

4.2

ekinex
CONTROL YOUR LIVING SPACE

Guest Room Management Application User Manual



DELÉGO SERVER Visualisation webserver

EK-DEL-SRV01 / EK-DEL-SRV01-M

Index

1 Introduction.....	5
1.1 Scope of this user manual.....	5
1.2 Conventions.....	5
1.3 Safety information.....	5
1.4 Warnings.....	6
1.5 Copyright.....	6
1.6 Open Source Licenses.....	6
1.7 More information.....	7
2 Overview.....	8
2.1 Introduction.....	8
2.2 Architecture.....	8
2.3 Usage.....	11
2.4 Configuration.....	11
2.5 Licensing.....	12
3 Settings.....	13
3.1 General settings.....	13
3.1.1 Structure information.....	13
3.1.2 Access methods.....	14
3.1.3 Ekinex devices.....	14
3.1.4 Mobile app.....	15
3.2 Welcome email.....	15
3.2.1 Default welcome email.....	15
3.2.2 Dynamic tags.....	16
3.2.3 Additional mail templates.....	16
3.3 Structure management page.....	17
3.4 Redeem voucher.....	18
4 Rooms and gates.....	19
4.1 Introduction.....	19
4.2 Rooms.....	19
4.2.1 Creating a new room.....	19
4.2.2 Room properties.....	20
4.2.3 Other info.....	22
4.3 Gates.....	22
5 Accédo Key.....	24
5.1 Introduction.....	24
5.2 Preliminary operations.....	24
5.3 Create a new device.....	25
5.3.1 Automatic authentication.....	26
5.3.2 Manual authentication.....	26
5.3.3 Save and check connection.....	28
5.4 Additional settings.....	29
5.5 Assigning to rooms and gates.....	30
6 Dico.....	32
6.1 Introduction.....	32
6.2 Preliminary operations.....	32

6.3 Create a new device.....	33
6.3.1 Automatic authentication.....	35
6.3.2 Manual authentication.....	35
6.3.3 Save and check connection.....	37
6.4 Additional settings.....	38
6.5 Assigning to rooms and gates.....	39
7 Ekinex KNX badge readers / holders.....	41
7.1 Introduction.....	41
7.2 Access control strategy.....	42
7.3 Readers and holders widget creation.....	43
7.3.1 Badge readers sub-objects.....	43
7.3.2 Badge holders sub-objects.....	46
7.4 Binding to rooms and gates.....	47
8 Automations.....	49
8.1 Introduction.....	49
8.2 Room connections.....	49
8.2.1 Door lock opening with DICO or ACCÉDO KEY.....	50
8.2.2 Ekinex badge readers and holders (centralized authentication).....	51
8.2.3 Ekinex badge readers and holders (decentralized authentication).....	53
8.2.4 Door lock opening with a KNX actuator.....	54
8.2.5 Connection example: Welcome scene at room status change.....	56
8.3 Gates connections.....	56
9 Permissions.....	57
9.1 User groups.....	57
9.2 Timetables.....	58
9.2.1 Create a new timetable.....	58
9.2.2 Timeslots.....	58
9.2.3 Restrictions.....	59
10 Access log.....	60
11 Virtual presence.....	61
11.1 Introduction.....	61
11.2 Activation and parametrization.....	61
11.3 Room configuration.....	62
12 Guest room management utilization.....	66
12.1 Introduction.....	66
12.2 Guests.....	66
12.2.1 Guests list.....	66
12.2.2 Adding a new guest.....	67
12.2.3 Welcome e-mail.....	70
12.3 Bookings.....	71
12.4 Rooms.....	72
12.5 Gates.....	73
12.6 Access log.....	74
12.7 Staff.....	74
12.8 Temporary QR code.....	75
12.9 Badge.....	76
13 Revision history.....	78

1 Introduction

1.1 Scope of this user manual

This document contains all the information to configure and how to use the access control module (identified from this moment with the name ACCÉDO) integrated with the visualisation functions of the DELÉGO SERVER.

The present user manual is part of the suite of application manuals dedicated to the DELÉGO SERVER, available on the section dedicated to this product in the EKINEX website. Before reading this document, it is recommended to consult the following application manuals:

REF	DOCUMENT	DESCRIPTION
[D1]	DOCUMENTATION PLAN	Overview of the application manuals of DELÉGO SERVER
[D2]	GENERAL FUNCTIONS - APPLICATION USER MANUAL	General installation manual of the webserver
[D3]	KNX - APPLICATION USER MANUAL	Configuration and visualisation of a KNX automation system in DELÉGO SERVER

These documents are available for download in the area of the EKINEX website dedicated to the webserver.

1.2 Conventions

The following conventions are used in this manual:

[KEY]	The keyboard keys that the installer must press are shown in square brackets
<i>Courier</i>	Software messages generated by the DELÉGO SERVER configuration software are reported in the “courier” font
<i>Function name</i>	Names of buttons, table fields or other graphic elements of the user interface of the DELÉGO SERVER configuration software are shown in italics
	Information note
	Important note that requires particular attention

1.3 Safety information

DELÉGO SERVER is a product intended for trained and specialized personnel only; before interacting with this device you must first read this user manual, in particular this safety information. This document supplements and does not replace any legislation or legal directives on safety.

The device has been developed following the safety regulations currently in force; however, it is not possible to exclude with certainty possible damage or interactions with other devices during its operation. The device complies with EMC guidelines and harmonized European standards; any modifications to the device may affect EMC compatibility.

The supply voltage must be strictly within the range indicated in the GENERAL FUNCTIONS application manual and on the device; risk of fire or explosion if powered outside this range. The CE declaration of conformity of the device can be requested from EKINEX®, at the references on the site www.ekinex-delego.com.



In compliance with Directive 2002/96/EC the DELÉGO SERVER electronic device must be disposed of in the appropriate facilities and not in the collection of solid urban waste.

1.4 Warnings

- This application manual is aimed for installers, system integrators and designers.
- The assembly, electrical connection, configuration and commissioning of the appliance can only be carried out by specialized personnel in compliance with the applicable technical standards and the laws in force in the respective countries
- Opening the appliance case causes the immediate interruption of the warranty period
- In the event of tampering, compliance with the essential requirements of the applicable directives for which the appliance has been certified is no longer guaranteed.
- EKINEX defective appliances must be returned to the manufacturer at the following address:
Ekinex S.p.A. Via Novara 37, 28010 Vaprio d'Agogna (NO)

1.5 Copyright

© Ekinex S.p.A. 2025

This application manual, the DELÉGO SERVER software and the DELÉGO iOS and Android apps are subject to copyright; all rights are reserved. Copying, reproduction, translation and/or modification, even partial, are expressly prohibited unless approved in writing by EKINEX®.

1.6 Open Source Licenses

DELÉGO SERVER contains open source software, such as the Linux operating system and its kernel. These software components are subject to various open-source licenses, including:

- GNU General Public License (GPL), <https://www.gnu.org/licenses/gpl-2.0.html>
- GNU Lesser General Public License (LGPL), <https://www.gnu.org/licenses/lgpl-2.0.en.html>

If you own a product, for a period of 3 years from the last production date, you can request from EKINEX the source code of the software components licensed under the GNU General Public License (GPL) or the GNU Lesser General Public License (LGPL), and use, distribute and modify them in accordance with the respective licenses.

EKINEX cannot be considered responsible in any way for the source code thus distributed, which is provided without guarantees. EKINEX cannot also be held responsible for any damage or consequence resulting from modifications (additions / removals) made to this software by third parties, unless specifically authorized.

1.7 More information

For further information on the product, you can contact EKINEX technical support® to the e-mail address: **support@ekinex.com** or consult the website www.ekinex.com

EKINEX® is a registered trademark of Ekinex S.p.A.

KNX® ed ETS® are registered trademarks of KNX Association cvba, Brussels

The company reserves the right to make changes to this documentation without notice.

2 Overview

2.1 Introduction

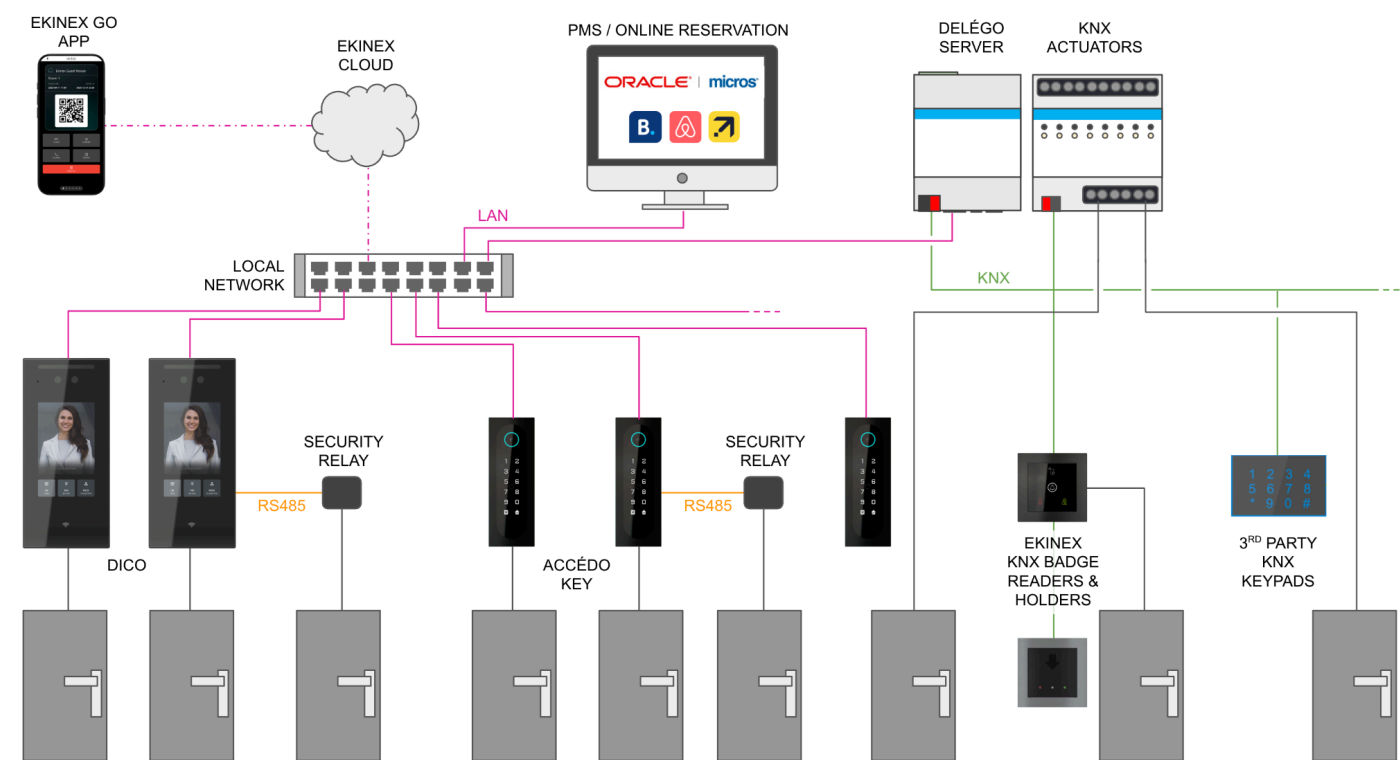
DELÉGO SERVER can act as an ACCESS CONTROL manager in combination with other products of the EKINEX catalogue, with the integrated software module called ACCÉDO:

- DICO (video intercom door station)
- ACCÉDO KEY (numeric keypad)
- EKINEX KNX BADGE READERS and HOLDERs

Third party KNX numeric keypads are also optionally supported by this module, although with some limitations compared to the EKINEX products.

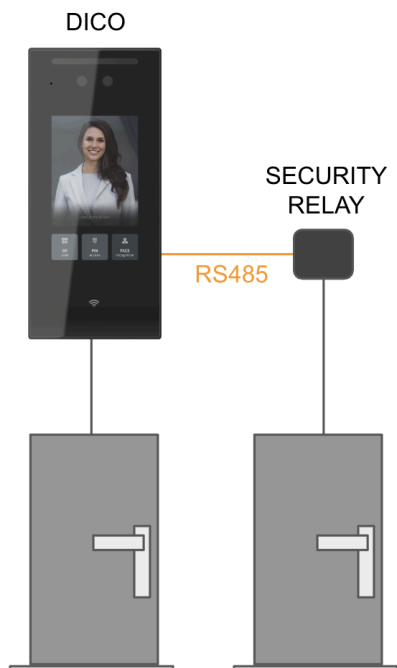
2.2 Architecture

The following schema describes the system architecture of a typical installation, where DELÉGO SERVER coordinates DICO, ACCÉDO KEY and KNX access control devices to regulate the entrance to rooms and gates in common areas:

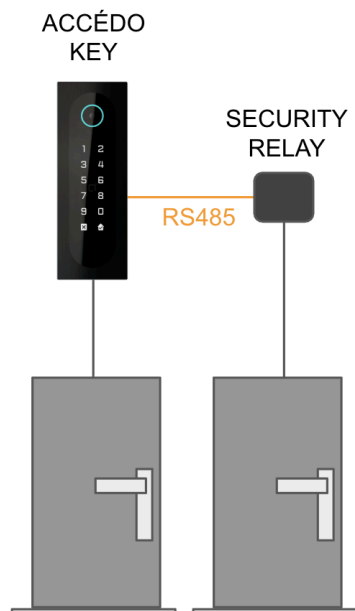


DELÉGO SERVER enables the user to configure and manage rooms / gates independently with an integrated approach. A *room* is a space “owned” exclusively by a guest during a specific period of time, while a *gate* is an access point to the building or to a common area, for example pool, SPA, warehouse.

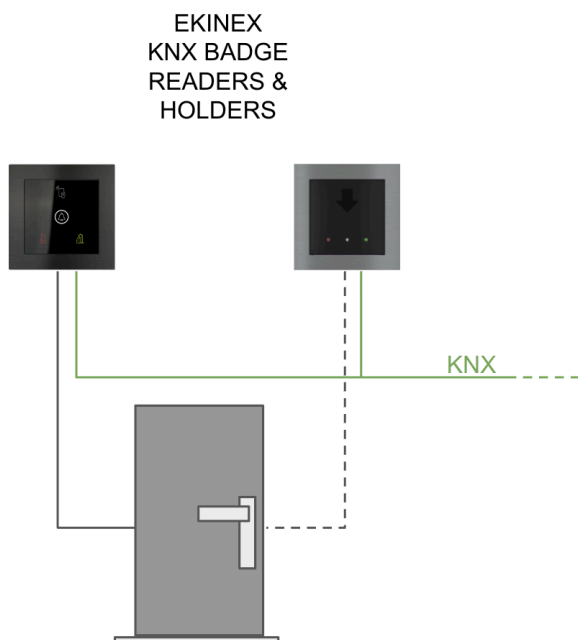
The *lock* of a door under the control of DELÉGO SERVER can be opened in one of the following ways:



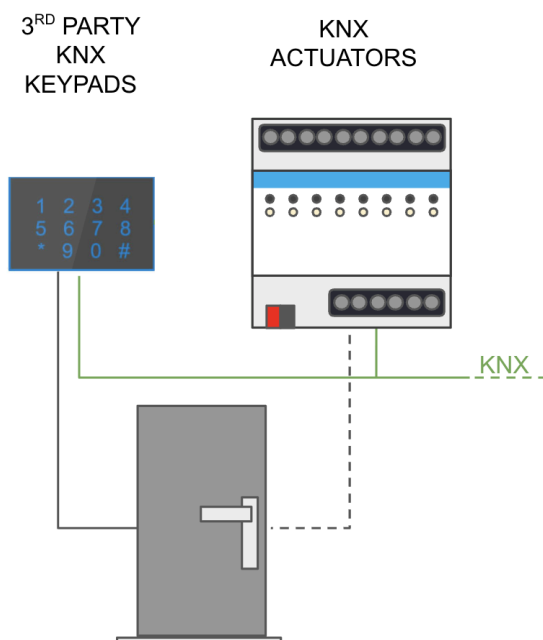
The INTERNAL RELAY of a DICO door station or a SECURITY RELAY connected via RS485



The INTERNAL RELAY of an ACCÉDO KEY or a SECURITY RELAY connected via RS485



One of the INTERNAL RELAYS of an EKINEX KNX BADGE READER or HOLDER



The RELAY of a KNX ACTUATOR or a 3rd party KNX KEYPAD

NEW

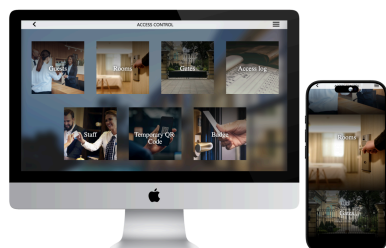
The *authorization* for one or more persons to open a specific door, is given by DELÉGO SERVER according to the *validity period* of the corresponding user and its *association* to the corresponding rooms / gates. This concept applies both to *guests* and *staff members*.

A user can typically open the doors with several *access methods*:

	 DICO	 ACCÉDO KEY	 EKINEX BADGE READERS / HOLDERS	 3 rd PARTY KNX KEYPADS
Numeric PIN	•	•		•
QR code	•	•		
RFID badge	•	•	•	

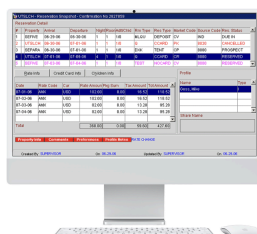
Additionally, users can use the EKINEX GO app to unlock the allowed doors without any physical interaction with them.

The *guest room management* (create / edit / delete users, assign validity periods and authorizations, control the room state etc...) can be done in different ways:



DELÉGO SERVER GUEST
ROOM MANAGEMENT
INTERFACE

(DESKTOP OR MOBILE)



COMPATIBLE PMS (PROPERTY
MANAGEMENT SYSTEM)



ONLINE RESERVATION
SYSTEM

(SUPPORTED BY A COMPATIBLE
CHANNEL MANAGER)

2.3 Usage

The manager(s) of the building can manage the bookings of the rooms and assign the access permissions to the guests or service personnel by means of:

- A web page running on a browser pointing to the DELÉGO SERVER (typically on the PCs of the reception).
- The DELEGO mobile app that is installed on their smartphones or tablets.
- Through the GUI of a supported PMS (Property Management System) interfaced with the webserver.

When a new guest or a new service personnel is created and assigned to a room and/or it has been given the permission to open one or more gates, a welcome message can be sent to him/her email address, containing:

- General information about the structure (e.g., address)
- The instructions to access the structure (room number and gates).
- The information about the access method (PIN and/or QR Code).

When arriving on site, the guest can access in the following manners:

- By entering the PIN on the display of DICO, on the ACCÉDO KEYs and the eventually installed 3rd party KNX keypads
- By showing the personal QR CODE in front of the DICO and ACCÉDO KEY devices
- With an RFID Card received at the reception, supported by the following devices:
 - DICO
 - ACCÉDO KEY
 - EKINEX KNX BADGE READERS
- With the EKINEX GO app installed on the smartphone

2.4 Configuration

In order for the ACCÉDO module to work properly, a CONFIGURATION procedure is required by the installer / system integration, in the administration space of the webserver.

The configuration normally requires the following steps to be done:

- General settings
 - Structure information and preferences
 - Access methods and options
- Welcome email settings
- Rooms and gates configuration
- DICO and ACCÉDO KEY settings
 - Devices configuration
 - Association with the rooms and/or gates
- EKINEX KNX BADGE READERS and HOLDERS configuration

The following optional aspects can be configured, according to the specific needs of each installation:

- User groups and timetables configuration
- Virtual presence setup
- PMS integration setup

The following chapters of this manual cover all these aspects in detail. The final part of this document is dedicated to the usage of the access control system, once it has been properly configured.

2.5 Licensing

The ACCÉDO module has a specific licensing model, based on the number of rooms and/or gates to be used. A base number of rooms and gates is available for free in the webserver; in order to increment it, it is necessary to:

- Buy one or more than one LICENSE VOUCHER
- Enter the following section of the administration space of DELÉGO SERVER:

ACCESS CONTROL > SETTINGS > REDEEM VOUCHER

- Copy and paste the voucher in the first textbox of the page
- In order to redeem multiple vouchers at the same time, press the ADD VOUCHER button as many times as necessary
- Press the SAVE button and wait until the procedure completes



DELÉGO SERVER must be connected to the internet in order to redeem the access control vouchers. Please contact the technical support in case of offline applications.

Also the integration with third-party PMS is subject to a license. In such a case, proceed in the following way:

- Buy the LICENSE VOUCHER for the PMS integration
- Access the VOUCHER PORTAL at the following address...

<https://voucher.ekinex.com>

... and redeem the voucher by creating a license for the serial number of the DELÉGO SERVER

- Enter the license in the SETUP > LICENSES AND MODULES page

For further information about the licenses and vouchers of DELÉGO SERVER, please refer to the application manual [D2], or contact your sales representative in EKINEX.

3 Settings

3.1 General settings

By accessing the section

GUEST ROOM MANAGEMENT > SETTINGS > GENERAL SETTINGS

in the administration space, the following general information can be set.

3.1.1 Structure information

STRUCTURE NAME	The name of the building / hospitality structure. It is used in the automatic email messages sent to the guest.
ADDRESS	Address of the structure. Used in the welcome email.
PHONE NUMBER	Phone number of the structure. Used in the welcome email.
CONTACT E-MAIL	E-mail of the structure. Used in the welcome email.
WEBSITE	URL of the structure. Used in the welcome email.
WIFI NETWORK NAME	Information about the WIFI network that can be used by the guests to access the internet. This information can be added in the welcome email.
WIFI NETWORK PASSWORD	The password to access the WIFI. This information can be added in the welcome email with the WIFI NETWORK NAME.
DEFAULT CHECK-IN TIME DEFAULT CHECK-OUT TIME	Default time for the validity start and end. Can be changed during the creation of a guest.
ELECTRIC LOCK IMPULSE DURATION (IN SECONDS)	Duration of the impulse to be given to electric locks for the doors opening
AVOID MULTIPLE BOOKINGS FOR SAME ROOM	If enabled, before granting access to a room to a new guest, a check for another booking on the same room and dates of check-in and check-out is done.
DELETE OLD GUESTS	If enabled, guests no longer active after some days are automatically deleted, in order to preserve an optimal system performance
TIMETABLE GRANULARITY	Normally the timetables can be defined with start / end times expressed in HOURS; this granularity ensures the full compatibility with all the access methods. It is possible to change this parameter to MINUTES, which brings an higher flexibility in the definition of the time slots, but it is only compatible with the centralized authentication and cannot work with 3rd party KNX keypads.

NEW

3.1.2 Access methods

The following options determine in which ways the guests or service personnel can access the structure:

MOBILE APP	Enables the access for guests and staff members with the EKINEX GO mobile app
EKINEX DEVICES	Enables the access with the following EKINEX devices: • KNX badge readers and holders • DICO • ACCEDO KEY
THIRD PARTY KNX KEYPADS	Enables the management for third-party KNX numeric keypads

3.1.3 Ekinex devices

When the access method with EKINEX devices is enabled, the following options can be additionally set:

ENABLE PIN	Enables the guests authentication by means of a personal PIN, automatically generated and sent in the welcome email.
ENABLE QR CODE	Enables the guests authentication with a personal QR CODE, automatically sent along the welcome email.
ENABLE BADGE MANAGEMENT	Enables the access to rooms and gates through a RFID Card
ENABLE LIMIT ON NUMBER OF ACCESSES	If this option is enabled, it is possible to activate, for each of the previous authentication methods, a limitation of the number of accesses for each guest, during their stay in the structure.
CENTRALIZED AUTHENTICATION	When active, the authentication is done centrally by DELÉGO SERVER, instead of being delegated to the access devices. This strategy is more flexible, but is not optimal for bigger buildings because it generates a higher load on the webserver. By default, starting from the 2.8 release, the centralized authentication is no longer active, meaning it is decentralized in the devices supporting it (the KNX badge readers and holders).



