Pamex

Enkore Series

A Multi-Family Door Access Control Solution

KE1-D7P1A, KE1-INP35A

Project Implementation Guide

Table of Contents

Introduction **4**

Before Installation **6**
- Check List 6
- Pamex MFSP Service Platform 6

Implementation Guide **7**
- Concepts 7
- Construction Phase 8
- Lock Registration Phase 9
  - Plan your area tree 10
  - Build the area tree using MF-Admin Server 11
  - Plan your programming cards 14
  - Setup Wifi AP and Create Programming Cards 16
  - Register Locks to MF-Admin Server 19
  - Verify lock registration using Master Card 21
- Go-live Phase 26
  - Create Tenant Cards 34
  - Create Staff Card 42
  - Create Vendor Card 47
  - Create Guest/Temp Card 54
  - Shutdown Public Area 58
    - Area Time Control 59
    - Lock Scheduling 60
  - Access Control Rule 64
  - Time Control - Add/Remove Holidays 66

Advanced Setup Guide **68**
  - Lock Report Interval 68
  - Alert Settings 69

Appendix **71**
- Lock UI Patterns (LED & Buzzer) 71
- Wall Reader 73
- Wall Reader 74
- Wifi AP Specification and Settings 75
- Factory default settings - Wall Reader 76
- Factory default settings - Deadbolt 77
- Factory default settings - Leverset 78
- Factory default settings - Interconnect 79
- MF-Admin Server Parameters default settings 80
  - Application Parameters 80

System Parameters 80
Mifare Card Specification 81
Card Types 82
Area Types 84
Lock Real Time Events 85
Default Severity of Alert Types 86
FCC Statement 87
NCC Statement 88

Introduction

The Pamex Enkore series is a total solution for multi-family door access control. It not only has several models of the lock but also the browser-based central management system (MF-Admin server).

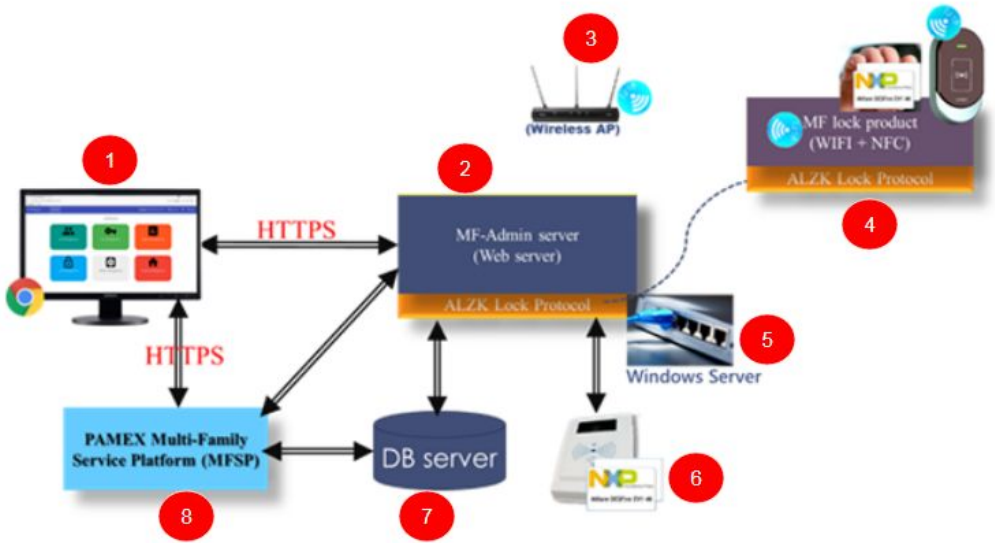


Figure 1 : Pamex Enkore System Architecture Overview

Figure 1 shows the system architecture of Pamex Enkore solution, Below are the brief description of each component:

1. Chrome browser: The user interface to the MF-Admin Server (2). You need a PC with a Chrome browser to use MF-Admin. The card reader/writer (No.6 in figure 1) will be connected to this PC using USB. You may also use the windows server (5) as the client PC.
2. MF-Admin Server: An application running on a Windows server (5). It provides all the functions to manage the access control of the locks and the cards/fobs.
3. Wifi AP: All the Enkore locks have the wifi capability and are necessary to connect to a wifi AP in order to be programmed by the MF-Admin server. There should be a few to many Wifi APs at a multi-family property. Wifi AP is not part of Enkore products. Check the lock specifications in the Appendix for the compatible Wifi AP.
4. Enkore smart locks and NFC cards: All the Enkore locks are smart locks that are accessed using NFC card/fob (Mifare Desfire).
5. Windows Server: MF-Admin server is installed on this server.
6. Card Reader/Writer: MP100 is the default reader to issue a new card/fob to users/residents.

Figure 2: MP100

7. DB Server : A database is installed on windows server to keep all the data of the system. It is installed and automatically configured by the install program. Please reference *MF-Admin & MP100 installation guide*.
8. MFSP platform : MFSP (Multi-Family Service Platform) is a cloud service for all the MF-Admin Servers around the world. This platform is operated by Pamex. Connected your MF-Admin Server to MFSP is not required but we encourage you to do so. MFSP will provide some enhancement to Enkore solution in the future.

Before Installation

Check List

- Locks
- Cards : Crypto Card x 2, Construction Card x 5, Blank Card x 10
- MF-Admin + MP100 Software
- MP100 Card Reader x 1
- Windows Server x 1

Pamex MFSP Service Platform

- **This section is for Pamex only.**
- Before any Enkore installation, Pamex admin will have to create a project in MFSP in order to get the unique project code.
- An Enkore installation will need at least one Crypto card to activate all the locks. Crypto cards can only be issued through MFSP by Pamex. MFSP will keep the encryption keys of the Mifare Desfire card for every project.

Implementation Guide

Concepts

Pamex Enkore setup can be thought of in terms of three phases: Depending on the progress of your project, there are three phases defined as :

- Construction Phase :
  All the door locks are installed but not programmed yet. MF-Admin server is not necessary for this phase.

- Lock Registration Phase :
  The door locks are ready to be programmed/registered to the MF-Admin server.

- Go-Live Phase :
  All the locks are registered to MF-Admin Server. The system is ready to go.

Normally, as time goes by, a project will first in the construction phase, then go to the lock registration phase, then the go-live phase. Each phase requires different tasks to be completed as described below.

In this guide, we will use the term Card or Key from time to time. Both terms refer to the Mifare Card or Mifare key fob is issued by Pamex Enkore solution. Used by the Pamex Enkore system.

MP100 is the only device you use to issue card/key. Note that sometimes you have to re-place (take a card off the reader then place the card on the reader again) the card on the reader to successfully complete your card operation. MF-Admin server will remind you to re-place the card as possible as it can. But remember to do so when you encounter MP100 reader error. It’s not a bug but the nature of Mifare Card operations.

Construction Phase

Make sure you have Crypto Cards and Construction Cards on hand. Crypto Card and Construction Card are shipped from Pamex together with physical locks. (See Appendix: Card Types)

In the scenario that wifi network and MF-Admin Server is not ready, and you have installed locks on the doors, you will need Construction Cards to unlock and open the door.

A lock can be unlocked using Construction Card only after it has successfully scanned the Crypto Card but before programmed by programming card. No other cards can unlock the doors at this moment.

A Construction Card can unlock any locks which have been scanned by Crypto Card given by Pamex for your project only.

Depending on the lock model, the lock will present below response when scanning Mifare Cards :

Lock Model	**Crypto Card Success**	**Crypto Card Fail**
Wall Reader	Green LED on 1 sec & long beep once	Red LED flash 3 times & beep 3 times
Deadbolt	Same as Wall Reader	Same as Wall Reader
Leverset	Same as Wall Reader	Same as Wall Reader
Interconnect	Same as Wall Reader	Same as Wall Reader

Construction Cards will remain valid until you scan Programming Card to a lock. Programming Cards can only be created using MF-Admin Server which means your wifi APs and network are ready and you are entering the next phase - Lock Registration Phase.

Lock Registration Phase

MF-Admin Server is required to complete all the tasks in this phase. Please follow the *MF-Admin Server & MP100 Installation Guide* to install MF-Admin Server.

MF-Admin Server is a web-based application with access controlled by login id and password. A newly installed MF-Admin Server has an admin user with login id = alzk, password = alzk. You may use this account to access all the functions in MF-Admin but we recommend you create another ids for all the users who need to access MF-Admin. Please check *MF-Admin Server User Guide* to see how to create users. The default admin user alzk can not be removed. Change the password of alzk immediately is recommended to secure the account. Please check *MF-Admin Server User Manual* to see how to change alzk password.

To better illustrate all the steps, we will use a SIMPLE example project to describe how to complete all the steps.

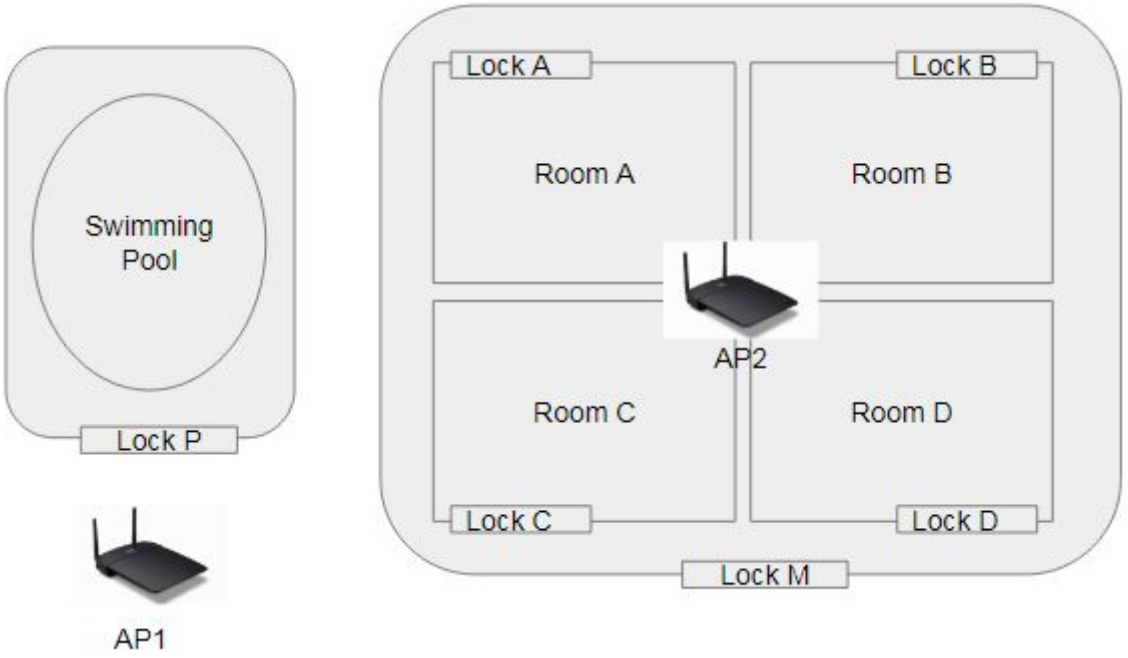


Figure 17: Project SIMPLE

In the SIMPLE project, there are 4 families (A, B, C, D) with one common entrance (M) and a shared swimming pool controlled by Lock P.

You will have to go through below steps to setup the MF-Admin server and register all the locks by using alzk account :

Plan your area tree

Area tree is the topology of your property. Before you can register your physical locks and link the locks to their corresponding lock place, you have to build the area tree in MF-Admin Server.

There are three types of areas : group, unit, public (See Appendix: Area Types for detail). An area may contain zero or several lock places which will linked to the physical lock one by one when registering.

For the SIMPLE project, you should prepare a table as below :

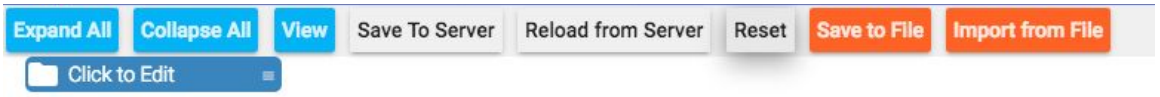
Root Area (Group area) (No lockplace)		
	Public Area P Lockplace P	
	Group Area M Lockplace M	
		Unit Area A Lockplace A
		Unit Area B Lockplace B
		Unit Area C Lockplace C
		Unit Area D Lockplace D

Note that the quantity of lock places will be exactly the same as the number of physical locks.

Build the area tree using MF-Admin Server

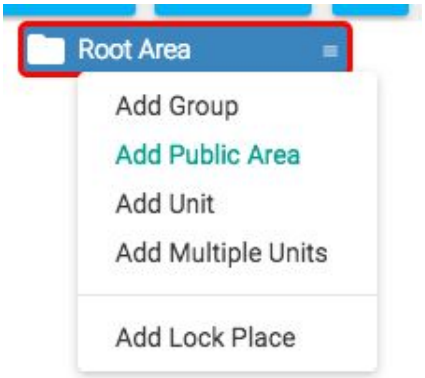
Navigate to build area tree page. **Property Management** => **Build Property**

For a brand new property, you will see only one node at beginning.



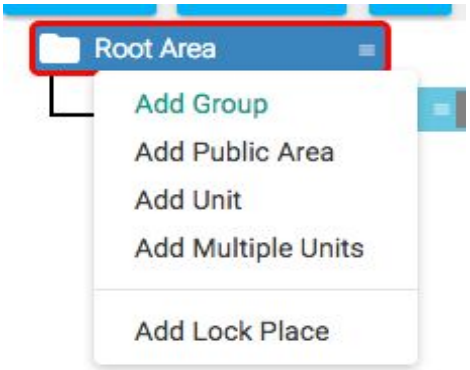
Click and edit root area name.

Click edit button on Root Area and select Add Public Area.

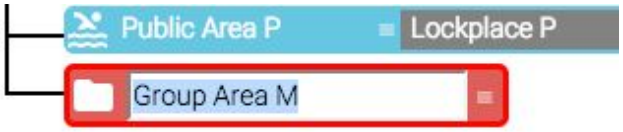


Click the name text to edit public area name and lockplace name.

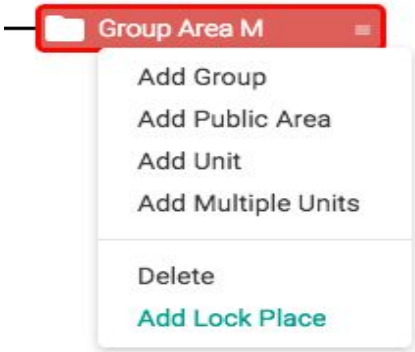
Click menu button on Root Area and select Add Group.



Click name text to edit group name.

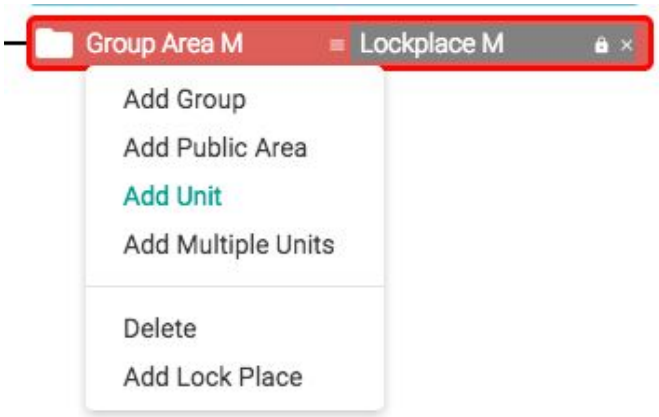


Click menu button on Group Area M and select “Add Lock Place”.



Edit lockplace name.

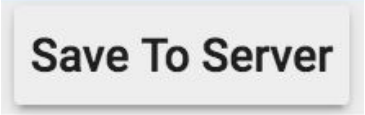
Click menu button on Group Area M and select “Add Unit”.



Click name text to edit unit name and lockplace name.

Keep adding unit from B to D

Click Save To Server to save the area tree.



Note that there are many ways to build an area tree as above. You may find another techniques in *MF-Admin Server User Manual.* If you make any mistakes during building the tree, just click “Reload from server” or “Reset” to return to the initial state.

Plan your programming cards

The area tree is now ready to be linked to physical locks. Pamex Enkore locks support WPA2 encryption to connect to the Wifi AP. When a lock is scanned by a programming card, the preferred Wifi AP SSIDs will be loaded into the lock from programming card. A programming card may save 1 ~ 5 SSIDs.

Normally, you only have to scan one time for a lock during its lifetime. The reasons to re-scan programming card will be :

- MF-Admin server ip is changed after go-live phase : This should be a rare case and usually can be avoid. If the MF-Admin Server ip has to be changed, then you have to make new programming cards and all the locks have to be programmed again.

- Some Wifi AP SSID changed : For those locks in the range of changed wifi APs, you have to scan them with new programming card which has the new SSID in it.

- Locks have been reset to factory default.

When any of the above cases happened, we recommend you to contact with the reseller for help.

In SIMPLE project, we assume that you have two Wifi APs with SSID = AP1 and SSID = AP2. In real world, depending on the size of your project. you may have tens to hundreds of Wifi APs. Therefore, prepare below table is recommended :

Wifi AP SSID	**WPA2 Key (32 characters)**	**Rooms in Range**	**Programming Card**
AP1	12345678	Unit A	Card 1
		Unit B	Card 1
		Unit C	Card 1
		Unit D	Card 1
AP2	abcdefg	Public Area P	Card 1

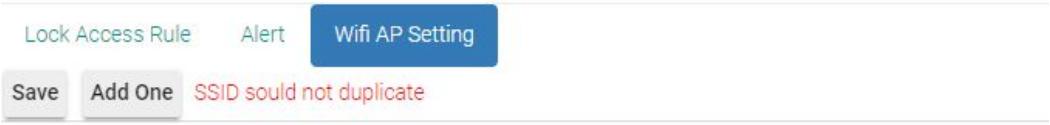
For SIMPLE project, AP1 and AP2 can be saved into one programming card. Programming card can be created by using MF-Admin Server and you may create

several cards with the same settings in order to program the locks in parallel by several workers. In the case that several workers are programming locks in parallel, please label the UID of the card (UID can be found on MF-Admin page when you create the programming card) on the programming card with a sticker or marker. When your lock is scanned, you will be able to tell which lock is yours via the UID. See the detail in registering locks.

Setup Wifi AP and Create Programming Cards

Navigate to system parameters page. **System Management** => **System Parameters**

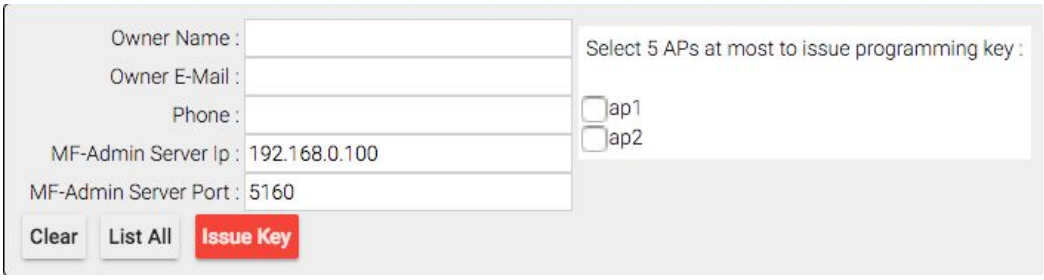
Select **Wifi AP Setting**



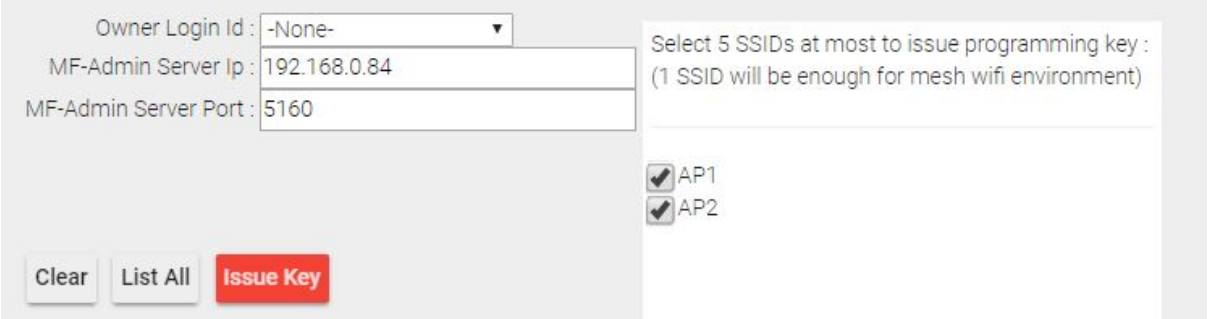
Click **Add One** to add wifi ap and click **Save** to save wifi ap.

