EN

OPERATION MANUAL

Bluetooth

Revision 1, 30.10.2025

min. reader firmware 1.6.240

min. control unit firmware 1.0.94

min. application version v1.0.5 (Inosmart Plus)

Dear User,

Thank you for choosing to purchase a fingerprint reader that will allow you to enter your home or business quickly and easily. Your reader can be used to open the door using a fingerprint, Authentication device or numeric code (keyboard reader model).

Although our readers are easy to use, please take a few minutes to read the instructions below. We have prepared all the information you need to pay attention to both for the first time and for subsequent use. For easier understanding, you can also visit our website www.inosmart.info/bt and watch the attached video content about the operation and use of the fingerprint reader.

The instructions are uniform for all modules: BT 600, BT 610, BT 620, BT 630, BT 640, BT 660 and BT 670.

We wish you pleasant and simple use.

TABLE OF CONTENTS

GLOSSARY 5

INOSMART BIOMETRIC MODULES (READERS) - FUNCTIONS 6

FIRST USE 8

REGISTRATION OF ADMINISTRATORY FINGERPRINTS 8

REPLACEMENT OF ADMINISTRATOR FINGERPRINTS 9

READER – CONTROL 9

CONTROL VIA THE CONTROL UNIT 10

ADD FINGERPRINT OF A NEW USER 10

ADD NEW CODE NUMBERS (MODULES BT 600, BT 610, BT630, BT660 AND BT 670) 11

REMOVE USER, SMARTPHONE OR CODE NUMBERS 12

RESET TO FACTORY DEFAULTS 12

READER – SECURITY LOCK 12

CONTROL VIA A SMARTPHONE 13

ESTABLISH FIRST CONNECTION BETWEEN READER AND SMARTPHONE 14

HELP WITH THE FIRST TIME CONNECTION OF READER AND SMARTPHONE 16

MENUS 17

USERS 18

REMOVE USER 19

TEMPORARILY DISABLE / ENABLE USER 20

ADD NEW FINGERPRINT 21

ADD NEW CODE NUMBERS (modules BT 600, BT 610, BT630, BT660 and BT 670) 22

TIMER 23

FREE ENTRANCE 24

SETTINGS 25

EVENT HISTORY 26

FINGERPRINT VERIFICATION 27

THE MOST COMMON REASONS FOR POOR FINGERPRINT RECOGNITION 27

ADJUSTING THE SENSITIVITY OF FINGERPRINT RECOGNITION 28

DOOR OPENING VIA BLUETOOTH CONNECTION 29

PHONE REGISTRATION TO UNLOCK VIA BLUETOOTH CONNECTION 30

BT DEMO MODE 31
SECOND RELAY 32
CONECTION WITH AN ADDITIONAL TELEPHONE 33
PAIR READER WITH RADIO BELL 34
CARE AND MAINTENANCE 35
ERROR MESSAGES 35
RESET TO FACTORY SETTINGS 35
FAQ – FREQUENTLY QUESTIONS 36
INOSMART READER SPECIFICATIONS 38
CE - CERTIFICATE OF CONFORMITY 39
INSTALLATION DIAGRAM 40
USER INSTRUCTIONS 41
MANUFACTURER WARRANTY 42

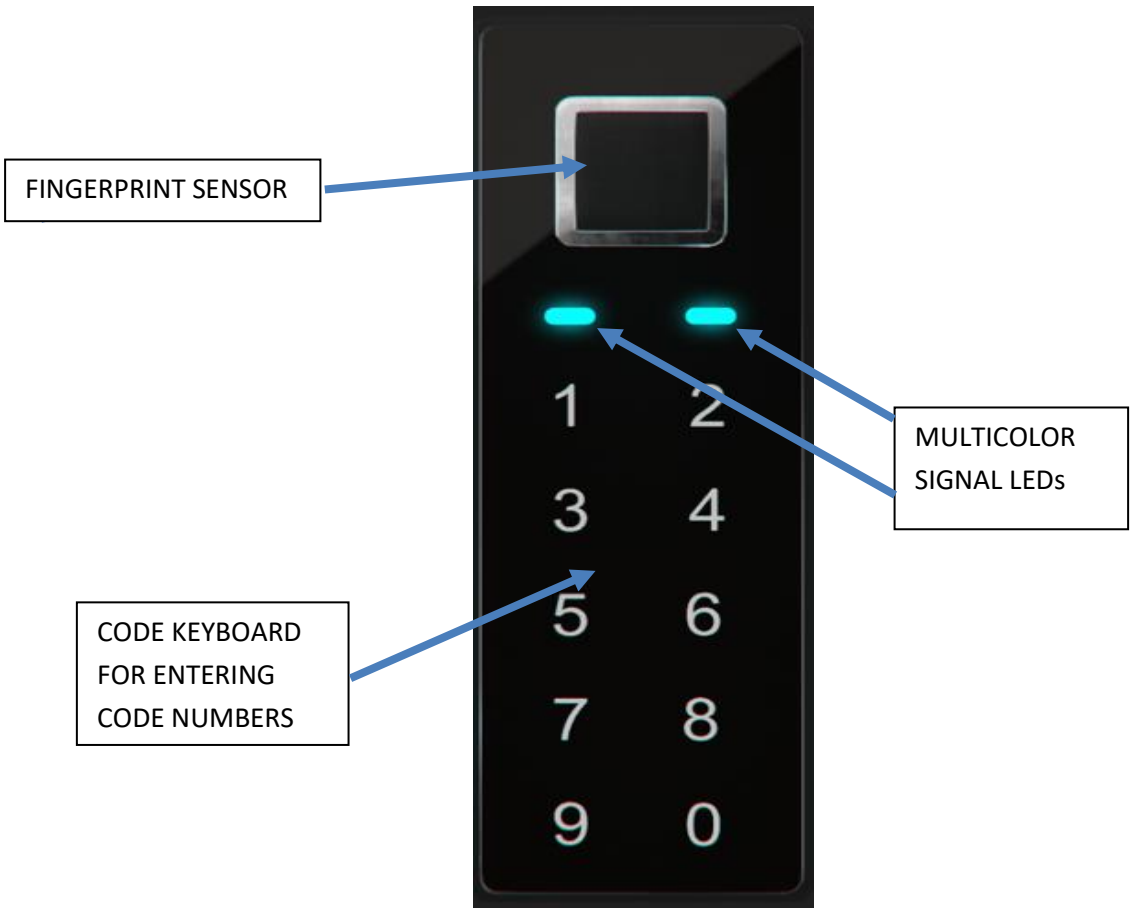
GLOSSARY

- **Bluetooth module –** Inosmart biometric module, a reader built into the outside of the sash or door handle. Allows you to open the door using your fingerprint, Authentication devices or keyboard.
- **Fingerprint sensor -** enables identification of your fingerprint. It is built into the reader.

- **Control unit -** enables el. communication between the sash, the door frame and the Inosmart reader. It is built into the side part of the door leaf.
- **LED –** light emitting diode. An electronic component that emits light.
- **Administrator fingerprint** – one of the 3 fingerprints you entered when using the reader for the first time.
- **Placing a finger** - the user places his finger on the fingerprint sensor built into the reader.
- **Relay -** is an electromagnetic switch that you turn on with the control voltage

INOSMART BIOMETRIC MODULES (READERS) - FUNCTIONS

BT 600, BT 630	BT 610, BT660 and BT670	BT 620, BT 640
		
• Fingerprint sensor • Keyboard • Bluetooth • Bell • Signal lights • Buzzer	• Fingerprint sensor • Keyboard • Bluetooth • Signal lights • Buzzer	• Fingerprint sensor • Bluetooth • Signal lights • Buzzer



CONTROL UNIT – FUNCTIONS

The fingerprint reader can be controlled using the buttons on the control unit installed in the door leaf.

<table>
<tr><td rowspan="6"> 
</td><td>KEY 1 (2 seconds)
Adding a new fingerprint, Authentication device or code number.</td></tr>
<tr><td>KEY 2 (2 seconds)
Removing a fingerprint, Authentication devices or code numbers.</td></tr>
<tr><td>KEYS 2 + 3 (2 seconds)
Registration of three administrator fingerprints. Without three registered administrator fingerprints, the unit cannot be put into operation. To enroll the three administrator fingerprints, press buttons 2 and 3 simultaneously.
If administrator fingerprints are already registered, pressing this key combination deletes them and registers the new fingerprints.</td></tr>
<tr><td>KEY 3 (2 seconds)
Activation of the Bluetooth connection.</td></tr>
<tr><td>KEYS 1 + 3 (2 – 4 seconds)
The LED on the control unit lights up purple and then by holding down buttons 1 or 3, the intensity of the lighting in the door is increased or decreased. The lighting adjustment mode is automatically turned off 30 seconds after the last press of button 1 or 3.</td></tr>
<tr><td>KEYS 1 + 2 (2 seconds)
A test of the entire Inosmart system is initiated. In the event of a malfunction of any of the functions, the control unit or reader will eventually turn on the error signaling (flashing red LED).</td></tr>
</table>

KEYS 1 + 2 + 3 (10 seconds)
The control unit is reset to the factory settings. All data will be deleted!

KEYS 2+3 (5 SECONDS)
By pressing the 2+3 keys, you initiate the deletion of already entered administrator fingerprints that you release with the existing administrator fingerprint.
The reader immediately requires the entry of 3 new administrator fingerprints, these are registered in the application under an undefined user.

The ADMINISTRATOR is responsible for managing the fingerprint reader. Up to three different fingerprints / persons can be determined on first use - e.g. B. a person with three fingerprints or three different people with one fingerprint each. At least two people are recommended for practicality and safety.

Unlike the other users, an administrator has full access to the reader and the control unit and can add new users, fingerprints, Authentication devices or code numbers and also remove them.

As long as the reader's memory is empty, anyone can register as an administrator with their fingerprints. An administrator should therefore be appointed immediately when the device is commissioned to prevent any misuse.

FIRST USE

	ADMINISTRATOR FINGERPRINT Before using the Inosmart **Bluetooth module** (reader) for the first time, one or more administrators must be specified. All subsequent changes, entries etc. require confirmation by the administrator.
	Before using the reader, **three administrator fingerprints** must be stored. This step is essential before the first use. Make sure the fingerprints are read correctly; the fingertip should cover at least 70% of the sensor.

The administrator has access to all security-related functions with his fingerprint. For this reason, at least two administrators are recommended.

REGISTRATION OF ADMINISTRATORY FINGERPRINTS

	PRESS **BUTTONS 2 AND 3** ON THE CONTROL UNIT AT THE SAME TIME (2 seconds)	The reader's two LEDs light up white.
	**READ THE FINDERPRINT OF THE RESPECTIVE ADMINISTRATOR THREE TIMES.** • Administrator 1: read in the fingerprint three times • Administrator 2: read in the fingerprint three times • Administrator 3: read the fingerprint three times	Make sure that the entire fingertip rests on the reader. The fingertip should cover at least 70% of the sensor.
	After the administrator fingerprints have been successfully stored, the two LEDs light up blue.	**THE READER IS READY TO OPERATE.**

REPLACEMENT OF ADMINISTRATOR FINGERPRINTS

	PRESS AT THE SAME TIME TO START REPLACEMENT **BUTTONS 2 and 3** ON THE CONTROL UNIT (2 seconds)	The reader beeps briefly and both LEDs flash green.
	To authorize the replacement of admin fingerprints, place one of the already registered admin fingerprints on the fingerprint sensor.	Admin fingerprint replacement is approved. The signal lights glow white.
	**PLACE EACH NEW ADMINISTRATOR FINGERPRINT THREE TIMES on the fingerprint sensor.** • administrator 1: fingerprint three times, • administrator 2: fingerprint three times, • administrator 3: fingerprint three times.	Make sure that the entire fingertip rests on the reader. The fingertip should cover at least 70% of the sensor.
	After the administrator fingerprints have been successfully stored, the two LEDs light up blue.	**THE READER IS READY TO OPERATE.**

You can also find a corresponding tutorial on our homepage **www.inosmart.info/bt.**

READER – CONTROL

The fingerprint reader can be controlled via the **control unit** or via the **Inosmart app** (smartphone).

