MAG Etegra Access Control

Integrated Access Control and Security System

MAG Etegra (ME-ACS) is an advance client / server access control software that is designed exclusively for Soyal's card and fingerprint access system. It extends SOYAL functionality to the next level with integrated CCTV surveillance, alarm monitoring and advanced time attendance functions. ME-ACS is fully loaded with powerful features into a single platform to achieve centralized security, surveillance and attendance management for small to big business operations.

WWW.MAG-ETEGRA.COM.MY

Table of Content

1) Introduction

MAG Etegra (ME-ACS)

MAG Etegra (ME-ACS) extends SOYAL hardware original capability and integrates all of them into single software for centralized **Access Control**, **Alarm Monitoring, Time Attendance** and **CCTV Surveillance**. ME-ACS supports client server architecture which allows control and management from a remote site over LAN or internet network.

MAG Etegra (ME-ACS) support the following function:

1) Door access
2) Elevator access
3) Parking access
4) Turnstile access
5) Fingerprint biometric access
6) Multi-shift time attendance
7) Access control monitoring, include area control monitoring, camera monitoring, door monitoring, E- map monitoring, I/O monitoring, IN/OUT monitoring and User Profile Monitoring. *(NEW **)*
8) CCTV video and picture capture.

MAG Etegra (ME-ACS) benefits are:

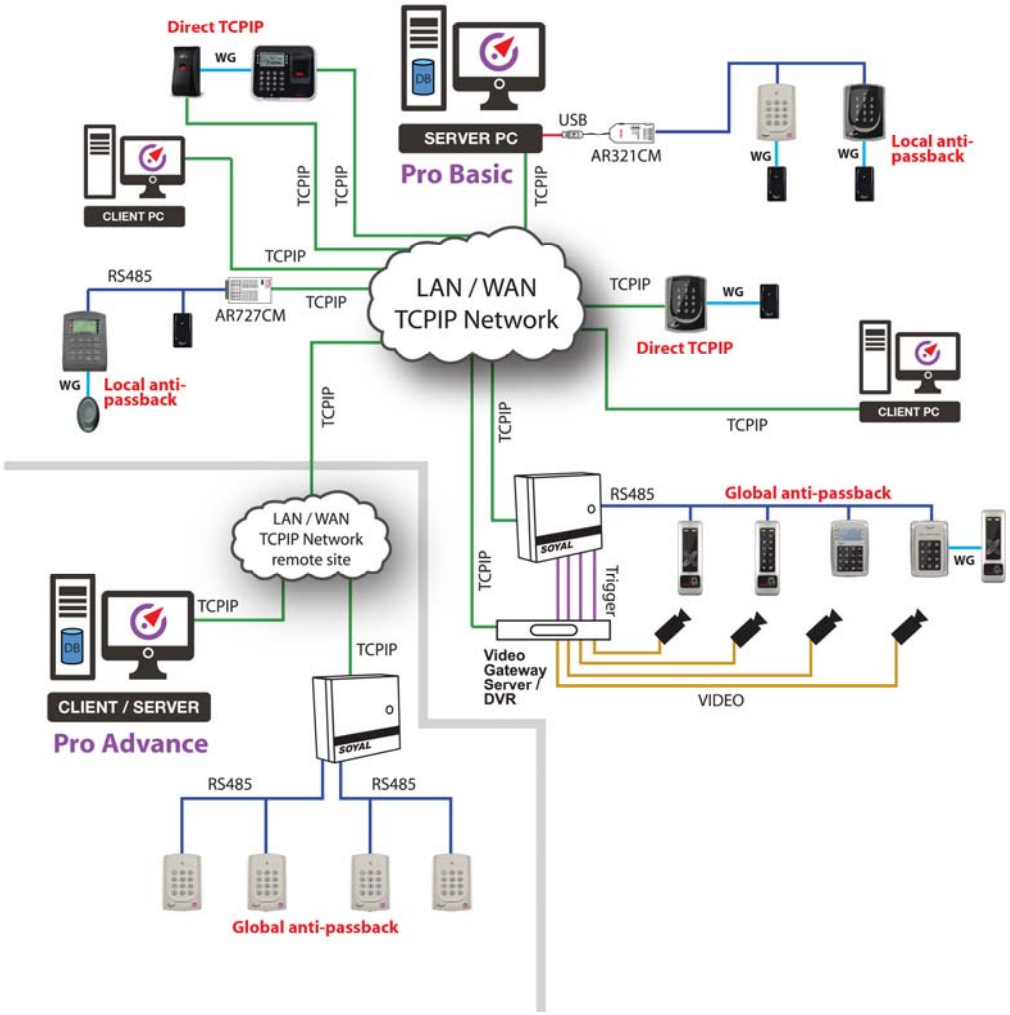
1) GUI has been optimized to provide very clean, uncluttered and simple interface yet with powerful functions beneath it. Skin color theme and background image can be changed to suit different user preferences.
2) SQL based database to fully support smooth operation in networking environment.
3) Client / Server architecture for maximum security. Server can be protected in secure room. All operators can only access the server via limited function using client.
4) Integrated alarm and CCTV monitoring allow operator to quickly check alarm event with picture and video. Visual evidence always provides a clearer picture of what is happening.
5) Integrated access and CCTV monitoring to capture picture on all users that badge card. Operator can visually verify the authentication user to catch "buddy punching". Guard can use this feature to easily verify all vehicles in and out of premises.

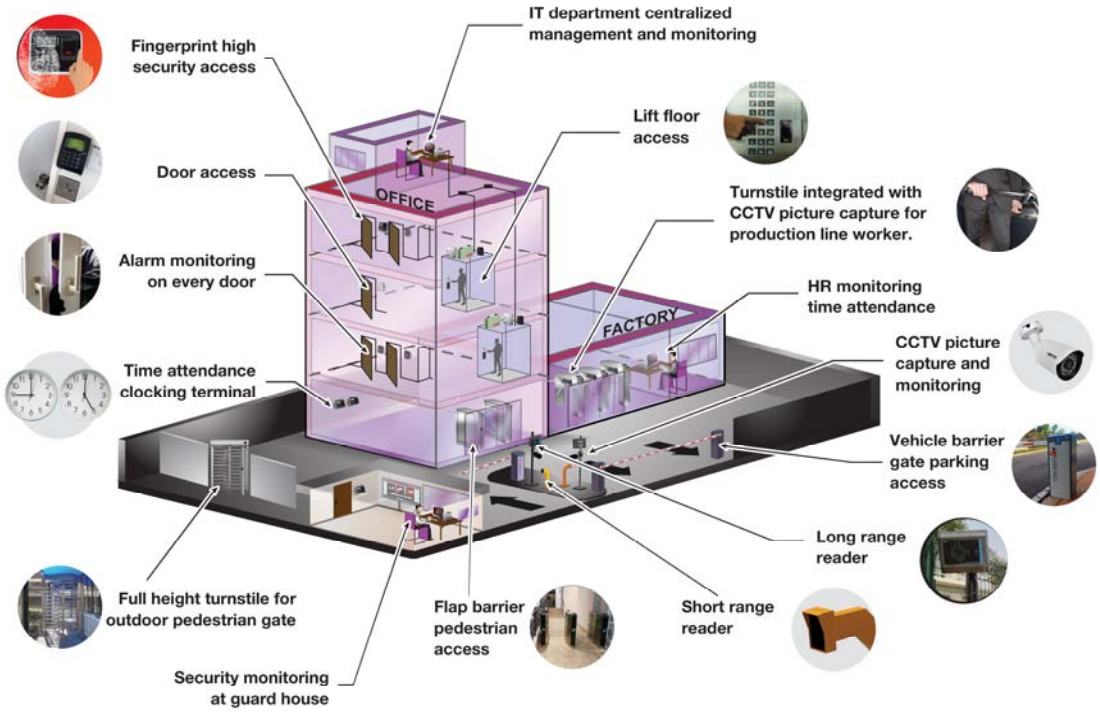
How to install the program and get started is explained in the Getting Started section.

