



ACCESS CONTROL V1.15.28

USER MANUAL

FREUND ELEKTRONIKA d.o.o

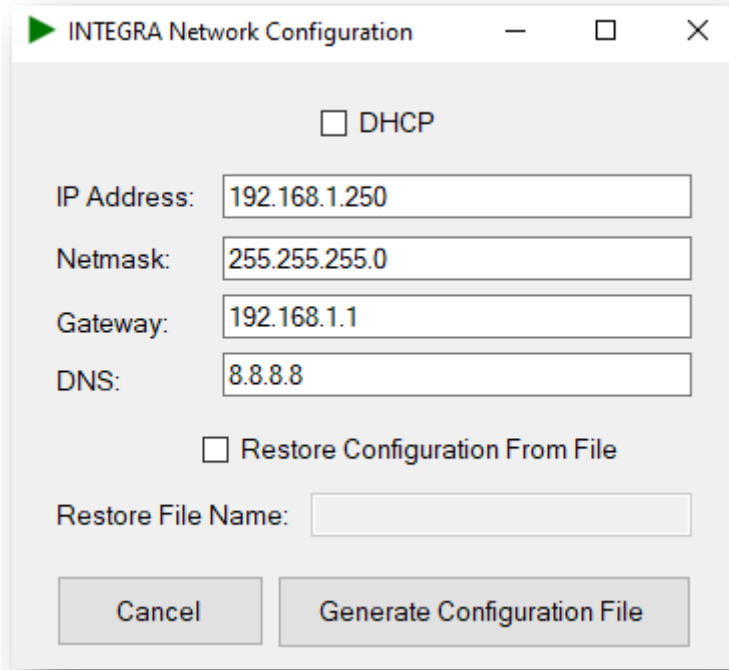
International Burch University | Francuske revolucije bb | 71210 Ilidza | Bosnia and Herzegovina
www.ip-integra.ba | info@ip-integra.com | Tel. +387 33 922 890

CONTENT

1. Product setup	4
2. Log in and Dashboard	5
3. My Profile	7
4. Accounts (SysAdmin, Admin and Manager)	8
5. Mobile devices	11
6. Cards (SysAdmin, Admin and Manager)	13
7. Groups (SysAdmin and Admin)	14
8. Devices (SysAdmin)	15
9. Scheduler (SysAdmin and Admin)	23
10. Elevator Control Module	24
11. Zones (SysAdmin and Admin)	32
12. Access Times (SysAdmin and Admin)	32
13. Access Rules (SysAdmin and Admin)	33
14. Logs	35
15. Settings (SysAdmin)	36
15.1 Cluster Settings	37
15.2 Signal Settings	38
15.3 Backup Settings	39
15.4 Network Settings	40
15.5 System Settings	41
15.6 Email settings	42
15.7 Date - Time Settings	43
15.8 Holiday Settings	44
15.9 Upload License	45
15.10 Web Relay	46
15.11 Self-Diagnostic Settings	47
15.12 Monitoring settings	48
15.13 Factory reset	49
15.14 System Upgrade	49
15.15 Remote Button	50
15.16 iLOQ Settings	52
16. System	53

1. Product setup

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



INTEGRA Network Configuration

DHCP

IP Address: 192.168.1.250

Netmask: 255.255.255.0

Gateway: 192.168.1.1

DNS: 8.8.8.8

Restore Configuration From File

Restore File Name:

Cancel Generate Configuration File

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

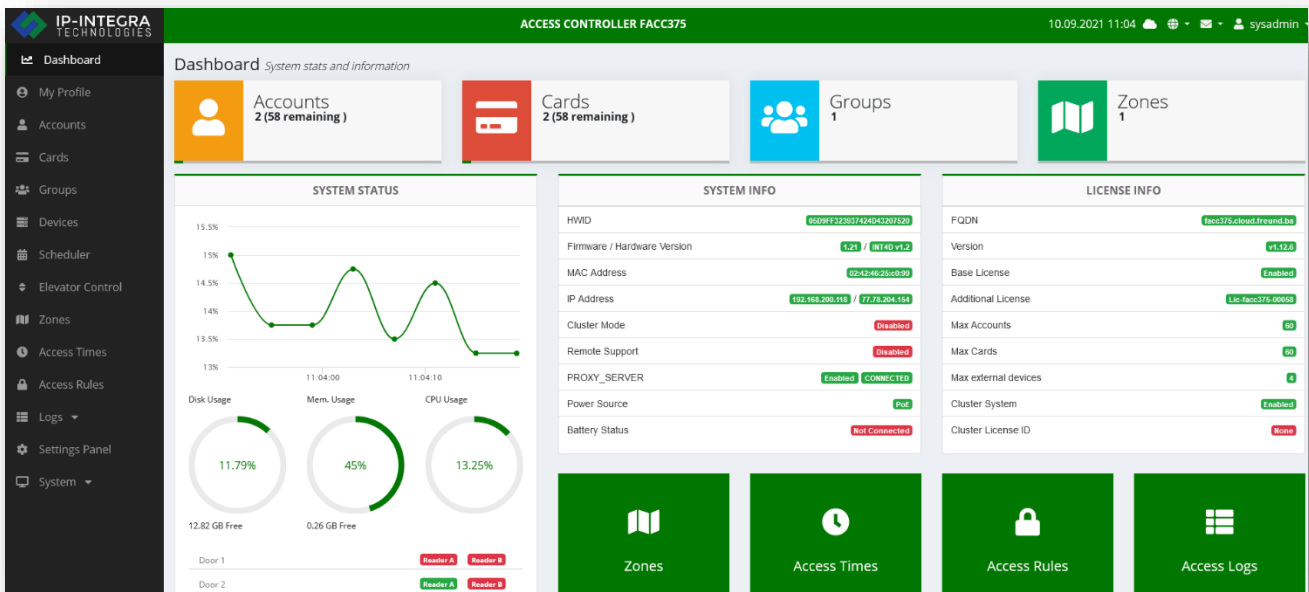


The screenshot shows the login interface for IP-INTEGRA TECHNOLOGIES. At the top left is the logo, which consists of two interlocking squares, one blue and one green. To the right of the logo is the text "IP-INTEGRA TECHNOLOGIES". Below the logo and text are three input fields: the first contains the IP address "192.168.1.250", the second is labeled "Username", and the third is labeled "Password". At the bottom of the form is a green button with the text "Login".

PICTURE 2 LOG IN FORM

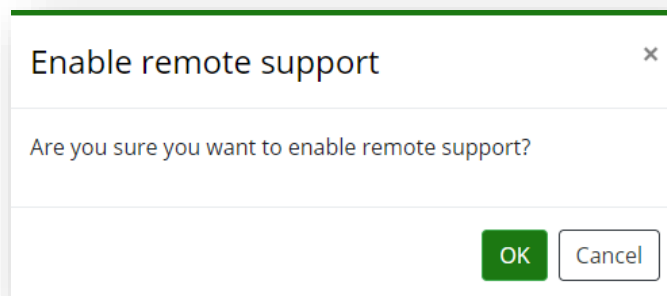
After clicking the **Submit** button, the web interface of the FREUND ACC server will open.

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

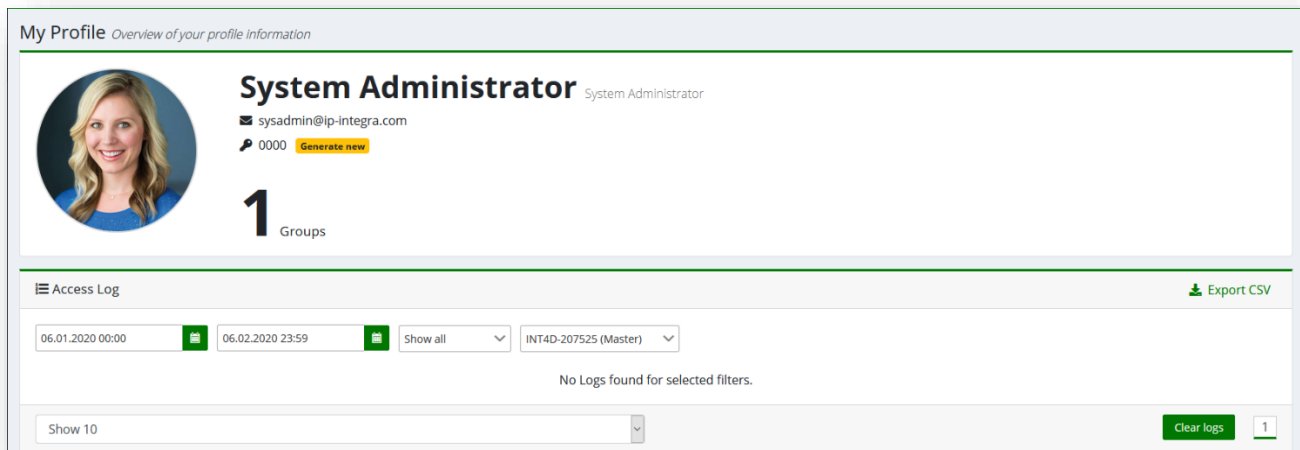
Service “Remote Support” requires your firewall settings not to forbid communication on port 22.

