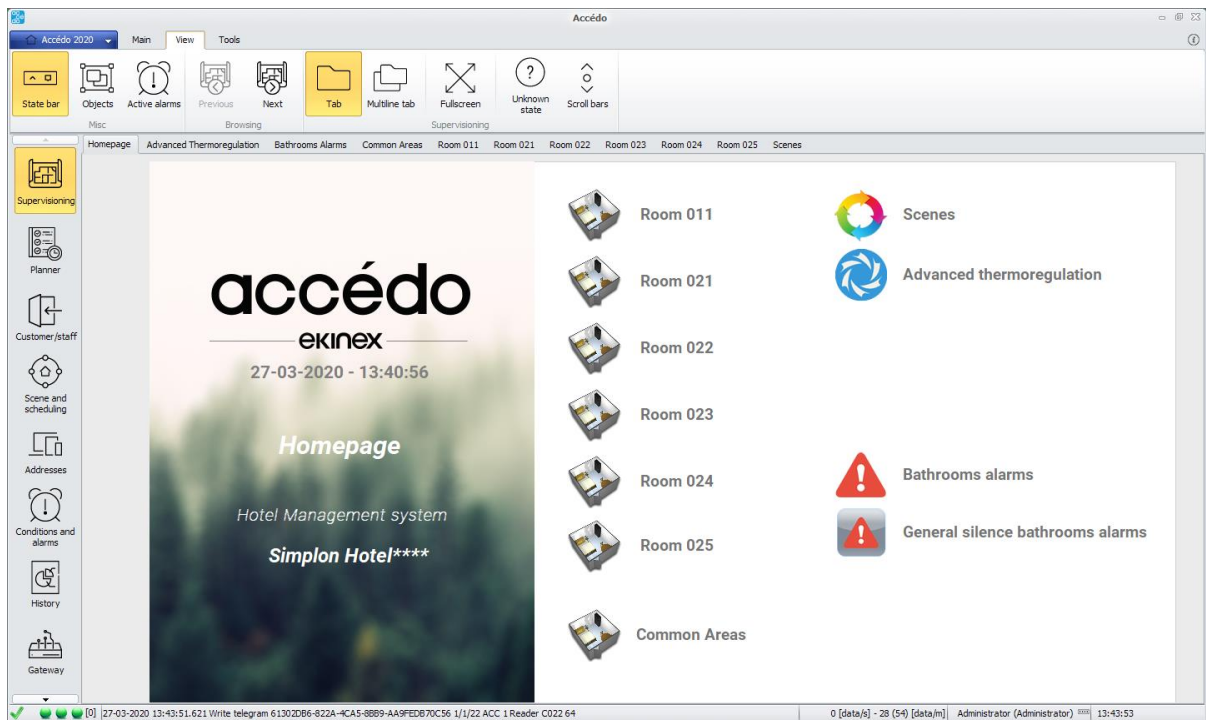


ekinex

CONTROL YOUR LIVING SPACE



Application Manual accédo EK-ACC-SW Access control software suite and supervision of hotels and accommodations

Summary

1	DOCUMENT PURPOSE	8
2	INTRODUCTION.....	9
2.1	Software prerequisites.....	10
2.2	Installation via setup wizard	11
3	TO GET STARTED.....	12
4	INFRASTRUCTURE.....	14
4.1	Automatic system monitoring	15
4.1.1	Unambiguity of the plant.....	15
4.1.2	Stability management.....	15
4.1.3	Reports.....	15
4.1.4	Services status.....	15
4.1.5	Gateways activation status.....	17
4.1.6	Gateway connection to the controlled device	17
4.1.7	Internal system control - gateway status	18
4.1.8	Order of error messages	18
4.1.9	Good footprints to maintain in the time configuration	19
5	START AND LOGIN	20
5.1	Login	20
6	GATEWAYS.....	22
6.1	General informations.....	22
6.2	KNX.....	22
6.2.1	ETS project import.....	23
6.2.2	Areas.....	24
6.2.3	Rooms.....	25
6.2.4	Devices	28
6.2.5	Group addresses.....	29
6.2.6	Bus KNX connection	30
6.3	Modbus	31
6.4	M-Bus.....	34
7	CONFIGURATION.....	37
7.1	General informations.....	37
7.2	Time strips.....	38
7.3	Rooms.....	38
7.3.1	General settings	39
7.3.2	Room status settings.....	40
7.3.3	Rooms groups.....	42
7.3.4	Presence management in the room	42
7.4	Access levels	44
7.5	User groups.....	45
7.5.1	Nodes/addresses visibility permissions.....	46
7.5.2	Nodes/addresses writing permissions.....	47
7.5.3	Supervisions.....	47
7.5.4	Rooms.....	47
7.6	Users.....	47

7.6.1	Nodes/addresses visibility permissions	49
7.6.2	Nodes/addresses writing permissions	49
7.6.3	Supervisions.....	49
7.6.4	Rooms.....	50
7.6.5	Contatti.....	50
7.7	Notifications.....	51
7.7.1	Registry section.....	51
7.7.2	Common configuration to all reporting methods.....	52
7.7.3	Popup configuration	52
7.7.4	Balloon configuration.....	53
7.7.5	Page jumping configuration.....	54
7.7.6	Audio configuration.....	54
7.7.7	E-mail configuration.....	54
7.7.8	SIP configuration	54
7.7.9	SMS configuration	55
7.8	Maintenances	56
7.9	Devices	57
7.9.1	Data.....	57
7.9.2	Configuration.....	58
7.9.3	Guest access actions	58
7.9.4	Other access actions.....	59
7.9.5	Guest access notifications.....	59
7.9.6	Other access notifications	60
7.10	Date, time, plant code	61
7.11	Smart-cards programmers	62
7.12	ekinex access control.....	62
7.12.1	Time strips.....	62
7.12.2	Time strips groups.....	65
7.12.3	Plant codes	66
7.12.4	Devices	67
7.12.5	Reading and writing.....	69
7.13	BLUMOTIX keypads.....	70
7.13.1	General Informations.....	70
7.13.2	Codes.....	70
7.13.3	Tools.....	71
7.13.4	Periodic sending of the “live server” message.....	71
7.13.5	Full keypad memory alarm	71
7.13.6	Filters	72
7.14	Payment profiles.....	72
7.15	Payment entity	72
8	VARIABLES.....	73
8.1	User variables	73
8.2	Gateway variables.....	74
9	LIFT/CABINET MANAGEMENT	75
9.1	Management with PLC and ekinex access control system.....	75
10	SUPERVISION.....	76

10.1	General informations	76
10.2	Supervision of a plant.....	77
10.3	Create supervision pages.....	79
10.4	Possible operations on supervisions	80
10.5	Modify supervision pages.....	80
10.6	Menù supervision objects	90
11	GUEST/STAFF SECTION	92
11.1	Add guest/staff	92
11.2	Importing guest/staff from xls	93
11.2.1	Importer configuration	93
11.2.2	Importing	94
11.2.3	Writing and activation of imported smart-cards	95
11.3	Users.....	96
11.3.1	User state list	96
11.4	Booking	96
11.4.1	Booking insertion.....	96
11.4.2	Booking status list	98
11.5	Smart-cards.....	99
11.5.1	Insert smart-cards	99
11.5.2	Smart-card expiration report.....	100
11.5.3	New card code report creation	101
11.6	Check-in.....	101
11.6.1	AutoCheck-in.....	102
11.7	Check-out.....	102
11.8	Fast Check-in	102
11.9	Access.....	103
12	CENTRALIZED ACCESS MANAGEMENT	105
12.1	Device configuration for centralized management	105
12.2	Configuration of time slots and calendars	106
12.3	Access control section.....	106
12.4	Accesses history	107
13	SEPARATE VIEW FOR USER GROUPS.....	108
13.1	Creator user tracking.....	108
13.2	Sections affected by separate display by competence.....	109
13.2.1	Access control.....	109
13.2.2	Guest/staff history	109
13.2.3	Keys history.....	109
13.2.4	Accesses history, presence history	109
14	SPECIAL CASES	110
14.1	User assigned to multiple groups	110
14.2	User moved from G1 group to G2 group	110
14.3	Delete a user.....	110
15	REPORTS	111
15.1	Access history	111

15.2	Login history	111
15.3	Commands history	112
15.4	Values history	112
15.5	Presence history.....	112
15.6	Keys history.....	112
15.7	Alarms history	113
15.8	Maintenance history	113
15.8.1	Registration	113
15.9	Payments	114
15.9.1	History	114
15.9.2	Generation	114
15.10	Communications.....	114
16	ANOMALIES MANAGEMENT	116
17	CONFIGURATION SETTINGS MENU	117
17.1	General	117
17.2	Server.....	118
17.3	Database.....	119
17.4	Backup Restore.....	120
17.5	Backup scheduling	121
17.6	Log	122
17.7	Alarm notification.....	124
17.8	Supervising.....	125
17.9	International options and languages.....	126
17.10	Access control.....	127
17.11	ekinex access control	129
17.12	Management interface software configuration.....	131
17.13	Misc configuration	132
17.14	SMTP server	133
17.15	Report	134
17.16	Export daily history	135
17.17	Astronomical clock	136
18	BACKUP/RESTORE	138
18.1	Backup	138
18.2	Restore.....	139
19	SCENES AND SCHEDULING	140
19.1	Scenes	140
19.2	Scheduling	141
19.3	Automatic writing between DB	142
20	ADDRESSES	143
20.1	Field details	143
20.1.1	Data.....	143
20.1.2	Readings	144
20.1.3	Log	145
20.2	Address types	145
21	LOGICS AND ALARMS	147

21.1	RPN notation.....	150
21.2	RPN notation in accédo.....	150
21.3	Active alarms.....	152
21.3.1	Alarms types and visibility of active alarms	152
21.3.2	Active alarms grid.....	153
22	UTILITIES.....	154
22.1	Shortcuts	154
23	WEB CLIENT	155
23.1	Web page structure	155
23.2	Login	156
23.3	Supervisions.....	157
23.4	Scenes	158
23.5	Settings	159
23.5.1	Informations	159
23.5.2	Server.....	164
24	WARNINGS.....	168
25	OTHER INFORMATION	168

Revision	Changes	Date
1.3.0	Added chapter <i>Client Web</i> , added note in the installation section on the full control privileges of the installation folder	22/05/2020
1.2.0	Added chapter <i>To get started</i> , with guidelines for implementing a new project	14/04/2020
1.1.0	Upgrade to software version accédo v1.0	28/03/2020

1 DOCUMENT PURPOSE

This manual describes the application details for version A1.0 of the ekinex® EK-ACCSW software suite. The document is intended for the system configurator as a description and reference guide for software functionality and application programming.

This application manual is available for download at www.ekinex.com.

Document	File name (## = versione)	Version	Last update
accédo software suite application manual	MAEKACCSW_##_EN.pdf	V1.0	03/2020

To get direct access to the latest available version of all documentation, use the following QR code:

EK-ACC-SW



2 INTRODUCTION

accédo is the ekinex® software suite for the automation of KNX hotels, accommodation and hospitality facilities. The software can be used in combination with ekinex devices for access control: the EK-TR2-TP smart-card reader for controlled access to rooms, the EK-TP2-TP card programmer and the EK-TH2-TP card holder for room presence detection. These products, together with push-button controls and ekinex® room thermostats, guarantee aesthetic uniformity to all wall mounted devices for the automation of hotel rooms and common areas. The series of devices is completed by the EK-HO1-TP panel-mounted controller, which provides the input, lighting and output control functions and the control of a 2/4 tube fan-coil in a single product.

The main functions performed by the software suite are:

- Programming of smart-cards using RFID technology. The communication between the accédo software and the programmer(s) in the reception, the readers outside the room or outside the entrances to the common areas and the card holder inside the room, takes place on KNX network infrastructure type TP twisted pair.
- Room reservation planning operations and check-in/check-out activities for guests and service staff.
- Execution of scenarios and scheduling to execute a sequence of operations through a single command. The same operations can be scheduled to be executed on predefined days and times. Possibility of using a software astronomical clock configured according to latitude and longitude of the site.
- Plant supervision through configurable graphic pages.
- Management of technological alarms.
- Realization of reports of all the accesses to the structure.

The system architecture of the accédo suite is of the multi-client server type: the server, with a PC-Windows-desktop interface, makes the connection with an SQL Server database and the local or remote connection of the hotel structure; multiple client workstations are possible, both with PC-desktop interface and Web interface. accédo can be used both for the management of hotel structures concentrated in a single building and for widespread structures (hotels or distributed Bed&Breakfast).

The accédo server has 3 gateways, built as Windows services, to communicate with the following communication protocols:

- 1 KNX gateway (with USB or KNX/NetIP interface)
- 1 Modbus master gateway (serial type with USB RTU/ASCII and TCP/IP interface)
- 1 M-Bus gateway (serial type with USB interface, for the acquisition of thermal and electrical consumption data)

The desktop interface of the accédo suite looks like a single document Windows application. There is a vertical toolbar in the left section of the program form; by selecting an entry in the vertical section, you can access the horizontal toolbar at the top. This allows you to access the central workspace of the tab. The sections of the vertical toolbar are:

- Supervisionig
- Planner
- Customer/staff
- Scene and scheduling
- Addresses
- Conditions and alarms
- History
- Gateway
- Configuration

The accédo suite has 7 access profiles based on credentials charged at startup, allowing a common interface and access to specific functions for each hotel operator:

- Administrator
- Manager
- Supervisor plus
- Supervisor
- Maintenance
- User plus
- User

The configuration of KNX devices for access control in rooms and common areas, the realization of scenarios and supervision pages are facilitated by the use of group addresses programmed in the devices and information from the Building view, extracted through direct import of the ETS project (version 3 and later) in .knxproj format.

2.1 Software prerequisites

- Operating System: Microsoft® Windows 7 or later. Windows 10® is recommended. In server environment you can use Windows® Server 2016 (in its various editions: Essential, Standard, Professional, Enterprise) or later.
- RAM: at least 8 GB for server installation
- SSD Hard disk: at least 40 GB free for server installation

accédo uses some third-party components which, if they are not present on your computer, will be installed during the program installation procedure.

- Microsoft .NET Framework 1.1
- Microsoft .NET Framework 2.2 SP2
- Microsoft .NET Framework 4.0
- Microsoft SQL CLR Types 2008 R2 e 2014 x86
- Microsoft SQL Management Objects 2008 R2 e 2014 x86
- Microsoft SQL Native Client 10.5 x86 e x64
- Microsoft Visual C++ 2010 SP1 x86
- Windows Imaging Component x86 e x64

2.2 Installation via setup wizard

The setup is started by double clicking on the setup.exe file. You must have administrator privileges on the machine to complete the setup procedure correctly.

Be careful that the ISetupPrerequisites folder (which contains the installation prerequisites) and the SQL folder (which contains the SQL Server setup files) are present.

The installation consists of several steps, in some of which you are asked to make a choice related to the setup itself or to options related to the operation it will have access to. Once you have made your choice, press Ok or Next. At any time the installation can be aborted by pressing Cancel.

- Select language
- Missing prerequisites list display. Proceeding with the installation of prerequisites may prompt you to restart the machine. After restarting, the setup will resume automatically.
- Continue the installation by clicking on next
- License Agreement
- By default, the creation of a new SQL Server instance is proposed. It is proposed a name (SQLEKINEXACCEDO) and the password of the user knows, which you can view and modify. Alternatively you can select an existing SQL Server instance, knowing the user's password sa.
- Confirm settings and start installation
- Installation progress
- End of installation. At the end of the installation, the last reboot of the system is required.

For the correct operation of the software, you must verify that the folder where the software has been installed has full control privileges.

Select the installation folder (example C:\Program Files\Ekinex), select the Access folder, press the right button and press Properties. A popup window will appear:



- Select the Security tab
- Press the Edit button
- Press the Add button
- Enter Everyone
- Allow complete control and save

3 TO GET STARTED

To configure the accédo software suite, it is recommended to start from a complete ETS project (version 4 or later) with the ekinex access control products: the EK-TR2-TP transponder card reader, the EK-TP2-TP card programmer and the EK-TH2-TP card holder. The Test-project containing the application programs for these products can be downloaded from www.ekinex.com in the product section (APEKTRTPH2TP.knxproj).

Configuration of a new project with accédo:

- ⇒ Open the accédo software suite and log in using the credentials with Administrator login profile (e.g. Login: Administrator, Password: Administrator).
- ⇒ Make sure you have cleaned the database from information related to previous configurations: press the *Accédo 2020* button at the top left of the menu bar and then *Settings*, open the *Database* section and press the *start cleaning* button.
- ⇒ To import a new ETS project: go to the *Gateway* section, *KNX* horizontal toolbar, *Tools* and *Import* menu: select the ETS project to import. If the ETS project has been realized by completing the *Building* view, the information concerning the accommodation will be directly imported. In particular, the structure of the rooms will already be configured, each one with a description and with a reader device and a card holder device.
- ⇒ After importing the ETS project: go to the *Gateway* section, *KNX* horizontal toolbar. The imported ekinex devices can be found in the *Devices* area in the tree under *Ekinex*.
- ⇒ How to create an Area: in the *Areas* area, select the *Tools* and *New Area* menu; in the view on the right of the page you can rename the area for example by entering the name Hotel Simplon
- ⇒ How to create rooms: select the area created, select the *Tools* menu and *New environment*; in the view on the right you can rename the room and above all you need to define the destination of use as Room in the *Environment type* field.
- ⇒ Drag&drop the device, reader or holder, from the *Devices* area to the *Environments* area; each room must have its own reader and holder.

Device configuration and choice of reader(s) with card programmer function

- ⇒ go to the *Configuration* and horizontal bar section of the *Ekinex* toolbar: you will find the list of all imported Ekinex access control devices
- ⇒ Select the *Tools* and *Firmware Read* menu after selecting each record in the table: *MAC Release 1* must appear in the *Firmware* area.
- ⇒ Set the readers with programmer function by placing the check in the programmer records with *Prog* field.
- ⇒ Disable the *Enable handshake* field in all records; remove the check in all records to the *Enable time* field to simplify configuration and verification.
- ⇒ Select the *Plant Codes* tab and enter at least 2 codes one for guest cards and one for master tags.
- ⇒ In all records, in the *Plant codes* field, select all codes that have been created.
- ⇒ One by one or by selecting all records (Ctrl+Shift) press the *Write* button in the horizontal toolbar: if the writing operations are successful in the *State* area at the bottom the green tick will be visible on all parameters.
- ⇒ Configure date and time in this way: go to the *Configuration* section, horizontal toolbar *Date and Time Cod. Plant* and set among the imported objects the date and time common to the whole ETS project; it is possible to update the system date and time in a cyclic way.
- ⇒ In the *Configuration* section and *Ekinex* horizontal toolbar, select the *Write* button in the menu to update the date and time on the devices if the cyclic update has not yet had effect
- ⇒ Back up the configuration by following these instructions: press *Accédo 2020* button at the top left of the menu bar and then *Settings*, open the *Backup Restore* section and press the *Backup* button. The standard

Windows window will open, choose a file name and a location in the PC's folders. The same file, with the *Restore* button, will restore the entire configuration.

4 INFRASTRUCTURE

The accédo suite consists of several components:

- The application (desktop or web) accédo, which acts as an interface between the user and the underlying system;
- The MasterGateway, which is responsible for keeping all the components connected to each other and for passing on the information;
- BIGOmnia, the brain of the system, is in charge of managing all the automations configured on the interface side;
- The gateways, which take care of communication between the system and the external one (for example the KNX gateway takes care of communication on the KNX bus); the possible gateways are listed and described in the appropriate section.

Finally, the last constituent component is SQLServer, the SQL service that allows access to the database. All the components (excluding the application) are Windows services and are present only on the server machine.

For the correct functioning of accédo it is necessary that all components are started and work correctly.

Monitoring by the user

The correct functioning of the hardware components can be monitored using the coloured dots on the left side of the application status bar; for each component (except SQLServer) there is a dot whose colour represents the status:



The service is stopped.



The service is started but fails to the external device; it is visible in the dots represented gateway and is usually a temporary situation typical of the start-up phase: the service starts and the dot turns yellow, when it connects to the external device (e.g. KNX bus) it turns green. If the dot remains yellow, it is necessary to check the configuration of the gateway and the correct functioning of the device to which the gateway is connected.



The service is working properly.

4.1 Automatic system monitoring

4.1.1 Unambiguity of the plant

Each installation is now identified by a plant name to be defined in the System Monitoring ⇒ Settings ⇒ Plant Name which is used within the error report (or error return) emails to identify the plant from which the error is derived.

The identifier is at the discretion of the installer, to be entered at the first start of the installation (it is requested with a popup at each start if not set).

4.1.2 Stability management

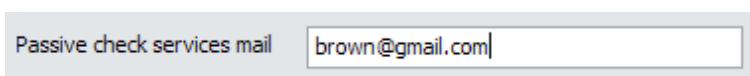
Given the indispensability of all the components for the correct functioning of the system, internal verification mechanisms (and possible reports) have been implemented:

1. The status of the services;
2. The status of the gateways;
3. The connection to devices by gateways;

4.1.3 Reports

Any error messages are sent by email to the address specified in the MailPassiveCheckService registry key under the BIG/accédo node.

The address can be configured in the accédo settings (in the case of multiple addresses these can be divided by ';').



Passive check services mail

4.1.4 Services status

All Windows services associated with the components are configured in Automatic or Automatic (delayed) startup mode so that they are started when the machine is started.

In addition, the Master Gateway and BIGOmnia periodically check the status of the Windows services associated with the components:

- If the services are correctly started, no action is taken;
- If a service with Start or Stop status is found, the service status is rechecked 5 times (10 seconds apart);
 - if during a subsequent check the service is found to have started, no action is taken;
 - If the service is interrupted during a subsequent check, the service is restarted;
 - if at the end the status is still in Start in progress or Stop in progress, the service interruption and restart is forced;
- If a service with Stopped status is found, the service is restarted.

The list of services to be monitored consists of all services not disabled that meet at least one of the following requirements:

- The name is **SRVMASTERGATEWAY**
- The name start with **SRVKONNEXFALCON**
- The name start with **SRVBIG**

In addition to these services, there are also those in the *BIGServicesToCheck* registry key under the *BIG/accédo* node.

The check is performed one minute after the start and then periodically according to the accédo settings (*CheckServicesInterval* and *CheckServicesMaxAttempt* registry keys):

Interval between two consecutive control of the services status	(MasterGateway) <input type="text" value="300"/> seconds	(BIGOmnia) <input type="text" value="900"/> seconds
Maximum number of services status check before send notification	(MasterGateway) <input type="text" value="2"/>	(BIGOmnia) <input type="text" value="2"/>

If after *CheckServicesMaxAttempt* attempts a service is not started, a report is sent by email.

If after sending the error message, the service is restarted correctly in a subsequent attempt, an error return email is sent.

Example of Master Gateway log in case of working services:

```
>> INFO: CheckAndRestartStoppedServices started...
>> INFO: CheckAndRestartStoppedServices info ->
*** Service srvBIGOmnia correctly running!
*** Service srvKonnexFalcon.NETGateway correctly running!
*** Service MSSQL$SQLBIGSTUDIO correctly running!
```

Example of Master Gateway log in case of stopped services:

```
>> INFO: CheckAndRestartStoppedServices info ->
*** Service srvBIGInnoEdgeGateway NOT RUNNING but Stopped
*** Service srvBIGInnoEdgeGateway status = Running
***Service srvBIGInnoEdgeGateway RESTARTED!
*** Service srvBIGOmnia NOT RUNNING but Stopped
*** Service srvBIGOmnia status = Running
***Service srvBIGOmnia RESTARTED!
*** Service srvKonnexFalcon.NETGateway NOT RUNNING but Stopped
*** Service srvKonnexFalcon.NETGateway status = Running
***Service srvKonnexFalcon.NETGateway RESTARTED!
*** Service MSSQL$SQLAKINEXACEDO correctly running!
```

4.1.5 Gateways activation status

In addition to the previous check, only the Master Gateway performs a check of the gateway activation status: the Master periodically sends a handshake message to each connected gateway and detects the response.

If after N handshake attempts a gateway does not respond, it is stopped (the automatic restart of services will restart it).

If a gateway does not respond after M handshake attempts (including restart), an alert is sent and the handshake count for that gateway is restarted.

If the service returns to answering the handshake after sending the error message, an error return message is sent.

N is defined by the registry key `CheckHandShakeMaxAttemptBeforeStop`.

M is defined by the registry key `CheckHandShakeMaxAttemptBeforeSendMessage`.

Interval between two consecutive handshakes	<input type="text" value="300"/>	seconds
Maximum number of missing handshake before restart services	<input type="text" value="5"/>	
Maximum number of missing handshake before send notification	<input type="text" value="7"/>	

Example of Master Gateway log in case of working services:

CheckAliveBIGServices started...

CheckAliveBIGServices send hello to 956B0F41-9CD1-4E44-8E1C-080B21990F6D

CheckAliveBIGServices send hello to A08D9D13-D387-42C8-AD88-93D525F2AA3B

CheckAliveBIGServices received hello from 956B0F41-9CD1-4E44-8E1C-080B21990F6D

CheckAliveBIGServices received hello from A08D9D13-D387-42C8-AD88-93D525F2AA3B

Example of Master Gateway log in case of service that does not respond to handshake (not even after restart):

CheckAliveBIGServices started...

CheckAliveBIGServices send hello to 956B0F41-9CD1-4E44-8E1C-080B21990F6D

CheckAliveBIGServices send hello to A08D9D13-D387-42C8-AD88-93D525F2AA3B

CheckAliveBIGServices received hello from 956B0F41-9CD1-4E44-8E1C-080B21990F6D [...]

CheckAliveBIGServices stopped service srvKonnexFalcon.NETGateway after 10 minutes of hello silence [...]

CheckAliveBIGServices send email for gateway Konnex Falcon .NET Gateway after 15 minutes of hello silence

4.1.6 Gateway connection to the controlled device

The master also receives reports about the connection of the gateway to the controlled device.

If the gateway remains disconnected from the device for more than N seconds, an alert is sent (this time also includes any restarts of the services provided by the services themselves or by other mechanisms).

If the service reconnects correctly after sending the error message, an error return message is sent.

The maximum waiting time before a reconnection is configurable in accédo (setting *CheckconnectionsMaxWait*).

Maximum wait in case of disconnection before send notify seconds

Example of Master Gateway log:

At startup:

Gateway :Konnex Falcon .NET Gateway (A08D9D13-D387-42C8-AD88-93D525F2AA3B) disconnected from the controlled device! Start disconnection timer...

- Alla connessione al dispositivo di un gateway

Gateway :Konnex Falcon .NET Gateway (A08D9D13-D387-42C8-AD88-93D525F2AA3B) has been disconnected from the device for more than 200 seconds! Sending mail!

4.1.7 Internal system control - gateway status

Each gateway monitors the connection status of the external device to which it is to connect:

- Falcon.NET Gateway: attempts the connection 15 times (10 seconds apart) and if at the end of the attempts the service restarts.
- ModBusGateway: is always connected.
- MBus: is always as connected.

4.1.8 Order of error messages

Errors have equal priority to the previous list, therefore:

1. The start of all services is checked
 - In the event that a service has not started in the expected time the report is sent
2. For all gateways handshake is attempted periodically
 - In the event that a service does not respond in the expected time, the report will be sent only if the service is active.
3. For all gateways the connection to the device is checked
 - In case a service does not connect to the device in the expected time, the report is sent only if the service is active and responds to the handshake

The single error report is instead sent periodically (e.g. if the service does not start and there is a check every 5 minutes and the email after 2 failed attempts will be sent a report every 10 minutes; the same goes for the other types of error).

4.1.9 Good footprints to maintain in the time configuration

Time check status of services < Handshake intervals * attempts before handshake reporting

Service status check time < Maximum waiting time in case of disconnection

- Otherwise if the services die a moment after the services check there is a risk that the other alerts will start when in reality the main problem is the service stopped and could be solved by the services status check without disturbing the user.

Handshake check time * number of handshakes missing before restart < Service status check time.

So the possible stop for handshake failure takes advantage of the restart of the service status control and avoids making two consecutive stops if the restart status control is not passed in the meantime.

Handshake check time * number of handshakes missing before restart < Maximum wait in case of disconnection.

This way we make sure that the handshake control is valid before sending the missed connection report (if there is no handshake there must be no missed connection report but a missed handshake report).

A good configuration can be the following:

Interval between two consecutive control of the services status	(MasterGateway) 300 seconds	(BIGOmnia) 900 seconds
Maximum number of services status check before send notification	(MasterGateway) 2	(BIGOmnia) 2
Interval between two consecutive handshakes	300 seconds	
Maximum number of missing handshake before restart services	5	
Maximum number of missing handshake before send notification	7	
Maximum wait in case of disconnection before send notify	60 seconds	

The Master:

- Every 5 minutes it checks the status of the services.
- If after 3 minutes he does not receive handshake he stops the service.
- If after 7 minutes it does not receive handshake it sends the report.
- If after 6 minutes you are not connected to the device, it sends the alert.

BIGOmnia checks the service status every 10 minutes.

5 START AND LOGIN

To start the program, double-click on the icon on your desktop.

At startup the program can be configured to automatically log in with the latest valid credentials or to always request authentication.

5.1 Login

After having executed the user authentication (default user: Administrator; Password: Administrator) through the appropriate window, the program re-proposes the page present at the time of the last closing. At the bottom left there is the menu that allows you to view the main areas of the program.

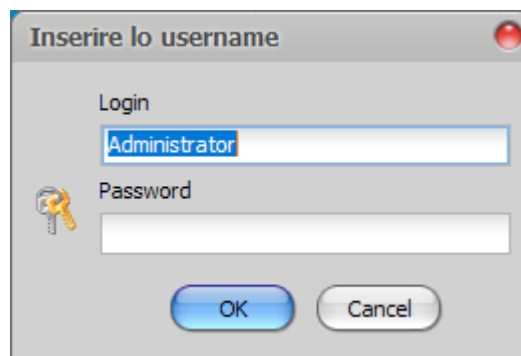


Figure 1 - Login at program startup

As soon as you start and finish the initial upload, accédo presents the last section of the software used in the previous login. On the left are displayed the sections of which the software is composed.

- Supervising
- Planner
- Customer/staff
- Scene and scheduling
- Addresses
- Conditions and Alarms
- History
- Gateway
- Configuration

At the top, in addition to the Main tab which is always available, there may be several tabs whose configuration depends on the section active at that time.

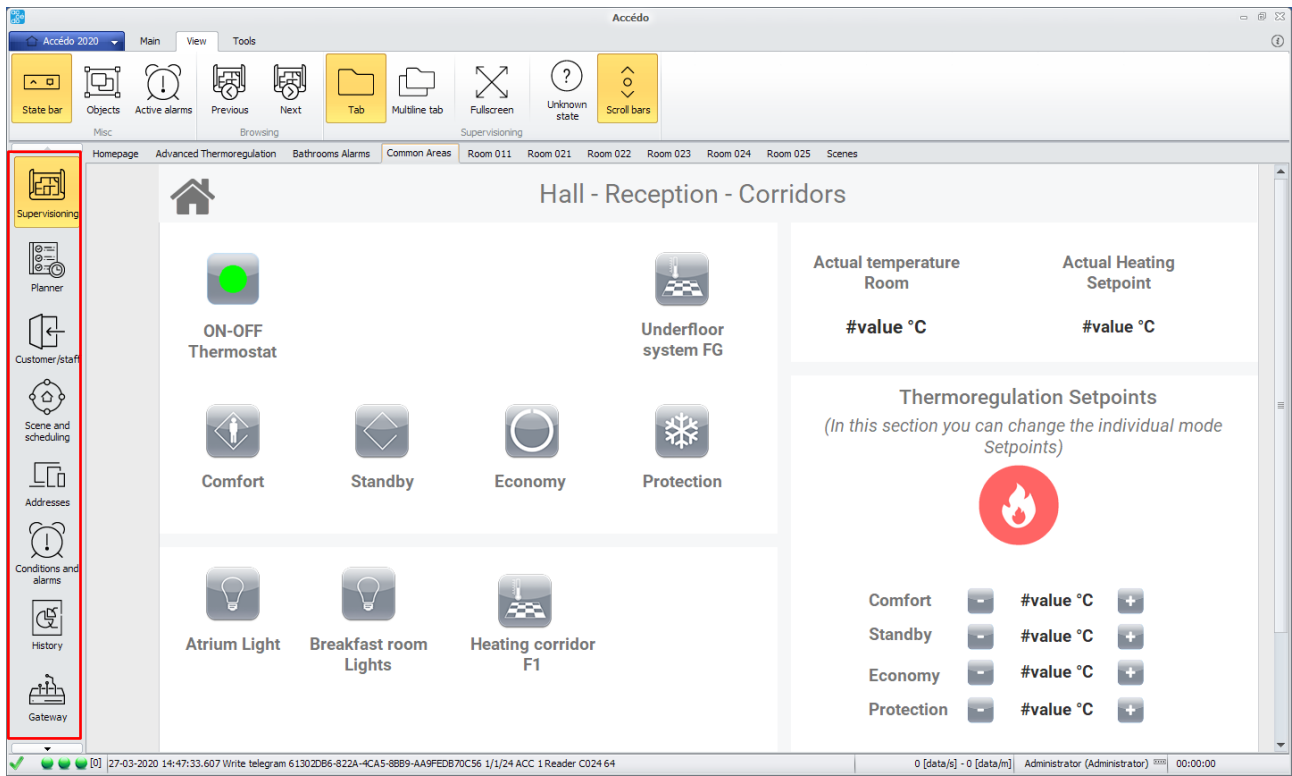


Figure 2 - Graphical appearance of the accédo software suite

6 GATEWAYS

6.1 General informations

The accédo configuration is divided into n sections.

The first sections are dedicated to the configuration of so-called gateways. A gateway is an accédo software extension (consisting of a Windows service) that manages a particular hardware or bus device. The gateways available in accédo are:

- bus KNX
- Modbus
- M-Bus

The other configuration sections are specific to particular features of the software:

- Level protections
- Users and User groups
- Calendars
- Notifications
- Data processor
- Report
- Charts
- Access control configuration

6.2 KNX

In the KNX section you can configure the gateway with the KNX bus.

For each gateway there is a common configuration section, which is located, once the gateway has been selected, at the top of the right column of the access window.

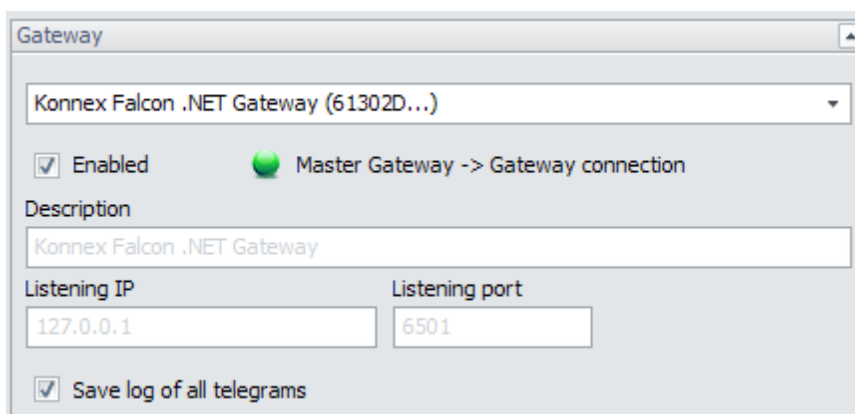


Figure 3 - General Gateway Settings

Since the software can manage multiple gateways for each type of gateway, there is a combobox from which you can select the gateway you want to configure. It displays the name and, in brackets, the first part of its GUID, i.e. the unique alphanumeric identifier that identifies it.

You can activate or deactivate the gateway. The TCP connection status between the Master Gateway and the gateway is also shown.

The other information, which cannot be changed, is the name, IP and listening port of the gateway.

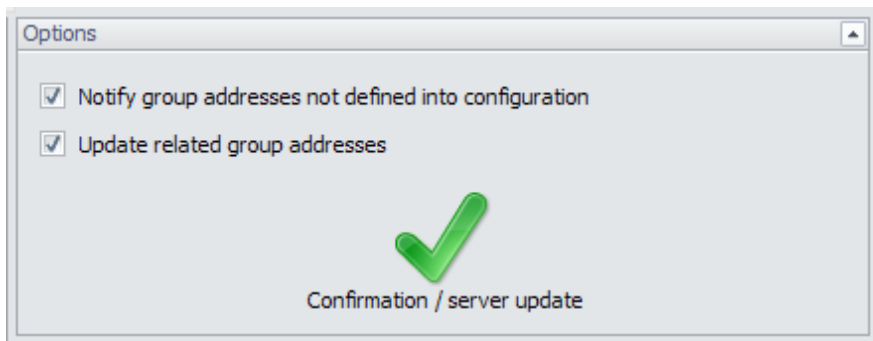


Figure 4 – gateway options

There is therefore a section that is always present, but different from gateway to gateway, in which to configure some specific features of the gateway in question.

In the case of a KNX gateway these characteristics are:

- Notification of group addresses not defined by the configuration: if enabled, this means that even group addresses not present in the imported ETS project will be detected and transmitted to the software for possible monitoring in the lower status bar.
- Update related group addresses: If enabled, the correlations between addresses determined by the ETS project configuration are taken into account, so that if the value of an address is changed following a bus telegram, the same value is also applied to all related addresses at software level.

6.2.1 ETS project import

The configuration of the KNX section essentially consists in importing an ETS project, which can be done with ETS3, 4 or 5. In the case of export from ETS4 or 5 it is very simple: just export the knxproj file.

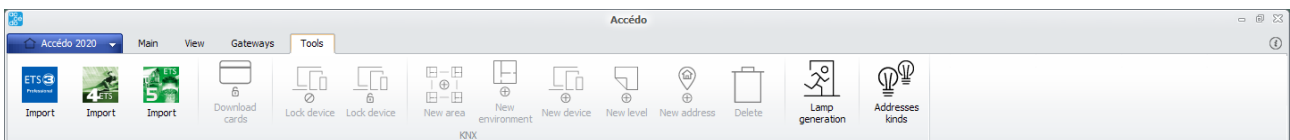


Figure 5 – KNX configuration toolbar

By pressing the Import keys (from ETS4 or 5) you are asked to select a knxproj file.

Once the file import procedure is finished, the 3 sections representing the KNX configuration are populated:

- Areas
- Rooms
- Group Addresses

The fourth area (Devices) represents the database of devices recognized by accédo. These are in particular KNX access control devices. Recognizing these devices determines the specific group addresses to be used for access control system management (adding and removing access permissions, logging access history, time zone configuration, etc.).

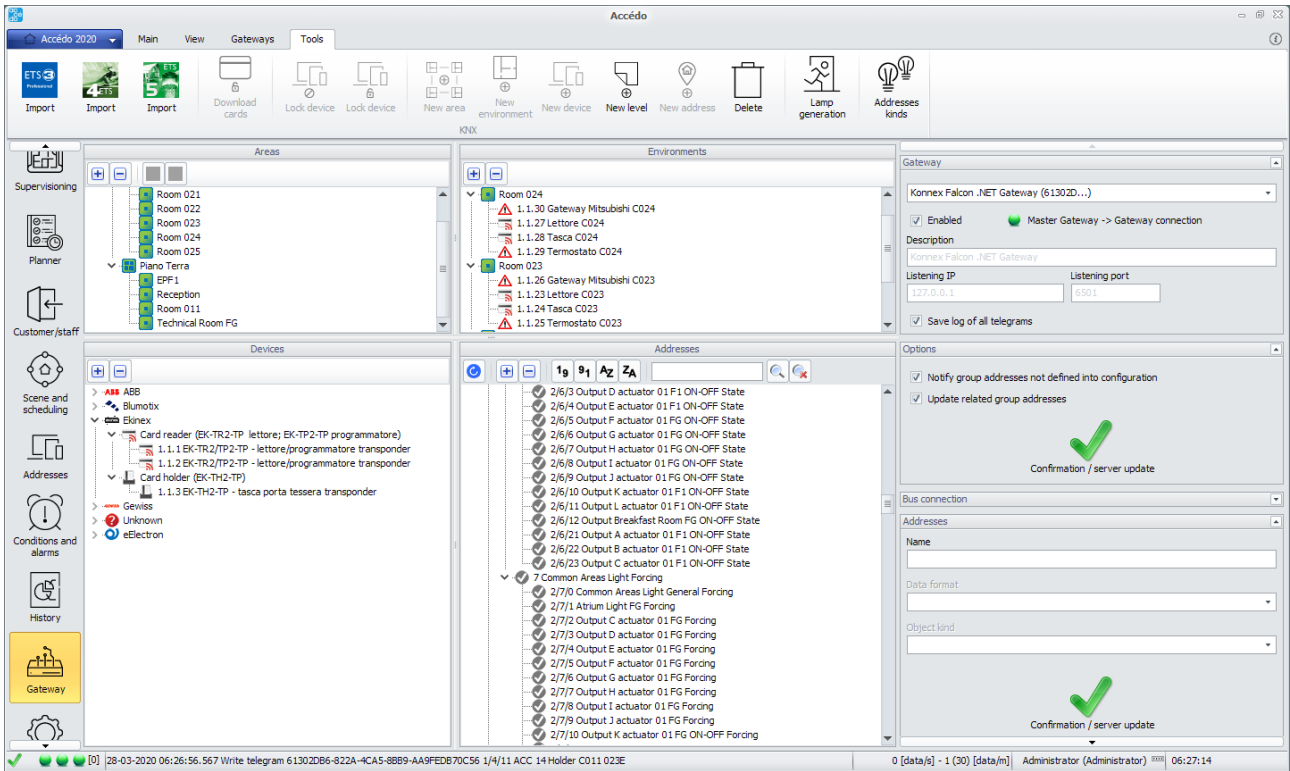


Figure 6 – KNX configuration form

6.2.2 Areas

The Areas window (top left) contains the information that can be found in the Building view in ETS. The root element is the building, which is divided into floors, rooms, etc.

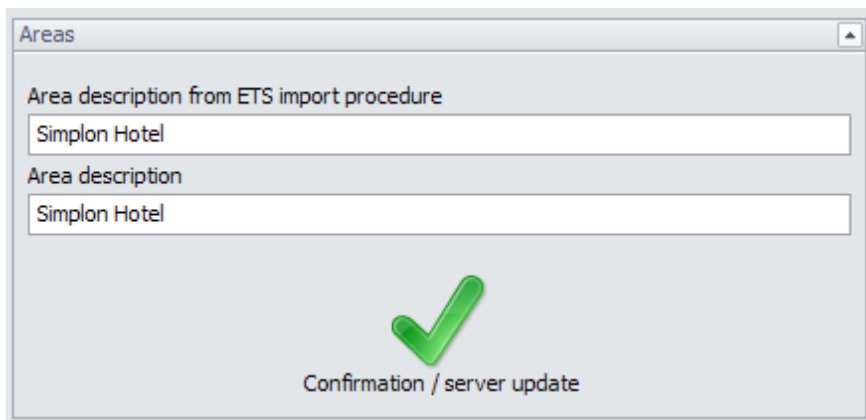


Figure 7 - Areas properties

The properties of an area are:

- Description from ETS import, not modifiable
- Area description, user customizable

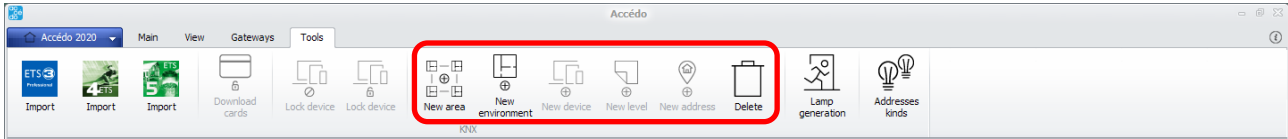


Figure 8 – Areas configuration toolbar

Working in the areas section you can decide to delete a selected area or room, but also to create a new area or room. Although technically possible, this is never recommended. The best thing is always to modify the ETS project so that it always reflects the actual configuration of the installation and then re-import the ETS project into accédo.

It is possible to reimport the ETS design endlessly. Keep in mind that a reimport never deletes any data, but only adds missing elements (be they areas, environments, devices or group addresses).

In the case of areas and rooms the only univocal information that allows to correlate what has already been imported and what is present in the new ETS project is the name. Therefore, the change to room names in the ETS project and the subsequent import involves the creation of a new environment in the accédo configuration. This new environment will obviously be related to the devices as defined in the ETS project. It follows that the old environment will be device free; there is a risk that cards with access permissions have already been created for the now "empty" environment. These cards will continue to function, as the card codes are stored on the devices themselves. However, if you remove the access permissions to the old environment, nothing happens (i.e. the cards continue to have access) because the software searches for devices for that environment to remove the card codes from, but finds nothing, because these devices are now associated with an environment with a new name.

The advice is therefore to pay particular attention to the names of the environments, in particular avoid modifying these names in ETS (and then reimporting the project in accédo) after creating cards for access to the rooms!

If you change a room name with accédo, it is saved and displayed as a "custom" description for that room. The software keeps in memory the original name derived from the ETS import in order to find the correct correspondence between ETS and accédo environments in case of reimport.

6.2.3 Rooms

The Rooms window (top right) contains the list of all rooms defined with ETS through the Building view, be they rooms, common areas or technical rooms.

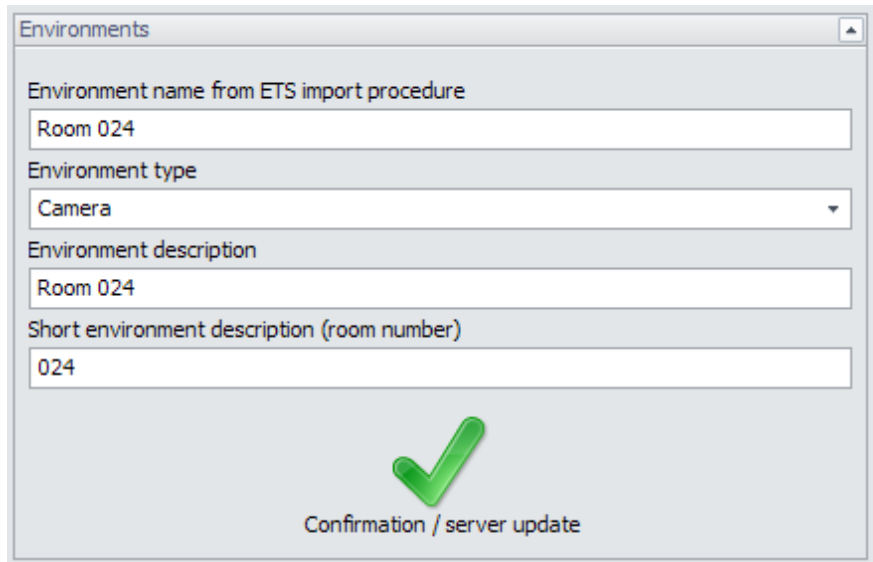


Figure 9 – Room properties

The properties of a room are:

- ETS import environment name, not modifiable
- Type of room, customizable in:
 - Common area
 - Room
 - Invisible
 - Technical area
 - Custom
- Room description, customizable by the user
- Short room description (room number)

The properties of a room are available in the same way both by selecting the environment in the area view and selecting it in the room view.

For each room, the devices contained in it are listed, whether they are devices recognized by the internal accédo database or devices not present in this database.

Recognized devices have their own specific icon:



which represents the type of device (card readers, card holder, thermostats, numeric keypads, etc.).

Devices that are not present in the database, but are still recognized and for which all associated group addresses are loaded, have this icon:



Figure 10 - Icon used for KNX devices not present in the accédo database

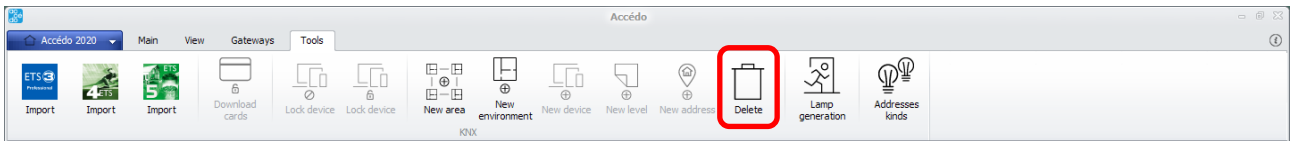


Figure 11 – Delete room or device

After selecting a device or environment, you can delete it.

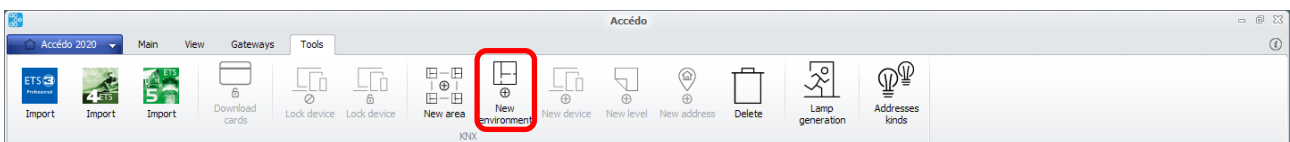
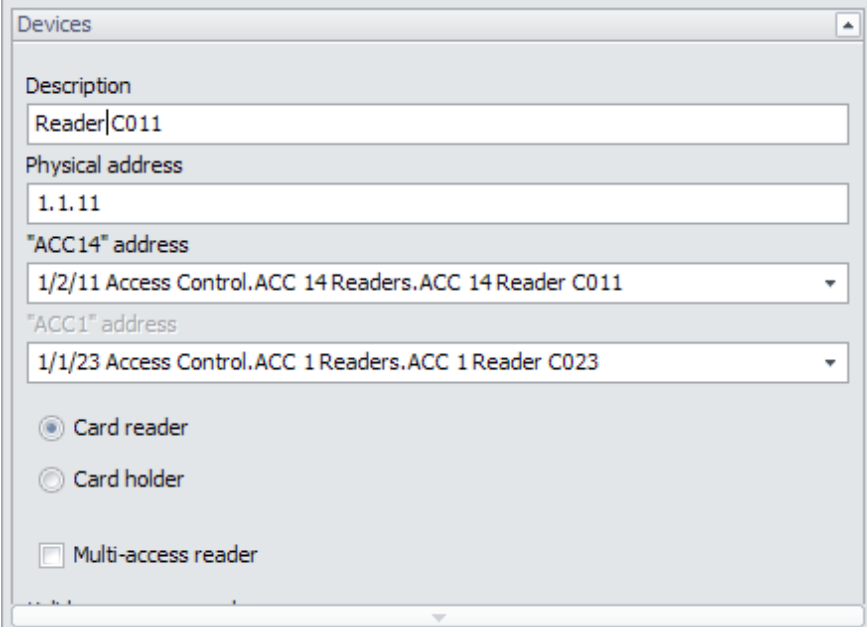


Figure 12 – New room toolbar button

Without any selection you can create a new room. The new room can be inserted into an area by dragging it to the appropriate area in the area view.

6.2.4 Devices

It represents the database of recognized devices. The first level of the tree is the manufacturers of the devices. For each manufacturer the products included in the database are listed. After the import, for each product code, the devices with that code entered in the ETS project are listed.



The screenshot shows a window titled "Devices" with the following fields and options:

- Description: Reader|C011
- Physical address: 1.1.11
- "ACC14" address: 1/2/11 Access Control.ACC 14 Readers.ACC 14 Reader C011
- "ACC1" address: 1/1/23 Access Control.ACC 1 Readers.ACC 1 Reader C023
- Radio buttons: Card reader, Card holder
- Checkbox: Multi-access reader

Figure 13 – Device properties

For the devices are displayed the master characteristics properties (description and physical address) and group addresses that allow the correct functioning of the communication with the device for access control management.

In the figure there is a particular reference to an ekinex access control system reader. In this particular case, since the ETS databank is identical for reader and programmer (it is the device itself that, according to the loaded firmware, performs one or the other function) the software is not able to distinguish which device it is. This is the only case in which the correct reader or programmer assignment must be confirmed or modified by the user.

6.2.5 Group addresses

Represents the Group Addresses view in ETS.

