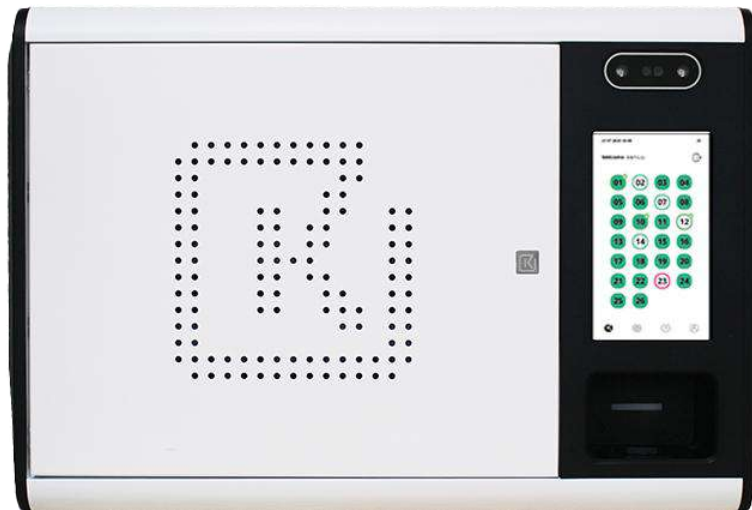


# K26

Nice appearance and  
user friendly



## User Guide

V1.9



# Content

|                                     |   |
|-------------------------------------|---|
| Revision Record .....               | 1 |
| Part 1 INTRODUCTION .....           | 1 |
| 1.1 What is the K26 solution .....  | 1 |
| 1.2 Glossary overview .....         | 1 |
| 1.3 Features .....                  | 2 |
| Part 2 K26 OVERVIEW .....           | 3 |
| 2.1 Panel .....                     | 3 |
| 2.2 The touch screen .....          | 4 |
| 2.2.1 Screen Saver .....            | 4 |
| 2.2.2 Touch Command .....           | 4 |
| 2.3 Fingerprint Sensor .....        | 4 |
| 2.4 Network .....                   | 4 |
| 2.5 Wall mounting .....             | 4 |
| 2.5.1 Planning the position .....   | 5 |
| 2.5.2. Preparation .....            | 5 |
| 2.5.3 Wall installation .....       | 6 |
| 2.5.4 How to dismantle .....        | 6 |
| 2.6 Power the System .....          | 7 |
| 2.6.1 Power Parameters of K26 ..... | 7 |
| 2.6.2 Using UPS backup power .....  | 7 |
| 2.6.3 Using battery .....           | 7 |
| Part 3 KEY FOB .....                | 8 |
| Part 4 USING THE SYSTEM .....       | 8 |
| 4.1 logging into the system .....   | 8 |
| 4.2 Removing & returning keys ..... | 8 |
| 4.3 Chang Password .....            | 9 |

|  |    |
|--|----|
| Part 5 ADMINISTRATOR MENUS .....                     | 10 |
| 5.1 First Run .....                                  | 11 |
| 5.2 Keys .....                                       | 11 |
| 5.3 Users .....                                      | 12 |
| 5.4 Permission Group .....                           | 12 |
| 5.5 Multi-verification .....                         | 13 |
| 5.6 Events .....                                     | 14 |
| 5.7 Report .....                                     | 14 |
| 5.8 Parameter Settings .....                         | 15 |
| 5.8.1 Login History .....                            | 15 |
| 5.8.2 Remote Control Prompt .....                    | 15 |
| 5.8.3 Key Preview .....                              | 15 |
| 5.8.4 The Standby Page and Home Logo .....           | 16 |
| 5.8.5 Snap pictures while key removal & return ..... | 16 |
| 5.8.6 Login Settings .....                           | 17 |
| 5.8.7 Cabinet name .....                             | 17 |
| 5.8.8 Switch between Standalone and Networked .....  | 17 |
| 5.8.9 Language .....                                 | 18 |
| 5.8.10 System .....                                  | 18 |
| Part 6 WEB-BASED MANAGEMENT .....                    | 18 |
| 6.1 Features Layout .....                            | 18 |
| 6.2 Home Page .....                                  | 20 |
| 6.3 Function Settings .....                          | 21 |
| 6.3.1 Department .....                               | 21 |
| 6.3.2 Key cabinet .....                              | 22 |
| 6.3.3 Key .....                                      | 22 |
| 6.3.4 Permission Group .....                         | 23 |
| 6.3.5 User .....                                     | 23 |

|  |    |
|--|----|
| 6.3.6 Key permission .....                   | 24 |
| 6.3.7 Multi-verification .....               | 25 |
| 6.3.8 Event .....                            | 26 |
| 6.4 Reports .....                            | 26 |
| 6.4.1 Key Record .....                       | 27 |
| 6.4.2 Abnormal record and processing .....   | 27 |
| 6.4.3 Operation log .....                    | 27 |
| 6.4.4 Mailbox Record .....                   | 28 |
| 6.5 Forgot the password .....                | 28 |
| Part 7 Applications for Cell Phone .....     | 28 |
| 7.1 How to obtain and activate the app ..... | 28 |
| 7.2 How to modify password .....             | 29 |
| 7.3 Key Overview & Remote Control .....      | 29 |
| 7.4 Reservation and Approval .....           | 30 |
| 7.5 Personal Info .....                      | 30 |
| 7.6 Records .....                            | 31 |
| Part 8 FAQs .....                            | 31 |
| 8.1 General .....                            | 31 |
| 8.2 Operation .....                          | 32 |
| 8.3 Others .....                             | 33 |

## Revision Record

| Version | Content   | Date       |
|---------|---|------------|
| V1.0    | Create  | 29/11/2020 |
| V1.2    | Add web management  | 06/04/2021 |
| V1.3    | Add part of cell phone  | 23/05/2021 |
| V1.4    | Modify <i>Apps for cell phone</i>   | 25/01/2022 |
| V1.5    | Add part of Power   | 16/03/2022 |
| V1.6    | Modify Key permission   | 20/06/2022 |
| V1.7    | Modify User setting   | 18/11/2022 |
| V1.8    | Edit Alarm options  | 29/11/2022 |
| V1.9    | First Run, ID format to 4-12 chars, Reset, Tap sound, Custom home logo, Encrypt user data | 30/12/2022 |

## Part 1 INTRODUCTION

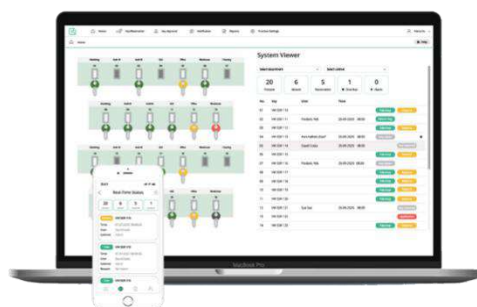
The purpose of this document is to help you (the end-user) understand the basic knowledge and operation specifications of the *Keylongest* intelligent key management system. It covers the relevant knowledge about how to use the intelligent key cabinet device and software, which is a supplement to the in-depth product training that you get from our experienced project manager after the system installation and commissioning. Please keep this guide handy for those times when you need to remember how to Add Users, Add Keys, run Reports, or other options.

### 1.1 What is the K26 solution

*Simplifying key management for small to medium-sized businesses and organizations.*

Physical keys management can be a common problem for a variety of businesses and organizations, including office, property, hostel, healthy centres, etc. In fact, almost any small to medium-sized business (SMB) can face challenges controlling and managing their keys. How many keys do you have in your management? And who owns which key?

Keylongest is an electronic key management system. It combines innovative RFID technology and robust design to provide businesses with advanced management capabilities for up to 26 keysets in an affordable plug-and-play unit. Its cloud-based management ensures that you can work safely from home. Modular key management solution that's smart and easily expandable. Keylongest can easily be integrated and linked with your existing software. Easily manage keys and the users of these keys.



### 1.2 Glossary overview

[1] **System** – The term 'system' refers to the K26 unit.

[2] **Key Fob** - The heart of the K26 system. It contains a small RFID chip that allows the system to identify the key(s) attached.

[3] **Security Seal** - The Security Seal is used to attach the key(s) to the Key-Fob. Once the seal has

been crimped, the only way to detach the keys from the Key-Fob is to cut the security seal using a pair of heavy-duty cutters.

[4] **Users** - Users are added to the system by an administrator and can either be a standard user or another administrator. This is done from the user wizard in the admin section of the K26.

[5] **Permissions** - The permissions section of the K26 allows you to easily identify who has access to what keys and allows you to edit each user's permission.

[6] **Permission Group** - A set of users with the same operation authority and the same key authority

[7] **Multi-Verification** - The person using the key will not be allowed to remove the preset key(set) unless one of the preset people login to K26 to provide proof

[8] **Event** - The purpose of using the key

[9] **Reservation** - Key reservation is a short-term exclusive use of the available keys within the permissions. The initiation takes effect immediately. During the validity period, no one except the administrator can access the key.

[10] **Application** – Key application is a request for temporary access to the key, and it will take effect after the administrator approves it.

## 1.3 Features

- 1) Plug & Play solution with advanced RFID technology
- 2) Keys are available 24/7 to authorized staff only
- 3) Big, bright 7" Android touchscreen, easier-to-use interface
- 4) 26 robust, long-life key fobs with security seals
- 5) Keys or key sets are individually locked in place
- 6) User, key, and access rights administration
- 7) PIN, Card, Fingerprint, Face ID access to designated keys
- 8) Keys audit and reporting capacity via screen/USB port/Web
- 9) Key reservation and application
- 10) Audible and visual alarms
- 11) Emergency Release System
- 12) Multi-system networking



## Part 2 K26 OVERVIEW

The Landwell K26 system uses touch screen technology for an easy, user-friendly interface. It does not require the use of a stylus or any other navigation device, to use the system simply click on the desired buttons with your finger.

### 2.1 Panel

From a structural point of view, K26 can be roughly divided into three areas: the keys storage area on the left, the User interaction area on the right, Rear power, and network interface on the back. There are 26 key slots in the keys storage area, each of them has an RFID reader, an electronic magnet lock, and a LED. The key slot is the basic unit in K26 caused its function of key monitoring, key controlling, and key locating. Besides, all keys will be locked inside K26's cabinet by an electric lock. Details are as follows:

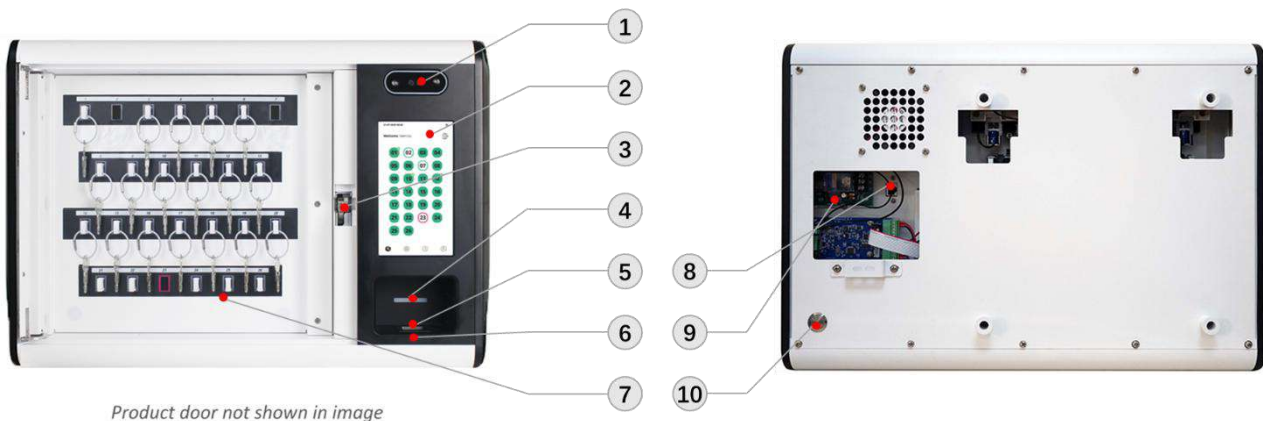


Figure 2-1 K26 panel (product door not shown in image)

- ① Facial reader – Register and identify users.
- ② 7" Touch Screen – Built-in Android OS, and provide user-friendly interaction.
- ③ Electric lock – Locking the cabinet door, controlled by Key or system apps.
- ④ Status Light – status of the system. Green: OK; Red: Error.
- ⑤ Fingerprint Reader – Collecting user fingerprints.
- ⑥ RFID Reader – External RFID reader for key fobs and user cards.
- ⑦ Key Slot – Key receptor slot strip.

