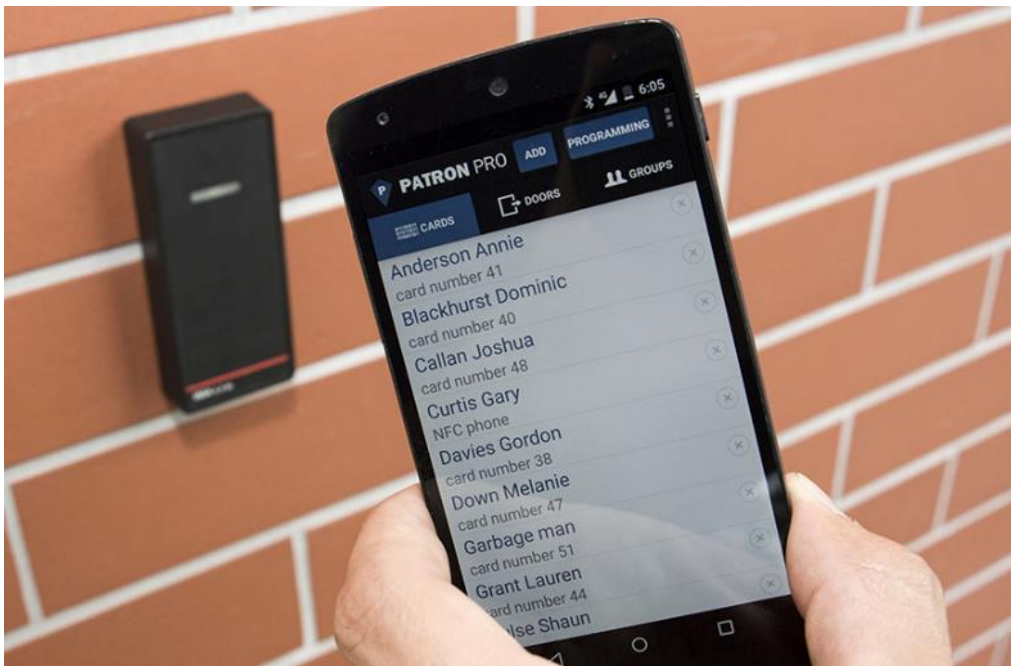


IMAporter Mobile Admin

Mobile Admin app for IMAporter Mobile and
IMAporter Basic Access Control Systems



User manual

DOCUMENT HISTORY

Revision	Date	Author	Description
v0.1	7. 8. 2015	Karel Kalivoda	First draft of document
v1.0	27. 10. 2015	Karel Kalivoda	First version
v1.1	14. 9. 2017	Karel Kalivoda	IDcloud update (Mobile Keys)
v1.2	9. 8. 2018	Karel Kalivoda	Added easy start-up guide

TABLE OF CONTENTS

1.	IMApporter Mobile Admin	4
1.1	Introduction to IMAporter ACS	4
1.2	Mobile Admin tabs and their purpose	5
1.2.1	Identifiers	5
1.2.2	Phones	5
1.2.3	Readers	5
1.2.4	Groups	5
1.2.5	Calendars	5
1.2.6	Free Entry	6
1.2.7	Holidays	6
1.3	Logical bonds and relations	6
1.4	Example database and system setup	7
2	Getting started – Easy start-up guide	9
2.1	First launch and settings	9
2.1.1	Fill in the Admin password	9
2.1.2	Load the settings	9
2.1.3	Enter the IMAporter IDcloud login (necessary to use MobileAccess)	9
2.1.4	Optionally load a DEMO database (backup file)	9
2.2	Create a Group	9
2.3	Add a Reader	10
2.4	Add an Identifier	10
2.5	Add a Mobile Key	10
2.6	Update the system	10
2.7	Test the system	10
2.8	Test the MobileAccess function	11
3	Mobile Admin manual	12

3.1	First launch	12
3.1.1	Entering Admin password	12
3.1.2	Loading system settings	12
3.2	System settings.....	13
3.3	Backup and restore function	13
3.4	Access logs backup	14
3.5	Identifiers tab	15
3.5.1	Adding a new card and editing current one	15
3.5.2	Identifier edit form	16
3.5.3	Deleting identifiers	16
3.6	Phones tab (MobileAccess function).....	17
3.6.1	Logging into IMAporter ID Management	18
3.6.2	Adding (editing) a new Mobile Key (Phone).....	19
3.6.3	Adding a new Mobile Key manually (optional)	20
3.7	Readers tab.....	21
3.7.1	Adding new readers and editing existing ones	21
3.7.2	Reader edit form	23
3.8	Groups tab	25
3.8.1	Adding a new Group.....	25
3.8.2	Group edit form.....	25
3.9	Calendars	27
3.9.1	Edit form and time zones	28
3.10	Free entry	29
3.11	Holidays	29
3.11.1	Adding and removing holidays	29
3.11.2	Edit form	29
3.12	Uploading changes (synchronizing access rights)	30

1. IMAporter Mobile Admin

1.1 Introduction to IMAporter ACS

The **IMAporter Mobile Admin app** is designed for site admins as a management tool to control and assign user access rights to individual doors. This app can be used with **IMAporter Mobile** as well as **IMAporter Basic systems**.

It is available only for Android mobile devices equipped with NFC technology.

The IMAporter Mobile Admin app can be purchased from here: <http://www.ima.cz/app/imapadmin>



Using the IMAporter Mobile Admin app, site admins can add new cards or tags to the system, create and assign user groups featuring specific access rights, create and assign calendars and access limitations, permanent unlock schedules and more.

Given both IMAporter Mobile and Basic systems are offline with distributed database, changes in access rights done using IMAporter Mobile Admin must be propagated separately to each reader in the system. Update of access rights is done by holding the Android NFC-enabled device on top of a reader for about 2-40sec depending on the size of transferred data.

The IMAporter Mobile Admin app is also fully **compatible with MobileAccess** ecosystem enabling the admin to easily create user Mobile Keys and propagate them automatically to the user's mobile devices.

Users with a Mobile Key assigned to their mobile device (Android/iOS) can use this device for identification and door opening using NFC and Bluetooth technologies.

1.2 Mobile Admin tabs and their purpose

The app is controlled using virtual buttons and tabs in the top bar and Android HW buttons of the device.

1.2.1 Identifiers

Identifiers represent all physical identification media that can be used by the user. Typically, identifiers are RFID cards or tags or any type of NFC tag (in any shape). RFID identifiers can be MIFARE Classic or MIFARE DESFire cards/tags. Each identifier belongs only to one Group (of access rights).

1.2.2 Phones

Phones are any mobile devices that are being used as an identification token. Devices added to this tab are issued a virtual Mobile Key that is remotely transferred to the device. Each phone belongs only to one Group (of access rights).

1.2.3 Readers

A reader represents a specific RSW.04-P(B) reader in the system. If a door is equipped with one reader from each side, then such readers are represented as two separate readers inside the app. It is therefore essential to use proper naming.

Each reader can be linked with up to 20 holiday days, one free-entry calendar and 20 access-limitation calendars.

1.2.4 Groups

A Group represents a user or group of users with specific access rights. A Group links **Identifiers** and **Phones** to **Readers**. If you want to enable a user to access through a specific reader, the users Identifier and the Reader must be linked to the same Group.

