◄FREUND►

ACCESS CONTROL V1.15.0

USER MANUAL

CONTENT

1. Product setup

Configure IP Address in **Integra Network Configurator** (Picture 1).

PICTURE 1 INTEGRA NETWORK CONFIGURATION

Extract Access Control module from the box, plug in the license USB dongle with a generated configuration file.

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). Default values are "sysadmin".

Username: sysadmin   Password: sysadmin


PICTURE 2 LOG IN FORM

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.**
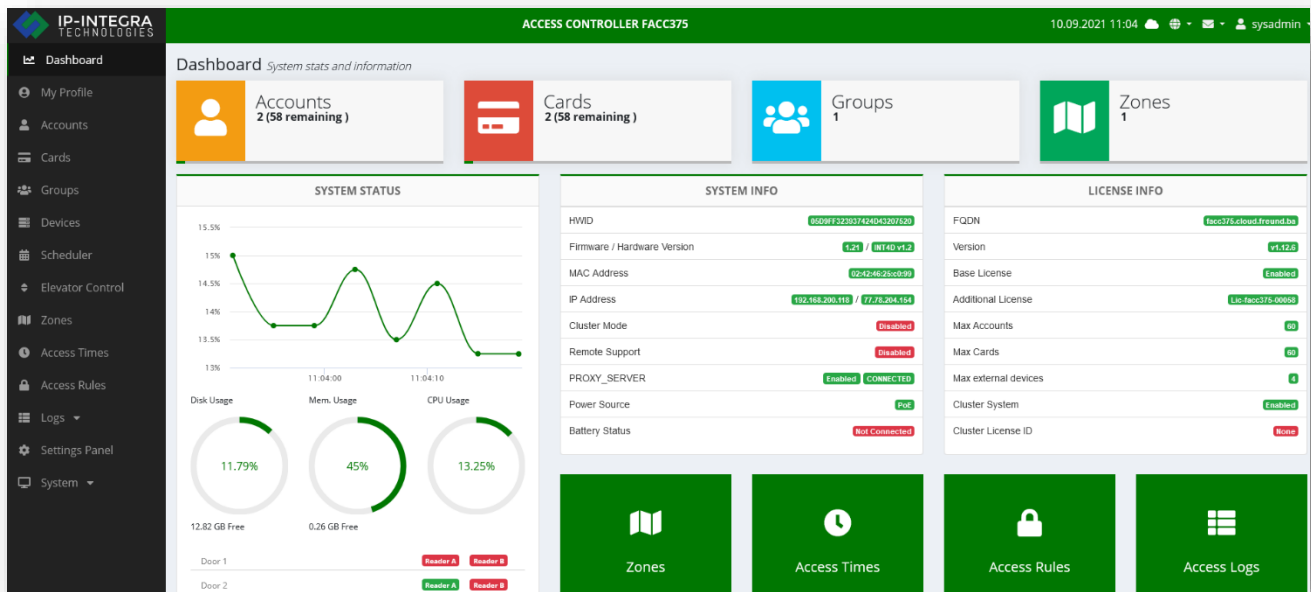
PICTURE 3 DASHBOARD

Under the **System info** within the **Dashboard** (Picture 3), **Remote support** is disabled by default. Clicking **'Disabled'** will open a window for enabling **Remote support** (Picture 4). This option is only provided in the **Dashboard**.
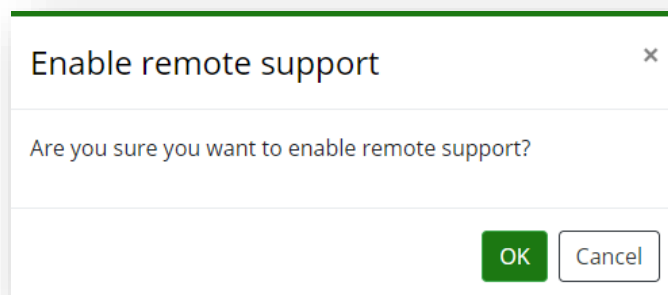

PICTURE 4 REMOTE SUPPORT

Service "Remote Support" requires your firewall settings not to forbid 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.

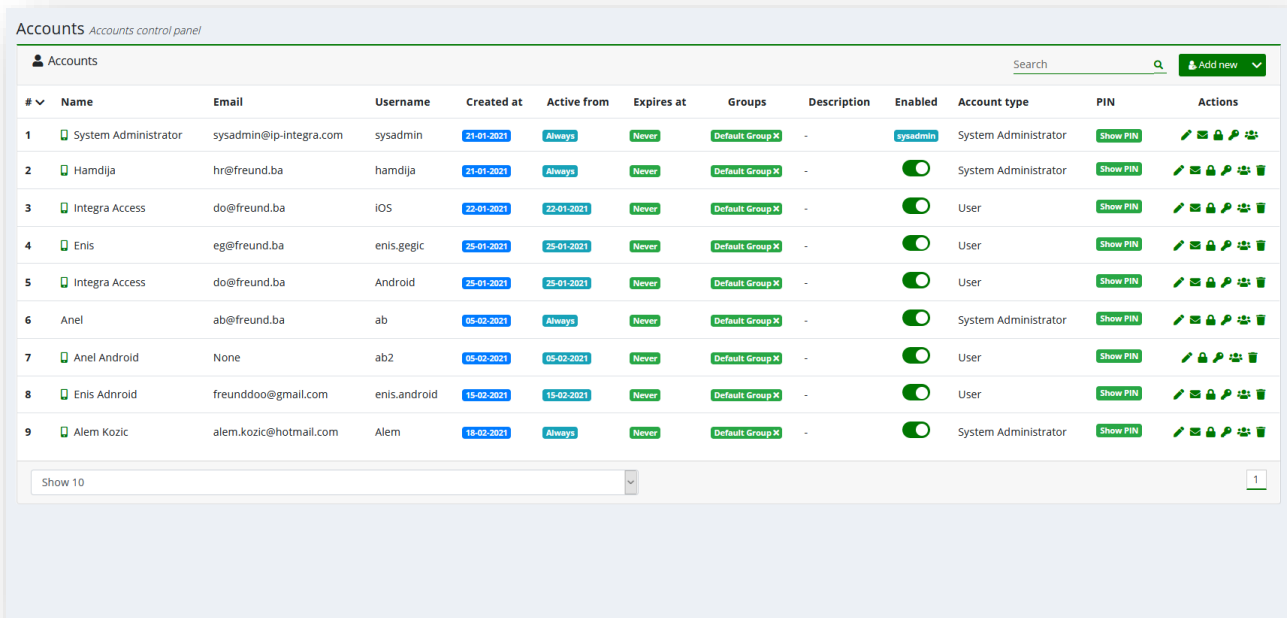| Name	Icon	Function
Translation	⊕ ▾	Changes the language of the system
Notifications	✉ ▾	Shows if there is a new firmware update available

3. My Profile

This section provides with information of the user that is currently using the system. Clicking on **Generate new** generates 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.
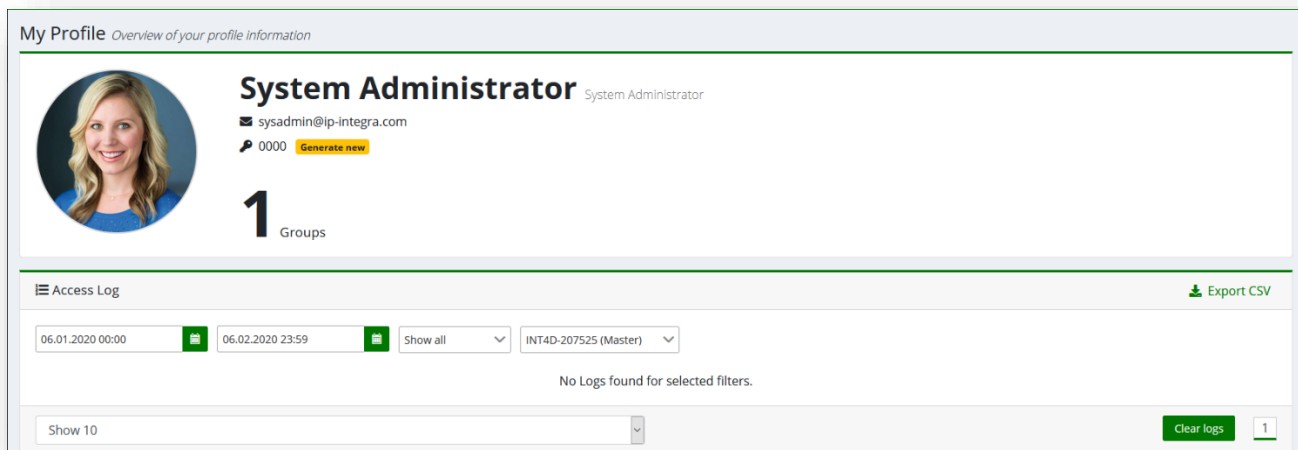
PICTURE 5 MY PROFILE

4. Accounts (SysAdmin, Admin and Manager)

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	-	sysadmin	System Administrator	Show PIN	
2	Hamdija	hr@freund.ba	hamdija	21-01-2021	Always	Never	Default Group X	-		System Administrator	Show PIN	
3	Integra Access	do@freund.ba	iOS	22-01-2021	22-01-2021	Never	Default Group X	-		User	Show PIN	
4	Enis	eg@freund.ba	enis.gegic	25-01-2021	25-01-2021	Never	Default Group X	-		User	Show PIN	
5	Integra Access	do@freund.ba	Android	25-01-2021	25-01-2021	Never	Default Group X	-		User	Show PIN	
6	Anel	ab@freund.ba	ab	05-02-2021	Always	Never	Default Group X	-		System Administrator	Show PIN	
7	Anel Android	None	ab2	05-02-2021	05-02-2021	Never	Default Group X	-		User	Show PIN	
8	Enis Adnroid	freunddoo@gmail.com	enis.android	15-02-2021	15-02-2021	Never	Default Group X	-		User	Show PIN	
9	Alem Kozic	alem.kozic@hotmail.com	Alem	18-02-2021	Always	Never	Default Group X	-		System Administrator	Show PIN	

PICTURE 6 ACCOUNTS

Under the **Actions** column, the following options are available:

Name	Icon	Function
Edit user	✏️	Opens form which enables changing account data.
Send welcome email	✉️	
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

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	Access to
System admin	Edit and view everything
Admin	Can 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 profile