Navigate to create programming cards page. **Property Management** => **Issue Programming Key**

You will see there are two wifi aps you added previously.

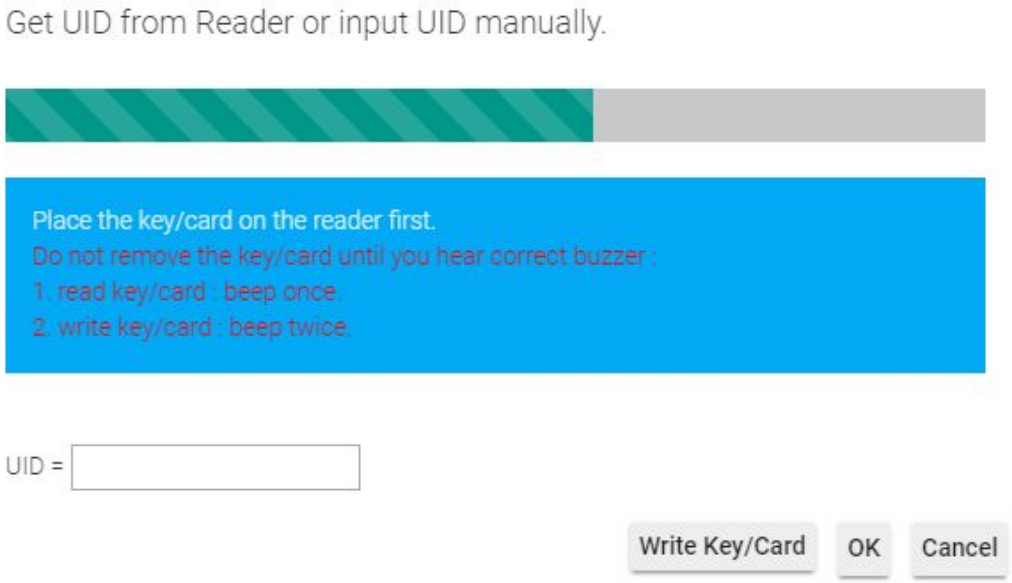


Check the checkbox on those wifi ap and click **Issue Key**.



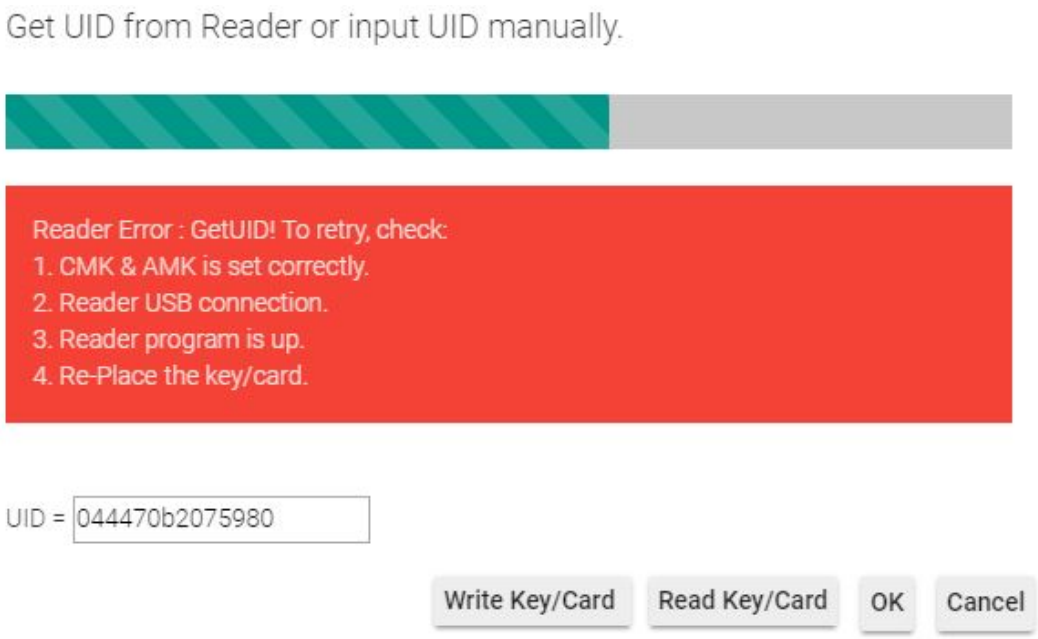
Place key/card on reader first.

Click **Write Key/Card** to get Key's UID.



The **green light** LED on **Read** will blink.

If **Write Key/Card** failed with **three** beep sounds and display following message, please re-place key/card and click **Write Key/Card** again.

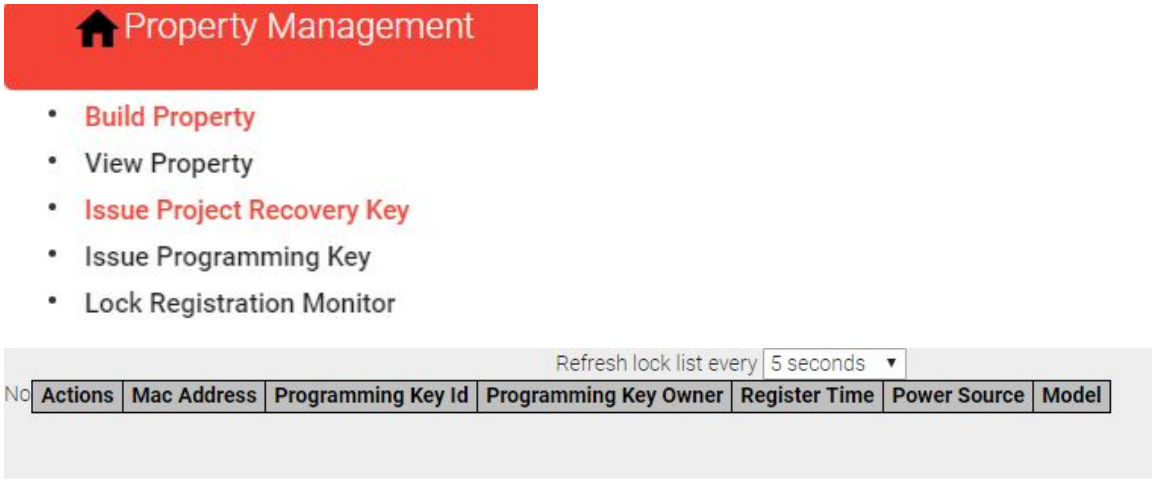


If programming key issued successfully, two beep sounds will be made.

Register Locks to MF-Admin Server

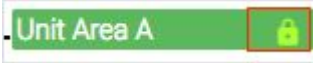
Please bring a tablet or mobile phone with Chrome browser.
Follow below steps to register a lock :

A. Open Chrome and type in MF-Admin server URL.
B. Login to MF-Admin using alzk id.
C. Go to Lock Registration Monitoring function on tablet.
Property Management => **Lock Registration Monitor**



D. Go to Room A
E. Scan programming card to the lock Lockplace A.
You will see the physical new lock connect to MF-Admin server.

F. Link the physical lock on Room A to the lockplace.
Click lock icon near Unit Area A.

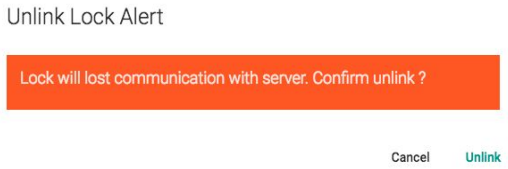


A pop-up window will show up listing all the locks not linked yet. Click the one you like to link.

G. Link the lock to **Room A** lockplace.

G.1. If you link to the wrong lockplace, Unlink and link again.
Click lockplace which you link to the wrong lockplace.

Click **Unlink** to unlink lock.



H. Repeat the steps D to G for Lockplace B,C,D,P and M
I. All set and all locks are ready for go-live phase.

Verify lock registration using Master Card

Master Card is granted unlimited access to any locks in the project. After locks are registered to MF-Admin server, only Residential Cards and Master Cards can be recognized.

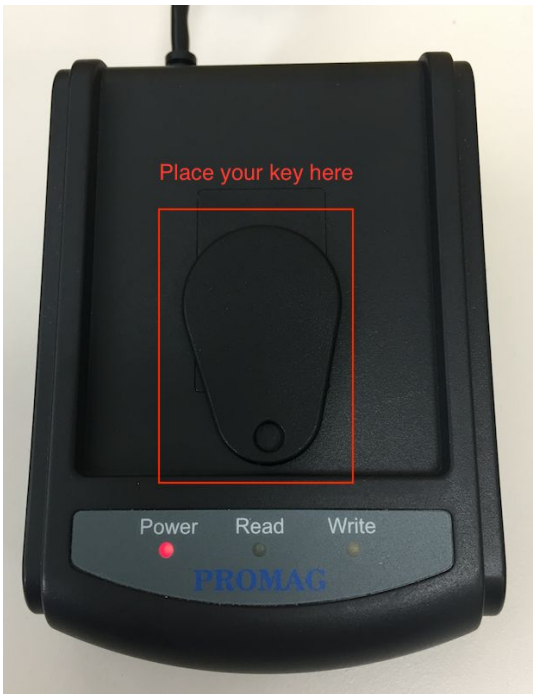
To verify that all the locks are successfully registered and linked to the right lock places in the area tree, let's first create the master card.

- How to create Master Card :

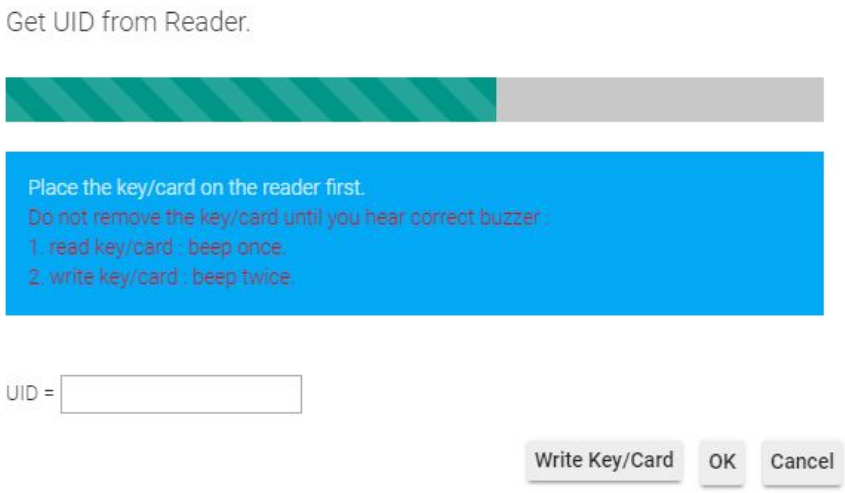
Navigate to issue master card page. **Key Management** => **Issue Master Key**

And click **Issue Key**

Place key/card on reader first.

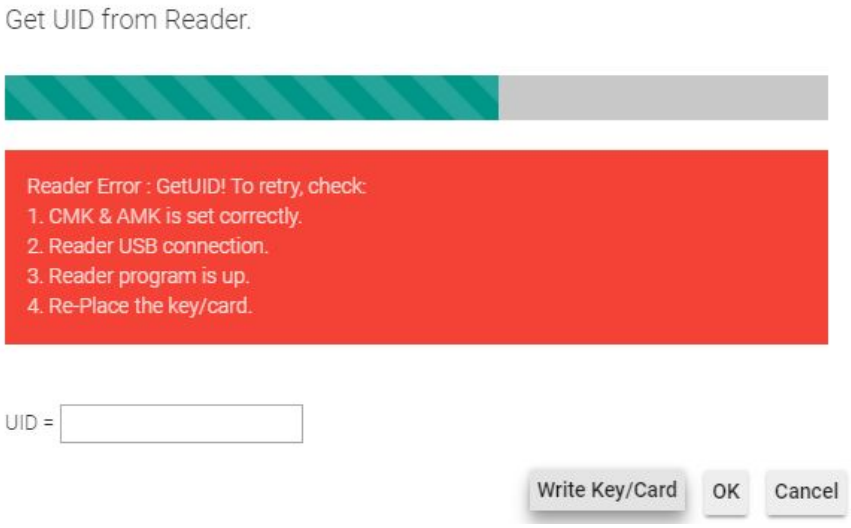


Click **Write Key/Card** to get Key's UID.



The **green light** LED on **Read** should blink.

If **Write Key/Card** failed with **three** beep sounds and display following message, please re-place key/card and click **Write Key/Card** again.



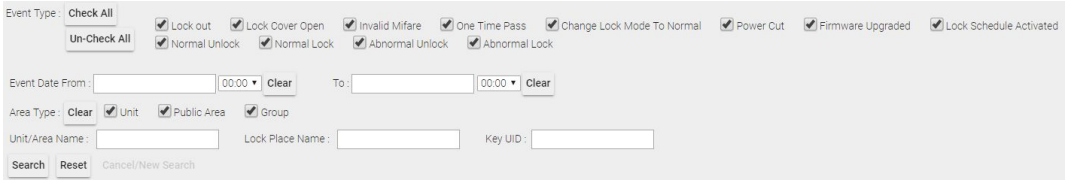
If master key issued successfully, two beep sounds will be made.

- How to verify Master Card to a lock :

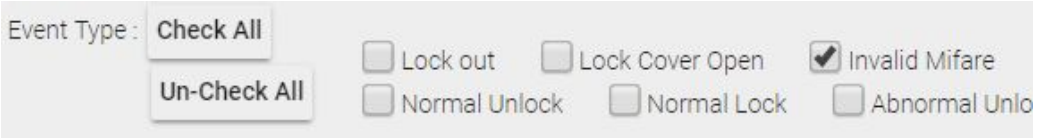
  Prepare an invalid Mifare Card X(You may issue an invalid card easily by assigning wrong area to the card). By default, a lock will report to MF-Admin Server and get the newly create card list from MF-Admin Server every 5 mins(Wall Reader). It means the newly created Master Card will go to the locks after 15 mins. Another way to enforce a lock to communicate with MF-Admin server is to scan an invalid card. We will use this approach to save us some time. Card X will be the invalid Card.

  - Go to lockplace A.
  - Scan Card X.
  - Scan Master Card and the lock should be opened.
  - Scan Card X again.(The event log will be transferred to MF-Admin server)
  - Check MF-Admin Server event log.

    - Navigate to MF-Admin Server event log page.
      Report Management => **Lock Events Report**

    - Check **Invalid Mifare** in **Event Type** fields only and click **Search**.

    - You will see **Invalid Mifare** event with scanning **invalid** card.

No	Actions	Event Date	Event Type	Lock Place Name	Area Type
1		02/12/2019 15:56:56	Invalid Key	Public Area P	
2		02/12/2019 15:59:41	Invalid Key	Room A	

  - Verify lock B, C, D, P, M using the same steps.
  - If lock A is not opened, please rescan Card X and try again.
  - If lock A is still not opened, please unlink the lock and register/link again. Then repeat the verification steps.

- If problem still exist, please contact your reseller for help.

Please keep the Master Card safe and secure.

Congratulations ! The system is ready and let’s go to Go-Live phase.

Go-live Phase

We will present several daily operations when the system goes live. Most of the daily work of an administrator or property owner should be card/key management.

You have seen several card types in the previous sections: Crypto Card, Construction Card, Programming Card and Master Card. Here we will create another card type called Residential Card. There are five types of Residential Card : Tenant, Staff, Vendor, Guest and Temp Card. You can tell the purpose of the card from its name.

There are three supporting features to help you create a residential card. You may create a card without using these features but leverage these template features will speed up the process when you have many cards to create :

- Time Control Template

  Here we will create two time control template which we will use in demonstrate the creation of Guest Card and Vendor Card.
  Please follow below steps to create the two time control templates :

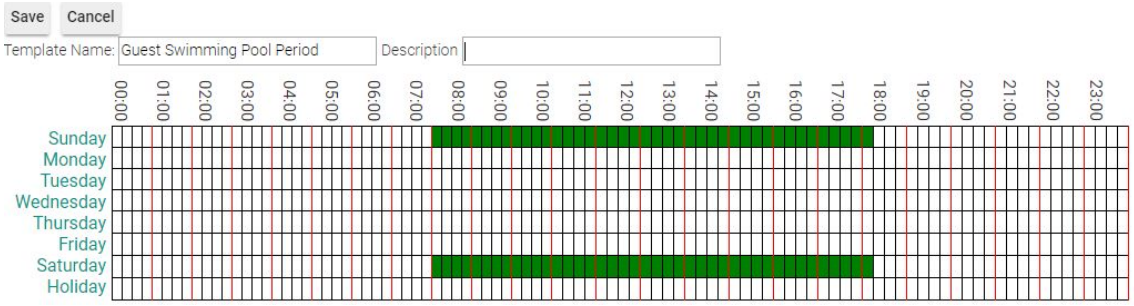
Guest Swimming Pool Period	8:00 ~ 18:00 Sat, 8:00 ~ 18:00 Sun
House Cleaning Period	8:00 ~ 12:00 Mon

❖ Steps to create time control template

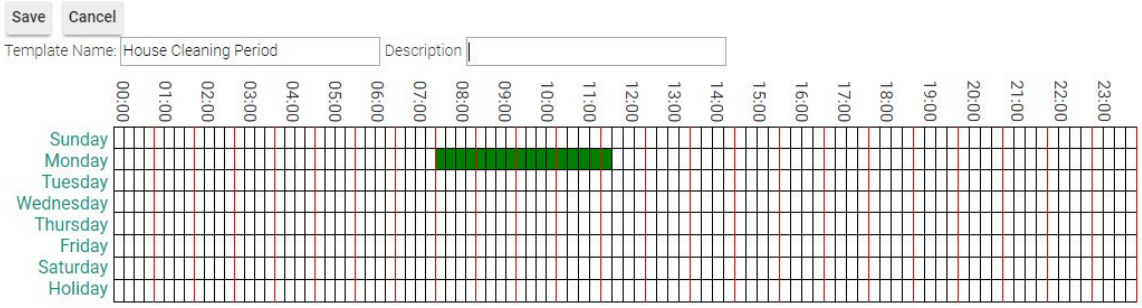
Navigate to create time control template page.
System Management => **Application Parameters**

In **Time Control Templates** click **Create** button.

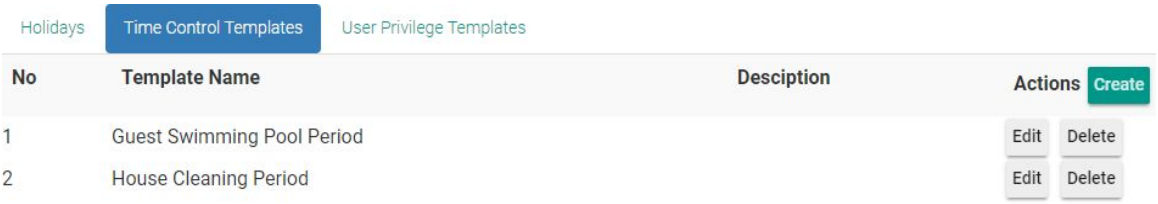
Edit the template name, According to the document, the Guest Swimming Pool Period only open on **8:00 ~ 18:00 Sat, 8:00 ~ 18:00 Sun**. Let's edit the time control to meet the requirement and click **Save** to save time control setting.