Each Group can consist of up to 2100 Identifiers and Phones (depending on reader FW version) and be linked with up to 255 Readers. Groups further enable the admin to pair each linked Reader with a specific Calendar. Each Reader can therefore have different Calendar for each Group.

1.2.5 Calendars

A Calendar represents a weekly timetable defining time intervals for granting access to the linked Readers. The Calendar repeats each week and consists 7 days from Monday to Sunday. Each day can consist of max 4 intervals of allowed access. Between the time intervals, it is not possible to access the reader and the door remains closed. If no Calendar is assigned to a Reader, such Reader does not have any access limitation and be accessed any time.

1.2.6 Free Entry

A Free Entry represents a weekly timetable with defined time intervals during which the readers remain activated (access is allowed to everyone). It has the same format as Calendar.

1.2.7 Holidays

Holidays is a list of National holiday days. In a system, where Calendars or Free Entry is used, such days behave as Sunday.

1.3 Logical bonds and relations

The following diagrams represent the logical bonds of the terms specified in previous chapter. The arrows specify connections between the individual features and provide the direction of how they are linked together (ex.: Identifier is linked with a Group from the Identifier edit tab; in the Group edit tab, Readers are paired to the Group and Calendars are linked to each paired reader).

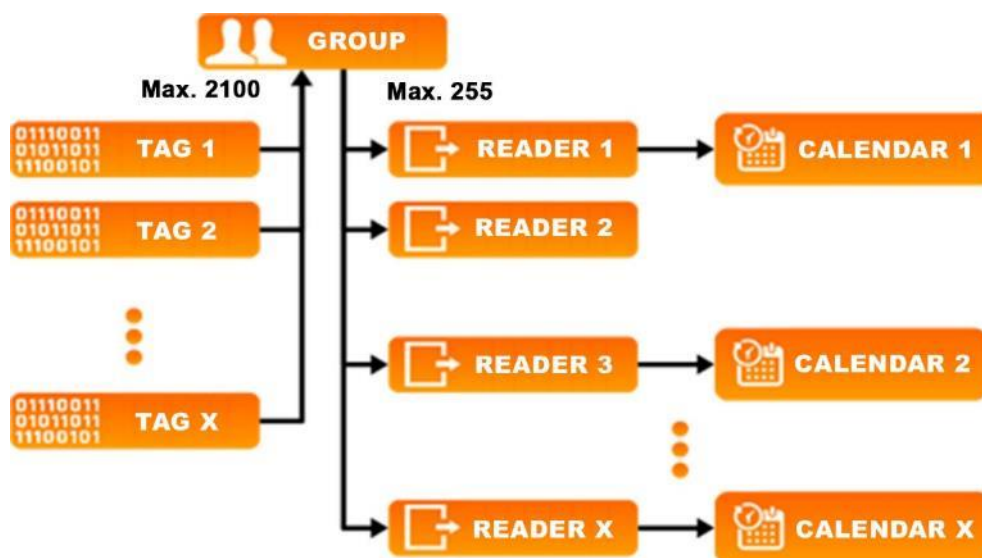


Image 1 - relations of a Group inside the app user interface

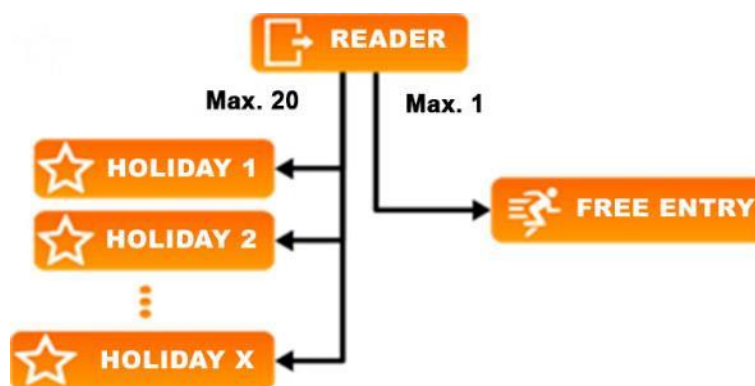


Image 2 - relations of a Reader inside the app user interface

1.4 Sample database and system setup

In this example, IMAporter Mobile is installed on the following doors:

- Front entry
- Back entry
- Wicket door
- Garage
- Cellar
- Office A – entrance reader
- Office A – exit reader

It is reasonable to create **Groups** with the following access rights:

Group	Assigned Reader
Tenants	Front entry, Back entry, Wicket door
Tenants with garage	Front entry, Back entry, Wicket door+ Garage
Tenants with cellar	Front entry, Back entry, Wicket door+ Cellar
Tenants with garage and cellar	Front entry, Back entry, Wicket door+ Garage + Cellar
Services	Front entry, Wicket door
Administrator	all readers
Company A - management	Front entry, Back entry, Wicket door+ Garage, Office A – entrance reader and exit reader
Company A - employee	Front entry, Wicket door+ Garage, Office A – entrance reader and exit reader

Each user (**Identifier** or **Phone**) is then assigned to the **Group** corresponding to his access rights. If the users access rights get changed (a tenant for example buys a Cellar), his **Group** gets easily updated to again correspond with his current level of access rights.

It is further possible to assign Calendars to Readers inside the specific Groups:

Group	Assigned Reader	Calendar	Note
<i>Services</i>	<i>Front entry</i>	<i>Services</i>	Can access from 7:00 AM to 9:30 AM
	<i>Wicket door</i>		
<i>Company A - management</i>	All assigned readers	without Calendar	Can access at any time
<i>Company A - employee</i>	<i>Office A – exit reader</i>	without Calendar	Can leave at any time, will not remain locked after working hours
	Remaining assigned readers	<i>Company A – working hours</i>	Can access only during working hours

Assigned Calendars – Services such as Post or Garbage men can access assigned doors only during morning hours. Management of Company A can access the building at any time, whereas its employees can access only during working hours. Groups that are not listed do not have any time-related access limitations.

Further employees of Company A are not allowed to access the building on public holidays. To enable this feature, their relevant **Calendar** must be set not to enable access on Sundays. Listed **Holidays** are therefore linked only to readers related to Company A. Its employees can therefore access the building, but are not allowed to enter the Company premises:

Reader	Holidays
<i>Office A – entrance reader</i>	National holidays
<i>Office A – exit reader</i>	National holidays

2 Getting started – Easy start-up guide

This chapter will guide you through the process of getting the system to work as quickly as possible while enabling just the most necessary features.

2.1 First launch and settings

2.1.1 Fill in the Admin password

When IMAporter Mobile Admin is launched for the first time on a new mobile device, it asks for Admin password (described here: [3.1 First launch](#))

The Admin password is provided to you by the system supplier (set using ACS Config app) and is necessary to fill in correctly in order to be able to pair and program readers. For demonstration purposes could be just “**demo**”.

2.1.2 Load the settings

While in the Settings menu, you need to load system configuration file. This file with **.imaportercrd** extension is provided by the distributor (*is generated by the ACS Config app for initial setup of the system*). Without loading this file, the system may not work properly.