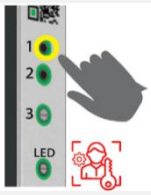
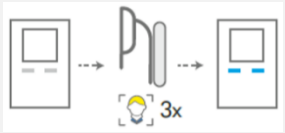
- Fingerprinst, Authentication devices or code numbers can be added and deleted via **the buttons** on the control unit.
- The **Inosmart app** enables central management of the device and all registered users - adding and removing users, Authentication devices or code numbers, creating timers and detailed management of other access authorizations.

The control unit does not allow controlling the lights, creating timers, naming users or managing access rights.

CONTROL VIA THE CONTROL UNIT

The **three buttons** on the control unit can be used to control the following main functions of the reader: adding or removing fingerprints, Authentication devices and code numbers (on models with a code pad).

ADD FINGERPRINT OF A NEW USER

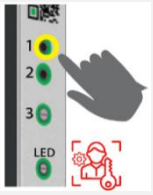
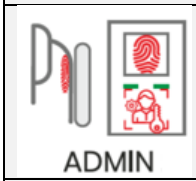
	PRESS **BUTTON 1** ON THE CONTROL UNIT (2 seconds)	The reader beeps briefly and both LEDs flash green.
	Put administrator's fingerprint on the sensor to authorize adding a new user's fingerprint.	A new fingerprint is approved. The LEDs light up white.
	Read the new user's fingerprint three times via the sensor. If this was successful, the LEDs light up green, otherwise red.	The reader beeps briefly and both LEDs light up green. **A NEW USER HAS BEEN ADDED SUCCESSFULLY.** The reader is ready for operation and both LEDs light up blue.

The skin, and thus also the fingertips, is subject to constant changes (different moisture content of the skin at different times of the year, injuries to the skin, etc.) and at the same time no two sensor operations are the same. For this reason, advanced sensors with 360° recognition are built into our fingerprint readers, which counteract these problems and correctly recognize every fingerprint at any angle.

Each time it is used, the reader compares the fingerprint with the one stored and also saves any new properties that have been identified. This means that individual fingerprint recognition is constantly improving over time. The system is able to store and automatically update up to 20 fingerprint variations for each individual user.

ADD NEW CODE NUMBERS (modules BT 600, BT 610, BT630, BT660 and BT 670)

The BT 600, BT 610, BT630, BT660 and BT 670 modules have a code keypad that can be used to open the door with a code number. The length of the code is pre-programmed at the factory to 4 digits. To add a new code number, please proceed as follows:

	**PRESS BUTTON 1** ON THE CONTROL UNIT (2 seconds)	The reader beeps briefly and both LEDs flash green.
	Place the administrator's fingerprint on the sensor to authorize the addition of a new numeric code.	A new code number is approved. The LEDs light up white.
	Enter the **four-digit code** number.	The reader beeps briefly and both LEDs light up green. **A NEW CODE NUMBER WAS SUCCESSFULLY ADDED.** The reader is ready for operation and both LEDs light up blue.

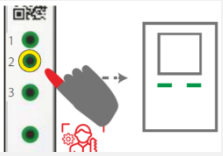
The length of the code number - from 4 to 10 digits - can be set via the Inosmart app.

If no code number was entered, the code keyboard is not functional, which is indicated by the LEDs and a beep. After entering the first code number, the keyboard is ready for use.

REMOVE USER, AUTHENTICATION DEVICES OR CODE NUMBERS

Removing a user, Authentication devices, or code numbers requires the appropriate user, Authentication devices, and code, and an administrator.

To remove, do the following:

	**PRESS BUTTON 2** ON THE CONTROL UNIT (2 seconds)	The reader beeps briefly and both LEDs flash green.
	Read the administrator's fingerprint via the sensor.	The deletion is approved.
	Do one of the following: ➢ read the user's fingerprint via the sensor, ➢ press the unlock button on your phone or ➢ Enter code numbers.	The reader beeps briefly and both LEDs light up green. **THE USER / AUTHENTICATION DEVICES/ CODE NUMBERS HAVE BEEN DELETED SUCCESSFULLY.** The reader is ready for operation and both LEDs light up blue.

RESET TO FACTORY DEFAULTS

On the control unit, press and hold all three buttons (1 + 2 + 3) for 10 seconds until you hear a beep. All users, fingerprints, smartphones and timers have been wiped and the reader has been factory reset.

READER – SECURITY LOCK

If a person has not been granted access seven times in a row with their fingerprint, Authentication devices or code numbers, the reader switches off automatically for 30 seconds. After this time, the reader is ready for operation again and switches off again for an additional 30 seconds - 1 minute - in the event of further unsuccessful access attempts. After each series of unsuccessful access attempts, the reader will turn itself off for an additional 30 seconds, up to a maximum of 5 minutes. With each successful access, the corresponding counter is reset to zero.

During this security lock, the reader is completely locked, which is indicated by the LEDs on the reader flashing alternately red and blue.

CONTROL VIA A SMARTPHONE

- Android

- iOS

The fingerprint reader can be controlled via a Bluetooth connection with the free Inosmart app. You can download the app for Android devices in the Google Play app store *https://play.google.com/store/apps/details?id=com.ismart.XF_InoSmart* or for Apple devices in the App Store (iOS) *https: http://apps.apple.com/us/app/inosmart/id1513984907*.
In order to successfully connect a smartphone to the reader, location and Bluetooth connectivity must be enabled (via your smartphone's settings).
If the smartphone is connected to the reader via the Bluetooth connection, it can be managed centrally via the app:

- Adding / removing users, code numbers or Authentication devices;
- Overview of all active users and their access rights;
- User management (rename, add/remove fingerprints, code numbers or Authentication devices);
- allocation of access rights to specific users;
- Creating timers and
- Management of additional functions (e.g. lighting, assignment of the secondary relay).

The range of the Bluetooth signal is limited for security reasons. For this reason, the smartphone should not be more than 1 m away from the control unit in the door and should be free of obstacles when performing administrator activities.

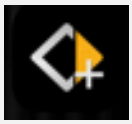
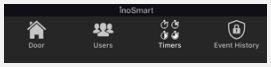
Android version 8.1 or later is required to manage the device. On iPhone devices, the inoSmart application works from iOS version 14. You can check the version in your phone settings. Get the latest version of the app by turning on automatic app updates on your phone. Door unlocking via iPhone is possible from iOS 14.

ESTABLISH FIRST CONNECTION BETWEEN READER AND SMARTPHONE

To activate the Bluetooth connection on the control unit, proceed as follows:

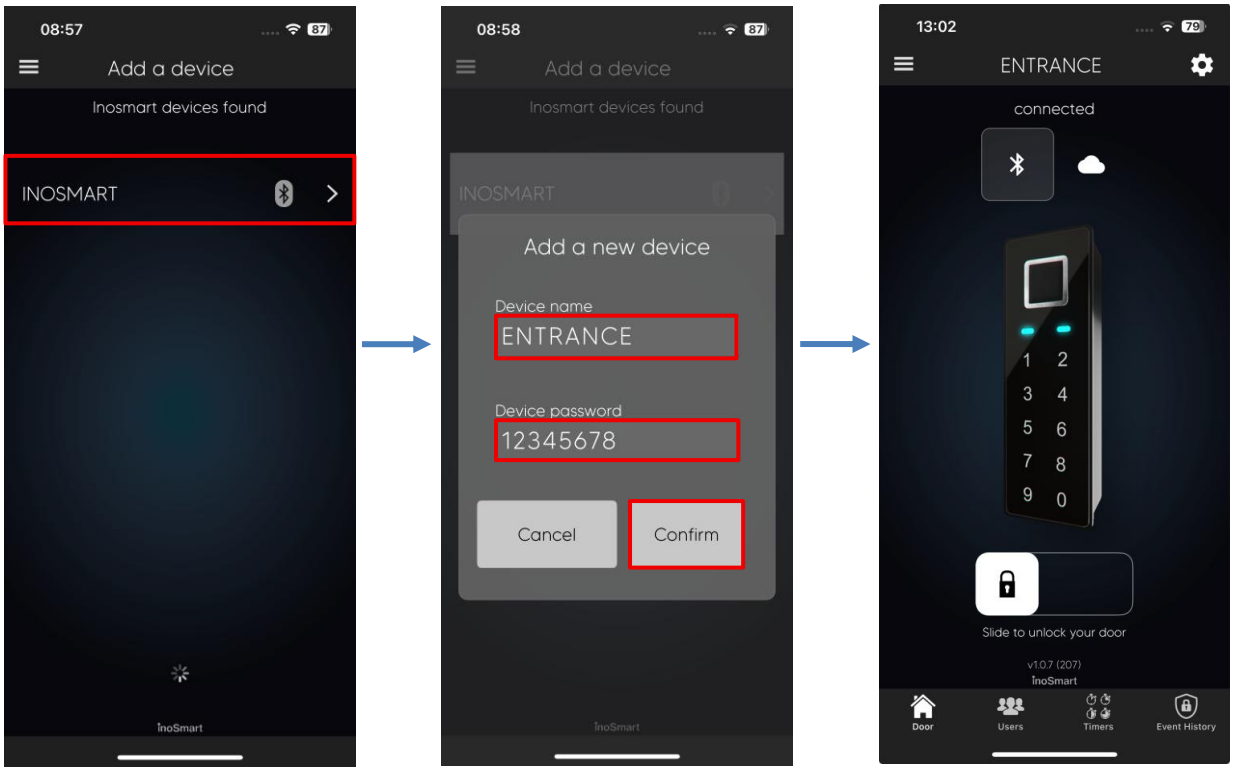
	**PRESS BUTTON 3** ON THE CONTROL UNIT (2 seconds)	The Bluetooth connection on the control unit is activated. The two LEDs on the control unit light up green.
	Read the administrator's fingerprint via the sensor.	The LEDs on the reader and the LED on the control unit light up blue. **BLUETOOTH MODEM IS ON.**

Download and install the free Inosmart app from the Google Play app store for Android devices or the App Store for iOS users and iPhone users.

 Enable location detection and Bluetooth connectivity on your smartphone.		
	Install the free Inosmart Plus app.	Once the installation is complete, the app is ready to use.
For security reasons, the range of the Bluetooth connection is limited, which is why the distance between the smartphone and the control unit should be as small as possible.		
	Welcome to your new app that allows you to centrally manage your reader.	Select "Reader settings and administration" in the app.
	CHOOSE YOUR DESIRED READER. When we open the Inosmart Plus app, the application automatically searches for available readers.	The app connects to the fingerprint reader. When using it for the first time, name it and enter an 8-10 digit password. The reader is now added to the list and can be connected to the smartphone.
	PAIRING THE READER WITH THE SMARTPHONE CONFIRM the 6-digit random code.	For a secure coupling (Bluetooth connection) between the smartphone and fingerprint reader, it is necessary to establish a connection on the first attempt and to confirm the 6-digit random code. ATTENTION! For some Android devices, the desired pairing must first be approved before the random code can be confirmed. In this case, please pay attention to the corresponding notification at the top of the screen.
If the device is renamed, this is automatically saved and automatically displayed each time the app is started.		
	QUICK MENUS	The reader can be easily managed via the four submenus.

The Bluetooth connection of the control unit switches off automatically after 10 minutes of inactivity.

Inosmart App Plus: **ADD NEW DEVICE**



1. After activating the Bluetooth module on the control unit, open the Inosmart Plus app.

2. The app will automatically detect the INOSMART network and offer it as an option.

3. After selecting the network, an input window will open:

• Enter the device name.

• If necessary, change the automatically generated password (it must be between 8 and 10 characters long).

