

Codeks Virtual Card

INSTRUCTION MANUAL FOR ADMINISTRATORS on using the additional **Codeks Virtual Card** license code and the configuration of virtual cards

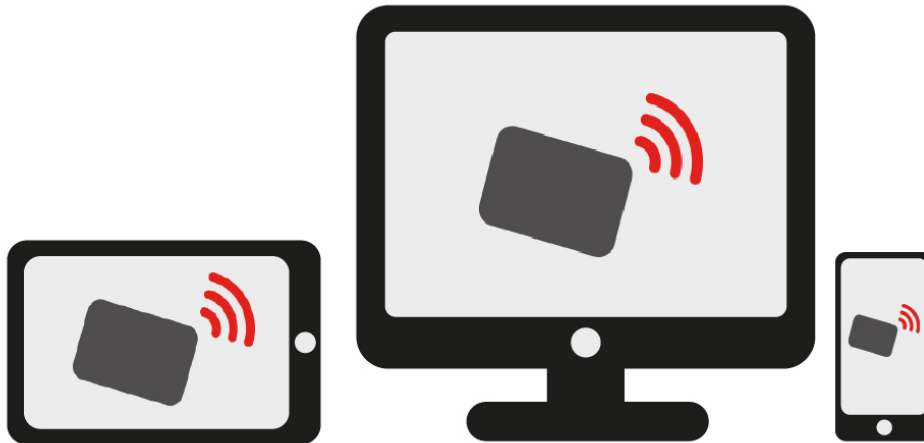


CONTENTS

0	INTRODUCTION.....	3
1	ADDING THE LICENSE CODE TO THE SOFTWARE	4
2	ASSIGNING A VIRTUAL CARD TO A USER	5
3	SETTINGS FOR TIME ATTENDANCE	5
	USER SETTINGS.....	5
	TIMETABLE AND GROUP SETTINGS.....	6
	SETTINGS FOR MOBILE T&A REGISTRATION WITH A VIRTUAL CONTROLLER	7
	* INSTALLING THE CODEKS MOBILITY MOBILE APPLICATION	9
	* ADDITIONAL SETTINGS FOR WEB TIME ATTENDANCE REGISTRATION....	9
	* ADDITIONAL SETTINGS FOR MOBILE TIME ATTENDANCE REGISTRATION	10
	REGISTERING TIME ATTENDANCE VIA A WEB BROWSER AND THE MOBILE APPLICATION.....	11
4	ADDITIONAL AND ADVANCED SETTINGS FOR THE USE OF THE CODEKS VIRTUAL CARD ADDITIONAL LICENSE CODE	12
	SETTINGS FOR MULTIPLE EMPLOYEE REGISTRATION ON A SINGLE MOBILE DEVICE.....	12
	SETTINGS FOR TIME REGISTRATION AT LOCATIONS WITH ASSIGNED LOCATION TAGS	15
5	SETTINGS FOR OPENING DOORS	18
	GENERAL PROGRAM SETTINGS	18
	SETTINGS FOR LOCATIONS.....	19
	SETTINGS FOR HARDWARE	20
	SETTINGS FOR USERS.....	21
	USING THE CODEKS MOBILITY TO OPEN DOORS	22
6	SSL CERTIFICATES.....	23

0 INTRODUCTION

This document provides instructions for administrators and describes how to use the additional Codeks Virtual Card license code. The instructions also describe the various configurations of the Codeks system settings, which in combination with the Codeks Virtual Card license code enable the registration of working hours via a web browser and the use of the Codeks Mobility mobile application.



The **Codeks Virtual Card** license code adds a number of virtual cards to the Codeks software, which can then be assigned to selected users and allow them to use the additional functionality of the Codeks software:

- **registration of working hours of employees via a web browser on the time attendance controller simulator,**
- **registration of working hours of employees via the Codeks Mobility mobile application**
- **opening doors using the mobile application Codeks Mobility.**

You can read more about the Codeks software and its add-ons on our website jantar.si.

1 ADDING THE LICENSE CODE TO THE SOFTWARE

After obtaining the **Codeks Virtual Card** license code you must add it to your Codeks system and activate it to enable the assignment of virtual cards to users in your system.

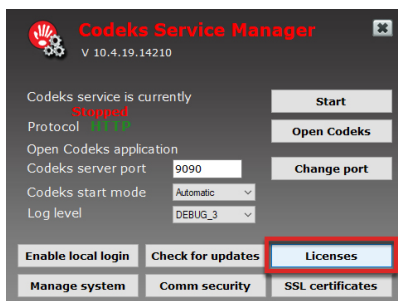
Add the *Codeks Virtual Card* license to your system using the **Codeks Service Manager** program.

The *Codeks Service Manager* program is installed on the Codeks server so to proceed you will need access to your Codeks server. You can open the program by double-clicking the **CodeksServiceManager.exe** file(C:\Program Files\Codeks or C:\Program Files (x86)\Codeks).

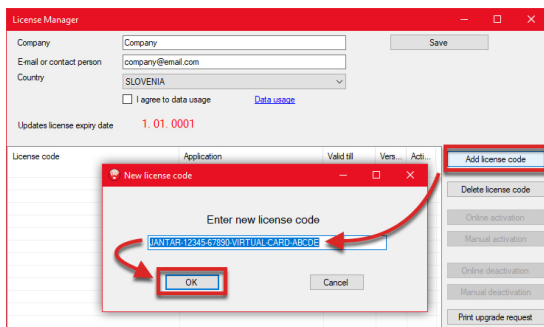
- 1 Before entering the license code, stop the Codeks service by clicking the **Stop** button. Before continuing make sure the service status is set to *Stopped*.



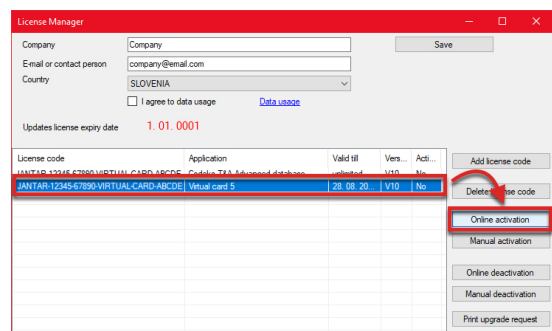
- 2 Then, click the **Licenses** button. A new pop-up window will open.



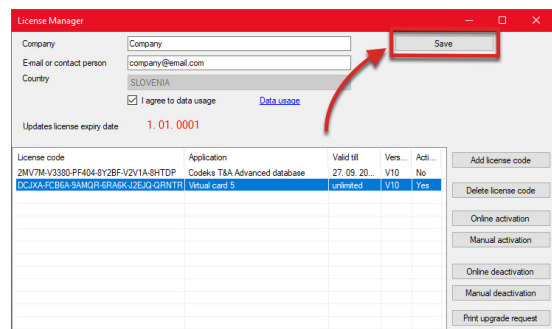
- 3 Click the **Add license code** button and the **License Manager** window will open where you can enter the license code and confirm your entry by clicking **OK**.



