

HORIZONE SERVER

IN00B02WEB

VIRTUAL BADGE MANUAL



Product:	IN00B02WEB
Description:	Horzone Server - Virtual Badge Manual
Date:	04/03/2020
Version:	1.3

Any information in this manual may be changed without notice.

This manual can be downloaded free of charge from the website: www.eelectron.com

Exclusion of responsibility:

Although the contents of this manual have been checked to ensure that they correspond to the hardware and software indicated in the title, changes may, however, be made. Consequently, Eelectron assumes no responsibility therein.

© 2020 Eelectron SpA. All rights reserved.

Microsoft, Windows, Windows 2000, Windows XP, Windows 2003, Windows Vista, and Internet Explorer are either registered trademarks or trademarks of Microsoft Corporation in the USA and other countries. Java is a trademark of Sun Microsystems, Inc. in the USA and other countries. All other product names mentioned herein are trademarks or registered trademarks of their respective manufacturers.

Summary

INTRODUCTION	5
Safety Information	5
Copyright	5
INTRODUCTION	6
Introduction	6
Purpose of this document	6
Requirements	7
License Upgrade	7
GENERAL SETTINGS	8
Introduction	8
Access with QR code	8
Email Configuration	11
Structure information	11
Geolocation	14
Welcome Email	15
Print Message	17
Main Menu	19
ROOMS	21
Introduction	21
New room	21
Room functions	23
CONTAINED OBJECTS	27
GATES	28
Introduction	28
New gate	28
MANAGEMENT	29
Introduction	29
Dedicated user	29
Home Page Setup	30
Access Management	30
Guests	31
Rooms	35
Access log	37

Staff	37
GUEST ACCESS FROM APP	38
Introduction	38
Welcome Email	38
Installation and first access to the app	39
Importing a Virtual Badge	40
Access to the structure	41
REVISIONS	43
OPEN SOURCE	43

INTRODUCTION

Safety Information

This manual contains the information necessary to safely operate the device. Anyone interacting with the device must first have read this documentation, especially this safety information. This document supplements and does not replace any safety laws or directives.

The device has been developed using state-of-the-art technologies and following current safety regulations; it is, however, not possible to totally exclude all possible damage or interaction with other devices during its operation. The device complies with EMC guidelines and harmonised European standards; any changes to the device may affect EMC compatibility.

The supply voltage must be strictly within the range indicated in this manual and on the device; danger of fire or explosion if power is supplied outside this range. The equipment shall be powered by a limited power supply circuit whose isolation from the mains shall be not less than that between the primary and secondary circuits of a safety transformer according to IEC 61558-2-6 or equivalent.

The CE declaration of conformity of the device can be requested from Eelectron SpA, at the contacts on the website www.eelectron.com



In accordance with Directive 2002/96/EC, electronic devices must be disposed of in dedicated facilities and not in the collection of municipal solid waste.

Copyright

HORIZONE SERVER technical instructions, manuals and software are subject to copyright; all rights are reserved. Copying, reproduction, translation and/or modification, even partial, are expressly prohibited unless approved in writing by Eelectron SpA.

INTRODUCTION

Introduction

HORIZONE SERVER allows you to virtually manage the opening of doors to enter rooms, offices or communal areas in accommodation or tertiary facilities, through a dedicated app for smartphones.

The locks associated with the doors are opened by sending the command to special KNX actuators; the VIRTUAL BADGE module allows you to manage the doors, bedrooms, guests and service personnel of the facility, the relative access permissions, plus all the settings required to operate the access via the virtual badge on the app.

Purpose of this document

This manual contains all the information required to configure virtual access control and to subsequently manage the facility by the owner, as well as the use of the smartphone app by end users.

It is assumed that the user has good knowledge of HORIZONE SERVER and KNX supervision through it; many sections of this document refer to general concepts of supervision that can be explored in the general product INSTALLATION MANUAL or in the specific manual for HORIZONE SERVER KNX technology.

Requirements

The VIRTUAL BADGE system requires the following components:

- A HORIZONE SERVER
- The license to activate the appropriate VIRTUAL BADGE module depending on the number of rooms/environments to which you wish to provide access

To enter the activation license:

- Log on to HORIZONE SERVER administration
- Select “SETUP” from the side menu, then “MANAGE MODULES AND LICENSES”
- Identify the “ACCESS CONTROL” item and enter the activation code
- Press the “SAVE” button and wait for the page to reload

Refer to the INSTALLATION MANUAL for further details.

License Upgrade

Since the number of rooms that can be managed with the VIRTUAL BADGE system depends on the license entered, if you need to expand the number of rooms, you can enter one or more activation *vouchers*; to do this, proceed as follows:

- Go to SETUP > ACCESS CONTROL > SETTINGS
- Select UPDATE LICENSE
- Enter the first *voucher* in the corresponding field
- If necessary, press ADD VOUCHER to enable additional fields, so as to enter all necessary vouchers
- Once all vouchers have been entered, press the SAVE BUTTON

For more information on vouchers and the number of corresponding rooms, please contact Eelectron customer service.

GENERAL SETTINGS

Introduction

In order to ensure that VIRTUAL BADGE works correctly, you must first configure the following general sections of HORIZONE SERVER:

- Access with QR code
- Email

In addition, the configuration requires you to enter/configure the following entries related to ACCESS CONTROL:

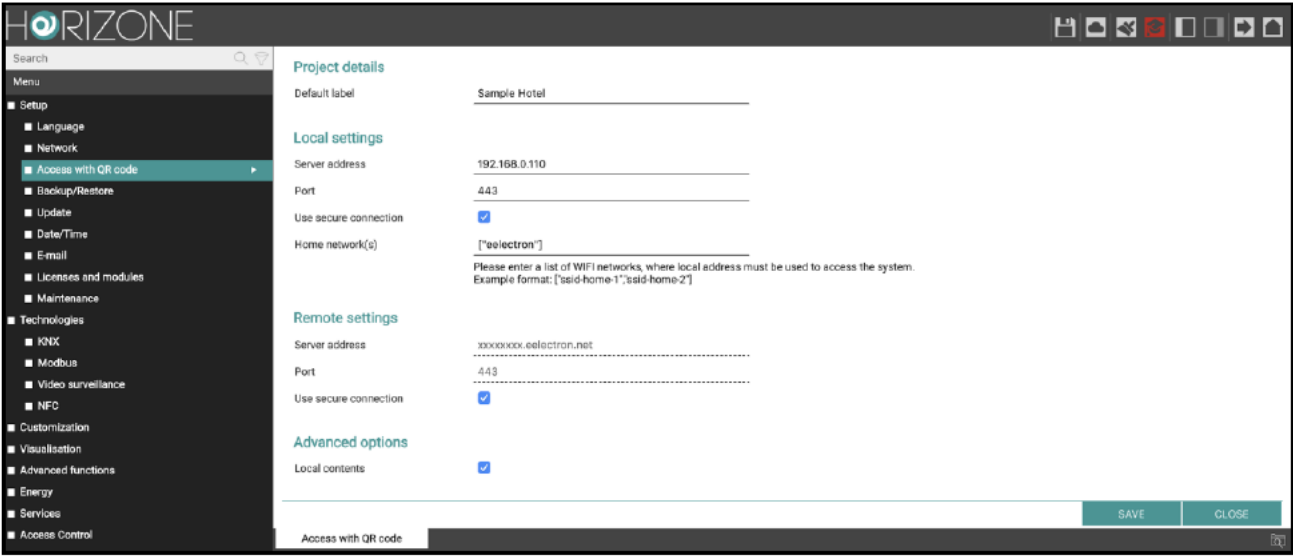
- Structure information
- Welcome email (recommended)
- Print message (recommended)
- Main menu (optional)

Access with QR code

Since *virtual badges* based on QR technology will be sent to the users of the facility, it is essential that QR code access to HORIZONE SERVER is correctly configured, through the appropriate section in the SETUP menu.

Proceed as follows to open the ACCESS WITH QR CODE page:

- Log on to HORIZONE SERVER administration
- Open the SETUP section of the side menu
- Press ACCESS WITH QR CODE: the following page is automatically accessed:



The following parameter is available in the "PROJECT DETAILS" section:

DEFAULT LABEL	This allows you to define the name of the structure: if present, this field will be displayed by the end user within the application and will be the name of the sender that will be displayed in the emails sent to users
---------------	--

The following parameters are available in the "LOCAL SETTINGS" section:

SERVER ADDRESS	enter the local IP address of the webserver
PORT	insert the local port since the https protocol will be used for security in communication between webserver and APPS, the port to be entered will be 443
USE SECURE CONNECTION	This flag indicates whether or not you want to use the https protocol; in the access control configuration, this flag must be checked for the same reason given in the description of the PORT parameter

HOME NETWORK(S)	<p>This field allows you to enter the list of Wi-Fi network names, where the app must use the local IP address to gain access, in the format described in the example.</p> <p>Sample format: ["ssid-casa-1", "ssid-casa-2"]</p> <p>Enter the WIFI network or WIFI networks in the list that, if used by guests' smartphones, will allow you to reach the HORIZONE webserver on the local network. If the guest WIFI network cannot be reached, enter a single "dummy" entry as in the following example:</p> <p>["dummy"]</p> <p>In this way, access will always be via the public network</p>
-----------------	--

The "REMOTE SETTINGS" section is optional but strongly recommended, to allow users to gain access even without being connected to the facility's WIFI network.

