



**IP-INTEGRA ACCESS CONTROL  
USER MANUAL  
V1.15.48**

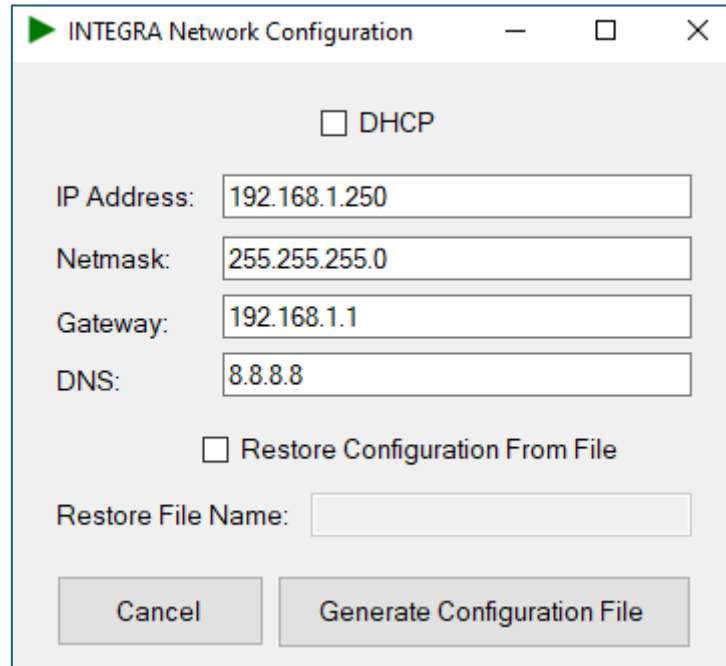
# Contents

1.	Product Setup .....	3
2.	Log in and Dashboard .....	4
2.1	Remote Support.....	5
3.	My Profile .....	6
4.	Accounts .....	7
5.	Mobile devices .....	10
6.	Cards.....	12
7.	Groups.....	13
8.	Devices.....	14
9.	Scheduler .....	21
10.	Elevator Control Module (ECM) .....	22
11.	Zones.....	30
12.	Access Times .....	31
13.	Access Rules.....	32
14.	Logs.....	33
15.	Settings.....	34
15.1	Cluster Settings .....	35
15.2	Signal Settings .....	36
15.3	Backup Settings .....	37
15.4	Network Settings.....	38
15.5	System Settings .....	39
15.6	Email Settings .....	40
15.7	Date and Time Settings.....	41
15.8	Holiday Settings.....	42
15.9	Upload License .....	43
15.10	Web Relay Settings.....	44
15.11	Self Diagnostic Settings.....	45
15.12	Monitoring Settings .....	45
15.13	Factory Reset.....	46
15.14	System Upgrade.....	46
15.15	Remote Button.....	47
15.16	iLOQ Settings.....	48
16.	System.....	49

## 1. Product Setup

**IP Address** can be configured using the **IP-INTEGRA Network Configurator**. This tool and instructions on how to use it are available on [www.ip-integra.com](http://www.ip-integra.com) webpage.

If the address is assigned by DHCP, then the tool can be used to scan the network and display the ACC controllers assigned IP address.



The image shows a screenshot of a software window titled "INTEGRA Network Configuration". The window has a standard Windows-style title bar with a green play button icon on the left and minimize, maximize, and close buttons on the right. The main content area is light gray and contains the following elements:

- A checkbox labeled "DHCP" which is currently unchecked.
- Four text input fields, each with a label to its left:
  - "IP Address:" with the value "192.168.1.250"
  - "Netmask:" with the value "255.255.255.0"
  - "Gateway:" with the value "192.168.1.1"
  - "DNS:" with the value "8.8.8.8"
- A checkbox labeled "Restore Configuration From File" which is currently unchecked.
- A text input field labeled "Restore File Name:" which is currently empty.
- Two buttons at the bottom: "Cancel" on the left and "Generate Configuration File" on the right.

Picture 1 IP Address Configuration

## 2. Log in and Dashboard

Enter **IP Address** that you configured in Integra Network Configurator. You will be prompted to enter a **Username** and **Password** (Picture 2 Login Page). It is strongly recommended to change the default credentials to a more complex one.

Default username: sysadmin

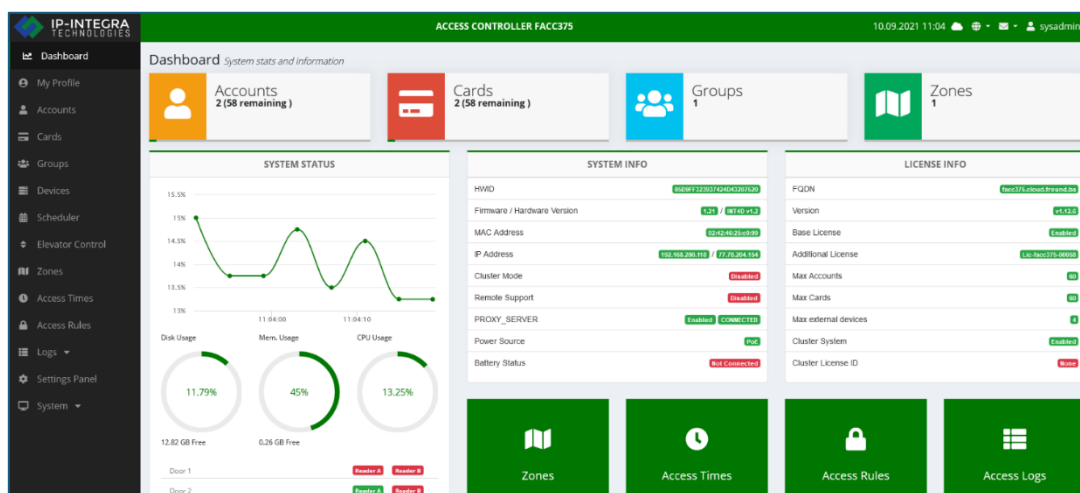
Default password: sysadmin



Picture 2 Login Page

After clicking the **Submit** button, the **Web interface** of the FREUND ACC server will open.

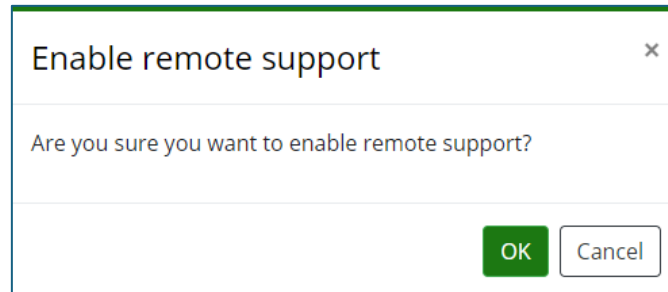
**Dashboard** is shown on Picture 3. On the left side of the Dashboard is the **Menu** that contains the following sections: **Dashboard, My Profile, Users, Cards, Groups, Devices, Zones, Access Time, Access Rules, Logs, Settings** and **System**. The right side of the Dashboard provides an overview of the **System Status - Disk Usage, Memory Usage, CPU Usage, System info, License info** and shortcuts for **Zones, Access Times, Access Rules** and **Access Logs**.



Picture 3 Dashboard

## 2.1 Remote Support

Under the **System info** within the Dashboard (Picture 3), **Remote support** is **disabled** by default. **Clicking 'Disabled'** will give user a prompt to enable Remote support (Picture 4). This option is only provided in the Dashboard.



Picture 4 Remote Support

NOTE: Service “**Remote Support**” requires your firewall settings not to forbid router communication on port 22.

In the upper right corner of the web interface, the user can change the language of the system and check for notifications.




Name	Icon	Function
Translation		Changes the language of the system
Notifications		Shows if there is a new firmware update available

Table 1

### 3. My Profile





This section shows information of the user that is currently logged in the system. Clicking on „**Generate new**“ will generate a new PIN code that the user can use for opening doors. Access log shows a list of actions done by that user (Picture 5). There are four types of System Access Levels: System Administrator, Administrator, Manager and User. All four will be explained in the next section.

My Profile *Overview of your profile information*


 **System Administrator** System Administrator  
✉ sysadmin@ip-integra.com  
🔑 0000 [Generate new](#)

**1** Groups

Access Log [Export CSV](#)

06.01.2020 00:00  06.02.2020 23:59  Show all  INT4D-207525 (Master) 

No Logs found for selected filters.

Show 10  [Clear logs](#) 1

Picture 5 My Profile Page

## 4. Accounts

Accounts tab within Menu lists all users and allows creating new accounts (Picture 6).

#	Name	Email	Username	Created at	Active from	Expires at	Groups	Description	Enabled	Account type	PIN	Actions
1	System Administrator	sysadmin@ip-integra.com	sysadmin	21-01-2021	Always	Never	Default Group X	-	System Administrator	System Administrator	Show PIN	[Edit] [Send Email] [Reset Password] [Reset PIN] [Assign Group] [Delete]
2	Hamdija	hr@freund.ba	hamdija	21-01-2021	Always	Never	Default Group X	-	System Administrator	System Administrator	Show PIN	[Edit] [Send Email] [Reset Password] [Reset PIN] [Assign Group] [Delete]
3	Integra Access	do@freund.ba	IOS	22-01-2021	22-01-2021	Never	Default Group X	-	User	User	Show PIN	[Edit] [Send Email] [Reset Password] [Reset PIN] [Assign Group] [Delete]
4	Enis	eg@freund.ba	enis.gegic	25-01-2021	25-01-2021	Never	Default Group X	-	User	User	Show PIN	[Edit] [Send Email] [Reset Password] [Reset PIN] [Assign Group] [Delete]
5	Integra Access	do@freund.ba	Android	25-01-2021	25-01-2021	Never	Default Group X	-	User	User	Show PIN	[Edit] [Send Email] [Reset Password] [Reset PIN] [Assign Group] [Delete]
6	Ariel	ab@freund.ba	ab	05-02-2021	Always	Never	Default Group X	-	System Administrator	System Administrator	Show PIN	[Edit] [Send Email] [Reset Password] [Reset PIN] [Assign Group] [Delete]
7	Anel Android	None	ab2	05-02-2021	05-02-2021	Never	Default Group X	-	User	User	Show PIN	[Edit] [Send Email] [Reset Password] [Reset PIN] [Assign Group] [Delete]
8	Enis Adnroid	freunddoo@gmail.com	enis.android	15-02-2021	15-02-2021	Never	Default Group X	-	User	User	Show PIN	[Edit] [Send Email] [Reset Password] [Reset PIN] [Assign Group] [Delete]
9	Alem Kozic	alem.kozic@hotmail.com	Alem	18-02-2021	Always	Never	Default Group X	-	System Administrator	System Administrator	Show PIN	[Edit] [Send Email] [Reset Password] [Reset PIN] [Assign Group] [Delete]

Picture 6 Accounts Page

Under the Actions column, the following options are available:

Name	Icon	Function
Edit user		Opens form which enables changing account data.
Send welcome email		Sends app activation instruction to user email address
Reset password		Reset log-in password for selected account
Reset PIN		Reset Door Access PIN-code for selected user
Assign account group		Add or remove groups for Account
Delete Account		Permanently Delete Account

Table 2

Clicking on **Add new** opens a form for adding a new account (Picture 7). Each account is defined by its **username**, **full name**, **phone**, **type** and **password**. Features of the **four user types** are listed in the table below:

Account type	Rights
System admin	Edit and view everything
Admin	Edit: Accounts, Cards, Groups, Doors, Zones, Access Times, Access Rules
Manager	Can edit: Accounts, Cards, Groups Can view: Doors, Zones, Access Times, Access Rules
User	Can only see own profile

Table 3

Each user account can have one or multiple own cards. Clicking on **Add** opens a form for manually adding a card to an account, by entering a card number (Picture 8). “**Active from**” and “**Expires at**” allows selection of time range in which account will be active. Account is labeled as Expired when expiration date has been reached.

**Accounts** *Accounts control panel*

**Add new account**

**Account information**

Full name

Username

Home Address

Password  
 **Generate**  
Leave empty to autogenerate password.

Phone  SIP Extension **None**

Type

Active from  Expires at

**Accounts image**  
 No image uploaded.  
**Select File**

**Description**

**Cards** **Add** **Scan**

#	Number	Color	Enabled	Actions
No cards found.				

**Groups** **Add**

#	Name	Actions
No groups found.		

Picture 7 Creating New Account Form


**Add new card** ×

**Save Changes** **Cancel**

Picture 8 Manually Adding New Card

Another way of assigning a card to an account is by **scanning** it (Picture 9). This requires a **USB RFID reader**. Once the card is scanned twice, it is automatically assigned to the account.

