Version No: 1.0.0
December, 2016.

Facework User's Manual

(Model No: FW-N10)

A1 COMMUNICATIONS KOREA

This page intentionally left blank.

Revision Sheet

Release No.	Date	Revision Description
Rev.1.0.0	12/12/2016	Release the Facework User’s manual V.1

Table of Contents

Chapter 1. Understanding of the Face Recognition Technology

Chapter 2. Introduction of the Facework

Chapter 3. Operation Guide for the Facework

Chapter I

Understanding of the Face Recognition Technology

This chapter describes the basic information about face recognition technology that is necessary to understand the Facial recognition device.

1. Face recognition process

First of all, all users reading this manual need to understand the operating principles of the face recognition device. Most important of all, the basic knowledge of face recognition process is especially required for better usage of the face reader device.

Independent of the solution vendor, face recognition is accomplished as follows:

① A digital camera acquires an image of the face.

② Software locates the face in the image, this is also called **face detection**.

③ When a face has been selected in the image, the **software analyzes the spatial geometry**. The techniques used to extract identifying features of a face are vendor dependent. In general, the software generates a template, this is a reduced set of data which uniquely identifies an individual based on the features of the face.

④ The generated template is then **compared with a set of known templates** in a database (identification) or with one specific template (verification).

⑤ The software calculates a score which indicates how well two **templates match**. It depends on the software how high a score must be for two templates to be considered as matching, for example an authentication application requires low FAR (False Acceptance Rate) and thus the score must be high enough before templates can be declared as matching. In a surveillance application however you would not want to miss out on any fugitive criminals thus requiring a low FRR (False Reject Rate), so you would set a lower matching score and security agents will sort out the false positives.

2. Authentication types

All of biometric devices including face recognition device have 2 types of authentication, which are described below.

- Identification
  - It is a synonym of '1 to many'.
  - The one-to-many process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the identity of the enrollee whose template was matched. The biometric system using the one-to-many approach is seeking to find an identity amongst a database rather than verify a claimed identity. Contrast with 'Verification'.

    - Simply stated, a person doesn't have to provide any input other than their biometric.

- Verification
    - It is a synonym of '1 to 1'.
    - The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. Contrast with 'Identification'.
    - Simply stated, a person swipes a card or enters a user code to select a biometric template to match against.

3. Measuring biometric effectiveness

There are 2 commonly used gauges for measuring the effectiveness of biometrics matching technology.

- False Rejection Rate (FRR): It is also known as False Non-Match Rate (FNMR). FRR is a value that measures the percentage of times a biometric sample is matched against a single or multiple biometric templates where a biometric template exists but the likeness between the sample and template is below the decision threshold setting so no match occurs.
  Put simply, it's the number of times people do not get identified when they should be identified.

- False Accept Rate (FAR): It is also known as False Match Rate (FMR). FAR is a value that measures the percentage of times a biometric sample is matched against a single or multiple biometric templates where a biometric template does not exist but the likeness between the sample and template is above the decision threshold setting so a match incorrectly occurs.
  Put simply, it's the number of times people get identified when they should not be identified.

4. Face recognition product types

Face reader products using a face recognition algorithm can be classified into two types. One is an embedded face recognition HW device and another is the SW product. The features of each product are as follows:

- Embedded Face recognition HW device: This is mainly used for a strict user authentication such as access control or time attendance. It generally uses infrared rays as light source that is necessary for detection of a face, which can enable the face reader to detect a face in the darkness.

- Face recognition SW product: This solution is generally used for the purpose of surveillance to find similar faces with matching score. Thus, it has an excellent ability to scan and compare multiple faces simultaneously. However, one of disadvantages is its accuracy and performance can be heavily affected by external light source because it uses visible light sources to detect video images.

  SW based face recognition product group generally works together with IP-CCTV or DVR as video input sources. The major application areas are Customer Relationship Management, Criminal Investigation and many others.

5. Why the Facework face recognition device

Unlike other face recognition devices, the Facework device has adopted many innovative cutting-edge technologies to maintain high reliability and accuracy.

- A specially designed Dual camera and Even light source patented technology

  As aforementioned, the Facework device uses infrared rays as light source. To eradiate enough infrared rays to the face, it arranged 48 units of LEDs around the IR camera emitting infrared rays and applied an even light source patented technology to capture better quality of face image.

  ⚠ Even-light source patented technology: It has a specially designed diamond pattern on the reflection plate placed at the back side of IR lights. The diamond pattern generates diffused reflection that can eradiate the IR lights to the face more evenly than direct lights. This even light source technology is greatly helpful to get high quality of face image.

- Intelligent template update

  One of disadvantage of face recognition technology is to require re-enrollment of the face periodically because the human-being face shape is usually being changed over times. To avoid this vexatious task, the Facework applied the intelligent template update technology. Whenever a user tries to get authenticated from the Facework, it always compares the sample template created at the recognition time with the enrolled templates. If it finds the quality of the image in the sample template is better than that of enrolled template, it automatically replaces the poorest image in the enrolled template with the new one of sample template. This feature can easily trace the face shape changes over times and keep the up-to-date face template without re-enrollment of face.

- Adopted market-proven face recognition engine

  Most of face recognition device manufacturers claim that they provide an excellent recognition performance and accuracy. It may be sometime true because its performance can usually satisfy customer's expectation in a small user group. But when it comes to a large user group, the story can be different as its accuracy and performance have much variance by the quality of face recognition algorithm. In order to minimize the variance, the face recognition algorithm should be fully optimized and proven in the large user environment. Our 'Face +' face recognition engine adopted to the Facework has been fully tested and optimized in 2K+ user environment with 1 to many authentication mode. The 'Face +' face recognition engine is certified by KISA (Korea Internet and Security Agency) sponsored by Korea government.

- Technology to make a precise template

  Unlike other face recognition devices, the Facework builds precise template with using more than 8,000 face features lying on virtual line linking 5 face landmarks.

  Additionally, 'Face +' engine applied 'state-of-the-art' normalization technology to minimize the processing time although it has more facial features than others.

  Thanks to these two technologies stated above, it makes high quality of template that can identify a face precisely.

This page intentionally left blank.

Chapter II

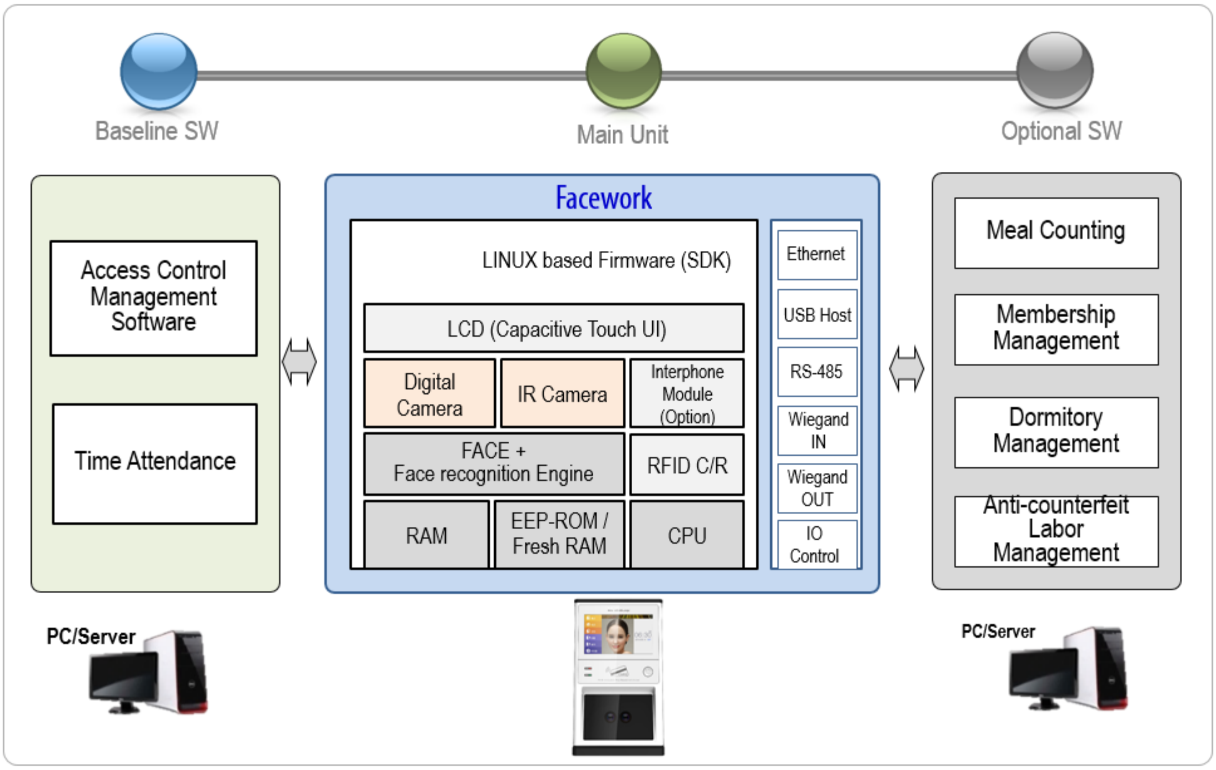
Introduction of the Facework

This chapter describes the basic information required to use the Facework. Please read this Chapter carefully to use full features of the Facework and keep consistent performance.

1. Basic Understanding of the Facework

1.1. Architecture

The Facework device package consists of Main device unit, baseline software and optional software. Its architecture is as follows:

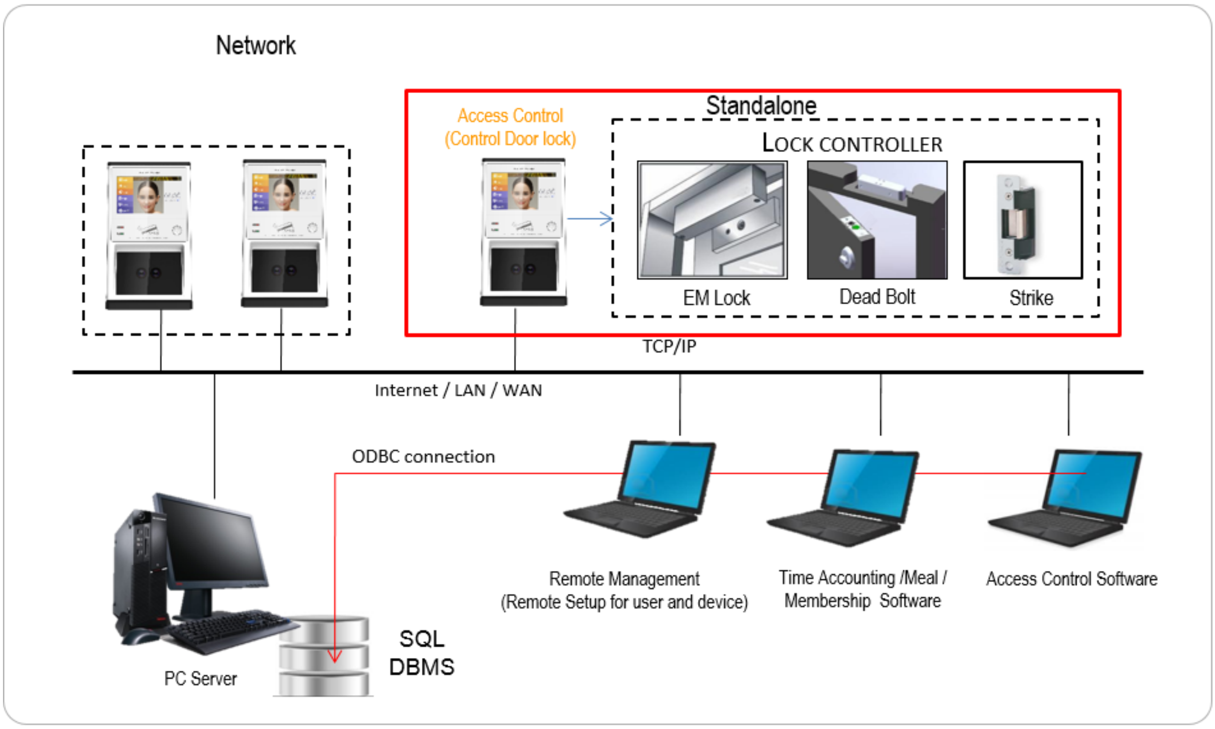


1.2. Configuration

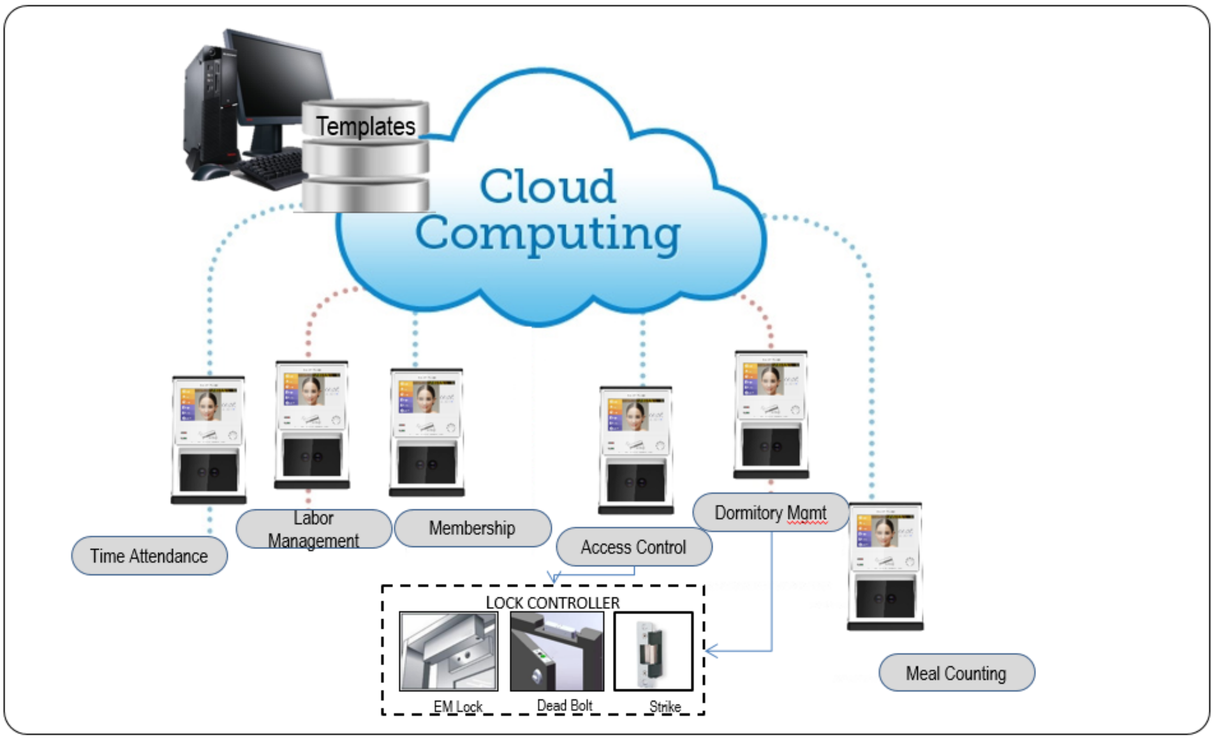
The Facework device can be configured with 3 types: Standalone, Network and Cloud (Optional).

- Standalone: The Facework device runs alone without network connection. Then all face registration, authentication and device management can be done on the Facework. Data and log files can be moved thru USB memory.
- Network: Single or multiple Facework devices are connected to Ethernet. In this environment, each Facework device needs to be configured with proper network parameters. Thru ACMS software, it can be controlled and managed from remote PC.

But all face capture, detection & comparison tasks are executed by each Facework device.



- Cloud: It is optional feature supported by Facework cloud add-on module. In this configuration, all user templates are saved to the server storage. The Facework device executes only face capture, detection, template build and door control. In usual, the Facework device sends user template to the server, installed the face comparison module, and then the server module compares the template from the device with enrolled templates stored in the server. After comparison is complete, it returns the result to the Facework device for taking a proper action such as door control.