The parameters available for this section are as follows:

SERVER ADDRESS	Remote IP address of the webserver (or its DNS)
PORT	Remote port for https communication
USE SECURE CONNECTION	This flag indicates whether or not you want to use the https protocol; in the access control configuration, this flag must be checked for the same reason given in the description of the PORT parameter

If you have enabled the remote cloud access service without opening ports on the router, these fields are automatically populated and cannot be edited.

Finally, in the "PROJECT DETAILS" section, the following parameter is available:

ENABLE LOCAL CONTENTS	This option can be enabled or disabled as desired; it is recommended to leave the option checked for greater speed when the project is loaded from the APP
-----------------------	--

When the configuration has been completed, press the SAVE button, otherwise the configuration will not be saved.

Email Configuration

Since HORIZONE SERVER will automatically send emails to the users of the facility, containing the instructions for access and the virtual badge to be used with the VIRTUAL BADGE app, the server must be correctly set up to send emails.

To configure the parameters for sending emails, go to the section

SETUP > EMAIL

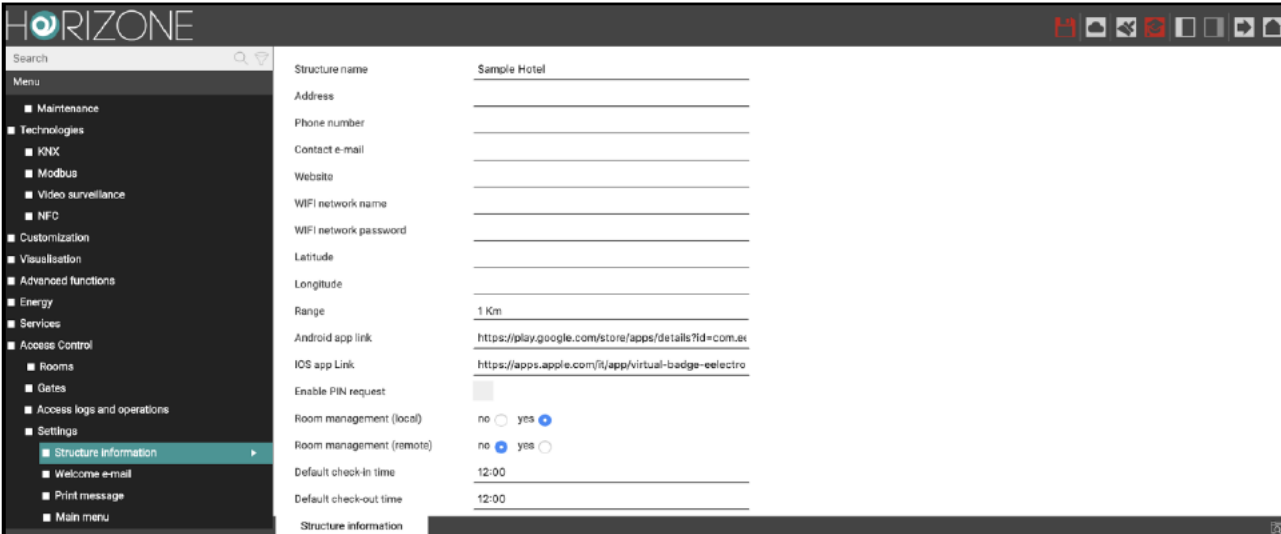
and fill in the required fields; for further information, refer to the general INSTALLATION MANUAL.

Structure information

To ensure the best experience for end users, it is advisable to enter a series of information related to the structure managed by HORIZONE SERVER; part of this information will be communicated to the customer through the VIRTUAL BADGE app and part will be used to configure ACCESS CONTROL behaviour.

To open the STRUCTURE INFORMATION page:

- Open the ACCESS CONTROL section of the side menu
- Open the SETTINGS sub-section of the side menu
- Press the STRUCTURE INFORMATION entry to open the following settings page



You can enter the following information:

STRUCTURE NAME	<p>This allows you to define the name of the structure: if present, this field will be displayed by the end user within the application and will be the name of the sender that will be displayed in the emails sent to users</p> <p>N.B. If this field is present, it replaces the functions of the default label field previously entered in the ACCESS WITH QR CODE section.</p>
ADDRESS	<p>This allows you to define the street name and street number of the structure; if entered, the end user can view the structure on google maps by pressing the appropriate button in the APP</p>
PHONE NUMBER	<p>This allows you to define the phone number; if entered, the end user can view and call the number directly by pressing the appropriate button in the APP</p>
CONTACT EMAIL	<p>This allows you to define the email to which the user can write for any eventuality, directly from the APP</p>

WEBSITE	Public website of the structure, which will be displayed in the app and the welcome email
WIFI NETWORK NAME	<p>Name of the structure's Wi-Fi network</p> <p>If entered, it is communicated to end users in the welcome email, so that they can connect and use the internet access and the ACCESS CONTROL functions of HORIZONE SERVER, without being force to go via a remote connection</p>
WIFI NETWORK PASSWORD	Structure's Wi-Fi password
ANDROID APP LINK	Link to download the VIRTUAL BADGE APP for customers using Android smartphones. Do not modify this link, except in the case of specific needs.
IOS APP LINK	Link to download the VIRTUAL BADGE APP for customers using Apple iPhone. Do not modify this link, except in the case of specific needs.
ENABLE PIN REQUEST	<p>If this flag is checked and there are no other gate identification technologies (e.g.: BEACON BLUETOOTH) or if there are problems with the latter, the app requires a PIN to open the door.</p> <p>If disabled, it allows you to open the doors directly, once you are in the VIRTUAL BADGE app.</p>
ROOM MANAGEMENT (LOCAL)	If checked, this flag allows the end user to manage the automation functions of their room, once he/she has entered the application with the local settings (connected in Wi-Fi to one of the networks listed in the HOME NETWORKS parameter)

ROOM MANAGEMENT (REMOTE)	If checked, this flag also allows remote control of room automation
DEFAULT CHECK-IN TIME	If set, it is used as the default virtual badge start time when entering a new guest
DEFAULT CHECK-OUT TIME	If set, it is used as the default virtual badge end time when entering a new guest

Geolocation

You can also fill in these fields in structure information:

LATITUDE LONGITUDE	The coordinates (in numeric format, using the point as decimal separator) of the site where HORIZONE SERVER is installed
RANGE	Distance within which the VIRTUAL BADGE app is enabled to enter the structure

If you fill in these fields, HORIZONE SERVER performs a further check on the smartphone location of guests using the VIRTUAL BADGE app; if it is not within the specified range, the virtual badge cannot be used, even if still valid.

This prevents doors being opened accidentally by users who are not physically present in the structure.

Welcome Email

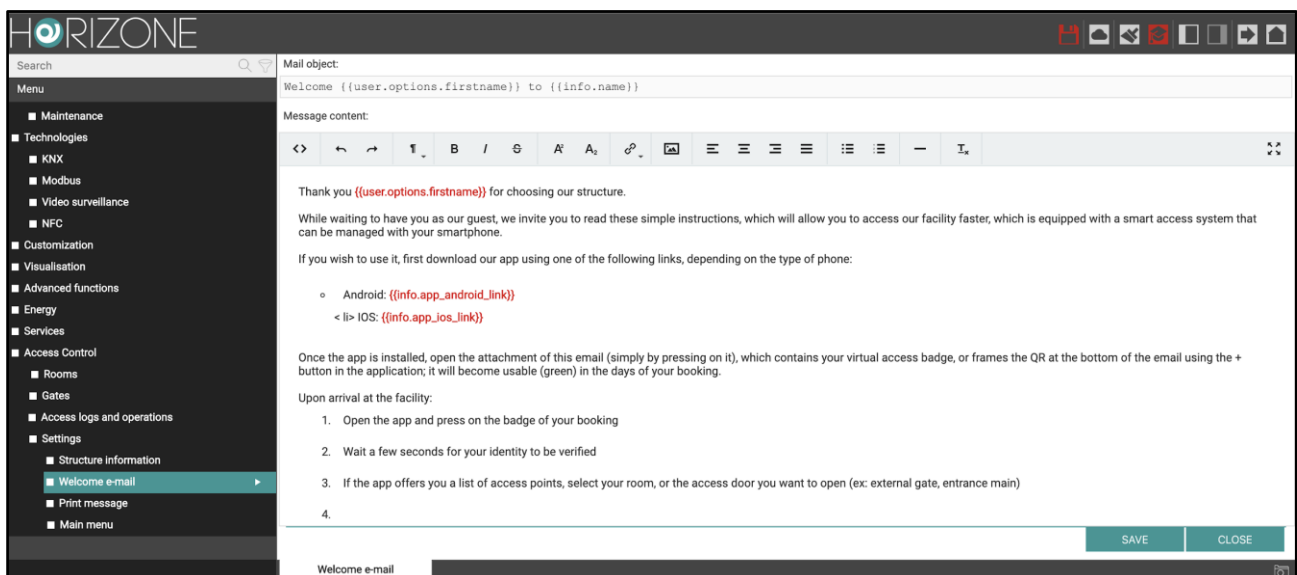
The WELCOME EMAIL page allows you to customise the welcome email that will be sent to the user telling them about the steps they will have to take to access the structure.