Each account can have its own card. 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 for selecting time range in which account will be active. Account is labeled as **Expired** when expire date lapse.
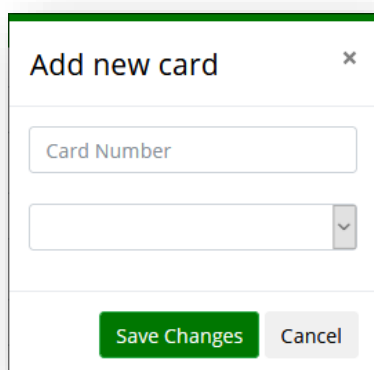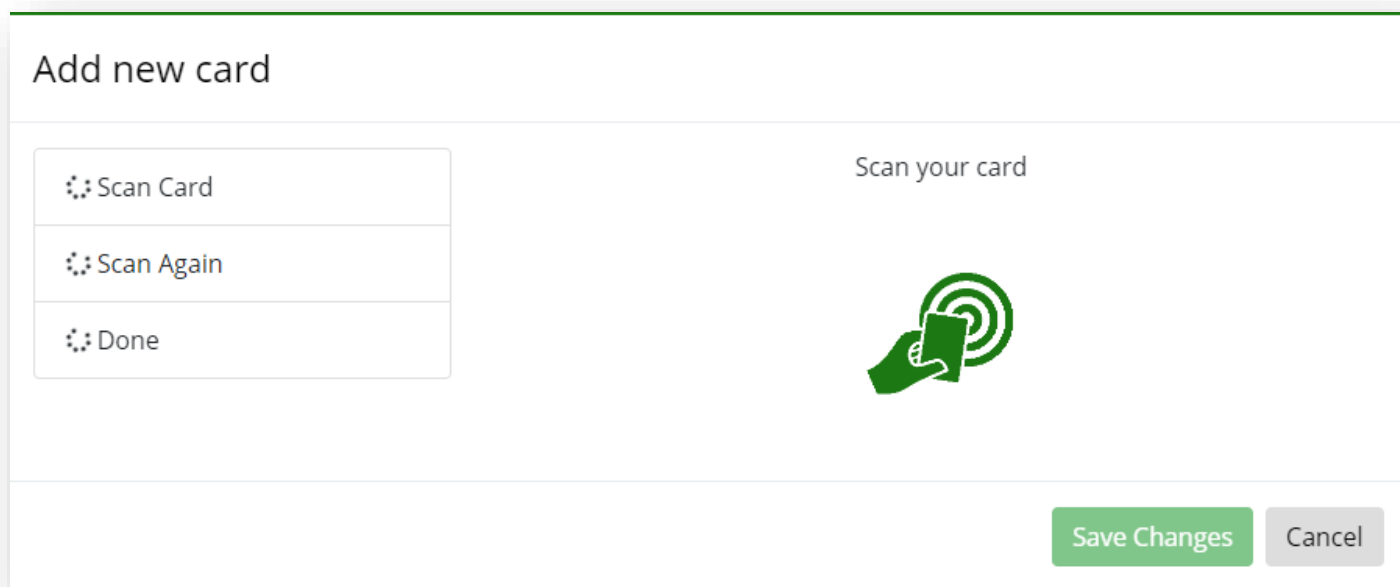

PICTURE 7 ADD NEW ACCOUNT

PICTURE 8 ADD NEW CARD

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

PICTURE 9 CARD SCANNING

5. Mobile devices

From version 1.12, the Access Control system will support the use of mobile devices with the IP-INTEGRA Access mobile application.

In order to use our Mobile application, we first need to add your mobile device into the system. Adding device is accomplished by using a QR code that will be delivered by the 'Welcome e-mail' feature. The 'Welcome e-mail' can be sent by either pressing the E-mail icon (✉   ) on the Account Management page(right side) or by pressing the 'Deliver QR code' button on the Edit User page (Picture 10).
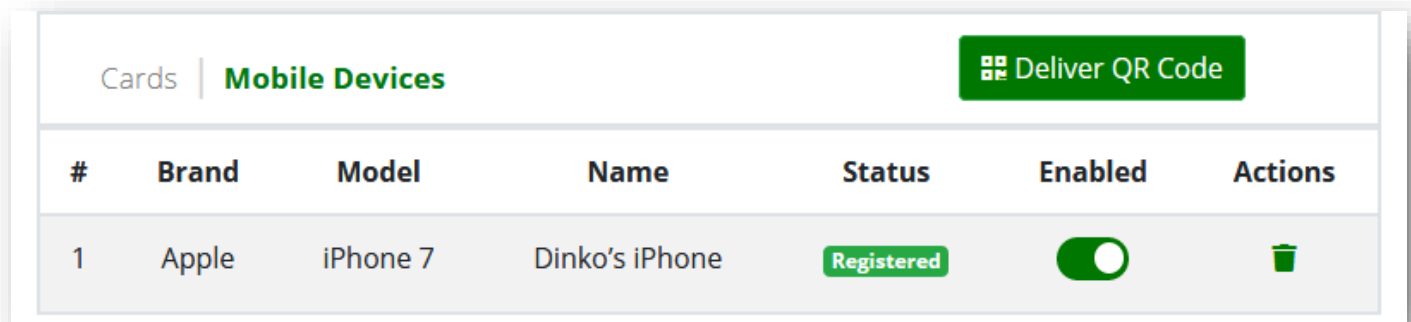
PICTURE 10 MOBILE DEVICE MANAGEMENT

QR code will arrive in the e-mail attached as a .pdf file. Once you open the .pdf you must scan the QR code shown in picture 11 with your IP-INTEGRA Access mobile application.
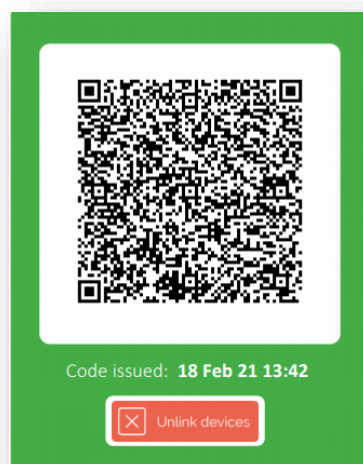
PICTURE 11 THE QR CODE IN THE .PDF FILE

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 two-factor authentication is enabled, you will be required to input a six-digit code that will be delivered to your e-mail address (Picture 12).

PICTURE 12 TWO-FACTOR AUTHENTICATION 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 two-factor authentication you need to open the 'System settings' panel and click the button shown in picture 13.
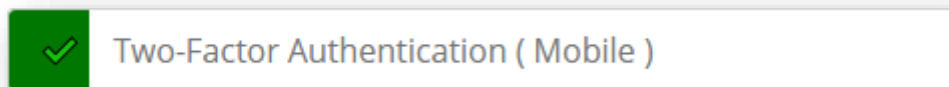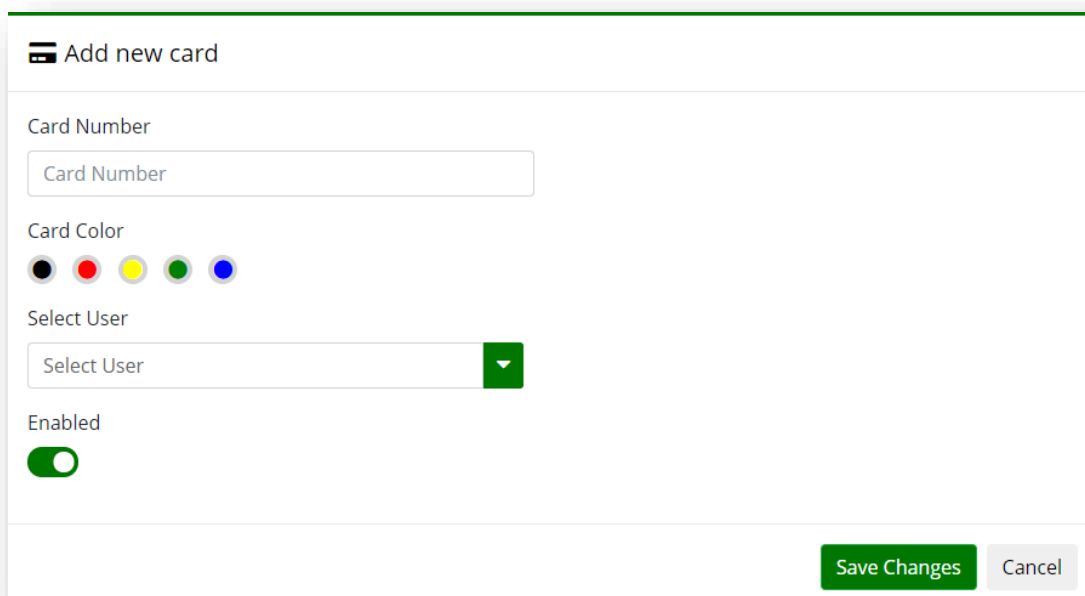
PICTURE 13 MANAGING TWO-FACTOR AUTHENTICATION

6. Cards (SysAdmin, Admin and Manager)

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).
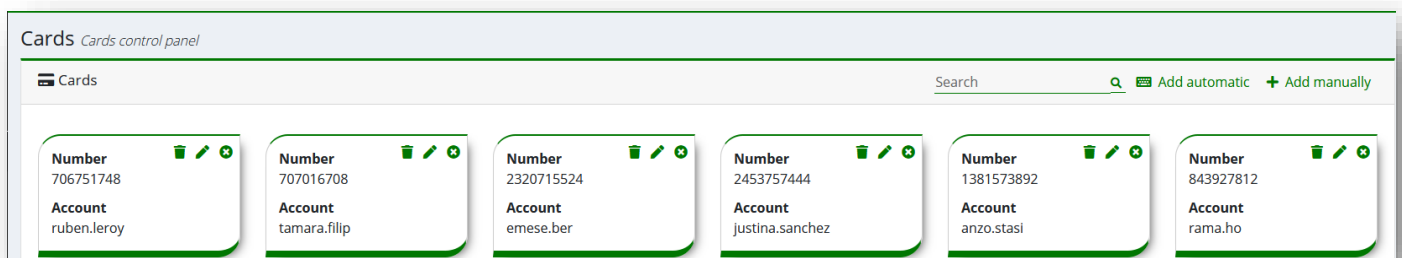
PICTURE 14 CARDS CONTROL PANEL

PICTURE 15 EDIT CARD

7. Groups (SysAdmin and Admin)

Groups section (Picture 16) lists all groups 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.**