PC minimum specifications:

Specifications	Requirements
a) Operating system	• Win 7 *64-bit* • Win 8 *64-bit* • *Win 10 64-bit*
b) Memory	• 4GB - Minimum standalone *or* • 8GB - Optimum performance if running picture capture and multi network environment.
c) HDD space	• 1GB for installation files. • 20GB for Microsoft SQL Server 2014 and database.

Client / Server Architecture Diagram





2) Getting started

Insert MAG Etegra (***ME-ACS***) DVD installer disc into DVD ROM drive, and select the compatible system for the PC OS by select the correct folder, there is *ME-ACS 64-bit Setup (Refer Fig 2.0.1).* Please read the installation guide before start the installation.

The information inside the CD:

DVD ROM Drive → *1. ME_ACS 64-bit Setup* → ***DatabaseSetup64.exe*** & ***ME-ACS_v6_Setup.exe***

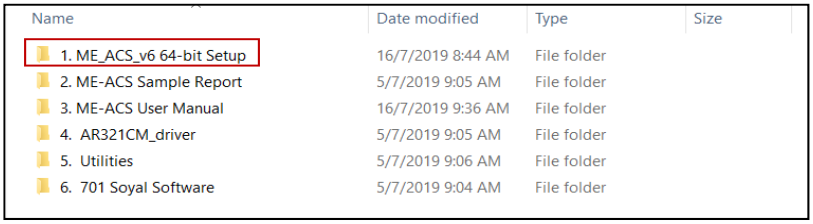


Fig 2.0.1: ME-ACS 64-bit installer folder.

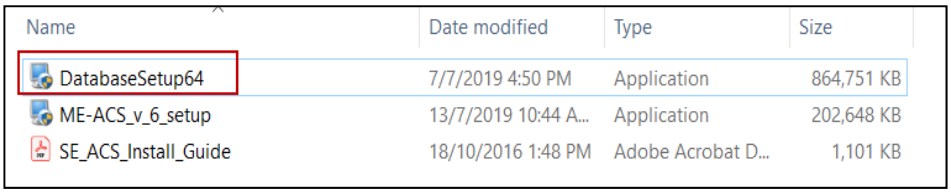


Fig 2.0.2: ME-ACS 64-bit installation.

The process of installation:

Step 1: Database installation - *Run the DatabaseSetup64.exe*

Step 2: ME-ACS installation - Run the *ME-ACS_setup.exe*

Step 1: Database Installation

a) Double-click on *DatabaseSetup64.exe* to start the database installation.

DVD ROM Drive → *1. ME-ACS 64-bit Setup* → *DatabaseSetup64.exe*

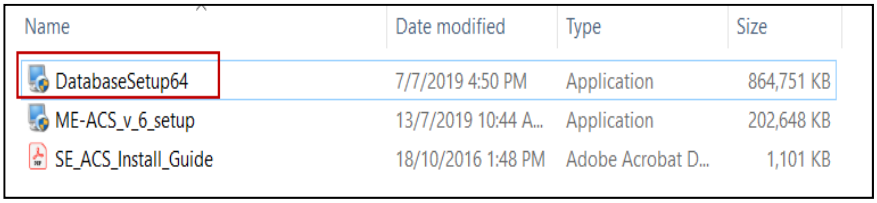


Fig 2.1.0: ME-ACS 32-bit or 64-bit installation.

b) If the system which not yet install SQL Server 2014 Express will prompt to request to install it. Please click **OK** button to install it.

c)

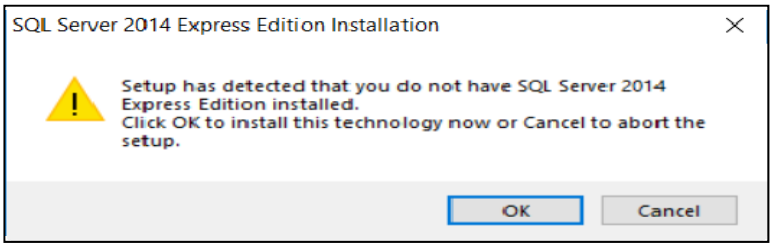


Fig 2.1.1: SQL Server 2014 Express Edition installation.

