

# Nova 2.3 software

## Administrator manual



Monitoring



Users & Access Rights



Hardware



Diagnostics



Info Boards



Personal Settings



Documents



Messages



Settings



## Table of Contents

1	Login page .....	9
1.1.1	Account types.....	10
2	Home page and main navigation .....	12
2.1	Account settings.....	14
2.2	Creating user widgets .....	16
3	Monitoring widget .....	18
3.1	Events widget .....	18
3.1.1	Event history .....	18
3.1.2	Manage error and warning events .....	19
3.2	Locations & Doors .....	20
3.2.1	Location management .....	22
4	Users and Access rights.....	24
4.1	Users.....	24
4.2	New users.....	25
4.2.1	Adding unknown card(s) to user.....	26
4.2.2	Card function assignment .....	26
4.2.3	Managing users, their access rights and apartments .....	28
4.2.4	Custom user preview.....	31
4.2.5	Importing users from .CSV or Excel file.....	32
4.2.6	Custom user search.....	32
4.2.7	Card authorization.....	33
4.3	Access groups widget .....	35
4.4	Managing time schedules .....	37
5	Hardware .....	40
5.1	Centrals.....	40
5.1.1	Searching and managing centrals in Local Area Network (LAN) .....	40
5.1.2	Changing a central's IP address.....	41
5.1.3	How to connect centrals over the internet using remote IP, DNS or DDNS.....	42
5.1.4	Central's WLAN settings.....	43
5.1.5	Adding, removing and editing centrals .....	45
5.1.6	Replacement of malfunctioning slave central .....	46
5.1.7	Replacement of malfunctioning master central.....	48
5.1.8	Central settings.....	48
5.1.9	Upgrade software on central .....	51
5.1.10	Communication based on IP address .....	52
5.1.11	Communication based on RS-485 BUS .....	52

5.1.12	Database synchronization .....	53
5.1.13	Adding new readers .....	54
5.1.14	Upgrading firmware on reader .....	54
5.1.15	Reader settings.....	55
5.1.16	Door settings.....	59
5.1.17	Scheduled door opening .....	62
5.1.18	Local Anti-Passback.....	62
5.1.19	Alarm, tamper and additional relays management.....	65
5.2	Offline readers .....	67
5.2.1	Offline readers and maintenance cards .....	71
5.2.2	Creation of configuration cards for offline devices in Nova software.....	72
5.2.3	Lost and blacklisted cards .....	73
5.2.4	Reading events from offline devices.....	74
5.2.5	Configuration of online reader settings for writing access rights .....	74
5.2.6	Offline readers and Nova software.....	75
5.2.7	Battery level on offline cylinders.....	75
5.2.8	Changing batteries in offline devices.....	75
5.2.9	Offline device feedback .....	77
5.2.10	Card segments of offline reader .....	78
5.2.11	Blacklist settings .....	79
5.2.12	Offline authentication keys.....	79
5.3	Special hardware devices .....	80
5.3.1	GSM Gateway .....	80
5.3.2	Remote control Reader .....	81
5.3.3	IP Camera .....	81
6	Settings.....	85
6.1	Add-ons and Modules.....	85
6.1.1	Online system registration .....	86
6.1.2	Offline system registration .....	87
6.2	Login Settings .....	88
6.3	Database Settings.....	89
6.3.1	Automatic database backup .....	89
6.3.2	Event archive.....	90
6.4	Other Settings.....	91
6.4.1	Time zone .....	91
6.4.2	Web server port.....	91
6.4.3	Security settings .....	91
6.4.4	Email and SMTP server settings.....	92
6.4.5	System PIN settings .....	93
6.4.6	Show IP camera picture.....	93
7	Module: Scripting .....	95

7.1	Writing EX FU modules .....	95
7.1.1	EX FU module installation .....	95
7.2	Custom EX FU events .....	97
7.2.1	Custom events editor .....	97
7.2.2	Adding new custom event.....	99
7.2.3	Editing and deleting custom events .....	100
7.2.4	Dispatching/assigning custom events.....	100
7.2.5	Built-in events .....	101
7.3	Simple alarm integration .....	102
7.3.1	System prerequisites and alarm script installation .....	102
7.3.2	Access group configuration .....	102
7.3.3	Activation of alarm .....	103
7.3.4	Deactivation of alarm .....	104
8	Module: Door stations .....	105
8.1	Door station module setup .....	105
8.2	Door station manager popup window .....	106
8.3	Managing apartments .....	106
8.3.1	Adding apartments.....	106
8.3.2	Editing apartment .....	107
8.3.3	Removing apartments .....	108
8.3.4	Sending messages to apartments .....	108
8.4	Door station management .....	109
8.4.1	Adding door stations .....	109
8.4.2	Editing door station.....	110
8.4.3	Removing door stations .....	111
8.4.4	Preview of door station information .....	111
8.4.5	Assigning apartments to the door station .....	112
8.4.6	Updating content on door station .....	113
8.5	Assigning apartments to the users .....	113
8.5.1	Advanced text manipulation .....	114
9	Module: Mailboxes .....	116
9.1	Managing mailbox units .....	116
9.2	Assigning mailboxes to apartments .....	117
9.3	Setting reader to work with the mailbox .....	118
9.4	Creating and assigning mailbox access rights .....	118
10	Module: Floor plan .....	120
10.1	Managing floor plans.....	120

10.2	Floor plan hardware.....	120
10.3	Floor plan navigation .....	121
11	Module: Presence.....	123
11.1	Managing presence places.....	123
11.2	Managing users in places .....	124
12	Module: Wireless online.....	126
12.1	Offline to online reader conversion.....	126
12.1.1	Advanced view.....	127
12.2	Removing function from wireless online readers.....	128
12.3	Wireless online reader functionalities.....	129
13	Module: Booking .....	130
13.1	Booking access groups.....	130
13.2	Reservation creation and cancellation in Booking module.....	132
13.3	Booking as a terminal application.....	134
14	Module: List Editor .....	138
14.1	Module installation and location .....	138
14.2	Management of different lists .....	139
14.2.1	User lists .....	139
14.2.2	Readers list .....	140
14.3	Assigning local administrators and their lists .....	140
15	Module: Card designer.....	142
15.1	Designing a card .....	142
15.2	Card layouts.....	143
15.3	Additional user fields.....	143
16	Module: Info boards.....	146
16.1	Info board driver .....	146
16.1.1	Info board driver settings .....	147
16.2	Info board layouts .....	148
16.3	Assigning layouts to info board drivers .....	152
16.4	Sending message to info board driver .....	152
17	Module: High security module .....	153
17.1	Uploading custom certificates .....	154
17.2	Custom certificates removal.....	154
17.3	Providing a secure connection between centrals.....	155

18	Module: Fire alarm module .....	156
18.1	Setting up alarm to affect only one central .....	156
18.2	Setting up global alarm .....	156
18.3	Setting up custom alarm .....	156
19	Module: Checkpoint.....	158
19.1	Setting up stationary checkpoint .....	158
19.2	Setting up mobile checkpoint.....	159
20	Special hardware.....	160
20.1	Elevator controller .....	160
20.1.1	Elevator reader setup .....	160
20.1.2	Setting up elevator destinations .....	160
20.1.3	Setting up access groups and access rights .....	161
20.2	FireAlpha .....	162
20.3	Parking controller .....	162
20.4	Nexus MO .....	163
20.4.1	Upgrading Nexus MO readers.....	163
20.4.2	Nexus MO PIN .....	163
20.4.3	On-board buttons.....	163
20.4.4	Upgrading older systems with new firmware .....	164
20.5	USB desktop reader .....	165
20.5.1	Installation .....	166
20.5.2	Using USB Desktop Reader .....	166
21	Central discovery tool .....	170
22	FAQ .....	173
23	Appendix A - Description of LEDs and buttons on central.....	177
24	Appendix B - Nova software feature possibility list .....	178

## Explanations of words and concepts

Central:	Electronic device, an integral part of an access control system
ID card:	Identification card, could be MIFARE card, EmMarine card...
PIN:	Personal identification number
Reader:	Electronic device used to register ID cards and PIN numbers with central
Access group:	A group consisting of specifically defined doors. A user is assigned one or more access groups. The user has then been granted access through the doors defined in the access groups
REX:	Request to exit
DM:	Door monitor
LAN:	Local area network
WLAN:	Wireless local area network
WAN:	Wide area network
MAC:	Media access control address – usually noted on the sticker of the centrals
GUI:	Graphical User Interface – the user-friendly software for controlling the central.
HTTP:	Hypertext Transfer Protocol - old and unsafe
HTTPS:	Secure version of HTTP

## Introduction to Access control

Access control is any system or mechanism that grants or revokes the proper access to system resources. Access control systems, in buildings and facilities, normally consist of hardware and software. It allows the user to access and use different doors in pre-specified time intervals.

The following manual describes the basic concepts for optimal and successful use of the Nova software.

The name "Nova" is used throughout this manual for addressing the different software versions:

- NovaSimpli
- NovaSimpli350
- Nova10
- Nova100
- NovaPRO
- NovaServer

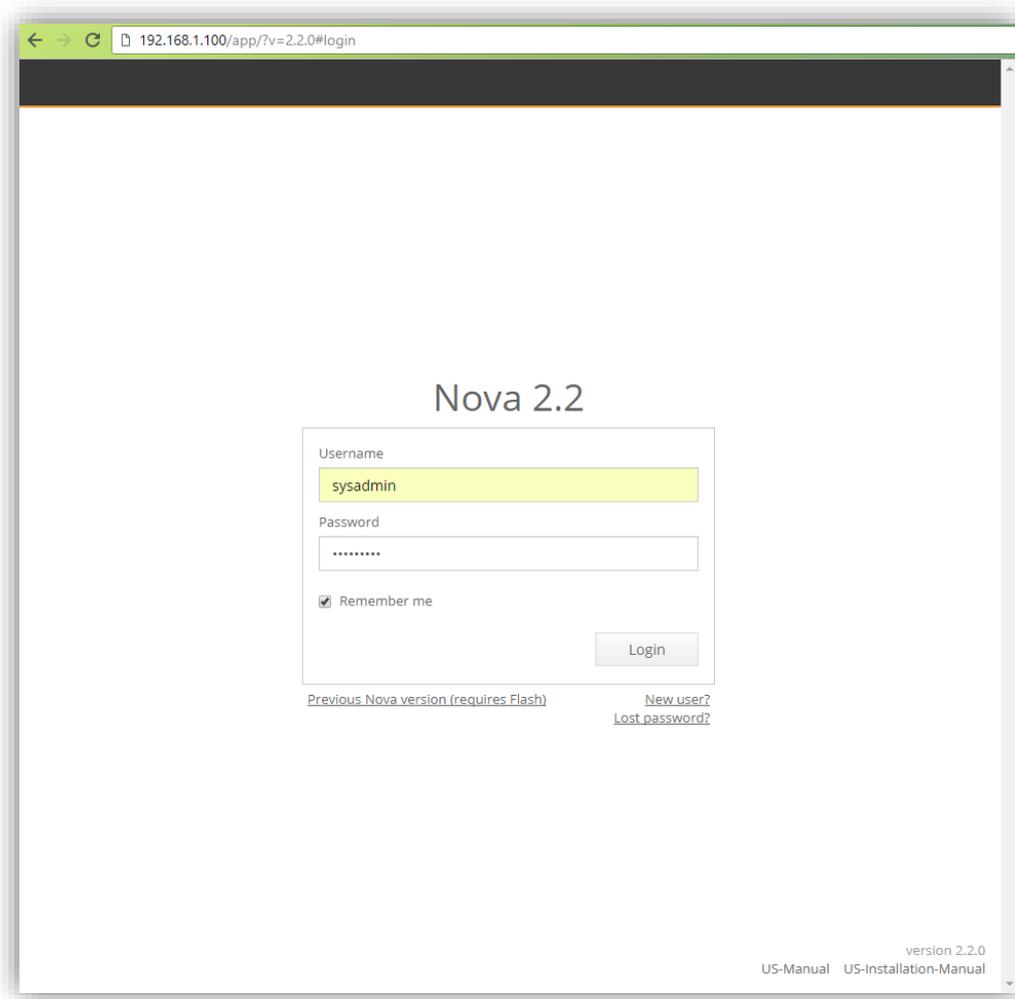
The core concepts in all software versions are identical. The differences between them will be explained when applicable. In most cases, the applications have different limits regarding the number of users, number of doors and some special functions.

More information about activation keys needed in chapter 6.1 Add-ons and Modules.

# 1 Login page

- Open web browser and navigate to the IP address of your central.
  - (Default central address is "**http://192.168.1.100**").

**NOTE:** If the installer made a shortcut on the desktop, use it to access the Nova software.



**Picture 1.1: Login page**

- Type your username and password into login page (Picture 1.1).  
If logging in for the first time, use predefined:
  - Username: **sysadmin**
  - Password: **sys4Admin**

**NOTE:** Passwords are **case sensitive**.

If login credentials were correct, the home page of the Nova software will appear on the screen.

**IMPORTANT!** Please change the predefined password and username to protect unauthorized access to your system! (See chapter 6 for further details).

**IMPORTANT!** Warning messages will appear on the home page of Nova to change the default password to increase system security and to change default IP address "http://192.168.1.100".

Clicking the message will allow the administrator to change the settings described in the message, otherwise clicking the X button (displayed on Picture 1.2) will prevent them from showing up again.



**Picture 1.2: Warning message**

### 1.1.1 Account types

Nova software implements different types of accounts:

- **User** – a normal user login, can change some of its own information, can add door widgets that has access to, has access to files (uploaded by sysadmin) and access to booking.
- **User (read only)** is used only for booking module. If this user's login information is provided for booking login, the clients that have a link to calendar can freely browse the calendar without a session drop (designed for displaying booking availability only!).
- **Checkpoint user login** – only has access to checkpoint widget, where he can monitor the cards that pass over a pre-defined reader.
- **Print administrator** – has access to all users (can create user, change their PIN, name, last name, account validity, additional fields, add Cards or Unauthorized cards, can set default card layout), card designer card/user reports and booking. Can not manage access groups or any other user data.
- **Local admin** – can only manage pre-defined user and hardware list. He can create new users that are automatically added to his user list and are invisible to another local administrator (the same goes for time schedules and access groups).
- **Administrator account** is used for the day-to-day system administration and permits/allows the management of users, access groups, schedules and control of doors in the system.
- **System administrator account** is used by the person installing the system and managing the hardware (e.g. adding centrals and readers).

**NOTE:** Do not use this account in normal workflow.

Since this account controls the access of all other administrator accounts, it should be assigned to the IT-responsible, the installing contractor etc.

- **Super administrator account** is primarily used for support purposes. The System administrator can disable the Super administrator account by navigating to **Home > Settings > Login Settings > Super administrator**.

## 2 Home page and main navigation

The main page consists of different widgets displayed based on the access rights of the person logging in:

- System administrator
  - Access to hardware widgets.
  - Access to user widgets.
  - Can create **link widgets** for all users.
  - Can create **door widgets** for all doors in the system if the system administrator has assigned access. Door widgets are only displayed on the home screen.
- Administrator
  - Access to user widgets.
  - **Sees the link widgets** created by System administrator.
  - Can create **door widgets** for all doors in the system if the administrator has assigned access. Door widgets are only displayed on the home screen.
- User
  - Sees link widgets created by System administrator.
  - Can create **door widgets** for all doors in the system if the user has assigned access. Door widgets are only displayed on the home screen.

Widget types:

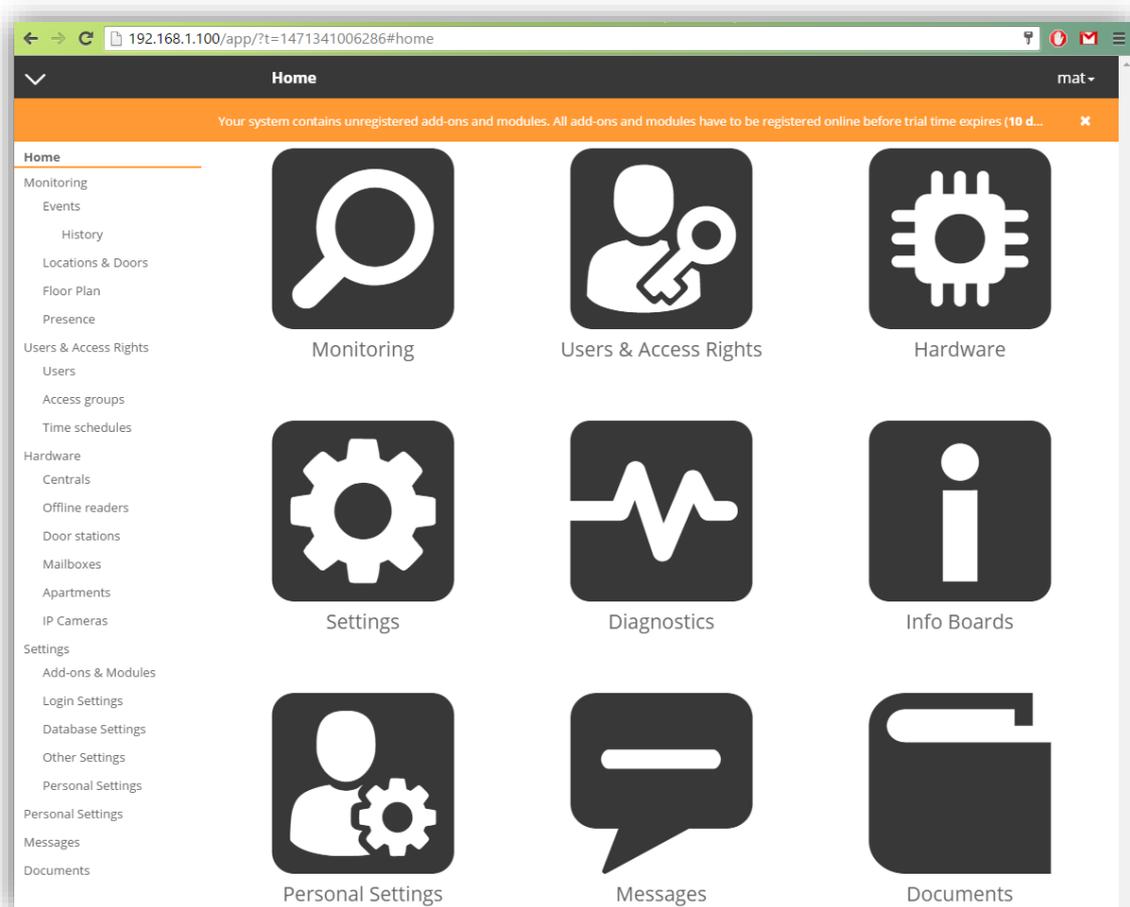
- **Web link widget** – Can create a link to external web page or linked file location.
- **Door widget** – Enables opening the desired door with a single click (very handy for mobile access).
- **User widget** – Used for user management.
- **Hardware widgets** – Used for managing system hardware.

A short description of the other non-user created widgets:

- **Monitoring** – Consists of widgets with different overviews.
  - **Events** – History/Live events feed.
  - **Floorplans** – Displays hardware location on the ground plan / blueprint.
  - **Locations & Doors** – An overview of locations and hardware displayed in a tree structure.
  - **Presence** – Displays groups of people that have checked-in.
- **Users & Access Rights** – All about users and their management.
  - **Users** – Add/edit/delete users.
  - **Access groups** – Create/edit/delete access groups.
  - **Time schedules** – Create/edit/delete Time schedules.
- **Hardware** – All about hardware.
  - **Centrals** – Add/edit/delete readers and centrals.
  - **Offline readers** – Add/edit/delete offline readers.
  - **Door stations** – Add/edit/delete door stations.
  - **Mailboxes** – Add/edit/delete mailbox units.
- **Settings** – Contains all general/system-wide settings.
  - **Add-ons & modules** – Includes addition and activation of different add-ons and modules.

- **Login settings** – Language settings, maintenance contact information, password recovery and new user registration and social login settings.
- **Database Settings** – Configuration/Events database download, automatic database backup.
- **Other Settings** – Time-zone, web server port, email settings and unique PINs.
- **Personal Settings** – Personal language and password.
- **Messages** – API for sending emails or messages to the door stations.
- **Documents** – Important files (seen by everyone) that can be uploaded to the central (maintained by administrator or system administrator).

For easier navigation, use the arrow on the left top side of the window to display or hide the **quick access menu**.



**Picture 2.1: Home page with widgets and navigation menu**

From every page, there is access to any of the previously selected widgets on the **header bar**.

E.g. to navigate from the **Home** page to **Users & Access Rights** and afterwards to **Time Schedules**, simply click on **Users & Access Rights** to return to the wanted widget (Picture 2.2).

**Picture 2.2: Steps and access to the current widget**

By clicking on the user-name on the right side of the header, a dropdown menu will display:

- **Account** – For managing currently logged-in account settings – furtherly described in the chapter 2.1 Account settings.
- **Widgets** – Used to create User widgets. Description of details are in the chapter 2.2 Creating user widgets.
- **Logout** – Logs out the current user.
- **Version number** - Software version of the Nova software. Providing the version number when contacting support is crucial for easier determination of the problem(s).

## 2.1 Account settings

This option enables user to manage their own account.

Basic settings:

- **Account language** – The user can change what language the website will be displayed in.  
**NOTE:** Changing the language will only affect the user who changed it and display the site in the set language.
- **Change Password** – Users can change their own login password.

**Account**

Language

English

Change

**Change Password**

New password

New password

Confirm password

Confirm password

Change

**Picture 2.3: Users can change their own language and password.**

**Nova 2.0 Self-service activation key** enables System administrator to extend the user settings. These options can be found in **Home > Settings > Personal Settings**.

**Settings for Personal Settings**

Change Email - Allow users to change their email

Change Phone - Allows users to enter or change their mobile number

Change BIC - Allow users to change their text displayed on door station

Change PIN - Allow users to change their pin

Add phone numbers - Allows users to add their phone numbers as an access identifier

Save

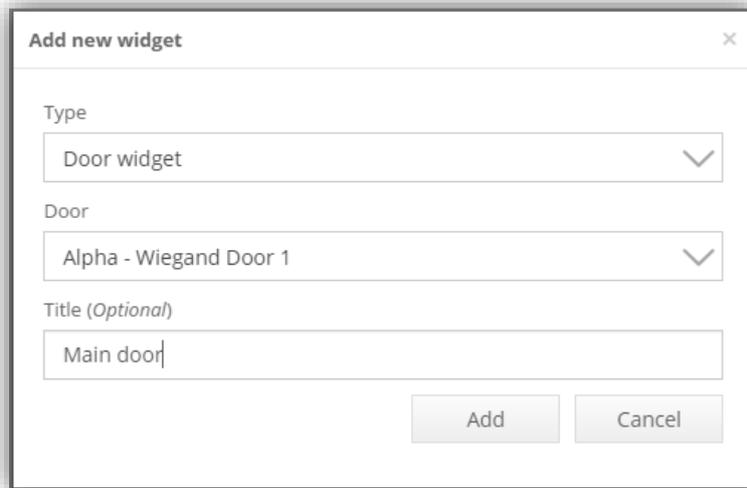
**Picture 2.4: Extended user personal settings**

Extended user settings consist of:

- **Changing email** – Allows users to enter or change their email address. This is an option for the Messaging module.
- **Changing phone number** – Allows users to enter or change their mobile number. This is an option for Messaging and Presence modules.
- **Changing PIN** – Enables users to change their own PIN.
- **Adding phone numbers** – Allows users to add their phone number as an access identifier. Used for accessing doors via mobile phone call.

## 2.2 Creating user widgets

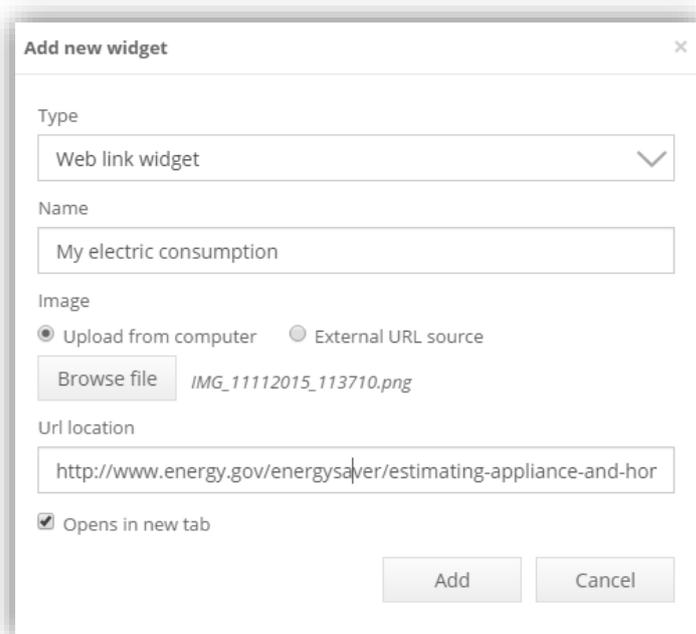
Users can create their own widgets by clicking on their username while logged in and navigating to the **Widgets** option. By pressing the **Add** button, a new pop-up window will appear. From there, users with access rights assigned, can create door widgets for a quick access. These widgets are only seen by the user who created them.



The screenshot shows a dialog box titled "Add new widget" with a close button (X) in the top right corner. It contains three input fields: "Type" with a dropdown menu set to "Door widget", "Door" with a dropdown menu set to "Alpha - Wiegand Door 1", and "Title (Optional)" with a text input field containing "Main door". At the bottom right, there are two buttons: "Add" and "Cancel".

**Picture 2.5: Creating a new Door widget**

**System administrator** can additionally create a Web link widget that can link to external websites or upload a file from the computer. Unlike the Door widgets, Link widgets are displayed to **everyone** on their home page.



The screenshot shows a dialog box titled "Add new widget" with a close button (X) in the top right corner. It contains several input fields and options: "Type" with a dropdown menu set to "Web link widget", "Name" with a text input field containing "My electric consumption", "Image" with two radio buttons: "Upload from computer" (selected) and "External URL source", a "Browse file" button next to the filename "IMG\_11112015\_113710.png", "Url location" with a text input field containing "http://www.energy.gov/energysaver/estimating-appliance-and-hor", and a checked checkbox labeled "Opens in new tab". At the bottom right, there are two buttons: "Add" and "Cancel".

**Picture 2.6: Creating a Link widget**

To create a Link widget:

1. Select widget type.
2. Enter its name.
3. Select the picture you wish to display as a cover of the widget (either upload it from the computer or provide the URL address to the picture, e.g. [www.example.xyz](http://www.example.xyz)).
4. Enter the URL address for the link.
5. Tick the checkmark if the web-page should open in a new window (otherwise it will open on the current page).

## 3 Monitoring widget

Monitoring widget is divided into:

### 3.1 Events widget

**Centre panel:** *Latest events* displays recent events in the system indicating time, location and name of the user that triggered the event. The *Clear* button removes all of the events from the currently active feed of events. New events are still displayed.

**NOTE:** The events are not deleted, just temporary hidden from the user.

When the Events page is loaded, it displays the last 50 events. This number extends to 300 if the browser page stays open while new events are added. Live events can be filtered by typing the keyword into the text box on the top of the panel (e.g. Reader connected).

**Right panel:** System information, Errors, Warnings, Disconnected centrals and readers and Unlocked and blocked doors.

These panels show the current state of the system:

- *System information:* shows the number of present doors and users, current time on the central, database usage and uptime of the central. Clicking on the time stamp will send a request to update time on all centrals in the system.
- Errors and Warnings, Disconnected centrals and readers and Unlocked and blocked doors: shows what needs to be inspected

#### 3.1.1 Event history

The event history is accessible by navigating to **Menu > History**.

The right panel offers the user a variety of filter types. The first filter is to set the beginning and the end of the time frame for searched events.

By clicking on predetermined tags, the events for that tag will automatically be selected (e.g. Clicking on the "Warnings" tag will select the Unknown PIN, no access events...).

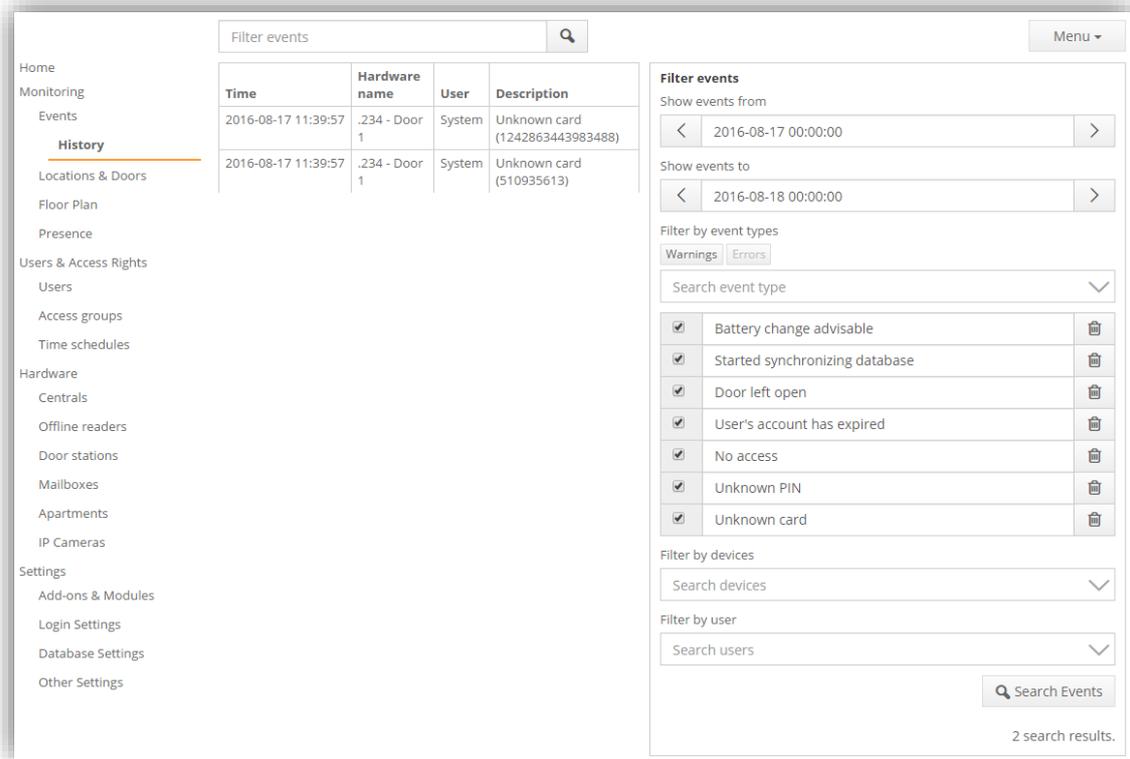
Event types can also be entered manually by selecting them from the dropdown menu. Selecting the devices from the device filter enables the search to work only on certain hardware.

Events can also be filtered by specific user(s).

**NOTE!** Leaving any of the fields empty will result in selection of all fields from that type.

**IMPORTANT!** Using a narrow History search will result in fewer results but will require more system resources and hence more time. Searching the events in a larger period will result in a longer waiting time as well. Instead, make your requests short and simple then run them multiple times if required.

History result page can be printed out or saved to an Excel file by navigating to the **Menu > Print** or **Menu > To Excel**.



**Picture 3.1: Event history with "Warnings" filter active**

**IMPORTANT!** Software version NovaSimpli350 does not display or store any history of the events in the system. Events can only be monitored through live feed of events on the events widget.

### 3.1.2 Manage error and warning events

The event managing window can be opened from the **Events** page by navigating to **Menu > Manage error and warning events**. By default, all Warning, Error and Custom events will be displayed. With a click on a cog wheel in the upper left, we can filter the event list to show **all events, events with priority, custom events and normal events**. The search function will also reduce the list if the contained string is found in the name of the event.

**NOTE:** Custom events can only be added if the scripting key is present in the system. To read more about the scripting module, please navigate to chapter 7 Module: Scripting.

By double clicking on the event or navigating to **Menu > Edit [Event name]**, a new popup will display:

- **Event name** (name can only be changed on custom events)
- Event priority
  - **None** – this event will not be displayed in the table.

- **Information** – if the event is triggered, it will be displayed on the bottom of the list with a grey icon.
- **Warning** – if the event is triggered, it will appear between the Information and Error section with a yellow icon.
- **Error** – if the event is triggered it will be displayed on the top with a red icon next to it.
- **Sound alert** – after the event happens, it will trigger the selected sound notification (their tune can be tested by clicking the button next to it).
- **Text instructions** – if the text instructions are provided, they will be displayed as a note when the operator tries to remove the notification.
- **Reason confirmation** checkbox – if the operator wishes to remove the notification, a response must be provided.

## 3.2 Locations & Doors

Access control can be installed in all types of buildings, regardless the number of rooms and doors.

- **Locations** - In the software these buildings and rooms are referred to as locations.

Doors – Doors are assigned to the locations in form of readers. Readers are added to the system using the hardware widget (see **5.1.13 Adding new readers**).

This model represents the logical scheme of the access control system and its components.

Overview on different locations

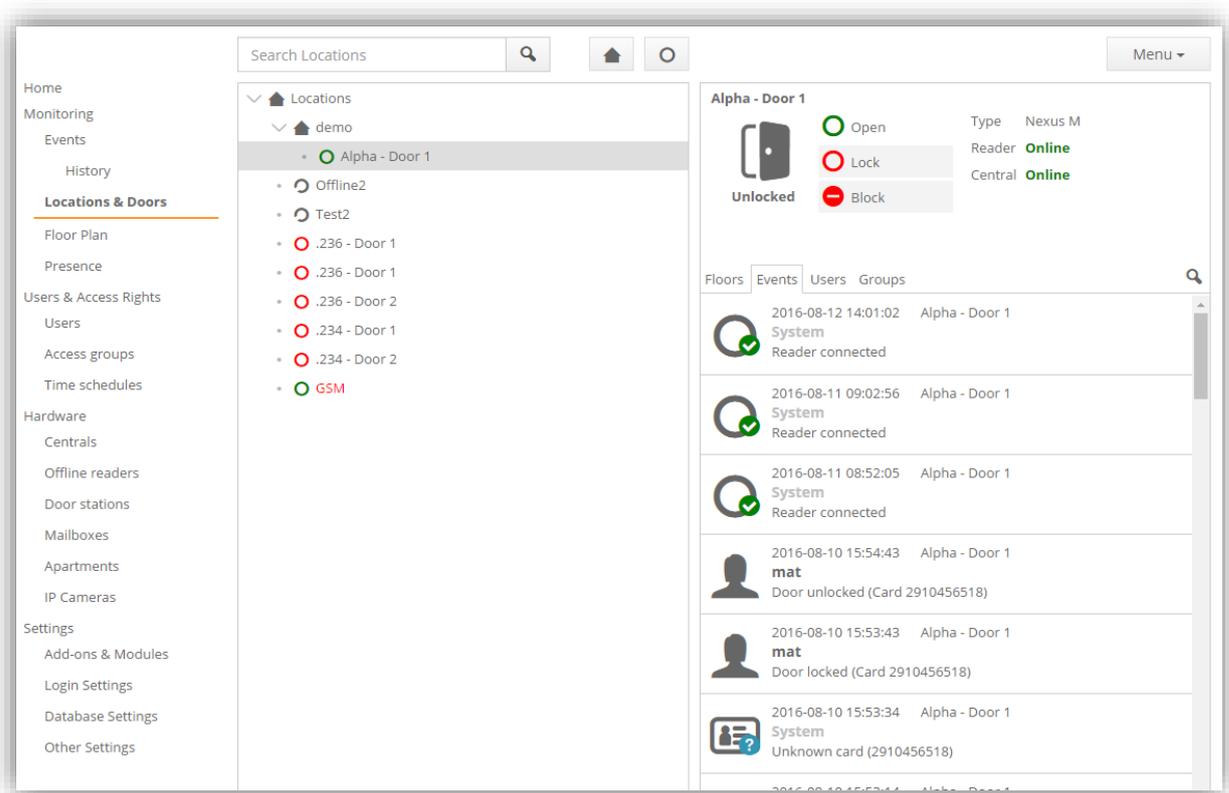
Navigate to **Home > Monitoring > Locations & Doors** to see the location tree displayed. Clicking on different icons will reveal different branches of the device tree:



- Displays only locations and unsorted readers.



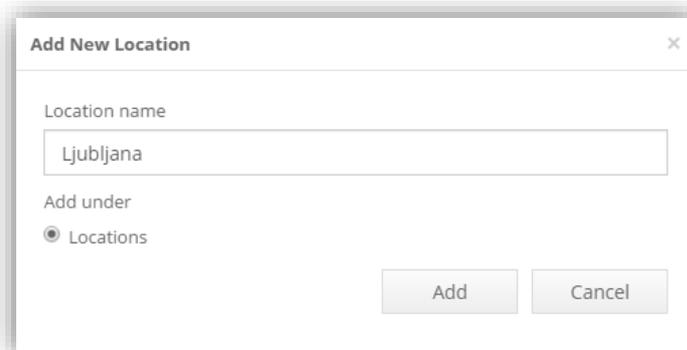
- Extends the entire tree with all locations and readers.



**Picture 3.2: Locations and detailed information**

Adding a new location:

1. Select the root location (the top position).
  - a. NOTE: If there are no locations created yet, the new one is the top location.
2. Click on **Menu > Add New Location** button.
3. Enter a name for the new location into popup window (Picture 3.3)
  - a. Optional: Select a previously created location that the new location is going to be a branch of (placed under).



**Picture 3.3: Adding new location**

Renaming locations:

1. Select the location for renaming.
2. Click on Menu > Edit location.
3. Rename it.

Removing location:

1. Select the location.
2. Click on Menu > Remove location.

**NOTE:** Locations that contain sub locations cannot be deleted. To remove a location, all sub locations and readers need to be transferred or deleted.

Arranging items:

1. To move an item, select it.
2. Click on **Menu > Move.**
3. Select the location that the item will be placed under.

### 3.2.1 Location management

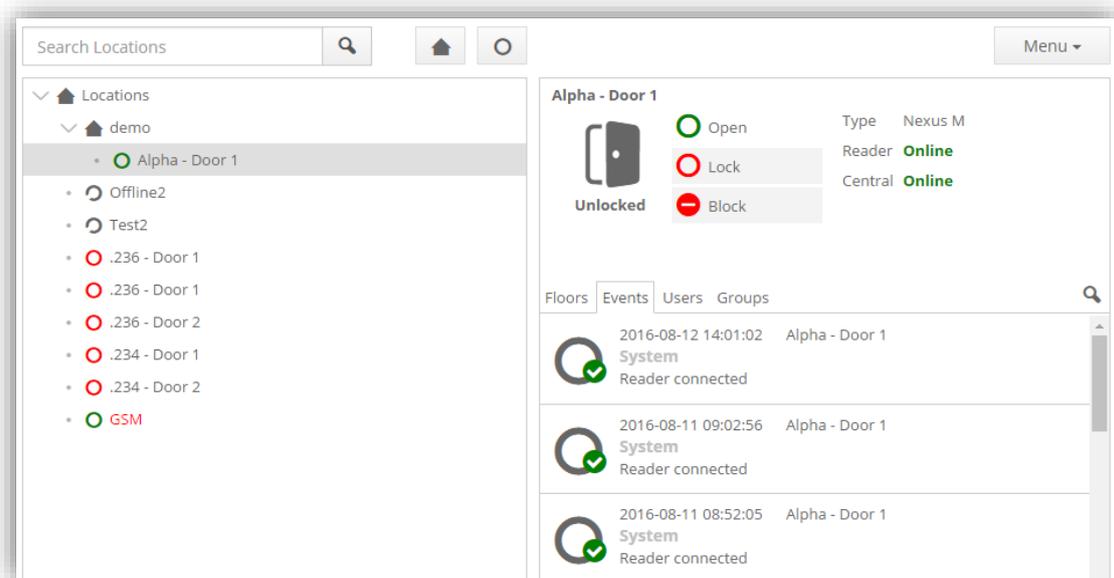
Selecting a location enables management of all readers located in the selected location and its sub locations.

By selecting their location and perform one of the next actions, all readers in the location can simultaneously:

- Lock
- Unlock
- Block
- Unblock

When selecting a reader, the GUI will show:

- Reader status
- Possibility to manage related door (Picture 3.4)



**Picture 3.4: Location and doors showing all readers in the system assigned to locations**

Description of the reader icons:

-  - Door is locked, reader is red
-  - Door is unlocked, reader is green
-  - Door is locked and reader is blocked
-  - Door is unlocked and reader is blocked
-  - Offline reader
-  - Door & reader status is unknown (the central did not receive an update)

In the lower right panel, additional information about the selected item is shown in columns:

1<sup>st</sup> tab: displays the **Floors** that the reader is shown on. **NOTE:** This tab is only visible if there is Floorplan module added in the system.

2<sup>nd</sup> tab: list of last **Events** related to the selected reader (if the selected item is a location, the events are not shown).

3<sup>rd</sup> tab: list of all **Users** having access rights to the selected item and all connected readers (when the selection is a location).

4<sup>rd</sup> tab: list of **Access groups** that have any access to the selected reader or location.

**NOTE:** To manage an offline reader, select it, and choose **Menu > Edit (Basic administrators cannot change hardware settings)**.

## 4 Users and Access rights

**IMPORTANT!** Creation of the access groups before adding users is strongly recommended – see part 4.3 Access groups widget for instructions.

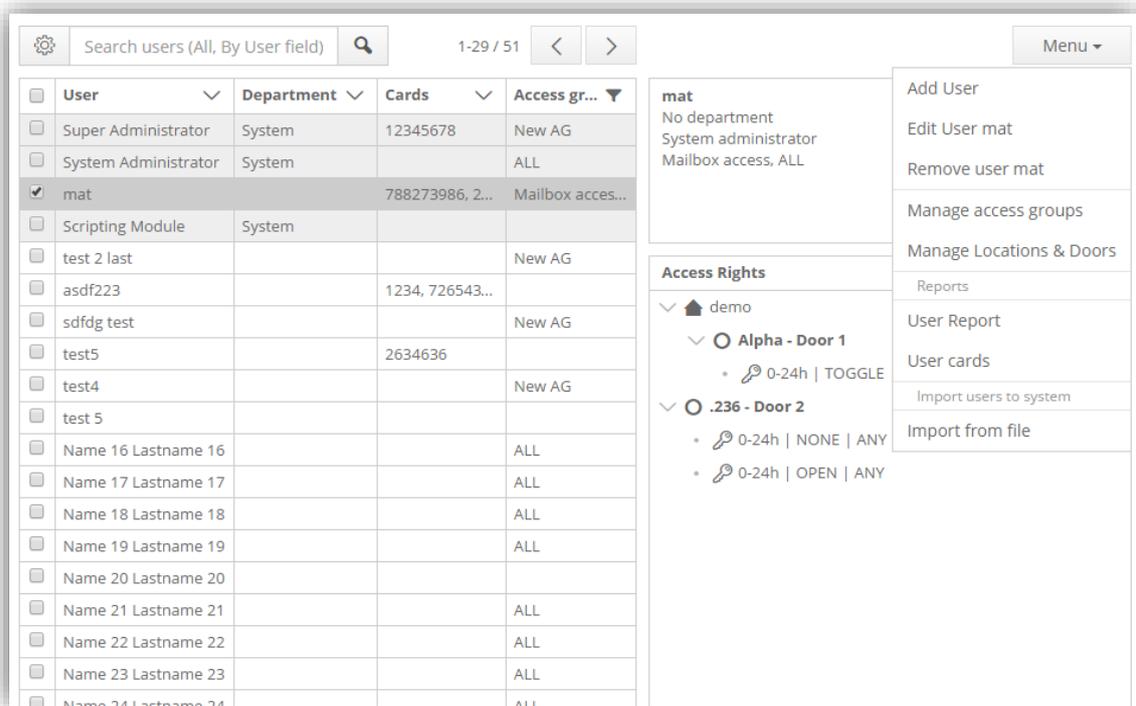
The Users and Access Rights page is used for managing users and the setup of:

- Users' access rights
- Access groups: pre-definition of doors that a user has access to, when being a member of this group.
- Time intervals: precise time interval can be set for user's access to specific doors

### 4.1 Users

When clicking the Users widget, the Menu contains the following options:

- Add User (see Picture 4.1)
- Edit User
- Remove User
- Manage access groups
- Select columns – read more about in chapter 4.2.4 Custom user preview.
- Manage Locations and Doors – a redirection to Locations & Doors
- Reports – different types of reports for the specific user(s) or their access cards
- Card designer – comes with activation key. You can read more about it in chapter 15 Module: Card designer.
- Import users – a function to import users from CSV files



Picture 4.1: User management

**User information** is displayed in the upper right panel. Access rights are displayed in the right panel below.

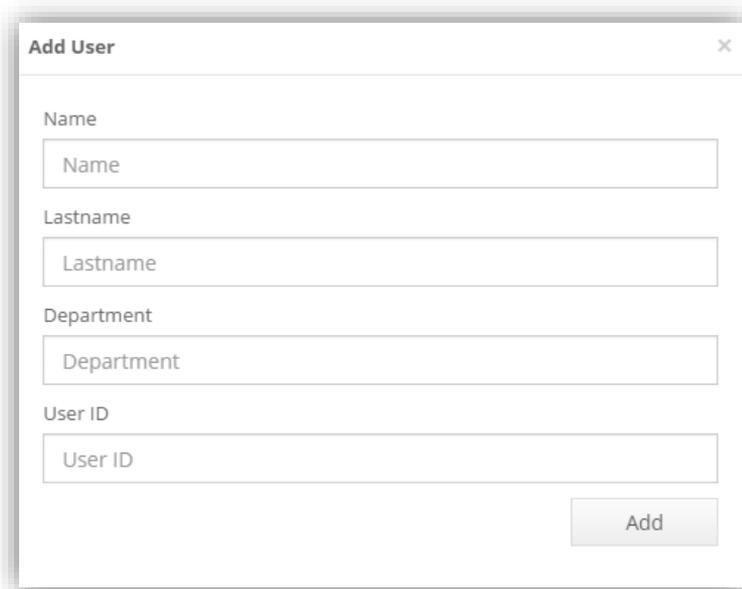
## 4.2 New users

A new user is added by clicking **Menu > Add user**.