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

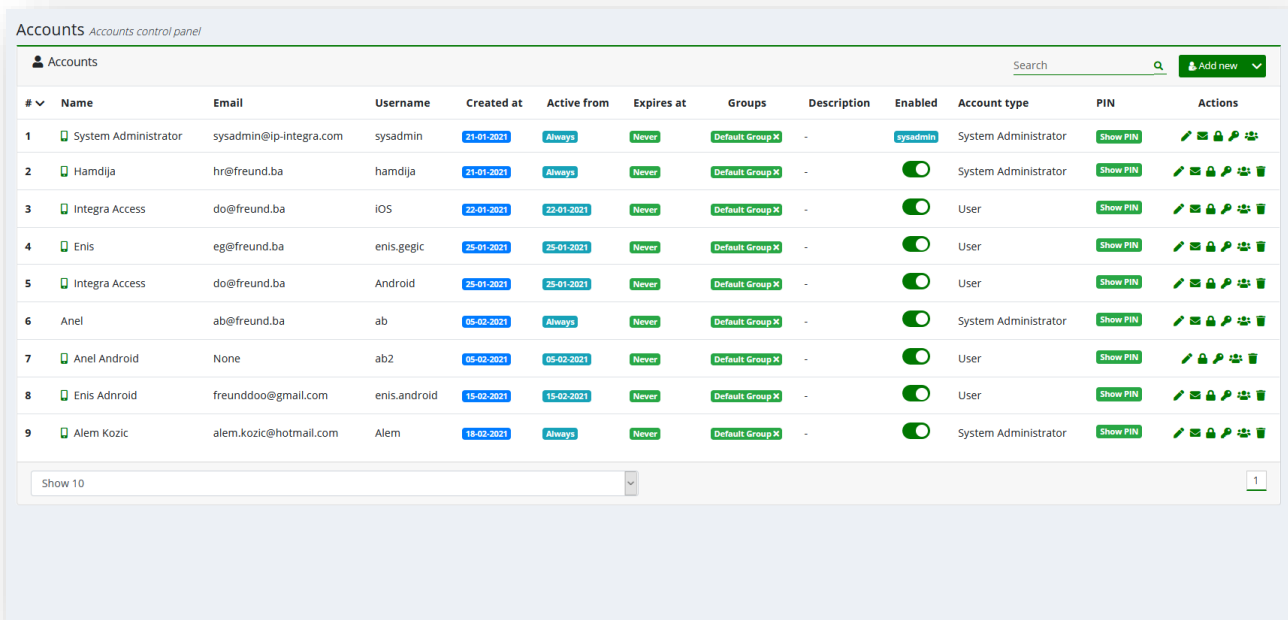
This section provides with information of the user that is currently using the system. Clicking on **Generate new** generates a new PIN code that the user can use for opening doors. **Access log** shows a list of actions done by that user (Picture 5). There are four types of System Access Levels: **System 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).



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.

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 ADD NEW ACCOUNT

A screenshot of a mobile application dialog box titled "Add new card" with a close button (X) in the top right corner. The dialog contains two input fields: the first is labeled "Card Number" and the second is an empty field with a downward arrow on its right side, indicating a dropdown menu. At the bottom of the dialog, there are two buttons: a green "Save Changes" button and a grey "Cancel" button.

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.

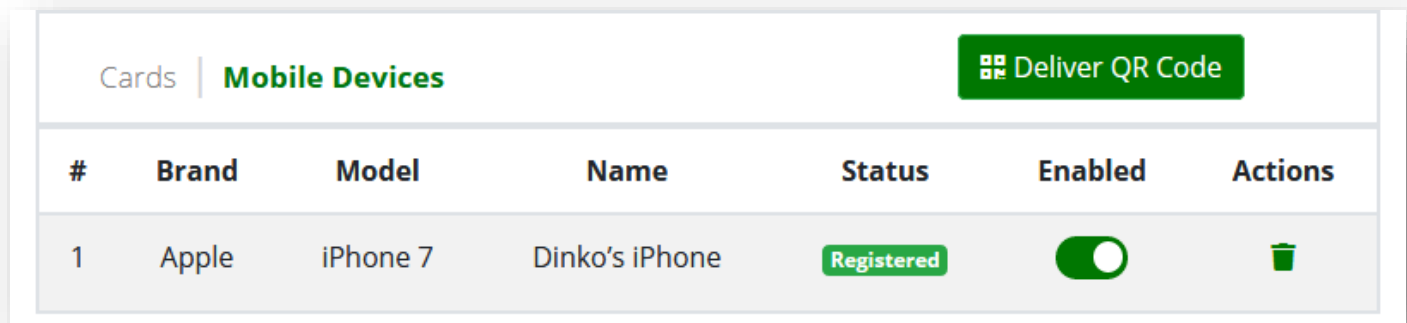
A screenshot of a mobile application dialog box titled "Add new card". On the left side, there is a vertical list of three buttons: "Scan Card", "Scan Again", and "Done", each with a circular arrow icon. On the right side, the text "Scan your card" is displayed above a green icon of a hand holding a card towards a target symbol. At the bottom right of the dialog, there are two buttons: a green "Save Changes" button and a grey "Cancel" button.

PICTURE 9 CARD SCANNING

5. Mobile devices

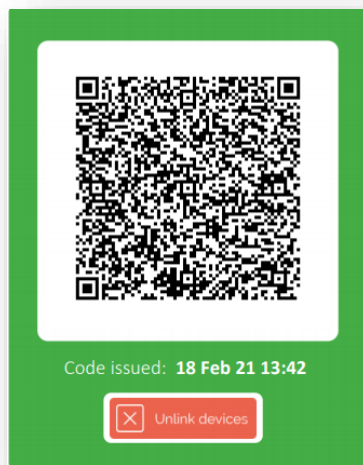
From version 1.12, the Access Control system will support the use of mobile devices with the IP-INTEGRA Access mobile application.

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).

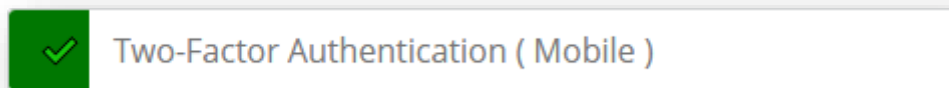
Once the code is scanned you will be able to use the IP-INTEGRA application. If two-factor authentication is enabled, you will be required to input a six-digit code that will be delivered to your e-mail address (Picture 12).



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.

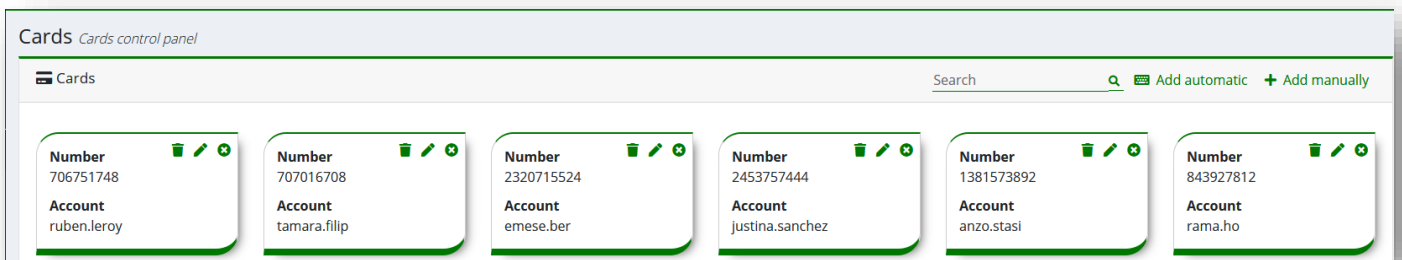
Enable or disable two-factor authentication you need to open the 'System settings' panel and click the button shown in picture 13.



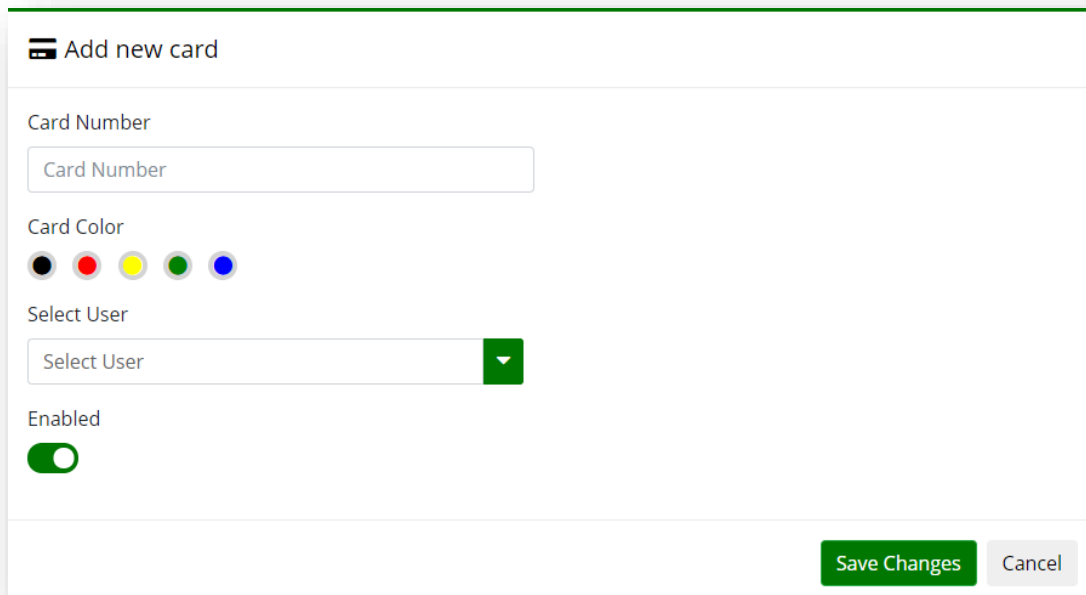
PICTURE 13 MANAGING TWO-FACTOR AUTHENTICATION

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**.

Group *Groups control panel*

#	Name	Accounts	Actions
1	Default Group	sysadmin X	
2	Full access	daniel.nicolosi.ceo X	
3	Employees	joel.lau X rut.dever X priya.hlav X emese.ber X dimitri.stef X justina.sanchez X alberta.iliev X anzo.stasi X rama.ho X danny.shea X stephen.mcafee X cari.salvatici X tamsyn.simonson X mehrab.kir X judith.te X	
4	Sales	joel.lau X rut.dever X agus.dreir X justina.sanchez X alberta.iliev X anzo.stasi X rama.ho X danny.shea X stephen.mcafee X	

PICTURE 16 GROUPS

Add new group X

Name

Save Changes
Cancel

PICTURE 17 ADD NEW GROUP

8. Devices (SysAdmin)

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

Devices *Overview of connected devices*

Type	Device Name	Host Name	IP Address	Cluster Info	Version	Doors	Status	Actions					
	INT2D-118240 <small>This device</small>	facc321	192.168.200.131 <small>77.78.204.154</small>	SA	v1.11.3	First Floor - East First Floor - West	OK						
				Reader A		Reader B							
				Door	Power	Type	Keypad	Tamper	Type	Keypad	Tamper	Zones	Actions
				First Floor - East	✓	Wiegand 34	✗	✗	Wiegand 34	✗	✗	First Floor X	
				First Floor - West	✓	Wiegand 34	✗	✗	Wiegand 34	✗	✗	First Floor X	

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, allows you to select a replacement controller

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.

