Keylongest Intelligent Key Management System User Guide

V1.2

06/04/2021

Beijing Landwell Electron Technology Co., Ltd

Content

Revision Record..... 1
Part 1 Document Purpose..... 2
Part 2 Terms and Conventions..... 2
Part 3 Keylongest Intelligent key management solution..... 2
3.1 What is Keylongest..... 2
3.2 Features..... 3
Part 4 K26 Cabinet..... 4
4.1 Panel..... 4
4.2 Parameters..... 4
4.3 How to start..... 5
4.4 Administrator..... 5
4.4.1 Connect to the internet..... 6
4.4.2 Keys..... 6
4.4.3 Users..... 6
4.4.4 Permission Group..... 7
4.4.5 Multi-verification..... 7
4.4.6 Event..... 8
4.4.7 System Settings..... 8
4.5 How to Take & Return Keys..... 9
4.5.1 Take keys..... 9
4.5.2 Return keys..... 10
Part 5 WEB Management..... 10
5.1 Function structure..... 10
5.2 Main Pages..... 11
5.2.1 Home Page..... 11
5.2.2 Settings..... 11
5.2.3 Reports..... 16
Part 6 App on cell phone..... 17
6.1 Get the app..... 17

6.2Account activation.....18

6.3 Main functions..... 18

Part 7 About Us..... 18

Revision Record

Version	Content	Date
V1.0	Create	29/11/2020
V1.2	Add web management	06/04/2021
V1.3	Modify *How does it work*	13/05/2021

Part 1 Document Purpose

The purpose of this document is to help you (the end user) understand the basic knowledge and operation specifications of *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.

Part 2 Terms and Conventions

[1] KMS, Key management system

[2] Keylongest/K26, modular key control cabinets with access control terminals

[3] KeyTag, RFID tag bound to a key

[4] KeySlot, the smallest unit for managing keys

[6] Key Register, upload RFID code of KeyTag to software

[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 person(s) login to K26 to provide proof

[8] Event, the purpose of using the key

[9] IPC, (Android) terminal of K26

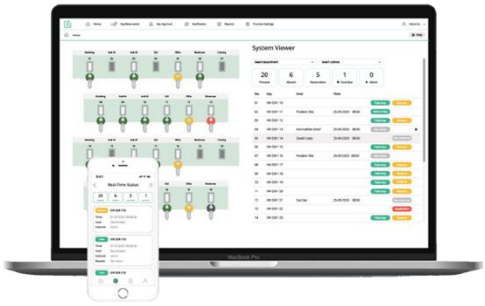
[10] 1:1, Verify, ID is needed before log in via fingerprint

[11] 1:N, Identity, login via face recognition

Part 3 Keylongest Intelligent key management solution

3.1 What is Keylongest

Keys give access to vehicles, lockers, facilities, equipment and more, making them one of your most valuable assets. 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. As the latest generation of Intelligent Key Control System, Keylongest introduces the concept of smart key management into modern commercial and office for the first time.

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.

3.2 Features

1) The electric control cabinet door and Key-Slot carry out double physical lock control on the key;
2) Support multiple identification methods such as face recognition, fingerprint, ID card, and password;
3) Master the real-time status of key through web station, mobile app, and key cabinet terminal.
4) Automatic recording, real-time understanding of the key's whereabouts, and retrospective use records;
5) When taking or returning the key, the key position is prompted by LED;
6) Support remote authorization to take opening via mobile phone or website;
7) Support abnormal alarms such as overdue opening, illegal opening;
8) Support multi-verification, it means, only when two or three people are present can the key be taken out;
9) Support both online and offline application modes.

3.3 How Does Keylongest work

1. Staff member accesses Keylongest key cabinet using a PIN, card reader, or biometric scanner
2. The Keylongest system unlocks the specific key(s) the staff member has been given access to.

3. After use, the staff member returns the key to the cabinet and make any necessary reports into the system
4. The system administrator has real-time data on which keys or equipment are signed out by whom and can access a full history of every transaction made.

Part 4 K26 Cabinet

4.1 Panel

From a structural point of view, K26 can be roughly divided into three areas: keys storage area on the left, User interaction area on the right, Rear power, and network physical interface. 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:

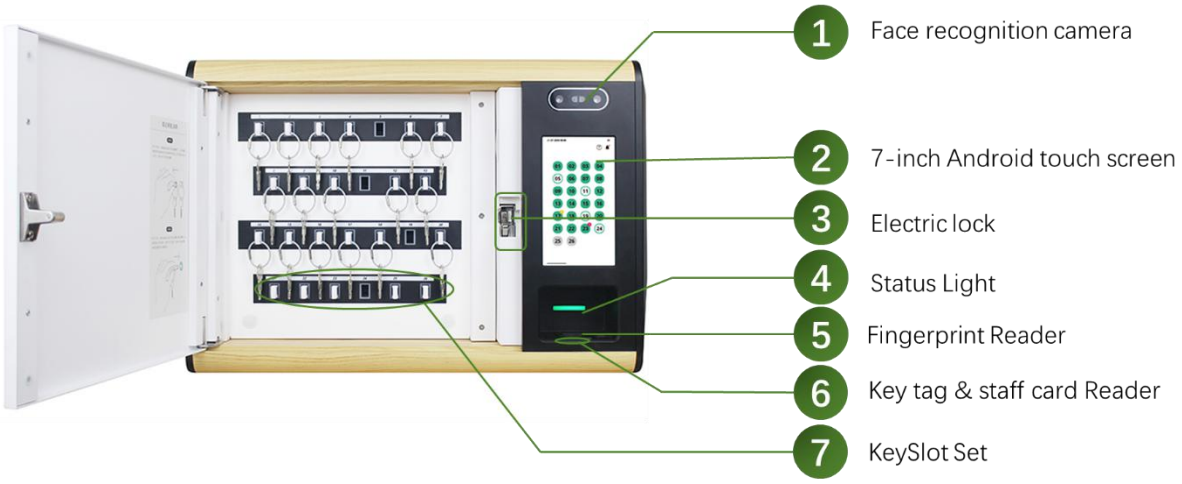


Figure 4-1 K26 panel

4.2 Parameters

	Product Name	Intelligent Key Management System
Basic Property	Model number	K26
	Key-Slots	26 pieces
	Materials	1.5mm Steel + ABS
	Surface Treatment	Paint baking
	Dimension(mm)	(L)566 X (W)177 X (H)380
	Weight	17Kg net
Master Control	Operation System	Built-in Android 4.4
	Display	7" Touch screen

	Network mode	Wi-Fi + Ethernet
	Data Storage	Cloud, Local memory
	Door lock	Electronic moto lock
	Access ways	Face + Finger + Card + Password
	Face Recognition Time	< 1s
	Finger Recognition Time	≈ 0.6s (1:1)
	User Card Type	125KHz / 13.56MHz(option)
Others	Working Voltage	DC 12V 5A(max)
	Power Supply	AC 110～240V 50～60Hz
	Temperature and humidity	-20～70℃, ≤95% RH

4.3 How do you set up Keylongest system

If the K26 you purchased is a network version, you will get a system account. It can be used to log in k26, key management system websites, and mobile applications. It can help you to use k26 more easily and become a good helper in your work and life.