- 4 The *Codeks Virtual Card* license will now be displayed on the list. You still need to activate the newly entered license by clicking the **Internet activation** button.



- 5 The license validity date has now been changed to **unlimited**. When you are done, save your changes by clicking **Save**.



- 6 Then in the main window of the *Codeks Service Manager* program click the **Start** button to restart the Codeks service.

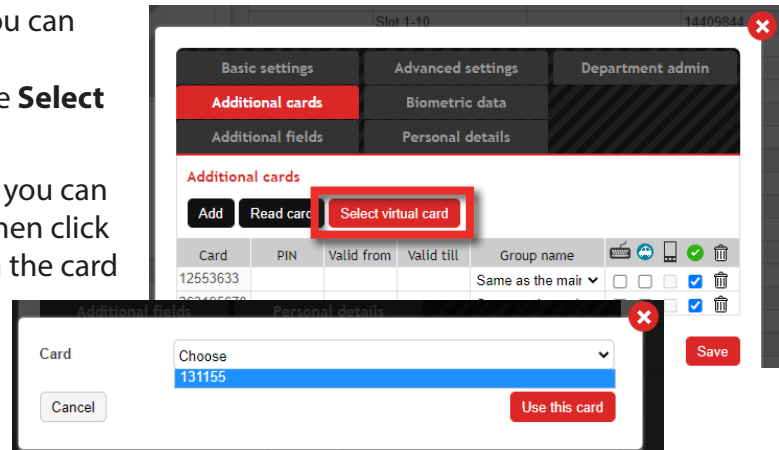


You can read more about adding, activating and removing license codes in the documentation of the main Codeks application (**CodeksManual-en_V10.pdf**).

2 ASSIGNING A VIRTUAL CARD TO A USER

After you have added the and activated the Codeks Virtual Card license code you can then start with assigning virtual cards to users.

- 1 To assign a user a virtual card, first, select the user on the list of all users in the *Users* editor and **double-click them**.
- 2 A new window will open where you can edit the user's settings.
In the *Additional cards* tab, click the **Select virtual card** button.
- 3 Another window will open, where you can select a virtual card number and then click the **Use this card** button to assign the card to the user.
- 4 Click **Save**.

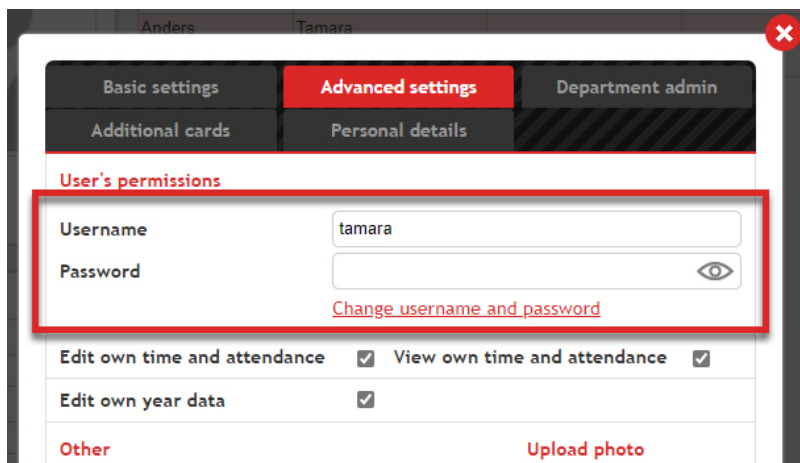


3 SETTINGS FOR TIME ATTENDANCE

Users who have an (additional) virtual card assigned in the Codeks system can register time registration events via a web browser using the T&A controller simulator and via the Codeks Mobility mobile application. This chapter describes the necessary settings to enable web T&A registration for users.

USER SETTINGS

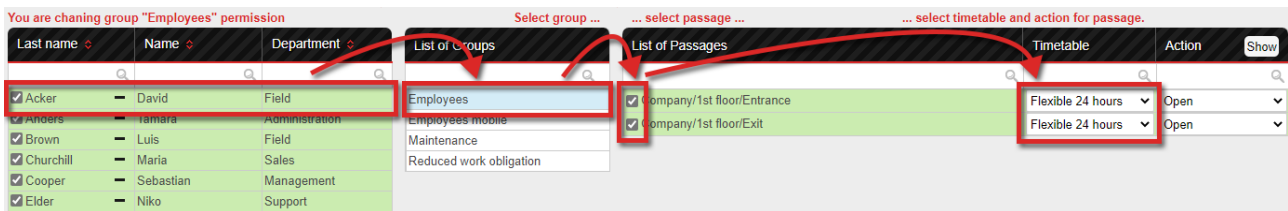
In addition to the assigned **virtual card**, each user will also require a **username and password** in order to login to Codeks via a web browser or to login to the Codeks Mobility app. You can assign these credentials to each user in the *Advanced settings* tab of their user settings in the *Users* editor.



TIMETABLE AND GROUP SETTINGS

Employees are assigned time attendance rights through the time attendance groups to which they belong, and the recording of work hours is regulated by timetables assigned to T&A locations.

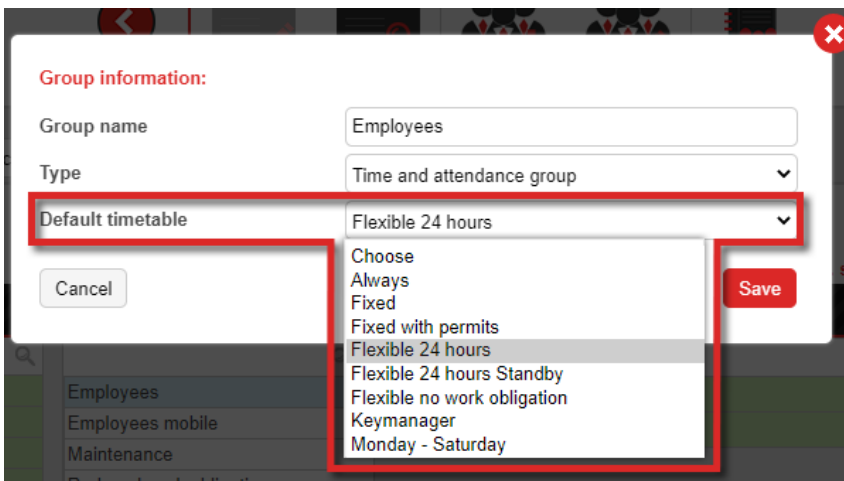
Each user must, therefore, be assigned to the appropriate time attendance group.



Timetables for time attendance specify the work obligation of employees, the times of arrival and departure from work, and the permitted exits during working hours (e.g. private or business exit).

Events that employees can register through a browser and mobile app are determined by the default timetable for time attendance of the T&A group they belong to.

To set the default group timetable, first, open the window for editing a groups settings and then, in the new pop-up window, select the appropriate timetable to be the default group timetable.