4. Confirm your entry.

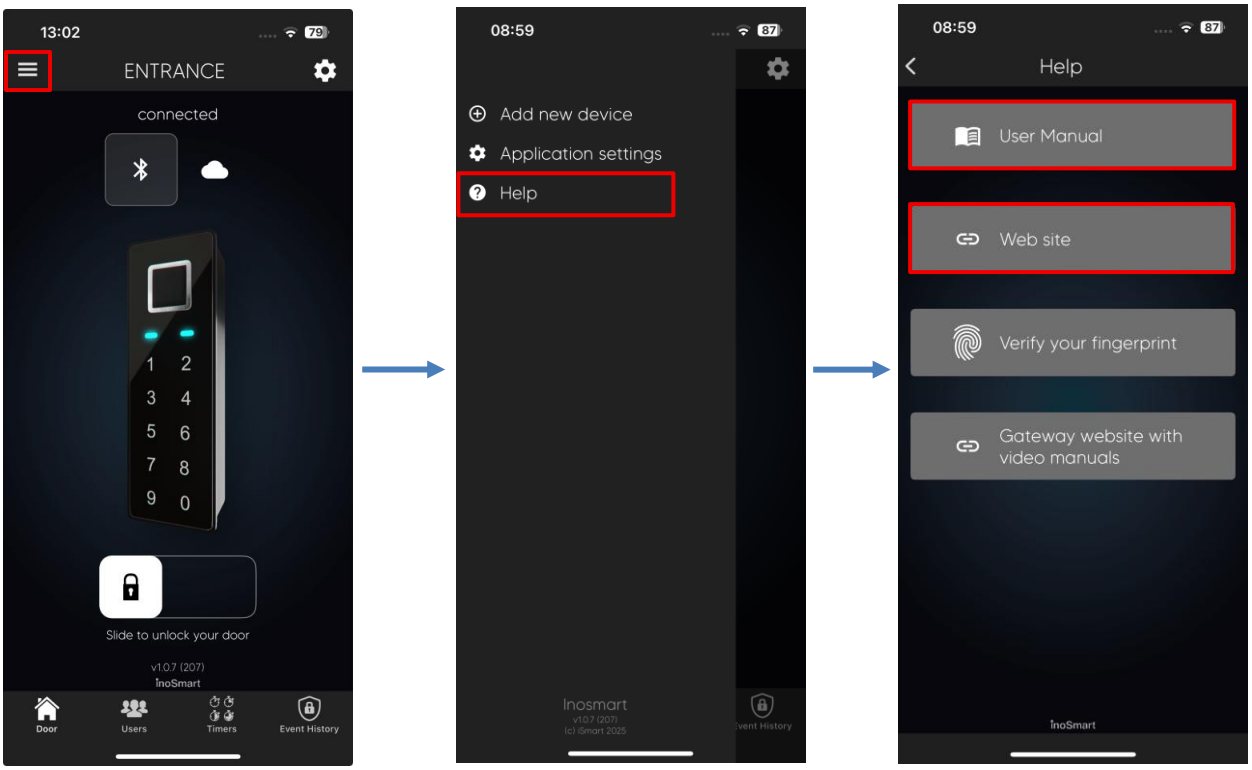
5. The app will then redirect you to the home screen, where the model installed in the door will be displayed.

HELP WITH THE FIRST TIME CONNECTION OF READER AND SMARTPHONE

If you experience connection problems, the main menu in the top left corner will help. Clicking it opens a Help window. You can find short video demonstrations or complete instructions there.

You can find more video content on our website: *https://www.inosmart.info/bt/en/*

Inosmart App Plus: **Help**



1. On the first screen, select "Main Menu."

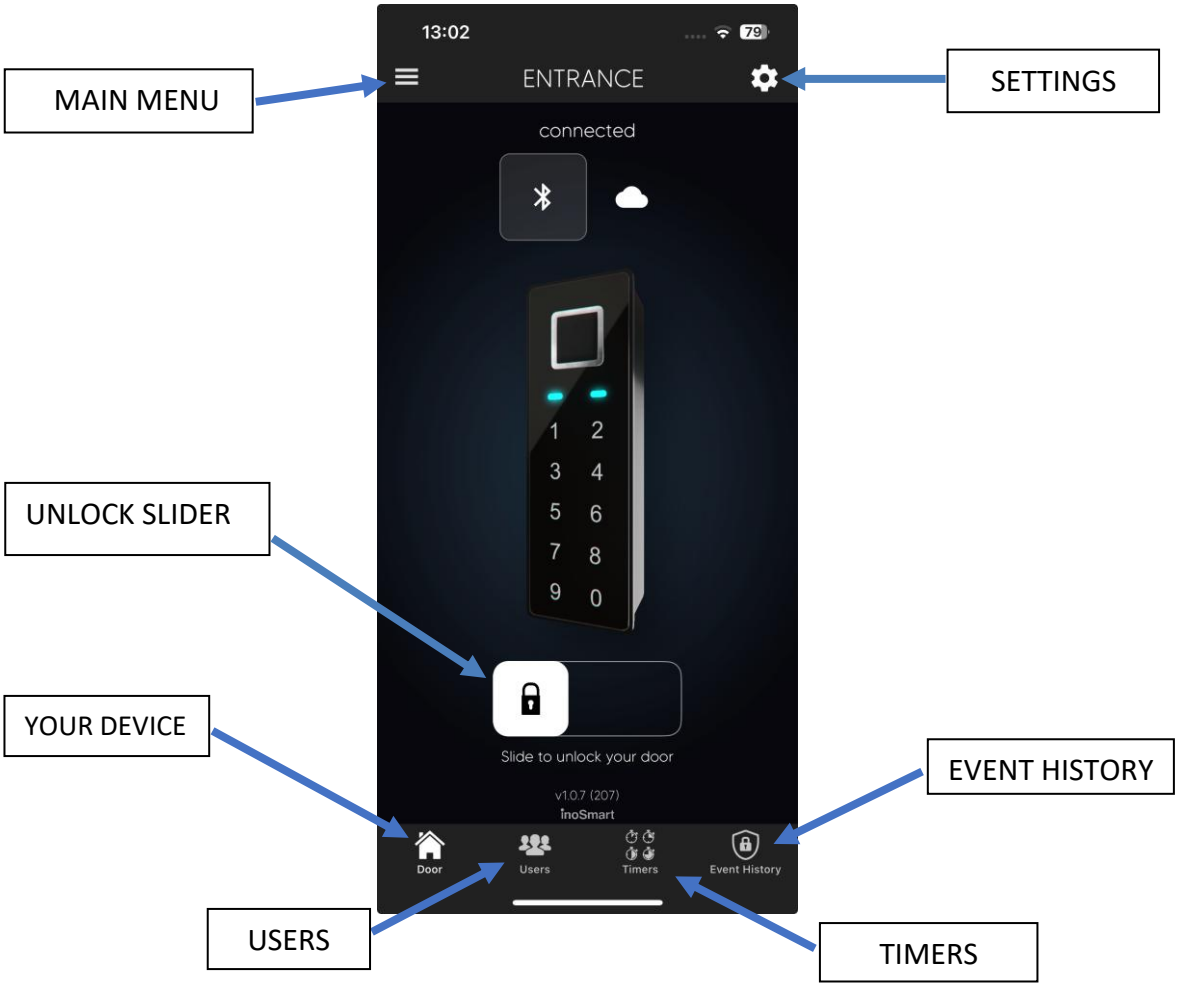
2. The general settings of the Inosmart Plus app will open.

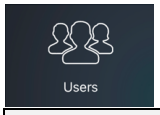
3. Select "Help."

4. A submenu will open containing a complete PDF manual and a link to a website with video content explaining various ways to use the Inosmart system.

MENUS

Inosmart app: **MENUS**

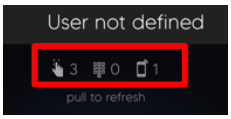




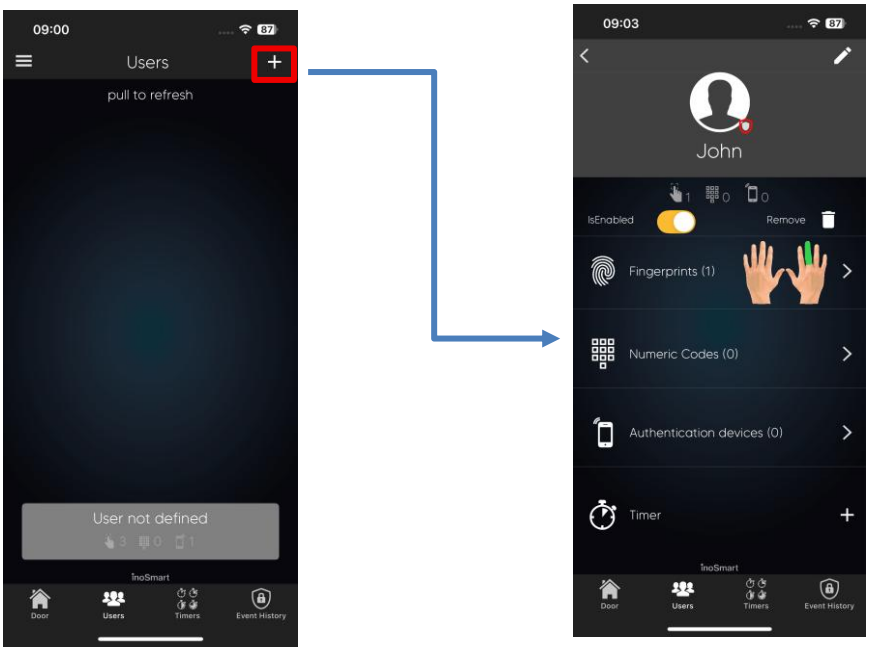
USERS

This sub-menu allows you to easily manage all users, their fingerprints, smartphones and code numbers. The directory shows all users with their permissions, with users who have access via the control unit appearing as unidentified users in the directory at the top.

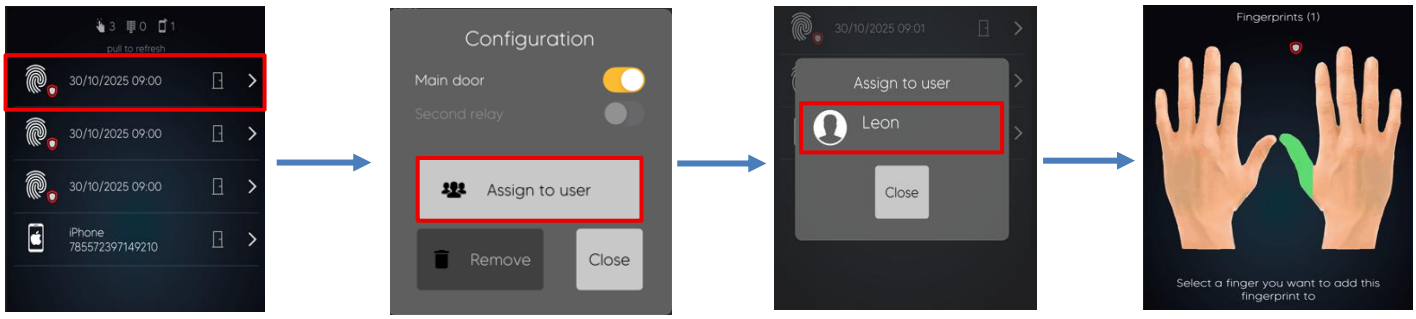
When logging in for the first time, all accesses that were added via the buttons of the control unit and for which no user is specified are recorded in the >>*User not defined*<< area.