A demo configuration file can be downloaded from here:
<https://www.ima.cz/app/imapadmin/Config-file.imaportercrd>
(Configuration: **Admin pass:** demo, **System ID:** demo0001,
Accepted media: UID from compatible tags + cards and
mobile devices via NFC and BLE)



2.1.3 Enter the IMAporter IDcloud login (necessary to use MobileAccess)

- 1) In the **Menu**, select **IDM Settings**
- 2) Fill in credentials provided by the system supplier

2.1.4 Optionally load a DEMO database (backup file)

- 1) **Download** the demo.ppj file to your mobile device from here:
<https://www.ima.cz/app/imapadmin/Demo-DB-backup.ppj>
- 2) In the **Menu**, select **Load backup**
- 3) Navigate to the downloaded Demo-DB-backup.ppj file (usually in Downloads) and load



2.2 Create a Group

- 1) Navigate to the **Groups** tab and tap the **Add** button
- 2) Create a new group of any name (for example “Group”)

- 3) Return to the main application screen

2.3 Add a Reader

- 1) Navigate to the **Readers** tab and tap the **Add** button
- 2) Tap your NFC enabled phone onto to front of the reader
- 3) Enter the name of the reader or leave the automatically generated one
- 4) Tap **Assigned groups** button and tap **Add** button (in the top-right corner) on the next screen
- 5) Select the group created in the previous steps and return to the main application screen

2.4 Add an Identifier

- 1) Navigate to the **Identifiers** tab and tap the **Add** button
- 2) Tap you RFID or NFC identifier to the back of your NFC device (or where the antenna is)
- 3) Enter the name of the Identifier/User and select a Group from the dropdown menu (the one that you in the previous steps created and paired with the reader)
- 4) Return to the main application screen

2.5 Add a Mobile Key

- 1) Navigate to the **Phones** tab and tap the **Add** button
- 2) Fill in the **User name**, **User email address** and select **access rights group**
- 3) *Optionally you can enter also **Key name**, **Device name**, **Phone number** and select **Key Validity***
- 4) Click **DONE** and wait for the identifier to create
- 5) Return to the main application screen

2.6 Update the system

- 1) Tap the Programming button in the top bar of the app
- 2) With green programming screen shown on the display, tap the reader and hold the device still until the programming process is finished.

2.7 Test the system

- 1) Try taping the reader with the RFID or NFC tag that you programmed in previous steps.
- 2) The reader should beep, light green LED and relay should switch (click) for the time previously specified in **Settings**.

2.8 Test the MobileAccess function

NOTE: This is only a fast test/setup guide, to learn more about the **IMAporter Mobile Key app**, please **download** the relevant manual.

- 1) For your test device, download the IMAporter Mobile Key app from here:

<http://ima.cz/app/key>



- 2) Launch the app and check if your mobile device is compatible (you should see a green smiling face accompanied with a text naming available technologies. Ideal is to have both NFC and Bluetooth.
- 3) Tap the button Go to **Mobile Keys download**
- 4) Check your email inbox for email with subject **MobileAccess Key** and load the attached QR code with your **Mobile Key** app.
- 5) Test procedure for **NFC mobile devices**:
 - a. Make sure the display is ON and tap the reader
 - b. The reader should blink green LED, beep and the relay should click
- 6) Test procedure for **Bluetooth mobile devices**:
 - a. Make sure that your reader HW supports Bluetooth communication (the sticker on the back of the reader must say **RSW.04-PB**)
 - b. In the **IMAporter Mobile Key** app navigate to menu **Available doors**
 - c. If the phone detects a "MAC" address, click the item to initiate communication.
 - i. The reader should blink green LED, beep and the relay should click
 - ii. First communication takes longer time
 - iii. If you do not detect any "MAC" address, then check the step 6) a. again
 - iv. The "MAC" address can be provided with a Name – this is done under **My Doors** menu and described in the **IMAporter Mobile Key manual**.

3 Mobile Admin manual

3.1 First launch

3.1.1 Entering Admin password

When we run the IMAPorter Mobile Admin app for the first time, the settings screen shows up requesting us to enter an **Admin password** ([Image 3 – Entering Admin password](#)). This password is used for pairing the admin device with the readers and to protect them from being overwritten by a third party. It is encoded to the readers by the system supplier using the **ACS Config** configuration app (available only to certified partners). Each admin should be provided with the Admin password by the supplier of the system.

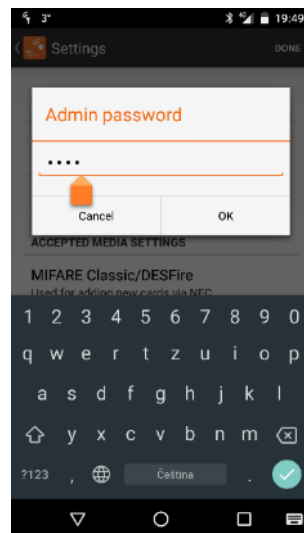


Image 3 – Entering Admin password

3.1.2 Loading system settings

While in the **Settings** menu, you need to load system configuration file. This file with **.imaportercrd** extension ([Image 4 – System settings](#)) is provided by the distributor (is generated by the **ACS Config** app for initial setup of the system). Without loading this file, the system may not work properly.

To be able to load the .imaportercrd settings file, a correct Admin password must be entered first!

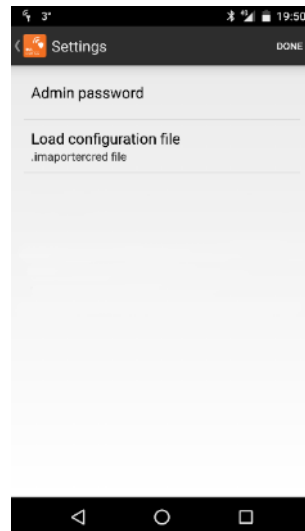


Image 4 – System settings

3.2 System settings

For security purposes, all system settings have been moved to external **ACS Config** app that is available only to certified partners. If you need to change some system settings, please contact your distributor.

Available settings are:

- 1) LED status blinking
- 2) Buzzer beeping
- 3) Setting lock timeout (5-35sec interval)
- 4) Activation of MobileAccess function (NFC / BLE / PIN verification)
- 5) Setting new MobileAccess system key and ID, reader ID
- 6) Accepted ID media + settings (MIFARE CLASSIC / MIFARE DESFire / NFC tags / UID reading / Encrypted file reading ...)

NOTE: the ACS Config app is available only to certified distributors. In order to learn more about the app, **please ask for the relevant manual.**

3.3 Backup and restore function

Selecting the **Save backup** item from the menu, we run a dialog asking for backup filename ([Image 6 - DB backup](#)). To successfully backup the data, we just need to fill in the filename and press **save** button.

Choosing the **Load backup** item from the same menu launches a file explorer ([Image 7 - Loading DB backup](#)) allowing us to choose a backup file we want to restore.