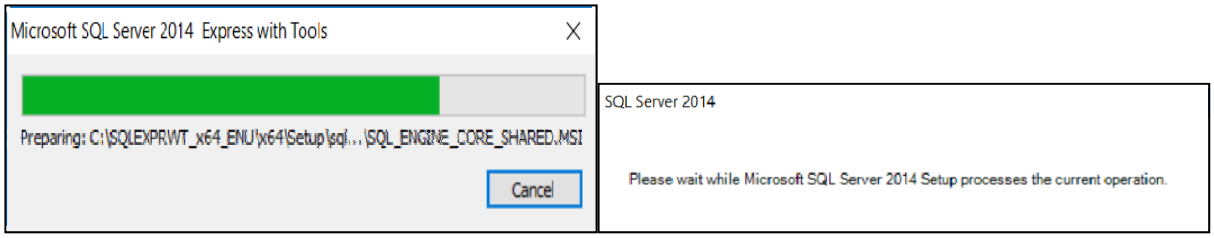


Fig 2.1.2: ***SQL Server 2014 Express Edition installation in progress.***

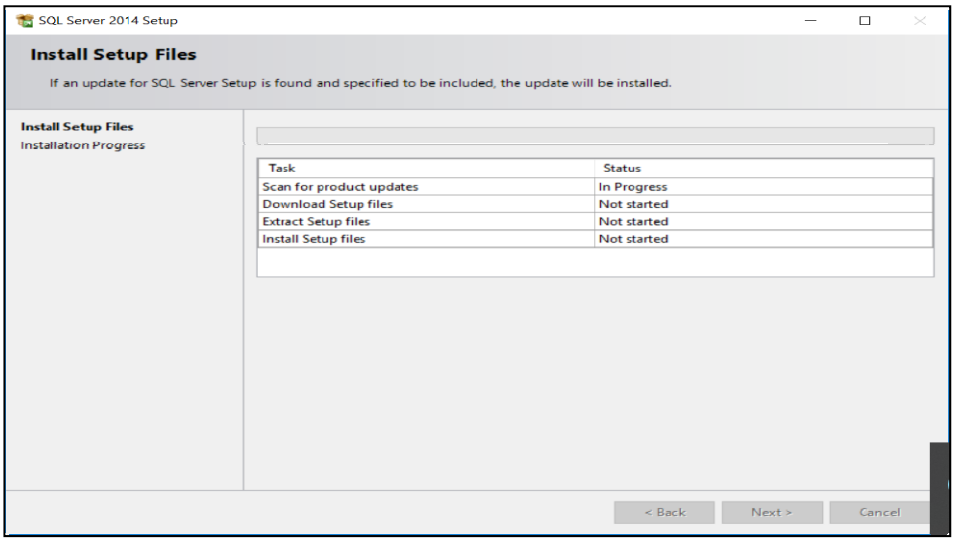


Fig 2.1.3: ***SQL Server 2014 Express Edition installation in progress.***

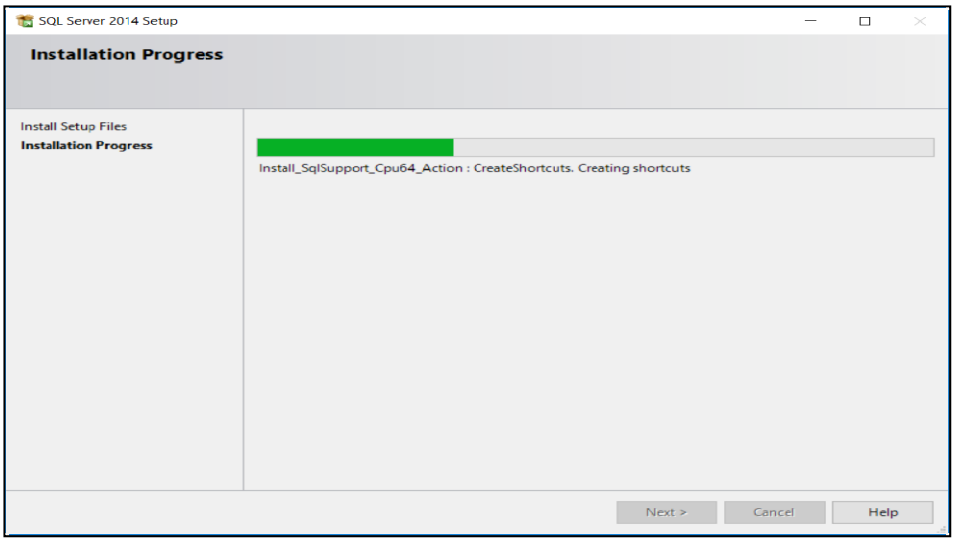


Fig 2.1.4: ***SQL Server 2014 Express Edition installation in progress.***

d) At the welcome screen, click on **Next** button to continue.

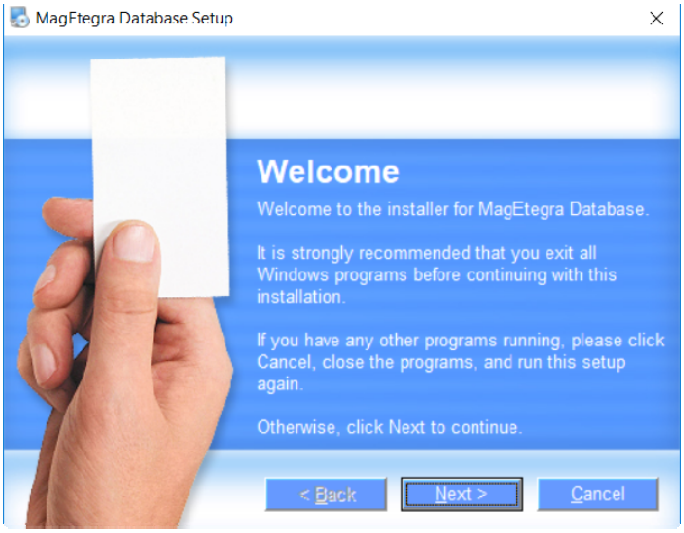


Fig 2.1.5: Click on Next to continue ME-ACS setup.

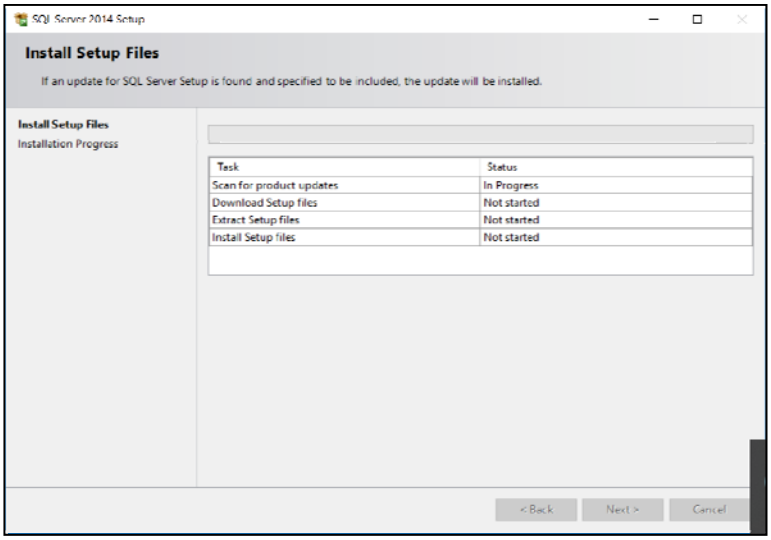


Fig 2.1.3: SQL Server 2014 Express Edition installation in progress.