NOTE

When using the T&A registration via a web browser, we recommend that you only one (the same) timetable, within a selected group, for all (physical) locations where employees are allowed to register time attendance.

NOTE

The default timetable, according to which users will register their T&A via a web browser or mobile application, must contain all time intervals assigned with buttons that are assigned to the timetables at (physical) locations.

SETTINGS FOR MOBILE T&A REGISTRATION WITH A VIRTUAL CONTROLLER

NOTE

All newer Codeks systems whose main Codeks license (Codeks TA Kit, Codeks TA or Codeks TA Advanced) was first activated AFTER October 1, 2021, WILL REQUIRE at least one Codeks Virtual Controller license to enable mobile T&A registration through the Codeks Mobility app.

The Codeks Virtual Controller license enables mobile registration, additionally, it also enables the geographical restriction of the area around the point of the virtual controller, where employees are still allowed to register their working hours via mobile app.

All older Codeks systems whose main Codeks license (Codeks TA Kit, Codeks TA or Codeks TA Advanced) was first activated BEFORE October 1, 2021, will NOT REQUIRE for the basic operation of mobile T&A registration. Owners of such systems will be able to purchase the additional Codeks Virtual Controller license if they wish to upgrade their system with the functionality of geographically restricting mobile registration. Older systems without a Codeks Virtual Controller license will continue to operate as before.

NOTE

The new functionality of the Codeks Virtual Controller license is only possible when using at least the version Codeks 10.2110.0.15840 of the main software or later.


Each Codeks Virtual Controller license replaces one physical T&A device. Each license allows you to specify one virtual controller i.e. determine the geographical coordinates of its position and the area of the greatest distance from these coordinates, where employees are still allowed mobile registration.

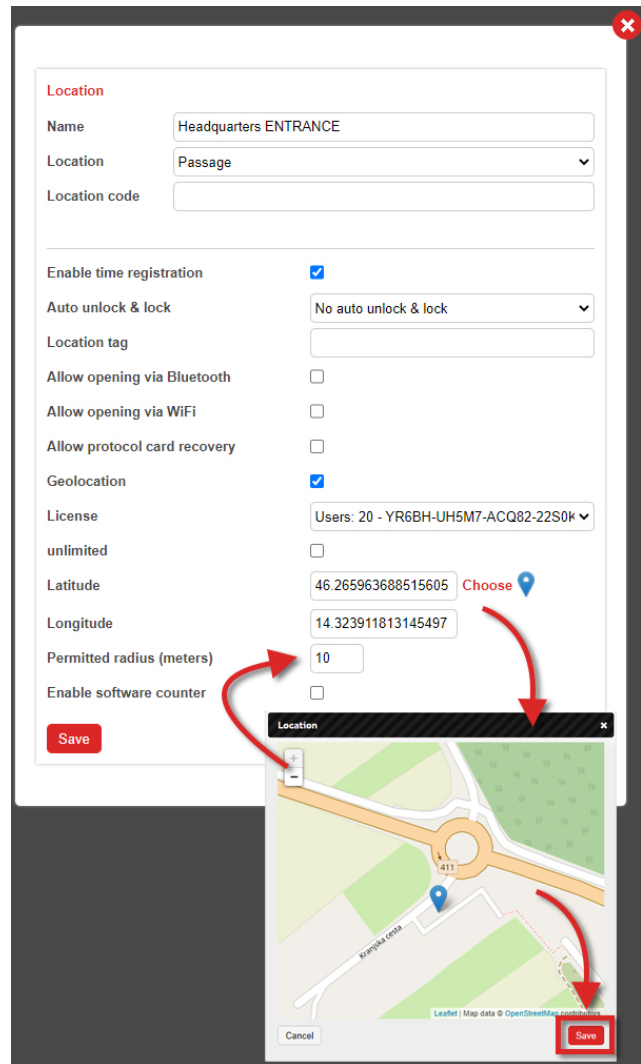
You can also leave the virtual controller geographically unrestricted, allowing employees mobile registration anywhere.

Each virtual controller location requires its own Codeks Virtual Controller license (e.g., to set up a system with 3 virtual controllers, you must purchase 3 Codeks Virtual Controller licenses). Additionally, each Codeks Virtual Controller license is limited by the number of employees who can register at each virtual location. Codeks Virtual Controller licenses are available for up to 40 users, up to 300 users, and unlimited users.

To activate the functionality of the virtual controller, it is **necessary to assign a Codeks Virtual Controller license to the selected location** in the *Hardware editor* and **adjust the location settings accordingly**.

- 1 In the *Hardware editor*, **create a new Passage location for the virtual controller, or use an existing location** (to which no device has yet been assigned) and *open the window to edit the location settings*.
- 2 **Enable the Geolocation setting.**
New location settings will open.
- 3 First, select the *Codeks Virtual Controller* license for this location from the **License** settings drop-down list.

- 4 * If you enable the **Unlimited** setting, the virtual controller will not have specific geographical coordinates and the area where employees are allowed to register mobile will not be restricted - employees will be able to register mobile anywhere.
- 5 **To limit the virtual controller area enter the geographical coordinates to which you want to bind the controller in the *Latitude* and *Longitude* settings fields.** You can also set the coordinates with the graphic selector by clicking the **Choose** button **Choose** .
- 6 Then set the **Permitted radius (meters)** from the selected geographical coordinates, where users will still be allowed to register their T&A. The minimum possible distance is 10 m.
- 7 Finally, click **Save**.
- 8 A new virtual controller with a virtual reader already connected to the newly added location will appear in the hardware list.

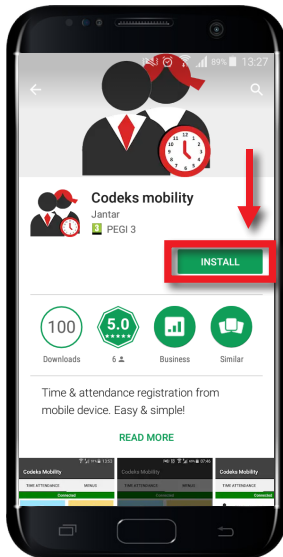


After editing the settings of the new location for the virtual controller, you must also edit the **rights of the user groups at the new location of the virtual controller** in the *Groups* editor and finally also **send tables**.

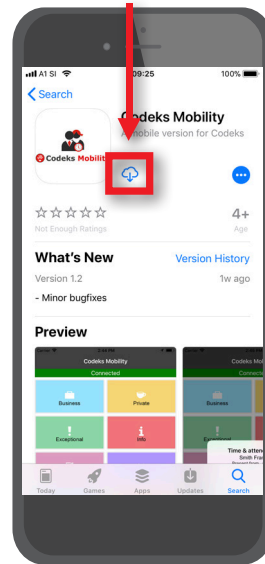
You can also read more about the Codeks Virtual Controller in the separate instruction manual for the add-on (**Codeks Virtual Controller EN Instructions for ADMINISTRATORS.pdf**).

