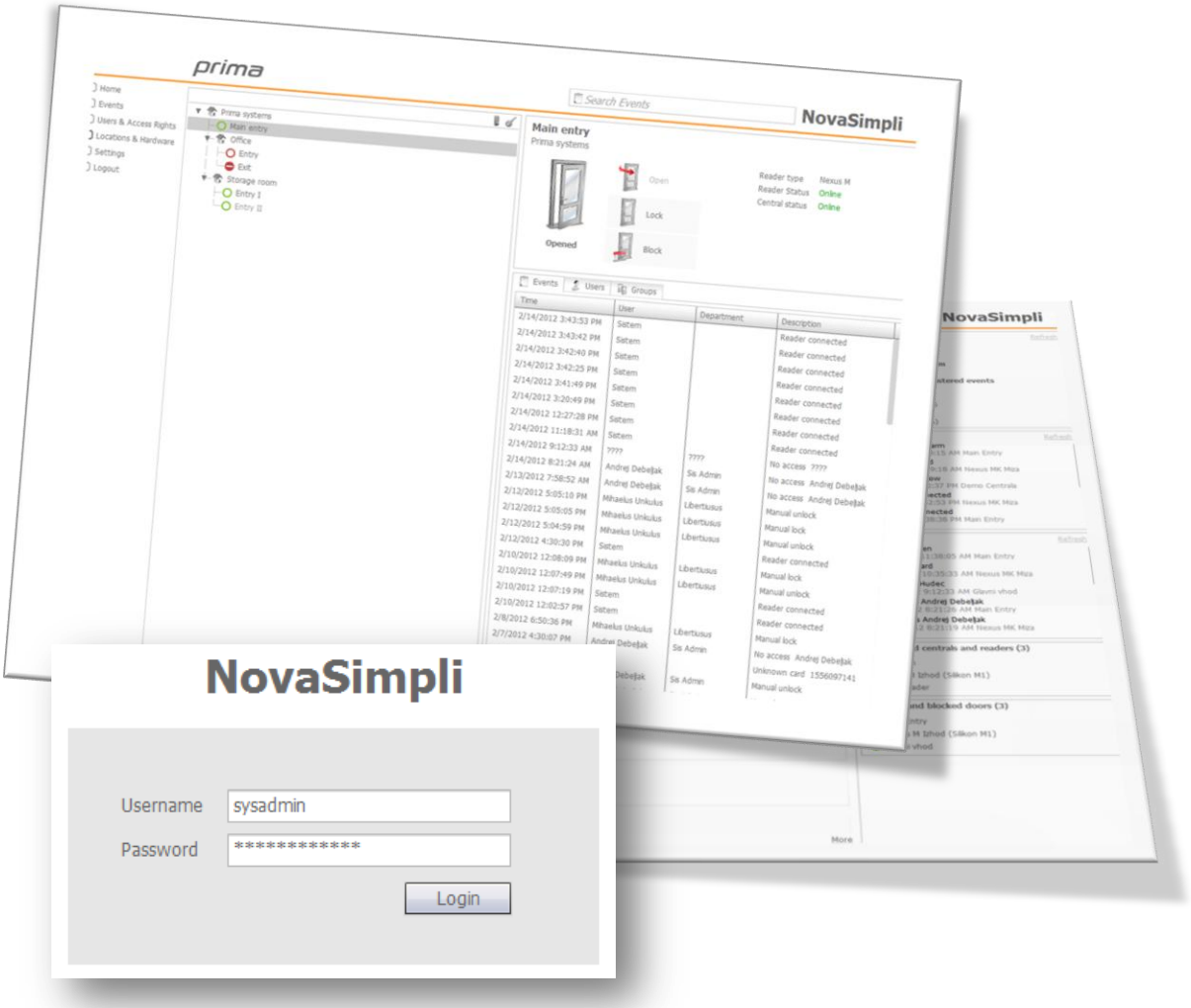
Nova software
Administrator manual

Version 2.1.0



prima

Index

Explanations of words and concepts

Central:	Electronic device, an integral part of access control system
ID card:	Identification card, can be Mifare card, EmMarine card etc.
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
RE:	Request to exit
DM:	Door monitor
LAN:	Local area network
WAN:	Wide area network

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.

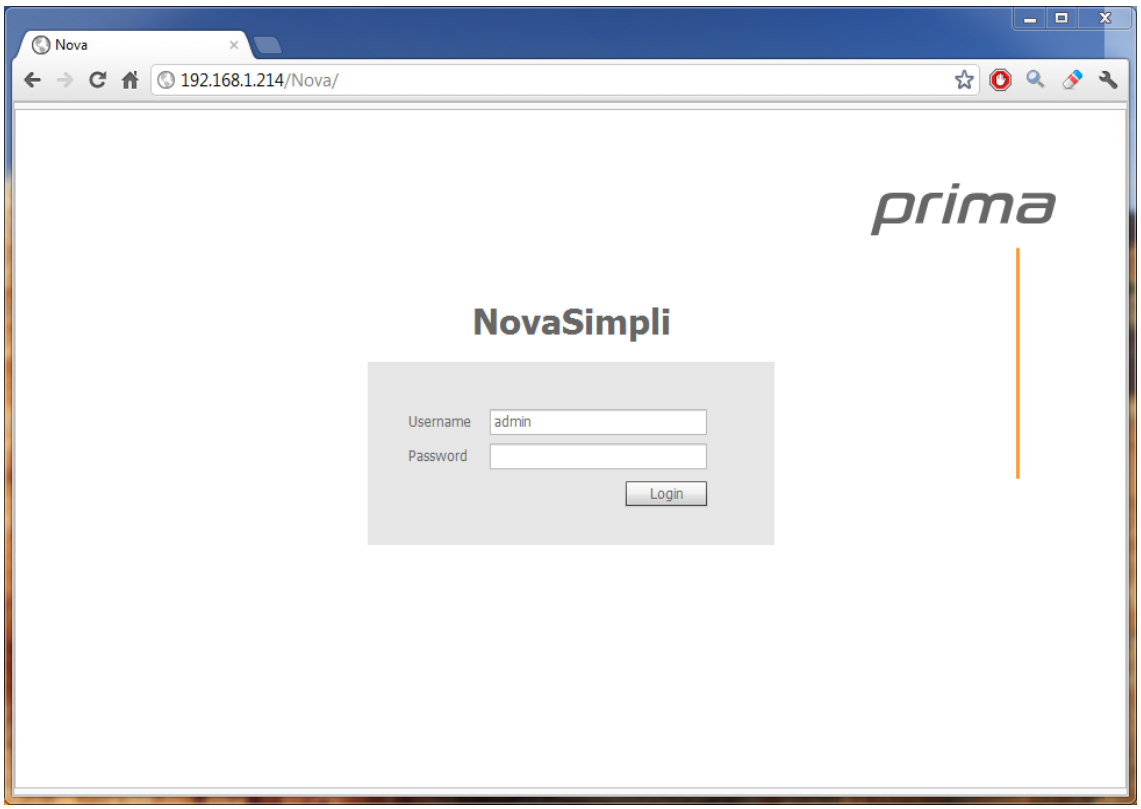
More information about activation keysneededis described in chapter 6.3Add-ons & Modules tab.

1 Login page

Open and navigate the web browser to the web address of the central (default central address is *http://192.168.1.100*). If there is a shortcut installed on the desktop, use it to access the Nova software.

Type username and password into the login page (Picture 1.1). For the first log-in, use the predefined username **sysadmin** and password **sys4Admin**. Remember that passwords are case sensitive.

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



Picture 1.1: Login page

Nova software implements three types of accounts:

1. *Basic administrator account* is used for the day-to-day administration of the system and permits the management of users and controlling doors in the system.

2. *System administrator account* is used by the person installing the system and to add centrals and its readers to the system. This account holds the rights of managing the hardware. This account controls which other administrator accounts are active. Do

not use this account in normal workflow.(This account can be assigned to the IT-responsible, the installing contractor etc.)

3. The third type of account is the *super administrator account*, which is primarily used for development purposes. Do not use this account in normal workflow. The *system administrator* can disable this type of account under "*Settings"* – *"Account"*.

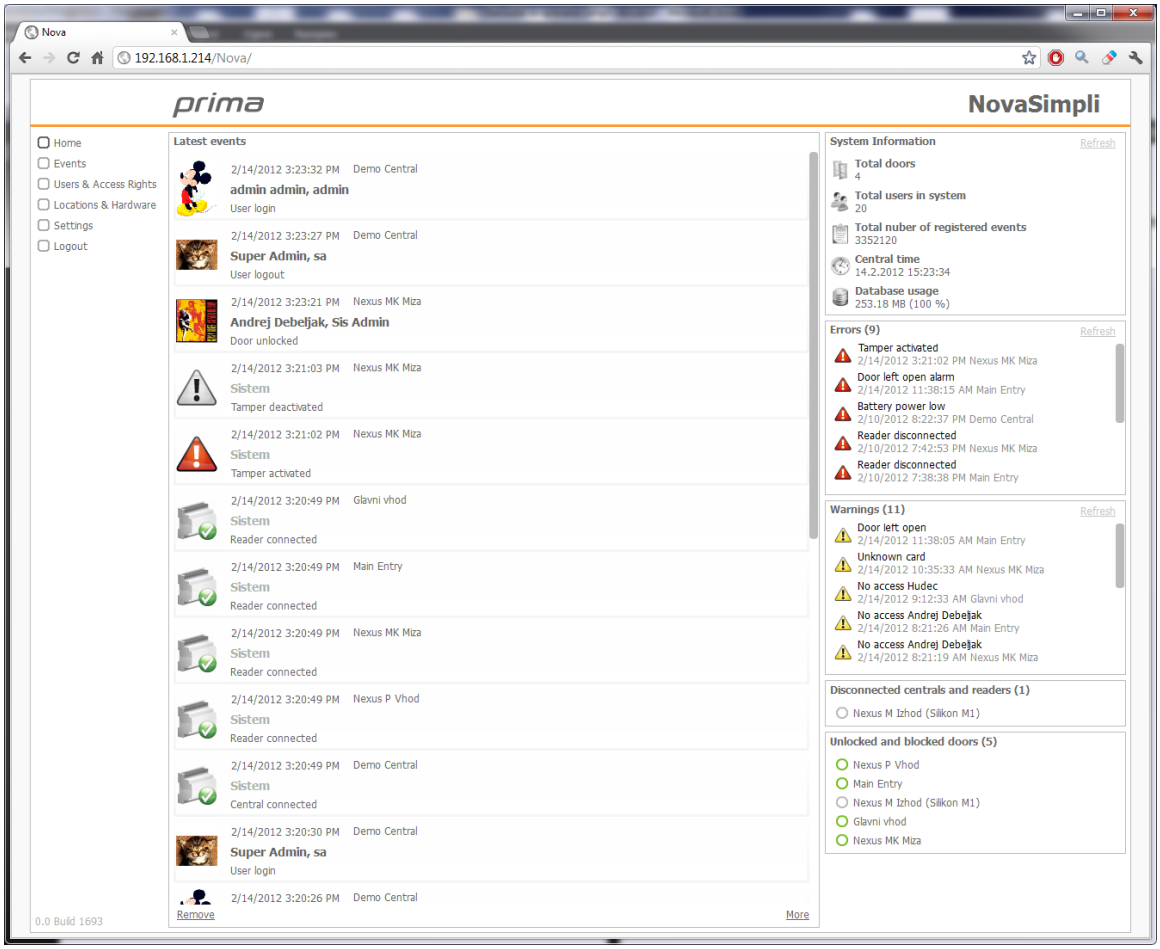
If the login credentials were correct, the Home page of the Nova software will appear on the screen.

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 192.168.1.100. To change the settings described in the message, they have to be clicked or they can be prevent from showing up again by clicking on the *"Do not show again"* link(Picture 1.2).

Picture 1.2: Warning message

2 Home and main navigation

The main page after login is called "*Home*" page with the main navigation menu on the left hand side of the browser. Middle column of the page holds the section "*Latest events*" with the most recent events in the system. Column on the right contains panels for "*System information*", "*Errors*", "*Warnings*", "*Disconnected centrals and readers*", "*Doors left open*" and "*Unlocked and blocked doors*".



Picture 2.1: Home page and main navigation menu

The main navigation menu holds links to access other pages of the Nova software:

- **Home**– main page with latest events and system overview
- **Events**–log of system events
- **Users & Access Rights**– users and access rights management page
- **Locations & hardware**– locations and hardware management page
- **Settings**– account management and advanced settings page
- **Logout**– logout page

The "*Latest events"* list displays events in the system as they happen. Each event in the list has a defined time, location and name of the user, who has triggered the event.

The panels on the right side are showing the current state of the system. The window "*System Information"* is providing brief information of total doors and users in the system, as well as the current time on the central and database usage. Below this window there are "*errors"*, "*alarms"* and "*warnings"* that need to be inspected, a list of "*Doors left open*" and a list of "*unlocked"* and "*blocked doors"* and a list of "*disconnected centrals and readers"*.

IMPORTANT! Sometimes the door will appear on the Doors left open list even when the door seems locked. This can happen because of the settings of the Door monitor (described in the chapter 5.2.15 Door settings). For monitoring doors left open, a function "*Door forced detection*" **must be enabled** (also described in the 5.2.15 Door settings).

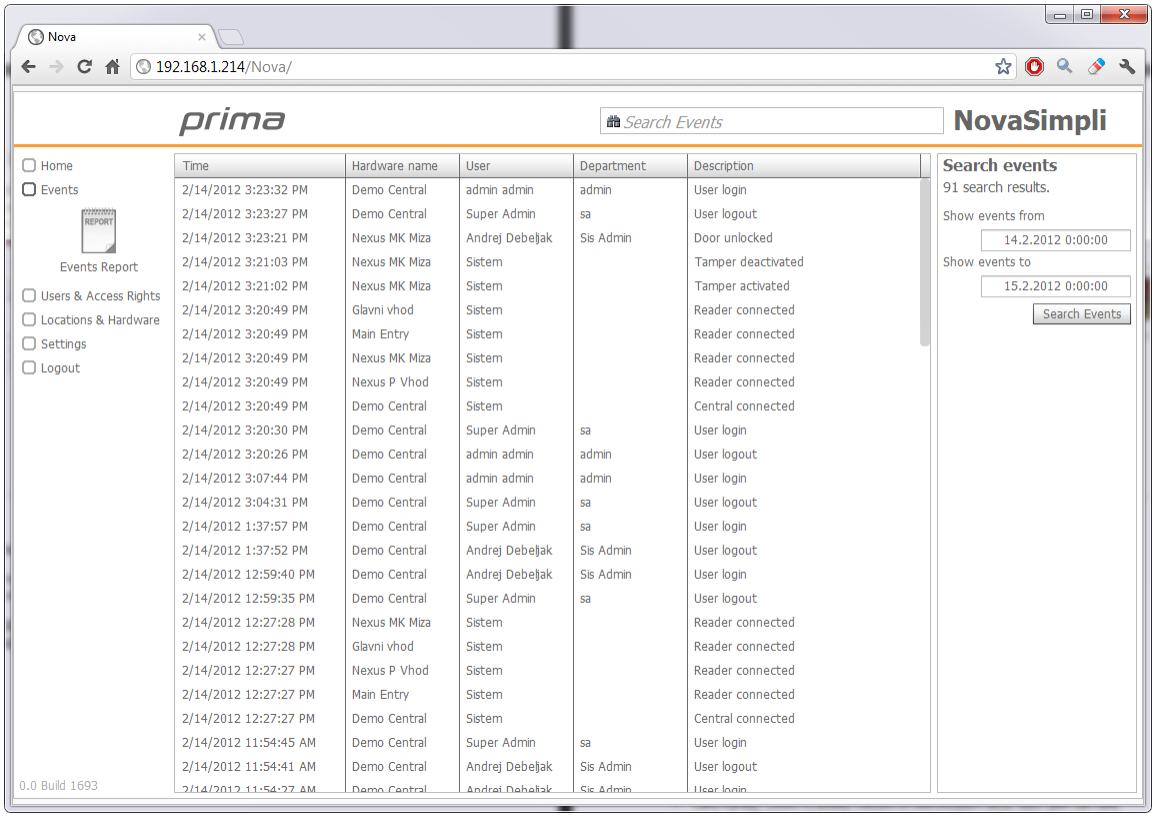
IMPORTANT! A reader must be connected to the door index in order to display the proper door state. If there are no readers physically connected to the central, manually add one and unchecked the *"Enabled"* option.

In the left bottom corner, software version of the central is displayed. Providing the software version is extremely helpful when contacting support for easier determination of the problem(s).

Most of the information at the "*Home"* page is clickable and can provide detailed insights.

3 Events

The "*Events*" page can be used to browse the event history of the system. The events can be limited to chronological search by selecting *start* and *end date* on the right side of the page. The Nova software can display up to 10000 events in one search. Further filter can be applied by using the search field in the Nova software header. The *Events* list will only display events that match the search criteria.



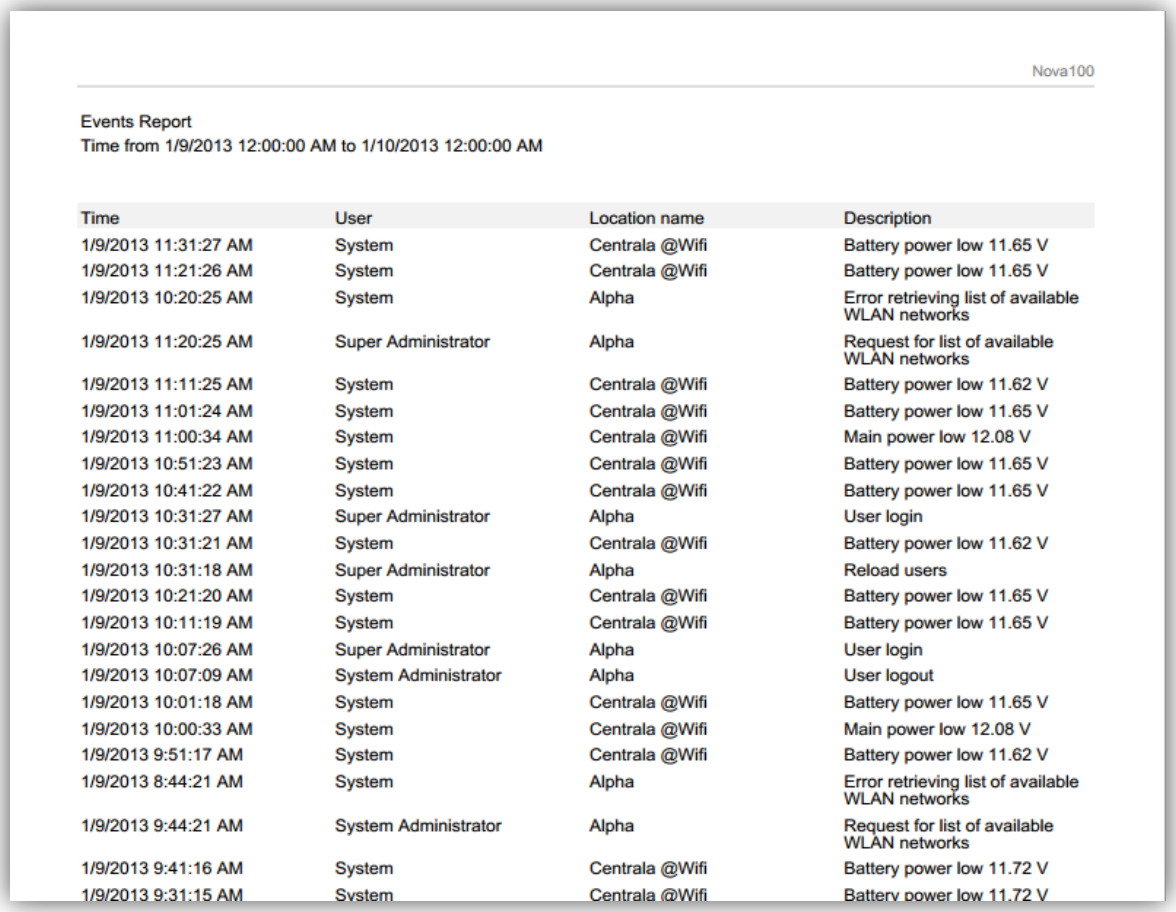
Picture 3.1: Events window

IMPORTANT! Having too many events in a set time period may cause an error of result set being too large. The error can be prevented by reducing the time limits to match the period that contains maximum of 10000 events.

The displayed events can be sorted by clicking on headers in the "*Events*" list.

All of the displayed events can be exported to a PDF file. The document can be created by clicking on the "*Events Report*" button in the main navigation menu.

IMPORTANT! For review of a PDF documents on computer,3rd party programs that support PDF file extensions must be installed. During export, browser will prompt users to allow popup windows. By enabling popup windows, user can then download the file to their computer.



Nova100

Events Report
Time from 1/9/2013 12:00:00 AM to 1/10/2013 12:00:00 AM

Time	User	Location name	Description
1/9/2013 11:31:27 AM	System	Centrala @Wifi	Battery power low 11.65 V
1/9/2013 11:21:26 AM	System	Centrala @Wifi	Battery power low 11.65 V
1/9/2013 10:20:25 AM	System	Alpha	Error retrieving list of available WLAN networks
1/9/2013 11:20:25 AM	Super Administrator	Alpha	Request for list of available WLAN networks
1/9/2013 11:11:25 AM	System	Centrala @Wifi	Battery power low 11.62 V
1/9/2013 11:01:24 AM	System	Centrala @Wifi	Battery power low 11.65 V
1/9/2013 11:00:34 AM	System	Centrala @Wifi	Main power low 12.08 V
1/9/2013 10:51:23 AM	System	Centrala @Wifi	Battery power low 11.65 V
1/9/2013 10:41:22 AM	System	Centrala @Wifi	Battery power low 11.65 V
1/9/2013 10:31:27 AM	Super Administrator	Alpha	User login
1/9/2013 10:31:21 AM	System	Centrala @Wifi	Battery power low 11.62 V
1/9/2013 10:31:18 AM	Super Administrator	Alpha	Reload users
1/9/2013 10:21:20 AM	System	Centrala @Wifi	Battery power low 11.65 V
1/9/2013 10:11:19 AM	System	Centrala @Wifi	Battery power low 11.65 V
1/9/2013 10:07:26 AM	Super Administrator	Alpha	User login
1/9/2013 10:07:09 AM	System Administrator	Alpha	User logout
1/9/2013 10:01:18 AM	System	Centrala @Wifi	Battery power low 11.65 V
1/9/2013 10:00:33 AM	System	Centrala @Wifi	Main power low 12.08 V
1/9/2013 9:51:17 AM	System	Centrala @Wifi	Battery power low 11.62 V
1/9/2013 8:44:21 AM	System	Alpha	Error retrieving list of available WLAN networks
1/9/2013 9:44:21 AM	System Administrator	Alpha	Request for list of available WLAN networks
1/9/2013 9:41:16 AM	System	Centrala @Wifi	Battery power low 11.72 V
1/9/2013 9:31:15 AM	System	Centrala @Wifi	Battery power low 11.72 V

Picture 3.2: Example of Events report

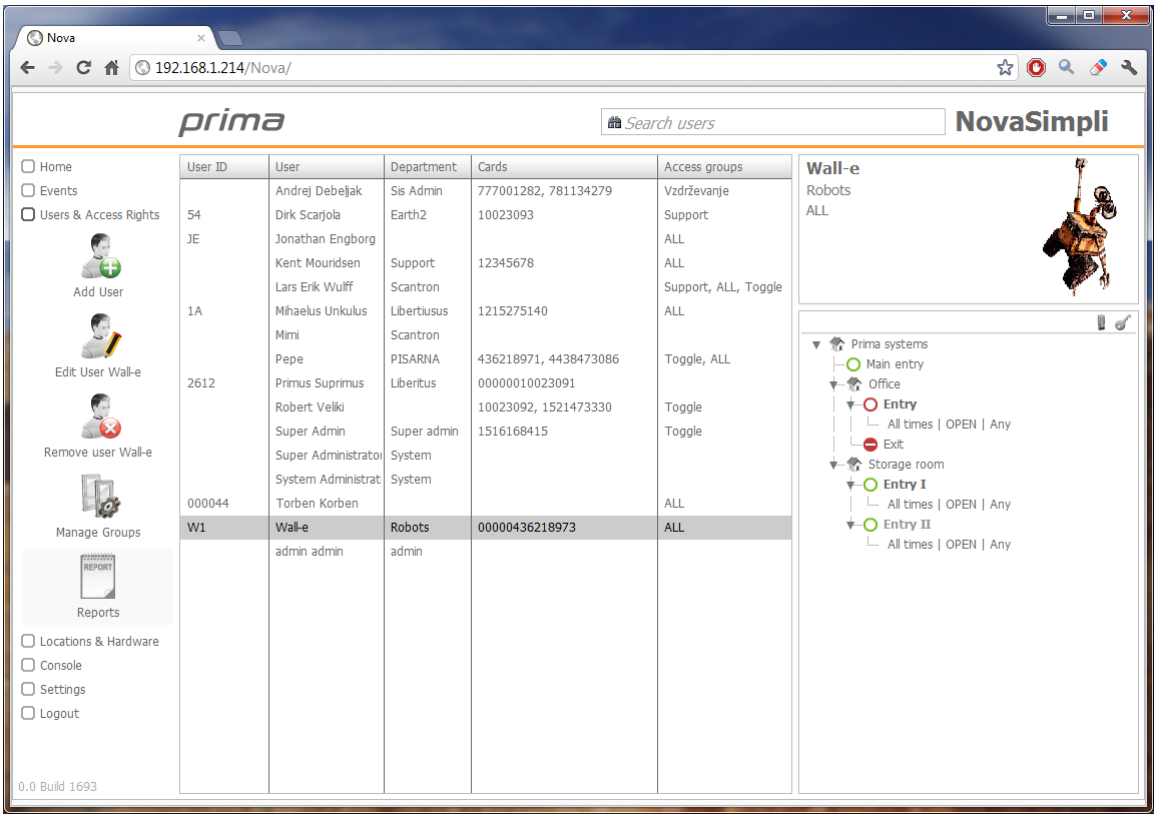
IMPORTANT! Software version NovaSimpli350 does not display or store any of the events in the system. Events can be monitored only trough live events on the home page.

4 Users & Access Rights

IMPORTANT! For initial setup, make sure to setup *Locations & Hardware* page before adding users to the system. See chapter 5, before continuing with the setup of *Users & Access Rights*. Creation of the access groups before adding users is strongly recommended – see part 4.2 for these instructions.

The *Users & Access Rights* page is used for managing users and their access rights and groups. Access groups can be seen as zones of pre-defined doors, which a user has access to, if the user is assigned the required access group. For each access group, a precise time interval can be set for user's access to specific doors.

When clicking the "*Users and Access Rights"* button, the main navigation menu contains buttons for adding, editing and removing users, a button for managing access groups and a button for accessing different types of reports for a specific user(s).



Picture 4.1: Users & Access Rights page

Detailed information regarding the selected user is displayed in the upper-right corner of the page, while his/her access rights are shown below.

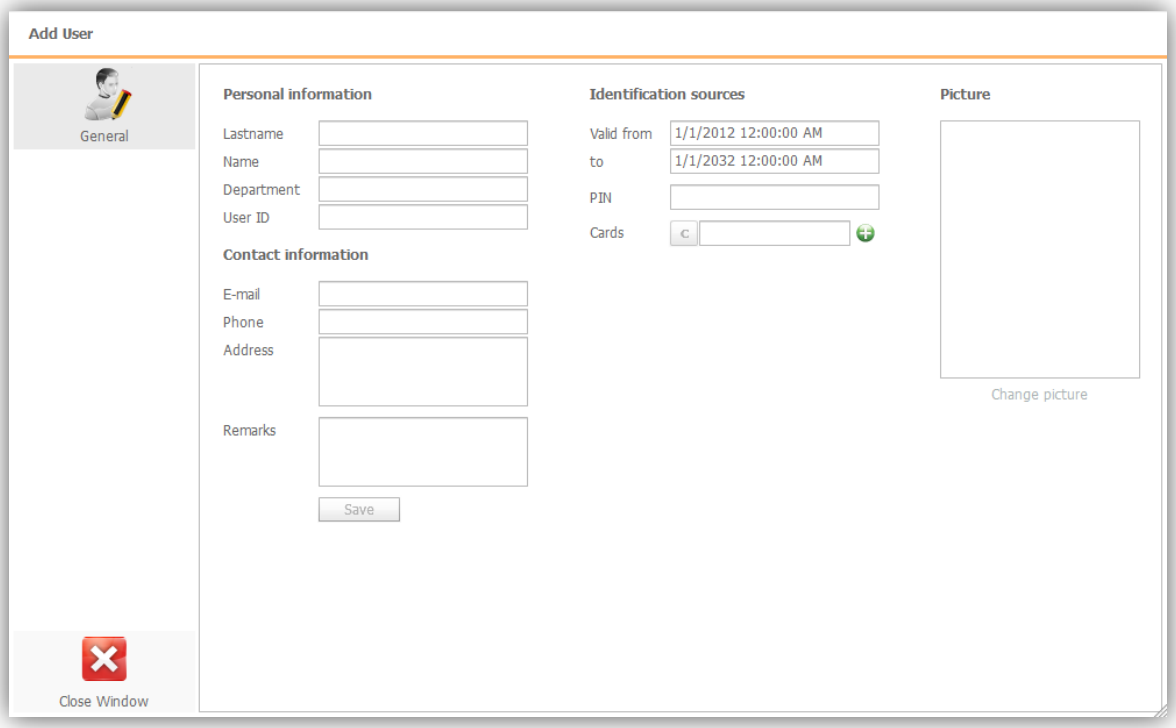
4.1 New users

A new user can be added by clicking the button "*Add user*" in the main navigation menu. User data can be entered in the opened popup window (Picture 4.2).