1) Install the key cabinet

Have the key cabinet installed in the best location in the facility.

2) Attach key to key-tags

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

3) Assign access to the key cabinet

System administrator can assign temporary or permanent access for users by way of PINs, card readers, or biometric scanners. The system automatically controls and records when a key is used and by whom on a central database and this information is available via the cabinet's display or on the administrator's computer. Depending on which system is installed, specific features like email reminders can be set up so that both the administrator and user are notified when a key isn't returned on time.

4.4 System Administrator

All the settings, except the registration of keys, user card, fingerprint, and facial features, can be realized through website or K26. For convenience, I will only introduce the setting method on K26.

4.4.1 Connect to the internet

1) Log in to k26 as the system administrator;

2) [Setting][Parameter Setting][System];

3) When returning to Android, configure the network connection as Wi-Fi or Ethernet static address, so that k26 can connect to the Internet.

4.4.2 Keys

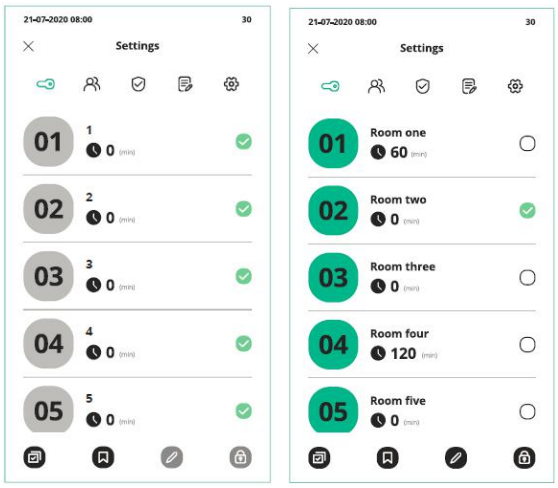


Figure 4-4-2 K26Keys

Button function:

- [press any key and hold on for 1s, then] Select all
- Register selected / all key
- Edit selected key, rename it, and set its maximum time(minute) to use
- lock/unlock selected key

4.4.3 Users

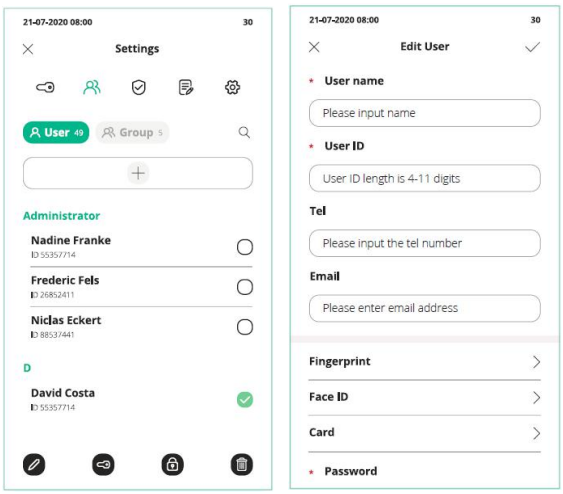


Figure 4-4-3 K26User

Button function:

Add a user

Edit selected user information

Edit key-permissions for the selected user

Lock / unlock selected user

Delete selected user

4.4.4 Permission Group

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

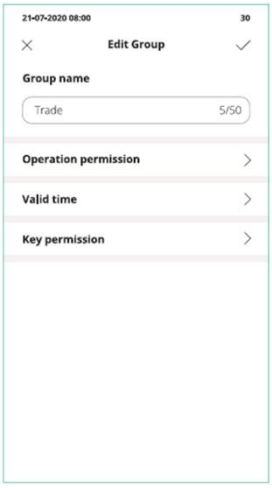


Figure 4-4-4 K26Group

✧ **Operation permission**

What functions can group members use?

✧ **Valid time**

When can group members use the keys?

✧ **Key permission**

What keys can group members use?

4.4.5 Multi-verification

Multi-Verification, the **person(s)** will not be allowed to remove the preset **key(set)** unless one of **other preset person(s)** log in to k26 to provide proof.

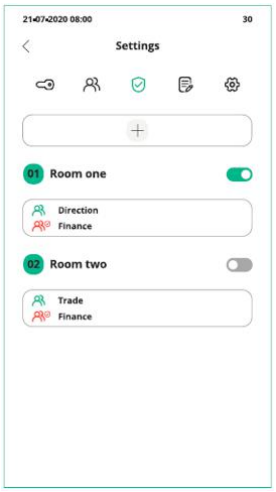


Figure 4-4-5 K26Multi-verification

Turn on / off multi-verification relationship of selected key

Add a new multi-verification relationship of keys

4.4.6 Event

Event, the purpose of using the key

Figure 4-4-6 K26Event

a) Press

b) Input *Event*, then save

c) Click

d) Select keys that need to active events.

4.4.7 System Settings

Setting of system operation parameters

No.	Item
1	Brightness

2	Sleep Time
3	Key preview
4	Standby page displayed or not
5	Snap a picture when taking & returning keys?
6	Volume
8	Door open overdue
9	Switch of Fingerprint/face/user card
10	Emergency password
10	Update checking
11	Language
12	Cabinet name
13	Return Android System(setting | resource explorer | browser)

4.5 How to Take & Return Keys

4.5.1 Take keys

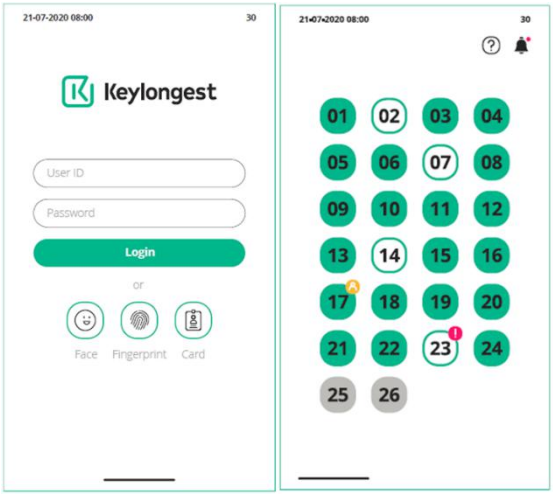


Figure 4-5-1 K26Taking keys

1) Log in K26

- Face Recognition
- User ID + Fingerprint
- User Card
- User ID + password

2) Select one from your available keys, the door will pop open automatically.