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

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: 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).

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:

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

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

PICTURE 19 MANUALLY ADD EXTERNAL DEVICE

The screenshot shows the "Add external device" form with the "From Network" tab selected. It displays a table of five devices that have been discovered on the network. Each row includes a device ID, type, IP address, MAC address, and a refresh button.

ID	Type	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 20 ADD EXTERNAL DEVICE FROM NETWORK

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 the 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.

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

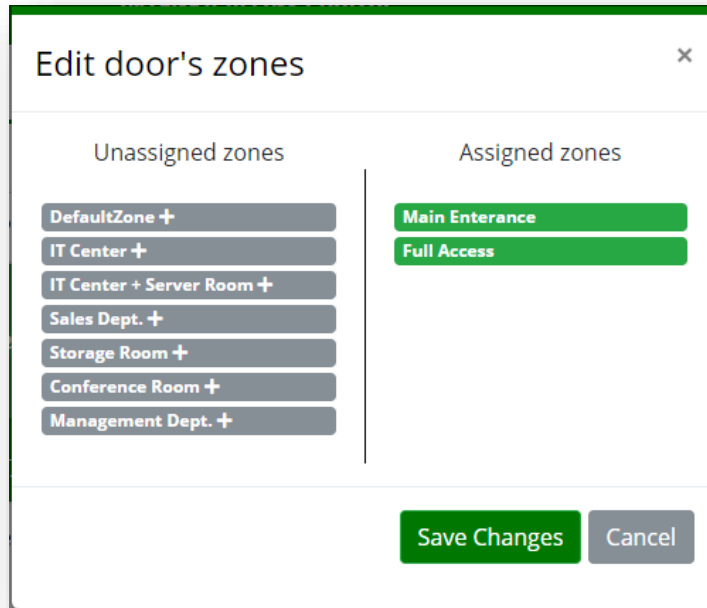
PICTURE 22 EDIT DOOR

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).

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

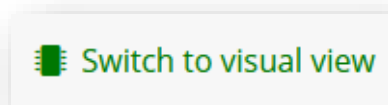
Relay open time: 2111
Pin Input Timeout: 5000
Button On Threshold:
Door Not Closed Alert:
Door Not Closed Timeout: 10000

PICTURE 23 EXIT BUTTON CONFIGURING

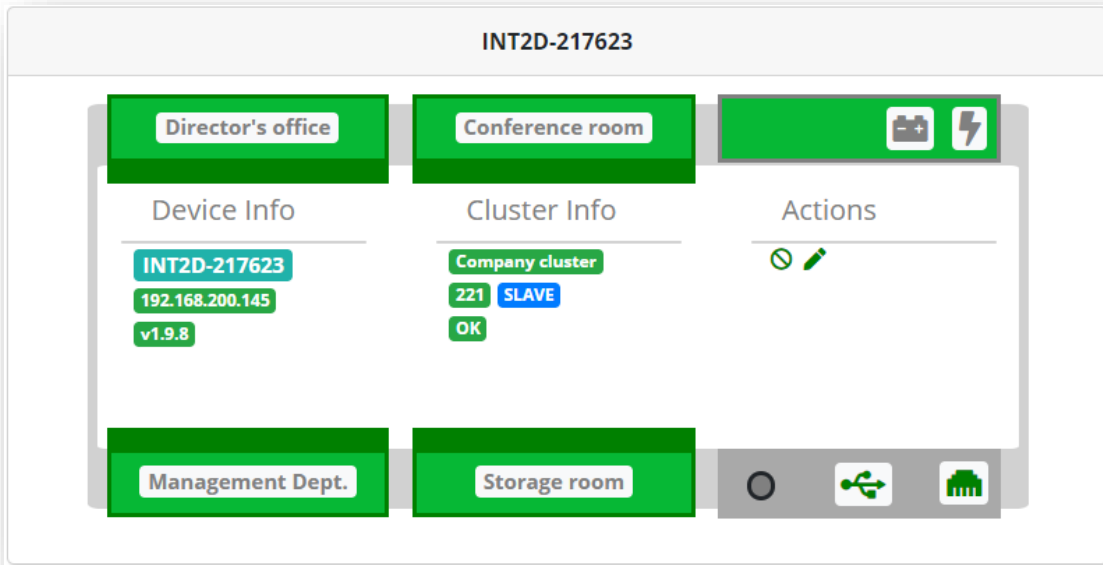


PICTURE 24 EDIT DOOR'S ZONES

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.

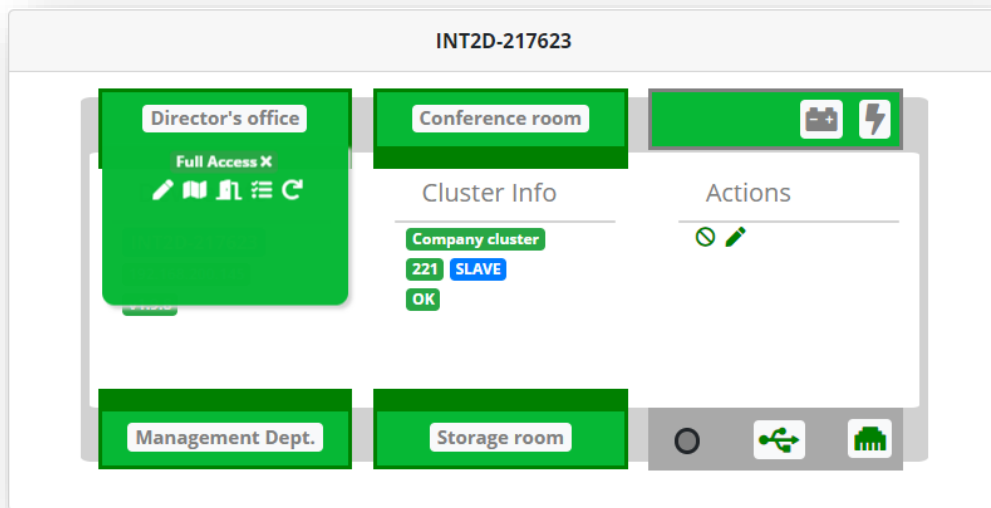


PICTURE 25 VISUAL VIEW BUTTON



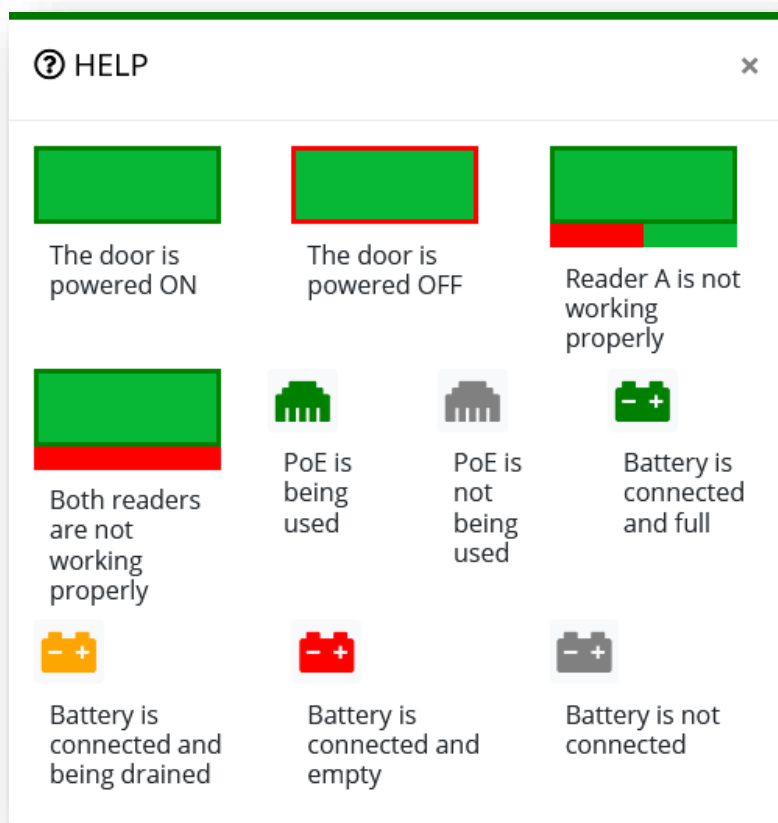
PICTURE 26 VISUAL VIEW OF A SINGLE DEVICE

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

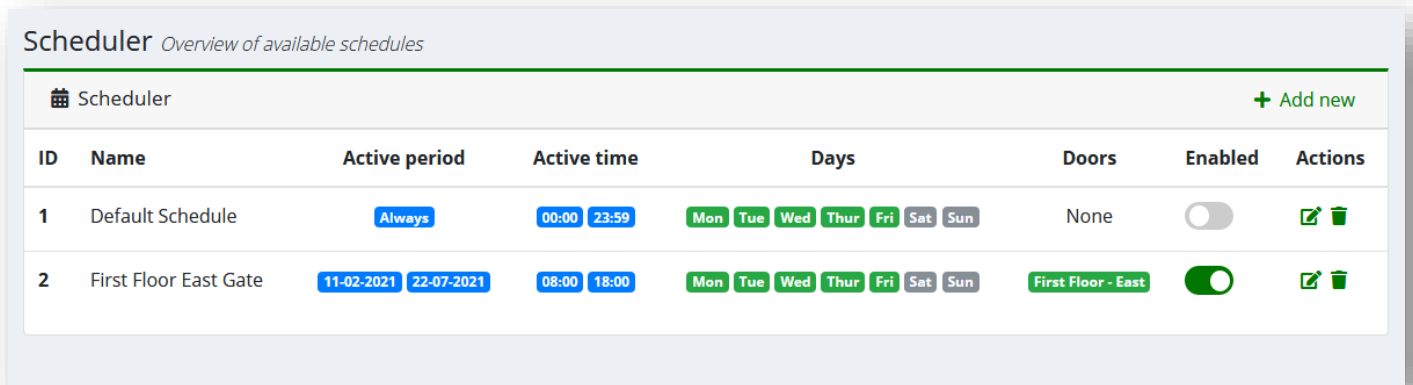
For an easier understanding, next to the view button, the user can find a help button which explains the state of the device components, as shown in Picture 28.