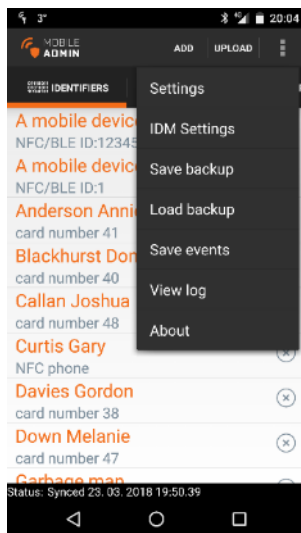


Image 5 - Application menu

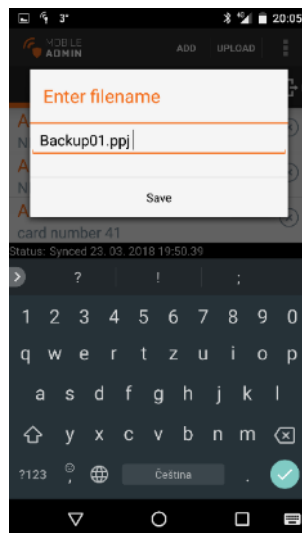


Image 6 - DB backup

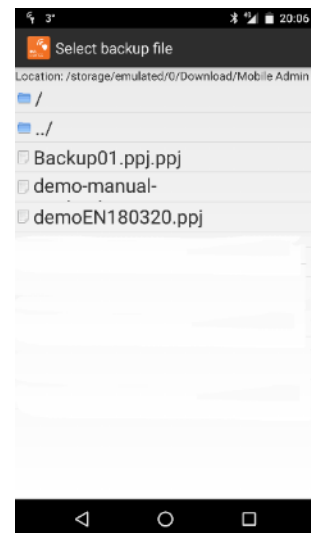


Image 7 - Loading DB backup

When saving a backup, we do not need to fill in the filename suffix **.ppj**, it is added automatically. All backups are saved into internal memory of the device into **Download\Mobile_Admin** folder. All saved backups can be transferred into PC (over USB cable, bluetooth, email etc.) for further processing using IMAporter PC Admin application or using another mobile device.

3.4 Access logs backup

Selecting the **Save events** item from the menu ([Image 5 - Application menu](#)), we run a dialog asking for filename under which we want to export the user access history ([Image 8 - Save events](#)).

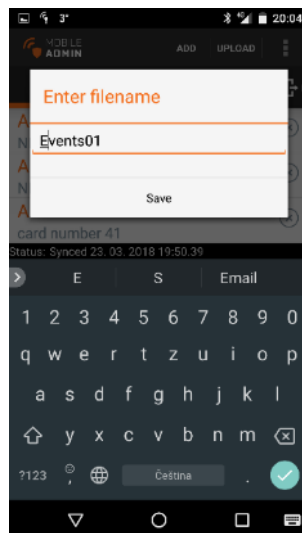


Image 8 - Save events

When saving, it is not necessary to fill in the suffix **.csv** – it is added automatically. The attendance data are saved in CSV format into the **Download\Mobile_Admin** folder in the internal phone memory. When copied into PC, they can be further processed using notepad or MS Excel or LibreOffice Calc.

NOTE: When exported, the attendance data is removed from the mobile app and is only accessible from the CSV file. It is recommended to export the data periodically and maintain it backed up in a PC.

3.5 Identifiers tab

Selecting the **Identifiers** tab shows a list of all available identification media ([Image 9 - Identifiers tab](#)). As it is the first tab of the IMAporter Mobile Admin app, it is displayed automatically after the app starts

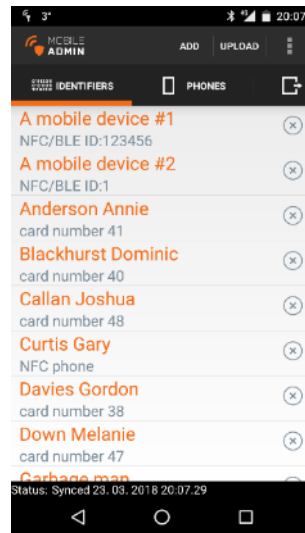


Image 9 - Identifiers tab

3.5.1 Adding a new card and editing current one

Tapping the **Add** button in the top button bar ([Image 9 - Identifiers tab](#)), while being at the **Identifiers** tab, will display an identifier-adding dialog ([Image 10 - Add a new tag](#)).

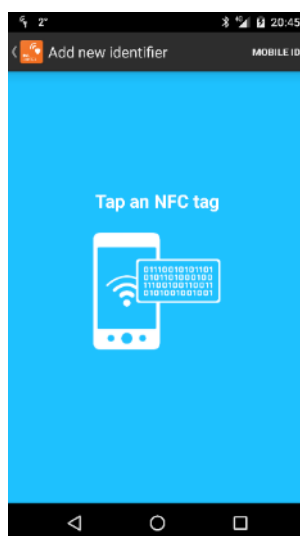


Image 10 - Add a new tag

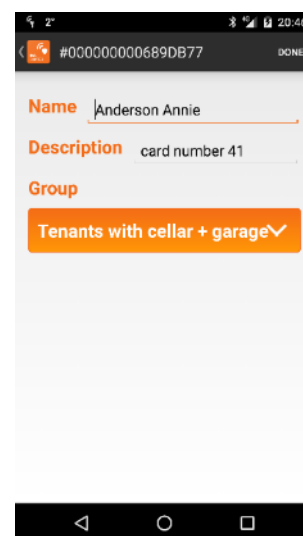


Image 11 - Name a new tag

By tapping a card, tag or other identification media to the back side of the phone (or elsewhere, where the NFC antenna is located), an identification ID is read and add-identifier edit form is displayed ([Image 11 - Name a new tag](#)).

The same edit form can also be displayed by tapping any random record from the list of available identifiers ([Image 9 - Identifiers tab](#)).

3.5.2 Identifier edit form

After filling the Name field of the add-identifier dialog a Group menu pops out ([Image 12 - Select group](#)). Using the Group menu we choose to which access-rights group the user belongs to ([Image 11 - Name a new tag](#)). The Name field is required and must be filled in, field description is optional. If we are not adding an identifier, but only editing, then all the fields are shown straight away – including the Group field ([Image 12 - Select group](#)).

Each card can be assigned to only one Group of access rights. How to create a group and set its access rights is described in chapter **Groups tab**.

If a card is lost or is not assigned, it can be assigned to group **<None>** and so it will not have any access rights.

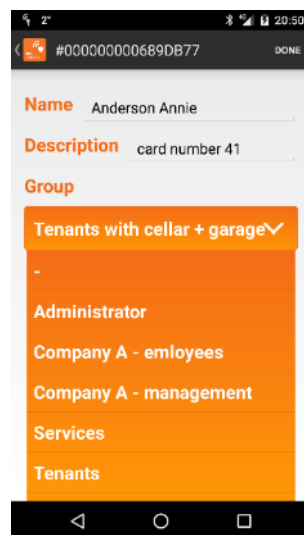


Image 12 - Select group

3.5.3 Deleting identifiers

In case we need to delete a specific identifier including all its access rights, we tap the cross icon on the specific row of the identifier to be deleted ([Image 9 - Identifiers tab](#)). By confirming the **Remove identifier** dialog, the identifier is permanently removed.

3.6 Phones tab (MobileAccess function)

Selecting the **Phones** tab shows a list of all mobile devices added to the system. This list is kept and periodically synchronized from the ID management server.

To be able to use this feature, the Mobile Admin app must be paired with the ID Management server (see next section).

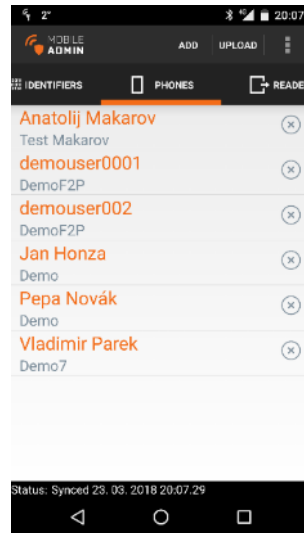


Image 13 - List of mobile devices (phones)

3.6.1 Logging into IMAporter ID Management

To be able to use the MobileAccess function, it is necessary to have pair the Mobile Admin app with your ID Management account.