HORIZONE SERVER provides a generic text, containing all the information that can be sent to the user; dynamic elements (highlighted in red) are inserted in the text that are replaced with the structure's and user's data when sending emails.

The text can be completely or partially revised, maintaining the dynamic elements.

Proceed as follows to open the WELCOME EMAIL page:

- Open the ACCESS CONTROL section of the side menu
- Open the SETTINGS sub-section of the side menu
- Press WELCOME EMAIL: you will automatically access the following page:



Using the built-in editor, you can view and edit the email to be sent, starting from the default text.

You can configure the following texts separately:

- EMAIL SUBJECT
- MESSAGE CONTENT

You can insert dynamic tags in each of these, which will allow you to send emails, for example, containing the name of the user to whom it is addressed; these tags are defined between two curly brackets: {{ }}.

Tags are defined by two or more parts separated by a period; the first part may contain the following keywords:

- **user:** dynamic tag that replaces the properties of the user to whom the email will be sent

- **info:** dynamic tag that replaces the structure information entered in the configuration

The following table contains all the possible dynamic tags that you can insert into the text:

USER/GUEST INFORMATION

user.name	Last name and first name of the user to whom the email is addressed
user.options.firstname	First name of the user to whom the email is addressed
user.options.lastname	Last name of the user to whom the email is addressed
user.options.pin	Pin code of the user to whom the email is addressed, which will allow them to access the doors if the PIN option is enabled in the web server configuration

STRUCTURE INFORMATION

info.name	Structure name, entered in the configuration
info.app_android_link	Android APP link, entered in the configuration
info.app_ios_link	IOS APP link, entered in the configuration
info.wifi_ssid	Name of the Wi-Fi network, entered in the configuration
info.wifi_pwd	Wi-Fi network password, entered in the configuration

info.phone	Phone number, entered in the configuration
info.email	Contact email, entered in the configuration
info.www	Site of the structure, entered in the configuration

When you have finished editing the email, press the SAVE button, otherwise the changes will not be made.

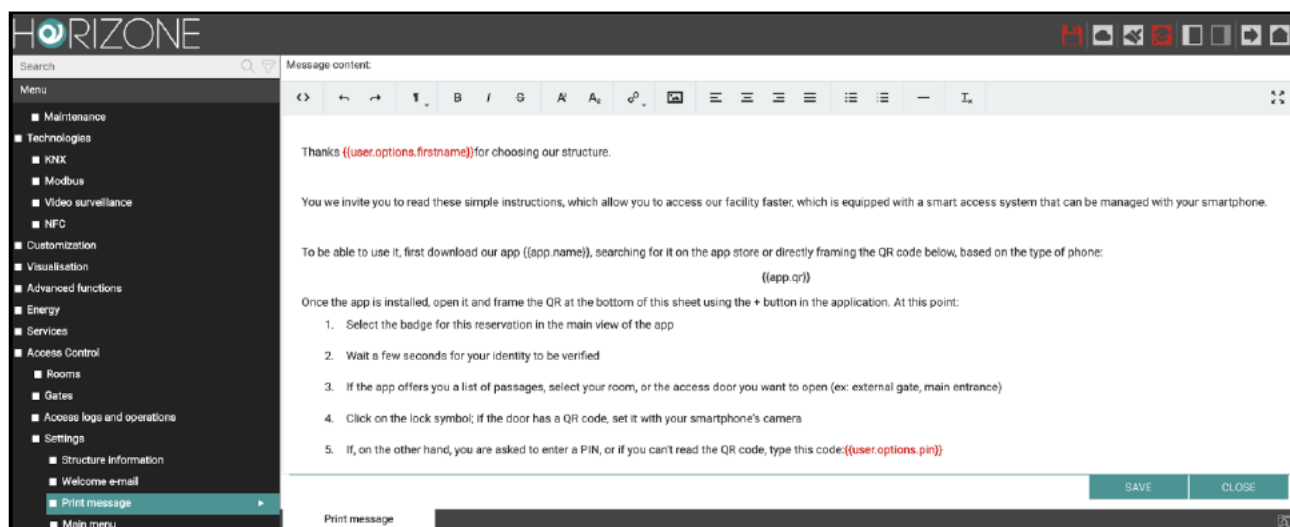
Print Message

The PRINT MESSAGE page allows you to customise the text that can be printed for the user, if you do not want to send the welcome email, for example because the guest is directly at the reception.

As with the welcome email, there is a default message here again containing user instructions, explaining the steps to be taken to start using the APP and the PIN code, which is different for each user, and will be entered if the PIN option is enabled in the webserver configuration.

Proceed as follows to open the PRINT MESSAGE page:

- Open the ACCESS CONTROL section of the side menu
- Open the SETTINGS sub-section of the side menu
- Press PRINT MESSAGE: the following page is automatically accessed:



The page is similar to the welcome email configuration: there is an editing page here as well with a message containing dynamic tags that can be edited. You can enter the following tags in addition to the tags previously described in this message:

app.name	The APP name will be displayed
app.qr	Generates a table containing two QR codes in the middle of the page, to be used to quickly download apps for Android and IOS respectively

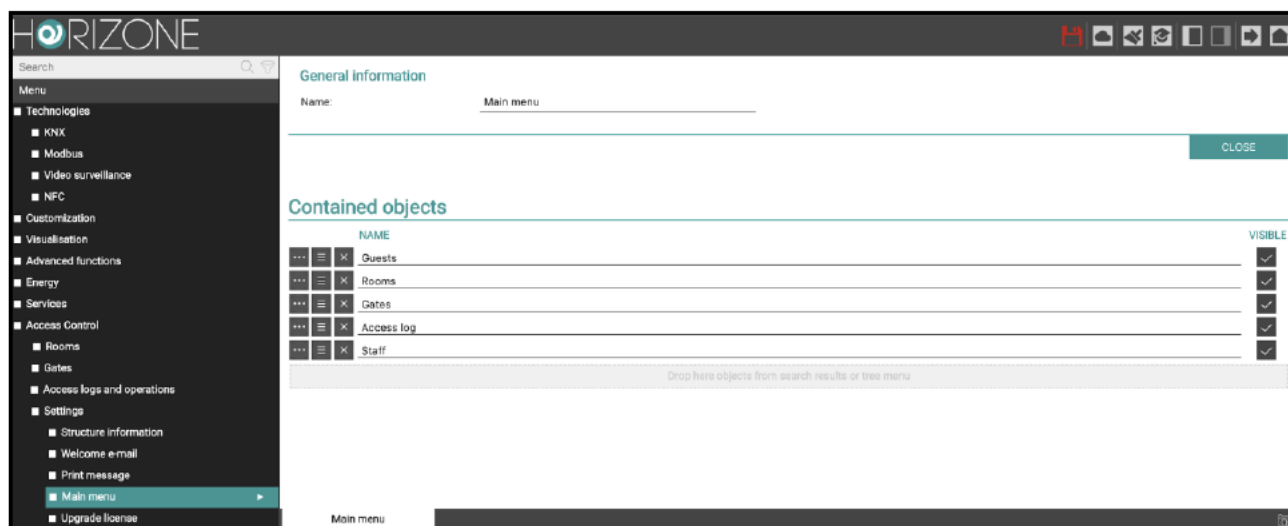
When you have finished editing the print message, press the SAVE button, otherwise the changes will not be made.

Main Menu

The MAIN MENU section allows you to customise the main menu that will be used in the HORIZONE SERVER frontend area, by the facility manager, for access management.

Proceed as follows to open the MAIN MENU page:

- Open the ACCESS CONTROL section of the side menu
- Open the SETTINGS sub-section of the side menu
- Select MAIN MENU and open the page by pressing the three dots next to the name: the following page is accessed:



In the GENERAL INFORMATION section, you can change the page title that acts as a menu, while in the CONTAINED OBJECTS section, you can change the following entries in the following sections:

GUESTS	This section allows you to view the list of pre-configured guests and create new ones
ROOMS	Section containing the list of environments managed through access control
ACCESS LOG	Table containing a list of operations performed by users through the access control system

STAFF	Section that allows you to manage the staff of the structure and create new enabled users
-------	---

For more information on the access control management menu, please refer to the next chapter of this manual.

ROOMS

Introduction

The ACCESS CONTROL management of HORIZONE SERVER typically allows you to manage access to one or more environments, for which the term “room” is used for hotel purposes. If you want to manage environments that are not rooms, simply assign them a different name, as illustrated in detail below.

