UBio Alpeta
USER GUIDE

UNION COMMUNITY

Table of contents

1. Access Group 5

1) Access Area 5

2) Access Group 6

3) Access Group User Management 7

4) Send Access Group Information to Terminal 8

2. Anti passback 9

1) Anti-Passback 9

2) Anti passback management 10

3. System Log 14

1) System log 14

2) Event log 14

4. Auth log 15

1) Export Auth Log 15

2) Auth Log Management 16

3) View Auth-log 17

5. Card Layout 18

1) Standard Card 18

2) FP Card 20

6. Task Manager 21

7. Elevator 22

1) Access Floor Management 22

8. Group 23

1) Manage the group 23

2) Select the user 24

3) Select the terminal 25

9. Integrated Report Management (AuthLog, TNA, Meal) 26

1) Integrated Report Management (PDF Save) 27

2) Integrated Report Management (PDF Setting) 28

10. License registration 29

11. LPR Management 33

12. Location visualization 35

1) Map management 35

2) Location positioning monitoring 37

3) Localization visualization 38

13. Meal Service 41

1) Meal Menu 41

2) Meal Service 42

3) Meal Statistics 44

14. Monitoring 47

1) Monitoring 47

2) Terminal Monitoring 48

3) Monitoring Authentication Image 49

15. Notice 51

16. Position - Staff 53

17. Privilege 54

18. Setting 56

1) Authentication 56

2) Emergency 58

3) General 59

4) Log 60

5) User 62

19. File Transfer 64

20. Terminal 65

1) Terminal Admin 65

2) Firmware 66

3) Terminal Log 67

4) Terminal management 68

5) Terminal Search 70

6) Terminal User Management 71

7) Terminal Info 73

21. Timezone 78

1) Holiday 78

2) Timeline Management 79

3) Timezone Management 81

22. TNA 83

1) TNA Payment 83

2) TNA Result 84

3) Work Type 85

4) Work Time 87

23. User 92

1) User Export 92

2) User Import 94

3) User 97

24. Wiegand 110

1) Wiegand Out 110

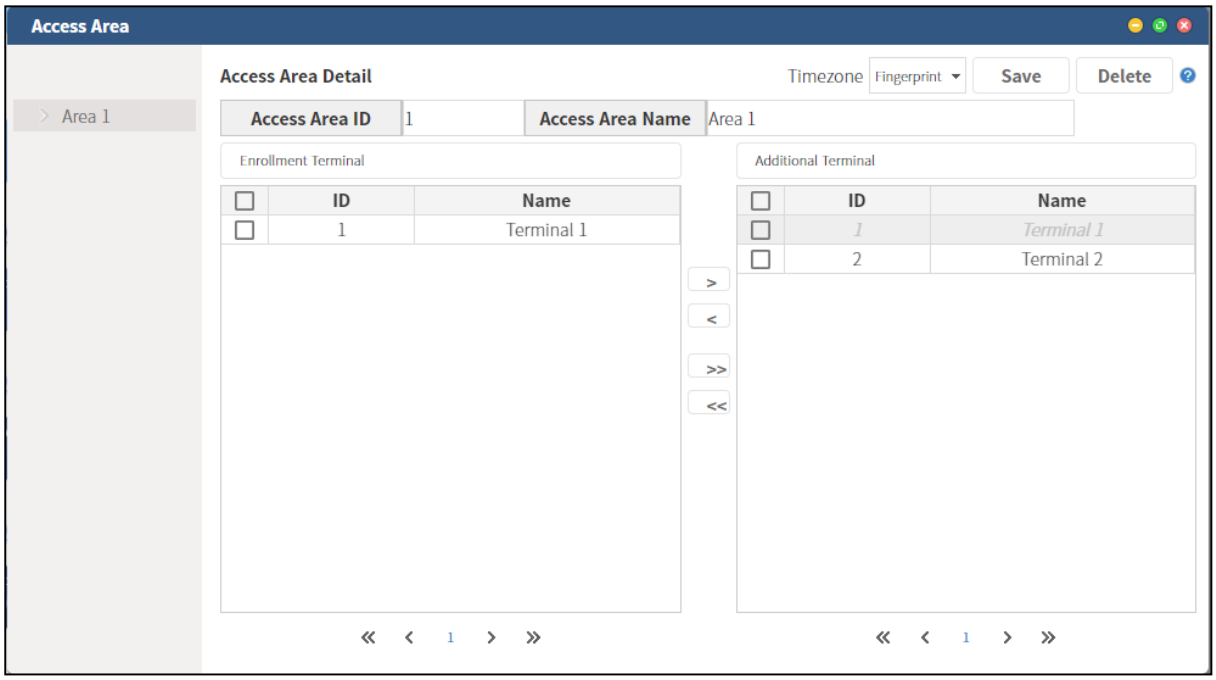
2) Wiegand In 112

1. Access Group

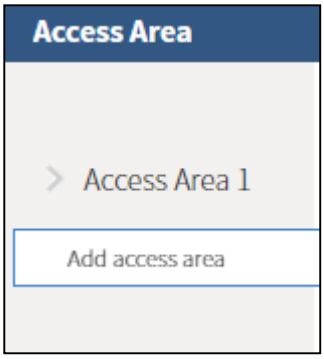
1) Access Area

It is the feature to manage the information of an access.

Specifically, it can set the access area to set in access group.



- **Access Area ID:** Enter a unique code.
- **Access Area Name:** Enter the name to use in access area.
- [**<**], [**<<**]: Move the terminal in 'Additional Terminal' to 'Enrollment Terminal'.
- [**>**], [**>>**]: Move the terminal in 'Enrollment Terminal' to 'Additional Terminal'.
- **Save**: Save the entered information.
- **Delete**: Delete the saved access group.
- **Add access area**: Add the new access area by right-clicking on the saved access area name or around the left side.

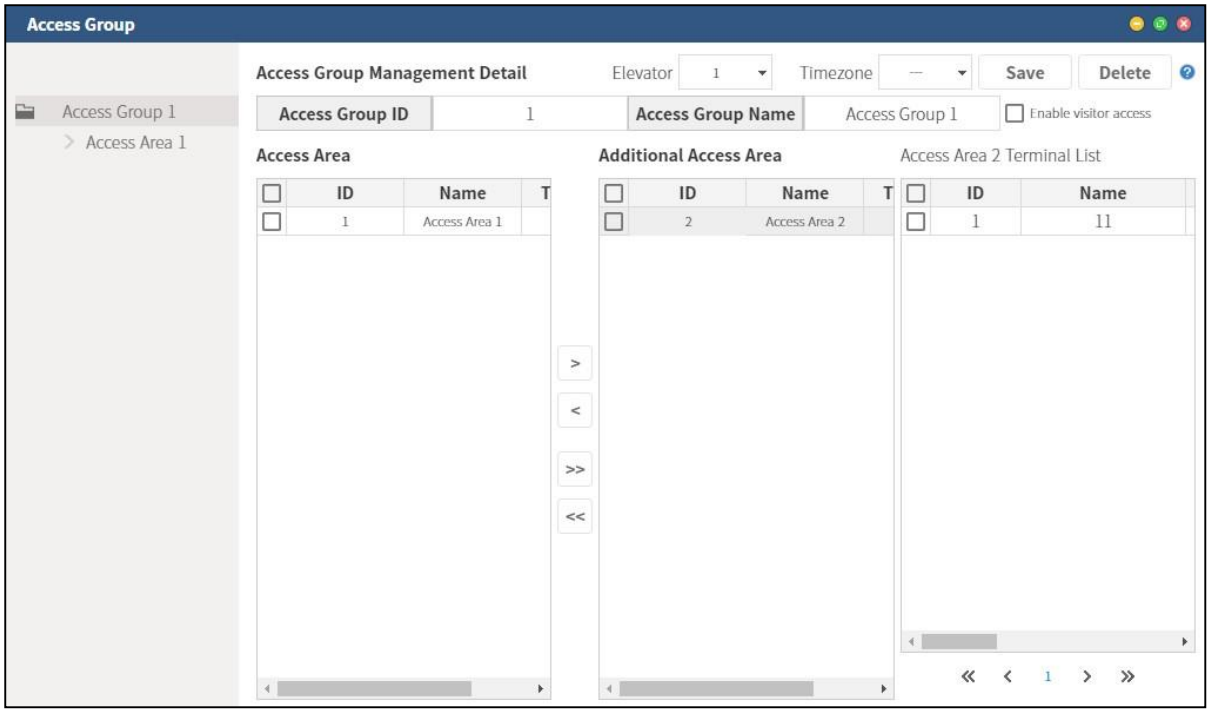


** The added and modified information of access group is used for the access group management.*

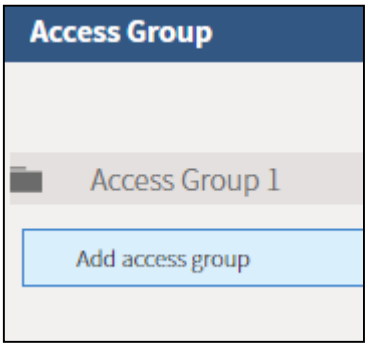
2) Access Group

It is the feature to manage the access group.

Specifically, it can set the access area to set in access group.



- **Access Group ID**: Enter a unique code.
- **Access Group Name**: Enter the access group.
- **Time zone**: Set the time zone to use in Access Group. Select the registered time zone in combo box and apply it. When clicking the time zone button, the screen for setting the time zone opens.
- [**<**], [**<<**]: Move the information in 'Additional Access Area' to 'Access Area'.
- [**>**], [**>>**]: Move the information in 'Access Area' to 'Additional Access Area'.
- **Save:** Save the setting information of the access group.
- **Delete**: Delete the selected access group in server.
- **Add access group:** Add the additional access group by right clicking on the saved access group name or around the left side.

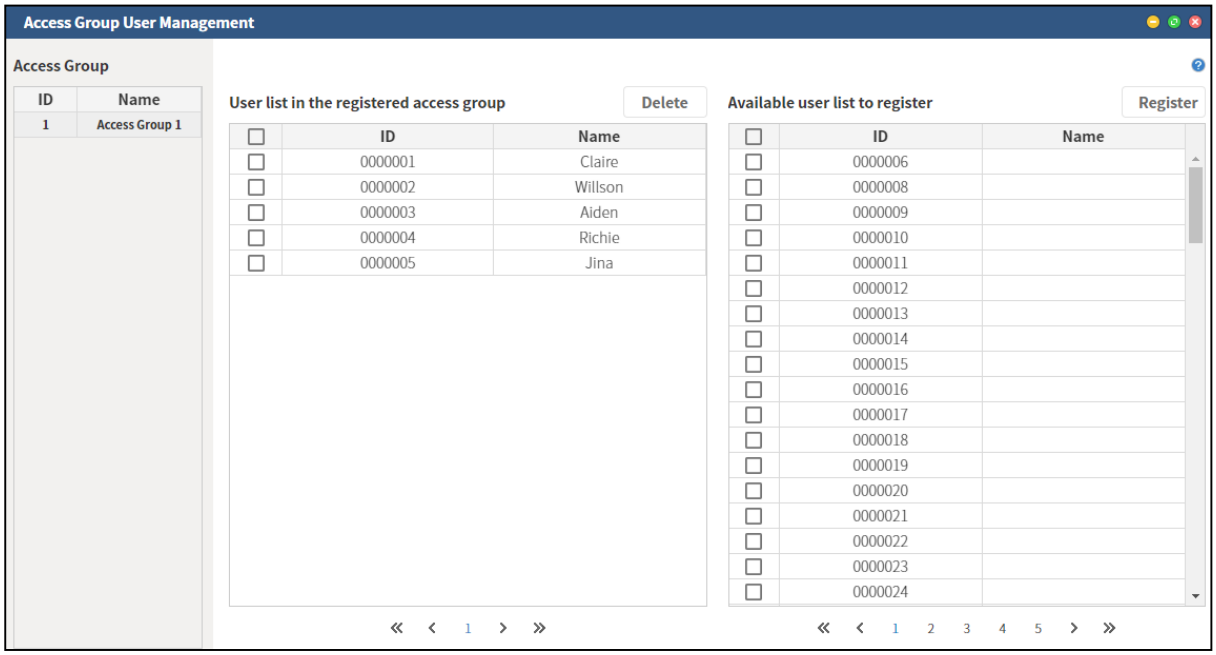


- **Elevator**: Set the access floor item added in the access floor management to the access group.
- **Enable visitor access**: When you check this option and save it, you can assign the visitors to the access group when approving the visitors

3) Access Group User Management

It is the screen to manage the user information of access group.

You can add the new user or delete the registered user in access group.

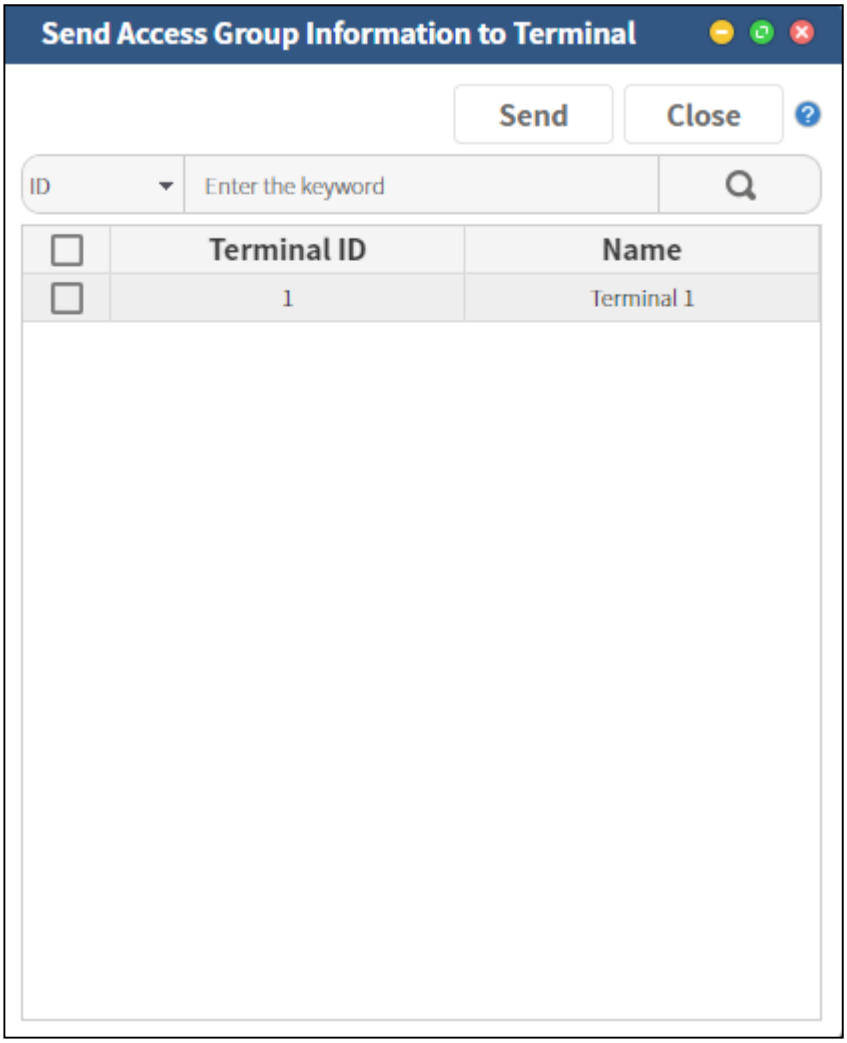


- **Access Group ID**: Show the access group list that is registered in server.
- **User list in the registered access group**: Show the user list included in access group.
- **Delete:** Check the user to delete in the registered access group user list and delete them in the access group.
- **Available user list to register:** It is the available user list to add in access group.
- **Register:** Check the user to register in '**Available user list to register**' and register the users in the access group.

4) Send Access Group Information to Terminal

It is the feature to send the registered access group information to terminal.

Specifically, it can send the access group information to the selected terminal.



- **Terminal ID**: Show the terminal ID available to send.
- **Name:** Show the name of terminal.
- **Send:** Send the access group information to the selected terminal.
- **Close:** Close this menu.

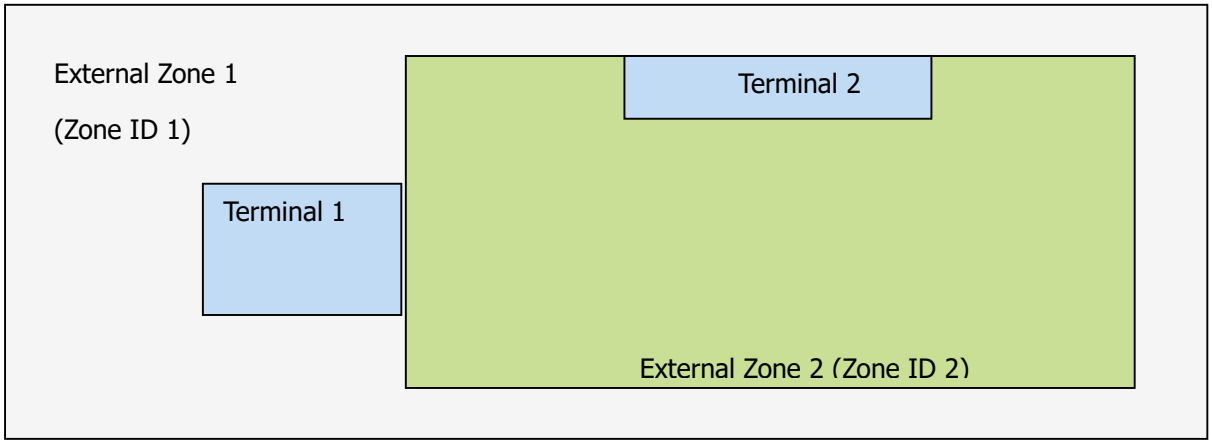
2. Anti passback

1) Anti-Passback

Anti-Passback (APB) is an access control system that prevents unauthorized access when entering to enhance security of an access area.

APB is managed by each area, and if you are authenticated at the entrance of the area, you must authenticate at the exit of that area to move to another area.

If you move to another area without authentication, an APB error will occur and you will be restricted from accessing that area.



In the figure above, Terminal 1 is the exit of the zone for the external zone (Zone 1) and zone entrance for zone 2 (zone 2)

Terminal 2 is the exit of the zone (Zone2) and zone entrance for external zone.

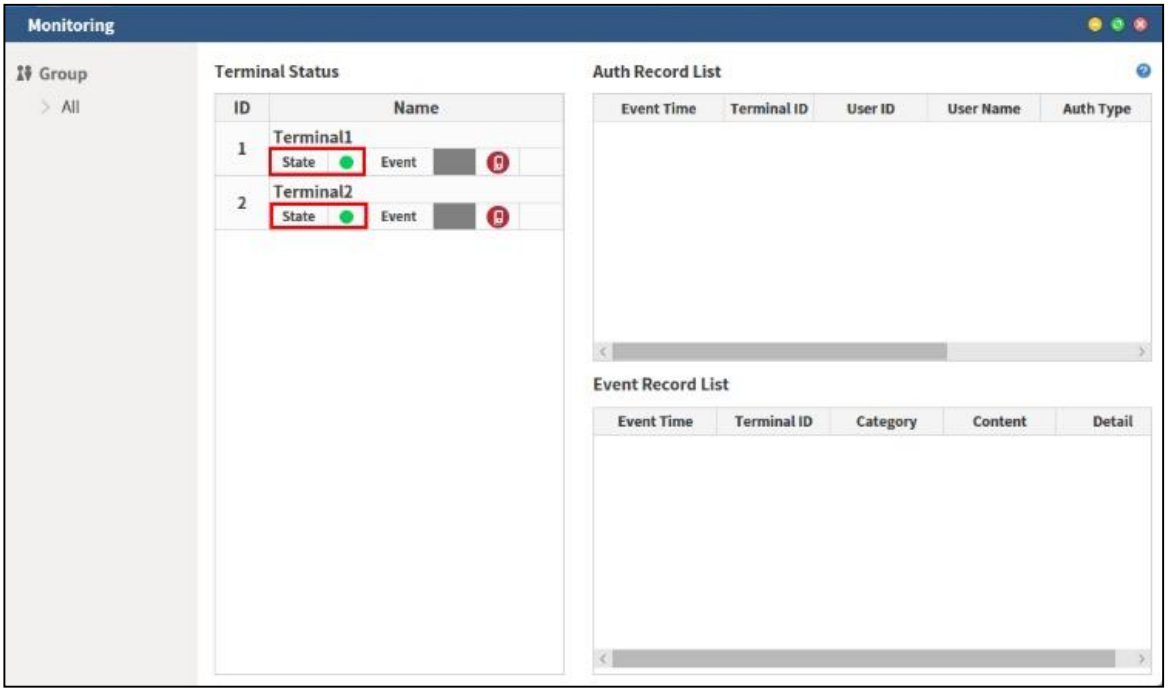
In order to apply APB, it is necessary to set zone exit and zone entrance for each terminal. If there is an entrance and exit terminal for the zone, at least one pair of terminals must exist.

It is the very simple explanation of the zone and you can set more terminals in various zones.

2) Anti passback management

It is the guide for how to use Anti-passback management.

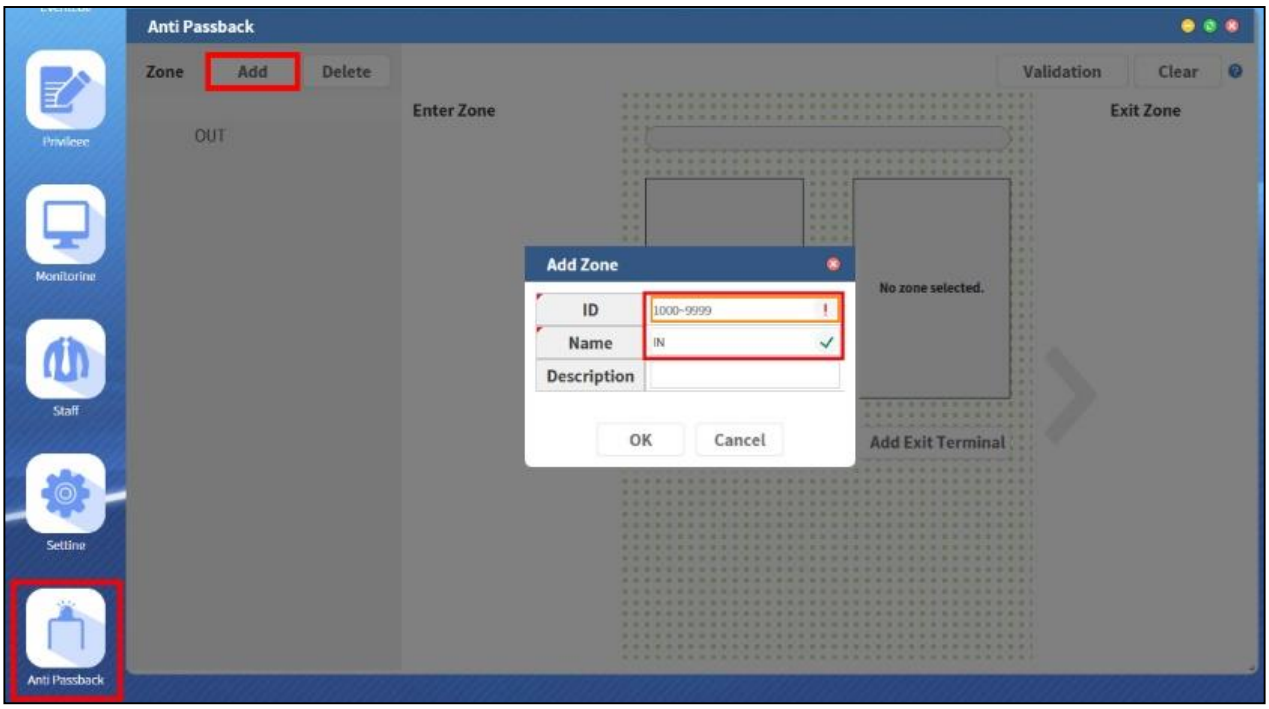
① Select [**Add**] to add the zone in the left side.



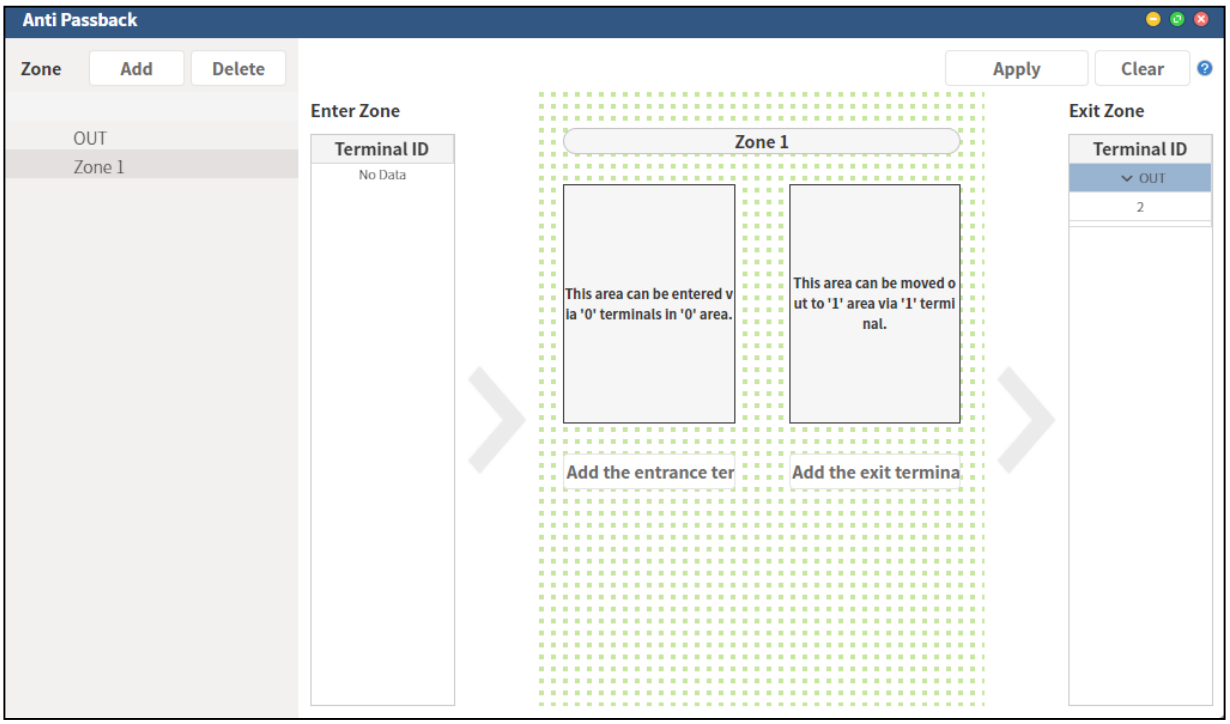
② Go to [**Terminal Info**] -> Select '**Access Allow**' or '**Access Denied**' when the network is disconnected.

※ Anti_Pass Back (=APB) can be operated based on normal Network (Server).

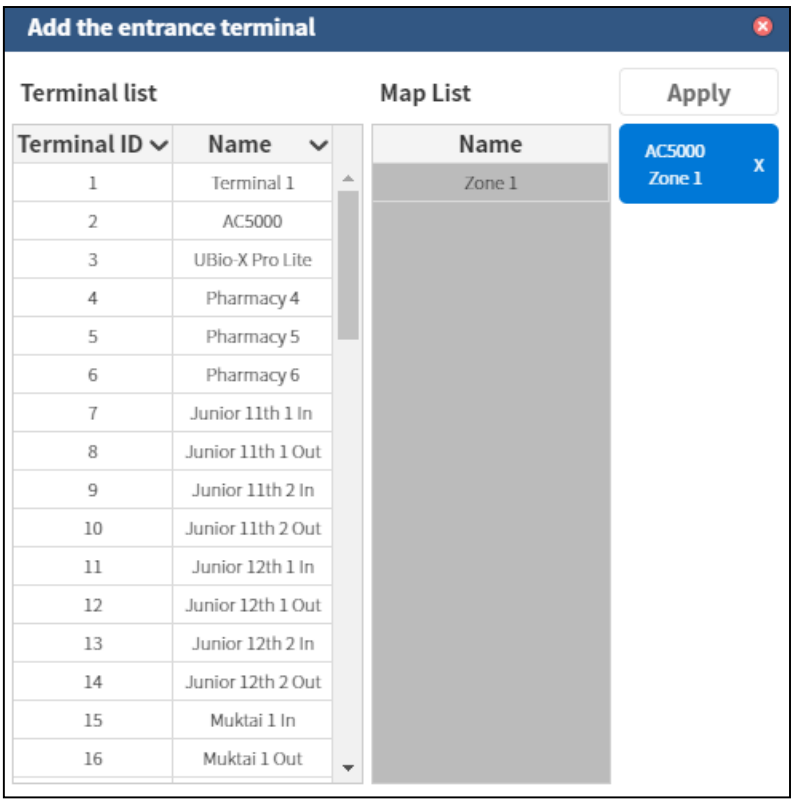
③ Go to '**Anti Passback**' and enter ID, Name and Description to add the zone.



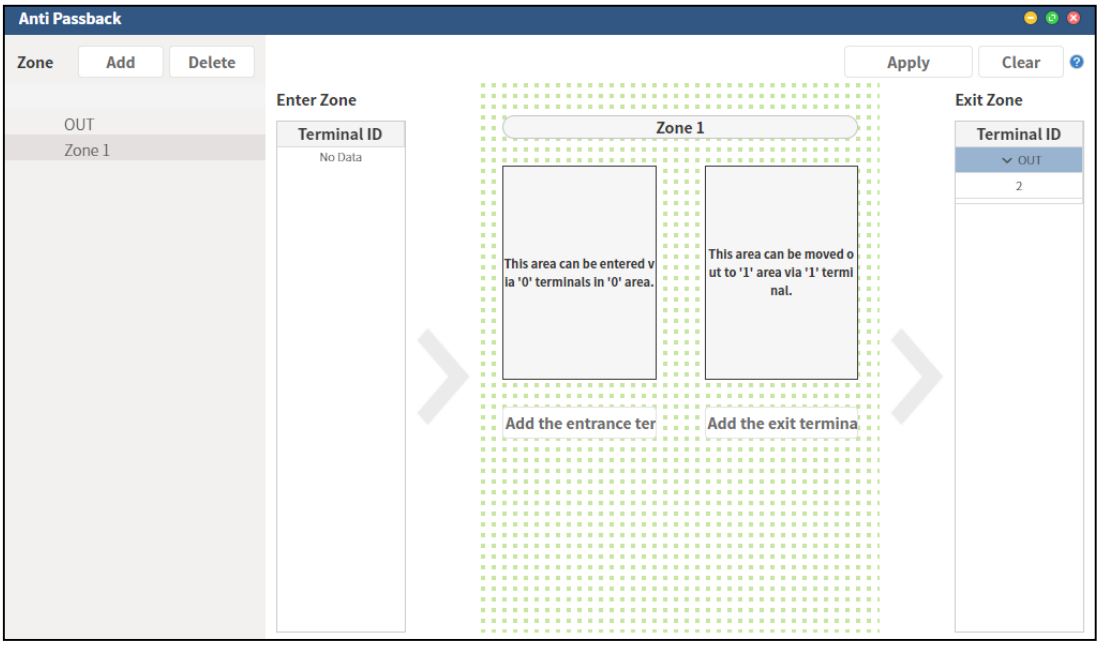
④ The zone you added is shown in the left side. Select [**Add the entrance terminal**] to add the terminal in the zone.



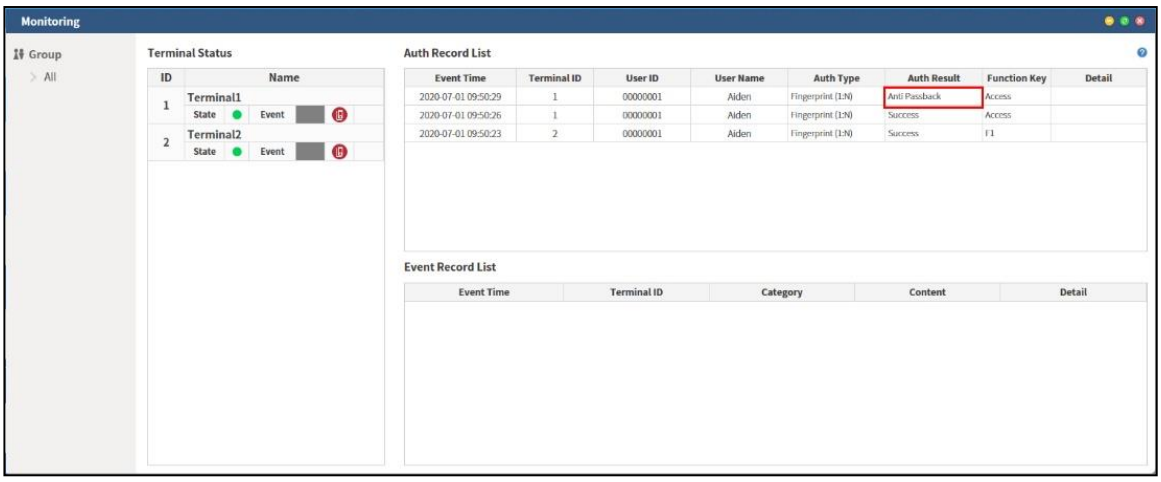
⑤ Click the terminal ID in the 'Terminal List' and Name in 'Map List' and then select [**Apply**].



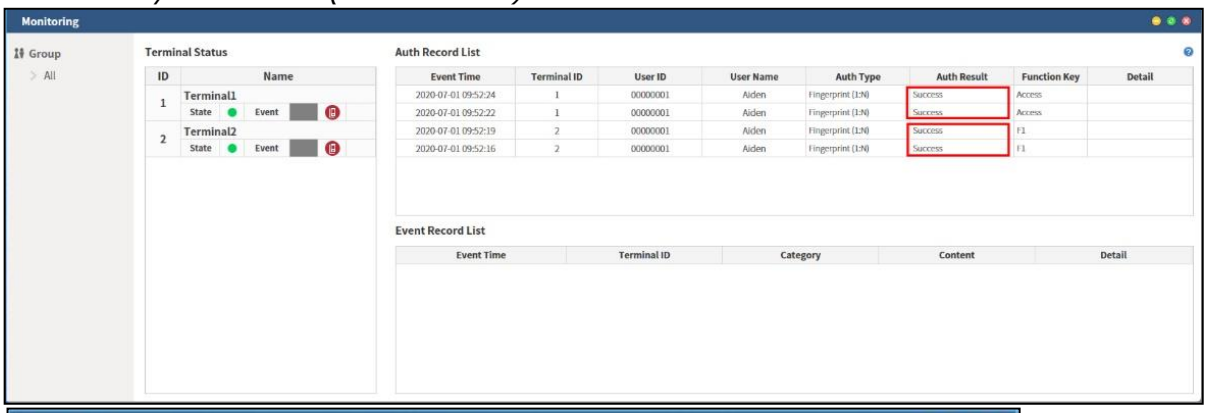
⑥ You can see the applied terminal and apply the same setting by selecting [**Add the exit terminal**]. After setting, select [**Apply**].

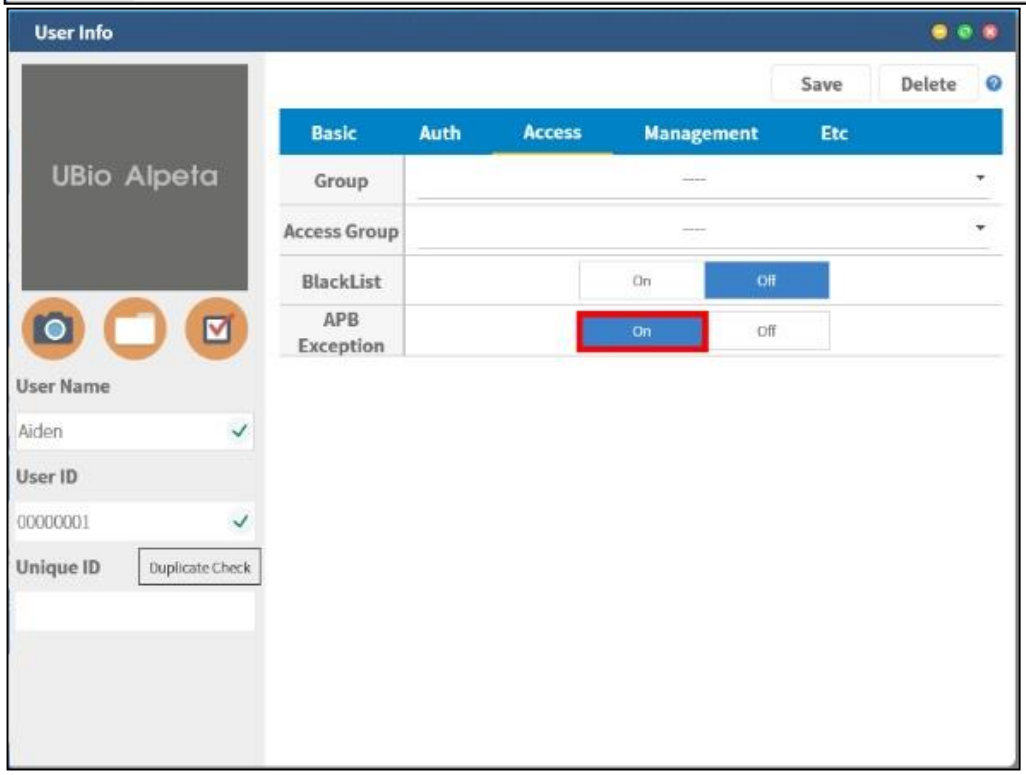


⑦ After that, you can see that Anti passback is normally set as below.



※ If the user has APB exception, the user can access as usual without going through APB system. This is usually used for VIP (main customer).



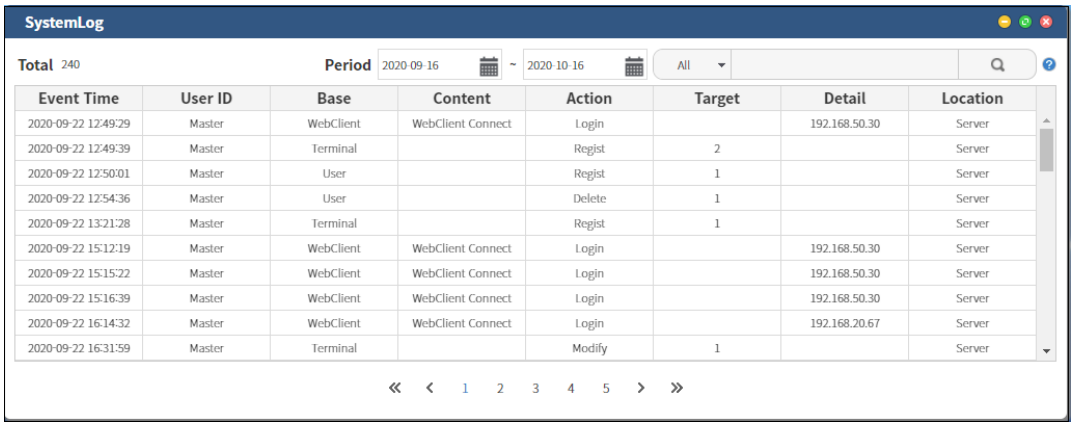


3. System Log

1) System log

The Alpeta administrator can search the operation history.

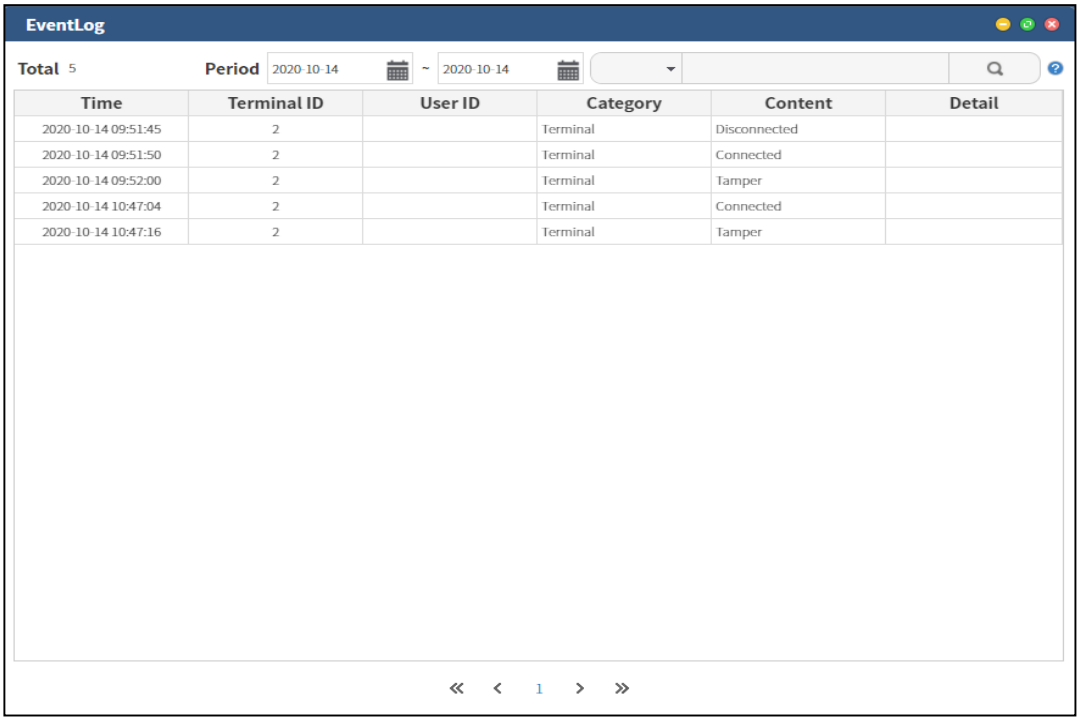
(ex. User information modification, client access log-in, etc.)



- **Total**: The number of searched log in a condition
- **Period**: Set the search period.
- **Condition**: Set the search condition.
- After setting all the search conditions, click button and search the log. The log is shown in page unit.

2) Event log

It searches the event log occurring from terminal.



