

# IMAporter PC Admin

PC Admin app for IMAporter Basic ACS



User manual

## DOCUMENT HISTORY

Revision	Date	Author	Description
v1.0	30. 8. 2017	Karel Kalivoda	First version
v1.1	9. 8. 2018	Karel Kalivoda	IDcloud update (Mobile Keys)

## TABLE OF CONTENTS

1.	IMAporter PC Admin .....	4
1.1	Introduction to IMAporter ACS .....	4
1.2	IMAporter logic and bonds.....	4
2	Getting started – 7 step guide .....	6
2.1.1	Install the IMAporter Admin SW .....	6
2.1.2	Settings tab.....	7
2.1.3	Communication ports tab.....	7
2.1.4	Readers tab.....	9
2.1.5	Groups tab .....	12
2.1.6	Identifiers tab .....	13
2.1.7	Upload data .....	16
3	Access rights management.....	17
3.1	Identifiers tab .....	17
3.1.1	Editing single/multiple entries .....	18
3.1.2	Adding and mass adding new IDs from reader .....	18
3.1.3	Importing IDs from CSV file .....	20
3.1.4	Adding Mobile Keys for mobile device .....	21
3.2	Groups tab.....	23
3.2.1	Adding and Editing Groups.....	24
3.2.2	Binding group with readers .....	25
3.2.3	Limiting group access according to calendar .....	26
3.3	Calendars tab.....	27
3.3.1	Standard calendars.....	28
3.3.2	Permanent unlock calendars.....	29
3.4	Holidays tab.....	30
4	Settings and configuration .....	31
4.1	Communication ports tab.....	31
4.1.1	Adding new USB connection .....	31

4.1.2	Adding new IP connection.....	32
4.2	Settings tab.....	34
4.2.1	General settings.....	35
4.2.2	Import from / Export for IMAporter Mobile Admin.....	35
4.2.3	Global reader settings .....	37
4.2.4	Login to IMAporter IDcloud.....	38
4.2.5	Admin login and Advanced settings .....	39
4.2.6	Admin: Selecting ID media and Reader configuration .....	39
4.2.7	Admin: app functions restriction.....	40
4.2.8	FW update .....	40
4.3	Readers tab.....	43
4.3.1	Adding new reader .....	43
4.3.2	Reader IDs and communication ports.....	44
4.3.3	Individual reader settings.....	44
4.3.4	Assigning permanent unlock and holidays.....	45
4.3.5	Reader overview.....	46
5	Communication .....	47
5.1	Operations above a single reader .....	47
5.2	Operations above multiple readers.....	48
5.2.1	Communication test .....	48
5.2.2	Data upload .....	50
5.2.3	Events download .....	50
5.2.4	Automatic events downloading .....	51
6	Browsing Events history and statistics .....	52
6.1	Browsing events .....	52
6.2	Statistics.....	52
6.3	Exporting events.....	52
7	Connecting 3 <sup>rd</sup> party SW.....	53
7.1	Direct DB access .....	53
7.2	Remotely triggered communication.....	54
8	LAN module configuration .....	55
9	Troubleshooting and support.....	<b>Chyba! Záložka není definována.</b>
9.1	Troubleshooting and communication errors .....	<b>Chyba! Záložka není definována.</b>

# 1. IMAporter PC Admin

## 1.1 Introduction to IMAporter ACS

The **IMAporter PC Admin** is designed for site admins as a management tool to control and assign user access rights to individual doors within the **IMAporter Basic system**. It is a computer software running on Windows XP, 7, 8, 10 and Windows Server.

All data is stored in SQLite file database in a file with **.sqlite** extension.

The app navigation is organized in individual tabs: **Identifiers, Groups, Readers, Calendars, Holidays, Communication ports, Settings** and menu items **Communication** and **Statistics**.

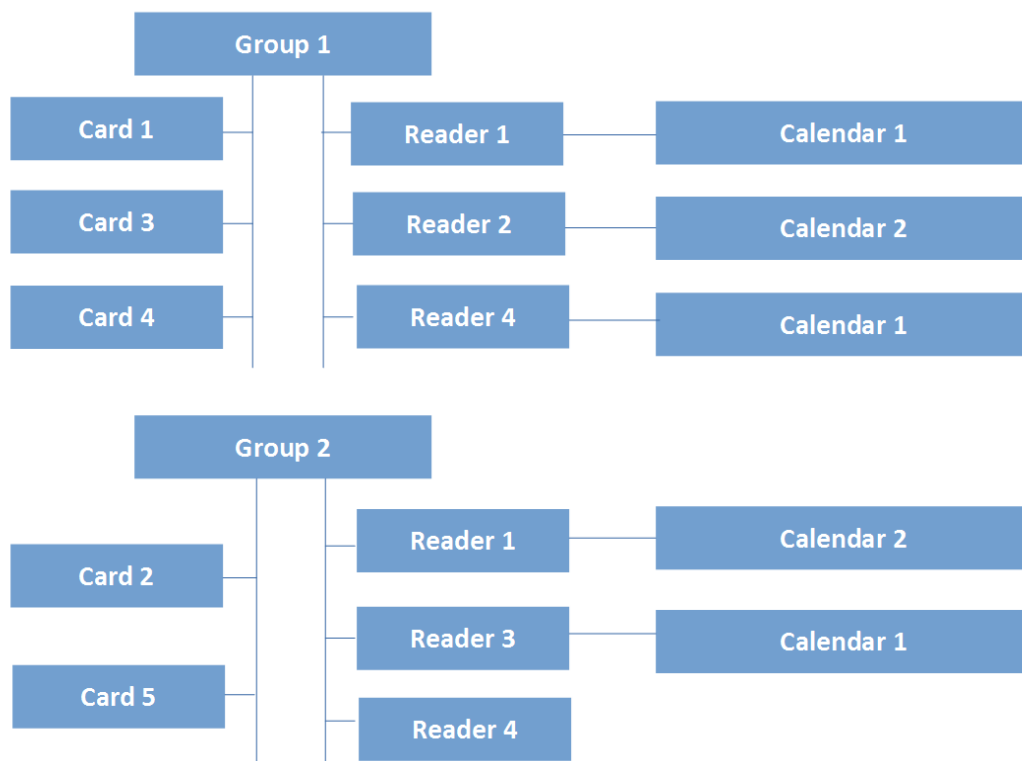
## 1.2 IMAporter logic and bonds

### Access rights and access groups

**Identifiers** (identification media such as cards and mobile devices) can be linked with a **Group** (of access rights). At the same time a **Group** is linked to specific **Readers** according to the diagram below. The link **Reader-Group** can be assigned with a **Calendar** limiting the access times of the **Groups** users to a specific door.

Each **Identifier** (card) can be a member of only one group.

A **Reader** can be linked up to 20 different **Groups** and 20 different **Calendars**.

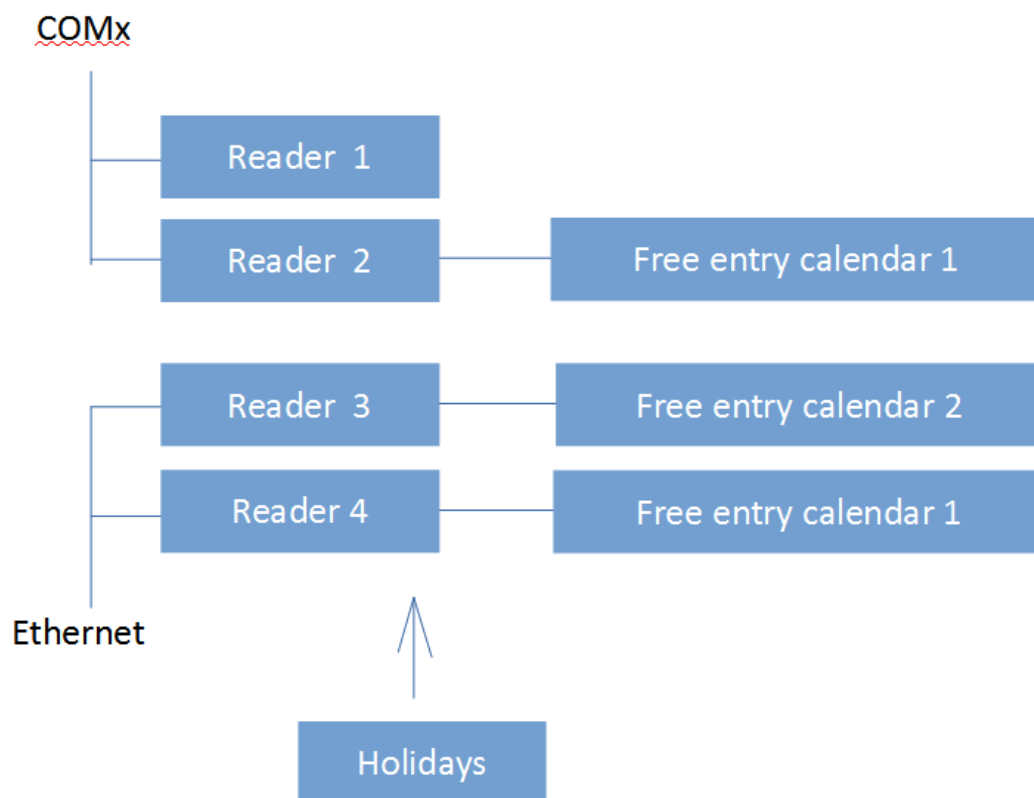


The logical bonds as shown above define a recommended order in which to set the system and the links between individual settings:

<b>Communic. ports:</b>	define communication interfaces
<b>Calendars:</b>	define access limiting calendars and calendars for free entry (if they will be used)
<b>Readers:</b>	define readers, assign communication ports and free entry calendars
<b>Groups:</b>	define groups, pair readers and access limiting calendars
<b>Identifiers:</b>	define ID cards, mobile devices and pair into predefined groups
<b>Holidays:</b>	define public holidays if not already loaded from CSV

## Communication bonds

The system allows to use multiple communication interfaces at once and each communication interface can connect up to 32 readers over RS485 serial bus as illustrated on the diagram below. The configuration copies the physical connection of the readers. Each reader on the serial bus must be assigned a unique ID number (1-32). This ID number is assigned by system supplier or installation company during Reader configuration using the IMAporter ACS Config mobile app.

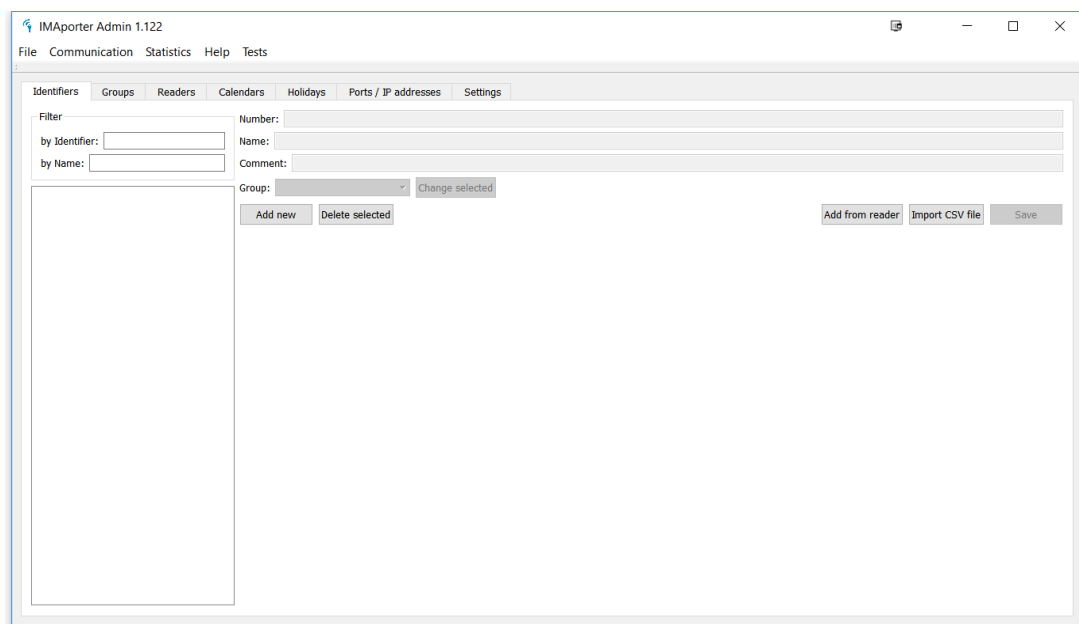


Each reader can also be set a different Free entry calendar allowing users to pass through this door at specified times without the need to identify themselves.

## 2 Getting started – 7 step guide

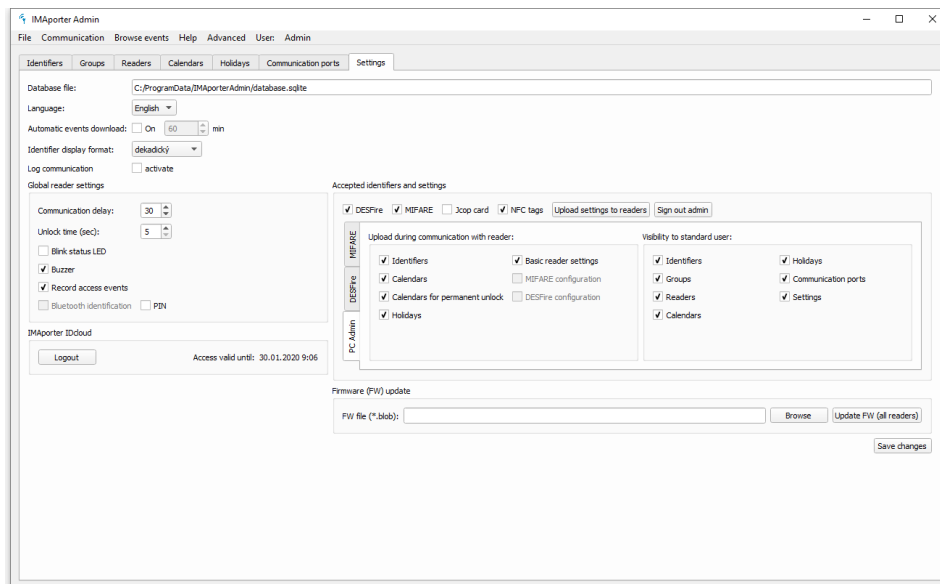
### 2.1.1 Install the IMAPorter Admin SW

1. Install it on your PC, launch it and create a new database
2. Select a holidays file corresponding to your country or create a new one and save it to installation folder\holidays\
  - CSV file with holidays needs to be created in the same format as the original files and must be in valid CSV format. To make sure CSV is valid, create it in Excel and save as CSV.
3. You will see a window with empty database



## 2.1.2 Settings tab

Start by navigating to **Settings tab** and entering basic system settings. When installing a new system press CTRL + Q and enter a password 1003001 to display additional settings for accepted identification media

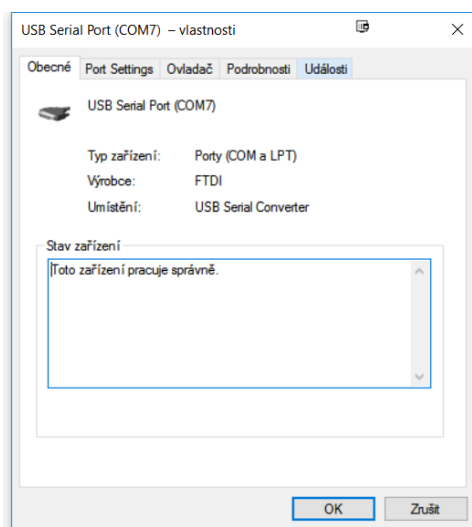


## 2.1.3 Communication ports tab

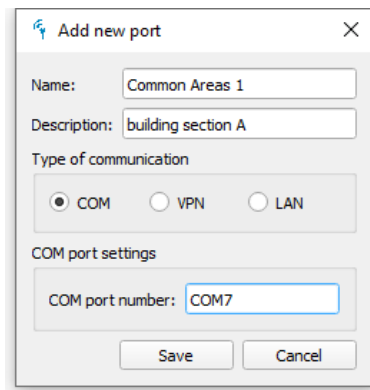
Now connect and configure the readers. If the readers are connected and set according to the installation manual, navigate to the **Communication ports tab** and add a new port:

### a) Add a device connected over serial (COM) port

- Connect the USB converter to your PC and look up the virtual COM port in the system settings



- Click the **Add communication port** button and type it down to the dialog window

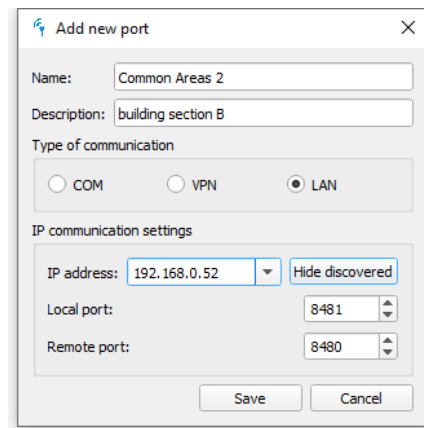


The screenshot shows the 'Add new port' dialog box with the following fields and settings:

- Name:** Common Areas 1
- Description:** building section A
- Type of communication:** COM (selected), VPN, LAN
- COM port settings:**
  - COM port number:** COM7
- Buttons:** Save, Cancel

#### b) Add a device connected over LAN

- In the **Add communication port** select LAN and hit **Discover devices** button or enter the IP address and ports of the specific ACS

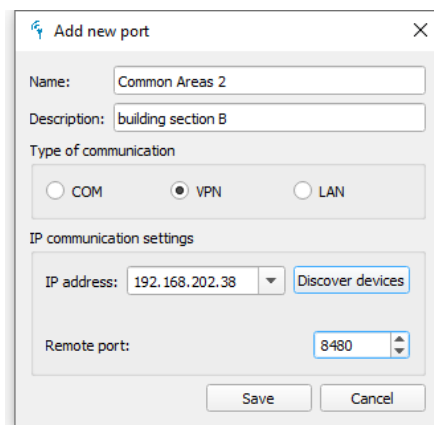


The screenshot shows the 'Add new port' dialog box with the following fields and settings:

- Name:** Common Areas 2
- Description:** building section B
- Type of communication:** COM, VPN, LAN (selected)
- IP communication settings:**
  - IP address:** 192.168.0.52 (dropdown menu)
  - Local port:** 8481 (spinner)
  - Remote port:** 8480 (spinner)
  - Buttons:** Hide discovered, Save, Cancel

#### a) Add a device connected over mobile network or VPN

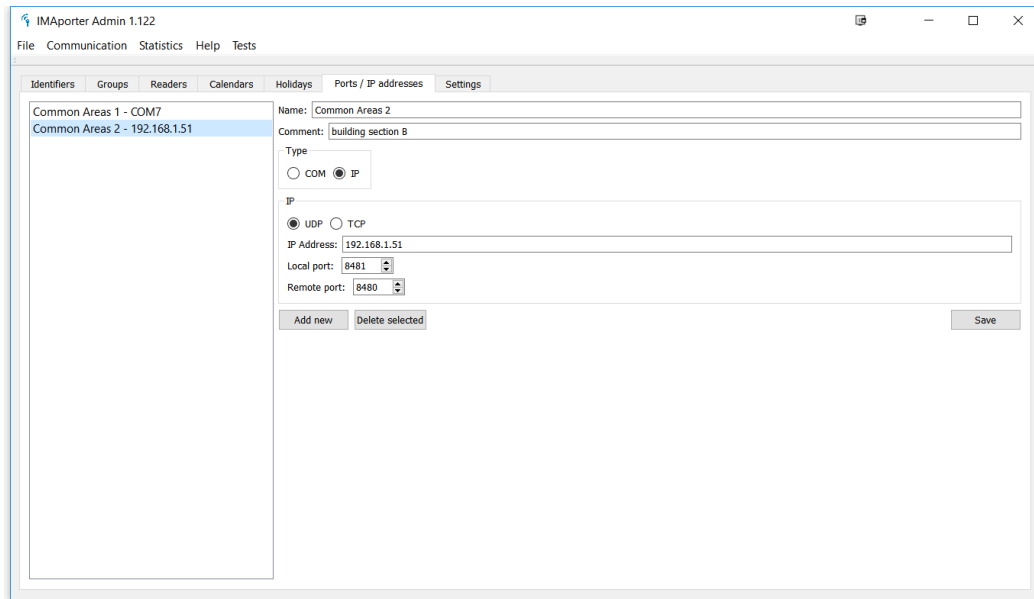
- In the **Add communication port** select VPN and type the IP address and ports of the specific ACS