Ethernet port – 10/100M adaptive Ethernet interface

Power port

Reset Button - Repower the system

## 2.2 The touch screen

### 2.2.1 Screen Saver

If the K26 system is not active for 30 seconds (or other settings), then the system will go into the “standby page”. To use the system again simply press anywhere on the touch screen.

### 2.2.2 Touch Command



Click - Selecting an onscreen button then immediately releasing will activate it.



Click & Hold - Selecting and holding certain directional buttons will cycle through menus and various options



Scroll: Swiping up and down on a list or menu will allow you to scroll through the various

## 2.3 Fingerprint Sensor

The high-security industrial-grade capacitive fingerprint in this system requires an adaptation period for its use, so don't have any concerns when it fails to succeed. Therefore, be sure to operate in a standardized manner, and you will get a higher success rate after getting used to it.

How to collect fingerprints correctly?

- Fingerprints with clear lines should be selected for the collection, and fingers should be kept clean;
- The finger should be in full contact with the collector without shaking the finger.
- The user should press slightly harder to make the fingerprint come into close contact with the collector and hold it for 1-2 seconds.



## 2.4 Network

There are two network-access methods for the K26 system: Ethernet and Wi-Fi. It is necessary to complete the network configuration when the system is first to run. And, you can change it while logging into the K26 system via administrator account later.

## 2.5 Wall mounting

**Notice:** Please do not leave spare keys in the box.

## 2.5.1 Planning the position

The Positioning of the key cabinet is a very important part of the installation process and is time well spent as poor planning will result in problems later down the line. From experience, things to take into account are:

- Who will use the key cabinet.
- 24 hours access. The key system should be positioned conveniently for the users.
- Security. The system is not designed as a high security safe, it's used to control and manage keys. The security of its location should be provided by the clients, so please place it in the view of the monitoring system.
- Indoor. We expect it to be used in ambient dry conditions rather than in exposed locations.
- Wall. The i-keybox systems can be quite heavy and therefore need a strong wall to fix to. And please ensure that any flammable materials, for example wall paper, are completely removed before fixing the cabinet to the wall.
- Others. In addition, the user's height, accessibility to the disabled, sunlight and other factors should also be considered.

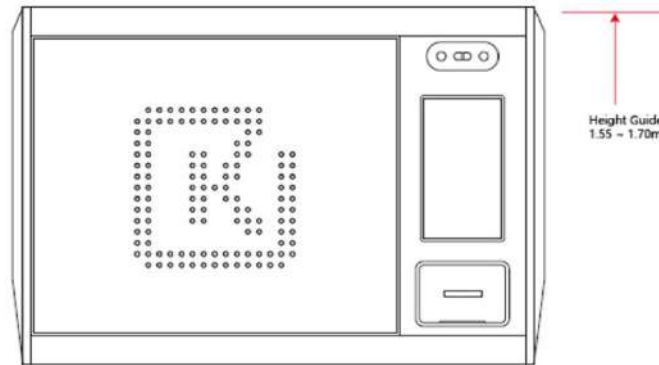
## 2.5.2. Preparation

Before installing the system, you should ensure that the following items are in place and working properly.

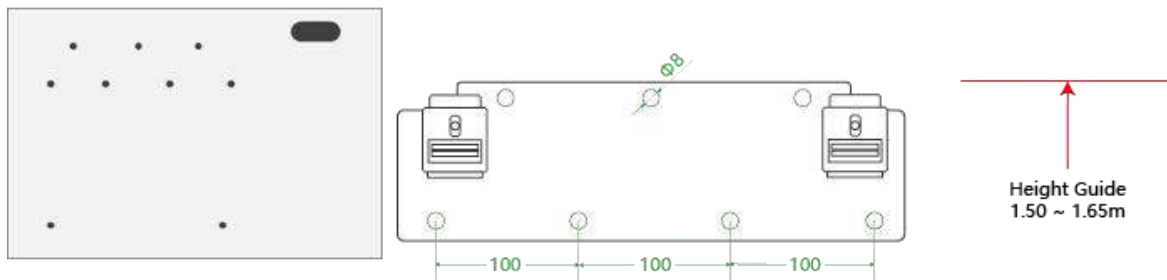
- A mains power supply.
- Mounting System Provided: wall bracket, 9 drywall anchors, 9 screws.
- Suitable Tools. Impact drill, 10mm drill bits, hammer, level ruler, pen or pencil, network crimper, screwdrivers, and so on.
- Networking. If you will use Ethernet to network the system, you need to install a convenient RJ45 wall socket near the system.

## 2.5.3 Wall installation

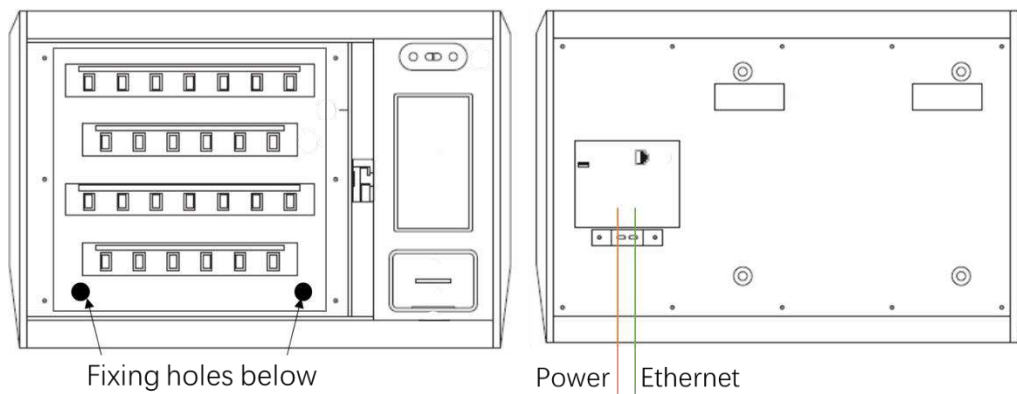
Step 1. Locate the unit on the wall where you want it to go. As a guide the top of the unit should be 1.55 – 1.70 meters from the floor and should no further than 1 meter from the mains spur.



Step 2. Mark and drill fixing holes and attach the wall bracket to the wall using the appropriate fixings.



Step 3. Pass the power cord (and network cable) through the hole and plug it into the internal Switch Power Supply and the Ethernet port as shown in [K26 Panel](#). Hang the key cabinet firmly on the bracket, and attach it to the wall. As shown in this image.



## 2.5.4 How to dismantle

Removal and installation are inverse processes.

## 2.6 Power the System

The K26 system should be connected to an electricity supply. It's suggested that connect the system to a UPS backup power. An optional battery backup will maintain the system in the event of power interruptions

### 2.6.1 Power Parameters of K26

|                   |                                    |
|-------------------|------------------------------------|
| Power Supply      | Input: 100-240V AC, Output: 12V DC |
| Power Consumption | 24W max, Typical 10W idle          |

### 2.6.2 Using UPS backup power

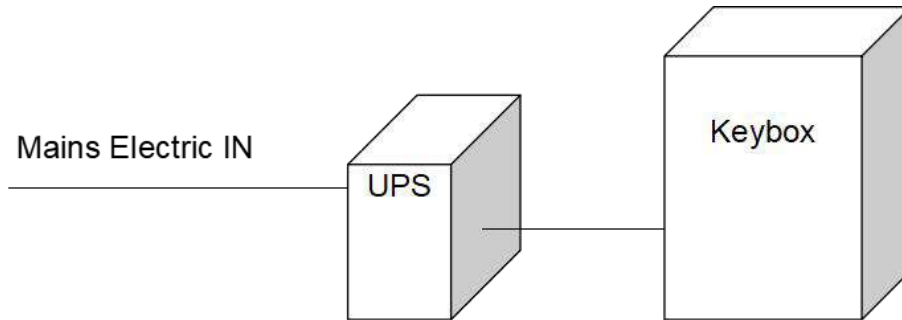


Figure 2-6-2 UPS for K26 key box

### 2.6.3 Using battery

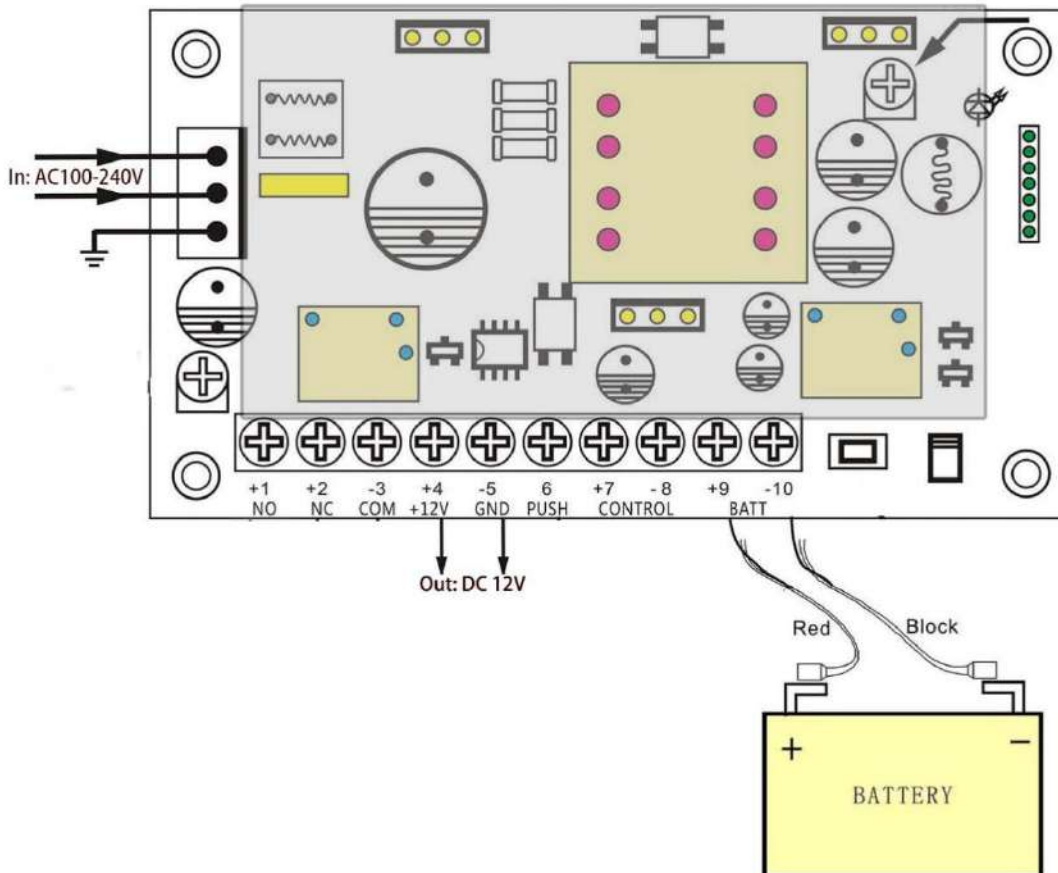


Figure 2-6-3 Power Supply

## Part 3 KEY FOB

Individual keys, key sets, key fobs, or access cards are permanently attached to a key fob with a robust security seal. The key tag is a bullet-shaped device that carries a unique electronic ID. Each key fob is assigned a specific port inside the key cabinet and locked in place until released by an authorized user.