PICTURE 16 GROUPS

PICTURE 17 ADD NEW GROUP

8. Devices (SysAdmin)

Devices section lists all connected devices with information about doors and zones that are assigned to them.
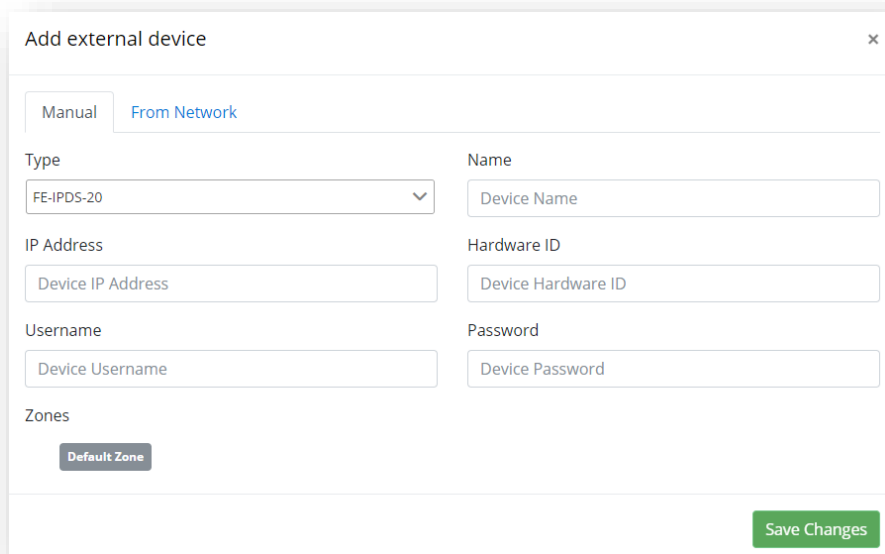
PICTURE 18 DEVICES

PICTURE 18 TABLE VIEW OF A SINGLE DEVICE

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

In **Devices** section (Picture 18) are listed information of all devices that are in cluster. Clicking on **Scan Devices** opens 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.

Changes made on **Master device** are applied to all **Slave devices**, while **Slave device's** settings cannot be changed.

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 19) or from network (Picture 20)**.**

PICTURE 19 MANUALLY ADD EXTERNAL DEVICE

PICTURE 20 ADD EXTERNAL DEVICE FROM NETWORK

16

Section	Description
Device Name	Name of the Device, it can be changed by clicking on ✏ under **Actions** column
IP Address	IP address of device
Cluster Info	Gives information in which cluster is device, and their position **M** – Master, **S** -Slave, **SA** - Stand Alone
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 working
Status	**OK** – device is working properly, **Pending** – device is doing some process before it can send or receive information, **Failed** – device is not working

⚠ You are currently running in Slave Mode. Any changes you make CANNOT be saved and applied. **Please switch to Master.**

PICTURE 21 MESSAGE WHEN LOGGED INTO SLAVE DEVICE

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 22). There are 3 types that can be chosen for readers: **Wiegand 34, Wiegand 26** (depending on reader) and **No reader** when there is no reader connected. Enabling **Snapshots** will require to RTSP link of device to be entered and it will take four pictures from devices camera which are available in **Access Logs**. Clicking on 📖 allows adding zones (Picture 23) to doors which will be explained later.

PICTURE 22 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 23).

PICTURE 23 EXIT BUTTON CONFIGURING

18
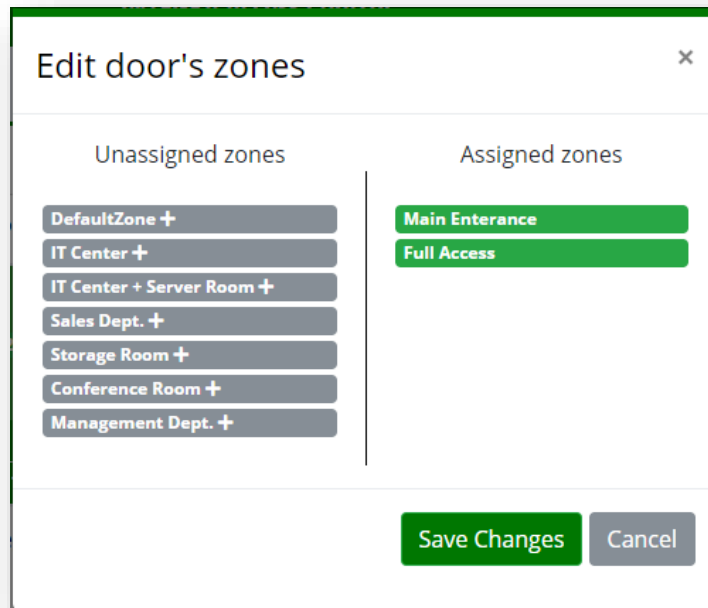
PICTURE 24 EDIT DOOR'S ZONES

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 25. An example of a single device in visual view is presented in Picture 25.
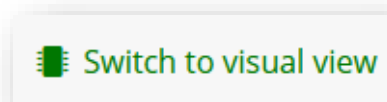
PICTURE 25 VISUAL VIEW BUTTON
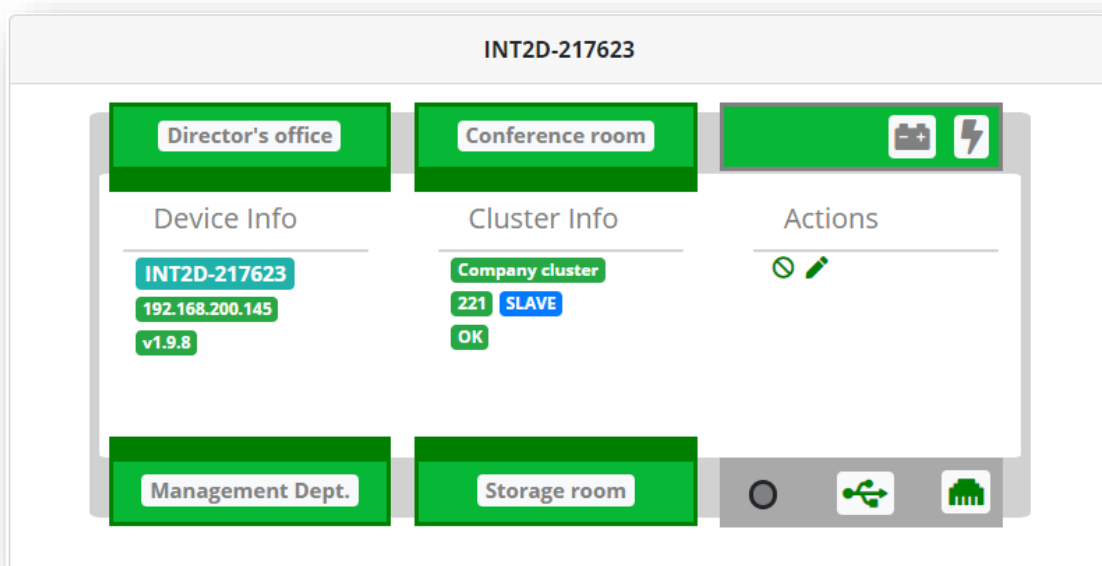
PICTURE 26 VISUAL VIEW OF A SINGLE DEVICE

To see the defined zones for each door in visual view, hover over the door name. A list with zones and editing options will appear, as shown in Picture 27.
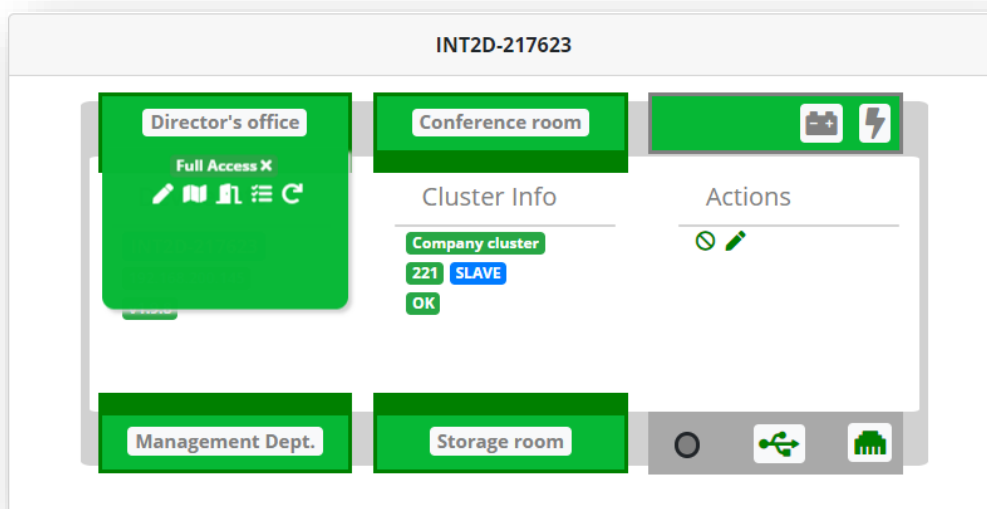
PICTURE 27 ZONES LIST IN VISUAL VIEW

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 28.
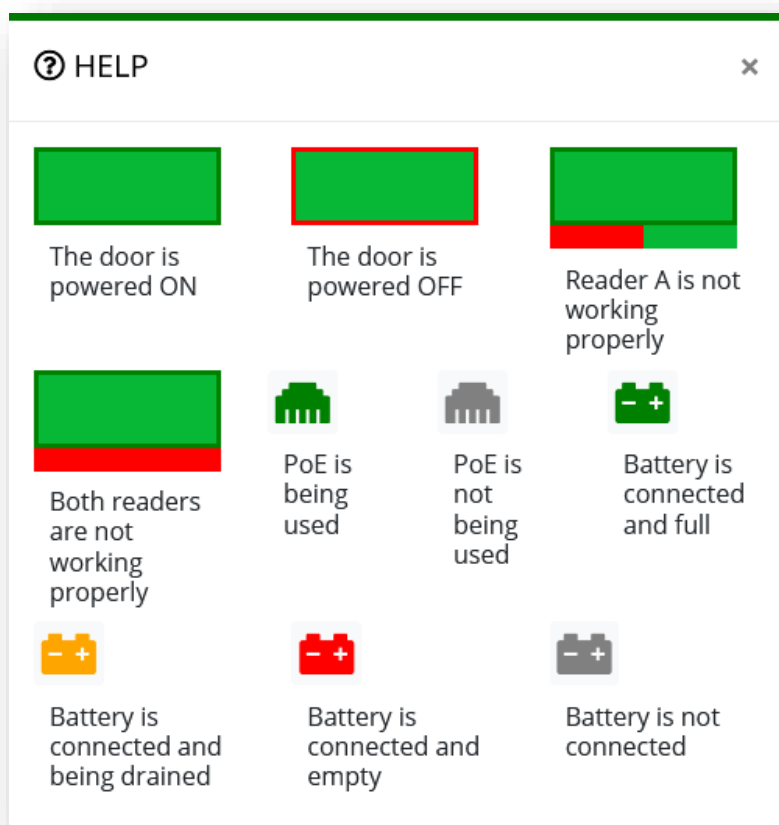
PICTURE 28 HELP WINDOW

9. Scheduler (SysAdmin and Admin)

The **Scheduler** feature is used to assign doors to remain opened for the specified time period. You can specify the time of day and the day of the week. In the picture 29 you can see an example of the scheduler panel.