The screenshot shows the 'Add new port' dialog box with the following fields and settings:

- Name:** Common Areas 2
- Description:** building section B
- Type of communication:** COM, VPN (selected), LAN
- IP communication settings:**
  - IP address:** 192.168.202.38 (dropdown menu)
  - Remote port:** 8480 (spinner)
  - Buttons:** Discover devices, Save, Cancel



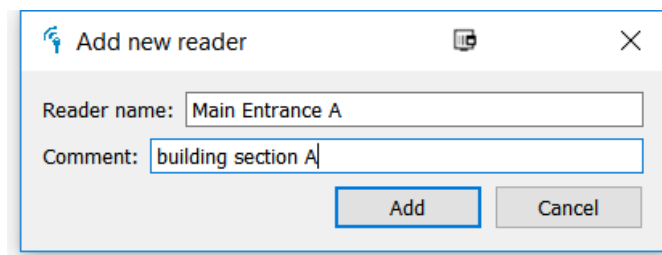


Now we have two addresses to be used for controlling our ACS

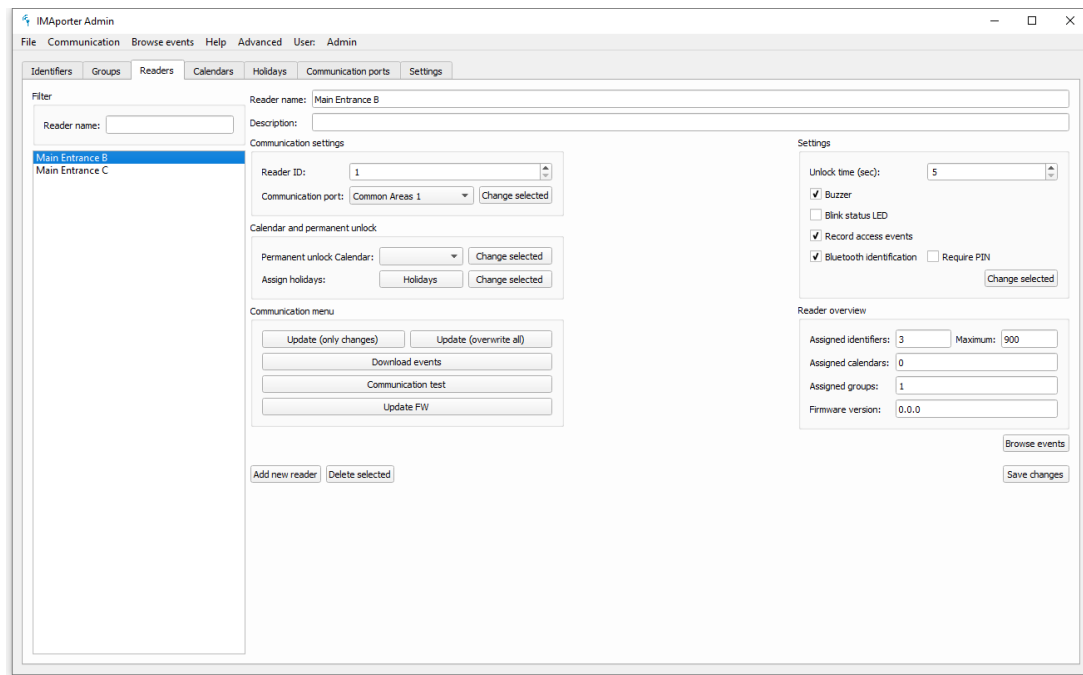
## 2.1.4 Readers tab

Let's now add the door readers.

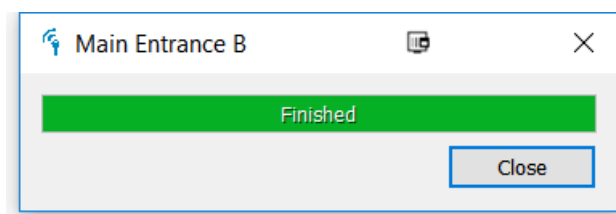
- Navigate to the **Readers tab** and **Add new reader**.



- Configure the newly added reader. You should select the **Communication port** to which the reader is connected and type in the reader ID that it was configured during installation (using ACS Config mobile app).  
In the settings section of the reader tab, you can set the individual settings for this particular reader.



- c) Once the reader is configured, click the **Communication test button** to test that it has been configured correctly. A dialog like this should appear:



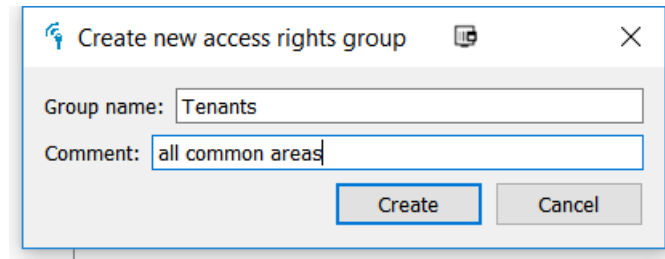
If in any case you receive a RED message with error code, you should check if everything has been configured correctly. The following list should help you with troubleshooting.

**The most common errors are:**

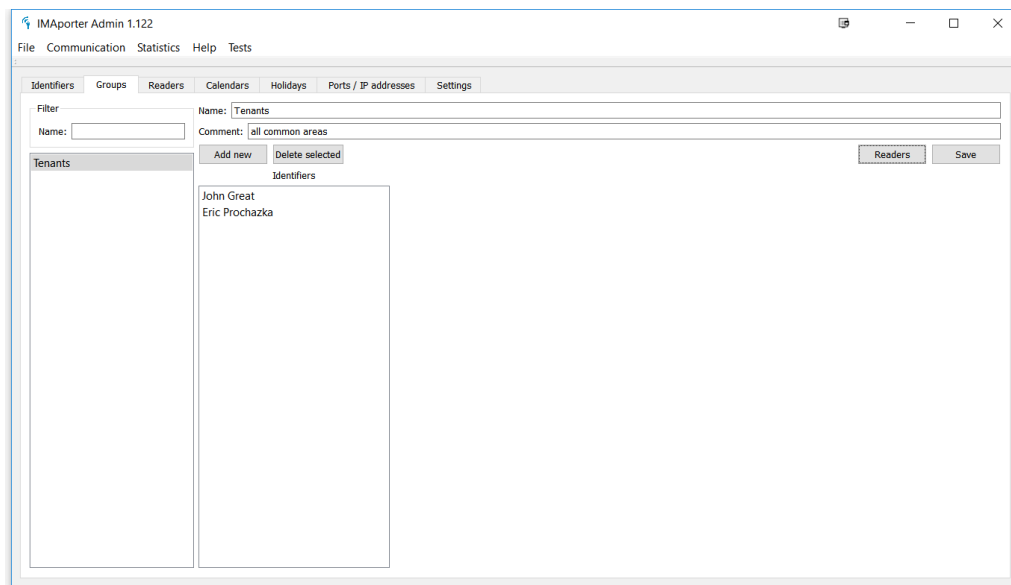
- Wires TxD and RxD between SMR.0x module and reader are not connected or switched
- Reader is assigned a different **Reader ID** than set in PC Admin app
- **Serial connection:** wires between SMR.0x module and USB converter are switched. Correct connection is **485+ -> RS-A and 485- -> RS-B**
- **LAN connection:** J2 DIP switch is in incorrectly position, please check with the manual. For single door installation, all J2 DIP should be in ON position.
- **LAN connection:** the reader and PC are not in the same network (e.g.: 192.168.1.xxx)
- **LAN connection:** the local and remote ports are not configured correctly (please mind that local on ACS is remote on PC)
- **LAN connection:** this connection must use LAN communication port (using UDP protocol), the VPN communication port uses TCP protocol and is only for mobile network connected devices or VPNs
- **LAN connection:** LANTRONIX is configured to a wrong baudrate, it should be 38400. Please check the installation manual.

## 2.1.5 Groups tab

When all readers are added and functional, navigate to **Groups tab** and create a **New group**

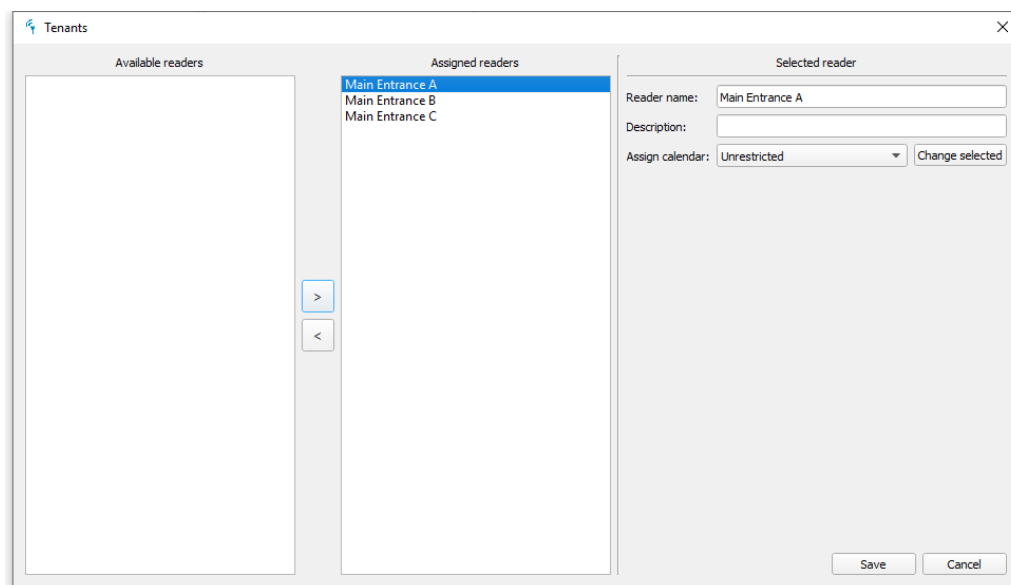


Dialog box titled "Create new access rights group". It contains two input fields: "Group name:" with the value "Tenants" and "Comment:" with the value "all common areas". At the bottom are two buttons: "Create" and "Cancel".



IMAporter Admin 1.122 Groups tab interface. The window title is "IMAporter Admin 1.122". The menu bar includes "File", "Communication", "Statistics", "Help", and "Tests". The "Groups" tab is selected. On the left, there is a "Filter" section with a "Name:" input field. Below it, a list of groups is shown, with "Tenants" selected. To the right of the list are buttons "Add new" and "Delete selected". On the far right are buttons "Readers" and "Save". The main area displays the details for the "Tenants" group: "Name: Tenants" and "Comment: all common areas". Below these are two lists: "Identifiers" (containing "John Great" and "Eric Prochazka") and "Readers" (empty).

Select the group and on the group settings page click the **Readers button**



Tenants group settings interface. The window title is "Tenants". It is divided into three main sections: "Available readers", "Assigned readers", and "Selected reader". The "Available readers" section is empty. The "Assigned readers" section contains a list of readers: "Main Entrance A", "Main Entrance B", and "Main Entrance C". Below this list are two buttons: ">" and "<". The "Selected reader" section contains three input fields: "Reader name:" with the value "Main Entrance A", "Description:" (empty), and "Assign calendar:" with a dropdown menu set to "Unrestricted". To the right of the dropdown is a button "Change selected". At the bottom right are buttons "Save" and "Cancel".

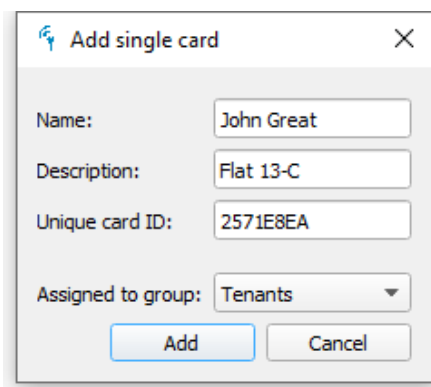
Select the readers that you want to bind with this group – all users in this group will be able to access these readers.

If necessary, each reader can be assigned a calendar. Calendar needs to be prepared in the **Calendars tab** and enables the admin to limit access of users from a specific group to specific doors in preset time periods or days of a week.

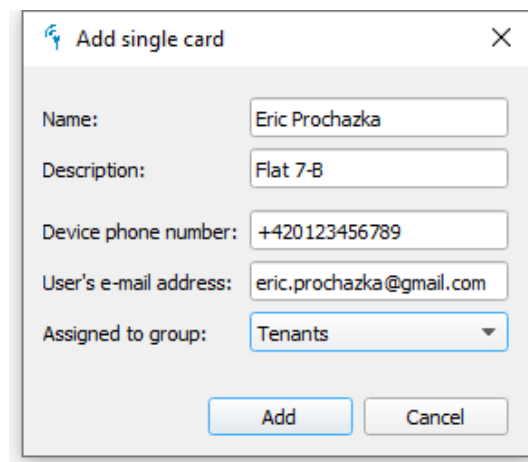
## 2.1.6 Identifiers tab

Navigate to **Identifiers tab** and depending on the Identifier that you want to add, do the following:

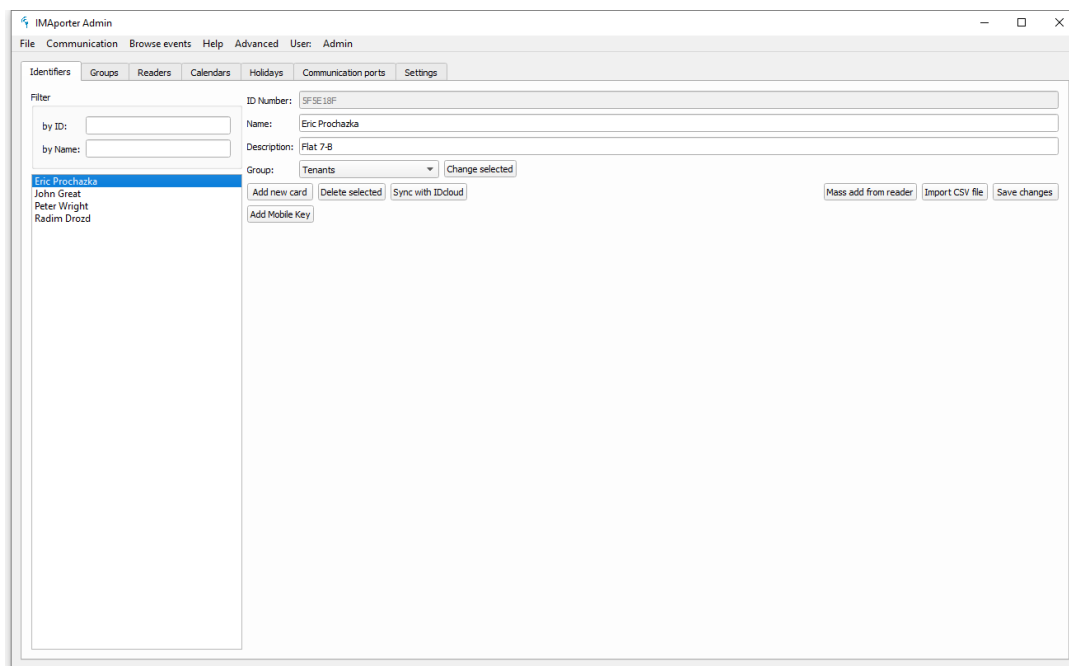
- To **add a card or NFC tag** manually or from a desktop reader (must be compatible with IMAporter), click the **Add new card** button



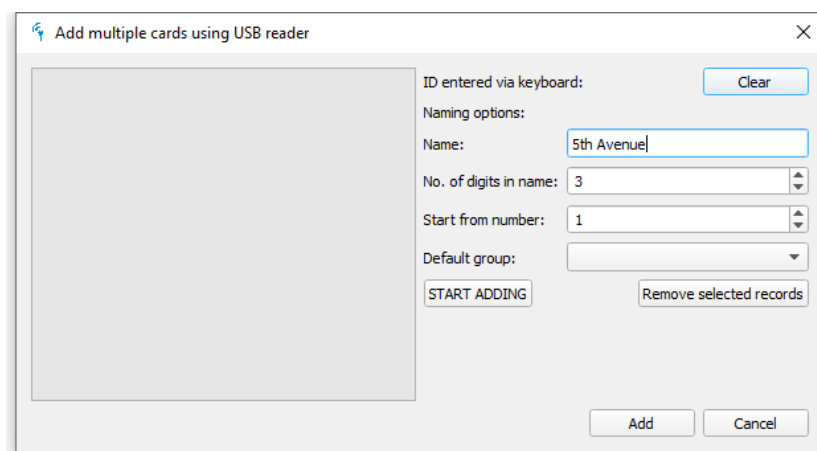
- To **add a Mobile Key** (system must be linked with IMAporter IDcloud and login credentials entered in **Settings tab**+ computer running the PC Admin app must be connected to internet) click the **Add Mobile Key** button.



Now we have two users assigned to user-rights-group Tenants.

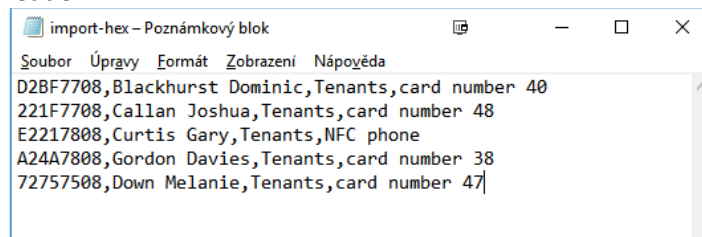


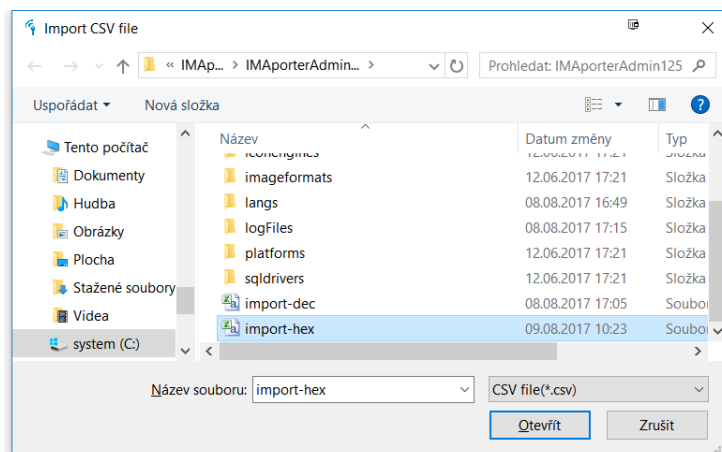
- c) Add from reader – to add multiple tags of the same name, you can use the **Mass add from reader** function. In the following dialog fill in how the cards/IDs should be named and start placing one by one onto the USB reader. Once all are read into the list, click Create to save them to DB.