## Part 4 USING THE SYSTEM

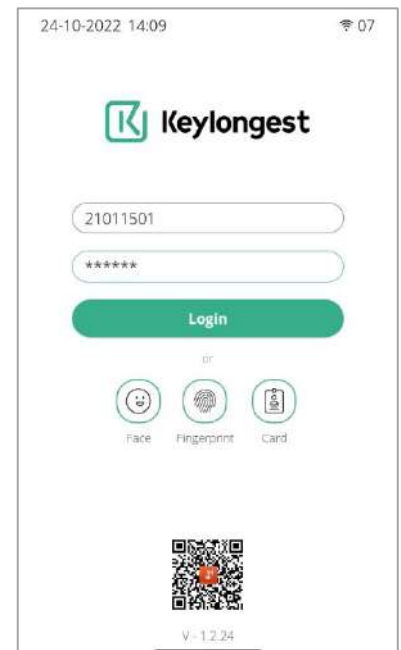
To use the K26 system, a user with the correct credentials must log in to the system.

### 4.1 logging into the system

There are four basic credentials to log in to the K26 system:

- ID + Password;
- ID + Fingerprint;
- Staff Card;
- Face Recognition;

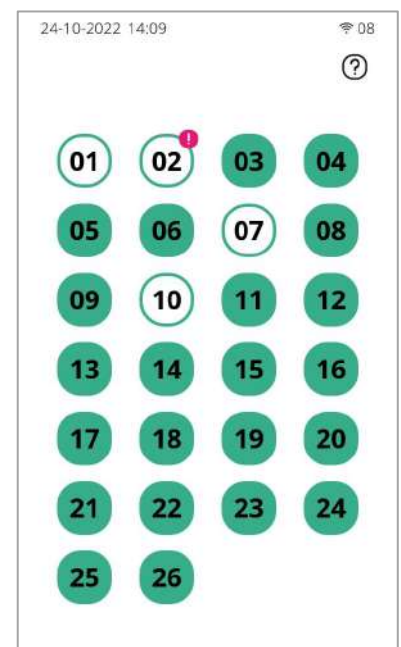
Administrators can turn these options on and off, or combine two of these options. [Learn now!](#)



### 4.2 Removing & returning keys

**Removing a key** is a handed operation.

1. Log in to the system.
2. The screen will show which keys you can access.



**Authorized** Keys will be illuminated **green**. **Unauthorized** keys will be illuminated **red**.

3. Press the icon on the screen for the key you wish to remove
4. The door will open.
5. The system will unlock the Key-Fob illuminated **blue**.
6. Remove the key and close the door.

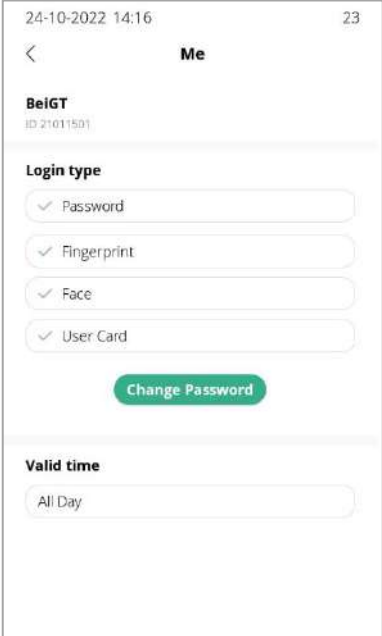
### Returning a Key

1. Swipe the Key-Fob on the [external RFID reader](#).
2. The door will open.
3. The position illuminated **blue** indicates the correct slot.
4. Insert Key-Fob into the matching slot.
5. Close the door.

**Note:** You must return the key to the correct receptor slot. If not, the system screen will notify you and request that you remove the key and return it to the correct slot as indicated. The positions in the system will also illuminate.

## 4.3 Chang Password

Users can change the password by themselves in the [My] menu.



The screenshot shows a mobile application interface for a user profile. At the top, the date and time are 24-10-2022 14:16, and the user's name is 'Me'. Below this, the user's name 'BeIGT' and ID 'ID 21011501' are displayed. The 'Login type' section has four options: Password, Fingerprint, Face, and User Card, each with a checkmark. A green 'Change Password' button is located below these options. The 'Valid time' section has one option: 'All Day'.

## Part 5 ADMINISTRATOR MENUS

All the settings, except the registration of keys, user card, fingerprint, and facial features, can be realized through the website or K26. These menus will be visible to administrators and they are laid out as follows:

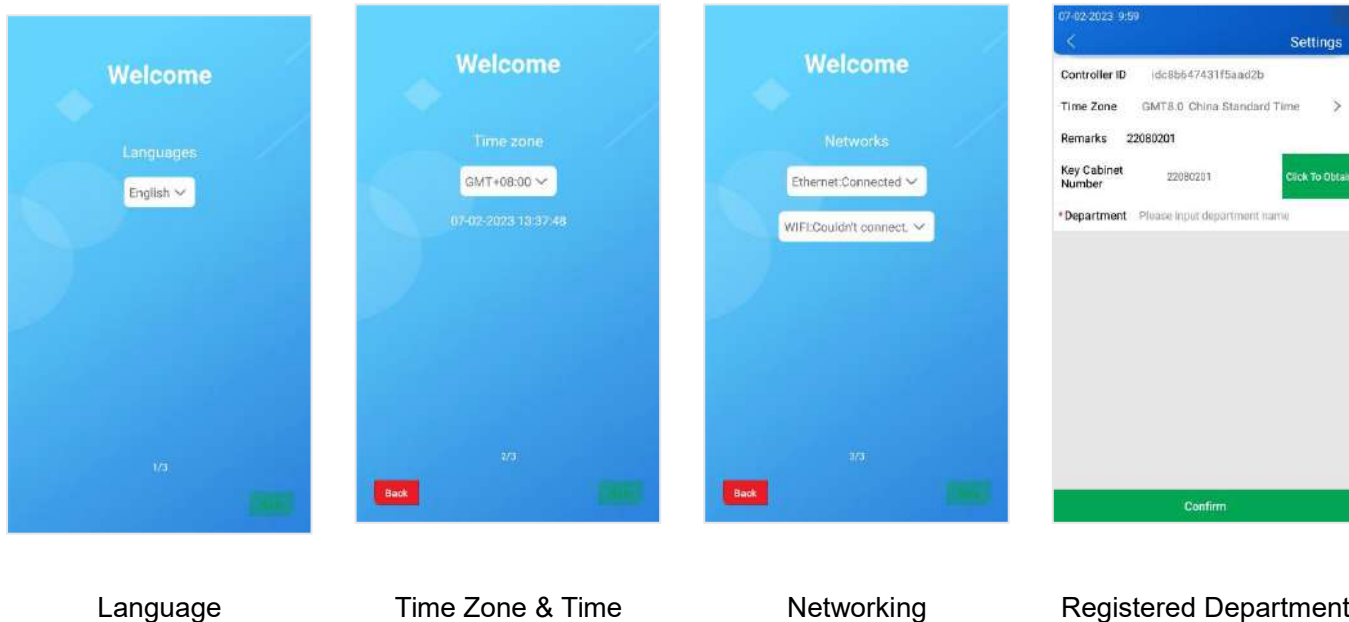
Table 5 - List of Administrator Menus

| v  | Level-1                | Level-2                    | Item   |
|----|------------------------|----------------------------|--|
| 1  | Key                    | Registration               | Register key tags  |
| 2  |                        | Editing                    | Edit keys' name, usage time (length or range)                      |
| 3  |                        | Permission Allocation      | Who can access the key   |
| 4  |                        | Lock                       | Freeze / Unfreeze a key  |
| 5  | User                   | Add                        | Add a new user   |
| 6  |                        | Edit                       | Edit users' names, credentials, permissions, and time-table        |
| 7  |                        | Delete                     | Delete a user  |
| 8  |                        | Lock                       | Freeze / Unfreeze a user   |
| 9  |                        | Permission Group           | Add, Edit, Delete a permission group                               |
| 10 | Multi-Verification     | Multi-Verification         | Add, edit, delete multi-verification relationships                 |
| 13 |                        | Turn on/off                | Whether to activate this feature while taking or returning the key |
| 14 | Event                  | Event                      | Add, edit, delete reasons to key use                               |
| 16 |                        | Turn on/off                | Whether to activate this feature while taking the key              |
| 17 | Parameters<br>Settings | Screen Brightness          | Adjust screen brightness   |
| 18 |                        | Sleep                      | The countdown of the standby page                                  |
| 19 |                        | Login History              | Whether the login history is visible                               |
| 20 |                        | Remote control ... prompt  | Whether to click on-site when remotely controlled                  |
| 21 |                        | Key preview                | Whether the key status is visible when not logged in               |
| 22 |                        | Standby page               | Three types: Clock, default picture, or custom picture             |
| 23 |                        | Home logo                  | Custom home logo   |
| 24 |                        | Snap a picture ... keys?   | Snap a picture when taking & returning keys?                       |
| 25 |                        | Sound                      | Voice + / -, Silent mode, Card reading voice, and Tap sound        |
| 26 |                        | Door open overdue          | Maximum opening time   |
| 27 |                        | Login settings             | What user credentials or their combinations are activated          |
| 28 |                        | Emergency PIN              | The administrator takes out all the keys in case of an emergency   |
| 29 |                        | Cabinet Name               | Edit the Key system name   |
| 30 |                        | Software Update            | Update checking  |
| 31 |                        | Language                   | Change the software language                                       |
| 32 |                        | Reset                      | Clear local data and re-register the system                        |
| 33 |                        | Transfer                   | Switching application mode to standalone or networked              |
| 34 |                        | System                     | Return Android OS  |
| 35 | About                  | View system configurations |  |



## 5.1 First Run

When the system is first started, the required parameters include language, network, time zone, time, and organization name on the network. as follows:

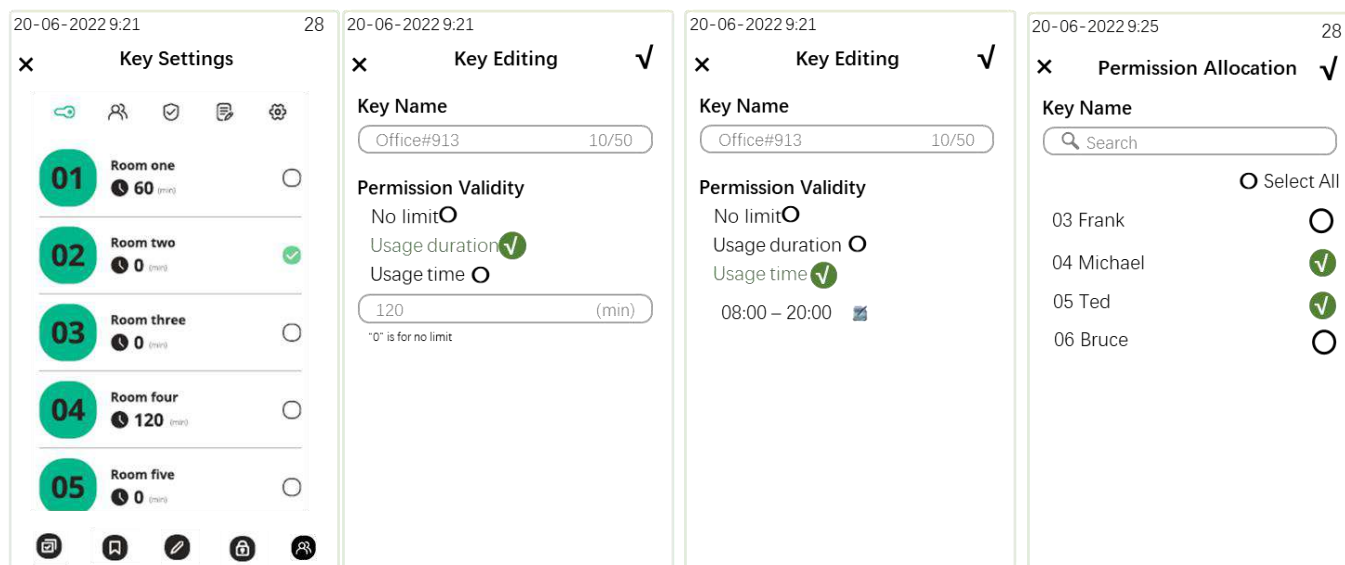


Language

Time Zone & Time

Networking




Registered Department





## 5.2 Keys

Figure 5-2 K26 Keys

Functions:

-  [press any key and hold on for 1s, then] Select all
-  Register selected / all key tags
-  Edit keys' name, usage time (length or range)

-  lock/unlock the key
-  Who can access it






In other cases:

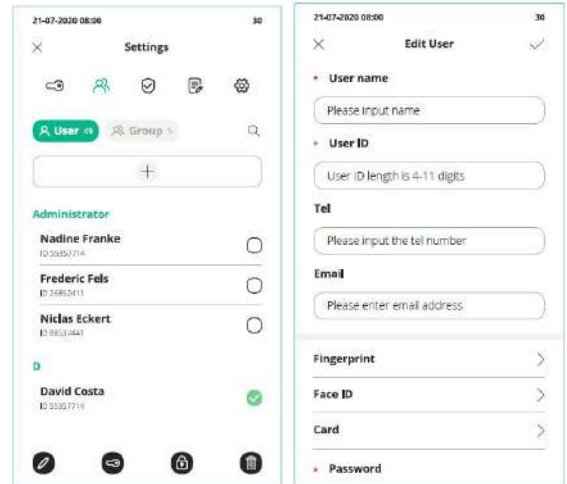
- Deregistration: Click the registration key and then close the door directly without inserting any key-tag.
- Key-tag is damaged: Register the single key-tag with a new one.