* INSTALLING THE CODEKS MOBILITY MOBILE APPLICATION

You can download the free *Codeks Mobility* application to your Android device from **Google Play**.



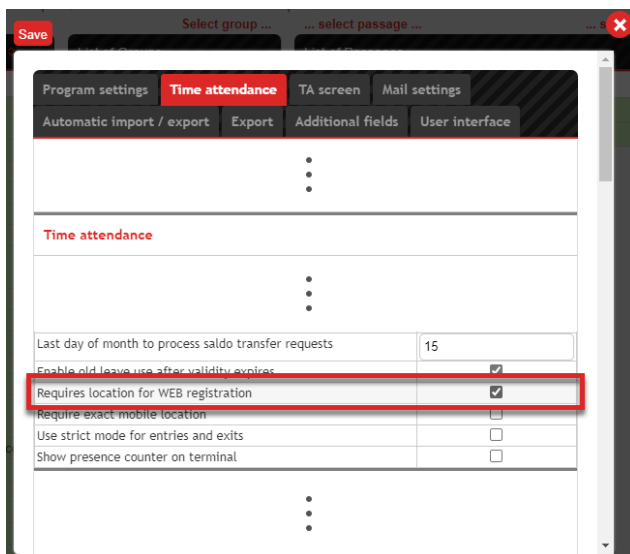
You can download the free *Codeks Mobility* application to your iOS device from **App Store**.



You can read more about the installation of the Codeks Mobility mobile application in the instruction manual for users of the Codeks Mobility ([Codeks Mobility-en.pdf](#)).

* ADDITIONAL SETTINGS FOR WEB TIME ATTENDANCE REGISTRATION

Additionally, you can enable the ***Requires location for WEB registration*** setting in the *Time attendance* tab in the *Settings -> Preferences* editor.



This setting specifies that **all users who will register their work hours through a web browser (the T&A controller simulator) will first have to select an appropriate physical location.** Depending on the selected location **a specific T&A timetable will be activated for the employee.**

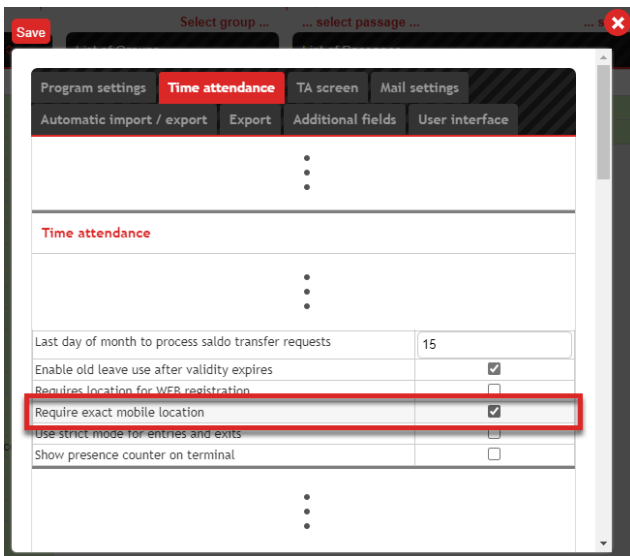
Such a configuration of the web T&A registration is especially useful in cases where employees regularly periodically move between locations that have different working hours (e.g. different branches).

NOTE

If you enable the *Requires location for WEB* setting, then the employee's timetable assigned to the selected location is activated when registering the users' work hours, and not the group's default timetable.

* ADDITIONAL SETTINGS FOR MOBILE TIME ATTENDANCE REGISTRATION

Additionally, you can enable the **Require exact mobile location** setting in the *Time attendance* tab in the *Settings -> Preferences* editor.



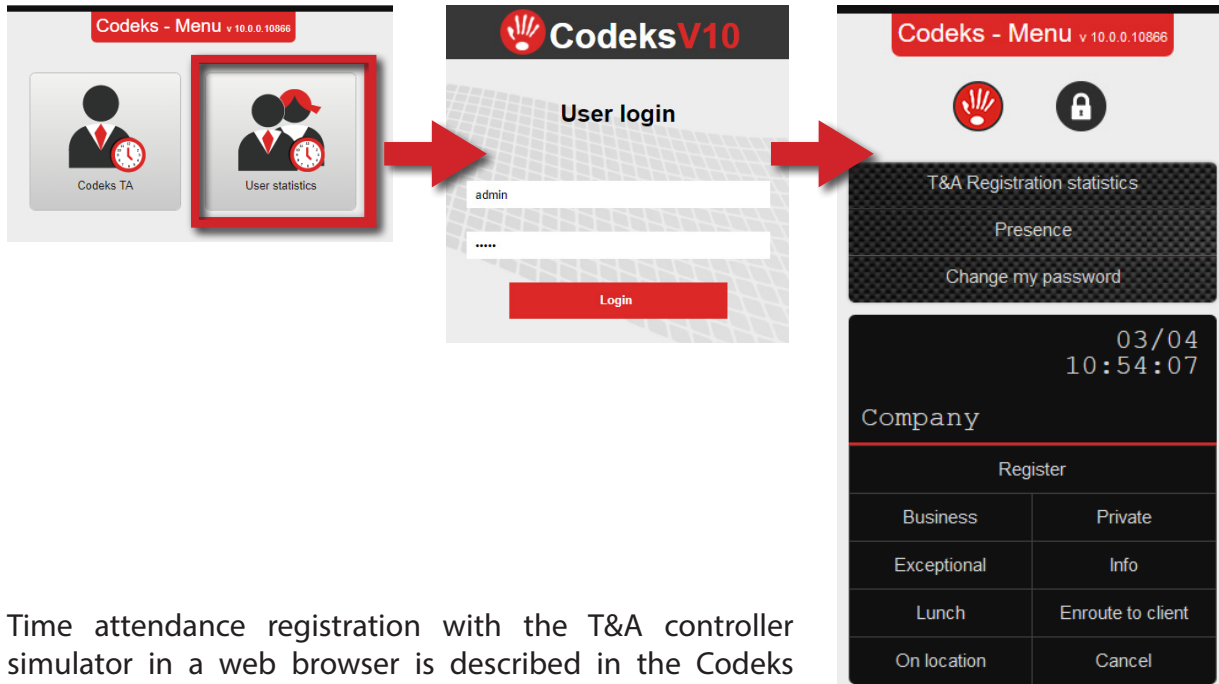
This setting specifies **that employees who register their work hours via the mobile app will also record their exact geographical location when registering their time attendance events.** Employees will thus have to enable location services on their mobile devices, as the registration of work hours is only possible if the location information is also available.

Such a configuration of mobile T&A registration is useful especially in cases when you need information about the location of the employee or you want to track the employees' travel.

REGISTERING TIME ATTENDANCE VIA A WEB BROWSER AND THE MOBILE APPLICATION

T&A registration via a web browser

Users who have an additional virtual card assigned to them in the Codeks system can register time attendance events via a web browser using the time registration controller simulator located at the bottom of the user access menu.