User data can be entered in the new window (Picture 4.2).

- Name
- Last name
- Department
- User ID

The data needs to be saved by clicking the button **Add**.



The image shows a dialog box titled "Add User" with a close button (X) in the top right corner. It contains four text input fields, each with a label above it and a placeholder text inside the field: "Name", "Lastname", "Department", and "User ID". At the bottom right of the dialog box is a button labeled "Add".

**Picture 4.2: Input for new user data**

Additional data that can be defined for selected/new user:

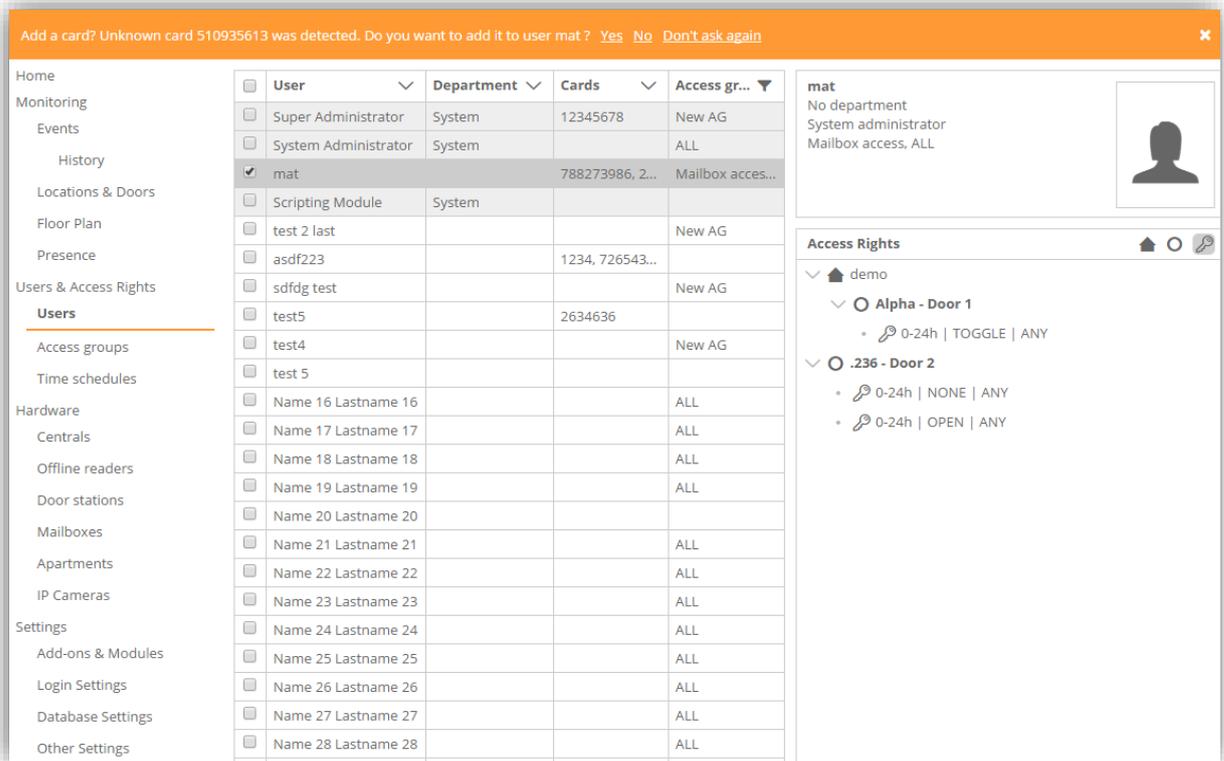
- PIN (must not exceed 20 characters)  
**IMPORTANT!** Each user needs a unique PIN. Length of the PIN code on **offline readers** is limited to a **maximum of 7 characters**.  
PIN that does not comply will not work and will not display any warning when writing data on user card.  
**IMPORTANT!** If a user enters a wrong PIN 5 times in a row, the reader will report Access suspended for any PIN entered in the next 30 seconds.
- Card number (usually marked on identification card). Each user can have up to 16 different card numbers/telephone numbers. A table card reader can be used for easier card number input.

- Validity of user account (before start date and after end date the user will not have valid access rights).
- E-mail, Phone, Address and Remarks.
- Add a picture

### 4.2.1 Adding unknown card(s) to user

When the system detects an unknown card (i.e. a card that is not assigned to any user) and the user is either currently selected in the user grid or the user editor is open, the option to assign the card to the currently selected user will appear in the bar at the top of the screen (Picture 4.3). In that case, the card will automatically be saved and listed like other assigned cards.

**NOTE:** This mechanism is used to quickly assign more cards to a single user. The downside is that a card reader is needed next to the PC, as the detection of a new card and assignment to a user has to be made simultaneously.



Picture 4.3: Assignment of the unknown card to user

### 4.2.2 Card function assignment

Different functions can be assigned to the user's cards by selecting the button to the left of the card number.

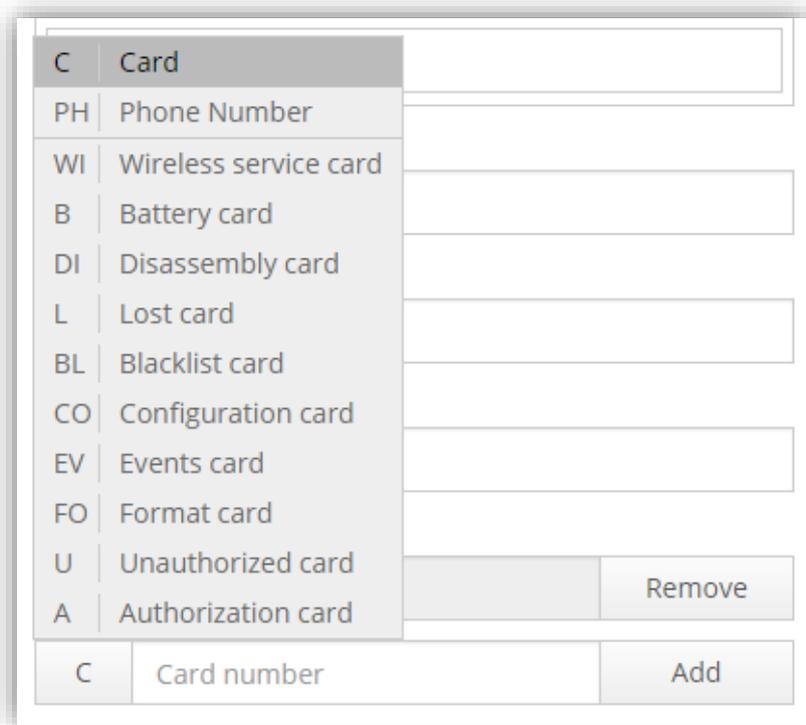
By default, each new card is tagged as **C (Card)**, but its function can be changed by

selecting a new function from the menu that opens (Picture 4.4), when clicking the button to the left of the card number:

- **L: Lost card** (in the case that a card was lost or stolen, it needs to be tagged with this option. Lost card event is displayed on the main page if someone tried to use the lost card)
- **PH: Phone number** if the user is able to open doors using a GSM gateway

The options below are **only visible to the system administrators** and are used for maintenance of offline readers:

- **WI: Wireless service card** (card for pairing offline readers with Antenna module)
- **B: Battery card** (card for replacing batteries on an offline reader, if applicable)
- **DI: Disassembly card** (card for disassembling an offline reader, if applicable)
- **BL: Blacklist card** (card for transferring the list of lost cards to an offline reader)
- **CO: Configuration card** (card for transferring configuration settings to an offline reader)
- **EV: Events card** (card for transferring the list of events from an offline reader to the central)
- **FO: Format card** (card will be formatted when detected on online reader)
- **U: Unauthorized card** (card will not work until it is activated by the authorization card; after that it will change its type to C - Card)
- **A: Authorization card** (used for activating unauthorized cards)



**Picture 4.4: Changing card's function**

## 4.2.3 Managing users, their access rights and apartments

After saving user data, additional options are available through the tabs appearing on top: Access rights, Card settings, setting Account options, previewing Last events.

Edit user:

By clicking the **Menu > Edit user** button in the main navigation menu or by double-clicking the user in the list of users, it is possible to edit user's data such as:

- Edit personal, contact and identification information
- Add/Remove access groups
- Change picture: by clicking the Change picture button on the right side of the window (Picture 4.5)
- Grab from camera – grabs a picture from a camera connected to PC
- Delete user picture

**NOTE:** These options are present every time someone is editing an existing user or after creating a new user.

**NOTE: Administrator or System Administrator** can edit all user data. Some of the data users can edit by themselves: Read which and how users can edit their own data in caption **2.1 Account settings**.

The screenshot shows the 'Edit user Peter Johnson' interface. It features a top navigation bar with 'Save' and 'Menu' buttons. Below are tabs for 'General', 'Advanced', 'Account', 'Latest events', and 'Additional fields'. The 'General' tab is selected. The form is organized into several sections: 'Name' (Peter), 'Last name' (Johnson), 'Department' (IT), 'User ID' (8), 'E-mail' (someemail@google.com), 'Phone' (0038630674835), 'Address', and 'User's apartment' (Apartment 4). The 'Access groups' section indicates 'No groups assigned' and provides a 'Manage access groups' link and a 'Click here to assign group' button. The 'Valid from' and 'Valid to' dates are 2012-01-01 00:00:00 and 2032-01-01 00:00:00. The 'PIN' is masked with dots. The 'Cards' section shows 'None' with a 'C' icon, 'Card number', and an 'Add' button. The 'Picture' section displays a photo of a cat and includes links for 'Change picture', 'Grab from camera', and 'Delete user picture'. The 'Remarks' section is empty. The 'Default card print layout' is set to 'Default layout'.

**Picture 4.5: User settings**

Assigning Access groups:

Assigning the Access group to a **single user** is done in the settings window for the user (Picture 4.5):

1. Type the name of the Access group in the corresponding field.

2. Select the correct Access group from the autocomplete dropdown list, it will be added to the field above. Assign groups as requested.
3. Save changes.

Assigning Access groups to **multiple users** is done from the user list by selecting multiple users. Selection can be made by holding Ctrl (adds non-consecutive selection) or Shift (adds consecutive selection) key. In case the selection is made from a touch device, multiple users can be selected by placing a check-mark in front of their entry.

Click the **Menu > Edit users** button.

- Left column includes all Unassigned access groups.
- Middle column includes Assigned access groups for selected users.
  - Access groups can be Assigned or removed by selecting the Access group and pressing the corresponding button on the middle (Add or Remove).
- **Right column** displays access of the currently selected access group.
- **Offline readers tab** – all settings are applied to selected users
  - Define validity of data written on cards for offline readers
  - Define if assigned user cards should be able to activate/deactivate the toggle mode on offline readers (Constantly unlocked/ activated so it works like a thumb turn on the inside of a door or a regular mechanical handle). This option is only displayed if the Offline+ activation key is applied in the system.
  - Specify time schedule to limit the usage of a user's card to follow defined intervals on offline readers.
 

**NOTE:** Offline readers only support 2 time intervals, so only the first two defined intervals in the selected time schedule will apply. The option of checking time intervals on user cards needs to be enabled on the offline reader (see Picture 4.6). This option is only displayed if the Offline+ activation key is applied in the system.

Tab **Advanced** (Picture 4.6):

- Define validity of data written on cards for offline readers
- Specify time schedule to limit the usage of a user's card to follow defined intervals on offline readers.
 

**NOTE:** Offline readers only support 2 time intervals, so only the first two defined intervals in the selected time schedule will apply. The option of checking time intervals on user cards needs to be enabled on the offline reader (see Picture 4.6). This option is only displayed if the Offline+ activation key is applied in the system.
- Define if assigned user cards should be able to activate/deactivate the toggle mode on the 2<sup>nd</sup> read on offline readers (Constantly unlocked/ activated so it works like a thumb turn on the inside of a door or a regular mechanical handle). This option is only displayed if the Offline+ activation key is applied in the system.
- **Privileged access** checkbox – users who have this checkmark set, will ignore any software limitations like blocked doors, anti-passback or interlock errors.
- Anti-passback function – the option to remove anti-passback limitations from this user. Pressing the Anti-passback status reset will open a window and ask the Administrator to reset anti-passback status for current or All users in the system.

- Apartment's visibility – option to show/hide the user on door-station. User's display data can be altered by writing the text in the overwrite textbox field. This option is only displayed if the Door station activation key is applied in the system.

The screenshot shows the 'Edit user Peter Johnson' interface with the 'Advanced' tab selected. The interface is divided into several sections:

- Card validity for offline readers after card registration on online reader:** A dropdown menu set to 'Unlimited'.
- Anti-passback function:** A checkbox labeled 'User can open doors even if they are blocked or limited by anti-passback function' is checked. Below it is an 'Anti-passback status reset' button.
- Apartment's visibility on door station:** A checkbox labeled 'User is visible on door station' is checked.
- Overwrite text on door station:** A text input field containing 'Johnson Jr.'
- Overwrite text on call button:** An empty text input field.
- Time schedule for offline readers:** A section with a 'Manage schedules' link and a note 'Select only time schedules with two (2) or less time intervals!'. Below is a trash icon and a dropdown arrow.
- Offline reader output toggle:** A checkbox labeled 'Toggle output on offline readers' is checked.

At the top right, there are 'Save' and 'Menu' buttons. At the top left, there are tabs for 'General', 'Advanced', 'Account', 'Latest events', and 'Additional fields'.

**Picture 4.6: User's advanced settings**

**Account** tab – Promote/demote user's access rights to the software:

1. Select user from user list (Picture 4.3).
2. Click the Account tab.
3. Choose the account type and language.
4. Fill out the form with user's login name and password.

To see user's history/event log:

1. Select user from user list (Picture 4.3).
2. Click Menu > Edit user button.
3. Navigate to tab **Last events**.

**Additional fields** tab:

Sometimes costumers wish to store some more information about a costumer, that isn't pre-determined by the Nova2.0. In such cases, they can create their own fields with custom labels and variable entries.

The additional fields work great with card manager, to read more about it, please navigate to chapter **15.3 Additional user fields**.

Removing a user:

1. Select the user from the user list (Picture 4.3).
2. Click on **Menu > Remove user** in main menu.  
**NOTE:** The user will be deleted, but card will remain in the system, in order for the administrator to see if someone is trying to gain access using a deleted card.
3. Follow steps from chapter 4.2.1 to re-use the card for a new user.  
This will make the card work normally and report all events as a new card.

Assigning apartments:

If there is a Module: Door stations or Module: Mailboxes applied in the system, Apartment widget becomes visible.

Make sure that apartments are created before they are assigned (reference - 8.3 Managing apartments).

To assign the apartment:

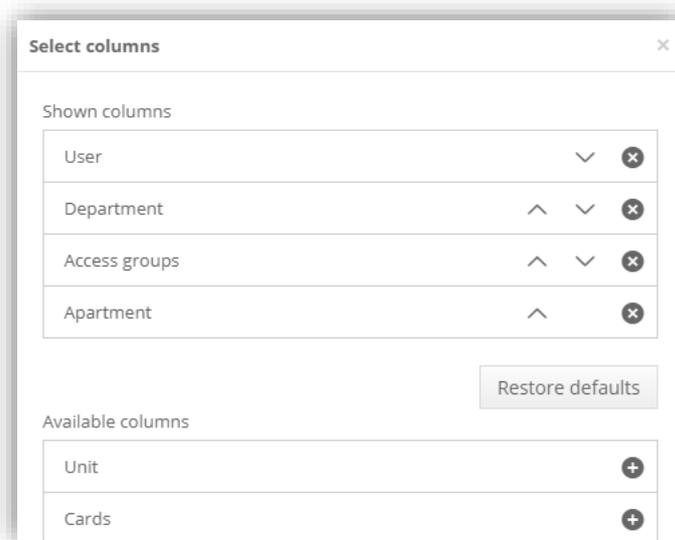
1. Enter user's **General** setting.
2. Under **User's apartment** start typing the name of the apartment.
3. When the selection narrows, select it from the drop-down menu.
4. **Save** changes.

#### 4.2.4 Custom user preview

Nova 2.2 supports resizable columns. Each column can be made wider or shorter by holding down the mouse key on the vertical line between columns and dragging it to left or right (the same as it works in any other table management software).

Columns can be added / removed or reordered by navigating to **Menu > Select Columns**. On the top, the shown columns are present. You can remove the column by pressing the X next to its name or the arrows for re-arrangement. To add additional column to the user list, a plus button needs to be clicked next to the column name. The custom fields can also be used with the custom preview (read more about them in chapter 15.3 Additional user fields).

**Restore to defaults** button will set the preview to the original state.



**Picture 4.7: We can select custom columns and create a unique view**

With the new columns, we are able to sort them alphabetically like we did with the others. Additionally, the search functionality has been extended. We can now specify (by clicking on the cog wheel before search field) to search on specific column.

**NOTE:** The custom selection is stored locally which means that any changes that are made on one computer won't be visible on another nor will work on a different browser.

## 4.2.5 Importing users from .CSV or Excel file

User data can be imported into the software from a .CSV (comma-separated values) or Excel file:

1. Click the **Menu > Import from file** button in the main user menu
2. Open the file that includes users from the opened popup window.  
**NOTE:** The CSV type file needs to have the data for each user in separate lines separated either by comma (,), semicolon (;) or TAB separator.
3. The data from the import file will be parsed and presented in a grid (Picture 4.8). If there are any changes that need to be resolved, data can be rewritten in the grid.

The header of the grid includes different options for determination of the parsed data. Please select the correct one that represents the column.

- Unused
- Last name
- Name
- Department
- Access group
- Card
- PIN
- User ID

**NOTE:** The lines that installer does not want to import, are easily removed by pressing x next to them.

**ATTENTION:** Values in the column matched as *Access group* must match valid Access group names, which are already present in the system. Furthermore, the values in the column matched as *Card* or *PIN* details must be valid numbers.

**NOTE:** Each user needs to have a unique PIN.

After everything is set, press **Start Import**. Users that are successfully imported will turn green, while the ones that have an error, will turn red and their status will change to the error message.

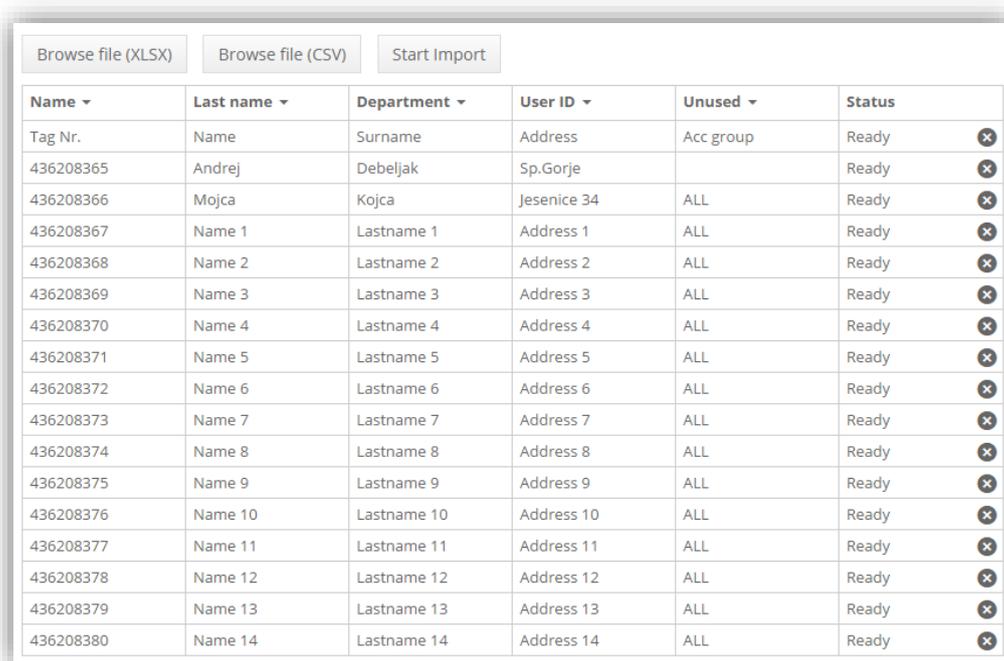
## 4.2.6 Custom user search

By navigating to users, the search filter defaults to match name or last name. The search was improved to have a better result set using spaces (for ex. Searching for "St K" or "St n" will find a "Stephan King" and "Steven Kong" users).

The filter to search on another column can be set by clicking on the cog wheel  before the search bar. The drop-down menu offers search between different columns and different access levels.

**NOTE:** NovaServer is a lot more powerful thus allowing the search to be run on all active columns.

In the Nova 2.2 we can also specify (in the same cog wheel drop-down menu), if we want to display users that have expired validity.



Name ▾	Last name ▾	Department ▾	User ID ▾	Unused ▾	Status
Tag Nr.	Name	Surname	Address	Acc group	Ready 
436208365	Andrej	Debeljak	Sp.Gorje		Ready 
436208366	Mojca	Kojca	Jesenice 34	ALL	Ready 
436208367	Name 1	Lastname 1	Address 1	ALL	Ready 
436208368	Name 2	Lastname 2	Address 2	ALL	Ready 
436208369	Name 3	Lastname 3	Address 3	ALL	Ready 
436208370	Name 4	Lastname 4	Address 4	ALL	Ready 
436208371	Name 5	Lastname 5	Address 5	ALL	Ready 
436208372	Name 6	Lastname 6	Address 6	ALL	Ready 
436208373	Name 7	Lastname 7	Address 7	ALL	Ready 
436208374	Name 8	Lastname 8	Address 8	ALL	Ready 
436208375	Name 9	Lastname 9	Address 9	ALL	Ready 
436208376	Name 10	Lastname 10	Address 10	ALL	Ready 
436208377	Name 11	Lastname 11	Address 11	ALL	Ready 
436208378	Name 12	Lastname 12	Address 12	ALL	Ready 
436208379	Name 13	Lastname 13	Address 13	ALL	Ready 
436208380	Name 14	Lastname 14	Address 14	ALL	Ready 

**Picture 4.8: Import users from CSV or Excel file**

**NOTE:** When importing from Excel file, make sure that the imported cells are set to "Text" and not as "Number".

### 4.2.7 Card authorization

Some installations require cards to be authenticated before they start working. To get such system working, system administrator needs to assign an administrator, provide him with username, password and a checkmark next to user authentication text show on the Picture 4.9.

**Edit user Theodora Martinson**

General   Advanced   **Account**   Latest events

Account type  
Administrator

Language - Preferred language after login  
English

Username - Name used for login into application  
theodora

New password  
.....

Confirm password  
.....

Company - Company name will be used in reports  
Company

User list - Only for Local Admin [Manage lists](#)  
User list

Hardware list - Only for Local Admin [Manage lists](#)  
Hardware list

User card authentication required - Administrator will only be able to add unauthorized cards. Users must authorize their cards with an authorization card.

**Picture 4.9: Assigning administrator who's cards will be added as unauthorized**

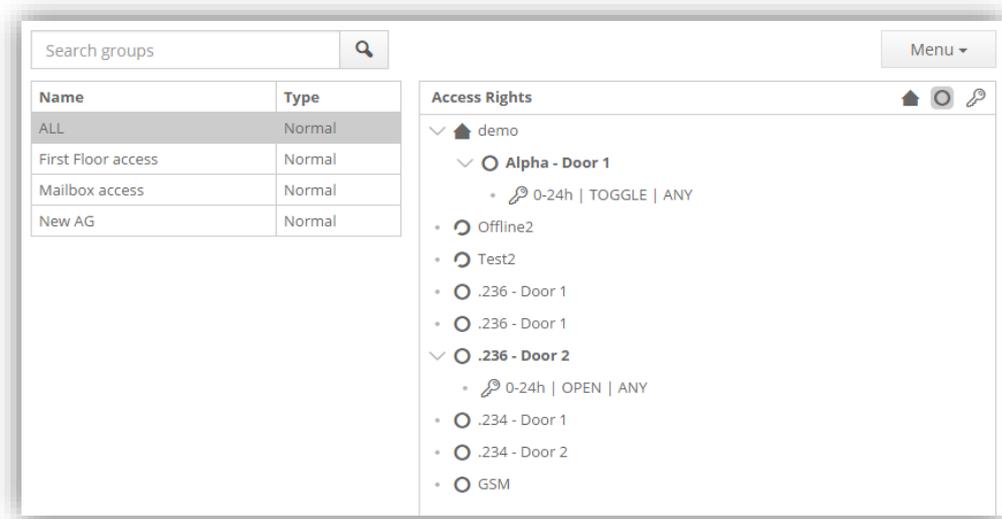
The system administrator can then assign authorization cards to users. When the Administrator logs into the nova, he/she is able to assign new cards to users, but are automatically set as **Unauthorized card** and won't work even if the user rights are correctly assigned.

Card will start working once the correct **Authorization card** is put on the reader; there will be a beeping sound, prompting for the correct user card. If the user card is put on the reader in the beeping period, it changes its status from **Unauthorized card** to **Card** and begins to work as a standard card.

Additionally, if more people are set in the same apartment, it is enough to set the **Authorization card** only to one person and use it to authorize other cards from that apartment.

## 4.3 Access groups widget

Clicking the button **Access groups** in the navigation menu will display the page below (Picture 4.10)



**Picture 4.10: Access groups editor**

By clicking the **Menu > Add group** button in the Access group editor a new access group can be added.

It is possible to:

- Enter new group name in the **Name** input box
- Enter group description or other info in the **Description** field optionally (Picture 4.11).
- Save the new Access group by clicking the **Add** button.

To edit an existing group:

- Select the group
- Click button **Menu > Edit** [group name] (Picture 4.11)

To remove an access group from the list:

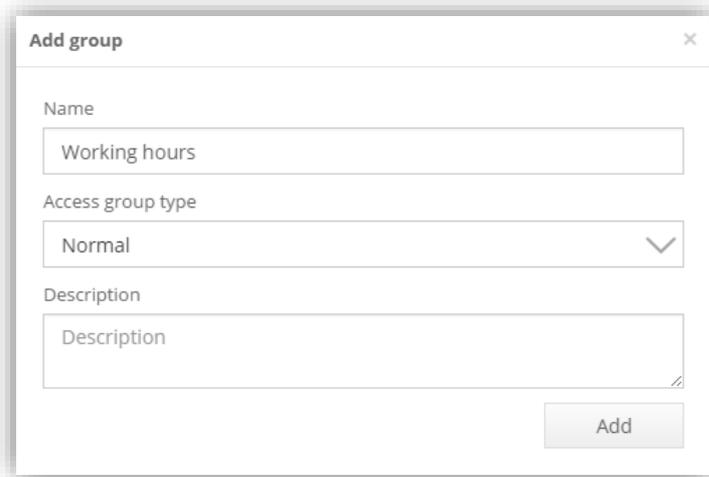
- Select the group
- Click the **Menu > Remove** [group name] button

**NOTE:** Access groups assigned to users cannot be deleted.

Booking module

In case the activation key for booking module is installed, the type of access group can be changed from **Normal**, which is used in Nova for defining access rights for users, to type **booking**, which is used in booking application. **Booking** access groups are shown

as different type in *Access group* editor. For more information about booking module please see chapter 13.

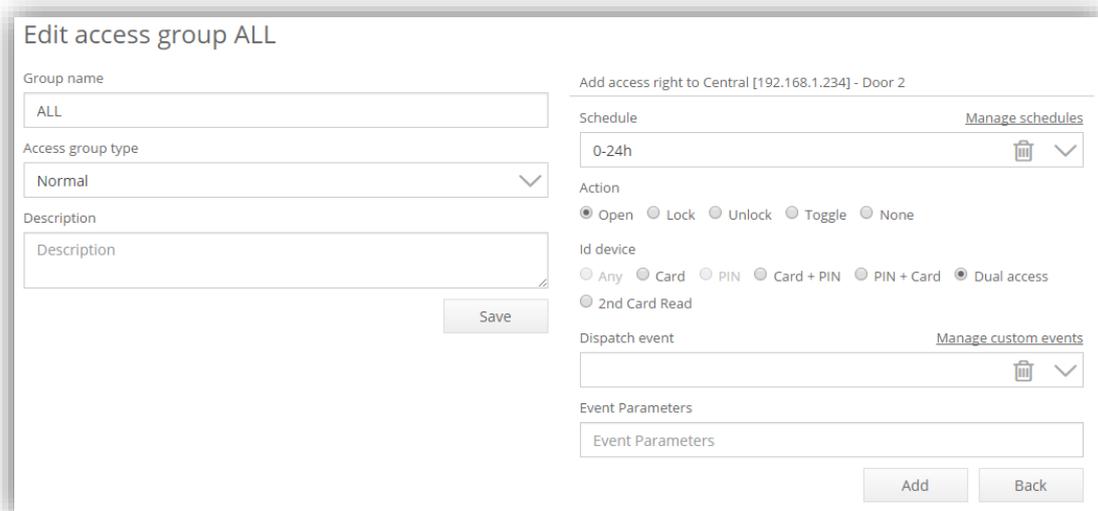


**Picture 4.11: New group editor**

### Access group editor

Access rights for selected access group in Access group editor (Picture 4.10) are visible in the hardware tree next to the list of groups. Buttons at the top of the tree can adjust current tree view and select which branches of the tree are displayed.

New access rights can be added to the selected group by clicking on the +button, which is visible when an item from the hardware tree is selected (Picture 4.10). This will switch hardware tree view into access properties for previously selected hardware.



**Picture 4.12: Time schedule, action and ID device selection**

Select time schedule, action and identification device

Here it is possible to:

- Select the desired time schedule
- Select action to be executed when identification device is presented to reader

Id devices available:

- Any (all ID sources with access will trigger the selected action)
- Card (only Cards with access will trigger the selected action)
- PIN (only the correctly entered PIN will trigger the selected action)
- Card + PIN (when a user shows card to the reader, the person's PIN has to be entered in the following couple of seconds to execute the selected action)
- PIN + Card (the PIN of the user has to be entered primarily and then card has to be checked for the selected action)
- Dual access (two cards with access must be presented on the reader in a limited time period)
- 2<sup>nd</sup> Card Read (on the 2<sup>nd</sup> Card read, execute the selected action)

If the Scripting module activation key is installed, an action can be set to trigger and dispatch a custom event, which is handled by the user script in the context of access right. For more information, please see chapter 7.

**NOTE:** The existing access rights can be edited or removed with the use of appropriate buttons shown on the selected tree item. Visibility of buttons for selected item depends on its type (location, offline reader or online reader).

**IMPORTANT!** When assigning access rights for offline readers, a default timetable *0-24h* (to add a new time schedule, please read chapter **4.4 Managing time schedules**) follows the actions **OPEN** and **CARD** as a source for executing action. Those access rights cannot be edited. This does not apply for the Nexus MKO which also supports PIN+card.

## 4.4 Managing time schedules

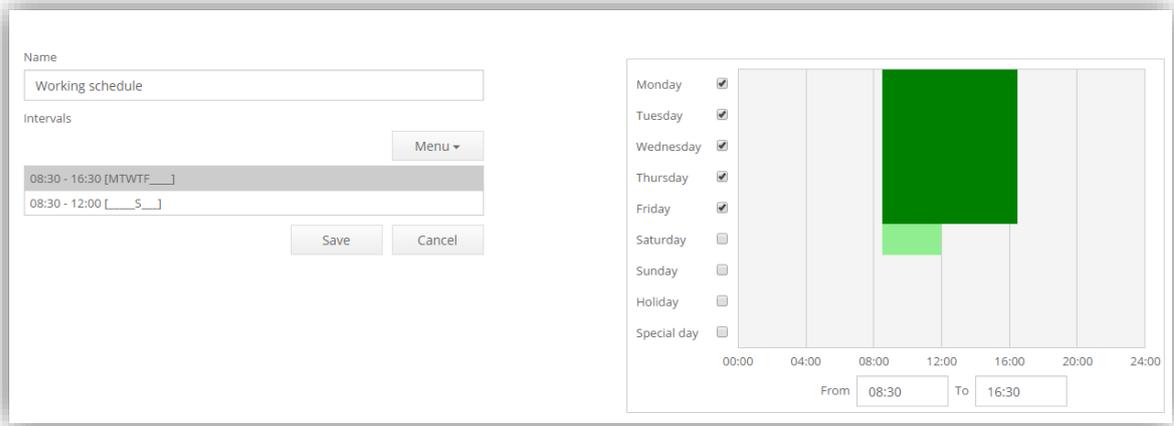
The NovaSimpli software includes one, predefined time schedule (0-24h), which is valid from 00:00 till 23:59 for every day of the week and cannot be modified or deleted. In other versions of Nova software, the option to manage and create additional time schedules is added. It can be accessed by clicking the **Time schedules** button found by navigating to **Home > Users & Access Rights > Time Schedules**.

In the **Time schedules and calendar** editor, the options are:

- Create, edit or delete existing schedules.
- Enter holidays and other special days in the calendar
- Add more time intervals to the schedule by clicking the **Add Interval** button

**NOTE:** Each time schedule contains one or multiple time interval(s), where each of them has a defined time span and days when the interval is valid (Picture 4.13).

**NOTE:** If the two schedules collide (ex. 00:00 – 24:00), the lock function will have a priority, therefore locking the doors at the last time set.



**Picture 4.13: Time intervals**

### Validity – country dependent

Time intervals can be defined on normal/ordinary days, special days or holidays, but please note that:

**Special days** and **Holidays** are predefined in the calendar and are country dependent. To access the calendar options, select the **Menu > Calendar** button from the **Time schedules** editor.

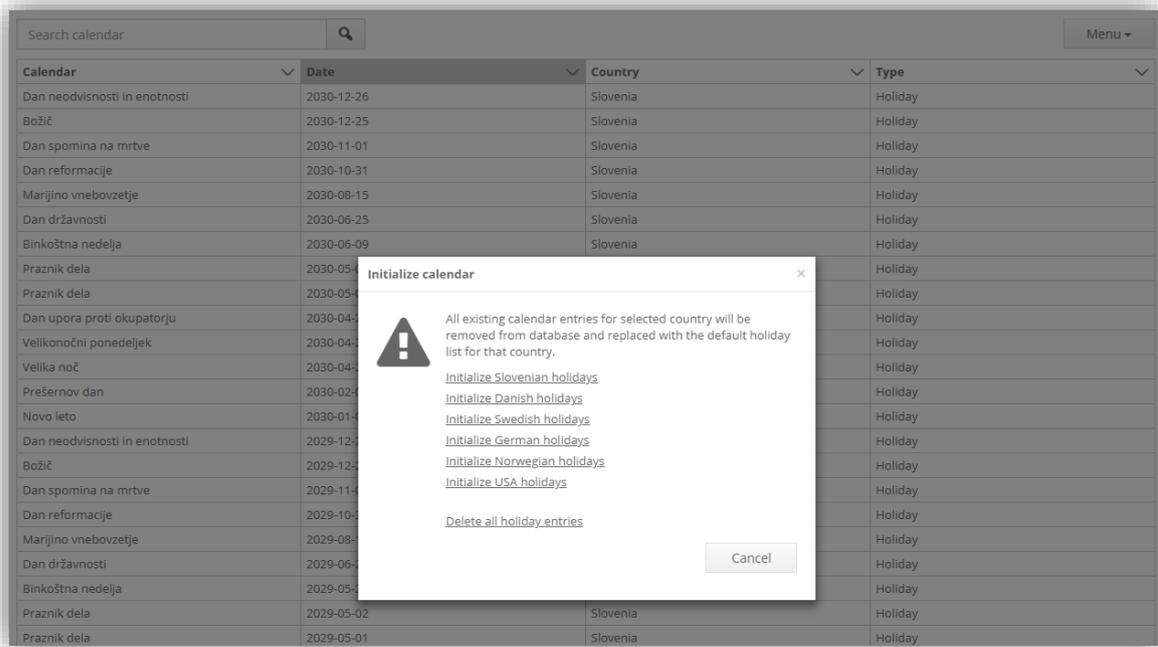
For each entry in the calendar:

- There is an option to specify for which country the entry is valid.
- The Country value is matched with the Country property of the central (see chapter 5.1.5 Adding, removing and editing centrals – Settings tab).
- If the country is not provided for a Holiday, the calendar entries are valid everywhere (independent of central's country).

### To automatically import Holidays for a country:

**IMPORTANT!** When assigning the holidays, make sure that the country on every central is selected correctly! If a system is installed in multiple countries, a customer can import different holidays and applicable countries need to be selected on the central(s).

- Click the button **Menu > Initialize calendar** in the calendar editor.  
**NOTE:** All existing calendar entries for selected country will be deleted from the database and replaced with the default list of holidays for the selected country. If any holidays are set wrong or missing, they can still be manually added/edited after the import is completed.
- To delete all holidays from the system, choose the last option from the menu.



**Picture 4.14: Initialize calendar with the default holiday list**

## 5 Hardware

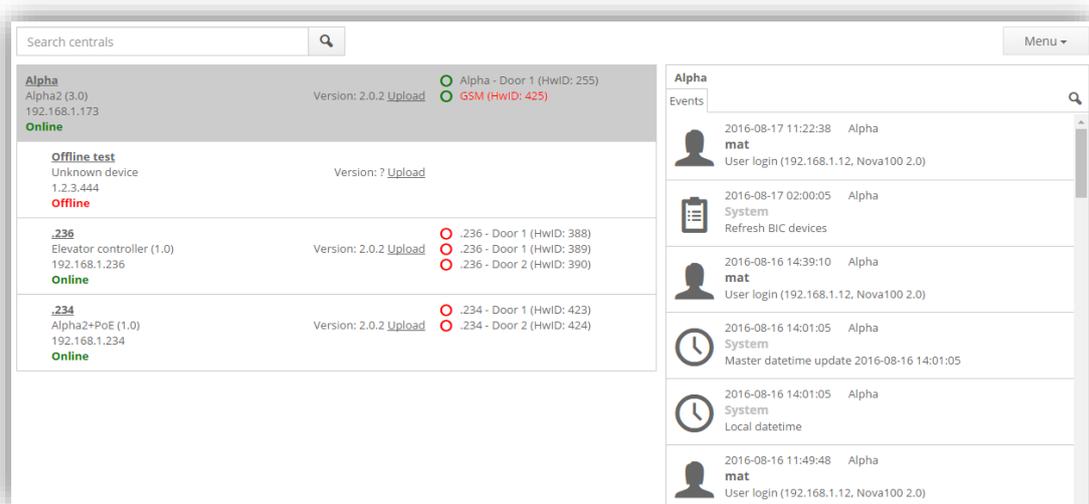
### 5.1 Centrals

The Central editor is used for previewing and managing hardware.

To open it, navigate to **Home > Hardware > Centrals** (Picture 5.1)  
Options in Menu:

- Search centrals
- Add new centrals
- Edit existing centrals
- Remove existing centrals
- Check for updates
- Upgrade all central

The right panel displays the last events of the selected central.



**Picture 5.1: Central editor**

**IMPORTANT!** In the NovaSimpli software, the number of centrals is limited to one (1) central.

#### 5.1.1 Searching and managing centrals in Local Area Network (LAN)

When clicking on the widget **Centrals** located in the **Home > Hardware**, and pressing the **Menu > Search centrals**, a list of all Nova centrals in the local network opens. The list consists of the centrals included in the system and other centrals also found in the LAN.

**CAUTION!** Some centrals may be part of another access control system so please be cautious when adding new centrals to the system!

By selecting the central that was found and is not yet in the system, the options are:

- Add a new central
- Add the central to system
- Replace existing slave central

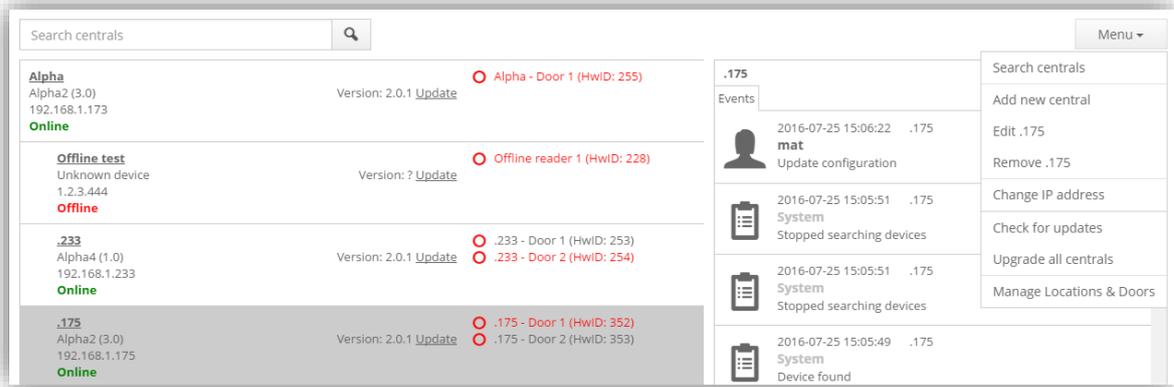
**NOTE!** Double clicking the central that is not in the system will bring up the *Add central* pop-up for a faster addition.

**IMPORTANT!** If a central in the system is RS-485 master, when searching the centrals, a pop-up will show up asking if the RS-485 master should run a search on RS-485 bus too. Keep in mind that the search on the mentioned bus is very slow. The centrals found on LAN will display orderly under the central that found them with their MAC and IP address next to them. Centrals on RS-485 bus will display under the RS-485 master central and only their RS-485 address will be displayed.

### 5.1.2 Changing a central's IP address

Change the IP address of a central by:

1. Selecting one of the centrals.
2. Make sure that the central is added in the system.
3. Selecting the Menu > Change IP address.
4. The correct network data must be provided.
5. By pressing **Change**, the network changes will be committed.



**Picture 5.2: Changing the IP address of a central**

**IMPORTANT!** The following must be entered:

- A new IP address.
- Subnet mask.
- Address of the default gateway.

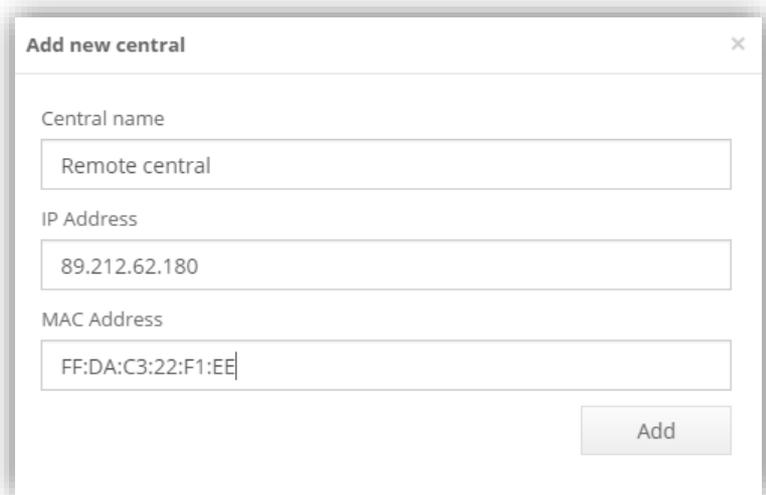
These parameters depend on your network settings. Before you change the address, carefully read displayed warnings, if any.

**REMEMBER:** The IP of the slave central needs to be in the same network as the master, unless you are adding a remote central. If the public IP address of the slave central is provided, and the slave central has the communication port (default 3543) open, the central will be added as a remote slave. Please make sure that the provided public IP is static.

### 5.1.3 How to connect centrals over the internet using remote IP, DNS or DDNS

**IMPORTANT!** When setting up the system this way, the **port 3543 must be port-forwarded on the target's central network**. Please make the requested changes on the router or inform a network administrator about this request.