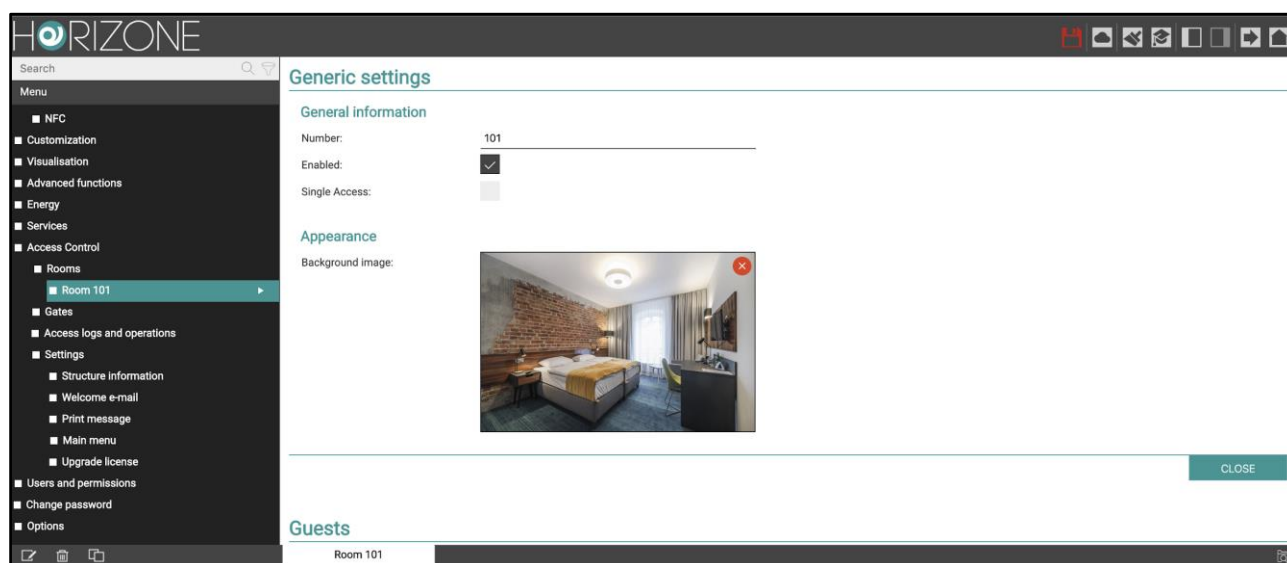
In addition to opening the access door, it is possible to allow both the building manager and end users to manage automation of devices in this environment, all through the same VIRTUAL BADGE app.

New room

Proceed as follows to create a new room:

- Open the ACCESS CONTROL section of the side menu
- Press the ROOMS sub-section of the side menu
- Press the '+' button at the bottom left

You access the configuration tab by selecting the new room and pressing the relevant shortcut (“three dots”) in the menu:



You can edit the following information in the GENERAL INFORMATION section:

NUMBER	This parameter indicates the room number; changing it will automatically update the room name with the number entered in this field
ENABLED	This flag indicates whether or not it is possible to interact with the room functions; if it is disabled, no user will be allowed to interact with the room through ACCESS CONTROL
SINGLE ACCESS	<p>If this flag is checked, the end user (guest) can only open the access door to the room ONCE via the VIRTUAL BADGE app.</p> <p>This feature is designed for unattended structures whereby the user can find the badge or key inside their room and to ensure that after the first access via app, they use the latter to access the structure.</p> <p><i>Note: In this particular configuration, to restore the possibility of opening the door (for a second time) to a guest, simply disable it, and re-enable it, as illustrated in detail below.</i></p>

You can also change the following parameter by activating the advanced mode (toolbar at the top right) in the GENERAL INFORMATION section:

NAME	This parameter allows you to customise the name of the room/environment with respect to the standard wording "Room X" (where X is its number)
------	---

You can also change the following parameter in the APPEARANCE section:

BACKGROUND IMAGE	This parameter allows you to choose an image that will be the background to the current room in the frontend
------------------	--

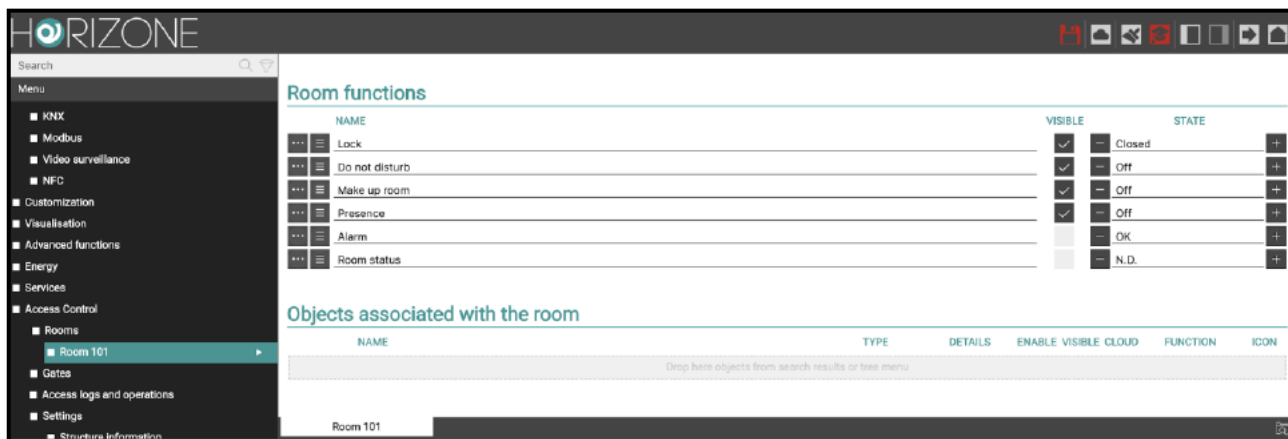
You can view all guests who are allowed to interact with the current room in the GUESTS section. For more information on guest management, please refer to the following chapter.

Room functions

When creating a room, the following “virtual” functions are provided:

LOCK	This represents the opening of the door to access the room
DO NOT DISTURB MAKE UP ROOM	They represent respectively the “DO NOT DISTURB” and “MAKE UP ROOM” functions typically used in hotels to request staff not to access the room or to clean it
PRESENCE	Identifies the presence or not inside the room
ALARM	Represents an alarm detected in the room, for example with the pull cord in the bathroom or a sensor
ROOM STATUS	Represents the general status of the room; it can be in one of the following: <ul style="list-style-type: none"> • Free • Booked • Assigned • Busy • Service

To view room functions, you need to enable ADVANCED viewing with the toolbar button at the top right

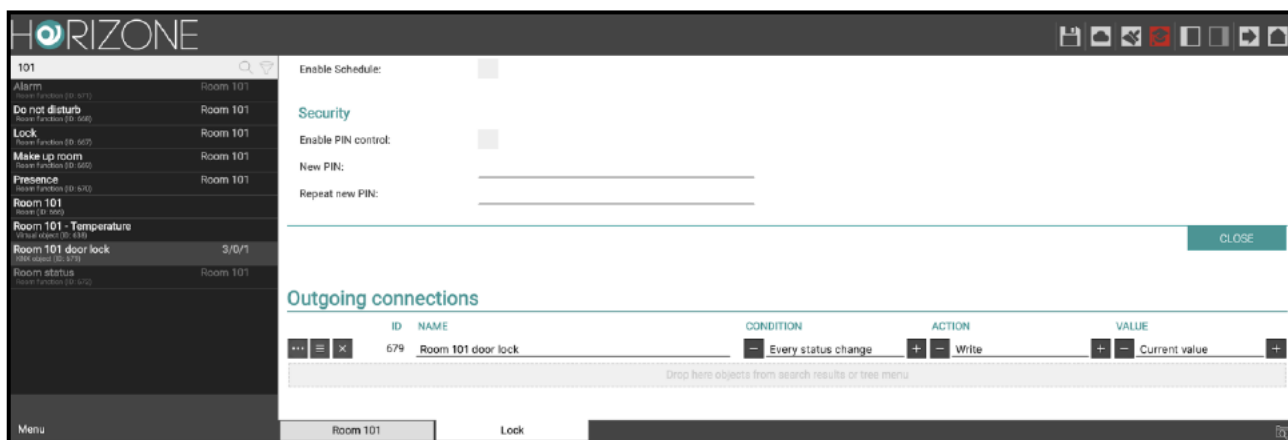


When creating the room these functions are completely virtual; if you want to use them materially, you must associate them with a KNX object.

Depending on the type of function, this association is seen as “outgoing” (to control a device, as in the case of the lock, for example) or “incoming” (to change the status of the room function, starting from a bus input module).

To do this, you can access the function tab and drag the technological objects with which it must interact, into the OUTGOING CONNECTIONS or INCOMING CONNECTIONS sections.