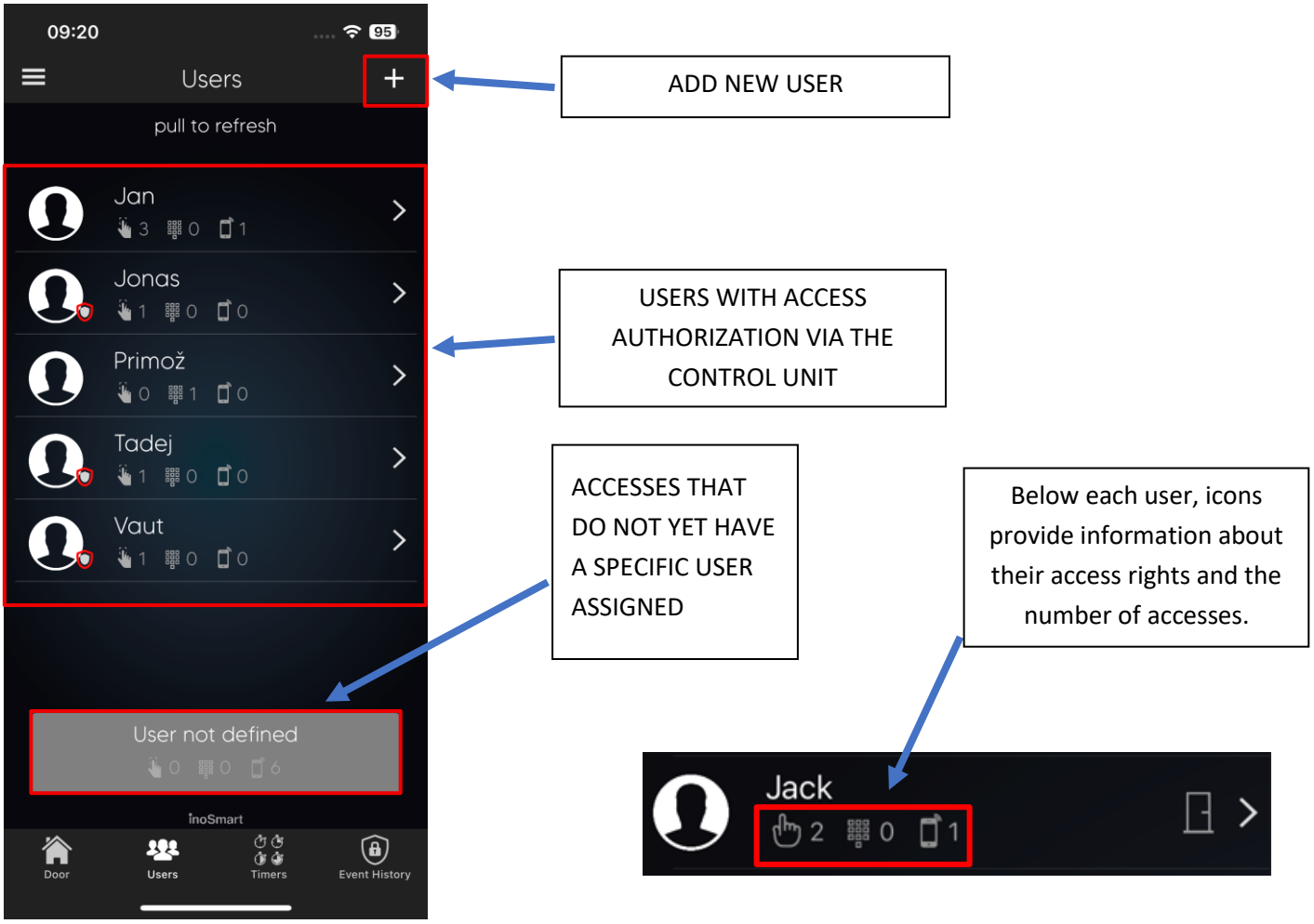
You ADD new users by clicking the **+** icon during registration. You can then assign any already logged unassigned authentications to the added users.



When you click ASSIGN TO USER, the application offers you all added users from the list. Select the desired person. In the case of assigning a fingerprint, the application offers you the option to select a finger. This way, when reviewing the user, you know which finger you have already added.



In the user list, enabled features are marked with an icon under each user. If you have enabled control unit button access, they will appear at the top of the list under Undefined User. On the right side each user is shown what opens the assigned authentication (door, second relay).



REMOVE USER

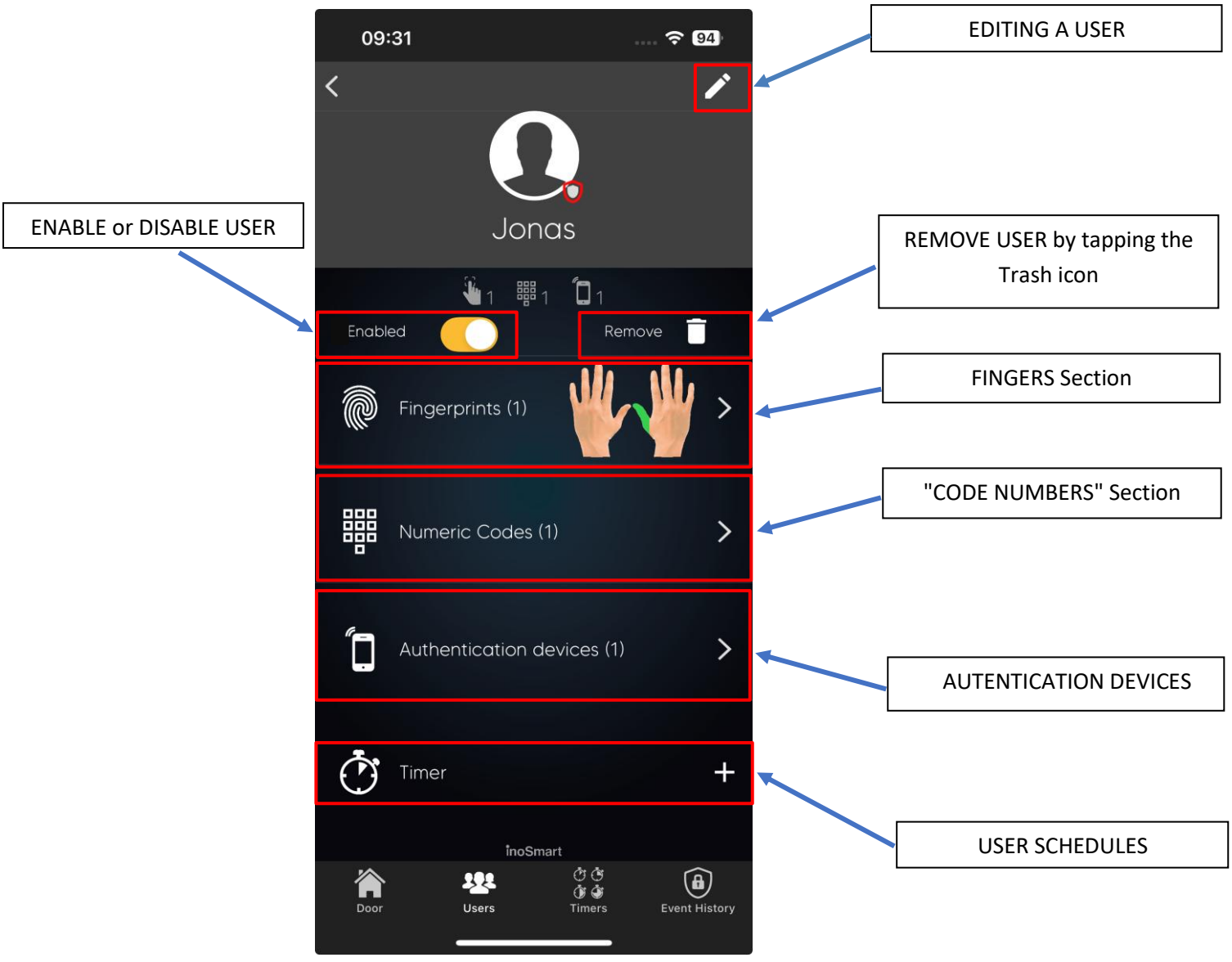
Individual users can be deleted from the user directory at any time. When a user is removed, all their access authorizations (fingerprints, authentication devices, code numbers) are also deleted.

To remove a user, tap the trash can in the top right corner of the user detail view.

TEMPORARILY DISABLE / ENABLE USER

You can use the button in the user detail view to deactivate or activate the user in question.

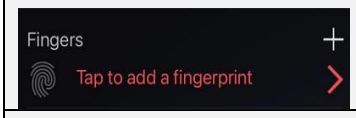
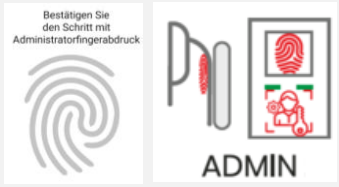
The individual user's button takes you to their DETAIL VIEW, where all their active access permissions - FINGERPRINTS, AUTHENTICATION DEVICES and CODE NUMBERS - are displayed as sections. By pressing the „+“-Buttons in the respective section allow you to grant the user the appropriate access authorization.



ADD NEW FINGERPRINT

The door can be opened by fingerprints.
In the user detail view, tap on the "FINGER" section and proceed as described below.

In the user detail view, the access authorizations for each individual fingerprint can be determined in detail and activated or deactivated.

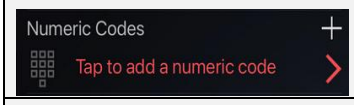
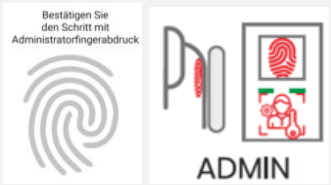
	Tap the Fingers section.	The program switches to the corresponding mode. The reader beeps briefly.
	All ten fingers appear on the display.	Fingers that have already been fingerprinted (active fingers) appear green.
	Tap the free or editable finger.	The process can be continued by selecting the free finger. The reader beeps briefly.
When editing an already assigned (active) finger, the "Options finger" button appears.		
	Place the administrator's fingerprint on the sensor to authorize the addition of a new fingerprint.	A new fingerprint is approved. Both LEDs light up white.
	A new fingerprint is validated by the administrator's fingerprint.	Place your finger on the sensor THREE TIMES, making sure that the fingertip covers the entire sensor surface and the green LED lights up. If the red LED lights up when reading in, the reading in of the fingerprint was unsuccessful and the process must be repeated.
	The reader beeps briefly and both LEDs light up green.	**A NEW FINGERPRINT HAS BEEN ADDED SUCCESSFULLY.** The reader is ready for operation and both LEDs light up blue**.**

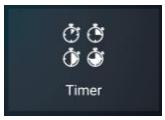
ADD NEW CODE NUMBERS (modules BT 600, BT 610, BT630, BT660 and BT 670)

The door can also be opened using a code number that is entered using the code keypad. The length of the code is preset to four digits at the factory. The length of the code can be changed in the reader settings.

In the user detail view, tap on the "CODE NUMBERS" section and proceed as described below.

In the user detail view, the access authorizations for each individual code number can be determined in detail and activated or deactivated.

	Touch the „Code Numbers“ section.	Click to initiate the addition of a new numeric code. The reader beeps briefly.
	Read the administrator's fingerprint via the sensor.	The process of adding a new numeric code is approved. Both signal lights glow white.
	The new code number can be entered.	Enter and confirm the 4-digit code on the smartphone or the keyboard of the fingerprint reader.
	The reader beeps briefly and both LEDs light up green.	**A NEW CODE NUMBER WAS SUCCESSFULLY ADDED.** The reader is ready for operation and both LEDs light up blue.



TIMER

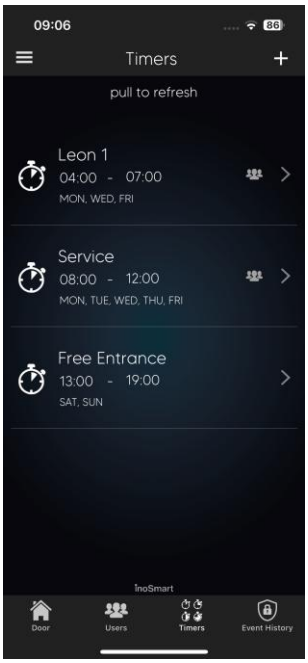
The timer function enables:


controlling the door lights ,


access validity for registered user - single or repeating timer
access to all (even unregistered users) - single or repeating timer


the setting of access time windows to the secondary relay (e.g. for the garage door, the alarm system).

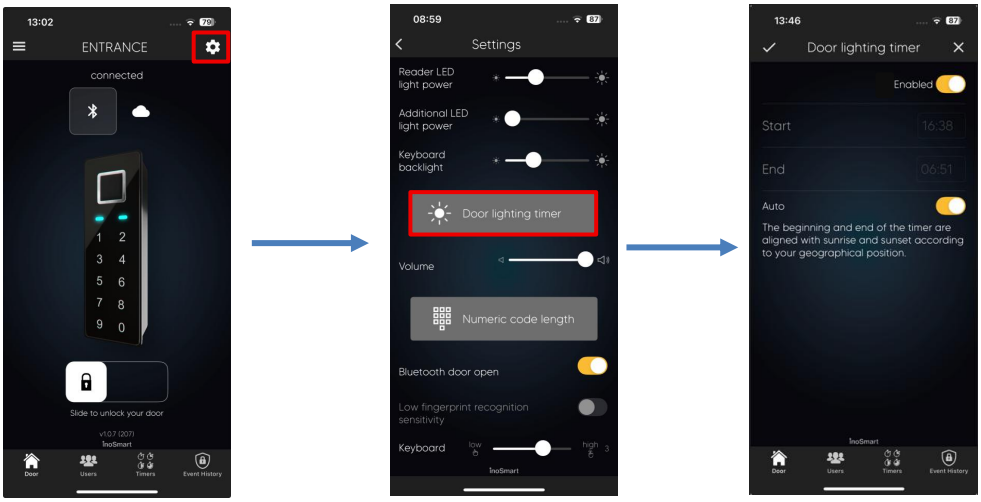
In addition to the door lighting, ten additional timers (e.g. for the cleaner, the caretaker, access by other people) can be added. The individual schedules can be changed, deleted, deactivated and activated at any time.