1.3. User types

In order to use the Facework device properly, the Facework manager, in charge of managing this device needs to understand the Facework user types and authentication modes before operation.

Generally, the Facework has two type of users holding different privilege as follows.

① User: It is a general user group only executing self-authentication without any Facework management function.

② Manager: It is a special user group that can execute all of Facework management functions. The Facework uses two types of manager by assigned privilege.

a. Super manager: It has full privileges to execute all control & management functions for the Facework device. The Super manager can;

- Add / Modify / Delete manager(s).
- Add / Modify / Delete user(s).
- Manage all parameters with relevant to authentication, network, log, IO and others
- Show the Facework device information.

b. Manager: It has limited privilege for the Facework device. The Manager can;

- Add / Modify / Delete user(s).

⚠ The Facework can have up to 10 managers with combination of Super managers and Managers.

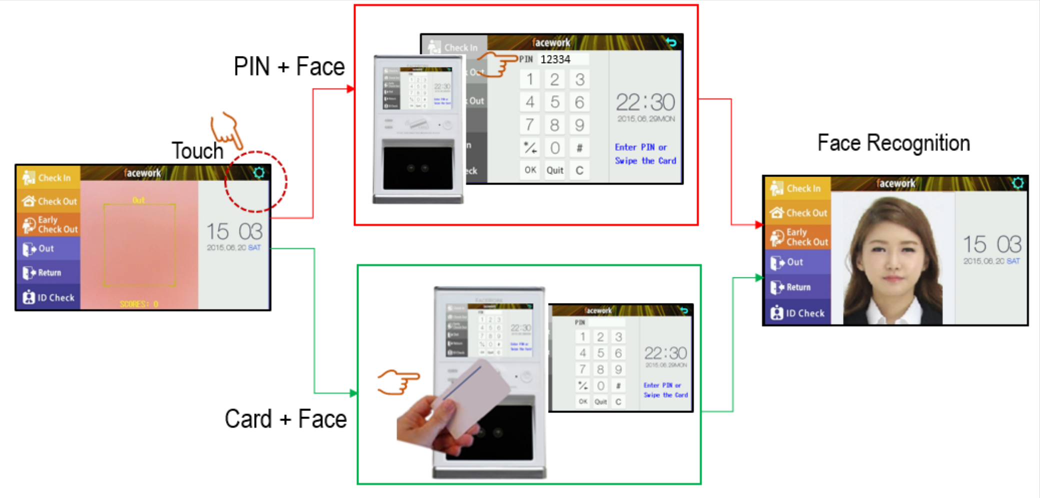
1.4. Authentication modes

The authentication mode is set at face enrollment time and can be assigned differently by use type and its security level. Anyone trying to access the Facework device should get authenticated with a proper authentication mode.

① Super manager or Manager: There are 4 available authentication modes for this Manager group and the Facework manager can assign a proper one at the Manager enrollment time.

a. PIN+Face: This mode enables two phase authentications. When Super manager or Manager with this mode tries to get authentication, it requires PIN code input prior to face recognition. The PIN code is set at the enrollment time [Figure 1].

b. Card+Face: It is a similar mode to “PIN +Face”. This authentication mode requires swiping of the RFID card instead of entering PIN code when to get authentication [figure 1].



➢ Authentication Step

- PIN + Face : enter PIN code
- Card + Face : swipe the Card

Try to get face authentication

[Figure 1] Authentication process when the Manager has ‘PIN + Face’ or ‘Card + Face’ authentication mode

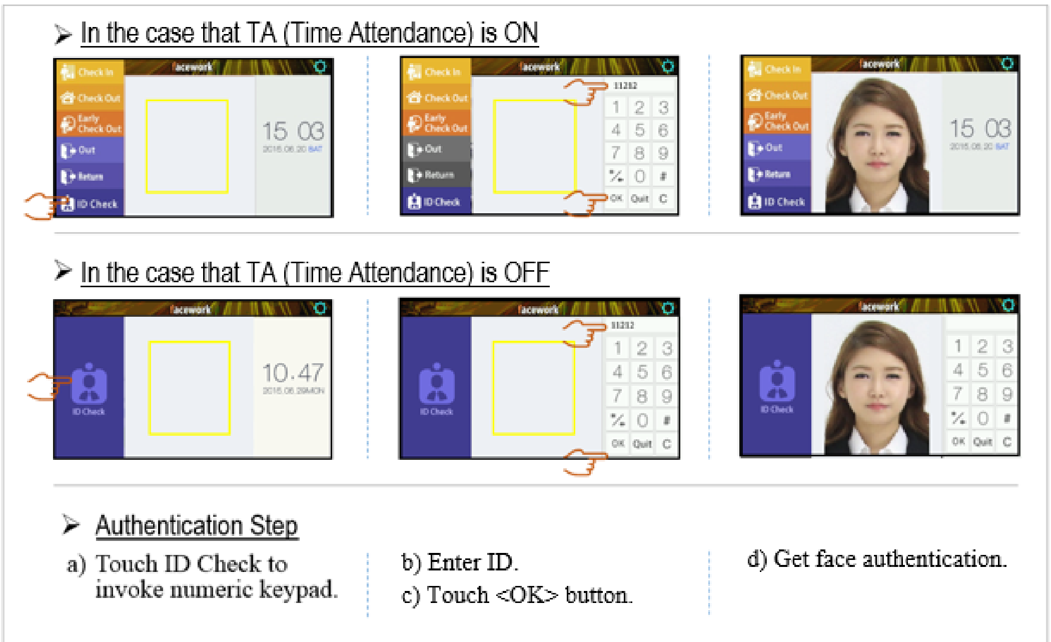
c. Face Only: It enables a single phase authentication and can access the Facework with only face authentication.

d. Card Only: The Manager can get the right to access the Facework with only swiping the RFID card on the card reader. This mode has the weakest security level, and thus it is not usually recommended as manager authentication mode.

② User: There are 6 available authentication modes for the user group and the Facework manager can assign a proper one at the User enrollment time.

a. ID +Face: This mode enables 1 to 1 authentication type. Thus, when the user assigned this authentication mode tries to get authenticated, it has to enter ID before the face recognition. In this authentication mode, the Super Manager or Manager should get the authentication with following steps.

b. Card+Face: It also enables 1 to 1 authentication type that is a similar to ID +Face.



➢ In the case that TA (Time Attendance) is ON

➢ In the case that TA (Time Attendance) is OFF

➢ Authentication Step

a) Touch ID Check to invoke numeric keypad.

b) Enter ID.

c) Touch <OK> button.

d) Get face authentication.

[Figure 2] Authentication Mode: When the User has 'ID + Face' authentication mode

This authentication mode requires swiping of the RFID card instead of entering user ID when to get the authentication. To understand how to authenticate at this mode, refer to [Figure 3].

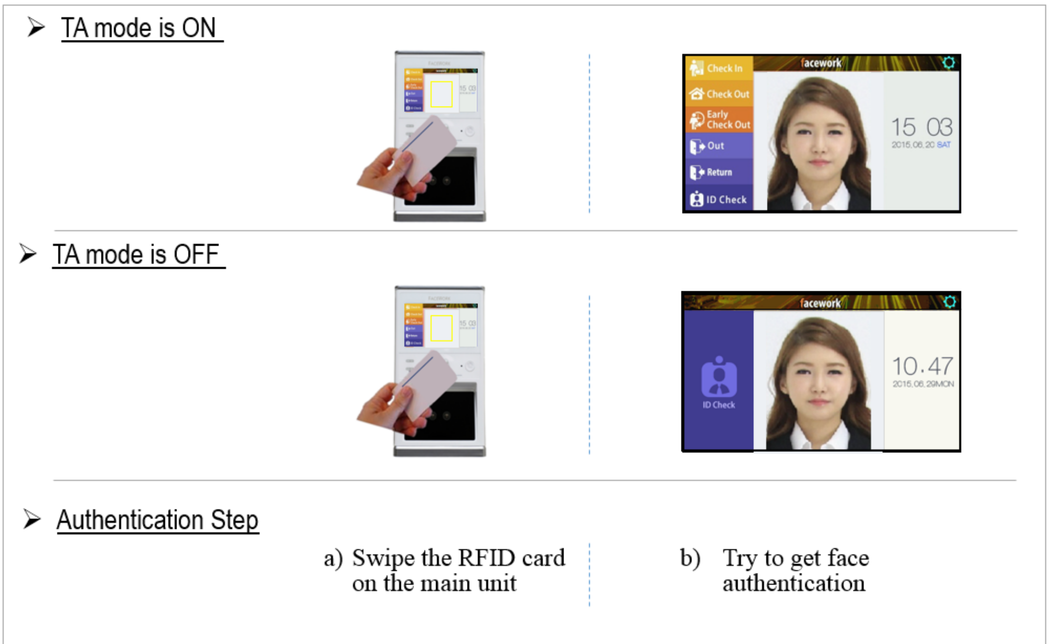
c. Face Only: It enables 1 to many authentication type. It is a single phase authentication that has been mostly used for the Facework. The user can get simply authenticated with the face only.

d. Card Only: The user can get authenticated by only swiping the RFID card without face authentication. This is somewhat useful for temporary visitors or some environments that face enrollment is not easy.

e. Card or Face: The user can get authenticated with either Face or RFID Card.

f. Card + Face Log: This mode enables the user to get authenticated with only RFID Card. But a difference from 'Card Only' is that the Facework additionally takes a picture for the user face when to try authentication and saves it to the log file. Although this mode allows the user to get authenticated with the card only, it can be more secure than 'Card Only' as it additionally logs the face photo taken at access time. It can be a kind of complementary measures to cover the weakness of card only authentication.

For easy operation of the Facework device, the Facework applied consistent UI operation style as follows:



[Figure 3] Authentication Mode: When the User has Card + Face authentication mode

1.5. UI operation style

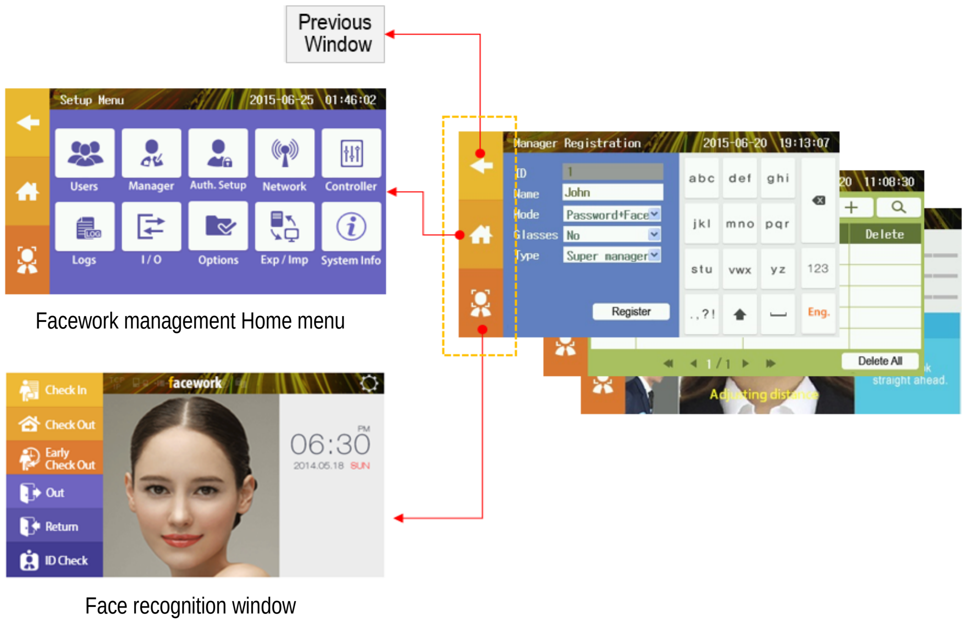
① Mode Selection Zone:

All of the Facework windows except for the ‘Face Recognition’ have Mode Selection Zone that consists of 3 different buttons.

← : This button always moves current window control to the previous window.

⌂ : This button always moves current window control to the Facework management home menu (Setup Menu).

👤 : This button always moves current window control to the face recognition window.



[Figure 4] Mode Selection Zone

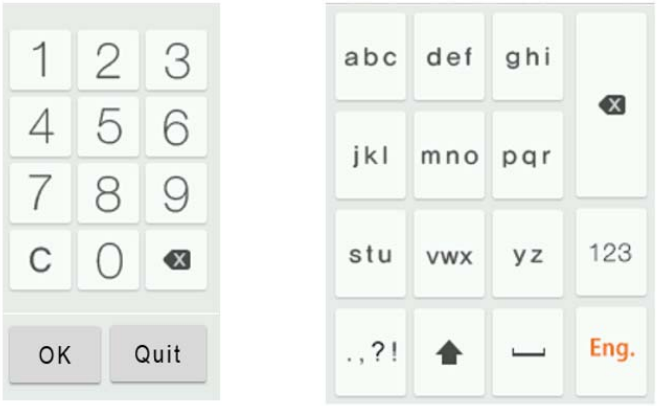
② Keypad Zone

Whenever input value is required, the Facework automatically pops up a proper keypad in the Keypad zone. The Facework has two types of keypad as follows:

a. Dedicated Numeric Keypad: It is composed of the numeric keypad and the command button. The numeric keypad is for the necessity of entering numeric data and the command buttons consisting of <OK> and <Quit> decide whether to save the entered values or discard them.

In the numeric keypad, the key C clears all data at input fields and the key ⌫ deletes 1 digit repeatedly whenever the key is touched.

b. Alphanumeric Keypad: This keypad allows to input all numeric and all characters. Whenever alphanumeric characters are required to be entered from the Facework UI, it automatically pops up this keypad on the screen. In order to exit from the keypad after the input is finished, touch any point outside of it. In this keypad, the key ⬆ is used for switching uppercase to lowercase or vice versa.



<Dedicated Numeric Keypad> <Alphanumeric Keypad >

[Figure 5] Keypad Types

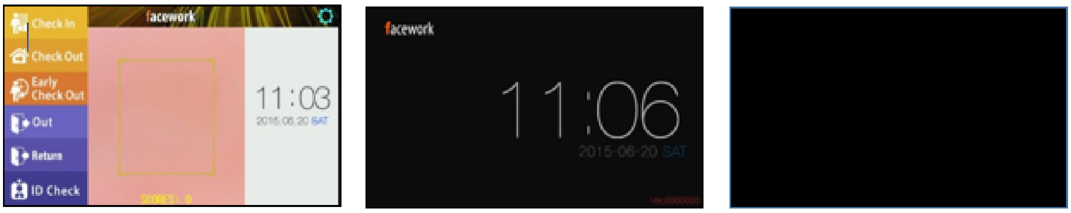
1.6. Operation modes for the Facework

The Facework has 3 different operation modes for the purpose of device protection. The Facework automatically changes the mode depending on the authentication activity.

① Face Recognition Mode: It is the active mode that can promptly recognize user face. The Facework automatically goes into the Standby mode when it detects nothing for 25 seconds.

② Standby Mode: It is the hibernating mode that can immediately turn to the face recognition mode when a user tries the face authentication. When the Facework goes into this Standby mode, the device displays only current data and time on the screen.

③ Screen Off Mode: If no user recognition is detected for 120 seconds after the standby mode, it automatically goes into the Screen off mode. But the device immediately activate the face recognition mode when it senses any object approaching the device. In order to use this feature, ‘Screen Off Mode’ should be turned on in the System option.



<Face Recognition Mode> <Standby Mode> <Screen Off Mode>

[Figure 6] Facework Operating Modes

1.7. Understanding the menu tree of the Facework

Note that all Facework management functions should be executed on the Setup Menu with Super manager privilege except for the User management (User management can be managed by Super manager privilege as well). As the Setup menu consists of many hierarchical sub-menus, understanding of its menu tree can save time in finding a proper function.

