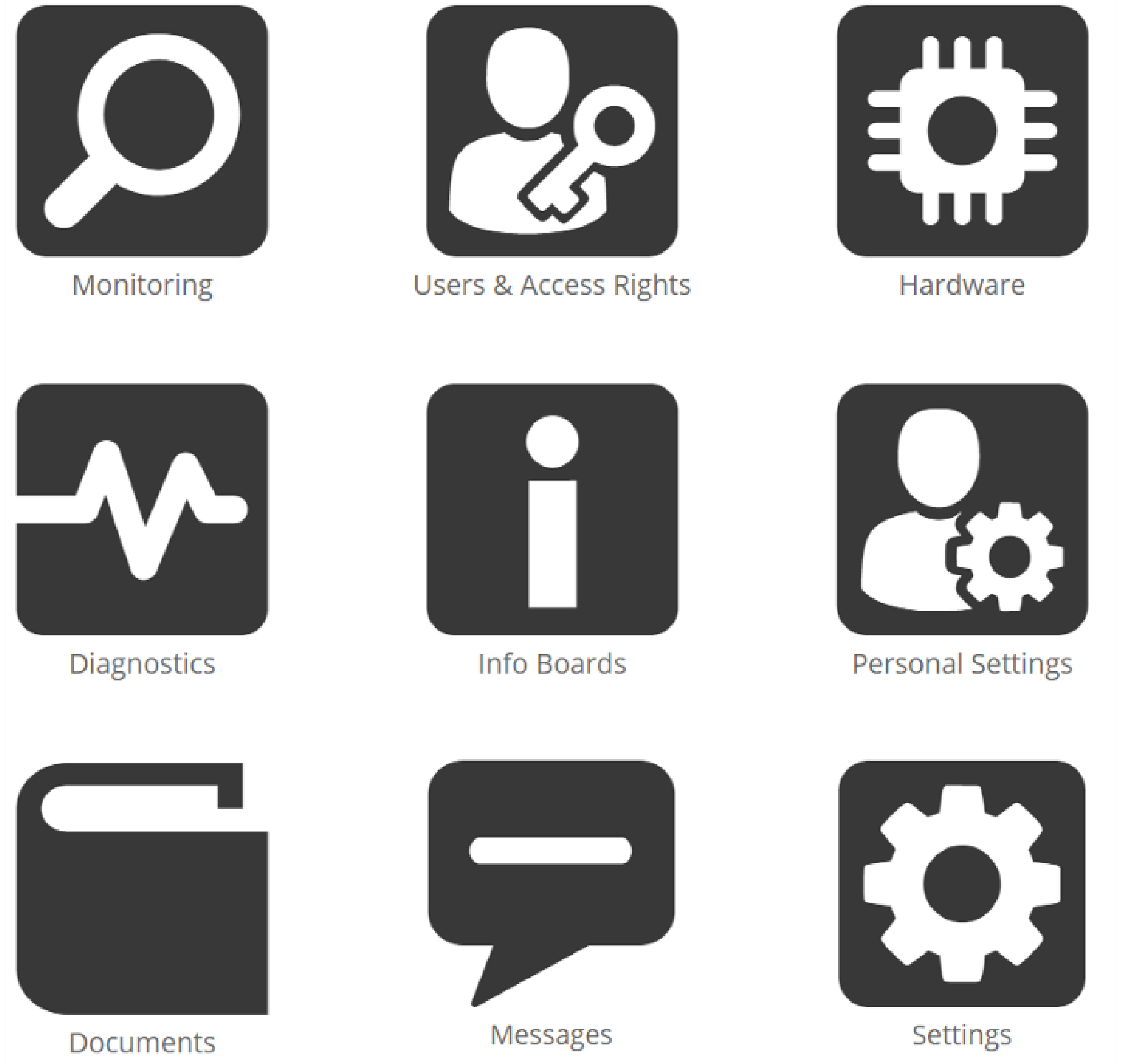
MAN8007 version 3.5.1

Nova 3.5 software Administrator manual



The functions work from 9. 5. 2025 with the Nova software 3.5.X

Table of Contents

Explanations of words and concepts

Central:	An electronic device, an integral part of an access control system.
NovaServer:	A designated computer that runs the same software as the central. Can also be a cloud solution.
Nova:	The software that is running on each central and can be accessed with a regular internet browser.
ID card:	The identification card could be a MIFARE card, EM Marine card, DESFire card…
PIN:	Personal identification number
Reader:	An electronic device used to register ID cards and PINs with central.
UHF reader:	Reader that supports Ultra-High frequency – used for long range detection.
LPR reader:	A camera that reports the car's license plate to Nova.
Access group:	A group consisting of specifically defined doors. A user is assigned one or more access groups. The user has then been granted access through the doors defined in the access groups.
REX:	Request to exit
DM:	Door monitor
LAN:	Local area network
WLAN:	Wireless local area network
WAN:	Wide area network
DHCP:	A network management protocol used for dynamically assigned IP addresses.
RS-485:	A communication standard that supports multiple devices on the same bus (2 wires). Each device has a designated address.
MAC:	Media access control address – usually noted on the side sicker of the central.
GUI:	Graphical User Interface – the user-friendly software for controlling the central.
HTTP:	Hypertext Transfer Protocol - old and unsafe
HTTPS:	Secure version of HTTP.
Custom certificates:	A user can upload their own domain certificates which makes access over HTTPS safe and secure.
Web port:	Used for accessing GUI – if access is done over HTTP, port 80 is used; over HTTPS, port 443 is used. This can also be changed for ease of port forwarding.
SSH:	A secure protocol used for accessing log on malfunctioning centrals. Disabled by default, enabled on demand.
NFC:	Near field communication – present on modern mobile

	phones and on online readers.
DoorApp:	A phone application used for unlocking doors.
Module:	Part of the Nova software that can be unlocked by providing the activation key.
Activation key:	Code that unlocks and expands Nova with additional features. Activation key only lasts for 30 days but can be made permanent by system registration.
System registration:	Unused activation keys can be deleted and used elsewhere (if less than 30 days have passed). Once the set-up is finished, the system administrator must register the system. The keys are now permanently tied to the system. Registration with the same activation key on the other system is not possible.
NovaSimpli, Nova10, Nova100, NovaServer:	The main activation key that brings main functionalities to the system. The number defines how many doors they can manage, making Nova10 suitable for small systems, Nova100 for medium-sized ones etc. Additional door or user extension can be added by providing the suitable activation key.
Account type:	Different account types have access to different parts of Nova. System administrator for ex. Has full access, while the standard administrator can only manage users and their access rights.
Apartment:	Virtual apartments can be created, and users can be assigned to them. The apartment can then be assigned to show the user's credentials (name, last name) on the door station, mailbox, info board etc.
Anti-pass back:	Functionality that allows the user to enter/exit only once per set period.
Presence:	A module that counts and displays users who have entered/exited through the entry/exit readers.
Floor plan:	Facility's blueprint can be uploaded and used to display the location of the readers, centrals, cameras, presence counters etc. Important events like access, break-ins, disconnects are also shown with full details. Doors and cameras can also be managed from this overview.
Door widget:	Easy way to open or unlock the door with a few clicks once a user is logged into Nova.
Weblink door widget:	Creates a sharable link. This way the access can be shared with other people. Links can also be saved and stored on the mobile phone's home screen.
Special day:	Like holiday – a special schedule is in use; this affects all the readers and automatic schedules.
Exception day:	Has the highest priority, but only affects the readers that

	use the schedule where the exception day special schedule was applied.
Card authorization:	Administrator issues user non-working user card that will only start working when the 2nd administrator authorizes them in combination with a special Authorization card.
Offline reader:	A reader that is set-up with a dedicated set of cards designed for doors on the remote locations or doors that do not support electric lock. The access rights for this reader are written on the card.
Offline authentication key:	Each system that includes offline readers is locked with a unique key. This unique key prevents access from another system.
Wireless online:	This is an antenna that wirelessly communicates with the offline reader(s) and reports all the events to the central. The offline readers in range of the antenna can be managed (open, unlock, lock) from Nova.
Configuration database:	A database that contains all the users, access groups, access rights and hardware data.
Events database:	The database contains event history up to 1 million events on central and up to 10 million on NovaServer.
XML API:	Pre-defined requests that allow 3rd party software to manage Nova configurations, users, identification devices and access groups.
(Python) script:	A custom script made in Python programming language, constantly running on the central and can be re-programmed to react on monitored events.
Custom events:	User made event, that can be set to trigger at chosen action to engage Python script's activity.
Booking terminal:	A designated terminal that displays availability of booking locations.
Info board driver:	A designated device that can display pre-set layout on the display. The content of the layout can be created in Nova and can vary from presentations to pictures or even display data from the apartments.
Elevator controller:	Central used for integration with the elevators. Users can get access only to the floors based on the assigned access group.
Parking controller:	Central that supports parking barriers, vehicle detections and can send light signals based on occupancy.
Local administrator:	An administrator that can only manage his own users and only part of the hardware that was assigned to him.
2FA:	Two-factor authentication can be enabled if the High security module is activated. This form of log-in requires password first and after it requires the code that was sent to

	the user’s email or SMS.
USB reader:	A special reader that can be connected to USB and using the dedicated software, it connects to the central and can write offline rights to the user cards.
Mini Cloud:	A cloud-based solution for small systems, where they can access Nova on the internet and use a USB reader to write access to the cards. Works with offline readers only and avoids costs of having a central.
Central discover tool:	A tool that searches the network for the connected centrals, IP cameras, info board drivers, UHF and LPR readers. The tool also supports changing the IP of the devices, so everyone has its own address.
FC:	Facility code used as part of the Wiegand card ID.

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. They allow the user to access and use different doors in pre-specified time intervals.
The following manual describes the basic concepts for optimal use of the Nova software.
The name "Nova" is used throughout this manual for addressing the different software versions:

- NovaSimpli (order code 804-001-000)
- NovaSimpli350 (804-001-350)
- Nova10 (804-001-0010)
- Nova100 (804-001-0100)
- NovaServer (804-001-0500)

The core concepts in all software versions are identical. The differences between them will be explained when applicable. In most cases, the applications have different limits regarding the number of users, number of doors, and some special functions.
More information about activation keys needed in chapter **6.1 Add-ons and Modules**.

Nova software limitations

Nova10 and Nova100 limitations

CPU limitation of the central Alpha affects the service of a web interface and automated data replication. Complex systems with numerous events, changes, and integrated modules (e.g., Info boards) can soon reach Nova100's limitations. An upgrade to NovaServer is suggested when one of the limits is reached:

(a) Max. 25 online centrals
(b) Max. 100 online or wireless online readers
(c) Max. 250 offline readers (with reader expansion modules)
(d) Max. 5.000 users (with user expansion modules)
(e) Max. 100 user photos can be stored on centrals Alpha2 or Alpha4. Use Alpha2+ or Alpha4+ with Alpha USB flash drive for extra storage when you have more than 100 user photos.
(f) Max. 5 Info boards can be used with Alpha2+ or Alpha4+ and Alpha USB flash drive.
(g) A burst of log volume due to 4 door openings per second on each central or continuous opening of 2 doors per second on the complete system

NovaServer and Virtual NovaServer limitations

NovaServer has a powerful CPU, but limitations should be considered for slave centrals. Please get in contact when one of the limits is reached:

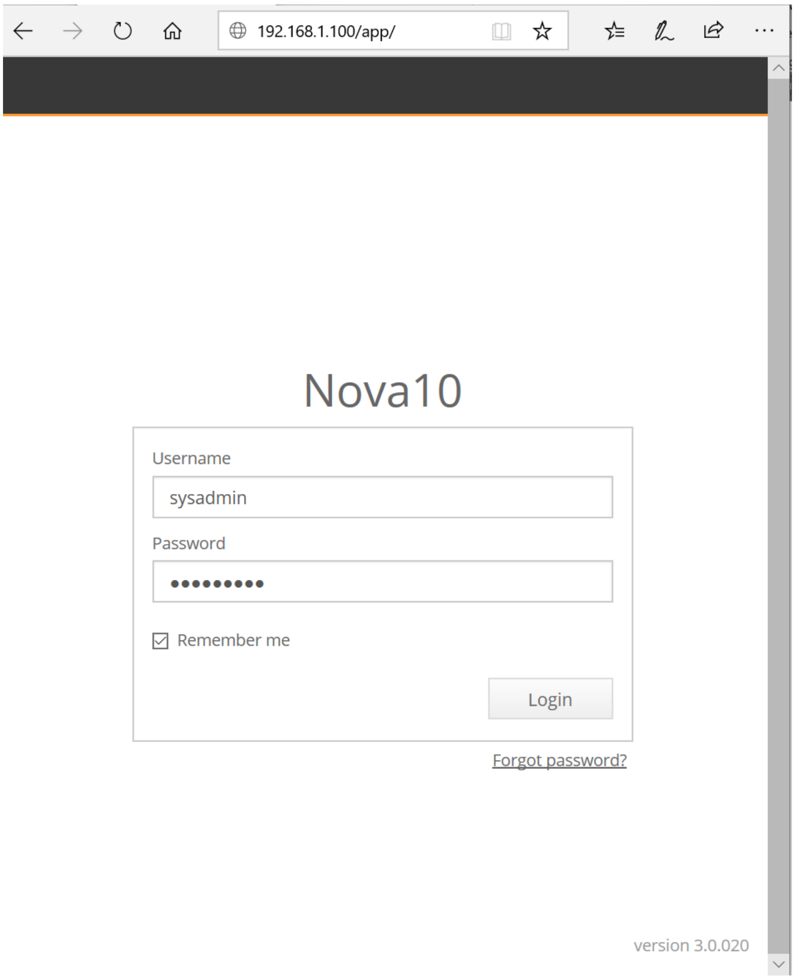
(a) Max. 250 online centrals
(b) Max. 5.000 online, wireless online or offline readers (with reader expansion modules)
(c) Max. 50.000 users (with user expansion modules)
(d) Max. 5.000 access groups
(e) Max. 100 Info boards
(f) A burst of log volume due to 4 door openings per second on each central or continuous opening of 10 doors per second on the complete system

1. Login page

Open a web browser and navigate to the IP address of your central.

- (Default central address is "**https://192.168.1.100**" Picture 1-1).

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



Nova10

Username

sysadmin

Password

●●●●●●●●●

☑ Remember me

Login

Forgot password?

version 3.0.020

Picture 1.1: Login page

- Type your username and password into the login page (Picture 1-1).
  If logging in for the first time, use predefined:
  - Username: **sysadmin**
  - Password: **sys4Admin**

NOTE: Passwords are case sensitive.

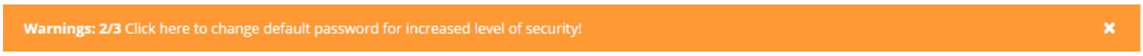
If login credentials were correct, the home page of the Nova software will appear on the screen.

Forgot password – if a user has an email or phone provided in the Nova account, the request to reset the password can be sent. **This function is not compatible with two-factor authentication.**

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

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

Clicking the message will allow the administrator to change the settings described in the message, otherwise clicking the X button (displayed on Picture 1-2) will prevent them from showing up again.



Warnings: 2/3 Click here to change default password for increased level of security!

Picture 1.2: Warning message

1.1.1 Account types

Nova software implements different types of accounts:

- **User** – a normal user login, can change some of its information, can add door widgets that have access to, has access to files (uploaded by sysadmin), and access to booking.
- **User (read-only)** is used only for booking module. If this user's login information is provided for booking login, the clients that have a link to the calendar can freely browse the calendar without a session drop (designed for displaying booking availability only!).
- **Checkpoint user login –** only has access to checkpoint widget, where he can monitor the cards that pass over a pre-defined reader.
- **Print administrator** – has access to all users (can create user, change their PIN, name, last name, account validity, additional fields, add Cards or Unauthorized cards, can set default card layout), card designer card/user reports and booking. He cannot manage access groups or any other user data.
- **Local admin** – can only manage pre-defined user and hardware list. He can create new users that are automatically added to his user list and are invisible to another local administrator (the same goes for time schedules and access groups).
- **Booking administrator** – used for receptionist for ex., they can create a booking for other people, they can also confirm user's booking reservations (if set-up).

- **Visitor manager –** uses its own part of the GUI to add visitors which are separated from regular users. Access groups are pre-determined. USB reader is required.
- **Administrator account** is used for the day-to-day system administration and permits/allows the management of users, access groups, schedules, and control of doors in the system.
- **The system administrator account** is used by the person installing the system and managing the hardware (e.g., adding centrals and readers).
  NOTE: Do not use this account in the normal workflow.
  Since this account controls the access of all other administrator accounts, it should be assigned to the IT-responsible, the installing contractor, etc.
- **A super administrator account** is primarily used for support purposes. This account is disabled by default.
  The System administrator can enable/disable the Super administrator account by navigating to **Home > Settings > Login Settings > Super administrator**.

In case the system administrator does not have access to the GUI, a super administrator account can also be enabled by a short press of the left button (next to the power lines) on any of the centrals.

2. Home page and main navigation

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

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

Widget types:

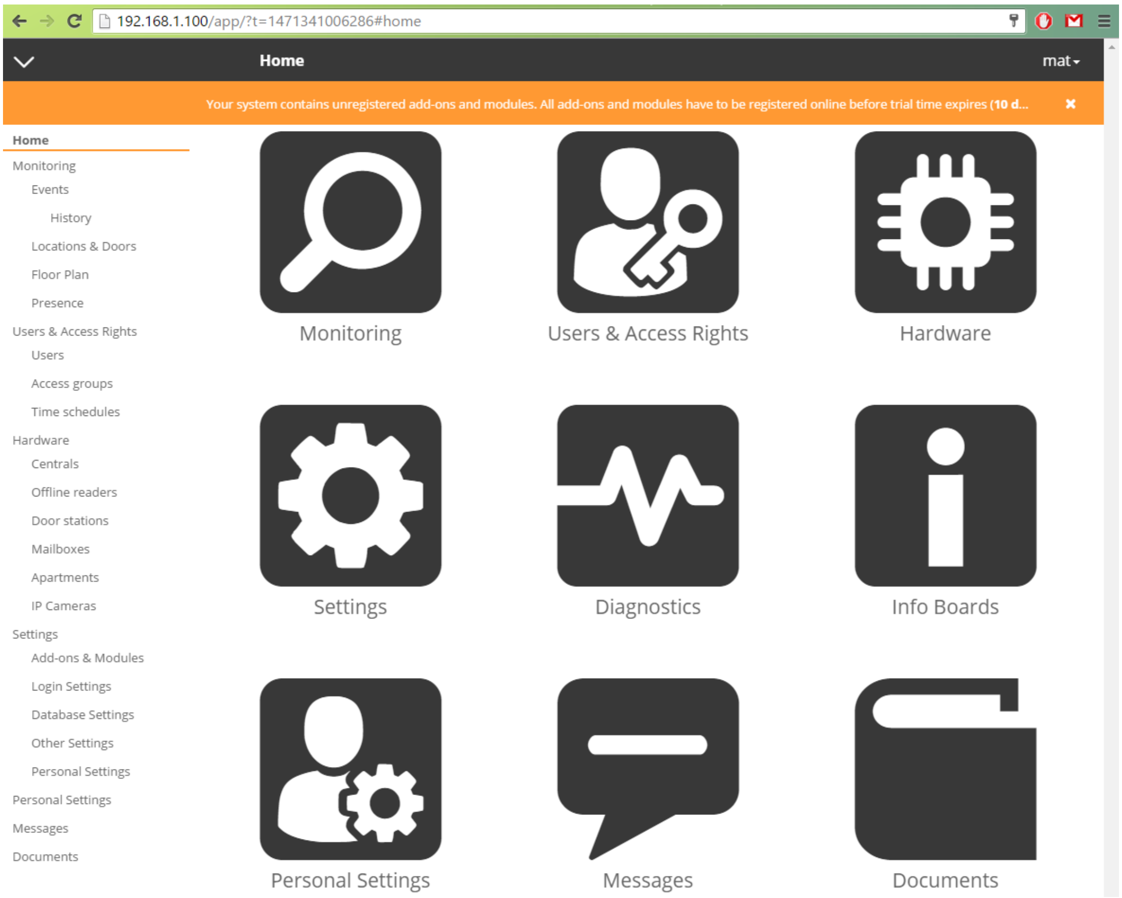
- **Weblink widget** – Can create a link to an external web page or linked file location.
- **Door widget** – Enables opening the desired door with a single click (very handy for mobile access).
- **User widget** – Used for user management.
- **Hardware widgets** – Used for managing system hardware.

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

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

  - **Mailboxes** – Add/edit/delete mailbox units.
- **Settings –** Contains all general/system-wide settings.
  - **Add-ons & modules –** Includes addition and activation of different add-ons and modules.
  - **Login settings –** Language settings, maintenance contact information, password recovery, and new user registration.
  - **Database Settings –** Configuration/Events database download, automatic database backup.
  - **Other Settings –** Time-zone, webserver port, email settings, and unique PINs.
  - **Personal Settings –** Personal language and password.
- **Messages –** API for sending emails or messages to the door stations.
- **Documents –** Important files (seen by everyone) that can be uploaded to the central (maintained by administrator or system administrator).

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



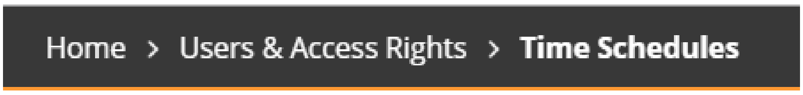
192.168.1.100/app/?t=1471341006286#home

Your system contains unregistered add-ons and modules. All add-ons and modules have to be registered online before trial time expires (10 d...

Picture 2.1: Home page with widgets and navigation menu

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

E.g., to navigate from the **Home** page to **Users & Access Rights** and afterward to **Time Schedules**, simply click on **Users & Access Rights** to return to the wanted widget (Picture 2-2).



Home > Users & Access Rights > **Time Schedules**

Picture 2.2: Steps and access to the current widget

By clicking on the username on the right side of the header, a dropdown menu will display:

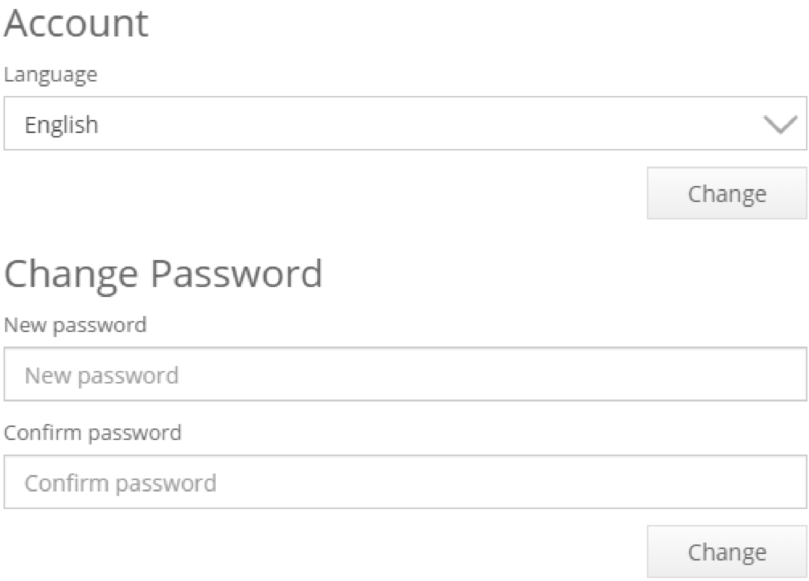
- **Account** – For managing currently logged-in account settings – furtherly described in chapter 2.1 Account settings.
- **Widgets –** Used to create User widgets. Description of details is described in chapter 2.2 Creating user widgets.
- **Logout –** Logs out the current user.
- **Version number**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

2.1 Account settings

This option enables a user to manage their account.

Basic settings:

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



Account

Language: English

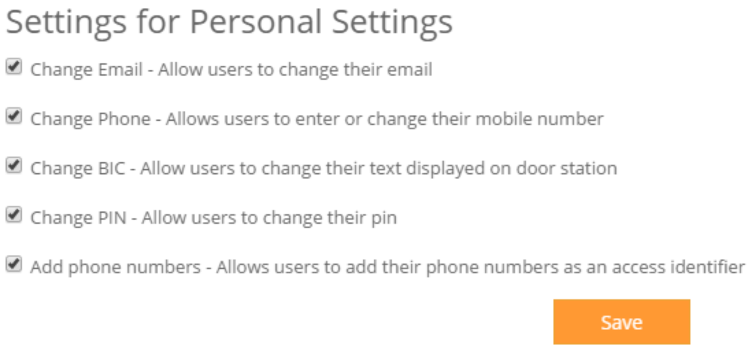
Change Password

New password

Confirm password

Picture 2.3: Users can change their language and password.

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



Settings for Personal Settings

☑ Change Email - Allow users to change their email

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

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

☑ Change PIN - Allow users to change their pin

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

Picture 2.4: Extended user personal settings

Extended user settings consist of:

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

2.2 Creating user widgets

2.2.1 Module: Door widgets

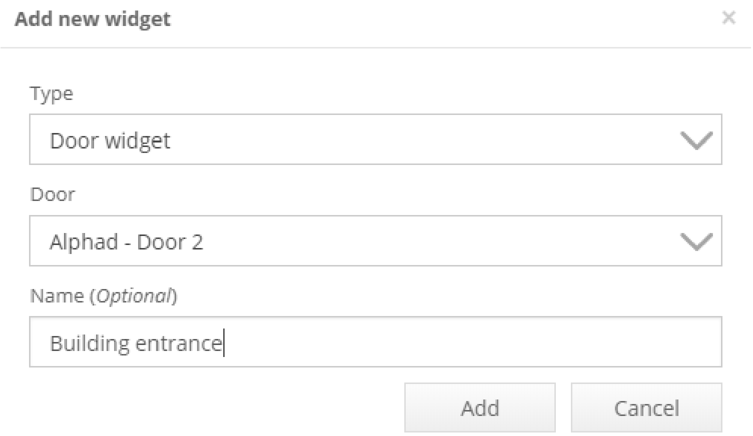
This module enables user's that have access to Nova to easily open the door(s) from the GUI. To activate this key, please follow the instruction in chapter **6.1 Add-ons and Modules**.

NOTE: Widgets created by Sysadmin or admin for themselves are free and are not counted toward the widget license quota.

IMPORTANT: When the first user's widget is created by a user/admin, it starts to count toward the widget license quota. Multiple widgets per user will still count as one (one person using widgets).

Users can create their widgets by clicking on their usernames while logged in and navigating to the **Widgets** option. By pressing the **Add** button, a new pop-up window will appear. Users who have at least some access rights to that door can create door widgets for specific quick door access. These widgets are only seen by the user who created them.
They will only be able to access the door(s) within their set access schedule.

Widgets can also be created and assigned by administrator; They need to navigate to the user list and **double click the user** they wish to create Widget for, navigate to **Door widgets tab** and create/edit/delete them from there.



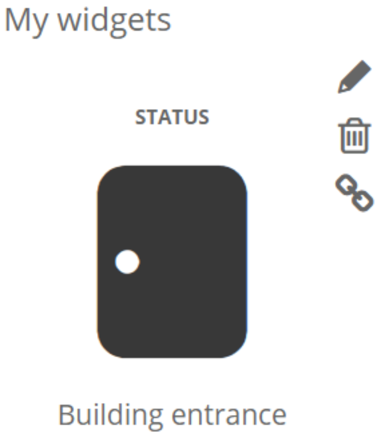
Add new widget

Type: Door widget

Door: Alphad - Door 2

Name (*Optional*): Building entrance

Picture 2.5: Creating a new Door widget



Picture 2.6: Door widget

2.2.2 Door widget - Weblink access

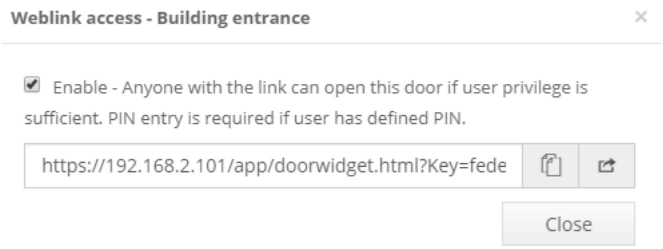
Every widget can generate link access to the door. This is useful for:

- Creating a link and sending it to a person with limited time access (mailman, renter…). A link can be easily copied by pressing the copy icon next to it - Picture 2-7.
- Creating a link widget on the mobile device – pressing the second button on Picture 2-7 will open a link in a new tab which can be saved to the desktop for easy access.

IMPORTANT! Users who enter via the link, in the GUI will be displayed as the Entry of the **user who created the widget**.

Additionally, the link will only work within access times; user validity also affects the ability to open doors.

IMPORTANT! Disabling and re-enabling the link widget will create a brand-new URL while making the old one obsolete.



Weblink access - Building entrance

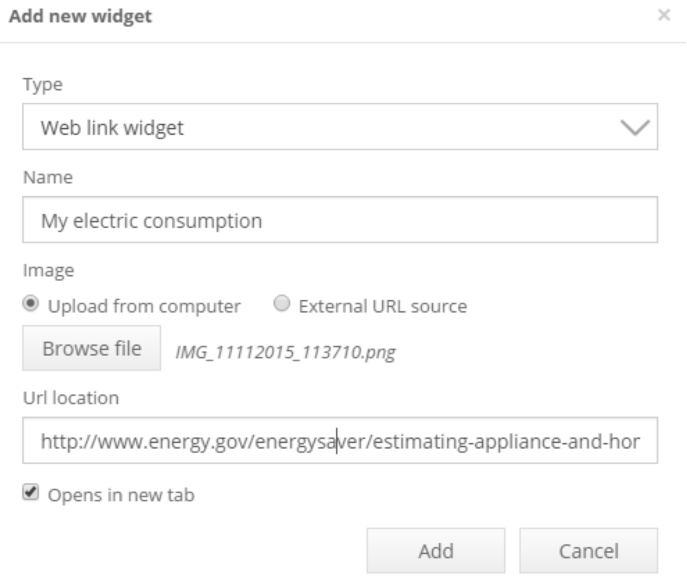
☑ Enable - Anyone with the link can open this door if user privilege is sufficient. PIN entry is required if user has defined PIN.

https://192.168.2.101/app/doorwidget.html?Key=fede

Picture 2.7: Access link

2.2.3 Weblink widget

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



Add new widget

Type: Web link widget

Name: My electric consumption

Image: ● Upload from computer ○ External URL source

Browse file IMG_11112015_113710.png

Url location: http://www.energy.gov/energysaver/estimating-appliance-and-hor

☑ Opens in new tab

Picture 2.8: Creating a Link widget

To create a Link widget:

1. Select widget type.
2. Enter its name.

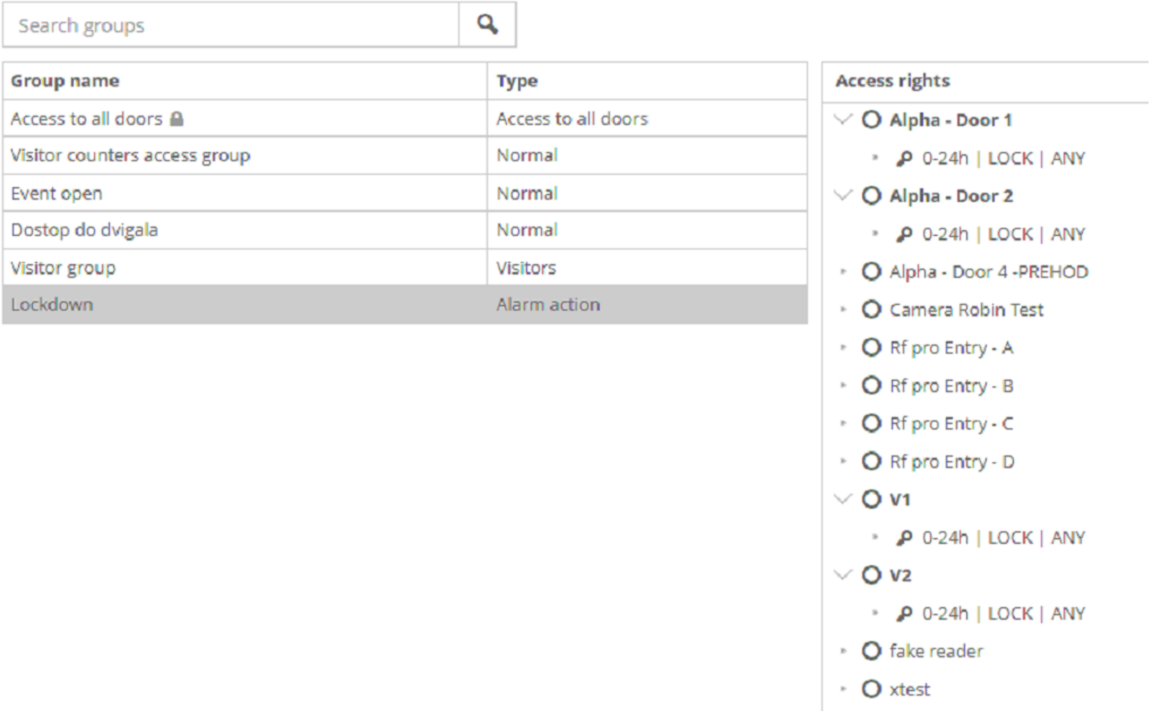
3. Select the picture you wish to display as a cover of the widget (either upload it from the computer or provide the URL address to the picture, e.g., www.example.xyz).
4. Enter the URL address for the link.
5. Tick the checkmark if the webpage should open in a new window (otherwise it will open on the current page).

2.2.4 Widget capable of triggering alarm action

Make sure that you are logged in as sysadmin! (Only sysadmin can **create and assign** these widgets; regular admin level does not have this option available).
Make sure that **all the centrals are updated to Nova 3.3.21 or higher**.
Make sure that **the widget** and **the alarm license** is present in the system.

Creating an ARM widget

1. Create an action group (what you wish to happen when the lockdown button is pressed, specify on those readers: (Access groups > Menu > Add group; provide name, choose Access group type to be Alarm action)).



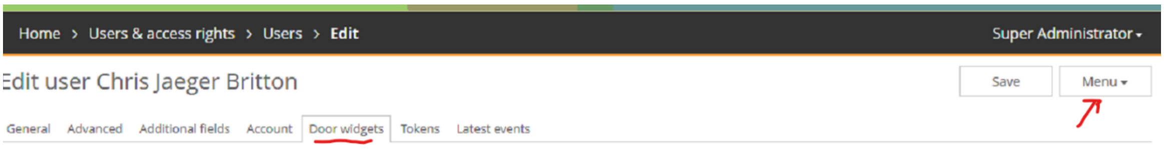
Search groups

Group name	Type
Access to all doors	Access to all doors
Visitor counters access group	Normal
Event open	Normal
Dostop do dvigala	Normal
Visitor group	Visitors
Lockdown	Alarm action

Access rights

- Alpha - Door 1
  - 0-24h \| LOCK \| ANY
- Alpha - Door 2
  - 0-24h \| LOCK \| ANY
- Alpha - Door 4 -PREHOD
- Camera Robin Test
- Rf pro Entry - A
- Rf pro Entry - B
- Rf pro Entry - C
- Rf pro Entry - D
- V1
  - 0-24h \| LOCK \| ANY
- V2
  - 0-24h \| LOCK \| ANY
- fake reader
- xtest

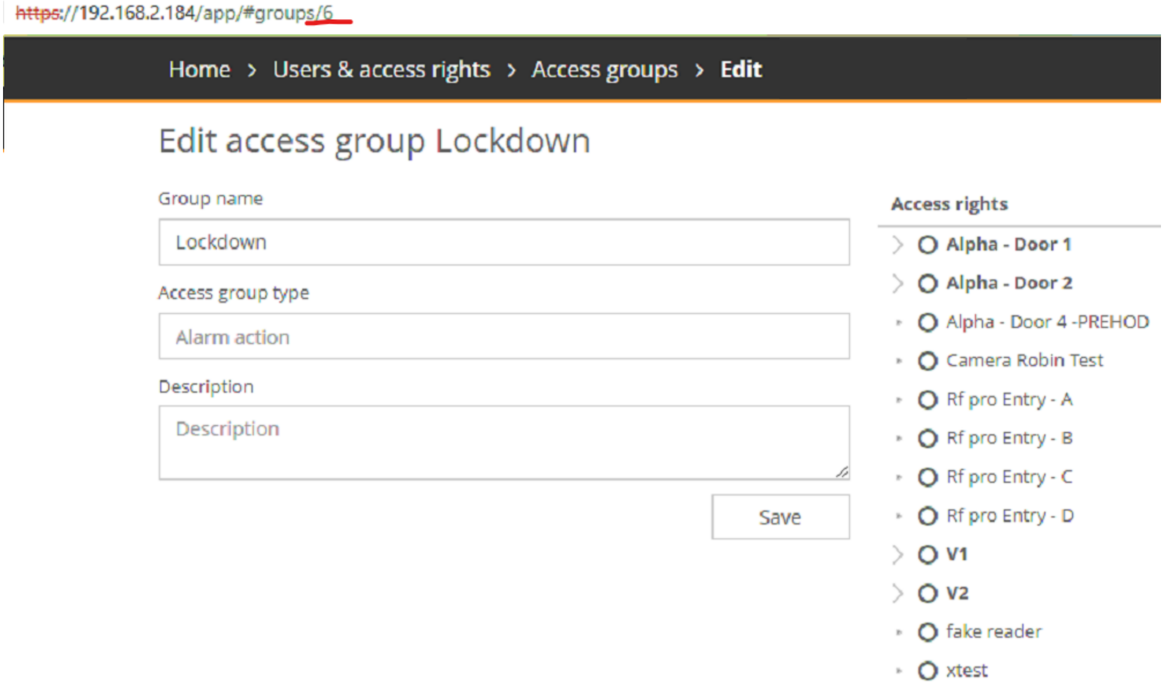
2. Assign a new widget to a user, by navigating to the user list, selecting the user that you wish to create the widget for:
   - (Double click user, navigate to Widgets tab, press Menu > Add new widget)



Home > Users & access rights > Users > Edit

Edit user Chris Jaeger Britton

In the new tab we will need to find out the ID of the alarm group and the ID of the central, so navigate to the alarm group and open it up:



https://192.168.2.184/app/#groups/6

Home > Users & access rights > Access groups > Edit

Edit access group Lockdown

Group name: Lockdown

Access group type: Alarm action

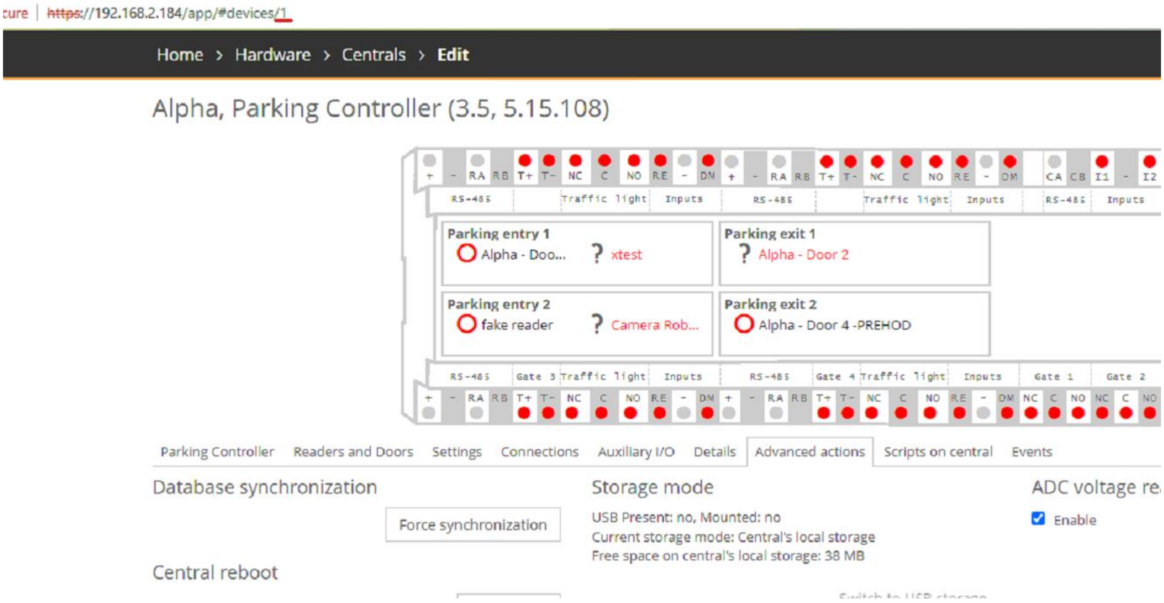
Description: Description

Access rights

- ○ Alpha - Door 1
- ○ Alpha - Door 2
- ○ Alpha - Door 4 -PREHOD
- ○ Camera Robin Test
- ○ Rf pro Entry - A
- ○ Rf pro Entry - B
- ○ Rf pro Entry - C
- ○ Rf pro Entry - D
- ○ V1
- ○ V2
- ○ fake reader
- ○ xtest

In the URL we can see the number 6, this is the id of the group of my demo central.

Then we need to find out the ID of the central that should trigger the lock-down (if you are unsure which one should trigger, use the top master’s id):



https://192.168.2.184/app/#devices/1

Home > Hardware > Centrals > Edit

Alpha, Parking Controller (3.5, 5.15.108)

Parking entry 1: ○ Alpha - Doo... ? xtest

Parking exit 1: ? Alpha - Door 2

Parking entry 2: ○ fake reader ? Camera Rob...

Parking exit 2: ○ Alpha - Door 4 -PREHOD

Database synchronization

Storage mode

USB Present: no, Mounted: no
Current storage mode: Central's local storage
Free space on central's local storage: 38 MB

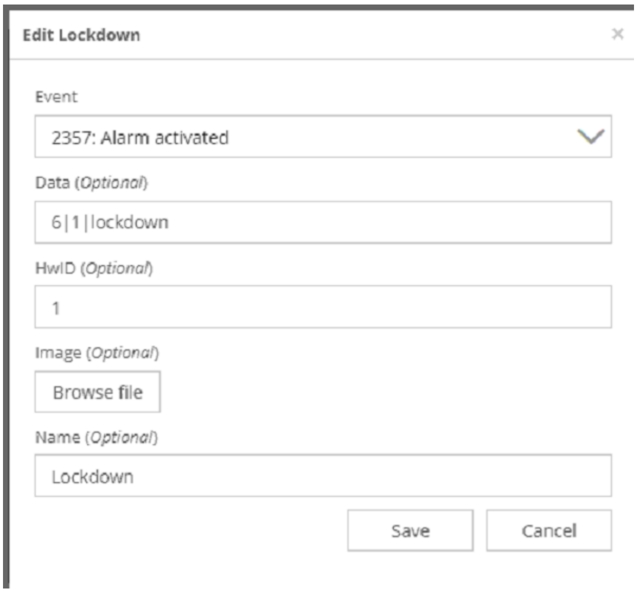
ADC voltage re

☑ Enable

Central reboot

From the URL that the ID of the central I wish the alarm to trigger is 1 in my case.

Close the tab and enter the data into the widget:



Edit Lockdown

Event: 2357: Alarm activated

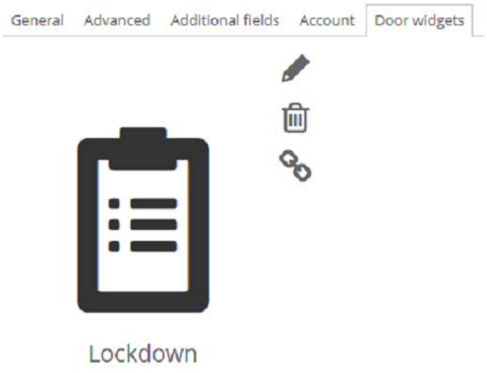
Data (*Optional*): 6|1|lockdown

HwID (*Optional*): 1

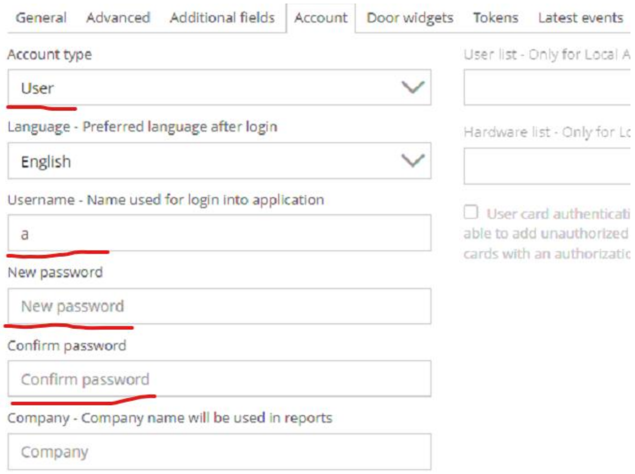
Image (*Optional*)

Name (*Optional*): Lockdown

Choose the Event number 2357 from the dropdown list.
For data you need to provide AlarmGroup ID|Central ID|Name of the lockdown group
For HwID use the Central ID that we have got in the previous step.
Select the picture if you wish, otherwise the widget will look like this:



3. Now that we have assigned the widget to this user, we need to give this user access to this widget:
   (On the user that you have created the widget for, navigate to Account tab, switch the Account type to type User and enter username/password)



Account type

User

Language - Preferred language after login

English

Username - Name used for login into application

a

New password

New password

Confirm password

Confirm password

Company - Company name will be used in reports

Company

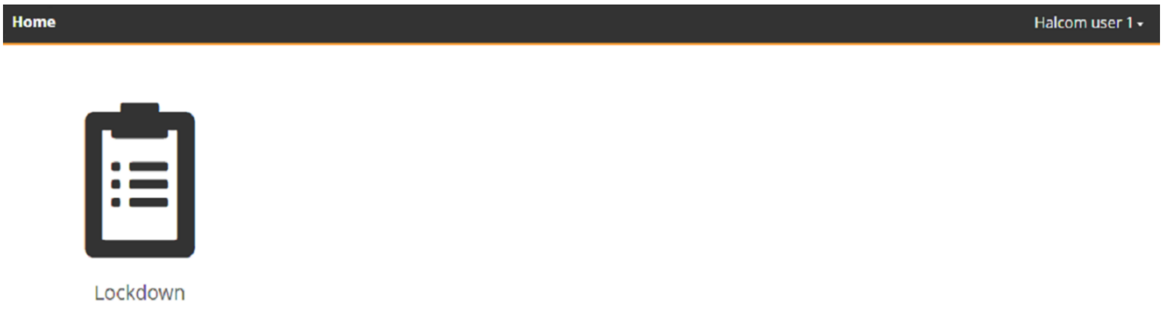
User list - Only for Local A

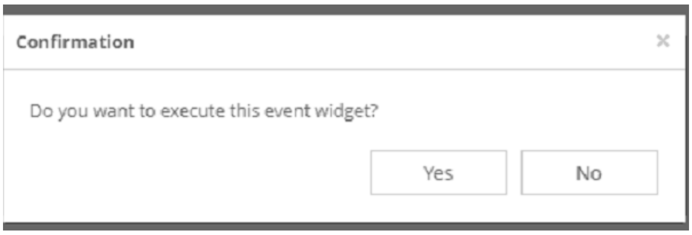
Hardware list - Only for Lc

☐ User card authenticati able to add unauthorized cards with an authorizatic

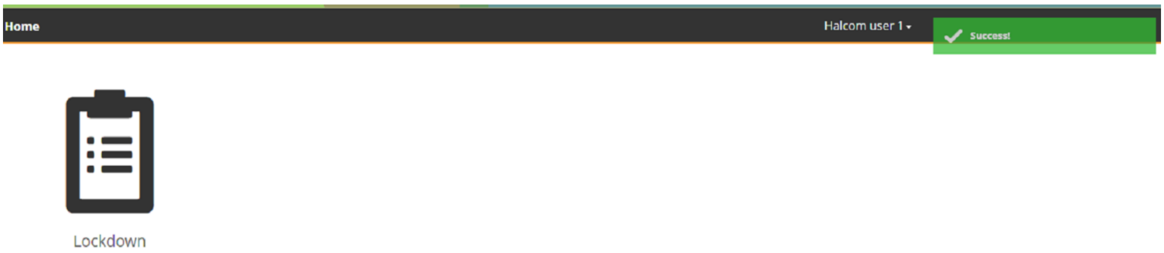
Test its execution:

Logout from existing account and log-into Nova with provided credentials:
User's login should look like this:

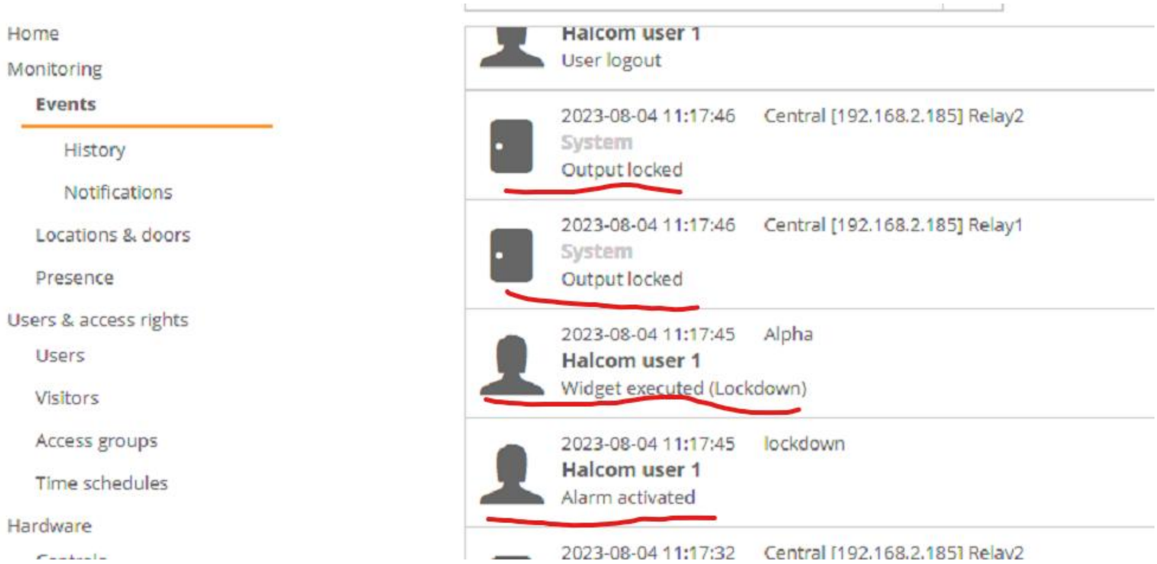




Do you want to execute this event widget?



And the doors should lock if they were unlocked previously.



Halcom user 1
User logout

2023-08-04 11:17:46 Central [192.168.2.185] Relay2
System
Output locked

2023-08-04 11:17:46 Central [192.168.2.185] Relay1
System
Output locked

2023-08-04 11:17:45 Alpha
Halcom user 1
Widget executed (Lockdown)

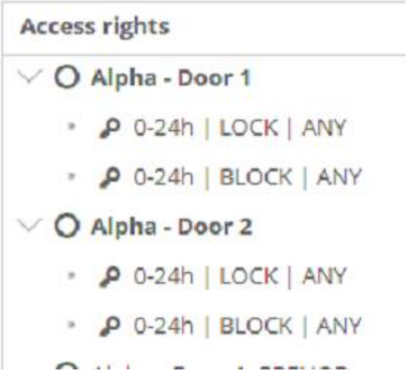
2023-08-04 11:17:45 lockdown
Halcom user 1
Alarm activated

2023-08-04 11:17:32 Central [192.168.2.185] Relay2

Creating an DISARM widget

If you wish to create the lockdown release widget, you use the exact same steps, but instead of the LOCK action which we used in step one, you use the UNLOCK one.

The example that I have used only locks the doors, which means, the tags/cards will still open the door if you put them on the readers.
If you wish to completely block the system so that the cards do not get access anymore, then you can also use the block action additionally like this:

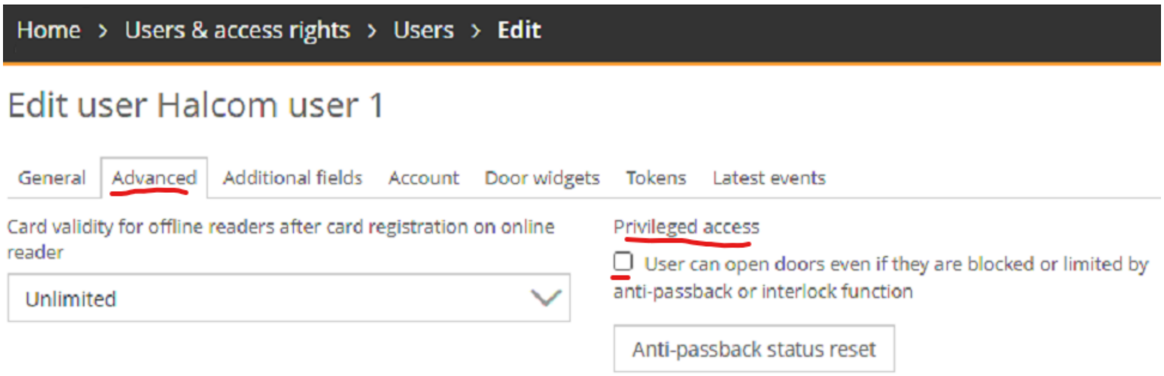


Access rights

○ Alpha - Door 1
- 0-24h | LOCK | ANY
- 0-24h | BLOCK | ANY

○ Alpha - Door 2
- 0-24h | LOCK | ANY
- 0-24h | BLOCK | ANY

In this case, only users that have special privilege get access:



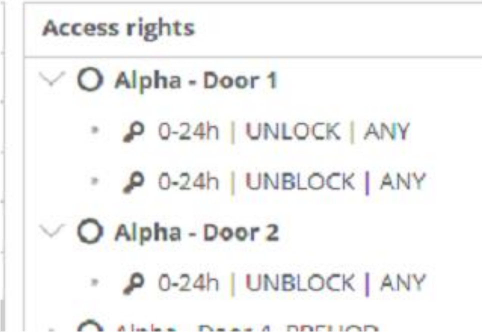
Home > Users & access rights > Users > Edit

Edit user Halcom user 1

Card validity for offline readers after card registration on online reader: Unlimited

Privileged access
□ User can open doors even if they are blocked or limited by anti-passback or interlock function

Once the lockdown is over you need to trigger the unblock action as well like this:



Access rights

- Alpha - Door 1
  - 0-24h | UNLOCK | ANY
  - 0-24h | UNBLOCK | ANY
- Alpha - Door 2
  - 0-24h | UNBLOCK | ANY

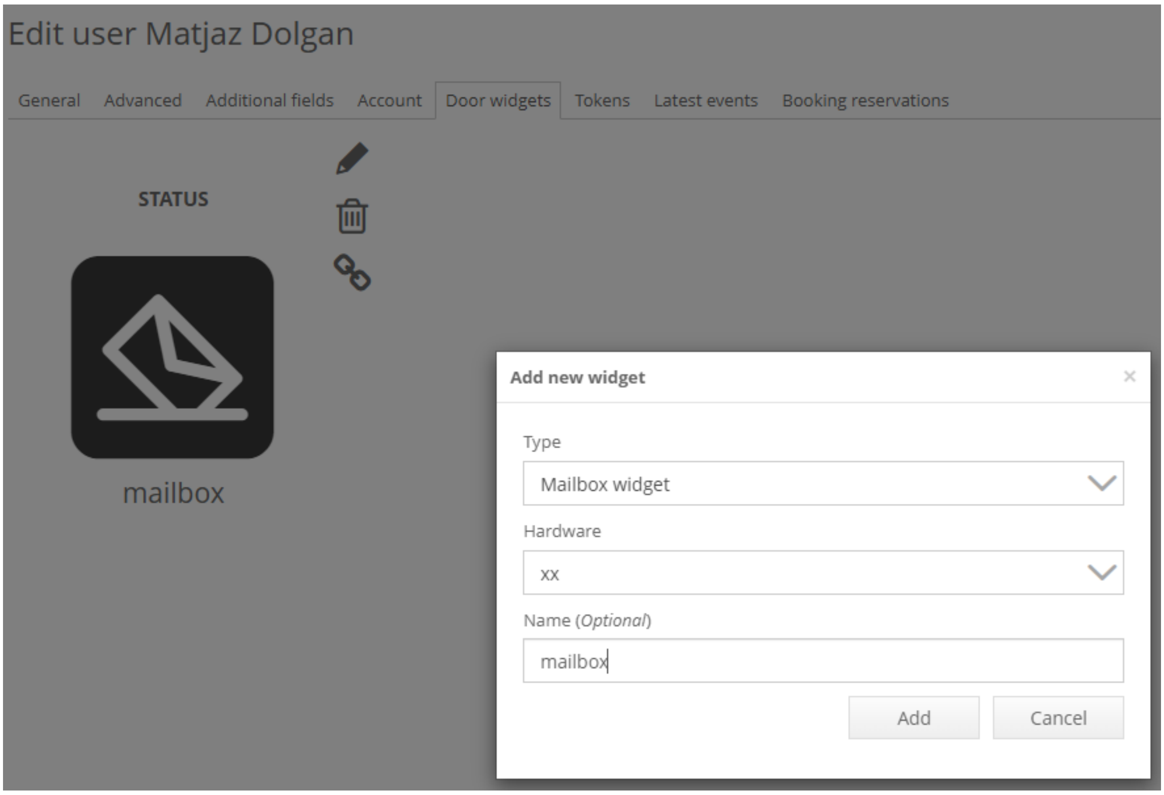
In my case the Door 1 will **unblock** and **unlock** and the Door 2 shall **remain locked but unblocked** after the Lockdown release.

2.2.5 Mailbox Widget

IMPORTANT! This widget can be created by admin/sysadmin only for themselves or the other users.

To create this widget, open the wanted user and navigate to **Widgets** tab, **Menu > Add new widget** and select **Mailbox** as type, select which mailbox you wish to open (only if apartment is assigned to a mailbox will show up) and give you can give it a name.

When the user logs into Nova, they will be able to open their mailbox by pressing on the widget.



Edit user Matjaz Dolgan

Add new widget

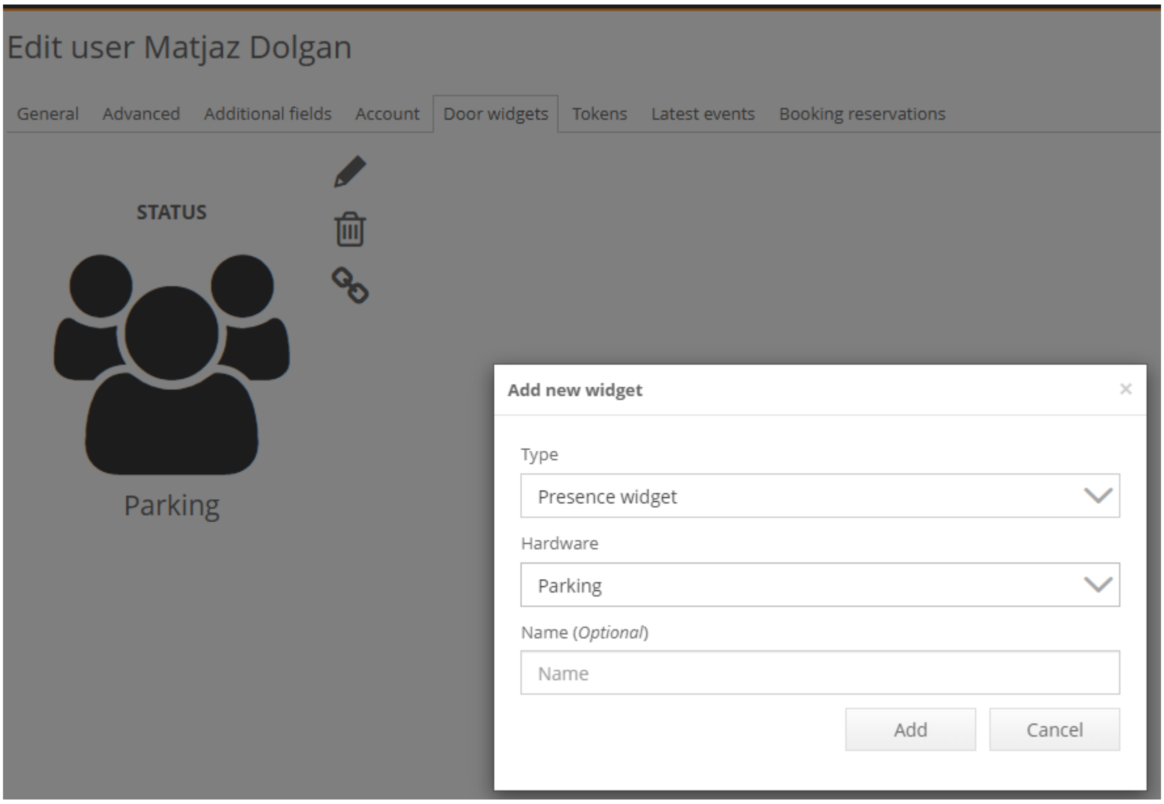
Type: Mailbox widget

Hardware: xx

Name (*Optional*): mailbox

2.2.6 Presence Widget

IMPORTANT! This widget can be created by admin/sysadmin only for themselves or the other users.
To create this widget, open the wanted user and navigate to **Widgets** tab, **Menu > Add new widget** and select **Presence** as type, select which presence you wish to display.
When the user logs into Nova, they will be able to see the **occupancy of the presence location, but not who is inside!**



Edit user Matjaz Dolgan

Add new widget

Type: Presence widget

Hardware: Parking

Name (Optional): Name

2.2.7 Elevator Widget

IMPORTANT! This widget can be created by admin/sysadmin only for themselves or the other users.
To create this widget, open the wanted user and navigate to **Widgets** tab, **Menu > Add new widget** and select **Elevator** as type, select which elevator controller you wish to use.
When the user logs into Nova, they will be able to press the widget which will enable the destinations in the elevator.

2.2.8 Alarm area Widget

IMPORTANT! This widget can be created by admin/sysadmin only for themselves or the other users.
To create this widget, open the wanted user and navigate to **Widgets** tab, **Menu > Add new widget** and select **Alarm area** as type, select which alarm area you wish to manage.

When the user logs into Nova, they will be able to press the widget which will enable the destinations in the elevator.

3. Event monitor

Monitoring widget is divided into:

3.1 Events button

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

NOTE: The events are not deleted, just temporarily hidden from the user.
When the Events page is loaded, it displays the last 50 events. This number extends to 300 if the browser page stays open while new events are added. Live events can be filtered by typing the keyword into the text box on the top of the panel (e.g., Reader connected).

Right panel: System information, Errors, Warnings, Disconnected centrals, and readers and unlocked and blocked doors.
These panels show the current state of the system:

- *System information:* shows the number of present doors and users,
  the current time on the central, database usage, and uptime of the central.
  Clicking on the time stamp will send a request to update time on all centrals in the system.

- Errors and Warnings, Disconnected centrals, and readers and
  Unlocked and blocked doors show what needs to be inspected

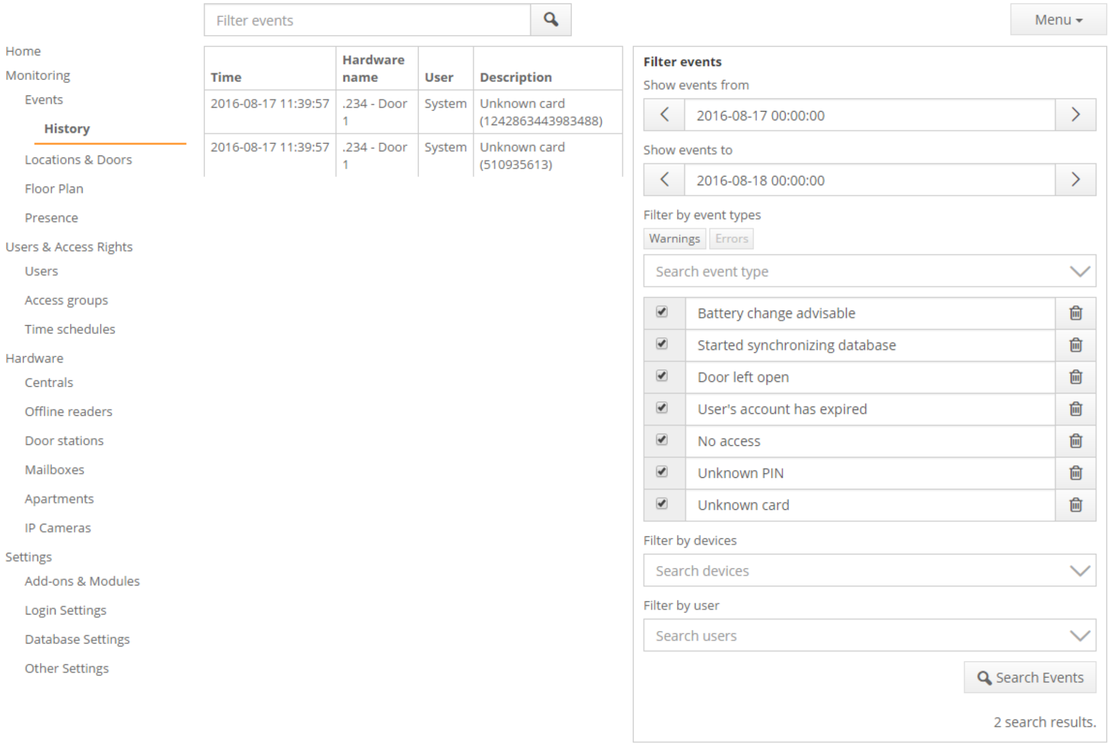
3.1.1 Event history

The event history is accessible by navigating to **Menu > History**.
The right panel offers the user a variety of filter types. The first filter is to set the beginning and the end of the time frame for searched events.
By clicking on predetermined tags, the events for that tag will automatically be selected (e.g., Clicking on the "Warnings" tag will select the Unknown PIN, no access events…).
Event types can also be entered manually by selecting them from the dropdown menu.
Selecting the devices from the device filter enables the search to work only on certain hardware.

Events can also be filtered by a specific user(s).
NOTE! Leaving any of the field's empty will result in a selection of all fields from that type.

IMPORTANT! Using a narrow History search will result in fewer results but will require more system resources and hence more time. Searching the events in a larger period will

result in longer waiting times as well. Instead, make your requests short and simple then run them multiple times if required.
The history result page can be printed out or saved to an Excel file by navigating to the **Menu > Print** or **Menu > To Excel**.



Time	Hardware name	User	Description
2016-08-17 11:39:57	.234 - Door 1	System	Unknown card (1242863443983488)
2016-08-17 11:39:57	.234 - Door 1	System	Unknown card (510935613)

Filter events
Show events from: 2016-08-17 00:00:00
Show events to: 2016-08-18 00:00:00
Filter by event types
- ☑ Battery change advisable
- ☑ Started synchronizing database
- ☑ Door left open
- ☑ User's account has expired
- ☑ No access
- ☑ Unknown PIN
- ☑ Unknown card

Filter by devices
Filter by user
2 search results.

Picture 3.1: Event history with "Warnings" filter active

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

NOTE: If you wish for specific columns to be added/exported, go to Menu > Select columns option.

3.1.2 Manage error and warning events

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

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

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

- **Event name** (name can only be changed on custom events)
- Event priority
  - **None** – this event will not be displayed in the table.
  - **Information** – if the event is triggered, it will be displayed on the bottom of the list with a grey icon.
  - **Warning** – if the event is triggered, it will appear between the Information and Error section with a yellow icon.
  - **Error** – if the event is triggered it will be displayed on the top with a red icon next to it.
- **Sound alert** – after the event happens, it will trigger the selected sound notification (their tune can be tested by clicking the button next to it).
- **Text instructions** – if the text instructions are provided, they will be displayed as a note when the operator tries to remove the notification.
- **Reason confirmation** checkbox – if the operator wishes to remove the notification, a response must be provided.

3.1.3 Notifications

Email/DoorApp notification can be sent as info when specific events occur. The messages contents are automatically generated and sent out immediately.

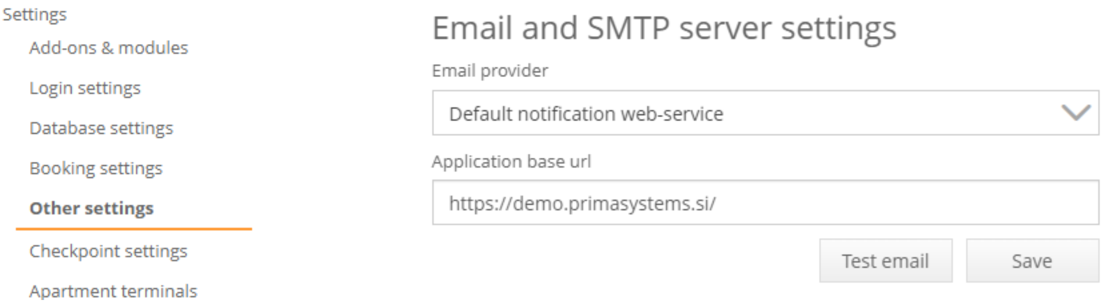
Within the standard Nova 10, Nova 100 and NovaServer basic license, notifications are limited up to 5 emails per day.
High security license grants up to 100 notification emails per day and up DoorApp notifications can be sent.

Note! Notifications sent for tests, booking invitation, custom (python) emails are not counted into quota.

Note! Notification sent to multiple recipients are counted as 1 and if multiple error notifications happen of the same type (for ex. Multiple Central disconnects) within a time, they will be also counted as 1.

IMPORTANT! For notifications to be sent, master central must have access to the internet.

To use a web service for notifications, make sure that the default one is selected in the Email and SMTP settings. Application base URL should point out to DNS or IP, so when you get an email, its content will include the link that will redirect the person who clicks it to Nova.



Settings

Add-ons & modules

Login settings

Database settings

Booking settings

Other settings

Checkpoint settings

Apartment terminals

Email and SMTP server settings

Email provider: Default notification web-service

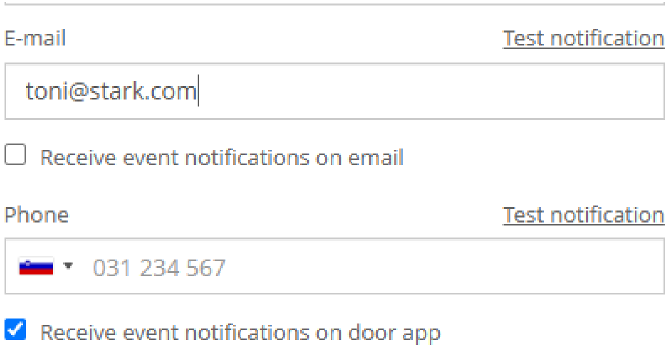
Application base url: https://demo.primasystems.si/

Picture 3.2: Default notification web-service setting

Notification recipients

How to subscribe user(s) to notifications:

1. Navigate to specific user (**Users & access rights > Users > user of choice**).
2. Mark the checkbox to include the email address,
   mark the checkbox to add them as DoorApp notifications recipient.
   The notifications can easily be tested by pressing the Test link.
3. Save changes.



E-mail: toni@stark.com

□ Receive event notifications on email

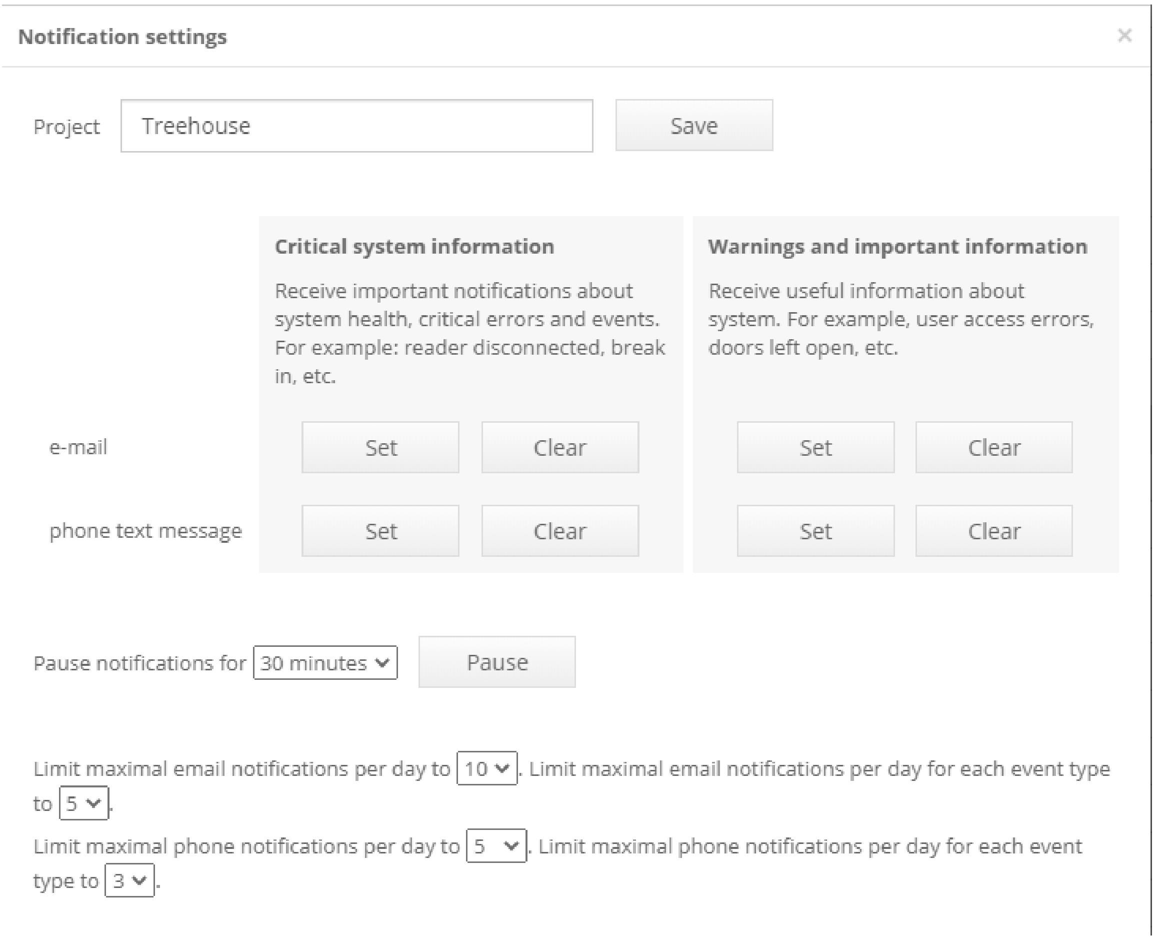
Phone: 031 234 567

☑ Receive event notifications on door app

Picture 3.3: User contact information example

Notification events and limits

If we navigate to **Monitoring > Events > Notifications > Menu – Notification settings**, a dialog shows up:



Notification settings

Project: Treehouse

Critical system information

Receive important notifications about system health, critical errors and events. For example: reader disconnected, break in, etc.

Warnings and important information

Receive useful information about system. For example, user access errors, doors left open, etc.

Pause notifications for 30 minutes

Limit maximal email notifications per day to 10. Limit maximal email notifications per day for each event type to 5.

Limit maximal phone notifications per day to 5. Limit maximal phone notifications per day for each event type to 3.

Picture 3.4: Notification settings and restrictions

Picture 3.4 represents the **notification settings**:

- **Project**: This is helpful to determine from which project the notifications are coming from.
- **Critical system information**: Pressing the Set button will place the checkmark next to the predefined events for the email/phone. This setting focuses on hardware errors/failures.
- **Warnings and important information**: Like the previous point, but focuses more on user interactions.
- **Pause notifications**: For any planned system maintenance, the notifications will be blocked for a set period. This also triggers automatically during the system upgrade.
- **Maximum email limit:** To prevent spam, this limit can be set. Additionally, one can set a limit for each event type.
- **Maximum DoorApp limit:** Same as email limit, but for phones.

Limits can be increased if **High-Security module** is added to the system.

How to add/remove events from the notification list:

- Navigate to **Monitoring > Notifications**.
- Double click on the wanted event or select it and press Menu > Edit

- ○ Select/deselect the notification checkboxes and save.

3.2 Locations & Doors

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

- **Locations** - In the software these buildings and rooms are referred to as locations.
- **Doors** – Doors are assigned to the locations in the form of readers. Readers are added to the system using the hardware widget (see **5.1.13 Adding new readers**).