Let's create another template for house cleaning period. According to the requirement, house cleaning period only allow at **8:00 ~ 12:00 Mon**. Let's edit the time control to meet the requirement and click **Save** to save time control setting.



Both **Guest Swimming Pool Period** and **House Cleaning Period** time control templates are created successfully.



- User Management

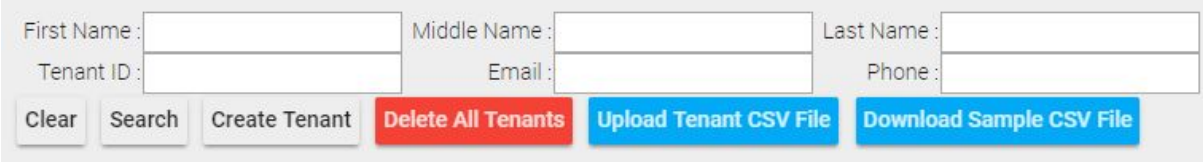
You may maintain tenants, staffs and vendors information in User Management module. The information you entered here is only for look up purpose when issuing card which we will demo later. The benefit to create entries here is to save you some typing when issue cards/keys.

Let's create some user templates. We just provide basic information for demo purpose.

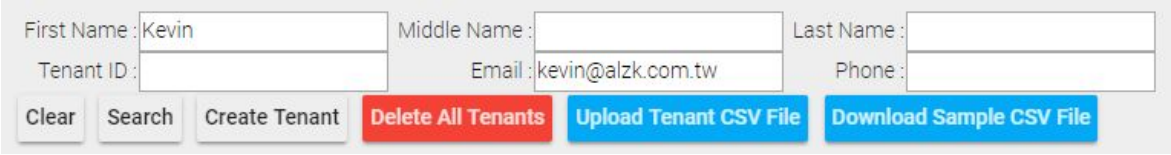
User Type	Information
Tanant A	Kevin Huang, kevin@alzk.com.tw
Tenant B	Tony Lin, lintungwei@gmail.com
Tenant C	Mark Chu, mark@alzk.com.tw
Tenant D	Jay Chen, jay@alzk.com.tw
Staff S1	Peter Liu, peter@alzk.com.tw
Staff S2	Ricky Chang, ricky@alzk.com.tw
Vendor V	Company Name : Dust Buster Employee name : Vincent Chou, vincent@gmail.com

❖ Steps to create tenants

Navigate to create tenants page. **User Management** => **Tenant**



Edit tenant information and click **Create Tenant**.

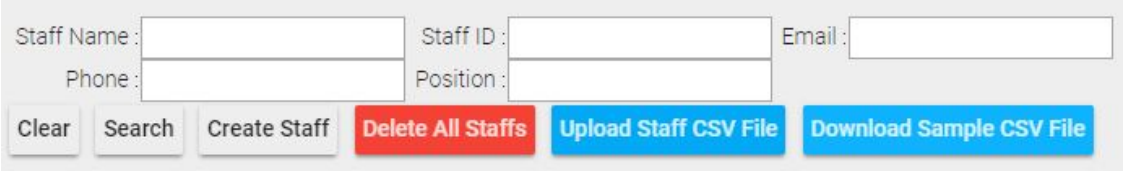


The table below the input area will list all the tenants created :

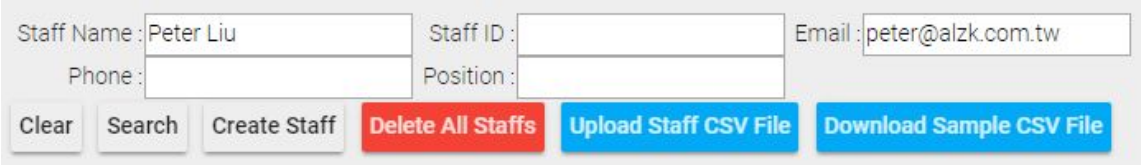
Please repeat the work and create tenant B, C, and D.

❖ Steps to create staffs

Navigate to create staffs page. **User Management** => **Staff**



Edit staff information and click **Create Staff**.

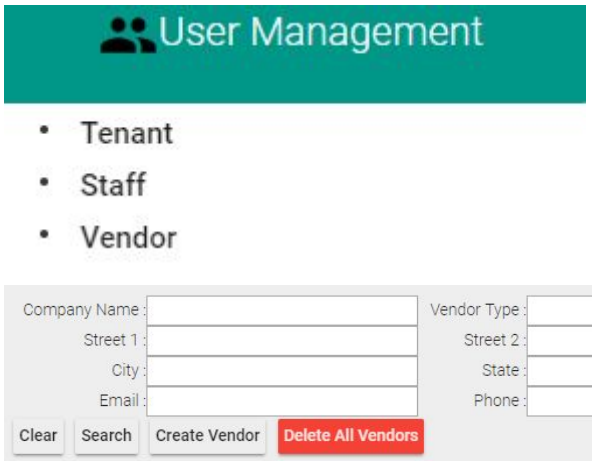


The table below the input area will list all the staffs created :

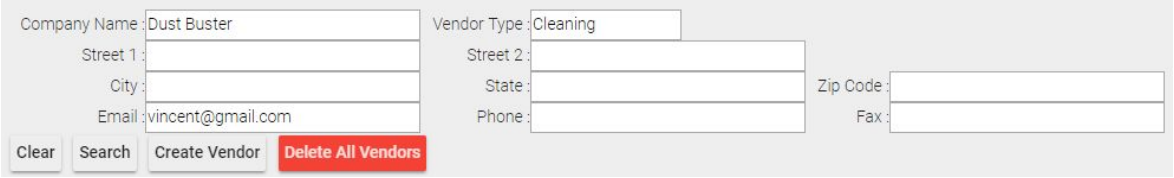
Follow the same process to create staff Ricky Chang.

❖ Steps to create vendors

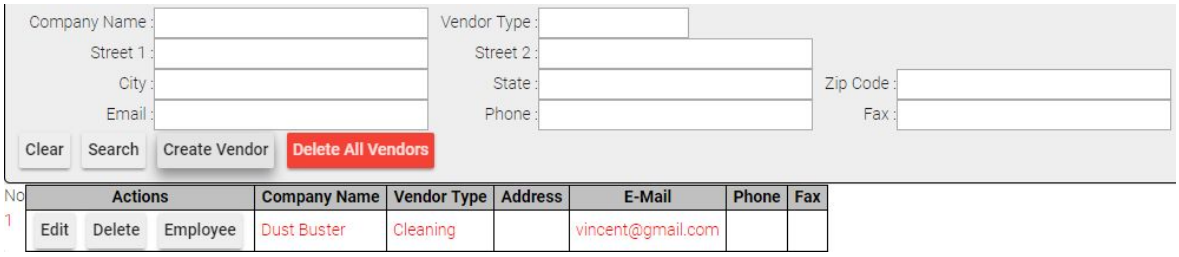
Navigate to create vendors page.
User Management => **Vendor**



Edit vendor information and click **Create Vendor**.



It will display vendor list below the input area.



Click **Employee** button on **Actions** filed to add employee.

Edit employee information and click **Create New Employee**

The employee list will be displayed at the bottom of this page.

- Key Template

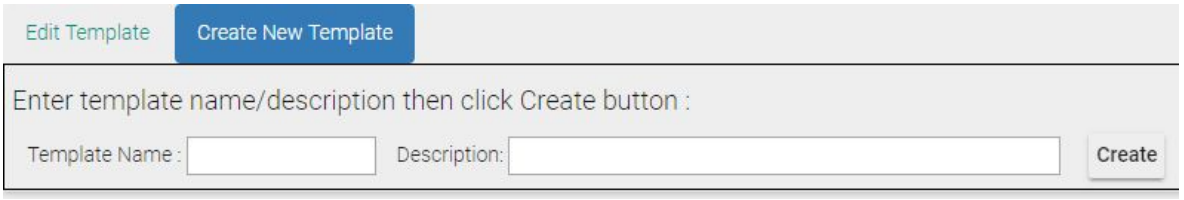
Key template probably is the most useful supporting features when issue abundant keys. It is almost the same as issue a key but you may save the setting for later use. Let's create two templates :

STAFFS	Public Area P (24 hours allowed), Group Area M (24 hours allowed)
TENANTS	Public Area P (6:00 ~ 21:00), Group Area M (24 hours allowed)

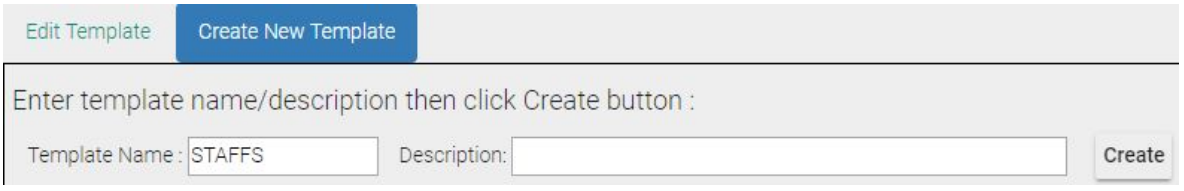
❖ Steps to create the key template

Navigate to create key time control template page.
Key Management => **Key Template**

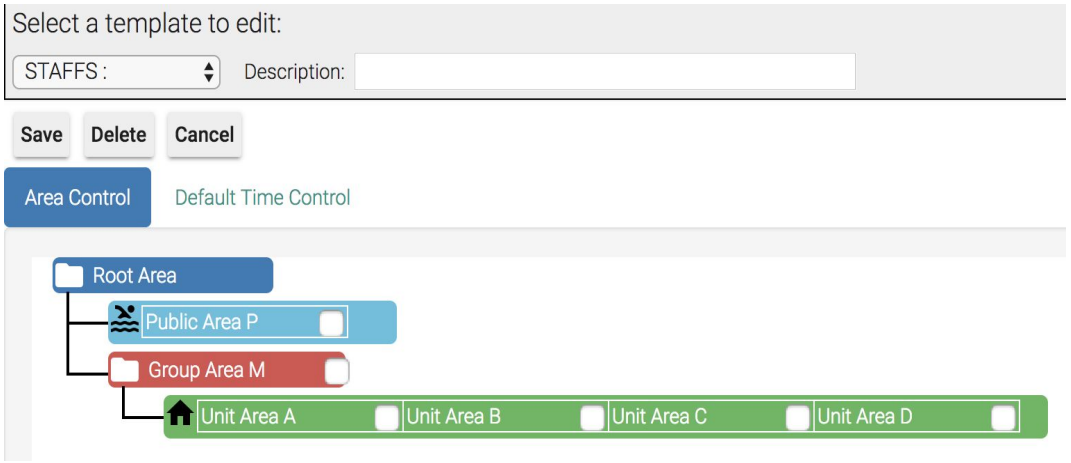
Select **Create New Template.**



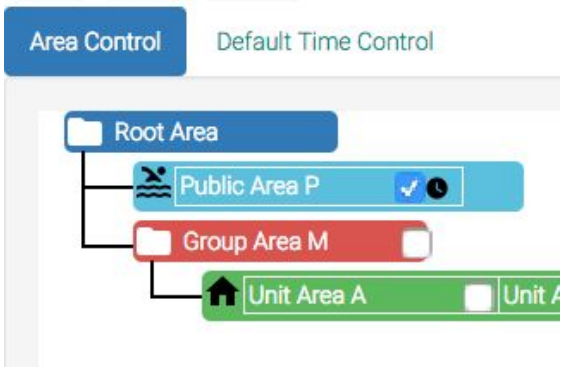
Edit **Template Name** and click **Create**



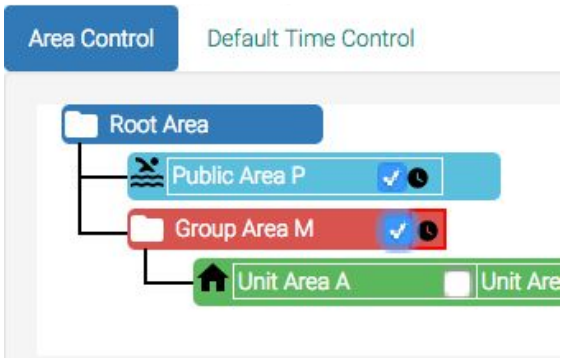
After clicking **Create** button it will display **Area Control** page.



According to the requirement, Staffs can access **Public Area P (24 hours allowed), Group Area M (24 hours allowed)**. Let's check the box on **Public Area P** and no need to edit time control because it's 24 hours open by default. (Click on the clock besides the checkbox can edit the time control settings to this area.)

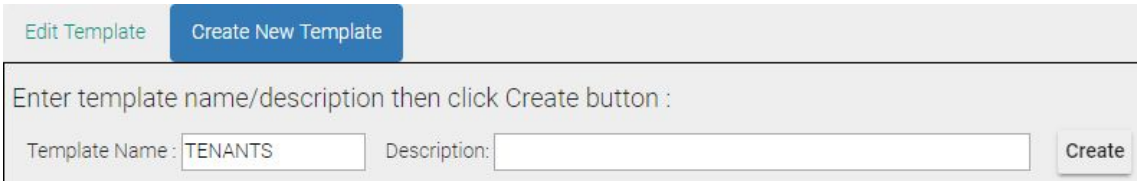


Tick the checkbox on **Group Area M** and leave the time control settings as default.

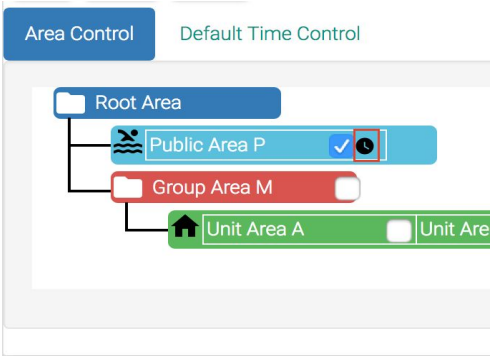


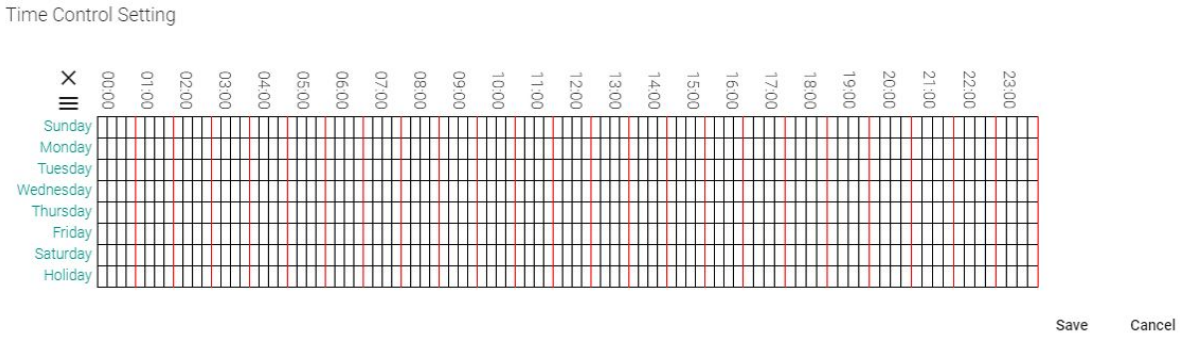
Click **Save** to save **STAFFS** key template.

Let's create another key template for **TENANTS.** Click **Create**.

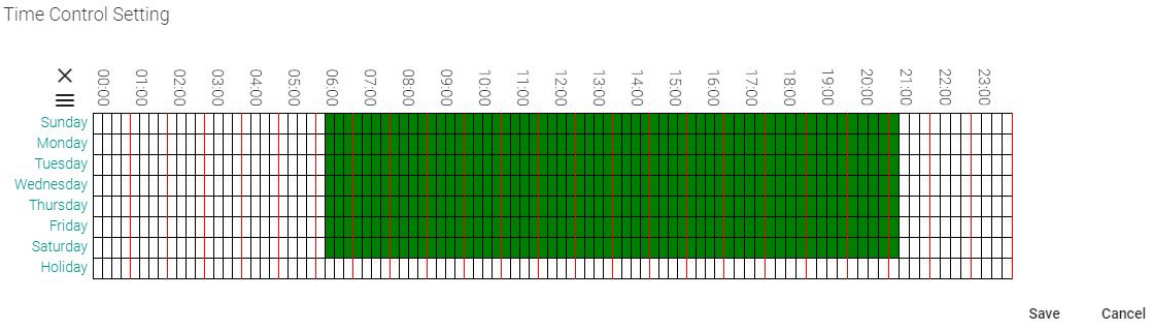


Check the box on **Public Area P** and click its **time control button**.

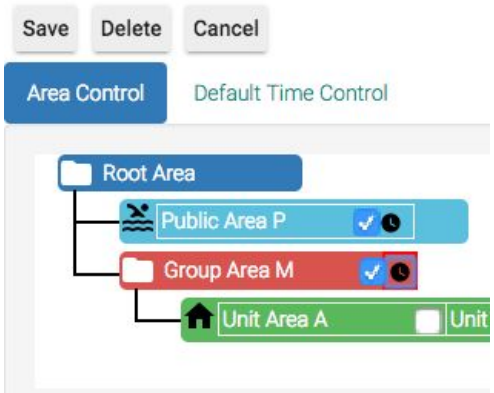




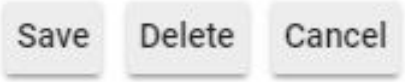
According to the requirement, Tenants can access **Public Area P (6:00 ~ 21:00), Group Area M (24 hours allowed)**. Let's edit the **Public Area P** time control and click **Save** to save time control setting.



Tick the checkbox on **Group Area M**, no need to edit time control this time because it's 24 hours open by default.



Click **Save** to save **TENANTS** key template.



Navigate to key template management page.
Key Management => **Key Template**

You can see those key templates has been created by pull down the select list.

Create Tenant Cards

In SIMPLE project, you should at least create 4 tenant cards (Card A~D) for Room A to D with below access control :

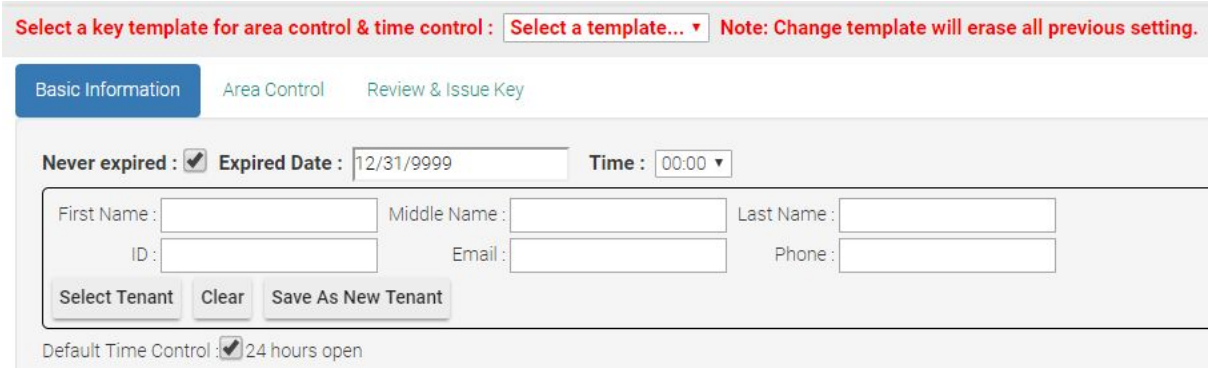
Card A	Public Area P (6:00 ~ 21:00), Group Area M (24 hours allowed), Unit A (24 hours allowed)
Card B	Public Area P (6:00 ~ 21:00), Group Area M (24 hours allowed), Unit B (24 hours allowed)
Card C	Public Area P (6:00 ~ 21:00), Group Area M (24 hours allowed), Unit C (24 hours allowed)
Card D	Public Area P (6:00 ~ 21:00), Group Area M (24 hours allowed), Unit D (24 hours allowed)

As you can see, leverage key template is a good idea to create the 4 tenants cards.