### Add new card

🔄 Scan Card	Scan your card 
🔄 Scan Again	
🔄 Done	

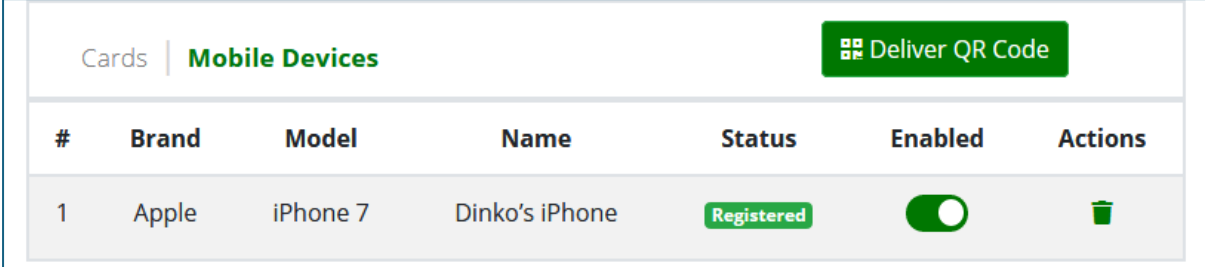
[Save Changes](#) [Cancel](#)

Picture 9 Automatic Adding New Card

## 5. Mobile devices

The IP-INTEGRA Access Control system supports the use of mobile devices with the **IP-INTEGRA Access** mobile app (Picture 10). The app is available on Apple Store and Google Play Store.

To use our Mobile app, we need to add your mobile device into the system. Adding device is accomplished by using a QR code that is delivered with the **'Welcome e-mail'**. Send Welcome e-mail button is explained in [Accounts](#) section, table 2.

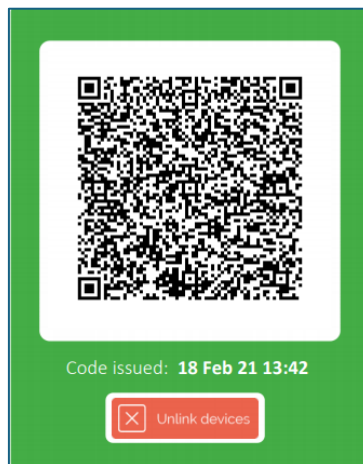


#	Brand	Model	Name	Status	Enabled	Actions
1	Apple	iPhone 7	Dinko's iPhone	Registered	<input checked="" type="checkbox"/>	

Picture 10 Mobile Device Management

QR code will arrive in the e-mail attached as a .pdf file. Once you have the app installed and running, open the .pdf and scan the QR code shown in Picture 11 with your **IP-INTEGRA Access** mobile application.

User manual for the IP-INTEGRA Access app is available on [www.ip-integra.com](http://www.ip-integra.com) webpage.



Picture 11 Mobile app Activation QR Code

You can use the 'Unlink devices' button under the QR code to disable any devices connected to the system (in case of losing access to your mobile device).

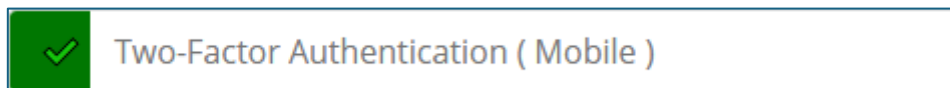
Once the code is scanned you will be able to use the IP-INTEGRA application. If administrator enables a two-factor authentication, users will be required to input a six-digit code that will be delivered to their e-mail address (Picture 12).



Picture 12 2FA Code

Once the code is entered, you will be able to use IP-INTEGRA Access application. For instructions on using the IP-INTEGRA Access you can consult the User manual for the application.

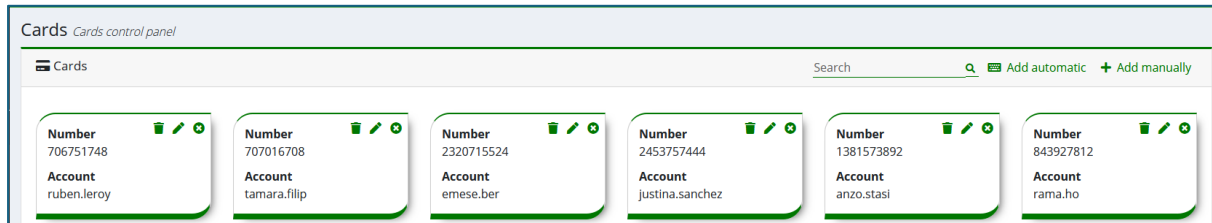
Enable or disable 2FA, you need to navigate to '**Settings - System Settings**' panel and click the button shown in Picture 13.



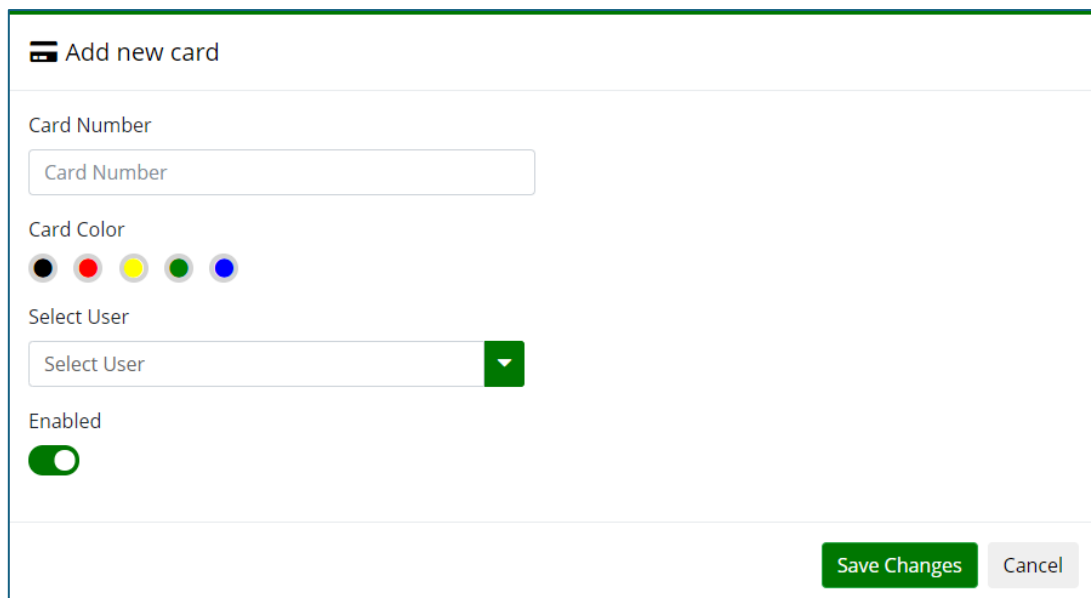
Picture 13 Enable/Disable 2FA

## 6. Cards

**Cards** section (Picture 14) gives an overview of all cards that are registered in the system and gives information about the card numbers and their users. Clicking on the **Edit** button opens a form for changing the card number and the assigned account (Picture 15).



Picture 14 Cards Control Panel













The screenshot shows a form titled "Add new card". It contains the following fields and controls:

- Card Number:** A text input field with the placeholder "Card Number".
- Card Color:** Five colored circles (black, red, yellow, green, blue) for selection.
- Select User:** A dropdown menu with the placeholder "Select User" and a green arrow icon.
- Enabled:** A toggle switch that is currently turned on (green).
- Buttons:** "Save Changes" (green) and "Cancel" (grey) buttons at the bottom right.

Picture 15 Add/Edit Card

## 7. Groups

**Groups** section (Picture 16) lists all groups in the system, to which users can be assigned to. Groups are used in **Access rules**, which will be explained in Access Rules section. Clicking on **Add new** opens a form for creating a new group (Picture 17). Under **Actions** column the following options are available: **Edit group**, **Edit group members** and **Delete group**.

Group <i>Groups control panel</i>			
Groups		Search	+ Add new
#	Name	Accounts	Actions
1	Default Group	<span>sysadmin</span> ✕	 
2	Full access	<span>daniel.nicolosi.ceo</span> ✕	  
3	Employees	<span>joel.lau</span> ✕ <span>rut.dever</span> ✕ <span>priya.hlav</span> ✕ <span>emese.ber</span> ✕ <span>dimitri.stef</span> ✕ <span>justina.sanchez</span> ✕ <span>alberta.iliev</span> ✕ <span>anzo.stasi</span> ✕ <span>rama.ho</span> ✕ <span>danny.shea</span> ✕ <span>stephen.mcafee</span> ✕ <span>cari.salvatici</span> ✕ <span>tamsyn.simonson</span> ✕ <span>mehrab.kir</span> ✕ <span>judith.te</span> ✕	  
4	Sales	<span>joel.lau</span> ✕ <span>rut.dever</span> ✕ <span>agus.dreir</span> ✕ <span>justina.sanchez</span> ✕ <span>alberta.iliev</span> ✕ <span>anzo.stasi</span> ✕ <span>rama.ho</span> ✕ <span>danny.shea</span> ✕ <span>stephen.mcafee</span> ✕	  

Picture 16 Groups Page

### Add new group ✕

Name

Save Changes Cancel

Picture 17 Add New Group

## 8. Devices

The **Devices** section lists all available devices for configuring, with information about doors and zones that are assigned to them. Each device name can be edited by clicking on the (Rename Device) icon.

Type	Device Name	Host Name	IP Address	Cluster Info	Version	Doors	Status	Actions																																															
Master Controller	facc782	192.168.200.111 109.165.233.173	Toggle test 65 M	v1.15.48	Door 0, Door 1, Door 2, Door 3	OK	[Edit] [Refresh]																																																
Slave - Elevator Module	facc1338	192.168.200.104 109.165.233.173	Toggle test 65 S	v1.15.48	Floor - 1, Floor - 2, Floor - 3, Floor - 4	OK	[Refresh] [Edit] [Settings]																																																
		<table border="1"> <thead> <tr> <th rowspan="2">Door</th> <th rowspan="2">Power</th> <th colspan="2">Reader A</th> <th colspan="2">Reader B</th> <th rowspan="2">Zones</th> <th rowspan="2">Actions</th> </tr> <tr> <th>Type</th> <th>Keypad</th> <th>Tamper</th> <th>Type</th> <th>Keypad</th> <th>Tamper</th> </tr> </thead> <tbody> <tr> <td>Floor - 1</td> <td>✓</td> <td>Wiegand 34</td> <td>✗</td> <td>✗</td> <td>Wiegand 34</td> <td>✗</td> <td>✗</td> <td>Default Zone X [Edit] [Refresh] [Open] [Test] [Reset] [Remove] [Substitute]</td> </tr> <tr> <td>Floor - 2</td> <td>✓</td> <td>Wiegand 34</td> <td>✗</td> <td>✗</td> <td>Wiegand 34</td> <td>✗</td> <td>✗</td> <td>Default Zone X [Edit] [Refresh] [Open] [Test] [Reset] [Remove] [Substitute]</td> </tr> <tr> <td>Floor - 3</td> <td>✓</td> <td>Wiegand 34</td> <td>✗</td> <td>✗</td> <td>Wiegand 34</td> <td>✗</td> <td>✗</td> <td>Default Zone X [Edit] [Refresh] [Open] [Test] [Reset] [Remove] [Substitute]</td> </tr> <tr> <td>Floor - 4</td> <td>✓</td> <td>Wiegand 34</td> <td>✗</td> <td>✗</td> <td>Wiegand 34</td> <td>✗</td> <td>✗</td> <td>Default Zone X [Edit] [Refresh] [Open] [Test] [Reset] [Remove] [Substitute]</td> </tr> </tbody> </table>		Door	Power	Reader A		Reader B		Zones	Actions	Type	Keypad	Tamper	Type	Keypad	Tamper	Floor - 1	✓	Wiegand 34	✗	✗	Wiegand 34	✗	✗	Default Zone X [Edit] [Refresh] [Open] [Test] [Reset] [Remove] [Substitute]	Floor - 2	✓	Wiegand 34	✗	✗	Wiegand 34	✗	✗	Default Zone X [Edit] [Refresh] [Open] [Test] [Reset] [Remove] [Substitute]	Floor - 3	✓	Wiegand 34	✗	✗	Wiegand 34	✗	✗	Default Zone X [Edit] [Refresh] [Open] [Test] [Reset] [Remove] [Substitute]	Floor - 4	✓	Wiegand 34	✗	✗	Wiegand 34	✗	✗	Default Zone X [Edit] [Refresh] [Open] [Test] [Reset] [Remove] [Substitute]		
Door	Power	Reader A				Reader B		Zones	Actions																																														
		Type	Keypad	Tamper	Type	Keypad	Tamper																																																
Floor - 1	✓	Wiegand 34	✗	✗	Wiegand 34	✗	✗	Default Zone X [Edit] [Refresh] [Open] [Test] [Reset] [Remove] [Substitute]																																															
Floor - 2	✓	Wiegand 34	✗	✗	Wiegand 34	✗	✗	Default Zone X [Edit] [Refresh] [Open] [Test] [Reset] [Remove] [Substitute]																																															
Floor - 3	✓	Wiegand 34	✗	✗	Wiegand 34	✗	✗	Default Zone X [Edit] [Refresh] [Open] [Test] [Reset] [Remove] [Substitute]																																															
Floor - 4	✓	Wiegand 34	✗	✗	Wiegand 34	✗	✗	Default Zone X [Edit] [Refresh] [Open] [Test] [Reset] [Remove] [Substitute]																																															

Picture 18 Devices

Name	Icon	Function
Edit door		Edit name, power status, readers, etc.
Assign zones		Add or remove zones to the door
Open door		Open the door through Access Control System
Test door		Checks if the doors are connected
Reset door		Resets the door to default values
Remove from cluster		Removes the device from the cluster
Substitute		In case a controller fails, it gives option to select a replacement controller*

Table 4

In Devices section (Picture 18) are listed information of all devices that are in cluster. Clicking on Scan Devices opens a window and shows Stand Alone devices which can be added to cluster as Slave devices by clicking on icon while clicking on removes device from cluster.