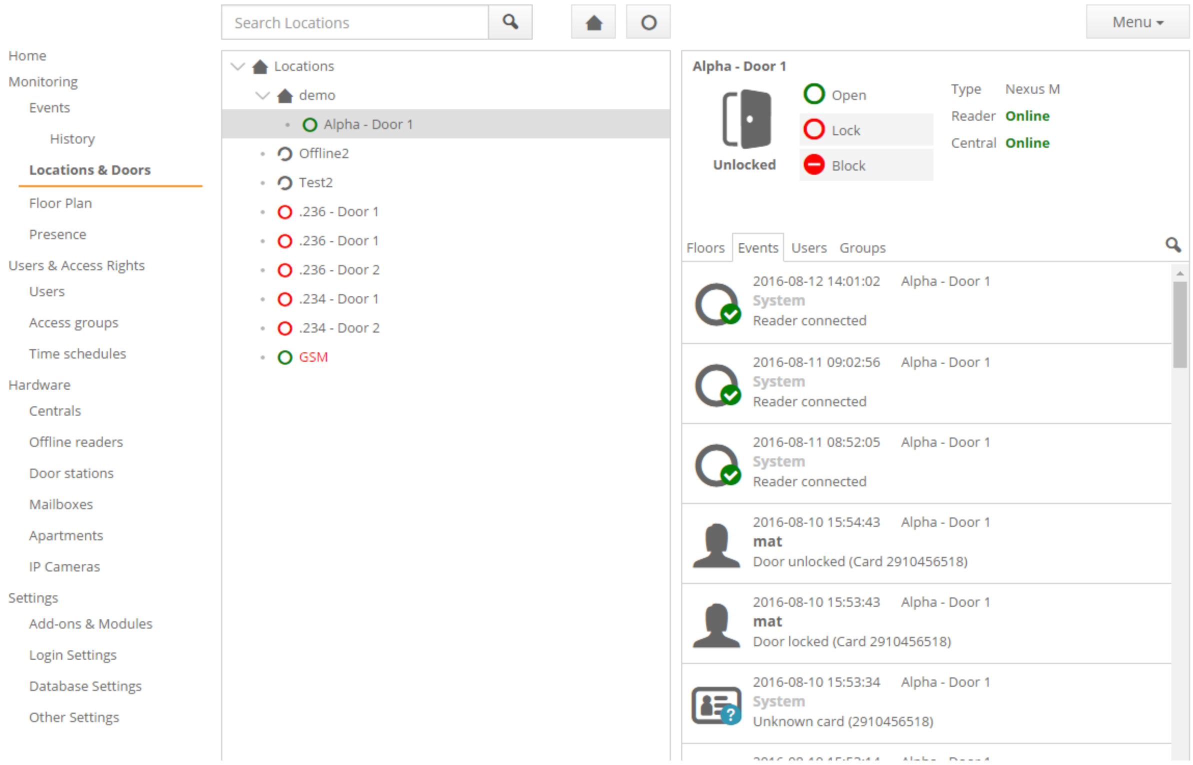
This model represents the logical scheme of the access control system and its components.

Overview of different locations

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

⌂ - Displays only locations and unsorted readers.

○ - Extends the entire tree with all locations and readers.



Alpha - Door 1

Unlocked

Type Nexus M
Reader **Online**
Central **Online**

2016-08-12 14:01:02 Alpha - Door 1
System
Reader connected

2016-08-11 09:02:56 Alpha - Door 1
System
Reader connected

2016-08-11 08:52:05 Alpha - Door 1
System
Reader connected

2016-08-10 15:54:43 Alpha - Door 1
mat
Door unlocked (Card 2910456518)

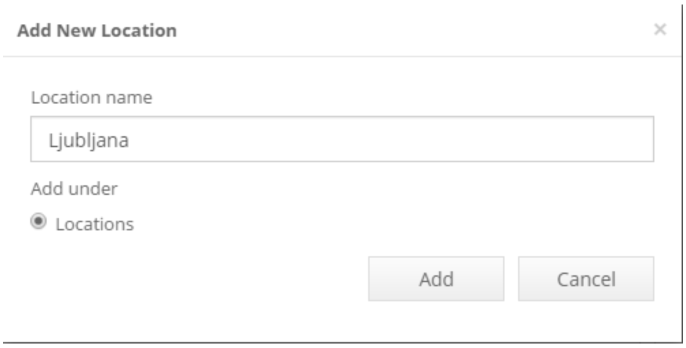
2016-08-10 15:53:43 Alpha - Door 1
mat
Door locked (Card 2910456518)

2016-08-10 15:53:34 Alpha - Door 1
System
Unknown card (2910456518)

Picture 3.5: Locations and detailed information

Adding a new location:

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



Add New Location

Location name

Ljubljana

Add under

● Locations

Picture 3.6: Adding a new location

Renaming locations:

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

Removing location:

1. Select the location you would like to remove.
2. Click on **Menu > Remove location**.

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

Arranging items:

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

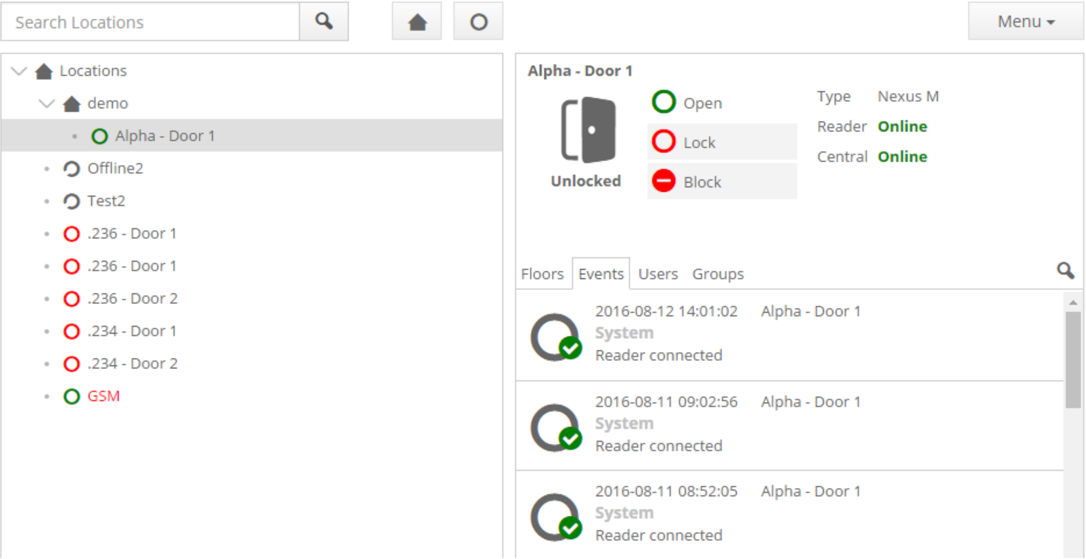
3.2.1 Location management

Selecting a location enables the management of all readers located in the selected location and its sub-locations.
By selecting their location and perform one of the next actions, all readers in the location can simultaneously:

- Lock
- Unlock
- Block
- Unblock

When selecting a reader, the GUI will show:

- Reader status
- Possibility to manage related door (Picture 3-4)



Type Nexus M
Reader **Online**
Central **Online**

2016-08-12 14:01:02 Alpha - Door 1
System
Reader connected

2016-08-11 09:02:56 Alpha - Door 1
System
Reader connected

2016-08-11 08:52:05 Alpha - Door 1
System
Reader connected

Picture 3.7: Location and doors showing all readers in the system assigned to locations

Description of the reader icons:

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

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

1st tab: displays the **Floors** that the reader is shown on. **NOTE:** This tab is only visible if there is a Floorplan module added in the system.
2nd tab: list of last **Events** related to the selected reader (if the selected item is a location, the events are not shown).
3rd tab: list of all **Users** having access rights to the selected item and all connected readers (when the selection is a location).
4th tab: list of **Access groups** that have any access to the selected reader or location.

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

4. Users and Access rights

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

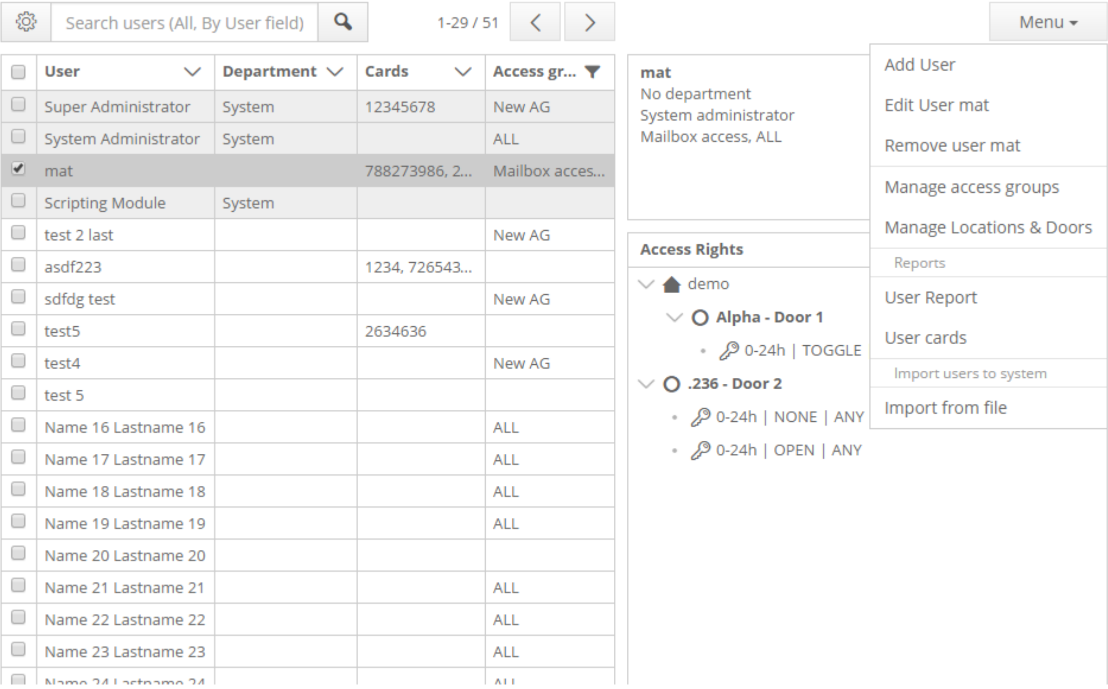
The Users and Access Rights page is used for managing users and the setup of:

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

4.1 Users

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

- Add User (see Picture 4-1)
- Edit User
- Remove User
- Manage access groups
- Select columns – read more about in chapter 4.2.4 Custom user preview.
- Manage Locations and Doors – a redirection to Locations & Doors
- Reports – different types of reports for the specific user(s) or their access cards
- Card designer – comes with an activation key. You can read more about it in chapter 15 Module: Card designer.
- Import users – a function to import users from CSV files



□	User	Department	Cards	Access gr...
□	Super Administrator	System	12345678	New AG
□	System Administrator	System		ALL
☑	mat		788273986, 2...	Mailbox acces...
□	Scripting Module	System		
□	test 2 last			New AG
□	asdf223		1234, 726543...	
□	sdfdg test			New AG
□	test5		2634636	
□	test4			New AG
□	test 5			
□	Name 16 Lastname 16			ALL
□	Name 17 Lastname 17			ALL
□	Name 18 Lastname 18			ALL
□	Name 19 Lastname 19			ALL
□	Name 20 Lastname 20			
□	Name 21 Lastname 21			ALL
□	Name 22 Lastname 22			ALL
□	Name 23 Lastname 23			ALL
□	Name 24 Lastname 24			ALL

mat
No department
System administrator
Mailbox access, ALL

Picture 4.1: User management

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

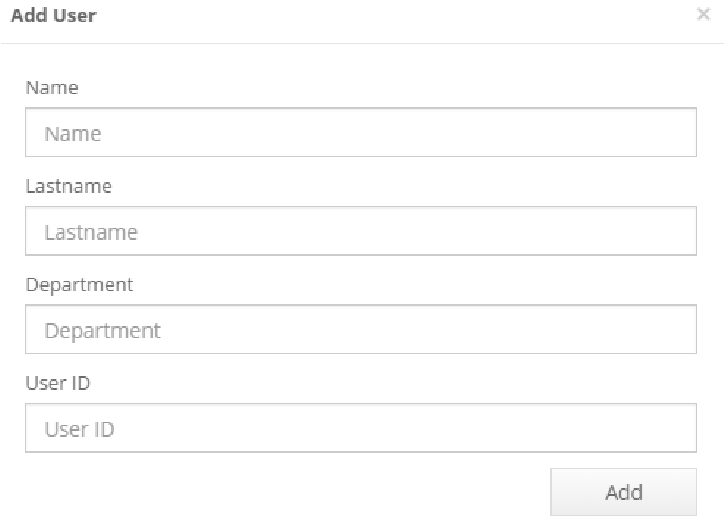
4.2 New users

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

User data can be entered in the new window (Picture 4-2).

- Name
- Last name
- Department
- User ID

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



Picture 4.2: Input for new user data

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

- PIN (must not exceed 20 characters)
  IMPORTANT! Each user needs a unique PIN. The length of the PIN-code on offline readers is limited to a maximum of 7 characters.
  A PIN that does not comply will not work and will not display any warning when trying to write data on a user card when using Card+PIN/PIN+Card.
  IMPORTANT! If a user enters a wrong PIN 5 times in a row, the reader will report Access suspended for any PIN entered in the next 30 seconds.
  - Generate a new PIN – this option generates a pin that is unique and complies with the global PIN length value.
- Card number (usually marked on identification card). Each user can have up to 16 different card numbers/telephone numbers. A table card reader can be used for easier card number input.

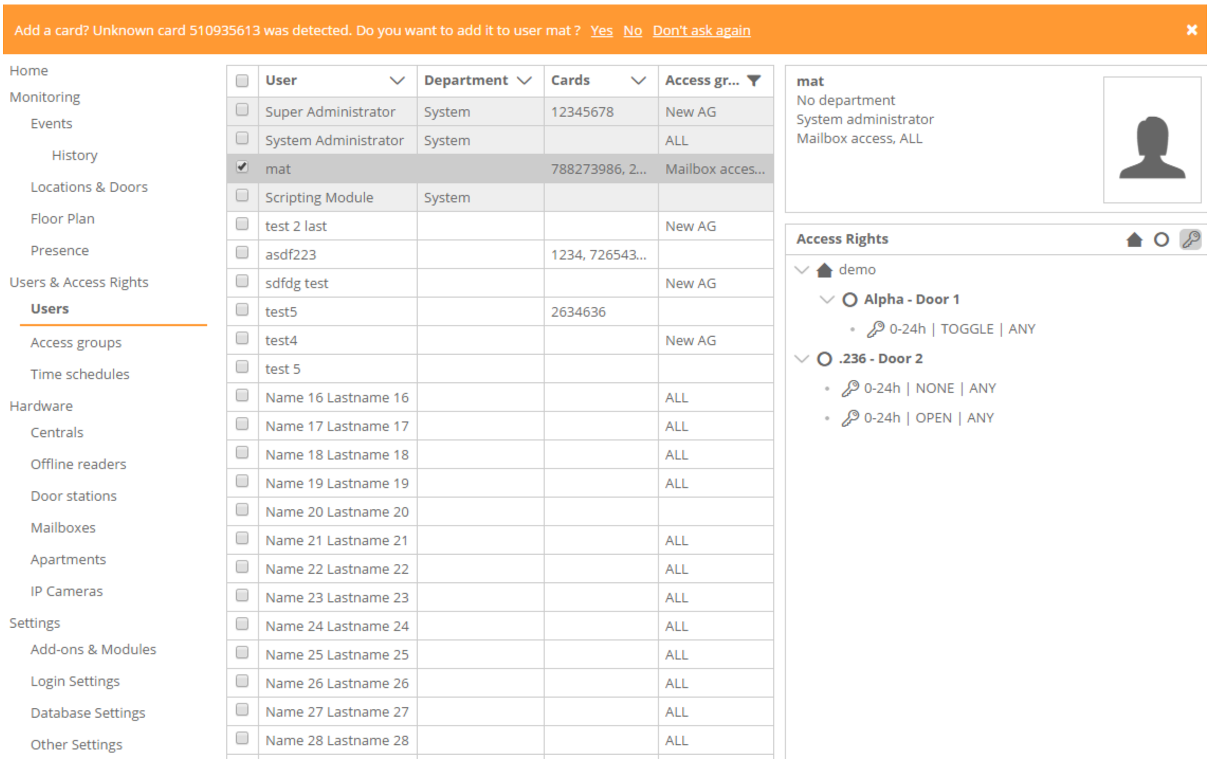
- The validity of the user account (before the start date and after the end date the user will not have valid access rights).
- E-mail, Phone, Address, and Remarks.
- Add a picture

Follow user checkbox will play an alert sound in the GUI if this user creates the event (Entry/Exit, etc.).

4.2.1 Adding unknown card(s) to user

When the system detects an unknown card (i.e., a card that is not assigned to any user) and the user is either currently selected in the user grid or the user editor is open, the option to assign the card to the currently selected user will appear in the bar at the top of the screen (Picture 4-3). In the case that you select that option, the card will automatically be saved and listed like other assigned cards.

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



Add a card? Unknown card 510935613 was detected. Do you want to add it to user mat ? Yes No Don't ask again

☐	User	Department	Cards	Access gr...
☐	Super Administrator	System	12345678	New AG
☐	System Administrator	System		ALL
☑	mat		788273986, 2...	Mailbox acces...
☐	Scripting Module	System		
☐	test 2 last			New AG
☐	asdf223		1234, 726543...	
☐	sdfdg test			New AG
☐	test5		2634636	
☐	test4			New AG
☐	test 5			
☐	Name 16 Lastname 16			ALL
☐	Name 17 Lastname 17			ALL
☐	Name 18 Lastname 18			ALL
☐	Name 19 Lastname 19			ALL
☐	Name 20 Lastname 20			
☐	Name 21 Lastname 21			ALL
☐	Name 22 Lastname 22			ALL
☐	Name 23 Lastname 23			ALL
☐	Name 24 Lastname 24			ALL
☐	Name 25 Lastname 25			ALL
☐	Name 26 Lastname 26			ALL
☐	Name 27 Lastname 27			ALL
☐	Name 28 Lastname 28			ALL

mat
No department
System administrator
Mailbox access, ALL

Access Rights
- demo
  - Alpha - Door 1
    - 0-24h | TOGGLE | ANY
  - .236 - Door 2
    - 0-24h | NONE | ANY
    - 0-24h | OPEN | ANY

Picture 4.3: Assignment of the unknown card to a user

4.2.2 Card function and icon assignment

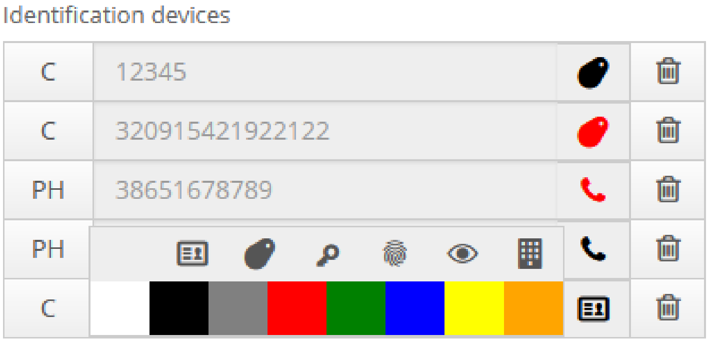
By default, each new card is tagged as **C** (**Card**), but its function can be changed by selecting a new function from the menu that opens (Picture 4-4), when clicking the button to the left of the card number:

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

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

- **WI: Wireless service card** - card for pairing offline readers with Antenna module, also used for firmware upgrade on the offline readers
- **B**: **Battery card** - card for replacing batteries on an offline reader, if applicable
- **DI**: **Disassembly card** - card for disassembling an offline reader, if applicable
- **BL**: **Blacklist card** - card for transferring the list of lost cards to an offline reader
- **CO**: **Configuration card** - card for transferring configuration settings to an offline reader
- **EV**: **Events card** - card for transferring the list of events from an offline reader to the central
- **FO**: **Format card** - the card will be formatted when detected on the online reader
- **U**: **Unauthorized card** - the card will not work until it is activated by the authorization card; after that, it will change its type to C - Card
- **A**: **Authorization card** - used for activating unauthorized cards
- **DA**: **Door App** – used with **22 Prima DoorApp** to open the door using phone’s NFC technology
- **RF**: **Pro remote control** – A remote control used for accessing garage doors, barrier gates, etc.
- **LP**: **License plate** – used with a license plate reader

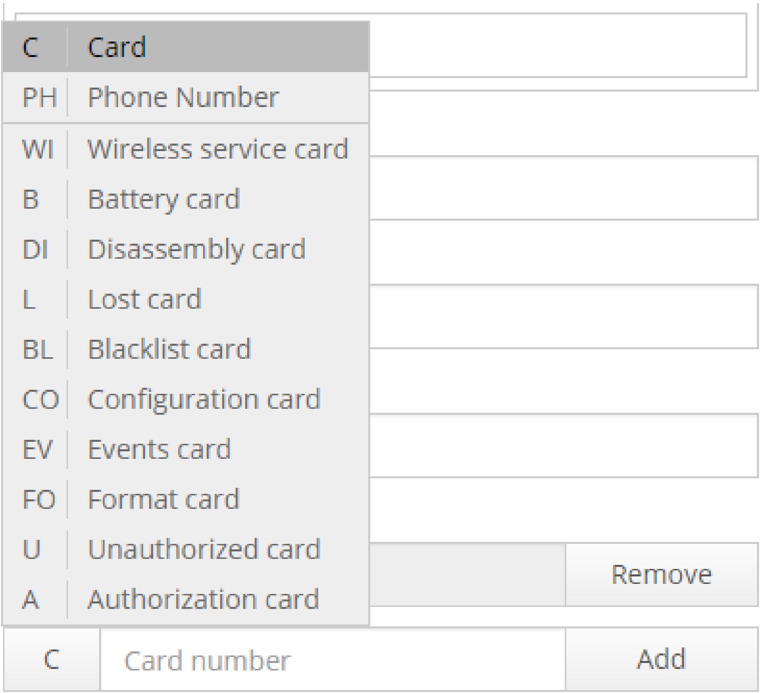
Some identification devices will automatically add a default icon next to the ID, to easy distinguish different identification devices. This way if ID is added via phone gateway, telephone handle will be added next to it; if license plate is read by LPR camera, a car icon will be appended.
Icons can be manually assigned by selecting the field between ID number and the trash button.
If icon is selected, we can also select the color of the icon. This way we can easily distinguish which card/tag has been lost for ex.
DESFire® cards or tags purchased from us will automatically report color as they are added to the Nova (Picture 4.4).



Identification devices

C	12345	●	🗑
C	320915421922122	●	🗑
PH	38651678789	☎	🗑
PH		☎	🗑
C			🗑

Picture 4.4: Colored icons next to identification devices



C	Card
PH	Phone Number
WI	Wireless service card
B	Battery card
DI	Disassembly card
L	Lost card
BL	Blacklist card
CO	Configuration card
EV	Events card
FO	Format card
U	Unauthorized card
A	Authorization card

Picture 4.5: Changing the card's function

4.2.3 Use of unprotected cards (804-00x-1005/1006/1007)

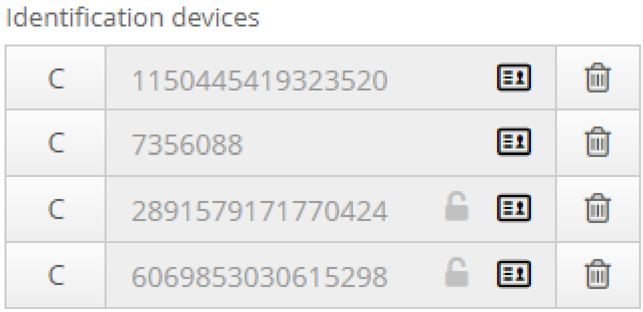
If the customers wish to use their own cards, they can do so, but they need to purchase the license for the number of cards they wish to use.

If there are only online readers in the system, no writing to the cards is required, and the system will work without any issues.
If they also wish to use them with the access to the offline readers, they need to provide the installer with the card key, so the Nova can unlock it and write the requested offline access data on the card(s).

IMPORTANT! Showing the protected card for the first time to the online reader will only read its ID and will still mark it as unprotected, showing it once more will update its status and its shape and its color.

Card numbers imported from Excel or csv file will always be set as unprotected first and then they will update its status once presented to the online reader.

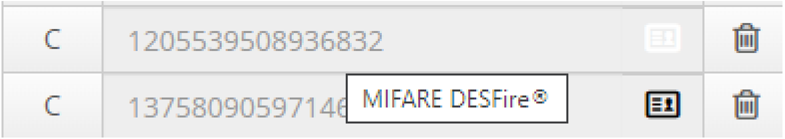
Unprotected cards issued by the third party will have the unlocked lock displayed next to them.


Identification devices

C	1150445419323520	
C	7356088	
C	2891579171770424 🔓	
C	6069853030615298 🔓	

4.2.4 Removing MIFARE Classic® cards from users

When switching from MIFARE Classic® cards (**<u>unsafe</u>**) to MIFARE DESFire® cards, you can see for each user what type of card it is by hoovering a mouse over the card number.


C	1205539508936832	
C	13758090597146 MIFARE DESFire®	

With checking the cards, you can manually remove the unwanted ones.
But if you wish to check who else has the unsafe cards and remove them from multiple people, you can:

1. Go to **Users**,
2. Press the **filter button** and select **Identification type: MIFARE Classic®** Only users that still have these cards in possession will show up.
3. **Select the users** that you wish to remove the MIFARE Classic® cards from.
4. Click Menu > Remove MIFARE Classic® cards.

4.2.5 Managing users, their access rights, and apartments

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

Edit user:

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

- Edit personal, contact and identification information
- Assign the **validity of the user and their identification devices** (set date from and to); When a user's time expires, they will not get access anymore and the event will report **Access suspended**.
- Assign a specific PIN or generate a random one.

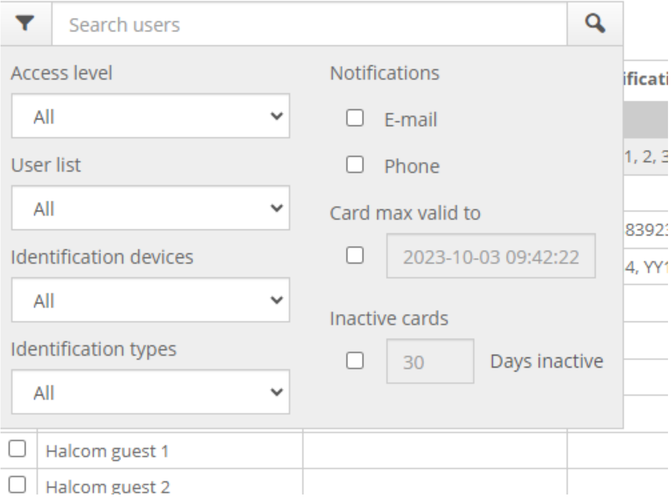
- Add/Remove access groups
- Change picture: by clicking the Change picture button on the right side of the window (Picture 4-5)
- Grab from camera – grabs a picture from a camera connected to PC
- Delete user picture

NOTE: These options are present every time someone is editing an existing user or after creating a new user.
NOTE: Administrator or **System Administrator** can edit all user data**.** Users can edit some of the data themselves: Read which and how users can edit their data in caption.

4.2.6 User list filters

When we have user list open, we can set different filters to only get the specific users from the list.

You can activate the filter by pressing the ▼ button before the search field.
This will open a dropdown where we can select multiple options, confirm the choices by pressing on the 🔍 button.



Search users

Access level: All

User list: All

Identification devices: All

Identification types: All

Notifications
☐ E-mail
☐ Phone

Card max valid to
☐ 2023-10-03 09:42:22

Inactive cards
☐ 30 Days inactive

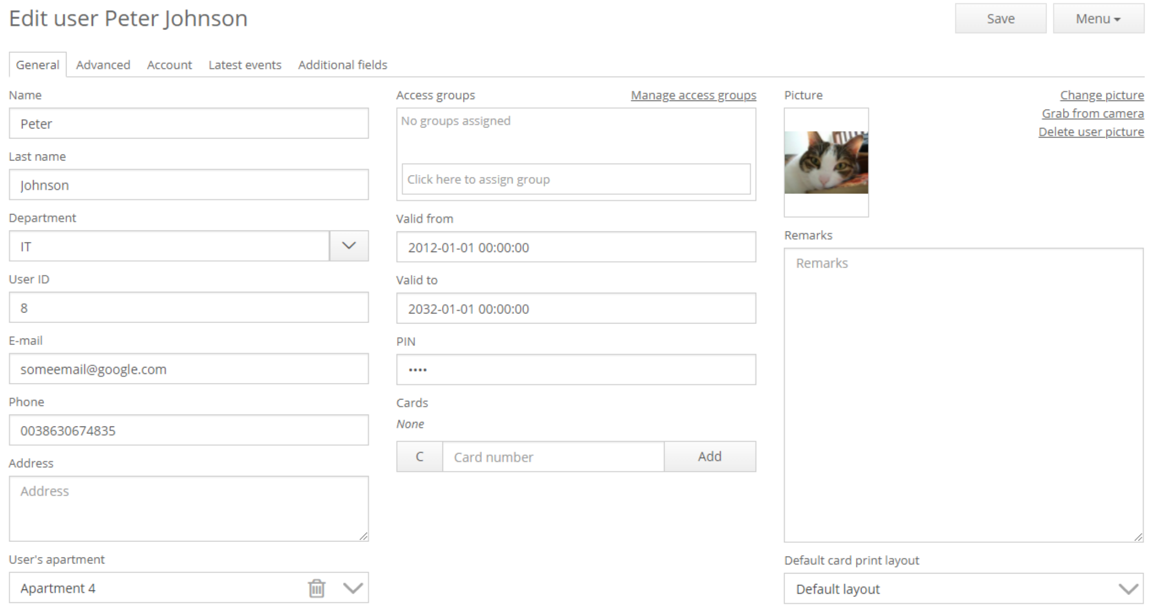
☐ Halcom guest 1
☐ Halcom guest 2

Picture 4.6: User list can be filtered out to only show the specific criteria

Access level: This enables to only display users with specific access level; Admins, Users, No access to Nova, Visitor managers…
User list: Only displays users from specific list.
Identification devices: Will only show users that have cards set as "Lost card" (at least 1), Unauthorized cards (at least 1) etc.
Identification types: Will filter the search only for specific Identification type – Selecting MIFARE DESFire® will only show users that have this card type assigned, searching for a number will now filter only over those cards in the system. The same goes for the MIFARE Classic® cards, DoorApp, License plates – you can now search by license plate text.
Email notifications: Only include users that have set to receive email notifications.

Phone notifications: Only include users that have set to receive phone notifications.
Card max validity: Set a date and only users that have validity set to specified date will be shown.
Inactive cards: Only shows the users that have at least one card that was not used for set number of days.

2.1 Account settings



Edit user Peter Johnson

Name: Peter

Last name: Johnson

Department: IT

User ID: 8

E-mail: someemail@google.com

Phone: 0038630674835

Address: Address

User's apartment: Apartment 4

Access groups: No groups assigned

Click here to assign group

Valid from: 2012-01-01 00:00:00

Valid to: 2032-01-01 00:00:00

PIN: ••••

Cards: *None*

C | Card number | Add

Picture

Remarks: Remarks

Default card print layout: Default layout

Picture 4.7: User settings

Assigning Access groups:

Assigning the Access group to a **single user** is done in the settings window for the user (Picture 4.7):

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

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

Click the **Menu > Edit user's** button.

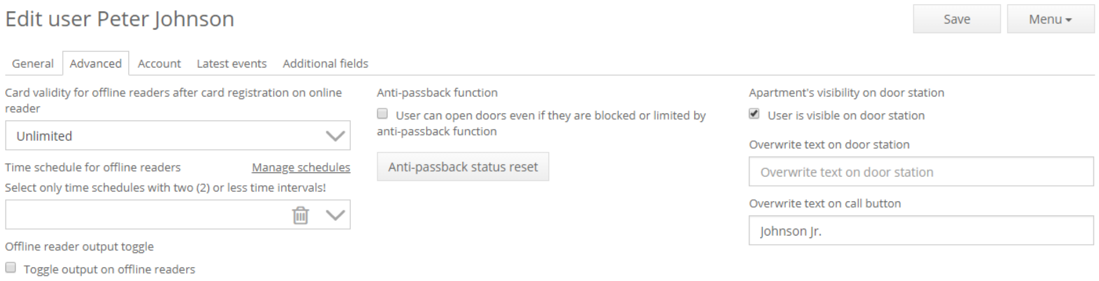
- The left column includes all Unassigned access groups.
- The middle column includes Assigned access groups for selected users.
  - Access groups can be Assigned or removed by selecting the Access group and pressing the corresponding button on the middle (Add or Remove).
- **The right column** displays the readers accessible to the currently selected access group.
- **Offline readers tab –** all settings are applied to selected users
  - Define the validity of data written on cards for offline readers

    - Define if assigned user cards should be able to activate/deactivate the toggle mode on offline readers (Constantly unlocked/ activated so it works like a thumb turn on the inside of a door or a regular mechanical handle). This option is only displayed if the Offline+ activation key is applied in the system.
    - Specify the schedule to limit the usage of a user's card to follow defined intervals on offline readers.
      NOTE: Offline readers only support 2-time intervals, so only the first two defined intervals in the selected schedule will apply. The option of checking time intervals on user cards needs to be enabled on the offline reader (see Picture 4-6). This option is only displayed if the Offline+ activation key is applied in the system.

Tab **Advanced** (Picture 4-6):

- Define the validity of data written on cards for offline readers
- Specify the schedule to limit the usage of a user's card to follow defined intervals on offline readers.
  NOTE: Offline readers only support 2-time intervals, so only the first two defined intervals in the selected schedule will apply. The option of checking time intervals on user cards needs to be enabled on the offline reader (see Picture 4-6). This option is only displayed if the Offline+ activation key is applied in the system.
- Define if assigned user cards should be able to activate/deactivate the toggle mode on the 2nd read on offline readers (Constantly unlocked/ activated so it works like a thumb turn on the inside of a door or a regular mechanical handle). This option is only displayed if the Offline+ activation key is applied in the system.
- **Privileged access** checkbox – users who have this checkmark set, will ignore any software limitations like blocked doors, anti-pass back, interlock errors or booked doors.
- **Anti-pass back** function – the option to remove anti-pass back limitations from this user. Pressing the Anti-pass back status to reset will open a window and ask the Administrator to reset anti-pass back status for current or All users in the system.

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



Edit user Peter Johnson

Card validity for offline readers after card registration on online reader: Unlimited

Time schedule for offline readers

Select only time schedules with two (2) or less time intervals!

Offline reader output toggle

□ Toggle output on offline readers

Anti-passback function

□ User can open doors even if they are blocked or limited by anti-passback function

Apartment's visibility on door station

☑ User is visible on door station

Overwrite text on door station: Overwrite text on door station

Overwrite text on call button: Johnson Jr.

Picture 4.8: User's advanced settings

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

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

To see a user's history/event log:

1. Select a user from the user list (Picture 4-3).
2. Click Menu > Edit user button.
3. Navigate to tab **Last events**.

Additional fields tab:

Sometimes customers wish to store some more information about a user, that is not pre-determined by Nova2.0. In such cases, they can create their fields with custom labels and variable entries.
The additional fields work great with card manager, to read more about it, please navigate to chapter **15.3 Additional user fields.**

Removing a user:

1. Select the user from the user list (Picture 4-3).
2. Click on **Menu > Remove the user** in the main menu.
   NOTE: The user will be deleted, but the card will remain in the system, for the administrator to see if someone is trying to gain access using a deleted card.
3. Follow steps from chapter 4.2.1 to re-use the card for a new user.
   This will make the card work normally and report all events as a new card.

Assigning apartments:

If there is a Module: Door stations or Module: Mailboxes applied in the system, the Apartment widget becomes visible.
Make sure that apartments are created before they are assigned (reference - 8.3 Managing apartments).
To assign the apartment:

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

4.2.7 Tokens

Tokens are virtual currency that we can add or remove from user(s) when they pass a specific door(s). Once the tokens are exhausted, the access is rejected.
Note: Tokens are **not counted for admin/sysadmin** level.

Creating a **new token**:

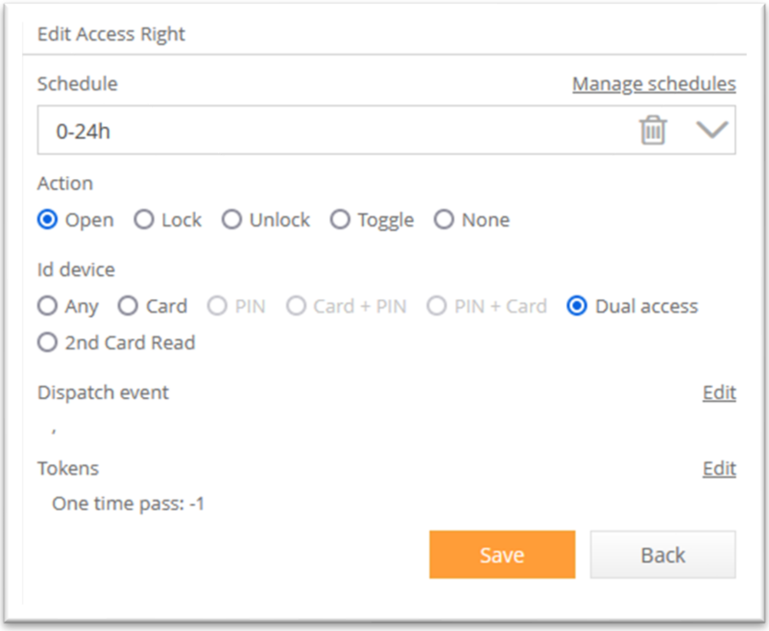
1. Navigate to user list and open a random user. Press **Menu** button > Tokens, a pop-up will appear.
2. Click on the **Menu** button on pop-up > Add new token.
3. Provide a suitable name and select the initial token value which will assign All users the initial value. Any newly created user will also be assigned the initial value of tokens.

Managing the amount of user’s tokens:

1. Once at least 1 token type is created, a new tab Tokens will show up for each user.
2. Open a specific user, navigate to Tokens tab, all token types will be shown along with the current user’s amount.
    a. **Add** will increase the user’s amount by the specified value.
    b. **Set** will change the amount to the provided value.
    c. **Remove** will decrease the user’s amount by specified value.

Defining token consumption:
It is recommended to create a new/special access groups for this because in most cases, regular users will not use tokens for normal access.

1. Create a new access group.
2. When assigning access right to the reader specify token usage (one or multiple types of token and negative/positive number of tokens that will be used/added).
3. Assign the access group to user(s) that should have limited number of accesses.



Edit Access Right

Schedule Manage schedules

0-24h

Action

● Open ○ Lock ○ Unlock ○ Toggle ○ None

Id device

○ Any ○ Card ○ PIN ○ Card + PIN ○ PIN + Card ● Dual access

○ 2nd Card Read

Dispatch event Edit

,

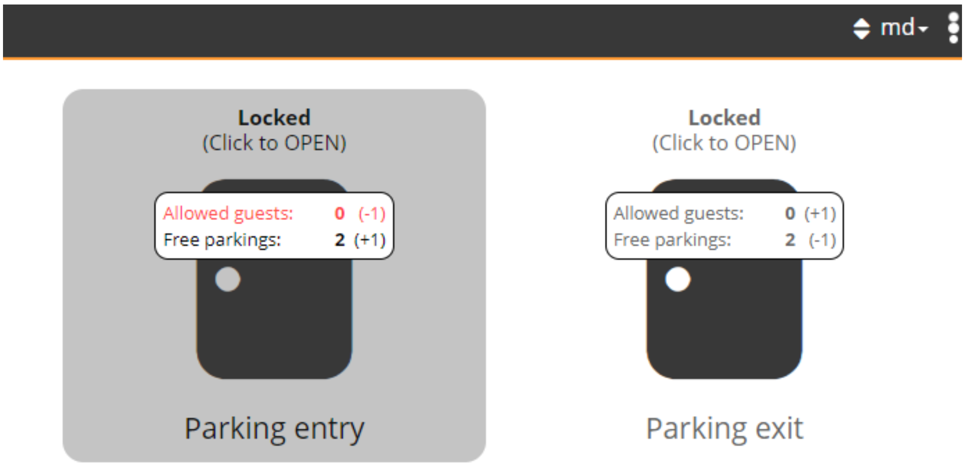
Tokens Edit

One time pass: -1

Save Back

Picture 4.9: Assigning token consumption to the reader's access right

When a user has assigned tokens for specific doors and they create/are assigned a widget, Nova will display their amount and entry consumption (tokens can be added too not just used).



md▾

Locked
(Click to OPEN)

Allowed guests: 0 (-1)
Free parkings: 2 (+1)

Parking entry

Locked
(Click to OPEN)

Allowed guests: 0 (+1)
Free parkings: 2 (-1)

Parking exit

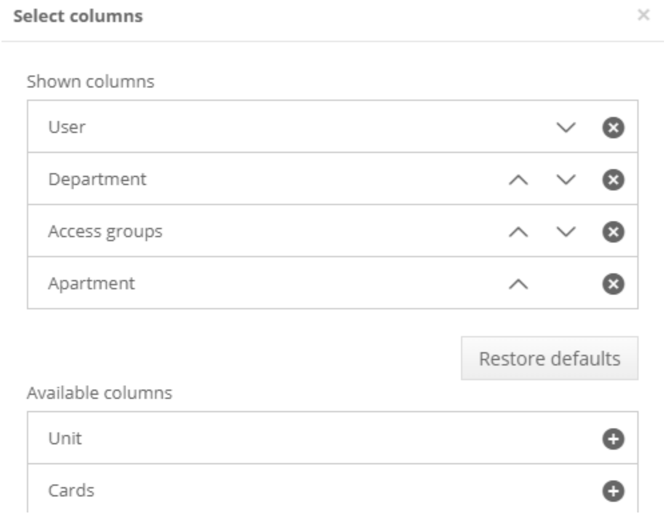
Picture 4.10: Multiple tokens visualization on user's widgets

4.2.8 Displaying custom columns

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

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

The **restore to defaults** button will set the preview to the original state.



Picture 4.11: We can select custom columns and create a unique view

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

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

4.2.9 Importing users from CSV or Excel file

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

1. Click the **Menu > Import from file** button in the main user menu
2. Open the file that includes users from the opened popup window.

NOTE: The CSV type file needs to have the data for each user in separate lines separated either by comma (,), semicolon (;) or TAB separator.

3. The data from the import file will be parsed and presented in a grid (Picture 4-8). If any changes need to be resolved, data can be rewritten in the grid.

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

- Unused
- Last name
- Name
- Department
- Access group
- Card

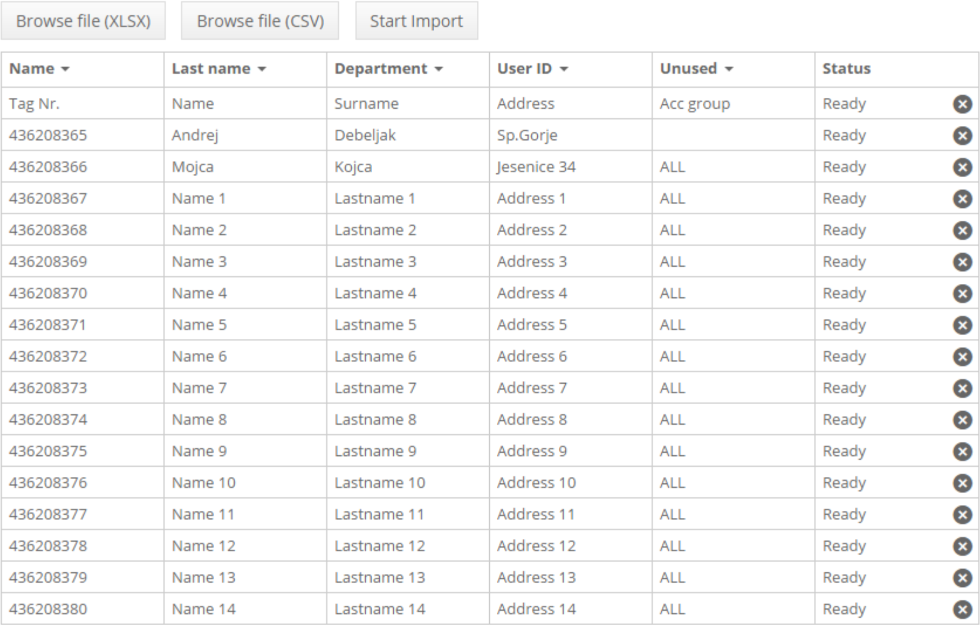
- PIN
- User ID

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

ATTENTION: Values in the column matched as *Access group* must match valid Access group names, which are already present in the system. Furthermore, the values in the column matched as *Card* or *PIN* details must be valid numbers. If the access groups do not exist yet, they will be created.

NOTE: Each user needs to have a unique PIN.

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



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

Picture 4.12: Import users from CSV or Excel file

4.2.10 Custom user search

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

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

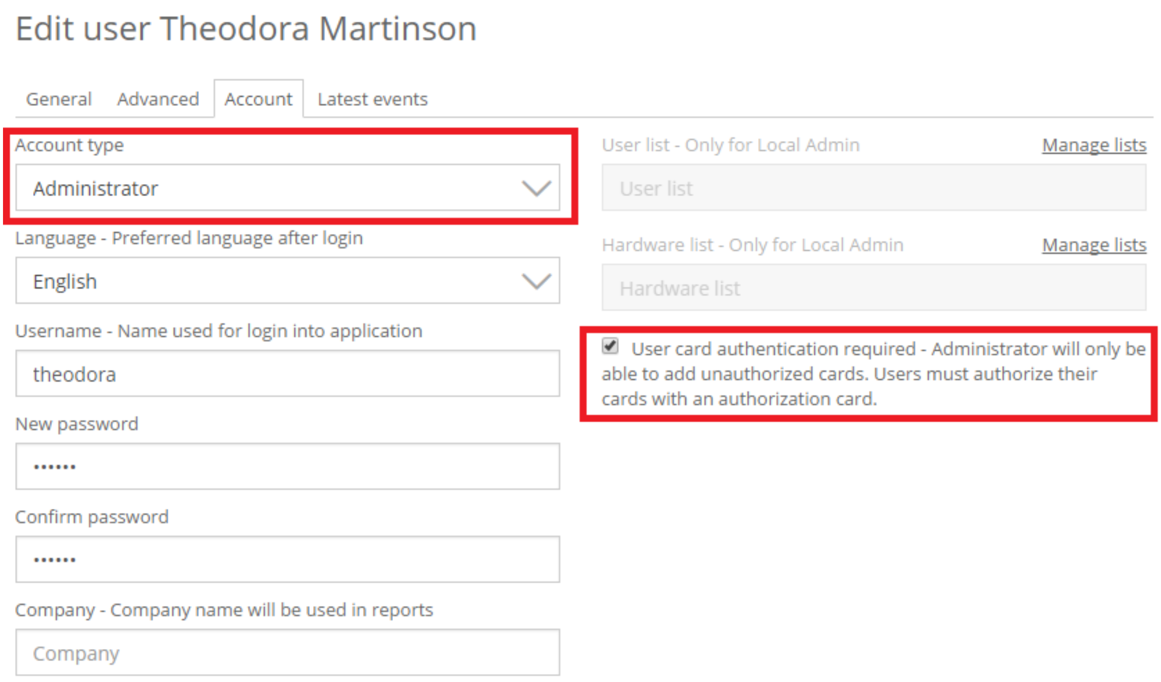
NOTE: NovaServer is a lot more powerful thus allowing the search to be run on all active columns.

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

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

4.2.11 Card authorization

Some installations require cards to be authenticated before they start working. To get such system working, the system administrator needs to assign an administrator, provide him with username, password, and a checkmark next to the user authentication text shown in Picture 4-9**.**



Edit user Theodora Martinson

General | Advanced | Account | Latest events

Account type: Administrator

Language - Preferred language after login: English

Username - Name used for login into application: theodora

New password: ••••••

Confirm password: ••••••

Company - Company name will be used in reports: Company

User list - Only for Local Admin: User list

Hardware list - Only for Local Admin: Hardware list

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

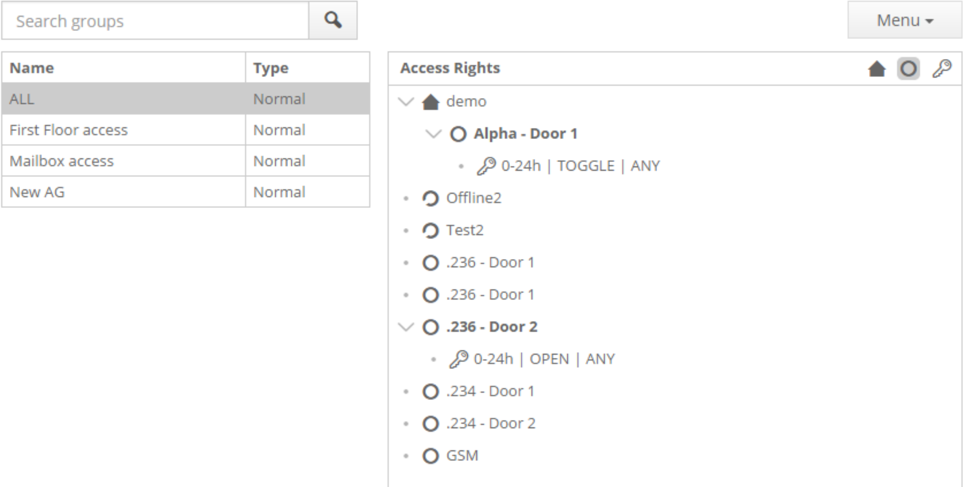
Picture 4.13: An assigning administrator whose cards will be added as unauthorized

The system administrator can then assign authorization cards to users.
When the Administrator logs into the nova, he/she can assign new cards to users, but are automatically set as **Unauthorized card** and will not work even if the user rights are correctly assigned.
The card will start working once the correct **Authorization card** is put on the reader; there will be a beeping sound, prompting for the correct user card. If the user card is put on the reader in the beeping period, it changes its status from **Unauthorized card** to **Card** and begins to work as a standard card.

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

4.3 Access groups

Clicking the button **Access groups** in the navigation menu will display the page below (Picture 4-10)



Name	Type
ALL	Normal
First Floor access	Normal
Mailbox access	Normal
New AG	Normal

```
Access Rights
demo
    Alpha - Door 1
        0-24h | TOGGLE | ANY
    Offline2
    Test2
    .236 - Door 1
    .236 - Door 1
    .236 - Door 2
        0-24h | OPEN | ANY
    .234 - Door 1
    .234 - Door 2
    GSM
```

Picture 4.14: Access groups editor

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

It is possible to:

- Enter the new group name in the **Name** input box
- Enter group description or other info in the **Description** field optionally (Picture 4-11).
- Save the new Access group by clicking the **Add** button.

To edit an existing group:

- Select the group
- Click button **Menu > Edit** [group name] (Picture 4-11)

To remove an access group from the list:

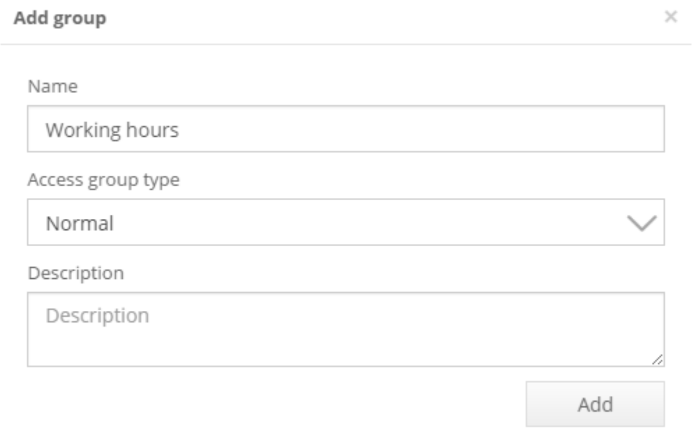
- Select the group
- Click the **Menu > Remove** [group name] button

NOTE: Access groups assigned to users cannot be deleted.

NOTE: If there are to be multiple similar access groups, one can copy an entire group by selecting the original group and clicking **Menu > Copy** and then adjust according to the needed changes.

Booking module

In case the activation key for booking module is installed, the type of access group can be changed from **Normal**, which is used in Nova for defining access rights for users, to type **booking**, which is used in the booking application. **Booking** access groups are shown as different types in *Access group* editor. For more information about the booking module please see chapter 13.



Add group

Name: Working hours

Access group type: Normal

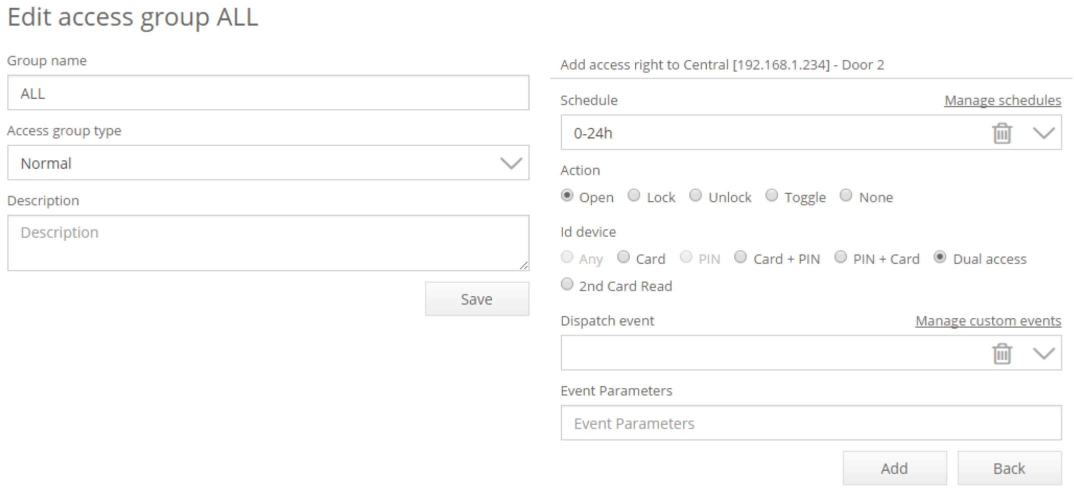
Description: Description

Picture 4.15: New group editor

Access group editor

Access rights for selected access group in Access group editor (Picture 4-10) are visible in the hardware tree next to the list of groups. Buttons at the top of the tree can adjust the current tree view and select which branches of the tree are displayed.

New access rights can be added to the selected group by clicking on the +button, which is visible when an item from the hardware tree is selected (Picture 4-10). This will switch the hardware tree view into access properties for the previously selected hardware.



Edit access group ALL

Group name: ALL

Access group type: Normal

Description: Description

Add access right to Central [192.168.1.234] - Door 2

Schedule: 0-24h

Action: ● Open ○ Lock ○ Unlock ○ Toggle ○ None

Id device: ○ Any ○ Card ○ PIN ○ Card + PIN ○ PIN + Card ● Dual access ○ 2nd Card Read

Dispatch event:

Event Parameters: Event Parameters

Picture 4.16: Schedule, action, and ID device selection

Select a schedule, action, and identification device

Here it is possible to:

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

Id devices available:

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

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

NOTE: Existing access rights can be edited or removed with the use of appropriate buttons shown on the selected tree item. The visibility of buttons for a 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* is selected (to add a new schedule, please read chapter **4.4 Managing time schedules**) and it follows the actions **OPEN** and **CARD** as a source for executing an action. Those access rights cannot be edited. This does not apply for the Nexus MKO which also supports PIN+card.

4.4 Managing schedules

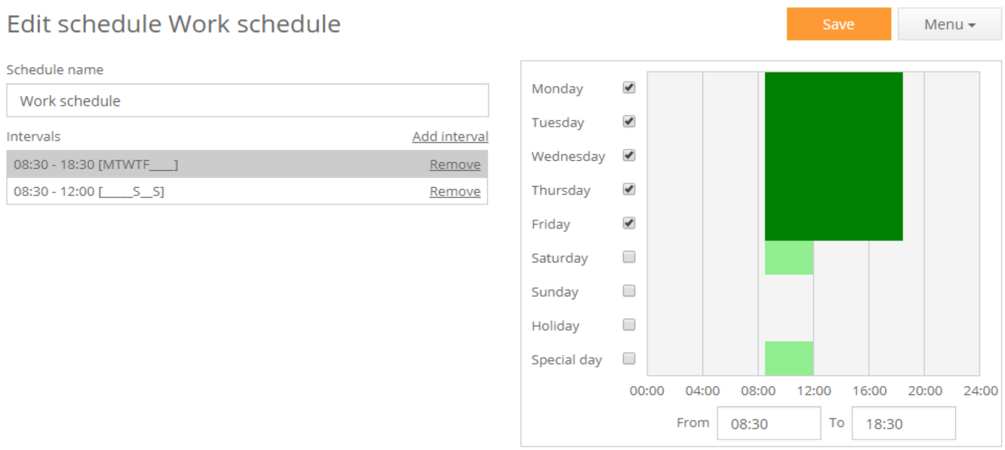
The NovaSimpli software includes one, predefined schedule (0-24h), which is valid from 00:00 until 23:59 for every day of the week and cannot be modified or deleted. In other versions of Nova software, the option to manage and create additional time schedules is added. It can be accessed by clicking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

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

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

NOTE: Each schedule contains one- or multiple-time interval(s), where each of them has a defined time span and days when the interval is valid (Picture 4-13).

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


Edit schedule Work schedule

Schedule name: Work schedule

Intervals

08:30 - 18:30 [MTWTF____] Remove

08:30 - 12:00 [_____S__S] Remove

Monday ☑
Tuesday ☑
Wednesday ☑
Thursday ☑
Friday ☑
Saturday ☐
Sunday ☐
Holiday ☐
Special day ☐

From 08:30 To 18:30

Picture 4.17: Time intervals

If there is a holiday (for **any** day of the week), the **holiday schedule is used instead**!

Special days have higher priority than holidays and standard weekdays (if they are set on the same day).

Exception day can be added by navigating to **Menu > Add exception day,** select the date range, and apply to the new schedule that will work on a set range of days. Only one-time range can be set, but multiple exception days can be added to cover the required time slot.
Exception day has the highest priority over Holidays, special days, and standard schedules.

IMPORTANT! Holidays and Special days are dependent on the country set on the central and affect all the readers in the system, while the **exception day** applies only to readers who have the schedule with exception day assigned.

Validity – country dependent

Time intervals can be defined on normal/ordinary days, special days, or holidays, but please note that:
Special days and **Holidays** are predefined in the calendar and are country dependent. To access the calendar options, select the **Menu > Calendar** button from the **Time schedules** editor.
For each entry in the calendar:

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

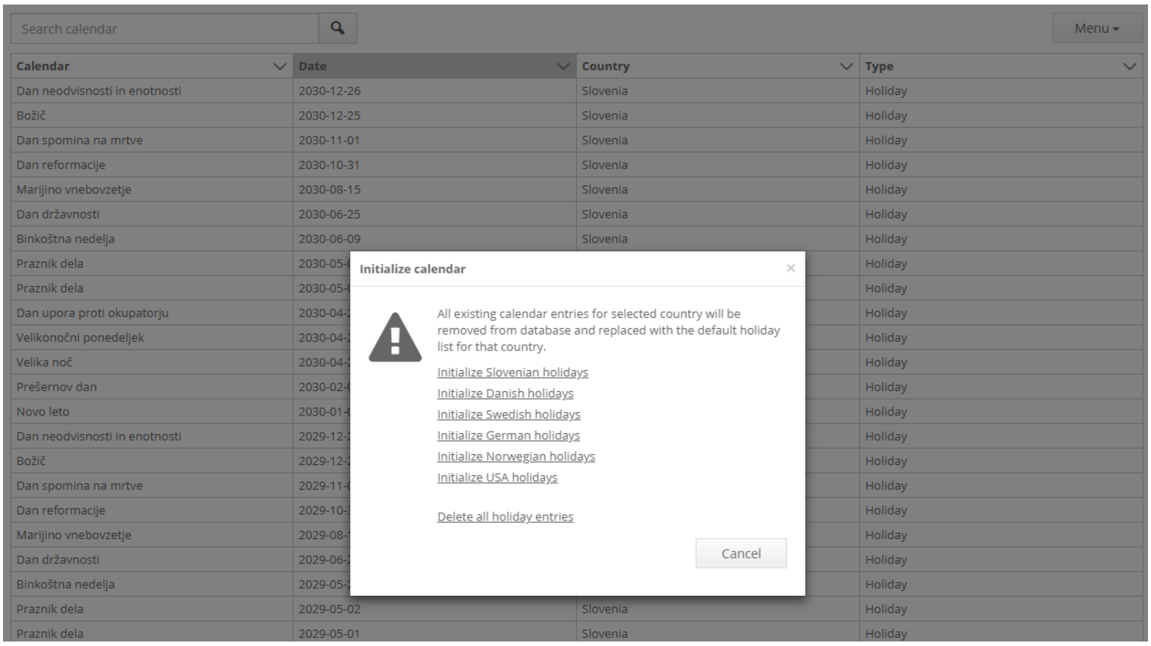
To automatically import Holidays for a country:

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

- Click the button **Menu > Initialize calendar** in the calendar editor.

NOTE: All existing calendar entries for the selected country will be deleted from the database and replaced with the default list of holidays for the selected country. If any holidays are set wrong or missing, they can still be manually added/edited after the import is completed.

- To delete all holidays from the system, choose the last option from the menu.



Initialize calendar

All existing calendar entries for selected country will be removed from database and replaced with the default holiday list for that country.

Initialize Slovenian holidays
Initialize Danish holidays
Initialize Swedish holidays
Initialize German holidays
Initialize Norwegian holidays
Initialize USA holidays

Delete all holiday entries

Calendar	Date	Country	Type
Dan neodvisnosti in enotnosti	2030-12-26	Slovenia	Holiday
Božič	2030-12-25	Slovenia	Holiday
Dan spomina na mrtve	2030-11-01	Slovenia	Holiday
Dan reformacije	2030-10-31	Slovenia	Holiday
Marijino vnebovzetje	2030-08-15	Slovenia	Holiday
Dan državnosti	2030-06-25	Slovenia	Holiday
Binkoštna nedelja	2030-06-09	Slovenia	Holiday
Praznik dela	2030-05-		Holiday
Praznik dela	2030-05-		Holiday
Dan upora proti okupatorju	2030-04-		Holiday
Velikonočni ponedeljek	2030-04-		Holiday
Velika noč	2030-04-		Holiday
Prešernov dan	2030-02-		Holiday
Novo leto	2030-01-		Holiday
Dan neodvisnosti in enotnosti	2029-12-		Holiday
Božič	2029-12-		Holiday
Dan spomina na mrtve	2029-11-		Holiday
Dan reformacije	2029-10-		Holiday
Marijino vnebovzetje	2029-08-		Holiday
Dan državnosti	2029-06-		Holiday
Binkoštna nedelja	2029-05-		Holiday
Praznik dela	2029-05-02	Slovenia	Holiday
Praznik dela	2029-05-01	Slovenia	Holiday

Picture 4.18: Initialize calendar with the default holiday list

NOTE: Multiple Holidays/Special days can be selected holding the Ctrl or Shift key on the keyboard.

Automatic schedules changes - examples:

- Time interval from 22:00 to 6:00, unlocks at 22:00, locks at 6:00, even if the time interval on the next day is not valid; for example, it is Saturday, holiday or even exception day, it will always lock it. Lock time is defined at the start of the time interval when doors are unlocked.
- If an automatic unlock schedule is added or removed to output, the user is asked if output should be locked or unlocked.
- If an automatic unlock schedule is modified and currently not valid anymore, the output is locked.
- If an automatic unlock schedule is modified, for example at 23:00 time interval is modified to 22:00-5:00, the output will be locked at 5:00. Lock time is redefined at 23:00 when the interval is modified.

The Time interval from 8:00 to 16:00 unlocks at 8:00, locks at 16:00.

- If manually locked at 15:00, it will stay locked. If back manually unlocked at 15:10, it will be locked at 16:00.
- If unlocked at 8:00 and the controller is powered off at 9:00, when powered back on, outputs are always put in the same state as before the reboot. If power comes back at 10:00 it will be unlocked, if it was unlocked before powering off, manually or with an automatic schedule. If power comes back at 17:00, the output will be locked and stay locked.
- If the controller is powered off at 7:00 (output was locked) and powered on back at 10:00, the output will be at the same state as at 7:00, locked. The schedule will unlock it since unlock was missed because of power down.

5. Hardware

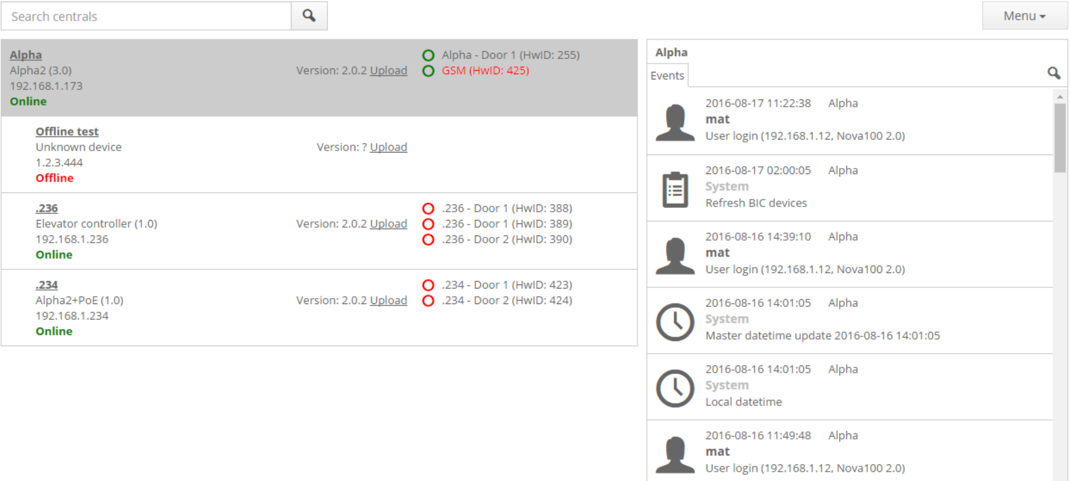
5.1 Centrals

The Central editor is used for previewing and managing hardware.

To open it, navigate to **Home > Hardware > Centrals** (Picture 5-1)
Options in Menu:

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

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



Alpha
Alpha2 (3.0)
192.168.1.173
Online
Version: 2.0.2 Upload
○ Alpha - Door 1 (HwID: 255)
○ GSM (HwID: 425)

Offline test
Unknown device
1.2.3.444
Offline
Version: ? Upload

.236
Elevator controller (1.0)
192.168.1.236
Online
Version: 2.0.2 Upload
○ .236 - Door 1 (HwID: 388)
○ .236 - Door 1 (HwID: 389)
○ .236 - Door 2 (HwID: 390)

.234
Alpha2+PoE (1.0)
192.168.1.234
Online
Version: 2.0.2 Upload
○ .234 - Door 1 (HwID: 423)
○ .234 - Door 2 (HwID: 424)

Alpha

2016-08-17 11:22:38 Alpha
mat
User login (192.168.1.12, Nova100 2.0)

2016-08-17 02:00:05 Alpha
System
Refresh BIC devices

2016-08-16 14:39:10 Alpha
mat
User login (192.168.1.12, Nova100 2.0)

2016-08-16 14:01:05 Alpha
System
Master datetime update 2016-08-16 14:01:05

2016-08-16 14:01:05 Alpha
System
Local datetime

2016-08-16 11:49:48 Alpha
mat
User login (192.168.1.12, Nova100 2.0)

Picture 5.1: Central editor

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

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

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

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

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

- Add a new central

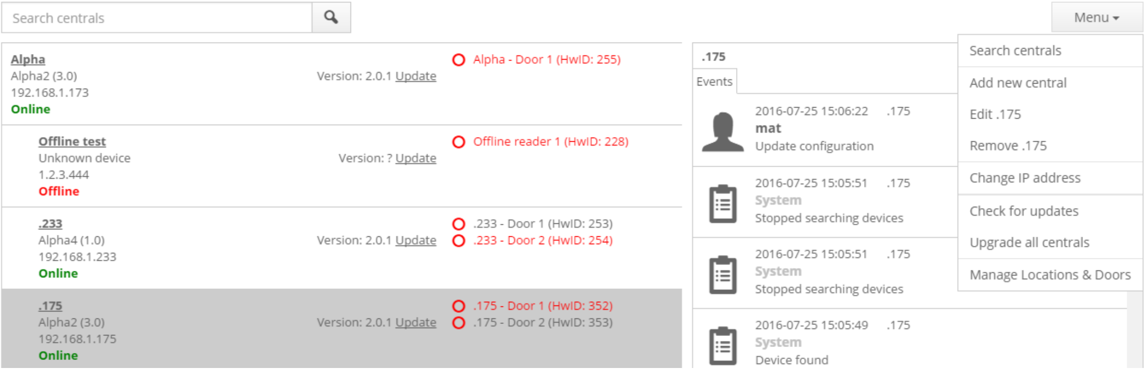
- Add the central to the system
- Replace existing slave central

NOTE! Double-clicking the central that is not in the system will bring up the *Add central* pop-up for a faster addition.
IMPORTANT! If a central in the system is RS-485 master, when searching the centrals, a pop-up will show up asking if the RS-485 master should run a search on RS-485 bus too. Keep in mind that the search for the mentioned bus is very slow. The centrals found on LAN will display orderly under the central that found them with their MAC and IP address next to them. Centrals on RS-485 bus will display under the RS-485 master central and only their RS-485 address will be displayed.

5.1.2 Changing a central's IP address

Change the IP address of a central by:

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



Alpha
Alpha2 (3.0)
192.168.1.173
Online
Version: 2.0.1 Update
○ Alpha - Door 1 (HwID: 255)

Offline test
Unknown device
1.2.3.444
Offline
Version: ? Update
○ Offline reader 1 (HwID: 228)

.233
Alpha4 (1.0)
192.168.1.233
Online
Version: 2.0.1 Update
○ .233 - Door 1 (HwID: 253)
○ .233 - Door 2 (HwID: 254)

.175
Alpha2 (3.0)
192.168.1.175
Online
Version: 2.0.1 Update
○ .175 - Door 1 (HwID: 352)
○ .175 - Door 2 (HwID: 353)

2016-07-25 15:06:22 .175
mat
Update configuration

2016-07-25 15:05:51 .175
System
Stopped searching devices

2016-07-25 15:05:51 .175
System
Stopped searching devices

2016-07-25 15:05:49 .175
System
Device found

Picture 5.2: Changing the IP address of a central

IMPORTANT! The following must be entered to change the static IP:

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

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

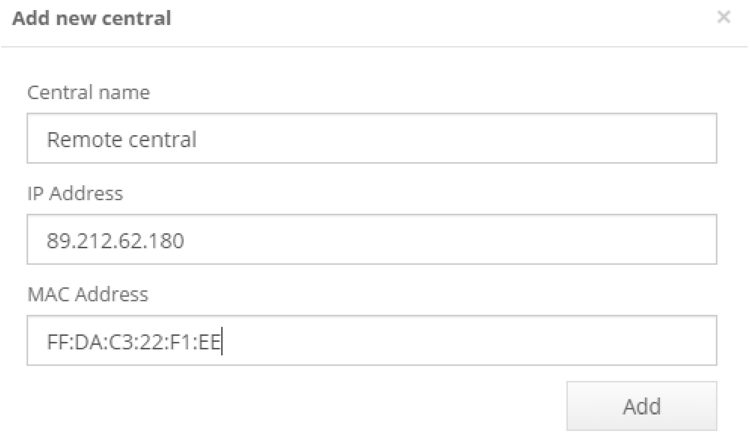
DHCP is also an option, it will request all the network data from the DHCP server and automatically apply them to the central.
Since the central's default connection type is to connect via IP, when applying DHCP settings, the type will automatically change to connect using automatic IP (MAC address). When this option is enabled, if the IP of the slave central changes, the master will trigger a network search and when the central is found, it will reconnect to the new IP and also update the database.

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

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

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

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


Add new central

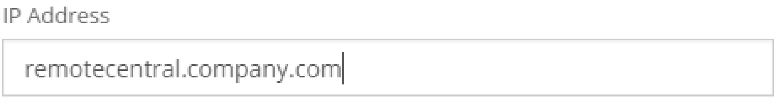
Central name: Remote central

IP Address: 89.212.62.180

MAC Address: FF:DA:C3:22:F1:EE

Picture 5.3: Adding a remote central

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


IP Address: remotecentral.company.com

Picture 5.4: Using DNS or DDNS instead of IP

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

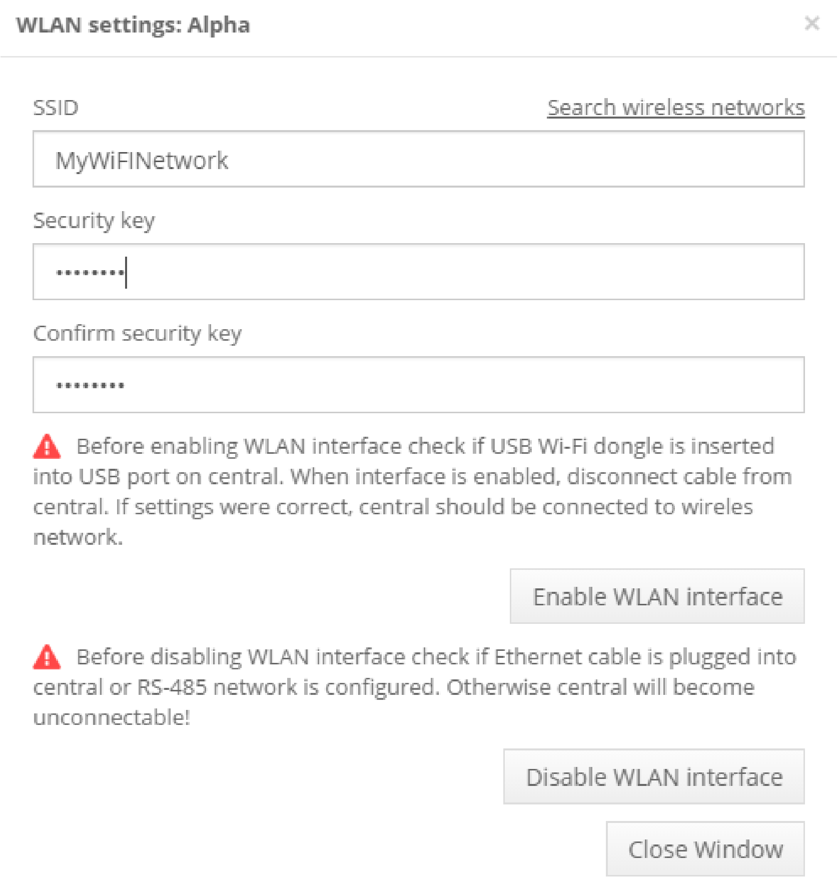
5.1.4 Central's WLAN settings

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

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

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

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



WLAN settings: Alpha

SSID: MyWiFINetwork

Security key: ••••••••

Confirm security key: ••••••••

⚠ Before enabling WLAN interface check if USB Wi-Fi dongle is inserted into USB port on central. When interface is enabled, disconnect cable from central. If settings were correct, central should be connected to wireles network.

⚠ Before disabling WLAN interface check if Ethernet cable is plugged into central or RS-485 network is configured. Otherwise central will become unconnectable!

Picture 5.5: WLAN settings

IMPORTANT! The wireless interface can only be enabled on the central that the administrator is currently logged in to. Also, the wireless interface of a slave cannot be enabled from the master central. Also note that during the installation of the wireless interface, the USB dongle and the network cable must both be connected to the central. After the wireless interface is enabled (confirmation dialog notice), the network cable can be unplugged. Nova is then accessible the same way as it was 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 (most likely a mistake in the SSID or the security key input). Plug the network cable into the central, wait for Nova to reconnect to the central and then try again.

Search for available wireless networks:

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

Disabling the wireless interface:

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

5.1.5 Adding, removing, and editing centrals

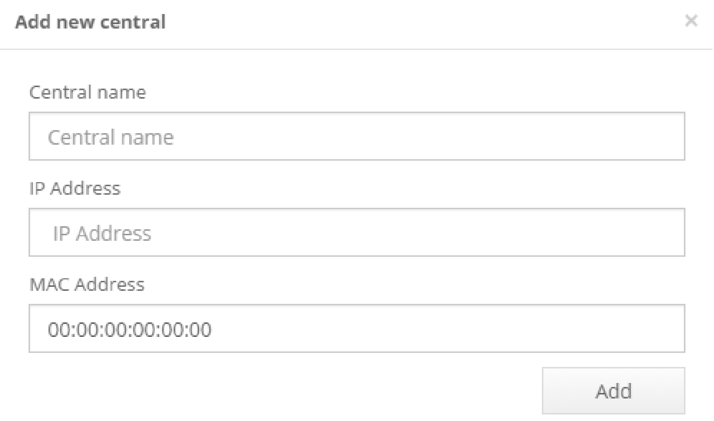
Adding new centrals automatically:

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

Adding new centrals manually:

1. Click **Menu > Add central** in the Central editor
2. Enter the name of the central, IP and MAC address in the popup window (Picture 5-6)
3. Save changes

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



Picture 5.6: Popup window for adding a new central

Remove centrals:

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

Edit centrals:

1. Select the central from the Central editor
2. Click **Menu > Edit [central name]** button or double click the central from the Central editor list.
3. A settings window for the central will be displayed (Picture 5-9).