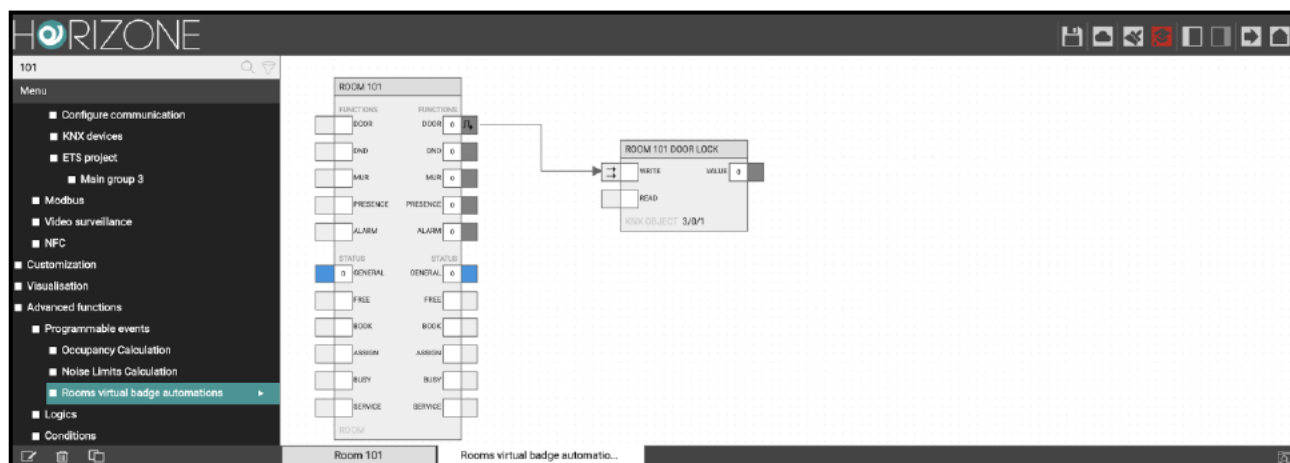
In the following example figure, a KNX electric lock has been associated with the room’s “LOCK” function by dragging the corresponding KNX OBJECT into the OUTGOING CONNECTIONS section:



The following fields must be filled in appropriately, according to the specific needs, and the type of object that is dragged:

CONDITION	<p>Specifies the value of the function for which you want to control the technological object</p> <p>E.g. only if the lock is opened</p>
ACTION	<p>Choose the required action if HORIZONE SERVER objects include multiple actions. The default value "WRITE" should normally be left.</p>
VALUE	<p>Value to be passed to the technological object. It can be an "ON" or "OFF", for example; by selecting the "CURRENT VALUE", the status of the starting function is used.</p> <p>In the case of the lock, if the "CURRENT VALUE" option is used, the parameter set in the general settings of the structure is used as the excitation time of the lock.</p>

You can create a PROGRAMMABLE EVENT (ADVANCED FUNCTIONS section) as an alternative to this configuration mode, by dragging the ROOM object and the technological objects you want to control, directly into it, as in this example:



For more information about CONNECTIONS and HORIZONE SERVER PROGRAMMABLE EVENTS, see the GENERAL INSTALLATION MANUAL.

At the time of creation, the functions are marked as NOT VISIBLE; this implies that they are available for any automation (necessary, in the case of the lock for example, if you want to activate the opening of the door/access gate) but not manageable through the FRONTEND, or through the VIRTUAL BADGE app by end users (guests).

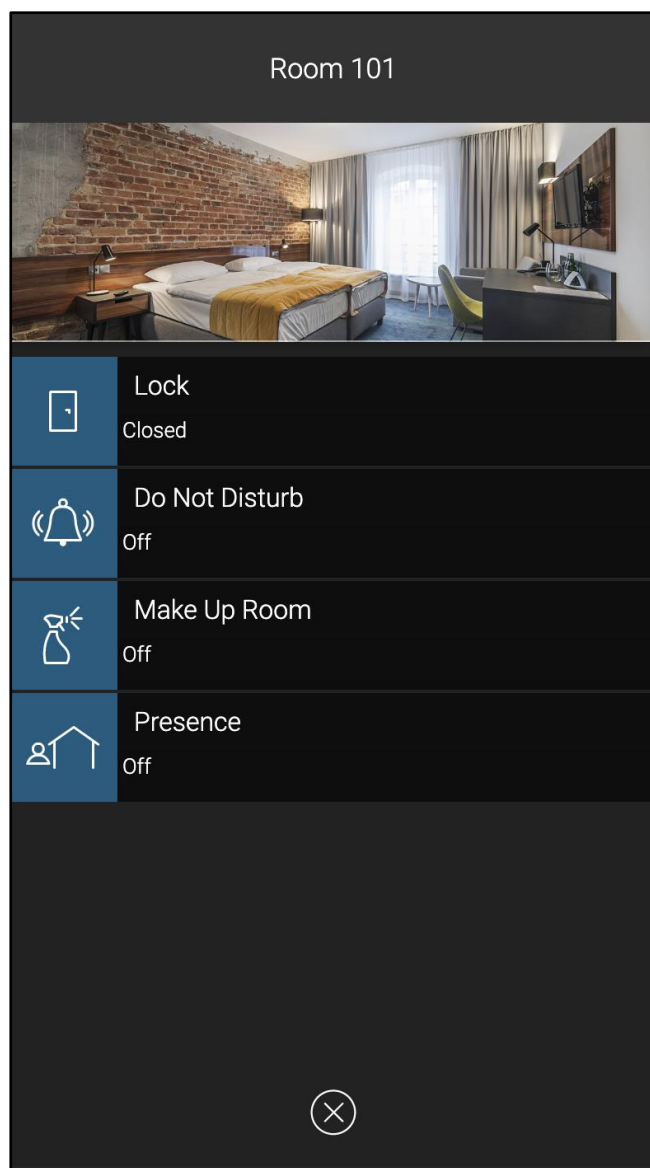
If you want to manage one or more of these functions from the frontend, simply check the corresponding visible flag; if a given function must not to be used either for automation or displayed, it can be permanently removed via the corresponding delete button (trash can icon).

CONTAINED OBJECTS

In addition to the functions, it is possible to associate one or more technological objects with a room, so that they can be managed by both the operator and the end users in their ROOM MANAGEMENT.

To do this, simply drag the objects you want from the respective menus into the TECHNOLOGIES section, or from the search results, into the CONTAINED OBJECTS section.

The end result, in the VIRTUAL BADGE app, looks like this example:



GATES

Introduction

In addition to the rooms, HORIZONE SERVER can also manage the opening of gates, which are not associated with environments, such as an external gate or main access door to the structure, or even the access door to communal parts.

These gates must be enabled for all users, regardless of their room, otherwise they will not be able to access the building, even before get to their assigned room.

As we will see, the configuration method of the gates is very similar to the rooms, but they have a slightly fewer functions because they do not need to be viewed by users and do not require an object to be inserted in them.

New gate

The creation and management of a gate is identical to that of a room with some minor differences:

- The gate does not have a number to associate with it, but you can still change its name.
- You cannot set a background image for the gate.
- The only function available for the gate is the lock.
- On the other hand, it offers the ACTIVE BASIC FLAG FOR GUESTS: if enabled when creating a guest, this gate will be assigned as the default; you can still decide to remove this assignment at this time. This flag is useful for speeding up the creation of users and is designed for gates which are accessed by all customers (such as the outside gate)

A KNX command is associated with the opening of the lock in the same way that it was for rooms, by accessing the lock function tab and associating the object to be controlled via the OUTGOING CONNECTIONS (or, alternatively, by configuring a PROGRAMMABLE EVENT).

MANAGEMENT

Introduction

Once the configuration has been completed as outlined above, the building manager can only operate in the HORIZONE SERVER FRONTEND to manage guests, staff and rooms.

Dedicated user

It is advisable to configure (at least) one dedicated user in HORIZONE SERVER as the building manager who differs from the admin user; this will limit accidental errors when configuring the webserver.

The access control module introduces a new user group called “ACCESS MANAGERS” which has all the rights strictly necessary for access administration; it is, therefore, advisable to:

- Create a user in the section named USERS AND PERMISSIONS > USERS
- Once created (and associated with a password), drag the “ACCESS MANAGERS” group into it
- Go to the SETUP section > ACCESS WITH QR CODE
- Identify the new user in the section at the bottom and press the corresponding “QR CODE” button
- Give the building manager the QR code generated by HORIZONE SERVER to speed up his/her configuration of the HORIZONE app

The manager must use the HORIZONE app to manage access; the VIRTUAL BADGE app, as will be seen below, is dedicated exclusively to the staff and guests of the structure and has functionalities closely linked to the opening of the gates and the management of their room.