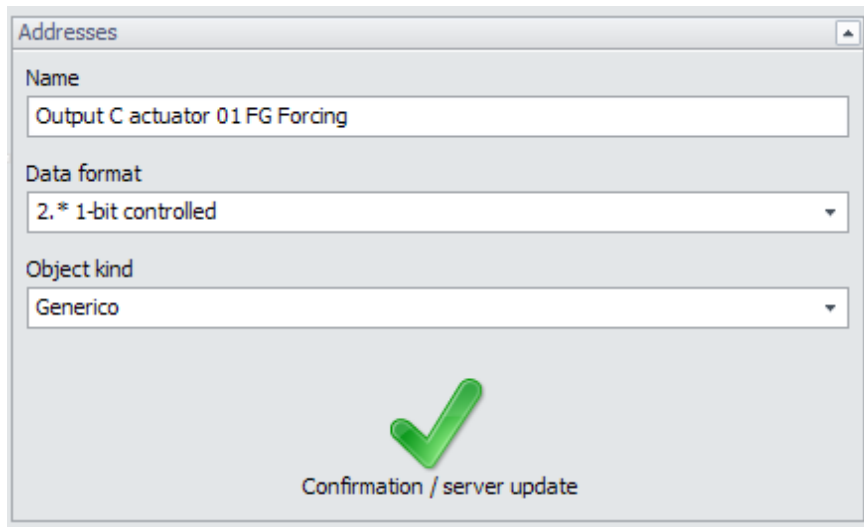


Figure 14 – Address properties

The properties of a KNX group address are:

- Name
- Data format
- Object type

The data format is correctly recognized if that address is associated with a device registered in the accédo database. If the address is associated with a device not in the database, the data size is correctly recognized. In the example in Figure 24 it is a 3 byte piece of data. It is possible for the user to modify this definition, for example by selecting another 3-byte data type, such as the "11.001 3-byte date". The modification of the format is left absolutely free, but it is obviously recommended not to make any changes without the necessary expertise.

The object type represents "high level" information useful to the supervisor, but not used for KNX data processing. For example, a 1-bit group address (addresses that make up the majority of addresses in a system) will always be physically valued with a bit of value "1" or "0". On a logical level we can attribute many different meanings to the values "1" and "0" as for example:

- On = 1, Off = 0
- Open = 1, Closed = 0
- Up = 1, Down = 0
- winter = 1, summer = 0
- On = 1, off = 0
- forward = 1, back = 0

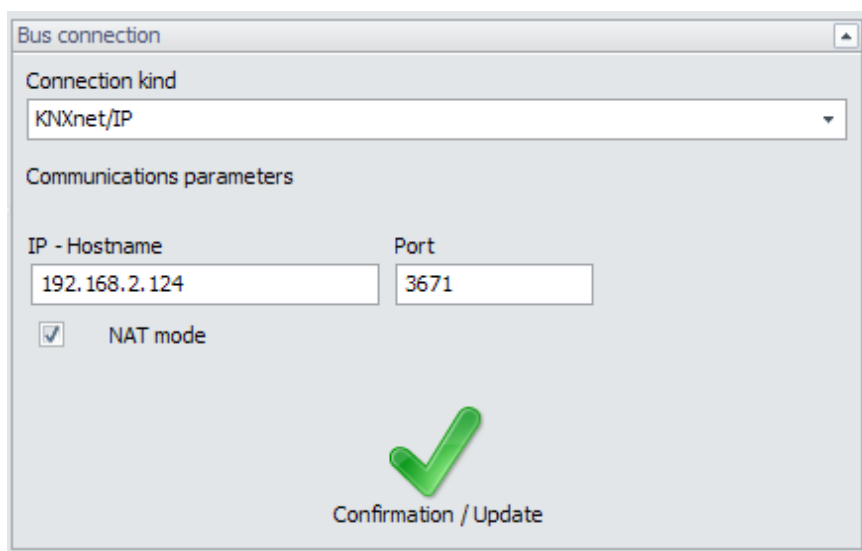
The object types are defined within the accédo database.

The correct assignment of this meaning to an address does not lead to any changes or malfunctions at the KNX system level, but facilitates the reading of the system status and its command through the supervisor.

6.2.6 Bus KNX connection

For each gateway, the mode of connection to the controlled bus or device must usually be defined. The connection possibilities are those that can also be used via ETS, made available through Falcon drivers.

- USB
- IP
- Serial



Bus connection

Connection kind
KNXnet/IP

Communications parameters

IP - Hostname: 192.168.2.124 Port: 3671

NAT mode

Confirmation / Update

Figure 15 – Bus connection

6.3 Modbus

The Modbus gateway allows the read/write of Modbus data by connecting to serial or IP devices. Starting from the connection type, a new serial interface can be defined, on which one or more Modbus slaves identified by a UnitID will be connected.



Figure 16 – Modbus configuration toolbar

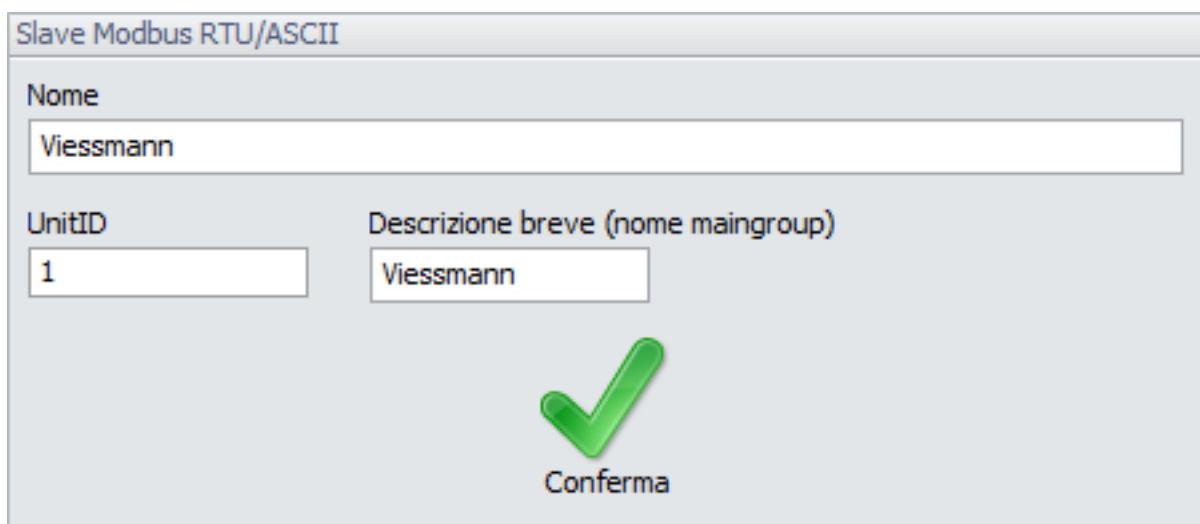


Figure 17 – Modbus RTU slave properties

Or you can define an Ethernet Modbus slave.

Figure 18 – Modbus Ethernet slave properties

Once the Modbus devices have been defined, whether serial or IP, the Modbus memory map where to read / write values must be defined. Since in some cases the data are many, you can organize them in folders.

By defining a Modbus memory address you are indicating a memory area in which you can read and/or write. This memory area will have an initial address and will consist of n word (16 bit), specified in the Quantity column. The Modbus function to be used is defined in the Function column. The following functions are available:

- 0x01 Read Coils
- 0x02 Read Discrete Inputs
- 0x03 Read Holding Register
- 0x04 Read Input Register

Figure 19 – Modbus configuration form

Defined an address, i.e. a memory area, this will contain n variables or address range. Within the memory area each variable is in a position specified by its start bit ("From bit" column) and occupies n bits ("Length" column).

The properties to define for a variable are:

- From bit: start bit of the variable within the memory area starting at the address defined in the upper grid
- Length: number of bits that make up the variable
- High level data format: defines how to interpret the variable's bits. Whether or not a type can be defined depends on the variable's bit length. The possible options are:
 - BOOLEAN
 - INTEGER
 - STRING
 - TIME
 - FLOAT
- Sign: determines whether the INTEGER data should be considered with sign or not
- Factor: indicates a factor by which to multiply the read data
- Offset: indicates an offset to be added to the given bed
- ID: is a unique number that identifies the variable. It contributes to the composition of the actual identifier
- Identifier: obtained from the name of the Modbus device previously defined + "/" + ID
- Type: as in the case of KNX group addresses, the type assigns a logical meaning to a Modbus variable to make supervisor use more intuitive.

6.4 M-Bus

The M-bus gateway allows the reading of the values contained in the memory of the M-Bus meters.

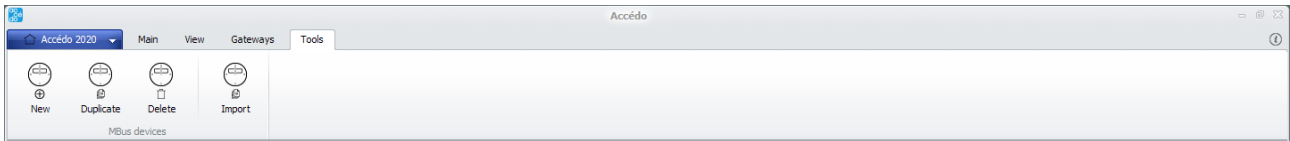


Figure 20 – M-Bus toolbar

The M-Bus configuration tools allow the definition of a new M-Bus counter, its duplication or deletion. It is also possible to import a new type of M-Bus counter not available in the access database. The configuration file that defines a new type is an XML file. Please contact accédo customer service for its definition.

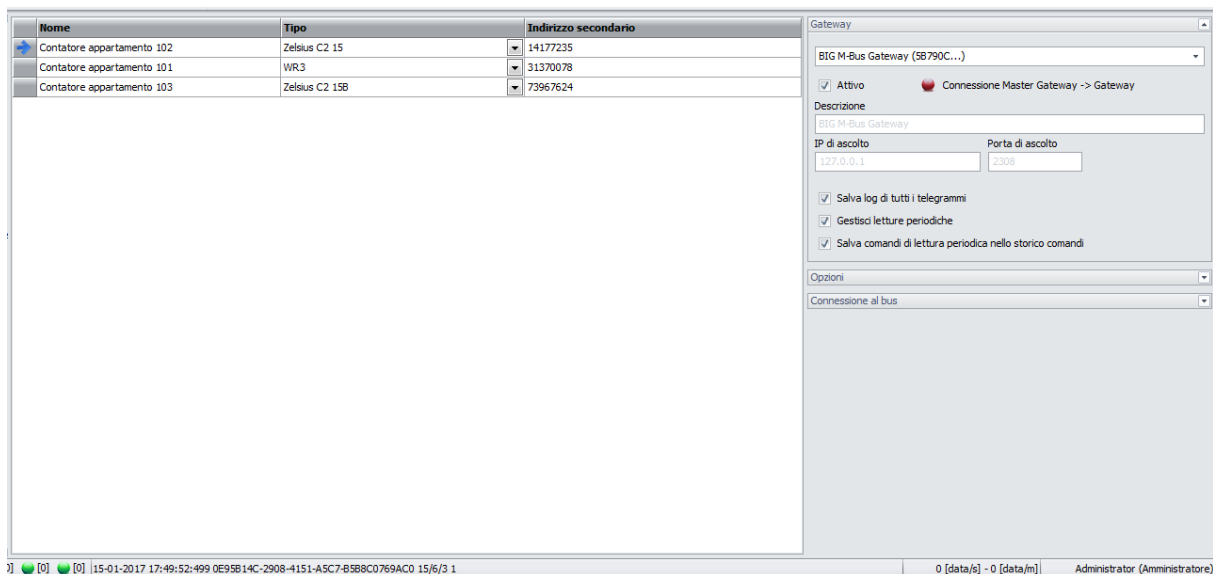


Figure 21 – M-Bus devices list

Defined a new M-Bus device the information required for its configuration are only 3:

- Name
- Type: to be chosen among the known types inserted in the software
- Secondary address: unique identifier printed on each M-Bus device

The screenshot shows a window titled "Gateway" with a dropdown menu set to "BIG M-Bus Gateway (5B790C...)". Below the dropdown, there is a checked checkbox labeled "Attivo" and a red status indicator with the text "Connessione Master Gateway -> Gateway". A section titled "Descrizione" contains a text box with "BIG M-Bus Gateway". Below this, there are two input fields: "IP di ascolto" with the value "127.0.0.1" and "Porta di ascolto" with the value "2308". At the bottom, there are three checked checkboxes: "Salva log di tutti i telegrammi", "Gestisci letture periodiche", and "Salva comandi di lettura periodica nello storico comandi".

Figure 22 – M-Bus gateway properties

In addition to the classic gateway properties, the M-Bus gateway has some special options by default that can be modified:

- Save log of all telegrams: automatically saves the value of all data read by an M-Bus device without setting the saving request for each value individually.
- Manage periodic readings: it is the gateway itself that takes care of the periodic readings set (relative to the M-Bus variables), while usually this task is performed by BIGOmnia.
- Save periodic read commands in the command history: if the previous point is set, the M-Bus management gateway, in addition to sending the periodic read commands, saves the required commands in the accédo database, in the command history.

The screenshot shows a window titled "Connessione al bus" with the following settings:

- COM Port: COM 7
- Baud rate: 2400
- Bit di dato: 8
- Bit di stop: 1
- Controllo di parità: Pari
- RTS: Set
- DTR: Set
- Timeout: 330
- Offset timeout: 0
- Offset byte: 40

At the bottom center, there is a green checkmark icon and a button labeled "Conferma / Aggiorna".

Figure 23 – M-Bus line properties

The M-Bus gateway reads data from M-Bus devices via an M-Bus master connected via serial. For a list of compatible M-Bus masters, please contact accédo technical assistance service.

7 CONFIGURATION

7.1 General informations

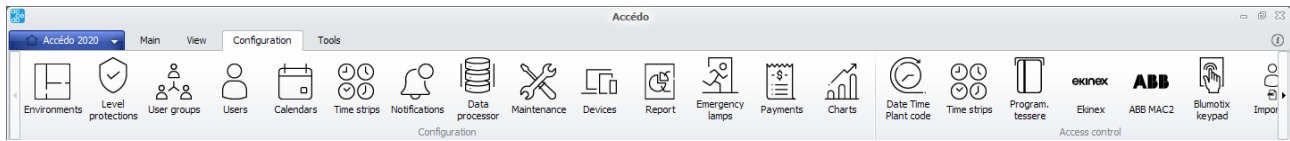


Figure 24 – Configuration section toolbar

The accédo configuration is divided into n sections.

The first sections are dedicated to the configuration of so-called gateways. A gateway is an accédo software extension (consisting of a Windows service) that manages a particular hardware or bus device. We therefore have the configuration of gateways related to:

- KNX / Konnex bus
- Modbus
- M-bus

The other configuration sections are specific to particular features of the software:

- Level protection
- Users and User groups
- Calendars
- Notifications
- Data processor
- Report
- Charts
- Configurations related to the access control section

7.2 Time strips

The time band configuration allows you to define a set of bands, each of which is made up of several sub bands (up to a maximum of 8).

The time bands and their sub-sections can be added, duplicated and removed from the dedicated instrument menu.

Each band can be identified by its own name.

For each sub-band you can define the days when the sub-band is active and the start and end times for the active days.

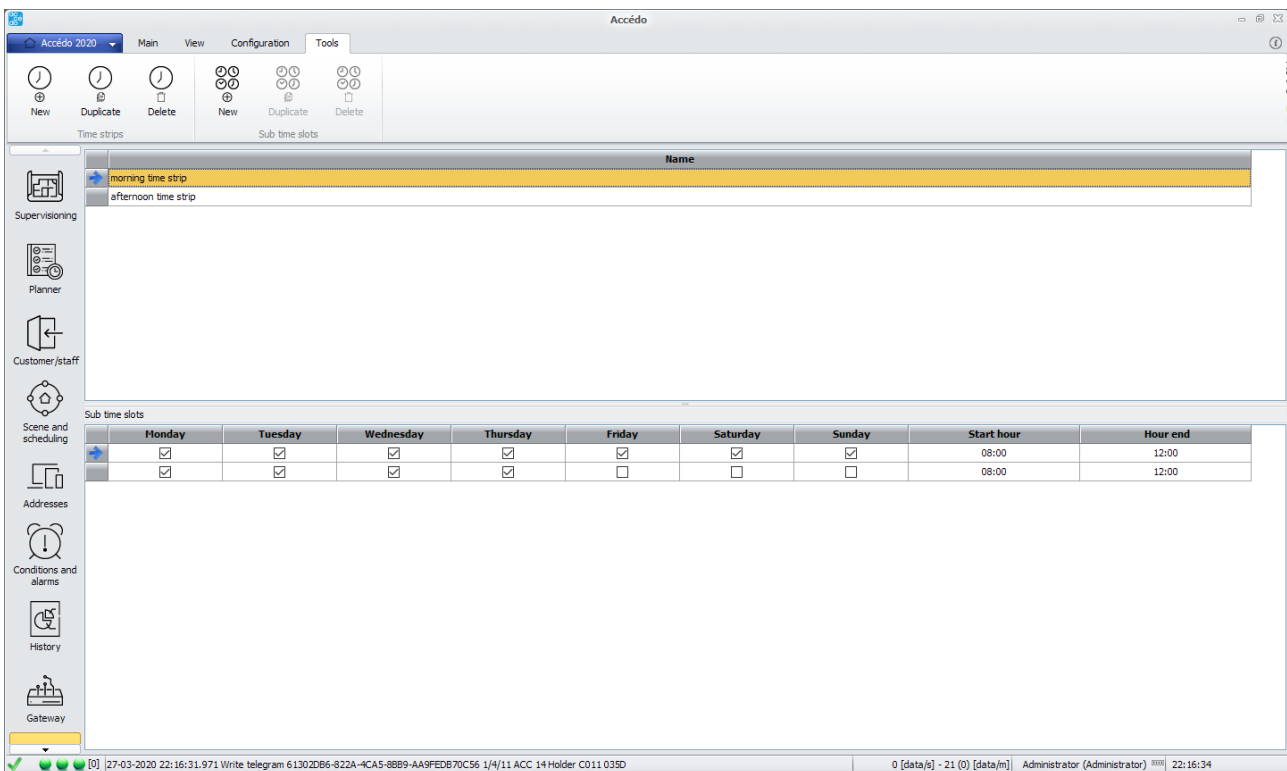


Figure 25 – creation of a time slot

7.3 Rooms

Through the Rooms configuration section you can have a summary view of the configuration of the environments; moreover it is possible to set some properties that are not present in the KNX configuration section.

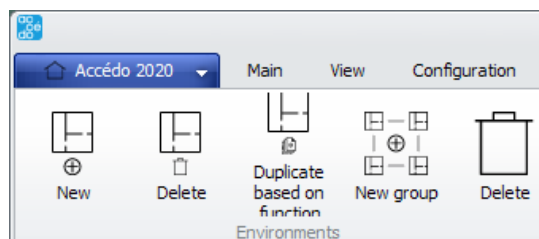


Figure 26 – tools for Rooms configuration

In addition to seeing the list of all existing rooms, generated by an ETS import in the KNX configuration section, or manually added in the same section, you can add or remove rooms via the Tools menu in the Room section.

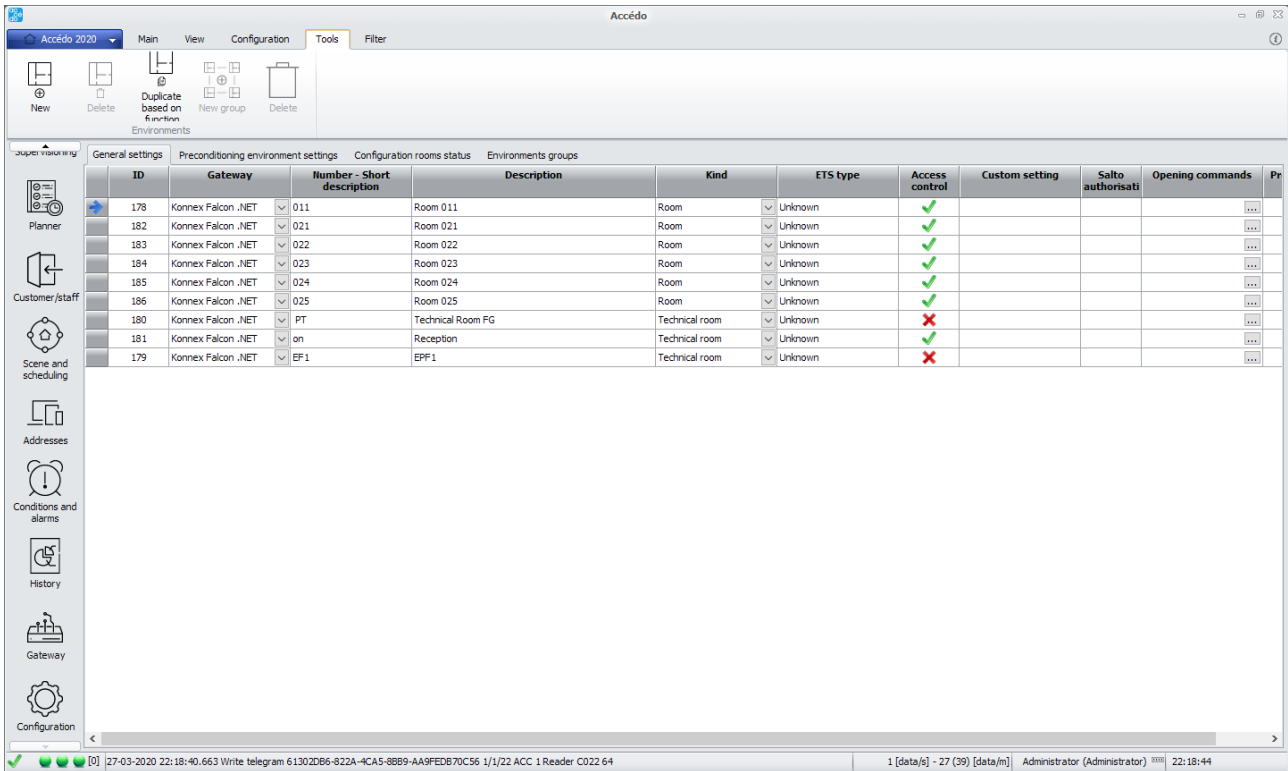


Figure 27 – Rooms grid

The room configuration is divided into 3 parts: general settings, preconditioning room settings and room status settings.

7.3.1 General settings

In the general settings you can configure the following parameters for each environment:

- Gateway
- Number/Short description
- Description
- Typology
- Custom setting
- Attendance: number of people currently inside the room; by clicking on the cell it is possible to see the list of customers/personnel present inside and, starting from this list, to force the entry or exit of a person from the room (see section *Presence Room management*).

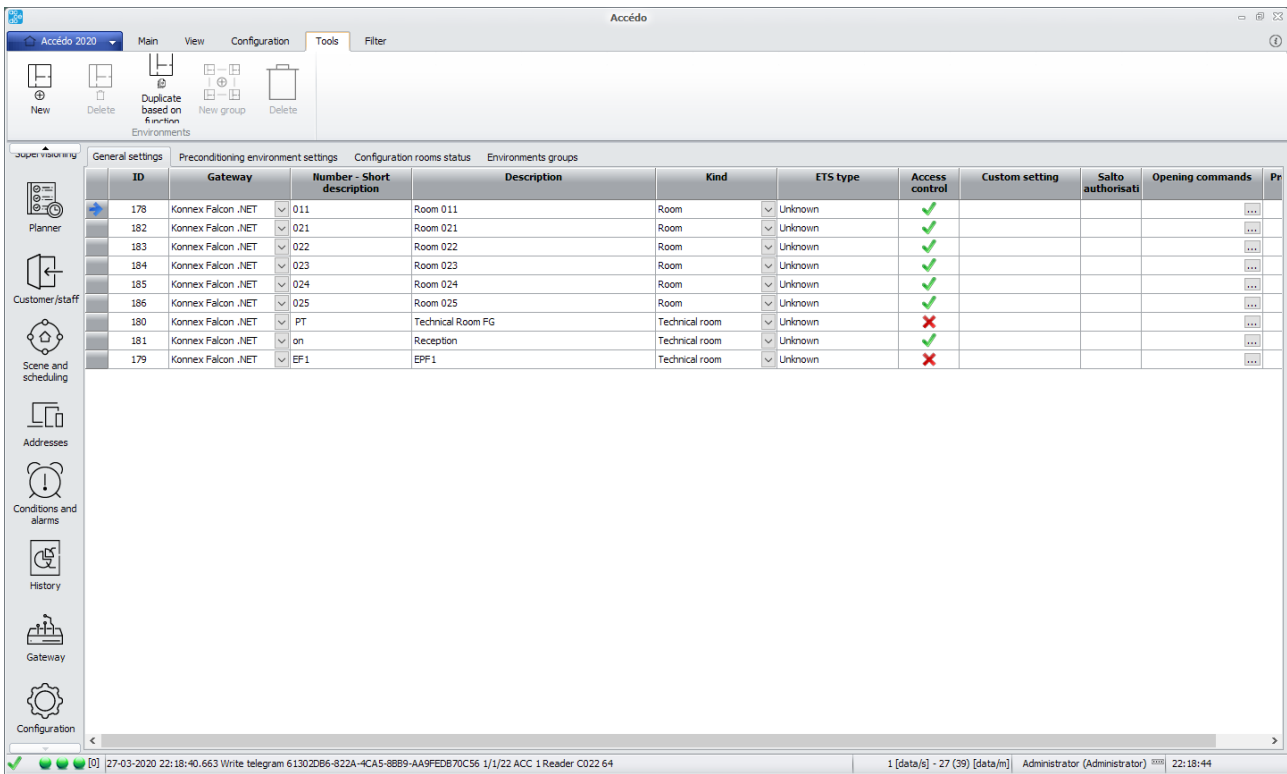


Figure 28 – general configuration

7.3.2 Room status settings

The room status grid allows to configure for each room type environment a set of addresses that represent a certain function within the environment itself.

Through this configuration it is possible to automatically generate room supervisions associating to each object only the function that that object represents, building a single supervision for all rooms and associating that supervision to all room type environments. Moreover, thanks to this configuration, in the section Histories -> Rooms -> Room status it is possible to see the current graphic status of the rooms in grid version.

The list of functions is grouped by categories:

- EnvironmentDescription: unchangeable room master information
- CleaningRoom: addresses related to room cleaning
- FridgeBar: addresses related to the status of the fridge bar
- OpenDoor: addresses related to door opening
- RoomPresence: addresses related to room presence
- BathroomAlarm: Bathroom alarm addresses
- Lights: addresses related to lights
- Thermostat1/thermostat2: addresses for room thermostats

By pressing on the pencil at the top left of the grid you can select which columns are used and displayed accordingly.

For each function there is both the status and the command.

To complete the grid is possible:

1. Click individually on the button present for each function, for each room and select the address to be inserted
2. Click on the button related to a function by selecting several lines (several rooms) and choosing the initial address; in the second line you will be asked for the offset to be used to complete the same function in the other selected rooms
3. Drag from the object tree a specific address to a configuration cell
4. Drag from the object tree a specific address on a configuration cell by selecting more than one line; as in case 2, the offset to be used to complete the same function in the other selected chambers is requested later on
5. Once one function has been configured, the others can be configured using the "Duplicate by functions" button: in this way you can select a start function and a destination function and, indicating the offset to be applied between the two, automatically fill in a second function.

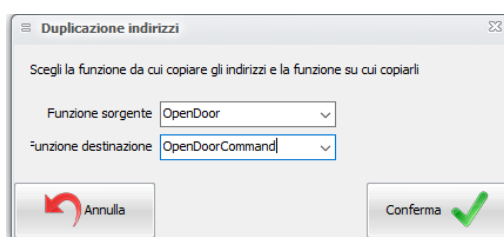


Figure 29 – addresses duplication form

Once the table is configured, i.e. each function used has been compiled for each room, in the section Historical->Room Status you can configure the grids to check the current status of the rooms.

As in the configuration phase, it is possible to define which columns/functions to show and you can divide the system into different pages (which can represent for example floors, or blocks) through the available tools:

- New: create a new rooms status page with all columns available
- Duplicate: creates a new rooms status page where only the columns visible are those visible on the current page
- Delete: Deletes the current page
- Rename: rename the current page
- Move in: when you select a set of rooms with the Move in button you can move the rooms to a second page; if the start page is the All rooms selected remain on the current page and are added to those of the destination page; if the start page is not the All rooms are moved, therefore they will no longer be present on the current page.
- Delete: deletes the selected room from the current page

7.3.3 Rooms groups

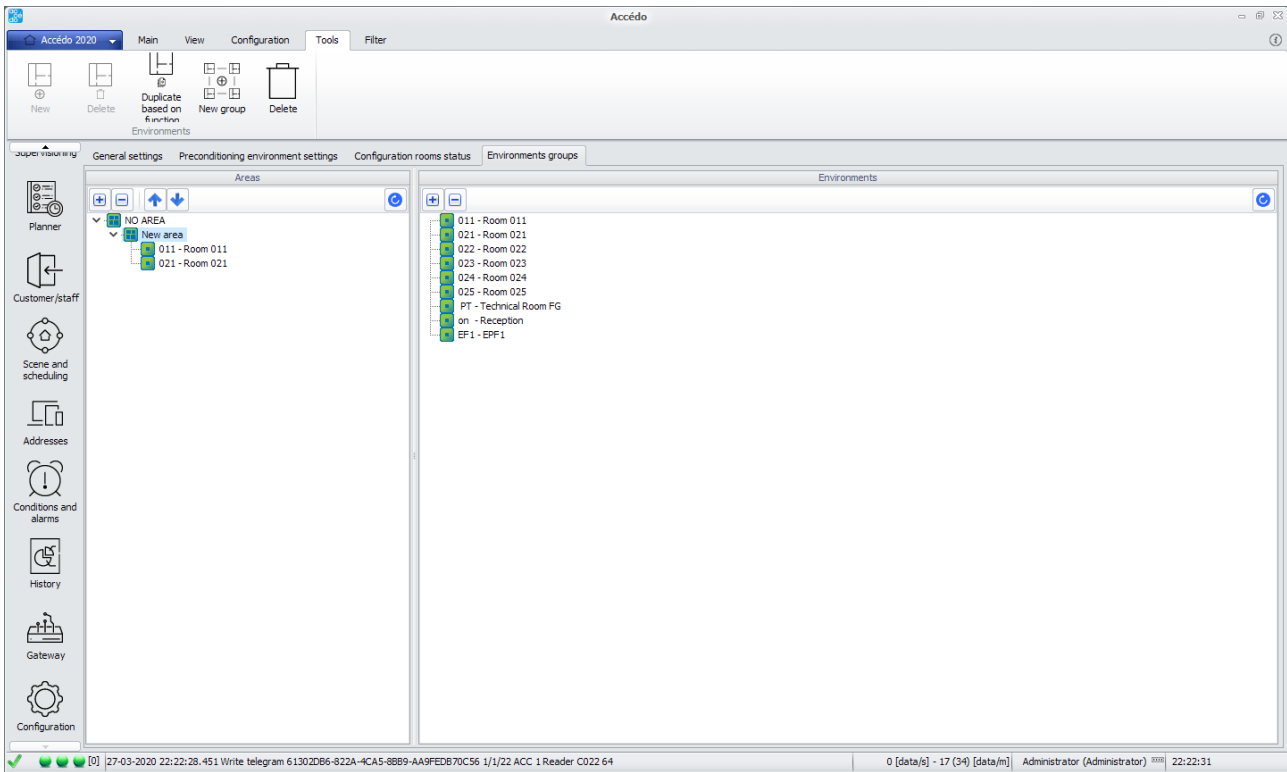


Figure 30 – Rooms groups

In the Groups of rooms section it is possible to define groups for the rooms: these groups are mirrored to the KNX areas during the first import, but can be modified at will by the user (without affecting the KNX configuration). In fact, the user can:

- Create a new group of rooms: using the New button after you have positioned yourself in the room groups tree; the new group is created below the selected group.
- Rename a group: by double-clicking on the group
- Add a room to a group: by dragging the room from the room tree to the desired group node

Each time you select a group of rooms, only the rooms that are not part of that group and its subgroups are displayed on the right.

The groups of rooms defined in this way are used in the access control section to assign accesses more quickly, acting directly on the groups and not on the individual rooms.

When a room is removed from a group of rooms, all the cards associated with that group of rooms (and consequently the removed rooms) lose their relationship with the removed room; in the same way, when a room is added to a group of rooms, all the cards associated with that group of rooms also receive access to the new room.

The changes of accesses on the cards take place both at the relationship level and at the level of sending telegrams to the indicated devices (if necessary).

7.3.4 Presence management in the room

Through accédo it is possible to trace the presence of customers and staff in the defined rooms.

The management is enabled through the setting "Trace presence in real-time in the rooms and areas" present under the Access Control section. Once enabled, it is necessary to restart BIGOmnia in order to generate the addresses necessary for tracking under the PresenceCounter node in the Variables group of each gateway.

For each area a node containing the following addresses is generated:

- AREA/CustomID/CountPresence [CountPresence]: contains the number of people currently present in the area, calculated as the sum of the number of people present in the sub-areas or sub-rooms;
- AREA/CustomID/ListPresence [ListPresence]: contains the list of IDs of the cards currently present in the room separated by ',', calculated as the sum of the IDs of the cards currently present in the sub-areas or sub-rooms.

The nodes of the areas and rooms are hierarchically structured below the *PresenceCounter* node according to the definition made inside the gateway.

The presence of these addresses is verified by the AccessManager at startup; the same AccessManager initializes the addresses of areas and environments calculating their initial values.

At the first start of BIGOmnia, the calculation of the initial presence in the rooms is made through the access history (table ACCESS_HISTORY): for each card that has made at least one access to a given room, the most recent date between the entry and exit access (if present) is verified and the presence or absence of that card (and its associated customer/personal) in the room is defined accordingly (if the most recent date corresponds to the entry access the customer/personal is still inside the room).

Access is considered to be either input or output depending on the device through which it was made and its configuration. For each access device it is possible to define in its configuration the type "*Input/Output*" with the values "*Not defined/Input/Output*". All devices are born with "*Not defined*" typology and must be configured as needed.

The calculation of the presences on the areas is made starting from the values present in the hierarchically linked environments.

At each subsequent start of BIGOmnia, the initial attendance values are defined as the last values of the relative addresses.

Each time you access an environment on which the input and output devices have been defined, the AccessManager updates the value of the relative *CountPresence* and *ListPresence* addresses for the room in question and the addresses of the hierarchically linked areas.

In some cases it may be necessary to force the entry or exit of a customer/personal from a certain room by bypassing the automatic calculation made by the accessManager. This can happen, for example, when accesses (entry or exit) are made in an a room while BIGOmnia is stopped; in this case the accesses are not recorded and the calculation made by BIGOmnia is misaligned with the real presence in the room.

The presences can be realigned in the section "*Configuration->Environment->General settings*" through the Presences column: for each room the number of clients/personnel currently present in the room is displayed and, by clicking on the cell, it is possible to see the list of names associated with presences. To force the removal of a callsign, simply remove the corresponding tick, while to insert one or more new callsigns, press the + button and enter the card numbers to simulate access. Forcing an entry or removal generates a simulated access in the room and updates all related addresses.

The presences are updated in real time only when the screen displayed is this one, otherwise it is necessary to re-filter the grid to update the data.

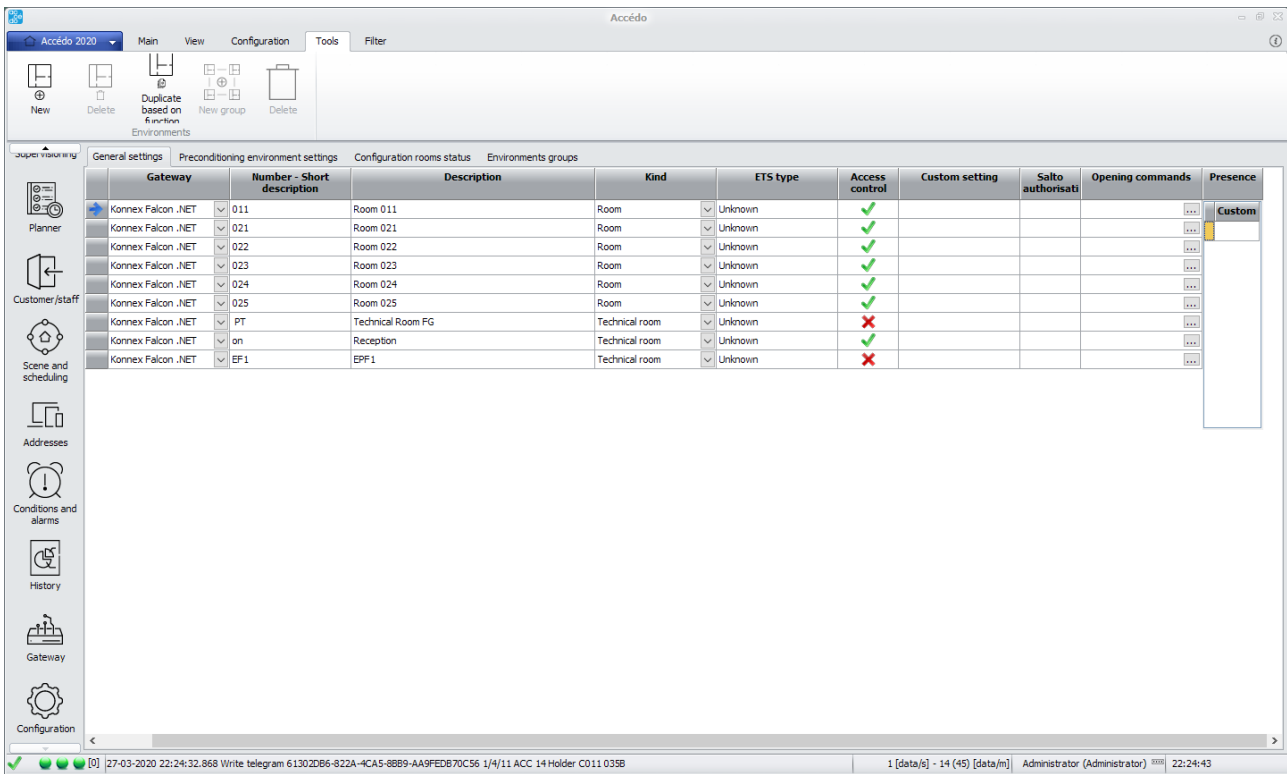



Figure 31 – presence in the rooms

Attendances can also be monitored from the section "Historical->Room Presences": the tree on the left shows the hierarchy of areas and rooms present in the system with the number of presences in that room/area.

Selecting the single area or the single rooms, the list of names present in the room is displayed on the right side.

Through the button  you can update the attendance data (which are updated in real time only if the screen displayed is this one).

7.4 Access levels

The configuration of the protection levels allows you to configure the visible sections of accédo for each level. There are 7 predefined protection levels, which can be associated with the user in the user configuration section:

- Administrator
- Manager
- Supervisor plus
- Supervisor
- Maintenance
- User plus
- User

For each level you can configure the different visibility permissions for the sections of the software, except for the *Administrator* level which always has visibility on each section.

Each section is visible from a certain level if the respective box is enabled.

The sections for which visibility can be configured include main sections, such as main menu areas and configuration areas, and detail areas, such as areas in application settings.

Categoria	Function	Administrator	Manager	Supervisor plus	Supervisor	Maintenance	User plus	User
Visibilità bottoni menù	Show supervision area	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Visibilità bottoni menù	Show planner area	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Visibilità bottoni menù	Show access control area	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Visibilità bottoni menù	Show devices area	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Visibilità bottoni menù	Show scene and schedules area	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Visibilità bottoni menù	Show logics/alarms area	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Visibilità bottoni menù	Show report area	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Visibilità bottoni menù	Show configuration area	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Visibilità bottoni menù	Show settings area	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Visibilità bottoni menù	Show emergency lamps area	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Visibilità bottoni menù	Show weekly plannings area	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Visibilità sezioni settings	Show general settings	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Visibilità sezioni settings	Show server settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Visibilità sezioni settings	Show database settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Visibilità sezioni settings	Show backup/restore settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Visibilità sezioni settings	Show schedule backup settings	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Visibilità sezioni settings	Show log settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Visibilità sezioni settings	Show alarm notification settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Visibilità sezioni settings	Show supervision settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Visibilità sezioni settings	Show country settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Visibilità sezioni settings	Show language settings	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Visibilità sezioni settings	Show PMS interface settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Visibilità sezioni settings	Show misc settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Visibilità sezioni settings	Show skin settings	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Visibilità sezioni settings	Show user password settings	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Visibilità sezioni settings	Show access control settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Visibilità sezioni settings	Show access control environments display settings	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Visibilità sezioni settings	Show ABB MAC2 access control settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Visibilità sezioni settings	Show SMTP server configuration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Visibilità sezioni settings	Show daily export history settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Visibilità sezioni settings	Show astronomical clock settings	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 32 – Access levels configuration

7.5 User groups

In this section you can define user groups, which are used to manage the following permissions for each group:

- Node/address visibility permission: allows you to define the visibility on each node/address;
- Node/address writing permission: allows you to define the writing on each node/address;
- Supervisions: allows you to define visibility on supervisions;
- Rooms: allows you to define visibility on rooms;

By default all permissions are granted.

Through the tools menu you can create a new user group or delete the selected user groups.

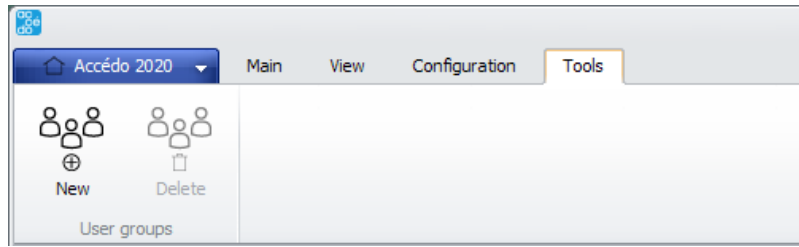


Figure 33 – User groups creation toolbar

For each user group you can define its name, description, and a set of user members.

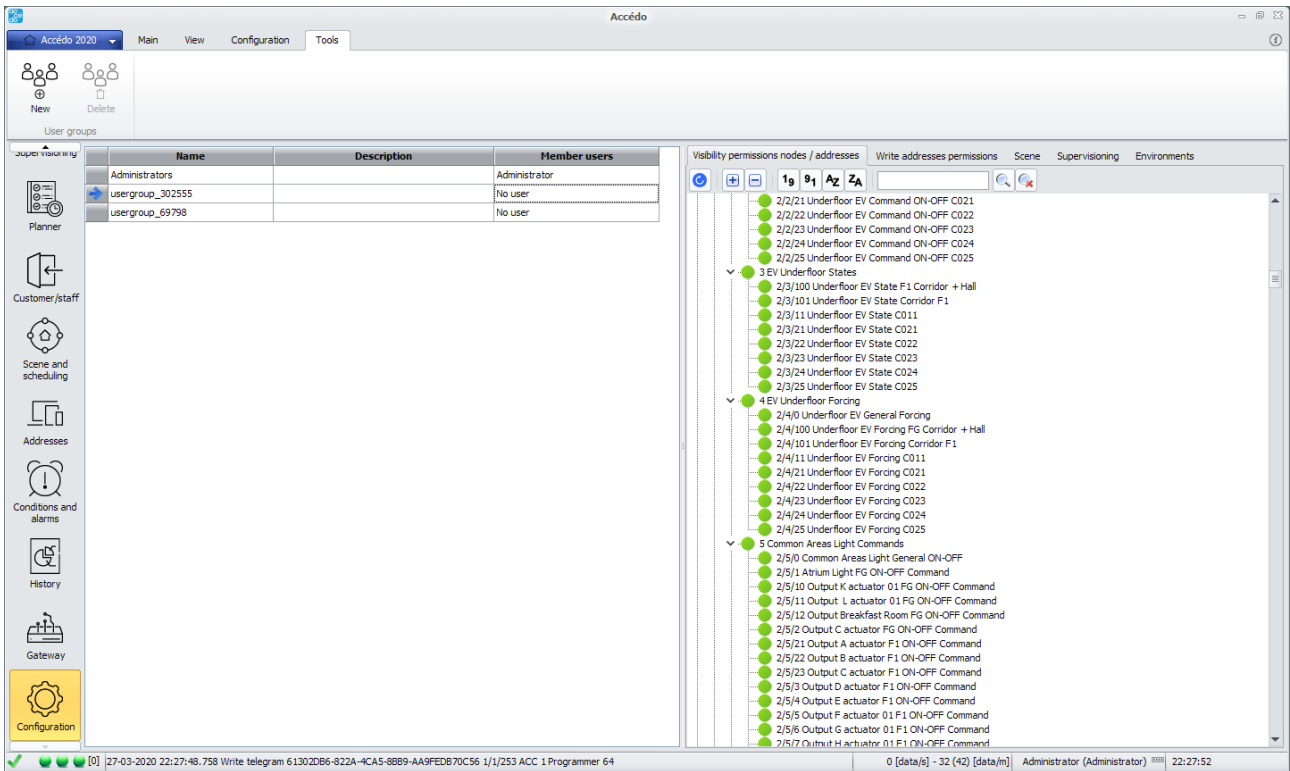


Figure 34 – User groups creation

7.5.1 Nodes/addresses visibility permissions





The permits follow the legend:

- The group has visibility on all its child nodes/addresses (or on itself if it is an address);
- The group has no visibility on its child nodes/addresses (or on itself if it is an address);
- The group has visibility on some of the child nodes/addresses, but not on all of them.

In case a node has denied visibility, it is not possible to make its nodes/children addresses visible. Clicking on a node changes the permission to the node and all its child nodes.

7.5.2 Nodes/addresses writing permissions



The permits follow the legend:

-  The group can write on all child nodes/addresses;
-  The group can write on the node/address;
-  The group has no visibility on its nodes/addresses children;
-  The group can write on some of the children's nodes/addresses, but not on all of them or has no visibility on all children.

Clicking on a knot changes the permission to the knot and all its child knots.

7.5.3 Supervisions

The permits follow the legend:



-  The group has visibility on supervision;
-  The group has no visibility on supervision.

Since supervisors can be organized into folders, right-clicking on the folder allows you to change the permission for all supervisors in the folder.

This permission affects the visibility of the supervisors.

7.5.4 Rooms

The permits follow the legend:

-  The group has visibility on the room;
-  The group has no visibility on the room;

This permission affects the visibility of the rooms in the access control section, allowing access to the cards only for the rooms that are visible to the user group. In addition, within the planner will be visible only the rooms for which the visibility permission is present on the rooms, and consequently only the reservations made on these rooms will be visible and manageable.

7.6 Users

This section defines the users for whom it is necessary to indicate username and password, the level of administration, first name, last name and groups they belong to. In addition, as for groups, you can define the following permissions:

- Node/address visibility permission: allows you to define the visibility on each node/address;
- Node/address writing permission: allows you to define the writing on each node/address;
- Supervisions: allows you to define visibility on supervisions;
- Rooms: allows you to define visibility on the rooms;

By default all permissions are granted.

Through the tools menu you can create a new user or delete selected users.

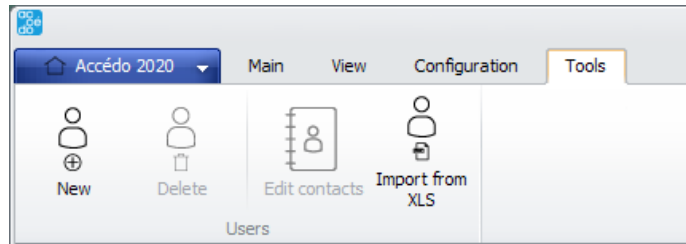


Figure 35 – New user definition

Through the *Import from xls* button you can import a set of users from an Excel file, formatted as follows:

- Column A: new user's username (required)
- Column B: new user password (required)
- Column C: surname of new user (optional)
- Column D: new user name (optional)

If a user with the same username is already present, his data is updated with the information in the excel. The booking level is required before import and all users created are associated to that level of protection. All new users are associated to the *Administrator* group.

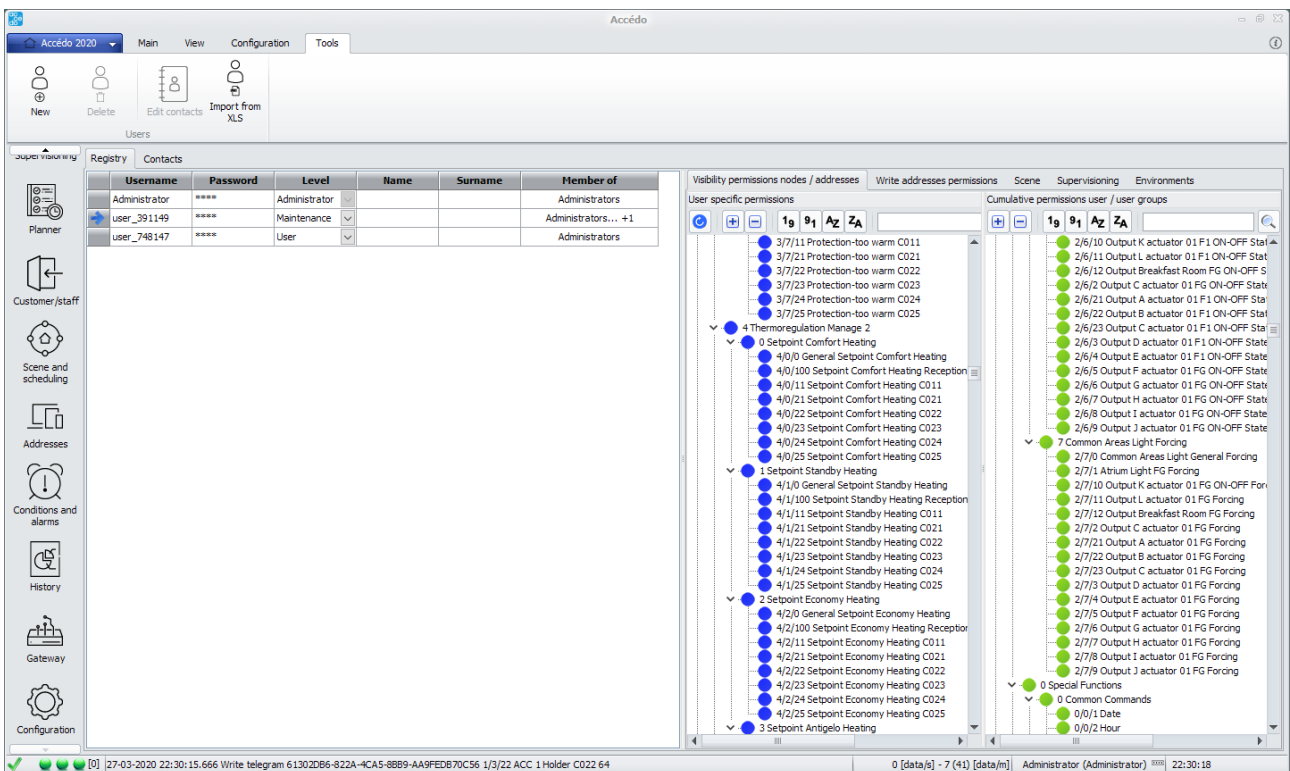







Figure 36 – User details

7.6.1 Nodes/addresses visibility permissions





Permissions follow the legend:

-  The user has visibility on all his child nodes/addresses (or on himself if it is an address) by selection on the node;
-  The user has no visibility on his child nodes/addresses (or on himself if it is an address) by selection on the node;
-  The user has visibility on the node by selection on the node and on some of the child nodes/addresses, but not on all of them;
-  The user has visibility inherited from the group for the node, but for some of his children he has defined a non-visibility permission;
-  The user has visibility inherited from the group for the node and child nodes (inherited from the group or selected on the node);

In case a node has denied visibility, it is not possible to make its nodes/children's addresses visible. Clicking on a node changes the permission to the node and all its child nodes.

7.6.2 Nodes/addresses writing permissions




Permissions follow the legend:

-  The group can write on all child nodes/addresses;
-  The group can write on the node/address;
-  The group has no visibility on its nodes/addresses children;
-  The group can write on some of the children's nodes/addresses, but not on all of them or has no visibility on all children;

In order for the node/address to be writable, a visibility permission on the node must be defined by the single user: the permission inherited from the group is not sufficient.

7.6.3 Supervisions

Permissions follow the legend:




-  The group has visibility on supervision;
-  The group has no visibility on supervision;
-  The user has inherited visibility from the group on supervision;

Since supervisors can be organized into folders, right-clicking on the folder allows you to change the permission for all supervisors in the folder.