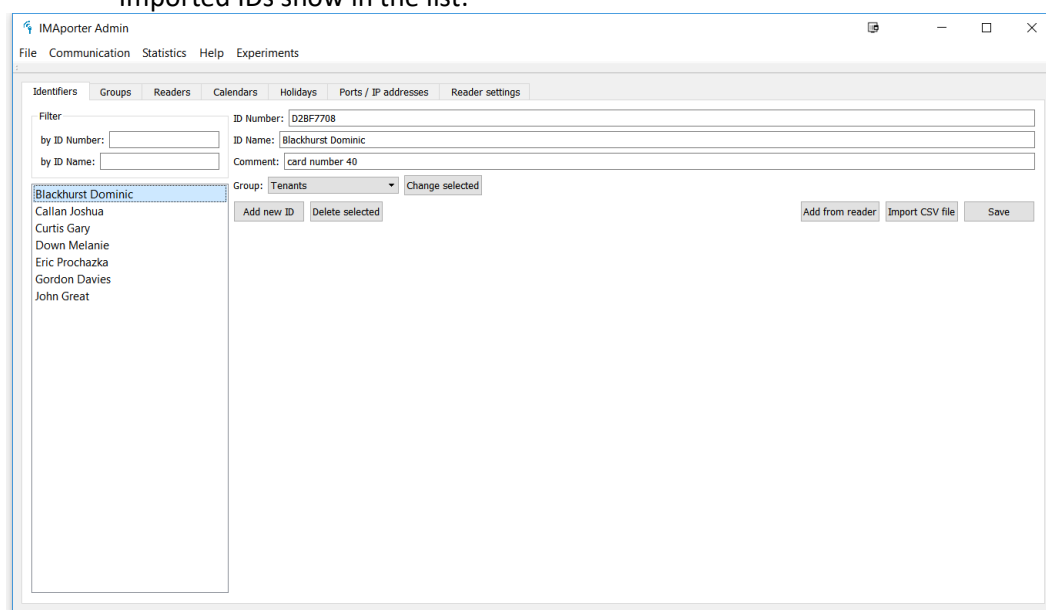
- d) Import CSV file – this feature allows you to prepare a list of cards/IDs in excel spreadsheet and import them to IMAporter Admin at once.

The CSV file needs to have the following structure. Make sure that you use certified USB reader.



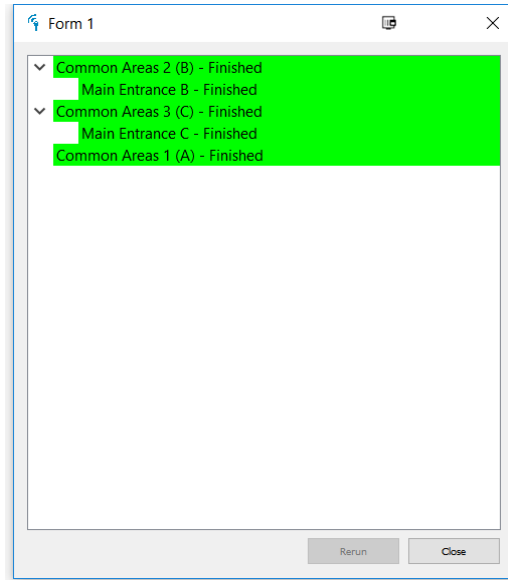


Imported IDs show in the list:



### 2.1.7 Upload data

From the Communication menu select Upload everything. You will be shown a communication dialog listing all reader connected to the system. The readers should one-by-one be uploaded with new data. For repeated communication you can also use the Upload changes option, where only readers with changes in access rights are synchronized.

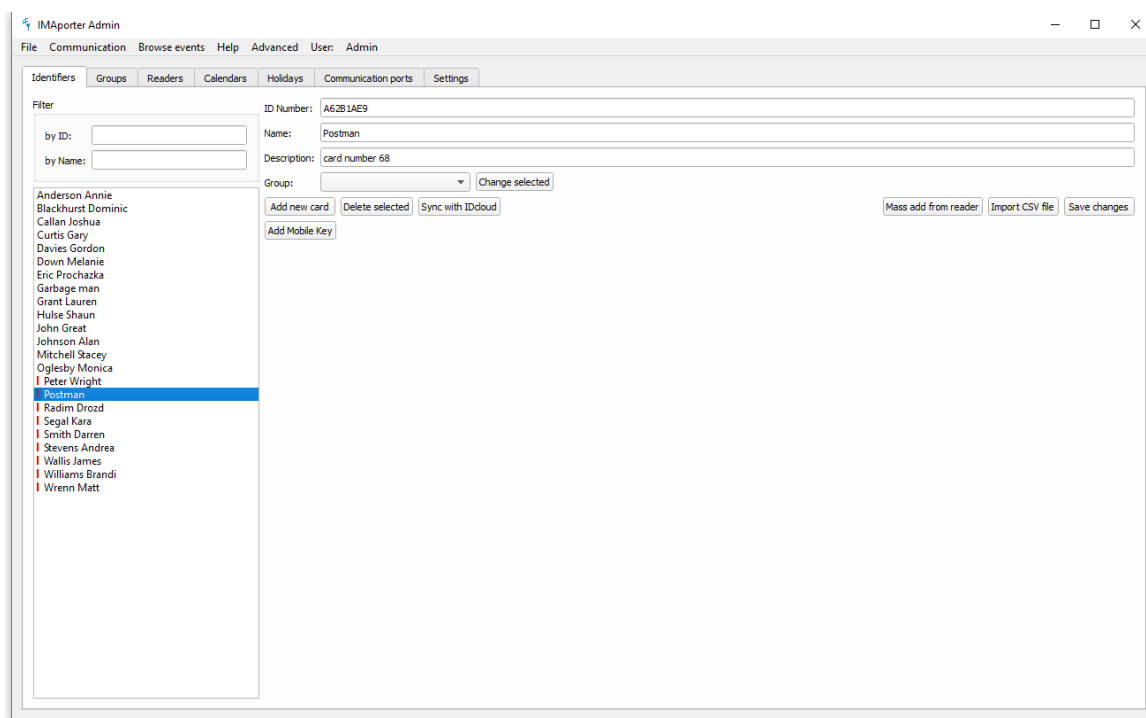




## 3 Access rights management

### 3.1 Identifiers tab

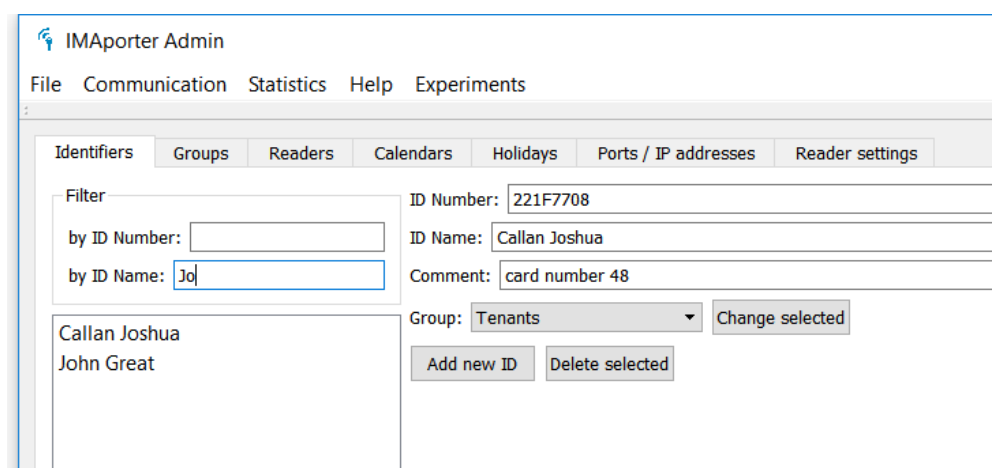
The Identifiers tab lists all user Cards, Tags and Devices added to the system.



The card ID number can be shown in DECADIC or HEXADECIMAL format according to the system settings in the **Settings** tab or during the initial system configuration.

Filtering records can be done by entering text into the **Filter** fields. Filter is always applied from the beginning of a word. In case of multiple words, all are taken into account.

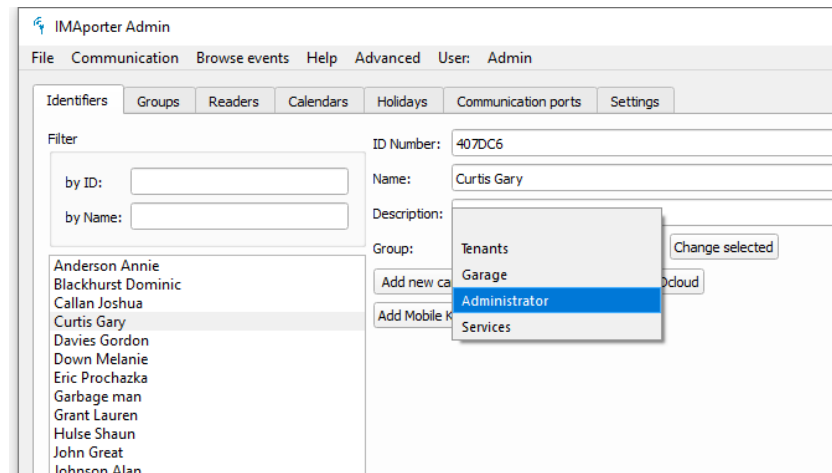
Identifiers without an assigned Group are **marked red** as can be seen in the above screenshot.



### 3.1.1 Editing single/multiple entries

#### Editing a single entry

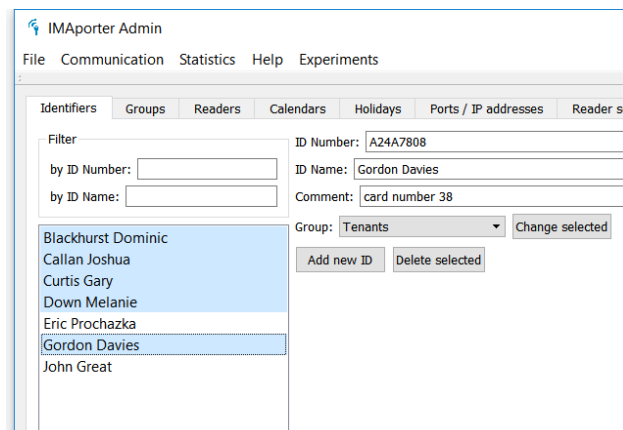
By clicking any record from the list of identifiers, it is opened for viewing and editing. All displayed fields can be changed. After making changes, do not forget to hit the **Save changes** button.



Identifiers without an assigned Group are **marked red**.

#### Editing multiple entries

To edit more records at once, the list supports multiselect. You can select more items by dragging over them with mouse or by holding down CTRL button and clicking the items for selection.



Multiselect function supports only mass change of assigned group. After a change of group has been made, click the **Change selected** button

### 3.1.2 Adding and mass adding new IDs from reader

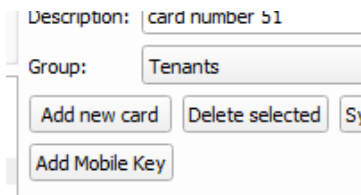
Adding new IDs to IMAporter PC Admin can be done in several ways. This chapter will describe adding directly from an USB reader.

Please make sure the USB reader is compatible with IMAporter system.

The program is compatible with HEX or DEC table readers (reading in a predefined IMAporter format) and the format must be selected in the **Settings** tab. For more information, see the Settings chapter.

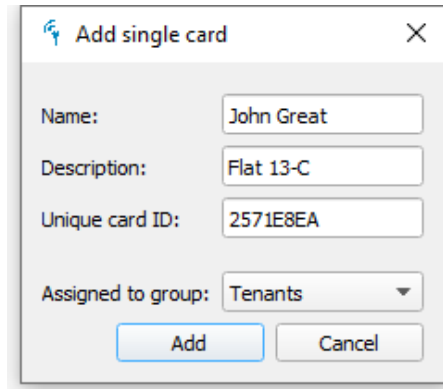
## Add new ID

Adding a single new ID/Card/Tag is done by clicking the **Add new card** button according to the image below.



Description: card number 51  
Group: Tenants  
Add new card Delete selected Sy  
Add Mobile Key

The following dialog appears:



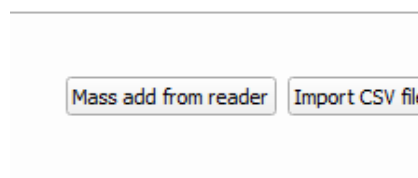
Add single card

Name: John Great  
Description: Flat 13-C  
Unique card ID: 2571E8EA  
Assigned to group: Tenants  
Add Cancel

By clicking **Add**, the record is stored in the database.

## Add multiple IDs

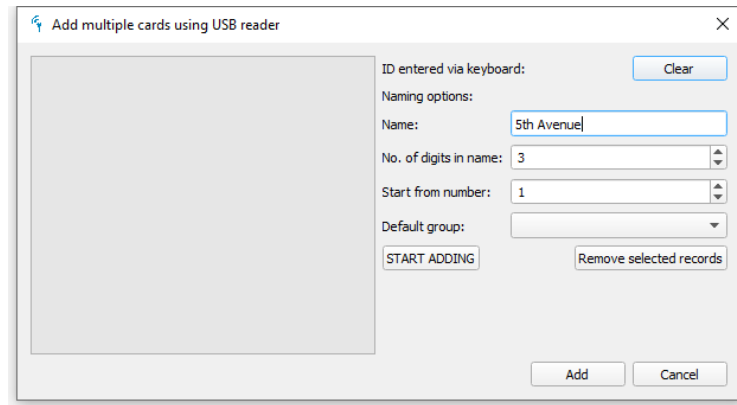
To add multiple IDs/Cards/Tags of the same name, you can use the **Mass add from reader** function.



Mass add from reader Import CSV file

In the following dialog fill in how the Cards/Tags/IDs should be named, what group they should be linked with and start placing one by one onto the USB reader. All loaded IDs will appear in the list on the left together with their generated names.

In case of an error, the list can be cleared to start again or any selected record from the list can be removed.



Once all tags/cards are read into the list, click **Add** to save them to DB.

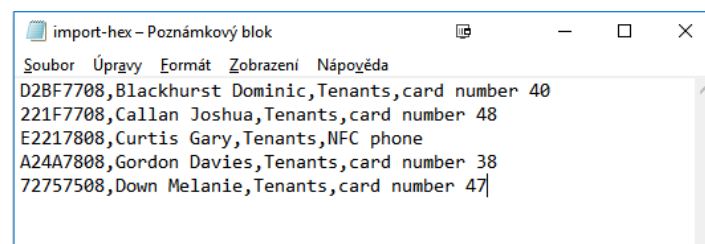
### 3.1.3 Importing IDs from CSV file

This feature allows you to prepare a list of Cards/Tags/IDs in MS Excel or other spreadsheet SW and import them to IMAporter Admin at once.

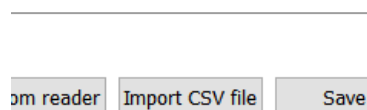
The CSV file needs to be divided by comas or semicolon and have the following structure.

*Note 1: Make sure that you use IMAporter compatible USB reader.*

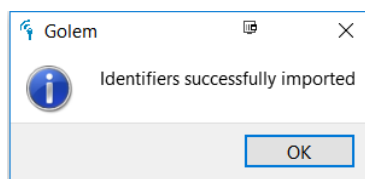
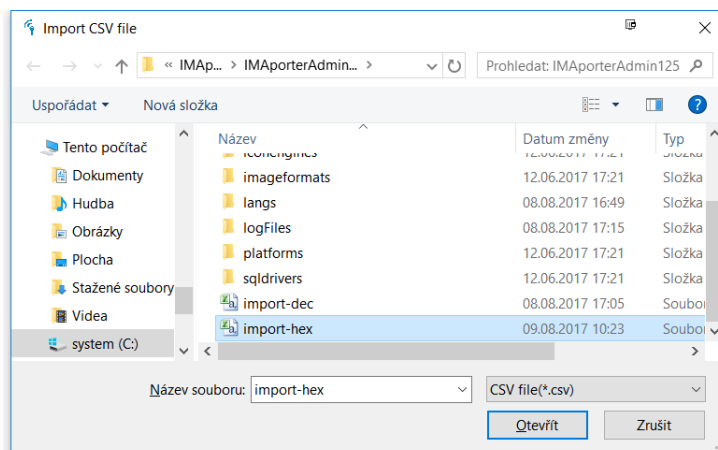
*Note 2: The ID can be in HEX or DEC format depending on the settings of the IMAporter PC Admin (see Settings chapter)*



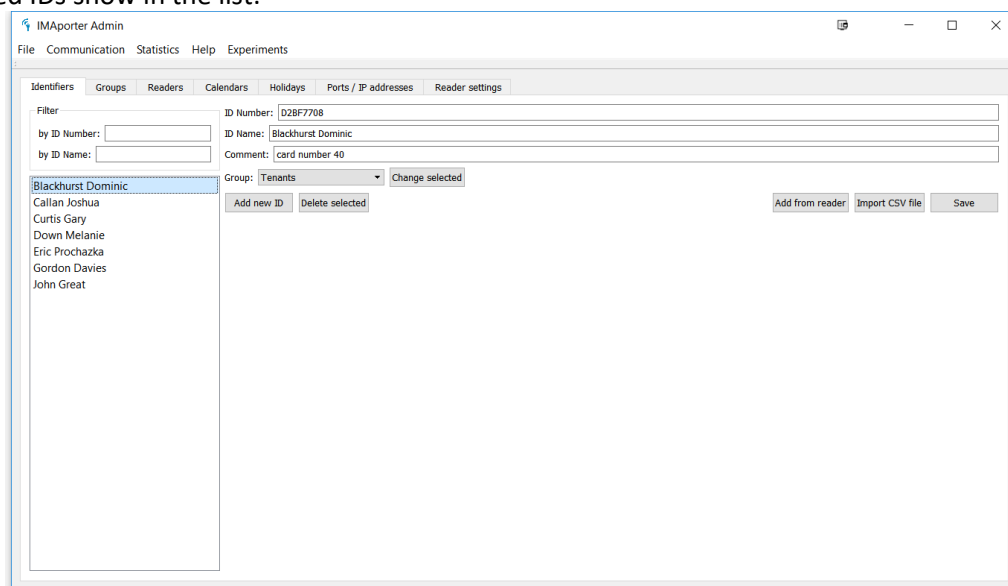
To import a CSV file, hit the **Import CSV file** button in the **Identifiers** tab.



The following dialog will appear:



Imported IDs show in the list:



### 3.1.4 Adding Mobile Keys for mobile device

To use a mobile device as user identifier, a Mobile Key featuring unique device ID needs to be assigned and activated.

To start adding Mobile Keys for mobile devices, you need to make sure that you have the following ready:

- Active IMAporter IDcloud account for your system (please see the relevant **IMAporter IDcloud manual**)
- IMAporter IDcloud credentials entered in the **Settings** tab (more in section [2.1.2 Settings tab](#))
- IMAporter Mobile Key app installed in the users device (please see the relevant **IMAporter Mobile Key app manual**)

All added Mobile Keys are automatically generated in the IMAporter IDcloud and sent to the user via a secure channel.

Each Mobile Key needs to be stored in both ends of the system:

- In the users mobile device (in IMAporter Mobile Key app)
- In the door reader as an authorized identifier (via IMAporter (Mobile/PC) Admin)

To store the Mobile Key into the door reader, it must be managed using the IMAporter Admin app.

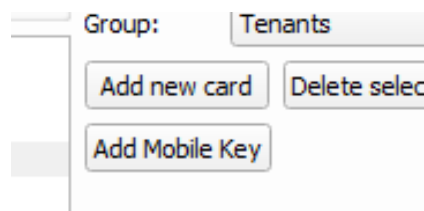
There are two ways how to create and store the Mobile Key:

- Create it directly in IMAporter PC Admin
- Create it through the IMAporter IDcloud web client and synchronize database with the PC Admin.