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

- Personal number.
- Name.
- Last name.
- Department.
- PIN (which must not exceed 20 characters) **IMPORTANT!** Each user needs to have a unique PIN. Length of the PIN code on **offline readers** is limited to **maximum of 7 characters**. PIN that doesn't comply won't work and won't display any warning when writing data on user card.
- Card number (which is usually marked on identification card). Each user can have up to 8 different card 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.

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

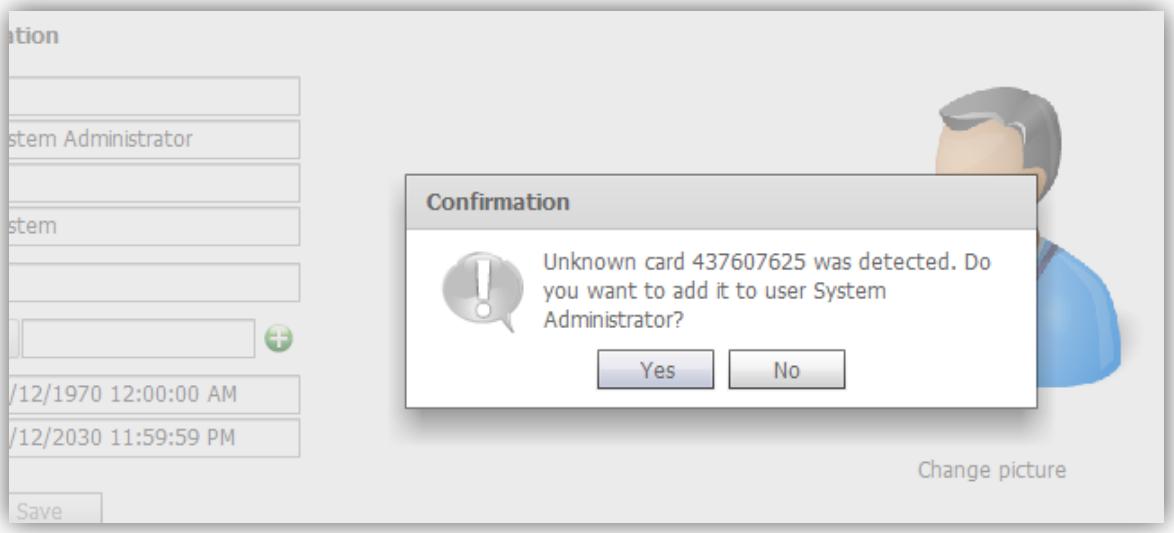


Picture 4.2: Input for new user data

4.1.1 Adding unknown card(s) to user

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

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 unknown card to user

4.1.2 Card role assignment

Different roles 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 (**C**ard), but its role can be changed by selecting a new role from the menu which opens, when the button to the left of the card number is pressed:

- **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

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

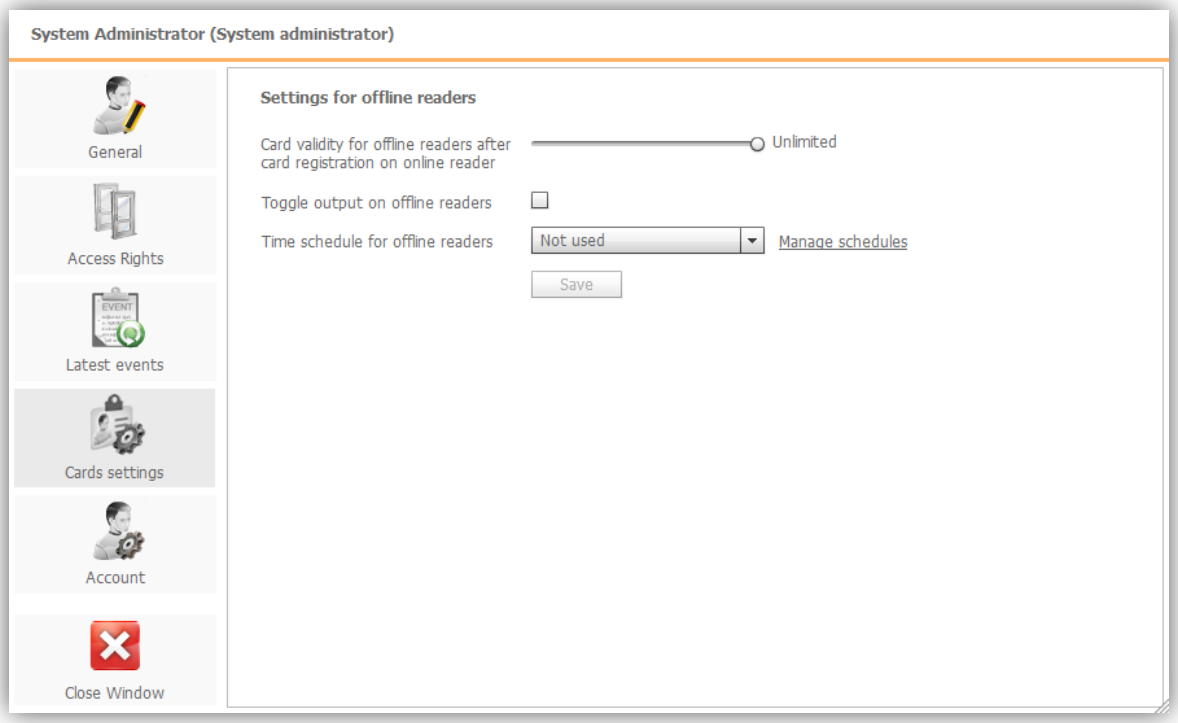
- **BL**: Blacklist card (card used to transfer the list of lost cards to an offline reader),
- **EV**: Events card (card used for transfer the list of events from an offline reader to the central)

- **CO**: Configuration card (card for transferring configuration settings to an offline reader),
- **B**: Battery card (card for replacing batteries on an offline reader, if applicable),
- **D**: Disassembly card (card for disassembly of an offline reader, if applicable),
- **F**: Format card (card will be formatted when detected on online reader).

4.1.3 Setup and managing users and access rights

After the user data is saved, additional options are shown – on the left side of the popup window buttons for editing the "*Access rights"*, previewing "*Last events", "Card settings"* and an "*Account"* option are added.

In the menu called "*Card settings"*(Picture 4.4)a validity of data written on cards for offline readers can be set. The options to set whether cards, assigned to the user, can activate and deactivate the toggle mode on offline readers (constantly unlocked/ activated so it works like a thumb turn on the inside of a door) is located here. Optionally a time schedule can be selected, which will limit the usage of a user's card on offline readers to the intervals defined in the selected time schedule. Offline readers only support two time intervals, so only the first two defined intervals in the selected time schedule will be used. The option of checking the time intervals on the user's cards needs to be enabled on the offline reader (see Picture 5.21).

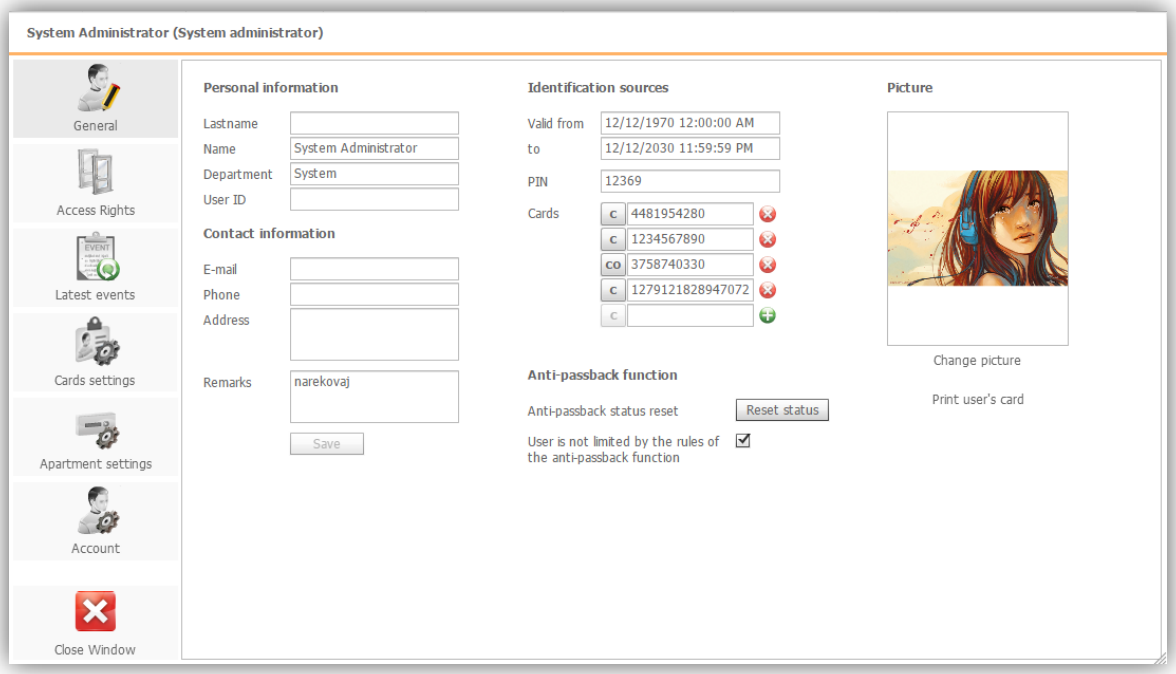


Picture 4.4: Card settings for offline readers

Change of the user picture can be done by clicking the "*Change picture"*button on the right side of the popup window (Picture 4.5). These options are preset every time someone is editing an existing user or after a new user's data is saved.

User's data can edited by clicking the "*Edit user"* button in the main navigation menu or by double clicking the user in the grid of users.

Nova software version 1.6 and higher includes Anti-passback functionality. The instructions on enabling it, please read chapter 5.2.8Advanced settings. In the user menu we are able to reset user status by clicking on the *"Reset status"* button. A new popup will offer the reset for **current** user or for **all** users in the system.
Under the reset button, there is a checkbox if we want to disable Anti-passback function for a target user.



Picture 4.5: Popup window for editing an existing user

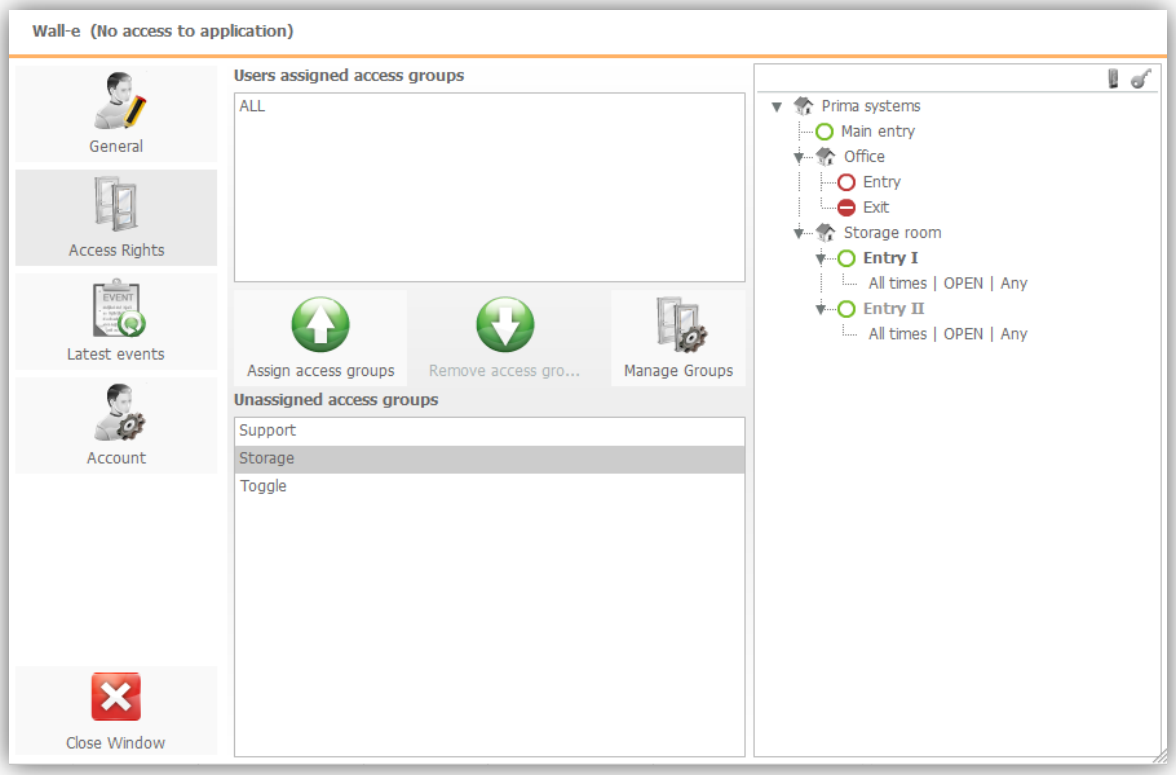
A user's access rights can be changed by clicking the "*Access Rights"* button (Picture 4.6). See part 4.2 of this manual for management of access groups.

The window will display two lists; the upper list contains the access groups already assigned to the user while the lower list contains the remaining unassigned groups. On the right side of the popup window with allowed access of the selected access group is shown. Access groups can be added or removed from user by selecting the "*Up"* or "*Down"* buttons with arrows on them.

Access groups can be assigned to multiple users at the same time. To do so, users must be selected from the user list (Picture 4.1) by holding Ctrl (adds non-consecutive selection) or Shift (adds consecutive selection) key and then clicking on the *Edit users* button in the main navigation menu. This button is only visible once multiple users are selected.

When one or multiple users are marked and the button *Last events* is selected, the history of this user(s)'s events is shown. This is useful for monitoring a user's actions in the system.

Promotion from a user to administrator can be done under the "*Account*" option. Clicking on the "*Account"* button will show a form where the user's login name and password can be set. The "*Account"* button is only visible to access of the system administrator. Lower level access like basic administrators do not have the permissions to grant a user access to the application.



Picture 4.6: Assigning access groups to user

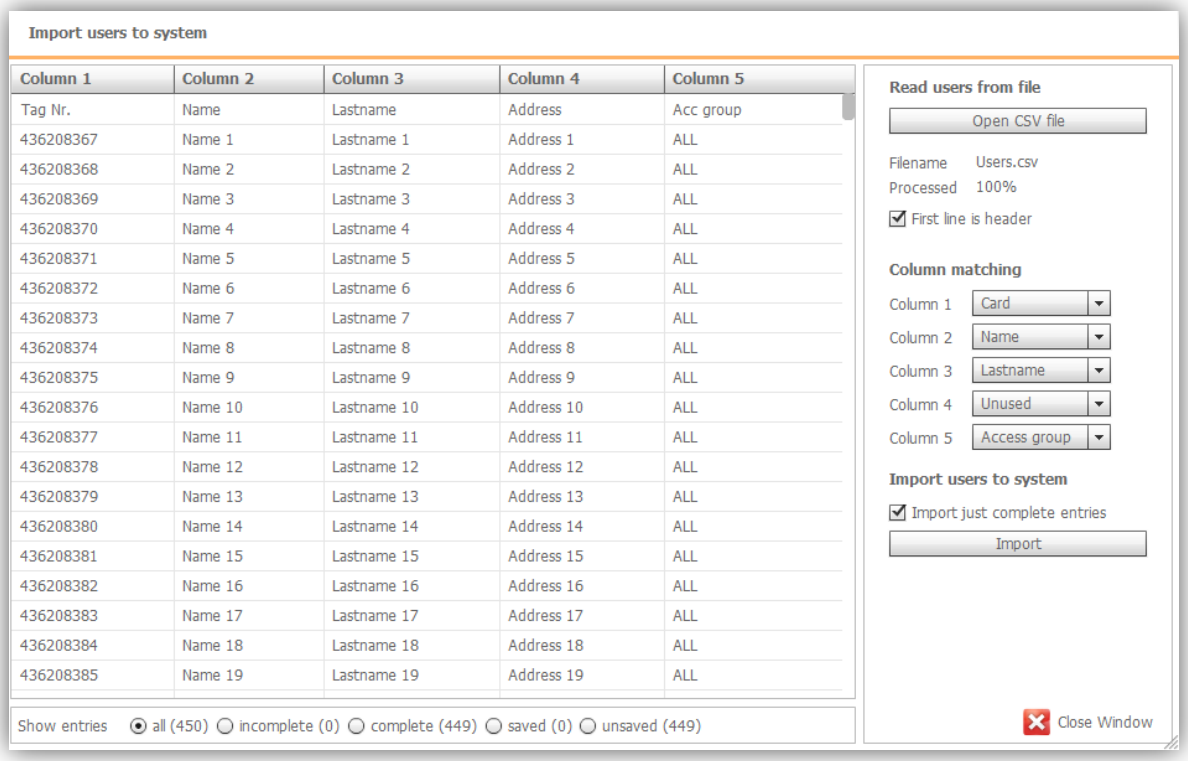
User can be removed from the system by selecting it from the list of users and then clicking on *Remove user* from the main navigation menu. The user will be deleted, but its cards will remain in the system. This way the administrator can see if someone is trying to get access using the deleted card(s).

The same card can be re-used for a new user, by following step 4.1.1. Following this, the card will work normally and all events are normally reported in the software.

4.1.4 Importing more users from .CSV file

User data can be imported into the software from a.CSV-file (comma separated values). *Add User* button must be pressed from the main navigation menu and the option to *Import from file* has to be selected. A new popup window will be opened requesting to the location of the file with users' data. The file needs to have the data for each user in separate lines. The data must be separated either by comma (,), semicolon (;) or TAB separator. The data from the import file will be parsed and presented in a grid (Picture 4.7). If there are any changes that need to be resolved, data can be rewritten in the grid.

Under the grid there are different options for filtering parsed data. Checkbox above the *Import* button allows *the* option to display only the complete entries (entries where all columns have data), incomplete entries (where some columns do not contain data), unsaved and saved entries. The first line in a CSV-file is usually the header line and if administrator does not wish to import it as a new user, the option *First line is header* must be selected. Columns names must be matched with user columns for additional details. The columns can be set to represent "*Unused*", "*Last-name*", "*First-Name*", "*Department*", "*Access group*", "*Card number*", "*PIN*" or "*User ID* "fields. Values in the column matched as "*Access group*" need to match a valid Access group names, which are already present in the system. Furthermore, the values in the column matched as "*Card*" or "*PIN*" details needs to be valid numbers. Note that every user needs to have a unique PIN.



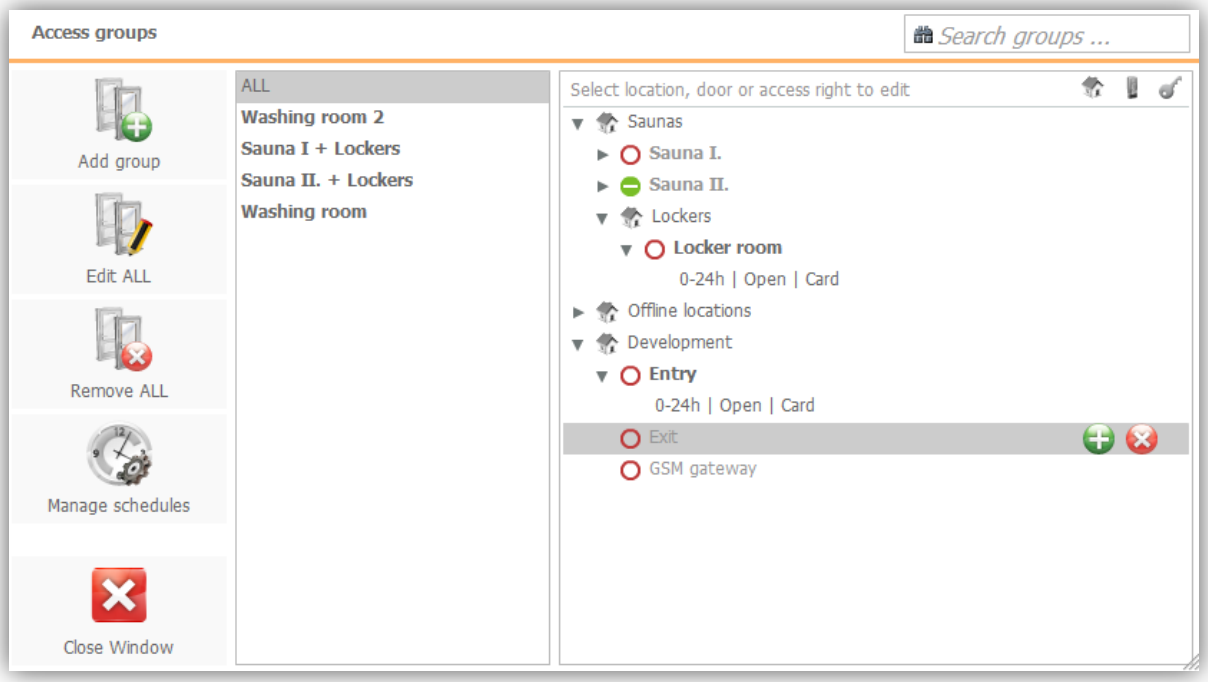
Picture 4.7: Import users from CSV file

After editing is done, import of the users to the system can be done by clicking the *Import* button. If the option "*Import just complete entries* is selected", only values where all columns have data will be imported. After the import is finished, a filter can be applied on the user list to see which entries were saved and which ones were not.

After the import is done, a re-log is needed. After a successful log-in, the correctly imported users will be added to the user-list.

4.2 Managing Access groups

A popup window for managing the access groups is accessible from the main navigation menu. Clicking on the button *Manage groups* will open the popup window shown on Picture 4.8.



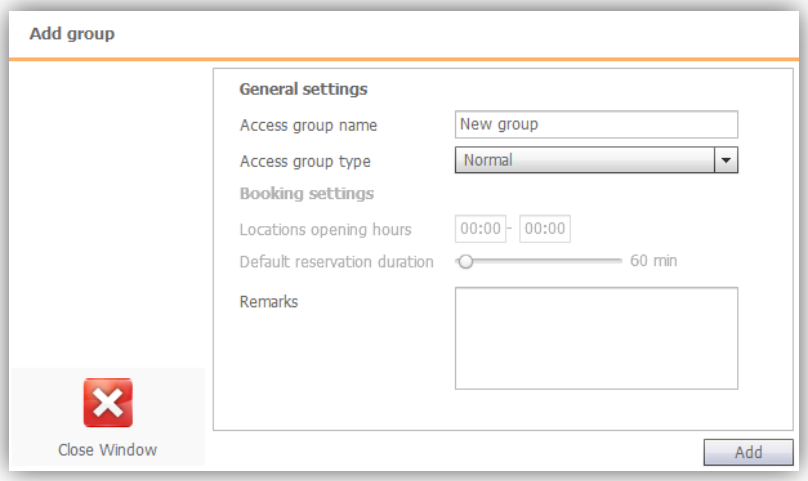
Picture 4.8: Access groups editor

A new access group can be added by clicking the *Add group* button in the Access group editor. A name for the new group needs to be provided in the *Access group name* input box and in the *Remarks* field there can be optionally entered the description of the group or some other information (Picture 4.9). Access group is saved with the click on the *Add* button.

Note: 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. Groups with type set to *Booking* are written in bold in Access group editor. For more information about Booking module please see chapter10.

An existing group can be edited by first selecting the group in the list of access groups and then clicking the *Edit group* button (Picture 4.8).

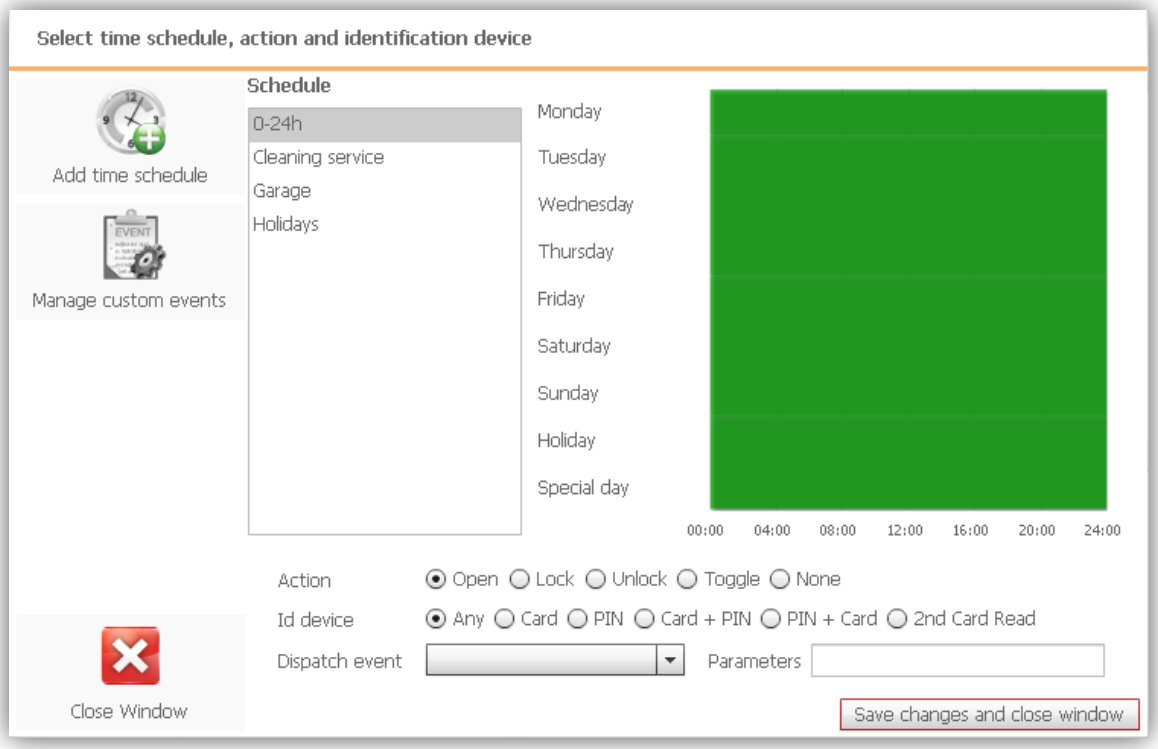
An access group can be removed from the list by first selecting the group and then clicking the *Remove group* button. Access groups that are assigned to users cannot be deleted.



Picture 4.9: New group editor

Access rights for selected access group in Access groups' editor (Picture 4.8) are visible in hardware tree next to the list of groups. Buttons at the top of the tree can adjust current tree view and select which brunches of the tree are displayed.

New access rights can be added to the selected group by clicking on the "*Plus" button*, which is visible when an item from the hardware three is selected (Picture 4.8). This will cause a new popup window to open.



Picture 4.10: Time schedule, action and ID device selection

Picture 4.10 shows the option to select the desired time schedule and the action which will be executed when an identification device is presented to the reader that controls selected door.