The Schedule function allows setting up:
repeating timer *(in this case, set the start and end time - interval and activity days, it will repeat the same every week) or*
one-time timer *(set the date and time). For both types of timer, you can define the validity of the access to the user or to the secondary relay.*

For the lighting timer, we recommend using the AUTOMATIC option. When the AUTOMATIC lighting function is activated, the reader will calculate the sunrise and sunset times for your location and automatically adjust the lighting on/off times accordingly.

Lighting timer:



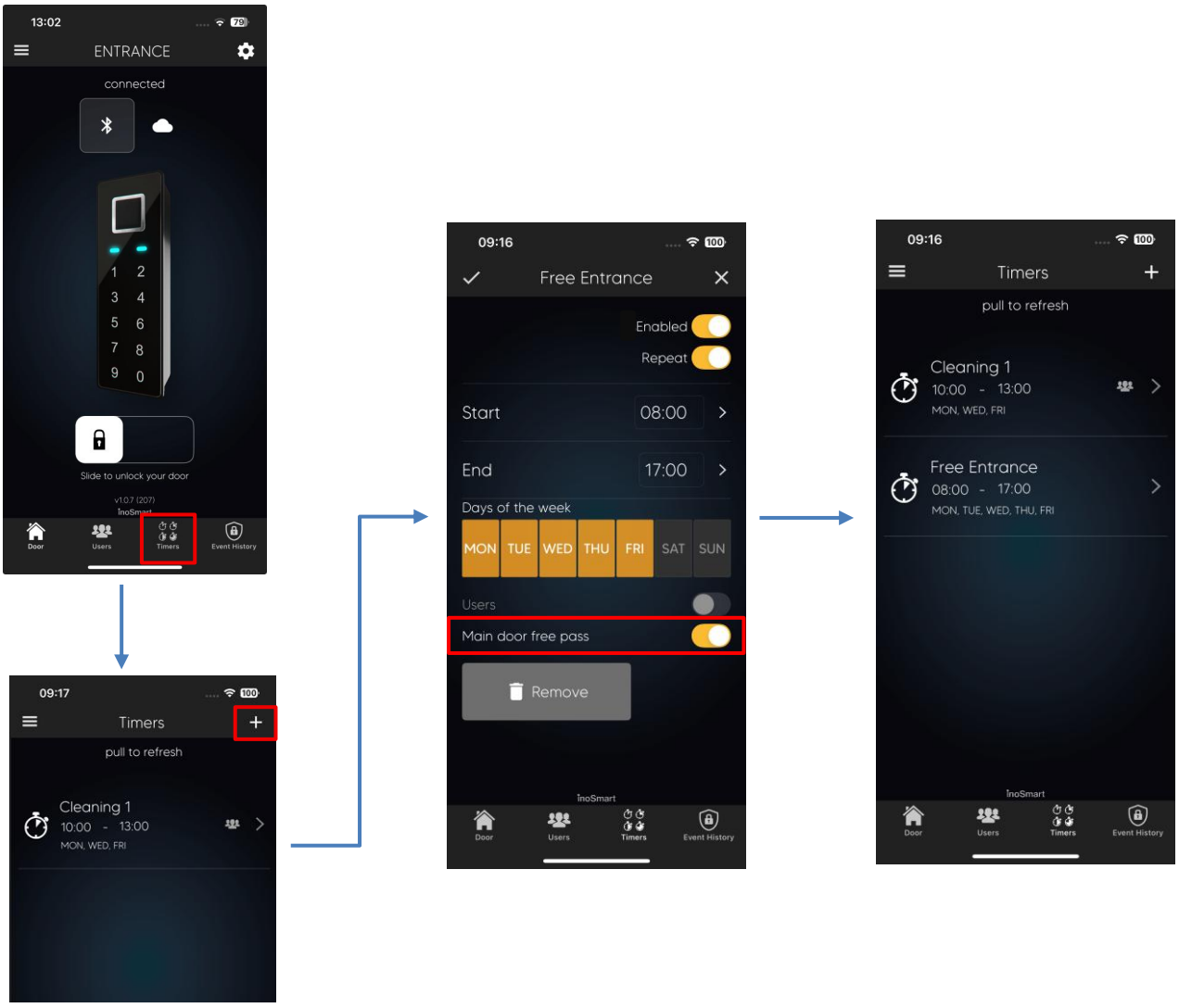
Attention! The access permissions granted to individual users – fingerprints, code numbers or Authentication devices – can be activated or deactivated. If all authorizations of a user are deactivated, he has no access during the granted time window.

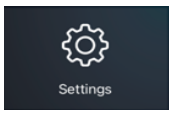
FREE ENTRANCE

Our readers also enable the “FREE ENTRANCE” function. With this feature enabled, any fingerprint, even if not enrolled, can open a specific door.

In the „Timers“ menu, you can easily define the time when the free pass should be active (once or repeatedly). During the time when the free pass function is on, the green signal lights on the reader light up continuously. After the selected time has passed, free passage is automatically switched off. The reader indicates this with a short beep, and the signal lights light up blue again.

Inosmart-App: **FREE ENTRANCE**





SETTINGS

The SETTINGS sentence in the main menu gives you options:

• Setting the level of built-in door lighting depending on the model: in the handle (back of the reader) or wing (additional door lighting), keyboard lighting and beeper volume.

• Setting the length of the numerical code.

• Setting the time for the relay to be open. The default is 2 seconds.

• Date, time and temperature of the reader.

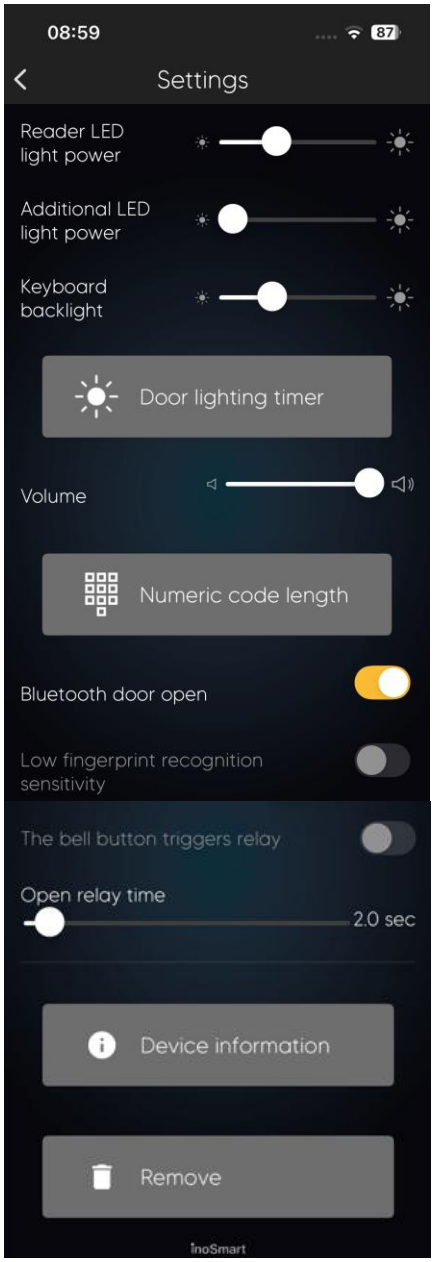
• At the bottom of the screen there is an additional Reader Information section where you have a detailed view of your device's data.

• Bluetooth door opening: Activate the door opening option with the button on the first screen of the Inosmart app

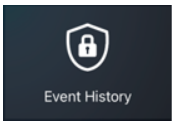
• Low sensitivity in fingerprint recognition: The sensor requires less fingerprint data and is designed for people with problematic fingerprints

• Setting the keyboard sensitivity for reader models with a keyboard. Possible values are 1 to 4. A value of 1 sets the keyboard to the least sensitive and a value of 4 sets the keyboard to the highest sensitivity. The default sensitivity value is 3. After changing the keyboard sensitivity setting, do not touch the keyboard keys for 30 seconds. This time is needed for the keyboard to calibrate to the new sensitivity.

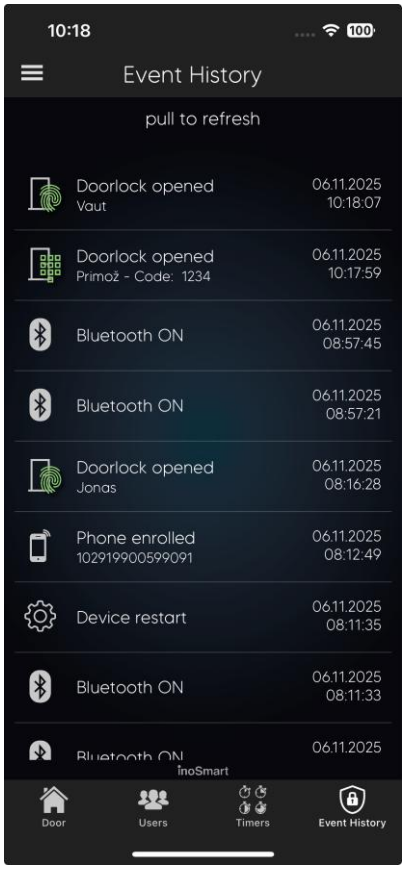
• Adjust the volume of the built-in beeper.



Attention! When the length of the code number is changed, all codes entered are deleted.



EVENT HISTORY

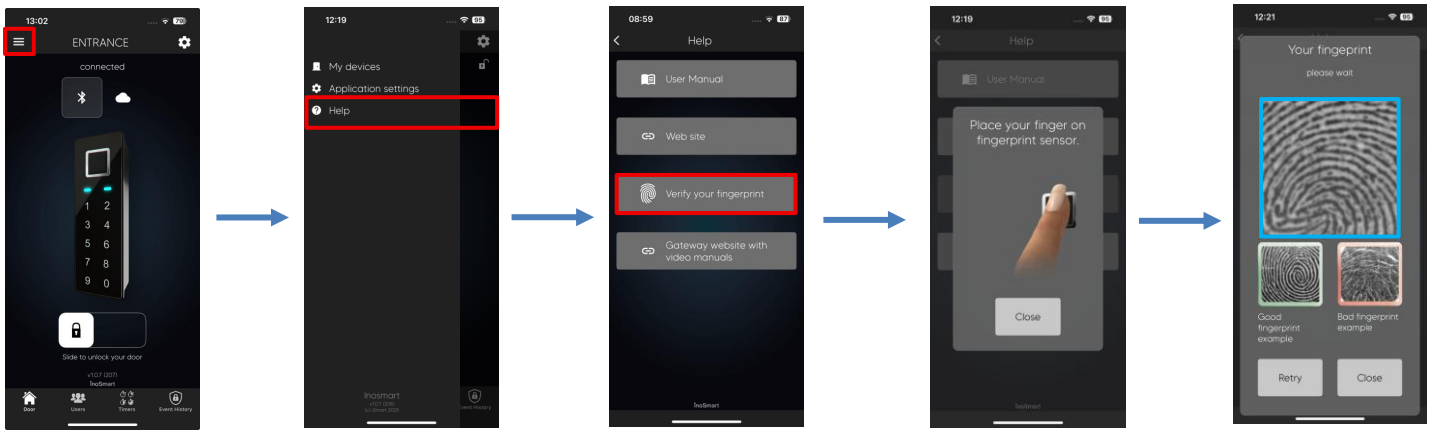


You can access the last 150 events via the “Event History” submenu.

You can find detailed information about individual accesses in the history: the date, time, person and their authorizations, as well as whether access was granted or denied.

FINGERPRINT VERIFICATION

A fingerprint test is available to the user under the main menu in the application. Your fingerprint is displayed at the top and a good and bad print below for comparison.