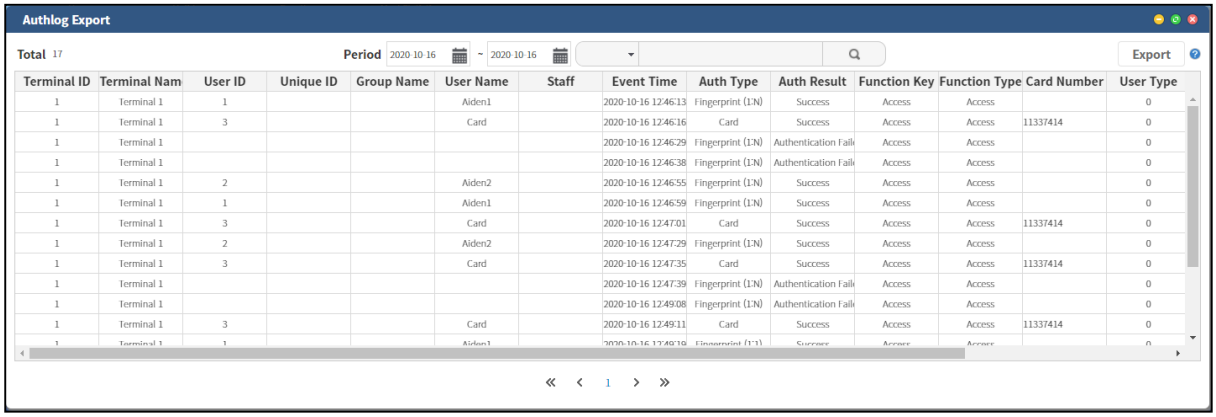
- **Total**: The number of log searched in a condition.
- **Period**: Set the search period.
- **Condition**: Set the search condition.
- [🔍]: After setting a search condition, click this button to search the log. You can see the log per page.

4. Auth log

1) Export Auth Log

It is the screen to export the authentication log.

You can download after converting the authenticated log saved in server into excel file.
This excel function is for saving the authentication log information.



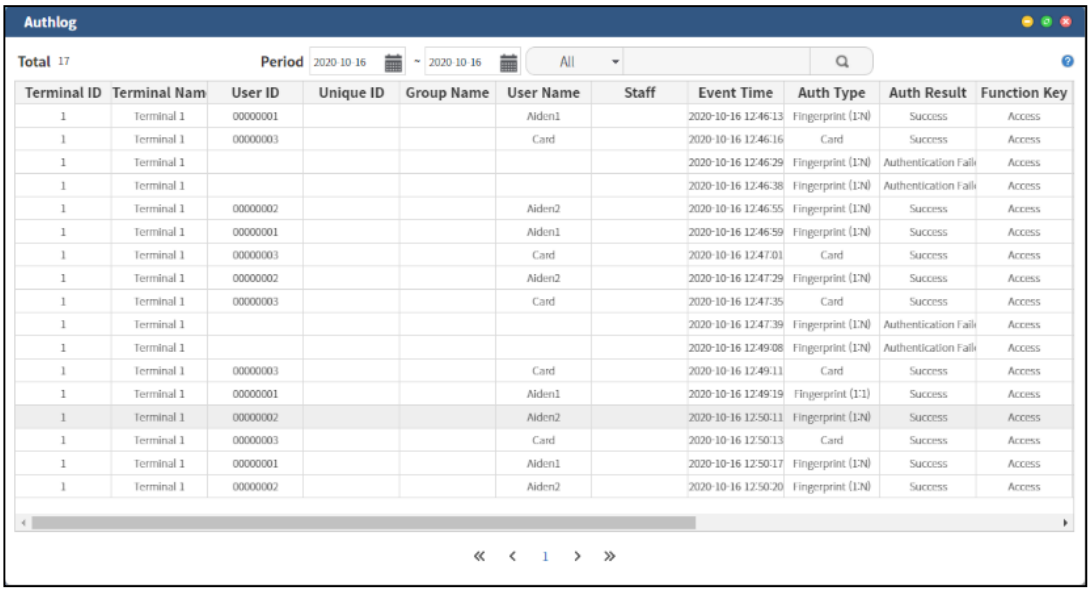
- **Total**: Show the number of the searched logs.
- **Period**: Set the period for log search. The search period is 30 days for a maximum.
- [🔍] : After setting the search condition and clicking this button, it searches the log within a setting period in a server. The searched log is displayed with 1,000 logs per page.
- **Export**: You can download the searched log by excel file. When clicking this button, the authentication log corresponding to the search condition is converted to an excel file and automatically downloaded.

2) Auth Log Management

It is the feature to search the authentication log of user.

It is not available to search after 30 days and the latest log can be searched in the last page.

If you want to export the authentication log as PDF, you can use it in 'Integrated report management'.

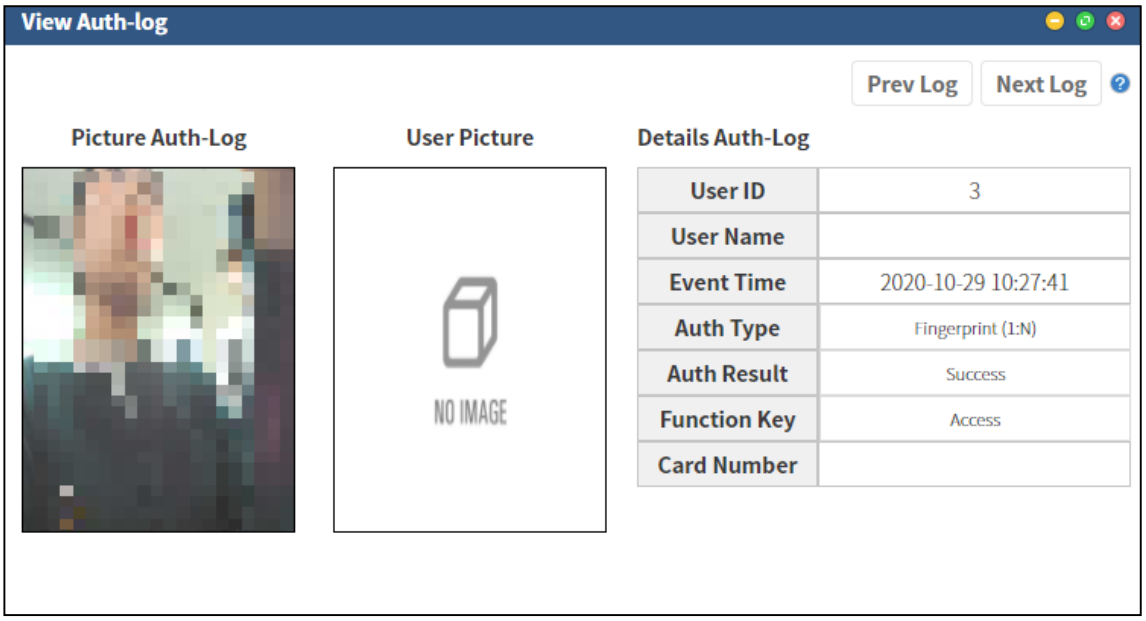


- **Total:** The number of log searched in a condition.
- **Period**: Set the search period.
-

: You can select one of categories among All / User ID / User name / Terminal ID / Terminal name / Unique ID and enter the keyword that you want to search. After setting all search conditions, click button to search. You can see the log per page.

3) View Auth-log

When you double-click the log in [**Auth-log**], you can see the detailed information.

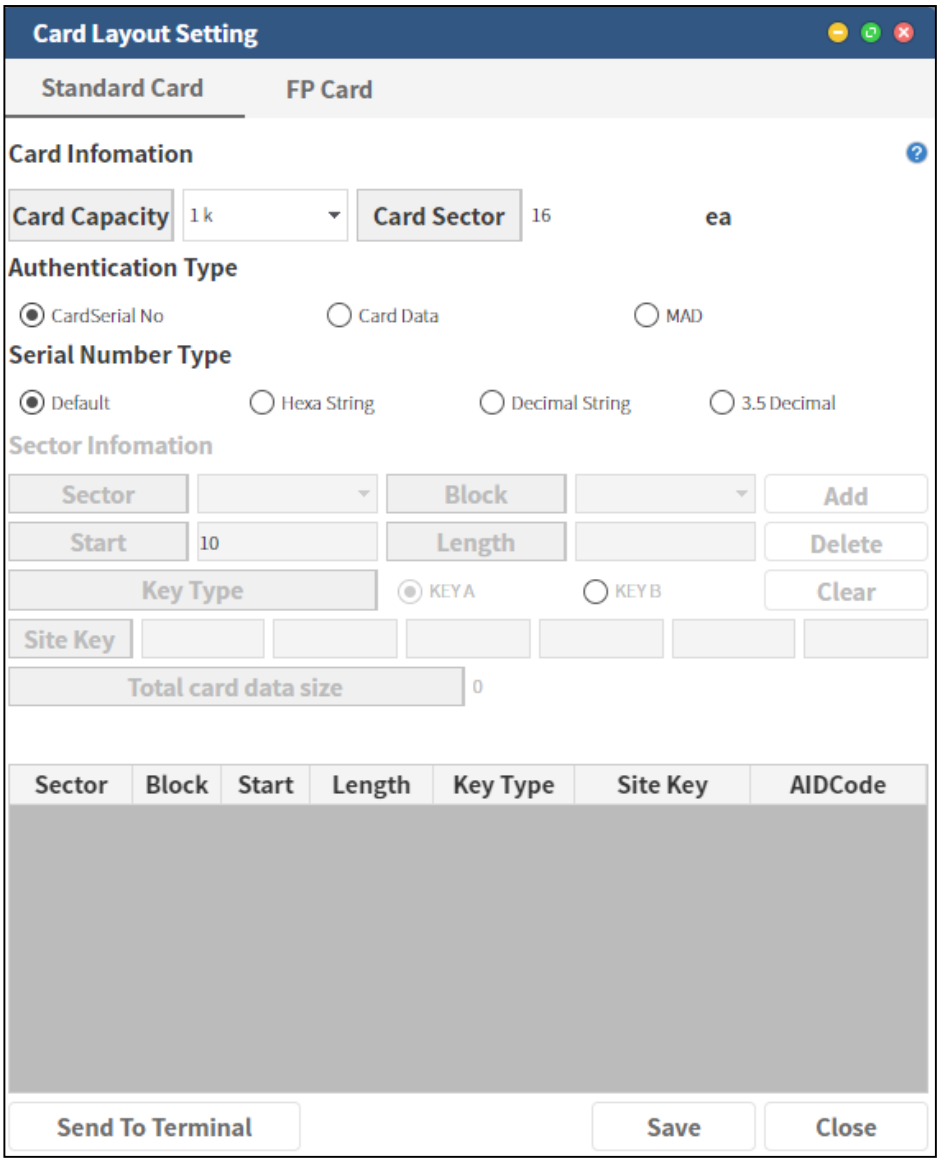


- **Auth-log Picture:** When authenticated on terminal equipped with camera, the captured photos are displayed in a real time.
- **User Picture**: If authenticated user was registered with photo, the registered photo is displayed.
- **Auth-log Detail:** Show the detailed information of Auth-log.
- **Previous log**: Show the detailed information of the previous log.
- **Next log:** Show the detailed information of the next log.

5. Card Layout

This feature to set the card layout for standard card and FP card.

1) Standard Card



- Card Information: Set the card capacity and card sector.
    - Card Capacity (Card Sector): Select among 1K, 4K, and 8K.
- Authentication Type
    - Card Serial No.: Select a smart card to authenticate with card serial number.
    - Card Data: Enter a specific data of card.
    - MAD: Select MAD as the authentication type.

- Serial Number Type

    - Default: 8-digit display with hex
    - Hexa String: Changing the order of Byte / 8-digit display with hex
    - Decimal String: 0-digit display with decimal number.
    - 3.5 Decimal : Change the hexadecimal number (8 digits) into decimal number (10 digits).

- Sector information

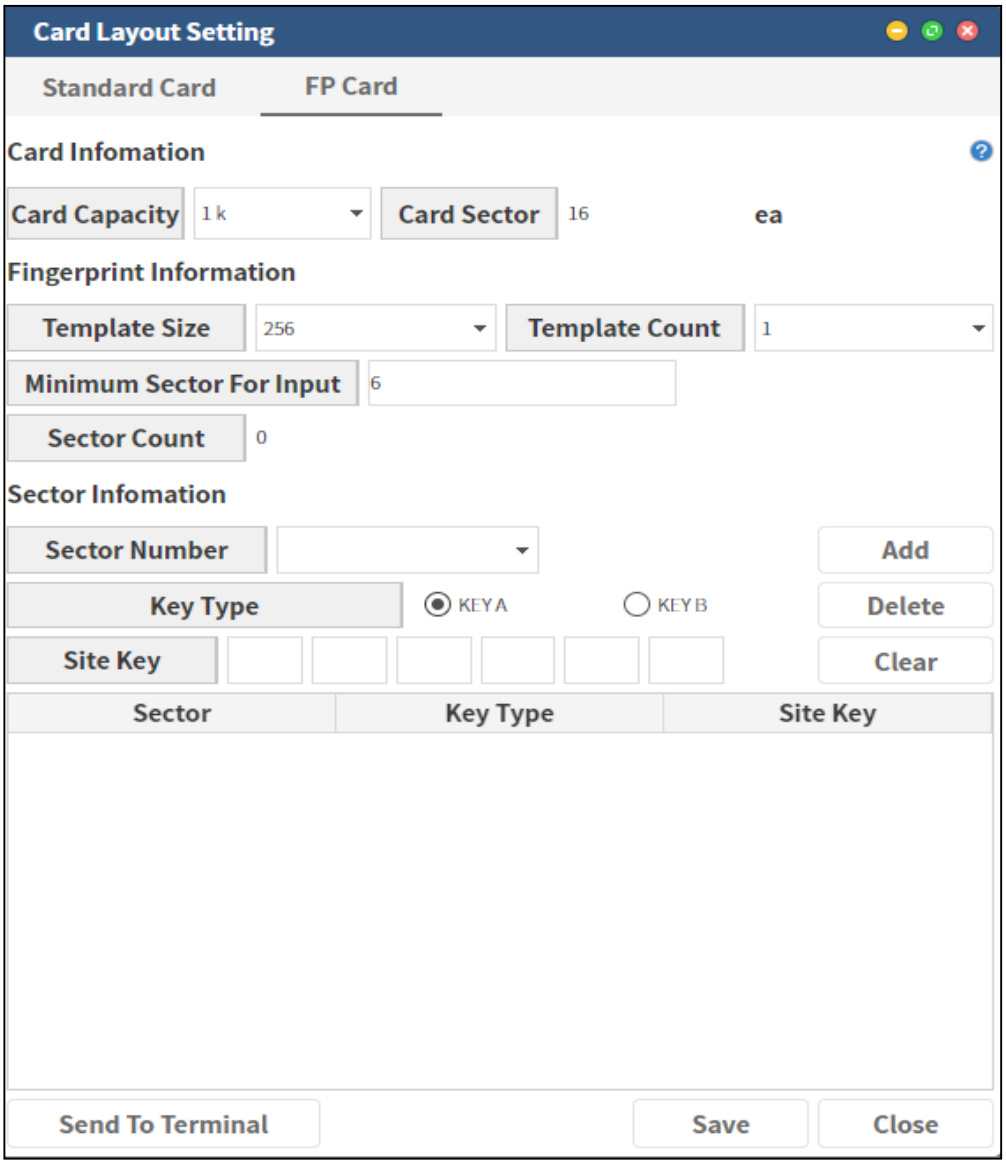
    - Sector: Select 000~015 depending on card capacity.
    - Block: Select 0~2 block.
    - Data Start / Data Length: Start of the data sequence number / Data Full length
    - Key Type: KEY A or KEY B
    - Site Key: Input key value depending on the key type.
    - Total card data size: It is the total card data size.

- **Add**: Press [**Add**] button to save the entered sector information.

- **Delete**: After selecting the data, select [**Delete**] button to delete it.

- **Clear**: Select [**Clear**] button to delete the entered sector information. Press [**Send to Terminal**] button to send the setting information to the terminal.

2) FP Card



- Card Information: Set the card capacity and card sector.
    - Card Capacity (Card Sector): Select among 1K, 4K, and 8K.
- Fingerprint Information
    - Template Size: Select FP template size (256, 300, 400, 800)
    - Template Count: Count the FP template size (1~5).
    - Minimum Sector For Input: Specify the minimum number of sectors.
    - Sector Count: Show how many sectors are added
- Sector information
    - Sector: Select the sector number. (1~5)

- Key Type: KEY A or KEY B
- Site Key : Input key value according to the key type

- **Add**: Press [**Add**] button to save the entered sector information.

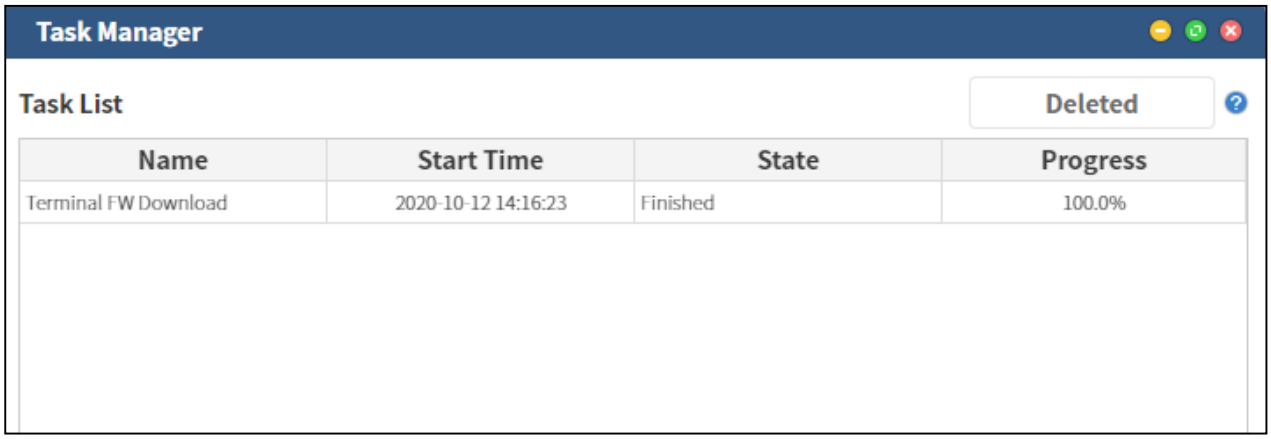
- **Delete**: After selecting the data, select [**Delete**] button to delete it.

- **Clear**: Select [**Clear**] button to delete the entered sector information. Press [**Send to Terminal**] button to send the setting information to the terminal.

6. Task Manager

It shows the task history operated in the server.

Specifically, the access group user update, terminal FW download, sending the access group information to the terminal, terminal user upload (import), Wiegand information download, DB encryption, meal process and synchronization, etc.

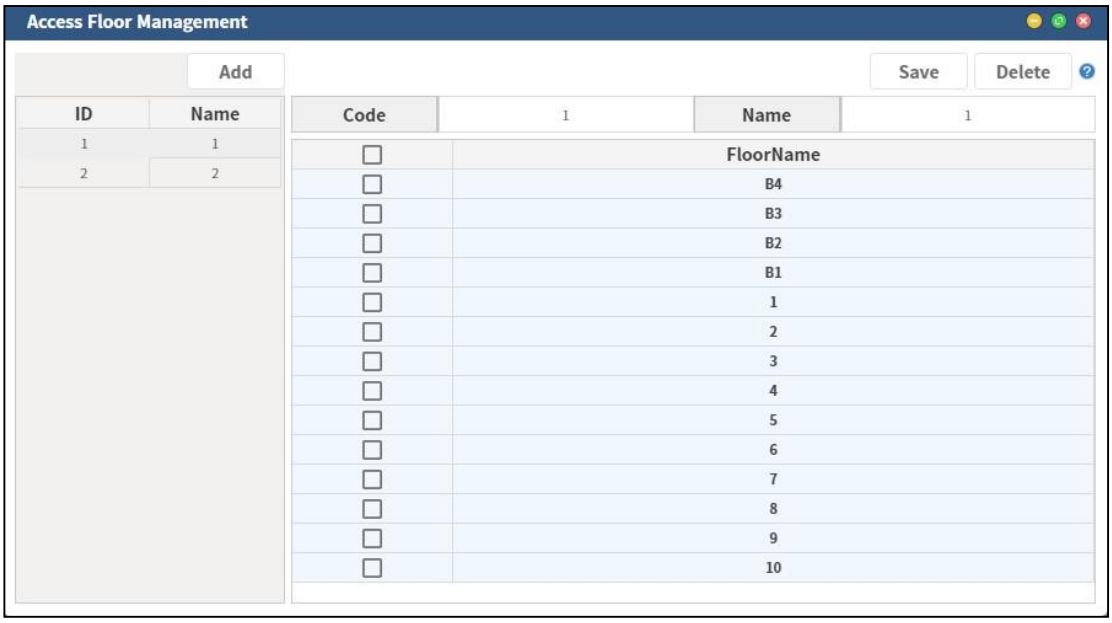


- **Name**: Show the operation name.
- **Start Time**: Show the start time of the task.
- **State**: Show the current status of the task. It shows the status with Ready, Waiting, Operating and Finished.
- **Progress**: Show the progress rate of the operation.

7. Elevator

1) Access Floor Management

It manages the access floor to be assigned to the access group.



- **Add**: Create the new access floor item.
- **Save**: Set the name and checks the floor (multiple checking available) to save.
- **Delete**: Delete the selected access floor information.

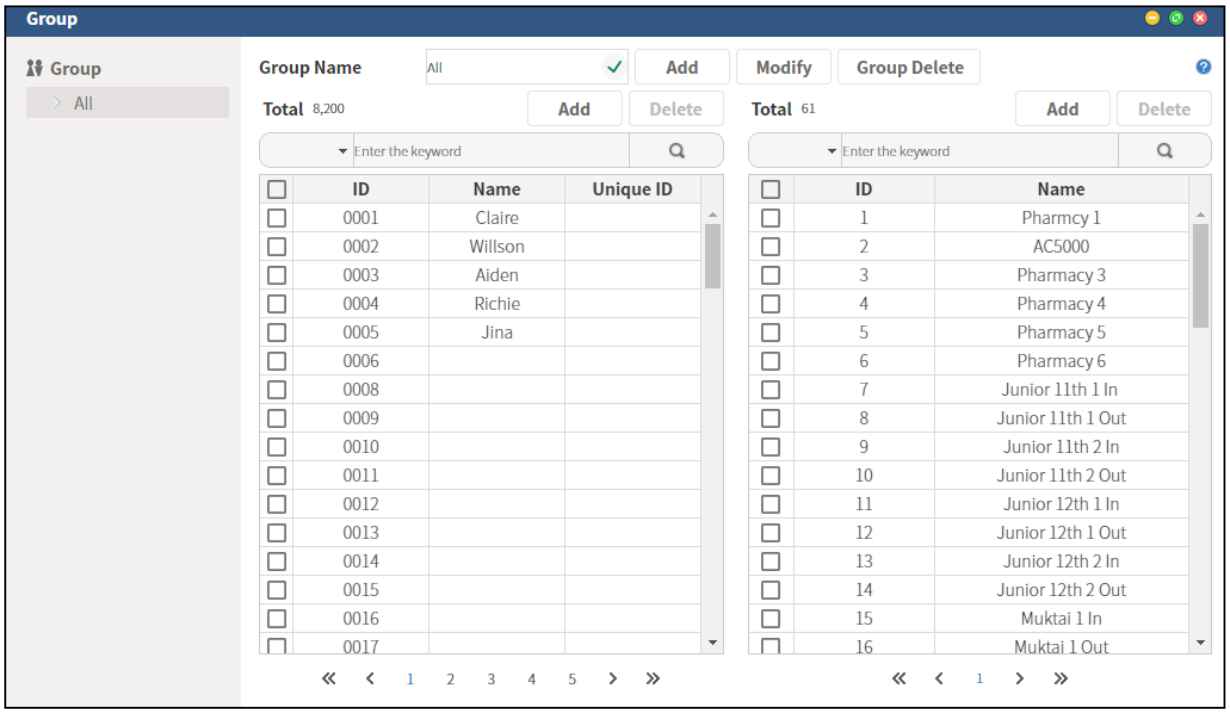
8. Group

It is the screen to manage the groups. You can add, modify and delete the group.

Also, you can add or delete the user and terminal in the created group.

The group integrates the user and terminal to operate and manages them.

1) Manage the group

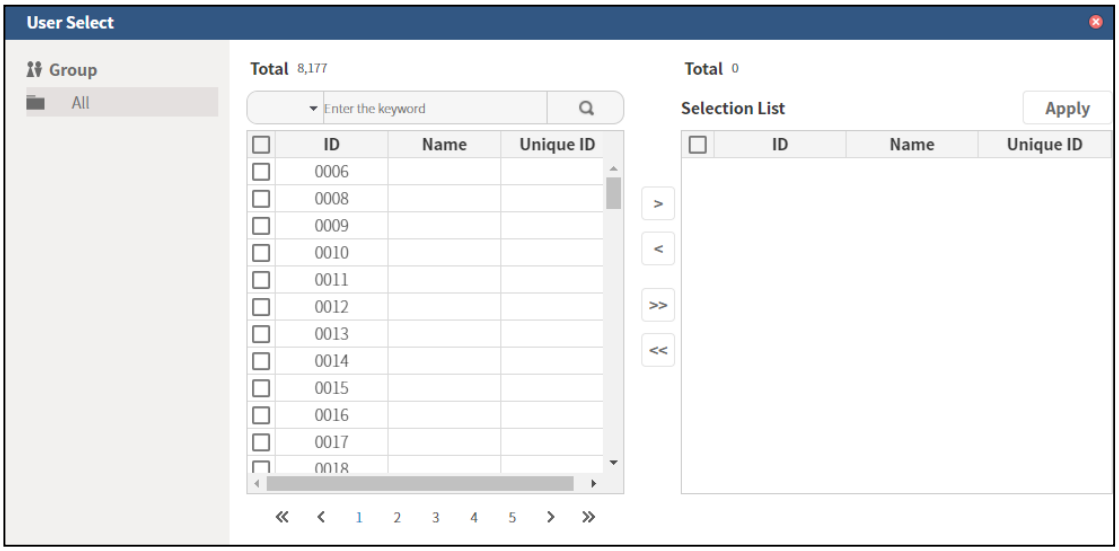


- **Group**: The registered group is shown with tree type. You can add 200 groups for a maximum. When clicking the group name, you can see the user and terminal included in the group.
- **Group Name**: It is the group name. You can enter 100 digits for a maximum.
- **Add**: Enter the group name and select [**Add**] button to add the new group.

  Since it is an empty group after creating a new group, you can assign the user and the terminal by clicking [**Add**] button each on user list and terminal list.
- **Modify**: Select the group name to modify in the left side and modify the user list and terminal list by click [**Add**]/[**Delete**] button each on the user and terminal list
- **Group Delete**: You can delete the created group.

2) Select the user

When you select the group in the left side, you can see the user included in a group.



-

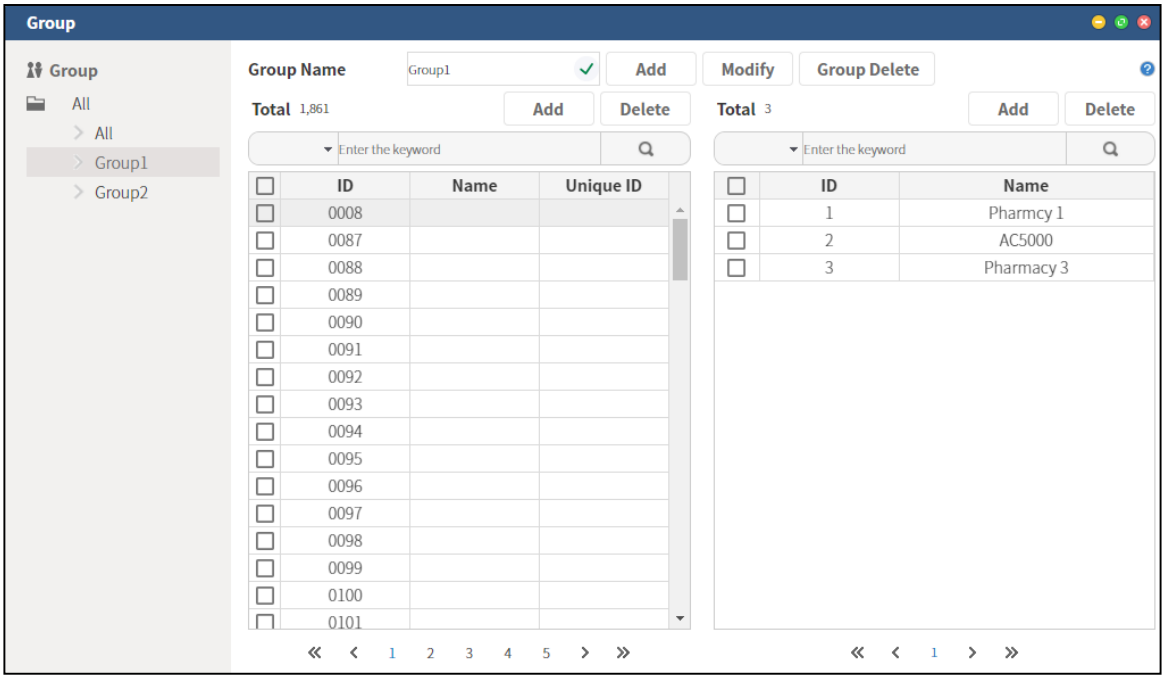
: It can search the user with ID/ Name/ Unique ID.

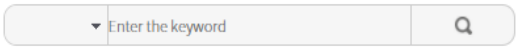
- **Add**: Select [**Add**] on the user list if you want to add the user in the group.

- **Delete**: Select the user to delete and [**Delete**] button on the user list if you want to delete the user in the group.

3) Select the terminal

When you select the group in the left side, you can see the terminal included in a group in right side.



- 

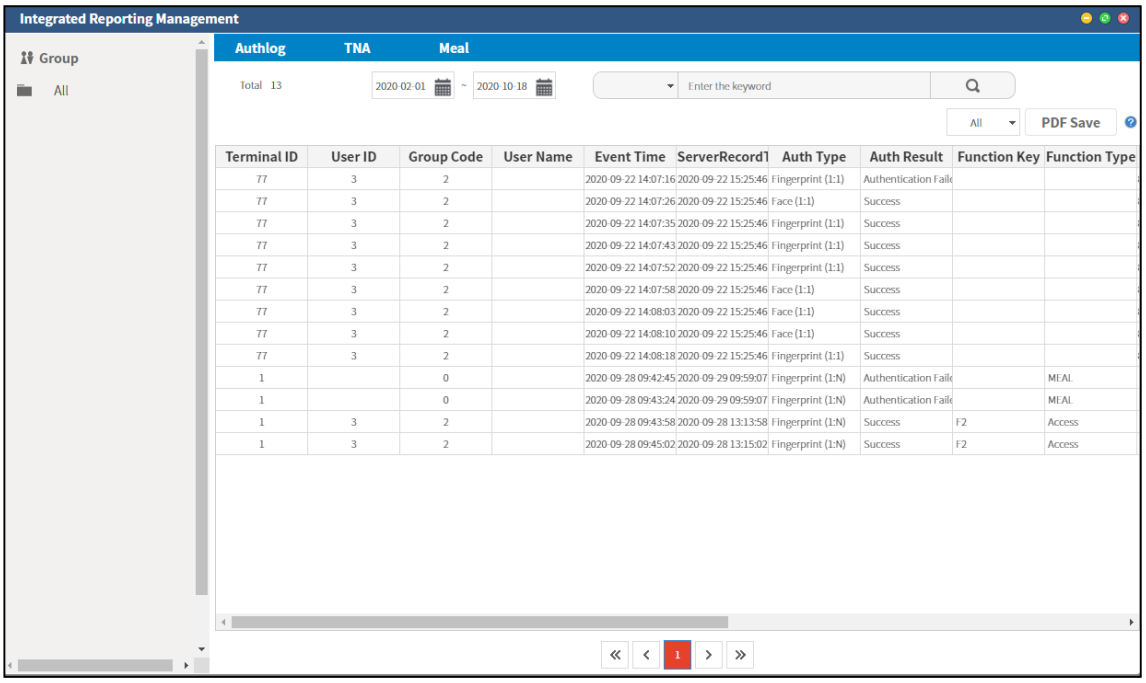
: Search the terminal in a group.

- **Add**: Select [**Add**] on the terminal list if you want to add the terminal in the group.

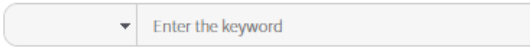
- **Delete**: Select the terminal to delete and [**Delete**] button on the terminal list if you want to delete the terminal in the group.

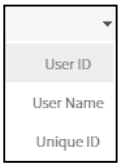
9. Integrated Report Management (AuthLog, TNA, Meal)

You can search the authentication log, TNA and meal result and save the search result as PDF.



The integrated reporting management screen consists of a group selection screen, authentication log, T&A, and meal service tab. You can search the data of each item by clicking the authentication log, T&A, and meal service tabs.

- **Total**: Total logs count searched in the condition.
- **Period**: Set the data period for searching.
- 

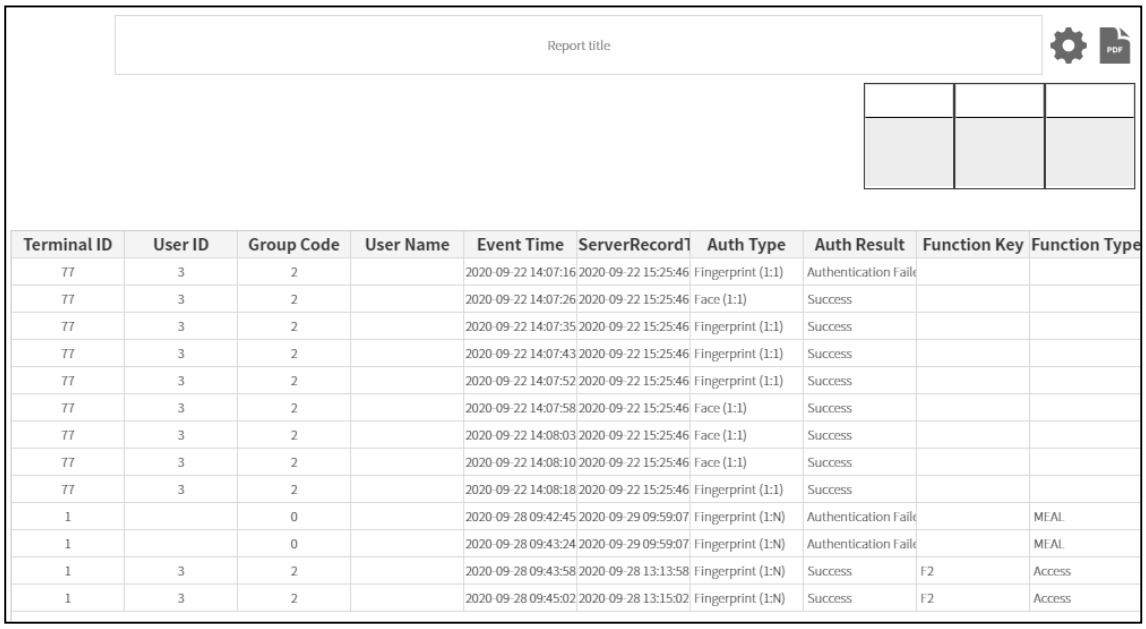
: Enter the keyword to search.
- 

: You can select one of 3 categories (User ID/ User Name/ Unique ID) for searching.
-

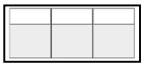
: You can get the result in the report among All/ Success/ Fail.
- **PDF Save**: Save the result as PDF file.

1) Integrated Report Management (PDF Save)

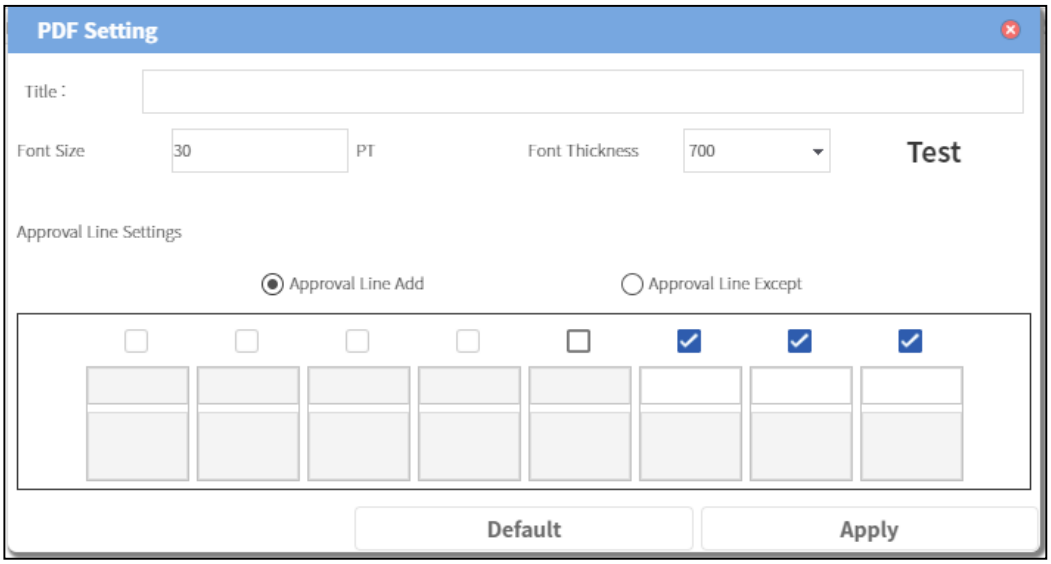
You can download the integrated report as PDF.



Terminal ID	User ID	Group Code	User Name	Event Time	ServerRecord1	Auth Type	Auth Result	Function Key	Function Type
77	3	2		2020-09-22 14:07:16	2020-09-22 15:25:46	Fingerprint (1:1)	Authentication Faile		
77	3	2		2020-09-22 14:07:26	2020-09-22 15:25:46	Face (1:1)	Success		
77	3	2		2020-09-22 14:07:35	2020-09-22 15:25:46	Fingerprint (1:1)	Success		
77	3	2		2020-09-22 14:07:43	2020-09-22 15:25:46	Fingerprint (1:1)	Success		
77	3	2		2020-09-22 14:07:52	2020-09-22 15:25:46	Fingerprint (1:1)	Success		
77	3	2		2020-09-22 14:07:58	2020-09-22 15:25:46	Face (1:1)	Success		
77	3	2		2020-09-22 14:08:03	2020-09-22 15:25:46	Face (1:1)	Success		
77	3	2		2020-09-22 14:08:10	2020-09-22 15:25:46	Face (1:1)	Success		
77	3	2		2020-09-22 14:08:18	2020-09-22 15:25:46	Fingerprint (1:1)	Success		
1		0		2020-09-28 09:42:45	2020-09-29 09:59:07	Fingerprint (1:N)	Authentication Faile		MEAL
1		0		2020-09-28 09:43:24	2020-09-29 09:59:07	Fingerprint (1:N)	Authentication Faile		MEAL
1	3	2		2020-09-28 09:43:58	2020-09-28 13:13:58	Fingerprint (1:N)	Success	F2	Access
1	3	2		2020-09-28 09:45:02	2020-09-28 13:15:02	Fingerprint (1:N)	Success	F2	Access

- **Report Title**: Set the title of the report.
- : You can set title, font size, font thickness and approval line.
- : You can download the current page as pdf.
-  : Approval Box

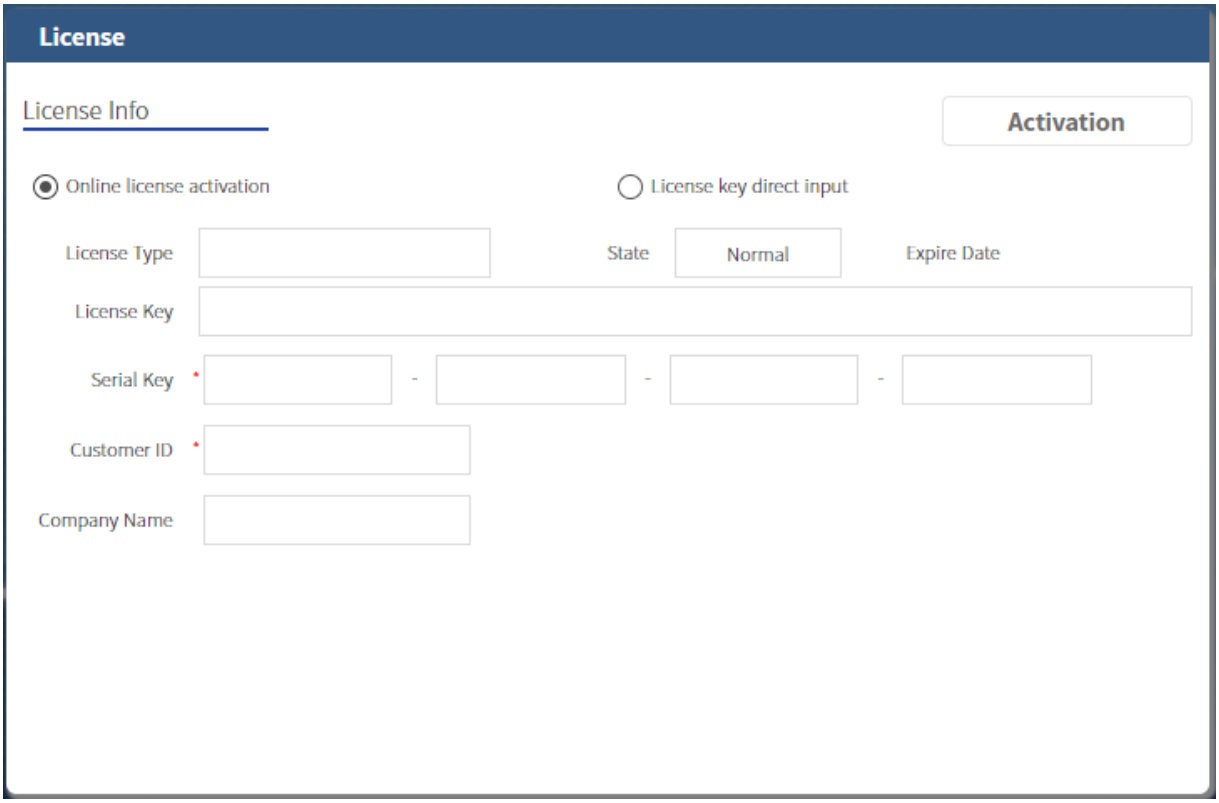
2) Integrated Report Management (PDF Setting)



- **Report Title**: Set the title.
- **Font Size**: Set the font size.
- **Font Thickness**: Set the font thickness.
- **TEST**: Preview of font size and font thickness you set.
- **Approval Line Settings**: You can add or delete the approval line.
- **Default**: Reset settings to default.
- **Apply**: Apply the current setting.

10. License registration

1. License screen will be pop-up when you install Alpeta first. Alpeta is available after activate License.



(1) Online License Activation

- Activate License from online. (Server PC should be available to access online.