PICTURE 29 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 the picture 30.

PICTURE 30 ADDING A 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.

22

10. Elevator Control Module

With the update 1.12. new major addition to the IP-INTEGRA ACC is **Elevator Control Module**.

Elevator Control Module (Picture 31) is used to introduce 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.
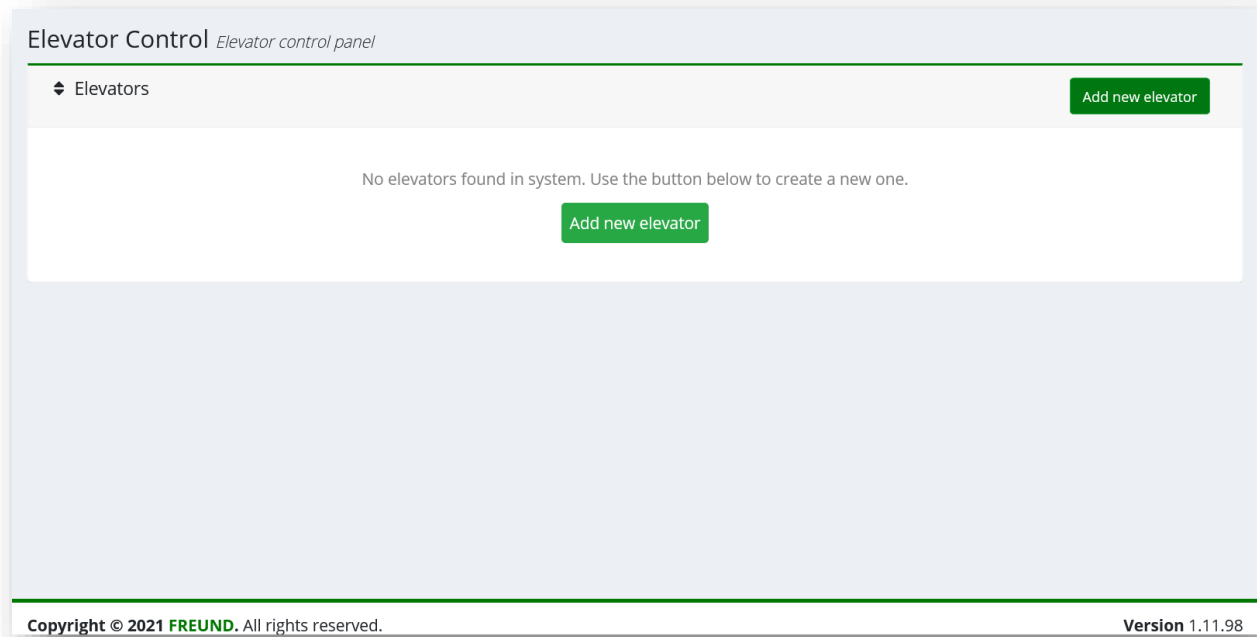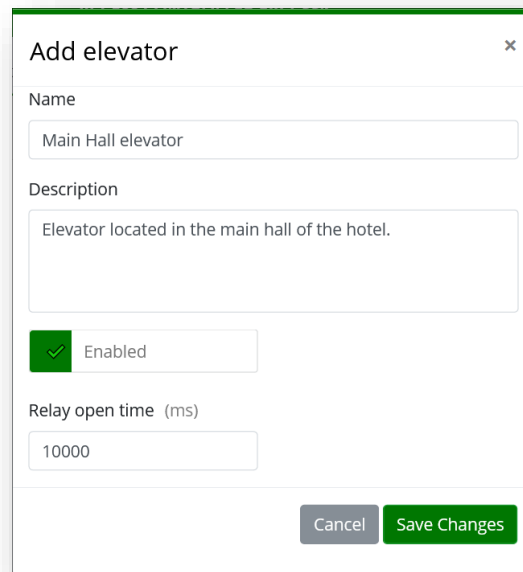
PICTURE 31 ELEVATOR CONTROL PANEL

Click on „**Add new elevator**" button shown in the Picture 32 and fill out the required fields.

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

Click on „**Save Changes**" button to finish adding the elevator.
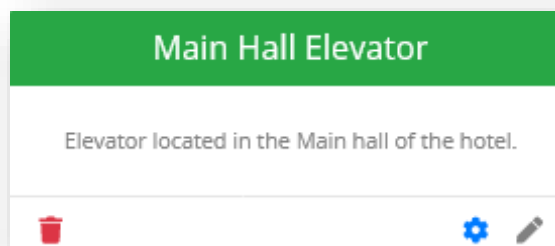
PICTURE 32 ADDING THE ELEVATOR

Your **Elevator Control Panel** should show the added elevator:

PICTURE 33 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:
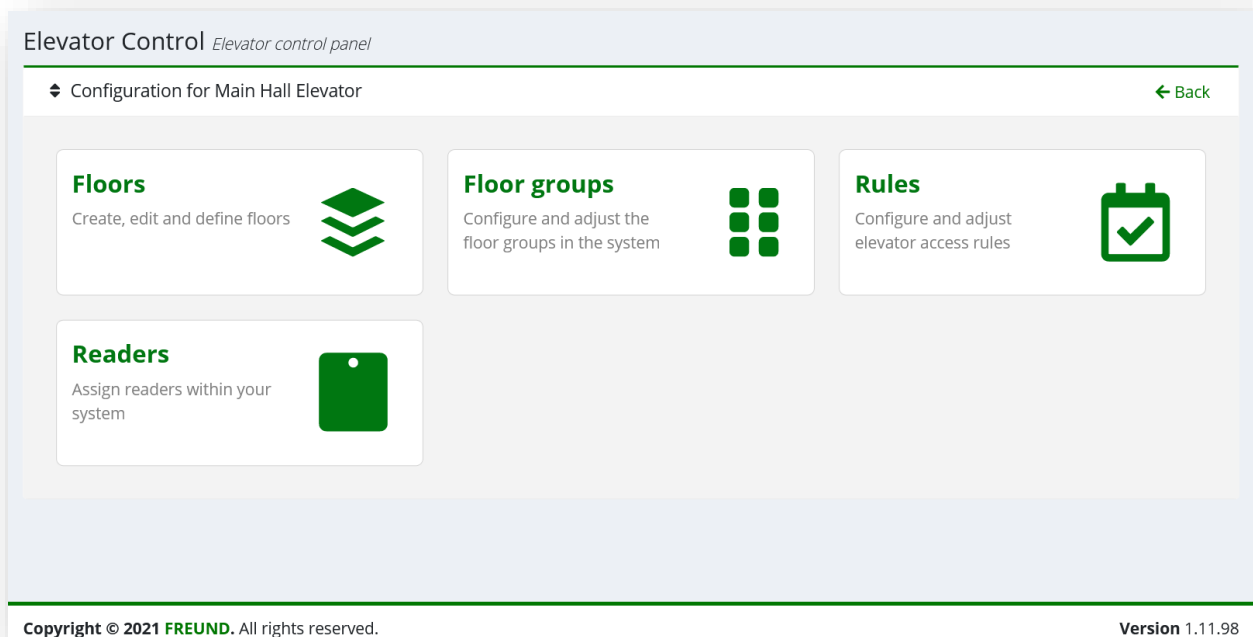
PICTURE 34 ELEVATOR CONFIGURATION

As shown in the Picture 34, 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. In order to do that, we are clicking on **Floors** button shown in Picture 34. Following screen will appear:
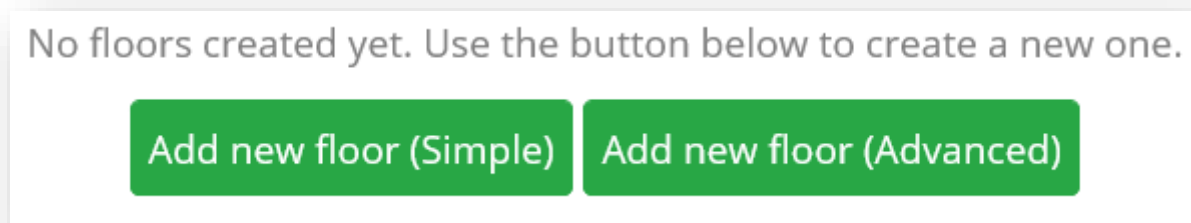
PICTURE 35 WAYS TO ADD NEW FLOOR

PICTURES 36 & 37 SHOWING DIFFERENT WAYS OF ADDING FLOORS

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).

PICTURE 38 SHOWING THE FLOORS LIST

Using the following icons, ✏ 🗑   the floors can be edited or deleted, respectively.
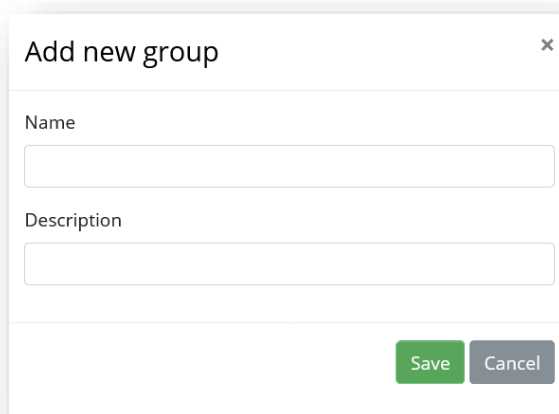
When you have added all the floors you need, click on the „**Back**" button.