Multiple tabs will show:

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

Settings tab: Consists of 3 columns:

- General and Network settings on the left – consist of the name of the central, country (Set the country for each central – suitable when covering multiple countries with different holidays, etc.), IP, netmask, DNS, and gateway addresses, along with the MAC address. From here, also select (by checking the checkmark) if the central is on a remote location. If the checkmark is marked, a new field will be added to fill the correct remote IP address.
- WLAN settings are only displayed for the central currently logged into if the central is the correct type to support Wi-Fi connections.
- Anti-Passback function settings – read more about the Anti-Passback function in chapter **11.3 Setting up global Anti** .

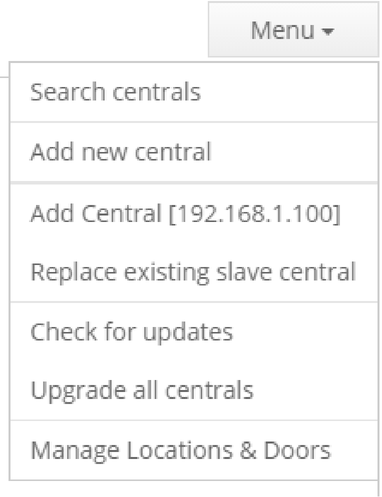
IMPORTANT! Advanced settings for the central are not available in the NovaSimpli software.

5.1.6 Replacement of malfunctioning slave central

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

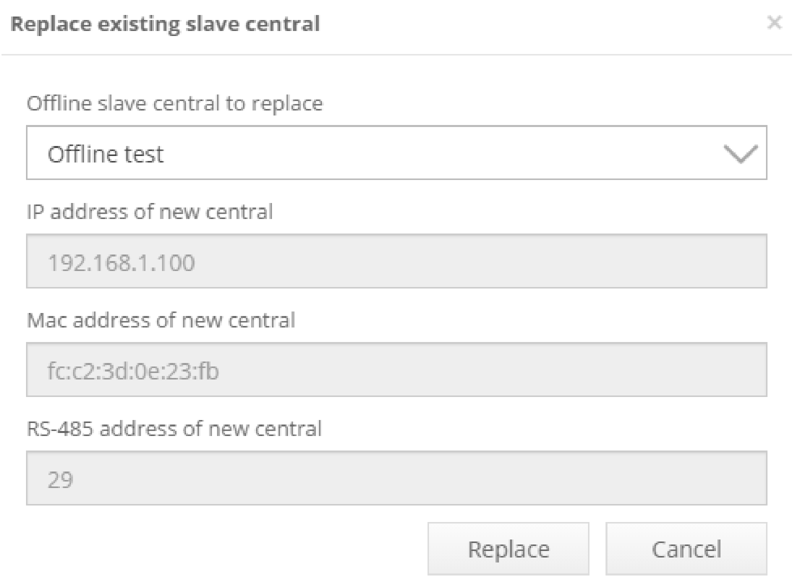
To keep all its data and just replace the malfunctioning central, the function **Replace slave central** can be used (Picture 5-7).
To get to manage centrals window on the main menu navigate to:

1. Home > Hardware > Centrals.
2. Search for new centrals by clicking **Menu > Search centrals**
3. Select the new central and find the options **Menu > Replace existing slave central**. This option is only available for the ones on a default IP address (192.168.1.100).
    - A new popup (Picture 5-8) will appear requesting a selection of the slave central that needs to be replaced while showing the information of the newly added central.
4. Press the **Replace existing slave central** button to start the procedure
    - The newly added central will get the data from the master of the system and adjust the time.



Picture 5.7: Replacing an existing slave central

NOTE: Synchronization can take up to a couple of minutes. After completion, the new central should appear online on **Picture 5-1 Central editor** and the IP address of the old central.



Replace existing slave central

Offline slave central to replace: Offline test

IP address of new central: 192.168.1.100

Mac address of new central: fc:c2:3d:0e:23:fb

RS-485 address of new central: 29

Picture 5.8: Replace existing central pop-up

5.1.7 Replacement of malfunctioning master central

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

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

- the new master central must already be installed in the system
- central must not have any slaves connected to it
- its master must be the malfunctioned central (current master)
    - A **Promote** button will appear in the Central’s advanced settings (Picture 5-9) if the slave central meets the requirements.

For a slave to become a new top master, navigate to slave’s IP, log into slave central, and follow these steps:

1. Home > Hardware > Centrals.
2. Double click the central that you wish to promote (the one you are currently logged into).
3. Navigate to the **Advanced settings** tab
4. Press the **Promote** button.
    - The system will reassign all the slave centrals including the malfunctioned master to the newly set master.

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

NOTE: When slave central gets promoted or master central replaced, if there are any **modules in the system will need to be re-activated**; contact the installer to help you through the process.

5.1.8 Central settings

Settings

- **Central name**: Used for easier central recognition.
- **Country**: Centrals that have the country set will obey any calendar entries set in the calendar settings.
- **MAC address**: Physical address of the central. It can be also found on the sticker on the side of the central. If the centrals are not properly named, this is the only way to distinguish central between each other.
- **Remarks**: A custom field where you can write notes about the central.

Connections

Options on top Master central:

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

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

Options on Slave central:

- **Select master central**: Each central must have a master assigned to receive any changes.
- **Connect using**:
  - **IP address** – standard static ethernet connection with the fixed IPs. More about the connection can be read in the chapter 5.1.10 Communication-based on IP address.
  - **Automatic IP (MAC address)** – this option is here for slave centrals that connect over DHCP settings. The master tries to connect via saved IP and if the central does not respond it triggers central discovery and if found, the IP data is updated accordingly.
  - **Remote central hostname or IP address** – a new field for entering the remote central hostname or IP is displayed below this option. Recommended for remote (over the internet) connections.
    Port 3543 - This port allows communication of the central to pass through. If the central needs to be connected over the internet, this port must be opened on the slave central (the master is the only one that issues commands so only one-way communication is needed). If there is a whole system located on the other side of the internet, it is enough forwarding only the local master port.

RECOMMENDATION: The default port is 3543 and should stay this way if possible. Changing different ports on the outside can be made from the port forwarding settings of the router. Please check the manual of the router on the subject before making any changes.

  - **RS-485** – connects centrals via an RS-485 connection. More about it can be read in the chapter 5.1.11 Communication-based on RS-485 BUS.
  - **NovaConnect** – The option for central to be connect over cloud server.

- **Connection type**: Here we can select how the master communicates with the slave central. By default, centrals come with **Secure, if possible,** option which will try to establish a secure connection and revert to Plain communication if the slave central is not capable. The **high security module** allows forcing the communication to always be established over secure channels.
- **Central will receive all events**: This option is here to disable event copying from the whole system to this central. If disabled, central will only receive the events only for itself and its slaves (if any). Centrals that have this option enabled will perform faster. Additionally, the event log will be reduced from 1 million events to 250 thousand to preserve disk space.
- **Allow system administration**: Allows changes to be made on a slave central. Usually, everything is done from the master central and if any changes are made on the slave central, they are overwritten with data from the master. Enabling this option allows Administrators to manage users on that central without losing any changes. This can be helpful if the Administrator is in a different network and do not have direct access to the master central (or the connection between the master and that central is not stable).
- **Set as RS-485 master central:** Assigns the central to be the master of the RS-485 bus. This should be set on the central that is connected to the Ethernet and the RS-485 bus at the same time.

Local option:

- **Wi-Fi settings** (displayed only if connected directly to the central and if the central has a USB port)

Auxiliary I/O

These options are related to the General Input 1, 2 and Relay 5, 6 on Alpha+ centrals. By default, General Input 1 is pre-programmed to be wired to tamper switch which is triggered if someone opened the electrical box. The tamper events can be turned off. General Input 2 is pre-programmed to work with Fire alarm module. Alarm events can be turned off if they are not used.
For centrals with additional relays, their open time, voltage level and automatic opening schedule can be set.

Advanced actions

- **Database synchronization:** Just in case something is wrong with the database of one of the slave centrals, press the Force synchronization button to copy the configuration database from master to slave. After pressing this button, go to the events page of the central and monitor the progress. After database synchronization, time will be updated as well (more in chapter **5.1.12**).
- **Central reboot:** Pressing this button will send the reboot command to the currently selected central (if online).
- **Reader and lock power reset:** By pressing this button the power to the lock and the reader will be cut – helpful for a remote reader or lock reset.
- **Upgrade firmware on central:** Selecting the Update button will open a File window, requesting to locate the upgrade software package.
- **Optimize database**: Pressing this button will run a database indexer that might speed up the system, but it takes from a few seconds up to a few minutes.
- **Database cleanup**: Manual trigger of the database cleanup. For more info, please check **6.3 Database Settings**.
- **Ping test**: The option to test the network access, also DNS resolution.
- **Delete user pictures, scripts, and uploaded files**
- **Reset central to default** – This will replace the current database with a default one (the same as holding the left button on the Alpha for 20 seconds).
- **Storage mode** (set locally on central)**:** Alpha2+ and Alpha4+ have a USB connector that supports storage expansion. When uploading larger files, such as pictures for the floorplans, pdfs for info boards, any documents, profile pictures, and database backups are all saved on the external USB storage if present.
- **ADC voltage read** (Superadmin only, set locally on central, old central only)**:** In a few cases on the old Alpha hardware, reading current voltage got stuck and resulted in a central periodical reboot. Removing this checkmark will cause central not to be stuck anymore and should work ok, but any power events will not be shown anymore.

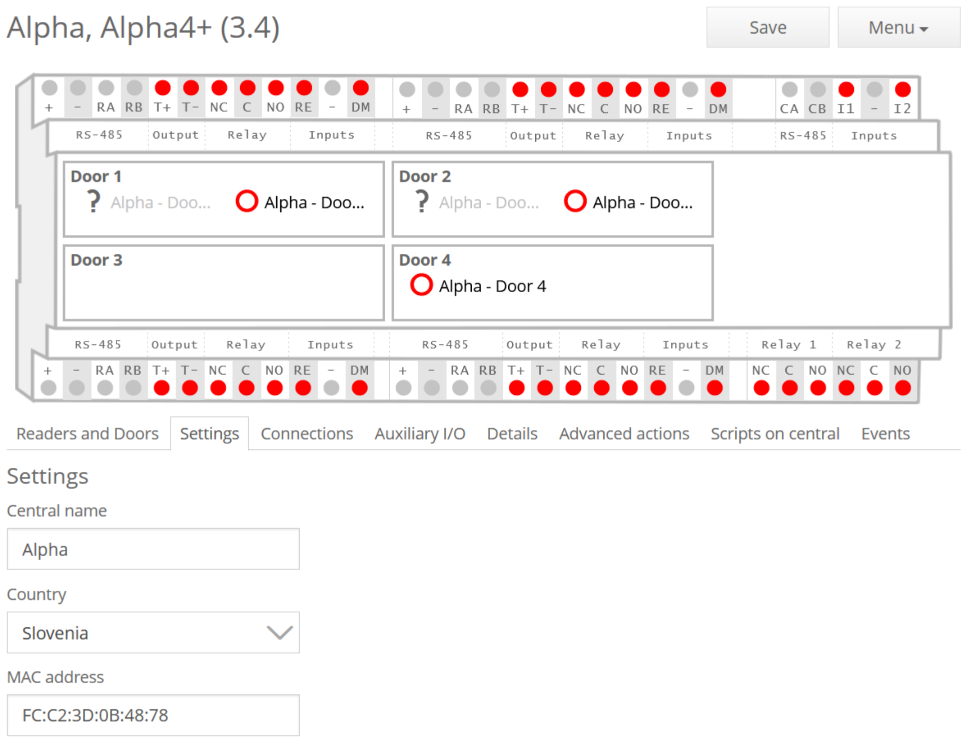
IMPORTANT! When inserting the USB, you need to tell the software to write to the USB storage by clicking on the button Switch to the USB storage button. **Before removing USB from the central make sure that the mode was switched back to central**; otherwise, some data might get lost!

Scripts on central

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

Events

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


Save
Menu
+ - RA RB T+ T- NC C NO RE - DM + - RA RB T+ T- NC C NO RE - DM CA CB I1 - I2
RS-485 Output Relay Inputs RS-485 Output Relay Inputs RS-485 Inputs
Door 1
Alpha - Doo...
Alpha - Doo...
Door 2
Alpha - Doo...
Alpha - Doo...
Door 3
Door 4
Alpha - Door 4
RS-485 Output Relay Inputs RS-485 Output Relay Inputs Relay 1 Relay 2
+ - RA RB T+ T- NC C NO RE - DM + - RA RB T+ T- NC C NO RE - DM NC C NO NC C NO
Readers and Doors
Settings
Connections
Auxiliary I/O
Details
Advanced actions
Scripts on central
Events

Alpha, Alpha4+ (3.4)

Settings

Central name

Alpha

Country

Slovenia

MAC address

FC:C2:3D:0B:48:78

Picture 5.9: Central settings

5.1.9 Online System-wide software upgrade and single upgrade

There are multiple ways to upload software to the central, the first two are a single central upgrade, while the last option upgrades the whole system.
NOTE: Centrals connected via the RS-485 bus need to be upgraded locally!

Local upgrade:

1. If the central is connected on RS-485, plug in the Ethernet cable (the central and the computer you are accessing from must be in the same network).
2. Navigate to central's IP address.
3. Log-in and navigate to the central's settings (Picture 5-9)
4. Navigate to the Advanced settings tab.
5. Click the **Upgrade** button.
6. Select the .tar package and wait for the process to finish.

Remote upload – **IMPORTANT!** Remote upload only works with central's software version 1.6 and higher and the central must be **online**:

1. Navigate to **Home > Hardware > Centrals** widget.
2. Find the remote central on the list and double click it (or select and Menu > Edit).
3. Navigate to the Advanced settings tab.
4. Select the **Upgrade** button.
5. You will be prompted to locate the upgrade file.

6. If the central is not master central, the transfer protocol will begin to transfer the upgrade package to the remote central. Once it is completed, the upgrade will start automatically; if the central is the one logged into, it will begin a local upgrade.

NOTE: If there is a local master between the remote central and top master, the package will be first uploaded to top master, then transferred to local master and then to the final slave central.

System-wide upgrade:

1. Navigate to **Home > Hardware > Centrals** widget.
2. Press **Menu > Upgrade** option from the dropdown menu**.**
3. Check all centrals you want to upgrade. (Offline centrals and centrals connected on RS-485 bus will be excluded)
4. Once ready, press the **Upgrade** button.
5. You will be prompted to select **the latest released package** (if the top master has access to the internet) or you can select to **Upload it from the** computer (for systems without internet access).
   a. For the online option, press the **Select** button next to the Package.
   b. The offline option will ask you to provide the packages from your PC.
6. The pop-up will ask if you also want to upgrade the readers to the latest software.
7. Wait until everything is finished and **do not close the window as this will terminate the upgrade process**.

After the upgrade is done, **Central was upgraded** event will be displayed in the Events log. If the upgrade was done locally, you will need to log-in again.
If there are some issues during upgrade or centrals that are connected on RS-485 bus (connect to the central with a network cable), navigate to their IP address and upgrade the central locally – following the 1st upgrade description

5.1.10 IP based communication

The communication between master and slave central is based on the IP address, set in the field *IP address* in the **Central editor – Connections tab** (Picture 5-9), and on the IP port written next to the IP separated by a colon ":".

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

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

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

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

5.1.11 Communication over RS-485 BUS

When a slave central is connected to the master central via an RS-485 BUS, option **RS-485 master central** must be enabled, located in the **Connections** tab of the RS-485 master central (Picture 5-9) by:

- Checking the **Set as RS-485 master** central checkbox.
  - This setting causes the master central to search and communicate with the slave centrals on the RS-485 BUS.
- Checking the **Set as RS-485 slave central** checkbox in the advanced settings will set the current central as an RS-485 slave (all RS-485 slave centrals must be set after the RS-485 master is set).

- Central search should now prompt the question to search for the centrals connected on RS-485 BUS. Select **Yes** and wait until the search is done. RS-485 centrals will display on the list showing only their Modbus address instead of their IP addresses.

NOTE: The communication between centrals on the RS-485 BUS is based on the RS-485 address, which is set in the field RS-485 address under the Connections tab settings of the central.
The default RS-485 address of the master central is always 1 and is automatically set when the central is set as RS-485 master. The default address of a slave central is set when adding the slave central to the system and it is also found in the central label.

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

Example of RS-485 address calculation:

MAC 00:50:C2:E6:30:6A
6A (hex) = 0110 1010 (bin)
0 1010 (bin, last 5 bits) = 10 (dec) + 2 = 12 (RS-485 address)

WARNING! The default address can be changed to any other unused address on the RS-485 BUS. Resetting the address back to its default address can be done by calculating it like in the example above or hold the left button on the central shown on Picture 26-2 for at least 10 seconds, which will:

- Reset the IP address and RS-485 address back to the default values:
  => 192.168.1.100 for IP address
  =>default value for RS-485 address and port to 80
- It also enables the **Super administrator account** again, if it was disabled.

See Appendix A - Description of LEDs and buttons on central for more details.

5.1.12 Database synchronization

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

- Clicking the button **Force synchronization** in the advanced settings of the slave
  - The master central updates the database on the slave central with the version from the master central.

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

5.1.13 Adding new readers

To add new readers to the central:

- Click the **Menu > Search readers** button in the upper right corner of the **Central Editor** (Picture 5-9)
  - This triggers the recognition of already connected readers and starts a search for readers recently connected to the central.

Change address, remove or add readers:

NOTE: Reader search **works ONLY from address 1 to 16 (max)**. Addresses from 16 to 64 are user-defined addresses and will not be displayed as a search result of a reader search. To avoid complications, keep the reader addresses within limits.
After the search is completed, the addresses of listed readers can be changed and the new readers can be added to the central:

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

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

5.1.14 Upgrading firmware on reader

Single reader upgrade:

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

- Double click on the reader you want to upgrade and navigate to the **Upgrade firmware** tab.
    1. Select the **Upgrade firmware** button. Select the *.bin extension file with the new firmware in the popup window
    2. The upgrade process will start, and it will last for approximately 30 ~ 120 seconds (depending on the workload of the central).
    3. During the upgrade process, an operation status dialog will be displayed
    4. The reader will beep three times after completing the upgrade process.

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

Upgrade ALL readers on a central:

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

5.1.15 Reader settings

The reader needs to be configured correctly and linked to the desired door for the system to function correctly.
When the reader is selected (Picture 5-10), the following info on the reader is shown:

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

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

- Deselecting the **Enable** checkbox

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

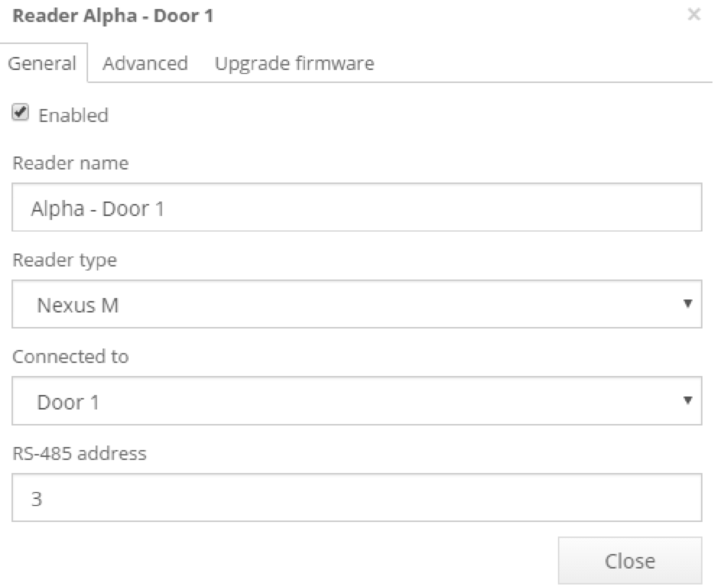
IMPORTANT! Disabled readers are shown in light grey in the locations tree while non-working readers are shown in red.

Set up of door that the reader is connected to:

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

NOTE: Usually the reader is connected to the same door that it controls, but a reader can control another door on the same central.
To do this, please check Picture 5-11: Advanced settings.).
This option is not included in NovaSimpli.

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



Reader Alpha - Door 1

☑ Enabled

Reader name: Alpha - Door 1

Reader type: Nexus M

Connected to: Door 1

RS-485 address: 3

Picture 5.10: Reader settings

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

Reader settings on Picture 5-10 show the settings needed for basic operation.

Change additional parameters by:

- Selecting the **Advanced** tab (Picture 5-10) – the options are:
  - Select which door the reader controls (additional relays on Alpha+ included)
  - Set direction for each reader (Entry, Exit, Pass-through, I1 entry – I2 exit)
  - Set sensitivity on the tamper sensor

Further options:

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

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

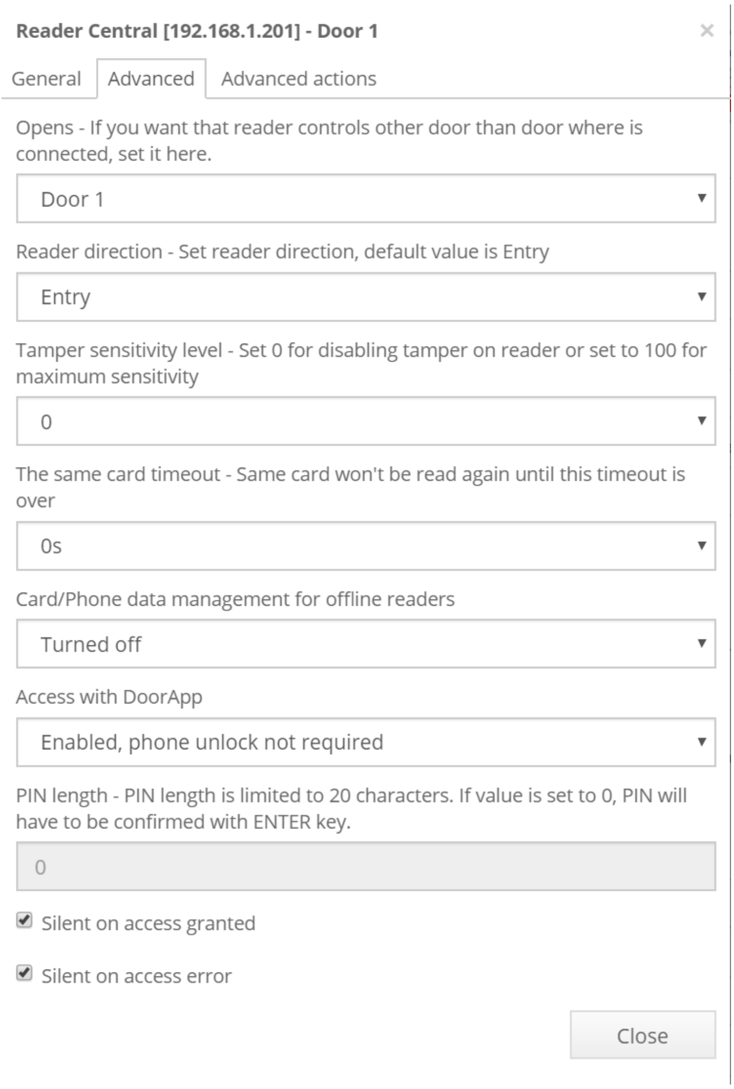
- **Enabling the writing of offline access rights to user cards** (only possible if the reader supports writing to cards). Offline readers read these access rights from the card. (See section 5.2 Offline readers for more information)
- Setting value in the **PIN length** field
    - This defines how users enter their PIN on the current reader
        - If the value is greater than 0, then PIN is accepted as soon as the last number is pressed on the keyboard.

Remember: When PIN length is defined, PINs of all users have to match the defined length.

- If a value is set to 0, users will have to confirm their PIN with the ENTER key on the keyboard.

- **Mailbox reader** checkmark – If this checkmark is set, the reader is assigned to open mailboxes instead of doors (including checking the rights).

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



Reader Central [192.168.1.201] - Door 1

Opens - If you want that reader controls other door than door where is connected, set it here.

Door 1

Reader direction - Set reader direction, default value is Entry

Entry

Tamper sensitivity level - Set 0 for disabling tamper on reader or set to 100 for maximum sensitivity

0

The same card timeout - Same card won't be read again until this timeout is over

0s

Card/Phone data management for offline readers

Turned off

Access with DoorApp

Enabled, phone unlock not required

PIN length - PIN length is limited to 20 characters. If value is set to 0, PIN will have to be confirmed with ENTER key.

0

☑ Silent on access granted

☑ Silent on access error

Picture 5.11: Advanced settings of readers

Reader sounds

Nova version 2.1 also brings the option to remove any sound from the Nexus readers. Different options are displayed in the reader's advanced settings - Picture 5-11.

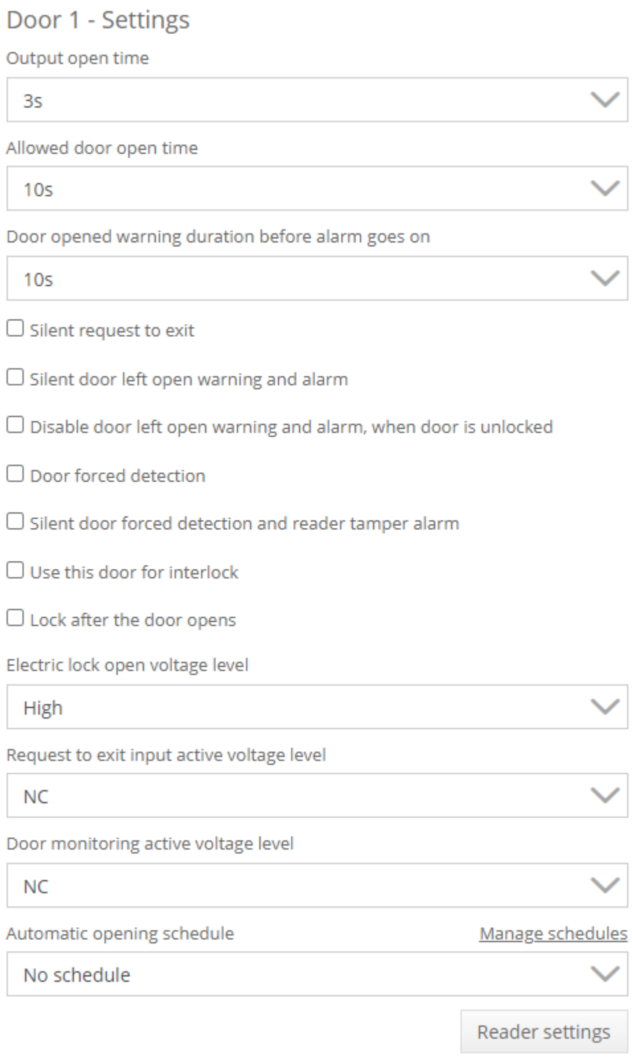
- **Silent on access granted** – removes any beeps when the access is granted.
- **Silent on access error –** reader stays silent whenever there is an error – reading/writing a card.

Additionally, there is an option to **remove sound from REX** input. This can be done by checking the corresponding option on the door settings (option displayed on Picture 5-12).

5.1.16 Door settings

Picture 5-12 shows the settings for doors on the central, which gives the following options:

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



Door 1 - Settings

Output open time: 3s

Allowed door open time: 10s

Door opened warning duration before alarm goes on: 10s

☐ Silent request to exit

☐ Silent door left open warning and alarm

☐ Disable door left open warning and alarm, when door is unlocked

☐ Door forced detection

☐ Silent door forced detection and reader tamper alarm

☐ Use this door for interlock

☐ Lock after the door opens

Electric lock open voltage level: High

Request to exit input active voltage level: NC

Door monitoring active voltage level: NC

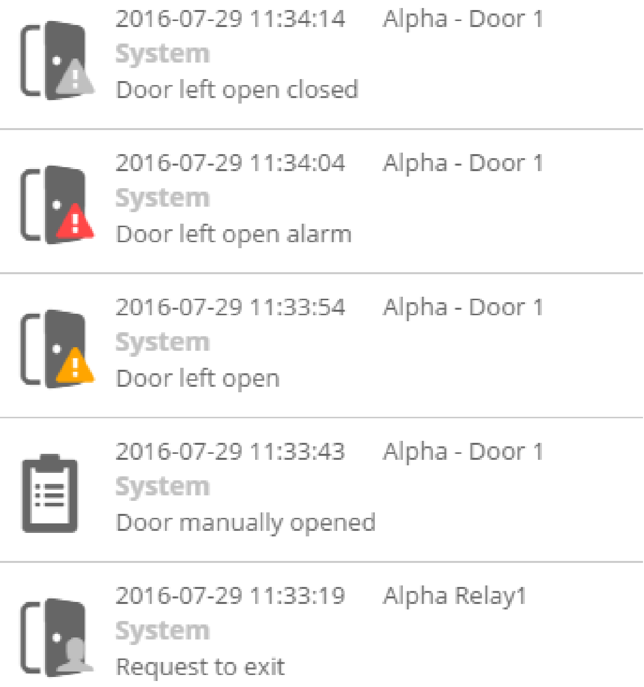
Automatic opening schedule: No schedule

Picture 5.12: Door settings

Picture 5-13 is an example that shows the relation between the described times.

- The door was opened at 11:33:43 and stayed open.
- Four seconds later the reader started to warn the user with a beeping sound that the door should be closed (11:33:54).
- The user did not react to the warning, so the alarm went on nine seconds later (at 11:34:04).

- The user finally closed the door at 11:34:14.
- The settings on the door were the same as Picture 5-12.



2016-07-29 11:34:14 Alpha - Door 1
System
Door left open closed

2016-07-29 11:34:04 Alpha - Door 1
System
Door left open alarm

2016-07-29 11:33:54 Alpha - Door 1
System
Door left open

2016-07-29 11:33:43 Alpha - Door 1
System
Door manually opened

2016-07-29 11:33:19 Alpha Relay1
System
Request to exit

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

Further options:

- **Silent request to exit** – reader will not make a sound when the request to exit button is pressed. This also works with multiple readers connected to the same door.
- Select **Silent warnings and alarms** to avoid the reader from making any sound at warnings or alarms. The events will still be displayed.
- **Disable warnings and alarms when the door is unlocked** – when checked, it will not display or trigger any mentioned events.
- Select **Door forced detection** when there are doors with readers on each side.
    - In this case, the central has total control over the door and can detect if the doors are not opened by readers and will trigger a "door forced" alarm.
    - The administrator can choose the **Silent door forced detection and reader tamper alarm** option if any alarm sound is too loud.
- **Use this door for interlock** – doors that are set to use interlock cannot be opened at the same time (we need to wait for other interlock doors to close before we can open a specific interlock door on the central).
  - A single interlock functionality will only work on that specific central and not on multiple centrals across the system.
  - A single interlock can be set up on each central.
  - Card or REX access will not be granted if other interlock doors are unlocked or opened or if you want to open the already opened door.

- **Privileged access users are not limited by this functionality**.
  - When access is denied, an event will be triggered.
- **Lock after the door opens** – enabling this option will only unlock the lock for a very short time, this way if the door closes early (or slams), it will stay locked.

IMPORTANT! The described settings (except Electric lock open time) can only be used with electrical locks having a DM (door monitor) signal line. If not, the central cannot detect if doors are open or not and the described settings will not work as expected.

In case of fire or power supply failure:
An electric lock usually requires a positive voltage level to be in the locked state and neutral (or low) voltage level for opened, unlocked state.
The reason is that in the case of fire or power supply failure the electrical lock switches to unlocked state and users can go through the door.
This option can be enabled by:

- Matching the option **Electric strike open voltage level** to the required voltage level for the locks used in the system.
- The options **RE input active voltage level** and **DM active voltage level** need to be set according to the system characteristics.
  - The central will open the door when the signal level on RE input (Request to Exit) matches the selected state.
    Unlock when active options will unlock the door until the **signal is terminated and then add additional lock open time**.

  - The central will know that the doors are open when the state of the DM signal matches the selected state (High or Low).

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

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

5.1.17 Scheduled door opening

In the Nova software, there is an additional option:

- A schedule can be selected from a drop-down list and assigned to target doors (Picture 5-12 – bottom option).
  - Doors will automatically be locked and unlocked based on the time intervals of the selected schedule (see part **4.4** for **Managing time schedules**).

- By clicking the **Manage Schedules** link, the **Time schedule editor** can be accessed and:

    - Edit schedules
    - Preview schedules

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

TIP: Set a defined time interval of 1 minute that runs out when doors need to be locked.

5.1.18 Management of alarm(s), tamper(s) and additional relays

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

Tamper Input

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

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

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

Alarm Input

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

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

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

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

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

The next two options require a Fire alarm module:

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

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

5.1.19 Mounting the USB storage and grabbing picture from the camera

IMPORTANT! The USB storage must be purchased from the central manufacturer otherwise we do not guarantee, nor support other USB sticks.

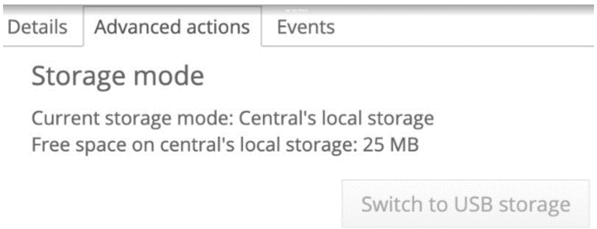
NOTE: Make sure that your top master unit has a USB slot to mount this device.

IMPORTANT! Make sure to mount and dismount the device properly to avoid losing any data.

Customers that wish to expand the storage for the user / blueprints /camera pictures can purchase an additional USB storage device that will also serve as an additional backup for your system (7 copies of the database instead of 3). When mounting the device, all the existing user files will be transferred to the USB storage. After the USB storage is unmounted/removed, user files remain on the USB and **ARE NOT transferred to the central**. Once the USB storage is remounted, the user files become available once again.

How to mount the USB storage device:

1. Plug the USB storage device into top master central.
2. In Nova, go to its Settings > Advanced actions and press button Switch to USB storage.



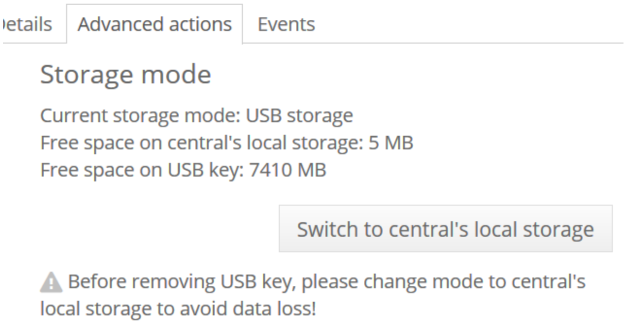
Storage mode

Current storage mode: Central's local storage
Free space on central's local storage: 25 MB

Picture 5.14: Switching storage mode from central’s internal to external USB

How to unmount it:

1. In Nova go to master’s settings > Advanced actions and press button Switch to central’s local storage.



Storage mode

Current storage mode: USB storage
Free space on central's local storage: 5 MB
Free space on USB key: 7410 MB

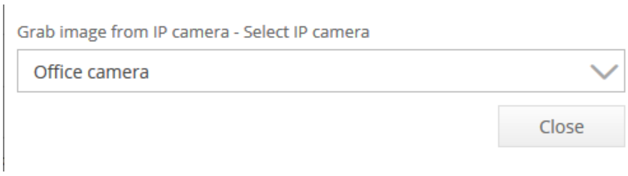
⚠ Before removing USB key, please change mode to central's local storage to avoid data loss!

Picture 5.15: Switching storage mode from USB to central's internal storage

2. Unplug the USB storage device.

Set-up grabbing pictures from local camera:

1. Make sure that the **High security module** is applied to the system.
2. Make sure that the **USB storage device** is plugged in and mounted (it must be top master central; NovaServer does not need it).
3. In the **Settings > Other settings** make sure that the **Show IP camera picture** checkbox is selected.
4. Make sure that the picture of IP camera is working. Read more about setting up IP camera in chapter 5.3.3 IP Camera.
5. Navigate to the reader that is mounted near the camera and open its advanced settings. At the bottom you will find a dropdown menu with all IP cameras listed.



Grab image from IP camera - Select IP camera

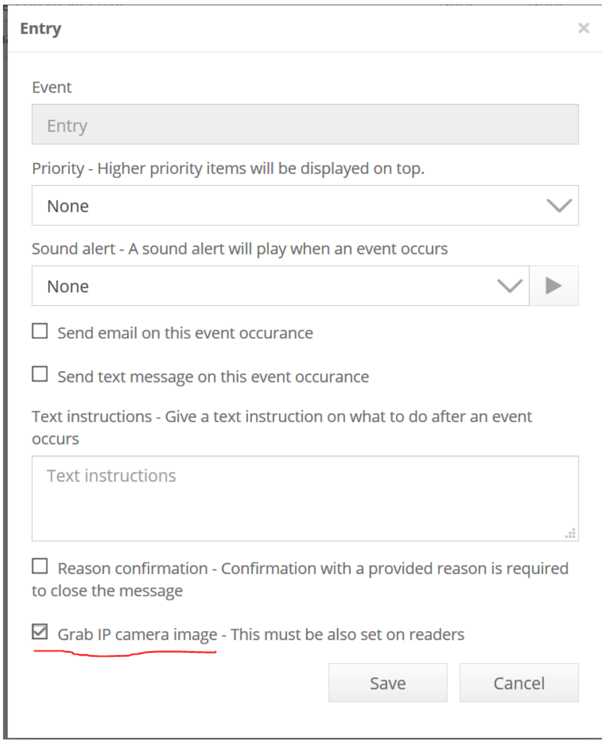
Office camera

Picture 5.16: Matching the reader with the correct IP camera.

Select the camera, close the pop-up and Save changes.

6. Navigate to **Events**, select **Menu > Manage error and warning events** and mark the events that you wish the

picture to be taken (only reader events can be captured!).



Entry

Event

Entry

Priority - Higher priority items will be displayed on top.

None

Sound alert - A sound alert will play when an event occurs

None

☐ Send email on this event occurance

☐ Send text message on this event occurance

Text instructions - Give a text instruction on what to do after an event occurs

Text instructions

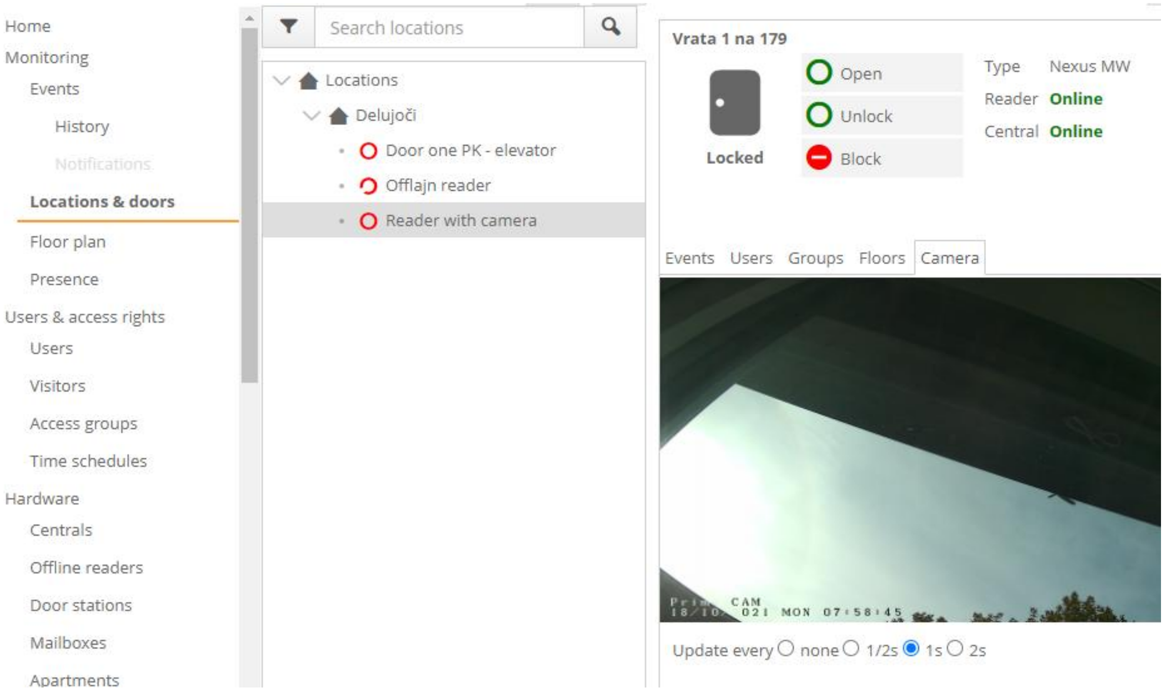
☐ Reason confirmation - Confirmation with a provided reason is required to close the message

☑ Grab IP camera image - This must be also set on readers

Picture 5.17: Select reader events that will trigger IP camera capture

IMPORTANT! Camera grab will take couple of seconds to get the picture from the camera, so make sure that it is positioned accordingly.

Once the camera is installed, its stream will be available in the Locations and doors once the correct reader is selected.



Type Nexus MW

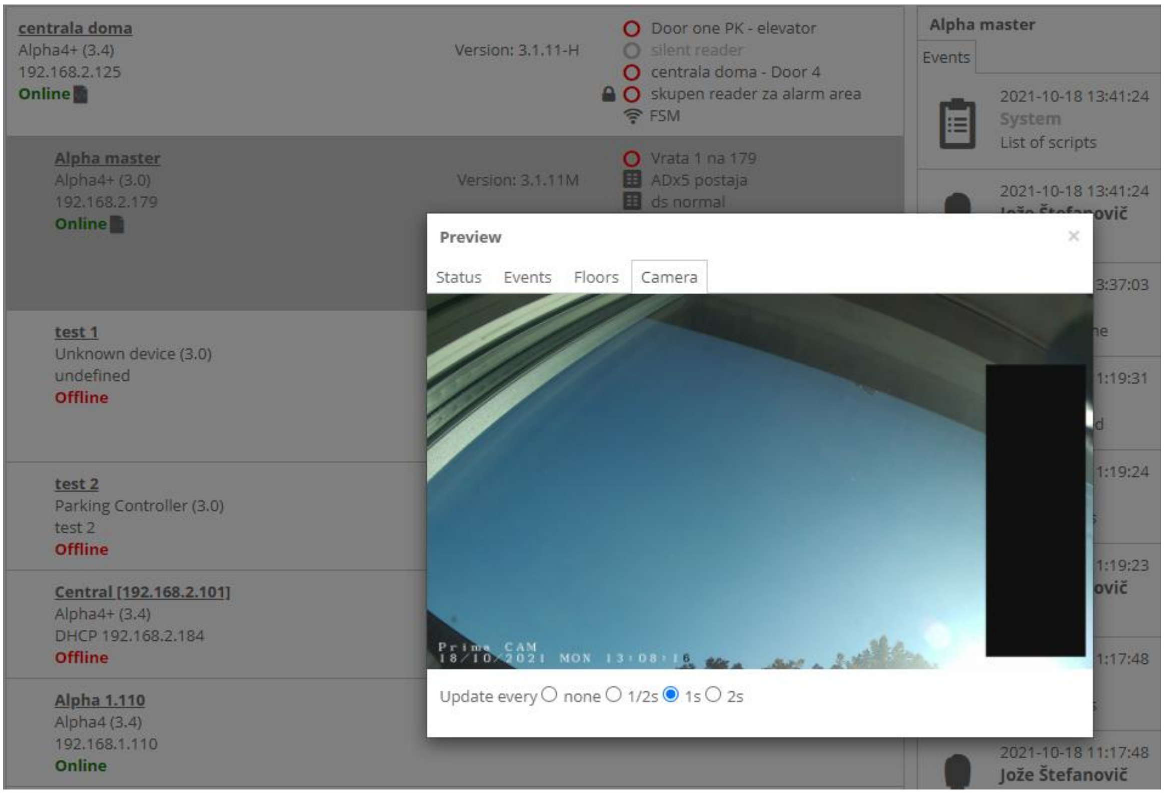
Reader **Online**

Central **Online**

Update every ○ none ○ 1/2s ● 1s ○ 2s

Picture 5.18: When IP camera is assigned to a reader, it can also display its picture stream

Picture can be also viewed from the central list if the reader is selected (the one that has the IP camera selected).



centrala doma
Alpha4+ (3.4)
192.168.2.125
Online
Version: 3.1.11-H
○ Door one PK - elevator
○ silent reader
○ centrala doma - Door 4
○ skupen reader za alarm area
FSM

Alpha master
Alpha4+ (3.0)
192.168.2.179
Online
Version: 3.1.11M
○ Vrata 1 na 179
ADx5 postaja
ds normal

test 1
Unknown device (3.0)
undefined
Offline

test 2
Parking Controller (3.0)
test 2
Offline

Central [192.168.2.101]
Alpha4+ (3.4)
DHCP 192.168.2.184
Offline

Alpha 1.110
Alpha4 (3.4)
192.168.1.110
Online

Alpha master
Events
2021-10-18 13:41:24
System
List of scripts
2021-10-18 13:41:24
2021-10-18 11:17:48
Jože Štefanovič

Preview ×
Status | Events | Floors | Camera

[redacted]

Prima CAM
18/10/2021 MON 13:08:16

Update every ○ none ○ 1/2s ● 1s ○ 2s

Picture 5.19: Camera picture stream can also be viewed from the central list overview

5.2 Offline readers

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

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

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

Management of offline readers:

Open **offline reader editor** (Picture 5-16) by:

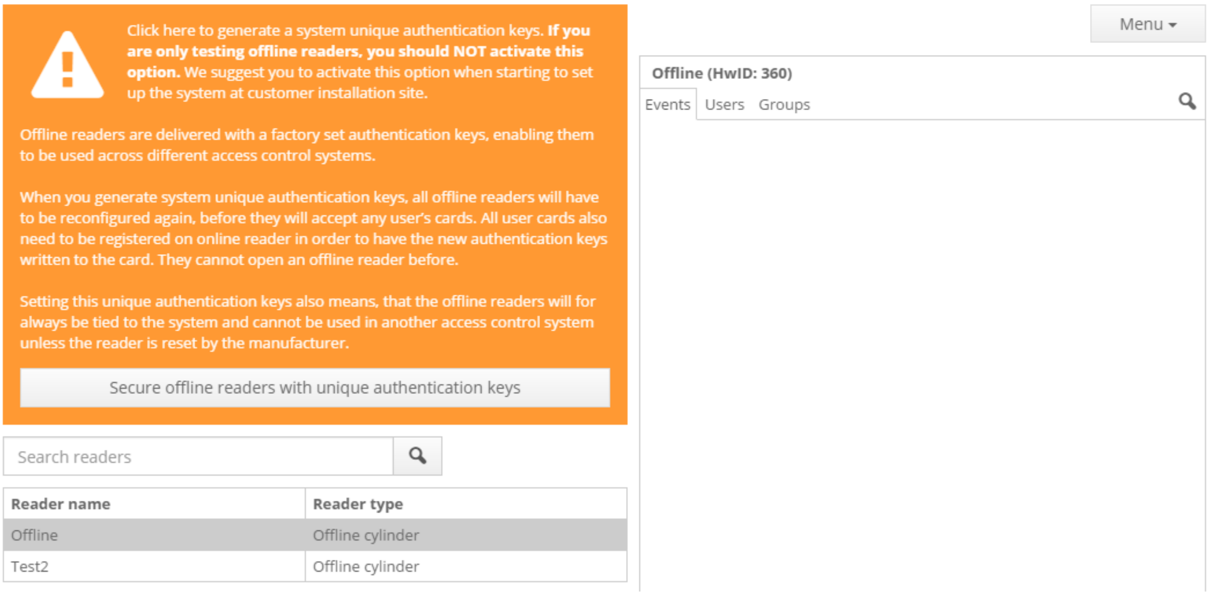
- Navigating to Home > Hardware > Offline Readers widget

Left panel:

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

Right panel:

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



Click here to generate a system unique authentication keys. **If you are only testing offline readers, you should NOT activate this option.** We suggest you to activate this option when starting to set up the system at customer installation site.

Offline readers are delivered with a factory set authentication keys, enabling them to be used across different access control systems.

When you generate system unique authentication keys, all offline readers will have to be reconfigured again, before they will accept any user's cards. All user cards also need to be registered on online reader in order to have the new authentication keys written to the card. They cannot open an offline reader before.

Setting this unique authentication keys also means, that the offline readers will for always be tied to the system and cannot be used in another access control system unless the reader is reset by the manufacturer.

Reader name	Reader type
Offline	Offline cylinder
Test2	Offline cylinder

Picture 5.20: Offline reader editor

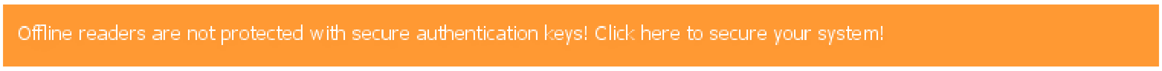
NOTE: All newly set-up systems generate offline keys automatically. If the system is upgraded or restored from an old database, it can happen to still have the old default keys ~ in this case you will see the warning message.

How to lock the system:

- Click on **<u>Secure offline readers with unique authentication keys</u>** button (Picture 5-16).

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

NOTE: Changing authentication keys later, will mean that all user cards and offline readers need to be re-configured with the new authentication keys.
If the system contains at least one offline reader and the offline keys are not protected, the new versions of software (version 1.6+) will display a warning at login (Picture 5-17).



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

Picture 5.21: Unprotected offline system warning

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

- Change its name
- Change its type

  - The system automatically generates the reader's address. This address differentiates between offline readers in the system (Picture 5-16).

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

Customized settings:
Based on reader type, some settings can be customized to control the offline device. The options not supported by the offline reader are greyed out (Picture 5-18).

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

Trace users
To trace users:

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

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

- Using the event's card (for further info see section 4.2.2 Card function assignment). Checking the option **Disable event log on the offline reader** will <u>disable</u> the log.

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

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

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

Toggle mode
To enable toggle mode for the individual user:

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

If wanting to overwrite toggle mode:

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

Time intervals

To check the time intervals on user cards:

- Select the **Check schedule on the user's cards** in the settings of the offline reader.
- The schedule can be set in the **Advanced Settings** for the individual user (see Picture 4-6) under **Cards Validity Settings**.

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

Disable automatic reader activation

This option controls its reading:

- This option is checked: The reader will need to be woken up (turn for a cylinder; a push on the handle…) before user cards are presented.
- If this option is not checked: The reader will repeatedly check for any present user card.
  NOTE: This option is more convenient for more "active" doors since the reader always needs to be checking for the card. This also means that the battery consumption is higher than normal.

Automatic schedule

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

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

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

Public holidays

If the holidays are imported to Nova, they will also be transferred with the offline configuration card.

IMPORTANT! Due to the size limitation on the card, we can only transfer the holidays for the one year ahead. Before that year runs out, the new holidays need to be updated using the configuration card.

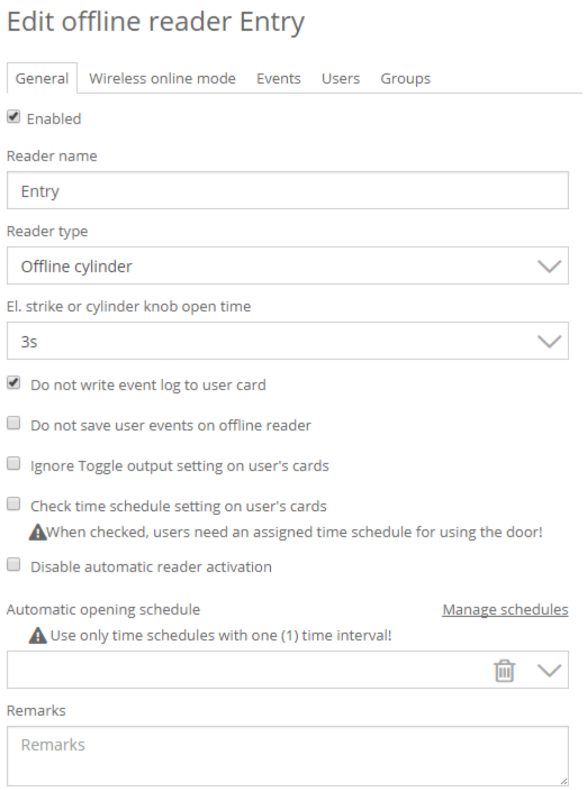
To edit and preview schedules, access the **schedule** editor by:

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

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

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

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



Edit offline reader Entry

General | Wireless online mode | Events | Users | Groups

☑ Enabled

Reader name

Entry

Reader type

Offline cylinder

El. strike or cylinder knob open time

3s

☑ Do not write event log to user card

□ Do not save user events on offline reader

□ Ignore Toggle output setting on user's cards

□ Check time schedule setting on user's cards

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

□ Disable automatic reader activation

Automatic opening schedule — Manage schedules

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

Remarks

Remarks

Picture 5.22: Offline reader settings

5.2.1 Offline readers and maintenance cards

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

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

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

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

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

5.2.2 Creation of configuration cards for offline devices in Nova software

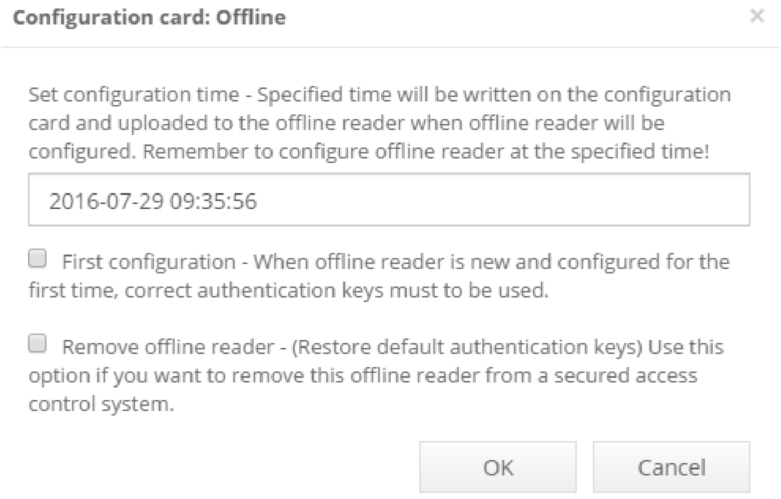
The maintenance card for transferring configuration settings to an offline device must be created for each offline reader.

To create a configuration card:

1. Select the offline reader in the Offline reader editor (Picture 5-16)
2. Click the button Create configuration card
3. Set time of actual device configuration in a popup window – actual time of when the configuration card will be presented to the offline reader (Picture 5-19)
    - This is necessary due to time synchronization between the online system and offline reader (Picture 5-19).

Adding new offline readers to the system:

1. Check the **First configuration** option (Picture 5-19).
    - This will ensure the right authentication keys on the configuration card.
2. **Confirm the settings** of the configuration card.
3. To upload the configuration, put the **configuration card** on an enabled online reader, which can **write data on cards.**
    - The configuration settings are written to the card and three "beep" sounds confirm the successful writing operation.


Configuration card: Offline

Set configuration time - Specified time will be written on the configuration card and uploaded to the offline reader when offline reader will be configured. Remember to configure offline reader at the specified time!

2016-07-29 09:35:56

□ First configuration - When offline reader is new and configured for the first time, correct authentication keys must to be used.

□ Remove offline reader - (Restore default authentication keys) Use this option if you want to remove this offline reader from a secured access control system.

Picture 5.23: Create a configuration card

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

NOTE: The configuration card transfers the settings of a particular reader, and it must, therefore, be registered on the offline reader it was created for. The configuration card with a particular setting can only be used once.
Three long beeps, three short beeps, and green LED flash to follow correct configuration.

REMEMBER to configure the offline reader on the set time from the pop-up window, for it to synchronize with the online system.

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

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

5.2.3 Lost and blacklisted cards

Lost user cards can be blocked on offline readers to prevent unauthorized entries. Offline readers will ignore cards, which are on their blacklist.
To report a lost card:

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

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

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

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

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

5.2.4 Reading events from offline devices

Offline devices keep track of internal events and can keep track of users' events. Events are stored in the internal memory of the device.
Events are written to the card and are then registered in the software when the card passes an online reader.
To transfer events from the offline reader internal memory:

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

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

NOTE: Same **Events card** can be used on all offline devices – one at a time.
The tracking of user events on the internal storage of the offline device can be turned off under the settings for the device in Nova.

5.2.5 Configuration of online reader settings for writing access rights

Transfer data between the central and an offline reader by writing data to a contactless card. This data writing usually takes place at building entries to guarantee the best user experience. The offline reader then reads the data.
To enable online readers to write access rights to cards:

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

5.2.6 Offline readers and Nova software

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

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

5.2.7 Battery level on offline cylinders

IMPORTANT! When changing the battery on any offline device, it is strongly recommended to update the time with the configuration card to avoid losing internal RTC.

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

Discovery of low battery level follows these three phases:

1. Five red flashes and sound signal appear when holding a tag/card in front of the cylinder knob.

    - Change the batteries using the **Battery card** and the battery tool as described in section 5.2.8.

2. A light and sound signal appears when holding a tag/card in front of the cylinder knob. It takes 5 seconds before the cylinder is ready for opening or closing.

    - Change the batteries using the **Battery card** and the battery tool as described in section 5.2.8.

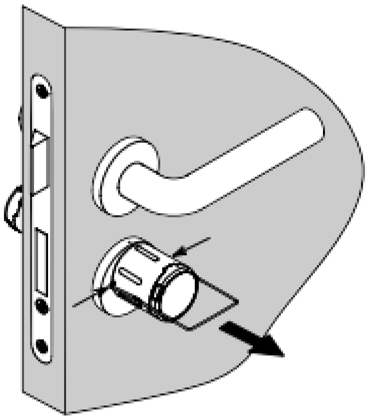
3. The cylinder will not read any activated tags/cards. When the cylinder is in phase 3, it is necessary to use an adapter for battery changes.

    - Remove the logo-plate and attach the battery-adapter with a 9V battery. Then change the batteries as described in section 5.2.8.

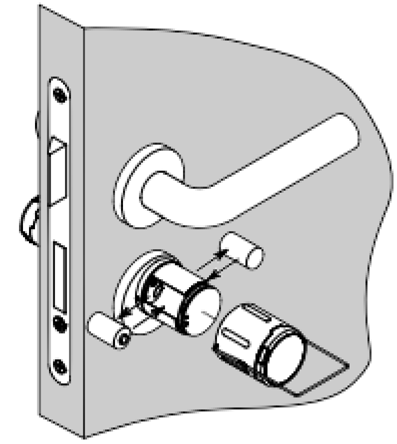
5.2.8 Changing batteries in offline devices

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

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

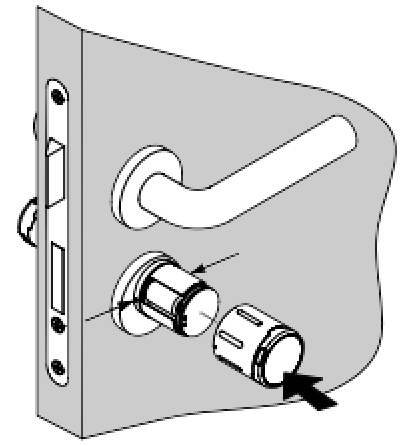


3. Replace the two CR2 3V Lithium batteries



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

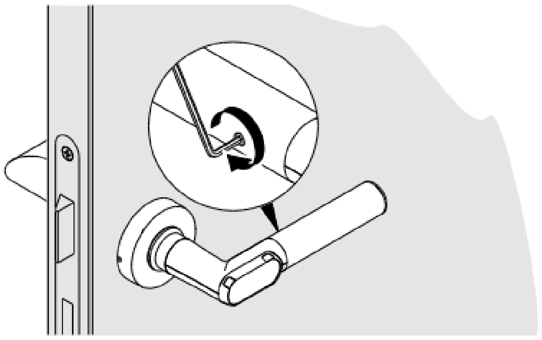
4. Push the cap back on the cylinder



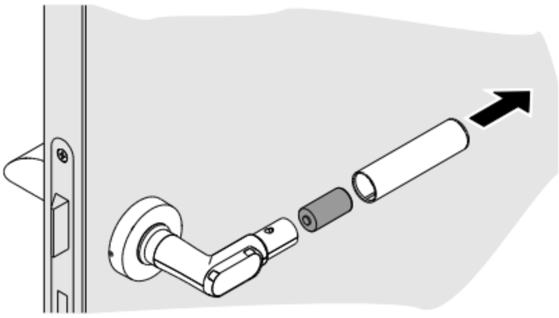
5. Make tabs fit into cap holes
6. Hold **Battery card** in front of the cylinder to lock the tabs

Offline handle battery replacement:

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



3. Remove the gripping sleeve.



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

5.2.9 Offline device feedback

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

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

Table 5.1 summarizes different functions and feedback from the device.

		Offline cylinder, Offline EvoLock cylinder, Offline locker lock, Offline handle			**Nexus offline**		
			LED			LED	
Group	Event	Buzzer	red	green	Buzzer	red	green
User	Card rejected	—	—		—	—	
	Wrong keys					· · · ·	
	Card accepted			—	·		——
	Schedule toggle/toggle			—	—		—
	Battery replacement	—	—	—			
	Response stale PIN				—		
System	Reset	—	—	—			
	Reader not in horizontal position	. . .					
	Anti-theft beep	· · periodically*					
	Battery low	· · · · · ·	· · · · · ·				
Service mode	Start	. ·					
	End	· .					
Whitelist mode	Start	— ·					
	Teach-in	· ·					
	Erase	— —					
	Memory full	— — — ·					
	End	· —					
	Read try		· · · · · ·				
Transponder	Read/Process		——				
	Accept			—			
	Reject	—	—				
	Toggle start	—		—			
	Toggle end	—	—				
	Configuration change	— — — · · ·		——	— — — · · ·		——
Error	Configuration/Memory	— — — — — ·			— — — — —		· · · ·
	Actuator	— — — — — · ·					
	RTC	— — — — — · · ·			— — — — —	· · · · · ·	
	Wake-up	— — — — — · · · ·					
	RFID IC	— — — — — · · · · ·					
	Radio	— — — — — · · · · · ·					
	RFID IC	— — — — — · · · · · · ·					
	Processing response					· · · · · · · · ·	

Table 5-1: Functions and feedback of different offline devices

*Present the Wireless service card right after the beeps to confirm ownership and the alarm should stop.

5.2.10 Card segments of offline reader

Nova software version 1.5 or higher support card segment settings for offline readers.
NOTE: To access this option, navigate to the Home > Hardware > Offline Readers and press Menu > Global Settings.
This functionality allows the System administrator to set different writing sectors on the cards.

- This is useful for those who keep other data stored on their cards. E.g.: If there is some 3rd party data already written on sectors seven and eight, authentication segment sectors can set in range 1-5 (5 sequenced sectors needed).
    - This will allow users to keep their data on wanted segments.
    - Additionally, feedback segment sectors can be changed the same way. Feedback sectors are only written on the card if the reader is set to **Write data on the card** and **Read events from user cards** (Please see chapter **4.2.3 Managing users, their access rights**).

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

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

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

The above example shows how sectors can be moved and which ones remain unmodified. The first example (the "not ok" one) shows the result of no unmodified sectors, which can be problematic for some people, who want to have some sectors reserved for some other data on the card. The remaining examples show a range of sectors that remain free for others to use.
The offline reader will work regardless of the unmodified sectors if it has set sectors "free".

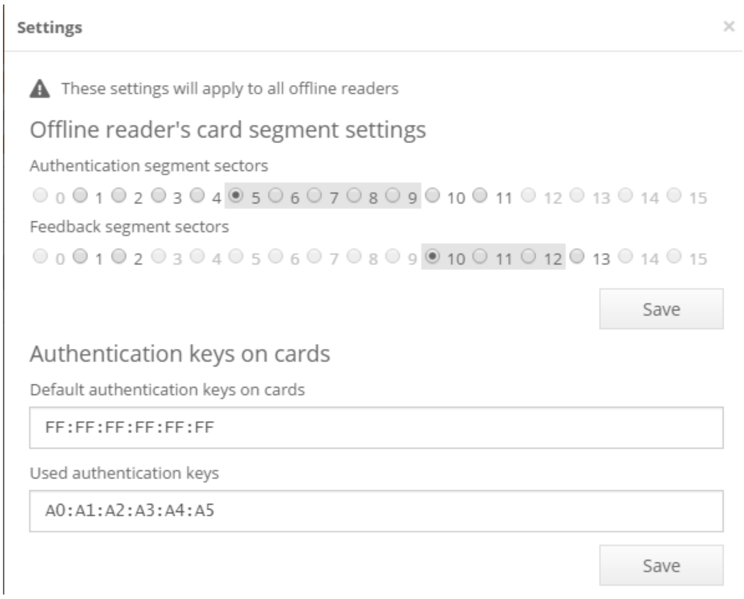
NOTE! Formatting a card will delete all accessible data, while 3rd party data is protected and will not change.

5.2.11 Blacklist settings

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

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

5.2.12 Offline authentication keys



Settings

These settings will apply to all offline readers

Offline reader's card segment settings

Authentication segment sectors

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ● 5 ○ 6 ○ 7 ○ 8 ○ 9 ○ 10 ○ 11 ○ 12 ○ 13 ○ 14 ○ 15

Feedback segment sectors

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7 ○ 8 ○ 9 ● 10 ○ 11 ○ 12 ○ 13 ○ 14 ○ 15

Save

Authentication keys on cards

Default authentication keys on cards: FF:FF:FF:FF:FF:FF

Used authentication keys: A0:A1:A2:A3:A4:A5

Save

Picture 5.24: Changing authentication keys

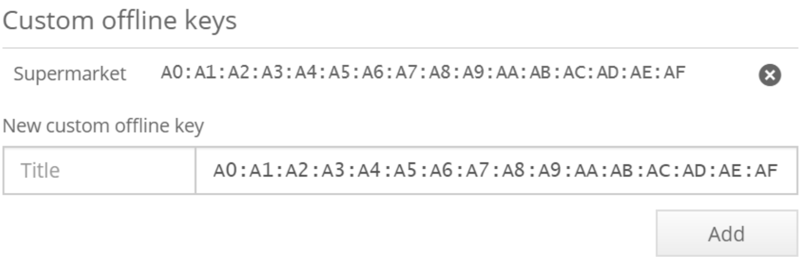
Section **Authentication keys on cards** allow changing authentication keys for protecting data on MIFARE cards.

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

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

5.2.13 Merging offline keys from multiple systems

Each system is locked with a unique key, so cards that work on one will not work on the other. Merging could be done by resetting the offline keys to default on one system and adding them as additional keys to the newly (merged) system.
Nova version 3.0 supports the inclusion of multiple keys.
Superadmin account can access the offline settings by navigating to **Hardware > Offline readers > Menu > Global settings**.
In the bottom, they can enter the Name of the merged project and its offline key.



Custom offline keys

Supermarket A0:A1:A2:A3:A4:A5:A6:A7:A8:A9:AA:AB:AC:AD:AE:AF

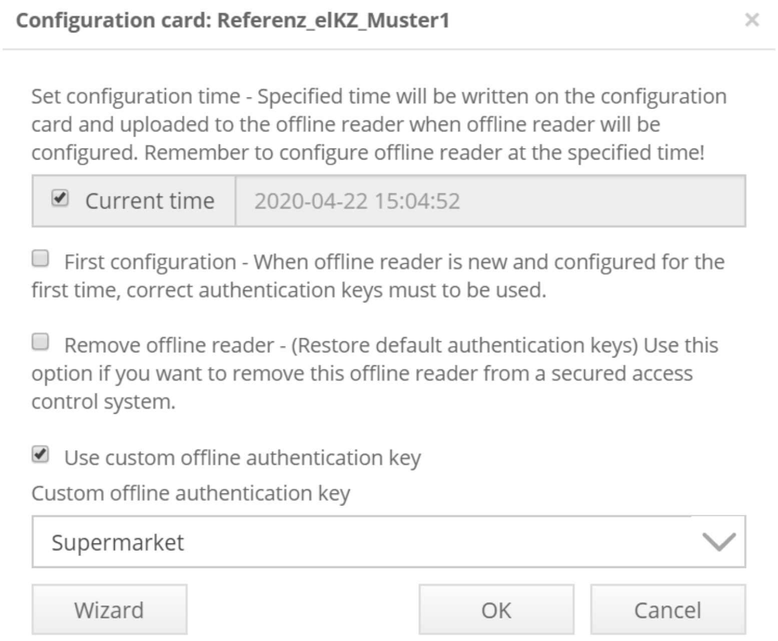
New custom offline key

Title	A0:A1:A2:A3:A4:A5:A6:A7:A8:A9:AA:AB:AC:AD:AE:AF

Add

Picture 5.25: Adding unique keys from another system during a merger

When creating a configuration card, a **sysadmin** must choose the old project under the custom offline authentication key. Once updated, this will replace the old key with the new one. Once reconfigured, all the user cards will stop working until they are updated on the online reader (that has writing enabled) or the USB reader.



Configuration card: Referenz_elKZ_Muster1

Set configuration time - Specified time will be written on the configuration card and uploaded to the offline reader when offline reader will be configured. Remember to configure offline reader at the specified time!

☑ Current time 2020-04-22 15:04:52

□ First configuration - When offline reader is new and configured for the first time, correct authentication keys must to be used.

□ Remove offline reader - (Restore default authentication keys) Use this option if you want to remove this offline reader from a secured access control system.

☑ Use custom offline authentication key

Custom offline authentication key

Supermarket

Wizard OK Cancel

Picture 5.26: Using the configuration card to replace the old unique key with a new one (in the merged system)

5.2.14 Offline partitions

Offline partitions are designed for systems that have a plan for more than 1500 offline devices in the system. **Offline+ activation key is required** to enable this feature.
If the maximum limit is reached, a new partition of additional 1500 readers can be added (up to 4500) ~ current maximum is 3 partitions (one main and two additional).

To enable the partitions, navigate to **Hardware > Offline readers**, click on the **Menu** button and select **Global settings.** Enable the checkmark in the Offline partitions sections and Save changes. A new sub-menu will be displayed under Offline readers; you can also access it via **Menu > Offline partitions**. If there were any offline readers present in the system, they are already part of the default partition.
From here we can now:

- Add: **Menu > Add offline partition**, provide a name, and select in which partition data should be saved.
- Edit: Select the partition you wish to edit, **Menu > Edit partition.**
- Delete: Select the wanted partition and press **Menu > Remove** (the default partition cannot be deleted).

Once the partitions are created, you can navigate back to the Offline reader's menu and in the process of adding an additional offline reader, the offline partition needs to be assigned. When creating the Offline Configuration card for this reader, it can be created on an online reader that has writing enabled, even the USB one (reader's writing partition is ignored in this case).

Online readers can only write a single partition to the card. To assign that partition, navigate to reader's Advanced settings; Card data management must be turned on to enable the next dropdown where the offline partition can be selected.

User access is stored differently based on the type of cards in use.
MIFARE Classic® cards, because of their small size, allow only **one partition** to be written on them. If a user uses mostly default partition, and has also access to the second partition, they need to visit an online reader that has second partition writing enabled to be assigned their new access for partition two (and the access to the default partition will be overwritten).
MIFARE DESFire® cards can contain multiple partitions on the same card. To get access rights from all the partitions written on the card, one must present (and have access) its card to all online writing readers from all different partitions.

NOTE! Reader firmware version 32+ is required to write multiple partitions.

5.2.15 Offline+ (804-00x3002/3010/3050)

When presenting this license to the system it must match the number of offline readers in the system as ALL online and offline readers will have additional functions.

Offline readers can now write events (up to 16 events) back to user cards, so when the card is presented to the online reader it will read out the events and report them to Nova along the battery status (reported separately).

If the user has multiple cards assigned and one gets lost, the card needs to be marked as Lost in Nova, then he can use his own user cards to update the blacklist on the offline devices (instead of using the blacklist card).

Each user can be assigned a schedule – up to 2 intervals and their access will only be available within this period.

User can be selected that will have to option to unlock offline any of the offline readers they have access to. The first card read will open the reader and if they have this option set, on the second read, the reader will stay unlocked.
IMPORTANT! Reader can then be locked by schedule, but other users that don't have this option to toggle, they will only be able to open it, so be mindfully that the reader can stay unlocked.

5.3 Special hardware devices

5.3.1 GSM Gateway

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

How it works:

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

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

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

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

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

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

IMPORTANT! The GSM gateway stores its configuration on the SIM card (e.g., RS-485 bus address). When a pre-configured SIM card is inserted into the device, **the configuration is restored from the SIM card**. Please note that changing SIM cards between devices will also change the RS-485 addresses of those devices and the system requires reconfiguration.
The GSM Gateway reports phone caller IDs in the form with the **country entry code** (e.g., 00386yyyyy for Slovenia). When assigning phone numbers to the user's profile, leading zeroes can be omitted.

5.3.2 Remote control Reader

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

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

For more information about adding new devices to the central see chapter **5.1.13 Adding new readers**.
For more information about adding new cards to users see chapter **4.2.1 Adding unknown card(s) to the user**.

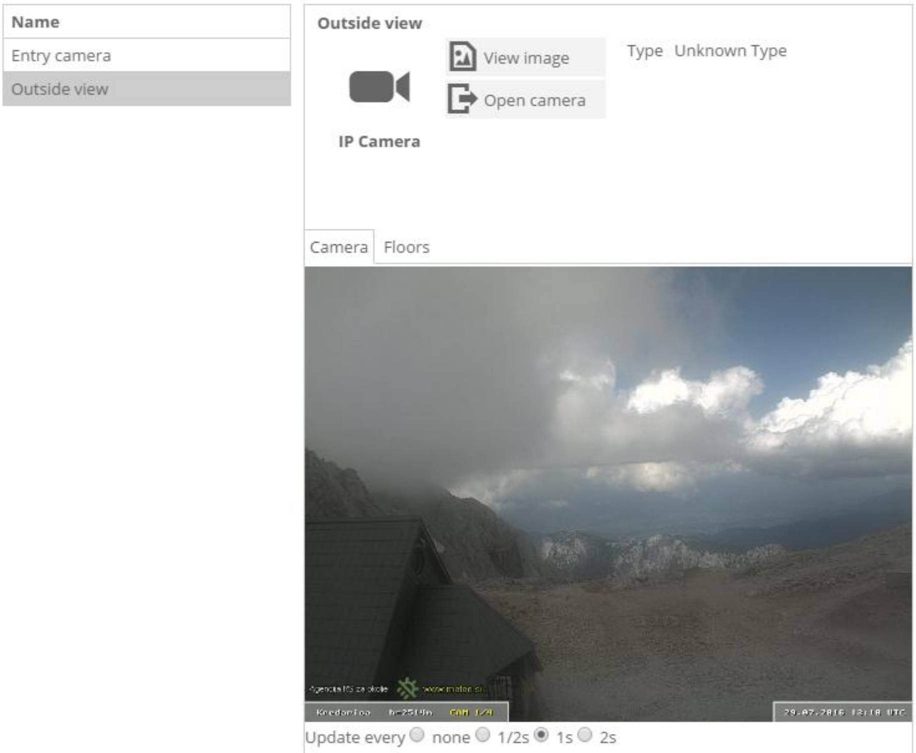
5.3.3 IP Camera

IP cameras can be added by providing direct access to the image.
Most of the cameras do not capture video, but images every few seconds and serve them to some IP address. To get the picture from the camera to the Nova software, we need to provide a direct link to the software (including login if required).

We can add a camera by:

1. Navigating to Home > Hardware > IP Cameras.
2. Press Menu > Add camera.
3. A pop-up menu will require the entry of Camera name, its IP Address, type, and image address.
    - If the camera type is not located in the dropdown menu, only the entry of the image address is required (Picture 5-23).
    - The supported camera type (Picture 5-24) will have a few additional options like detecting if the camera is online, IP change, flipping or rotating the screen, the ability to move the camera (if the camera supports it), the option to display custom text on the image (a preview of the settings is displayed on Picture 5-25) …
      Supported cameras are also found with the **Central discovery tool** (see chapter 24)**.**
4. Pressing **Add** adds the camera to the system.