❖ Steps to create tenant cards

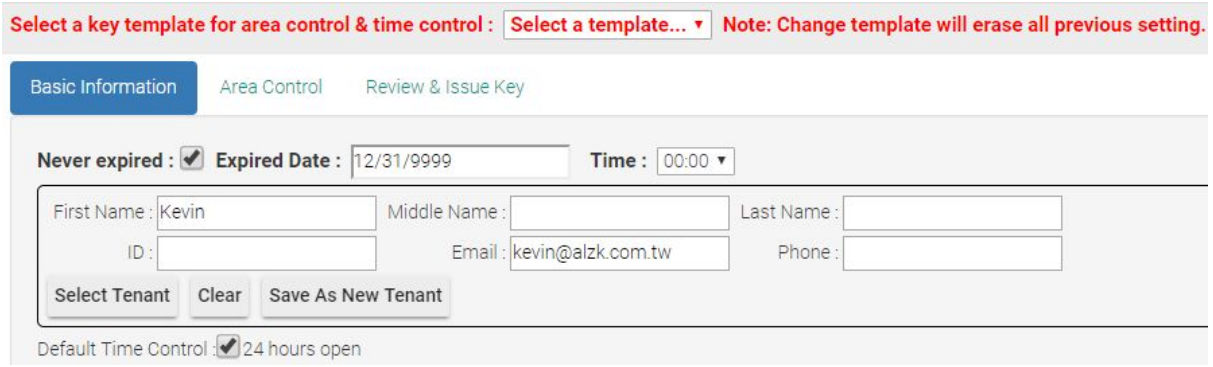
Navigate to Issue Key page. **Key Management** => **Issue Key**

Select **Tenant** at the key type drop down list**.**

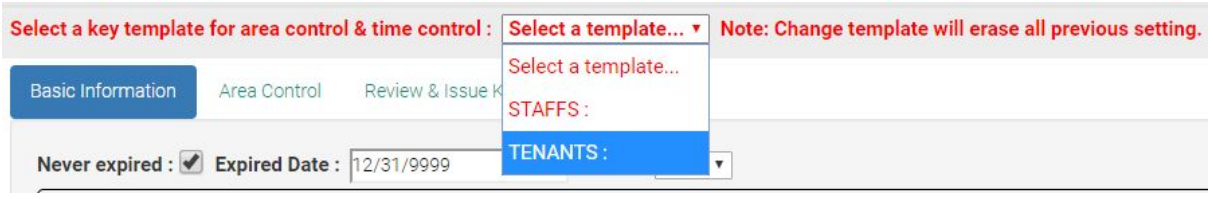


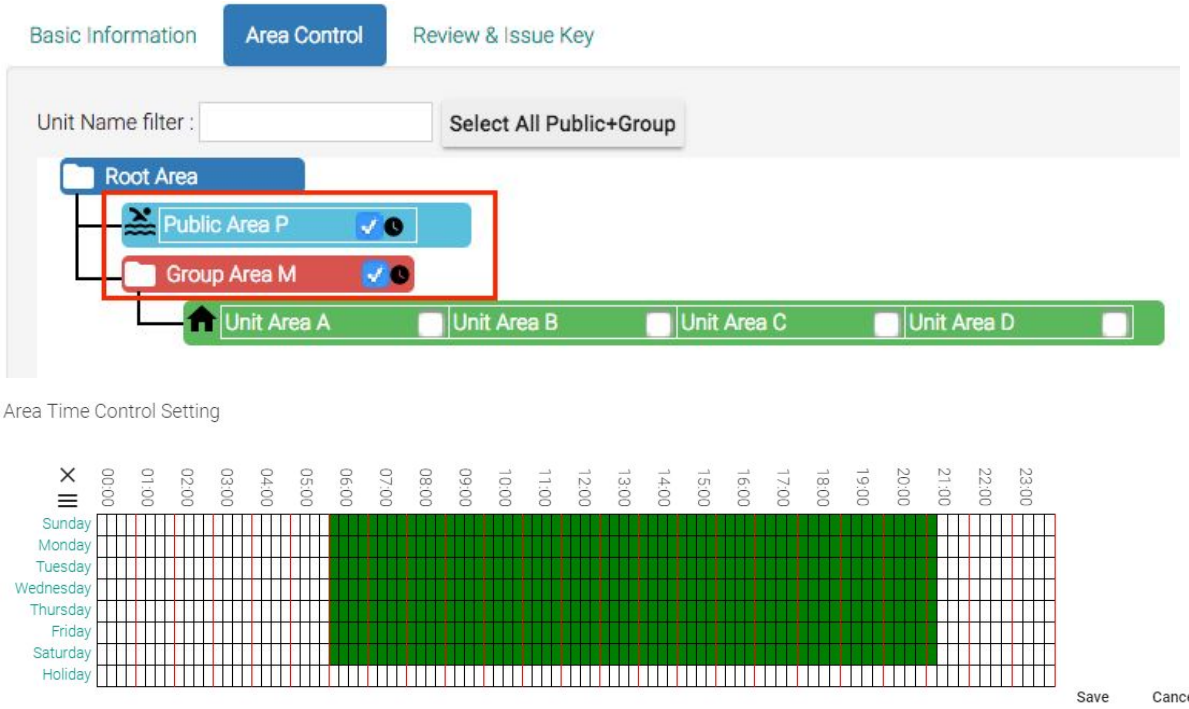
Click **Select Tenant** and it will pop up a window to display all tenants you created in user management function. Select tenant **kevin** to issue key.

Select tenant kevin will automatically bring his information back to the Basic Information tab.

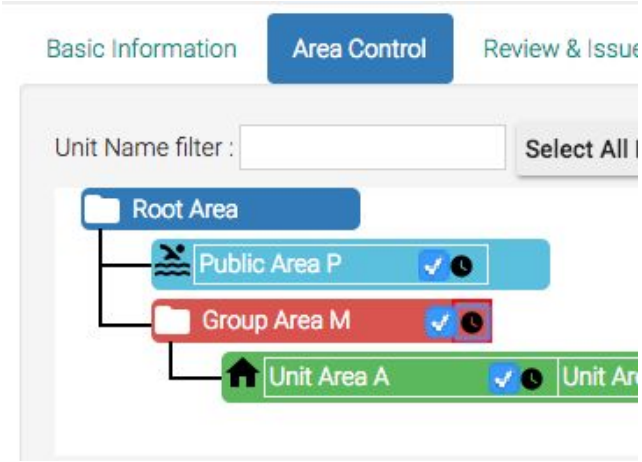


Select **TENANTS** key template and you will see TENANTS time control settings in **Area Control** page

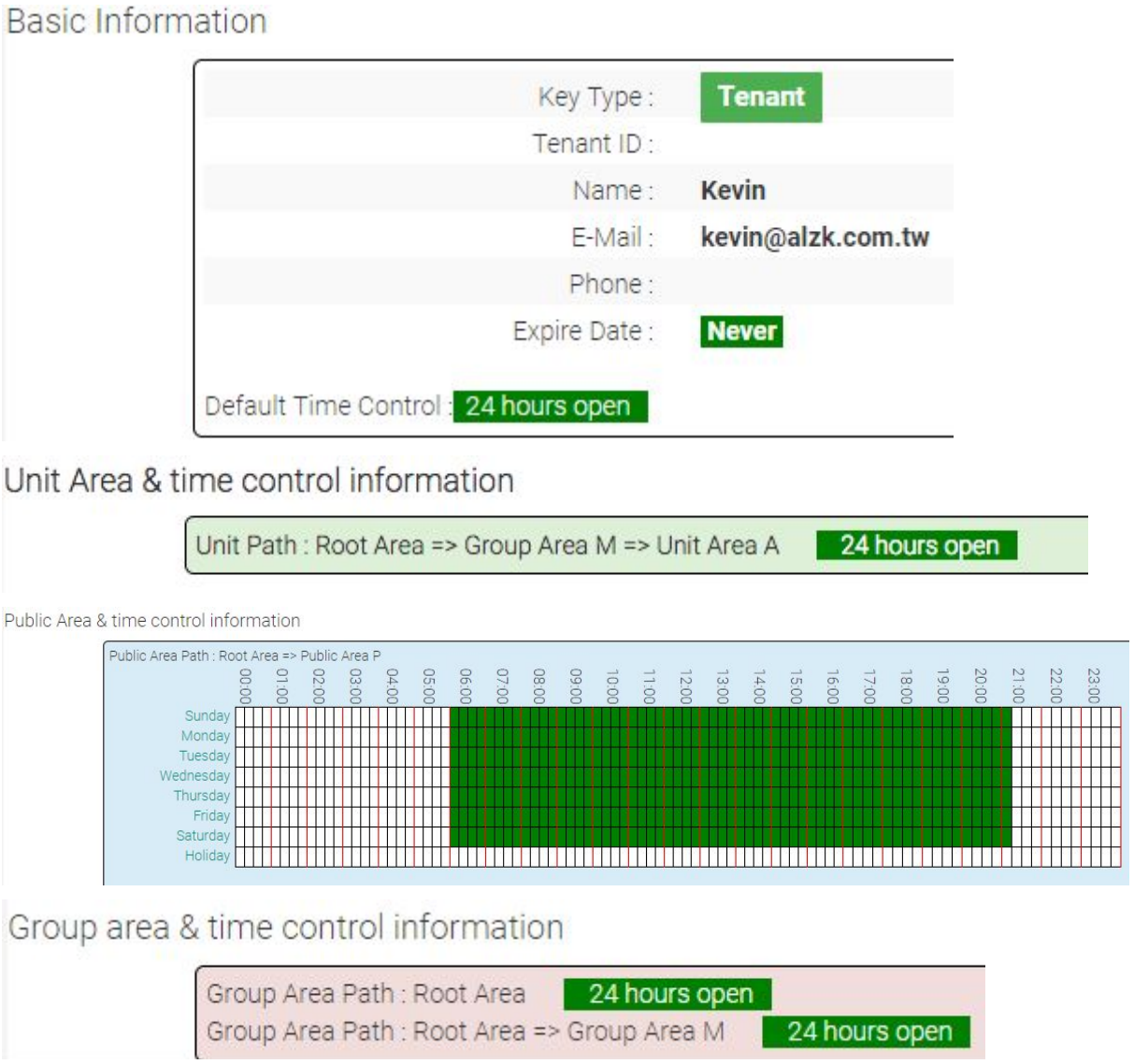




According to the requirement, tenant **Kevin** can access **Public Area P (6:00 ~ 21:00), Group Area M (24 hours allowed), Unit A (24 hours allowed)**. We had already set up time control of **Public Area P** and **Group Area M** via tenant key template, so let's check **Unit A** to grant access to Room A.

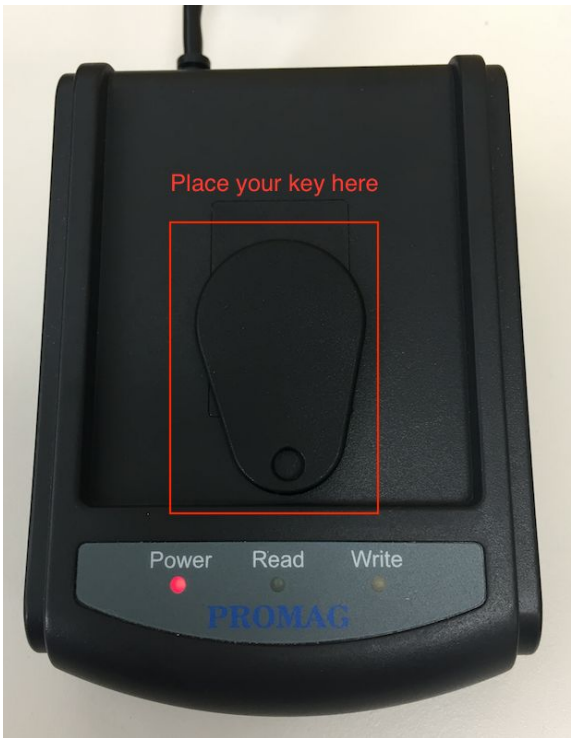


At the **Review & Issue Key** page we can verify the information of tenant key including **Basic Information**, **Unit Area & time control information, Public Area & time control information**, **Group area & time control information**

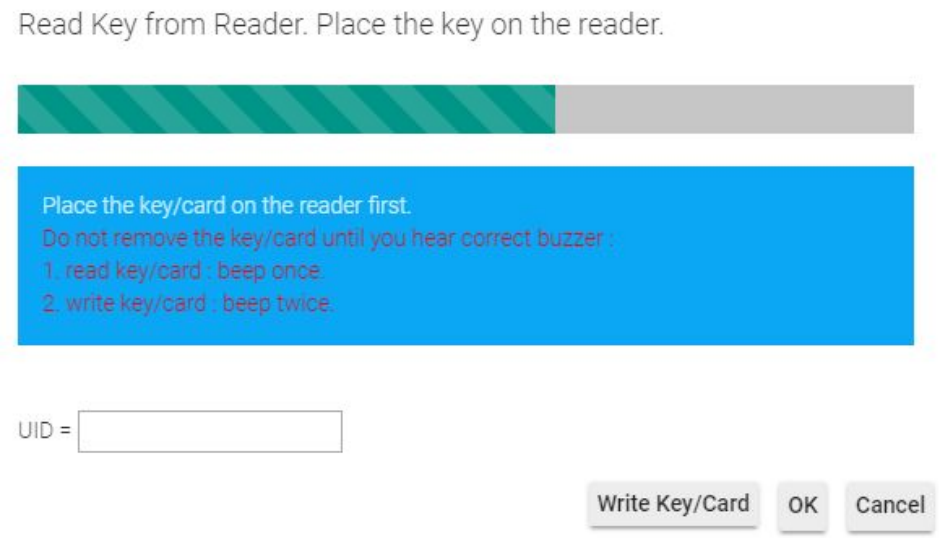


Click **Issue/Write Key** to issue tenant key.

Place key/card on reader first.

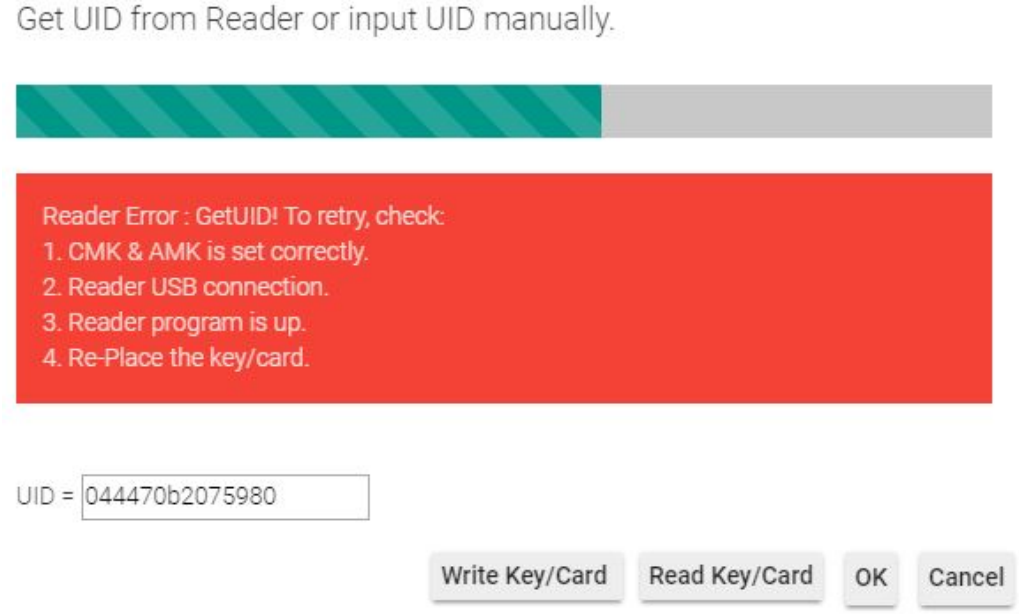


Click **Read Key From Reader** to get Key's UID.

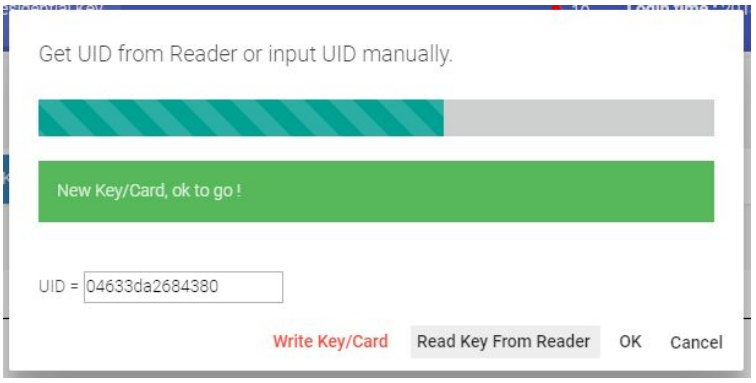


The **green light** LED on **Read** should blink.

If **Write Key/Card** failed with **three** beep sounds and display following message, please re-place key/card and click **Write Key/Card** again.



If read key successfully click **Write Key/Card** to issue master key.



Write Key/Card successfully with **two** beep sounds.

Repeat the similar process to create Tenant Cards for B,C and D.

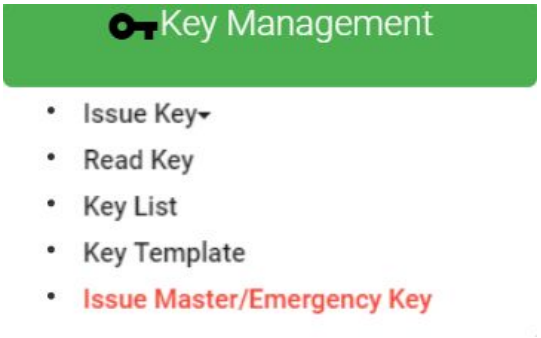
Create Staff Card

We will then create 2 staff cards in SIMPLE project. Again, you may use the STAFFS key template to complete this job. This time you can practice to choose the staff information from the staff users you created previously.