## 5.3 Users

Press and hold for 1s to edit a user.

Functions:

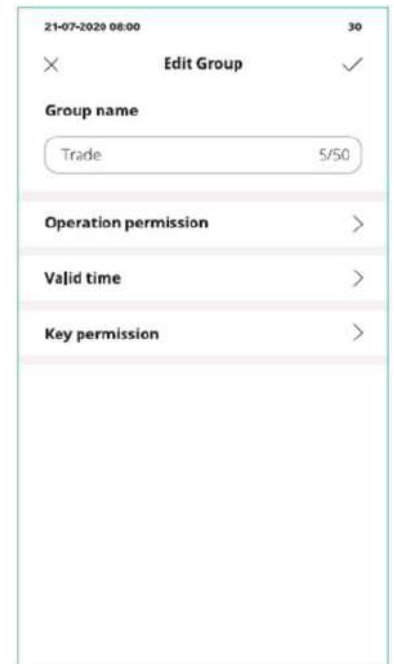
-  Add a user
-  Edit the selected user
-  Edit key permissions for the selected user
-  Lock / unlock selected user
-  Delete selected user



## 5.4 Permission Group

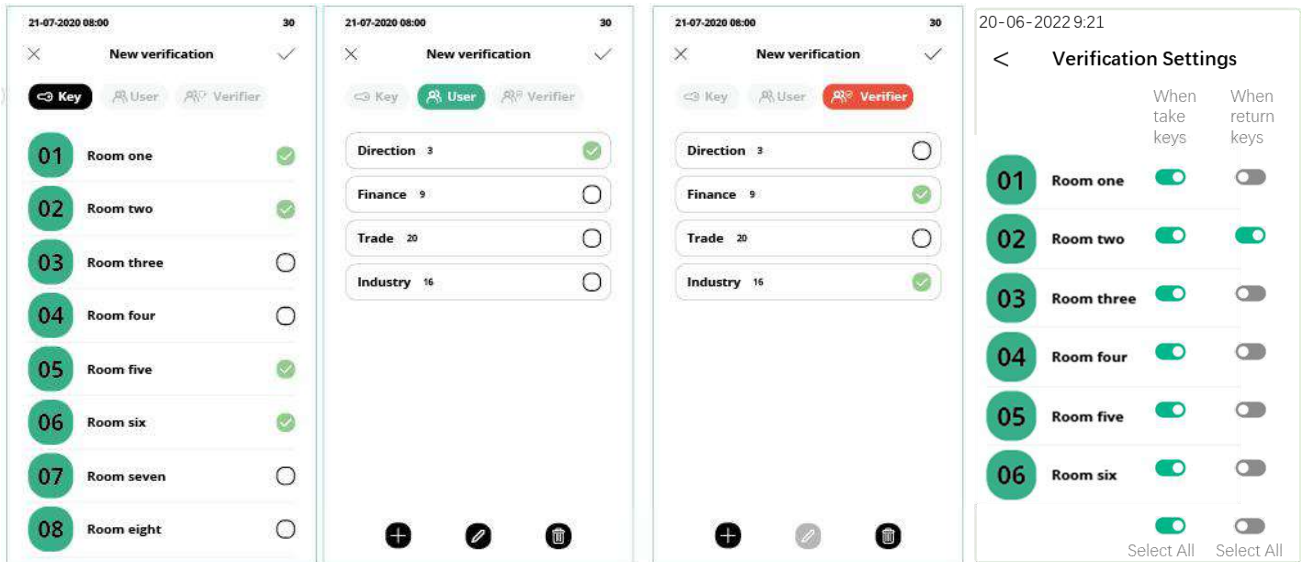
Permission Group, a set of users with the same operation authority and the same key authority.

- ✧ **Operation permission** - What menus can group members access?
- ✧ **Valid time** - When can group members use the keys?
- ✧ **Key permission** - What keys can group members use?



## 5.5 Multi-verification

Multi-verification gives multiple protection of key safety. It means that if one user wishes to use a key, he or she is required to obtain another user's permission or finalization of the request, the key will then be released. Important keys that lead to vital assets usually is suggested to use the



multi-verification function.

Figure 5-5 K26 Multi-verification

Three factors: What keys (**Keys** group), used by whom (**User** group), verified by whom (**Verifier** group).

Activate it: Which keys enable this feature, when removed or returned?

**E.g:**

a) One person to authorized

| Key | User Group | Verification Group |
|-----|------------|--------------------|
| 8   | User-A     | Veri-B             |

Removing key [8] by any member of the group [User-A] should be verified by any member of the verification group [Veri-B].



b) Two persons to authorized

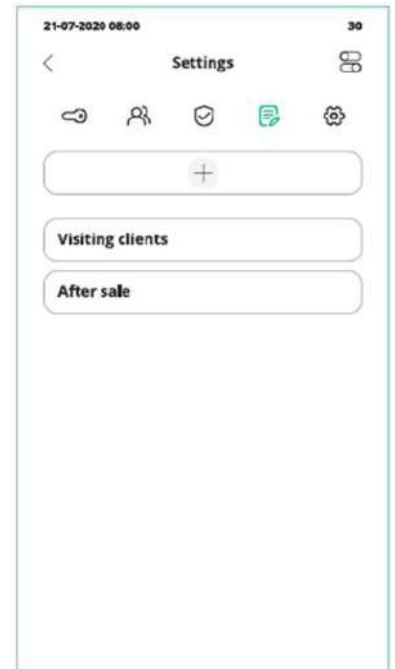
| Key | User Group | Verification Group |
|-----|------------|--------------------|
| 8   | User-A     | Veri-B             |
| 8   | User-A     | Veri-C             |

Removing key [8] by any member of the group [User-A] shall be verified by any member of [Veri-B] followed by any member of [Veri-C].

## 5.6 Events

The event, the purpose of using the key.

-  Add a new event
-  what keys need to activate the event option.



## 5.7 Report


Reports allow you to view all the transactions and events that have occurred in the system. Through the report, you can easily understand all records:


Who's got a key?

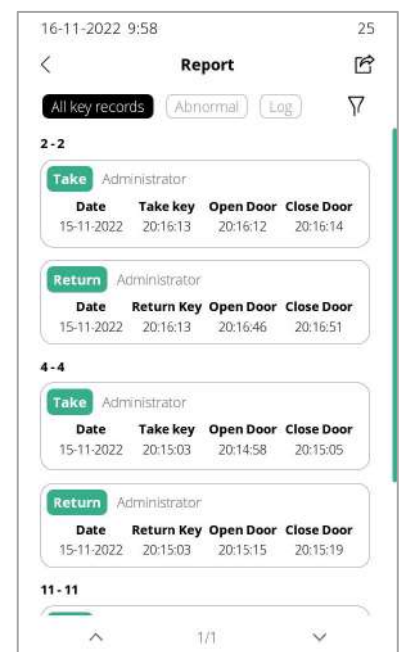
Who's had a key?

What abnormal records occurred?

System events log?

 Filtering records by key, user, etc.

 Exporting reports as Excel files via USB devices, or Emails (Email option only available in stand-alone version)

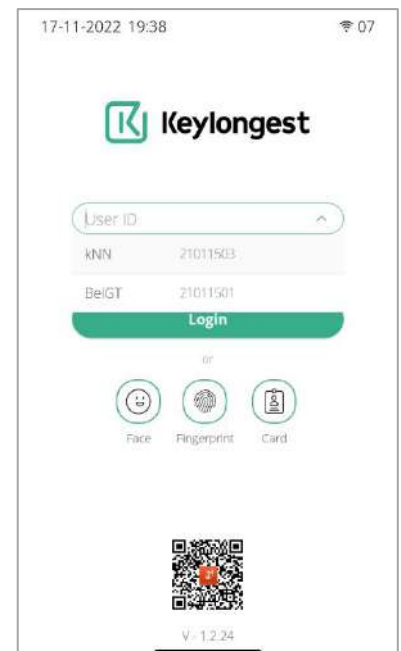


## 5.8 Parameter Settings

For an explanation of the options refer to this [list](#).

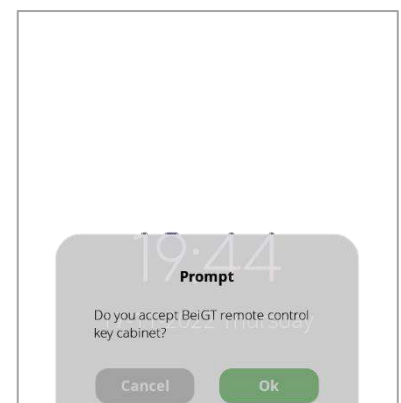
### 5.8.1 Login History

The system will remember you when the option is enabled, as shown.



### 5.8.2 Remote Control Prompt

With this option turned on, the K26 system will pop up a window for confirmation after being controlled by off-site admins, as shown.



### 5.8.3 Key Preview

With this option turned on, any user can get an overview of keys from the screen, as



shown.

### 5.8.4 The Standby Page and Home Logo

There are three types of standby pages:

- Time Clock
- K26 Picture default
- Custom ( $\leq 5$  pictures)

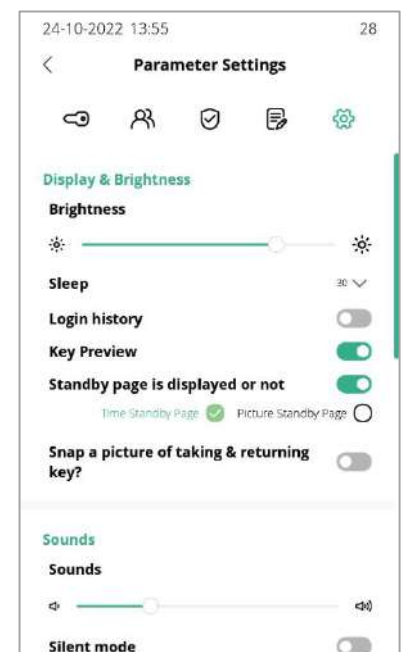
Steps for custom standby page:

- Make a standby picture with 600\*1024 pixels;
- Copy it to the folder ".../keybox/standby/" of a USB memory stick;
- [Settings] -> [standby page display or not] > [Picture Standby Page].
- Insert the USB stick into the port inside the box, and upload the file as follow the system's guidelines.

You can also change the homepage logo in the same way, just change the path to ".../keybox/img".

### 5.8.5 Snap pictures while key removal & return

With this option turned on, the K26 system will capture an image when the key is removed or returned.