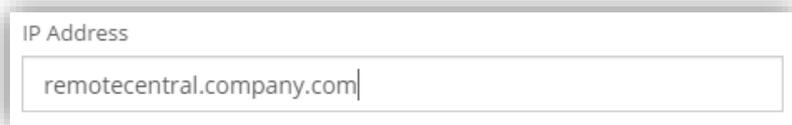
To add a remote central to the system, log-into the top master central and follow the steps of manually adding the central (chapter 5.1.5) while providing the **remote IP address**. Having a static IP address is **mandatory** for such set-up.



The screenshot shows a dialog box titled "Add new central" with a close button (X) in the top right corner. It contains three input fields: "Central name" with the text "Remote central", "IP Address" with the text "89.212.62.180", and "MAC Address" with the text "FF:DA:C3:22:F1:EE". An "Add" button is located at the bottom right of the dialog.

**Picture 5.3: Adding a remote central**

To add a central on DNS or DDNS, instead of IP address, the **Domain name** can be used instead.



The screenshot shows a single input field labeled "IP Address" containing the text "remotecentral.company.com".

**Picture 5.4: Using DNS or DDNS instead of IP**

After the central is successfully added to the system, the central search (chapter 5.1.1) will trigger on both networks, displaying all centrals found.

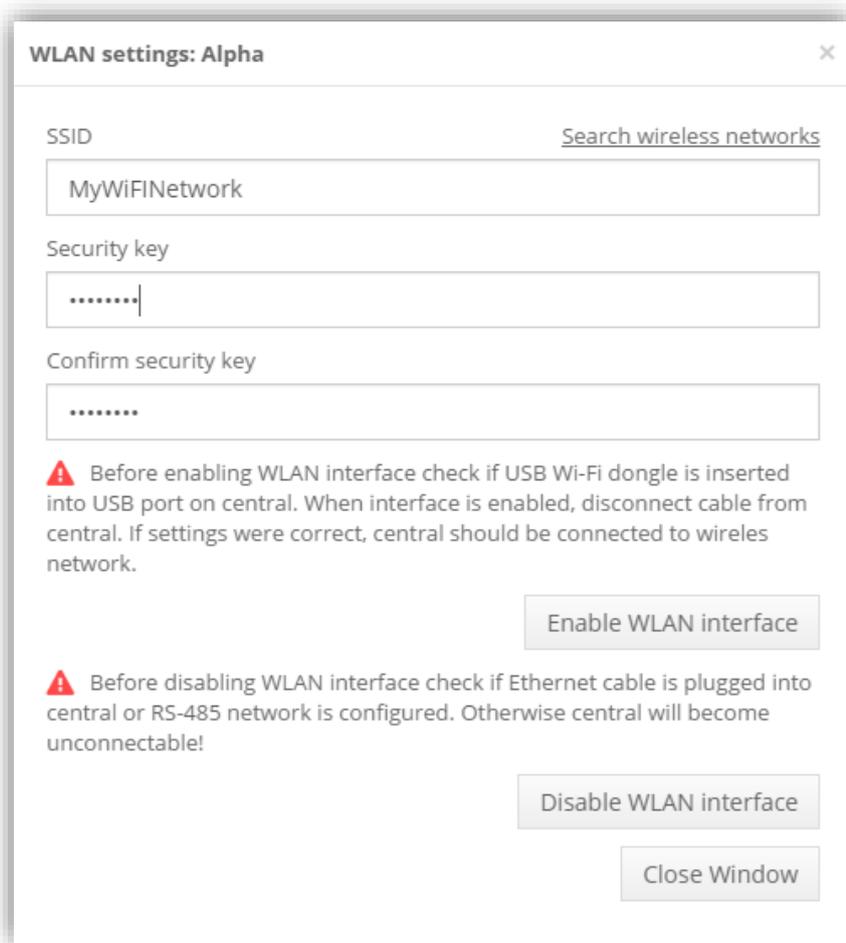
### 5.1.4 Central's WLAN settings

If the central has a USB port installed, it is possible to connect the central via a USB Wi-Fi dongle to an existing wireless network. Connection requires name (SSID) and security key for the wireless network.

**WARNING!** The central only supports wireless networks protected with WPA-PSK (TKIP) and WPA2-PSK (TKIP) encryption!

The wireless settings of the central can be accessed by following these steps:

1. Click the widget Home > Hardware > Centrals.
2. Select the central that you are logged onto.
3. Select **Menu > WLAN settings** from the menu.
4. Type the **SSID** and **security key** into the corresponding fields
5. Click the button **Enable WLAN interface** to establish connection
  - The central will enable the wireless interface and if the provided parameters are correct, it will connect to the provided wireless network.



**Picture 5.5: WLAN settings**

**IMPORTANT!** The wireless interface can only be enabled on the central that the administrator is currently logged-in to. In addition, the wireless interface of a slave cannot be enabled from the master central. Also note that during installation of the wireless interface, the USB dongle and the network cable must both be connected to the central.

After the wireless interface is enabled (confirmation dialog notice), the network cable can be unplugged. Nova is then accessible the same way as before on the network cable.

**IMPORTANT!** If Nova stops working (e.g. the progress spinner in the top right corner keeps spinning), there were some errors with the connection to the wireless network (probably either the SSID or the security key was wrong). Plug the network cable into the central. Wait for Nova to reconnect to the central and then try again.

Search for available wireless networks:

- Click the **Search wireless networks** button next to SSID field in the WLAN settings
- Select from the list of found networks and populate the SSID field, once search is complete

Disabling the wireless interface:

- Click the button **Disable Wireless interface** (visible when central is connected to a wireless network).

### 5.1.5 Adding, removing and editing centrals

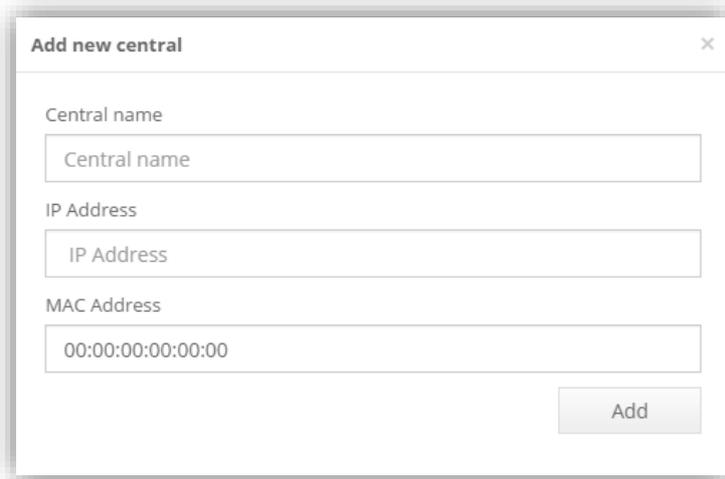
Adding new centrals automatically:

1. Click **Menu > Search centrals** button in the Central editor
  - The list of centrals will be populated
2. Select the wanted central
3. Press Add new central [central's IP address]
  - Popup window: all information will be entered automatically
4. Edit name of the central
5. Press **Add** to save changes

Adding new centrals manually:

1. Click **Menu > Add central** in the Central editor
2. Enter name of the central, IP and MAC address in popup window (Picture 5.6)
3. Save changes

**IMPORTANT!** The default IP address and MAC address are found on the label of the central.



**Picture 5.6: Popup window for adding a new central**

Remove centrals:

1. Select the central from the Central editor
2. Click on Menu > Remove [central name] button

Edit centrals:

1. Select the central from the Central editor
2. Click **Menu > Edit [central name]** button or double click the central from the Central editor list
  - A settings window for the central displays (Picture 5.9):

Multiple tabs will show:

**Readers and Doors** tab (opened by default): Includes management of the readers on the left half, while the right half represents the door settings of the central.

**Settings** tab: Consists of 3 columns:

- General and Network settings on the left – consist of name of the central, country (Set the country for each central – suitable when covering multiple countries with different holidays etc.), IP, netmask, DNS and gateway addresses, along with the MAC address. From here, also select (by checking the checkmark) if the central is on a remote location. If the checkmark is marked, a new field will be added to fill the correct remote IP address.
  - WLAN settings are only displayed for the central currently logged into if the central is the correct type to support Wi-Fi connections.
  - Anti-Passback function settings – read more about Anti-Passback function in chapter 5.1.18 Local Anti-Passback.

**IMPORTANT!** Advanced settings for the central are not available in the NovaSimpli software.

## 5.1.6 Replacement of malfunctioning slave central

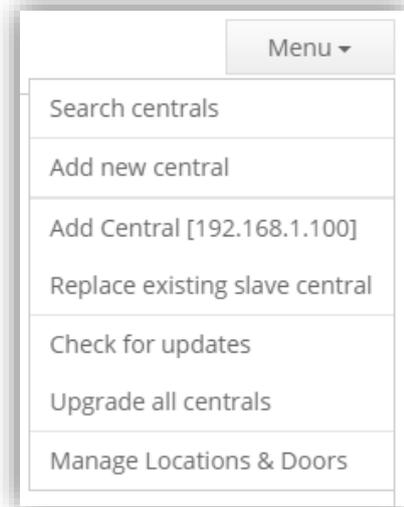
There are many reasons why a central can malfunction and needs to be replaced. Centrals usually have readers and user access groups assigned to them, preventing the deletion of the central.

To keep all of its data and just replace the malfunctioning central, the function **Replace slave central** can be used (Picture 5.7).

To get to manage centrals window on the main menu navigate to:

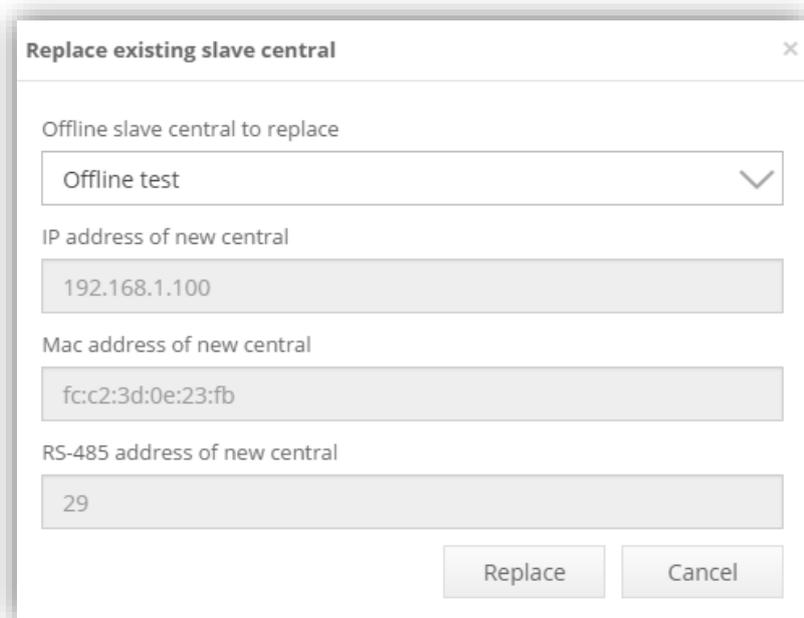
1. Home > Hardware > Centrals.
2. Search for new centrals by clicking **Menu > Search centrals**
3. Select the new central and find the option **Menu > Replace existing slave central**. This option is only available for a central on a default IP address (192.168.1.100).

- A new popup (Picture 5.8) will appear requesting a selection of the slave central that needs to be replaced, while showing the information of the newly added central.
4. Press the **Replace existing slave central** button to start the procedure
- The newly added central will get the data from the master of the system and adjust the time.



**Picture 5.7: Replacing an existing slave central**

**NOTE:** Synchronization can take up to a couple of minutes. After completion, the old central should appear online on the **Picture 5.1 Central editor** and on the IP address of the old central.



**Picture 5.8: Replace existing central pop-up**

## 5.1.7 Replacement of malfunctioning master central

Replacing a master central is similar to the replacement of the slave central but a more complicated process.

To replace a malfunctioning master central, the following conditions must exist:

- the new master central must already be installed in the system
- central must not have any slaves connected to it
- its master must be the malfunctioned central (current master)
  - A **Promote** button will appear in the of the central (Picture 5.9), if the slave central meets the requirements.

For a new master to be promoted:

Log into the slave's GUI (Graphical User Interface) and navigate to the of the central (see chapter 0) from the main menu:

1. Home > Hardware > Centrals.
2. Double click the central that you wish to promote.
3. Navigate to the **Advanced settings** tab.
  - The system will reassign all of the slave centrals including the malfunctioned master to the newly set master.

**NOTE:** Master reassignment and database synchronization can take a couple of minutes to finish.

## 5.1.8 Central settings

### Standard settings

- **Central name:** Used for easier central recognition.
- **Country:** Centrals that have the country set will obey any calendar entries set in the calendar settings.
- **MAC address:** Physical address of the central. Can be also found on the sticker on the side of the central. If the centrals are not properly named, this is the only way to distinguish central between each other.
- **Anti-passback:** Local anti-passback functionality (works only on this central). More about its option can be read in chapter 5.1.18 Local Anti-Passback.

### Connections settings

Master central options:

- **Set central as master:** If this setting is set, this central will not accept any communications from any other master. This setting makes sure data is not lost, if the master should, mistakenly, be added to another system.  
**Master central** is responsible for dividing load to slave centrals. If there are many centrals in the system, it is advisable to have Local master hierarchy,

where there is a top master that handles local masters and local master handles slave centrals.

**RECOMMENDATION:** The Top Master central should be the one that has the least load (least work and readers/doors connected).

Slave central options:

- **Select master central:** Each central must have a master assigned to receive any changes.
- **Connection type:**
  - **IP address** – standard static ethernet connection with the fixed IPs. More about the connection can be read in the chapter 5.1.10 Communication based on IP address.
  - **Remote central host name or IP address** – a new field for entering the remote central hostname or IP is displayed below this option. Recommended for remote (over the internet) connections.
    - **Port 3543** - This port allows communication of the central to pass through. If the central needs to be connected over the internet, this port must be opened on the slave central (the master is the only one that issues commands so only one-way communication is needed). If there is a whole system located on the other side of the internet, it is enough forwarding only the local master port.
      - **RECOMMENDATION:** The default port is 3543 and should stay this way if possible. Changing different port on the outside can be made from the port forwarding settings of the router. Please check the manual of the router on the subject before making any changes.
  - **RS-485** – connects centrals via RS-485 connection. More about it can be read in the chapter 5.1.11 Communication based on RS-485 BUS.
- **Allow system administration:** Allows changes to be made on a slave central. Usually everything is done from the master central and if any changes are made on the slave central, they are overwritten with data from the master. Enabling this option allows Administrators to manage users on that central without losing any changes. This can be helpful if the Administrator is in a different network and do not have direct access to the master central (or the connection between master and that central is not stable).

Common options:

- **Ethernet settings**

Local options (displayed only if connected directly to the central and if the central has USB port):

- **Wi-Fi settings**

## Advanced settings

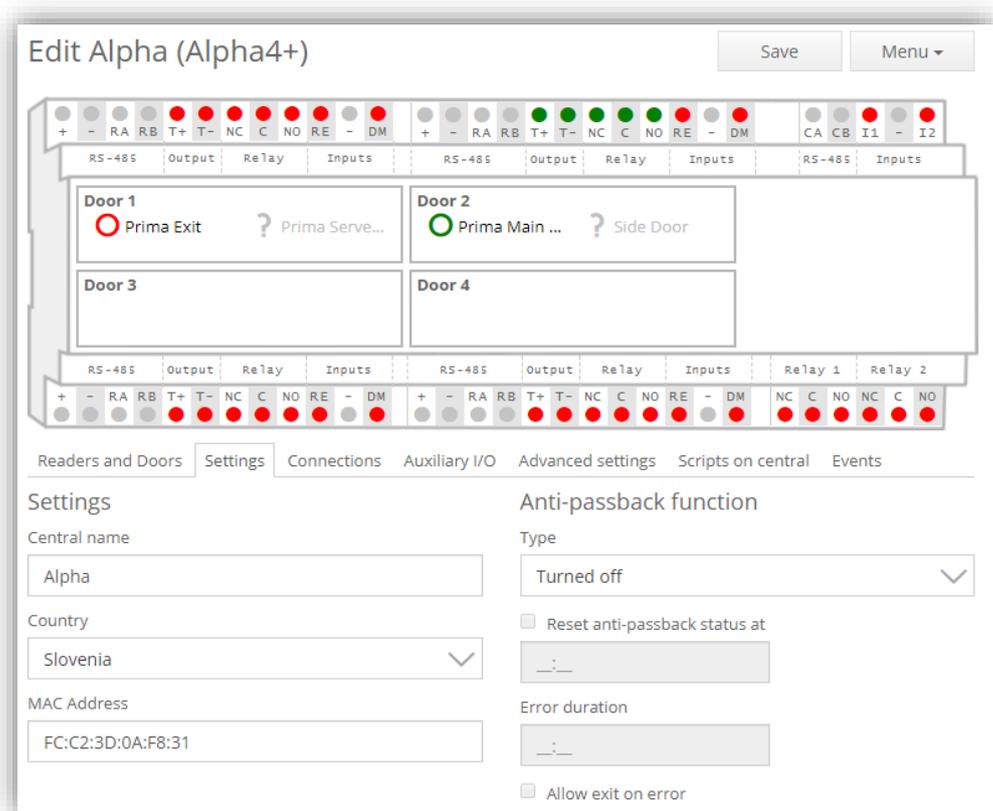
- **Database synchronization:** Just in case something is wrong with the database of one of the slave centrals, press the Force synchronization button to copy configuration database from master to slave. After pressing this button, go to the events page of the central and monitor the progress. After database synchronization, time will be updated as well (more in chapter **5.1.12**).
- **System reboot:** Pressing this button will send the reboot command to any of the central in the system.
- **Upgrade firmware on central:** Selecting the Update button will open a File window, requesting to locate the upgrade software package.
- **Optimize database:** Pressing this button will run a database indexer that might speed up the system, but it takes from a few seconds up to a few minutes.
- **RS-485:** Options to set RS-485 master or RS-485 slave and its address (more on RS-485 connection in chapter 5.1.11 Communication based on RS-485 BUS).

## Scripts on central

These options are only shown if the Scripting activation key and at least Nova10 is applied in the system. For further information on scripting please read chapter **7 Module: Scripting**.

## Events

Displays events that are limited to this **central only!** (The events from readers or any other centrals will not be displayed in this event list).



**Picture 5.9: Central settings**

## 5.1.9 Upgrade software on central

There are three ways to upload software to the central:

1. Navigate to settings of the central (Picture 5.9)
  - Navigate to Advanced settings tab.
  - Click the **Upload** button.
  - Select the .tar package and wait for the process to finish.
  
2. Remote upload – **IMPORTANT!** Remote upload only works with central's software version 1.6 and higher:
  - Navigate to Home > Hardware > Centrals widget.
  - Press the Upgrade link next to the displayed version of the central.
  - You will be prompted to locate the upgrade file.
  - If the central is not master central, the transfer protocol will begin to transfer the upgrade package to the remote central. Once it is completed, the upgrade will start automatically; if the central is the one logged into, it will begin a local upgrade.

3. Remote upgrade of all centrals in the system – **IMPORTANT!** Function only works with centrals version 1.6+ and not for centrals connected on RS-485 bus:
  - Navigate to Home > Hardware > Centrals widget.
  - Press **Menu > Upgrade all centrals** option from the dropdown menu.
  - You will be prompted to locate the upgrade file.
  - The upgrade file will be transferred to **all slave centrals**. **IMPORTANT!** Master central will not be upgraded with this function (some systems have NovaServer as master and require a different upgrade package); it needs to be updated manually!

After upgrade is done, **Central was upgraded** event will be displayed in the Events log. If upgrade was done locally, you will need to log-in again.

If there are some issues during remote upgrade or centrals that are connected on RS-485 bus (connect to the central with network cable), navigate to their IP address and upgrade the central locally – following the 1<sup>st</sup> upgrade description

### 5.1.10 Communication based on IP address

The communication between master and slave central is based on the IP address, set in the field *IP address* in the **Central editor – Connections tab** (Picture 5.9), and on the IP port written next to the IP separated by colon “:”.

**NOTE:** The master central always uses the address in the field **IP address** and port number when communicating with a slave central.

When the master central and the slave central are on the same network:

- The IP address in the Central editor must be the same as the interface IP address of the central (see the section on changing the IP address of a central).
- The port needs to be set to 3543.

Remote network:

When a slave central is located in a remote network (from the master central point of view):

- The field IP address in the central editor must be set to the address of the remote network.
- The address of the remote network is not the same as the interface IP address of the remote central.
- The port must be set to the port number of the remote network, which is forwarded to port 3543 on the remote slave central.

### 5.1.11 Communication based on RS-485 BUS

When a slave central is connected to the master central via a RS-485 BUS, option **RS-485 master central** must be enabled, located in the **Connections** tab of the RS-485 master central (Picture 5.9) by:

- Checking the Set as RS-485 master central checkbox.
  - This setting causes the master central to search and communicate with the slave centrals on the RS-485 BUS.
- Checking the **Set as RS-485 slave central** checkbox in the advanced settings will set the current central as a RS-485 slave (all RS-485 slave centrals must be set after the RS-485 master is set).
- Central search should now prompt the question to search for the centrals connected on RS-485 BUS. Select **Yes** and wait until the search is done. RS-485 centrals will display on list showing only their Modbus address instead of their IP addresses.

**NOTE:** The communication between centrals on the RS-485 BUS is based on the RS-485 address, which is set in the field RS-485 address under the Connections tab settings of the central.

The default RS-485 address of the master central is always 1 and is automatically set when the central is set as RS-485 master. The default address of a slave central is set when adding the slave central to the system and it is also found on the central label.

**IMPORTANT!** The RS-485 address of the slave central is calculated from the last 5 bits of the MAC address, to which you add the value 2 (addresses 0 and 1 are reserved).

Example of RS-485 address calculation:

MAC 00:50:C2:E6:30:6A

6A (hex) = 0110 1010 (bin)

0 1010 (bin, last 5 bits) = 10 (dec) + 2 = 12 (RS-485 address)

**WARNING!** The default address can be changed to any other unused address on the RS-485 BUS. Resetting the address back to its default address, can be done by calculating it like in the example above or hold the left button on the central shown on Picture 23.2 for at least 10 seconds, which will:

- Reset the IP address and RS-485 address back to the default values:
  - => 192.168.1.100 for IP address
  - => default value for RS-485 address and port to 80
- It also enables the **Super administrator account** again, if it was disabled. See Appendix A - Description of LEDs and buttons on central for more details.

### 5.1.12 Database synchronization

The system master central takes care of data synchronization between centrals in the system. In the case where the database of a central is incomplete, a manual synchronization can be done by:

- Clicking the button **Force synchronization** in the advanced settings of the slave

- The master central updates the database on the slave central with the version from the master central.

**NOTE:** Only use this option when there is a certainty that differences between database data exist.

### 5.1.13 Adding new readers

To add new readers to the central:

- Click the **Menu > Search readers** button in upper right corner of the **Central Editor** (Picture 5.9)
  - This triggers recognition of already connected readers and starts search for readers recently connected to the central.

Change address, remove or add readers:

**NOTE:** Reader search **works ONLY from address 1 to 16 (max)**. Addresses from 16 to 64 are user defined addresses and will not be displayed as a search result of a reader search. To avoid complications, keep the reader addresses within limits.

After the search is completed, the addresses of listed readers can be changed and the new readers can be added to the central:

1. Click the **Menu > Change address** button from the menu to change address.
2. **Write new address** and the reader will return with the new entry
3. Select the reader and click the **Menu > Remove reader** button to remove readers from the central
4. Click the **Menu > Add reader** button to add a reader manually, if the address and the connected door of the reader are known.

**IMPORTANT!** When the address of the reader is changed, it remains saved on the reader – if the reader's door socket or central is changed, it will not reset. If the address is changed to more than 16, the central will not find it. The only way to change back from such state is by adding it manually (the address needs to be provided) and once it's connected and online, change its address back to the requested range.

### 5.1.14 Upgrading firmware on reader

SINGLE reader upgrade:

The firmware of a reader can be upgraded to a newer version by:

- Double click on the reader you want to upgrade and navigate to **Upgrade firmware** tab.
  1. Select the option **Upgrade firmware** button. Select the \*.bin extension file with the new firmware in the popup window
  2. The upgrade process will start and it will last for approximately 30 ~ 120 seconds (depending on the workload of the central).

3. During the upgrade process, an operation status dialog will be displayed
4. The reader will beep three times after completing the upgrade process.

**NOTE:** The upgrade option is disabled on readers that cannot be upgraded.

**IMPORTANT!** Centrals with Nova version 1.5 or lower need to update the readers by logging in on every central and update its readers. Higher version software allows the update of the readers from the master central only, which makes it faster and more convenient. The upgrade option is disabled on readers that cannot be upgraded.

Upgrade ALL readers on a central:

1. Navigate to the central on which you wish to upgrade readers.
2. Press the Menu > Upgrade all readers button
3. Select the option **Upgrade firmware** button. Select the \*.bin extension file with the new firmware in the popup window
4. The readers will beep three times after completing the upgrade process.

### 5.1.15 Reader settings

The reader needs to be configured correctly and linked to the desired door for the system to function correctly.

When the reader is selected (Picture 5.10), the following info on the reader is shown:

- State of Enabled flag
- Reader Name and Reader type
- Which door the reader is controlling
- RS-485 address

If the reader is not working or is not needed in the system anymore, it can be disabled by:

- Deselecting the **Enable** checkbox

Now the central will cease to communicate with the reader and its warnings and errors are not visible on the **Events** page.

**IMPORTANT!** Disabled readers are shown in light grey in the locations tree while non-working readers are shown in red.

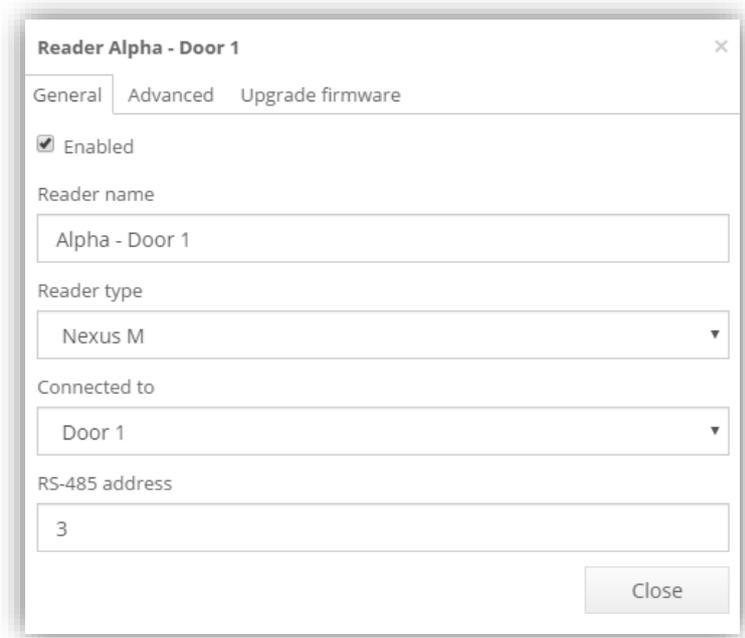
Set up of door that the reader is connected to:

- Set up of doors controlled by the reader
- Set up address of reader

**NOTE:** Usually the reader is connected to the same door that it controls, but it is possible for a reader to control another door on the same central.

To do this, please check Picture 5.11: Advanced settings.). This option is not included in NovaSimpli.

**IMPORTANT!** Note that if the **Connected to** setting of a reader is changed, the option **Opens** (controls what doors are opened by the reader) under **Advanced settings** tab will be updated to the same door. If there were any manual changes previously made in the system, this change resets the manual ones. To make previous options work, the settings need to be manually changed to the previous values.



**Picture 5.10: Reader settings**

**IMPORTANT!** Communication with readers is based on their addresses. It is important that all readers connected to the same door, have unique addresses. If not, the system can behave unpredictably.

Reader settings on Picture 5.10 shows the settings needed for basic operation.

Change additional parameters by:

- Selecting the **Advanced** tab (Picture 5.10) – the options are:
  - Select which door the reader controls
  - Set direction for each reader (Entry, Exit, Pass through, I1 entry – I2 exit)
  - Set sensitivity on the tamper sensor

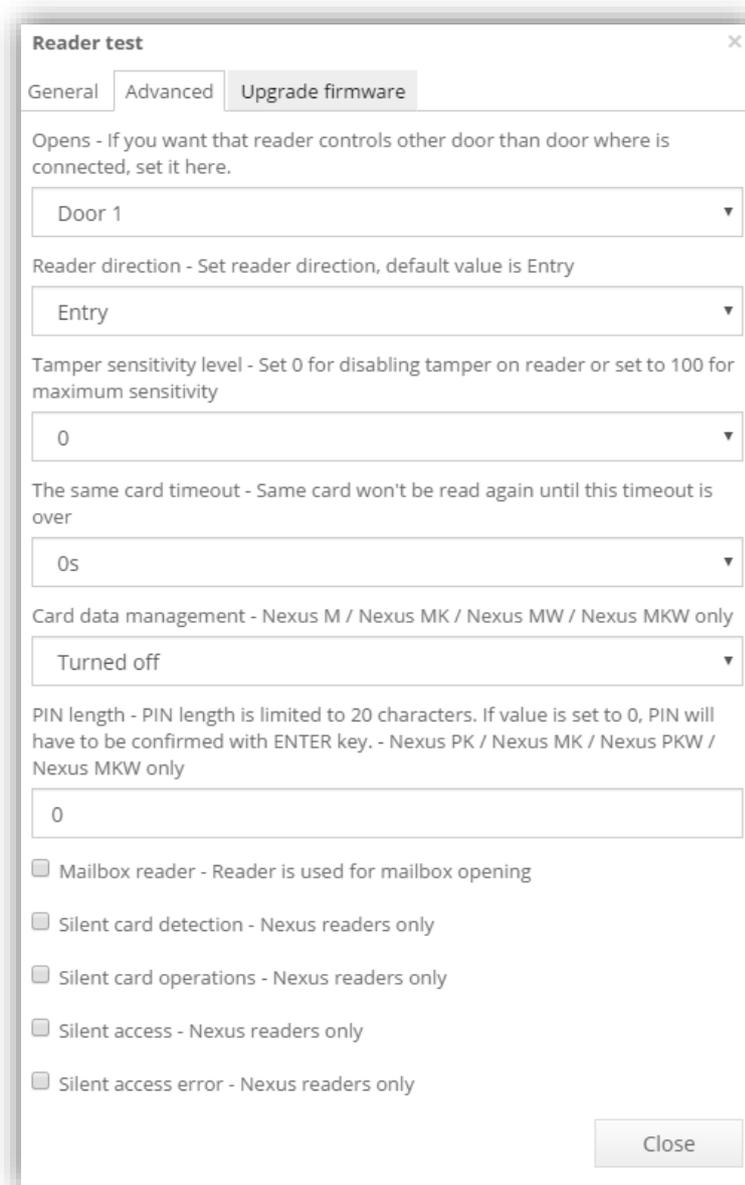
Further options:

- Setting value for **Same card timeout**
  - This setting enables a timeout before the central will process a card from the same user again.

E.g.: After a user has opened a door with the card, the user will not be able to open it again with the same card until the timeout is over. However, the central will process cards from other users during this period.

- **Enabling the writing of offline access rights to user cards** (only possible if the reader supports writing to cards). Offline readers read these access rights from the card. (See section 5.2 Offline readers for more information)
  - Setting value in **PIN length** field
    - This defines how users enter their PIN on current reader
      - If the value is greater than 0, then PIN is accepted as soon as the last number is pressed on the keyboard.
- Remember:** When PIN length is defined, PINs of all users have to match the defined length.
- If value is set to 0, users will have to confirm their PIN with the ENTER key on keyboard.
- **Mailbox reader** checkmark – If this checkmark is set, the reader is assigned to open mailboxes instead of doors (including checking the rights).

**IMPORTANT!** Last four options are not available in the NovaSimpli software.



**Picture 5.11: Advanced settings of readers**

## Reader sounds

Nova version 2.1 also brings the option to remove any sound from the Nexus readers. Different options are displayed in the reader's advanced settings - Picture 5.11.

- **Silent card detection** – removes the first beep when card is detected by reader.
- **Silent card operations** – whenever the reader is set to writing data to the card, the card should be held on the reader until it's done and then grant access. This option silences the sound during the procedure.
- **Silent access** – replaces access granted sound with green LED blink.
- **Silent access error** – replaces error beep with a red LED blink.

Additionally, there is an option to **remove sound from REX** input. This can be done by checking the corresponding option on the door settings (option displayed on Picture 5.12).

### 5.1.16 Door settings

Picture 5.12 shows the settings for doors on the central, which gives the following options:

- Set allowed time for the **electric lock open time** (Electric lock open time)
- Set allowed time for a door to **stay open** (Allowed door open time)
- Set allowed time for how long a reader should **warn user to close door before alarm turns on** (Door opened warning duration before alarm goes on)

The screenshot shows a settings window titled "Door 1 - Settings". It contains the following elements:

- Electric lock open time:** A dropdown menu set to "800ms".
- Allowed door open time:** A dropdown menu set to "4s".
- Door opened warning duration before alarm goes on:** A dropdown menu set to "5s".
- Checkboxes:**
  - Silent request to exit
  - Silent warnings and alarms
  - Door forced detection
  - Door forced detection - Silent mode
  - Use this door for interlock
- Electric lock open voltage level:** A dropdown menu set to "High".
- RE input active voltage level:** A dropdown menu set to "NC".
- DM active voltage level:** A dropdown menu set to "NC".
- Automatic opening schedule:** A field containing "06:00 - 18:00" with a trash icon and a dropdown arrow. A link "Manage schedules" is located to the right.
- Reader settings:** A button at the bottom right.

**Picture 5.12: Door settings**

Picture 5.13 is an example that shows the relation between the described times.

- The door was opened at 11:33:43 and stayed open.
- Ten seconds later the reader started to warn the user with a beeping sound that door should be closed (11:33:54).
- The user did not react on the warning, so ten seconds later the alarm went on (at 11:34:04).
- The user finally closed the door at 11:34:14.
- The settings on the door were the same as Picture 5.12.

	2016-07-29 11:34:14	Alpha - Door 1	<b>System</b> Door left open closed
	2016-07-29 11:34:04	Alpha - Door 1	<b>System</b> Door left open alarm
	2016-07-29 11:33:54	Alpha - Door 1	<b>System</b> Door left open
	2016-07-29 11:33:43	Alpha - Door 1	<b>System</b> Door manually opened
	2016-07-29 11:33:19	Alpha Relay1	<b>System</b> Request to exit

**Picture 5.13: Doors left open and alarm times, example case**

Further options:

- **Silent request to exit** – reader won't make a sound when the request to exit button is pressed. This also works with multiple readers connected to the same door.
- Select **Silent warnings and alarms** to avoid reader from making any sound at warnings or alarms. The events will still be displayed.
- **Disable warnings and alarms when door is unlocked** – when checked, it will not display or trigger any mentioned events.
- Select **Door forced detection** when there are doors with readers on each side.
  - In this case, the central has total control over the door and can detect if the doors are not opened by readers and will trigger a "door forced" alarm.
  - If no alarm sound is wanted, the administrator can choose the **Silent mode** option

- **Use this door for interlock** – doors that are set to use interlock cannot be opened at the same time (we need to wait for other interlock door to close before we can open a specific interlock door on the central).
  - A single interlock functionality will only work on that specific central and not on multiple centrals across the system.
  - A single interlock can be set up on each central.
  - Card or REX access will not be granted if other interlock doors are unlocked or opened or if you want to open the already opened door.
  - Users with **Privileged access** (page 29) are not limited by this functionality.
  - When access is denied, an event will be triggered.

**IMPORTANT!** The described settings (except Electric lock open time) can only be used with electrical locks having a DM (door monitor) signal line. If not, the central cannot detect if doors are open or not and the described settings have no meaning.

In case of fire or power supply failure

An electric lock usually requires a positive voltage level to be in the locked state and neutral (or low) voltage level for opened, unlocked state.

The reason is that in the case of fire or power supply failure the electrical lock switches to unlocked state and users can go through the door.

The option can be enabled by:

- Matching the option **Electric strike open voltage level** to the required voltage level for the locks used in the system.
- The options **RE input active voltage level** and **DM active voltage level** need to be set according to the system characteristics.
  - The central will open the door when the signal level on RE input (Request to exit) matches selected state.  
**Unlock when active** options will unlock the door until the **signal is present with additional lock open time**.
  - The central will know that the doors are open when the state of the DM signal matches the selected state (High or Low).

If there is a need to use DM and RE inputs with Scripting module or Parking Controller, the option can be set to:

- Select **Unused** option in drop down menu.
  - This will effectively unbind default behavior of DM and RE inputs, which can then be used for other purposes.
- **Unused NO / Unused NC** option can be set for solutions like Parking controller where a loop would have to give signal in order to get access, but it cannot be mounted for whatever reason, we can fake the activity with these options.

### 5.1.17 Scheduled door opening

In the Nova software, there is an additional option:

- A schedule can be selected from a drop-down list and assign to target doors (Picture 5.12 – bottom option).
  - Doors will automatically be locked and unlocked based on the time intervals of the selected schedule (see part **4.4** for **Managing time schedules**).
- By clicking the **Manage Schedules** link, the **Time schedule editor** can be accessed and:
  - Edit schedules
  - Preview schedules

**NOTE:** This is not possible in NovaSimpli as time intervals here are always set to 0-24 hours.

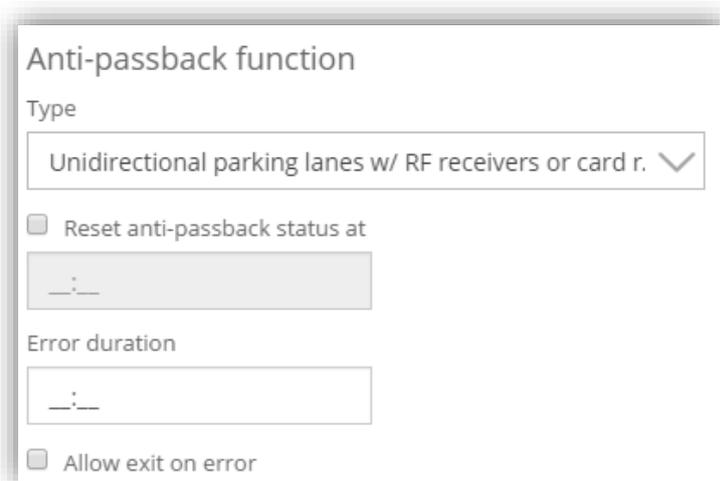
**TIP:** The option to automatically lock doors can be assigned by an automatic schedule with defined time interval of 1 minute that runs out when doors need to be locked.

### 5.1.18 Local Anti-Passback

Sometimes the system needs to control the entrances and exits of users. There are multiple ways of achieving the results based on the hardware setup.

**IMPORTANT!** This instance of anti-passback can be only set-up and it's working on a single central with its local readers.

- The settings can be enabled in the **Settings** tab shown on the target central (**Home > Hardware > Centrals > Edit**).



The screenshot shows a configuration window titled "Anti-passback function". It contains the following elements:

- A "Type" dropdown menu with the selected option "Unidirectional parking lanes w/ RF receivers or card r." and a downward arrow.
- A checkbox labeled "Reset anti-passback status at" which is currently unchecked. Below it is a time input field showing "0:00".
- A label "Error duration" above another time input field, also showing "0:00".
- A checkbox labeled "Allow exit on error" which is currently unchecked.

**Picture 5.14: Anti-passback settings**

There are numerous ways of setting up the method depending on requested functionality:

1. Bidirectional entry and exit lanes with one RF receiver
2. Unidirectional entry and exit lanes with RF receivers on card readers
3. Bidirectional door with card readers
4. Bidirectional doors with card readers and DM confirmation.
5. Turned off

Below section will describe in details and explain how to set-up:

### **1. Bidirectional entry and exit lanes with one RF receiver.**

This method only uses a single ramp for entry and exit from the parking space.

To set up **bidirectional** entry and exit lanes:

- RF receiver direction must be set to **I1 Entry - I2 Exit** (please see chapter 5.1.15 for Reader settings).

### **2. Unidirectional entry and exit lanes with RF receivers on card readers.**

This method is meant for parking spaces with separated entry/exit ramps.

E.g. When the car stops at the entry, Input1 on the central is triggered and with the proper RF signal opens the ramp. The same way goes for the other direction, but this time Input2 triggers for the exit direction.

To set up **unidirectional** entry and exit lanes:

- RF receiver direction must be set to **I1 Entry - I2 Exit** (please see chapter 5.1.15 for Reader settings).

**IMPORTANT!** If **DM active voltage level** on Entry is set to NO, and an automatic schedule opens the door, the timeout alarm will possibly go off when the car leaves (Input activated). If **DM active voltage level** on Entry is set to NC, and door on Entry opens, the alarm will trigger the same when the car is at ramp for too long. To solve the alarm problem, DM active voltage level must be set to **Unused**.

### **3. Bidirectional door with card readers.**

To set up bidirectional door with card readers:

- There has to be at least two (2) readers connected to the system. The direction of the readers has to be specified in Nova. One has to be set as **Entry** while the other one has to be set as **Exit** (Please see chapter 5.1.15 for Reader settings). The system keeps track on when the user places his/her card on the readers for entry/exit.

#### 4. Bidirectional doors with card readers and DM confirmation.

To set up bidirectional doors with card readers and DM confirmation:

- The option with "DM confirmation" works on the same general principle as the previous one. The main difference is the tracking of the doors. When the doors are opened, the door monitor is activated and the user entry is counted when door closes.

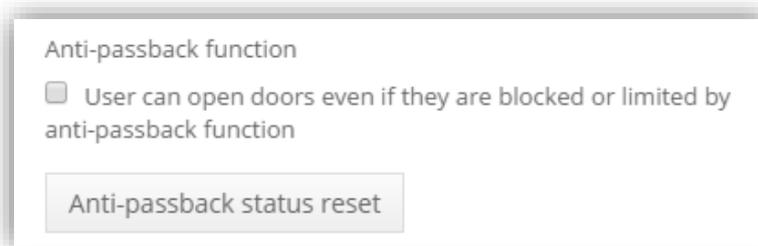
#### 5. Turned off

This method disables the Anti-passback functionality.

Additional anti-passback settings:

- The **Reset anti-passback status** option is there to reset all set states once per day (if enabled and the hour is provided).
- Setting **Error duration** option will prevent users to re-Enter/re-Exit for a set time and only allow access when that time passes.  
E.g.: Setting it to 00:30, will allow user to enter, but on the second try, the access will be denied. After 30 minutes, the user can make another entry.
- The last setting for anti-passback function is called **Allow exit on error**.
  - Enabling this allows users to exit even when there is an anti-passback error.  
E. g.: A user entered a building but entered with the entry card of someone else. If the user then wants to get out it is not possible, because the card of the user was never put on entry reader. Allowing exit on error will allow the user to exit with their card.

**Individual user settings** – found under the **Advanced** tab of a user:



**Picture 5.15: Individual Anti-passback options**

- If the Anti-passback function is set on the central and we wish that some of the users are not affected, tick the checkbox next to the **User can open doors even if they are blocked or limited by anti-passback function**.
- Pressing the **Anti-passback status reset status reset** button will show a pop-up window, allowing you to:

- Manually reset status of the current user.
- Reset status for ALL users in the system.

### 5.1.19 Alarm, tamper and additional relays management

In the software version 2.1, a new tab was added under Edit central page - **Auxiliary I/O**. This option enables you to control the general inputs and the two additional relays (if the central is correct type).

#### Tamper Input

**Input 1** is intended to be used as Tamper when the central is mounted in the DIN-rail box. This way the administrator is informed, if someone had opened it.

- **NC:** The default state – when the box is opened, the circuit is broken and Tamper activated event triggers. Once the box is closed again, the event Tamper deactivated will be shown in the event list.
- **NO:** The inverted version of NC.
- **Unused:** No event will be triggered.

**NOTE:** Except the Tamper activated event displayed in the Errors section, there is no other action executed on the central. For other custom actions, please refer to the chapter 7 Module: Scripting).

#### Alarm Input

**Input 2** is intended to be used as an alarm trigger.

- **NC:** The default state – when the circuit is broken, the Alarm activated event will be added and displayed under Errors. Whenever the circuit is re-connected, Alarm deactivated event will be shown.
- **NO:** The inverted version of NC.
- **Unused:** No events displayed/triggered.

**IMPORTANT!** The alarm settings are not a reliable source and are not approved by any fire regulations or norms. Please use this only as a helping tool in case of emergency.

After you agree with the disclaimer, the dropdown with the Alarm functions are displayed:

- **Turned off** – this central does not react on signal received from its own Input 2.
- **Open doors on this central** – if the central receives a signal from alarm, it will unlock/lock all local relays and transistors until the signal ends.