PICTURE 28 HELP WINDOW

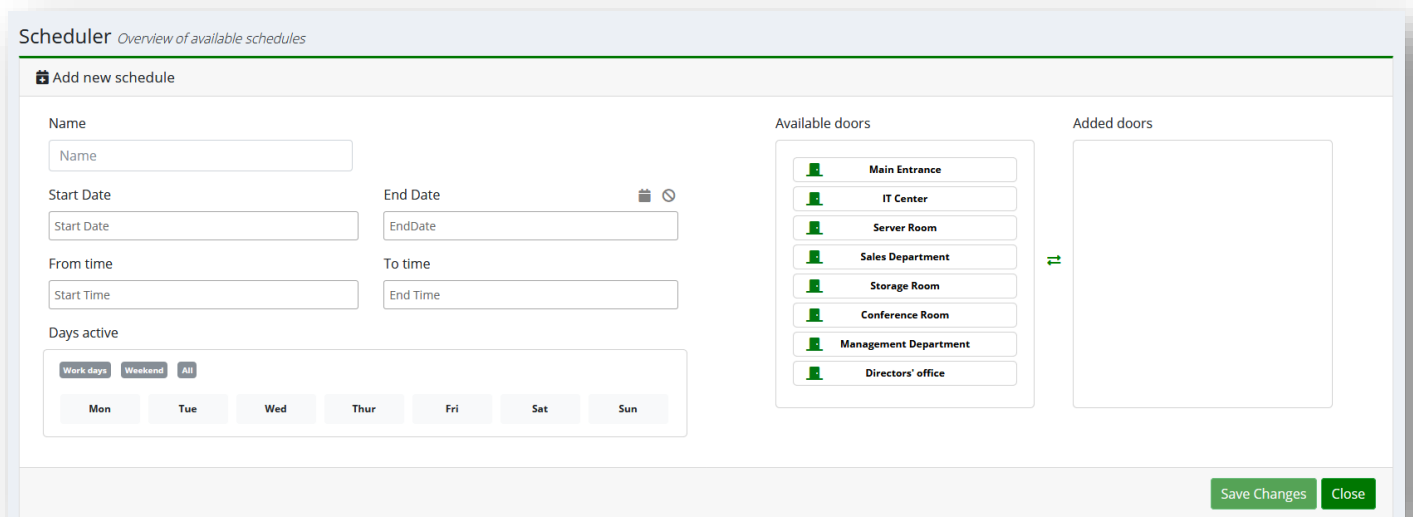
9. Scheduler (SysAdmin and Admin)

The **Scheduler** feature is used to assign doors to remain open 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'.

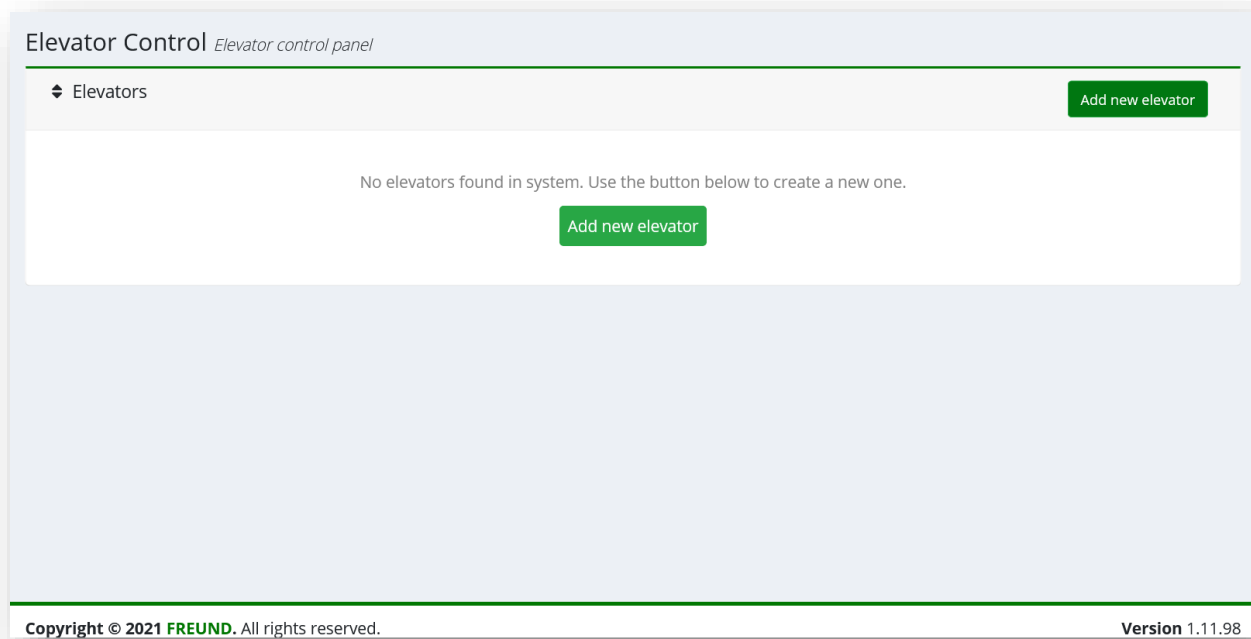
On the right side, you select the doors to which the scheduler will apply. All these settings can be changed later by pressing the 'Edit' Button on the Scheduler panel.

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

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

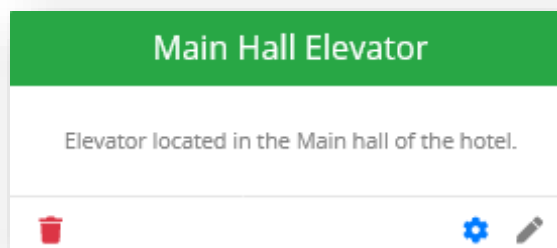
Click on „**Add new elevator**“ button shown in the Picture 32 and fill out the required fields.

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:



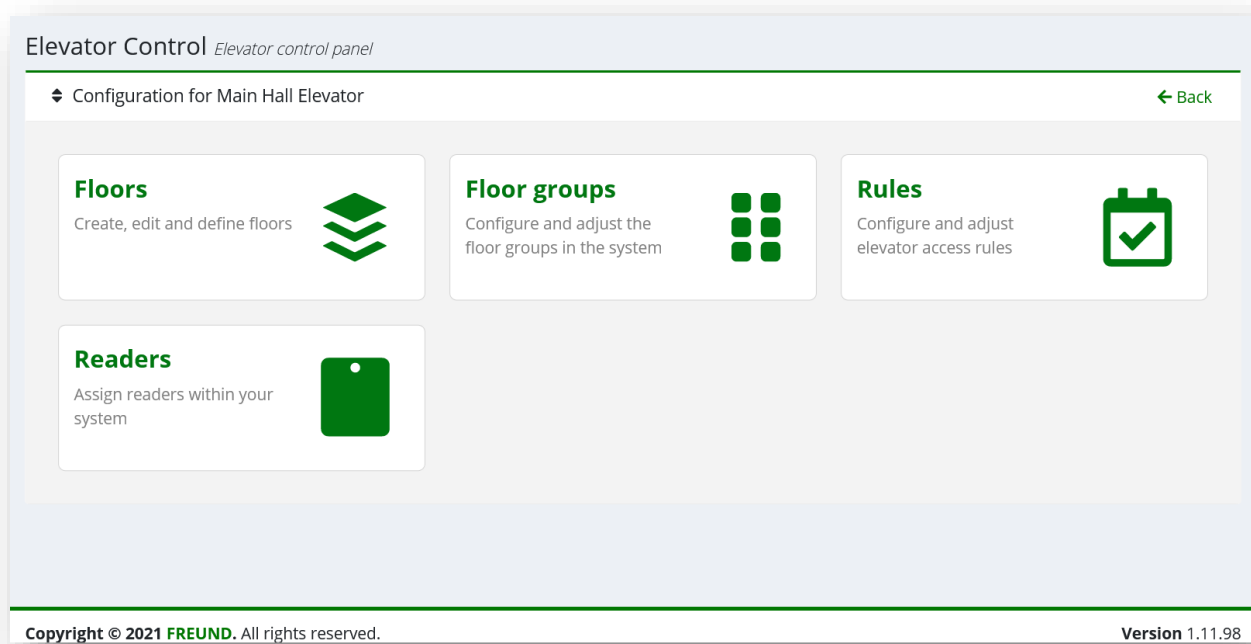
PICTURE 33 CREATED ELEVATOR

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.

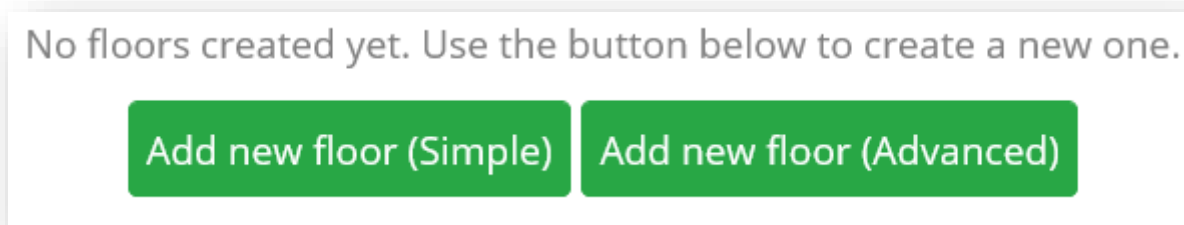
Following screen will show:



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).

Floor configuration for Main Hall Elevator + Add new floor (Simple) + Add new floor (Advanced) ← Back

#	Name	Device	Readers	Groups	Actions
1.	-1 Spa & Wellness	INT4D-195331	A B	VIP+ VIP	
2.	0 Ground floor	INT4D-195331	A B	Default VIP+ VIP	
3.	1 Rooms	INT4D-195331	A B	Default VIP+ VIP	
4.	2 Lounge	INT4D-195331	A B	VIP+	

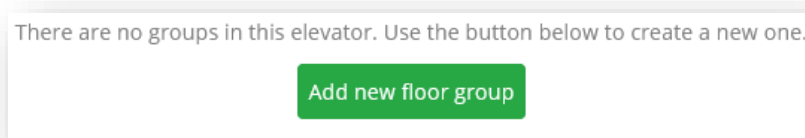
Back

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.