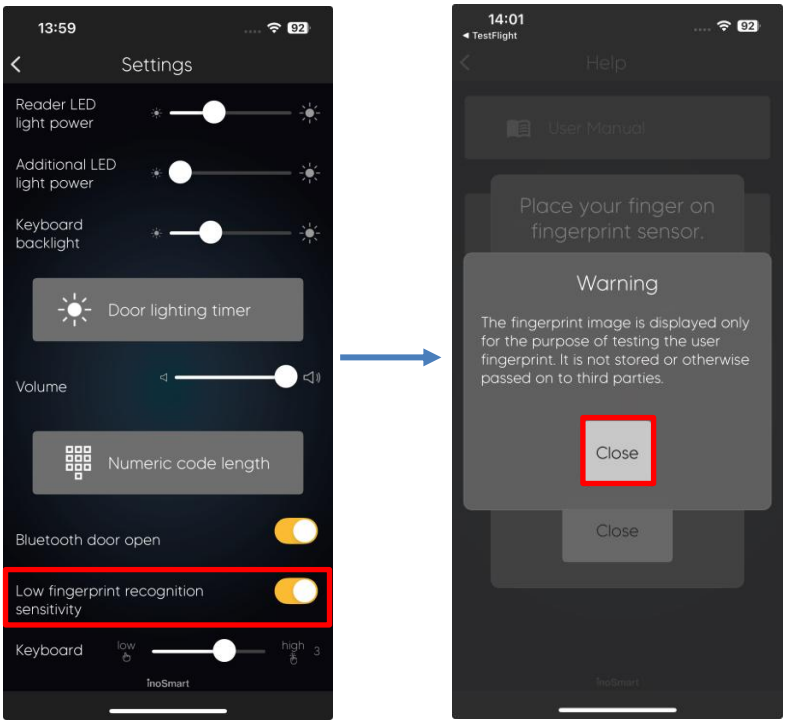
THE MOST COMMON REASONS FOR POOR FINGERPRINT RECOGNITION

- DRY SKIN: The most common reason for poor detection is dry skin or a damaged fingertip.
- The problem of dry skin is most pronounced during the winter months.
- INCORRECT USE: The finger has not been placed on the sensor correctly or in a different way than when it was entered.
- SENSOR CONDITION: The fingerprint sensor must be dry and clean. Both moisture and dirt interfere and prevent successful identification.
- WRONG INPUT:
  - The finger covers less than 70% of the sensor area when entering.
  - The finger is pressed too hard.
  - The finger is placed perpendicular to the fingerprint sensor.
- BAD FINGERPRINTS: A small percentage of people have their fingerprints so damaged or unclear that they can no longer use the reader. This problem often occurs in the elderly, tradesmen and children up to 9 years old.

ADJUSTING THE SENSITIVITY OF FINGERPRINT RECOGNITION

For people who have problems with fingerprint recognition, it is possible to set a lower fingerprint recognition sensitivity in the Inosmart app.

In this mode, fewer features of an individual fingerprint are required for successful recognition. A low level of security is in some ways comparable to using a 5-digit numeric code.



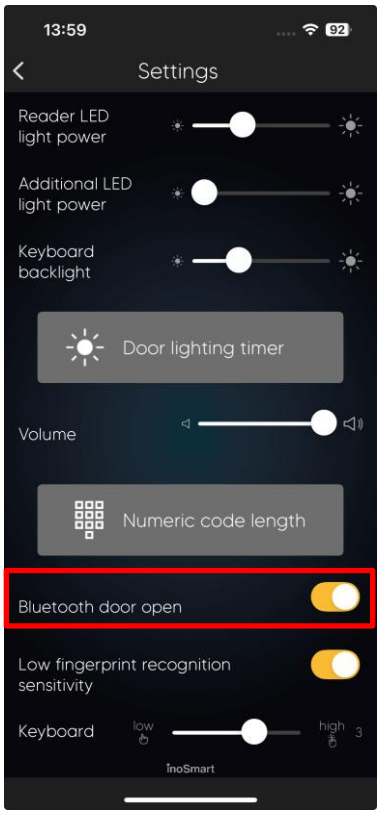
After confirmation of activation, the connection is terminated. All fingerprints remain saved and do not need to be re-entered.

Your reader supports Bluetooth Low Energy technology, which allows you to open the door from a distance of several meters.

DOOR OPENING VIA BLUETOOTH CONNECTION

By integrating Bluetooth low energy technology into the Inosmart system, we have made it possible to unlock the door from a few meters away directly by pressing a button in the Inosmart app.

The door unlocking function via Bluetooth is enabled when the device is connected to the Inosmart application for the first time. The phone automatically registers for unlocking and displays the unlock slider on the home screen. To unlock the door, simply swipe the slider to the right. Unlocking takes 1-3 seconds, depending on the phone.



The setting in the Inosmart app for "Bluetooth door open" is switched on after the first connection to the reader, but can be switched off in the "SETTINGS" menu.

PHONE REGISTRATION TO UNLOCK VIA BLUETOOTH CONNECTION

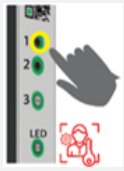
For each added Authentication device you can set what the user opens and whether a specific identification method is activated or deactivated in the user's detailed view.

The prerequisite for operating the remote door opening is that the "Bluetooth door opening" mode of the control unit is switched on. In this mode you can open the door with your phone. In "Bluetooth door opening" mode, the light on the control unit flashes white.
Attention: To manage the reader it is necessary to press button 3 and place the administrator's finger. The light on the control unit in administrator mode is blue.

We can register the phone we want to open the door to in two ways:

1. Install the application on the phone, add the reader (we need to know the reader's password) and connect to the reader. After successful connection, the phone will be automatically added to the list of phones to open the door. On the first screen of the application, a blue button will appear with the reader's name. Pressing the button opens the door.
2. If we do not want the phone to have access to the reader's management, but just open the door, follow the steps below:
   - Install the Inosmart application on the phone
   - Press button 1 on the control unit and place the administrator's finger on it (the reader lights up white with both lights).
   - On the first phone screen, press the + button and select the reader
   - The reader will beep after a few seconds, a blue button will appear on the screen
   - The phone is registered to unlock

Opening the door via Bluetooth connection is possible at a distance of a few meters from the door. It depends on the signal strength. The door open button in the Inosmart app turns blue when your door is within range and opening is possible.

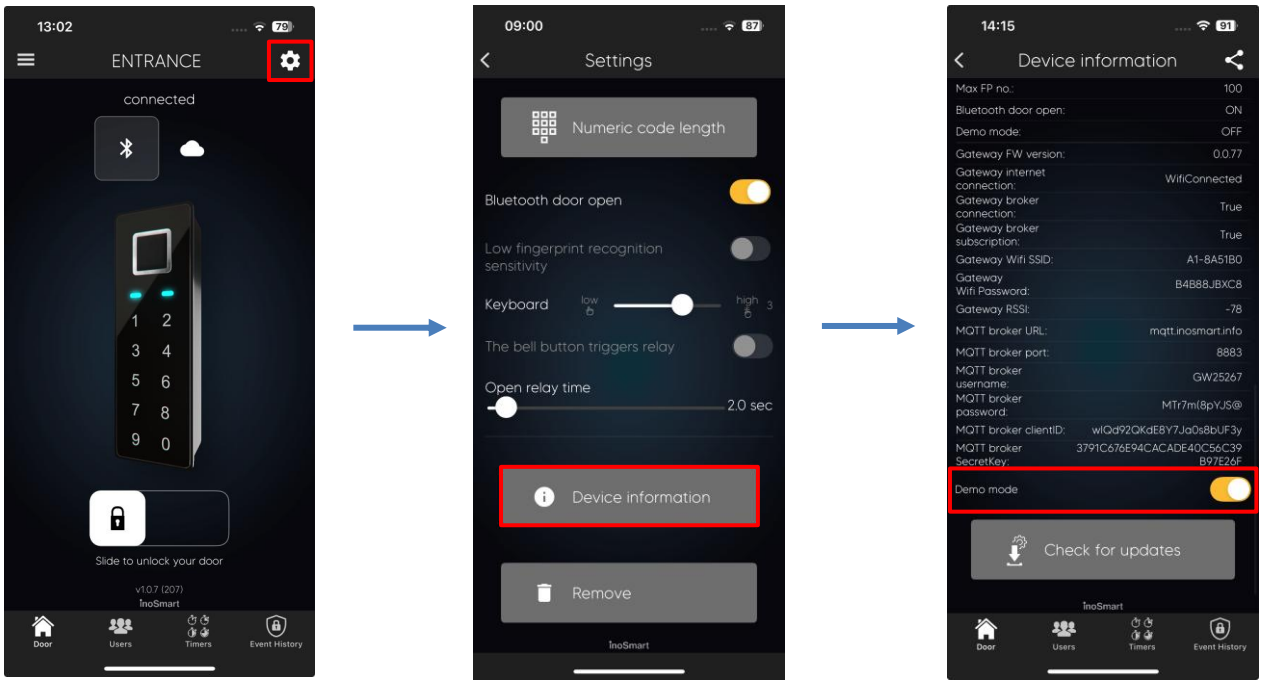
	Press button 1 on the control unit	**Enable Bluetooth on the phone you want to add.**
 	Place the administrator's fingerprint on the fingerprint sensor.	The process of adding a new smartphone is approved. Both signal lights light up white.
	On the first phone screen, press the **+** button, select the reader and confirm.	**The reader beeps briefly. A blue button will appear on the screen with which we can open the door.**

BT DEMO MODE

This mode allows the permanent activation of the administrative BT mode, intended for connection with the Inosmart App. It is primarily intended for showrooms and the like where there is no need for high security.

In this mode we can connect to the Inosmart system at any time without having to first turn on BT with the 3 button on the control unit and confirm it with the administrator's finger on the reader.

After activating demo mode, the connection is disconnected and the system restarts.



Attention!

The BT demo mode is used to present the Inosmart system in showrooms.

Activation for home use is not recommended due to reduced security!

SECOND RELAY

In addition to opening the door, our readers also enable the control of an additional door (e.g. a side door or the garage door) or an additional device that is connected to the control unit. In this case too, the permissions (for one or both relays) can be set individually for each user. The secondary relay can be opened with users and their access authorizations: FINGERPRINTS, PHONES and CODE NUMBERS.

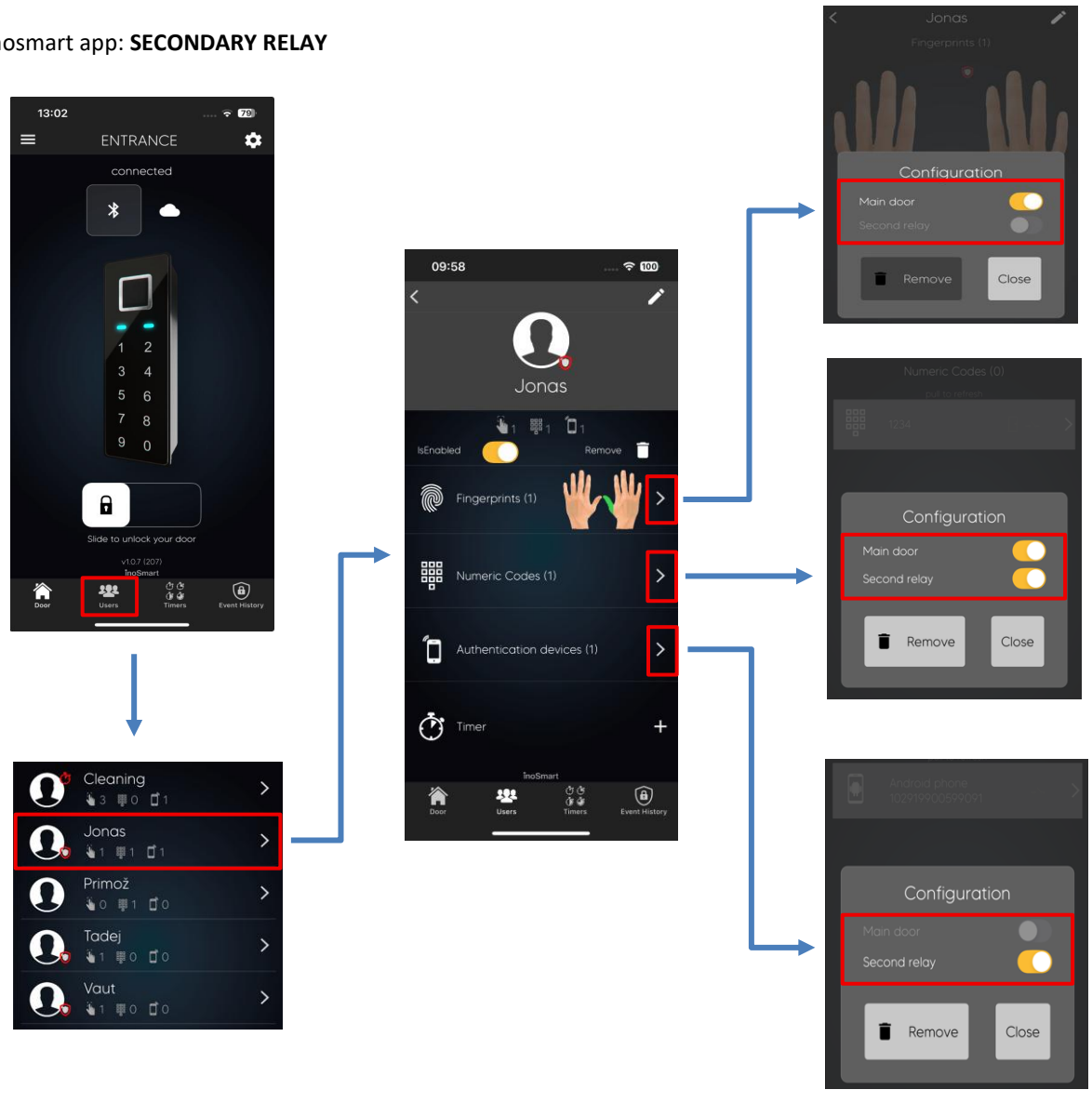
Setting the activation of the additional relay is only possible via the application with the control unit v1!