The distributed authentication (centralized authentication not enabled) is compatible with the KNX BADGE READER (EK-TO2-TP) and HOLDER (EK-TI2-TP) only starting from the following versions, which introduce the WHITELIST functionality:

- Firmware: 2.0.0
- ETS library: 0.2

If your products have a lower version, update them or activate the centralized authentication.

3.1.4 Mobile app

The following options, specific for the EKINEX GO mobile app, are available if the corresponding access method is enabled:

GEOLOCATION CHECK MAXIMUM DISTANCE	The maximum distance from the structure allowed to interact with rooms and gates. If the mobile phone is farer, the app does not allow to open the doors and the room automation. Leave empty to disable the geolocation control.
ENABLE PIN REQUEST	If enabled, an additional PIN check is requested to the user before opening a door / gate
ROOM MANAGEMENT LOCAL / REMOTE	If enabled (in local network and remotely) the mobile app users can control the room automation
SORT GATES BEFORE ROOMS IN THE LIST	Determine the order of gates and rooms in the list of the app (normally the room(s) are listed before the gate(s))

3.2 Welcome email

3.2.1 Default welcome email

By entering this section, it is possible to customize the default message sent via email to new guests or staff members, to provide them information about the structure, how to access, and their personal PIN / QR CODE.

The default message reflects the language of the webserver; when the language setting is modified, the email is translated to the new language. In order to manage different messages for guests speaking different languages, please refer to the next paragraph.

The page contains the following buttons:

SAVE	Saves the new template subject and body
CLOSE	Closes the editor without saving the template
OPTIONS	Gives access to the email sending options. Please refer [D2] for further details about the email sending methods
HELP	A context help containing the list of dynamic tags (se below)

3.2.2 Dynamic tags

Both the subject and the body of the email template, can contain the following *dynamic tags* which are automatically substituted with the corresponding information about the structure and the guest:

USER (GUEST) INFO

{{user.name}}	The complete username of the guest
{{user.options.firstname}}	The first name of the guest
{{user.options.lastname}}	The last name of the guest
{{user.options.valid_from}}	The start day of the validity period for the guest in the structure
{{user.options.valid_to}}	The end day of the validity period for the guest in the structure
{{user.rooms}}	The list of room(s) assigned to the guest. In case of multiple rooms (only for a service personnel), they are separated with a comma.
{{user.gates}}	The list of gate(s) that the guest can open. In case of multiple gates, they are separated with a comma.

STRUCTURE INFO

{{info.name}}	The name of the structure
{{info.location}}	The address of the structure
{{info.phone}}	The phone number of the structure
{{info.www}}	The structure website URL
{{info.wifi_ssid}}	The WIFI network name
{{info.wifi_pwd}}	The WIFI network password

ACCESS INFO

{{pin}}	The personal PIN to be digitated on the keypads
{{qr_code}}	The image of the QR CODE to be presented in front of the DICO and ACCÉDO KEY devices

3.2.3 Additional mail templates

By selecting the menu item

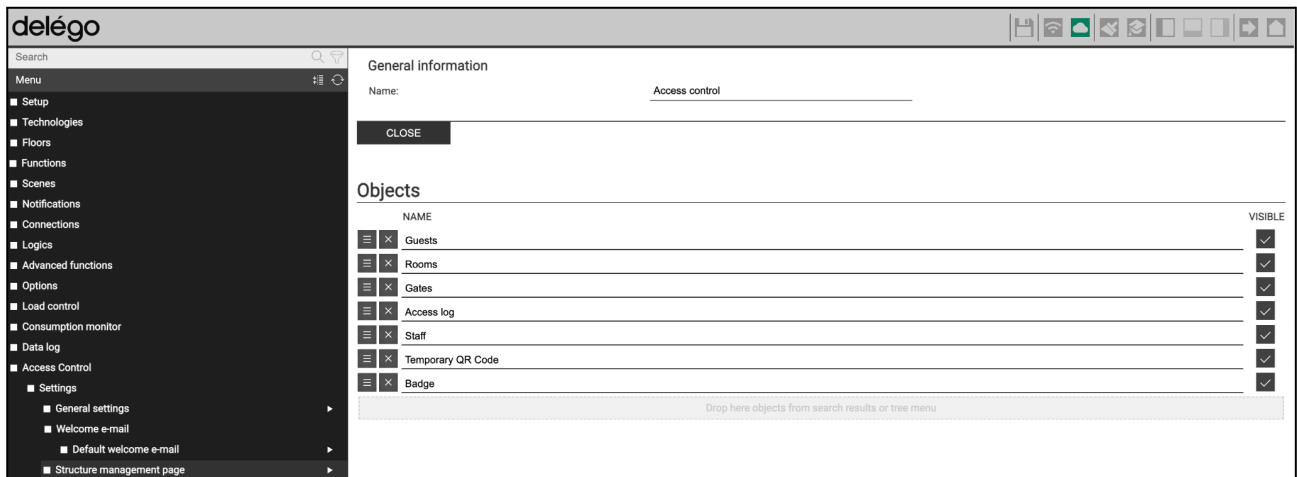
ACCESS CONTROL > WELCOME E-MAIL

And pressing the [+] button in the toolbar, it is possible to add other email templates; each of them can be customized in the way already seen for the default one.

In this way, it is possible to create multiple templates for different languages, or for different categories of guests.

3.3 Structure management page

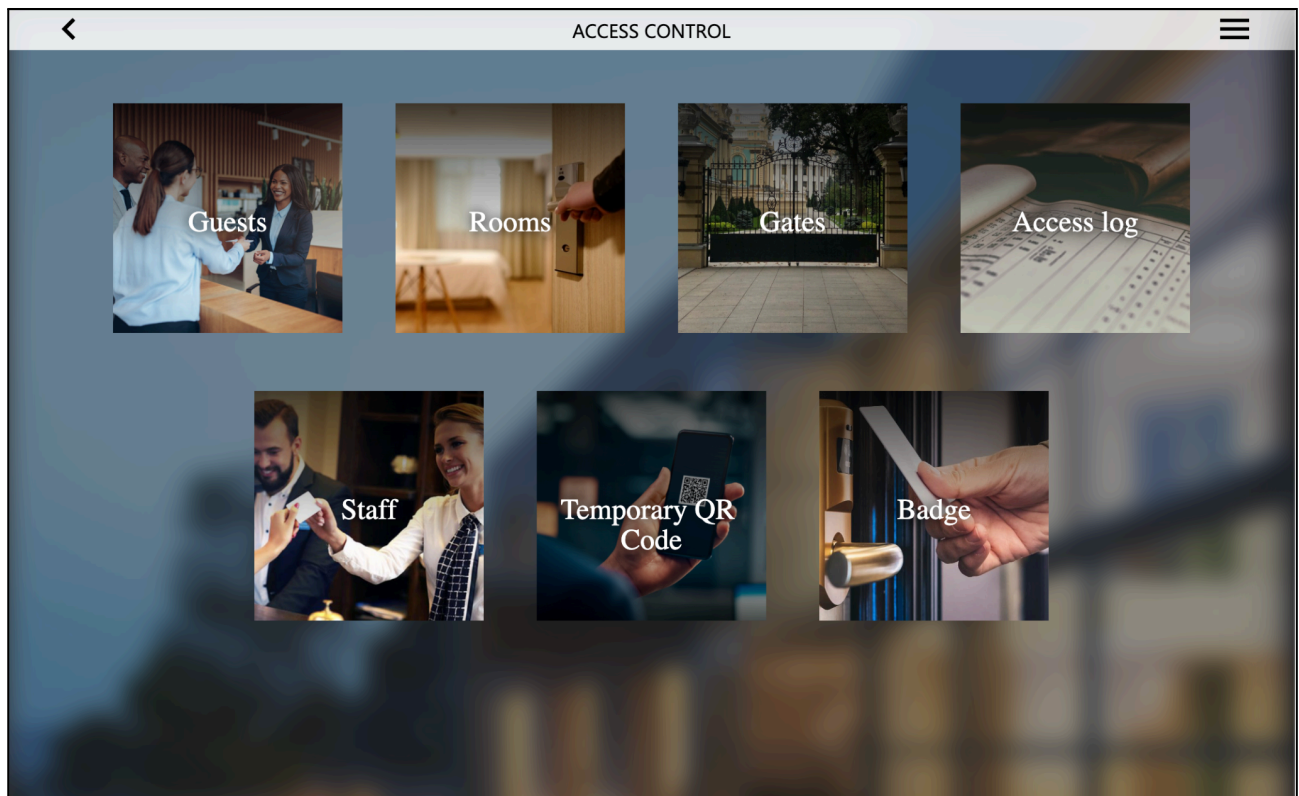
This page contains the list of items visible in the visualisation, when accessing the ACCESS CONTROL item of the navigation menu:



This page offers the possibility to:

- Change the name of the navigation menu item, by customizing the default NAME label at the beginning of the page
- Change the label for each of the items in the page
- Hide one or more items, if not suitable for the specific needs of the structure (by deselecting the corresponding checkbox in the VISIBLE column)

The corresponding result in the visualisation is similar to the following picture:



3.4 Redeem voucher

As mentioned in [section 2.5](#), this page allows you to extend the number of rooms and gates, by entering one or more license vouchers.

4 Rooms and gates

4.1 Introduction

In the terminology of ACCÉDO, a ROOM is intended as a space protected by one or more doors under the control of the access control module of a DELÉGO SERVER. Normally a room is occupied by one guest at a time.

A GATE is a door under the control of the webserver, granting the access to the building itself (from outside) or to an internal common area (e.g., a SPA).

Normally a GUEST is associated with only one ROOM at a time, but can have the right to open more than one GATE.

4.2 Rooms

4.2.1 Creating a new room

By selecting the menu item

GUEST ROOM MANAGEMENT > ROOMS

And pressing the [+] button, a new ROOM is created.

By entering its details page, the following general information can be set; some of the following information requires the EXPERT mode () to be active.

GENERAL INFORMATION

NAME	Label identifying the ROOM. Leave this field in its default state, in order to reflect the given NUMBER; to assign a different name, change the NUMBER before and then, assign a free label.
NUMBER	Numeric identifier of the ROOM. When changing the NUMBER, the NAME is automatically adjusted to reflect the new number,
ENABLED	If this checkbox is not selected, the ROOM is not presented in the list of options for the assignment to guests, and no access is possible.
DEFAULT ACCESS LIMIT	Visible only if in the General Settings the flag ENABLE LIMIT ON NUMBER OF ACCESSES is enabled. Allows the user to insert a default access limit number to the room when creating a new Guest or Service Personnel.

APPEARANCE

BACKGROUND IMAGE	Upload and assign a custom picture to the ROOM, to be displayed in the visualisation, when the room popup is opened.
------------------	--

VIRTUAL PRESENCE

If the virtual presence algorithm is activated, it is possible for each ROOM, to see the following options / info:

ENABLE VIRTUAL PRESENCE	When enabled, the virtual presence is calculated for the current ROOM, to determine if at least one guest is inside the room. Please refer to chapter 10 for further information.
VIRTUAL PRESENCE STATUS	The status of the algorithm for the determination of the presence in the room

4.2.2 Room properties

Enabling the EXPERT mode () the list of all available PROPERTIES for the ROOM are displayed. These items are dynamic attributes of the ROOM, which can be set manually (here or in the visualisation) or related to other objects, by means of CONNECTIONS or TRIGGERS (see the [section 7](#) for more details). The properties of a room can be hidden in the visualisation by deselecting the corresponding VISIBLE checkbox.

A room has the following properties:

ROOM STATUS	The actual status of the ROOM, changing according to the operations done by a guest.
-------------	--

	See the table below for all the possible values of the ROOM STATUS. It is possible to trigger an action on other objects (e.g. SCENES, KNX WIDGETS or OBJECTS etc...) when the status changes.
LOCK	This property will be set automatically to OPEN when a valid PIN, QR CODE or a valid RFID Card is used by guests or the service personnel to open the door. The property keeps the Open value for the impulse time set in the general setting explained in section 3.1. A <i>relationship</i> with the object representing the command for the lock must be established, in order for the door to actually open, as explained in chapter 7 dedicated to the connections.
PRESENCE	The actual presence of at least one guest inside the ROOM. This information can be given by physical sensors (e.g. a <i>RFID Card holder</i>) or calculated by the VIRTUAL PRESENCE algorithm. In any of the two situations, this property can be associated with a <i>relationship</i> to an object to be commanded when somebody is in the ROOM, e.g. the room loads relay, the air conditioning, a light etc...
DO NOT DISTURB	Active when the guests request not to be disturbed by the personnel during the staying, even for the room cleaning.
ALARM	Active when an alarm (e.g., fire and smoke or the alarm in the shower) is triggered.
MAKE UP ROOM	Active when the guests request an additional cleaning of the ROOM
DOOR SENSOR MOTION SENSOR 1 MOTION SENSOR 2	Inputs required by the VIRTUAL PRESENCE algorithm, as better explained in chapter 10. These properties are not visible in the visualisation.

The ROOM STATUS can have one of the following values:

ROOM STATUS	DESCRIPTION	NUMERIC
FREE	Available for the booking to a guest	1
BOOKED	Booked for a guest, which has still not entered the structure (before the starting period of validity)	2
ASSIGNED	Given in exclusive use to a guest, which is not actually inside the room at the moment (but is in the structure, or anyway, in the validity period of his/her staying)	3
OCCUPIED	The guest is inside the room	4
SERVICE	Under cleaning or maintenance	5
N.D.	None of the previous statuses	0

4.2.3 Other info

The details page of a ROOM can contain also the following information, according to the general settings (and in particular, the access methods that have been enabled for the structure):

TIME TABLES	Access limitations along the week for specific user groups
GUESTS	List of users that have access to the room
DICO ACCÉDO KEY	List of IP-based devices that can open the door's room
EKINEX BADGE READERS / HOLDERS	List of EKINEX KNX badge readers / holders that can open the room's door
KNX KEYPADS PROGRAMMING / ENABLE	Specific group addresses for 3 rd party KNX keypads

Please refer to the next chapters for an explanation of the corresponding arguments and their configuration.

4.3 Gates

GATES are similar to the ROOMS, except the fact the only property that a gate has is the LOCK.

In the GENERAL SETTINGS the following attributes are available:

NAME	Label identifying the GATE
NUMBER	Numeric representation of the GATE
ENABLED	If this checkbox is not selected, the GATE is not presented in the list of options for the assignment to guests, and no access is possible.
DEFAULT ACTIVE FOR GUESTS	If this checkbox is selected, the GATE will be checked by default in the visualisation, when a new guest is going to be created
DEFAULT ACCESS LIMIT	Visible only if in the General Settings the flag ENABLE LIMIT ON NUMBER OF ACCESSES is enabled. Allows the user to insert a default access limit number to the room when creating a new Guest or Service Personnel.

delégo

Search

Menu

- Setup
- Technologies
- Floors
- Functions
- Scenes
- Notifications
- Connections
- Logics
- Advanced functions
- Options
- Load control
- Consumption monitor
- Data log
- Access Control
 - Settings
 - Rooms
 - Gates
 - Gate 1
 - Accédo Key
 - User groups
 - Timetables
 - Access logs and operations

Generic settings

General information

ID

1193

Name:

Gate 1

Number:

Enabled:

☒

Default active for guests:

☐

CLOSE

CONNECTIONS

Properties

NAME

STATE

...

Lock

-

Closed

+

Time tables

NAME

Drop here objects from search results or tree menu

Gate 1

0

2

0

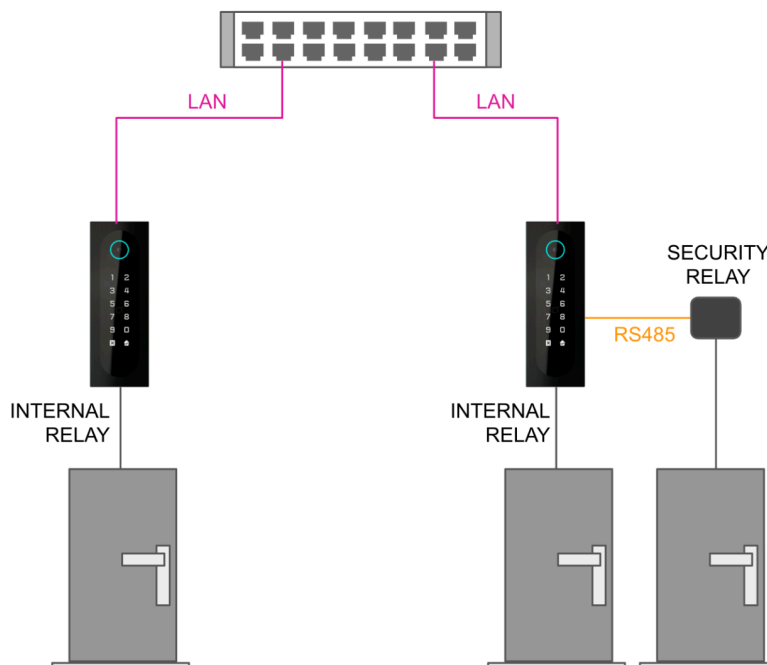
5 Accédo Key

5.1 Introduction

An ACCÉDO KEY is an IP-based numeric keyboard with the capability to scan a QR CODE and to read a RFID Card. The power supply can be provided either with a POE network cable, or a dedicated power supplier.

It offers the possibility to open an electric lock in two ways:

- Directly wired to its internal relay
- Wired to a SECURITY RELAY, connected through the integrated RS485 port

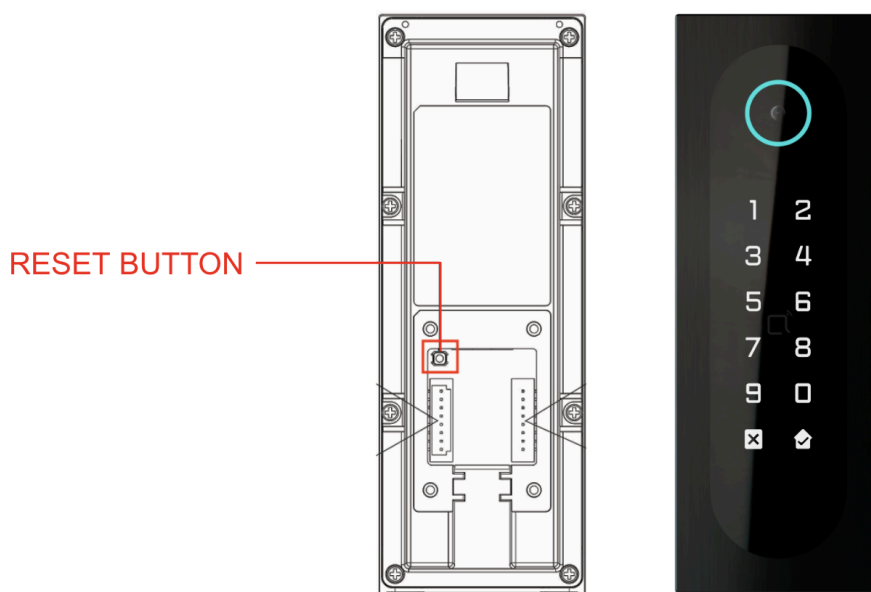


5.2 Preliminary operations

In order to use an ACCÉDO KEY in combination with DELÉGO SERVER for the access control, it is necessary to:

1. Connect it to the lock(s) to be opened
2. Connect it to the LAN with an RJ45 cable
3. Connect the power supply (if not provided with a POE network cable)
4. Identify the IP address assigned by the DHCP server

In order to discover the actual IP address of an ACCÉDO KEY, press the RESET button on the back of the device. A voice will say the IP address (in English language).



For further details, please refer to the technical documentation and application manual of the product in its related section of the EKINEX website

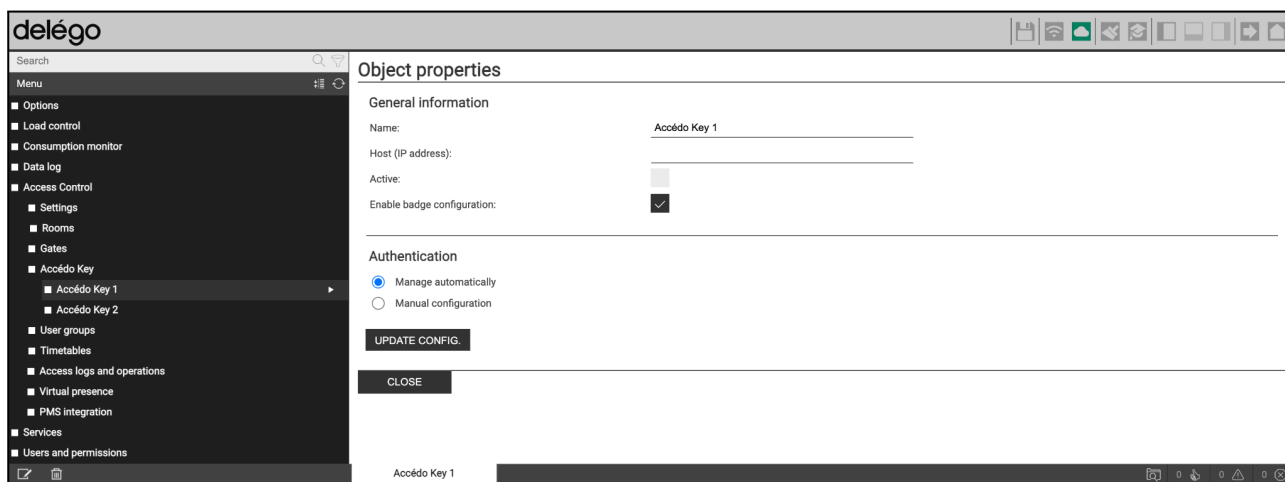
5.3 Create a new device

By selecting in the menu

ACCESS CONTROL > ACCÉDO KEY

section and pressing the [+] button on the bottom of the toolbar, a new ACCÉDO KEY device is created.

The following figure depicts the details page of the ACCÉDO KEY.



The user must insert the following information:

GENERAL INFORMATION

NAME	Label identifying the ACCÉDO KEY
HOST (IP ADDRESS)	The IP address of the ACCÉDO KEY in the local network
ACTIVE	This field (in read-only) is flagged only when the ACCÉDO KEY is successfully configured.
ENABLE BADGE CONFIGURATION	If the RFID Card management is enabled (see section 3.1.3), when this checkbox is selected, this ACCÉDO KEY can be used to enable an RFID Card to open a Room or Gate by means of the function SCAN (see section 12.2.8)

AUTHENTICATION

MANAGE AUTOMATICALLY	When selected, the configuration of the ACCÉDO KEY is automatically managed by DELÉGO SERVER that will provide a username and a password to set up a safe communication between the keyboard and the server. This automatic configuration is recommended for most of the use cases, since it is more secure and simple instead of the manual configuration.
MANUAL CONFIGURATION	When selected, the configuration of the safe communication between the ACCÉDO KEY and the DELÉGO SERVER must be managed by the user that has to select the authentication type (none, allowist, basic, digest) and if basic or digest are selected, must enter a username and password.