To proceed, we must create Floor Groups and assign created Floors to them. click on the Floor groups button(shown in Picture 34). Following screen will show:
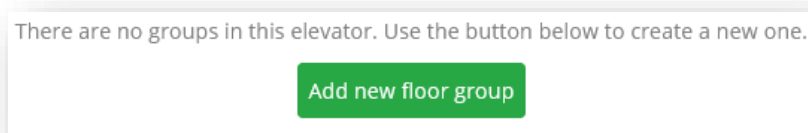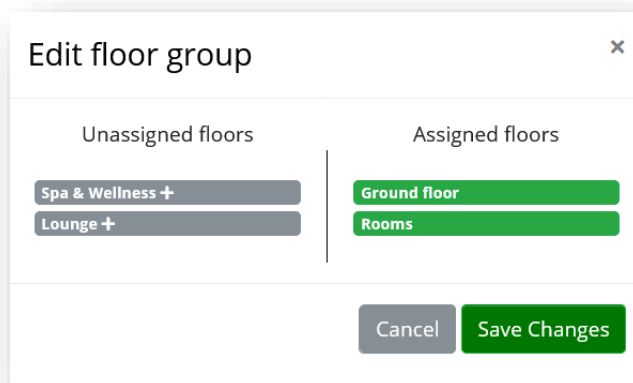

PICTURE 39 ADDING NEW FLOOR GROUP

Click on the „**Floor Groups**" button and fill out the forms shown in Picture 39.
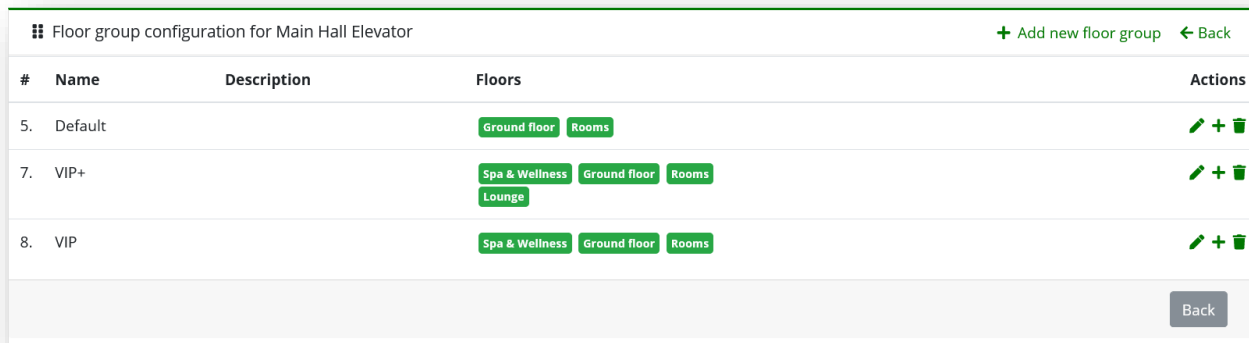
PICTURE 40 GROUP ADDING FORM

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.

PICTURE 41 ASSIGNING FLOORS TO THE FLOOR GROUPS

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

PICTURE 42 SHOWING THE FLOOR GROUPS LIST
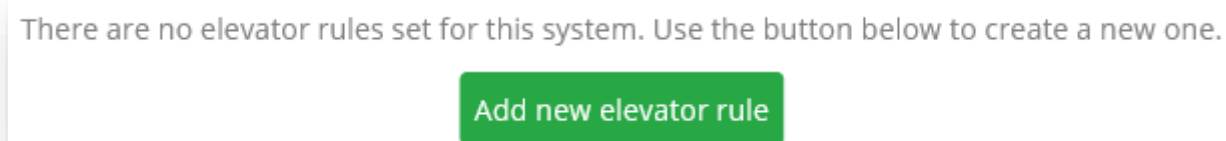
You can add as many groups as you need.

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 the rules which will allow the Elevator Control to function. Click on Rules button shown in Picture 34. The following screen will show:
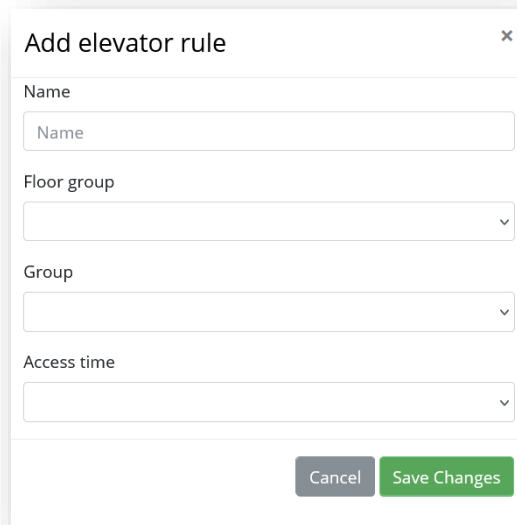
PICTURE 43 ADD NEW ELEVATOR RULE BUTTON

Click on the „**Add new elevator rule**" button and fill out the required fields shown in Picture 44.

In the following screen, you can assign a User Group to the Floor Group:
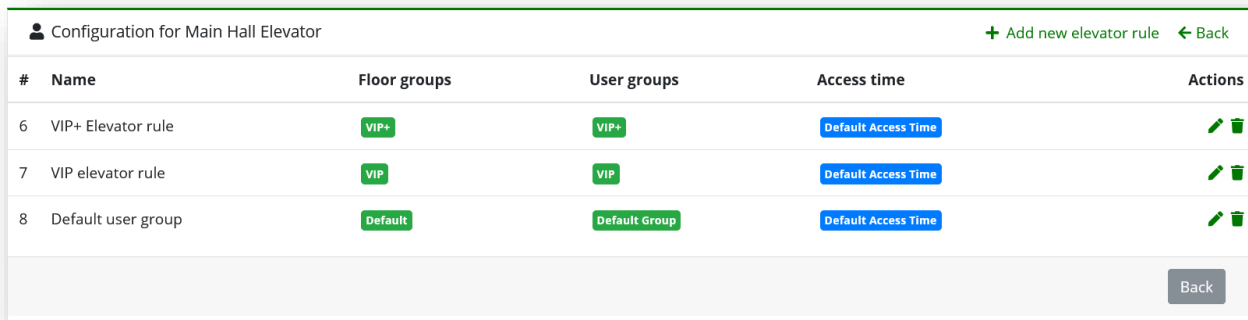
PICTURE 44 – RULE ADDING FORM

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

PICTURE 45 ELEVATOR RULES LIST

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 the Picture 34. Following screen will show:
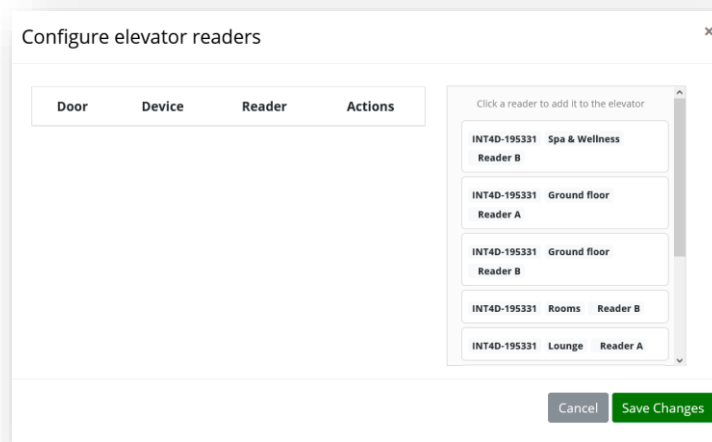
PICTURE 46 ADDING READER TO THE ELEVATOR

We have connected an elevator reader to the Relay 1 on the ACC module, which also contains the button for floor -1. Here is how it looks like when configured:
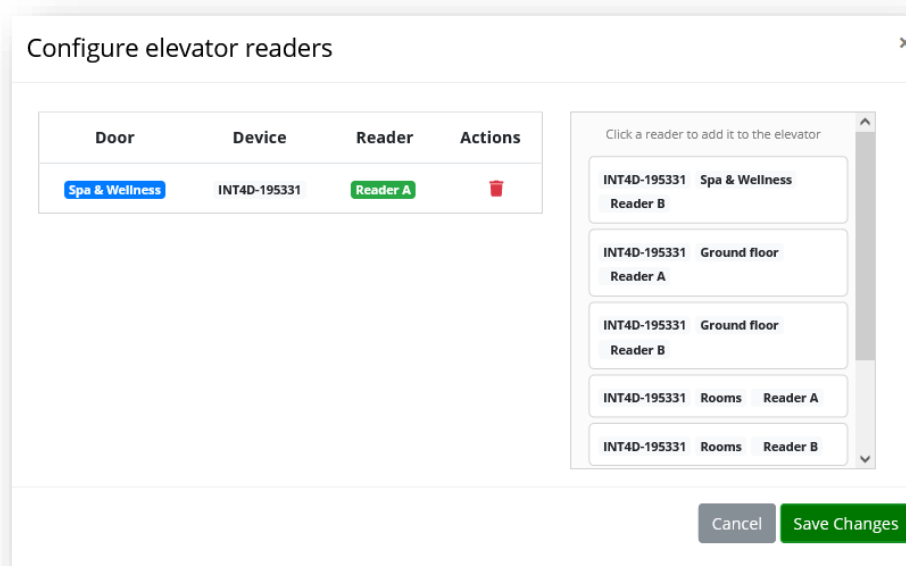
PICTURE 47 CONFIGURED READER

Click „**Save Changes**" to confirm.

![FREUND logo]

11. Zones (SysAdmin and Admin)

Zones section (Picture 48) allows grouping of doors so it can be easier to manage **Access rules**.

