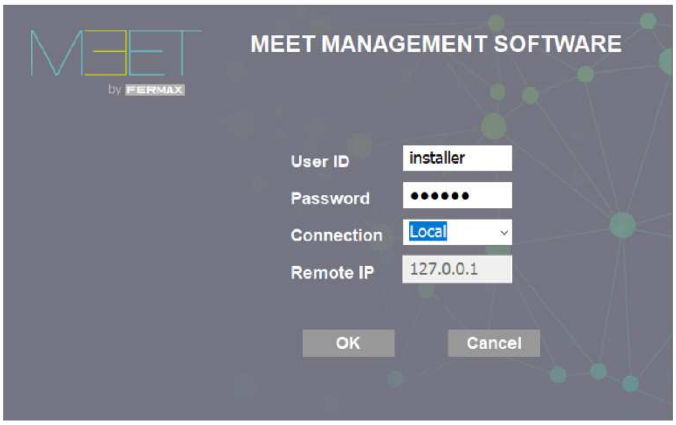
- The computer will need to be running constantly, with an internet connection and a fixed local IP address.
- The PUBLIC IP must be fixed, and known.
- The devices and users must be fully configured with MMS on the local computer, as explained in the various sections in this manual. When finished, close MMS, but leave the computer powered on with the watchdog.exe application running.
- **A NAT must be done in the router from the public IP to the local IP, using ports 8088, 9800, 4406, 5060, 5080 and 5081**.

On the remote computer side:

- A computer with an internet connection.
- Start MMS, as already explained in this manual.
- Log in with a **User ID** -which must have been registered locally on the installation computer- and the corresponding **Password**.
- Under **Connection**, choose Remote.
- Under **Remote IP**, enter the Public IP for the installation site.

Example configuration for remote MMS use





User ID: installer

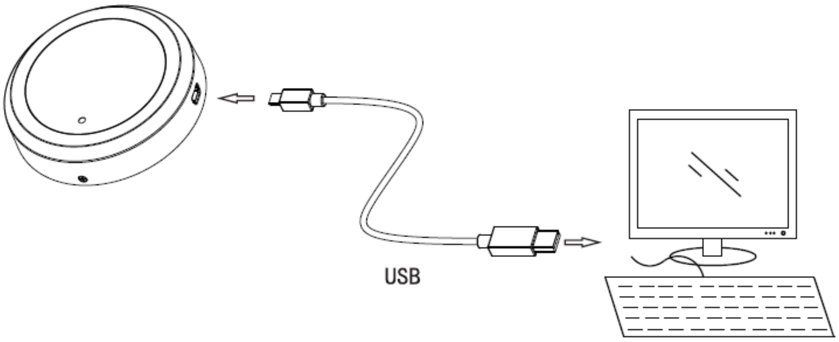
Password: ••••••

Connection: Local

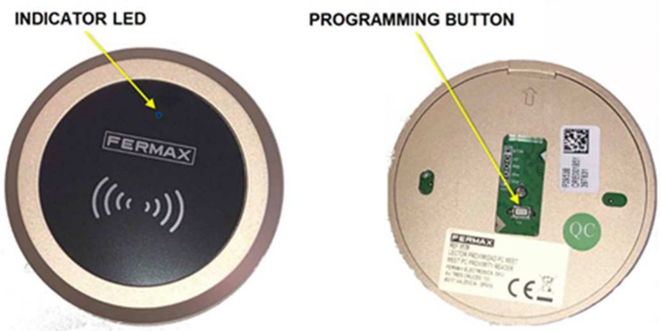
Remote IP: 127.0.0.1

5.2 Installation and configuration of COMPUTER PROXIMITY CARD READER Ref. 9538

- **Connection to the computer**
  - Use the included USB cable to connect the Meet Proximity Reader to your computer. You will hear a confirmation beep.

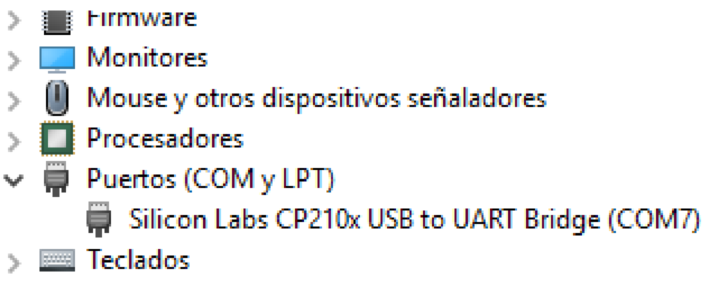


- **MEET protocol selection**
  - The MEET Computer Proximity Reader can work with different protocols, so you will need to select the one corresponding to MEET so it connects to the computer correctly.