Home Page Setup

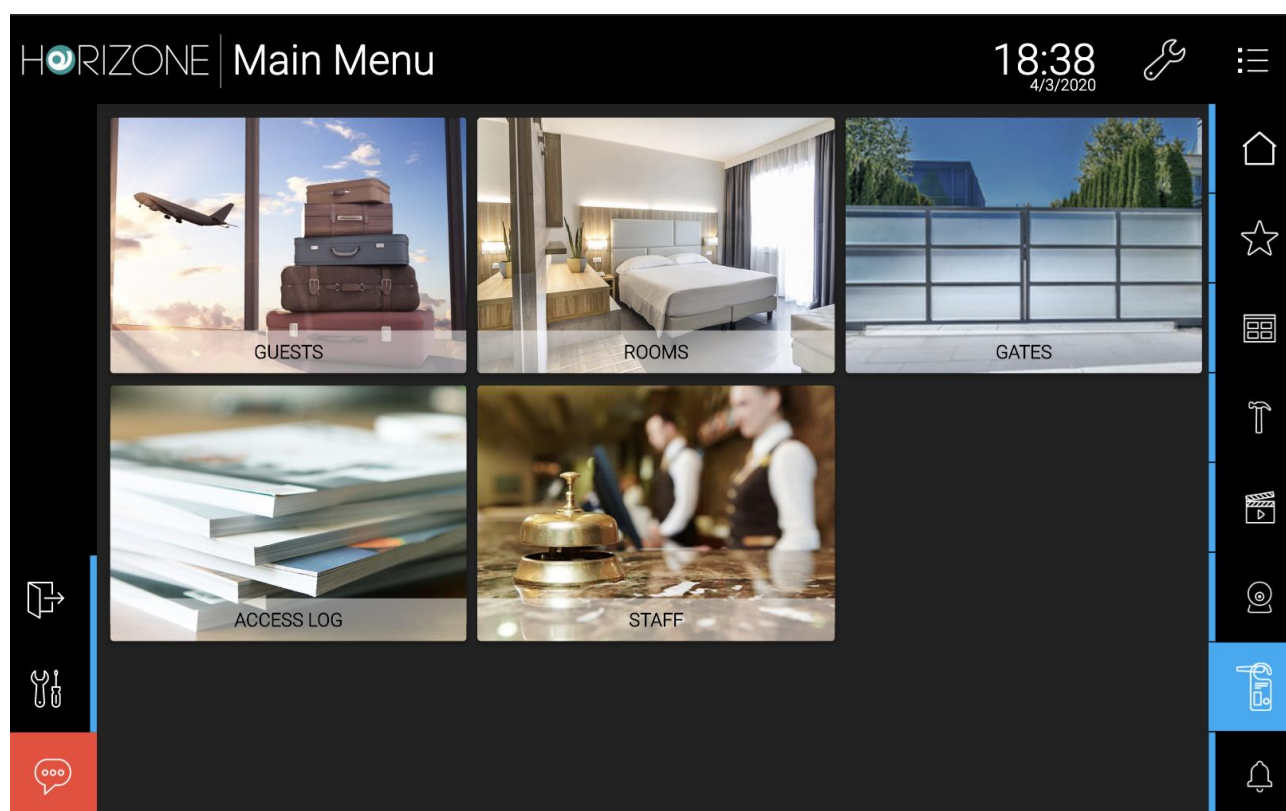
You should set the main menu of ACCESS CONTROL as the homepage for the building manager user; to do so:

- Open the user tab created in the previous step
- Identify the “ENVIRONMENT FOR HOMEPAGE” field
- Expand the ACCESS CONTROL menu > SETTINGS
- Drag the ACCESS MANAGEMENT sub-entry

If you have not set access control as the default home, however, you can access its menu from the HOME PAGE by selecting ACCESS MANAGEMENT.

Access Management

The access management screen appears as follows:



The basic entries available are:

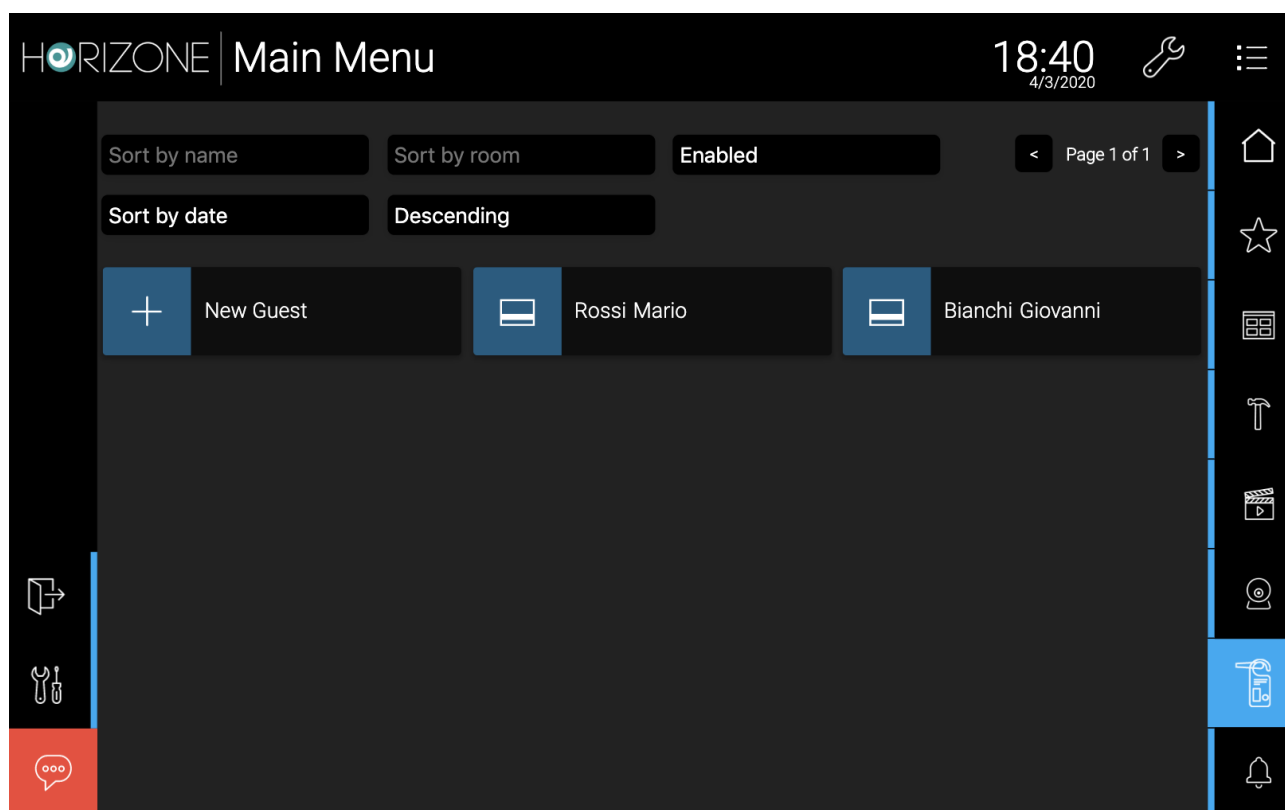
- GUESTS
- ROOMS
- GATES
- ACCESS LOG
- STAFF

You can add HORIZONE SERVER environments to this menu; this is useful for making supervision pages available to the building manager when his/her homepage becomes this menu, as outlined in the previous point. To do this, simply:

- Open ACCESS CONTROL in edit mode > SETTINGS > MAIN MENU
- Drag the HORIZONE SERVER environments, making sure they are associated with a background image (which is used as an image in the menu)

Guests

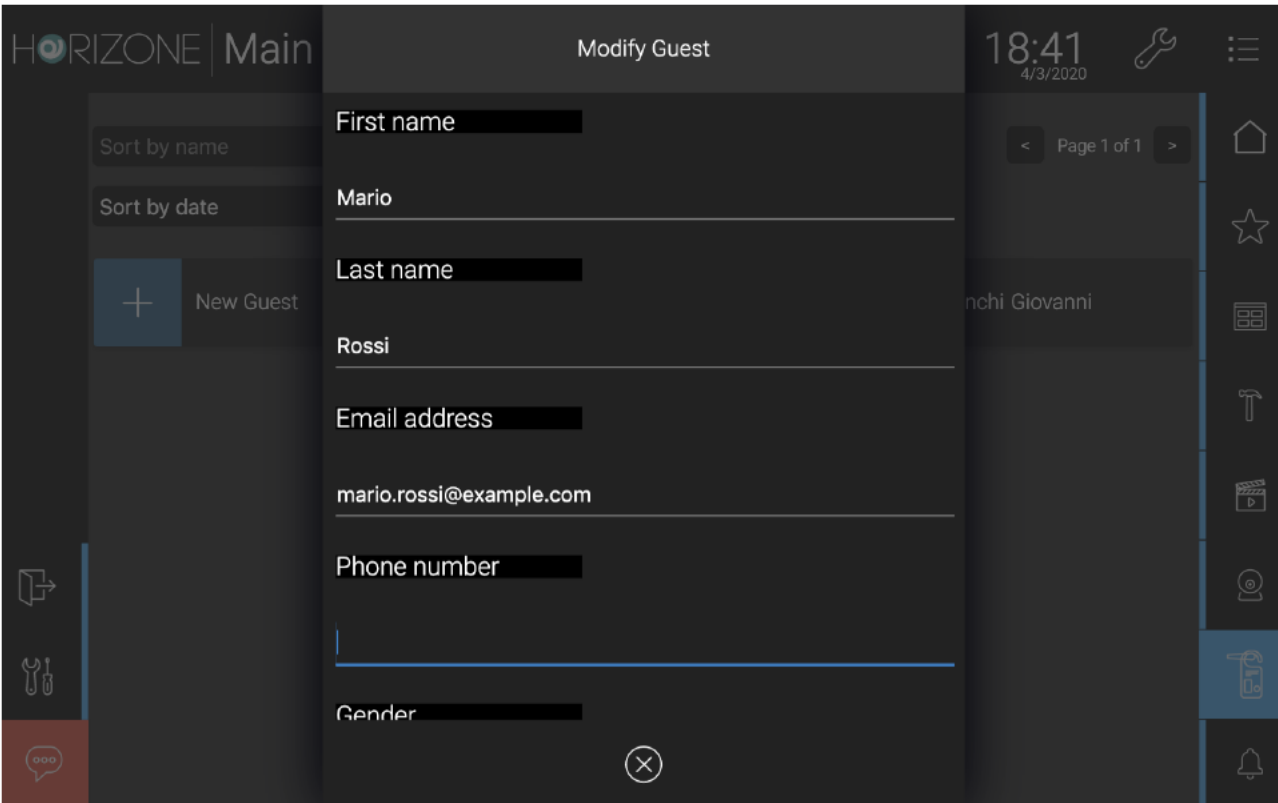
This entry allows you to create and manage guests for the structure. The following page opens, allowing you to create new customers and manage previously created ones:



There is a search bar in the top left corner, which is useful for finding a specific user by NAME, by ROOM assigned to them or their status (ENABLED/DISABLED); you can also SORT the search by NAME or DATE created (default) in ASCENDING or DESCENDING ORDER (default).