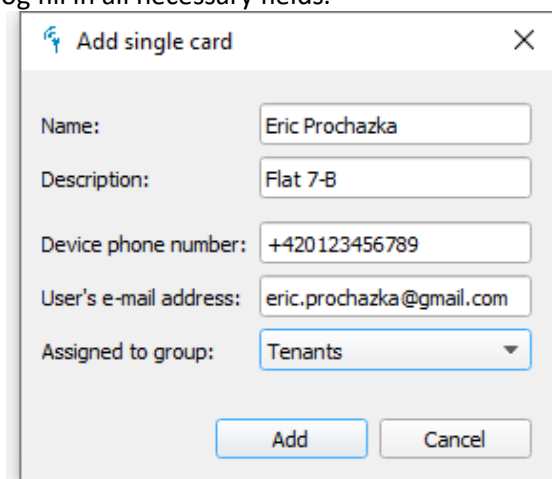


After synchronization, the identifier may have a red rectangle shown next to it. This means that user rights group is not yet assigned.

To create Mobile Key through IMAporter PC Admin, make sure that you have met the above listed conditions and click the **Add Mobile Key** button in the **Identifiers** tab according to the image below.



In the **Add Mobile Key** dialog fill in all necessary fields.



**Add single card**

Name: Eric Prochazka

Description: Flat 7-B

Device phone number: +420123456789

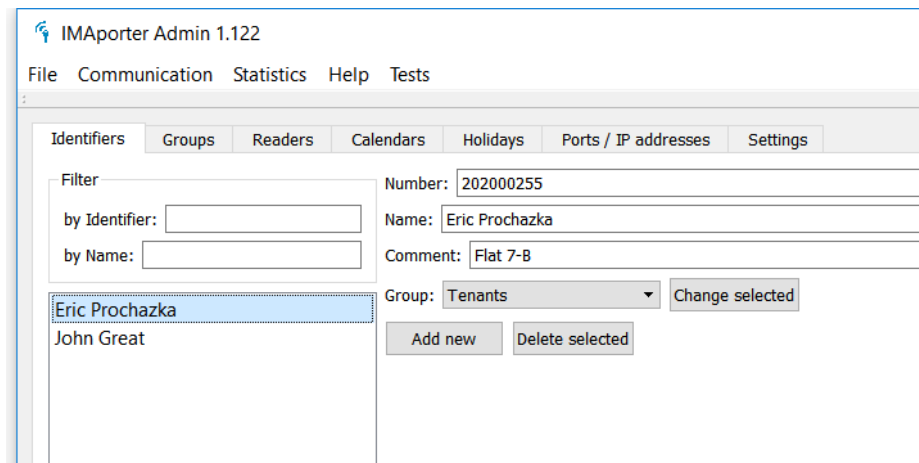
User's e-mail address: eric.prochazka@gmail.com

Assigned to group: Tenants

Add Cancel

Once you click the **Add** button, the PC Admin will contact the IMAporter IDcloud and download the newly generated Mobile Key ID. This process may take few seconds.

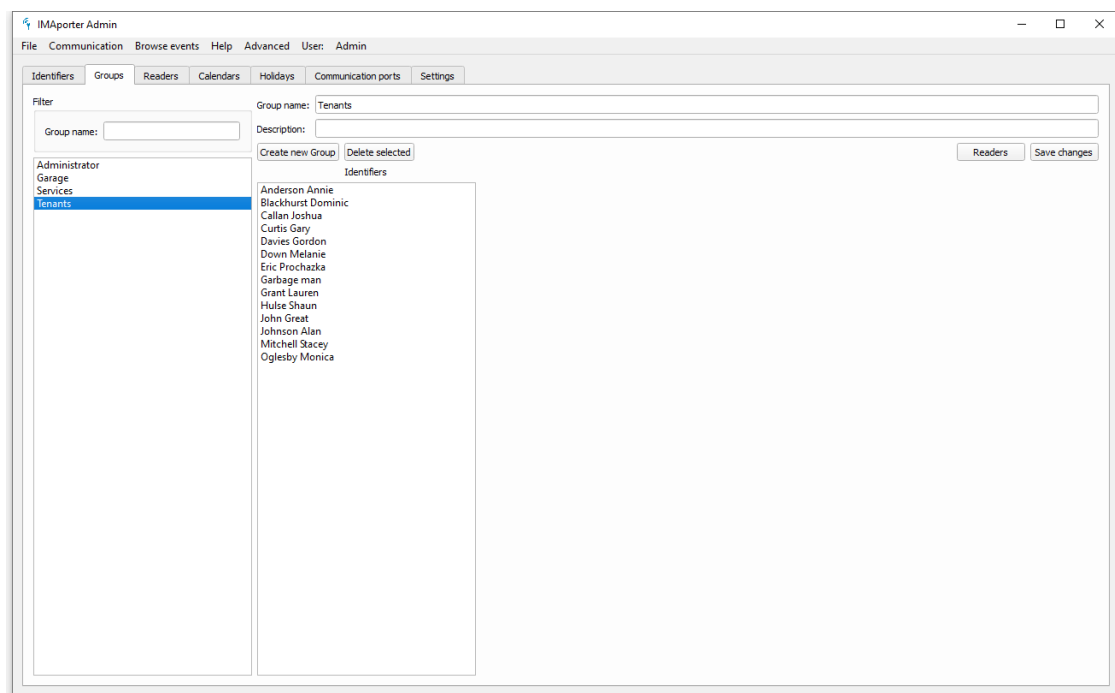
Once an Mobile Key is received, the dialog automatically closes and you will find the user in the Identifiers list.



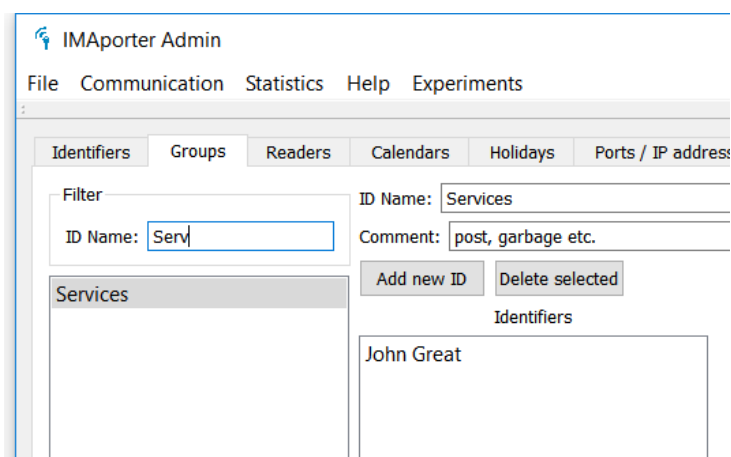
At the same time, the user will receive an Email or SMS with activation code and simple instructions.

## 3.2 Groups tab

The **Groups** tab lists all access rights groups available in the system and shows Identifiers assigned to the individual groups. Link between a group and authorized readers is created using the **Readers** button under each group.



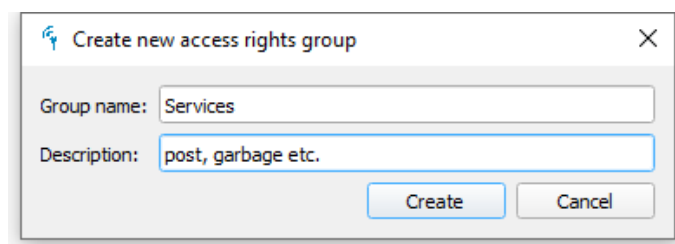
Filtering records can be done by entering text into the **Filter** fields. Filter is always applied from the beginning of a word. In case of multiple words, all are taken into account.



### 3.2.1 Adding and Editing Groups

#### Adding new Groups

Creating a new group is done using the **Create new group** button that will open the following dialog:



When a new group is created, it is necessary to link it to readers its users will be authorized to access. The procedure is described in next chapters.

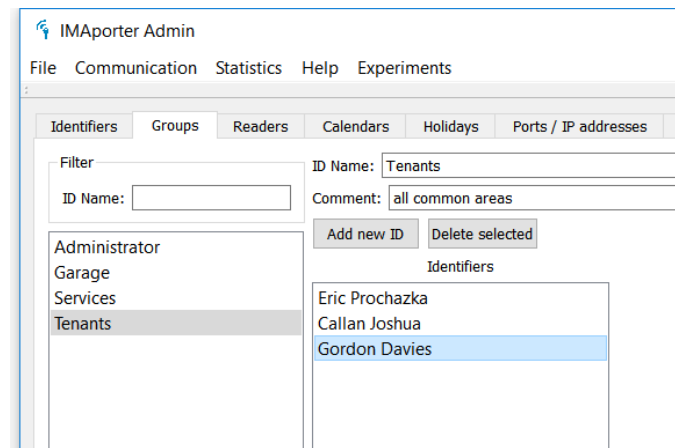
#### Editing Groups

By clicking any record from the list, it is opened for viewing, editing and linking to readers (see next chapter). All displayed fields can be changed. After making changes, do not forget to hit the **Save changes** button.

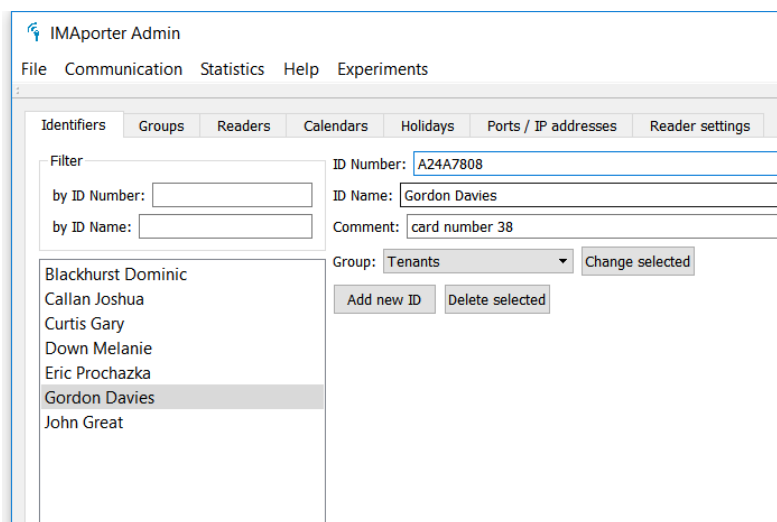
For deletion purposes, it is possible to select more groups at once. You can select more items by dragging over them with mouse or by holding down CTRL button and clicking the items for selection.

Clicking a specific group also shows a list of Identifiers (users) assigned to this group. By double-clicking a listed identifier, the system navigates you to identifier edit form under the **Identifiers** tab.



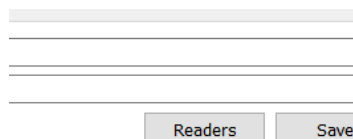


Double-clicking any identifier navigates you to identifier edit form:

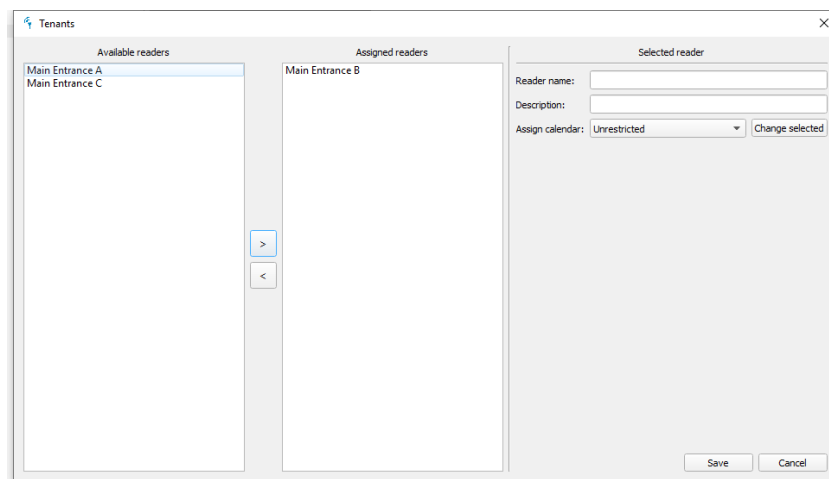


### 3.2.2 Binding group with readers

To assign which readers will be authorized for entry by users of a specific group, select a group and in the edit form click the **Readers** button.



This will open the following dialog:



Here you are able to choose from a list of all available readers the ones that members of this group will be allowed to access.

Access to any assigned reader can further be limited with a calendar. This feature is described in next chapter.

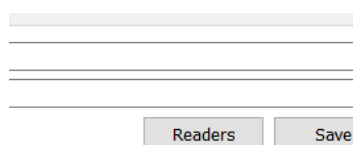
### 3.2.3 Limiting group access according to calendar

In the dialog window for linking Groups with readers (chapter [3.2.2 Binding group with readers](#)) is an option to add access limitation according to a calendar.

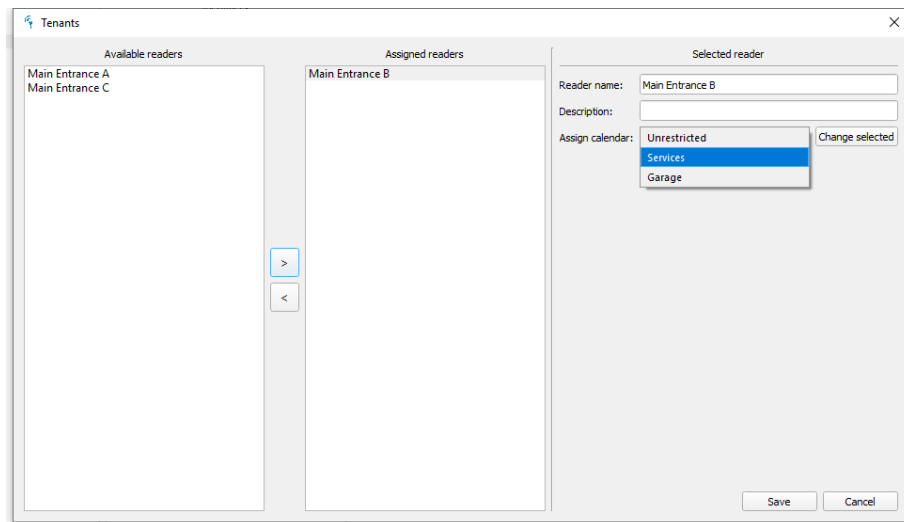
The system logic and bonds between Identifiers, groups, readers and calendars can be found here: [1.2 IMAporter logic and bonds](#). More information about how to prepare a calendar here: [3.3 Calendars tab](#).

As stated above, to add a calendar to the Group-Reader link, it needs to be created first in the **Calendars** tab.

Once a calendar is prepared, navigate to the **Group** tab, select a group for edit and click the **Readers** button.



The following dialog will appear showing the available and linked readers.



By selecting a specific (or multiple by holding down CTRL button) reader/s from the list of assigned readers, you are able to assign a calendar to such reader/s.

The **Unrestricted** calendar in this case means that access to such reader is not limited and users are allowed to enter 24/7.

Selecting any of the predefined calendars limits the access rights to such reader only to time intervals specified under the **Calendars** tab.

### 3.3 Calendars tab

According to the system logic described in chapter [1.2 IMAporter logic and bonds](#) each group can be linked with multiple readers (doors). Identifiers (users) assigned to this group are able to access all the readers that are linked with the group.

Furthermore, the system allows assigning a specific calendar to each linked reader. This means users of a certain group may be for example allowed to enter main door all the time, but garage door only at specific times during the day.

How to link a group with a reader and calendar is described in chapter [3.2.3 Limiting group access according to calendar](#)

This chapter will describe how to edit or prepare new calendars.

Calendar data and limitations:

- A system can have up to 20 weekly calendars (both types together)
- A calendar can have up to 4 intervals per day
- Minimum time for an interval is 1 minute
- Each day of a week can have specific time intervals
- Each reader can have up to 20 holiday days (date) that are treated like Sunday

The system recognizes two types of calendars:

- Standard calendars – limiting user access to specific door
- Permanent unlock calendars – setting specific doors to open-for-everyone mode

We will describe each type of calendar in the following topics.

### 3.3.1 Standard calendars

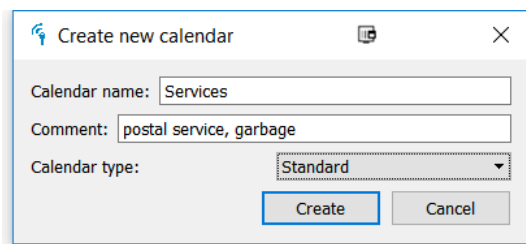
Standard calendars are used for limiting entry to certain areas (readers) to predefined time intervals.

Access is allowed only during the intervals. Between intervals, users are not allowed to enter – the reader blinks red.

#### Adding a calendar

To add a new calendar click the **Create new calendar** button in the **Calendars** tab.

The following dialog will appear:



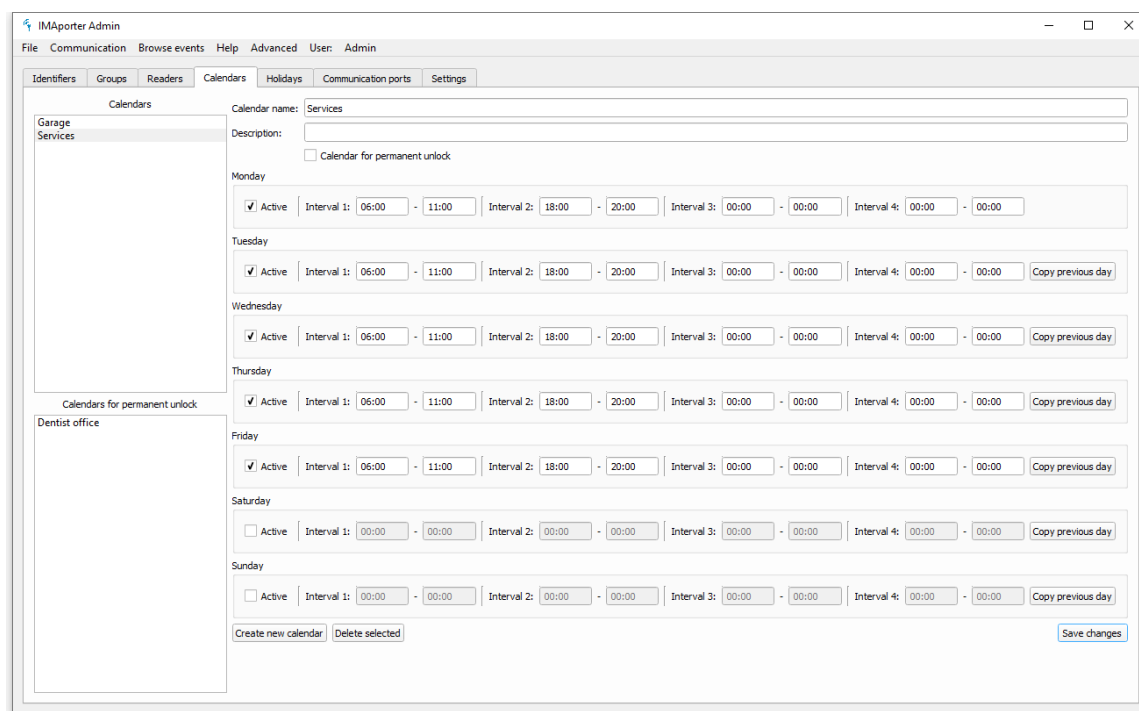
The dialog box titled "Create new calendar" contains the following fields and buttons:

- Calendar name:** Services
- Comment:** postal service, garbage
- Calendar type:** Standard (selected from a dropdown menu)
- Create** button
- Cancel** button

Write down the calendar information and select **Standard** calendar type.