This permission affects the visibility of the supervisors.

7.6.4 Rooms

Permissions follow the legend:

-  The group has visibility on the environment;
-  The group has no visibility into the environment;
-  The user has inherited visibility from the group on the environment;

This permission affects the visibility of the environments in the access control section, allowing access to the cards only for the environments that are visible to the user group. In addition, within the planner will be visible only the rooms for which there is a visibility permission on the environment, and consequently only the reservations made on these environments will be visible and manageable.

7.6.5 Contatti

Each user can associate their contacts, in particular telephone numbers, e-mails and SIP extensions.

In the *Contacts* section you can see the contacts associated to each user; these contacts can be edited by pressing the *Edit* contacts button after selecting the user concerned.

The contact management form allows you to manage phone numbers, e-mails and SIP numbers of the selected user. The contacts are used both for information purposes and for sending notifications to users.

For each contact you can define the description and value. In addition, for each type of contact you can define a bookmark: the bookmark is used as a preferred choice in case you want to send notifications to the selected user.

Phone numbers and emails are freely definable, while SIP numbers can be selected according to the SIP numbers configured in the system.

7.7 Notifications

Notifications are reports that are made when a certain event occurs, such as the occurrence or non-occurrence of a logic (or alarm) or the occurrence of an access (allowed or denied).

In this section only the notifications are configured, while the association with a certain event is made in the section dedicated to the event itself (for example, if the notification must be associated with an alarm, the association with the notification is defined during the configuration of the alarm).

Through the tools menu it is possible to add a new notification or duplicate/eliminate a pre-existing one.

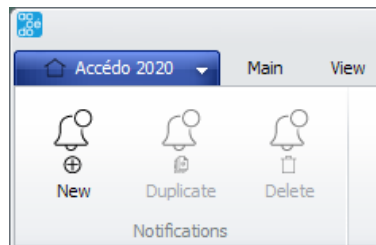


Figure 37 – Notification creation tools

For each notification, you may indicate one or more reporting methods among those present: popup, balloon, page jump, audio, email, SMS, SIP.

7.7.1 Registry section

In the master section you can define the following properties for each notification:

- Name: name identifying the notification
- Description: full description of the notification, used to build the default text if any
- Use the default text: the system is able to build a default text to be inserted in the notification based on the type of notification chosen and the event that triggered the notification
- Popup notification: enable the popup notification method for notification
- Page Skip Notification: enables the page skip notification method for notification
- Audio Notification: enable the audio notification method for notification
- Email notification: enable the email notification method for notification
- SMS notification: enable SMS notification method for notification
- SIP Notification: enables the SIP notification method for notification
- Notification with Telegram: enable the Telegram reporting method for notification

Name	Description	Use default text	Popup notification	Balloon notification	Page jump notification	Audio notification	Email notification	SMS notification	SIP notification	Telegram notification
Bathroom Alarms		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Split Error Alarms		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 38 – Registry sheet

7.7.2 Common configuration to all reporting methods

Each reporting method is specifically configurable, but the following configurations are common to all reporting methods:

- **Masking time:** given a certain notification, defines the minimum time that elapses between two successive releases of that notification as a result of the same event. If the notification is associated with two different events, the masking time is calculated individually for each event. *Example: If the notification is associated with an event that occurs every 5 seconds but you want to receive the associated notification no more than once per minute, you can indicate a masking time of one minute so that the notification will not be issued unless at least one minute has passed since its last issue.*
- **Users:** list of users to send the notification to or to be excluded for sending the notification. From the list of available users it is possible to define the users to whom the notification should be sent (tick), to whom the notification should not be sent (empty square) or for whom the decision to send or not to send the notification is left to the groups they belong to (full square). In the latter case the notification is sent to the user if at least one of his groups is enabled to send the notification. The user receives the notification according to the reporting method defined for the notification.
- **User groups:** list of user groups to send the notification to or to exclude for sending the notification. From the list of available user groups you can define the groups to send the notification to (tick) or not to send the notification to (empty square). The user group receives the notification according to the reporting method defined for the notification.
- **Time bands:** list of time bands in which the notification is enabled. From the list of time bands available, you can define the time bands in which the notification is sent. If no time slot is selected, the notification is always sent, otherwise it is sent if the time at which the notification is to be sent falls within one of the selected time slots.
- **Calendars:** list of calendars in which notification is enabled. From the list of available calendars you can define the calendars in which the notification is enabled. In case no calendar is selected the notification is always sent, otherwise it is sent if the time when the notification is to be sent falls in one of the selected calendars.

7.7.3 Popup configuration

When the event associated with the notification is triggered, a popup appears on the screen containing the information associated with the event triggered. The popup configuration foresees to define the following fields:

- **Custom title:** if the use of the default text is disabled you can define the title that appears on the popup.
- **Custom text:** if the use of the default text is disabled you can define the text that appears on the popup.
- **Allow closing:** if enabled, it prevents the closing of the popup with the close button.
- **Users and user groups:** the popup appears only on PCs where accédo is started and logged in with a user among those enabled to receive the notification.

The popup that is created accordingly is differentiated according to the event that generated it.

If the event is a logic or an alarm the popup contains the following data:

- **Date and time events**
- **Title and text**
- **List of previous events of the same type associated with the same alarm/logic**
- **View:** button to view the event; the logged in user who presses the button is registered as the user who viewed the event.

- Solve: button to solve the event; the logged in user who presses the button is registered as the user who solved the event.
- Notes: any notes to be associated to the viewing or to the resolution
- Close: button to close the popup while ignoring the event.

If the event is an access contains the following data:

- Date and time of event
- Event (access denied, allowed, card insertion or removal)
- Environment to which you are logged in
- Card/number plate/phone number used to log in
- Customer/Personal who logged in (based on card number, license plate number or telephone number used to log in)
- The following customer/personal data (taken from your personal data)
 - Image (if any)
 - Name and surname
 - Date of birth
 - Company
 - Office
 - Business function/grade
 - Assignment
 - License Plate

In case of access event, any custom title and text will be ignored.

7.7.4 Balloon configuration

When the event associated with the notification is triggered, a balloon appears on the screen (bottom right) containing the information associated with the event triggered. The popup configuration foresees to define the following fields:

- Custom title: If the use of the default text is disabled you can define the title that appears on the balloon.
- Custom Text: If the use of the default text is disabled you can define the text that appears on the balloon.
- Type: "single": the creation of a balloon leads to the deletion of the previous balloon (if present); "cascading": new balloons are placed above the previous ones until the previous ones disappear. Cascading balloons, in case they are used as an access signal, also contain the possible photo of the customer/staff who tried to access.
- Icon: icon on the balloon, choose between information, alert, error.
- Timeout: time in which the balloon remains visible before closing by itself (unless previously closed by a user).
- Users and user groups: the balloon appears only on PCs where accédo is started and logged in with a user among those enabled to receive the notification.

7.7.5 Page jumping configuration

When the event associated with the notification is triggered, if accédo is on a supervision page, the display jumps to the page defined in the notification. The configuration of the page jump involves defining the following fields:

- Page: page of supervision to which to blow up accédo.
- Users and user groups: the page jump takes place only on the pc where accédo is started and logged in with a user among those enabled to receive the notification.

7.7.6 Audio configuration

When the event associated with the notification is triggered, an audio alert is emitted. The following fields are defined in the audio configuration:

- Audio file: Audio file to be output when the notification is triggered.
- Repeat until solution: audio is repeated until the associated event (usually an alarm) is resolved
- Number of repetitions: fixed number of times the event is repeated (if Repeat until solution is not active).
- Repeat interval: time interval between the execution of two successive repetitions (if the number of repetitions is greater than 1).
- Users and user groups: the audio is played only on the PC where access is started and logged in with a user among those enabled to receive the notification.

7.7.7 E-mail configuration

When the event associated with the notification is triggered, an email containing the information associated with the event triggered is sent. The configuration of the email foresees to define the following fields:

- Custom title: if the use of the default text is disabled you can define the subject of the email.
- Custom text: if the use of the default text is disabled you can define the email text; an email editor is used for its definition, which can be opened using the button in the column.
- Recipients: list of recipients, separated by ';' to whom the mail should be sent.
- Users and user groups: the mail recipients are added to the mail marked as favourites of the users enabled to receive the notification.

7.7.8 SIP configuration

A call is made when the event associated with the notification is triggered. The following fields are defined in the SIP configuration:

- Sender number: any of the SIP numbers configured
- Recipient number: list of SIP numbers (system extensions or traditional SIP numbers) divided by ';' to which the call should be made.
- Users and user groups: SIP numbers marked as favourites of the users enabled to receive the notification are added to the recipients of the SIP call.

7.7.9 SMS configuration

An SMS is sent when the event associated with the notification is triggered. The SMS configuration foresees to define the following fields:

- GSM: GSM gateway to be used for sending the message
- Recipients: list of phone numbers divided by ';' to send the message to
- Custom text: if the use of the default text is disabled you can define the text to insert in the message
- Users and user groups: SMS recipients are added to the phone numbers marked as favorites of the users enabled to receive the notification.

7.8 Maintenances

The maintenance configuration allows you to define a set of maintenance that must be performed periodically following a time interval (for example every 100 hours), or a calendar.

In the first case, a total hour counter address must be specified (which increases by one every hour), which will be used as a reference to determine the time at which the next maintenance is scheduled: this is calculated starting from the time at which the last maintenance was performed, to which the time period dividing two maintenance operations is added.

In the second case a calendar must be specified: the next maintenance is scheduled as the first calendar day following the current day; the time is in the format 00:00.

Name	Description	Calendar	Interval between	Total hourcounter address	Address partial countour to previous maintenance	Address partial countour to next maintenance	Notice notification	Notice hour for the notify	Delay notification	Delay hour for the	Counthour hours from	Timestamp last executi	Period of next executi
Lighting maintenance			2	...	MAINTENANCE/1/1 ...	MAINTENANCE/1/2 ...		0		0	0	30-12-18	
Calendar maintenance			0	...	MAINTENANCE/2/1 ...	MAINTENANCE/2/2 ...		0		0	0	30-12-18	

Figure 39 – Maintenances grid

Maintenance can be managed through the tools menu, which allows to insert, duplicate or eliminate a maintenance.

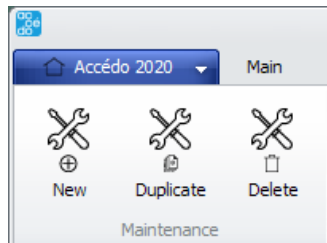


Figure 40 – Maintenance toolbar

For each maintenance you can define:

- Name
- Description
- Calendar: When a calendar is selected, the next scheduled maintenance is calculated on the first day after the current day and belonging to the calendar at 00:00. E.g. if I want to carry out maintenance on the first of the month, I define a calendar having as days the first of each month and I associate it with the maintenance. On each day, the next maintenance is calculated as the first day of the following month.
- Time range: when a time range is indicated, the next scheduled maintenance is calculated as the time (at the hour counter) when this maintenance was last performed, to which the time range is added. E.g. if I want to do a maintenance every 200 hours I associate the total hour counter and define the time range 200; In each hour, the next maintenance is calculated as the hour at the hour counter in which the maintenance to which the time range 200 is added was last performed.
- Total hour meter address: address that tracks the passage of hours. It is only mandatory if maintenance is defined according to a time range.

- Partial hour counter address at the previous maintenance: virtual address (automatically created at the generation of the maintenance or chosen at will by the user) that contains the number of hours from which the last maintenance was performed.
 - The automatically created partial addresses are virtual and in the form: MAINTENANCE/ID_MANAGEMENT/1 [HourMeterPrevious *Maintenance Name*].
- Partial hour counter address at the next maintenance: virtual address (automatically created at the generation of the maintenance or chosen at will by the user) which contains the number of hours between which the next maintenance must be done.
 - The automatically created partial addresses are virtual and in the form: MAINTENANCE/ID_MANAGEMENT/2 [HourMeterPrevious *Maintenance Name*].
- Notification notice: notification to be used to give notice of maintenance expiration.
- Hours notice: hours before the maintenance expiration date to send the notification.
- Delay notification: notification to be used to report with a delay in the execution of the maintenance.
- Hours delay: hours after the maintenance deadline to send the report.
- Last execution time: total hour counter value at last execution.
- Date time of last execution:
- Hours until next execution
- Date time next execution

Notifications use partial hour counter addresses for counting hours of notice and delay, so it is always necessary to define them.

The calendar and time range are mutually exclusive.

Attention! In the event of a machine change and/or counter reset, it is necessary to create a dummy maintenance at time 0 with a machine change notification.

7.9 Devices

The device configuration allows you to view the master data of imported devices and configure their properties. The configuration is divided into 6 tabs:

- Registry
- Configuration
- Guest access actions
- Actions other accesses
- Guest access notifications
- Other access notifications

7.9.1 Data

The master data section allows the display of the devices present and their characteristics. The information comes from the KNX project import with ETS and the subsequent configuration and cannot be modified from this section.

The only column that can be modified is the *Access Strategy*, valid only for Readers, Holder or Numeric Keypads devices. The possible access strategies are:

- White list: the card codes for which access is allowed are specified to the device

- Black list: only used by ekinex devices; the card codes for which access is denied are specified to the device
- Centralized: the card codes are sent only to the pockets (to avoid the continuous sending of the denied access signal): the access devices always send the code and it is then decided whether access is allowed or denied and the command to open the gate is sent (see section *Centralized Access control*).

Description	Gateway	Gateway kind	Physical address	Access code	Guest data	Confirma server	Constructor	Family	Product code	Access strategy
Alimentatore KIX	Konnex Falcon .NET	KIX	1.1					Unknown device	0	
Attuatore 01 P1	Konnex Falcon .NET	KIX	1.1.102					Unknown device	0	
Attuatore 01 PT	Konnex Falcon .NET	KIX	1.1.101					Unknown device	0	
EK-TH2-TP - tasca porta	Konnex Falcon .NET	KIX	1.1.3	7/0/6 R01_Holder_ACC1	7/0/7 R01_Holder_ACC14		Ekinex S.p.A.	Card holder	33	White
EK-TR2/TP2-TP -	Konnex Falcon .NET	KIX	1.1.1	7/0/0	7/0/1		Ekinex S.p.A.	Card reader	32	White
EK-TR2/TP2-TP -	Konnex Falcon .NET	KIX	1.1.2	7/0/2 R01_Reader_ACC1	7/0/3 R01_Reader_ACC14		Ekinex S.p.A.	Card reader	32	White
Gateway Mitsubishi C021	Konnex Falcon .NET	KIX	1.1.18					Unknown device	0	
Gateway Mitsubishi C022	Konnex Falcon .NET	KIX	1.1.22					Unknown device	0	
Gateway Mitsubishi C023	Konnex Falcon .NET	KIX	1.1.26					Unknown device	0	
Gateway Mitsubishi C024	Konnex Falcon .NET	KIX	1.1.30					Unknown device	0	
Gateway Mitsubishi C025	Konnex Falcon .NET	KIX	1.1.34					Unknown device	0	
IPS/S3. 1.1	Konnex Falcon .NET	KIX	1.1.255					Unknown device	0	
Lettore C011	Konnex Falcon .NET	KIX	1.1.11	1/1/11 ACC 1 Reader	1/2/11 ACC 14 Reader		ABB	Card reader	8458	White
Lettore C021	Konnex Falcon .NET	KIX	1.1.15	1/1/21 ACC 1 Reader	1/2/21 ACC 14 Reader		ABB	Card reader	8458	White
Lettore C022	Konnex Falcon .NET	KIX	1.1.19	1/1/22 ACC 1 Reader	1/2/22 ACC 14 Reader		ABB	Card reader	8458	White
Lettore C023	Konnex Falcon .NET	KIX	1.1.23	1/1/23 ACC 1 Reader	1/2/23 ACC 14 Reader		ABB	Card reader	8458	White
Lettore C024	Konnex Falcon .NET	KIX	1.1.27	1/1/24 ACC 1 Reader	1/2/24 ACC 14 Reader		ABB	Card reader	8458	White
Lettore C025	Konnex Falcon .NET	KIX	1.1.31	1/1/25 ACC 1 Reader	1/2/25 ACC 14 Reader		ABB	Card reader	8458	White
Modulo Logico KIX	Konnex Falcon .NET	KIX	1.1.254					Unknown device	0	
Programmatore tessere 1	Konnex Falcon .NET	KIX	1.1.253	1/1/253 ACC 1	1/2/253 ACC 14		ABB	Card reader	8458	White
Ragnetto 1 Reception	Konnex Falcon .NET	KIX	1.1.110					Unknown device	0	
Ragnetto 2 Reception	Konnex Falcon .NET	KIX	1.1.111					Unknown device	0	
Tasca C011	Konnex Falcon .NET	KIX	1.1.12	1/3/11 ACC 1 Holder C011	1/4/11 ACC 14 Holder		ABB	Card reader	8458	White
Tasca C021	Konnex Falcon .NET	KIX	1.1.16	1/3/21 ACC 1 Holder C021	1/4/21 ACC 14 Holder		ABB	Card reader	8458	White
Tasca C022	Konnex Falcon .NET	KIX	1.1.20	1/3/22 ACC 1 Holder C022	1/4/22 ACC 14 Holder		ABB	Card reader	8458	White
Tasca C023	Konnex Falcon .NET	KIX	1.1.24	1/3/23 ACC 1 Holder C023	1/4/23 ACC 14 Holder		ABB	Card reader	8458	White
Tasca C024	Konnex Falcon .NET	KIX	1.1.28	1/3/24 ACC 1 Holder C024	1/4/24 ACC 14 Holder		ABB	Card reader	8458	White
Tasca C025	Konnex Falcon .NET	KIX	1.1.32	1/3/25 ACC 1 Holder C025	1/4/25 ACC 14 Holder		ABB	Card reader	8458	White
Termostato C021	Konnex Falcon .NET	KIX	1.1.17					Unknown device	0	

Figure 41 – Devices list

7.9.2 Configuration

The configuration section allows you to configure the following information:

- Ping enabled: in case of ping enabled a ping is sent to the device with an interval equal to the delay configured in the column "Ping delay";
- Ping delay: allows you to configure the interval with which the ping is sent to the device (if ping is enabled);
- Notification address: allows you to define a notification address; every time the accessManager detects a change on the device (for example an access attempt) the notification address is written to 1 (immediately) and then to 0 (with a delay of two seconds). The notification address can only be a one-bit address given its use.

7.9.3 Guest access actions

The *Guest access actions* section allows you to configure a list of commands or scenarios to be executed in case the access manager detects an access attempt on a device through a guest card.

The configuration is only possible for devices belonging to the Readers or Holder families.

The enabling flag allows to enable the actual execution of commands and scenarios.

For readers it is possible to configure a list of commands or a single scenario in cases where:

- The card is passed in front of the reader and access is allowed (columns "Valid access controls (reader)" and "Valid access scenario (reader)");
- The card has been passed in front of the reader and access is denied ("Access denied (reader) controls" and "Access denied (reader) scenario" columns).

For holders you can configure a list of commands or a single scenario in case:

- The card is inserted in the holder and access is allowed (columns "Card commands inserted valid access" and "Card Scenario inserted valid access");
- The card is inserted in the holder and access is denied (columns "Card commands inserted access denied" and "Card scenario inserted access denied").
- The card is removed from the holder ("Card commands removed" and "Card scenario removed" columns).

The actions are performed only if the device is configured in spontaneous emission and not in polling.

7.9.4 Other access actions

The *Other access actions section* allows the same configuration as the *Guest access actions section* for non-guest cards.

7.9.5 Guest access notifications

The *Guest Access Notifications section* allows you to configure a list of notifications to be executed in case the access manager detects an access attempt on a device through a guest card.

The configuration is only possible for devices belonging to the Readers or Pockets families.

Enabling notifications follows the action enabling for the selected device defined in the *Guest access actions section*.

Notifications are configured in the *Configuration->Notifications section*, and are associated to the device in this section.

A list of notifications can be configured for readers:

- The card has been passed in front of the reader and access is allowed ("Valid access notification (reader)" column).
- The card is passed in front of the reader and access is denied (column "Notify access denied (reader)")

For holders you can configure a list in case:

- The card is inserted in the holder and access is denied (column "Card notification inserted valid access").
- The card is inserted in the holder and access is denied (column "Card notification inserted access denied").
- The card is removed from the holder ("Notification card removed" column)

Notifications are performed only when the device is configured for spontaneous emission and not polling.

If the configured notification is popup type, a popup containing the data of the customer/staff that attempted to access is created when the notification is configured (see section *Configuring notifications*).

7.9.6 Other access notifications

The *Other Access Notifications* section allows the same configuration as the *Guest Access Notifications* section for non-guest cards.

7.10 Date, time, plant code

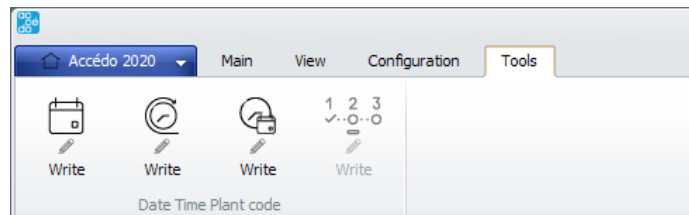


Figure 42 – date, time toolbar

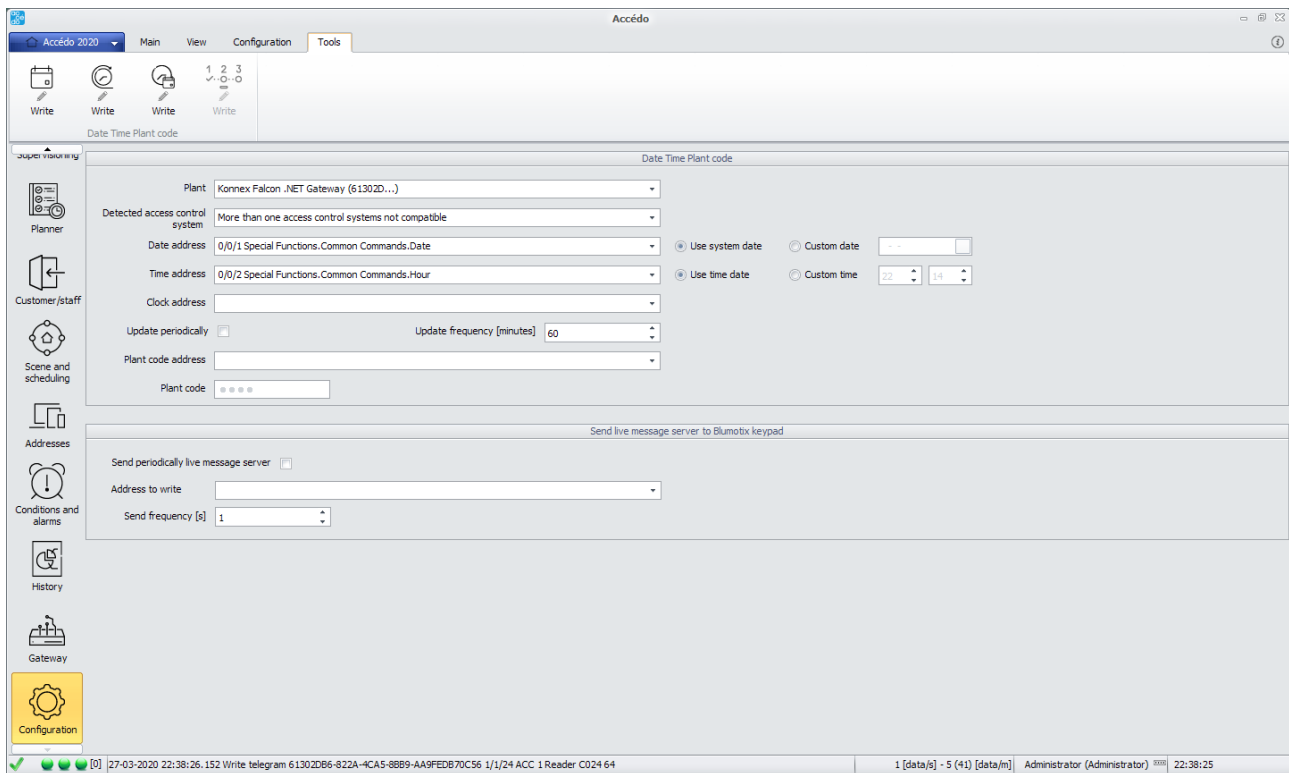


Figure 43 - configurations available for date and time of installation

7.11 Smart-cards programmers

This section defines the card programmers in use in the system, in particular those programmers that are to be used with the following access control systems:

- KNX ekinex

For these programmers, simply enable the *Programmer* flag in the specific ekinex configuration, without making further configurations in the card programmers section.

7.12 ekinex access control

In this section the specific configuration of ekinex access control devices is performed. The configuration is divided into 4 tabs:

- Devices
- Plant codes
- Time strips groups
- Time strips

7.12.1 Time strips

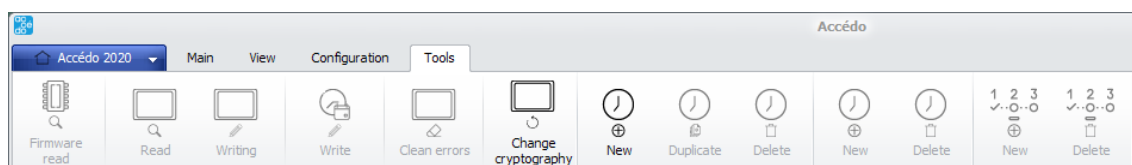


Figure 44 – Time strips toolbar

Time strips allow the definition of time periods to be combined later in the *Time strips groups* for the definition of periods in which access to ekinex devices is allowed or not.

Each time strip provides for the definition of:

- Name
- *All days* option
- *Start day* option
- *Start time* option
- *End day* option
- *End time* option
- Time strip type (positive or negative)

If the "All days" option is activated, only the values of "Start time" and "End time" should be considered. What you get, assuming you set a positive range that has 6:00 as start time and 14:00 as end time, is such a situation:

	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY	SUNDAY
00.00 – 01.00							
01.00 – 02.00							
02.00 – 03.00							
03.00 – 04.00							
04.00 – 05.00							
05.00 – 06.00							
06.00 – 07.00							
07.00 – 08.00							
08.00 – 09.00							
09.00 – 10.00							
10.00 – 11.00							
11.00 – 12.00							
12.00 – 13.00							
13.00 – 14.00							
14.00 – 15.00							
15.00 – 16.00							
16.00 – 17.00							
17.00 – 18.00							
18.00 – 19.00							
19.00 – 20.00							
20.00 – 21.00							
21.00 – 22.00							
22.00 – 23.00							
23.00 – 00.00							

You get a band, positive, i.e. granting access, which covers every day of the week from 6:00 to 14:00.

If, on the other hand, you define a band, positive, which starts on Monday at 6:00 and ends on Friday at 14:00, the result is this:

	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY	SUNDAY
00.00 – 01.00							
01.00 – 02.00							
02.00 – 03.00							
03.00 – 04.00							
04.00 – 05.00							
05.00 – 06.00							
06.00 – 07.00							
07.00 – 08.00							
08.00 – 09.00							
09.00 – 10.00							
10.00 – 11.00							
11.00 – 12.00							
12.00 – 13.00							
13.00 – 14.00							
14.00 – 15.00							
15.00 – 16.00							
16.00 – 17.00							
17.00 – 18.00							
18.00 – 19.00							
19.00 – 20.00							
20.00 – 21.00							
21.00 – 22.00							
22.00 – 23.00							
23.00 – 00.00							

What you get is no longer a period that crosses the days of the week, but a time period that actually starts on Monday at 6:00 a.m. and ends on Friday at 2:00 p.m. In order to create again a time band that includes the hours between 6:00 and 14:00, from Monday to Friday, you need to combine this positive time band with 2 other negative time bands.

The negative bands will have to be defined:

- All days, from 00:00 to 6:00
- All days, from 14:00 to 00:00

Combining the 3 bands the result is as follows:

	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY	SUNDAY
00.00 – 01.00							
01.00 – 02.00							
02.00 – 03.00							
03.00 – 04.00							
04.00 – 05.00							
05.00 – 06.00							
06.00 – 07.00							
07.00 – 08.00							
08.00 – 09.00							
09.00 – 10.00							
10.00 – 11.00							
11.00 – 12.00							
12.00 – 13.00							
13.00 – 14.00							
14.00 – 15.00							
15.00 – 16.00							
16.00 – 17.00							
17.00 – 18.00							
18.00 – 19.00							
19.00 – 20.00							
20.00 – 21.00							
21.00 – 22.00							
22.00 – 23.00							
23.00 – 00.00							

The devices combine the time slots that are downloaded into their memory and allow access only during the period indicated in green. The devices' algorithm provides that the result (the access period) is obtained as the OR function of the positive time bands and AND of the negative time bands.

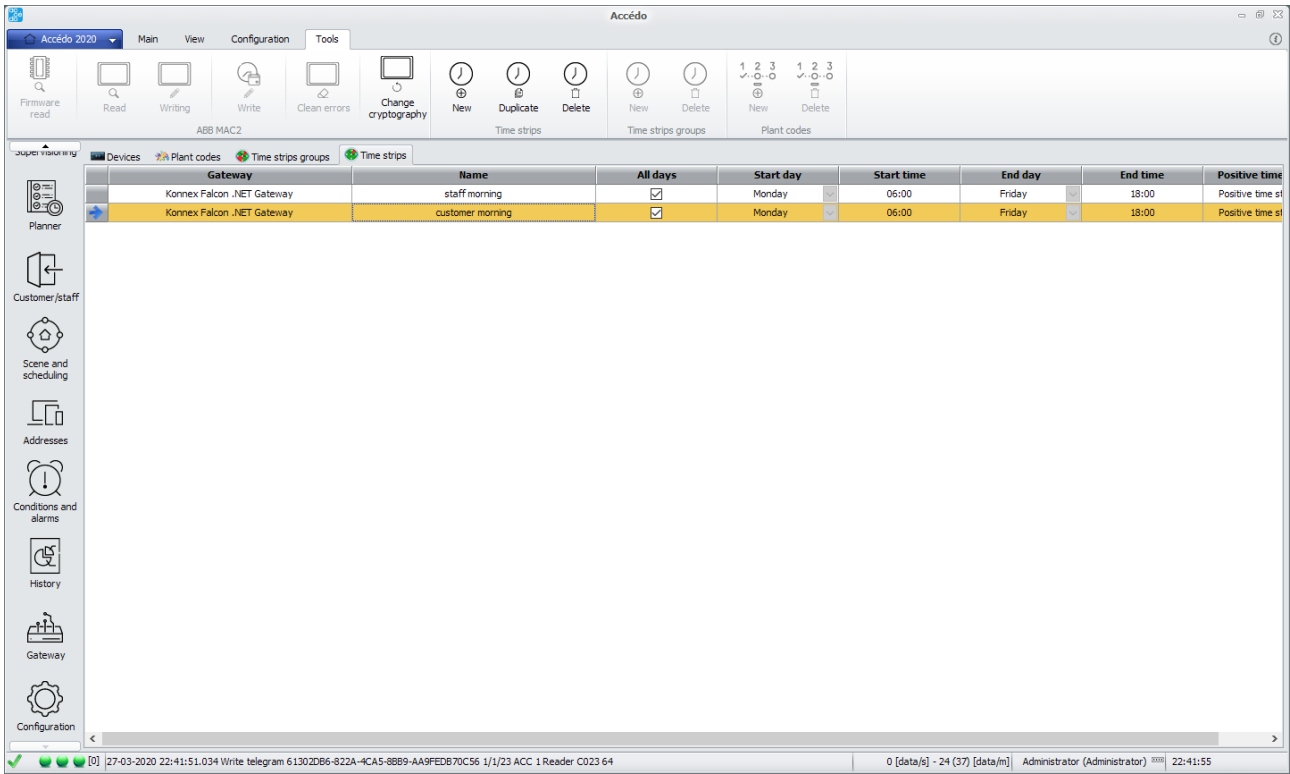


Figure 45 – Time strips list

7.12.2 Time strips groups

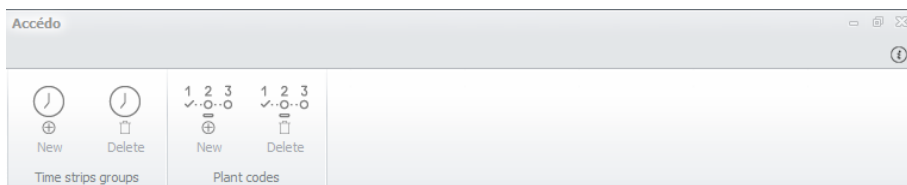


Figure 46 – Time strips group toolbar

A time strips group allows you to tie several time slots together to achieve the desired result. Each group also has a type; when creating cards, a Customer type card can only be associated to groups of Customer type bands, while a Service type card can only be associated to groups of Service type bands.

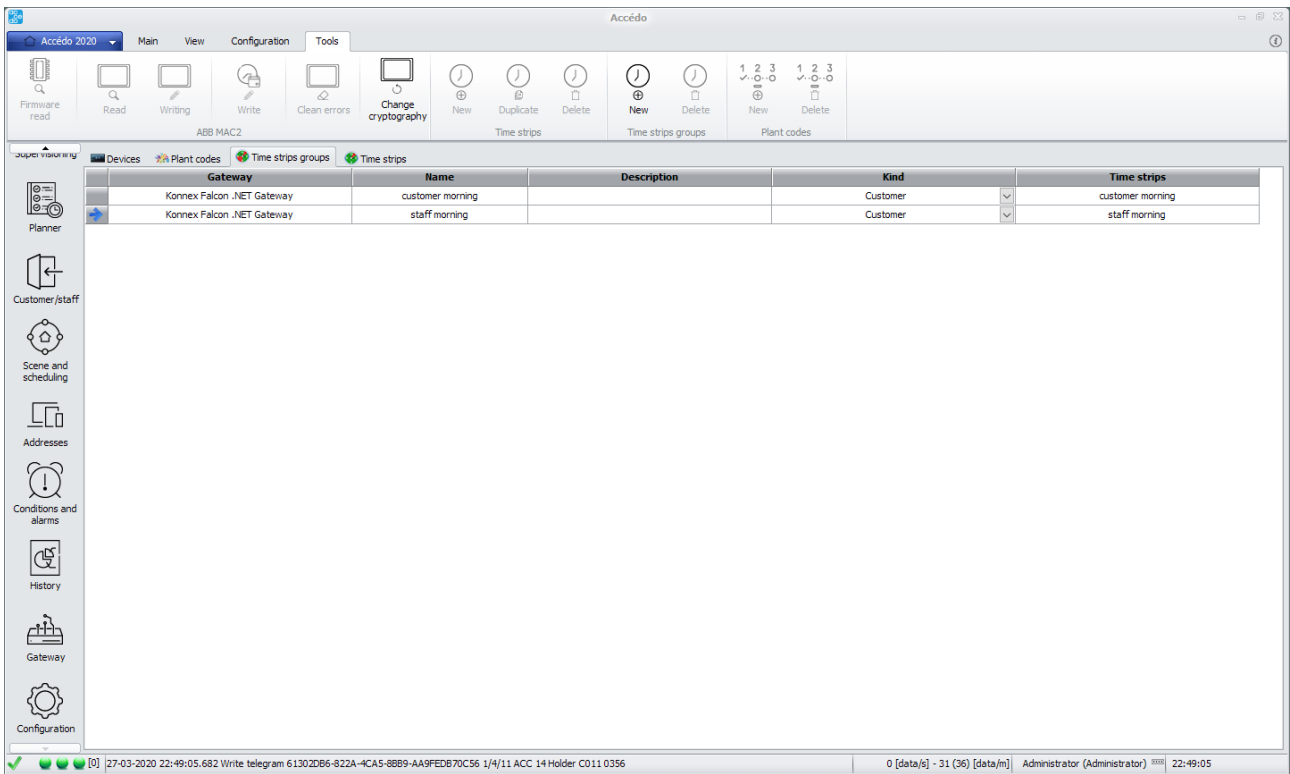


Figure 47 – Time strips group list

7.12.3 Plant codes

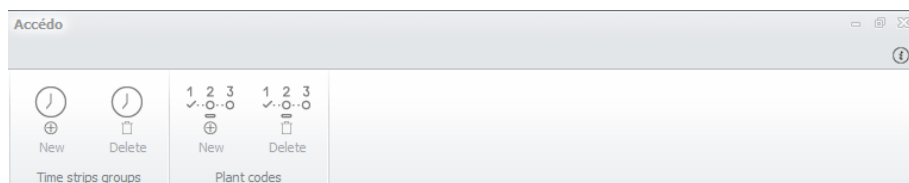


Figure 48 – Plant codes toolbar

Multiple system codes can be associated with each ekinex device. Only one implant code can be associated with each card. For the card to have access to that device, it is essential that the plant code written on the card matches one of the plant codes downloaded to the device memory. The possibility of having several system codes allows, in addition to ensuring that cards from one structure cannot access another structure, to divide the cards into categories. For example, customers, maintenance, rescue, security personnel, service personnel, etc.. If this subdivision is implemented, it is very quick to disable access, for example for security reasons, to a certain category of card/plant code: simply remove that plant code from all devices.

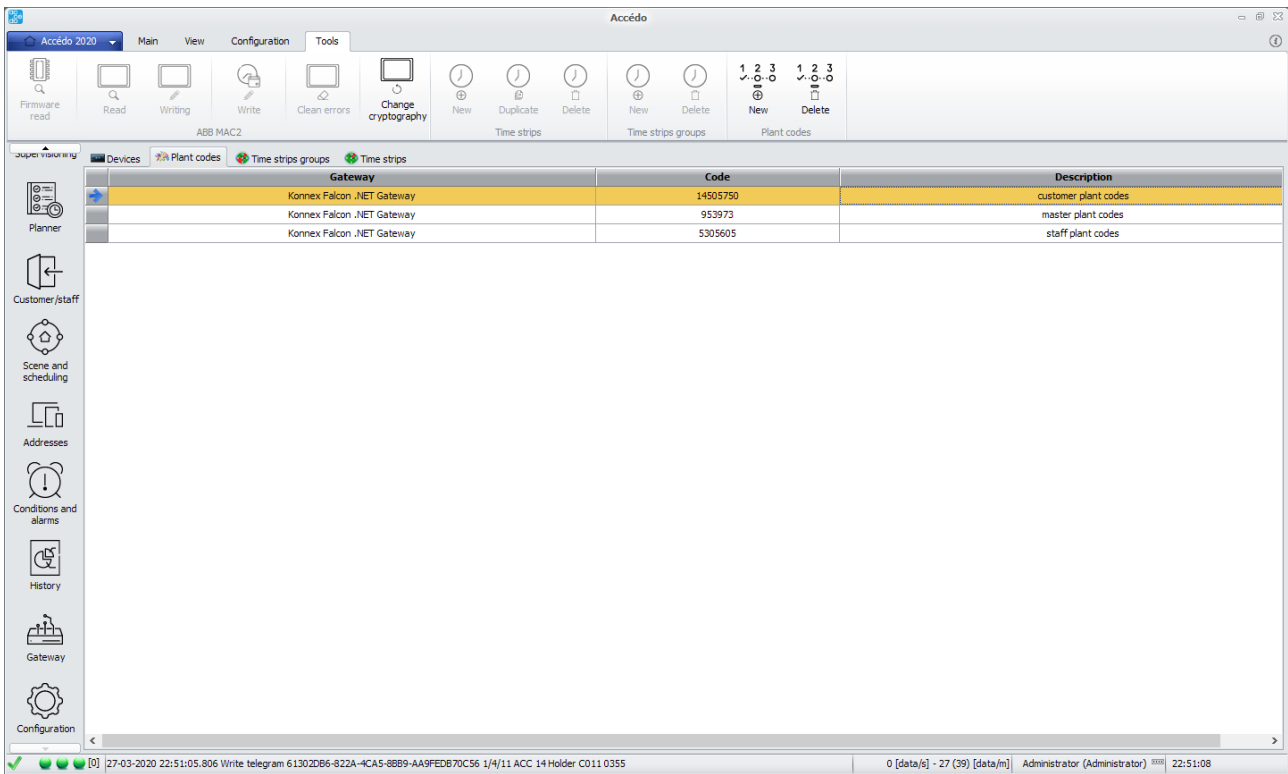


Figure 49 – Plant codes list

7.12.4 Devices

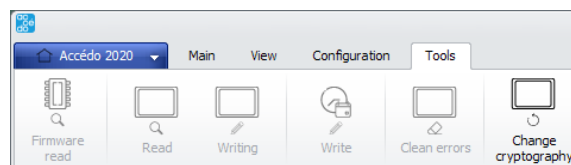


Figure 50 – Access control devices toolbar

This configuration menu is certainly the most important in the ekinex access control section. Before starting with the actual configuration you must select the devices recognized by the ETS import procedure and proceed to read the firmware.

Once the firmware is read, the software is able to recognize exactly the type of device it is dealing with and consequently enable or disable or set as default some parameters:

- Enable PBI: Pocket operation enabled; available and enabled by default for badge pocket type devices
- Programmer: enables operation as a card programmer; only available and enableable at the user's discretion for reader-type devices with programmer functionality.

The other possible settings for each device are:

- Enable MAC: if disabled the device will not read any card and will not perform any of the operations defined through ETS programming. Normally it should be left active!

- Tariff 1, 2, 3 and 4: tariffs that are deducted from the credit on the card in case you use a POS type device with prepaid cards.
- Programmer: allows you to select which devices will be used as card programmers
- Enable time bands: enables time band management; if activated, the device will grant access only during the allowed periods according to the time bands that have been downloaded into its memory. If you want to always give access (24/24, 7/7) the simplest solution is to disable the time bands. Another solution could be to enable time zone control and define an always valid time zone ("Every day", from 00:00 to 00:00).
- Enable handshake: enables the memory of transits within MACs. In this way you are guaranteed not to lose transits in the access history stored by the software as the device keeps in its memory the transit data until it receives confirmation from the software that these data have been stored.
- Plant codes: allows the association between the plant codes defined in the appropriate tab and the device.
- Time slot groups: allows the association between the time slot groups defined in the tab and the device.

Gateway	Physical address	Description	Kind (from database)	Kind (from firmware)	Kind	Enable MAC	Enable PBI	Enable POS	Rate 1	Rate 2	Rate 3	Rate 4	Prog.	Enable time	Enable hand	Plant codes	Time strips groups	Notify method	Access strategy
Konnex	1.1.1	EK-TR2/TP2-TP -	Card reader	READ FIRMWARE!	EK-TR2-TP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0,00	0,00	0,00	0,00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	No plant code	No time strips group	Spontaneous	White list
Konnex	1.1.2	EK-TR2/TP2-TP -	Card reader	READ FIRMWARE!	EK-TR2-TP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0,00	0,00	0,00	0,00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	No plant code	No time strips group	Spontaneous	White list
Konnex	1.1.3	EK-TH2-TP - tasca	Card holder	READ FIRMWARE!	EK-TH2-TP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0,00	0,00	0,00	0,00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	No plant code	No time strips group	Spontaneous	White list

Figure 51 – Access control device list

- Notification method: allows the choice between the 2 notification methods available for MACs: spontaneous release or polling.
- Access strategy: allows the choice between the 4 access strategies available for MACs: white list, black list, no list, centralized.

7.12.5 Reading and writing

Once the parameterization of the ekinex devices is finished (which can be done very quickly by selecting all the rows of the table and applying the same parameters to all the devices), the defined parameterization must be written. This operation is done through the "Write" button. Also in this case the writing can be done on several devices in sequence, with the appropriate multi-selection on the grid.

Writing starts a dialogue with the device which consists in sending all the parameter setting information (enable, plant codes, time band groups, time bands, notification method and access strategy). In addition to this information, the device is also requested to delete all the card codes in its memory and then proceed with their rewriting. Then, following a write, we have the guarantee that the device is absolutely aligned with the configuration set by the software. This operation must usually be done only once during the start-up phase of the structure, but nothing prevents us from repeating it even afterwards because, as written, it does nothing to align the device with the software. It can be very useful in case of replacement of a device; after the reprogramming of the product with ETS, the writing procedure aligns the new device for the correct functioning and recognition of the cards.

The Error Cleaner button is used to clean the error register inside the device: the cleaning procedure is performed either while writing the device or by pressing the appropriate button.

7.13 BLUMOTIX keypads

Blumotix KNX standard keypads can be configured in the configuration section, through the two available sections:

- General
- Codes

7.13.1 General Informations

In the general section you can view the following device information:

- Gateway
- Physical address
- Description
- Memory size: maximum number of codes that can be stored on the keypad
- Number of codes in memory: number of codes currently stored in the keypad
- Live message server alarm: An alarm sent from the keypad to indicate that the keypad is not connected to the server; the alarm is reported when the keypad does not receive a Live message controller from the server for 255 seconds.
- Date and time last live message sent: The keypad periodically sends a bit to signal its operation; in this column you can see the date and time of the last live message sent.
- Date and time last keypad ID sent: the keypad periodically sends its ID to update the server information; in this column you can see the date and time of the last ID sent.
- Last keypad ID sent: The keypad periodically sends its ID, to update the server information; in this column you can see the last ID sent.
- Last button pressed: information about the last button pressed on the keypad; on 12-key keypads the '#' and '*' keys are not separated.
- Backlight status: keypad backlight status; the information is only present from version 3 of the keypads.
- Buzzer status: status of the keypad buzzer (the sound emitted when a key is pressed); the information is present only from version 3 of the keypads.

Each time the grid is loaded, the information shown is partly from the last reading made on the keypad (memory size, number of codes in memory, live message server alarm, backlight status and buzzer status), partly from the last value recorded on the corresponding address (date and time last live message sent, date and time last keypad ID sent, last keypad ID sent, last button pressed).

The information of a keypad can be completely updated through the Read button in the Tools menu (after selecting the line to read).

7.13.2 Codes

In the Codes section you can view the card codes stored on the device.

When the grid is loaded, the only information shown is the number of cards stored on the device: the information dates back to the last reading made on the device. To update this information and see the list of card codes currently present on the selected keypad you can press the Read codes button.

To update the list of codes stored on a particular keypad you can press the Write button, which, given the device and its associated environments, determines the cards that can be accessed by the keypad and writes the codes to the device memory. The card codes previously stored on the keypad are removed.

7.13.3 Tools

The tools menu allows the following functions:

- Reading: updates the information in the general grid by reading the data from the keypad.
- Reading codes: updates the information in the code grid by reading the data from the keypad. Writing: downloads the codes with access allowed on the keypad according to the information configured in the accesses;
- Add code: adds a user-defined code to the code list in the keypad memory;
- Remove Code: Remove a user-defined code from the code list in the keypad memory;
- Send server message: allows you to send a message from the server to the keypad to inform it that the server is still connected and active; the message must be sent periodically, because if it is not sent for 255 consecutive seconds the keypad raises the Live controller alarm through the associated group address, detecting the failure to connect to the server.

7.13.4 Periodic sending of the “live server” message

It is possible to configure the periodic sending of the *Live controller message*, to prevent the keypad from activating the relevant alarm.

The configuration is performed in the configuration section *Date time System code*, in the section *Send live message* server to blumotix keypads.

The configuration allows you to enable periodic sending, define the address to write (you can choose between those found that correspond to sending the Live controller message) and the frequency, in seconds, of sending the information.

7.13.5 Full keypad memory alarm

If necessary, logic can be configured to warn the user that the keypad has almost full memory.

To do so, the logic must be based on "*Codes number request*" addresses, which must be set to 1, while "*codes number reply*" contains the number of codes on board the keypad.

7.13.6 Filters

The two grids can be filtered through the filter section on the basis of the following fields:

- Description
- Physical address
- Code: For the code filter to work correctly, you must read the codes of all keypads at least once.

7.14 Payment profiles

Through this screen you can define the tariffs to be applied to particular addresses used as counters. In addition to the description you can define a unit cost and up to 4 discount percentages that will be applied in the total cost calculation.

TOTAL COST = Quantity * Unit Cost * (100% - Discount1) * (100% - Discount2) * (100% - Discount3) * (100% - Discount4)

In order to correctly define the unit cost, it is necessary to correctly determine the unit of measurement with which the data is stored and then accounted for. For example, many KNX energy meters, while displaying a value expressed in kWh on their display, transmit the same data expressed in Wh on the bus.

7.15 Payment entity

Payment entities are similar to rooms. They can be existing rooms defined by KNX configuration or other gateway configurations, or they can be rooms created ad-hoc.

Once the room has been selected, it must be related to the counters (addresses) that have been defined as counters. Two types of counters are available:

- progressive: their value saved in the database is an increasing number. To determine the consumption in a given period A-B is calculated the difference between the value saved on day B and the value saved on day A. E.g. electricity or heat meters
- pulse: usually their value, in numerical form, is "1" (this value can be translated logically as "on", "switch on", "valid access", etc.) To determine the consumption in a given A-B period, the sum of the values stored in the database from day A to day B is calculated. E.g. meters for access to paid rooms, meters for the use of paid facilities (e.g. showers), etc.).

For each counter/address, for a given environment, it is defined:

- a description
- a payment profile: in this way it is possible that the same type of service (e.g. electricity) is charged at full price to particular categories of users, while a discount is applied to others.
- a value in thousandths (with the possibility to use also decimal digits): in the formula.

8 VARIABLES

8.1 User variables

accédo allows the definition of variables.

The variables are designed to be used as "support" memories for information that must be able to be exchanged between accédo clients, including the BIGOmnia service. Variables are identified because they have a particular GUID value (11111111-1111-1111-11111111"). They can be read and written as normal addresses. In case of writing the Master Gateway receives the information and turns it over to all connected clients; in case of reading it is the Master Gateway that answers with the last known value.

Except for these differences, the variables can be configured exactly like the addresses and in the same way they can be used to create supervisions, define logics and alarms, etc.

The variables are loaded when the software is started and appear in a special section in the address tree. There is no user definable node organization. The software generates at runtime a structure to organize the variables, based on the name of the variables themselves.

User variables can be created from different sections of the software:

- In the *Tools* of the address configuration section through the *Add Variable button*;

accédo permette la definizione di variabili.

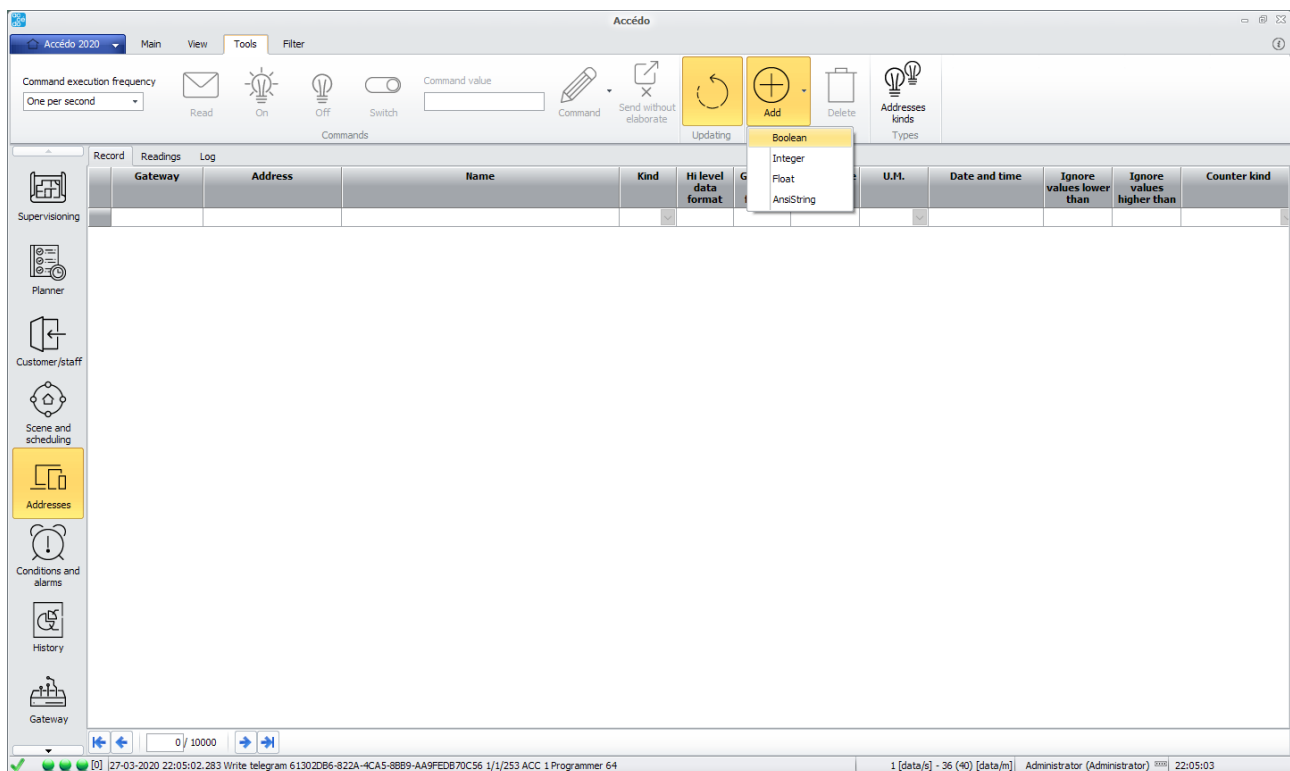


Figure 52 – Add new variables toolbar

- Right-click on the Variables node in the address tree and select the *Add Variable item*;
- The address selection panel can be opened in several places by clicking on the *Add variable button*;

To create a new variable you must always indicate its type (*Boolean, Integer, Float or String*) and name.