Next two options require Fire alarm module:

- **Open all doors in the system** – if there is alarm signal received on this central, it will unlock/lock all doors in the system until the signal ends.
- **Alarm action access group** – a custom alarm that triggers a special access group on alarm start/end.

Find the detailed instructions in chapter 18 Module: Fire alarm module.



## 5.2 Offline readers

Offline readers are units that act as part of an access control system when correctly configured, but they are not wired to the central.

Management is done through the Nova software with help of configuration cards and the read/write function of online readers.

Access rights are written to the card when registered on an online reader. When same card is used on offline reader, the data is read from the card and access is granted or denied.

Management of offline readers:

Open **offline reader editor** (Picture 5.16) by:

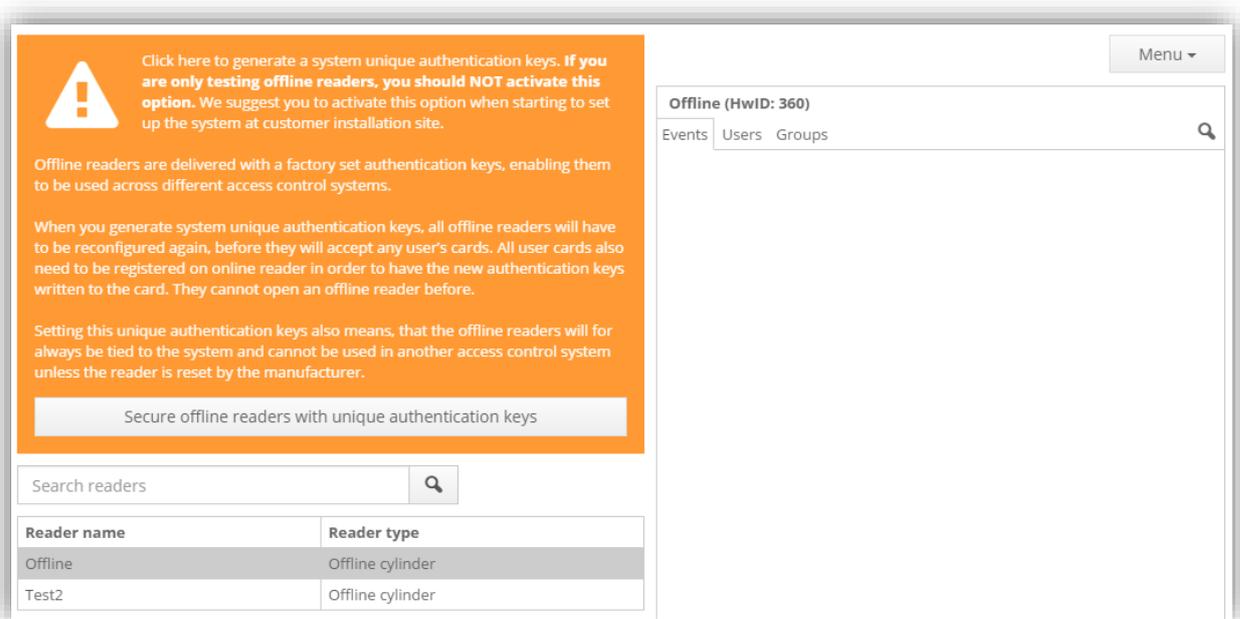
- Navigating to Home > Hardware > Offline Readers widget

Left-panel:

- **Search** option to display only groups/types of readers OR for faster access of the reader if the list of offline readers is long.
- **List** of all offline readers in the system and their type.

Right-panel:

- Preview of currently selected offline readers.
  - Last **events** transferred from the offline reader.
  - List of **users** with access to the selected offline reader.
  - List of **Access Groups** with access to the selected offline reader.



**Picture 5.16: Offline reader editor**

**IMPORTANT!** The system is using (**UNSAFE**) default authentication keys on MIFARE cards until manual activation of security in the software.

How to do this:

- Click on **Secure offline readers with unique authentication keys** button (Picture 5.16).

**RECOMMENDATION:** Change authentication keys before adding the first offline reader to the system to ensure that user cards and newly added offline readers use secured authentication keys from the beginning.

**NOTE:** Changing authentication keys later, will mean that all user cards and offline readers need to be re-configured with the new authentication keys. If the system contains any offline reader and the offline keys are not protected, the new versions of software (version 1.6+) will display a warning at login (Picture 5.17).

Offline readers are not protected with secure authentication keys! Click here to secure your system!

**Picture 5.17: Unprotected offline system warning**

Differentiating between offline readers:

When adding a new or editing an existing offline reader, the administrator can:

- Change its name
- Change its type

- The system automatically generates the reader address. This address differentiates between offline readers in the system (Picture 5.16).

**IMPORTANT!** NovaSimpli does not include the offline functionality. Consider upgrading to Nova10 or higher to utilize the offline functionality of the access control system.

Customized settings:

Based on reader type, some settings can be customized to control the offline device. The options not supported by the offline reader are greyed out (Picture 5.18).

### **Time slider**

The time sliders offer the same functionality as for online readers (for detailed information see chapter 5.1.16 Door settings for online readers). This allows the option to set different kinds of timeouts for the offline reader devices.

### **Trace users**

To trace users:

- Uncheck the option at Disable events log on user's card.
  - The offline reader writes the time of card registration to the user card.
  - This data is copied to the system the next time the user uses this card on an online reader.
  - This option uses more battery on the offline reader.

### **Transfer of events:**

Offline devices have an internal log of all events that is transferred to the system by:

- Using the events card (for further info see section 4.2.2 Card function assignment). Checking the option **Disable event log on offline reader** will disable the log.

### **Increase security:**

To increase the security, the system can be set to require a PIN when entering a door with a card.

- Check the option Request input of user's pin.

**NOTE:** This option is only available, when the offline reader has a keypad.

### **Toggle mode**

To enable toggle mode for the individual user:

1. Navigate to Home > Users & Access Rights > Users.
2. Double click a user and navigate to the **Advanced** tab.
3. Check Toggle output on offline readers.
4. Transfer the settings to card by placing it on the online reader that has writing to card enabled.
5. Hold the card (2<sup>nd</sup> read) on the offline reader to toggle it.

If wanting to overwrite toggle mode:

- Check **Ignore Toggle output setting on user's cards** in the settings of the individual offline reader. This prevents the reader from using toggle mode, even if the user has the rights to activate toggle mode on readers.

### Time intervals

To check the time intervals on user cards:

- Select **Check time schedule on user's cards** in the settings of the offline reader.
- The time schedule can be set in the **Advanced settings** for the individual user (see Picture 4.6) under **Cards Validity Settings**.

**NOTE:** Only the first two intervals will apply, if more time intervals are defined.

### Disable automatic reader activation

This option controls its reading:

- This option is checked: The reader will need to be woken up (turn for a cylinder; a push on handle...) before user cards are presented.
- If this option is not checked: The reader will repeatedly check for any present user card.

**NOTE:** This option is more convenient for more "active" doors, since the reader always needs to be checking for card. This also means that the battery consumption is higher than normal.

### Automatic schedule

An offline reader has the option to be automatically locked or unlocked by using an automatic schedule:

- Select a schedule from the drop-down list at **Automatic schedule**
  - The reader will use selected schedule after reconfiguration

**NOTE:** Only the first interval will apply for automatic function, if more time intervals are defined in selected schedule.

To edit and preview schedules, access the **Time schedule** editor by:

- Clicking the **Manage Schedules** link (read more in 4.4 Managing time schedules).

**TIP:** The doors can automatically lock doors by assigning them an automatic schedule with defined time interval that starts and ends at the exact time that they are set to lock the door (E.g. 16:00 – 16:00).

**Remarks** input field allows saving some information regarding the offline reader. For example, the administrator can write information about last battery change.

**IMPORTANT!** Remember to save changes by clicking the **Save** button before closing the editor!

Edit offline reader Entry

General Wireless online mode Events Users Groups

Enabled

Reader name

Entry

Reader type

Offline cylinder

El. strike or cylinder knob open time

3s

Do not write event log to user card

Do not save user events on offline reader

Ignore Toggle output setting on user's cards

Check time schedule setting on user's cards

⚠ When checked, users need an assigned time schedule for using the door!

Disable automatic reader activation

Automatic opening schedule [Manage schedules](#)

⚠ Use only time schedules with one (1) time interval!

Remarks

Remarks

**Picture 5.18: Offline reader settings**

### 5.2.1 Offline readers and maintenance cards

Offline reader maintenance is done with special cards. These cards are delivered to the system administrator during system installation and are labelled according to their functionality:

- **BL:** Blacklist card (used for blacklisting user cards)
- **EV:** Events card (used for transferring event list from offline reader to central)
- **CO:** Configuration card (used for transferring configuration settings to an offline reader)
- **B:** Battery card (used for replacing batteries on an offline reader, if applicable)
- **DI:** Disassembly card (used for disassembling an offline reader, if applicable)

**IMPORTANT!** The cards must be assigned to the system administrator and the matching function for each card must be selected (see the section on adding users for information on how to change the card function).

All cards, except the **configuration card**, work on all offline readers after they are registered on an online reader and data has been written to them. The **configuration card** must be created for the individual reader every time due to access configuration details.

The function **Format card** clears data content from card when presented on online reader.

## 5.2.2 Creation of configuration cards for offline devices in Nova software

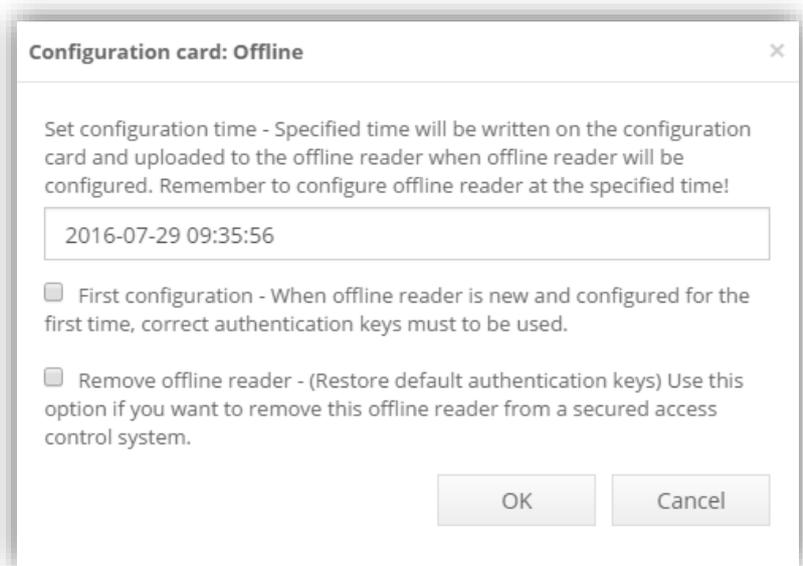
The maintenance card for transferring configuration settings to an offline device must be created for each offline reader.

To create a configuration card:

1. Select the offline reader in the Offline reader editor (Picture 5.16)
2. Click the button Create configuration card
3. Set time of actual device configuration in popup window – actual time of when the configuration card will be presented to the offline reader (Picture 5.19)
  - This is necessary due to time synchronization between online system and offline reader (Picture 5.19).

Adding new offline readers to system:

1. Check the **First configuration** option (Picture 5.19).
  - This will ensure the right authentication keys on configuration card.
2. **Confirm the settings** of the configuration card.
3. To upload the configuration, put the **configuration card** on an enabled online reader, which has the ability to **write data on cards**.
  - The configuration settings are written to the card and three “beep” sounds confirm the successful write.



**Picture 5.19: Create configuration card**

**IMPORTANT!** There is a 15 minutes period to register the configuration card on an online reader. After these 15 minutes, the procedure will have to be repeated.

**NOTE:** The configuration card transfers the settings of a particular reader, and it must therefore be registered on the offline reader it was created for. The configuration card with the particular setting can only be used once.

Three long beeps, three short beeps and green LED flash follow correct configuration.

**REMEMBER** to configure the offline reader on the set time from the pop-up window, in order for it to be synchronized with the online system.

Restoring default authentication keys

The configuration card also allows removing the offline reader from the system. The procedure is the same as creating the offline reader for the first time; instead, check **Remove offline reader**. After approaching the configuration card to the online reader and transferring the configurations to the offline handle, its **keys are restored** to default ones. Removing the offline device from the system is now safe.

**NOTE:** This option is only visible when using unique authentication keys in the system.

### 5.2.3 Lost and blacklisted cards

Lost user cards can be blocked on offline readers to prevent unauthorized entries. Offline readers will ignore cards, which are on their blacklist.

To report a lost card:

- Go to user card settings
- Set function of the card to **Lost card**

- (See section on adding users for information on how to change card functions)
- The **Blacklist card** transfers the database of **lost cards** to offline readers.
- When a **Blacklist card** is registered on the online readers all cards with the function **Lost card** are written to it.
- Offline readers will read the ID numbers of lost cards from the **Blacklist card**.

**NOTE:** The same **Blacklist card** can be used on all offline readers.

To remove a card from the blacklist, change **lost card** to usable **card**:

- Change the function to **Card**
- Repeat the procedure described above

Lost cards can be also transferred via user cards. To read more about this setting, please read chapter 5.2.11 Blacklist settings.

## 5.2.4 Reading events from offline devices

Offline devices keep track of internal events and can keep track of users' events. Events are stored in the internal memory of the device.

Events are written to the card, and are then registered in the software when the card passes an online reader.

To transfer events from the offline reader internal memory:

- Use the **Events card** on the offline reader that the events should be transferred from.
  - The events are now transferred to the Events card and deleted from the offline device internal memory!

**REMEMBER** to register the **Events card** on the online reader before reading events from another device!

**NOTE:** Same **Events card** can be used on all offline devices – one at a time.

The tracking of user events on the internal storage of the offline device can be turned off under the settings for the device in Nova.

## 5.2.5 Configuration of online reader settings for writing access rights

Transfer data between the central and an offline reader by writing data to a contactless card. This data writing usually takes place at building entries to guarantee the best user experience. The offline reader then reads the data.

To enable online readers to write access rights to cards:

- Go to the **Advanced settings** of the reader
- Enable writing with the option in Card data management dropdown list (See 5.1.15 Reader settings).

## 5.2.6 Offline readers and Nova software

Offline readers act in the same way as online readers in the Nova software. The only difference is the icon in the hardware tree that:

- Does not show the current door status.
- When assigning access rights to offline readers the administrator does **not** have the option to select a time schedule, action and source identification device.
  - These are pre-selected and fixed to a '0-24h' time schedule with the actions OPEN and CARD as source identification device.
  - Limit access using time schedules on user level.

## 5.2.7 Battery level on offline cylinders

SensoLock®, the offline cylinder, has a built-in battery management that has three different ways to display battery capacity and inform when replacement is necessary. The battery status can be seen in the Nova software, if the **Offline+ activation key** is registered in the system.

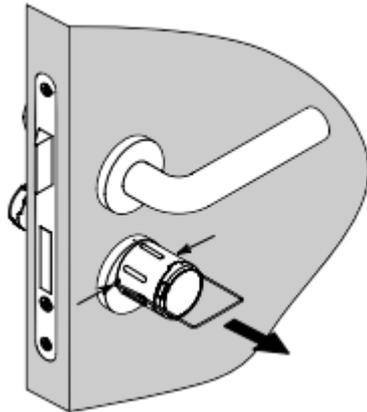
Discovery of low battery level follows these three phases:

1. Five red flashes and sound signal appear when holding a tag/card in front of the cylinder knob.
  - Change the batteries using the **Battery card** and the battery tool as described in section 5.2.8.
2. A light and sound signal appears when holding a tag/card in front of the cylinder knob. It takes 5 seconds before the cylinder is ready for opening or closing.
  - Change the batteries using the **Battery card** and the battery tool as described in section 5.2.8.
3. The cylinder will not read any activated tags/cards. When the cylinder is in phase 3, it is necessary to use an adapter for battery changes.
  - Remove the logo-plate and attach the battery-adapter with a 9V battery. Then change the batteries as described in section 5.2.8.

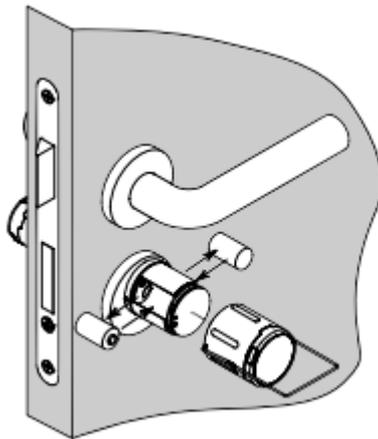
## 5.2.8 Changing batteries in offline devices

When a card is assigned as **Battery card** (see section 4.2.2), it can be used to replace dead batteries in offline cylinders:

1. Present **Battery card** to cylinder
  - o The two small side tabs on the SensoLock® will loosen
2. Use battery change tool to push the tabs and remove the cap

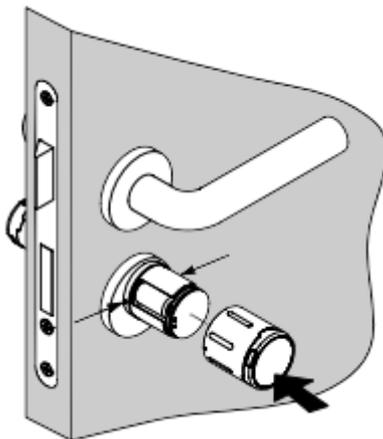


3. Replace the two CR2 3V Lithium batteries



**IMPORTANT!** Make sure that the batteries are placed in correct position regarding plus and minus.

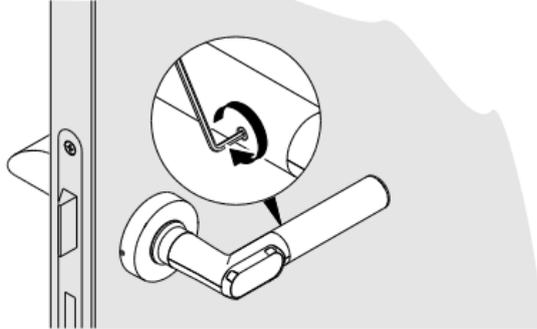
4. Push the cap back on cylinder



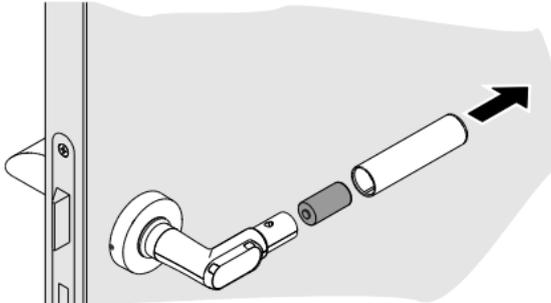
5. Make tabs fit into cap holes
6. Hold **Battery card** in front of cylinder to lock the tabs

Offline handle battery replacement:

1. Open the door where the handle is located.
2. Use the provided key to screw the screw into the inside of the handle.



3. Remove the gripping sleeve.



4. Remove the battery and insert the new battery. Pay attention on the correct polarity. Insert the battery into the gripping sleeve with the negative pole first.
5. Slide the gripping sleeve back on.
6. Unscrew the screw on the inside of the door handle.

### 5.2.9 Offline device feedback

Offline devices give feedback to users in the form of sound and light signals in numerous variations:

- Short or long beeps
- Different combinations
- Different variations of green and red LED flashes.

Table 5.1 summarizes different functions and feedback from the device.

Function	Offline cylinder, OfflineEvoLock cylinder, Offline locker lock, Offline handle		Offline Nexus reader	
	Acoustic signal	Visual signal	Acoustic signal	Visual signal
Quiet mode / Sleep				
Service mode start	- o		/	/
Service mode end	o -		/	/
Reading card after wakeup				
User card rejected	—			
User card accepted				
Scheduled toggle / toggle			—	
Battery replacement / reset	—	+		
Actuator error	— — — — — o o	5X	/	/
Configuration change	— — — o o o		— — — o o o	
Battery warning Phase 1	o o o o o	5X	o o o o o	5X
Battery warning Phase 2	o o o o o	5X  5X	o o o o o	5X  5X
Battery warning Phase 3	o o o o o	5X	o o o o o	5X

- green LED on
- green LED blink
- red LED blink
- red LED on
- long low beep
- short low beep
- o short high beep

**Table 5.1: Functions and feedback of different offline devices**

### 5.2.10 Card segments of offline reader

Nova software version 1.5 or higher support card segment settings for offline readers.

NOTE: To access this option, navigate to the Home > Hardware > Offline Readers and press Menu > Global Settings.

This functionality allows the System administrator to set different writing sectors on the cards.

- This is useful for those who keep other data stored on their cards. E.g.: If there is some data already written on sectors seven and eight, authentication segment sectors can be moved to take place from one to five.
  - o This will allow users to keep their data on wanted segments.
  - o Additionally, feedback segment sectors can be changed the same way. Feedback sectors are only written on card if the reader is set to **Write data on card** and **Read events from user cards** (Please see chapter **4.2.3 Managing users, their access rights**).

IMPORTANT! Whenever sectors are changed, ALL cards need to be reprogrammed! It's recommended to set the different sectors before programming the cards.

**IMPORTANT!** If the system was already set-up and the card segments were changed after cards were already programmed, the old sectors will remain on the old position, while the new ones will be written on the newly set positions. To ensure enough space on the card for the (offline and 3<sup>rd</sup> party) data, please follow the examples in the next table:

Default sectors		Newly set sectors		Unmodified sectors	
User data	Feedback	User data	Feedback		
5-9	10-12	1-5	13-15	none	<b>0 FREE</b>
5-9	10-12	8-12	5-7	1-4, 14-15	<b>5 FREE</b>
5-9	10-12	1-5	6-8	13-15	<b>2 FREE</b>
5-9	10-12	8-12	13-15	1-4	<b>4 FREE</b>

Above example shows how sectors can be moved and which ones remain unmodified. The first example (the "not ok" one) shows the result of no unmodified sectors, which can be problematic for some people, who want to have some sectors reserved for some other data on the card. Remaining examples show a range of sectors that remain free for others to use.

The offline reader will work regardless of the unmodified sectors as long as it has set sectors "free".

**NOTE!** Formatting a card will delete all accessible data, while 3<sup>rd</sup> party data is protected and will not change.

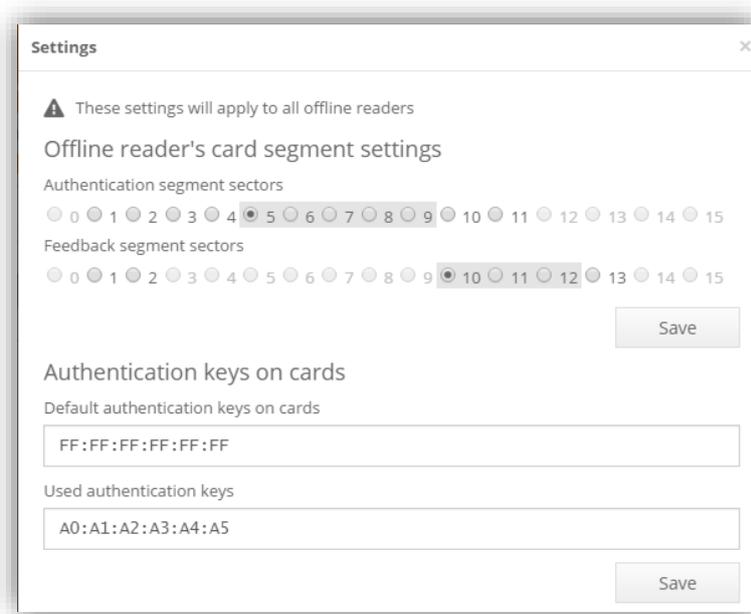
### 5.2.11 Blacklist settings

By navigating to offline Global settings (**Home > Hardware Offline Readers and Menu > Global settings**) a popup window will display the option to enable the Blacklist setting. If the option is checked, the blacklisted cards will be transferred via user cards. The procedure is the same as with blacklisted card – admin sets a card to lost in user interface. After a user puts a card on the online reader, a lost card is added to his card. When this card is put on the offline reader, the setting is now stored on the offline handle and the access rejected for the lost card.

If the card is later found and set as a standard card again, the access limitation can be removed by updating the Blacklist card and showing it to the offline reader.

### 5.2.12 Offline authentication keys

**NOTE:** The option to change authentication key is limited to **Super administrator only!**



**Picture 5.20: Changing authentication keys**

Section **Authentication keys on cards** allow changing authentication key for protecting data on MIFARE cards.

**NOTE:** The Authentication keys can only be changed by a Super administrator.

**WARNING!** After key change, cards that were configured with the old key will not be recognized by system as valid cards!

## 5.3 Special hardware devices

### 5.3.1 GSM Gateway

GSM Gateway is an advanced GSM communication device for remote control of the access control system.

#### How it works:

- User calls gateway phone number or sends SMS to (gate) device
  - The system recognizes the user phone number and grants access, if applicable.

#### **GSM Gateway combined with Scripting module**

Combining the GSM Gateway with the **Scripting module** (see chapter 7) it can be used for remote control of different devices connected to the Alpha central outputs. Connect the GSM gateway to the system like this:

- Install the GSM Gateway to the Alpha central in same way as contactless card (online) readers.
- Use the Nova software to locate the device in central editor by using the **Search readers** option.

For more information about adding new devices to the central, see chapter 5.1.13 Adding new readers.

**NOTE:** The GSM Gateway default **RS485 address** is set to **1**, but can be changed to meet system requirements.

**IMPORTANT!** A GSM gateway requires working **micro SIM** card for normal operation (please be aware to insert the SIM card correctly). If the SIM card is not inserted into the device, the Alpha central will not be able to find it on RS-485 bus.

**IMPORTANT!** The GSM gateway stores its configuration on the SIM card (e.g. RS-485 bus address). When a preconfigured SIM card is inserted into the device, **the configuration is restored from the SIM card**. Please note that changing SIM cards between devices will also change the RS-485 addresses of those devices and the system requires reconfiguration.

The GSM Gateway reports phone caller IDs in the form with the **country entry code** (e.g. 00386yyyyy for Slovenia). When assigning phone numbers to user's profile, leading zeroes can be omitted.

### 5.3.2 Remote control Reader

The remote-control reader is a RF (radio frequency) receiver device used to receive signals from RF remote control key chains. The usual use is for controlling parking ramps or garage doors where usage of traditional contactless cards is not suitable.

The remote-control reader:

- Is installed on the Alpha central in same way as contactless card readers.
- Can use Nova software to locate device in central editor by using **Search readers** option.
- Receives RF signal transmitted by remote control when the access giving RF remote control button is pressed down
  - The RF signal is decoded and shown as an integer in the Nova software
  - The integer can be added as an identification device to selected user

For more information about adding new devices to the central see chapter 5.1.13 Adding new readers.

For more information about adding new cards to user see chapter 4.2.1 Adding unknown card(s) to user.

### 5.3.3 IP Camera

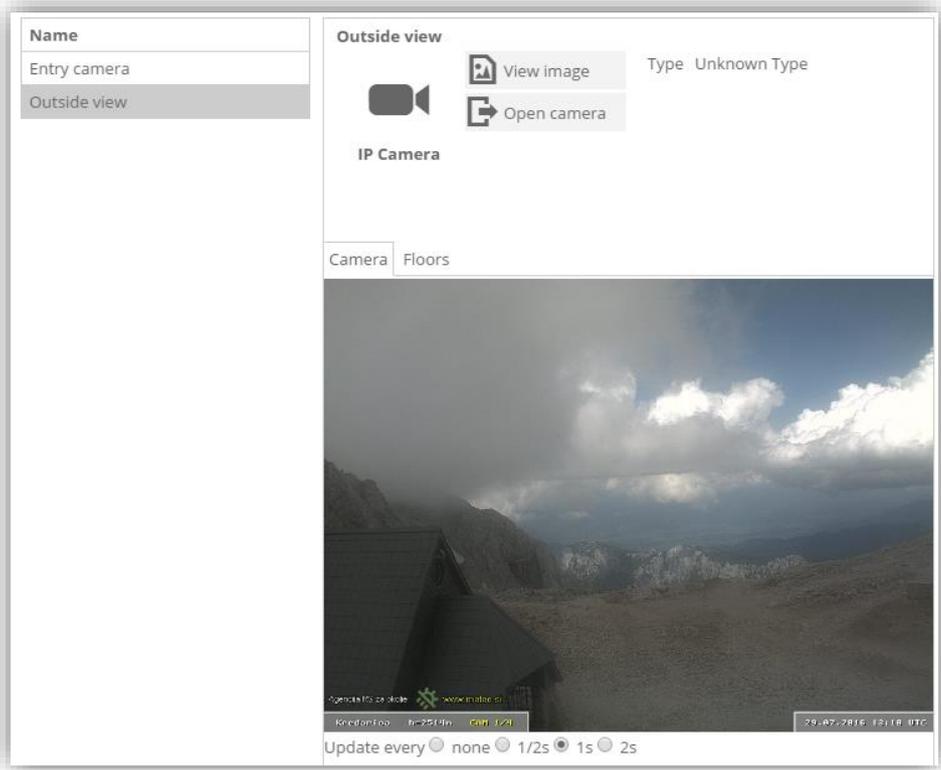
IP cameras can be added by providing direct access to the image.

Most of the cameras are not actually capturing video, but images every few seconds and are serving them to some IP address. In order to get the picture from the camera to the Nova software, we need to provide direct (including login if required) link to the software.

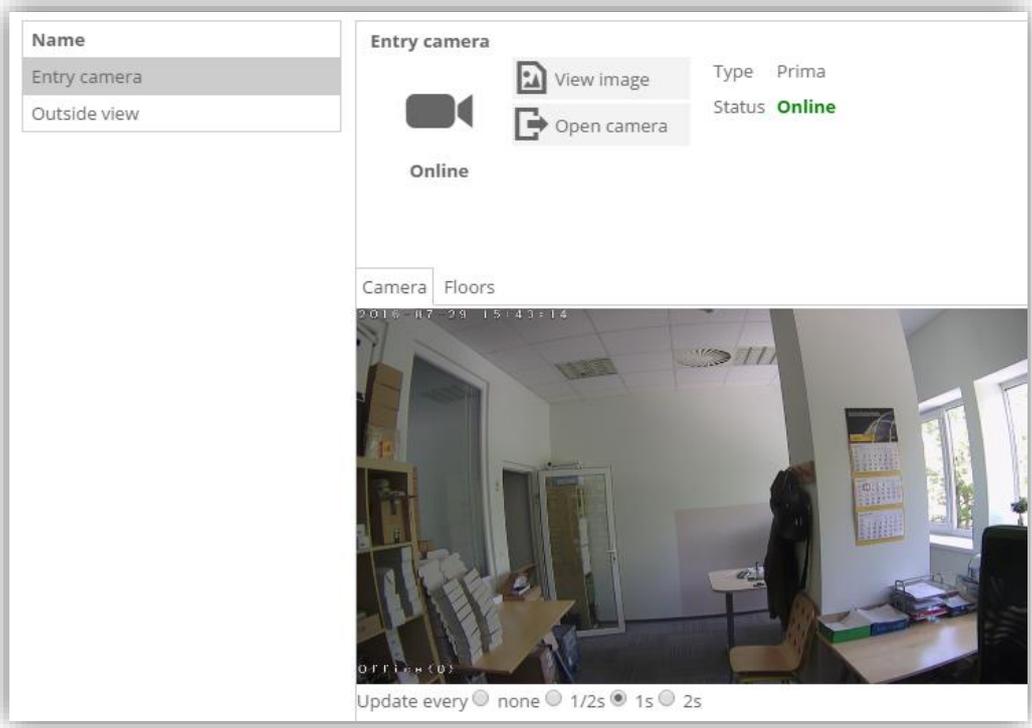
We can add a camera by:

1. Navigating to Home > Hardware > IP Cameras.
2. Press Menu > Add camera.
3. A pop-up menu will require entry of Camera name, its IP Address, type and image address.
  - If the camera type is not located in the dropdown menu, only the entry of the image address is required (Picture 5.21).
  - The supported camera type (Picture 5.22) will have a few additional options like: Detecting if the camera is online, IP change, flipping or rotating the screen, the ability to move the camera (if the camera supports it), the option to display custom text on the image (a preview of the settings is displayed on Picture 5.23) ...  
Supported cameras are also found with the **Central discovery tool** (see chapter 21).
4. Pressing **Add**, adds the camera to the system.

After the camera is added, its settings open. Navigating one step back: **Home > Hardware > IP Cameras**, and selecting the wanted camera, shows the picture if the provided information was correct.



**Picture 5.21: IP camera picture of the unknown type**

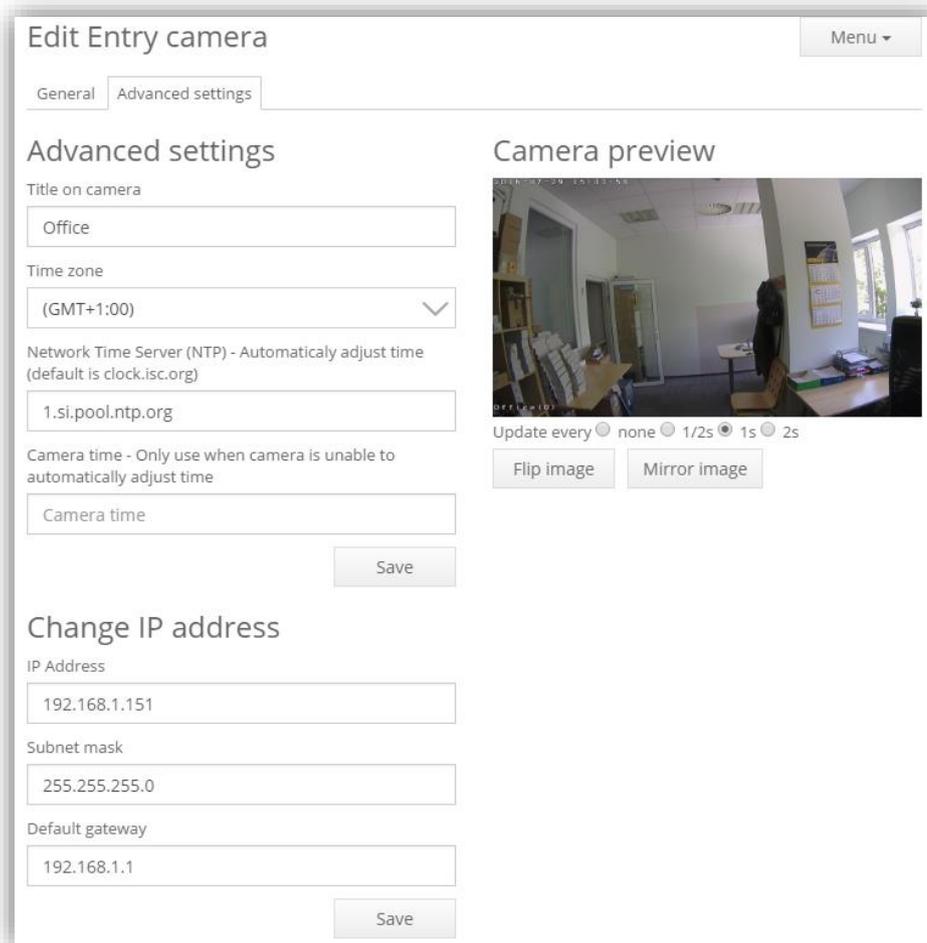


**Picture 5.22: IP camera picture from the Prima type**

To edit camera data, double click on the camera.

To delete the camera from the system:

1. Select the camera from the camera list.
2. Press Menu > Remove [IP camera name].



The screenshot displays the 'Edit Entry camera' web interface. At the top, there is a 'Menu' dropdown. Below it, two tabs are visible: 'General' and 'Advanced settings', with 'Advanced settings' being the active tab. The 'Advanced settings' section includes a 'Title on camera' field with the value 'Office', a 'Time zone' dropdown menu set to '(GMT+1:00)', a 'Network Time Server (NTP) - Automatically adjust time (default is clock.isc.org)' field with the value '1.si.pool.ntp.org', and a 'Camera time - Only use when camera is unable to automatically adjust time' field with the value 'Camera time'. A 'Save' button is located below these fields. Below the 'Advanced settings' section is the 'Change IP address' section, which includes an 'IP Address' field with '192.168.1.151', a 'Subnet mask' field with '255.255.255.0', and a 'Default gateway' field with '192.168.1.1'. A 'Save' button is also present at the bottom of this section. On the right side of the interface, there is a 'Camera preview' section showing a live video feed of an office interior. Below the preview, there is an 'Update every' control with radio buttons for 'none', '1/2s', '1s', and '2s', where '1s' is selected. Two buttons, 'Flip image' and 'Mirror image', are located below the update control.

**Picture 5.23: Known camera type, advanced settings**

## 6 Settings

### 6.1 Add-ons and Modules

Add-ons and Modules contains Nova details and input boxes for entering a new activation key (Picture 6.1).

By purchasing the desired activation key, a system upgrade is made for Nova software from NovaSimpli, to other Nova versions.

**NOTE:** NovaSimpli does not require any activation key.

The screenshot displays the 'Add-ons & Modules' settings page. At the top, an orange banner contains a warning icon and text: 'Your system contains unregistered activation keys. All activation keys have to be registered online before trial time expires (17 days left). Expired trial will cause limited access to user interface. If central has access to the internet, you are able to Register with a single click. Else you need to use Manual Register'. Below the banner are two buttons: 'Register' and 'Manual registration'. The main content area is titled 'Add-ons & Modules' and lists various system parameters:

- Application type: Nova10
- Number of users: 66 / 100 (used / allowed to use)
- Number of readers: 10 / 10 (used / allowed to use)
- Number of administrators: 3 / 3 (used / allowed to use)
- Number of local administrators: 0 / 1 (used / allowed to use)
- Number of BIC apartments: 2 / 50 (used / allowed to use)
- Number of Booking locations: 1 / 7 (used / allowed to use)
- Number of floor plans: **Activation key for floorplans is missing!**
- Use of unprotected cards: No (Number of allowed unprotected cards 0)
- Support for offline readers: Yes
- Offline+ readers: No activation key
- XML integration: No
- New add-ons and modules: Activation key - Activation key is case sensitive. Includes a form with a date field and an 'Add' button.
- Activated add-ons and modules: A table listing registered keys with their dates and types.

Date	Type	Status	Action
2016-07-12 14:33:28	Scripting module		
2016-07-14 10:12:43	Nova10	Not registered - (17 days left)	<a href="#">Remove</a>
2016-07-25 11:28:02	Booking (1 location)	Not registered - (28 days left)	<a href="#">Remove</a>
2016-07-25 11:28:32	Booking (5 locations)	Not registered - (28 days left)	<a href="#">Remove</a>
2016-07-25 11:29:52	Booking	Not registered - (28 days left)	<a href="#">Remove</a>

Picture 6.1: Add-ons & Modules tab

Upgrading to the NovaSimpli350 software version is free and can be done with the use of free activation key: **ZWJh-ZjQ1-NTUw-ZTY5**).

- Please remember that with the NovaSimpli350 software, the maximum number of users in the system is limited to 350 and the tracking of the events is disabled
- The only way to see the events flow is through the live events displayed on the home page.

**IMPORTANT!** After the activation keys are entered, you have 30 days to register your system. During this period, you are free to use your system as you wish. The activation keys can also be deleted from the system if they are not needed (by pressing the **Remove** button next to the key). Once the lowest timer runs out (if you have 3 and 5 days left on 2 activation keys, 3 days will be taken into count), the system will keep working with the set settings, but the access to the GUI will be locked to the **Add-ons and Modules** page until the system is registered. The option to remove activation keys will be disabled as well.

**Suggestion:** Adding a new activation key after the system was already registered, will require a new registration, so it is advisable to register the system once all activation keys are entered.

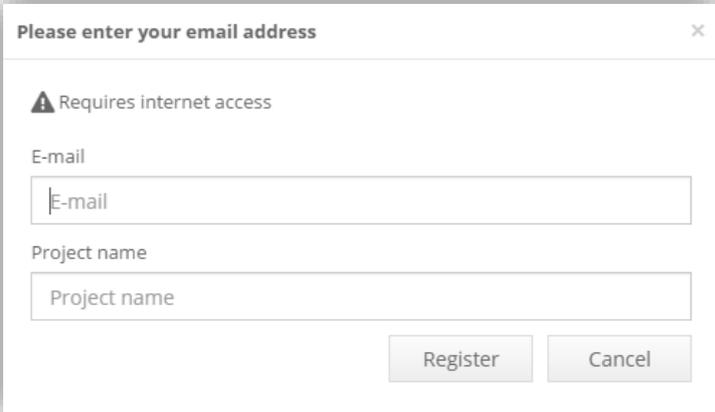
**Note:** Deleting and re-entering the same keys will not reset the Registration days left counter.

The next sub-chapters describe an online/offline activation based on your computer connectivity. If the computer from which the system is managed is connected to the internet, use the online registration (much faster); otherwise if the connection to the internet fails, the administrator will be redirected to offline registration procedure.

### 6.1.1 Online system registration

To register system online:

1. Press the **Online Registration** button (located at the top of the Picture 6.1). A pop-up window will appear (shown on Picture 6.2).
2. Enter e-mail and a project name. Provided data will be used for easier assistance and software update/upgrade notifications.
3. Press **Register** button. If the registration was successful, the green box will appear with the OK message (Picture 6.4); if there are any issues with the internet connection and the registration fails, it is advised to proceed with manual registration.



The image shows a dialog box with the title "Please enter your email address" and a close button (X) in the top right corner. Below the title is a warning icon and the text "Requires internet access". There are two input fields: "E-mail" and "Project name". At the bottom of the dialog are two buttons: "Register" and "Cancel".

**Picture 6.2: Online system registration form**

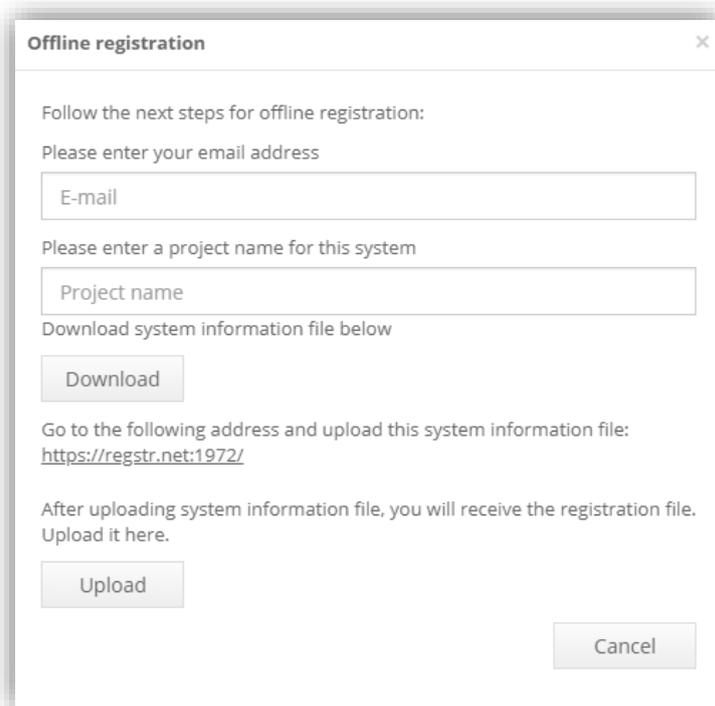
## 6.1.2 Offline system registration

Offline registration steps:

1. Press the **Offline Registration** button (located at the top of the Picture 6.1). A pop-up window will appear (shown on Picture 6.2).
2. Enter e-mail and a project name. Provided data will be used for easier assistance and software update/upgrade notifications.
3. Press the **Download** button – a window will open to save system information file to your computer. Select a folder with easy access.
4. Transfer the file to USB stick and plug it into computer with internet access. If the procedure is done on a mobile device (i.e. laptop/tablet/phone ...), it is enough to move to a location with internet access.