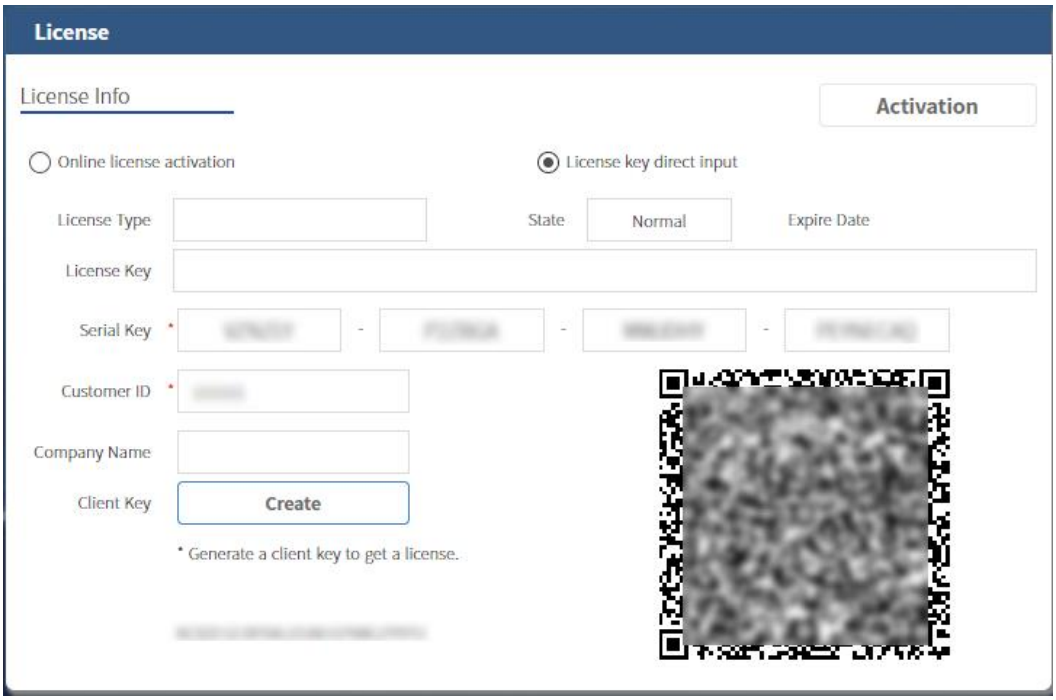
- Serial Key: Find serial key from installation package and enter here. (Required)

- Customer ID: Input 6~20 characters of customer ID. The customer ID will be used later for license management. (Required)

- Company Name: Input company name. Up to 50 characters. (Option)

- Input serial key and customer ID. Click Activation button to activate online license activate.

(2) License key direct input



① Input Serial key to activate.

② Input Customer ID.

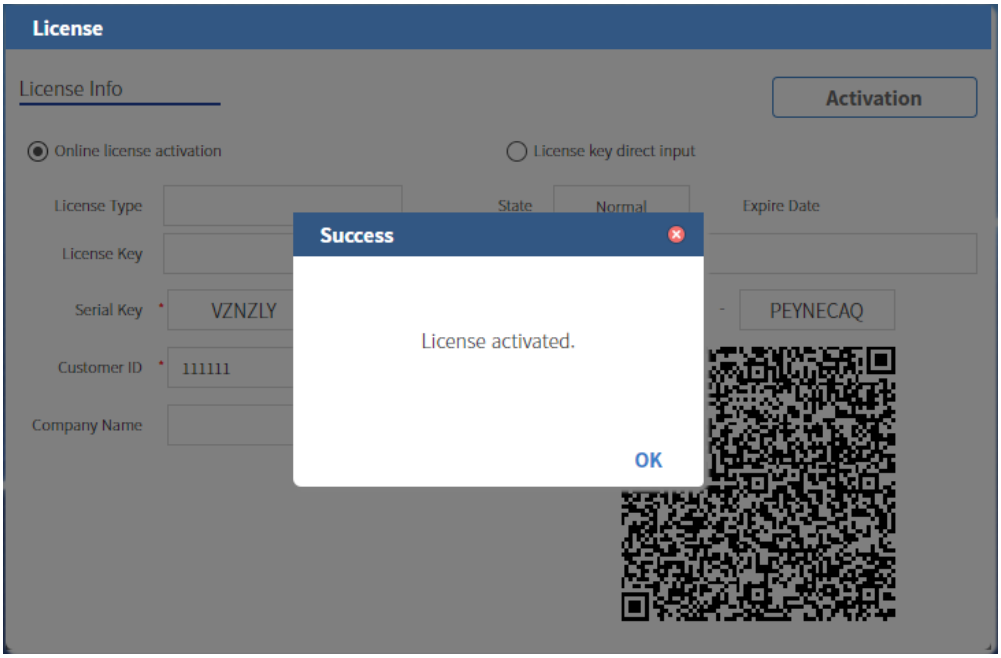
③ Click [**Create**] button.

④ Send serial key, client key, customer ID to our sales team.

⑤ Enter the issued license key and click [**Activation**] button

- Serial Key: Find serial key from installation package and enter here. (Required)
- Customer ID: Input 6~20 characters of customer ID. The customer ID will be used later for license management. (Required)
- Company Name: Input company name. Up to 50 characters. (Option)
- Enter Serial Key and Customer ID. Click "Generate" button. Client key will be generated.
- License Key: You can obtain the license key by providing the information of the generated client key, serial key, and customer ID to our sales team, or obtain the license key through QR code recognition.

-After entering the license key, click the [Activate] button to activate the license.

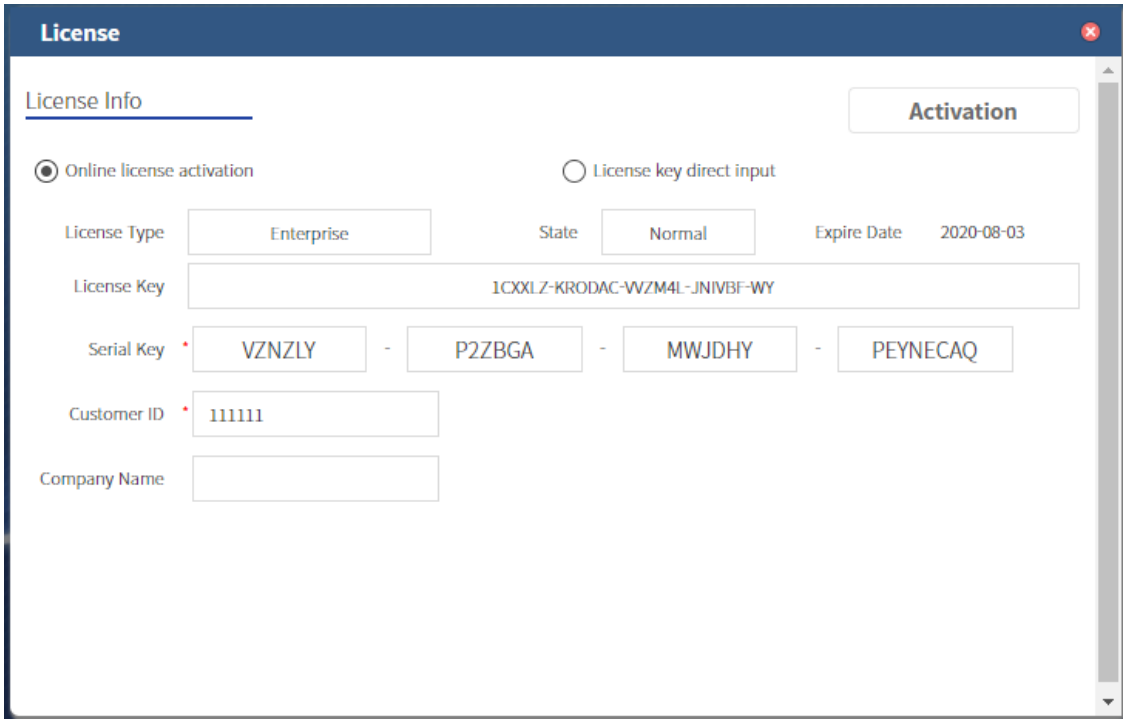


- You can check the message if the license if activated successfully.

2. Checking license information

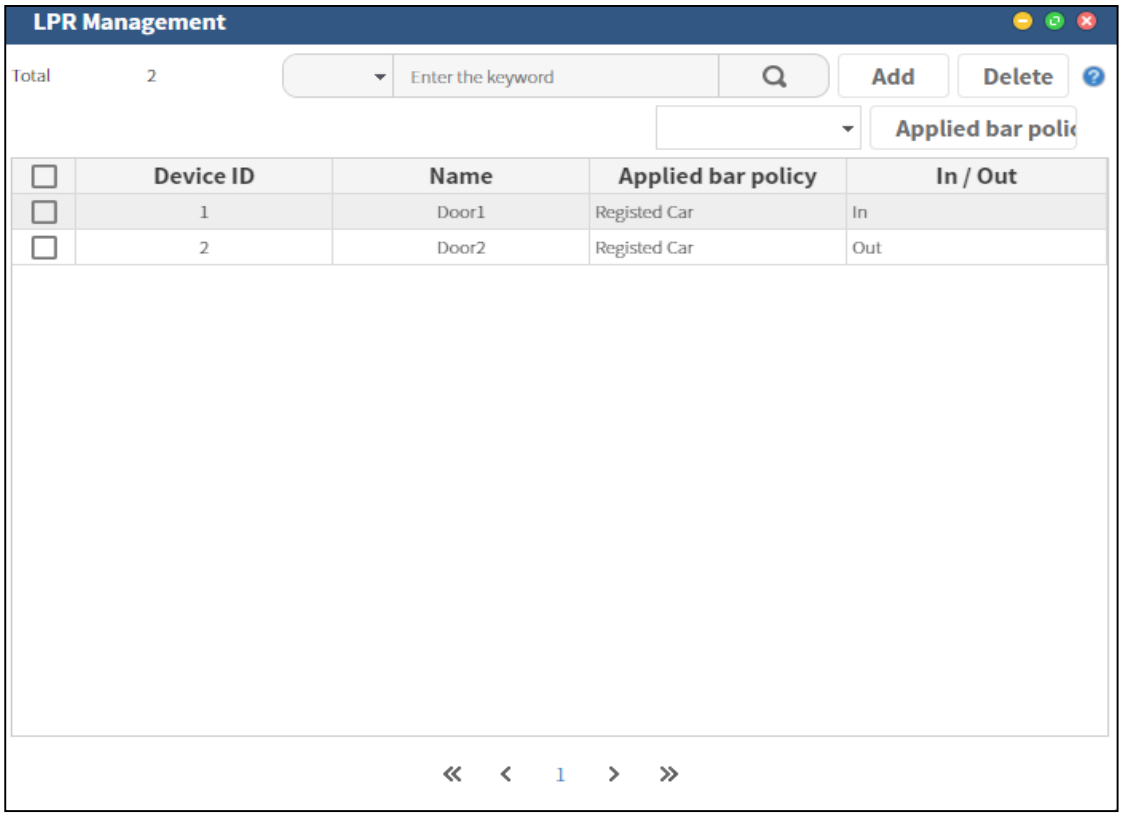
- You can check current license information by clicking icon of top menu bar.

- Click License button to check current license information.



11. LPR Management

It is the screen to manage LPR (License Plate Recognition).



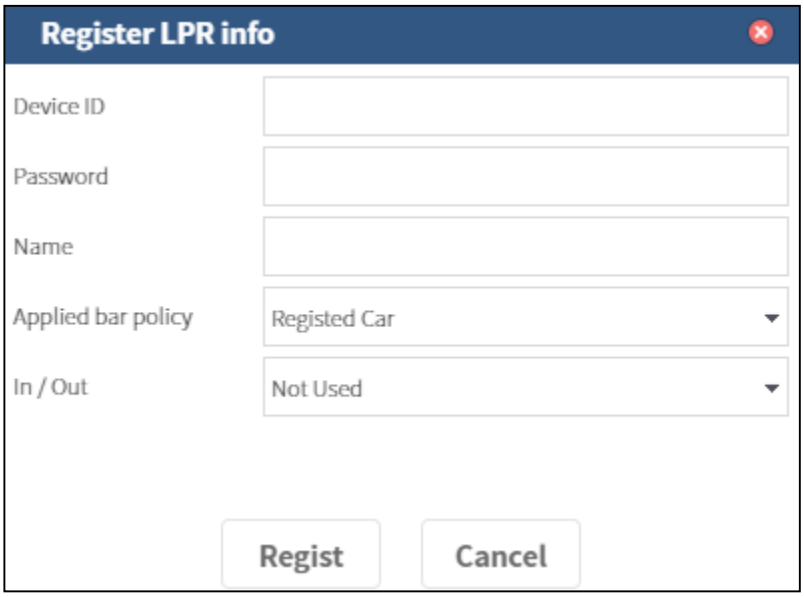
-

: For searching, you can select Device ID or Name in the category and enter the keyword.

- **Add**: Add the LPR device registration information.

- **Delete**: Delete the LPR device information.

- **Apply**: It can set the policy for 'Registered Card', 'Auto Pass', and 'Manual Pass'.

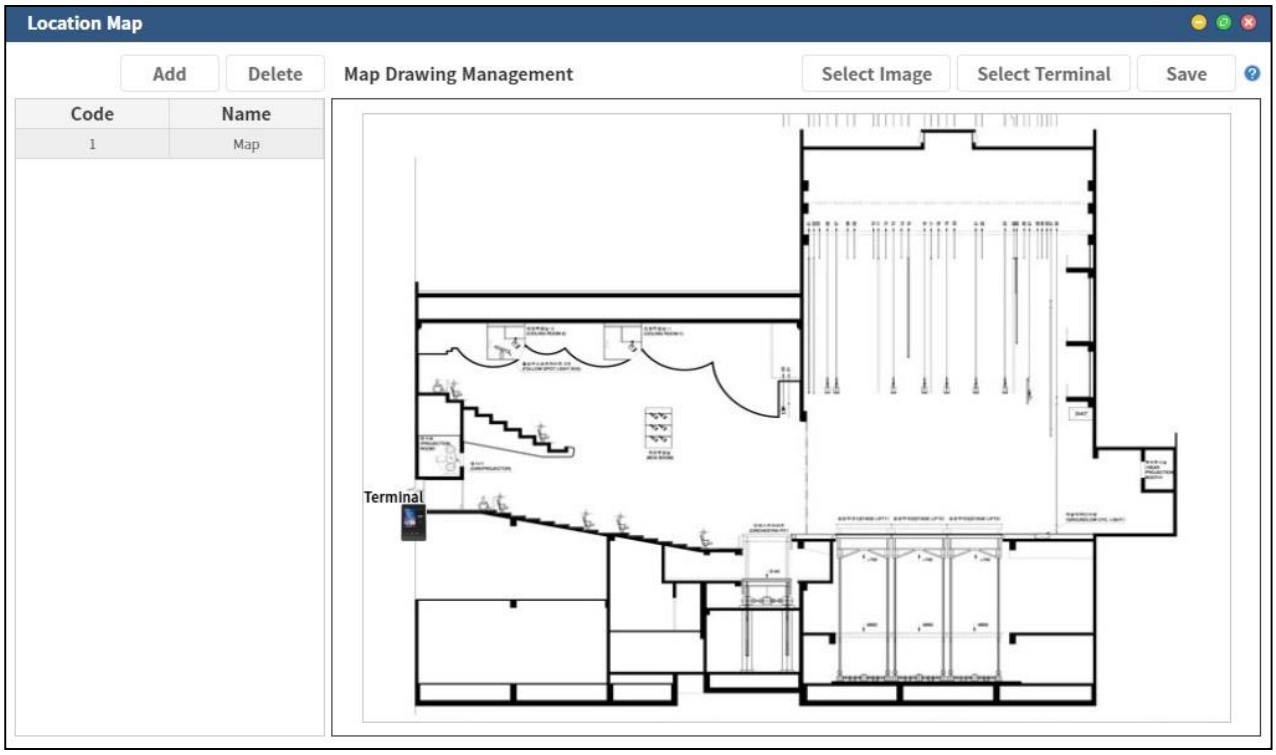


- **Device ID**: The ID of LPR device. It can enter the duplicated ID.
- **Password**: It can enter the password of registered LPR device, which can be up to 8 digits.
- **Name**: It can enter the name of LPR device.
- **Applied bar policy**: It can set the policy for opening/closing the LPR parking barrier among 'Registered Car, 'Auto Pass', and 'Manual Pass'.
- **In/Out**: When saving the LPR device, it can separate and set if it is installed in the entrance or exit. You can set one of 3 options; 'No use', 'Entrance' and 'Exit'.

After setting all, select [**Register]** to complete this setting.

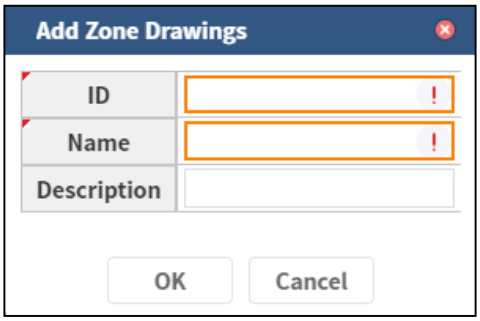
12. Location visualization

1) Map management



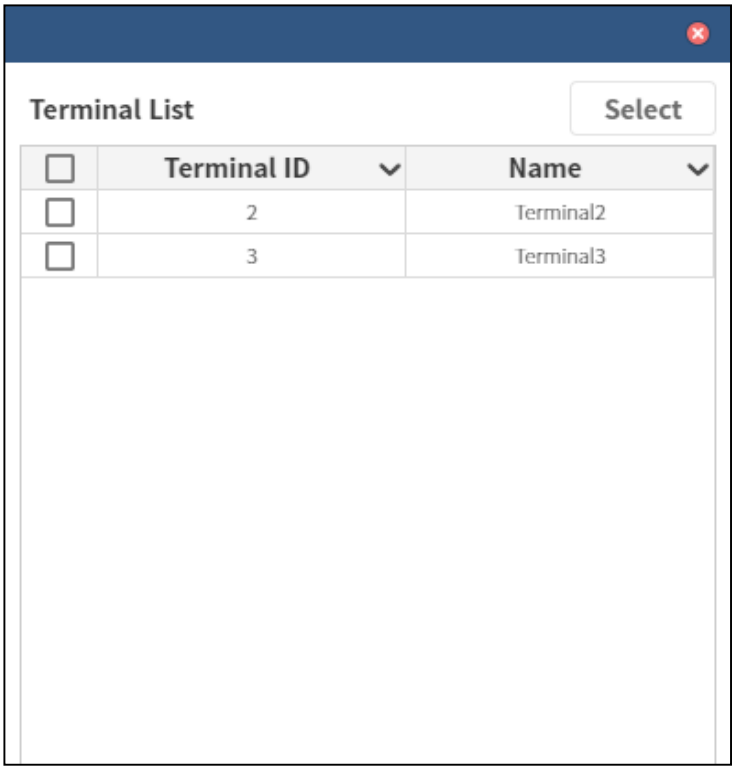
To use the location position, you should add the area map first. If you use the map management, it can set the map image and terminal location about the area.

- **Add**: Add the information of a draft.



- **Delete**: Delete the selected map.
- **ID**: Enter a unique numeric code. If the code already exists, it is not available.
- **Name**: Enter the name.
- **Description**: Enter the description of the map.

- **Select Image**: Set the image to use in a draft.
- **Select Terminal**: Select the terminal to use in a draft.
- **Save**: Save the modified one.



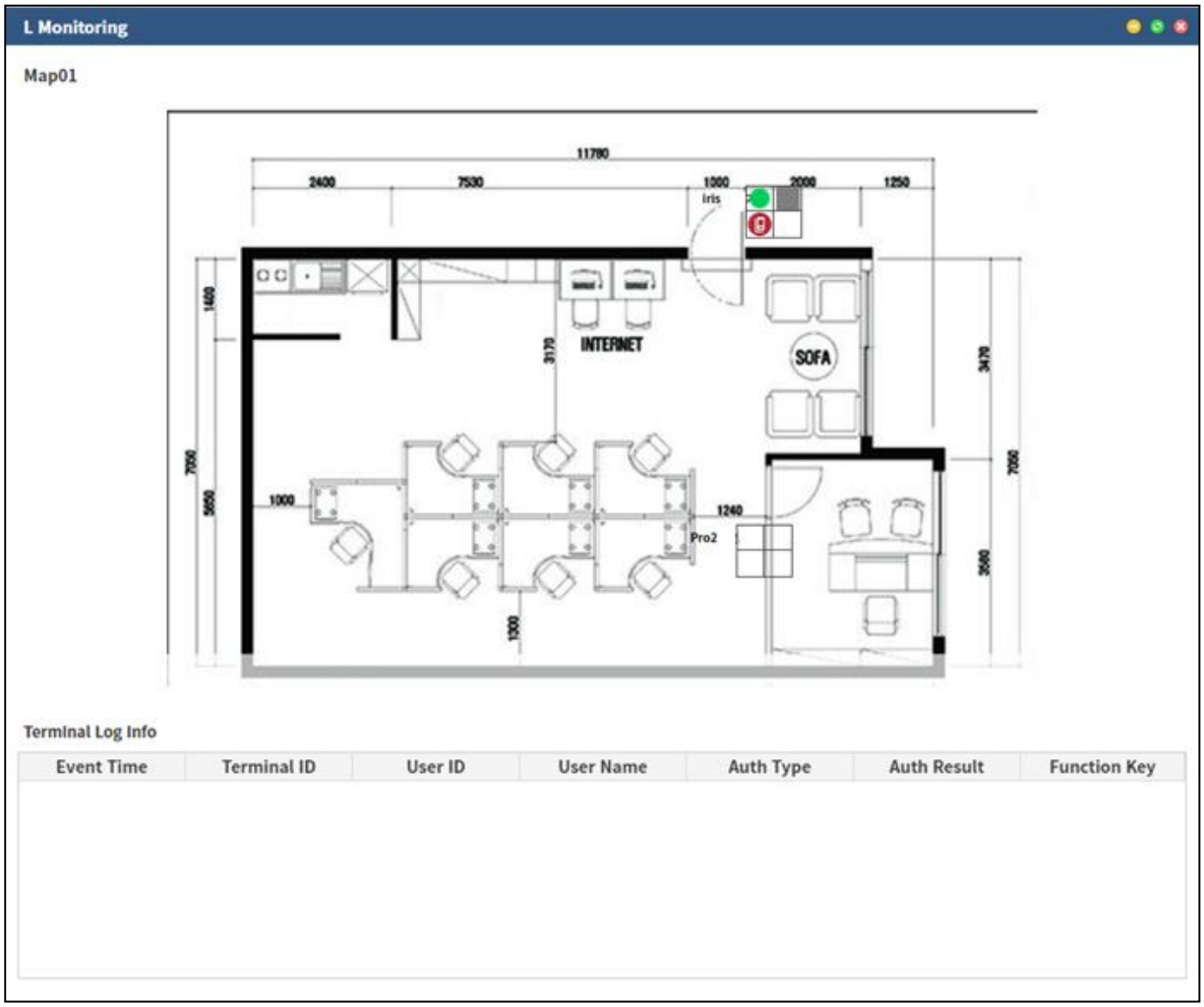
It displays the registered terminal. After selecting the terminal to set, click [**Select**] button to create the icon in a draft.

-

: Drag this icon with mouse and set it in the location that you want.

2) Location positioning monitoring

Double click on the icon in a draft to see the log or status of the terminal in the area.



The draft image and terminals are displayed in the center of screen. The icon of terminal status is displayed in the right bottom of terminal icon together.

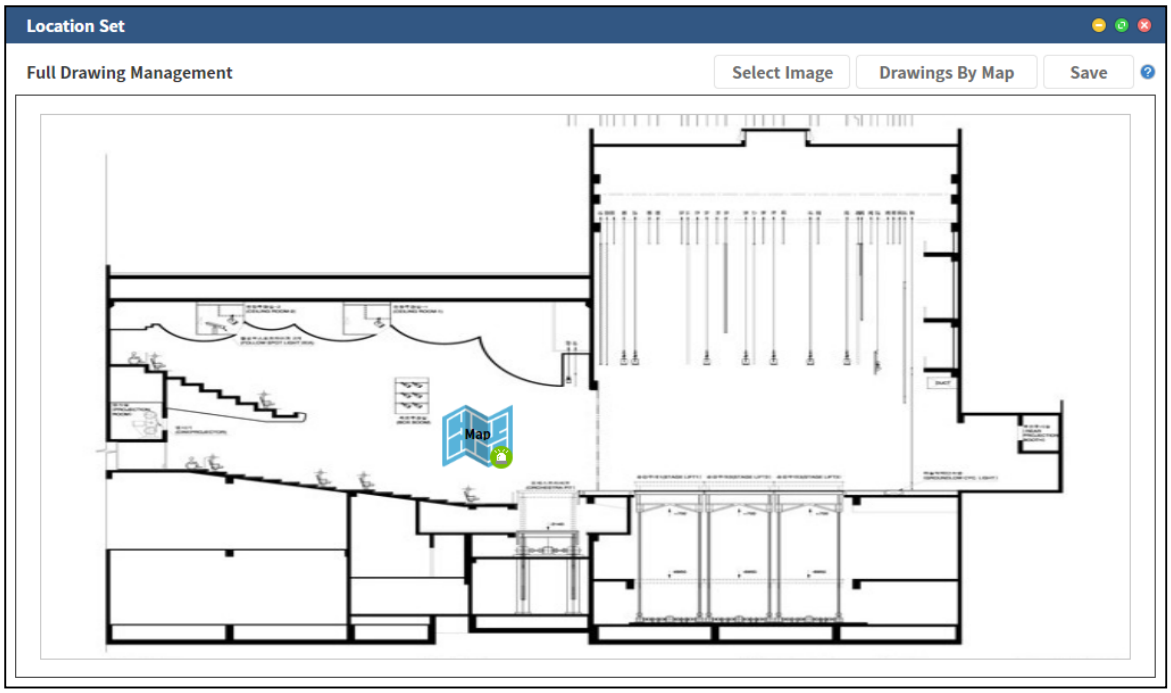
- **Terminal log information**: The event log that occurs in the terminal of the area is displayed in a real time.

3) Localization visualization

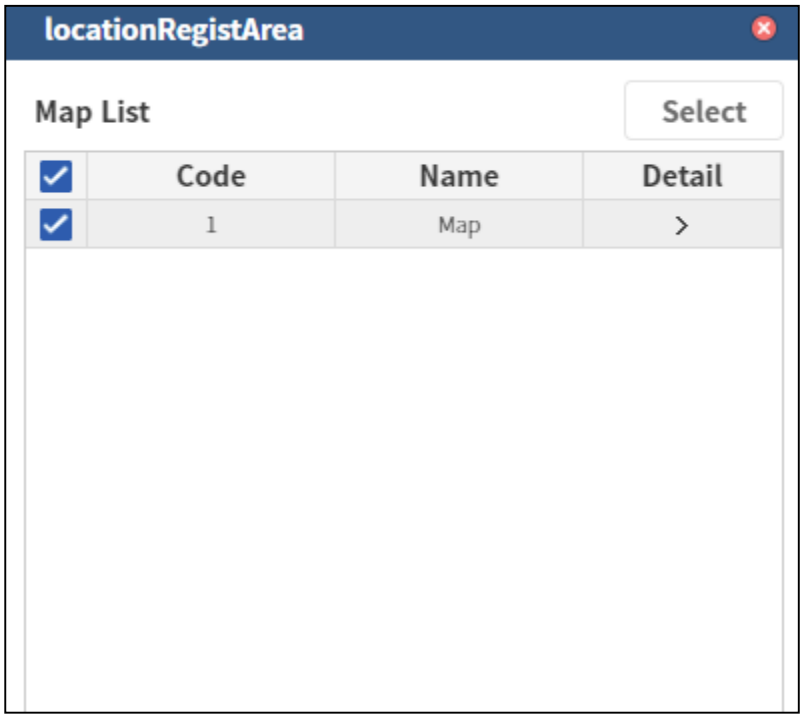
It is the feature to monitor the terminal status in a registered map, not in the monitoring menu, in a real time.

Set the created area in a draft and add and manage the terminal in the area.

The image file to register in a location position is available for JPEG, BMP and PNG.



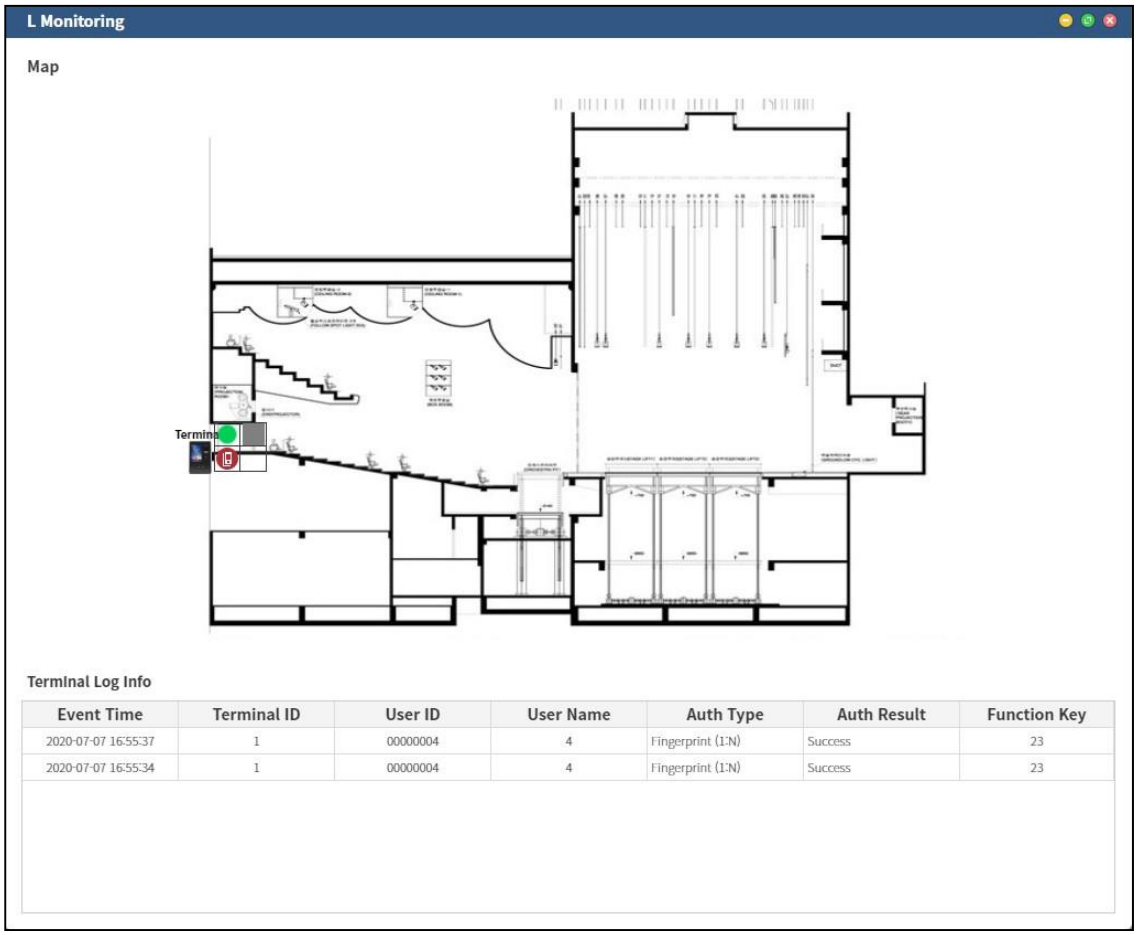
- **Select Image**: Select the image to use in the entire draft. It supports JPEG, BMP, and PNG.
- **Drawings By Map**: Set the area to add.



Select the map code to add in a dialogue box and click [**Select**] button to create the icon in the entire map management.

Drag the icon with mouse and set it in the location you want. You can refer [**Map management**] to manage the area map.

- **Save**: Save the modified one. You can delete the area map by using [**Delete**] button after clicking right-mouse button. Double-click on the area map to access the Location Monitoring page.



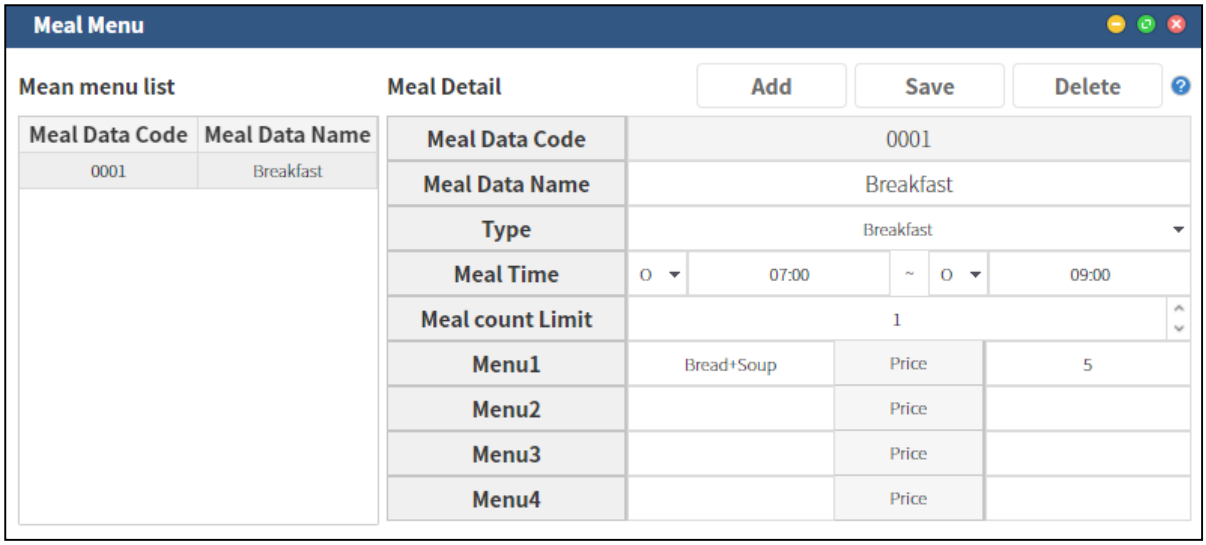
You can check the terminal status and authentication log of area map. (For the terminal status, refer to the monitoring page.)

13. Meal Service

1) Meal Menu

It manages each meal menu that make up Meal. Register a new meal menu code, and modify or remove the registered meal menu code.

The registered meal menu code is used for meal management.



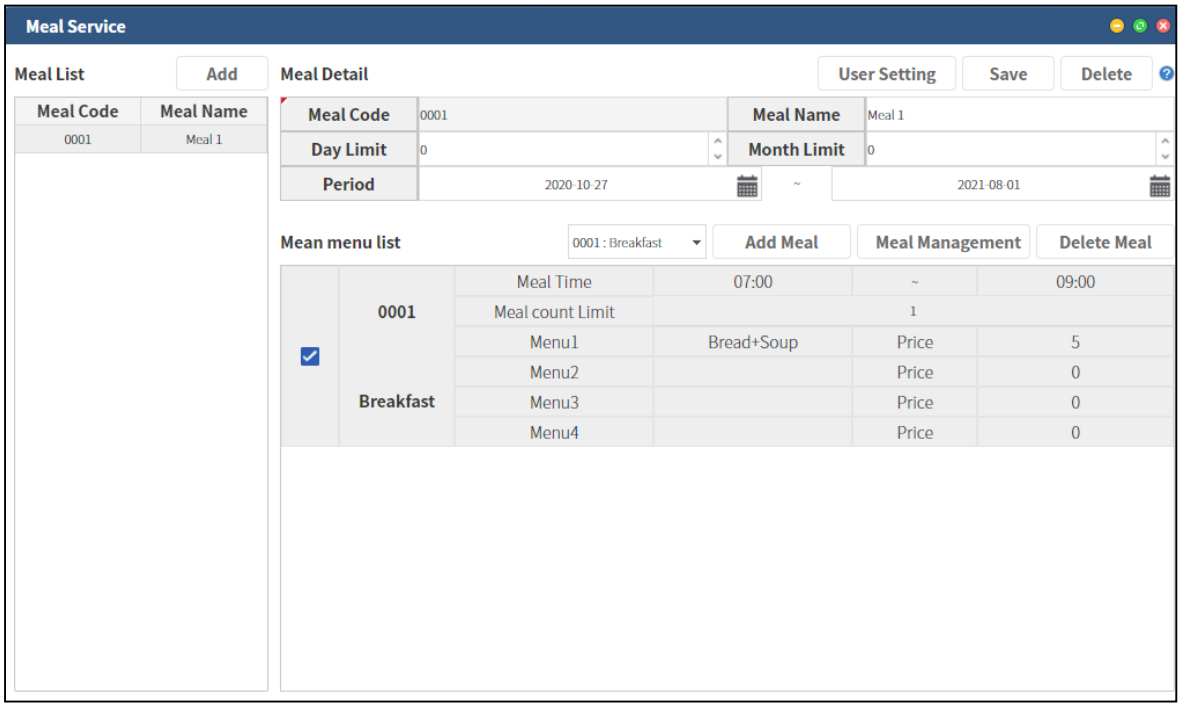
- **Meal Data Code**: An unique Meal Data code. It consists of 4 digits.
- **Meal Data Name**: Meal Data name. Up to 30 characters can be entered here.
- **Meal Time**: Meal-applied time
- **Meal Count Limit**: The available count for duplicate meal. It is unlimited when it set as 0.
- **Menu 1~4**: The menu can be set from 1 to 4.
- **Price**: Set the price of each menu.
- **Add**: The detailed setting is displayed to register a new meal data. The available code is automatically assigned in the code field and can be changed by the user. Fill each column and click [**Save**] button to register the meal data code in the server.
- **Modify**: Modify the registered meal data. When selecting the registered data in the meal list, it shows the setting information. Click [**Save**] button after modifying details.
- **Delete**: Delete the registered meal data code. When selecting the registered data in the meal list and click [**Remove**] button, it deletes that code in the server.

2) Meal Service

It manages the data to use for the meal mode.

It can register a new meal code, modify or delete registered meal code.

The meal data code registration is needed before registering the meal code.

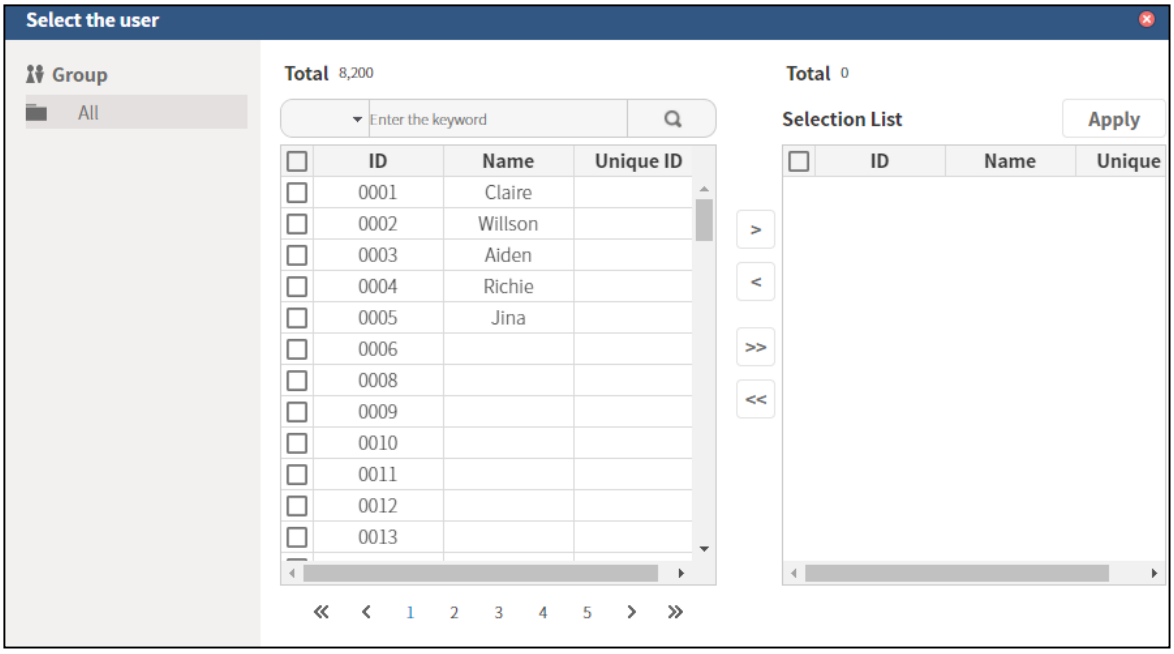


- **Meal List**: Meal code list registered on the server. When clicking a meal code, it shows the details in the right side.
- **Meal Code**: An unique meal code. It is up to 4 digits.
- **Meal Name**: Name of meal code. Up to 30 characters can be entered.
- **Day Limit**: Daily meal time limitation.
- **Month Limit**: Monthly meal time limitation.
- **Period**: The applied period with this setting.
- **Add**: The detail settings are displayed to register a new meal code.
  The available code is automatically assigned in the code field and can be changed by the user. Other data is set as default.
  Set data and click [**Save**] to register server.
- **Save**: Modify the registered meal code.
  When clicking the registered meal in the meal list, it shows meal details and meal list.
  After modifying the setting information, click [**Save**] button to register it in the server
  Modify details and click [**Save**] button.

- **Delete**: Delete registered meal data code.

  Select registered meal data code and click [**Delete**] button.

- **User Setting**: The user setting screen is popup to assign meal code to users.