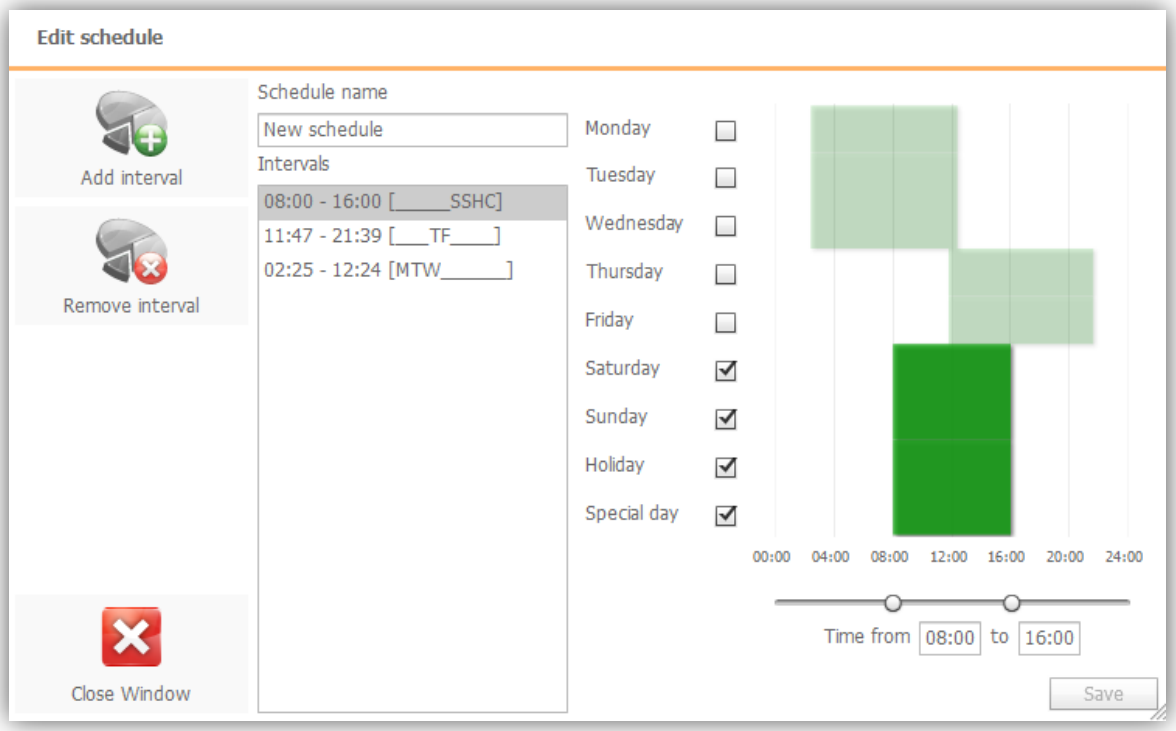
In case of Scripting module activation key installed, a custom event can be set to trigger a dispatch event and handled by the user script in the context of access right. For more information please see chapter 8.
The existing access rights can be edited or removed with the use of appropriate buttons 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* will be used with the actions *OPEN* and *CARD* as a source for executing action. Those accesses cannot be edited.

4.2.1 Managing time schedules

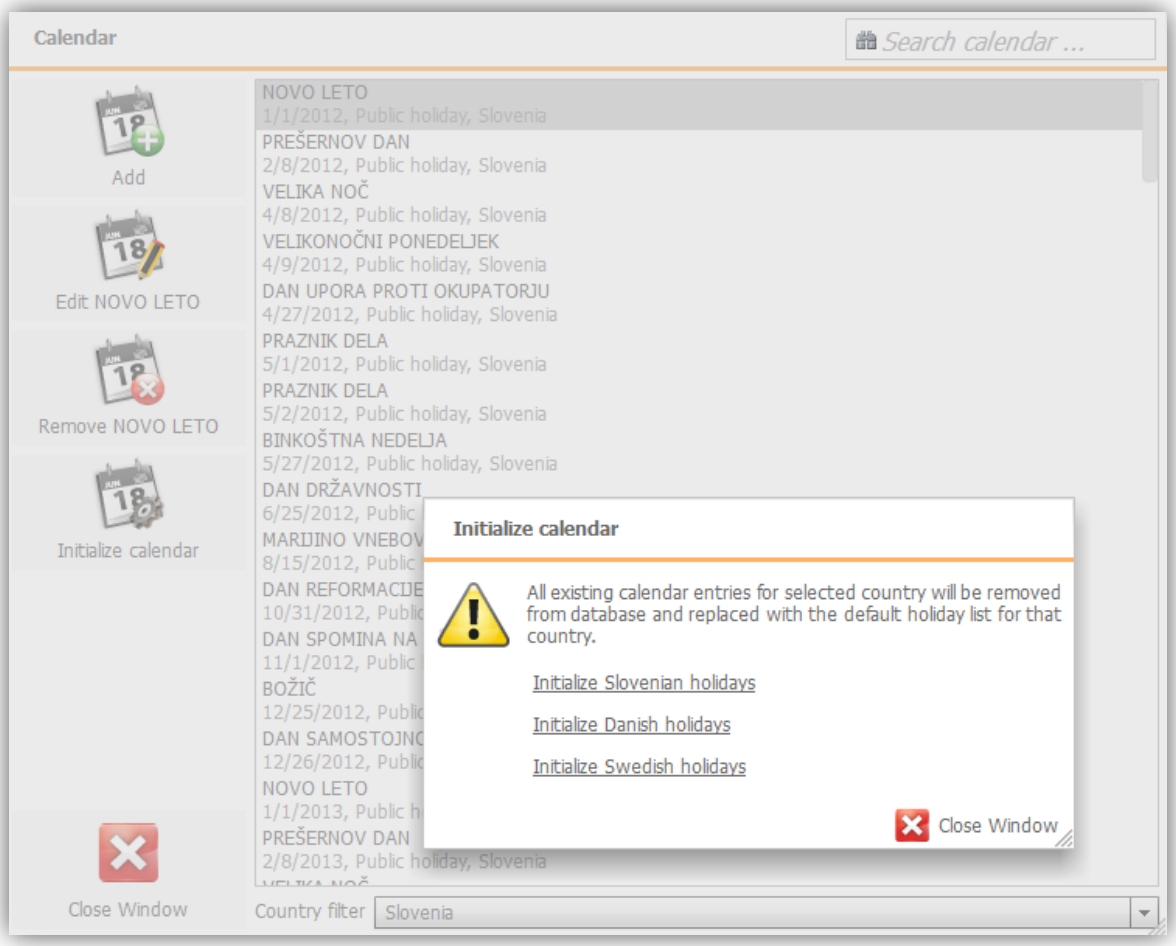
The NovaSimpli software includes one, predefined time schedule (0-24h), which is valid from 00:00 till 23:59 for every day of the week and cannot be modified or deleted. In other versions of Nova software the option to manage and create additional time schedules is added. It can be accessed by clicking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

T*ime schedule editor* enables the creation, editing or deletion of existing schedules. Access to Calendar enables adding new holidays and any special days. Each time schedule contains one or more time interval(s), where each of them has a defined time span and days when the interval is valid (Picture 4.11). Additional time intervals can be added to the schedule by clicking the *Add Interval* button.



Picture 4.11: Time intervals

Each time interval can be valid on any day and also on a "*Special day"* (any day that has different time interval values than normal one) and on "*Holidays*. *Special days"* and "*Holidays"* are defined in the Calendar and are country dependent. For each entry in the calendar there is an option to assign the country in which the entry is valid. The *Country* value is then matched with the *Country* property of the central (see chapter5.2). If the country is unassigned, the calendar entries are valid everywhere.
Clicking the *Initialize calendar* button in the Calendar editor displays the options to initialize calendar with the default list of holidays for the selected country. Please remember that all of the existing entries in the calendar for the selected country will be deleted from the database and replaced with the default list of holidays for selected county.

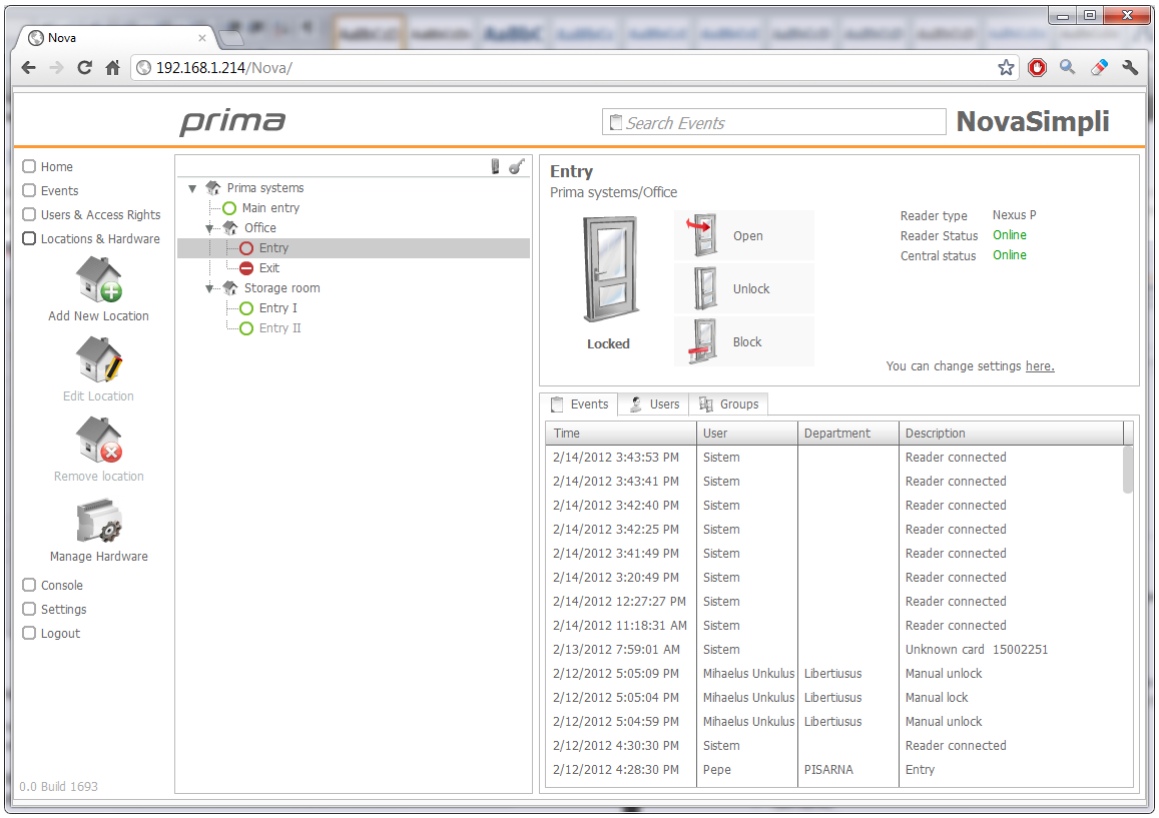


Picture 4.12: Initialize calendar with the default holiday list

5 Locations & Hardware page

Access control is usually installed on single or multiple buildings having just one or several rooms and doors. In the software, buildings and rooms are mapped with the use of locations and afterwards doors are assigned to those locations in form of readers, which are added to the system with the "*Hardware editor*". This model represents the logical scheme of the access control system and its components.

Managing buttons for different locations are in the main navigation menu on the left side. Submenu contains the button for accessing the "*Hardware editor*" displayed on Picture 5.1.



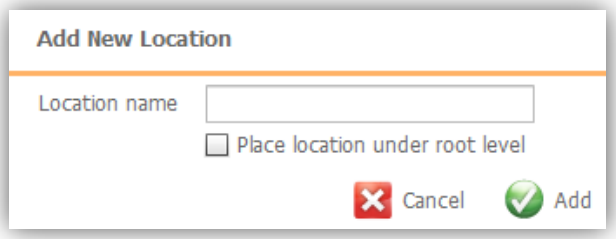
Picture 5.1: Locations and detailed information

5.1 Locations

A new location is added to a selected location by clicking the "*Add new location*" button and entering the new location name into the popup window shown on Picture 5.2. To add the location to root level, select that option in the popup window.

Existing locations and readers can be rearranged at any time by simply dragging the selected location or reader into the target location. The selected location can be edited by selecting the "*Edit location*" button and removed with the "*Remove location*" button.

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



Picture 5.2: Adding new location

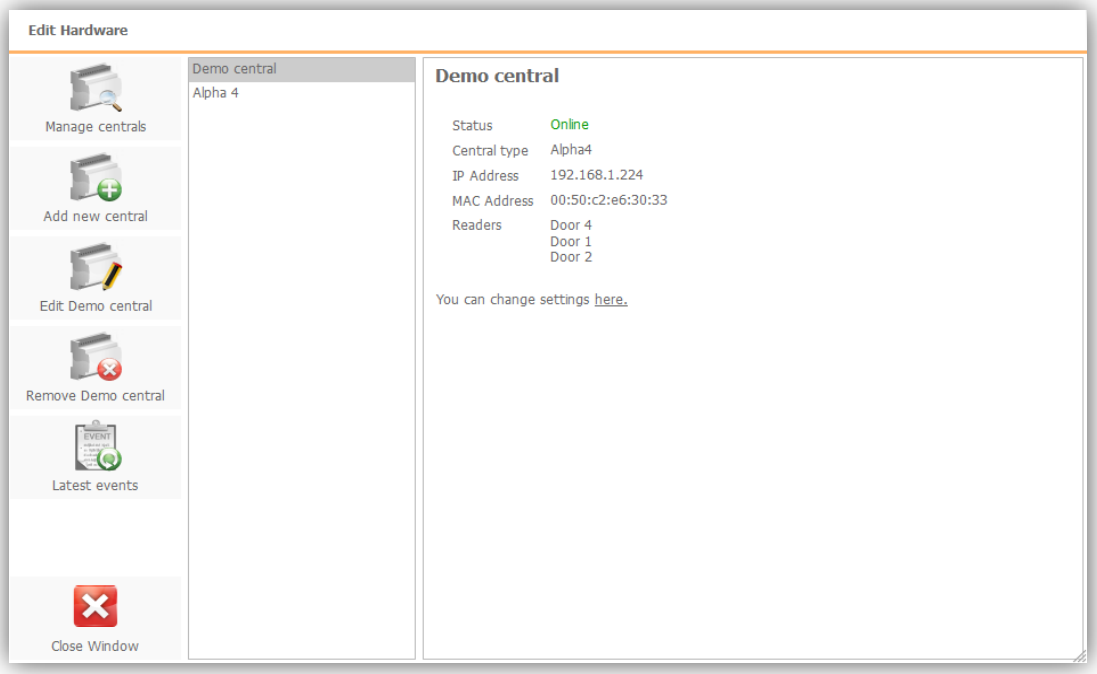
5.1.1 Location management

On the right side of the locations tree, detailed information about the selected item in the tree is shown. Selected location enables management of all connected readers located in the selected location and its sub locations. All readers from selected location can be *locked*, *unlocked*, *blocked* or *unblocked* at the same time. Selecting a reader will display its status and the status of any related door. The related door can also be managed from the selected preview shown on Picture 5.1.Selection of an offline reader will display its details and the button to access the offline readers' editor (*Basic administrators* cannot change hardware settings).

Beneath the details panel, several tabs with additional information about the selected item are located. The first tab contains the *list of last events* related to the item (if the selected item is a location, the events are not shown).The second tab contains a *list of all users* who have access rights to the selected item and all of its connected readers (when the selection is a location). The last tab contains a complete *list of access groups,* which contains the selected reader in the group (or connected readers, if the selected item is a location).

5.2 Hardware editor

The "*Hardware editor*" is used for previewing and managing hardware. Selecting the *Manage hardware* button in the main navigation menu opens the hardware editor (Picture 5.3). The popup window is used for adding and editing existing centrals. The right side of the window displays a quick preview of the selected central. Additionally, an option of previewing the *Latest events* of any selected central is displayed.



Picture 5.3: Hardware editor

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

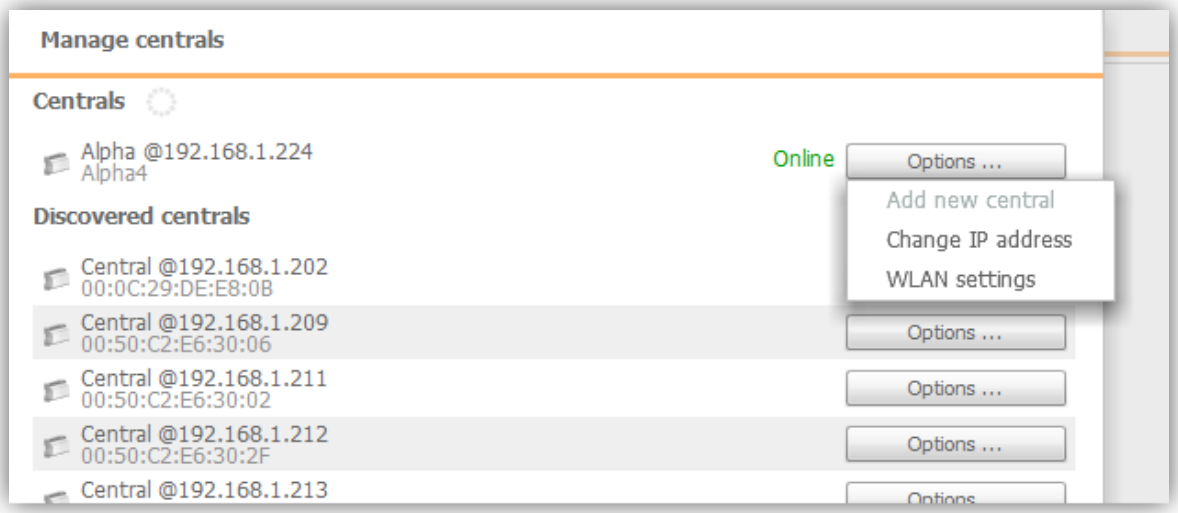
5.2.1 Searching and managing centrals in LAN

Clicking on the button *Manage centrals* in the hardware editor opens a new popup window with a list of all Nova centrals in the local network. The list consists of the centrals already included in the system and other centrals, which are also found in the LAN. Those centrals may be part of another access control system so only add new centrals to the system with caution! Each listed central has the associated button *Options*, which allows adding the central to the system, change the central's interface IP address or manage wireless settings for the central, if applicable.

IMPORTANT! The list of centrals only contains the centrals found on LAN. It does not include centrals connected through a RS-485 bus!

5.2.2 Changing a central's interface IP address

A central's interface IP address is changed by clicking the "*Manage centrals"* button. A popup window will open, which contains a list of all centrals in the system. The central's interface IP can be changed by selecting the button "*Options"* next to the central's description and selecting "*Change IP address"* from the dropdown menu.



Picture 5.4: Manage centrals

A new IP address, subnet mask and address and the default gateway can be set. These parameters depend on the central's network settings. Before changing the address, carefully read displayed warnings.

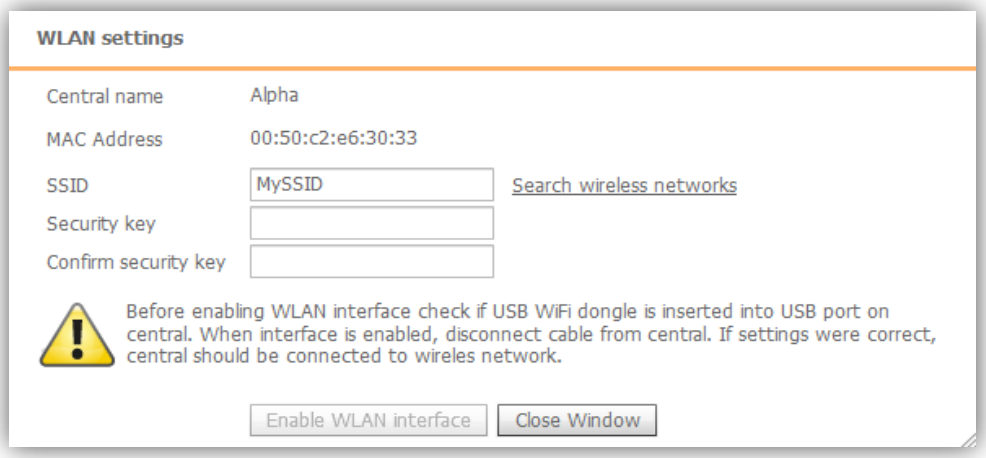
Remember that this option changes the central's interface IP address (the central's address in the local network). The IP address, as seen in *Hardware editor* shown on Picture 5.6, represents the central's global IP address. A master central always uses the global IP address to connect to slave centrals. If the central is in the same network as the master central, those two addresses are the same. If the slave central is located outside the network where the master central is, the slave's interface (local) IP address will depend on the remote network settings, and the global IP address in *Hardware editor* will be the IP address of the remote network, so the master central will be able to connect to the slave central. Usually in that scenario the port for a global IP address needs to be set (thiscan be done in the central's advanced settings).

5.2.3 Managing a central's WLAN interface

If the central has a USB port installed, the central can be connected via a USB Wi-Fi dongle to the existing wireless network. Connection requires the wireless network's name (SSID) and the network's security key to be entered.

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

The central's wireless settings can be accessed by clicking the "*Manage centrals"* button in the *Hardware editor* and then selecting *WLAN settings* in the *Options* menu next to the central's description.



Picture 5.5: WLAN settings

SSID and the security key needs to be entered into the corresponding fields. Connection can be established by selecting the button *Enable WLAN interface*. The central will enable the wireless interface and if the provided parameters were correct, it will connect to the provided wireless network.

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

After the wireless interface is enabled (confirmation dialog notice), network cable can be unplugged. Nova can be now accessed 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.

Clicking the *Search wireless networks* button next to the SSID field in the WLAN settings triggers a search for available wireless networks. A desired network can be selected from the list of discovered networks and populate the SSID field when the search is complete.

Wireless interface can be disabled by selecting the button *Disable Wireless interface* which is visible when the central is connected to a wireless network. Do not forget to connect the network cable back to the central or to configure the RS-485 network otherwise the connection with the central will be lost.

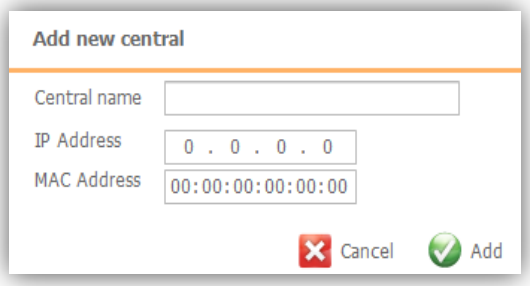
5.2.4 Adding, removing and editing centrals

New centrals can be added automatically to the system by clicking the "*Manage centrals"* button in the "*Hardware editor"*. The popup window, which opens, will contain a list of centrals discovered on the network. A new central can be added to the system by clicking the *Options* button next to the new central's description and selecting the option *Add new central.* The new popup window will contain all information needed. Only the central's name must be provided and the changes can be saved.

New centrals can be added manually by clicking the *Add central* button in the *Hardware editor* and then entering the central's information in the popup window (Picture 5.6): name of the central, IP and MAC address. When saved, the new central will be added to the list of centrals.

IMPORTANT! The central's default IP address and MAC address are written on the central.

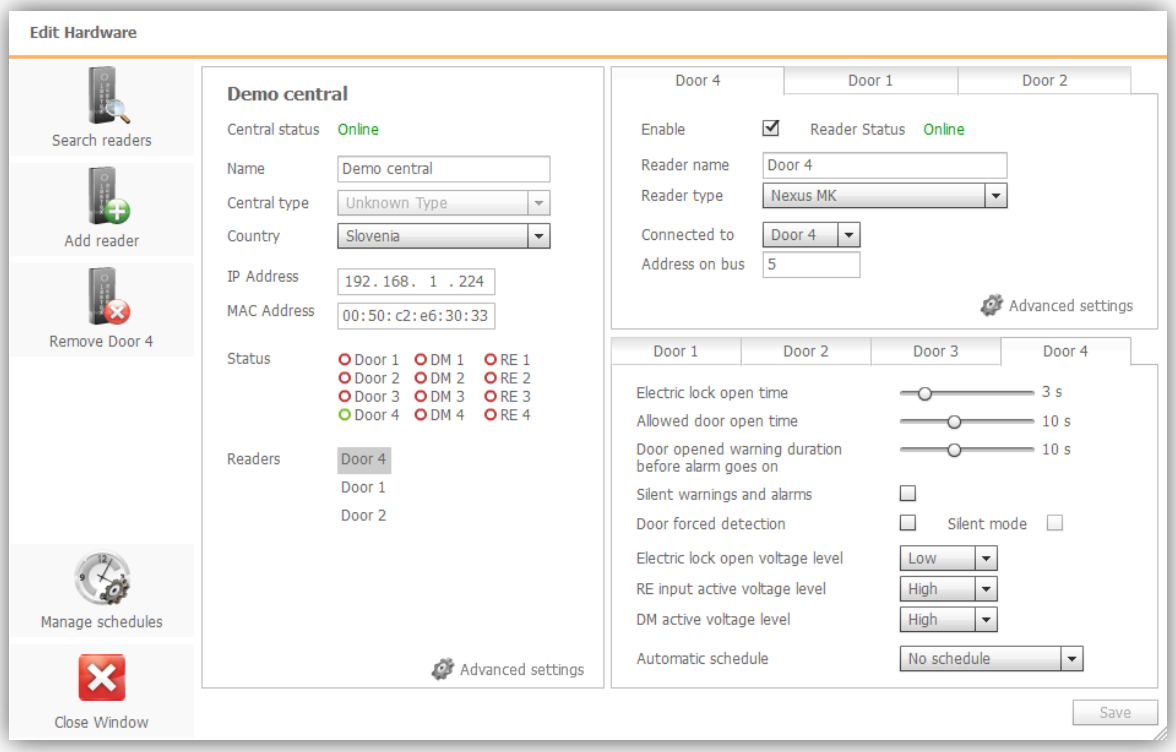
The central can be removed from the system by clicking the "*Remove central"* button in the "*Hardware editor"*.



Picture 5.6: Popup window for adding a new central

Any existing central can be edited by clicking the *Edit central* button in the *Hardware editor*. A *Central editor* popup window will be opened (Picture 5.7). The popup window is split into three sections: on the left side there are buttons for *searching*, *adding* and *removing* readers; the middle section holds details about the selected central and in the right part of the popup window there are tabs with the readers (on top) and doors (on bottom) connected to the central.

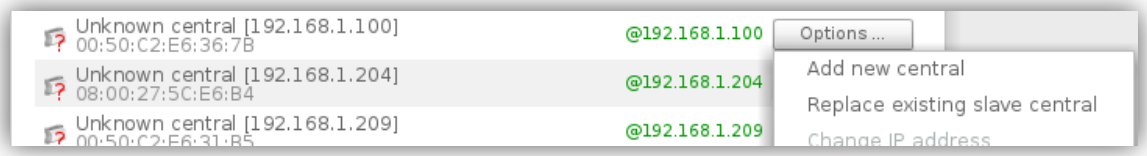
The central's name, IP address and MAC address can be modified. Additionally, for every central, a country can be set. This is valuable when the access control system is spanning over multiple countries and the used time schedules contain different dates for national holidays and other special days.



Picture 5.7: Central editor

5.2.5 Replacement of malfunctioned slave central

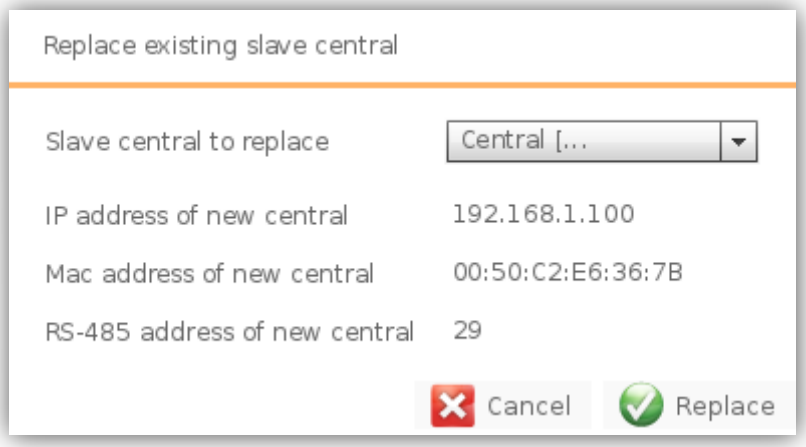
There are many reasons why a central can malfunction and needs to be replaced. Centrals usually have readers and user access groups assigned to them, preventing the deletion of the central. Because we want to keep all of its data and just replace the malfunctioned central, we can use the replace slave central function which can be found under manage centrals (Picture 5.4 above). To get to manage centrals window, on the main menu navigate to Locations & Hardware page→Manage hardware → Manage centrals→select the new slave central that is not in the system yet and select *Replace existing slave central* option. This option is only available for a central on a default IP address (192.168.1.100).



Picture 5.8: Replacing an existing slave central

A new popup show on Picture 5.9 will appear requesting a selection of a slave central that needs to be replaced and shows the information of the newly added central. If everything seems to be in order, a replacement is done by pressing the *Replace* button. Newly added central will get the data from the master of the system and adjust the time. Synchronization

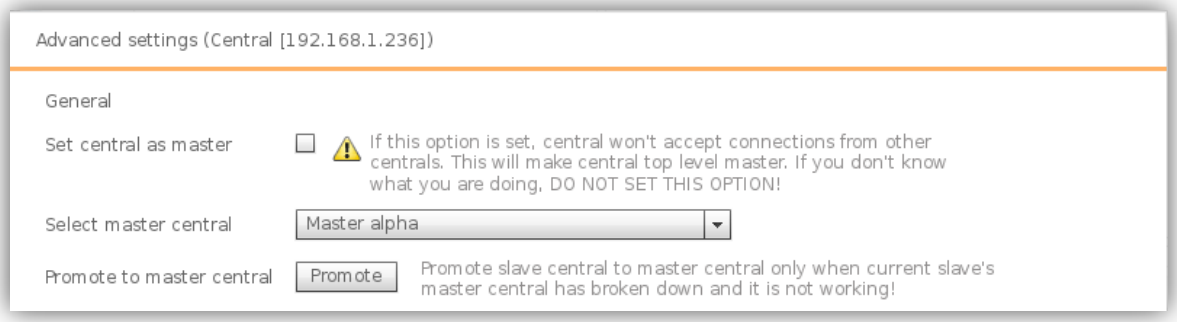
can take up to couple of minutes. After everything is done, the old central should appear online on the Hardware editor (Picture 5.3) and on the IP address of the old central.