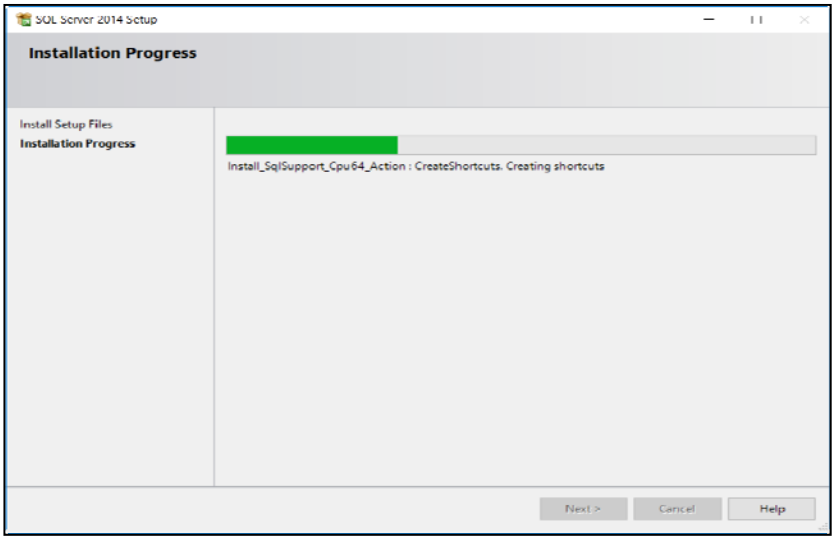


Fig 2.1.4: SQL Server 2014 Express Edition installation in progress.

e) At the welcome screen, click on **Next** button to continue.

Fig 2.1.5: ***Click on Next to continue ME-ACS setup.***

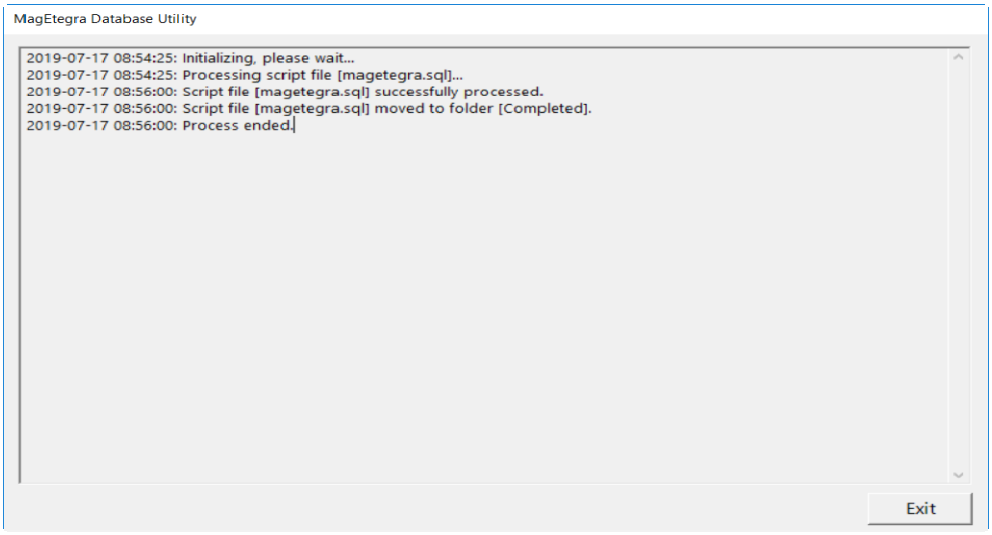


Fig 2.1.9: ***The installation of ME-ACS database.***

f) When message box just like below will prompt. Click **Finish** button to close it.

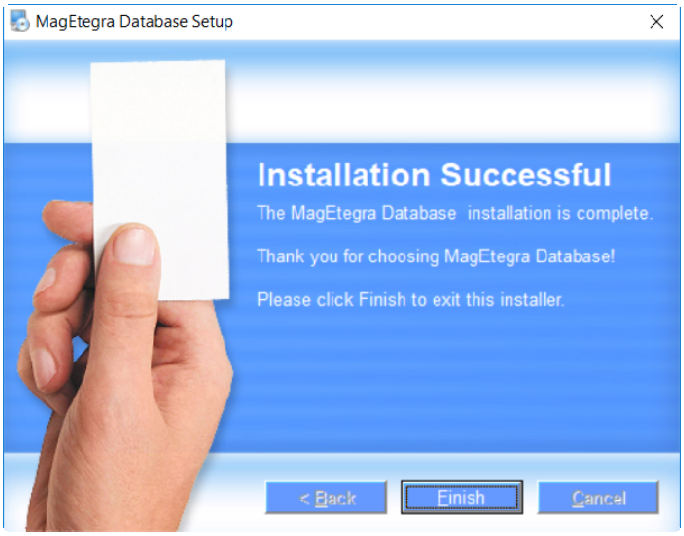


Fig 2.1.10: ***The SQL database installation is successful and clicks on Finish to close it.***

Step 2: ME-ACS Installation

a) Double-click on *ME_ACS_setup.exe* to start the ME-ACS installation.

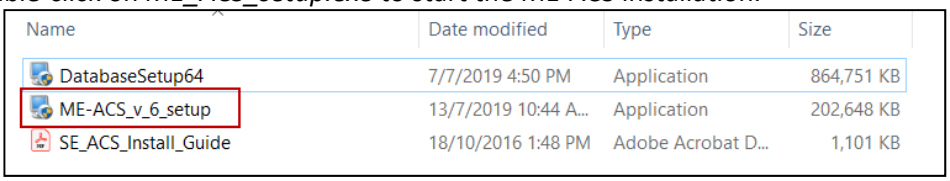


***Fig 2.2.0:* ME-ACS 64-bit installation.**

b) At the welcome screen, click on **Next** button to continue.

***Fig 2.2.1:* Click on Next to continue ME-ACS setup.**

c) Read the EULA and click on **Next** button upon checking the Agree radio box.

***Fig 2.2.2:* If you agree the terms of license agreement and click the Next to continue.**

d) Select the MAGClient and MAGServer and click on **Next** button to proceed.

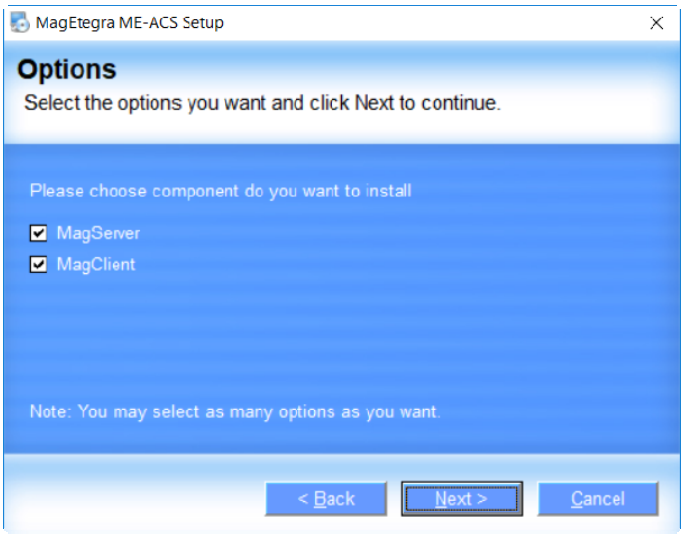


***Fig 2.2.3:* Select the components you want to install.**

e) Click on **Next** button to continue.