A white 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 gray "Cancel" button.

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.

A white 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 gray buttons with plus signs: "Spa & Wellness +" and "Lounge +". Under "Assigned floors", there are two green buttons: "Ground floor" and "Rooms". At the bottom right, there are two buttons: a gray "Cancel" button and a green "Save Changes" button.

PICTURE 41 ASSIGNING FLOORS TO THE FLOOR GROUPS

When you have finished adding the needed groups, 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	✎ + 🗑

PICTURE 42 SHOWING THE FLOOR GROUPS LIST

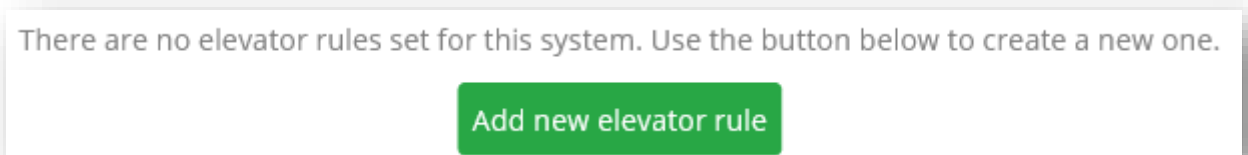
You can add as many groups as you need.

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.

Configuration for Main Hall Elevator					+ Add new elevator rule ← Back
#	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	

Back

PICTURE 45 ELEVATOR RULES LIST

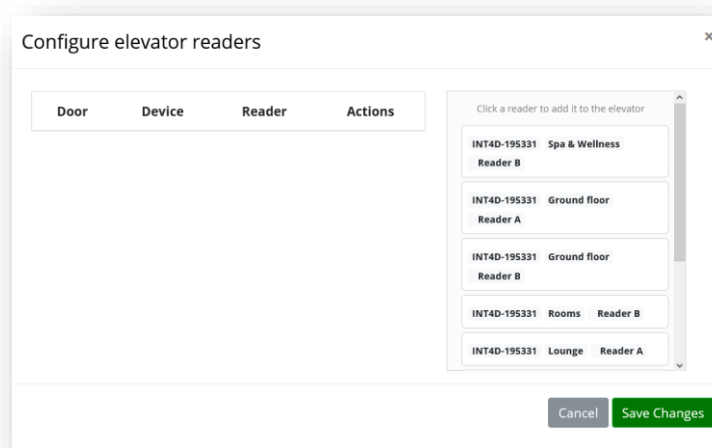
For easier tracking, we have named the **Floor Groups** and **User Groups** with same names.

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.

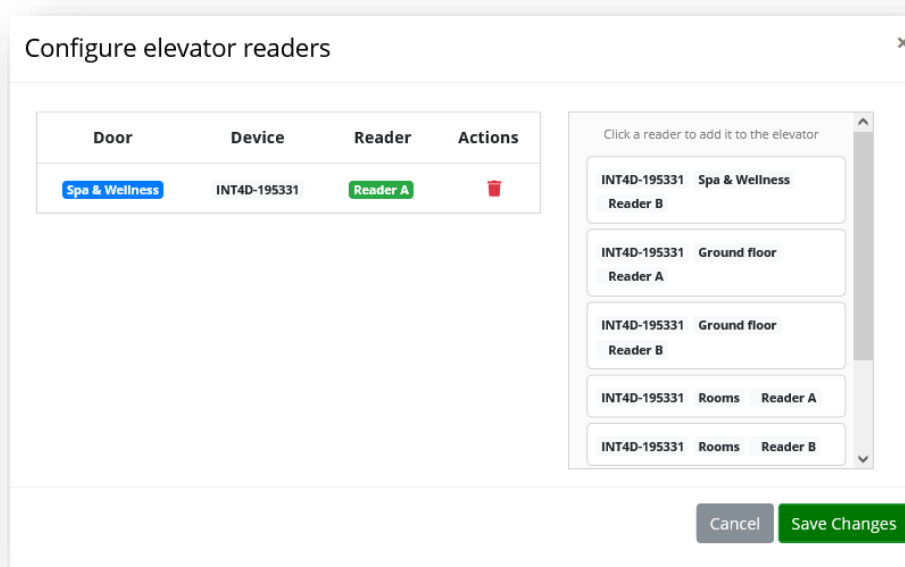
Only thing left now is to assign the reader to the elevator.

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.

11. Zones (SysAdmin and Admin)

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

Zones *Zones control panel*

Zones		+ Add new										
#	Name	Doors										Actions
1	Default Zone	Door 1 X	Door 2 X	Door 1 X	Door 2 X	Door 1 X	Door 2 X	Door 1 X	Door 2 X	Door 3 X	Door 4 X	

PICTURE 48 ZONES

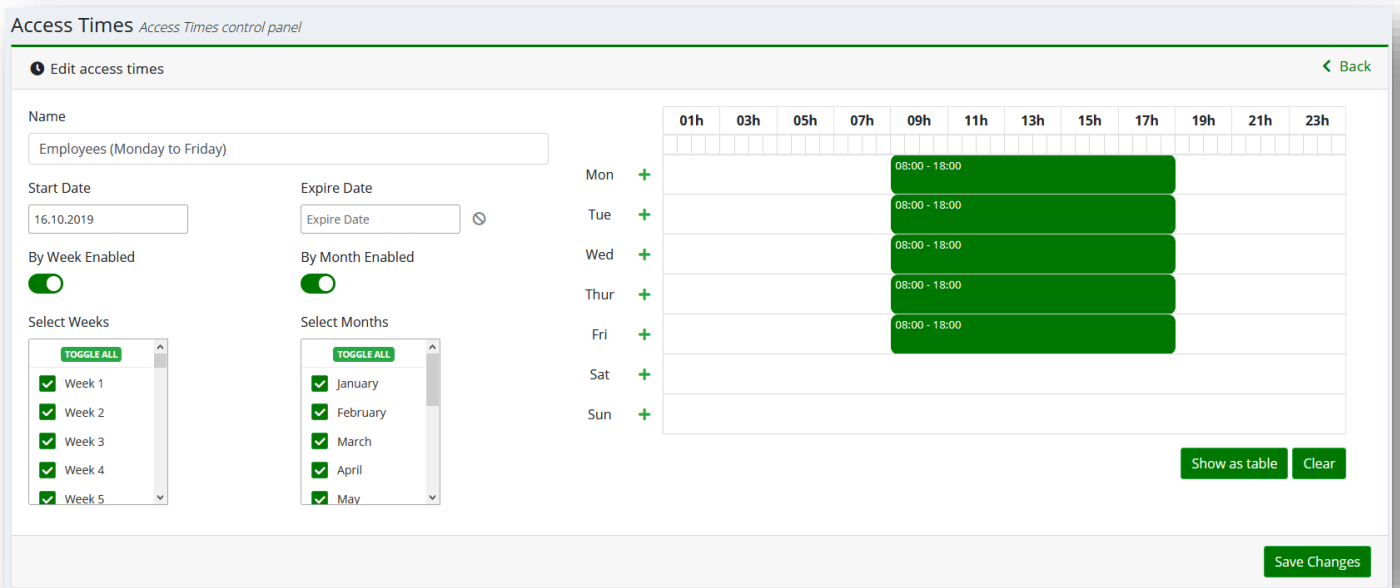
12. Access Times (SysAdmin and Admin)

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

Access Times *Access times control panel*

Access Times		+ Add new			
#	Name	Type	Start Date	Expire Date	Actions
1	Default Access Time	AccessTimeByWeek	01.01.2019		

PICTURE 49 ACCESS TIMES



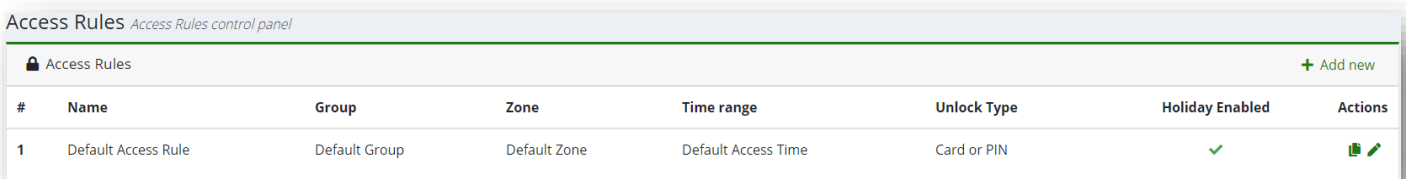
PICTURE 50 NEW ACCESS TIME

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

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).