PICTURE 48 ZONES

12. Access Times (SysAdmin and Admin)

Access Times section (Picture 49) gives brief information of created access times and allows creating new ones by clicking on **Add new.**

PICTURE 49 ACCESS TIMES

PICTURE 50 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

13. Access Rules (SysAdmin and Admin)

Access rules section gives information about created access rules (Picture 51). Access rules combine **Group, Zone, Access Time** to create rules which can be later easily modified for multiple users.
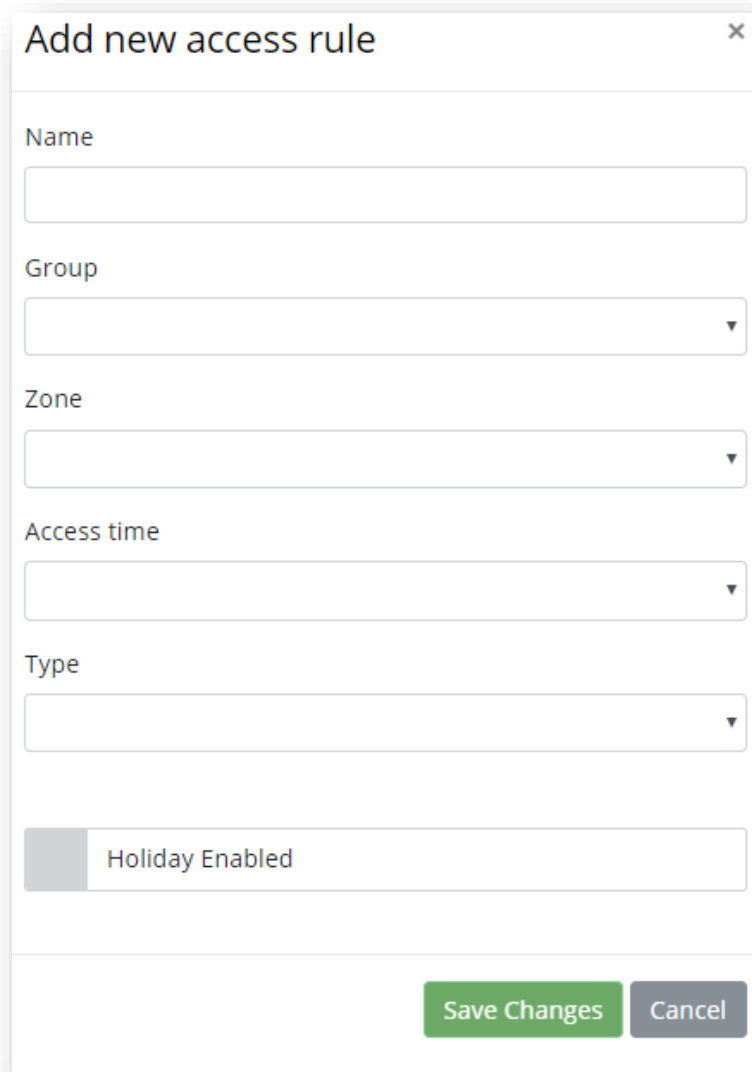
Clicking on **Add new** opens a form for creating a new **Access rule**. In case 'Holiday enabled' is checked, the specific rule will not work (Picture 52).

PICTURE 51 ACCESS RULES

32

FREUND

PICTURE 52 FORM FOR CREATING 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 **Card, PIN, Card and PIN, Card or PIN** and **Card Toggle**
Holiday Enabled	If enabled all users from group will not be able to access selected zone at selected dates which will be explained later.

14. Logs

Logs section gives information when someone logged into the system (Picture 53) and when someone used a card or a PIN (Picture 54).

**PICTURE 53 SYSTEM LOG**

PICTURE 54 ACCESS LOG

15. Settings (SysAdmin)

Settings panel allows modifying: **System Settings, Cluster Settings, Backup Settings, Network Settings, Email Settings, Signal Settings, Date-Time Settings, Web Relay Settings, Holiday Settings, Monitoring Settings, Upload License, System Upgrade, Self-Diagnostics and Factory Reset.**
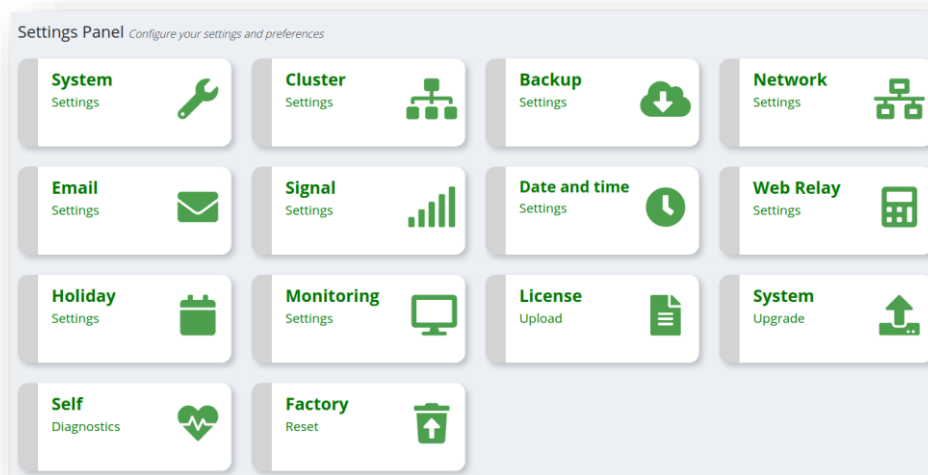
PICTURE 55 SETTINGS PANEL

15.1 Cluster Settings

The cluster panel 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.
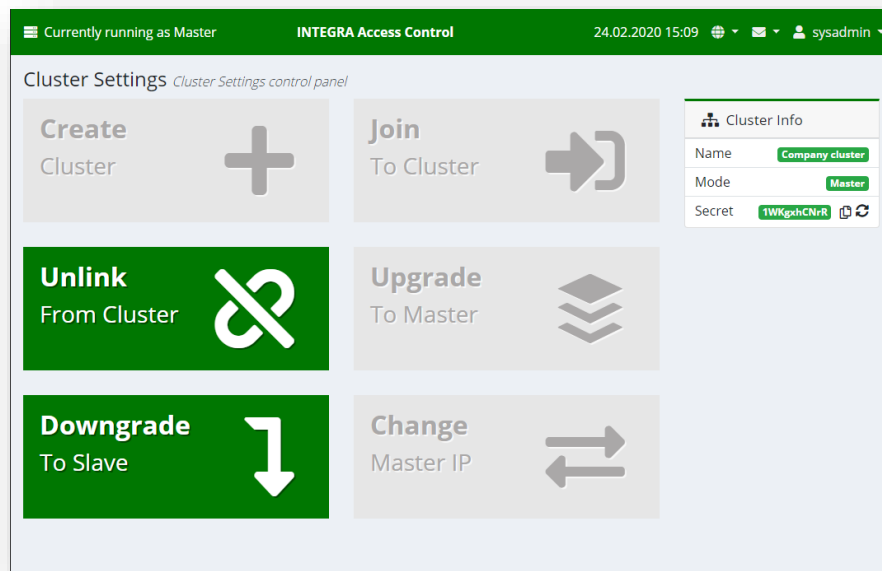
PICTURE 56 CLUSTER SETTINGS

The basic cluster functionalities are explained in the table below:

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

15.2 Signal Settings

Signal settings (Picture 57) control timers for Buzzers and LED 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

PICTURE 57 SIGNAL SETTINGS

15.3 Backup Settings

Backup Settings allows modifying configuration and loading, deleting or downloading backups (Picture 58).

Section	Icon	Function
Upload configuration	Upload Configuration	Upload configuration for whole system
Download current configuration	Download current configuration	Download configuration for whole system
Make Backup	+ Make Backup	Creates Backup file
Load Backup		Loads selected Backup
Delete Backup		Deletes selected Backup
Download Backup		Downloads Backup file

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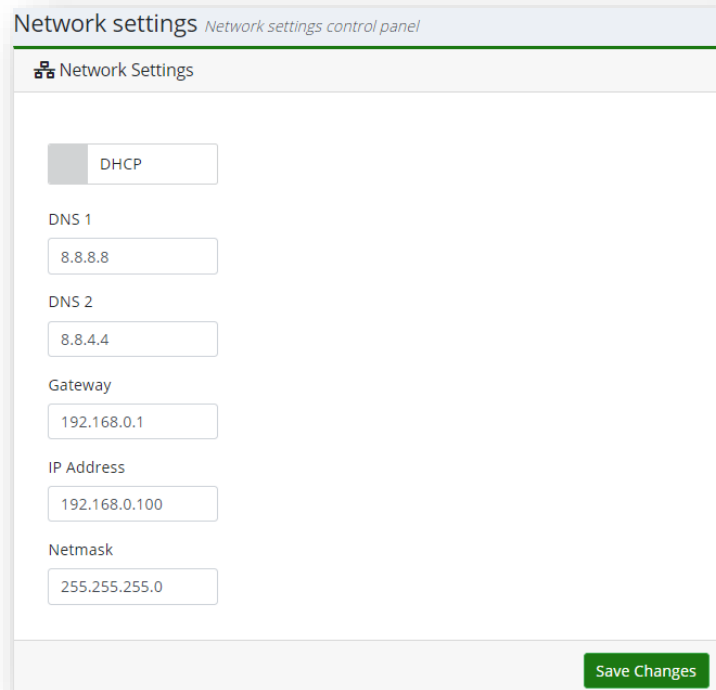
Name	Date	Time	Action
integra_ac_2019_06_13_10_38_10.bak	13.06.2019	10:38AM	
integra_ac_2019_06_12_14_07_46.bak	12.06.2019	2:07PM	
integra_ac_2019_06_12_14_06_13.bak	12.06.2019	2:06PM	
integra_ac_2019_06_12_13_59_30.bak	12.06.2019	1:59PM	
integra_ac_2019_06_12_13_55_37.bak	12.06.2019	1:55PM	
integra_ac_2019_06_12_13_53_37.bak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

PICTURE 58 BACKUP SETTINGS

15.4 Network Settings

In **Network Settings** user can adjust IP address, Netmask, Gateway, DNS1 and DNS2 for access control device (Picture 59).
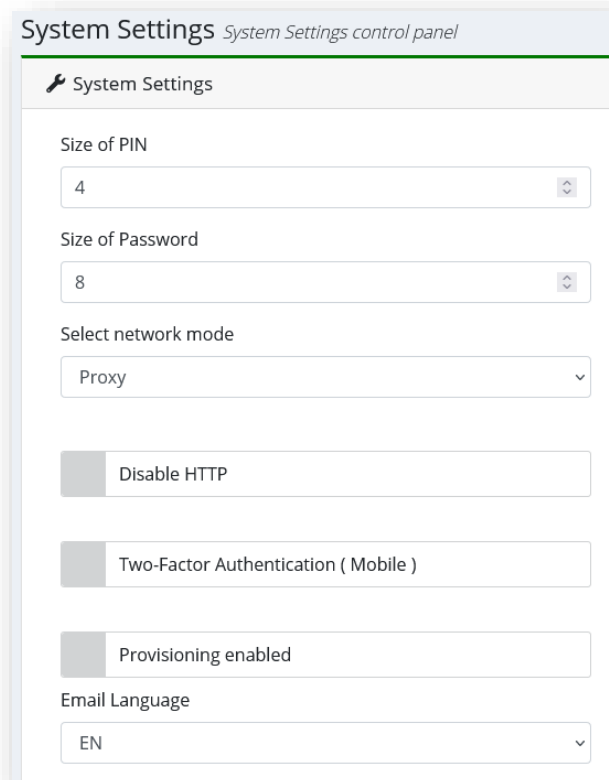
PICTURE 59 NETWORK SETTINGS