8.2 Gateway variables

Each gateway is able to process (i.e. read and write) its own addresses (encoding them before writing to the controlled bus/device and decoding them after reading from the controlled bus/device, if necessary). In addition to these addresses (in the case of KNX the classic 2 or 3-level addresses of type x/y or x/y/z) each gateway defines its own variables, used to process particular data or accessories. These variables have as GUID the gateway GUID; in this way the read and write commands (if possible) of variables of a gateway will not be managed by the Master Gateway, but by the specific gateway with that GUID.

These variables are defined by the gateway itself (and loaded into the database) or are defined by BIGStudio in particular situations.

For example, in the management of KNX emergency lamps (either native Gewiss lamps or DALI lamps managed through KNX/DALI gateways), there are KNX addresses (1, 2 or 4 bytes) that carry coded data. To make the individual information contained in these bytes available, accédo defines variables following the definition of a lamp or following its automatic recognition during ETS import. These variables have as already written GUID equal to the gateway GUID and therefore, in order to correctly discriminate them as variables and not as addresses, a special database field is used (ADDRESSES table, ISVARIABLE field). If it is necessary to group these variables, a special node is generated to contain them. Also in this case, to discriminate a node that contains addresses, a special database field (TREENODES table, ISVARIABLE field) is used from a node that contains variables.

9 LIFT/CABINET MANAGEMENT

9.1 Management with PLC and ekinex access control system

- Perform normal ETS import
- In KNX configuration define Custom environments that will correspond to the doors to be opened (lift floors or lockers).
- In "Rooms Configuration" go to define for each Custom room the value in the "Custom Setting" column. This is a value between 0 and 23, which basically indicates the bit that will be written with value "1" in the credit field of the EKINEX cards (this is a field of 3 bytes, therefore 24 bits total). Hence the limit to be able to access 24 floors of the building or open 1 (or more lockers) for a maximum of 24
- In KNX configuration define a new ekinex virtual device of the type "Virtual Device". E.g. "Elevator Reader".
- Drag the newly created "Elevator Reader" virtual device into any Custom environment
- Create ekinex cards normally and associate access permissions. Leave the cards set as "No POS". In this configuration the card credit field will be written taking into account the possible access to Custom environments and the value of the "Custom Setting" parameter.

E.g. Access permissions to PT plans ("Custom Setting" = 0), P1 (1), P2 (2) and P5 (5) -> Credit = byte 3: 0000 0000 byte 2: 0000 0000 byte 1: 0010 0111 = 39

If you change the access permission to one of the virtual environments once you have written the card, you need to rewrite the card; a reminder message is still shown on the screen!

The card written in this way is read by a card programmer, installed in the lift or locker room. This programmer must be configured in spontaneous emission mode, so that as soon as a card is placed in front of it, the ACC14 telegram with the card code is issued. The PLC connected to the KNX bus of the programmer captures this information and immediately sends the command for the complete reading of the card data, including credit. As soon as the credit is read, it will command appropriate relays on board PLC or KNX relays for enabling lift buttons or opening cabinets.

10 SUPERVISION

The "Supervision" module displays the pages to monitor and manage the rooms and, for example, the reports of the bathroom tie rods.

10.1 General informations

The "Home page" contains links to the subpages. To access the pages you are interested in, simply click on the appropriate link.

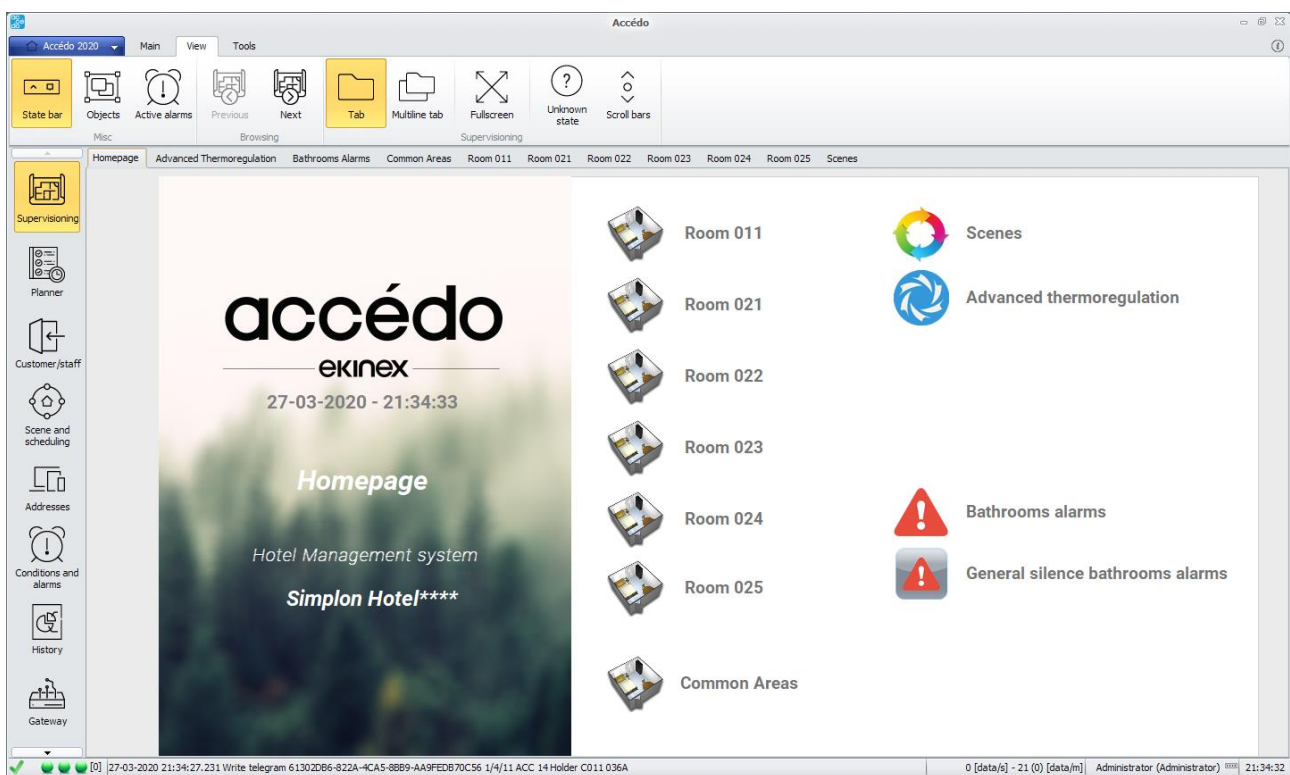


Figure 53 – Example of a supervision page

10.2 Supervision of a plant

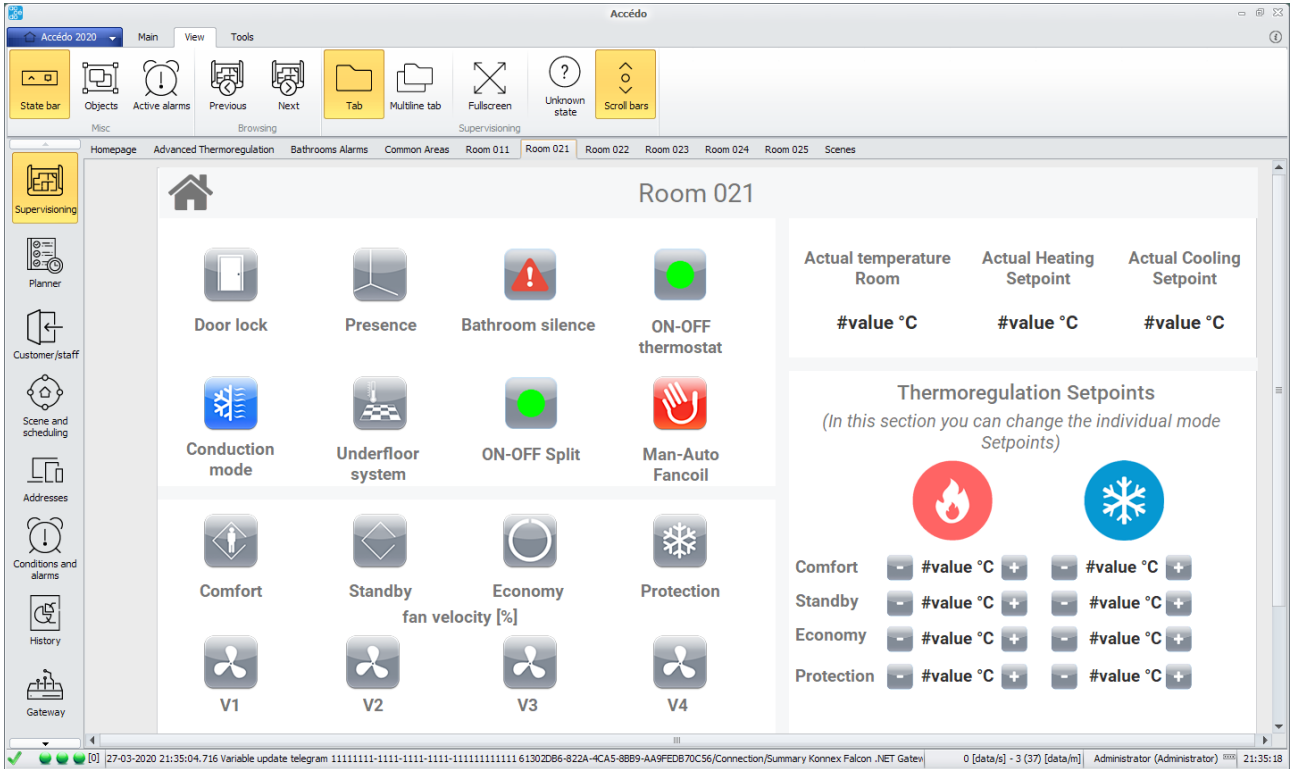


Figure 54 - example of supervisory synoptic for the rooms of an accommodation facility

For example, the following information can be displayed for each room in the accommodation:

- "Door opening" button: allows to activate the electric lock of the entrance door
- Camera energy button:
 - Black color: indicates camera energy not active
 - Red color: indicates active chamber energy
- "Do not disturb" button:
 - Black color: indicates do not disturb not active
 - Orange colour: indicates do not disturb active
- "Water alarm" button:
 - Black colour: indicates bathroom alarm not active
 - Red color: indicates bathroom alarm active
- "Message Camera" button:
 - Black color: indicates in camera message not active
 - Green color: indicates message in active room
- "Seasonal mode" button:
 - Red color: indicates that the heating is on.
 - Blue color: indicates that cooling is active
- "Comfort" button: by pressing it you can display/set the comfort mode of the thermostat.
 - Black colour: indicates comfort mode not active
 - Red color: indicates active comfort mode
- "Standby" button: Pressing it allows to display/set the thermostat standby mode.
 - Black color: indicates standby mode not active
 - Orange color: indicates active standby mode

- Economy" button: by pressing it you can display/set the economy mode of the thermostat.
 - Black color: indicates economy mode not active
 - Yellow color: indicates active economy mode
- Antifreeze" button: pressing it allows to display/set the antifreeze mode of the thermostat.
 - Black color: indicates antifreeze mode not active
 - Blue color: indicates active antifreeze mode
- Window" icon: indicates the status of the window contact
 - Black color: window closed
 - Blue color: window open
- Buttons - "+ / - comfort setpoint" icons: display/increase/decrease the value of the comfort mode setpoint.
Note if the temperatures are displayed with ??? and not numerical values, the system may have been restarted recently, wait a few minutes before operating. If the "?" remain, it is necessary to check the communication status with the system, the operating status of the thermostat, etc..
Buttons - Icons "+ / - standby setpoint": allow to display / increase / decrease the value of the standby mode setpoint.
Note if the temperatures are displayed with ??? and not numerical values, the system may have been restarted recently, wait a few minutes before operating. If the "?" remain, it is necessary to check the communication status with the system, the operating status of the thermostat, etc..
- Fancoil" icon: indicates the status of the fans.
 - Black color: active fans
 - Blue colour: fans not active

You can change the type of button according to the user's needs, through the images in the Icons folder inside the accédo folder. The user has the possibility to choose different sizes and colors of the images according to his preferences.

10.3 Create supervision pages

- To create a new supervision page you have to select the supervision section, then in the toolbar you have to select tools and then new:

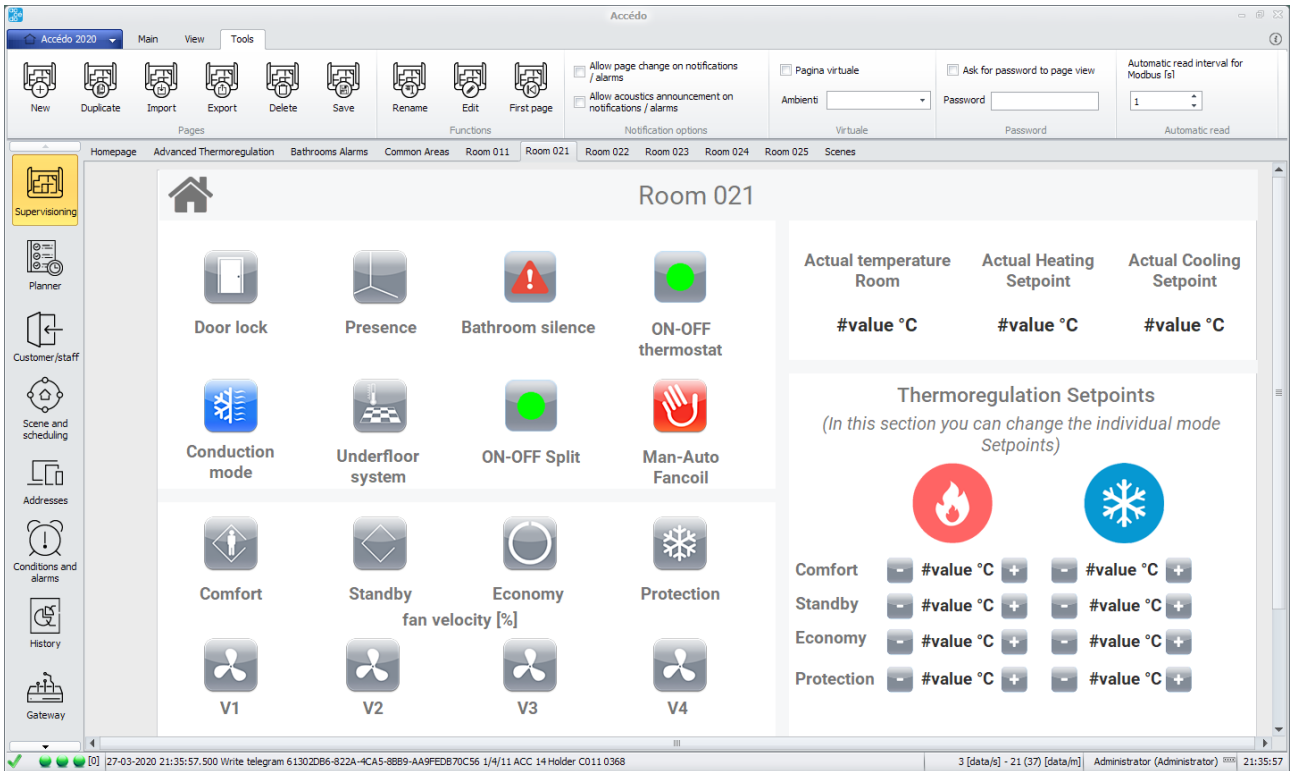


Figure 55 – supervision toolbar



Figure 56 - toolbar button for creating a supervision page

- Name the new page you created
- This page can be duplicated, others can be imported, exported and removed using multifunction bar at the top of page.

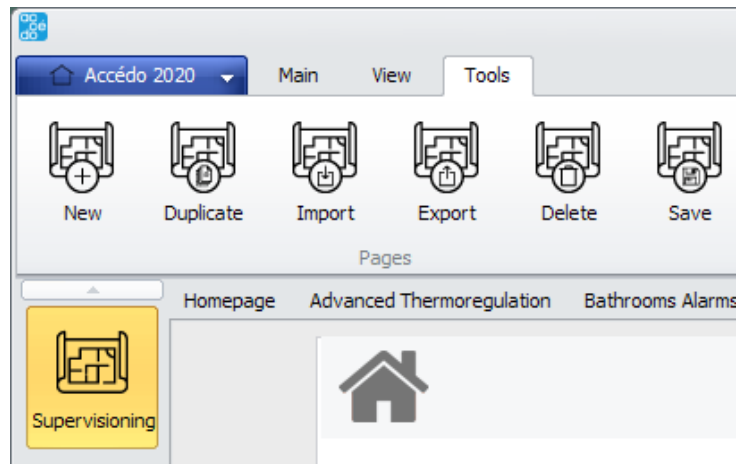


Figure 57 – Pages menu

- In the *functions* section it can be renamed or modified or can be set as the first page of supervision

10.4 Possible operations on supervisions

- Scrollbar activation: Associated with individual supervision; if a user activates scrollbars on supervision all users will see them.
- Unknown status activation: insert a red ? next to the objects to which an unknown address is assigned; the setting is saved in the settings (so it is valid for all supervisions) and divided by user.
- Duplication: the duplication also allows an automatic increase of addresses based on the address format and the type of modification you want to apply; the type of modification is defined through the appropriate form.

The form also allows you to choose how many pages to generate: if the number is greater than one you can also automatically define the name to give to the supervisions:

1. By a name consisting of a fixed root and a value that increases with each supervision and whose initial value can be defined.
2. Through an address (chosen among those present in the supervision) that satisfies the characteristic: it is associated to a device that is present in only one environment. Through this relation the associated room is identified and the supervision takes the name of that room.

10.5 Modify supervision pages

- If you click on edit in the Functions section, a new page is displayed where you can use a number of functions to make changes to the page

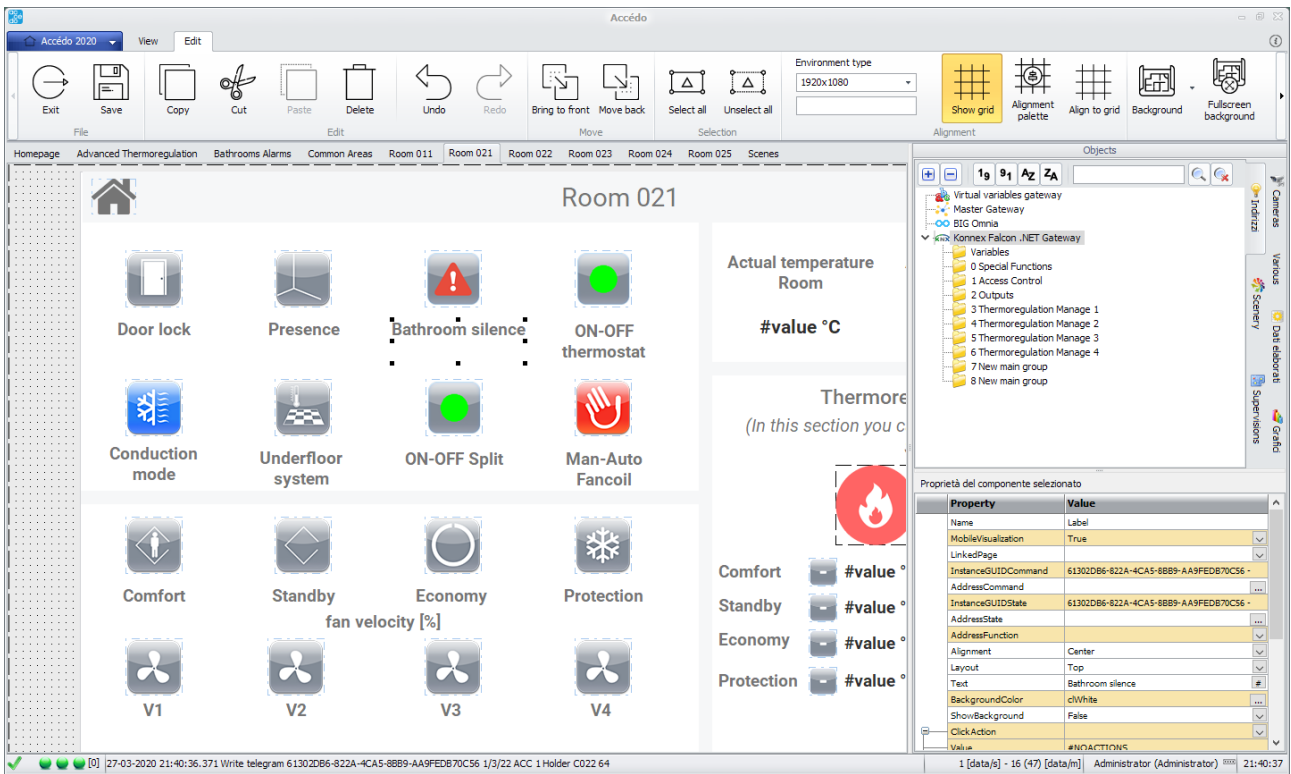


Figure 58 - Edit supervision page

- Through the Options section you can click on the Background button and change the background of the page loading it from your computer, or set.

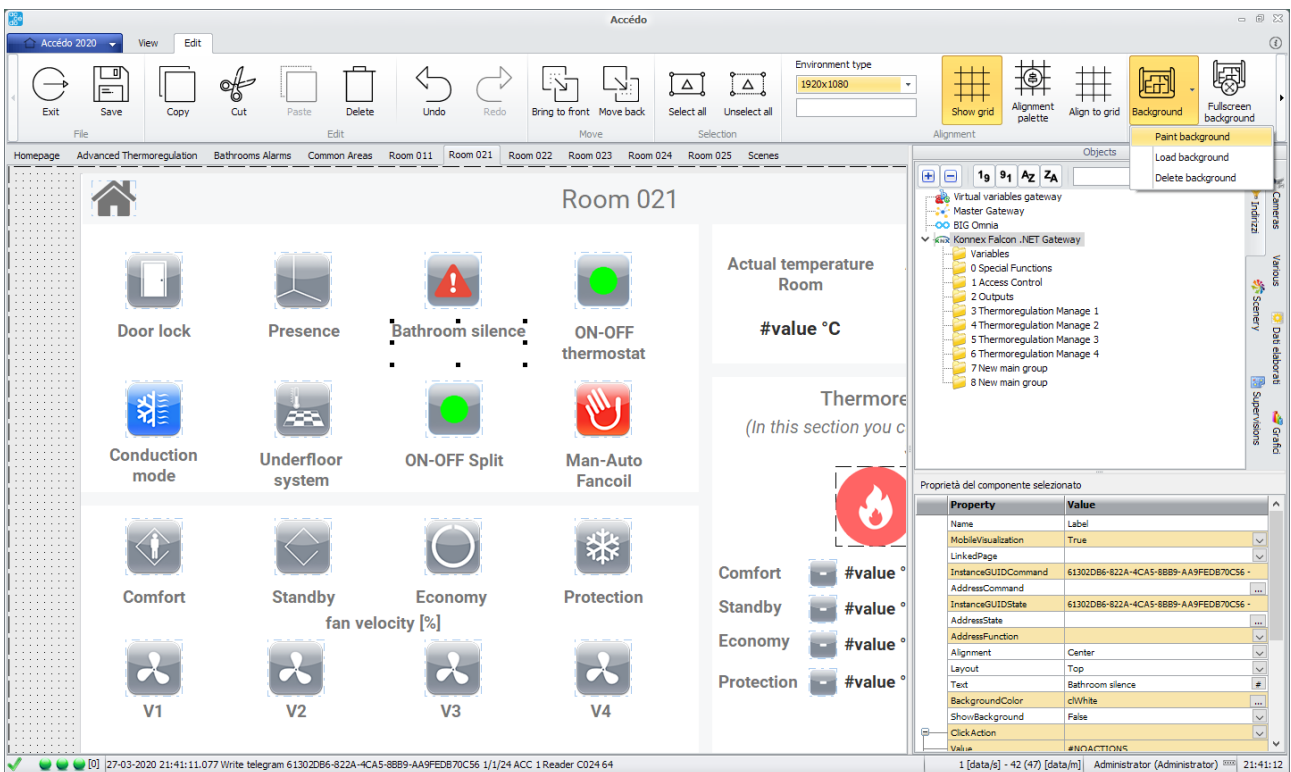


Figure 59 - background edit button

- The menu on the right hand side, on the other hand, allows you to transport several objects to the page

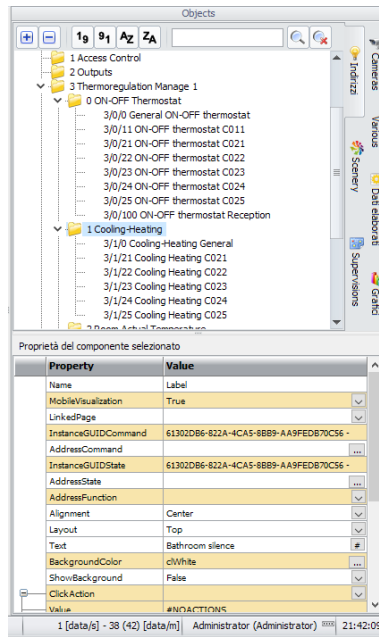


Figure 60 - objects menu

- When the objects are dragged, a pop-up menu is displayed that gives you the choice between a button or a label

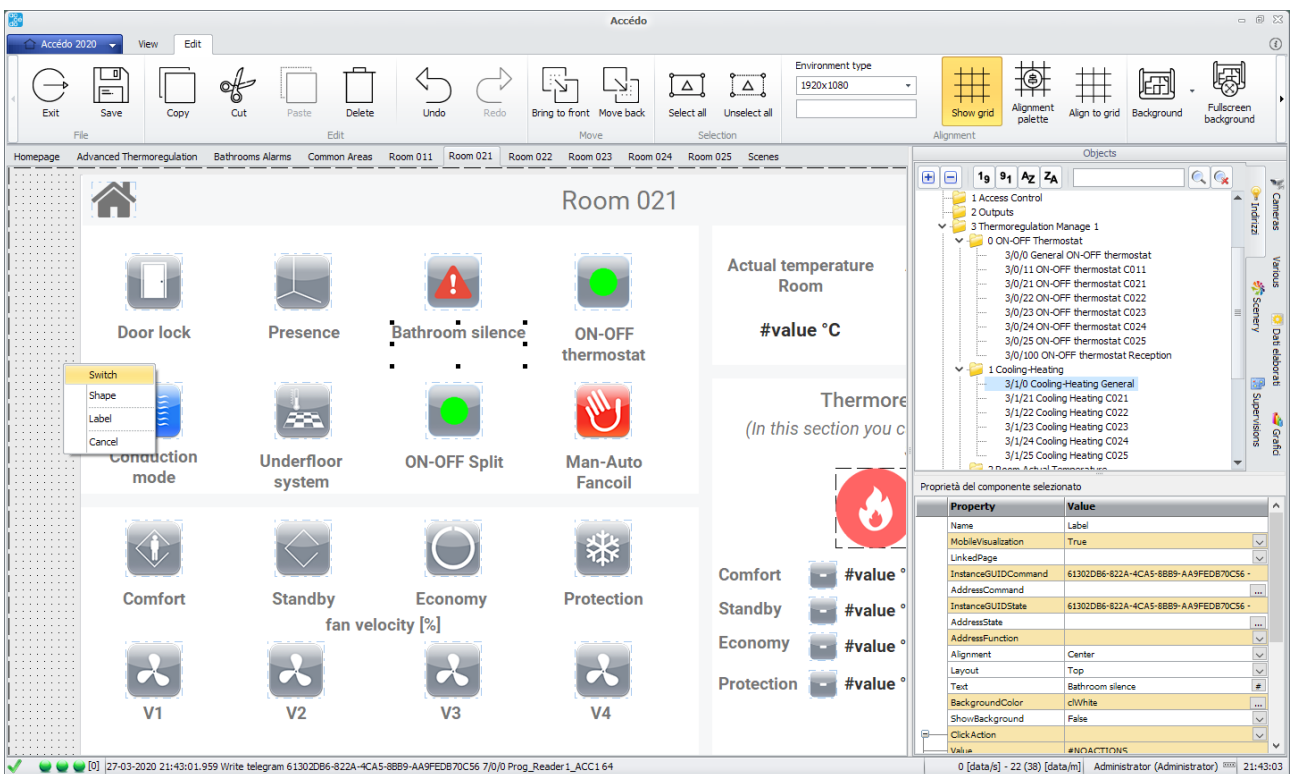


Figure 61 - detail creation of a supervision page

- After choosing the procedure to be performed, a new window is displayed

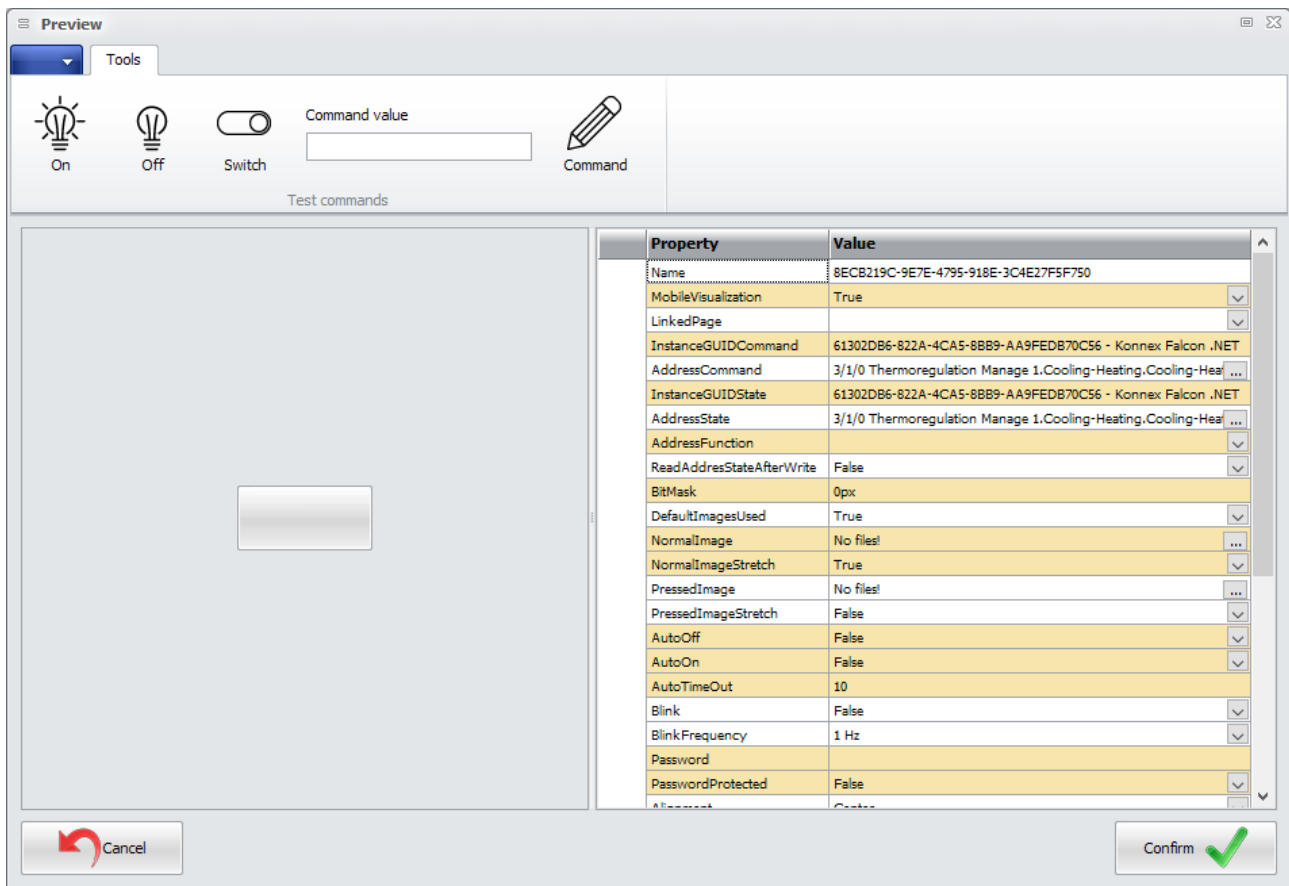


Figure 62 - Address properties

- This window can be used to create command buttons, functions and shapes as you wish, for example

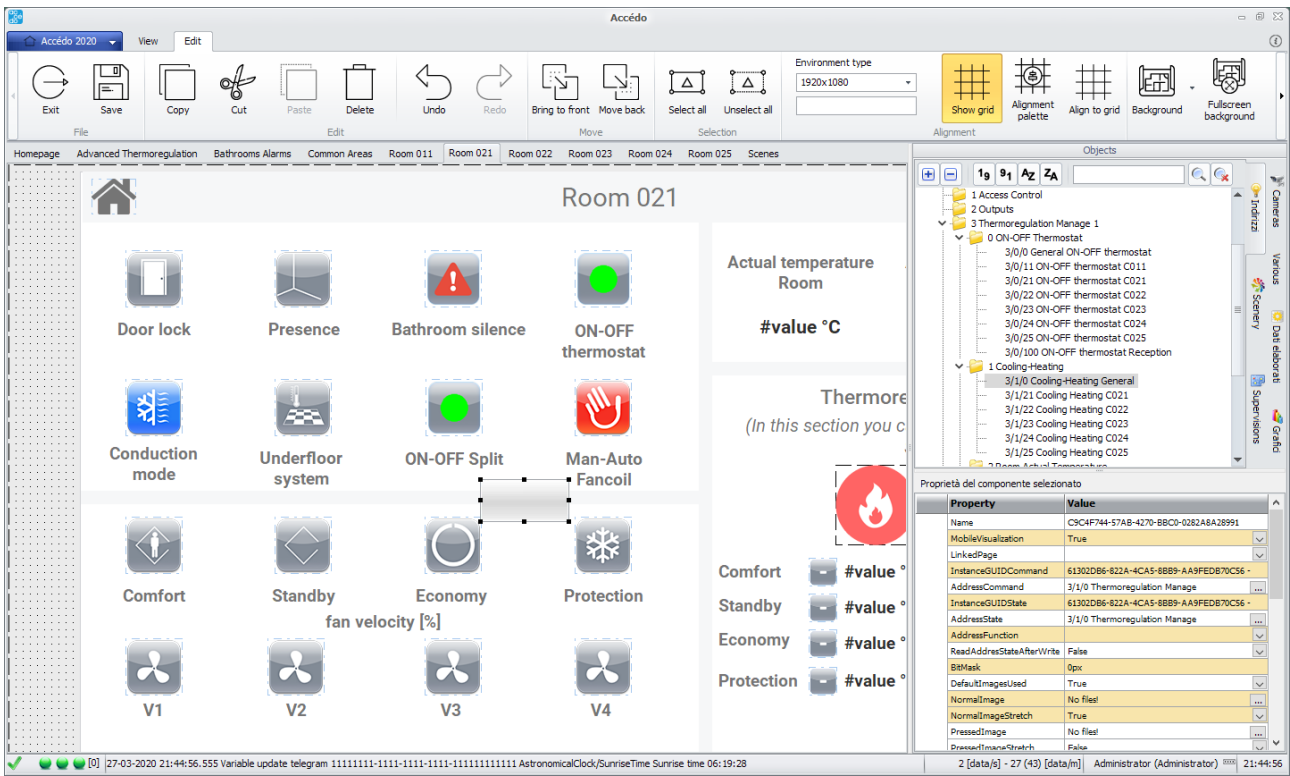


Figure 63 - detail creation of a supervision page

- The functions/properties that can be used are many:

Proprietà	Valore
Name	DFEE1EB1-A626-43E7-8E10-C2E04222C71C
InstanceGUIDCommand	EBF2C8DA-4ADD-4368-A954-2D3EE971D7FE - USB KNX Interface
AddressCommand	1/0/1 Contatti.Porte.Porta Nr 1 P.T. ...
InstanceGUIDState	EBF2C8DA-4ADD-4368-A954-2D3EE971D7FE - USB KNX Interface
AddressState	1/0/1 Contatti.Porte.Porta Nr 1 P.T. ...
NormalImage	Nessun file ...
NormalImageStretch	False ▼
PressedImage	Nessun file ...
PressedImageStretch	False ▼
AutoOff	False ▼
AutoOn	False ▼
AutoTimeOut	10
Blink	False ▼
BlinkFrequency	1 Hz ▼
CustomSkin	Nessun file ...
UseCustomSkin	False ▼
Password	****
PasswordProtected	False ▼
Text	#name
TextOnControl	False ▼
TextPosition	CenterBottom ▼
ClickAction	No action [#NOACTION] ▼
Value	#NOACTION
Font	Calibri,cBlack,14,Bold ...
GUIType	Drawing ▼
StateImages	+
Visible	True ▼
Height	48
Left	190
Top	248
Width	48

Figure 64 – Properties menu

- **AddressCommand:** you can filter the commands after clicking the button with the three dots and allows the selection of the necessary command.

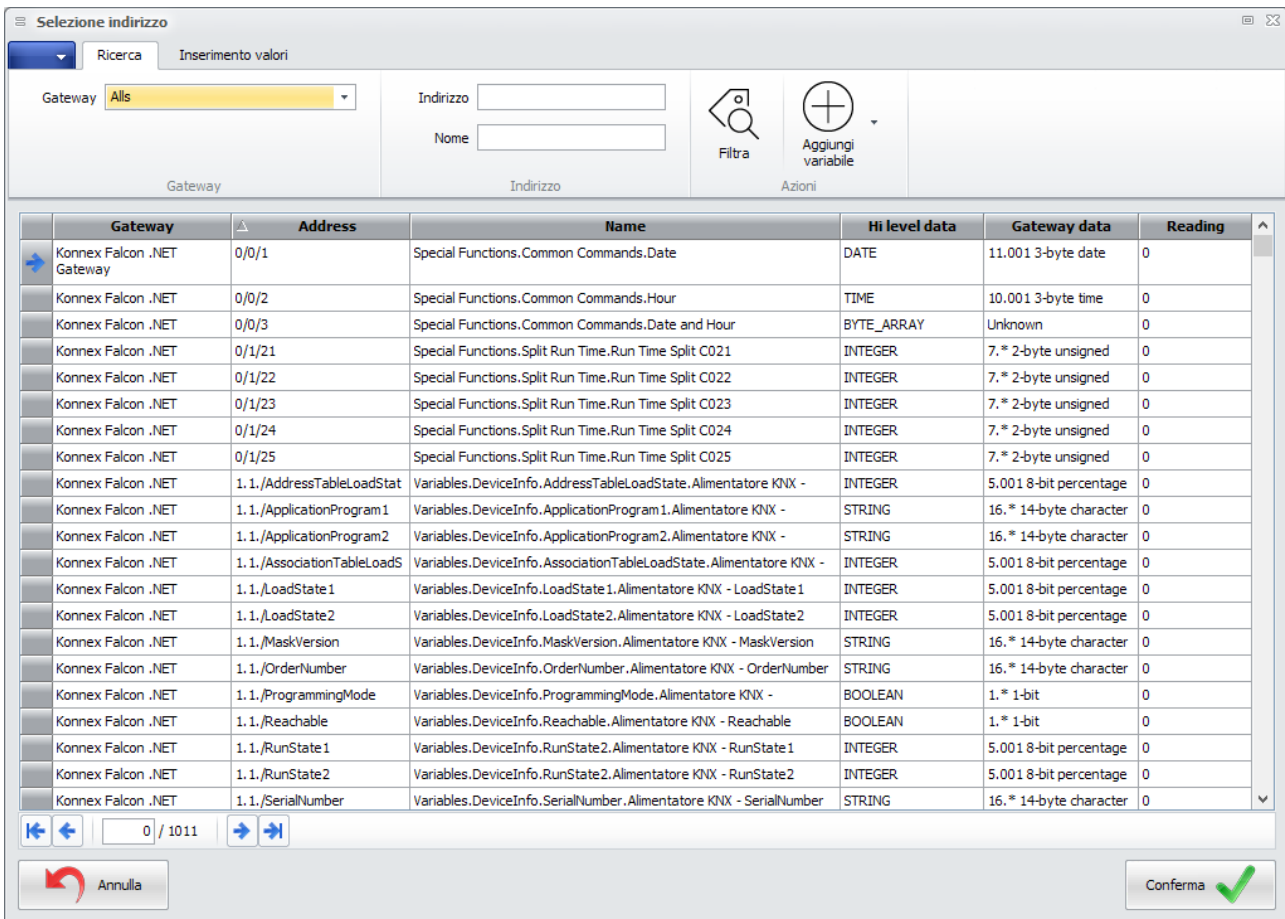


Figure 65 - Filter on the available address list

- **AddressState:** indicates the status of the group address
- **NormalImage:** allows you to choose an image for the selected button
- **NormalImageStretch:** Stretch makes sure that when the button is resized, the image adapts to the new size.
- **PressedImage:** allows you to choose the image that will be displayed when the button is pressed.
- **PressedImageStretch:** stretch ensures that the image adapts to the new dimensions when the button is resized
- **AutoOff:** allows the program startup to keep the selected object deactivated
- **AutoOn:** allows the start of the program to activate the selected object
- **Blink:** Allows you to choose whether to blink the object
- **BlinkFrequency:** allows you to set the frequency with which the object blinks
- **Password:** allows you to enter a password
- **PasswordProtected:** Boolean variable that allows you to select whether to protect your password or not
- **Text:** allows text input; you can use the following keywords to enter information related to the selected object:
 - KEYWORD ON GENERAL ADDRESS
 - **#value:** shows the value of the status address;
 - **#name:** shows the name of the status address;
 - **#fullname:** shows the full name of the status address, including the address hierarchy;
 - **#address:** shows the status address;

- **#hileveldataformat**: shows the format of the status address;
- **#formattedvalue**: shows the value of the state address formatted according to the type assigned to the address;
- **#techvalue**: shows the value as received by the bus;
- **#timestamp**: shows the timestamp of the last received value on the status address;
- **#roomnumber**: shows the number of the environment to which the status address is associated; this keyword should only be used if the address is associated with only one device located in one environment, so the value assigned by the keyword is unique. Otherwise the first relationship found with an environment (not always significant) is shown;
- **#roomname**: shows the name of the environment to which the status address is associated; the precautions to use for #roomnumber apply;
- KEYWORD ON DECIMAL ADDRESS
 - **#decimaldigitsN**: given an address with a decimal value defines the number of decimals (N) to be shown;
- KEYWORD ON LABEL (NOT LINKED TO A SPECIFIC ADDRESS)
 - **#clock**: shows the current time in the format hh:mm:ss
 - **#clockshort**: shows the current time in the format hh:mm:ss
 - **#hours**: shows the current time in format h
 - **#hours2digits**: shows the current time in hh format
 - **#minute**: shows the current time in the format m
 - **#minute2digits**: shows the current time in mm format
 - **#seconds**: shows the current time in the format s
 - **#seconds2digits**: shows the current time in ss format
 - **#date**: shows the current date in dd-mm-yyyy format
 - **#dateshort**: shows the current date in dd-mm format
 - **#day**: shows the current day in the format d
 - **#day2digits**: shows the current day in dd format
 - **#daynameshort**: shows the name of the current day in short format
 - **#dayname**: shows the name of the current day in long format
 - **#month**: shows the current month in the format m
 - **#month2digits**: shows the current month in mm format
 - **#monthnameshort**: shows the name of the current month in the short format
 - **#monthname**: shows the name of the current month in long format
 - **#year**: shows the current year in y format
 - **#year2digits**: shows the current year in y format
- KEYWORD ON ListPresence ADDRESS
 - **#cardnumber**: shows the list of card numbers within the room associated with the address separated by ',';
 - **#cardcode**: moves the list of card codes within the room associated with the address separated by ',';
 - **#Presencenamesurname**: shows the name and surname of the guest/staff present within the address room separated by ',';
 - **#Presencesurname**: shows the surname of the guest/staff present within the room associated with the address separated by ',';
- KEYWORD ON SCENARIO
 - **#name**: shows the name of the scenario;
- KEYWORD ON SUPERVISION
 - **#name**: shows the name of the supervision;
- KEYWORD ON GRAPHICS OR SERIES OF GRAPHICS
 - **#name**: show the name of the chart;

- **#description:** shows the description of the chart;
 - **TextOnControl:** Boolean variable for text control
 - **TextPosition:** allows you to choose where to place the text
 - **Click Action:**allows you to choose the action that is triggered when the button is pressed
 - **Value:**allows you to set the value that obtains the address when the button is pressed.
 - **Font:**allows you to choose the type of writing font
 - **GUIType:**
 - **StateImages:** allows you to insert different images depending on the state of the object
 - **Visible:** allows you to make the selected button or label visible
 - **Height:** allows you to change the height of the selected object
 - **Left:** allows you to increase or decrease the distance to the left margin of the selected object
 - **Top:** allows you to increase or decrease the distance from the top margin of the selected object
 - **Width:** allows you to change the width of the selected object
- At the bottom left on the status bar there are LEDs of different colors

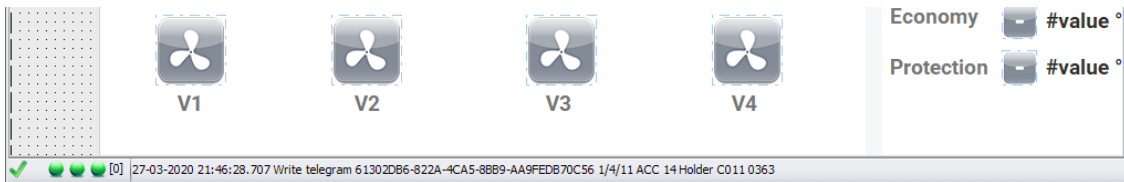


Figure 66 – status bar

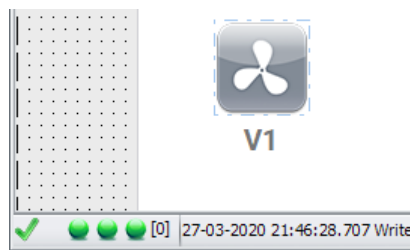


Figure 67 - telegrams on the bus

- **Green:** indicates that the connection is active
 - **Yellow:** indicates that he is connecting or attempting a connection
 - **Red:**indicates that the connection is not active
- By clicking on active alarms in the top menu, the list of active alarms appears at the bottom of the page

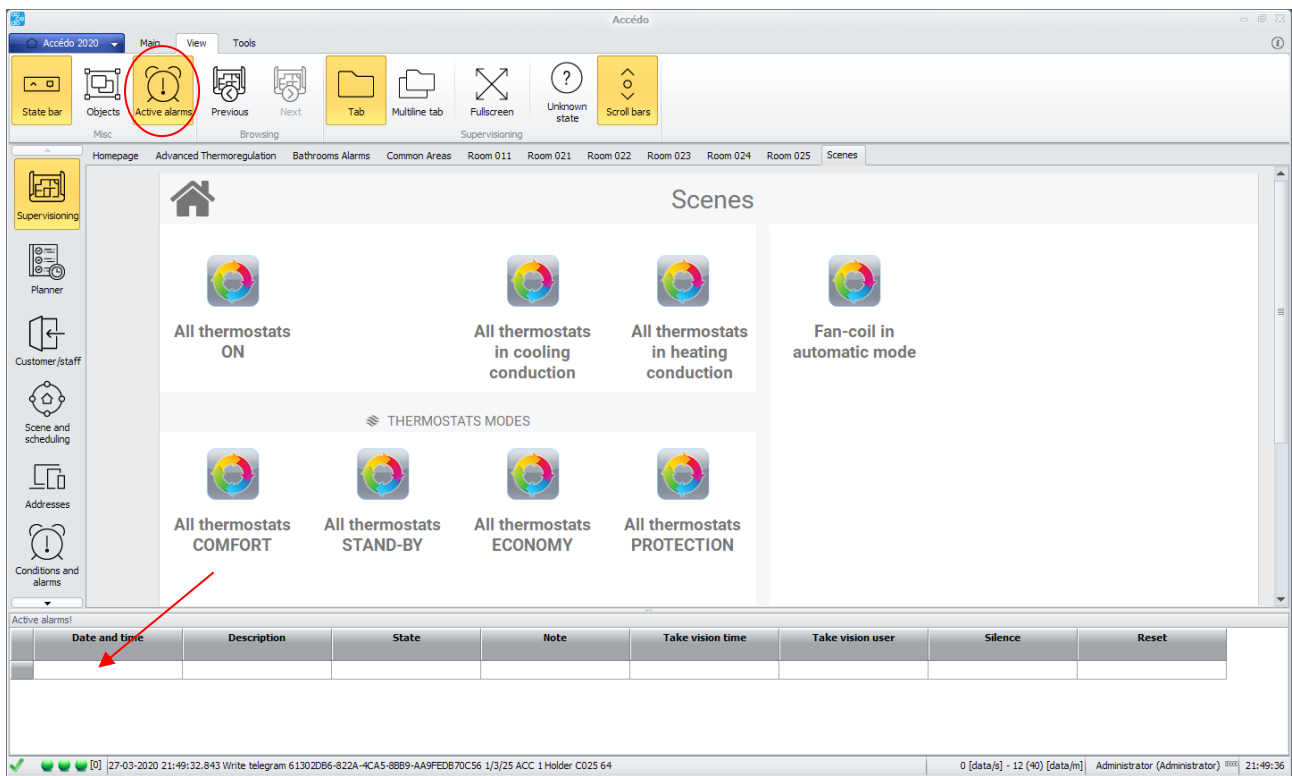


Figure 68 - active alarms display

- In the objects menu, which appears on the right, there are numerous functions accessible from the submenu on the right

10.6 Menù supervision objects

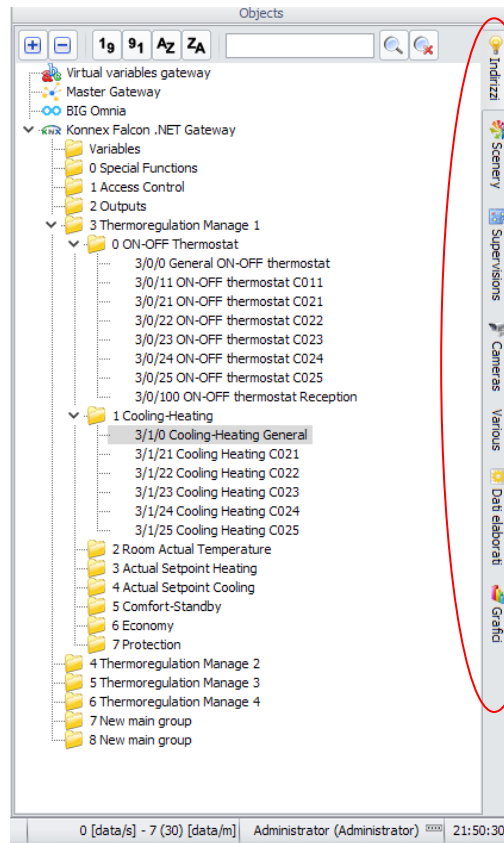


Figure 69 - supervision objects menu

In *Groups and users* you can see all the groups within the application and the users who are part of these groups.

In *Properties* in the example there are no properties available.

In *Scenes* you can see all available scenarios connected to the current supervision. You can drag a scenario within the supervision that will become a button that allows the desired scenario to be executed.

The *Supervisions* menu allows you to drag one of these objects within the screen and then have a button that sends the user to the page just selected.