\*Available in Cluster mode only. For replacement controller to show up in web interface, it must be powered on and connected to the network.

Master Controllers set up in Cluster Mode will have another button available – Additional Device Config. Clicking on this icon brings up following window:

Device Additional Config

Enable Support

Enable Web Relay

Web Relay Secret

5678

Disable Log

Web Relay 1 Open Time

3000

Web Relay 2 Open Time

3001

Web Relay 3 Open Time

3002

Web Relay 4 Open Time

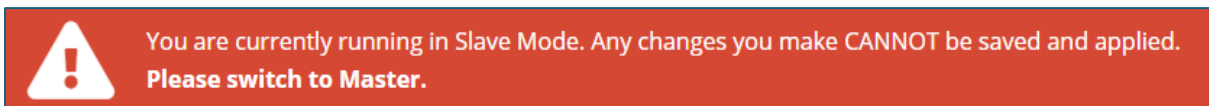
3003

Save Changes Cancel

Picture 19 Device Additional Configuration

This window allows you to control certain options on Slave Controllers: **enable** or **disable Remote Support**, enable or disable **web relays** on Slave controllers, **disable Logging** of Web Relay actions and **regulate Web Relay timers**.

NOTE: Slave device's settings are configured on Master Controller. No settings can be changed from Slave controller.



Picture 20 Slave Device Warning

Clicking on **Add external device** will open a form for adding device which has RFID reader hardware, and it can be added as reader, either manually (Picture 21) or from network (Picture 22).

The screenshot shows a web form titled "Add external device" with a close button (x) in the top right corner. At the top, there are two tabs: "Manual" (selected) and "From Network". The form contains several input fields and a dropdown menu:

- Type:** A dropdown menu with "FE-IPDS-20" selected.
- Name:** A text input field with "Device Name" as a placeholder.
- IP Address:** A text input field with "Device IP Address" as a placeholder.
- Hardware ID:** A text input field with "Device Hardware ID" as a placeholder.
- Username:** A text input field with "Device Username" as a placeholder.
- Password:** A text input field with "Device Password" as a placeholder.
- Zones:** A button labeled "Default Zone".

A green "Save Changes" button is located at the bottom right of the form.

Picture 21 Adding External Device Manually

The screenshot shows the "Add external device" form in "From Network" mode. The "From Network" tab is selected. Below the tabs is a table listing five discovered devices. Each row contains a device ID, name, IP address, MAC address, and a green arrow icon pointing right.

ID	Name	IP Address	MAC Address	Action
1	FE-IPDS-29S	192.168.200.158	0C:11:05:05:A7:80	➔
2	FE-IPDS-20	192.168.200.113	0C:11:05:06:25:6B	➔
3	FE-IPDS-20	192.168.200.121	0C:11:05:09:71:91	➔
4	FE-IPDS-28A	192.168.200.114	0C:11:05:09:E7:D7	➔
5	FE-IPDS-26B	192.168.200.125	0C:11:05:0A:A9:E4	➔

Picture 22 Adding External Device from Network






Section	Description
Device Name	Name of the Device, it can be changed by clicking on  under <b>Actions</b> column
IP Address	IP address of device
Cluster Info	Gives information in which cluster is device, and their position <b>M</b> – Master, <b>S</b> - Slave, <b>SA</b> -Stand Alone  - Input 1/2 Active
Version	Version of software
Doors	Gives information about readers that are connected to doors. Since each door can have two readers they are labeled as  . Green color – reader is connected; Red color – reader is not connected  - Door Open indicator  - Door Closed indicator
Status	<b>OK</b> – device is working properly, <b>Pending</b> – device is doing some process before it can send or receive information, <b>Failed</b> – device is not working

Table 5

Clicking on **dropdown arrow**  opens a **list of Doors**. Two readers can be connected to one door from each side or, one reader and one exit button. Clicking on  opens a form for editing door configuration (Picture 23).

Section	Description
Type	Reader type: Wiegand 26, Wiegand 34, OSDP and No reader (not connected).
Keypad	Enable this option when connecting readers with a Keypad
Floor Mode	This option will automatically be enabled when the Elevator Control Module is used.
W26	When connecting <b>Fermax Wiegand 26 readers</b> this option must be enabled(read format conversion)
HID	Support for HID readers
Toggle Mode	If enabled, when card is scanned, door will <b>toggle open</b> or <b>toggle close</b> .
Combine Readers	(Card + PIN only) Card scan input on reader A; PIN input(keypad) on reader B.
Tamper	Enable tamper protection
HTTP Action	Ability to trigger up to 2 HTTP links when ACC relay is triggered
Relay open time	Determine how long the relay will stay open
Pin Input Timeout	Determines the time duration for PIN entry(Keypad)
Door Not Closed Timeout (DNC)	Duration of DNC alarm

Table 6

**Edit door**
✕

---

Description

Door 1

Power Status

Floor Mode

Snapshots

W26

HID

Combine Reader

Readers	Type	Keypad	Tamper
Reader A	Wiegand 34	<input type="checkbox"/>	<input type="checkbox"/>
Reader B	Wiegand 34	<input type="checkbox"/>	<input type="checkbox"/>

Relay open time: 3000

Pin Input Timeout: 5000

Button On Threshold: 100

Door Not Closed Alert:

Door Not Closed Timeout: 10000

HTTP Action Enabled:

**Picture 23 Edit Door**

In Reader B drop down menu, you can select “Exit Button” option if you want to have an Exit button connected to the ACC module (Picture 24).

Readers	Type	Keypad	Tamper
Reader A	Wiegand 34	<input type="checkbox"/>	<input type="checkbox"/>
Reader B	Exit Button	<input type="checkbox"/>	<input type="checkbox"/>

Relay open time: 2111

Pin Input Timeout: 5000

Button On Threshold:

Door Not Closed Alert:

Door Not Closed Timeout: 10000

**Picture 24 Exit Button Configuration**

**Edit door's zones**
✕

---

Unassigned zones

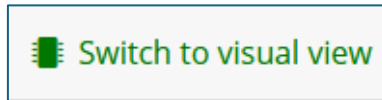
- DefaultZone +
- IT Center +
- IT Center + Server Room +
- Sales Dept. +
- Storage Room +
- Conference Room +
- Management Dept. +

Assigned zones

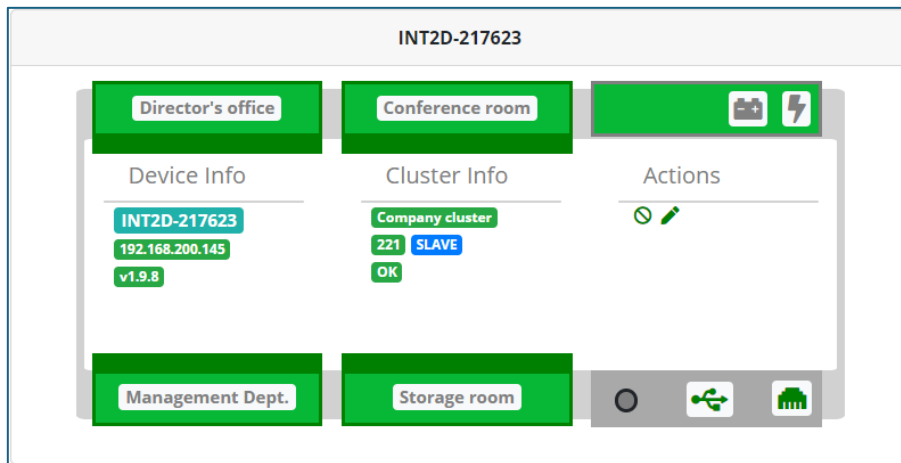
- Main Entrance
- Full Access

**Picture 25 Assigning Zones**

In the right upper corner, the user can switch from the default table view to visual view, by clicking on a button shown in Picture 26. An example of a single device in visual view is presented in Picture 27.

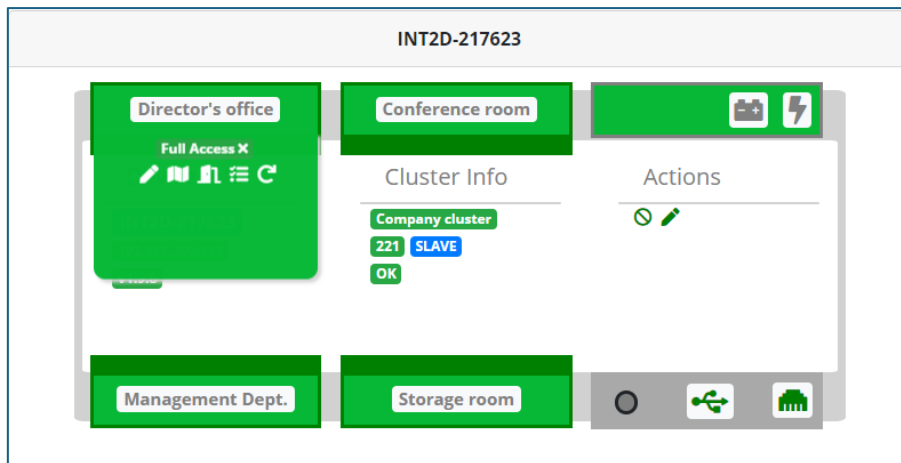


Picture 26 Visual View Button



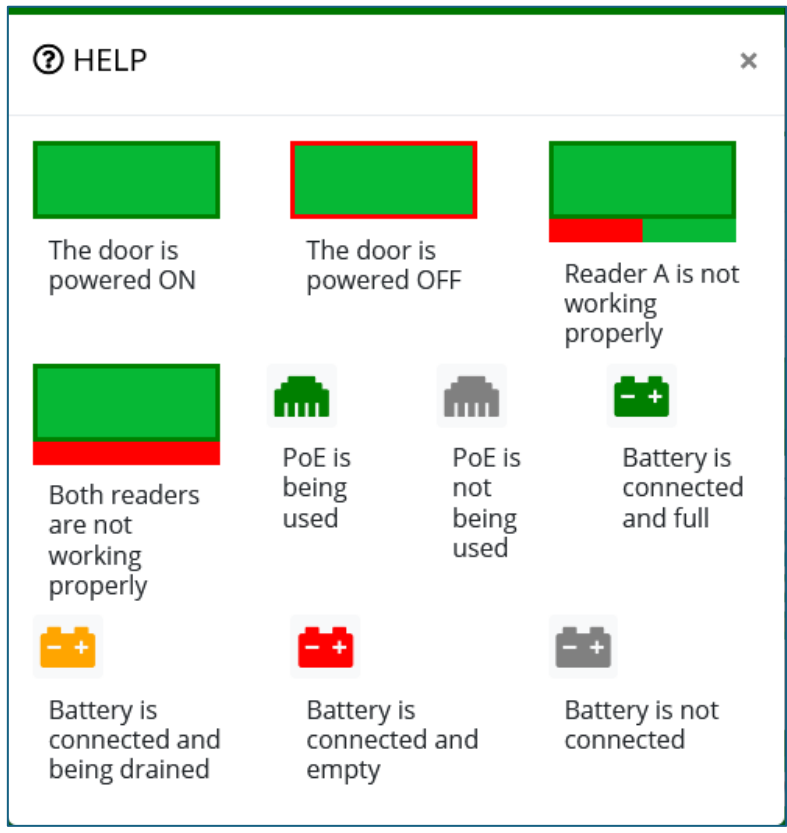
Picture 27 Standalone Device in Visual View

To see the defined zones for each door in visual view, hover over the door name. A list of zones and editing options will appear, as shown in Picture 28.