15.5 System Settings

In **System Settings** (Picture 60) 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
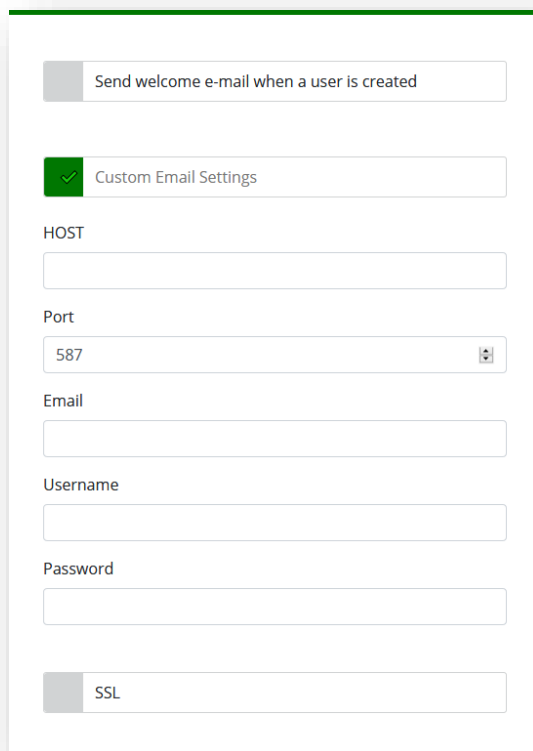- E-mail language – Select language for Welcome e-mail

PICTURE 60 SYSTEM SETTINGS

15.6 Email settings

Email settings allows configuration of custom Email (Picture 61).

PICTURE 61 EMAIL SETTINGS

15.7 Date – Time Settings

Date – Time settings allows configuring time and date for Access control devices (Picture 62).


PICTURE 62 DATE - TIME SETTINGS

15.8 Holiday Settings

Holiday Settings (Picture 63) allows configuration of time when users won't be able to access their zones. This option can be enabled in **Access Rules**.
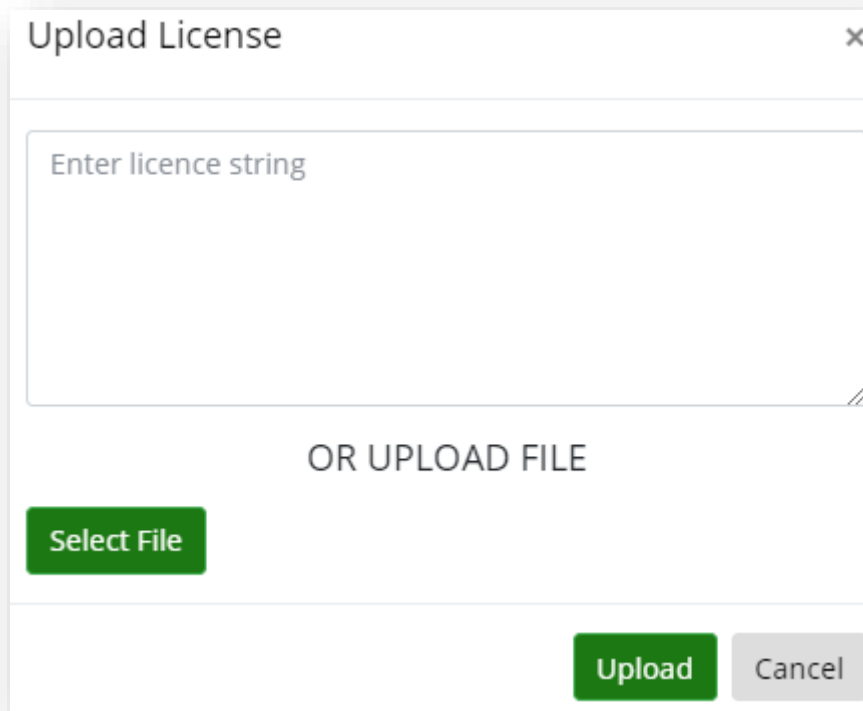
PICTURE 63 HOLIDAY SETTINGS

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

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 64)**.**

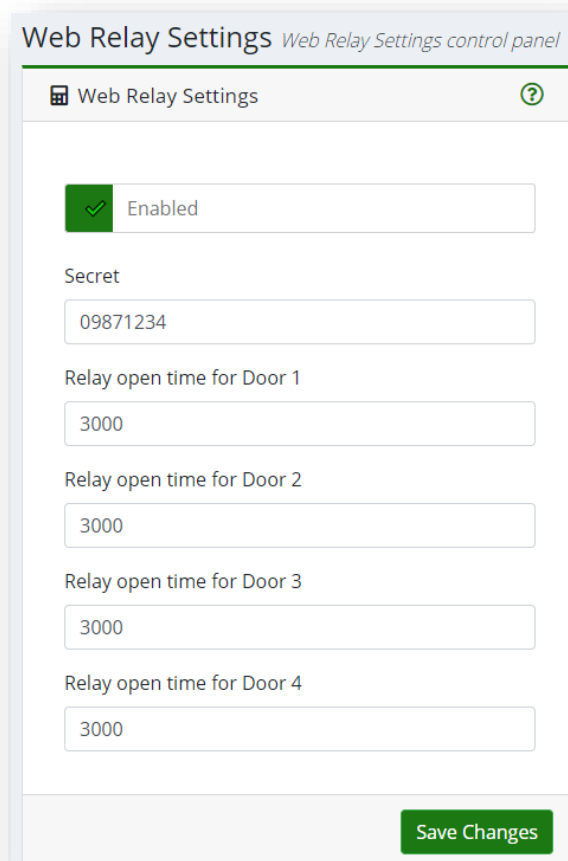**PICTURE 64 UPLOAD LICENSE**

15.10   Web Relay

Web relay option provides remote control. Relay can be turned on or off using web browser or configuring Freund's intercoms such as FE-IPDS-29S to trigger relay with DTMF code it receives.

PICTURE 65 WEB RELAY

Clicking on icon ⊘ in top right corner will open form shown on Picture 66.

Section	Icon	Function
Trigger		Triggers relays and opens door for certain amount of time.
Toggle		Toggles relay to open. Needs to be toggled again to close the door
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.
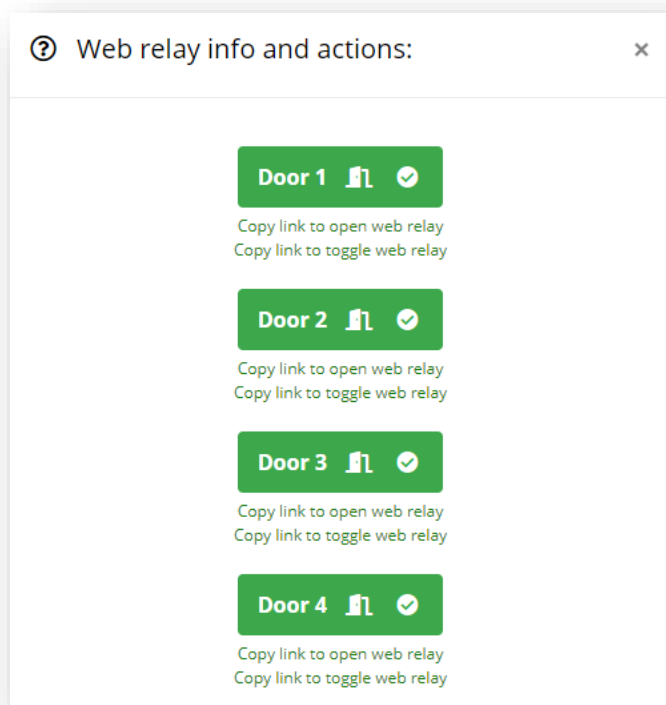
PICTURE 66 WEB RELAY INFO AND ACTIONS