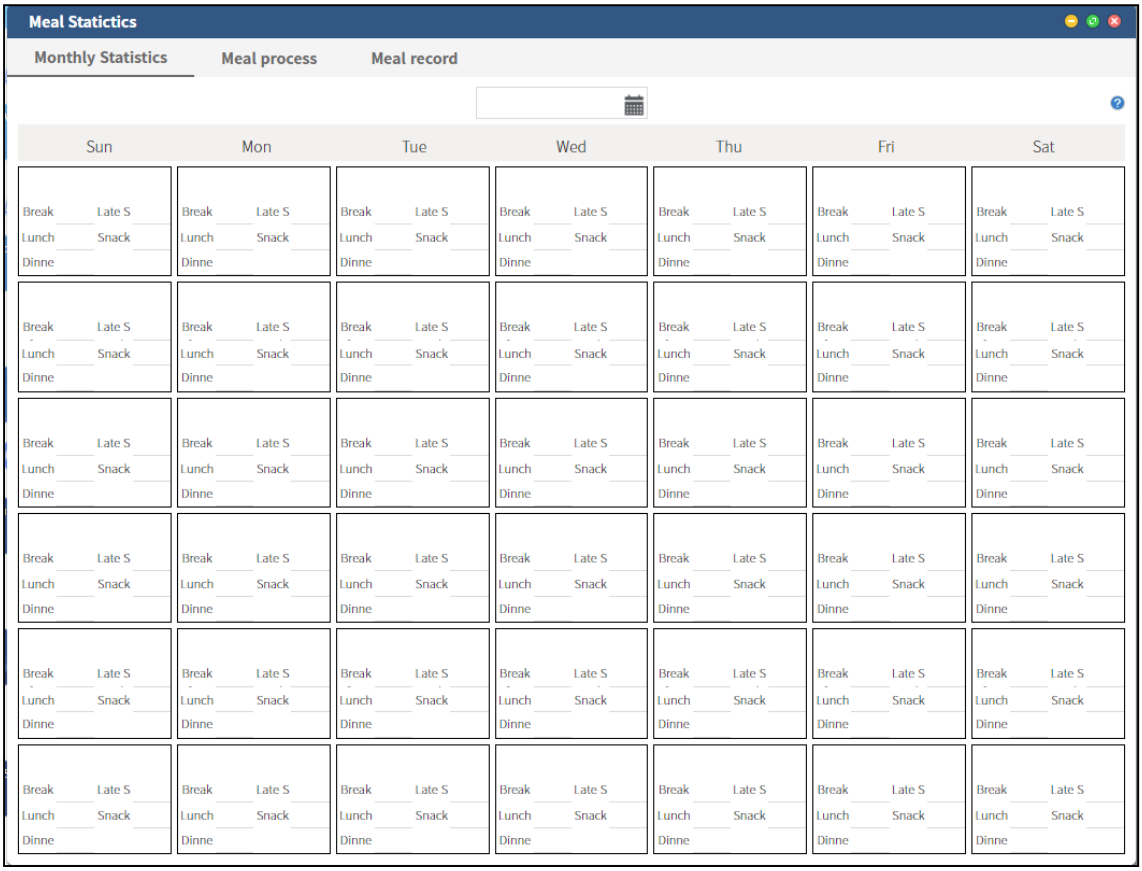
- **Select the user**: Check users to change meal code and move them to the selection list and then click [**Apply**].
- [**<**], [**<<**]: Move the users to 'Selection List'.
- [**>**], [**>>**]: Move back the users from 'Selection List'.

3) Meal Statistics

It searches monthly statistics, runs meal process and finds meal record.

- **Monthly Statistics:**

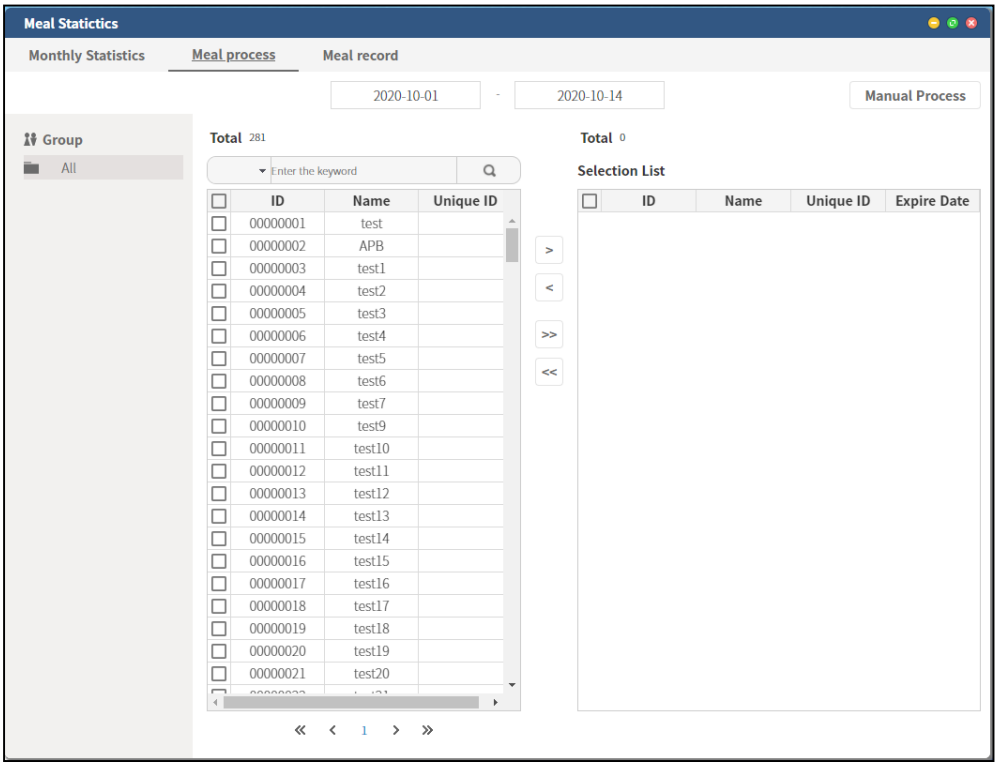
Show the total number of Meal usage by Meal data type per month. Select a month to view in the calendar, then the total number of meals for that month will be displayed.



- **Meal Process:**

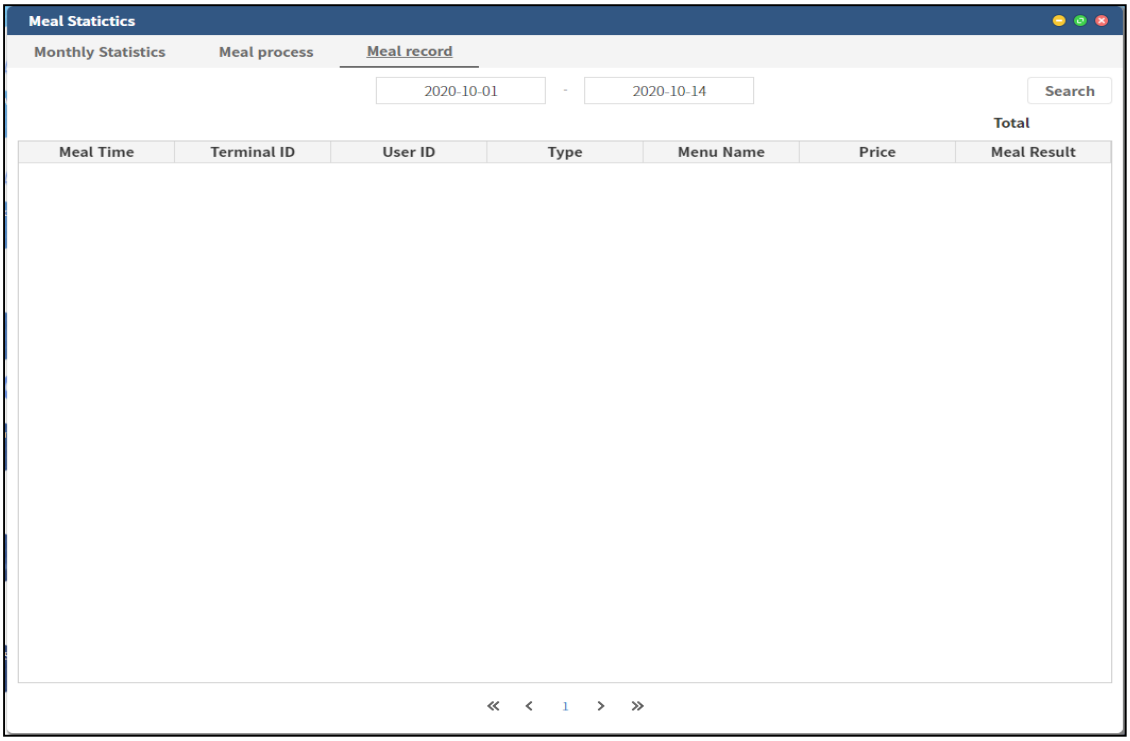
It collects the meal history for each user in the specified period.

It should be proceeded before having a result of statistics.



- **Manual Process**: When clicking this button, it processes the user's total meal statistics in the selection list.

- **Meal Record:** Show the total meal record for each user.

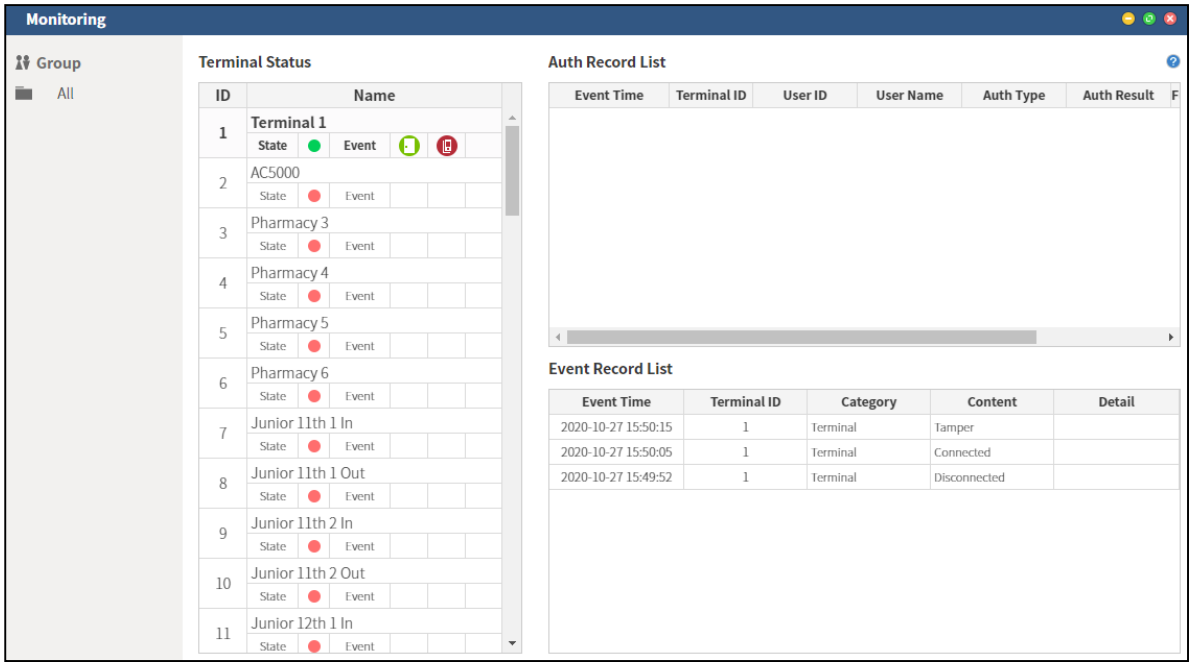


- **Search**: When clicking, it searches the total meal result for a specified period in the calendar.

14. Monitoring

1) Monitoring

It is the feature to check terminal status in real-time. You can check terminal connection status, real-time authentication log and event log in this page.



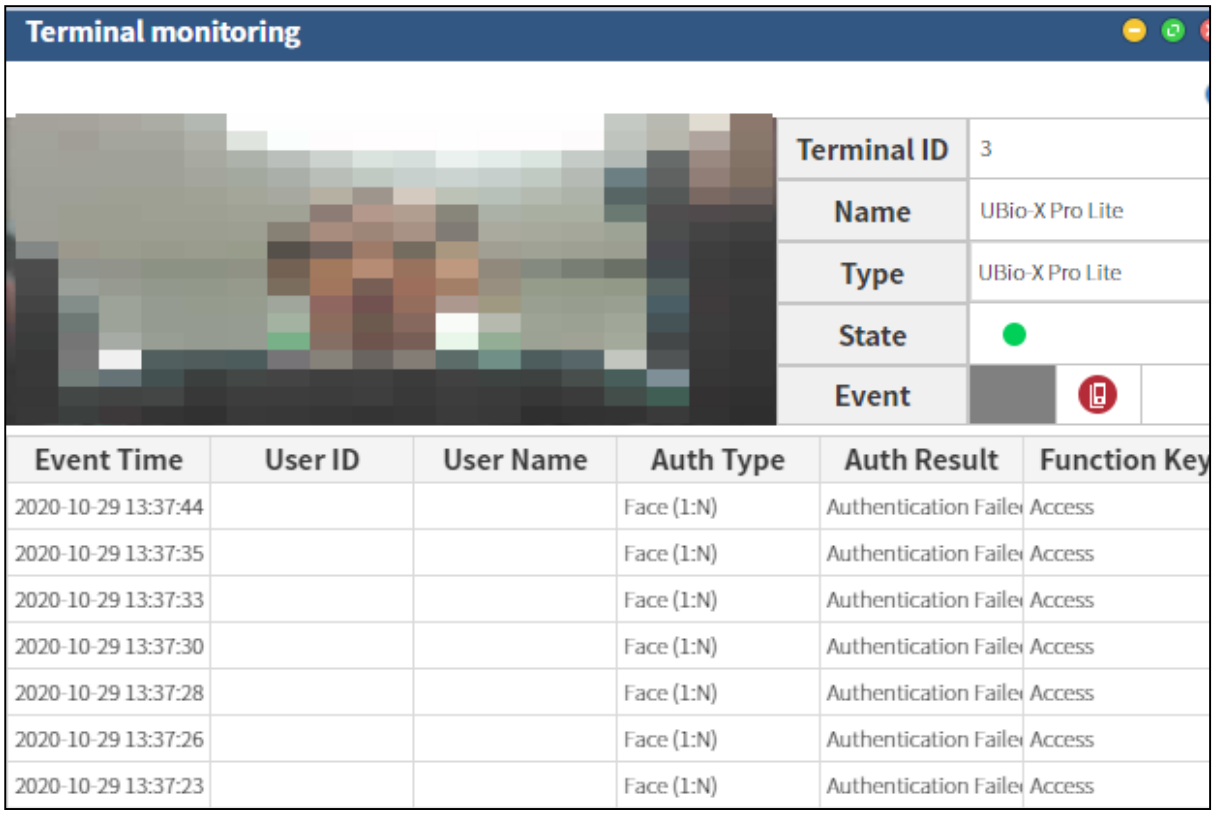
- **Group**: Show the registered group.
- **Terminal List**: Show registered terminals list.
- **Status**: Show terminal connection status.
    - : Terminal is connected to the server.
    - : Terminal is disconnected to the server.
- **Event**: Show the terminal event status.
    - : Door opened
    - : Door closed
    - : Door lock opened
    - : Door opened forcedly
    - : Door opened after close time
    - : Terminal disarmed

- : Terminal lock error
- : Fire alarm
- : Panic alarm

- **Auth Record List**: Show the authentication log in a real-time.
- **Event Record List**: Show the authentication log in a real-time.

2) Terminal Monitoring

It is the screen to monitor 1 of terminal you select in a real-time. You can check the terminal connection status, real-time authentication log and etc.



- **Terminal ID**: Display the ID of selected terminal.
- **Name**: Display the terminal name.
- **Type**: Display the terminal model name.
- **State**: Indicate the terminal connection status.
  - : Terminal is connected to the server.

- : Terminal is disconnected to the server.

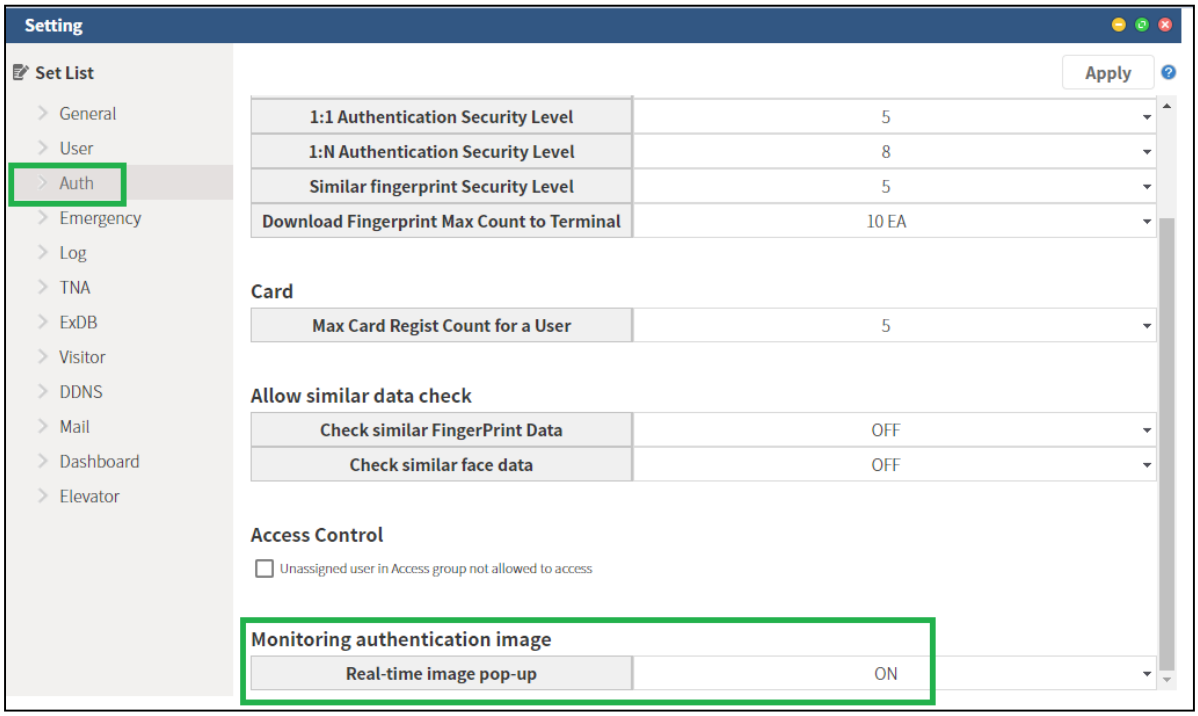
- **Event**: It indicates terminal event status.

  - : Door opened
  - : Door closed
  - : Door lock opened
  - : Door opened forcedly
  - : Door opened after close time
  - : Terminal disarmed
  - : Terminal lock error
  - : Fire alarm
  - : Panic alarm
  -

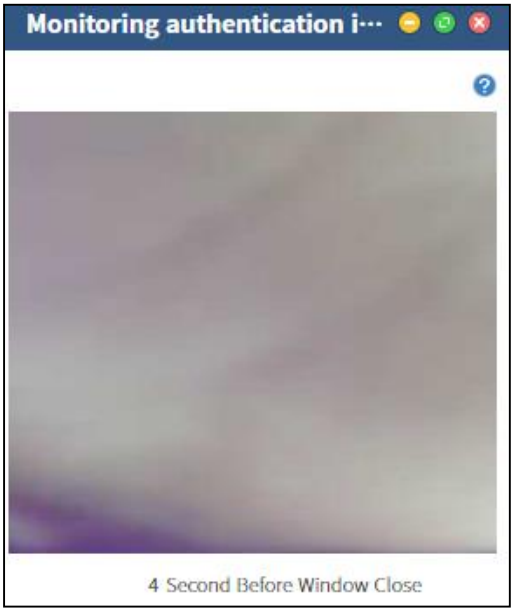
3) Monitoring Authentication Image

It shows the image taken when the user tries to authenticate from the terminal, which is used in the terminal equipped with the camera like AC7000, UBio-X Pro and etc.

To use this feature, check '**Real-time image pop-up'** is **ON'** in '**Auth'** from [**Setting**].

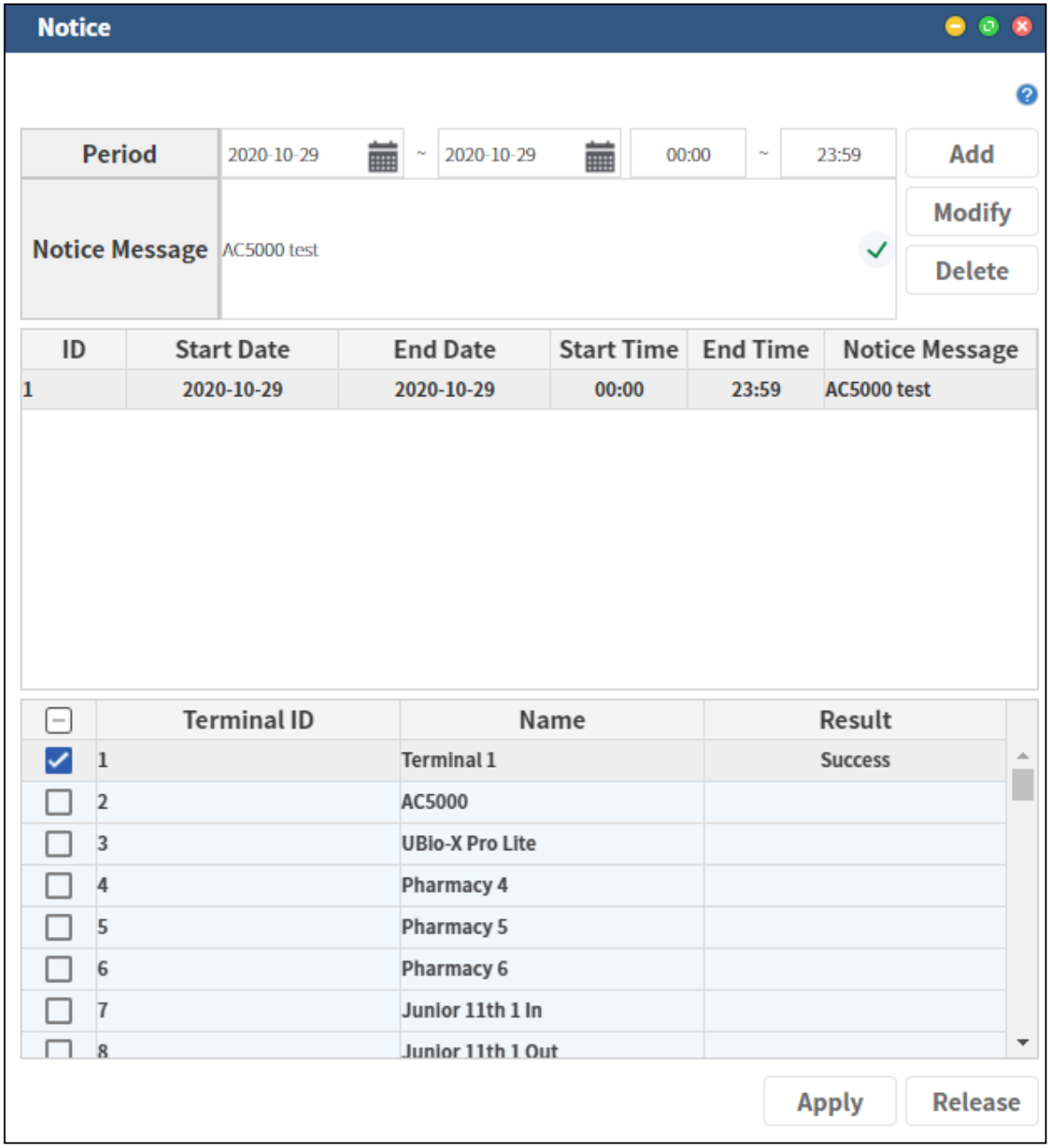


Then, when you authenticate with the selected authentication methods, it shows the pop-up window which is automatically closed in 5 seconds.



15. Notice

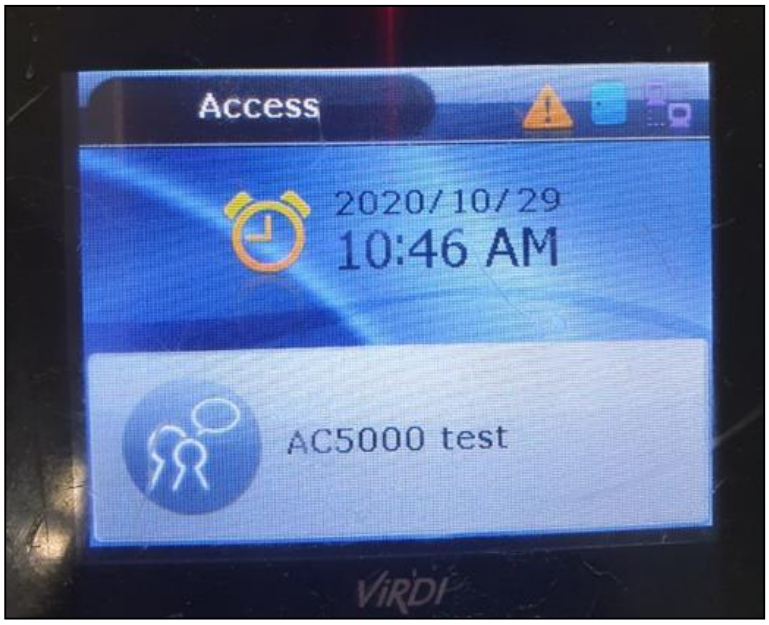
This feature is to send the notice message to the terminal via server, which is available only **AC5000**, **AC6000** and **AC7000**.



To use this feature, select the period and write the notice message and then select [**Add**].

After setting it, select the terminal in the terminal list and select [**Apply**] button.

Then, you can see the notice in the terminal as below.

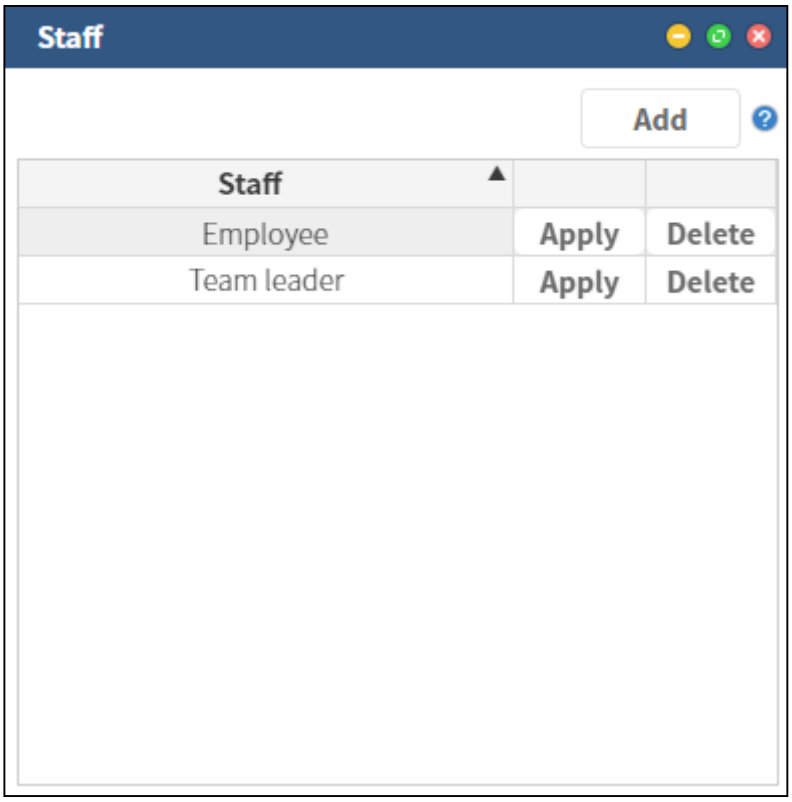


Additionally, below is the explanation for other buttons.

- **Period**: Set the period to display the notice.
- **Notice Message**: Write the notice message. It is available to write up to 64 characters.
- **Add**: Register the notice message.
- **Modify**: Update the registered message.
- **Delete**: Delete the registered message.
- **Apply**: Send the notice message to the selected terminal.
- **Release**: Remove the notice from terminal.

16. Position - Staff

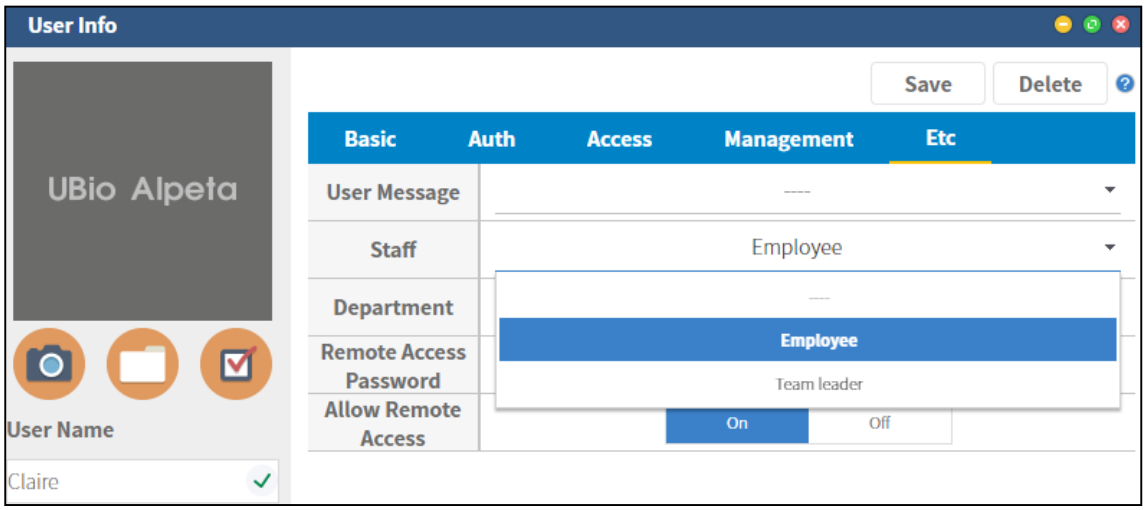
It is the feature to manage the position of staff to assign for users.



- **Add**: Add a new position.
- **Apply**: Input the name of position and click [**Apply**] button to save position name.
- **Delete**: Remove the selected staff position.

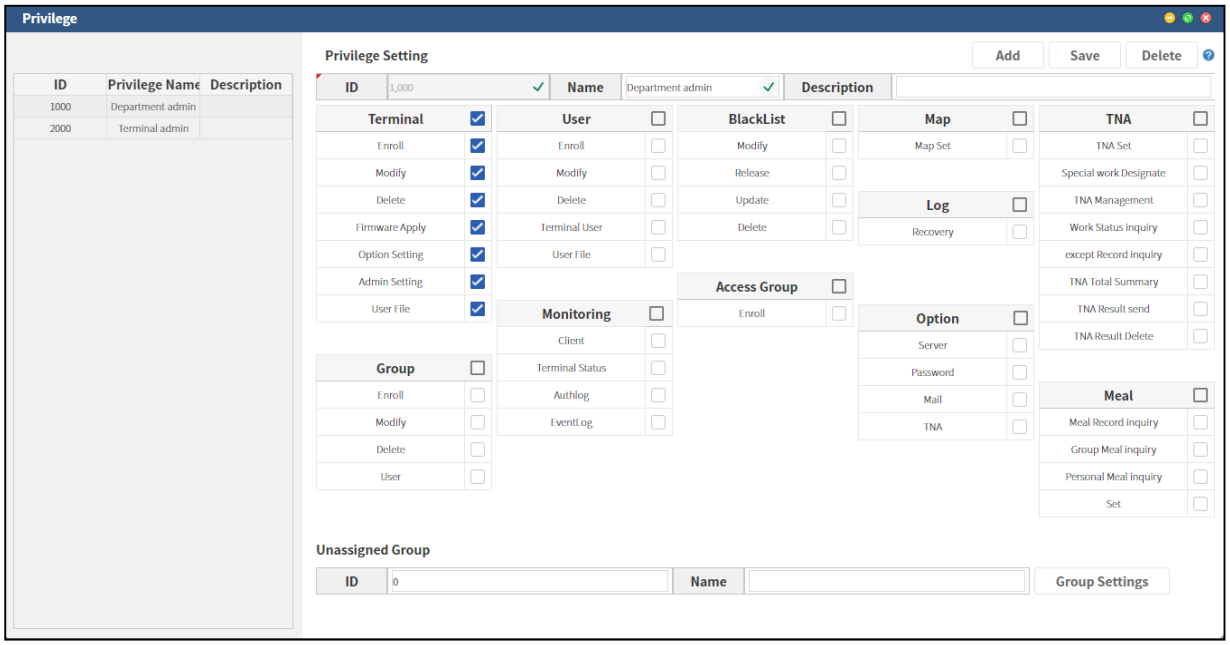
To modify the name of position, click the name and write it as you want and then select [**Apply**] button.

After setting them, you can use the positon of staff in [**Department**] section from '**User Info**' as below.



17. Privilege

It is the feature to create the privilege and assign in to a specific admin to limit some authorities. This is only used and managed by Master admin.

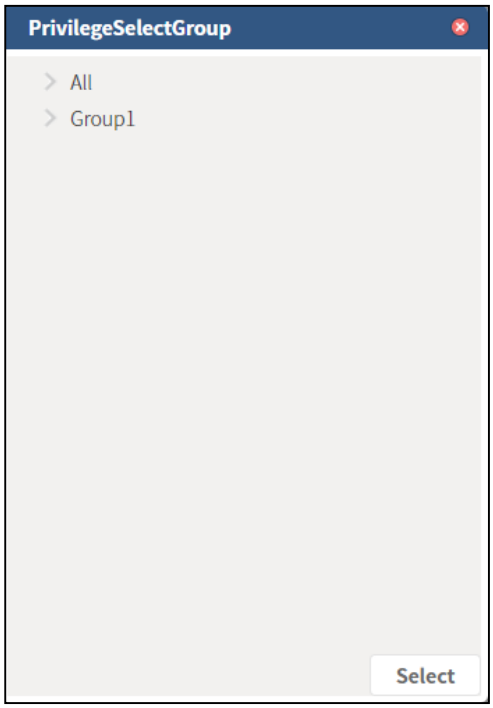


Enter the **ID** (1,000 ~ 9,999), **Name** (Mandatory) and **Description** (Selectable) and select [**Add**] button.

To modify the registered privilege, select it in the left side, modify what you want and select [**Save**] button.

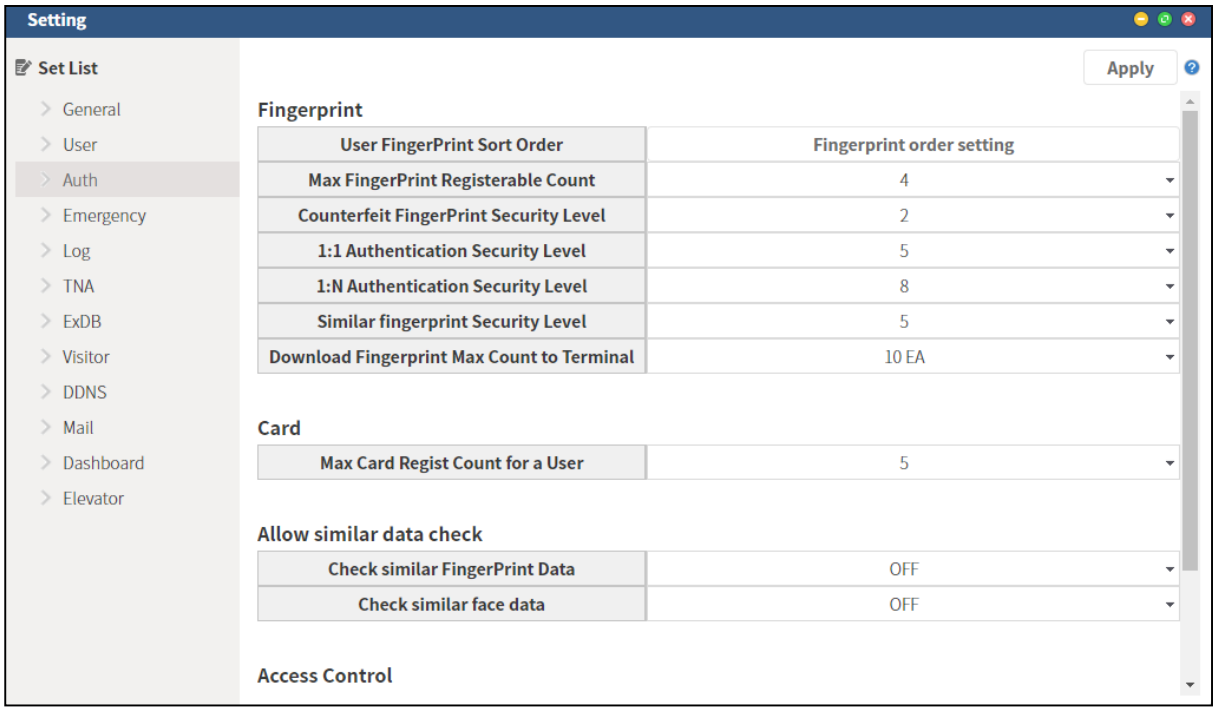
If you want to delete the registered privilege, select the code in the left side and select [**Delete**] button.

- **Group to apply the privilege**: It can apply the privilege to the users and terminal included in the group. Only one privilege can be set in one group and the sub group can be set same.


PrivilegeSelectGroup
All
Group1
Select

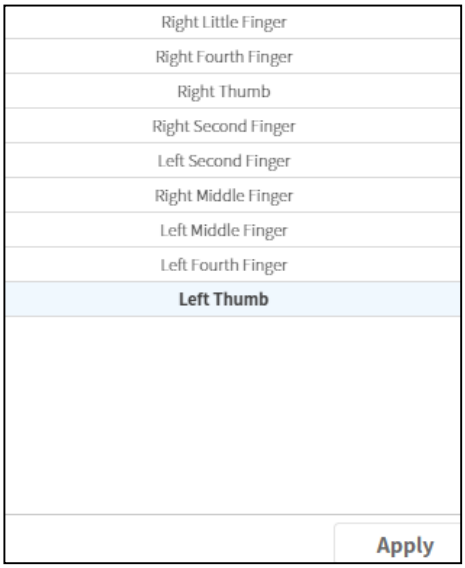
18. Setting

1) Authentication



- **Fingerprint**

  - **Set the priority of user's fingerprint when sending to the terminal**: Set the priority of user's fingerprint when sending it to the terminal. When you select 'Fingerprint order setting' you can drag the priority of fingerprint by using the mouse. After setting them, click [**Apply**] button.



  - **The available registered count of max fingerprint**: Set the maximum number of fingerprint to register. (1 ~ 10)

  - **Counterfeit fingerprint security level**: Set counterfeit fingerprint check level. (0 ~ 9)

- **1:1 Authentication level**: Set 1:1 Authentication level. (1 ~ 9)
- **1:N Authentication level**: Set 1:N Authentication level. (1 ~ 9)
- **Similar fingerprint security Level**: Set the similar fingerprint security level. (1 ~ 9)
- **The max count of fingerprints for each user to send the terminal:** Set the max count of fingerprints for each user to send the terminal. It can set the count from 1ea to 10ea.

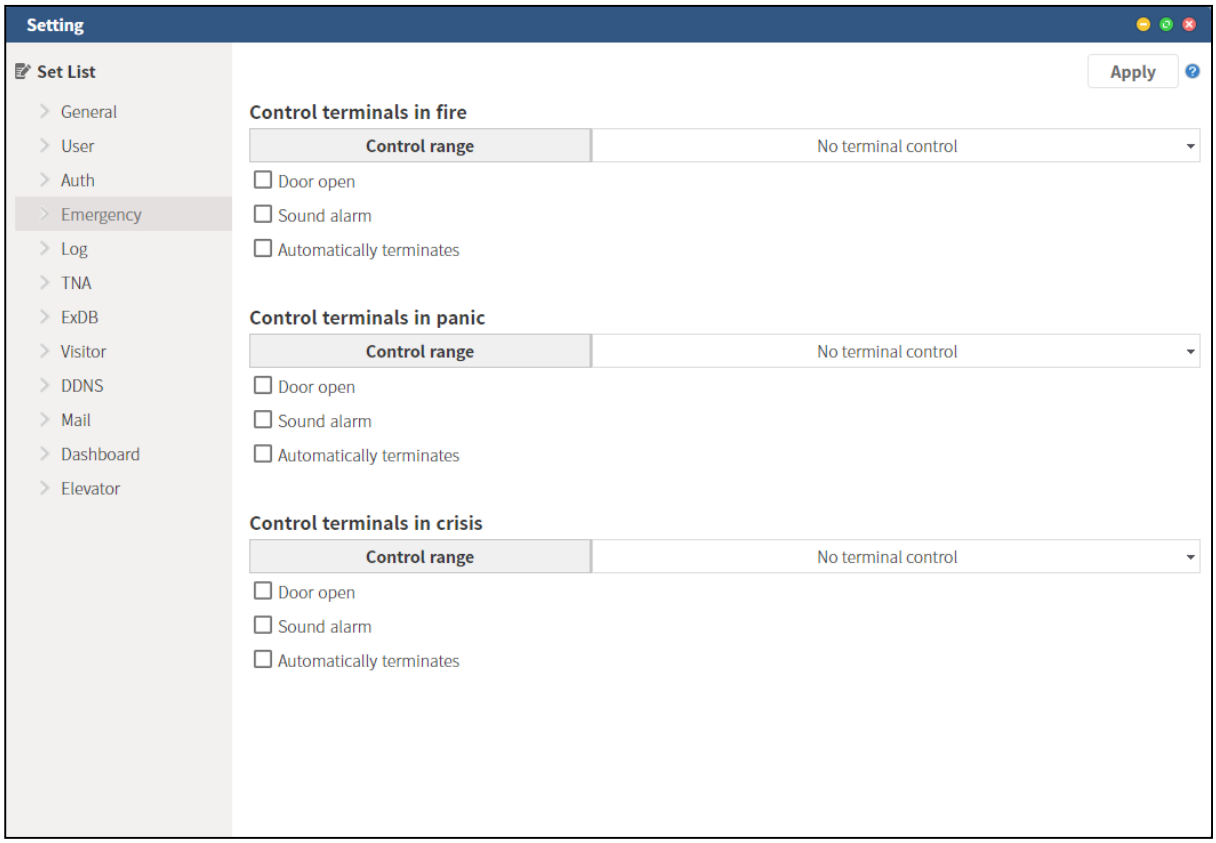
- **Card**
  - **The available registered count of max card**: Set the maximum number of card for each user. (1 ~ 5)

- **Check the similar data**
  - **Check the similar fingerprint data:** Check the similar fingerprint data and verify the duplicated data
  - **Check the similar face data:** Check the similar face data and verify the duplicated data.

- **Access Control**
  - **Unassigned user in Access group not allowed to access**: Set that the unassigned user in Access group is not allowed to access.

- **Monitoring authentication image**
  - **Real Time image pop-up:** Show the user's image when authenticating in a pop-up window. This feature is used only in the terminal equipped with the camera and automatically closed after 5 seconds.