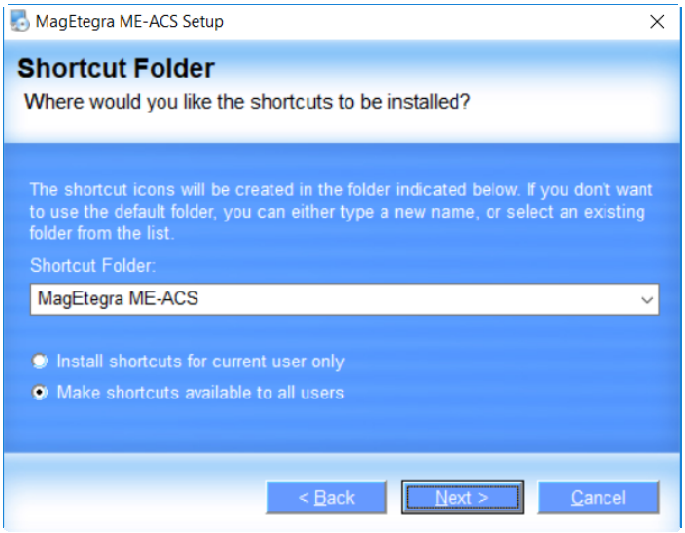


***Fig 2.2.4:* Click on Next to continue ME-ACS setup.**

f) Fill in user information and click on **Next** button.

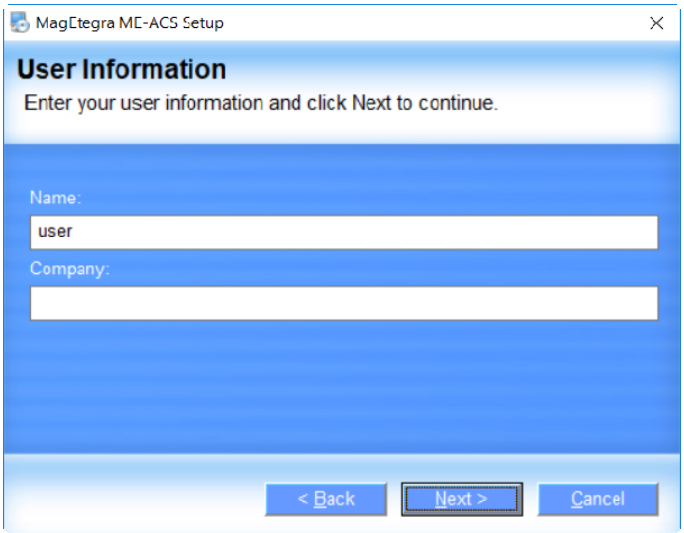


***Fig 2.2.5:* User information.**

g) Click on **Next** button to start the installation.

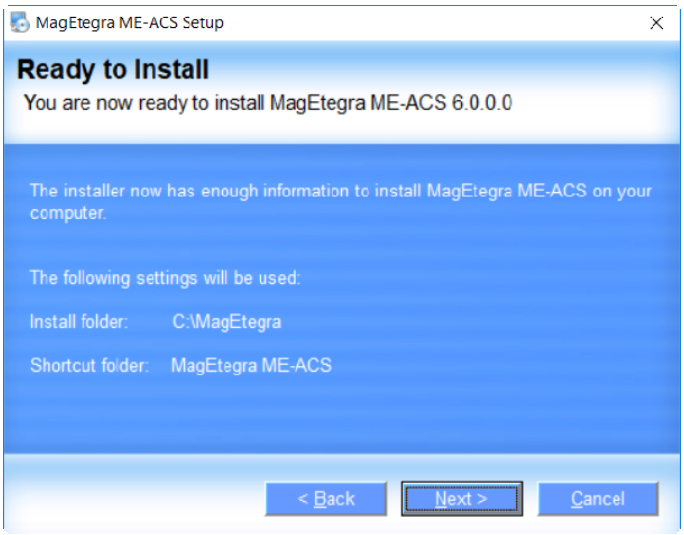


Fig 2.2.6: ***Ready to install process.***

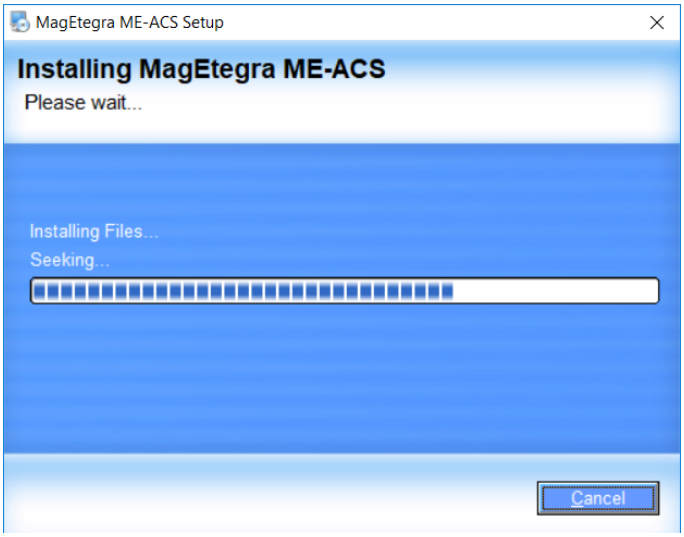


Fig 2.2.7: ***Installation in progress.***

h) When the message box just like below (Refer Fig 2.2.8), then click on **NEXT** button to install it.