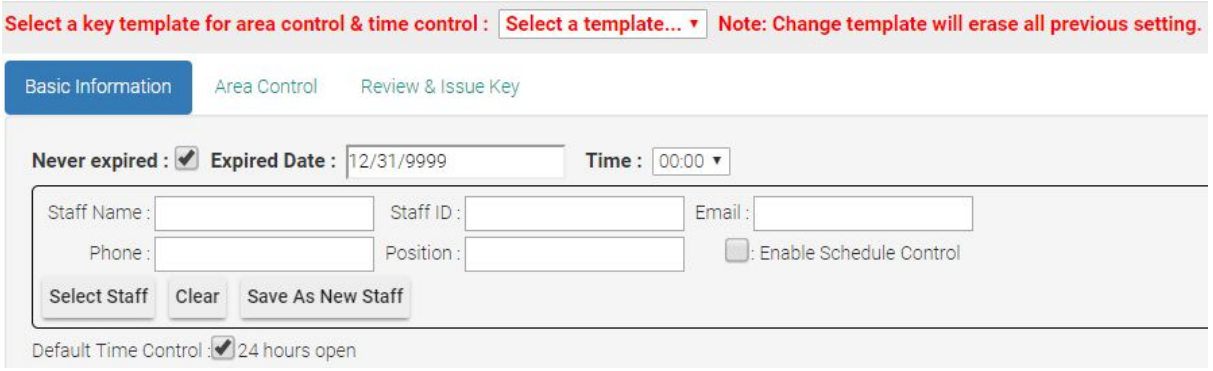
Staff S1	Public Area P (24 hours allowed), Group Area M (24 hours allowed)
Staff S2	Public Area P (24 hours allowed), Group Area M (24 hours allowed)

❖ Steps to create staff card

Navigate to Issue Key page. **Key Management** => **Issue Key**

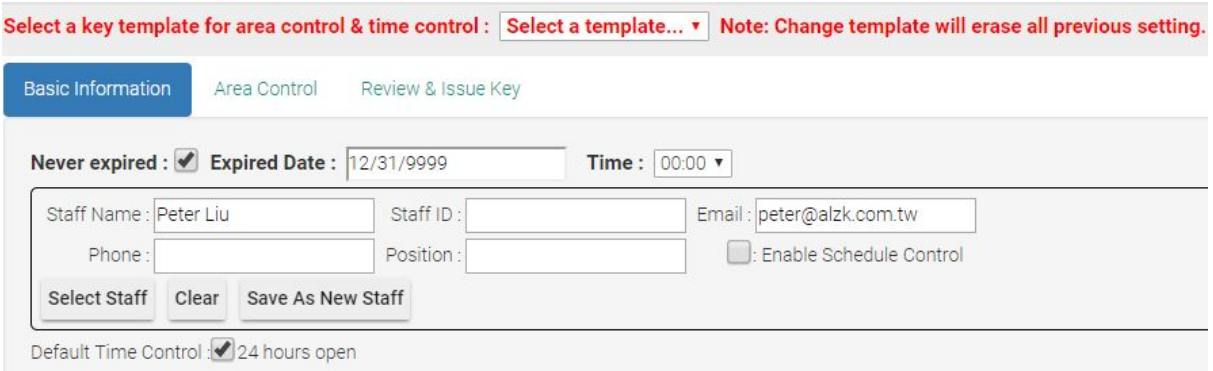


Select key type as **Staff.**

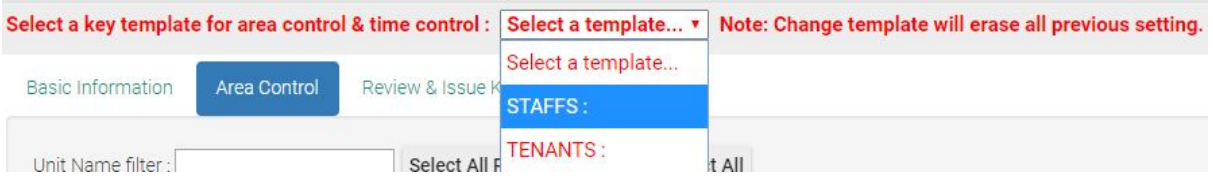


Click **Select Staff** and it will pop up a window to display all staffs you created at user management. Select staff **Peter** to issue key.

After selecting staff peter the **Basic Information** page will automatically attach staff's information.

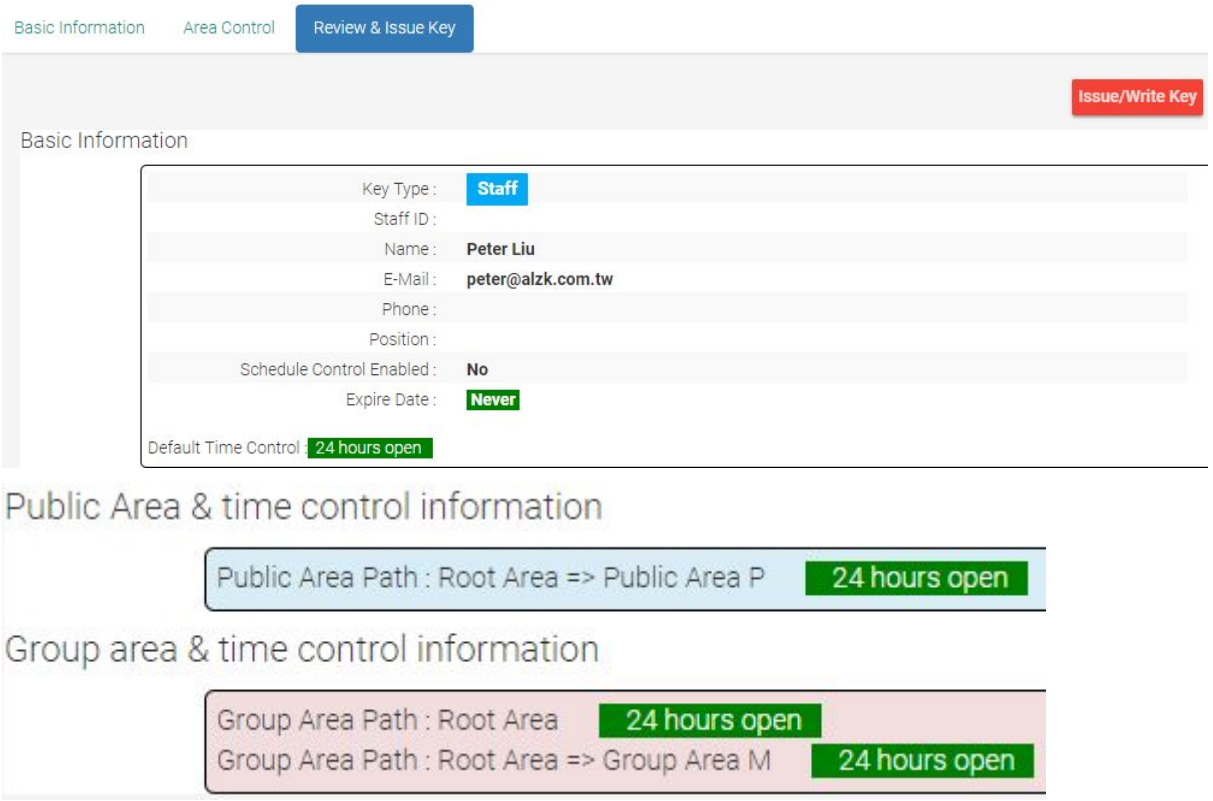


Select **STAFFS** key template and you will see STAFFS time control settings in **Area Control** page.



According to the requirement, staff **Peter** can access **Public Area P (24 hours allowed), Group Area M (24 hours allowed)**. We had already set up 24 hours access privilege of **Public Area P** and **Group Area M** via staff key template. So you may go to the review & Issue Key tab.

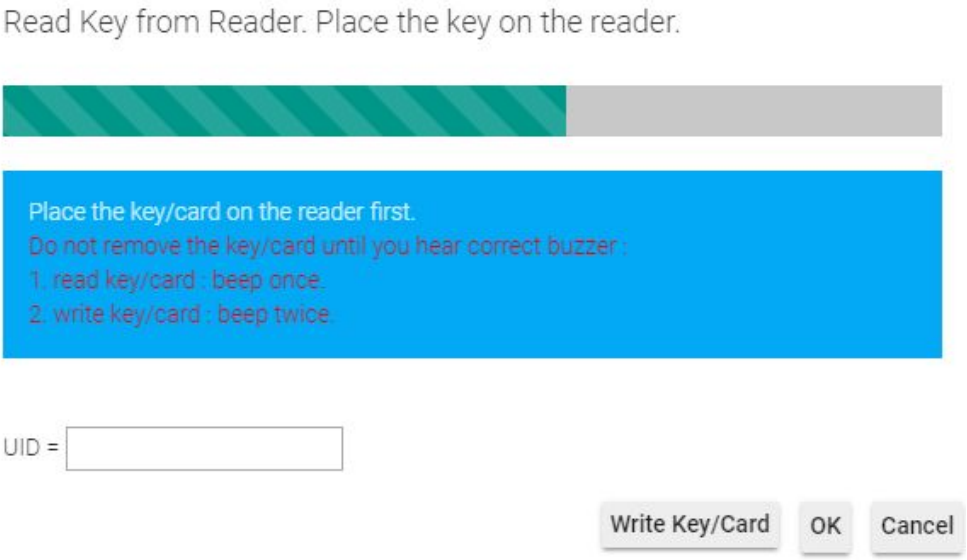
At the **Review & Issue Key** page we can verify the information of staff key including **Basic Information**, **Unit Area & time control information, Public Area & time control information**, **Group area & time control information**



Click **Issue/Write Key** to issue **Peter** staff key.

Place key/card on reader first.

Click **Write Key/Card** to get Key's UID.

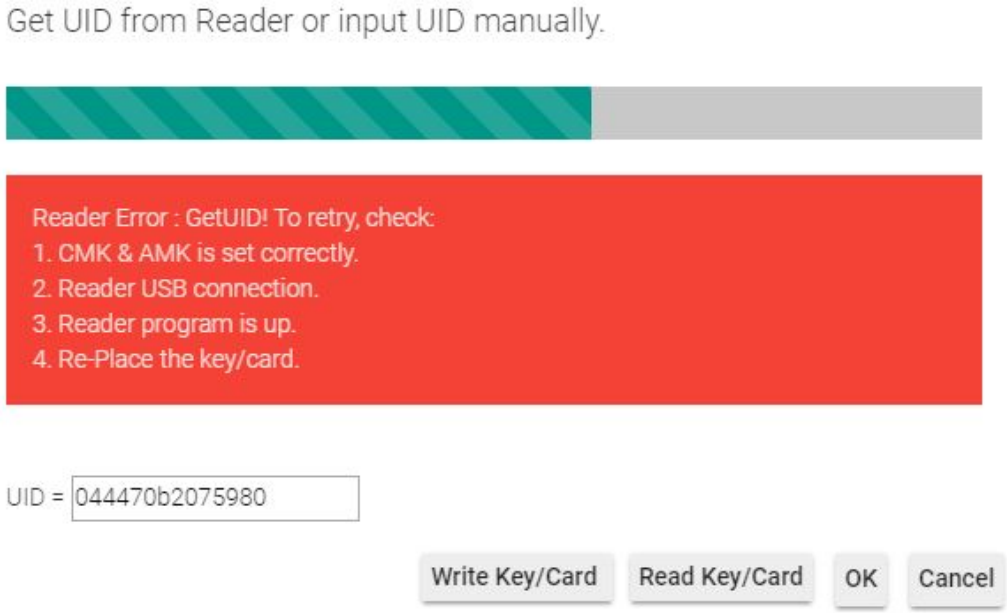


The **green light** LED on **Read** should blink.

If **Write Key/Card** failed with **three** beep sounds and display following message, please re-place key/card and click **Write Key/Card** again

Write Key/Card successfully with **two** beep sounds.

Repeat the similar process to create S2 Staff Card..



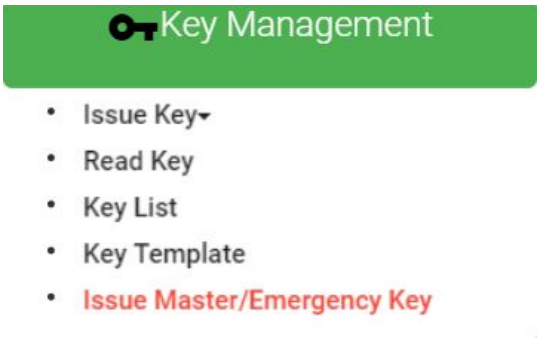
Create Vendor Card

Create a vendor card for Vincent Chou, an employee of Dust Buster cleaning company.

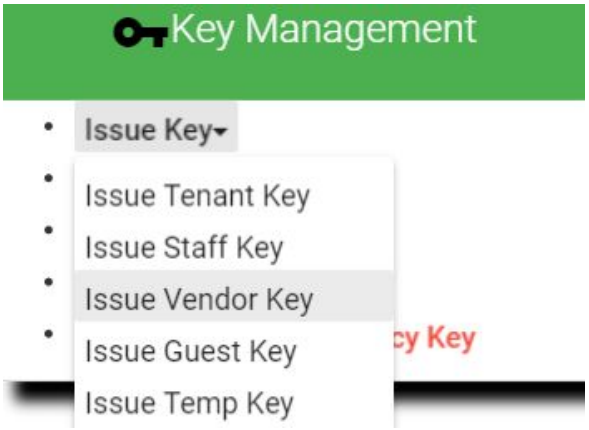
He will come to clean the swimming pool and the area around Room A~D at 8:00 - 12:00 on every Monday. So we will create a card for him to enter Lockplace P and Lockplace M with time control template : House Cleaning Period.

❖ Steps to create vendor card

Navigate to Issue Key page. **Key Management** => **Issue Key**



Select key type as **Vendor.**



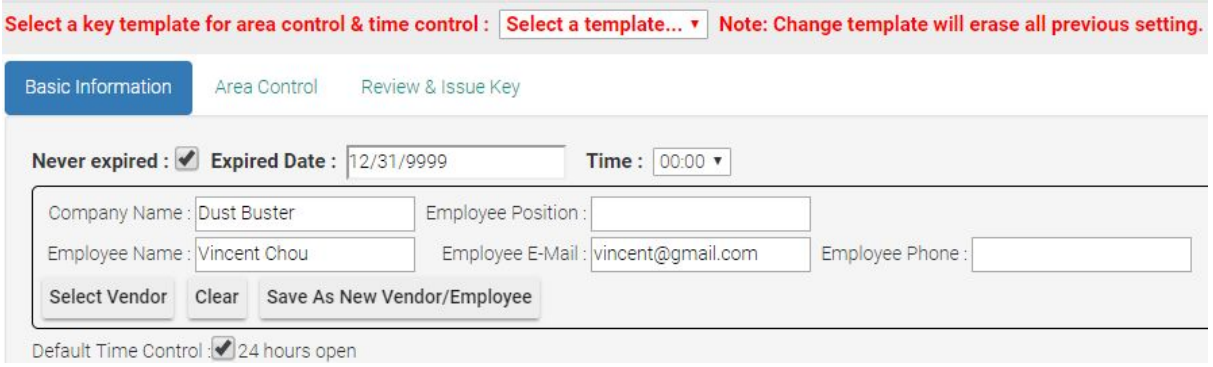
Click **Select Vendor** and it will pop up a window to display all vendors you created before at user management function. Select vendor **Vincent** from Dust Buster to issue key.

Click the row to select :

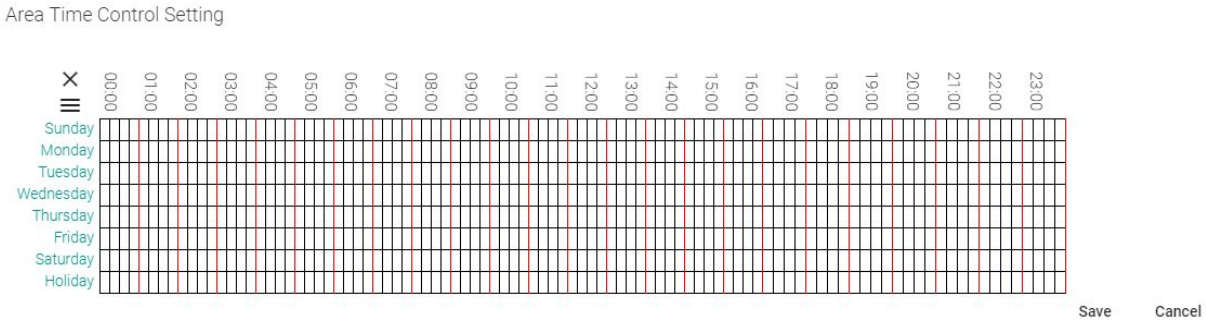
No	Company Name	Vendor Type	Address	Vendor E-Mail	Vendor Phone	Vendor Fax	Emp Name	Emp Position	Emp E-Mail	Emp Phone
1	Dust Buster			vincent@gmail.com			Vincent Chou		vincent@gmail.com	

Cancel

After selecting vendor vincent, the **Basic Information** page will automatically attach vendor's information.

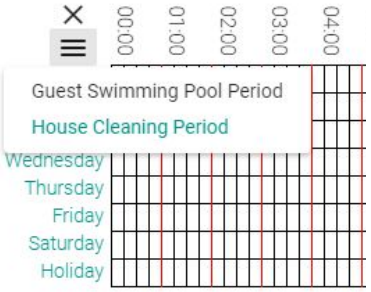


Check the box on **Public Area P** and click **time control button** to edit.

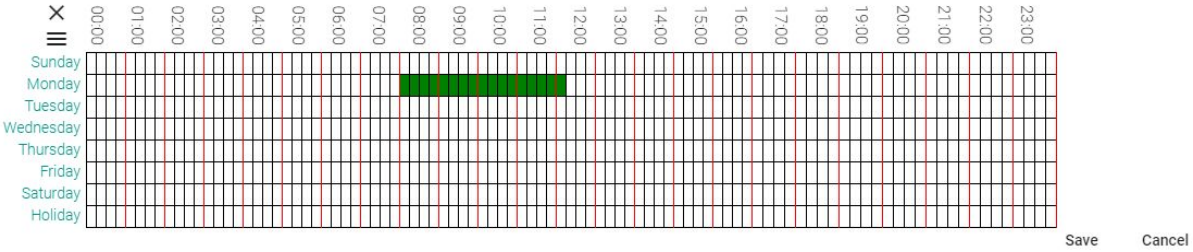


According to the requirement, Vendors can access at **8:00 - 12:00 on every Monday**. Let's use **House Cleaning Period** time control template we created before on **Public Area P** then click **Save** to save time control setting.

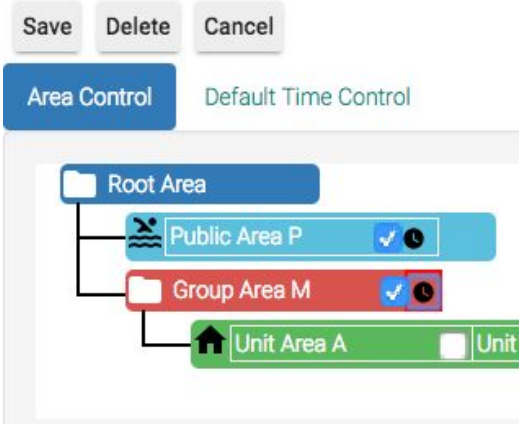
Area Time Control Setting



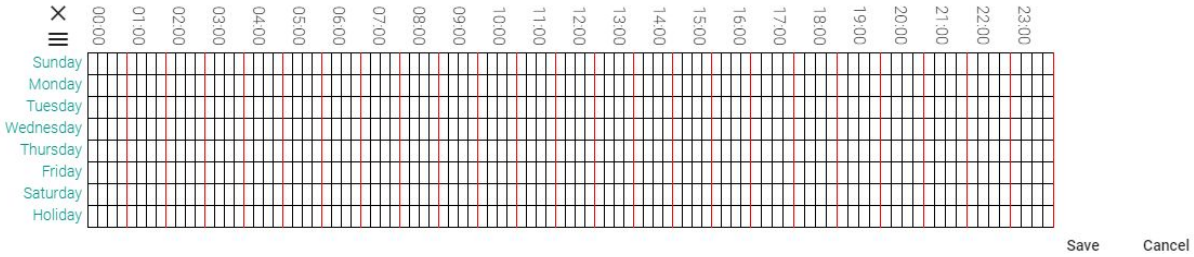
Area Time Control Setting



Check the box on **Group Area M** and click **time control button** to edit.