#### Setting time intervals

To set time intervals, select the calendar that you want to edit and fill in the starting and ending time for each interval. If more days use the same intervals, you can use the **Copy previous day** button.



The screenshot shows the "IMApporter Admin" window with the "Calendars" tab selected. The "Services" calendar is chosen from the left sidebar. The main area displays the configuration for this calendar:

- Calendar name:** Services
- Description:** (empty field)
- ☐ Calendar for permanent unlock
- Monday:**
  - ☒ Active
  - Interval 1: 06:00 - 11:00
  - Interval 2: 18:00 - 20:00
  - Interval 3: 00:00 - 00:00
  - Interval 4: 00:00 - 00:00
- Tuesday:**
  - ☒ Active
  - Interval 1: 06:00 - 11:00
  - Interval 2: 18:00 - 20:00
  - Interval 3: 00:00 - 00:00
  - Interval 4: 00:00 - 00:00
  - Copy previous day** button
- Wednesday:**
  - ☒ Active
  - Interval 1: 06:00 - 11:00
  - Interval 2: 18:00 - 20:00
  - Interval 3: 00:00 - 00:00
  - Interval 4: 00:00 - 00:00
  - Copy previous day** button
- Thursday:**
  - ☒ Active
  - Interval 1: 06:00 - 11:00
  - Interval 2: 18:00 - 20:00
  - Interval 3: 00:00 - 00:00
  - Interval 4: 00:00 - 00:00
  - Copy previous day** button
- Friday:**
  - ☒ Active
  - Interval 1: 06:00 - 11:00
  - Interval 2: 18:00 - 20:00
  - Interval 3: 00:00 - 00:00
  - Interval 4: 00:00 - 00:00
  - Copy previous day** button
- Saturday:**
  - ☐ Active
  - Interval 1: 00:00 - 00:00
  - Interval 2: 00:00 - 00:00
  - Interval 3: 00:00 - 00:00
  - Interval 4: 00:00 - 00:00
  - Copy previous day** button
- Sunday:**
  - ☐ Active
  - Interval 1: 00:00 - 00:00
  - Interval 2: 00:00 - 00:00
  - Interval 3: 00:00 - 00:00
  - Interval 4: 00:00 - 00:00
  - Copy previous day** button

At the bottom, there are buttons for "Create new calendar", "Delete selected", and "Save changes".

In the example above, service users (postal services, garbage men etc.) are allowed to enter only in working days in intervals between 6AM - 11AM and 6PM – 8PM.

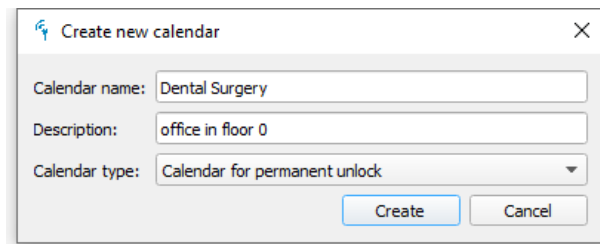
To activate a calendar follow the instructions in chapter [3.2.3 Limiting group access according to calendar](#)

### 3.3.2 Permanent unlock calendars

Permanent unlock calendars are used to “unlock” a specific reader for a given interval. This feature is mainly useful if you need to leave the door open during the day. An example could be businesses in apartment building that need door unlocked for their clients during the working hours. After working hours, the door automatically locks and only users with a valid identifier are allowed to enter.

#### Adding a calendar

To add a new calendar click the **Add new calendar** button in the **Calendars** tab. The following dialog will appear:



The dialog box titled "Create new calendar" contains the following fields:

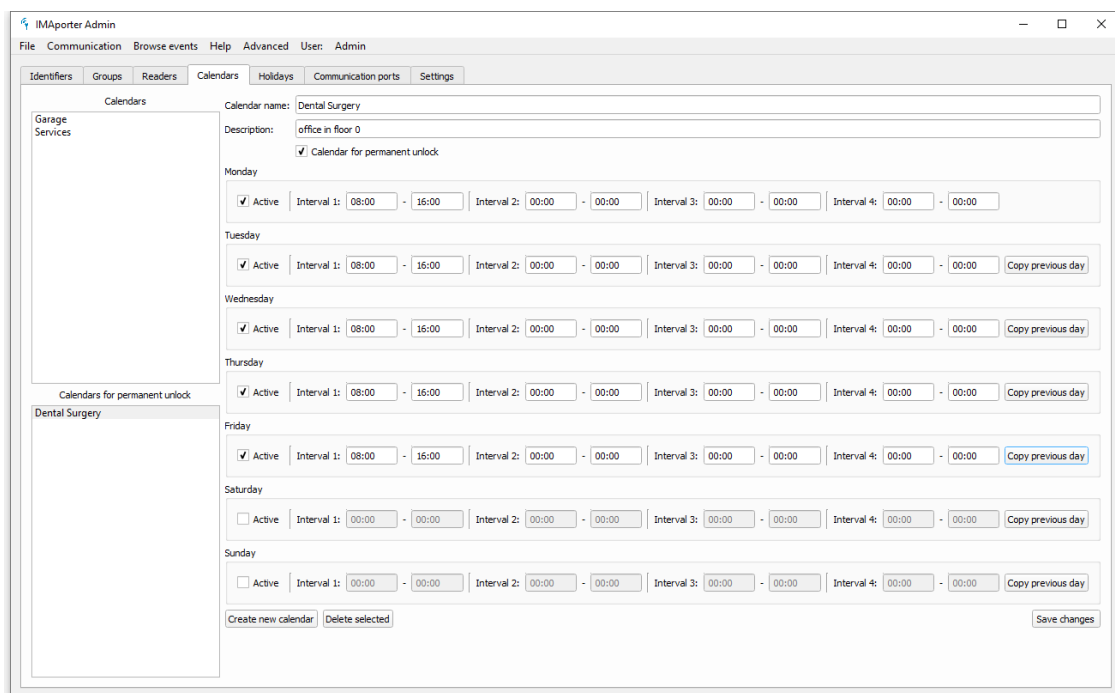
- Calendar name:** Dental Surgery
- Description:** office in floor 0
- Calendar type:** Calendar for permanent unlock (selected from a dropdown menu)

At the bottom right are two buttons: **Create** and **Cancel**.

Write down the calendar information and select **Permanent unlock** calendar type.

#### Setting time intervals

To set time intervals, select the calendar that you want to edit and fill in the starting and ending time for each interval. If more days use the same intervals, you can use the **Copy previous day** button.



The screenshot shows the "IMAporter Admin" window with the "Calendars" tab selected. The "Dental Surgery" calendar is selected in the left sidebar. The main area shows the configuration for this calendar:

- Calendar name:** Dental Surgery
- Description:** office in floor 0
- Calendar type:** ☒ Calendar for permanent unlock

Below are the settings for each day of the week:

- Monday:** ☒ Active. Interval 1: 08:00 - 16:00. Interval 2: 00:00 - 00:00. Interval 3: 00:00 - 00:00. Interval 4: 00:00 - 00:00.
- Tuesday:** ☒ Active. Interval 1: 08:00 - 16:00. Interval 2: 00:00 - 00:00. Interval 3: 00:00 - 00:00. Interval 4: 00:00 - 00:00. **Copy previous day**
- Wednesday:** ☒ Active. Interval 1: 08:00 - 16:00. Interval 2: 00:00 - 00:00. Interval 3: 00:00 - 00:00. Interval 4: 00:00 - 00:00. **Copy previous day**
- Thursday:** ☒ Active. Interval 1: 08:00 - 16:00. Interval 2: 00:00 - 00:00. Interval 3: 00:00 - 00:00. Interval 4: 00:00 - 00:00. **Copy previous day**
- Friday:** ☒ Active. Interval 1: 08:00 - 16:00. Interval 2: 00:00 - 00:00. Interval 3: 00:00 - 00:00. Interval 4: 00:00 - 00:00. **Copy previous day**
- Saturday:** ☐ Active. Interval 1: 00:00 - 00:00. Interval 2: 00:00 - 00:00. Interval 3: 00:00 - 00:00. Interval 4: 00:00 - 00:00. **Copy previous day**
- Sunday:** ☐ Active. Interval 1: 00:00 - 00:00. Interval 2: 00:00 - 00:00. Interval 3: 00:00 - 00:00. Interval 4: 00:00 - 00:00. **Copy previous day**

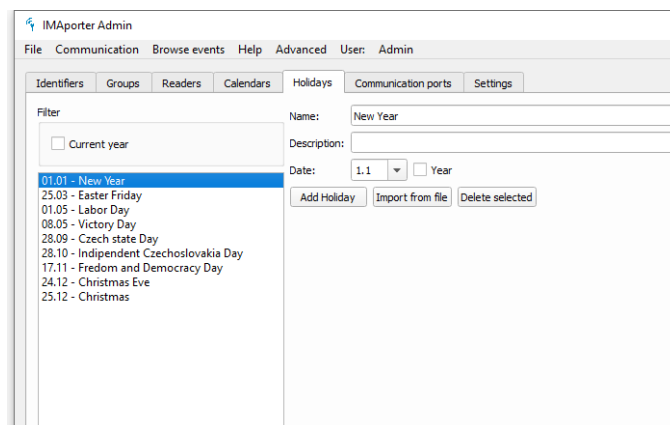
At the bottom, there are buttons: **Create new calendar**, **Delete selected**, and **Save changes**.

In the example above, entry door to an apartment building is left open on working days in intervals between 8AM - 4AM so that visitors can enter the Dental Surgery without any identifier.

To activate a calendar follow the instructions in chapter [4.3.4 Assigning permanent unlock and holidays](#).

## 3.4 Holidays tab

Holidays function is primarily designed for listing Public holidays or other free days. In the IMAPorter system, days marked Holidays are treated according to calendars for Sunday.



### Adding holidays manually

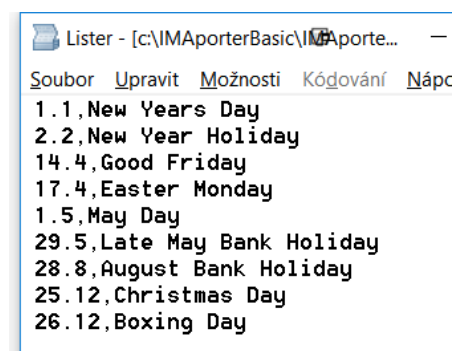
Holiday days can be added using the **Add Holiday** button. By opening the new record for editing, you can specify a day and month.

If a holiday repeats every year on the same date, you can enter only date without entering a year. For holidays (such as Easter) that occur on various dates enter also the year for which the holiday date is valid.

### Importing from a CSV file

Holidays can be also imported from a CSV file of the following structure.

CSV files with holiday dates are to be saved in **%ROOT% \holidays\**. Do make sure that the CSV file is CSV valid. Invalid records are skipped during import. It is best to prepare the file in MS Excel or other spreadsheet SW and export to CSV.



CSV file can be imported in two ways. Either when creating a new database – you will be prompted to choose from available holiday CSV files.

Or by clicking the **Import from file** button under the Holidays tab.

To holidays to a specific reader, follow the instructions in chapter [4.3.4 Assigning permanent unlock and holidays](#).

## 4 Settings and configuration

In this chapter you will find mainly advanced setup and configuration settings. These settings are to be set during installation by system supplier. Unless a change in system or connection configuration occurs, there should not be a need to alter these settings.

### 4.1 Communication ports tab

When setting up a new system, it is necessary to set up the communication ports.

Communication ports are used to connect single reader or group of readers to the management server running IMAporter PC Admin app.

Each server can operate an unlimited number of communication ports in any combination.

The communication options are:

- Serial communication over USB connection
- IP communication over Local Area Network
- IP communication over Mobile Networks or Virtual Private Networks

Communication ports created and listed in this tab are to be assigned to specific readers. The procedure is described in chapters [4.3.2 Reader IDs and communication ports](#) and [5.2.1 Communication test](#).

#### 4.1.1 Adding new USB connection

USB connection is used for connecting readers equipped with serial RS485 communication interface. For connecting the RS485 serial communication to USB port, you need to buy an USB/RS485 converter.

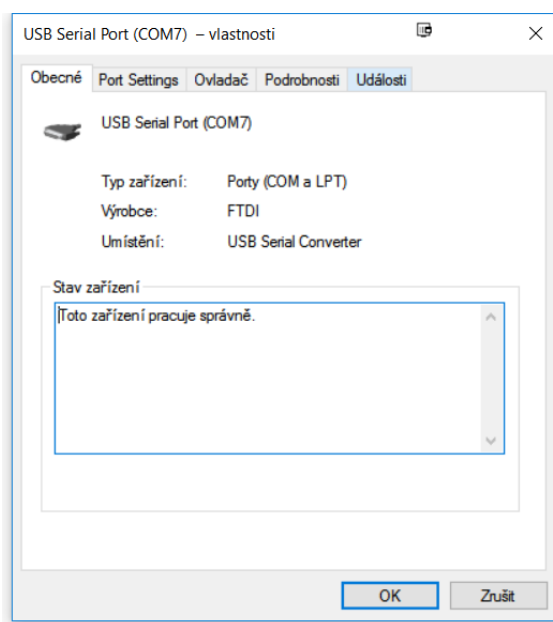
We recommend buying a certified converter from the system supplier to ensure proper function of the system.

##### Technology behind

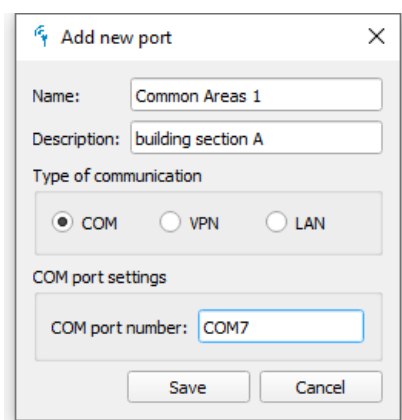
RS485 is a 2 wire serial bus able to connect up to 32 devices (IMApporter Basic sets) with maximum length of the communication wires up to 1,2km. The connection must be done in series and proper line termination must be used. The construction of serial bus is described in the **Installation Manual for IMAporter Mobile and Basic Systems**.

##### Adding a new USB port

Connect the USB converter to your PC and look up the virtual COM port in the system settings: **Control Panel – System – Device Management – USB controllers – right click USB Serial Port – Properties**.



Return to IMAporter PC Admin and type it down to the **Add new port** dialog according to the following image:



You can name each of the ports according to the location / readers that will be connected using this port. In larger systems names are necessary for system clarity mainly during communication with readers.

To assign communication ports to readers and test connection, navigate to [4.3.2 Reader IDs and communication ports](#) and [5.2.1 Communication test](#).

## 4.1.2 Adding new IP connection

IP connection is used for connecting readers or groups of readers over Local Area Network (LAN) or remote readers connected over Internet via Mobile Network or Virtual Private Networks (VPN).

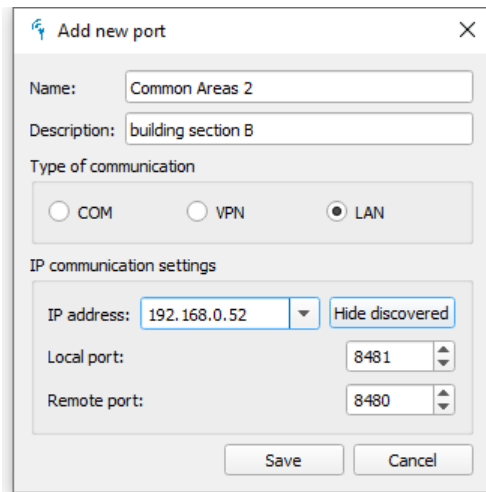
Based on the connection type, different settings are to be used. LAN connected readers use UDP protocol, whereas remote Internet or VPN connected readers use TCP protocol.



One IP port can host up to 32 devices connected together using a RS485 serial line. The connection variants and technical description is described in the **Installation Manual for IMAporter Mobile and Basic Systems**.

## Adding a new IP connection

Click **Add communication port** button to open the following dialog:



The screenshot shows a dialog box titled "Add new port". It contains the following fields and controls:

- Name:** Text box containing "Common Areas 2".
- Description:** Text box containing "building section B".
- Type of communication:** Three radio buttons: COM, VPN, and LAN. The LAN button is selected.
- IP communication settings:**
  - IP address:** A text box containing "192.168.0.52" and a "Hide discovered" button.
  - Local port:** A spin box set to "8481".
  - Remote port:** A spin box set to "8480".
- Buttons:** "Save" and "Cancel" buttons at the bottom right.

### LAN connection:

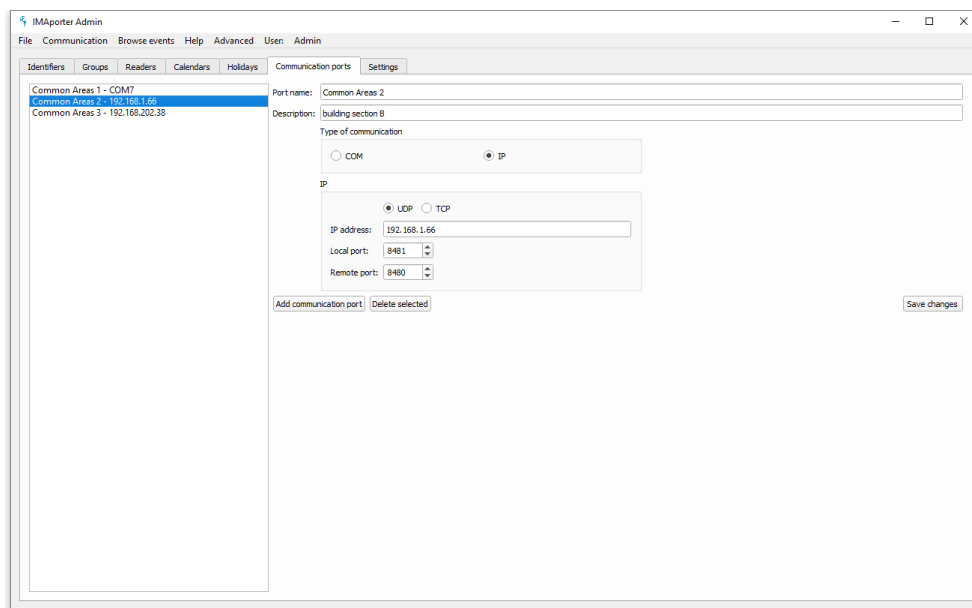
The following settings require a SMR.0x switching module equipped with LAN connection module and correctly configured for the local network. A detailed manual how to configure the LAN module and set Local and Remote ports is available in chapter [8 LAN module configuration](#)

- 1) Enter a name and description of the connection and for a device connected over LAN select **Type of communication: LAN**.
- 2) Enter **IP address** of the remote reader
  - a. Either by directly typing it into the relevant field in case you know the IP address
  - b. Or by clicking the **Discover devices** button and selecting it from the list (the app automatically lists all compatible devices available in the local network).
- 3) Enter the **Local** and **Remote ports** of the connected device  
**KEEP in mind**, that **Local port** on server is **Remote port** on reader and vice-versa and that each communication port on server must have unique **Local port** (or else: each reader must be configured with unique **Remote port**)

### Remote Internet or VPN connection

- 1) Enter a name and description of the connection and for a device connected over Internet or VPN select **Type of communication: VPN**.
- 2) Enter **IP address** and **Remote port** of the reader

Listed communication ports can be edited when needed.