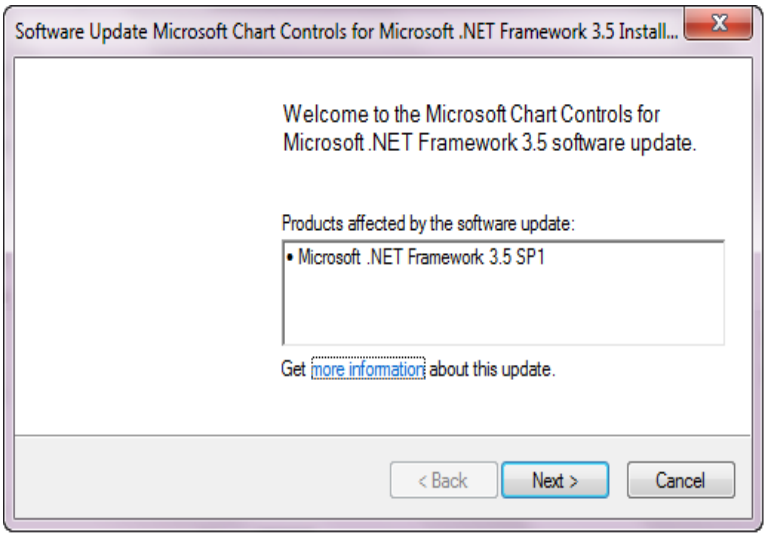


Fig 2.2.8: ***MSchart.exe installation.***

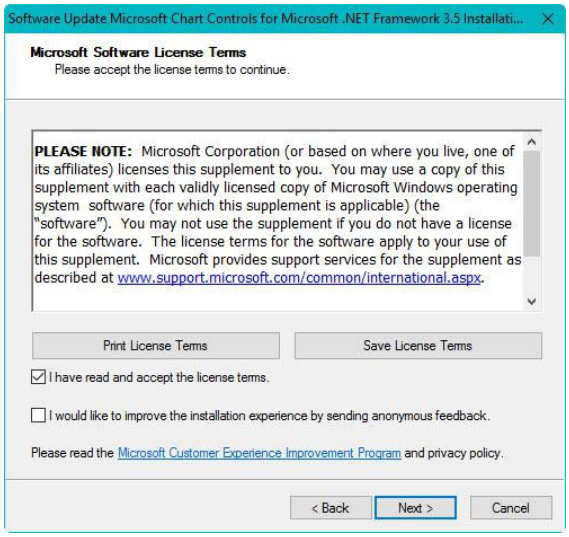


Fig 2.2.8: ***MSchart.exe installation.***

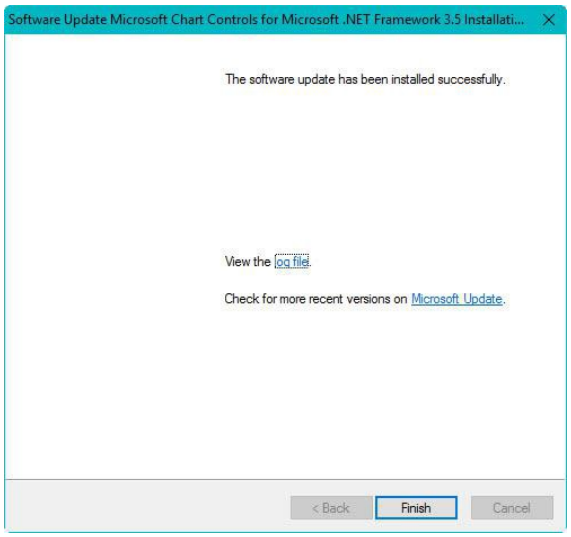


Fig 2.2.10: ***Mschart installation complate.***

i) Setup will continue with SAP Crytal Reports installation.

Fig 2.2.11: ***SAP Crystal Reports installation.***

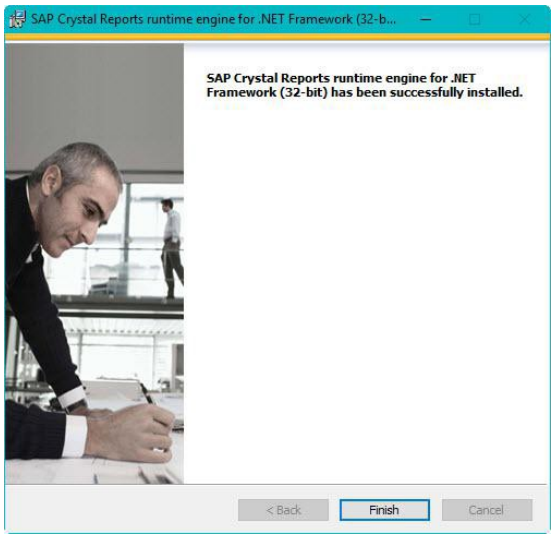


Fig 2.2.12: SAP Crystal Reports finish.

j) Setup will continue with SQL Server 2014 Management Objects Setup.

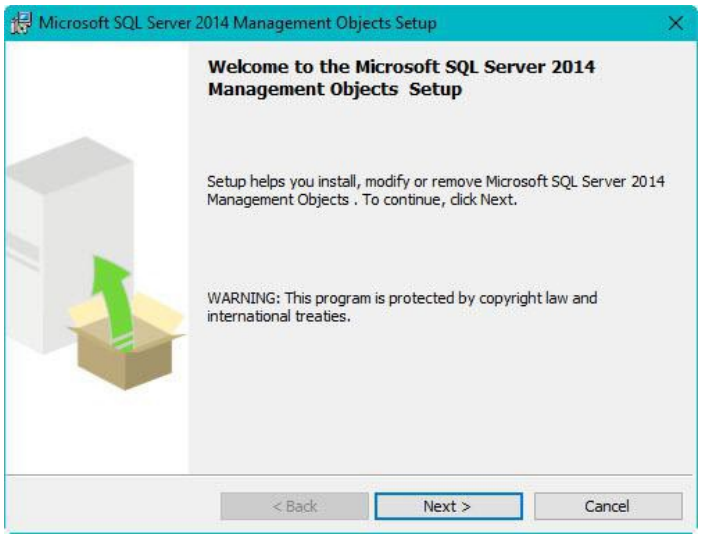


Fig 2.2.13: SQL Server 2014 Management Object.exe installation

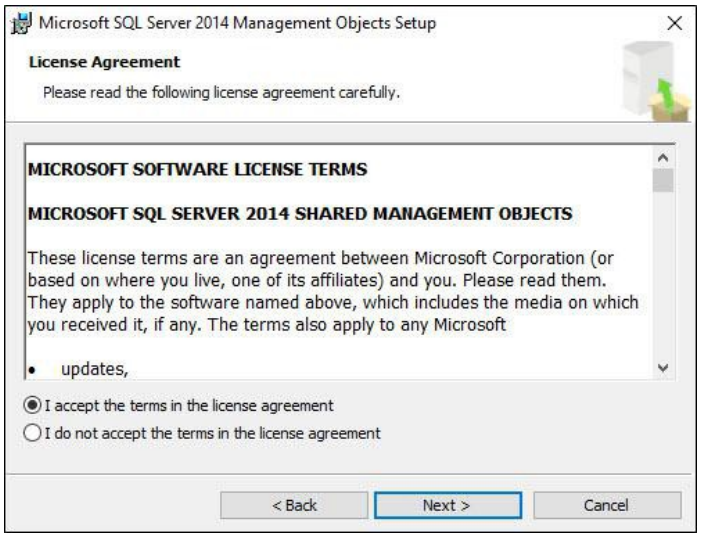


Fig 2.2.14: If you accept the term of license agreement, then click the Next to continue process of installation.