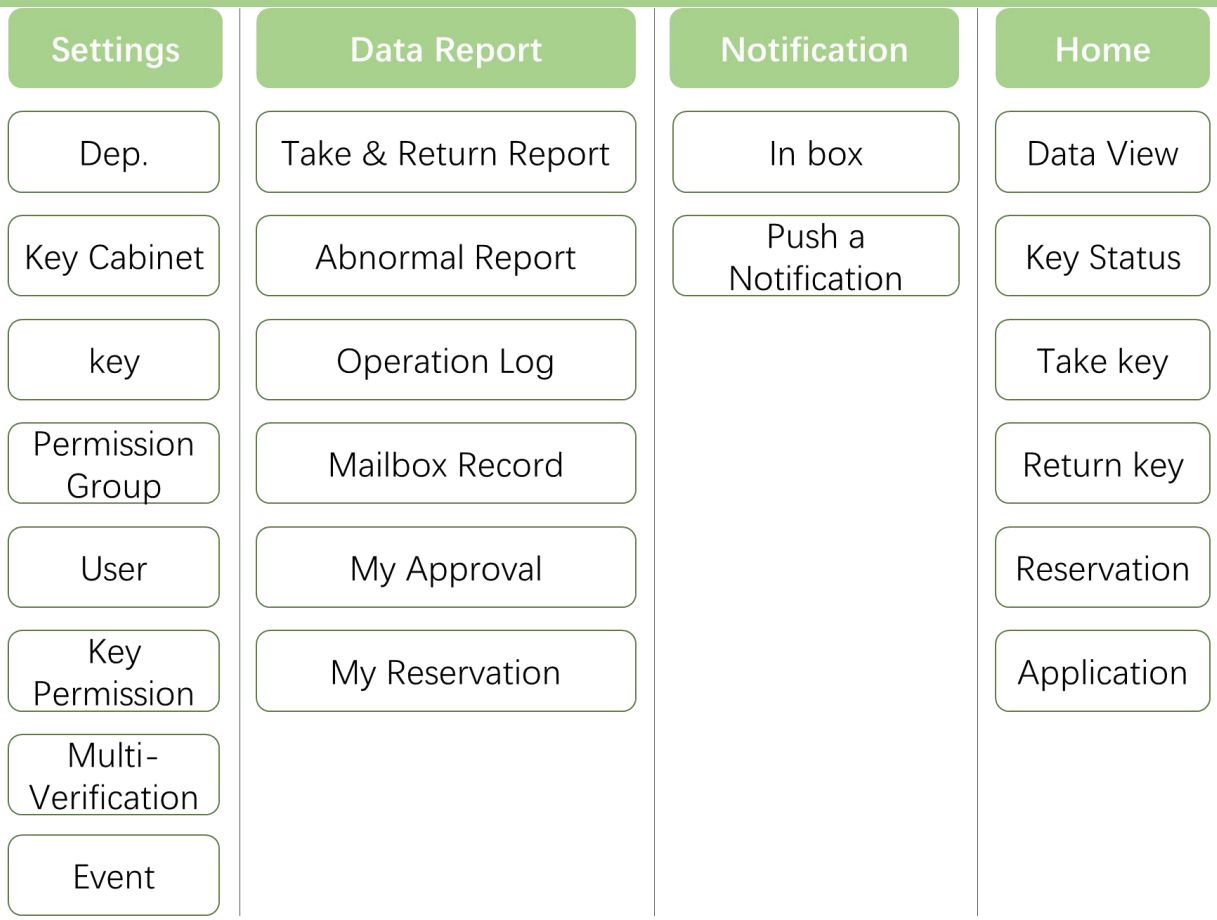
3) Take out the key and close the door.

4.5.2 Return keys

After swiping the key card, the cabinet door will open automatically, and you can put it in the correct position according to the LED prompt.

Part 5 WEB Management

5.1 Function structure



5.2 Main Pages

5.2.1 Home Page

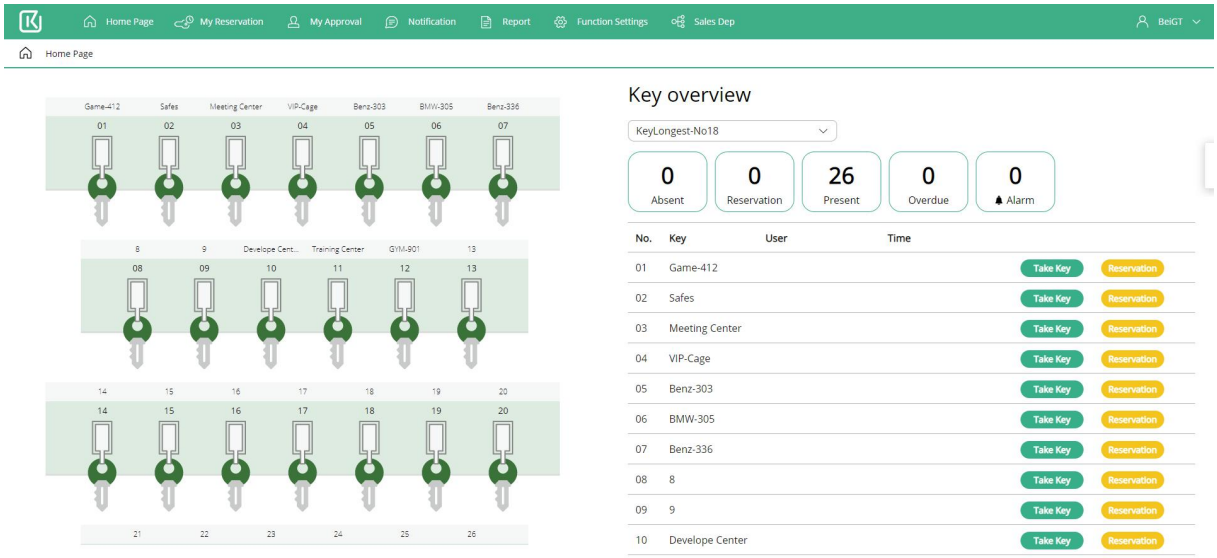


Figure 5-2-1 HomePage

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 present, the status of permission, the status of reservation, the status of registration, and so on.