5.3.1 Automatic authentication

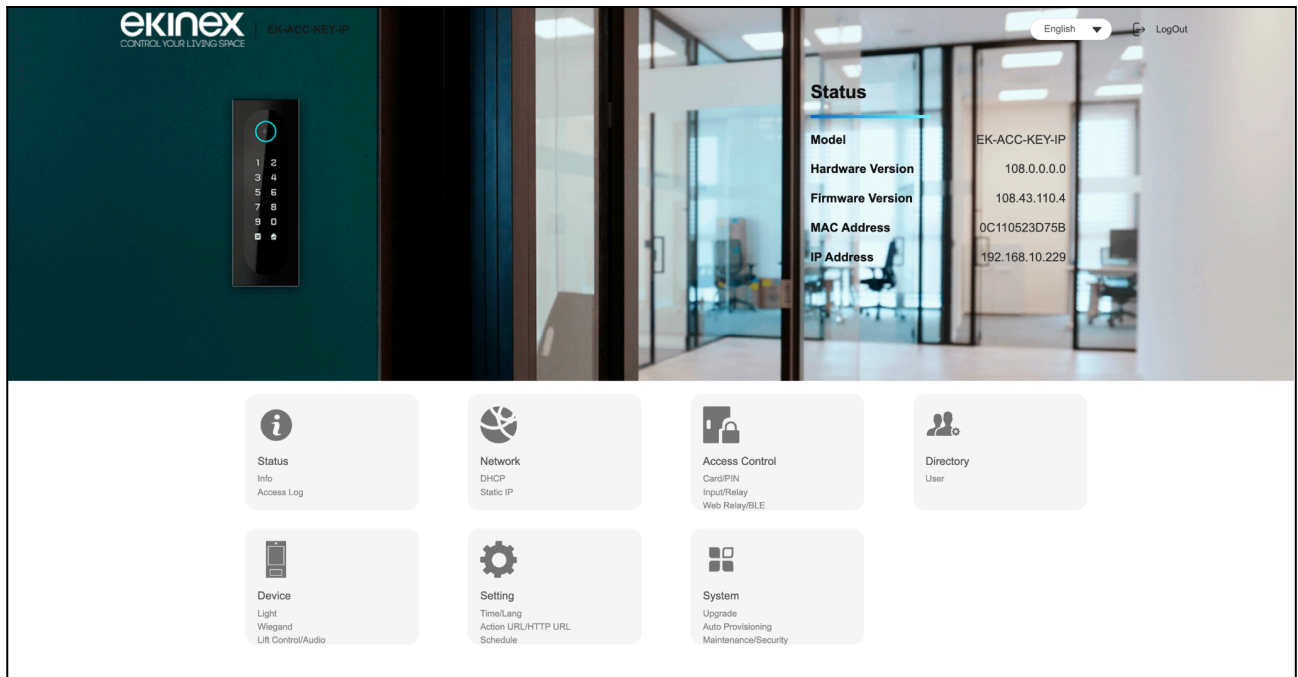
In this case, the DELÉGO SERVER manages centrally the authentication of the ACCÉDO KEY, by setting automatically the following parameters:

- Credentials for the web access
- Credentials for the HTTP API communication (and the corresponding enable flag)
- Credentials for the relay command through the network (and the corresponding enable flag)

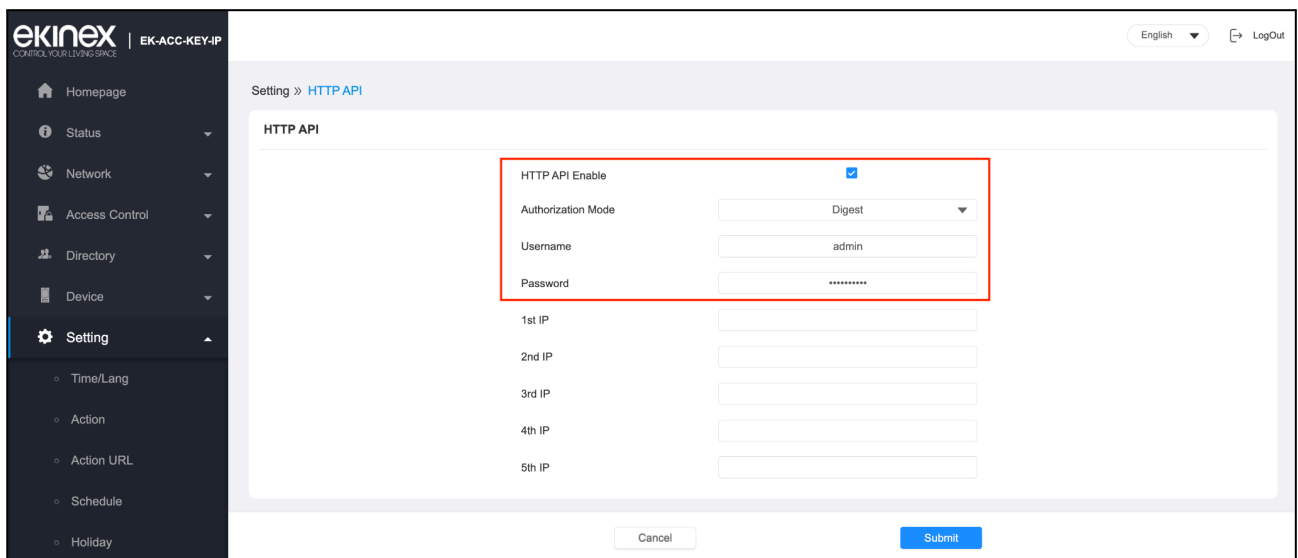
5.3.2 Manual authentication

If the MANUAL CONFIGURATION is selected, before proceeding with the configuration on DELÉGO SERVER it is required to perform the following preconditions steps:

- Open a browser and search the IP address of the ACCÉDO KEY device that you need to configure



- If it's the first time entering this Web Page, enter the default credentials (username: admin / password: admin) **and change them as required, for security reasons**
- Enter the menu **SETTING > HTTP API** and change the following settings:
 - Select the checkbox "HTTP API enable"
 - Select an authentication method (it is recommended to use DIGEST)
 - Enter a USERNAME and a PASSWORD to be used for the communication between the device and DELÉGO SERVER (and/or third party software)
 - Confirm the changes by pressing the SUBMIT button



- Enter the menu **ACCESS CONTROL > RELAY** and in the section "OPEN RELAY VIA HTTP":
 - Select the checkbox "Enabled"
 - Enter **the same USERNAME and PASSWORD** set in the "HTTP API" menu
 - Confirm the changes by pressing the SUBMIT button

When the preconditions steps are completed, return to the ACCÉDO KEY menu configuration on the DELÉGO SERVER web page and enter the following information:

AUTHENTICATION TYPE	Select the same authentication method that has been set in the device's web interface
USERNAME PASSWORD	Credentials for DIGEST or BASIC authentication

5.3.3 Save and check connection

Regardless of the configuration method selected, to complete the configuration it must be pressed the button UPDATE CONFIG. The DELÉGO SERVER will attempt to establish a communication channel with the device and in case of success, the following changes will occur:

- The ACTIVE checkbox will be flagged
- In case of an automatic configuration, the username and password will become visible
- The *additional settings* will be displayed below, as depicted in the following picture:

The screenshot shows the 'delégo' web interface. On the left is a sidebar menu with categories like Setup, Technologies, Floors, Functions, Scenes, Notifications, Connections, Logics, Advanced functions, Options, Load control, Consumption monitor, Data log, Access Control, Settings, Rooms, Gates, Accédo Key, User groups, Timetables, Access logs and operations, Virtual presence, Services, Users and permissions, and Change password. The main area is titled 'Additional settings' and contains several sections: 'Authentication' with radio buttons for 'Manage automatically' (selected) and 'Manual configuration', and fields for 'Username' (admin) and 'Password' (masked); 'Relay' with input fields for 'Internal relay - Trigger delay [s]' (0) and 'Internal relay - Hold delay [s]' (5), and 'Security relay - Trigger delay [s]' (0) and 'Security relay - Hold delay [s]' (5), each with a 'TEST' button; 'Network' with radio buttons for 'DHCP' (selected) and 'Static IP'; 'Audio' with sliders for 'Voice feedback volume' and 'Keyboard volume'; and 'Light' with a 'Keyboard backlight mode' dropdown (Off), a checkbox for 'Enable status light' (checked), and a 'Status light intensity' slider. At the bottom of the settings area are 'CLOSE' and 'SAVE' buttons. A blue box highlights the authentication fields with the label 'Credentials for the device', and a pink box highlights the entire settings area with the label 'Additional settings'.

In the *additional settings* the user can

- verify if the internal relay and the security relay of the ACCÉDO KEY are working correctly and can change the trigger and hold delay of both the relays.
- Change the network configuration (DHCP or Static IP, it is suggested to keep the default option DHCP).
- Change the audio volume and the light settings of the keyboard.

See [section 5.4](#) for further details.

If the configuration is not completed successfully, a popup error is displayed on the upper part of the menu. The possible issues can be the following:

- The IP address field is empty.
- The IP address inserted is not correct (i.e., device does not have that IP address) or has an invalid format (usually it must be 192.168.XXX.YYY).
- In case of manual configuration, the precondition steps explained above were not followed correctly.
- In case of manual configuration, the authentication information was not populated correctly as in the ACCÉDO KEY web page.

5.4 Additional settings

RELAY

TRIGGER DELAY	The delay before the opening of the relay. The min value is 0 and the max value is 10. The option is the same for both the INTERNAL RELAY and the SECURITY RELAY (connected to the RS485 port of the ACCÉDO KEY)
---------------	---

HOLD DELAY	The time for which the relay is excited (e.g. the time for which the lock of the room or gate is kept open). The Min value is 0 and the max value is 60. The option is the same for both the INTERNAL RELAY and the SECURITY RELAY (connected to the RS485 port of the ACCÉDO KEY)
------------	--

NETWORK

NETWORK MODE	Allows to determine if the device must be addressed automatically (DHCP) or manually (Static IP)
IP ADDRESS SUBNET MASK DEFAULT GATEWAY PRIMARY DNS SECONDARY DNS	In case the Static IP is selected, enter the information for the static IP assignment: - IP Address - Subnet mask - Default Gateway - Primary DNS - Secondary DNS Once saved, if the IP Address was changed it is necessary to change also the IP address in the General Information section and re-do again the communication configuration of the ACCÉDO KEY.

AUDIO

VOICE FEEDBACK VOLUME	Volume of the audio feedback
KEYBOARD VOLUME	Volume of the feedback when the numeric keypad is pressed

LIGHT

KEYBOARD BACKLIGHT MODE	Allows to determine when the backlight of the numeric keyboard must be switched ON: • Never (OFF) • Always (ON) • When the proximity sensor detects a movement (AUTOMATIC)
ENABLE STATUS LIGHT	Enables or not the light around the camera
STATUS LIGHT INTENSITY	Brightness of the light around the camera

When changing one or more of the settings listed above, confirm the modifications by pressing SAVE.

5.5 Assigning to rooms and gates

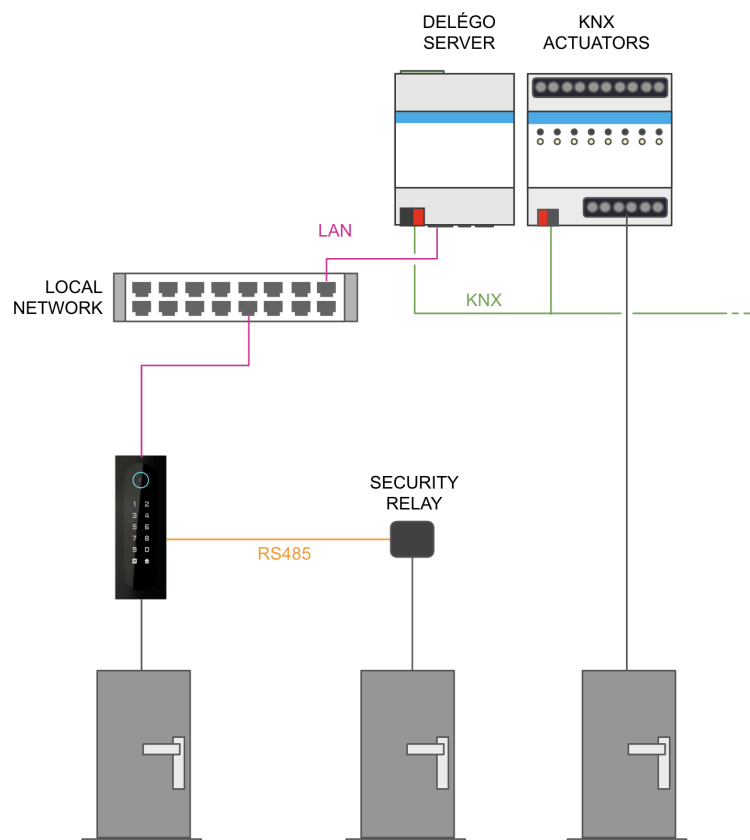
After the creation and configuration of an ACCÉDO KEY device, it is now possible to associate it to a ROOM or a GATE. To connect a keyboard to a Room/Gate:

- Open the details page of the desired ROOM or GATE (see [section 4.2](#) or [section 4.5](#))
- Enable the EXPERT mode ()

- From the side bar menu select the ACCÉDO KEY that you want to map to the Room or Gate and Drag&Drop it in the ACCÉDO KEY section of the ROOM or GATE.

With this operation, the INTERNAL RELAY of the ACCÉDO KEY will be automatically linked to the LOCK of the ROOM / GATE. By means of the CONNECTIONS function, this relationship can be modified (see [section 7](#)).

One ACCÉDO KEY can be associated with more than one ROOM or GATE. In this way when a Guest or a Service personnel successfully access the Room or Gate assigned to him (by means of a PIN, QR Code or RFID Card), the system will open only the door related to the Room or Gate of the user. The following figure depicts a use case of this architectural design:



In this kind of configuration, it is fundamental to set the relationship for the LOCK of each ROOM / GATE with the appropriate

- Internal relay
- Security relay
- KNX actuator



The same relay of an ACCÉDO KEY cannot be related with multiple ROOM(s) or GATE(s). Otherwise, all the locks would open simultaneously.

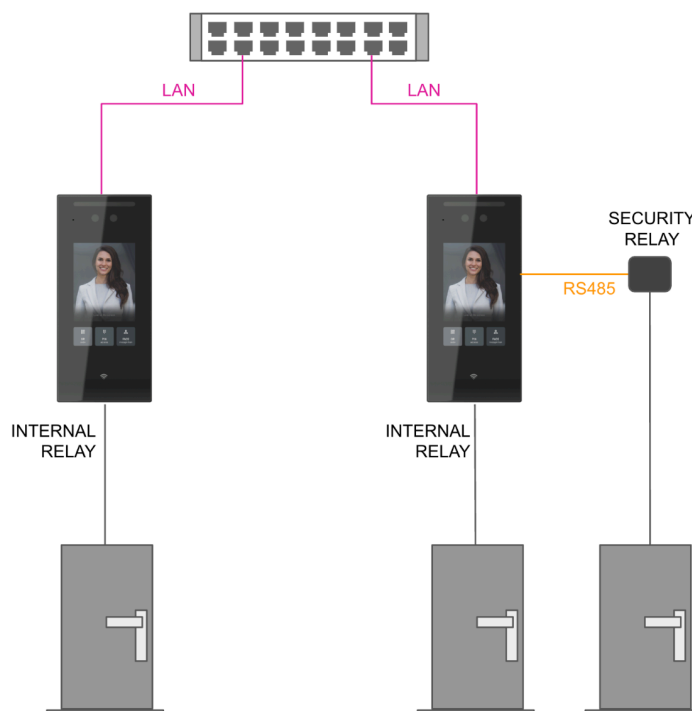
6 Dico

6.1 Introduction

DICO is an IP-based video intercom that can allow an user to type a PIN on its display, scan a QR CODE with its integrated camera and read a RFID Card. The power supply can be provided either with a POE network cable, or a dedicated power supplier.

Like the ACCÉDO KEY, it offers the possibility to open an electric lock:

- Directly wired to its internal relay
- Wired to a SECURITY RELAY, connected through the integrated RS485 port

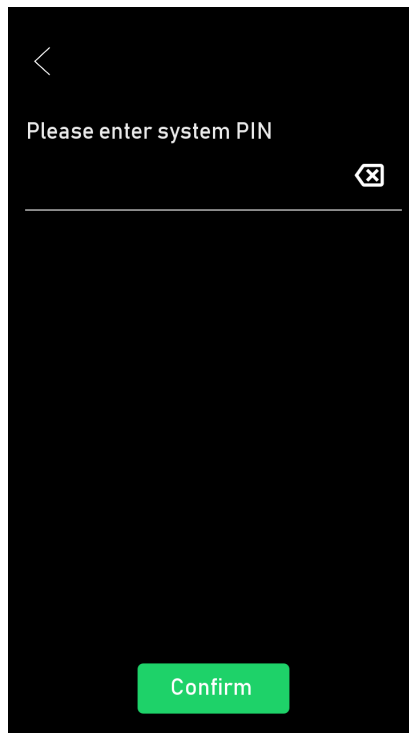


6.2 Preliminary operations

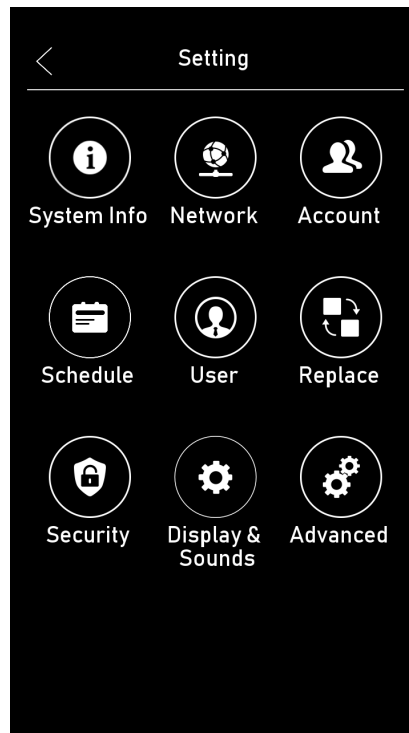
In order to use a DICO in combination with DELÉGO SERVER for the access control, it is necessary to:

1. Connect it to the lock(s) to be opened
2. Connect it to the LAN with an RJ45 cable
3. Connect the power supply (if not provided with a POE network cable)
4. Identify the IP Address assigned by the DHCP server

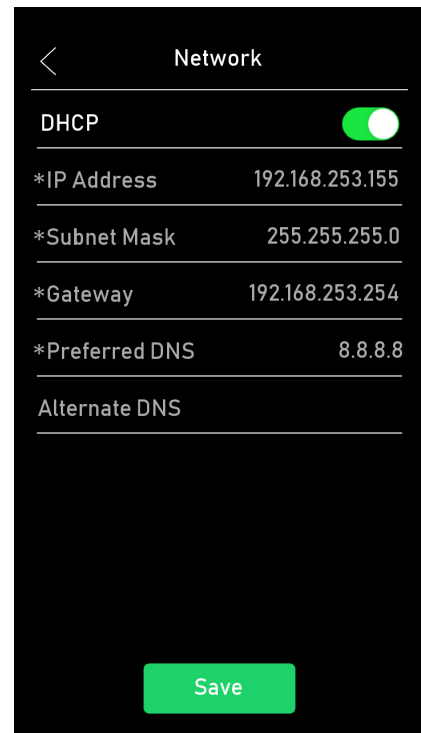
To know the IP Address of a DICO you must access the settings of the video intercom in the following way:



Press anywhere on the screen of the DICO and hold your finger down for more than 10 seconds until you are asked for a password. Enter *admin* and press Confirm



Select *Network*



Take note of the IP Address of the Outdoor Unit



For further details, please refer to the technical documentation and application manual of the product in its related section of the EKINEX website

6.3 Create a new device



Since a DICO is a video intercom that uses VoIP protocol, in the DELÉGO SERVER the configuration menu is found in the VOIP INTERCOM technology section.

To add a new DICO device, in the DELÉGO SERVER web page, navigate to the section

TECHNOLOGIES > VOIP INTERCOM > DICO

and press the [+] button in the toolbar.

The following figure depicts the details page of the DICO.

The user must insert the following information:

GENERAL INFORMATION

NAME	Label identifying the DICO
NUMBER	VoIP number to be used to call the DICO device. To be populated if DELÉGO SERVER is the SIP server. Note: for access control functionalities, this entry can be ignored.
PASSWORD	Password to protect the VoIP function. To be populated if DELÉGO SERVER is the SIP server. Note: for access control functionalities, this entry can be ignored.
HOST (IP ADDRESS)	The IP address of the DICO in the local network
ACTIVE	This field (in read-only) is flagged only when the DICO is successfully configured.
ENABLE BADGE CONFIGURATION	If the RFID Card management is enabled (see section 3.1.3), when this checkbox is selected, this DICO can be used to enable a RFID Card to open a Room or Gate by means of the function SCAN (see section 12.2.8)

AUTHENTICATION

MANAGE AUTOMATICALLY	When selected, the configuration of the DICO is automatically managed by DELÉGO SERVER that will provide a username and a password to set up a safe communication between the intercom and the server. This automatic configuration is recommended for most of the use cases, since it is more secure and simple instead of the manual configuration.
MANUAL CONFIGURATION	When selected, the configuration of the safe communication between the DICO and the DELÉGO SERVER must be managed by the user that has to select the authentication type (none, allowist, basic, digest) and if basic or digest are selected, must enter a username and password.