The Setup menu tree is organized as follows.

Class	Function	Sub-Function	Reference
Manager	Add		Page 31
	Modify		Page 34
	Delete		Page 36
	Delete All		Page 36
Users	Add		Page 37
	Modify		Page 38
	Delete		Page 39
	Delete All		Page 40
Authentication Setup	Authentication Threshold		Page 41
	Update Threshold		
	Multi-register Threshold		
	Authentication Effective time		
	Sensibility		
	Retry Threshold		
	Retry Count		Page 42
	Retry Timeout		
Network	IP Address		Page 42
	Sub-mask		
	Gateway Address		
	DNS		
	Server IP		
	Port		Page 43
Controller			Page 43
Logs	List		Page 43
	Delete All		
	Log Setup		Page 44
I/O	Door Sensor		Page 44
	Fire Sensor		Page 45
	Lock Sensor		
	Relay Signal		
	Relay Effective time		
	Door Open Timeout		
Options	Time	Standard Time	Page 46
		Set Date	
		Set Time	
		Act as NTP-Server	
		Synchronization to NTP-Server	
	Security	Super PIN	Page 46

		Cover Opened Alarm	Page 47
		Default Authentication Mode	Page 47
		Auth. Failed Alarm	
		Configuration Reset	
		Factory Reset	
	Auto Door Open	Setup	Page 47
	Event Alarm	Setup	Page 48
	Time Attendance	Check In	Page 48
		Check Out	
		Early Check Out	
		Out	
		Return	
		Mode	
		Auto Check In Mode	Page 49
		Auto Check Out Mode	
		Turn On/Off 'Out/Return'	
	Device Schedule	Create Schedule	Page 49
		Modify Schedule	Page 50
		Delete Schedule	
		Setup Special Holidays	
	User Schedule	Create Schedule	Page 52
		Apply Schedule to a specific user	
		Apply Schedule to all users	Page 53
		Remove Schedule	
		Setup Special Holidays	
	Others	Turn On/Off Keystone	Page 53
		Turn On/Off Voice	
		User Message	Page 54
		Volume Up/Down	
		Test Volume	
		Screen Off Mode setting	
		Language Selection	
Export /Import	Export T/A Log	Export	Page 54
	Export by User	Select	Page 55
		Export	
	Export All Users	Export	Page 55
	Import All Users	Import	
	Import Users (CSV)	Import	
	Extract User IDs	Extract	
	Export System Logs	Export	Page 56
	System Update	Update	
	Export Configuration File	Export	
	Import Configuration File	Import	
System Info	Network, Firmware, User #, Template #, Access Log#		Page 57

2. Recommended method for face enrollment and recognition

When to use the Facework device, it cannot be overemphasized the importance of the correct face pose at the time of enrollment and authentication to maximize accuracy and performance. So please read carefully the followings.

2.1. Recommended Face Enrollment Method

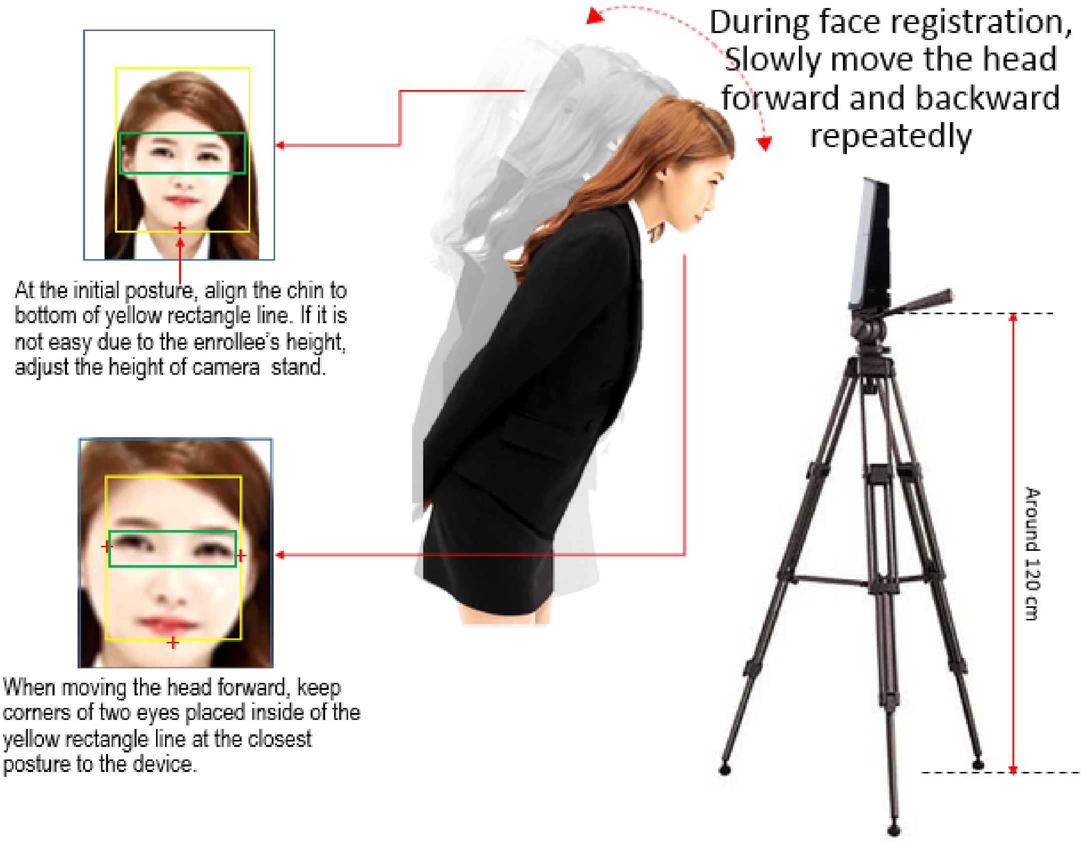
In order for accurate and fast face recognition, creation of the best quality of user template is essential. For this one, the Facework should capture high quality of pictures during the face enrollment process. If it has poor quality pictures such as eye closing, opening mouth and strange face expression, it has no choice but to create the poor quality template which negatively affects to recognition performance.

Here are some guidelines to get good quality of face images during the face enrollment process.

① Adjust the height to let the face be positioned inside the yellow rectangle on the screen.

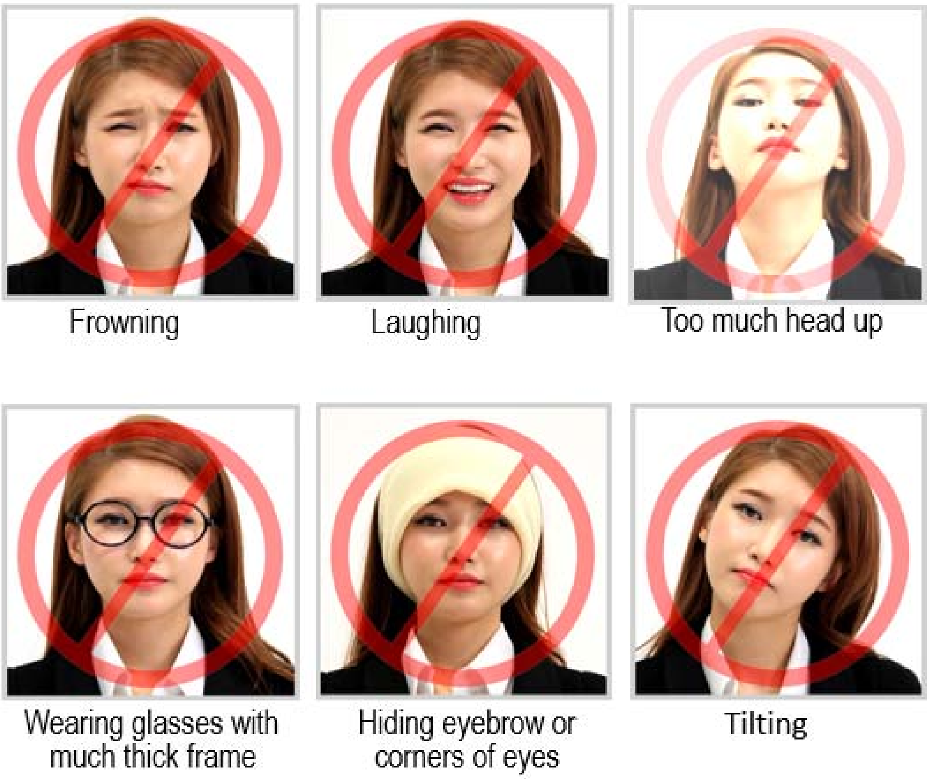
② When to register many users, using the camera tripod is highly recommended because it can easily adjust the height of the Facework device to match the user’s height.

③ During face enrollment, move your head forward and backward slowly to capture different sized face images at different face poses.


During face registration,
Slowly move the head
forward and backward
repeatedly
At the initial posture, align the chin to bottom of yellow rectangle line. If it is not easy due to the enrollee’s height, adjust the height of camera stand.
When moving the head forward, keep corners of two eyes placed inside of the yellow rectangle line at the closest posture to the device.
Around 120 cm

[Figure 7] Correct Face Enrollment

④ During face enrollment, avoid the followings.


Frowning

Laughing

Too much head up

Wearing glasses with much thick frame

Hiding eyebrow or corners of eyes

Tilting

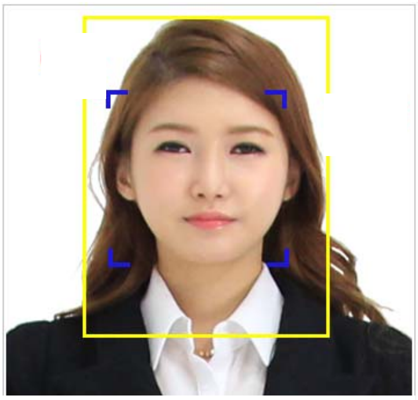
[Figure 8] Incorrect Poses during Face enrollment

2.2. Recommended Face Recognition Method

Like the face enrollment, a correct pose is also required at the face recognition time. Therefore, the Facework manager has to train users until they become familiar with face recognition method. Correct face recognition methods are guided as below.

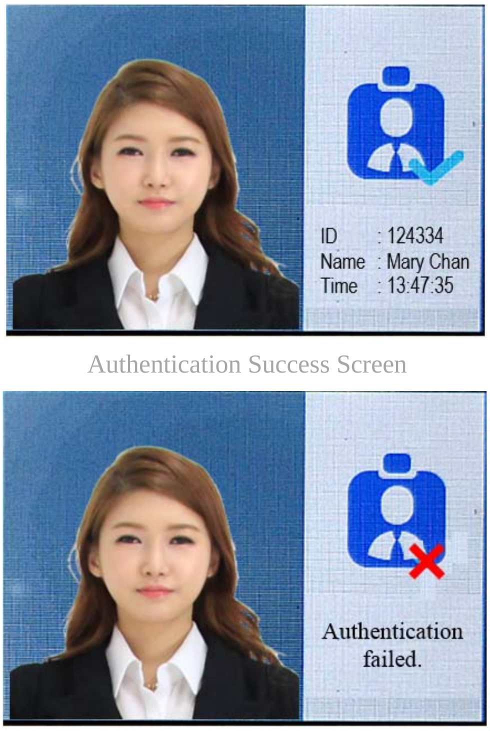
The Facework is contactless authentication device. Thus, it can identify your face at the distance somewhat away from the Facework device. Its allowable recognition distance is usually ranged from 50cm to 80cm (100cm at maximum) away from the device.

① Adjust the posture to place the face inside the yellow frame if possible [Figure 9] and slowly


[Figure 9] Correct Face position

move your head forward and backward. In most cases, the Facework device immediately recognizes the face even before moving your head.

② If the Facework device successfully authenticates the face, it shows the user profile such as the captured face image, ID, Name and turning on “Successfully authenticated” voice massage. Otherwise, it turns on “Authentication failed” voice message and shows the error symbol as depicted in [Figure 10].



ID : 124334
Name : Mary Chan
Time : 13:47:35

Authentication Success Screen

Authentication failed.

Authentication Failure Screen

[Figure 10] Authentication Results

- When the Facework detects the face at the most ideal distance, 4 blue angles are shown on the screen [Figure 9], and then it immediately starts authentication process. But if the recognition distance is not correct, red angles are shown with asking the distance adjustment in text message.
- During face authentication, when your face cannot be mostly placed into the yellow rectangle at the right distance, the position of installed device may be too much higher or lower than the user height. Then ask your Facework manager to adjust the Facework device on the right position with correct height. When the Facework is installed at the place of 120cm height from the floor, it usually covers 150cm to 180cm. For the person taller than 180cm, he /she can get authentication by bending the body toward the Facework at the somewhat longer distance than the recommendation. For the right installation of the Facework, refer to the ‘Quick installation guide’ enveloped in the Facework package.

3. Setup Network

Once the Facework device is connected to the network environment, it has to be properly configured at the network setup as the next step. For correct network configuration, refer to 5. Network Setup in Chapter 3.

4. ACMS Installation and Setup

The ACMS (Access Control and Management System) is bundled software for the Facework device. The ACMS basically includes essential functions for Access Control application and the central management and monitoring functions for the Facework device regardless of its configuration. The ACMS supports lots of management functions such as template provisioning, privilege management, device management, backup/restore of user template, filling up user profile missed at the enrollment time. For example, complete filling up user information at the Facework device is a little bit time consuming job because the screen keypad is not convenient to enter the alphanumeric characters. In this case, enter only Face ID at the device. Later, you can upload the user profile in batch mode after filling up missed fields such as your name from the ACMS. For detailed functions of ACMS, refer to the ACMS User's guide.

5. Setup Policies for the Facework Users

Before using the Facework device, the Facework manager should setup the operation policy for user and manager as follows;

① The Facework manager: The Facework has 2 types of managers. One is the Super Manager holding full privilege to access and control the Facework device, another is the Manager to have only User management privilege. Before using the Facework, more than 1 person should be enrolled as the Super manager. In the case that the Super Manager is not enrolled in the Facework device, the 1st enrolled manager is automatically set to the Super Manager. The Facework can have up to 10 Managers (including Super managers) and usually recommends to enroll 2 super managers and 1 manager against emergency case.

② Face ID Policy: Face ID policy for Users or Managers is very important. It is a kind of identification code for each face. It should be unique and surely entered at face enrollment time. When enrolling many users on multiple Facework devices in a large organization, the Facework manager should carefully assign the Face ID to whole users, not to duplicate the Face ID by mistake.

③ Employee ID /Visitor ID: This takes the role of the primary key which never allows duplication and modification. Thus, the Facework manager should carefully consider the ID that uniquely identifies each user. Employee No, Student No or SSN can be good examples of unique ID.

④ Authentication schedule by user: The Facework manager can grant or deny the authentication for all users or an individual at the specific time zone. If this option is necessary for the organization, it is recommended to create the authentication schedule before starting user enrollment. Of course, it can be applied to an individual or all users after the enrollment.

⑤ Authentication schedule by device: The Facework manager can define the time zone to grant or deny authentication by device. The time zone can be selectively applied to the day of the week or the special holiday defined by the Facework manager.

This page intentionally left blank.