- Take key： The cabinet will open after your confirmation, so please take the key out .
- Reservation: Make an appointment for the key within the existing authority
- Application: Apply for keys without permission

5.2.2 Settings

Option	Details	Remarks
Department	Add, edit, delete a child department	
Key Cabinet	Edit Cabinet’s name	
	Set the max-time for door opening	
	Transfer current cabinet to another department	
Key	Edit current key’s name	
	Set the max usage time of current key	
	Lock / unlock current key	

	Enable or close the current key's event	
	Enable or close the current key's multi-verification	
Permission Group	Add, edit, delete a permission group(menu module & key permission)	
User	Add, edit, delete a user	
	User type: system administrator, administrator, common user	
	Lock / unlock a user account	
Key permission	Set common user's key permission	
Multi-verification	Add / delete / edit multi-verification for current key/group	
Event	Add / edit / delete reasons of taking keys	

5.2.2.1 Department

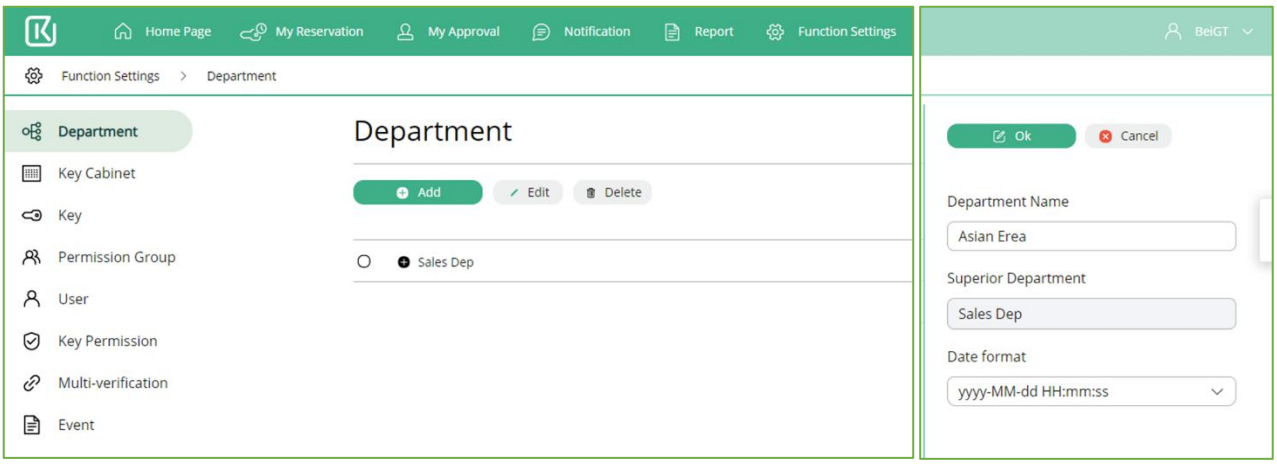


Figure 5-2-2(1) Department

Click **[Add]** to 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.

5.2.2.2 Key cabinet

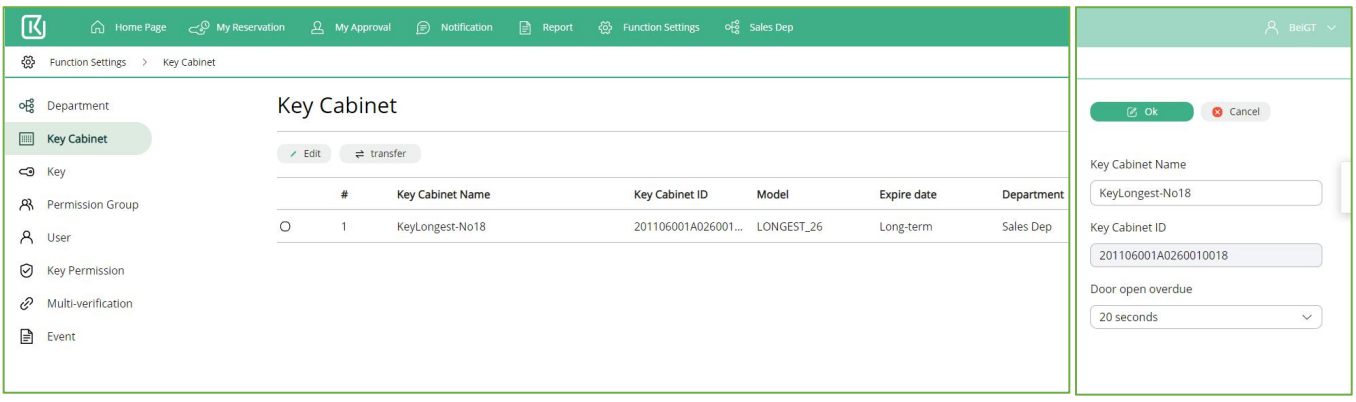


Figure 5-2-2(2) KeyCabinet

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

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

5.2.2.3 Key

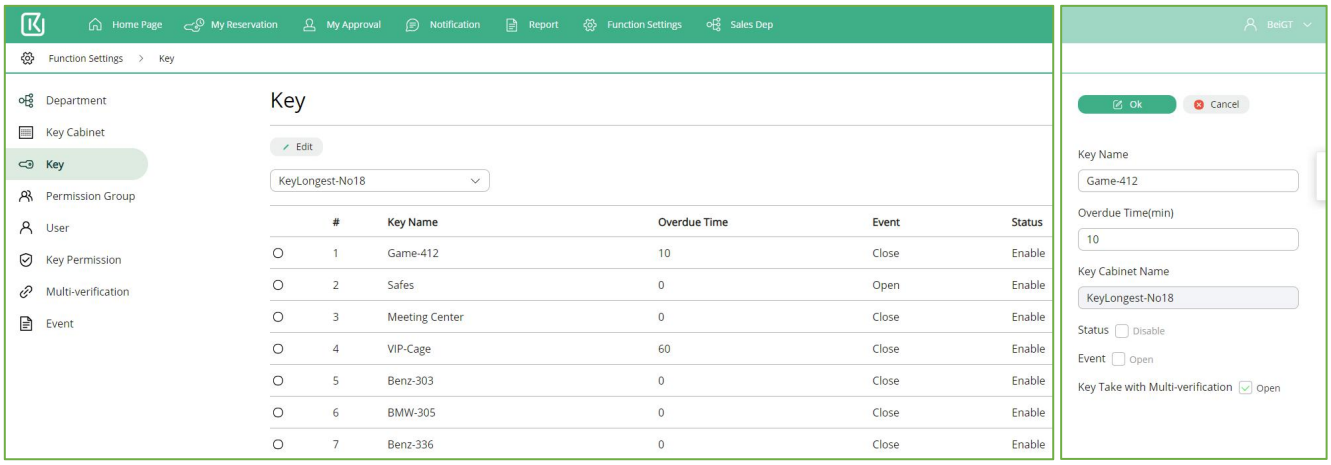


Figure 5-2-2(3) Key

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

[Edit], rename keys, set keys' max usage time(minute), change the available state, event state, and multi authentication state of keys.