Picture 28 Zones List in Visual View

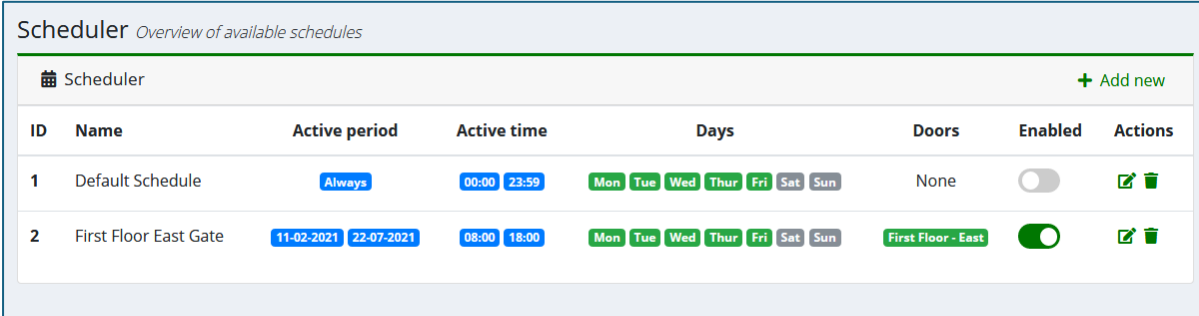
For an easier understanding, next to the view button, the user can find a help button which explains the state of the device components, as shown in Picture 29.



Picture 29 Icons Explained

## 9. Scheduler

The **Scheduler** feature is used to assign doors to remain open for the specified period of time. You can specify the time of day and the day of the week. In Picture 30 you can see an example of the scheduler panel.



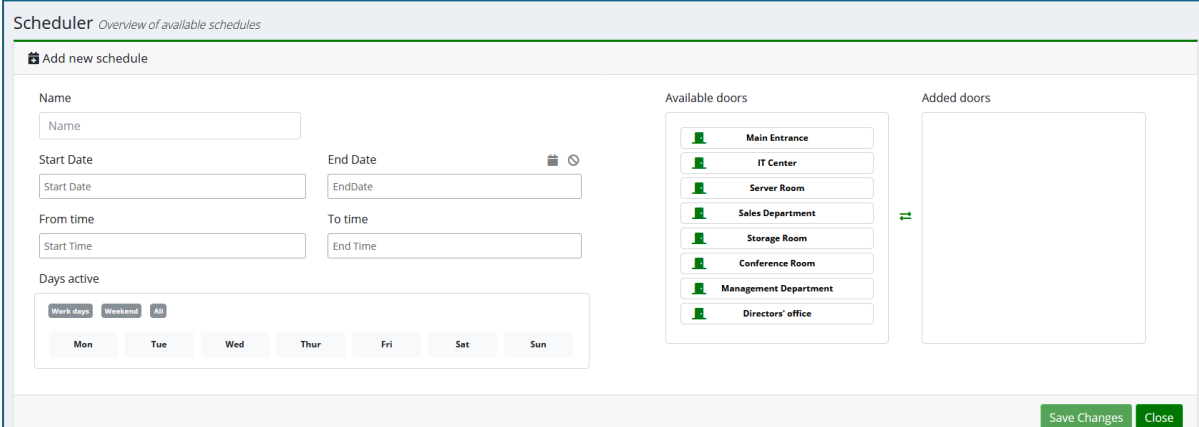
Scheduler *Overview of available schedules*

Scheduler + Add new

ID	Name	Active period	Active time	Days	Doors	Enabled	Actions
1	Default Schedule	Always	00:00 23:59	Mon Tue Wed Thur Fri Sat Sun	None	<input type="checkbox"/>	
2	First Floor East Gate	11-02-2021 22-07-2021	08:00 18:00	Mon Tue Wed Thur Fri Sat Sun	First Floor - East	<input checked="" type="checkbox"/>	

Picture 30 Scheduler

By clicking Add new, a form to add new Schedule will open. The form will allow you to create a schedule to your preferences. The form is shown in Picture 31.



Scheduler *Overview of available schedules*

Add new schedule

Name

Start Date  End Date

From time  To time

Days active  
 Work days  Weekend  All

Mon Tue Wed Thur Fri Sat Sun

Available doors

- Main Entrance
- IT Center
- Server Room
- Sales Department
- Storage Room
- Conference Room
- Management Department
- Directors' office

Added doors

Picture 31 Adding New Schedule

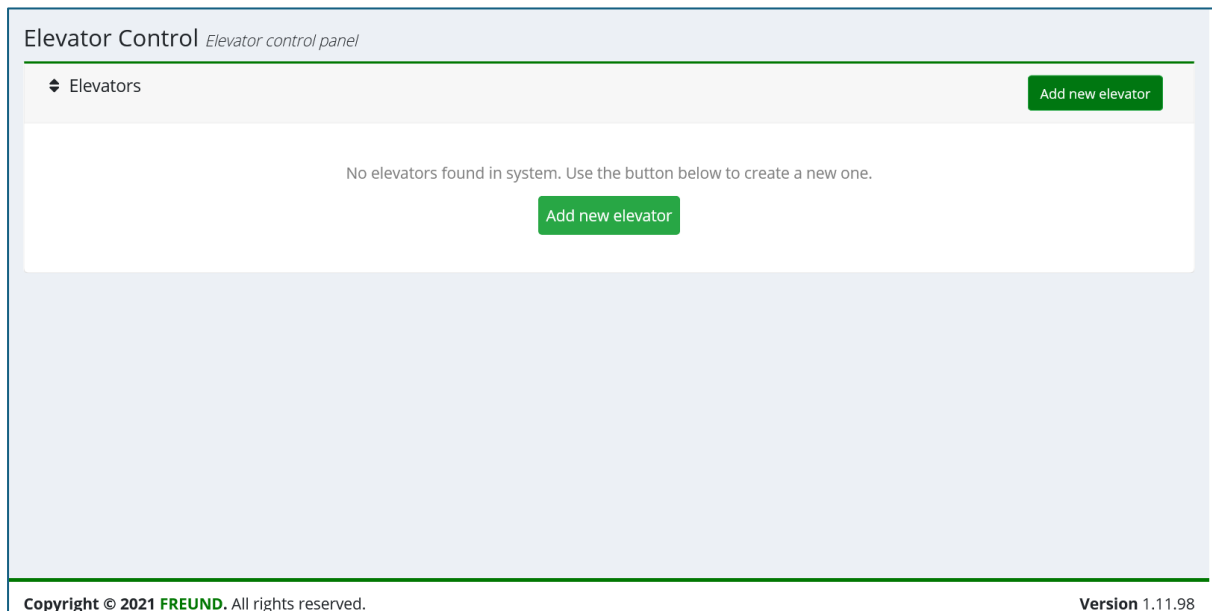
On the left side, you can name the scheduler along with setting its start and end dates/times. On the bottom of the left side, you must select the weekdays during which you want the scheduler to be active. The buttons on the end date allow you to clear the input field or set the end date as 'Never'.

On the right side, you select the doors to which the scheduler will apply. All these settings can be changed later by pressing the 'Edit' Button on the Scheduler panel.

Once you are finished click the 'Save changes' button to commit your changes to the system.

## 10. Elevator Control Module (ECM)

Elevator Control Module (Picture 32) introduces an access control ability to the elevator. Through correct configuration, you can designate which users can gain access to which floors and at what time.



Picture 32 Elevator Control Panel

Click on „**Add new elevator**“ button shown in the Picture 33 and fill out the required fields.

Note: „**Relay open time**“ field determines a period of time during which user can choose the wanted floor after scanning his card.

Click on „Save Changes“ button to finish adding the elevator.

**Add elevator** [x]

Name  
Main Hall elevator

Description  
Elevator located in the main hall of the hotel.

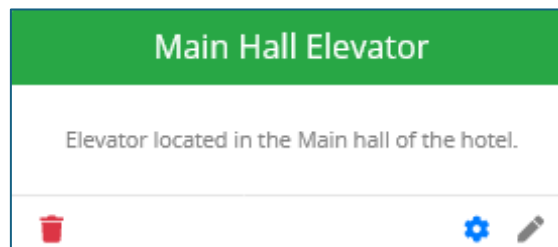
Enabled

Relay open time (ms)  
10000

Cancel Save Changes

**Picture 33 Adding New Elevator**

Your Elevator Control Panel should show the added elevator:

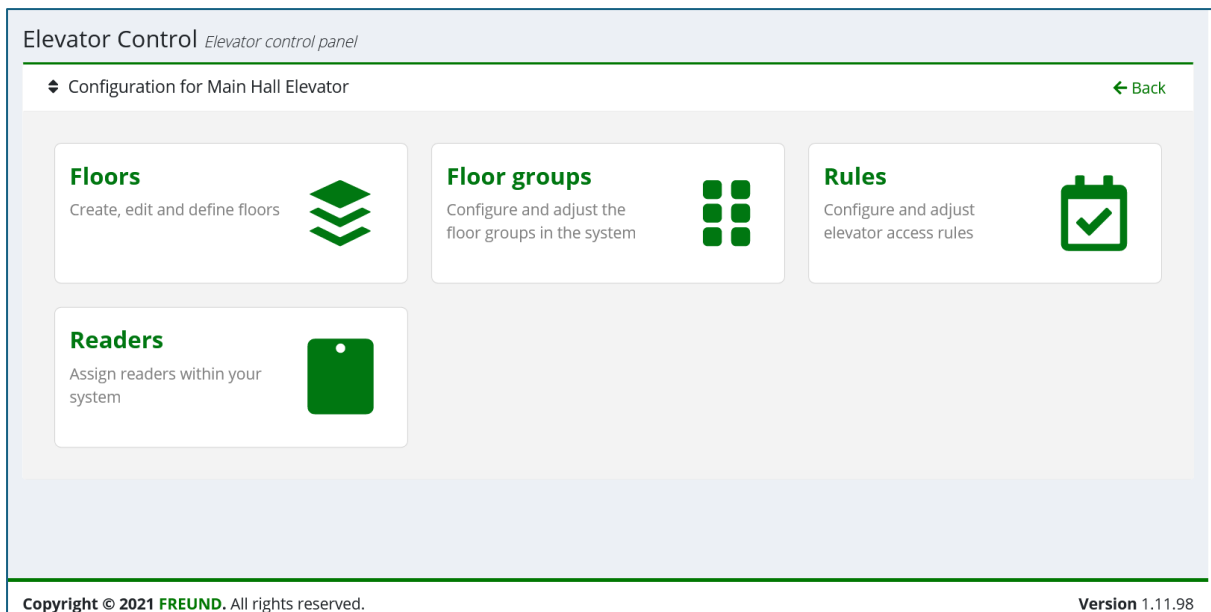


**Picture 34 Created Elevator**

Following icons allow you to Delete, Configure or Edit the elevator, respectively:

Since we want to configure the Elevator, go ahead and click on the blue wheel.

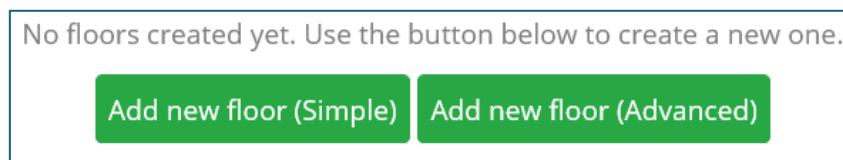
Following screen will show:



**Picture 35 Elevator Configuration**

As shown in Picture 35, we have 4 buttons appearing in front of us: Floors, Floor groups, Rules and Readers. These allow us to define which user groups can go to which floor and at what time.

Next thing we need to do is add floors accessible by an elevator. To do that, we are clicking on Floors button shown in Picture 35. Following screen will appear:



**Picture 36 Add New Floor Buttons**

Add floor to elevator
✕

Name

Floor number

Select door

Create own group

Create user group

SELECT\_FLOOR\_GROUPS

Groups

Cancel

Add new floor

Picture 37 Add New Floor Advanced

Simple floor creation
✕

Name

Floor number

Select door

**A notice about simple floor creation**

Using simple floor creation will automatically assign the floor to its own new group. It will assign it the default access time of the system (00h-24h). You can change every parameter of the created floor using the edit floor button on the table.

Cancel

Add new floor

Picture 38 Add New Floor Simple

As you can see, we have two ways to add the new floor. Using Simple floor creation will automatically assign the floor to its own new group. It will assign to it the default access time of the system (00h-24h).

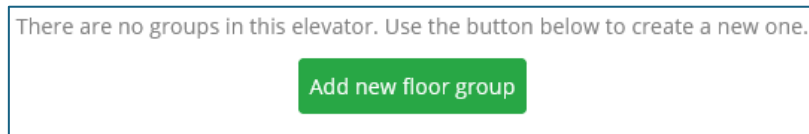
Using the following icons, the floors can be edited or deleted, respectively.