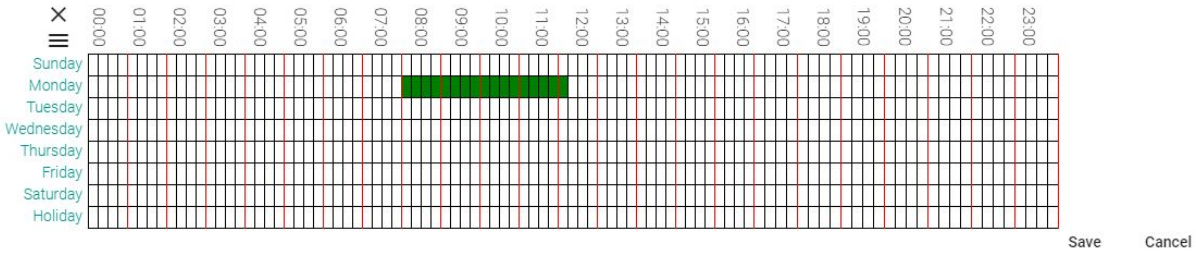


Area Time Control Setting

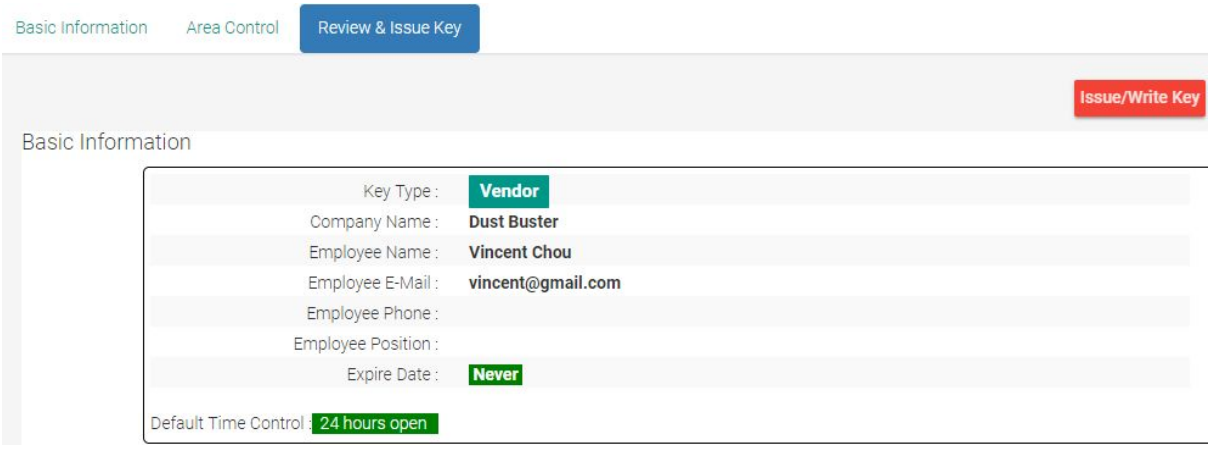


Use **House Cleaning Period** time control template we created before on **Group Area M** then click **Save** to save time control setting.

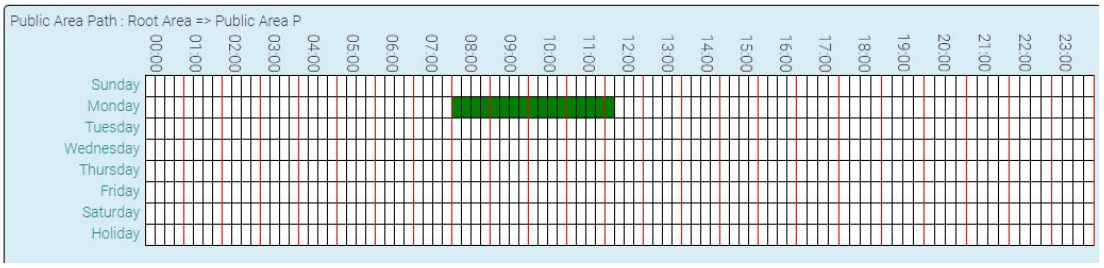
Area Time Control Setting

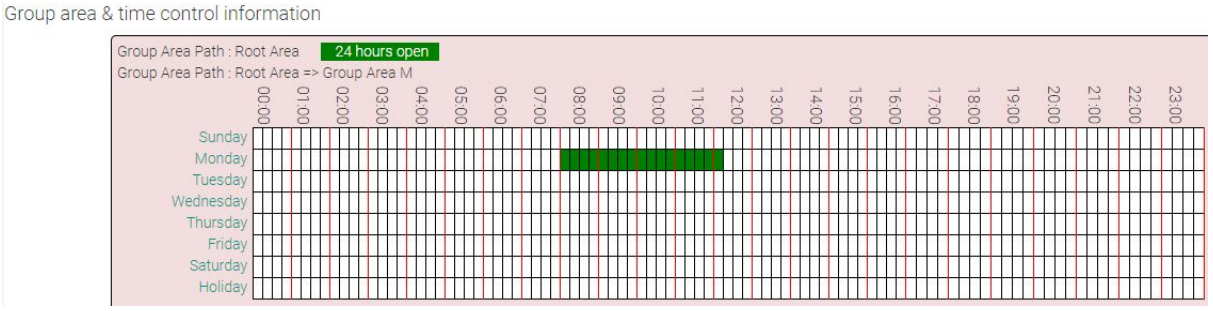


At the **Review & Issue Key** page we can verify the information of vendor key including **Basic Information**, **Unit Area & time control information, Public Area & time control information**, **Group area & time control information**



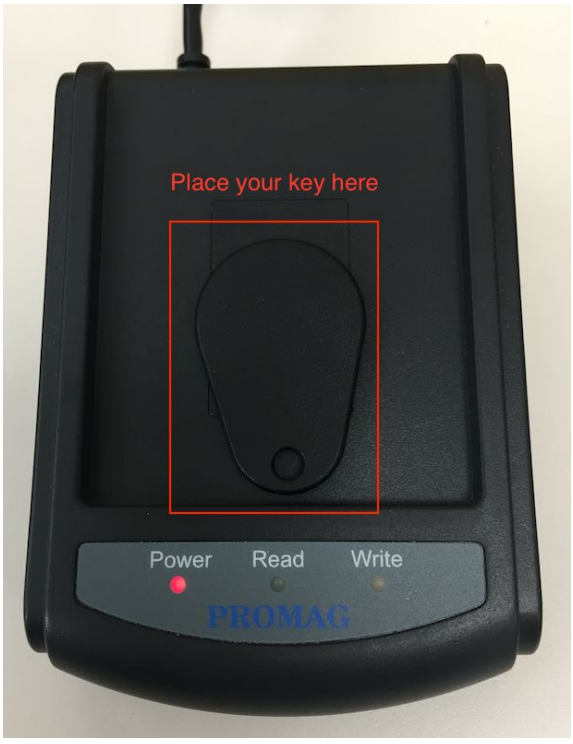
Public Area & time control information



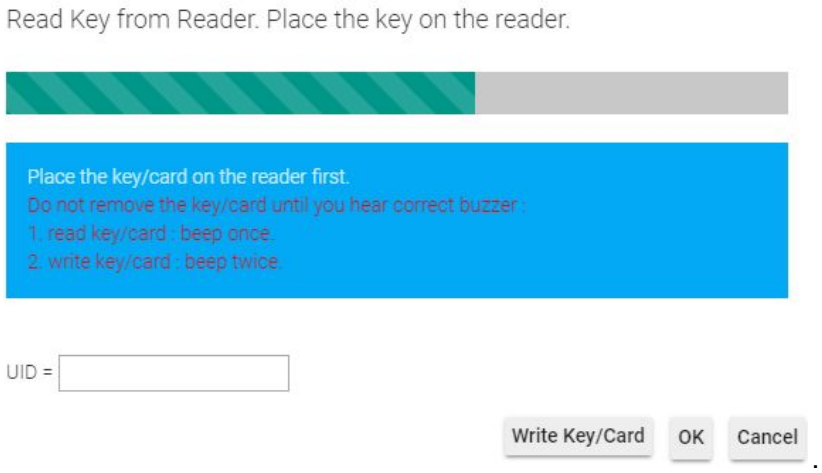


Click **Issue/Write Key** to issue the vendor key.

Place key/card on reader first.



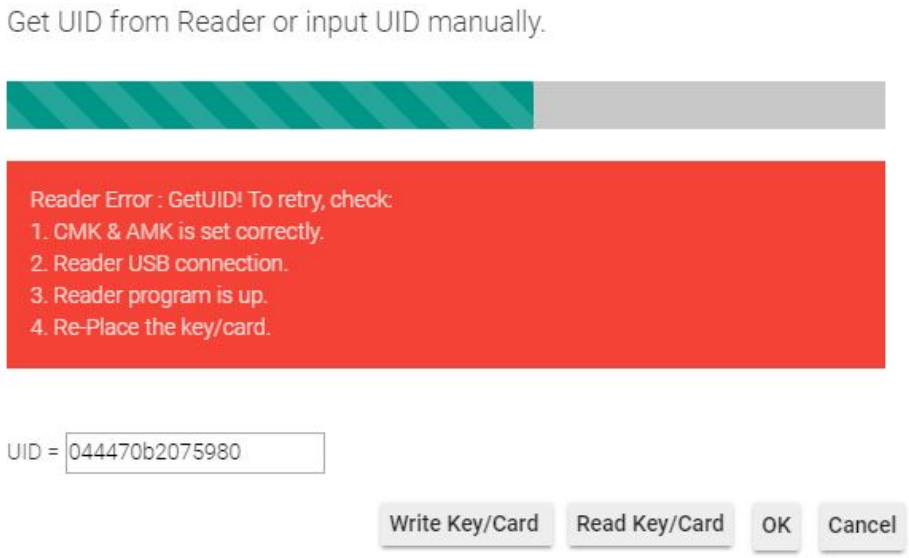
Click **Write Key/Card** to get Key's UID.



The **green light** LED on **Read** should blink.

If **Write Key/Card** failed with **three** beep sounds and display following message, please re-place key/card and click **Write Key/Card** again.

Write Key/Card successfully with **two** beep sounds..



Create Guest/Temp Card

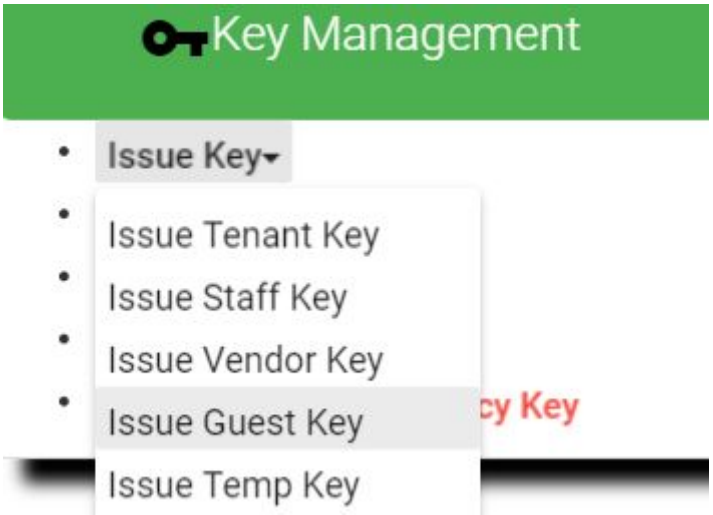
Guest Card and Temp Card are almost the same. They serve the purpose to temporarily grant access to a visitor. The default expired date will be one day only. The one time pass attribute can be used to further restrict access to lockplace to only one time for all the lockplaces granted. Below is a demo to create a Guest Card. Create a temp card is the same.

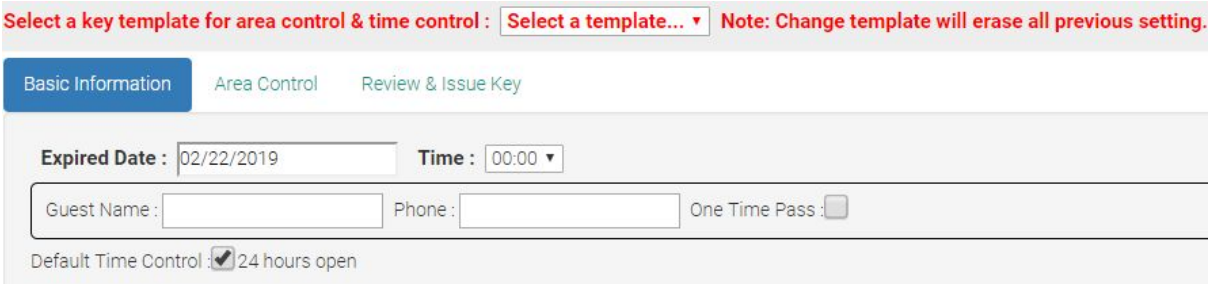
You will request the visitor to return the Guest/Temp Card when they leave the property. The returned card can be reused to issue any card types.

- Steps to create a guest card

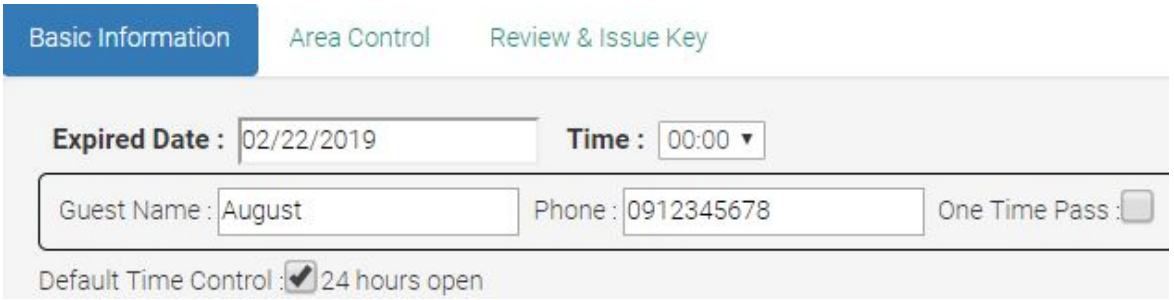
Navigate to Issue Key page. **Key Management** => **Issue Key**

Select key type as **Guest.**

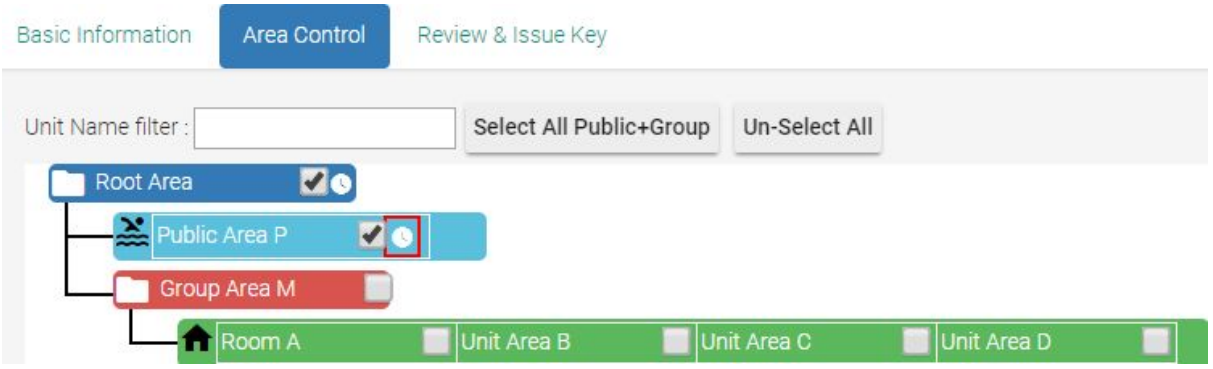




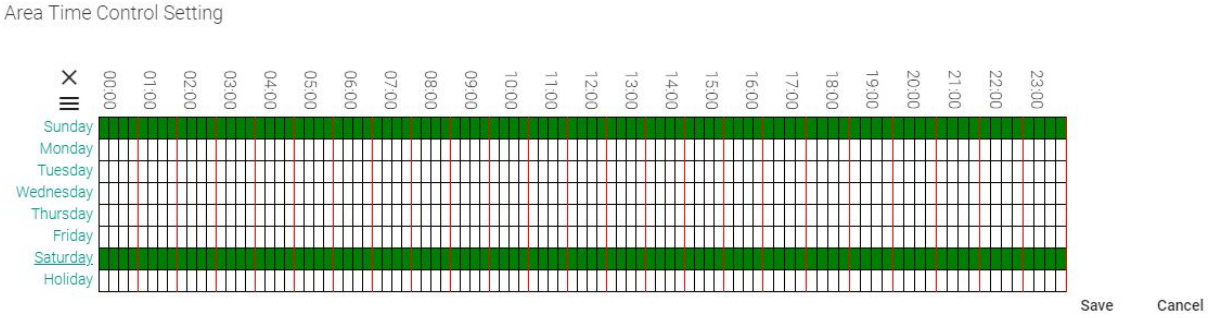
Edit guest information.



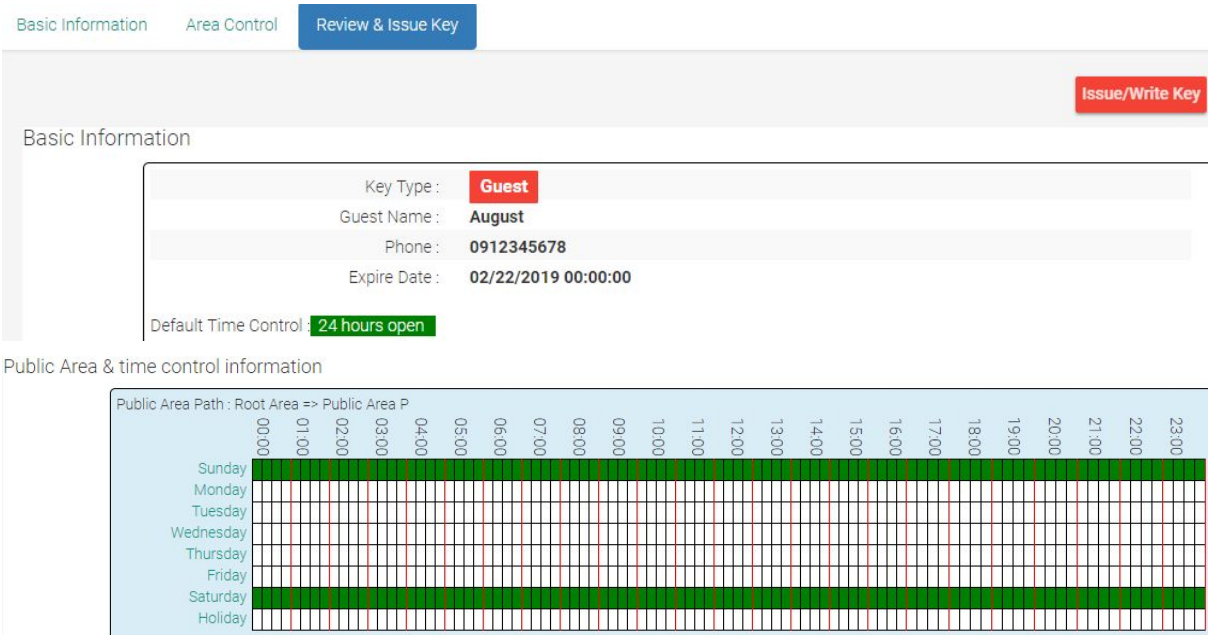
At **Area Control** page, Check the box on **Public Area P** and click edit **time control button**.



Let's assume guest **August** can access **Public Area P** on this **weekend**, edit time control settings and click **Save** to save time control setting.

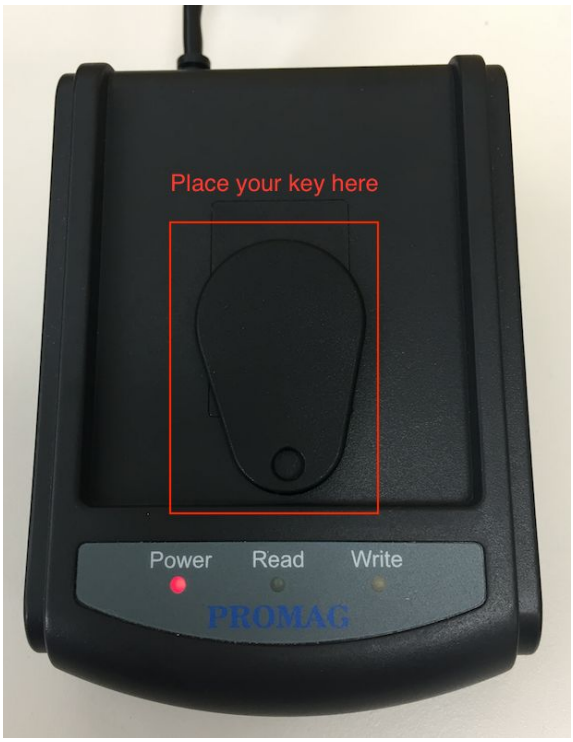


At the **Review & Issue Key** page we can verify the information of guest key including **Basic Information**, **Unit Area & time control information, Public Area & time control information**, **Group area & time control information**

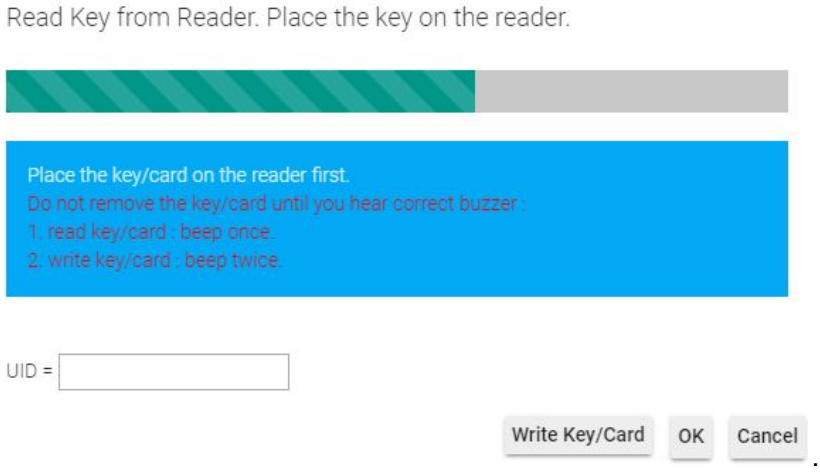


Click **Issue/Write Key** to issue **August** guest key.