Picture 5.9: Replace existing central pop-up

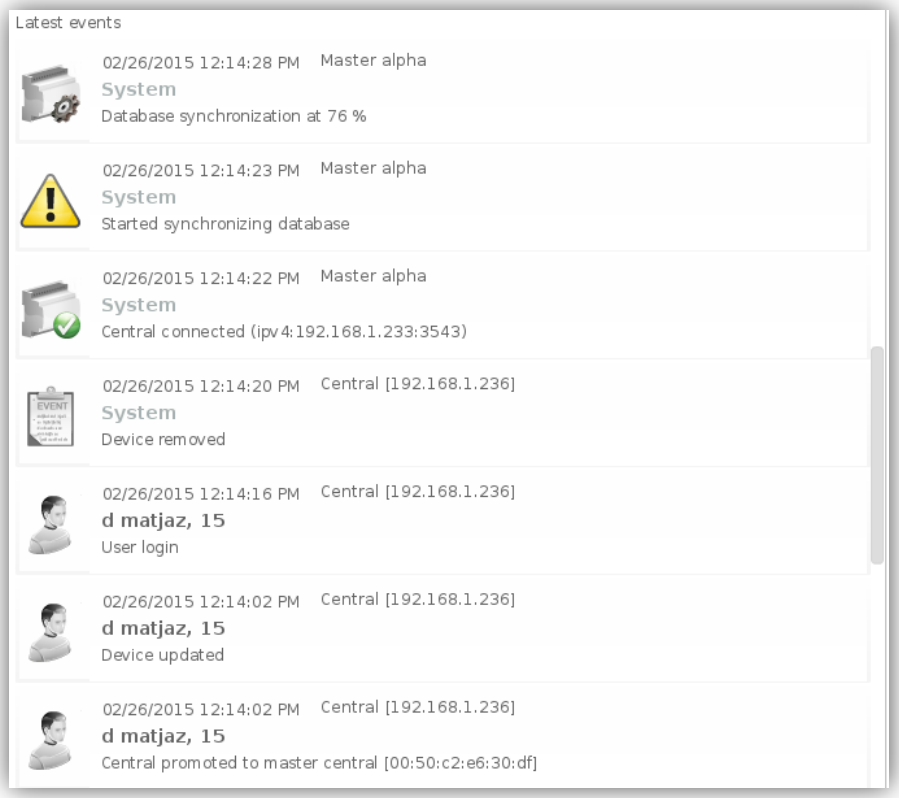
5.2.6 Replacement of malfunctioned master central

Replacing a master central is similar to the replacement of the slave central but more complicated process. In order to replace a malfunctioned master central, the new master central must be already installed in the system, central must not have any slaves connected to it and its master must be the malfunctioned central (current master).If the slave central meets the requirements, a *Promote* button will appear in the *Advanced settings* as shown on Picture 5.10. For a new master to be promoted, log into the slave's GUI and navigate to *Advanced settings*. These can be accessed by navigating from main menu to Locations & Hardware page→Manage hardware →Manage Centrals → double click on the current central (future master central) → on the pop-up window click *Advanced settings* located on the bottom of the window. The system will reassign all of the slave centrals including the malfunctioned master to the newly set master. Master reassignment and database synchronization can take couple of minutes to finish.



Picture 5.10: Option to replace malfunctioned master central

After confirming the master replace, all of the users will be logged out. Master central replace events are displayed on the Home and main navigation (Picture 5.11).



Picture 5.11: Central promoted to master central

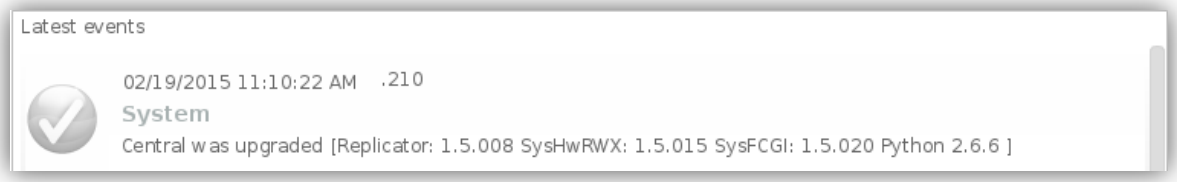
5.2.7 Remote software upgrade of the centrals

Nova version 1.5 and higher also supports remote software upgrade of the slave centrals. Note that both master and a slave must have proper software installed in order for remote upgrade to work.

To upgrade software on a remote central, navigate to Hardware menu and open up Hardware editor as shown on Picture 5.3. Select a slave central and check the description on the right hand side. Nova software version 1.5 and higher will display Software version and it's update link next to it as show on the Picture 5.12.

Picture 5.12: Central's software version

Clicking on Update link will bring forward the window requesting the latest software package. After the package is successfully uploaded to the master central, it will begin automatic transfer and upgrade. The procedure can take up to 10 minutes. After the upgrade is done, the slave central will be restarted and a new event (Picture 5.13) will appear on the Main page along with the all of the connected hardware.



Picture 5.13: Central's successful software upgrade

IMPORTANT! Remote upgrade can be done from a **master central ONLY**!

5.2.8 Advanced settings

The described settings are sufficient for simple system configurations (e.g. in access control with NovaSimpli software where there is only one central in the system). For advanced configurations with more centrals, with centrals in different networks or in the case where centrals share the same IP address, the system needs additional information which can be set in the central's advanced settings (Picture 5.15). The button is located in the lower middle part of the *Central editor*.

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

Configurations with more centrals are challenging from the settings point of view. The centrals are interconnected in a tree like structure, where each central can have one or multiple slave centrals and at the same time a central is the slave central to some other central. Most specific is the central, which is not the slave central to any other centrals. This central is called *system master central* and is responsible for serving the Nova application and for synchronization of the whole system. Other (slave) centrals are only synchronizing their slave centrals, if any, and are therefore called *local master centrals*.

Each central in the system needs to have an assigned master central (except the system master central). The master central can be assigned to a slave central with *Select master central* dropdown list under advanced settings. The *system master central* is set as default master central for all slave centrals and this is suitable in most cases.

System master central is top most central in the system and has only slave centrals assigned. In networks with more systems in the same subnet such master central can erroneously be added to another system. To prevent this scenario, a central must explicitly set to system as *master central* by checking "*Set central as master"* checkbox. With this option enabled, central will reject all incoming connections from other centrals. Slave centrals by default ignore incoming connections from centrals that are not set as their master central.

Port represents a setting that centrals communicate on with the other centrals over the network. The same port has to be forwarded on the router for external (over the internet) communications. The default port is 3543 and it's best to keep it this way.

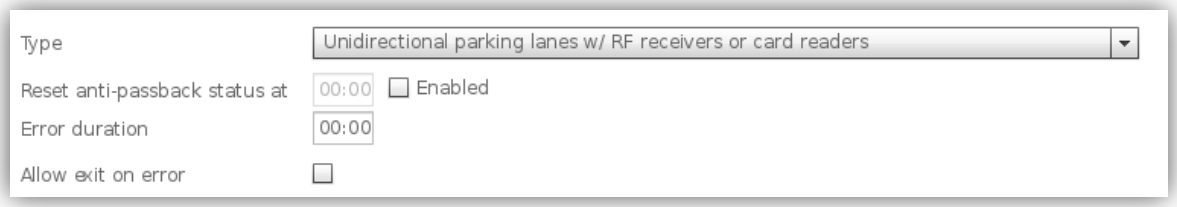
Database synchronization allows the system administrators to copy master's database to overwrite slave's one. After selecting the button, the events with update progress will show the on the Home page as the events come in. After the database synchronization is done, the master central will update slave's time as well.

Selecting the "***Reboot***" button will remotely restart the central.

Nova software version 1.6 supports the **upgrade of all of the readers** on a single central. By selecting the "*Upgrade firmware"* button and selecting the software from the computer will begin to upgrade all of the connected readers on the target central.

Anti-Passback settings

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. The settings can be enabled in the "*Advanced window"* shown on of the target central (to see how to get to this window, see chapter 5.2.8).



Picture 5.14: Anti-passback settings

There are numerous ways of setting up the function depending on the type wanted:

- Bidirectional parking lane with one RF receiver.

This example only uses a single ramp for entry and exit from the parking space. The direction on the RF receiver must be set to "*I1 Entry - I2 Exit"* (description on how to set is explained in chapter 5.2.14 Reader settings).

- Unidirectional parking lanes with RF receivers on card readers.

This method was meant for parking spaces with separated entry/exit ramps. E.g.: When the costumer's car stops at the entry, *Input 1* 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 make this method work, direction must be set to "*I1 Entry - I2 Exit*". The description on how to set reader's directions is described in chapter 5.2.14 Reader settings.

IMPORTANT! If Door monitor on Entry is set to NO, automatic schedule might open door and because of the timeout alarm to go off when the car leaves ("Input activated"). If the Door monitor is set to NC, and door on Entry is opened, when the car is at ramp for too long the alarm will trigger the same. To solve the alarm problem, DM active voltage level must be set to Unused.

- Bidirectional door with card readers.

To make this choice work, there have to be at least two (2) readers connected to the system. One of the reader's direction has to be set on "*Entry*" while the other one has to be set on "*Exit"*. How to set reader's directions describes chapter 5.2.14 Reader settings. The system keeps track on when the user places his/her card on the reader's entry/exit.

- Bidirectional doors with card readers and DM confirmation.

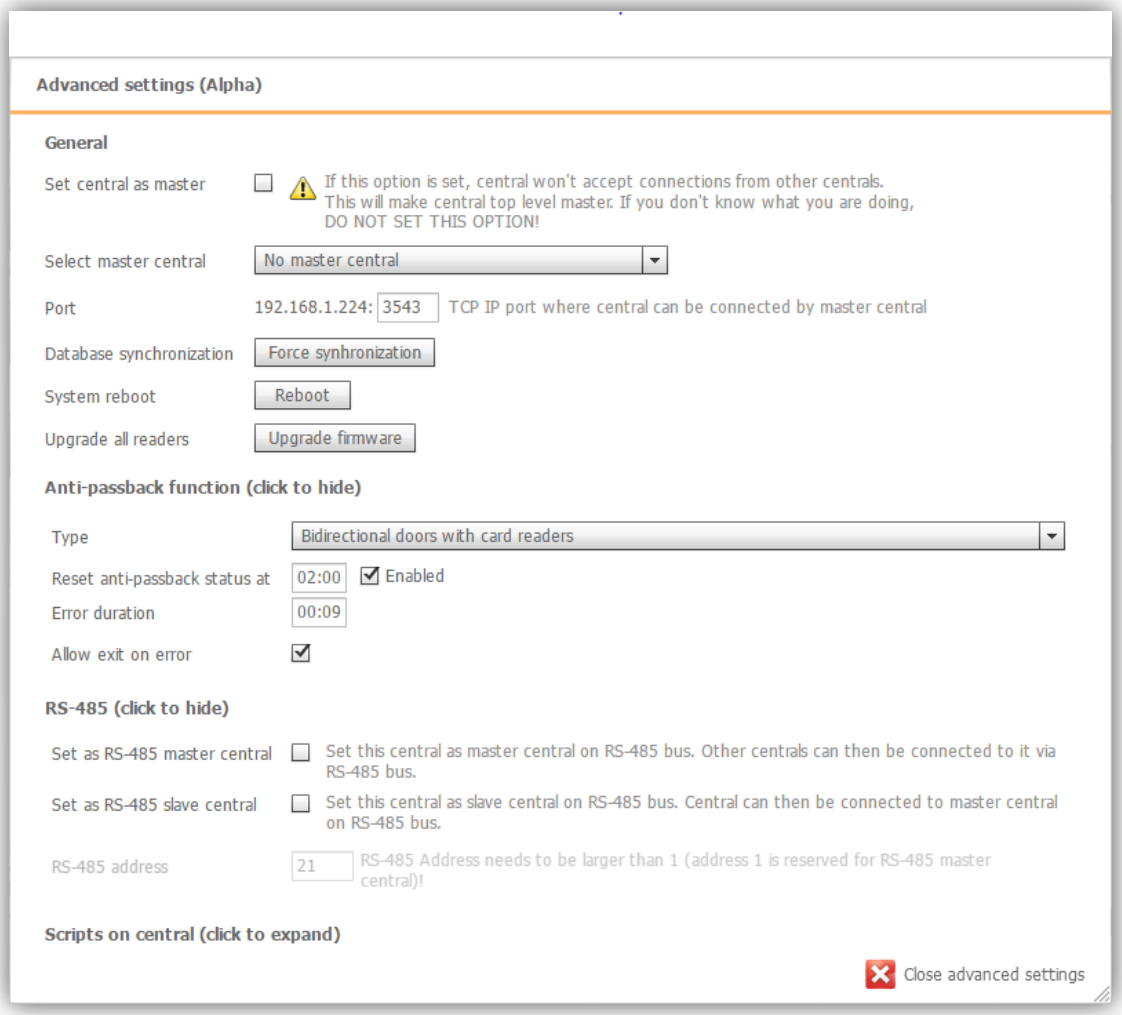
Option with "DM confirmation" works on the same general principle as the previous one. The main difference is the tracking of the doors. When the doors are opened, the door monitor activates and the user entry is counted when door closes.

- Turned off.

Decision disables Anti-passback functionality.

Reset of the anti-passback status shown on can be enabled by checking the checkbox next to it. Setting will enable the reset status for all users at the selected timer. This reset can be done manually trough the user settings – chapter 4.1.3 Setup and managing users and access rights.
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 premises but he entered with someone else's entry card. If he wants to get out he can't, because his/her card was never put on entry reader. Allowing "*exit on error"* will allow him/her to exit with their own card.

Centrals are connected to each other either through an IP network or a RS-485 bus. The RS-485 bus is much slower in comparison to an IP network because information can only be sent in one direction at any time and as a result not recommended. Larger database updates to the slave centrals might take several minutes per central on the RS-485 bus.



Picture 5.15: Advanced settings

5.2.9 Communication based on IP address

The communication between the master and a slave central is based on the IP address, set in the field *IP address* in the *Central editor* (Picture 5.7), and on the IP port, set in the field *Port* in the central's *Advanced settings* (Picture 5.15).

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

When both centrals are on the same network, the *IP address* in the *Central editor* needs to be the same as the interface IP address of the central (see the section on changing a central's IP address). The interface IP address is always related to the network in which the central is located. The port needs to be set to 3543.

When a slave central is located in a remote network (from the slave's master point of view), the field IP address in the Central editor **needs to be set to the address of remote network**. The address of the remote network is not the same as the interface IP address of

the remote central. The same goes for the field Port in advanced settings. The port needs to be set to the port number of the remote network, which is forwarded to port 3543 on the remote slave central.

5.2.10 Communication based on RS-485 bus

When a slave central is connect to the master central via a RS-485 bus, option *RS-485 master central* must be enabled, located in master's "*Advanced settings*" (Picture 5.15). *Set as RS-485 master central* checkbox must be ticked. This setting causes that the master central becomes aware of slave centrals on RS-485 bus.

After setting a master, the similar process needs to be set for every RS-485 slave central. *Set as RS-485 slave central* in the slave's advanced settings. For assigning a slave RS-485 central, the master's centralRS-485must be enabled.

The communication between centrals on the RS-485 bus is based on the RS-485 address and is set in the field *RS-485 address* under the central's advanced settings. 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 written on the central.

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

Example of RS-485 addresses 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 14.1 for at least 10 seconds. This 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 the port to 80). It also enables the super administrator's account again, if it was disabled. See appendix A for more details.

5.2.11 Database synchronization

The system master central takes care of data synchronization between centrals in the system. In case where a central's database is incomplete, a manual synchronization can be done. Clicking the button *Force synchronization* in the slave's advanced settings will cause that the master central updates the database on the slave central with the copy from the master central. This option should be used only when there is a certainty that differences between database data exist.

5.2.12 Adding new readers

New readers are added to the central by clicking the *Search readers* button located in the upper left corner of the Central editor (Picture 5.7). This triggers recognition of the already connected readers and search for readers newly connected to the central. After the search is completed, the addresses of listed readers can be changed and the new readers can be added to the central. The address can be changed by writing a new address, replacing the old one and confirming the change by clicking on the option *Change Address* in the *Options* menu. Upon a new reader search, a new address will be shown.

IMPORTANT! If reader's address is changed, it remains physically on the reader. The only way to change it is to manually change the address in the "*Central editor"* under "*reader settings".*

If the reader's address and the doors to which the reader is connected are known, the reader can be manually added by clicking the "*Add reader"* button.

Existing readers can be removed from the central by clicking the "*Remove reader"* button.

5.2.13 Upgrading firmware on reader

The readers' firmware can be upgraded to a newer version byselecting the "*Search readers"* button in the upper left corner of the Central editor. When the search is completed a list of readers connected to the central will appear. The option "*Upgrade firmware"* has to be selected that displays under each reader's *Options* menu. In the popup window, a file with ".bin" extension needs to be selected to update it with the new firmware. The upgrade process will start and will last for approximately 30 ~ 120 seconds (depending on the central's workload and the port to which the reader is connected). During the upgrade process, an operation status dialog will be displayed. The reader will beep three times after the upgrade process is done.

IMPORTANT! Centrals with Nova version 1.5 or lower need to update its 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 will be disabled on readers that cannot be upgraded.

5.2.14 Reader settings

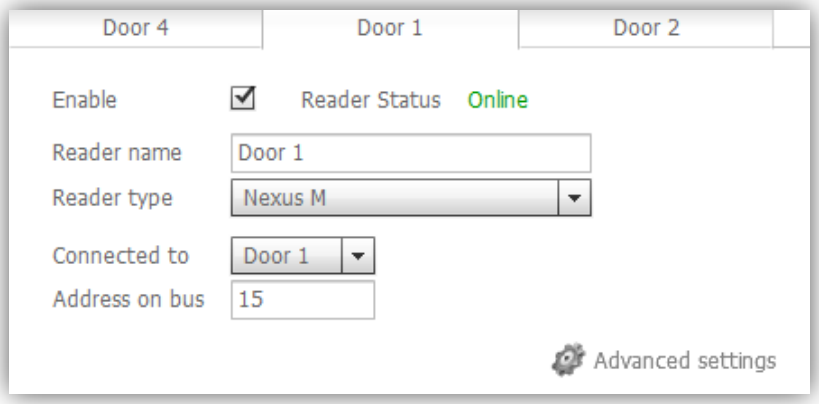
The reader needs to be configured correctly and linked to the desired door for the system to function correctly.

When the reader is selected (Picture 5.16), its "*Online/Offline"* status is shown. Along with the state of "*Enabled"* flag, the "*Reader name"* and the "*Reader type"* are displayed. If the reader is not working or it is not needed in the system anymore, it can be disabled by deselecting the "*Enable"* checkbox. In this case, the central will seize to communicate with the reader and its warnings and errors will be removed from the "*Home"* page.

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

The door that the reader is connected to has to be set. The address and the door will now be controlled by that reader. The reader is usually connected to the same door it controls, but it is possible for a reader to control another door on the same central (the option to set it is found under the reader's "*Advanced settings"* and it is not included in the NovaSimpli software).

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



Picture 5.16: Reader settings

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

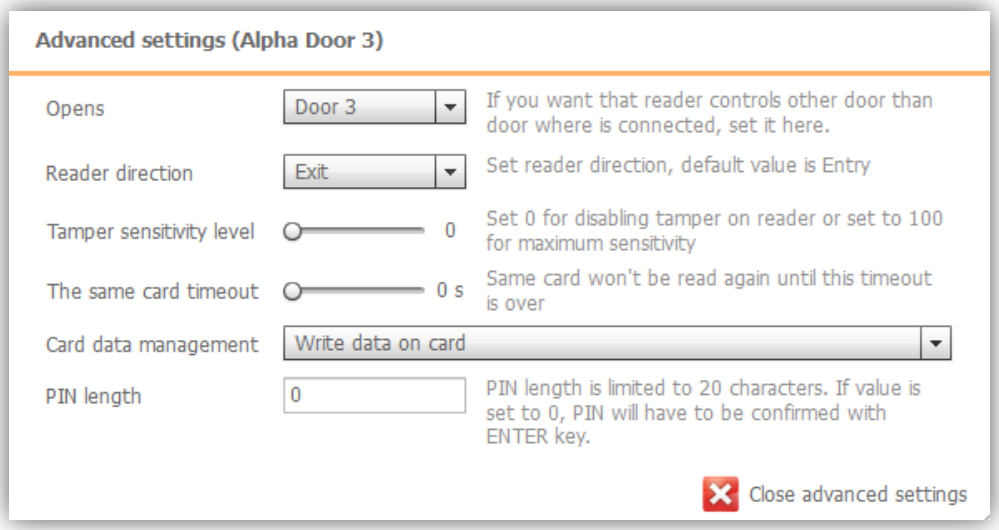
Picture 5.16 shows the settings needed for basic operation. Additional parameters can be changed by selecting the button "*Advanced settings"* (Picture 5.17): The option to set the sensitivity on the **tamper sensor,** the **direction** for each reader ("*Entry"*, *"Exit"*, "*Pass through"*, *"I1 entry – I2 exit"*) and select the **different doors** which the reader controls.

There is also an option to enable writing of access rights to user's cards (the option is only visible, if the reader supports it). Those rights are then read by offline readers (see section *5.3Offline readers* for a detailed description).

Additionally, a setting set for the value of the "*Same card timeout".* This setting enables a timeout on the central before a card from the same user will be processed 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, which is set here, passes. The central will process cards from other users in this time.

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

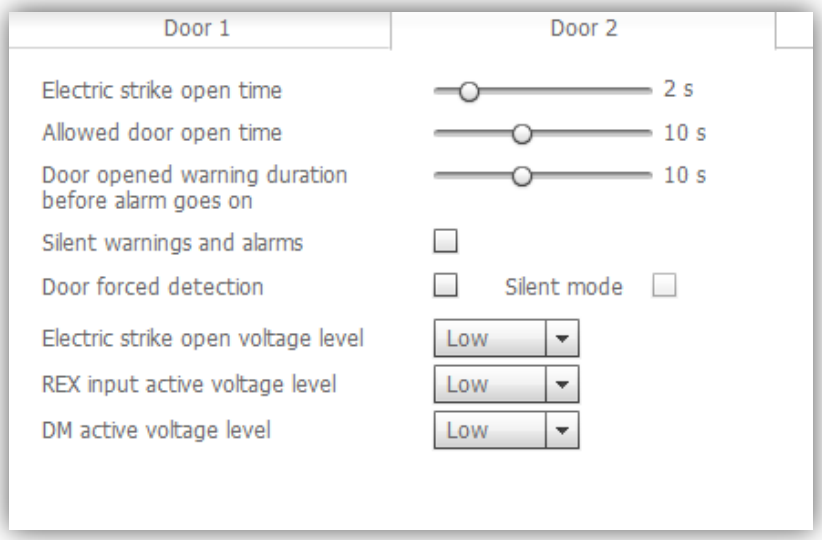
Value in "*PIN length*" field defines how users enter their PIN on current reader. If the value is set to a number greater than 0 then PIN is accepted as soon last number is pressed. Value set to 0 means that users will have to confirm their PIN with the ENTER key on keyboard. Remember that for the first case when length of the PIN is defined, PINs of all users will have to match here defined length. If PIN length will be shorter, users will have to use ENTER key.



Picture 5.17: Reader's advanced settings

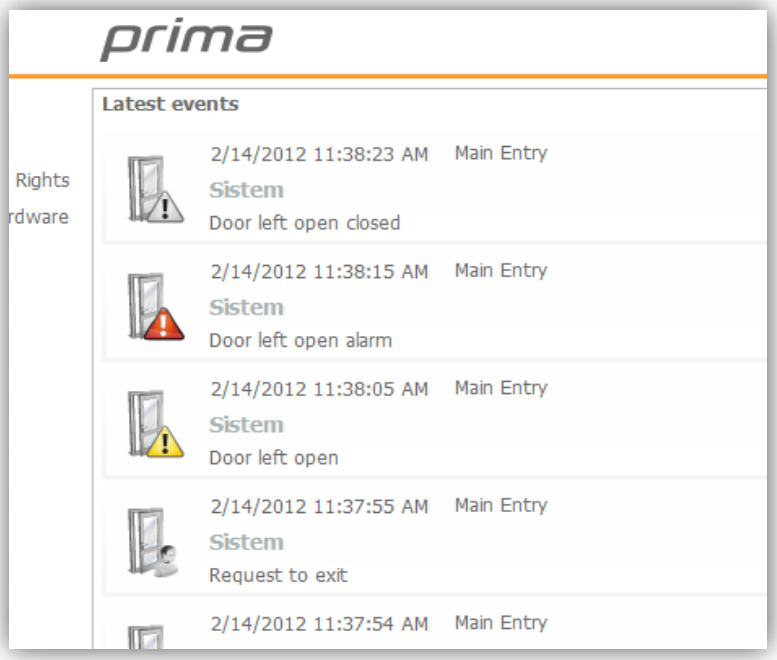
5.2.15 Door settings

Picture 5.18 shows the settings for doors on the central. There are many settings that can achieve a desired door behavior. The setting for electric lock open timeout ("*Electric lock open time*"), the allowed time for a door to stay open ("*Allowed door open time*") and how long a reader should warn user to close the door before the alarm turns on ("*Door opened warning duration before alarm goes on*").



Picture 5.18: Door settings

Picture 5.19 shows the relation between the described times. The door was opened at 11:37:55 and stayed open. Ten seconds later the reader started to warn the user with a beeping sound that door should be closed (11:38:05). The user did not react on the warning, so ten seconds later the alarm went on (at 11:38:15). The user finally closed the door at 11:38:23. The settings on the door were the same as shown on Picture 5.18.



Picture 5.19: Doors left open and alarm times, example case

If the administrator does not want the reader to make any sound at warnings and alarms, he/she can set the option "*Silent warnings and alarms*".

The option "*Door forced detection"* is used when there are doors with readers on each side. In this case the central has total control over the door and it can detect if the doors are not opened by readers and will trigger a "door forced" alarm. Administrator can choose the *Silent mode* option if he/she does not want the readers to make any sound on door forced detection.

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

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 that are uses in the system.

The options "*RE input active voltage level"* and "*DM active voltage level"* need to be set according to the system's characteristics. The central will open the door when the signal level on RE input (Request to exit) will match selected state and will know that the doors are open when the state of the DM signal will match the selected state (High or Low).

If there is a need to use DM and RE inputs with "*Scripting module"*, the option can be set to "*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.

5.2.16 Scheduled door opening

Picture 5.18 shows door settings for the NovaSimpli software. In other versions of the Nova software there is an additional option: A schedule can be selected from a drop down list and assigned to target doors. Doors will automatically lock and unlock based on the time intervals of the selected schedule (see part 4.2.1 for Managing time schedules). The "*time schedule editor*" can access for editing and previewing schedules from the *Central editor* by clicking the "*Manage Schedules"* button.

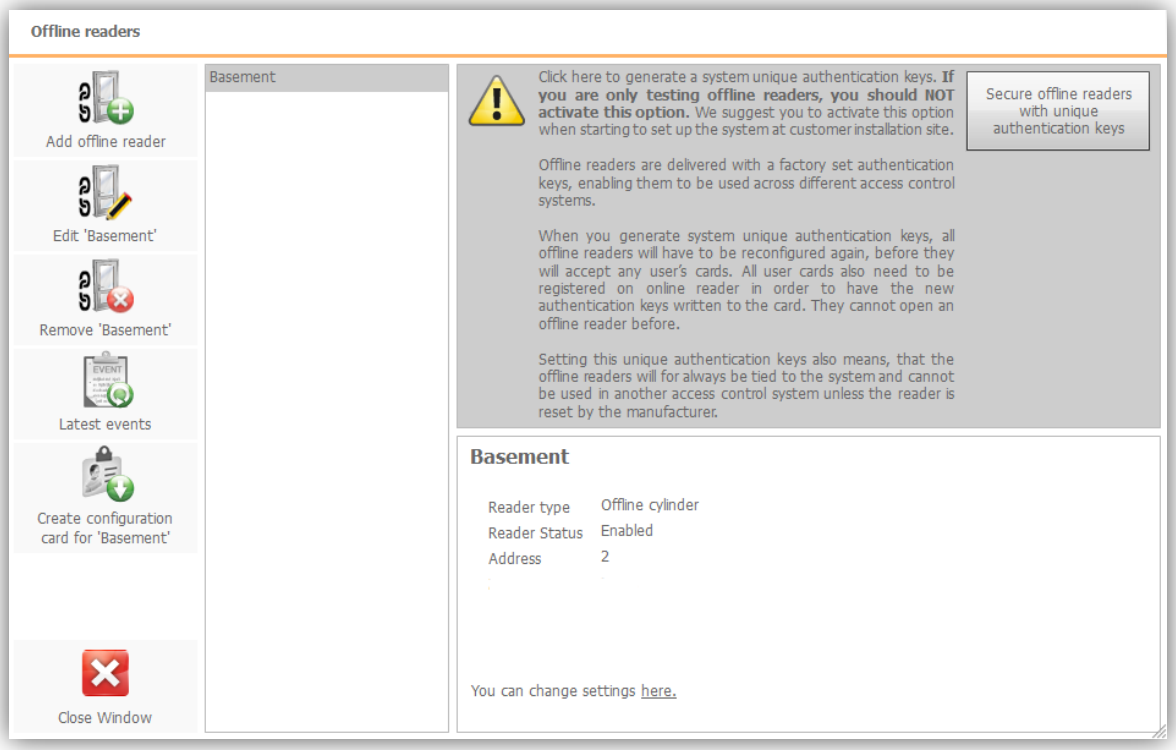
TIP: The option to automatically lock doors can be assigned by an automatic schedule with defined time interval of 1 minute that ends on time when doors needs to be locked.