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



Name
Entry camera
Outside view

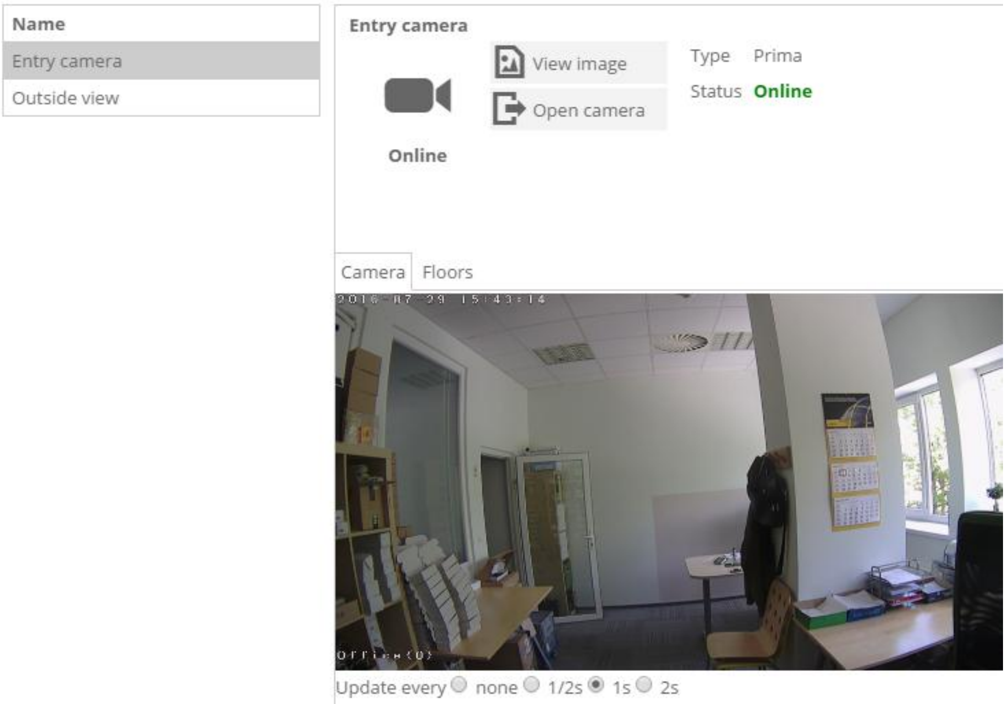
Outside view

IP Camera

Type Unknown Type

Update every ○ none ○ 1/2s ● 1s ○ 2s

Picture 5.27: IP camera picture of the unknown type



Name
Entry camera
Outside view

Entry camera

Online

Type Prima

Status **Online**

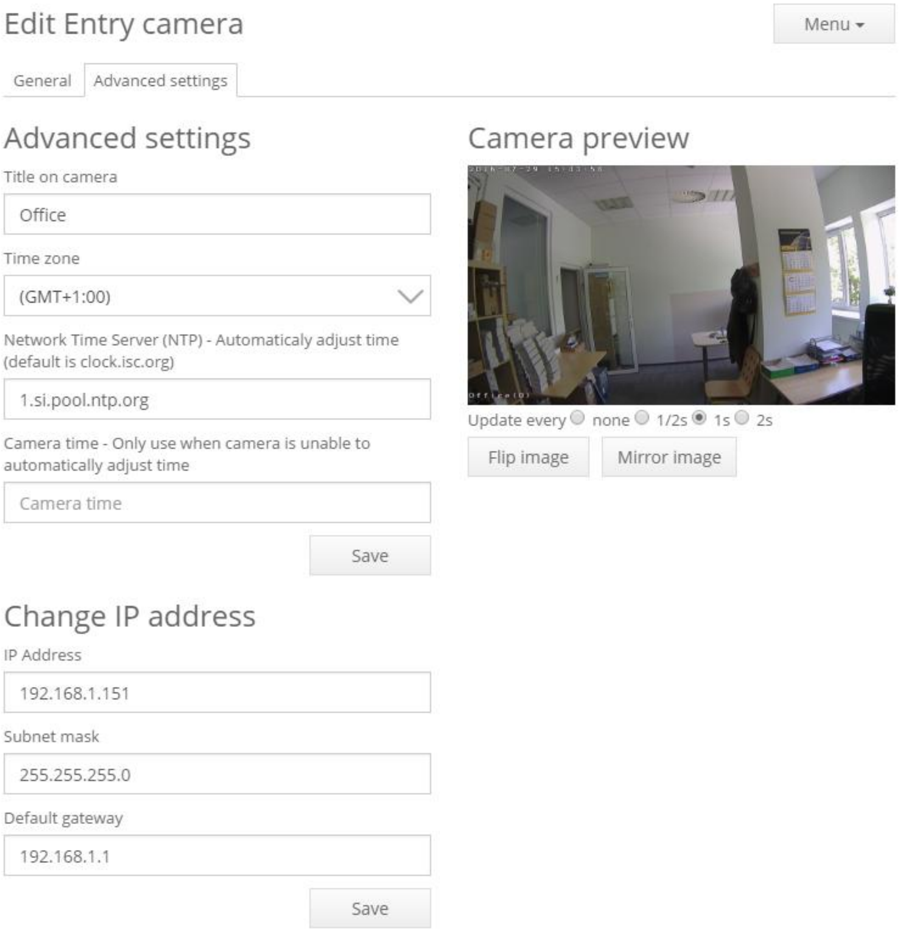
Update every ○ none ○ 1/2s ● 1s ○ 2s

Picture 5.28: IP camera picture from the Prima type

To edit camera data, double click on the camera.

To delete the camera from the system:

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



Edit Entry camera

Menu ▾

General | Advanced settings

Advanced settings

Title on camera

Office

Time zone

(GMT+1:00)

Network Time Server (NTP) - Automaticaly adjust time (default is clock.isc.org)

1.si.pool.ntp.org

Camera time - Only use when camera is unable to automatically adjust time

Camera time

Save

Change IP address

IP Address

192.168.1.151

Subnet mask

255.255.255.0

Default gateway

192.168.1.1

Save

Camera preview

Update every ○ none ○ 1/2s ● 1s ○ 2s

Flip image | Mirror image

Picture 5.29: Known camera type, advanced settings

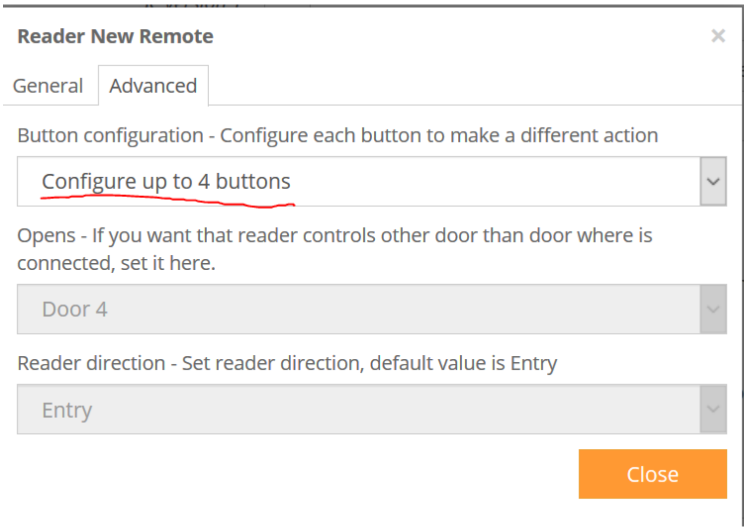
5.3.4 Pro remotes

The hand remotes are special hardware that allow users to access their garage doors/ramps from a longer distance.
The remote receiver is a device that can be wired to the central the same way as an online reader. There is also a special USB option (that also works with USB reader software) which can be used for assignment of the remotes to users. This hardware contains a rolling code and protected communication which prevents any malicious copy of the signal.

How to set-up the remote receiver that is connected to the central:

1. Navigate to the central that has the remote receiver connected and trigger a reader search.
2. Double click on the found reader to add it to the system.
3. Name it to where it is mounted or what it opens.
4. Save settings.

Hand remotes can have 2 or 4 buttons that by default just open (if the rights are assigned) the door that the remote receiver is connected to. We can however program them for each button to open different doors of that central. To do so, navigate to the remote receiver's advanced settings and choose the 2 or 4 buttons settings, close the pop-up, and save.



Reader New Remote

Button configuration - Configure each button to make a different action

Configure up to 4 buttons

Opens - If you want that reader controls other door than door where is connected, set it here.

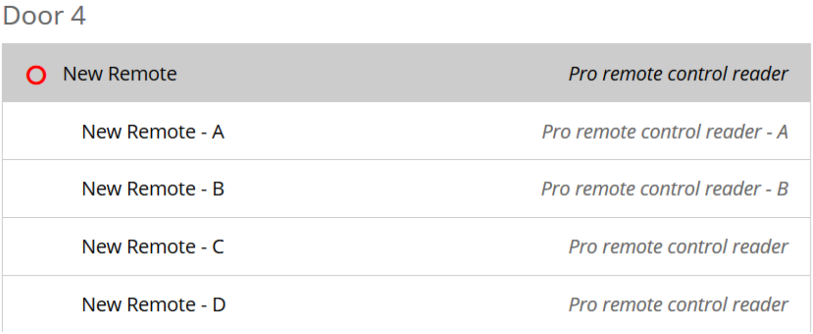
Door 4

Reader direction - Set reader direction, default value is Entry

Entry

Picture 5.30: Buttons can be set-up for all to open a single door or to open multiple

The remote will now show as many buttons as we have chosen.



Door 4

New Remote	*Pro remote control reader*
New Remote - A	*Pro remote control reader - A*
New Remote - B	*Pro remote control reader - B*
New Remote - C	*Pro remote control reader*
New Remote - D	*Pro remote control reader*

Picture 5.31: 4 buttons setting

Inside each button's advanced settings, we can specify which door it should open and the direction (important for Anti-pass back).
The access groups will show 1/2/4 buttons depending on the setting and we can specify the schedule, their action along with dispatch events (if the scripting is present).

To assign a remote reader to a user, navigate to that user and press one button on it, this will trigger the new Identification device banner, asking you to assign the ID to the current user. Do not forget to assign the access rights too.

Transmitter LED notifications:

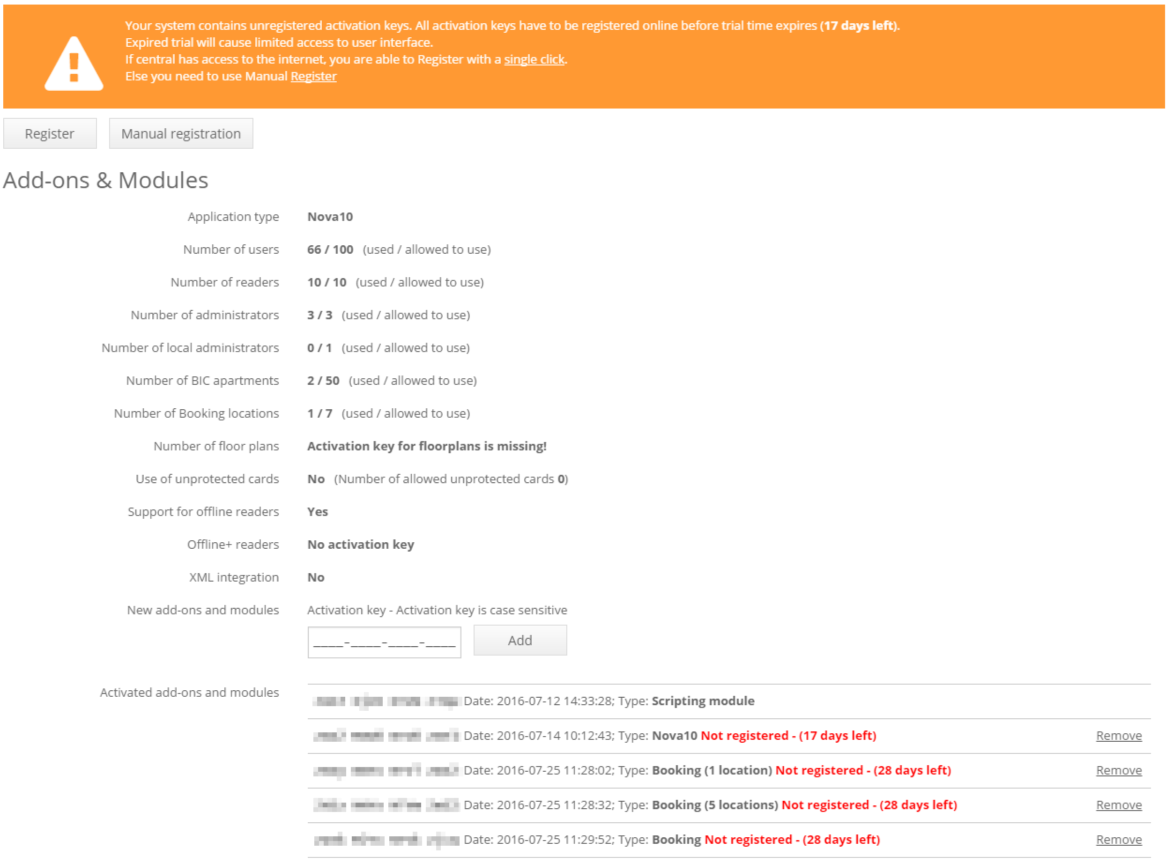
LED Status	Color	Description
Solid	GREEN	Transmitting
Solid	RED	Battery low
Blink slow	GREEN	Authorization in-progress
Blink fast	GREEN	Auto-installing authorized
Off	-	Authorization transferred

6. Settings

6.1 Add-ons and Modules

Add-ons and Modules contain Nova details and input boxes for entering a new activation key (Picture 6-1).
By purchasing the desired activation key, a system upgrade is made for Nova software from NovaSimpli to other Nova versions.

NOTE: NovaSimpli does not require any activation key.



Your system contains unregistered activation keys. All activation keys have to be registered online before trial time expires (**17 days left**).
Expired trial will cause limited access to user interface.
If central has access to the internet, you are able to Register with a single click.
Else you need to use Manual Register

Add-ons & Modules

Application type	**Nova10**
Number of users	**66 / 100** (used / allowed to use)
Number of readers	**10 / 10** (used / allowed to use)
Number of administrators	**3 / 3** (used / allowed to use)
Number of local administrators	**0 / 1** (used / allowed to use)
Number of BIC apartments	**2 / 50** (used / allowed to use)
Number of Booking locations	**1 / 7** (used / allowed to use)
Number of floor plans	**Activation key for floorplans is missing!**
Use of unprotected cards	**No** (Number of allowed unprotected cards **0**)
Support for offline readers	**Yes**
Offline+ readers	**No activation key**
XML integration	**No**
New add-ons and modules	Activation key - Activation key is case sensitive ____-____-____-____ Add
Activated add-ons and modules	[redacted] Date: 2016-07-12 14:33:28; Type: **Scripting module** [redacted] Date: 2016-07-14 10:12:43; Type: **Nova10 Not registered - (17 days left)** Remove [redacted] Date: 2016-07-25 11:28:02; Type: **Booking (1 location) Not registered - (28 days left)** Remove [redacted] Date: 2016-07-25 11:28:32; Type: **Booking (5 locations) Not registered - (28 days left)** Remove [redacted] Date: 2016-07-25 11:29:52; Type: **Booking Not registered - (28 days left)** Remove

Picture 6.1: Add-ons & Modules tab

Upgrading to the NovaSimpli350 software version is free, the activation code is provided by the issuer of the hardware.

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

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

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

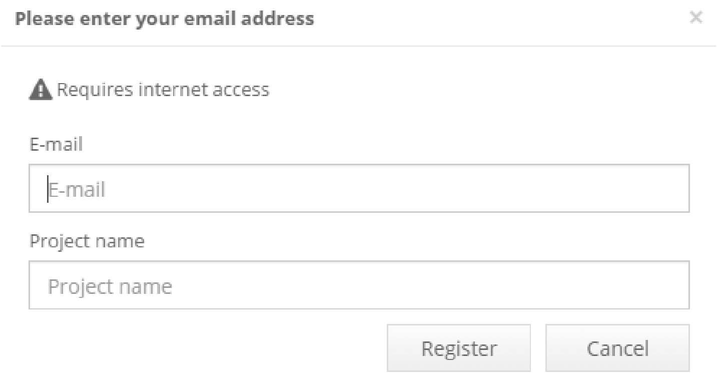
Note: Deleting and re-entering the same keys will not reset the Registration count-down.

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

6.1.1 Online system registration

To register the system online:

1. Press the **Online Registration** button (located at the top of Picture 6-1). A pop-up window will appear (shown in Picture 6-2).
2. Enter e-mail and a project name. Provided data will be used for easier assistance and software update/upgrade notifications.
3. Press the **Register** button. If the registration was successful, the green box will appear with the OK message (Picture 6-4); if there are any issues with the internet connection and the registration fails, it is advised to proceed with manual registration.



Please enter your email address

Requires internet access

E-mail

E-mail

Project name

Project name

Picture 6.2: Online system registration form

6.1.2 Offline system registration

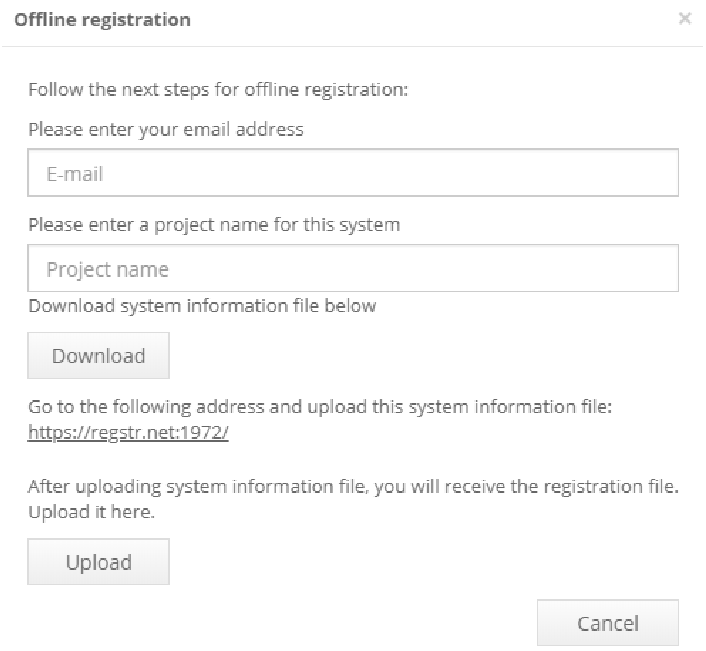
Offline registration steps:

1. Press the **Offline Registration** button (located at the top of Picture 6-1). A pop-up window will appear (shown in Picture 6-2).
2. Enter e-mail and a project name. Provided data will be used for easier assistance and software update/upgrade notifications.
3. Press the **Download** button – a window will open to save the system information file to your computer. Select a folder with easy access.
4. Transfer the file to the USB stick and plug it into a computer with internet access. If the procedure is done on a mobile device (i.e., laptop/tablet/phone …), it is enough to move to a location with internet access.

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

- Click on the button to **upload the system information** file that was previously downloaded.
- If the upload was a success, continue to download the **Registration file**. Download it to a folder with easy access.

5. Transfer the file **Registration file** back to the USB stick and plug it back to the computer that is connected to the central OR if using a mobile device, go back to the network with central access.
6. Open the Nova 2.0 window and press the **Upload** button. Select the **Registration file.** The system is now registered (Picture 6-4).



Offline registration

Follow the next steps for offline registration:

Please enter your email address

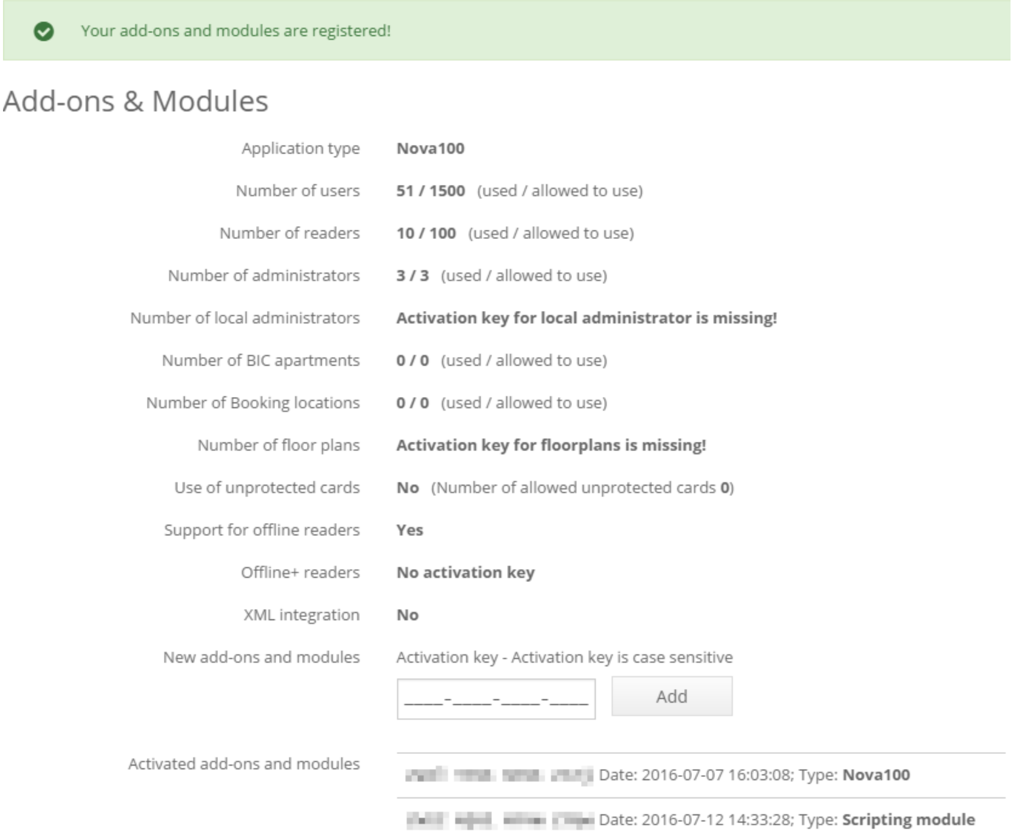
Please enter a project name for this system

Download system information file below

Go to the following address and upload this system information file:
https://regstr.net:1972/

After uploading system information file, you will receive the registration file. Upload it here.

Picture 6.3: Offline system registration pop-up



✔ Your add-ons and modules are registered!

Add-ons & Modules

Application type	**Nova100**
Number of users	**51 / 1500** (used / allowed to use)
Number of readers	**10 / 100** (used / allowed to use)
Number of administrators	**3 / 3** (used / allowed to use)
Number of local administrators	**Activation key for local administrator is missing!**
Number of BIC apartments	**0 / 0** (used / allowed to use)
Number of Booking locations	**0 / 0** (used / allowed to use)
Number of floor plans	**Activation key for floorplans is missing!**
Use of unprotected cards	**No** (Number of allowed unprotected cards **0**)
Support for offline readers	**Yes**
Offline+ readers	**No activation key**
XML integration	**No**
New add-ons and modules	Activation key - Activation key is case sensitive ____-____-____-____ Add
Activated add-ons and modules	[redacted] Date: 2016-07-07 16:03:08; Type: **Nova100** [redacted] Date: 2016-07-12 14:33:28; Type: **Scripting module**

Picture 6.4: Completed registration

6.2 Login Settings

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

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

6.3 Database Settings

The **Database Settings** widget is used for advanced settings and is only enabled for system administrators.
This widget offers these options:

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

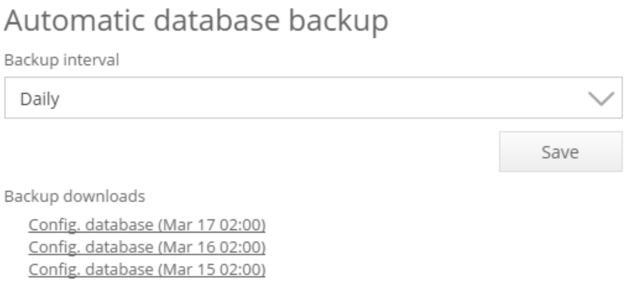
CAUTION: When uploading a configuration database with new settings, be aware that a damaged database file can cause the system to stop working.

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

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

6.3.1 Automatic database backup

Nova version 1.5 and higher support automatic backup of the configuration database as shown in Picture 6-5.



Automatic database backup

Backup interval

Daily

Save

Backup downloads

Config. database (Mar 17 02:00)
Config. database (Mar 16 02:00)
Config. database (Mar 15 02:00)

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

Automatic database backup can be set to:

- Turned off
- Daily
- Weekly
- Monthly

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

- *Daily* backup will be created at 2:00 AM.
- *Weekly* backup will be created every Monday at 2:00 AM.
- *Monthly* backup will be created every 1st day of the month at 2:00 AM.

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

Backup and local memory

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

If backups are stored in local memory, it will keep three copies of the last periods (e.g., if the automatic database backup is set to daily, it will keep backups for the last three days; for weekly - last three weeks and for monthly - last three months).
NOTE: At any time, the backup is switched from off to on, it will create a new backup after a few minutes. Backup copies are downloaded by clicking on the corresponding text.

Automatically optimize database option will automatically run database optimization each day which benefits larger systems.

Automatically clean-up database - expired booking reservations, deleted users, deleted access groups, and deleted hardware remain inactive in the database, and by enabling this option, they will be permanently deleted after 6 months.

6.3.2 Event archive

Nova's option to remove events older than N days can be enabled by selecting how long you wish to keep the events in the archive.
NOTE: Some countries are required to delete events older than N days. Please check the regulations of the country where the central is located.

6.3.3 GDPR settings

The EU General Data Protection Regulation is the privacy regulation that we need to comply with. The drop-down offers different time options after that:

- User data will be replaced with "**Anonymous user"** in the Events after the set time.

- The Event data could also hold sensitive information, so it is deleted too.
- Deleted users (whom we keep checking this user's event history), have their name and last name replaced with "**Anonymous user.**"

6.4 Other Settings

6.4.1 Time zone

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

NTP server

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

6.4.2 Web server port

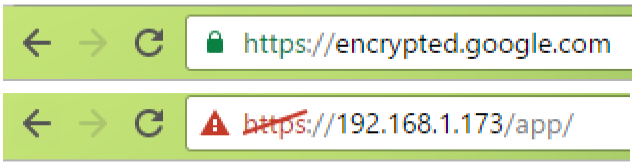
Sometimes the software needs to be accessed from the internet in cases where something is already occupying the default HTTP port (80), internal ports can be changed and forwarded to meet the needs.

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

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

6.4.3 Security settings

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


https://encrypted.google.com

~~https~~://192.168.1.173/app/

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

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

HTTPS redirect

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

Disable SSH access

If the customer is having certain issues, we use the SSH port (22) to check "behind the curtain" to see why something is not working. This also presents a security risk when SSH vulnerabilities are discovered. System administrators can choose to turn off SSH access completely if this is a concern.

A secure connection between centrals

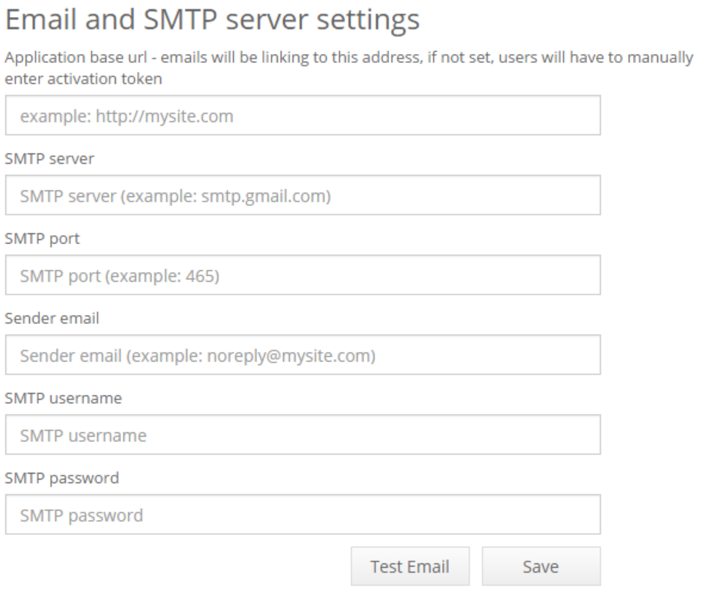
Available options:

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

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

6.4.4 SMTP server settings

With the new version of Nova software, we can send emails to users in the system. This is used in **Module: Presence, Module: Messaging, New user creation, Password recovery…**
The grey text in the text box is an example of Gmail settings.
IMPORTANT! The google account must **allow less secure apps** to be able to connect to the Gmail account. Please make sure that this option is **turned ON,** in the used Gmail account.



Email and SMTP server settings

Application base url - emails will be linking to this address, if not set, users will have to manually enter activation token

example: http://mysite.com

SMTP server

SMTP server (example: smtp.gmail.com)

SMTP port

SMTP port (example: 465)

Sender email

Sender email (example: noreply@mysite.com)

SMTP username

SMTP username

SMTP password

SMTP password

Picture 6.7: Email and SMTP server settings

6.4.5 Global reader settings

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

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

Second card read – (works with reader firmware 29+) sets up the timeout on all readers in the system between the first and the second card read ~ users must hold their card on the reader to trigger it. Second read can be used for all kind of actions like arming the alarm, disarming, opening, or unlocking a door, triggering the alarm action etc.

Reader encryption – communication with the readers should be already enabled by default, but for older system that were running older reader firmware; now they can upgrade the reader's firmware version 29+ and once all are updated, they can mark the checkbox that will encrypt the communication between the central and the reader.

Cards security – used for systems that are migrating from unsafe MIFARE Classic® cars/tags to secure MIFARE DESFire® ones.
The card replacement can take a lot of time, so there are different steps that we can manage:

- (Default) Unsafe Allow MIFARE Classic® on online and offline readers.
- Unsafe **Disable MIFARE Classic® on Offline readers –** Offline readers will not read classic cards anymore, but they can still be used for regular online access.
- Safe **Disable MIFARE Classic® on online and offline readers –** completely disable any old cards from working and being written on.

IMPORTANT! When switching the any of the above modes, the configuration card must be created and updated **for each offline** reader in the system.
Configuration card can be used single time once prepared; for faster offline reader programming, you can use USB reader's offline configuration data to connect to the central and then repeat the process: Configuration card to the USB reader, configuration card to the offline device …
If the MIFARE Classic® card is put on system where reading/writing of such cards is disabled, there will be no audio feedback; reader firmware is 51+ will beep two times, the events will still be reported int Nova.

Card initialization is used during the system set-up phase to make sure that all the cards get the correct offline key and rights assigned on the online readers. Once all the cards are already in the system and there is no need to check/change the offline key, we can turn this option off, so it prevents any changing of the key that we do not want (especially on some publicly exposed readers). Once this is turned off, new user cards can be added into the system only with the USB reader.

6.4.6 User cards with facility code

This option should be available only when dealing with the Wiegand cards.
By enabling this option, Nova will calculate and present the facility code in front of the card ID. Facility code is also considered when calculating access.

6.4.7 Use only last 3 bytes of user card ID

This option is available for Superadmin only.

This option is only available when dealing with the Wiegand cards.
On the system where users are already using the cards, but the facility code is unknown, we can enable this option and when calculating for access, facility code will be ignored.
IMPORTANT! Since FC is ignored, the card ID becomes much shorter and it could happen that multiple users have different FC and the same Card ID – which is legal for Nova, but will report wrong access for 1 person!!! Please make sure that the card IDs are unique to avoid such problems.

7. Scripting and integrations module (804-00x-2100)

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

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

7.1 Writing Python modules

Scripting modules are written in Python programming language and are run on the central:

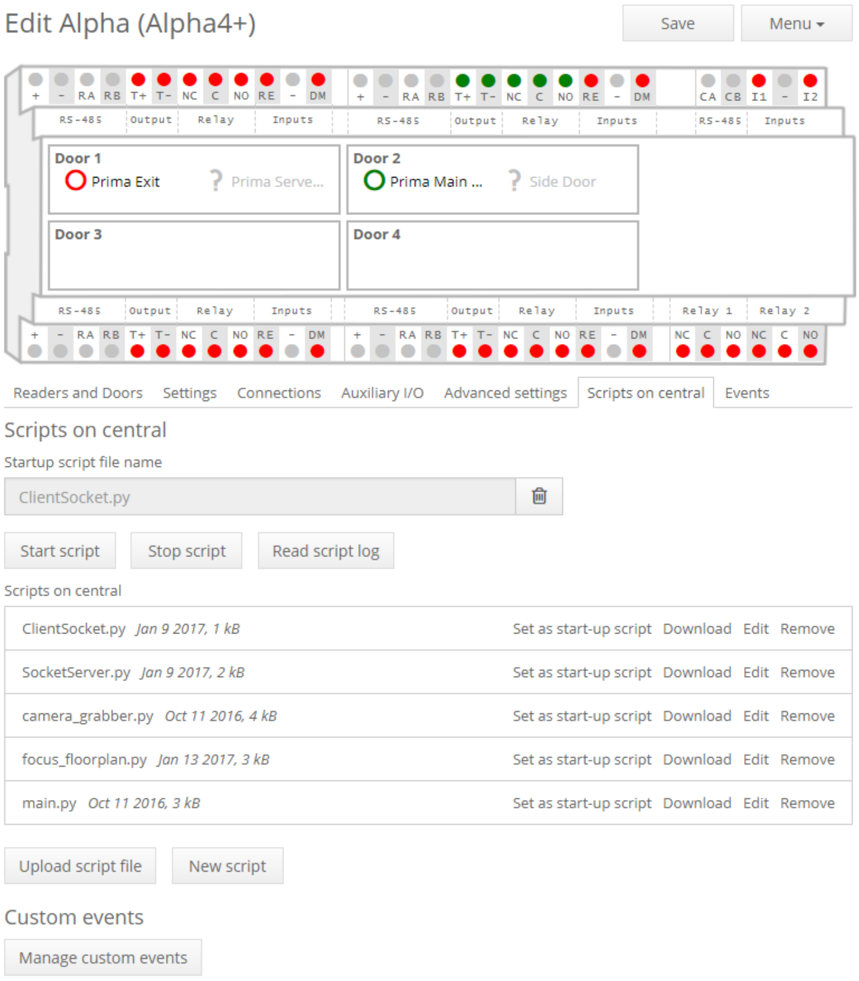
- Which receives events from the system
- Which acts upon events by triggering new events such as:
  - opening multiple doors
  - activating alarm
  - performing other predefined actions

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

7.1.1 Python script installation

EX|FU modules are uploaded to the central in the **Central settings** (Picture 5-9) of the central under the **Scripts on the central** section shown in the picture below. This is found by:

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



Scripts on central

Startup script file name: ClientSocket.py

Scripts on central

ClientSocket.py *Jan 9 2017, 1 kB*	Set as start-up script Download Edit Remove
SocketServer.py *Jan 9 2017, 2 kB*	Set as start-up script Download Edit Remove
camera_grabber.py *Oct 11 2016, 4 kB*	Set as start-up script Download Edit Remove
focus_floorplan.py *Jan 13 2017, 3 kB*	Set as start-up script Download Edit Remove
main.py *Oct 11 2016, 3 kB*	Set as start-up script Download Edit Remove

Picture 7.1: Scripts on a central

Upload a script:

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

The options are:

- **Download -** script from central to a local hard drive.
- **Edit –** allows users to edit the script directly on the central.
- **Remove** script from central.
- **Set script as a start-up script**:
  - A startup script starts together with the central.
  - A startup script file name is listed under the **Startup script file name** field above the list of scripts.
    - This field can only be set through the listed scripts options.

        - To remove the script from this field, click on the trash button next to the file name.

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

To manage a start-up script:

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

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

7.2 Custom events

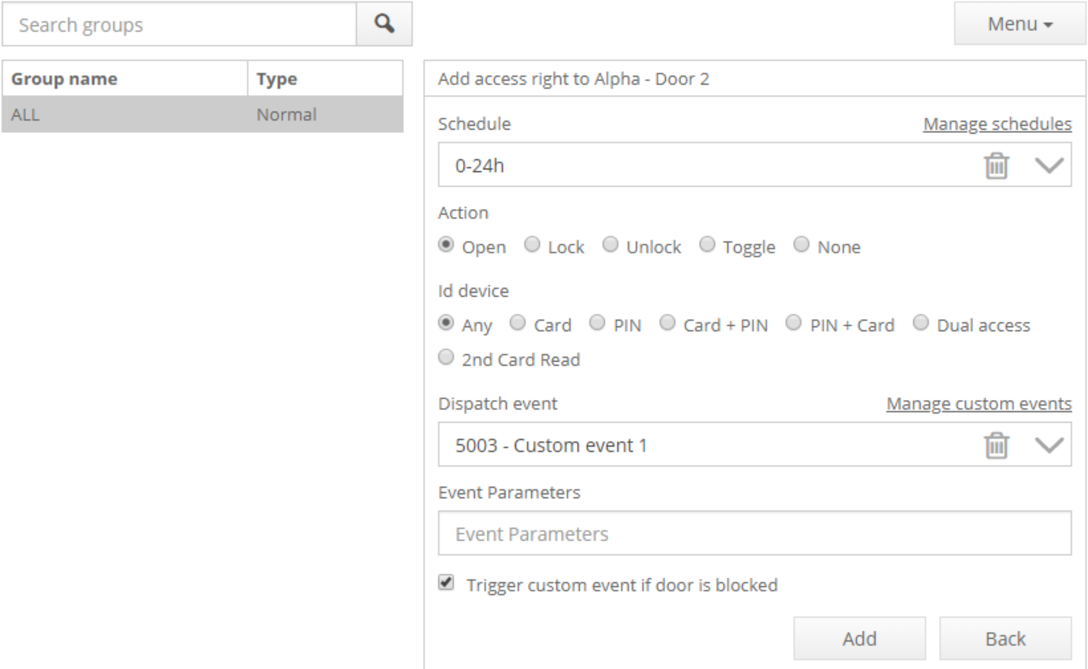
It is possible to add custom events to the Nova system and later dispatch them in the context of user-created events.

7.2.1 Custom events editor

There are two ways to access the **Custom events editor**:

1. Go to Home > Users & Access Rights > Access Groups.
    - Click on the (+) button next to the reader you want to assign a custom event OR click on the pen button for existing rights.
    - Click Manage custom events

2. On master central go to Home > Hardware > Centrals > [master central]> Edit
    - Click tab Scripts on central.
    - Click the button Manage custom events



Group name	Type
ALL	Normal

Add access right to Alpha - Door 2

Schedule — Manage schedules

0-24h

Action

● Open ○ Lock ○ Unlock ○ Toggle ○ None

Id device

● Any ○ Card ○ PIN ○ Card + PIN ○ PIN + Card ○ Dual access ○ 2nd Card Read

Dispatch event — Manage custom events

5003 - Custom event 1

Event Parameters

Event Parameters

☑ Trigger custom event if door is blocked

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

Manage custom events

To open the **Custom events editor**:

- Click the **Manage custom events** text displayed on Picture 7-2.

The menu contains options to:

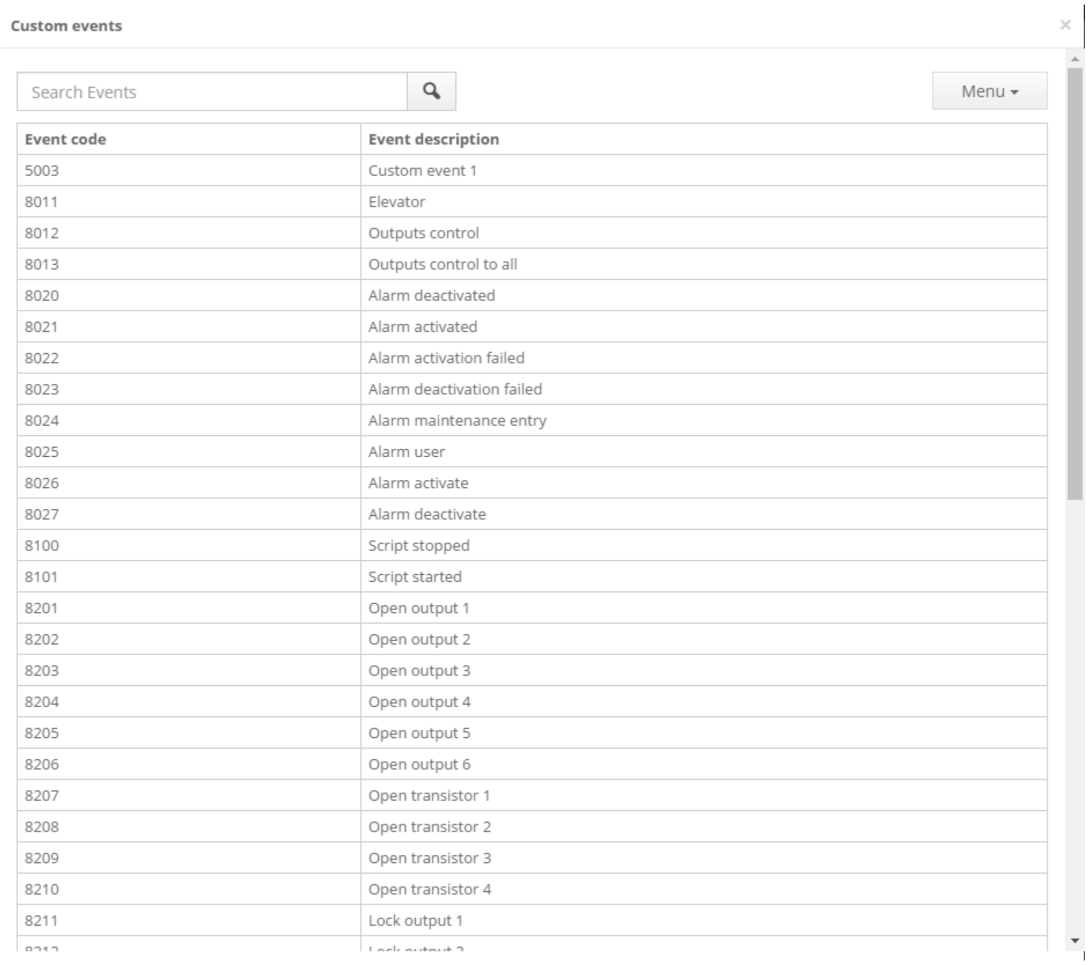
- **Add** user assigned event
- **Edit** an existing event entry (must be selected)
- **Delete** unwanted events (must be selected)

The left panel contains:

- List of all custom event codes in the Nova system

Right panel contains:

- Description of the event codes.



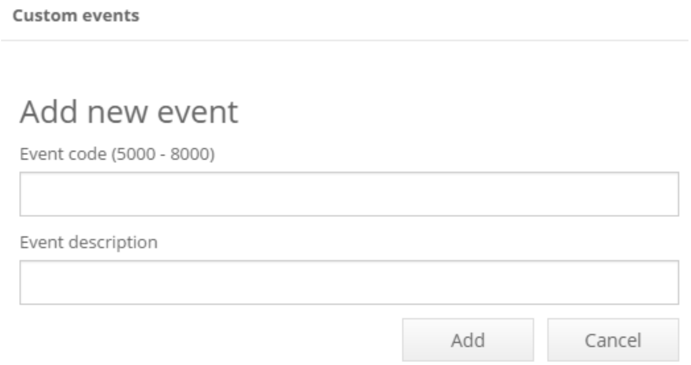
Event code	Event description
5003	Custom event 1
8011	Elevator
8012	Outputs control
8013	Outputs control to all
8020	Alarm deactivated
8021	Alarm activated
8022	Alarm activation failed
8023	Alarm deactivation failed
8024	Alarm maintenance entry
8025	Alarm user
8026	Alarm activate
8027	Alarm deactivate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

Picture 7.3: Manage custom events

7.2.2 Adding a new custom event

To add a new custom event:

1. Click on Menu > Add
   - A new form will open (Picture 7-4)
2. Enter the required **Event code** number (range: 5000-8000)
   - Event code number must be unique
   - Event description must be unique
3. Pressing the **Add** button will add it to custom events lists in custom events editor


Custom events

Add new event

Event code (5000 - 8000)

Event description

Picture 7.4: Add new custom event

7.2.3 Editing and deleting custom events

To **edit** custom events:

- Double click on the event in the events list

OR

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

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

To delete custom events:

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

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

7.2.4 Dispatching/assigning custom events

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

- **Select custom event** from the dropdown list
- **Save** changes
  - Optionally, by providing additional parameters (arbitrary string values) it is possible to add values to the script when the event is dispatched (see Picture 7-2 for the dropdown list with selected event **Alarm ON**).

7.2.5 Built-in events

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

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

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

Event name	Parameters	Description
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 outputs and transistors; 1,2,3:1000 opens output 1,2 and 3 for 1 second, ...
Open output X	[time in milliseconds]	Opens output X for the defined time
Open transistor X	[time in milliseconds]	Opens transistor X for the defined time
Lock output X		Sets output X to a locked state
Lock transistor X		Sets transistor X to a locked state
Unlock output X		Sets output X to unlocked state
Unlock transistor X		Sets transistor X to unlocked state
Toggle output X		Toggles state of output 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 7.3 Simple alarm integration for more information.

Table 7-1: List of built-in events

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

7.3 Simple alarm integration

Alarm integration allows users to:

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

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

7.3.1 System prerequisites and alarm script installation

To enable alarm functionality:

- The scripting activation key is required
  - Please see chapter 6.1 Add-ons and Modules for more information on activation key installation
- Scripts **Alarm.py** and **main_simple_alarm.py** are required on central to control selected alarm zone.
- User with system administrator rights must have the **same authentication credentials** as the ones defined in *main_simple_alarm.py* script
- The default user to log-in is defined in the special user known as the **Scripting module.**

⇨ Install the above-mentioned scripts on central and select **main_simple_alarm.py** as **a startup script**. For more information on how to install scripts on the central, please refer to chapter 7.1.1 EX|FU module installation*.*

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

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

7.3.2 Access group configuration

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

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

1. Create a **new access group** and give it a descriptive name, e.g., Main Door Alarm Activation.
2. **Add a new access definition to the reader** picked to control an alarm zone in the context of the newly created access group.
3. **Select a schedule,** which will define a period for activating an 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 an **alarm deactivation access group**, please follow these steps:

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

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

7.3.3 Activation of alarm

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

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

7.3.4 Deactivation of alarm

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

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

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

- The alarm deactivation request is sent to the alarm central when a card is read for the second time.

- Positive confirmation signal: doors will open, and the reader will beep three times with short OK signal.
  - Event 8020 – Alarm off will be triggered.
- Negative confirmation signal: the reader will beep with a long ERROR signal.
  - Event 8023 – Alarm deactivation failed will be triggered.

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

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

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

7.4 Web services

Web services are used to relay an action to the central using a generated link.
To create a Web service:

1. Navigate to Settings > Integrations > Web services.
2. Click on the Menu button > New.
3. Provide the:
   - Custom **name** of the service
   - **Action**: can be set to **open / unlock / lock / toggle a door** or **arm / disarm an alarm zone**.
   - **Enabled**: will start to work as soon as its created, can be later disabled if you wish to keep the web service in non-working condition.
   - **User:** we can specify which user will be displayed when the action takes place, you can choose one from the drop-down menu or select the **parametric** option, if you wish to provide the optional user ID in the URL.
   - **Hardware:** possible **parametric** option via hardware ID or choose one from the drop-down of hardware devices.
   - **Central:** specifies if the web service will trigger on a specified central or all of them.

7.5 Event triggers

This feature catches set events that immediately trigger a specific action.
To create an event trigger:

1. Navigate to Settings > Integrations > Event triggers.
2. Click on the Menu button > New.
3. Provide:
    - **Title**: name of the trigger.
    - **Type**: type of the event trigger.
    - **Action**: which URL will be called when the event happens.
    - **Enabled**: for quickly enabling/disabling the functionality.
    - **Event**: specify which event will become a trigger.
    - **User**: specify for which user the trigger will happen (you can use **System** for system related events and **Any** for all the users).
    - **Hardware**: specify on which hardware the event will trigger the action (use **Any** for all the hardware).
    - **Central**: you can specify the trigger only to happen on set central.

7.6 API key

For any advanced (local) admin, regular admin or system admin, API key can be generated by navigating to the wanted user and under **Account tab** select **Create API key** button.
This will generate a unique key that can be used to create a permanent GUI session.

User creation example:

https://demo.primacloud.si/bin/sysfcgi.fx?Request=CreateUser&ApiKey=xxxx&UsrName=Janez&UsrLastName=Novak&UsrAccessLevel=5&UsrLoginName=janez.novak@gmail.com&UsrEMail=janez.novak@gmail.com&UsrPhone=0038631360762

The response will return status 0 and newly created User ID.

```
<?xml version="1.0" encoding="UTF-8" ?>
<responses>
<response name="CreateUsers" status="0" message="OK.">
<data>
<UsrID>4</UsrID>
</data>
</response>
</responses>
```

Reading user data
Single user example:

https://demo.primacloud.si/bin/sysfcgi.fx?Request=ReadUsers&ApiKey=xxxx&Range=UsrID&UsrID=4

Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<responses>
<response name="ReadUsers" status="0" message="OK.">
<data>
<user UsrID="4" UsrName="Janez" UsrLastName="Novak" UsrEMail="janez.novak@gmail.com"
UsrOfflineScheduleID="1" UsrLanguage="en_US" UsrAccessLevel="5" UsrValidFrom="2000-01-01
12:00:00" UsrValidTo="2035-01-01 12:00:00" UsrLoginName="janez.novak@gmail.com" />
</data>
</response>
</responses>
```

In case of using the XML API with sending XML via POST, then the header "Session-ID" is replaced with "ApiKey".

Reading multiple users' example

https://demo.primacloud.si/bin/sysfcgi.fx?Request=ReadUsers&ApiKey=xxxx&Range=All-preview

Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<responses>
<response name="ReadUsers" status="0" message="OK.">
<data>
<user UsrID="4" UsrName="Janez" UsrLastName="Novak" UsrEMail="janez.novak@gmail.com"
UsrOfflineScheduleID="1" UsrLanguage="en_US" UsrAccessLevel="5" UsrValidFrom="2000-01-01
12:00:00" UsrValidTo="2035-01-01 12:00:00" UsrLoginName="janez.novak@gmail.com" />
</data>
</response>
</responses>
```

Updating a user:

https://demo.primacloud.si/bin/sysfcgi.fx?Request=UpdateUser&ApiKey=xxxx&UsrID=5&UsrValidFrom=2023-01-01 00:00:00&UsrValidTo=2023-12-31 23:59:59

Deleting a user:

https://demo.primacloud.si/bin/sysfcgi.fx?Request=DeleteUser&ApiKey=xxxx&UsrID=5

7.6.1 Automatic login, page redirects

Some customers require automatic login and redirect to specific page from a single link. Here are the steps:

1. Create an API Key
   Go to users with the admin or sysadmin rights and under tab "Account" find the button called "Create API key". **Scripting or XML module is needed for this!**
2. Create a link with the API Key
   The API Key can now be used for the GUI to use instead of a session id to create a permanent session.
   We can pass it as a GET parameter API Key for the URL navigation and use #place to go to the wanted site.

The URL should look like this:

https(s)://<ip>/app/?ApiKey=<api_key_from_step_1>#<gui_location>

Example:

http://192.168.1.80/app/?ApiKey=0f0a7743-0908-466d-8482-323549a8893c#events

3. Embed to iframe – copy link to the iframe

```
<iframe src="<link>" width=<width> height=<height>></iframe>
```

Example:

```
<iframe src="http://192.168.1.80/app/?ApiKey=0f0a7743-0908-466d-8482-323549a8893c#events" width=1920 height=1080></iframe>
```

The sequence of parameters is important! ?ApiKey must be first and #events should be last.

This is OK:

http://192.168.1.80/app/?ApiKey=0f0a7743-0908-466d-8482-323549a8893c#events

This is NOT OK:

http://192.168.1.80/app/#events?ApiKey=0f0a7743-0908-466d-8482-323549a8893c

8. Door stations module (804-00x-3102/3105/3125)

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

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

1. Enter a valid Door station module activation key (See chapter **6.1** - **Add-ons and Modules** section for help on adding new activation keys)
2. Navigate to **Home > Hardware > Door stations** in the widget menu

8.1 Door station module setup

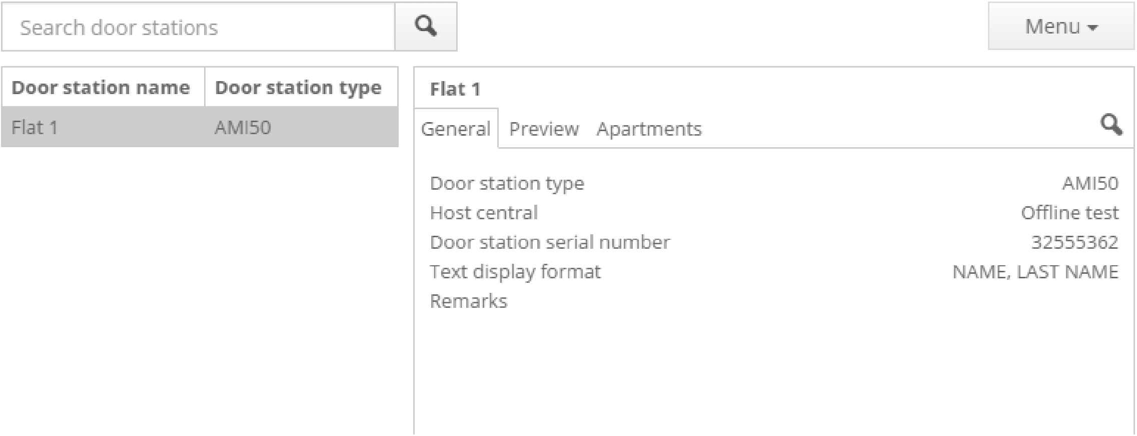
To set-up the Door station module:

1. Import apartments into the Door station module with **Apartments manager**
2. Access **Apartments manager** via widgets **Home > Hardware > Apartments** or directly from the Door-station widget: **Menu > Manage apartments** (Picture 8-1)
3. Insert serial numbers of installed hardware (call button and indoor video station)
   - Serial numbers are required to communicate with apartment hardware
   - For more information, read the **Manage apartments** section
4. Insert serial numbers of door stations
5. Insert names of central connected to door stations
   - See **Adding door stations** section for more information
6. Link apartments and door stations
   - Each door station must-have apartments assigned to show text on the different displays
   - See the **Assigning apartments to door station** section for more information
7. Assign apartments to users
   - This can be accessed through **Users & Access rights** in the Nova main menu
   - Here a user is selected from the list by clicking on **Menu > Edit User [name]**
   - A user profile will show up
   - Select the button **apartment settings**
   - See section **8.5 Assigning apartments to users** for more information

8.2 Door station manager popup window

Picture 8-1 shows the Door station manager:

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



Door station name	Door station type
Flat 1	AMI50

Door station type	AMI50
Host central	Offline test
Door station serial number	32555362
Text display format	NAME, LAST NAME
Remarks	

Picture 8.1: Door station manager popup window

8.3 Managing apartments

Apartments need to be added to the software before they can be assigned to door stations or users.
It is possible to manage the apartments by clicking on the widgets **Home > Hardware > Apartments** or directly from the Door station widget: **Menu > Manage apartments**. This presents the apartment manager (Picture 8-2).

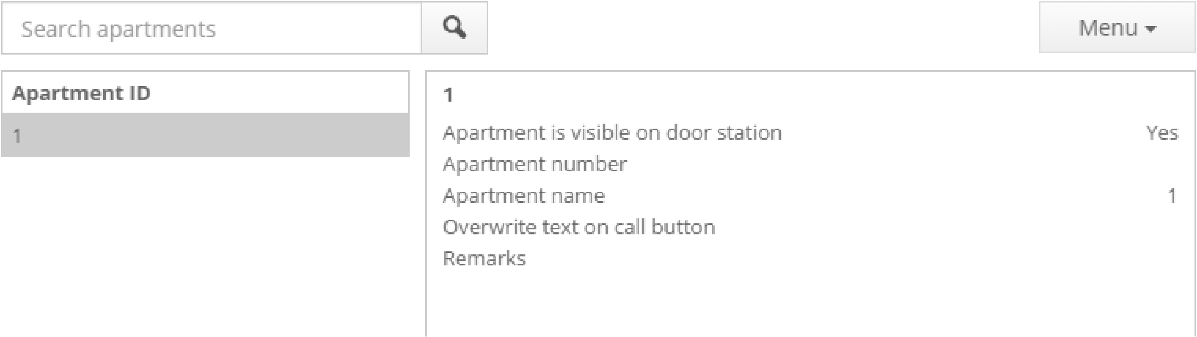
8.3.1 Adding apartments

To add new apartments to the system:

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

Search function:

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



Apartment ID
1

1

Apartment is visible on door station	Yes
Apartment number	
Apartment name	1
Overwrite text on call button	
Remarks	

Picture 8.2: Apartment manager

8.3.2 Editing apartments

To edit an apartment:

- Double-click on the apartment ID in apartment list
- OR select the apartment and click **Menu > Edit [apartment ID]** button
  - The apartment editor (Picture 8-3) will open

How it works:

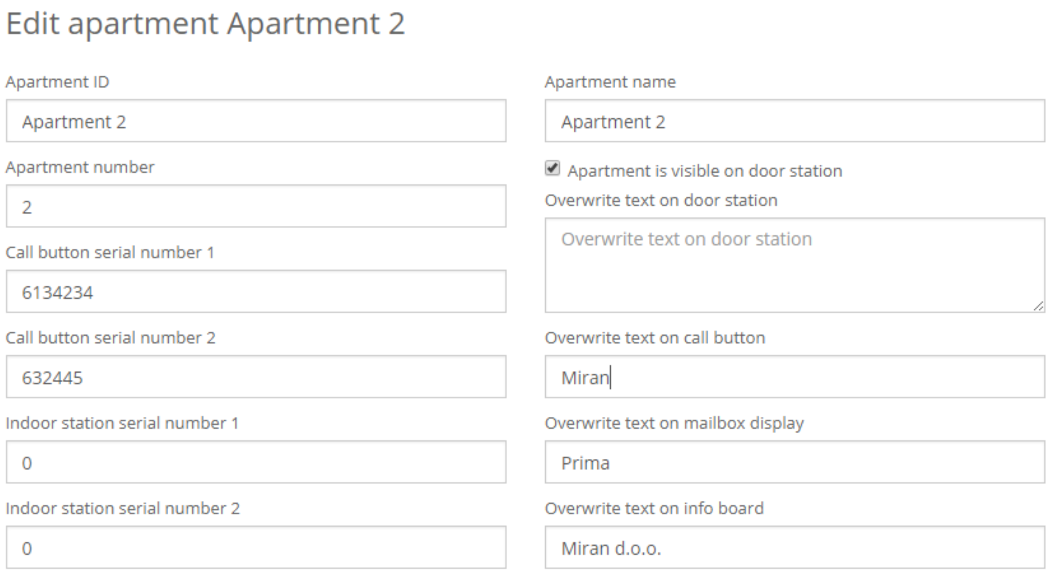
- The hardware components of an apartment (call button and video indoor station) and the Nova software are linked by entering serial numbers of installed hardware into the corresponding input fields in the **Apartment editor**.
- Nova uses serial numbers when relaying information and communicating with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

Important to remember:

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

Door station text and call button:

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



Edit apartment Apartment 2

Apartment ID: Apartment 2

Apartment name: Apartment 2

Apartment number: 2

☑ Apartment is visible on door station

Call button serial number 1: 6134234

Overwrite text on door station: Overwrite text on door station

Call button serial number 2: 632445

Overwrite text on call button: Miran

Indoor station serial number 1: 0

Overwrite text on mailbox display: Prima

Indoor station serial number 2: 0

Overwrite text on info board: Miran d.o.o.

Picture 8.3: Apartment editor

8.3.3 Removing apartments

Apartments can be removed when they are no longer needed, e.g., they are not assigned to any door stations and not assigned to any of the users.
To remove the apartment from the Door station module:

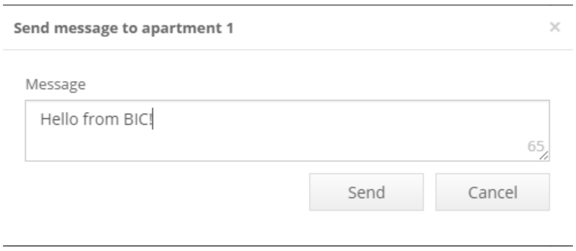
- Click the **Menu > Remove [apartment ID]** button in the **Apartment editor** (Picture 8-2)
    - After removal confirmation, the apartment is removed from the list

8.3.4 Sending messages to apartments

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

To send messages:

1. Select apartment(s) from the apartment list
    - Use the **shift** button (on your keyboard) to select multiple apartments
2. Click on **Send a message to apartment** button (see Picture 8-2; the same button is also present in the apartment editor)
3. Type message into popup window (Picture 8-4)
4. Click on **Send a message to apartment** button



Send message to apartment 1

Message

Hello from BIC!

Picture 8.4: Message input popup window

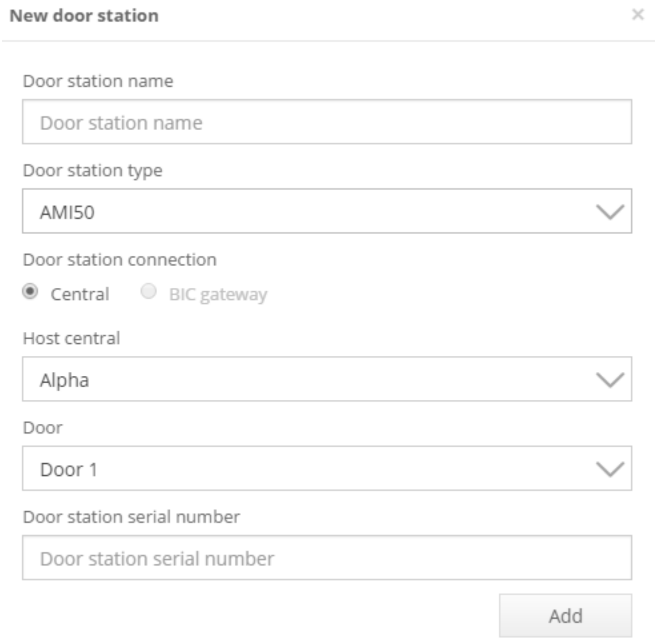
8.4 Door station management

Enter settings for door stations in the door station manager.

8.4.1 Adding door stations

To add door stations:

1. Click the **Menu > New door station** button in the Door station editor
   - This opens popup window (Picture 8-5)
2. Enter the name, serial number, and type for the new door station
3. Select host central and door of selected central that is wired to the door station
4. Save door station by clicking on **Add** button
   - The newly created door station will be added to the door stations list where it can be selected and managed



New door station

Door station name: Door station name

Door station type: AMI50

Door station connection: ● Central ○ BIC gateway

Host central: Alpha

Door: Door 1

Door station serial number: Door station serial number

Picture 8.5: New door station popup window

8.4.2 Editing door stations

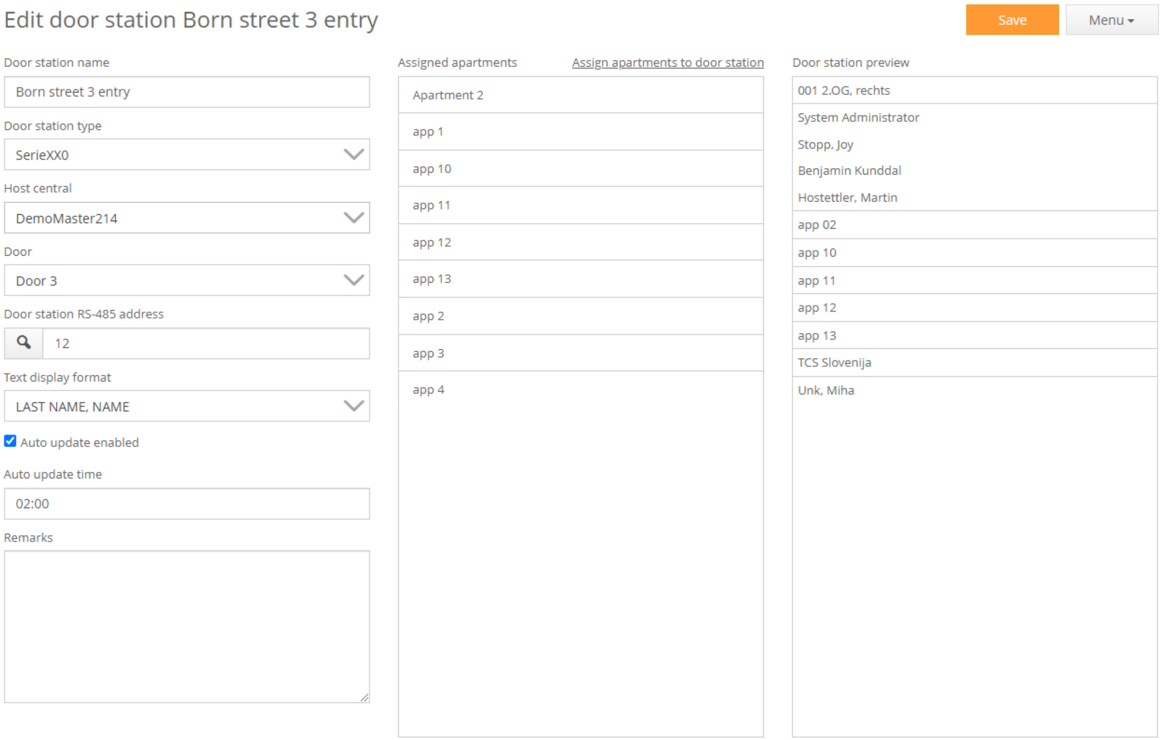
To edit a door station (Picture 8-6):

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

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

- Name
- Type
- Host central
- Host door, that the central is connected to
- Serial number or RS-485 address
- Text display format
- Option to turn on/off auto updates
    - Time when the auto update should be triggered. On the larger systems where they have a lot of door stations, the updates can generate a lot of traffic at once, so it is recommended to pick different update timings.

Remember to save any changes!



Edit door station Born street 3 entry

Door station name: Born street 3 entry

Door station type: SerieXX0

Host central: DemoMaster214

Door: Door 3

Door station RS-485 address: 12

Text display format: LAST NAME, NAME

☑ Auto update enabled

Auto update time: 02:00

Remarks:

Assigned apartments:
Apartment 2
app 1
app 10
app 11
app 12
app 13
app 2
app 3
app 4

Door station preview:
001 2.OG, rechts
System Administrator
Stopp, Joy
Benjamin Kunddal
Hostettler, Martin
app 02
app 10
app 11
app 12
app 13
TCS Slovenija
Unk, Miha

Picture 8.6: Door station editor

8.4.3 Removing door stations

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

To remove a door station:

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

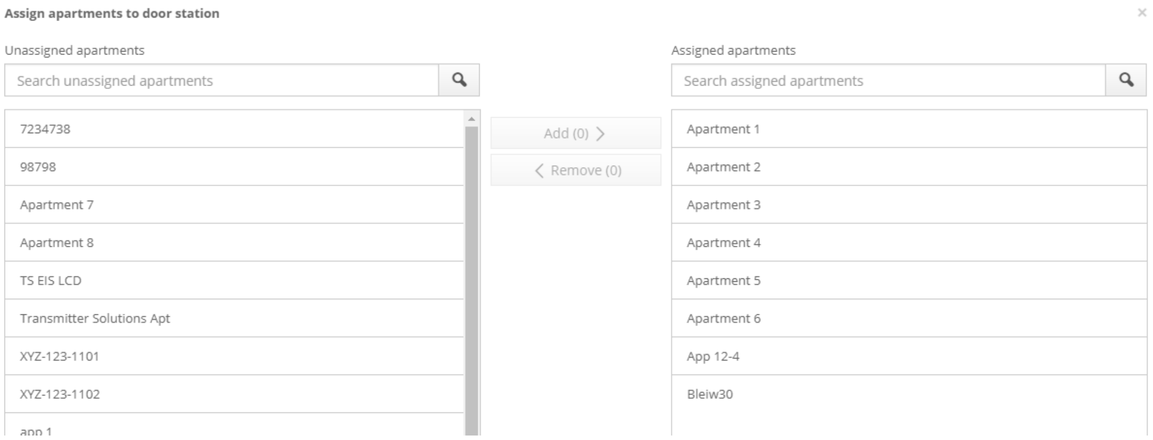
8.4.4 Preview of door station information

Preview of display text on the edited door station is visible in the **Door station preview** tab in the **door station editor.**
It contains the apartments associated with the edited door station, the users that are associated with the apartments, and on the option selected in the **Text display format** drop-down menu.
For more information on the apartment assignment, see section **8.5 Assigning apartments to the users**.

8.4.5 Assigning apartments to door stations

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

- Enter the Door station settings – select the text box **Assign apartments to door station** that is located in the middle column.
    - A new pop-up will appear with a display of all un-assigned apartments noted in the left column and assigned apartments in the right one - see Picture 8-7.



Assign apartments to door station ×

Unassigned apartments

Search unassigned apartments

7234738
98798
Apartment 7
Apartment 8
TS EIS LCD
Transmitter Solutions Apt
XYZ-123-1101
XYZ-123-1102
app 1

Add (0) >
< Remove (0)

Assigned apartments

Search assigned apartments

Apartment 1
Apartment 2
Apartment 3
Apartment 4
Apartment 5
Apartment 6
App 12-4
Bleiw30

Picture 8.7: Assigning apartments to the door station

Assigning apartment(s) to door station:
Start typing the Apartment ID into the search field on the left, and when it is shown in the list, select it and press the Add button. The apartment(s) will be assigned to the door station and will appear in the list of assigned apartments.
Un-assigning apartment(s) from the door station:
Select apartments from the right panel and remove it by pressing the **Remove** button. The apartment (s) will be unassigned from the door station.

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

Search function:

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

8.4.6 Updating content on the door station

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

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

To update content on door station:

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

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

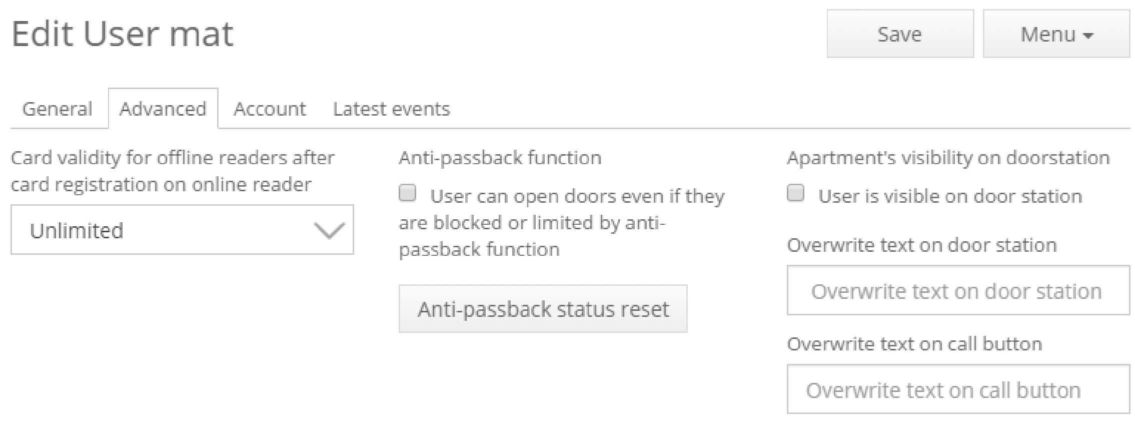
8.5 Assigning apartments to the users

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

To assign apartment settings to a user:

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

8.5.1 Advanced text manipulation


Edit User mat

Card validity for offline readers after card registration on online reader

Unlimited

Anti-passback function

□ User can open doors even if they are blocked or limited by anti-passback function

Apartment's visibility on doorstation

□ User is visible on door station

Overwrite text on door station

Overwrite text on door station

Overwrite text on call button

Overwrite text on call button

Picture 8.8: Advanced apartment settings for a user

Advanced settings for door stations and call buttons

To leave out username from door station:

1. Navigate to the specific user and select its **Advanced** tab like shown in Picture 8-8.
2. Un-check the field User is visible on the door station

To overwrite text on door station or call button:

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

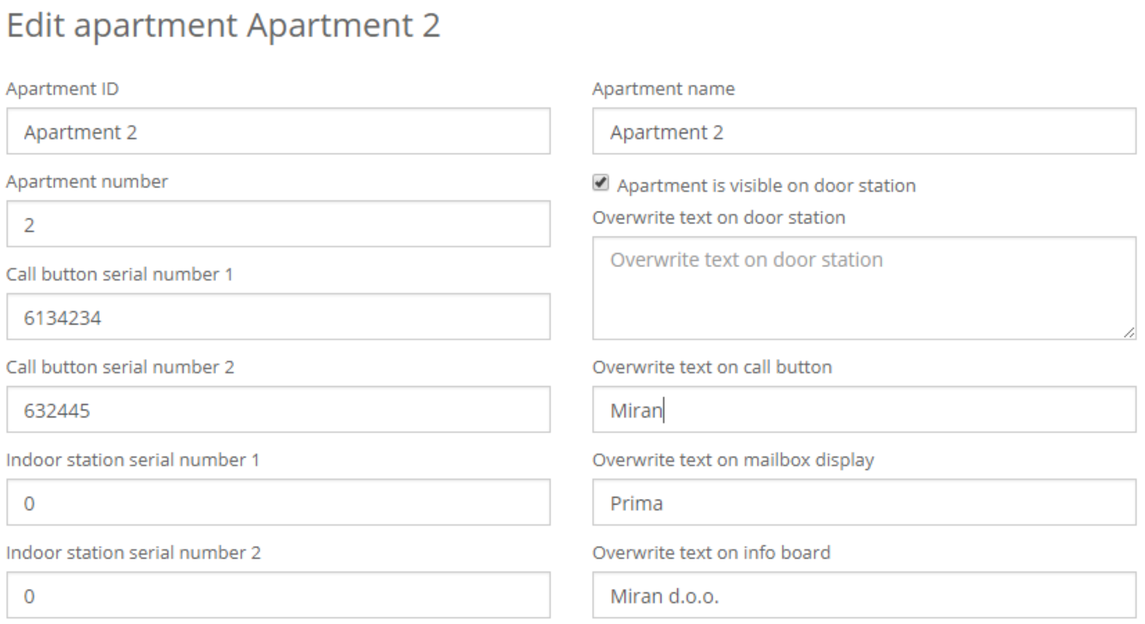
Useful for: Situations where an administrator is administering users but has no privileges to alter the hardware settings.

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

Advanced settings for door mailbox display and info board

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

1. Navigate to **Apartments** widget and access the specific apartment
2. Change the **Overwrite text** entry like shown in Picture 8-9.



Edit apartment Apartment 2

Apartment ID: Apartment 2

Apartment name: Apartment 2

Apartment number: 2

☑ Apartment is visible on door station

Overwrite text on door station: Overwrite text on door station

Call button serial number 1: 6134234

Call button serial number 2: 632445

Overwrite text on call button: Miran

Indoor station serial number 1: 0

Overwrite text on mailbox display: Prima

Indoor station serial number 2: 0

Overwrite text on info board: Miran d.o.o.