Floor configuration for Main Hall Elevator					<a href="#">+ Add new floor (Simple)</a> <a href="#">+ Add new floor (Advanced)</a> <a href="#">← Back</a>
#	Name	Device	Readers	Groups	Actions
1.	-1 Spa & Wellness	<span style="background-color: #2196F3; color: white; padding: 2px;">INT4D-195331</span>	<span style="background-color: #4CAF50; color: white; padding: 2px;">A</span> B	<span style="background-color: #4CAF50; color: white; padding: 2px;">VIP+</span> <span style="background-color: #4CAF50; color: white; padding: 2px;">VIP</span>	
2.	0 Ground floor	<span style="background-color: #2196F3; color: white; padding: 2px;">INT4D-195331</span>	A B	<span style="background-color: #4CAF50; color: white; padding: 2px;">Default</span> <span style="background-color: #4CAF50; color: white; padding: 2px;">VIP+</span> <span style="background-color: #4CAF50; color: white; padding: 2px;">VIP</span>	
3.	1 Rooms	<span style="background-color: #2196F3; color: white; padding: 2px;">INT4D-195331</span>	<span style="background-color: #4CAF50; color: white; padding: 2px;">A</span> B	<span style="background-color: #4CAF50; color: white; padding: 2px;">Default</span> <span style="background-color: #4CAF50; color: white; padding: 2px;">VIP+</span> <span style="background-color: #4CAF50; color: white; padding: 2px;">VIP</span>	
4.	2 Lounge	<span style="background-color: #2196F3; color: white; padding: 2px;">INT4D-195331</span>	A B	<span style="background-color: #4CAF50; color: white; padding: 2px;">VIP+</span>	
<span style="border: 1px solid #ccc; padding: 5px 10px; background-color: #f0f0f0;">Back</span>					

Picture 39 Floors List

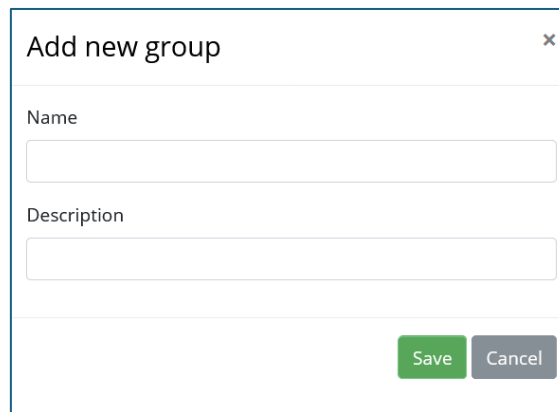
When you have added all the floors you need, click on the „Back“ button.

To proceed, we must create Floor Groups and assign created Floors to them. click on the Floor groups button(shown in Picture 35). Following screen will show:



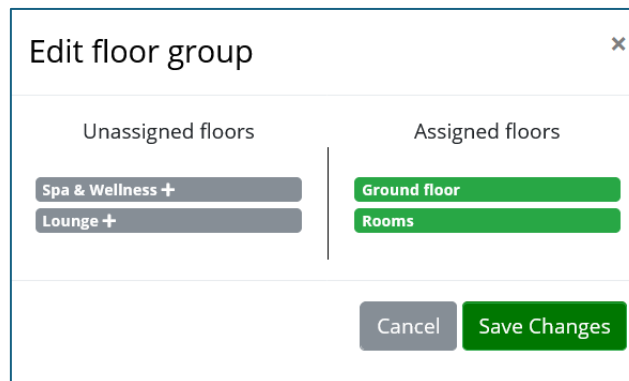
**Picture 40 Adding New Floor Group**

Click on the „Floor Groups“ button and fill out the forms shown in Picture 41.

A modal window titled "Add new group" with a close button (x) in the top right corner. It contains two text input fields: "Name" and "Description". At the bottom right, there are two buttons: a green "Save" button and a grey "Cancel" button.

**Picture 41 Group Adding Form**

Clicking on the Plus icon, we can add Floors to the Floor Group. In this way, we are assigning which User Groups have access to which floor.

A modal window titled "Edit floor group" with a close button (x) in the top right corner. It is divided into two columns: "Unassigned floors" and "Assigned floors". Under "Unassigned floors", there are two grey buttons with plus signs: "Spa & Wellness +" and "Lounge +". Under "Assigned floors", there are two green buttons: "Ground floor" and "Rooms". At the bottom, there are two buttons: a grey "Cancel" button and a green "Save Changes" button.

**Picture 42 Assigning Floor Groups**




When you have finished adding the groups needed, your Floor Groups list should look like this:

#	Name	Description	Floors	Actions
5.	Default		Ground floor Rooms	✎ + 🗑
7.	VIP+		Spa & Wellness Lounge Ground floor Rooms	✎ + 🗑
8.	VIP		Spa & Wellness Ground floor Rooms	✎ + 🗑

[Back](#)

Picture 43 Floor Groups

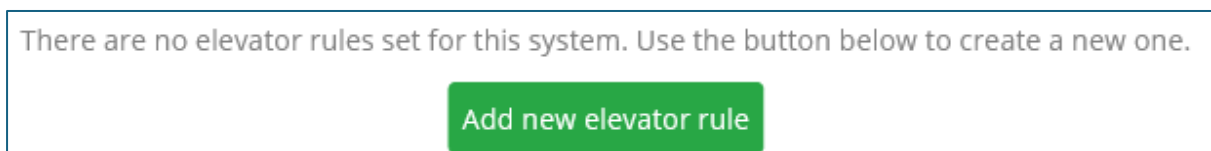
You can add as many groups as you need.

Using the following icons,    the groups can be edited, floors added, or deleted, respectively.

**NOTE: Process of creating User groups is described in [Chapter 7](#).**

When you have added all the floor groups you need, click on the „Back“ button.

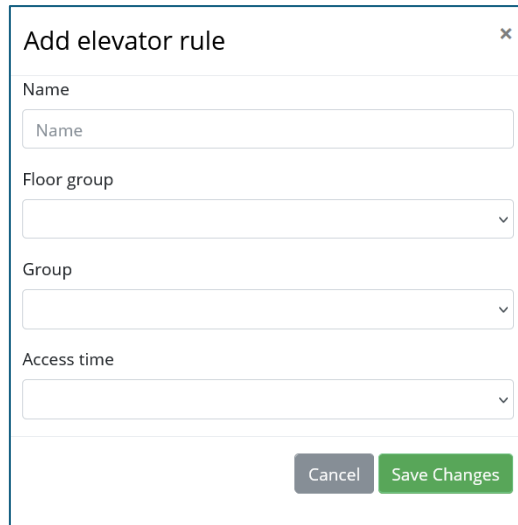
Finally, we need to add rules which will allow the Elevator Control Module to function. Click on Rules button shown in Picture 35. The following screen will show:



Picture 44 Button for Adding New Rule

Click on the „Add new elevator rule“ button and fill out the required fields shown in Picture 45.

In the following screen, you can assign a User Group to the Floor Group:



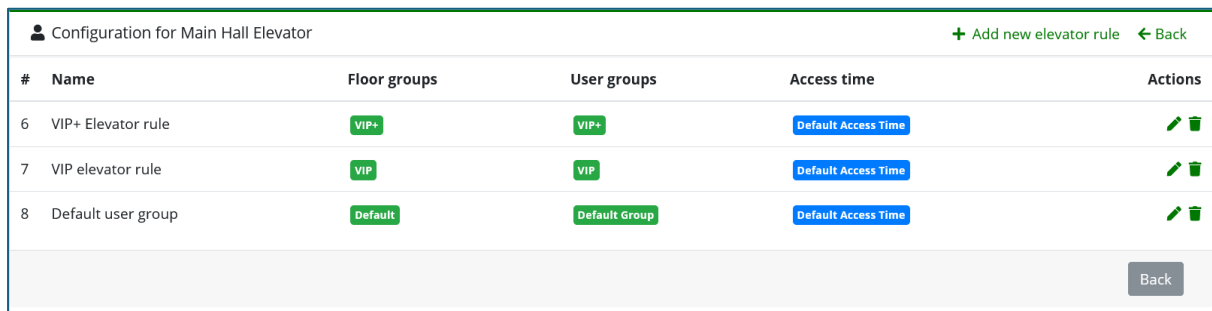
The form titled "Add elevator rule" includes the following fields:







- Name: Text input field.
- Floor group: Dropdown menu.
- Group: Dropdown menu.
- Access time: Dropdown menu.

Buttons: Cancel, Save Changes.

Picture 45 Rule Adding Form


In practice, it means that you are here defining which Users have access to which floors at which time.



#	Name	Floor groups	User groups	Access time	Actions
6	VIP+ Elevator rule	VIP+	VIP+	Default Access Time	 
7	VIP elevator rule	VIP	VIP	Default Access Time	 
8	Default user group	Default	Default Group	Default Access Time	 

Picture 46 List of Elevator Rules

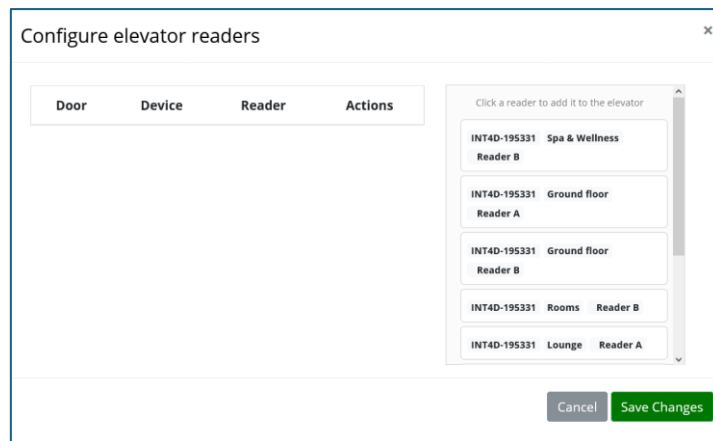
For easier tracking, we have named the Floor Groups and User Groups with same names.

Using the following icons   the floors can be edited or deleted, respectively.

When you have added all the rules you need, click on the „Back“ button.

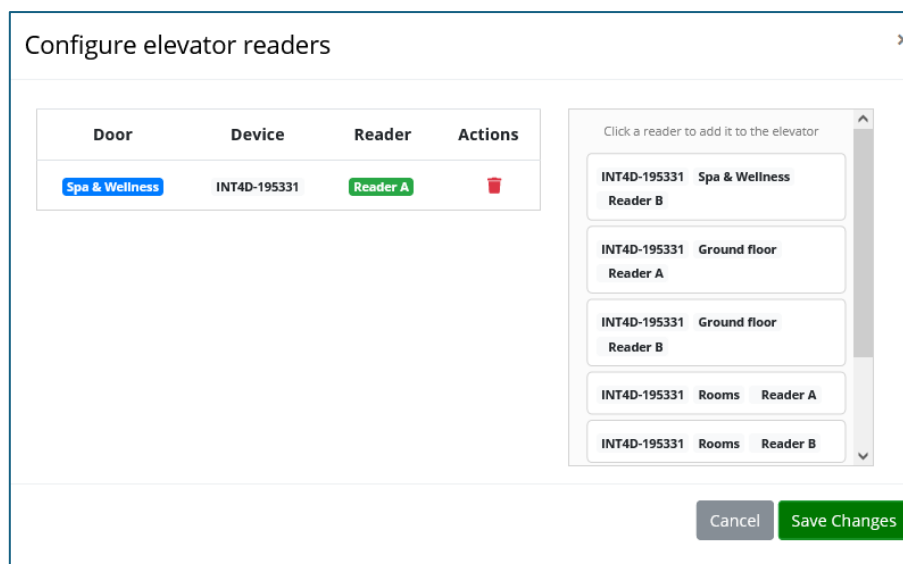
Only thing left now is to assign the reader to the elevator.

Click on Readers button shown in Picture 35. Following screen will show:



Picture 47 Assigning an Elevator Reader

We have connected an elevator reader to Relay 1 on the ACC module, which also contains the button for floor -1. Here is how it looks when configured:

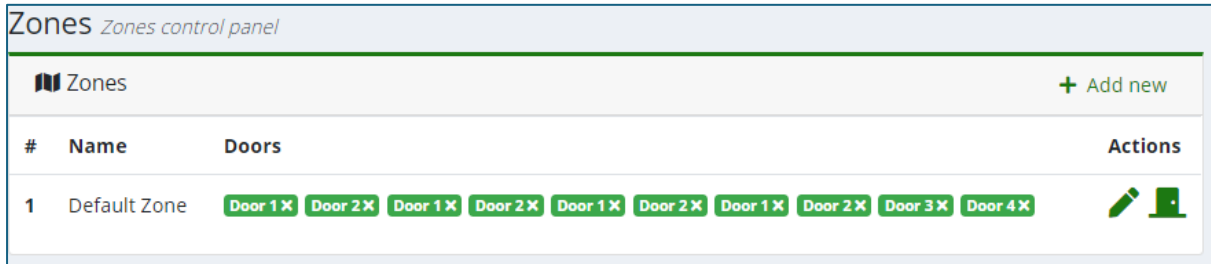


Picture 48 Configuring Readers

Click „Save Changes“ button to confirm.