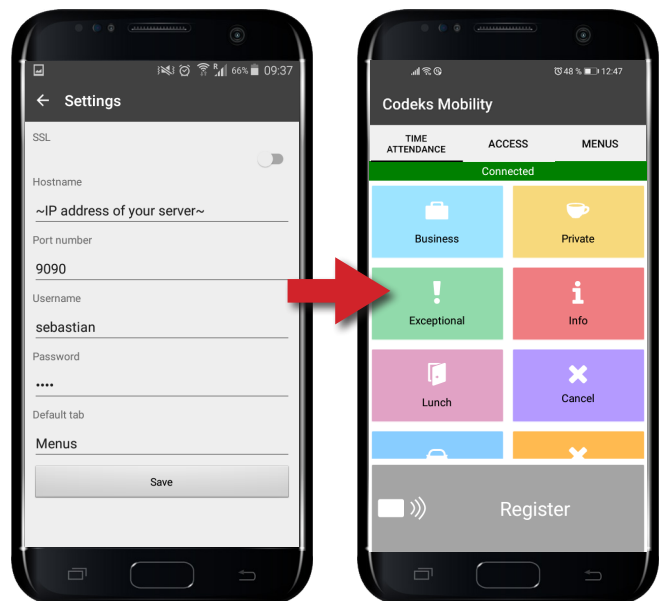
Time attendance registration with the T&A controller simulator in a web browser is described in the Codeks manual for users ([Manual for users-en.pdf](#)).

T&A registration via the mobile application

When launching the Codeks Mobility application for the first time, users will be required to enter their user login information into the application. For all subsequent launches of the application, the login will be automatic.

The **time registration controller simulator**, which allows users to register via the app on their mobile device, is located under the *Time attendance* tab.

You can read more about the time attendance registration via the Codeks Mobility mobile application in the instruction manual for users of Codeks Mobility ([Codeks Mobility-en.pdf](#)).



4 ADDITIONAL AND ADVANCED SETTINGS FOR THE USE OF THE CODEKS VIRTUAL CARD ADDITIONAL LICENSE CODE

SETTINGS FOR MULTIPLE EMPLOYEE REGISTRATION ON A SINGLE MOBILE DEVICE

Using the **NFC technology (Near Field Communication)** of mobile devices the Codeks Mobility application also **allows multiple users to register on the same mobile device with their contactless cards.**

NOTE

Time registration for multiple employees on the same mobile device is currently only available for Android devices. To date, iOS mobile devices do not allow NFC card reading.

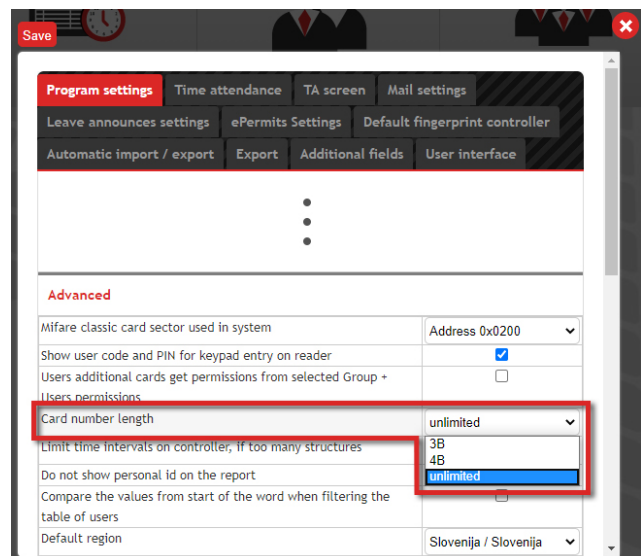
NOTE

Multiple user registration on the same mobile device is only possible with MIFARE (13.56MHz) cards. All users must be assigned MIFARE cards, either as the main user card or an additional card.

To enable this system to operate correctly, a specific combination of settings must be set. The necessary settings are listed below:

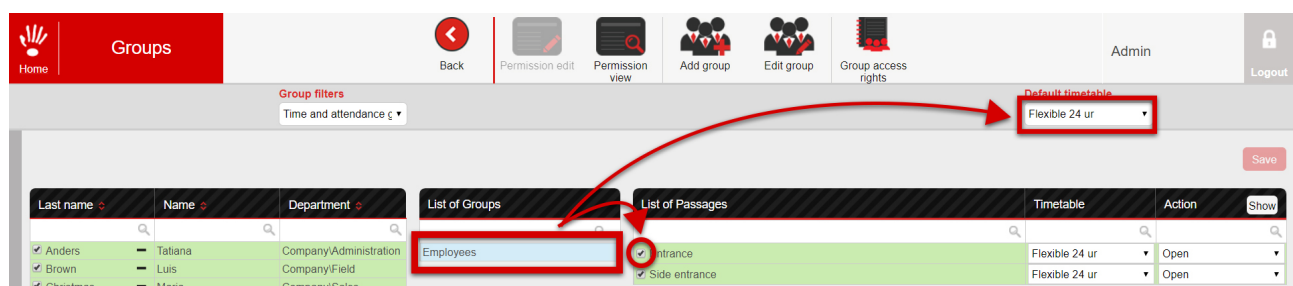
Card length settings

The NFC readers in mobile devices can only read the entire ID number of a MIFARE card. This means that you need to set the **Card number length** setting to **Unlimited** value in the **Program settings** tab of the *Preferences* editor.



Assigning groups and default timetables

All the involved users (employees and heads of departments) **must have at least one T&A passage enabled for their T&A groups as well as an assigned default timetable.**



Settings for heads of departments

Employees register on the mobile device through their head of department's user login into the mobile application this is why the heads of department must be assigned the following settings:

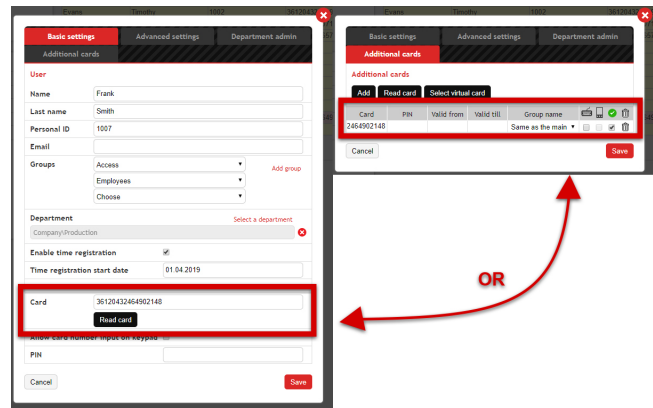
- a **An assigned username and password** in the *Advanced settings* tab of their user's settings in the *Users* editor.
- b The **View time and attendance** setting in the *Department admin* tab of their user's settings must be enabled in the *Users* editor.
- c **A virtual card must be assigned to the manager** in the *Additional cards* tab of their user's settings in the *Users* editor.