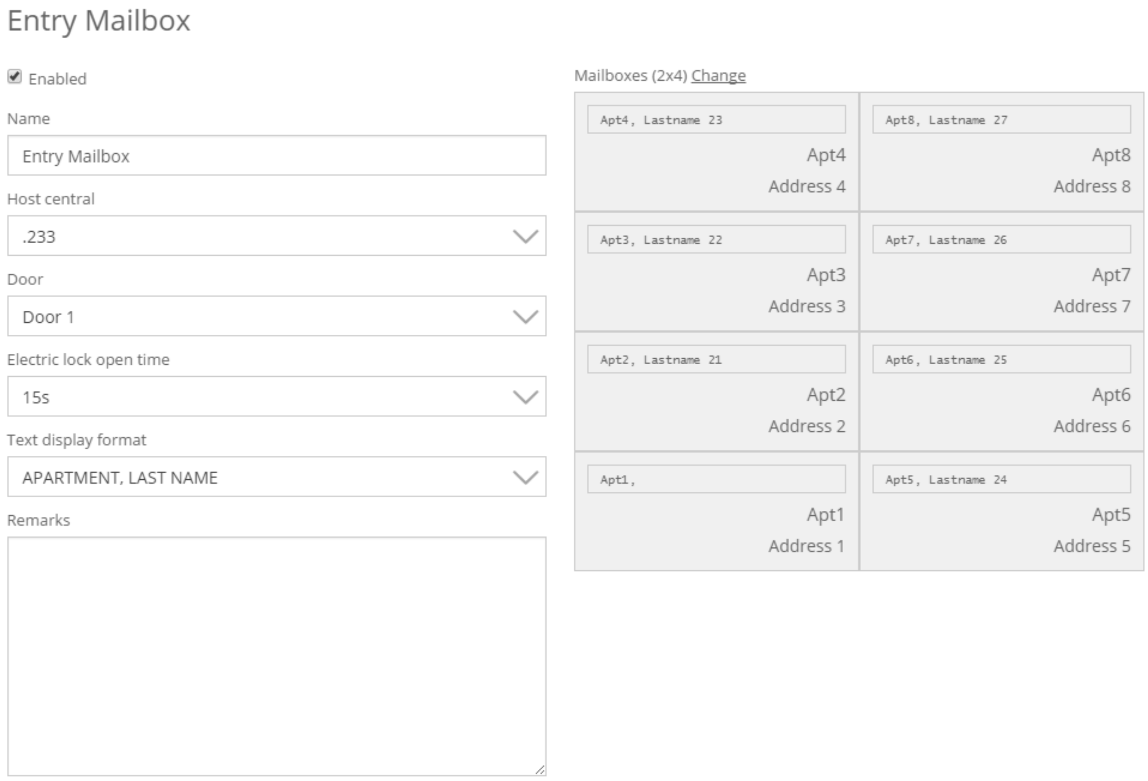
Picture 8.9: Apartment management

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

9. Mailboxes module (804-00x-3132/3135/3155)

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

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



Entry Mailbox

☑ Enabled

Name: Entry Mailbox

Host central: .233

Door: Door 1

Electric lock open time: 15s

Text display format: APARTMENT, LAST NAME

Remarks:

Mailboxes (2x4) Change

Apt4, Lastname 23 Apt4 Address 4	Apt8, Lastname 27 Apt8 Address 8
Apt3, Lastname 22 Apt3 Address 3	Apt7, Lastname 26 Apt7 Address 7
Apt2, Lastname 21 Apt2 Address 2	Apt6, Lastname 25 Apt6 Address 6
Apt1, Apt1 Address 1	Apt5, Lastname 24 Apt5 Address 5

Picture 9.1: Mailbox settings

9.1 Managing mailbox units

To create a mailbox section:

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

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

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

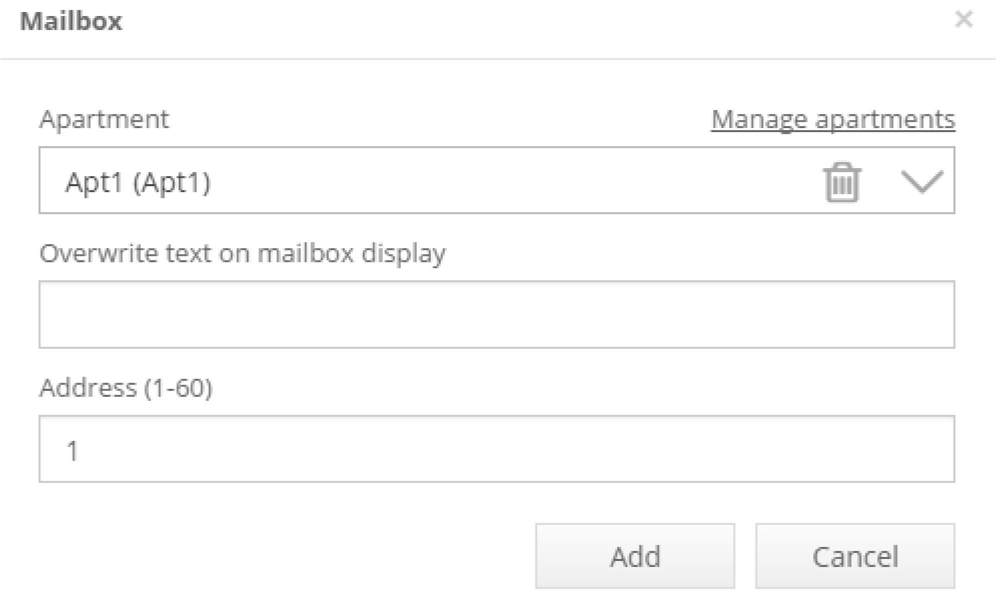
To remove mailbox:

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

9.2 Assigning mailboxes to apartments

Assigning an apartment to the mailbox:

1. Enter the **mailbox** settings by double-clicking on its name found in the list or by clicking **Menu > Edit [mailbox name].**
2. On the right panel, there is a visual presentation of the mailbox with the dimensions provided when created.
3. By clicking on the single entity, a pop-up window displays, asking for **Apartment**, **overwritten text on the display** and the **mailbox address -** Picture 9-2 (displayed on the screen if nothing is sent as a replacement).
4. Once everything is set-up, press the **Add** button.


Mailbox

Apartment: Apt1 (Apt1)

Overwrite text on mailbox display:

Address (1-60): 1

Picture 9.2: Assigning mailboxes to apartments

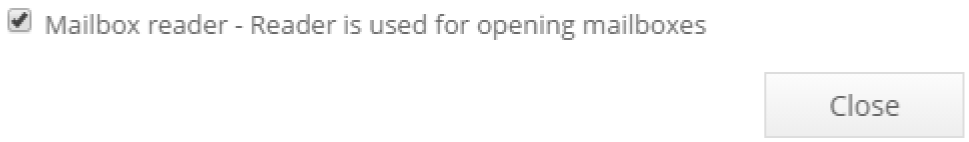
NOTE: The apartment and the mailbox address must be unique for every mailbox unit (can only be assigned to a single entity).

NOTE: The addresses on the old mailboxes varied from 1-64 based on the deep-switches on the mailbox board, while the new mailboxes are automatically numbered starting from addressing 50 to 80 (depending on how many mailbox interfaces there are – 10 addresses per interface).

9.3 Setting the reader to work with the mailbox

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

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

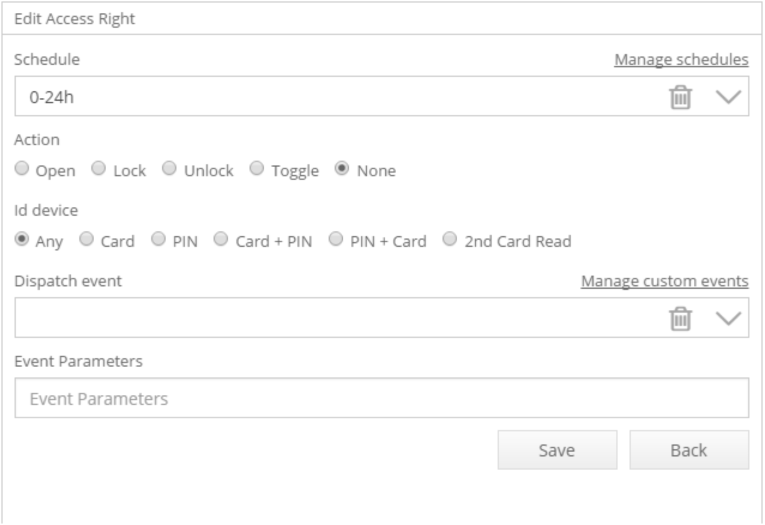


☑ Mailbox reader - Reader is used for opening mailboxes

Picture 9.3:: Assigning the reader for mailbox handling

9.4 Creating and assigning mailbox access rights

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



Edit Access Right

Schedule: 0-24h

Action: ○ Open ○ Lock ○ Unlock ○ Toggle ● None

Id device: ● Any ○ Card ○ PIN ○ Card + PIN ○ PIN + Card ○ 2nd Card Read

Dispatch event:

Event Parameters: Event Parameters

Picture 9.4: Access rights of the mailbox access reader

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

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

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

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

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

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

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

10. Floor plan module (804-00x-4300)

The floor plan module is an overview of the set system. Import your own building blueprint and visually place hardware objects onto it. Moreover, control the set object. **NOTE!** To have a larger overview of the Floor plan, the left menu is automatically hidden. To show it again, just click the down-pointing arrow on the left corner of the screen.

10.1 Managing floor plans

To create a floor plan:

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

If there were some mistakes made during creation, correct them by:

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

To remove the floor plan:

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

10.2 Floor plan hardware

To add items to your floor plan:

- ○ Navigate to the **Hardware** tab on the right panel.
- ○ Press Menu > Add item to the floorplan.
- ○ The software will offer three options to choose from:
  - Reader
  - IP Camera
  - Label
  - Presence
  - Intrusion alarm
  - GPIO

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

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

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

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

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

Adding a **Presence** elements shows the current number of users that have entered a presence location. Presence module must be used to create a presence location that can be then placed on the floor plan.

Adding the **intrusion alarm**; at least 1 alarm zone must be present in Nova. Once placed on the Floor plan we are asked to create a polygon area by clicking over the floorplan location that is covered by the alarm zone. The zone will color green when alarm is disarmed/red when armed. The alarm can be also managed by selecting the Intrusion alarm from the Hardware list, the Arm/Disarm button will show on the top right field.

Inputs and outputs can also be added as objects on the floor plan, each of them has and active/non-active state that can be displayed with a square (like reader) or it can be set as a polygon to represent the specific area.

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

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

- **Camera** tab (displays camera’s picture)

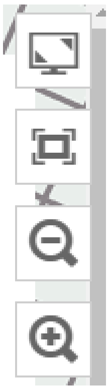
10.3 Floor plan navigation

The navigation on the Floor plan is like navigation on mobile devices. Click and drag to move over different areas of the image. Scrolling in and out will zoom the image (on mobile devices use pinch and stretch gestures to get the same result).
Moving Hardware objects around can be done by clicking on them – a menu will show:

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

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

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



10.4 Floor plan event triggers

Event triggers can be set to display some animation/sound when predefined event happens.

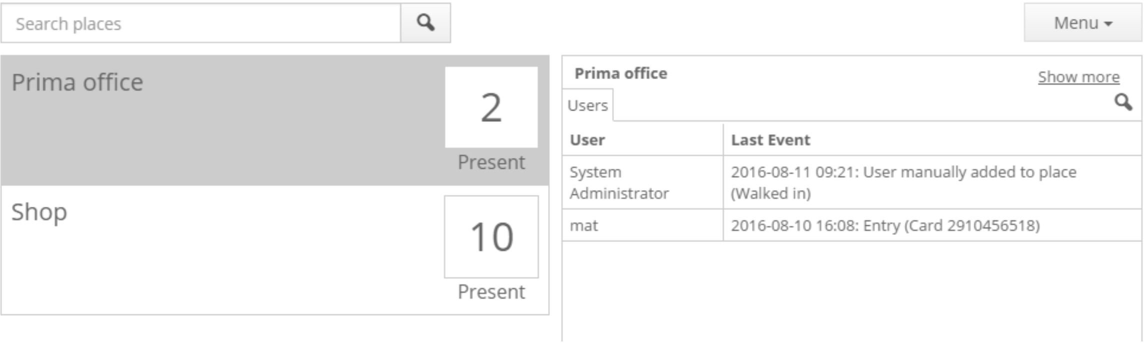
How to create event trigger

1. Navigate to wanted floor plan.
2. Select and click the which hardware you wish to add event trigger to.
3. Select **Menu > Event triggers** (or double click on the hardware item).
4. Select the Menu once again > Add event trigger.
5. Provide the requested data from the pop-up:
    - Event – From the drop-down menu choose which event will trigger the animation.
    - Sound – If selected, it will play the wanted beep sound.
    - Animation – Selecting none will only display the icon in different color, while selecting the blink option will continuously change color every few seconds.
    - Color – When event happens, the icon will be set to the wanted color.
    - Time – How much time the icon will be colored/flashing.
    - Jump to floorplan – If selected, when the evet happens, if any other floor plan is selected, it will immediately switch to this one.

11. Presence module (804-00x-5230)

The presence module is a great way to keep track of how many people enter or exit predefined facilities. Determine people who are still located within the premises with the help of direction set on the readers. Also, if adding the user telephone numbers in the software and connecting a **GSM module** (chapter 5.3.1) to the central, the administrator can send them an SMS with a prompt to answer with a **keyword**. Based on the answer, it is possible to check if they are still inside, otherwise, they will be removed from the group of people listed as present.
This module is activated with the activation key (read about activation keys and how to enter them in chapter **6.1 Add-ons and Modules**).

11.1 Managing presence places



User	Last Event
System Administrator	2016-08-11 09:21: User manually added to place (Walked in)
mat	2016-08-10 16:08: Entry (Card 2910456518)

Picture 11.1: Presence locations

To add a new place:

1. Navigate to Home > Monitoring > Presence.
2. Press Menu > Add a new place.
3. Enter:
    - **Name** of the place.
    - **Hardware list** that includes all readers that belong to that place (read about creating a new Hardware list in chapter **14.1.2 Hardware list**).
    - **User list** – if no user list is provided, all users are included for this presence (how to create a **14.1.1 User list(s)**).
    - **Max users** – the maximum number of users of presence. If the User list is specified, only they will count toward the limit; if the user list is empty, all users will be counted. When the limit is reached, an event of presence full will be triggered. Once one person leaves, another event (freed) will be triggered. The events are helpful for scripting to trigger relays with lights for ex.
    - **Reset at –** Automatically remove people from presence.
    - **Anti-pass back function** – **Error duration** determines how long 2nd entry or exit will be blocked for.
      Allow entry/exit on error will still allow people to pass, but the Anti-pass back error event will still be triggered.

Max allowed time to stay inside – If a user exceeds the set time, he will be marked and unable to exit until its Anti-pass back status has been cleared.

- **Entry keyword** – in case a user telephone number is correctly set up and if the user was not added to the list of present persons, the user can send an SMS with keyword and be added to the list.
- **Exit keyword –** in case someone left the location without registering on the exit reader, it is possible to respond to a warning message by SMS and be removed from this location.
- **Template message** – An SMS template that should explain why the user received this message and how to respond (which keywords to use).

4. Click the **Add** button to create a new presence location.

To edit an existing place:

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

To delete an existing place:

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

11.2 Managing users in places

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

Manually add or remove users from a specific location by:

1. Entering the location by double-clicking on it.
2. User management:
   - To manually add a user to the list (Picture 11-2), click on **Menu > Manually add users**
     - Select the user to add (selecting multiple users can be done by holding Ctrl or Shift key). Press **Add selected (number of users)** and provide a reason when asked in the pop-up window.
   - To remove the user(s) from the list, select them from the list and press **Menu > Manually remove users (number of users)**.

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

- **Hide all** options, turned on by default, and hides users who left.
- **Today's** option displays users who are inside, and users who left in the last 24 hours are displayed in red.

- **Last N days** option displays users who are inside and users who left in the last N days (set in the Location settings).

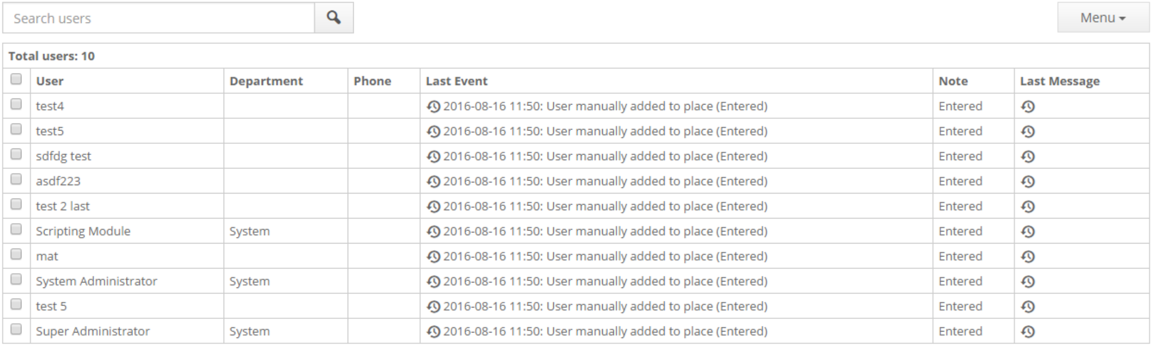
To send an SMS to the user:

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

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

IMPORTANT! If there are two locations and the keyword for one of them is a sub-string from another (ex. "OUT" and "OUTSIDE"), and a user replies "OUT", the user is removed from both locations; but if the user replies "OUTSIDE", it will only be from the single location.

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



Total users: 10

□	User	Department	Phone	Last Event	Note	Last Message
□	test4			↺ 2016-08-16 11:50: User manually added to place (Entered)	Entered	↺
□	test5			↺ 2016-08-16 11:50: User manually added to place (Entered)	Entered	↺
□	sdfdg test			↺ 2016-08-16 11:50: User manually added to place (Entered)	Entered	↺
□	asdf223			↺ 2016-08-16 11:50: User manually added to place (Entered)	Entered	↺
□	test 2 last			↺ 2016-08-16 11:50: User manually added to place (Entered)	Entered	↺
□	Scripting Module	System		↺ 2016-08-16 11:50: User manually added to place (Entered)	Entered	↺
□	mat			↺ 2016-08-16 11:50: User manually added to place (Entered)	Entered	↺
□	System Administrator	System		↺ 2016-08-16 11:50: User manually added to place (Entered)	Entered	↺
□	test 5			↺ 2016-08-16 11:50: User manually added to place (Entered)	Entered	↺
□	Super Administrator	System		↺ 2016-08-16 11:50: User manually added to place (Entered)	Entered	↺

Picture 11.2: Presence user list

11.3 Setting up global Anti pass back

Anti pass back is a function to prevent the cardholders from entering the premises using the same card(s). Access will be granted only to the first person and then if he lends his/her card to some other person, the access will not be granted until the "original" person is checked-out at the Exit reader.

IMPORTANT! The readers need to have the Entry/Exit direction set! The description on setting the reader direction is described in chapter **5.1.15 Reader settings** under Advanced settings.

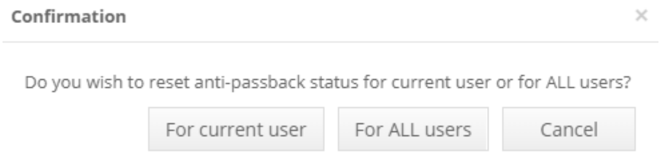
IMPORTANT! Readers must be assigned under a special hardware list. The set-up of those is described in the chapter **14.1.2 Hardware list**.

The user list can also be assigned to the location – this will count the number of the users specified on the user list. This way we can limit the presence max user count for specific presence location.

Once the Anti-pass back function is enabled, there are some additional settings we can set:

- Error duration (in minutes) – the time duration before the user's card is acceptable again. Default 00:00 means that the card will be rejected until the card is set to Exit reader or user's Anti-pass back status has been reset.
- Allow exit on error – the user can always leave (no matter if the card was registered on the Entry reader or not).
- Allow entry on error – The Anti pass back will still be reported in Nova as events but will allow users to enter the location even if the card was already presented to that Entry reader.

IMPORTANT! Status of a single user or a complete status reset can be done by navigating to that user -> Advanced tab and pressing on the Anti pass back status reset button. The options for reset are displayed in Picture 11-3.



Confirmation

Do you wish to reset anti-passback status for current user or for ALL users?

Picture 11.3: Options to reset Anti pass back status

12. Wireless online (804-00x-3032/3040/3055)

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

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

IMPORTANT! Nexus offline does not support this functionality.

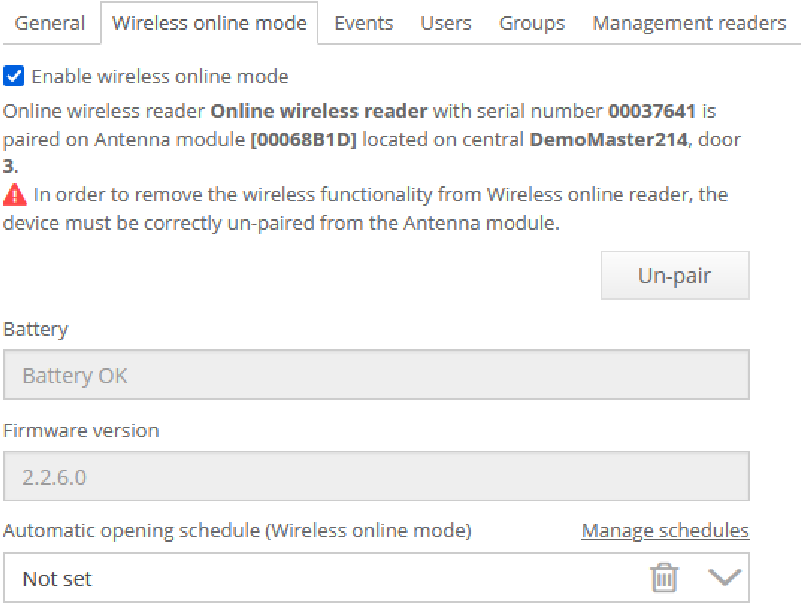
NOTE! Readers connected via wireless online antenna have their times synchronized every time the battery status is requested – at least once per day.

12.1 Offline to online reader conversion

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

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

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



☑ Enable wireless online mode

Online wireless reader **Online wireless reader** with serial number **00037641** is paired on Antenna module **[00068B1D]** located on central **DemoMaster214**, door **3**.

⚠ In order to remove the wireless functionality from Wireless online reader, the device must be correctly un-paired from the Antenna module.

Battery: Battery OK

Firmware version: 2.2.6.0

Automatic opening schedule (Wireless online mode): Not set

Picture 12.1: Wireless online mode

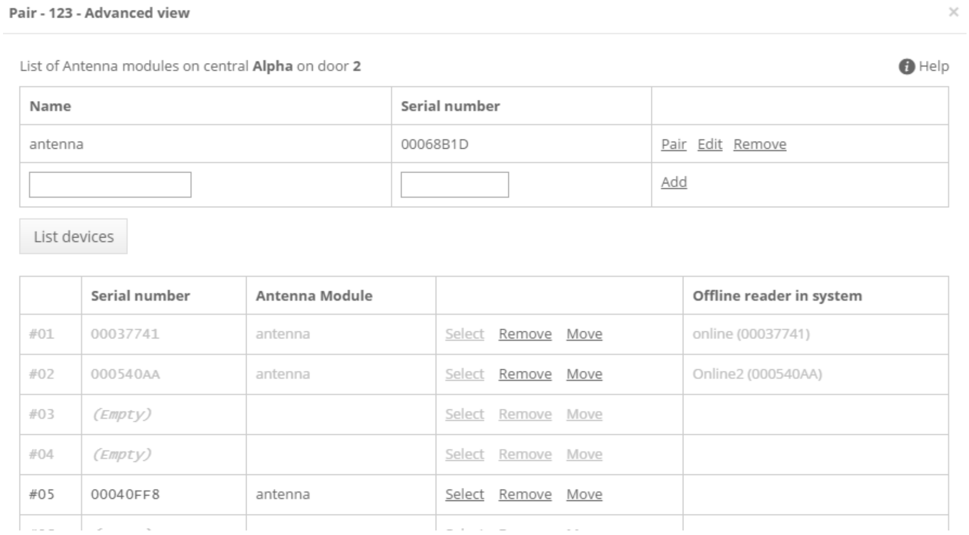
12.1.1 Advanced view

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

Description of columns:

- Wireless offline address (from 1 to 16 for readers via 868 MHz or over Bluetooth).
- The serial number of the Antenna Module.
- Name assigned to the Antenna Module.
- The options to Select, Remove, Move Readers
- The name of the Wireless online reader and its serial number.

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



Pair - 123 - Advanced view

List of Antenna modules on central **Alpha** on door **2**

Name	Serial number	
antenna	00068B1D	Pair Edit Remove
		Add

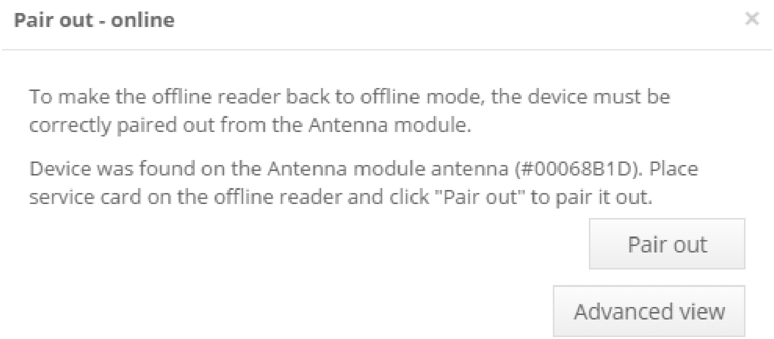
	Serial number	Antenna Module		Offline reader in system
#01	00037741	antenna	Select Remove Move	online (00037741)
#02	000540AA	antenna	Select Remove Move	Online2 (000540AA)
#03	*(Empty)*		Select Remove Move	
#04	*(Empty)*		Select Remove Move	
#05	00040FF8	antenna	Select Remove Move	

Picture 12.2: Wireless online advanced view

12.2 Removing function from wireless online readers

To remove the wireless functionality:

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



Pair out - online

To make the offline reader back to offline mode, the device must be correctly paired out from the Antenna module.

Device was found on the Antenna module antenna (#00068B1D). Place service card on the offline reader and click "Pair out" to pair it out.

Picture 12.3: Wireless online reader pair-out

12.3 Wireless online reader functionalities

Having a reader activated in the system, we can:

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

IMPORTANT! Maximum readers that can be connected to a single Antenna module is 16 if connected via 868 MHz communication or up to 1-8 over Bluetooth.

IMPORTANT! When enabling online schedule, the reader will continuously check status with the antenna every 5th minute (at :00, :05, :10…), so when creating a schedule, match the minutes to start/end on XX:X0 or XX:X5.

Different device types react differently to opening. Cylinder for example, will be set into "unlocked state", but the user will still need to turn it to Un/Lock it; once the schedule ends, it will stay in the last state it was in. **WARNING! If the cylinder remains unlocked, regular user usually does not have toggle capability, so they won't be able to lock it.**
Offline handle will work as expected, when automatic schedule starts, the handle will open and when it ends, it will not open the door anymore unless tag or card is used.

13. Booking module (804-00x-5100)

The booking module is for reservation of the premises at the specified date for a defined time.
The booking activation key must be added to the system as described in **6.1 Add-ons and Modules**.

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

IMPORTANT! The booking can only be set to work with online readers; offline readers work if they are made into online readers using the wireless antenna.

13.1 Booking locations

To create a booking location:

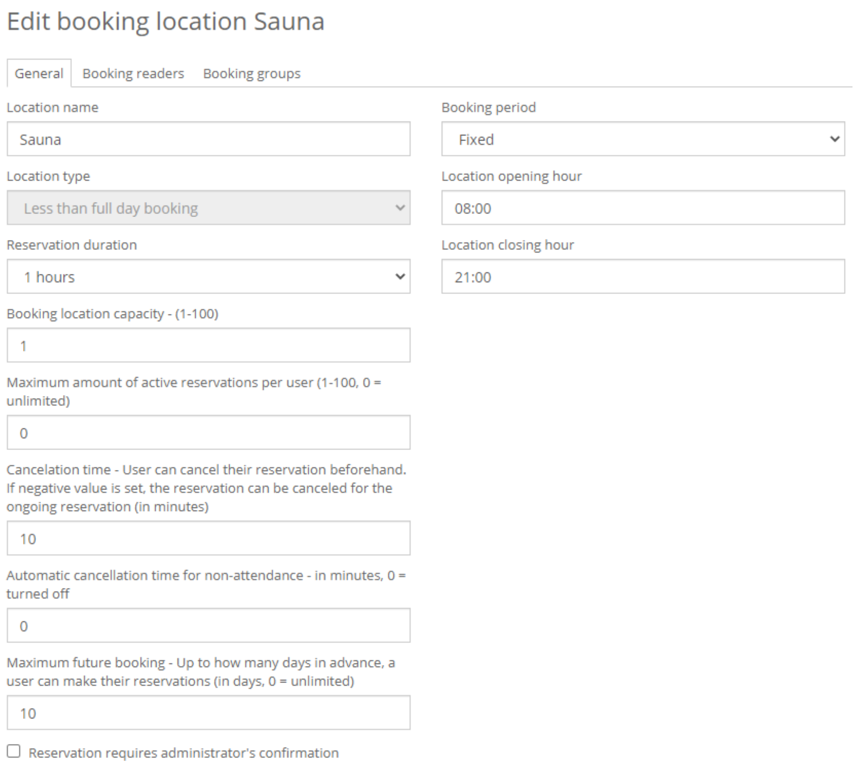
1. Navigate to **Home > Settings > Booking settings**.
2. Click on the **Menu > Add booking location**
   - enter booking location name
   - select location type depending on the location reservation time (daily or short time bookings)
3. Click the **Add** button to create a new booking location.
   NOTE: It is recommended to name according to the booking resource.

Picture 13-1 shows additional parameters that must be filled for each booking location:

- **Reservation duration** – represents the period of how long users can use the premises after claiming the reservation. (Only available for a less than a day booking)
- **Location capacity** – sets the maximum number of reservations per reservation duration. When the limit is reached, the location is marked as full. Further reservations for that duration are not possible.
- **Maximum active reservations per user** – a user will have limited number of active reservations.
- **Maximum invitations** – if enabled (number must be more than 0), means that the user who is creating the reservation is offered other users in Nova to join their reservation.
- **Cancelation time** – defines how much time a user can not cancel the reservation (for example: a user tries to cancel their reservation last minute, he is blocked, because the setting is set to 30 and only allows users to cancel their reservation for 30+ minutes before booking starts).
  If a negative number is provided, a user can cancel an active reservation up to that time (for example: reservation is 1 hour long, cancelation time is set to -30,

which means a user can cancel their reservation early ~ before 30 minutes and allow someone else to take the location, but if one has already been inside for longer than cancelation time, he cannot cancel it in the last half hour).

- **Automatic cancellation time for non-attendance** – When a person books a location and there is no activity on the reader (the booker did not show up) for a set time, the booking will be deleted and free to book for other people.
- **Maximum future booking** – up to how many days in advance a user can create bookings.
- **Reservation requires administrator's confirmation –** a reservation will not be active until administrator confirms it. The request can be sent to email with **Notification module**.
- **Allowed to book –** a user list can be selected for those who can book – for the rest of the users, this option will be greyed out.
- **Period for max bookings –** limits the user to have only N reservations within that week/month (used reservations that week/month also count).
- **Booking period:**
  - **Schedule** – same schedule assignment as for the access groups.
  - **Fixed** – set opening and closing hours for booking location.
- **Reservation notes** – displays a custom message to users who are making the reservations. The message should provide additional guides to users and their reservation (e.g., location of the entrance to the facility, where to park, etc.).
- **Visible to users without reservation rights** – By enabling this checkmark, users that do not have access to this reservation location will be able to check it, but they will not be able to create reservations.
- **Hide names on reservations –** display/hide names or other users that made the reservations.



Edit booking location Sauna

Location name: Sauna

Location type: Less than full day booking

Reservation duration: 1 hours

Booking location capacity - (1-100): 1

Maximum amount of active reservations per user (1-100, 0 = unlimited): 0

Cancelation time - User can cancel their reservation beforehand. If negative value is set, the reservation can be canceled for the ongoing reservation (in minutes): 10

Automatic cancellation time for non-attendance - in minutes, 0 = turned off: 0

Maximum future booking - Up to how many days in advance, a user can make their reservations (in days, 0 = unlimited): 10

☐ Reservation requires administrator's confirmation

Booking period: Fixed

Location opening hour: 08:00

Location closing hour: 21:00

Picture 13.1: Adding a new booking location

Picture 13-1 shows an example of:

- New Booking access for "Sauna" that opens at 8 a.m. and closes at 9 p.m.
- Each user can make a reservation for 1 hour.

13.2 Booking reader(s)

Assigning the reader to the booking location:

- Each booking location can be associated with one or multiple readers in the Nova software.
- To assign it, navigate to booking location's **Booking readers** tab and press **Menu > Add a booking reader**.
- Assigning the:
  - **Hardware** – select a reader you wish to connect to this booking.
  - **Schedule** – this is used if you wish to limit the access further (for example: a room is booked for 23 hours, 1 hour is reserved for housekeeping).
  - **Action** – what will happen to the door when the user will put their card on the reader
  - **ID device**
  - **Allow access before reservation**
  - **Allow access after reservation**
  - **Block if booked**
  - **2nd card read to end the active reservation**
  - **Automatically lock the door when the reservation ends**

  - Custom events data (displayed only if the scripting license is present in the system)

13.3 Booking groups

Assigning different booking locations into a Booking group is beneficial because they can be displayed together and some of the common settings can be applied to the whole group.

How to create/add booking locations to group:

1. Navigate to **Home > Settings > Booking settings.**
2. Select one or more booking locations and press **Menu > Add selected to group.**
3. To add them, provide a group name or select an existing group.

To display a list of booking groups, navigate to **Home > Settings > Booking settings** and select **Menu > Booking groups.**

How to show/remove booking location from group:

1. At least 1 Booking location must be present.
2. Navigate to filter button (near the search field)
3. Select the wanted group and press **Apply**.
4. Only locations that are in the group will be displayed.
5. To remove the booking location from the group, check it and press **Menu > Remove selected from group.**
6. To return to all previews, navigate to the filter button, un-select the group checkmark and **apply**.

How to display booking group:

1. Navigate to **Home > Booking**.
2. From the dropdown select the booking group.

How to embed/create a URL for single booking location:

1. Navigate to **Home > Settings > Booking.**
2. Select the wanted booking location.
3. Press **Menu > <embed/>**
4. Select the:
   - **Title** if you wish to be displayed
   - **Time controls** enables interaction of displaying different weeks/days.
   - **Login controls** enables the users to log-in either with username and password or a card (in this case, the login reader will need to be specified and the user must have access to this reader).
5. The option to generate URL or embed code (for web page integration).

Booking language can be set with the lang param for example:
https://demo.primacloud.si/app/booking/index.html?location=172&lang=en_US

13.4 Reservation creation and cancellation

After the booking was set-up, it can be accessed with a web browser on address:

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

- Under **Booking settings**, booking locations embed code can be generated
  - ⇨ For single booking – select it and press **Menu > Embed** and select the requested fields.
  - ⇨ For multiple bookings – select the filter icon and select a booking group from the dropdown menu and apply the filter. After selecting all booking locations, press **Menu > Embed** and select the wanted parameters.

NOTE: For basic reservations on behalf of other users, use an administrator type of account for creating or canceling the existing reservations.

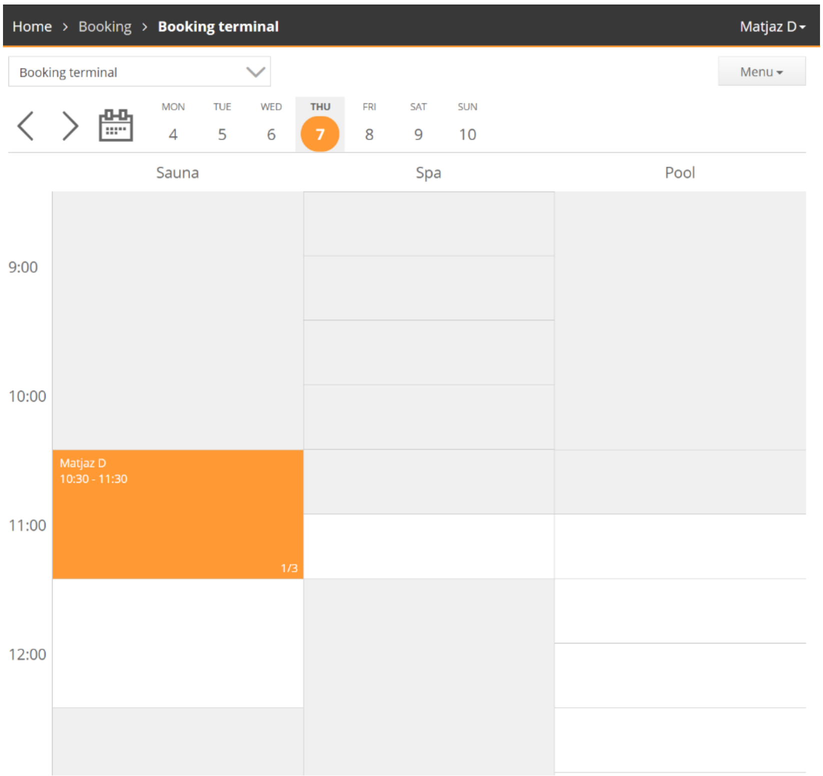
Example in Picture 13.2 shows:

- A calendar page of the Booking application where the resources are listed in the top left corner.
- Currently, the location is set to Sauna as added in the previous example:
  - Switch locations by clicking on the name and selecting the other location from the list.
  - The calendar is set by days, marking the current day in a darker gray color. Reservation times are separated depending on the" Default reservation duration" set (Picture 13-1).
  - The buttons on the top right above the grid are used for switching between different weeks.
  - The middle button resets the overview of the current week.

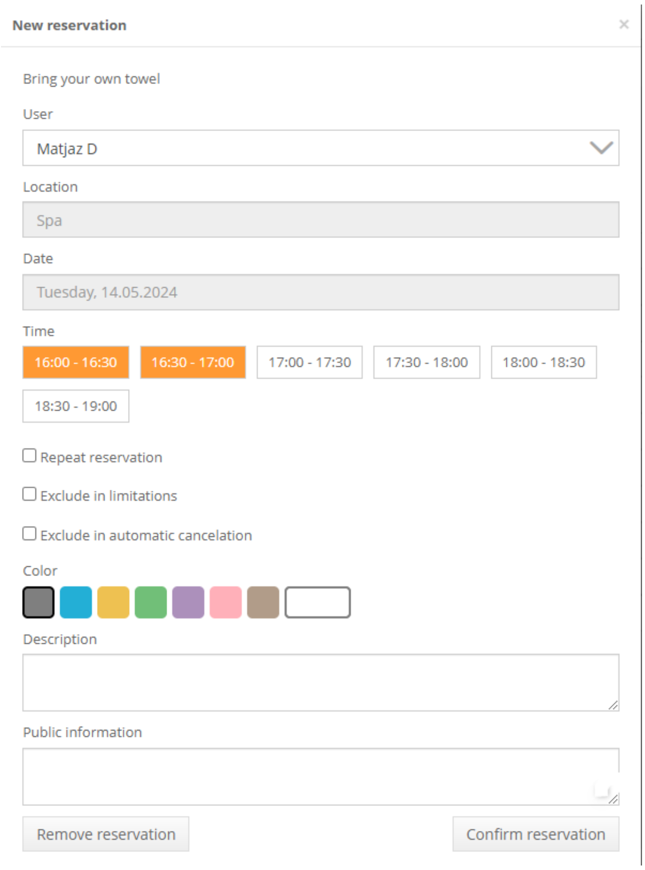
Creating a new reservation

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

- Click the **Confirm reservation** button to confirm the reservation (Picture 13-3)



Picture 13.2: Calendar page of Booking module



New reservation

Bring your own towel

User

Matjaz D

Location

Spa

Date

Tuesday, 14.05.2024

Time

16:00 - 16:30 | 16:30 - 17:00 | 17:00 - 17:30 | 17:30 - 18:00 | 18:00 - 18:30 | 18:30 - 19:00

□ Repeat reservation

□ Exclude in limitations

□ Exclude in automatic cancelation

Color

Description

Public information

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

- It is only possible to make reservations in the future and not for elapsed time. The **Confirm reservation** window has previously set reservations grayed out and they cannot be selected.

- Click the **Cancel reservation** button to cancel the reservation selected in the calendar.

Navigation over calendar can be done with the arrows on the top left, daily calendar will then switch to one week ahead, while monthly jumps to a new month.
Navigation can also be done with date picker by clicking/tapping on the calendar icon.

Different booking locations/groups can be selected from the drop-down menu on the left top side.
NOTE: If the location is greyed out, the user is not included in the user list that has access to this booking site.

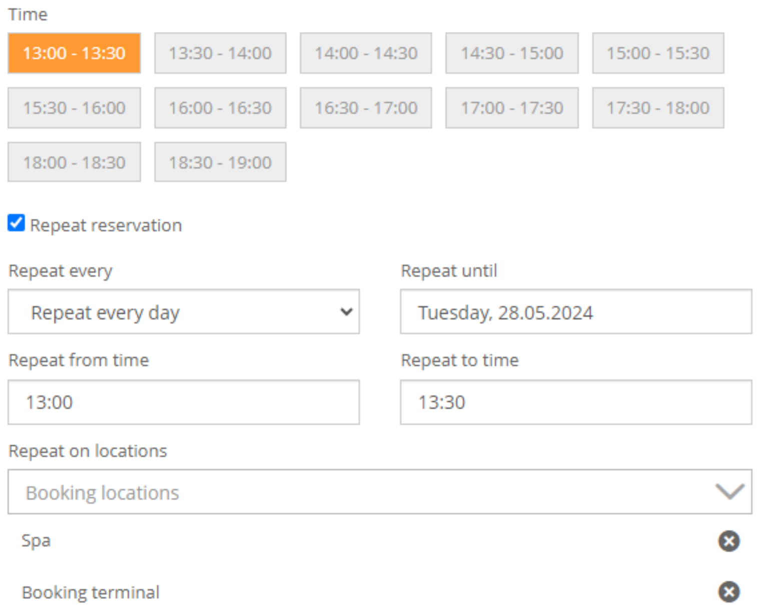
Default color scheme:

- White square – free to book.
- Light grey – booking not available at that time or expired.
- Orange square – user's own reservation.
- White square with dark grey side border – the location was already booked, but it accepts multiple reservations (and it is not yet full).
- Dark grey – booking location is full.

13.4.1 Reoccurring reservations

In some cases, users want to have a repeating reservation for every week/month. It must be done by admin/sysadmin for specific user.

1. Navigate to booking location and open the wanted term.
2. Select the **Repeat reservation** checkmark which will extend the option with repetition options (every day, every week, every other week, every month on set date)
   - date limit until the reservation should last,
   - list of other bookings where this should also be applied.



Time

13:00 - 13:30 | 13:30 - 14:00 | 14:00 - 14:30 | 14:30 - 15:00 | 15:00 - 15:30
15:30 - 16:00 | 16:00 - 16:30 | 16:30 - 17:00 | 17:00 - 17:30 | 17:30 - 18:00
18:00 - 18:30 | 18:30 - 19:00

☑ Repeat reservation

Repeat every: Repeat every day

Repeat until: Tuesday, 28.05.2024

Repeat from time: 13:00

Repeat to time: 13:30

Repeat on locations: Booking locations

Spa ⊗

Booking terminal ⊗

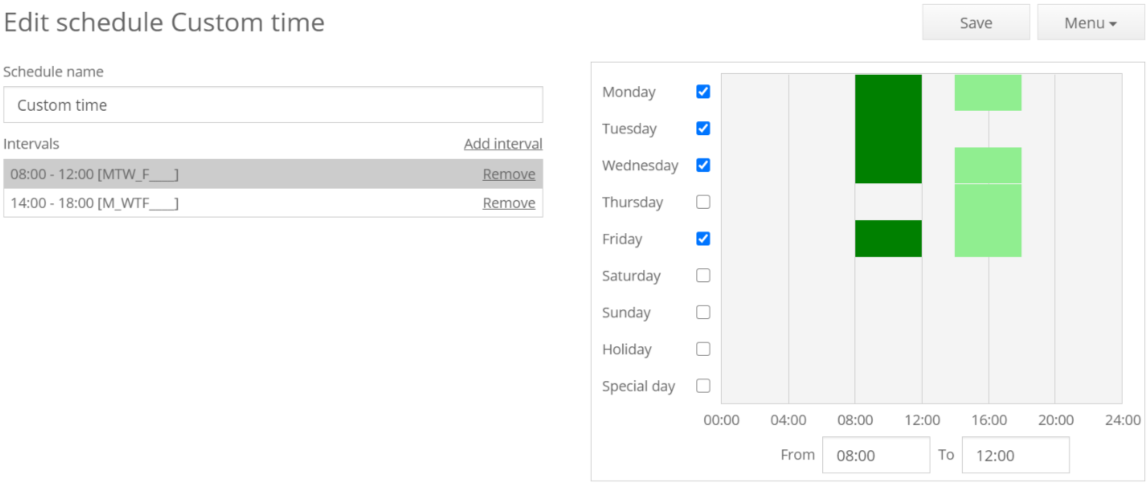
Picture 13.4: Setup of reoccurring reservations

13.4.2 Custom time slots

Booking slots can differ based on the time of the day and even for different days (for ex., reservation for a booked room in the morning can last longer than the reservation made for the afternoon).

To create a custom time slot:

1. Navigate to **Booking settings** and select or create a new booking you wish to assign custom time slots to.
2. Under **Booking period**, you can select a **fixed schedule** or a **standard schedule** for more flexibility.
3. Reservation duration should be set to **Custom**.
4. The custom fields should fit the same schedule.
   For example: In the morning we have a 4-hour slot from 0800 to 1200 and in the afternoon, we have another 4-hour slot from 1400 until 1800. On Tuesday the booking will not be available in the afternoon hours, on Thursday, the booking will not be available in the morning.



Edit schedule Custom time

Schedule name

Custom time

Intervals

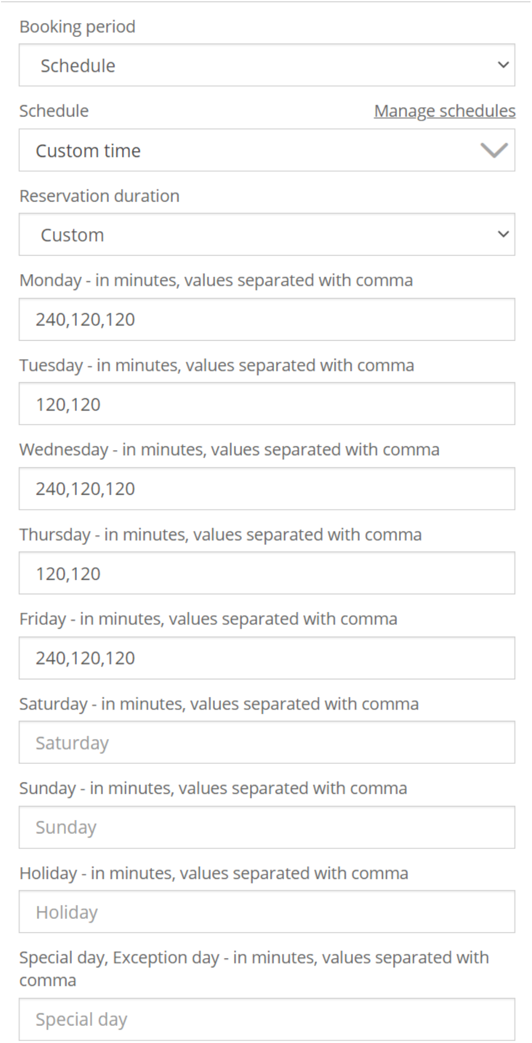
08:00 - 12:00 [MTW_F___] Remove

14:00 - 18:00 [M_WTF___] Remove

Monday	☑
Tuesday	☑
Wednesday	☑
Thursday	□
Friday	☑
Saturday	□
Sunday	□
Holiday	□
Special day	□

From 08:00 To 12:00

5. On the custom fields we need to match the reservation length.
   For the above example: On Monday, we have 4-hour (240 minutes) reservation in the morning, and 2x 120 minutes in the afternoon, while on Tuesday we have 2x 120 minutes in the morning.



Booking period

Schedule

Schedule

Custom time

Reservation duration

Custom

Monday - in minutes, values separated with comma

240,120,120

Tuesday - in minutes, values separated with comma

120,120

Wednesday - in minutes, values separated with comma

240,120,120

Thursday - in minutes, values separated with comma

120,120

Friday - in minutes, values separated with comma

240,120,120

Saturday - in minutes, values separated with comma

Saturday

Sunday - in minutes, values separated with comma

Sunday

Holiday - in minutes, values separated with comma

Holiday

Special day, Exception day - in minutes, values separated with comma

Special day

Holidays, Special days, and Exception days still apply!

13.5 Booking rules

These settings apply stricter rules to the existing booking environment.
To add a new booking rule, navigate to **Hardware > Booking > Booking rules** and **Menu > New rule.**
A new popup will show with the next options:

- **User list** – By default the rule will apply for everyone, but you can select a list of users this rule will apply to.
- **Booking** - To which booking location this rule will apply.
- **Parameter** – different options to choose from:
  - **Reservation window period: (Everyday reservation)** you can specify a time window a user can make a reservation. **(Next day reservation)** Users will be allowed to create a reservation within a set time for the next day.
  - **Reservation duration**: You can specify the shortest and the longest time for each reservation.
  - **Period for max booking:** Specify how many reservations a user can create per day/week/month.
  - **Time limitation**: A user can create reservation(s) until the set time is all used up.
  - **Maximum future booking**: How long in advance a user can create reservation.
  - **Book before:** Sets a limitation on how early a user can book a location. For ex. If set to 30, a user can create a reservation no more than 30 minutes before the reservation begins; If set to -30 means that it can create a reservation even if the reservation up to 30 min into reservation slot (if free).
  - **Default reservation color**: The reservation of users will be displayed in specified color code.
  - **Reservation color of logged user**: You can specify the what color reservation a user will make/see.
  - **Reservation color of available slot**: Specify the color of free to reserve slots.
  - **Maximum amount of active reservation per user**: A limitation of how many reservations a user can make.
  - **Maximum amount of concurrent reservation per user**: How many reservations a user can make at the same time. (For ex. If set to 1 on booking group of 2 location, a user can make a reservation at 13:00 for one location but not the other.)
  - **Token requirement:** Specify which/how many token(s) will be used for the reservation.
  - **Instant booking:** Is used for booking location reservation and its reservation does not count into other daily/weekly rules.
    - Time window for reservation must be defined,
    - maximum amount of active reservation a user can make has to be defined,

    - the minimum/maximum reservation duration.

    (For ex. Teachers can reserve the lecture hall if they see that it is free)
- **New reservation email:** When the customer creates a reservation, they will get an email with reservation details.
    - Reservation can be also sent to Google calendar (and similar).
- **Reservation updated email:** When the customer's reservation is postponed or moved, they will receive a new email with the updated data.
- **Reservation cancelation email:** When the customer's reservation is canceled, they will be notified with an email.
    - Reservation can be also sent to Google calendar (and similar).

Booking levels – the default is main level and if the first rule fails, it will check for the next level rules etc. Example:
Rule 1 (Main level): Requires 10 'X' tokens. If you do not have enough, the system moves to Level 1.
Rule 2 (Level 1): Requires 1 'Y' token.
Effect: If you run out of 'X' tokens, you will be required to use 'Y' tokens instead.

13.6 Booking closing times

Scheduled maintenance for our facilities can be arranged in advance, allowing us to proactively display when bookings are unavailable during these periods.

13.6.1 Ignoring the booking rules

Some customers wish for some reservation to not follow the regular rules. So, we can make some exceptions to the reservation:

- Open the reservation as admin/sysadmin,

From the reservation you can select:

- **Exclude in limitations** – the reservation will ignore any rules applied to this booking location or this user.
- **Exclude in automatic cancelation** – this will make sure that even if the rule for automatic cancelation is applied, this reservation will remain.

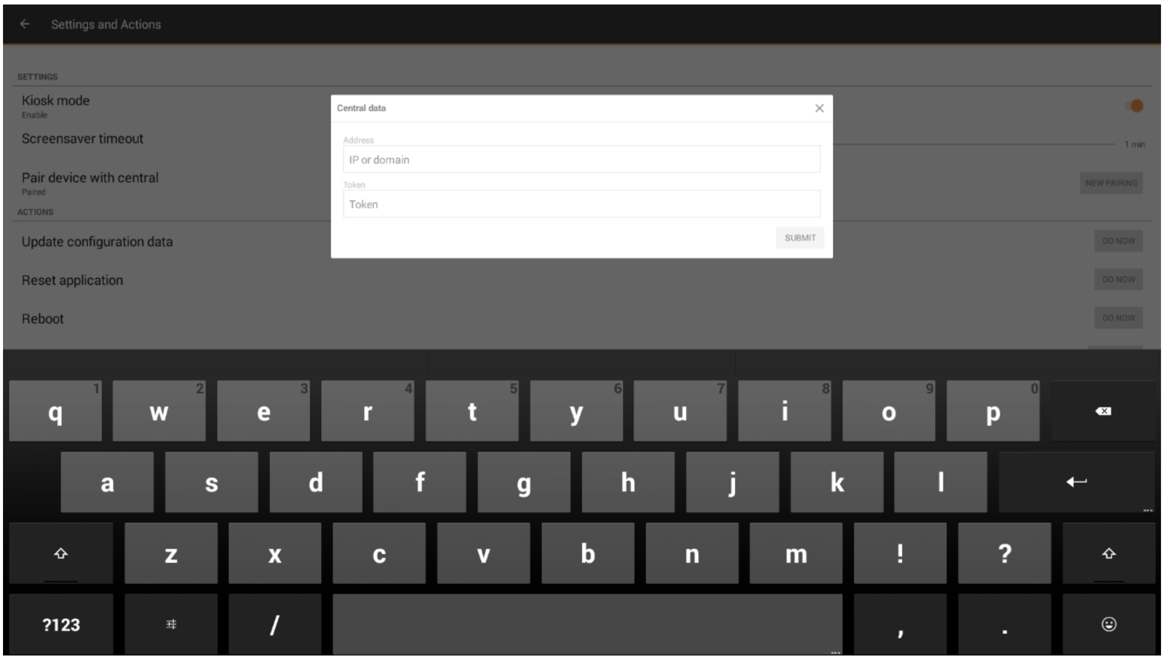
13.7 Booking as a terminal application

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

13.7.1 How to pair a booking terminal

To pair a terminal:

1. Start the **Booking** application on the terminal.
2. Drag two fingers on the top bar from right to left for at least two seconds.
3. A pop-up will show up asking for a password, enter the password 267267.
4. In Nova navigate to **Home > Hardware > Info Boards** and add a new device **– Make sure that you are adding version 2.**
5. From the right column click on the **Generate new token** button and remember it.
6. Go back to the terminal, press the cogwheel button, and then press the **pair device** button.
7. A pop-up will show requesting the DNS/IP of the central and the token generated at step 5.



Settings and Actions

SETTINGS

Kiosk mode
Enable

Screensaver timeout 1 min

Pair device with central
Paired

ACTIONS

Update configuration data

Reset application

Reboot

Central data

Address: IP or domain

Token: Token

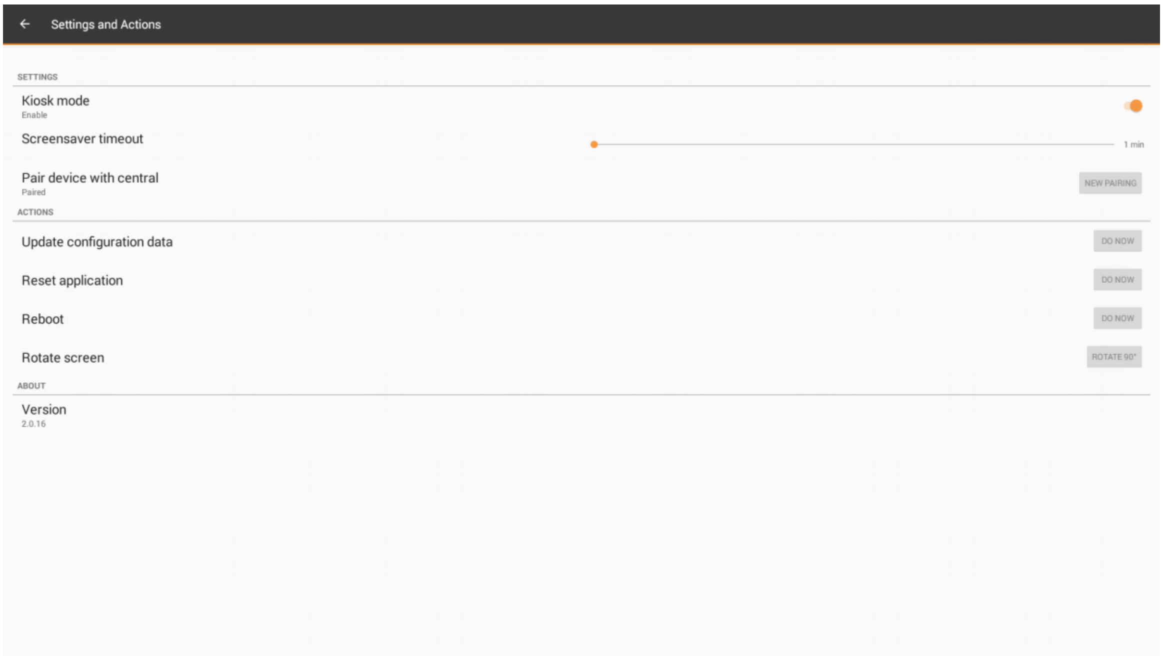
Picture 13.5: A token needs to be generated in Nova to pair the device

13.7.2 Booking terminal settings

After the password has been entered, the installer can set-up various settings that can be found in the app's settings.

Kiosk mode - unlock it if you wish to gain access to the android settings beyond this application. Once it is locked, standard users should not get access to it.
Screen saver timeout – The display can handle "Active" and "Screen saver" lists to turn off (display black) or display a completely different layout after set timeout. The time is counted from the lastly touched display.
Pairing the device with the central – this step pairs the Nova and the terminal's application together. To learn more about it, please read a previous chapter.

Update configuration data - used for application upgrade.
Reset application – Warning! This deletes all the data made in the app. The pairing must be done again. Used if booking tablet is moved or used elsewhere.
Reboot – This will reboot the device.
Rotate screen – Used if the screen is mounted in portrait mode or upside down.
Version – displays a current version of the application installed on the device.



Settings and Actions

SETTINGS

Kiosk mode
Enable

Screensaver timeout
1 min

Pair device with central
Paired

ACTIONS

Update configuration data

Reset application

Reboot

Rotate screen

ABOUT

Version
2.0.16

Picture 13.6: Terminal app settings

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

13.7.3 Booking terminal display lists

When booking terminal has been added in Nova and paired, Active and Screensaver lists can be added.
NOTE: If Info board module is in the system, it can also display its contents.

We add the list by navigating to Nova's terminal settings (**Home > Hardware > Info boards > select the terminal**) and press **Add** in the middle column.
This will bring up a pop-up window asking for:

- Title – name of the item for easier recognition
- Idle switch time – if a positive number is provided, the terminal will display this item for the set number of seconds. If the terminal ever gets to the list item that has a 0 set, the switcher will stop. (For example: a user has touched the screen and activated the active list that will display first item for 5 seconds, then second item for another 5 seconds and stop at the display of the 3rd item).

The items can vary from Layout (if info-board license active), Booking (if booking license is present).

When selecting a booking, we can specify if we want to display a single booking location or a booking group, we can also display or hide the title, time controls, and enable login/card login.

The same should be done for the Screensaver list – this list will be displayed after the terminal's set timeout.

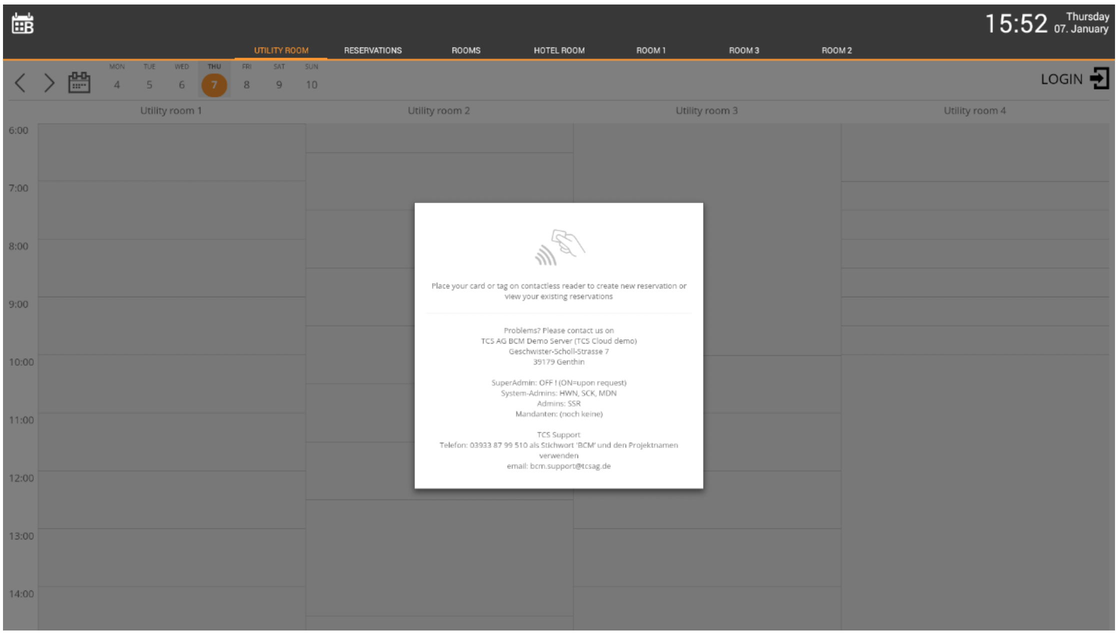
13.7.4 Terminal login

Log-in when the terminal mode is enabled. Picture 13-6 shows a preview of the login-screen when in terminal mode.

To log in the user needs to:

- Place the card on the Nexus reader.

NOTE: The maintenance contact information set in Nova is shown on the terminal login screen.



Place your card or tag on contactless reader to create new reservation or view your existing reservations

Problems? Please contact us on
TCS AG BCM Demo Server (TCS Cloud demo)
Geschwister-Scholl-Strasse 7
39179 Genthin

SuperAdmin: OFF ! (ON=upon request)
System-Admins: HWN, SCK, MDN
Admins: SSR
Mandanten: (noch keine)

TCS Support
Telefon: 03933 87 99 510 als Stichwort 'BCM' und den Projektnamen verwenden
email: bcm.support@tcsag.de

Picture 13.7: Terminal login screen

Alternative login:

- In case of trouble, the normal login form is accessed by tapping on the login text in the top right corner

Log-in credentials and user access:

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

- The drop-down menu at the top of the window enables the setting of the user access to the application.

13.8 Hospitality module (8004-00x-5400)

This booking is suitable when there is receptionist that only has access to the booking part of the Nova. They use their own credentials for log-in and can create new users and reservations via the booking GUI.
NOTE: When the reservation is done by hospitality administrator – for each reservation a new user will be created in the background and deleted once the reservation passes, so be mindful on the max user limit.

13.8.1 Creating a room booking location

1. Navigate to **Home > Settings > Booking settings**.
2. Click on the **Menu > Add booking location**
3. Provide the name and on Location type choose **Room booking**.

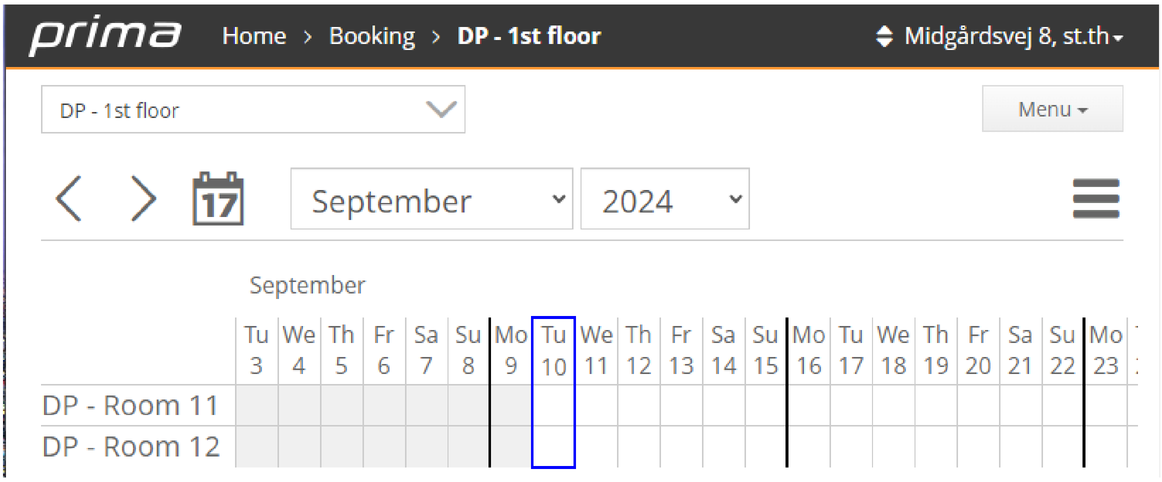
13.8.2 Creating a booking administrator

Booking administrator will only have access to the booking GUI.
To create a new booking administrator:

1. Create a new user.
2. Under Account type select **Booking administrator** and assign him log-in credentials.

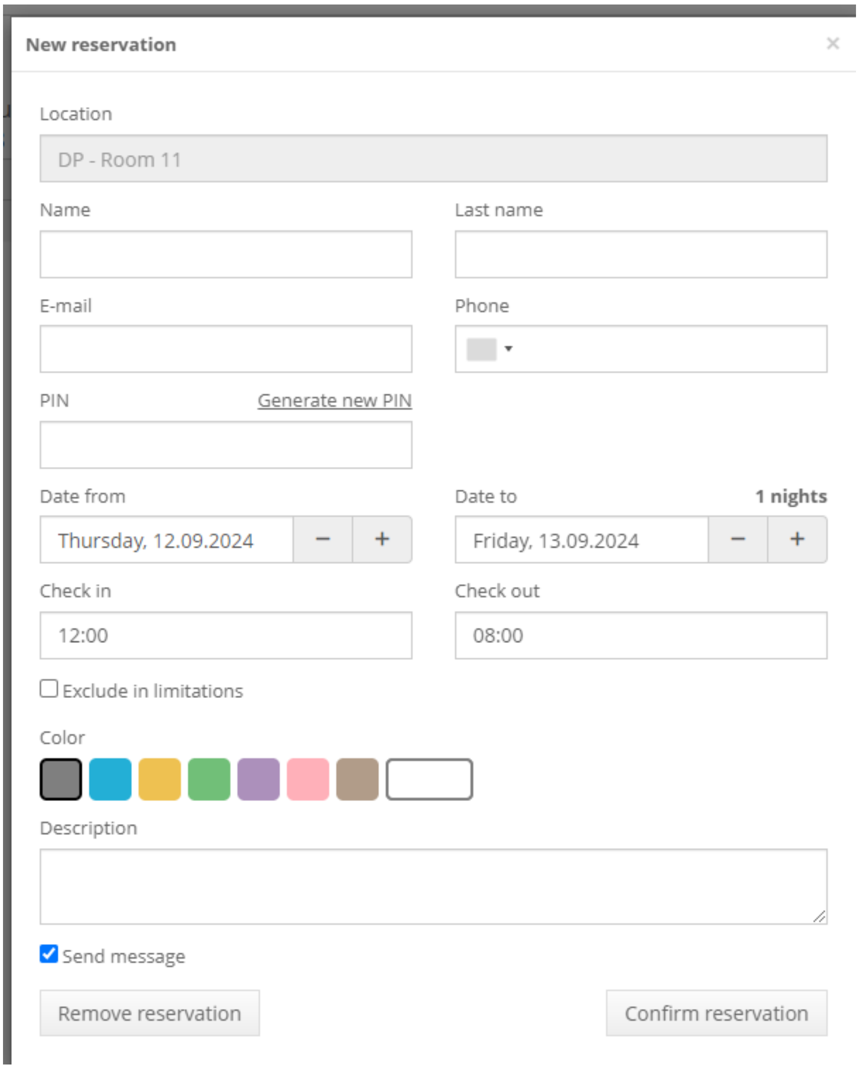
13.8.3 Reservation creation

This is the preview of the group of daily bookings from the booking administrator's perspective.


prima
Home > Booking > DP - 1st floor
Midgårdsvej 8, st.th
DP - 1st floor
Menu
17
September
2024
September
Tu 3 We 4 Th 5 Fr 6 Sa 7 Su 8 Mo 9 Tu 10 We 11 Th 12 Fr 13 Sa 14 Su 15 Mo 16 Tu 17 We 18 Th 19 Fr 20 Sa 21 Su 22 Mo 23
DP - Room 11
DP - Room 12

Picture 13.8: Daily booking group as part of the hospitality module

When selecting any free time slot, it will bring up the pop-up for creating a new user/reservation.



New reservation ×

Location: DP - Room 11

Name:

Last name:

E-mail:

Phone:

PIN — Generate new PIN

Date from: Thursday, 12.09.2024 − +

Date to: Friday, 13.09.2024 − + **1 nights**

Check in: 12:00

Check out: 08:00

☐ Exclude in limitations

Color

Description:

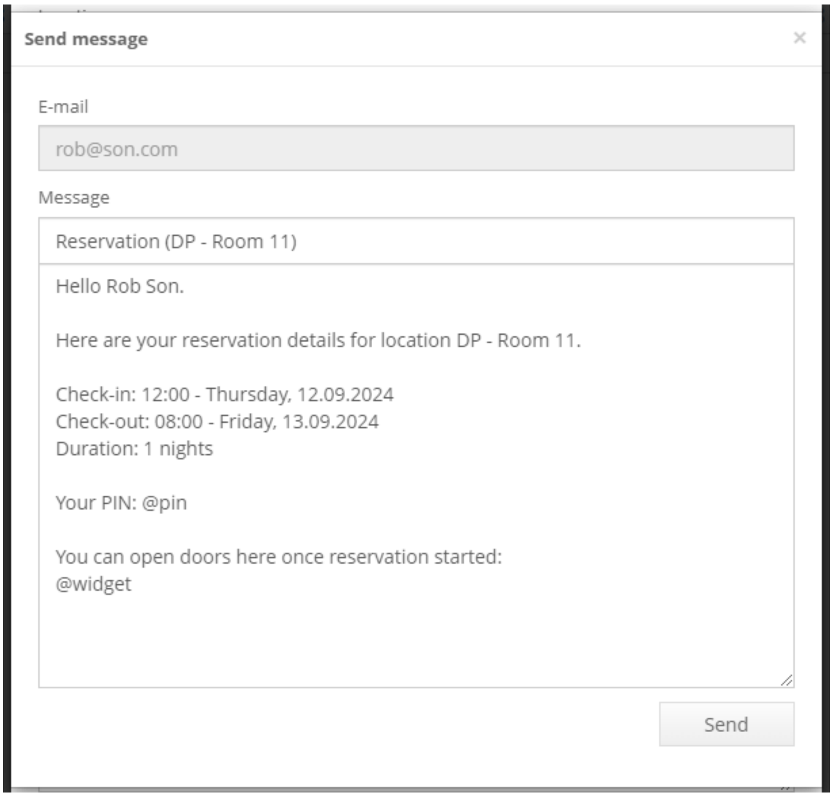
☑ Send message

Remove reservation

Confirm reservation

Picture 13.9: Reservation specifications

The booking administrator can fill in the required data and provide them with a PIN (optional), it can also check the send message option, this will send the PIN and reservation data to their email address (if provided).



E-mail

rob@son.com

Message

Reservation (DP - Room 11)

Hello Rob Son.

Here are your reservation details for location DP - Room 11.

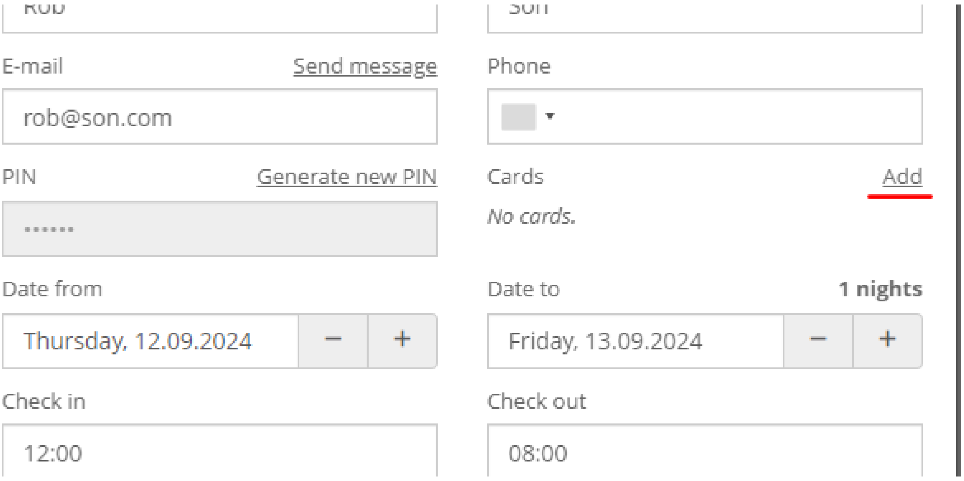
Check-in: 12:00 - Thursday, 12.09.2024
Check-out: 08:00 - Friday, 13.09.2024
Duration: 1 nights

Your PIN: @pin

You can open doors here once reservation started:
@widget

Picture 13.10: Reservation template that will be sent to the customer

After the reservation is created, a booking admin can also assign guest a card via the USB reader by presenting an "empty" card and holding it on the USB reader.



E-mail: rob@son.com

Phone:

PIN: ••••••

Cards: *No cards.*

Date from: Thursday, 12.09.2024

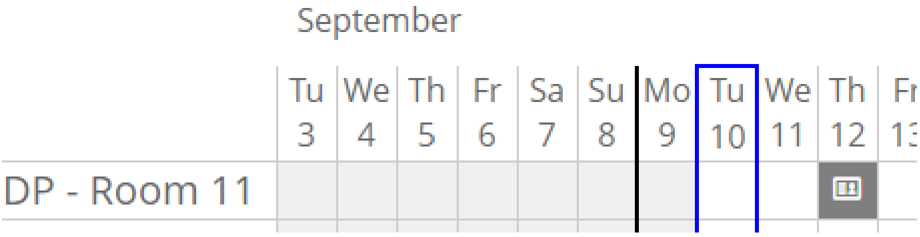
Date to: Friday, 13.09.2024 **1 nights**

Check in: 12:00

Check out: 08:00

Picture 13.11: Guest can be also assigned a card via the USB reader

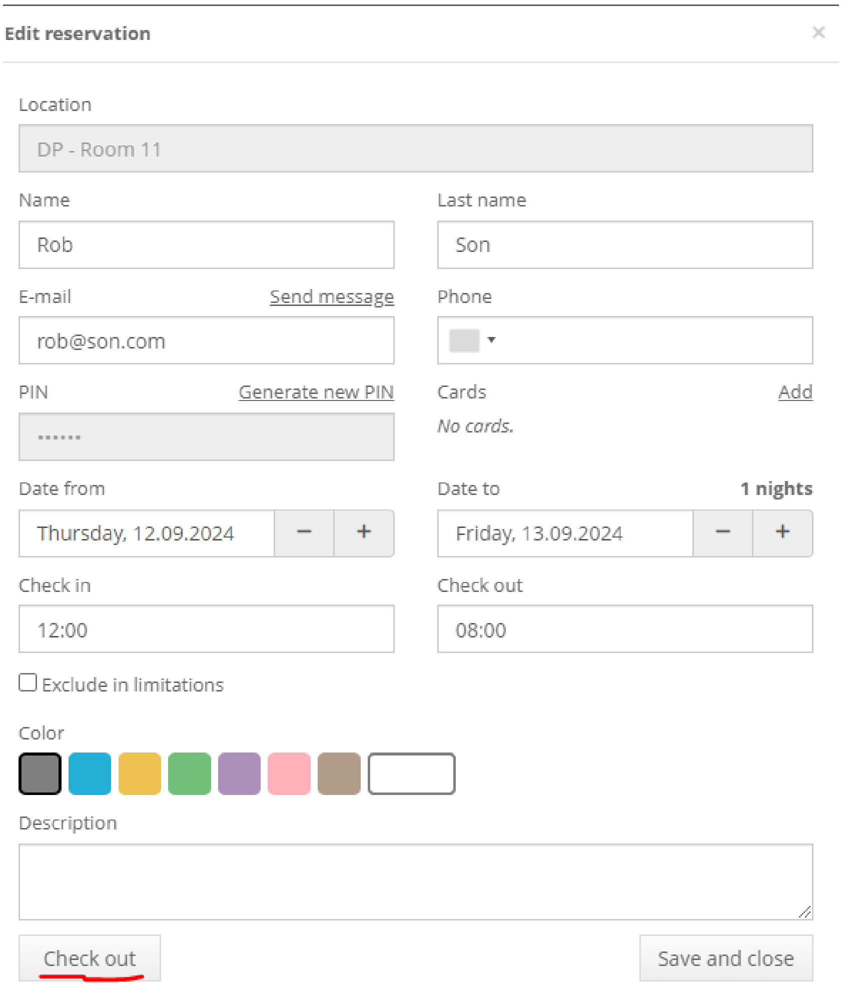
The reservation is completed.



Picture 13.12: Reservation shown on the calendar

13.8.4 Reservation end/cancelation

Once the reservation ends, the amin needs to find it, open it and press the checkout button. This will delete the temporary user made in Nova and its cards (if any) can now be assigned to a new guest.