It also allows you to organize the supervisions into folders:

- Right-click on a folder to create a child folder, rename the selected folder, or delete the selected folder (the latter operation removes the selected folder and all child folders and moves the supervisors below under the root folder "Supervisions");
- Dragging and dropping folders and supervisions from one node to another in the tree allows you to reorganize the structure.
- Double-clicking on a supervision opens the supervision itself (only if you are in the supervisor screen).

Allows you to drag one of the following objects:

- label: as soon as the default label is inserted the time is displayed through the following string inserted in the command name#hour2digitsminutes2digits.
- Form
- Image: where you can insert an image taken from a file or define a url to display an image taken from a camera. In the latter case you can define the polling time (refreshInterval) in seconds.
- Camera: in which you can define a url for the display of a streaming from a camera.
- Software link: to start a program external to the software.

In the case of the polled image or camera streaming, the url to be configured depends on the type of camera. For Axis, please refer to <https://www.ispyconnect.com/man.aspx?n=Axis>.

You can open the folders by clicking on the + on the left of the folder and allow the user to enter the subfolders and then the objects. By right-clicking on an object the following options appear:

- **ON**: Activate our object;
- **OFF**: Deactivates our object;
- **SWITCH**: Activates or deactivates the status of our object;
- **READ**: Reads the values of the object.

Finally you can save the changes made to the page using the save button in the *file* section. After saving the user must exit the edit mode by clicking on the exit button to see the actual supervision.

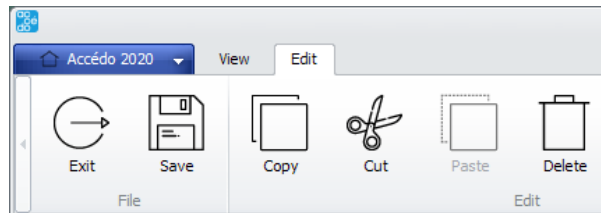


Figure 70 - tools for saving the created supervision page

11 GUEST/STAFF SECTION

Selecting Access Control from the side menu on the left and the item "**Tools**" from the top menu, the menu for managing access control operations is displayed as shown in the figure.

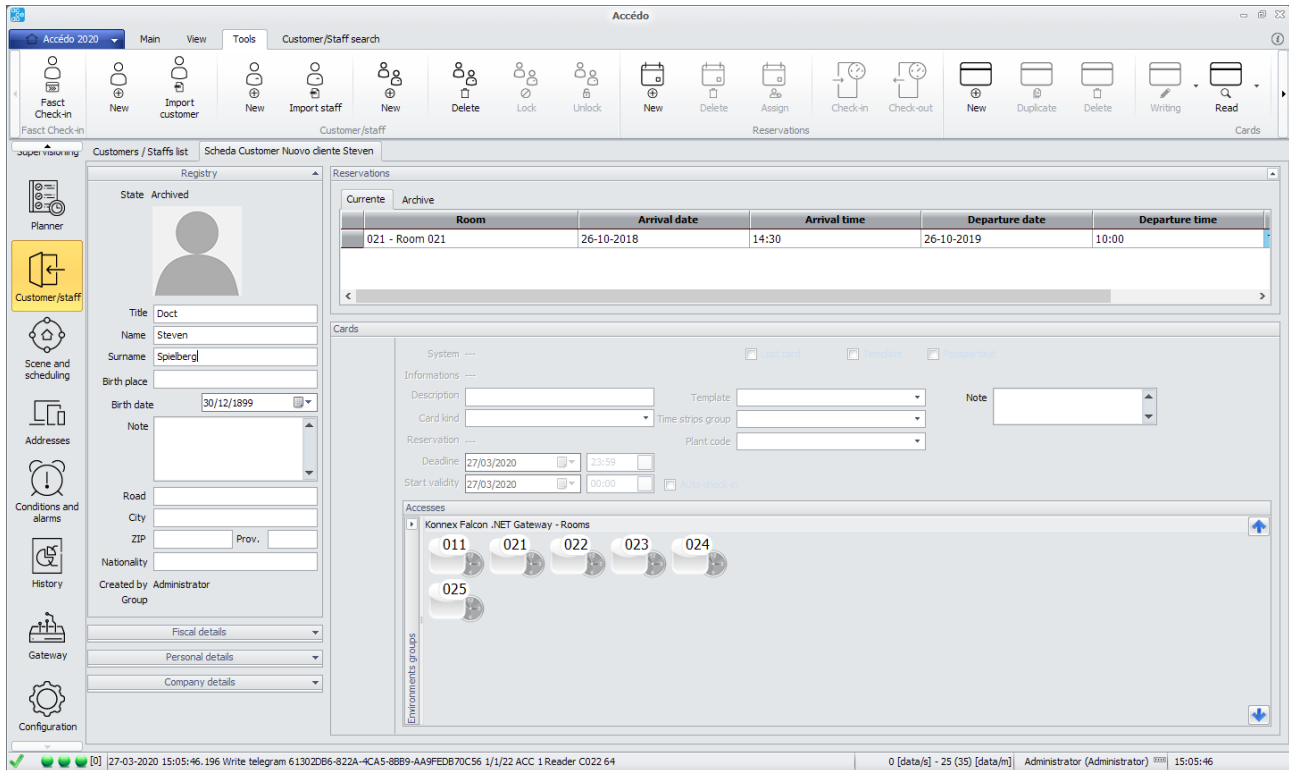


Figure 71 – Customer/Staff section

In this section you can:

- Create/Edit/Edit/Delete customer and staff records
- Import customer and staff records from xls
- Search for personal data in the archive
- Creating/Editing/Limiting bookings
- Check-in check-out on reservations
- Create/Edit/Edit/Duplicate cards
- Writing/reading cards via card programmer
- Activate cards on KNX readers and holders
- Lock/Activate all customer cards

Card creation not linked to reservation: Expiry date = today + 10 years

11.1 Add guest/staff

To enter a new customer press the "**New**" button in the section "**Customers**" and enter the data in the registry section, the field "**Last Name**" is mandatory while the rest are optional.

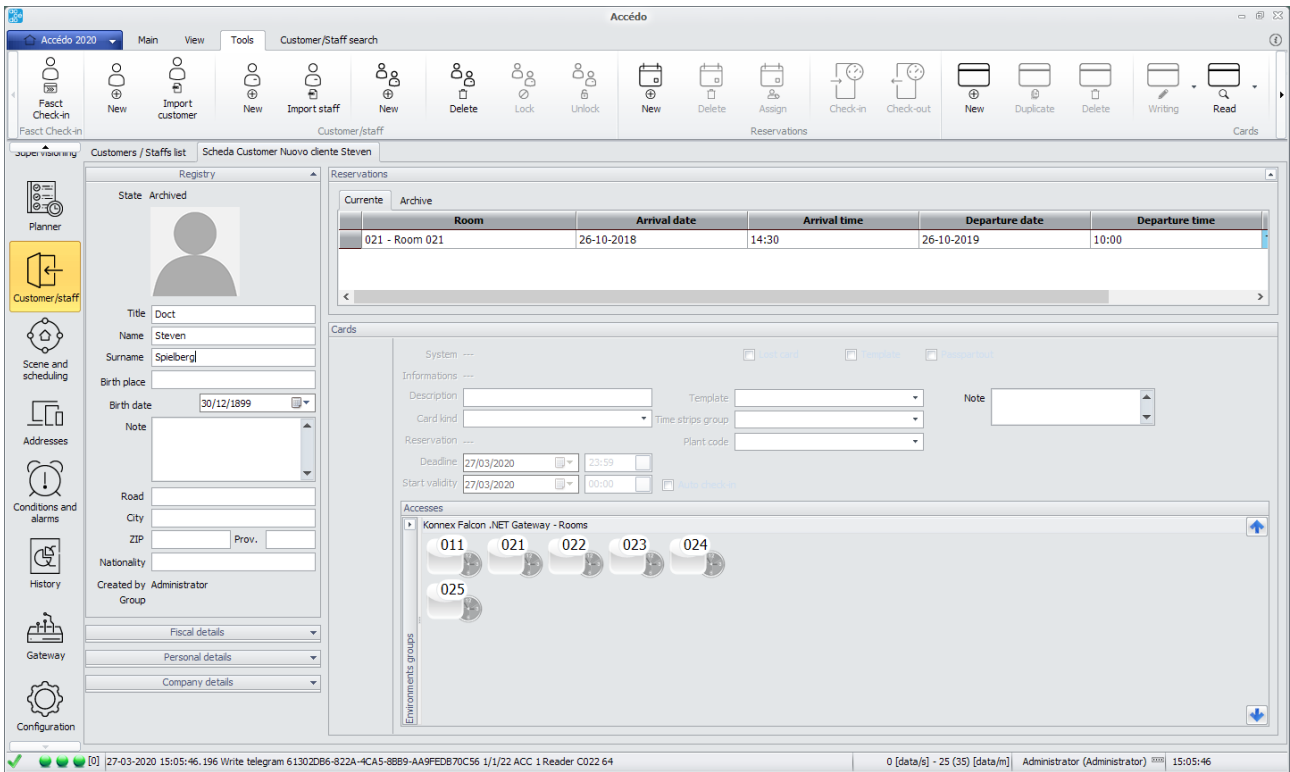


Figure 72 – New customer tab

11.2 Importing guest/staff from xls

The **Import from xls** button, valid for customers and staff, allows you to massively import a set of names and create, for each name, a card with access to a set of rooms.

11.2.1 Importer configuration

In order to correctly import the data in the xls (or xlsx) file it is necessary to configure the importer so that it recognizes in the different columns of the Excel file the significant data to be used.

The configuration can be defined in the *Configuration -> Importer* section.

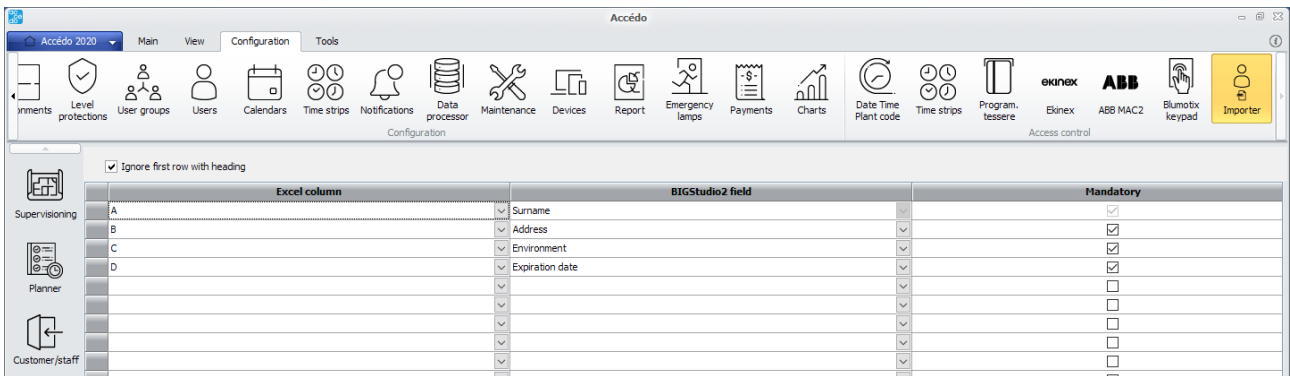


Figure 73 – importer page

The following informations are required in the configuration:

- Ignore the first line containing the header: If the first line of the file contains the header, you must enable the tick so that the line is not considered as a line of data;
- In each line of the configuration you must indicate:
 - The excel column containing the data of interest;
 - The associated accédo field;
 - The mandatory field: if the cell that should contain a mandatory value is found empty, the import is cancelled.

It is necessary to keep in mind that for customer/personal creation the last name field is mandatory (for this reason the first line is blocked).

The creation of the card associated with the customer is done only if there is a column associated with the room field and one associated with the Expiration Date field. Otherwise only the customer/personal is created. The Excel column associated with the Room field can contain multiple rooms separated by ';'. However, the room must be indicated by the room code on accédo for the association to be recognized.

11.2.2 Importing

At the end of the configuration you can proceed to import the customers/personnel in the access control section.

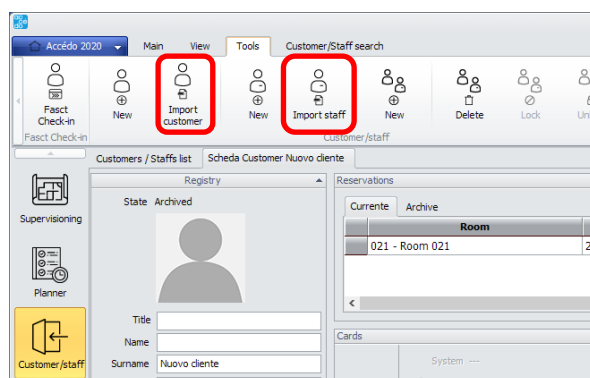


Figure 74 – Importing customer/staff

At the end of the import a popup indicates the result of the import which can be among the following:

- The import has been successfully completed: all customers/personals have been created and any enabled cards for the indicated rooms have been associated;
- The import ended successfully but the following names have not been created because they are already present: the excel file contained names that are already present in the accédo archive (the customer is recognized on the basis of surname, first name and date of birth); in this case a new customer is not created but a new card is associated to the existing customer.
- The import failed because some rooms have not been recognized: some of the rooms indicated in the Excel file do not match the rooms in accédo. In this case only the client associated to the unrecognized room is not created.

The import failed because some of the required fields are not highlighted: in this case no customer and no card is created.

11.2.3 Writing and activation of imported smart-cards

If the import was successful you can write and activate the cards created by accessing the form using the *Manage imported cards* button.

The form lists the imported cards that are still to be written or imported.

Chen Zmr	AA JNC-6177	36981	30-06-2018	006, 121, 011	✘
Chui Dee	AA JNC-6177	30763	01-07-2018	121	✘
CHUNG Pa	AA JNC-6177	48248	02-07-2018	430	✘
Dang Su	AA JNC-6177	24764	03-07-2018	011	✘
Driver Driver	AA JNC-6177	59720	04-07-2018	009	✘
Ha Kim	AA JNC-6177	34495	05-07-2018	007	✘
Hoang Do	AA JNC-6177	7719	06-07-2018	111	✘
Kwan Su	AA JNC-6177	40562	07-07-2018	112	✘
Liao Do	AA JNC-6177	23618	08-07-2018	116	✘
LING KIM	AA JNC-6177	38766	09-07-2018	302	✘
tizio casio		49170	10-07-2018	115	✘
Mak Cu	AA JNC-6177	16844	11-07-2018	324	✘
Ngo Na	AA JNC-6177	8714	12-07-2018	310	✘
Palattao Lee	AA JNC-6177	33349	13-07-2018	210	✘
Pon Do	AA JNC-6177	43961	14-07-2018	410	✘
romero ems	AA JNC-6177	54916	15-07-2018	321	✘
trines-mercado ams	AA JNC-6177	723	16-07-2018	106	✘
Woo Won	AA JNC-6177	58683	17-07-2018	401	✘
Yu Ra	AA JNC-6177	39892	18-07-2018	210	✘
Zhang Jen	AA JNC-6177	53891	19-07-2018	015	✘
Amato Maurizio		43990	20-07-2018	408	✘
ambruosi Nicola		26788	21-07-2018	102	✘

Navigation: 1 / 73

Buttons: [Back] [Forward] [Fine]

Figure 75 - form for writing and activating cards

Through the form is possible:

- Select the individual card and write it down;
- Select the single written card or a set of written cards and activate them;
- Press the Activate all button which activates all the cards that can be activated
- Read the card on the programmer
- Delete selected cards

11.3 Users

Only users in **Archived** status can be deleted!

11.3.1 User state list

- **Archived**: a client or staff is born "Archived" (and in a standard situation it comes back to us after check-out)
- **Active**: only for OFFICE version. If the customer has active cards.
- **Authorized**: when a customer has "Registered" cards and written on bus for access to certain rooms, but has no reservations.
- **Blocked**: when you decide to block all user accesses (wins on every other status!).
- **Check-In**: when the customer has at least one reservation in "Check-In" status (wins on "Booked").
- **Booked**: when the customer has at least one reservation.
- **InArrival**: not used in accédo at the moment; it is only a status displayed if today's date corresponds to the start date of a reservation, but not actually saved in the database.
- **InDeparture**: not currently used in accédo; it is only a status displayed if today's date corresponds to the end date of a reservation, but not actually saved in the database.
- **Not Arrived**: not used in accédo at the moment; it is only a status displayed if today's date is greater than the start date of a reservation, but the client has not yet checked in. Not really saved in the database.
- **Overtime**: not yet used in accédo; it is only a status displayed if today's date is greater than the end date of a reservation, but the customer has not checked out yet. Not really saved in the database.

Move reservation from one room to another: possible if you are <>Filed and <>CheckIn.

11.4 Booking

11.4.1 Booking insertion

Reservations can be entered in two ways:

- through the menu "**Planner**": using the mouse you select the period of stay expected for the customer, the reservation will be in temporary status and blue. Then by double click or Assign button you will have to assign the reservation to a new customer or one in the registry by making the search in the section Customer/Personal Search.
- through the menu "**Clients/Personal**": in the section "**Reservations**" through the button "**New**".

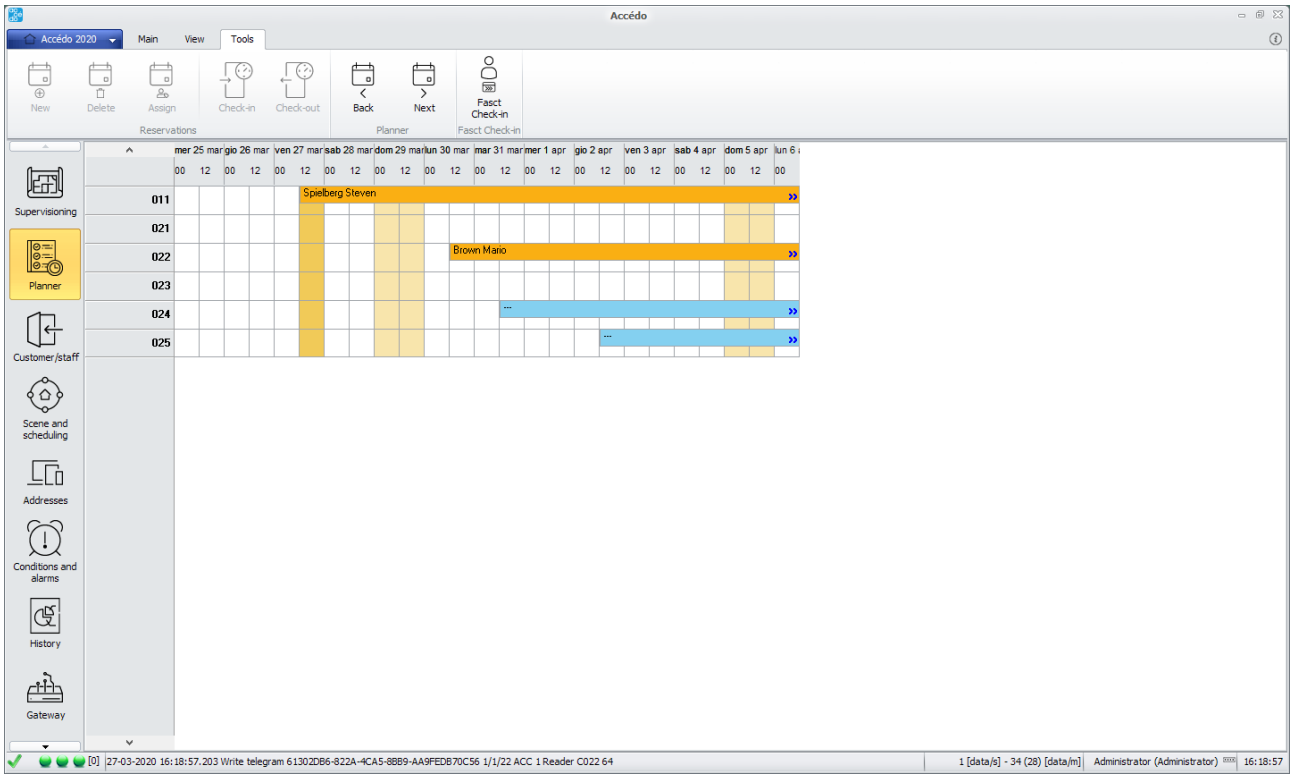


Figure 76 – Planner section

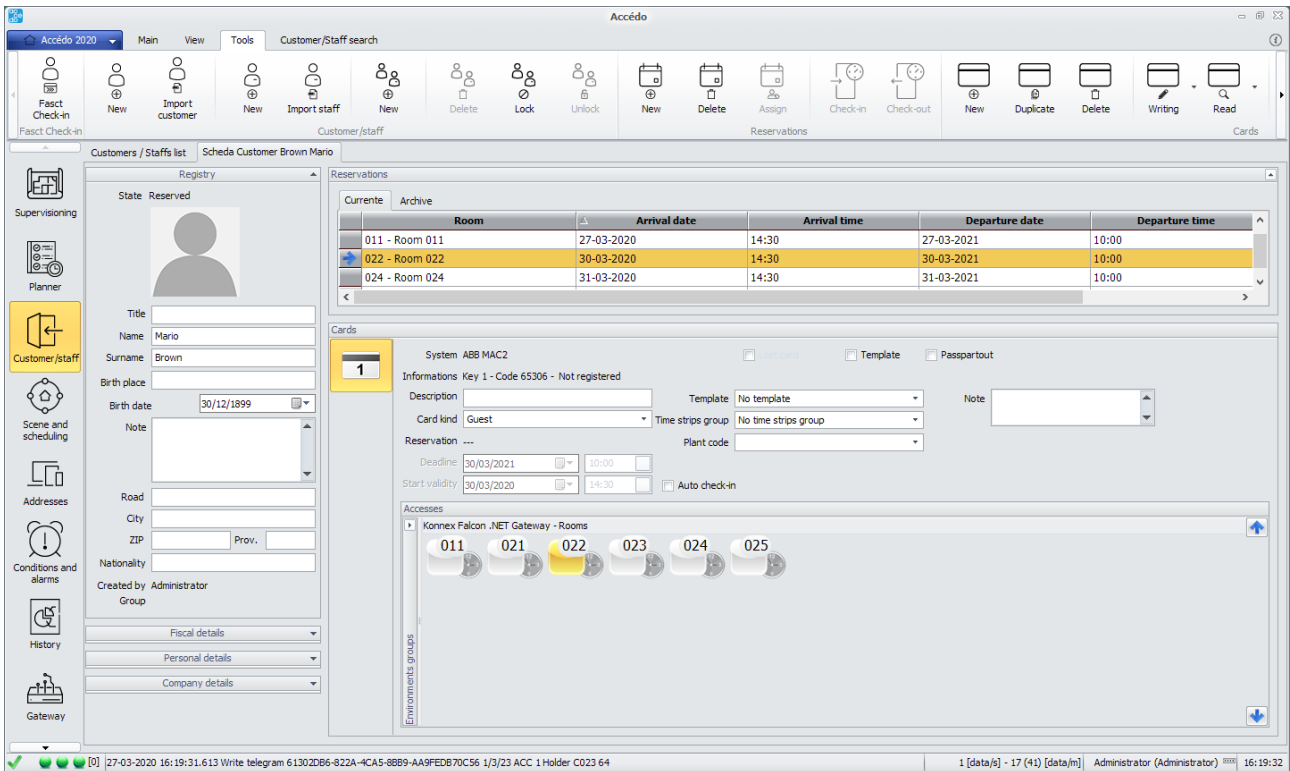


Figure 77 – Customer/staff section

After the reservation has been assigned to a customer his status becomes "**Booked**" and orange.

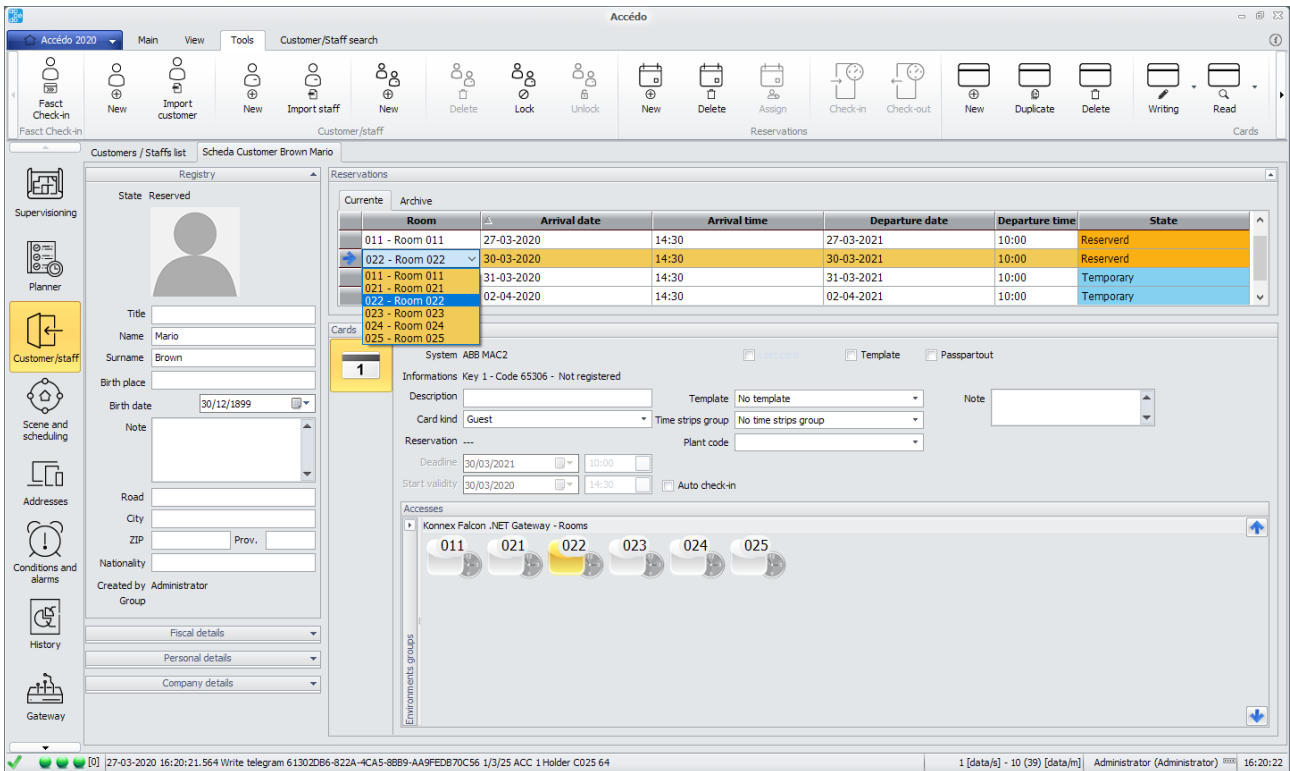


Figure 78 - booking insertion

In case you select the reservation you can make changes: room, period, etc..

- Change booking arrival date: only if Temporary or Booked status.
- Change departure date reservation: only if Temporary, Booked or CheckIn status.
- When creating a reservation, if the customer's status is "Archive" it goes to "Booked".
- Reservations can only be cancelled if in "Filed" or "Booked" status. The deletion of a reservation has no effect on the user's cards: there may still be cards with access to rooms related to the deleted reservation.

11.4.2 Booking status list

- **Assigned:** Office, corresponds to Booked. In the Office version there are only people who have keys that have room access permissions. The relationship between customer and environment with "Assigned" status is used for start and end dates. If I change the end date of validity of the relationship I have to update the expiry date of all the cards. In the Hotel version the customer/environment relationship is used for the job list.
- **Archived:** after the check-out procedure
- **Check-In:** "Booked" reservation after the check-in procedure
- **Maintenance:** Special status to indicate that the chamber is under maintenance
- **Booked**
- **Temporary:** when working on the planner, before selecting the associated client!

11.5 Smart-cards

When the card is created, the expiry date is equal to the farthest departure date among the customer's bookings (status = check-in, booked or assigned) + check-out default time, or 10 years if it is a service card.

When the departure date of a reservation is changed (when possible), the expiry dates of the cards that have access to that room are updated. The date is updated if the new departure date is greater than the card's current expiry date. In the bus update, the devices of the room for which the reservation is extended and the devices of all common accesses (to which the card has access) are involved. The writing on the bus is always bound to the fact that the card has already been written on the programmer, i.e. "Registered".

The expiry date of the card is ALWAYS editable. If necessary, appropriate telegrams are transmitted on the bus.

CARD COLORS:

- **White:** card created in the database, not written by the programmer, nor on the bus.



- **Yellow:** card written by the programmer ("Recorded"), but not yet on bus...



- **Green:** card written by the programmer ("Registered") and also sent to bus access control devices. A green card should guarantee access to certain rooms.



- **Red:** Blocked card ("Registered Blocked" or "Not Registered Blocked"). It is a card belonging to a user that you have decided to block! The necessary telegrams were sent on the bus to prevent this user from accessing any environment to which he was entitled.



Duplicate card: A card is created with the same access rights as the selected card. No bus telegram is written, as a newly created card has yet to be registered with the programmer.

Card deletion: The access rights of the card to each room are removed. The card is then set to NOT valid in the database. From this moment on, it will no longer be visible in the software.

11.5.1 Insert smart-cards

Use the "**New**" button in the "**Keys**" section to assign a new key to the selected customer. When creating the key its color is White: card created in the software archive.

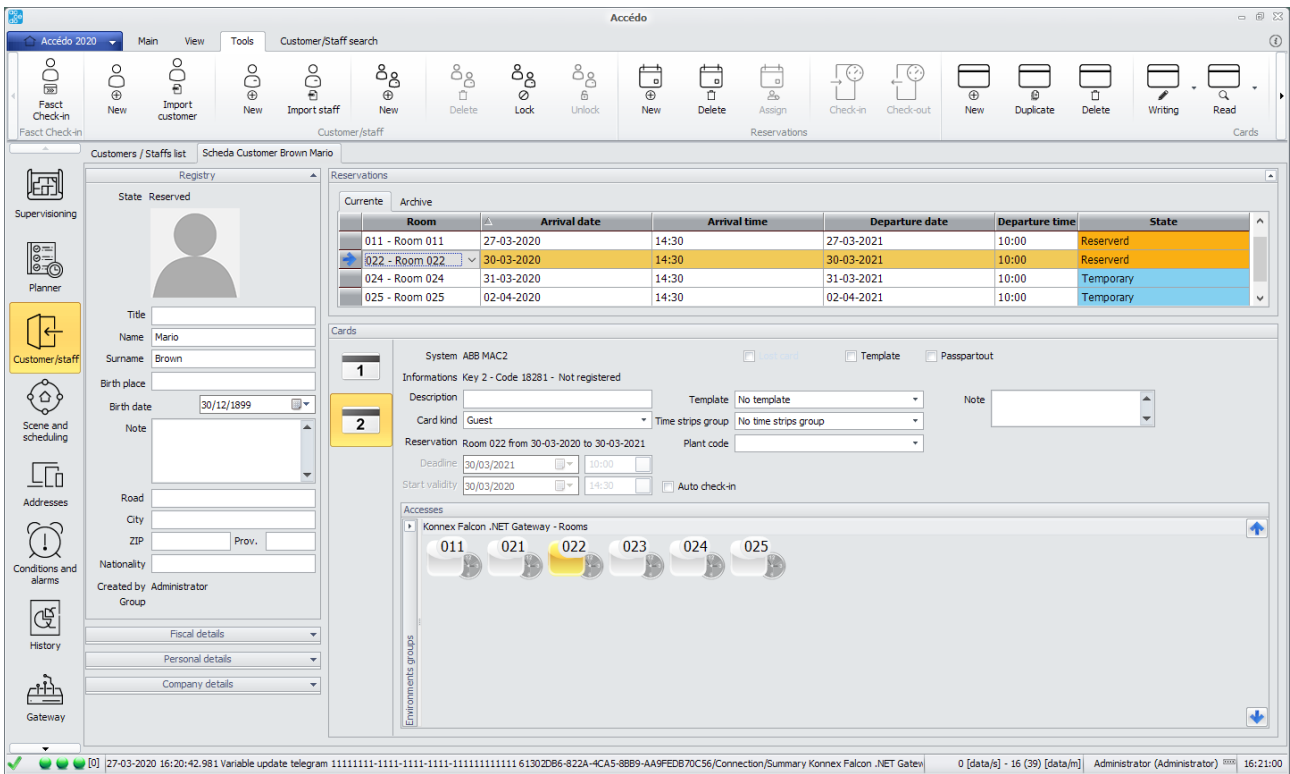


Figure 79 - inclusion of a card in the program

Then it is necessary:

- Write the card through the card programmer, inserting the card appropriately in the card programmer and pressing the "Write" button - The color of the card will turn orange, if the selected card programmer does not match the one in which the card has been inserted, a warning message will be displayed
- Select the gates where the card will have access rights
- Activate the card on the gates using the "Activate" button - the colour of the card turns green

11.5.2 Smart-card expiration report

accédo allows you to activate a daily alert to remind you when a card's expiry date is approaching.

The functionality is enabled in the Access Control section of the settings, where it is necessary to define the number of days to be considered (in the image you can see the cards expiring in the next 7 days), the time to report and the notification to be made. The latter is defined in the section Configuration->Notifications.

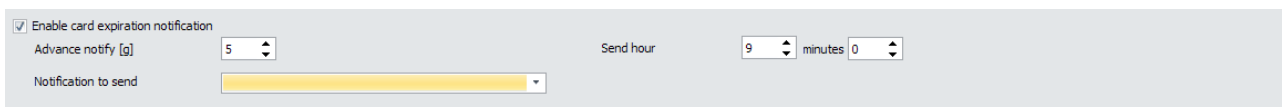


Figure 80 - card expiry configuration

11.5.3 New card code report creation

accédo allows you to send the customer a message indicating the card code generated and its expiry date, which is particularly useful when using Blumotix Keypad.

The notification is related to the selected customer and the selected card.

To send the notification it is necessary to configure a notification (in the relevant section), containing the desired text.

The text can be customized using an email editor.

The text you enter may contain the following keywords:

- #SURNAME: replaced when sending with the customer's last name
- #NAME: replaced when sending with the customer's name
- #CARDNUMBER: replaced when sending with the generated code
- #EXPIRATIONDATE: replaced during sending with the expiry of the generated code
- #STARTDATE: replaced during sending with the start date of validity of the generated code
- #ROOMNUMBER: replaced at the time of sending with the start of validity date with the number of the room to which it has access
- #CUSTOMERNOTE: replaced when sending with customer notes

In case the text contains a given keyword this will be replaced with the card and customer data selected at the moment.

An example text can be the following:

Good morning #SURNAME #NAME,

we generated for you the #CARDNUMBER code valid until #EXPIRATIONDATE.

Best regards

Test hotels

You must then activate the functionality in the *Settings -> Access Control - Code generation notifications section*. And select the previously created notification.

At this point in the access control section appears the *Send notification to customer* button.

That on the basis of the personal data entered on the customer (personal and work email), sends the notification to the customer. It is important to remember that the email is sent only if it is indicated on the customer in his personal data section.

11.6 Check-in

- Check-in can be performed on bookings in "Booked" status if today is a date included in the booking period.
- At check-in the status of the customer becomes "Check-In", as well as the status of the reservation.
- All customer cards are scanned at check-in. For each card, if that card is "Registered" and has access to the room for which you are checking in, guestdata telegrams are written on the bus that allow the access of the card to the room and common areas.

11.6.1 AutoCheck-in

For each card it is possible to define a start of validity date associated with automatic check-in: if the auto check-in is activated at the start of the minute of validity, if the card is "Registered", guestdata telegrams are written on the bus that allow the card access to the rooms and common areas on which access has been defined.

If the card is not registered, auto check-in will take place automatically the minute after the card has been written.

Car check-in and the start of validity date cannot be changed if the card has already been activated; moreover, if the card is linked to a reservation, its start of validity and expiry dates can only be changed through the relevant reservation.

11.7 Check-out

- It is only possible to check out if the customer's status is "Check-In".
- Selected bookings are scanned, looking for bookings in "Check-In" status. The status of these reservations becomes "Archive". For each of these, the customer's cards are scanned. If the card has access only to the room for which you are checking out (plus any common accesses), all accesses (to the room and common accesses) are removed; if the card has access to the room for which you are checking out and also to other rooms (plus any common accesses), only the access to the room for which you are checking out is removed.

11.8 Fast Check-in

In order to speed up the check-in operations when the customer arrives at the structure, it is possible to use the quick check-in that can be done through the appropriate button in the access control section.

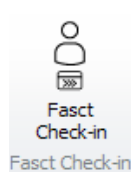


Figure 81 – Fast Check-in button in the toolbar

Through the popup that opens you can proceed with the creation of a customer (or a staff) by entering only surname, first name (optional), room to which it has access (selectable from the list or by writing the name of the room) and the date and time of expiry of the card generated.

Check-in

Cliente Personale

Cognome

Nome

Template

Ambiente

Zone comuni

Data di scadenza

Annulla

Check-in

Figure 82 – Fast Check-in form

Pressing the Check-in button performs the following actions:

1. Creation of the customer/personal;
2. Creation of the card associated to the customer with an expiration date equal to that indicated;
3. Assigning access to the selected room;
4. Writing the card (it is therefore necessary to already place the card on the programmer before pressing the check-in button)
5. Propagation of access to devices of competence.

If the quick check-in was successful, you can load the customer and the newly created card into the access control screen.

Quick check-in has the following features

1. Only one card is created: if you need to create a second card, you can use the classic procedures in the access control section by rewriting the already created card or duplicating it.
2. Only one room can be assigned: common rooms are added to the selected room if the relative setting is enabled; if it is necessary to add other rooms, the classic procedures are used in the access control section.

11.9 Access

At any time you can allow or deny a card access to a specific room by clicking on the icon representing the room. The software writes telegrams to the bus for each device associated with that room. Writing on bus is bound to the fact that the card is "Registered" (it is useless to write on bus cards that have not yet been written

even on the programmer!). There is also a customer status check: only if the status is one of "Active", "Authorized", "Check-In" or "Locked" do you continue writing telegrams on the bus. Users with status "Archive" or "Booked" cannot (should not!!!) have cards with access to any room!

Alternatively, it is possible to use room groups (left section): By clicking on a room group, access to all rooms and groups below is assigned/removed.

The color of the dots is in agreement with the color of the buttons:

- Green: active card
- Yellow: relationship between the card and the room
- Grey: no relationship present between the card and the room
- Grey and green: some of the underlying groups/rooms are active, others are not.
- Grey and yellow: some of the groups/rooms below are related, others are not.

12 CENTRALIZED ACCESS MANAGEMENT

Access management can be centralised via accédo, so that the access devices always send the transit telegram and it is the accédo server that decides whether or not to open the gateway.

In this way it is possible to evaluate whether or not access to the gate is allowed, both on the basis of the association made between the card and the gate (as in the traditional management of access control devices), and on the basis of the day and time when access is attempted, by adding time bands and calendars in the relationship between the individual gate and the individual card.

Time band management is also present in some access controls, but its management is extended in this case; calendar management, on the other hand, exists only in the case of a centralized access strategy.

Example. Through centralized management it is possible to define the following cards simultaneously:

- Administrator cards that always have access to every doorway
- Employee cards that have access to the offices only in the morning (8-12) and in the afternoon (14-18) and, at the same time, to the canteen during lunchtime (12-14); all accesses only on non-holiday days
- Maintenance cards that have access to all offices in one wing only on Saturdays (if not public holidays) during 8-12 hours and to all offices in another wing only on Fridays (if not public holidays) during 8-12 hours.

In centralized access management, the time elapsing between the passage of the card on the reader (and the related transit) and the opening of the access (or the denied access signal) typically takes less than 500 milliseconds (tests performed with 10 transit telegrams sent per second). It should be taken into account that this time may increase if the bus is overloaded.

12.1 Device configuration for centralized management

In order for the centralized management to work properly you need to configure the devices in the Configuration->Devices section as follows:

- Access strategy: centralized
 - N.B. there cannot exist rooms with mixed access strategy, i.e. with some centralized devices and others not; for this reason, when you change the access strategy of a device in Centralized all the other access control devices present in the same room receive the same access strategy.
 - The ekinex devices for which the access strategy is modified must be reloaded in the Configuration->ekinex section using the Download button.

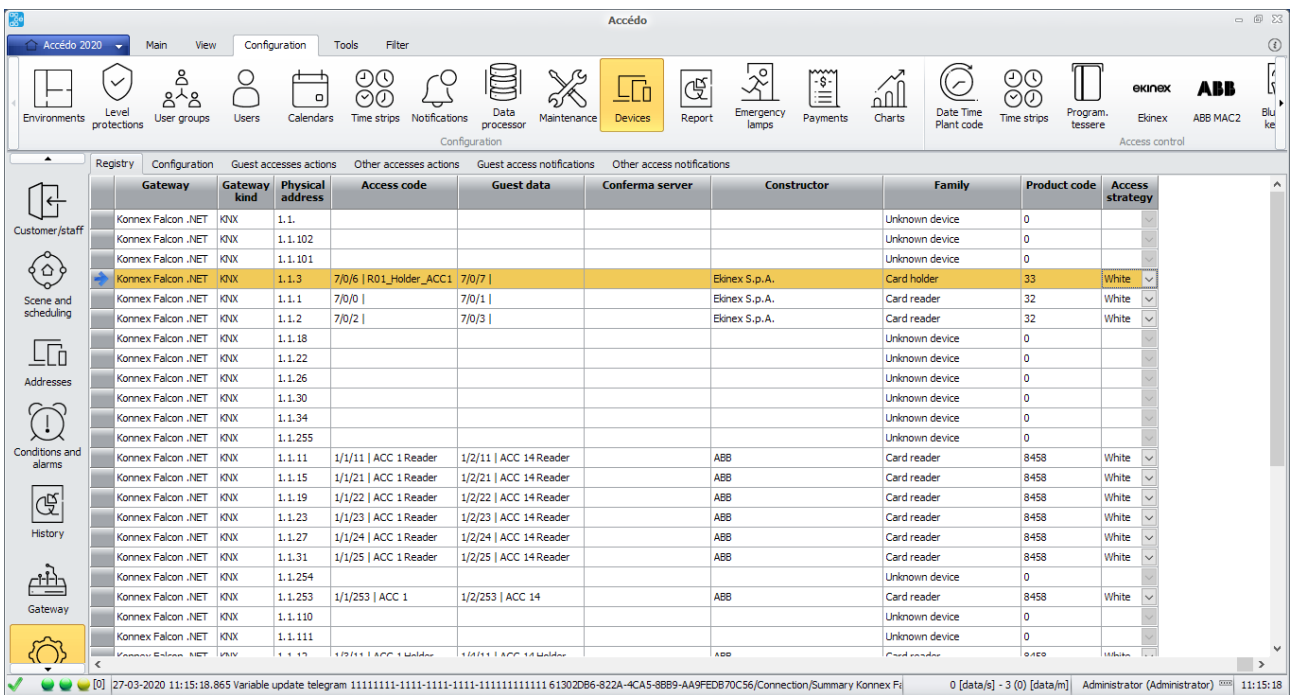


Figure 83 – Configuration section, Devices toolbar, registry tab

- Since the centralized management allows to know the reason why an access is denied, it is possible to insert the custom valid/denied access commands in order to manage the possible switching on of signalling leds: for each device it is necessary to indicate the commands for the following outcomes:
 - Valid access: the command is the one used to open the passageway MANDATORY
 - Generic denied access
 - Access denied expired card (used for centralised management only)
 - Access denied card not yet valid (used for centralised management only)
 - Access denied incorrect time slot (used for centralised management only)
 - Access denied incorrect calendar (used for centralized management only)
 - Card denied access blocked (used for centralized management only)

12.2 Configuration of time slots and calendars

In the sections *Configuration->Time bands* and *Configuration->Calendars* you can define time bands and calendars to be used when defining the accesses of a card. The configuration is explained in detail in the appropriate sections.

12.3 Access control section

In the access control section, for each access available with centralized strategy, you can see the button for the gate association, the time zone selection area and the calendar selection area.

- Access valid every hour and every day
- Access valid at specific times (one active time slot) and every day
- Access valid in specific hours (an active time slot) and specific days (a specific calendar)

When you create a new card and give access to a room with centralized strategy, the associated time slot and calendar by default always allow access (on any day and at any time).

If you have defined time bands or calendars in the appropriate sections by clicking on the band or calendar icon, you can add the respective access restriction.

For each access and each card it is possible to indicate at most one calendar and one time zone.

When access is enabled for a card, telegrams are propagated only to the holders, so that in case of denied access, the holder does not periodically send an error message.

12.4 Accesses history

In the case of centralized management the access history contains the access data, including the type of denied access detected by the software.

13 SEPARATE VIEW FOR USER GROUPS

A user can only view a subset of existing customers/personals, their cards and their access and attendance history according to the user's group.

This is useful when you want to keep user groups isolated, so that each group can see and manage only the customers/personals (and their access data) that are within its competence.

The competence of a user group on a given client/personal (and their access data) is assigned in case a user in the group has created the client/personal in question. Therefore, each user will only be able to see and manage clients/personals that have been created by the user himself or by another user belonging to the same group.

The only users excluded from this logic are those belonging to the Administrator group, who always have access to all customers/personals and their access data.

The separate view by user groups is disabled by default (therefore all users can manage, according to their protection levels, all clients/personal and their access data), but it can be enabled through the "View clients/personal divided by user groups" flag in the Access Control section of the settings.

13.1 Creator user tracking

In order for the separate display by user groups to work properly, the association between the customer/personal and their creator user must be properly tracked and managed.

When creating a new customer/personal, the user who actually created it is set as the creator user.

If you want to change it, thus associating the customer/personal to a different user and consequently to a different group of users, you can do so in the *Clients/Personal* history by choosing a different user in the *Creator User* column.

▲	Cognome	Nome	Città	Stato	Tessere attive	Utente creatore
➔	Affittuario A			Autorizzato	1	Agenzia1
	Affittuario B			Archiviato	0	Administrator
	Affittuario C			Archiviato	0	System
	Affittuario D			Archiviato	0	Farmacia1
	Farmacista A			Autorizzato	1	Farmacia2
	Farmacista B			Archiviato	0	Medico1
	Farmacista C			Archiviato	0	Medico2
	Farmacista D			Archiviato	0	Agenzia2
	Medico A			Autorizzato	1	Agenzia1
	Medico B			Archiviato	0	Farmacia2
	Medico C			Archiviato	0	Farmacia2
	Medico D			Archiviato	0	Farmacia2

Figure 84 – Creator user modify

Creator user editing is enabled only for users belonging to the Administrator group.

Example: in case a set of clients/personals is created through the Administrator user, it is possible to make these clients/personals belonging to a specific group by associating a user belonging to that specific group as creator user.

13.2 Sections affected by separate display by competence

13.2.1 Access control

In the access control customer/personnel search you can only find the customer/personnel of the user group to which the logged in user belongs. As a result, it is only possible to manage cards and accesses for visible customers/personals.

13.2.2 Guest/staff history

In the customer/staff history only the customers/personals of the user group to which the logged in user belongs appear.

13.2.3 Keys history

In the key history only the cards associated with customers/personals belonging to the user group to which the logged-in user belongs appear.

13.2.4 Accesses history, presence history

In the historical accesses/presences only the accesses and presences made with cards belonging to customers/personals belonging to the user group to which the logged in user belongs appear.

14 SPECIAL CASES

14.1 User assigned to multiple groups

In case the user is assigned to more than one group he will see and can manage all the customers/personals and their access data belonging to all his groups, i.e. all those created by users who are in his own groups. If one of these groups is *Administrator* the user will have full visibility on all clients/personals.

14.2 User moved from G1 group to G2 group

In case the user is moved from a G1 group to a G2 group the customers/personals created by the user and their access data will no longer be visible from the G1 group but will become visible from the G2 group.

However, if these clients/personals should remain in the G1 group, you can reassign the correct competence by assigning as their creator user a user belonging to the G1 group. In this way you lose the relationship between the customers/personals and their real creator user (the one that has been moved to G2), but you restore the relationship between those customers/personals and the correct competence group, i.e. G1.

14.3 Delete a user

If a user who is a creator user of a set of customers/personals is deleted, the *Administrator* user is assigned as the new creator user.

15 REPORTS

15.1 Access history

Selecting "**Report**" from the side menu on the left you can access the "event history" module.

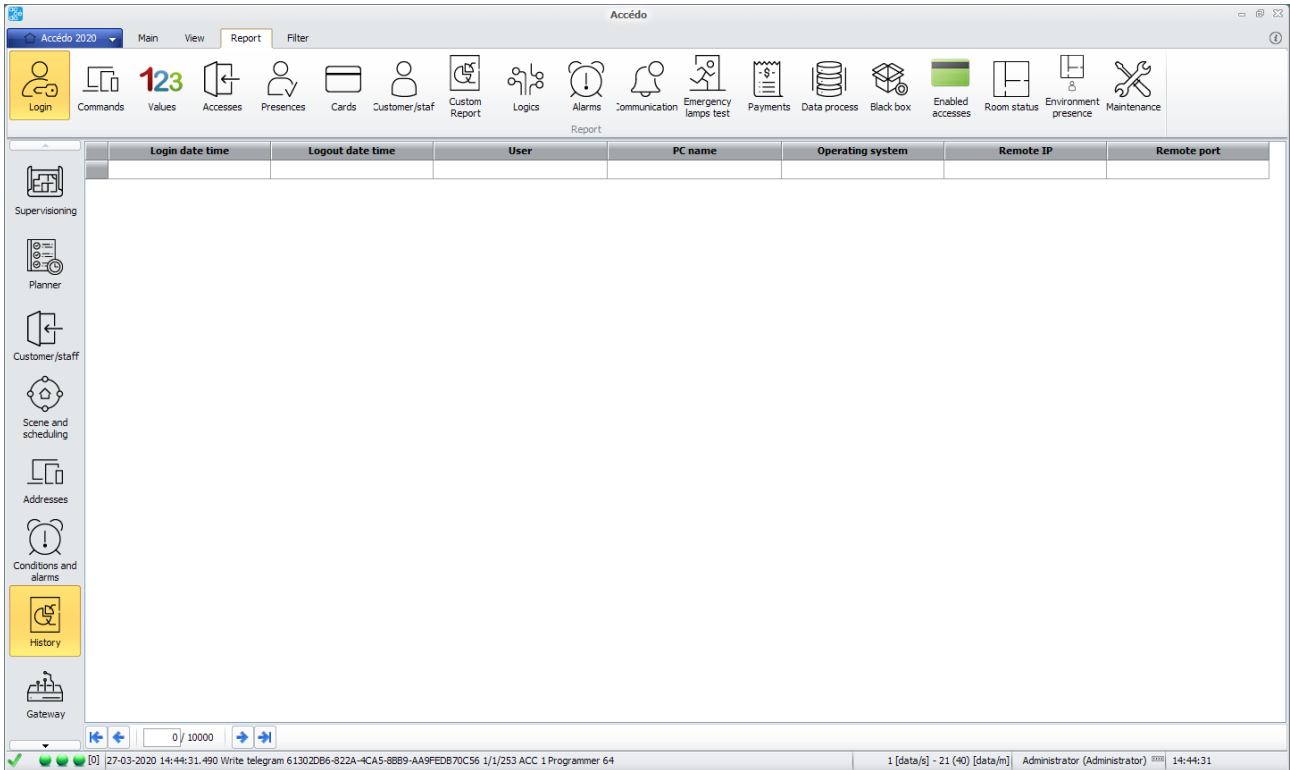


Figure 85 – Access history section

By selecting "**Accesses**" and then "**Filters**" you can access the section that allows you to set the search criteria for accesses:

- By date
- By event outcome
- For room

After defining the criteria, press the "Filter" button to display the data available in the archive for this search.

15.2 Login history

The parameters represented in Login history are the following:

- Login time date
- Date time logout
- User
- PC Name
- Operating System
- remote IP
- Remote door

15.3 Commands history

The parameters shown are:

- Date and time
- Username
- PC Name
- Type
- Gateway
- Address
- Address name
- Command
- Value
- Result
- Scene

15.4 Values history

The parameters shown are as follows:

- Date and time
- Gateway
- Address
- Address name
- Value
- Telegram type

15.5 Presence history

The parameters shown are the following:

- Input date and time
- Date time out
- Result
- Number
- Description
- Device
- Key code
- Key ID
- Owner

15.6 Keys history

The parameters displayed are:

- Code
- ID
- Type
- Owner
- Validity
- Status

- Lost
- Written on the bus
- System
- Validity start date
- Expiry date
- Booking
- Group of time slots
- System code
- POS type
- Payment profile
- Credit

15.7 Alarms history

The alarm history allows to display all and only the reset alarms, which can be filtered by description, room, start date, end date and reset status. The alarms of other status (in progress, silenced, returned) are visible in the active alarms grid.