Inosmart systems with the control unit v2 (from 1.1.2025 onwards) no longer have an integrated relay in the control unit. Additional relays are only available with the added Inosmart Gateway module.

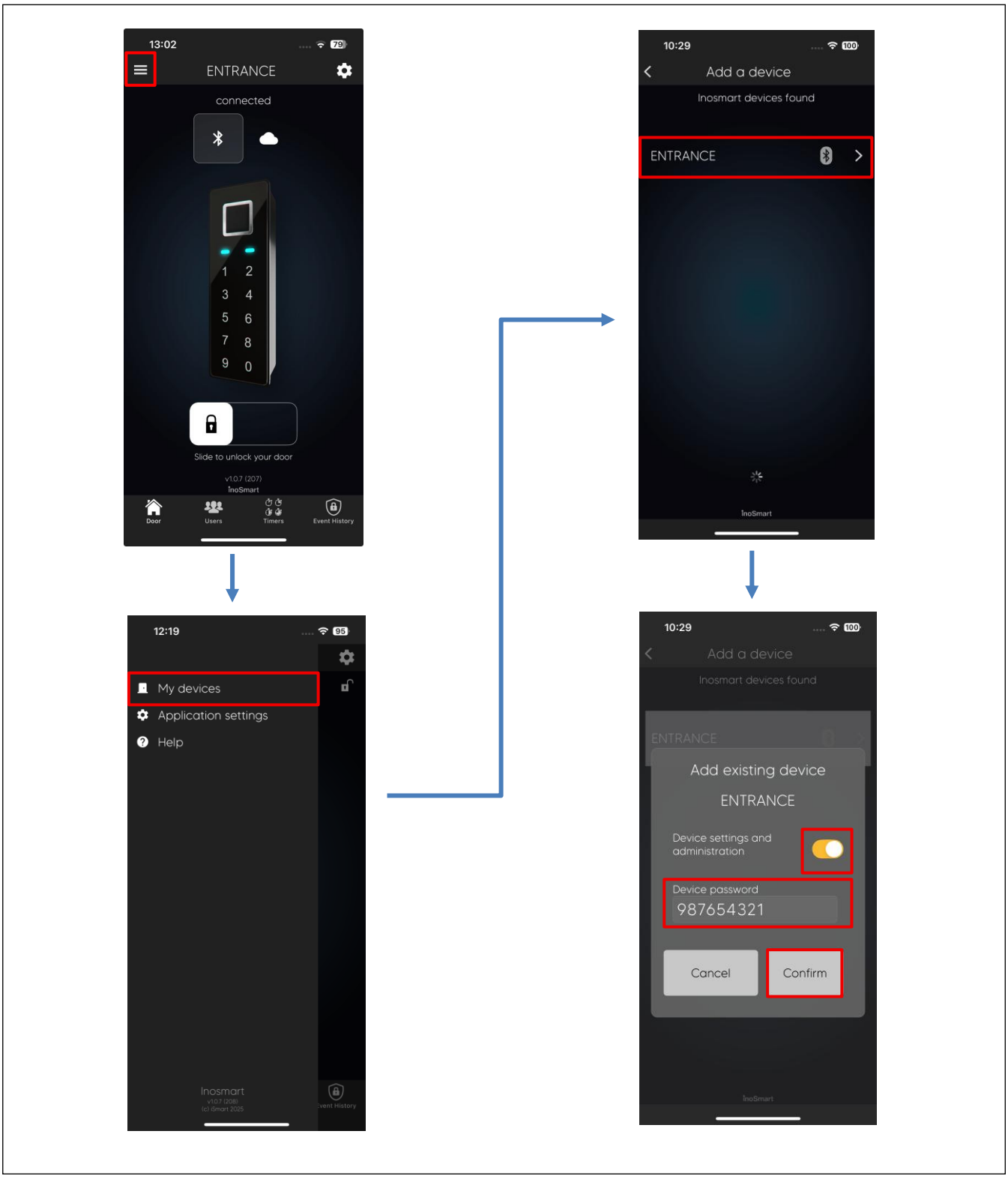
Details are available at: ***https://www.inosmart.info/gateway/en/***

The second relay is only accessible via the app!

Inosmart app: **SECONDARY RELAY**



CONECTION WITH AN ADDITIONAL TELEPHONE



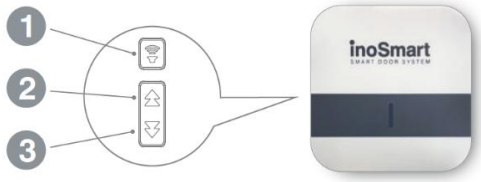
Enter the password you set when renaming this reader.

PAIR READER WITH RADIO BELL

The **BT 600** and **BT 630** readers can be used to control one or more WiFi radio bells, which must first be connected to the reader for this purpose.

Danger! Metal structures can limit the range of the wireless doorbell, as can walls and ceilings. Other devices may cause radio interference that affects the doorbell.

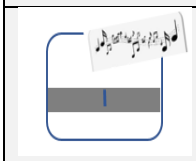
Quick Start:



1. VOLUME BUTTON: switches between high and low volume,

2. BACK BUTTON and 3. FORWARD BUTTON: Choose your favorite ringtone.

To pair the wireless bell with the reader, proceed as follows:

	The two LEDs on the reader light up blue.	Plug the radio bell into the socket.
	Select ringtone.	➢ Select the desired melody using the “Select ringtone” button on the bell. ➢ Press the same button for a few seconds until the LED on the front of the doorbell starts flashing blue.
	Press the bell button on the reader within five seconds.	After pressing the bell button, the LED on the bell stops flashing and the ringtone sounds. The bell is connected to the reader. The process can be repeated if necessary. **THE BELL IS READY TO WORK.**

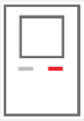
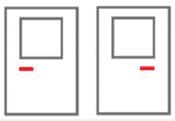
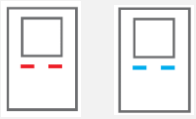
To change the ringtone, the bell must be reconnected to the reader as described above.

CARE AND MAINTENANCE

Our fingerprint readers do not require any special care or maintenance; However, the sensor must always be free of contamination. These can form and impair the function of the reader if it is operated with greasy or dirty fingers. If the sensor becomes dirty, clean it with a soft, damp cloth.

Do not use aggressive cleaning agents, polishing pastes or acids when cleaning! Do not clean the sensor with hard or sharp objects, which may damage the sensor and cause reader failure and void the warranty.

ERROR MESSAGES

	Only the left LED flashes red.	Reader error **Disconnect the cable transition (see the relevant chapter).**
	If the LEDs continue to flash, disconnect the control unit from the power supply or power supply.	
	Only the right LED flashes red.	Error on the control unit **Disconnect the cable transition (see the relevant chapter).**
	The left and right LEDs flash red alternately.	The reader and the control unit are not connected.
	The left and right LEDs flash red and blue alternately.	The device is locked due to unsuccessful access attempts.

RESET TO FACTORY SETTINGS

To reset the device to factory settings, press all three buttons on the control unit at the same time and hold them for 10 seconds until you hear a beep. All fingerprints, smartphones, code numbers, users and timers are deleted and the reader's factory settings are restored.

After restoring the factory settings, the reader must be removed from the reader directory of the Inosmart app and reinstalled since it is no longer recognized by the controller.

FAQ – FREQUENTLY QUESTIONS

1. *CONNECTION TO THE SMARTPHONE WAS NOT SUCCESSFUL*

- Check whether Bluetooth is activated on the control device. Activated Bluetooth access is signaled by a blue light on the control unit.
- Install the latest version of the Inosmart application.
- Open the door and bring the phone as close to the door as possible when connecting.
- Restart your phone. Typically, this step, along with Step 2, is the most effective in troubleshooting connection issues.
- Enable Bluetooth and location on your phone (Android only). The latest version of the Inosmart application takes care of the automatic activation of Bluetooth communication and positioning
- When installing the Inosmart Plus application, you must confirm all the permissions that are requested
- When connecting to a device that has already been named, it is necessary to correctly enter the password that was set during the first connection (lowercase / uppercase letters, ...)
- When establishing the FIRST connection, the phone will automatically display a confirmation window with a randomly generated 6-digit number that needs to be confirmed. Without this confirmation, the connection between the control device and the telephone is not possible.
- Reset the reader to factory settings (press buttons 1+2+3 on the control unit for 10 seconds). Enter admin finger and repeat steps 1 to 5.

2. *FINGER MEMORY*

- For comfortable use and in case of injury, we recommend inserting one finger from each palm. Preferably it should be the same finger.
- To improve finger recognition, it is better to enter a single finger multiple times than to enter multiple fingers. This increases the probability of detection even under marginal operating conditions (very dry finger, wet finger, partially damaged finger).
- We must take into account that fingerprints develop in children up to 8 years of age. It is possible that younger children may not have a sufficiently developed fingerprint for successful identification. Typically, children's fingers are too small to cover at least 70% of the sensor, which is a prerequisite for successful detection.
- For children, the elderly and people with partially damaged fingers, we strongly recommend entering the same finger multiple times.

3. ENTRY OF NEW FINGERPRINT FAILED

- The reading sensor must be dry and clean. Both moisture and dirt impair or prevent successful identification.
- The finger was pressed too lightly or too hard on the sensor. It should be pressed with normal force.
- The finger was placed on the sensor at too great an angle. Place it parallel to the sensor.
- Not enough finger area was pressed onto the sensor. The sensor must receive an image large enough to input the pressure. Please try again.
- The fingerprint database is full. If you delete one of the existing fingerprints, you can enter a new fingerprint.
- The skin on the finger is very dry. Ensure sufficient skin moisture.
- To solve problems entering fingerprints for children, the elderly, and people with damaged fingers, see “Storing Fingers.”

4. THE SAVED FINGER WAS NOT RECOGNIZED

- The reading sensor must be dry and clean. Both moisture and dirt impair or prevent successful identification.
- The finger was pressed too lightly or too hard on the sensor. It should be pressed with normal force.
- Place your finger on the sensor the same way you placed it while learning.
- Not enough finger area was pressed onto the sensor. The sensor must receive an image large enough to input the pressure. Please try again.
- The skin on the finger is very dry. Make sure the skin on your finger is sufficiently moist.
- To resolve problems recognizing fingerprints of children, the elderly, and people with damaged fingers, see “Store Your Fingers.”
- Enter the problem finger several times as correctly as possible – 3x or 4x. This significantly increases the chance of successful finger recognition.

5. THE FINGERPRINT IS IDENTIFIED, THE LIGHTS ARE GREEN, BUT THE LOCK WILL NOT ACTIVATE

- A different relay is assigned to the finger you are using. If you want to open the door with this finger, you can activate it using the application. Please refer to the instructions for use for the exact procedure.
- Reader or lock error. Call an authorized service technician.