5.2.2.4 Permission group

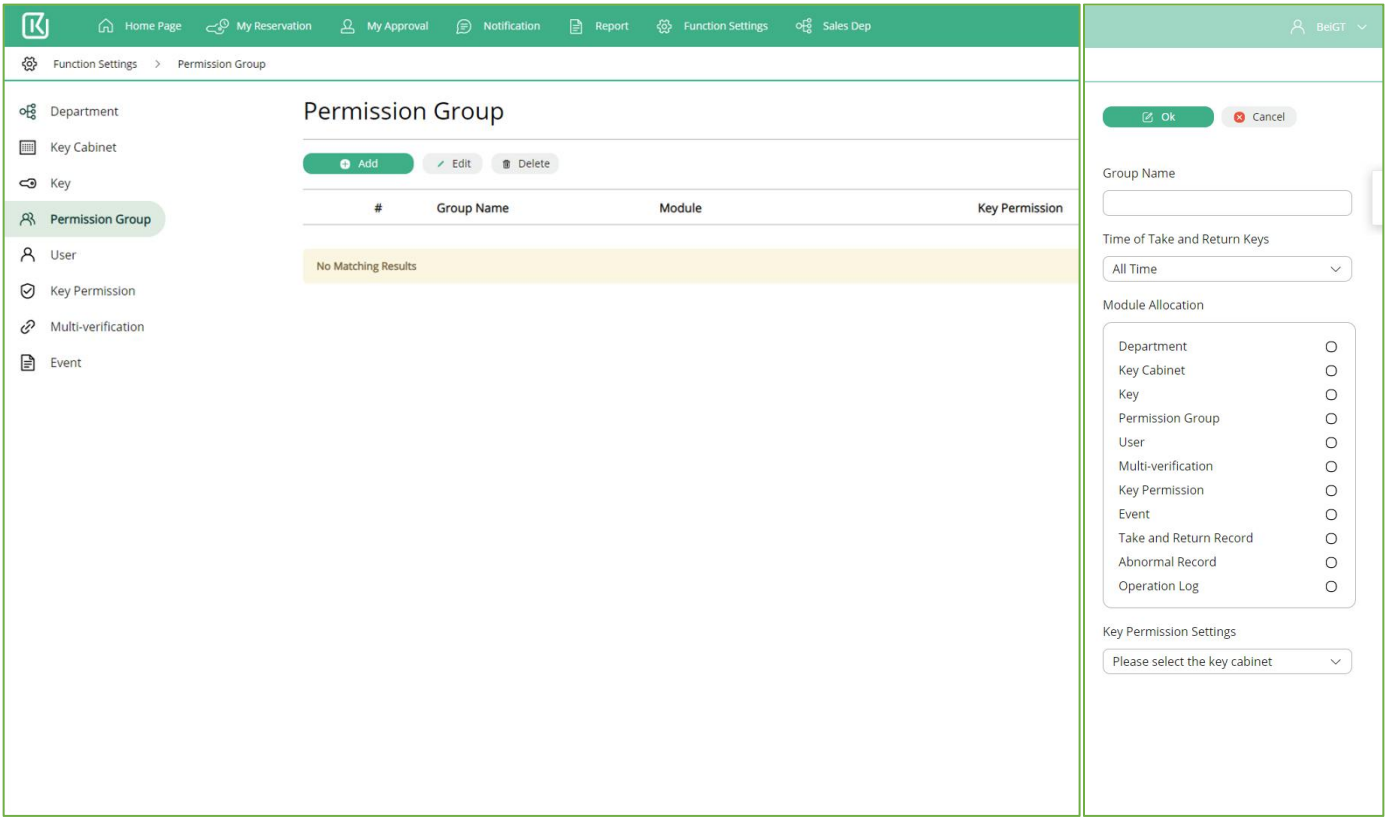


Figure 5-2-2(4) Permission Group

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

5.2.2.5 User

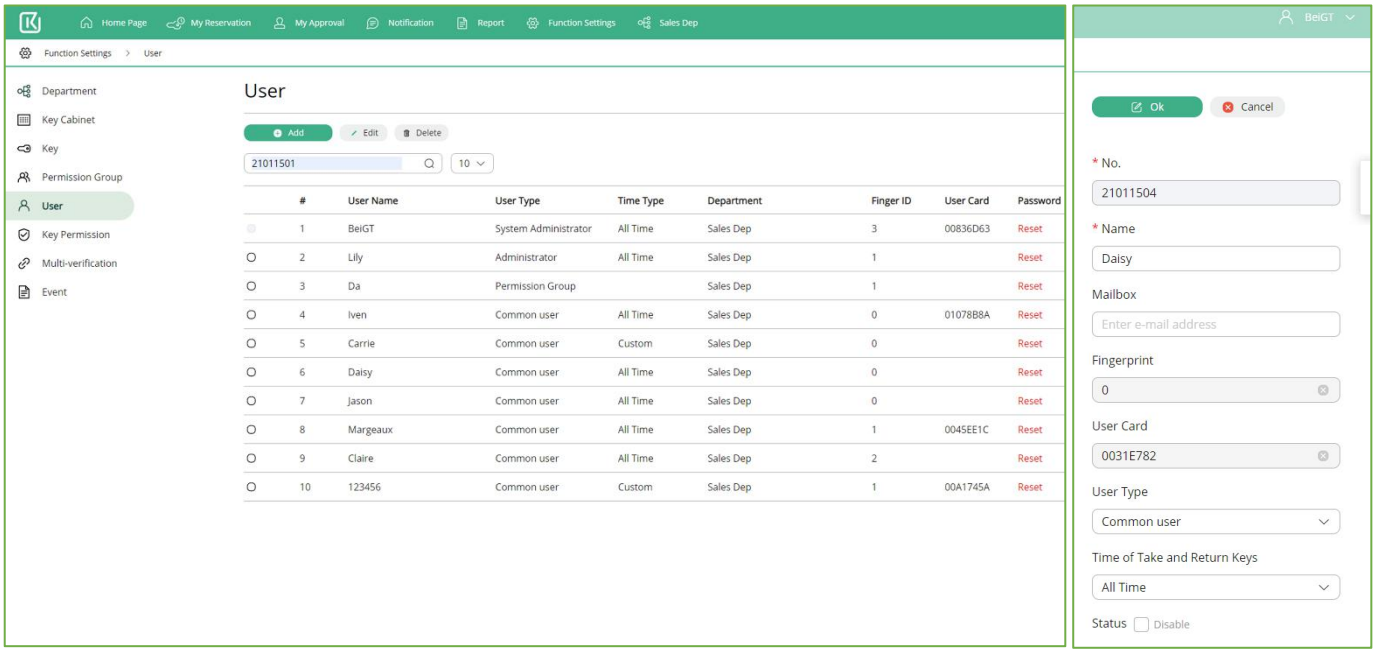


Figure 5-2-2(5) User

When users' finger, face, and card are registered on k26, all this information will be automatically synced on the web page.