The following information is visible for each alarm:

- Alarm: Date and time the alarm was triggered.
- Solution: Alarm reset date and time
- Duration: difference between the previous ones
- Alarm type: as defined in the alarm configuration phase
- Description: as defined in the alarm configuration phase
- Room: as defined in the alarm configuration phase
- User who has taken vision and possible note
- User who reset the alarm and possible note

15.8 Maintenance history

The maintenance history allows you to record the maintenance and view the maintenance previously recorded.

15.8.1 Registration

La registrazione avviene attraverso il pulsante *Inserisci*

The input form allows you to indicate:

- Maintenance: the maintenance that is being recorded
- Maintenance staff: maintenance staff are chosen from the access control staff (the Company is included in brackets)
- The date of execution: the current date can be changed at will
- The execution time counter: the current one (if present) can be modified at will
- The execution notes

When the maintenance is registered, you can only delete it and insert a new one, but not modify a previous one.

Maintenance can be filtered and exported to Excel.

15.9 Payments

From the "Payments" report it is possible both to see the history of payments generated and confirmed, and to generate new payments for time periods of your choice and then export them in PDF, Excel and/or confirm them, thus inserting them in the archive.

15.9.1 History

By setting the filters relating to the description of the payment profile (environment) and the time period you can view the payments generated and confirmed.

15.9.2 Generation

In the generation section you can generate new payments for any time period of your choice. Use the filters to search for payment entities (rooms). Found the entities of interest, these can be selected in the grid and then, from the instruments tab, you can generate the payment note for the set period.

With the option "Starting date from last day paid" the software automatically determines the starting date by going to search in the archive the last payment generated and confirmed related to that payment entity (room). If you do not use the option the start and end dates are free.

When counting, set the dates A and B, for each progressive counter, the software searches for the last value associated with the counter on date B and subtracts the last value associated with the counter on date A - 1 day. This value represents the counter consumption in the period A - B. In this way no payment time period is lost.

For impulse type counters, the sum of the counter values recorded in the period between A and B inclusive is made.

Once payment generation is complete, all values appear in a window. They can be exported in PDF or Excel format. If you press "Cancel" the calculated values are lost. If you press "Confirm" the calculated values are saved in the payment history.

15.10 Communications

From the "Communication" report you can see the history of all incoming and outgoing communications managed by accédo. The communications concerned are:

- Incoming and outgoing calls made via the GSM gateway;
- Incoming and outgoing messages sent/received via the GSM gateway;
- E-mails sent following the triggering of a notification by e-mail.

- Communications can be filtered by date and time (initial and final), type of communication (call, message or e-mail), and result.

16 ANOMALIES MANAGEMENT

In the lower left corner, **two icons** of the operating status of the color software system can be visible:

- **Green:** the system is correctly started and communicates correctly
- **Yellow:** the system is started but there are anomalies in communications
- **Red:** the system is not started correctly

Check that the icons are green.

There may be a number in **square brackets** next to the icons, this number **must be 0 or decreasing**. If the number is constant or increasing, there are communication anomalies with the system.

The following devices must be accessible via Ethernet from the reception desk:

IP/KNX interface - address 92.223.168.7

Logic control module 1 - 92.223.168.8

Logic control module 2 - 92.223.168.8

The external readers have signalling leds, in case of problems with the opening of the camera check which led and which colour it lights up. In case of correct operation and allowed access the led must light green.

17 CONFIGURATION SETTINGS MENU

17.1 General

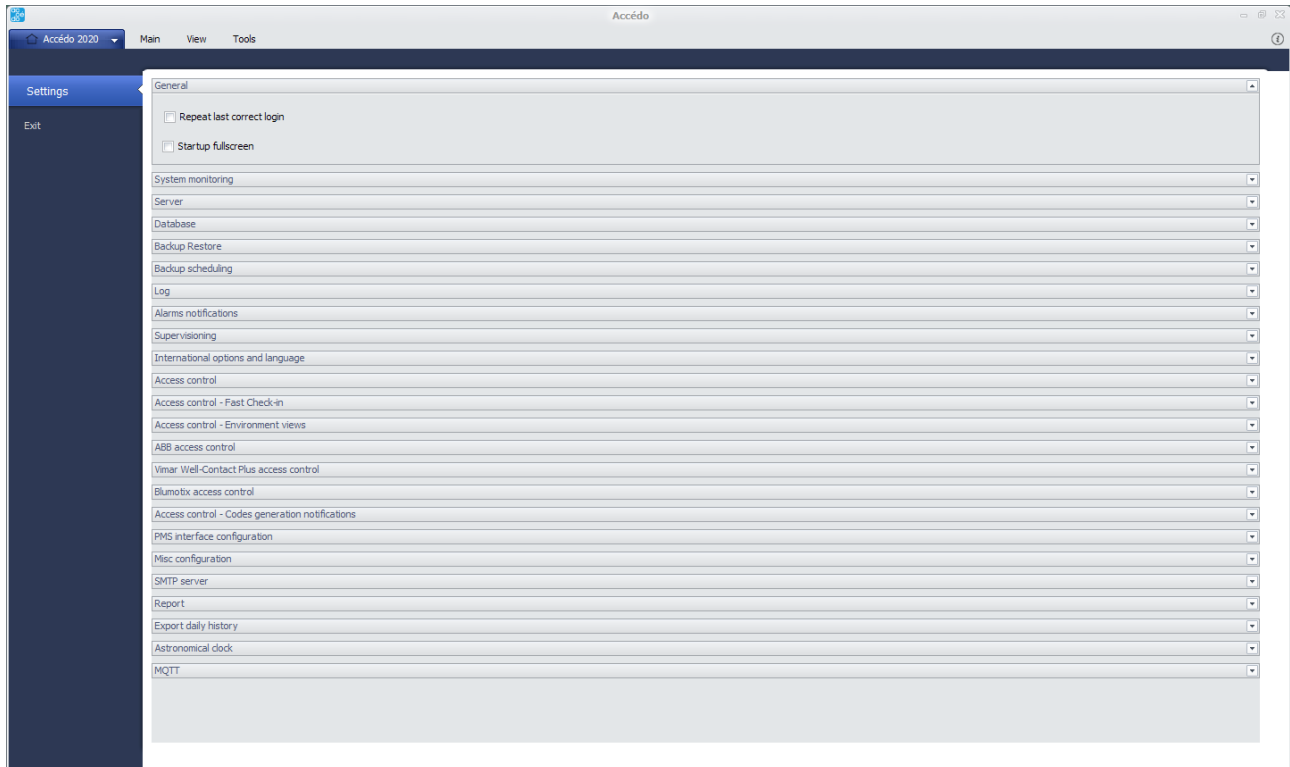


Figure 86 – Settings, General section

In the General section there are two options that the user can select:

- Repeat the last correct login
- Fullscreen at startup

Repeat the last correct login allows you to log in with the last successful login.

Fullscreen at startup allows the user to have the full screen at application startup.

17.2 Server

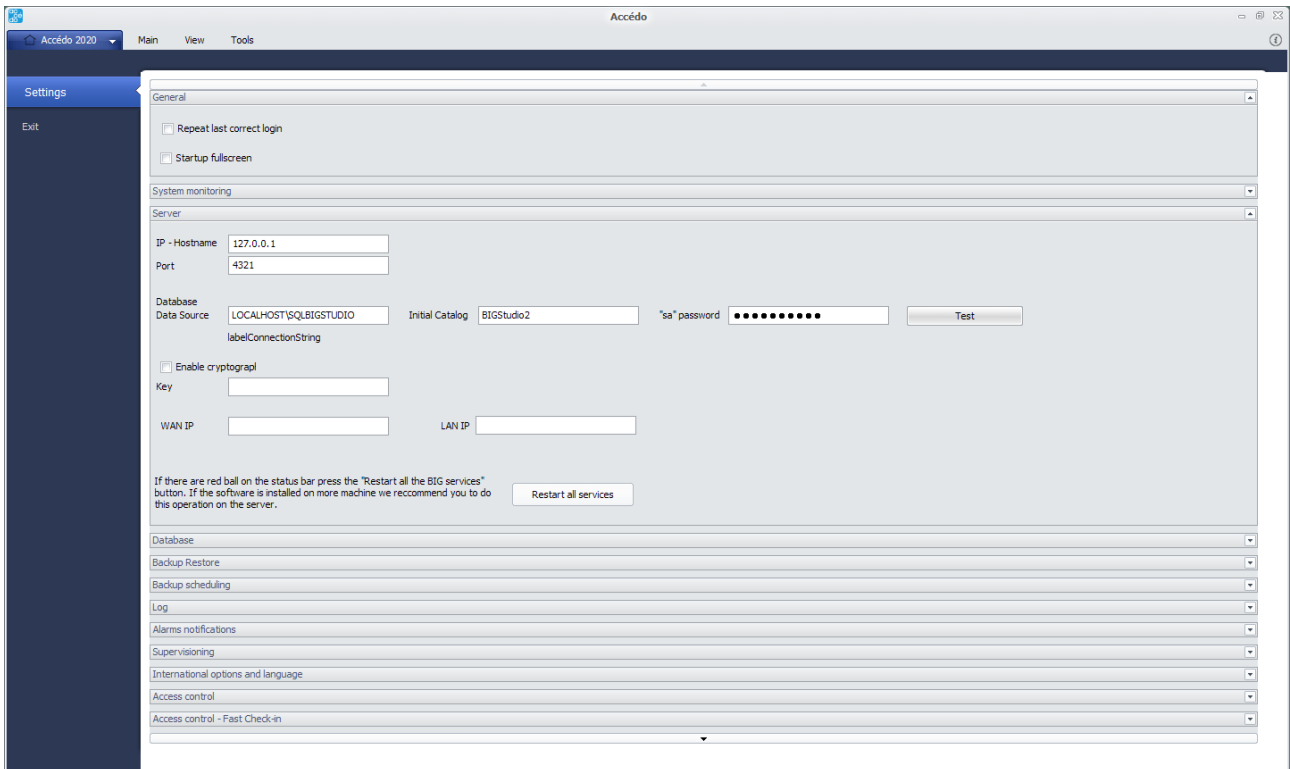


Figure 87 – Settings, Server section

In the accédo *Server* section the options that the user has the possibility to modify concern the server and database parameters.

- IP
- Door
- Database data source
- Initialcatalog
- "Account name" password
- Enable Encryption
- Key

IP is the IP address of the server to which the machine connects.

Port is used to connect to the server and is the useful information along with the IP address.

Database data source where the data is stored.

Initialcatalog: the reference folder for saving.

"Account name" password allows you to enter the password to access the database.

Enable encryption can be selected by the user to encrypt the information that will be entered into the database.

Key the user can decide through a text area what type of cryptographic key is desired.

17.3 Database

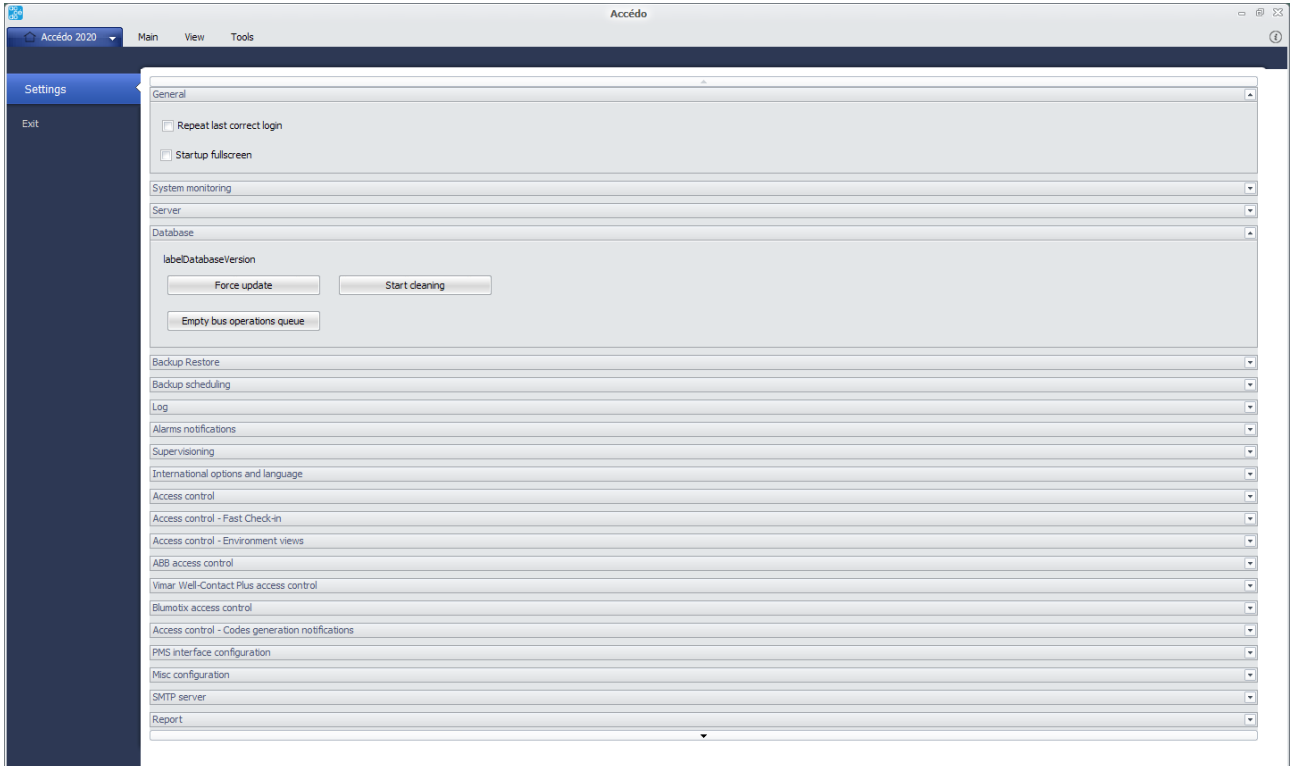


Figure 88 – Settings, Database section

In the *Database* section there are three buttons that the user can press as needed. There is a label that says which version is used.

- Force update
- Perform cleaning
- Empty bus operations queue

Force update allows you to force the database version update even if the database version updates every time the application is updated.

Run cleanup allows you to empty the database. Useful in case you need to completely change the project and instead of creating a database use the old one.

Empty bus operations queue allows you to delete the bus write operations that the program has yet to execute.

17.4 Backup Restore

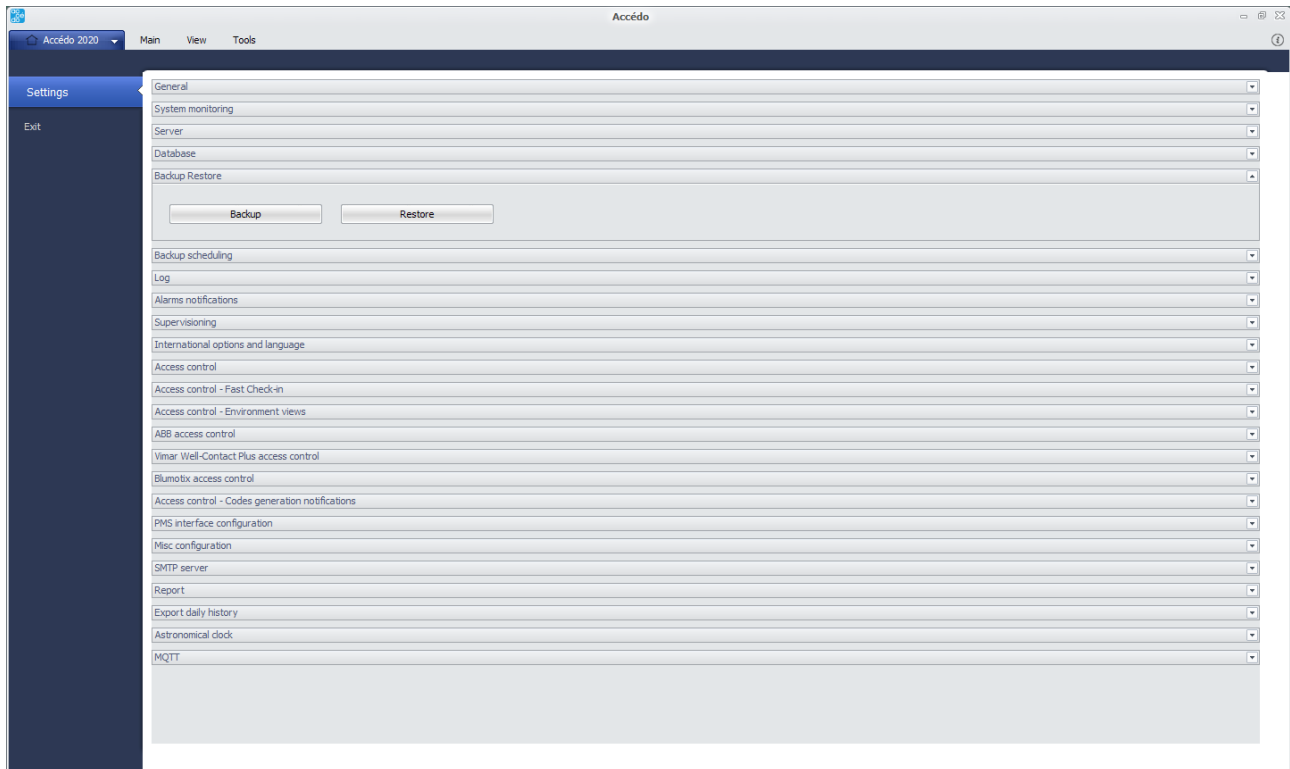


Figure 89 – Settings, Backup Restore section

There are only two buttons in the *Backup Restore* section.

- Backup
- Restore

Backup allows you to back up your project. See the proper paragraph of the manual for a more detailed description.

Restore allows you to perform a project restore. See the proper paragraph of the manual for a more detailed description.

17.5 Backup scheduling

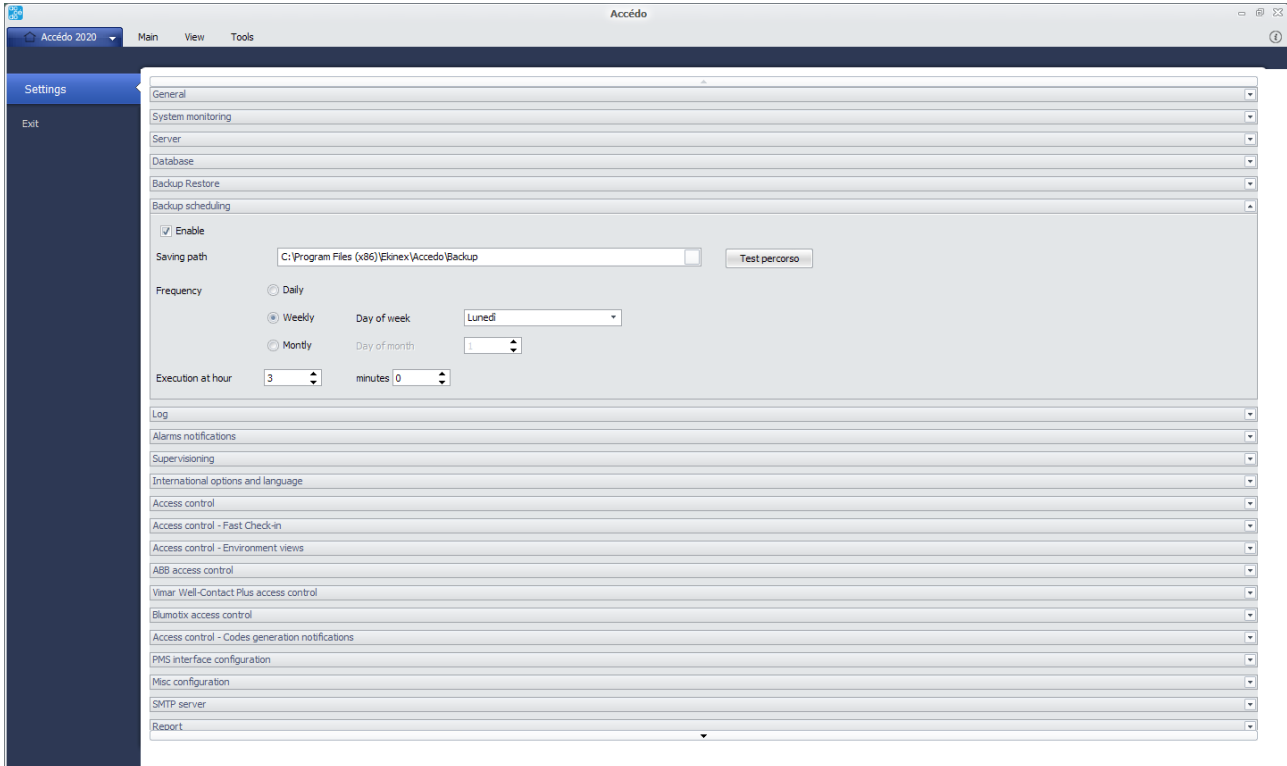


Figure 90 – Settings, Backup scheduling

In the *Backup Scheduling* section the user must press Enable to change the backup schedule settings. After checking Enable the options that can be configured are as follows:

- Save path
- Frequency
- Day of the week
- Day of the month
- Execution at hours
- Minutes

Save Path allows you to set the save path of the backup schedule.

Frequency allows you to set the frequency with which to make the backup and the available options are as follows:

- Daily
- Weekly
- Monthly

Day of the week allows you to select the day of the week on which to make the backup schedule.

Day of the month allows you to select the day of the month on which to schedule the backup.

Hourly Scheduling allows you to set the time at which to schedule the backup.

Minutes after setting the time allows you to select the minutes in which to schedule the backup, for example 15:09.

17.6 Log

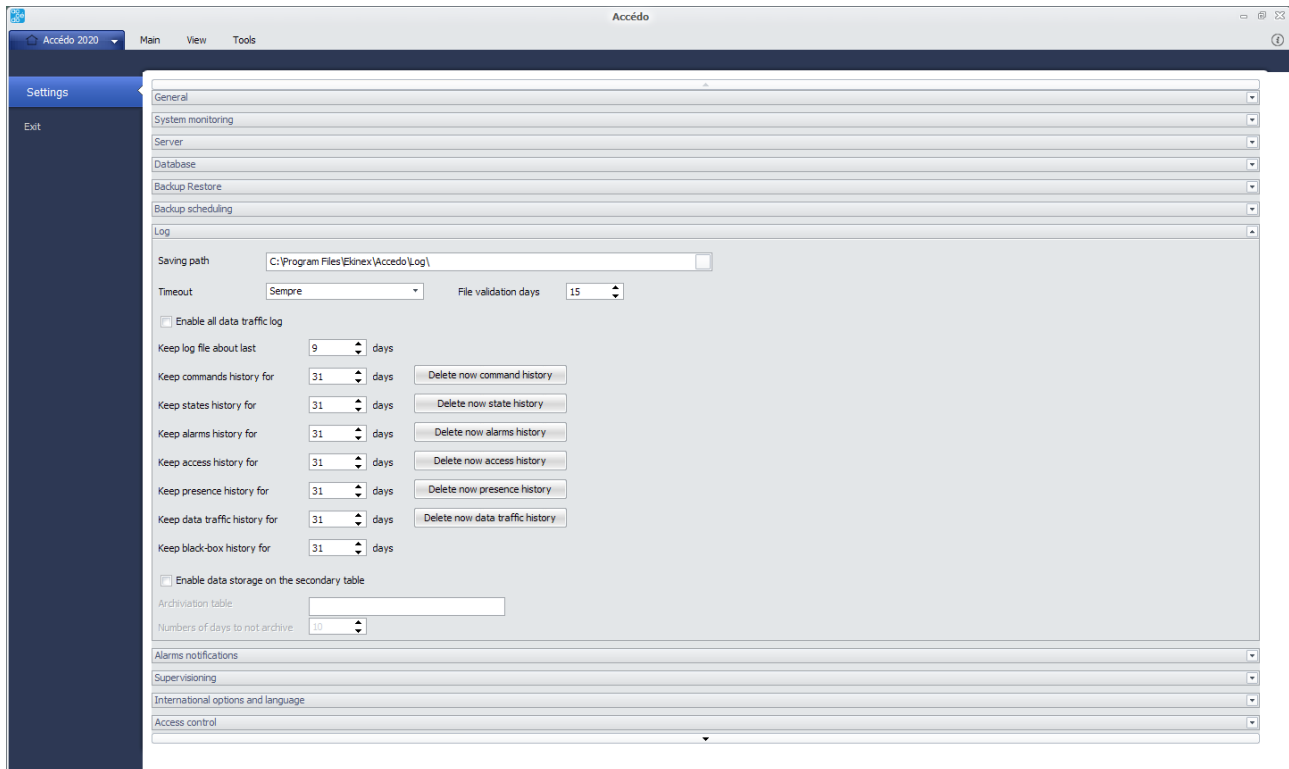


Figure 91 – Settings, Log section

In the *Log* section it is possible to set the memory permanence, the path to save the log files concerning the application. The available options are therefore the following:

- Save path
- Timeout
- Days of file validity
- Enable recording of all data traffic
- Keep the log files of the last n days
- Maintain command history for n days
- Delete command history now
- Keep the historic state for n days
- Delete now the historical states
- Maintain alarm history for n days
- Delete alarm history now
- Maintain historical access for n days
- Delete access history now
- Maintain historical attendance for n days
- Delete now the historical presence
- Maintain data traffic history for n days
- Delete data traffic history now
- Keep the historic black box for n days

Save Path allows you to set the save path for the various log files.

Timeout allows you to select from a combo box the type of log files to record.

Days of validity of the file allows you to set the number of days of validity of the file.

Enable the recording of all data traffic allows you to record all data traffic in the various log files.

Keep log files for n days allows you to define the number of days on which the log files will be kept.

Keep command history for n days allows you to define the number of days on which all command history will be kept.

Delete Command History is a button that allows you to instantly delete the entire command history.

Keep status history for n days allows you to define the number of days on which all status history will be kept.

- It is also possible to enable the storage of the values history in a support db: to do this it is necessary to define the following parameters in the *Settings* table:
 - CoreManager_LogTelegrams_EnableArchive: True
 - CoreManager_LogTelegrams_ArchiveDaysOlder: 10 (number of days not to archive)
 - CoreManager_LogTelegrams_ArchiveDBTable:
[BIGStudio2_Archive].[dbo].[LOG_TELEGRAMS] (name of the database and table where to store the data)
 - If the storage table is present, the deletion of states older than X days is done on the storage table, otherwise it is done on the LOG_TELEGRAMS table.

Delete state history now is a button that allows you to instantly delete the entire state history.

Keep alarm history for n days allows you to define the number of days on which the entire alarm history will be kept.

Delete alarm history is a button that allows you to delete the entire alarm history instantly.

Keep access history for n days allows you to define the number of days on which the entire access history will be kept.

Delete now the access history is a button that allows you to instantly delete the entire access history.

Keep attendance history for n days allows you to define the number of days on which the entire attendance history will be kept.

Delete now the attendance history is a button that allows you to instantly delete the entire attendance history.

Keep data traffic history for n days allows you to define the number of days on which all data traffic history will be kept.

Delete now the data traffic history is a button that allows you to instantly delete the entire data traffic history.

Keep the black box history for n days allows you to define the number of days on which all the black box history will be kept.

17.7 Alarm notification

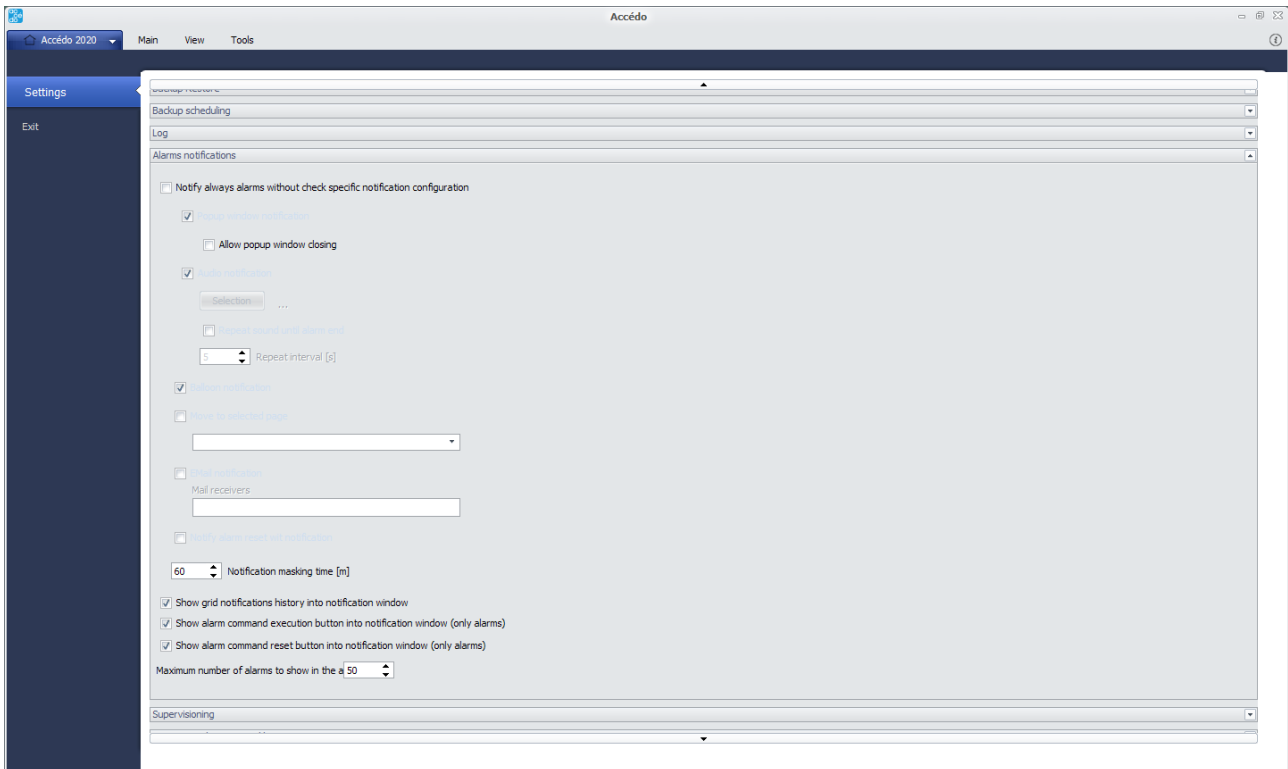


Figure 92 – Settings, Alarm notification

In the *Alarm Notifications* section there are options to tick to select the type of alarm notification desired:

- Always notify alarms without considering the specific notification settings
- Popup notification
- Allow the popup window to close
- Notification with audio
- Button selection that allows you to select an audio track as an alarm
- **Repeat audio** until the alarm is silenced
- **Repeat interval [s]** allows you to set the number of seconds every time the audio notification is repeated
- **Balloon** notification
- **Move supervision** to the page allows you to select a page that will be displayed when the alarm is triggered
- Email notification
- Email recipients if notification with email is enabled allows you to enter the recipients of alarm emails
- Notify the return of the alarm by email
- Notifications masking time [m] allows you to set the number of minutes after the notification is hidden
- Display notification recurrence grid in the notification window
- View alarm acknowledgement commands execution button in the notification window (alarms only)
- Display alarm reset button in the notification window (alarms only)

17.8 Supervising

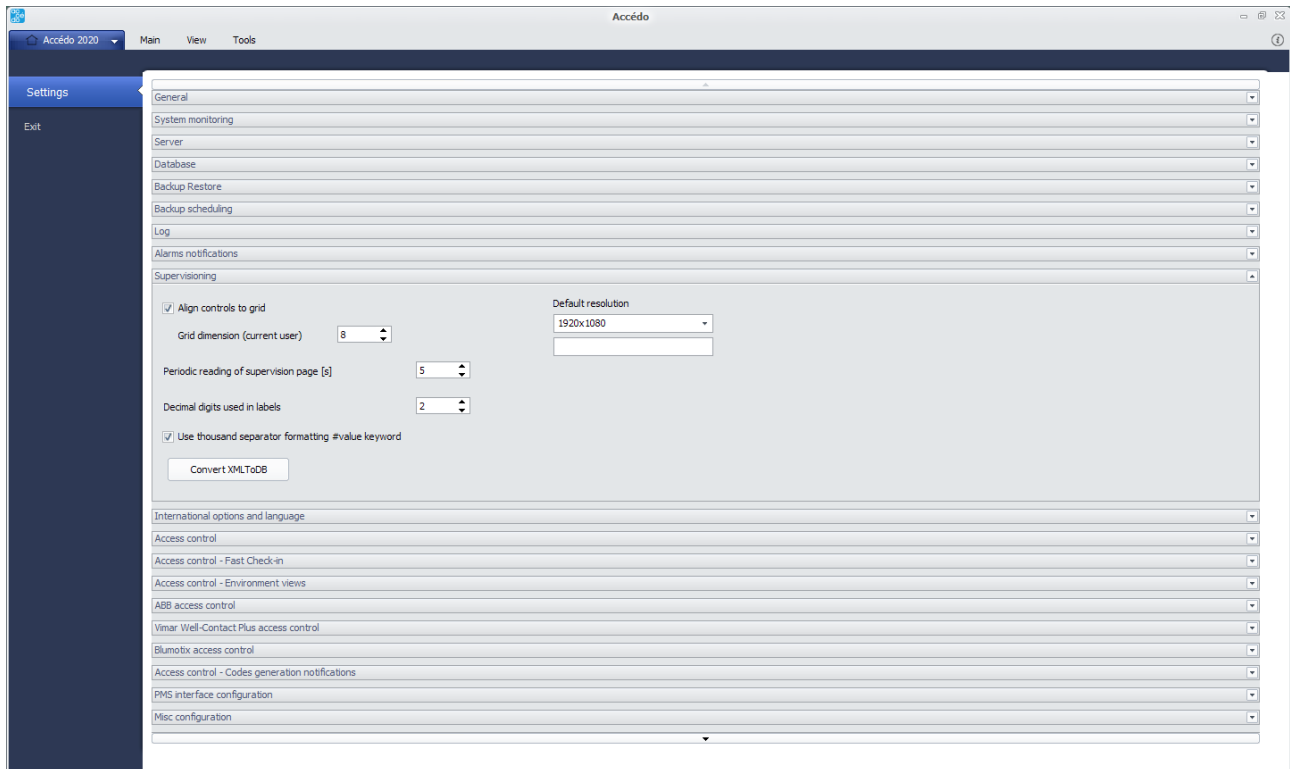


Figure 93 – Settings, Supervising section

In the *Supervision* section there are three options that the user can manage.

- **Align graphic** components to the grid
- **Grid size** (current user) allows you to set the grid size
- **Periodic address reading** of the supervision page [s] allows you to set the number of seconds of interval between one reading and another.

17.9 International options and languages

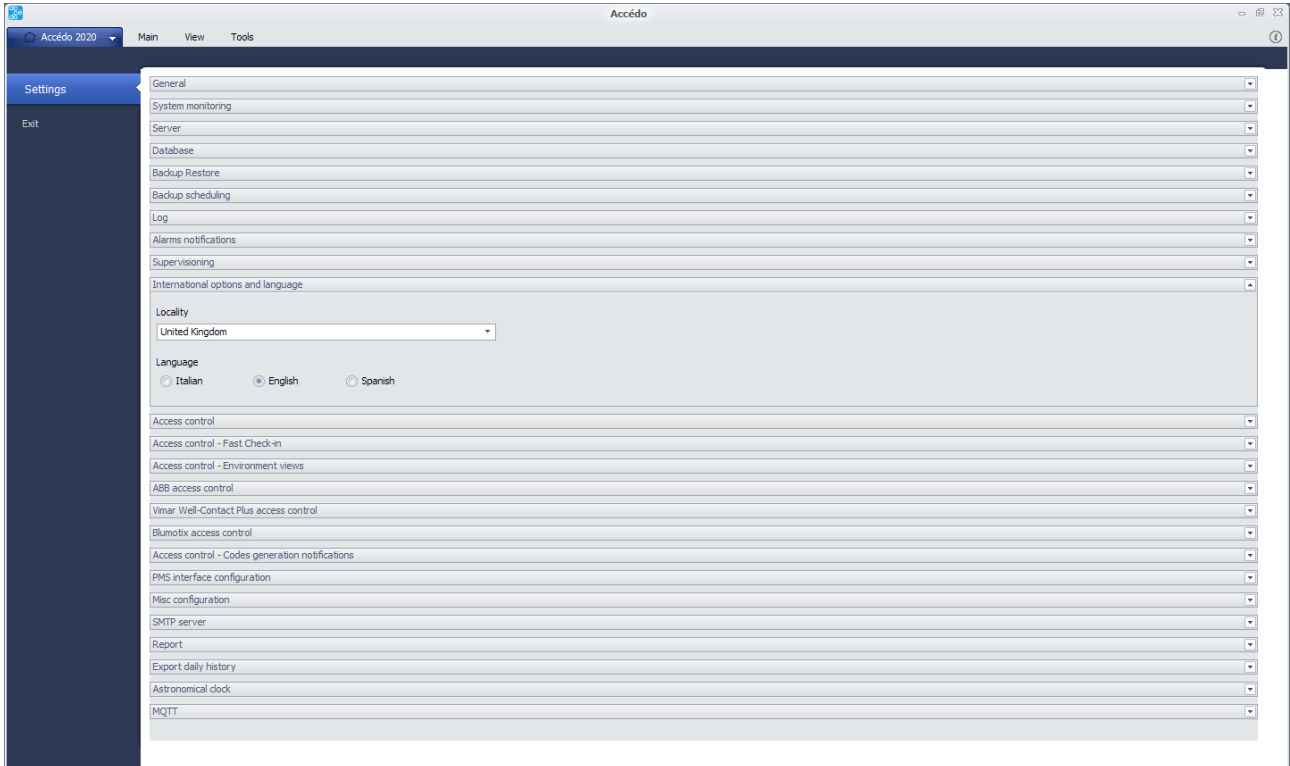


Figure 94 – Settings, International options and languages section

In the *International and Language Options* section you can choose the location with a combo box for the location and three buttons for the language.

- Location
- Language

Location allows you to choose the location as a country to inherit international options such as temperature units, decimal separator and other parameters. The possible locations are:

- Italy
- United Kingdom
- France
- Germany
- Spain

Language allows language selection. At the moment the application is available in:

- Italian
- English
- Spanish

17.10 Access control

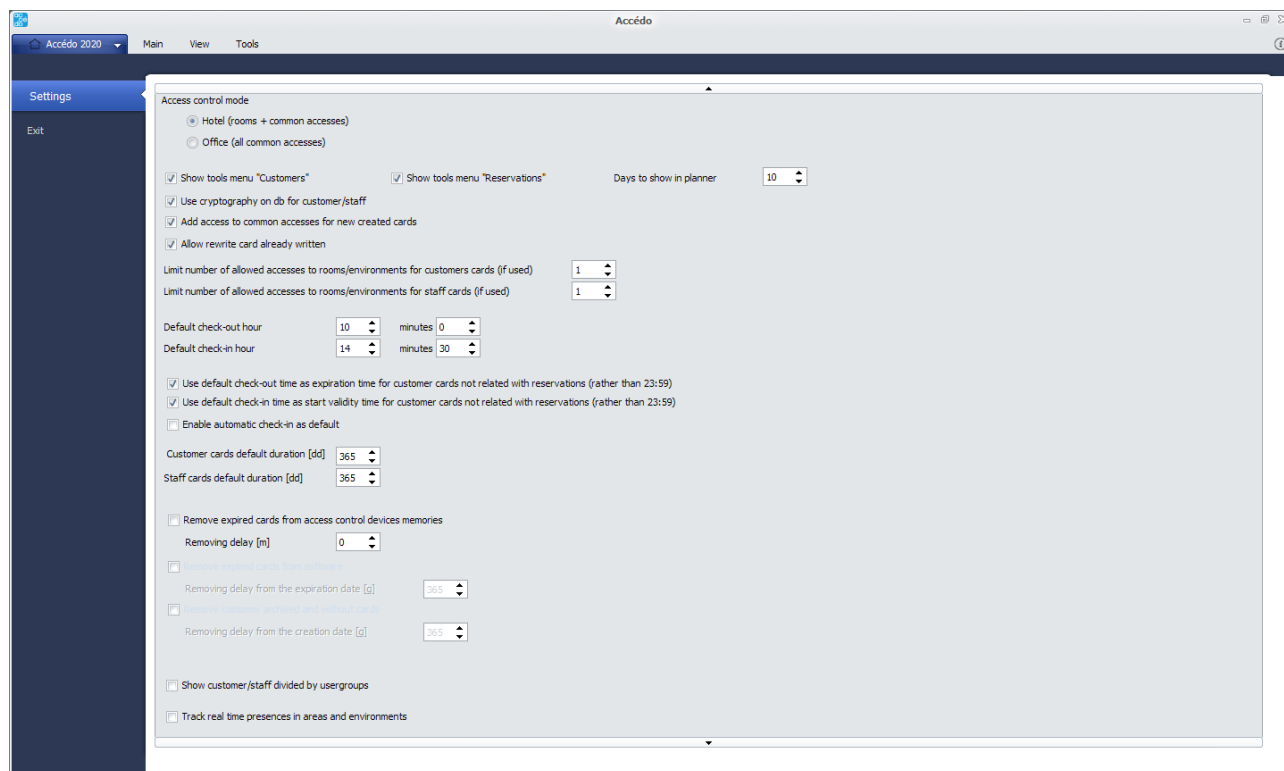


Figure 95 – Settings, Access Control section

In the *Access Control* section the user can configure different options regarding access control.

- Access control mode
- Show "Clients" tools menu
- Show "Personal" tools menu
- Show menu tools "Reservations"
- Add access to common access for newly created cards
- Room access limit allowed for customer keys (if applied)
- Room access limit allowed for personal keys (if applied)
- Now default check-out
- Default check-in time
- Use the default check-out time as expiry time for customer cards not related to reservations (instead of 23:59)
- Default duration customer card [dd]
- Default duration personal cards [dd]
- Remove expired customer cards from the access control device memory
- Removal delay [m]

Access control mode allows the selection of the type of access control between two options:

- Hotel (rooms + common access)
- Tertiary (all common areas)

Show menu tools "Customers" allows the user to select whether to show the menu to the customer or not.

Show "Personal" tools menu allows the user to select whether to show the menu to the staff or not.

Show menu tools "Reservations" allows the user to select whether to show the menu to the booking staff or not.

Add access to common accesses for new cards created allows the user to select whether to allow access to common accesses for new cards created or not.

Room access limit allowed for customer keys (if applied) allows the user to set the maximum number of room accesses for customer keys.

Room access limit allowed for personal keys (if applied) allows the user to set the maximum number of accesses to rooms and environments for customer keys.

Default check-out time allows the user to set the default check-out time.

Default check-in time allows the user to set the default check-in time.

Using the default check-out time as expiry time for customer cards not related to reservations (instead of 23:59) allows the user to select as expiry time for customer cards the check-out time that has been set above as default.

Default duration customer cards [dd] allows the user to set the number of days of default duration for customer cards.

Default duration of personal cards [dd] allows you to set the number of days of default duration of personal cards.

Remove expired customer cards from the memory of access control devices if the user selects this option, expired customer cards are removed from the memory.

Removal delay [m] is the delay time for removing cards from the memory after their expiration.

Remove expired customer cards from the access control system if the user selects this option, customer cards that have expired for more than n days are removed from the system.

Removal delay from the expiration date [g] is the time delay for removing cards from the system since their expiration.

Remove archived customers if the user selects this option archived customers without cards are removed from the system.

Removal delay from creation date [g] is the delay time for removing archived customers.

17.11 ekinex access control

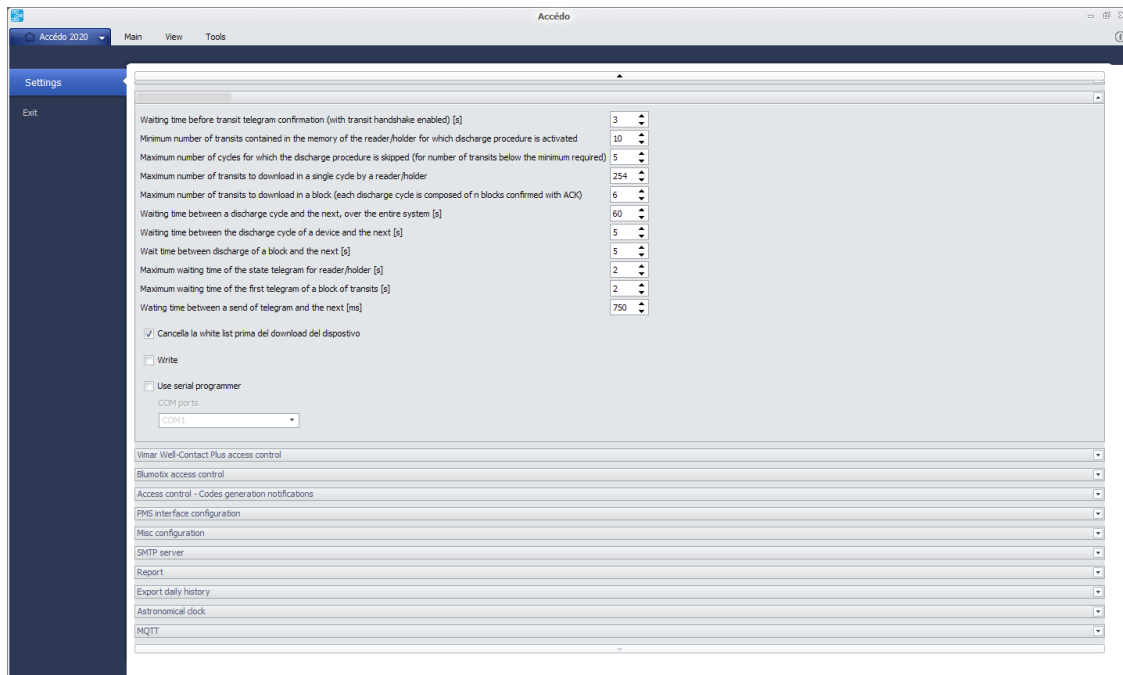


Figure 96 – Settings, ekinex Access Control section

In the accédo *Access Control* section the user has the possibility to set different options which are as follows:

- Waiting time before confirmation of a transit telegram (with transit handshake enabled) [s]
- Minimum number of transits contained in the reader/pocket memory for which the download procedure is activated
- Maximum number of cycles for which the discharge procedure is skipped (for fewer transits than the minimum required)
- Maximum number of transits to download in a single loop from a reader/pocket
- Maximum number of transits to unload in a block (each unloading cycle consists of n blocks confirmed with ACK)
- Waiting time between one discharge cycle and the next, on the whole system [s].
- Waiting time between one device discharge cycle and the next [s]
- Waiting time between unloading one block and the next [s]
- Maximum waiting time of the reader/task status telegram [s].
- Maximum waiting time for the first telegram of a transit block [s].
- Write on the cards the access permissions for special entrances
- Use serial card programmer

Waiting time before confirmation of a transit telegram (with transit handshake enabled) [s] allows you to set the number of seconds to wait before confirmation of a transit telegram.

Minimum number of transits contained in the reader/holder memory for which the download procedure is activated allows to set the minimum number of transits contained in the reader/holder memory.

Maximum number of cycles for which the download procedure is skipped (for fewer transits than the minimum required) allows to set the maximum number of cycles for which the download procedure is skipped.

Maximum number of transits to be downloaded in a single cycle from a reader/task allows to set the maximum number of transits to be downloaded in a single cycle.

Maximum number of transits to download in a block (each download cycle consists of n blocks confirmed with ACK) allows to set the maximum number of transits to download in a block.

Waiting time between one unloading cycle and the next, on the whole system [s] allows to set the number of seconds to wait between one unloading cycle and the next on the whole system.

Waiting time between one unloading cycle of one device and the next [s] allows to set the number of seconds to wait between one unloading cycle of one device and the next.

Waiting time between unloading one block and the next [s] allows you to set the number of seconds to wait between unloading one block and the next.

Maximum waiting time of the reader/holder status telegram [s] allows you to set the maximum number of seconds of waiting for the reader/pocket status telegram.

Maximum waiting time of the first telegram of a transit block [s] sets the maximum number of seconds of waiting for the first telegram of a transit block.

Write the access permissions for special access points on the cards [s] allows you to write the access permissions for special access points on the cards.

Use Serial pass programmer selected allows the user to select the COM Port through a combo box.

17.12 Management interface software configuration

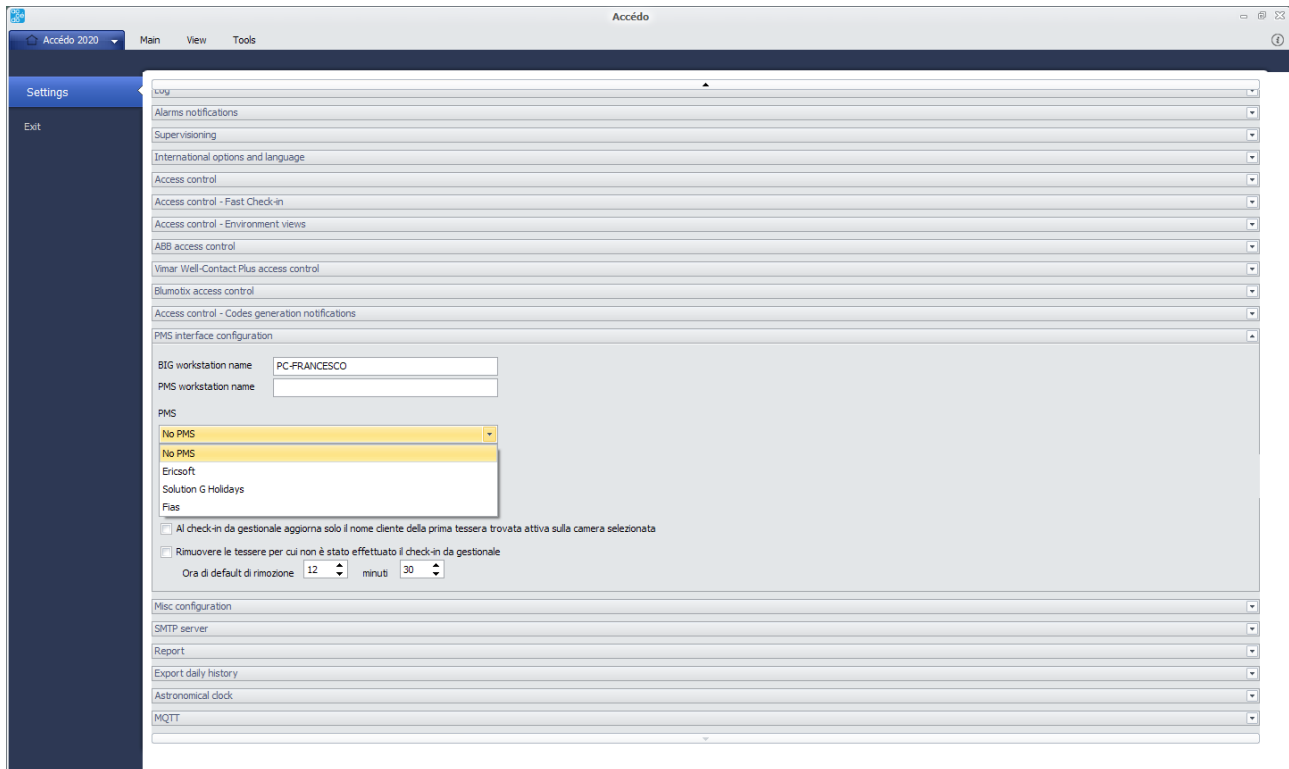


Figure 97 – Settings, PMS interface section

In the *Management Interface Configuration* section the user has the possibility to modify some interface options.

- Workstation name accédo
- PMS workstation name
- PMS

Accédo workstation name allows you to change the name of your accédo workstation.

PMS workstation name allows you to change the name of your PMS workstation.

PMS is a combo box that allows the user to select the PMS type.