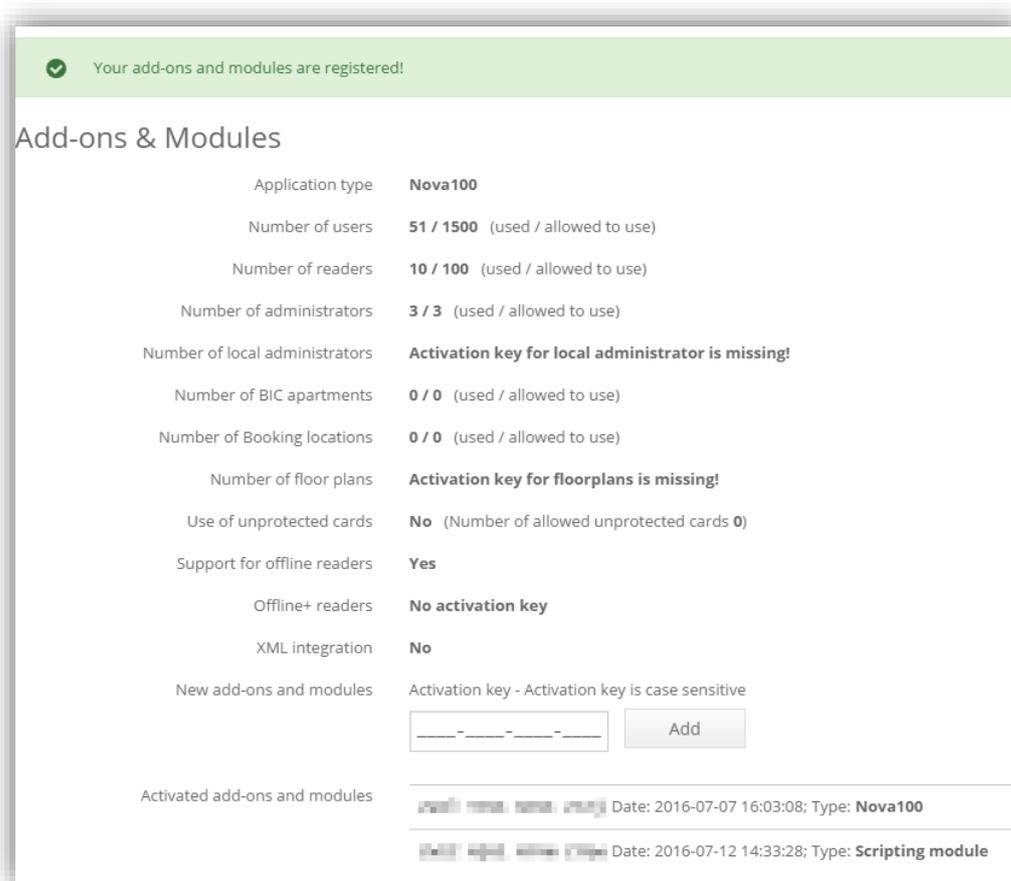
Navigate to <https://regstr.net:1972> and follow the steps:

- Click on the button to **upload the system information** file that was previously downloaded.
  - If the upload was a success, continue to download the **Registration file**. Download it to a folder with easy access.
5. Transfer the file **Registration file** to USB stick and carry it back to the computer that is connected to the central OR if using a mobile device, go back to the network with central access.
  6. Open the Nova 2.0 window and press the **Upload** button. Select the **Registration file**. The system is now registered (Picture 6.4).



The screenshot shows a dialog box titled "Offline registration" with a close button (X) in the top right corner. The text inside the dialog reads: "Follow the next steps for offline registration: Please enter your email address" followed by an input field containing "E-mail". Below that, it says "Please enter a project name for this system" followed by an input field containing "Project name". Then, "Download system information file below" is followed by a "Download" button. The next line says "Go to the following address and upload this system information file:" followed by the URL "https://regstr.net:1972/". The final instruction is "After uploading system information file, you will receive the registration file. Upload it here." followed by an "Upload" button. A "Cancel" button is located at the bottom right of the dialog.

**Picture 6.3: Offline system registration pop-up**



Picture 6.4: Completed registration

## 6.2 Login Settings

- **Default language:** Is the global settings of the GUI. Users can still set their own display language in the personal settings. Read about personal settings in chapter 2.1 Account settings.
- The **Maintenance contact** field is used for contact information of the person maintaining the system. The field is visible on the login screen for quick access in case of problems. The recommended information here is the phone number of the person maintaining the system.
- **Super administrator account suspension:** The option to Enable/Disable Super administrator account. This account is only used by the installers and should be disabled once the system is set up. This way we increase security and prevent unwanted access. Resetting the central to its default IP will enable Super administrator.
- Password recovery and user registration settings:
  - **Allow forgotten password:** If the option is enabled, a new link shows up that allows password reset. This only works if the user email set in the GUI matches the one in password reset request. The system provides an example of an email that is sent, but the content can be changed to custom text.

- **Allow registration of new users:** The installer can allow users to create their own account by using this option. Similar to forgotten password option, an email is sent and its content can be changed accordingly.

## 6.3 Database Settings

The **Database Settings** widget is used for advanced settings and is only enabled for system administrators.

This widget offers these options:

- Download a backup copy of a configuration database.
- Upload a backup copy of a configuration database to restore it to the previous state.
- Download Event database backup.
- Enable/Disable automatic database backup.
- Turn on/off Event archive.

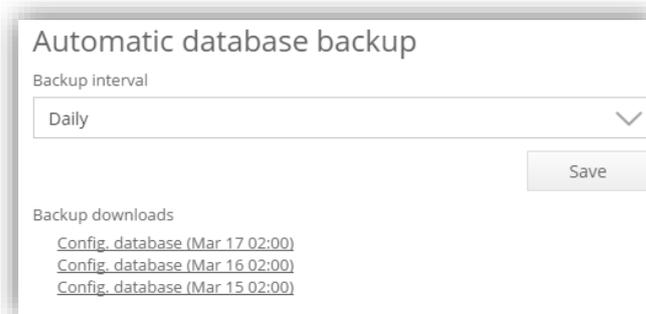
**CAUTION:** When uploading a configuration database with new settings, be aware that a damaged database file can cause the system to stop working.

**RECOMMENDATION:** It is recommended to create a backup of the old configuration database prior to uploading the new file, in order to avoid system breakdown, just like it is recommended to make a backup of the system after first complete configuration. This is done by:

- Clicking the **Create backup file** for the configuration and event database.
  - The database files can now be stored on the local computer

### 6.3.1 Automatic database backup

Nova version 1.5 and higher support automatic backup of the configuration database as shown on Picture 6.5.



**Picture 6.5: Different copies of backups from central without USB storage**

Automatic database backup can be set to:

- Turned off
- Daily
- Weekly
  
- Monthly

**NOTE:** Each option represents a period of backup creation. A new copy of configuration database is created every set period at 2:00 AM.

- *Daily* backup will create backup every day at 2:00 AM.
- *Weekly* backup will create backup every Monday at 2:00 AM.
- *Monthly* backup will create backup every 1<sup>st</sup> day of the month at 2:00 AM.
- *Turned off* will stop backup creation.

Backup configuration can be set on master central and the rule applies to all centrals in the system.

Backup and local memory

- Centrals with proper **backup USB storage:**
  - Create a copy on them and **save local memory.**
  - Additionally, they will also create a copy of an **events database.**
    - Also, **all of the user pictures** will be saved on it.
    - Centrals with **USB storage** connected will keep up to **seven copies** of **configuration and event databases** (without USB, only three copies of configuration database are made).
- Centrals without USB storage will also store copies of previous backups for a period.

If backups are set and stored on local memory, it will keep three copies of the last periods (e.g. if the automatic database backup is set to daily, it will keep backups for the last three days; for weekly - last three weeks and for monthly - last three months).

**NOTE:** At any time, the backup is switched from off to on, it will create a new backup after a few minutes. Backup copies are downloaded by clicking on the corresponding text.

### 6.3.2 Event archive

Nova Drive has the option to remove events older than N days. This can be enabled by selecting the number of days you wish to keep as an archive.

**NOTE:** Some countries are required to delete events older than N days. Please check the regulations of the Country where the central is located.

## 6.4 Other Settings

### 6.4.1 Time zone

Setting the time zone is not mandatory but recommended. Having track of the local time is important for displaying all events time with the correct time stamp. The setting is global which means that once you set it, the same time zone will be set on all centrals in the system.

#### **NTP server**

If case of NovaServer or central type (you can check version of the central in **Hardware > Centrals**, next to its type, the hardware version should be at least (3.0)) and has internet access, providing a NTP address will sync the system time with the provided time server daily. It is enough to set this option on master only (the other slave centrals are automatically updated with the master's time – their hardware version does not matter). There are many servers that provide this service for free, so pick the one that is close to you (less delay).

### 6.4.2 Web server port

Sometimes the software needs to be accessed from the internet, but in cases where something is already occupying the default http port (80), internal ports can be changed and forwarded to meet the needs.

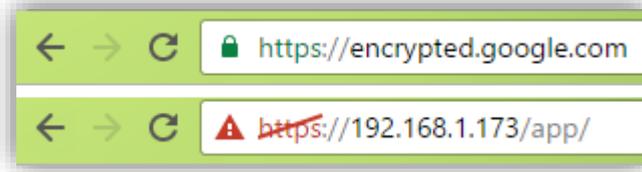
- The Nova software currently supports five (5) different ports: 80, 81, 8000, 8080 and 8181.
- The GUI will automatically restart, once the port is changed. In a couple of seconds, the new page can be accessed locally on <http://<CentralIP>:<port>>.
- Ports are now ready and **MUST** be forwarded on the **router** from newly changed port on central to external ports.

**IMPORTANT!** If you are making any changes to web server port, please write it down somewhere, because it is easy to forget that the option was changed and the central is not accessed normally, which could cause confusion and thereby waste a lot of time when support is required.

### 6.4.3 Security settings

**IMPORTANT!** Accessing any https page with incorrect (self-signed) certificates will display an unsecure connection because the certificates are not signed for the correct web address (usually local IP if the access is from the local network). The connection is encrypted but the target self-signed certificate was not confirmed by a third party. Adding an exception will allow you to visit the site, however, if we want the connection to be secure, the certificates for the web address must be bought and uploaded to the

central (example: Certificates bought for x-company will allow secure connection for <https://x-company.com> and the identification is confirmed by the company who issued the certificates).



**Picture 6.6: Difference between HTTPS access with a certificate / site with self-signed certificate**

More on custom certificates and secure connections can be read in 17 Module: High security module.

### HTTPS redirect

The new central types (you can check version of the central in **Hardware > Centrals**, next to its type, the hardware version should be at least (3.0)) support HTTPS access, which is always turned on (it just depends if you write http or https in front). This option, if enabled, redirects anyone who wishes to access the site from http to https.

### Secure connection between centrals

There are three options that can be set:

- **None** – the communication between centrals will not be encrypted. **NOTE:** The connections between the centrals are unsafe. Using this method is **NOT RECOMMENDED**.
- **Optional** – the communication between centrals will try to be encrypted, but if it can't, it won't be. Since the old type (Hardware < 3.0) of centrals do not support encrypted communication, **any communication with the old central will not be safe**. The communication between the new centrals will remain encrypted.
- **Required** – ignores the centrals that are not able to communicate securely.

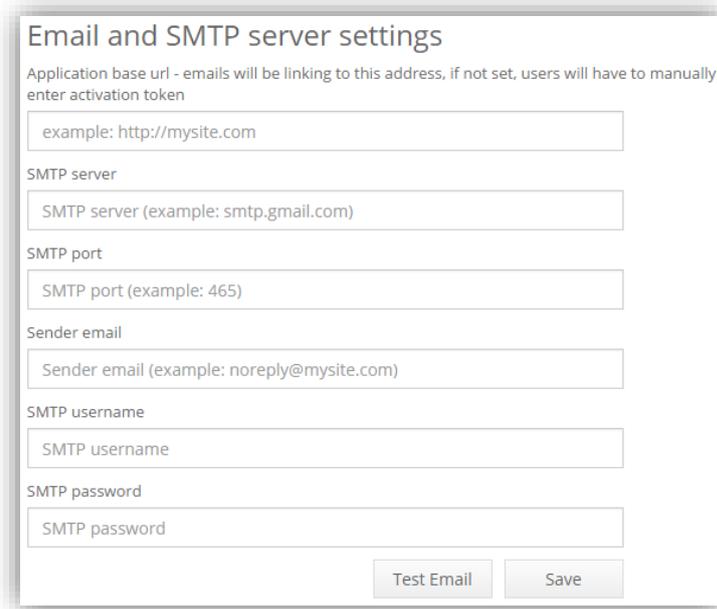
To read more about the additional security module, please read chapter **17 Module: High security module**.

## 6.4.4 Email and SMTP server settings

With the new Nova 2.0 software, we are able to send emails to users in the system. This is used in the **Module: Presence, Module: Messaging, New user creation, Password recovery...**

The grey text in the text box is an example for Gmail settings.

**IMPORTANT!** The google account must **allow less secure apps** to be able to connect to the Gmail account. Please make sure that this is **turned ON**, on your Gmail account that you wish to use in Nova 2.0 for email sending.



The screenshot shows a web form titled "Email and SMTP server settings". Below the title is a note: "Application base url - emails will be linking to this address, if not set, users will have to manually enter activation token". The form contains several input fields: "example: http://mysite.com", "SMTP server (example: smtp.gmail.com)", "SMTP port (example: 465)", "Sender email (example: noreply@mysite.com)", "SMTP username", and "SMTP password". At the bottom right, there are two buttons: "Test Email" and "Save".

**Picture 6.7: Email and SMTP server settings**

### 6.4.5 System PIN settings

Selecting the option to enable **Unique PIN** will prevent users from having the same PIN in the system (more secure).

The alternative option is to disable Unique PIN, which will let users use the same PIN. Users with the same PIN will be able to access areas that they have rights to, but if they enter the doors that multiple users have access with the same pin, an event **Access with common PIN** will be displayed in the event list (the system cannot keep track who entered – this is a less secure option).

**Global PIN length** – by providing the global PIN length, the software will apply a PIN length to all readers in the system. Whenever adding new PIN to user, it's length will be checked. If any of the readers is set to custom PIN length, the user PIN length check will be disabled; this setting will still apply to other readers. This option can't be turned on until users who have longer PIN shorten it to same length as wanted option. By default, the PIN length is 5.

### 6.4.6 Show IP camera picture

This option is tied to a script that manages a camera (read more on scripting in chapter 7 Module: Scripting). The script triggers to different events like entry or unknown cards and takes a picture of a person at monitored door. Pictures are then saved to that central and displayed next to the events. For someone that is running such script can

enable/disable displaying of the pictures displayed in the events and event history (also displayed/hidden in the report).

## 7 Module: Scripting

The basic functionality of a central can be extended with **EX|FU module**. These modules are scripts that can define custom rules and actions to take place when a normal system event or a user-defined custom event occurs. To enable the script module:

- A valid EX|FU module activation key is needed
- Enter the key under the Home > Settings > Add-ons and Modules widget (chapter 6.1).

### 7.1 Writing EX|FU modules

EX|FU modules are written in Python programming language and are run on the central:

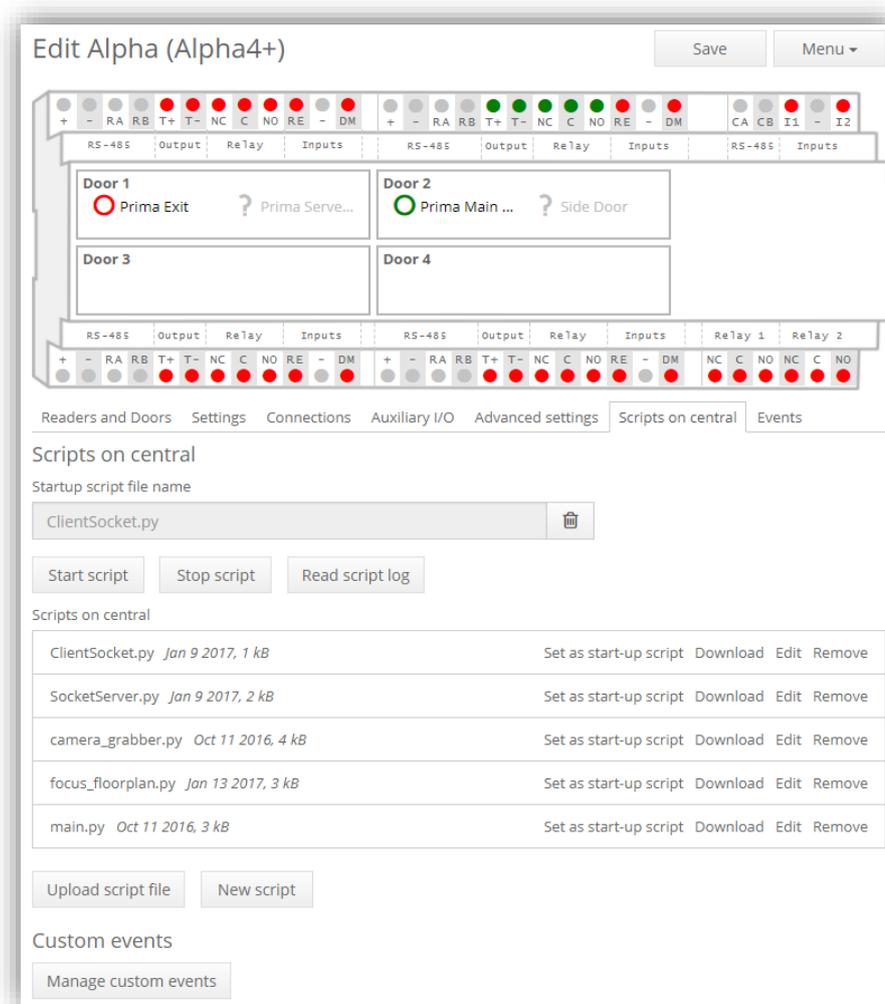
- Which receives events from the system
- Which acts upon events by triggering new events such as:
  - opening multiple doors
  - activating alarm
  - performing other predefined actions

**NOTE:** It is possible to define custom events that are triggered when a specific event happens. For information about how to write scripts please see the **Scripting manual**, which consists of available **API methods** and practical **examples**.

#### 7.1.1 EX|FU module installation

EX|FU modules are uploaded to the central in the **Central settings** (Picture 5.9) of the central under the **Scripts on central** section shown on the picture below. This is found by:

1. Navigating to Home > Hardware > Centrals
2. Double click OR select and **Menu > Edit [central name]** the central that you wish to upload the script to.
3. Navigate to Scripts on central tab



**Picture 7.1: Scripts on a central**

Upload a script:

1. Select the button Upload script file.
2. Search for script on list presented in browser window.
3. Select script from local hard drive.
  - The script is uploaded to the central.
  - Uploaded script is visible in list above the button **Upload script file**.
  - When the script it uploaded, its additional information and options are shown.

Different options are:

- **Download** - script from central to local hard drive.
- **Edit** – allows users to edit the script directly on the central.
- **Remove** script from central.
- Set script as a start-up script:
  - A startup script starts together with the central.

- A startup script file name is listed under **Startup script file name** field above the list of scripts.
  - This field can only be set through the listed scripts options.
  - To remove the script from this field, click on the trash button next to the file name.

**IMPORTANT!** The scripting engine of the central re-starts if there is a new start-up script set and it will stop if the script is removed from the start-up script field. The engine also restarts after uploading new script files to the central or after removing scripts from the central.

To manage a start-up script:

1. Click **Start script** button to start script manually.
2. Click **Stop script** button to stop script manually.
  - Above is useful for testing purposes such as new functionalities and behavior.
3. Click on the button **Read script log** to check a file containing the script log.
  - The log includes the standard output of any running script.

**IMPORTANT!** If a script crashes, the compilation errors are not present in the script execution log file! One solution to avoid this is to trace script progress to a standard output and discover errors based on this.

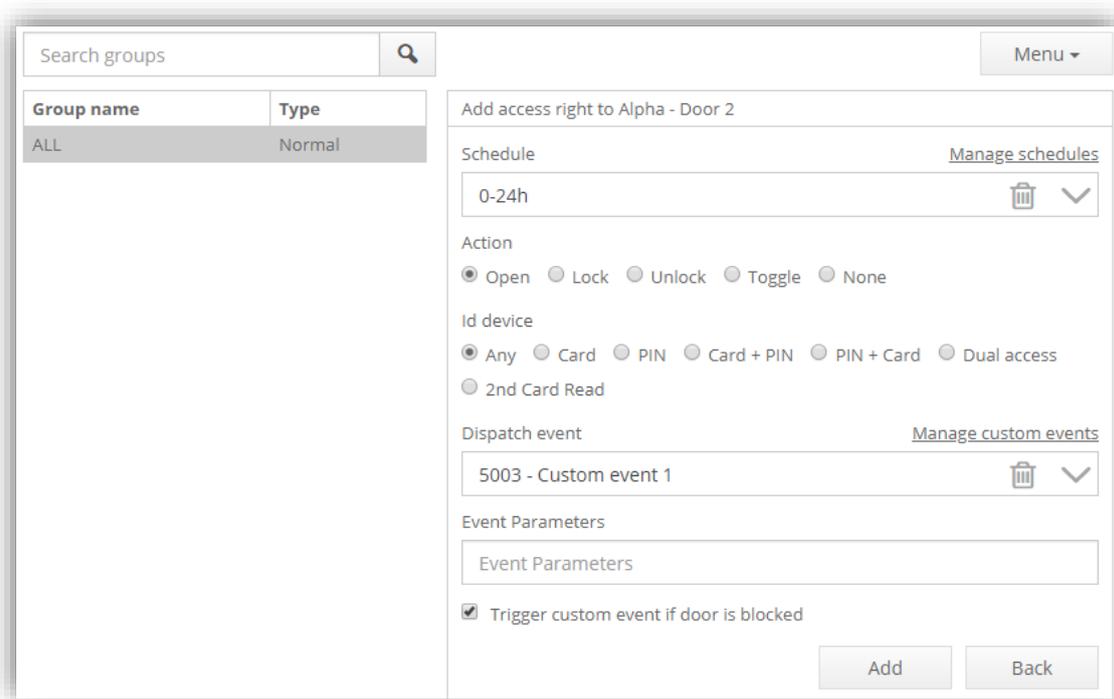
## 7.2 Custom EX | FU events

It is possible to add custom events to the Nova system and later dispatch them in the context of user created events.

### 7.2.1 Custom events editor

Two ways to access the **Custom events editor** :

1. Go to Home > Users & Access Rights > Access Groups.
  - Click on the (+) button next to the reader you want to assign a custom event, OR click on the pen button for existing rights.
  - Click Manage custom events
2. On master central go to Home > Hardware > Centrals > [master central]> Edit
  - Click tab Scripts on central.
  - Click the button Manage custom events



**Picture 7.2: Select time schedule, action, identification device and dispatch event**

## Manage custom events

To open the **Custom events editor**:

- Click the **Manage custom events** text displayed on Picture 7.2.

Menu contains options to:

- **Add** user assigned event
- **Edit** an existing event entry (must be selected)
- **Delete** unwanted events (must be selected)

Left panel contains:

- List of all custom event codes in the Nova system

Right panel contains:

- Description of the event codes.

Event code	Event description
5003	Custom event 1
8011	Elevator
8012	Outputs control
8013	Outputs control to all
8020	Alarm deactivated
8021	Alarm activated
8022	Alarm activation failed
8023	Alarm deactivation failed
8024	Alarm maintenance entry
8025	Alarm user
8026	Alarm activate
8027	Alarm deactivate
8100	Script stopped
8101	Script started
8201	Open output 1
8202	Open output 2
8203	Open output 3
8204	Open output 4
8205	Open output 5
8206	Open output 6
8207	Open transistor 1
8208	Open transistor 2
8209	Open transistor 3
8210	Open transistor 4
8211	Lock output 1
8212	Lock output 2

**Picture 7.3: Manage custom events**

## 7.2.2 Adding new custom event

To add a new custom event:

1. Click on Menu > Add
  - A new form will open (Picture 7.4)
2. Enter the required **Event code** number (range: 5000-8000)
  - Event code number must be unique
  - Event description must be unique
3. Pressing the **Add** button will add it to custom events lists in custom events editor

**Picture 7.4: Add new event**

### 7.2.3 Editing and deleting custom events

To **edit** custom events:

- Double click on event in the events list

OR

- Select event and click on **Menu > Edit** button

**NOTE:** The description of the event is only changeable after adding it to the system.

To delete custom events:

- Select unwanted event in events list
- Click **Menu > Remove** button

**NOTE:** It is not possible to delete events assigned to the access definition(s).

### 7.2.4 Dispatching/assigning custom events

A custom event can be assigned to **any access definition** and it will be dispatched when the access definition is matched with an incoming event (e.g. when a user registers the card on the reader, to which the user has access rights). We also can decide with a checkmark, if we want to trigger the custom event if the door is blocked or no.

To assign a custom event to an access definition:

- **Select custom event** from the dropdown list
- **Save** changes
  - Optionally, by providing additional parameters (arbitrary string values) it is possible to add values to the script when event is dispatched (see

Picture 7.2 for dropdown list with selected event **Alarm ON**).

## 7.2.5 Built-in events

Some events are built into Nova and can be used in the same way as manually added events. See below table for a presentation of these.

**IMPORTANT!** Note that some events are part of python scripts on the central, e.g. alarm events. Inappropriate use of those events can cause scripts to fail. Please read event description for more information on how to use them.

**IMPORTANT!** Using Outputs control or Outputs control for all, the parameters from 1 to 6 represent relays, 7 – 10 are transistors.

Event name	Parameters	Description
<b>Output control</b>	comma separated list of outputs (1-10): [time in ms] : [Open (default)   Lock   Unlock  Toggle]	Advanced output control, e.g.: 1,2,3,4,5,6,7,8,9,10:Toggle toggles all outputs and transistors; 1,2,3:1000 opens output 1,2 and 3 for 1 second, ...
<b>Open output X</b>	[time in milliseconds]	Opens output X for defined time
<b>Open transistor X</b>	[time in milliseconds]	Opens transistor X for defined time
<b>Lock output X</b>		Sets output X to locked state
<b>Lock transistor X</b>		Sets transistor X to locked state
<b>Unlock output X</b>		Sets output X to unlocked state
<b>Unlock transistor X</b>		Sets transistor X to unlocked state
<b>Toggle output X</b>		Toggles state of output X
<b>Toggle Transistor X</b>		Toggles current state of transistor X
<b>Alarm activate, Alarm user, Alarm ...</b>		Events are used with simple alarm integration script and SHOULD NOT BE USED DIRECTLY, exceptions are only Alarm activate event and Alarm user event. See chapter 8.3 Simple alarm integration for more information.

**Table 7.1: List of built-in events**

**IMPORTANT!** The built-in events are only useable if there is a Scripting activation key entered in the system.

## 7.3 Simple alarm integration

Alarm integration allows users to:

- Control alarm zones with their cards and online readers
- Get a detailed log of alarm state changes in the form of system events
  - The system events can be printed out

**NOTE:** A central in the access control system can control one alarm zone. If there is a need to control multiple alarm zones, there have to be other centrals in the system for each alarm zone. Also, note that each alarm zone is controlled independently of other alarm zones.

### 7.3.1 System prerequisites and alarm script installation

To enable alarm functionality:

- Scripting activation key is required
  - Please see chapter 6.1 Add-ons and Modules for more information on activation key installation
- Scripts **Alarm.py** and **main\_simple\_alarm.py** are required on central to control selected alarm zone.
- User with system administrator rights must have **same authentication credentials** as the ones defined in *main\_simple\_alarm.py* script
- Default user to log-in is defined in script as **Scripting module**.
  - ⇒ Install above mentioned scripts on central and select **main\_simple\_alarm.py** as **startup script**. For more information on how to install scripts on the central, please refer to chapter 7.1.1 EX|FU module installation.

**IMPORTANT!** Nova software automatically adds a scripting user to the system when the scripting key is entered. When writing credentials to the script, username can be set to "**scripting**" and the password can be left empty (""). This prevents abuse of a scripting account, because the password cannot be gathered from a python script.

**IMPORTANT!** The added scripting account needs to be set as **system administrator** to be able to log-in to the system and **its credentials need to stay intact**.

### 7.3.2 Access group configuration

Create special access groups to give users rights to activate or deactivate alarm zones. Some users may only activate alarm while others are also allowed to deactivate it. There is a need for two access groups to achieve described user cases, one for alarm activation and one for alarm deactivation.

To create **alarm activation access group**, please follow these steps:

1. Create a **new access group** and give it a descriptive name, e.g. Main Door Alarm Activation.
2. **Add a new access definition to the reader** picked to control an alarm zone in the context of the newly created access group.
3. **Select time schedule**, which will define period for activating alarm.
4. Set Action to None.
5. Set ID device to 2nd card read.
6. Set Dispatch event to Alarm activate.
7. **Save** changes.

To create **alarm deactivation access group**, please follow these steps:

1. Create a **new access group** and give it a descriptive name, e.g. Main Door Alarm Deactivation.
2. **Add new access definition to the reader** picked to control an alarm zone in the context of the newly created access group.
3. Select **time schedule**, which will define period for activating alarm.
4. Set Action to None.
5. Set ID device to Any.
6. Set Dispatch event to Alarm user.
7. **Save** changes.

After creating access groups, **assign to users responsible for alarm zone management**. Both of the access groups need to be assigned the users with rights to activate and deactivate alarm. Some groups can be assigned only to the users who can activate alarm (**alarm activation access group**).

### 7.3.3 Activation of alarm

When the alarm is disabled and a user assigned with "**alarm activation access group**" presents the card on a reader included in the access group, the door will be opened (regardless of **Action** setting of **None**, set under step 4).

At this point the user can:

- Remove his card from the reader and **pass the door**.
- Activate the alarm by holding card on reader for two reads (app. 5 sec).
  - The central will send a request signal for alarm activation and wait for confirmation signal.
  - Positive confirmation signal: reader will **beep five times** with **short OK tone**.
    - Event 8021 – Alarm on is triggered.
  - Negative confirmation signal: **reader will beep** with **long ERROR tone**.
    - Event 8022 – Alarm activation failed is triggered.
  - When **alarm is set**, **all readers** on the central are **blocked**.

### 7.3.4 Deactivation of alarm

All readers in an alarm zone are blocked when alarm is activated and users are not able to access any doors:

- Result: **Error sound** will inform that alarm is activated.
- **Users cannot enter** the doors until alarm is deactivated.

Users assigned with alarm deactivation access group can **deactivate alarm by presenting the card on the reader**:

- Alarm deactivation request is sent to the alarm central when card is read for the second time.
- Positive confirmation signal: doors will open and reader will beep three times with short OK signal.
  - Event 8020 – Alarm off will be triggered.
- Negative confirmation signal: reader will beep with long ERROR signal.
  - Event 8023 – Alarm deactivation failed will be triggered.

**NOTE:** If alarm deactivation fails three times in one minute:

- Doors will be opened.
- Reader will beep the same way as when alarm is activated (five short OK beeps) and event 8024 – Alarm maintenance entry will be triggered.

**IMPORTANT!** Readers do not signalize whether alarm is ON or OFF due to security reasons.

## 8 Module: Door stations

- The Door station module in Nova is a part of the door and building information communication system
- The Door station module is installed with the Nova access control system
- The Door station module allows the control of text on various displays e.g. door stations, call buttons and video indoor stations

To use the Door station module in Nova, enabled it by:

1. Enter a valid Door station module activation key (See **Add-ons and Modules** section for help on adding new activation keys)
2. Navigate to **Home > Hardware > Door stations** in the widget menu

### 8.1 Door station module setup

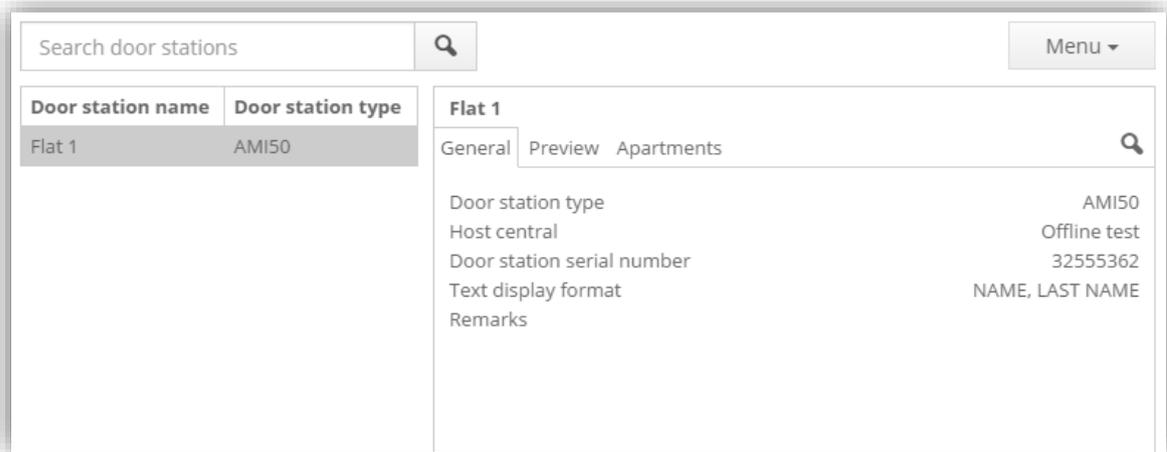
To set-up the Door station module:

1. Import apartments into the Door station module with **Apartments manager**
2. Access **Apartments manager** via widgets **Home > Hardware > Apartments** or directly from the Door-station widget: **Menu > Manage apartments** (Picture 8.1)
3. Insert serial numbers of installed hardware (call button and indoor video station)
  - Serial numbers are required to communicate with apartment hardware
  - For more information, read the **Manage apartments** section
4. Insert serial numbers of door stations
5. Insert names of central connected to door stations
  - See **Adding door stations** section for more information
6. Link apartments and door stations
  - Each door stations must have apartments assigned to show text on the different displays
  - See the **Assigning apartments to door station** section for more information
7. Assign apartments to users
  - This can be accessed through **Users & Access rights** in the Nova main menu
  - Here a user is selected from the list by clicking on **Menu > Edit User [name]**
  - User profile will show up
  - Select the button **apartment settings**
  - See the section 8.5 Assigning apartments to the users for more information

## 8.2 Door station manager popup window

Picture 8.1 shows the Door station manager:

- Left panel: All door stations created are listed here with their type.
- Right panel: Details of the selected door station.



**Picture 8.1: Door station manager popup window**

## 8.3 Managing apartments

Apartments need to be added to the software before they can be assigned to door stations or users.

It is possible to manage the apartments by clicking on the widgets **Home > Hardware > Apartments** or directly from the Door-station widget: **Menu > Manage apartments**. This presents the apartment manager (Picture 8.2).

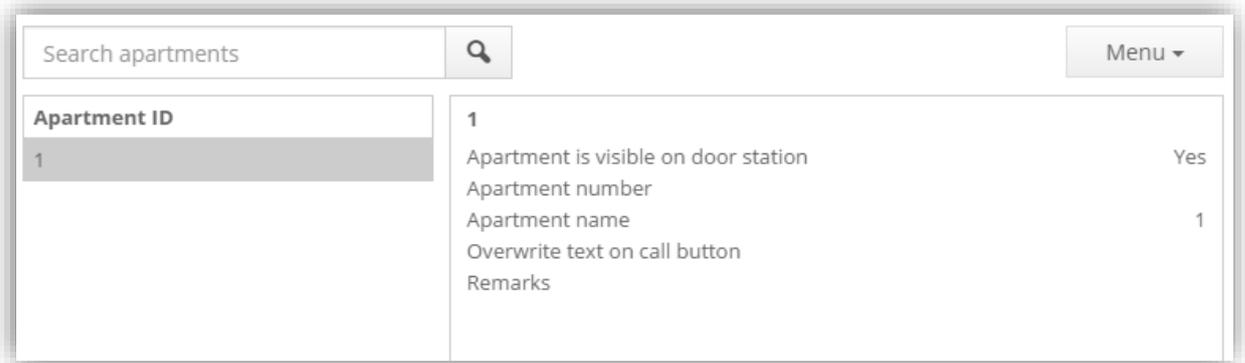
### 8.3.1 Adding apartments

To add new apartments to the system:

- Click the button Menu > Add apartment
- Enter unique apartment ID
  - Apartment will be added to apartment list in apartment manager
  - The apartment list allows to edit or delete apartments

Search function:

- Search in apartment list in upper corner of the apartment manager
  - Preview of selected apartment is shown on the right side of the manager window
  - Here important information about an apartment is shown and it is possible to edit it if necessary



**Picture 8.2: Apartment manager**

### 8.3.2 Editing apartment

To edit an apartment:

- Double-click on the apartment ID in apartment list
- OR select the apartment and click **Menu > Edit [apartment ID]** button
  - The apartment editor (Picture 8.3) will open

How it works:

- The hardware components of an apartment (call button and video indoor station) and the Nova software are linked by entering serial numbers of installed hardware into the corresponding input fields in the **Apartment editor**.
- Nova uses serial numbers when relaying information and communicating with door station components.

Important to remember:

- Each apartment needs a unique ID
- The apartment ID is used throughout the software as a reference
- All apartments are listed on the door station by default
  - To change this: un-check the option **Apartment is visible on door station**
    - The apartment will not be listed on the door station
    - This is relevant in cases where the door station is showing the apartment number (not the resident name)
- Additional information about an apartment can be saved in the **Remarks** field

- Changes made to the apartment must be saved by clicking on the button **Save**.

Door station text and call button:

- Defined by field **Apartment name**
  - The same name will appear on the call button
  - UNLESS it is overwritten: Entering a custom name in **Overwrite text on call button** field.

**Picture 8.3: Apartment editor**

### 8.3.3 Removing apartments

Apartments can be removed when they are no longer needed, e.g. they are not assigned to any door stations and not assigned to any of the users.

To remove apartment from the Door station module:

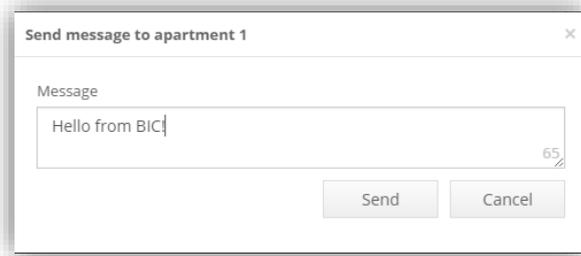
- Click the **Menu > Remove [apartment ID]** button in the **Apartment editor** (Picture 8.2)
  - After removal confirmation, the apartment is removed from the list

### 8.3.4 Sending messages to apartments

- Short messages can be sent to each apartments' video indoor station where users can read them
- Each message can contain up to 80 characters

To send messages:

1. Select apartment(s) from the apartment list
  - Use the **shift** button (on your keyboard) to select multiple apartments
2. Click on **Send message to apartment** button (see Picture 8.2; same button is also present in the apartment editor)
3. Type message into popup window (Picture 8.4)
4. Click on **Send** message to apartment button



**Picture 8.4: Message input popup window**

## 8.4 Door station management

Enter settings for door stations in the door station manager.

### 8.4.1 Adding door stations

To add door stations:

1. Click the **Menu > New door station** button in the Door station editor
  - Opens up popup window (Picture 8.5)
2. Enter the name, serial number and type for the new door station
3. Select host central and door of selected central that is wired to door station
4. Save door station by clicking on **Add** button
  - The newly created door station will be added to the door stations list where it can be selected and managed

**Picture 8.5: New door station popup window**

## 8.4.2 Editing door station

To edit door station (Picture 8.6):

- Select the door station and **Menu > Edit [door station name]** button
- OR double-click on the door station name on the list

In the Door station editor, the central panel allows user to modify:

- Name
- Type
- Host central
- Host door, that the central is connected to
- Serial number or RS-485 address
- Text display format

Remember to save any changes!

**Picture 8.6: Door station editor**

### 8.4.3 Removing door stations

Door stations can only be removed from the system if there are no apartments associated with them. For details on assigning and un-assigning apartments to the door station, please see the section **Assigning apartments to the door station**. To remove a door station:

- Select the Door station and press **Menu > Remove [door station name]** button from the drop-down menu
  - The door station will be removed from the list and from the system

### 8.4.4 Preview of door station information

Preview of display text on the edited door station is visible in the **Door station preview** tab in the **door station editor**.

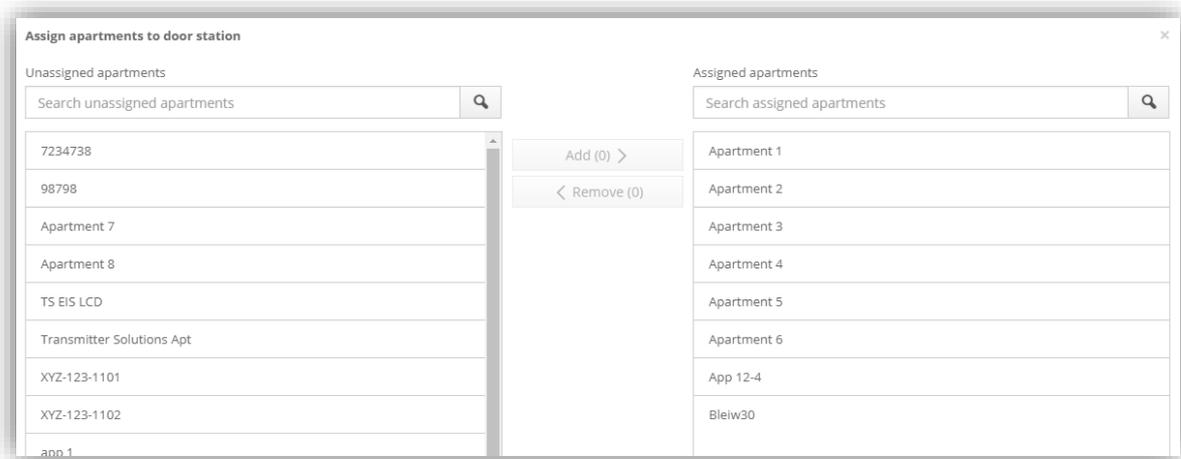
It contains the apartments associated with the edited door station, the users that are associated with the apartments and on the option selected in the **Text display format** drop down menu.

For more information on apartment assignment, see the section **8.5 Assigning apartments to the users**.

## 8.4.5 Assigning apartments to the door station

Before assigning apartments to the door station, add all apartments to the system that should be visible on the door station. See explanation in the previous section. In the following it is assumed that all apartments are already present in the system. To assign apartments to door station:

- Enter the Door station settings – select the text box **Assign apartments to door station** that is located in the middle column.
  - A new pop-up will appear with the display of all un-assigned apartments noted in the left column and assigned apartments in the right - see Picture 8.7.



**Picture 8.7: Assigning apartments to the door station**

Assigning apartment(s) to door station:

Start typing Apartment ID into the search field on the left, and when it is shown in the list, select it and press the Add button. The apartment(s) will be assigned to the door station and will appear in the list of assigned apartments.

Un-assigning apartment(s) from the door station:

Select apartments from the right panel and by pressing the **Remove** button.

Apartment(s) will be unassigned from the door station.

**NOTE:** Multiple apartments can be selected using the "Shift" or the "Ctrl" key.

Search function:

- If any of the lists contains a lot of apartments, it can be narrowed by entering the apartment name into the search field. Once the correct apartment is displayed, it can be easily assigned or removed.

## 8.4.6 Updating content on door station

**NOTE:** The sysadmin can always manually update data from GUI. If the user's data or apartment is changed by the administrator, its data will be updated the next day. In the morning hours, the system will check if any changes were made in the previous day and automatically apply them. The data is not updated immediately because on some devices this takes a long time and during that time the device is inaccessible.

When all settings for the door station are saved and the apartments are assigned, this data needs to be updated on the display of the door station.

To update content on door station:

- **Select the Door station** from the Door station editor.
- Click the button Menu > Update data on the door station.
  - Updated data is sent to the door station.
  - The door station replaces old data with new.
  - Door station device is restarted

**NOTE:** Sending data and updating information on the door station can take some time. It takes approximately 10 minutes to send and update data of 100 users/apartments.

## 8.5 Assigning apartments to the users

The user needs to have an **apartment assigned** in order to be visible on the display of the door station/mailbox/info board.

To assign apartment settings to a user:

1. Navigate to **Users** widget.
2. Select a user from the list.
3. Double click on the user or select **Menu > Edit user [Name]**.
  - User's profile is displayed.
4. Enter Apartment's name to the **User's apartment** field.

## 8.5.1 Advanced text manipulation

The screenshot shows a web interface titled "Edit User mat". At the top right, there are "Save" and "Menu" buttons. Below the title, there are four tabs: "General", "Advanced", "Account", and "Latest events". The "Advanced" tab is selected. The interface is divided into three columns of settings:

- Left Column:** "Card validity for offline readers after card registration on online reader" with a dropdown menu set to "Unlimited".
- Middle Column:** "Anti-passback function" with a checkbox "User can open doors even if they are blocked or limited by anti-passback function" (unchecked) and an "Anti-passback status reset" button.
- Right Column:** "Apartment's visibility on doorstation" with a checkbox "User is visible on door station" (unchecked). Below this are two text input fields: "Overwrite text on door station" and "Overwrite text on call button".

Picture 8.8: Advanced apartment settings for a user

### Advanced settings for door stations and call buttons

To leave out username from door station:

1. Navigate to the specific user and select its **Advanced** tab like shown on the Picture 8.8.
2. Un-check the field User is visible on door station

To overwrite text on door station or call button:

- The fields **Overwrite text** directly changes the settings for the assigned apartment (it overwrites text on door station/call button) and it is meant for custom text changes.

**Useful for:** Situations where an administrator is administering users but has no privileges to alter the hardware settings.

**IMPORTANT!** Remember to update all data on door stations after changing any of the **Apartment settings** for a user.

### Advanced settings for door mailbox display and info board

To provide a custom text on mailbox display/info board:

1. Navigate to **Apartments** widget and access the specific apartment
2. Change the **Overwrite text** entry like shown on the Picture 8.9.