Add, edit users' information, include: [User Type (administrator, common user or permission group)], [Time of take & return keys], [Status], and so on.

User Type	Menu module	Key permission
System Administrator	All	All
Administrator	All, except creating an administrator account	All
Common User	[Function Setting] Forbidden	Settable
Permission Group	Inherits from the selected group	

Notice: [No.] Once added, it cannot be modified again

5.2.2.6 Key permission

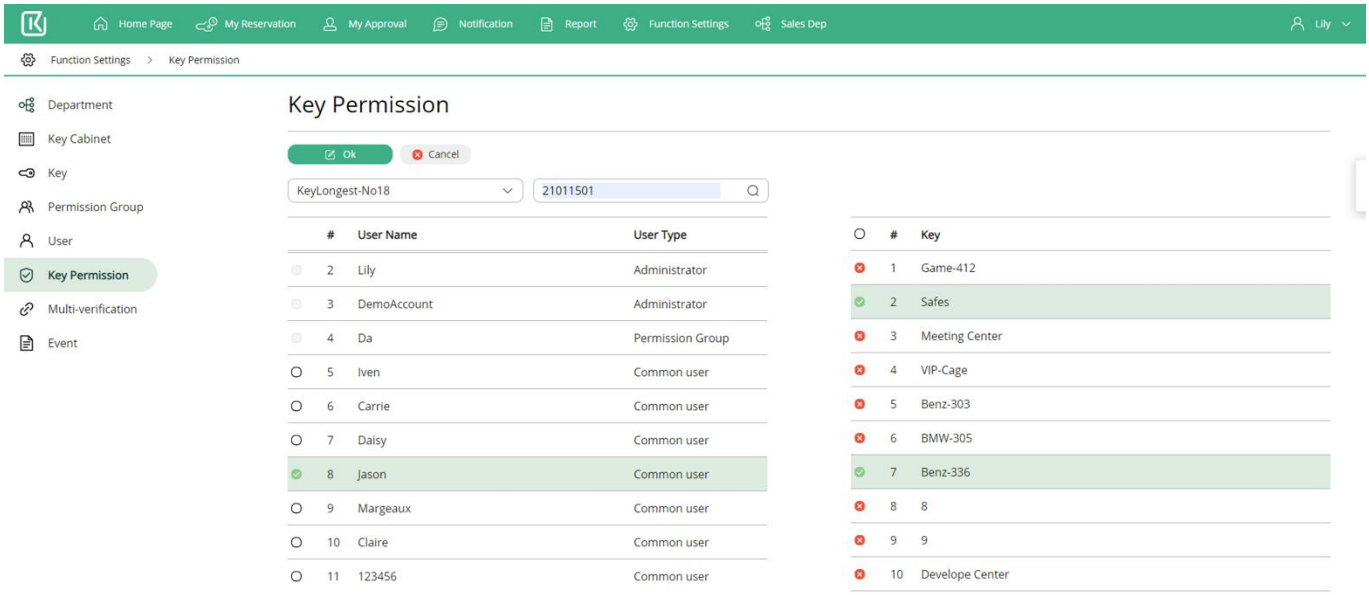


Figure 5-2-2(6) KeyPermission

Function: Set who can use which keys.

5.2.2.7 Multi-verification

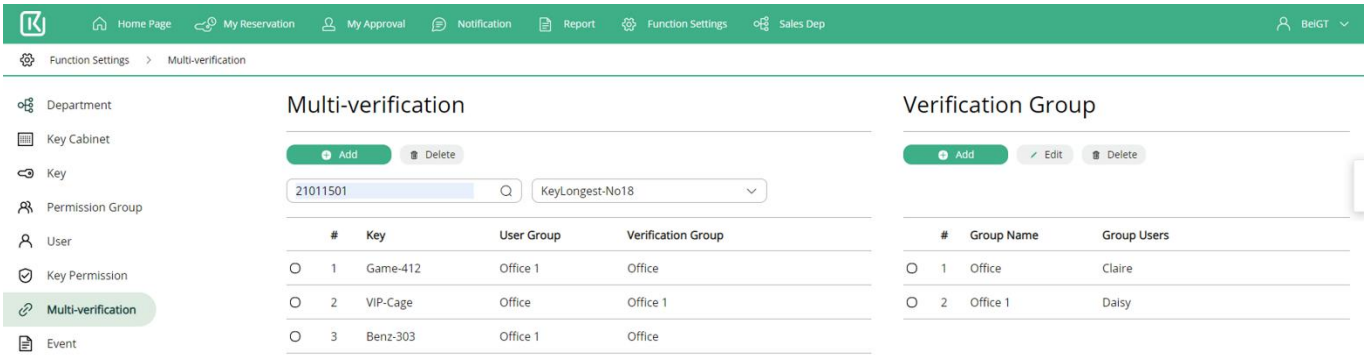


Figure 5-2-2(7) Multi-verificaion

Function: the person using the key will not be allowed to remove the preset key(set) unless one of preset person(s) login to k26 to provide proof.

[add (verification group)], add user-group;

[add (multi-verification)], Associate key, user group, and authentication group.