2) Emergency



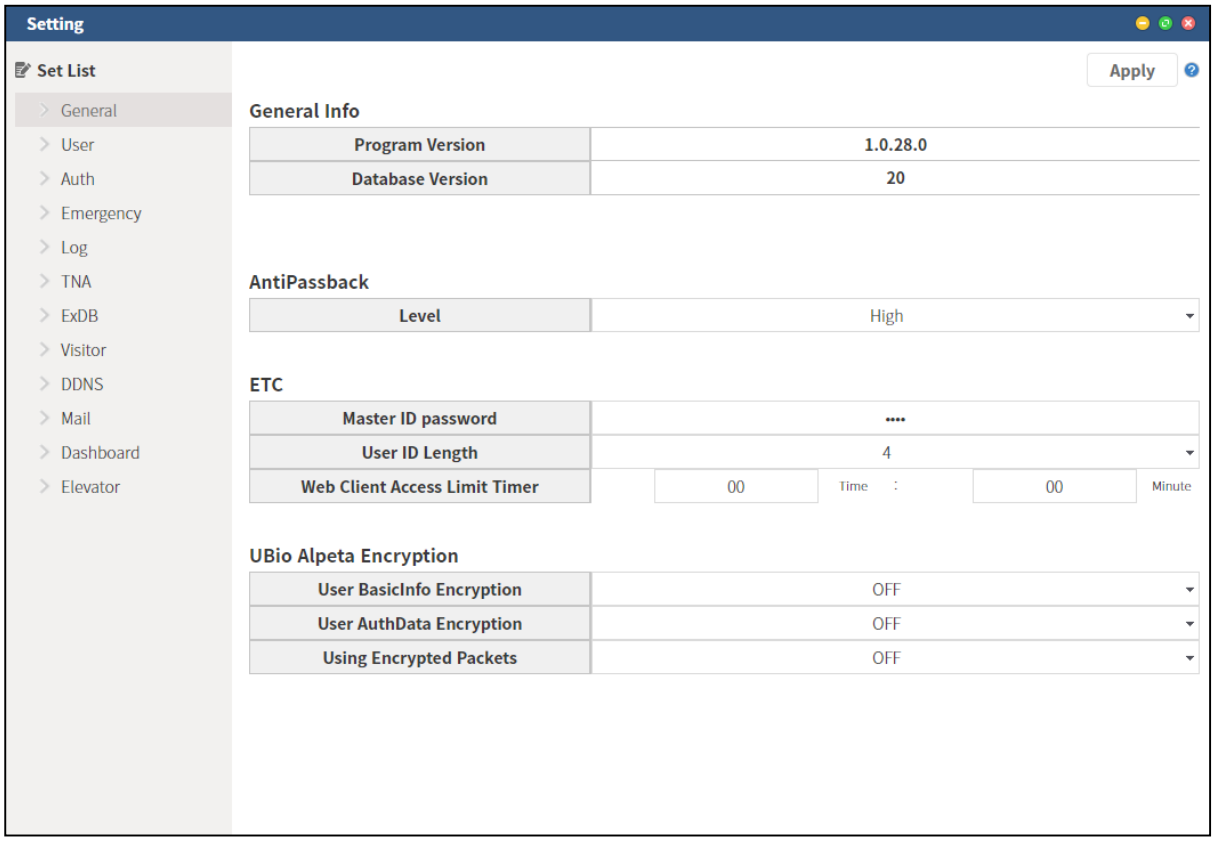
- **Control terminals in fire**
  - **Control range**: Select one among 'No terminal to control', 'Group terminal control', and All terminal controls.
  - **Door open**: Open doors when there is fire situation.
  - **Sound alarm**: The alarm sounds when there is fire situation.
  - **Automatically closed**: When the fire situation is finished, the control is automatically closed.

- **Control terminals in panic**
  - **Control range**: Select one among 'No terminal to control', 'Group terminal control', and All terminal controls.
  - **Door open**: Open doors when there is panic situation.
  - **Sound alarm**: The alarm sounds when there is fire situation.
  - **Automatically closed**: When the panic situation is finished, the control is automatically closed.

- **Control terminals in crisis**

  - **Control range**: Select one among 'No terminal to control', 'Group terminal control', and All terminal controls.
  - **Door open**: Open doors when there is emergency situation.
  - **Sound alarm**: The alarm sounds when there is crisis situation.
  - **Automatically closed**: When the crisis situation is finished, the control is automatically closed.

3) General



- **General Info**

  - **Program Version**: Show the program version information.
  - **Database Version**: Show the database version.

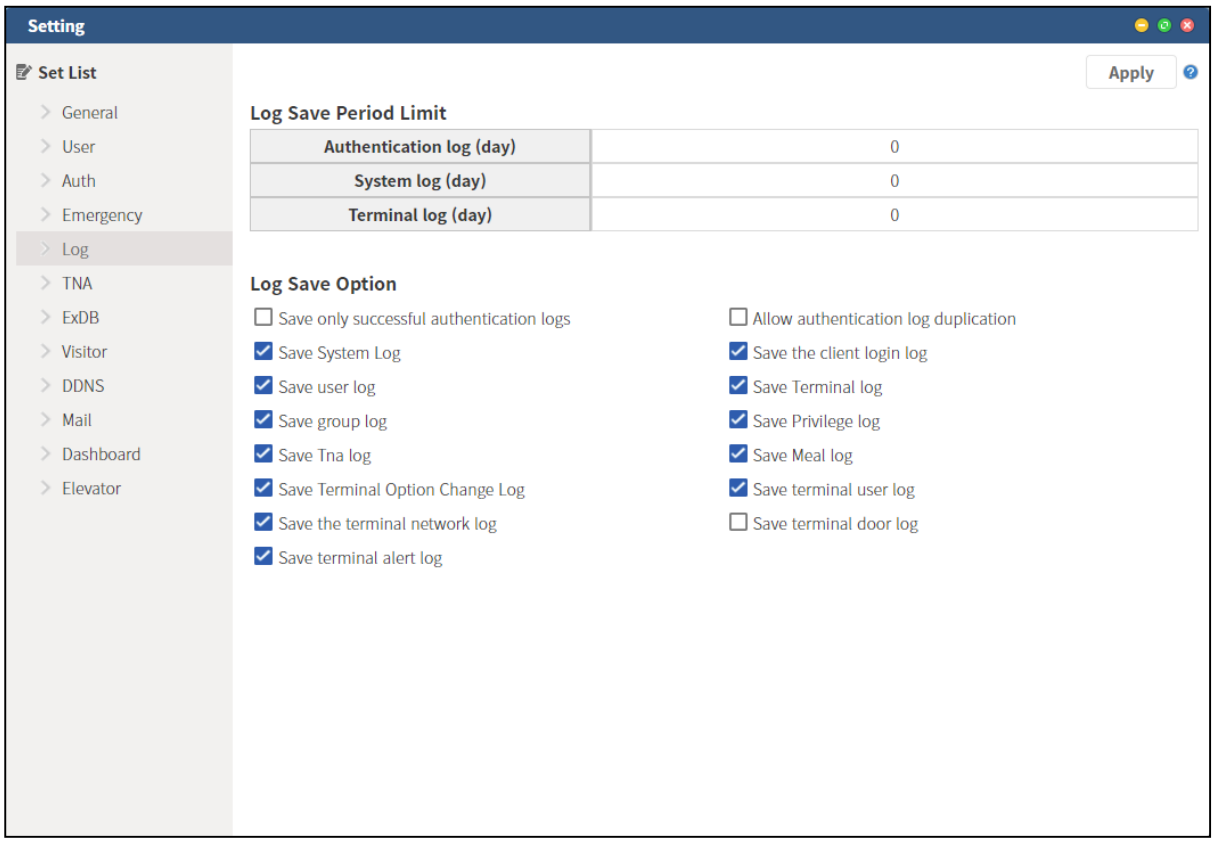
- **AntiPassback**

  - **Level**: Set the level of anti-passback. (Low/High)

- **ETC.**
  - **Master ID password**: Set the password of master admin.
  - **User ID length**: You can set user ID length. (1 ~ 8)
  - **Web client access limit timer:** Set Limit time for web client access.

- **UBio Alpeta Encryption**
  - **Encrypt user's basic information**: Encrypt the User basic information.
  - **Encrypt user's authentication data**: Encrypt the user's authentication data.
  - **Use the encrypted data:** Encrypt the packet data.

4) Log

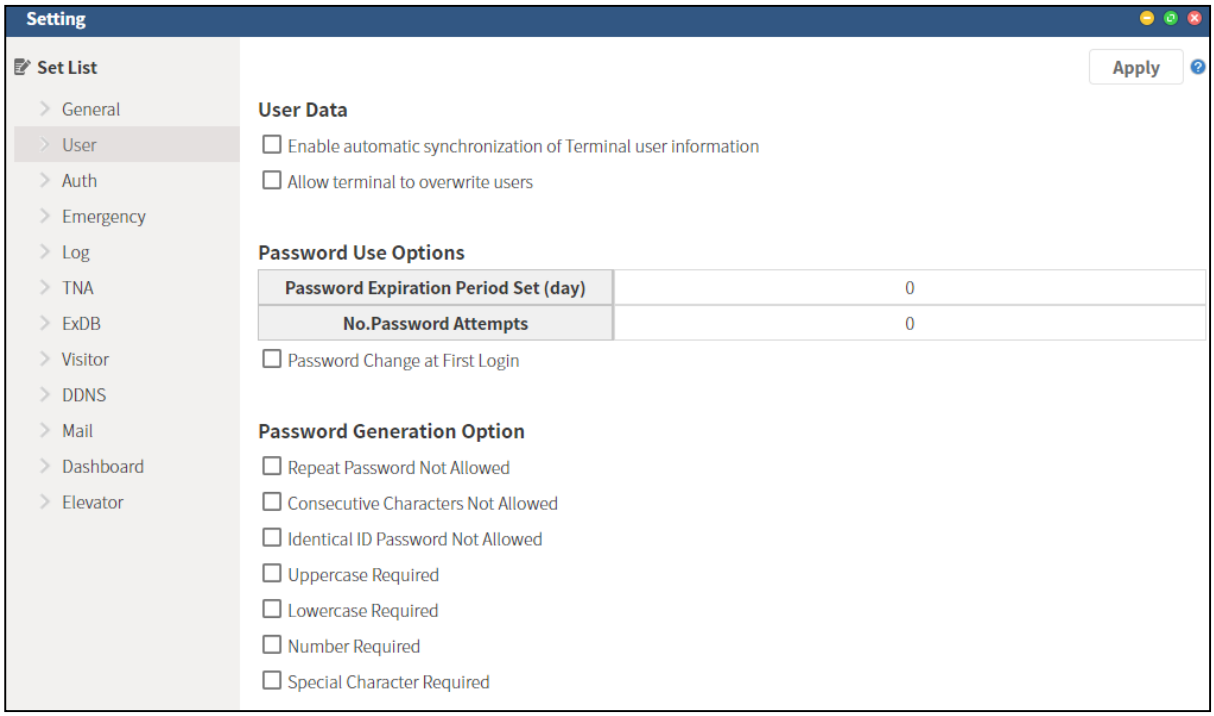


- **Set the log saving period**
  - **Authentication log (day)**: Set the period to save the authentication log. (0=Unlimited)
  - **System log (day)**: Set the period to save the system log. (0=Unlimited)
  - **Terminal log (day)**: Set the period to save the system log. (0=Unlimited)

ex) If you set 300 days, you can delete the records older than 300 days

- **Log Saving Option**
  - **Save only successful authentication log**: Save only 'Success' in the authentication logs.
  - **Allow the duplicated authentication log**: Check the duplicated authentication before saving the log.
  - **Save the system log**: Save the system log.
  - **Save the client log-in log**: Save the log-in log of client in DB.
  - **Save the user log**: Save the user log in the server.
  - **Save the terminal log**: Save the terminal log in the server.
  - **Save the group log**: Save the group log.
  - **Save the privilege log**: Save the privilege log.
  - **Save TNA log**: Save the TNA log.
  - **Save Meal log**: Save the meal log.
  - **Save the terminal's option change log**: Save the terminal's option change log.
  - **Save the terminal user log**: Save the terminal user log.
  - **Save the terminal network log**: Save the terminal network log.
  - **Save the terminal door log**: Save the terminal log.
  - **Save the terminal alert log**: Save the terminal alert log.

5) User

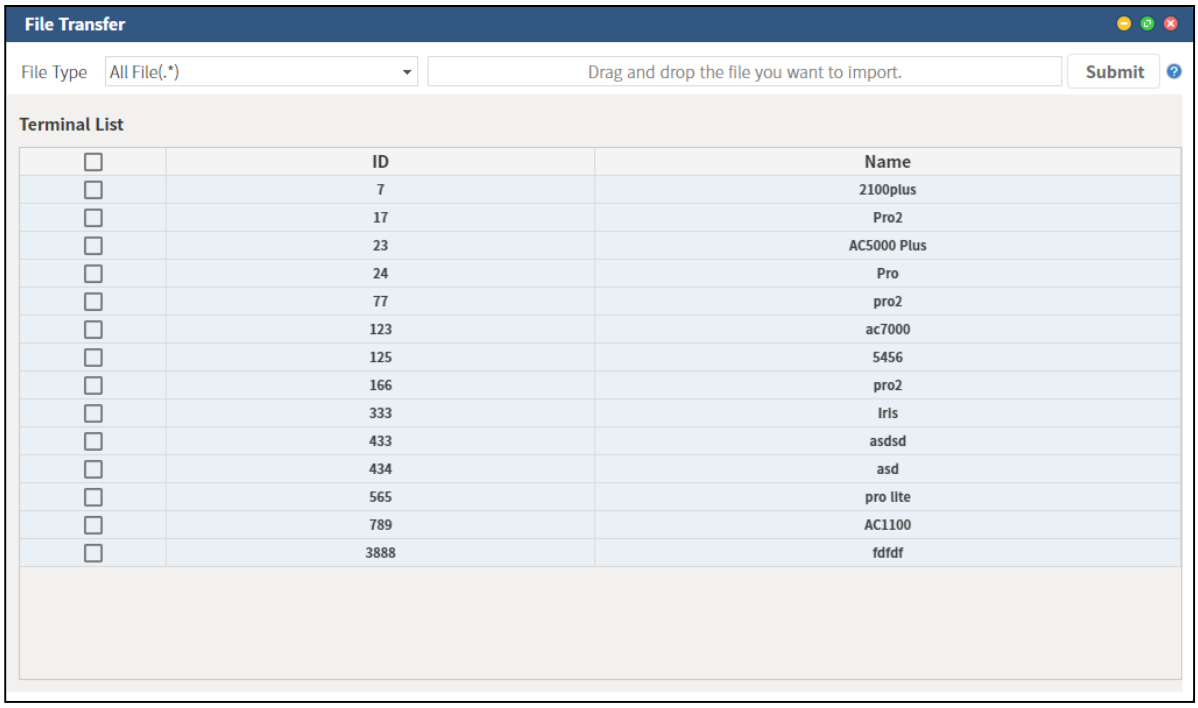


- **User data**
  - **Enable automatic synchronization of terminal user information**: It enables the feature to automatically transmit to the terminal when modifying user information in the server. When the user information is added or modified, the feature is activated to automatically synchronize to the terminal. In this case, the synchronization is possible only when the user and the terminal are set to the same access group. However, if the administrator directly transfers the user from Alpeta to the terminal after adding the terminal user from **[Terminal User]** in Alpeta, it is synchronized to the terminal even if they are not the same access group.
  - **Overwrite the duplicated user when uploading terminal users**: When importing user information from the terminal, select whether to overwrite if there are duplicated users.
- **Password use options**
  - **Set the password expiration period (Day)**: Set the expiration date based on the password creation date. (0=Unlimited)
  - **Allowed number of log-in failure:** Set the allowed number of login when the admin fails to log in. (0=Unlimited)
  - **Change the password in 1st log-in**: Change the password when the user log in at the first time.
- **Option to create the password**
  - **Old password not available:** Not available to use the old password that the user has used before.

- **Consecutive characters not available:** Not available to use the consecutive characters. (ex. aa, AA, BB...)
- **The same password as ID not available:** Not available to use the same password with the user ID.
- **English upper case required:** At least, one capital letter is mandatory. (ex. aaaA1234)
- **English lower case required:** At least, one small letter is mandatory. (ex.bA1234)
- **Number required:** At least, one number is mandatory. (ex.a0bC)
- **Special character required:** At least, one Special Characters is mandatory such as ({ } [ ] / ? . , ; : | ☐) * ~ ` ! ^ - _ + < > @ ☐ # $ % & = (' ").

19. File Transfer

It is the feature to send the file to the terminal.



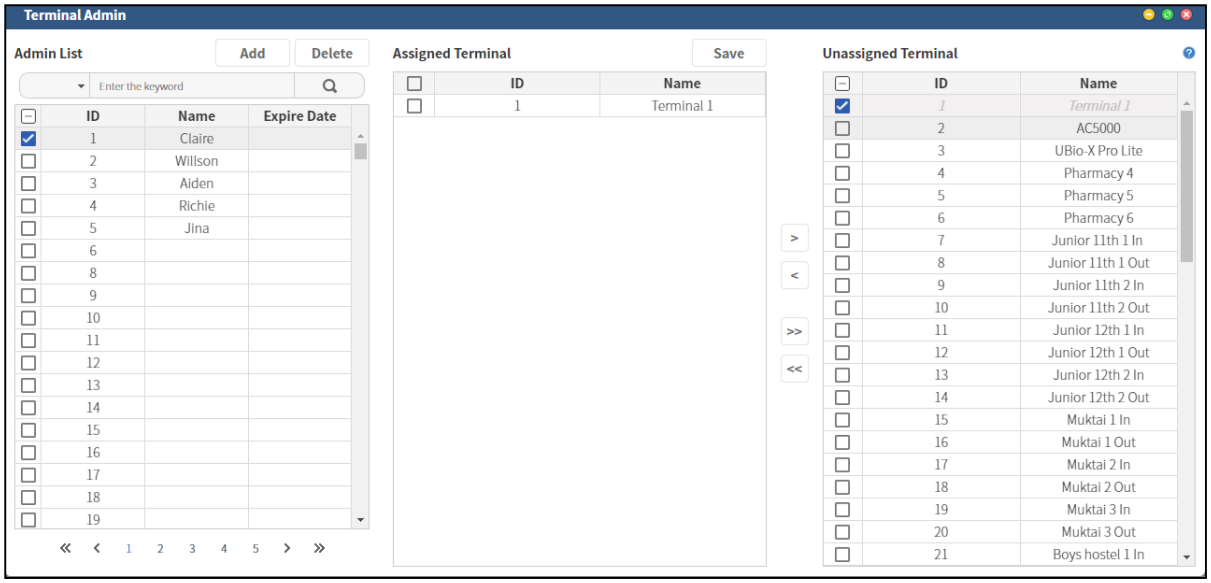
- **File Type**: Set the file type to send to terminal. 'Defined text file', 'Background image file', 'Success voice file', 'Fail voice file' and 'Movie file' can be sent to the terminal.
- **Drag and drop the file you want to import.**: Drag and drop a file to send or click to select a file.
- **Terminal list**: Show the terminal list registered on the server. You can select the terminal to send file.
- **Send:** Send the file to the marked terminal in the list.

20. Terminal

1) Terminal Admin

It is the screen to manage the terminal admin.

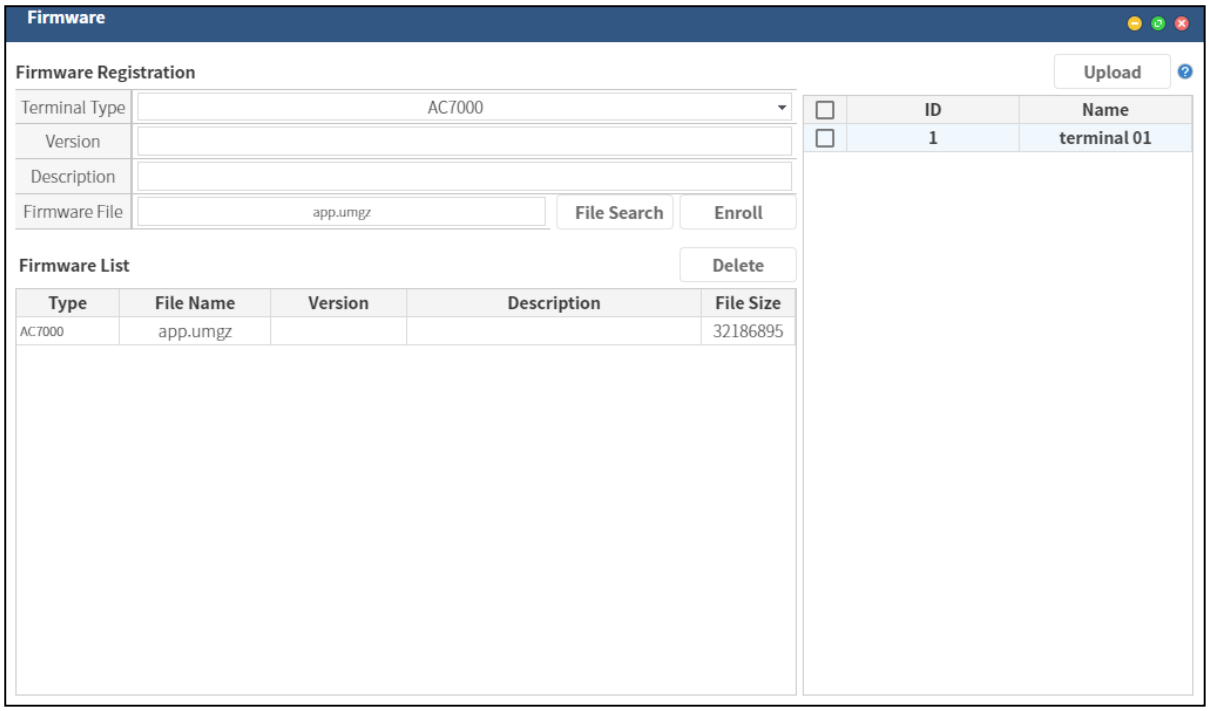
You can add or delete the terminal admin user. Also, you can add or delete the terminal managed by the terminal admin.



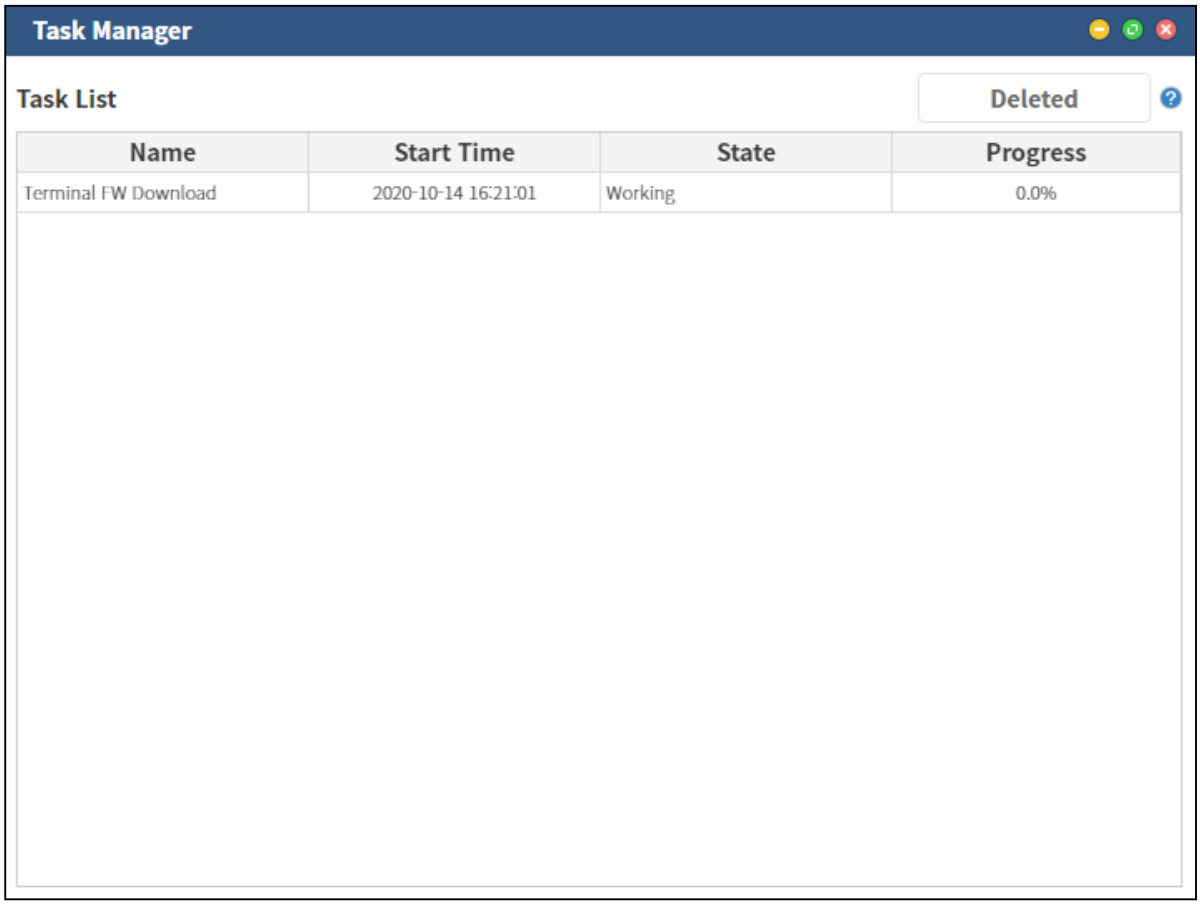
- **Admin list**: The user list registered as the terminal admin
- **Add**: Add a user in the terminal admin. When you click it, the pop-up window to select the user is shown. Select users on the screen and click **[Apply]** button to move users to the terminal admin.
- **Delete:** Remove the selected users in the terminal admin list.
- **Assigned terminal:** When selecting the user in the terminal admin list, it shows the terminal list managed by the terminal admin.
- **Unassigned terminal:** Show all the terminals registered on the server.
- **[>], [>>]:** Move the terminal from [**Unassigned terminal**] to [**Assigned terminal**].
- **[<], [<<]:** Move the terminal from [**Assigned terminal**] to [**Unassigned terminal**].
- **Save:** Click this button to apply this setting.

2) Firmware

It is the screen to manage the terminal firmware.

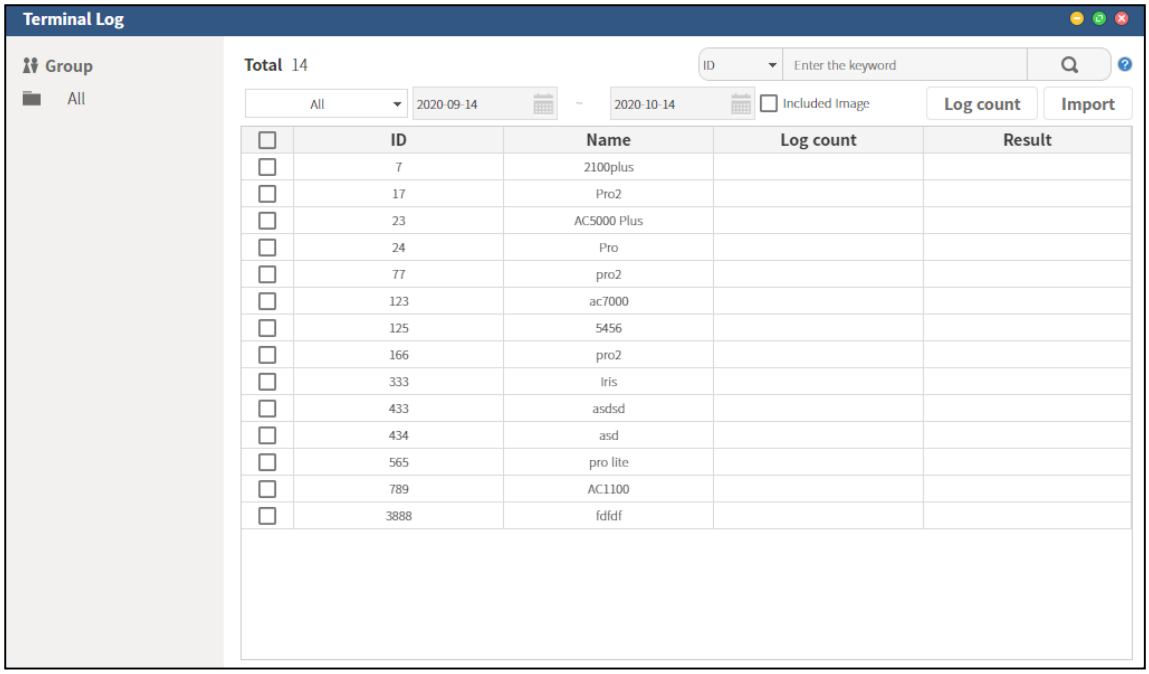


- **Register the FW:** Register the terminal firmware to the server. The registered firmware in server is used for sending to terminal.
- **Terminal type:** Select the terminal type (model). (ex. AC7000, UBio-X Pro2..)
- **Version:** Enter the firmware version information. You can enter up to 100 characters.
- **Description:** Enter the firmware description. You can enter up to 255 characters.
- **Firmware file:** Select the firmware file from user's PC.
- **Register:** Register the firmware file on the server.
- **Firmware list:** Show the firmware list registered on the server.
- **Type:** Show the terminal type (model).
- **File name:** Show the firmware file name.
- **Version:** Show the version of firmware.
- **Description:** Show the description of firmware.
- **File size:** Show the size of firmware file.
- **Send:** Send the firmware to the selected terminal. You can check the download progress in [**Task Manager**] as below.



3) Terminal Log

It is the screen to manage the terminal log. You can check the log count saved in the terminal and import them from the terminal to server.



-

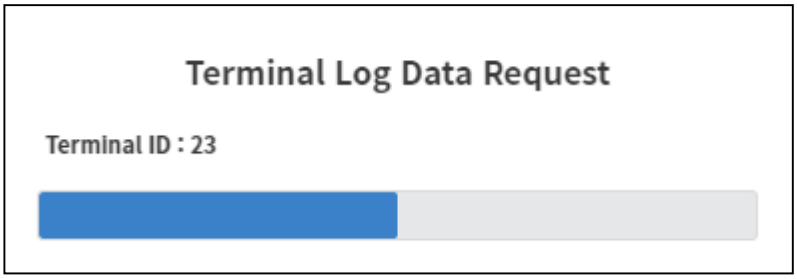
: You can set the option to import.

  All: Get all logs from terminal.

  Not Uploaded: Get the log that is not imported from terminal.

  Period setting: Get the log in the period that you set.

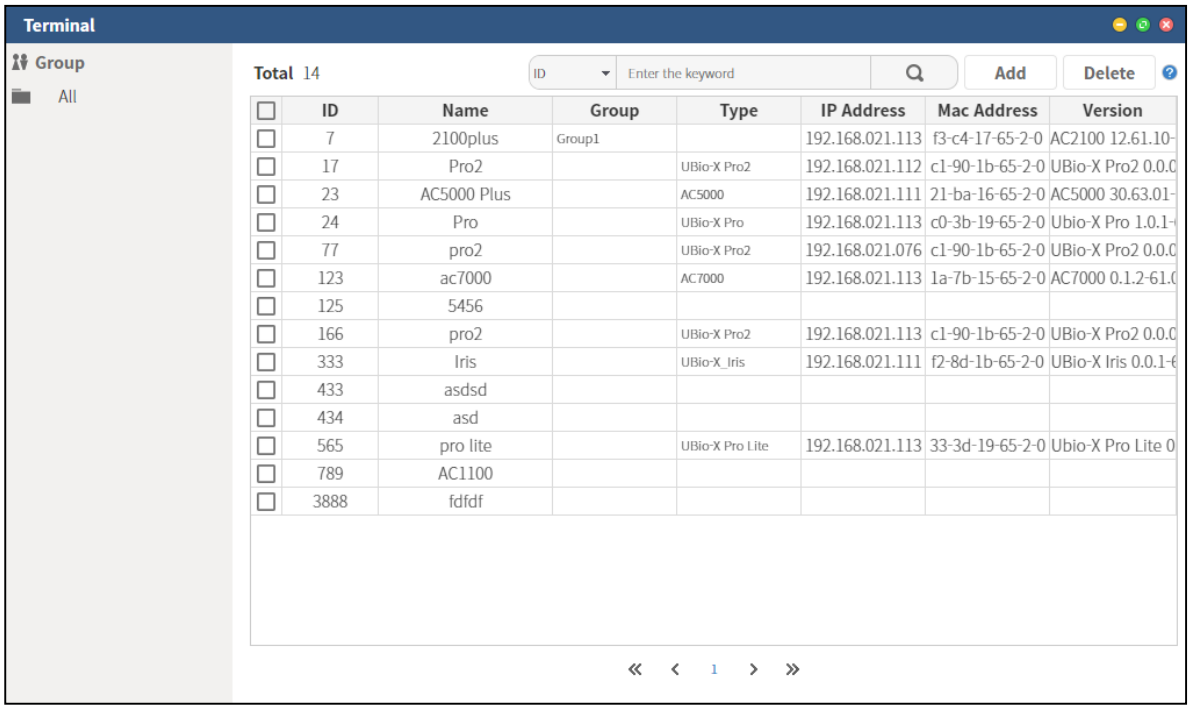
- **Include the image**: Select whether to get the log image together.
- **Log count**: Show the log count of the selected terminal.
- **Import**: Upload the log saved in the terminal to the server. When selecting this button, you can see the progress as below.

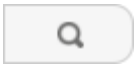


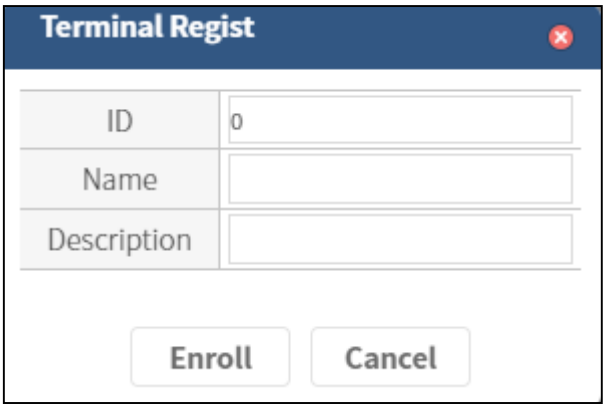
4) Terminal management

It is screen to manage the terminals.

You can search, add and delete the terminal in the terminal list registered in server. Also, you can see the pop-up window of terminal information when double-clicking the terminal in the list.



- **Group:** Show the group list registered on the server. When you click a group, only the terminal included in the group is shown.
- **Total:** Show all the terminals searched.
-  : Set the search condition and select this button. The terminals are displayed at 20 per page.
- **Add:** Terminal Registration page is displayed.



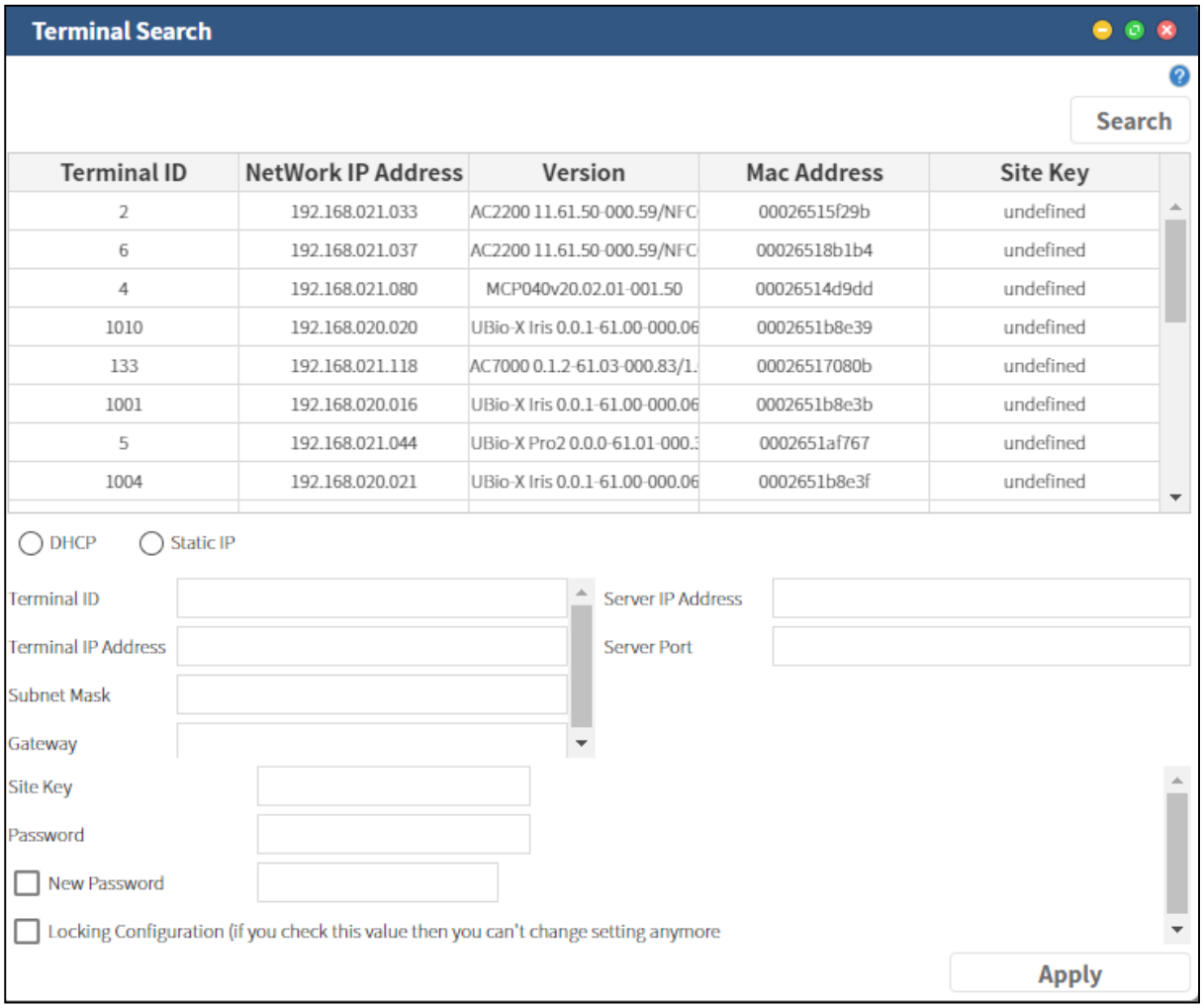
- **ID:** Enter the terminal ID. You can set terminal ID between 1~2000.
- **Name:** Enter the terminal name. Maximum 50 characters can be used for the terminal name.

- **Description:** Set the terminal description. Maximum 255 characters can be used for the description.

5) Terminal Search

It is the feature to find the terminal in the network via UDP communication.

You can search the terminal to connect and change the network setting.



- **Search:** Search the terminal to connect in the network by using UDP communication.

- **DHCP / Static IP:** Check if the selected terminal is DHCP or Static IP and change as you want. (When you select DHCP, terminal IP, subnet mask and gateway is not available to modify.)

- **Terminal ID:** Check the terminal ID and change it.

- **Terminal IP Address:** Check the terminal IP and change it.

- **Subnet Mask:** Check the terminal subnet mask and change it.
- **Gateway:** Check the terminal gateway and change it.
- **Server IP Address:** Check the server IP address of terminal and change it.
- **Server Port:** Check the server port of terminal and change it.
- **Site Key:** Check the site key of terminal and change it.
- **Password:** Necessary to enter the password to change the terminal setting.

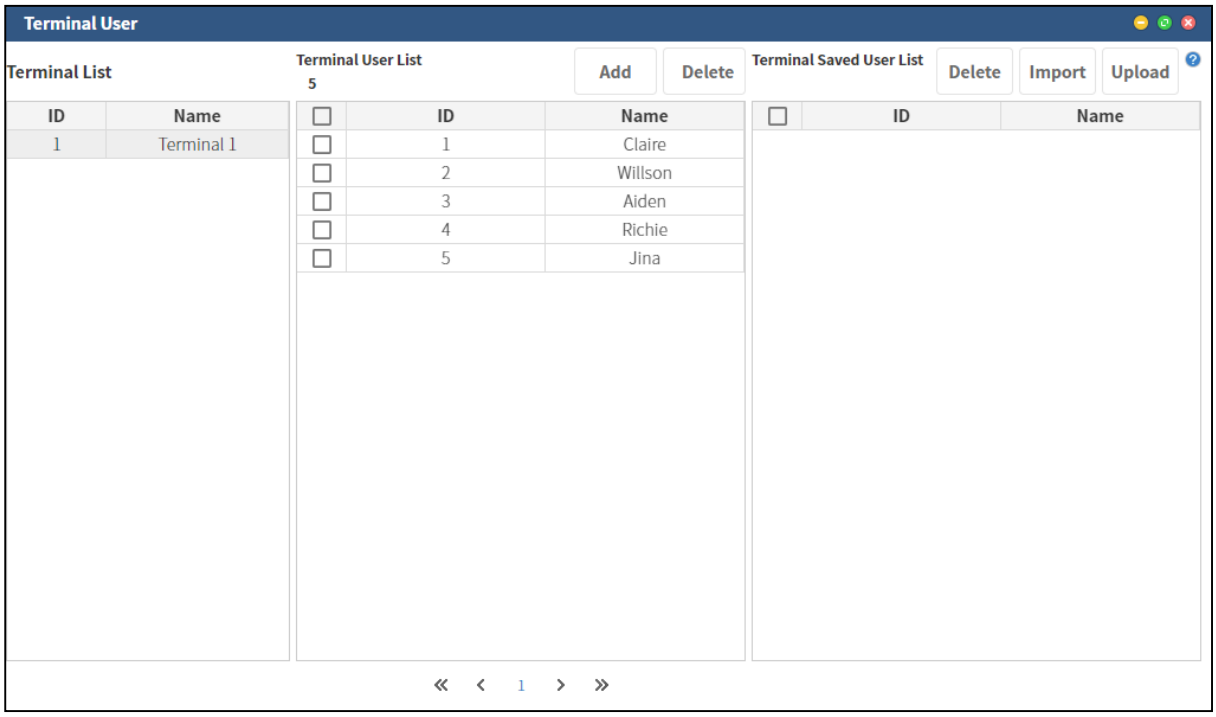
  (Not available to change the terminal setting if not entered. The default password is 0842650)
- **New Password:** Change the current password to new one.
- **Lock the setting (If you check this, not available to change the setting anymore):** Lock the setting change via UDP communication.
- **Apply:** Save the change.

6) Terminal User Management

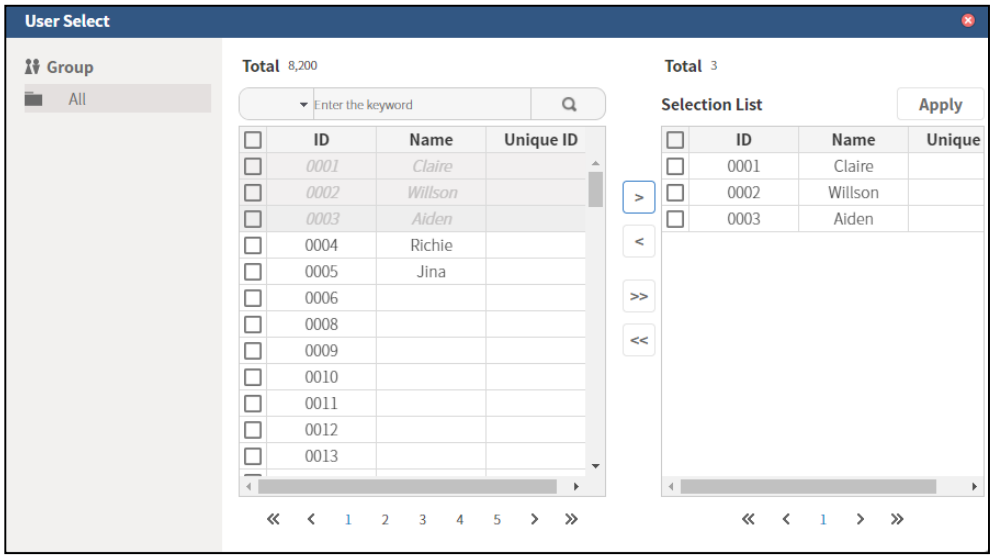
It is the feature to send the users from server to terminal or from terminal to server.