6. DOOR OPENING WITH SMARTPHONE WAS NOT SUCCESSFUL

- Check whether the door opening button in the Inosmart application is colored blue and stand 1 m away from the door. If it is not colored blue, close and restart the Inosmart application
- Check that the light on the control unit is flashing white. If it does not flash, enable “Bluetooth door opener” mode in the application settings.
- Turn on Bluetooth on your phone and restart the app.
- Check if your phone is registered to unlock.

INOSMART READER SPECIFICATIONS

- Capacity: 50 users, 100 fingerprints, 10 Authentication devices, 100 numeric codes, 10 timers.
- Supply voltage: 24V DC, regulated.
- Consumption by reader model without additional lighting in the door (the consumption of any additional lighting and electric lock must be added to the consumption):
  - o BT610, BT660, BT670 (min/max): 1.2W / 2.6W
  - o BT620: 1.2W
  - o BT680: 0.6W
- Fast fingerprint recognition: < 1 s.
- Operating temperature range: -25 ºC to +70 ºC.
- Fingerprints, registered phones and numeric codes remain stored in memory even in the event of a power failure.
- Capacitive sensor, resolution 508dpi, ESD range ±3kV, reading 360º.
- User interface: two 5-color LEDs, buzzer, buttons on the control unit, smartphone application.
- Support for KFV motor locks.
- Certificates of conformity: C251-0049/21 and T251 – 0280/25 (EN 303 446-1 V1.2.1)
- Cybersecurity test conducted by the Slovenian Institute for Quality and Metrology SiQ Slovenia. Testing was carried out according to the internationally recognized OSSTMM methodology and OWASP vulnerability tests and taking into account the good practices of the international standards ISO/IEC 27001:2013, ISO/IEC 27002:2013 and ISO/IEC 27008:2011.
- Warranty 2 years.

CE - CERTIFICATE OF CONFORMITY

SLOVENSKA AKREDITACIJA
SIST EN ISO/IEC 17065
CP-001

Certificate of Conformity

Number:	**C251-0023/25**	Project file: C20250692
Product:	**Inotherm door**	
Type reference:	**Exclusive, Select**	
Trademark:	Inotherm	
Applicant:	**Inotherm d.o.o.** **Prigorica 98, SI-1331 Dolenja vas, Slovenia**	
Manufacturer:	Inotherm d.o.o. Prigorica 98, SI-1331 Dolenja vas, Slovenia	
Place of manufacture:	Inotherm d.o.o. Prigorica 98, SI-1331 Dolenja vas, Slovenia	

This certificate is granted subject to the SIQ's rules on product certification. SIQ certifies the conformity of the products with the requirements of the listed standards.

Ratings:	100 – 240 V a.c.; 50/60 Hz
Standard:	EN 303 446-1 V1.2.1
Test report:	T251-0280/25 (2025-04-24)
Remarks:	This certificate shall apply to the products identical to the tested sample and shall remain valid for the period of 3 years until 2028-04-24 or until the validity date of the listed standards, whichever occurs earlier.

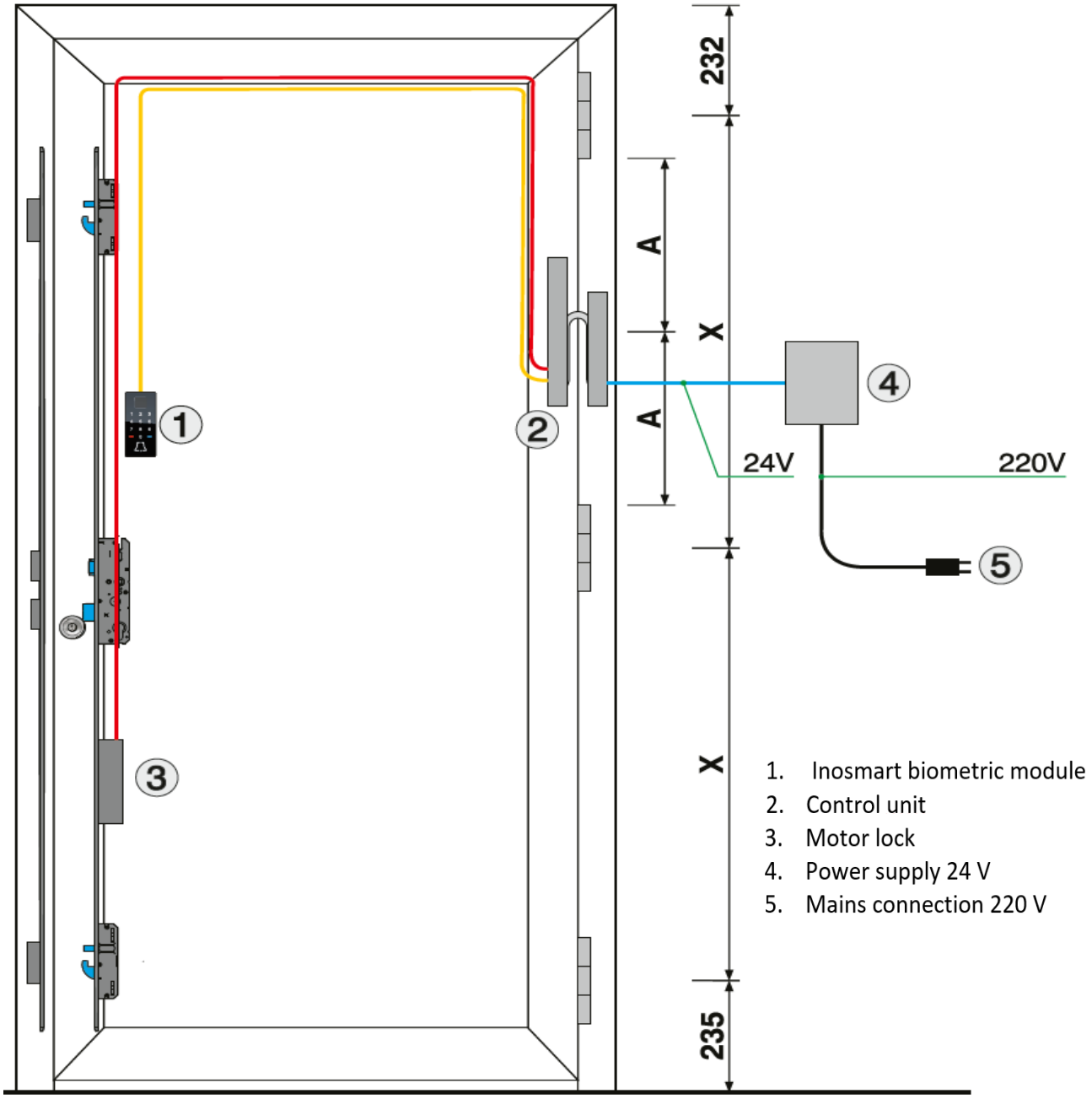
Date: 2025-04-24

Authorized signature: Matej Žontar

SIQ Ljubljana, Mašera-Spasićeva ulica 10, SI-1000 Ljubljana, Slovenia
T +386 1 4778 100, F +386 1 4778 444, info@siq.si, www.siq.si

CN500E-02

INSTALLATION DIAGRAM



ATTENTION:

The low-voltage cable, from the door frame to the box with the power supply, must be run separately from the electrical installations, in no case in the same pipe together with the high-voltage conductors. The minimum distance to high-voltage conductors of electrical installations is 200 mm.

Failure to comply with this regulation causes induced interference in the low-voltage conductor, which disrupts the operation of the reader (poor keyboard response, automatic keyboard activation, unresponsiveness of the fingerprint sensor, poor fingerprint recognition...).

More detailed requirements are given in the SIST standard IEC 60364-4-44:2007/A2.

DANGER!

Risk of electrocution!

All Inosmart devices are to be operated with Safety Extra Low Voltage (SELV). Only use power supplies rated protection class 2.

Failure to do so will create a risk of fatal electrocution.

Only certified electritians are authorized to carry out the electrical installation Work!

USER INSTRUCTIONS

Fingerprint recognition technology has its limitations. When using the reader every day

The following conditions and restrictions must therefore be observed:

Fingerprint reader:

- The sensor surface must be dry and clean
- The keyboard and the bell button must be dry and clean

We recommend that the reader avoid direct weather influences such as rain and all day

Is exposed to sunlight.

Finger:

- The fingertips must be clean and normally moist,
- Moisture, sweat, creams, oils, dust, injured fingertips, dry skin can affect detection. The same applies to activities such as swimming, sports, showering,
- Cooking or similar activities that can change the texture of the fingertips

MANUFACTURER WARRANTY

The guarantee period is 24 months from the day the product is handed over to the end buyer. The manufacturer of the product guarantees trouble-free operation of the Inosmart fingerprint reader (hereinafter: product) for the warranty period and that the materials used to make the product are free of defects and damage. If the buyer discovers a functional defect in the product, he can claim the warranty from the seller or manufacturer. In the event of a justified complaint, the seller undertakes to remedy the functional defect within 45 days from the day of the complaint. If the defect cannot be remedied, the buyer will receive a new product from the seller within 45 days of the day of the complaint.

Notes on warranty claims:

The customer assumes all risks and costs incurred in transporting the product to an authorized dealer or an authorized service center. The guarantee is only valid if the guarantee card has been completely filled out by the authorized seller, or if the circumstances of the purchase are sufficiently clear from other documents. Make sure that the original invoice contains: your name, the seller's name, the product serial number, the year, month and day of purchase. Make sure that the invoice you receive at the time of purchase the original warranty card is attached, which indicates the name of the seller, the date of purchase and the type of product. iSmart d.o.o. reserves the right to refuse a free repair if neither a fully completed warranty card nor the above-mentioned document (proforma invoice, invoice) is presented, or in the event that the information on the warranty card is incomplete or illegible.

Please keep the warranty card safe as we will not issue you a duplicate!

Warranty extension:

In the event that the buyer has claimed the warranty for the product and the authorized service has determined that the complaint is justified, the warranty period is extended by the time the product was at the service. However, if a major service intervention has been carried out on the advertised product or the product has been replaced with a new product, the buyer will be granted a new warranty for a period of 24 months.

The warranty claim expires in the following cases:

1. In the event of damage resulting from repairs, mechanical damage, modifications, cleaning or other interventions in the product by persons not authorized by Inotherm d.o.o. are authorized.

2. In the event of damage caused by transport, drops, impacts, etc. caused after purchasing the product.

3. In the event of damage caused by fire/fire, earthquakes, floods, lightning strikes, other natural disasters, environmental pollution and incorrect mains voltage or type of current.

4. Any damage caused by fire, earthquake, flood, lightning, other natural disasters, polluted environment and improper power supply voltage.

5. Any defects caused by negligent handling or improper feeding/storage of the product (e.g. feeding at high temperatures and high humidity, alongside insecticides such as mothballs, or alongside medications, poisons and chemicals that may cause damage), improper maintenance, etc become .

6. If the product submitted for repair is not accompanied by a warranty card.

7. Any changes to the warranty card regarding year, month and day of purchase, name of buyer or seller and serial number.

8. If the warranty card is not accompanied by a proof of purchase (receipt).

Inosmart app upgrade:

Due to technical or functional upgrades to the Inosmart app, Inotherm has the right to publish a new version of the Inosmart app.

The user is informed about this via the Inosmart app itself. To update you must select the update confirmation. If the user rejects the updates, Inotherm is not responsible for any errors in the operation of the app or the connection between the app and the Inosmart system. It also assumes no responsibility for the inability to use the new/changed features included in the app upgrade.

Limitation of liability:

iSmart d.o.o. makes no representations or warranties, express or implied, on behalf of the suppliers or in relation to the content of the written material and is under no obligation to guarantee the purchased material or its fitness for a particular purpose or for any consequential, incidental or direct damages Damages (including, without limitation, damages or loss of business profits, business interruption and loss of business information) arising from the use or inability to use these publications or devices.

Some states do not allow the limitation of liability for consequential or incidental damages, so the above provision may not apply to you. In the event that the buyer sends the product by mail due to a complaint, we recommend insuring the shipping. The seller and the manufacturer are not liable for any damage that occurs during transportation.