5.2.2.8 Event

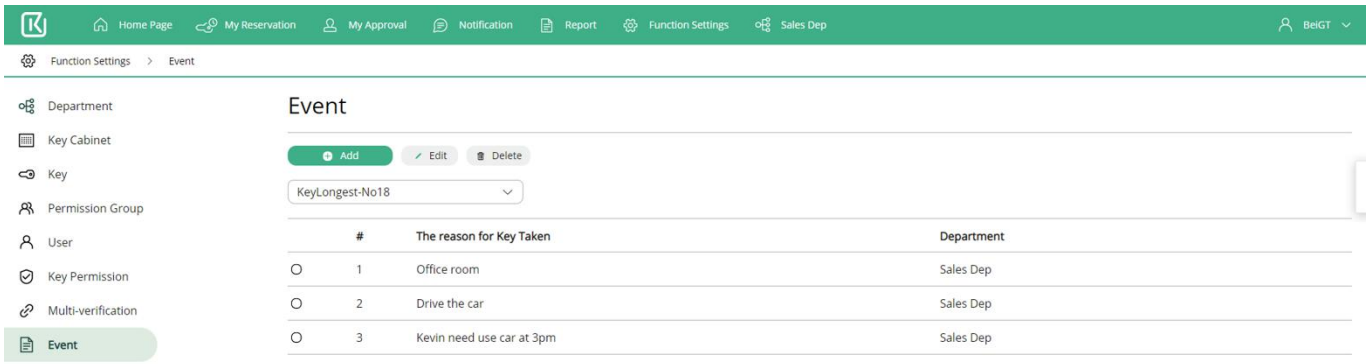


Figure 5-2-2(8) Event

Function: Preset several reasons for key use.