To obtain access and login to the IMAporter ID Management server, please contact your distributor.

Login window can be launched from the menu by tapping the IDM Settings item ([Image 14 - Application menu - IDM settings](#)).

In the login window ([Image 15 - ID Management login](#)) you can activate Auto update feature. All Phones data are stored on the server and can be edited also from there. In case of such edit, changes automatically propagate to the mobile app.

Each login is stored and valid for 1 year. After this period it is necessary to login again.

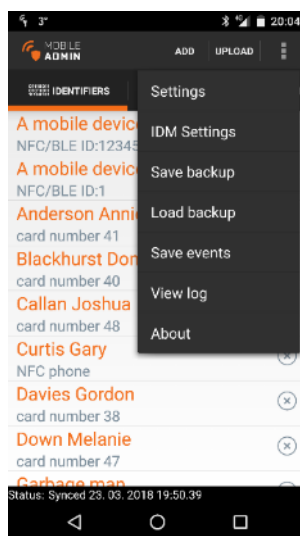


Image 14 - Application menu - IDM settings

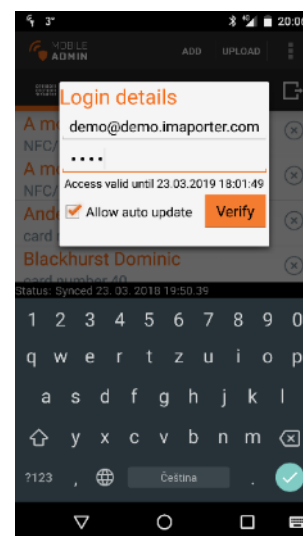


Image 15 - ID Management login

3.6.2 Adding (editing) a new Mobile Key (Phone)

To add a new mobile key for a mobile device or phone, tap the **ADD** button on the **Phones** tab ([Image 13 - List of mobile devices \(phones\)](#)).

An **Add/edit phone** dialog shows up ([Image 16 - Add a new Mobile Key](#)). It is necessary to fill in the **Person** name, **Email** address and **Group** of access rights. All other fields are optional and do not need to be filled.

The purpose of each field is described below:

Person:	Required field, name of the user
Key:	Optional field, the Mobile Key name as it shows in users mobile phone (if not filled-in, a system default name is used)
Device:	Optional field, name of the device for internal system purposes (if not filled-in, a default name is used)
Phone:	Optional field, phone number of the user including country prefix, can be used for sending Mobile Key over SMS (not yet active)
Email:	Required field, Mobile Key is sent to this email address
Group:	Required field, similar as in Identifiers tab, assigns access rights to the user
Valid from/to:	Optional field, defines validity of the Mobile Key (if not filled-in, default validity is used)

All entered data are transferred to the **IMApporter ID Management server** upon saving the form. A unique user identifier is instantly generated by the server and returned back to the **Mobile Admin app** and stored in local DB. At the same time, the new Mobile Key is sent from the server to the users email address.

To successfully create a **new Mobile Key**, it is therefore **necessary to be on-line**.

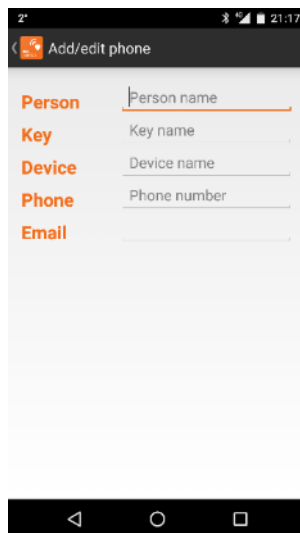


Image 16 - Add a new Mobile Key

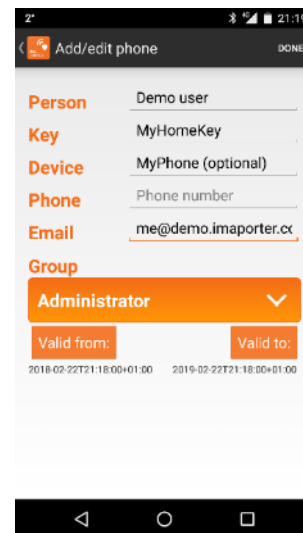


Image 17 - New device credentials

To activate the newly added Mobile Key (Phone), it is necessary to **Upload changes to the reader**. This is described in section [0](#)

Uploading changes (synchronizing access rights).

NOTE: How to enroll a new Mobile Key into user's mobile devices is described in **IMAporter Mobile Key manual** that can be **downloaded from our website**.

3.6.3 Adding a new Mobile Key manually (optional)

This part is for users who do not have IMAporter ID management activated and still want to use IMAporter Mobile Keys.

To add a Mobile Key manually, it is necessary to navigate to the Identifiers tab and tap **ADD** button ([Image 18 - List of identifiers](#)). In the **Add new identifier** dialog, navigate to menu in top right corner and tap **MOBILE ID** button ([Image 19 - Add a new tag / mobile ID](#)).

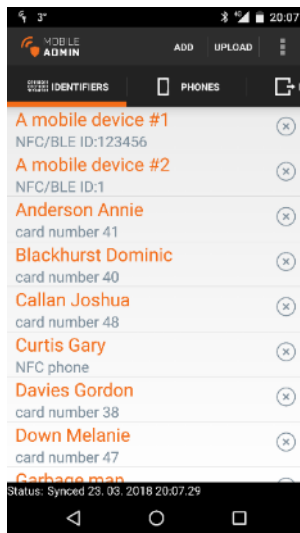


Image 18 - List of identifiers

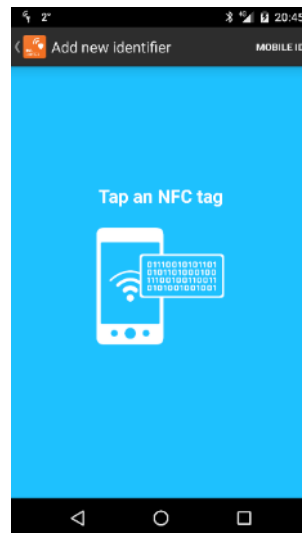


Image 19 - Add a new tag / mobile ID

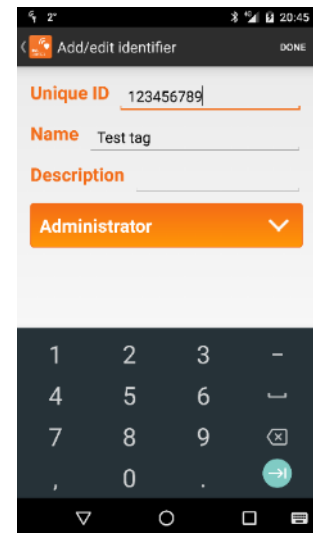


Image 20 - Add new ID manually

To add a new Mobile Key manually, you need to enter a **unique ID**, **name** of the user and **Group** of access rights ([Image 20 - Add new ID manually](#)).

It is necessary to remember the ID as it needs to be manually entered into the users IMAporter Mobile Key app. This procedure is described in **IMAporter Mobile Key manual** that can be **downloaded from our website**.

3.7 Readers tab

Selecting the **Readers** tab, displays a list of available doors/readers ([Image 21 - Readers tab](#)).