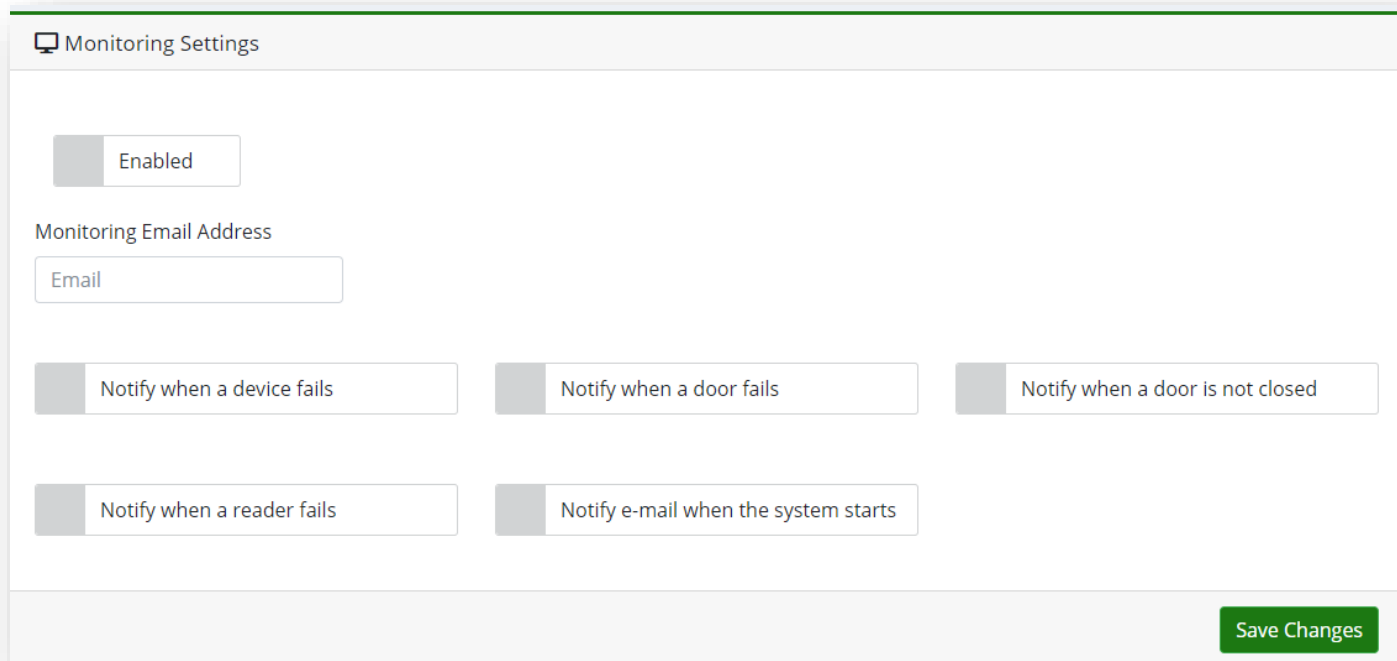## 15.11   Self-Diagnostic Settings

When Self Diagnostic is enabled, system will check itself for any malfunctions at specified time.
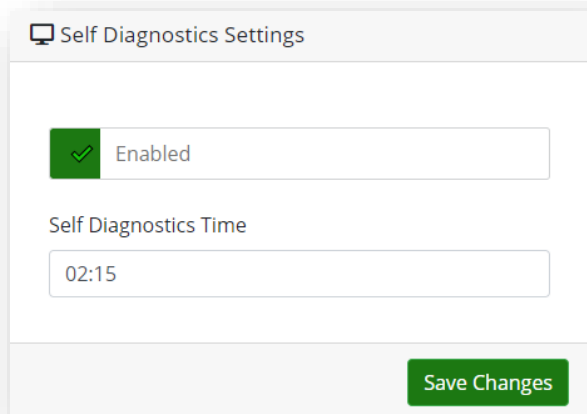
PICTURE 67 SELF DIAGNOSTIC

15.12   Monitoring settings

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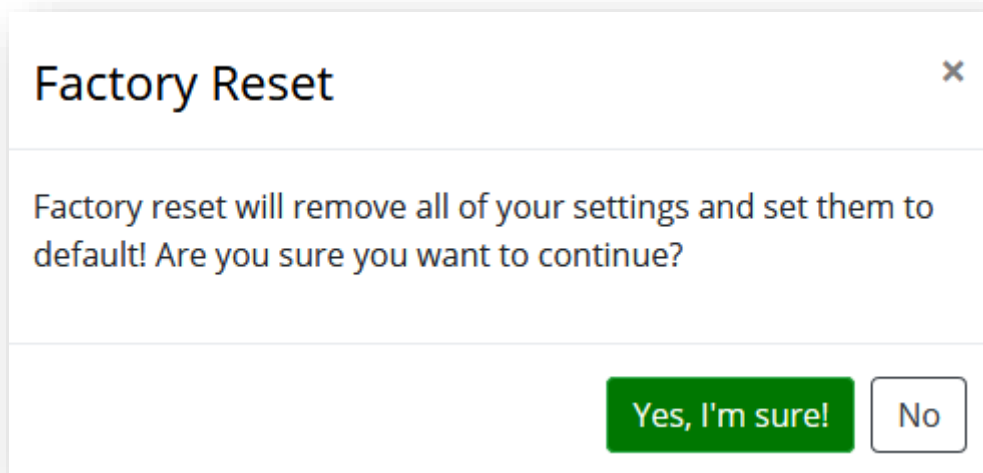

PICTURE 68 MONITORING SETTINGS
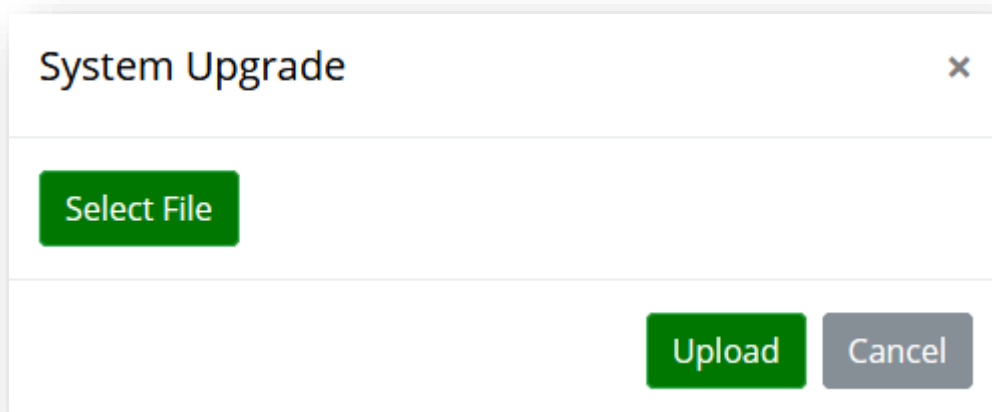
15.13   Factory reset

Resets the device to factory settings.

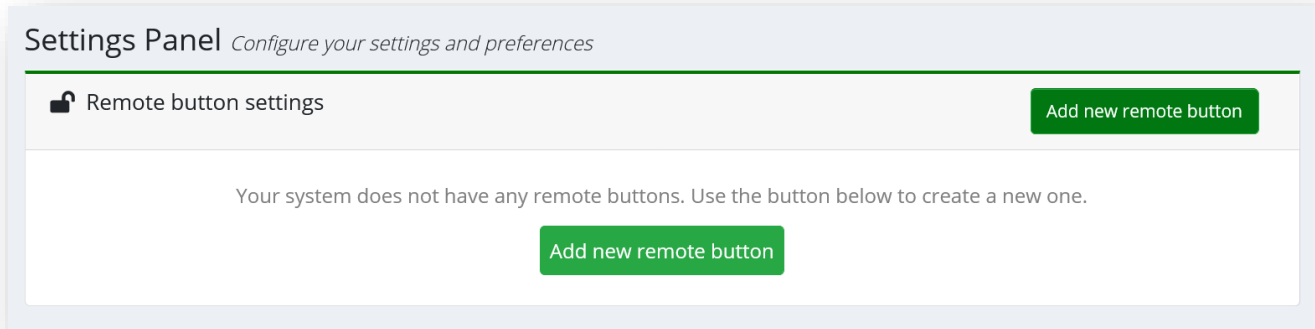**PICTURE 69 FACTORY RESET**

15.14   System Upgrade

Upgrade Access Control software by selecting file.
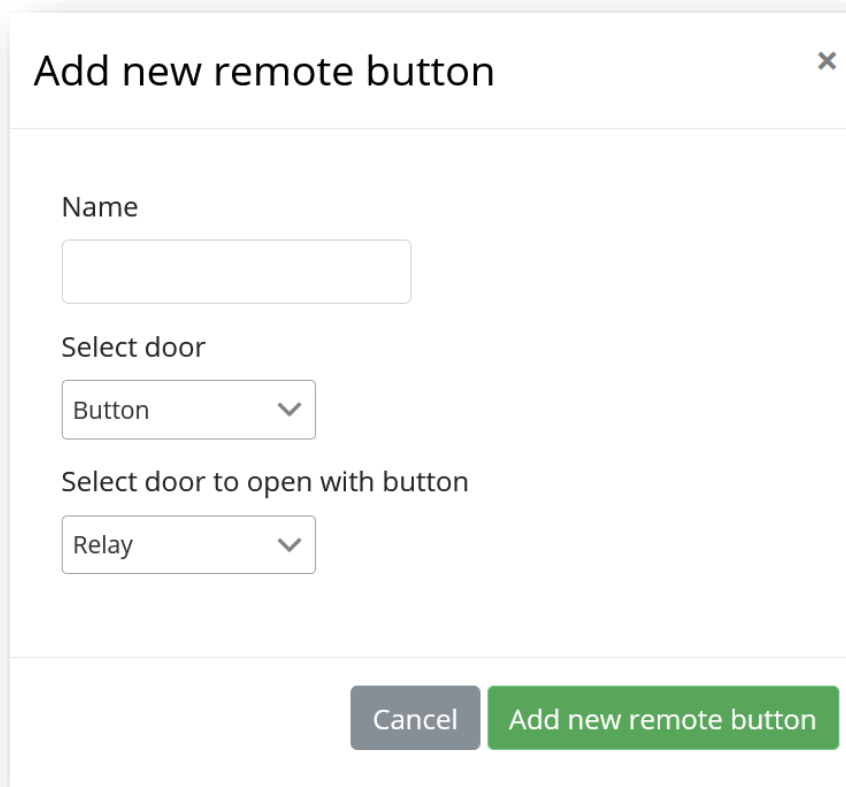

PICTURE 70 SYSTEM UPGRADE

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 documents section 8. Devices).
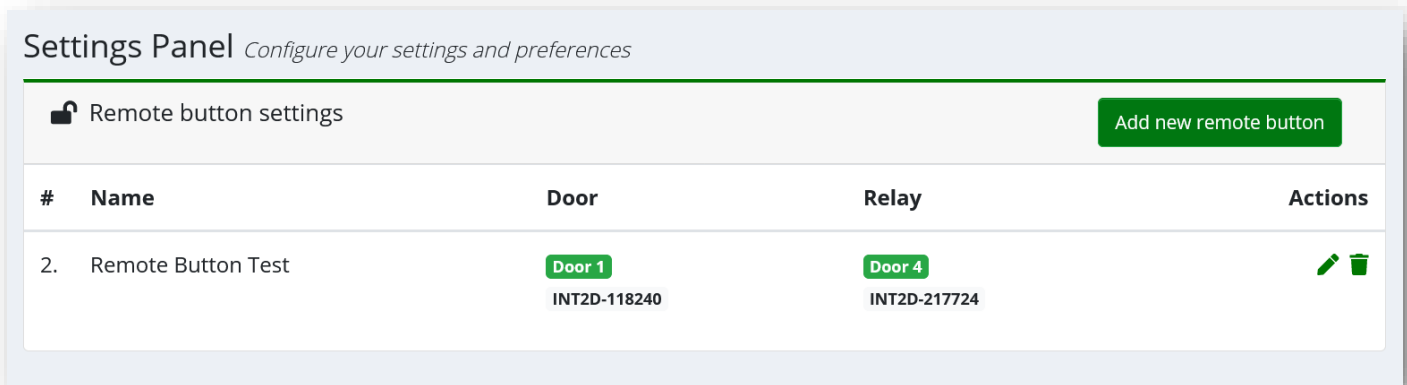

PICTURE 71 REMOTE BUTTON

By clicking on "Add new remote button" (Picture 71), following form will show:

PICTURE 72 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 below.

PICTURE 73 PROPERLY CONFIGURED REMOTE BUTTON

16. System

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