5.2.3 Reports

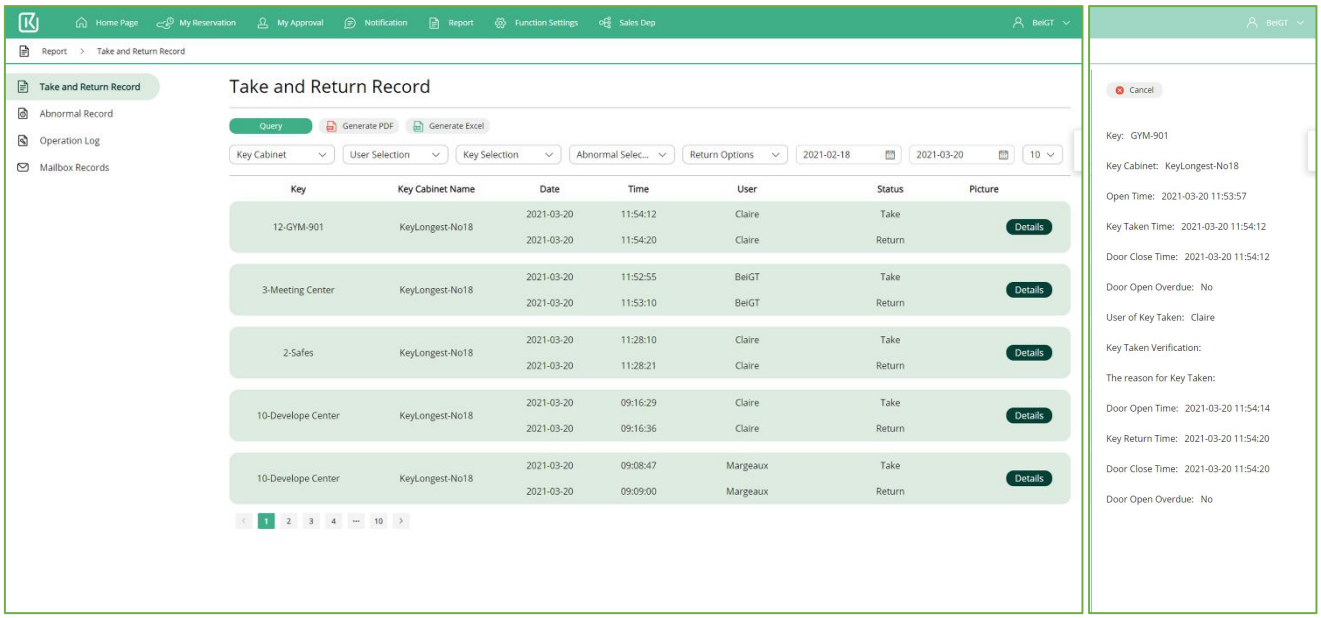


Figure 5-2-3(1) Key usage record and record details

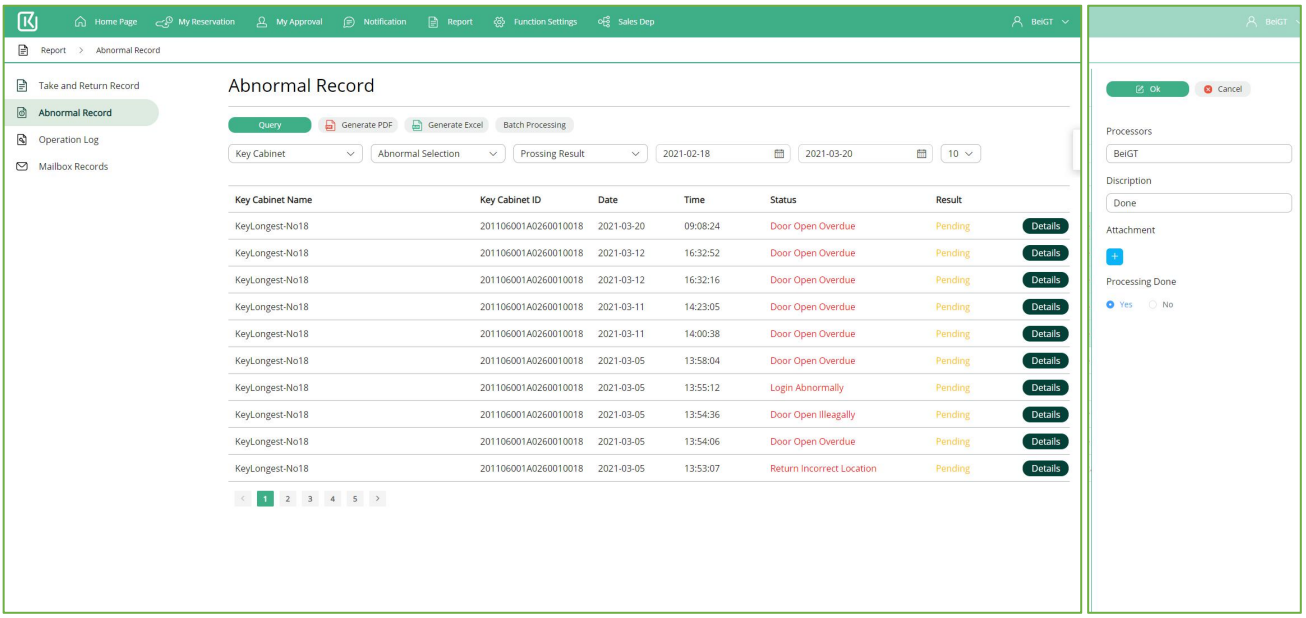


Figure 5-2-3(2) Abnormal record and processing

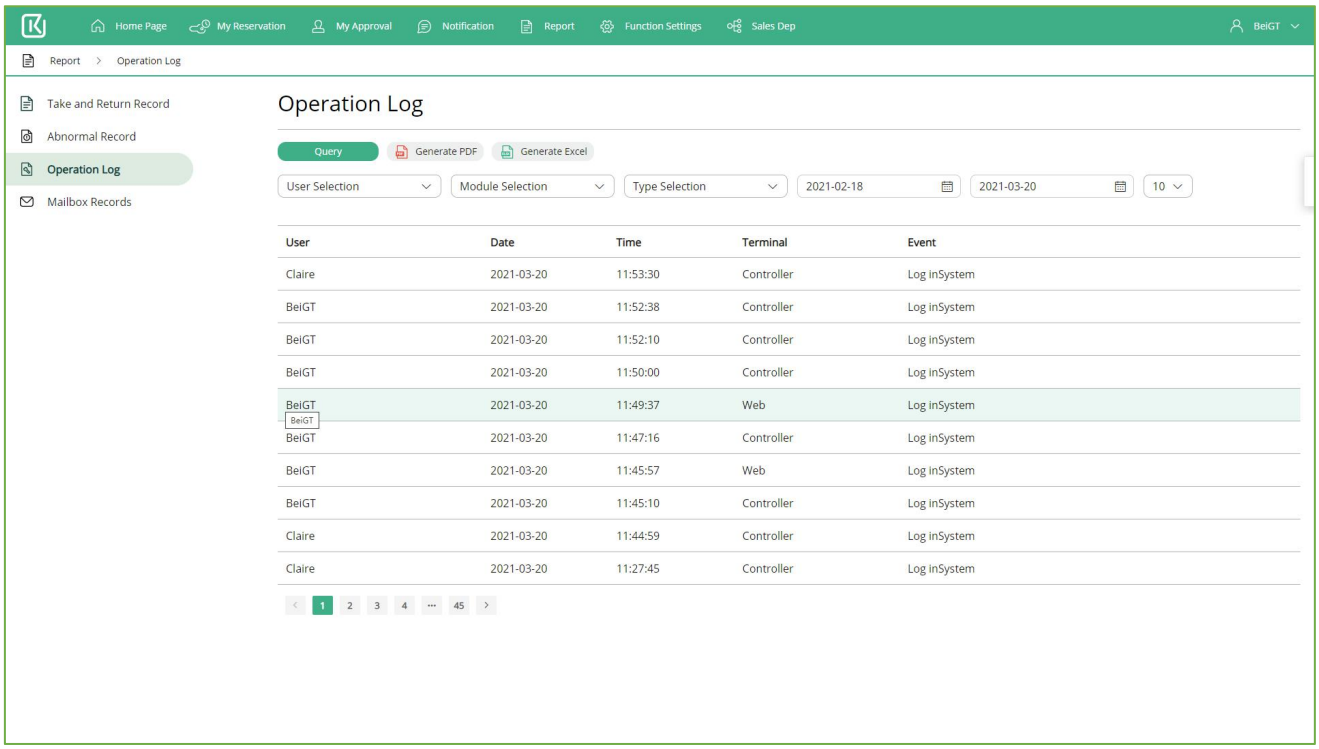


Figure 5-2-3(3) Operation log

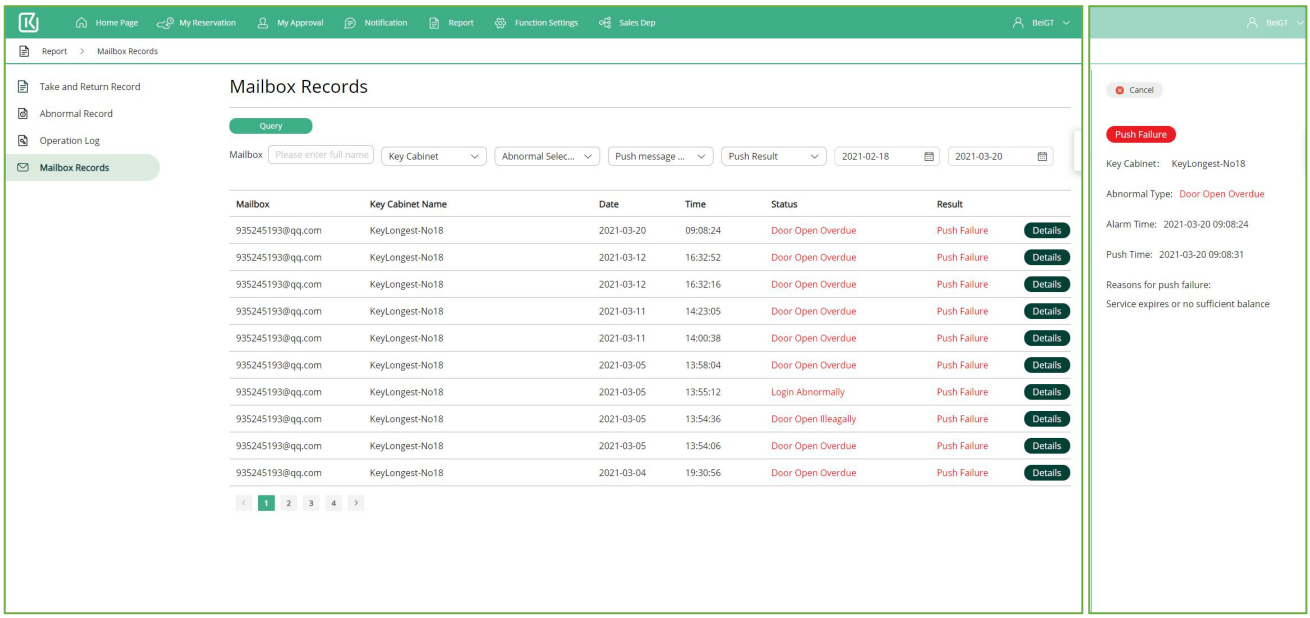


Figure 5-2-3(4) Mailbox Record

Part 6 App on cell phone

6.1 Get the app

Scan the [app download] QR code at the bottom of K26's home page to download the app.

6.2 Account activation

Scan the [Version] QR code at the bottom of the K26's home page to get the unique ID of K26, then activate your account on your cell phone.

6.3 Main functions

(1) Get key status on real-time

(2) Remotely take/return keys

(3) Key reservation/application and approval

(4) View record

(5) Change personal password

Part 7 About Us

Company: Beijing Landwell Electron Technology Co., Ltd

Address: Floor 9, A6 Huguang Middle Street, Beijing, China

Email: ad@land-well.com

Tel: 86-10-84717640

Website: http://www.guard361.com