## 11. Zones

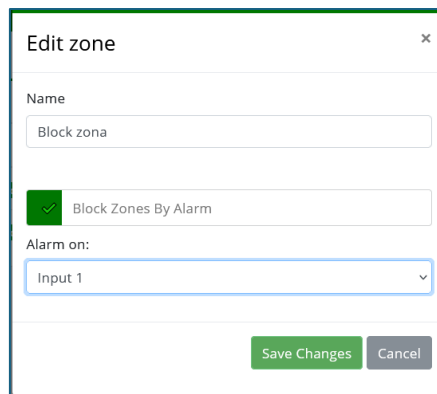
Zones section (Picture 49) allows grouping of doors so it can be easier to manage Access rules.



Picture 49 Zones

In the Zones section you can create specific zones that you want blocked based on an input to the controller (i.e. Fire alarm input to the ACC controller can block certain zones).

To configure this function when adding new Zone, enable the “Block Zones by Alarm” option. It is also possible to reconfigure existing zones by clicking on “Edit Zone” button  , shown in Picture 50.



Picture 50 Edit Zone

Finally, **Save** and **Apply** changes.

If input is active, it will be shown in the Devices section Cluster info (See Table 5 and Picture 18).

## 12. Access Times

Access Times section (Picture 51) gives brief information of created access times and allows creating new ones by clicking on **Add New**.

Access Times <i>Access times control panel</i>					
Access Times					+ Add new
#	Name	Type	Start Date	Expire Date	Actions
1	Default Access Time	AccessTimeByWeek	01.01.2019		

Picture 51 Access Times

Access Times <i>Access Times control panel</i>																																																																																																																	
Edit access times									< Back																																																																																																								
Name Employees (Monday to Friday)																																																																																																																	
Start Date 16.10.2019		Expire Date Expire Date		<table border="1"> <thead> <tr> <th></th> <th>01h</th> <th>03h</th> <th>05h</th> <th>07h</th> <th>09h</th> <th>11h</th> <th>13h</th> <th>15h</th> <th>17h</th> <th>19h</th> <th>21h</th> <th>23h</th> </tr> </thead> <tbody> <tr> <td>Mon +</td> <td></td><td></td><td></td><td></td><td>08:00 - 18:00</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td>Tue +</td> <td></td><td></td><td></td><td></td><td>08:00 - 18:00</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td>Wed +</td> <td></td><td></td><td></td><td></td><td>08:00 - 18:00</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td>Thur +</td> <td></td><td></td><td></td><td></td><td>08:00 - 18:00</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td>Fri +</td> <td></td><td></td><td></td><td></td><td>08:00 - 18:00</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td>Sat +</td> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td>Sun +</td> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> </tbody> </table>							01h	03h	05h	07h	09h	11h	13h	15h	17h	19h	21h	23h	Mon +					08:00 - 18:00								Tue +					08:00 - 18:00								Wed +					08:00 - 18:00								Thur +					08:00 - 18:00								Fri +					08:00 - 18:00								Sat +													Sun +												
	01h	03h	05h	07h	09h	11h	13h	15h	17h	19h	21h	23h																																																																																																					
Mon +					08:00 - 18:00																																																																																																												
Tue +					08:00 - 18:00																																																																																																												
Wed +					08:00 - 18:00																																																																																																												
Thur +					08:00 - 18:00																																																																																																												
Fri +					08:00 - 18:00																																																																																																												
Sat +																																																																																																																	
Sun +																																																																																																																	
By Week Enabled <input checked="" type="checkbox"/>		By Month Enabled <input checked="" type="checkbox"/>								Show as table Clear																																																																																																							
Select Weeks <input checked="" type="checkbox"/> Week 1 <input checked="" type="checkbox"/> Week 2 <input checked="" type="checkbox"/> Week 3 <input checked="" type="checkbox"/> Week 4 <input checked="" type="checkbox"/> Week 5		Select Months <input checked="" type="checkbox"/> January <input checked="" type="checkbox"/> February <input checked="" type="checkbox"/> March <input checked="" type="checkbox"/> April <input checked="" type="checkbox"/> May																																																																																																															
										Save Changes																																																																																																							

Picture 52 New Access Time

Section	Description
Name	Name for new access time
Start Date	Select a starting date
Expire Date	Select end date
By Week Enabled	Select weeks for access time
By Month Enabled	Select months for access time

Table 7

### 13. Access Rules

Access rules section gives information about created access rules (Picture 53). Access rules combine Group, Zone, Access Time to create rules which can be later easily modified for multiple users.

Clicking on Add new opens a form for creating a new Access rule. In case ‘Holiday enabled’ is checked, the specific rule will not work (Picture 54).

Access Rules <small>Access Rules control panel</small>							
Access Rules							+ Add new
#	Name	Group	Zone	Time range	Unlock Type	Holiday Enabled	Actions
1	Default Access Rule	Default Group	Default Zone	Default Access Time	Card or PIN	✓	

Picture 53 Access Rules

Add new access rule ×

Name

Group

Zone

Access time

Type

Holiday Enabled

Picture 54 New Access Rule

Section	Function
Name	Access rule name
Group	Select created group of users
Zone	Select created zone
Access time	Select created access time
Type	Choose how relays will be triggered between <b>Card, PIN, Card and PIN, Card or PIN and Card Toggle</b>
Holiday Enabled	If enabled all users from group will not be able to access selected zone at selected dates which will be explained later.

Table 8

## 14. Logs

Logs section contains System Logs (Picture 55) and Access Logs (Picture 56). System logs show information when someone logged into the system, changes they have made and various System information (i.e. Diagnostic reboots, Proxy Server state, etc.). Access logs show both Granted and Denied access events, with information whether Card or PIN or both were used to gain access. Timestamps for each entry are also available here.

System logs *System Log records*

System Log Export CSV

22.01.2021 00:00 📅 22.02.2021 23:59 📅 Show all ▼

Date	Type	Log Text	Account
22/02/21, 10:11	Info	Login successful!	sysadmin
22/02/21, 09:43	Info	Login successful!	sysadmin
22/02/21, 09:29	Info	Login successful!	sysadmin

Picture 55 System Logs

Access Logs *Access Log records*

Access Log Export as PDF Export CSV

22.01.2021 00:00 📅 22.02.2021 23:59 📅 Show all ▼ Show all ▼  🔍

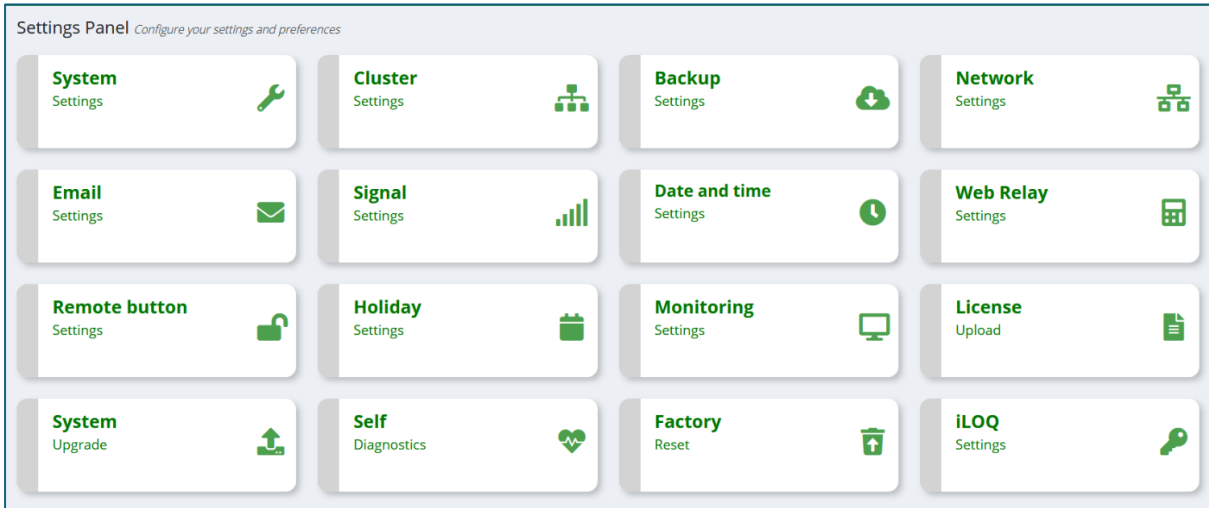
Date	Event	Access	Zone Name	Door Number	Reader	Card	PIN	Account Name	Snapshots
2/22/2021, 10:47:44 AM	Card	Granted	IT + Server Room	3	Server Room	B	571821060	oly.er	📷 Disabled
2/22/2021, 10:47:36 AM	Card	Granted	Main Entrance	1	Main Entrance	A	707405572	joel.we	📷 Disabled
2/22/2021, 10:47:05 AM	Card	Granted	Management Dept.	3	Management Department	B	40978180	dimitri.ma	📷 Disabled
2/22/2021, 10:47:00 AM	Card	Denied	Management Dept.	3	Management Department	B	304163076	tamsyn.ch	📷 Disabled
2/22/2021, 10:46:41 AM	Card	Granted	Full Access	4	Directors' office	A	2316586500	daniel.ni	📷 Disabled
2/22/2021, 10:46:45 AM	Card	Granted	Full Access	3	Server Room	A	2316586500	daniel.ni	📷 Disabled
2/18/2021, 10:38:36 AM	Card	Denied	IT + Server Room	2	IT Center	B	272938	N/A	📷 Disabled
2/2/2021, 1:05:15 PM	Card	Denied	Conference Room	2	Conference Room	B	707406340	N/A	📷 Disabled

Show 10 ▼ Clear logs 1

Picture 56 Access Logs

## 15. Settings

Settings panel allows modifying: System Settings, Cluster Settings, Backup Settings, Network Settings, Email Settings, Signal Settings, Date-Time Settings, Web Relay Settings, Remote Button, Holiday Settings, Monitoring Settings, Upload License, System Upgrade, Self-Diagnostics, Factory Reset and iLOQ Settings.



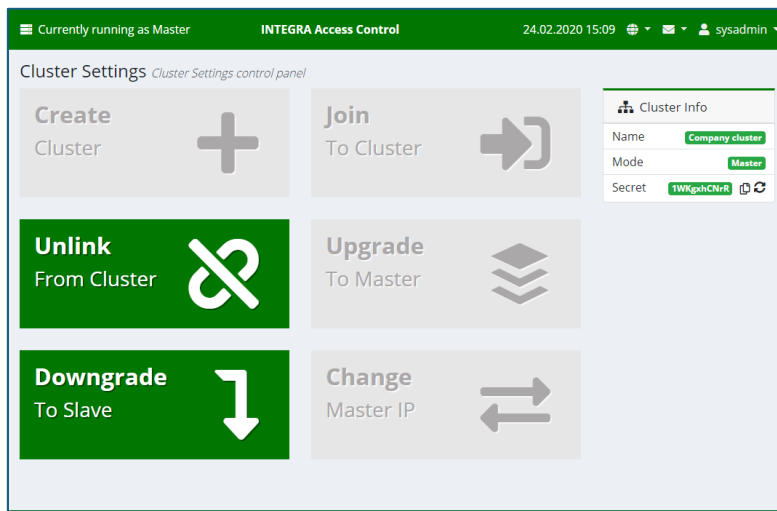
Picture 57 Settings Page

## 15.1 Cluster Settings

The cluster panel (Picture 58) shows all the basic information and settings for managing a cluster. Only the devices with a cluster license can be Masters while all devices can be slaves. Additionally, a cluster secret, which is provided in the cluster info section, is used to join a cluster.

ACC Cluster combines multiple ACC controllers into single system managed from one spot. It is used when there is a need for more relays than available on single controller (>4 doors).

All settings made on the cluster Master device are automatically synced to all cluster Slave devices.