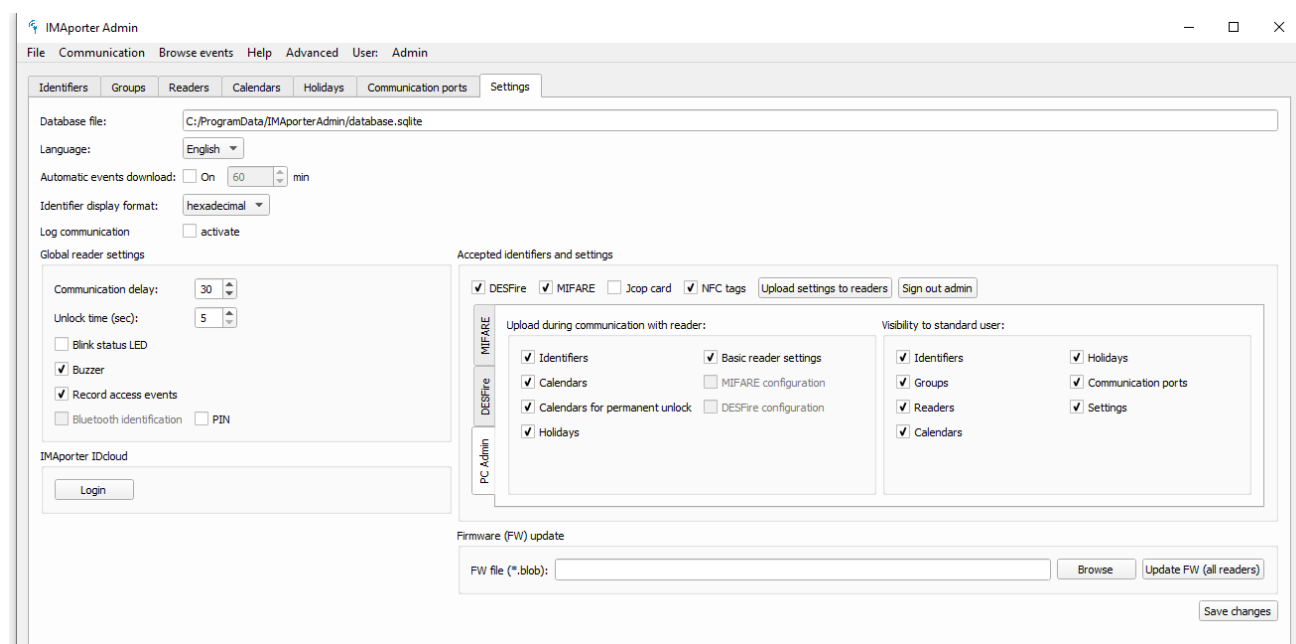


To assign communication ports to readers and test connection, navigate to [4.3.2 Reader IDs and communication ports](#) and [5.2.1 Communication test](#).

## 4.2 Settings tab

The Settings tab groups all necessary system settings including database location and Global reader settings.

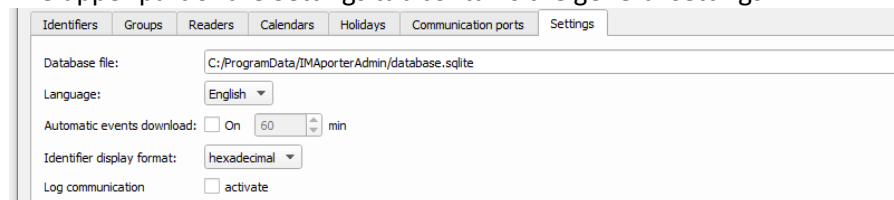
When setting up a new IMAporter system, it is necessary to start here.



The screen above shows the **Settings** tab with **activated Advanced Settings** available after Admin login. How to login as Admin is fully described here: [4.2.5 Admin login and Advanced settings](#)

## 4.2.1 General settings

The upper part of the Settings tab contains the general settings.



### Database file

This field shows the path to the currently open database file. The default location of the database file is in the relevant ProgramData folder. It is possible to operate more databases on one server and switch them from the main app menu **File - Open database**. New database can be created by navigating to **File - New database**.

### Languages

The system is available in English and Czech languages. However adding a new language is possible upon request.

### Automatic download of events

This feature enables to set an interval in minutes for automatic download of events stored in the reader. The capacity for events stored in the reader is limited to 1000 events (or 250 based on FW variant) and they get cyclically overwritten from the oldest. On the other hand capacity for events stored inside the IMAporter PC Admin app is unlimited.

### Identifier display format

The IMAporter PC Admin allows working with IDs displayed DECADIC or HEXADECIMAL format. The setting must correspond with the USB desktop reader and the format in which it outputs data. It is also relevant when importing data from a CSV file, where it must again correspond with the format in which IDs are recorded.

It is possible to change this setting during work with the app.

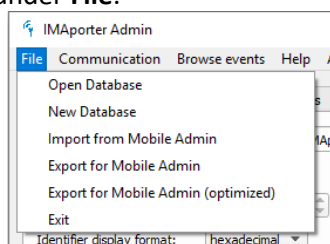
### Communication logging

Logging of communication with readers (all forms of communication) is recommended when setting up and testing a new system. It records all communication and may help to troubleshoot possible installation errors.

When a system is stable and running, it is best to turn logging OFF as it uses a lot of HDD space.

## 4.2.2 Import from / Export for IMAporter Mobile Admin

The app enables to import and export database file from and to Mobile Admin app. These functions are available in the main app menu under **File**.



## Two Admin apps

The two Admin apps are not designed to be used simultaneously. User should decide which Admin app suits him better and then stick to this app.

However transfer of data from one app to another is possible using the below described functions.

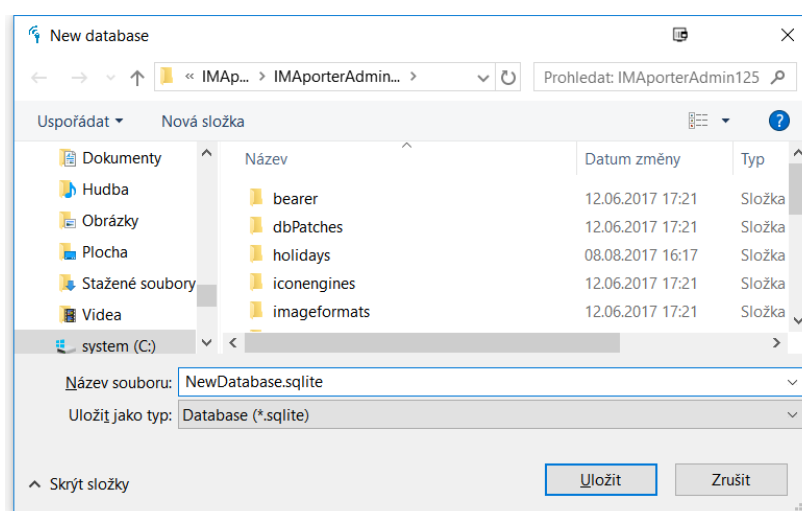
## Different databases

Each Admin app uses a different database format. The PC Admin uses SQLite DB, whereas the Mobile Admin uses JSON DB in .ppj file.

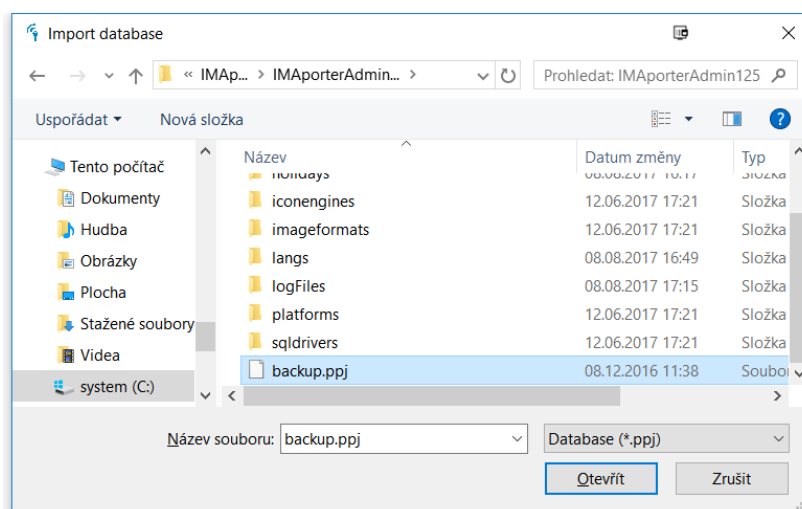
## Importing a PPJ DB

To import a DB from the Mobile Admin, you first need to create a backup PPJ file in the Mobile Admin app and transfer the file to the server running PC Admin app. Please see the [Mobile Admin manual](#) to find out how to create a backup.

Once the [backup.ppj](#) file has been saved to your server, click the **Import from Mobile Admin** item in the **File** menu. Importing to an existing database is not possible, so the system will first prompt you to create a new database file.



After you have created a new database, you will be prompted to navigate to the [backup.ppj](#) file for import.



Once you click Open, a new database will be created.

**Please note** that since the Mobile Admin is used for direct transfer of data between reader and mobile device over NFC, it lacks many advanced settings. The imported database will lack **Communication ports** settings, **assigned ports to readers** and **most settings from the Settings tab**. Only access rights settings are transferred including: Identifiers, Groups, Readers, Calendars and Holidays. No specific reader settings, accepted media or recorded events are transferred during import.

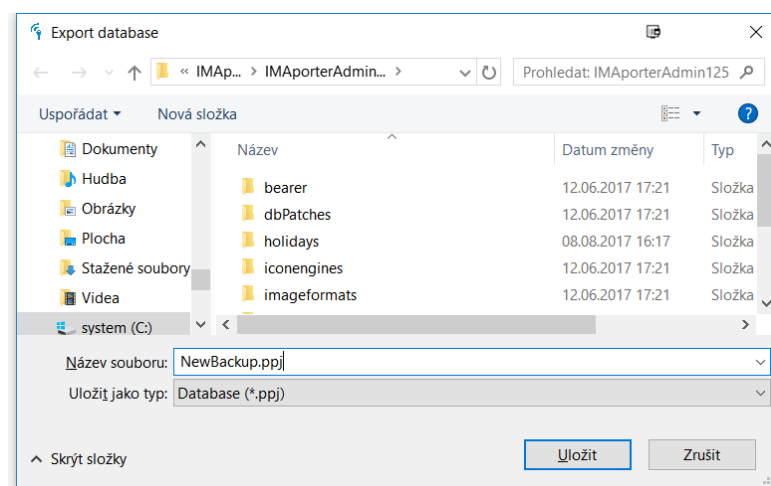
### Exporting to PPJ DB

When exporting database from PC Admin to PPJ file, you have the option to choose between **Export for Mobile Admin** and **Export for Mobile Admin (optimized)** options in the main **File** menu.

The “optimized” option is designed for larger systems running many readers distributed over many ports. Although it is recommended to assign a unique **Reader ID** to every reader (more in chapter [4.3.2 Reader IDs and communication ports](#)), a system running more communication ports also supports duplicate IDs (as long as duplicates are not located on the same communication port). However, Mobile Admin does not support duplicate IDs at all as **Reader ID** is used for distinguishing between readers and **Communication ports** are not present.

It is therefore necessary to select the “optimized” option in case duplicate **Reader IDs** are occurring in the PC Admin database.

After clicking Export button, an export dialog is shown and a .ppj database is saved.



This file needs to be saved to the mobile device in order to load it using the Mobile Admin app. Please see the [Mobile Admin manual](#) to find out how to create a backup.

### 4.2.3 Global reader settings

Global settings are valid for all readers that do not have individual settings defined in the **Readers tab** (more in [4.3.3 Individual reader settings](#)). Once individual settings are set, the readers stops accepting changes in the global settings.

Global reader settings

Communication delay:	30
Unlock time (sec):	5
<input type="checkbox"/> Blink status LED	
<input checked="" type="checkbox"/> Buzzer	
<input checked="" type="checkbox"/> Record access events	
<input type="checkbox"/> Bluetooth identification	<input type="checkbox"/> PIN

### Communication delay

Delay between two following communication attempts in seconds

### Unlock time

Duration for holding a relay switched after accepting a valid identifier

### Blink status LED

Setting for turning off flashing green light when the reader is active. This setting does not influence flashing green or red LED after a valid/invalid identifier has been presented.

### Buzzer

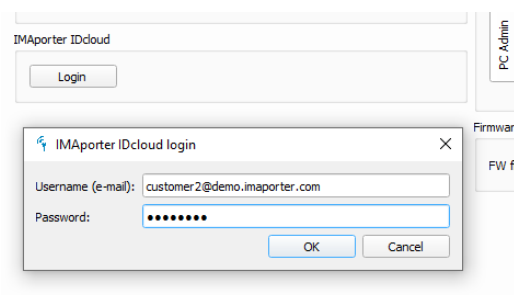
Setting for turning a beeper off. If on, the reader beeps each time an identifier is presented.

### Record access events

For privacy protection purposes the system supports turning off reading of historical access events data. To turn this feature on, the operator should have consent of the users and meet other legal criteria.

## 4.2.4 Login to IMAporter IDcloud

To enable MobileAccess feature and assign of Mobile Keys to users mobile devices directly from IMAporter PC Admin app, it is necessary to create an account in the IMAporter IDcloud and fill in login credentials.



The screenshot shows the IMAporter PC Admin interface with a sidebar containing 'PC Admin', 'Firmware', and 'FW file'. A 'Login' button is visible in the background. In the foreground, an 'IMAporter IDcloud login' dialog box is open. It contains two input fields: 'Username (e-mail):' with the value 'customer2@demo.imaporter.com' and 'Password:' with masked characters. There are 'OK' and 'Cancel' buttons at the bottom right of the dialog.

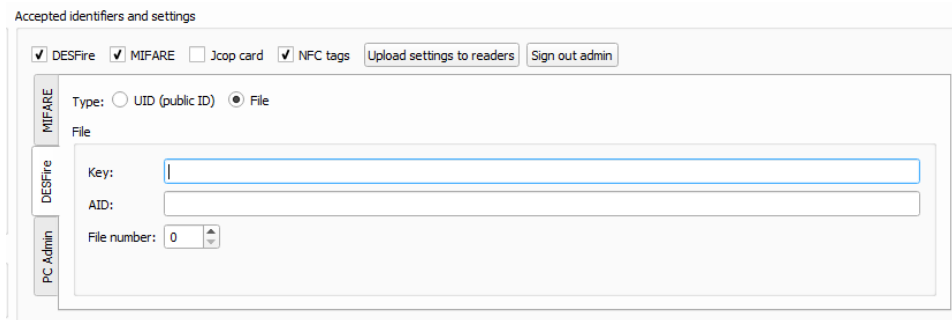
Filling in login credentials will enable adding Mobile Keys directly from the **Identifiers** tab (more here: [3.1.4 Adding Mobile Keys for mobile device](#))

## 4.2.5 Admin login and Advanced settings

For security, maintenance and usage reasons features the app an **Administrator login** enabling advanced settings, identification media settings, system and usage restrictions and advanced reader configuration.

To access the **Advanced settings** navigate to **Advanced** in the main menu and select **Login** - the Admin password is **1003001**.

Upon login, additional tabs will be shown on the Settings tab.



## 4.2.6 Admin: Selecting ID media and Reader configuration

The first option in the Advanced settings is configuration of the accepted media types and security levels.

This setting is not necessary in new systems as accepted media types and security is configured by the system supplier using the IMAporter ACS Config app. The settings inside the PC Admin is to be used as backup in case that reconfiguration of the current state would be necessary.

In the top row you may enable the accepted ID media types such as DESFire, MIFARE Classic and NFC tags – this is recommended setting for most installations.

Based on the intended security of the system you may choose to read either Unique Identifier (UID) that can be potentially cloned or a Sector (for MIFARE) / File (for DESFire) adding more security to the system.

To use Sector/File, this feature must be supported by the physical identification media and you may need to the supplier to provide card login information.

After changes have been made, you may need to upload the settings to the readers to take effect. This can be done by pressing the **Upload settings to readers** button.

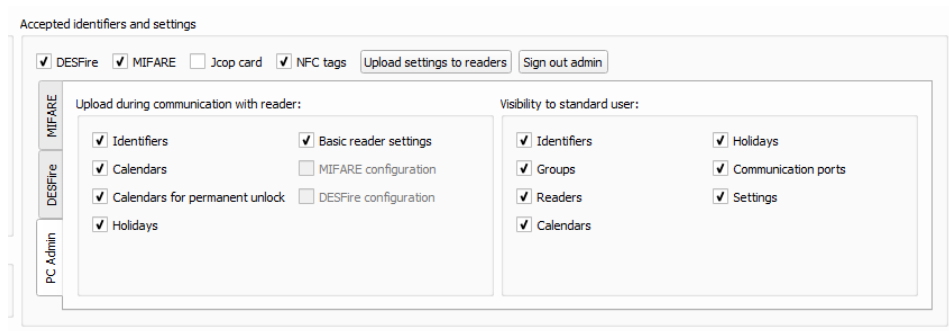
**NOTE: Make sure that you know what you are doing. Reconfiguring a functional system may result in user identifiers not being accepted.**

## 4.2.7 Admin: app functions restriction

It may be necessary to restrict the functions of the PC Admin app for the Standard user.

The app allows restriction in two ways:

- Restricting the data uploaded during communication
- Restricting access to specific tabs



### Restricting the data uploaded during communication

Restricting data uploaded during communication may come handy in cases when some functions are not planned to be used or are not up to date and synchronization is not required. All features to be synced with reader during standard communication are to be ticked on the left side of the above screen.

The only features that cannot be ticked are MIFARE and DESFire configurations as these are uploaded only by the **Upload settings to readers** button.

### Restricting access to specific tabs

For some installation it may be necessary to disable access to specific tabs of the PC Admin app in order to prevent the user from altering the system settings.

This can be done by removing the ticks in the right side of the window. The unticked tabs will remain grey and inaccessible for the Standard user.

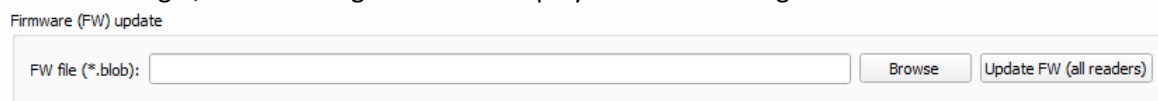
**NOTE: Be aware that all restrictions are active only for the Standard user. When the Admin is logged in, all functions are visible and available.**

## 4.2.8 FW update

**FW update is expert feature and should be carried out only in necessary occasions. Mishandling FW update may result in system malfunctions and void warranty.**

To enable FW update, it is required to login as Admin as described in chapter: [4.2.5 Admin login and Advanced settings](#)

After Admin login, the following function is displayed on the Settings tab.



In the next step a .blob file needs to be acquired from system supplier or manufacturer and path saved to **FW file** field in the **Settings**.