6.3.1 Automatic authentication

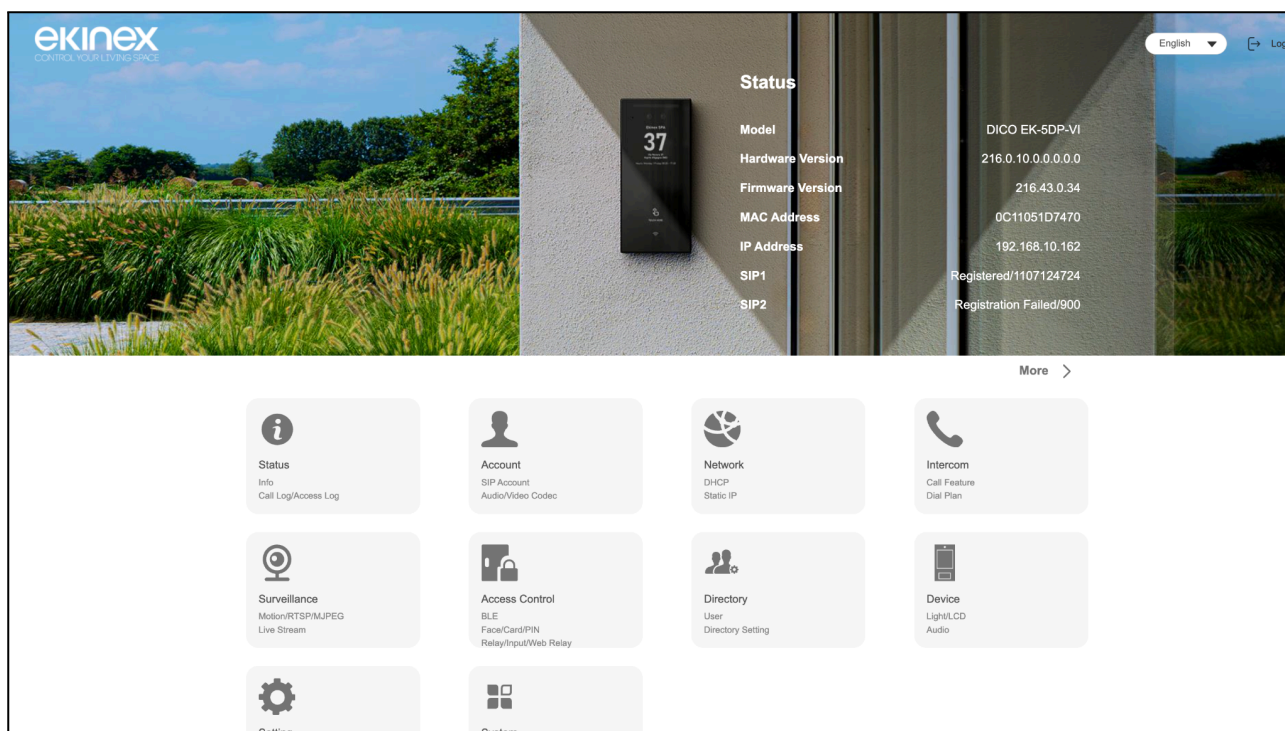
In this case, the DELÉGO SERVER manages centrally the authentication of the DICO, by setting automatically the following parameters:

- Credentials for the web access
- Credentials for the HTTP API communication (and the corresponding enable flag)
- Credentials for the relay command through the network (and the corresponding enable flag)

6.3.2 Manual authentication

If the MANUAL CONFIGURATION is selected, before proceeding with the configuration on DELÉGO SERVER it is required to perform the following preconditions steps:

- Open a browser and search the IP address of the DICO device that you need to configure



- If it's the first time entering this Web Page, enter the default credentials (username: admin / password: admin) **and change them as required, for security reasons**
- Enter the menu **SETTING > HTTP API** and change the following settings:
 - Select the checkbox "HTTP API enable"
 - Select an authentication method (it is recommended to use DIGEST)
 - Enter a USERNAME and a PASSWORD to be used for the communication between the device and DELÉGO SERVER (and/or third party software)
 - Confirm the changes by pressing the SUBMIT button

- Enter the menu **ACCESS CONTROL > RELAY** and do the following operations and in the section “OPEN RELAY VIA HTTP”:
 - Select the checkbox “Enabled”
 - Enter **the same USERNAME and PASSWORD** set in the “HTTP API” menu
 - Confirm the changes by pressing the SUBMIT button

When the precondition steps are completed, return to the DICO menu configuration on the DELÉGO SERVER web page and enter the following information:

AUTHENTICATION TYPE	Select the same authentication method that has been set in the device's web interface
USERNAME PASSWORD	Credentials for DIGEST or BASIC authentication

6.3.3 Save and check connection

Regardless of the configuration method selected, to complete the configuration it must be pressed the button UPDATE CONFIG. The DELÉGO SERVER will attempt to establish a communication channel with the device and in case of success, the following changes will occur:

- The ACTIVE checkbox will be flagged
- In case of an automatic configuration, the username and password will become visible
- The *additional settings* will be displayed on the bottom part of the page as depicted in the following picture:

The screenshot shows the Delégo web interface. On the left is a sidebar menu with categories like Setup, Technologies, VoIP Intercom, etc. The main area is titled 'Authentication' and has two options: 'Manage automatically' (selected) and 'Manual configuration'. Below these are fields for 'Username' (admin) and 'Password' (masked with dots). A blue box highlights these fields with the label 'Credentials for the device'. Below the authentication section is a 'Relay' section with fields for 'Internal relay - Trigger delay [s]' (0) and 'Internal relay - Hold delay [s]' (5), and 'Security relay - Trigger delay [s]' (0) and 'Security relay - Hold delay [s]' (5). There are 'TEST' buttons for each relay. Below the relay section is a 'Language' section with a dropdown menu set to 'Italian'. Below that is a 'Network' section with radio buttons for 'DHCP' (selected) and 'Static IP'. Below the network section is an 'Audio' section with sliders for 'Voice feedback volume', 'Microphone volume', and 'Speaker volume', and a checkbox for 'Enable door opening tone' which is checked. Below the audio section is a 'Light' section with a dropdown for 'Lighting mode' set to 'Automatic' and a slider for 'Status light intensity'. A pink box highlights the 'Relay', 'Language', 'Network', 'Audio', and 'Light' sections with the label 'Additional settings'.

In the *additional settings* the user can

- Verify if the internal relay and the security relay of the DICO are working correctly and can change the trigger and hold delay of both the relays.
- Change the network configuration (DHCP or Static IP, it is suggested to keep the default option DHCP).
- Change the audio volume, the light and the video settings.

See [section 6.4](#) for further details.

If the configuration is not completed successfully, a pop-up error is displayed on the upper part of the menu. The possible issues can be the following:

- The IP address field is empty.
- The IP address inserted is not correct (i.e., device does not have that IP address) or has an invalid format (usually it must be 192.168.XXX.YYY).
- In case of manual configuration, the precondition steps explained above were not followed correctly.
- In case of manual configuration, the authentication information was not populated correctly as in the DICO web page.

6.4 Additional settings

RELAY

TRIGGER DELAY	The delay before the opening of the relay. The min value is 0 and the max value is 10. The option is the same for both the INTERNAL RELAY and the SECURITY RELAY (connected at the RS485 port of the DICO)
HOLD DELAY	The time for which the relay is excited (e.g. the time for which the lock of the room or gate is kept open). The Min value is 0 and the max value is 60. The option is the same for both the INTERNAL RELAY and the SECURITY RELAY (connected to the RS485 port of the DICO)

NETWORK

(NETWORK MODE)	Allows to determine if the device must be addressed automatically (DHCP) or manually (Static IP)
IP ADDRESS SUBNET MASK DEFAULT GATEWAY PRIMARY DNS SECONDARY DNS	In case the Static IP is selected, enter the information for the static IP assignment: - IP Address - Subnet mask - Default Gateway - Primary DNS - Secondary DNS Once saved, if the IP Address was changed it is necessary to change also the IP address in the General Information section and re-do again the communication configuration of the DICO.

AUDIO

VOICE FEEDBACK VOLUME	Volume level of the feedback audio of the DICO when accessing the Room or gate
MICROPHONE VOLUME	Volume level for the integrated microphone of the DICO
SPEAKER VOLUME	Volume level for the speaker during a call
ENABLE DOOR OPENING TONE	Enables or not the audio effect when the relay is opened

LIGHT

LIGHTING MODE	Activation status of the LED on the top of the product: • Always OFF • Automatic with proximity and brightness sensor
---------------	--

STATUS LIGHT INTENSITY	Brightness of the LED
------------------------	-----------------------

VIDEO

ENABLE RTSP	Enables the video streaming for voice calls
FORMAT	Video cropping of the video streaming: • Vertical • Horizontal

When changing one or more of the settings listed above, confirm the modifications by pressing SAVE.

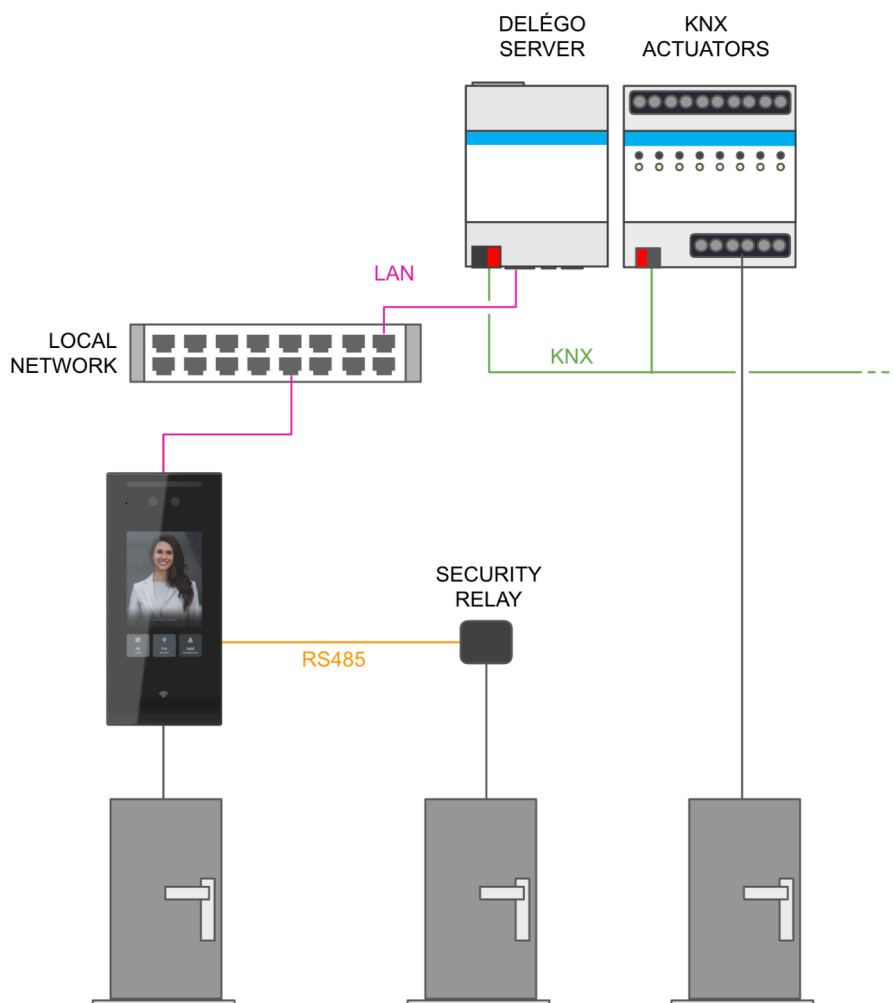
6.5 Assigning to rooms and gates

After the creation and configuration of a DICO device, it is now possible to associate it to a ROOM or a GATE. To connect an intercom to a Room/Gate:

- Open the details page of the desired ROOM or GATE (see [section 4.2](#) or [section 4.5](#))
- Enable the EXPERT mode ()
- From the side bar menu select the DICO that you want to map to the Room or Gate and Drag&Drop it in the DICO section of the ROOM or GATE.

With this operation, the INTERNAL RELAY of the DICO will be automatically linked to the LOCK of the ROOM / GATE. By means of the CONNECTIONS function, this relationship can be modified (see [section 7](#)).

Like for the ACCÉDO KEY, also a single DICO can be associated with more than one ROOM or GATE. In this way when a Guest or a Service personnel successfully access the Room or Gate assigned to him (by means of a PIN, QR Code or RFID Card), the system will open only the door related to the Room or Gate of the user. The following figure depicts a use case of this architectural design:



In this kind of configuration, it is fundamental to set the relationship for the LOCK of each ROOM / GATE with the appropriate:

- Internal relay
- Security relay
- KNX actuator



The same relay of a DICO cannot be related with multiple ROOM(s) or GATE(s). Otherwise, all the locks would open simultaneously.

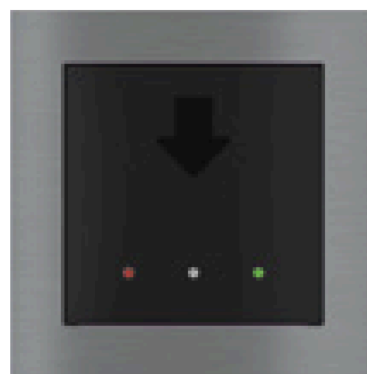
7 Ekinex KNX badge readers / holders

7.1 Introduction

The EKINEX badge readers and holders based on KNX technology can be integrated in the guest room management of Delégo Server.

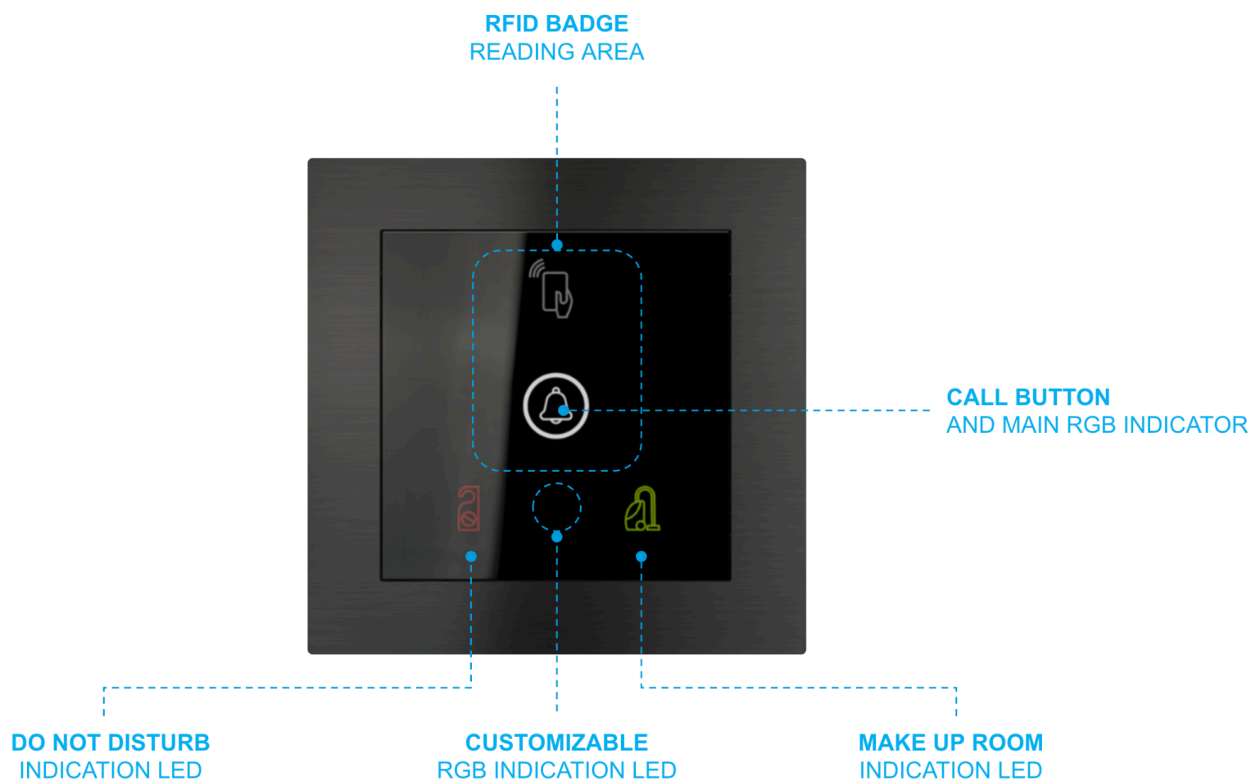


BADGE READER
EK-TO2-TP

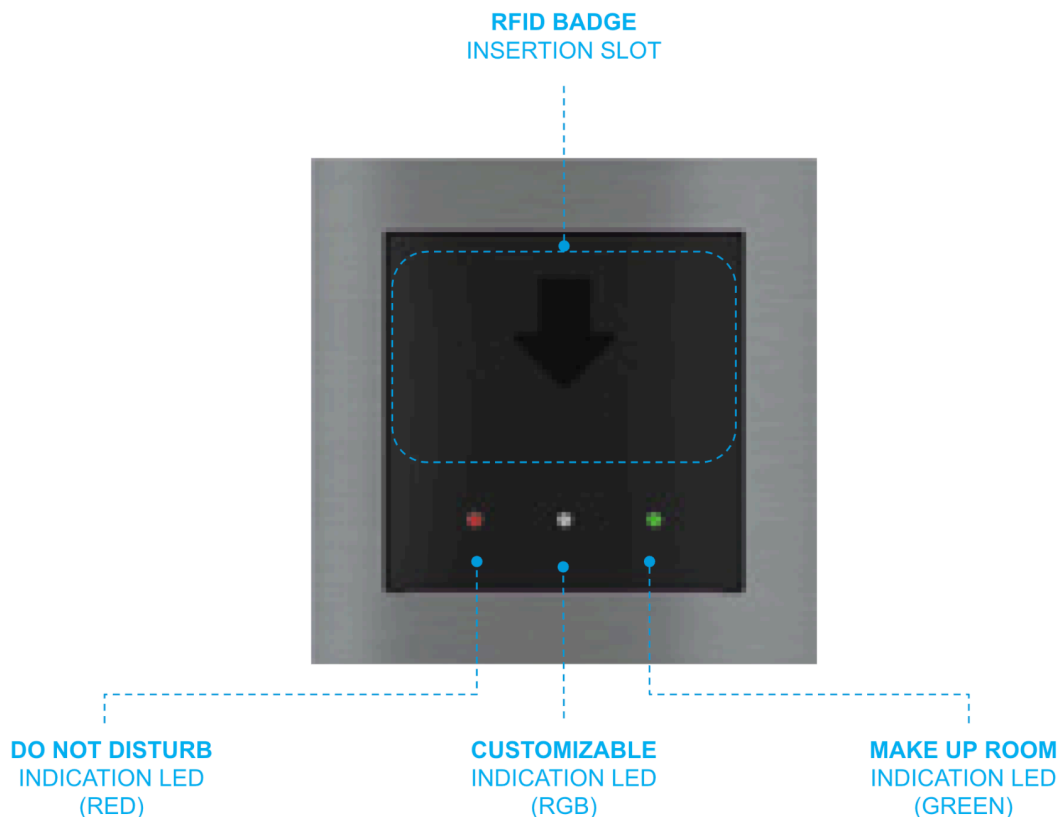


BADGE HOLDER
EK-TI2-TP

The BADGE READERS protect the access to the rooms and common areas, by reading an RFID badge and checking if it's allowed to open the corresponding door. They are normally installed outside a space which access must be restricted.



The BADGE HOLDERS are installed inside a room / common area; when a badge is inserted in, the presence information is given to the system, and corresponding actions can be taken (e.g. enable loads, A/C, execute scenes etc...)



Both the READERS and HOLDERS have two integrated relays that can be used for multiple purposes:

- Open the door
- Switch ON / OFF a courtesy light
- Enable / disable the room loads / HVAC
- Etc...

7.2 Access control strategy

DELÉGO SERVER can regulate the access to doors protected by the EKINEX BADGE READERS with two different strategies:

CENTRALIZED	When a badge is presented to the readers, they send a TRANSIT information on the KNX bus. According to the authorizations valid for that moment, DELÉGO SERVER determines if the badge is entitled or not to open the door. If so, an ON command is sent to the ACCESS GRANTED address of the reader; the relay connected to the lock is expected to be enabled by the
-------------	---

	reader itself, and the main LED indicator is set to GREEN for some seconds. As opposed, if the badge is not valid, a command is sent to the ACCESS DENIED address; in such a case, the relay is not enabled, and the LED indicator is temporarily set to RED.
DECENTRALIZED	At the beginning and end of the validity period of a badge (or after any change to its authorizations) DELÉGO SERVER sends to the interested reader(s) the information about the permission grants for that badge. When the badge is presented to the entitled readers, they autonomously trigger the ACCESS GRANTED or DENIED (by setting the LED colour and eventually enabling the relay connected to the lock) and send on the bus the TRANSIT information (containing in this case also the information if the transit was valid or not)



The decentralized strategy requires the following minimum versions for the BADGE READER (EK-TO2-TP) and HOLDER (EK-TI2-TP):

- Firmware: 2.0.0
- ETS library: 0.2

7.3 Readers and holders widget creation

When an ETS project is imported, the EKINEX KNX BADGE READERS and HOLDERS are automatically detected, and the corresponding widgets are created in the section

FIELD TECHNOLOGIES > KNX > KNX WIDGETS > ACCESS CONTROL

These widgets can be eventually also created manually; for more information on the ETS import and the KNX widgets, please refer to the KNX FIELD TECHNOLOGY CONFIGURATION MANUAL [D3].

7.3.1 Badge readers sub-objects

The following table contains all the sub-objects offered by the modeling of the EKINEX BADGE READERS in DELÉGO SERVER; these objects are normally associated to one or more KNX group addresses for the bidirectional communication between the webserver and the device.

TRANSIT	When a badge is read, its unique ID and other additional information are sent to the KNX bus on this address. This object is monitored by DELÉGO SERVER to detect the transit of a badge on each installed reader.
STATUS	Contains status information of the device. If this item is assigned to a group address, the STATUS OBJECTS section is displayed below.

	<i>Note: this item can be assigned to an address only if the WHITELIST has been enabled in ETS</i>
WHITELIST	This item is necessary for the decentralized authentication strategy, being used by the webserver to add or remove the badges from the internal whitelist of the access device
DO NOT DISTURB (DND)	When enabled, the corresponding LED is switched ON on the reader, meaning that the guest(s) inside the room don't want to be disturbed by the staff members (e.g. for the daily cleaning)
MAKE UP ROOM (MUR)	When enabled, the corresponding LED is switched ON on the reader, meaning that the guest(s) want an additional cleaning of the room
RELAY 1 RELAY 2	First and second integrated relay, if they have been configured in ETS to be controlled independently (and not associated to a functionality e.g. the door lock)
INPUT 1 INPUT 2	First and second integrated digital input, if they have been configured in ETS to be monitored independently (and not associated to a functionality e.g. DND or MUR)
RING	When the ring button is pressed (if enabled in ETS) this object is set temporarily to the ON value (normally it is OFF)
LED ON/OFF LED COLOR LED RGB	These objects offer three different ways to take control of the customizable LED: • ON/OFF: LED is switched ON or OFF • COLOR: the LED is set to a specific colour given by a palette, where each colour has a corresponding numeric value • RGB: the LED is set to a custom colour that can be freely assigned
ACCESS GRANTED	This special object is set to ON by the READER if the presented badge is valid to unlock the door (and the corresponding RELAY is activated for a specific amount of time, as specified in the ETS configuration)
ACCESS DENIED	This special object is set to ON by the READER if the presented badge is <u>not</u> valid to unlock the door
VIRTUAL PRESENCE	If enabled in ETS, this item represents the virtual presence calculated by the internal algorithm of the device. This algorithm is an alternative to the virtual presence elaborated centrally in the webserver.

The screenshot shows the delégo webserver interface. On the left is a navigation menu with categories like Setup, Field technologies, User interface, and Settings. The main area is divided into 'Object properties' and 'KNX addresses'.

Object properties:

- General information:** ID: 1622, Name: Badge reader 1, Description: Badge reader 1.
- Permissions:** Visible: ☒.
- Access control:** Use for badge scan: ☐.

KNX addresses:

FUNCTIONALITY	COMMAND	FEEDBACK	ETS ENCODING	MIN	MAX	STEP	VIS.	WRITE	READ	SCH/TRG	SCEN.	STATE	LIBRARY
Transit	+	-	14 byte extended access data									Off	
Do Not Disturb	+	-	1 bit (DPT 1.x)									Off	
Make Up Room	+	-	1 bit (DPT 1.x)									Off	
Relay 1	+	-	1 bit (DPT 1.x)									Off	
Relay 2	+	-	1 bit (DPT 1.x)									Off	
Input 1	+	-	1 bit (DPT 1.x)									Off	
Input 2	+	-	1 bit (DPT 1.x)									Off	
Ring	+	-	1 bit (DPT 1.x)									Off	
LED ON/OFF	+	-	1 bit (DPT 1.x)									Off	
LED color	+	-	1 byte unsigned int (DPT 5.010)									0	
LED RGB	+	-	3 byte RGB (DPT 232.600)									0	
Access granted	+	-	1 bit (DPT 1.x)									Off	
Access denied	+	-	1 bit (DPT 1.x)									Off	

If the status item is associated to an address, the following additional information items are listed in the STATUS OBJECTS list; this is only available when the WHITELIST (decentralized authentication) is activated in ETS:

LAST OPERATION	Result of the last operation regarding the whitelist
MAXIMUM TIMETABLES COUNT	The maximum number of timetables that can be stored in the device for an user group. Normally this value is NO LIMITS meaning that each weekday can have an independent timetable for each group. In the ETS library it is possible to limit the number of timeslots (e.g. 2 per week) in order to increase the number of badges that can be stored in the whitelist; in that case, it is important to keep the number of timetables under the limit.
MAXIMUM CARDS COUNT	The maximum number of badges that can be stored in the whitelist
ACTIVE CARDS COUNT	The number of badges actually present in the whitelist, authorized to access the door

In normal conditions DELÉGO SERVER does not take directly control of the relay where the door lock is connected, but it handles the ACCESS GRANTED or DENIED objects instead; this permits not to care (in the webserver) which is the relay to be activated to unlock the door (this is configured in ETS).