Chapter III

Operation Guide for the Facework

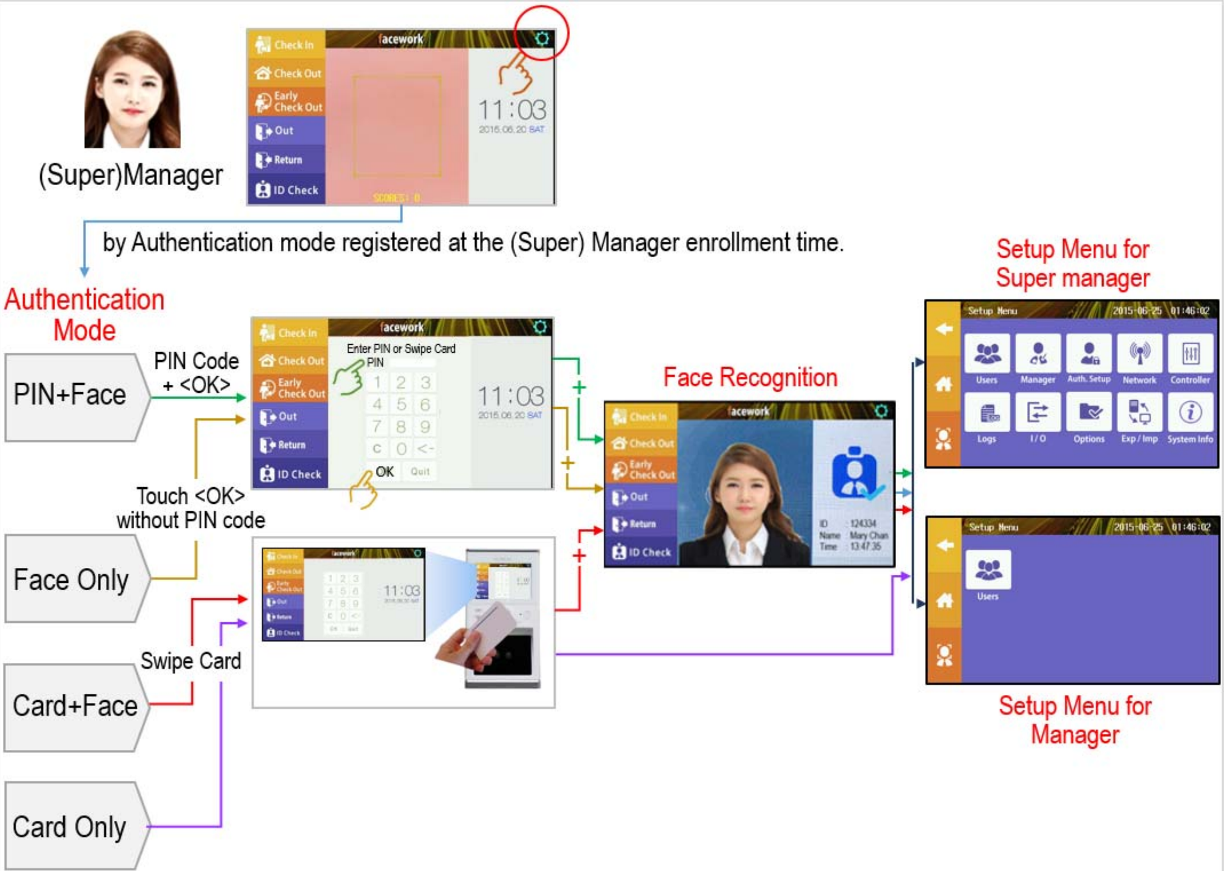
For proper use of the Facework device after installation, the Facework manager has to understand full operational functions provided by the Facework such as manager& user management (enrollment /modification /deletion), authentication mode setup and many others.

This section describes all necessary functions to setup and control the Facework device.

1. Setup Menu

The Setup Menu is a kind of control and management dashboard for the Facework device. In the Setup Menu, the Facework manager can execute all functions with relevant to the Facework control and management, which can setup user and manager profile, device backup/restore, device parameter, access log and view system information. The Facework manager can go into the Setup Menu by touching ⚙ icon, located at the right top of the face recognition screen.

The Setup menu can be accessed by any general user when the Super manager is not enrolled in the Facework device. But if the Super manager is already existed in the device and (Super) Manager touches ⚙ icon, it asks (Super) Manager to get authenticated before getting ‘Setup Menu’ [Figure 11].



[Figure 11] Manager Authentication Process when manager is already existed

2. Manager Setup

As mentioned in 1.1 of Chapter 2, the Facework has two types of managers: the Super Manager and the Manager. The Manager setup can be executed by only the Super manager.

In order to access the Setup Menu in the case that the Super Manager is already enrolled as the Facework manager, the Facework manager should get authenticated from the Facework in advance. Refer to [Figure 11].

⚠ Hereafter, 'Facework manager' means Super manager and 'Manager' represents both 'Super manager' and 'Manager'.

2.1. Add Manager

This section guides how to add the Manager to the Facework device.

The detailed steps for adding Manager are as follows;

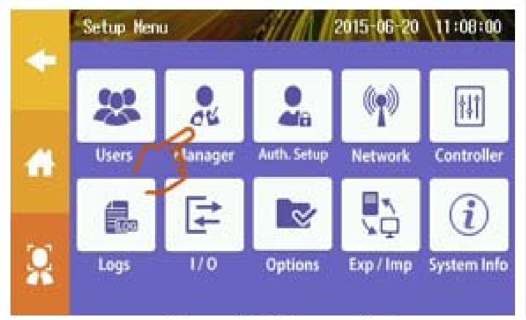
① To add new manager to the Facework, the Facework manager should get authenticated from Facework device [Figure 11].

② When the Facework manager got successful authentication, the Facework displays the Setup Menu.

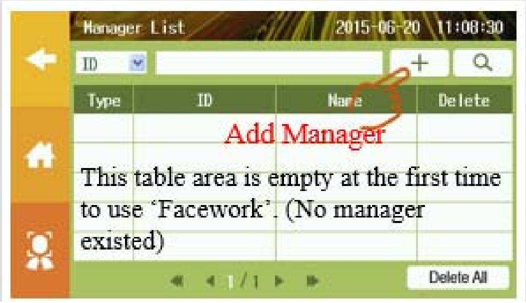
③ To add a new manager, touch 'Manager' in the Setup Menu [Figure 12], and then it shows 'Manager List' window [Figure 13].

④ Touch '+' symbol to add a new Manager [Figure 13]. Then it shows 'Manager Registration' window [Figure 14].

⑤ In the 'Manager Registration' window, enter Manager ID and Manager Name. Manager name can be optional here as the name can be filled at the ACMS software later. After it, select a proper 'Authentication mode' at the 'Mode' field [Figure 14]. For more information about manager authentication modes, refer to Section 1.2 of Chapter 2.



[Figure 12] Setup Mode



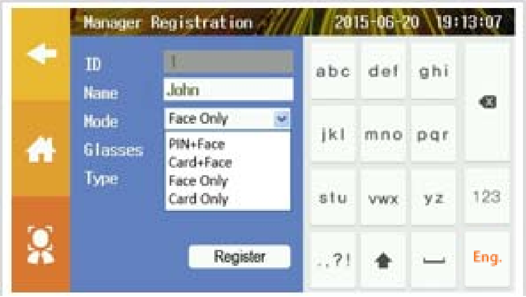
Add Manager

This table area is empty at the first time to use 'Facework'. (No manager existed)

[Figure 13] Add Manager

⑥ As the next step, select 'Glasses' option [Figure 14]. If enrolling manager puts on glasses, choose 'Yes'. However, it is usually recommended to select 'No' in most cases except that the frame of glasses are not much thick.

⑦ In the 'Type' field, choose one of two types: 'Super Manager' or 'Manager', and touch <Register> if every field value is correct [Figure 14]. As mentioned repeatedly, in the case that the Super manager is not existed, the 1st enrolled Manager is automatically assigned to the Super manager although it select 'Manager' in the type field.


Manager Registration 2015-06-20 19:13:07

ID 1

Name John

Mode Face Only

Glasses

Type

PIN+Face
Card+Face
Face Only
Card Only

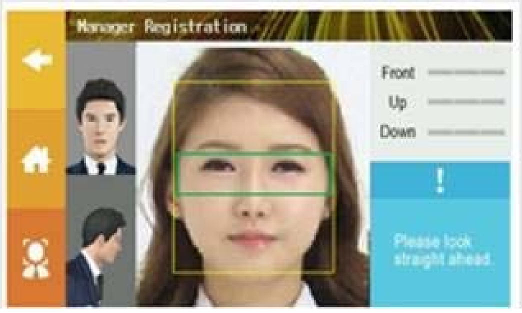
[Figure 14] Manager Enrollment

⑧ Except for the selection of 'Card Only' at 'Mode' field, the Facework starts face enrollment process. During enrollment process, it takes total 9 pictures at 3 different face poses: face front, face up and face down in order. If the enrolling manager is chosen to use 'Card only' at 'Mode' field, skip following face enrollment steps and directly go to Step⑩. Otherwise, continue the following steps.

a. At the first time, the Facework device takes 3 pictures at front face. The Facework asks you to position your eyes inside the green rectangle with "Please position your eyes in the box" voice message. When it detects your face correctly, it starts taking pictures 3 times [Figure 15].

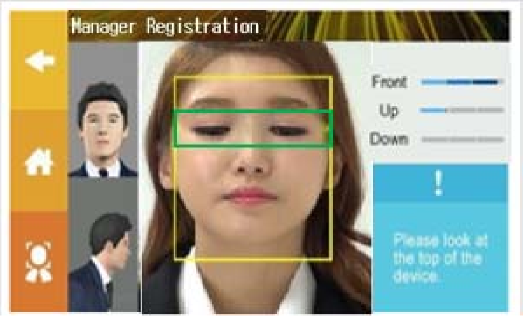
b. The green rectangle moves up with "Please look upward slightly" voice message. Then position your eyes correctly as guided. Like step (a), it takes another 3 pictures at this posture [Figure 16].

c. Lastly, the green rectangle moves down with "Please look downward slightly" voice message. Again position your eyes inside it, and then the Facework takes pictures 3 times at this pose [Figure 17].


Manager Registration

Please look straight ahead

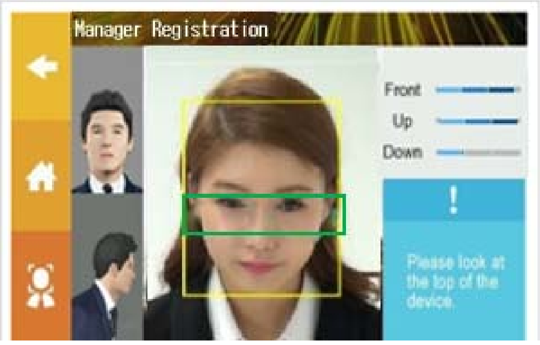
[Figure 15] Take picture at Face front pose


Manager Registration

Please look at the top of the device

[Figure 16] Take picture at Face up pose

⑨ In Step⑤, if 'PIN+Face' is selected as authentication mode, the Facework will ask you to enter PIN code at the next window after finishing the face enrollment process. Then enter password at the 'PIN code' field and reenter same password at the 'Confirm' field [Figure 18]. After it, touch <OK> button to save it and go to the step ⑬. Otherwise, touch <Quit>.

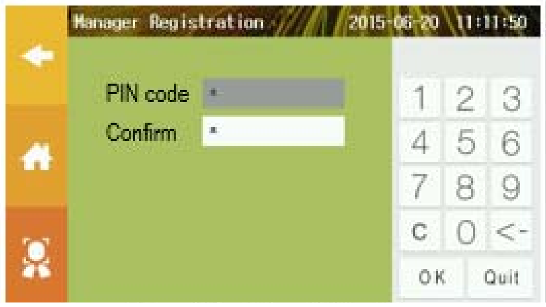


Please look at the top of the device.

[Figure 17] Take picture at Face down pose

⑩ In Step⑤, if 'Card+Face' is selected as authentication mode, the Facework asks to swipe the RFID card on the card symbol located front-middle of the Facework after completing the face enrollment [Figure 20]. After enrollment of the card, go to the step ⑬.

⑪ In Step⑤, if 'Card Only' is selected as authentication mode, the Facework skips the face enrollment step ⑧ and directly asks to swipe the RFID card on the Facework main unit [Figure 20].



PIN code *

Confirm *

[Figure 18] Setup PIN code

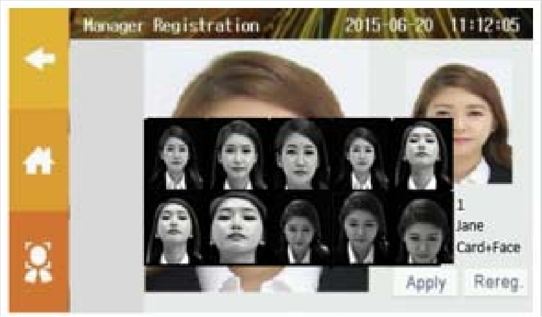
⑫ In Step⑤, 'Face Only' is selected at 'Mode' field, continue the following steps.

⑬ The Facework shows the profile of the Manager including the picture taken in the step⑧. At here, check whether enrolled manager information is correct or not. If the information is correct, touch <Apply> button. Then the Facework shows 10 black and white photos taken at the step⑧.

⚠ The Facework internally uses 1 more picture randomly from 9 pictures taken during the enrollment to make better quality of template. That's why it shows 10 black and white pictures.

At this step, the most important things are:

a. Check black and white photos carefully. First of all, find any abnormal face pose like eye closing, open mouth, laughing, frowning, hiding eyebrow with hair, hiding jaw line by collar and others [Figure 19]. Additionally, if it consists of different sized faces



1

Jane

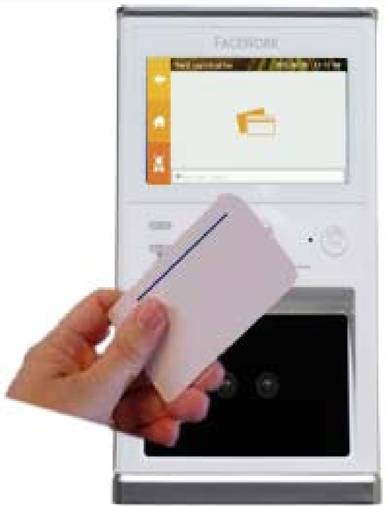
Card+Face

[Figure 19] Black and white pictures

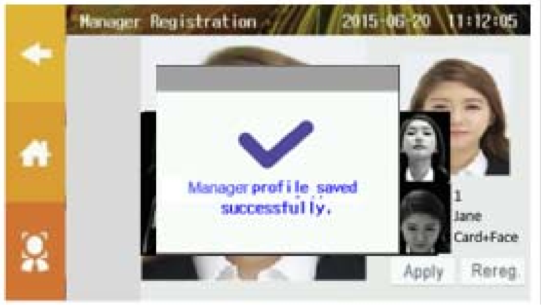
and different face poses at face front, face up and face down, it can be ready to make good template. When each photo turned out good, touch <Apply> button again [Figure 19]. Then, the Facework finishes the manager enrollment process with showing "Manager Profile saved successfully" message [Figure 21].

b. If you need to enroll the face again to get better quality of photos. Touch <Rereg.> button for re-enrollment [Figure 19]. Then the Facework repeats the Step⑧.

⑭ In Step ⑥, if you choose 'YES' in Glasses option, the Facework repeats the same face enrollment process two times: enrollment with and without wearing Glasses. Then, take proper actions as guided by the voice message.



[Figure 20] Register Card


Manager Registration 2015-06-20 11:12:05

Manager profile saved successfully.

1
Jane
Card+Face

[Figure 21] Complete Manager Enrollment

⚠ The Facework can have up to 10 managers with any combination of Super managers or Managers.

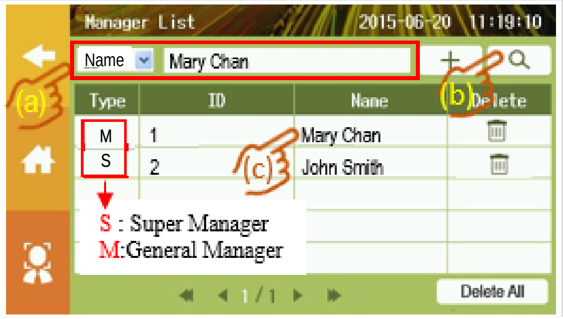
2.2. Modify (Edit) Manager

After enrollment of the manager, the manager profile sometimes needs to be modified due to the necessity of authentication mode change, newly wearing glasses or manager type change. The followings are steps to modify the manager profile.