### Edit apartment Apartment 2

Apartment ID	Apartment name
<input type="text" value="Apartment 2"/>	<input type="text" value="Apartment 2"/>
Apartment number	<input checked="" type="checkbox"/> Apartment is visible on door station
<input type="text" value="2"/>	Overwrite text on door station
Call button serial number 1	<input type="text" value="Overwrite text on door station"/>
<input type="text" value="6134234"/>	Overwrite text on call button
Call button serial number 2	<input type="text" value="Miran"/>
<input type="text" value="632445"/>	Overwrite text on mailbox display
Indoor station serial number 1	<input type="text" value="Prima"/>
<input type="text" value="0"/>	Overwrite text on info board
Indoor station serial number 2	<input type="text" value="Miran d.o.o."/>
<input type="text" value="0"/>	

**Picture 8.9: Apartment management**

**IMPORTANT!** If there are **multiple users assigned** to the **same apartment**, some of the display option allow displaying text for more than one person. If more than two persons with different last names are assigned in the same apartment, the software will use the data from the first two created (for any modifications, please use the overwrite function explained at the beginning of the sub-chapter).

## 9 Module: Mailboxes

Use the **Mailbox module** for managing mailbox units. It goes hand in hand with a **Door station module** since they both use the same apartment structure. To read about apartment creation and management, please read chapter 8.3 Managing apartments and 8.5 Assigning apartments to the users.

After creating and assigning the apartments, it is possible to create a mailbox unit in the software.

Mailboxes (2x4) <a href="#">Change</a>	
Apt4, Lastname 23 Apt4 Address 4	Apt8, Lastname 27 Apt8 Address 8
Apt3, Lastname 22 Apt3 Address 3	Apt7, Lastname 26 Apt7 Address 7
Apt2, Lastname 21 Apt2 Address 2	Apt6, Lastname 25 Apt6 Address 6
Apt1, Apt1 Address 1	Apt5, Lastname 24 Apt5 Address 5

Picture 9.1: Mailbox settings

### 9.1 Managing mailbox units

To create a mailbox section:

1. Navigate to Home > Hardware > Mailboxes.
2. Press Menu > Add new mailbox.
3. Set its name and provide data about its master central, which door socket it is connected to, its text display format and its dimensions.
4. After adding all information, press button **Add**.

If some mistakes occur during creations, correct by navigating to:

1. Select the mailbox from the list.
2. Press Menu > Edit [mailbox name].

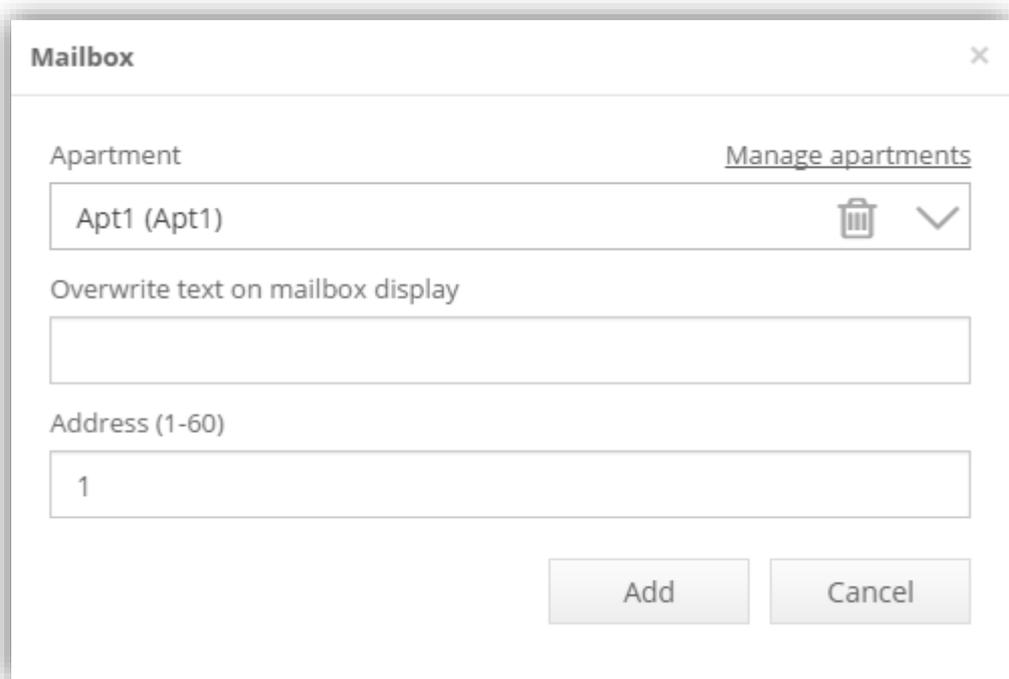
To remove mailbox:

1. Select the mailbox from the list.
2. Press Menu > Remove [mailbox name].

## 9.2 Assigning mailboxes to apartments

Assigning an apartment to the mailbox:

1. Enter the **mailbox** settings by double-clicking on its name found in the list or by clicking **Menu > Edit [mailbox name]**.
2. On the right panel, there is a visual presentation of the mailbox with the dimensions provided when created.
3. By clicking on the single entity, a pop-up window displays, asking for **Apartment, overwritten text on the display** and the **mailbox address** - Picture 9.2 (displayed on the screen if nothing is send as a replacement).
4. Once everything is set-up, press button **Add**.



The image shows a dialog box titled "Mailbox" with a close button (X) in the top right corner. The dialog contains three input fields and two buttons. The first field is labeled "Apartment" and contains the text "Apt1 (Apt1)". To the right of this field is a link labeled "Manage apartments" and a trash can icon. The second field is labeled "Overwrite text on mailbox display" and is currently empty. The third field is labeled "Address (1-60)" and contains the number "1". At the bottom of the dialog are two buttons: "Add" and "Cancel".

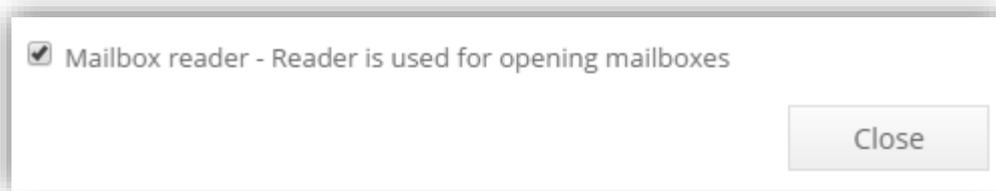
**Picture 9.2: Assigning mailboxes to apartments**

**NOTE:** The apartment and the mailbox address must be unique for every mailbox unit (can only be assigned to a single entity).

### 9.3 Setting reader to work with the mailbox

In order to assign a reader for opening the mailbox, navigate to its Advanced settings (Home > Hardware > Centrals > Edit > double click on reader > Advanced tab).

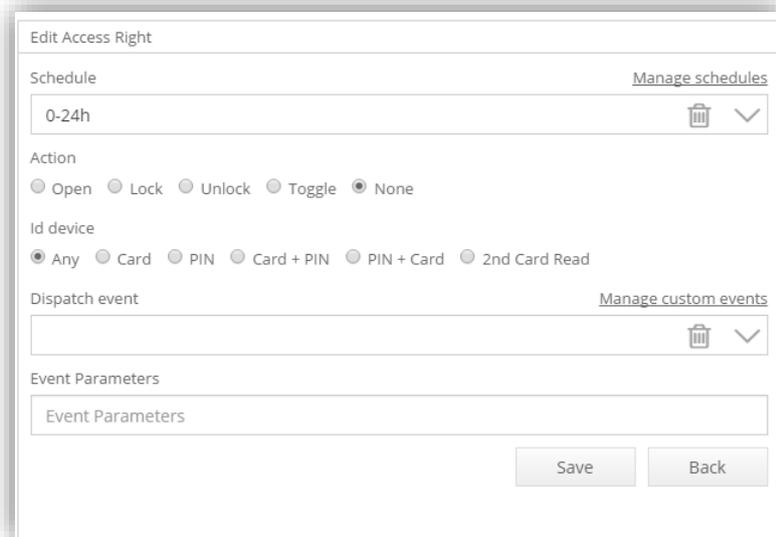
On the bottom of the popup menu, there is an option: Mailbox reader. Ticking this checkmark, assigns the selected reader to mailbox handling.



Picture 9.3: Assigning the reader for mailbox handling

### 9.4 Creating and assigning mailbox access rights

By assigning access rights to the reader previously set as **Mailbox reader**, and assigning the correct access group to the user with the apartment, allows the user to access the mailbox by showing the card to the mentioned reader.



Picture 9.4: Access rights of the mailbox access reader

**NOTE:** The mailbox reader does not have to be connected to the central that has mailbox unit connected to it.

IMPORTANT! Only 1 entity can be opened at a time. If someone tries to open a second mailbox, the reader will sound an error message, until the first lock is closed.

**IMPORTANT!** Lower hardware centrals (sold before August 2016) **only** support connections of mailboxes on Door 1 & 2!

After all mailboxes are assigned to apartments, they should update with the correct text on the display. Moreover, the option to **Open** mailbox from the GUI becomes available when opening the mailbox entity popup. To replace the text on the mailbox display, fill in text in the field.

The mailbox displays should update automatically, but to update them manually, just press the **Save** button.

If the communication between the central and the mailbox drops, there will be a warning sign next to the display text in the Mailbox preview.

Whenever making any changes to the users who have apartment assigned, their display on the mailbox should update immediately.

## 10 Module: Floor plan

Floor plan module is an overview on the set system. Import own building blueprint and visually place hardware objects onto it. Moreover, control the set object.

**NOTE!** To have a larger overview of the Floor plan, the left menu is automatically hidden. To show it again, just click the down pointing arrow on the left corner of the screen.

### 10.1 Managing floor plans

To create a floor plan:

1. Navigate to Home > Monitoring > Floor plan.
2. On the right panel make sure that the tab **Floors** is selected.
3. Press Menu > New floor plan.
4. Set its name and provide a picture from the local computer or from the internet (in both cases, the picture will be downloaded to the central).
5. Press button **Add** to save the changes.

If there were some mistakes made during creations, correct by:

1. Select the floor plan from the **Floors** tab.
2. Press Menu > Edit [floor plan name].

To remove floor plan:

1. Select the floor plan from the **Floors** tab.
2. Press Menu > Remove [floor plan name]

### 10.2 Floor plan hardware

To add items to your floor plan:

1. Navigate to **Hardware** tab on the right panel.
2. Press Menu > Add item to the floorplan.
3. The software will offer three options to choose from:
  - Reader
  - IP Camera
  - Label

To add a **Reader** to the floor plan, select the wanted reader from the dropdown list and press **Add**. Clicking on the image places the wanted reader to a position on the image.

To add **IP Camera** to the floor plan, an IP camera must first be installed in the Nova software (more on IP cameras and their implementation in chapter **5.3.3 IP Camera**). Select the wanted camera from the dropdown list and press **Add**. Clicking on the image places the wanted camera to a position on the image.

By selecting a **Label**, first give the label a proper name, then select its type:

- Link to URL web address will redirect anyone who will click on it to the URL provided in the bottom entry.
- Link to floor plan will make a mesh of easier navigation between floors (create at least two floor plans in order to link between them). It is a good idea to make it both ways (ex. Main floor link to the 1<sup>st</sup> floor of floor plan and on the 1<sup>st</sup> floor of floorplan link back to the Main floor).
- Link to the central: If there is a massive installation of separate systems, it is possible to navigate to another central without remembering its correct IP address by providing it here with the username (if the username and password is the same on both centrals, the administrator is directly logged-in when pressing this widget).

Press **Add**. Clicking on the image, places the wanted label to a position on the image.

Navigating to the **Hardware** tab, all the added hardware shown on the floor plan is visible. By selecting one, it will be displayed in bold on the image for easier recognition and the tabs next to **Hardware** will change based on the hardware type.

- Selecting a Reader will display:
  - **Events** tab (displays last events of the reader)
  - **Users** tab (displays users that have access to the reader)
  - **Groups** tab (displays Access groups that have access to the reader)
- Selecting an IP camera will display:
  - **Camera** tab (displays picture from the camera)

## 10.3 Floor plan navigation

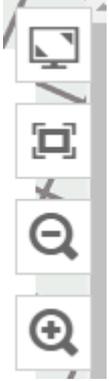
The navigation on the Floorplan is similar to navigation on mobile devices. Click and drag to move over different areas of the image. Scrolling in and out will zoom the image (on mobile devices use pinch and stretch gestures to get the same result).

Moving Hardware objects around can be done by clicking on them – a menu will show:

- Reader menu:
  - Open
  - Unlock/Lock
  - Block/Unblock
  - **Move** – allows relocation of the reader to some other location on the floor plan.
  - **Remove** – removes the hardware from the floor plan.
- IP camera menu:
  - **View image** – will open a new pop-up with the camera image.
  - **Open camera** – will open the GUI of the camera (only for the known types).
  - **Rotate** – will rotate the **icon of the camera ONLY!** for easier determination to where the camera is pointed at.
  - **Move** – allows relocation of the camera to some other location on the floor plan.
  - **Remove** – removes the hardware from the floor plan.
- Label menu:

- **View** – will redirect anyone to the provided target.
- **Edit** – allows edition of the Label.
- **Move** – allows relocation to some other location on the floor plan.
- **Remove** – removes it from the floor plan.

Here are the descriptions of the buttons displayed next to the floor plan image:



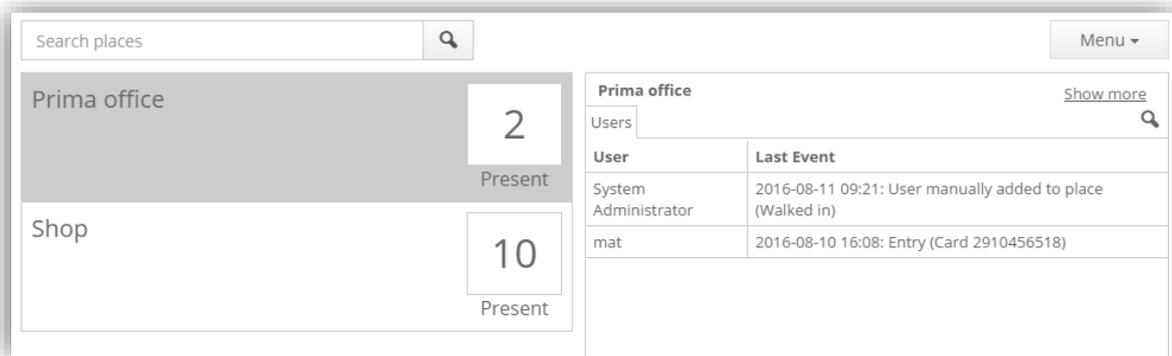
- Full screen mode
- Fit image to the size of the screen
- Reduce zoom
- Increase zoom

## 11 Module: Presence

Presence module is a great way to keep track on how many people enter or exit predefined facilities. Determine people who are still located within the premises with the help of direction set on the readers. In addition, if adding the user telephone numbers in the software and connecting a **GSM module** (chapter 5.3.1) to the central, the administrator can send them a SMS with prompt to answer with a **keyword**. Based on the answer, it is possible to check if they are still inside, otherwise they will be removed from the group of people listed as present.

This module is activated with the activation key (read about activation keys and how to enter them in chapter **6.1 Add-ons and Modules**).

### 11.1 Managing presence places



Picture 11.1: Presence locations

To add a new place:

1. Navigate to Home > Monitoring > Presence.
2. Press Menu > Add new place.
3. Enter:
  - **Name** of the place.
  - Hardware list that includes all readers that belong to that place (read about creating a new Hardware list in chapter 14.2.2 Readers list)
  - **Past Days** – determines how long the history of user entries should be kept.
  - **Entry keyword** – in case a user telephone number is correctly set up and if the user was not added to the list of present persons, the user can send a SMS with keyword and be added to the list.
  - **Exit keyword** – in case someone left the location without registering on the exit reader, it is possible to respond to a warning message by SMS and be removed from this location.
  - **Template message** – A SMS template that should explain why the user received this message and how to respond (which keywords to use).
4. Click **Add** button to create the new presence location.

To edit an existing place:

1. Select the place from the menu.
2. Click on the button Menu > Edit [place name].
3. Update settings and **Save**.

To delete an existing place:

1. Select the place from the menu.
2. Click on the button Menu > Remove [place name].

## 11.2 Managing users in places

Users who enter through readers with a set direction entry/exit (check on how to set **Reader direction** in chapter **5.1.15 Reader settings**) and the readers are included in the Hardware list of the Location are automatically added/removed from the place.

Manually add or remove users from a specific location by:

1. Entering the location by double clicking on it.
2. User management:
  - To manually add user to the list (Picture 11.2), click on **Menu > Manually add users**
    - Select the user to add (selecting multiple users can be done by holding Ctrl or Shift key). Press **Add selected (number of users)** and provide a reason when asked in the pop-up window.
  - To remove the user(s) from the list, select them from the list and press **Menu > Manually remove users (number of users)**.

By default, only users who are inside are shown. To also display users that left, a couple of options exist when pressing the **Menu** button:

- **Hide all** option, turned on by default and hides users who left.
- **Today** option, displays users who are inside and users who left in the last 24 hours are displayed in red.
- **Last N days** option, displays users who are inside and users who left in the last N days (set in the Location settings).

To send a SMS to user:

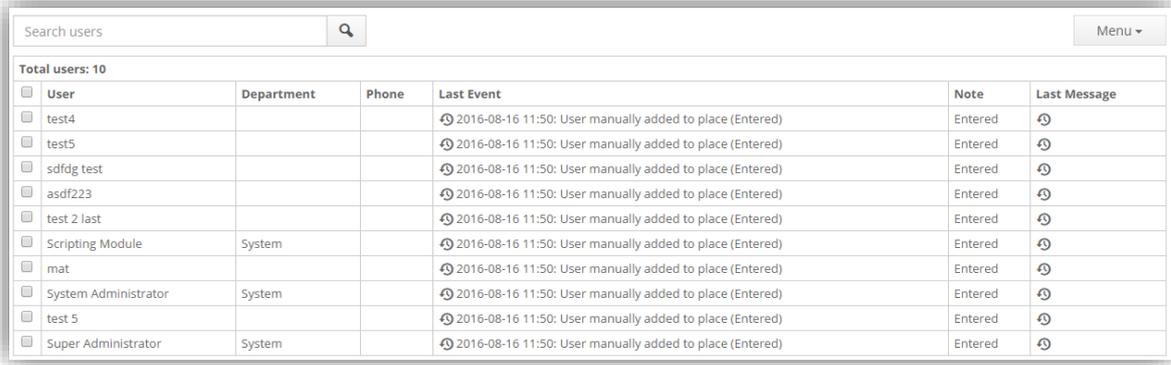
1. Select the user(s) in the location.
2. Press Menu > Send message to users (number of users).
  - If there is a template message for the location, it will be entered automatically.
3. Press **Send** to send the message.

**IMPORTANT!** If the keywords are the same in multiple locations, a user will be added/removed from all of them.

**IMPORTANT!** If there are two locations and the keyword for one of them is a sub-string from another (ex. "OUT" and "OUTSIDE"), and a user replies "OUT", the user is removed

from both locations; but if the user replies "OUTSIDE", it will only be from the single location.

**IMPORTANT!** If the user SMS does not include the keyword at the beginning of the message, it will not affect the user presence and the message will be displayed next to the user name.



The screenshot shows a web interface for viewing user presence. At the top, there is a search bar labeled "Search users" with a magnifying glass icon and a "Menu" dropdown. Below this, a summary states "Total users: 10". The main content is a table with the following columns: "User", "Department", "Phone", "Last Event", "Note", and "Last Message". Each row represents a user, with checkboxes in the "User" column and a refresh icon in the "Last Message" column. The "Last Event" column contains a timestamp and a description of the event, such as "2016-08-16 11:50: User manually added to place (Entered)".

<input type="checkbox"/>	User	Department	Phone	Last Event	Note	Last Message
<input type="checkbox"/>	test4			🔄 2016-08-16 11:50: User manually added to place (Entered)	Entered	🔄
<input type="checkbox"/>	test5			🔄 2016-08-16 11:50: User manually added to place (Entered)	Entered	🔄
<input type="checkbox"/>	sdfdg test			🔄 2016-08-16 11:50: User manually added to place (Entered)	Entered	🔄
<input type="checkbox"/>	asdf223			🔄 2016-08-16 11:50: User manually added to place (Entered)	Entered	🔄
<input type="checkbox"/>	test 2 last			🔄 2016-08-16 11:50: User manually added to place (Entered)	Entered	🔄
<input type="checkbox"/>	Scripting Module	System		🔄 2016-08-16 11:50: User manually added to place (Entered)	Entered	🔄
<input type="checkbox"/>	mat			🔄 2016-08-16 11:50: User manually added to place (Entered)	Entered	🔄
<input type="checkbox"/>	System Administrator	System		🔄 2016-08-16 11:50: User manually added to place (Entered)	Entered	🔄
<input type="checkbox"/>	test 5			🔄 2016-08-16 11:50: User manually added to place (Entered)	Entered	🔄
<input type="checkbox"/>	Super Administrator	System		🔄 2016-08-16 11:50: User manually added to place (Entered)	Entered	🔄

**Picture 11.2: Presence user list**

## 12 Module: Wireless online

In some cases, it is not possible to mount a wired reader (due to lack of space, door material etc.), but there is a desire to manage the door from the software. For such mounts, a special hardware called **Antenna module** is needed for conversion of the offline readers. To make this option work in the software, provide the activation key (read about activation keys and how to enter them in chapter **6.1 Add-ons and Modules**).

**IMPORTANT!** If the connection between the wireless online reader and the Antenna module is lost, the reader will flash green/red LED and the reader will beep whenever the card is shown for a few seconds. After that, it will switch to offline mode until the wireless connection is established again. That is why **it is recommended that the reader is set-up as an offline reader first!** before proceeding with the wireless upgrade.

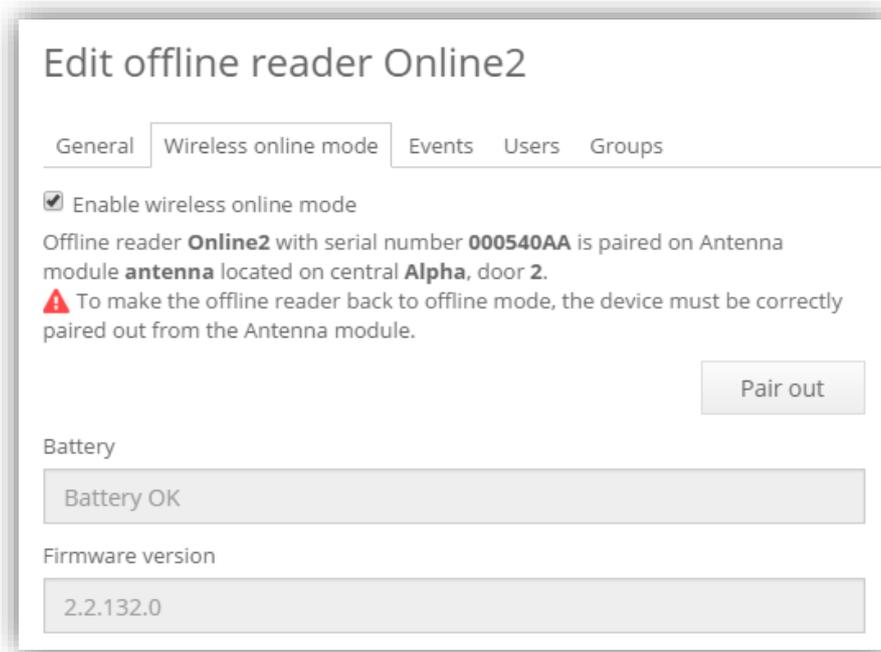
**IMPORTANT!** Nexus offline does not support this functionality.

### 12.1 Offline to online reader conversion

In the Offline reader settings, a new tab is displayed – **Wireless online mode**. Checking the **Enable wireless online mode** will show additional options to connect the current offline device with the Antenna module. A new button **Pair** will appear. Click it to open a pop-up wizard that will help pair the Antenna module and the offline reader. This is done in three steps:

1. First, add new Antenna module by clicking on **Menu > Add new Antenna module**.
  - A pop-up will require Name, Serial number, and information regarding to which central and what door socket Antenna module is connected to.
  - After entering the data, select the new device in the list and press the **Next** button.
2. Put the **Wireless service card** on the offline handle and press the button **Pair**. A green LED will flash and a sound confirmation will notify you of a successful pair. The GUI will display the OK message and automatically redirect you to step 3.
3. In order to confirm the offline reader, a **serial number** from the reader **needs to be checked** and selected from the list. By pressing Finish, the offline reader and the Antenna module will try to establish a connection.

**NOTE:** The wireless online reader data (battery and firmware version) updates every time the reader is used.



**Picture 12.1: Wireless online mode**

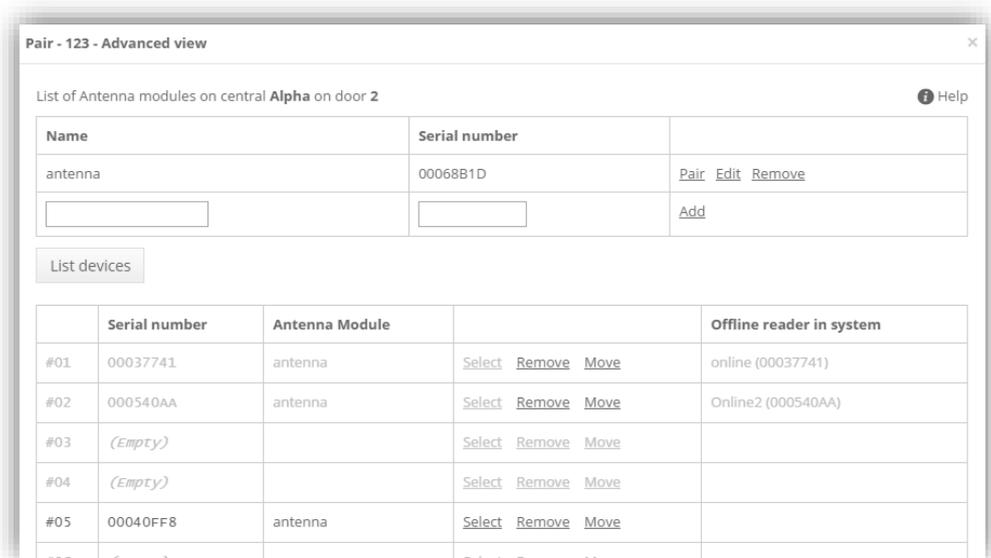
### 12.1.1 Advanced view

In the second step after selecting the Antenna module, it is possible to select the **Advanced view**. From here, there is a table displaying different information about the connected and assigned wireless online readers.

Columns description:

- Wireless offline address (from 1 to 16).
- Serial number of the Antenna Module.
- Name assigned to the Antenna Module.
- The options to Select, Remove, Move Readers
- The name of the Wireless online reader and its serial number.

If there are any errors like address collisions, a wireless online reader that has no antenna module set, wireless online reader connected to multiple antenna modules etc., these are visible from **Advanced view**. Detectable errors like address collision will also display in a red marked row and an error message.

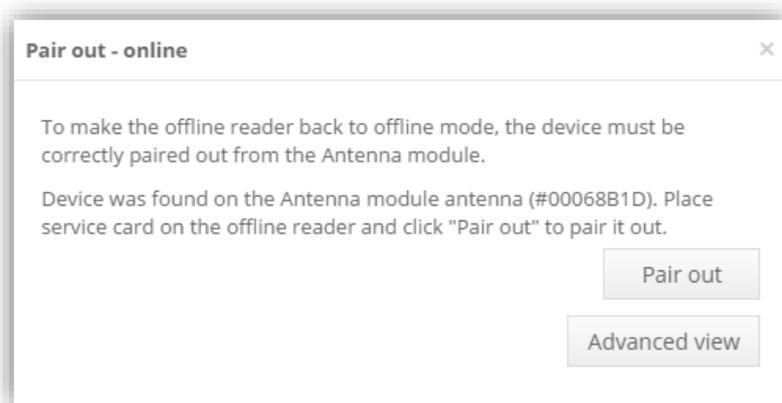


Picture 12.2: Wireless online advanced view

## 12.2 Removing function from wireless online readers

To remove the wireless functionality:

1. Navigate to the **Home > Hardware > Offline Readers**, double click on the wanted wireless online reader, click on the **wireless online mode** tab and press the **Pair out** button.
2. Put the **Wireless service card** on the wireless online reader and press **Pair out** button in the GUI. A green LED, sound and GUI message will display the successful pair-out.



Picture 12.3: Wireless online reader pair-out

## 12.3 Wireless online reader functionalities

Having a reader activated in the system, we can:

- See the battery status next to its name (located in **Home > Hardware > Offline Readers**).
- Actively edit its time schedule (only 1 allowed).
- Use the Open, Un/Lock, Un/Block functions. **IMPORTANT!** Whenever one of these commands is sent to the wireless online reader, it needs to be woken up (turn it a few times) before the setting changes.
- Active door events are displayed in the **Events** list.
- If the Antenna module is disconnected, it is displayed under the **Disconnected centrals and readers**.

**IMPORTANT!** Maximum readers that can be connected to a single Antenna module is 16.

## 13 Module: Booking

The booking module is for reservation of the premises at the specified date for a defined period.

Add booking activation key to the system:

The booking activation key must be added to the system as described in **6.1 Add-ons and Modules** along with the booking software that can be found on the Prima's homepage.

When the package is downloaded to the local storage, upload it to the central the same way upgrade package is uploaded – described in the caption 5.1.9 Upgrade software on central.

**IMPORTANT!** The booking module must be uploaded and used on the **master central**; otherwise, no reservations can be done (the feedback will be "Error! User privileges are not sufficient").

**NOTE!** The booking can only be set to work with the online readers.

### 13.1 Booking access groups

After activation and software update:

1. Click on the Menu > Add group
  - New type of Access group type, called **Booking location**, is now added to the list of access groups
2. Click **Add group** button to create new booking location.  
**NOTE:** It is recommended to name the access group according to the booking resource.

Picture 13.1 shows additional parameters that must be filled for each booking access group:

- **Location opening hours** – defines the working hours of the resource, e. g. opening and closing time of the Sauna.
- **Default reservation duration** – represents the period of how long can users use the premises after claiming the reservation.
- **Remarks** – displays a custom message to users who are making the reservations. The message should provide additional guides to users and their reservation (e.g. location of entrance to the facility, where to park, etc.).

- When the booking access group is created, it will be added to the list with other access groups. For easier distinction between user access groups and booking access groups, the type of group is displayed next to the group name.

**Picture 13.1: Adding a new booking location**

Picture 13.1 shows an example of:

- A new Booking access for "Sauna" that opens at 8 o'clock in the morning and closes at 9 o'clock in the evening.
- Each user can make a reservation for 30 minutes.

Assigning the booking access group to a reader:

- Each booking access group can be associated with an existing reader in the Nova system.
- Assigning booking access group is the same as assigning any other group to the reader (see **chapter 4.2.3**).
- Assigning one or more readers to a booking access group creates a new access zone thus granting access in the selected zones during the time interval defined by user reservations.

## 13.2 Reservation creation and cancellation in Booking module

After access group configuration in Nova, the Booking module can be accessed with a web browser on address:

- `http:// <IP of the central> / Booking`
  - (Replace the text inside <> with IP address of the specified central).
  - A new login page will appear and grants access with the same credentials as in Nova.

**NOTE:** For basic reservations, use an administrator type of account for creating or cancelling the existing reservations.

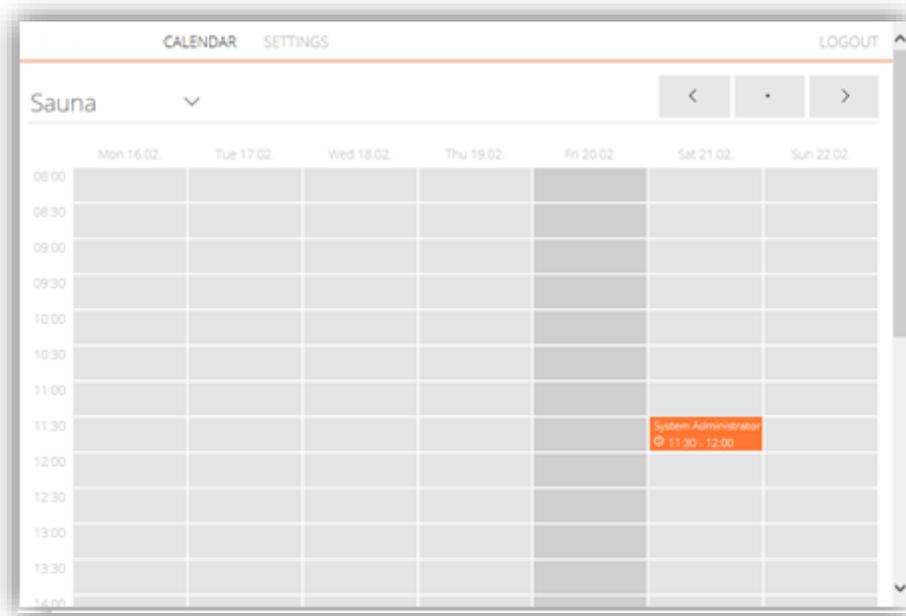
Example in Picture 13.2 shows:

- A calendar page of the Booking application where the resources are listed in the top left corner.
- Currently the location is set to Sauna as added in previous example:
  - Switch locations by clicking on the name and selecting the other location from the list.
  - The calendar is set by days, marking the current day in darker gray color. Reservation times are separated depending on the "Default reservation duration" set (Picture 13.1).
  - The buttons on the top right above the grid are used for switching between different weeks.
  - The middle button resets the overview to the current week.

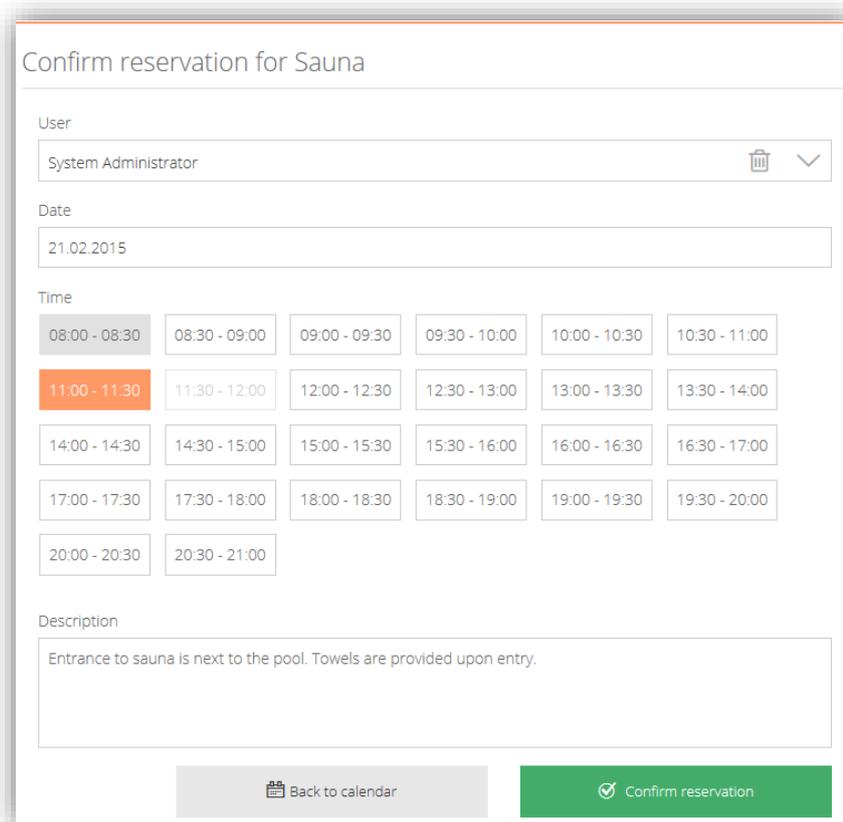
Creating a new reservation:

Creating new reservation requires a user to select the corresponding part of the calendar.

- Click the **Confirm reservation** button to confirm the reservation (Picture 13.3)

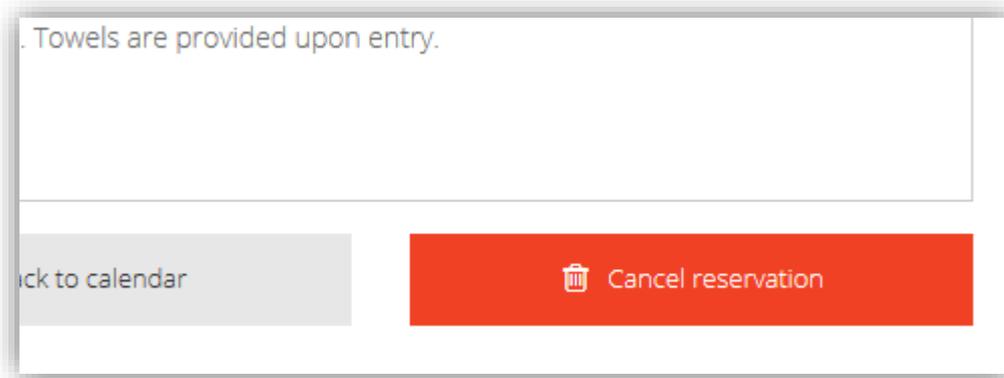


**Picture 13.2: Calendar page of Booking module**



**Picture 13.3: Reservation confirmation (system administrator can see all time reservation hours, while a user only sees the one that was selected)**

- It is only possible to make reservations in the future and not for elapsed time. **Confirm reservation** window has previously set reservations grayed out which cannot be selected.
- Click the **Cancel reservation** button to cancel the reservation selected in the calendar (Picture 13.4).



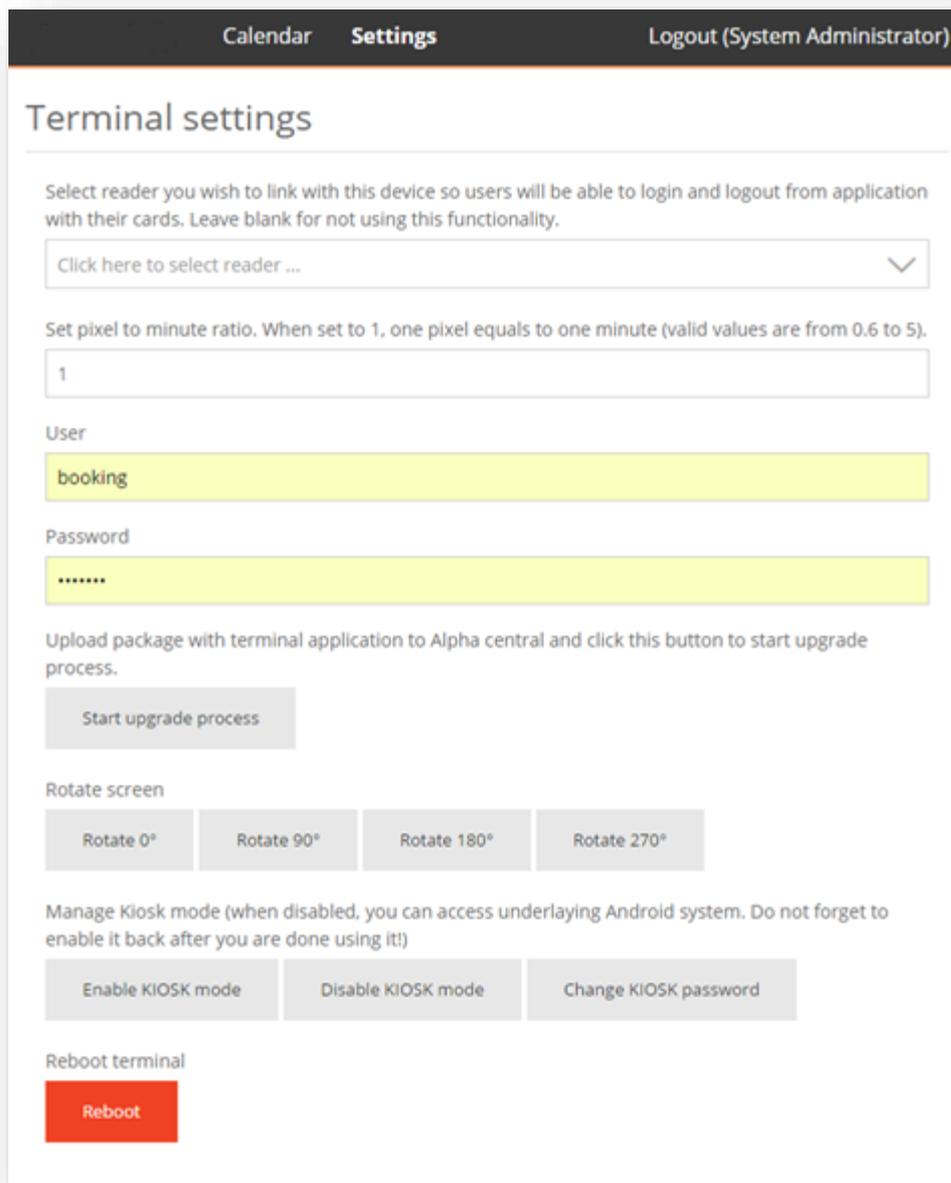
**Picture 13.4: Cancelling reservation**

### 13.3 Booking as a terminal application

- The booking module can be run standalone in terminal mode.
- Suggested prerequisites for this mode are touch capabilities of terminal screen and a Nexus reader connected to the central (Android standalone booking terminal requires a special *booking.apk* installed, the device must also be rooted for kiosk mode where users have no access to underlying Android platform).
- Users can use their RFID (Radio frequency ID) – cards to log-into application and confirm their reservations.

To enable terminal mode:

1. Start the **Booking** application on the terminal
2. Log into application as **System administrator**
3. Select a reader in the settings menu (Picture 13.5) - to provide user authentication and access to Booking page.
4. For User and Password provide account information with at least Administrator privileges – this is a security feature that prevents other users from amending any unwanted requests.
  - Entered data is automatically saved.



**Picture 13.5: Booking terminal settings (Android booking terminal has a few extra settings)**

Pixel to minute ratio allows adjustment of the calendar grid to actual screen size. This way all of the bookable time slots are displayed on the screen without need of scrolling.

booking.apk can be upgraded by pressing on Start upgrade process button. For upgrade to work you need to upload upgrade package to central (same central to which Booking is connected). Correct files will then be downloaded from central and existing application will be replaced by new one.

You can also upgrade terminal by copying booking.apk to terminal via USB flash drive and manually install it

Setting menu also provides functions to work with Android OS through Booking application. You can change screen orientation, disable and enable Kiosk mode and reboot terminal if needed. Some described features are also accessible by swiping two fingers on terminal screen. List below summarizes swipes on screen and corresponding actions:

- Two finger swipe from BOTTOM to TOP: Disable Kiosk mode
- Two finger swipe from TOP to BOTTOM: Enable Kiosk mode
- Two finger swipe from RIGHT to LEFT: Set central IP address
- Two finger swipe from LEFT to RIGHT: Reload Booking application
- Slow (> 5 sec.) two finger swipe from LEFT to RIGHT: Reboot terminal

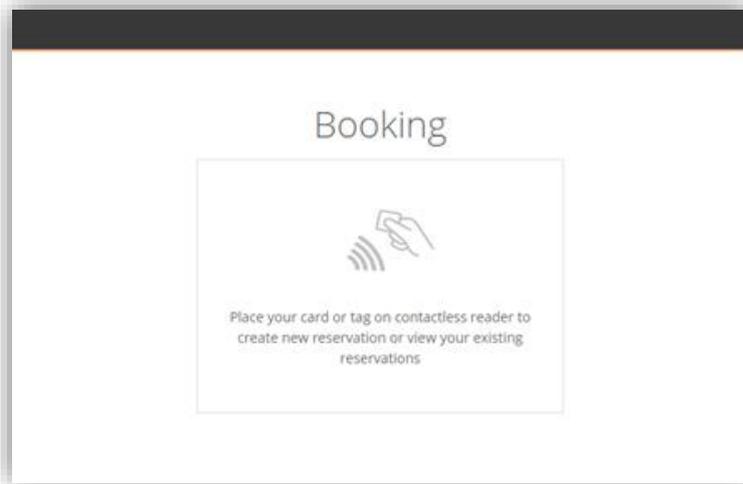
NOTE! Swipes are accessible from all screens of Booking application and are password protected. You do not need to be logged into application to use them. Default password is set to 267267, but it is **strongly recommended to change it** by tapping on Change KIOSK password button (Picture 13.5).

Log-in when terminal mode is enabled. Picture 13.6 shows a preview of the login-screen when terminal mode is enabled.

To login the user needs to:

- Place the card on the Nexus reader.
  - When the reader detects the card, the Booking application will take care of login and redirect the user to the Calendar page after a few seconds.