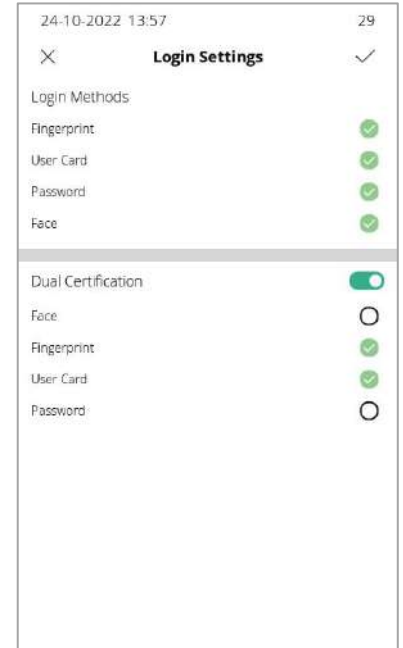


## 5.8.6 Login Settings

What user credentials are activated?

And which pair of credentials combination?

*As shown in the figure on the right, the user should provide both fingerprint and card credentials to access the system.*



## 5.8.7 Cabinet name

Edit the K26 system name, it will be shown at:

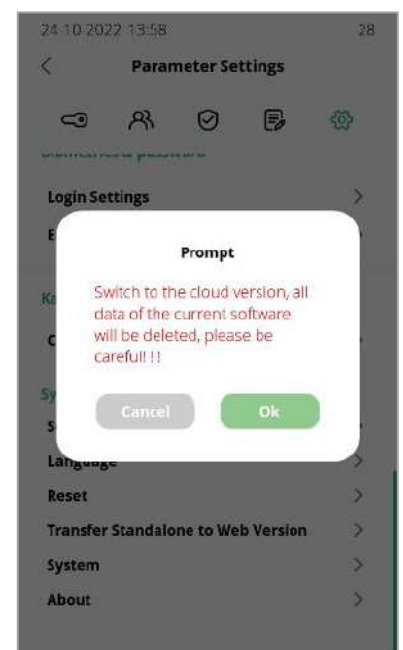
- The first page after entering the K26 system
- Web management software
- Mobile Apps

## 5.8.8 Switch between Standalone and Networked

Stand-alone: Only be managed locally, almost all of its features remain available without a network connection.

Networked: It can also be managed on the web, mobile phone, or tablet. When the network is disconnected, the removal and return of keys will not be affected, and the system setting features will not be available.

*Notice: All local data will be cleared when the mode changed.*



### 5.8.9 Language

Set the language of the app.

The Chinese and English app contains voice packs by default, and other languages need to click the voice icon to download.



### 5.8.10 System

Return to Android Operating System.

You can set the network, time and region, language, and more.



## Part 6 WEB-BASED MANAGEMENT

Keylongest key management system is a web management software with a B/S structure, which realizes multi-system network management so that you don't need to install additional tools and extensions on your computer. As long as you need a web browser, you can easily manage it, providing you with More convenience.

### 6.1 Features Layout

Table 6-1 List of Web-based key management software

| No. | Menus     | Items            | Detailed / Explanations  |
|-----|-----------|------------------|--|
| 1   | Home Page | Key Overview     | Get an overview of all keys                                    |
| 2   |           | Remote Control   | Remote control by off-site administrator to take / return keys |
| 3   |           | Reserve Keys     | Adding a key reservation to avoid being removed by others      |
| 4   |           | Apply for Keys   | Apply for key permissions from the administrator               |
| 5   |           | Application info | View existing applications                                     |



|    |                |                    |   |   |
|----|----------------|--------------------|---|---|
| 6  | Report         | Key Records        | who removed what keys and when  |   |
| 7  |                | Abnormal Records   | System Abnormal Events  |   |
| 8  |                | Operation Logs     | admin history report  |   |
| 9  |                | Mailbox Records    | mail sending report   |   |
| 10 |                | Exporting logs     | report download history   |   |
| 11 | Settings       | Department         | Add, edit, and delete a sub-department  |   |
| 12 |                | Cabinet            | Rename a K26 system<br>Set the max time for door opening<br>Transfer a cabinet to another department<br>Export a list of all cabinets that belong to the current department |   |
| 13 |                | Key                | Rename a key<br>Set keys' available time<br>freeze / unfreeze keys<br>Enable or close the current key's event<br>Enable or close the current key's multi-verification       |   |
| 14 |                | Permission Group   | Add, edit, and delete a permission group(menu module & key permission)  |   |
| 15 |                | User               | Add, edit, or delete a user<br>User type: system admin, admin, common user, custom type<br>Lock / unlock a user account   |   |
| 16 |                | Key Permission     | Set common user's key permission  |   |
| 17 |                | Multi-verification | Add/delete/edit multi-verification for current key/group  |   |
| 18 |                | Event              | Add / edit/delete reasons for taking keys   |   |
| 19 |                | Others             | My Password   | Changed   |
| 20 |                |                    | My Approval / Application   | History of my (current user) approval/application |
| 21 | My Reservation |                    | History of my (current user) reservation  |   |

## 6.2 Home Page

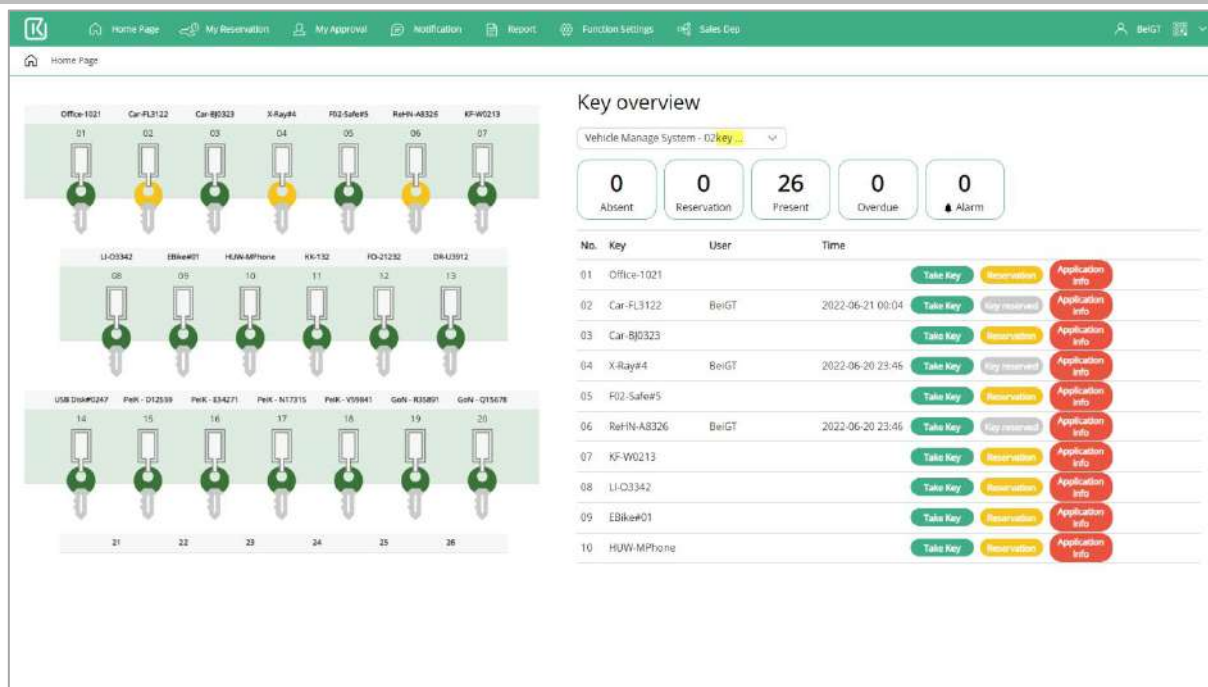


Figure 6-2 Home Page

As shown in the figure above, the left side of the home page shows the key status of the current K26, including the status of the present, the status of permission, the status of reservation, the status of registration, and so on.

- Take/return key: The K26 system will open the door and release the key lock [after your confirmation](#), so please remove/return the key ASAP.
- Reservation: Make an appointment for the key within the existing authority.
- Application: Apply for keys without permission.
- Application info: View applications for the current keys. **Only visible to administrators.**

## 6.3 Function Settings

### 6.3.1 Department

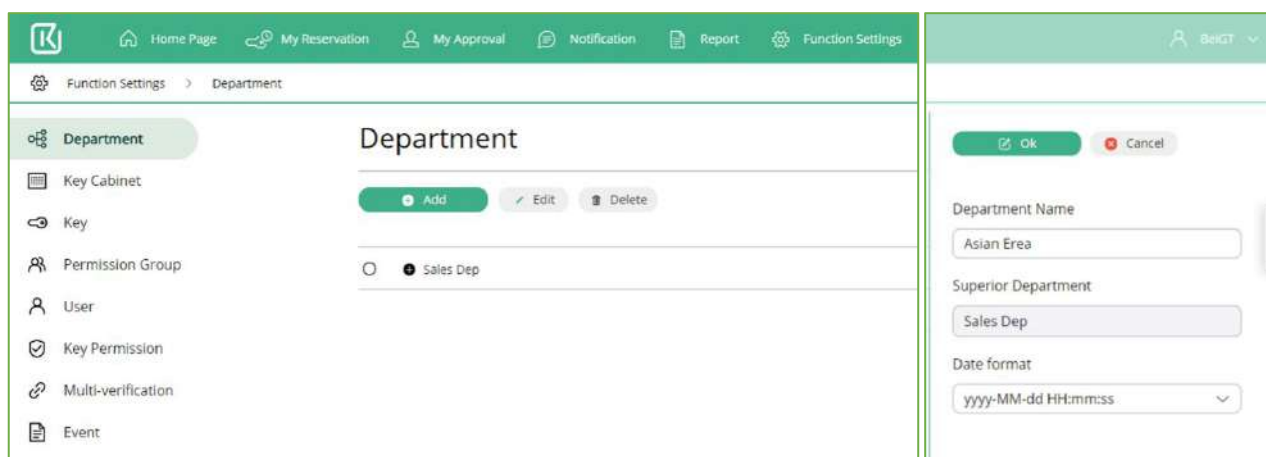


Figure 6-3-1 Department

**[Add]**, Add a sub-department to the current department. The items that can be edited include the name and time format of the sub-department.

**[Edit]**, Edit the name and time format of the current department.

**[Delete]**, Delete the current department.

**[Alarm Option]**, Turn on and off alarm options for the selected department, details as shown in table below.

Table 6-3-1 List of the Alarm Options

| No. | Alarm Options                            | Description   |
|-----|--|---|
| 1   | Door Open Illegally                      | The door opening process caused by non-system commands, usually is door opening using the emergency key ;   |
| 2   | Door Open Overdue                        | When taking out the key, returning the key but forgetting to close the cabinet door, the system will send an alarm (audio, email) after the set time. |
| 3   | Login Abnormal                           | Wrong password entered three times and more   |
| 4   | Door Open abnormally                     | There is no response to the system's door open command  |
| 5   | Key Taken Overdue                        | The key was not returned on time  |
| 6   | Reserved Key was taken                   | The key you reserved was taken by administrators  |
| 7   | Reserved key was return                  | The key you reserved was returned   |
| 8   | Other apply for overlapping time periods | Whether the system allows two applications for a key to overlap in time.  |