Place key/card on reader first.

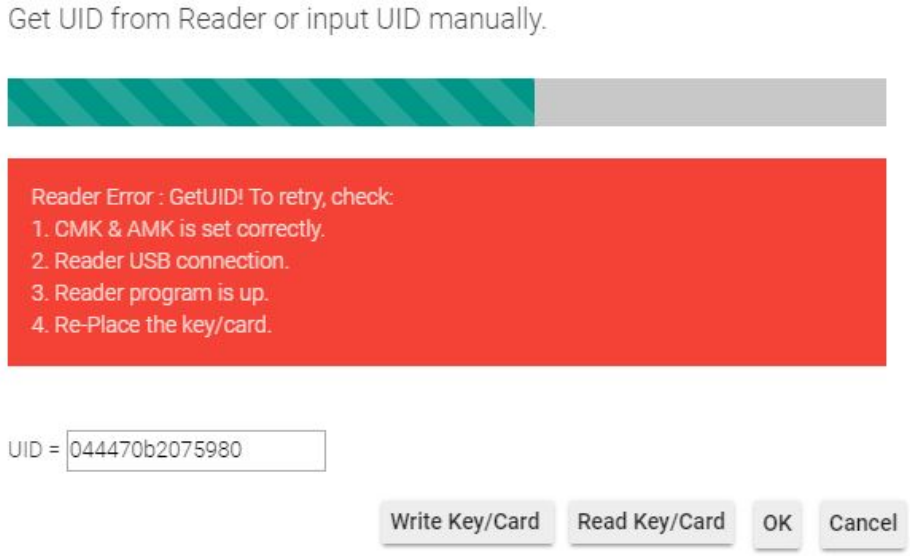


Click **Write Key/Card** to get Key's UID.



The **green light** LED on **Read** should blink.

If **Write Key/Card** failed with **three** beep sounds and display following message, please re-place key/card and click **Write Key/Card** again.
Write Key/Card successfully with **two** beep sounds.



Shutdown Public Area

The only public area we have in SIMPLE project is the swimming pool. Suppose you need to close the swimming pool in the winter or for maintenance purpose, it is not a good idea to re-issue all the cards to remove the swimming pool access right.

MF-Admin server has two features: Area Time Control and Lock Scheduling which will help you to complete this task in a second without re-issuing any cards.

- Area Time Control

  Area Time Control is another layer of time control which logically AND with the time control you set on the Mifare card during card creation for a specific area/lockplace.

  Area Time Control setting will take effect to all the residential cards (NOTE: exceptions exist if you change the access rule, we will discuss it later). Therefore, when you want to restrict the access of swimming pool to a certain time period of a day in a weekly manner, area time control is here for this task.

  Suppose your card has the access right of swimming pool for 24 hours everyday. And the area time control of swimming pool is only for Saturday and Sunday 24 hours. Then you are only able to access swimming pool on Saturday and Sunday.

  Note that this approach can not completely shut down the swimming pool because if you leave all the time control cells blank, it means NO time control. To complete shut down a public area, you better use Lock Scheduling feature.

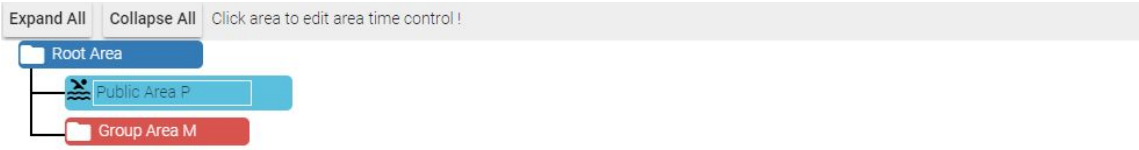
  To demonstrate how to set the area time control, follow below steps. (Note that you set time control for an area, not a lock.).

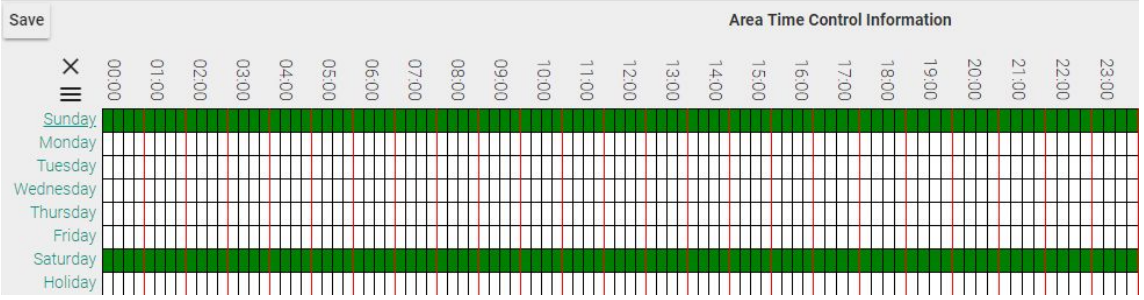
  Area time control allows to set the public

  ❖ Steps to set area time control for swimming pool

    Navigate to Area Time Control Setup page.
    Lock Management => **Area Time Control**

Assume the area time control of swimming pool is only for **Saturday and Sunday 24 hours**. Let's edit swimming pool time control to meet the requirement, click **Save** to save time control setting.





You can see the lock on **Public Area P** is blinking which means there is a time control setting over this area**.**

- Lock Scheduling

Lock scheduling has nothing to do with Mifare card. It can be used to control the schedule to lock/unlock a lock. In SIMPLE project case, we may use lock operation mode to control the locking status. Three modes are available for a lock (not an area):

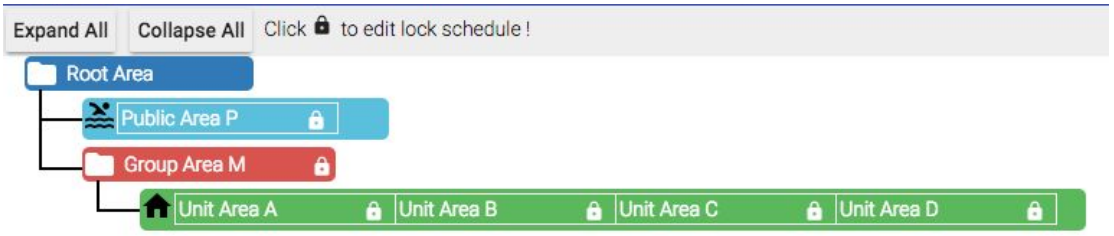
- ❖ Normal (default) : Scan card is needed.
- ❖ Passage : Keep the lock unlocked, scan card is not necessary.
- ❖ Private : It acts like normal mode. In combination with the NoPrivacy access rule, only Staff Card (and Master Card of course) can access the private area. But you may change the access rule to block all cards except Master Card.

Therefore, set the operation mode to Private will block all non-staff cards now.

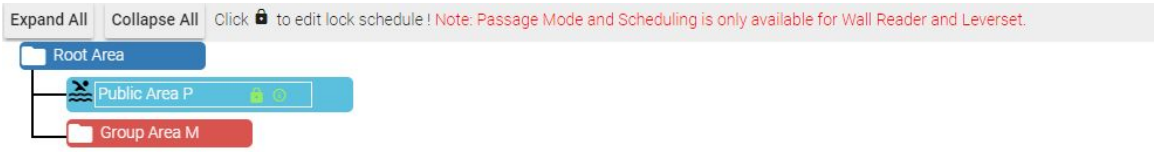
- ❖ Steps to set operation mode

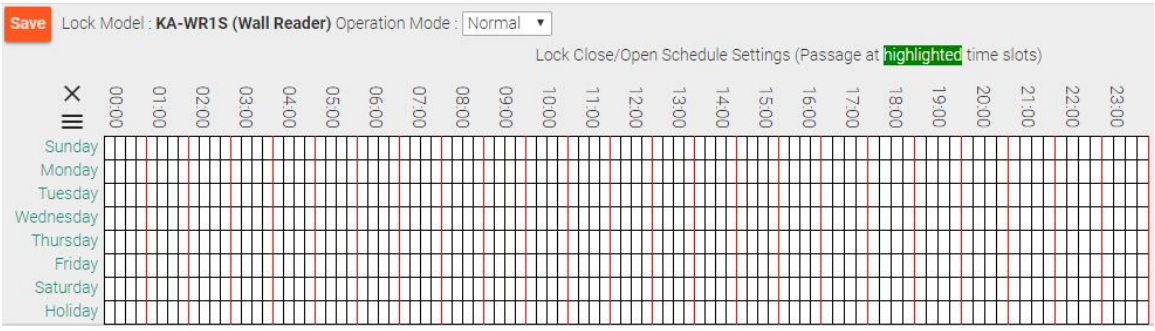
  Navigate to lock operation page. **Lock Management** => **Lock Scheduling**

Lock Management
Lock Info
Area Time Control
Lock Scheduling
Lock Operation

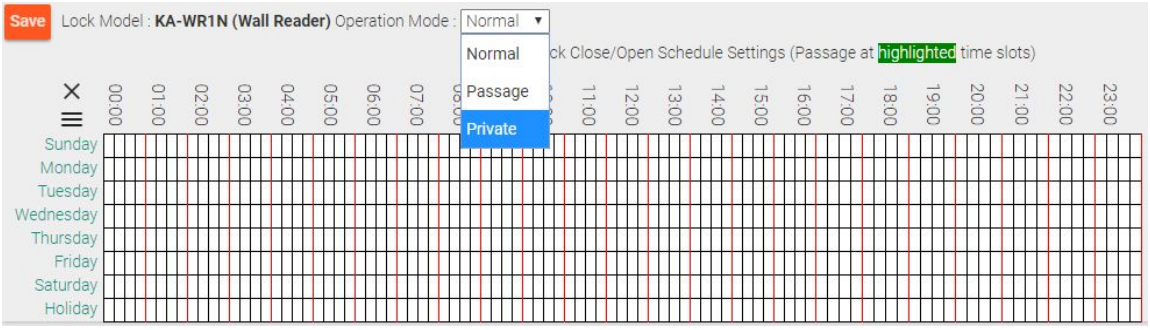

Expand All
Collapse All
Click to edit lock schedule !
Root Area
Public Area P
Group Area M
Unit Area A
Unit Area B
Unit Area C
Unit Area D

Click the lock icon in **Public Area P**.





In **Operation Mode** dialog, select **Private** and click **Save**.



The **Public Area P** lock icon color will turn to light green which means it is not normal setting**.**

As you can see in the previous screenshots, there is also a time control table which you can set when operation mode is in normal mode. It is used to manage a public/group area where you like it to be passage mode for some period of time of a

day in a weekly manner. We will not demo it here. Please see *MF-Admin Server User Manual* for detail.

Access Control Rule

It is time to elaborate how access rules works. All the locks will apply the access rule when scan a card. Below is the default access rule settings :

	Tenent	Guest	Temp	Staff	Vendor
Public	Lock+Key	Lock+Key	Lock+Key	Lock+Key	Lock+Key
Unit	Lock+Key	Lock+Key	Lock+Key	Lock+Key	Lock+Key
Group	Lock+Key	Lock+Key	Lock+Key	Lock+Key	Lock+Key
NoPrivacy	No	No	No	Yes	No

You have to choose one of the three settings to apply to a combination of card types and area types. The three choices are :

- Lock+Key : Area time control will be taken into consideration together with the settings on the card/key to decide whether lock can be unlocked or not.
- Lock only : The system only takes area time control into consideration and ignore the card/key settings.
- Key only : The system will take card/key setting into consideration and ignore the area time control.

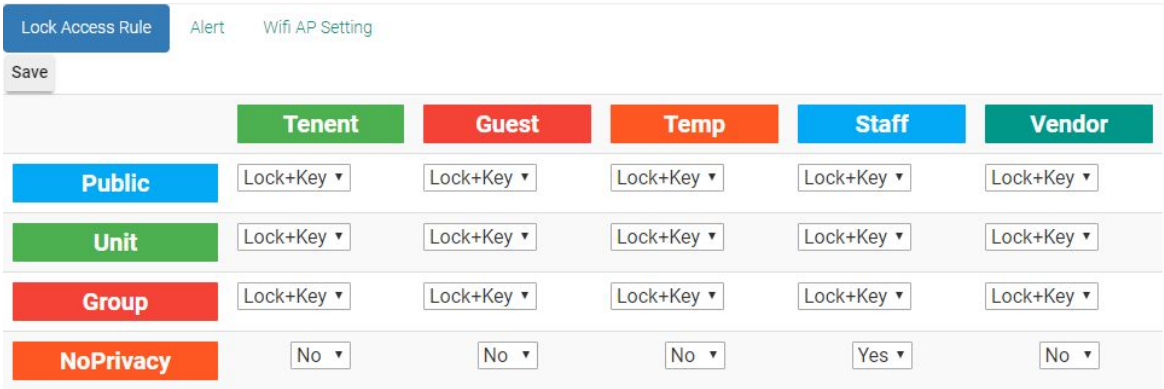
The NoPrivacy rule is a special rule for privacy locks (the mode you set at lock scheduling features). The card type with NoPrivacy set to yes will ignore the private mode which means the card is allowed to unlock the lock.

Therefore, if you like to block all users including the staff to enter swimming pool in SIMPLE project, You have to do two things : 1. At lock scheduling function, set lockplace P to private mode. 2. At lock access rule of system parameters function, set Staff's NoPrivacy to No.

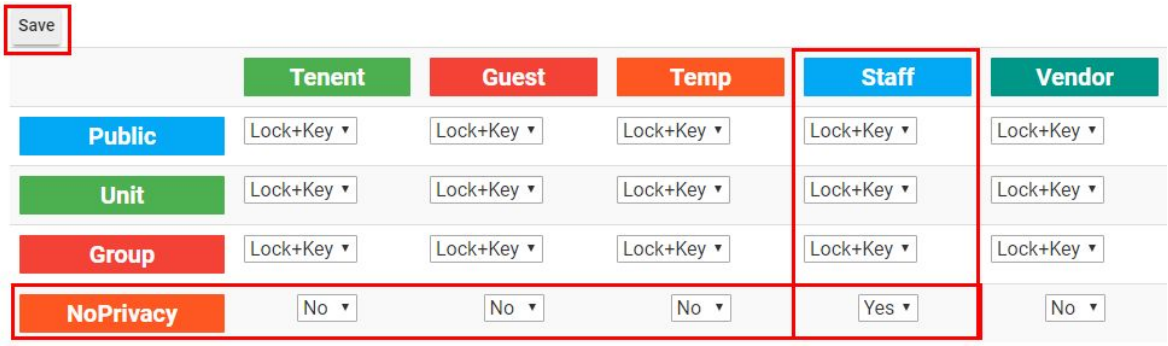
- Steps to shut down swimming pool completely except Master Key

  Previously we set swimming pool's lock operation to **Private** mode, so let's try to edit **Access Rule Control** now. Navigate to edit page first.

System Management => System Parameters



According to the document, we would want to block all users including the **staff** to enter swimming pool in private mode. Find out the **Staff** field and edit **NoPrivacy** to **No** and click **Save**.



Now, the swimming pool has been shut down completely except Master Key.

Time Control - Add/Remove Holidays

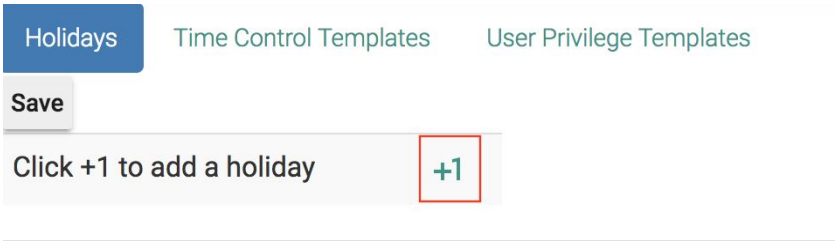
Time control settings can be found in many places in the system and it is straightforward to use. There is only one thing to remind, the holiday.
In addition to the settings for 7 days a week, you have another row (the bottom row) to set time control which is the holiday setting. For system to recognize which days are holiday, you have use the application parameters function to add/remove holidays.

- Steps to add/remove holiday

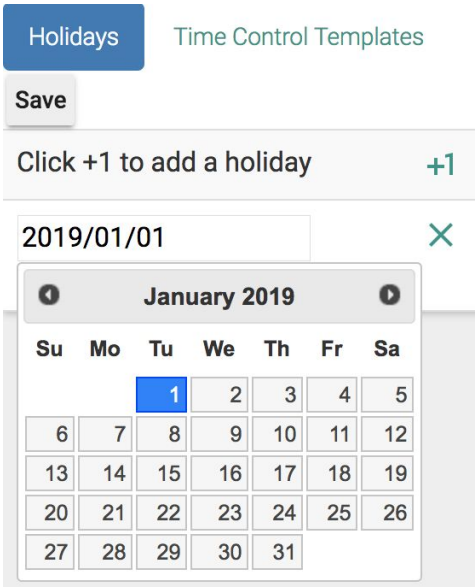
  - ❖ Add holiday

    Navigate to Holidays tab in Application Parameters page.
    System Management => **Application Parameters**

    Click **+1** to add a holiday.



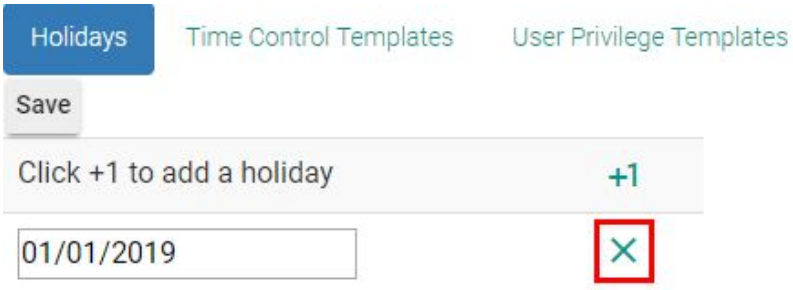
    Click the blank field to edit holiday assume that **2019/01/01** is a holiday.



Click Save to save the holiday.

❖ Remove holiday

Click **X** to remove holiday and click **Save**.



The holiday setting takes precedence over weekly settings. It means if today is a holiday and Monday, then the system will check holiday's settings instead of Monday's settings.

Advanced Setup Guide

Note : Do not try this section without assistance from reseller or Pamex. Changing any of the parameters in this section to unreasonable value might lead to unexpected system behavior.