In specific conditions, the relays of the reader could be left unassigned and freely controllable with the corresponding KNX group addresses; in such a case, it is necessary to bind the specific relay to the LOCK command of a room or gate, as explained in the next chapter dedicated to the *automations*.

7.3.2 Badge holders sub-objects

The following table contains all the sub-objects offered by the modeling of the EKINEX BADGE HOLDERS in DELÉGO SERVER; these objects are normally associated to one or more KNX group addresses for the bidirectional communication between the webserver and the device.

TRANSIT	When a badge is inserted, its unique ID and other additional information are sent to the KNX bus on this address.
WHITELIST	If the WHITELIST is enabled in the ETS library, the corresponding group address must be entered here. In such a case, DELÉGO SERVER writes the allowed badges for a room not only in the reader(s) but also in the holder(s) meaning that other badges cannot enable the room loads.
PRESENCE	When a badge is inserted, this object is set to ON and remains that state until the badge is removed.
RELAY 1 RELAY 2	First and second integrated relay, if they have been configured in ETS to be controlled independently (and not associated to a functionality e.g. the door lock)
INPUT 1 INPUT 2	First and second integrated digital input, if they have been configured in ETS to be monitored independently (and not associated to a functionality e.g. DND or MUR)
RING	When the ring button is pressed (if enabled in ETS) this object is set temporarily to the ON value (normally it is OFF)
LED ON/OFF LED COLOR LED RGB	These objects offer three different ways to take control of the customizable LED: • ON/OFF: LED is switched ON or OFF • COLOR: the LED is set to a specific colour given by a palette, where each colour has a corresponding numeric value • RGB: the LED is set to a custom colour that can be freely assigned Note: which of these object(s) to be used depend on the ETS configuration
DO NOT DISTURB (DND)	When enabled, the corresponding LED is switched ON to indicate (inside the room) that the DO NOT DISTURB function has been activated.
MAKE UP ROOM (MUR)	When enabled, the corresponding LED is switched ON to indicate (inside the room) that the MAKE UP ROOM function has been activated.

delégo

Object properties

General information

ID: 1636

Name: Badge holder 1

Description:

Permissions

Visible: ☒

Access control

Use for badge scan: ☐

KNX addresses

FUNCTIONALITY	COMMAND	FEEDBACK	ETS ENCODING	MIN	MAX	STEP	VIS.	WRITE	READ	SCH/TRG	SCEN.	STATE	LIBRARY
Transit		+/+	14 byte extended access data										
Presence		+/+	1 bit (DPT 1.x)										
Relay 1	+/+	+/+	1 bit (DPT 1.x)									Off	
Relay 2	+/+	+/+	1 bit (DPT 1.x)									Off	
Input 1		+/+	1 bit (DPT 1.x)										
Input 2		+/+	1 bit (DPT 1.x)										
LED ON/OFF	+/+	+/+	1 bit (DPT 1.x)									Off	
LED color	+/+	+/+	1 byte unsigned int (DPT 5.010)									0	
LED RGB	+/+	+/+	3 byte RGB (DPT 232.600)									0	
Do Not Disturb	+/+	+/+	1 bit (DPT 1.x)									Off	
Make Up Room	+/+	+/+	1 bit (DPT 1.x)									Off	

Access Control Badge holder 1

7.4 Binding to rooms and gates

By enabling the expert mode, the following section is made available in the details page of a ROOM or a GATE:

EKINEX BADGE READERS AND HOLDERS

In order to bind a READER and/or a HOLDER to the ROOM / GATE, do as follow:

- Search for the READER / HOLDER by entering its name (or a part of the name) in the SEARCH.
As an alternative, press on the section title: the complete list of devices will be automatically displayed in the side menu
- Drag & drop the desired device(s) into the section

The screenshot shows the delégo web interface. On the left is a sidebar with a search bar and a tree menu. The tree menu has three items: 'Room 1 - Badge Holder', 'Room 1 - Badge Reader', and 'Room 1 - Badge Reader (ID: 1564)'. A red arrow points from the 'Room 1 - Badge Reader' item to the 'KNX badge readers / holders' section in the main content area.

The main content area has a top toolbar with icons for file operations. Below the toolbar is a table of settings:

...	...	...	...	...	...	...	...	...	...
Presence	✓	-						Off	+
Do not disturb	✓	-						Off	+
Alarm	✓	-						OK	+
Make up room	✓	-						Off	+
Door sensor		-						Off	+
Motion sensor		-						Off	+
Motion sensor 2		-						Off	+

Below this table are sections for 'Time tables', 'Guests', 'Dico', 'Accédo Key', and 'KNX badge readers / holders'. Each section has a table with columns for NAME, HOST, and ENABLE. The 'KNX badge readers / holders' section has a table with columns for NAME, TYPE, DETAILS, ENABLE, VISIBLE, CLOUD, and LIBRARY.

NAME	TYPE	DETAILS	ENABLE	VISIBLE	CLOUD	LIBRARY
Room 1 - Badge Holder	Badge Holder		✓	✓		
Room 1 - Badge Reader	Badge Reader		✓	✓		

The bottom of the interface shows a 'Menu' button and a status bar with 'Room 1' and 'Access Control' tabs.

When a READER is associated with a ROOM / GATE, it is automatically used to validate RFID badges and to trigger the ACCESS GRANTED / DENIED, through the CONNECTIONS as explained in the following chapter.

8 Automations

8.1 Introduction

When a GUEST uses a valid PIN, QR CODE or RFID Card, the property LOCK of the corresponding ROOM or GATE is set to OPEN for a certain amount of seconds (as configured in the GENERAL SETTINGS in [section 3.1](#)). Furthermore, also the GRANTED property is set to ON for the same time interval; if the access is invalid, as opposite, the DENIED attribute is triggered.

These are *virtual objects* representing the lock of the associated door and the valid / invalid access; they can be associated (with a *relationship*) with the real object that sends the command to the relay, which is physically connected to the electric lock.

As previously mentioned, it can be:

- The integrated RELAY of a DICO or ACCÉDO KEY
- A SECURITY RELAY connected to a DICO or ACCÉDO KEY via RS485
- The relay of an EKINEX KNX badge reader (or holder)
- The channel of a KNX actuator (represented with a KNX WIDGET inside DELÉGO SERVER)

This relationship can be done in 3 ways¹:

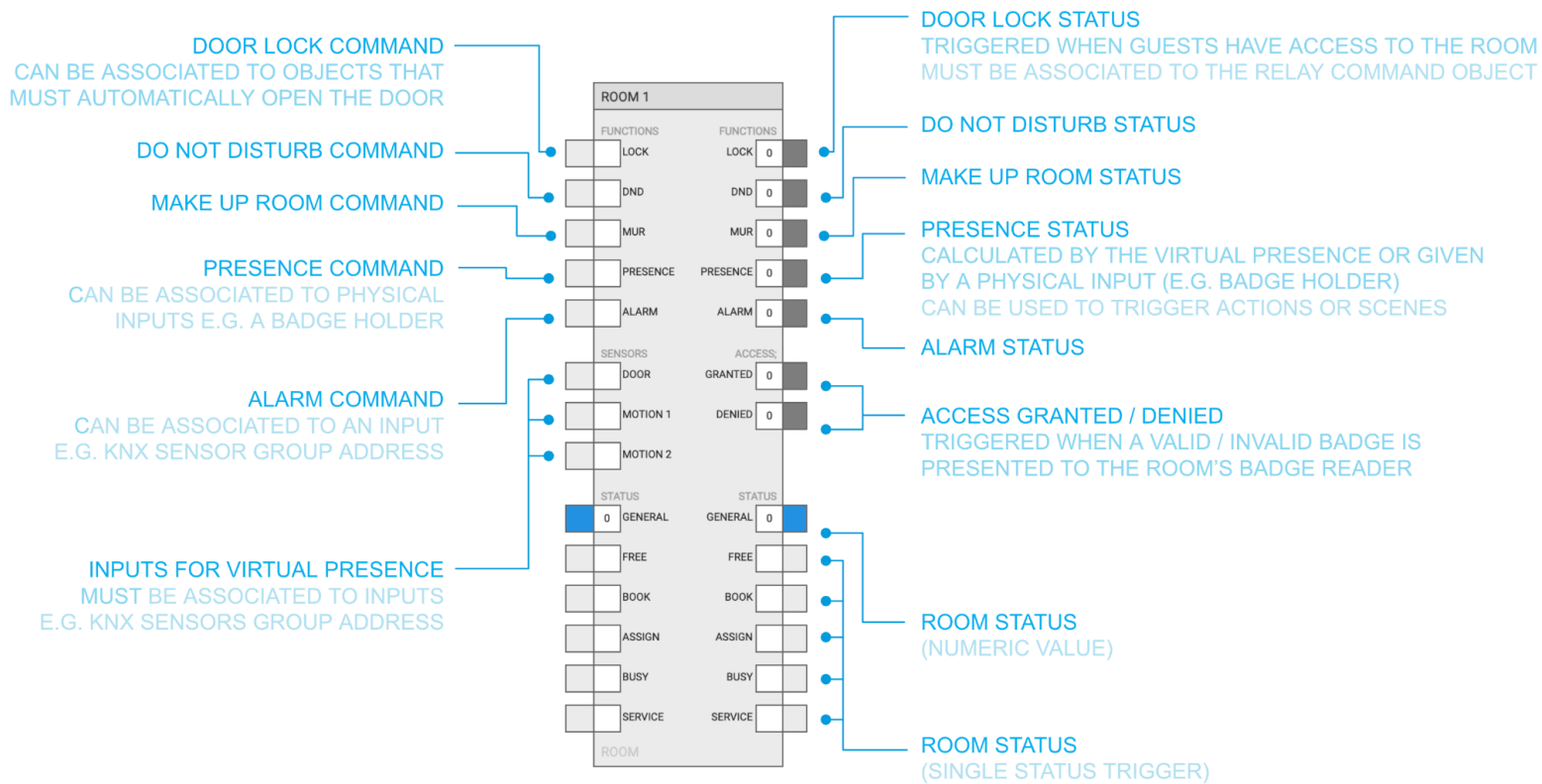
- With a CONNECTION
- With a TRIGGER
- With a LOGIC

In order to make the configuration of such relationships easier, the configuration page of a ROOM or a GATE ([section 4.2](#) and [section 4.3](#)) offer the possibility to edit an “implicit” CONNECTION. This editor is accessible by pressing the CONNECTIONS button.

8.2 Room connections

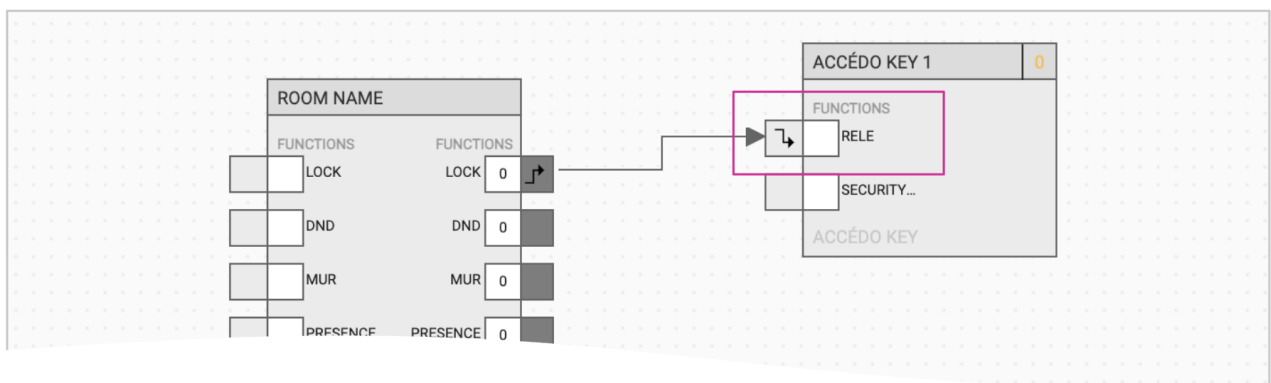
The block representing the ROOM in the connections editor offer the following nodes:

¹ For more general information about these automations, please refer to the AUTOMATIONS application manual of DELÉGO SERVER.



8.2.1 Door lock opening with DICO or ACCÉDO KEY

If a DICO or ACCÉDO KEY is associated to the room, as described in [section 5.5](#) and [section 6.5](#), its internal relay is automatically associated with a *relationship* to the DOOR property, as depicted in the following example:

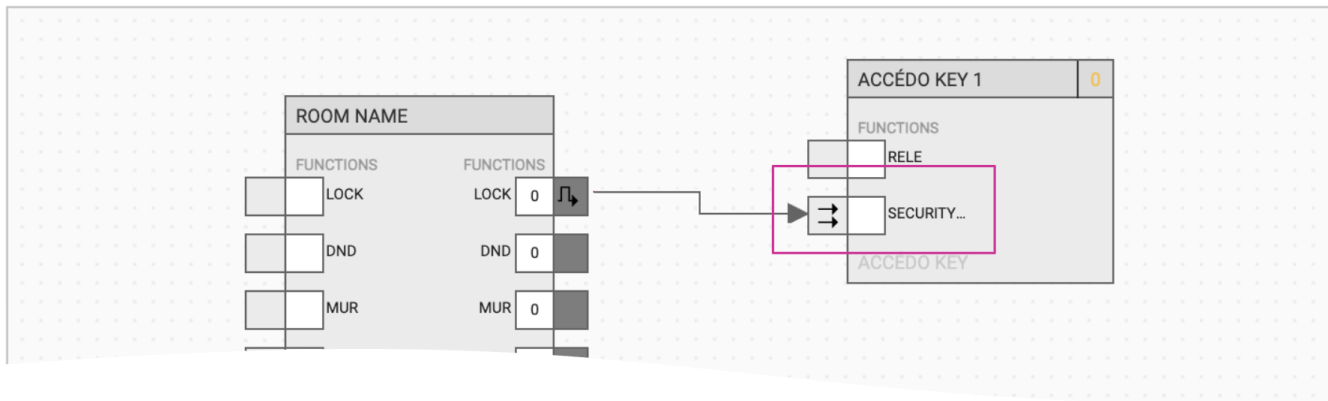


With this automatic relationship, when a Guest or a Service personnel accesses the room through that ACCÉDO KEY 1, the door is opened without the need of any other configuration.

In case the door is not physically connected to the internal relay of the access control device, it is required to change the *relationship*. An example is the use of a SECURITY RELAY connected to the ACCÉDO KEY or DICO: in this case, it is necessary to:

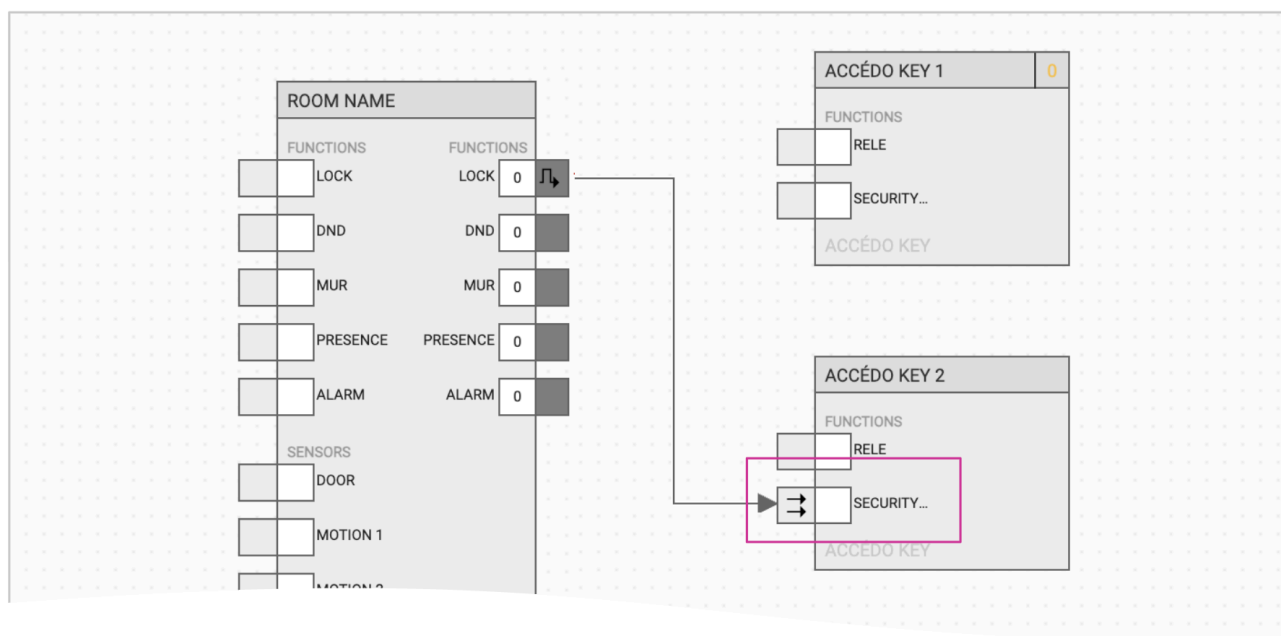
- Remove the predefined relationship by selecting the arrow and pressing CANC key
- Drag a new *arrow* starting from the DOOR output node (on the right side of the room block) into the SECURITY node

The result will appear as in the figure below:



If the door is opened by a relay connected to another DICO or ACCÉDO KEY device, it is necessary to:

- Drag the new device from the side menu into the CONNECTIONS editor
- Move it somewhere in the editor (because it is initially *overlapped* over the previous device)
- Remove the useless arrow(s)
- Eventually connect with an arrow the DOOR with the appropriate relay



8.2.2 Ekinex badge readers and holders (centralized authentication)

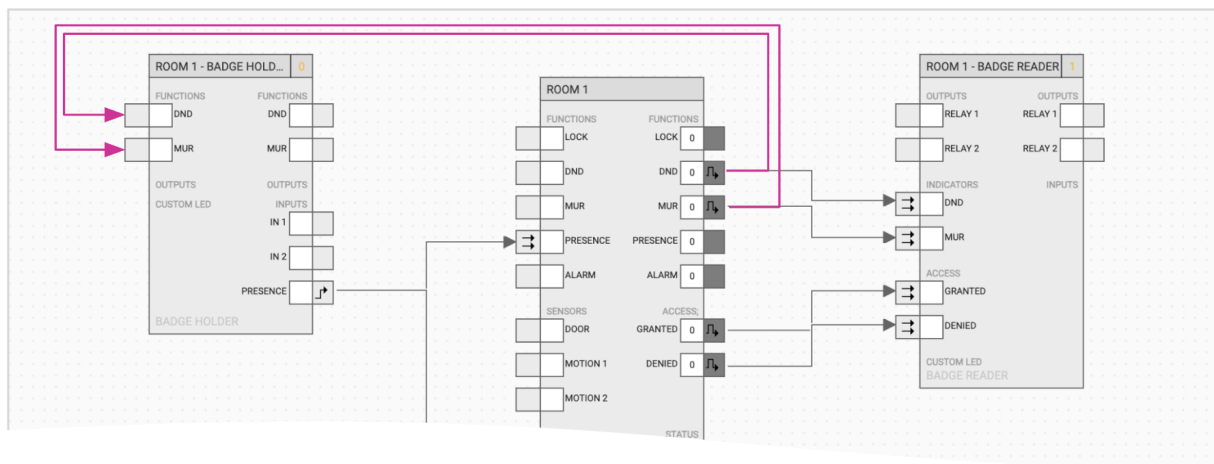
When an EKINEX KNX BADGE READER or HOLDER is assigned to a ROOM / GATE, and the CENTRALIZED AUTHENTICATION is active, the following connections are automatically created, in order to obtain bi-directional automations:



Revision 2.8.0 - Update: 15/04/2026
© Ekinex S.p.A. - All rights reserved

Note: the GRANTED and DENIED elements could be missing in the reader, if the corresponding KNX group addresses are not set

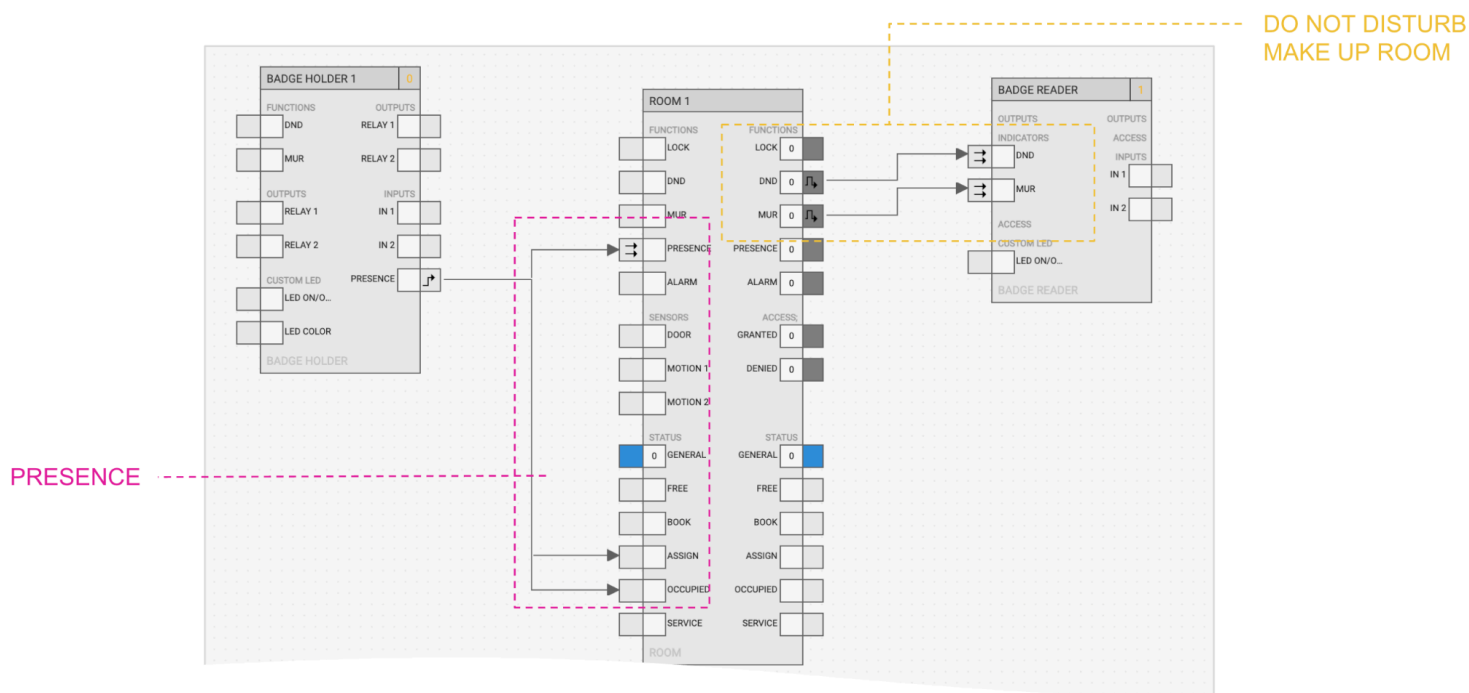
The following additional connections are suggested to be (manually) made, in order to switch the HOLDER's green and red LEDs respectively to the MAKE UP ROOM and DO NOT DISTURB:



Furthermore, in case of specific needs, the LOCK attribute of the ROOM / GATE can be directly connected to one of the specific physical RELAYs (1 or 2) of the READER / HOLDER.