Card	PIN	Valid from	Valid till	Group name			
131247				Same as the main	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Settings for employees

- a **Employees**, who will register their T&A hours on the mobile device of a specific department manager, **must be assigned to appropriate departments**. Users can only register their hours through a particular department manager if the manager has admin rights enabled for the corresponding department.

- b Multiple user registration on the same mobile device is only possible with MIFARE (13.56MHz) cards.** All users must be assigned MIFARE cards, either as the main user card or an additional card.



Multiple employee registration on a single mobile device

When Codeks Mobility is launched for the first time, the heads of departments will be required to enter their user login information into the application, however, login for all subsequent launches of the application will be automatic.

Heads of departments will need to **enable NFC functionality** on their mobile devices before users can register on their devices.

All employees register on the head of department's mobile device **using the time registration controller simulator** in the *Time attendance* tab.

You can read more about multiple employee registration on a single device with the Codeks Mobility app in the user manual for the Codeks Mobility mobile app users ([Codeks Mobility-en.pdf](#)).



SETTINGS FOR TIME REGISTRATION AT LOCATIONS WITH ASSIGNED LOCATION TAGS

Using the **NFC technology** (Near Field Communication) of mobile devices the **Codeks Mobility application also enables time&attendance registration at specific locations where contactless cards are installed.** This functionality is particularly useful for patrols or security guards who have to do regular rounds to various locations of the company premises. For such use, the **user** (patrol) who will register at these locations **must have a virtual card assigned.** Similarly to classic mobile time attendance registration, all users register using the simulated T&A controller in the Time attendance tab of the mobile application.

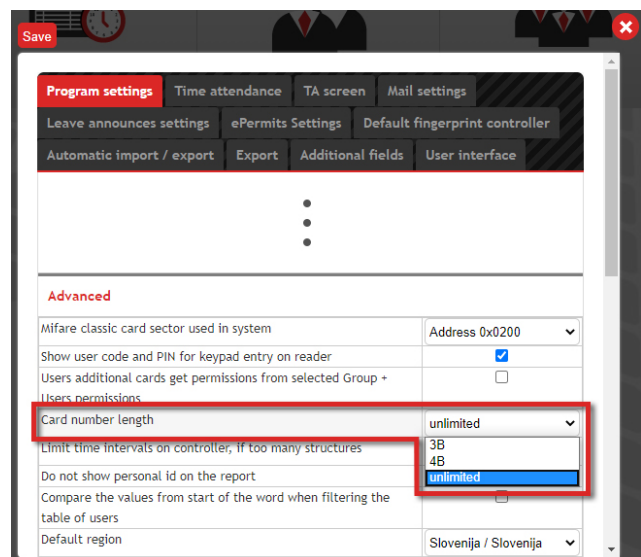
NOTE

This function is only available on Android devices. To date, the iOS mobile devices do not allow NFC card reading.

For such a system to work properly, a very specific combination of settings must be set. The procedure for setting all the necessary settings is described below:

Card length settings

The NFC readers in mobile devices can only read the entire ID number of a MIFARE card. This means that you need to set the Card number length setting to **Unlimited** value in the **Program settings tab** of the *Preferences* editor.

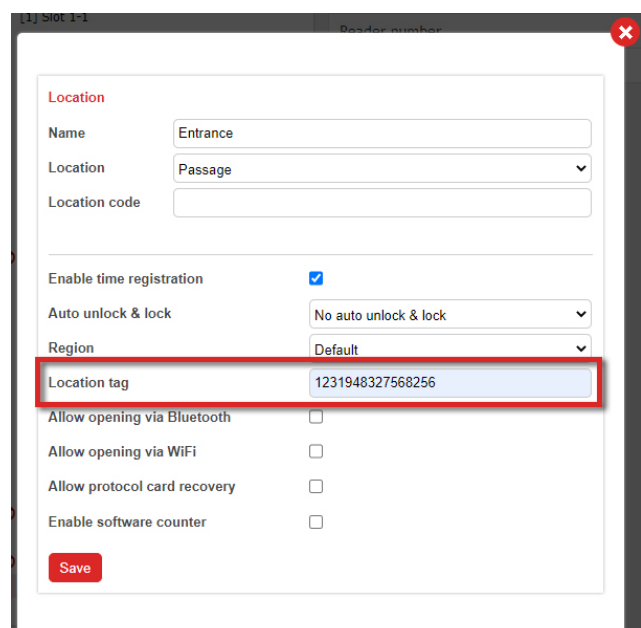


Tag (card) at location

At each passage where users will be able to register, **you must enter the number of the card that will be installed at the location under the *Location tag* setting.**

NOTE

User registration at locations with location tags is only possible with MIFARE (13.56MHz) cards. The specified locations must, thus, be equipped with MIFARE cards.



Assigning user access and a virtual card to users (patrolling personnel)

NOTE

To assign virtual cards to users, you need to purchase the Codeks Virtual Card license.

Employees register using the time&attendance controller simulator in the Codeks Mobility app on their mobile device and must, thus, be assigned the following settings:

- a **An assigned username and password** in the Advanced settings tab of their user's settings in the *Users* editor (in the **Advances settings** tab).
- b **A Virtual card must be assigned** to each user in the **Additional cards** tab of their user's settings in the *Users* editor.

Time attendance groups and timetables

In the *Groups* editor, all users (making rounds) **must be granted access rights and be assigned the appropriate time attendance timetable at all passages where the location tags (contactless cards) are installed.**

Last name	Name	Department	List of Groups	List of Passages	Timetable	Action	Show
<input checked="" type="checkbox"/> Acker	David	Field	Employee 2	<input checked="" type="checkbox"/> Company/1st floor/Entrance	Fixed	Open	
<input checked="" type="checkbox"/> Anders	Tamara	Administration	Employees	<input checked="" type="checkbox"/> Company/1st floor/Exit	Fixed	Open	
<input type="checkbox"/> Brown	Luis	Field					

T&A registration at a location equipped with an NFC tag

When Codeks Mobility is launched for the first time, the users (making patrols) will be required to enter their user login information into the application, however, login for all subsequent launches of the application will be automatic.

The **T&A controller simulator**, which allows users to register via an app on their mobile device, is located under the *Time attendance* tab. Before users can register they will need to **enable the NFC functionality** on their mobile devices.

To register an event at a location with an assigned tag, the employee simply brings their mobile device closer to the tag installed at the location.

You can read more about users time registration at a location with an assigned tag in the user manual for the Codeks Mobility mobile app users ([Codeks Mobility-en.pdf](#)).



5 SETTINGS FOR OPENING DOORS

The Codeks Mobility mobile application, **from version Codeks Mobility 3.1.4 for Android and Codeks Mobility 1.8 for iOS devices**, now also includes tools **for opening doors via a Bluetooth or Wifi connection**.