Picture 58 Cluster Settings

The basic cluster functionalities are explained in the Table 9 below:

Name	Icon	Function
Create cluster	<b>Create Cluster</b>	Creates cluster and makes current device the Master device
Join cluster	<b>Join To Cluster</b>	Allows device to join existing cluster by entering Cluster Join Secret and Cluster Master device IP
Unlink from cluster	<b>Unlink From Cluster</b>	Unlinks device from cluster
Upgrade to master	<b>Upgrade To Master</b>	If there is no <b>Master device</b> in cluster, upgrade device to <b>Master device</b>
Downgrade to slave	<b>Downgrade To Slave</b>	Downgrades <b>Master device</b> to <b>Slave device</b>
Change master IP	<b>Change Master IP</b>	Changing master IP allows device to switch from cluster to cluster

Table 9

## 15.2 Signal Settings

Signal settings (Picture 59) control the timers for Buzzers and LEDs on events:

- Success – Entered card or PIN are correct
- Fail – Entered card or PIN are not correct
- Wait for PIN – For cases where card and PIN are required to open door, after card entry is successful waits for PIN to be entered
- DNC – Door not closed, when door is opened too long - send a signal

Section	Function
Buzz on Time	How long Buzzer is on
Buzz off Time	How long Buzzer is off
Buzz Repeat	How many times Buzzer repeats ON/OFF time
LED on Time	How long LED is on
LED off Time	How long LED is off
LED Repeat	How many times LED repeats ON/OFF time

Table 10

Signal settings *Signal settings control panel*

---

**Global Signal Settings**

<b>Success</b>			<b>Fail</b>		
Buzz On Time	Buzz Off Time	Buzz Repeat	Buzz On Time	Buzz Off Time	Buzz Repeat
<input type="text" value="500"/>	<input type="text" value="500"/>	<input type="text" value="2"/>	<input type="text" value="2000"/>	<input type="text" value="0"/>	<input type="text" value="1"/>
Led On Time	Led Off Time	Led Repeat	Led On Time	Led Off Time	Led Repeat
<input type="text" value="500"/>	<input type="text" value="500"/>	<input type="text" value="2"/>	<input type="text" value="2000"/>	<input type="text" value="0"/>	<input type="text" value="1"/>
<b>WaitForPin</b>			<b>DNC</b>		
Buzz On Time	Buzz Off Time	Buzz Repeat	Buzz On Time	Buzz Off Time	Buzz Repeat
<input type="text" value="100"/>	<input type="text" value="100"/>	<input type="text" value="2"/>	<input type="text" value="5000"/>	<input type="text" value="0"/>	<input type="text" value="1"/>
Led On Time	Led Off Time	Led Repeat	Led On Time	Led Off Time	Led Repeat
<input type="text" value="100"/>	<input type="text" value="100"/>	<input type="text" value="2"/>	<input type="text" value="100"/>	<input type="text" value="100"/>	<input type="text" value="25"/>

Picture 59 Signal Settings

### 15.3 Backup Settings

Backup Settings allows modifying configuration and loading, deleting or downloading backups (Picture 60).
































Section	Icon	Function
Upload configuration		Upload system configuration
Download current configuration		Download complete system configuration
Make Backup		Creates Backup file
Load Backup		Loads selected Backup
Delete Backup		Deletes selected Backup
Download Backup		Downloads Backup file

Table 11

**Backups** *Backups control panel*

 Backups
  Upload Configuration
 Download current configuration
 + Make Backup

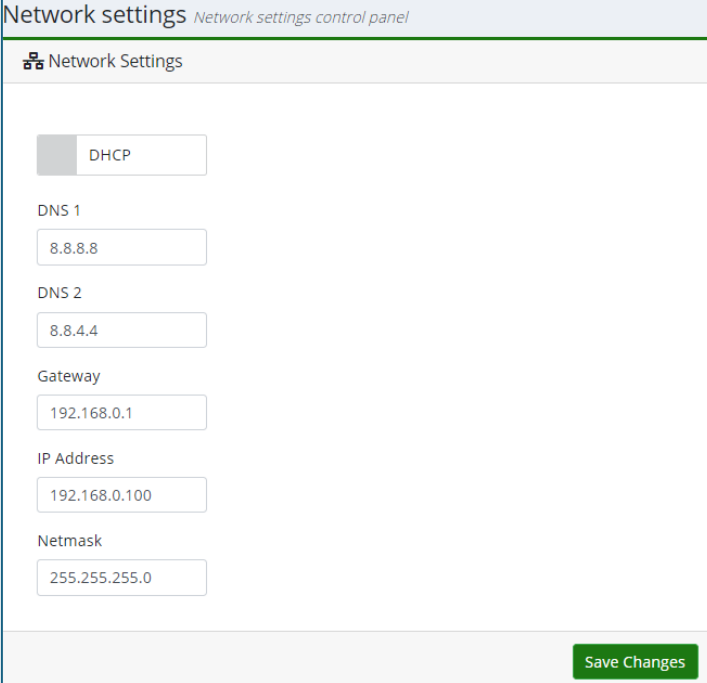
Name	Date	Time	Action
integra_ac_2019_06_13_10_38_10.bak	13.06.2019	10:38AM	  
integra_ac_2019_06_12_14_07_46.bak	12.06.2019	2:07PM	  
integra_ac_2019_06_12_14_06_13.bak	12.06.2019	2:06PM	  
integra_ac_2019_06_12_13_59_30.bak	12.06.2019	1:59PM	  
integra_ac_2019_06_12_13_55_37.bak	12.06.2019	1:55PM	  
integra_ac_2019_06_12_13_53_37.bak	12.06.2019	1:53PM	  
integra_ac_2019_06_12_13_51_54.bak	12.06.2019	1:51PM	  

Picture 60 Backups

We strongly advise making periodical system backups.

## 15.4 Network Settings

In Network Settings users can adjust IP address, Netmask, Gateway, DNS1 and DNS2 for access control device (Picture 61).



The screenshot displays the 'Network settings' control panel. At the top, there is a header 'Network settings' with a subtitle 'Network settings control panel'. Below this is a section titled 'Network Settings' with a gear icon. The main area contains several configuration options, each with a text input field:

- DHCP**: A toggle switch is currently turned off.
- DNS 1**: Input field containing '8.8.8.8'.
- DNS 2**: Input field containing '8.8.4.4'.
- Gateway**: Input field containing '192.168.0.1'.
- IP Address**: Input field containing '192.168.0.100'.
- Netmask**: Input field containing '255.255.255.0'.

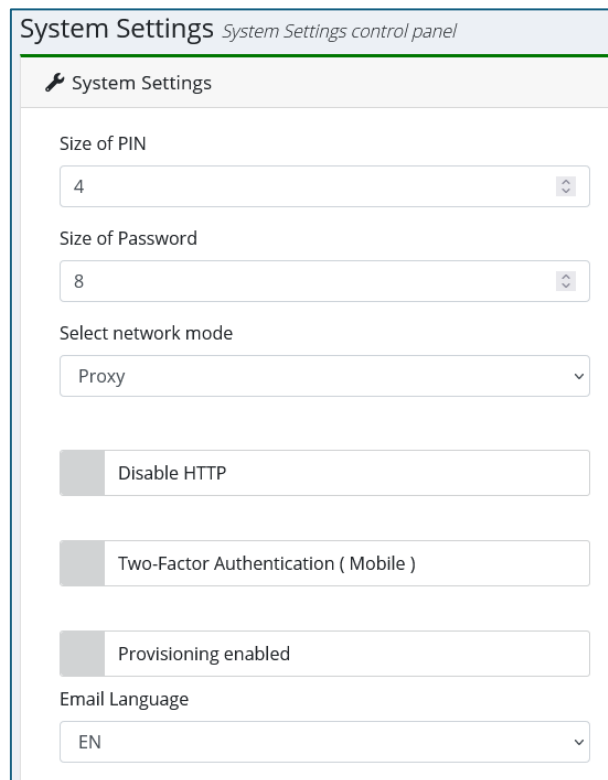
At the bottom right of the panel, there is a green button labeled 'Save Changes'.

Picture 61 Network Settings

## 15.5 System Settings

In System Settings (Picture 62) following parts can be modified:

- Size of PIN – Size of PIN that is assigned to users
- Size of Password – Size of password for entering system for users
- Select Network Mode – Determines how mobile application is connected to the ACC module (select “Proxy” to be able to unlock the door on your property from any network with an internet access)
- Disable HTTP – Do you want to have HTTP server with a HTTPS server
- Two-factor Authentication (Mobile) – Enable e-mail confirmation when registering a new mobile device (requires user to have an e-mail)
- Provisioning enabled – Enable the provisioning functionality between the ACC and SIP server systems. If you enable provisioning, you must enter a secret (min. 8 characters) and enter the same secret in your SIP server web interface
- E-mail language – Select language for Welcome e-mail



The screenshot displays the 'System Settings' control panel. At the top, there is a title bar with 'System Settings' and a subtitle 'System Settings control panel'. Below this, the settings are organized into a list:

- Size of PIN:** A dropdown menu currently set to '4'.
- Size of Password:** A dropdown menu currently set to '8'.
- Select network mode:** A dropdown menu currently set to 'Proxy'.
- Disable HTTP:** A toggle switch that is currently turned off (grey).
- Two-Factor Authentication ( Mobile ):** A toggle switch that is currently turned off (grey).
- Provisioning enabled:** A toggle switch that is currently turned on (dark grey).
- Email Language:** A dropdown menu currently set to 'EN'.

**Picture 62 System Settings**

## 15.6 Email Settings

Email settings allow configuration of custom Email (Picture 63).

Send welcome e-mail when a user is created

Custom Email Settings

HOST

Port

587

Email

Username

Password

SSL

**Picture 63 E-mail Settings**


## 15.7 Date and Time Settings


Date – Time settings allow configuring time and date for Access control devices (Picture 64).

**Date and time settings** *Date and time settings control panel*

---

**Date-Time Settings**

Date  
 

Time  
 

Timezone  
 ▼

NTP Enabled

NTP Server 1

NTP Server 2

NTP Server 3

**Picture 64 Date and Time Settings**

## 15.8 Holiday Settings

Holiday Settings (Picture 65) allows configuration of time when users won't be able to access their zones. This option can be enabled in Access Rules.

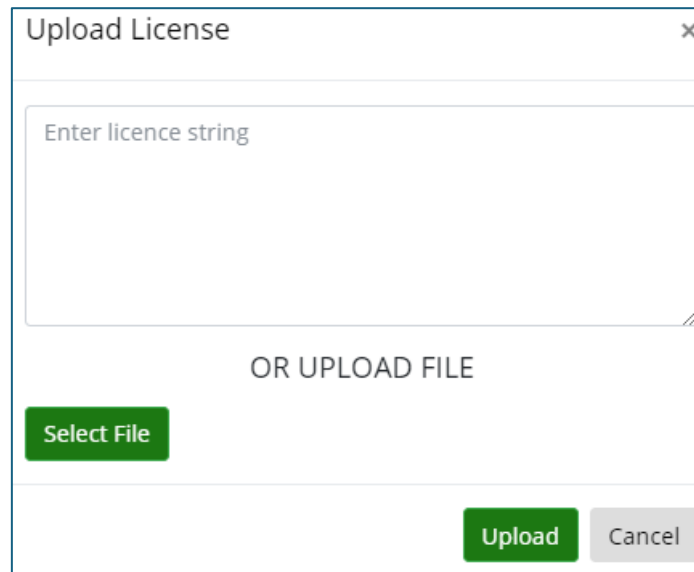
**Picture 65 Holiday Settings**

Section	Function
Holiday Name	Name of holiday
Date	Select date for that holiday
Multiple days	Allow selection of more days if holiday takes more than one day
Repeat Annually	Repeats every year

**Table 12**

## 15.9 Upload License

Clicking on Upload License gives option to upload license for Access control device either by License string or by uploading License File (Picture 66).




The image shows a dialog box titled "Upload License" with a close button (X) in the top right corner. Inside the dialog, there is a large text input field with the placeholder text "Enter licence string". Below the input field, the text "OR UPLOAD FILE" is centered. Underneath this text is a green button labeled "Select File". At the bottom right of the dialog, there are two buttons: a green "Upload" button and a grey "Cancel" button.



**Picture 66 License Upload**

## 15.10 Web Relay Settings

Web relay option provides remote control. Relay can be turned on or off using web browser.

**Picture 67 Web Relay**

Clicking on icon  in top right corner will open a form shown on Picture 68.

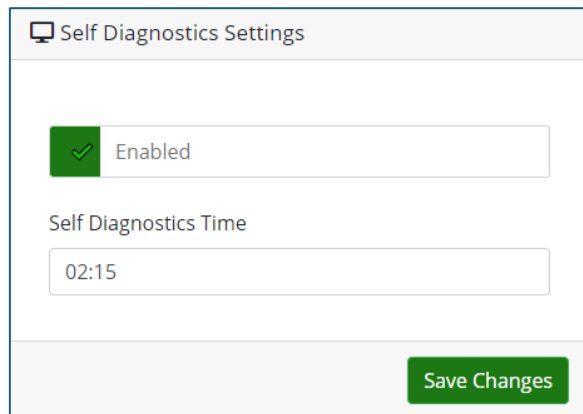
Section	Icon	Function
Trigger		Triggers relay and opens door for specified period of time.
Toggle		Toggle open or Toggle close a relay.
Copy link to open web relay	-	Pasting this link into browsers address bar will trigger relay.
Copy link to toggle web relay	-	Pasting this link into browsers address bar will toggle relay.

**Table 13**

**Picture 68 Web Relay Info and Actions**

## 15.11 Self Diagnostic Settings

When **Self Diagnostic** is enabled, system will check itself for any malfunctions at specified time and **perform a reboot**.