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 53 SYSTEM LOG

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 ▼ Keyword Search

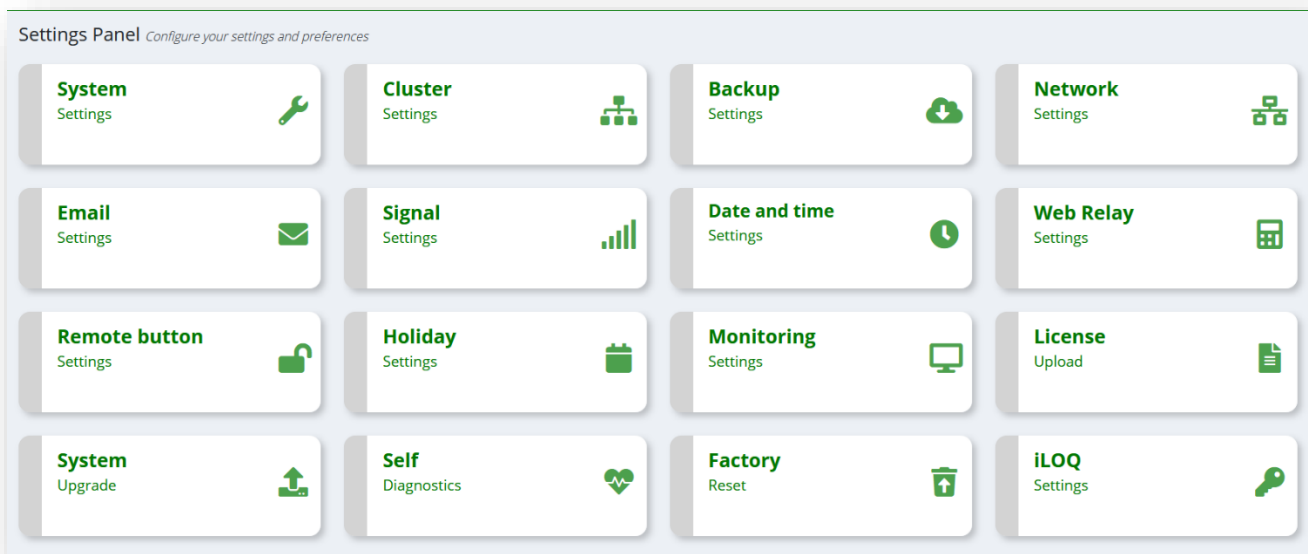
Date	Event	Access	Zone Name	Door Number	Reader	Card	PIN	Account Name	Snapshots
2/22/2021, 10:47:44 AM	Card	Granted	IT + Server Room	3 Server Room	B	571821060		oly.er	Disabled
2/22/2021, 10:47:36 AM	Card	Granted	Main Entrance	1 Main Entrance	A	707405572		joel.we	Disabled
2/22/2021, 10:47:05 AM	Card	Granted	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

PICTURE 54 ACCESS LOG

15. Settings (SysAdmin)

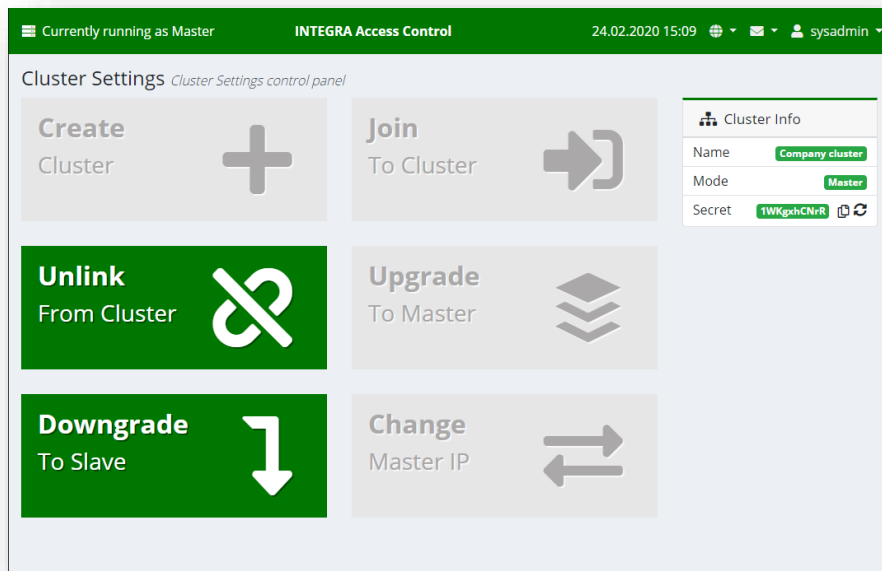
Settings panel allows modifying: **System Settings, Cluster Settings, Backup Settings, Network Settings, Email Settings, Signal Settings, Date-Time Settings, Web Relay Settings, Remote Button, Holiday Settings, Monitoring Settings, Upload License, System Upgrade, Self-Diagnostics, Factory Reset and iLOQ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



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:

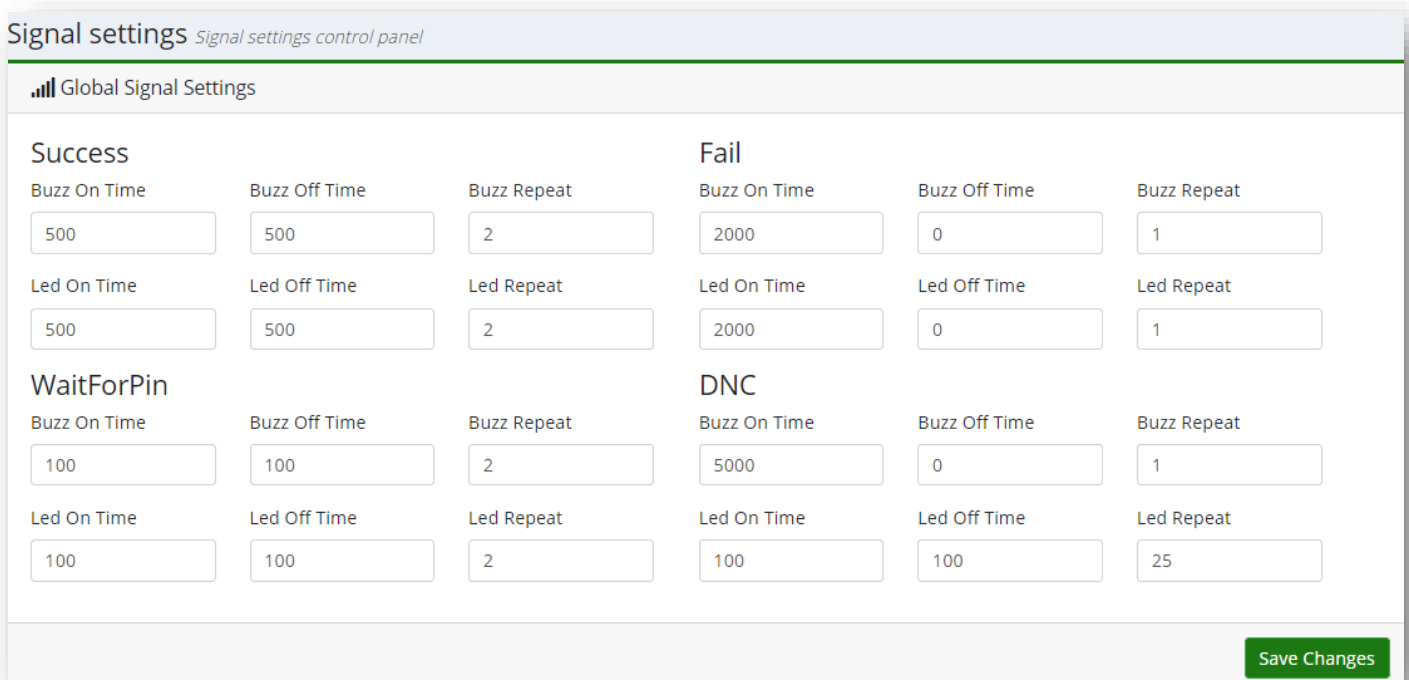
Name	Icon	Function
Create cluster	Create Cluster	Creates cluster and makes device Master device
Join cluster	Join To Cluster	Allows device to join cluster by entering Cluster Join Secret and Cluster Master device IP
Unlink from cluster	Unlink From Cluster	Unlinks device from cluster
Upgrade to master	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

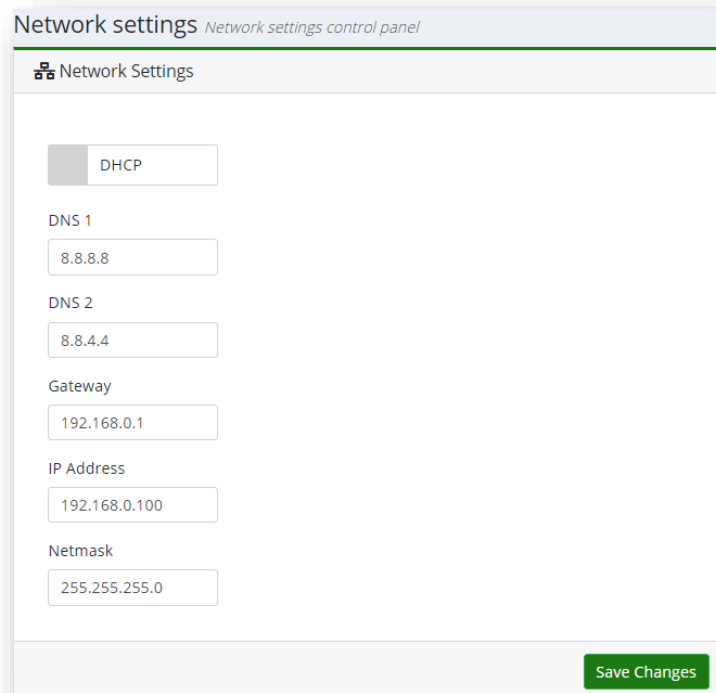
Backups *Backups control panel*

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 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).



The screenshot shows a web interface titled "Network settings" with the subtitle "Network settings control panel". Below the title is a section labeled "Network Settings" with a gear icon. The settings are as follows:

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

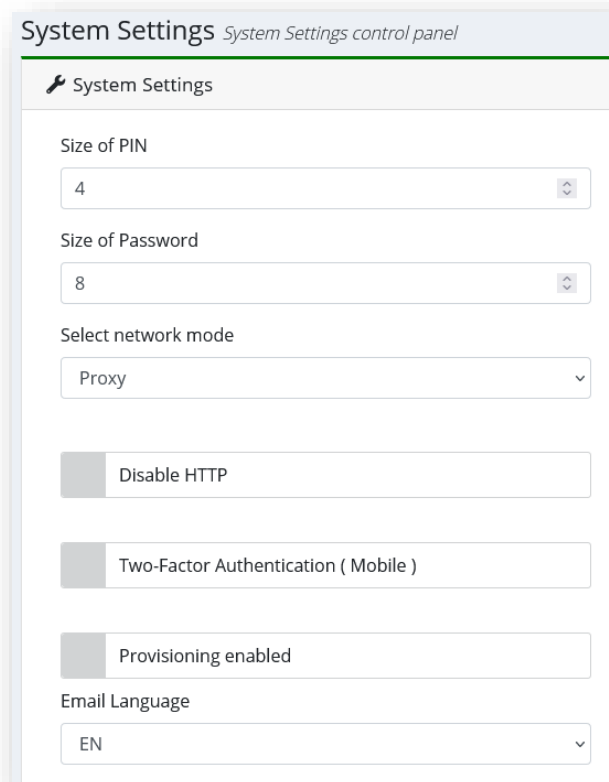
A green "Save Changes" button is located at the bottom right of the form.