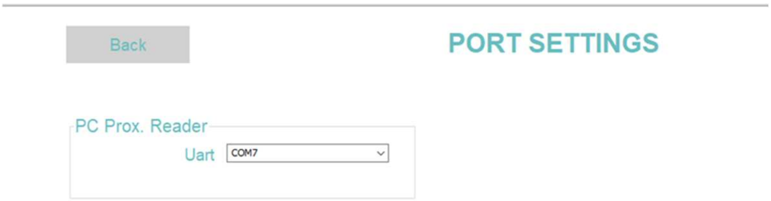
  - Each time you do a short press on the PROGRAMMING BUTTON (see image below), you will hear a series of one, two, three or four beeps, depending on the selected protocol. The INDICATOR LED will also blink simultaneously with these beeps.
  - To select the MEET protocol, press the PROGRAMMING BUTTON repeatedly until you only hear one beep.

- **Driver installation**
  - Download the updated Silicon Labs**CP210ISB to UART Bridge** driver from **https://www.fermax.com/spain/pro/soporte-online.html** by clicking on the MEET-Drivers Ref. 9538 link. Install and take a note of the assigned COM port.
  - In the following example, the assigned port is COM7.



Firmware
Monitores
Mouse y otros dispositivos señaladores
Procesadores
Puertos (COM y LPT)
Silicon Labs CP210x USB to UART Bridge (COM7)
Teclados

- **Select the Computer Proximity Reader UART**
  - Start the MEET Management Software application and go to the PORT CONFIGURATION section.

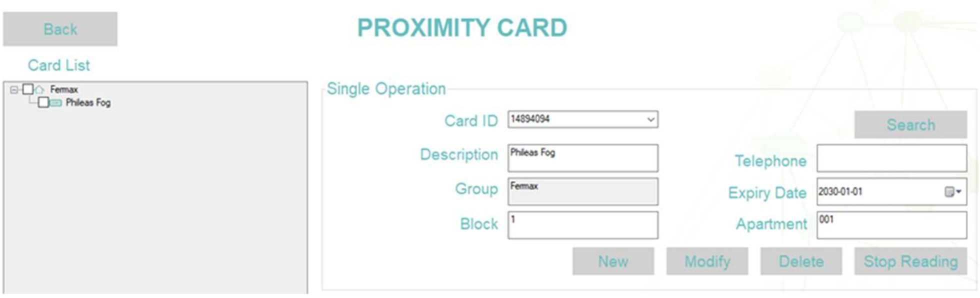


PORT SETTINGS

PC Prox. Reader
Uart: COM7

  - Select the same UART port assigned by the driver.

- **Program the cards**
  - Go to the PROXIMITY CARD section in the MEET Management Software and try to program the first card**:**



PROXIMITY CARD

Card List
Fermax
Phileas Fog

Single Operation
Card ID: 14894094
Description: Phileas Fog
Group: Fermax
Block: 1
Telephone:
Expiry Date: 2030-01-01
Apartment: 001

1 Fill in the details for the new user (name, apartment number, block, etc.)

2 Select the "Start Reading" button.

3 Place the card to be programmed on the upper part of the Card Reader.

5 The card ID number should appear in the Card ID box. (*)

6 Confirm by selecting the "New" button.

(*) NOTE:

If the card ID does not appear in the Card ID box, this will be because the computer baud parameter does not match the one selected in the Card Reader.
Adjust it correctly according to the procedure indicated in the following section.

- **Select the baud parameter.**
  - The MEET Computer Proximity Reader can work with two different baud parameter values: 9600 and 19200 bps. You can change them by pressing and holding the PROGRAMMING BUTTON (for more than 6 seconds).
  - This will change the value from 9600 to 19200 bps, or vice versa, and you will hear three beeps as a confirmation.
  - To find out if the selected value matches the one configured on the computer, try programming a new card. If the reader is configured correctly, its identifier will appear in the Card ID box, otherwise you will need to change the
  - reader baud rate value.