**NOTE:** Maintenance contact information set in Nova is shown on the terminal login screen.



**Picture 13.6: Terminal login screen**

Alternative login:

- In case of troubles, the normal login form is accessed by tapping on RFID icon seven times.
  - Login proceeds normally as described in the first paragraph of chapter **13.2**.

Log-in credentials and user access:

- Regular users can also enter the Booking application with the same credentials as they have in Nova when their account type is at least **User**.
- Account type can be set in Nova – see 4.2.3 Managing users, their access rights:
  - Double click the user field to access the user information and then navigate to the **Account** tab on the left menu.
- The drop-down menu at the top of the window enables the setting of the user access to the application.

### Confirm reservation on terminal:

When trying to confirm the reservation on the terminal, a button with RFID icon will appear (Picture 13.7).

- To confirm, users must place their card on the Nexus reader to finish the process.



**Picture 13.7: RFID icon on Confirm reservation button in terminal mode**

- Inactive users will receive a warning about automatic sign-out after 30 seconds.
- If there is no interaction with the application for another 10 seconds, they will be automatically logged-out to prevent any unauthorized access.

**Note!** Booking also detects user inactivity and it knows how to start daydream mode (part of Android OS which acts as screensaver). Daydream has to be enabled in Android settings application under Screen section. Daydream will be cancelled when user places her card on the reader or when screen is touched.

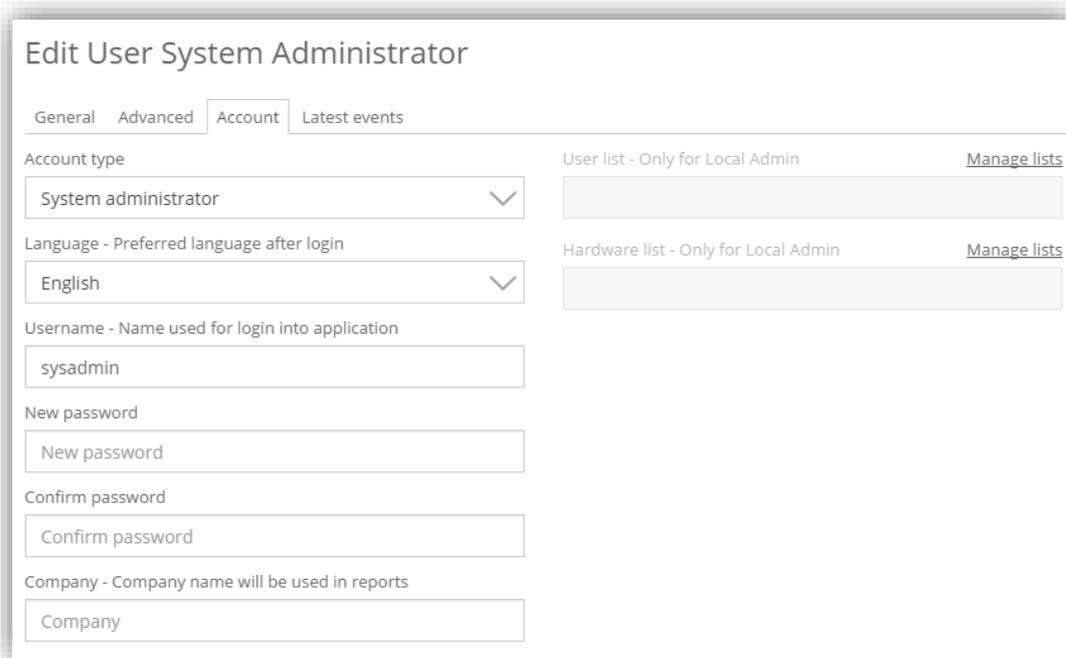
## 14 Module: List Editor

List editor is a perfect module for buildings with several smaller companies. It allows the system administrator to create groups and assign them specific hardware that they have access to. This way there are no unauthorized accesses because the local company administrators only have control over their own users/readers.

To get started with the List editor, install **Nova software version 2.0** or newer. The latest software package can be found on Prima's web page.

### 14.1 Module installation and location

To enable the List editor module, enable the activation key in the system. The procedure of adding an activation key is described in **6.1 Add-ons and Modules**. After activation, the List editor can be accessed by navigating to **Home > Settings > List Editor** or by navigating to **Manage lists** link in the user **Account tab** by selecting and editing one of the users, as displayed on Picture 14.1.



The screenshot shows a web interface titled "Edit User System Administrator". At the top, there are four tabs: "General", "Advanced", "Account" (which is selected), and "Latest events". Below the tabs, the "Account" tab contains several form fields:

- Account type:** A dropdown menu with "System administrator" selected.
- Language - Preferred language after login:** A dropdown menu with "English" selected.
- Username - Name used for login into application:** A text input field containing "sysadmin".
- New password:** A text input field containing "New password".
- Confirm password:** A text input field containing "Confirm password".
- Company - Company name will be used in reports:** A text input field containing "Company".

On the right side of the interface, there are two sections:

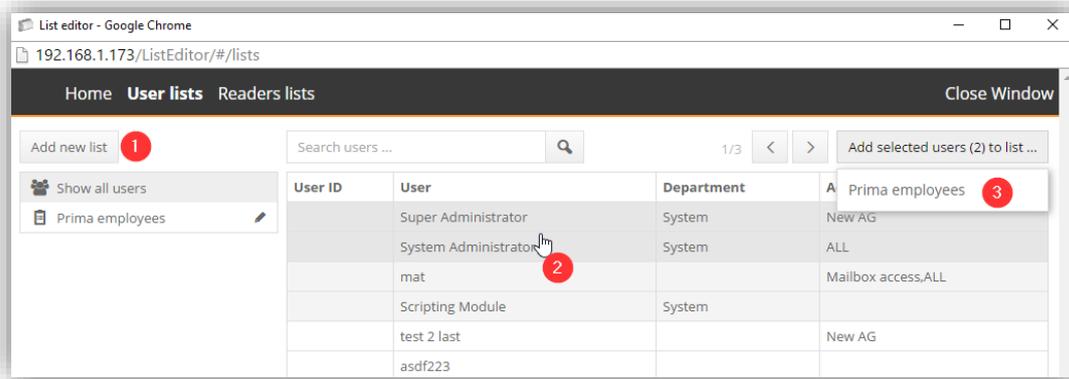
- User list - Only for Local Admin:** A section with a "Manage lists" link and a list area.
- Hardware list - Only for Local Admin:** A section with a "Manage lists" link and a list area.

Picture 14.1: List editor accessed through user settings

## 14.2 Management of different lists

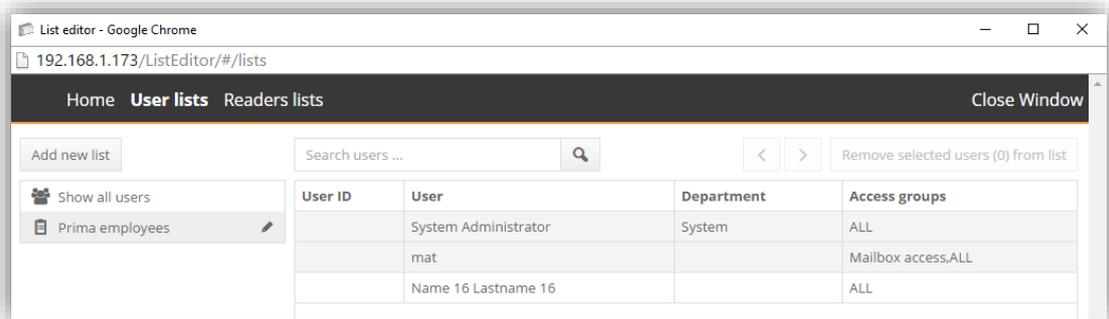
### 14.2.1 User lists

Upon opening the List editor page (Picture 14.2), a list of all users in the system is displayed. To create a new list, select the button on the left and provide a list name. Find the newly created list on the left side below **Show all users**. To add people to the list, select them from the user table. Multiple non-sequential users are selected by holding CTRL key on the keyboard while multiple sequential users are selected by holding SHIFT key. When completing the selection, press the button on the top right corner **Add selected users (n) to list** and from the dropdown menu select the corresponding list.



**Picture 14.2: Creating new user list, selecting users and assigning them to the new list**

To view users on a certain list, select the appropriate list on the left side and the users are displayed as shown on Picture 14.3. To remove user(s) from the list, simply select those the same way they were added and press the **Remove selected users (n) from list** button in the top right corner of the application.



**Picture 14.3: An example of user list employee list**

Deletion or renaming of the list can be done by pressing the pen icon (  ) next to its name and choosing the corresponding button from the popup window.

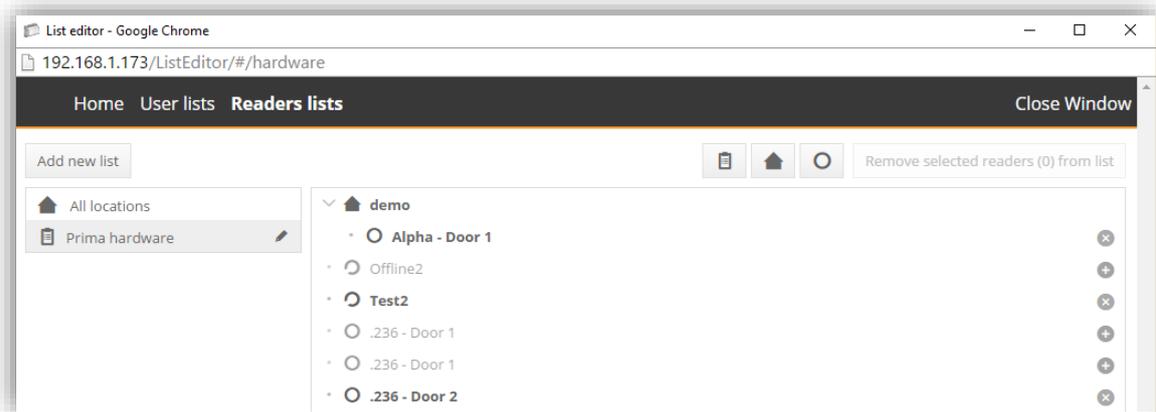
## 14.2.2 Readers list

A reader list is created similarly to the user list. It is accessed by selecting the **Readers lists** text in the top row of the application. A new reader list is created by clicking on the **Add new list** button on the left side and providing its new name. The newly created list is added to the end of the right column. Add readers to the specific list by selecting one or multiple readers and pressing the **Add selected readers (n) to list** button to the wanted list. Selecting a Reader list on the left side will display all readers included in the corresponding list in a bold font. Pressing the (+) button will add reader to the currently selected reader list.

Removing a reader from the list, can be done by pressing the (x) button for the removal of multiple readers select them and press the "Remove selected readers (n) from list" in the top right corner of the application.

Deletion or rename of the list can be done by pressing the pen icon (✎) next to its name and choosing the corresponding button from the popup window. A completed Reader list is displayed on the Picture 14.4.

**IMPORTANT!** Only readers marked with bold text are in the selected list, others are there just for an easier perception of their location.



Picture 14.4: An example of reader list

## 14.3 Assigning local administrators and their lists

After creating the user and reader lists, they can be assigned to local administrators. To do so, navigate back to **Users and access rights** in the Nova software, Edit the selected administrator and switch to the Account tab as shown in Picture 14.5. The account type must be set to "Local admin". By doing so, two dropdown menus become available under Local admin settings at the bottom of the pop-up. Select the desired lists and do not forget to save the new settings.

The screenshot shows the 'Edit User mat' interface with the following elements:

- Account type:** A dropdown menu set to 'Local Admin'.
- Language - Preferred language after login:** A dropdown menu set to 'English'.
- Username - Name used for login into application:** A text input field containing 'md'.
- New password:** A text input field containing 'New password'.
- Confirm password:** A text input field containing 'Confirm password'.
- Company - Company name will be used in reports:** A text input field containing 'Company'.
- User list - Only for Local Admin:** A list containing 'Prima employees' with a trash icon and a dropdown arrow. A [Manage lists](#) link is visible.
- Hardware list - Only for Local Admin:** A list containing 'Prima hardware' with a trash icon and a dropdown arrow. A [Manage lists](#) link is visible.

**Picture 14.5: Assigning account type and corresponding lists**

Local administrators are now able to log-into the Nova software and manage the assigned users, access groups and time schedules. They can also see current events and already created floor plans along with the listed hardware.

**IMPORTANT!** Local administrators have the same rights as administrators in Nova but are limited to users and hardware from the assigned lists.

## 15 Module: Card designer

If we have intentions of printing custom cards, Card designer module can help us with that. The procedure of adding an activation key is described in chapter **6.1 Add-ons and Modules**.

To access the software, we need to navigate to User list, select the users that we wish to create custom designs for and press **Menu > Card designer**.

### 15.1 Designing a card

On the left side, we are presented with an edit box, while on the right side will be displayed the preview of the current card for every user that we have selected. NOTE! At the beginning, the back side of the card is not displayed, because it's empty. After we populate it, the preview will expand, showing us both sides.

#### Card size

By selecting the element, we are offered with option to use "Card bleed" which helps get rid of the empty card edges due to some printer limitations.

Clicking on **Advanced** button will display the current(default) card size. From there, a custom card size can be entered.

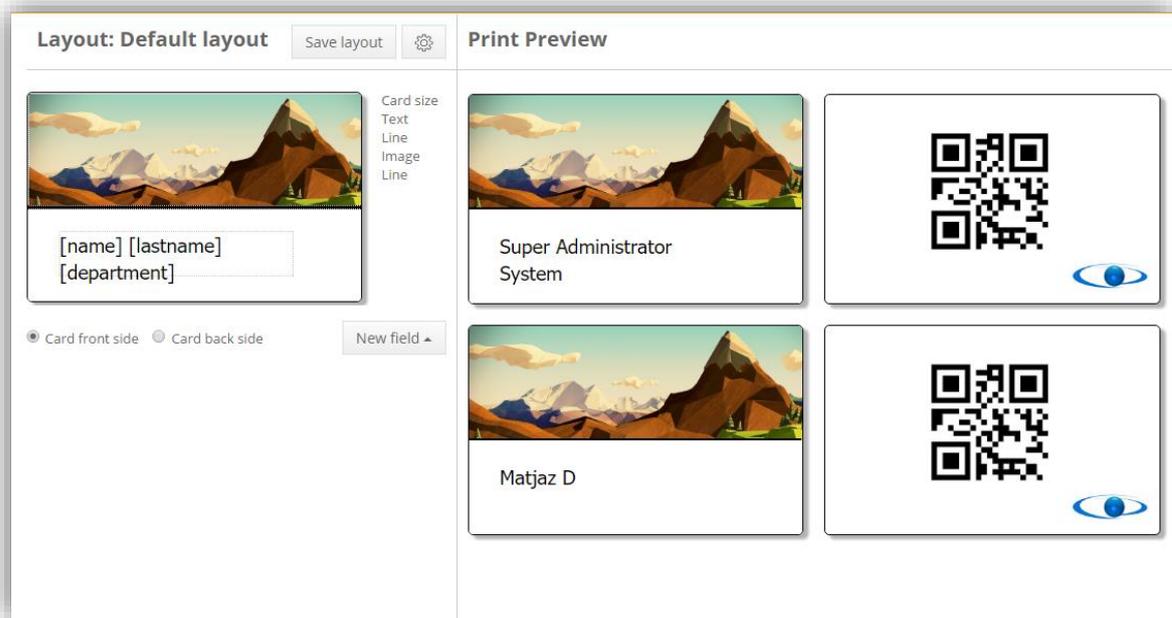
The other items that can be added on the card by pressing on the **New field** button. When the items are put on the layout, they are displayed on the list – right side of the card. By clicking on them, their settings are brought up. Common settings for all fields are:

- The field can be moved by clicking on it and dragging it to the wanted position. The position can also be set by offsets: **From top** and **from left**.
- Resizing the field can be done by clicking on the edge and drag or by changing the values in **Width** and **Height** fields underneath.
- **Depth** represents a value that defines which field is displayed under or over another. Lower number depth is displayed behind the others with a higher value.
- **Colour** will open a colour palate to choose colour for the field background (behind text, image...). To remove colour from the background field, just delete the text.

Some settings are dependent based on the selected field:

- Text – additional settings are **text font, size, colour** and **align**. To change the text, simply replace the text in the text field. To make text **bold** or **italic**, select it and press the corresponding button on the left. To enter user dependent text, press on the button **Insert**. The options are: Name, Last name, Department, User ID, E-mail, Phone, Company.
- Image
- Profile Image
- Horizontal line
- Vertical line

To remove a field, click it and press the **Remove** button. When everything is done, do not forget to **Save layout!**



**Picture 15.1: Front and back side preview of a card design**

## 15.2 Card layouts

After a layout is completed it will be saved as a default layout. If we wish to manage multiple layouts, we can do so by selecting the **cog wheel** (next to the Save layout button) and create a New layout. This opens a pop-up with request with:

- Layout name.
- Make copy of current layout – creates a copy, so you can preserve the original layout and make changes on a new one.
- Save changes before creating a new layout.

Once there is more than one layout present in the system, we can switch layouts by pressing on the cog wheel and click on the name of the other layout you wish to use. The currently active layout has a grey block in front of its name. The other options that are available from the same dropdown menu once a new layout is created and active:

- New layout
- Rename
- Remove

## 15.3 Additional user fields

Nova 2.2.10 and higher versions support creating additional fields that can be displayed on the card designer preview. Additionally, we can integrate some logic into card creation.

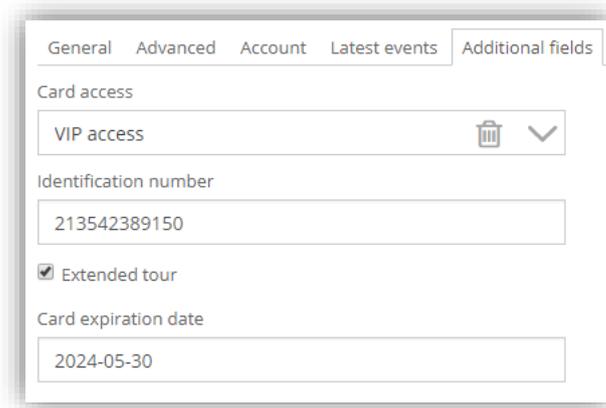
The fields can be accessed by navigating to **Users > Menu > Manage additional fields**.

A new pop-up will open showing any already created fields.

New custom field can be created by pressing **Menu > Add**.

There are different types of fields:

- Text – a custom text can be provided/displayed.
- Date time – Entry can be filled with the set date and time text.
- Date – Custom date can be set.
- Time – Custom time.
- Checkbox – We can react if the checkbox is enabled or not.
- Dropdown – Multiple predefined choices can be made.



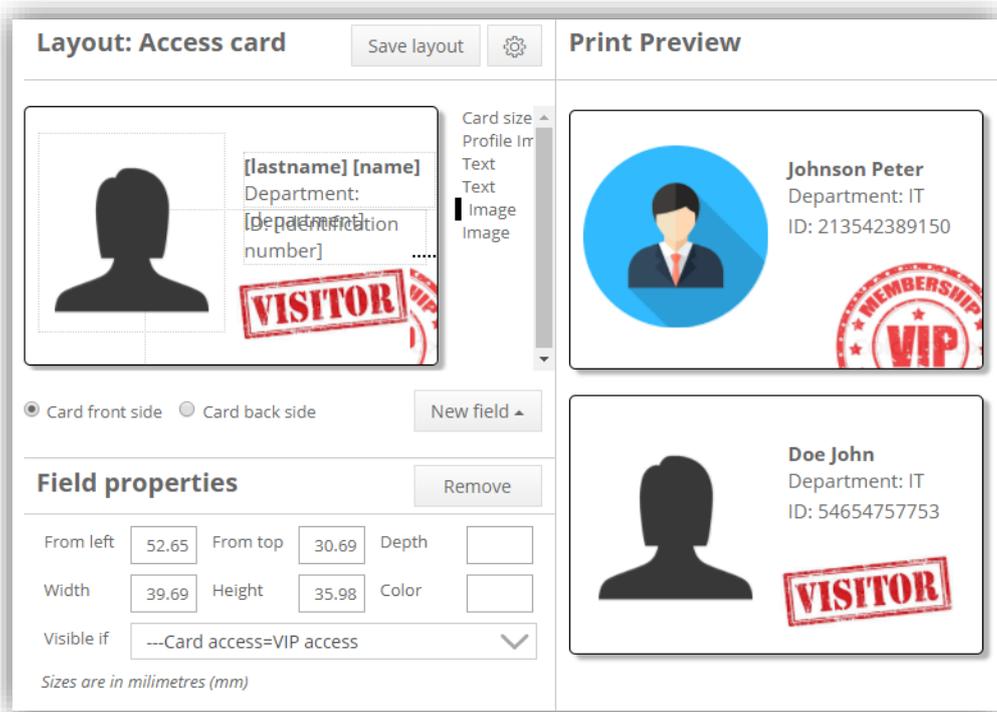
The screenshot shows a user interface for configuring additional fields on a card. The 'Additional fields' tab is selected. The fields are:

- Card access:** A dropdown menu with 'VIP access' selected and a trash icon to its right.
- Identification number:** A text input field containing the value '213542389150'.
- Extended tour:** A checkbox that is checked.
- Card expiration date:** A date input field containing the value '2024-05-30'.

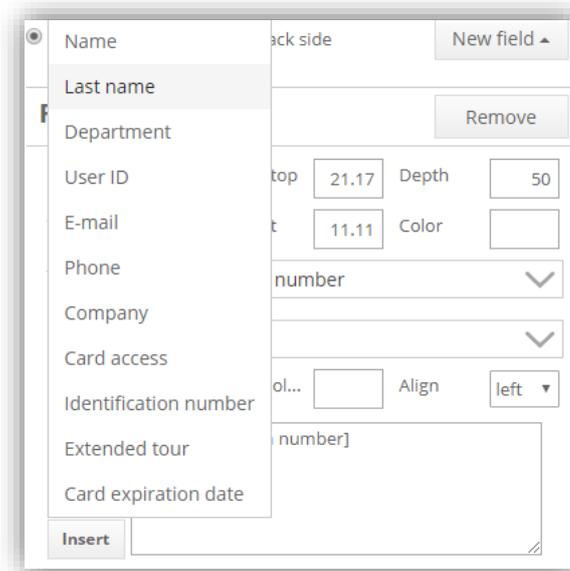
**Picture 15.2: An example of additional user fields**

In the card designer we can invoke the costume fields by selecting the “Visible” field properties. This way we can display a picture if the user has the correct checkbox filled or if the selection from the dropdown menu is valid.

This does not only affect the pictures, we can manipulate text too. For ex.: The text in the text field is present we can display it on a card.



**Picture 15.3: With custom fields we can create one layout with different custom content**



**Picture 15.4: Additional text options are displayed because of custom fields**

## 16 Module: Info boards

**Note: The info board module should only be used with NovaServer or with Alpha with external USB storage.**

This module enables users to create, assign and change the display of an Info board.

**Note: The Info board module requires separate hardware – info board driver and a display.**

To enable the Info board module, apply an activation key to the system. The procedure of adding an activation key is described in chapter **6.1 Add-ons and Modules**. After activation, the Info boards widget can be accessed by navigating to **Home > Hardware > Info boards**.

**IMPORTANT!** The default IP of the Info board driver is 192.168.1.101.

### 16.1 Info board driver

When all hardware is set up, search for info board in the network by clicking **Menu > Search info board**. If the central and info board are connected to the same network, it will be displayed in the left side list along with its version, IP and MAC address.

- If the info board driver is in a different network from the central, it needs to be moved to the same network as the central. This can be done by using Central discovery tool (you can read more about it in chapter **21 Central discovery tool**).

To add it to the software:

1. Double click on the found info board driver or
2. Navigate to Menu > Add [info board name] or

Add it manually by navigating to **Menu > Add info board**.

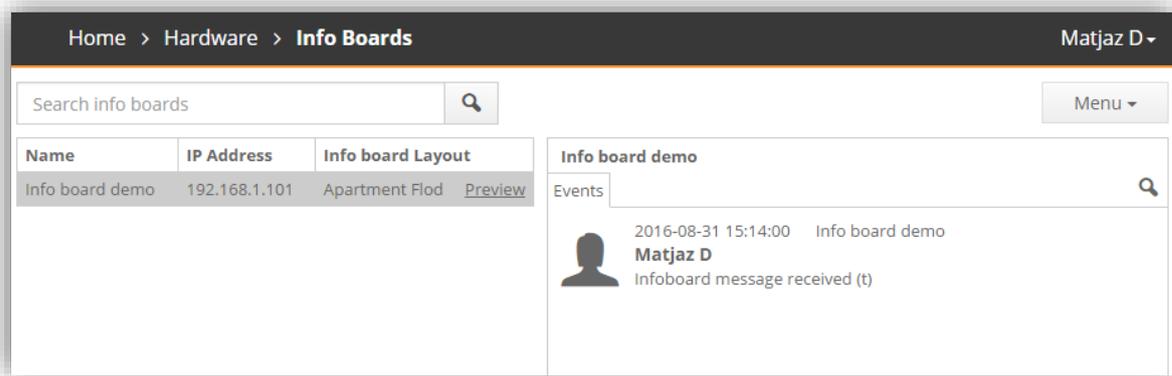
3. Provide/make sure that the name is entered and its IP address is correct.

To edit the info board:

1. Select the existing info board and press **Menu > Edit [info board name]** or
2. Double click to edit.

To remove info board:

1. Select it from the list and press **Menu > Remove [info board name]**.

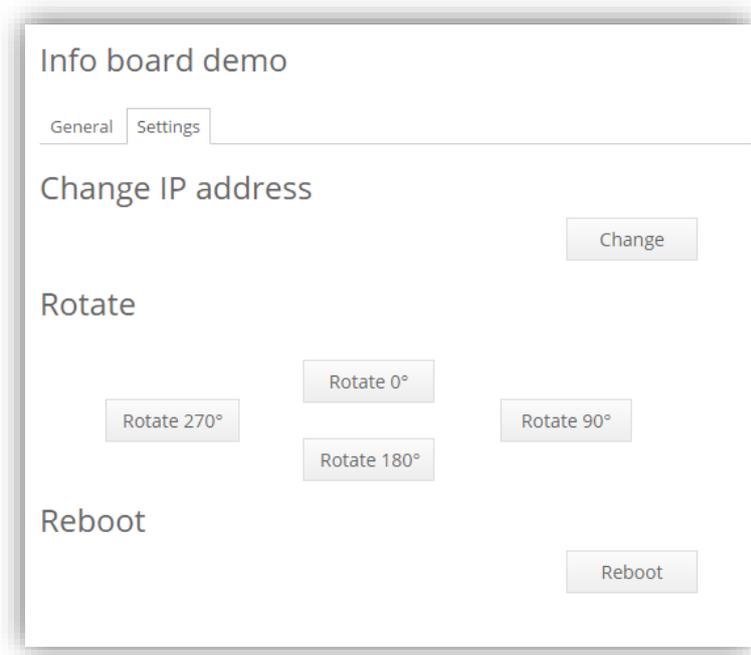


**Picture 16.1: List of info boards**

### 16.1.1 Info board driver settings

To access the settings of the info board driver, simply double click on the info board in the list or select it and navigate to **Menu > Edit [info board name]**. The general tab will open by default. Selecting the **Settings tab**, gives the next options:

- Change the info board IP address (make sure that the info board is located on the IP provided when added to the software).
  - Enter the new IP address.
  - Enter the subnet mask.
  - Enter the default gateway and press **Change** button to send the command.
- Rotate option:
  - Rotate 0° - For standard mounting.
  - Rotate 90° - Rotate the image for 90° CW.
  - Rotate 180° - Rotate the image upside down. Appropriate for ceiling mount.
  - Rotate 270° - Rotate the image for 270° CW.
- Reboot option- Sends a reboot command to the info board driver.

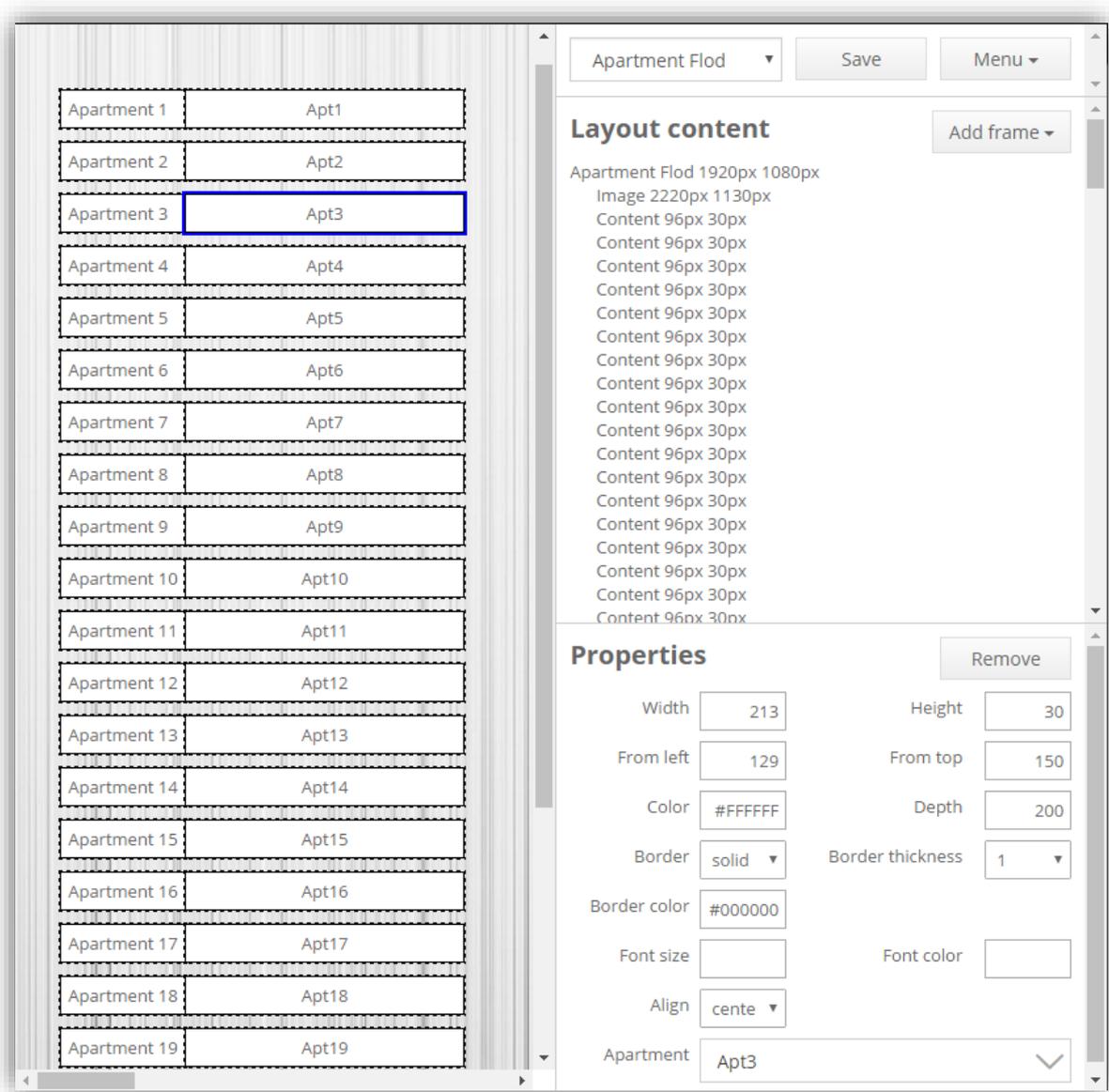


**Picture 16.2: Info board settings**

## 16.2 Info board layouts

Layouts are the web pages created in the Nova software. After creation, preview them in the browser before uploading them to info board.

To create a new layout, please navigate to **Menu > Manage Layouts** from Info Boards widget; a pop-up window will open with the canvas on the left side and the settings panel on the right.



**Picture 16.3: Info board layout example**

Description of panel sections:

- On the top, there is a text field with the layout name. Before creating a layout, please name it first.  
NOTE: To rename a layout, make sure that the first entry in the Layout content is selected – this will display the Name property that needs to be filled. Once there are multiple layouts created, it is possible to select a single one from the dropdown menu.
  - To close the pop-up window, navigate to **Menu > Close window**.
  - **Menu > Preview** will open a new web page that will show a preview of the created layout.
  - Removing a layout can be done by pressing **Menu > Remove [layout name]**.

- **Menu > Duplicate layout** will create a copy of the currently selected layout. This can be helpful if similar layouts are needed with different information.
- In the middle, a **Layout content** includes the list of items placed on the canvas.
  - Multiple frames can be added to the canvas. The following items can be chosen from, by clicking on **Add frame**:
    - **Content**: Most common item, that either can include a text or can be used as a background coloured object. To add/edit text to the content, please press the **Edit content** button. A new pop-up editor will open to freely edit the text font, size etc. Content can also display HTML code or video (Source code and Insert/edit video buttons).
    - **Image**: Adds an image from your computer.
    - **Iframe**: Enables display of web-pages that are enabled for Iframe like booking, videos... If the web-page is designed with the Iframe in mind, this is the best solution to implement it.
    - **Embed**: Enables adding embedded HTML code – used for YouTube videos (navigate to video and under it press Share and Embed tab; copy generated code to the text embed entry), Twitter (use external sites to generate a custom twitter feed that can be embedded into the info board) ...  
**IMPORTANT! Twitter videos do not support auto-play, so tweets that include GIF-s or videos will not play.**  
**IMPORTANT! High quality videos are really demanding and might not play smoothly. To fix the issue, please embed the video that plays lower resolution video. YouTube and other HTML5 videos might need some additional parameters like autoplay and loop to keep them going.**
    - **Apartment label**: When selected, an apartment can be assigned and the text from the apartment will be displayed the same way as it is on the Door stations or Mailboxes. The apartment text display format can be set under info board driver general settings.
    - **Message**: Local admin, Administrator and System administrator can all send messages to the info board, which will be displayed and updated in this frame.
    - **Slideshow**: Designed to display multiple frames in an endless loop. Each slide can have a custom timer assigned. By selecting Slideshow settings, slides can be added/removed/reordered.
    - **Copy selected**: Creates a copy of the currently selected frame. Very useful for creating multiple objects with the same content.
  - The first item is always the canvas. Clicking on it will bring different settings to the **Properties** panel – the layout name, its size in pixels (make sure to enter the resolution of the display that will be connected to the info board driver). You can also select the background colour.

Note: To remove any colour from the object, delete the text field contents and press Enter.

- Clicking on the different objects from the Layout content will select it on the canvas (blue border colour) and bring the object properties in the bottom panel – general settings:
  - **Width**: frame width.
  - **Height**: frame height.
  - **From left**: distance (in pixels) of the frame from the left side.

- **From top:** distance (in pixels) of frame from the top side.
  - **Colour:** colour of the frame (if text is empty, it is see-through).
  - **Depth:** determines which frames are displayed in front (frames with the highest number, will appear on top).
  - **Border:** border type – solid, dashed or dotted.
  - Border thickness.
  - Border colour.
- To remove a frame, select it from the **Layout content** and press the **Remove** button in the **Properties tab**.

Frames can be dragged and dropped anywhere on the layout. To access a frame that is covered with other frames, you can give those temporary lower Depth or you can just move them to the side, re-position the troubled frame and return the top frame to the previous position.

Note! When dealing with multiple frames, select them using the Ctrl key and click more frames into selection. Once selected, move all selected at once by moving them the same way.

Sometimes the frame cannot be moved due to its content (ex. Videos have click to start/stop and do not allow mouse drag). To move such frames, use the **From left** and **From top** properties.

Note! Some property fields can be increased or decreased by clicking on them and pressing the up/down arrows. A single press on the up arrow on keyboard will increase the current field by 10; this also works when selecting multiple frames – it is good for increasing width or height of selected objects.

When done editing, press **Save** button and close the layout pop-up.

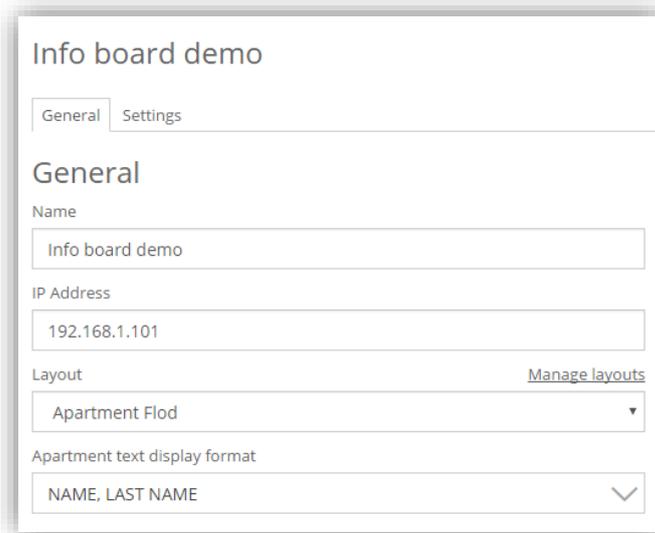


**Picture 16.4: Info board layout preview**

## 16.3 Assigning layouts to info board drivers

To select which layout will be displayed on the info board, navigate to **Home > Hardware > Info Boards** widget and double click on the wanted widget. From here, select the Layout to display from the dropdown menu. If there are any apartments set on the active layout, also choose the appropriate display format. Once all is set, it is possible to:

- Preview the currently assigned layout: **Menu > Preview.**
- Upload the layout to the info board by pressing **Menu > Update display.**



The screenshot shows a web interface for configuring an info board. At the top, it says "Info board demo". Below that are two tabs: "General" (selected) and "Settings". Under the "General" tab, there are four main sections: "Name" with a text input field containing "Info board demo"; "IP Address" with a text input field containing "192.168.1.101"; "Layout" with a dropdown menu showing "Apartment Flod" and a "Manage layouts" link to its right; and "Apartment text display format" with a dropdown menu showing "NAME, LAST NAME".

**Picture 16.5: Info board General settings**

## 16.4 Sending message to info board driver

Along with the info board widget, a **Messages** widget becomes visible too. Navigate to **Home > Messages.**

To create a new message press Menu > New info board message.

Click on the **To:** label in order to display available info boards, select the correct info board from the dropdown menu, provide a Title for your message (only displayed in the software and not on the info board) and create a new message that can include text, picture or a video.

Once done with message creation, click the button to preview it on the info board. This will open layout from the selected info board and put the message inside the **Message** frame (if it exists) and open a preview page in another window. If satisfied with the result, close the preview window and send the message. The display should update with the new message after a couple of seconds.

## 17 Module: High security module

This module makes some software changes, that improves overall security. To activate this key, please follow the instruction in chapter 6.1 Add-ons and Modules.

By entering this module, new section: **Security settings** and **Reader encryption** will be displayed in the Other Settings menu.

Enable HTTPS redirect

Centrals with hardware version 3.0 support HTTPS access by default. Navigation on HTTP protocol is unsecure – the data between the computer and the central can be monitored by someone else on the network. Using HTTPS protocol (**https://<central-IP>**) will create a secure handshake with the target central. After the handshake is done, the connection will be encrypted.

**NOTE:** When accessing the webpage via HTTPS, the browser will report that the site is untrusted due to the self-signed certificates that are provided by the central. The site can still be accessed by putting the site to ignore list – the connection is encrypted, but there is no way to check if the target recipient is actually the central or not. To avoid the browser warning, the custom certificates need to be uploaded to the central for unique and secure connection. Details are better described in the chapter 17.1 Uploading custom certificates.

In the **Other Settings**, there is an option under **Security settings** to redirect all traffic from HTTP to HTTPS. After this setting is set, anyone who wishes to access the central via unsecure connection, will be automatically redirected to a secure one.

### Disable web server port on slave centrals

Access on all slave centrals is usually read-only, but to increase security, we can disable the GUI access on all slave centrals at once. The software must be at least version 2.1 installed on all centrals for this feature to work. If the central is reset to defaults, the GUI becomes accessible again. Adding new centrals into the system while having this option enabled, will automatically disable access to that central's GUI.

### PIN changes

The PIN codes are hidden from all users for security purposes.

Additionally, **PIN only access can be DISABLED**, Card + PIN and PIN + Card combination require **PIN length can be set to require at least 4 numbers**.

Due to the security reasons, if the PIN on reader is entered incorrectly, it won't be displayed at the event.

Entering the faulty PIN multiple (5) times, the reader will report a faulty pin even if it's entered correctly until the end of the time period (1 minute).

Password changes

The system will require password length of at least 8 characters. Additionally, password cannot contain more than 2 repeated characters and cannot include sequential numbers or characters (ex. **111OX12** – not suitable, **AgEf432** is not suitable, **65gbcA539** is also not suitable).

Idle log-outs

If this option is checked, the account type: **system administrator** will be automatically logged out of the system after 10 minutes of inactivity. The timer is not active if the GUI is opened on **Events** or **Floor plan** page (for monitoring reasons).

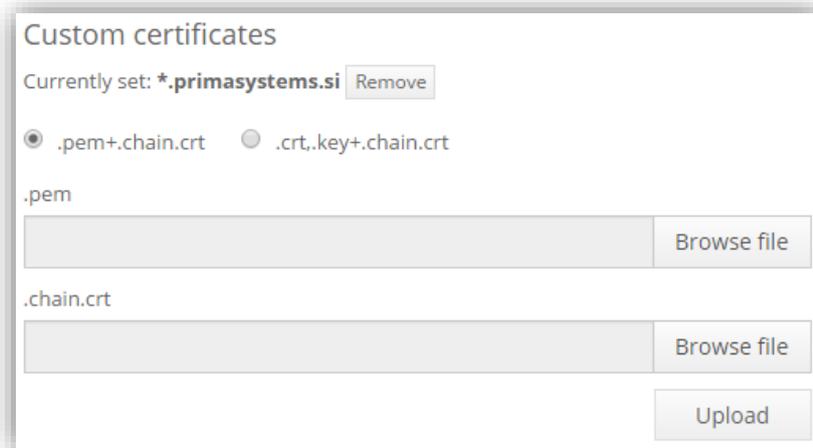
Reader encryption

This option enables encryption on the wire between the central and the reader. Enabling this option will result in reader working a bit slower, but more secure.

## 17.1 Uploading custom certificates

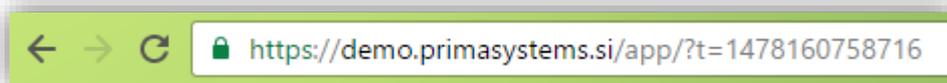
The option allows custom certificates to be uploaded to the master central and creates a correct introduction when accessing the application. To upload personal certificates, navigate to **Home > Settings > Other Settings**. There is the option to upload multiple files. Please select all the files you have regarding certificates. The software will extract the needed information and use it to provide a secure access to the central. The custom certificates will replace the self-signed ones and ensure a secure connection to the master central.

After certificates are uploaded, the URL of the safe access will be displayed, along with the currently set common name (as shown on Picture 17.1).



**Picture 17.1: The uploaded certificates provide a secure connection to the top master central**

Central access should now be displayed with the secure connection icon:



**Picture 17.2: Secure connection to the site (top master)**

## 17.2 Custom certificates removal

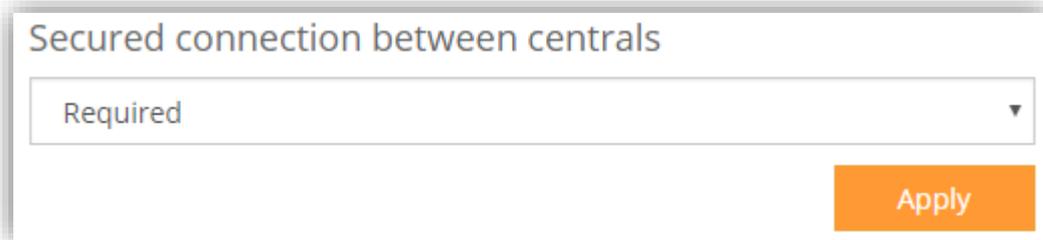
If we do not wish to keep the personal certificates on the central, they can be deleted with the press of the **Remove** button as displayed on Picture 17.1.

After the certificates are deleted, the centrals will continue to work using the default self-signed certificates.

**IMPORTANT!** Central reset (the left button held for more than 20 seconds) will also delete personal certificates and continue to use the self-signed ones.

## 17.3 Providing a secure connection between centrals

Module allows option for a **Required** secure connection between the centrals. This ensures that there are no plain connections between the centrals. The connection uses a secure protocol TLS 1.2.



The image shows a configuration window with the title "Secured connection between centrals". Inside the window, there is a dropdown menu currently displaying the word "Required". To the right of the dropdown menu is an orange button with the text "Apply".

**Picture 17.3: The option to ensure encrypted connections only!**

**IMPORTANT!** Centrals with hardware version less than 3.0 do not support secure connections, so this option cannot be set until they are removed from the system.