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).

Send welcome e-mail when a user is created

Custom Email Settings

HOST

Port

587

Email

Username

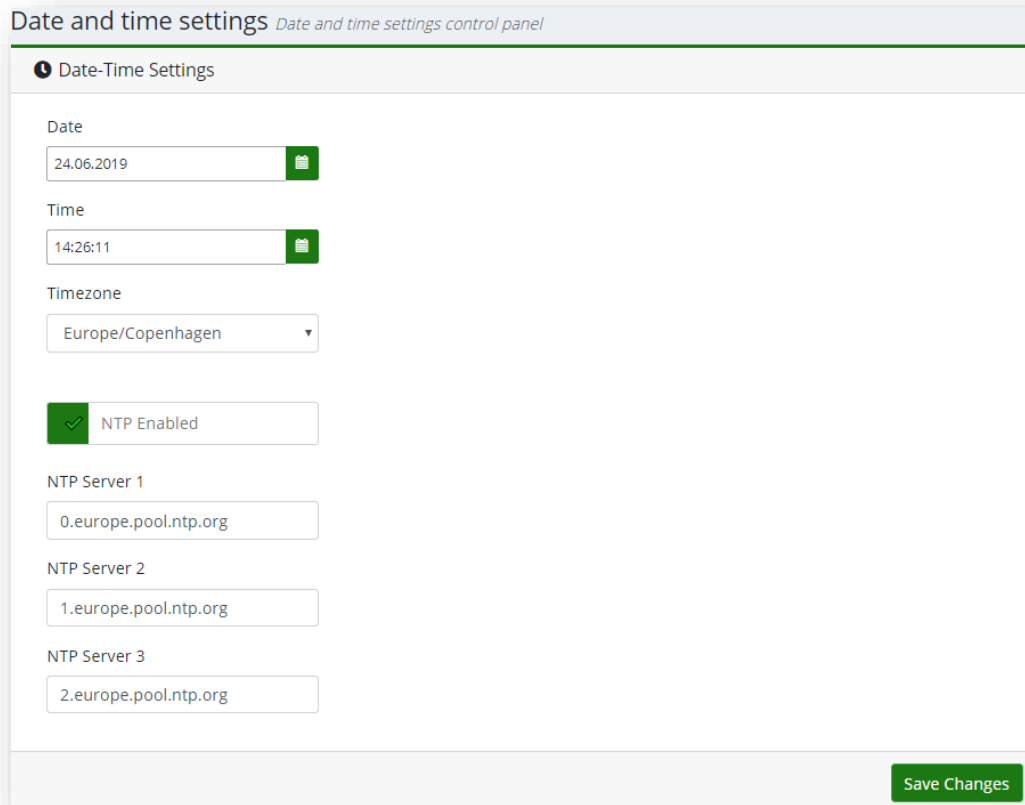
Password

SSL

PICTURE 61 EMAIL SETTINGS

15.7 Date – Time Settings

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



The screenshot shows a web interface titled "Date and time settings" with a subtitle "Date and time settings control panel". The main content area is titled "Date-Time Settings" and contains the following fields:

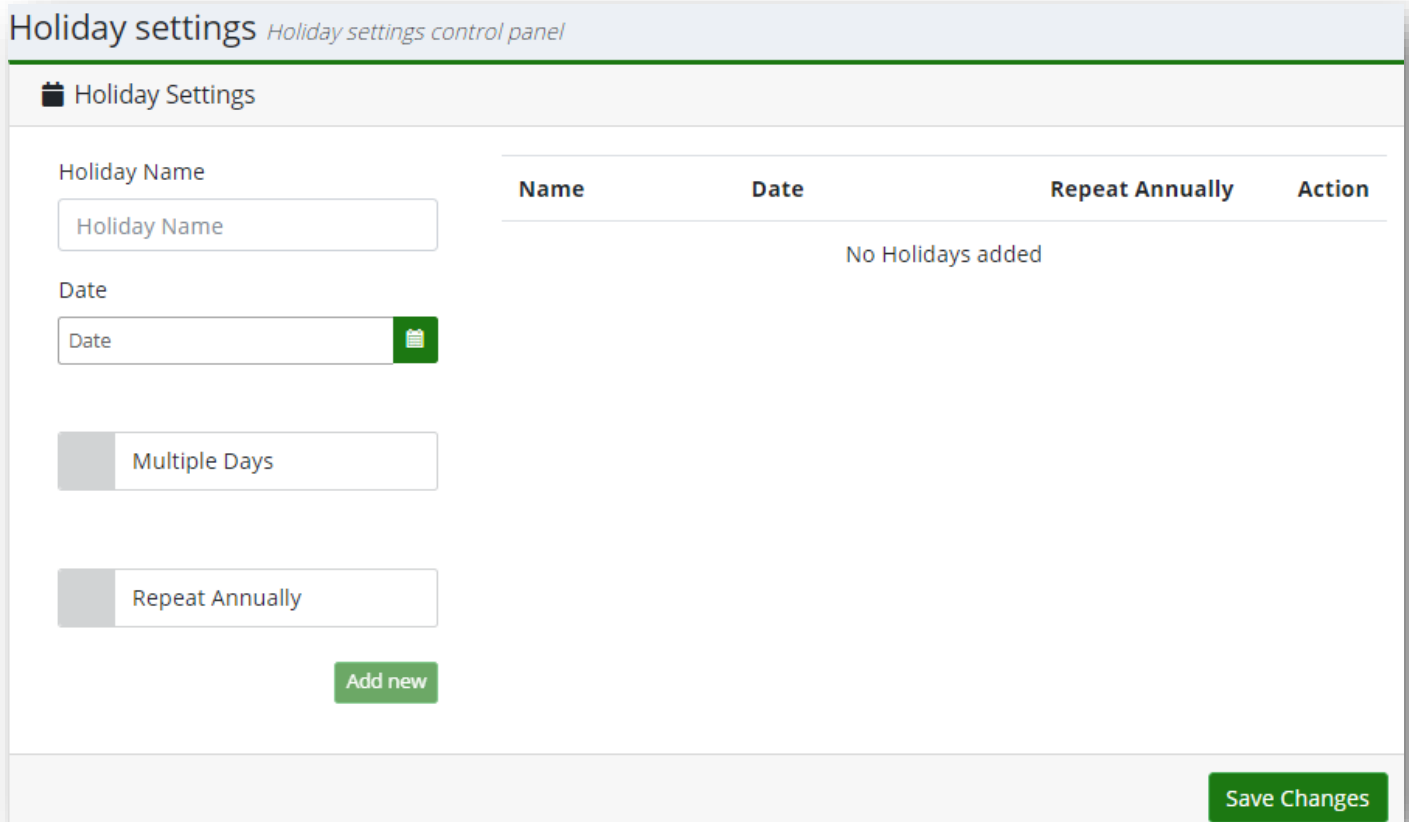
- Date:** A text input field containing "24.06.2019" with a calendar icon to its right.
- Time:** A text input field containing "14:26:11" with a calendar icon to its right.
- Timezone:** A dropdown menu currently showing "Europe/Copenhagen".
- NTP Enabled:** A checkbox that is checked, with the text "NTP Enabled" to its right.
- NTP Server 1:** A text input field containing "0.europe.pool.ntp.org".
- NTP Server 2:** A text input field containing "1.europe.pool.ntp.org".
- NTP Server 3:** A text input field containing "2.europe.pool.ntp.org".

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

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**.

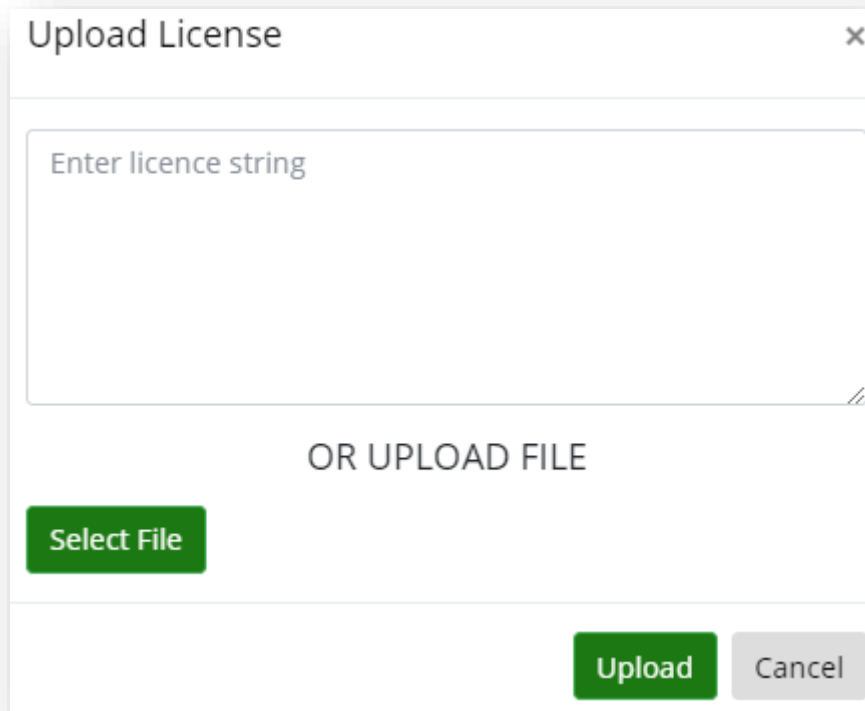


PICTURE 63 HOLIDAY SETTINGS

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).