## Checking FW version

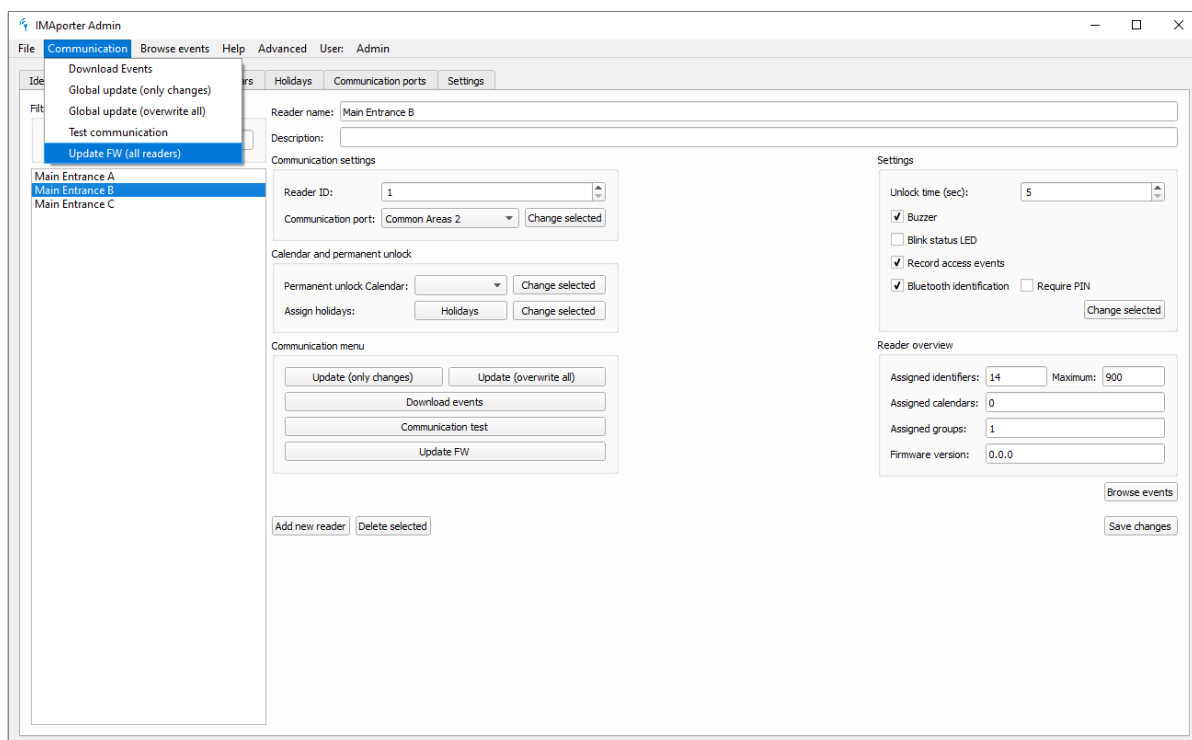
Prior to updating FW, it is recommended to check the FW version in readers. This information is shown on **Readers tab** in **Reader overview** section.

Reader overview

Assigned identifiers:	14	Maximum:	900
Assigned calendars:	0		
Assigned groups:	1		
Firmware version:	0.0.0		

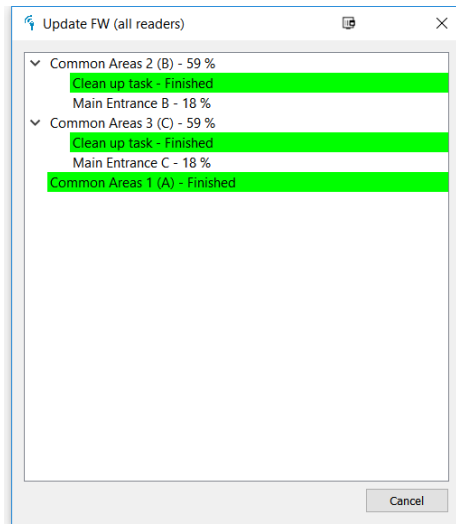
## FW update - global

To update FW in all readers, navigate to the communication menu and click **Update FW (all readers)**. Prior to running the **Update FW** function, it is recommended to carry on **Download Events** and **Global update (overwrite all)** to make the readers up-to-date.



The screenshot shows the IMAporter Admin application window. The 'Communication' menu is open, and 'Update FW (all readers)' is selected. The interface includes a sidebar with a tree view showing 'Main Entrance A', 'Main Entrance B', and 'Main Entrance C'. The main area displays settings for 'Main Entrance B', including 'Reader ID: 1', 'Communication port: Common Areas 2', and 'Settings' for 'Unlock time (sec): 5', 'Buzzer', 'Blink status LED', 'Record access events', 'Bluetooth identification', and 'Require PIN'. A 'Reader overview' section at the bottom right shows 'Assigned identifiers: 14', 'Maximum: 900', 'Assigned calendars: 0', 'Assigned groups: 1', and 'Firmware version: 0.0.0'. Buttons for 'Add new reader', 'Delete selected', 'Browse events', and 'Save changes' are visible.

An update dialog will open showing the progress of FW update.

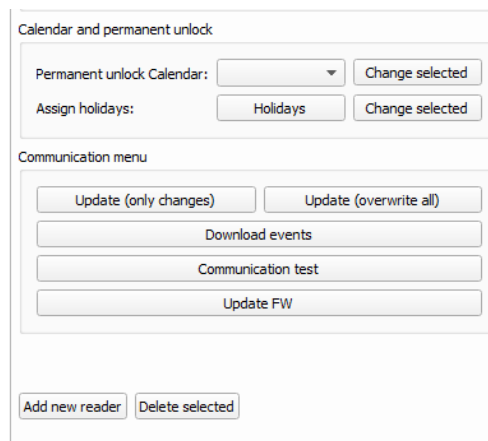


Please note that FW update takes a longer time during which the readers do not operate. FW update is signaled by lighting red LED on the reader. After update, the reader restarts and shortly blinks green and red LED. Then returns to normal operation mode.

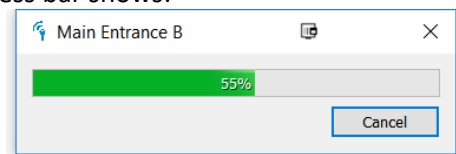
In case that any reader on the communication line fails to update, all following readers are skipped (marked red) to prevent further damage. To continue updating FW on such communication line, the failed reader must be re-uploaded (repeating FW update) or physically disconnected from the communication line.

### FW update – individual reader

It is also possible to update FW only in selected readers. This operation can be launched by clicking the **Update FW** button on the **Readers** tab. Please note that this option is only visible under Admin login.



Single reader FW update progress bar shows:

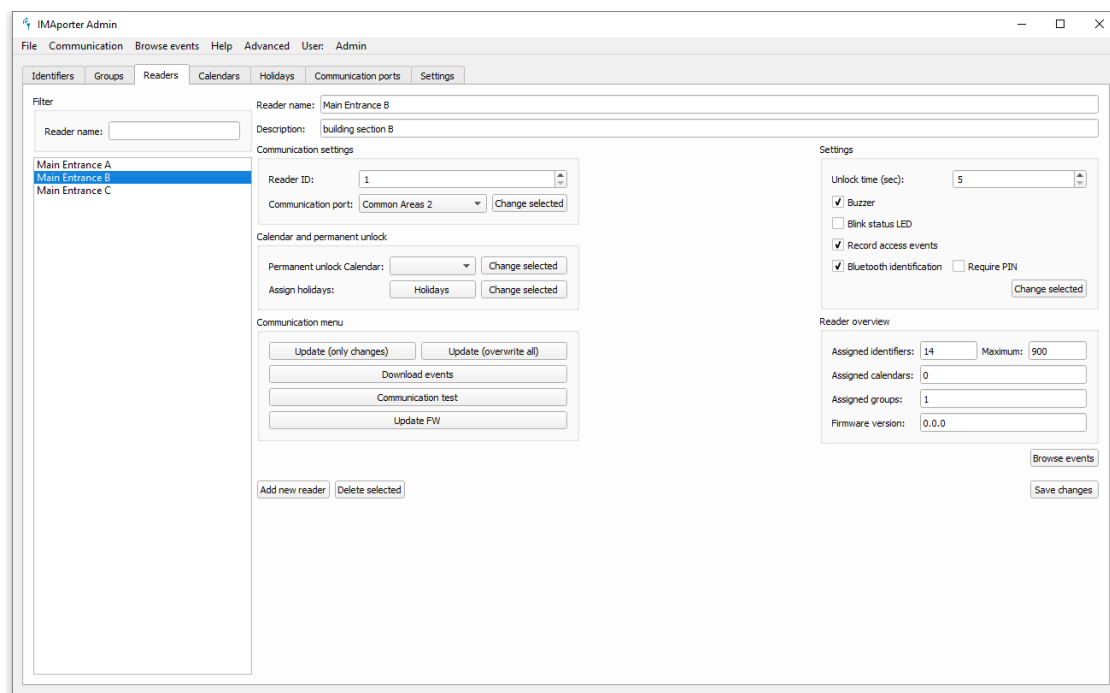


Please note that when running an individual reader FW update, all other readers on the same communication line must be either disconnected or in full operation mode. In case there would be another reader with failed FW update online, update will fail resulting in locking the reader from operation.

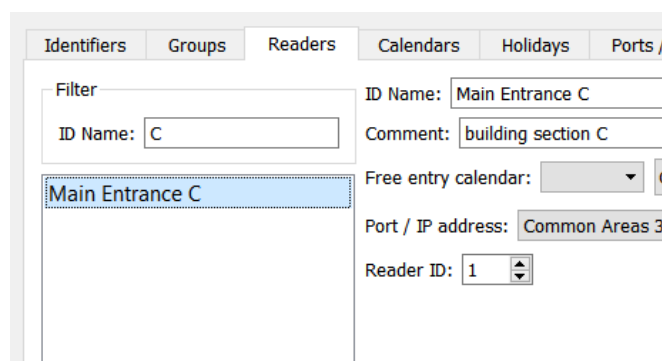
## 4.3 Readers tab

The **Readers** tab lists all readers available in the system, their memory and storage capacities, FW version, allows editing reader specific settings.

The **Reader tab** also provides communication operations (data download/upload) for a single reader.

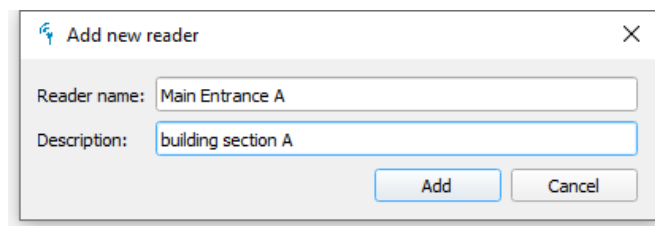


Filtering readers can be done by entering text into the **Filter** fields. Filter is always applied from the beginning of a word. In case of multiple words in the Reader name, all are taken into account.



### 4.3.1 Adding new reader

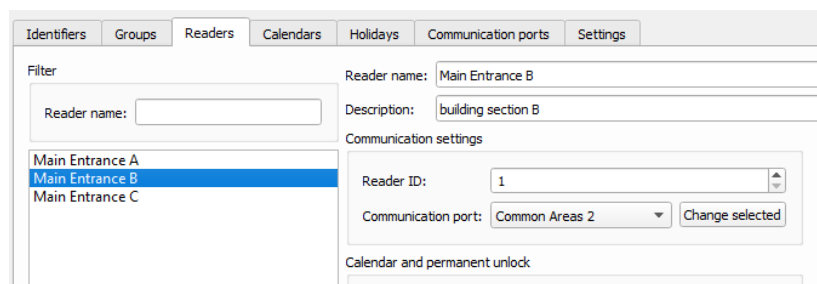
To add a new reader click the **Add new reader** button on the **Readers** tab. The following dialog will appear:



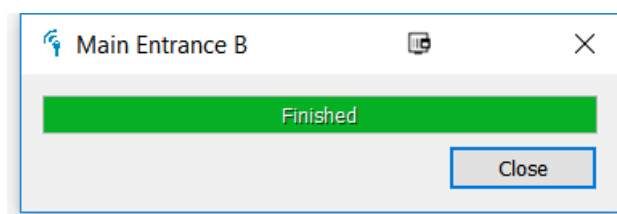
Enter the name and comment and click the **Add** button and continue to [4.3.2 Reader IDs and communication ports](#).

### 4.3.2 Reader IDs and communication ports

To configure a newly added reader, you should select the **Communication port** to which the reader is connected (communication ports are described here: [4.1 Communication ports tab](#)) and type in the **Reader ID** that was configured to the reader during installation (initial reader configuration is described in the [IMAporter ACS Config app Manual](#))



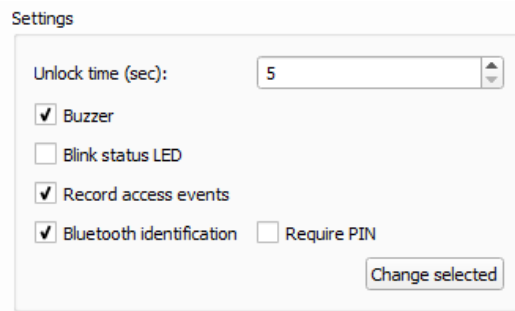
Once the reader is configured, click the **Communication test** button to test out it has been configured correctly. A dialog like this should appear:



If in any case you receive a RED message with error code, you should check if everything has been configured correctly (more about error codes in [Chyba! Nenalezen zdroj odkazů. Chyba! Nenalezen zdroj odkazů.](#)).

### 4.3.3 Individual reader settings

Reader settings can be assigned globally from the **Settings tab** (more to be found here: [4.2.3 Global reader settings](#)) or locally in the **Reader tab** as shown on the image below.



Changing reader settings individually on the **Reader tab** overrides **Global reader settings**. Any future change of the **Global settings** will not affect the reader that has been individually set.

Description and meaning of individual settings items can be found here: [4.2.3 Global reader settings](#)

### Bluetooth identification

It is the only item that cannot be set globally due to compatibility issues. All readers that are to enable the MobileAccess function using Bluetooth are to have this feature enabled locally.

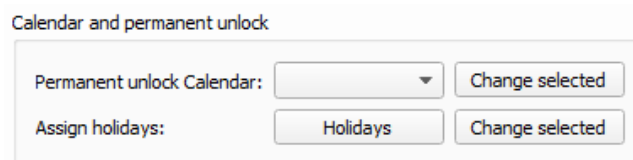
MobileAccess over NFC is enabled automatically in all IMAporter Basic readers.

## 4.3.4 Assigning permanent unlock and holidays

### Permanent unlock calendar

Each reader can be assigned a Permanent unlock calendar specifying time intervals during which the door is to remain open.

Permanent unlock calendars need to be created in advance in the Calendars tab. More to be found here: [3.3.2 Permanent unlock calendars](#).

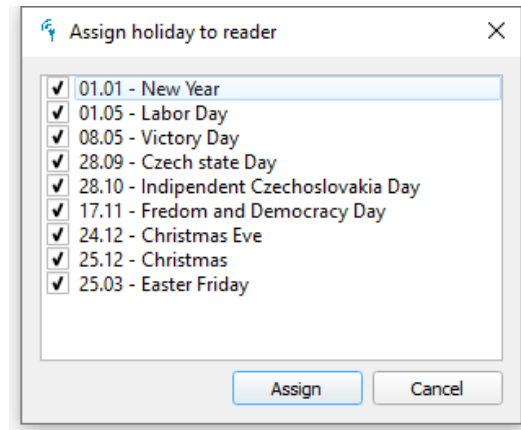


### Holidays

For purposes of using calendars to limit user access rights to predefined time intervals (described here: [3.3.1 Standard calendars](#) and here: [3.2.3 Limiting group access according to calendar](#)) it may be necessary to define dates of public holidays.

How to create a list of public holidays (days treated like Sunday) is described here: [3.4 Holidays tab](#).

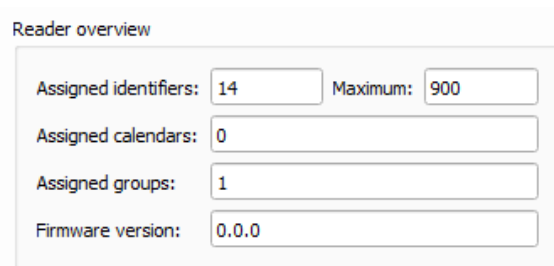
When created it is possible to choose which of these days will be taken into account by the specific reader. This holiday pairing dialog is available in the **Readers tab** under the **Holidays** button.



In this dialog window, select which public holiday days should be taken into account by the specific reader.

### 4.3.5 Reader overview

Reader overview on the Readers tab is an information bar to display current capacity of reader's memory and overall status of the reader including FW version.



The FW version and maximum memory capacity fields are updated during communication with the reader. To update the fields, click **Upload changes** or **Upload everything** buttons

## 5 Communication

The IMAPorter PC Admin offers two communication or programming options. Readers can be updated globally from the **Communication menu** or locally one-by-one from the **Readers tab**.

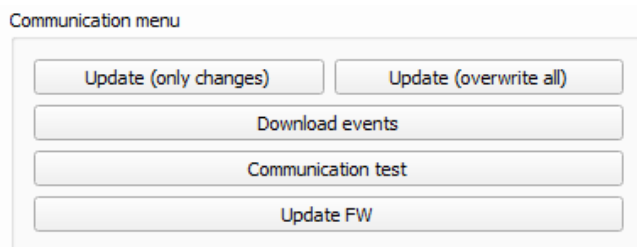
Each type of communication has its benefits according to the situation.

List of communication options (both single reader and global):

- **Download Events**  
Downloads all events recorded by the reader under the assumption that events recording is allowed in reader settings. Once events are downloaded, they are deleted from the reader memory.
- **Update (only changes)**  
Uploads all changes including updates of user access rights, new identifiers, erased identifiers etc. Only readers influenced by the change are updated.
- **Update (overwrite all)**  
Uploads all changes including updates of user access rights, new identifiers, erased identifiers etc. Upload is propagated to all readers independently on whether they are influenced by the changes or not.
- **Test communication**  
Easy and fast ping to all readers ideal for testing the communication line
- **Update FW**  
Function for uploading new FW file, this function is fully described here: [4.2.8 FW update](#) (this option is available only under Admin login)

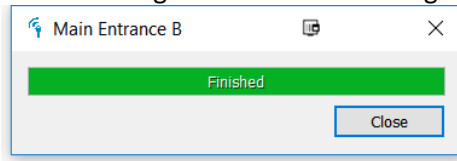
### 5.1 Operations above a single reader

For purposes of testing communication or uploading changes / downloading events from just one specific reader, it may be handy to navigate to the **Readers tab**, select the reader and choose one of the buttons below:

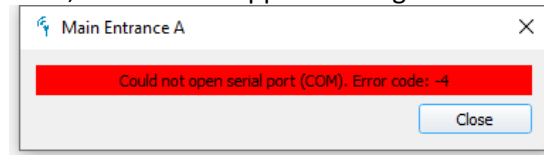


Functions of specific buttons are described here: [5 Communication](#).

After a successful communication with a single reader the following window should appear:



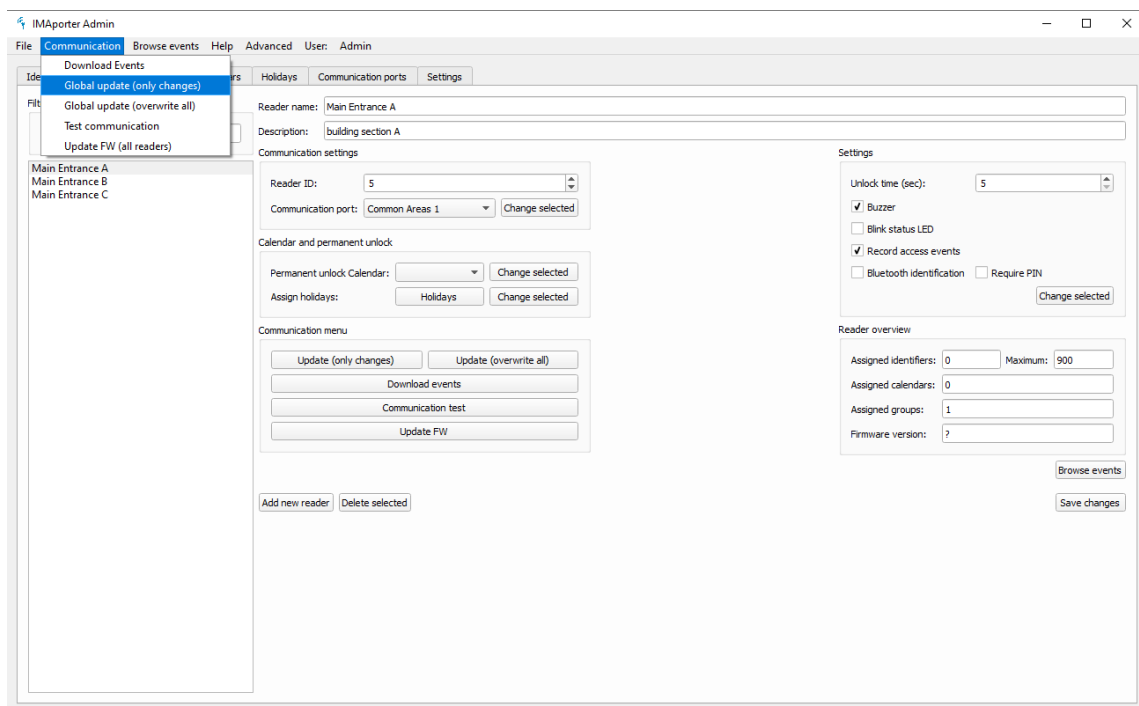
In case of communication failure, this window appears listing the failure reason:



## 5.2 Operations above multiple readers

For communication with all readers at once, navigate to the **Communication menu** and select the corresponding communication option.