Edit reservation

Location: DP - Room 11

Name: Rob

Last name: Son

E-mail: rob@son.com

Phone:

PIN: ••••••

Cards: *No cards.*

Date from: Thursday, 12.09.2024

Date to: Friday, 13.09.2024 — 1 nights

Check in: 12:00

Check out: 08:00

☐ Exclude in limitations

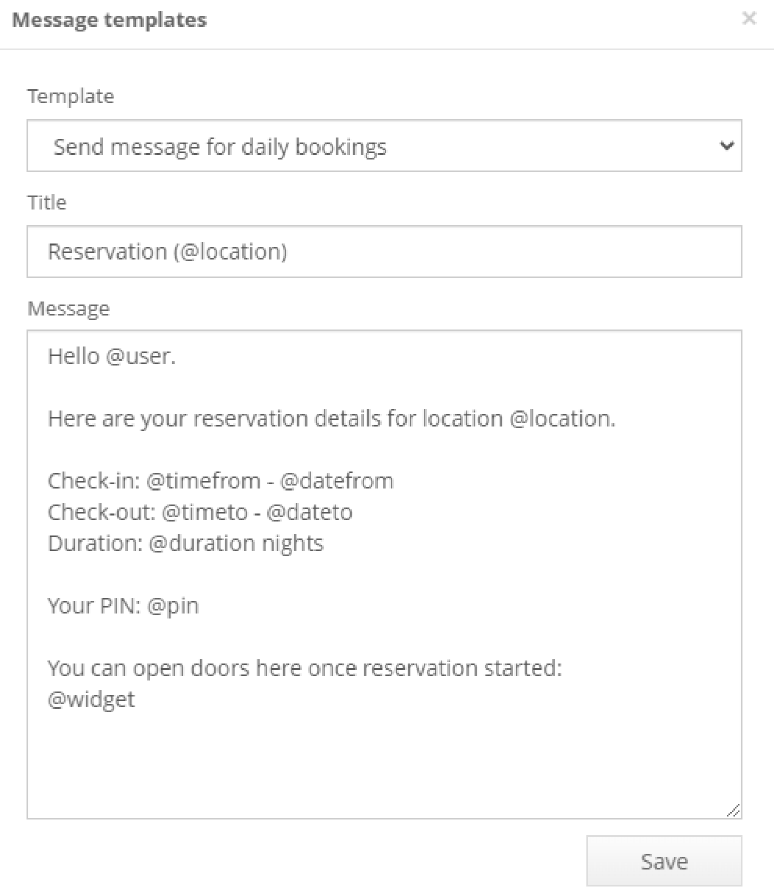
Color

Description

Picture 13.13: Reservation end

13.8.5 Email templates

When a reservation is created, we provide you with a sample email that can be changed to any custom text.
To do so, navigate to **Booking settings > Menu button > Message templates.**
From the first dropdown menu select Send message for daily bookings and update the title and message text with your own. **IMPORTANT! Keywords that start with @ need to be left in the same format otherwise the message will not be correctly generated.**



Template

Send message for daily bookings

Title

Reservation (@location)

Message

Hello @user.

Here are your reservation details for location @location.

Check-in: @timefrom - @datefrom
Check-out: @timeto - @dateto
Duration: @duration nights

Your PIN: @pin

You can open doors here once reservation started:
@widget

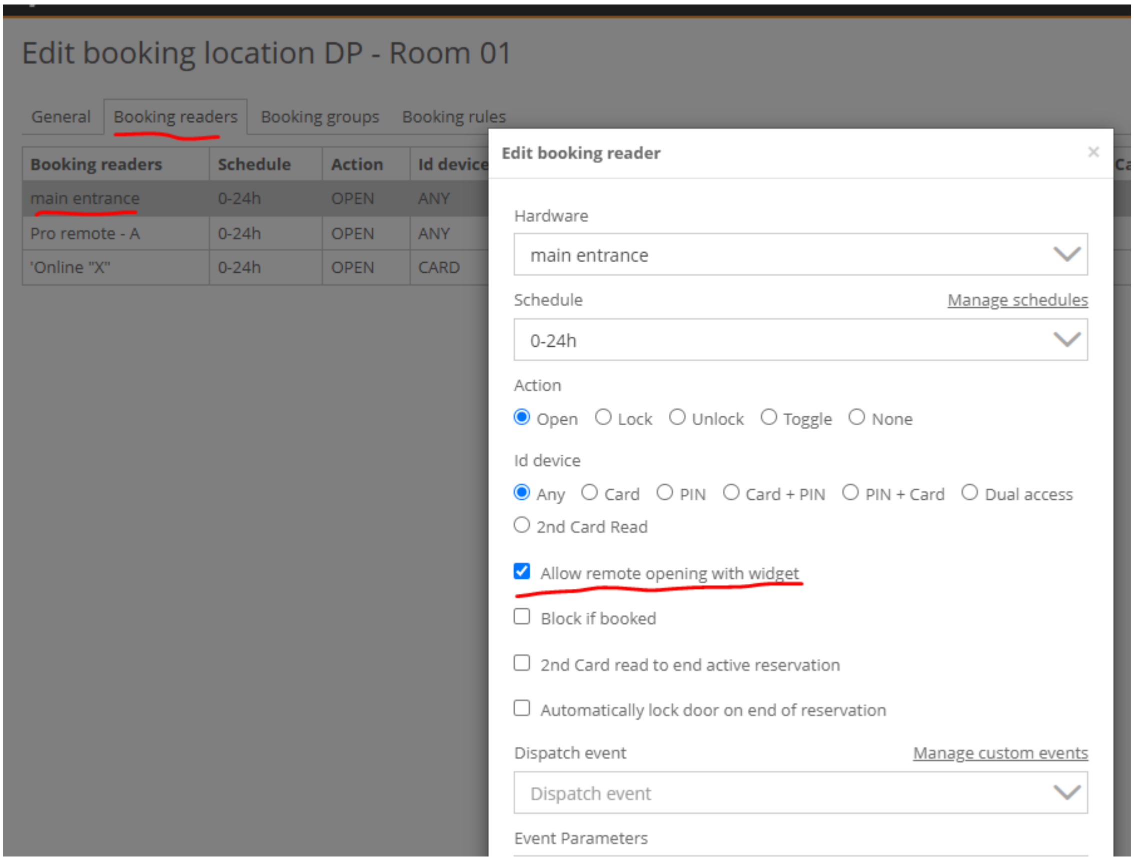
Picture 13.14: Message templates can be change to any custom text

13.8.6 Door widgets for remote opening

Requirements: widget license and central must be set-up for cloud access (Nova remote access or working DNS + certificates).
This option adds the ability to remotely from the email have access to a widget that can open the door (remotely). **PIN assignment is required because of security reasons**.

Firstly, you will need to specify which of the remote readers can be accessed by the customer. For this you will have to

1. Navigate to the daily booking location,
2. Select the booking reader’s tab
3. Double click on the ones you wish to enable remote opening and select the checkmark.



Edit booking location DP - Room 01

Booking readers	Schedule	Action	Id device
main entrance	0-24h	OPEN	ANY
Pro remote - A	0-24h	OPEN	ANY
'Online "X"	0-24h	OPEN	CARD

Edit booking reader

Hardware: main entrance

Schedule: 0-24h — Manage schedules

Action: ● Open ○ Lock ○ Unlock ○ Toggle ○ None

Id device: ● Any ○ Card ○ PIN ○ Card + PIN ○ PIN + Card ○ Dual access ○ 2nd Card Read

☑ Allow remote opening with widget

□ Block if booked

□ 2nd Card read to end active reservation

□ Automatically lock door on end of reservation

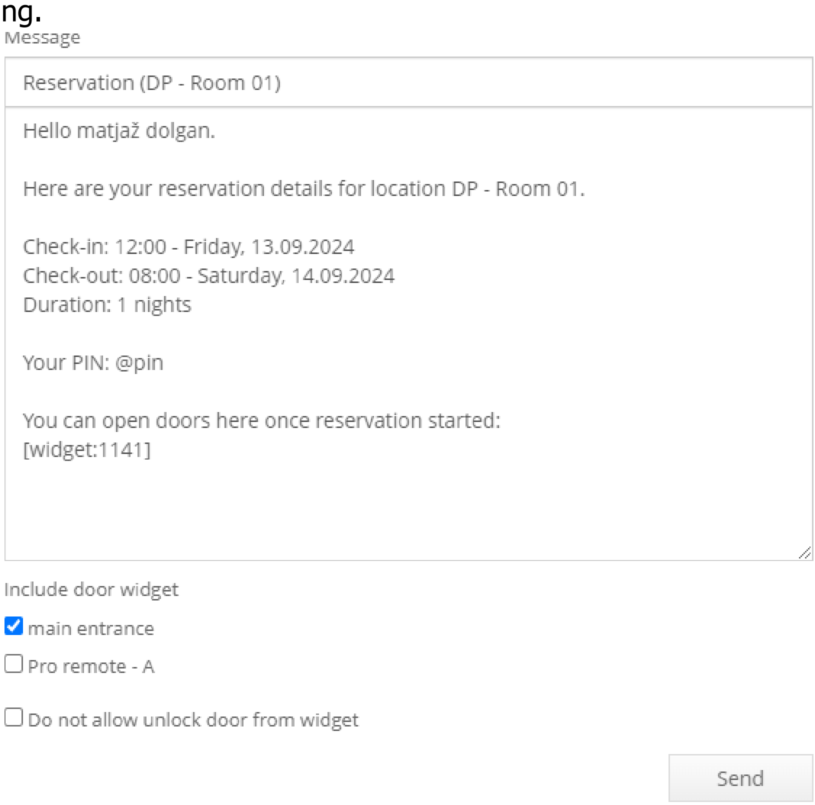
Dispatch event — Manage custom events

Dispatch event

Event Parameters

Picture 13.15: The customer will only get remote access to the wanted readers

Once the email is generated, you will be prompted to include the readers that allow remote opening.



Message

Reservation (DP - Room 01)

Hello matjaž dolgan.

Here are your reservation details for location DP - Room 01.

Check-in: 12:00 - Friday, 13.09.2024
Check-out: 08:00 - Saturday, 14.09.2024
Duration: 1 nights

Your PIN: @pin

You can open doors here once reservation started:
[widget:1141]

Include door widget

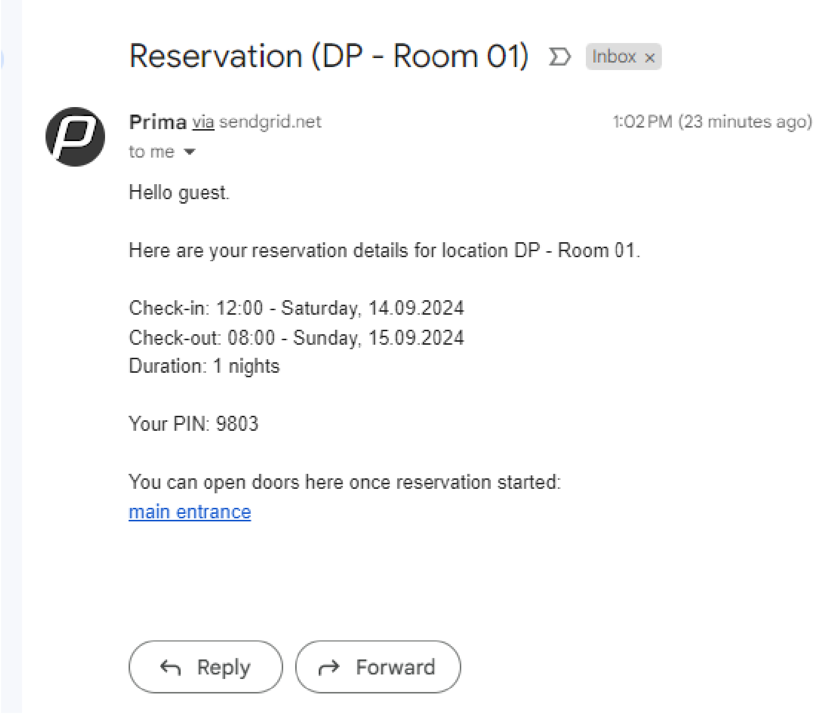
☑ main entrance

□ Pro remote - A

□ Do not allow unlock door from widget

Picture 13.16: The inclusion of the widgets for remote opening

The email will look like this:



Reservation (DP - Room 01)

Prima via sendgrid.net 1:02 PM (23 minutes ago)

to me

Hello guest.

Here are your reservation details for location DP - Room 01.

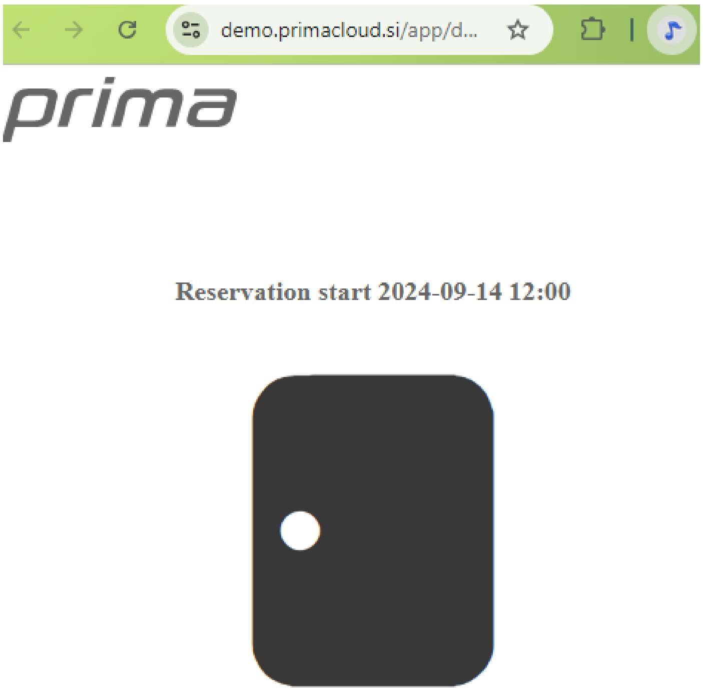
Check-in: 12:00 - Saturday, 14.09.2024
Check-out: 08:00 - Sunday, 15.09.2024
Duration: 1 nights

Your PIN: 9803

You can open doors here once reservation started:
main entrance

Picture 13.17: Customer's email contends with addition of widgets

And when clicking on the main entrance link a new pop-up will open asking for the PIN which the customer has to provide and then get access to the door opening which will work only during the reservation.



Reservation start 2024-09-14 12:00

Picture 13.18: Remote widget that the customer can remotely open the door.

14. Nova local administrator - advanced (804-00x-0004)

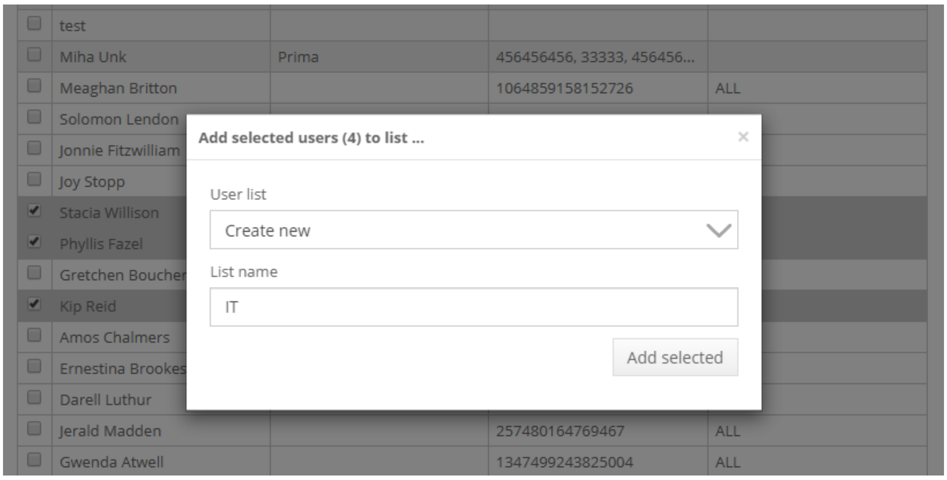
List editor is a perfect module for buildings with several smaller companies. It allows the system administrator to create groups and assign them specific hardware that they have access to. This way there are no unauthorized accesses because the local company administrators only have control over their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

14.1 Management of different lists

14.1.1 User list(s)

Creating and adding users to list:

1. Navigate to **Users** section and select users by ticking the checkmarks in front of their names.
2. Press **Menu > Add selected users to list**.
3. Provide the name for the **new list** or select the **existing one** from the dropdown menu.



Add selected users (4) to list ...

User list: Create new

List name: IT

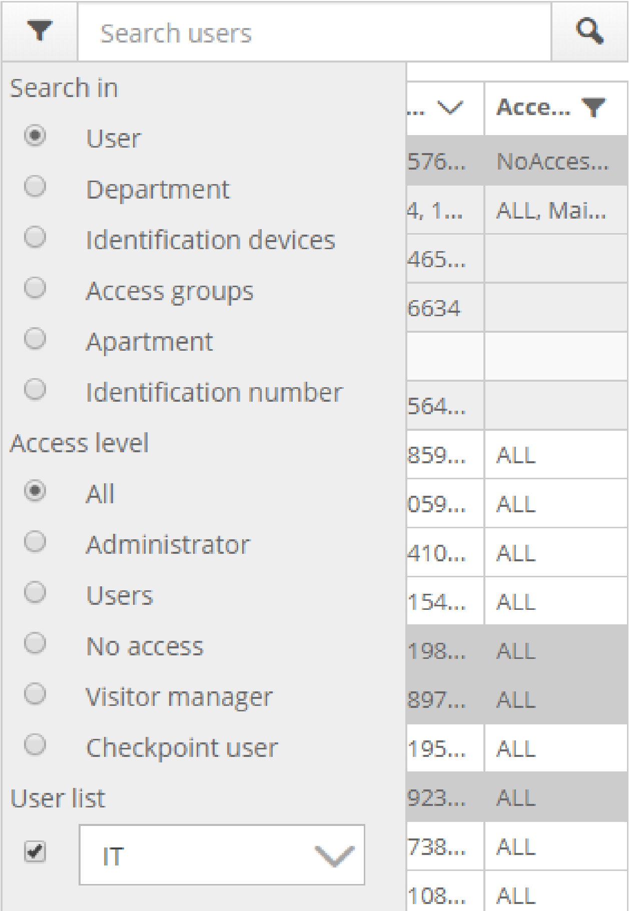
Picture 14.1: Creating new user list, selecting users and assigning them to the new list

Displaying users in list:

1. Navigate to users.
2. Select the Filter icon (before the search bar).
3. Check the box at User lists and find the requested list as displayed on Picture 14-1. Press **Apply** at the end of the menu.

Removing users from the list:

1. Make sure you select and show the users in the user list.
2. Select the users you wish to remove by setting checkmarks in front of their names.
3. Press **Menu -> Remove selected users from the list.**



Search users

Search in

● User

○ Department

○ Identification devices

○ Access groups

○ Apartment

○ Identification number

Access level

● All

○ Administrator

○ Users

○ No access

○ Visitor manager

○ Checkpoint user

User list

☑ IT

...	Acce...
576...	NoAcces...
4, 1...	ALL, Mai...
465...	
6634	
564...	
859...	ALL
059...	ALL
410...	ALL
154...	ALL
198...	ALL
897...	ALL
195...	ALL
923...	ALL
738...	ALL
108...	ALL

Picture 14.2: An example of a user list of employees

Removing or editing lists:

1. Navigate to Users.
2. Press **Menu > User lists** and select the wanted list.
3. a) Remove list by pressing **Menu > Remove list.**
   b) Edit list name by pressing **Menu > Edit list** and providing a new list name.

14.1.2 Hardware list

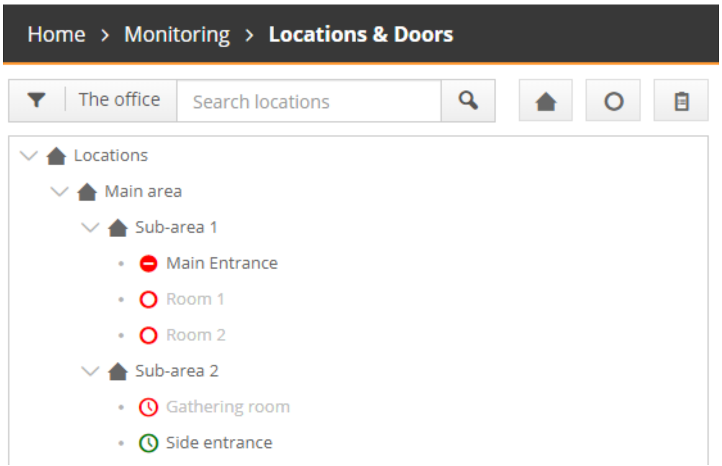
Creating and adding readers to Hardware list:

1. Navigate to **Locations & doors** and select readers (multiple can be selected by holding down the Ctrl key).
2. Press **Menu > Add selected readers to list**.
3. Provide the name for the **new list** or select the **existing one** from the dropdown menu.
4. Pressing the ⊕ button next to the selected reader will add it to the currently selected list. ⊗ will remove the reader from the current list.

Displaying readers in list:

1. Navigate to **Locations & doors**.
2. Select the Filter icon (before the search bar).
3. Check the box at User lists and find the requested list as displayed on Picture 14-3. Press **Apply** at the end of the menu.

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



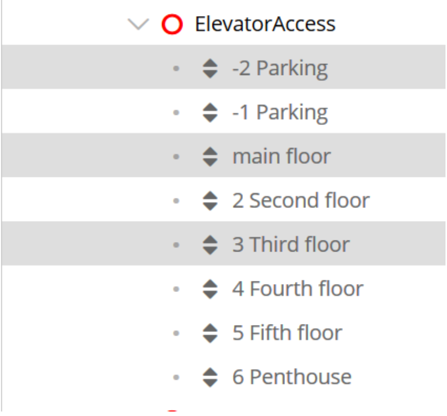
Picture 14.3: An example of a reader list

Removing or editing lists:

1. Navigate to **Locations & doors**.
2. Press **Menu > Reader lists** and select the wanted list.
3. a) Remove list by pressing **Menu > Remove list.**
   b) Edit list name by pressing **Menu > Edit list** and provide a new list name.

Assigning elevator floors to hardware list:

1. Navigate to Locations & doors.
2. Select one or multiple floors using Ctrl or Shift key on keyboard.



Picture 14.4: Selection of multiple elevator floors

3. **Menu > Add selected readers to list** and select to which hardware list you wish the floors to be assigned.

14.1.3 Info board list

Info boards can also be added to their lists and the list can be created/edited/deleted the same way as Hardware list except it is done in the **Info boards** section. Multiple devices can be selected using the Ctrl (single select) or Shift (sequence select) key on the keyboard.

Grouping info boards allow users to send a message to multiple devices at the same time - **21.3 Info board messages**. To learn more about Info boards and how to create message areas, navigate to 16.2 **Info board layouts**.

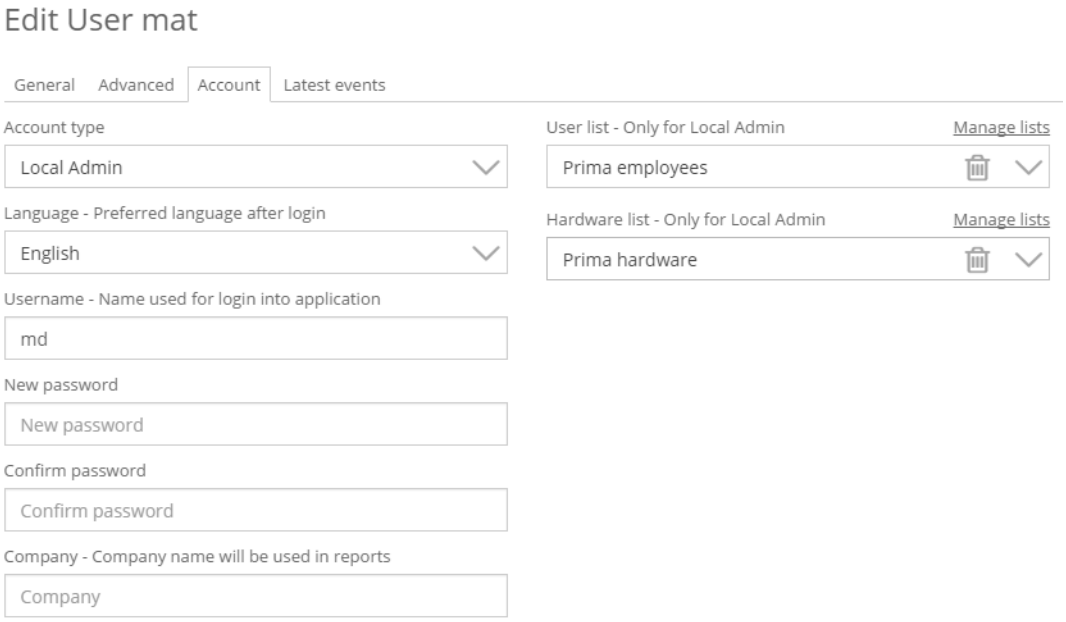
14.1.4 Apartment terminal list

Apartment terminals can also be added to their lists and the list can be created/edited/deleted the same way as Hardware list except it is done in the **Apartments terminals** section. Multiple devices can be selected using the Ctrl (single select) or Shift (sequence select) key on the keyboard.

Grouping apartment terminals allows sending messages to single or multiple apartments at once. You can read more about it in chapter **21.2 Apartment messages**.

14.2 Promotion to local administrator and list assignment

After creating the user and reader lists, they can be assigned to local administrators. To do so, navigate back to **Users and access rights** in the Nova software, Edit the selected administrator, and switch to the Account tab as shown in Picture 14-4. The account type must be set to "*Local admin*". By doing so, two dropdown menus become available under Local admin settings at the bottom of the pop-up. Select the desired lists and do not forget to save the new settings.



Edit User mat

Account type: Local Admin

Language - Preferred language after login: English

Username - Name used for login into application: md

New password: New password

Confirm password: Confirm password

Company - Company name will be used in reports: Company

User list - Only for Local Admin: Prima employees

Hardware list - Only for Local Admin: Prima hardware

Picture 14.5: Assigning account type and corresponding lists

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

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

14.3 Assigning a card layout to local administrator

Make sure that the local admin's hardware list has been created.
Assigning **new printing layout** to hardware list:

1. In the card designer select cog wheel icon and select the new layout option.
2. Provide the name and select the correct hardware list.

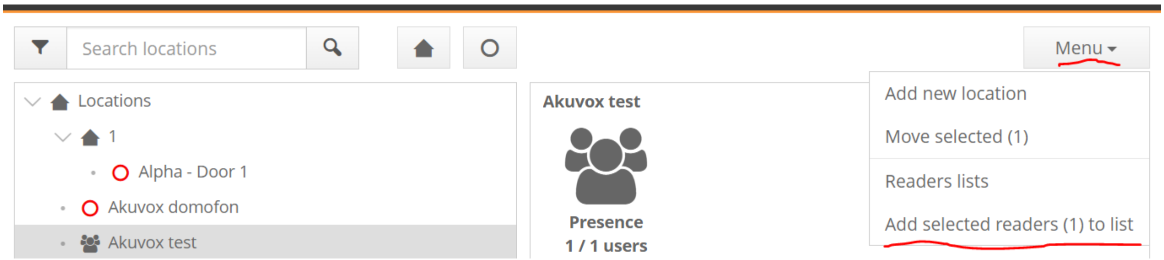
Assigning an **existing print layout** to hardware list:

1. Select the wanted layout in the card designer.
2. Navigate to cog wheel icon and select the rename option.
3. Select the hardware list from the dropdown.

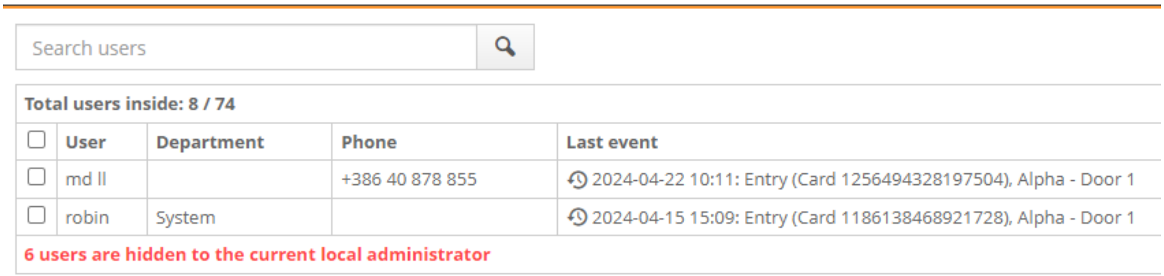
Any layout that is assigned to a hardware list will be also displayed for the local admin, but he will not be able to make any changes on it (**only sysadmin type is able to modify it**).

14.4 Assigning presence location to local administrator

If there is at least 1 presence location, you can navigate to **Locations & doors**, find the presence from the hardware list, select it, and assign it to local administrator's hardware list by selecting Menu > add selected item to list.



Users that are not part of their user list will be **hidden**.



Total users inside: 8 / 74

□	User	Department	Phone	Last event
□	md ll		+386 40 878 855	2024-04-22 10:11: Entry (Card 1256494328197504), Alpha - Door 1
□	robin	System		2024-04-15 15:09: Entry (Card 1186138468921728), Alpha - Door 1

6 users are hidden to the current local administrator

15. Card design and printing module (804-00x-4200)

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

To access the software, we need to navigate to the User list, select the users that we wish to create custom designs for and press **Menu > Card designer.**

15.1 Designing a card

On the left side, we are presented with an edit box, while on the right side will be displayed the preview of the current card for every user that we have selected.
NOTE! In the beginning, the backside of the card is not displayed, because it's empty. After we populate it, the preview will expand, showing us both sides.

Card size
By selecting the element, we are offered an option to use "Card bleed" which helps get rid of the empty card edges due to some printer limitations.
Clicking on the **Advanced** button will display the current(default) card size. From there, a custom card size can be entered.

The other items can be added to the card by pressing on the **new field** button. When the items are put on the layout, they are displayed on the list – the right side of the card. By clicking on them, their settings are brought up. Common settings for all fields are:

- The field can be moved by clicking on it and dragging it to the wanted position. The position can also be set by offsets: **From top** and **from left**.
- Resizing the field can be done by clicking on the edge and drag or by changing the values in the **Width** and **Height** fields underneath.

- **Depth** represents a value that defines which field is displayed under or over another. A lower depth value item is displayed behind the ones with a higher value.
- **Color** will open a color palette to choose a color for the field background (behind the text, image...). To remove the color from the background field, just delete the text.

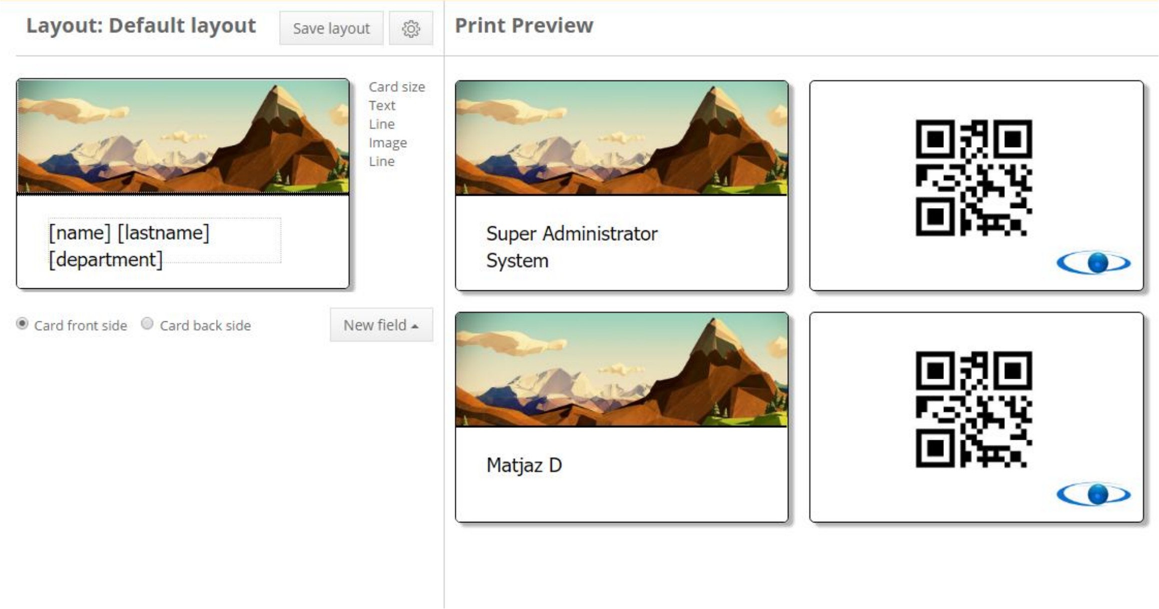
Some settings are dependent based on the selected field:

- Text – additional settings are **text font**, **size**, **color** and **align**. To change the text, simply replace the text in the text field. To make text **bold** or **italic**, select it and press the corresponding button on the left. To enter user-dependent text, press on the button **Insert**. The options are Name, Last name, Department, User ID, E-mail, Phone, Company.
  Any of the text field can be modified like this:

[validfrom] will print out 2024-01-01 12:00:00
[validfrom|dddd, DD MMMM YYYY] will print out Saturday, 12 December 2014
[Field|upper] will capitalize any text that is part of the field.
[Field|lower] will put any text that’s in field value to small case letters.
[Field|capital] will capitalize any text in field value.

- Image
- Profile Image
- Horizontal line
- Vertical line

To remove a field, click it and press the **Remove** button.
When everything is done, do not forget to **Save the layout**!



Picture 15.1: Front and back side preview of a card design

15.2 Card layouts

After a layout is completed, it will be saved as a default layout. If we wish to manage multiple layouts, we can do so by selecting the **cogwheel** (next to the Save layout button) and create a new layout. This opens a pop-up which requests:

- Layout name.
- Make a copy of the current layout – creates a copy, so you can preserve the original layout and make changes to a new one.
- Save changes before creating a new layout.

Once there is more than one layout present in the system, we can switch layouts by pressing on the cogwheel and click on the name of the other layout you wish to use. The currently active layout has a grey block in front of its name. The other options that are available from the same dropdown menu once a new layout is created and active:

- New layout
- Rename

- Remove

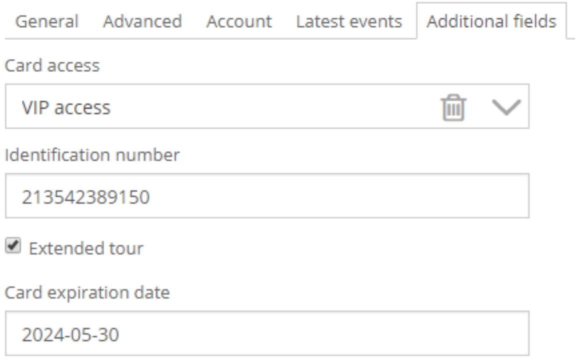
15.3 Additional user fields

Nova 2.2.10 and higher versions support creating additional fields that can be displayed on the card designer preview. Additionally, we can integrate some logic into card creation.
The fields can be accessed by navigating to **Users > Menu > Manage additional fields**.
A new pop-up will open showing any already created fields.

A new custom field can be created by pressing **Menu > Add**.

There are different types of fields:

- Text – a custom text can be provided/displayed.
- Date time – Entry can be filled with the set date and time text.
- Date – Custom date can be set.
- Time – Custom time.
- Checkbox – We can react if the checkbox is enabled or not.
- Dropdown – Multiple predefined choices can be made.



Card access
VIP access

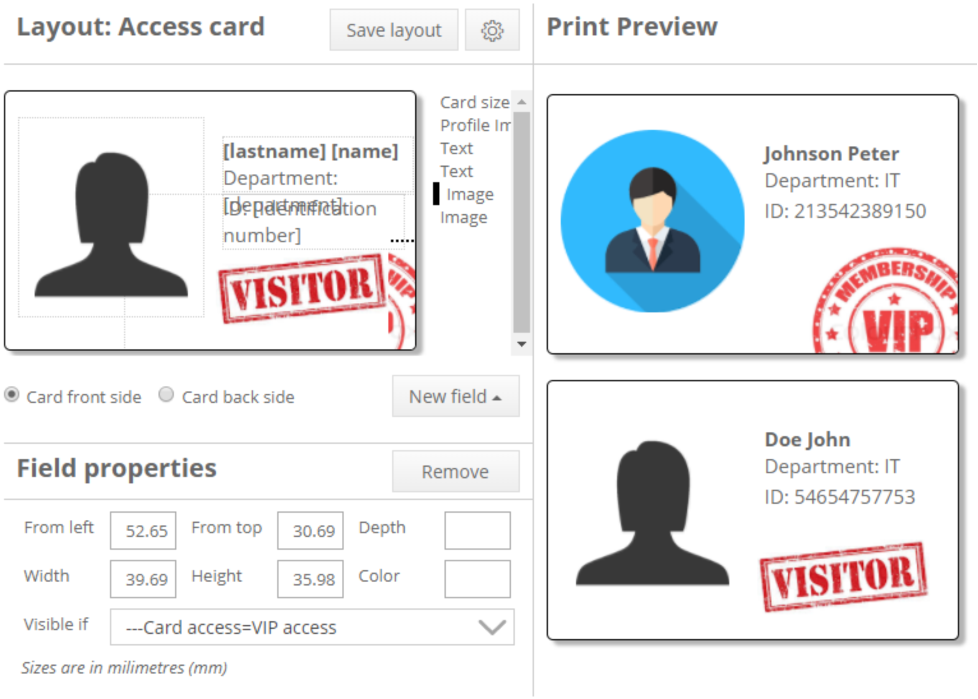
Identification number
213542389150

☑ Extended tour

Card expiration date
2024-05-30

Picture 15.2: An example of additional user fields

In the card designer, we can invoke the custom fields by selecting the "Visible" field properties. This way we can display a picture if the user has the correct checkbox filled or if the selection from the dropdown menu is valid.
This does not only affect the pictures, but we can also manipulate text too. e.g., if the text in the text field is present, we can display it on a card.



[lastname] [name]
Department: [department]
ID: [identification number]

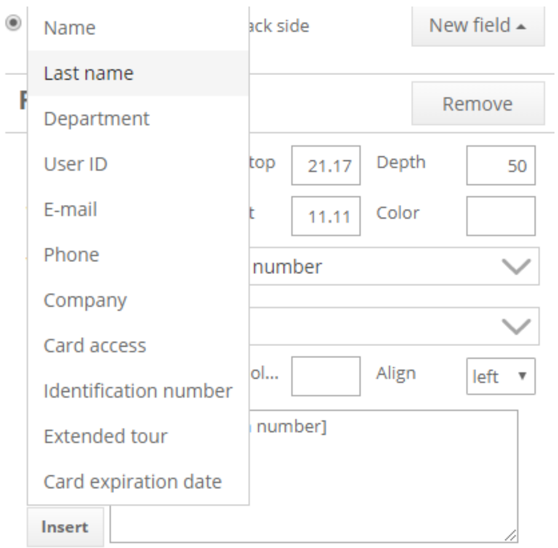
Johnson Peter
Department: IT
ID: 213542389150

Doe John
Department: IT
ID: 54654757753

From left 52.65 From top 30.69 Depth
Width 39.69 Height 35.98 Color
Visible if ---Card access=VIP access

Sizes are in millimetres (mm)

Picture 15.3: With custom fields, we can create one layout with different custom content



top 21.17 Depth 50
t 11.11 Color
number
ol... Align left
number]

Picture 15.4: Additional text options are displayed because of custom fields

16. Info screen module (804-00x-5200)

Note: The info screen module should only be used with NovaServer or with Alpha with external USB storage plugged into the top master central.
This module enables users to create, assign, and change the display of an Info screen.
Note: The Info screen module requires separate hardware – info screen driver and a display.
To enable the Info screen module, apply an activation key to the system. The procedure of adding an activation key is described in chapter **6.1 Add-ons and Modules**. After activation, the Info screen section can be accessed by navigating to **Home > Hardware > Info screens.**

IMPORTANT! The default IP of the Info screen (hardware v.1) driver is 192.168.1.101. Info screen v.4 is set on DHCP by default.

IMPORTANT! The old hardware Info screen is verry susceptible to power loss – SD card can get damaged very easily, so we recommend having an UPS that prevents permanent damage of the hardware.

16.1 Managing info screen driver

16.1.1 Info screen driver v1.X

When all hardware is set up, search for info screen in the network by clicking **Menu > Search for info screens.** If the central and info screens are connected in the same network, it will be displayed in the left side list along with its version, IP, and MAC address.

- If the info screen driver is in a different network from the central, it needs to be moved to the same network as the central. This can be done by using the Central discovery tool (you can read more about it in chapter **24 Central discovery tool**).

To add it to the software:

1. Double click on the found info screen driver or
2. Navigate to Menu > Add [info screen name] or
3. Add it manually by navigating to **Menu > Add info board.**
4. Provide/make sure that the name is entered and its IP address is correct.

To edit the info board:

1. Select the existing info board and press **Menu > Edit [info screen name]** or
2. Double click the list entry to edit.

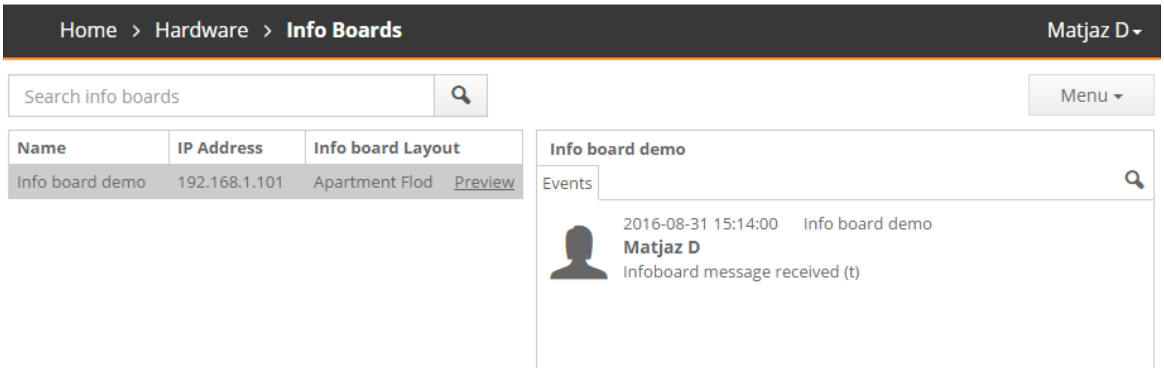
Info screen update:

1. Select the info screen you wish to update.
2. **Menu > Update info screen display.**

3. Select the package from the PC and wait for events to report the finished update.

Info screen Removal:

1. Select it from the list
2. Press **Menu > Remove [info screen name].**



Name	IP Address	Info board Layout	
Info board demo	192.168.1.101	Apartment Flod	Preview

Info board demo

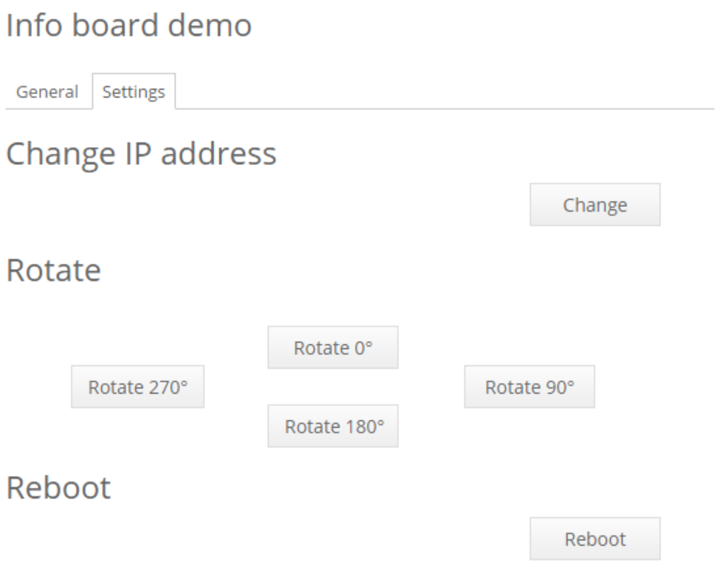
2016-08-31 15:14:00 Info board demo
Matjaz D
Infoboard message received (t)

Picture 16.1: List of info screens

Info screen driver settings

To access the settings of the info screen driver, simply double click on the info screen in the list or select it and navigate to **Menu > Edit [info screen name].** The general tab will open by default. Selecting the **Settings tab** gives the next options:

- Change the info screen's IP address (make sure that the info screen is located on the IP provided when added to the software).
  - Enter the new IP address.
  - Enter the subnet mask.
  - Enter the default gateway and press the **Change** button to send the command.
- Rotate option:
  - Rotate 0° - For standard mounting.
  - Rotate 90° - Rotate the image for 90° CW.
  - Rotate 180° - Rotate the image upside down. Appropriate for ceiling mount.
  - Rotate 270° - Rotate the image for 270° CW.
- Reboot option- Sends a reboot command to the info screen driver.



Info board demo

General | Settings

Change IP address

Change

Rotate

Rotate 0°

Rotate 270°

Rotate 90°

Rotate 180°

Reboot

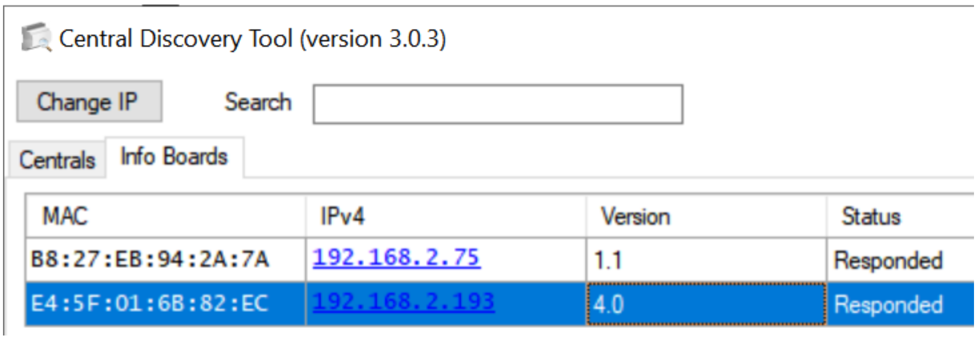
Reboot

Picture 16.2: Info board settings

16.1.2 Info screen driver v4.X

Plug in the micro-HDMI, the ethernet cable and the **power cable last!** The device will boot up in a couple of minutes.
Download the latest Central discovery tool (chapter **29 Central discovery tool**) and navigate to the Info screens tab. If there is a DHCP enabled network, the device will respond on the DHCP assigned IP address.

- If there is no DHCP server on site, the set-up must be done beforehand and switch the networking to the static configuration.



Central Discovery Tool (version 3.0.3)

Change IP   Search

Centrals | Info Boards

MAC	IPv4	Version	Status
B8:27:EB:94:2A:7A	192.168.2.75	1.1	Responded
E4:5F:01:6B:82:EC	192.168.2.193	4.0	Responded

Picture 16.3: Info boards found by discovery tool

Once listed on discovery tool click on the IP to access its GUI.
The default password is **sys4Admin** the same as for the central. **It is strongly recommended to change the password once logged in.**

Settings:
Pair – Used for pairing the device with the Nova.
Change password
Network settings – Options for the DHCP or static IP address.
Advanced options:

- Reboot device
- Turn off (use to shut down the device when scheduled electricity outage for e.g.)
- Restart app – force reload the app that runs the info board.
- Restart browser – force reload the browser.

Rotate screen display – Used for picture rotation if the monitor is mounted on the wall or the ceiling.

How to pair the device:
In Nova:

1. Navigate to Hardware > Info screens.
2. Click on Menu > Add info screen, provide the name, and select **Type version 2**.
3. Under Pairing column click on Create new token button and copy it.

In Info screen GUI:

1. Click on pair the device button.
2. Provide the token and the URL to the central (you can use http or https).

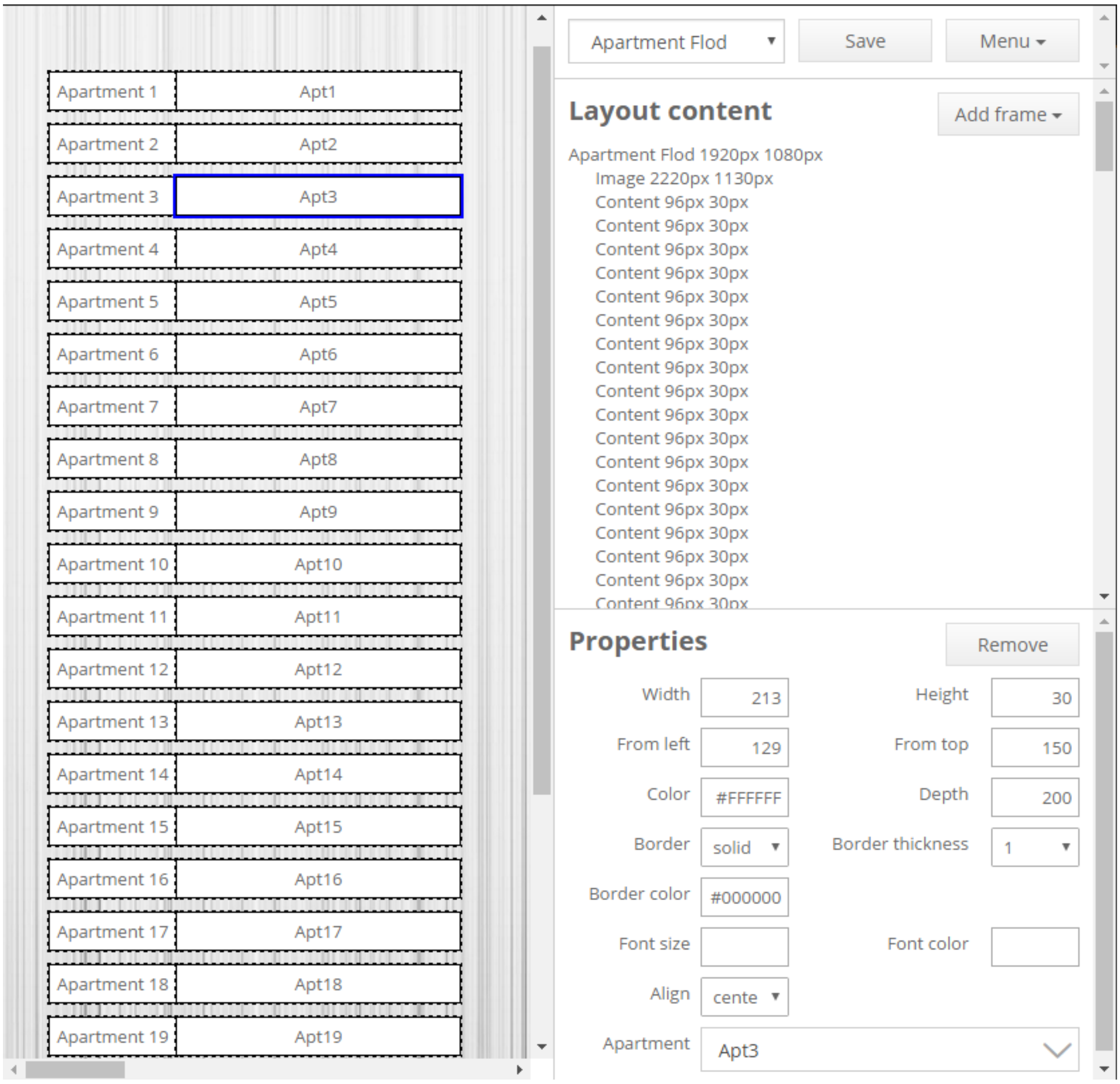
How to display layout items:

1. Navigate to Hardware > Info screens.
2. Double click on the wanted info screen.
3. Populate the **Active list** by pressing **Add** and fill the requested fields. **Screensaver list is not used.**

16.2 Info screen layouts

Layouts are the web pages created in the Nova software. After creation, preview them in the browser before uploading them to the info screen.

To create a new layout, please navigate to **Menu > Manage Layouts** from Info screens widget**;** a pop-up window will open with the canvas on the left side and the settings panel on the right.



Apartment 1	Apt1
Apartment 2	Apt2
Apartment 3	Apt3
Apartment 4	Apt4
Apartment 5	Apt5
Apartment 6	Apt6
Apartment 7	Apt7
Apartment 8	Apt8
Apartment 9	Apt9
Apartment 10	Apt10
Apartment 11	Apt11
Apartment 12	Apt12
Apartment 13	Apt13
Apartment 14	Apt14
Apartment 15	Apt15
Apartment 16	Apt16
Apartment 17	Apt17
Apartment 18	Apt18
Apartment 19	Apt19

Layout content

Apartment Flod 1920px 1080px
Image 2220px 1130px
Content 96px 30px
Content 96px 30px
Content 96px 30px
Content 96px 30px
Content 96px 30px
Content 96px 30px
Content 96px 30px
Content 96px 30px
Content 96px 30px
Content 96px 30px
Content 96px 30px
Content 96px 30px
Content 96px 30px
Content 96px 30px
Content 96px 30px
Content 96px 30px
Content 96px 30px
Content 96px 30px

Properties

Width	213	Height	30
From left	129	From top	150
Color	#FFFFFF	Depth	200
Border	solid	Border thickness	1
Border color	#000000		
Font size		Font color	
Align	cente		
Apartment	Apt3		

Picture 16.4: Info screen layout example

Description of panel sections:

- On the top, there is a text field with the layout name. Before creating a layout, please name it first.
  NOTE: To rename a layout, make sure that the first entry in **Layout content** is selected – this will display the **Name** property which you need to input.
  Once there are multiple layouts created, it is possible to select one from the dropdown menu.
  Next to the Name, there is also a layout orientation, its resolution, and its color.
  NOTE: The max resolution supported is FHD (1080p). Upscaling to 4k resolution is done by the TV.
    - To close the pop-up window, navigate to **Menu > Close window.**
    - **Menu > Preview** will open a new web page that will show a preview of the created layout.
    - Removing a layout can be done by pressing **Menu > Remove [layout name].**

    - **Menu > Duplicate layout** will create a copy of the currently selected layout. This can be helpful if similar layouts are needed with different information.
- In the middle, **Layout content** includes the list of items placed on the canvas.
    - Multiple frames can be added to the canvas. The following items can be chosen from, by clicking on **Add frame:**
        - **Content**: Most common item, that either can include a text or can be used as a background-colored object. To add/edit text to the content, please press the **Edit content** button. A new pop-up editor will open to freely edit the text font, size, etc. Content can also display HTML code or video (Source code and insert/edit video buttons).
        - **Image**: Adds an image from your computer.
        - **Iframe**: Enables display of web-pages that are enabled for Iframe like booking, videos… If the web-page is designed with the Iframe in mind, this is the best solution to implement it.
        - **Embed**: Enables adding embedded HTML code – used for YouTube videos (navigate to video and under it press Share and Embed tab; copy generated code to the text embed entry), Twitter (use external sites to generate a custom twitter feed that can be embedded into the info board) …
          IMPORTANT! Twitter videos do not support auto-play, so tweets that include GIF-s or videos will not play.
          IMPORTANT! High-quality videos are demanding and might not play smoothly. To fix the issue, please embed the video that plays a lower resolution video. YouTube and other HTML5 videos might need some additional parameters like autoplay and loop to keep them going.
        - **Apartment label:** When selected, an apartment can be assigned and the text from the apartment will be displayed the same way as it is on the Door stations or Mailboxes. The apartment text display format can be set under info board driver general settings.
        - **Message:** Local admin, Administrator, and the System administrator can all send messages to the info board, which will be displayed and updated in this frame.
        - **Slideshow:** Designed to display multiple frames in an endless loop. Each slide can have a custom timer assigned. By selecting Slideshow settings, slides can be added/removed/reordered.
        - **Copy selected:** Creates a copy of the currently selected frame. Very useful for creating multiple objects with the same content.
    - The first item is always the canvas. Clicking on it will bring different settings to the **Properties** panel – the layout name, its size in pixels (make sure to enter the resolution of the display that will be connected to the info screen). You can also select a background color.

Note: To remove any color from the object, delete the text field contents, and press Enter.

- Clicking on the different objects from the Layout content will select it on the canvas (blue border color) and bring the object properties in the bottom panel – general settings:
    - **Width**: frame width.
    - **Height**: frame height.
    - **From left**: distance (in pixels) of the frame from the left side.
    - **From top**: distance (in pixels) of the frame from the top side.
    - **Color**: color of the frame (if the text is empty, it is see-through).
    - **Depth**: determines which frames are displayed in front (frames with the highest number, will appear on top).
    - **Border**: border type – solid, dashed, or dotted.
    - **Border thickness**.
    - **Border color**.
- To remove a frame, select it from the **Layout content** and press the **Remove** button in the **Properties tab.**

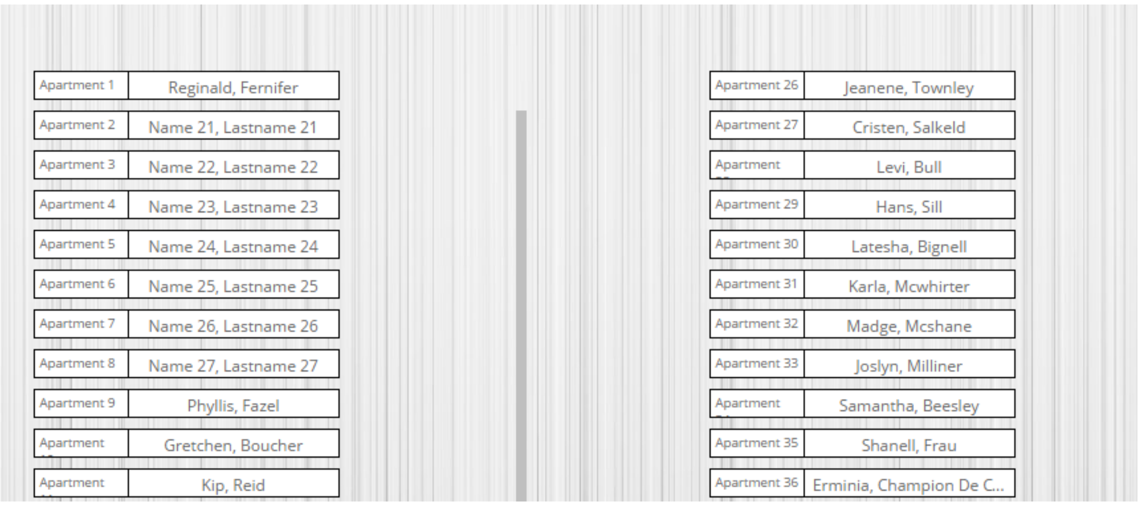
Frames can be dragged and dropped anywhere on the layout. To access a frame that is covered with other frames, you can give those temporary lower Depth or you can just move them to the side, re-position the troubled frame and return the top frame to the previous position.

Note! When dealing with multiple frames, select them using the Ctrl key and click more frames into selection. Once selected, move all selected at once by moving them the same way.

Sometimes the frame cannot be moved due to its content (ex. Videos have click to start/stop and do not allow mouse drag). To move such frames, use the **from left** and **from top** properties.

Note! Some property fields can be increased or decreased by clicking on them and pressing the up/down arrows. A single press on the up arrow on the keyboard will increase the current field by 10; this also works when selecting multiple frames – it is good for increasing the width or height of selected objects.

When done editing, press the **Save** button and close the layout pop-up.



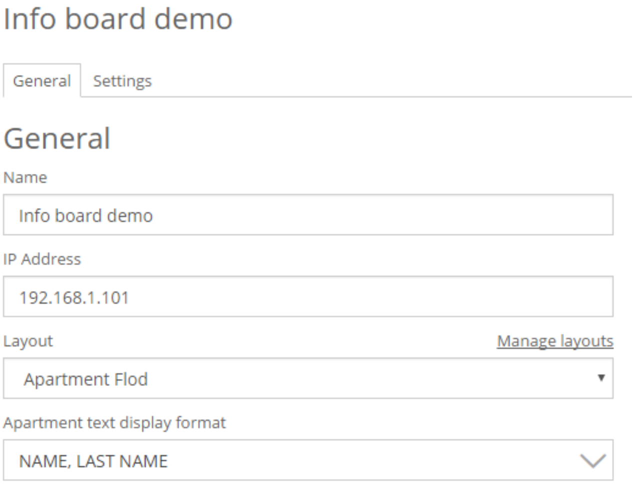
Apartment 1	Reginald, Fernifer	Apartment 26	Jeanene, Townley
Apartment 2	Name 21, Lastname 21	Apartment 27	Cristen, Salkeld
Apartment 3	Name 22, Lastname 22	Apartment	Levi, Bull
Apartment 4	Name 23, Lastname 23	Apartment 29	Hans, Sill
Apartment 5	Name 24, Lastname 24	Apartment 30	Latesha, Bignell
Apartment 6	Name 25, Lastname 25	Apartment 31	Karla, Mcwhirter
Apartment 7	Name 26, Lastname 26	Apartment 32	Madge, Mcshane
Apartment 8	Name 27, Lastname 27	Apartment 33	Joslyn, Milliner
Apartment 9	Phyllis, Fazel	Apartment	Samantha, Beesley
Apartment	Gretchen, Boucher	Apartment 35	Shanell, Frau
Apartment	Kip, Reid	Apartment 36	Erminia, Champion De C...

Picture 16.5: Info screen layout preview

16.3 Assigning layouts to info screens

To select which layout will be displayed on the info board, navigate to **Home > Hardware > Info screens** and double click on the wanted widget.
From here, select the Layout to display from the dropdown menu. If there are any apartments set on the active layout, also choose the appropriate display format.
Once all is set, it is possible to:

- Preview the currently assigned layout: **Menu > Preview.**
- Upload the layout to the info board by pressing **Menu > Update display.**



Info board demo

General

Name: Info board demo

IP Address: 192.168.1.101

Layout: Apartment Flod

Apartment text display format: NAME, LAST NAME

Picture 16.6: Info screen's General settings

16.3.1 Booking terminal as info screen

The new booking terminal app allows displaying content from info screen and different booking locations too.

How to get started with the terminal? Pair it first.

1. Go to Info screen section and press **Menu > New info screen** and select **Version 2**.
2. In its settings press **Generate token** to create a pairing token and write it down.
3. Go to the booking terminal, set the correct top master IP/URL and enter the pairing token.
4. Once the connection is established, different active and screen saver lists can be created.

The **Active list** means that when a person makes an interaction with the device, the layouts from the active list will be displayed in sequence. The sequence will be stopped at the layout with 0 idle switch time. If there is no layout with a stop timer, the active list will endlessly rotate through Active list items. After a set time of inactivity (set on the terminal), the device will switch and display **the screen saver list**.

Clickable parameter in the item's list allows/prevents users from interacting with selected layout/booking (this can prevent users from navigating to other web sites).

16.4 Sending a message to info board driver

Along with the info screen widget, a **Messaging** widget becomes visible too. Navigate to **Home > Messages**.
To create a new message press Menu > New info screen message.

Click on the **to:** label to display available info screens, select the correct info screen from the dropdown menu, provide a Title for your message (only displayed in the software and not on the info screen) and create a new message that can include text, picture, or a video.

Once done with message creation, click the button to preview it on the info screen. This will open the layout of the selected info board and put the message inside the **Message** frame (if it exists) and open a preview page in another window. If satisfied with the result, close the preview window, and send the message. The display should update with the new message after a couple of seconds.

17. High security module (804-00x-1600)

This module makes some software changes that improve overall security. To activate this key, please follow the instruction in chapter **6.1 Add-ons and Modules**.
By entering this module, a new section: **Security settings** and **Reader encryption** will be displayed in the Other Settings menu.

Enable HTTPS redirect
Centrals with hardware version 3.0 support HTTPS access by default. Navigation on HTTP protocol is unsafe – the data between the computer and the central can be monitored by someone else on the network. Using HTTPS protocol (**https://<cental-IP>**) will create a secure handshake with the target central. After the handshake is done, the connection will be encrypted.
NOTE: When accessing the webpage via HTTPS, the browser will report that the site is untrusted due to the self-signed certificates that are provided by the central. The site can still be accessed by putting the site to ignore the list – the connection is encrypted, but there is no way to check if the target recipient is the central or not. To avoid the browser warning, custom certificates need to be uploaded to the central for a unique and secure connection. Details are better described in chapter 17.1 Uploading custom certificates.
In the **Other Settings**, there is an option under **Security settings** to redirect all traffic from HTTP to HTTPS. After this setting is set, anyone who wishes to access the central via unsafe connection will be automatically redirected to a secure one.

Disable webserver port on slave centrals
Access on all slave centrals is usually read-only, but to increase security, we can disable the GUI access on all slave centrals at once. The software version installed on all centrals must be at least 2.1 for this feature to work. If a central is reset to defaults, the GUI becomes accessible again. Adding new centrals into the system while having this option enabled, will automatically disable access to that central's GUI.

PIN changes
The PIN codes are hidden from all users for security purposes.
Additionally, **PIN only access can be DISABLED**, Card + PIN and PIN + Card combination requiring **PIN** length can be **set to require at least 4 numbers**.
Due to the security reasons, if the PIN on the reader is entered incorrectly, it won't be displayed in the event.
Entering a faulty PIN multiple (5) times, will result in the reader reporting a faulty pin even if it's entered correctly until the end of a set time (1 minute).

Password changes
The system will require a password length of at least 8 characters. Additionally, the password cannot contain more than 2 repeated characters and cannot include sequential

numbers or characters (ex. **111**OX12 – not suitable, AgEf**432** - not suitable, 65g**bca**539 - not suitable).

Note! If the passwords were assigned before this function was enabled, the existing users will not be forced to change it, so it is recommended to enable it before creating other user's accounts.

Idle log-outs

If this option is checked, the account type: **system administrator** will be automatically logged out of the system after 10 minutes of inactivity. The timer is not active if the GUI is opened on the **Events** or **Floor plan** page (for monitoring reasons).

Reader encryption

This option enables encryption on the wire between the central and the reader. Enabling this option will result in readers working a bit slower, but more secure.

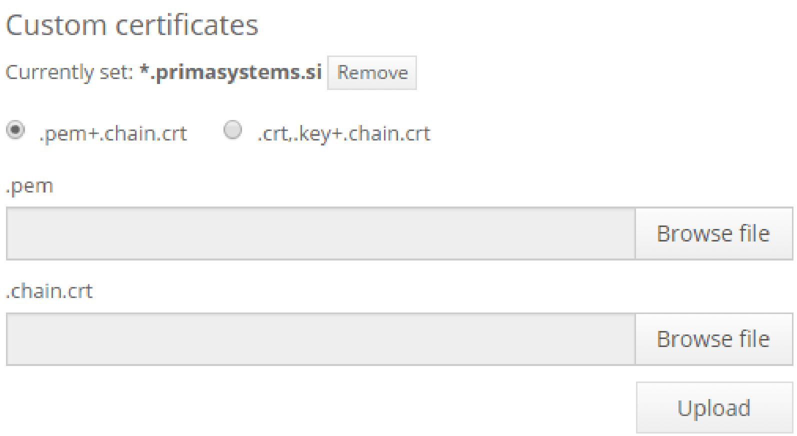
Increased notification limit

With the regular standard basic licenses, the notifications are limited to 5 email notifications per day and SMS notifications are disabled, while this license increases the limit up to 100 emails per day and up to 5 SMS-es per day. Follow these steps on how to set-up notifications: **3.1.3 Notifications**.

17.1 Custom certificates

Adding the custom certificates

The option allows custom certificates to be uploaded to the master central and creates a correct introduction when accessing the application. To upload personal certificates, navigate to **Home > Settings > Other Settings**. Here you can find the option to upload multiple files. Please select all the files you have regarding certificates. The software will extract the needed information and use it to provide secure access to the central.
The custom certificates will replace the self-signed ones and ensure a secure connection to the master central.
After certificates are uploaded, the URL of the safe access will be displayed, along with the currently set common name (as shown in Picture 17-1).



Custom certificates

Currently set: ***.primasystems.si** Remove

● .pem+.chain.crt ○ .crt,.key+.chain.crt

.pem

Browse file

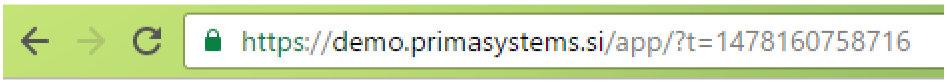
.chain.crt

Browse file

Upload

Picture 17.1: The uploaded certificates provide a secure connection to the top master central

Central access should now be displayed with the secure connection icon:



https://demo.primasystems.si/app/?t=1478160758716

Picture 17.2: Secure connection to the site (top master)

Custom certificates removal

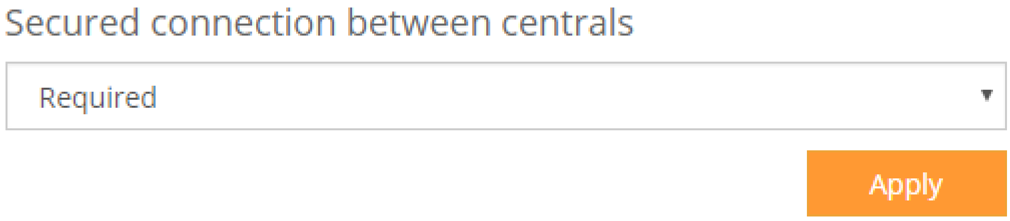
If we do not wish to keep the personal certificates on the central, they can be deleted with the press of the **Remove** button as displayed on Picture 17-1.

After the certificates are deleted, the centrals will continue to work using the default self-signed certificates.

IMPORTANT! Central reset (the left button held for more than 20 seconds) will also delete personal certificates and continue to use the self-signed ones.

17.2 Providing a secure connection between centrals

The module allows an option for a **Required** secure connection between the centrals. This ensures that there are no plain connections between the centrals. The connection uses a secure protocol TLS 1.2.



Secured connection between centrals

Required ▾

Apply

Picture 17.3: The option to ensure encrypted connections only!

IMPORTANT! Centrals with hardware version less than 3.0 do not support secure connections, so this option cannot be set until they are removed from the system.

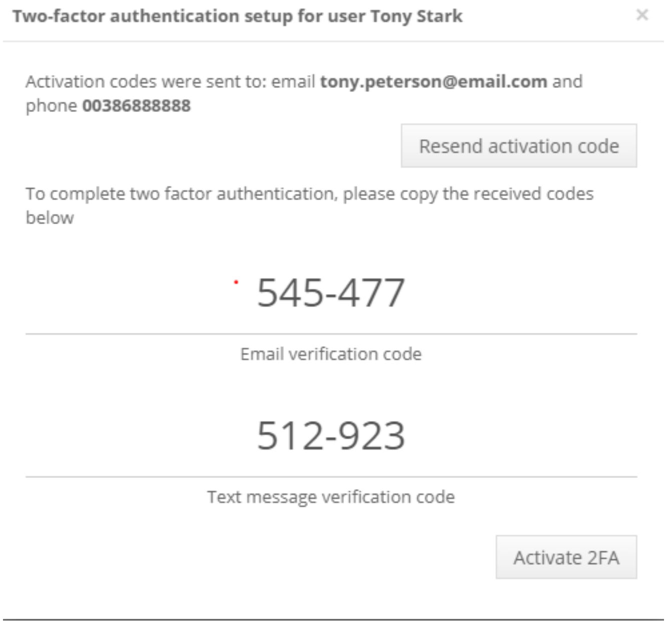
17.3 Two-factor authentication

To enable two-factor authentication:

1. Navigate to the user (top right) and from the drop-down select the **Account**.
2. Enter the **required email**.
3. Select the button to Setup 2FA.
4. A unique code will be sent to your email, copy it over to Nova's window.

Note: The code is only valid for a couple of minutes and upon expiration, you can resend them.

5. Once two-factor authentication is enabled, it can be tested by logging out and back in.



Two-factor authentication setup for user Tony Stark

Activation codes were sent to: email **tony.peterson@email.com** and phone **00386888888**

To complete two factor authentication, please copy the received codes below

Email verification code: 545-477

Text message verification code: 512-923

Picture 17.4: Two-factor authentication window

To disable Two-factor authentication:

1. Navigate to the user (top right) and from the drop-down select the **Account**.
2. Press the button **Disable 2FA**.
3. The code will be sent off to email, copy it over to disable it.

17.4 Time limited access group

The access group is created as a normal group, but if the High security module is present, a checkbox will appear where the selection can be made for this group to be only valid between set dates.

17.5 Dual access with privileged access user

The dual access changes so that at least one of the persons needs to have Privileged access set to get access. Privileged access can be set by navigating to specified user > Advanced tab > Privileged access checkmark.

17.6 Grabbing the picture from the IP camera on specified events

You can read more about it in the chapter **5.1.19 Mounting the USB storage and grabbing picture from the camera**.

18. Fire alarm module (804-00x-4010)

The fire alarm module supports the connection of one or more external alarm unit(s) to one or multiple centrals in the system. To activate this part of the software, please follow the instruction in chapter **6.1 Add-ons and Modules**.
IMPORTANT! Alarm functions only work on the online and offline readers connected via antenna!
IMPORTANT! All centrals in the system must have software version 2.1 or higher for this module to work correctly.
IMPORTANT! The alarm contact needs to be connected to general Input 2 and one of the settings below needs to be selected on the corresponding central in GUI.
To access the Alarm settings, please navigate to **Home > Hardware > Centrals > Edit central > Auxiliary I/O tab > Input 2**. For the alarm to be triggered, the Active voltage level should be set on NC (default) or NO.
IMPORTANT! Fire alarm overrides any openings, so if a door was open before according to its schedule and is now set to lock after the alarm is over, the lock will take priority.

18.1 Setting up an alarm to affect only one central

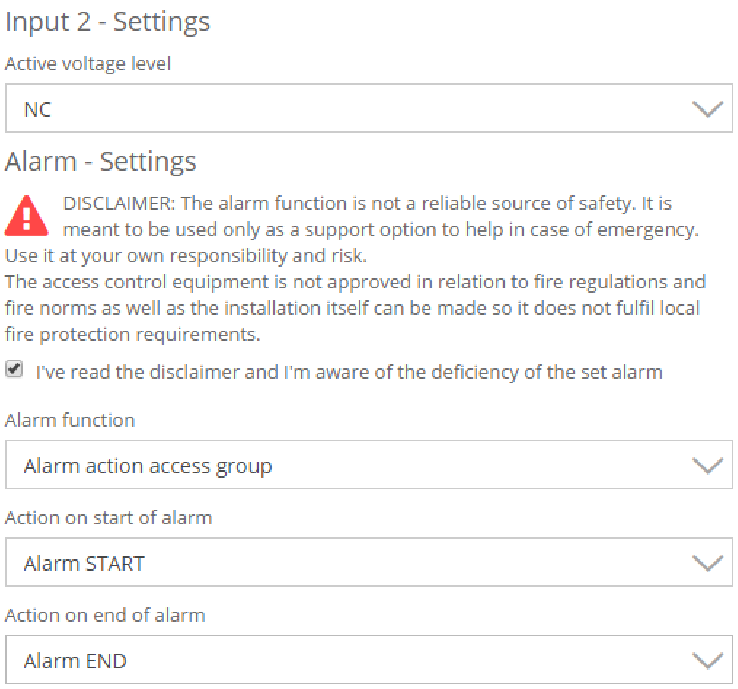
This option is free and allows the alarm to manage doors connected to that central. If the alarm is triggered, the alarm will unlock all doors on this central. Once the alarm is over, all doors will be locked.

18.2 Setting up a global alarm

Setting this will unlock all doors in the system when the alarm is triggered and then lock them when the alarm is turned off.
NOTE: Doors that were previously unlocked – manually or by schedule will **LOCK** once the alarm is over.

18.3 Setting up a custom alarm

Advanced setting that allows creating a new, special Alarm action access group with custom settings for the beginning and the end of the alarm time frame.
To create a custom alarm group, please navigate to **Home > Users & Access rights > Access groups**, and create a new group with the **Alarm action** as an access group type. The access group is assigned similarly as a standard access group with some limitations (the time is always 0-24 and actions can be set to Lock/Unlock/Block/Unblock/None). Along with the Action, custom events can also be triggered if the scripting module is applied in the system. More about the scripting module can be read in **chapter 7 Module: Scripting**.
Once the access groups are created and configured, they can be selected in the alarm's dropdown menu as shown in Picture 18-1.



Input 2 - Settings

Active voltage level

NC

Alarm - Settings

DISCLAIMER: The alarm function is not a reliable source of safety. It is meant to be used only as a support option to help in case of emergency. Use it at your own responsibility and risk.

The access control equipment is not approved in relation to fire regulations and fire norms as well as the installation itself can be made so it does not fulfil local fire protection requirements.

☑ I've read the disclaimer and I'm aware of the deficiency of the set alarm

Alarm function

Alarm action access group

Action on start of alarm

Alarm START

Action on end of alarm

Alarm END

Picture 18.1: Custom alarm with a start/end groups assigned

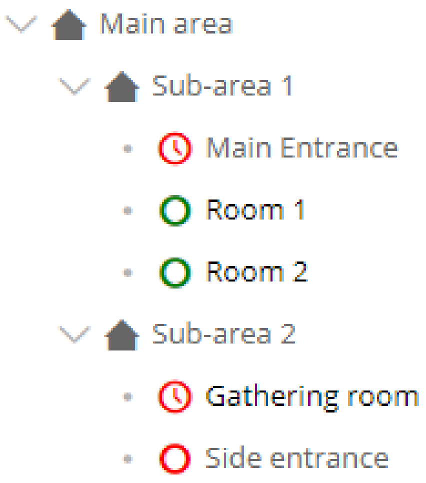
18.3.1 Setting up a custom alarm in case of terror threats

In some situations, there are special zones that we need to block. Here is an example:

Our area will be divided into two smaller areas, each covered with a different alarm signal. Each alarm covers its area and when the alarm is active, it will block all access to that sub-area.