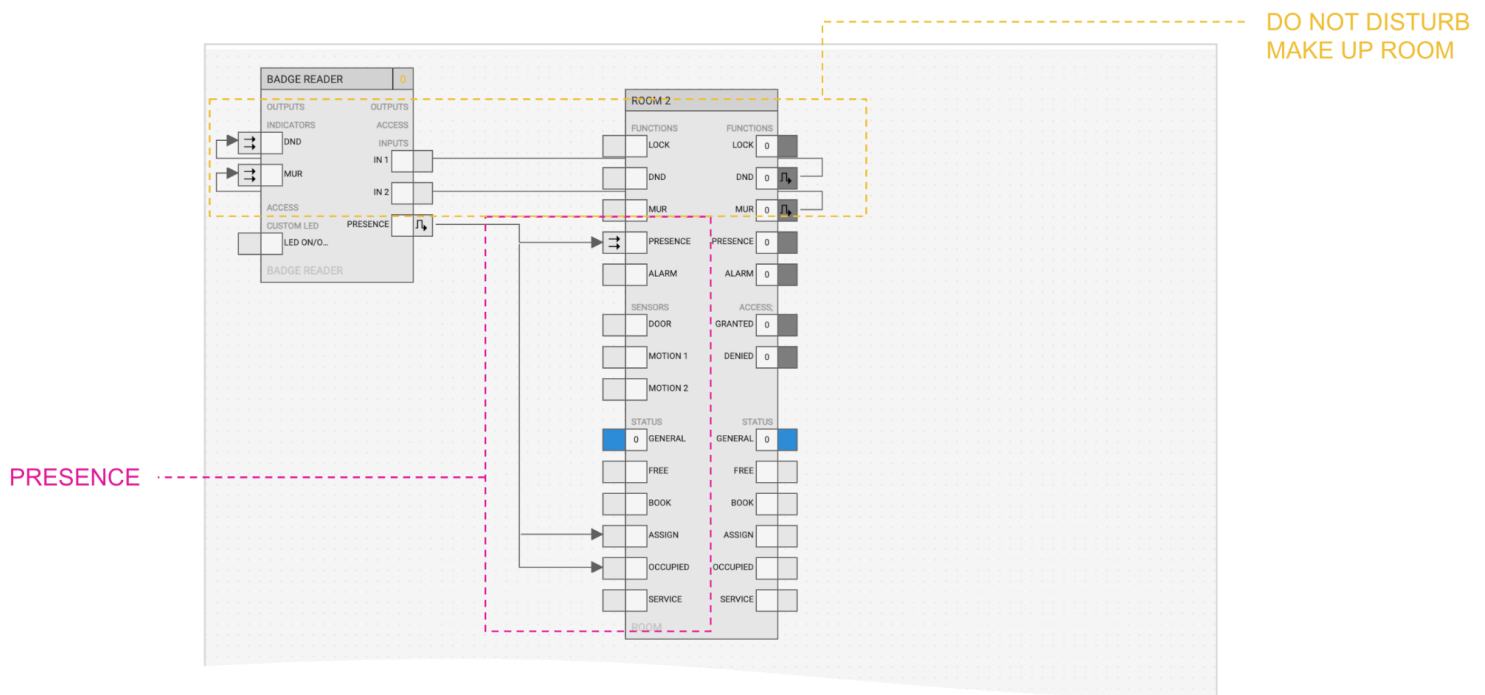
8.2.3 Ekinex badge readers and holders (decentralized authentication)

When an EKINEX KNX BADGE READER or HOLDER is assigned to a ROOM / GATE, and the CENTRALIZED AUTHENTICATION is not active, the following connections are automatically created:



In this case it is no longer sent a command by DELÉGO SERVER on the ACCESS GRANTED and DENIED (as in the centralized authentication) being the access granted internally by the reader for the badges in the WHITELIST.

In the eventuality of a reader with the active virtual presence, an holder is typically not installed (being surrogate by the virtual presence algorithm), and the following connections are automatically created (with the reader placed on the left of the room):



8.2.4 Door lock opening with a KNX actuator

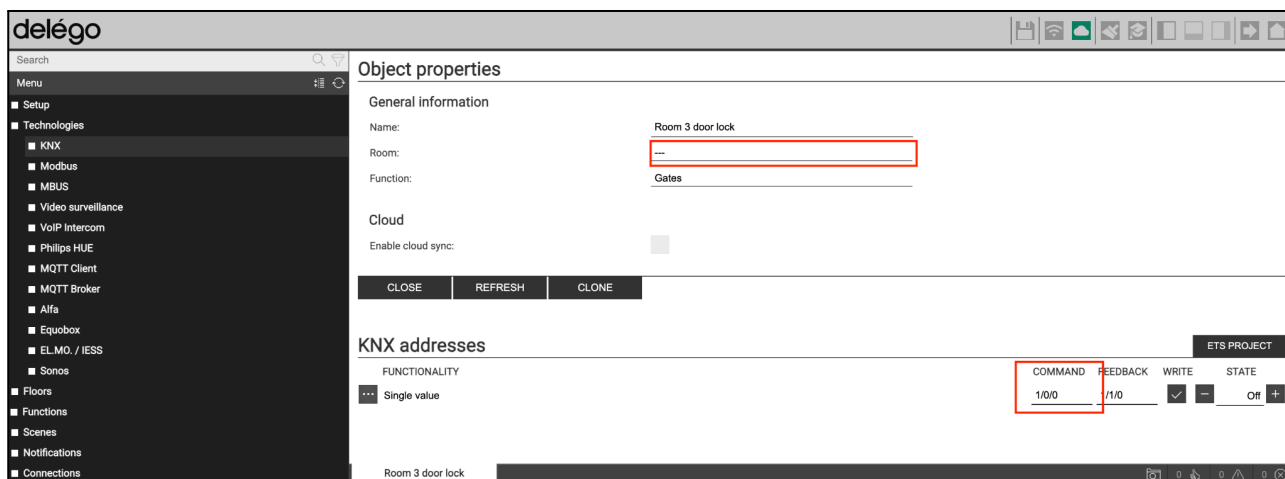
In case the door or gate is opened by a KNX actuator, the procedure to create a relationship in the CONNECTIONS is the following:

- On the DELÉGO SERVER menu navigate to the section

TECHNOLOGIES > KNX > KNX WIDGETS > OTHER

and add a new SINGLE VALUE widget by pressing the ADD button.

- Give a significant name to the WIDGET (e.g. "ROOM X DOOR LOCK").
- Enter its details page and insert the KNX group address in the COMMAND field (or drag&drop the appropriate address from the ETS PROJECT tree menu on the right panel). Leave the Room field blank.



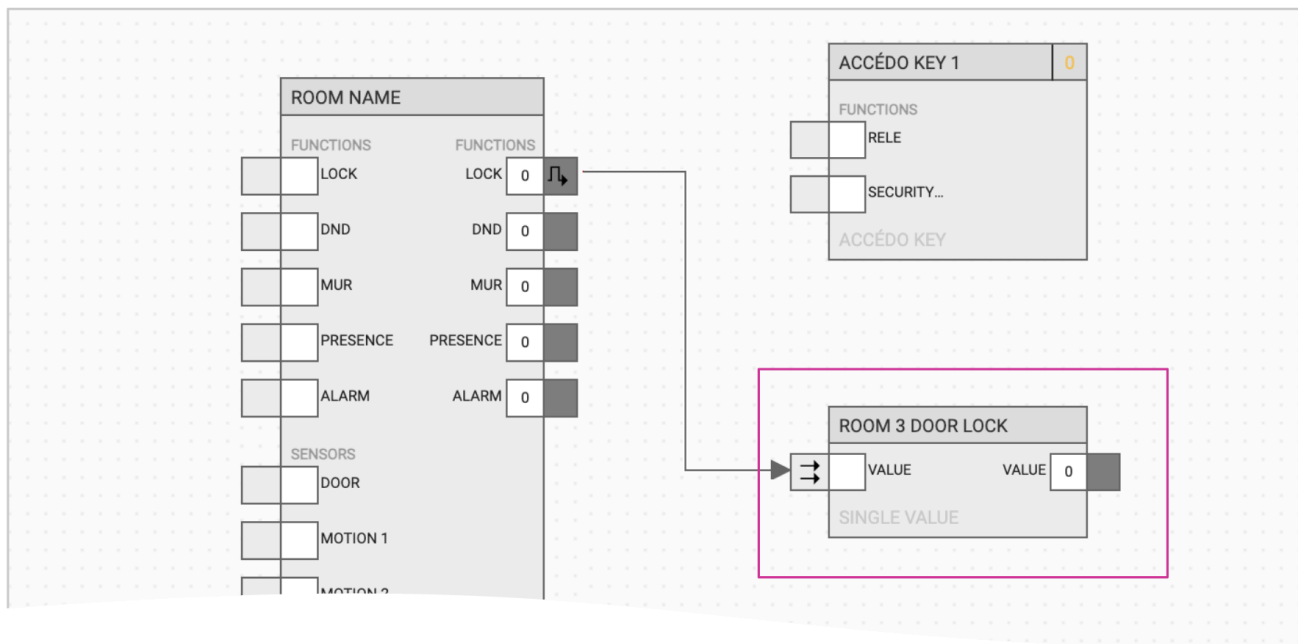
- Open the CONNECTION editor of the Room and search the widget created in the previous steps using the SEARCH engine or the FILTER typing the name of the widget; as an alternative you can search the KNX OBJECT by typing the KNX group address.
- Drag&Drop the WIDGET / KNX OBJECT into the CONNECTION editor.
- Connect with an arrow the LOCK output node of the ROOM into the input node of the KNX widget.



In the KNX WIDGET(s) that are created only for an automation, like in the example, are not required to be added to a ROOM (in the FLOORS → ROOM structure) because they do not need to be commanded directly from the app.

Also the assignment to a FUNCTION is optional.

The following picture shows an example of a CONNECTION between a Room and a KNX WIDGET:

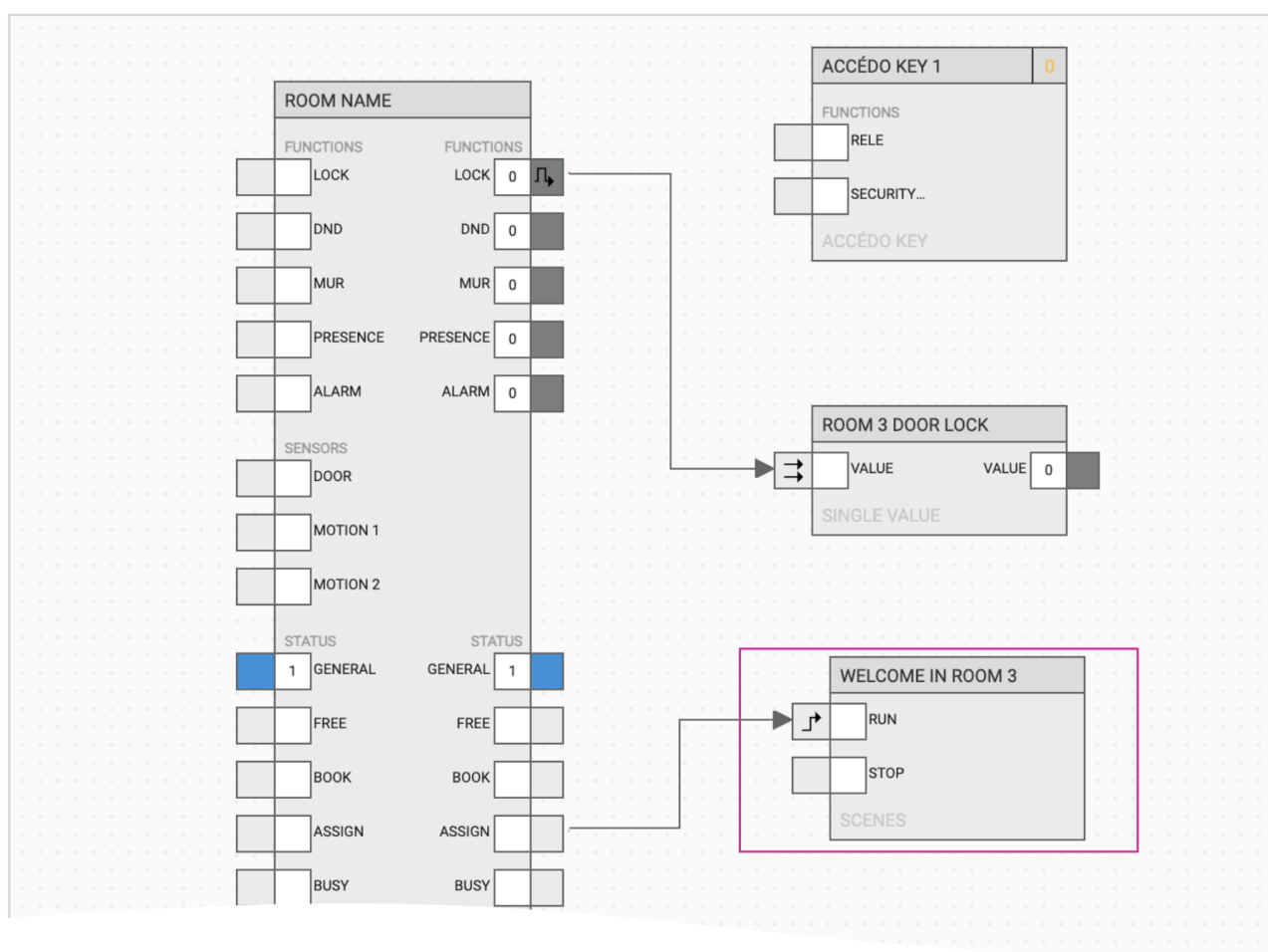


8.2.5 Connection example: Welcome scene at room status change

Another useful automation can be the execution of a “welcome scenario” when a room is assigned to a guest, i.e., the validity period of the guest is starting and the guest will arrive soon in the structure.

The procedure to create this type of automation is the following:

- In the DELÉGO SERVER menu, navigate to the SCENES section and create a new Scenario.
- Drag&Drop all the needed actions in the ACTIONS section (e.g., start the heating / cooling, set shadings / lights to a certain status etc...) in the way explained in the GENERAL FUNCTIONS application manual [D2].
- Drag&Drop the scene into the CONNECTIONS editor.
- Drag an arrow from the ASSIGNED output node of the Room and connect it to the RUN input node of the scene, like in the following example.



8.3 Gates connections

The management of connections between a DICO or ACCÉDO KEY and a GATE is similar to the one described for the ROOMS. The difference is that the GATE has only the DOOR as a node.

9 Permissions

9.1 User groups

User groups can be used to define access rules for multiple guests and/or staff with similar needs.

The system offers two predefined user groups:

SERVICE	Staff personnel
GUESTS	Visitors of the structure

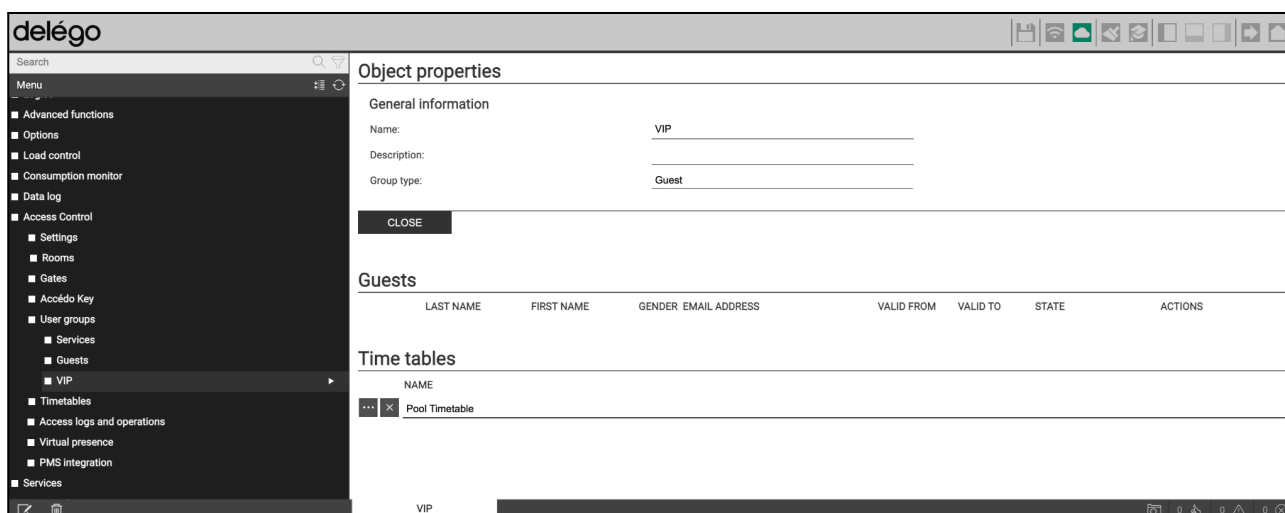
Additional user group(s) can be created, by navigating in the the DELÉGO SERVER menu

ACCESS CONTROL > USER GROUPS

and pressing the [+] button in the toolbar. The following information are requested in the GENERAL INFORMATION:

NAME	Label associated to the user group (e.g., VIP, Cleaning, etc)
DESCRIPTION	Optional additional description
GROUP TYPE	The typology of users that can be associated to the group: • Guests • Service • Both
GROUP LEVEL	The badge level associated to the group. Can be one of the following: • Guest • Service • Maintenance • Security • Administrator This selection has a practical impact only on the Ekinex KNX badge readers and holders in WHITELIST mode; in that case, this selection determines the <i>badge level</i> written in the WHITELIST. Different <i>badge levels</i> can be enabled or not (statically with parameters or dynamically with group objects) and can trigger different welcome / goodbye actions, as specified in the ETS library.
GROUP COLOR	The color to be used in the BOOKINGS view to indicate a reservation for an user belonging to this group

Example of configuration for a user group:



9.2 Timetables

Timetables are used to restrict the access for one or more ROOM(s) / GATE(s) on specific days of the week and time ranges.

9.2.1 Create a new timetable

In order to create a new timetable, navigate to

ACCESS CONTROL > TIMETABLES

In the menu of the DELÉGO SERVER menu, and press the [+] button in the toolbar.

The following information is requested in the GENERAL INFORMATION:

NAME	Label associated to the timetable
DESCRIPTION	Optional additional description
ENABLED	Determines if the timetable can be used or not

9.2.2 Timeslots

A timetable grants the access in one or more timeslot(s); in the TIMESLOT section press the ADD button to add a new timeslot. The following information is required to define a timeslot:

NAME	Label identifying the timeslot
START DAY	Initial weekday of validity for the timeslot
END DAY	Final weekday of validity for the timeslot
VALID FROM	Start and end time of validity for the timeslot.

VALID TO	In case of HOURLY granularity (default) it must be selected from a drop-down menu (from 00:00 to 24:00 meaning the start and end of the day). In case of MINUTES granularity, an hour + minutes can be set.
ENABLE	Determines if the timeslot is active or not

9.2.3 Restrictions

A timetable applies to one or more ROOM / GATE(s) when users belonging to one or more USER GROUP(s) attempt the access.

Drag&Drop the corresponding room or gate into the ROOMS / GATES LINKED section, and the user groups affected by the timetable in the USER GROUP list.

The following figure shows an example of a configured timetable:

The screenshot displays the 'delégo' application interface. On the left is a dark sidebar menu with various system settings categories. The main area is titled 'Object properties' and shows the configuration for a 'Pool Timetable'. Below this, there are three sections: 'Timeslots', 'Rooms / Gates', and 'User Group'. The 'Timeslots' section contains a table with two entries: 'Morning' and 'Afternoon'. The 'Rooms / Gates' section shows 'Pool Entrance' as a linked room. The 'User Group' section shows 'VIP' as a linked user group.

NAME	START DAY	END DAY	VALID FROM	VALID TO	ENABLE
Morning	Monday	Friday	08:30	12:30	☒
Afternoon	Monday	Friday	14:30	19:30	☒

NAME	ENABLE
Pool Entrance	☒

NAME
VIP

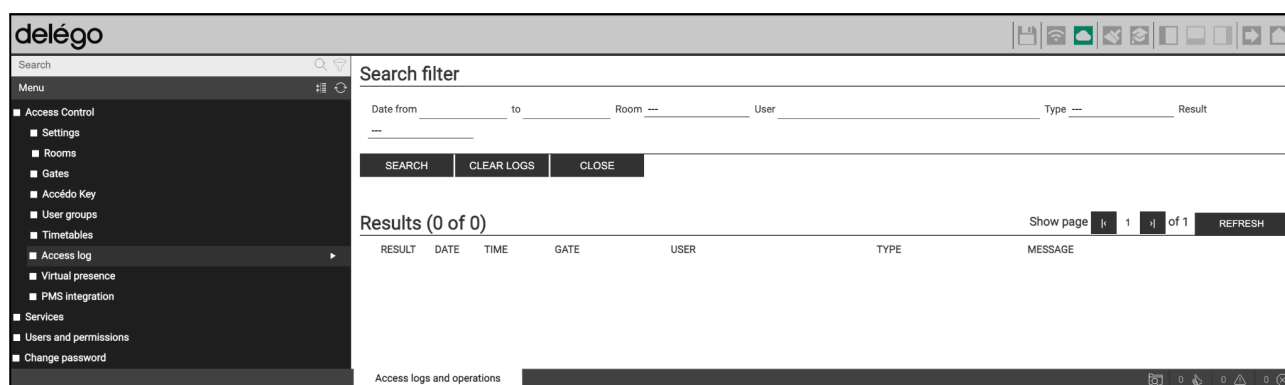
10 Access log

By entering the DELEGO SERVER menu section

ACCESS CONTROL > ACCESS LOG

It is possible to consult the log of the activities related with the access control devices. It is possible to filter the results by entering one or more than one of the following filters:

DATE FROM	Initial date for the search in the log
DATE TO	Final date for the search in the log
ROOM	A specific room to restrict the log to
USER	User to restrict the log to
TYPE	A specific access method (PIN, QR Code, RFID Card)
RESULT	The result of the access to a Room or Gate (ok or error)



In case of Ekinex KNX badge readers with decentralized (WHITELIST) authentication, the message in case of invalid access give also the information about the reason why the badge was not allowed:

INVALID BADGE	The badge is not associated with the reader / room
INVALID TIME / WEEKDAY	The badge is associated to the reader / room but the transit is outside the allowed time slot(s)
INVALID LEVEL	The badge belongs to a user associated with a USER GROUP of a LEVEL which is not allowed for the reader
ACCESS LIMIT EXCEEDED	The badge is valid but the allowed number of transits has been reached

11 Virtual presence

11.1 Introduction

DELÉGO SERVER can determine the presence of one or more guest(s) in a ROOM by evaluating the state of motion sensors by means of an algorithm called "VIRTUAL PRESENCE".

If at least one ROOM needs this feature, the algorithm must be started; it is possible to enable the VIRTUAL PRESENCE for each ROOM that requires it; it is not necessary to activate it on all of the rooms.

In order for the algorithm to work it is needed to configure a connection between the ROOM(s) and the corresponding presence sensor(s), as explained in the next paragraphs.



The VIRTUAL PRESENCE is supported only by the new 4-DIN module hardware version of DELÉGO SERVER.



The Ekinex KNX BADGE READER (EK-TO2-TP) starting from version 2.0 (ETS library 0.2 or higher) offers an integrated virtual presence algorithm directly in the device.

In such a case it is recommended to use it being more distributed instead of a central management, for performance and reliability reasons.