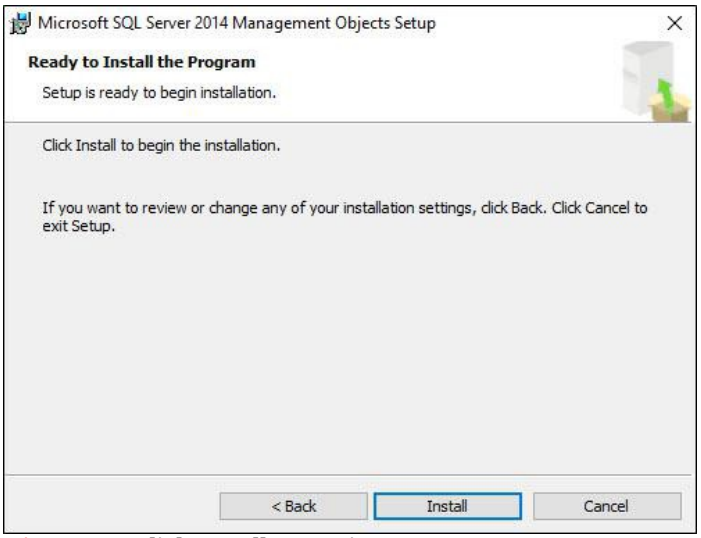


Fig 2.2.15: Click Install to continue SQL Server 2014 Management Object.

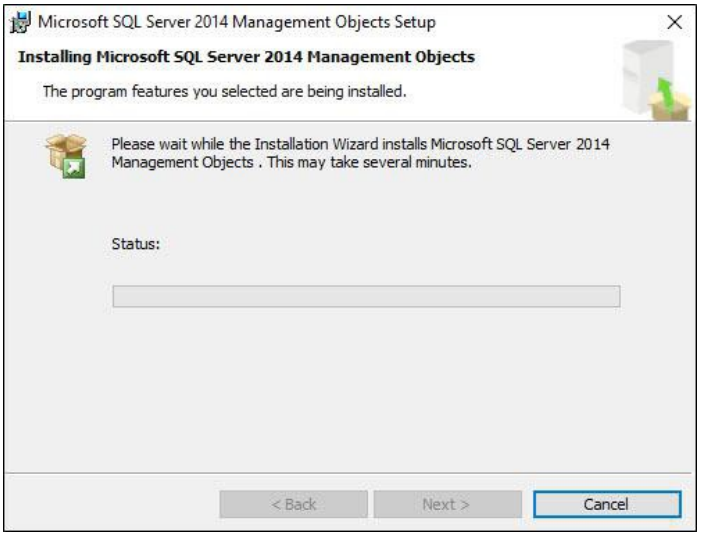


Fig 2.2.16: Installation

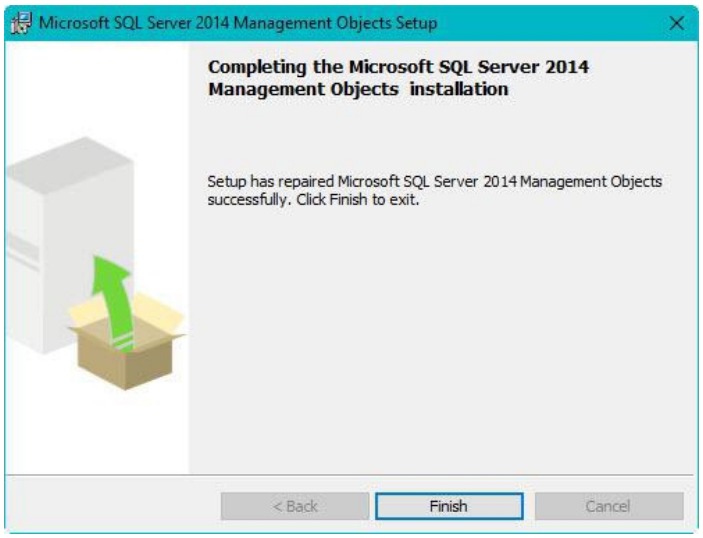


Fig 2.2.17: Installation finish.

k) When the message box just like below will prompt and click on **Finish** button to close it.

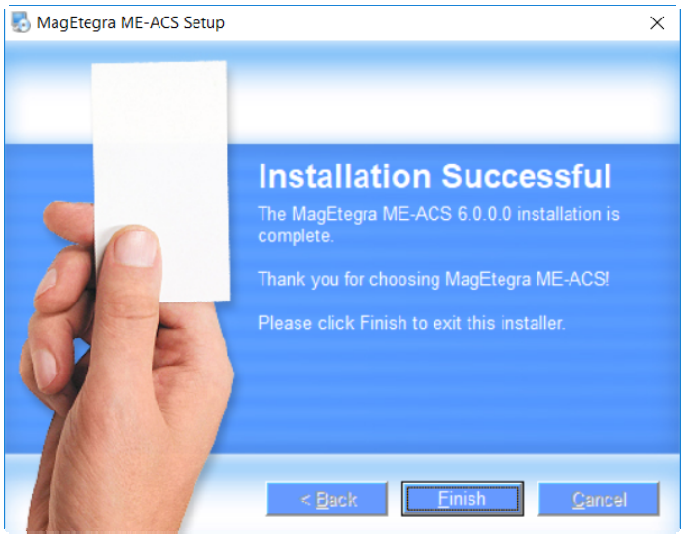


***Fig 2.2.9:* The ME-ACS installation is successful and clicks on Finish to close it.**

**** Note:**

The following 2 shortcut icons will be created in desktop.

- *MAGClient* is the **client** application. You can use the Client application for settings, viewing reports and all monitoring function available.

- *MAGServer* is the **server** application. Server responsibility is to run in the background managing communication with hardware controller.

If fail to read report in pdf format in ME-ACS system. Please install the SAP Crystal Report runtime to view:

DVD ROM Drive → *6. Utilities* → *6.14 SAP CrsytalReports* → ***CRRuntime_x32_13_0_13.msi***

**** Note:**

Please install the SAP Crystal Report runtime to view the reports in ME-ACS system:

DVD ROM Drive → *5. Utilities* → *6.14 SAP CrsytalReports* → ***CRRuntime_x32_13_0_13.msi***

2.3 Starting The Program

To start ME-ACS, click the *MAG Client* icon found in the Start menu, in Programs / ME-ACS. For first time installation it is **compulsory** to run MAG Etegra client first. Running server first will cause improper operation. Registration is needed when running client for the first time.

Attention: Make sure the MAG Client and MAG Server are **Run as administrator.

Right-click MAG Client icon→Properties →click Advance in Shortcut tab →Tick Run as administrator →OK.