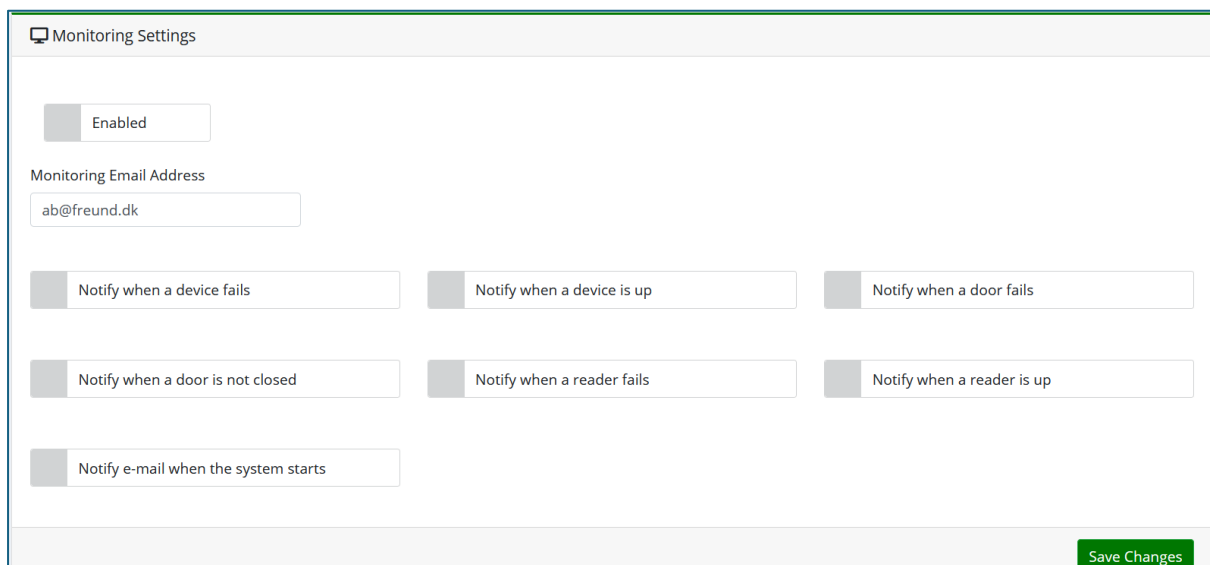


The screenshot shows a web interface titled "Self Diagnostics Settings". At the top, there is a status indicator consisting of a green checkmark icon and the text "Enabled". Below this, there is a text input field labeled "Self Diagnostics Time" containing the value "02:15". At the bottom right of the form, there is a green button labeled "Save Changes".

Picture 69 Self Diagnostic

## 15.12 Monitoring Settings

Monitoring settings allow notifying through email if devices fail, door fails, door fails, door fails, door is not closed, reader fails and when system restarts.

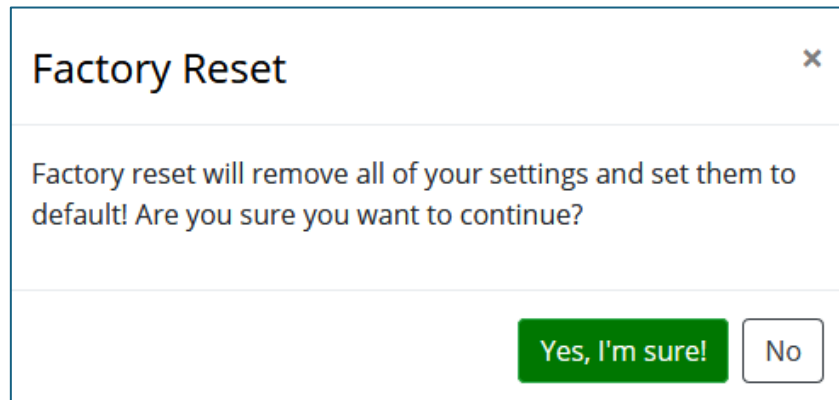


The screenshot shows a web interface titled "Monitoring Settings". At the top, there is a status indicator consisting of a grey square and the text "Enabled". Below this, there is a text input field labeled "Monitoring Email Address" containing the value "ab@freund.dk". There are seven toggle switches for different monitoring events, each with a grey square on the left and a text label on the right: "Notify when a device fails", "Notify when a device is up", "Notify when a door fails", "Notify when a door is not closed", "Notify when a reader fails", "Notify when a reader is up", and "Notify e-mail when the system starts". At the bottom right of the form, there is a green button labeled "Save Changes".

Picture 70 Monitoring Settings

### 15.13 Factory Reset

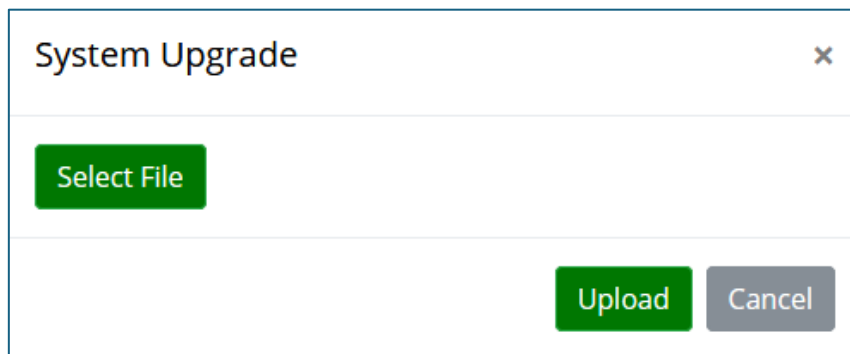
Use this option to perform a factory reset of the device.



Picture 71 Factory Reset

### 15.14 System Upgrade

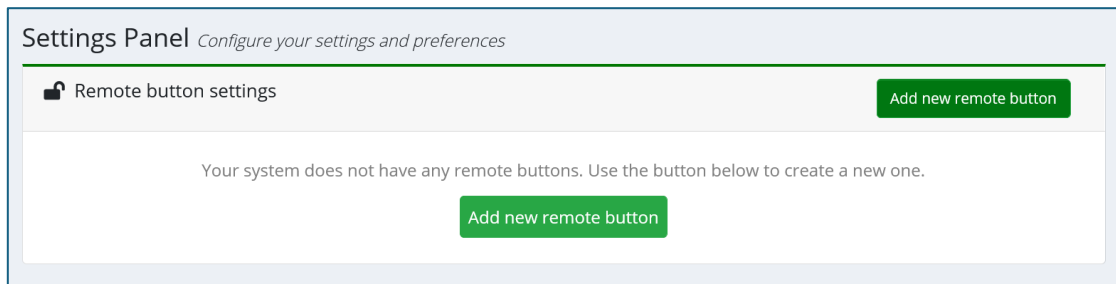
This option is used to upgrade Access Control software by selecting a file.



Picture 72 System Upgrade

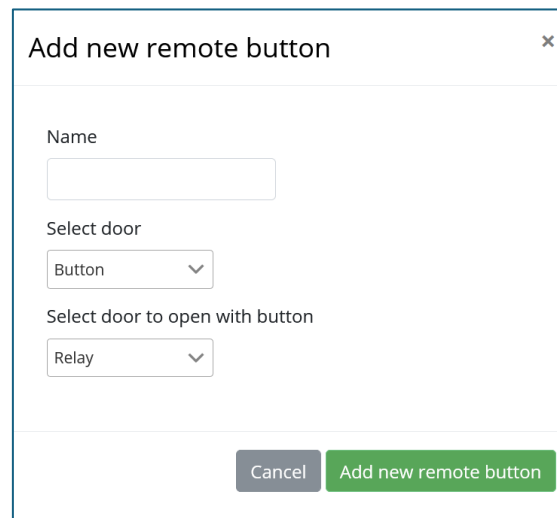
## 15.15 Remote Button

Remote Button allows opening an external door remotely. To have it work properly, an Exit button needs to be set up first (described in this document's section 8. [Devices](#)).



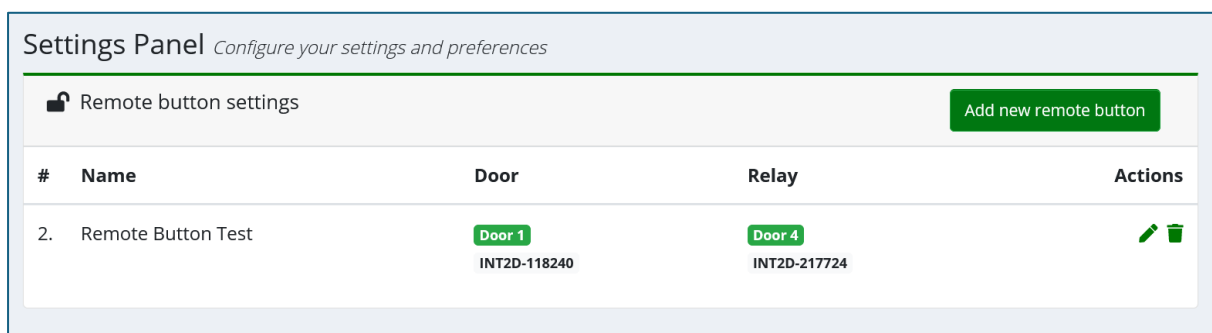
Picture 73 Remote Button Configuration



By clicking on “Add new remote button” (Picture 74), following form will show:



Picture 74 Add New Remote Button form

In the form, a name can be given to the External Button, as well as the door that has a physical button attached to it needs to be selected. To finish the configuration, assign the door which will be opened by pressing the button under “Select door to open with button”. Configured button will look as shown in the Picture 75 below.

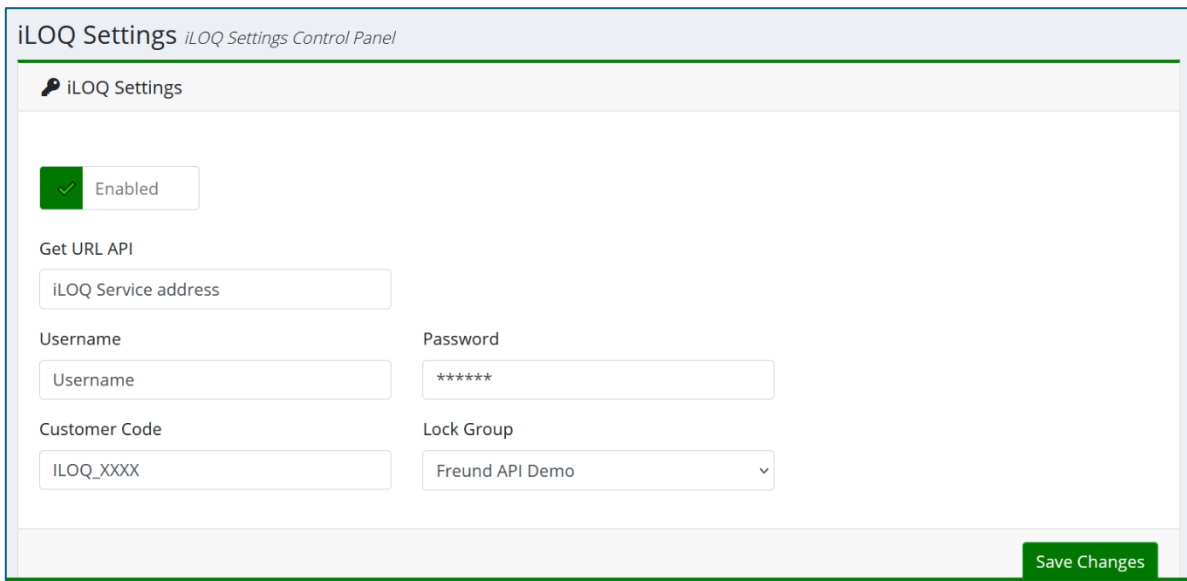


#	Name	Door	Relay	Actions
2.	Remote Button Test	Door 1 INT2D-118240	Door 4 INT2D-217724	 

Picture 75 Configured Remote Button

## 15.16 iLOQ Settings


IP-INTEGRA ACC has been integrated with iLOQ product lineup. This introduces an offline option for the ACC system.



Picture 76 iLOQ Settings

To link our ACC controller to the iLOQ system, fill out the required fields shown in Picture 76. Input information will be provided by iLOQ. To enable the integration, make sure 'Enabled' button is ticked.

Key/Card information changes from iLOQ will be synchronized\* automatically to IP-INTEGRA access controller.

To assign Account Group to the iLOQ user account, in the navigation menu on the left click on Accounts and then click on Assign Account Group button - 

No other changes can be made to the iLOQ user accounts.

\*Synchronization is done periodically every 40 seconds if there have been changes made in the iLOQ Manager.

Application note with **complete setup instruction** is available on [www.ip-integra.com](http://www.ip-integra.com) webpage.

## 16. System

- Reboot – Restarts the device.
- Shutdown – Turns off the device.