The page navigation menu in the top right corner; if you have more than 15 guests (maximum number of guests viewed per page), you can switch between pages to view all of them.

To create a new guest, simply press the NEW GUEST button and fill out the form that is proposed in the form of a popup window:



The parameters that can be entered are the following:

<p>FIRST NAME (required)</p> <p>LAST NAME (required)</p>	<p>Guest's first and last name</p>
<p>EMAIL ADDRESS</p>	<p>Guest's email address</p> <p>This will be used to send automatic welcome emails</p>

PHONE NUMBER	Guest's phone number
GENDER	Specify whether male or female
ACTIVE FROM NOW	A drop-down menu that defines whether the guest should have the check-in date and time as the date and time he/she is created or another date.
VALID FROM	The date and time when the virtual badge associated with the guest becomes valid.
VALID TO	Virtual badge end-of-validity date and time
ROOM	This drop-down menu contains all available rooms (those created in backend). You can only assign one room to each guest
GATES	One or more gates that the guest can open, in addition to their room

There are X's Next to the VALID FROM and VALID TO fields that allow you to leave the VALID FROM, VALID TO or both fields blank.

Pay attention to these fields because if they are left blank, it means that the user you are going to create will ALWAYS be able to access the room functions available to them.

After entering all the information, press the CREATE button to create the new user.

Once the user has been created, new buttons will be activated:

EMAIL QR	This button is activated only if an email address has been entered when the guest is created; if pressed, it automatically sends the welcome email, using the preset text, in which the <i>dynamic tags</i> are replaced with the data for the structure and the guest in question
PRINT QR	Opens a new browser tab with the welcome message in print format

Press the X key to return to the guest page; the newly created user will appear in the list.

The colour of the icon on the left of the guest's name may differ depending on the validity period (check-in/check-out) and current date and time:

GREEN	The current date and time fall within the check-in and check-out period of that user; It means that the user is enabled to use the room functions that available to him/her
RED	The current date and time do not fall within the check-in and check-out period for that user; It means that the user is not enabled to use the room functions at this time

To change any parameter entered during creation, to resend the email or to print the sheet containing the print message, you must open the user for whom you want to perform one of these actions in "edit". To do this, simply press on the grid object that corresponds to the user you want to select; a pop-up window similar to the previous one will automatically open, this time in "Edit" mode.

When the change has been completed, press the SAVE button to save the configuration or X (top right) to cancel the changes. There are two new buttons in the editing phase:

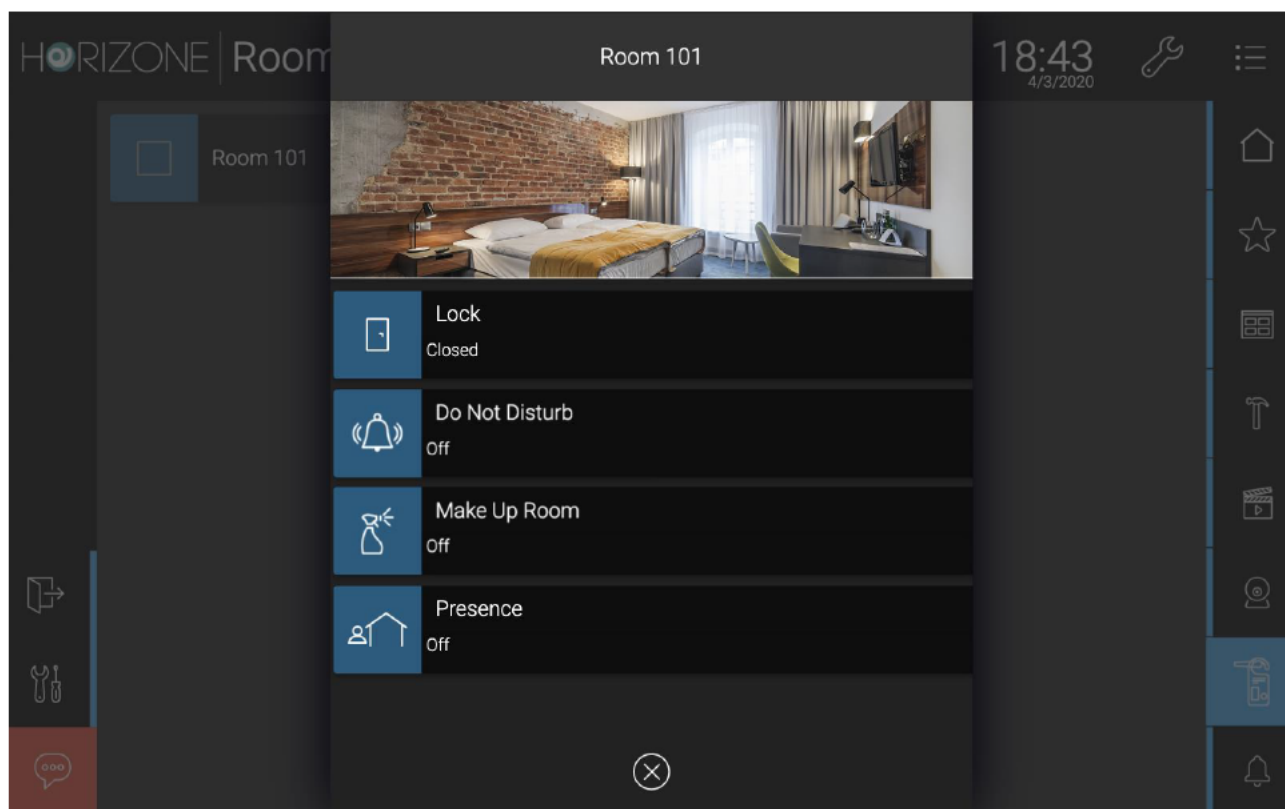
DISABLE/ENABLE	<p>The disable button is active when the user is enabled at that time; this button, if pressed, changes the check-out date to the current date and time and clears the check-in date so that the user will no longer be enabled to use the room functions.</p> <p>Conversely, if the user is disabled, the ENABLE button appears, which changes the check-in date to the current date and time and clears the check-out date so that from then on, the user will be enabled to use the room functions.</p> <p>After this operation, it is very important to remember to enter an expiration date, otherwise the user will be enabled to use the room functions forever.</p> <p>In addition to changing the check-in and check-out dates, the ENBABLE function also assigns a new PIN to the user;</p> <p>You will then need to communicate the new PIN to the user</p>
DELETE GUEST	<p>This button opens a confirmation window;</p> <p>Confirming the notification deletes the user</p>

Rooms

This section of the main menu allows the manager to control all the rooms in the building, acting on the associated objects in the same way that guests can, if room management is enabled, from the VIRTUAL BADGE app, each guest on their own room.

The different colours depend on each ROOM STATUS; by making this *function* visible to the rooms (see room configuration section above), the manager can modify it directly from this section of the frontend making it easier to identify the condition of the rooms.

When you press on a room, the popup windows containing the associated objects will be displayed:



Note: Some objects, even if made visible, cannot be managed by guests through the VIRTUAL BADGE app, such as the lock. This allows the manager to conveniently open the doors of the rooms from the app, while guests must use the lock management provided by the VIRTUAL BADGE app, as shown below.

Access log

Each login operation is stored by HORIZONE SERVER and can be consulted in the ACCESS LOG section. There are also fields at the top of this page that allow you to filter the search for logs based on the specified parameters.

Staff

This section allows you to create and manage one or more users representing staff (service or maintenance technician, etc.) who will use the VIRTUAL BADGE app to access the structure and its environments protected by the access control.

The management is exactly the same as the one for guests, with the sole difference that for service staff, it is possible to associate more than one room at the same time, so as to enable the person to enter all the environments.