NOTE

The new door opening functionality in the Codeks Mobility app can only be used simultaneously with the Codeks software versions Codeks 10.4.14.13794 or newer for T&A systems and Codeks 10.2103.0.15031 or newer for access control systems.

Older versions of the Codeks software do not yet support this functionality in Codeks Mobility. When using older versions of the Codeks application the new version of Codeks Mobility will work in the same way as before.

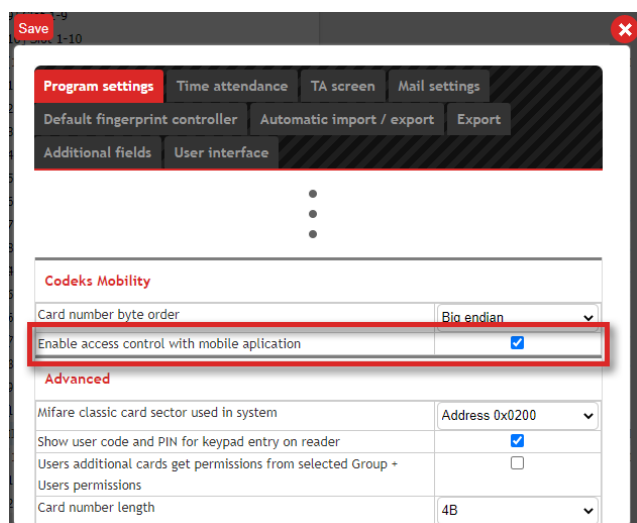


In Codeks systems, where this functionality is enabled, users who have an (additional) virtual card assigned can open doors and enter at locations using the Codeks Mobility mobile application.

GENERAL PROGRAM SETTINGS

You must first enable the option to open the door via the mobile application for all users in your system in the program settings of the Codeks application.

- 1 To turn on the option to open the door with a mobile application for all users in your Codeks system, select the Program settings tab in the Preferences menu and under the Codeks Mobility section enable the **Enable access control with mobile application** setting.
- 2 Click **Save**.



SETTINGS FOR LOCATIONS

In the *Hardware* editor you have to enable the option of opening door using a Bluetooth or Wifi connection with the Codeks Mobility app on all passages.

- 1 To enable the option of opening doors using a Bluetooth or Wifi connection at a specific passage, first, **find and double-click the selected passage**.
- 2 A new pop-up window will open where you can edit the passage settings. In the lower part of the window enable the **Allow opening via Bluetooth** or the **Allow opening via Wifi** setting and enter any other necessary settings.
- 3 Click **Save**.

Settings	Description
Allow opening via Bluetooth	If you enable this setting, employees will be able to open the door at this location via Bluetooth.
Bluetooth device identifier	Under this setting, always enter the prefix JantarBT followed by the device address (e.g., JantarBT123 if 123 is the device address). Always enter the address of the device on which the Bluetooth module is located (i.e., the address of the controller when the reader and the Bluetooth module are in the controller housing, or the address of the reader when the Bluetooth module is installed on a reader separate from the controller).
Bluetooth MAC address	Under this setting, copy the Bluetooth MAC address of the device (that is, the unique device identifier), which is written on the device label or on the packaging of the device.
Allow opening via WiFi	If you enable this setting, employees will be able to open doors at this location via a WiFi connection.
List of allowed SSIDs	Under this setting, enter the names of the wireless networks (SSIDs) through which users will be able to open the door at this location. You can specify multiple networks, separating them by commas.

SETTINGS FOR HARDWARE

In the *Hardware* editor you have to enable the option of opening door using a Bluetooth or Wifi connection with the Codeks Mobility app on all passages.

NOTE

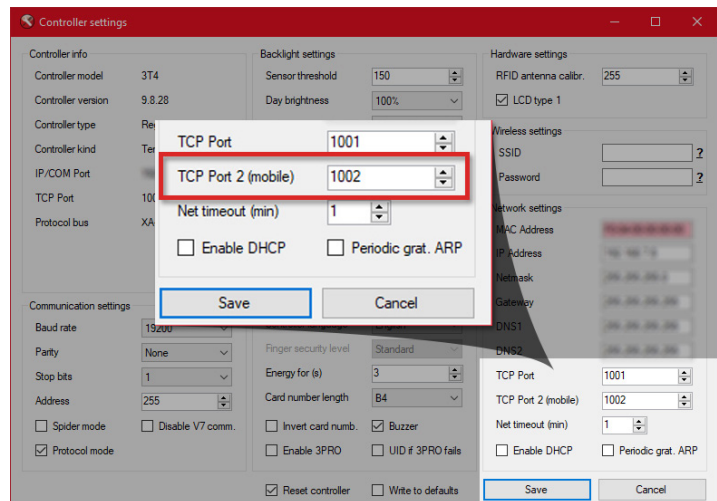
It is only possible to open passages via Wifi through readers linked to controllers that are directly connected to the local area network (LAN).

NOTE

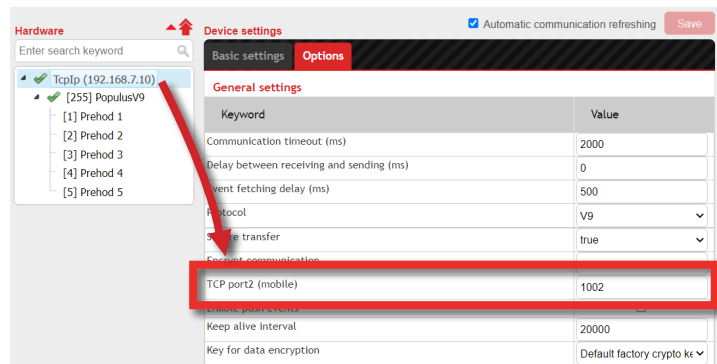
It is only possible to open passages via Bluetooth if they are equipped with the new H-line or A-line controllers (for apartments and hotels) which already contain a Bluetooth module.

NOTE

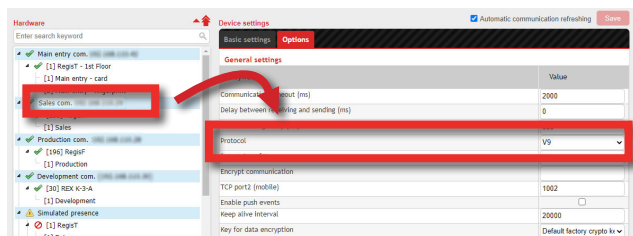
The controllers through which users will be able to open the door with the mobile application need Codeks Tools hardware programs to continue the communication port (ports) for mobile communication. In the controller settings, the *TCP Port 2 (mobile)* setting is required. Continue with the parallel port (port), e.g. 1002.