## 6.3.2 Key cabinet

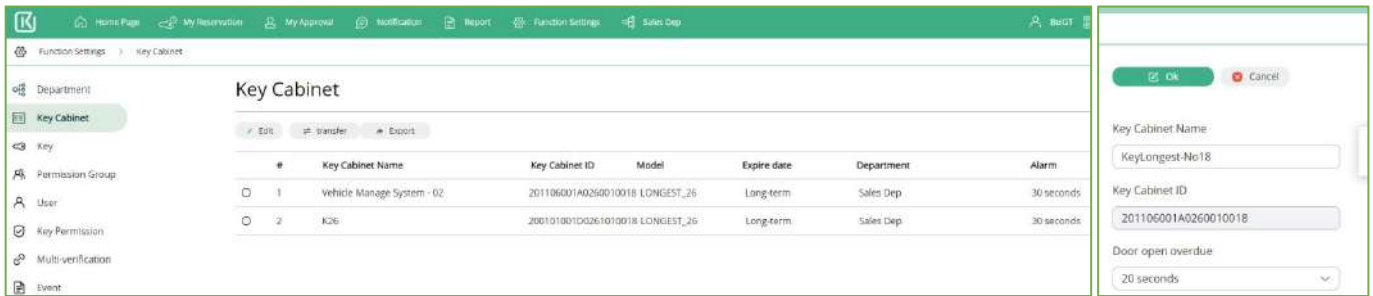


Figure 6-3-2 Key Cabinet

**[Edit]**, Edit Key-cabinet's name and maximum opening time (auto-sync to device).

**[Transfer]**, Transfer current cabinet to other (sub) department.

**[Export]**, Export key cabinets list to an excel file.

## 6.3.3 Key

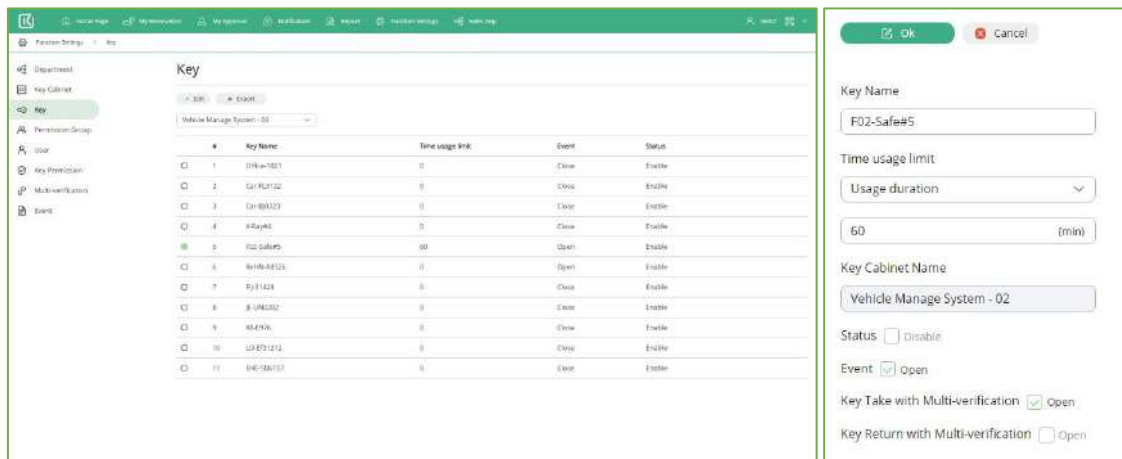


Figure 6-3-3 Key

When keys are registered on k26, keys information will be automatically displayed on the web page.

### [Edit a Key]

- Rename it
- Set when it's available. There are three types of "Time usage limit": (1) No limit; (2) Duration; (3) Use time.
- Freeze and unfreeze it.
- Turn the "Event" feature on/off.
- Turn the "Multi-verification" on/off while removing it.
- Turn the "Multi-verification" on/off while returning it.

**[Export]** - Export keys list to an excel file.

### 6.3.4 Permission Group

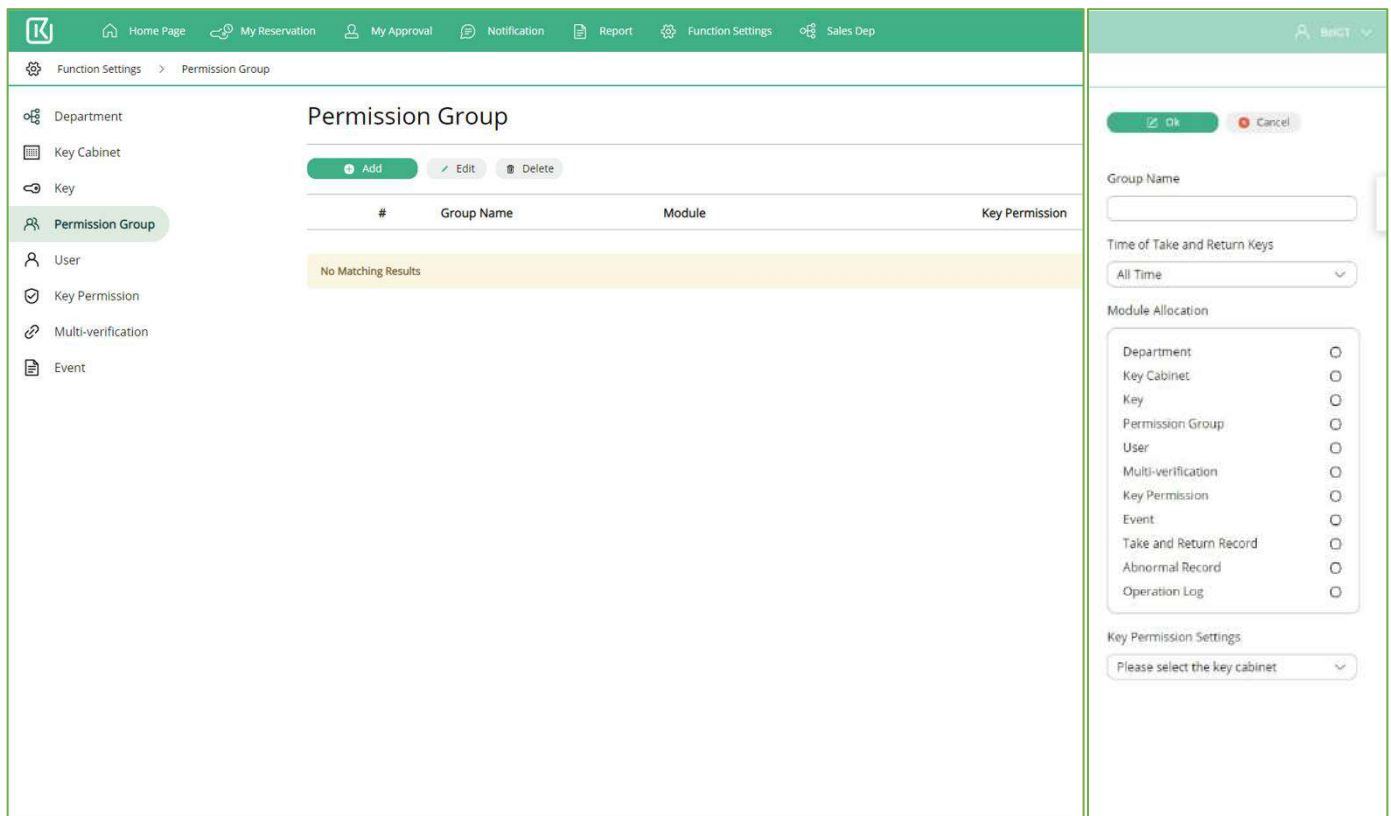


Figure 6-3-4 Permission Group

Add, edit, delete a permission group (menu module & key permission)

### 6.3.5 User

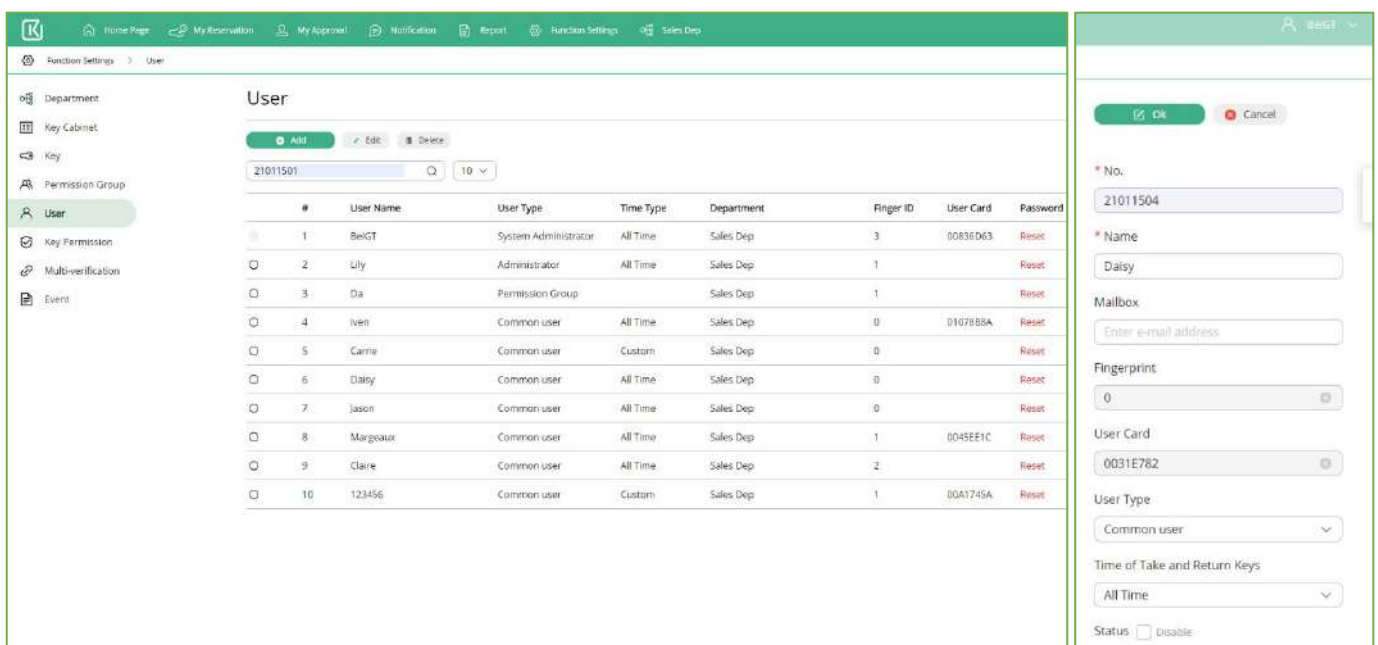


Figure 7-3-5 User

When users' fingerprints, faces, and cards are registered on k26, all this information will be automatically synced on the web server.

Add / edit users' information, including:

- \*User ID, 4~12 chars (a~z, 0~9, “@”, “\_”, “.”), can not be updated after adding.
- \*User Name, no more than 50 characters.
- \*Password, 3~11 letters, digits and special characters (“@”, “\_”, “.”), only allowed to be changed by himself/herself or to be reset as 333 by the administrator. When it was forgotten, please do as [this guide](#).
- User Type, there are 4 types, as the below list.
- Access time, when can he/she access the keys?
- Status, lock / unlock this user account.