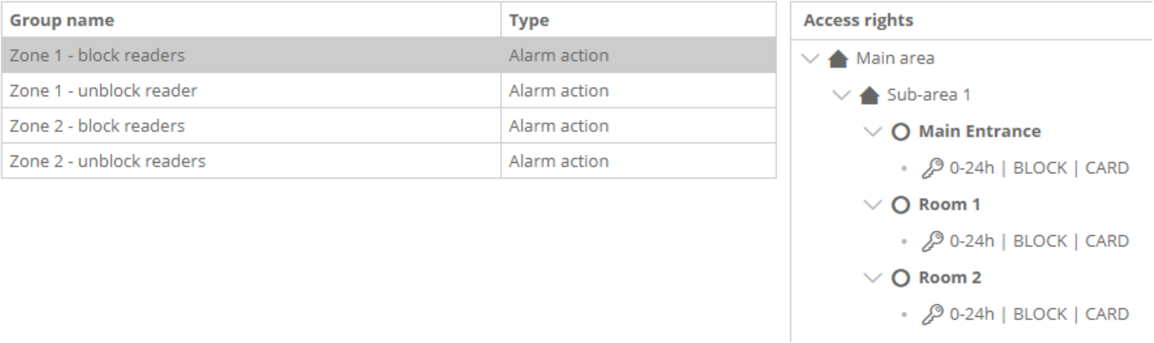
After the thread is cleared, we want to unblock all readers, so everyone authorized to have access again.

Here is a structure of the set-up:



- Main area
  - Sub-area 1
    - Main Entrance
    - Room 1
    - Room 2
  - Sub-area 2
    - Gathering room
    - Side entrance

Here are the access groups:



Group name	Type
Zone 1 - block readers	Alarm action
Zone 1 - unblock reader	Alarm action
Zone 2 - block readers	Alarm action
Zone 2 - unblock readers	Alarm action

Access rights

- Main area
  - Sub-area 1
    - Main Entrance
      - 0-24h | BLOCK | CARD
    - Room 1
      - 0-24h | BLOCK | CARD
    - Room 2
      - 0-24h | BLOCK | CARD

Picture 18.2: Access groups for Alarm action groups

Now that the access groups are created, they can be assigned to the correct central as described in chapter **18.3** for both centrals that have alarms connected.

When the alarm is active, the readers are blocked which means that no one can pass except the users who have Privileged access ~ found in chapter **4.2.3** Managing users, their access rights, and apartments.

19. Checkpoint or guard tour module (804-00x-7050)

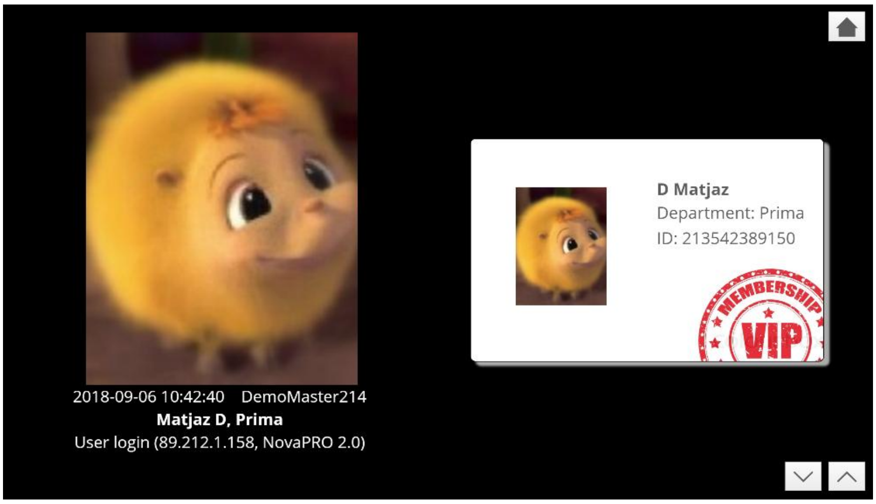
The checkpoint module supports card checks for secure facilities such as airports. There are two (2) ways to check the cards – **stationary checkpoints**, where a guard can check cards of users that pass by via predefined reader(s) or **mobile checkpoints** that allow guards with a designated mobile device to scan cards on the field.
To activate this part of the software, please follow the instruction in chapter **6.1 Add-ons and Modules**.
IMPORTANT! Master central must be upgraded with the package version 2.3 or higher for these functionalities.

Firstly, we need to set-up a **Checkpoint user(s)**. To read more about user account types and how to assign them, please read 1.1.1 Account types.

19.1 Setting up a stationary checkpoint

Once the users are created, navigate to **Settings > Checkpoint settings**.
On the top select the checkpoint user and fill out which events show as **OK** and which ones as **Error**. You can also assign sounds to any event you have selected by pressing on the **Play** button.

When the guard logs in, he can see the checkpoint widget.
When opened, the screen is black until one of the set events occurs.
At that time, the layout selected at the Default card print layout (can be changed at the user's general settings) will be displayed.



2018-09-06 10:42:40 DemoMaster214
Matjaz D, Prima
User login (89.212.1.158, NovaPRO 2.0)

D Matjaz
Department: Prima
ID: 213542389150

Picture 19.1: User's card layout displayed on the screen

Picture 19-1 shows a checkpoint preview.
There are 3 buttons:

- The home button, that navigates back to Nova
- The up/down buttons that allow us to go through card history.

NOTE: Card history is limited to 50 cards max and the cards are stored only for 10 minutes!

In the case of the **Error** event type occurring, the text from other settings will be displayed instead. Additionally, you can select a different layout and text if the card is unknown.

19.2 Setting up a mobile checkpoint

After the checkpoint users are created, the special android app must be installed on the devices capable of reading RFID cards.

After opening the app, the guard will have to login by showing their card + PIN.

The mobile app can only detect if the card is lost, deleted, expired, or the unknown card type (unauthorized or any of the offline cards).

NOTE: In the app, the person responsible has to set-up the IP of the top master central. These settings are locked behind a set PIN, so the normal user does not have access to them.

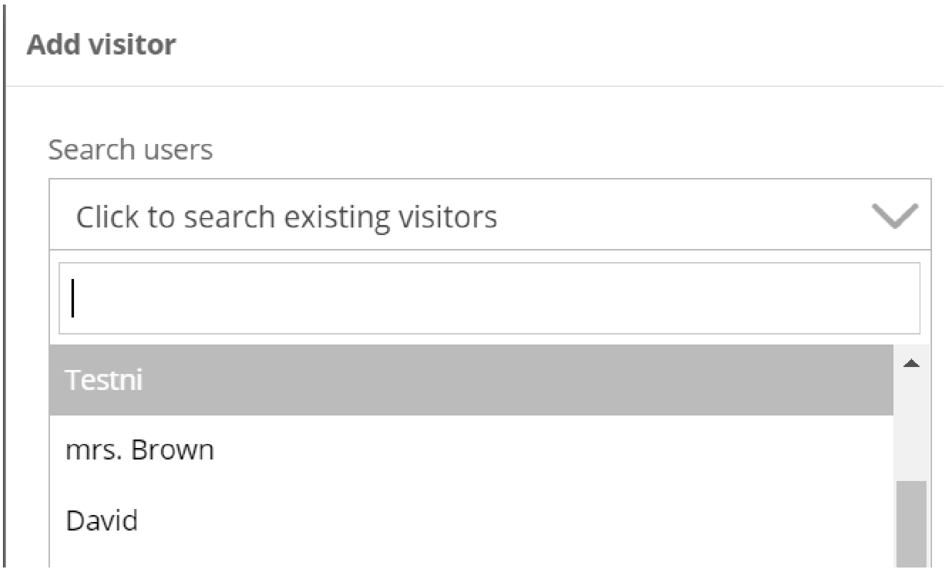
20. Visitor manager module (804-00x-5310)

IMPORTANT! For this module, you need special hardware – **USB desktop reader.** There is more information about USB desktop reader described in chapter **23.5 USB desktop reader.**

This module is locked by default and can be activated with an activation code. To do so, please follow the instruction in chapter **6.1 Add-ons and Modules**.
IMPORTANT! Master central must be upgraded with the package version 2.3 or higher for these functionalities.

To create the visitor manager:

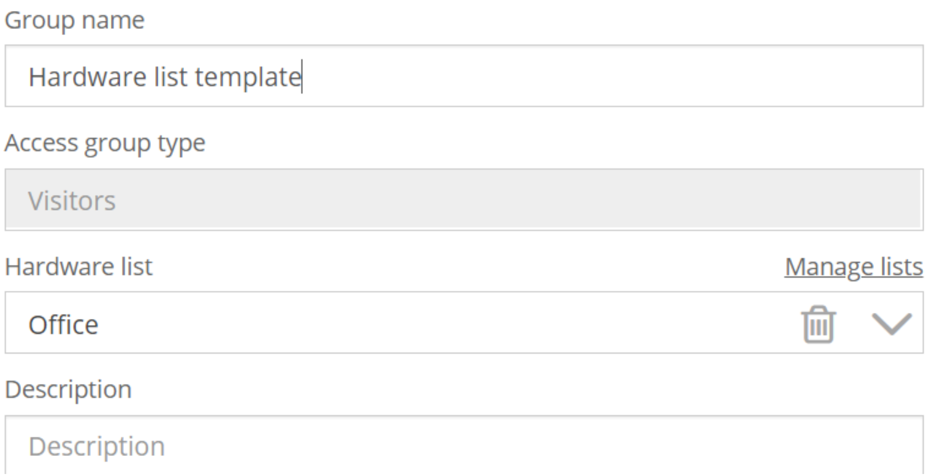
1. Navigate to **new user creation**.
2. After the user is created, navigate inside his settings, and select tab **Account**
3. Change its **Account type** to **Visitor manager**
    a. (Not required) selection of the user/hardware list – by default no list is selected which means that all users, new users (created by visitor manager) and all visitor access groups will be displayed to the manager.



Add visitor

Search users

By selecting the user list, the manager will only see people he created + users from the selected user list will be displayed



Group name

Hardware list template

Access group type

Visitors

Hardware list

Office

Description

Description

By selecting the hardware list, only access groups that are included on the Hardware list will be displayed

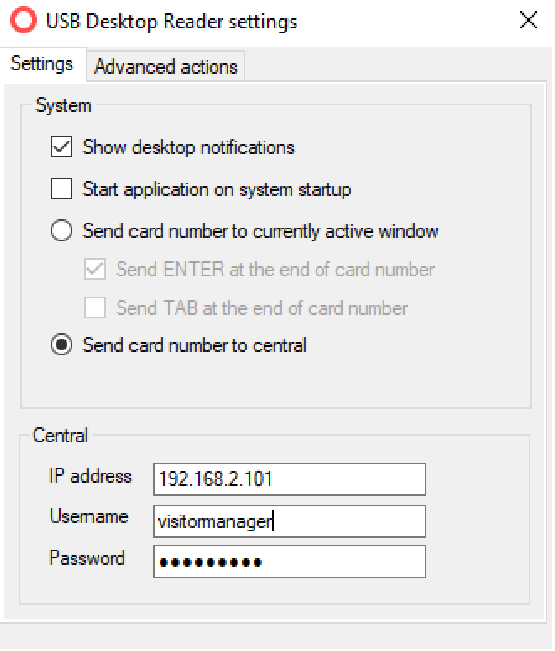
To learn more about the lists, please read **14.1.1 User list(s)** and **14.1.2 Hardware list**.

4. Provide login credentials.

Create different access groups that he can assign:

1. Create a **new access group**, make sure to select **Visitor** as **Access group type**.
2. Assign access rights accordingly (for the visitors).

Run USB reader software and navigate to its settings (right mouse click on the red circle near the clock). Make sure that **Send card number to central** is selected. Fill in the central's IP and Visitor manager's credentials.



System

☑ Show desktop notifications

□ Start application on system startup

○ Send card number to currently active window

☑ Send ENTER at the end of card number

□ Send TAB at the end of card number

● Send card number to central

Central

IP address: 192.168.2.101

Username: visitormanager

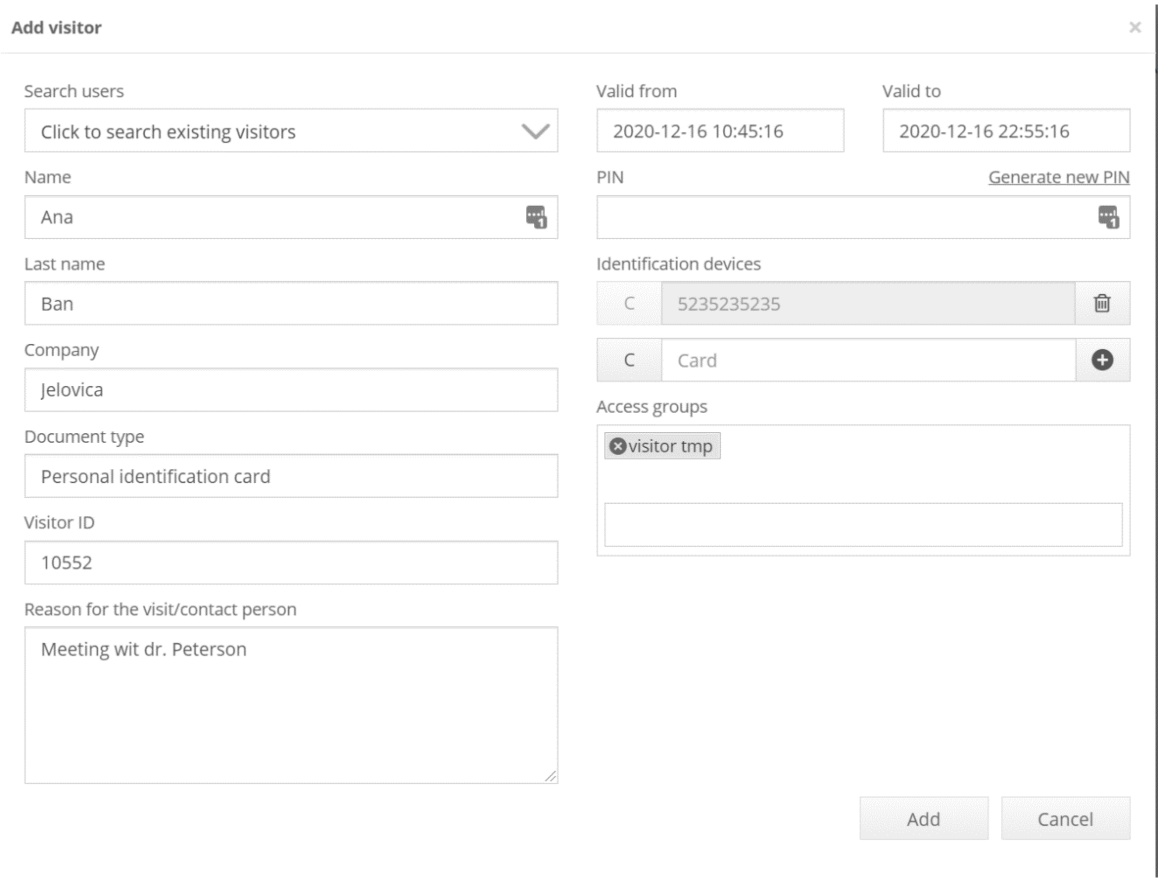
Password: •••••••••

Picture 20.1: USB desktop reader's setting for visitor manager

Open Nova and use its credentials to log in.

Workflow:
Once the manager presents the Unknown card to the USB reader, a new pop-up window will appear asking for data (like new user creation).

- The manager can also manually add/create users by clicking on **Menu > Add visitor**.



Add visitor

Search users: Click to search existing visitors

Name: Ana

Last name: Ban

Company: Jelovica

Document type: Personal identification card

Visitor ID: 10552

Reason for the visit/contact person: Meeting wit dr. Peterson

Valid from: 2020-12-16 10:45:16

Valid to: 2020-12-16 22:55:16

PIN:

Identification devices: C 5235235235

Access groups: visitor tmp

Picture 20.2: New visitor window

<u>The visitor will be added to the manager's list.</u>

Later, when this visitor comes back and returns the card to the Manager must show to the USB again which will bring up the filled window, prompting for visitor removal.

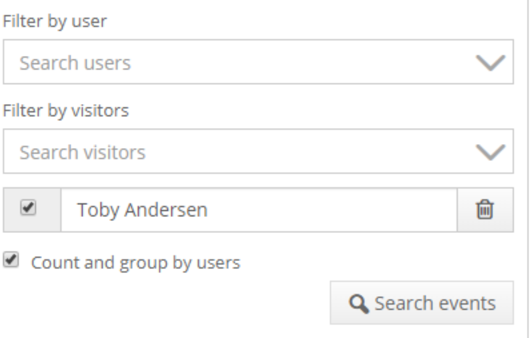
- A visitor can also be removed manually by selecting (double click) it from the list and pressing the **Remove visitor** button.

The next time the visitor's card is presented to the USB reader, it will be presented as a new card, ready to be assigned to the next visitor.

20.1 Visitor history

Admin or Sysadmin can check the event history and are able to filter specific visitor's events.

If the visitor comes on multiple days and the name was entered correctly every time, the event history will list all visitor’s activity from different days.



Filter by user

Search users

Filter by visitors

Search visitors

☑ Toby Andersen

☑ Count and group by users

Picture 20.3: Event history allows displaying events from visitors too

21. Messaging module(804-00x-7202/7205/7225)/Communications module(804-00x-7402/7405/7425)

This module is locked by default and can be activated with an activation code. To do so, please follow the instruction in chapter **6.1 Add-ons and Modules**.
IMPORTANT! Master central must be upgraded with the package version 2.3 or higher for these functionalities.

NOTE: The **messaging modul**e is used for **sending** the message(s), while the **communications module** brings the **option to reply** to a received message (usually via some poll/confirmation buttons).

21.1 Email messages

IMPORTANT! The **email and SMTP server settings** in the **other settings** must be filled! For more information read chapter 6.4.4 Email and SMTP server settings.

Navigate to **Messages > Menu > New email message.**

When pressing the drop-down or the user search button, it will only show the ones who updated their email address in black.

Emails can also be sent to a list of users – Clicking on the list button will bring up the existing user list. To read more about how to create user lists, read chapter **14.1.1 User list(s)**.

21.2 Apartment messages

IMPORTANT! Special display hardware (AT – Apartment terminal) is required for the messages to be displayed.

Users created by the AT are counted differently, and if there is even one present in the system, the **Apartment terminals** option will show up in Nova. From there, apartments can be added to the apartment list.

To send a message, navigate to **Messages > Menu > New apartment message.**

From there, only AT users will be displayed. A message to multiple apartments can be sent by clicking on the list button and selecting the wanted list(s)

21.3 Info board messages

IMPORTANT! Special hardware – info board is required for the messages to be displayed.

To send a message, navigate to **Messages > Menu > New info board message.**

The messages sent to the info board will be displayed within the **Message** field. This makes everything more convenient since the layout does not have to be changed every time a new message is sent onto it.

Additionally, timed messages can be created. A timed message has a higher priority than a regular message, so whenever a timed message is in effect, it will be displayed instead of the regular message. After the timer runs out, the regular message will be displayed again. In case that multiple timed messages overlap, the more recent one will have a higher priority.

22. Prima DoorApp (804-00x-2325/2310/2350)

This module adds support for door opening by placing the phone on the **Nexus online readers**. Depending on the number of phones used to get access, the DoorApp module must match or exceed that number (for example DoorApp 25 can have up to 25 phones registered). Each user can have up to 5 phones assigned (if so, it will still count as 5 used phones).

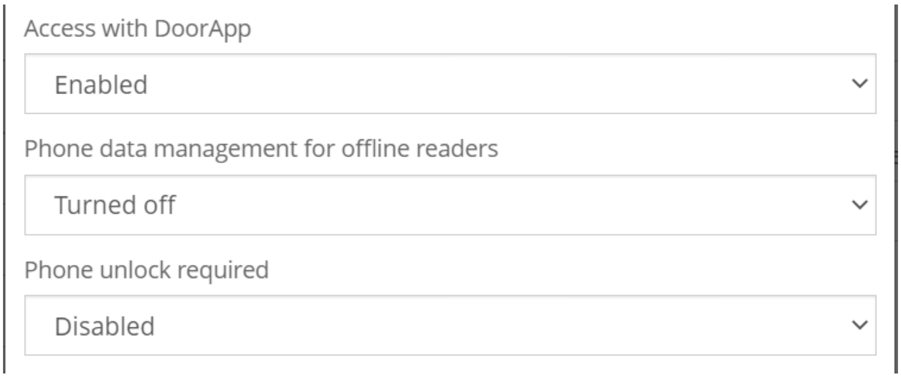
Prerequisites:

- The system must be upgraded to Nova 3.0+
- Reader's software must be upgraded to firmware 30 or above
- Android download: The application can be downloaded from Google Play store: https://play.google.com/store/apps/details?id=si.primasystems.doorapp&hl=en
- Apple download link: https://apps.apple.com/us/app/prima-doorapp/id1619287068
- When pairing over email, the central **it is recommended to have a working domain**, either via cloud connection or customer's own domain.

22.1 Reader set up

Navigate to the reader's advanced settings:

1. Make sure that the Access with DoorApp is **Enabled**.
2. Open the app on the phone and follow the steps. If any of the steps fail during pairing, just repeat the process until you get a positive result.
3. Phone unlock required – for better security; if phone gets lost, someone can use it to unlock the door. If the option is enabled, they need to provide a pattern or a biometric scan before they are allowed to open the door.



Access with DoorApp: Enabled

Phone data management for offline readers: Turned off

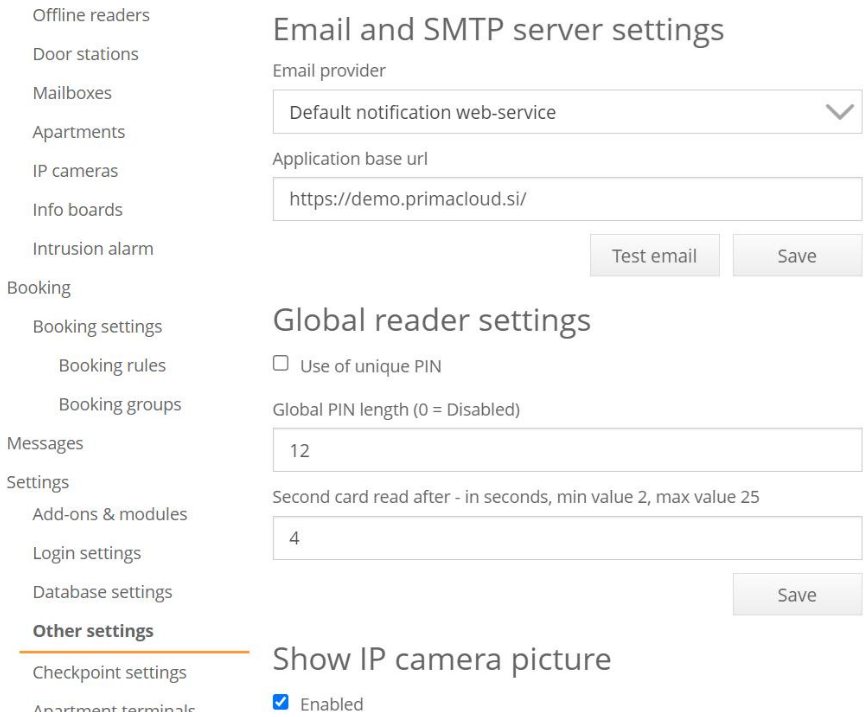
Phone unlock required: Disabled

Picture 22.1: Make sure that settings in the reader's advanced options are enabled

22.2 E-mail pairing

1. Make sure that top master central (or server) has access to the internet.
2. A valid domain to the master is recommended.

3. Navigate to Settings > Other settings > Email and SMTP server settings and provide the cloud access name or domain or public IP for the Application base URL.



Email and SMTP server settings

Email provider: Default notification web-service

Application base url: https://demo.primacloud.si/

Global reader settings

□ Use of unique PIN

Global PIN length (0 = Disabled): 12

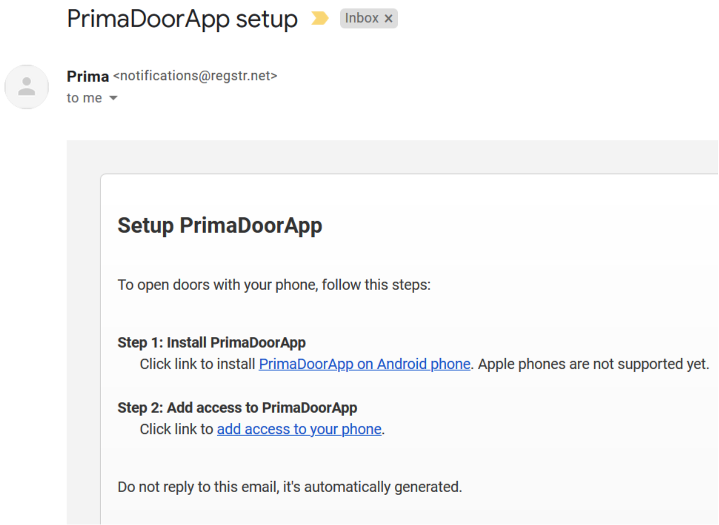
Second card read after - in seconds, min value 2, max value 25: 4

Show IP camera picture

☑ Enabled

Picture 22.2: Provide the Application base URL

4. Navigate to a user and make sure that their email is provided.
   Press **pair a phone** button that will send out an e-mail with instructions.
5. Open the e-mail on the phone and follow the instructions.



PrimaDoorApp setup

Prima <notifications@regstr.net>
to me

Setup PrimaDoorApp

To open doors with your phone, follow this steps:

Step 1: Install PrimaDoorApp
Click link to install PrimaDoorApp on Android phone. Apple phones are not supported yet.

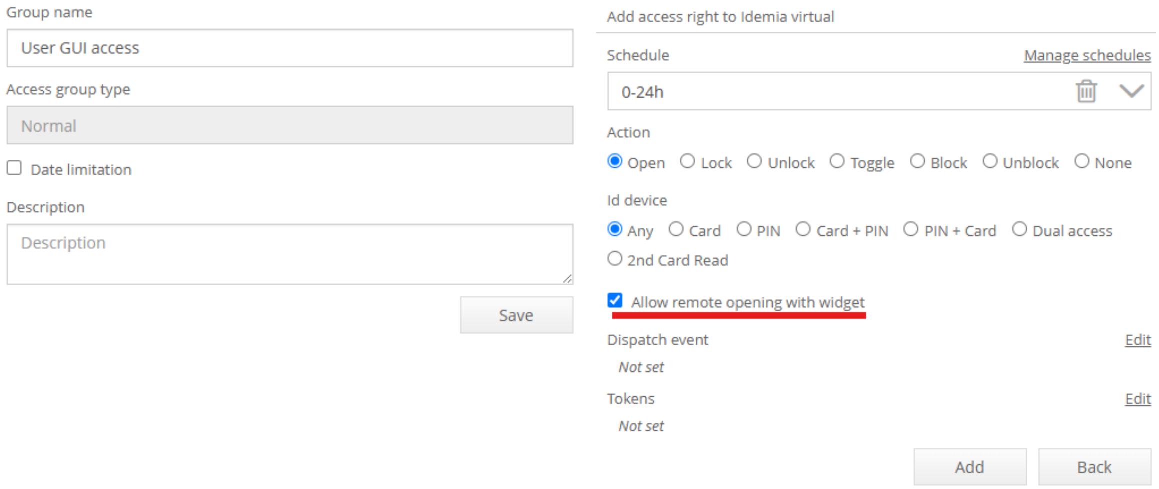
Step 2: Add access to PrimaDoorApp
Click link to add access to your phone.

Do not reply to this email, it's automatically generated.

Picture 22.3: DoorApp email example

22.3 Access group set up

By default, access group that unlocks all doors does not allow remote opening, to only allow specific users to be able to remotely open the set door.
When creating a new access group and granting access to specific online door, you will have a special checkmark to allow door remote opening.



Group name

User GUI access

Access group type

Normal

□ Date limitation

Description

Description

Save

Add access right to Idemia virtual

Schedule — Manage schedules

0-24h

Action

● Open ○ Lock ○ Unlock ○ Toggle ○ Block ○ Unblock ○ None

Id device

● Any ○ Card ○ PIN ○ Card + PIN ○ PIN + Card ○ Dual access ○ 2nd Card Read

☑ Allow remote opening with widget

Dispatch event — Edit

Not set

Tokens — Edit

Not set

Add Back

Picture 22-1 Access group ALL does not support remote opening.

IMPORTANT! The NFC antenna is located on the backside of the phone (different phones have different NFC antenna location), so make sure that your phone's backside is facing the Nexus reader. The ideal position is 1 cm off reader in parallel, with nothing in-between them.

IMPORTANT! NFC on apple is not working, but you can still open doors with the widget or Bluetooth (Bluetooth reader is required).

If the phone is not yet registered in the system, it will act like an unknown card – a banner will show up to add it to the selected user.

Once paired, the phone should open doors on all readers that have DoorApp access enabled and users are also required to have access to that door.

22.4 Remote doors

When a user is assigned access group with the new access group rights that allows remote opening with widget checkmark, they can navigate to the remote door area, and all the doors they have access to will be shown and they can decide which doors will be shown in their favorites area. Admin and sysadmin's account has access to all doors, so all the doors will be displayed by default.

22.5 Widgets

Widgets are only available if they are done by admin/sysadmin for themselves or other users. When Elevator/Alarm/Presence/Mailbox/Web-Link widget is created, a user can then add them inside the app, the same way they can assign remote doors.

23. Nova Remote Access (122-00x-1031)

This module allows the end user to choose their own URL name to access their system, while we provide the requested certificates for the domain. Since the certificates need to be renewed every so often, this license is also charged upon renewal.

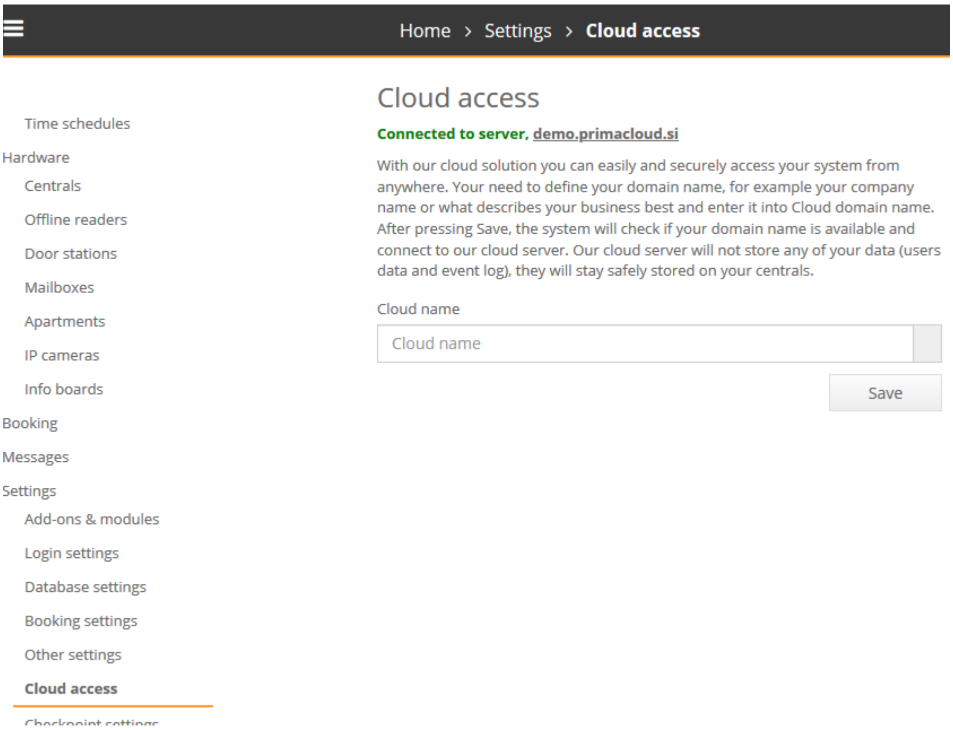
IMPORTANT! Make sure that master central's/server's network settings are correct (gateway and DNS).

Note: When the license expires, the certificates will expire too, but **the system will still work and it will still be accessible from the local network**.

Note: Since the service uses standard ports to access the cloud server, **no modem/access point port forwarding is required!**

How to set-up a name:

- Make sure that you are logged on the master central/server.
- Make sure that the Cloud access license was entered.
- Make sure that the master central/server has access to the internet (gateway and DNS should be working).
- Navigate to **Settings > Cloud access** and provide a cloud name.
  The system will then test if the name is available. If the name is already in use, an error will be reported, prompting for a name change.
- Once a successful connection is established, the connected to text will turn green and provide you with a public link you can use.



Cloud access

Connected to server, demo.primacloud.si

With our cloud solution you can easily and securely access your system from anywhere. Your need to define your domain name, for example your company name or what describes your business best and enter it into Cloud domain name. After pressing Save, the system will check if your domain name is available and connect to our cloud server. Our cloud server will not store any of your data (users data and event log), they will stay safely stored on your centrals.

Cloud name: Cloud name

Picture 23.1: Successful Cloud access connection

The cloud name can be changed by providing a new name in the text field below.

What happens if the master central is changed/damaged/replaced?
Since the cloud server remembers which central/server registered the cloud name, if the master central/server is replaced/exchanged, the name will still be reserved for the previous hardware and the cloud server will report **Cloud name already in use**. In such case, please inform the system installer about the issue, so we can delete the old settings and you will be able to re-register the name again.

To disable cloud access, leave the cloud name empty and press Save.

24. Nova Remote Access Lite (122-00x-1030)

This module is the same as the regular module, but it is designed only for a single central system.
Its set-up is the same, so please follow the procedure from the previous chapter.

25. Nova Connect (122-00x-9110/9111/9112)

This module allows the communication connection to be established over the cloud server. The cloud server is hosted by the manufacturer (in multiple states to reduce latency), but it can also be purchased and set-up for the customer and use it only for their large system.

What are the benefits of this connection?

- If the master and the slave centrals are not in the same network, the installer must do a port-forwarding to get them connected. To avoid the nuisance of reconfiguring the router, the installer can establish a connection over the cloud server by just uploading this configuration to the slave central.
- Installations where there is no network access, there is a possibility to connect the central to 3G/4G network and make it work over the cloud.

IMPORTANT! Make sure that master central's/server's and slave's network settings are correct (**gateway AND DNS**).

IMPORTANT! If there are some connection issues, please contact the network administrator and let them know that the TCP port 3553 should be opened.

There are two ways of setting up the system:

25.1 Pre-setting the connections

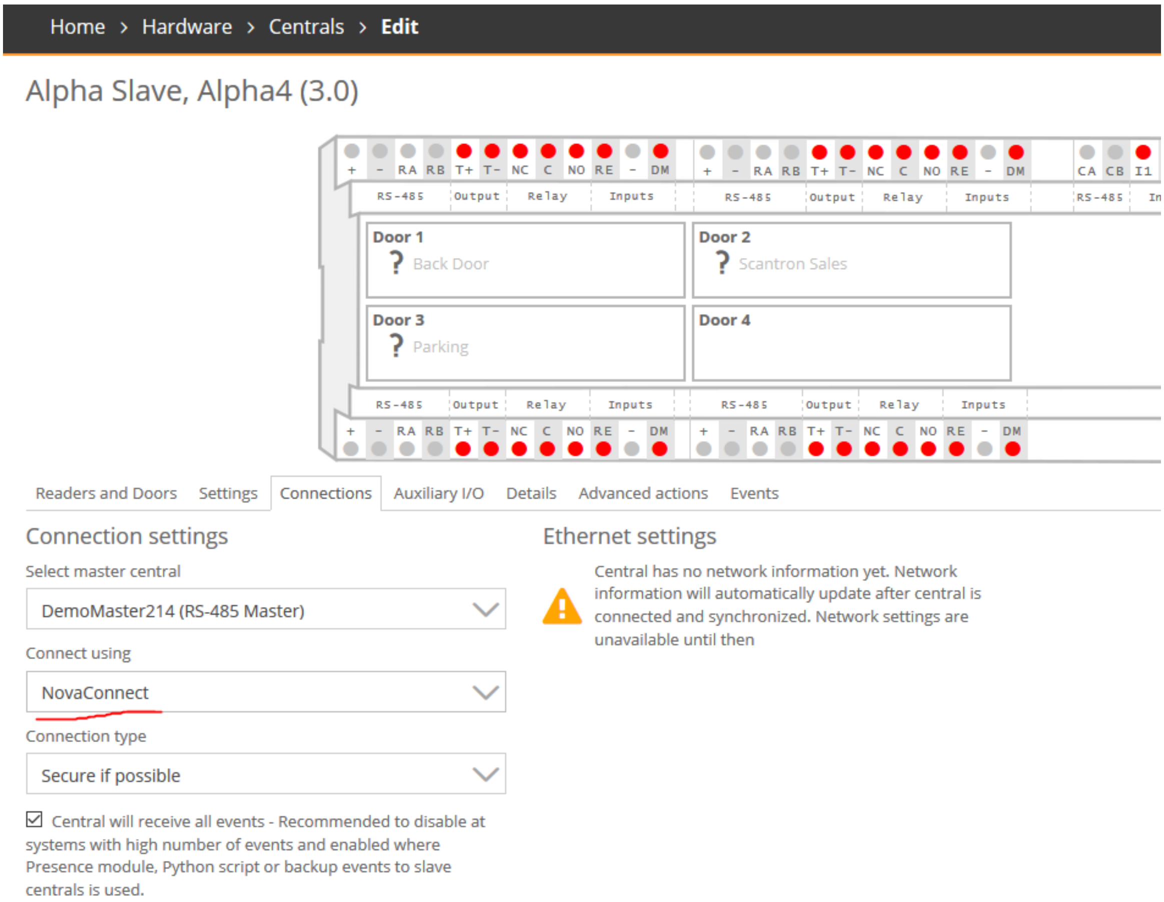
The point of this set-up is to create a working system in the working environment as online and then uploading the connections to Nova Connect. This way when the centrals are transferred to the customer, they already have the correct database and settings, just the network settings will need to be updated.

How to set it up:

- Set up the system as online and connect the centrals via IP.

Once the system is online, provide the Nova Connect license.

Go to slave central's connection settings and switch Connect using IP to Nova Connect.



Home > Hardware > Centrals > **Edit**

Alpha Slave, Alpha4 (3.0)

Readers and Doors | Settings | Connections | Auxiliary I/O | Details | Advanced actions | Events

Connection settings

Select master central: DemoMaster214 (RS-485 Master)

Connect using: NovaConnect

Connection type: Secure if possible

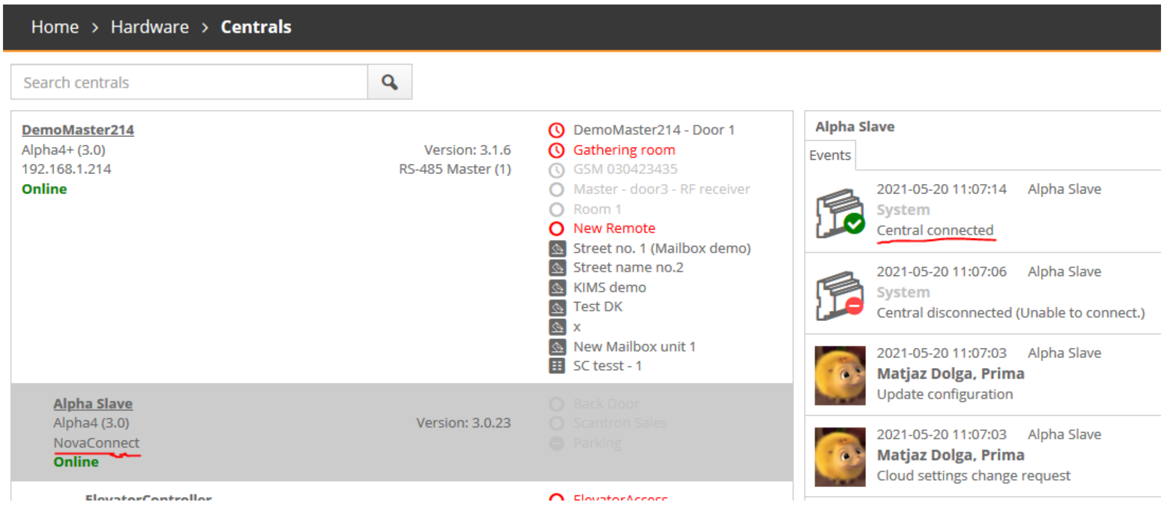
☑ Central will receive all events - Recommended to disable at systems with high number of events and enabled where Presence module, Python script or backup events to slave centrals is used.

Ethernet settings

Central has no network information yet. Network information will automatically update after central is connected and synchronized. Network settings are unavailable until then

Picture 25.1: Switching connection type to Nova Connect

Save settings and wait for re-connect (in a few seconds).



Home > Hardware > **Centrals**

Search centrals

DemoMaster214
Alpha4+ (3.0)
192.168.1.214
Online
Version: 3.1.6
RS-485 Master (1)

DemoMaster214 - Door 1
Gathering room
GSM 030423435
Master - door3 - RF receiver
Room 1
New Remote
Street no. 1 (Mailbox demo)
Street name no.2
KIMS demo
Test DK
x
New Mailbox unit 1
SC tesst - 1

Alpha Slave
Alpha4 (3.0)
NovaConnect
Online
Version: 3.0.23

Back Door
Scantron Sales
Parking

ElevatorController
ElevatorAccess

Alpha Slave

Events

2021-05-20 11:07:14 Alpha Slave
System
Central connected

2021-05-20 11:07:06 Alpha Slave
System
Central disconnected (Unable to connect.)

2021-05-20 11:07:03 Alpha Slave
Matjaz Dolga, Prima
Update configuration

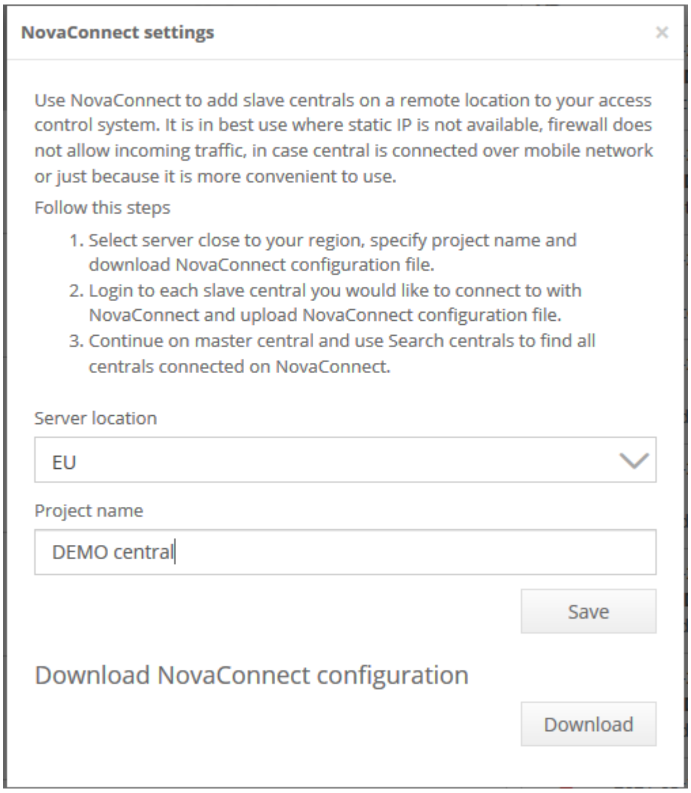
2021-05-20 11:07:03 Alpha Slave
Matjaz Dolga, Prima
Cloud settings change request

Picture 25.2: Central connected with Nova Connect.

Disconnect the central and take it to the remote site and make sure that the network settings of the central is the same as on the remote site.
Once the central gets access to the internet, it will automatically connect to the cloud server and then to top master.

25.2 Uploading settings on remote site

1. Set-up the top master central/server.
2. Navigate to Centrals, click on Menu > Nova Connect settings.
3. From the dropdown select a server closer to you and provide a project name, save, and download a file to PC/USB stick.



NovaConnect settings

Use NovaConnect to add slave centrals on a remote location to your access control system. It is in best use where static IP is not available, firewall does not allow incoming traffic, in case central is connected over mobile network or just because it is more convenient to use.

Follow this steps

1. Select server close to your region, specify project name and download NovaConnect configuration file.
2. Login to each slave central you would like to connect to with NovaConnect and upload NovaConnect configuration file.
3. Continue on master central and use Search centrals to find all centrals connected on NovaConnect.

Server location

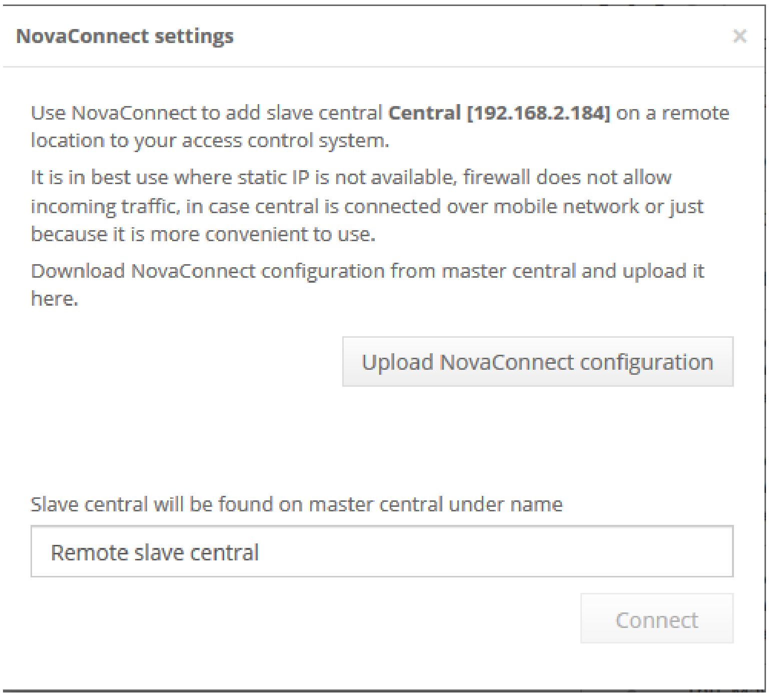
EU

Project name

DEMO central

Picture 25.3: Top master Nova Connect settings.

- Install the slave central in remote location and login, navigate to Hardware > Centrals, Menu > Nova Connect settings.



Use NovaConnect to add slave central **Central [192.168.2.184]** on a remote location to your access control system.

It is in best use where static IP is not available, firewall does not allow incoming traffic, in case central is connected over mobile network or just because it is more convenient to use.

Download NovaConnect configuration from master central and upload it here.

Slave central will be found on master central under name

Remote slave central

Picture 25.4: Nova Connect settings on the slave central

Go back to top master and trigger a central search, remote centrals will show up on the list too and can be added the same way as the regular ones.

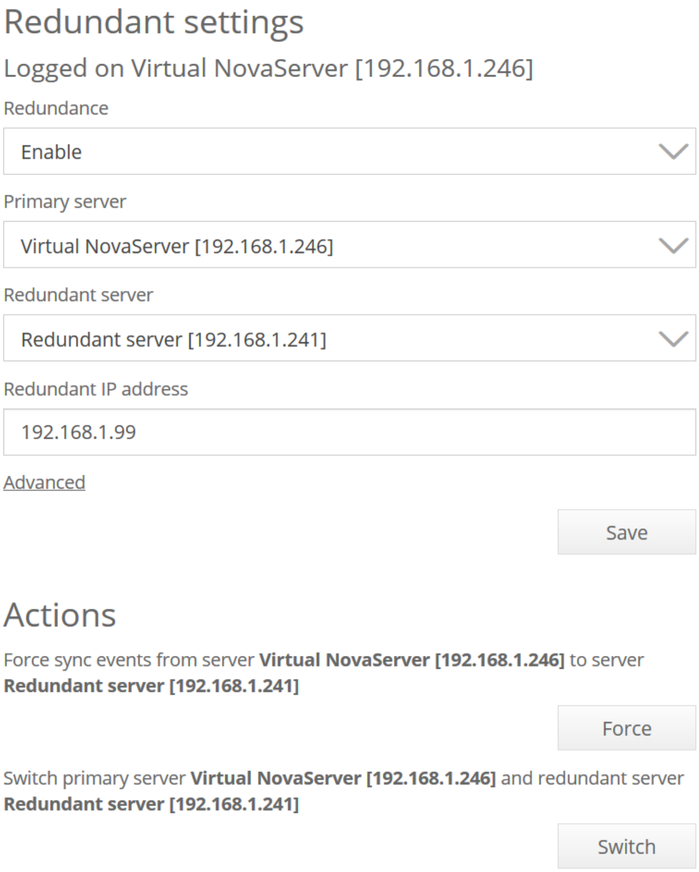
26. Redundant NovaServer (804-00x-1550)

This module assigns another central/NovaServer to be a temporarily promoted top master until it is fixed/replaced.
Additionally, if there are 2 NovaServers (top and redundant), all the files that are uploaded are also copied over to the redundant one.
WARNING! **If a central is set as a redundant device, THE FILES UPLOADED TO MASTER WILL NOT BE COPIED TO THE REDUNDANT CENTRAL**.

NOTE: It is strongly recommended that the 2 servers have a high-speed communication for the faster file sync.

Redundant server set-up:

1. Navigate to Settings > Redundant settings.
2. Select **Enable redundance** from the dropdown menu.
3. Select which should be primary (top) server and which should be redundant from the dropdown menu.
4. Select a **redundant IP address** – when the administrator accesses this IP, it will access the top master or redundant server if the top master is not available. The system will continue to work normally without any interruptions.



Redundant settings

Logged on Virtual NovaServer [192.168.1.246]

Redundance: Enable

Primary server: Virtual NovaServer [192.168.1.246]

Redundant server: Redundant server [192.168.1.241]

Redundant IP address: 192.168.1.99

Actions

Force sync events from server **Virtual NovaServer [192.168.1.246]** to server **Redundant server [192.168.1.241]**

Switch primary server **Virtual NovaServer [192.168.1.246]** and redundant server **Redundant server [192.168.1.241]**

Picture 26.1: Redundant server settings

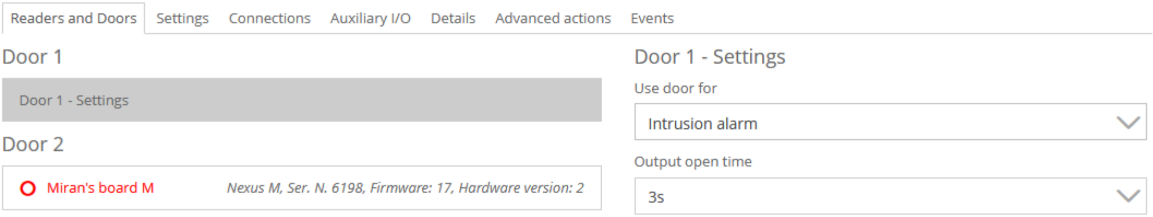
Actions:

- Force sync events from top server to redundant one – by default, the system already handles event syncing, but if something strange were to happen on the network and we want to make sure that the servers have the same event database we can press this button to ensure it.
- Switch button – this button comes into play when the top master is not available any more (either malfunction or network issues…). Now the redundant server is set as top master and will stay until the top master is fixed, up and running. Once it is, we can press the Switch button to access the top master when accessing redundant IP.

27. Intrusion alarm module (804-00x-4100)

This module allows users to manage their alarm activation/deactivation from Nova software. Users can manage a single/multiple alarm areas from a single/multiple reader(s) depending on set-up.

IMPORTANT! Door socket relays and inputs **will not be displayed on the intrusion alarm's settings by default**. You can specify in advance that the door socket will be used for intrusion alarm. You can do so by navigating to wanted central, select the wanted door and from the central's overview from the right column select from the first drop-down **to use the door for the intrusion alarm** (Picture 27.1). After door settings are set and saved, navigate back to the Alarm area's settings and the inputs/relays should be included in the drop-down menu.



Door 1

Door 1 - Settings

Door 2

○ Miran's board M   Nexus M, Ser. N. 6198, Firmware: 17, Hardware version: 2

Door 1 - Settings

Use door for: Intrusion alarm

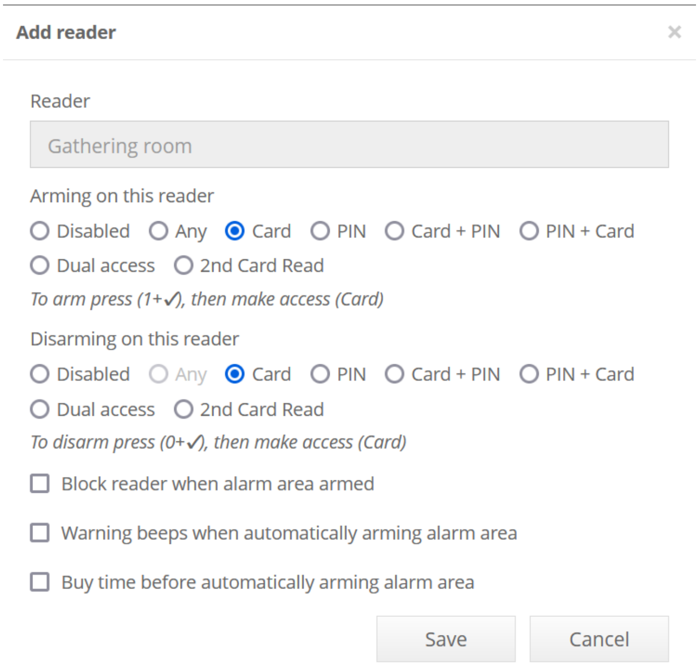
Output open time: 3s

Picture 27.1: Door reserved for intrusion alarm

How to set up the alarm area:

1. Navigate to Hardware > Intrusion alarm and press Menu > Add intrusion alarm area and provide a suitable name.
2. **Alarm area ID** is used in sequence while arming/disarming an alarm area if there are multiple areas assigned the same reader.
3. **Host central** determines to which central the alarm device is connected.
4. **Alarm area status feedback** – some alarm devices give some kind of signal or acknowledgment that the alarm is ready to be set. Use "Not set" if the device does not support this function, otherwise "Input I1/Input I2/REX or DM from intrusion alarm door" depending on where the feedback is connected.
5. **Key switch output –** determines the output on the Host central where the alarm device connected.
6. **Automatic arming schedule –** if the automatic opening schedule is assigned, as soon as the system finishes the locking procedure, it will also enable automatic alarm and when it is scheduled for automatic unlock, it will disable the alarm too. If this is not suitable, a new arming schedule can be created and assigned.
7. **Pre-warning duration –** if set, a beeping sound will emit from the reader until the alarm turns on.
8. **Time buying –** if enabled, users that are still in the facilities can present their card to the reader (this reader must be part of the alarm area), to postpone alarm activation for a set time (it can be done multiple times and by multiple people, but the delay always counts from the any user's last "check-in").

Adding readers to alarm area:
Navigate to **Alarm area's - Readers tab** and press **Menu > Add reader**, a pop-up will show up with different options as shown on Picture 27.2.



Add reader ×

Reader

Gathering room

Arming on this reader

○ Disabled ○ Any ● Card ○ PIN ○ Card + PIN ○ PIN + Card
○ Dual access ○ 2nd Card Read

To arm press (1+✓), then make access (Card)

Disarming on this reader

○ Disabled ○ Any ● Card ○ PIN ○ Card + PIN ○ PIN + Card
○ Dual access ○ 2nd Card Read

To disarm press (0+✓), then make access (Card)

□ Block reader when alarm area armed

□ Warning beeps when automatically arming alarm area

□ Buy time before automatically arming alarm area

Save Cancel

Picture 27.2: Alarm reader's settings

Reader must be selected from the drop-down menu.

Arming on this reader can be enabled by selecting one of the options from the radio menu. Some features are only supported on some reader types (MK or MKW readers are required for any PIN combination);
Note: Most of PIN features might be disabled if there is a High Security module in the system.

Arming examples:
On a **keyboard reader**, then you will need to **press 1(arm) and ✓(check) and the user identification (which was selected in the previous step)**.
On a **regular reader**, you need to **hold the card on the reader until it reads it the second time** and the alarm area will arm.

NOTE: If there are multiple alarm areas assigned to a specified reader, the arming sequence will be: **1(arm), Alarm area ID, ✓(check) and the user identification.**

Disarming on this reader can be set similar way as arming but instead **0(disarm) needs to be pressed, then ✓(check) and then the user identification (PIN/card)**.

On the readers without keyboards, double card read can be used.

NOTE: If there are multiple alarm areas assigned to a specified reader, the disarming sequence will be: **0(disarm), Alarm area ID, ✓(check) and the user identification.**

IMPORTANT! If there is an error while arming the area, there will be a clear sound signal (refer to Table 27-1 for detailed sound and visual descriptions), someone needs to check why the alarm could not be triggered and retry to arm the area.

Block reader when alarm area is armed – When enabled, if the alarm area is armed, all the area assigned readers will be blocked. This means the access will be denied for the regular users without alarm permissions.

Warning beeps when automatically arming alarm area – If the pre-warning duration for the alarm area is set, you can choose here for the reader to remain silent during that time.

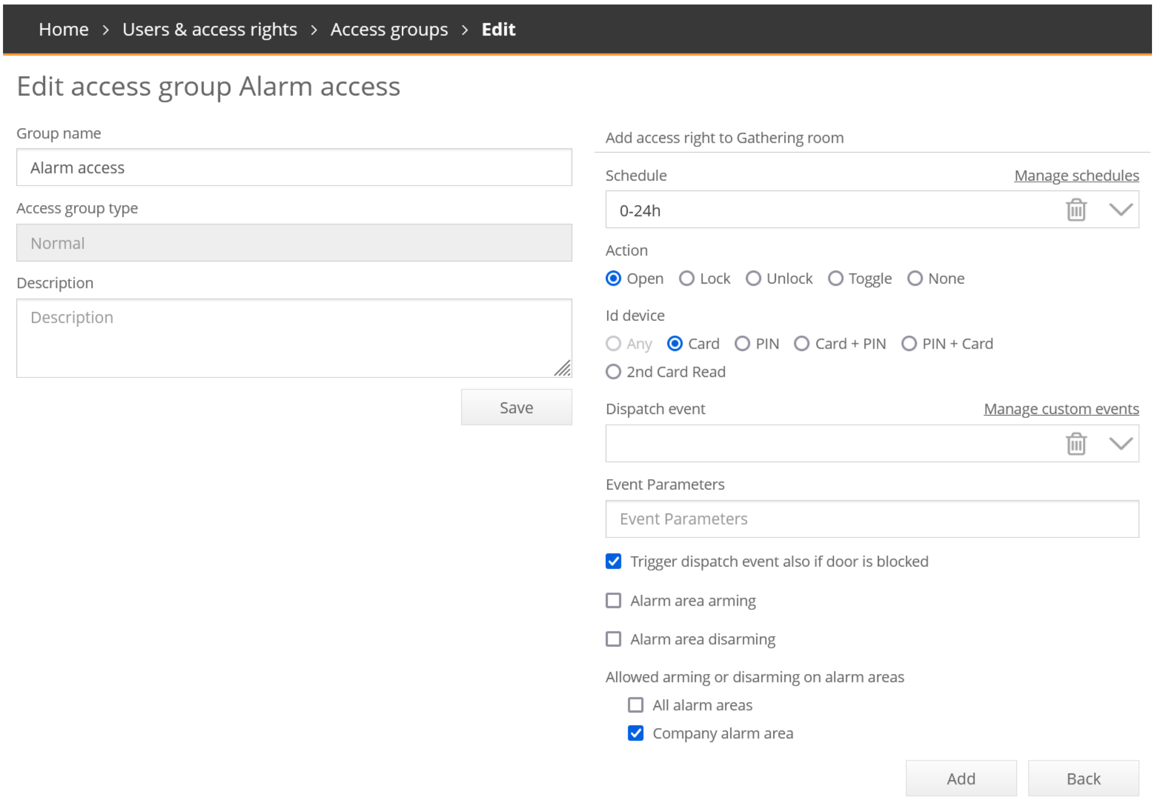
Buy time – If buying time is enabled, users with access can extend the alarm area arming time on this reader.

Error description	Sound from the reader	Reader LED response
Reader blocked	_	red ON
	To be updated!	

Table 27-1: Description of alarm reader sounds and visuals

How to define alarm administration eligibility?

To distinguish users that will have the option to arm/disarm the alarm, you can create a new access group and while adding access rights to the alarm reader, there are some additional options to choose from as shown on Picture 27.3.



Home > Users & access rights > Access groups > **Edit**

Edit access group Alarm access

Group name: Alarm access

Access group type: Normal

Description: Description

Add access right to Gathering room

Schedule: 0-24h

Action: ● Open ○ Lock ○ Unlock ○ Toggle ○ None

Id device: ○ Any ● Card ○ PIN ○ Card + PIN ○ PIN + Card ○ 2nd Card Read

Dispatch event:

Event Parameters: Event Parameters

☑ Trigger dispatch event also if door is blocked

□ Alarm area arming

□ Alarm area disarming

Allowed arming or disarming on alarm areas

□ All alarm areas

☑ Company alarm area

Picture 27.3: Additional settings for alarm reader

Only the readers included in the alarm area will have these additional options:
Alarm area arming will allow users with this group to arm the alarm area.
Alarm area disarming will allow users with this group to disarm the alarm area.
All alarm areas activation will allow the users to arm/disarm (based on the previous settings) all alarm areas assigned to that reader. If the reader only has a single alarm area, only one will be shown as displayed on Picture 27.3.
If there are multiple assigned and only a couple of the areas are selected, they can only manage the chosen ones.

IMPORTANT! If the alarm area reader is set to unlock on a schedule, it will stay locked until someone disables the alarm for the first time. After that, if it is within the scheduled unlock time, the reader will unlock as expected.

28. Special hardware

28.1 Elevator controller

The elevator controller is based on the regular Alpha central and has support for controlling access for up to ten floors by activating only those floor buttons in the elevator to which the user has access.

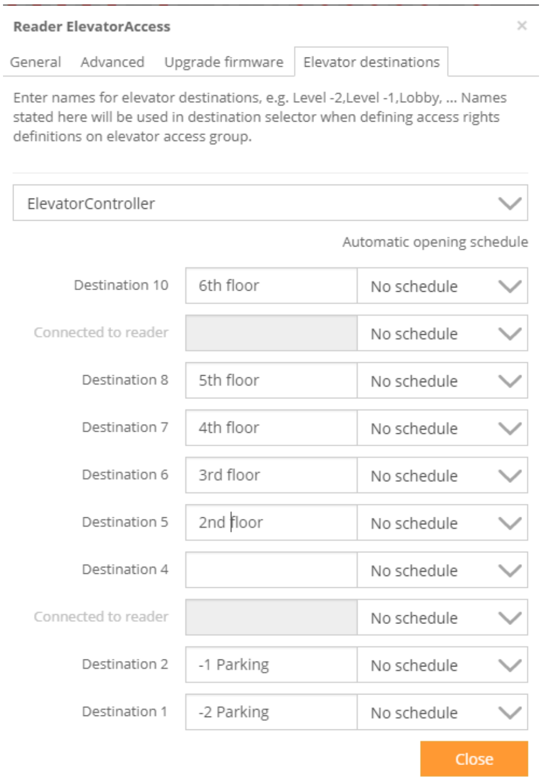
28.1.1 Elevator reader setup

- The reader must be installed on **Door 1** on the Elevator controller.
- Reader and Door 1 settings are applied in the same way as for a normal reader.
- Please see the section on setting up an RFID reader for more information.

NOTE: The only difference is that the **Electric lock open time** setting for Door 1 is controlling how long the elevator buttons are enabled.
IMPORTANT! In cases where the central is controlling less than 10 floors, unused outputs can be used for normal access control with additional readers connected to Door 2, Door 3, or Door 4.

28.1.2 Setting up elevator destinations

To set-up elevator destination, navigate to reader settings (described in chapter **5.1.15 Reader settings**) and enter the desired destinations (an example is displayed on Picture 24-1).
We can make some floors publicly available by assigning a schedule next to the destination name.



Reader ElevatorAccess ×

General | Advanced | Upgrade firmware | Elevator destinations

Enter names for elevator destinations, e.g. Level -2,Level -1,Lobby, ... Names stated here will be used in destination selector when defining access rights definitions on elevator access group.

ElevatorController

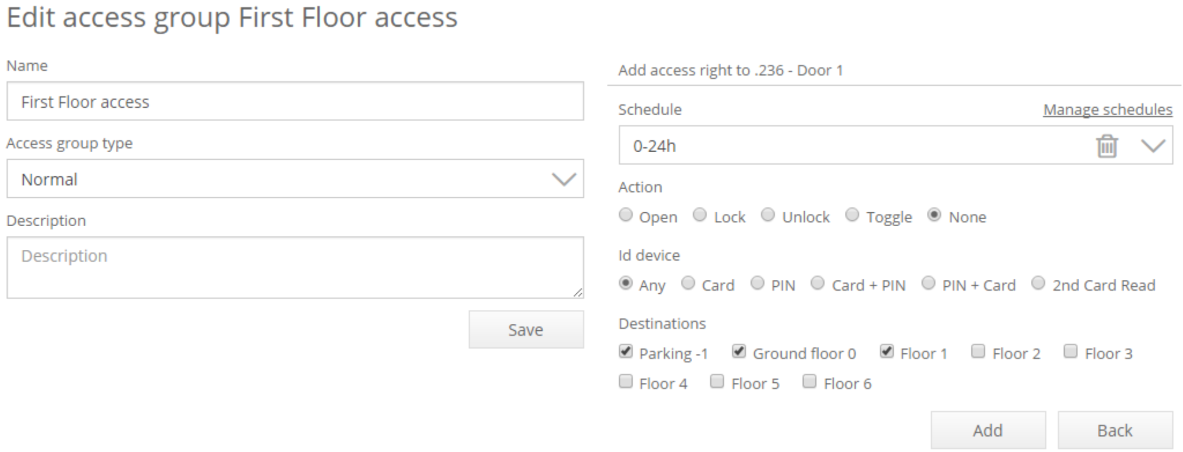
		Automatic opening schedule
Destination 10	6th floor	No schedule
Connected to reader		No schedule
Destination 8	5th floor	No schedule
Destination 7	4th floor	No schedule
Destination 6	3rd floor	No schedule
Destination 5	2nd floor	No schedule
Destination 4		No schedule
Connected to reader		No schedule
Destination 2	-1 Parking	No schedule
Destination 1	-2 Parking	No schedule

Picture 28.1: Elevator destinations

28.1.3 Setting up access groups and access rights

1. Users need to be assigned with **special access groups** defining which floor should be activated when the elevator is used.
2. A **special access group** is created in the same way as a normal access group. Here you create a new access definition of the elevator reader and select the desired **schedule, Id device,** and **floors**.
3. Action must be set to **None** (Picture 24-2).

NOTE: New access groups must be created for each different combination of floors.



Edit access group First Floor access

Name: First Floor access

Access group type: Normal

Description: Description

Add access right to .236 - Door 1

Schedule — Manage schedules

0-24h

Action: ○ Open ○ Lock ○ Unlock ○ Toggle ● None

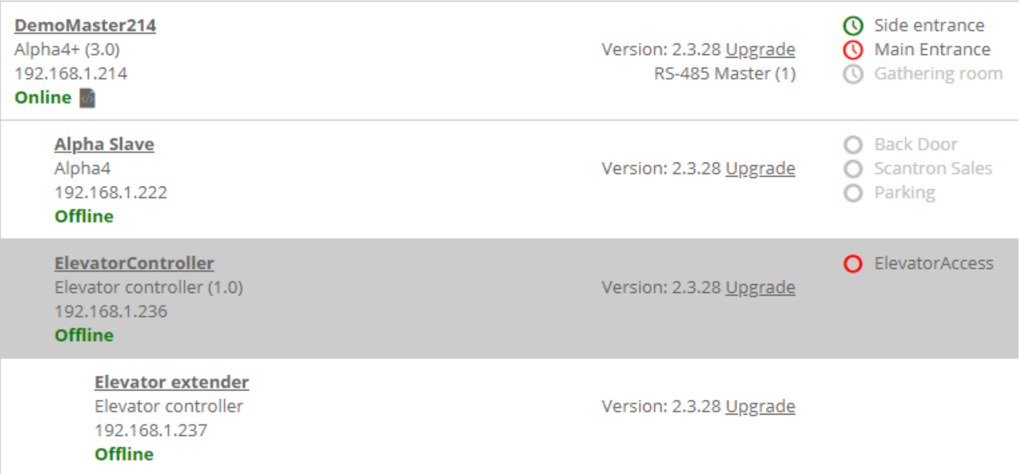
Id device: ● Any ○ Card ○ PIN ○ Card + PIN ○ PIN + Card ○ 2nd Card Read

Destinations: ☑ Parking -1 ☑ Ground floor 0 ☑ Floor 1 □ Floor 2 □ Floor 3 □ Floor 4 □ Floor 5 □ Floor 6

Picture 28.2: Access definition for floors -1, 0, and 1.

28.1.4 How to control more than 10 destinations

A single elevator controller can handle up to 10 floors on its own, however, we can have multiple elevator controllers to extend the maximum floor value by 10 per controller. The extension must be done in Nova by assigning the “extended” elevator controller as a direct slave to the main elevator controller as shown in Picture 24-3.



DemoMaster214
Alpha4+ (3.0)
192.168.1.214
Online
Version: 2.3.28 Upgrade
RS-485 Master (1)
Side entrance
Main Entrance
Gathering room

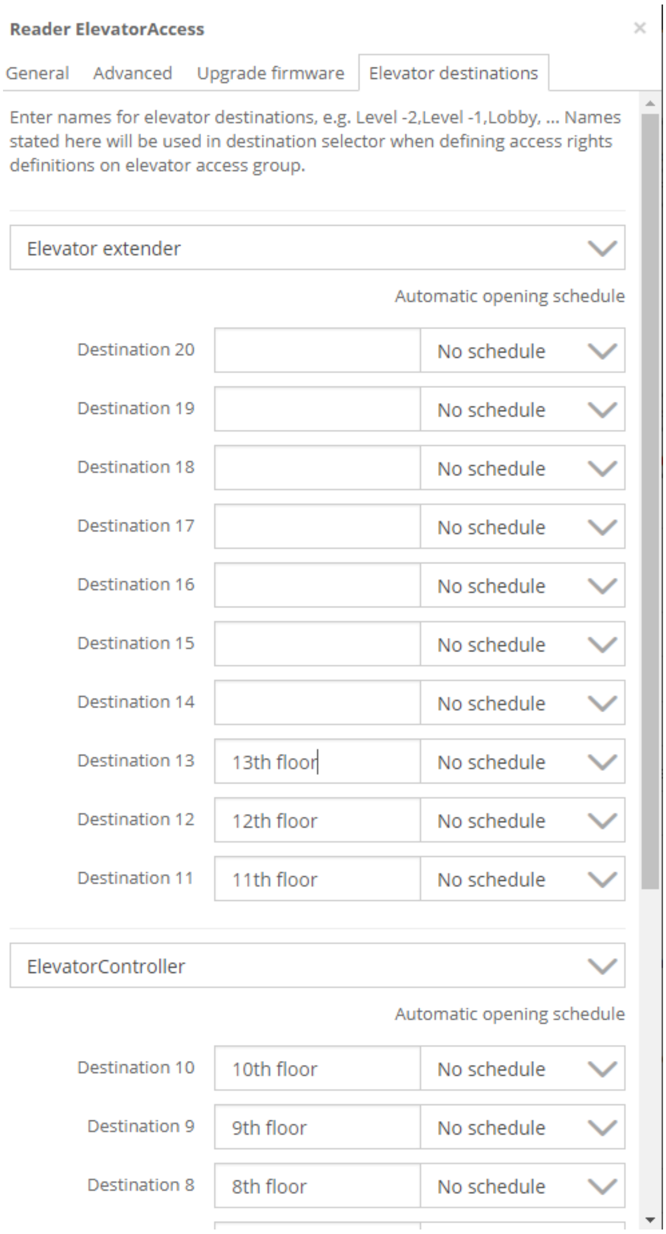
Alpha Slave
Alpha4
192.168.1.222
Offline
Version: 2.3.28 Upgrade
Back Door
Scantron Sales
Parking

ElevatorController
Elevator controller (1.0)
192.168.1.236
Offline
Version: 2.3.28 Upgrade
ElevatorAccess

Elevator extender
Elevator controller
192.168.1.237
Offline
Version: 2.3.28 Upgrade

Picture 28.3: Example of an elevator controller with 20 destinations

The destination pop-up will now contain 20 items in total.



Reader ElevatorAccess

Enter names for elevator destinations, e.g. Level -2,Level -1,Lobby, ... Names stated here will be used in destination selector when defining access rights definitions on elevator access group.

Elevator extender

		Automatic opening schedule
Destination 20		No schedule
Destination 19		No schedule
Destination 18		No schedule
Destination 17		No schedule
Destination 16		No schedule
Destination 15		No schedule
Destination 14		No schedule
Destination 13	13th floor	No schedule
Destination 12	12th floor	No schedule
Destination 11	11th floor	No schedule

ElevatorController

		Automatic opening schedule
Destination 10	10th floor	No schedule
Destination 9	9th floor	No schedule
Destination 8	8th floor	No schedule

28.2 Parking controller

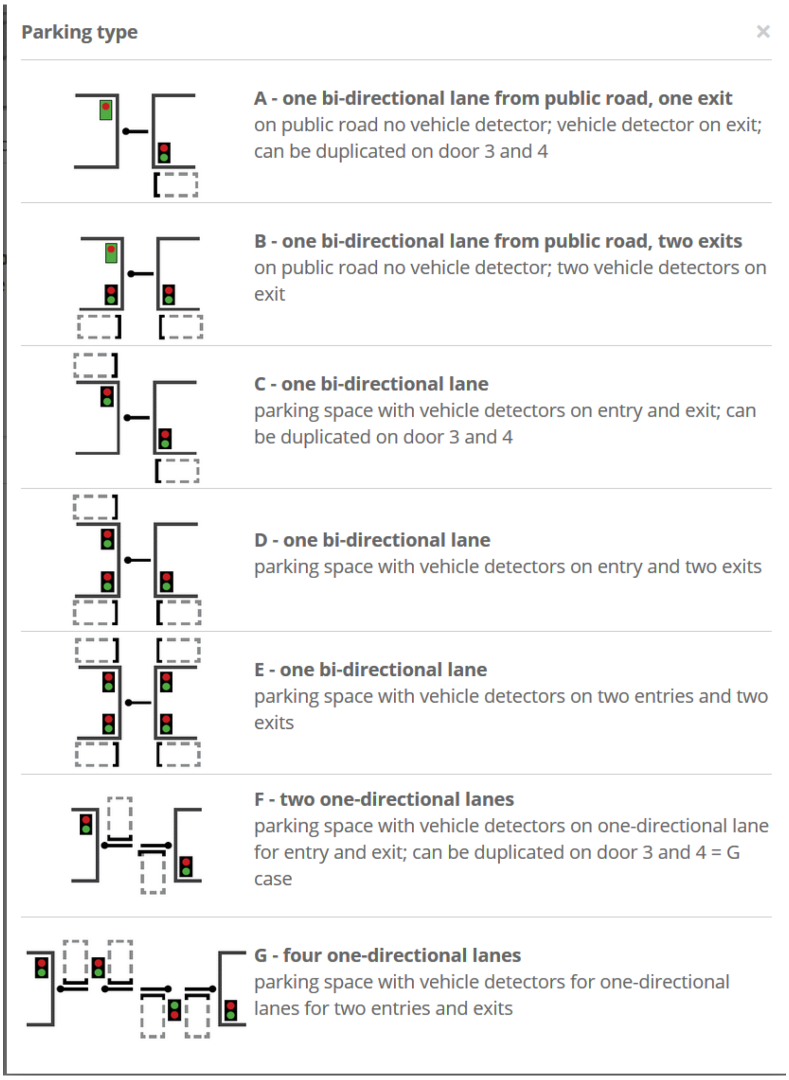
The Parking controller is a stand-alone central that manages parking garages entry/exits.

NOTE: When adding parking controller into a system, 1 presence location will also be automatically available.

For a simple entry/exit set-up, you can wire the Entry reader to Door #1 and Exit reader to Door #2. The traffic lights connected to those door outputs will automatically switch upon user's entry/exit. Instead of regular door monitors, Parking controller uses Vehicle detectors which are required by default (can be disabled if unused). Along with the traffic light, there are also 2 gate outputs to control the barriers (Entry - Gate 1, Exit – Gate2).

For advanced set-ups where there are 3 or 4 Entry/Exit points we can use the Doors #3 and #4. Each of those also has their own Gate control, but they need to be mounted on the external relays.