① To modify manager profile, the Facework requires the Super manager privilege.

② To understand how to get the Setup Menu with the Super manager privilege, refer to [Figure 11].

③ In the Setup Menu, touch 'Manager' [Figure 12].



Name ▾ Mary Chan

Type	ID	Name	Delete
M	1	Mary Chan	🗑
S	2	John Smith	🗑

S : Super Manager
M:General Manager

[Figure 22] Search & Select Manager to modify

④ In the case that the manager to be modified is shown in the Manager list table, directly touch the line holding the manager ID & name [Figure 22(c)].

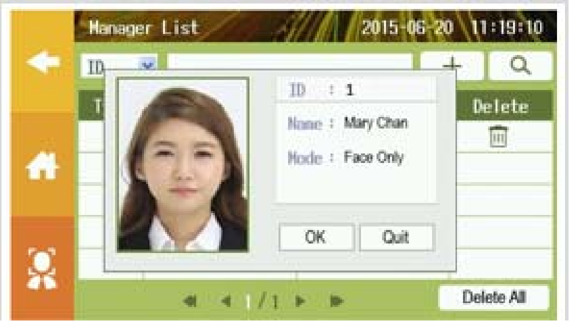
Or to use search condition,

a. select search key ('ID' or 'Name') from the drop down list box and enter a specific ID or manager name depending on selected search key [Figure 22(a)].

b. Touch the magnifier symbol to explore it [Figure 22(b)].

c. Touch the line showing the manager ID & name to be modified from the manager list table [Figure 22(c)].

⑤ The Facework shows the manager information on the screen and then touch <OK> button if it is the right manager to be modified [Figure 23]. Otherwise, touch <Quit> button.

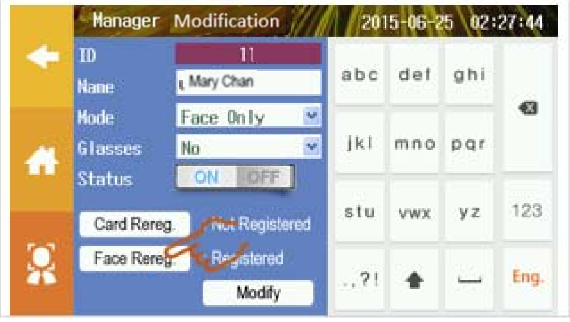


ID : 1
Name : Mary Chan
Mode : Face Only

[Figure 23] Manager Information to Modify

⑥ At here, the Facework manager can change name, authentication mode or PIN code. But if the Facework manager wants to re-enroll the face due to wearing glasses, pick 'YES' at the 'Glasses' field, and then re-enroll the face by touching <Face Rereg>. In the case of re-enrolling the face with other reasons, skip 'Glasses' field and directly go to face enrollment step by touching <Face Rereg> button [Figure 24].

⚠ As ID means Face ID featuring uniqueness, it can't be changed. To change ID, the Facework manager should delete the manager and add it as a new manager again.



ID 11
Name Mary Chan
Mode Face Only
Glasses No
Status ON OFF
Card Rereg Not Registered
Face Rereg Registered

[Figure 24] Manager Modification

⑦ If 'Card+Face' was selected as authentication mode, it asks to swipe the RFID card on the Facework main unit after face enrollment [Figure 20].

⑧ If you chose 'Card Only' as authentication mode, it skips the face enrollment process and directly asks to swipe the RFID card on the Facework [Figure 20].

⑨ Touch <Modify> to update it, and then pop up window will appear with text message "the modification is done successfully".

2.3. Delete Manager

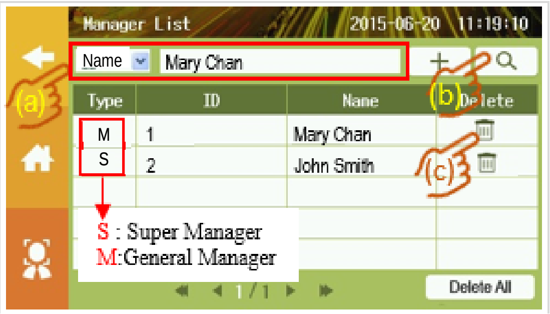
When the enrolled manager resigned the company or transferred to other organization, the manager needs to be removed from the Facework device. The process of manager deletion is as follows:

① To delete the manager profile, the Facework requires the Super manager privilege.

② To understand how to get the Setup Menu with the Super manager privilege, refer to [Figure 11]

③ In the Setup Menu. Touch 'Manager' [Figure 12].

④ In the case that the manager to be modified is shown in the manager list table, directly touch the line holding the manager ID & name [Figure 25(c)].



Manager List 2015-06-20 11:19:10

Name: Mary Chan

Type	ID	Name	Delete
M	1	Mary Chan	
S	2	John Smith	

S : Super Manager
M:General Manager

[Figure 25] Search & Select Manager to delete

Or to use search condition,

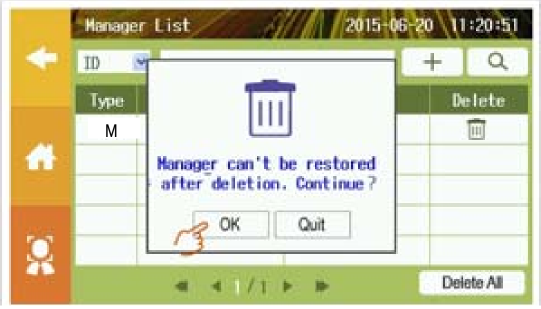
a. Select search key ('ID' or 'Name') from the drop down list box and enter a specific ID or manager name depending on selected search key [Figure 25(a)].

b. Touch the magnifier symbol to explore it [Figure 25(b)].

c. As the result of it, the Facework shows the searched results. Then touch the 'wastebasket' on the line showing the manager name to delete from the manager list table [Figure 25(c)].

⚠ The last Super manager can be deleted with only 'Delete All' function.

⑤ The Facework shows the Manager information on the screen, and then touch <OK> if it is the right manager to be deleted. Otherwise, touch <Quit> button.



Manager List 2015-06-20 11:20:51

Manager can't be restored after deletion. Continue?

[Figure 26] Confirmation of Manager Deletion

⑥ Once the Manager is deleted, it can't be recovered. To avoid unintended deletion, the Facework confirms it again. To delete it, touch <OK> button [Figure 26].

⑦ To delete all managers at once, touch <Delete All> button in the Step ④, with skipping all inputs. Then the Facework confirms it again and deletes all managers when the Facework manager touchs <OK> button.

⚠ The deleted manager can't be restored. So be careful to use 'Delete' or 'Delete All' command.

3. User Setup

The term 'User' means all users that are already enrolled or enrolling on the Facework device. All general users should be enrolled to the Facework device prior to taking authentication service from the Facework device. The User Setup (Enrollment / Modification /Deletion) process is very similar to Manager Setup except for the authentication mode. Regarding authentication mode, a user has more 3 authentication modes ('ID + Face' mode, 'Card + Face Log' mode and 'Card or Face' mode) than a manager. But the 'PIN+Face' authentication mode for a manager is not applicable to a user.

The user enrolled to the Facework device can get only face authentication service but can't access any control or management function for the Facework device if the Facework manager is already existed.

⚠

- The Facework Model FW-N10 supports 1,000 users at maximum with 1:N mode.
- If the Manager has to get authentication service from the Facework applications like Access Control and Time Attendance, the Manager must be enrolled again as a general user.

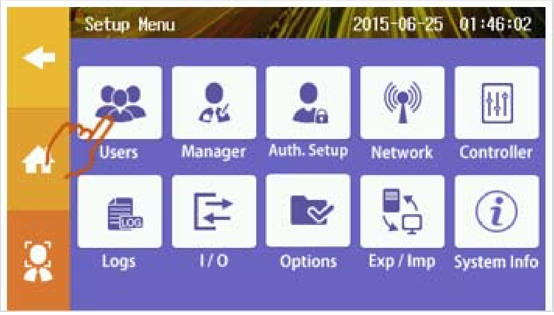
3.1. Add User

The Manager can add new user to the Facework device by touching 'Users' in the Setup Mode.

Detailed steps for adding new user are as follows:

① To get the Setup Menu, the Facework manager needs to get authentication from the Facework. For more information about it, refer to [Figure 11].

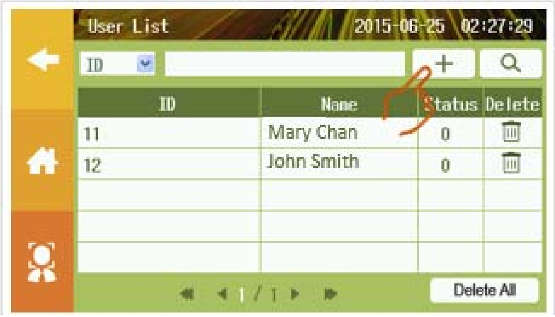
② Touch 'Users' in the 'Setup Menu' [Figure 27].



[Figure 27] Users Setup

③ Touch ‘+’ symbol to add a new user [Figure 28] and then ‘User Registration’ window will appear.

④ Enter User ID and User name firstly. The User name can be optional here as the name can be filled from ACMS software later. And then select a proper authentication mode in the ‘Mode’ field [Figure 29]. There are 6 available authentication modes for a user. For more information about authentication mode, please refer to section 1.2 of Chapter 2.

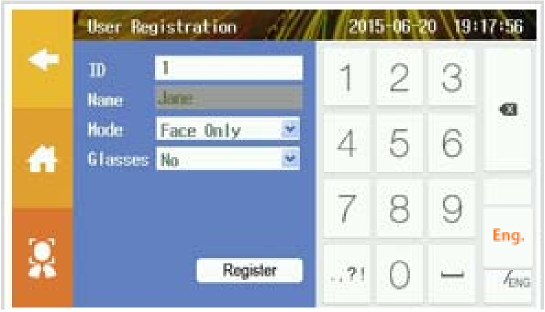

User List 2015-06-25 02:27:29

ID	Name	Status	Delete
11	Mary Chan	0	🗑
12	John Smith	0	🗑

[Figure 28] Add User

⑤ Select ‘Glasses’ option [Figure 29]. If the user puts on glasses, choose ‘Yes’. However, it is recommended to select ‘No’ except that the frame of glasses are not much thick.

⑥ It starts face enrollment process. For more details about face enrollment process, please refer to 2.1 Add Manager section.


User Registration 2015-06-20 19:17:56

ID: 1
Name: Jane
Mode: Face Only
Glasses: No

[Figure 29] User Enrollment

3.2. Modify (Edit) User

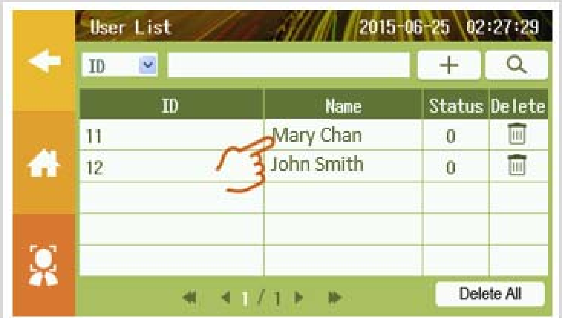
While the Facework is being used in the organization, user profile may need to be modified due to some reasons such as change of authentication mode, newly wearing glasses or temporary authentication block. The followings are detailed steps to modify the user profile. This function should be done by Facework manager.

① To modify user profile, the Facework requires the Super manager privilege.

② To understand how to get the Setup Menu with the Manager privilege, refer to [Figure 11].

③ In the Setup Menu, touch ‘Users’ [Figure 27].

④ Enter user ID or the name to be modified and touch the Magnifier symbol to start the user exploration. Then the device shows the searched user records on the user list table. As the next step, touch the line showing the user from the user list


User List 2015-06-25 02:27:29

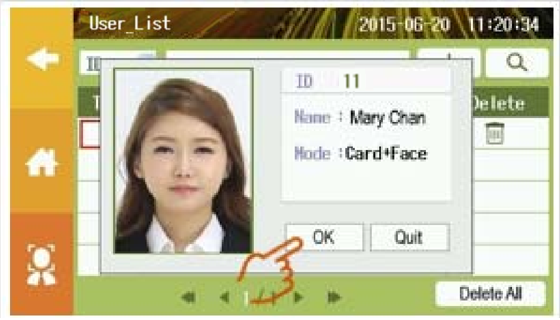
ID	Name	Status	Delete
11	Mary Chan	0	🗑
12	John Smith	0	🗑

[Figure 30] Search & Select User to modify table. Or when a target user is shown in the user list table, directly touch the line [Figure 30].

⑤ The Facework shows the user information on the screen, and then touch <OK> button if it is the right user to be modified [Figure 31]. Otherwise, touch <Quit> button.

⑥ The Facework manager can change the user name, and authentication mode. But if face re-enrollment is required due to wearing glasses, pick 'YES' at the 'Glasses' field and reenroll the face by touching <Face Rereg>. In the case of re-enrolling the face with other reasons, skip 'Glasses' field and directly go to the face enrollment step by touching <Face Rereg> button [Figure 32].

⚠ As ID is set to a primary key, it can't be changed. To change ID, it should be deleted in advance and newly added again.


User_List 2015-06-20 11:20:34

ID 11

Name : Mary Chan

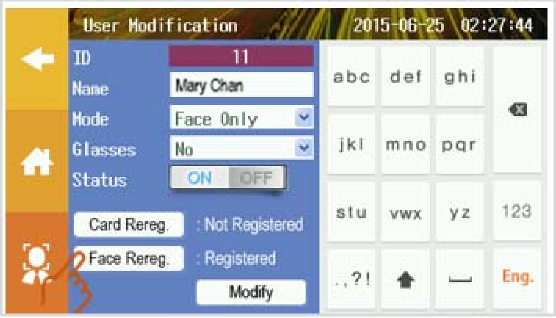
Mode : Card+Face

[Figure 31] Information of the searched user

⑦ If the Facework needs to block the user from authentication, turn off the status switch. Later the Facework manager can unblock the user by turning on the status.

⑧ If 'Card+Face' is selected as authentication mode, it asks to swipe the RFID card on the Facework main unit after face enrollment.

⑨ If 'Card Only' is selected as authentication mode, it skips the face enrollment step and directly asks to swipe the RFID card on the Facework.


User Modification 2015-06-25 02:27:44

ID 11

Name Mary Chan

Mode Face Only

Glasses No

Status ON OFF

Card Rereg. : Not Registered

Face Rereg. : Registered

[Figure 32] Face Reenrollment

⑩ The Facework shows Informational window with 'Modification is successfully done' text message.

3.3. Delete User

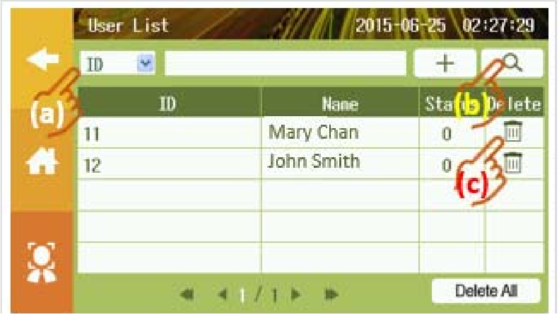
If the enrolled user resigned the company or transferred to other organization, the user template needs to be removed from the Facework. The user deletion steps are as follows:

① To delete a user, the Facework requires the Super manager privilege.

② To understand how to get the Setup Menu with the Manager privilege, refer to [Figure 11].

③ In the Setup Menu. Touch 'Users' [Figure 27].

④ Enter user ID or User name to delete [Figure 33(a)], and then touch the Magnifier symbol to explore the user [Figure 33(b)]. Then the device shows the searched user records on the list table. As the next step, touch the wastebasket symbol located at the right side of the line showing the user to be deleted [Figure 33(c)]. Or when a target user is shown in the user list table, directly touch the wastebasket symbol on the line [Figure 33(c)].