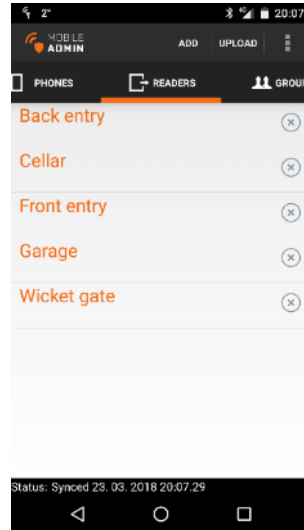


Image 21 - Readers tab

3.7.1 Adding new readers and editing existing ones

Tapping the **ADD** button in the top button bar ([Image 21 - Readers tab](#)), while being at the **Readers** tab, will display a reader-adding dialog ([Image 22 - Add a new reader](#)).

It is possible to add only readers that are configured using the same **Admin Password** as the one entered in the **settings** of the **Mobile Admin app**. The Admin Password is encoded to the readers by the system supplier using the **ACS Config** configuration app and is identical to all readers within the installation site. Each admin (customer) should be provided with the **Admin password** by the system supplier. Readers from other sites (buildings) using different Admin passwords therefore cannot be added – the IMAporter Mobile Admin will ignore them.

A reader is added by tapping it using the mobile device.

Each reader within the site (if more than one reader is installed) is encoded by the system supplier with a different **Reader ID**. This ID is internally used for distinguishing between the readers. When adding a new reader, the name will be filled automatically providing the **Reader ID**. It is possible to rewrite this name.

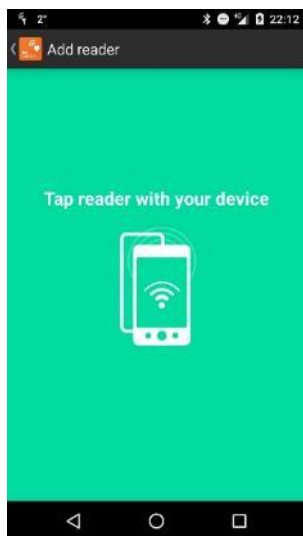


Image 22 - Add a new reader

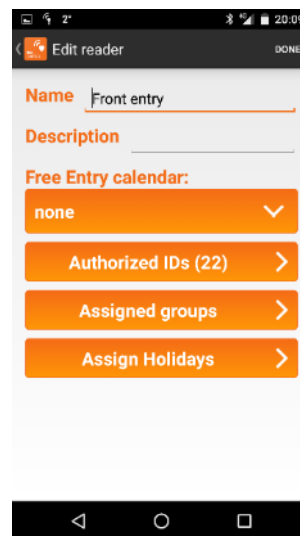


Image 23 - Reader edit form

When new reader is detected, an edit form is displayed. The same edit form can be displayed by tapping any random reader on the Readers tab ([Image 21 - Readers tab](#)).

3.7.2 Reader edit form

In the edit form ([Image 23 - Reader edit form](#)) it is required to fill in the **Reader name** and optionally the description. Following that, there is option to assign **Free Entry calendars**, display a list of **Authorized (paired) IDs** and assign access-rights **Groups** and **Holidays**.

The number of **Groups** a Reader is paired with is individual. A Reader can be paired to all of them or none.

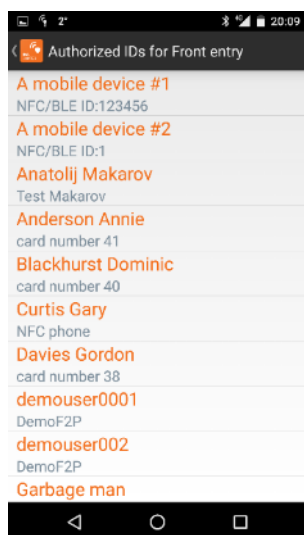


Image 24 - List of authorized IDs

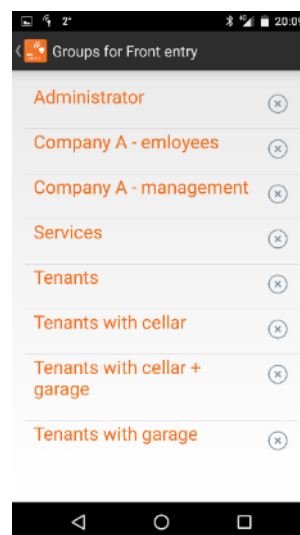


Image 25 - List of paired Groups

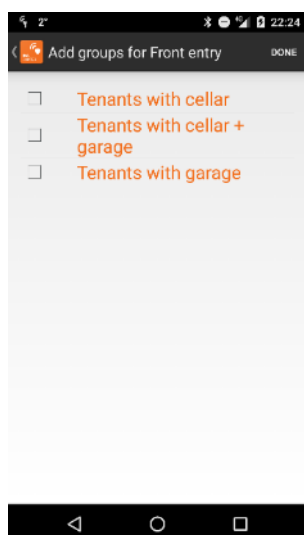


Image 26 - Groups for pairing

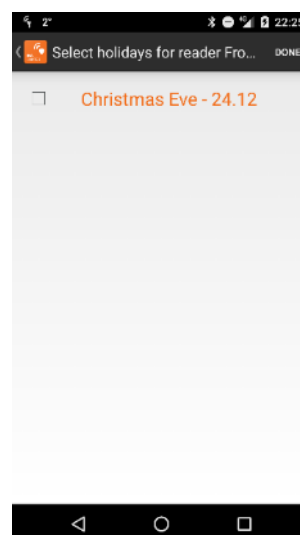


Image 27 - Holidays for pairing

Free Entry

Tapping the drop down menu labeled **Free Entry** ([Image 23 - Reader edit form](#)) it is possible to select and assign or create a new **Free Entry calendar**. The Reader/door then remains open/unlocked in the time intervals specified in the calendar

Allowed Identifiers

Each Reader allows us to view a list **Identifiers** that are linked via **Groups** ([Image 24 - List of authorized IDs](#)). All the linked Identifiers are enabled to access the specific reader. This list has only informative nature.

Assigned Groups

Tapping the **Assigned Groups** button displays a list of **Groups** that the Reader is paired with ([Image 25 - List of paired Groups](#)). By tapping **Add** button, we can display a complete list of available **Groups to be assigned** ([Image 26 - Groups for pairing](#)).

Assigned Holidays

Tapping the **Assigned Holidays** button displays a list of Holidays available to be paired with the Reader ([Image 27 - Holidays for pairing](#)). This feature is only usable together with using Calendars or Free Entry as on the dates specified by the paired Holidays the Reader behaves as if it was Sunday.

Removing reader from Group

Reader can be removed from a group by tapping the **cross icon** next to each group ([Image 25 - List of paired Groups](#)). A confirmation dialog appears for this action

View access log

If some access history has been recorded for the current Reader, the Reader edit form shows an **Events button** as the last item on the site. By tapping button, we can view a chronologically sorted list of individual passes together with a name of the user (if it was recorded) and time and date stamp

The mobile app only shows a limited overview of the access history. To view detailed records, the access history must be saved to a file (chapter [3.4 Access logs backup](#)) in CSV format and open in PC using a spreadsheet processor (e.g. MS Excel or LibreOffice Calc).

NOTE: When exported all access logs are removed from the mobile app and are only accessible from the CSV file. It is recommended to export the data periodically and maintain it backed up in a PC.

3.8 Groups tab

Selecting the **Groups** tab will display a list of available access-rights Groups ([Image 28 - List of access rights Groups](#)).