'**(Server -> Terminal) User list**' can send the users from server to terminal and add / delete them.

'**(Terminal -> Server) User list**' can import the users from terminal and upload them to server.



- **(Server -> Terminal) User list**
  - **Add**: Add the users to send them saved in Alpeta to the terminal. When clicking it, the pop-up window to add the users is shown and they are sent to the terminal at the same time.



Check the users and move them to '**Selection List**' and then click [**Apply**] button.

  - **Delete**: Delete the users who were sent to terminal. When clicking it, the users are deleted only in terminal, not server.

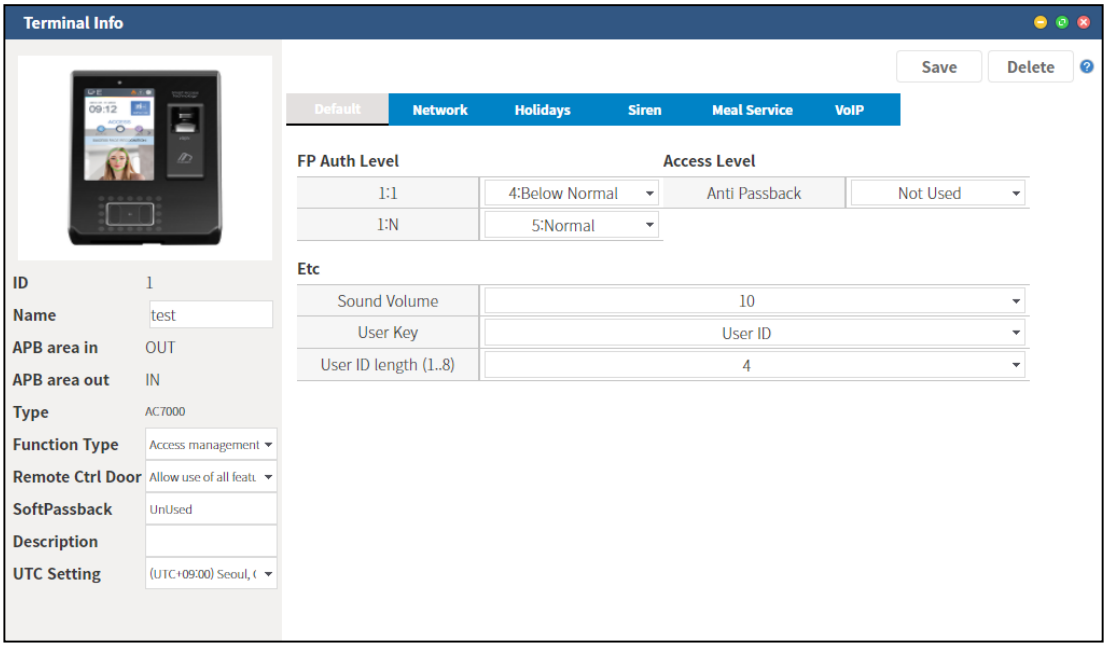
- **(Terminal -> Server) User list**
  - **Delete**: Delete the users in server.
  - **Import**: Import the users from terminal.

- **Upload**: Upload the users imported from terminal to the server.

7) Terminal Info

It is the feature to check the detailed information of terminal registered on the server.

You can modify or delete the terminal information.

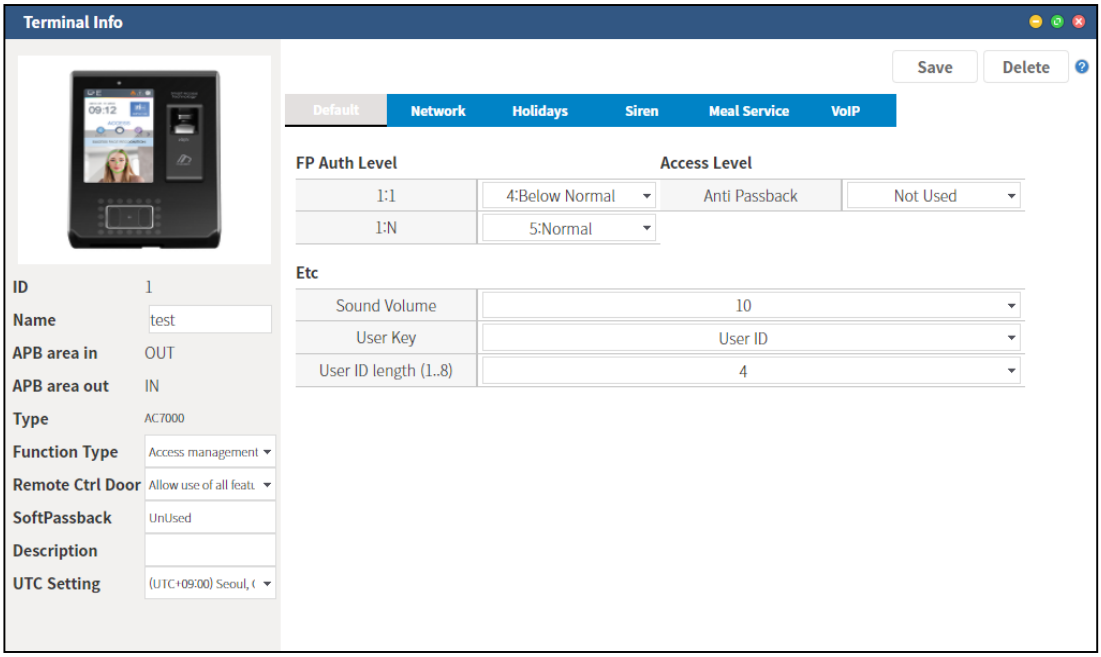


To connect the terminal to Alpeta, it should set the terminal port as 9003.

- **ID:** Display the terminal ID.
- **Name:** Enter or modify the terminal name. It can enter up to 100 characters.
- **APB area in, APB area out:** Display the Anti-Passback information.
- **Type**: Display the terminal model name connected.
- **SoftPassback:** Set Soft-Passback function. It is activated only when the terminal is set for anti-passback. Even if the user is restricted with passback, it can successfully authenticate in terminal or server. To do this option, it should activate this option in 'Anti-Passback management'.
- **Description:** Make a note for this terminal.

① Default

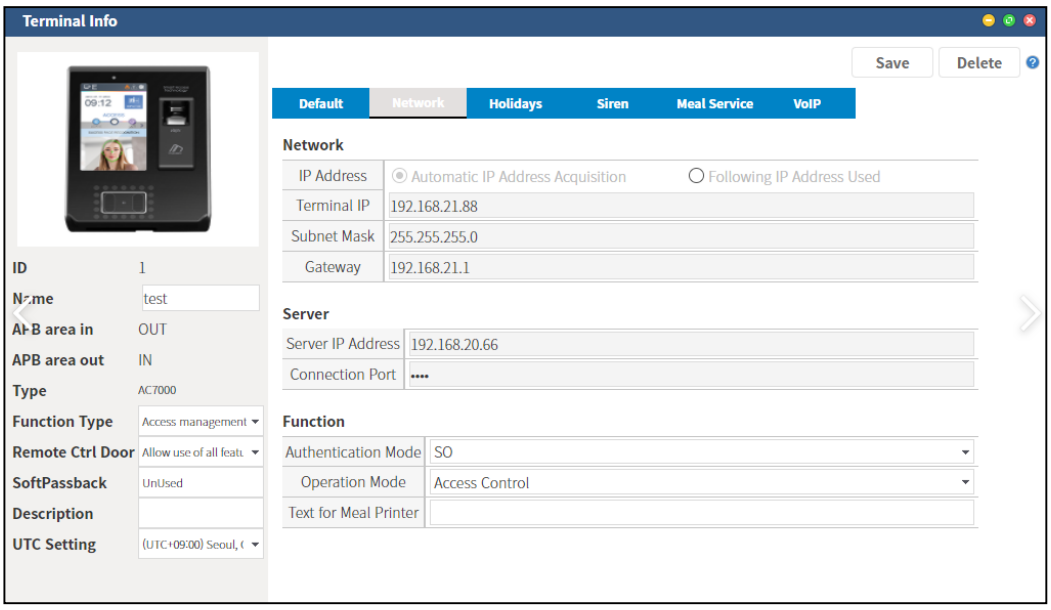
: It is the feature to modify and check the current default setting of terminal.



- **FP Auth Level:** Import 1:1, 1:N authentication level from the terminal and change it.
- **Access Level:** Import Anti-Passback information of terminal and change it.
- **Sound Volume:** Set the terminal sound volume. (1~20)
- **User Key:** Select the user key as 'User ID' or 'Employee Number'.
- **User ID Length (1..8):** Set the user ID length to be displayed in the terminal. (1~8)

② Network

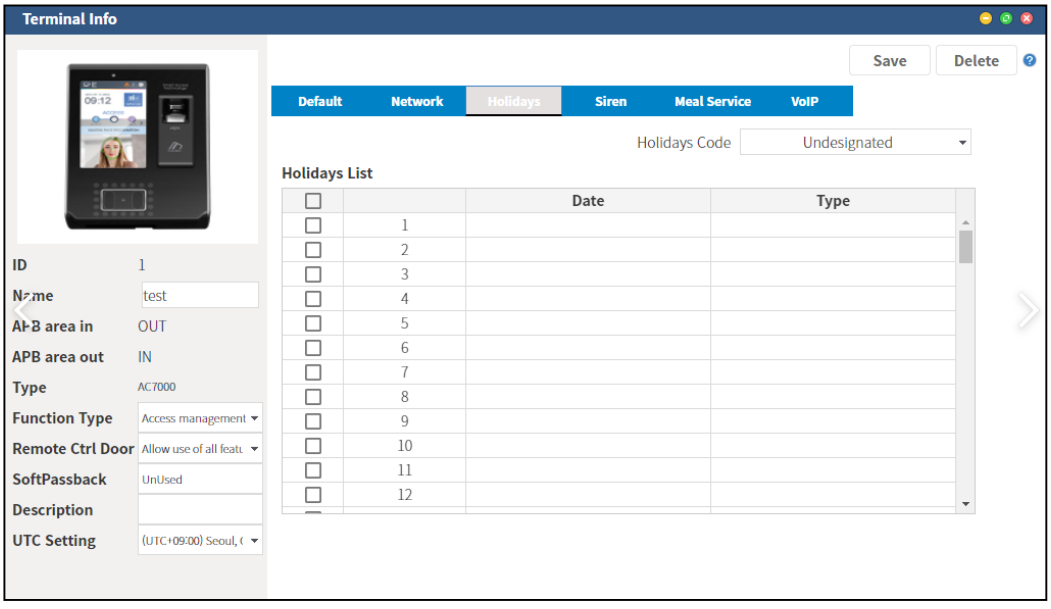
: It is the feature to check the current network setting and only modify the function part.



- **Authentication Mode:** Check the current authentication mode of terminal and change it among 'NS', 'SN', 'NO' and 'SO'.
- **Operation Mode:** Select the operation mode among 'Access Control', 'TNA' and 'Meal'.
- **Text for Meal Printer:** When connecting to the meal printer, it is available to enter the text.

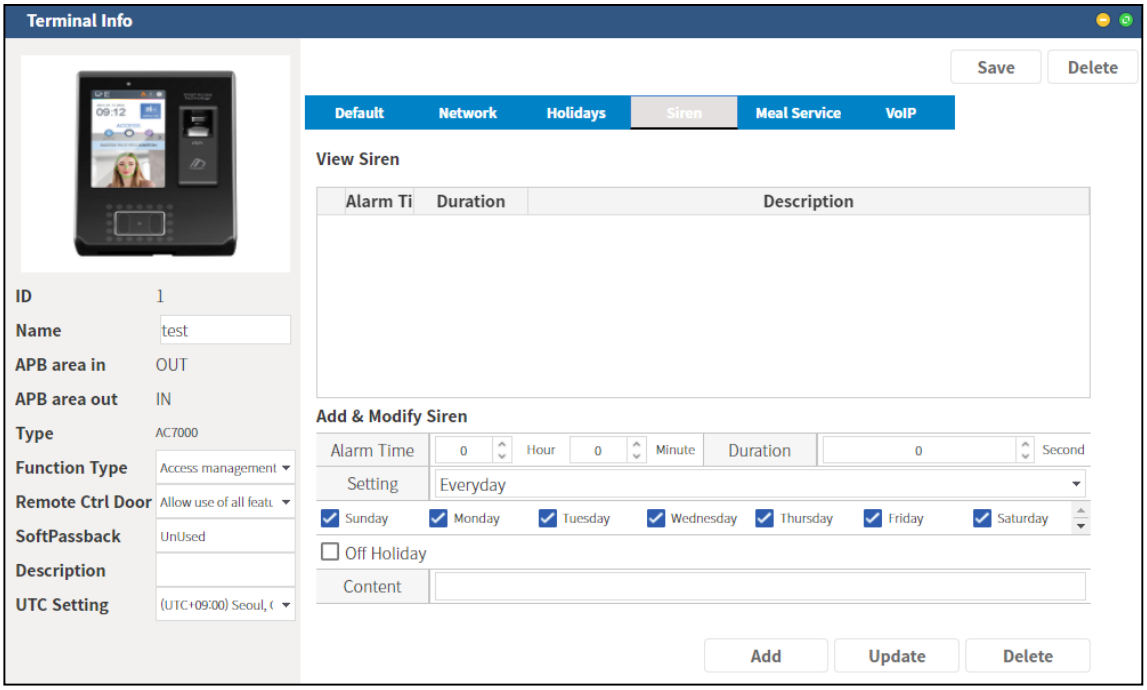
③ Holidays

: It is the feature to import the holiday list registered on the terminal. Also, set the holiday information and click [**Save**] button to send it to terminal.



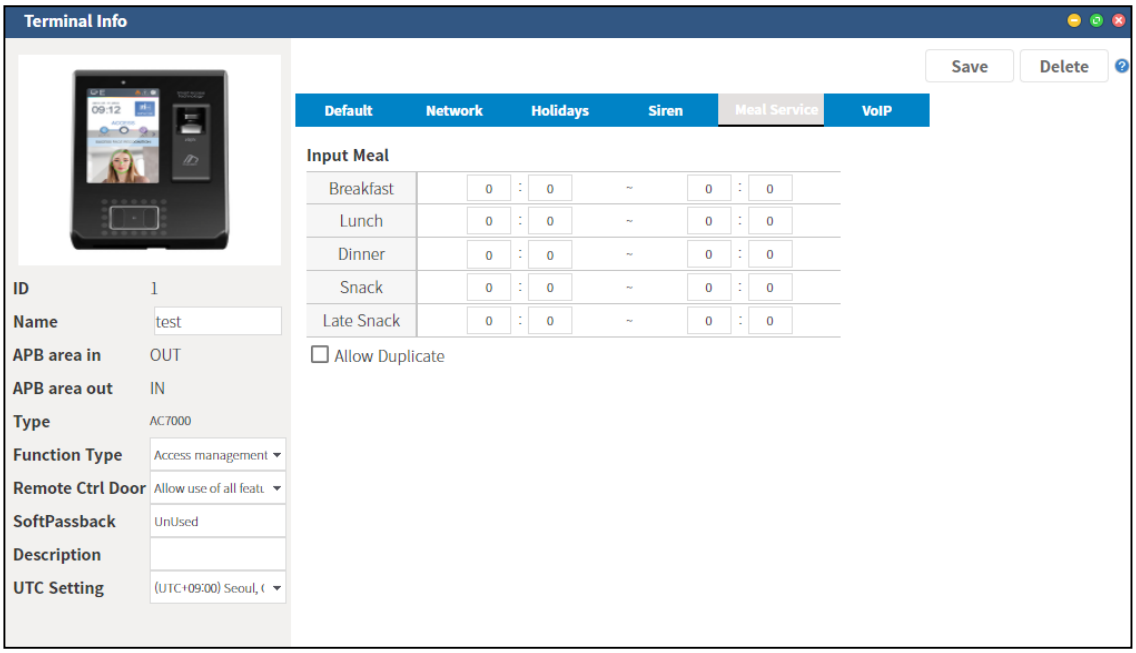
④ Siren

: It is the feature to set the alarm time of terminal.



⑤ Meal

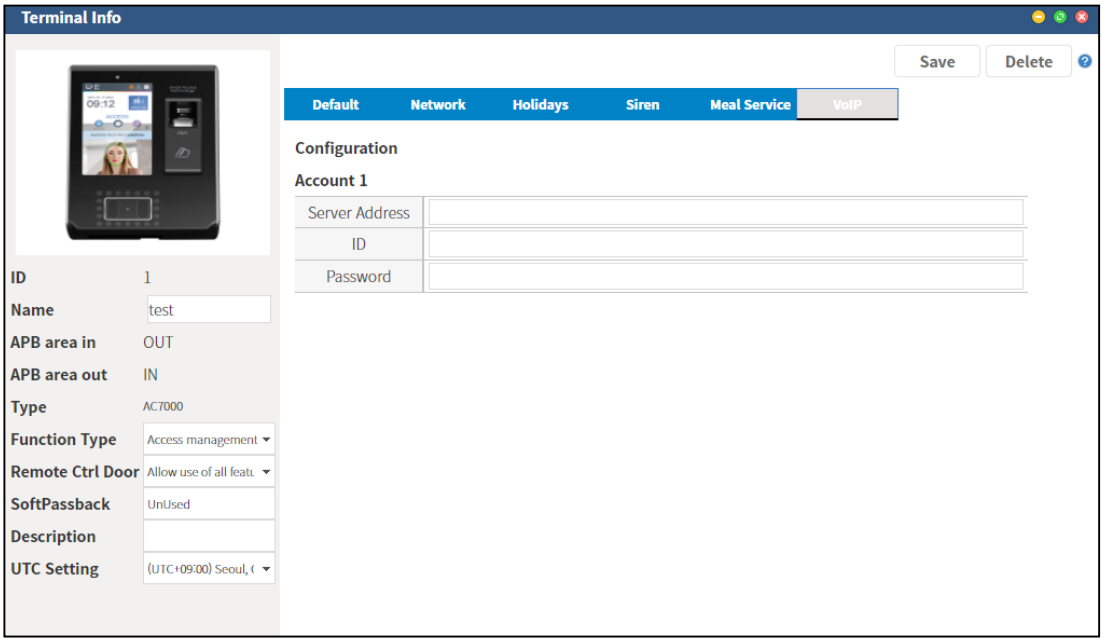
: It is the feature to set the time of 'Breakfast', 'Lunch', 'Dinner', 'Snack', and 'Late Snack'.



- **Allow duplication**: When a user authenticate in terminal for meal, it is the feature to allow the duplicated authentication.

⑥ VoIP

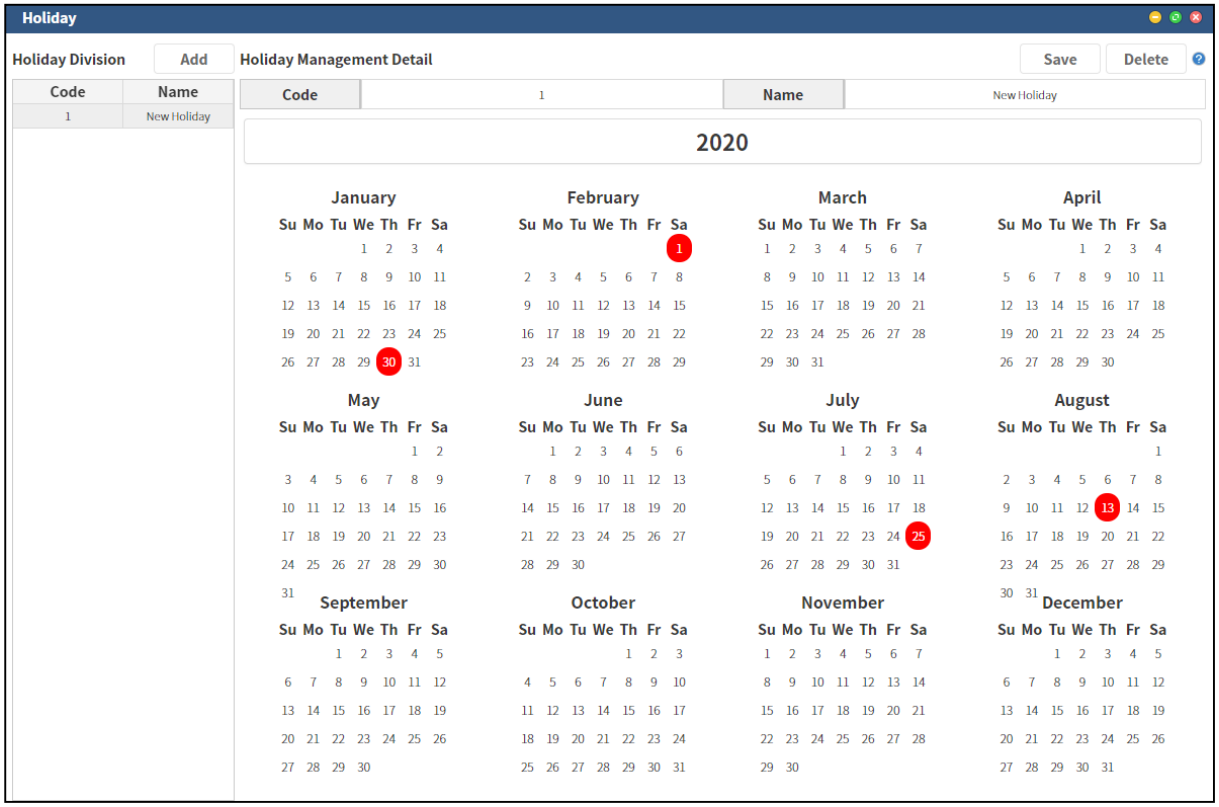
: It is the feature to set VoIP in terminal. When setting without server address, the existing VoIP is disabled. This feature is only for AC7000.



21. Timezone

1) Holiday

It is the feature to set the annual holiday. You can add 30 holidays for maximum in 1 holiday code.



Enter the code and name, set the date to make a new holiday code.

- **Add**: Enter the code and name and click [**Add**] button to make a new holiday code.
- **Save**: After making a new code, set the date and click [**Save**] button.
- **Delete**: If you want to delete the holiday code, select it in the left side and click [**Delete**] button.

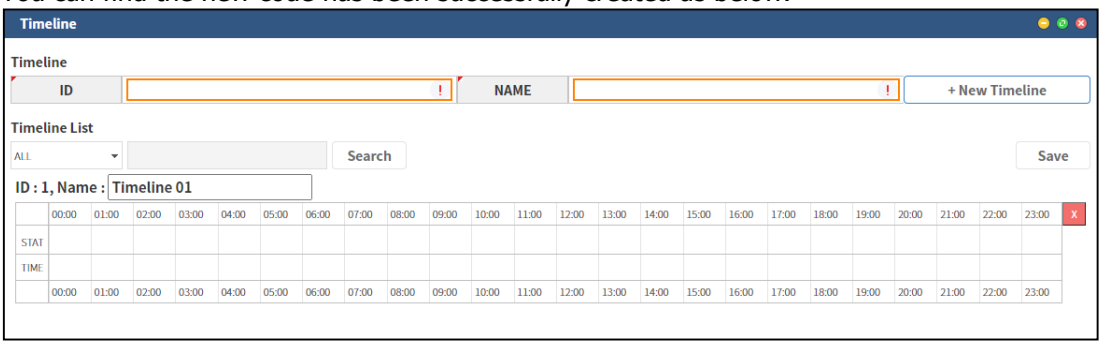
2) Timeline Management

It is the feature to set a time line for door open / close and authentication type by time.

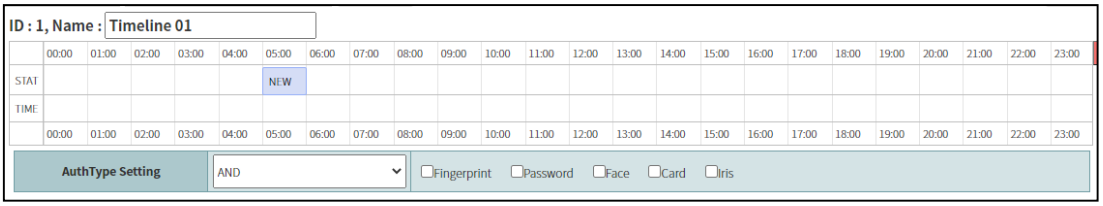
To set a time line, you can refer the instruction below.

① Enter the ID and Name and then select **[+New Timeline**] button.

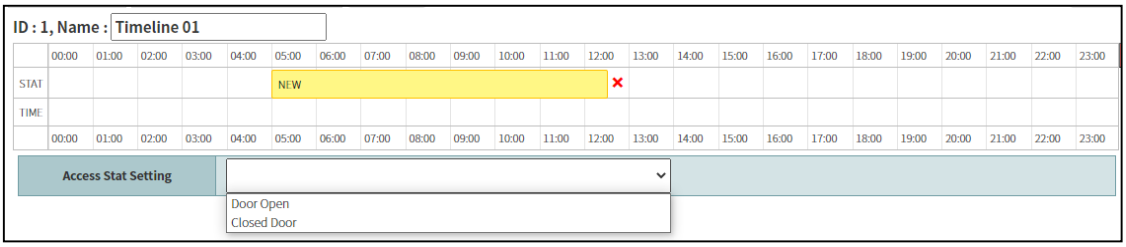
② You can find the new code has been successfully created as below.



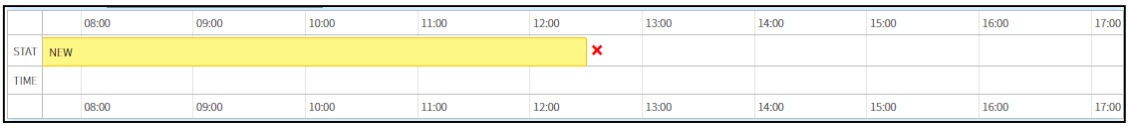
③ Double click on the start area.

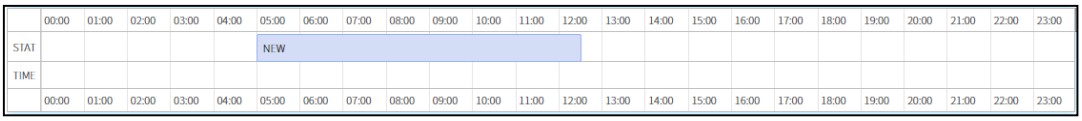


④ Click the created start area and drag to set a time range. And you can set 'Door open' or 'Door closed' in [**Access Start Setting**].

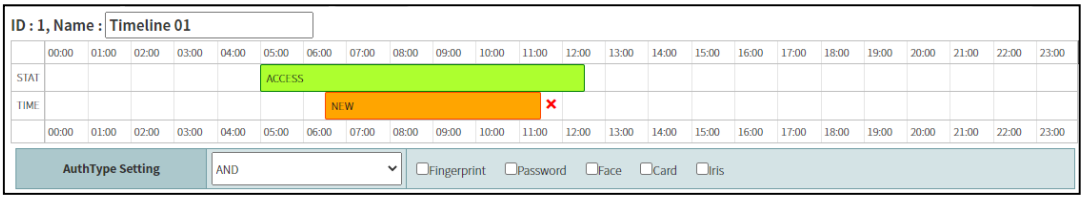


⑤ You can set the time line in more detail by using mouse wheel to expand or reduce. When you select button, the selected area is deleted.





⑥ You can set the authentication type by time. When you select button, the selected area is deleted.



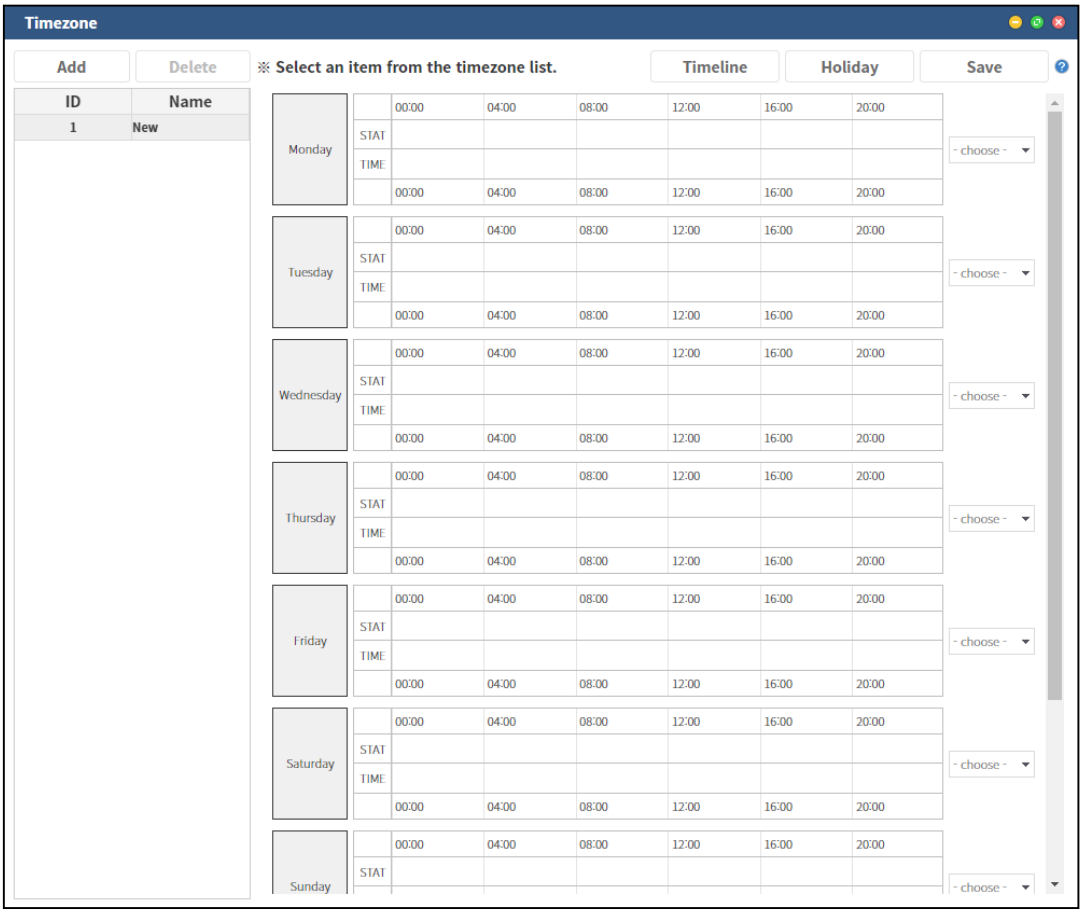
⑦ After setting all, select [**Save**] button.

3) Timezone Management

It manages the allowed authentication time of terminals and users, door open time and authentication type by time.

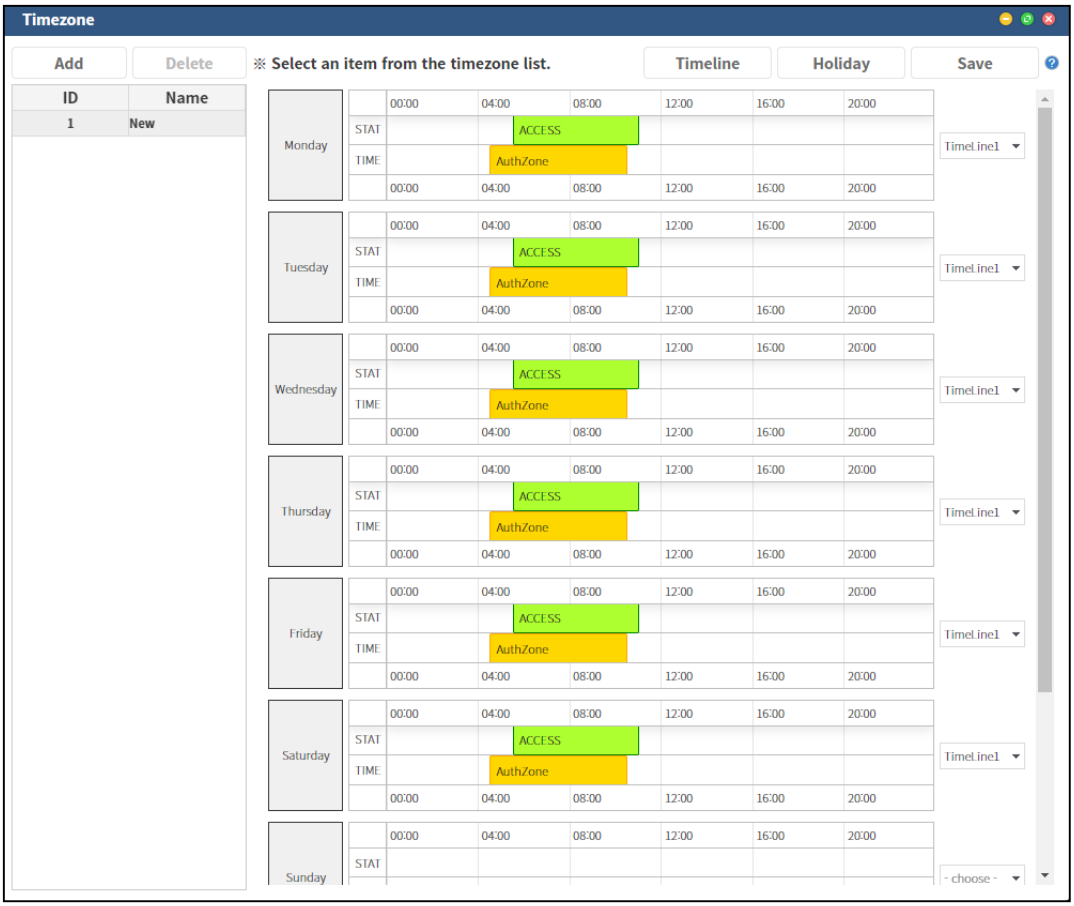
It sets a daily schedule by using the time line management and manages the weekly schedule in time zone management.

① Click **[Add]** button to create a new time zone and set a weekly schedule.



② Set each day or select saved timeline on the right list box to set the daily schedule.

To set the time range in more detail, you can also expand or reduce by using the mouse wheel.



The day without timeline setting follows terminal default setting.

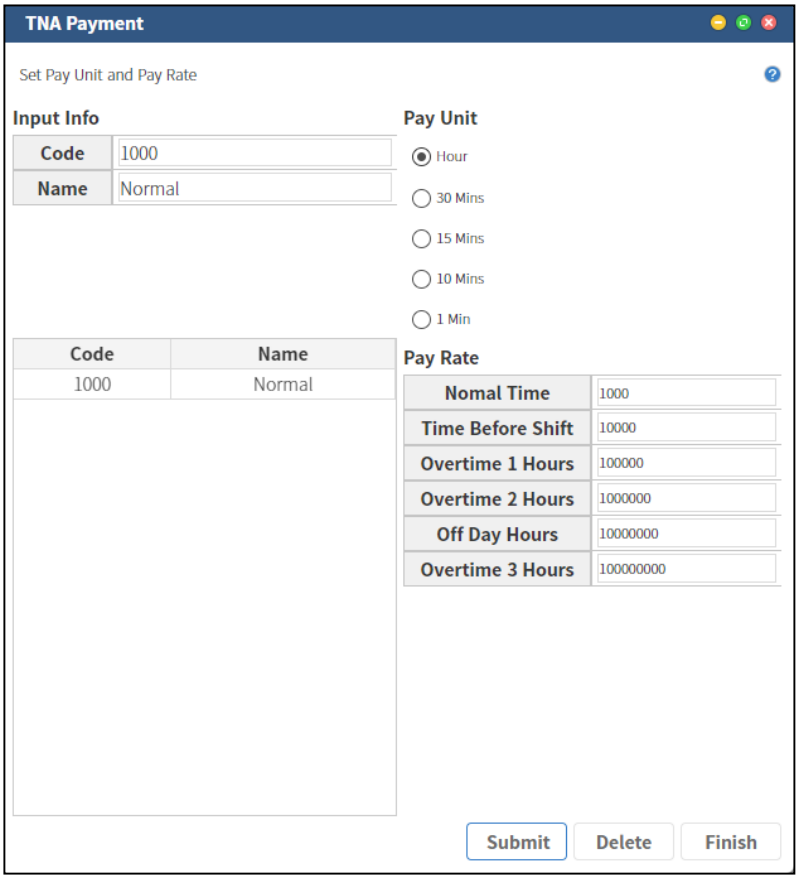
You can select the holiday from the holiday list below. The holiday list is shown in the holiday management as below.

③ The created time zone can be applied in the access group.

22. TNA

1) TNA Payment

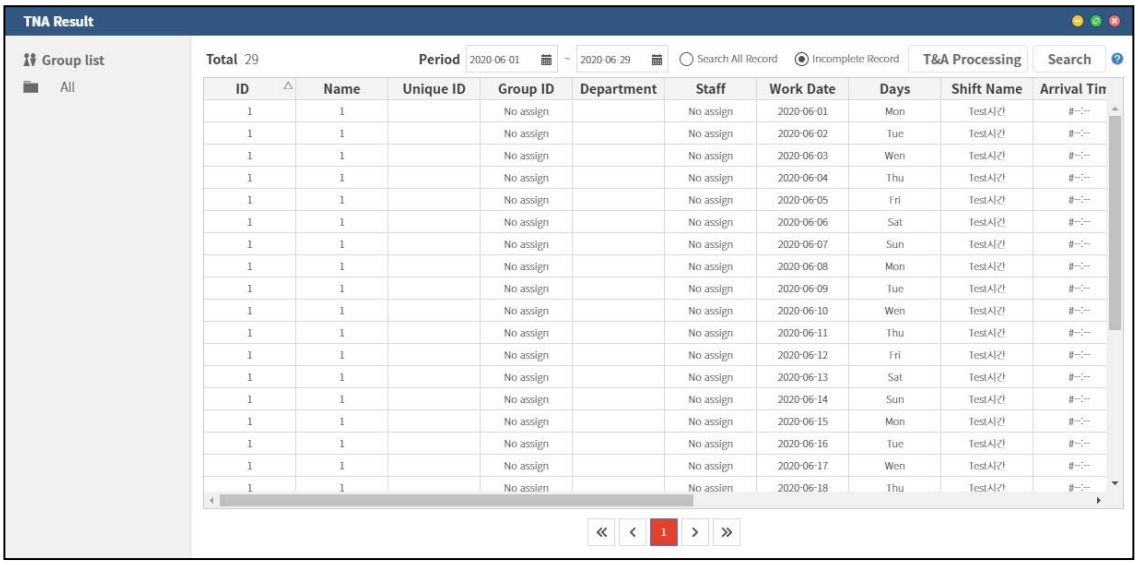
It sets the payment amount and unit for each working hour.



- **Code:** Set a unique code for TNA. It can enter 4 characters (alphabet and number) without duplication.
- **Name:** Set a TNA payment name.
- **Pay Unit:** Set the payment unit among 'Hour', 30 Min, 15 Min, 10 Min and 1 Min.
- **Pay Rate:** Set the payment rate for each working hour among 'Normal', 'Time Before Shift', 'Overtime 1 Hours', 'Overtime 2 Hours', 'Off Day Hours', and 'Overtime 3 Hours'.
- **Save**: Set the TNA payment setting and save it.
- **Delete**: Delete the selected TNA payment code.
- **Close**: Close the TNA Payment page.

2) TNA Result

It is the feature to search the TNA result by period.



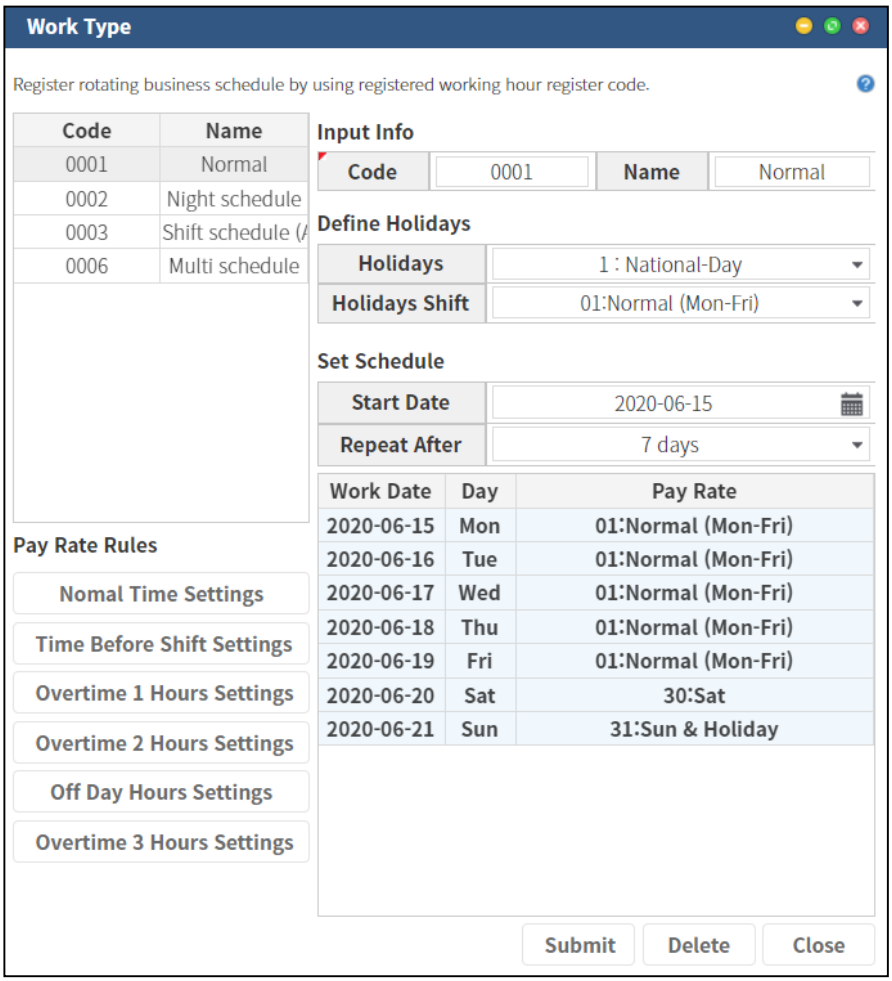
- **Period:** Set period to search TNA result.
- **Search All Record:** Get all the TNA result.
- **Incomplete Record:** Get only incomplete TNA result.
- **Total:** Display the total TNA result number.
- **TNA Processing**: Select this button to calculate total TNA processing.
- **Search:** Get the TNA result in condition of setting.