## 18 Module: Fire alarm module

The fire alarm module supports the connection of one or more external alarm unit(s) to one or multiple centrals in the system. To activate this part of software, please follow the instruction in chapter **6.1 Add-ons and Modules**.

**IMPORTANT!** All centrals in the system must have software version 2.1 or higher for this module to work correctly.

**IMPORTANT!** The alarm contact needs to be connected to general Input 2 and one of the settings below needs to be selected on the corresponding central in GUI.

To access the Alarm settings, please navigate to **Home > Hardware > Centrals > Edit central > Auxiliary I/O tab > Input 2**. In order for the alarm to be triggered, the Active voltage level should be set on NC (default) or NO.

### 18.1 Setting up alarm to affect only one central

This option is free and allows alarm to manage doors connected to that central. If the alarm is triggered, the alarm will unlock all doors on this central. Once the alarm is over, all doors will be locked.

### 18.2 Setting up global alarm

Setting this will unlock all doors in the system when the alarm is triggered and then lock them when the alarm is turned off.

**NOTE:** Doors that were previously unlocked – manually or by schedule will lock once the alarm is over.

### 18.3 Setting up custom alarm

Advanced setting that allows creating a new, special Alarm action access group with custom settings for the beginning and the end of the alarm time frame.

To create a custom alarm group, please navigate to **Home > Users & Access rights > Access groups**, and create a new group with the **Alarm action** as an access group type. The access group is assigned similarly as a standard access group with some limitations (the time is always 0-24 and actions can be set to: Lock, Unlock, Block, Unblock, None). Along with the Action, custom events can also be triggered if the scripting module is applied in the system. More about the scripting module can be read in chapter 7 Module: Scripting.

Once the access groups are created and configured, they can be selected in the alarm's dropdown menu as shown in the Picture 18.1.

**Input 2 - Settings**

Active voltage level

NC

**Alarm - Settings**

 **DISCLAIMER:** The alarm function is not a reliable source of safety. It is meant to be used only as a support option to help in case of emergency. Use it at your own responsibility and risk.  
The access control equipment is not approved in relation to fire regulations and fire norms as well as the installation itself can be made so it does not fulfil local fire protection requirements.

I've read the disclaimer and I'm aware of the deficiency of the set alarm

Alarm function

Alarm action access group

Action on start of alarm

Alarm START

Action on end of alarm

Alarm END

**Picture 18.1: Custom alarm with a start/end groups assigned**

## 19 Module: Checkpoint

Checkpoint module supports card checks for secure facilities such as airports. There are two (2) ways to check the cards – a **stationary checkpoints**, where a guard can check cards of users that pass by via predefined reader(s) or **mobile checkpoints** that allow guards with a designated mobile device to scan cards on the field.

To activate this part of software, please follow the instruction in chapter **6.1 Add-ons and Modules**.

**IMPORTANT!** Master central has to be upgraded with the package version 2.3 or higher for these functionalities.

Firstly, we need to set-up **Checkpoint user(s)**. To read more about user account types and how to assign them, please read 1.1.1 Account types.

### 19.1 Setting up stationary checkpoint

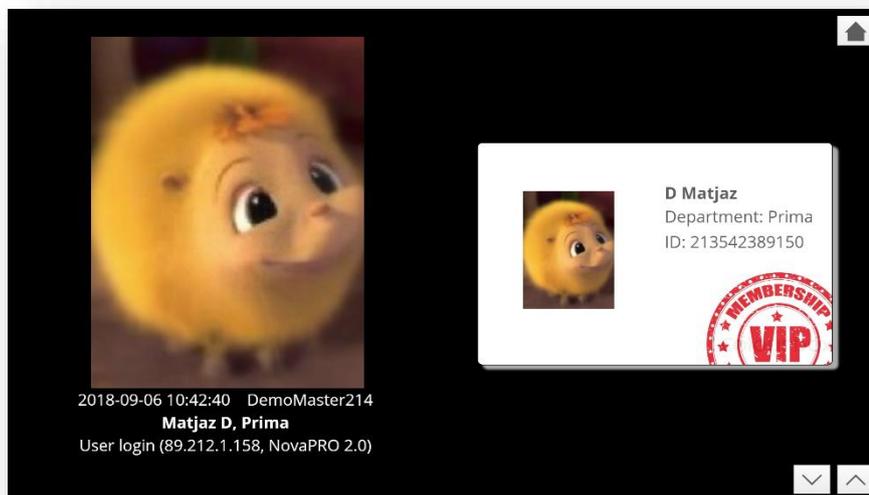
Once the users are created, navigate to **Settings > Checkpoint settings**.

On the top select the checkpoint user and fill out which events show as "OK" and which ones as "Error". You can also assign sounds to any event you've selected by pressing on the "Play button".

When the guard logs in, he can see the checkpoint widget.

When opened, the screen is black until one of the set events occur.

At that time, the layout selected at Default card print layout (can be changed at user's general settings) will be displayed.



**Picture 19.1: User's card layout displayed on the screen**

Picture 19.1 shows a checkpoint preview.

There are 3 buttons:

- The home button, that navigates back to Nova
- The up/down buttons that allows us to go through card history.

**NOTE:** Card history is limited to 50 cards max and the cards are stored only for 10 minutes!

In case of "Error" event type occurs, the text from Other settings on the bottom will be displayed instead of the card. Additionally, you can select a different layout and text if the card is unknown.

## 19.2 Setting up mobile checkpoint

After the checkpoint users are created, the special android app has to be installed on the devices capable of reading RFID cards.

After opening the app, the guard will have to login by showing their own card + PIN. The mobile app can only detect if the card is lost, unknown, deleted, expired or unknown card type (unauthorized or any of the offline cards).

**NOTE:** In the app, the person responsible has to set-up the IP of the top master central. These settings are locked behind set PIN, so the normal user doesn't have access to them.

## 20 Special hardware

### 20.1 Elevator controller

The elevator controller is based on the regular Alpha central and has support for controlling access for up to ten floors by activating only those floor buttons in the elevator to which the user has access.

#### 20.1.1 Elevator reader setup

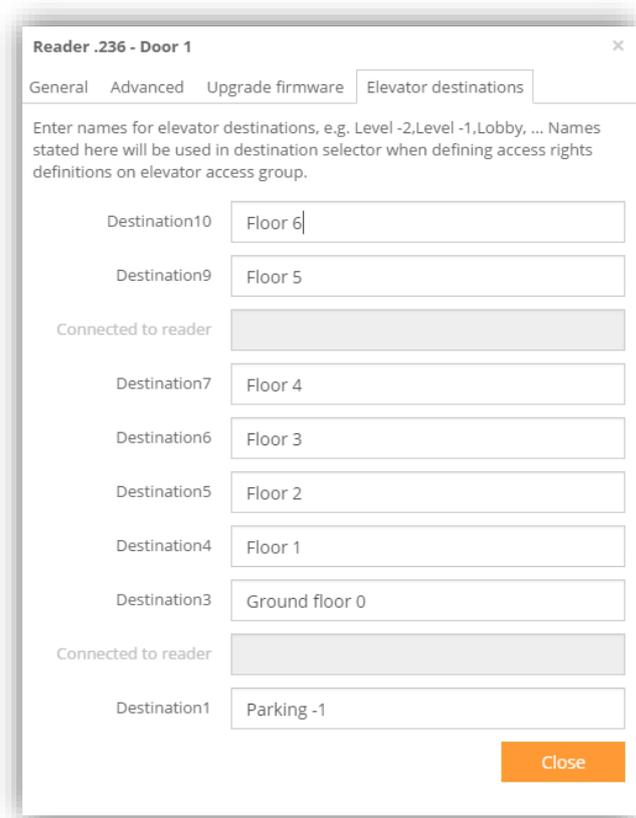
- The reader has to be installed on **Door 1** on the Elevator controller.
- Reader and Door 1 settings are applicable in the same way as for a normal reader.
- Please see section on setting up RFID reader for more information.

**NOTE:** Only difference is that **Electric lock open time** setting for Door 1 is controlling how long the elevator buttons are enabled.

**IMPORTANT!** In cases where the central is controlling less than 10 floors, unused outputs can be used for normal access control with additional readers connected to Door 2, Door 3 or Door 4.

#### 20.1.2 Setting up elevator destinations

To set-up elevator destination, navigate to reader settings (described in chapter **5.1.15 Reader settings**) and enter the desired destinations (an example is displayed on Picture 20.1).



**Picture 20.1: Elevator destinations**

### 20.1.3 Setting up access groups and access rights

- Users need to be assigned with **special access groups** defining which floor should be activated when the elevator is used.
- A **special access group** is created in the same way as a normal access group. Here you create a new access definition of the elevator reader and select desired **schedule, Id device** and **floors**.
- Action has to be set to **None** (Picture 20.2).

**NOTE:** New access groups must be created for each different combination of floors.

**Edit access group First Floor access**

Name: First Floor access

Access group type: Normal

Description: Description

Add access right to .236 - Door 1

Schedule: 0-24h [Manage schedules](#)

Action:  Open  Lock  Unlock  Toggle  None

Id device:  Any  Card  PIN  Card + PIN  PIN + Card  2nd Card Read

Destinations:  Parking -1  Ground floor 0  Floor 1  Floor 2  Floor 3  Floor 4  Floor 5  Floor 6

Buttons: Save, Add, Back

**Picture 20.2: Access definition for floors -1, 0 and 1.**

## 20.2 FireAlpha

FireAlpha is a stand-alone central that serves to ping devices on the RS485 bus. It contains its own graphical user interface to manage the connected devices from a pre-determined list.

Detailed FireAlpha manual is in a separate file. Please contact the support that can be found on Prima's webpage.

## 20.3 Parking controller

The Parking controller is a stand-alone central that manages parking garages entry/exits.

Detailed manual is written in a separate file. Please contact the support that can be found on Prima's webpage.

## 20.4 Nexus MO

Nexus MO is a stand-alone hardware that supports the connection of up to **two readers**. It needs to be programmed the same way as the offline readers are programmed. You can read more on programming offline readers in chapter 5.2 Offline readers.

There are no special readers for this hardware – meaning the readers from Alpha central can be connected to Nexus MO and the other way around.

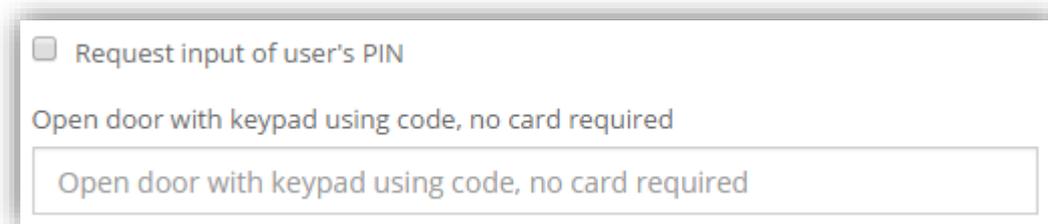
### 20.4.1 Upgrading Nexus MO readers

1. Disconnect reader(s) from the Nexus MO.
2. Connect them to port on a central.
3. Run a search and add them to the system.
4. Double click on it and navigate to tab **Upgrade firmware**.
5. Press the button **Upgrade firmware** and find the upgrade software on your PC.
6. After the upgrade is done, the readers can be removed from the software and connected back to Nexus MO.
7. Reboot the Nexus MO to detect the readers.

**NOTE:** Nexus MO only detects readers at its boot. Connected readers after boot will not be recognized. Please press the reboot button to start the initial search again.

### 20.4.2 Nexus MO PIN

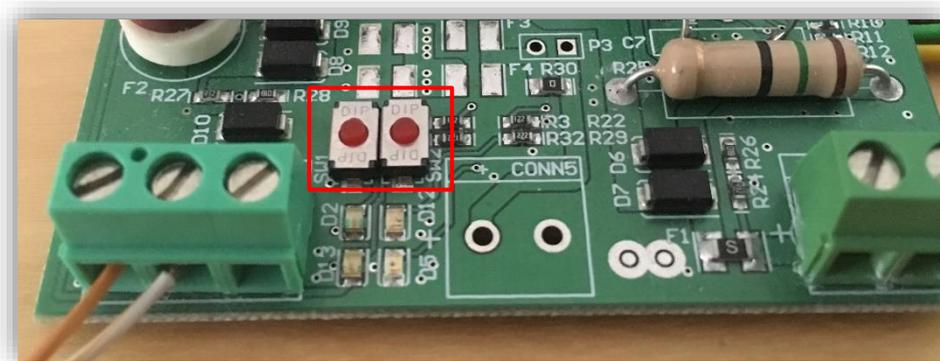
When changing the configuration of different offline types, when we select **Offline Nexus reader**, we are presented with the option to request user's PIN or we have an option to enter with a shared PIN.



Picture 20.3: Nexus MO additional PIN settings

### 20.4.3 On-board buttons

Next to the power connectors, there are two buttons like there are on the central. Pressing the left one will reset the board. By pressing and holding the right one until the LED starts blinking faster will reset all settings (the board needs to be re-programmed).



Picture 20.4: Nexus MO on-board buttons

#### 20.4.4 Upgrading older systems with new firmware

Older version of Nexus MO can be upgraded to the latest version, but during the procedure, all data will be lost, so after the upgrade is done, it needs to be re-programmed.

To update **old reader** software, a RS485 connection must be made from PC to reader. At reader boot, it expects a new firmware for a couple of seconds. It needs to be provided with the flashing tool. If the time window is missed, reader needs to be rebooted and the process repeated.

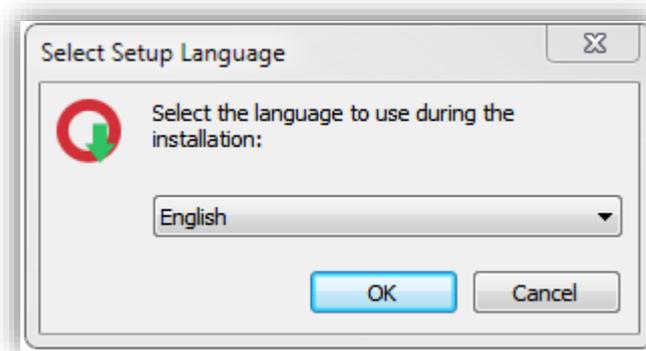
Updating the **old board** with the new software is similar to upgrading readers. The connection must be established with the PC via RS485 cable and the flashing tool needs to be used in a first couple of seconds to upload new software.

## 20.5 USB desktop reader

- **Overview:** USB Desktop Reader consists of reader and companion software application. Reader is connected to PC with USB connector.
- **LED Status:** In normal operation red LED is lit on reader and red LED and green LED are blinking on the USB connector signaling ongoing communication between application and reader. When new card is read, red LED on reader blinks and short beep is produced. When card is accessed for read/write operations, short beeping sound is produced.
- **System Requirements:**  
Windows XP/7/8/8.1/10 with .NET 4.0 installed  
USB 2.0 Port,  
Internet connection
- **Safety:** In order to ensure the safe operation of the device and its users, please read and act in accordance with the following safety instructions.  
USB Desktop Reader is designed for indoor use only; do not place it outdoors. Do not place the USB Desktop Reader in or near hot/humid places, such as a kitchen or bathroom.  
Please keep the USB Desktop Reader out of reach of children.  
There are no user-serviceable parts inside the USB Desktop Reader. If you experience problems, please contact your dealer of purchase and ask for help.  
The USB Desktop Reader is an electrical device and as such, if it becomes wet for any reason, stop using it immediately.

## 20.5.1 Installation

1. Turn on your computer and **plug in USB Desktop Reader** into an available USB port on your computer. Never use force to insert USB connector.
  2. **Wait for Windows to detect inserted device** and that required drivers are installed. **This procedure can take some time**, as Windows may contact update servers to download required files.
  3. Download the installation file **USB Desktop Reader Setup <version>.exe**.
  4. Double click USB Desktop Reader Setup <version>.exe **setup application** and follow next installation steps:
- Select desired **language** you wish to use during installation of the USB Desktop Reader.



**Picture 20.5: USB Desktop Reader language selection**

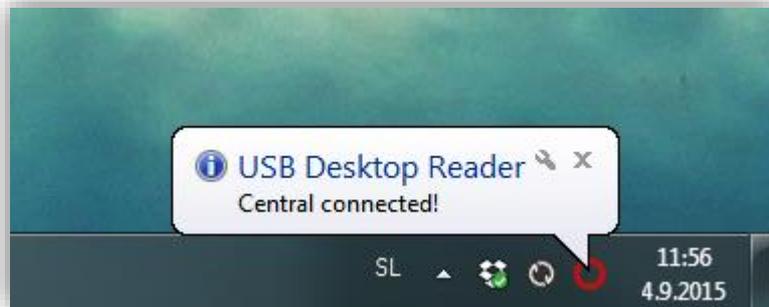
- The next screen welcomes you in **setup wizard**. You can proceed with setup process or you can cancel it by clicking on *Cancel* button. Click *Next* button to proceed with installation.
- Select desired installation location. It is recommended to use the default location.
- Select Start Menu folder name. Under this folder you will later access installed application.
- Select if you wish to create desktop icon.
- The next screen displays setup summary information, please read it carefully and click *Install* when you are ready to continue. If you have an older version of the software installed on your computer, it will be closed before installation.
- When installation process is finished, you will be able to run USB Desktop Reader on your PC. Click *Finish* to close setup wizard.

## 20.5.2 Using USB Desktop Reader

### Starting application

**IMPORTANT!** In order to use USB Desktop Reader, host central needs to be running SysFCGI version 1.7.172 or greater. You can check installed version on central's user interface under Settings in Advanced tab, next to the Upgrade software button. You may need to upgrade central to the latest firmware if SysFCGI version is not correct.

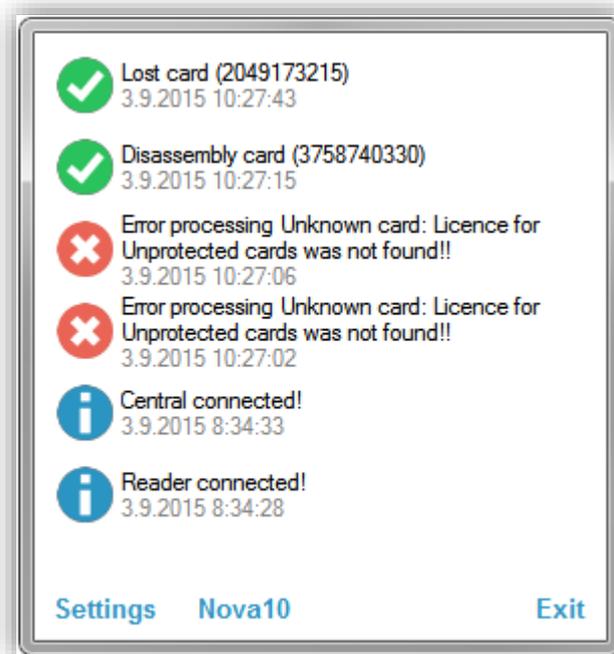
Start USB Desktop Reader application by double clicking on desktop shortcut or click on Windows start menu and selecting USB Desktop Reader shortcut under USB Desktop Reader folder (*shortcuts may not be available if you have decided not to create them during installation process*). USB Desktop Reader will start in system tray where it can be accessed by clicking on its icon. If icon is not visible, you can click the *up arrow* on the left side of the system tray and rearrange USB Desktop reader icon by dragging it to the desired location on system tray.



**Picture 20.6: USB Desktop Reader software running in the system tray**

### USB Desktop Reader settings

Mouse click on USB Desktop Reader icon will open main application window with six latest events and access to application settings and connected central.

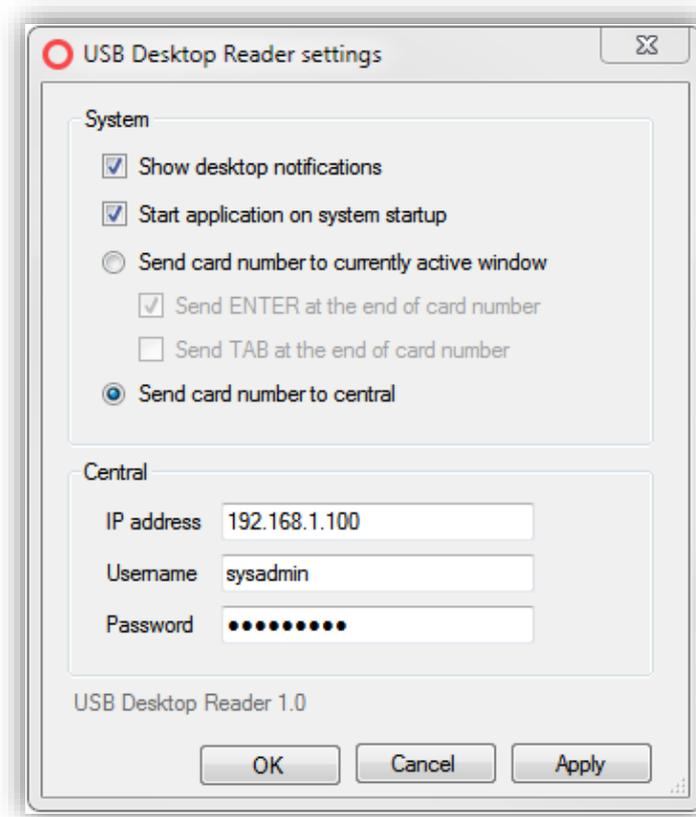


**Picture 20.7: USB Desktop Reader log**

Click on *Settings* will open application settings where you can change system and central related settings.

Under *System* section desktop notification balloons can be enabled or turned off. When desktop notifications are enabled, balloon messages will show status of all card related operations and system state changes (disconnected reader, ...).

When option *Start application on system startup* is selected, USB Desktop Reader will automatically start whenever PC is turned on.



**Picture 20.8: USB Desktop Reader settings**

### **USB Desktop Reader can be run in two different modes:**

- When option *Send card number to currently active window* is selected, application will send read card number to opened application that has focus (*this mode is useful if you need to create list of user cards in Excel spreadsheet*). In this mode you can also select if card number is combined with ENTER or TAB key press.
- If option *Send card number to central* is selected, then read card number is send to the central and card is treated in the same way as it would be on an online reader.

For second option valid central IP address, username and password needs to be entered under applicable fields in *Central* section of the settings window.

When you have edited application settings you can close settings window by clicking on the *OK* button or you can apply new settings with the click on the *Apply* button. If you wish to discard changes, you can click on the *Close* button to close the settings window.

### **Exiting application**

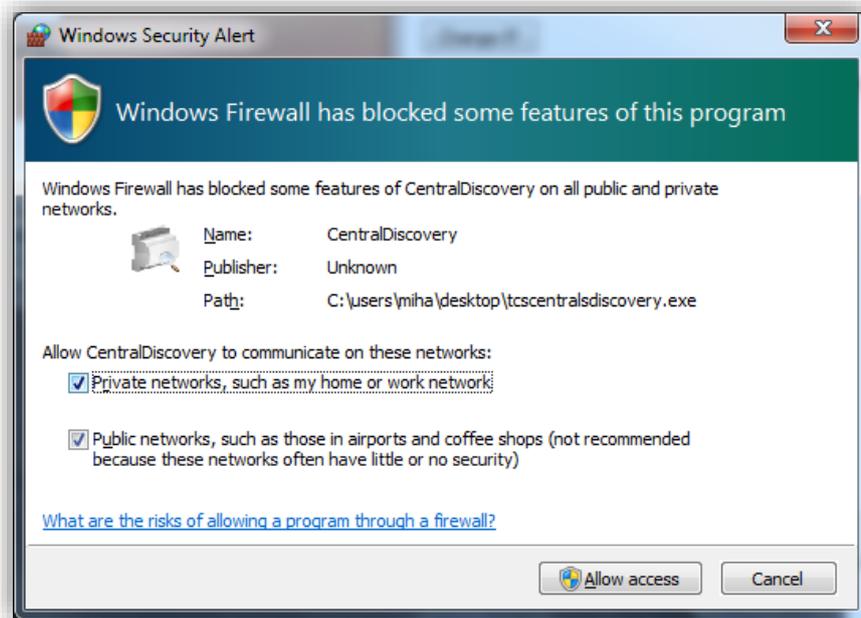
You can close USB Desktop Reader application by clicking on the *Exit* label in main application window or by right clicking on application icon in system tray and selecting menu option Exit.

## 21 Central discovery tool

This tool allows installers to manage all centrals connected to the local network. This software can be found and downloaded from Prima's webpage.

After downloading the software:

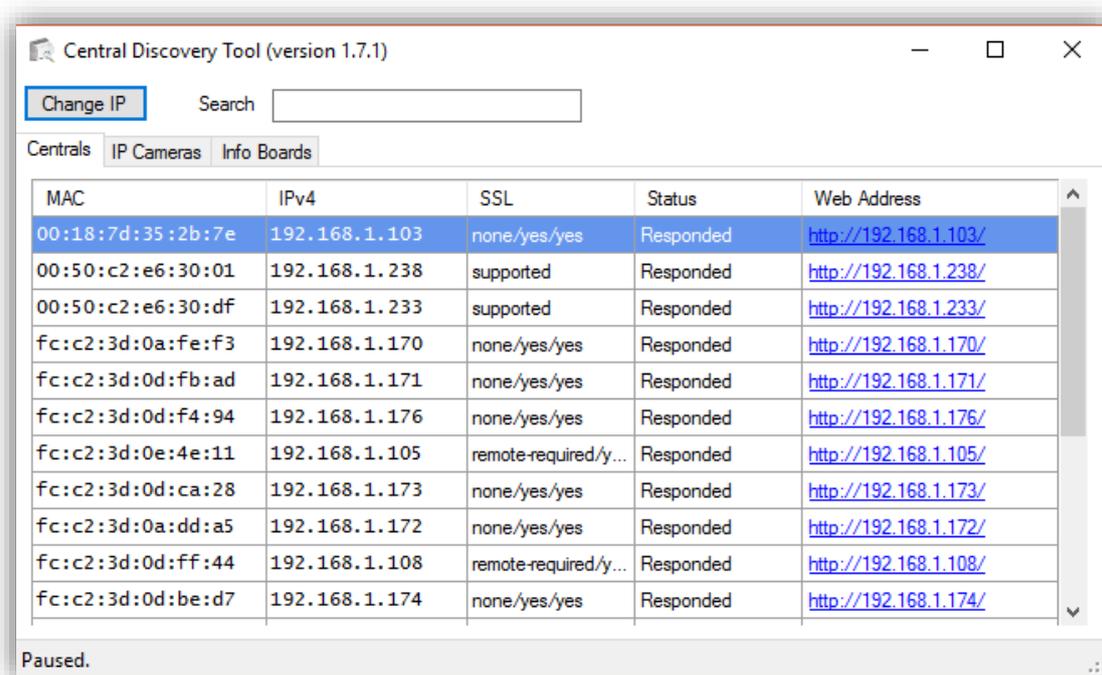
1. Open it
2. Both checkmarks must be checked and the tool must be allowed access to the network in the Firewall enable window (Picture 21.1)



**Picture 21.1: Allowing access to the tool beyond the firewall**

From the main window (Picture 21.2) the MAC and IP address are visible for the corresponding centrals.

- Here it is possible to navigate to the central web page by clicking on the active link in the **Web Address** column.
- Changing the IP of the central is only available from the default IP (192.168.1.100) address.
  - This prevents any unwanted changes outside the system. If the central is reset, its IP changes to the default address. See the explanation of central reset in chapter 23.



**Picture 21.2: Central discovery tool main page**

- This tool scans the network for any new central every few seconds.
  - In case a central fail to respond due to IP change or network error, its entire row will turn red and its status will show **'No response'**.
    - This is extremely helpful to determine if there are any problems on the local network.

### Search function

The search box on the top applies a filter to display centrals only in specific network or just a simple search for central IP or MAC address.

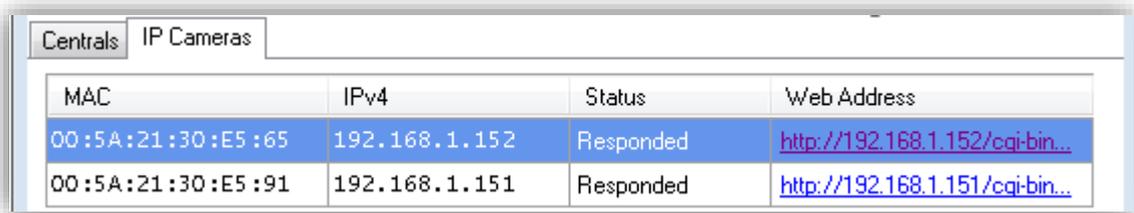
### SSL support

This column reports if the central is capable of connecting via secure SSL connection. Centrals with **old hardware do not support SSL!** The SSL options:

- Not supported
- **Supported** – the old way of reporting SSL capable connection
- Mode / Require peer certificate / Strict certificate check
  - **Mode:** The current SSL mode the central is set on (required, optional, optional+, none)
  - **Require peer certificate:** (yes/no) if the central presents and requires connection with a certificate.
  - **Strict certificate check:** (yes/no) checks the contents of the certificates and revokes the connection if the certificate is unfamiliar.

## IP cameras

For the system with IP cameras on the network, there is an **IP Cameras** tab.



MAC	IPv4	Status	Web Address
00:5A:21:30:E5:65	192.168.1.152	Responded	<a href="http://192.168.1.152/cgi-bin...">http://192.168.1.152/cgi-bin...</a>
00:5A:21:30:E5:91	192.168.1.151	Responded	<a href="http://192.168.1.151/cgi-bin...">http://192.168.1.151/cgi-bin...</a>

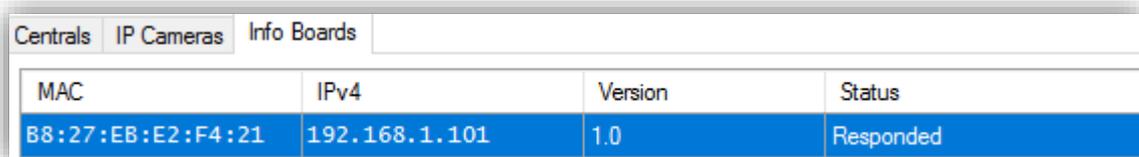
**Picture 21.3: Display of IP cameras on the network**

Contrary to the centrals, IP addresses of the cameras can be changed anytime to any address by:

- Clicking on the **Web Address** of the IP camera
  - A new web page containing net settings will be displayed, confirming that the camera is up and running.

Prior to setting up IP Cameras in the system, please make sure that the camera is compatible with the Nova software.

## Info boards



MAC	IPv4	Version	Status
B8:27:EB:E2:F4:21	192.168.1.101	1.0	Responded

The tool also finds the Info boards connected on the same network. Moreover, it allows changing the network settings to the found info board.

**NOTE:** The discovery and search tool work the same as the one for centrals.

**ATTENTION!** Central discovery uses UDP (User Datagram Protocol) packets, which means that the discovery will display all centrals from local network (for centrals with Nova version 1.4 and lower) and the centrals from other sub-networks (if the router/access point allows it and the software on centrals is **version 1.5 or higher**).

**IMPORTANT!** This tool does not need to be installed. It was designed to run on any version of Windows OS. Different OS systems can also run the tool via emulation software.

## 22 FAQ

### **Difference between the physical IP address of a central and the IP address, on which the central is visible**

If all centrals are inside the same LAN, every central can be connected to another central by registering the IP address of the other central. This IP address is the physical address of the central and can be changed in the **Central Settings** (see chapter 5.1.5 – Settings section). This address is the address where the central is visible to other centrals. If all centrals are in the same LAN, the physical address is also the visible address. The visible address is the address, which can be set in the **Central Settings** (Picture 5.9).

If any central in the LAN should be connected to a central located in a remote LAN, the address of the remote LAN must be identified. Routers control the communication between two different LANs, and if a message is sent from a central in one LAN to a central in another LAN, it is first sent to the router of the other LAN, which then sends it to the central. In the latter case the router address becomes the visible address of the central in the other LAN (and is set in the **Central editor**).

A central in a remote LAN still has its own physical address, which is needed for message delivery. This physical address can be changed in **Manage Centrals (5.1.1 Searching and managing centrals in Local Area Network (LAN))** popup window.

The warning message in Picture 22.1 shows on the main page. It is displayed, if the physical address of the central is on 192.168.1.100. The best way to properly set the system is to set the central database IP to 192.168.1.[any other number between 1 and 255 excluding 100] – with database update. If the central interface IP needs to be changed, repeat the process setting the new interface IP without database update.



**Picture 22.1: Default IP warning message**

### **RS-485 BUS between Alpha centrals - Capacity and rules**

On the RS-485 BUS, the bandwidth available for replication is greatly reduced compared to Ethernet. The RS-485 communication is also much slower because the communication can only take place from one central to another at the time, where Ethernet allows many centrals to communicate all the time. This means that the limit of maximum 10 slave centrals connected to a 'RS-485 master central' on one RS-485 BUS is pre-set. Replication over a RS-485 BUS can handle up to 750 door openings per hour (3.000 events).

This amounts to up to 300 door openings per minute between centrals connected over TCP/IP connection run on Alpha centrals – if more capacity is needed the Nova software should be placed on a Linux server with more processing power which basically is a NovaServer version, which includes the server.

When the system is running, the slave centrals send their events to the master, but receive no events back from the master or any other centrals in the system except if an

event concerns a function on the slave central – e.g. an event generated on another central should open a relay on the central. So regarding the slaves, most of the communication is one-way and means that the slaves have no back-up of events in the system, but only contain its local events and the settings for the system (users, access groups, etc.).

The 'RS-485 master central' receives all events from its 'RS-485 slaves', which it replicates to all other Alpha centrals in the access control system that are on Ethernet. It also sends all settings to the 'RS-485 slaves' as well as events which shall activate a function on a 'RS-485 slave'.

A system where centrals are on RS-485 BUS should not contain more than 1.000 users due to the time it takes to upload them and distribute the information to all centrals. It takes approximately 3 minutes per central on a RS485 BUS, which means that it takes 30 minutes for 10 centrals connected on one RS-485 BUS. This can be important under commissioning or for systems where there are many changes to the settings.

Port forwarding for remote central on fixed IP address

Here, two possible cases can occur:

- First case is when master central needs to communicate with the slave central in another network.
- The other case is when wanting to access publicly available Nova application through browser.

In the first case, when the master needs to access remote slave central, one port needs to be forwarded on remote router. Usually port number 3543 on the remote router (number is configurable under advanced settings of the remote central) needs to be forwarded to internal port 3543 on the slave central (not configurable). Through this port, the master central (or the local master central) sends the database to slaves.

In the second case, port 80 (which is used as the default port for all HTTP traffic) on the router needs to be routed to port 80 on the central serving Nova application.

If using a domain name (dynamic DNS service or custom domain name) instead of an IP number, that domain name is connected only to the IP address and all port settings remain the same.

### **What happens in case of replicator overload?**

If the system generates more than approximately 3.000 events per hour on a RS-485 BUS it builds up a backlog. This means that events are lined up in a queue and not reported instantly. In many cases this does not matter as the local centrals continue to work normally, so users will not notice any difference. However, in systems where an event (e.g. an input) on one central should release a function on another (e.g. an output) it can cause the event to be delayed when registered in the queue. A built-up backlog of events will be phased out in the minutes afterwards if the number of events gets fewer than 50 per minute (approximately 12 door openings). If the backlog only builds up and up the system will stop working.

A 'RS-485 slave central' is not affected locally by a replicator backlog. It will continue to operate according to the memory settings: doors will be opened for users, period validation and access rights to offline readers will be written to users' cards, etc.

### **Capabilities of RS-485 system**

A system with RS-485 BUS between the centrals can be set up in three ways:

1. One master central connected directly to a PC and with up to 10 slave centrals connected on the RS-485 BUS.
2. One master central on TCP/IP connection and with up to 10 slave centrals connected on the RS-485 BUS.
3. Several 'RS-485 master centrals' on TCP/IP – all part of the same big access control system – and each has up to 10 RS-485 centrals connected on the local RS-485 BUS.

The rule of max 10 centrals on an RS-485 BUS and max 1.000 users in an access control system with centrals on RS-485 BUS is as a guideline, which in some cases can be adapted to local circumstances. If a system has few users and few events, it is possible to have more centrals on the BUS and it will work well.

The same goes for more than 1.000 users in an access control system, where it is only possible to have few slave centrals on a separate RS-485 BUS.

On the opposite side, it is possible to have a system with 500 users, but with many events and changes to the users. In this case, it might be unsuitable to install any centrals on RS-485 BUS.

On the 'RS-485 slaves' read/write readers can be installed to be used as update readers for period validation and access rights for offline readers. Input on the centrals can also be used to generate outputs on other. The RS-485 does not limit these possibilities.

Which memory sectors are used on MIFARE cards by offline system?

User cards use sectors 5 – 9 (4 sectors) and 10 - 12 (3 sectors) by default. The starting sector for the access rights segment is configurable. It is currently the 5<sup>th</sup> sector, followed by 4 consecutive sectors. The starting sector for the feedback segment is also configurable. By default, the segment starts at the 10<sup>th</sup> sector followed by 2 consecutive sectors. All sectors are protected by unique authentication keys.

Usage of cards in other applications

Configuration cards for offline readers should not be shared between different applications and are linked only to our system. User cards are usable for other applications as long as the other applications use 'free' sectors on cards.

How is a user informed about low battery level on offline reader?

The user is informed by the device (with delay, red LED, etc.) as well as by software reports of battery status, when Offline+ activation key is used and user feedback (events on user card) is enabled. If the battery status is low, it can be found between Errors on Home screen. In the settings for every offline reader there is a Remarks box to note date of last battery change.

### **How to replace existing or add new central to the existing system**

When adding a new central or replacing some centrals in the existing system, follow these instructions:

1. Disconnect faulty central from the system if applicable.
2. Login to master central and add new slave central to the system or edit existing slave MAC address with the MAC address of the new slave central. The MAC address of the central is written on the central side label.
3. Reset new slave centrals to default, so there is no old data on it (it might be an old master and will try to connect to some centrals, etc...).
4. Login to Nova application (NovaSimpli when reset to default) using default credentials and change central IP address to the new value, which is set on master central.
5. Connect slave central to network. Master central will connect to it and update slave central configuration.

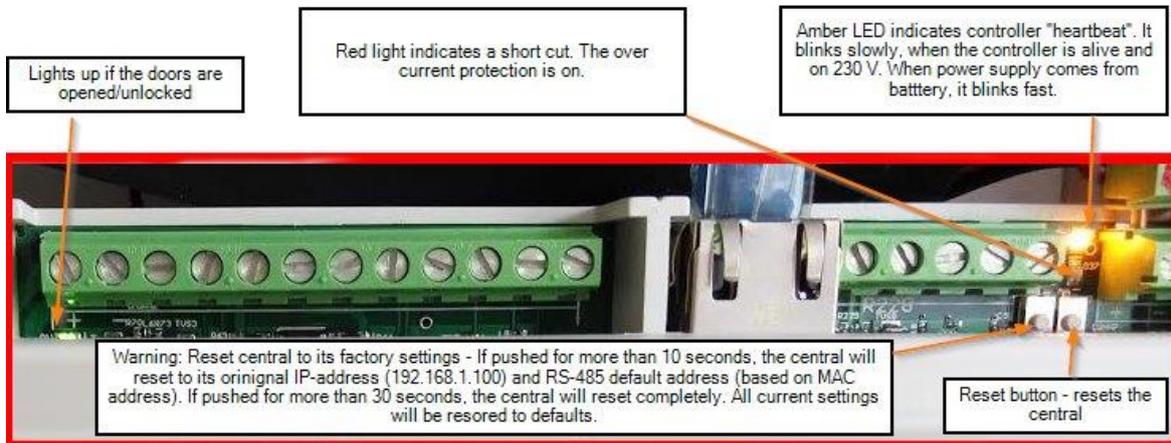
The replacement of master central is described in chapter 5.1.7 Replacement of malfunctioning master central.

### **How many cards are stored on the blacklist card?**

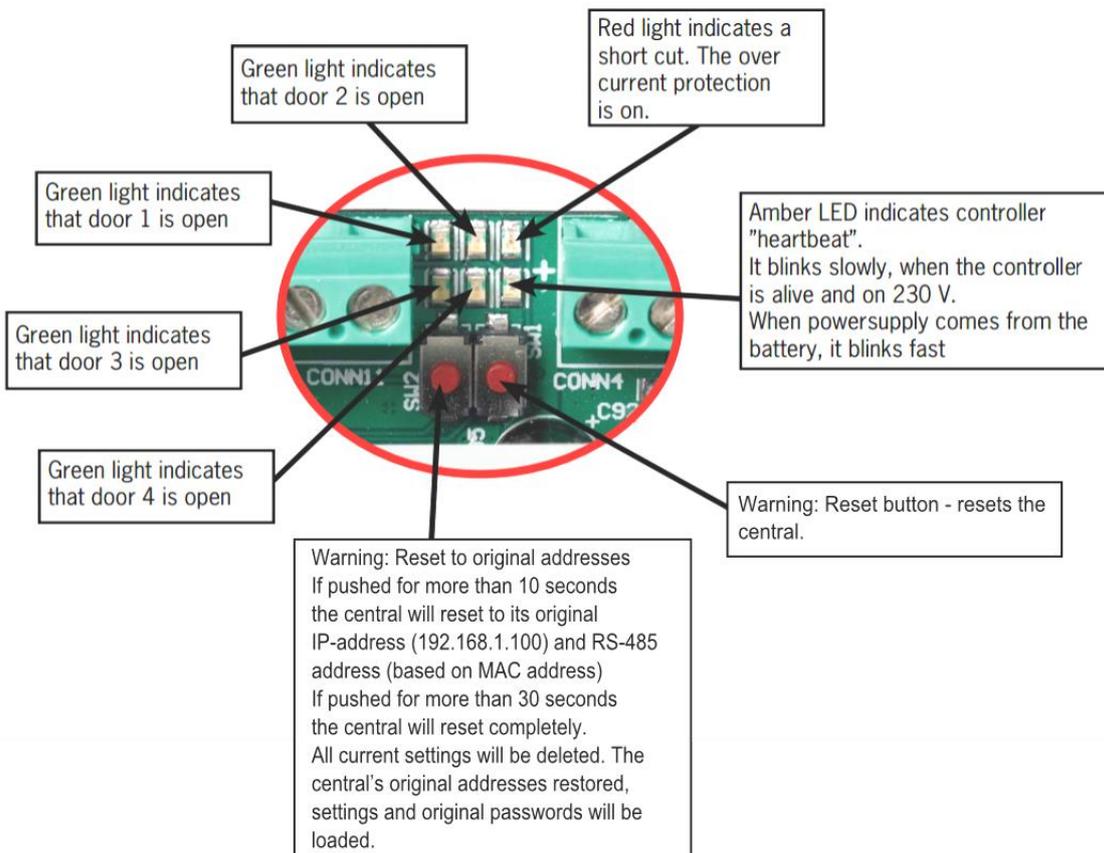
The blacklist itself can store up to 1133 cards.

## 23 Appendix A - Description of LEDs and buttons on central

There are two types of central Hardware and some differences in position/colour of the LEDs and buttons. Here are the descriptions of both:



**Picture 23.1: LEDs and buttons on the new Alpha central**



**Picture 23.2: LEDs and buttons on the old Alpha central**

## 24 Appendix B - Nova software feature possibility list

Package/Module	Description	Administrator client	200 extra users	10 extra doors	Use any card	XML integration	Offline+	Door stations	Python scripting
NovaSimpli	price: free, no schedules - only 24h, no offline doors, only one - standalone central	no	yes	no - only one standalone central	yes	no	no	no	no
NovaSimpli 350	price: free, no schedules - only 24h, no offline doors, no events history, only one - standalone central	no	yes	no - only one standalone central	yes	no	no	no	no
Nova10	10 doors/100 users	yes	yes	yes	yes	yes	yes	yes	yes
Nova100	100 doors/1500 users	yes	yes	yes	yes	yes	yes	yes	yes
NovaPRO	250 doors/3000 users	yes	yes	yes	yes	yes	yes	yes	yes
NovaServer	500 doors/5000 users	yes	yes	yes	yes	yes	yes	yes	yes

**Table 24.1: Nova software feature possibility list**

The company was founded by a group of engineers with years of experience in the field of access control. We combine our specialist expertise with our solid first-hand experience to develop convenient solutions for our customers. We aim to develop access control systems based on what our clients want and need with high security in mind.

Our systems also include high flexibility and quality, which make it possible to create dynamic, innovative solutions. Prima develops solutions suitable for all industrial, office, home

systems, saving both money and time. We base our solutions on an open platform, which is easy to integrate with video, time and attendance, booking, house automation and other customized solutions that you might require.

We provide 100% access control systems focused on software, hardware and centrals. We co-operate with experts in the field to develop secure, yet user-friendly products for customers.

Our production and development is located