5.3 Offline readers

Offline readers are stand alone units that act as part of an access control system when they are correctly configured. The management of offline readers is done through the Nova software with help of contactless read/write cards. When a card is registered on an online reader, the user's access rights are written to the card. When this card is later used on an offline reader, the data is read from the card and access is either granted or denied (it depends on the access data written to the card). The same principle applies for the offline reader configuration.

Offline readers can be managed with the "*Offline reader editor"* seen on Picture5.20. The editor is opened by clicking the "*Manage offline readers "*button in the main menu under *Locations & Hardware –> Manage Hardware.*

On the left side of the "*Offline reader editor"* there are the buttons for management of the offline readers and a button for creating a configuration card for the selected offline reader. Next to them, a list of all the offline readers in the system can be found and on the right side is a preview of the currently selected offline reader (Picture5.20).



Picture5.20: Offline reader editor

IMPORTANT! System is using default authentication keys on Mifare cards until they are changed manually by clicking on *Secure offline readers with unique authentication keys* (Picture5.20). It is advisable to change authentication keys before adding the first offline reader to the system. This way ensures that users cards and newly added offline readers use the secured authentication keys from the beginning. Before changing the authentication

keys to already set system, keep in mind that all users cards and offline readers will have to be re-configured with the new authentication keys.
When adding a new or editing an existing offline reader, administrator can change its name and its type. Address of the reader is generated automatically by the system. This address differentiates between offline readers in the system (Picture5.20).

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

Based on the reader's type, there are some other settings that can be customized regarding the behavior of the offline device. The options that are not supported by the offline reader are grayed out (Picture 5.21).

The time sliders offer the same functionality as for online readers (for detailed information see chapter5.2.15Door settings for online readers). This allows the option to set different kinds of timeouts for the offline device.

To trace users, the option has to be unchecked at "*Disable events log on user's card".* The offline reader will then write the time when a card was registered on a reader to the user's card and this data will be copied to the system the next time the user will use his card on an online reader. This option uses more battery on the offline reader.

Offline devices have an internal log of all events. These can be transferred to the system with the *events card* (for information on how to create an events card, see the section4.1.2Card role assignment). Disabling the log can be done by checking the option "*Disable event log on offline reader"*.

The security can be increased by requesting that a user also enters his PIN number when entering a door with a card by checking the option *Request input of user's pin*. This option is only available, when the offline reader has a keypad.

When checked, the *"Ignore Toggle" output setting on user's cards* option bypasses any settings, which is written on cards that normally causes the device to enter toggle mode, where the device toggles its state and stays in that state until the next time a card with toggle rights is registered. This setting can be set in the "*User editor"* popup menu under "*Cards Settings"*.

When "*Check time schedule on user's cards"* is enabled, it instructs the offline reader to check the time intervals written on the card. If the current time is within the time boundaries written on the card, the user will be able to open the door. The schedule with time intervals can be set in the "*User editor"* popup menu (see Picture 4.4) under *Cards Settings* (if there are more time intervals defined under the selected schedule, only the first two intervals will be used on user's cards).

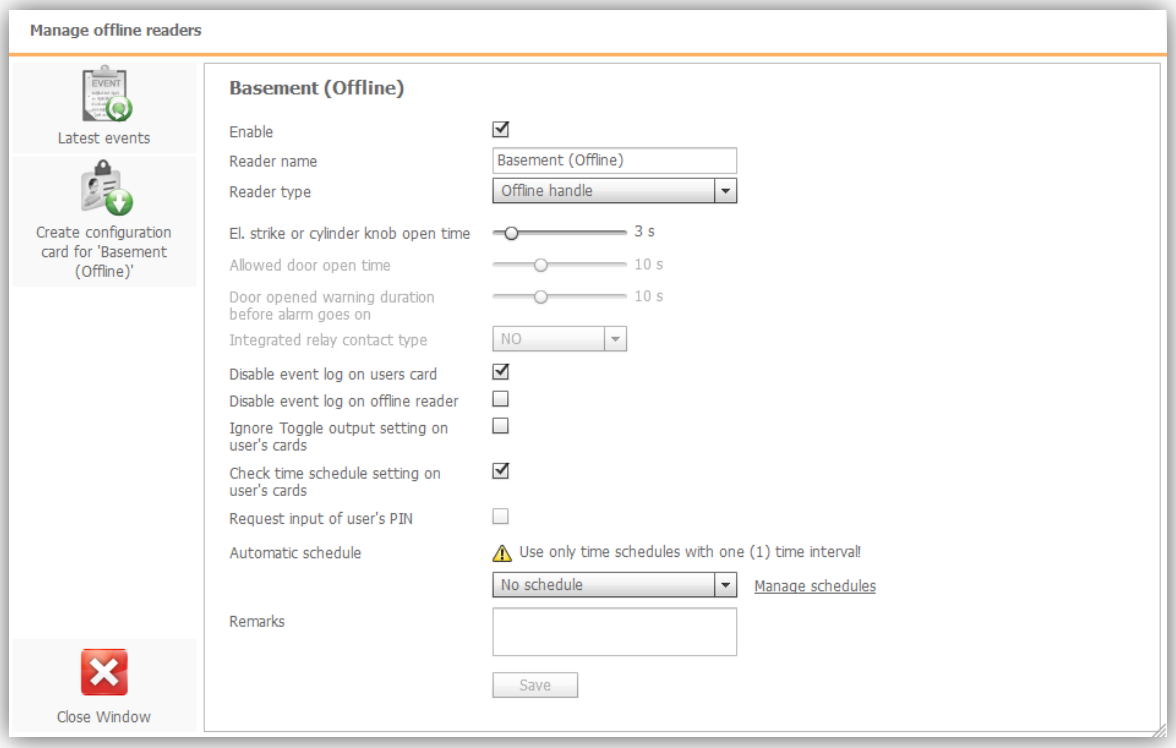
An offline reader has the option to be automatically locked or unlocked by means of an automatic schedule. Schedule can be selected from the drop down list at "*Automatic*

schedule", and the reader will act accordingly after reconfiguration (if there are more time intervals defined under selected schedule, only the first interval will be used for automatic function). The "*Time schedule editor"* can be accessed for editing and previewing schedules from the editor by clicking the "*Manage Schedules"* link (see part 4.2.1).

TIP: The doors can automatically lock by assigning them an automatic schedule with defined time interval of 1 minute that ends on time when doors needs to be locked.

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

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



Picture 5.21: Offline reader settings

5.3.1 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 labeled according to their functionality:

- Blacklist card (card used to transfer the list of lost cards to an offline reader).
- Events card (card used for transfer the list of events from an offline reader to the central).
- Configuration card (card for transferring configuration settings to an offline reader).
- Battery card (card for replacing batteries on an offline reader, if applicable).

- Disassembly card (card for disassembly of an offline reader, if applicable).

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

All cards, with the exception of the Configuration card, work on all offline readers after they have been registered on an online reader and data has been written to them. The configuration card needs to be created for the individual reader every time because of access configuration details.

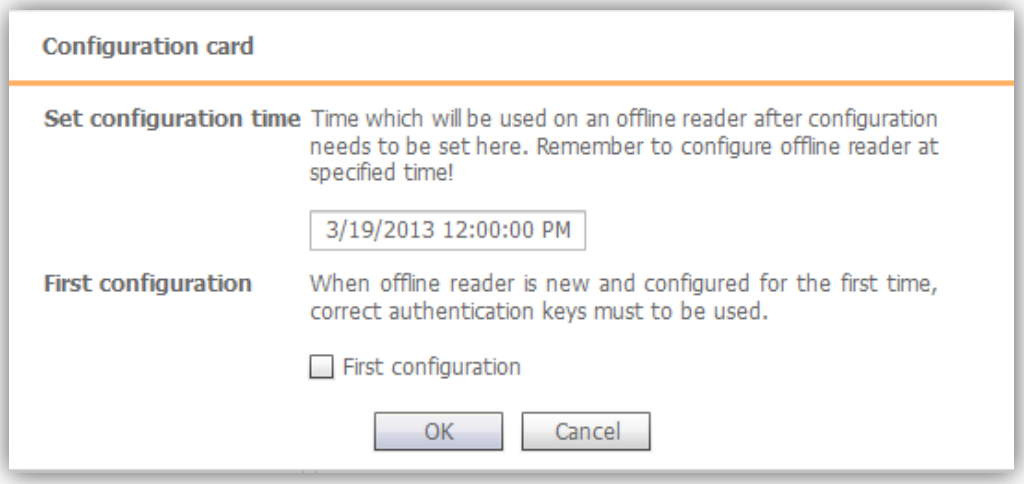
There is also special card type "*Format card*", which when assigned to card, clears all of the data content from card when card is presented on online reader.

5.3.2 Creation of configuration cards for offline devices in Nova software

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

A new configuration card can be created by firstly selecting the offline reader in the *offline reader editor* (Picture5.20) and then clicking the button "*Create configuration card*". In opened popup time of device configuration must be set. This is used for time synchronization between online system and offline reader (Picture 5.22).

When adding a new offline reader to the system, make sure the "First configuration" option is checked which will insure the use of the right authentication keys on configuration card. Option is visible only when unique authentication keys are generated for the system.



Picture 5.22: Create configuration card

After confirming the settings of the configuration card, the configurations need to be uploaded. To do so, put the *configuration card* on an online reader that is enabled and has

the ability to write data on cards. The configuration settings will be written to the card and there will be three "beep" sounds after the successful write.
IMPORTANT! There is a 15minutes period to register the configuration card on an online reader. After these15minutesthe procedure will have to be repeated.
The configuration card then needs to be registered on an offline reader for which it was created and it can only be used once. The offline device will signal the successful operation with three long and three short "beep" sounds. Remember to configure the offline reader on the set time from the pop-up window.

5.3.3 Lost cards, blacklist and offline readers

Users' cards that get lost can be blocked on offline readers to prevent unauthorized entries. Offline readers will ignore cards which are on their blacklist.

IMPORTANT! Each card reported as lost needs to be marked as a lost card in Nova under the owner's card settings, where the role of the card needs to be set to "*Lost card"* (see the section on adding users for information how to change the role of the card).

The database of *lost cards* is transferred to offline readers with the *Blacklist maintenance card* (card with assigned *Blacklist card* role). When such card is registered on the online reader, all cards with the role *Lost card* are written to it. Offline readers will read the ID numbers of lost cards from the Blacklist maintenance card, when the Blacklist maintenance card is registered on them.

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

When a lost card is found and administrator wishes to remove it from the blacklist on the offline readers, he/she first needs to change the role of the card in Nova to *Card* and then repeat the procedure described above.

5.3.4 Reading events from offline devices

Offline devices keep track of internal events and can keep track of users' events. Events are stored on the internal storage of the device and to transfer them to Nova, "*Events maintenance card*" must be used(card with assigned *Events card* role). Same *Events card* can be used on all offline devices – one at a time.

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

The transfer of events can be done with the registration of "*Events card"* on the offline device from which the events can be transferred. They are written to the card, which then needs to be registered on an online reader. The online reader will read events from the *Events card* and make them available in Nova.

IMPORTANT! Events are deleted from the offline device's internal storage after they have been transferred to the "*Events card"*. Remember to register the "*Events card"* on the online reader before reading events from another device!

5.3.5 Configuration of online readers' settings for writing access rights

Data transfer between the central and an offline reader is done by writing data to a contactless card. This data is then read by the offline reader. Writing large quantities of data to a card is a time consuming task, so to guarantee the best user experience, the data writing is usually only done on readers at entry points to buildings. Reader's writing ability and its writing access rights to cards can be enabled by going to the reader's "*Advanced settings"* and enable writes with the option in "*Card data management"* dropdown list showed on Picture 5.17.

5.3.6 Offline readers and Nova software

Offline readers act in the same way as online readers in the Nova software. They only differentiate from online readers by having a different icon in the hardware tree (they do not show the current door status) and when assigning access rights to those readers, administrator does not have the option to select a time schedule, action and source identification device. They are pre-selected and fixed to a '0-24h' time schedule with the actions "OPEN" and "CARD" as source identification device.

5.3.7 Battery level on offline cylinders

SensoLock®, the offline cylinder, has a built-in battery management. It has a3 different phases to displays battery capacity and when replacement is necessary. It is also possible to see the battery status in the Nova software, if there is the "*Offline+"*activation key registered in the system.

The low battery level can be discovered in three phases:

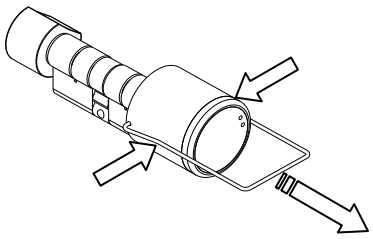
1. Alight and sound signal appears when a tag/card is held in front of the cylinder knob. Change the batteries using the *battery card* and the battery tool as described in section 5.3.6.
2. Alight and sound signal appears when a card or piece held in front of the cylinder knob. Due to low battery level it will take5 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 5.3.6.
3. The cylinder will not read any activated tags/cards. When the cylinder is in phase3, 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 5.3.6.

5.3.8 Changing batteries in offline cylinders

Assigned battery card (for description on card assignment read section 4.1.2)is used to replace dead batteries in offline cylinders.

When the card is presented to the cylinder, the two small tabs on the side, which normally keep the cap in place, are weakened (the battery change tool can help with to removal of the cap) and the two CR2 3V Lithium batteries can now be replaced.

IMPORTANT! Be aware of the correct placement of batteries according to plus and minus!



When the batteries are placed correctly, push the cap back onto the cylinder, and make the tabs fit in the holes of the cap, before presenting the battery card to the cylinder again, which will lock the tabs.

5.3.9 Offline device feedback

Offline devices give feedback to users in the form of sound and light signals. Signals can consist of any combination and number of short or long "beep" sounds along with any combination and number of green and red LED flashes on the device. Table 5.1 summarizes different functions and feedbacks from the device.

	SensoLock, LockerLock		Offline Nexus, PrimaLock	
Function	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	5s ○ 5X ○	o o o o o	5s ○ 5X ○
Battery warning Phase 3	o o o o o	5X ○	o o o o o	5X ○

● green LED on
○ green led blinking
○ red LED blinking
● red LED on

– long low beep
- short low beep
o short high beep

Table 5.1: Functions and feedbacks of different offline devices

5.4 Special hardware devices

5.4.1 GSM Gateway

GSM Gateway is an advanced GSM communication device that can be used for remote control of access control system. Whenever user calls on the gateway's phone number or sends SMS to the device, system recognizes users phone number as an identification source and grants access if applicable. In combination with *Scripting module* GSM Gateway can be used for remote control of different devices connected to the Alpha central's outputs.

GSM Gateway is installed to the Alpha central in the same way as contactless card readers. When device is properly wired to the central it can be discovered through Nova software under central's editor with the option *Search readers*. For more information about adding new devices to the central see chapter*5.2.12Adding new readers*.

GSM Gateway's default *RS485 address is set to 1* and can be changed to meet system requirements.

IMPORTANT!GSM gateway needs working micro SIM card for normal operation (please refer to devices manual for instructions on how to properly install SIM card). If card is not inserted into the device, Alpha central will not be able to be discovered on RS485 bus.

IMPORTANT! GSM gateway stores its configuration on the SIM card (RS485 bus address, ...). When preconfigured SIM card is inserted into device, configuration is restored from SIM card. Please note than changing SIM cards between devices will also change RS485 addresses of those devices and system reconfiguration will be needed.

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

5.4.2 Remote control Reader

Remote control reader is a RF (radio frequency) receiver device used to receive signals from RF remote control key chains. Usually it is used to control parking ramps or garage doors where usage of classical contactless cards is not practical.

Remote control reader is installed to the Alpha central in the same way as contactless card readers. When device is properly wired to the central it can be discovered through Nova software under central's editor with the option "*Search readers"*. For more information about adding new devices to the central see chapter*5.2.12 Adding new readers*.

When button on RF remote control keychain is pressed RF signal is transmitted by keychain and received by remote control reader. RF signal is decoded and shown in the Nova software as an integer number. This number can then be added as an identification device to the selected user in the same way as contactless cards.

For more information about adding new cards to user see chapter *4.1.1Adding unknown card(s) to user*.

6 Settings page

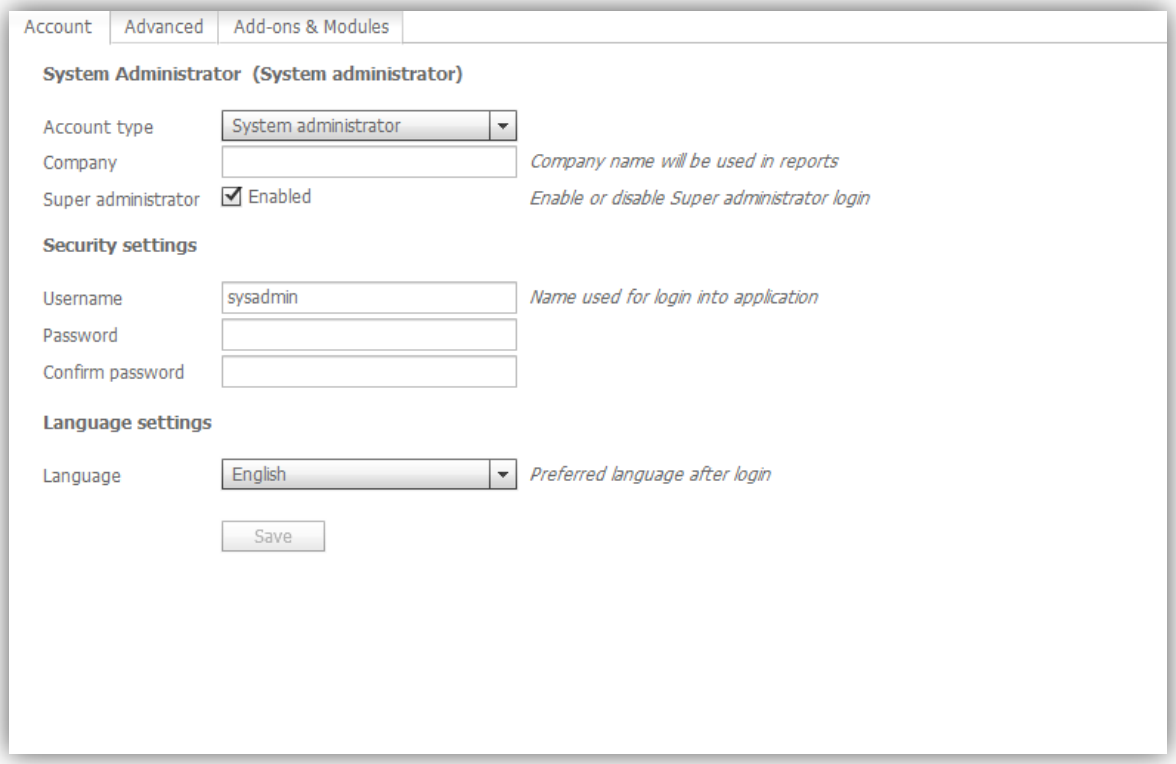
Settings page can be accessed through the main navigation menu. Multiple tabs will be presented for different kinds of settings.

6.1 Account tab

The *Account* tab is used for managing own user account. From here, username, password and default language can be changed upon re-login (Picture 6.1).

WARNING! There is also the option to change the type of currently logged in account. Selecting the option "No access to application" and saving the changes, will prevent current account to sign in the future! Use this option only when disabling own account.

System administrator can disable the super administrator's account by unmarking the checkbox *Super Administrator*. The super administrator's account is used by developers in case of errors.



Picture 6.1: Account settings

6.2 Advanced Tab

The *Advanced* tab is used for more advanced settings and is only enabled for system administrators.

From this tab databases can be downloaded or uploaded. When uploading a configuration database with new settings, proceed with caution! In case of a damaged database file, the whole system can stop working. We recommend backing-up of the old configuration database prior to uploading the new file.

To download the database file with all events in the system click the "*Create backup file*". The database files can now be stored on local computer.

6.2.1 Automatic database backup

Nova version 1.5 and higher support automatic backup of the configuration database shown on Picture 6.2.

Picture 6.2: Different copies of backups from central with USB storage

Automatic database can be set on *"Turned off", "Daily", "Weekly"* or *"Monthly"* backup. Each option represent time period of backup creation. A new copy of configuration database will be created every set time 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 1st day of the month at 2:00 AM.
- Turned off will stop backup creation.

Backup configuration can be set on master central and applies the rule to the all of the centrals in the system. Centrals with proper backup USB storage inserted will create a copy on them instead of the local memory. Additionally, they will also create a copy of an events database and all of the user pictures along with it.
Centrals will also store copies of previous backups for a time period. If the backups are set and stored on local memory, it will keep three (3) copies of the last periods (e. g. if the automatic database backup is set to daily, it will keep backups for the last three (3) days, for weekly - last three (3) weeks and for monthly - last three (3) months). Centrals with USB storage connected will keep up to seven (7) copies of configuration and event databases.

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

6.2.2 Web server port

Sometimes central's GUI needs to be accessed from the internet but something is already occupying default http port (80). In this case internal ports can be changed and forewarned to meet the needs. Nova software currently supports five (5) different ports: 80, 81, 8000, 8080 and 8181. After the port is changed, GUI will automatically restart. 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.

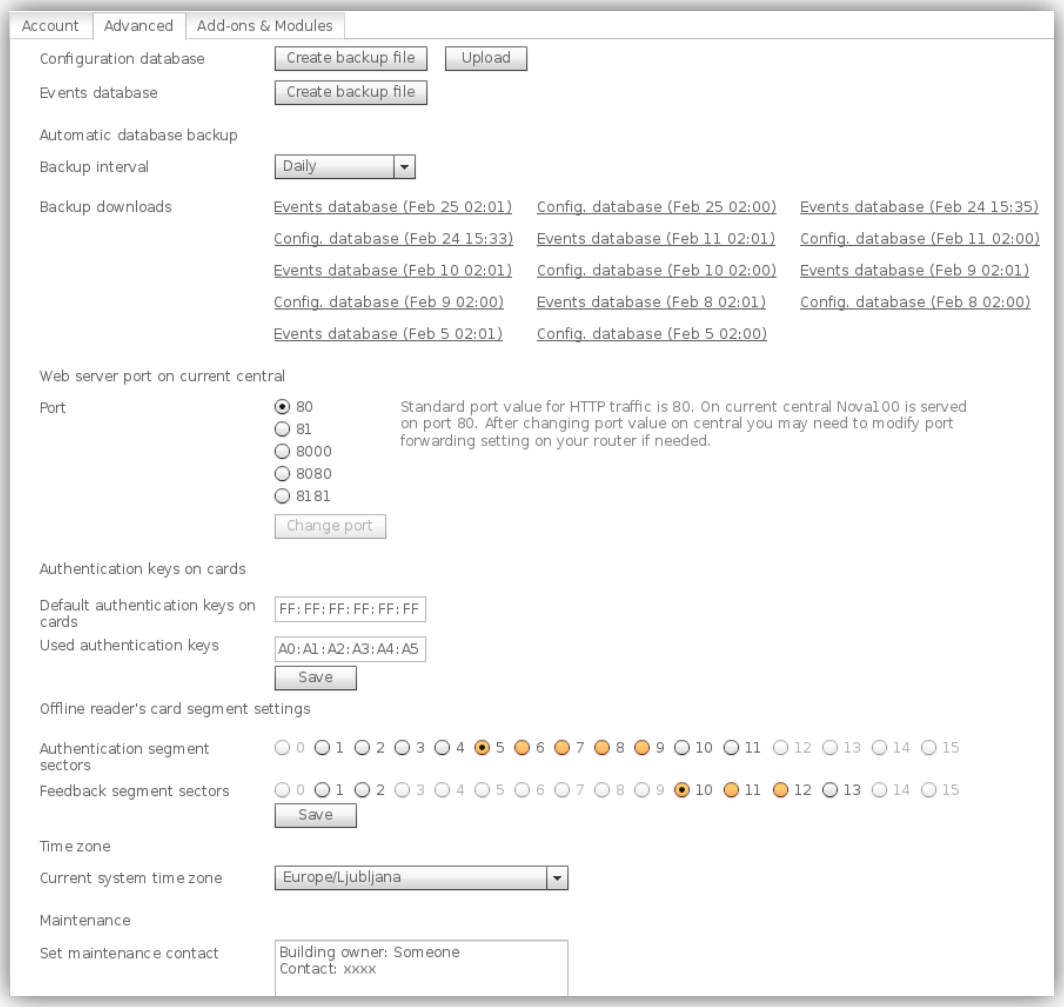
6.2.3 Offline authentication keys

"*Authentication keys on cards"* allow changing authentication keys that is used to protect data on Mifare cards. "*Default authentication key" on cards* field must contain default key from new empty cards which was set by the card manufacturer. This key is usually the same as the key on the Picture 6.3. "*Authentication key in use"* is the key which will be used in normal system operation and replaces default authentication key. This key is automatically generated first time any offline device is added to the system.

WARNING! Change this key with caution! After key change cards that were configured with the old key will not be recognized by system as valid cards! Option to change authentication key is visible only to super administrator.

6.2.4 Offline reader's card segments

Version 1.5 of Nova software introduced Offline reader's card segment settings. Previously mentioned functionality allows system administrator to set different writing sectors on the cards. This is useful for those who keep other data stored on their cards. For ex.: If there is some data already written on sectors seven (7) and eight (8), authentication segment sectors can be moved to take place from one (1) to five (5). This will allow users to keep their data on wanted segments. Additionally, we can also change feedback segment sectors the same way. Feedback sectors are only written on card if the reader's "*Card data management"* is set to "*Write data on card"* and "*read events form user cards".* Description on how to set different card data management is described in chapter *5.2.14Reader settings*.



Picture 6.3: Advanced tab

The "*Time zone"* drop down list enables the selection of system time zone. The time zone setting is important from its daylight savings time (DST). The system will automatically change time according to DST on the last Sunday in March and the last Sunday in October.

The *"Maintenance contact"* field is used for writing the 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.

6.2.5 Software upgrade on central

Under the section "*Upgrade software"* there is the option to upgrade the firmware on a central. Click the "*Upload"* button and select the .tar file to upload it to the central. After uploading the new firmware, the central will start the upgrade process and all of users will be logged-out until the update is done. To resume work, please log-in again.

IMPORTANT! After the upgrade process is complete and the application reloads, please check if the version of the Nova software is correct (the versions of the Nova software can

be checked by right clicking on the gray area in the login page or in the bottom left corner of the application when logged-in).

Sometimes web browsers caches files for quick access and displays the old information versions of Nova software after software upgrade. If this is the case, click in the browser's address bar and press the keys **CTRL + SHIFT + DELETE**. This combination of keys will show the dialog for cleaning the browser's cache (e.g. old browsing history). Delete the cache and reload the Nova application. The new data of the latest Nova application should now be properly displayed.