17.13 Misc configuration

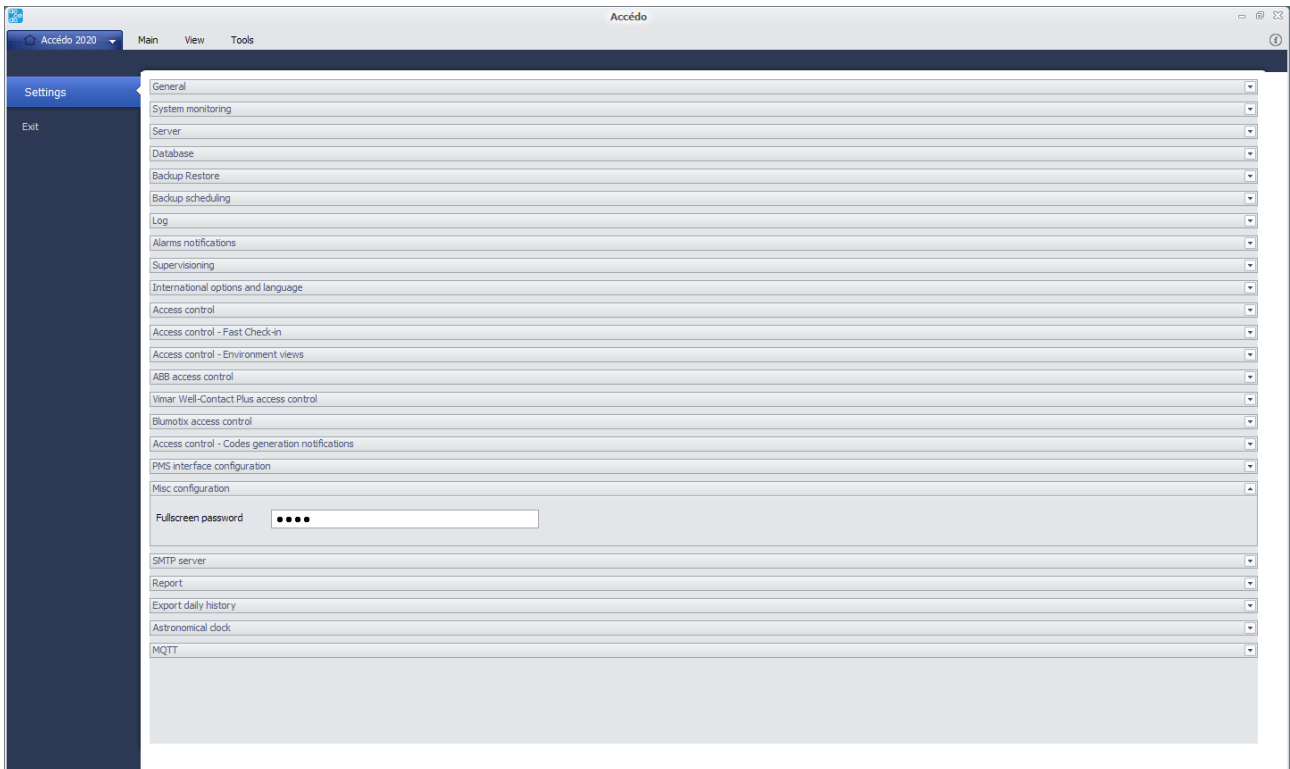


Figure 98 – Settings, Misc configuration section

In the *Miscellaneous Configurations* section the options available to the user are as follows:

- Fullscreen password

Fullscreen password the user has the ability to set a password for fullscreen mode.

17.14 SMTP server

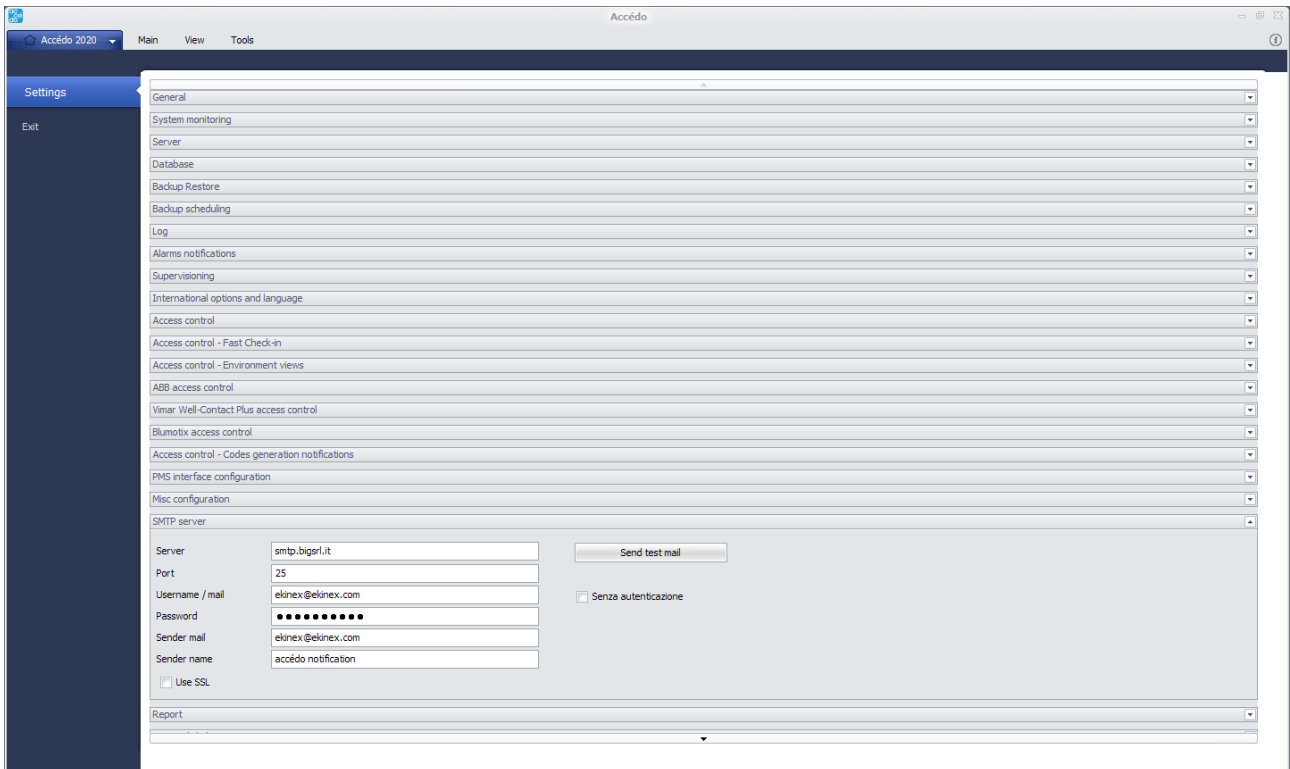


Figure 99 – Settings, SMTP server section

In the *SMTP Server* section the user has the possibility to set the SMTP server options:

- Server
- Door
- Username/mail
- Password
- Sender email address
- Sender name
- Use SSL

Server allows you to set the IP address of the server.

Port allows you to set the SMTP server port.

Username/mail allows you to set the username and mail of the SMTP server.

Password allows you to set the SMTP server password.

Sender email address allows you to set the sender's email address.

Sender name allows you to set the name of the sender.

Use SSL if enabled allows the user to use SSL certification.

17.15 Report

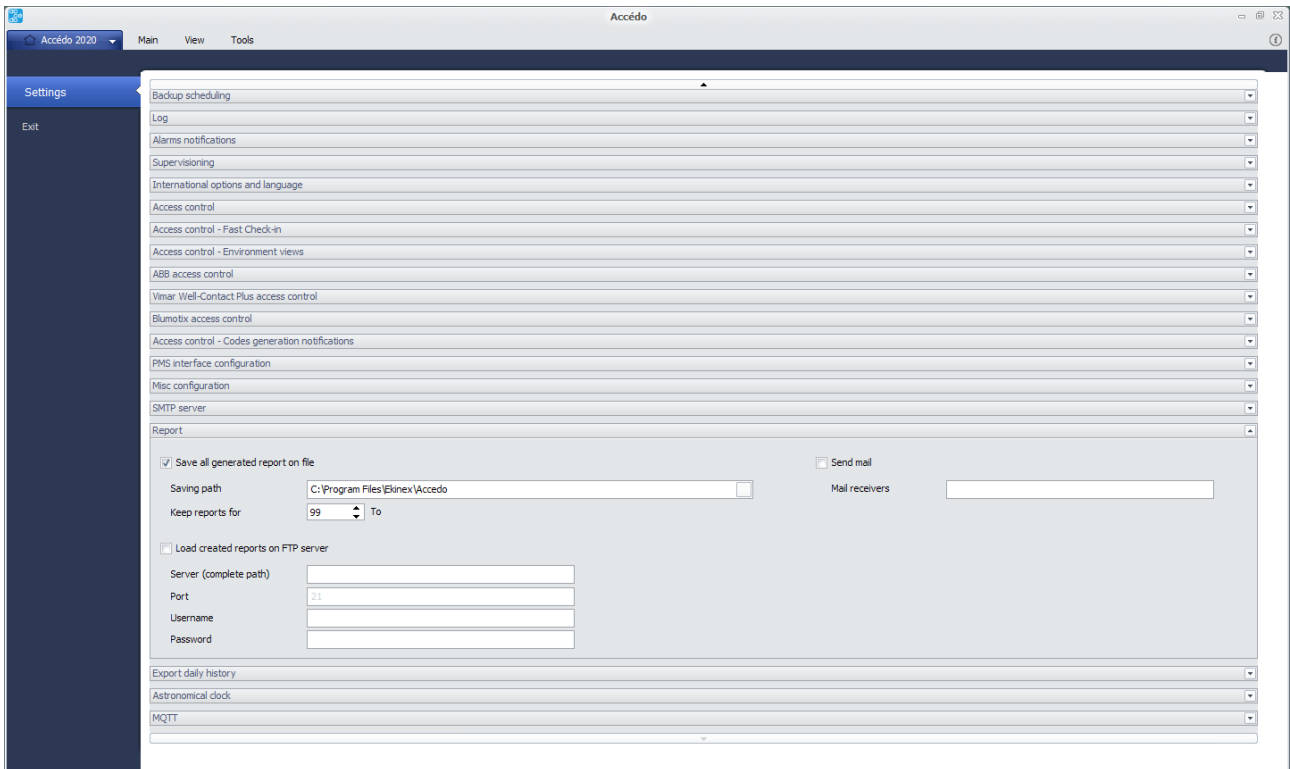


Figure 100 – Settings, Report section

In the *Reports* section the user has the option to set the report configuration options.

- Save generated reports to file
 - Rescue route
 - Keep report files for
- Upload generated reports to FTP server
 - Server (full path)
 - Door
 - Username
 - Password
- Sending emails
 - Email Recipients

Save the generated reports to file if this option is selected, it is allowed to set the saving path and the report file storage setting.

Save path allows you to set the save path for report files.

Keep report files to allow you to set the number of days the report files remain in memory.

Upload generated reports to FTP server enables uploading generated reports to FTP server.

Server (full path) allows you to set the IP address and FTP server name to upload report files.

Port allows you to set the port of the FTP server to upload report files.

Username allows you to set a username for the FTP server to upload report files.

Password allows you to set a password for the FTP server to upload report files.

Email if this option is selected the generated report file is emailed to the specified recipients.

Email recipients allows you to define the recipients to send the email to, separated by ';

17.16 Export daily history

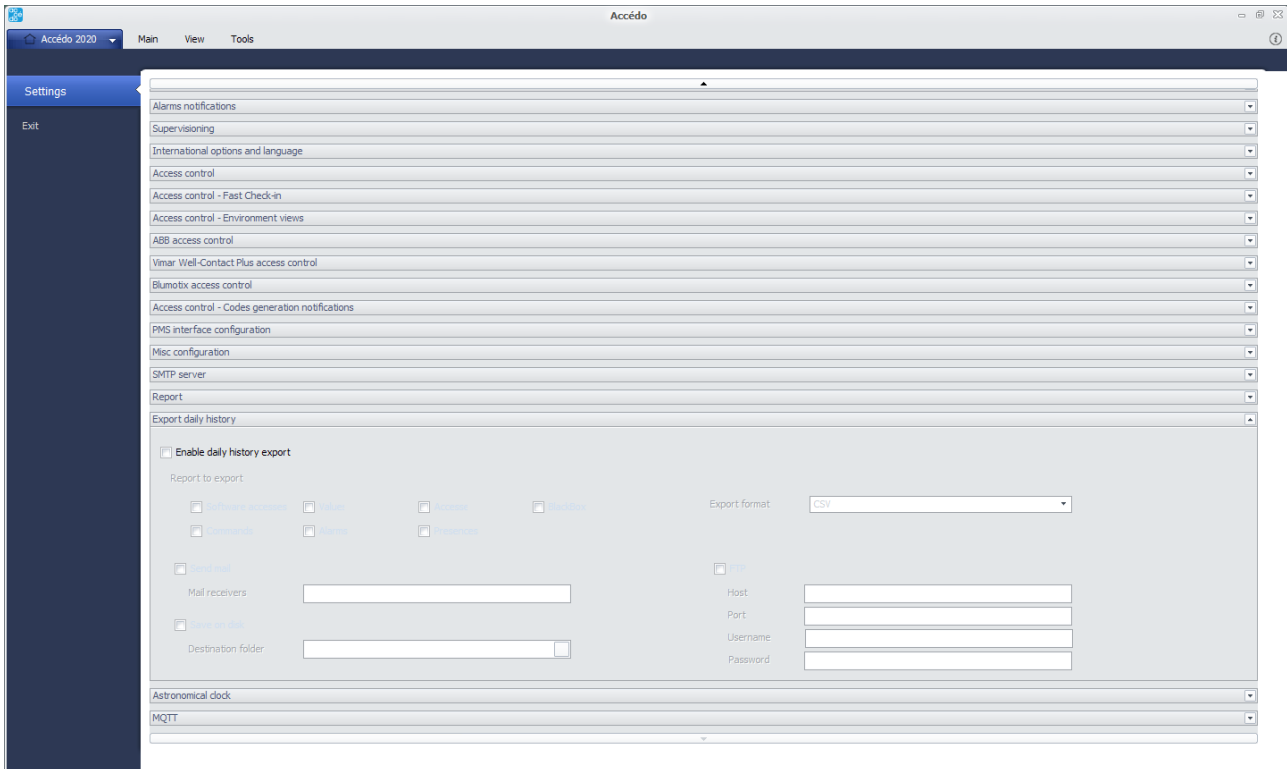


Figure 101 – Settings, Export daily history section

The *Daily History Export* section allows you to define which histories are to be exported daily and to configure the export mode.

- *Enable daily historical export*;
- *Historians* to export: list of exportable histories;
- *Export format*: file format to export: choice between csv, xml and json.
- *Send mail*: enable the selected histories to be sent by mail: if enabled, it is possible to define the recipients to be sent to (separated by ';'); the mailbox used for sending is the one configured in the SMTP Server section;
- *Saving on disk*: enable to save on disk the selected histories: if enabled, it is possible to define the destination folder for saving.
- *FTP*: enable the upload via FTP of the selected histories: if enabled, it is possible to define the *Host*, *Port*, *Username* and *Password* of the FTP server.

17.17 Astronomical clock

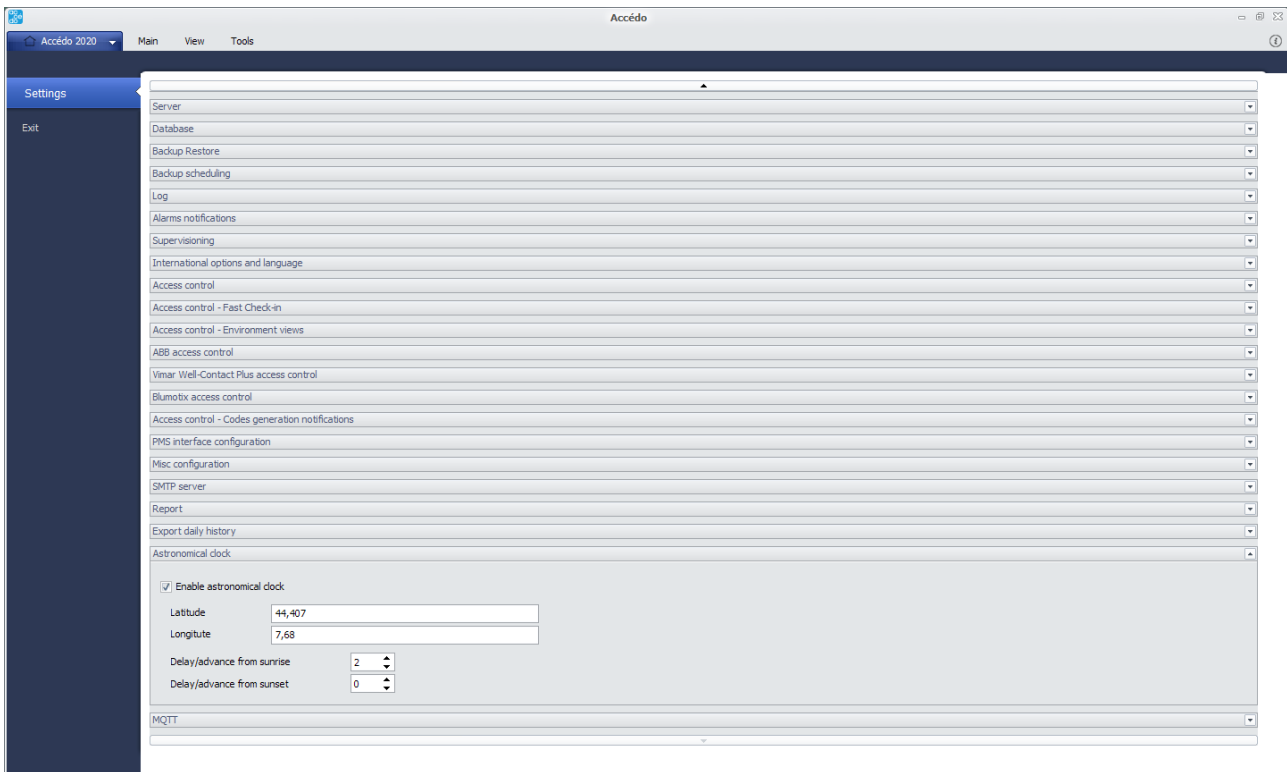


Figure 102 – Settings, astronomical clock

The astronomical clock is an instrument of accédo that allows you to automatically calculate the time of sunrise and sunset in a certain place according to its geolocation. These values are useful in case you want to perform a scenario at a time of day that is not fixed, but depends on sunrise or sunset, for example switching external lights on and off.

For the correct functioning of the astronomical clock it is necessary to define the reference position with its coordinates as in image 126 and restart master gateway and accédo.

In the object tree, under the node Variables, the following addresses appear:

- SunriseTime: the time of dawn.
- SunsetTime: the time of sunset.
- IsDay: enhanced to On if the current time is between SunriseTime and SunsetTime
- IsNight: enhanced to On if the current time is between SunsetTime and SunriseTime

If you want to run a logic at a certain time distance from the SunriseTime or SunsetTime you can use the settings "Delay/anticipate to sunrise" and "Delay/anticipate to sunset": these settings allow you to define an advance (if the value is negative) or a delay (if the value is positive) in minutes with respect to the reference time.

This results in the following addresses:

- Sunrise time with Offset: contains the time calculated as sunriseTime +/- delay/anticipate
- Sunset time with Offset: contains the time calculated as sunsetTime +/- delay/anticipate
- Sunrise Offset verified: Valued to On if the current time is equal to "Sunrise time with Offset".
- Sunset Offset verified: Valued to On if the current time is equal to "Sunset time with Offset".

It is therefore possible to build logics on the variation of "Sunrise Offset verified" and "Sunset Offset verified".

Example: Execution of the scenario "External lights on" half an hour before sunset.

1. Defining the latitude and longitude of the reference position.
2. Definition of the advance before sunset with value "-30".
3. Definition of a logic 'Switching on external lights 30min before sunset' whose only condition is 'Sunset Offset Verified = On'.
4. Association of the "External lights on" scenario to the newly built logic.

When the time [Sunset time - 30 minutes] is triggered, the address "Sunset Offset verified" becomes On and the logic is triggered by running the scenario. After one minute, the address "Sunset Offset verified" returns to Off.

18 BACKUP/RESTORE

18.1 Backup

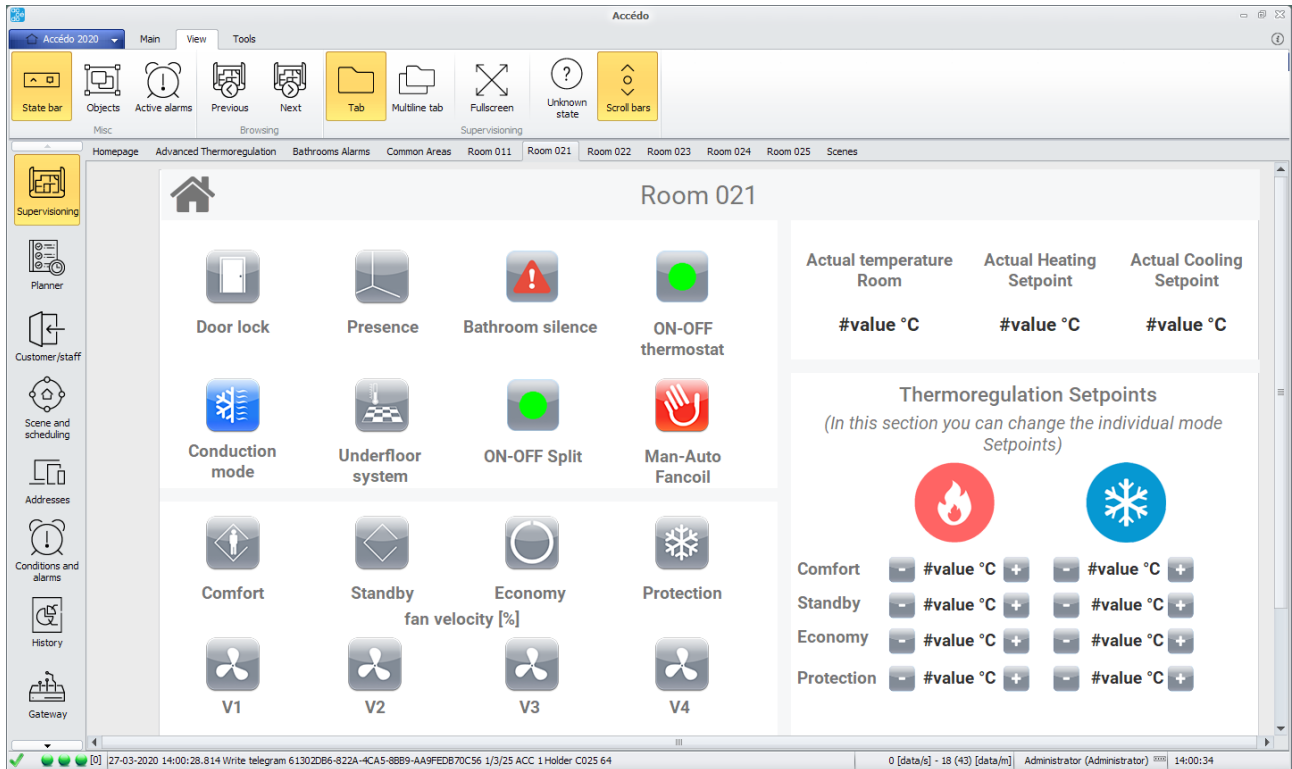


Figure 103 – project example for which backup is required

To make a backup of the software you have to open the drop-down menu in the top left corner.

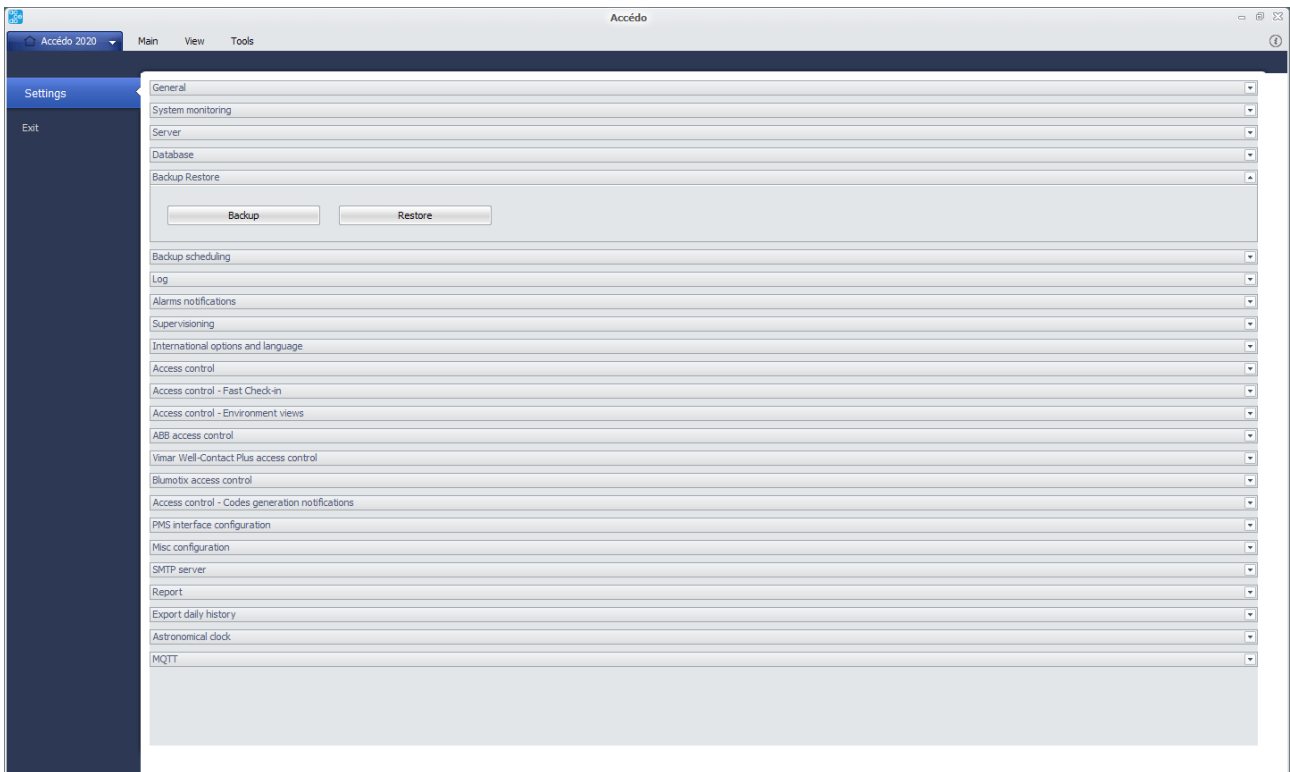


Figure 104 – Settings, Backup Restore section

Then you have to click on the Backup Restore section and start the Backup
 Then save your backup by giving it a name and clicking on Save

18.2 Restore

To restore the software you have to open the drop-down menu in the top left corner.
 Then you have to click on the Backup Restore section and start the Restore.
 Confirm for data overwriting.

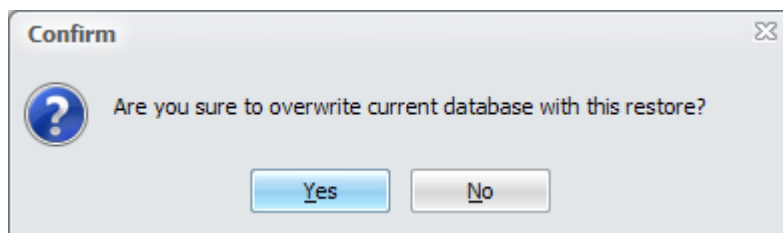


Figure 105 - Data overwriting confirmation window

19 SCENES AND SCHEDULING

19.1 Scenes

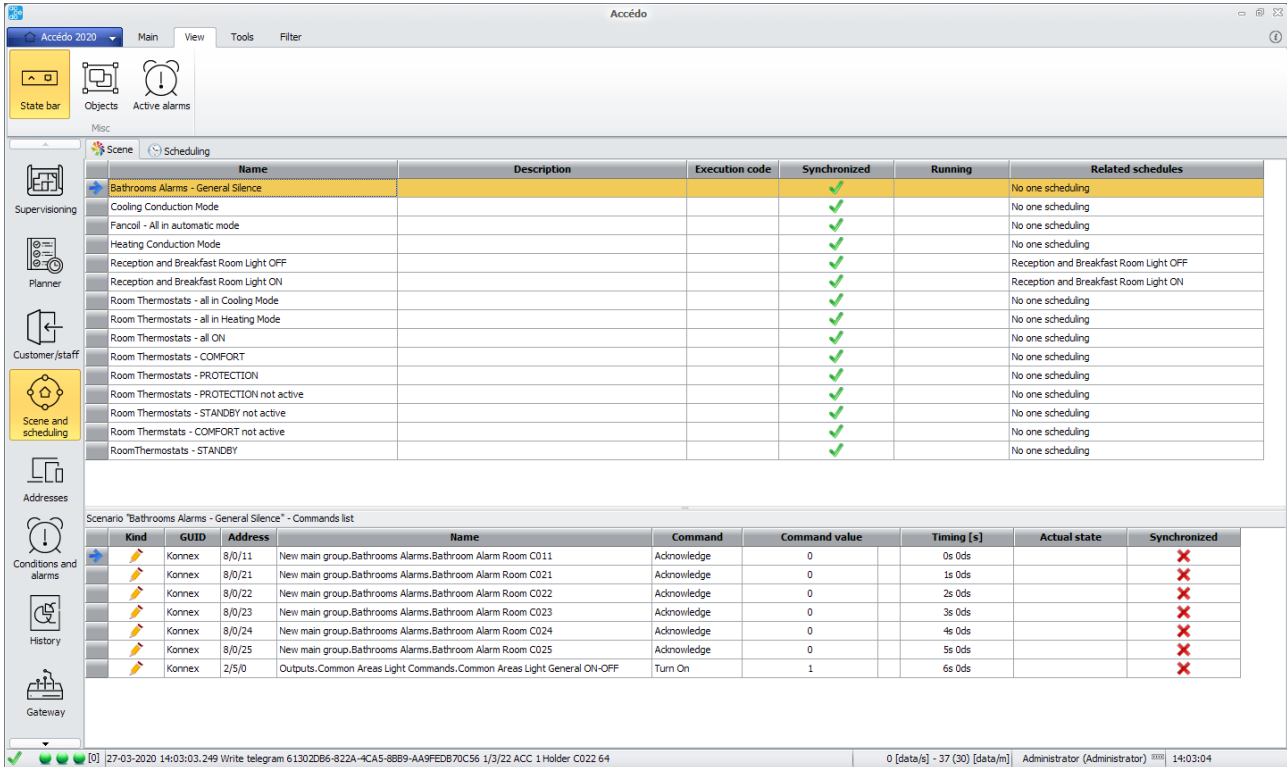


Figure 106 – Scene and scheduling, Scene tab

The options available when opening Scenes are:

- New
- Duplicate
- Delete
- Execute
- Stop
- Time-out
- Duplicate
- Delete
- Execute
- Move Up
- Move Down

New allows you to create a new scenario.

Duplicate allows you to duplicate the used scenario.

Delete allows you to delete the selected scenario.

Run allows you to run the selected scenario.

Stop allows you to stop the execution of the selected scenario.

Timer allows you to set the time interval between two or more selected commands.

Duplicate allows you to duplicate one or more selected commands.

Delete allows you to delete one or more selected commands.

Execute allows you to execute one or more selected commands.

Move Up allows you to move one or more selected commands up.

Move Down moves one or more selected commands down.

To select multiple commands, hold down the **Ctrl** key while left-clicking on the desired commands.

If you want to keep track of scenario synchronization via addresses you can add the SendRefresh_ScenarioSynch to True in the db in the SETTINGS table. In this way a virtual variable is generated for each scenario that tracks the synchronization status.

19.2 Scheduling

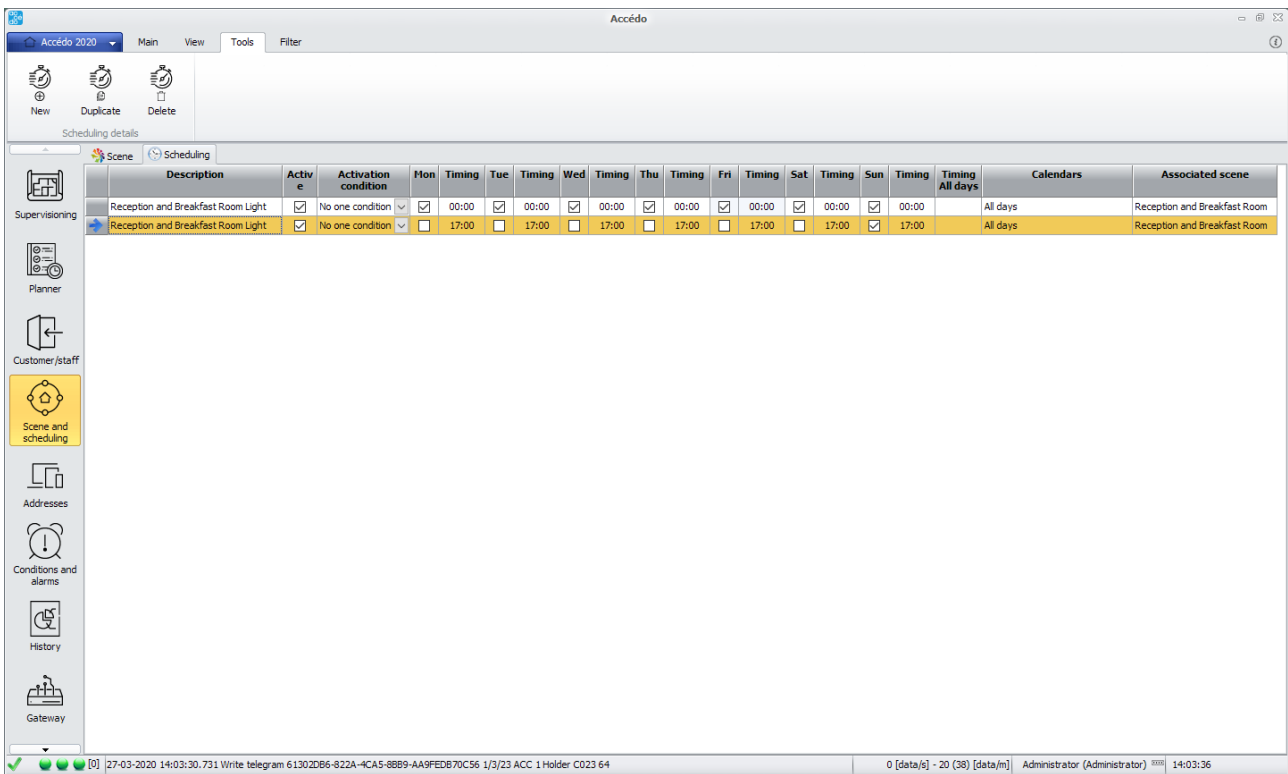


Figure 107 - Scene and scheduling, scheduling tab

In the schedules screen you can see the schedules you have created and the function you have performed.

- New
- Duplicate
- Delete

New allows you to create a new schedule.

Duplicate allows you to duplicate any schedule on the screen and just selected.

Delete allows you to delete a schedule.

19.3 Automatic writing between DB

If you need to perform readings and writes between accédo and other DBs you can use the SQL_COMMANDS_SCHEDULER table in which are indicated

- CommandText: command to execute
- ExecutionMode: between

```
public enum SQLCommand_ExecutionMode
{
    OnServiceStart = 0,
    Periodically = 1,
    OnServiceStop = 2
}
```

- Interval: command execution interval
- Interval_UM: Unit of measure of the execution interval

BIGOmnia service at startup is responsible for reading the table and executing the commands according to their setting.

20 ADDRESSES

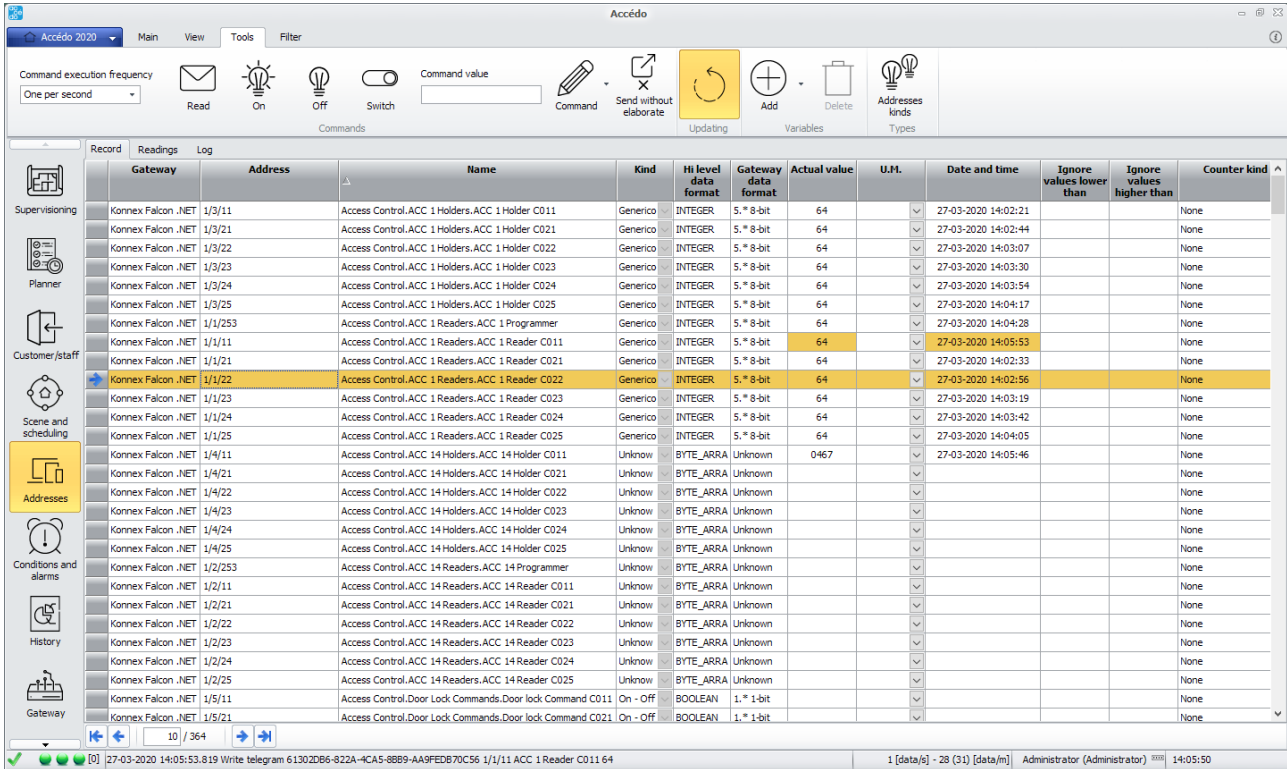


Figure 108 – Address section

If you select **Devices** from the side menu, this screen appears first. To make devices appear, select the **Filters** section (circled in photo) from the top bar.

In the next picture you will see how to filter and what types of filters you can use.

As you can see, various connected devices have appeared that you can filter by:

- Gateway
- Address
- Name

After selecting which filters to use (you can also not use any filters leaving Gateway set at all), click on **Filter**, circled in the picture, which makes the connected devices appear.

You can also export the list of the user's connected devices using the Export function next to Filter. In this way there is the possibility to have a file external to the program to verify the connected devices at a given time.

20.1 Field details

20.1.1 Data

- Gateway

- Name of the gateway that manages the address
- Address
- Group address
- Full name of the address, including the name of all levels in which the address is entered
- High level data format
- Identifies the macro typology of the value that can take the address
- Gateway data format
- Particularly useful for KNX gateways, it expresses the data-point type DPT
- Current value
- Last known value
- U.M. Unit of measurement
- Date and time
- Instantaneous recognition of the last value
- Ignore values below
- Optional; if present it indicates the lowest value allowed for the address: values lower than this will be ignored and not transmitted by the gateway
- Ignore values above
- Optional; if present it indicates the higher value allowed for the address: values higher than this will be ignored and not transmitted by the gateway.
- Counter type. If the address represents a counter, on which reports/consumption/cost analysis will be built, it is possible to indicate the type of counter, on the basis of which such reports/consumption analysis will be based.

20.1.2 Readings

- Reading at startup. If selected, the address will be read when the Windows service of the relevant gateway is started.
- Periodic reading. If selected, the address will be read periodically directly from the relative gateway; if the periodic reading is introduced, the minimum change per send (based on the modified address format) and the maximum non-sending window (300 sec.) are automatically modified to avoid bus overload (the change is introduced for all addresses belonging to the same Modbus range).
- Reading interval [s]. If periodical reading is enabled, it specifies the time interval in seconds between one reading and the next; optionally required when associating the address with a data processing unit.
- Automatic reading interval [s]. Read only; Indicates any interval of readings imposed by the software automatically, for example if the address is part of an alarm condition for which verification time is active
- Modbus Range ID. Read only; valued only in the case of Modbus address; it represents the identification of the group of which the address is part: in practice, at the Modbus gateway only one reading is enough to have the value of all addresses with the same ModbusRangeID; this means that it is not recommended to have several addresses in reading at startup and/or periodically with the same ModbusRangeID, only one is enough for ModbusRangeID, with the lower interval.

20.1.3 Log

- Transit Log. If selected, it involves saving the measured values of the address, which will then be available in the Report - Values section.
- Offset Log. Optional; identifies any value that will be added to the value detected, e.g. in the case of meters, if they have lost or wrong progressive values
- Reset after reset. If selected, it automatically checks the detected values, which must always be progressive; if this is not the case, the LogOffset value is automatically set as the difference between the last detected value and the current and then added to it.
- Minimum value change per log. Specifies the minimum variation of the current value from the last detected (+/-) for which to save the value in the archive, if Log Transiti is selected.
- Maximum non-log window [s]. Specify the number of seconds after which the address value will be saved back into the archive, assuming Log Transiti is selected, ignoring any check on the minimum change per log
- Minimum change in value per shipment. Specifies the minimum change in the current value from the last detected (+/-) for which the gateway will notify the connected clients.
- Maximum non-sending window [s]. Specifies the number of seconds after which the address value will be sent back to the connected clients, ignoring any control over the minimum change per send
- Offset. Value added to the current value, before the various checks on send/log/signature
- Factor. Multiplication value (set 0.1 to divide by 10, for example) applied to the current value, before the various checks on send/log/signature
- PLEASE NOTE: the resulting value will be = (Current Value x Factor) + Offset

20.2 Address types

The types of addresses can be configured by clicking on the appropriate button in the address section:

Each address in the system is associated with a typology (identified by a name) that defines it:

- Methods: the commands that can be used on that address; the methods are in the form Label=Value, separated by |. For example for the on-off command address of a light bulb the methods could be "On=1|Off=0".
- States: the value that can assume that address; states are in the form Label=Value, separated by |. For example for the on-off status address of a light bulb the states could be "On=1|Off=0".
- High level data format: The general data format of the address.
- Gateway data format: The declination of the high-level data format based on the type of gateway to which the address is associated.
- Normal image: Default image used as normal image in supervision for the buttons to which an address of this type is associated as status address.
- Pressed image: default image used as a pressed image in supervision for buttons associated with this type of address as status address.
- Image On: default image used as the "ON" status image in supervision for buttons associated with this type of address as status address. (enabled only for types with BOOLEAN high level format)
- Image Off: Default image used as the "OFF" status image in supervision for the buttons to which an address of this type is associated as the status address. (enabled only for BOOLEAN high-level format types).
- Status images: according to the defined states it is possible to associate for each state the corresponding image, which will be used as status images in supervision for the buttons to which an address of this type is associated as status address. (enabled only for types with high level format not BOOLEAN).

- Default action: method (among those defined) used by default when a button is pressed with an address of this type as status address.

The address types can be filtered according to the gateway they belong to, the language (which defines different methods and states), the name, the high-level type and the System or Custom distinction.

The System types are the ones present by default in accédo: for these types you can modify only the name, the images, the default action and the labels of the methods and states.

The Customized typologies are those inserted by hand by the user: these typologies are completely customizable.

From the action menu you can:

- Add a new type of address: the type is born as customized and is associated to the gateway selected at that time.
- Delete a pre-existing type: this is only possible if the type is not system.
- Import/export types: this allows you to insert new devices or update data (e.g. labels and images) of pre-existing types, without having to redo the whole configuration each time. To export a set of typologies, simply select the types of interest and press the export button, through which the export path is defined. The export generates a .JSON file and a folder of images.
- Propagate modifications: if a series of buttons associated to a type of address whose data has been changed (e.g. images) have been inserted in supervision, it is possible to apply the modification to all these objects; just select the types to propagate and press *Propagate modifications*. If you want to exclude a certain button from the massive modification you must set its *DefaultImagesUsed* property to the False value, indicating that it does not use the default images and therefore must not be updated. All the buttons created before the update containing the device type management have the property *DefaultImagesUsed* = false; all those created afterwards start with *DefaultImagesUsed* = true.

21 LOGICS AND ALARMS

	Group	Description	Active	Activation condition	Reporting	Log	Alarm kind	Last evaluation	Datetime last evaluation
Supervising	Bathrooms Alarm Group	Bathroom Alarm C011	<input checked="" type="checkbox"/>	No one condition	Reports always	<input checked="" type="checkbox"/>	Not defined	!	27-03-2020
	Bathrooms Alarm Group	Bathroom Alarm C021	<input checked="" type="checkbox"/>	No one condition	Reports always	<input checked="" type="checkbox"/>	Not defined	!	27-03-2020
	Bathrooms Alarm Group	Bathroom Alarm C022	<input checked="" type="checkbox"/>	No one condition	Reports always	<input checked="" type="checkbox"/>	Not defined	!	27-03-2020
	Bathrooms Alarm Group	Bathroom Alarm C023	<input checked="" type="checkbox"/>	No one condition	Reports always	<input checked="" type="checkbox"/>	Not defined	!	27-03-2020
	Bathrooms Alarm Group	Bathroom Alarm C024	<input checked="" type="checkbox"/>	No one condition	Reports always	<input checked="" type="checkbox"/>	Not defined	!	27-03-2020
	Bathrooms Alarm Group	Bathroom Alarm C025	<input checked="" type="checkbox"/>	No one condition	Reports always	<input checked="" type="checkbox"/>	Not defined	!	27-03-2020
	Split Errors Group	Error Alarm Split C025	<input checked="" type="checkbox"/>	No one condition	Reports always	<input checked="" type="checkbox"/>	Not defined	!	27-03-2020
Customer/staff	Split Errors Group	Error Alarm Split C021	<input checked="" type="checkbox"/>	No one condition	Reports always	<input checked="" type="checkbox"/>	Not defined	!	27-03-2020
	Split Errors Group	Error Alarm Split C022	<input checked="" type="checkbox"/>	No one condition	Reports always	<input checked="" type="checkbox"/>	Not defined	!	27-03-2020
	Split Errors Group	Error Alarm Split C023	<input checked="" type="checkbox"/>	No one condition	Reports always	<input checked="" type="checkbox"/>	Not defined	!	27-03-2020
	Split Errors Group	Error Alarm Split C024	<input checked="" type="checkbox"/>	No one condition	Reports always	<input checked="" type="checkbox"/>	Not defined	!	27-03-2020
	Bathrooms Alarm Group	General Bathrooms Alarm State	<input checked="" type="checkbox"/>	No one condition	Reports always	<input checked="" type="checkbox"/>	Not defined	!	27-03-2020
	Logics Group	Bathroom Alarms logic OR	<input checked="" type="checkbox"/>	No one condition	Reports always	<input checked="" type="checkbox"/>	Not defined	!	27-03-2020
	Logics Group	FM Room -> AUTO/MAN Split C011	<input checked="" type="checkbox"/>	No one condition	Variation reporting	<input checked="" type="checkbox"/>	Not defined	!	27-03-2020
	Logics Group	FM Room -> AUTO/MAN Split C021	<input checked="" type="checkbox"/>	No one condition	Variation reporting	<input checked="" type="checkbox"/>	Not defined	!	27-03-2020
	Logics Group	FM Room -> AUTO/MAN Split C022	<input checked="" type="checkbox"/>	No one condition	Variation reporting	<input checked="" type="checkbox"/>	Not defined	!	27-03-2020
	Logics Group	FM Room -> AUTO/MAN Split C023	<input checked="" type="checkbox"/>	No one condition	Variation reporting	<input checked="" type="checkbox"/>	Not defined	!	27-03-2020
	Logics Group	FM Room -> AUTO/MAN Split C024	<input checked="" type="checkbox"/>	No one condition	Variation reporting	<input checked="" type="checkbox"/>	Not defined	!	27-03-2020
	Logics Group	FM Room -> AUTO/MAN Split C025	<input checked="" type="checkbox"/>	No one condition	Variation reporting	<input checked="" type="checkbox"/>	Not defined	!	27-03-2020
	Logics Group	ON-OFF Clima Vel 0 C021	<input checked="" type="checkbox"/>	No one condition	Reports always	<input checked="" type="checkbox"/>	Not defined	!	27-03-2020
	Logics Group	ON-OFF Clima Vel 0 C022	<input checked="" type="checkbox"/>	No one condition	Reports always	<input checked="" type="checkbox"/>	Not defined	!	27-03-2020
	Logics Group	ON-OFF Clima Vel 0 C023	<input checked="" type="checkbox"/>	No one condition	Reports always	<input checked="" type="checkbox"/>	Not defined	!	27-03-2020
	Logics Group	ON-OFF Clima Vel 0 C024	<input checked="" type="checkbox"/>	No one condition	Reports always	<input checked="" type="checkbox"/>	Not defined	!	27-03-2020
	Logics Group	ON-OFF Clima Vel 0 C025	<input checked="" type="checkbox"/>	No one condition	Reports always	<input checked="" type="checkbox"/>	Not defined	!	27-03-2020

Figure 109 – Logic and Alarm section

By clicking on **Logics and Alarms** from the side menu this screen appears representing the logics and alarms activated at this time.

Columns detail:

- : indicate whether the line corresponds to a logic or an alarm;
- Group: reference group for logic/alarm; groups can be defined through the appropriate tab;
- Description:
- Active:
- Activation condition: used to start the evaluation of a logic only if another logic is true;
- Signal: Always signal indicates that the signal linked to the logic/alarm is executed every time an address in the logic is updated; Change signal indicates that the signal linked to the logic/alarm is executed only if at the address change the new evaluation of the logic is different from the previous one.
- Log: to store the evaluation of the logic/alarm in the relative history;
- Alarm type: to categorize alarms;
- Last evaluation:
 - the last evaluation resulted in False;
 - the last evaluation resulted in True;
 - the last evaluation found an error in the composition of the logic (e.g. you are making the or between 2 strings) or some address of the logic is not valued.
- Date of last evaluation: the date on which it was last evaluated.

On this page there are several possibilities that are:

- New logic: allows you to create a new logic;
- New alarm: allows you to create a new alarm
- Duplicate: allows you to duplicate the selected logic. After pressing the button the dynamic address duplication mask is presented, so that you can duplicate the logic by modifying the addresses as you like. The address variation applies both to the addresses present in the condition and to the commands in case of verification, non-verification, reset and taking vision.
- Delete: allows to delete the selected logics
- Definition: allows you to change the definition of the logic (visible in detail in the next image)
- Generate KNX alarms: generates one alarm for each KNX address defined with Alarm type. If there is already an alarm associated with that address and containing only one condition of the type "ADDRESS = 0" or "ADDRESS = 1" the alarm generation does not regenerate that alarm. All the generated alarms have as alarm value the value 1 which can be changed by opening the alarm definition.

By clicking on Definition you can change the logic/alarm structure.