User List 2015-06-25 02:27:29

ID	Name	Status	Delete
11	Mary Chan	0	🗑
12	John Smith	0	🗑

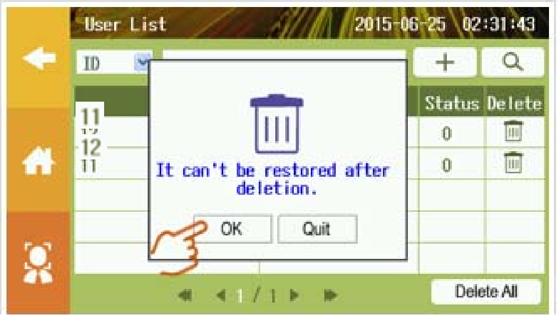
[Figure 33] Search & Select User to delete

⑤ The Facework shows the user information on the screen and then touch <OK> button if it is the right user to be deleted. Otherwise, touch <Quit> button.

⑥ Once the user is deleted, it can't be recovered. Thus, the Facework confirms it one more time to prevent unintended deletion. To delete it, touch <OK> button [Figure 34].

⑦ To delete all users at once, touch <Delete All> button in the Step ④, with entering nothing on the screen. Then the Facework confirms deletetion of all users ,and then delete all users when <OK> button is touched.

⚠ The deleted user can't be restored. So be careful to use 'Delete' or 'Delete All' command.


User List 2015-06-25 02:31:43

It can't be restored after deletion.

[Figure 34] Search & Select User to delete

4. Authentication Setup

The Facework device has a plenty of key parameters that can affect to the performance of face recognition. The Facework manager can adjust all relevant parameters in the 'Auth. Setup' menu with following steps.

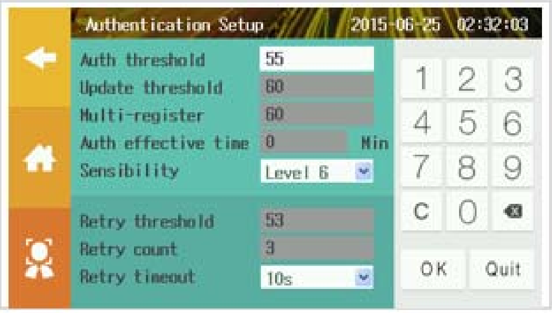
① To change authentication parameters, the Facework requires the Super manager privilege.

② To understand how to get the Setup Menu with the Super manager privilege, refer to [Figure 11].

③ In the Setup Menu. Touch 'Auth. Setup'.

④ The Facework shows ‘Authentication Setup’ window including 8 parameters [Figure 35]. The detailed information of each parameter is as follows:

a. Auth. Threshold: It is the reference value on deciding whether the captured face at the recognition time is genuine or not. When user gets authenticated, the Facework makes the temporary template by using the captured images at the recognition time, and then compares it with the enrolled template. At this time, it calculates the matching score to analyze the similarity with the internal algorithm. If it has higher value, the Facework requires stricter matching rate which negatively affects to recognition rate with more accuracy. On the contrary. If it has lower value, it requires less strict matching rate which positively affects to recognition rate with less accuracy. When the value is set to lower than the default one, it can cause the false acceptance.



Authentication Setup 2015-06-25 02:32:03

Auth threshold 55

Update threshold 60

Multi-register 60

Auth effective time 0 Min

Sensibility Level 6

Retry threshold 53

Retry count 3

Retry timeout 10s

[Figure 35] Authentication Setup

b. Update Threshold: This parameter affects to automatic template update process. As stated in the beginning, the Facework has an intelligent template update function to trace the shape of face that is being changed over times. When the Facework finds the template score calculated from the captured image at the recognition time is higher than the update threshold value, the Facework rebuilds the registered template with the new captured image and updates it.

c. Multi-register: This parameter is used to prevent multiple enrollment of the same person. At the enrollment time, it makes the template for new user with comparing it with all other templates stored in the template database. During comparison process, if the Facework finds the registered template with higher score than the parameter value, it denies to enroll the user as the Facework regards it as the enrolled user in the device.

d. Auth. effective time: It is the threshold value to decide authentication effective time. On getting user authentication, the user can try the authentication repeatedly. At this time, the Facework calculates the time gap and do not execute authentication with “You are already authenticated” voice message if the time gap is within this threshold value.

e. Body Induction: The Facework automatically activates the device into face recognition device when someone comes close to the device. Thus, this parameter is used to decide the sensibility level to detect the human body. The ‘Level 6’ is the most sensitive level for it.

f. Retry threshold: When the Facework authenticates the user, it sometimes fails to do it when the user posture is wrong or other reason. In this case, the Facework does not regard it as failure immediately. Instead, it checks the authenticated matching score and retries authentication process when it is higher than the threshold value.

g. Retry count: This parameter decides the loop count for repetitive authentications based on 'Retry threshold'

h. Retry timeout: During recognition process based on 'Retry threshold' and 'Retry count', the Facework continuously captures the user face and repeats this process until it gets successful authentication. But the Facework stops this loop when it reaches this timeout value.

⑤ After setting parameters, touch <OK> button to apply them to the Facework.

⚠ All parameters stated above can seriously affect to the performance or accuracy if it is set with wrong value. So it is highly recommended to use default values.

5. Network Setup

The Facework can be connected to Ethernet for network application. Then the Facework network parameters should be configured properly. All network parameters are mostly customer dependent. Therefore, please contact to your network manager to get the right values.

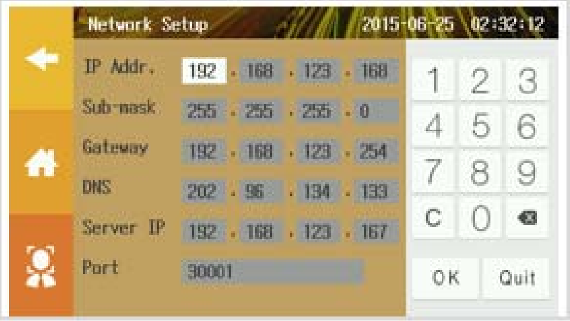
The Facework manager can set all relevant parameters in the 'Network Setup' menu with following steps.

① To change authentication parameters, the Facework requires Super manager privilege.

② To understand how to get the Setup Menu with the Super manager privilege, refer to [Figure 11].

③ In the Setup Menu, touch 'Network Setup'.

④ The Facework shows 'Network Setup' window including 6 parametes [Figure 36]. The description of each parameter is as follows:



Network Setup 2015-06-25 02:32:12

IP Addr. 192 . 168 . 123 . 168

Sub-mask 255 . 255 . 255 . 0

Gateway 192 . 168 . 123 . 254

DNS 202 . 96 . 134 . 133

Server IP 192 . 168 . 123 . 167

Port 30001

[Figure 36 Network Setup]

a. IP Address: It is IP Address assigned to the Facework device. Contact your network manager to get a right value.

b. Sub-mask: It is used to divide the IP address into network and host addresses. Contact your network manager to get a right value.

c. Gateway: it is a router interface address connected to the local network that sends packets out of the local network. Contact your network manager to get a right value.

d. DNS: It is abbreviation of Domain Name Service. It is the service used to convert human readable names of hosts to IP address. Contact your network manager to get a right value.

e. Server IP: It is reserved for the Facework manufacturer.

f. Port: It is used for the Facework manufacturer only, and thus do not change it. This port number is necessary for communicating the Facework device with SDK user application or ACMS (Access Control Management Software) bundled in the Facework.

⑤ After setting parameters, touch <OK> button to apply them to the Facework device.

6. Controller

This is reserved for ACS (Area Control System) and disabled at present.

7. Logs

The Facework logs all history of access control or time attendance for the purpose of security tracing, later. It stamps user ID, name, access time, time attendance (T/A) code and the authentication result.

The Facework manager can manage all log relevant activities in the 'Log Setup' menu with following steps.

① To manage log files, the Facework requires upper manager privilege.

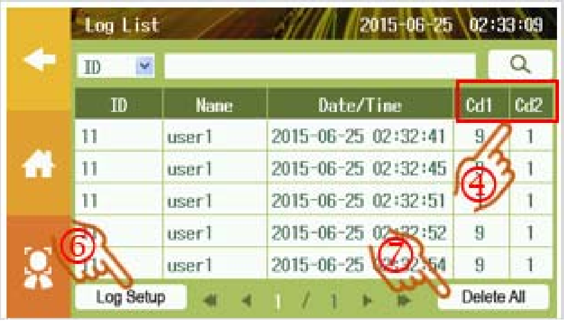
② To understand how to get the Setup Menu with the Supper Manager privilege, refer to [Figure 11].

③ In the Setup Menu, touch 'Logs'.

④ Then the Facework lists all logs accessed by the Facework users with ID, name, accessed date&time, T/A code and authentication result. In the log list table, T/A code and Authentication result are shown as 'Cd1' and 'Cd2', respectively with following meaning.

a. Cd1: It shows the code of access types at the accessed time: Control or Time Attendance. The meaning of each code number is.

0: Check In / 1: Check Out / 2: Early Check Out / 3: Out / 4: Return / 9: Access Control



Log List 2015-06-25 02:33:09

ID

ID	Name	Date/Time	Cd1	Cd2
11	user1	2015-06-25 02:32:41	9	1
11	user1	2015-06-25 02:32:45	[illegible]	1
11	user1	2015-06-25 02:32:51	[illegible]	1
[illegible]	user1	2015-06-25 02:32:52	9	1
11	user1	2015-06-25 02:32:54	9	1

[Figure 37] Log Setup

⚠

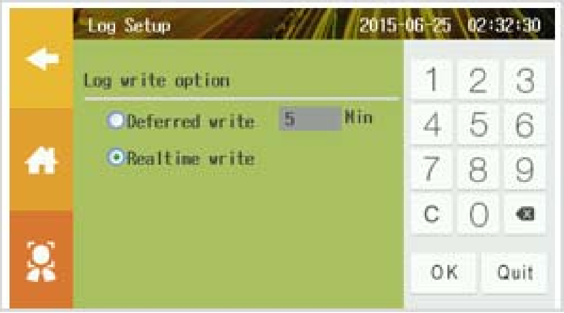
- Above codes will be shown only in the case that both T/A mode is 'ON' and a user touches proper T/A code on the Face recognition window.
- T/A Mode can be turned On or Off at the 'Setup Menu' → 'Options' → 'Time Attendance'.
- In the case of either T/A Mode is 'OFF' or T/A code is not touched, the Facework logs '9'
- This code can be used by ACMS or user developed application, later.

b. Cd2: It shows the result of authentication. '1' or '0' in the Cd2 column mean the result of authentication is 'Success' or 'Failure', respectively.

⑤ Optionally, only a specific user's log can be listed by user ID or user name.

⑥ By touching <Log Setup> button, the log writing mode can be changed [Figure 38].

a. Deferred write: When the option is chosen, the Facework buffers log data in the memory and stores them in a batch to the storage every specified time. The deferred writing time can be specified in the 'Min' field. After entering the number, touch <OK> to apply it. Otherwise, touch <Quit>.



Log Setup

2015-06-25 02:32:30

Log write option

○ Deferred write 5 Min

◉ Realtime write

[Figure 38] Log writing Option

b. Realtime write: It enable the Facework to write the log event to log file immediately whenever access or T/A event is occurred.

⑦ To delete all log histories, touch <Delete All>. Then the Facework confirms deletions of all logs and delete them when <OK> is touched.

8. I/O (Input / Output)

The Facework provides rich I/O ports to interface diverse external devices like lock controller, fire detection sensor or others. Some attributes of them can be defined at the 'I/O' on the Setup Menu.

① To change authentication parameters, the Facework requires Super manager privilege.

② To understand how to get the Setup Menu with the Super manager privilege, refer to [Figure 11].

③ In the Setup Menu. Touch 'I/O'.

④ The Facework shows ‘I/O Setup’ window with 6 parametes [Figure 39]. The function of each parameter and settings are as follows:

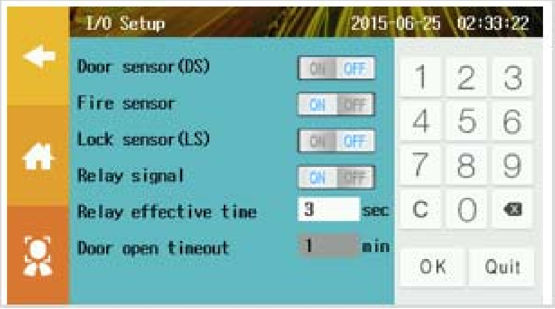
a. Door Sensor: This parameter enables or disables the Facework to sense door open status. When it is set to ON, it can detect the door open status.

⚠ In order to sense the door open status, the Facework should interface with a lock controller with a proper cable connection.

b. Fire sensor: It decided whether to activate or deactivate the fire detection sensor in the case that the fire detector is connected to the Facework.

c. Lock Sensor: This parameter is reserved for the Access Control Unit.

d. Relay Signal: The relay signal is used to open or close the lock. It uses 3 points electrical contacts: NO, COM, NC. An electrical contact can be operated by ‘Exit’ switch or an access control device like a biometric recognition device or a card reader, by mechanical pressure in sensors or electromechanically in relays. In the normal status, NC and COM are usually maintained as short status. But when an external event like fire detection or authentication success is occurred, it shorts COM and NO instead of using NC to change the relay status. Using this feature, the Facework can transmit the signal to the external devices using an independent lock controller (ex: Speed gate, Sliding door…)



Door sensor (DS) ON OFF
Fire sensor ON OFF
Lock sensor (LS) ON OFF
Relay signal ON OFF
Relay effective time 3 sec
Door open timeout 1 min

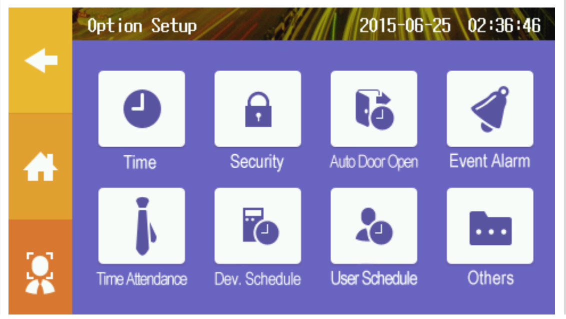
[Figure 39] Log writing Option

e. Relay effective time: It sets the time that the relay re-sets its current status to initial status (NC-COM short) after detecting the door opened. That means the door will be automatically closed from door open status after this parameter. The time can be set ranged from 1 to 255s.

f. Door open timeout: When the door has not closed during this parameter, it generates the alarm.

9. Options

In the Setup Menu, the Facework manager can execute the Option menu after authentication as Super manager. In the Option menu, the Facework manager can set System time / Security related values / Auto door open / Event alarm / Time Attendance / Device schedule / User schedule and other options.



[Figure 40] Option Menu

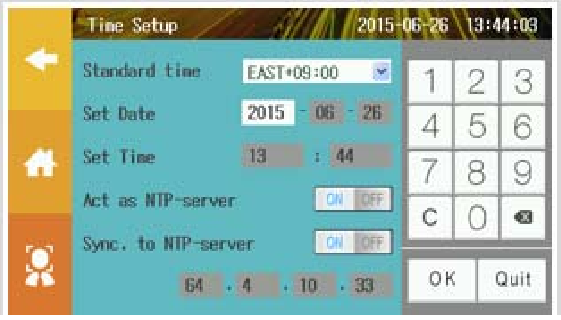
① To get the Setup Menu with Super manager privilege, refer to [Figure 11].

② In the Setup Menu, touch ‘Options’.

There are 8 options in the ‘Option Menu’ and function of each option is explained at below.

9.1. Time:

The Facework time can be set by this Time setup function [Figure 41].