Table 6-3-5 List of user types

| User Type                   | Menu module   | Key permission       |
|-----------------------------|---|----------------------|
| <b>System Administrator</b> | All   | All                  |
| <b>Administrator</b>        | All, except creating an administrator account   | All                  |
| <b>Common User</b>          | [Function Setting] Forbidden  | set by administrator |
| <b>Permission Group</b>     | All permissions of menus and keys are Inherited from the selected group, and three roles for keys including: (1) Normal use only, (2) Application only, (3) Approval. Means that, although this group has access to a particular key, those users marked as [Application only] should not be able to access this key until the submitted application is approved. |                      |

### 6.3.6 Key permission

Function: Set who can access which keys. The system allows configuring key permissions from both user and key perspectives

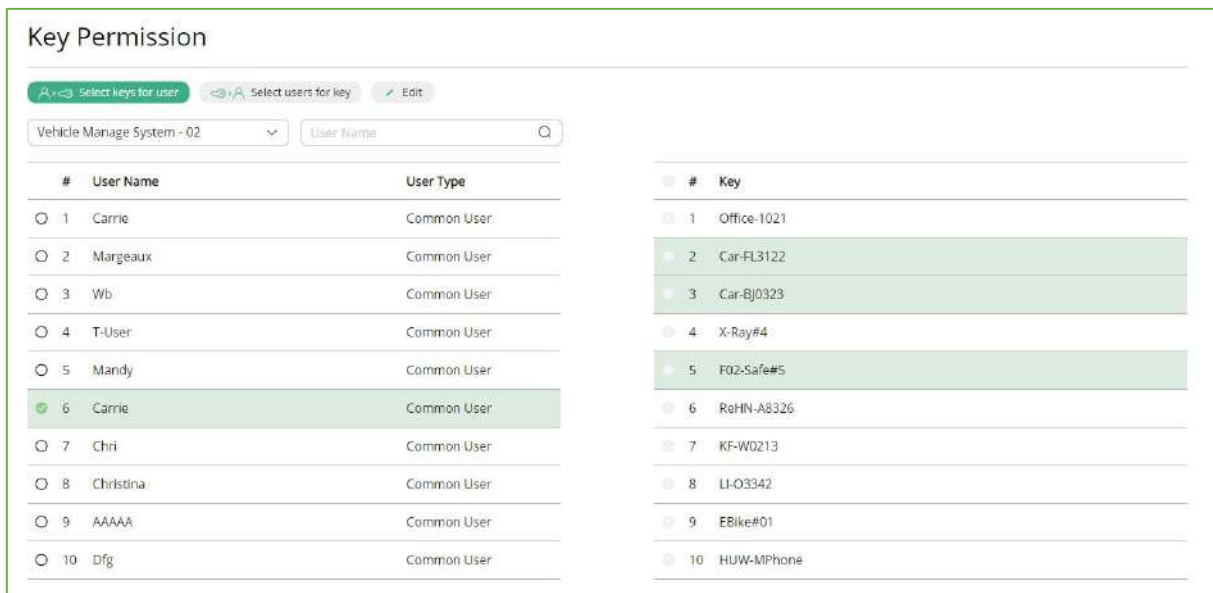


Figure 6-3-6(a) select keys for a user

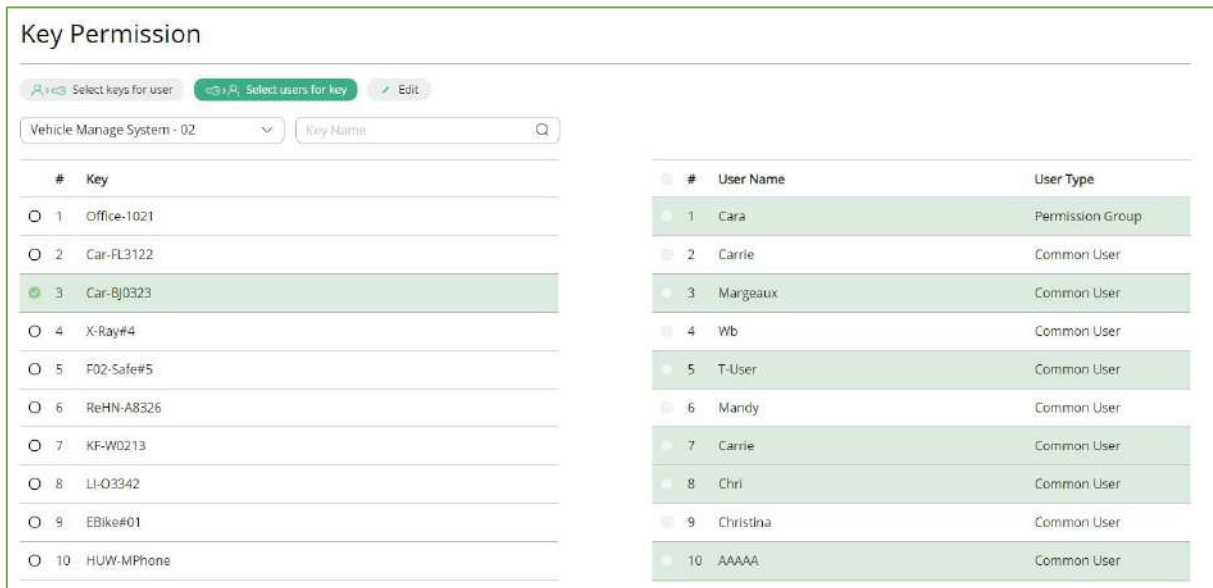


Figure 6-3-6(b) select users for a key

### 6.3.7 Multi-verification

Multi-verification gives multiple protection of key safety. It means that if one user wishes to use a key, he or she is required to obtain another user's finalization. Important keys that lead to vital assets usually are suggested to use the multi-verification function.

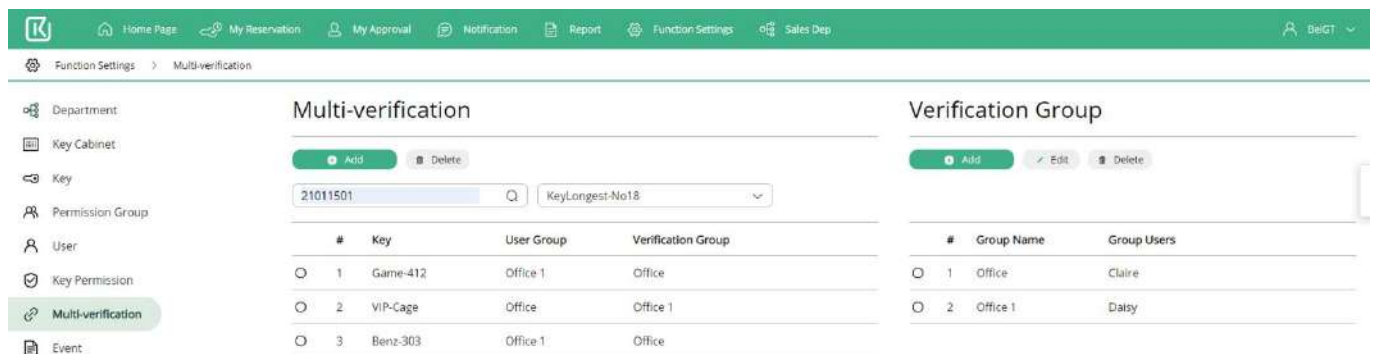


Figure 6-3-7 Multi-verification

The persons will not be allowed to remove the preset key(set) unless one of the preset person(s) login to K26 to provide proof, it's similar to the Two-Man Rule. There are three factors:

- ✓ What keys? - **(Keys group)**
- ✓ used by whom? - **(User group)**
- ✓ verified by whom? - **(Verifier group)**

And do not forget to activate it in [\[key settings\]](#)

**E.g:**

a) One person to authorized

| Key | User Group | Verification Group |
|-----|------------|--------------------|
| 8   | User-A     | Veri-B             |

Removing key [8] by any member of the group [User-A] should be verified by any member of the verification group [Veri-B].

b) Two persons to authorized

| Key | User Group | Verification Group |
|-----|------------|--------------------|
| 8   | User-A     | Veri-B             |
| 8   | User-A     | Veri-C             |

Removing key [8] by any member of the group [User-A] shall be verified by any member of [Veri-B] followed by any member of [Veri-C].

### 6.3.8 Event

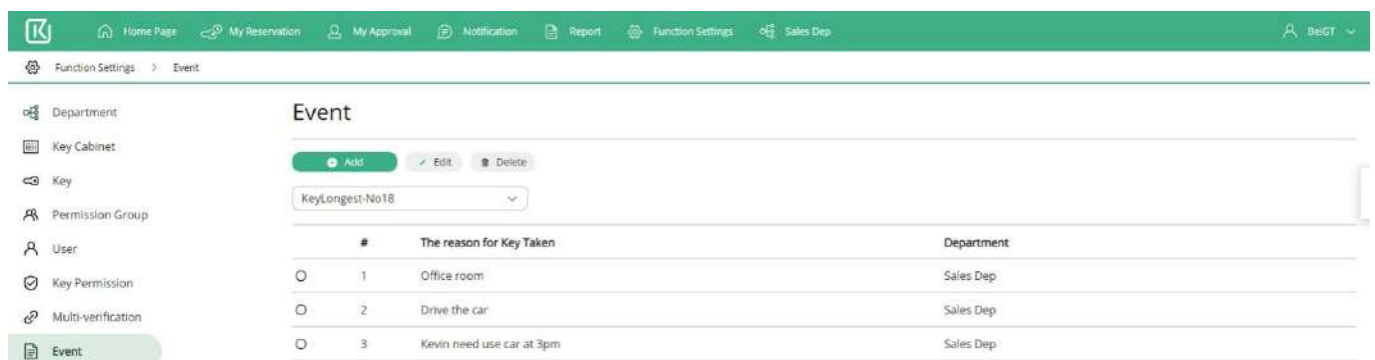


Figure 6-3-8 Event

Function: Preset several reasons for key use.

And do not forget to activate it in [\[key settings\]](#)

## 6.4 Reports

There are two types of records and three types of logs. You can filter the required data according to the specified conditions, and export the report in excel or pdf file format.



## 6.4.1 Key Record

The screenshot shows the 'Take and Return Record' page. The table lists the following records:

| Key          | Key Cabinet Name    | Date       | Time     | User    | Status              | Image |
|--------------|---------------------|------------|----------|---------|---------------------|-------|
| B-LI-03342   | Vehicle Manage S... | 2022-11-17 | 19:57:16 | BeiGT   | Take                |       |
| 3-Car-BI0329 | Vehicle Manage S... | 2022-11-11 | 14:15:11 |         | Emergency Key Taken |       |
| 7-KF-W0213   | Vehicle Manage S... | 2022-11-11 | 11:58:17 | Margosa | Take                |       |
| 7-KF-W0213   | Vehicle Manage S... | 2022-10-21 | 09:46:09 | BeiGT   | Door Open Overdue   |       |

The details panel on the right contains the following information:

- Cancel
- Key: LI-03342
- Key Cabinet: Vehicle Manage System - 02
- Open Time: 2022-11-17 19:57:08
- Key Taken Time: 2022-11-17 19:57:16
- Door Close Time: 2022-11-17 19:57:17
- Take door open overdue: No
- User of Key Taken: BeiGT
- Key Taken Verification:
- The reason for Key Taken:
- Not returned

Figure 6-4-1 Key usage record and details

## 6.4.2 Abnormal record and processing

The screenshot shows the 'Abnormal Record' page. The table lists the following records:

| Key Cabinet Name           | Key Cabinet ID       | Date       | Time     | Status                    | Result  | Details |
|----------------------------|----------------------|------------|----------|---------------------------|---------|---------|
| Vehicle Manage System - 02 | 201106001A0260010018 | 2022-11-18 | 12:53:11 | Key cabinet offline       | Pending |         |
| Vehicle Manage System - 02 | 201106001A0260010018 | 2022-11-18 | 12:06:52 | Key cabinet offline       | Pending |         |
| Vehicle Manage System - 02 | 201106001A0260010018 | 2022-11-18 | 05:01:46 | Key cabinet offline       | Pending |         |
| Vehicle Manage System - 02 | 201106001A0260010018 | 2022-11-18 | 02:28:11 | Key cabinet offline       | Pending |         |
| Vehicle Manage System - 02 | 201106001A0260010018 | 2022-11-17 | 19:37:15 | Return incorrect location | Pending |         |
| Vehicle Manage System - 02 | 201106001A0260010018 | 2022-11-17 | 19:36:47 | Return incorrect location | Pending |         |
| Vehicle Manage System - 02 | 201106001A0260010018 | 2022-11-15 | 20:09:30 | Key cabinet offline       | Pending |         |
| Vehicle Manage System - 02 | 201106001A0260010018 | 2022-11-15 | 20:04:30 | Key cabinet offline       | Pending |         |
| Vehicle Manage System - 02 | 201106001A0260010018 | 2022-11-15 | 15:24:41 | Key cabinet offline       | Pending |         |
| Vehicle Manage System - 02 | 201106001A0260010018 | 2022-11-13 | 03:00:40 | Key cabinet offline       | Pending |         |

The processing panel on the right contains the following information:

- Processors: BeiGT
- Description: Done
- Attachment:
- Processing Done:  Yes  No