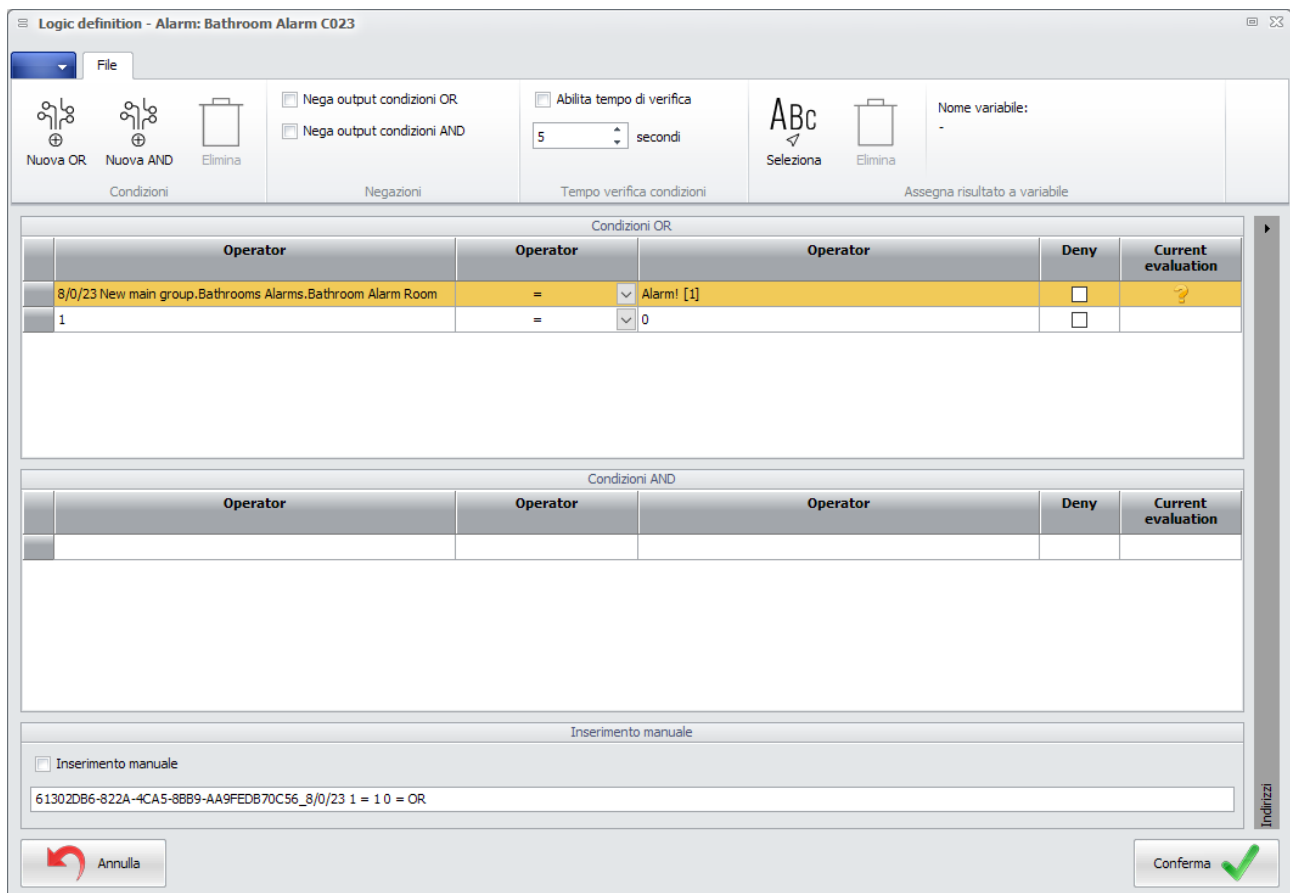


Figure 110 – Alarm logic definition

Allows you to compare or make operations between two variables with RPN logic. The user to give a value to the inserted operand can right click on the operand to insert values through the menu that appears.

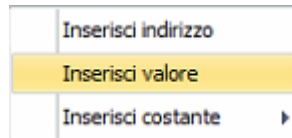


Figure 111 – popup on operand field

Alternatively, you can drag and drop the addresses directly from the address tree on the right into the relevant grid. If the address is dragged into the empty area of the grid a new condition is added, but if you drag into the operand of an existing condition that operand is replaced.

In the top bar there is the possibility to configure some parameters, deny the output values of AND and OR conditions by checking the desired box, set a number of seconds to check if the conditions entered are true or false and define an output variable that contains the result of the logic.

The current evaluation column is filled in as follows:

- the condition is currently False;
- the condition is currently True;
- an error has been detected in the condition (e.g. you are making the or between 2 strings) (Type mismatch)
- one of the addresses of the condition is not valorized; clicking on the symbol starts reading that address.

It is also possible to filter alarms and logics through the appropriate item in the top menu. Let's see an example image.

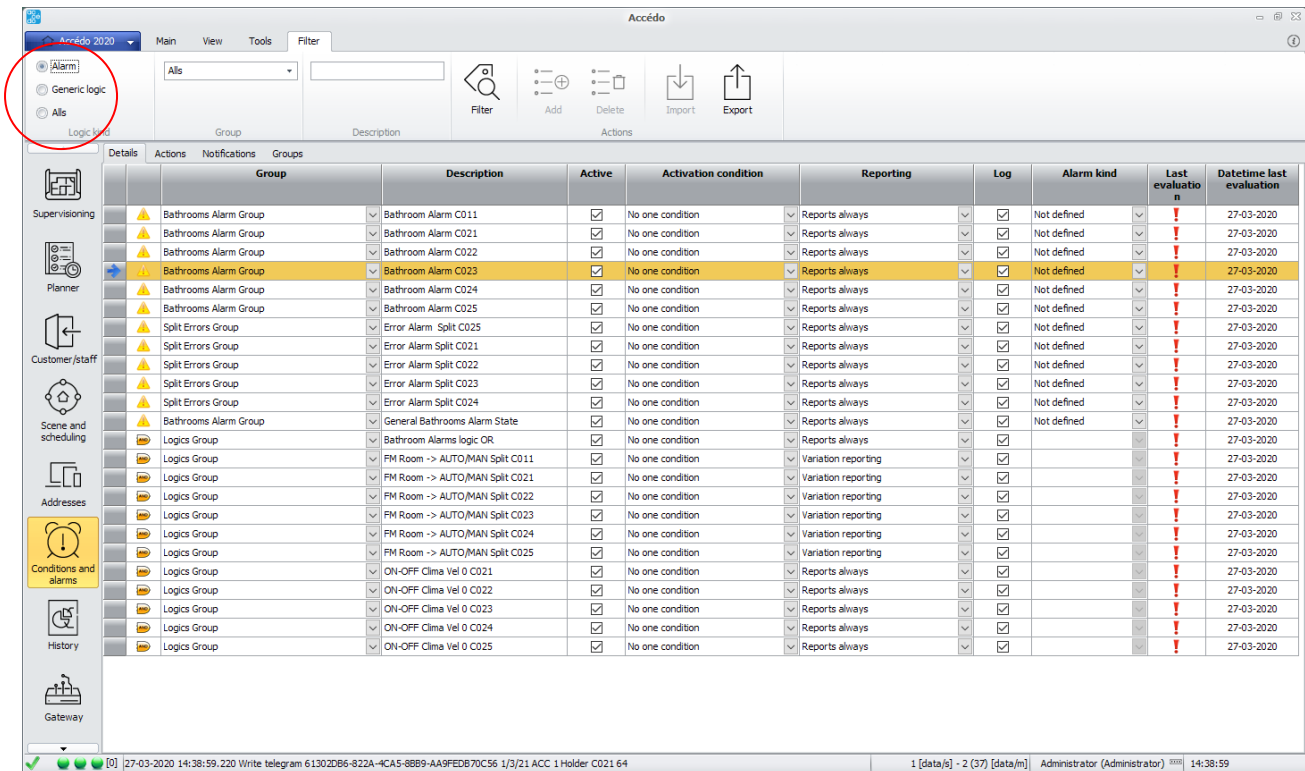


Figure 112 – Filtering alarm list

We can filter by **Alarm**, **General Logic** or **All**.

Then alarm will show us only the alarms, logic generic all cases of logic or display everything by filtering everything. After selecting the type of filter press Filter to display the desired list.

21.1 RPN notation

The Polish reverse polish notation (RPN) is a syntax used for mathematical formulas and is due to JanLukasiewicz, 1958. With RPN notation it is possible to perform any kind of operation, with the advantage of eliminating the problems due to parentheses and precedence of the operators (first the division, then the addition, etc...). Some professional calculators use RPN because it avoids the annotation of intermediate results during operations. In the Polish inverse notation, also called post-fixed notation in contrast to the normal fixed notation, first the operands are entered and then the operators: an example of RPN is $3\ 2\ +$ which is equivalent to the classic $3 + 2$, or $10\ 2\ /$ which gives 5.

When you use the RPN notation, you have a stack on which the operands accumulate: first you stack the 3, then the 2. An operator picks from the top of the stack all the operands he needs, executes the operation, and reposit the result. The lowest element is always the left operand. If the complete expression is correct, at the end of all the operations on the stack you will have only one element, the final result.

This stack allows, as already said, to avoid the use of parentheses to prioritize the operations, it is enough to insert in the left part of the formula all the operands of the operations with more external parentheses, in the middle the most elementary operations, on the right all the operators of combinations of the results of the central operations with the operands already present. In fact, there are conversion algorithms from fixed notation to post-fixed notation and vice versa. As you can see, RPN is easily implemented on computers.

An example: $(10 * 2) + 5$ becomes $5\ 10\ 2\ *\ +$

Before multiplication are present on the stack 5, 10, 2. The "*" retrieves the first two elements (10, 2) multiply them and modify the stack so that it contains 5, 20. Operation "+" adds 5 and 20, now in the stack, replacing them with the result: 25.

Other more complex examples: $((10 * 2) + (4 - 5)) / 2$ in RPN will be $10\ 2\ *\ 4\ 5\ -\ +\ 2\ /$
 $(7 / 3) / ((1 - 4) * 2) + 1$ becomes $1\ 7\ 3\ /\ 1\ 4\ -\ 2\ *\ / +$ or $7\ 3\ /\ 1\ 4\ -\ 2\ *\ / 1\ +$

The reverse Polish notation takes its cue from the simple Polish notation, in which the operators are placed before the operands (so: $+ 1\ 2$ instead of $1\ 2\ +$), but only the first one is easily implemented electronically or via software, and has therefore become much better known.

21.2 RPN notation in accédo

The elements of the syntax used in accédo that allow you to write logic in RPN notation are as follows:

Constants

BEFOREYESTERDAY, YESTERDAY, TODAY, TOMORROW, AFTERTOMORROW (1)

MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, SATURDAY, SUNDAY (2)

NOW (current date and time, in HH:MM format)

HOUR (value between 0 and 23), MINUTE (value between 0 and 59), DAY(value between 1 and 31),
MONTH(value between 1 and 12)

Value

Based on the address present in the condition, the values that the address can assume are presented.

Address

After right-clicking and selecting enter address, the screen to enter an address appears to the user.

Indirizzo.

Operators

The operators that the user has the possibility to use are the following:

<

>

=

NOT

AND

OR

Timer: stops the logic evaluation for N seconds and at the end returns the M value in the stack; it takes two parameters N and M.

Locking Timer

Break

Interval: makes the condition true only for one second every N; it takes the N parameter as input.

+

-

*

/

ABS: associated with a single operand returns its absolute value (ES RPN. VALUE ABS)

CALENDAR: returns true if the indicated day is present in the indicated calendar (ES RPN. TODAY IDCALENDAR CALENDAR)

21.3 Active alarms

21.3.1 Alarms types and visibility of active alarms

The alarms defined in the configuration section are triggered when the associated logics become true. From that moment on, the alarm is considered to be in progress.

The alarm triggered can change its status to one of the following:

- Silenced Alarm: An alarm triggered that a user has seen.
- Returned alarm: A triggered alarm whose associated logic has become false.
- Alarm reset: An alarm no longer in progress, reset by the user.

Alarms in progress, silenced, and returned are visible through the active alarm grid at the bottom of the screen. Reset alarms are not visible in that grid, but only in the alarm history.

The visibility of the grid of active alarms is managed through the Active Alarms button in the display menu.

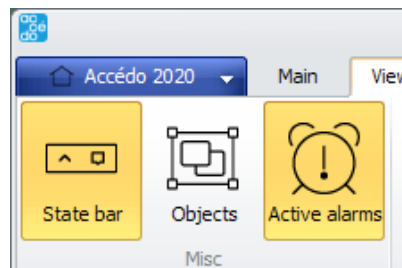


Figure 113 – toolbar to visualize Alarms




Active alarms							
Date and time	Description	State	Note	Take vision time	Take vision user	Silence	Reset
[27-03-2020 14:40:22.321 Write telegram 61302DB6-822A-HCA5-8B89-AA9FEDB70C56 1/1/25 ACC 1 Reader C025 64]							
					2 [data/s] - 18 (41) [data/m]	Administrator (Administrator) [1111]	14:40:26

Figure 114 – Alarm grid active

When you click on the Active Alarms button, the grid of active alarms is filled with the most serious type of alarms (excluding reset alarms):

- if there are triggered alarms, the grid is populated with these alarms;
- if there are no triggered alarms but there are silenced alarms, these are shown;
- if there are no alarms triggered or silenced, but there are some returned, the grid is populated with these alarms;
- if there are no alarms of any type, the empty alarm grid is shown.

The presence or absence of alarms belonging to one of the three types involved is visible on the left side of the status bar (whose visibility is managed by the appropriate button in the display menu): for each type the associated alarm icon and the number of alarms present of that type ([n]) are shown. If there are no alarms of a certain type, the icon is hidden. The associated icons are:

-  [n] : Alarms *in progress*
-  [n] : Alarms *tacitated*
-  [n] : Allarmi *returned*

As said before, the click on the *Active Alarms* button populates the grid of the most serious type of alarm present at the moment of the click. It is possible to view the other types of alarms present by double clicking on the corresponding icon in the status bar.

21.3.2 Active alarms grid

The grid of active alarms contains the following information:

- Date and time: instant when the alarm was triggered.
- Description: name of the alarm as defined during configuration.
- Status: current status of the alarm.
- Note: note entered by the user during viewing.
- Time of viewing: date and time of viewing.
- Viewing user: name of the user who viewed the alarm.
- Silent: Silence button; allows the user to view the alarm and enter the note. The viewing button is active only in the current alarm grid.
- Reset: reset button; allows the user to reset the alarm and enter the relative note: the alarm is no longer visible in the active alarm grids but only in the alarm history.

22 UTILITIES

22.1 Shortcuts

Within the grids you can use some key combinations to perform operations quickly:

F4: copies the contents of the cell above the selected one into the selected one, increasing the last number found in the text by 1:

- In case the string starts with a text that contains '/' that is considered as an address, therefore the precedence is given to the address increment (its subgroup);
 - E.g. "1/1/1 | Room 1 bathroom alarm" -> "1/1/2 | Room 2 bathroom alarm".
 - This is the typical format for displaying an address in a grid
 - The address returns to the table in the instanceguid_address form so that it handles it as a change made by a button
- In case in the cell above the selected one there is a TStringList object that contains a string, this is considered as a command in the form InstanceGUID_Address Timing Command; in this case the address is increased, keeping the other information the same;

If the string does not fall in the previous cases, the right-most number is found and incremented by 1

23 WEB CLIENT

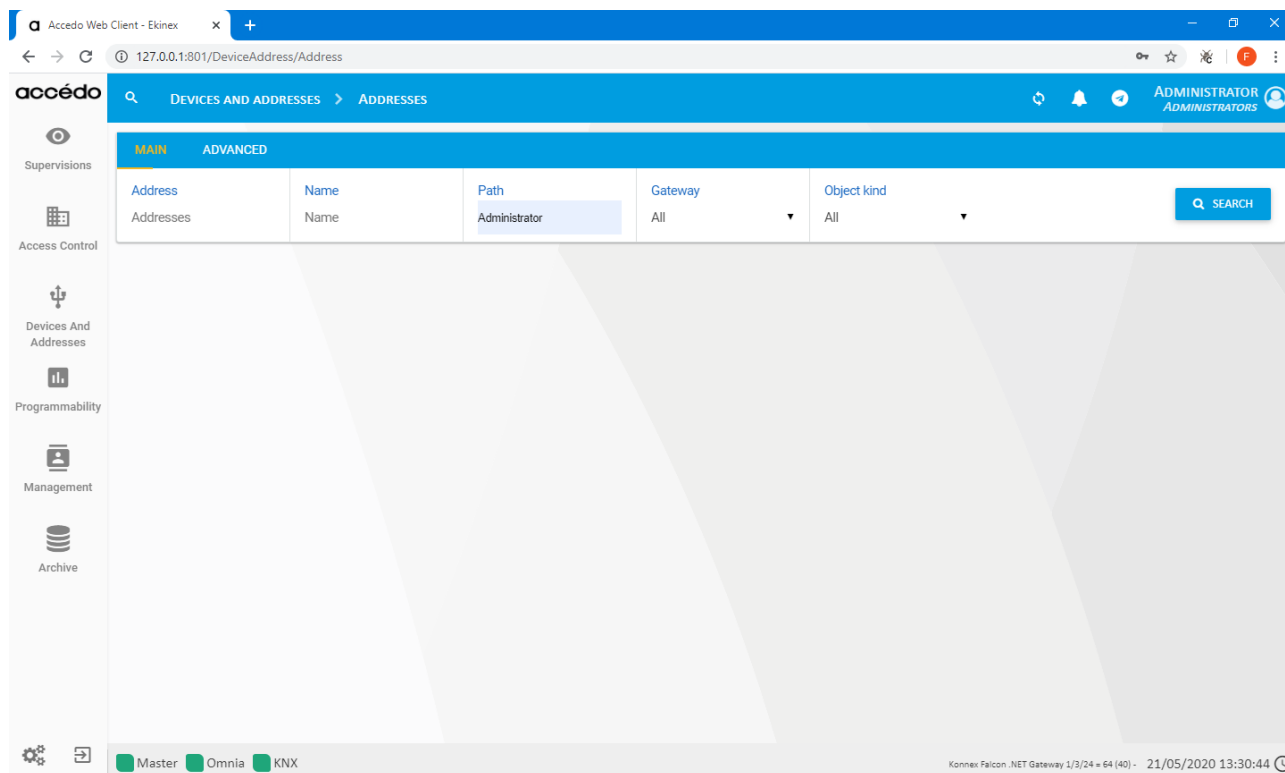
23.1 Web page structure

The accédo suite has a Web interface accessible via browser (Chrome is suggested) from multiple local and/or remote clients. For proper operation, the desktop application, usually installed on a local server, must be configured correctly.

The Web pages are organized with a side menu from which you can access the various sections.

The sections include:

- Supervisions
- Access Control
- Devices and Addresses
- Programmability
- Management
- Archive
- Settings
- Logout

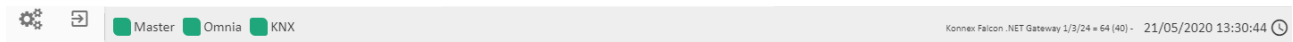


The Access Control section allows the management of reservations: the Web interface does not allow the programming of cards: for this activity you need to access the desktop version of the software suite.

The header at the top of the page indicates the navigation path between the pages.



At the bottom of the pages is the footer which is one of the main parts of the navigation page components, as it defines the connection status of the Gateways and the Web Socket. To the right of the footer are displayed the messages that are written on the bus.



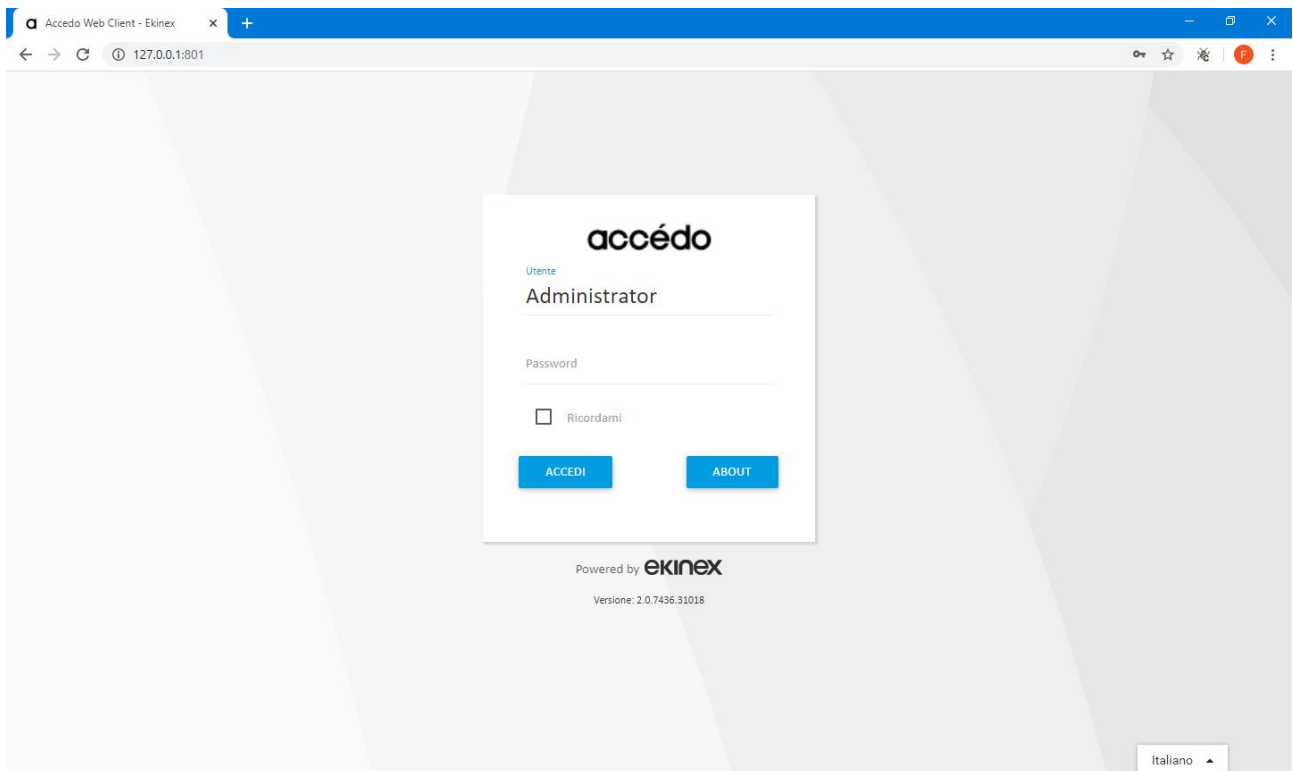
The connection status of the gateways is represented with colored boxes:

- Green: the connection is active
- Yellow: the gateway is being connected
- Red: the gateway is not connected

The Web Socket is essential for communication between client and server in real time.

23.2 Login

Access to the web session must be authenticated according to the user profiles defined in the desktop software or directly in the appropriate section of the web client.



23.3 Supervisions

All the supervision pages are accessible through the Web client to monitor and control, according to the user profile of the session, the parameters of the room and/or plant.

The screenshot displays the 'Camera 023' supervision interface. On the left is a navigation sidebar with categories: Supervisions, Access Control, Devices And Addresses, Programmability, Management, and Archive. The main area is titled 'Camera 023' and contains several control panels:

- Top Row:** Serratura (Lock), Presenza Camera (Camera Presence), Tacitazione allarme bagno (Bathroom Alarm Bypass), Termostato ON-OFF (Thermostat ON-OFF).
- Second Row:** Modo di conduzione (Operating Mode), Riscaldamento Pavimento (Floor Heating), Split ON-OFF, Man-Auto Fancoil (Manual/Auto Fancoil).
- Third Row:** Comfort, Standby (with 'Velocità ventole [%]' indicator), Economy, Protezione (Protection).
- Bottom Row:** Four fan coil units labeled V1, V2, V3, and V4.

On the right side, there is a temperature control section:

Temperatura Attuale Camera	Setpoint Attuale Riscaldamento	Setpoint Attuale Raffrescamento
°C	°C	°C

Below this is the 'Gestione Termoregolazione di camera' section, which includes a note: '(In questa sezione si potranno modificare i singoli setpoint dei modi operativi)'. It features two large circular icons (a red fire icon for heating and a blue snowflake icon for cooling) and a control table:

Mode	Heating Setpoint (°C)	Cooling Setpoint (°C)
Comfort	°C	°C
Standby	°C	°C
Economy	°C	°C
Protezione	°C	°C

At the bottom, there are status indicators for 'Master', 'Omnia', and 'KNX', and a footer with the text: 'Konnex Falcon .NET Gateway 2/4/11 = 0C94 (0C94) - 21/05/2020 13:42:12'.

23.4 Scenes

To access the scenarios, you must go to the *Programmability* section and then select *Scenarios*.

The screenshot shows the 'accédo' web client interface. The top navigation bar includes 'PROGRAMMABILITY' and 'SCENARIOS'. The left sidebar contains icons for Supervisions, Access Control, Devices And Addresses, Programmability, Management, and Archive. The main content area features a table of scenarios with the following data:

Running	Name	Description	Execution code	Schedules	Synchronized
	Accensione luci reception e colazione			Accensione luci reception e colazione	✓
	ALLARMI WC - Tacitazione Generale			-	✓
	Fancoil - Tutti in Automatico			-	✓
	Modalità ESTATE			-	✓
	Modalità INVERNO			-	✓
	Spegnimento luci reception e colazione			Spegnimento luci reception e colazione	✓

Below the table, there is a 'NEW' button and a table with columns: Kind, Object, Timing [s], Command, State, Synchronized. The 'Synchronized' column shows 'Administrator'. A message 'No data to display' is shown below the table. The footer includes status indicators for Master, Omnia, and KNX, and a timestamp: 'Konnex Falcon .NET Gateway 1/4/9 = 0CC4 (0CC4) - 21/05/2020 13:45:35'.

To run the scenario you must select the scenario you want to run, after selecting it the following options will appear:

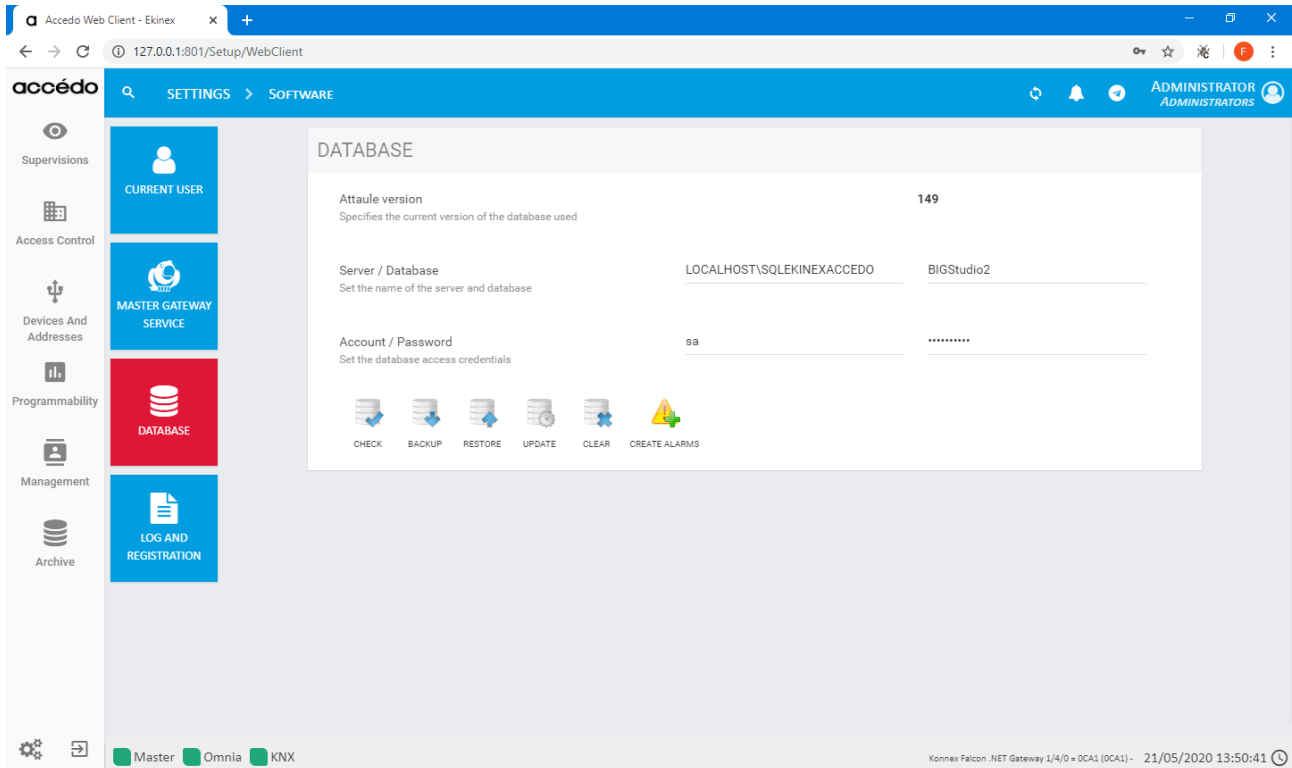
- New
- Duplicate
- Edit
- Delete
- Run

To run the scenario, press Execute.

23.5 Settings

23.5.1 Informations

When you first access the application, you must select *Settings*, *Software* and *Database*.



The available options are:

- Check
- Backup
- Restore
- Update
- Clean up
- Create alarms

Check allows you to check the version of the database .

Backup allows you to save a copy of the current database.

Restore allows you to restore a previously saved copy of the database.

Force update the database to update.

Clean allows you to remove any data from the database securely.

Create Alarms allows you to create new types of alarms.

This screen also contains other information about the database used:

- Current version
- Server / Database

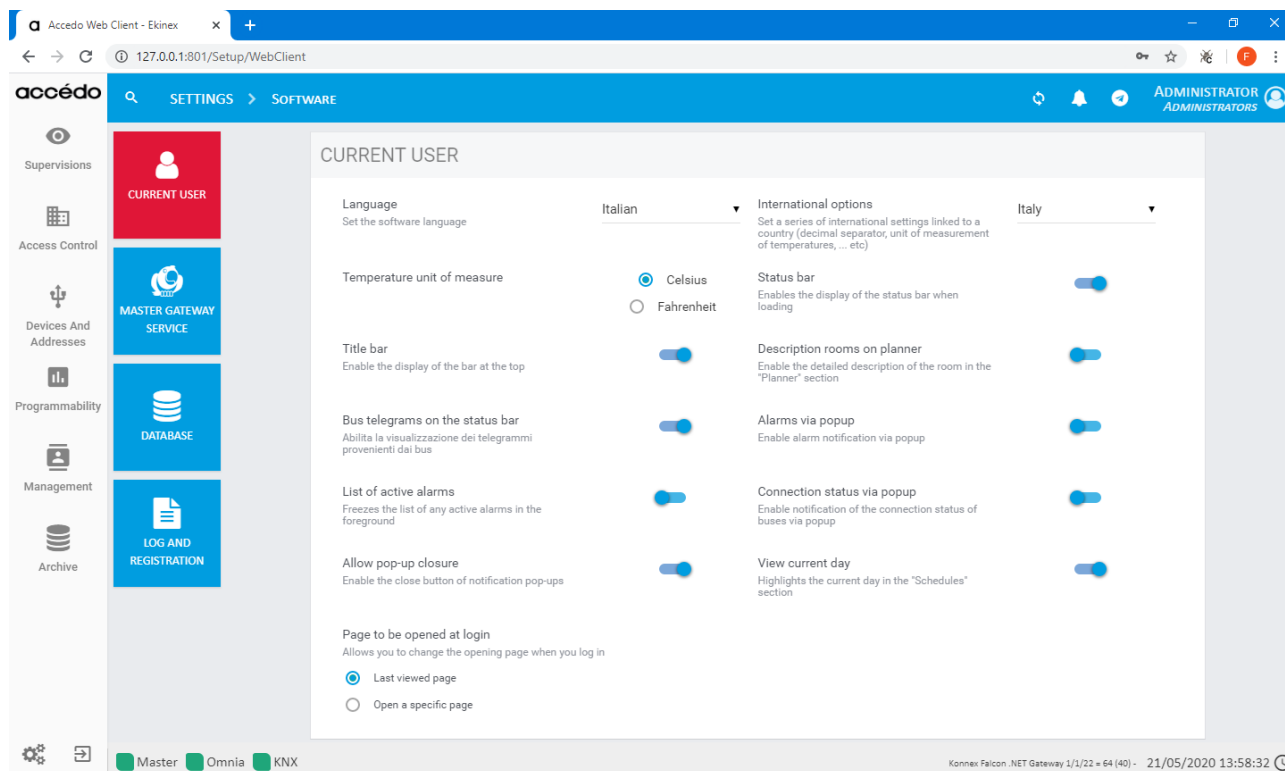
- Account / Password

Current version specifies the version of the database that is used.

Server/Database sets the name of the server and database.

Account/ Password sets the access credentials to the database.

In *Settings, Software*, you can configure the information display criteria.



In *Current User* there are the settings for the type of display that the user wishes to have of their web application.

The options on this page are:

- Language
- Unit of temperature measurement
- Status bar
- Rooms description on planner
- Popup alarms
- Connection status via popup
- International options
- View side menu
- Title bar
- Bus telegrams on the status bar
- Active alarms list
- Allow popup closure

Language allows the user to choose the language of the application, Italian and English are available.

Temperature unit allows to change the temperature in Celsius or Fahrenheit degrees.

Status bar allows you to enable the status bar when loading the application.

Room description on planner enables the detailed description of the rooms in the planner section located in Access Control.

Alarms via popup enables the notification of alarms via popup.

Connection status via popup enables notification of bus connection status via popup.

International options allows to set a series of international parameters related to a country (Italy is set by default and these parameters concern temperature units, decimal separator and other parameters).

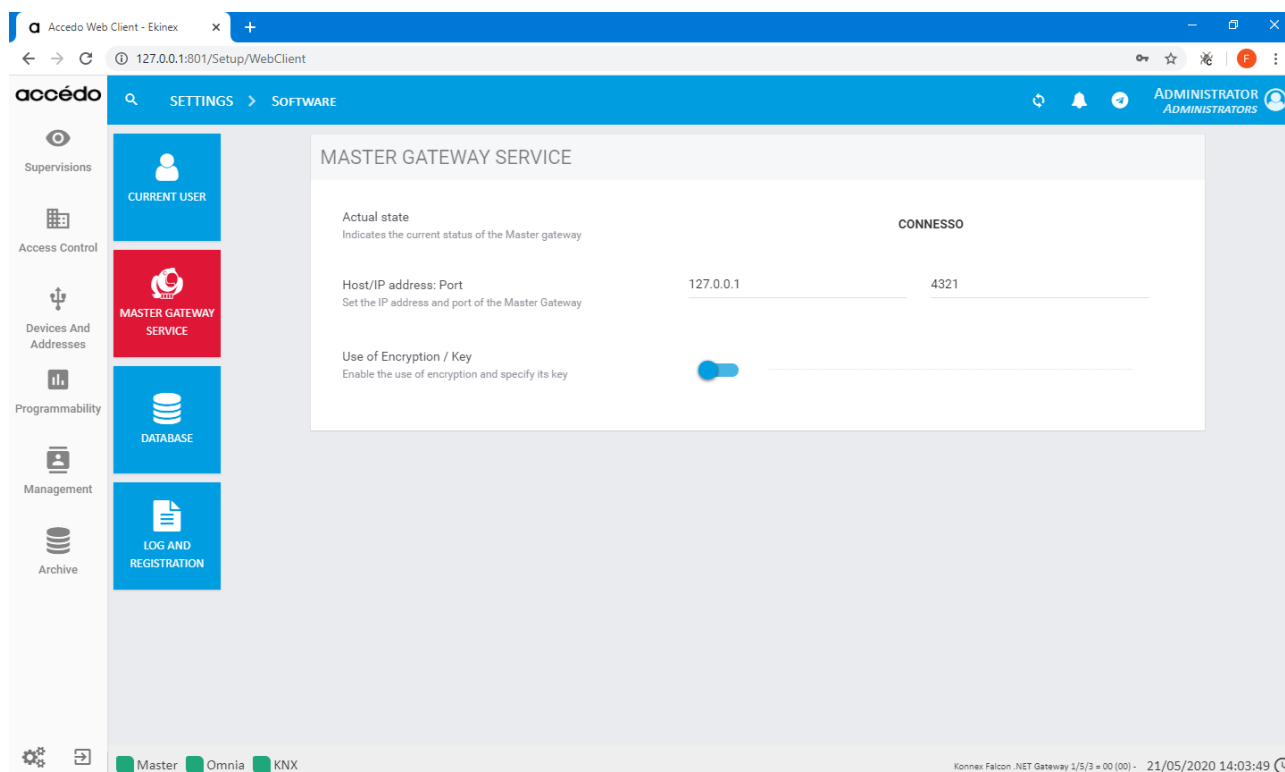
View side menu allows the opening of the side menu when the application is loaded.

Title bar enables the display of the title bar at the top.

Bus telegrams on the status bar enables the display of telegrams from buses on the status bar.

List of active alarms enables the list of active alarms to be locked in the foreground.

Allow popup closure enables the close button to allow the user to close the notification popups.



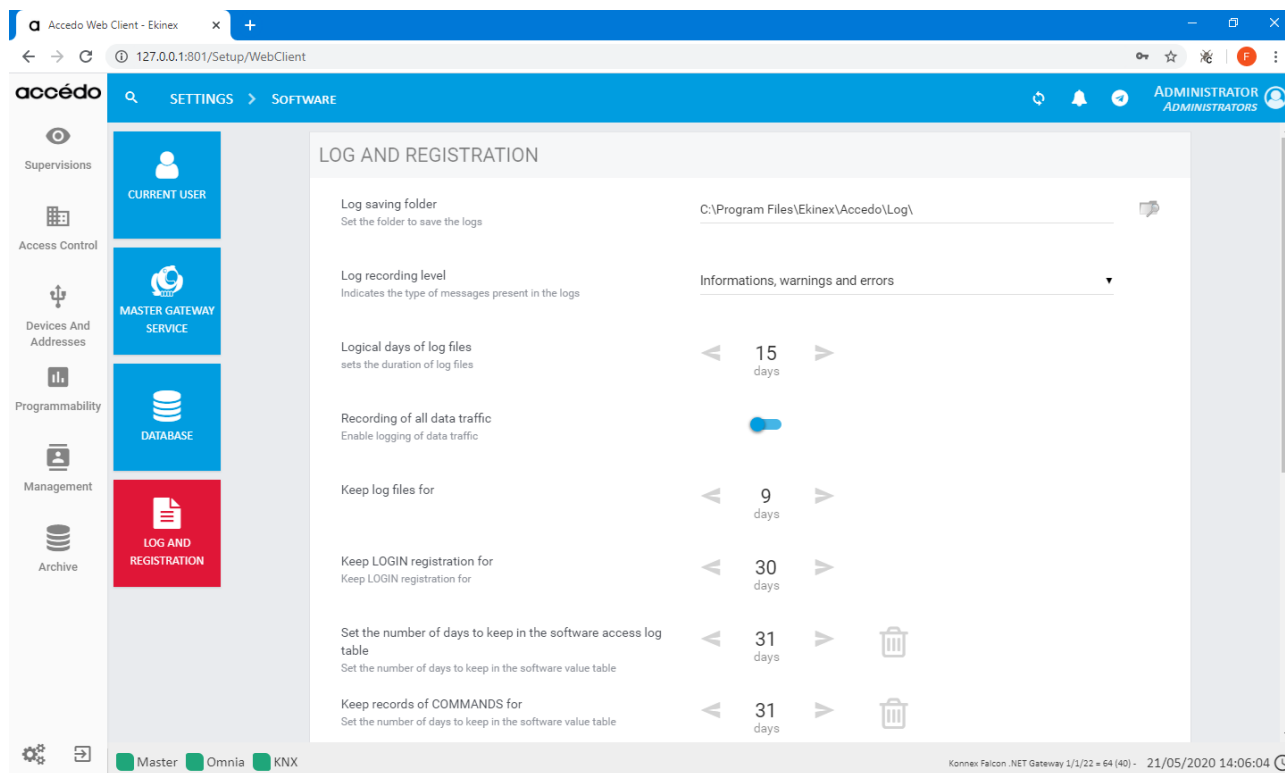
This screen displays information about the Master Gateway Service. The parameters are:

- Current status
- IP address (server name) : Port
- Using encryption/key

Current status indicates the current status of the Master Gateway e.g. connected.

IP address (server name) : Port allows you to set the IP address and port of the Master Gateway.

Use encryption / key enables the use of encryption and allows you to specify the key to be used.



This page sets the settings to keep the log files in memory. You can select the number of days the user wants to keep these files, you can download the history of the files in csv format and you can also delete the history instantly.

The options on this page are:

- Save logs folder
- Logging level
- Days of validity of log files
- Recording all data traffic
- Keep log files for
- Keep LOGIN registration for
- Keep recording VALUES for
- Maintain the recording of COMMANDS for
- Keep ALARMS recording for
- Maintain ACCESS registration for
- Keep the PRESENCES registration for
- Maintain DATA TRAFFIC management for
- Keep records of SOFTWARE ACTIVITIES to

Logs save folder allows you to set the logs save folder.

Log logging level indicates the type of log messages.

Log file validity days sets the duration of the log files.

Logging all data traffic allows you to log data traffic.

Keep log files to set how long to keep the log files in memory.

Keep LOGIN logging allows you to set the number of days to keep in the log table of software accesses.

Maintain the VALUES recording to set the number of days to preserve in the software values table.

Maintain the recording of COMMANDS to set the number of days to be preserved in the software commands table.

Maintain ALARMS recording to set the number of days to preserve in the software alarm table.

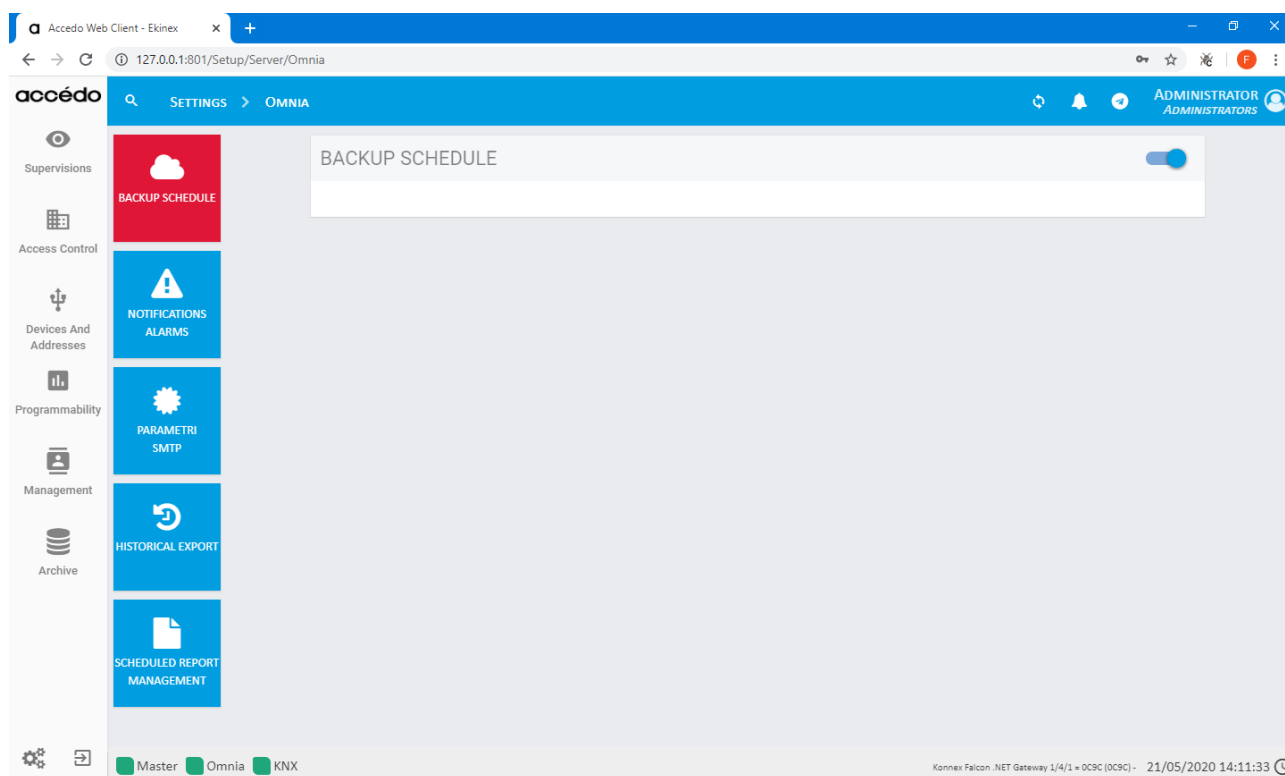
Maintain ACCESS logging to set the number of days to preserve in the software access table.

Maintain the PRESENCE record to set the number of days to be preserved in the software attendance table.

Keep the DATA TRAFFIC management to set the number of days to be preserved in the software data traffic table.

Maintain records of SOFTWARE ACTIVITIES to set the number of days to be preserved in the table of software values.

23.5.2 Server



In the *Settings* section you can access the Server section where you can set the *Backup Scheduling*, *SMTP Parameters*, *Historical Export* and *Scheduled Reports management*.

In the first image you can see *Omnia Backup Scheduling* section.

The options available on this page are as follows:

- Path
- Frequency
- Day of the week
- Day of the month
- Time of execution

Path allows you to set the scheduling path.

Frequency allows you to set the scheduling frequency.

Day of the week allows you to set the day of the week on which you want to schedule.

Day of the month allows you to set the day of the month on which you want to schedule.

Time of execution allows you to set the time of execution of the schedule.

The *SMTP Parameters* page of the server settings allows you to change the following parameters:

- Outgoing mail server
- Port
- Username
- Password

- Sender's email address
- Sender name
- SSL

Outgoing mail server allows you to set the outgoing mail server address.

Port allows you to set the port of the outgoing mail server.

User name allows you to set the user name of the SMTP server.

Password sets the password of the SMTP server.

Sender's email address allows you to set the sender's email address.

Sender Name sets the name of the sender.

SSL enables the use of the SSL certificate.

In the *Historical export* section there are several functions that will be analyzed one at a time starting from historical export. In this area you can configure the following parameters:

- Access history
- Historical black box
- Login history
- Reservations status
- File format
- Alarm history
- Command history
- Historical presences
- Historical values

Access history enables the export of the access history.

Black box history enables the export of the black box history.

Login history enables the export of the access history.

Reservation status enables the export of the reservation status.

Format sets the export format that can be chosen among 3 extensions:

- CSV
- XML
- JSON

Alarm history enables the export of the alarm history.

Command history enables the export of the command history.

Attendance history enables the export of the attendance history.

Value history enables the export of the value history.

In the *Historical Export* section you can find the configuration settings for *Disk Save* and *Email Parameters*. The disk saving options that you can configure are as follows:

- Set the path to save to disk
- Keep files open for

Set the save path to disk allows you to decide where to save the log files.

Keep files open allows you to set the opening time of the files.

In the email parameter settings area there is only one option that the user can configure and it is the following:

Recipients (separated by ;)

Recipients (separated by ;) allows you to set the recipients of the email and it is therefore possible to enter more than one recipient.

AA@gmail.com; BB@gmail.com for example.

Also on the *Export History* page under the email parameters section you can configure the *FTP parameters* that are:

- Host (full path)
- Port
- Username
- Password

Host (full path) allows you to set the full path to save.

Port allows you to set the FTP server port.

User name allows you to set the FTP server user name.

Password allows you to set the FTP server password.

The *Disk Save Settings*, *Email Parameter Setting* and *FTP Parameter Setting* are set to No by default. When the user selects the activation of these functions, a save bar appears at the bottom of the page.

Clicking on save settings if all goes well, a subsequent bar appears that confirms the saving with the changes made.

If, on the other hand, we are configuring the *Email Parameters* and nothing is inserted in the recipients when you click on *Save Settings* a message appears indicating this particular situation.

The *Scheduled Report Management* section has two areas within it: *Save to disk settings* and *FTP server settings*.

Within Disk Save Settings the user has the possibility to configure two options:

- Save path
- Keep generated files for

Save path allows you to set the save path. Next to the path there is a folder that you can click on; after the user has clicked on the folder a window will open that allows you to go to select the save path. In the text line will be taken the saving path that has been selected through the dialog box.

Keep generated files to allow you to set the number of days the files remain on disk.

The options within *FTP Server Settings* are as follows:

- Host (full path)
- Port

- Username
- Password

Host (full path) allows you to set the FTP server host.

Port allows you to set the FTP server port.

Username allows you to set the FTP server access credentials.

Password allows you to set the FTP server access credentials.

As for the *Historical Export* section also in *Scheduled Report Management* you can open the various areas by clicking on the No option.

Subsequently, if the saving is successful, the bar will appear to confirm the successful completion of the saving operation.

If, on the other hand, the saving has had some errors or the parameters have not been configured correctly, a red bar will appear to indicate the saving problems.

24 WARNINGS

- Installation, electrical connection, configuration and commissioning of the device can only be carried out by qualified personnel in compliance with the applicable technical standards and laws of the respective countries
- Opening the housing of the device causes the immediate end of the warranty period
- In case of tampering, the compliance with the essential requirements of the applicable directives, for which the device has been certified, is no longer guaranteed
- ekinex[®] KNX defective devices must be returned to the manufacturer at the following address:

Ekinex S.p.A. Via Novara 37, 28010 Vaprio d'Agogna (NO), Italy

25 OTHER INFORMATION

- The instruction sheet must be delivered to the end customer with the project documentation
- For further information on the product, please contact the ekinex[®] technical support at the e-mail address: support@ekinex.com or visit the website www.ekinex.com
- Each ekinex[®] device has a unique serial number on the label. The serial number can be used by installers or system integrators for documentation purposes and has to be added in each communication addressed to the Ekinex technical support in case of malfunctioning of the device
- ekinex[®] is a registered trademark of Ekinex S.p.A.
- KNX[®] and ETS[®] are registered trademarks of KNX Association cvba, Brussels

© Ekinex S.p.A. S.p.A. 2020. The company reserves the right to make changes to this documentation without notice.

End User License Agreement

The installation of the accédo software implies acceptance of the terms and conditions of this contract. This document constitutes a license agreement, pursuant to which the Building Intelligence Group S.r.l. (hereinafter referred to as BIG) will remain the sole owner of the intellectual property rights relating to the software and any other copies that the end user is authorized to make under this contract. "accédo" is a trademark owned by Ekinex S.p.A..

This contract does not grant the end user any intellectual property rights on the software. The end user acquires on the software only a time-limited license to use it and subject to compliance with the license terms and conditions.

The user license cannot be transferred and / or sub-licensed to third parties.

The end user, unless expressly authorized in writing by the BIG:

- * cannot lease, loan, or make available in any case to third parties, for any reason, the software
- * cannot in any way make it available, in any form, on the internet and / or other means of electronic and non-electronic disclosure
- * cannot modify, adapt or translate the Software
- * cannot re-engineer, decompile, disassemble or otherwise try to trace the source code of the Software
- * cannot develop software as an extension and / or customization of the created software
- * cannot develop 'stand alone' software that uses the databases used by the software created and / or extends it functionally for reading and / or writing

Any infringement detected by BIG may allow the early termination of the contract due to the fault of the end user and will also entail the charge of Euro 10,000.00 (ten thousand / 00) as a penalty for any infringement detected, without prejudice to the compensation of any further damage.

Any customized interventions of any nature will be borne entirely by the end user.

The software license contained in this installation package is valid for 60 days, after which it will no longer be possible to start the software. To extend the license, contact Ekinex S.p.A at +39 0321.1828980.

The license does not automatically provide the right to receive software updates, for which a specific maintenance contract is required.

This license will be automatically suspended in the event of non-compliance by the end user with any provision of the license itself, in case of non-payment, for any reason, by the end user.

In the event of suspension of the license, the end user undertakes to immediately cease using the software and the BIG has the right to use the technologies it deems most appropriate to guarantee such termination.

This rule applies to all copies, in any form: partial, complete, modified, intact or integrated into other software.

The software is licensed "as is". You use it at your own risk.

BIG does not warrant that the operation of the software will be uninterrupted or error free or that the software will be able to operate in combinations of hardware and software other than that authorized by BIG.

BIG warrants that the software product materially conforms to its specifications, if any, and is free of malware upon delivery.

This warranty lasts 12 (twelve) months from the date of installation and is subject to correct maintenance and updating of the software. Any malfunctions identified during the warranty period must be communicated to Ekinex S.p.A. by email or by phone. In the absence of a maintenance contract, the warranty service is provided in "best effort" mode without a guaranteed intervention and / or resolution time.

BIG's liability towards the end user is limited to the direct damage, with the express exclusion of the loss of profit and, in any case, it cannot exceed the price paid for the license and the software concerned.