Time Setup 2015-06-26 13:44:03

Standard time EAST+09:00

Set Date 2015 - 06 - 26

Set Time 13 : 44

Act as NTP-server ON OFF

Sync. to NTP-server ON OFF

64 . 4 . 10 . 33

[Figure 41] Time Setup

① Standard time: It can set local time based on Eastern Standard Time. Select the right time zone of your country to set current local time.

② Set date: It sets the date of the Facework device. Enter the correct date at this field with yyyy-mm-dd format.

③ Set time: It sets the time of the Facework device. Enter the correct time with ‘hh:mm’ format.

④ Act as NTP-server: When multiple Facework devices are configured as same network, a specific device can be the NTP-Server to synchronize times across all connected Facework devices. For enabling this feature, this option switch must be set to ‘ON’

⑤ Syn. to NTP-server: If a specific computer needs to be configured as the NTP-Server in your organization, set this option to ‘ON’, and enter IP Address of the computer. Then, this Facework device gets the time from the designated NTP server and applies it to the Facework device. Or the time on the Facework device can be synchronized with world-wide certified NTP-Server by entering IP address of it. When this option is set to ON, the default server will be Microsoft certified NTP-Server.

9.2. Security:

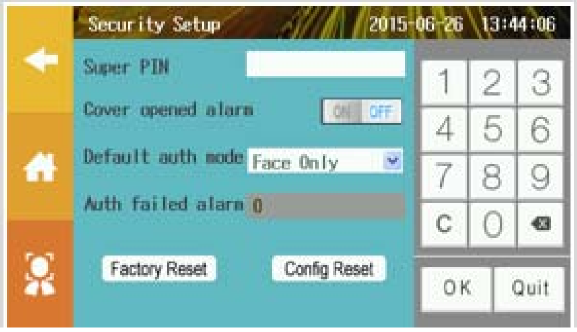
In the Security option, some security options can be set or modified [Figure 42].

① Super PIN: This option will be useful when the Facework manager needs to force to open the door at emergency situation. To use this function,

a. Enter PIN code to ‘Super PIN’ field.

b. Touch <OK> button to save it.

c. To change the Super PIN, repeat step (a) and (b).



Security Setup 2015-06-26 13:44:06

Super PIN

Cover opened alarm ON OFF

Default auth mode Face Only

Auth failed alarm 0

[Figure 42] Security Setup

When the Facework manager wants to open the door forcibly with the Super PIN’,

a. Touch the ‘ID Check’ button on the Face Recognition window.

b. Enter ‘*#’ and your ‘PIN code’, subsequently. Then the door will be immediately opened without face recognition step.

⚠

This function can cause much sensitive security issue in the case that ‘Super PIN’ code is exposed to unauthorized people because they can intrude into the security area without authentication. Therefore, the Facework manager should strictly manage this ‘Super PIN’ code. If Super PIN code is blank, this feature is disabled automatically.

② Temper alarm: When a malicious person forces to dismantle the Facework device, the device generates alarm when this option is enabled.

③ Default auth. mode: This parameter sets the default authentication mode for the Facework device when new user is added. This authentication mode can be manually changed at the time of new user enrollment.

④ Auth. failed alarm: This parameter sets maximum number of authentication failures. If it exceeds the parameter value, the Facework turns on alarm beep sound.

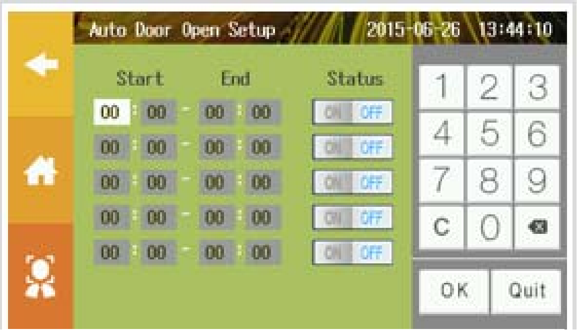
⑤ Config Reset: This command button resets all parameters to default values. Before resetting configuration, the backup of configuration file is highly recommended. Regarding detailed procedure for configuration backup, refer to the Section 10 ‘Export / Import’ of this chapter.

⑥ Factory Reset: This command button will initialize the Facework device to factory mode with deleting all enrolled users and managers. Before factory reset, user backup is highly recommended as all data can’t be recovered after factory reset. Regarding detailed procedure for user backup/restore, refer to the Section 10 ‘Export / Import’ of this chapter.

⚠ Backup for managers cannot be supported. Thus all managers should be enrolled again after factory, reset if they are not saved into ACMS database.

9.3. Auto Door Open:

The Facework manager can define the time zone that door automatically opens (ex: lunch time). The Manager can define up to 5 time zones at maximum and selectively turns on or off it as necessary. After entering time intervals of the door open time zone, make sure of pressing <OK> to save it [Figure 43].



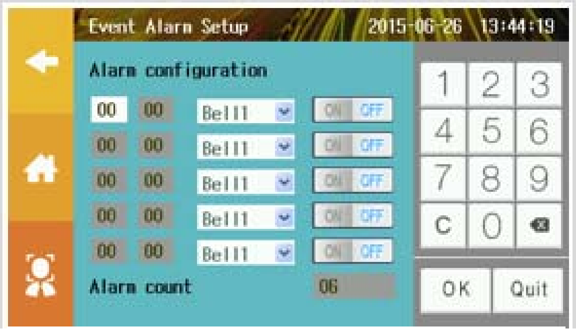
00 : 00 - 00 : 00 ON OFF
00 : 00 - 00 : 00 ON OFF
00 : 00 - 00 : 00 ON OFF
00 : 00 - 00 : 00 ON OFF
00 : 00 - 00 : 00 ON OFF

[Figure 43] Auto Door Open Setup

9.4. Event Alarm:

This option generates the alarm sound when the Facework meets the time set by this event alarm. The Facework allows to set up to 5 event alarms with different alarm bell. It can set maximum number of alarm loop with the Alarm count.

After setting parameters, touch <OK> to save it [Figure 44].



00 00 Bell1 ON OFF
00 00 Bell1 ON OFF
00 00 Bell1 ON OFF
00 00 Bell1 ON OFF
00 00 Bell1 ON OFF
Alarm count 06

[Figure 44] Event Alarm Setup

9.5. Time Attendance (T/A):

Most of organizations may use ‘time attendance’ to record employees’ start (check-in) and stop work time (check-out). The Facework device has 5 T/A choices as below:

① Check In: It is the time that the user comes to the office for work. When <Check In> button is touched, the Facework device logs T/A code ‘0’ with stamping the work start time.

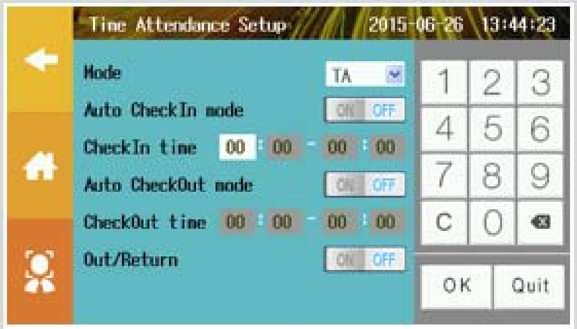
② Check Out: It is the time that the user gets off. When <Check Out> button is touched, the Facework device logs T/A code ‘1’ with stamping the work stop time.

③ Early Check Out: It is the time that the user early gets off. When <Early Check Out> button is touched, the Facework device logs T/A code ‘2’ with stamping the early check out time.

④ Out: It is the time that the user goes out from the working place during business hour. When <Out> button is touched, the Facework device logs T/A code ‘3’ with stamping the time to go out.

⑤ Return: It is the time that the user returns to the working place after going out. When <Return> button is touched, the Facework device logs T/A code ‘4’ with stamping the return time.

For using the time attendance function, each user should touch a proper T/A code before face authentication. The Facework manager can setup T/A relevant parameters as follows [Figure 45];



Time Attendance Setup 2015-06-26 13:44:23

Mode: TA

Auto CheckIn mode: ON OFF

CheckIn time: 00 : 00 ~ 00 : 00

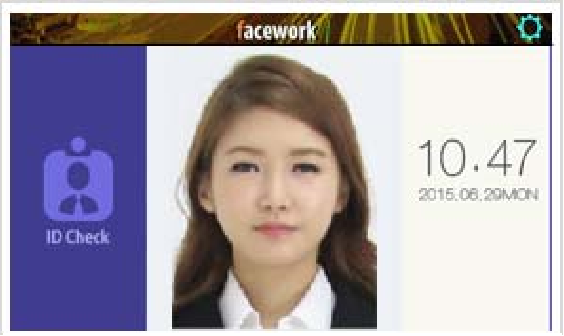
Auto CheckOut mode: ON OFF

CheckOut time: 00 : 00 ~ 00 : 00

Out/Return: ON OFF

[Figure 45] Time Attendance Setup

① Mode: If the organization wants to use the time attendance function, the mode must be set to 'TA'. If so, the Facework device activates 'TA' buttons on the face recognition window. On the contrary, when it is set to 'None', TA buttons will be hidden on the screen [Figure 46]. For this case, only 'ID Check' button is activated instead of TA buttons. When the user with 'ID + Face' authentication mode tries to get authentication, the user must touch this button to get the keypad for the ID code input before face authentication.

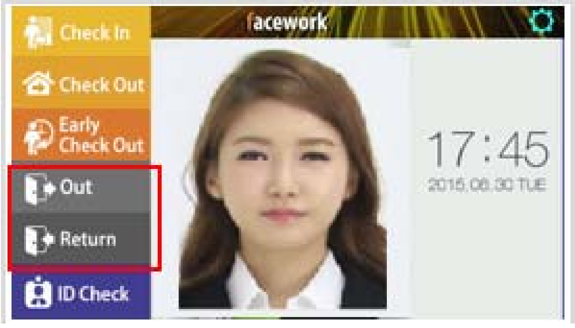


[Figure 46] Face Recognition Window when TA mode is set to 'NONE'

② Auto Check In mode: For some cases, it may be somewhat cumbersome to touch <Check In> button every day. However, In the case that 'Auto Check In mode' is set to 'ON' and 'Check In time' is defined, the Facework device automatically considers that all users authenticated during the check-in time interval touched the 'Check In' button, although they do not touch it.

③ Auto Check Out mode: It is similar to 'Auto Check In' mode. In the case that 'Auto Check Out mode' is set to 'ON' and the 'Check Out time' is defined, the Facework device will automatically consider all users authenticated during the time interval touched the 'Check Out' button, although they didn't touch it.

④ Out / Return: This option enables or disables the 'Out / Return' function. If this feature is set to 'OFF', the <Out> and <Return> buttons will be inactive on the face recognition window [Figure 47].

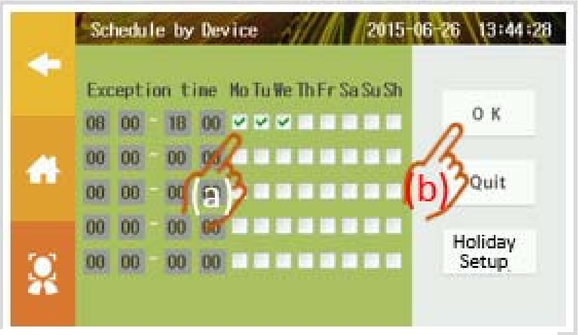


[Figure 47] Face Recognition Window when 'Out/Return' is set to 'OFF'

⚠ This option is only applicable when 'Mode' is set to 'TA'.

9.6. Device Schedule:

For the purpose of security control, the Facework manager can define the schedule to block user authentication by the device. The schedule can be set by time of the day of week or a user defined special holiday. The Facework manager can define up to 5 schedules. The detailed setup process is as follows;



Exception time					Mo	Tu	We	Th	Fr	Sa	Su	Sh
08	00	-	18	00	☑	☑	☑	□	□	□	□	□
00	00	-	00	00	□	□	□	□	□	□	□	□
00	00	-	00	00	□	□	□	□	□	□	□	□
00	00	-	00	00	□	□	□	□	□	□	□	□
00	00	-	00	00	□	□	□	□	□	□	□	□

[Figure 48] Device Schedule Setup

① Create the schedule:

a. Enter the time interval for blocking authentication to 'Exception time' and touch check box below the day of week to apply this schedule [Figure 48(a)].

b. Touch <OK> button to save it. Then the Facework will block all of user authentications during specified time interval on the day of the week checked in the box.

② Modify the schedule:

a. In the 'Device Schedule Setup' window [Figure 48], change the value on the time interval and the day of the week applied to the schedule.

b. Touch <OK> button to save it.

③ Delete the schedule:

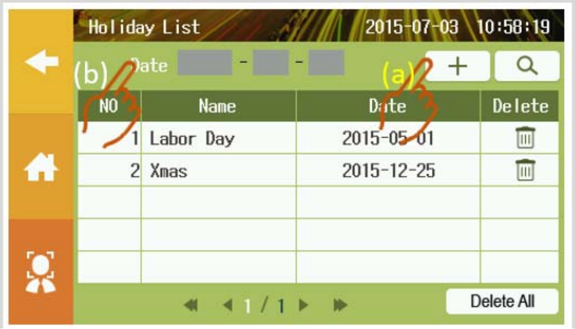
a. Uncheck the check box pointing to the day of the week.

b. Touch <OK> button to save it.

④ Add / Modify / Delete User-defined holidays:

a. Touch <Holiday Setup> at the 'Device Schedule Setup' window [Figure 48(b)]. Then 'Holiday List' window will appear [Figure 49].

b. Touch '+' symbol to add the user-defined holiday [Figure 49(a)]. To explore the schedule name by date, enter 'Year / Month / Day at the Date field and touch the 'Magnifier' [Figure 49(b)].



NO	Name	Date	Delete
1	Labor Day	2015-05-01	🗑
2	Xmas	2015-12-25	🗑

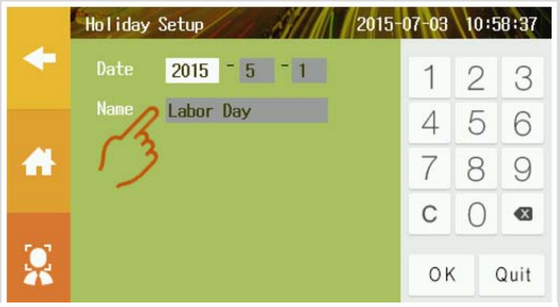
[Figure 49] Holiday List

c. Enter Date thru the Numeric keypad. When the date input is complete [Figure 50], the Facework automatically moves to 'Name' field with shifting the numeric keypad to 'Alphanumeric' one to get the name value. Enter the name of user-defined holiday at the Name field [Figure 51].

d. To exit from 'Alphanumeric' keypad, touch any point at outside of keypad after the schedule name input.

e. To save the created user-defined holiday, touch <OK> located below the numeric keypad [Figure 52].

f. To apply the user defined holiday to the schedule, go to 'Holiday List' window [Figure 48] and touch the check box 'Sh' field on the proper 'Exception time' interval.

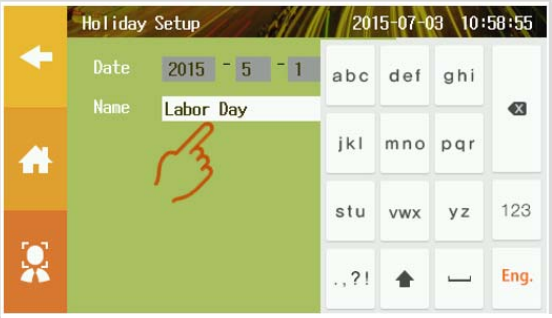


Date 2015 - 5 - 1

Name Labor Day

[Figure 50] Holiday Setup (1)

g. To modify the date of the user defined holiday, touch <Holiday Setup> button on the 'Holiday List' window [Figure 48], then the Facework shows the list of user defined holidays on the screen [Figure 49]. Touch the holiday name to modify and enter new date in the 'Holiday Modification' window. To save the modification, touch <OK> button.