3) Work Type

After setting Work Time, you need to set Work Type in accordance in work schedule.

Set a unique rotated work schedule code using **[Work Time]** code registered before.

You can set maximum 30 days of rotated work schedule.

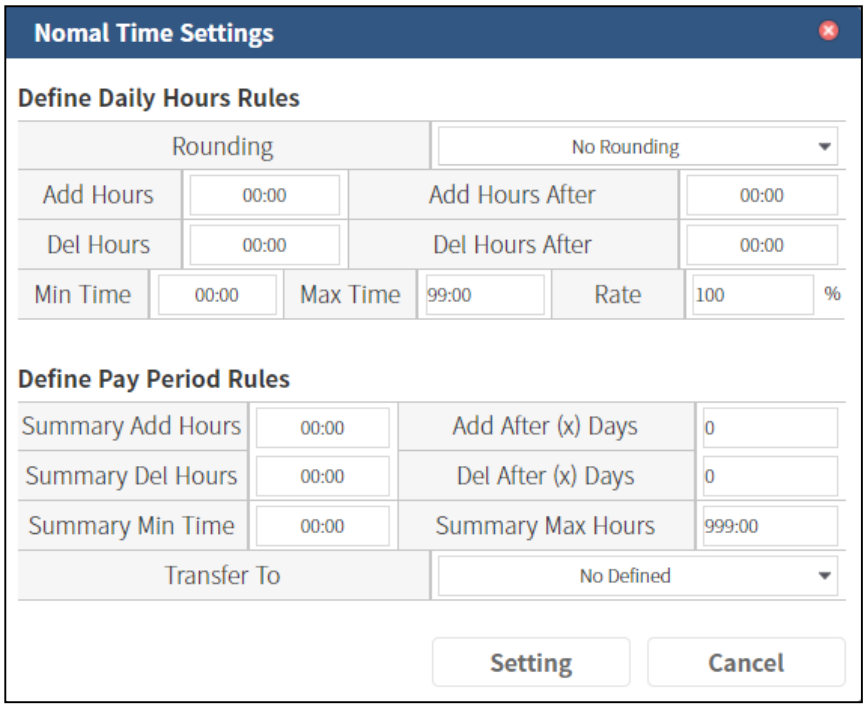


- **Input Info**
  - **Code:** Set a unique code for TNA. Enter 4 characters (alphabet and number) without duplication.
  - **Name:** Set name of Work Type.
- **Define Holidays**
  - **Holidays:** Select the registered holiday code edited from [**Timezone**] – [**Holiday**].

    (If the holiday code is not assigned, it cannot create the work type.)
  - **Holiday Shift:** Set Holiday code registered from [**Work Time**] Menu.
- **Set Schedule**
  - **Start Date:** Set the date to start the schedule. It will be start date of rotated schedule.
  - **Repeat After:** Set the rotation days. Normally, it is 7 days.

When you set the start date, the setting days are searched in the list based on the start date. Double click on Pay Rate part of the table then you can see and set work time code registered from **[Work Time]** menu.

- **Pay Rate Rules:** Set each work time TNA setting. Click each work type to set individually.
- **Normal Time Settings**



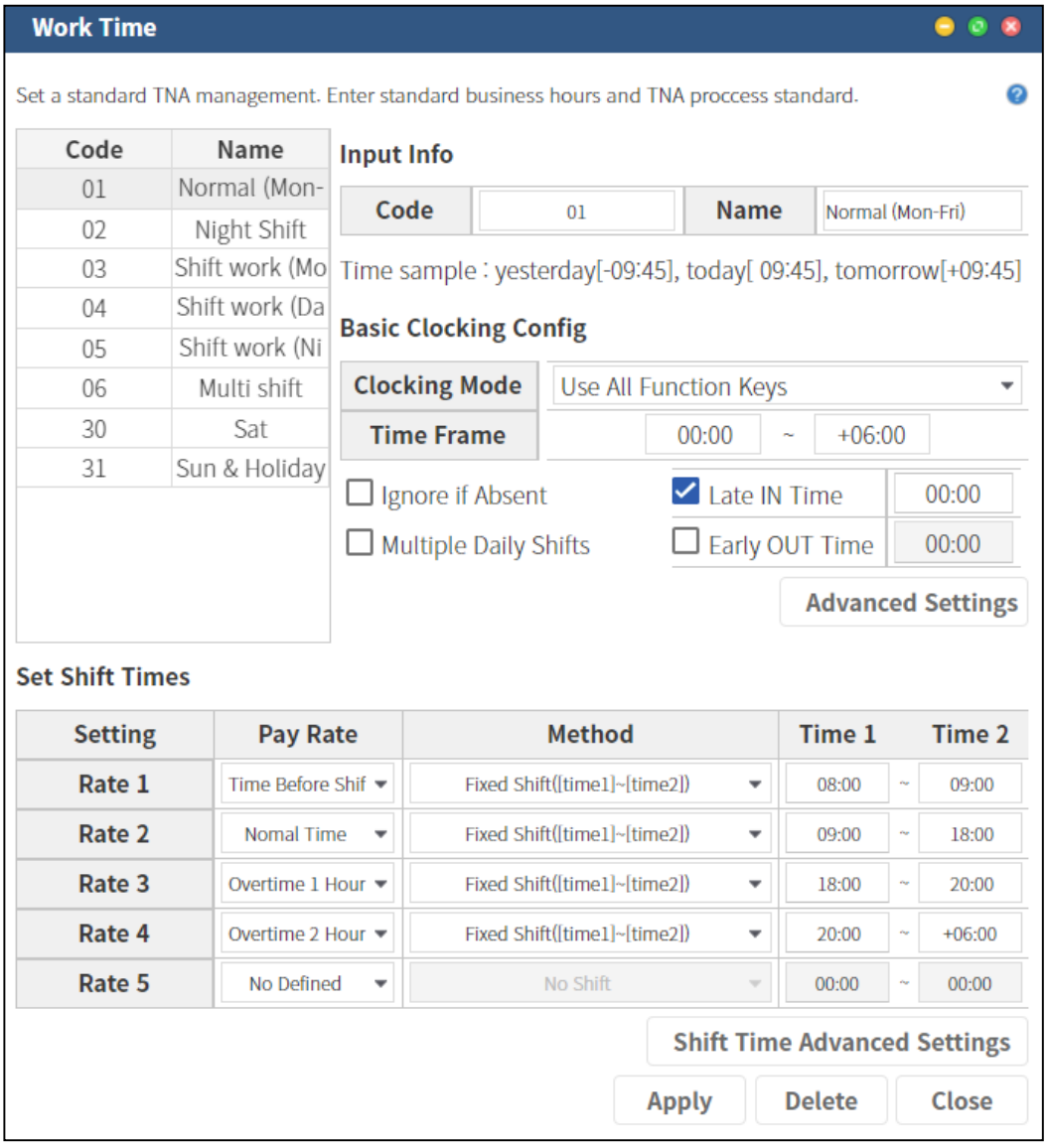
- **Rounding:** Set the TNA processing result as ±10 mins, ±15 mins, and ±30 mins on TNA calculation.
- **Add hours:** Set the additional time on TNA calculation.
- **Add Hours After:** Set the additional time after setting work time on TNA calculation.
- **Del Hours:** Set a deducted time on TNA calculation.
- **Del Hours After:** Set the deducted time after setting work time on TNA calculation.
- **Min Time:** Minimum time for TNA calculation.
- **Max Time:** Maximum time for TNA calculation.
- **Rate:** Set the extra charge rate.
- **Summary add Hours:** Set the additional time in total calculation.
- **Add after (x) days:** Set the minimum work day in total calculation.
- **Summary Del Hours:** Set the deducted time in total calculation.
- **Del after (x) days:** Set the minimum work hour to apply in total calculation.
- **Summary Min Time:** Set the minimum time in total calculation.
- **Summary Max Hour:** Set maximum time in total calculation.

- **Transfer to:** Set the total calculation result to other work hour.
- **Setting**: Save the details.
- **Cancel**: Delete the details.

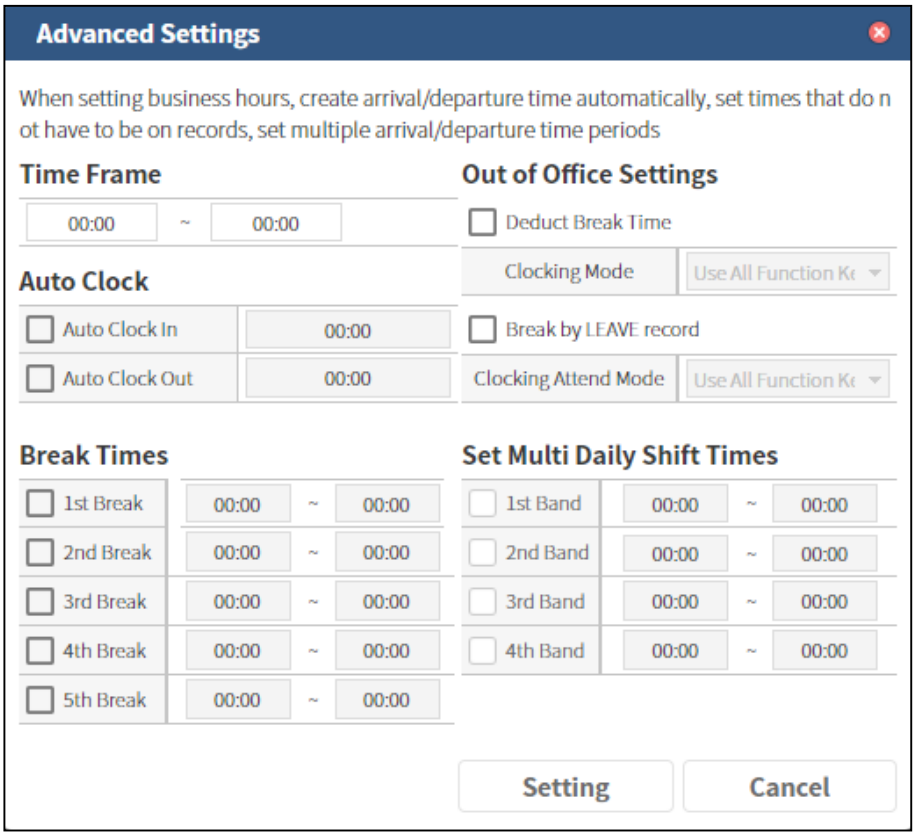
4) Work Time

Set a standard of TNA management. Enter the normal hours and set as you. Set the work time based on a day and extra details such as late, leaving early, exception hours. If there are 2 different working hours and types, you should create the code separately.

The time is set as DHH:MM (D: Day, HH: Hour, MM: Minute) and the previous day is described with '-'and then the next day is done with '+'. (All timeline is entered between 00:00 ~ 23:59.)



- **Input Info**
    - **Code:** Set a unique code for TNA. Enter 4 characters (alphabet and number) without duplication.
    - **Name:** Set name of Work time
- **Basic Clocking Config.**
    - **Clocking mode:** Select whether to use all function keys or use only attendance key (F1, F2) for the TNA calculation. When you select [**User All Function Keys**], it recognizes all authentication report as TNA record and. And [**Use Only ATTEND Key**] is used to only recognize 'Attend' and 'Leave' mode as the TNA record.
    - **Time Frame**: Set the time frame for TNA processing.
    - **Ignore if Absent:** Even if it is absent on that day, it doesn't process absent. (Ex. for holiday or weekend)
    - **Late IN / Early OUT Time:** Set time to calculate as Late IN or Early OUT.
    - **Multiple Daily Shifts:** If 'attendance' and 'leave' are more than twice each per day, use this option.
- **Advance Settings**: It can set the work time in more detail.

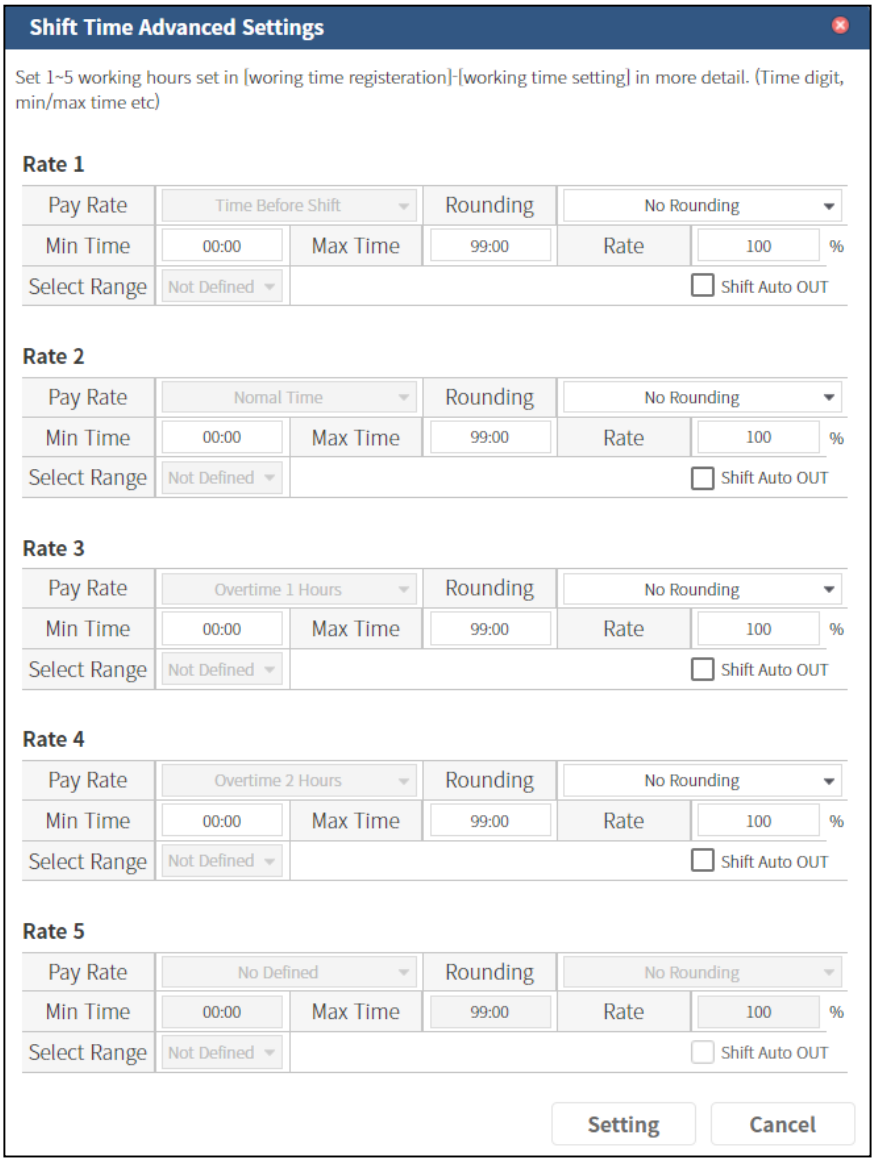


- **Time Frame:** Calculate Arriving/Leaving record between the time as TNA.
- **Auto Clock:** Create IN/OUT record automatically even there are logs after/before set time.
- **Auto Clock IN:** If there is an authentication record after the setting time, the attendance record is recorded as the setting time.
- **Auto Clock OUT:** If there are no authenticated records after the work hours, automatically logged OUT at the setting time.
- **Out of Office Settings:** Use these options if you want not to calculate the time such as break time.
- **Deduct Break Time:** Not calculate the time not in the office.
- **Clocking Attend Mode:** Select whether to use all function keys or use only attendance key (F1, F2) for the TNA calculation. When you select [User All Function Keys], it recognizes all authentication report as TNA record and. And [Use Only ATTEND Key] is used to only recognize 'Attend' and 'Leave' mode as the TNA record.
- **Break by LEAVE record:** If you want to exclude the time, you leave work in the middle of the day.

- **Set Multi Daily Shift Times:** If 'attendance' and 'leave' are more than twice each per day, use this option.
- **Setting**: Save the setting.
- **Cancel**: Delete the setting.

- **Set Shift Times**
  - **Pay Rate:** Select one among 'Normal Time', 'Time before Shift', 'Overtime 1~3 hours', and 'Off Day Hours'.
  - **Method**
    - ✓ No Shift: Not calculate the work hours.
    - ✓ Fixed Shift ([Time1] ~ [Time2]): Recognize as working hour between time1 and time2.
    - ✓ Actual time: Calculate all work time.
    - ✓ Over Time [Time 1] ~ [Time 2]: Based on the record of work, time is passed after time 1, and time 2 is recognized as working time.

- **Shift Time Advanced Settings**

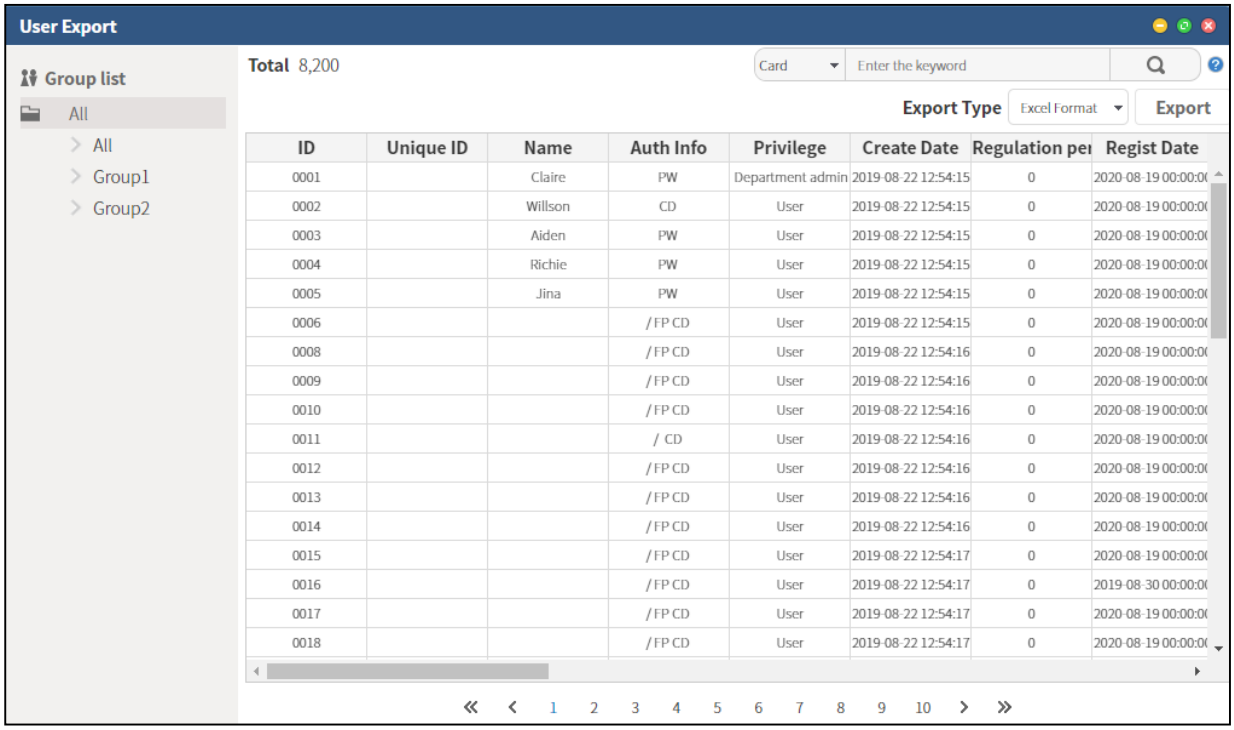


- **Pay Rate:** Show the pay rate setting.
- **Rounding**: Setting for rounding. Least rounding unit is 10 minutes.
- **Min Time:** Minimum TNA calculating time.
- **Max Time:** Maximum TNA calculating time.
- **Rate:** Extra charge rate.
- **Select Range:** IN/OUT detail setting except for **[all range]**. It can be added according to Multiple Daily Shift setting.
- **Shift Auto OUT:** Automatically OUT even there is no OUT log.

23. User

1) User Export

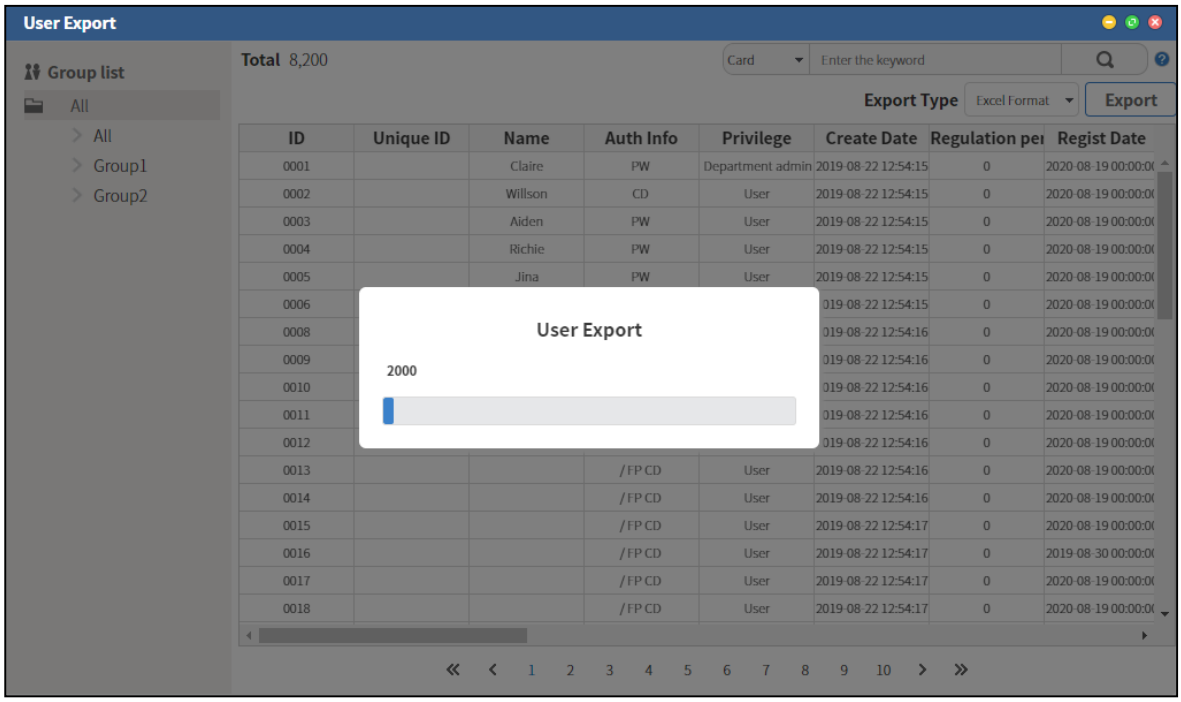
It is the feature to export the user information registered in the server as file according to the detailed condition.



-

: Select one of categories among 'ID', 'Name', 'Unique ID', 'Group Name', 'Access Group' and 'Card or enter the keyword that you want to search.

- **Export Type**: Select Excel format or Data format.



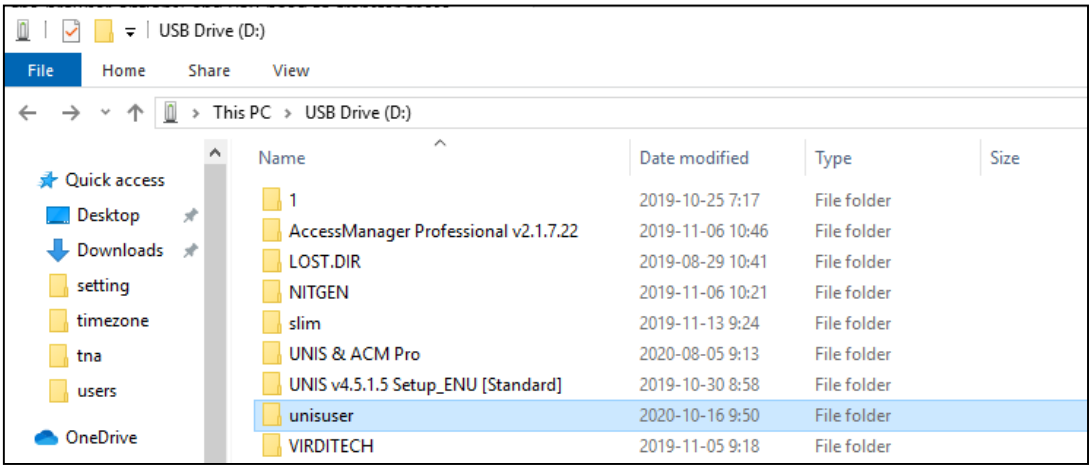
When selecting [**Export**] button, you can see the progress to export the data as a file.

The followings are how to use when the file format is the data.

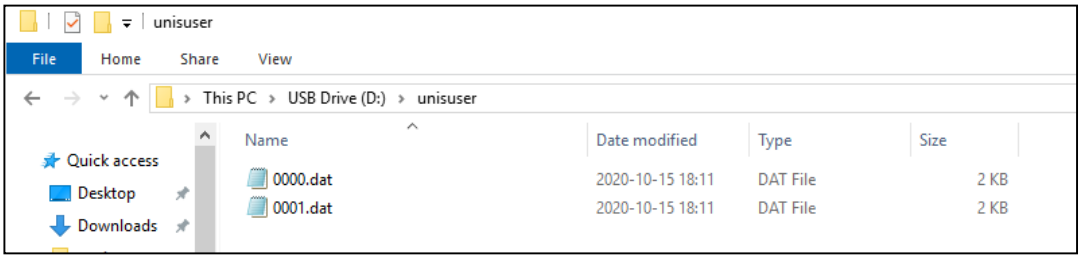
① When you use Data format, the file extension is .dat and the name is saved in order from 0000.

② The files are saved into 'Download' folder (or any folder specified in the browser options) and you need to transfer these files into USB or SD card.

③ Create 'unisuser' folder from in the drive.



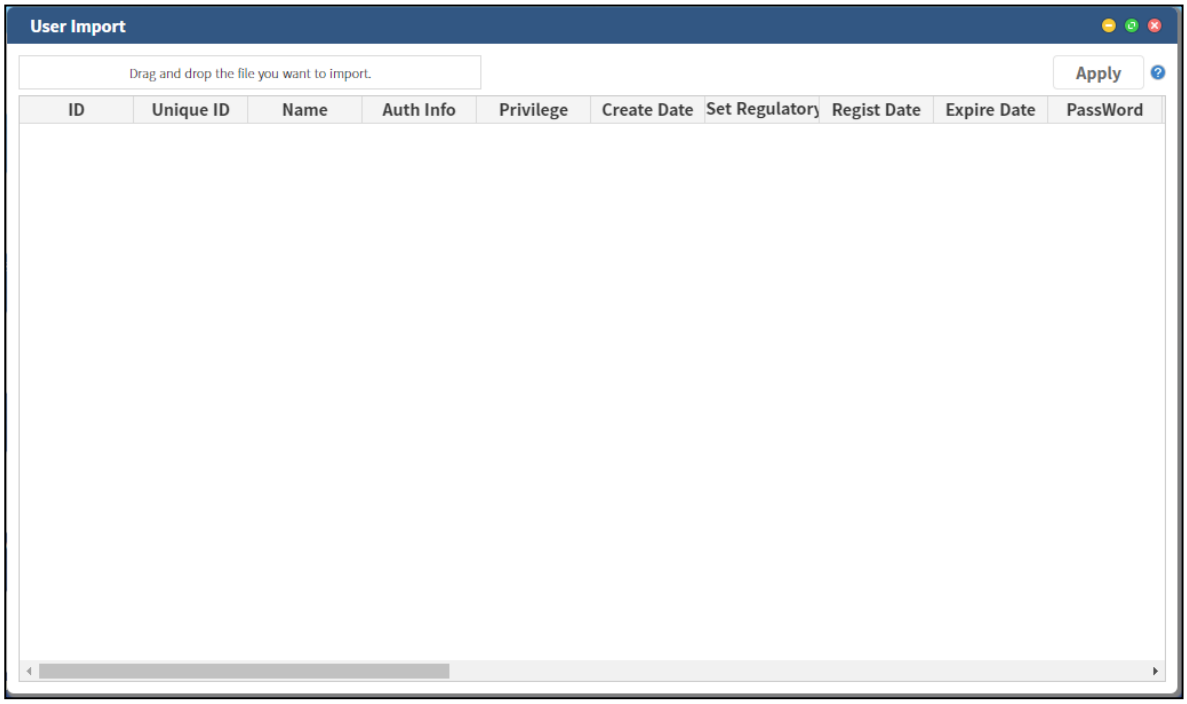
④ Move all downloaded .dat files into ‘unisuser’ folder.



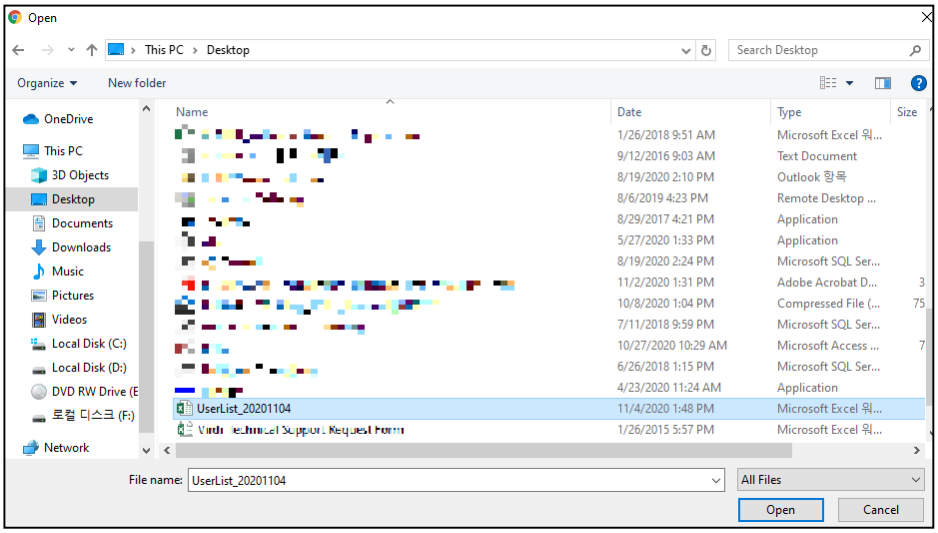
⑤ Connect SD Card / USB to the terminal and transfer users.

2) User Import

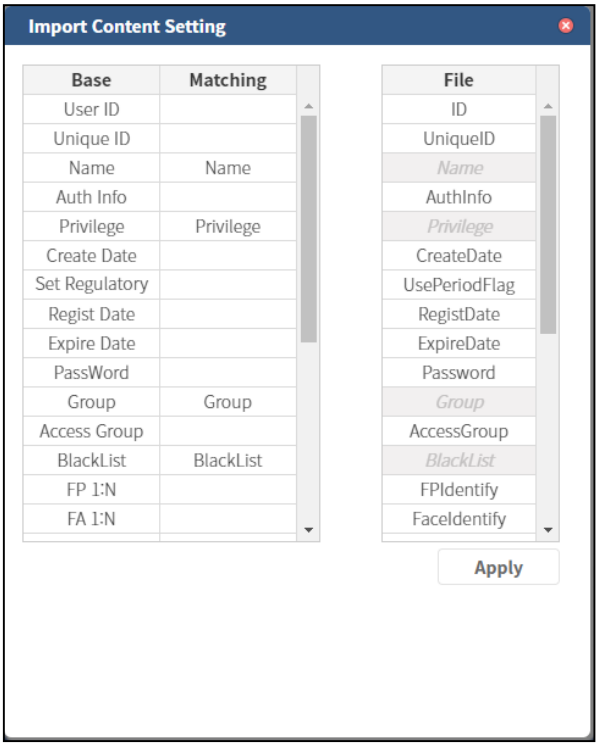
This feature helps you to register bulk size of users using excel file.



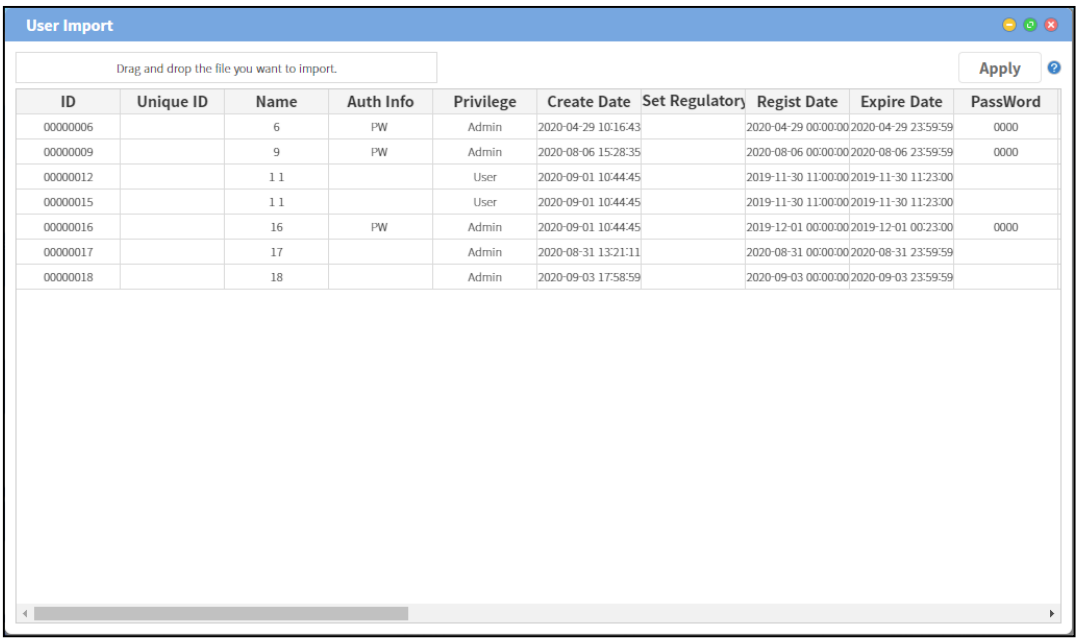
① Click '**Drag and drop the file you want to import**' button and find the user file to import.



Select the item to import. Drag and drop the item from right side to left side to import the information.



② Check the imported user information.



ID	Unique ID	Name	Auth Info	Privilege	Create Date	Set Regulatory	Regist Date	Expire Date	PassWord
00000006		6	PW	Admin	2020-04-29 10:16:43		2020-04-29 00:00:00	2020-04-29 23:59:59	0000
00000009		9	PW	Admin	2020-08-06 15:28:35		2020-08-06 00:00:00	2020-08-06 23:59:59	0000
00000012		1 1		User	2020-09-01 10:44:45		2019-11-30 11:00:00	2019-11-30 11:23:00	
00000015		1 1		User	2020-09-01 10:44:45		2019-11-30 11:00:00	2019-11-30 11:23:00	
00000016		16	PW	Admin	2020-09-01 10:44:45		2019-12-01 00:00:00	2019-12-01 00:23:00	0000
00000017		17		Admin	2020-08-31 13:21:11		2020-08-31 00:00:00	2020-08-31 23:59:59	
00000018		18		Admin	2020-09-03 17:58:59		2020-09-03 00:00:00	2020-09-03 23:59:59	

* When importing users via Excel file, only password types are supported as authentication types.

When entering the authentication method in the Excel file, you can enter a password or blank. The blank input is used to register the authentication method later after user registration.

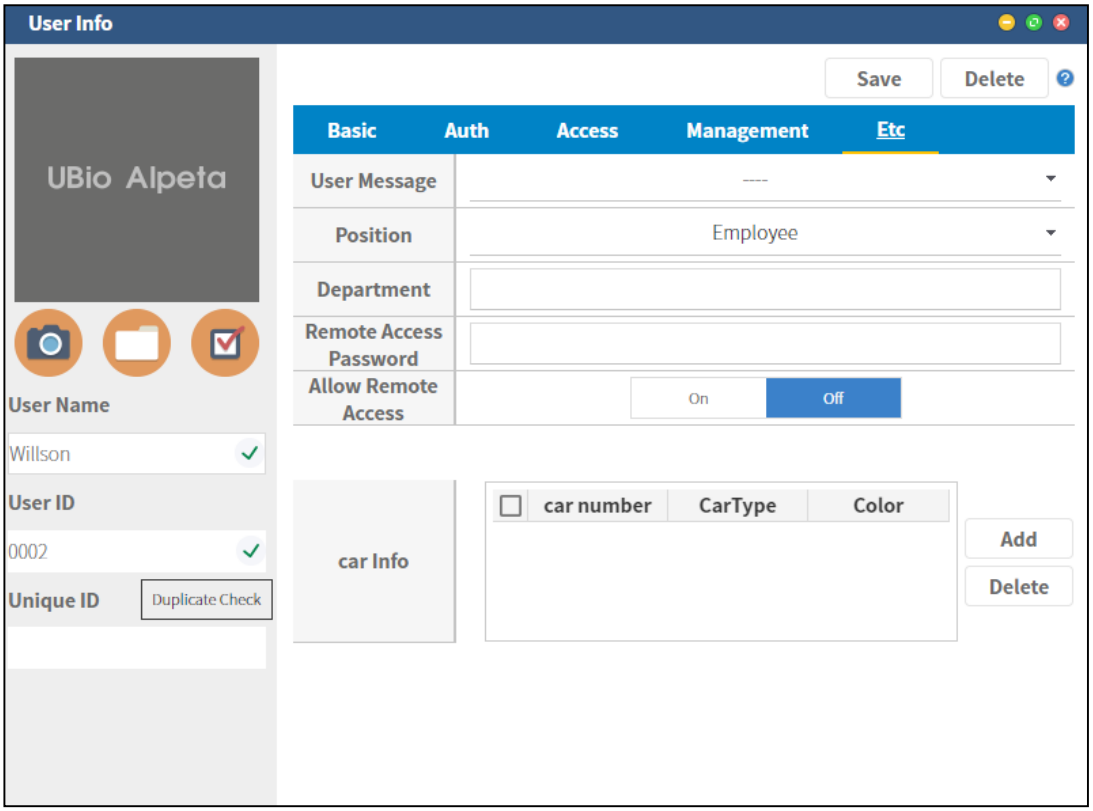
However, in case of data file, you can import all authentication methods.

③ Check if the user is properly imported in 'User Management'.

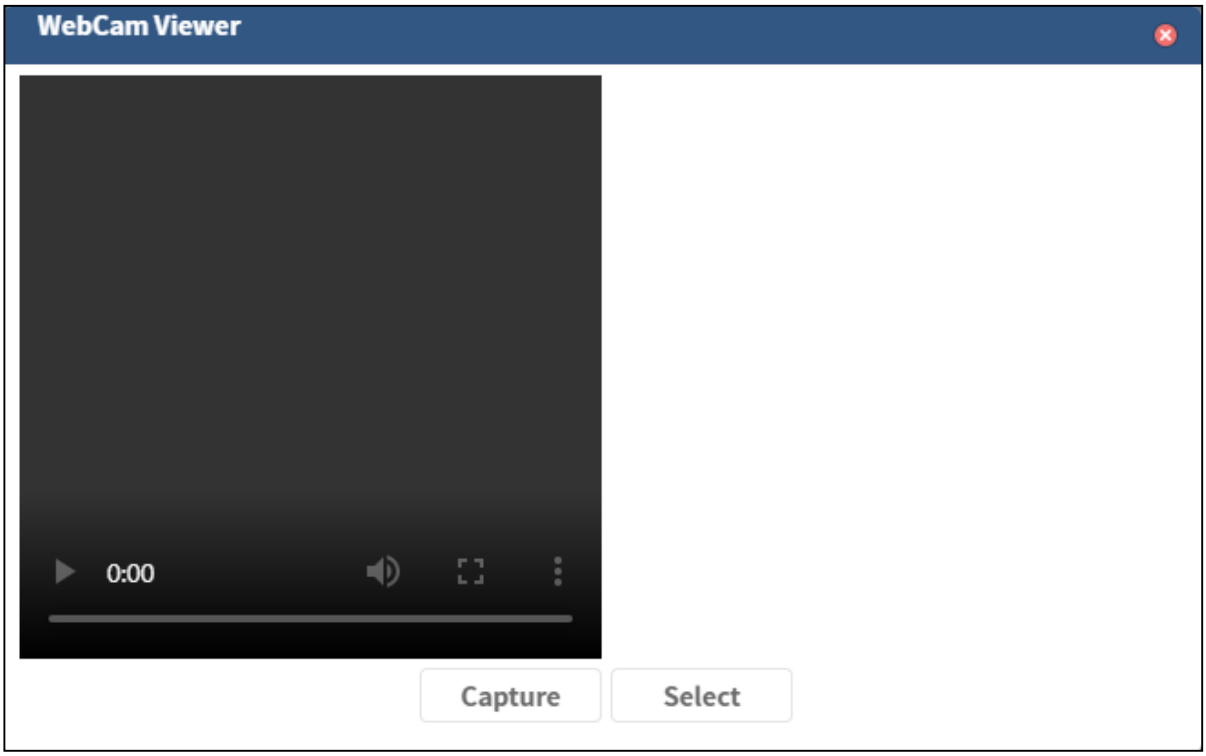
3) User

It is the feature to manage the user information. You can see, edit, and delete user information.

① Basic

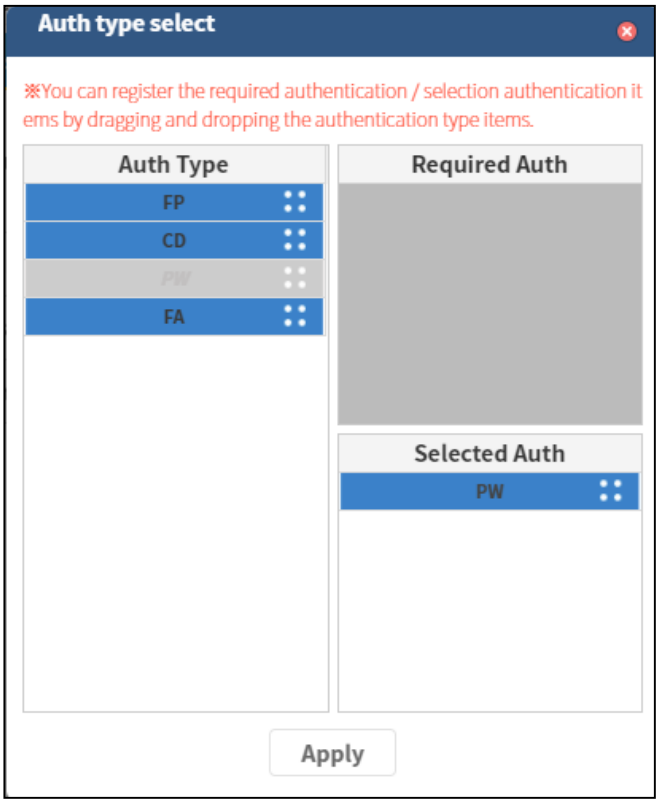


- **User Name:** Maximum 50 characters are available.
- **User ID**: Only number are available. 12 digits for Virdi, 19 digits for Nitgen.
- **Unique ID:** Maximum 20 Alphanumeric characters are available.
- : Capture the user picture using PC webcam. The pop-up window for Webcam is shown.