Figure 6-4-2 Abnormal record and processing

## 6.4.3 Operation log

The screenshot shows the 'Operation Log' page. The table lists the following records:

| User  | Date       | Time     | Terminal | Event                    |
|-------|------------|----------|----------|--------------------------|
| BeiGT | 2022-11-18 | 14:46:31 | Web      | PasswordLog in           |
| Sigma | 2022-11-18 | 14:44:58 | Web      | PasswordLog in           |
| BeiGT | 2022-11-18 | 14:44:35 | Web      | PasswordLog in           |
| Sigma | 2022-11-18 | 14:40:37 | Web      | PasswordLog in           |
| BeiGT | 2022-11-18 | 14:03:54 | Web      | PasswordLog in           |
| Sigma | 2022-11-18 | 13:40:00 | Web      | PasswordLog in           |
| BeiGT | 2022-11-18 | 13:39:29 | Web      | PasswordLog in           |
| Sigma | 2022-11-18 | 13:39:12 | Web      | PasswordLog in           |
| BeiGT | 2022-11-18 | 13:39:03 | Web      | ResetSigmaLogin Password |
| BeiGT | 2022-11-18 | 10:59:36 | Web      | PasswordLog in           |

Figure 6-4-3 Operation log

## 6.4.4 Mailbox Record

The screenshot shows the 'Mailbox Records' page. On the left is a navigation menu with options: 'Take and Return Record', 'Abnormal Record', 'Operation Log', 'Mailbox Records', and 'Export Log'. The main area contains a search bar and a table of records. The table has columns for Mailbox, Key Cabinet Name, Date, Time, Status, and Result. A details panel on the right shows information for a specific record, including 'Key Cabinet: KeyLongest-No18', 'Abnormal Type: Door Open Overdue', 'Alarm Time: 2021-03-20 09:08:24', 'Push Time: 2021-03-20 09:08:31', and 'Reasons for push failure: Service expires or no sufficient balance'.

| Mailbox          | Key Cabinet Name           | Date       | Time     | Status              | Result       |
|------------------|----------------------------|------------|----------|---------------------|--------------|
| 935245193@qq.com | Vehicle Manage System - 02 | 2022-11-11 | 14:21:55 | Door Open Overdue   | Push Success |
| 935245193@qq.com | Vehicle Manage System - 02 | 2022-11-11 | 14:14:55 | Door Open Illegally | Push Success |
| 935245193@qq.com | Vehicle Manage System - 02 | 2022-11-11 | 13:58:30 | Door Open Overdue   | Push Success |
| 935245193@qq.com | Vehicle Manage System - 02 | 2022-11-11 | 13:54:20 | Door Open Overdue   | Push Success |
| 935245193@qq.com | K26-3                      | 2022-11-05 | 06:22:15 | Login Abnormal      | Push Success |
| 935245193@qq.com | K26-3                      | 2022-11-03 | 06:21:47 | Login Abnormal      | Push Success |
| 935245193@qq.com | Vehicle Manage System - 02 | 2022-10-21 | 09:44:40 | Door Open Overdue   | Push Success |

Figure 6-4-4 Mailbox Record

## 6.5 Forgot the password

Steps:

[Forgot the password] -> [Email & Author-code] -> [Reset your password].



Figure 6-5 Reset password

Additionally, the password can be [reset by the administrator](#).

## Part 7 Applications for Cell Phone

### 7.1 How to obtain and activate the app

Scan the [Download QR Code] at the bottom of the screen of the K26 smart key cabinet through the mobile browser, and select the corresponding download link according to the mobile phone system type in the pop-up interface.

Other ways to obtain it: visit the WEB management website, scan the QR



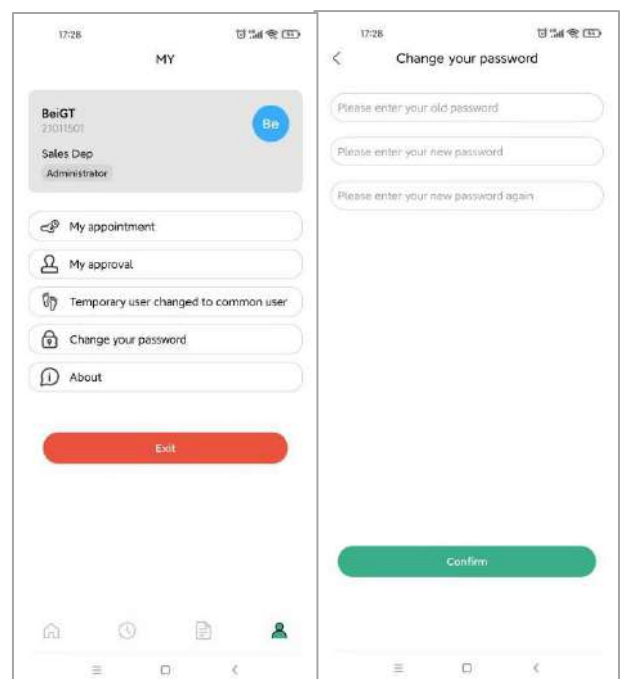
code at the bottom right of the page through the mobile browser, enter the download link, or click the QR code with the mouse to download the APP installation package to the PC, and then forward it to the mobile phone

After the software is running, directly enter the key cabinet ID or scan the QR code at the bottom of the key-cabinet screen, and then click [activate].

**Notice:** Users of IOS devices can search “intelligent key cabinet” on app store to obtain the app.

## 7.2 How to modify password

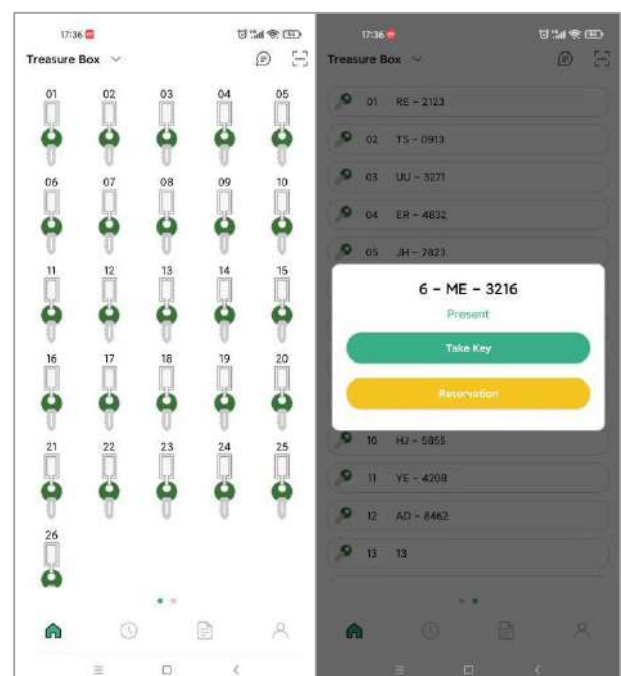
With the account and password provided by the administrator, log in to the system, and modify the password by yourself. Method: [My] > [Change your password].



## 7.3 Key Overview & Remote Control

(Select a system) Swipe the screen left and right to view the basic information of the keys in the key cabinet of the selected current department and whether they are available.

[Take/Return Key] - Remote control by off-site



administrator to take / return keys.

## 7.4 Reservation and Approval

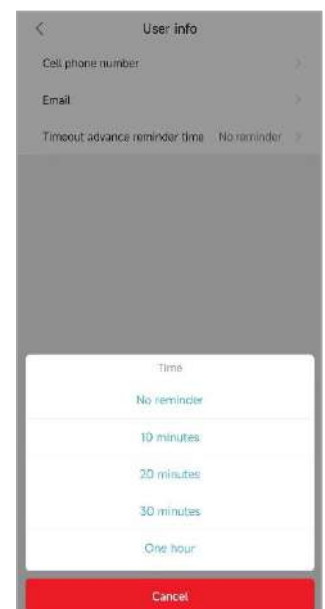
A key reservation is an appointment for the use of a specific key within the authority. After the reservation is successful, the key can only be taken out by the reservation person and the system administrator within the set time.

Method: On the key overview page, click on the key location and select [Reservation] in the pop-up interface.

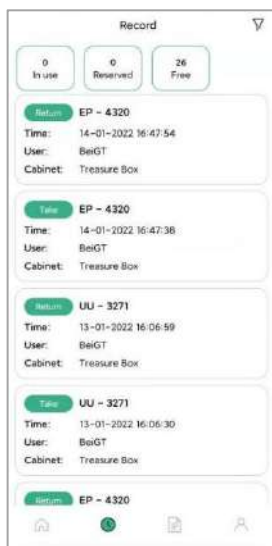
## 7.5 Personel Info

Any user can set his/her mailbox and reminder time in the mobile App.

The system will send an email to remind you to take action when your key is about to expire.



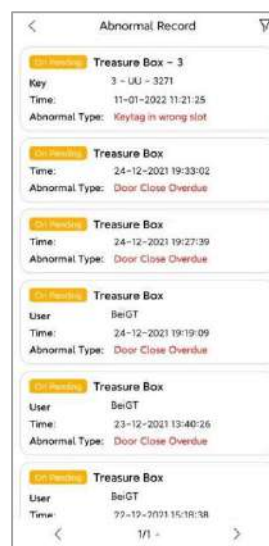
## 7.6 Records



Key Record



Operation Log



Abnormal Record

## Part 8 FAQs

### 8.1 General

#### 1. How many users can use K26?

Up to 10,000 people per system.

#### 2. What happens when someone leaves the door open?

(1) After 30 seconds, the audible alarm is activated and all key receptor slots indicators turn red. The system requests that the door is closed and all keys stay locked in position until someone does it. (2) An alert email will be sent to the administrator.

#### 3. Who can change the password?

Every user can change their password after they have logged in. The administrator can reset the user's password to 333.

#### 4. What if a user forgets their password code?

Reset the password after verifying the email on the web or mobile app, or else ask the administrator for help.

#### 5. How much information can K26 save about keys activities?

No limit.

#### 6. What will happen with system during a power failure?

The door and all keys will be inaccessible. Keys can be removed urgently with the help of the

mechanical keys, as the description in chapter 6 of this article. You can also use an external UPS to ensure system operation.

#### 7. What if I lose my spare keys?

You can order replacement spare keys from the sales manager or local distributors.

#### 8. Can I access the system through a web browser?

Yes. The cloud-based management allows users to access and manage the K26 system through web browser, cell phone, and tablet.

## 8.2 Operation

#### 1. Can I book the key for a determined day or hour?

Yes.

#### 2. What if it needs two persons for authorizing a key removal?

Add two pieces of multi-verification, so that they have the same key group and same user group, and different verification group. As described in Chapter 4.5.

#### 3. Can I check who has the particular key right now?

Yes, you can easily get an overview of keys from the K26 system, from the web, and from the cell phone.

#### 4. How many types of user roles are there in the system? Who can add new users?

There are four user types:

system administrator (all menu and key permissions, unique per department),

Administrator (all key permissions, most menu permissions, create common and custom user),

common user (key permissions granted or approved by an administrator),

and custom type (custom menu permissions and key permissions).

#### 5. Can I give user key access only during working hours?

Yes, this is a function of the user schedule.

#### 6. How do I know where to return the key?

Illuminated key slot will tell you where to return the key.

#### 7. What if I return the key into wrong positions?

The system will sound an audible alarm, and the door will not be allowed to close.

#### 8. When will an audible alarm activate?

The alarm will activate:

when forgetting to close the door

When opening the door using the spare key

When returning to the wrong location

9. Does the user know to which keys he/she has access?

Yes. The accessible keys are indicated with a green icon when he/she login to K26.

## 8.3 Others

1. Can I use my staff card?

It depends on the RFID type. The system can recognize 125KHz ID card, and 13.56MHz IC card (optional).

2. Can i integrate my card reader?

No. The standard system can't offer this option. Please contact us and we will help you choose the best solution, which suits your needs.

3. Can I integrate with existing systems?

No. The standard system can't offer this option. Please contact us and we will help you choose the best solution, which suits your needs.

4. Can multiple authentication methods be combined to log in to the system?

No. The standard system can't offer this option. Please contact us and we will help you customize this option.

5. Can the key locker still be used without the Internet?

Yes. There are two editions: the standalone edition and the internet edition. In case of internet disconnection, all menus of standalone edition and key-removing and returning menus of network edition remain accessible.