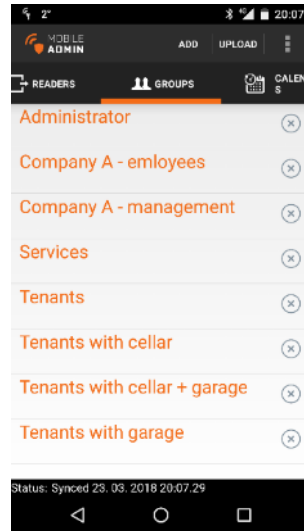


Image 28 - List of access rights Groups

The number of **Groups** is unlimited and corresponds to the number of different types of access rights.

3.8.1 Adding a new Group

Tapping the **Add** button in the top button bar ([Image 28 - List of access rights Groups](#)), while being at the **Groups** tab, will display a group-adding dialog (image 25). An edit form of an existing group can be displayed by tapping on its name in the list.

3.8.2 Group edit form

Both above described procedures display the **Group edit form** ([Image 29 - Group edit form](#)). The field **Name** is required and must be filled every time, while the description is optional.

Using the **Assigned card reader** button we are able to display and manage the doors assigned to this Group. This function is duplicate and can be as well carried out from the **Reader** tab as described in the previous chapter.

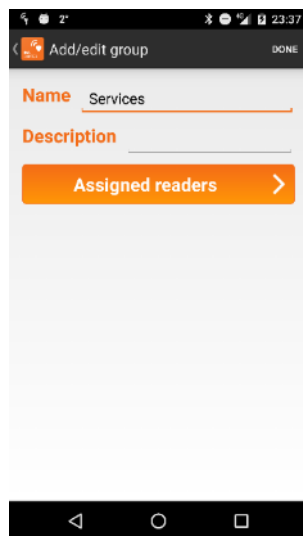


Image 29 - Group edit form

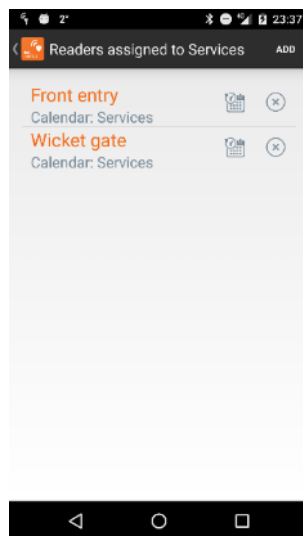


Image 30 - Assign Readers to Group

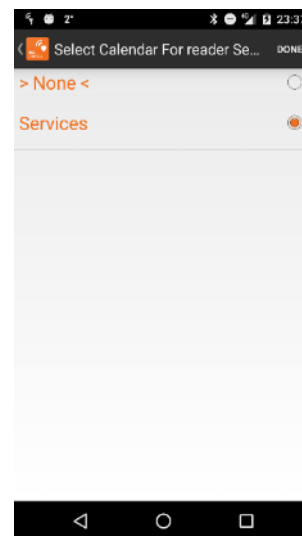


Image 31 - Assign Calendar to Group-Reader pair

Adding and removing Readers

Taping the **Assigned card readers** button ([Image 29 - Group edit form](#)) opens a list of readers assigned to this group ([Image 30 - Assign Readers to Group](#)). Taping the **Add** button in top-right corner, we are able to view a list of all available, yet unassigned readers and pair them with the Group

To remove already assigned doors from the list ([Image 30 - Assign Readers to Group](#)), we must tap the cross icon located right from each list item. Confirming the remove-confirmation dialog will definitely delete the pairing.

Adding and removing Calendars

Calendars are always assigned to the pair Group-Reader, meaning that one Reader can behave according to a different Calendar for each Group of access rights. Displaying the **Assigned card readers** screen ([Image 30 - Assign Readers to Group](#)), we can display or pair a new Calendar. This is done by taping the Calendar icon next to the paired Reader on the Assigned card readers screen ([Image 30 - Assign Readers to Group](#)). After taping the icon, app shows a list of available calendars to choose from. If we want to cancel calendar pairing and enable unrestricted access at any time, we need to select calendar **> None <**.

3.9 Calendars

Under the tab **Calendars**, it is possible to prepare a list of specific Calendars to be used to limit group access rights according to time and day of the week.

The system recognizes two types of Calendars:

- Access limiting calendars
- Free entry calendars

Under this tab we will prepare the Access limiting Calendars.

To create a new Calendar, tap the **ADD** button on the Calendar tab ([Image 32 - List of available Calendars](#))

Prepared Calendars are to be paired to the **Group-Reader link** as described in previous chapter ([Image 30 - Assign Readers to Group](#)).

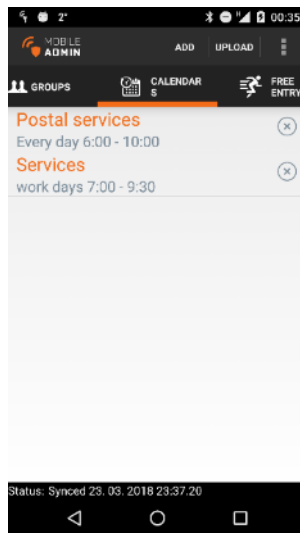


Image 32 - List of available Calendars

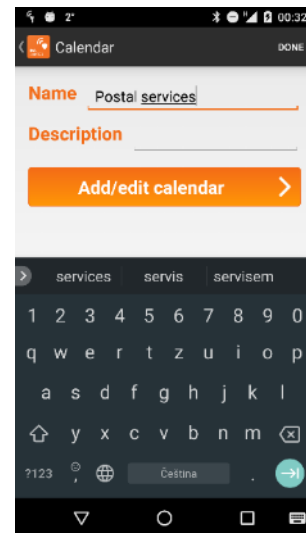


Image 33 - Calendar edit form

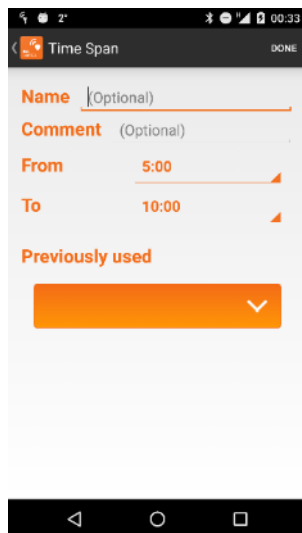


Image 34 - Setting Calendar time-span

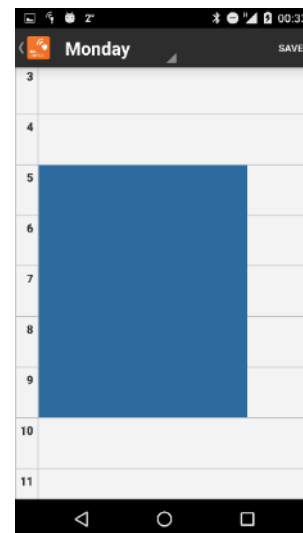


Image 35 - Access-Granted period

3.9.1 Edit form and time zones

Adding a new calendar or selecting one of already prepared calendars opens an Edit form ([Image 33 - Calendar edit form](#)). In the Edit for, the calendar can be named and in this case it is also very helpful to fill-in the description providing the time-spans the calendar is set for.