6.2.6 Software upgrade – system-wide

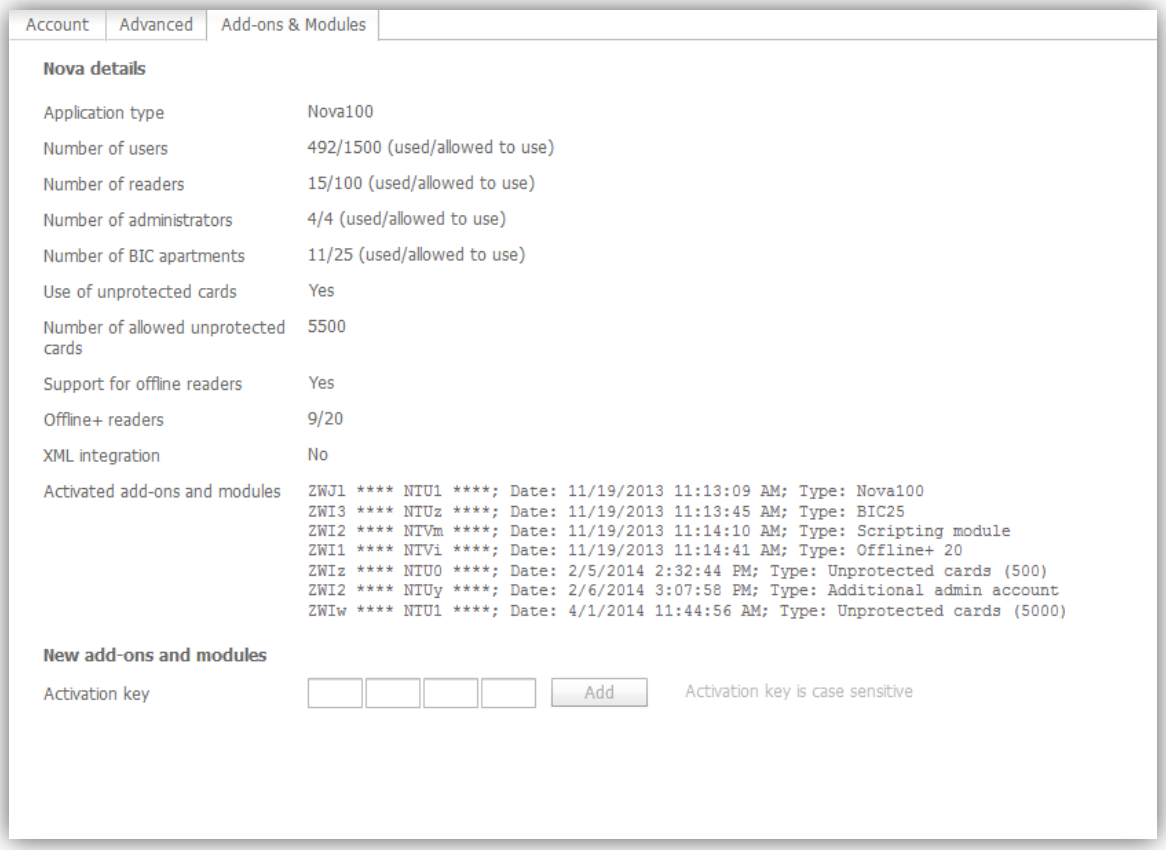
Sometimes we have a big system set-up and it would take a while **upgrading all of the centrals to the latest firmware**. Nova software 1.6 introduces to the new button in the Advanced settings that enables the upgrade of all slave centrals (without the ones connected on RS-485). Selecting this button will bring up a pop-up menu to select the upgrade package. After it is selected and uploaded, the centrals will start to upgrade simultaneously.

IMPORTANT! Master central and slave centrals connected on RS-485 network will not be upgraded. The centrals on RS-485 are very slow and need to be upgraded manually. Master central in some cases is Nova Server which require a different upgrade package.

IMPORTANT! Slave centrals need to have at least Nova version 1.6 installed to support the remote upgrade.

6.3 Add-ons & Modules tab

The third tab (*Add-ons& Modules*) holds Nova details and has input boxes for entering a new activation key (Picture 6.4). By purchasing the desired activation key, a system upgrade be made for Nova software from NovaSimpli, to other Nova versions. NovaSimpli does not require any activation key.

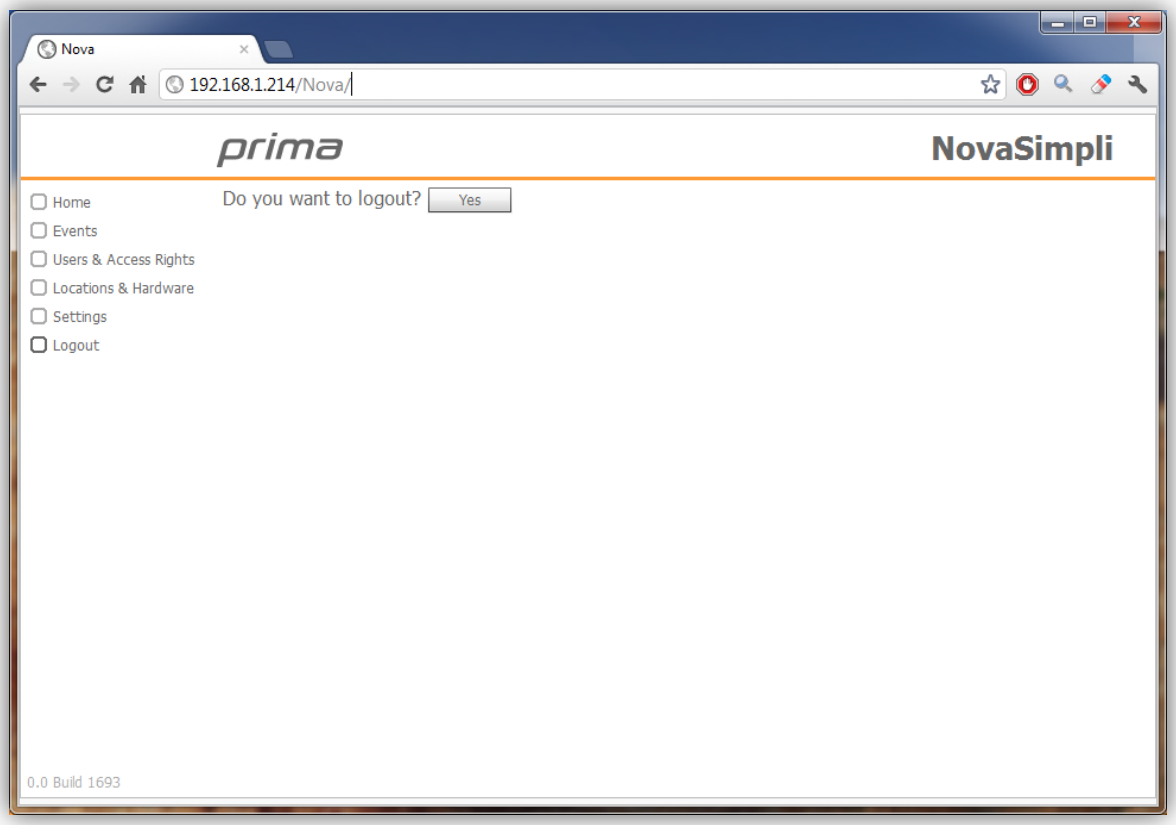


Picture 6.4: Add-ons & Modules tab

Upgrade to the NovaSimpli350 software version is free and can be done with the use of the activation key**ZWJm-ZTQ1-NTUw-ZTM4**. Please remember that with the NovaSimpli350 software, the maximum number of users in the system is limited to 350and the tracking of the events is disabled. The only way to see the events flow is trough the live events displayed on the home page.

7 Logout page

Logging out of the Nova software is accomplished by clicking the "*Logout*" button in the main navigation menu. After the logout confirmation the page will be redirected to the login page. If the administrator does not want to log out, a click on any other option in the main navigation menu will navigate him/her to selected page.



Picture 7.1: Logout page

8 Scripting module

The basic functionality of a central can be extended with custom made scripts. These scripts can define custom rules and actions that will take place when a normal system event or a user defined custom event occurs in the system. To enable the script module a valid "*Script module activation key"* is needed, which has to be entered under the "*Add-ons& Modules"* tab in the "*Settings"* section in the Nova software (chapter 6.3).

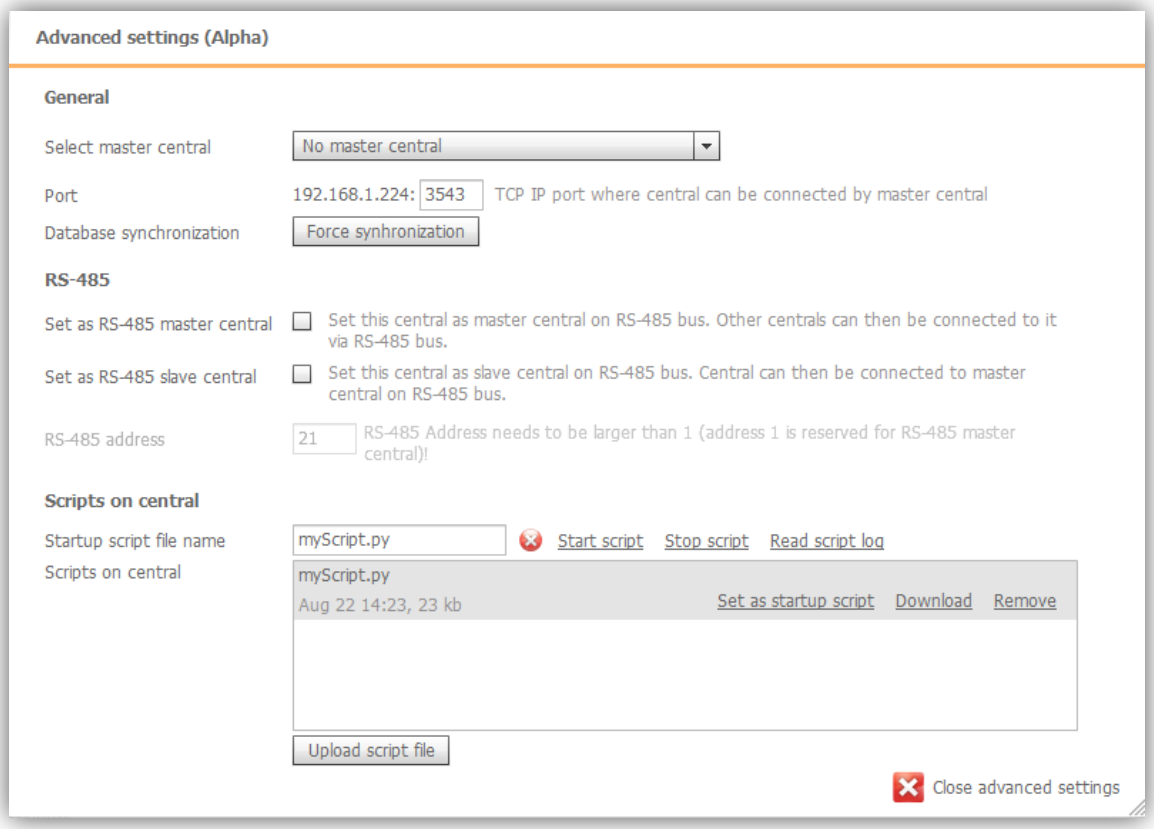
8.1 Writing scripts

Scripts are written in Python programming language. In its simplest form, scripts are run on the central, which receives events from the system and act upon them by triggering new events such as opening multiple doors, activate alarm or perform another predefined action. It is also possible to define custom events that get triggered when a specific event happens in the system.

For information about how to write scripts please refer to the dedicated manual for writing scripts, which consists of available API methods and practical examples.

8.1.1 Script installation

Scripts can be uploaded to the central in the central's "*Advanced settings"* pop-up window under the *Scripts on central* section shown on the picture below.



Picture 8.1: Scripts on central

The scripts can be uploaded to the central by selecting the "*Upload script file"* button. A browser window will show up, where a python file must be selected from local hard drive, which will then be uploaded to the central.

Uploaded scripts are visible in the list above the "*Upload script file"* button. When a script is selected in the list, its additional information and options are displayed. There are options to "*download script"* from the central to the local hard drive, "*remove"* it from the central or "*set script as a startup script ".*A startup script is started together with the central.

When selected, the 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 options of the scripts in the list. To remove the script from this field, there is a red X button next to the file name. Do not forget to save the changes after everything is done.

IMPORTANT! The scripting engine of the central will be restarted if there is a new startup script set and it will be stopped if the script is removed from the startup script field. The engine will also be restarted after uploading new script files to the central or after scripts are removed from the central.

The startup script can be stopped manually by clicking on the *Stop script* button and started by clicking on the *Start script* button. This is useful when the script is tested for new

functionalities and its behavior is not clearly defined. With a click on the "*Read script log"* button a file containing script log can be downloaded/previewed. The log includes the standard output of any running script.

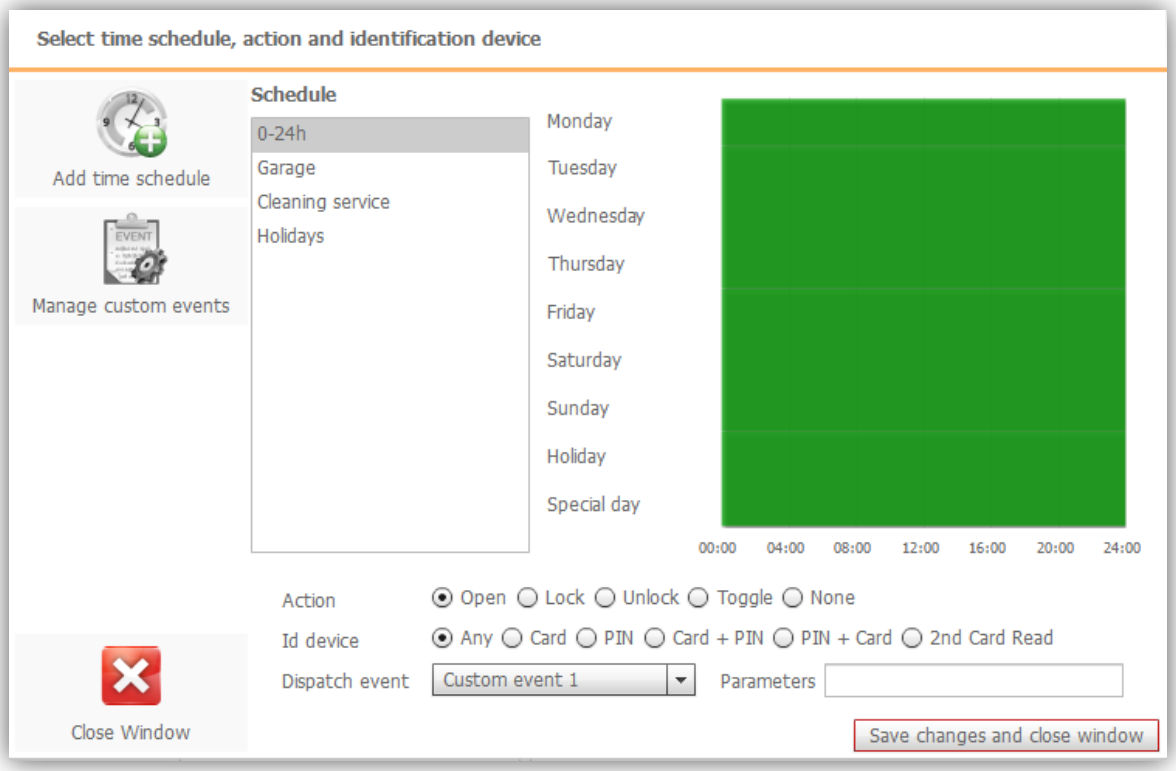
IMPORTANT! If a script crashes, the compilation errors are not present in the script execution log file! One solution to get over this limitation is to trace script progress to a standard output and based on those statements discover errors that caused the script to crash.

8.2 Custom scripting events

Custom events can be added to the Nova system and later dispatched in the context of user created events.

8.2.1 Custom events editor

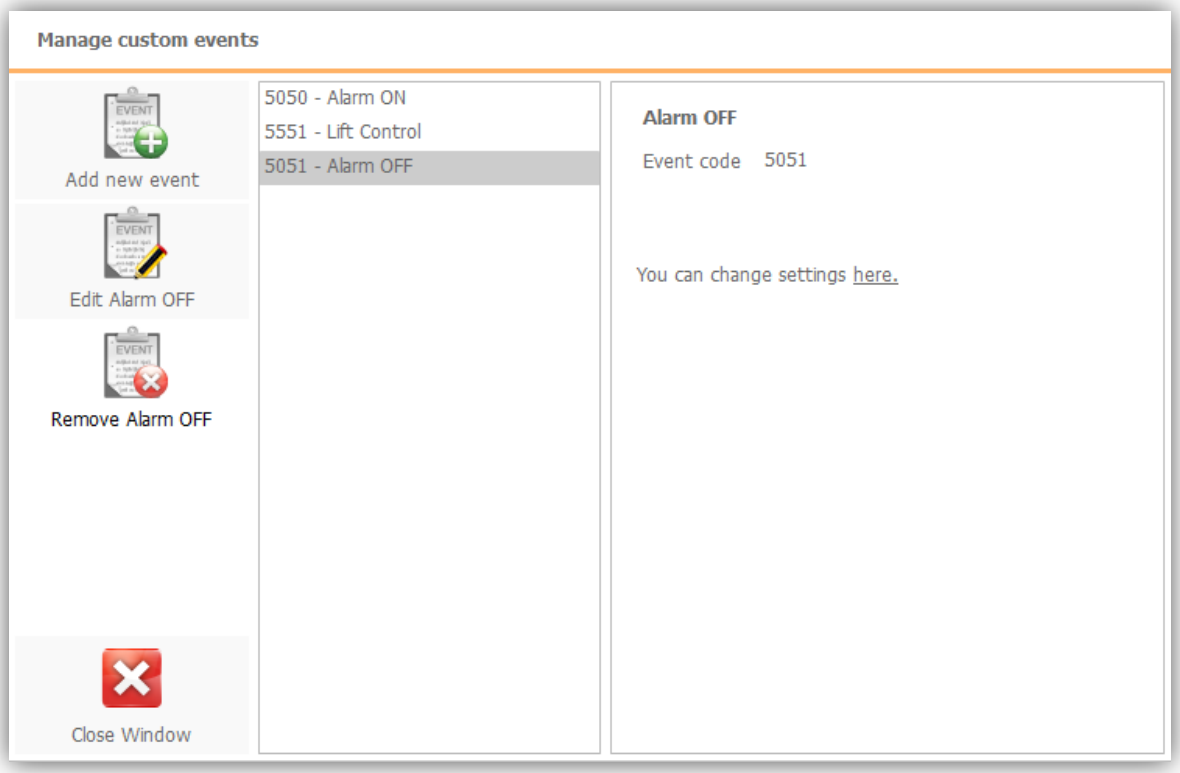
The "*Custom events editor"* can be accessed from "*Access definition editor"*, which is shown on the Picture 8.2 below. Editor can be accessed through "*Access group editor"* (see the section on editing access groups).



Picture 8.2: Access definition editor

By clicking on the "*Manage custom events"* button, the "*Custom events editor"* shown on Picture 8.3 will open.

On the left side of the editor there is a button for adding new events, a button for editing existing events and a button for deleting unwanted events. In the central part of the editor is a list of all custom events in the Nova system and to the right side of the list there is a preview of the currently selected custom event.



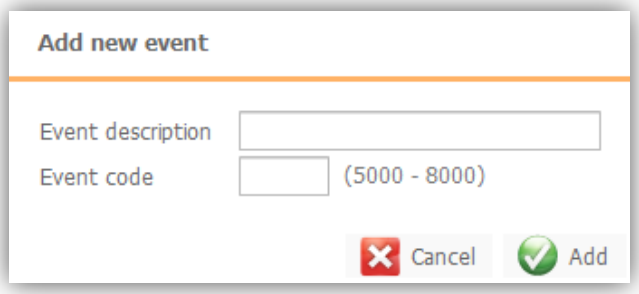
Picture 8.3: Custom events editor

8.2.2 Adding new custom event

A new custom event is added to the system by clicking on the "*Add new event*" button. The popup window shown on Picture 8.4 will be opened.

When creating a new custom event, an event code number in the range between 5000 and 8000 must be provided. This number needs to be unique, just like the event description which will be used throughout the Nova application and in reports.

When saved, the newly created event will appear in the list of custom events in the Custom events editor.



Picture 8.4: Add new custom event

8.2.3 Editing and deleting custom events

Custom events can be edited by double clicking on them in the events list or by selecting them and clicking on the "*Edit*" button. The description of the even can only be changed after it has been added to the system.

Events can be deleted from the system by selecting the unwanted event in the list of events and clicking on the "*Delete*" button. Events assigned to the access definition(s) cannot be deleted.

8.2.4 Dispatching 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 his card on the reader, where he has access rights).

To assign a custom event to an access definition, select it from the drop down list and save changes. Optionally, additional parameters can be provided (arbitrary string values) that will be passed into the script when event will be dispatched (see Picture 8.2 for drop down list with selected event Alarm ON).

8.2.5 Built-in events

Some events are already built into Nova and can be used in the same way as manually added events. They are presented in the table below.

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

Event name	Parameters	Description
Output control	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 relays(1-6) and transistors(7-10); *1,2,3:1000* opens relays 1,2 and 3 for 1 second, ...
Open output X	[time in ms]	Opens relay and transistor X for a time period
Open transistor X	[time in ms]	Opens transistor X for a time period
Lock output X		Sets transistor X to locked state
Lock transistor X		Sets transistor X to locked state
Unlock output X		Sets transistor X to unlocked state
Unlock transistor X		Sets transistor X to unlocked state
Toggle output X		Toggles state of relay and transistor X
Toggle Transistor X		Toggles current state of transistor X
Alarm activate, Alarm user, Alarm ...		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 8.1: List of built-in events

The first six (1-6) indexes of output control represent the relays of the central, while the 7-10 represent the transistors (7 is transistor 1, 8 is transistor 2 etc.).

IMPORTANT! The built-in events can only be used if there is a Scripting activation key entered in the system.

8.3 Simple alarm integration

Alarm integration allows users to control alarm zones with their cards and online readers and provide detailed log of alarm state changes in the form of system events which can be printed out.

Central in 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.

8.3.1 System prerequisites and alarm script installation

Scripting activation key is needed for enabling alarm functionality. Please see chapter *6.3 Add-ons & Modules* tab for more information on activation key installation.

Scripts "*Alarm.py"* and "*main_simple_alarm.py" are* needed on the central that will control selected alarm zone and user with "*system administrator"* account type needs to be added into the system.

IMPORTANT! User with "*system administrator"* account type is needed for python scripts to be able to log-into the system.

User with system administrator rights needs to have same authentication credentials as the ones defined in "*main_simple_alarm.py"* script. Default username defined in script is "*Python"* and default password is set to "*python"*.

IMPORTANT! Nova software version 1.5 and above 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.

It is advisable to change default username and default password with new unique values. To change them in script file, open "*main_simple_alarm.py"* in text editor and look for definitions of username and password in the file and replace them with new values– possibly "scripting" for username and "" for password if there is a new version of Nova software.

Install above mentioned scripts on the 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 *8.1.1Script installation.*

8.3.2 Access group configuration

Special access groups are used to give users rights to activate or deactivate alarm zones. Some users may only activate alarm while others are also allowed to deactivate it.

Two access groups are needed to achieve described use 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 alarm zone in the context of the newly created access group.
3. Select time schedule which will define time frame 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 alarm zone in the context of the newly created access group.
3. Select time schedule which will define time frame for activating alarm.
4. Set "*Action"* to "*None".*
5. Set "*ID device"* to "*Any"*.
6. Set "*Dispatch event"* to "*Alarm user"*.
7. Save changes.

Once access groups are created, they need to be assigned to users responsible for alarm zone management. Both of the access groups needs to be assigned the users with rights to activate and deactivate alarm. Some groups can be assigned only to the users who can only activate alarm (*alarm activation access group)*.

8.3.3 Activation of alarm

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

At this point, user can remove his card from the reader and pass the door. For alarm activation, the card must be presented to the reader until it is read for the second time (approximately 5 seconds). At this point alarm activation will begin: central will send a request signal for alarm activation to alarm central and it will wait for the confirmation signal.

On positive confirmation signal from alarm central reader will make a "beep" sound five times with OK tone and "*event8021 – Alarm on"* will be triggered. In case of negative

confirmation signal from alarm reader will beep with long ERROR tone and "*event 8022 – Alarm activation failed"* will be triggered.

When alarm is set, all readers on the central are blocked.

8.3.4 Deactivation of alarm

All readers on alarm zone controlling central are blocked when alarm is activated and users are not able to access any doors. Error sound will inform them that alarm is activated and that they cannot pass until alarm is deactivated.

User assigned with "*alarm deactivate access group"* can deactivate alarm by presenting his/her card on the reader. Alarm deactivation request is sent to the alarm central when card is read.

On positive confirmation signal from the alarm central doors will open and reader will beep three times with short OK sound. "*Event 8020 - Alarm off"* will be triggered. In case of negative confirmation signal from the alarm central reader will beep long ERROR sound and "*event 8023 - Alarm deactivation failed"* will be triggered.

If alarm deactivation will fail three times in one minute then doors will be opened. Reader will beep the same way as when alarm is activated (five short OK beeps as alarm is still activated) and event "*8024 – Alarm maintenance entry"* will be triggered.

IMPORTANT! Readers do not signalize weather alarm is ON or OFF as that can represent security issue.

9 BIC Module

Building Information Control(BIC) module in Nova is a part of the door and building information communication system installed in parallel with the Nova access control system. The BIC module allows the control of text on various displays – among others the display on door stations, call buttons and video indoor stations.

To use BIC module in Nova it has to be enabled by entering valid BIC module activation key. See the *Settings* section of this manual for help on adding new activation keys. After activation of the module you can access the BIC management window by clicking the *Manage Hardware* button under *Location & Hardware* in the Nova main menu. Clicking on the button *Manage door stations* will open the *BIC manager* popup window.

9.1 BIC module setup

First step needed for BIC module setup is to import apartments into the BIC module with the *Apartments manager* which can be accessed through *BIC manager*(Picture 9.1). Apartments can also be imported using special Excel file. When setting up apartments, you will need the serial numbers of the installed hardware (call button and video indoor station) in apartments. Serial numbers are needed in the BIC module to communicate with apartment's hardware. For more information read the *Manage apartments* section.

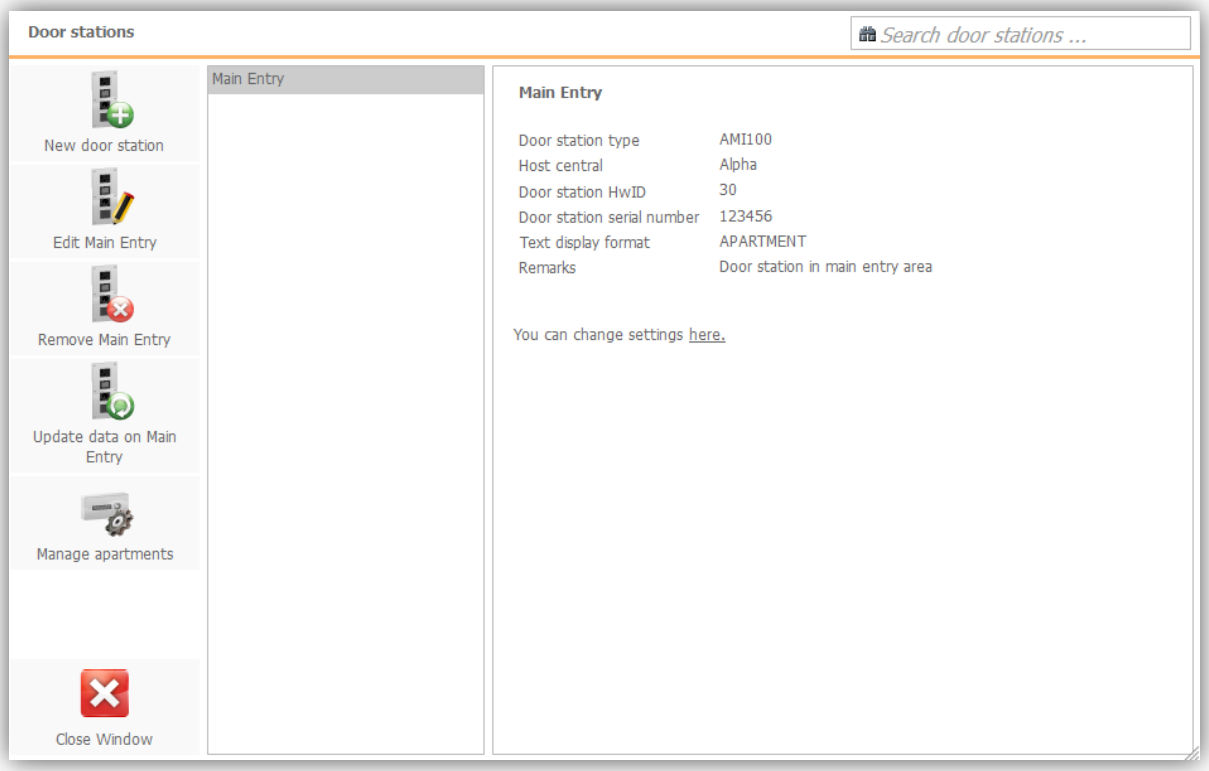
With apartments set up you can proceed with setting up door stations with BIC manager. Here you will need serial numbers of door stations that you want to include in the BIC module and names of the centrals to which these door stations are connected to. See the *Adding door stations* section for more information.