Lock Report Interval

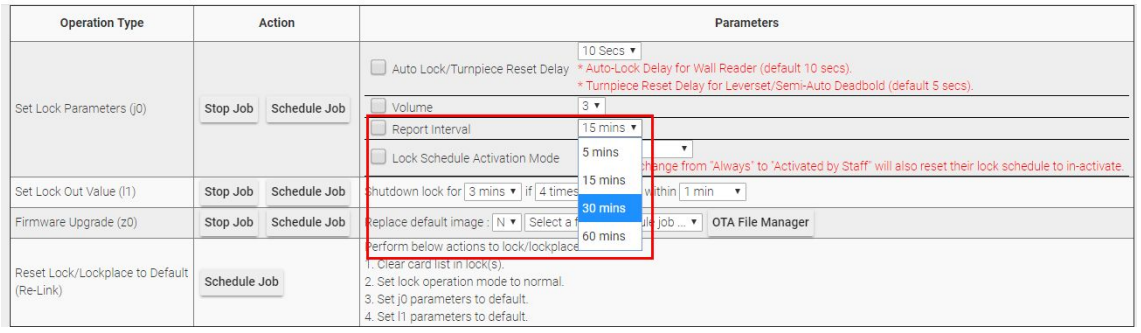
Lock report interval can be changed at the Lock Operation function.
The default value of this parameter is 300 secs (5 mins) for Wall reader and 900 secs (15 mins) for deadbolt and leverset.

❖ Steps to change the report interval setting for Lock P

Navigate to **lock operation** page to change the report interval.
Lock Management => Lock Operation

Operation Type	Action	Parameters
Set Lock Parameters (j0)	Stop Job / Schedule Job	Auto Lock/Turnpiece Reset Delay: 10 Secs * Auto-Lock Delay for Wall Reader (default 10 secs). * Turnpiece Reset Delay for Leverset/Semi-Auto Deadbold (default 5 secs). Volume: 3 Report Interval: 15 mins Lock Schedule Activation Mode: Always * Note that change from "Always" to "Activated by Staff" will also reset their lock schedule to in-activate.
Set Lock Out Value (l1)	Stop Job / Schedule Job	Shutdown lock for 3 mins if 4 times fail tries within 1 min
Firmware Upgrade (z0)	Stop Job / Schedule Job	Replace default image : N / Select a file to schedule job ... / OTA File Manager
Reset Lock/Lockplace to Default (Re-Link)	Schedule Job	Perform below actions to lock/lockplace : 1. Clear card list in lock(s). 2. Set lock operation mode to normal. 3. Set j0 parameters to default. 4. Set l1 parameters to default.

Click lock icon to select lockplace **Public Area P (**multiple selections is allowed**)**, at **Set Lock Parameters (j0)** field find out **Report Interval** parameters and set up it to **30 mins**.



Click **Schedule Job** to change the report interval setting.

To save the battery's life, Pamex Enkore smart lock is not always connected to MF-Admin Server. The locks will connect to the MF-Admin Server as the report interval.

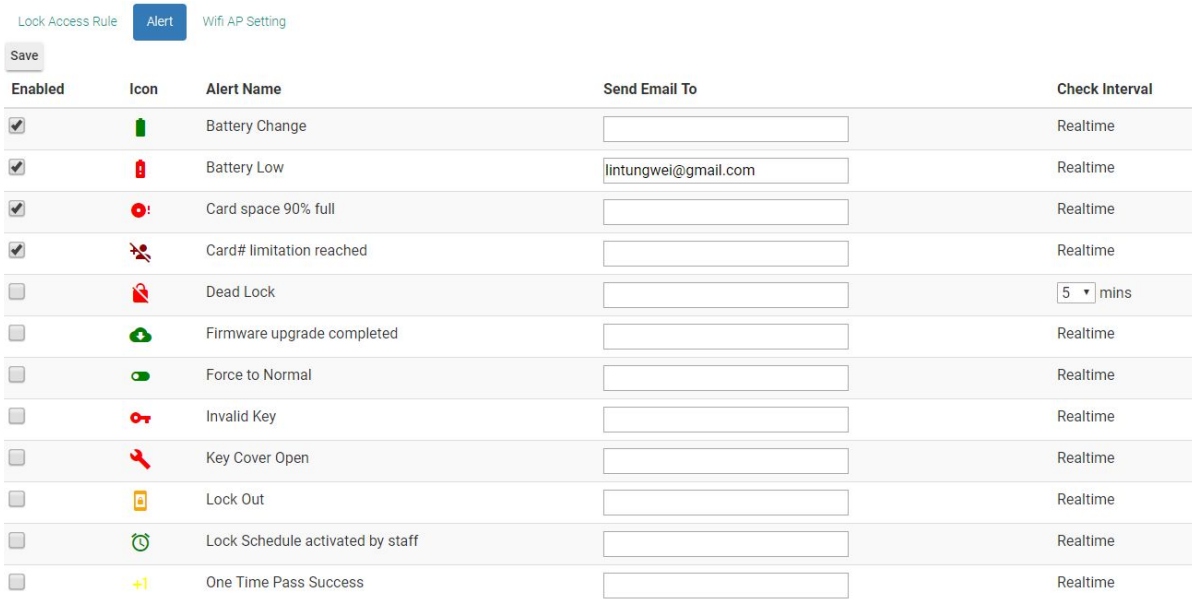
Also, this indicate one thing:every change to the card or lock will sync to locks in the given default secs at most if the report interval remains in default. For example, when you issue a card at 9:00 am, the card number will be downloaded to the related physical lock(s), Wall Reader, at next reporting time which could be anytime before 9:05 am depending on the last report time.

There is another way to force a lock to communicate with MF-Admin server immediately. Real time events(See Appendix Lock Real Time Events) can make a lock to communicate with the MF-Admin server. Therefore, when you want to make sure the lock to sync cards or execute lock operation commands immediately without waiting for a period, just prepare an invalid Mifare card (You may issue an invalid card easily by assigning no area to it) and tap to a lock to serve this purpose.

Alert Settings

When you login the MF-Admin Server, there are two icons showing the total number of new alerts at the navigation bar :

In the Alert tab of the system parameters, you can see there are twelve types of alert that will be generated in the system:



Enabled	Icon	Alert Name	Send Email To	Check Interval
☑		Battery Change		Realtime
☑		Battery Low	lintungwei@gmail.com	Realtime
☑		Card space 90% full		Realtime
☑		Card# limitation reached		Realtime
☐		Dead Lock		5 mins
☐		Firmware upgrade completed		Realtime
☐		Force to Normal		Realtime
☐		Invalid Key		Realtime
☐		Key Cover Open		Realtime
☐		Lock Out		Realtime
☐		Lock Schedule activated by staff		Realtime
☐		One Time Pass Success		Realtime

There is no alert enabled by default. You may check the checkbox to enable the alerts you need.

You may enter valid email addresses in the “Send Email To” field to enable email notification for an alert. Multiple addresses can be entered delimited by semicolon.

The check intervals are all realtime and can not be modified except the “Dead Lock” alert. Dead Lock alert checking interval can be set larger than the default(5 mins). This value is related to the lock report interval. It is unreasonable to set a dead lock checking interval smaller than the lock report interval. Note that the unit of this value is minute.

For every alert types, there is a severity value config in the MF-Admin Server appConfig.json file. For the default severity setting, please see default severity of alert types in Appendix. The alerts has lower severity category (Yellow alerts on the navigation bar) and higher severity category (Red alerts on the navigation bar).

Appendix

Lock UI Patterns (LED & Buzzer)

Leverset & Deadbolt

第一次換電池 (Recovery Card後)	Beep一聲紅燈亮, 馬達校正, 紅綠交替一次,, 完成後鎖舌伸出, Beep 一聲紅燈閃
非第一次換電池	**紅燈亮, beep一聲, 紅綠交替兩次, beep一聲, 不作馬達校正. 鎖舌不動.**
Crypto Card	**綠燈亮, 長beep**
刷卡開門	**Beep一聲, 綠燈亮, 鎖舌收**
刷卡鎖門	**Beep一聲, 紅燈亮, 鎖舌出**
非法卡	**紅燈閃三次, Beep三聲** 紅燈間隔一秒閃一次, 持續一分鐘(預設) - <Lock Out>
Construction Card	(同開關門)
Programming Card	綠燈閃兩次 beep 兩聲. 紅燈持續閃 (Wifi連線) 直到連線成功後, 綠燈閃+beep一長音 嘗試完所有AP後若不成功即放棄連線
Recovery Card	綠燈閃三次, Beep三聲 => 綠燈亮, Beep 一長聲 重新開機
韌體更新	**紅燈閃五次, beep五聲** **綠燈閃五次 (下載完畢), beep五聲** **If 下載失拜紅燈閃三次, beep三聲** **Else 等候重新開機完畢**
重新開機完畢	綠燈亮兩秒, beep一聲兩秒
產測程式 (刷Crypto 前以任意卡啟動)	**紅燈閃, 綠燈閃**, beep一聲 馬達轉動 **<Unlock> + <Lock>** 紅燈持續閃 (Wifi連線) 直到連線成功後, 綠燈閃+beep一長音 預設AP若連線不成功30秒後放棄連線
Lock Out 閉鎖	紅燈亮三分鐘(預設)
鎖匙蓋開啟	紅燈閃10次, Beep 10聲
刷卡開門誤動作	鎖舌無法伸出時, 馬達持續轉動, 紅燈閃三次 beep三聲 30秒後放棄嘗試. 之後刷卡可正常開門
刷卡鎖門誤動作	鎖舌無法收入時, 馬達持續轉動, 紅燈閃三次 beep三聲 30秒後放棄嘗試

	之後刷卡可正常鎖門
弱電處理	鎖在每次運作後, 餘600次開關電力時 : 紅燈每10秒閃一次, 持續1分鐘 餘400次開關電力時 : 紅燈每5秒閃一次, 持續1分鐘 餘200次開關電力時 : 紅燈每2秒閃一次, 持續1分鐘
斷電處理	餘待機電力3個月, 可支援一次刷卡開門電力

Leverset & Deadbolt

Change the battery (the first time after tapping a recovery card)	a beep with a red blink + motor adjustment + a red blink + a green blink(finished with a latch appear) + a beep with a red blink
Change the battery	A red blink with a beep + a red blink + a green blink + a red blink + a green blink + a beep (No motor adjustment, latch has no motion.)
Crypto Card	A green blink with a long beep.
Tap to lock	a beep with a green blink + the lock tongue in
Tap to unlock	a beep with a red blink + the lock tongue out
Invalid card	3 red blinks + 3 beeps Red blinks between seconds lasting a minute as a default.(Lock Out)
Construction Card	(same as lock/unlock)
Programming Card	2 green blinks with 2 beeps. Red blinks continuously till a success connect with AP along with a green blink + a long beep. *Note that only when tried every nearby APs will the lock stop connecting.*
Recovery Card	3 green blinks with 3 beeps + a green blink with a long beep > + reboot
Firmware upgrade	5 red blinks with 5 beeps + (5 green blinks with 5 beeps)* + reboot *Download success. If download failed will tell 3 red blinks with 3 beeps)
Reboot	green blink with a long beep for 2 secs.
Test program (Execute by taping any card before tapping a Crypto	A red blink + a green blink + a beep + motor adjustment + red blinks continuously till a success connect with AP along with a green blink and a long beep. *Note that it will last 30 secs as a default for keeping trying to*

card)	*connect with the APs.*
Lock Out	Red blinks for 3 mins as a default
Key cover open	10 red blinks + 10 beeps
Malfunction when tapping to unlock	the latch jammed, the motor rotate continuously with 3 red blinks + 3 beeps, failed to try after 30 secs, be able to open the door by tapping the card.
Malfunction when tapping to lock	the latch jammed, the motor rotate continuously with 3 red blinks + 3 beeps, failed to try after 30 secs, be able to lock the door by tapping the card.
Battery low	Red light and beep in every 10 secs lasting for one minute. 餘600次開關電力時 : 紅燈每10秒閃一次, 持續1分鐘 餘200次開關電力時 : 紅燈每2秒閃一次, 持續1分鐘
Power Cut	Allowed to tap the card once when the power is subject to 3 months left.

Wall Reader

Crypto Card	**綠燈亮, 長beep**
刷卡開門	**Beep一聲, 綠燈亮**
刷卡鎖門	**Beep一聲, 紅燈亮**
非法卡	**紅燈閃三次, Beep三聲** 紅燈間隔一秒閃一次, 持續一分鐘(預設) - <Lock Out>
Construction Card	(同開關門)
Programming Card	綠燈閃兩次 beep 兩聲. 紅燈持續閃 (Wifi連線) 直到連線成功後, 綠燈閃+beep一長音 嘗試完所有AP後若不成功即放棄連線
Recovery Card	綠燈閃三次, Beep三聲 => 綠燈亮, Beep 一長聲 重新開機
韌體更新	**紅燈閃五次, beep五聲** **綠燈閃五次 (下載完畢), beep五聲** **If 下載失拜紅燈閃三次, beep三聲** **Else 等候重新開機完畢**
重新開機完畢	綠燈亮兩秒, beep一聲兩秒
產測程式 (刷Crypto前以任意卡啟動)	**紅燈閃, 綠燈閃**, beep一聲 紅燈持續閃 (Wifi連線) 直到連線成功後, 綠燈閃+beep一長音 預設AP若連線不成功30秒後放棄連線

Lock Out 閉鎖	紅燈亮三分鐘(預設)

Wall Reader

Crypto card	a green blink with a long beep.
Tap to lock	a green blink with a beep.
Tap to unlock	a red blink with a beep.
Invalid card	3 red blinks with 3 beeps Red blinks between seconds lasting 1 minute as a default.(Lock Out)
Construction Card	(same as lock/unlock)
Programming Card	2 green blinks with 2 beeps. Red blinks continuously till a success connect with AP along with a green blink + a long beep. *Note that only when tried every nearby APs will the lock stop connecting.*
Recovery Card	3 green blinks with 3 beeps + a green blink with a long beep + reboot
Firmware upgrade	5 red blinks with 5 beeps + (5 green blinks with 5 beeps)* + reboot *Download success. If download failed will tell 3 red blinks with 3 beeps)
Reboot	green blink with a long beep for 2 secs.
Test program (Execute by taping any card before tapping a Crypto card)	A red blink + a green blink + a beep, red blinks continuously till a success connect with AP along with a green blink and a long beep. *Note that it will last 30 secs as a default for keeping trying to connect with the APs.*
Lock Out	Red blinks for 3 mins as a default

Wifi AP Specification and Settings

Wifi network is necessary for Pamex Enkore solution. The network setup is out of the scope of this manual. Please make sure your network is well configured with your system vendors.

Pamex Enkore locks support most of the popular wifi APs in the market. Please make sure your Wifi AP has the features listed below :

- Support 802.11 bgn, 2.4 G
- WAP2 encryption

Factory default settings - Wall Reader

- Model No:KA-WR1S/KA-WR1N
- Operation Mode:Normal
- Lock Parameters
    a. Volume:3 (high)
    b. Enabled Locking Mode:Auto lock
    c. Auto Lock Delay:10 secs
    d. Report Interval:300 secs
- Lockout Settings
    a. Time to count fail(secs):60
    b. Fail Try(times):3
    c. Time to Shutdown(secs):180

Factory default settings - Deadbolt

- Model No:
    a. D1:KA-D7P1S
    b. D2:KA-D7P1A
- Operation Mode:Normal
- Lock Parameters
    a. Volume:3 (high)
    b. Enabled Locking Mode:
        - D1:Auto reset turnpiece
        - D2:Scan lock
    c. Auto Lock/Reset Turnpiece Delay (secs)
        - D1:5
        - D2:N/A
    d. Report Interval:900 secs
- Lockout Settings
    a. Time to count fail(secs):60
    b. Fail Try(times):4
    c. Time to Shutdown(secs):180

Factory default settings - Leverset

- Model No:KA-LNP5C
- Operation Mode:Normal
- Lock Parameters
    a. Volume:3 (high)
    b. Enabled Locking Mode:Auto lock
    c. Auto Reset Turnpiece Delay(secs):5
    d. Report Interval:900 secs
- Lockout Settings
    a. Time to count fail(secs):60
    b. Fail Try(times):4
    c. Time to Shutdown(secs):180

Factory default settings - Interconnect

- Model No:
    a. I1:KA-INP35S
    b. I2:KA-INP35A
- Operation Mode:Normal
- Lock Parameters
    a. Volume:3 (high)
    b. Enabled Locking Mode:
        - I1:Auto reset turnpiece
        - I2:Scan lock
    c. Auto Lock/Reset Turnpiece Delay (secs)
        - I1:5
        - I2:N/A
    d. Report Interval:900 secs
- Lockout Settings
    a. Time to count fail(secs):60
    b. Fail Try(times):4
    c. Time to Shutdown(secs):180

MF-Admin Server Parameters default settings

Application Parameters

Please see *MF-Admin Server User Manual.*

System Parameters

Please see MF-Admin Server User Manual.

Mifare Card Specification

You may purchase Mifare Card or Key fob from 3rd party. **MIFARE**® is the NXP Semiconductors-owned trademark of a series of chips widely used in contactless smart cards and proximity cards. The MIFARE® brand name covers proprietary solutions based upon various levels of the ISO/IEC 14443 Type A 13.56 MHz contactless smart card standard. It incorporates AES and DES/Triple-DES encryption standards, as well as an older proprietary encryption algorithm.

Pamex Enkore supports only MIFARE DESFire EV1/EV2 compatible cards/key fobs.

Card Types

Pamex Enkore defines below card types :

	Card Type
1	Crypto Card (CRC)
2	Construction Card (COC)
3	Programming/Registration Card (PRC)
4	Residential Card (RSC) – sub-typed into five different residential card : Tenant card, Staff card, Vendor card, Guest card, and Temp card depending how you issue the card using MF-Admin server
5	Master Card (MAC)

Crypto Card :

To recognize any other types of card, a lock has to read Crypto card. Crypto card is not issued from MF-Admin server. It should be provided by Pamex and is unique to your project.

Construction Card :

Before the wifi network is ready, the only way to unlock the door locks will be using the construction cards. Construction cards can not be issued from MF-Admin Server. It should be provided by Pamex and is unique to your project.

Programming Card :

Once your wifi network is ready and MF-Admin server is installed, programming card can be used to register lock to the MF-Admin Server. Programming card can be created/issued using MF-Admin Server. In a large project, you may create several programming cards to speed up the registration process.

Residential Card :

There are five types of residential card : Tenant, Staff, Vendor, Guest and Temp. Residential cards are issued using MF-Admin Server by property owner or administrator when project goes live.

Master Card :

Master Card is an unrestricted access card to any door locks in the project. It is created using MF-Admin server. Master Card is only valid to the locks which has registered to MF-Admin server.

Area Types

There are three types of area you may create in MF-Admin Server :

Group Area :
Group area is like a folder. It is used to group together the units and public areas in the same floor/building for example.

Unit Area :
An unit area represents an unit for one family.

Public Area :
A public area represents a shared facility like swimming pool.

These areas will be organized into a single root area tree to represent your property. All the areas can be programmed to grant access to residential cards by time control and area control in the MF-Admin Server.

Lock Real Time Events

1. Battery Change
2. Battery Low
3. Card space 90% full
4. Card# limitation reached
5. Firmware upgrade completed
6. Force to Normal
7. Invalid Key
8. Key Cover Open
9. Lock Out
10. Lock Schedule activated by staff
11. One Time Pass Success

Default Severity of Alert Types

No.	Alert Name	Severity
1	Battery Change	10
2	Battery Low	100
3	Card space 90% full	90
4	Card# limitation reached	100
5	Dead Lock	100
6	Firmware upgrade completed	20
7	Force to Normal	10
8	Invalid Key	80
9	Key Cover Open	100
10	Lock Out	50
11	Lock Schedule activated by staff	10
12	One Time Pass Success	10

FCC Statement

FCC Statement:
This device compile with part 15 of the FCC Rules.
Operation is subject to the following two conditions:
(1)This device may not cause harmful interference, and
(2)This device must accept any interference received, including interference that may cause undesire d operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.
This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
—Consult the dealer or an experienced radio/TV technician for help.
Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and a human body.

NCC Statement

NCC Statement:

Taiwan Regulatory Information(NCC)

低功率電波輻射性電機管理辦法

第十二條

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電通信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。