By tapping the **Add/edit calendar button**, a time-span setting appears ([Image 35 - Access-Granted period](#)). Double tapping into the calendar opens a new screen enabling the user to set the exact time-span ([Image 34 - Setting Calendar time-span](#)) or select a previously created time-span from the dropdown menu. When edited and saved, it colors the Access-Granted period as can be seen in ([Image 35 - Access-Granted period](#)).

It is possible to set up to 4 time zones for each day.

Users can navigate between days of the week by sliding to the side or by selecting a specific day from the dropdown menu ([Image 36 - Navigation between days](#))

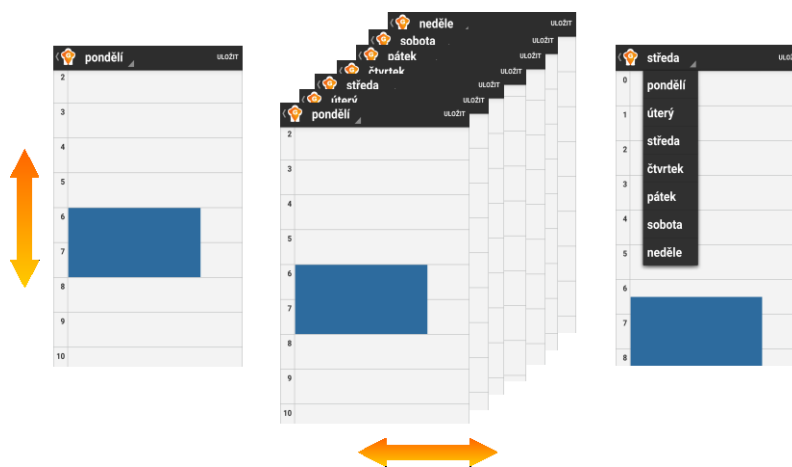


Image 36 - Navigation between days

To delete a time zone, simply tap it in the ([Image 35 - Access-Granted period](#)) view and tap the **DELETE** button

3.10 Free entry

Free entry calendars are available under the tab Free Entry and are prepared in the same way as standard access limiting calendars. The purpose of **Free entry** calendars is to define time zones, when the door will hold open for everyone.

Free Entry calendars are to be paired to a specific reader on the **Reader edit** screen ([Image 23 - Reader edit form](#)).

3.11 Holidays

Holidays are closely bound to both types of Calendars providing a list of “special” days that act as Sunday. Such days are typically National holiday Days.

3.11.1 Adding and removing holidays

Similarly to other tabs, a new Holiday is added by tapping the ADD button on the Holidays tab. Such action opens the Holiday edit form ([Image 38 - Holiday edit form](#)).

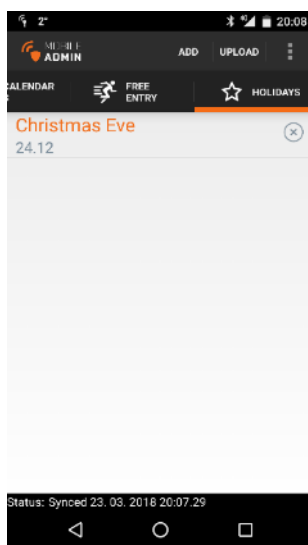


Image 37 - List of created Holidays

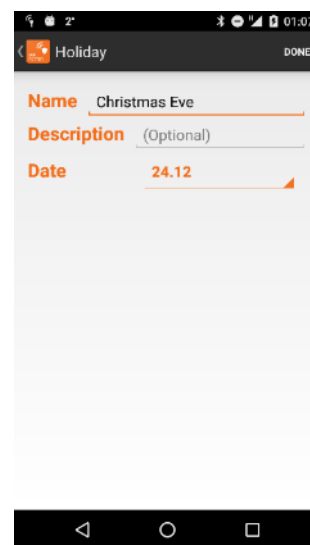


Image 38 - Holiday edit form

3.11.2 Edit form

In the Holiday edit form, it is necessary to enter the **Name** of the holiday and its **Date**.

3.12 Uploading changes (synchronizing access rights)

Uploading or should we call it synchronization of access rights in phone with access rights saved in IMAporter Mobile/Basic Access Systems can be initiated by pressing the **Upload** button in top-right corner of the app ([Image 39 - App homescreen](#)).

A **data upload** screen ([Image 40 - Data upload dialog](#)) is shown, where we can select using two tickboxes if we want to only **upload access rights** (sync changes) or **read access history** (download events). After ticking the selected boxes we just tap the reader with the back of the phone. The reader identifies itself and relevant data is uploaded to it.

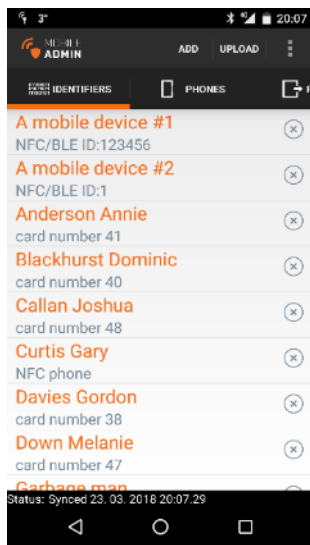


Image 39 - App homescreen

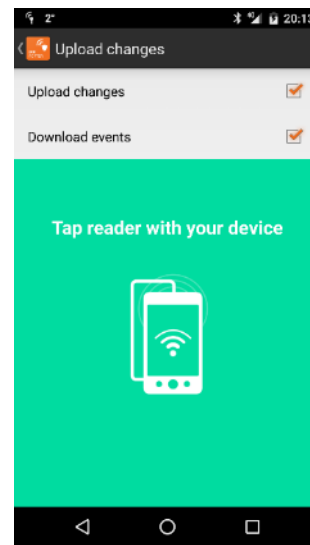


Image 40 - Data upload dialog

During the update process a screen informing about the state of communication is shown ([Image 41 - Upload in progress](#)).

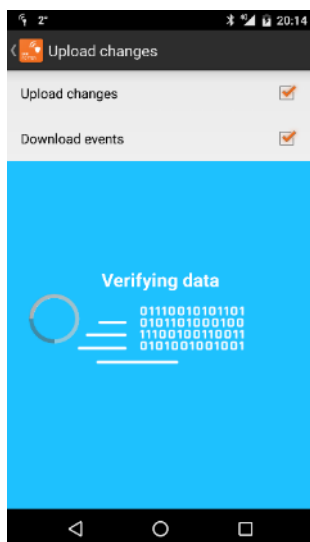


Image 41 - Upload in progress

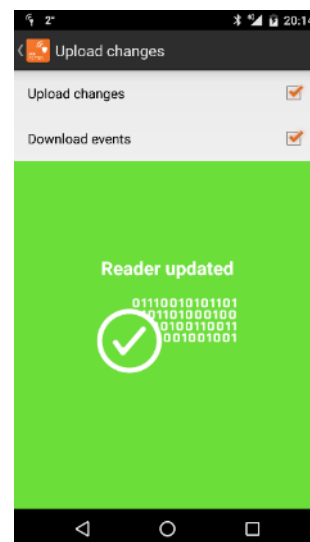


Image 42 - Data upload successfully finished

After the upload process is finished, an information screen shows informing about the results of data upload ([Image 42 - Data upload successfully finished](#)). If the upload fails for any reason, it is enough to take the phone further from the reader and tap the reader again. The communication continues from where it failed.

The upload time depends on how much data is transferred and the NFC performance of the phone, it takes usually from 2 to 90 seconds.