Upload License

Enter licence string

OR UPLOAD FILE

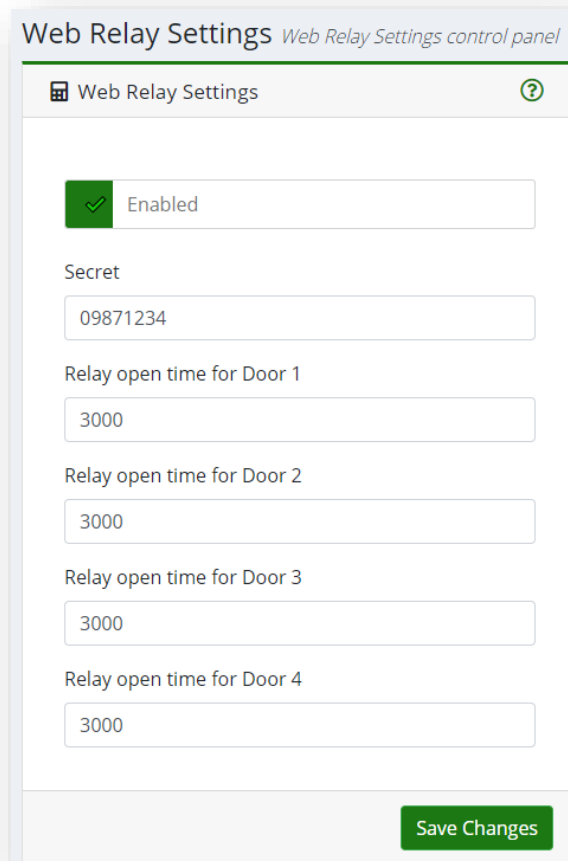
Select File

Upload Cancel

PICTURE 64 UPLOAD LICENSE

15.10 Web Relay

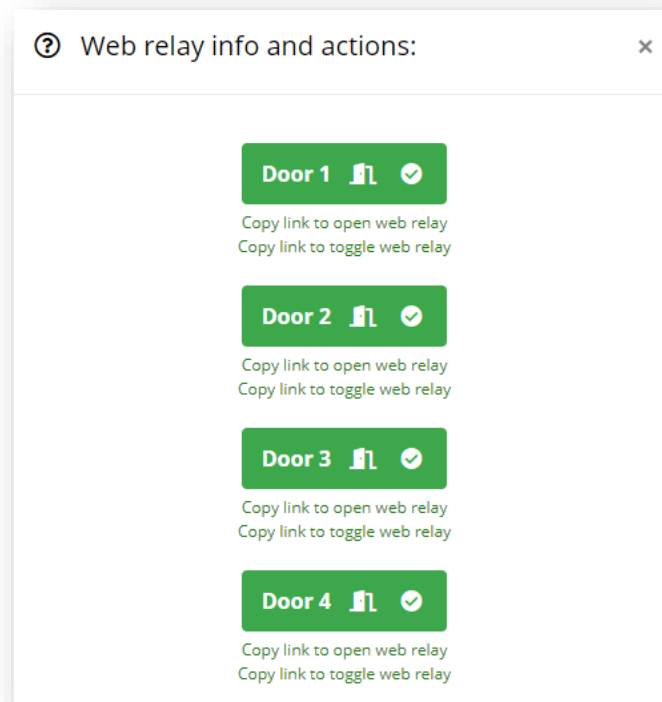
Web relay option provides remote control. Relay can be turned on or off using web browser or configuring Freund's intercoms such as FE-IPDS-29S to trigger relay with DTMF code it receives.



PICTURE 65 WEB RELAY

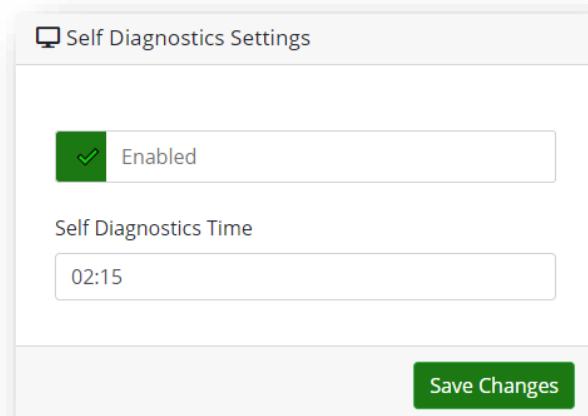
Clicking on icon in top right corner will open form shown on Picture 66.

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

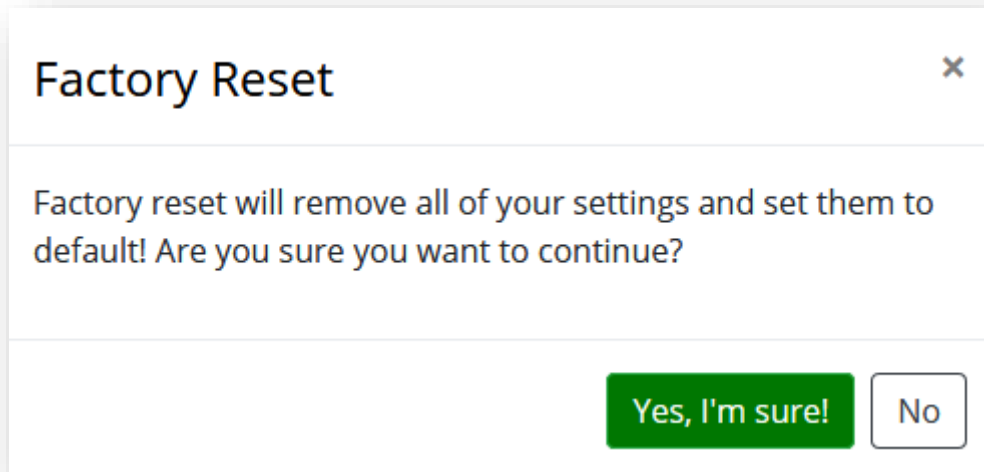
Monitoring settings allow notifying through email when device fails, door fails, door is not closed, reader fails and when system restarts.

The screenshot shows a web interface titled "Monitoring Settings". At the top left, there is a toggle switch labeled "Enabled". Below this is a text input field for "Monitoring Email Address" containing the value "ab@freund.dk". The main area contains seven toggle switches for various notification events: "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". All these switches are currently turned on. A green "Save Changes" button is located in the bottom right corner of the form.

PICTURE 68 MONITORING SETTINGS

15.13 Factory reset

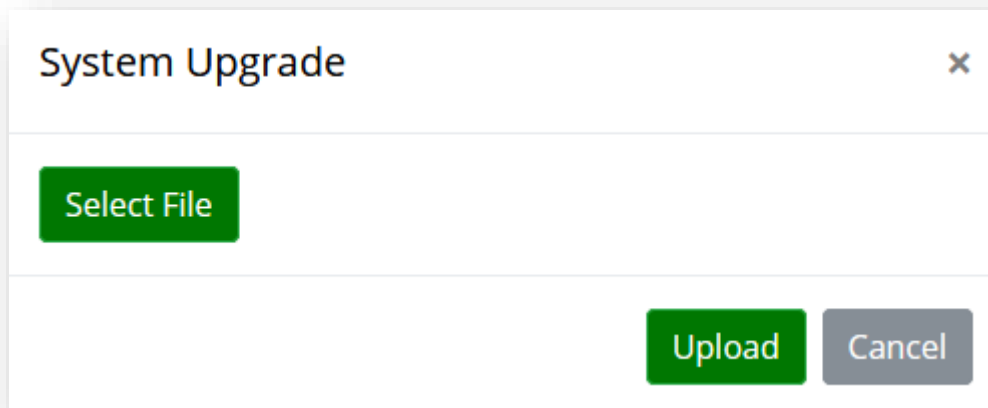
Resets the device to factory settings.



PICTURE 69 FACTORY RESET

15.14 System Upgrade

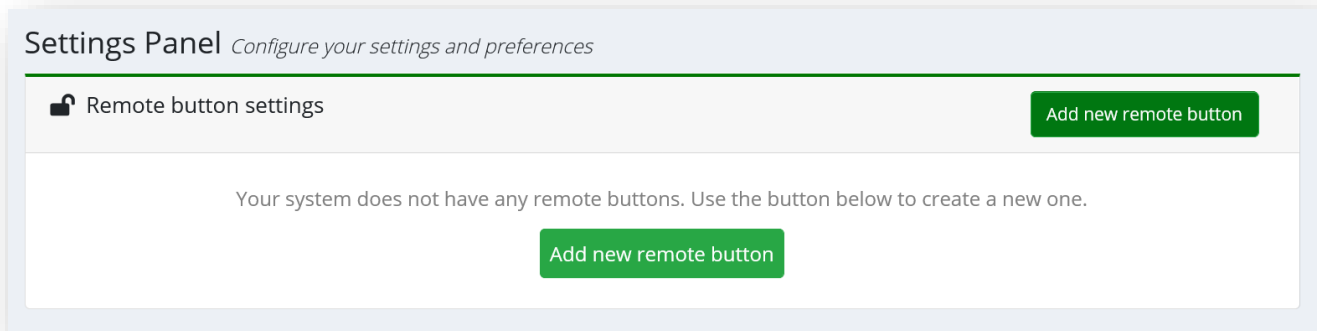
Upgrade Access Control software by selecting file.



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:

The form is titled 'Add new remote button' and includes a close button (X) in the top right corner. It contains the following fields:

- Name:** A text input field.
- Select door:** A dropdown menu with 'Button' selected.
- Select door to open with button:** A dropdown menu with 'Relay' selected.

At the bottom of the form, there are two buttons: a grey 'Cancel' button and a green 'Add new remote button' button.

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.

Settings Panel *Configure your settings and preferences*

Remote button settings Add new remote button

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

PICTURE 73 PROPERLY CONFIGURED REMOTE BUTTON

15.16 iLOQ Settings

IP-INTEGRA ACC has been integrated with iLOQ's S5 product lineup. This gives FREUND offline solution for the ACC system.

The screenshot shows the 'iLOQ Settings Control Panel' with the following fields:

- iLOQ Settings:** A green checkmark icon and the text 'Enabled'.
- Get URL API:** A text input field containing 'iLOQ Service address'.
- Username:** A text input field containing 'Username'.
- Password:** A text input field containing '*****'.
- Customer Code:** A text input field containing 'ILOQ_XXXX'.
- Lock Group:** A dropdown menu with 'Freund API Demo' selected.
- Save Changes:** A green button at the bottom right.

PICTURE 74 ILOQ SETTINGS

To link our ACC controller to the iLOQ system, fill out the required fields shown in Picture 74. 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 has been changes made in the iLOQ Manager.

16. System

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