Next step is to link apartments and door stations. Each door station has to have apartments assigned to show text on the different displays. See the *Assigning apartments to door station* section for more information.

Last step needed is to assign apartments to the users. This is done through the user's settings popup window which can be accessed through *Users & Access rights* in the main Nova menu. See the *Assigning apartments to users* section for more information.

9.2 BIC manager popup window

Picture 9.1 shows the BIC manager popup window. On the left side of the window there are buttons for adding, editing and removing door stations and for updating data on the selected door station. In the centre there is a list of all door stations added to the BIC module. Details of the selected door station are visible on the right side of the popup window.



Picture 9.1: BIC manager popup window

Additionally, you see the button *Manage apartments*, which will be described next.

9.3 Managing apartments

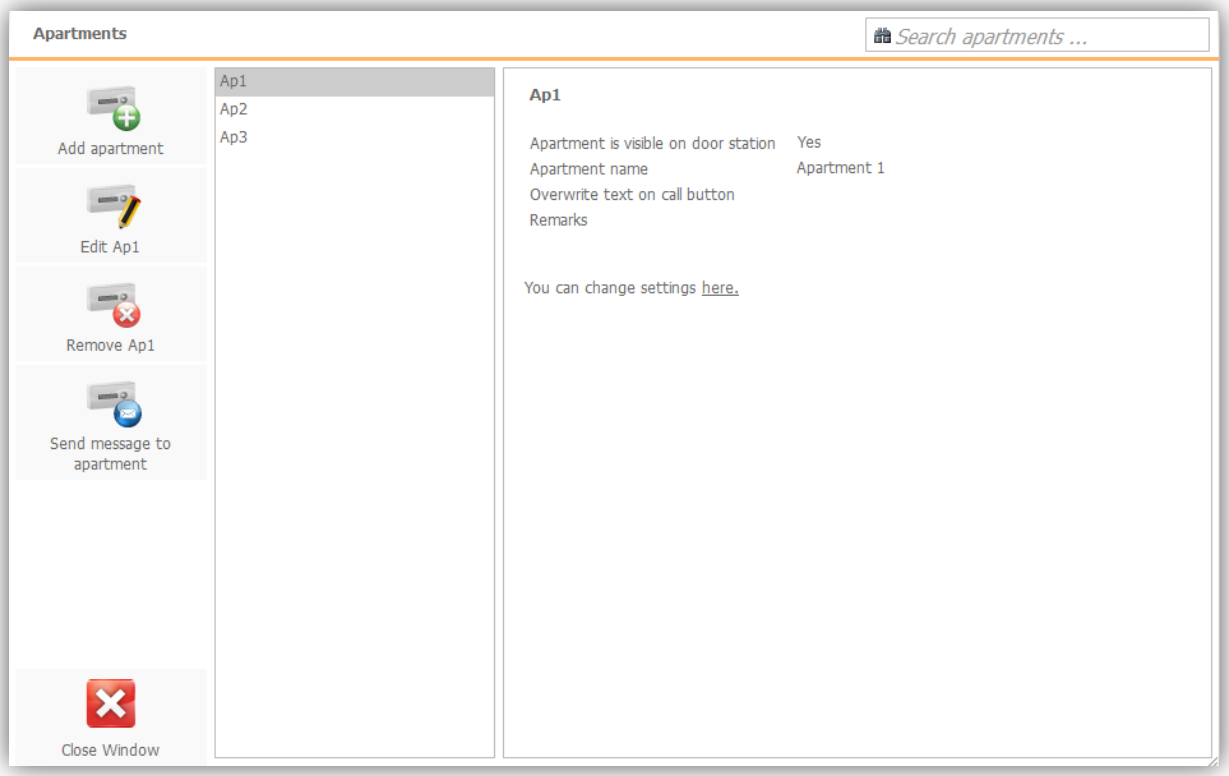
Apartments need to be added to the software before they can be assigned to door stations or users.

You can manage apartments by clicking on the *Manage apartments* button in the Door station manager popup window. You will be presented with the apartment manager popup window (Picture 9.2).

9.3.1 Adding apartments

New apartments are added to the system by clicking the *Add apartment* button. After entering a unique apartment ID, the apartment will be added to the list of apartments in the apartment manager. You can manage this list by adding new apartments to it or you can edit or delete existing ones.

You can search between apartments in the list with the search function in the upper right corner of the apartment manager. Preview of the selected apartment is shown on the right side of the manager window. You can quickly see important information about an apartment and edit it if necessary.



Picture 9.2: Apartment manager

9.3.2 Editing apartment

Apartment can be edited either by double-clicking on the apartment ID in the list of apartments or by selecting the apartment and clicking the *Edit* button next to the list. The apartment editor (Picture 9.3) will open.

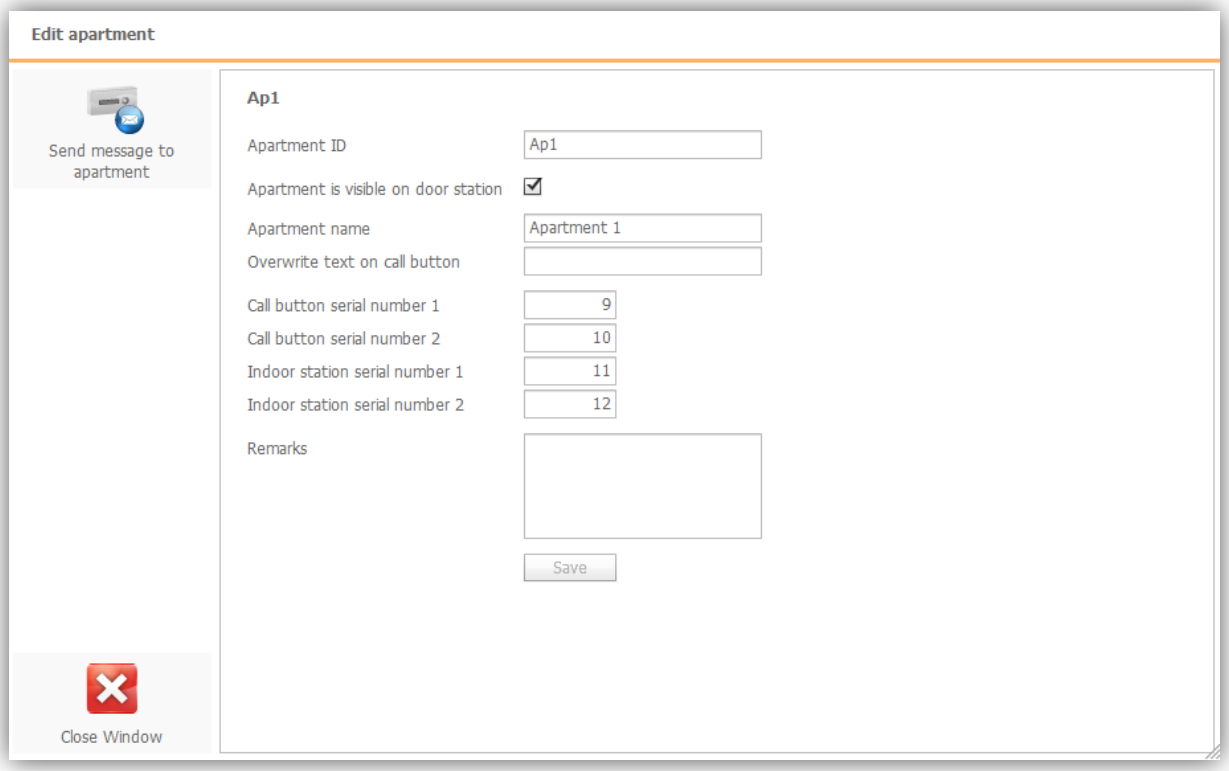
Each apartment needs a unique ID in the context of the BIC module. The apartment's ID is used throughout the software as a reference to it.

All apartments are listed on the door station by default, but un-checking the option *Apartment is visible on door station* will cause that this apartment will not be listed on the door station.

The text which is shown on door stations for each apartment is defined with the field *Apartment name*. The same name is used on the apartment's call button, but you can overwrite it by entering a custom name in the *Overwrite text on call button* field.

An apartment's hardware components (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 BIC components.

Additional information about an apartment can be saved in the *Remarks* field.



Picture 9.3: Apartment editor

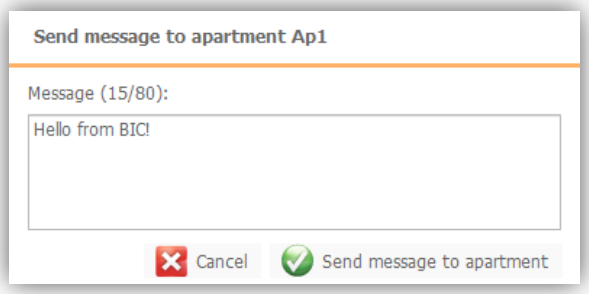
Changes made to the apartment must be saved by clicking on the *Save* button.

9.3.3 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. Apartment is removed from the BIC module by clicking on the *Remove* button in the *Apartment editor* (Picture 9.2). After removal confirmation the apartment will be removed from the list.

9.3.4 Sending messages to apartments

Short messages can be sent to each apartment and will be seen on apartments' video indoor station where users can read them. Each message can be up to 80 characters long and can be sent by first selecting apartment(s) from the list of apartments and then clicking on the *Send message to apartment* button (see Picture 9.2; same button is also present in the apartment editor).



Picture 9.4: Message input popup window

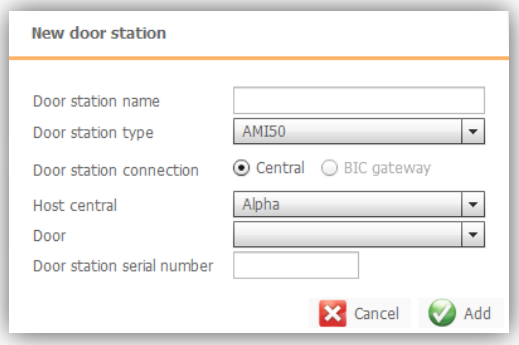
The message for the selected apartment can be typed into the popup window seen on the Picture 9.4and sent to the apartment by a click on the *Send message to apartment* button.

9.4 Door station management

Door stations can be managed with the door station manager.

9.4.1 Adding door stations

Door stations can be added to the Nova software by clicking the *New door station* button Picture 9.5in the door station editor which will invoke the popup window on Picture 9.5. You have to provide the name for the new door station, serial number and the type of the door station. You also need to select the host central and which door on the selected central the door station is wired to physically. Door stations can currently only be connected to the Nova centrals, so *BIC gateway* option is disabled for now.



Picture 9.5: New door station popup window

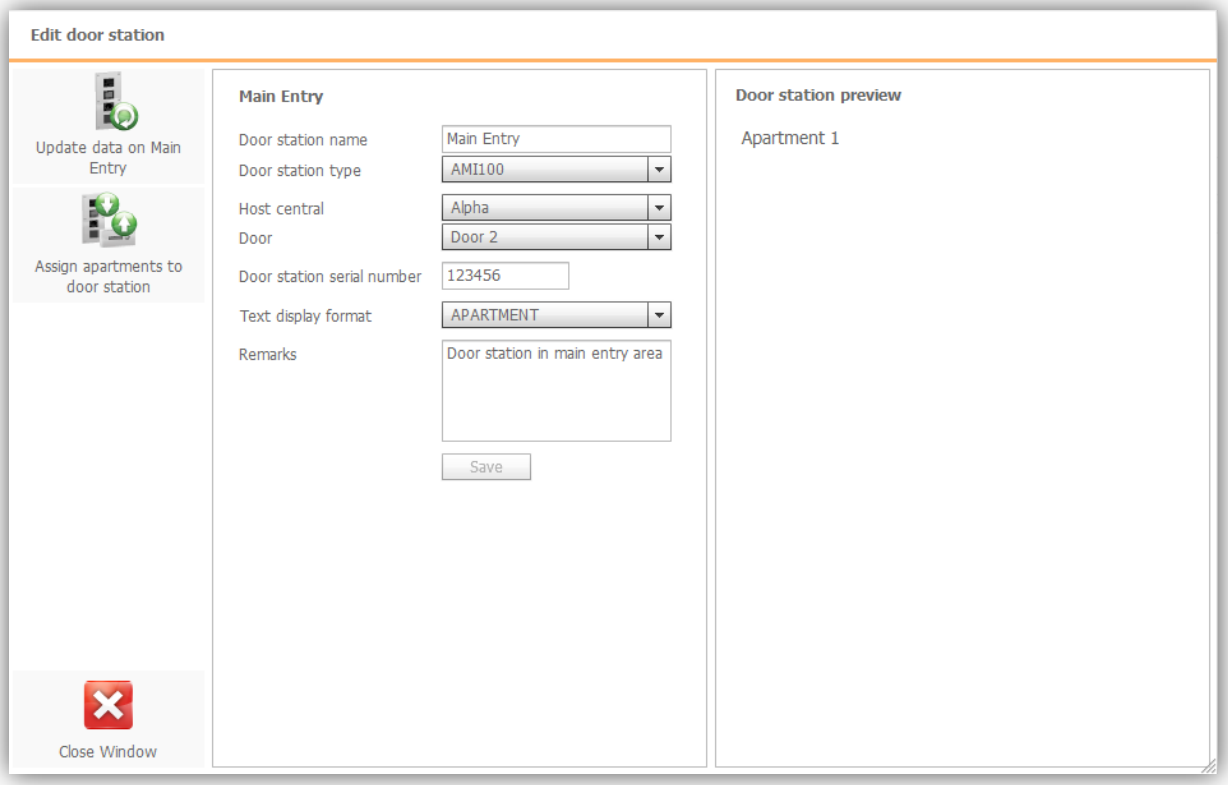
Door station is saved by clicking on the *Add* button. The newly created door station will be added to the list of all door stations where it can be selected and managed.

9.4.2 Editing door station

Picture 9.6 shows popup window for editing door station. You can edit a door station by either clicking on the *Edit* button or by double-clicking on the door station's name in the door station manager window.

The editor's central section allows you to modify the parameters of the door station: *name*, *type*, *host central* and *host door*, the *serial number* and *Text display format*, which defines the format of how data is shown on the door station's display. You can choose between different text combinations that can consist of an apartment's name, the user's name and/or user's last name.

IMPORTANT! There is an option under apartment properties to overwrite the default name with the custom name which will be shown instead.



Picture 9.6: Door station editor

9.4.3 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 see the section *Assigning apartments to door station.* You can remove a door station by clicking on the *Remove* button in the door station manager popup window. The door station will be removed from the list and from the system.

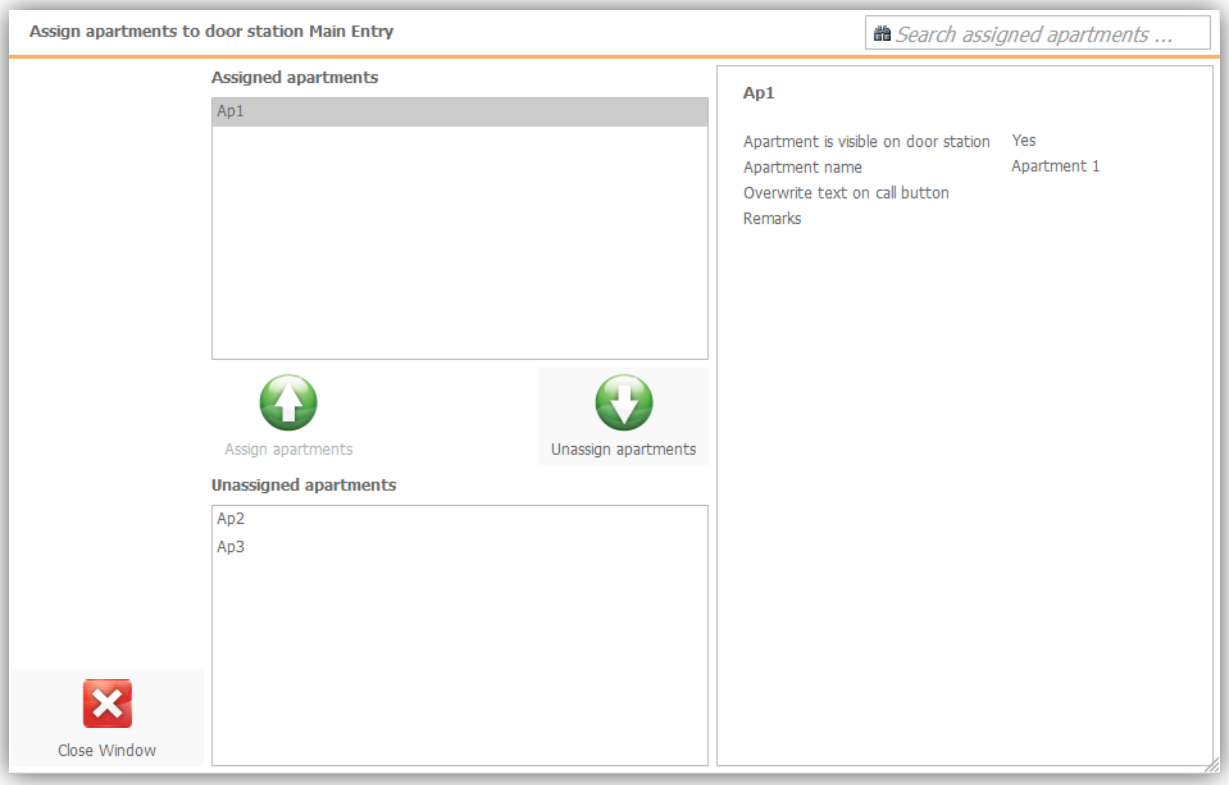
9.4.4 Preview of door station information

Preview of text on the display of the edited door station is visible in the *Door station preview* section in the *door station editor*. It is based on the apartments that are 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.

9.4.5 Assigning apartments to the door station

Before you can assign apartments to the door station, all apartments that you want to be visible on the door station need to be added to the system. See explanation on how to add apartments in the earlier section. Here it is assumed that all of the apartments are already present in the system.

Assigning apartments to the door station is done by clicking on the *Assign apartments to door station* button on the left side of the *door station editor*. This will open the window shown on the picture below (Picture 9.7).



Picture 9.7: Assign apartments to door station

The central part of the popup window is comprised of two lists containing assigned and unassigned apartments. Between them there are two buttons for moving apartments between lists. If you want to assign apartment(s) to the door station, you need to select desired apartment(s) from the list of unassigned apartments and click on the *Assign apartments* button. Selected apartment(s) will be assigned to the door station and will

appear in the list of assigned apartments. Apartments can be unassigned from the door station in the opposite way.

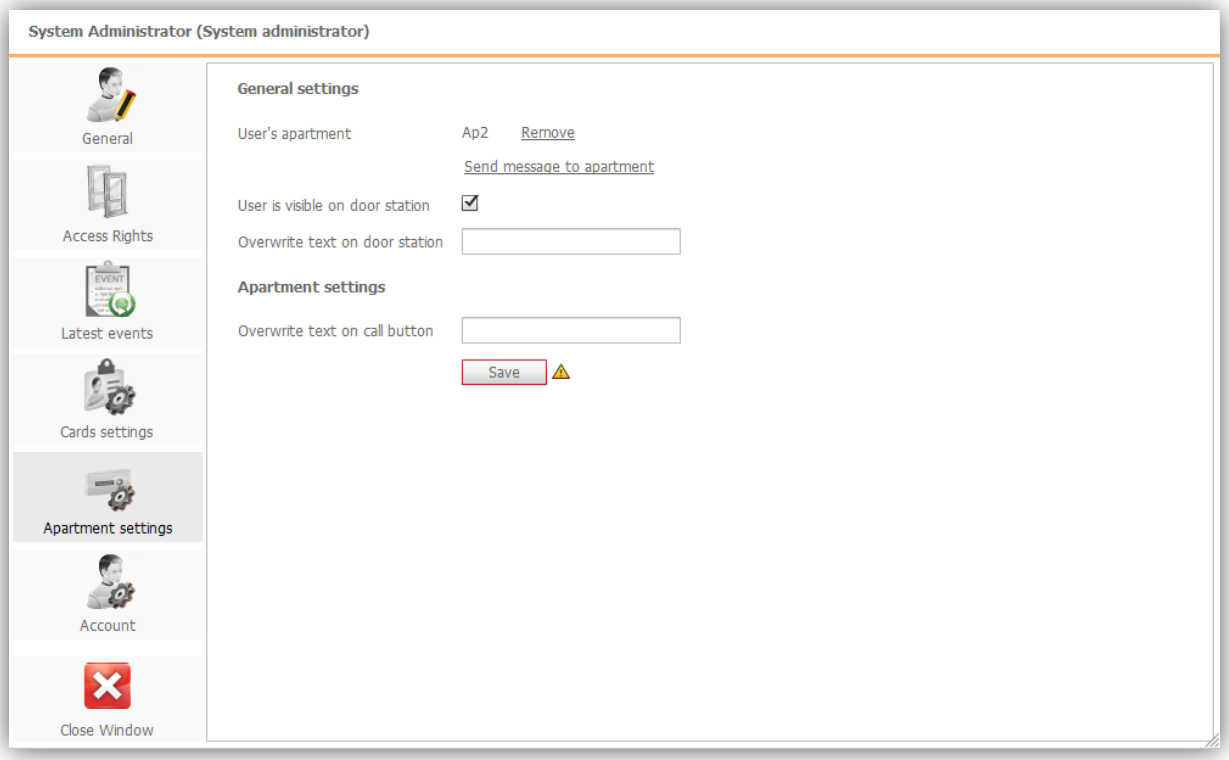
When the lists contain a lot of apartments you can use the search function in the upper right corner of the popup window. A search will be done between the apartments in the list where at least one apartment is selected. You can preview the details of the selected apartment on the right side of the popup window.

9.4.6 Updating content on door station

When all changes on the door station are saved and the apartments are assigned, this data needs to be updated on the door station. Clicking the button "*Update data*" in the *door station editor* will cause that the updated data will be sent to the door station which will then update old texts with the new ones. Sending data and updating information on the door station can take some time. On the average it takes approximately 10 minutes to send and update data of 100 users/apartments.

9.5 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. Picture 9.8 shows the user's apartment settings which can be accessed by clicking on the *Apartment settings* button in the *user's editor popup* window (see section on managing users for how to edit a user).



Picture 9.8: User's apartment settings where apartment is assigned

The user's apartment settings are divided into two groups, *General settings* and *Apartment settings*. General settings are associated directly with the user, while apartment settings directly change properties of the assigned apartment.

You can assign an apartment to the user by clicking on the *Select apartment* button. A popup window will be opened in which you will be able to find and select the user's apartment, which will then be listed under the *User's apartment* field.

When the option *User is visible on door station* is checked, the user will be listed on the door station. If you want to omit user's name from being shown on the door station, you can un-check this option. And if you would like to use custom name instead of the default user's name, you can enter it to the *Overwrite text on door station* field.

The field *Overwrite text on call button* directly changes the assigned apartment's setting (it overwrites text on call button) and it is meant for changing the text on the call button outside the apartment. One case where this is useful is when an administrator is administering users but has no privileges to alter the hardware settings.

Changes must be saved by clicking on the *Save* button in order for them to be effectively used.

IMPORTANT! Remember that after changing the user's *Apartment settings*(general and apartment settings) all data on the door stations needs to be updated.

10 Booking module

Booking module is designed for reservation of the premises at the specified date for a defined period of time. Booking activation key must be added to the system as described in *6.3Add-ons & Modules tab* along with the booking software that can be found on the next web address:
http://packages.primasystems.si:8083/Central%20firmware/release_candidate/Booking/

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 *6.2.5Software upgrade on central.*

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

10.1 Booking access groups

After activation and software update, navigate to *Users & Access Rights* and click on the *Manage Groups* button. New type of Access group type is now added to the list of access groups called *Booking location*. Create new booking location by clicking *Add group* button on the left top corner as seen on Picture 4.8. Naming access group after representing resource is considered a good practice.

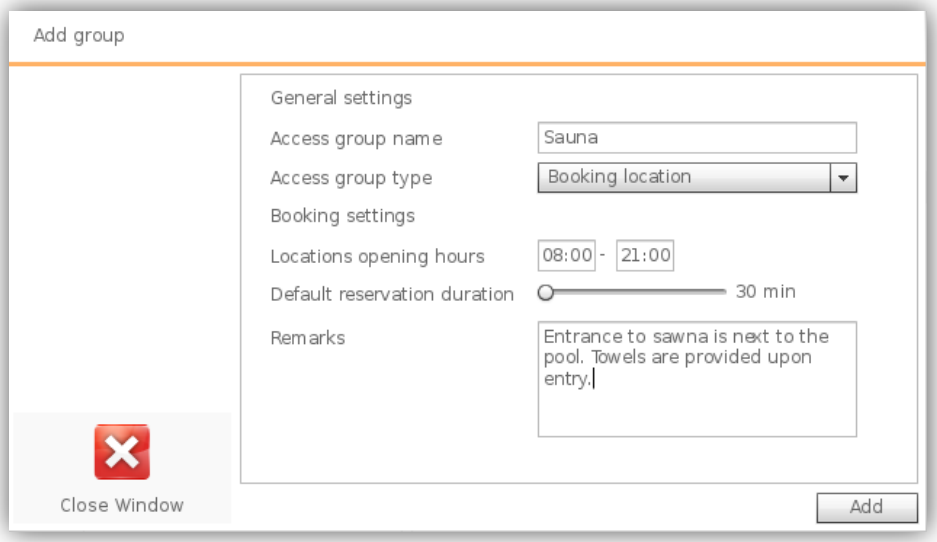
Picture 10.1 shows some additional parameters that must be filled for each Booking access group:

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 his/her reservation.

Remarks–displays a custom message to users who are making the reservations. Message should provide additional guides to users and their reservation (where is the 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, we made names of the booking ones display in **bold** font.



Picture 10.1: Adding a new booking location

On Picture 10.1 we have created a new Booking access for Sauna which 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.

Each booking access group can be associated with existing reader in Nova system. Assigning booking access group is the same as assigning any other group to the reader (described in chapter *4.2Managing Access groups*).

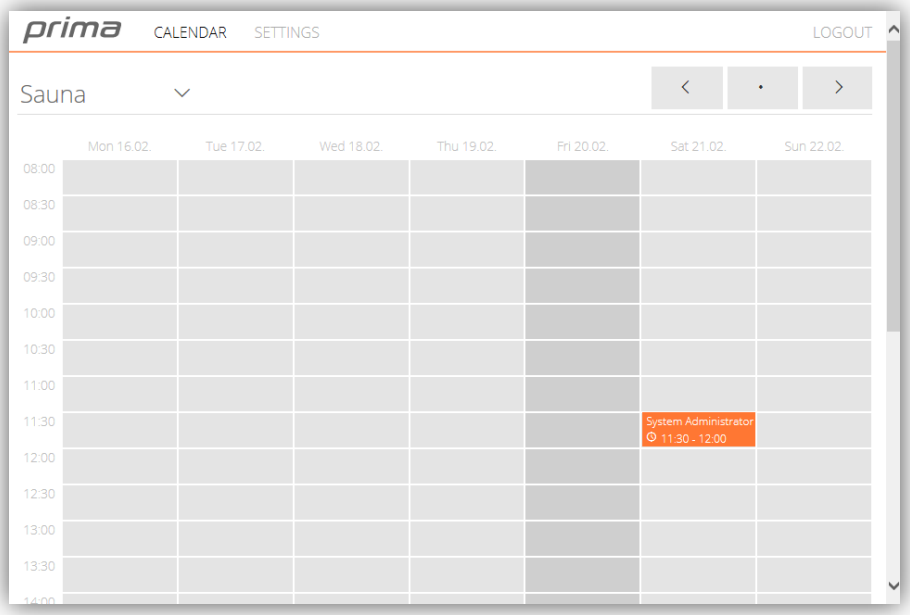
By assigning one or more readers to booking access group, a new defining access zone is created thus granting access in the selected zones during time interval defined by user's reservation.