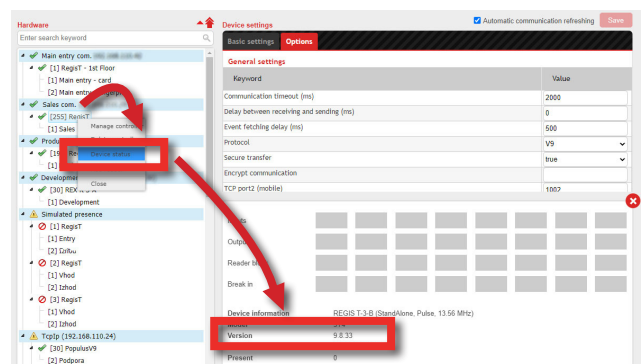
The selected port number for mobile communication must also be set on the communication line leading to the controller in the Codeks application. In the communication line settings, in the *Options* tab under the *TCP port2 (mobile)* setting, enter the same port number as on the controller, e.g. 1002.



Communication lines to controllers must have the **communication protocol set to V9**.



Controllers on which users will be able to open doors with the mobile app must have **at least the firmware version 9.8.0 or newer**.



SETTINGS FOR USERS

In order to be able to open doors using the Codeks Mobility mobile app, all such users must be assigned a user name and password as well as a Virtual Card in the *Users* editor.

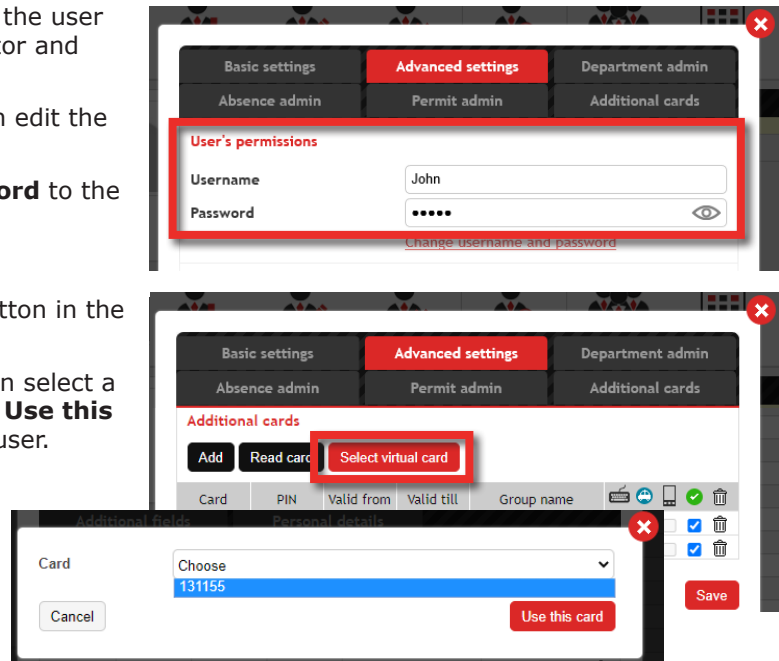
NOTE

To assign virtual cards to users, you need to purchase the Codeks Virtual Card license. A virtual card must be assigned to each user by a Codeks system administrator in the *Users* editor.

NOTE

Users who are assigned a Virtual card will be able to open doors using their Codeks Mobility mobile app at all passages where they are granted access rights to (through group rights or user exceptions).

- 1 To edit the user's settings, first, select the user on the *list of all users* in the *Users* editor and **double-click them**.
- 2 A new window will open where you can edit the user's settings.
- 3 First, assign a **username and password** to the user in the *Advanced settings* tab.
- 4 Next, click the **Select virtual card** button in the *Additional cards* tab.
- 5 A new window will open, where you can select a virtual card number and then click the **Use this card** button to assign the card to the user.
- 6 Click **Save**.



USING THE CODEKS MOBILITY TO OPEN DOORS

NOTE

Users can open doors with the mobile app via a Wifi connection only when they are located within the local network or if they are provided with a direct connection to the local Codeks network.

NOTE

Users can only open doors using the Codeks Mobility app via Bluetooth when they also have their location (location services) enabled on their mobile devices.

NOTE

Before trying to open doors using the Codeks Mobility app make sure your Wifi or Bluetooth options on your mobile device are turned on.

The links for opening doors are located under the **Access** tab in the Codeks Mobility app.

To open the door at a selected location simply **click the button with the name of the location**.



If you are **using a custom V9 encryption key** for the communication between the controllers and the Codeks server it is **essential to maintain an active connection with the Codeks server** when using the Codeks Mobility app to open doors.

Your custom encryption key is not stored in the database of your mobile device for security reasons, instead, the encryption key is provided by the Codeks Service, which runs on the server, every time the command for opening doors is executed.

You can read more about custom V9 encryption keys in the documentation of the main Codeks application.

6 SSL CERTIFICATES

SSL certificates are used to protect the transfer of data between clients, i.e. users who access the Codeks application through browsers on their computers, and the Codeks software server.

The main advantage of using the *HTTPS (HyperText Transfer Protocol Secure)* communication is the encryption of data transferred between the client and server. The use of SSL (Secure Sockets Layer) certificates guarantees that the user is truly communicating with your server and that all the data sent is protected against unauthorized viewing.

When establishing HTTPS communication, the data exchange between your server and the user's (client's) computer is encrypted with an encryption key stored in an SSL certificate. Such encrypted data is unreadable without the decryption key, which only the server knows.

Codeks software also allows HTTPS communication using SSL certificates. To use an SSL certificate in Codeks software, you must:

- 1. Obtain a domain name for Codeks software on your server;**
You need to obtain a domain for your Codeks server, which will later be used to issue an SSL certificate for your Codeks server (we suggest you use a subdomain of your website). Obtain a domain for your Codeks server from your domain registrar (often also your web host provider), and then edit the DNS server settings so that the selected domain points to the entry point of your local network (router) where the Codeks software.
- 2. Obtain an SSL certificate for the domain on the server where the Codeks software is running;**
Codeks software allows you to use any paid SSL certificate, as well as free SSL certificates created with Let's Encrypt (<https://letsencrypt.org/>).
- 3. Import the certificate to the Codeks software server;**
The obtained SSL certificate must be imported (installed) on the Codeks server.
- 4. Configure the firewall settings at the entry point of your local network accordingly (router);**
You must allow access through the firewall of the entry point (router) of your local system, which allows external queries to access the server where the Codeks software is running within the local network.
- 5. Configure the firewall settings on the Codeks software server accordingly;**
You must allow access through the server's firewall, where the Codeks software is running, which allows external queries to access the Codeks application on the server.
- 6. Turn on HTTPS communication and edit HTTPS communication settings in the Codeks software;**
You need to enable the use of the installed SSL certificate in the Codeks software and edit some additional settings in order for the Codeks software to work properly.

You can read more about SSL certificates for the Codeks software in the documentation of the main Codeks application ([CodeksManual-en_V10.pdf](#)).



Jantar d. o. o., elektronski sistemi

Kranjska cesta 24, 4202 Naklo, SLOVENIJA

T: +386 (0)4 277 18 12, +386 (0)4 277 18 09 | **E:** sales@jantar.si

www.jantar.si