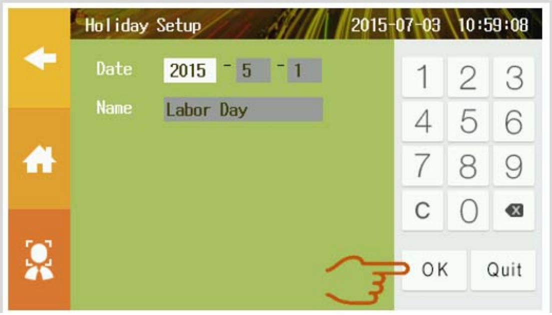
Date 2015 - 5 - 1

Name Labor Day

[Figure 51] Holiday Setup (2)

h. To delete the user-defined holiday, touch <Holiday Setup>. Then the Facework will show the list of user defined holidays. Touch 'wastebasket' symbol on the line holding the user defined holiday name to delete. Then it shows confirmation popup window, and then touch <OK> to delete it.

i. The Facework manager can delete all user-defined holidays by touching <Delete All>.



Date 2015 - 5 - 1

Name Labor Day

[Figure 52] Holiday Setup (3)

- When time zones are overlapped for multiple schedules, it blocks the user authentication from the earliest time to the latest time across those time zones.
- When the time zone is spanned over two days (ex: 23:00 on Monday to 06:00 on Tuesday), touch the box on the day of the week starting the schedule when to set the schedule.

9.7. User Schedule:

Unlike Device schedule, The Facework manager can define the time zone to block or to allow the authentication by a specific user. The time zone can be set by the day of week or the user defined holiday. The Facework manager can define up to 5 schedules. The detailed setup process of user schedule is as follows;

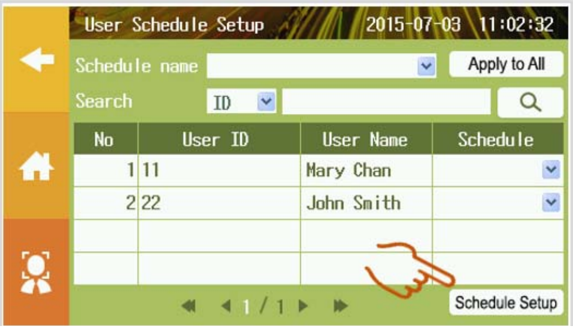
Touch ‘User Schedule’ in the Option Menu, then the Facework lists the users assigned schedule on the user list table of the ‘User Schedule Setup’ window by default.

① Create the schedule.

a. Touch <Schedule Setup> [Figure 53].

b. Touch any point on the user list table [Figure 54]. Then the Facework shows ‘Schedule Setup’ window [Figure 55].

c. Enter Schedule name in the ‘Name’ field [Figure 55 (a)].



User Schedule Setup 2015-07-03 11:02:32

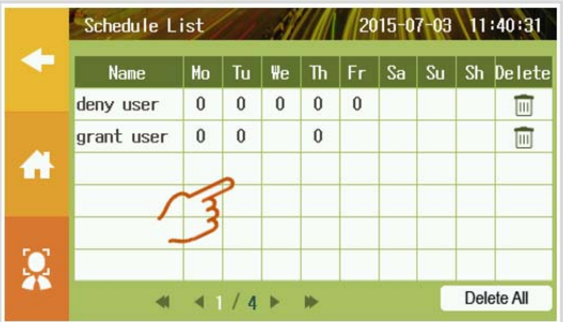
Schedule name

Search ID

No	User ID	User Name	Schedule
1	11	Mary Chan	
2	22	John Smith	

[Figure 53] User Schedule Setup

d. Select ‘Grant’ or ‘Deny’ at Schedule type [Figure 55 (b)]. The ‘Grant’ enables the Facework to authenticate for the time zone specified by the schedule. On the country, the ‘Deny’ enables the Facework to block authentication for the time zone specified by the schedule.



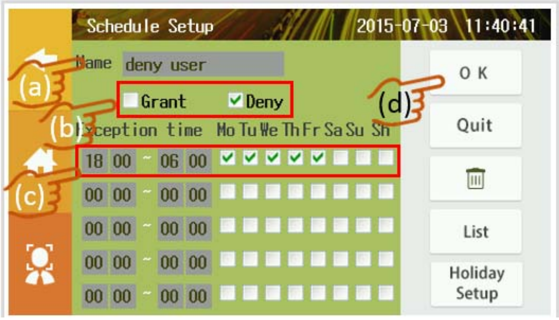
Schedule List 2015-07-03 11:40:31

Name	Mo	Tu	We	Th	Fr	Sa	Su	Sh	Delete
deny user	0	0	0	0	0				🗑
grant user	0	0		0					🗑

[Figure 54] Schedule List

e. Define the time zone and day of the week or the user-defined holiday to deny or grant authentication [Figure 55 (c)].

f. To save the schedule, touch <OK> button [Figure 55 (d)].



Schedule Setup 2015-07-03 11:40:41

Name deny user

□ Grant ☑ Deny

Exception time	Mo	Tu	We	Th	Fr	Sa	Su	Sh
18 00 ~ 06 00	☑	☑	☑	☑	☑	□	□	□
00 00 ~ 00 00	□	□	□	□	□	□	□	□
00 00 ~ 00 00	□	□	□	□	□	□	□	□
00 00 ~ 00 00	□	□	□	□	□	□	□	□
00 00 ~ 00 00	□	□	□	□	□	□	□	□

[Figure 55] Schedule Setup

② Apply the schedule to a specific user.

a. Explore or find a specific user to apply the schedule in the ‘User Schedule Setup’ window.

b. Touch the drop down list on the ‘Schedule’ column of the user list table and select the schedule name to apply [Figure 56]. To delete the schedule applied to the user, select blank value.

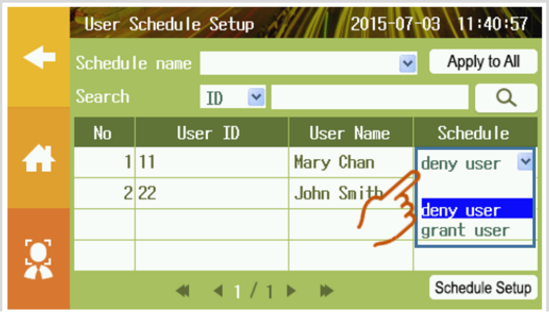
③ Apply the schedule to all users.

a. Find the schedule name to apply to all users from the drop down list at the Name field.

b. Touch <Apply to All>.

④ List the schedule

a. In the ‘Schedule Setup’ window, touch <List> button [Figure 55]. Then the Facework shows the user-defined schedule list.



No	User ID	User Name	Schedule
1	11	Mary Chan	deny user
2	22	John Smith	

deny user
grant user

[Figure 56] Apply the Schedule to user

⑤ Remove the schedule from the user(s).

a. To remove the applied schedule from user, select blank value at the ③(c).

b. To remove the applied schedule from all users, select blanks value at the ④(a) and touch <Apply to All>.

⑥ Add / Modify / Delete user-defined holiday(s).

a. In the ‘Schedule Setup’ window [Figure 55], touch <Holiday Setup> button.

b. Execute the same steps as guided at the section “9.6 Device Schedule.④”

- A specific user must have only one schedule type (Grant or Deny).
- When time zones are overlapped from multiple schedules, it blocks or grants the user authentication depending on the schedule type from the earliest time to the latest time across those time zones.
- When the time zone is spanned over two days (ex: 23:00 on Monday to 06:00 on Tuesday), touch the box on the day of the week starting the schedule when to set the schedule.
- If the schedule is conflicted between the Device schedule and the User schedule, the User schedule has priority.

9.8. Others:

In this menu, the Facework manager can setup the followings:

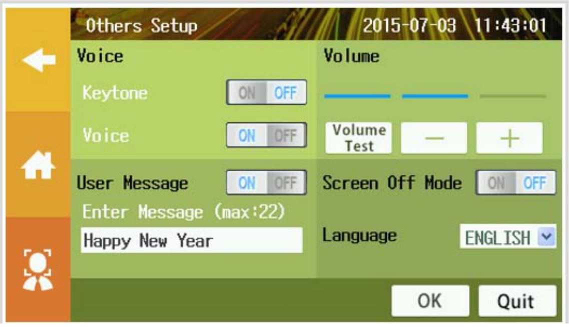
① Activate or deactivate the key tone with the switch ON or OFF.

② Activate or deactivate the voice message with the switch ON or OFF.

③ Activate or Deactivate user defined message. If the switch is set to ON, enter text message in the text box.

Then the input text is displayed on the face recognition window [Figure 58].

④ Adjust the system volume with < + > and < - > key touch. It has 3 levels of sound volume. After setting the volume level, volume sound can be tested with <Volume Test> button touch



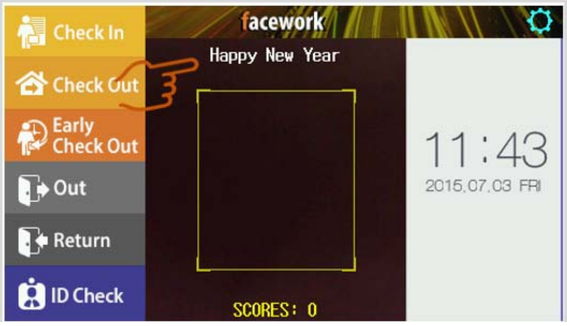
Happy New Year

ENGLISH

[Figure 57] Other Options

⑤ Enable or Disable the 'Screen Off Mode' with the switch ON or OFF. If the switch is set to 'OFF'. The Facework device disables the Screen Off mode in the face recognition window.

⑥ Set the default language being used in the Facework device. The current version 1.2.5 supports only English as default language.



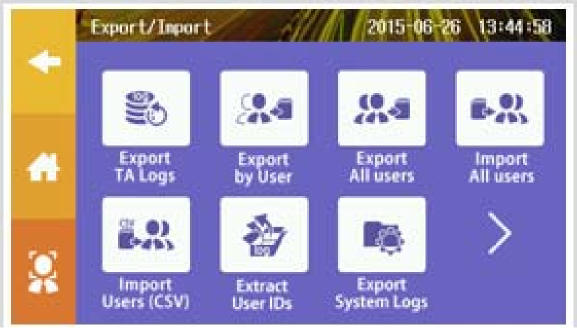
Happy New Year

[Figure 58] Displaying User defined Message

⑦ After setting all values, touch <OK> button to save it.

10. Export / Import

This menu can execute backup & restore of user templates, access logs. Additionally it can execute firmware update at here. Before executing this menu, plug the USB memory into the USB port on the Facework device. Its detailed functions for setup procedures are as follows:



[Figure 59] Export/Import Window (1)

① Export TA Logs:

It extracts all time attendance logs on the Facework device to the USB memory. When you touch this menu, it displays the pop-up window to confirm the task and touch <OK> to continue it.

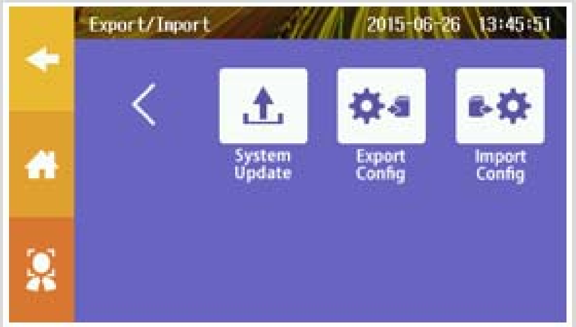
② Export by User:

It extracts individual user(s) to the USB memory. The followings are detailed export processes.

a. To select the user, touch ☑ on the line holding the user name [Figure 61 (a)]. The Facework manager can select multiple users by repeating this step.

b. After user selections, the Facework manager can list all selected users on the user list table by touching ☑ next to the magnifier symbol [Figure 61 (b)].

c. After selection, touch <Export> to export the user(s) to the USB memory.



[Figure 60] Export/Import Window (2)

But in the case that many users are saved in the Facework device, you can explore the user by ID or User name with:

d. Select the key in the drop down list.

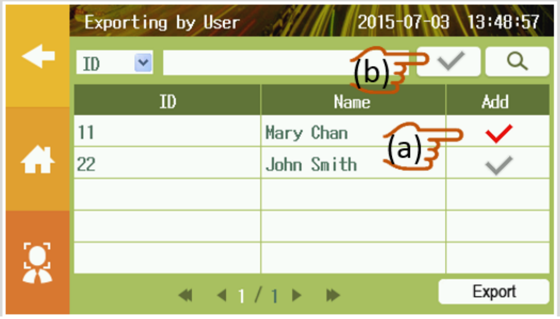
e. Enter ID or Name depending on the key selection.

f. Touch the magnifier symbol.

g. Touch ☑ symbol on the line holding the user name.

h. Touch <Export>.

i. For multiple user selection with other user name, repeat the step (d) to (g) and finally touch <Export> to export all selected users.



ID	Name	Add
11	Mary Chan	✓
22	John Smith	✓

[Figure 61] User selection for Exporting

③ Export All users:

The Facework manager can export all users to USB memory at once with this function. When this menu is touched, it displays the popup window for the confirmation. To continue it, touch <OK> button.

④ Import All users:

The Facework manager can import all users with this function. Unlike user exporting function, individual import is not supportable. Thus, the Facework always restores all users saved in the USB memory to the Facework. When this menu is touched, it displays the popup window for the confirmation. To continue it, touch <OK>.

⑤ Import Users (CSV):

This feature is reserved for future use purpose.

⑥ Extract User IDs:

This function extracts user ID and the folder number pointing to the position of a specific user template to excel file. This function is usually helpful for debugging an authentication error. After this function is done, you can find the excel file named UserIDMapFolderNum_xx.xls in the USB memory.

⑦ Export System Logs:

This function exports all access logs to the USB memory. The Facework manager needs to delete log files periodically as it can cause memory full error! The bundled ACMS can monitor the available storage size for all Facework devices connected to the ACMS server. The ACMS can periodically back up system logs and delete them to prevent this error.

⑧ System Update:

The Facework firmware can be sometimes released under the necessity of adding more functions or bug fixes. The detailed update process is as follows;

a. Download the firmware from our partner website to the USB memory connected to the computer.

b. Connect the USB memory to the Facework USB port, placed the right side of the Facework.

c. Touch <System Update> button.

d. The Facework will update it automatically.

⑨ Export Config:

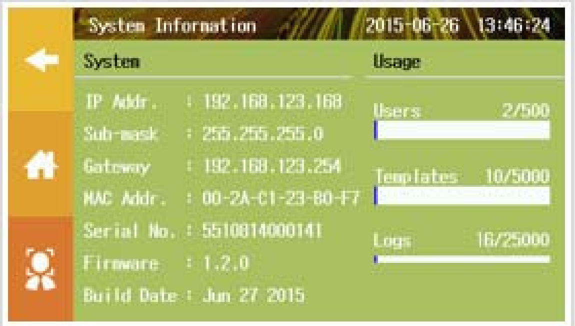
This function extracts all of configuration parameters currently set to the Facework to the USB memory.

⑩ Import Config:

This function is used to restore the extracted configuration parameters into the Facework device from the USB memory.

11. System Information

In this menu, the Facework manager can check network information, firmware version, and #of enrolled users, #of saved templates and #of accessed logs in the Facework [Figure 62].



System Information 2015-06-26 13:46:24

System

IP Addr. : 192.168.123.168
Sub-mask : 255.255.255.0
Gateway : 192.168.123.254
MAC Addr. : 00-2A-C1-23-B0-F7
Serial No. : 5510814000141
Firmware : 1.2.0
Build Date : Jun 27 2015

Usage

Users 2/500
Templates 10/5000
Logs 16/25000

[Figure 62] System Information Window

FCC Compliance Information

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules.
These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.
Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This device complies with Part 15 of FCC Rules. Operation is subject to the following two conditions:
(1) the device may not cause interference, and (2) the device must accept any interference, including interference that may cause undesired operation of this device.