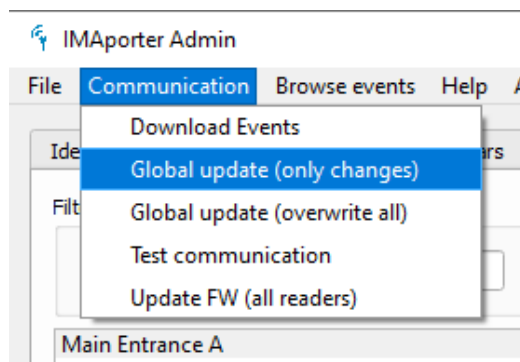
All communication options are described here: [5 Communication](#).



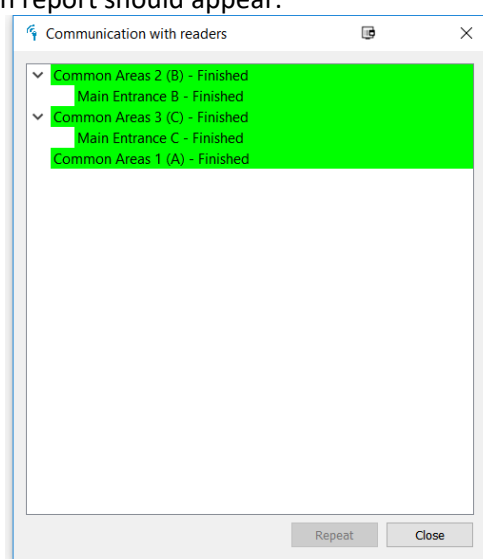
### 5.2.1 Communication test

Easy and fast ping to all readers ideal for testing the communication line and diagnose possible errors.

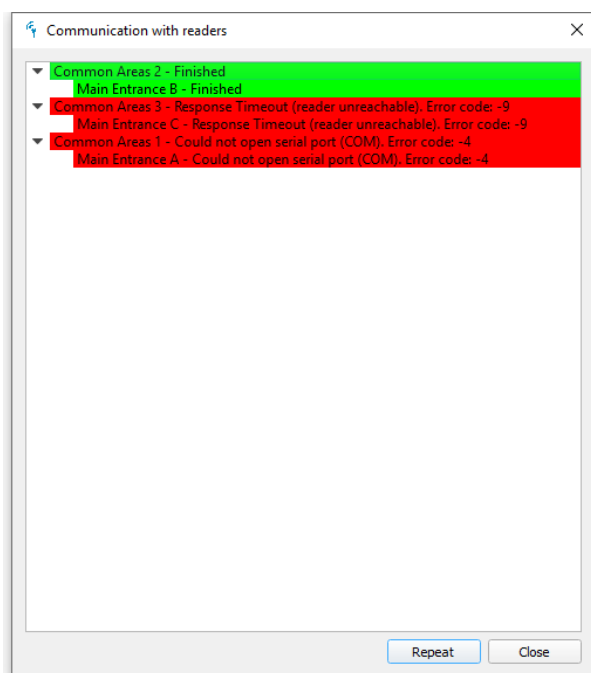




If everything is correct, a green report should appear:



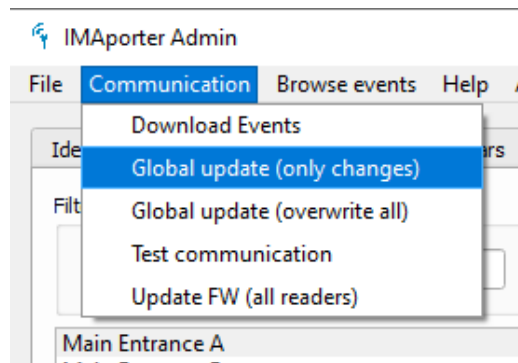
In case of a failure, a red report will appear with error description and code, recommendation of repair methods can be found in chapter: [Chyba! Nenalezen zdroj odkazů. Chyba! Nenalezen zdroj odkazů.](#)



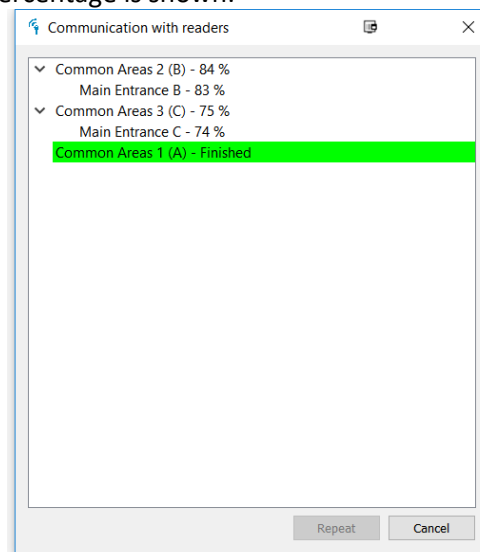
### 5.2.2 Data upload

Changes to access rights made by the system admin can be propagated to the system in two different ways:

- **Upload only changes**  
uploads changes only to readers whose data was changed
- **Upload – overwrite everything**  
updates all readers in the system regardless of changes

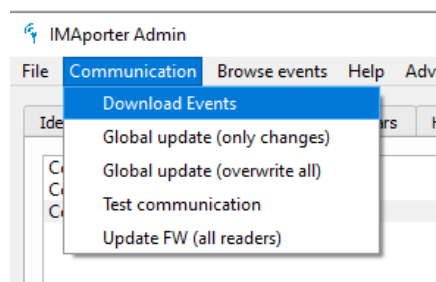


During data upload a status percentage is shown:

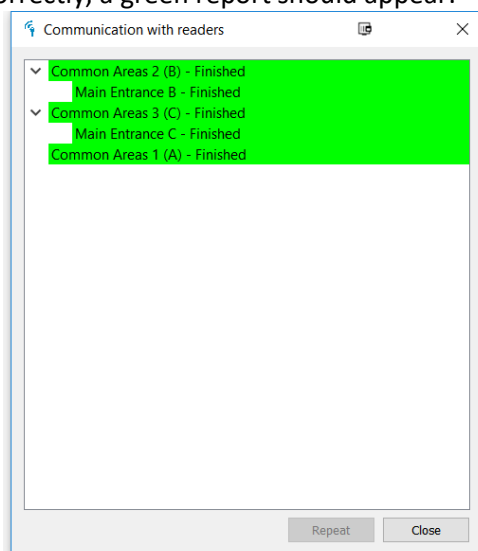


### 5.2.3 Events download

Downloads all events recorded by the reader under the assumption that events recording is allowed in reader settings. Once events are downloaded, they are deleted from the reader memory:



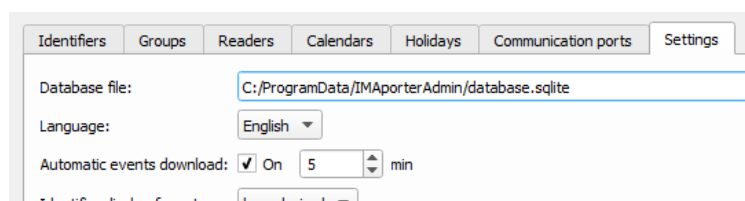
If everything is downloaded correctly, a green report should appear:



Downloaded events can be filtered and analyzed using the statistical and viewing function. More about Events processing can be found here: [6 Browsing Events history and statistics](#)

## 5.2.4 Automatic events downloading

If the server and PC Admin app are left running, it is then also possible to use the **Automatic events download** function.



This function is available on the **Settings tab** and performs only Global events download (from all connected readers).

The automatic download interval can be specified in minutes starting from a period of 1 minute up to 10400 minutes (1 week)

## **6 Browsing Events history and statistics**

### **6.1 Browsing events**

### **6.2 Statistics**

### **6.3 Exporting events**

## 7 Connecting 3<sup>rd</sup> party SW

The IMAPorter PC Admin software not only enables complex management of the Access Control System, but also allows management from 3<sup>rd</sup> party apps and systems.

These functions are handy for applications such as reservation systems, building management and similar. Such systems can be enabled direct access to the SQLite DB together with remotely triggered communication commands to upload changes.

### 7.1 Direct DB access

This is a simple example of table structure of the IMAPorter PC Admin file database.

In this example we suggest that all identifiers, settings and other data are managed by the PC Admin and the third party app is used only for assigning and removing assignments of an Identifier to specific Groups of access rights.

```

/*
Navicat SQLite Data Transfer

Source Server        : CleanGolem
Source Server Version : 30706
Source Host          : :0

Target Server Type    : SQLite
Target Server Version : 30706
File Encoding         : 65001

Date: 2019-02-26 17:07:51
*/

PRAGMA foreign_keys = OFF;

--
-- Table structure for "main"."cards"
--
DROP TABLE "main"."cards";
CREATE TABLE "cards" (
  "_id" INTEGER PRIMARY KEY AUTOINCREMENT NOT NULL,
  "number" TEXT NOT NULL,
  "name" TEXT NOT NULL,
  "comment" comment
, webCreated TEXT DEFAULT "", webExpires TEXT DEFAULT "", webStatus INTEGER DEFAULT 0, webId
INTEGER DEFAULT 0);

--
-- Records of cards
--

--
-- Table structure for "main"."cardsgroups"
--
DROP TABLE "main"."cardsgroups";
CREATE TABLE "cardsgroups" (
  "_id" INTEGER PRIMARY KEY AUTOINCREMENT NOT NULL,
  "cardId" INTEGER NOT NULL,
  "groupId" INTEGER NOT NULL,
  CONSTRAINT "FK_cardgroups_cards" FOREIGN KEY ("cardId") REFERENCES "cards" ("_id") ON DELETE
CASCADE ON UPDATE CASCADE,
  CONSTRAINT "FK_cardgroups_group" FOREIGN KEY ("groupId") REFERENCES "groups" ("_id") ON DELETE
CASCADE ON UPDATE CASCADE
);

```

```
-- Records of cardsgroups
-- -----

-- -----
-- Indexes structure for table cards
-- -----
CREATE UNIQUE INDEX "main"."cardsIdIndex"
ON "cards" ("_id" COLLATE BINARY ASC);
```

There are also other and more complex options how to access and edit the SQLite DB, but these are subject to individual consultations.

## 7.2 Remotely triggered communication

It may be necessary to trigger upload of access rights or download of events from a remote or third-party app.

Such feature is often used by third-party systems used for managing access rights (e.g. reservation systems etc.). These systems access directly the PC Admin DB and after making changes use the PC Admin only for communication with the readers.

The communication is triggered by calling the PC admin .exe file with a specific parameter I the following way (please mind that you need to call it from the app installation directory or keep the complete target address):

**IMAporterAdmin.exe [option]**

**C:\Program Files (x86)\IMA\IMAporterAdmin\IMAporterAdmin.exe [option]**

The options are following:

help	shows help
console	runs app together with console showing log of all communication – this parameter can be combined with other parameters
clearSettings	erases all registry entries of the IMAporter PC Admin and opens the app as new installation
receive	starts app directly into Download events dialog and after finishing the download, it automatically closes
transmit	starts app directly into Upload changes dialog and after finishing the upload, it automatically closes

## 8 LAN module configuration

All our Ethernet modules are set to obtain IP address from DHCP server. It is therefore essential to find out what IP address it has received.

This can be done in three ways:

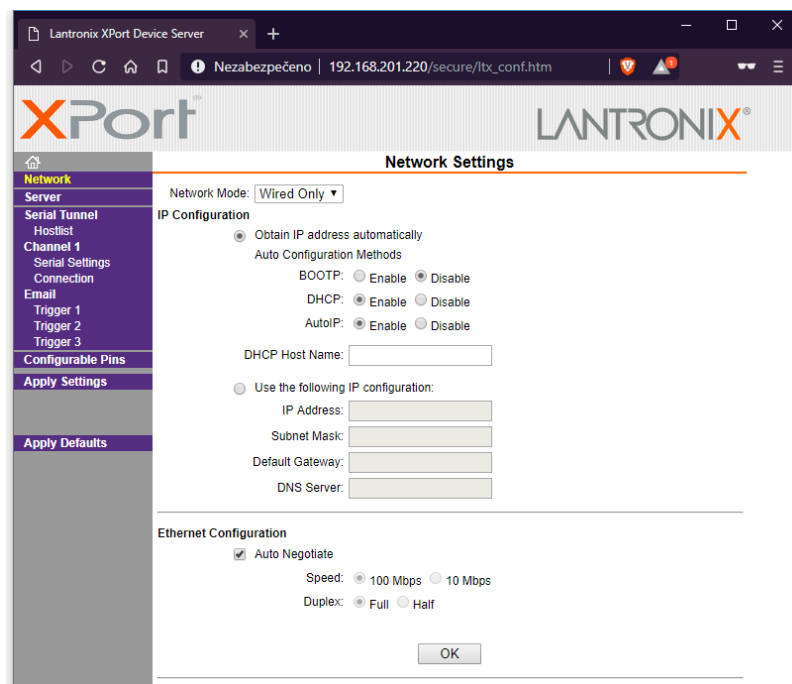
- By checking DHCP server connected clients table (to be found in router settings)
- By discovering devices using the PC Admin (described in chapter: [4.1.2 Adding new IP connection](#))
- By downloading LANTRONIX DeviceInstaller from [here](#) + [manual](#)

If you know the IP address of the LAN module, you can use a standard internet browser to view the settings as can be seen on screenshot below.

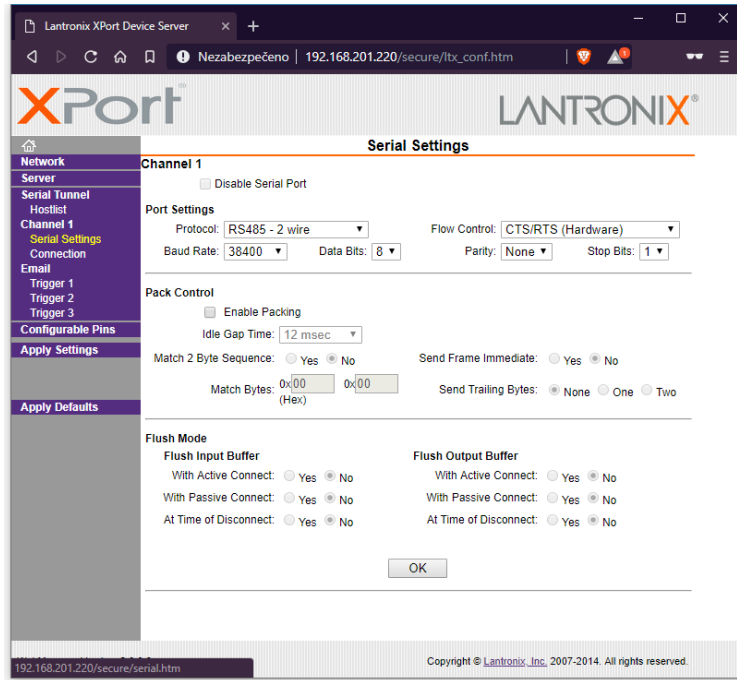
The login credentials are as follows:

- Option 1: leave both username and password blank
- Option 2: leave username blank and as password type in \*\*\*\* (4 stars)

On the following screenshots, you will find the standard module settings for IMAPorter Basic ACS. We are listing only screens with crucial settings. Screens that are not listed in this manual have no effect on the systems function.



Network settings – set to obtain IP from DHCP server



**Serial Settings**

Channel 1

☐ Disable Serial Port

**Port Settings**

Protocol: RS485 - 2 wire Flow Control: CTS/RTS (Hardware)

Baud Rate: 38400 Data Bits: 8 Parity: None Stop Bits: 1

**Pack Control**

☐ Enable Packing

Idle Gap Time: 12 msec

Match 2 Byte Sequence: ☐ Yes ☒ No Send Frame Immediate: ☐ Yes ☒ No

Match Bytes: 0x00 0x00 (Hex) Send Trailing Bytes: ☒ None ☐ One ☐ Two

**Flush Mode**

**Flush Input Buffer**

With Active Connect: ☐ Yes ☒ No

With Passive Connect: ☐ Yes ☒ No

At Time of Disconnect: ☐ Yes ☒ No

**Flush Output Buffer**

With Active Connect: ☐ Yes ☒ No

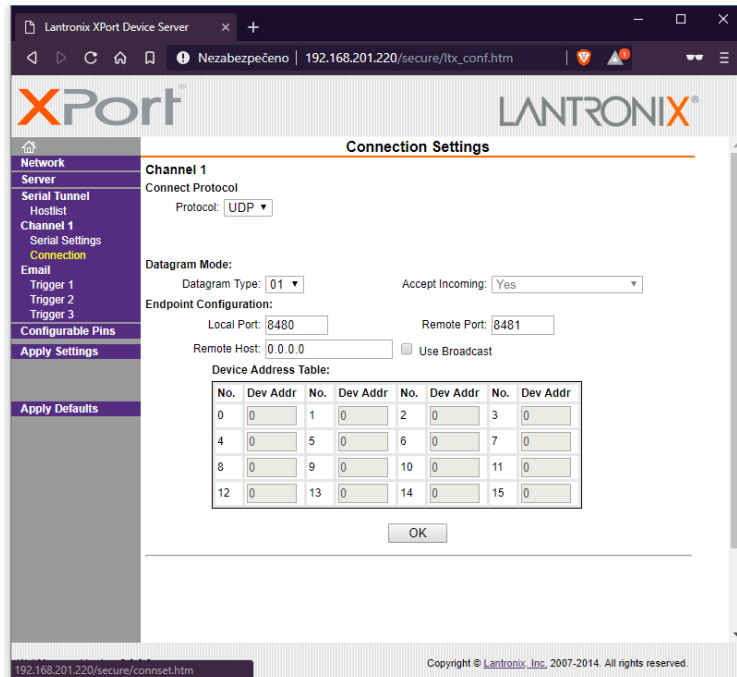
With Passive Connect: ☐ Yes ☒ No

At Time of Disconnect: ☐ Yes ☒ No

OK

Copyright © Lantronix, Inc. 2007-2014. All rights reserved.

Serial settings - make sure to use RS485 2wire and 38400 baud



**Connection Settings**

Channel 1

Connect Protocol

Protocol: UDP

**Datagram Mode:**

Datagram Type: 01 Accept Incoming: Yes

**Endpoint Configuration:**

Local Port: 8480 Remote Port: 8481

Remote Host: 0.0.0.0 ☐ Use Broadcast

**Device Address Table:**

No.	Dev Addr	No.	Dev Addr	No.	Dev Addr	No.	Dev Addr
0	0	1	0	2	0	3	0
4	0	5	0	6	0	7	0
8	0	9	0	10	0	11	0
12	0	13	0	14	0	15	0

OK

Copyright © Lantronix, Inc. 2007-2014. All rights reserved.

Connection Settings - protocol must be UDP and correct and unique Ports filled in