When setting up parking controller, we can choose between pre-defined set-ups:



Parking type

A - one bi-directional lane from public road, one exit
on public road no vehicle detector; vehicle detector on exit; can be duplicated on door 3 and 4

B - one bi-directional lane from public road, two exits
on public road no vehicle detector; two vehicle detectors on exit

C - one bi-directional lane
parking space with vehicle detectors on entry and exit; can be duplicated on door 3 and 4

D - one bi-directional lane
parking space with vehicle detectors on entry and two exits

E - one bi-directional lane
parking space with vehicle detectors on two entries and two exits

F - two one-directional lanes
parking space with vehicle detectors on one-directional lane for entry and exit; can be duplicated on door 3 and 4 = G case

G - four one-directional lanes
parking space with vehicle detectors for one-directional lanes for two entries and exits

Picture 28.4: Different pre-defined parking set-ups

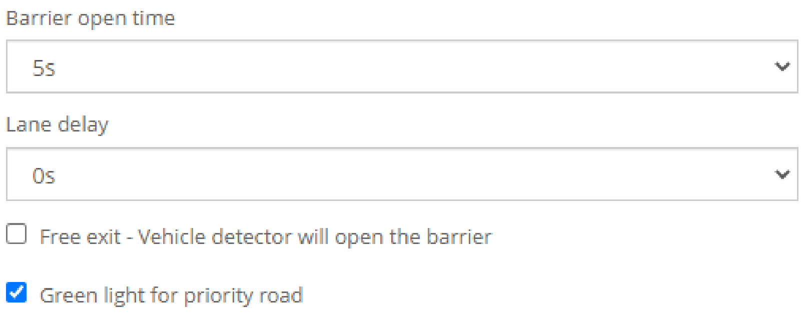
Picture 28.4 shows rectangles where the vehicle detectors should be mounted as well as how many gates and traffic lights are required. The first 2 option also include the public road where the vehicle detector cannot be mounted, so the traffic light is green by default for public road entry unless someone is coming out, then it switches accordingly.

Under the set-ups there is also an option on how long the central will give signal for the barrier to be open (this timer is usually set-up on the barrier itself, so in most cases only a short pulse is required).

The **Free exit** option is there if the anti-passback is not required or should not be as strict when vehicle exits the parking space.

If the **vehicle detector is not installed**, navigate to wanted door and next to Automatic opening schedule **switch DM active voltage level from NC to Unused NO**.

In cases with long ramps leading to the main road, it can take some time before the vehicle exits the premises and the light on the public road switches green before the car has managed to drive off. For such cases we have a **Lane delay** which you can set up the GUI.
The **Green light** checkmark will always show green light (required for entry from the public road and a single drive lane); the light will turn red if someone tries to go out for a timeout of Barrier open time + Lane delay, afterwards it switches the light back to green.



Barrier open time

5s

Lane delay

0s

☐ Free exit - Vehicle detector will open the barrier

☑ Green light for priority road

Picture 28.5: Additional parking controller settings

28.3 USB desktop reader

- **Overview**: USB Desktop Reader consists of a reader and companion software application. The reader is connected to the PC with a USB connector.
- **LED Status:** In normal operation, a red LED is lit on the reader and red LED and green LED are blinking on the USB connector, signaling ongoing communication between application and reader. When a new card is read, the red LED on the reader blinks and a short beep is produced. When a card is accessed for reading/write operations, a short beeping sound is produced.

System Requirements:

Windows XP/7/8/8.1/10 with .NET 4.0 installed USB 2.0 Port, Internet connection

- **Safety:** To ensure the safe operation of the device and its users, please read and act following the safety instructions.

USB Desktop Reader is designed for indoor use only; do not place it outdoors.

Do not place the USB Desktop Reader in or near hot/humid places, such as a kitchen or bathroom.

Please keep the USB Desktop Reader out of reach of children.

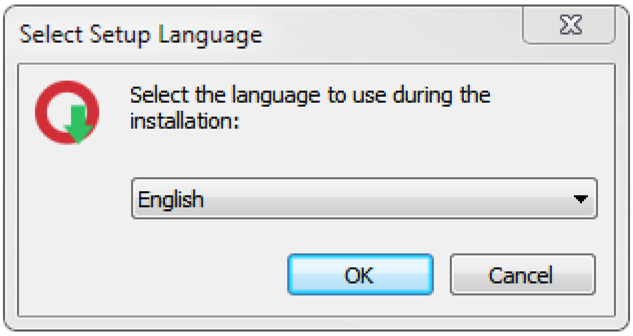
There are no user-serviceable parts inside the USB Desktop Reader. If you experience problems, please contact your dealer, and ask for help.

The USB Desktop Reader is an electrical device and as such, if it becomes wet for any reason, stop using it immediately.

28.3.1 Installation

1. Turn on your computer and **plug-in USB Desktop Reader** into an available USB port on your computer. Never use force to insert a USB connector.
2. **Wait for Windows to detect the inserted device** and that required drivers are installed. **<u>This procedure can take some time</u>**, as Windows may contact update servers to download required files.
3. Download the installation file **USB Desktop Reader Setup <version>.exe**.
4. Double click USB Desktop Reader Setup <version>.exe **setup application** and follow the next installation steps:

- Select the desired **language** you wish to use during the installation of the USB Desktop Reader.



Select Setup Language

Select the language to use during the installation:

English

Picture 28.6: USB Desktop Reader language selection

- The next screen welcomes you in the **setup wizard**. You can proceed with the setup process or you can cancel it by clicking on the **Cancel** button. Click the **Next** button to proceed with the installation.
- Select the desired installation location. It is recommended to use the default location.
- Select the Start Menu folder name. Under this folder, you will later access the installed application.
- Select if you wish to create a desktop icon.
- The next screen displays setup summary information, please read it carefully and click **Install** when you are ready to continue. If you have an older version of the software installed on your computer, it will be closed before installation.

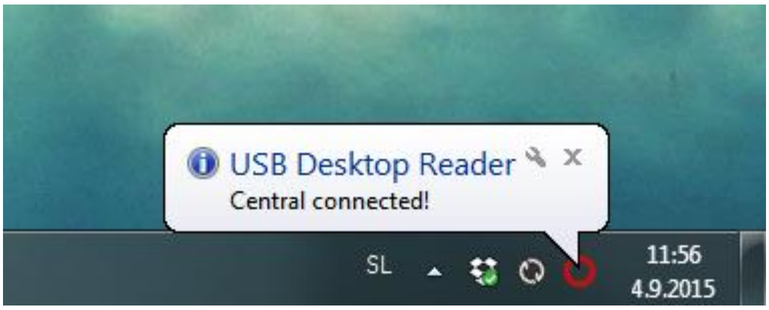
- When the installation process is finished, you will be able to run USB Desktop Reader on your PC. Click **Finish** to close the setup wizard.

28.3.2 Using USB Desktop Reader

Starting application

Start USB Desktop Reader application by double-clicking on the desktop shortcut or click on Windows start menu and selecting USB Desktop Reader shortcut under USB Desktop Reader folder *(shortcuts may not be available if you have decided not to create them during the installation process)*.

USB Desktop Reader will start in the system tray where it can be accessed by clicking on its icon. If the icon is not visible, you can click the *up arrow* on the left side of the system tray and rearrange the USB Desktop reader icon by dragging it to the desired location on the system tray.



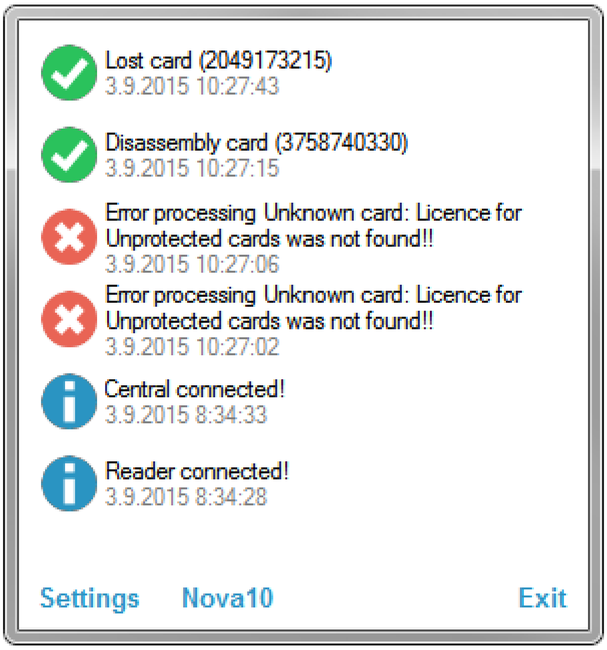
USB Desktop Reader

Central connected!

Picture 28.7: USB Desktop Reader software running in the system tray

USB Desktop Reader settings

A mouse click on the USB Desktop Reader icon will open the main application window with six latest events and access to application settings and the connected central.



Lost card (2049173215)
3.9.2015 10:27:43

Disassembly card (3758740330)
3.9.2015 10:27:15

Error processing Unknown card: Licence for Unprotected cards was not found!!
3.9.2015 10:27:06

Error processing Unknown card: Licence for Unprotected cards was not found!!
3.9.2015 10:27:02

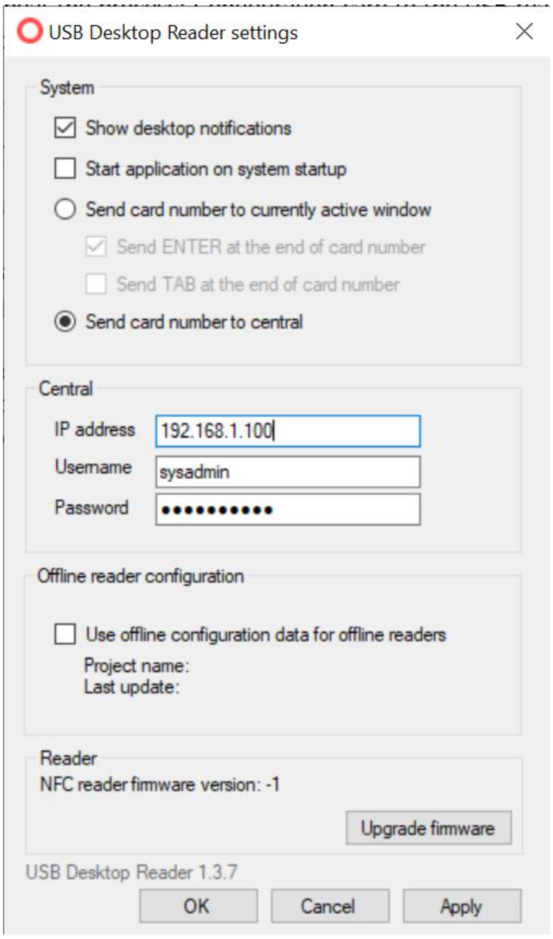
Central connected!
3.9.2015 8:34:33

Reader connected!
3.9.2015 8:34:28

Picture 28.8: USB Desktop Reader log

Clicking on **Settings** will open application settings where you can change the system and central related settings.

Under the **System** section, desktop notification balloons can be enabled or turned off. When desktop notifications are enabled, balloon messages will show the status of all card-related operations and system state changes (disconnected reader, ...).
When the option **Start application on system startup** is selected, USB Desktop Reader will automatically start whenever the PC is turned on.



USB Desktop Reader settings

System

☑ Show desktop notifications

□ Start application on system startup

○ Send card number to currently active window

☑ Send ENTER at the end of card number

□ Send TAB at the end of card number

● Send card number to central

Central

IP address 192.168.1.100

Username sysadmin

Password ••••••••••

Offline reader configuration

□ Use offline configuration data for offline readers

Project name:
Last update:

Reader

NFC reader firmware version: -1

USB Desktop Reader 1.3.7

Picture 28.9: USB Desktop Reader settings

USB Desktop Reader can be run in two different modes:

- When the option **Send card number to the currently active window** is selected, the application will send read card numbers to the opened application that has focus (this mode is useful if you need to create a list of user cards in Excel spreadsheet). In this mode, you can also select if the card number is combined with ENTER or TAB keypress.

- If option **Send card number to central** is selected, then read card number is sent to the central, and card is treated in the same way as it would be on an online reader.

  For the second option valid central IP address, username and password need to be entered under applicable fields in the **Central** section of the settings window.
  When you have edited application settings you can close the settings window by clicking on the **OK** button or you can apply new settings with the click on the **Apply** button. If you wish to discard changes, you can click on the **Close** button to close the settings window.

Offline reader configuration option

This option is used to **disable reading of Mifare Classic ®** cards on offline/online reader(s).

1. Make sure that all the users switched to Mifare DESFire ® cards.
2. The system should have at least one set of **Mifare DESFire ® configuration card set**.
3. In the **Settings > Other settings**, the option **Cards security** should be set to **Disable Mifare Classic ® on offline readers** or **Disable Mifare Classic ® on online and offline readers**.
4. Navigate to the offline readers and select ANY of the reader and create an offline configuration for it (it should not be first configuration) and put the Mifare DESFire ® config card to the USB reader.

Configuration card can be used a single time once prepared; for faster offline reader programming, you can use USB reader's offline configuration data to connect to the central in advance (once the central is connected and checkmark set, the config card can be created without an active connection to the central). The configuration can be then transferred like this:

1. Configuration card to the USB reader,
2. configuration card to the offline device.

Exiting the application

You can close the USB Desktop Reader application by clicking on the **Exit** label in the main application window or by right-clicking on the application icon in the system tray and selecting menu option **Exit**.

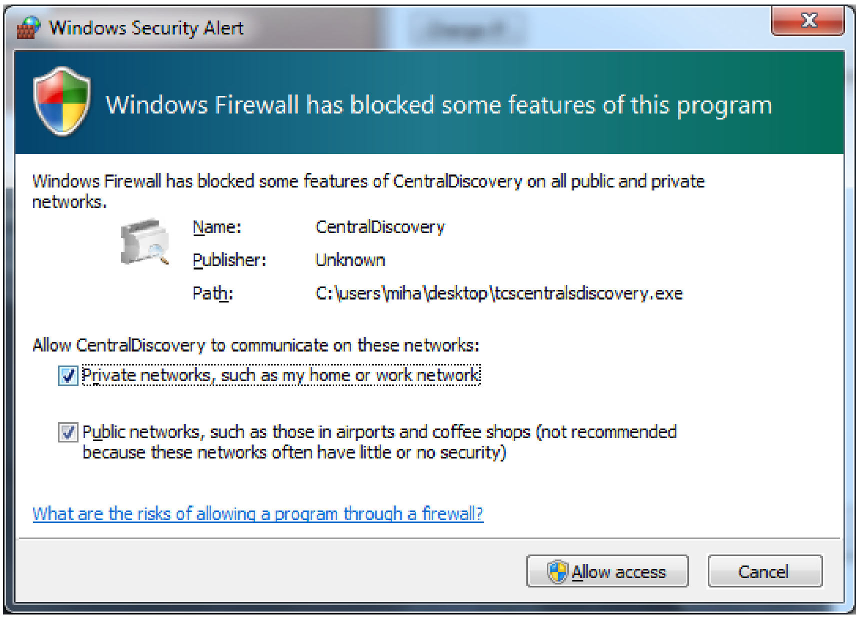
NOTE: When transferring the offline events with the events card, the events will be inserted into Nova periodically over a couple of seconds (this can take up to couple of minutes depending on the number of the events). During this critical procedure, any changes to the hardware settings are prohibited as this could cause loss of the events. If the Save action is pressed during the procedure, Nova will display the *central is busy* error. Please wait until the operation is complete.

29. Central discovery tool

This tool allows sysadmins to manage all centrals connected to the local network. This software can be found and downloaded from the vendor's webpage.

After downloading the software:

1. Open it
2. Both checkmarks must be checked and the tool must be allowed access to the network in the Firewall enable window (Picture 25-1)



Windows Security Alert

Windows Firewall has blocked some features of this program

Windows Firewall has blocked some features of CentralDiscovery on all public and private networks.

Name: CentralDiscovery
Publisher: Unknown
Path: C:\users\miha\desktop\tcscentralsdiscovery.exe

Allow CentralDiscovery to communicate on these networks:

☑ Private networks, such as my home or work network

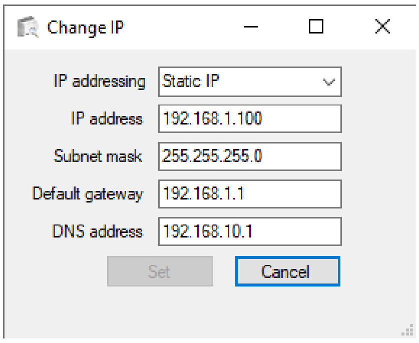
☑ Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)

What are the risks of allowing a program through a firewall?

Picture 29.1: Allowing access to the tool beyond the firewall

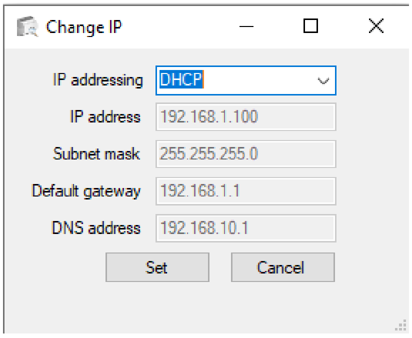
From the main window (Picture 25-2) the MAC and IP address are visible for the corresponding centrals.

- Here it is possible to navigate to the central web page by clicking on the active link in the **Web Address** column.
- Changing the IP of the central is only available from the default IP (192.168.1.100) address.
  - The central can be set to static IP or DHCP.



Change IP

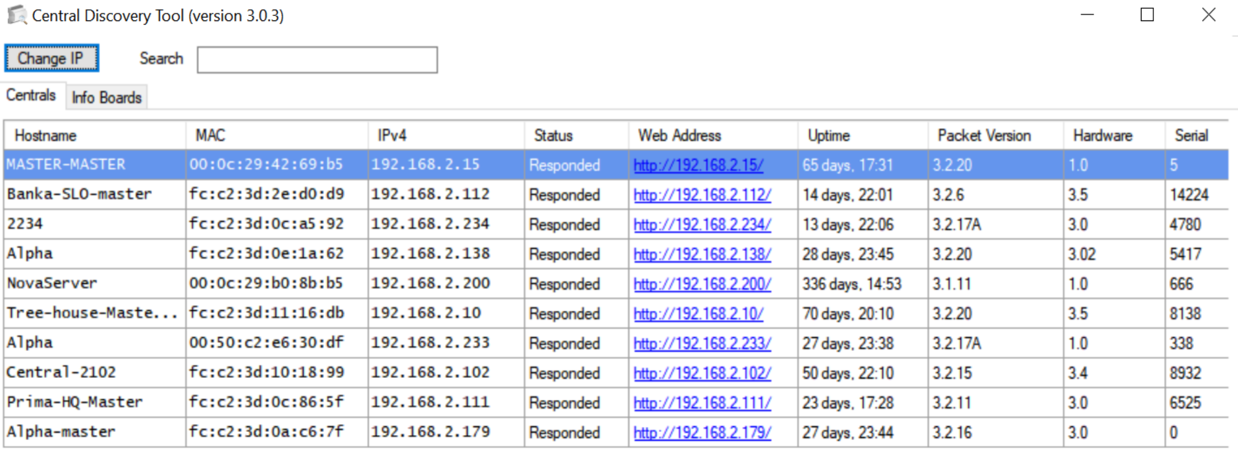
IP addressing: Static IP
IP address: 192.168.1.100
Subnet mask: 255.255.255.0
Default gateway: 192.168.1.1
DNS address: 192.168.10.1



Change IP

IP addressing: DHCP
IP address: 192.168.1.100
Subnet mask: 255.255.255.0
Default gateway: 192.168.1.1
DNS address: 192.168.10.1

  - Allowing the IP to be changed from the default IP prevents any unwanted changes outside the system. If the central is reset, its IP changes to the default address. See the explanation of central reset in chapter 26.



Hostname	MAC	IPv4	Status	Web Address	Uptime	Packet Version	Hardware	Serial
MASTER-MASTER	00:0c:29:42:69:b5	192.168.2.15	Responded	http://192.168.2.15/	65 days, 17:31	3.2.20	1.0	5
Banka-SLO-master	fc:c2:3d:2e:d0:d9	192.168.2.112	Responded	http://192.168.2.112/	14 days, 22:01	3.2.6	3.5	14224
2234	fc:c2:3d:0c:a5:92	192.168.2.234	Responded	http://192.168.2.234/	13 days, 22:06	3.2.17A	3.0	4780
Alpha	fc:c2:3d:0e:1a:62	192.168.2.138	Responded	http://192.168.2.138/	28 days, 23:45	3.2.20	3.02	5417
NovaServer	00:0c:29:b0:8b:b5	192.168.2.200	Responded	http://192.168.2.200/	336 days, 14:53	3.1.11	1.0	666
Tree-house-Maste...	fc:c2:3d:11:16:db	192.168.2.10	Responded	http://192.168.2.10/	70 days, 20:10	3.2.20	3.5	8138
Alpha	00:50:c2:e6:30:df	192.168.2.233	Responded	http://192.168.2.233/	27 days, 23:38	3.2.17A	1.0	338
Central-2102	fc:c2:3d:10:18:99	192.168.2.102	Responded	http://192.168.2.102/	50 days, 22:10	3.2.15	3.4	8932
Prima-HQ-Master	fc:c2:3d:0c:86:5f	192.168.2.111	Responded	http://192.168.2.111/	23 days, 17:28	3.2.11	3.0	6525
Alpha-master	fc:c2:3d:0a:c6:7f	192.168.2.179	Responded	http://192.168.2.179/	27 days, 23:44	3.2.16	3.0	0

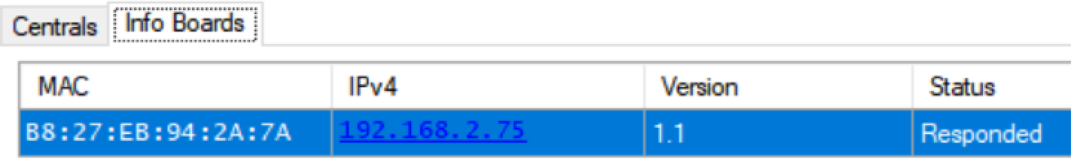
Picture 29.2: Central discovery tool main page

- This tool scans the network for any new central every few seconds.
    - In case a central fail to respond due to IP change or network error, its entire row will turn red and its status will show **No response**.
        - This is extremely helpful to determine if there are any problems with the local network.
- Right mouse click brings up a dropdown to copy IP or MAC address.

Search function

The search box on the top applies a filter to display centrals only in the specific network or just a simple search for central IP or MAC address.

Info boards



MAC	IPv4	Version	Status
B8:27:EB:94:2A:7A	192.168.2.75	1.1	Responded

The tool also finds the Info boards connected on the same network. Moreover, it allows changing the network settings to the found info board.

NOTE: The discovery and search tool work the same as the one for centrals.

ATTENTION! Central discovery uses UDP (User Datagram Protocol) packets, which means that the discovery will display all centrals from local network (for centrals with Nova version 1.4 and lower) and the centrals from other sub-networks (if the router/access point allows it and the software on centrals is **version 1.5 or higher**).

IMPORTANT! This tool does not need to be installed. It was designed to run on any version of Windows OS. Different OS systems can also run the tool via emulation software.

30. MQTT integration

NOTE: Scripting module is required to run this script. To get the required script, please contact your distributor.

All available MQTT topics:

30.1 Subscribe topics

To receive messages on a topic you will need to subscribe to the topic or topics. When you subscribe to a topic or topics you are effectively telling the broker to send you messages on that topic.

You can subscribe to multiple topics using two wildcard characters (+ and #)

Plus sign (+): It is a single level wildcard that matches any name for a specific topic level. For example, in case we want to receive all the messages related to reader status for one central, we can use the **+** single level wildcard instead of a specific reader name. Topic would be:

"<**Central name>/+/Status/"**

Hash (#): it a multi-level wildcard that we can use only at the end of the topic filter. For example, in case we want all reader topics would be:

"<Central name>/<Reader name>/#"

30.1.1 Alarm

Get a message when someone breaks in trough your door. You can view all alarms events simply with one topic or specific reader alarm events.
Events that are sent to alarm topics: Break in, Door left open alarm, Central offline, Reader offline.

All alarm events topic: "All Alarms/"

Reader alarm topic: "<Central name>/<Reader name>/Alarm/"

Central alarm topic: "<Central name>/Alarm/"

30.1.2 All events

Get all events that happens with one topic.
All events on central topic: "All events/"
Example: Event: 2022-06-10 11:39:07 400 0 3 2, 1

All text events on central topic: "All events text/"
Example: Event: 2022-06-23 11:34:49 Door entry at Meeting room
NOTE: Not all events are supported with topic "All events text/"

30.1.3 MQTT script

MQTT script runs on master central (or server). **MQTT script status topic** is important because is the only way you know if script is **still running** inside MQTT broker.

Status topic: "MQTT script/Status/"

First start up time: "MQTT script/First startup/"

Last restart time: "MQTT script/Last restart/"

30.1.4 Reader

New readers are automatically added to the MQTT broker. You can see reader status if it goes offline/online. If someone opens the door, event will be sent to reader door events. (Click for more info)

Reader status

Topic: "<Central name>/<Reader name>/Status/"

Available values: online, offline

Door events

Topic: "<Central name>/<Reader name>/Door events/"

All available door events:
Door entry, door exit, door entry exit, door locked, door unlocked, door blocked, unknown card, unknown pin, door open from software, door unlocked from software, door locked from software, door blocked from software, after break in closed door, door left open, door closed after left opened, door left opened alarm, user put the card on but did not enter, break in.

30.1.5 Central

New centrals are automatically added to the MQTT broker. You can check the status of the central.

Central status

Central status topic:

"<Central name>/Status/"

Available values: online, offline

30.2 Publish topic:

A client is free to publish on any topic it chooses. A message can be received by a group of clients if they subscribe to the same topic.

MQTT supports QOS levels 0, 1, 2.

- **QOS -0** – **Default** and does not guarantee message delivery.
- **QOS -1** – Guarantees message delivery but could get duplicates.
- **QOS -2** -Guarantees message delivery with no duplicates.

When a client publishes a message to a broker it needs to send:

- The message topic
- The message QOS
- Whether the message should be retained. - **Retain Flag**

The retain Flag is normally **set to False** which means that the broker doesn't keep the message.

If you set the retain flag to True then the **last message** received by the broker on that topic with the **retained flag set** will be kept. New subscriber or reconnects subscriber gets the last message saved in the topic with retained flag.

The next message published on that topic **replaces** the **last retained** message for that topic. If the last message is retained and the next one is not a new subscriber gets last retained message!

30.2.1 Door entry

To unlock the door, you can publish a message to the door topic:

"<Central name>/<Reader name>/Door entry/

Important: Do not use retained flag with this topic! If the script restarts or reconnects it will unlock the door if last retained message is Open or Unlock.

Available messages

Open – Unlocks and locks the door

Unlock – Unlocks the door

Lock – Locks the door

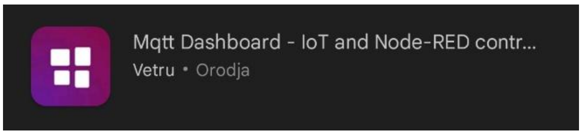
30.3 How to open a door with a phone

Requirements:

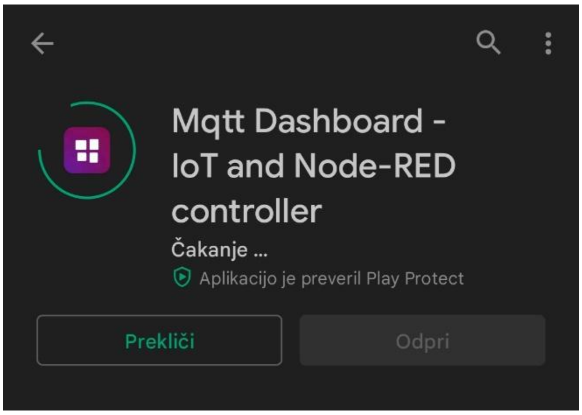
- Phone
- MQTT Broker (secured one)
- Certificate for secure connection to the broker
- MQTT script running on central
- Internet connection on phone, central, Broker
- Any app which provides a secure connection to MQTT Broker (In my case MQTT Dashboard)

1. First, get the certificates on your phone. Certificates depends on the broker configuration. Save them somewhere save.

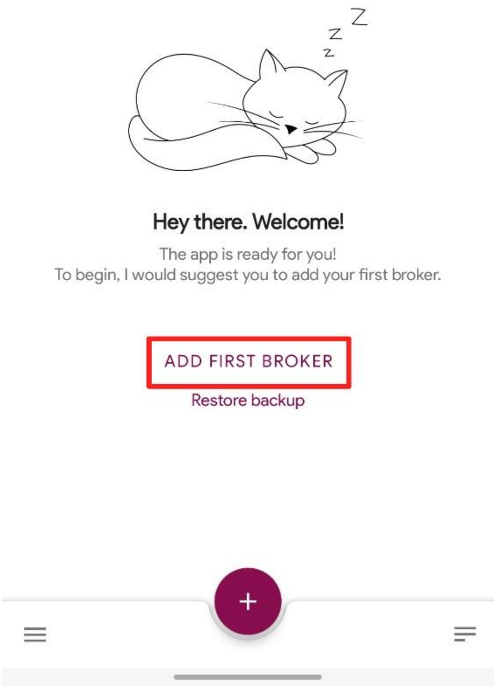
2. For demonstration purposes I will use MQTT Dashboard – IoT and Node-RED controller app. Search it on google play:


Mqtt Dashboard - IoT and Node-RED contr...
Vetru • Orodja

3. Click on the app and download it.


Mqtt Dashboard - IoT and Node-RED controller
Čakanje ...
Aplikacijo je preveril Play Protect

4. When the app opens it should look like the picture below. Now click on "ADD FIRST BROKER".



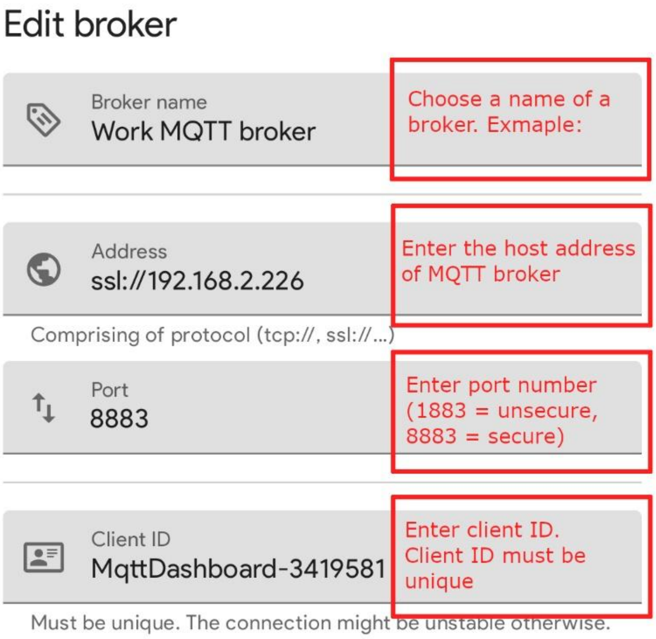
Hey there. Welcome!

The app is ready for you!
To begin, I would suggest you to add your first broker.

ADD FIRST BROKER

Restore backup

5. You will see a broker edit menu. Choose a name for the broker. Then enter the host address of your broker and port number. Client ID must be unique otherwise connection may be unstable. Please use port 8883 (secure)



Edit broker

Broker name
Work MQTT broker

Choose a name of a broker. Exmaple:

Address
ssl://192.168.2.226

Enter the host address of MQTT broker

Comprising of protocol (tcp://, ssl://...)

Port
8883

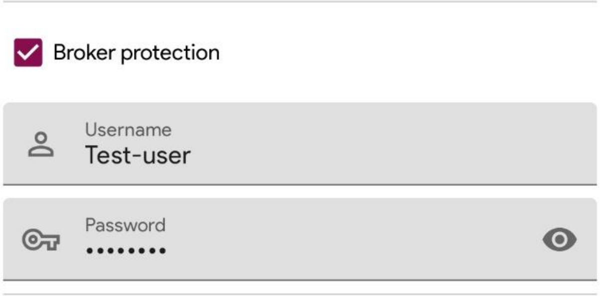
Enter port number (1883 = unsecure, 8883 = secure)

Client ID
MqttDashboard-3419581

Enter client ID. Client ID must be unique

Must be unique. The connection might be unstable otherwise.

6. Click on the check box for broker protection and enter username and password for broker account.

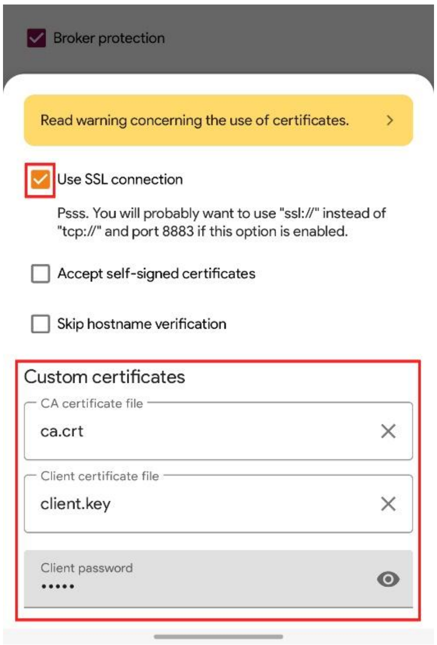


☑ Broker protection

Username
Test-user

Password
••••••••

7. Click on "Use SSL connection" option. It will show a popup menu for a secure connection. Click on the check box for Use SSL connection. Now add all your certificate files.



☑ Broker protection

Read warning concerning the use of certificates. >

☑ Use SSL connection

Psss. You will probably want to use "ssl://" instead of "tcp://" and port 8883 if this option is enabled.

☐ Accept self-signed certificates

☐ Skip hostname verification

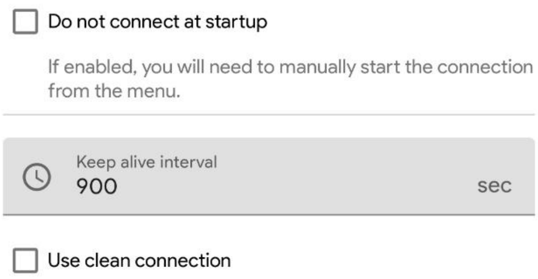
Custom certificates

CA certificate file
ca.crt ✕

Client certificate file
client.key ✕

Client password
•••••

8. Keep alive interval is used for checking if a connection is still established between phone and broker. Using clean connection means that broker does not store any subscription information or undelivered messages for the client when a client



☐ Do not connect at startup

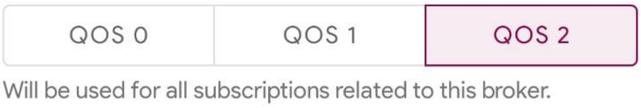
If enabled, you will need to manually start the connection from the menu.

Keep alive interval
900 sec

☐ Use clean connection

reconnects.

9. Buttons QOS 0, QOS 1, QOS 2 mean how should message be delivered (QOS = Quality of service). Click on the QOS 2.

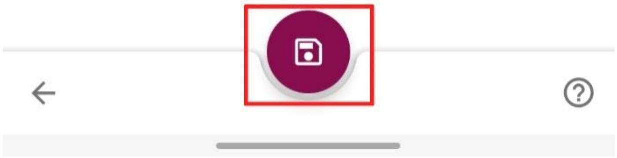


Will be used for all subscriptions related to this broker.

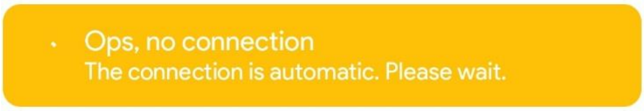
- QOS 0: Once (not guaranteed to be received by other clients)
- QOS 1: At least Once (guaranteed to be received by other clients at less once, but may be delivered more than once)
- QOS 2: Only once (guaranteed to be delivered only once. This is the slowest method but the safest)

More info here: https://www.hivemq.com/blog/mqtt-essentials-part-6-mqtt-quality-of-service-levels/

10. Then click on the Save button.

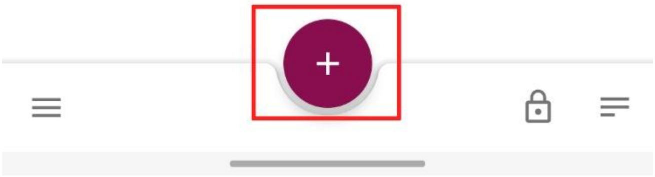


11. Go back to the main menu. If a popup like the one on the image below doesn't go away after a few seconds that means you didn't connect to broker successfully.

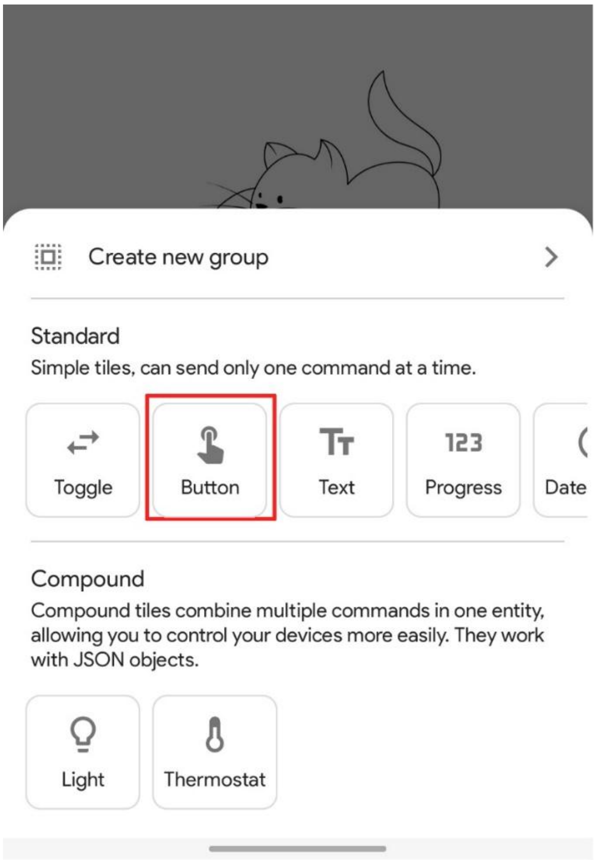


Ops, no connection
The connection is automatic. Please wait.

12. When you are connected to the broker click on the plus button.

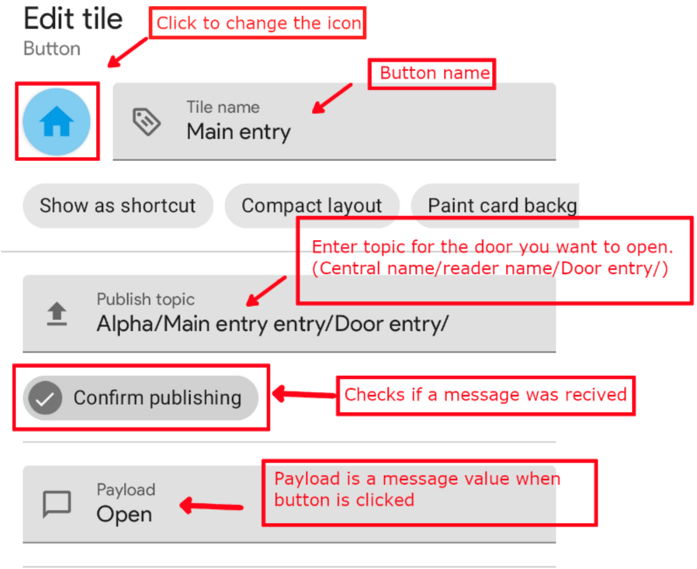


13. It will show which tiles you can add. Select Button tile.



Create new group
Standard
Simple tiles, can send only one command at a time.
Toggle
Button
Text
Progress
Date
Compound
Compound tiles combine multiple commands in one entity, allowing you to control your devices more easily. They work with JSON objects.
Light
Thermostat

14. Now enter the button name example: Main entry. Click on the icon if you want to change the color of icon or icon itself. Publish topic depends on the door you like to open. The Topic for the doors: "<Central name>/<Reader name>/Door entry/". The payload can be "Open", "Unlock", "Lock". (Open = door unlocks and locks, unlock = door only unlocks, lock = door only locks)



Tile name: Main entry

Enter topic for the door you want to open. (Central name/reader name/Door entry/)

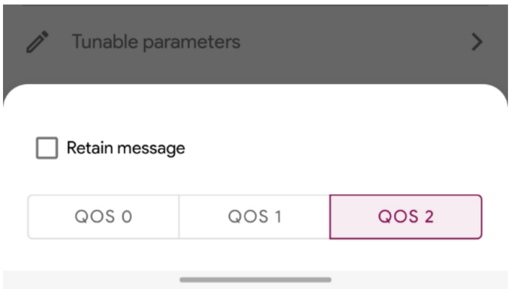
Publish topic: Alpha/Main entry entry/Door entry/

Confirm publishing

Payload is a message value when button is clicked

Payload: Open

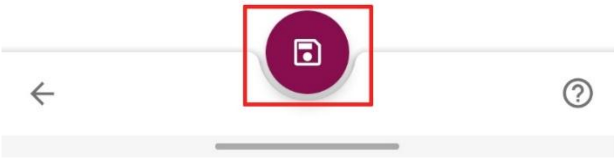
15. Quality of Service means how should the message be delivered. Click on QOS 2. Don’t use retain messages for door entry because if the MQTT script on central reconnects it will automatically open or closes the door because it will get the last message that was sent to broker!



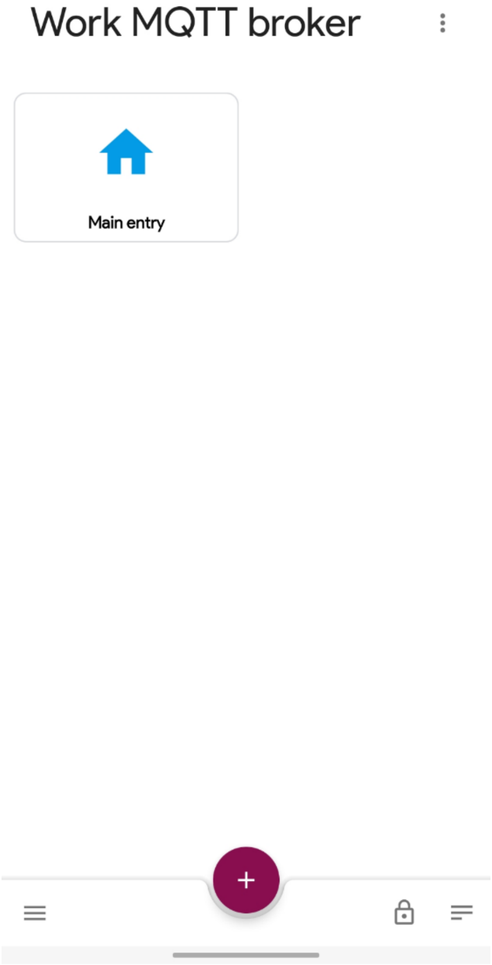
☐ Retain message

QOS 0 QOS 1 [✓ QOS 2]

16. Then click on the Save button



Now on the main menu new button will appear. If you click on it will open the door

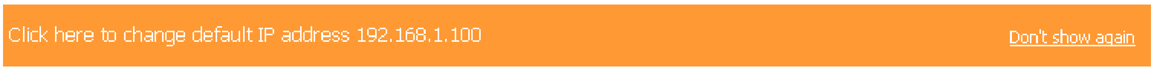


31. FAQ

Difference between the physical IP address of a central and the IP address, on which the central is visible
If all centrals are inside the same LAN, every central can be connected to another central by registering the IP address of the other central. This IP address is the physical address of the central and can be changed in the **Central Settings** (see chapter 5.1.5 – Settings section). This address is the address where the central is visible to other centrals. If all centrals are in the same LAN, the physical address is also the visible address. The visible address is the address, which can be set in the **Central Settings** (Picture 5-9).

If any central in the LAN should be connected to a central located in a remote LAN, the address of the remote LAN must be identified. Routers control the communication between two different LANs, and if a message is sent from a central in one LAN to a central in another LAN, it is first sent to the router of the other LAN, which then sends it to the central. In the latter case, the router address becomes the visible address of the central in the other LAN (and is set in the **Central editor**).
A central in a remote LAN still has its physical address, which is needed for message delivery. This physical address can be changed in **Manage Centrals** (**5.1.1 Searching and managing centrals in Local Area Network (LAN)**) popup window.

The warning message in Picture 26-1 shows on the main page. It is displayed, if the physical address of the central is on 192.168.1.100. The best way to properly set the system is to set the central database IP to 192.168.1.[any other number between 1 and 255 excluding 100] – with database update. If the central interface IP needs to be changed, repeat the process setting the new interface IP without a database update.


Click here to change default IP address 192.168.1.100

Picture 31.1: 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. RS-485 communication is also much slower because the communication can only take place from one central to another at the time, whereas Ethernet allows many centrals to communicate all the time. This means that the limit of maximum 10 slave centrals connected to an 'RS-485 master central' on one RS-485 BUS is pre-set. Replication over an RS-485 BUS can handle up to 750 door openings per hour (3.000 events).

This amounts to up to 300 door openings per minute between centrals connected over TCP/IP connection run on Alpha centrals – if more capacity is needed the Nova software should be placed on a Linux server with more processing power which is a NovaServer version, which includes the server.

When the system is running, the slave centrals send their events to the master but receive no events back from the master or any other centrals in the system except if an event concerns a function on the slave central – e.g., an event generated on another central should open a relay on the central. So, regarding the slaves, most of the communication is one-way and means that the slaves have no back-up of events in the system, but only contain its local events and the settings for the system (users, access groups, etc.).

The 'RS-485 master central' receives all events from its 'RS-485 slaves', which it replicates to all other Alpha centrals in the access control system that is on Ethernet. It also sends all settings to the 'RS-485 slaves' as well as events that shall activate a function on an 'RS-485 slave'.

A system where centrals are on RS-485 BUS should not contain more than 1.000 users due to the time it takes to upload them and distribute the information to all centrals. It takes approximately 3 minutes per central on an RS485 BUS, which means that it takes 30 minutes for 10 centrals connected on one RS-485 BUS. This can be important under commissioning or for systems where there are many changes to the settings.

Port forwarding for remote central on fixed IP address
Here, two possible cases can occur:

- The first case is when master central needs to communicate with the slave central in another network.
- The other case is when wanting to access publicly available Nova application through the browser.

In the first case, when the master needs to access remote slave central, one port needs to be forwarded on a remote router. Usually, port number 3543 on the remote router (the number is configurable under advanced settings of the remote central) needs to be forwarded to internal port 3543 on the slave central (not configurable). Through this port, the master central (or the local master central) sends the database to slaves.

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

If using a domain name (dynamic DNS service or custom domain name) instead of an IP address, that domain name is connected only to the IP address and all port settings remain the same.

What happens in the case of replicator overload?
If the system generates more than approximately 3.000 events per hour on an RS-485 BUS it builds up a backlog. This means that events are lined up in a queue and not reported instantly. In many cases, this does not matter as the local centrals continue to work normally, so users will not notice any difference. However, in systems where an event (e.g., an input) on one central should release a function on another (e.g., an output), it can cause the event to be delayed when registered in the queue.

A built-up backlog of events will be phased out in the minutes afterward if the number of events gets fewer than 50 per minute (approximately 12 door openings). If the backlog only builds up and up the system will stop working.

An ‘RS-485 slave central’ is not affected locally by a replicator backlog. It will continue to operate according to the memory settings: doors will be opened for users, period validation and access rights to offline readers will be written to users’ cards, etc.

Capabilities of RS-485 system

A system with RS-485 BUS between the centrals can be set up in three ways:

1. One master central connected directly to a PC and with up to 10 slave centrals connected on the RS-485 BUS.
2. One master is central on TCP/IP connection and with up to 10 slave centrals connected on the RS-485 BUS.
3. Several ‘RS-485 master centrals’ on TCP/IP – all part of the same big access control system – and each has up to 10 RS-485 centrals connected on the local RS-485 BUS.

The rule of max 10 centrals on an RS-485 BUS and max 1.000 users in an access control system with centrals on RS-485 BUS is only as a guideline, which, in some cases, can be adapted to local circumstances. If a system has few users and a few events, it is possible to have more centrals on the BUS and it will work well.

The same goes for more than 1.000 users in an access control system, where it is only possible to have few slave centrals on a separate RS-485 BUS.

On the other hand, it is possible to have a system with 500 users, but with many events and changes to the users. In this case, it might be unsuitable to install any centrals on RS-485 BUS.

On the ‘RS-485 slaves’ read/write readers can be installed to be used as update readers for period validation and access rights for offline readers. Input on the centrals can also be used to generate outputs on other centrals. The RS-485 BUS does not limit these possibilities.

Which memory sectors are used on MIFARE cards by the offline system?

User cards use sectors 5 – 9 (5 sectors) and 10 - 12 (3 sectors) by default. The starting sector for the access rights segment is configurable. It is currently the 5th sector, followed by 5 consecutive sectors. The starting sector for the feedback segment is also configurable. By default, the segment starts at the 10th sector followed by 2 consecutive sectors. All sectors are protected by unique authentication keys.

Usage of cards in other applications

Configuration cards for offline readers should not be shared between different applications and are linked only to our system. User cards are usable for other applications if the other applications use 'free' sectors on cards.

How is a user informed about a low battery level on the offline readers?
The user is informed by the device (with delay, red LED, etc.) as well as by software reports of battery status when Offline+ activation key is used and user feedback (events on user card) is enabled. If the battery status is low, it can be found between Errors on the Home screen. In the settings for every offline reader, there is a Remarks box to note the date of the last battery change.

How to replace existing or add new central to the existing system
When adding a new central or replacing some centrals in the existing system, follow these instructions:

1. Disconnect faulty central from the system if applicable.
2. Login to master central and add new slave central to the system or edit existing slave MAC address with the MAC address of the new slave central. The MAC address of the central is written on the central side label.
3. Reset new slave centrals to default, so there is no old data on it (it might be an old master and will try to connect to some centrals, etc...).
4. Login to Nova application (NovaSimpli when reset to default) using default credentials and change the central IP address to the new value, which is set on master central.
5. Connect the slave central to the network. Master central will connect to it and update the slave central configuration.

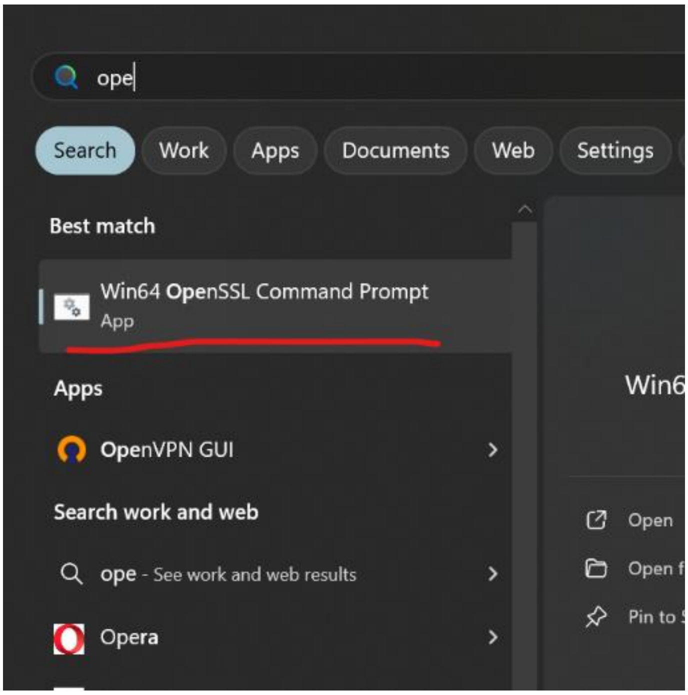
The replacement of master central is described in chapter 5.1.7 Replacement of malfunctioning master central.

How many cards are stored on the blacklist card?
The blacklist itself can store up to 1133 cards.

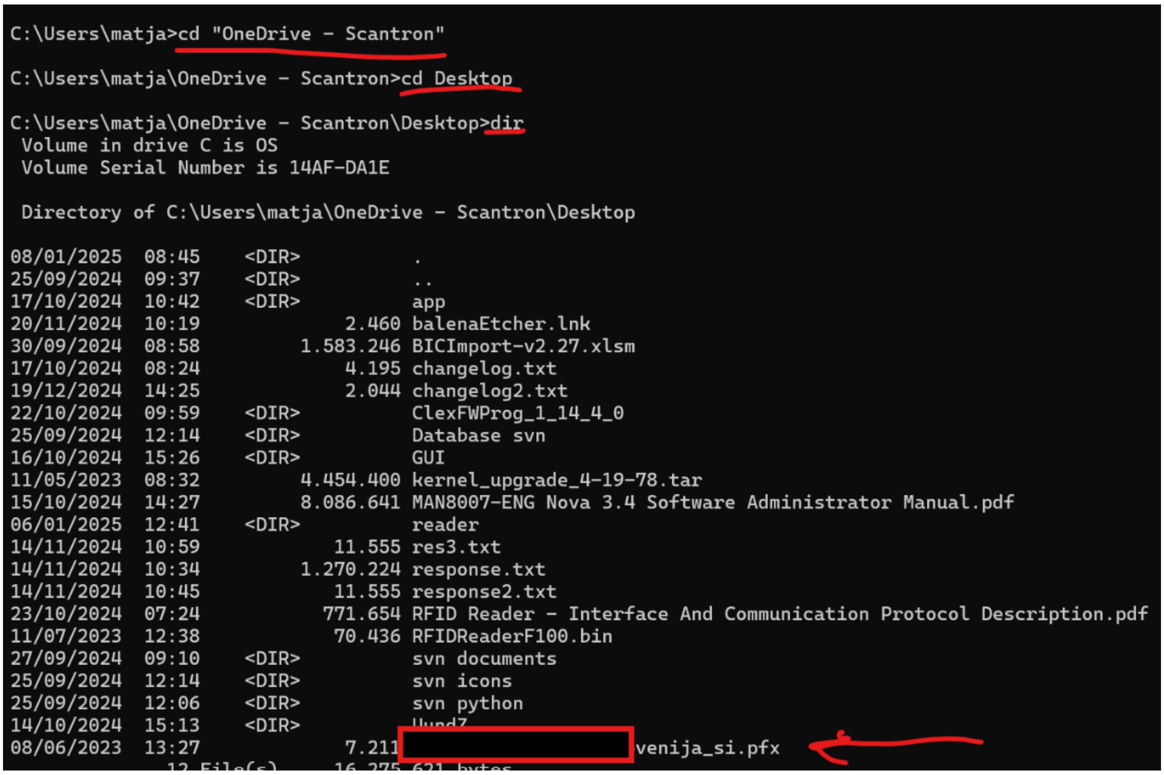
How to convert .pfx certificate to .crt, .key, .chain that are acceptable by Nova on Windows?
What we need are at least 3 files: your_certificate_name.cert (or .crt), your_certificate_name.key (which can be combined into .pem or .cert or .crt) and the chain cert (could be multiple).
The .pfx file contains a password that we need to get rid of.

1. Download and install OpenSSL for Widows: https://slproweb.com/download/Win64OpenSSL_Light-3_4_0.msi

2. Open OpenSSL Command prompt.



3. Navigate to where your .pfx cert is:



```
C:\Users\matja>cd "OneDrive - Scantron"

C:\Users\matja\OneDrive - Scantron>cd Desktop

C:\Users\matja\OneDrive - Scantron\Desktop>dir
 Volume in drive C is OS
 Volume Serial Number is 14AF-DA1E

 Directory of C:\Users\matja\OneDrive - Scantron\Desktop

08/01/2025  08:45    <DIR>          .
25/09/2024  09:37    <DIR>          ..
17/10/2024  10:42    <DIR>          app
20/11/2024  10:19             2.460 balenaEtcher.lnk
30/09/2024  08:58         1.583.246 BICImport-v2.27.xlsm
17/10/2024  08:24             4.195 changelog.txt
19/12/2024  14:25             2.044 changelog2.txt
22/10/2024  09:59    <DIR>          ClexFWProg_1_14_4_0
25/09/2024  12:14    <DIR>          Database svn
16/10/2024  15:26    <DIR>          GUI
11/05/2023  08:32         4.454.400 kernel_upgrade_4-19-78.tar
15/10/2024  14:27         8.086.641 MAN8007-ENG Nova 3.4 Software Administrator Manual.pdf
06/01/2025  12:41    <DIR>          reader
14/11/2024  10:59            11.555 res3.txt
14/11/2024  10:34         1.270.224 response.txt
14/11/2024  10:45            11.555 response2.txt
23/10/2024  07:24           771.654 RFID Reader - Interface And Communication Protocol Description.pdf
11/07/2023  12:38            70.436 RFIDReaderF100.bin
27/09/2024  09:10    <DIR>          svn documents
25/09/2024  12:14    <DIR>          svn icons
25/09/2024  12:06    <DIR>          svn python
14/10/2024  15:13    <DIR>          
08/06/2023  13:27             7.211 [redacted]venija_si.pfx
              12 File(s)     16.275.621 bytes
```

And run this command to extract the key (you will be asked to provide a password for extraction, but do not set a new password if asked; just press enter as an empty password):

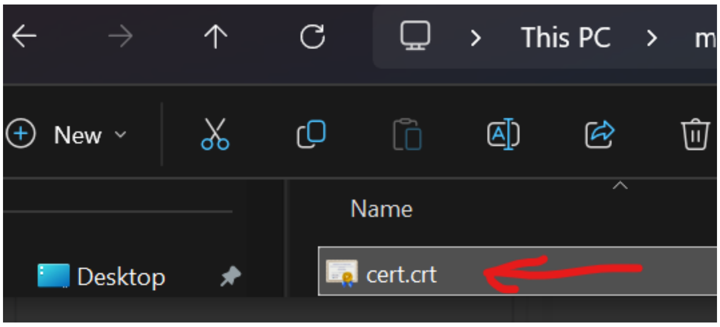
openssl pkcs12 -in input.pfx -nocerts -nodes -out private.key

And the other to extract the cert:

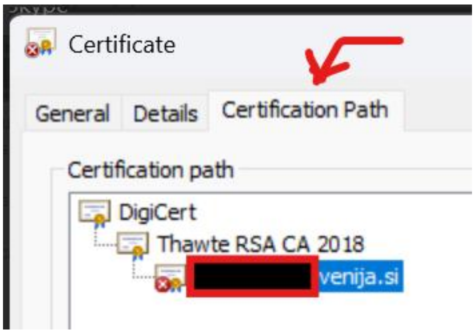
```
openssl pkcs12 -in input.pfx -clcerts -nokeys -out certificate.crt
```

You will get the private.key file and the certificate.crt which we will use later.

4. Chain file is also required:
   Double-click on the .crt which will open a pop-up window



Navigate to the last tab – Certification path.

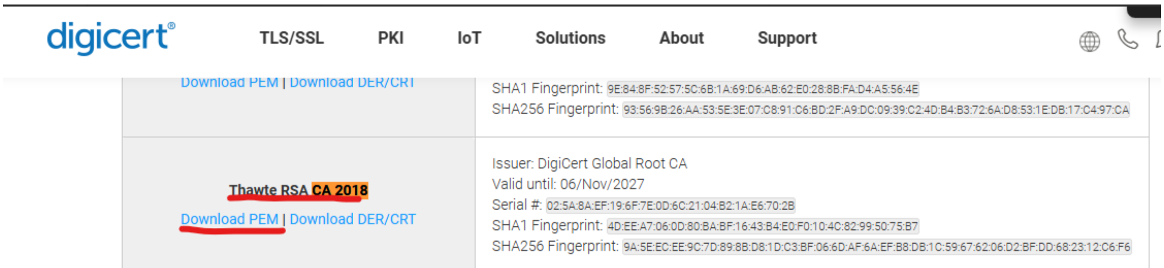


Here you will see the cert issuer tree; it could be only 1 or it can be multiple, you will need to download them for each one.

Now you need to Navigate to the issuer site (in my case DigiCert) and search for "Root certificates".

My case:

https://www.digicert.com/kb/digicert-root-certificates.htm



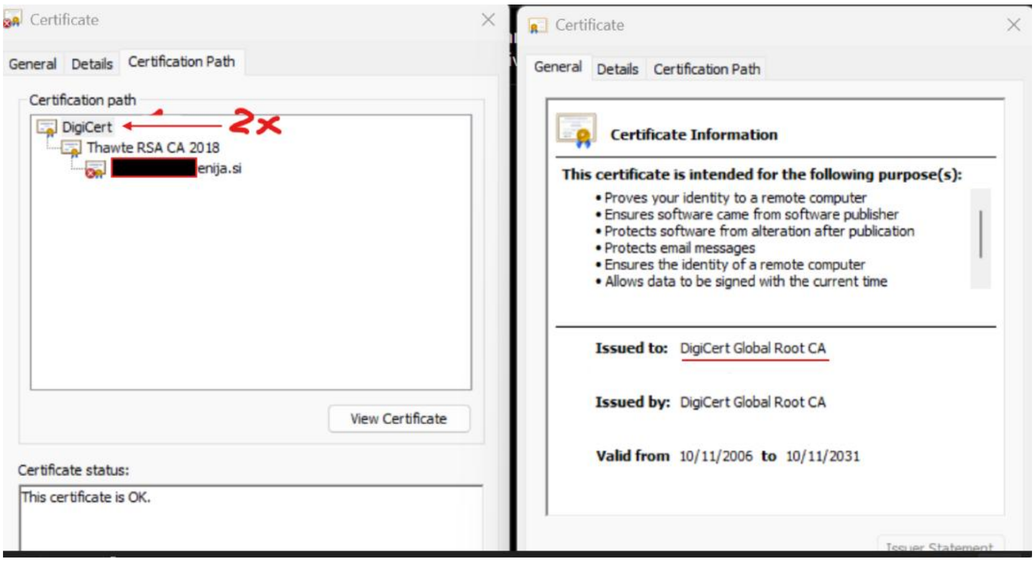
Download PEM | Download DER/CRT

SHA1 Fingerprint: 9E:84:8F:52:57:5C:6B:1A:69:D6:AB:62:E0:28:8B:FA:D4:A5:56:4E
SHA256 Fingerprint: 93:56:9B:26:AA:53:5E:3E:07:C8:91:C6:BD:2F:A9:DC:09:39:C2:4D:B4:B3:72:6A:D8:53:1E:DB:17:C4:97:CA

Thawte RSA CA 2018
Download PEM | Download DER/CRT

Issuer: DigiCert Global Root CA
Valid until: 06/Nov/2027
Serial #: 02:5A:8A:EF:19:6F:7E:0D:6C:21:04:B2:1A:E6:70:2B
SHA1 Fingerprint: 4D:EE:A7:06:0D:80:BA:BF:16:43:B4:E0:F0:10:4C:82:99:50:75:B7
SHA256 Fingerprint: 9A:5E:EC:EE:9C:7D:89:8B:D8:1D:C3:BF:06:6D:AF:6A:EF:B8:DB:1C:59:67:62:06:D2:BF:DD:68:23:12:C6:F6

This was only the middle cert; now we also need to grab the main cert. We will check who was the issuer.



Certificate

General | Details | Certification Path

Certification path

- DigiCert
  - Thawte RSA CA 2018
    - [redacted]enija.si

View Certificate

Certificate status:

This certificate is OK.

Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures software came from software publisher
- Protects software from alteration after publication
- Protects email messages
- Ensures the identity of a remote computer
- Allows data to be signed with the current time

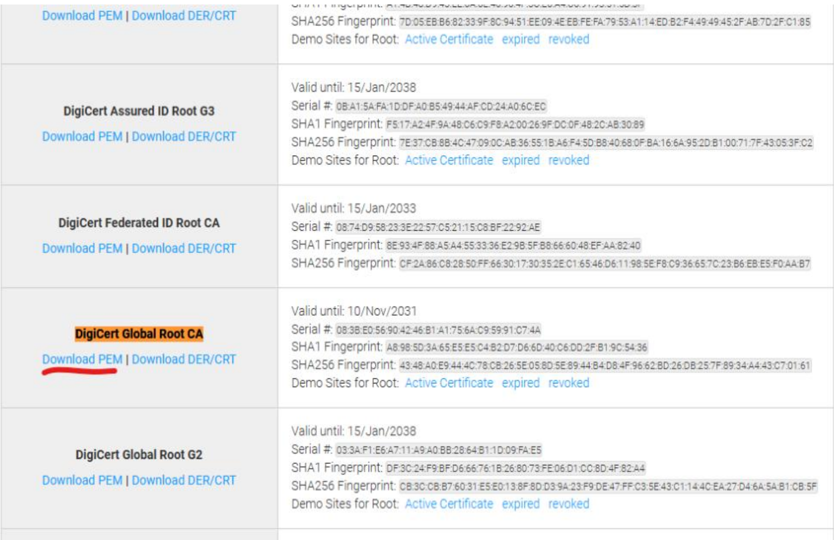
Issued to: DigiCert Global Root CA

Issued by: DigiCert Global Root CA

Valid from 10/11/2006 **to** 10/11/2031

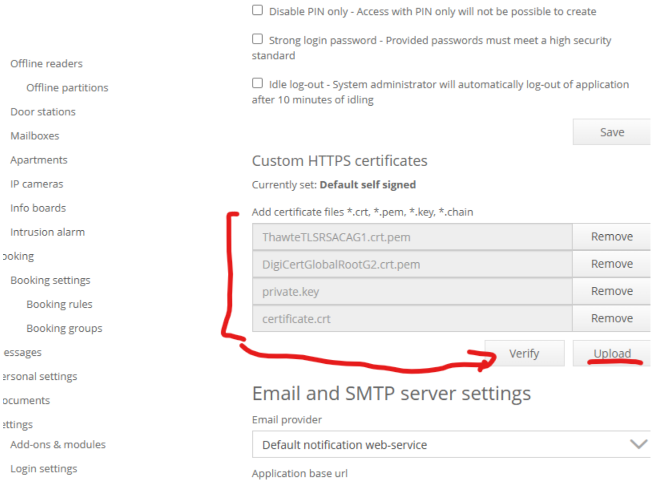
Issuer Statement

And download it again from the Root cert site.



Download PEM | Download DER/CRT	SHA256 Fingerprint: 7D:05:EB:B6:82:33:9F:8C:94:51:EE:09:4E:EB:FE:FA:79:53:A1:14:ED:B2:F4:49:49:45:2F:AB:7D:2F:C1:85 Demo Sites for Root: Active Certificate expired revoked
DigiCert Assured ID Root G3 Download PEM | Download DER/CRT	Valid until: 15/Jan/2038 Serial #: 0B:A1:5A:FA:1D:DF:A0:B5:49:44:AF:CD:24:A0:6C:EC SHA1 Fingerprint: F5:17:A2:4F:9A:48:C6:C9:F8:A2:00:26:9F:DC:0F:48:2C:AB:30:89 SHA256 Fingerprint: 7E:37:CB:8B:4C:47:09:0C:AB:36:55:1B:A6:F4:5D:B8:40:68:0F:BA:16:6A:95:2D:B1:00:71:7F:43:05:3F:C2 Demo Sites for Root: Active Certificate expired revoked
DigiCert Federated ID Root CA Download PEM | Download DER/CRT	Valid until: 15/Jan/2033 Serial #: 08:74:D9:58:23:3E:22:57:C5:21:15:C8:BF:22:92:AE SHA1 Fingerprint: 8E:93:4F:88:A5:A4:55:33:36:E2:9B:5F:B8:66:60:48:EF:AA:82:40 SHA256 Fingerprint: CF:2A:86:C8:28:50:FF:66:30:17:30:35:2E:C1:65:46:D6:11:98:5E:F8:C9:36:65:7C:23:B6:EB:E5:F0:AA:B7
DigiCert Global Root CA Download PEM | Download DER/CRT	Valid until: 10/Nov/2031 Serial #: 08:3B:E0:56:90:42:46:B1:A1:75:6A:C9:59:91:C7:4A SHA1 Fingerprint: A8:98:5D:3A:65:E5:E5:C4:B2:D7:D6:6D:40:C6:DD:2F:B1:9C:54:36 SHA256 Fingerprint: 43:48:A0:E9:44:4C:78:CB:26:5E:05:8D:5E:89:44:B4:D8:4F:96:62:BD:26:DB:25:7F:89:34:A4:43:C7:01:61 Demo Sites for Root: Active Certificate expired revoked
DigiCert Global Root G2 Download PEM | Download DER/CRT	Valid until: 15/Jan/2038 Serial #: 03:3A:F1:E6:A7:11:A9:A0:BB:28:64:B1:1D:09:FA:E5 SHA1 Fingerprint: DF:3C:24:F9:BF:D6:66:76:1B:26:80:73:FE:06:D1:CC:8D:4F:82:A4 SHA256 Fingerprint: CB:3C:CB:B7:60:31:E5:E0:13:8F:8D:D3:9A:23:F9:DE:47:FF:C3:5E:43:C1:14:4C:EA:27:D4:6A:5A:B1:CB:5F Demo Sites for Root: Active Certificate expired revoked

5. Now I have 4 files in my case, which you can upload into the GUI of Nova and once you are done, click on Verify which will check all the files together and check if they are valid, a pop-up will show with the error what went wrong or the OK message informing you about the cert content.
   If OK, you can press confirm, and it will overwrite the existing (expired) certs.



□ Disable PIN only - Access with PIN only will not be possible to create

□ Strong login password - Provided passwords must meet a high security standard

□ Idle log-out - System administrator will automatically log-out of application after 10 minutes of idling

Save

Custom HTTPS certificates

Currently set: **Default self signed**

Add certificate files *.crt, *.pem, *.key, *.chain

ThawteTLSRSACAG1.crt.pem	Remove
DigiCertGlobalRootG2.crt.pem	Remove
private.key	Remove
certificate.crt	Remove

Verify | Upload

Email and SMTP server settings

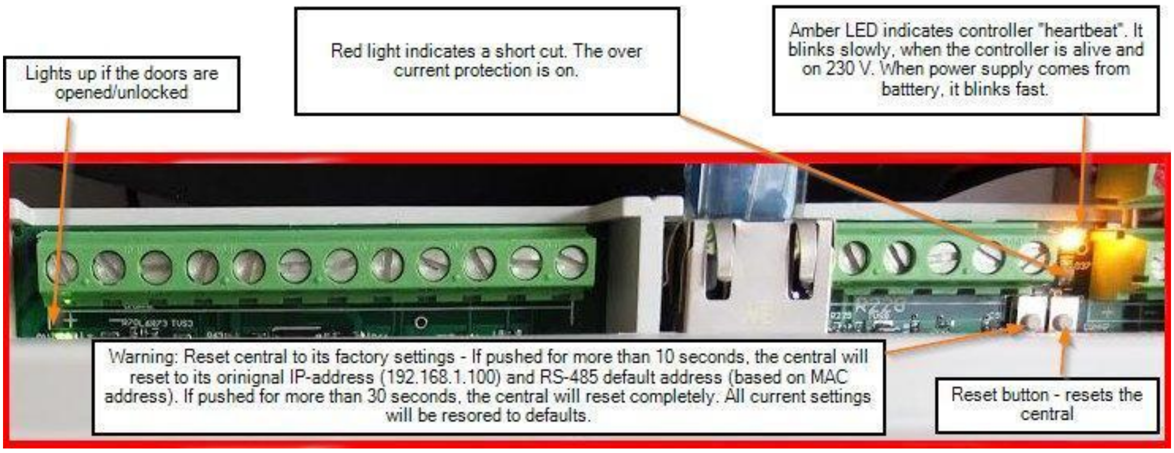
Email provider

Default notification web-service

Application base url

32. Appendix A - Description of LEDs and buttons on central

There are two types of central Hardware and some differences in position/color of the LEDs and buttons. Here are the descriptions of both:



Lights up if the doors are opened/unlocked

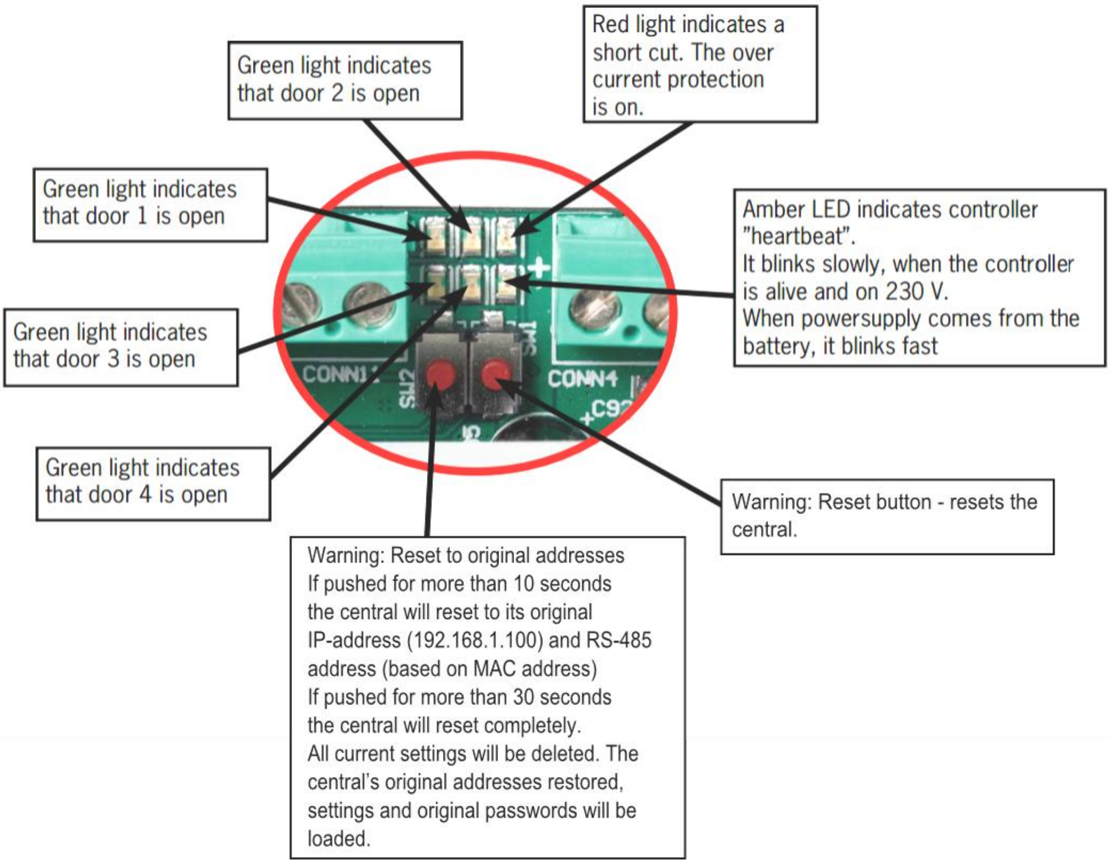
Red light indicates a short cut. The over current protection is on.

Amber LED indicates controller "heartbeat". It blinks slowly, when the controller is alive and on 230 V. When power supply comes from batttery, it blinks fast.

Warning: Reset central to its factory settings - If pushed for more than 10 seconds, the central will reset to its orinignal IP-address (192.168.1.100) and RS-485 default address (based on MAC address). If pushed for more than 30 seconds, the central will reset completely. All current settings will be resored to defaults.

Reset button - resets the central

Picture 32.1: LEDs and buttons on the new Alpha central



Green light indicates that door 2 is open

Red light indicates a short cut. The over current protection is on.

Green light indicates that door 1 is open

Amber LED indicates controller "heartbeat".
It blinks slowly, when the controller is alive and on 230 V.
When powersupply comes from the battery, it blinks fast

Green light indicates that door 3 is open

Green light indicates that door 4 is open

Warning: Reset button - resets the central.

Warning: Reset to original addresses
If pushed for more than 10 seconds the central will reset to its original IP-address (192.168.1.100) and RS-485 address (based on MAC address)
If pushed for more than 30 seconds the central will reset completely.
All current settings will be deleted. The central's original addresses restored, settings and original passwords will be loaded.

Picture 32.2: LEDs and buttons on the old Alpha central

33. Appendix B - Nova software feature possibility list

Package/Module	Description	Administrator client	200 extra users	10 extra doors	Use any card	XML integration	Offline +	Door stations	Python scripting
NovaSimpli	price: free, no schedules - only 24h, no offline doors, only one - standalone central	no	yes	no - only one standalone central	yes	no	no	no	no
NovaSimpli 350	price: free, no schedules - only 24h, no offline doors, no events history, only one - standalone central	no	yes	no - only one standalone central	yes	no	no	no	no
Nova10	10 doors/100 users	yes	yes	yes	yes	yes	yes	yes	yes
Nova100	100 doors/1500 users	yes	yes	yes	yes	yes	yes	yes	yes
NovaPRO	250 doors/3000 users	yes	yes	yes	yes	yes	yes	yes	yes
NovaServer	500 doors/5000 users	yes	yes	yes	yes	yes	yes	yes	yes

Table 31.1: Nova software feature possibility list

List of licenses compatible with NovaSimpli or NovaSimpli350:

- Nova10, Nova100, NovaServer,
- Extra users,
- Unprotected cards,
- Door widgets,
- Cloud access,
- DoorApp.