GUEST ACCESS FROM APP

Introduction

As already mentioned, guests (or service staff) use a dedicated app to access the building, called a VIRTUAL BADGE which can be downloaded from Android and IOS stores:

Android

<https://play.google.com/store/apps/details?id=com.eelectron.virtualbadge>

Apple IOS

<https://apps.apple.com/us/app/virtual-badge-eelectron/id1482374881>

Welcome Email

As explained in the previous chapter, when the manager enters a guest's personal data in the system, HORIZONE SERVER automatically sends a welcome email, which contains all the instructions for accessing the structure.

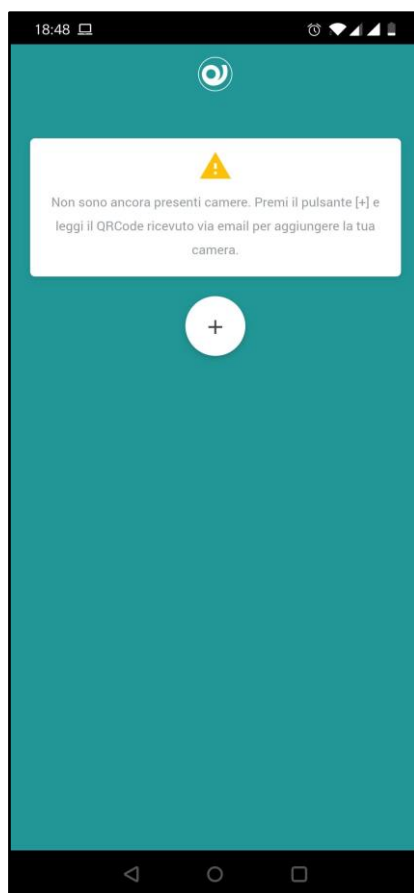
The welcome email, based on the previously preset text, typically contains instructions for:

- Downloading the VIRTUAL BADGE app
- Logging in to the app and importing the virtual badge
- Accessing the structure's WIFI network
- Other general information, such as contacts, references, address, etc.

Installation and first access to the app

Once the APP has been installed, the first time you open it, you will be prompted to protect your access, depending on your device unlock security setting (sequence, fingerprint, or facial recognition), if present. If you enable this mode, third parties will not be able to access the app and open the gates, including if your phone is lost or stolen.

The app welcome screen looks like this:



Importing a Virtual Badge

Initially, the app does not have a virtual badge; the guest is provided with a virtual badge, for each reservation, in the following ways:

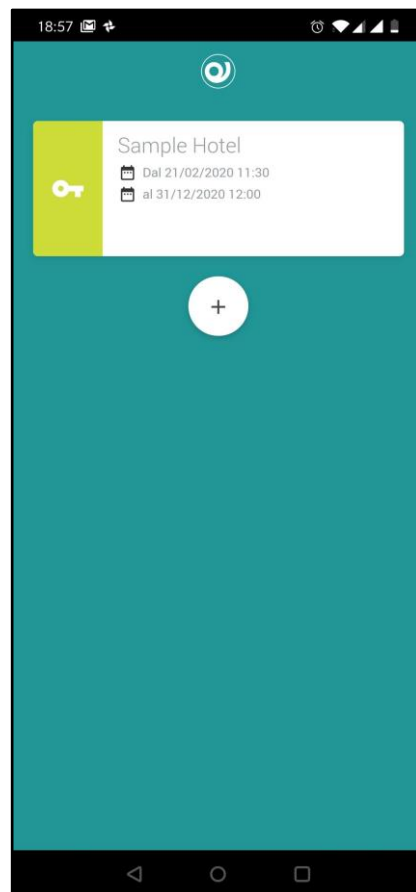
- In the form of a QR code within the welcome email
- As an attachment to the welcome email
- In the form of a QR code, in the case of a sheet of paper printed at the reception

If you cannot access the welcome email directly from your phone, you will need to do the following from the VIRTUAL BADGE app:

- Press the + button
- Line up the personal QR code, contained in the email (lining up the PC monitor or a print-out of the email, for example)

If, on the other hand, you have access to the email directly from your phone, simply press on the attached file; the phone (depending on the system settings) asks which app you want to use to open it. You must then select VIRTUAL BADGE.

In both methods, a new virtual badge is obtained in the master list, which shows the summary structure information and the validity dates of the badge.



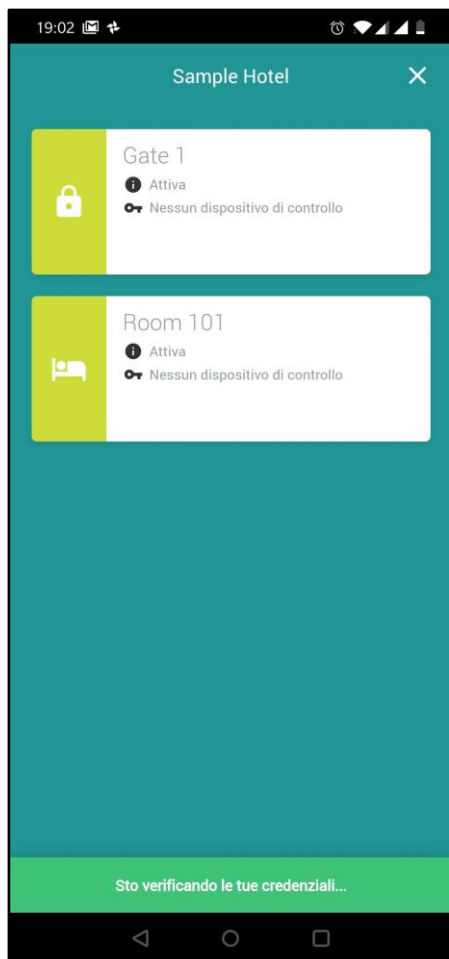
Green indicates that you can already access the application and perform the operations related to the assigned room (QR reading and object command).

Other badge colours can be:

- red: if the user is not authorised to interact with the room at that given time;
- orange: if the user is about to be activated, or if he/she is out of range (if geolocation is enabled).

If the structure provides an address and phone number, they are available as shortcuts for the phone app and satellite navigation respectively.

Access to the structure



If the badge is active, you can access the structure; by pressing the virtual badge, an authentication call is made to the HORIZONE SERVER (depending on your phone settings, via the Internet or locally via WIFI, if you have obviously already accessed the structure's wireless network).

If successful, the app enables the next screen, in which the list of gates that can be opened is shown.

If the structure has only one gate to open, this step is omitted, and you proceed immediately to the next screen.

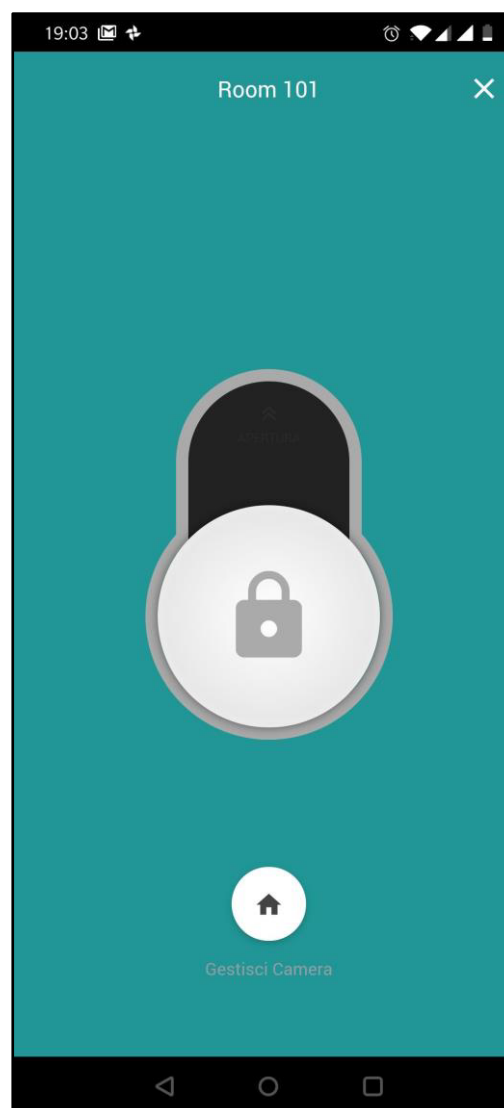
If the gate (or room) is yellow, it means that it is protected by a PIN. You will then need to enter the numerical code received in the welcome email, in order to open it.

Conversely, if the gate is green, it can be opened without further validation steps.

Once the gate has been selected, the app displays a screen in which there is a *widget* representing the lock, in the centre of the screen. At the top is the name of the gate you are about to open.

If the gate is not protected by a PIN, the lock opens immediately; if not, you will be asked to enter the personal identification code, received by email (or in the welcome print handed to you at the reception).

If you have selected your room and the structure has enabled in-room automation management, the corresponding button is available at the bottom; pressing it loads the room management graphics, as shown previously.



REVISIONS

DATE	REFERENCE	COMMENTS
04/03/2020	IN00B02WEBFI00060134	

OPEN SOURCE

HORIZONE SERVER contains open source software, such as the Linux operating system, and its kernel. These software components are subject to several 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>

For further information, please contact Eelectron customer service.

Copyright 2020 Eelectron SpA
All rights reserved
<http://www.eelectron.com>