- **Capture:** Capture the preview screen in left side. The captured screen is shown in the right side.
- **Select:** To use the captured photo, select this button.
- : Select a picture file from the photo to use as user's picture.
- : Save the selected user picture.

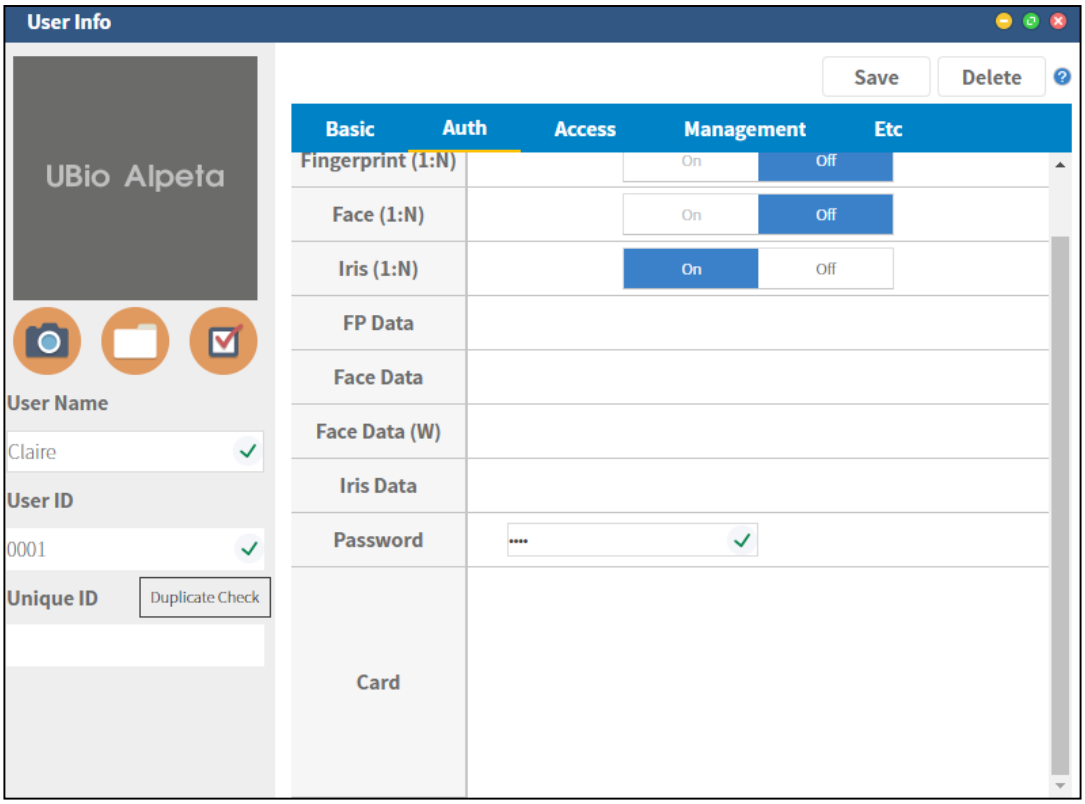
- **Auth Info:** Display the user authentication method.



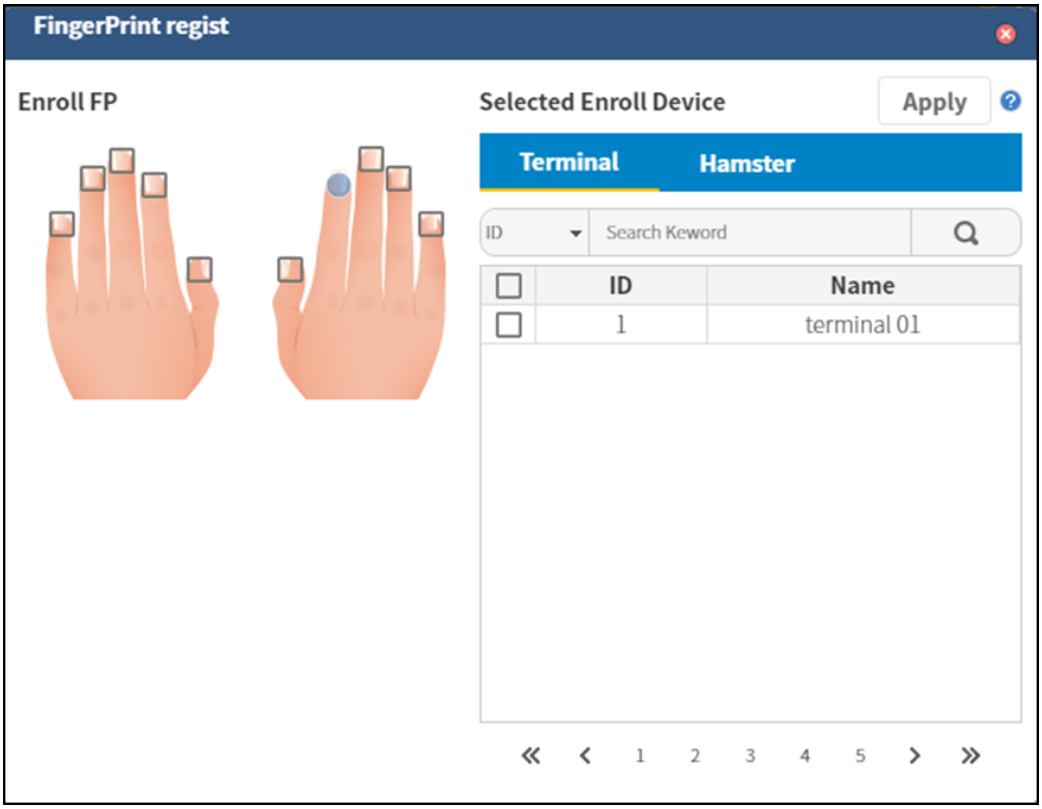
- **Auth Type:** Authentication methods available to select. The selectable type is blue and the selected type is gray.
- **AND Auth:** Set the authentication types as AND combination.
- **OR Auth:** Set the authentication types as OR combination.

- **Privilege:** Set user privilege. It can be selected among '**Admin'**, '**User'** or other privileges that the admin adds and creates.
- **Regulation Period:** Set the use period of the user.
- **Expiration Date:** Set whether to use the expiration date of the user. If you select '**Use'**, the user can be used in the set expiration period.

② **Auth**



- **Auth Level**: Set the 1:1 authentication level in the fingerprint authentication. The level is 1 ~ 9. The number is higher; the matching score is set higher. The default value is '5'.
- **Fingerprint (1:N)**: Set the user's fingerprint in 1:N matching list. When off, only 1:1 fingerprint matching is available for this user.
- **Face (1:N):** Set the user's face in 1:N matching list. When off, only 1:1 face matching is available for this user.
- **FP Data:** Select [**Edit**] button to register the user's fingerprint. [**Edit**] button is activated if you selected 'FP' in the authentication type.

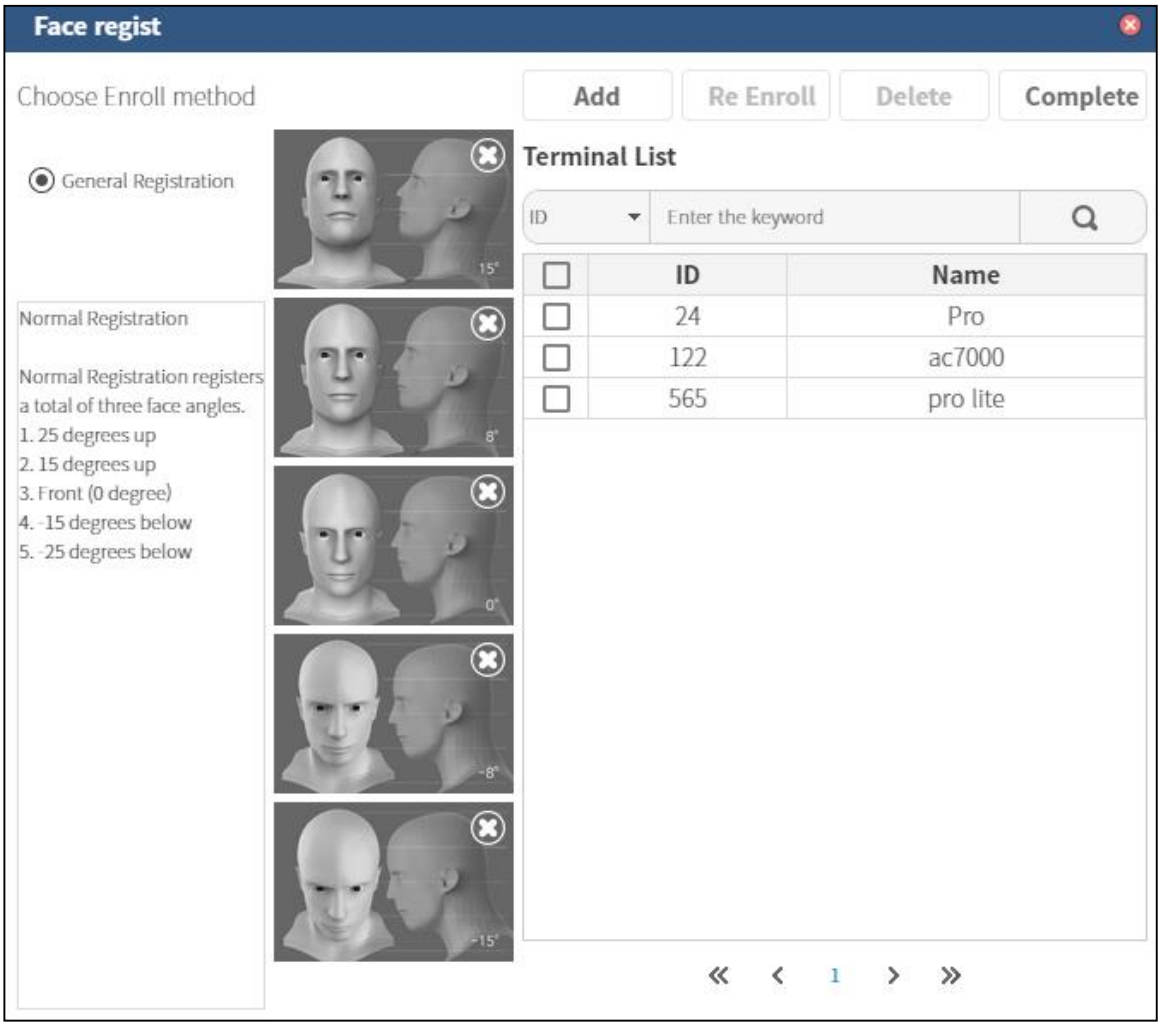


- **Enroll FP:** Show the registered user's fingerprint. The registered fingerprint is shown as blue, duress fingerprint is red and the fingerprint that is not registered is square box. If you use Nitgen device, the duress fingerprint is not reflected.
- **Selected Enroll Device:** Select a device to register fingerprint.

  When you click 'Terminal' tab, display the connected terminals and select one for getting the fingerprint image. Select one terminal and click [**Apply**] button to register fingerprint from terminal.

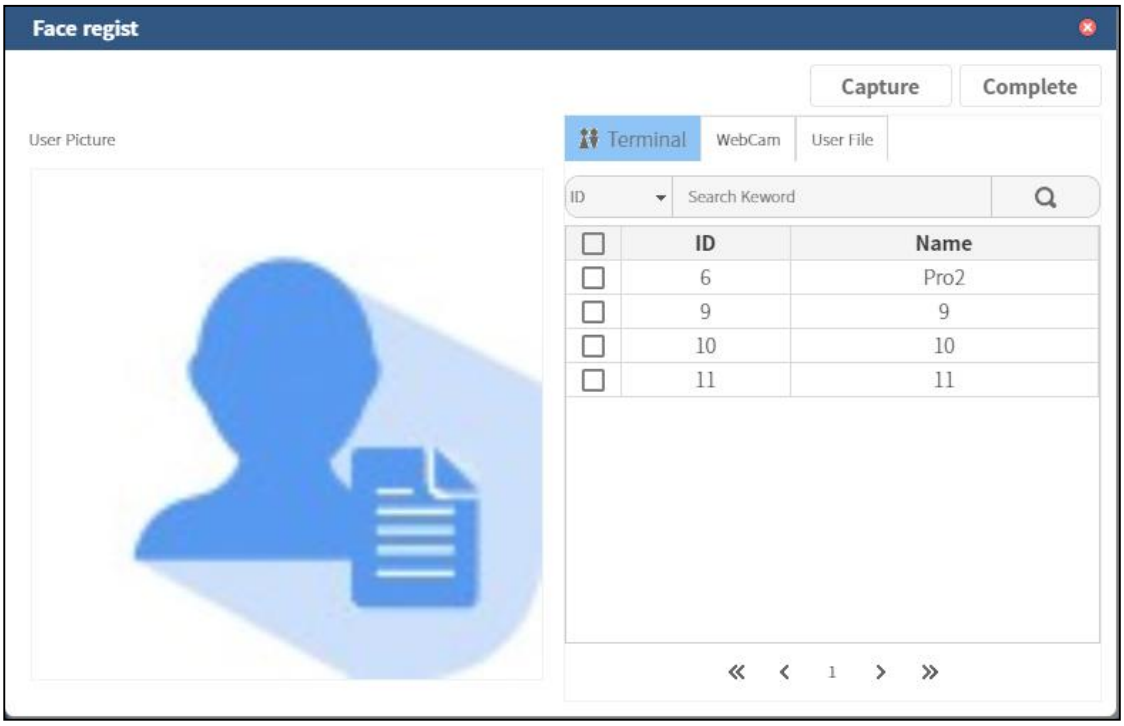
  When you click 'Hamster' tab, register fingerprint from Hamster such as FOH02. The additional program is required for register fingerprint with Hamster.

- **Face Data:** Register the face data. [**Edit**] button is activated when there is a face in the authentication type.



- **General registration**: Register the face 5 times according to the guide.
- **Add**: Add the face. When clicking this button, the face registration starts via the checked terminal.
- **Re Enroll**: Remove the current face data and enroll it again.
- **Delete:** Remove the registered face data.
- **Complete:** Save the face data on the user information. Click **[Save]** button from user info to send the data to the server.

- **Face Data (FAW)**: Register the users' face for Walk-through terminal. [**Edit**] button is activated when there is Face (FAW) in the authentication type.



- **Terminal:** From UBio-X Pro2 terminal, scan user's picture and register it.

  After checking the terminal to scan the picture and clicking the **[Capture]** button, the picture capture screen will pop up on the terminal. After capturing the picture on the terminal, click the **[Finish]** button to reflect it in user information.

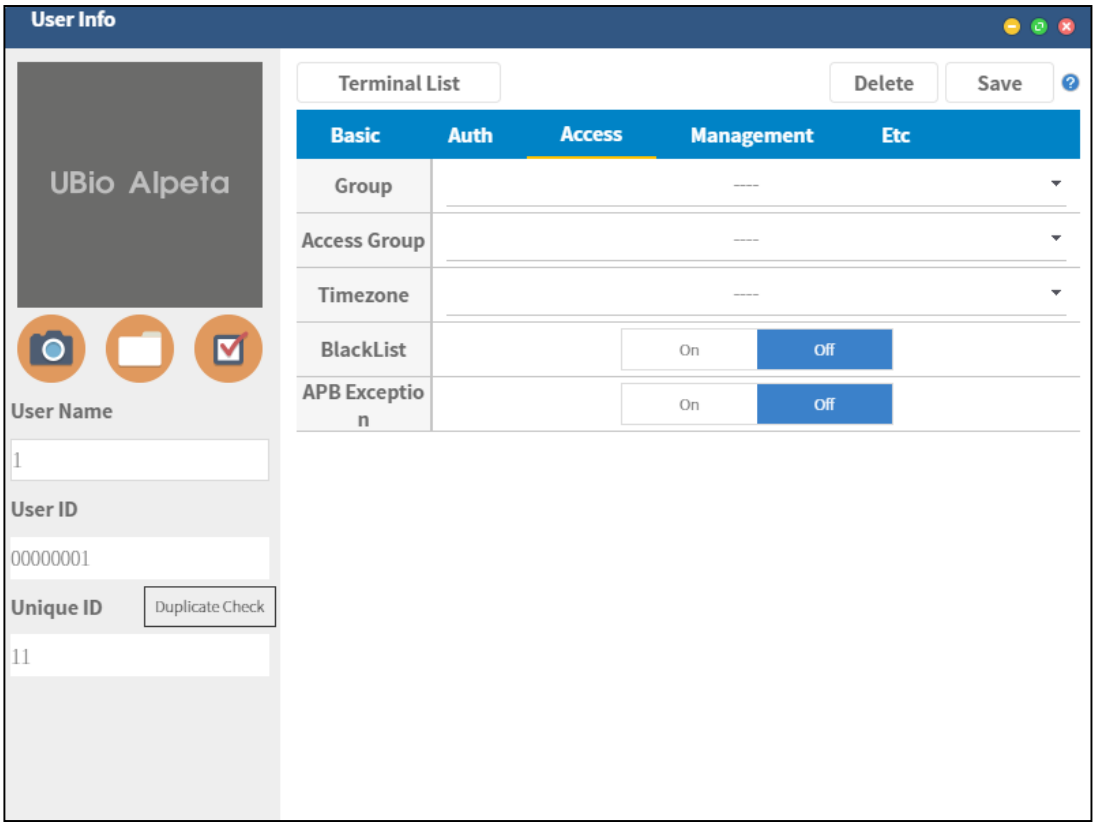
- **Webcam:** If a webcam is connected to the user's PC, the user's picture can be registered via the webcam. The webcam preview screen is displayed on the screen. When you click **[Capture]** button, a preview screen is displayed on the user picture item. Click the **[Finish]** button to apply the captured photo to the user information.

- **User file:** If you have a user photo as an image file, you can register with this file.

  If you click the **[Find File]** button, the file selection window pops up. When you select a user photo file to use, the user photo is displayed on the right. When you click the **[Capture]** button, a preview screen is displayed on the user picture. Click the **[Finish]** button to apply the captured photo to the user information.

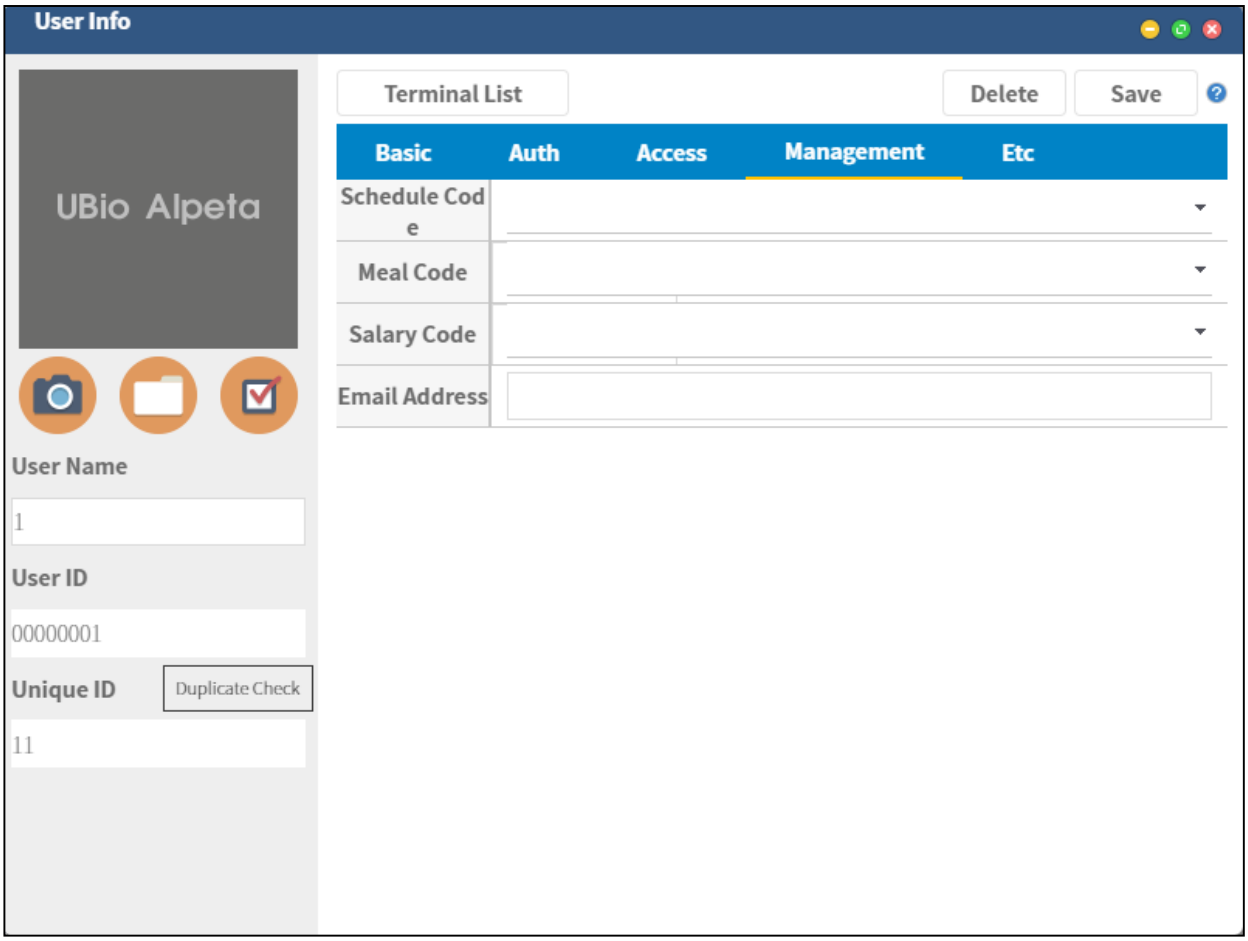
  Click **[Finish]** button to reflect the user's photo in the user information, and then click the [**Save**] button in the [**User Information screen**] to request the server to save the changes.

③ Access



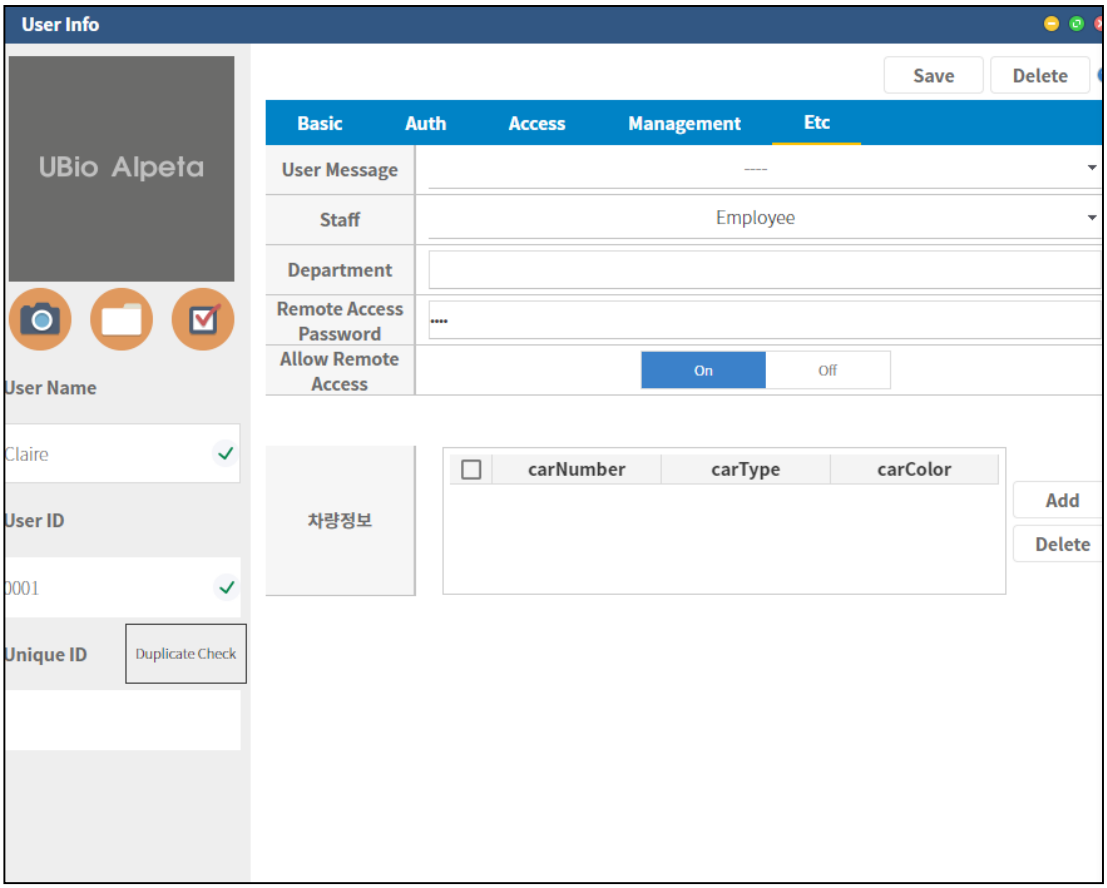
- **Group:** Set the group of user.
- **Access Group:** Set the access group of user.
- **Timezone:** Set the time zone of user.
- **Blacklist:** Set whether to apply the blacklist for the user. If setting 'ON' it is applied as a blacklist.
- **APB Exception:** Set whether to apply the Anti-passback exception for the user. If setting 'ON', it applies this option for the user.

④ **Management**



- **Schedule Code:** Set TNA code.
- **Meal Code:** Set Meal code.
- **Salary Code:** Set the payment code
- **Email address:** Enter the user's email address.

⑤ **Etc.**

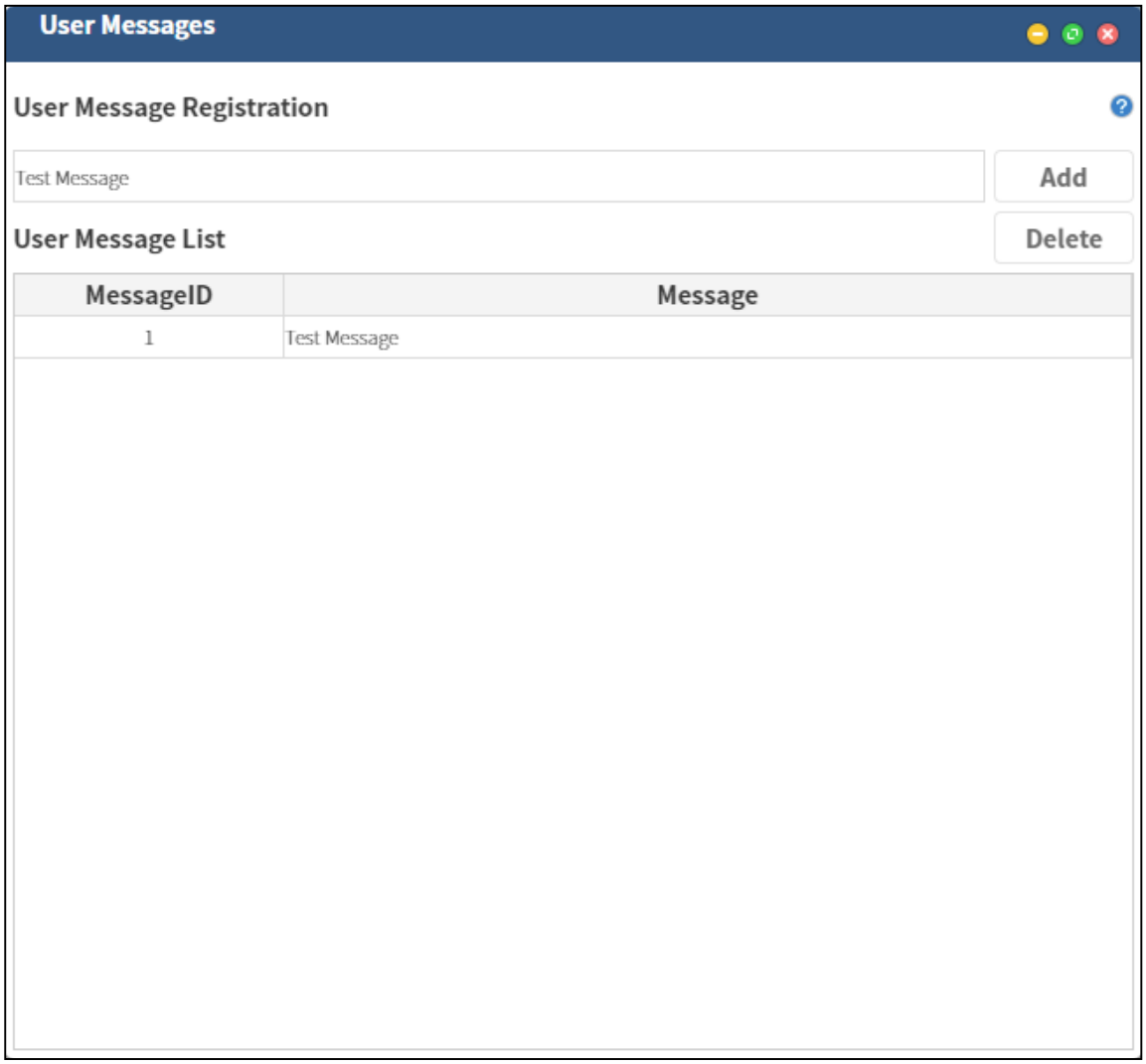


- **User message:** Set the user message.
- **Staff:** Set the position of staff.
- **Department:** Set the department.
- **Remote Access Password**: Enter the login password for the user. This password is to log in Alpeta.
- **Allow Remote Access:** Give the permission so that the user can log in. If the users' privilege is user, it basically doesn't allow to log in.

⑥ User Messages

It is the feature to set the user message.

It can register, modify, or delete the message displayed on the terminal when the user successfully authenticates on the terminal.

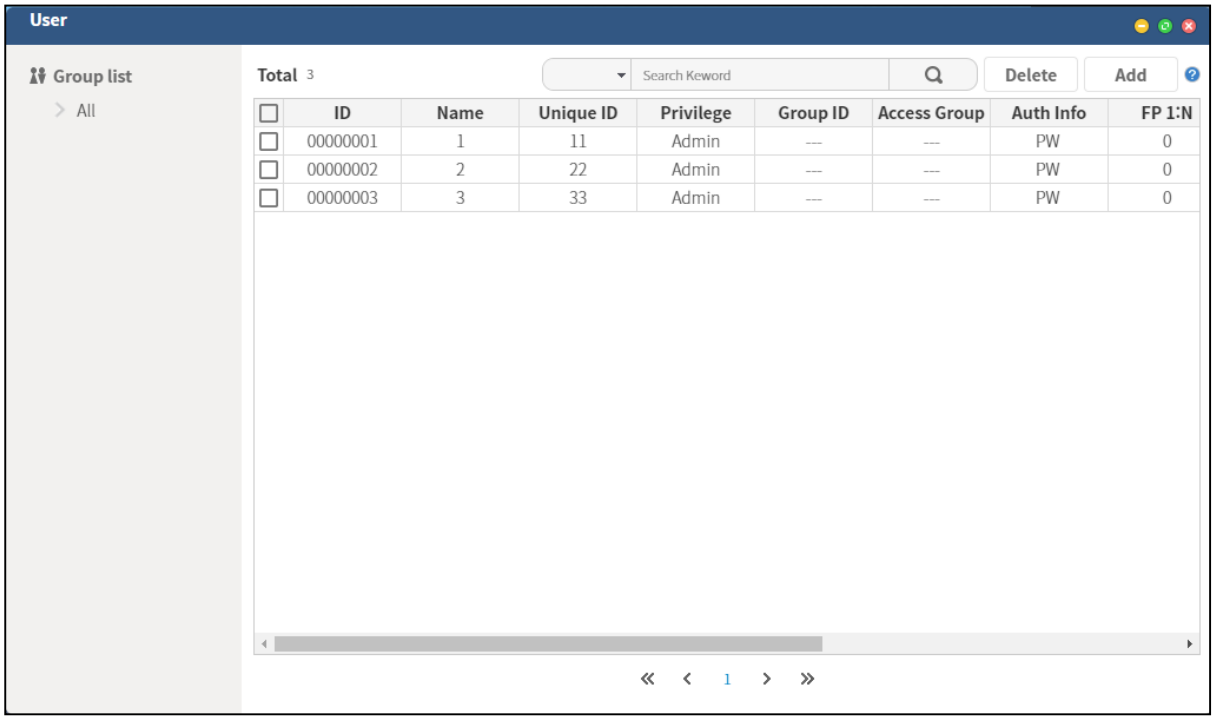


- **User Message Registration:** Enter the user message to register.
- **Add:** Register the user message on the server.
- **Modify:** Click this button to modify the message.
- **Delete:** Delete the registered message.

⑦ User management

It is the feature to manage users in user list.

It can search the user in user list, and add or delete the users.



- **Add:** Add the user and show the pop-up window to add the user.
- **Delete:** Check the user to delete and delete them.
- **Group List:** Group list is shown in the left side. When you select a group, only users in the group can be seen.
- **ID:** Display the ID of user.
- **Name:** Display the name of user.
- **Unique ID:** Display the unique ID of user.
- **Privilege:** Display the privilege of user.
- **Group ID:** Display the group ID of user.
- **Access Group:** Display the access group ID of user.
- **AuthInfo:** Display the authentication information of user.
- **FP 1:N:** Display whether to use 1:N FP feature of user.
- **Face 1:N:** Display whether to use 1:N Face feature of user.
- **Timezone:** Display the timezone information of user.
- **Blacklist:** Display if the user is blacklist or not.

- **Registration Date:** Display the registration date of user.
- **Expiration Date:** Display the expiration date of user.
-

: Select the category and enter the keyword to search the users.

24. Wiegand

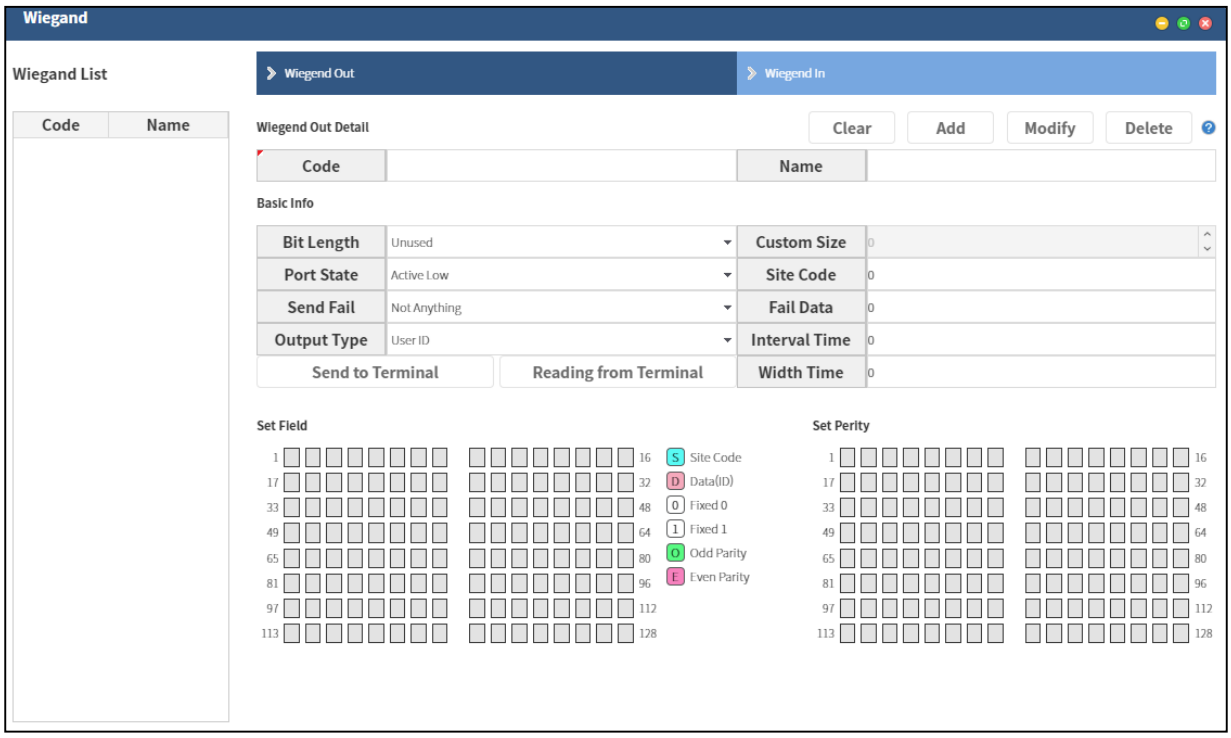
In order to connect Wiegand card reader or external devices to your terminal, you have to put setting values.

Users can set both of Wiegand in and Wiegand out.

Not only for standard 26bit or 34bit cards, but you can also set your terminal for various types of cards.

Moreover, you can also change Parity, bit length, data field, and etc. to adjust your terminal to your condition.

1) Wiegand Out



- **Bit Length**: length selection
  - Unused: when deactivated
  - St. 26bit: for a standard 26bit card
  - St. 34bit: for a standard 34bit card
  - Customize: choose this option when your card type is uncommon
- **Port State**: Active Low(default) / Active High
- **Send Fail:** if you want to send a message for both of failed authentication and successful authentication.
  - Not Anything: deactivated

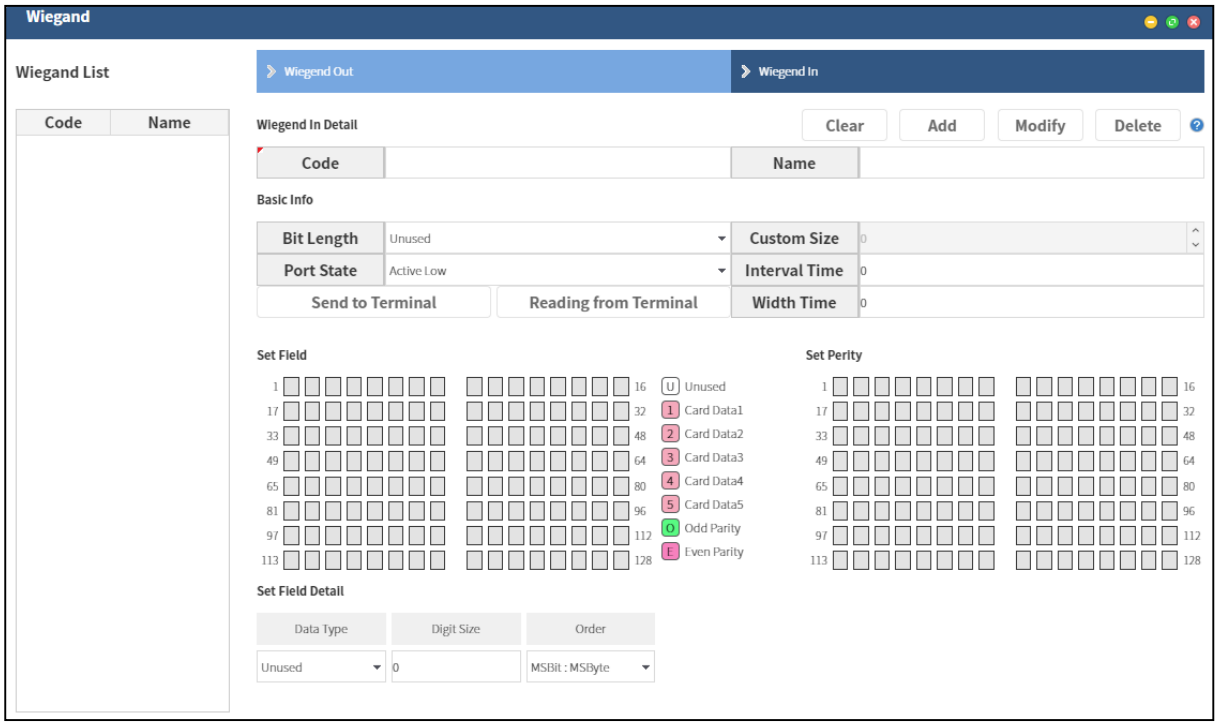
- Send Fail Data: when you want to send data of failed authentication
- Invert Parity: while failure signals are being sent, it inverts E/0 into 0/E (E: Even Parity / O: Odd Parity)

- **OutPut Type**: select data types that you want to extract (User ID / Card Serial)
- **Custom Size**: length selection when Bit Length option is set as [Customize] (range: 1~128bit)
- **Site Code**: when you want to set one for each (terminal setting range: 0~255)
- **Fail Data**: when Send Fail's option is set to [Send Fail Data], choose data format of the transmitted failure signals.

  (Tip: when Fail Data is set as 1234 1=SiteCode/234=UID)
- **Interval Time(us)**: 0 (default value = 2ms)
- **Width Time(us)**: 0 (default value = 50 μs)
- **Set Field**: Select an item on the right side first before you set the value.
  - S : 1byte (= 8bit)
  - D : User ID data, set length to the number of digits
  - 0 : select this when you want the Data value fixed at '0'
  - 1 : select this when you want the Data value fixed at '1'
  - O : Odd Parity bit
  - E : Even Parity bit
- **Set Parity**
  - To set the accuracy verification range of Even Parity and Odd Parity

  (Tip: 26bit =set 12bit except for Even Parity + set 12bit except for Odd Parity)

2) Wiegand In



- **Bit Length**: length selection
  - Unused: when deactivated
  - St. 26bit: for a standard 26bit card
  - St. 34Bit: for a standard 34bit card
  - Customize: choose this option when your card type is uncommon
- **Port State**: Active Low(default) / Active High
- **Custom Size**: length selection when Bit Length option is set as [Customize] (range: 1~128bit)
- **Interval Time(us)**: 0 (default = 2ms)
- **Width Time(us)**: 0 (default = 50~100 μs)
- **Set Field**: Select an item on the right side first before you set the value.
  - 1 : input data 1
  - 2 : input data 2
  - 3 : input data 3
  - 4 : input data 4
  - 5 : input data 5
  - O : Odd Parity bit
  - E : Even Parity bit

    - Set Parity: To set the accuracy verification range of Even Parity and Odd Parity
- **Data Type:** Card Data type selection regarding [**Set Field**]
    - Unused: When deactivated
    - Binary: When it's written in binary
    - Decimal String: When it's written in decimal
    - Hexa String: When its' written in hexadecimal
- **Digit Size**: The number of digits
- **Order**: The data transmission type
    - MSB: It is transmitted in order from the beginning to the end.
    - LSB: It is transmitted backwards from the end to the beginning.