11.2 Activation and parametrization

Navigate in the DELÉGO SERVER administration menu to the following section

ACCESS CONTROL > VIRTUAL PRESENCE

and flag the "EXECUTE AT STARTUP" checkbox, in order to start the algorithm. Activating the EXPERT mode () the following parameters can be set to adjust the algorithm:

PARAMETER	DESCRIPTION	DEFAULT
TIMEOUT BADGE EVENT [ms]	Time in milliseconds to wait for RFID Card before next scan.	20000
TIMEOUT OPEN/CLOSE DOOR EVENT [ms]	Waiting time in milliseconds for an opening/closing door event after RFID Card scanning. If this event does not occur after the timeout, the VIRTUAL PRESENCE algorithm returns to the state of waiting for an RFID Card scan event.	20000
TIMEOUT PRESENCE EVENT [ms]	Waiting time in milliseconds for a presence sensor event after an opening/closing door event. If the sensor does not register a movement event after timeout, the VIRTUAL PRESENCE	20000

	algorithm returns to the state of waiting for an RFID Card scan event.	
TIMEOUT RESET SENSOR [ms]	Time in milliseconds to stop and reset the presence detection of the algorithm after the VIRTUAL PRESENCE already detected a first presence in the room. Use the value of the sensor parameter. If the sensor does not register a room exit event, the VIRTUAL PRESENCE algorithm returns to the state of waiting for an RFID Card scan event.	20000

When all the settings are performed, press the START button and check that the EXECUTION STATE changes from *Stop* to *Running*, and proceed with the next steps of the configuration as explained in the following sections.

11.3 Room configuration

In the details page of a ROOM ([section 4.2](#)), select the ENABLE VIRTUAL PRESENCE checkbox to enable the algorithm for that room; a pop-up message will inform that the algorithm is activated.

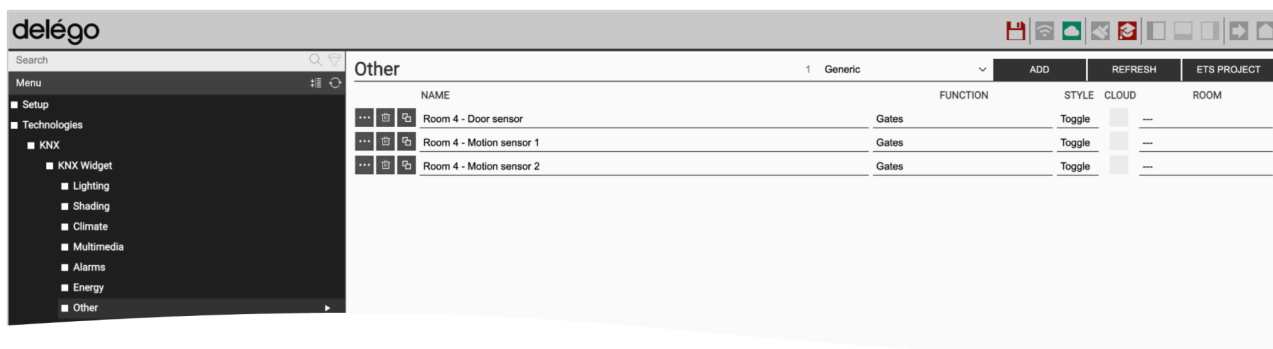
The VIRTUAL PRESENCE algorithm determines the presence of a guest in the ROOM with the elaboration of the signals coming from a door sensor or motion sensors. The higher the number of connected sensors, the more accurate the algorithm is.

The connection between sensors and the algorithm is done by creating *relationships* with the corresponding PROPERTIES of the ROOM, in the CONNECTIONS view of the ROOM (as previously explained in [section 7](#)). In particular, the involved properties are listed in the following table:

PROPERTY	REQUIRED	DESCRIPTION / NOTES
LOCK	Yes	Status of the electric lock. This is <i>implicit</i> in the command for the door opening.
DOOR SENSOR	Yes	Status of a sensor connected to the door, giving a value 1 (ON) when the door is OPENED and 0 (OFF) when CLOSED.
MOTION SENSOR 1	Yes	Status of a motion sensor installed in the room, giving a value 1 (ON) when a movement is detected, and 0 (OFF) after a certain time of no detection
MOTION SENSOR 2	No	Similar to the previous, for a second sensor if existing (e.g. motion sensor in the bathroom)

Usually the status of the sensors is made available using KNX group addresses. In such a case, the procedure is the following:

- Create a SINGLE VALUE KNX WIDGET (in TECHNOLOGIES > KNX > KNX WIDGET > OTHER) and enter in the details page of the widget insert the KNX group address.

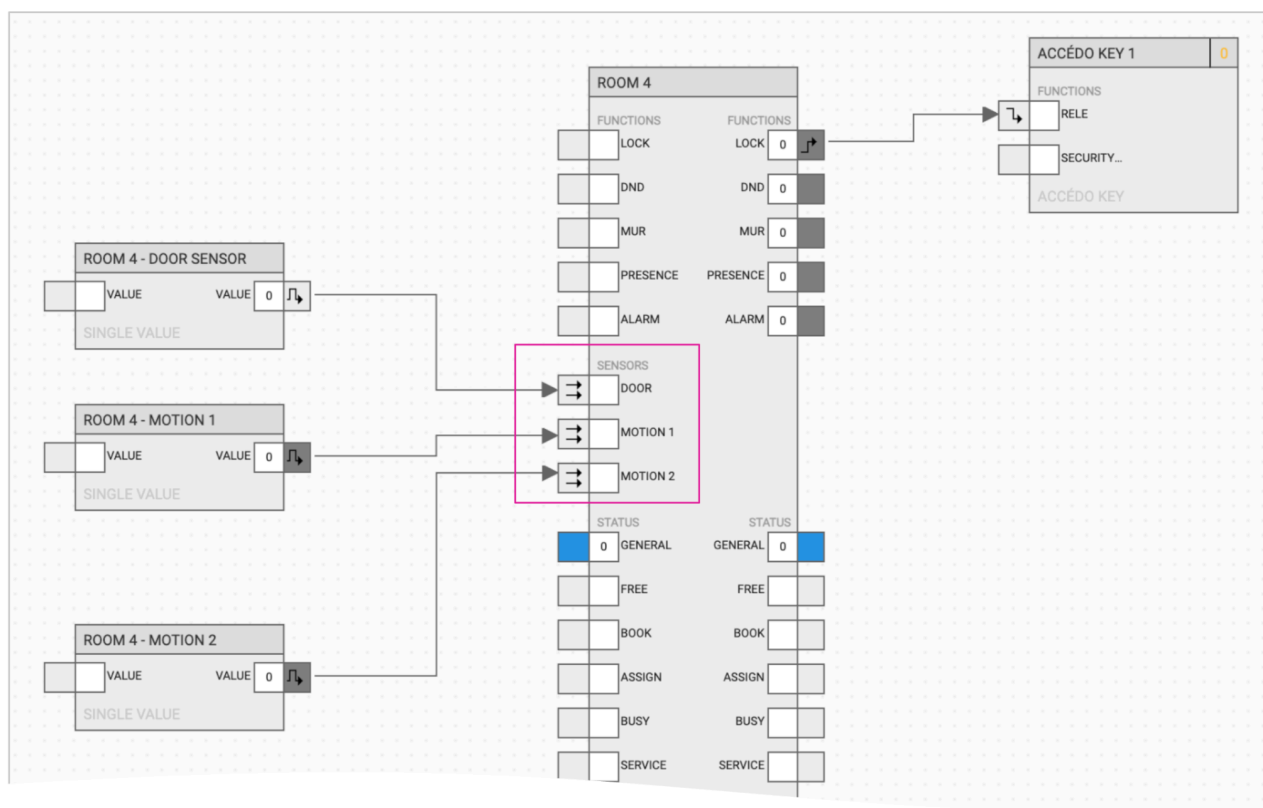


- Drag&Drop the KNX WIDGETS of the sensors into the CONNECTIONS editor of the room (like explained in [section 7.2.2](#) for a KNX lock).
- Draw an arrow (relationship) between the sensor and the corresponding sensor input node of the ROOM.



It is not necessary to draw a connection with the LOCK because it is *implicit*.

The following picture shows an example of relationships between a ROOM and the input motion sensors in the CONNECTIONS editor:

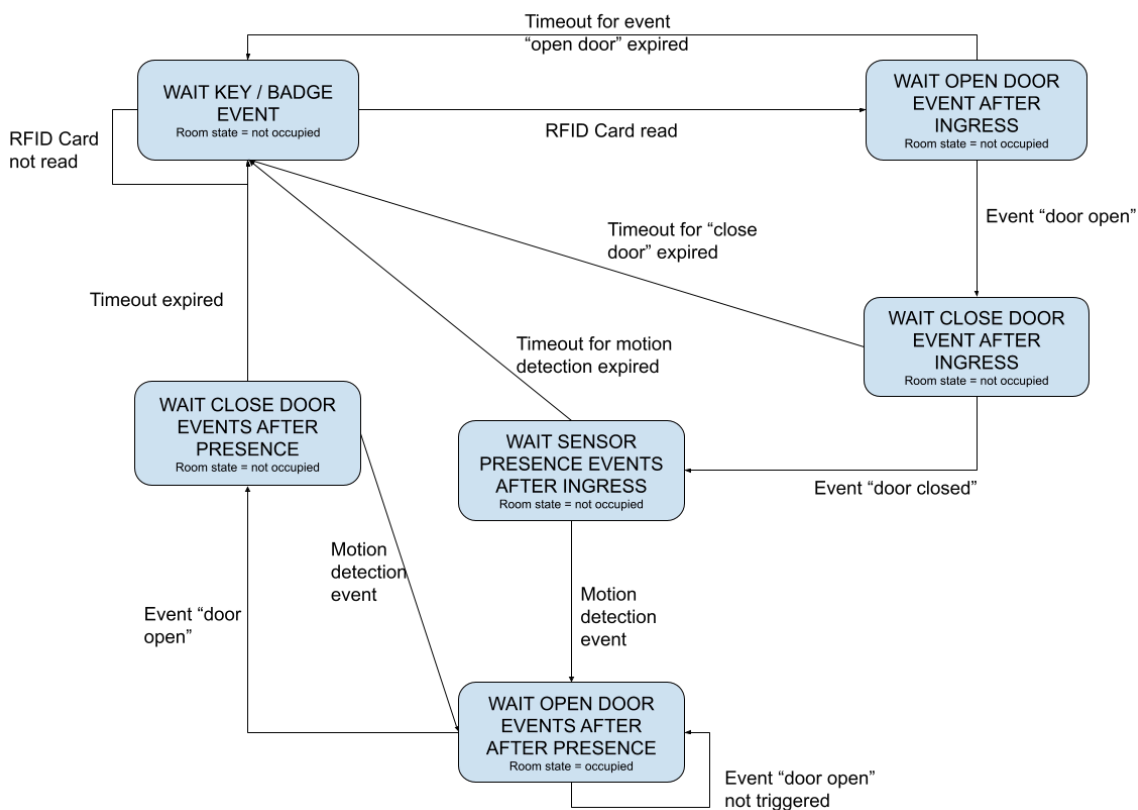


In the VIRTUAL PRESENCE section of the details page of the ROOM, it is possible to monitor in which condition is the algorithm, with the VIRTUAL PRESENCE STATUS indicator.

The possible states of the algorithm are:

WAIT KEY / BADGE EVENT	VIRTUAL PRESENCE algorithm is in a waiting state for a valid RFID Card reading.
WAIT OPEN DOOR EVENT AFTER INGRESS	When a valid RFID Card is read, the VIRTUAL PRESENCE goes in a waiting state for an "open door" event. If door is not opened until a timeout, the algorithm will return to the state WAIT KEY / BADGE EVENT and the room state will be "not occupied"
WAIT CLOSE DOOR EVENT AFTER INGRESS	If the door is open after a valid RFID Card is read, the VIRTUAL PRESENCE algorithm goes in a waiting state for a "close door" event. If the door is not closed until a timeout, the algorithm will return to the state WAIT KEY / BADGE EVENT and the room state will be "not occupied"
WAIT SENSOR PRESENCE EVENTS AFTER INGRESS	If in state WAIT CLOSE DOOR EVENT AFTER INGRESS the door is closed, the algorithm will wait for a movement detection from the motion sensor. If after a timeout the sensor does not reveal a movement in the room the algorithm will return to the state WAIT KEY / BADGE EVENT and the room state will be "not occupied", otherwise room will go in a "occupied" state.
WAIT OPEN DOOR EVENTS AFTER PRESENCE	If in state WAIT SENSOR PRESENCE EVENTS AFTER INGRESS the algorithm detects by means of a motion sensor the guest presence in the room, the room state will be in an "occupied" state and the VIRTUAL PRESENCE stays in a "idle" state until an "open door" event occurs.
WAIT CLOSE DOOR EVENTS AFTER PRESENCE	If, while the algorithm is in state WAIT OPEN DOOR EVENTS AFTER PRESENCE, an "open door" event is detected, the algorithm will go in a waiting state for a "door close" event. If the door is not closed after a timeout, the algorithm goes in a waiting state for a motion sensor detection event in the room. If in this state the algorithm does not receive any motion detection after a timeout, the room goes in a "not occupied" state and the VIRTUAL PRESENCE will go back to WAIT KEY / BADGE EVENT.

The following picture represents the State Machine of the algorithm:



12 Guest room management utilization

12.1 Introduction

In the Visualization view of the DELÉGO SERVER Web Page, by entering the ACCESS CONTROL section in the navigation menu, it will be displayed the following screen (on PC/MAC or Smartphone):



All the options will give access to all the useful sections needed for the management of guests, rooms, etc. Some of the options could be missing according to the configuration done by the installer / system integrator (in particular according to the settings applied in [section 3.3](#)).

12.2 Guests

In this area it is possible to create or edit the guests of the structure, and manage all the related permissions; this is the core section of the access control management console.

12.2.1 Guests list

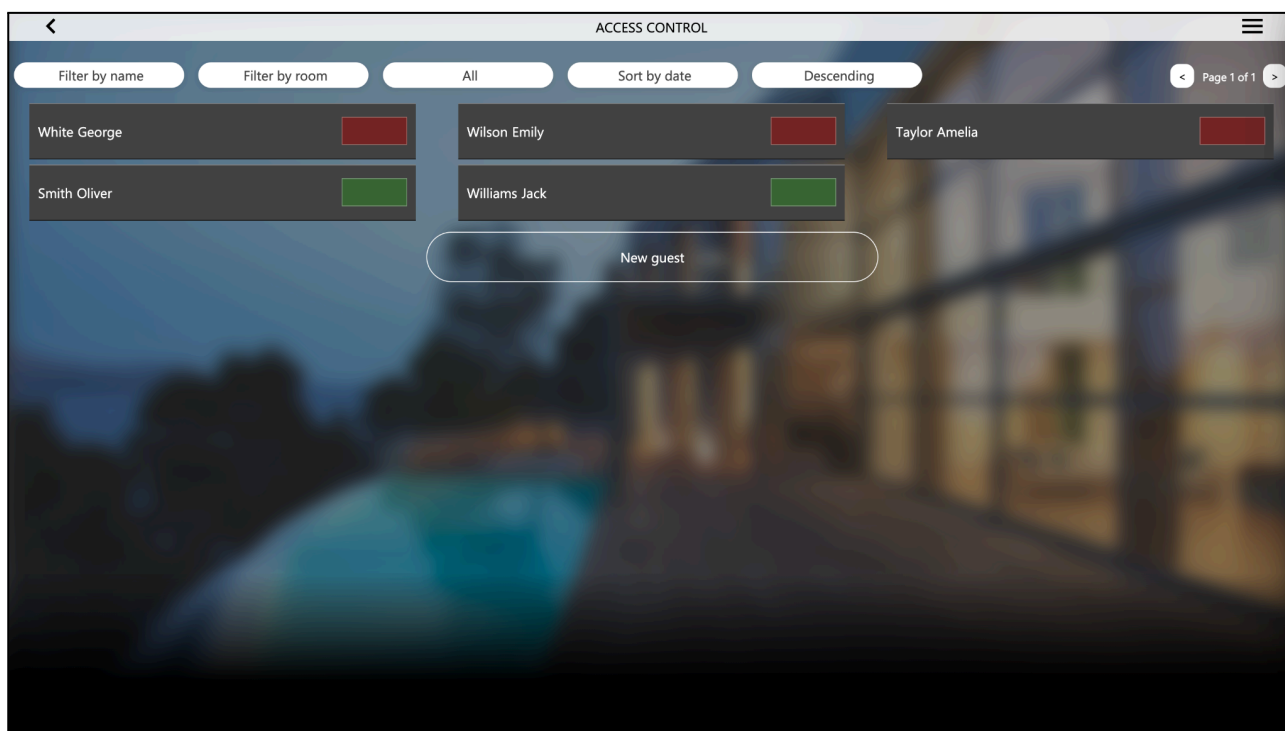
By entering the section, it is displayed a list of the available guests (if any), with the possibility to filter the list by one or more among the following criteria:

FILTER BY NAME	In this form it is possible to enter one or more keyword(s) (name and surname) to be searched.
----------------	--

FILTER BY ROOM	In this form it is possible to enter the room number assigned to the searched guest.
STATUS	Drop down menu that allows to select one of the possible status of a guest: • Enabled • Disabled • All

The filter results can be sorted with the following criteria (both criteria are drop down menus):

SORT BY	One of the following fields: • Date • Name
SORT ORDER	Ascending or descending



12.2.2 Adding a new guest

By pressing the NEW GUEST button it is displayed a pop-up menu, where all the information about the new guest can be entered. There are three main windows to be populated with the Guest information:

REGISTRY

FIRST NAME	Name of the guest
LAST NAME	Surname of the guest
GROUP	Select the User Group (section 8.1) to which the guest must belong.

	The user group determines the permissions and possible timeslots limitation of the access through certain Rooms or Gates.
EMAIL ADDRESS	Enter a valid e-mail address of the Guest.
PHONE NUMBER	Enter the phone number of the guest, without spaces or punctuation.
GENDER	Select the appropriate option between M (male) or F (female)

AUTHORIZATIONS

ACTIVE FROM NOW	This field can be: • Yes (valid from the current date and time. Only an end date must be set) • No (it must be set a starting date and an end day for the permanence validity of the guest)
VALID FROM	Enter the date / time for the start of the validity period. The guest will be entitled to enter the structure only from this starting period.
VALID TO	Enter the date / time for the end of the validity period. The guest will be no more entitled to enter the structure from that day.
RFID CARD INFO	Visible only if the option ENABLE BADGE MANAGEMENT described in section 3.1.3 is flagged. Allows the structure manager to assign to a Guest an RFID Card or to scan an RFID Card for the Guest

ACCESS

ROOM	A drop down menu that allows the user to select and assign one of the available Rooms to a guest. A guest can also not be associated with any room.
GATES	List of all available Gates for which a guest can access. A guest can also not be associated with any Gate.
REMAINING	If the ENABLE LIMIT ON NUMBER OF ACCESSES (section 3.1.3) is flagged, it is possible to enter, for each room or gate, a limited number of times for the guest to enter that Room or Gate(s).

The image displays three sequential screenshots of the 'NEW GUEST' form, illustrating the data entry process. Blue dashed lines and labels identify key sections:

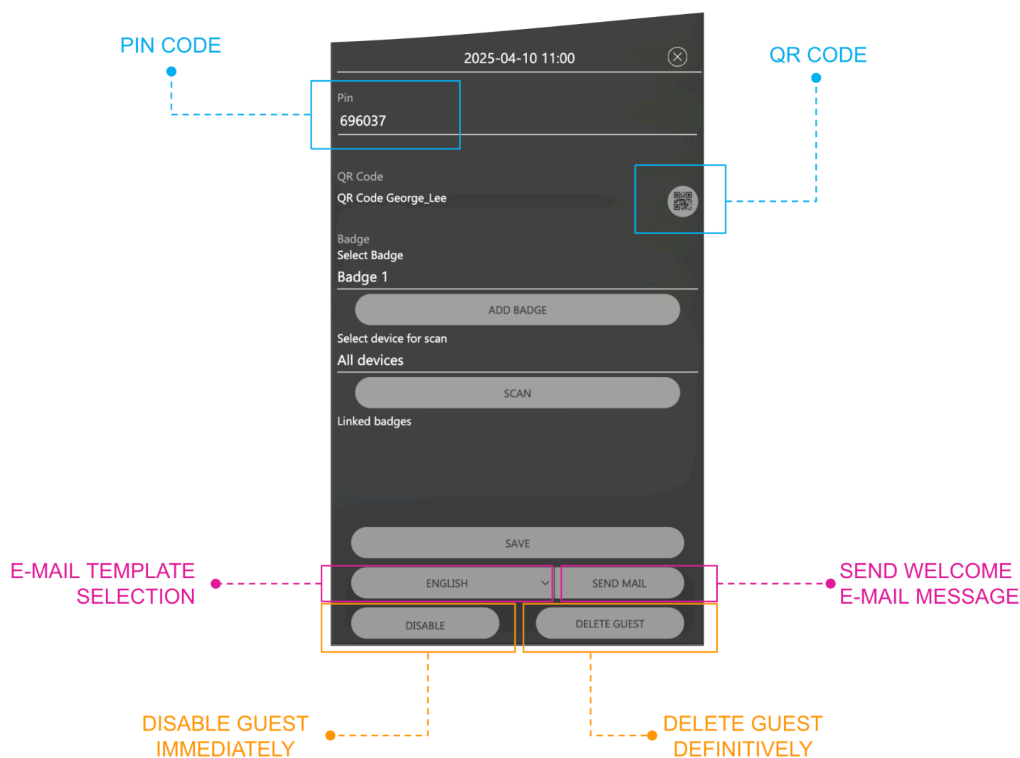
- PERSONAL DATA:** Points to the first screenshot, which includes fields for First name (George), Last name (Lee), Group (Guests), Email address (george.lee@example.com), Phone number (+44 1234567890), and Gender (M/F).
- VALIDITY PERIOD:** Points to the second screenshot, which includes fields for Active from now (No, select days), Valid from (2025-04-09 14:00), Valid to (2025-04-10 11:00), Badge selection (Badge 1), and a SCAN button.
- ROOM SELECTION:** Points to the third screenshot, which includes a Room selection field (Room 4) and a Remaining count (10).
- GATES AUTHORIZATION:** Points to the third screenshot, which includes a Gates section with checkboxes for Gate 1, Gate 2, and Gate 3.
- LIMIT ON NUMBER OF ACCESSSES:** Points to the third screenshot, which includes a Remaining count field (10).

Pressing the CREATE button, the new guest is added to the system, and eventually enabled (if the the dates selected in the Authorizations window are valid).



If a Guest is not assigned to any Room or Gate(s) and the structure manager creates the Guest, the system will display a pop-up message stating that the new Guest was created but he/she does not have access to any Room or Gate(s).

After the creation, in the AUTHORIZATION tab, a random (6-digits) PIN and a QR CODE (depending on the access method chosen for the structure during the configuration) are generated and assigned to the guest:



It is possible to change the PIN with a preferred sequence of 6 digits. Press the SAVE button after changing it, and eventually send the welcome e-mail.

After the creation of the Guest, in the pop-up the following elements will become visible:

E-MAIL TEMPLATE SELECTION	When more than one email template have been created (e.g., for multiple languages) it allows the selection of the desired one, before sending
SEND MAIL	Send the welcome e-mail message to the guest.
DISABLE	Allows to disable the guest immediately, even during the validity period.
DELETE GUEST	Removes definitively the guest from the system.



For the authorization with a RFID Card, refer to [section 12.8](#).

12.2.3 Welcome e-mail

When the SEND MAIL button is pressed, the DELÉGO SERVER will send a welcome e-mail to the guest starting from the chosen E-MAIL TEMPLATE SELECTION (created in the WELCOME MAIL menu described in [section 3.2](#)), replacing the *dynamic tags* with the information of the guest and the structure.