10.2 Reservation creation and cancelation in Booking module

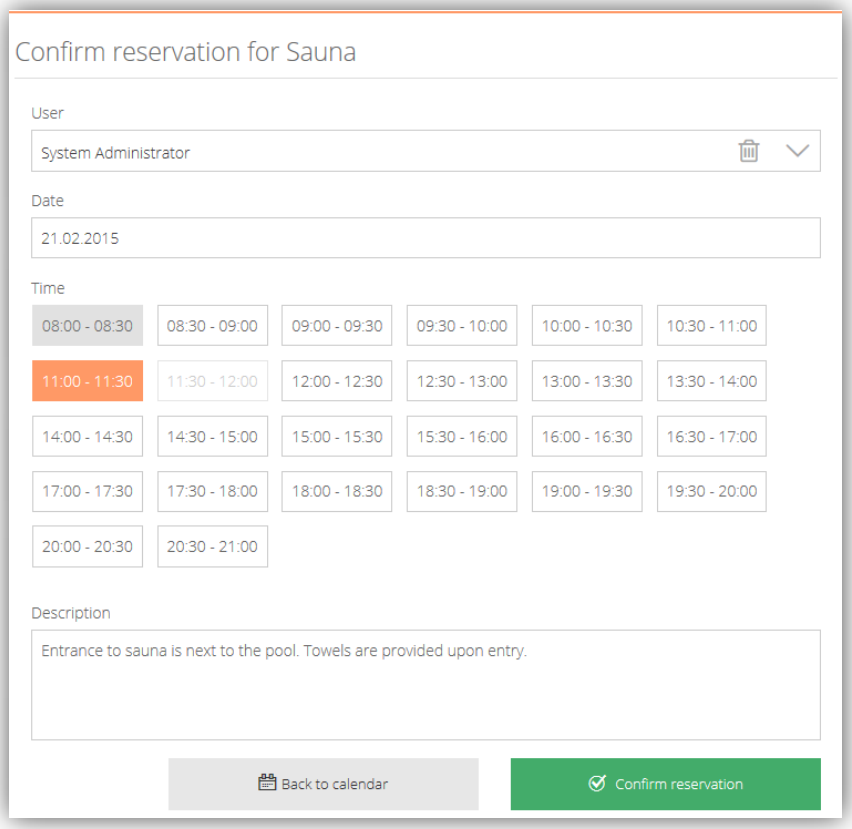
After access group configuration is done in Nova, Booking module can be accessed with a web browser on address **http:// <IP of the central>/Booking** (replace the text inside <> with IP address of the specified central). A new login page will appear and can be entered with the same credentials as in Nova. For basic reservations, an administrator type of account must be used for creating or canceling the existing reservations.

Picture 10.2 shows Calendar page of Booking application where the resources are listed in the top left corner. Currently our location is set to Sauna as we added it in the previous example. The locations can be switched 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 in Picture 10.1. The buttons on the top right above the grid are used for switching between different weeks. The middle button resets the overview to the active weekend.

Creating new reservation requires a user to select the corresponding part of the calendar. To confirm the reservation, the *Confirm reservation* button must be pressed as seen on Picture 10.3.



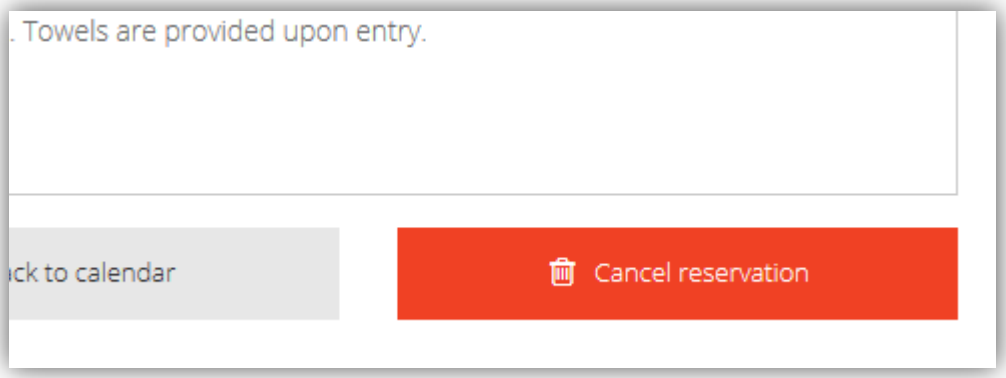
Picture 10.2: Calendar page of Booking module



Picture 10.3: Reservation confirmation

Reservations cannot be done for elapsed time. Confirm reservation window has set reservations grayed out and cannot be selected.

Canceling reservations can be done by clicking on the unwanted entry in the calendar and clicking the *Cancel reservation* button (Picture 10.4).

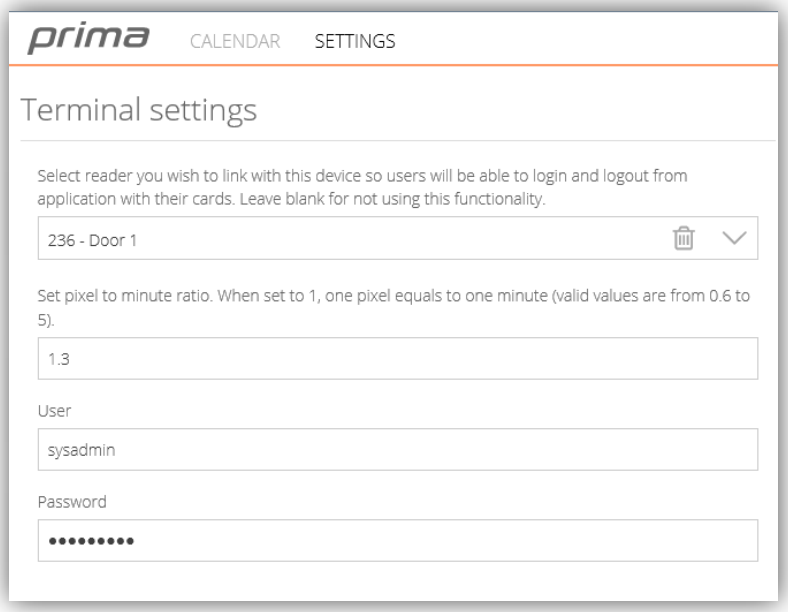


Picture 10.4: Reservation abort

10.3 Booking as a terminal application

Booking can be run standalone in terminal mode. Suggested prerequisites for this mode are touch capabilities of terminal's screen and a Nexus reader connected to the central. Users can use their RFID – cards to log-into application and confirm their reservations.

To enable terminal mode, start Booking application on the terminal and log-into application with administrative rights. In the settings menu (Picture 10.5), a reader must be selected to provide user's authentication and access to Booking. Additionally, an existing system administrator's authentication credentials must be assigned for secure checking – for new card events on the reader. Entered data will automatically be saved.

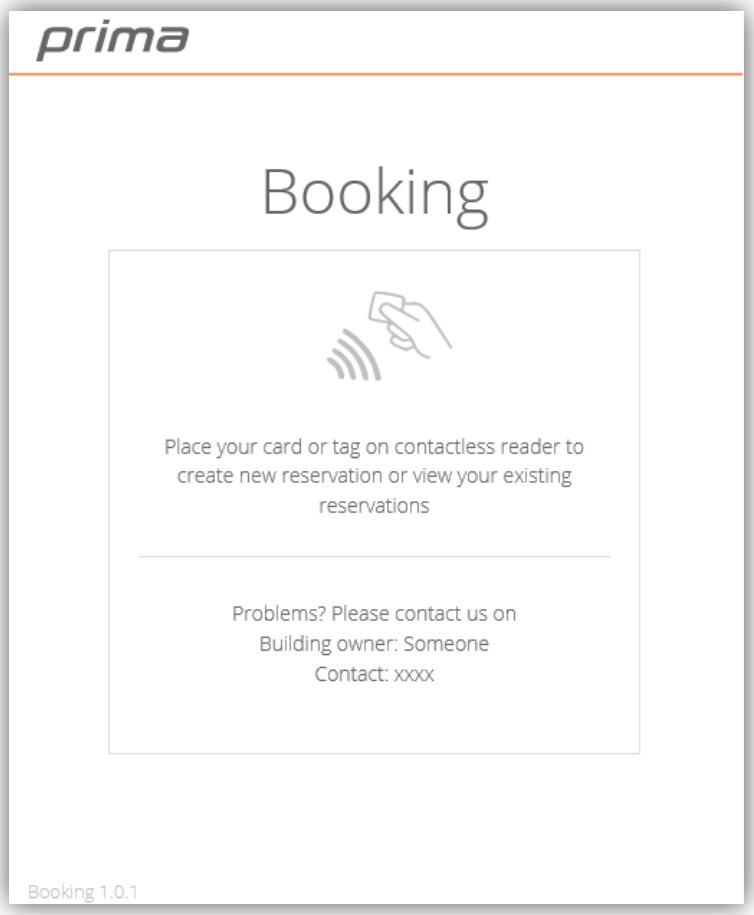


Picture 10.5: Booking terminal settings

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

Picture 10.6shows the preview of the login screen when terminal mode is enabled. To login, user needs to place his/her card on the Nexus reader. When the card is detected, Booking application will take care of login and redirect them to Calendar page after a few seconds.

Maintenance contact information set in Nova will be also shown on the terminal's login screen.

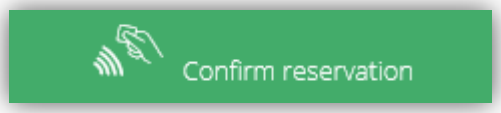


Picture 10.6: Terminal login screen

In case of troubles, the normal login form can be accessed by tapping on RFID icon seven (7) times. Login proceeds normally as described in the first paragraph of chapter10.2.

Regular users can also enter the Booking application with the same credentials as they have in Nova and their Account type is set to at least User type. Account type can be set in Nova on *Users & Access Rights*, user must be clicked two (2) times to access his/her information and *Account* button must be selected on the left menu. The top option enables setting user's type and access to the application.
User account type is especially reserved for Booking. They can use Booking application but don't have access to Nova software.

When trying to confirm the reservation on the terminal, a button with RFID icon will appear (Picture 10.7). To confirm, user must place their card on the Nexus reader to finish the process.



Picture 10.7: 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 second, they will be automatically logged-out to prevent any unauthorized access.

11 Special centrals

11.1 Elevator controller

Elevator controller is based on regular Alpha central and in addition it has support for controlling access to up to ten floors in building by activating only those floor buttons in elevator where user was granted access.

11.1.1 Elevator reader setup

Reader has to be installed on *Door 1* connector on Elevator controller. Reader and Door 1 settings are applicable in the same way as for normal reader. Please see section on setting up RFID reader for more information.

Only difference is that *Electric lock open time* setting for Door 1 is controlling how long elevator buttons are enabled.

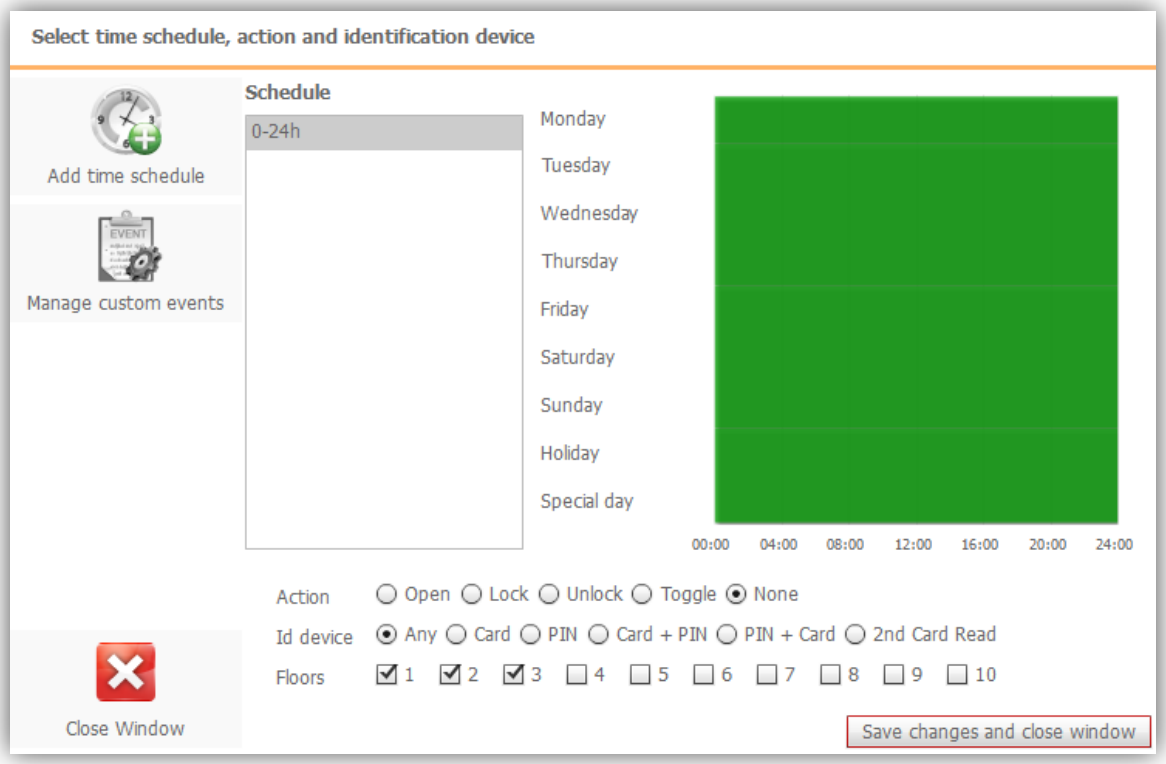
IMPORTANT! In cases when central is controlling less than 10 floors, unused outputs can be used for normal access control with additional readers connected to Door 2, Door 3 or Door 4.

11.1.2 Setting up access groups and access rights

Users need to be assigned with "*special access groups"* that define which floor will be activated when elevator will be used.

"Special access group" is created in the same way as normal access group. In it, new access definition on elevator reader can be created along with selections desired "*schedule"*, "*Id device"* and "*floors"*. Action has to be set to "*None"* (Picture 11.1).

For each different combination of floors needed to create new access group, which can then be assigned to users.

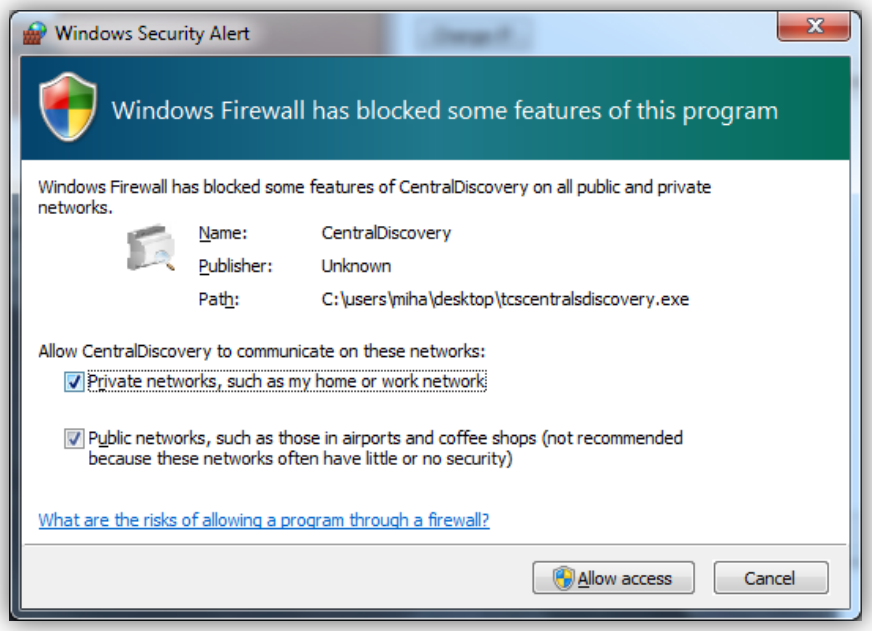


Picture 11.1: Access definition for floors 1, 2 and 3

12 Central discovery tool

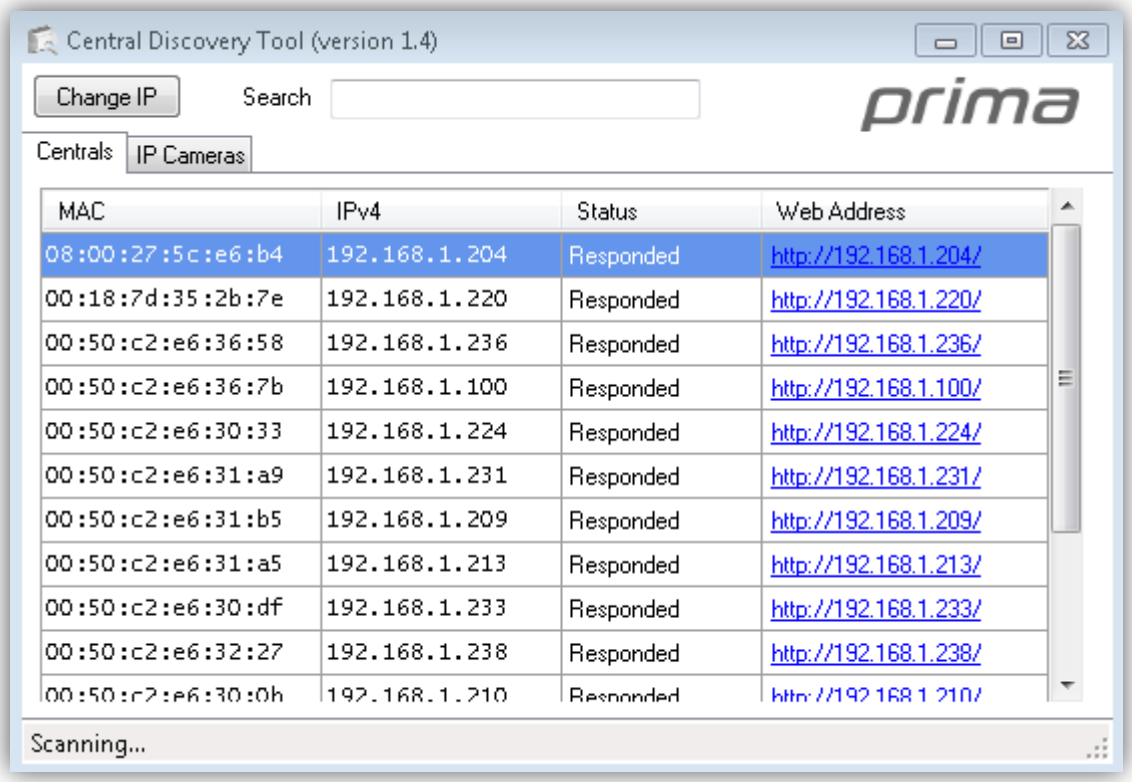
This tool allows installers to manage all of the centrals connected to local network. This software can be found and downloaded from this link: https://packages.primasystems.si:1972/Centrals%20Discovery%20Tool/.

After downloading the software, open it. On the Firewall enable window, both of the checkmarks must be set and the tool must be allowed access to the network as shown on the Picture 12.1.



Picture 12.1: Allowing access to the tool beyond the firewall

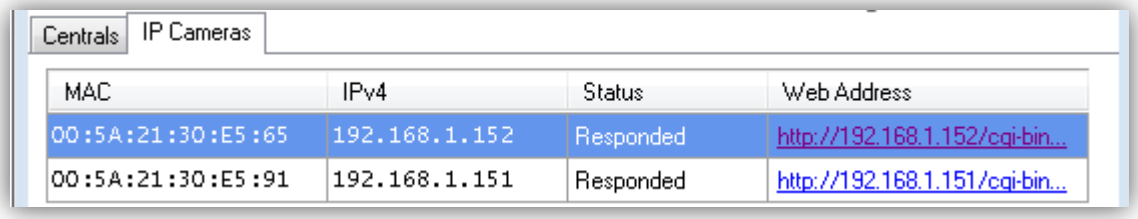
From the main window (Picture 12.2 below) we can see the MAC and IP address for the corresponding centrals. We can also easily navigate to the central's web page by clicking on the active link in the last column.
Changing the IP of the central is available on centrals with Nova version 1.5 or higher, but is limited only to be changed from the default "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. Central reset is explained in Picture 14.1.



Picture 12.2: Central discovery tool main page

Tool scans the network for any new central every few seconds. In case some central fails to respond due to IP change or network error, its entire row will turn red and its status to *"No response"*. This is extremely helpful to determine if there are any problems on the local network.
The search box on the top applies a filter to display centrals only in specific network or just a simple search by central's IP or its MAC address.

For the system with IP cameras on the network, there is an "IP Cameras" tab.



Picture 12.3: Display of IP cameras on the network

Contrary to the centrals, IP's of the cameras can be changed anytime to any address. Clicking on the *"Web Address"* of the IP camera will display a new web page containing net settings, confirming that the camera is up and running.
Discovery and search tool work the same as the central's one.

IMPORTANT! Central discovery uses UDP packets, which means that the discovery will display 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 and it was designed to run on any version of Windows OS. Different OS system can run the tool via emulation.

13 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 connect to another central by knowing the other central's IP address. This IP address is the physical address of the central and is changed in the *Manage Centrals* popup window. We can say that this address is the address, on which 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 you set in the *Central editor* (Picture 5.6).

If any central in the LAN wants to connect to a central located in a remote LAN, it first needs to know the address of that remote LAN. The communication between two different LANs is controlled by routers, and if a message is sent from a central in one LAN to a central in another LAN, it is first sent to the other LAN's router, which then sends it to the central. In the later case the router's address becomes the visible address of the central on the other LAN (and is set in the *Central editor*, Picture 5.6). 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 the "*Manage Centrals" (Picture 5.4)* popup window.

The warning message onPicture 13.1shows on the main page is still displayed if the central's physical IP is on the 192.168.1.100. The best way to properly set the system is to set the central's database IP to 192.168.1.(any other number between 1 and 255 excluding 100) – with database update. If the central's interface IP needs to be changed, repeat the process setting the new interface IP without database update.

Picture 13.1: 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 allow many centrals to talk to each other 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 has been pre-set.

Replication over a RS-485 BUS can handle up to 750 door openings per hour (3.000 events).

This compares to up to 300 door openings per minute between centrals connected over TCP/IP connection as long everything is 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 (a function which is under development). So regarding the slaves, most of the communication is one-way and mean that the slaves have no back-up of events in the system. It does 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 its replicates to all other Alpha centrals in the access control system which 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 is 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 we have two possible cases. First case is when master central needs to communicate with the slave central in another network and the other case is when we want to access publically available Nova application with our browser.

In the first case, when 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 remote central) needs to be forwarded to internal port 3543 on the slave central (not configurable). Through this port master central (or local master central) sends database to slaves.

In Second case port 80 (which is used in the web browser as the default port for all HTTP traffic) on the router needs to be routed to port 80 on the central which is serving Nova application.

Using a domain name (dynamic DNS service or custom domain name) instead of an IP number, that domain name is resolved only to IP address and all port settings remains the same.

What happens in case of overload of the replicator?

If the system generates more than app. 3.000 events per hour on a RS-485 BUS it builds up a backlog. This means that events are sat in a queue and not reported instantly. In many cases this does not matter as the local centrals will continue to work normally so users will see no difference. But in systems where an event (e.g. an input) on one central should

release a function on another (e.g. an output) it can matter as the event will be delayed 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 (app. 12 door openings). If the backlog only build up and up the system will stop working.

A 'RS-485 slave central' is locally not affected by a replicator backlog. It will continue to operate accordingly to the settings in the memory so 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 built in a number of 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 max 10 centrals on an RS-485 bus rule and max 1.000 users in an access control system with centrals on RS-485 bus rule can in some cases be seen as a guideline, which can be adapted to local circumstances. If you have a system with few users and few events, you can 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 you only have a few slave centrals on separate RS-485 bus.

On the opposite side you can also have a system with 500 users, but with many events and changes to the users. In this case it might be a very bad idea to have any centrals on RS-485 bus.

On the 'RS-485 slaves' you can also install read/write readers to be used as update readers for period validation and access rights for offline readers. You can also use input on the centrals to generate outputs on other (under development). The RS-485 does not limit these possibilities.

Which memory sectors are used on Mifare cards by offline system?

Users card currently use sectors 5 – 9(4 sectors) and 10-12 (3 sectors).We can configure starting sector for access rights segment, currently 5^{th} sector, followed by 4 unbreakable sectors. We can configure starting sector for feedback segment, currently 10^{th}, followed by 3 unbreakable sectors. All sectors are protected by unique authentication keys.

For events returned on users cards three (3) unbreakable sectors are used. Currently we use sectors 10, 11 and 12. Starting sector is configurable. 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. Users cards can be used for other applications until other applications use 'free' sectors on cards.

How is user informed about low battery level on offline reader?

User is informed by device alone (with delay, red LED, etc.) plus with software reports of battery status, when Offline+ activation key is used and user feedback (events on user card) is enabled. If battery status is low, it can be found between Errors on Home screen. On every offline reader there is the Remarks edit box, where you can write down when battery was changed.

How to replace existing or add new central to the existing system?

When you are adding new central or replacing some central 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's MAC address with the MAC address of the new slave central. MAC address of the central is written on the central's side sticker.
3. New slave central first needs to be reset to default, so there is no old stuff on it (it might be an old master and will try to connect to some centrals, etc.).
4. When slave central is reset to default, its Nova application will say it is NovaSimpli. Login to it using default credentials and change central's IP address to a new value which is set on master central.
5. Connect slave central to network. Master central will connect to it and update slave central's configuration.

What is the average write cycle time on NEXUS when writing rights for offline readers (We would like to give the user an impression of how long writing takes. The user interface is clearly the transition to the green LED. But as technical data it would be good to display the time in the documentation)?

Measured timings are*:

1. Nexus reader only writes access rights for offline readers to card:

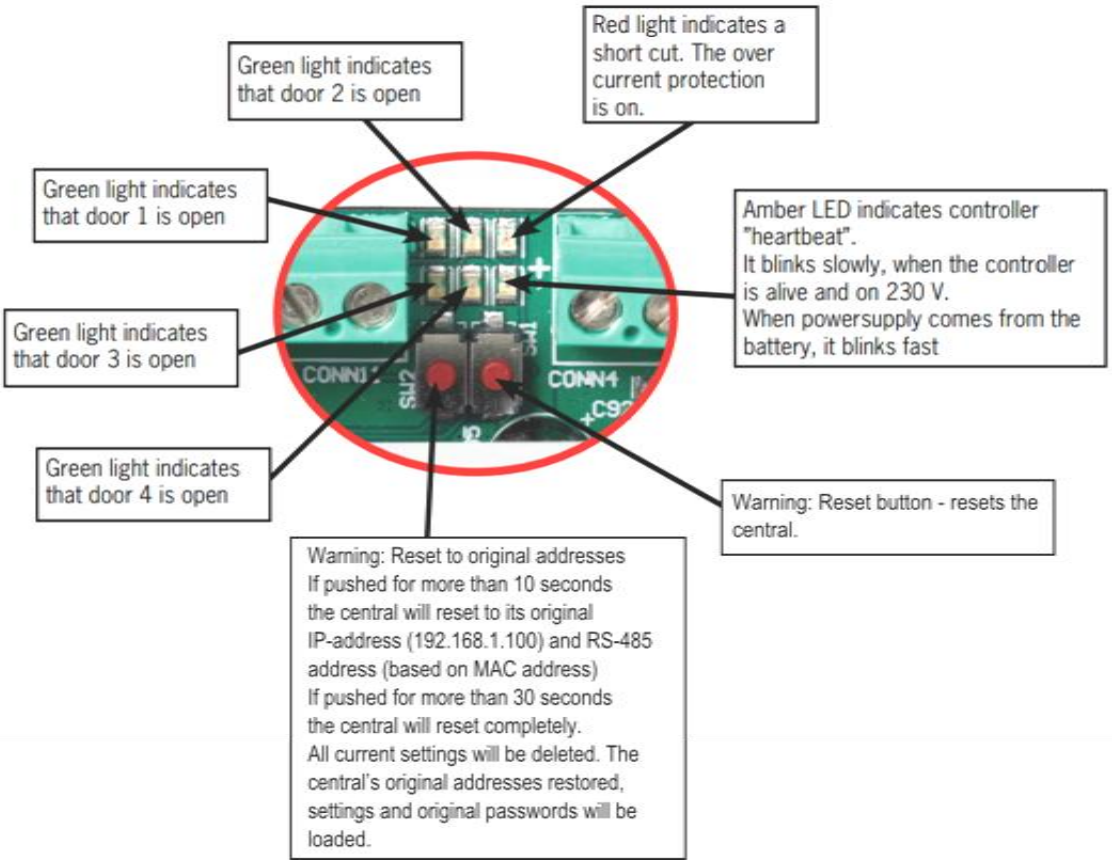
- only 2 sectors are written (48*8 = up to 384 offline door in system) average is below one and a half second
- 5 sectors are written (48*8*4 = up to 1536 offline door in system) average was just below two seconds

2. Nexus reader reads users event from card and write access rights for offline readers to card

- only 2 sectors are written (48*8 = up to 384 offline door in system) average was around two seconds
- 5 sectors are written (48*8*4 = up to 1536 offline door in system), 5 events on user card average was just below three seconds

*only one reader connected on door port 1 (port 3 and 4 are a bit slower), 500 users in database

14 Appendix A -Description of LEDs and buttons on central



Picture 14.1: LEDs and buttons on Alpha central

15 Appendix B - Nova software feature list

Package/Module	Description	NovaTouch	Administrator client	200 extra users	10 extra doors	Use any card	XML integration	Offline+	BIC	Python scripting
NovaPRO	250 doors/3000 users	yes	yes	yes	yes	yes	yes	yes	yes	yes
NovaServer	500 doors/5000 users	yes	yes	yes	yes	yes	yes	yes	yes	yes

Table 15.1: Nova software feature list


prima