The e-mail will contain, the following information useful for the access (according to what was configured on the Administration web page and access method):

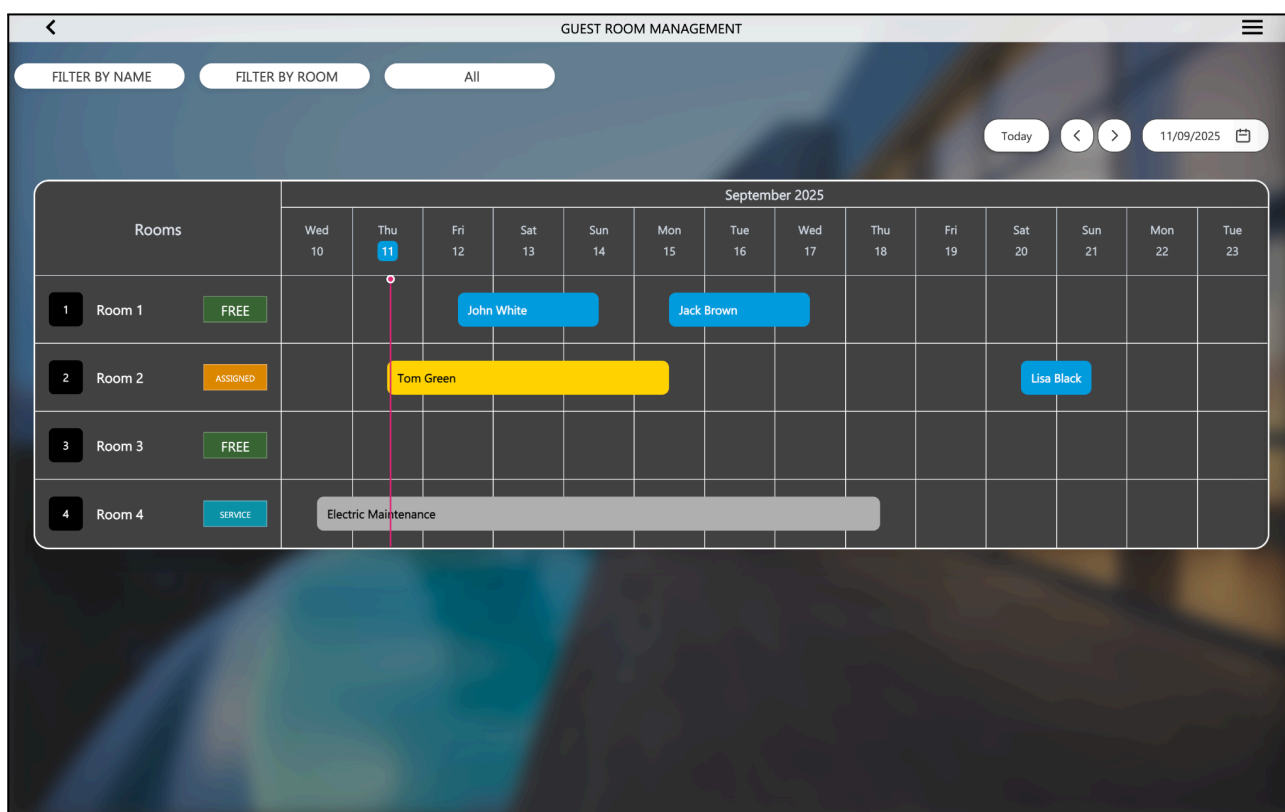
- The numeric PIN, that can be typed on the DICO or ACCÉDO KEY.
- The QR CODE, that can be scanned (from a printed paper or from the smartphone) in front of the camera of the DICO or ACCÉDO KEY.

NEW

12.3 Bookings

In this section of the guest room management it is possible to manage the reservations for the rooms with a calendar view, which gives an overview of the rooms occupancy and is a quicker way to create new guests.

The calendar always gives a view of the 2 weeks starting from the day before the actual; each row of the calendar is room:



It is possible to scroll week-by-week with the arrow buttons, or to select a specific date; the TODAY button brings back to the default view at any moment.

In order to create a new reservation for a guest, simply click on a "cell" (corresponding to a specific day for a given room) or drag & drop until the day when it must end; the same popup already presented in the previous paragraph, that creates a new guest, is displayed, already filled with the start / end dates and the room.

In a second moment, it is always possible to change the start and/or end date for a reservation, by "stretching" it with the handles appearing when the cursor is on the left / right side.

The colour of a reservation in the booking view represents the USER GROUP to which the guest (or the staff member) belongs. The default groups have respectively the blue (GUESTS) and gray (STAFF) colours, but they can be changed in the configuration area; new user groups are requested to have a different colour to identify them at a glance.

The elements in the top-left part of the view allow to filter the calendar by guest name, room number or user state; this can be useful especially in large structures.

12.4 Rooms

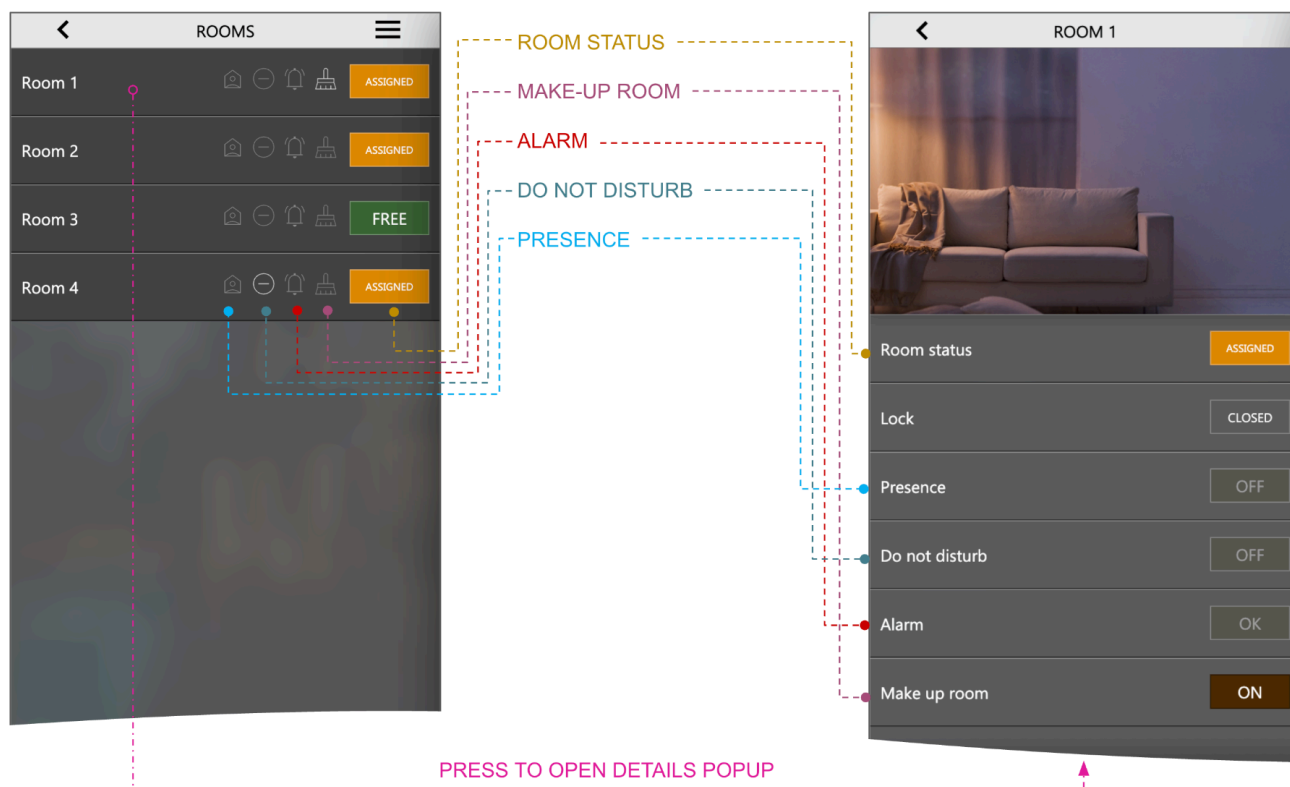
This section contains all the configured rooms in the Administration view of the DELÉGO SERVER ([section 4.2](#)). Each Room displays its name and, if enabled in the PROPERTIES section of the Room configuration, the pictograms related (Virtual presence, do not disturb, alarm, make up the room and room status).

Clicking on a room, the system will open a pop-up window that will detail all the pictograms:

ROOM STATUS	Can be one of the following:	
	FREE	Available for new guests
	BOOKED	Reserved for a guest who is still not in the validity period
	ASSIGNED	Reserved for a guest in the validity period (supposed to be in the structure)
	BUSY	The guest is inside the room
	SERVICE	Room to be cleaned or in maintenance
	N.D.	None of the previous
LOCK	The status of the electric lock. Normally closed (OFF).	
PRESENCE	Indicates the presence of the guest(s) in the room.	
DO NOT DISTURB	The request by the guest not to be disturbed by the staff.	
ALARM	The status of the internal alarm sensor (e.g. bathroom).	
MAKE-UP ROOM	The request by the guest to do an additional room cleaning.	

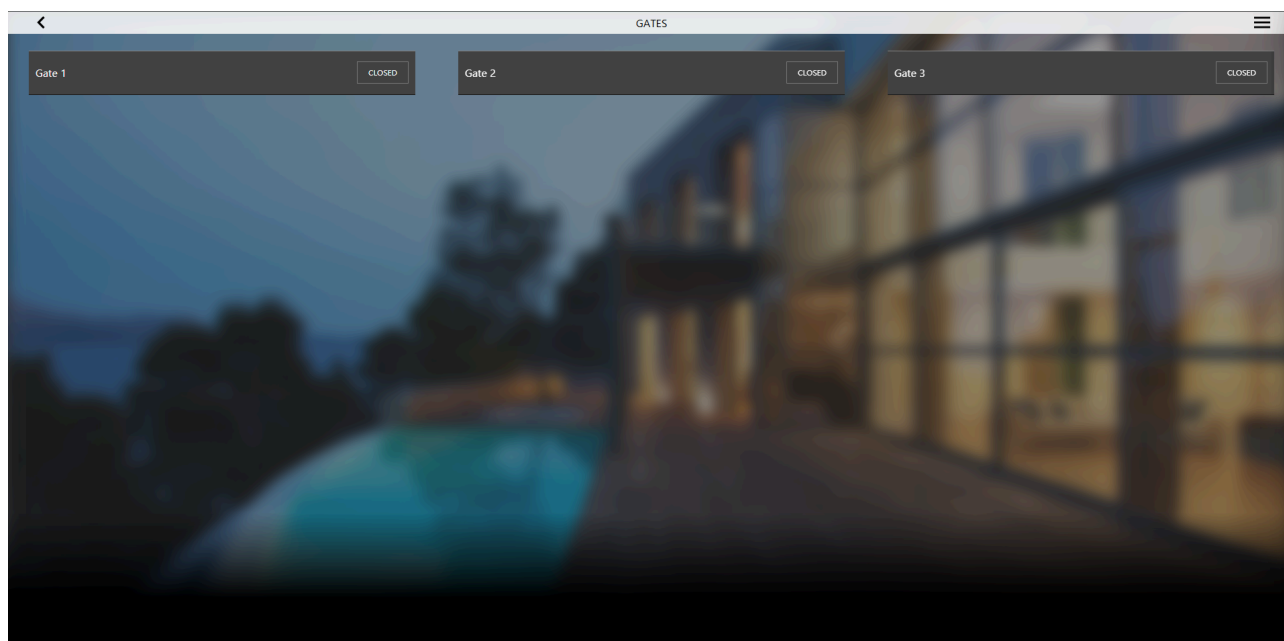
The following properties can be directly commanded by the details popup:

- LOCK (to open the door remotely).
- Do not disturb.
- Make-up room.



12.5 Gates

This section is similar to the ROOMS, but contains the GATES. In this case, the door can be directly opened by pressing the rectangular element in the list.



12.6 Access log

This section contains the history of all the accesses done to rooms or gates. It is the same log present in the Administration view (see [section 9](#)). It is possible to apply filters:

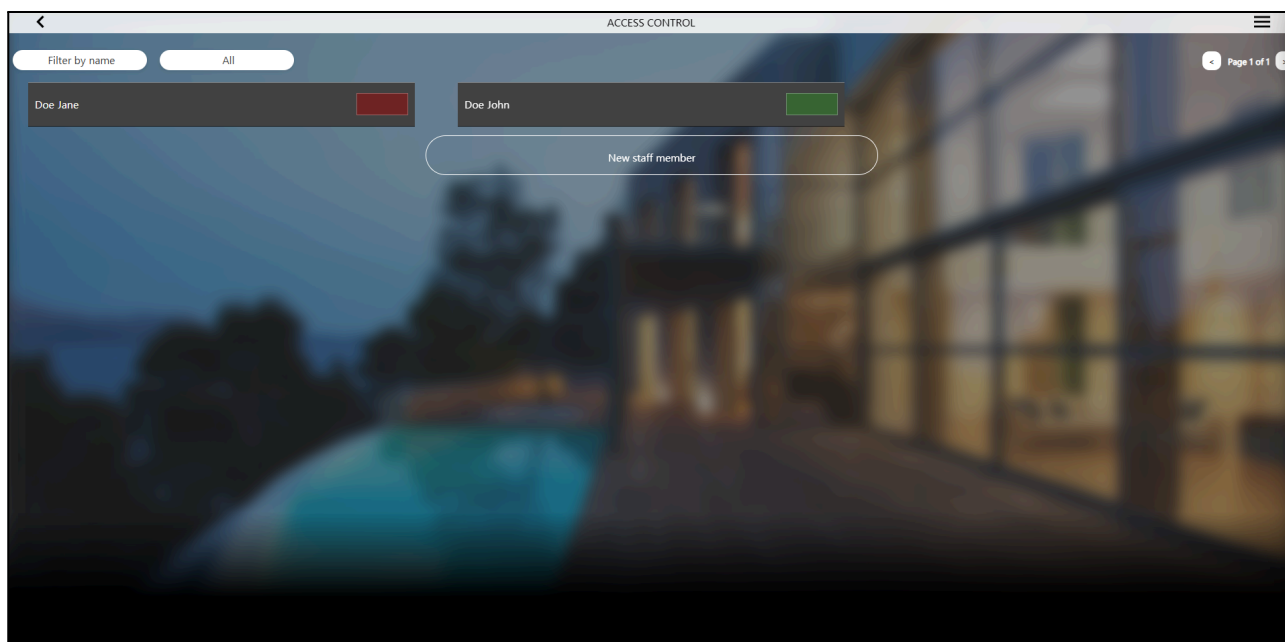
DATE FROM DATE TO	Range of dates
USERNAME	One or more keywords (name and surname) of the guest that must be searched
ACCESS POINT	Drop down menu that allows to select for which access point (Room, Gate, all) the log must be restricted
TYPE	The access method used for the access (or the attempt of transit). It can be QR Code, RFID Card or PIN.
RESULT	Permits to restrict the search to successfully or failed transits (ok or error)

The screenshot shows the 'ACCESS CONTROL' web interface. At the top, there are filter buttons: 'Date from' (with a clear icon), 'to' (with a clear icon), 'Username', 'All rooms', 'All types', and 'All results'. Below the filters, it says 'Results (20 of 166)'. On the right, there are icons for download, refresh, and navigation, along with 'Page 1 of 9'. The main table has the following columns: DATE, TIME, GATE, USER, TYPE, and MESSAGE. The table contains 20 rows of access logs, including successful logins for 'Williams Jack' and failed attempts for 'QR temp 2'.

DATE	TIME	GATE	USER	TYPE	MESSAGE
2025/4/9	16:22:12	Room 1	Williams Jack	Accédo Key Badge	The user Williams Jack has logged in to 'Room 1'
2025/4/9	16:22:08	Room 1	Williams Jack	Accédo Key Badge	The user Williams Jack has logged in to 'Room 1'
2025/4/9	16:22:04	Room 1	Williams Jack	Accédo Key Badge	The user Williams Jack has logged in to 'Room 1'
2025/4/9	16:22:00	Room 1	Williams Jack	Accédo Key Badge	The user Williams Jack has logged in to 'Room 1'
2025/4/9	16:21:48	Room 1	Williams Jack	Accédo Key Badge	The user Williams Jack has logged in to 'Room 1'
2025/4/9	16:21:41	Room 1	Williams Jack	Accédo Key Badge	The user Williams Jack has logged in to 'Room 1'
2025/4/9	15:51:57	Room 1	Williams Jack	Accédo Key Badge	The user Williams Jack has logged in to 'Room 1'
2025/4/9	15:51:52	Room 2	---	Accédo Key Badge	Invalid code
2025/4/9	15:51:52	Room 1	Williams Jack	Accédo Key Badge	The user Williams Jack has logged in to 'Room 1'
2025/4/9	15:51:48	Room 1	Williams Jack	Accédo Key Badge	The user Williams Jack has logged in to 'Room 1'
2025/4/9	15:50:00	Room 1	Williams Jack	Accédo Key Badge	The user Williams Jack has logged in to 'Room 1'
2025/4/9	15:49:56	Room 1	Williams Jack	Accédo Key Badge	The user Williams Jack has logged in to 'Room 1'
2025/4/9	15:49:52	Room 1	Williams Jack	Accédo Key Badge	The user Williams Jack has logged in to 'Room 1'
2025/4/4	15:04:21	Room 3	QR temp 2	Accédo Key QRCode	Invalid code
2025/4/4	15:04:19	Room 2	QR temp 2	Accédo Key QRCode	Invalid code
2025/4/4	15:04:18	Room 1	QR temp 2	Accédo Key QRCode	Invalid code
2025/4/4	15:04:13	Gate 1	QR temp 2	DICO QRCode	Invalid code
2025/4/4	15:04:08	Gate 1	QR temp 2	DICO QRCode	The user 'QR temp 2' has logged in to 'Gate 1'
2025/4/4	15:04:02	Gate 1	QR temp 2	Accédo Key QRCode	The user 'QR temp 2' has logged in to 'Gate 1'

12.7 Staff

This section is similar to the GUESTS area, but is dedicated to the creation of service personnel of the structure. The difference between staff members and guests, is that staff members can be associated with multiple rooms (in order to enter potentially in all of them).



12.8 Temporary QR code

This section allows the creation of QR CODE(s) not related to a specific guest or staff member and that can be used only for a limited period (e.g., maintenance people need to access one or more rooms of the structure).

The following information can be set in the popup that appears when the button CREATE QR CODE is selected:

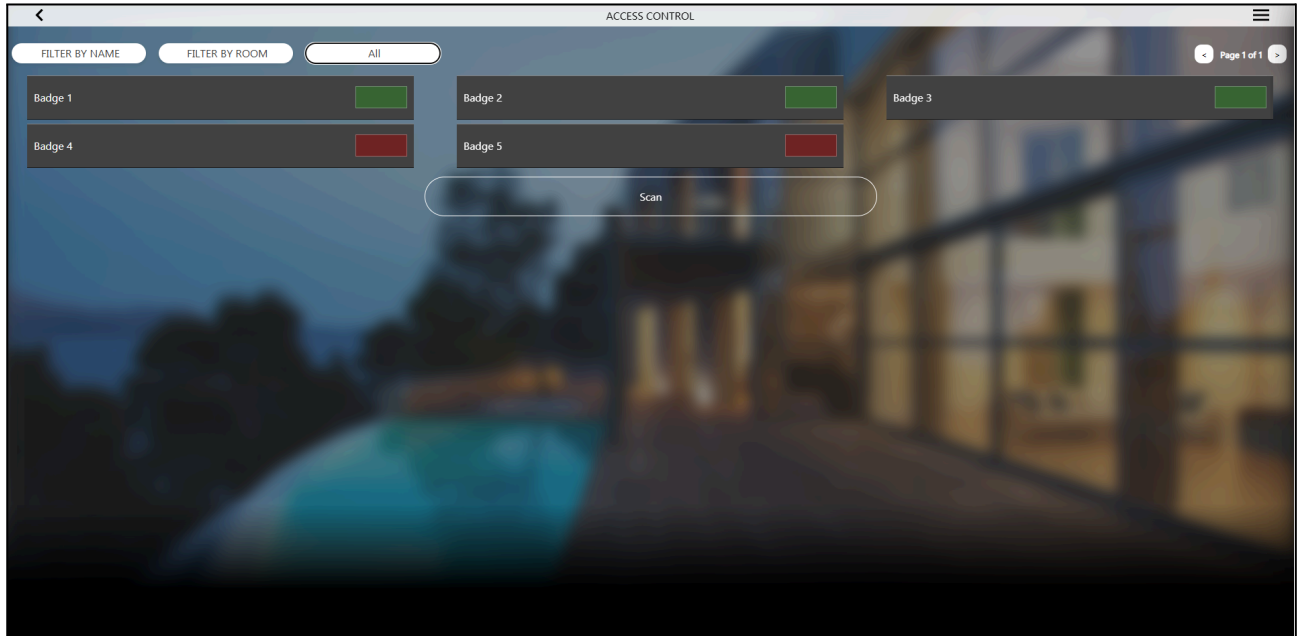
NAME	Label useful to identify the QR CODE
EMAIL ADDRESS	The email where to send the QR Code (if desired)
VALID FROM	Starting date and time of the QR Code validity period
VALID TO	Ending date and time of the QR Code validity period
ROOM	List of checkboxes of the Rooms for which the QR Code can be used to access.
GATES	List of checkboxes of the Gates for which the QR Code can be used to access.

When the QR Code is created by means of the button CREATE, the following buttons become available:

SAVE	Confirms and creates the QR Code.
SEND QR CODE VIA MAIL	If an email address is entered, it allows the user to send the mail.
PRINT	Opens in the browser a new tab containing the QR CODE suitable for the printing.
DELETE QR CODE	Deletes the QR CODE.

12.9 Badge

This section of the Visualization allows the user to visualize all the RFID Cards created or to generate a new RFID Card. RFID Cards are compatible with the MIFARE standard at 13,56MHz frequency. The access method to the structure by means of an RFID Card is enabled in the Administration view (see [section 3.1.3](#)).



By clicking the SCAN button the system will open a pop-up displaying which device (DICO or ACCÉDO KEY) the user wants to use to scan the RFID Card. After choosing the device and pressing SCAN again, the system will open a new pop-up with an information message telling the user to swipe the RFID Card on the device. When the card is read a message will ask for confirmation to add the RFID Card. After the confirmation the card will be added.

It is also possible to grant access to the structure from the Guest or Staff creation, by assigning to the guests and staff member one or more than one RFID Card. The part of the popup dedicated to this access method contains the following sections:



MANUAL SELECTION OF BADGE(S)	If this section is activated in the Administration view, the drop-down menu allows the user to select from a list all the previously created RFID Cards. Press the ADD BAGE button after the selection, to add it to the LINKED BADGES list. Note: this approach is particularly indicated for structures with a limited number of RFID Cards.
SCAN BADGE SECTION	If more than one ACCÉDO KEY is enabled for the scan, select it before doing a SCAN, or leave the option "all devices". Press the SCAN button and put the RFID Cards in front of the device; when detected, it is added to the LINKED BADGES list. If the scanned RFID Card is already in the system an error message is eventually displayed.
LIST OF ASSOCIATED BADGE(S)	This section contains the list of RFID Card(s) associated with the guest (or staff member).

13 Revision history

The following table contains the most relevant changes in the software releases, concerning the topics of this application manual:

Release	Changes	Date
2.8.0	Introduced the support for the DECENTRALIZED (WHITELIST) AUTHENTICATION for the KNX BADGE READER and HOLDER, having this impact on several sections of the guest room management	15/04/2026
2.7.0	Added Ekinex KNX badge readers and holders management	01/09/2025
	Moved PMS and CHANNEL MANAGERS to a dedicated integration manual	
	Introduced the BOOKINGS view	
	Adapted the manual to the changes introduced in the software release 2.7.0	
2.6.0	First revision of the document	02/04/2025



Before the software release 2.6 the application manuals of DELÉGO SERVER were organized differently. An exact correspondence with older versions of the manuals and the changelog could not be found for this reason.