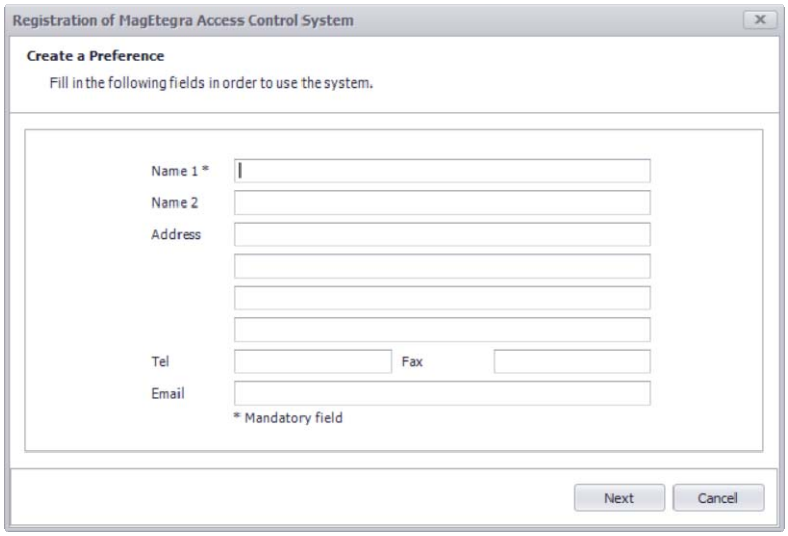


***Fig 2.1:* User information.**

Only Name 1 is mandatory field. Enter the serial number when you purchase. Package *(Lite, Professional Basic or Professional Advanced)* selection must be matched with the serial number entered.

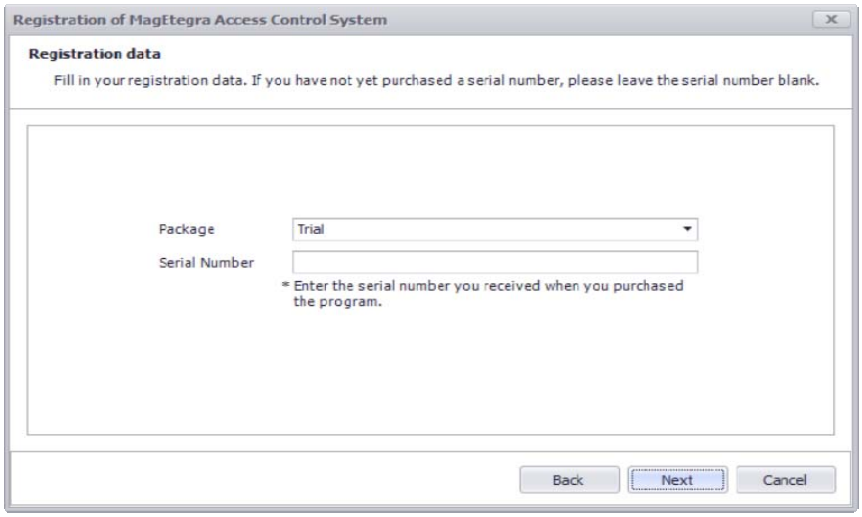


***Fig 2.3.2:* Registration data and package of ME-ACS versions.**

Registration completed. You must activate the software ***within 60 days*** from a successful registration. Software can be activated from the Licensing Management by submitting Serial number and MAC address to activate@soyal.com.my. Upon verification, an activation key will be send back to you.

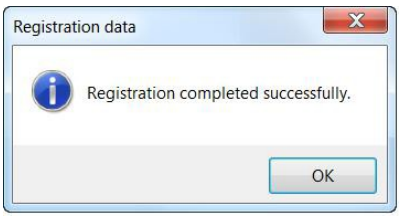


***Fig 2.3.3:* Registration completed successfully.**

Enter the default user name ***"ADMIN"*** and default password ***"123456".*** It is recommended that you change the login name and password before final deployment to avoid unauthorized usage of ME-ACS.

Fig 2.3.4: ***The default ME-ACS login setting just like as below:***

User ID ***:*** *ADMIN*
Password : *123456*

After fill in it, then click on Login.

ME-ACS MAG Client will show current event log by default upon a successful login.

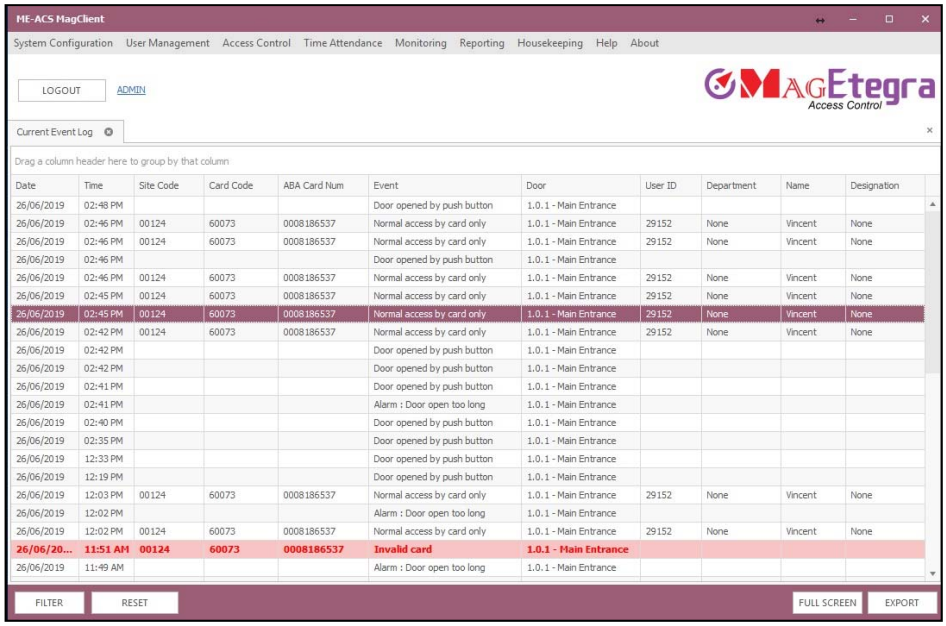


Fig 2.3.5: ***The default view of ME-ACS after login.***

From desktop, double-click the **MAG Server** icon to run the MAG server system.

3) System Configuration

The system configuration module is responsible for managing the settings for the Card Access Hardware, Card Users and the System functionality. There are 9 functions under this module: ***Hardware Manager, Preferences, Download, Operator Management, Function Access Authority, Control Panel, Branch, Department and Designation****.*

3.1 Hardware Manager

Hardware Manager is used to configure hardware connecting and hardware operation parameter for multi site networking environment. Hardware Manager allows controllers from local site (USB or LAN TCPIP) and remote site (WAN TCPIP) to be managed from a centralized Server PC. Operator can add new hardware, read/write hardware parameter and define remote/local site communication via Hardware Manager.

Hardware Manager consists of **Site Manager** (LEFT SIDE) and **Controller Manager** (RIGHT SIDE). Site Manager allows you to setup communication related to local and remote site. Controller Manager allows you to add/edit/delete hardware under a site.

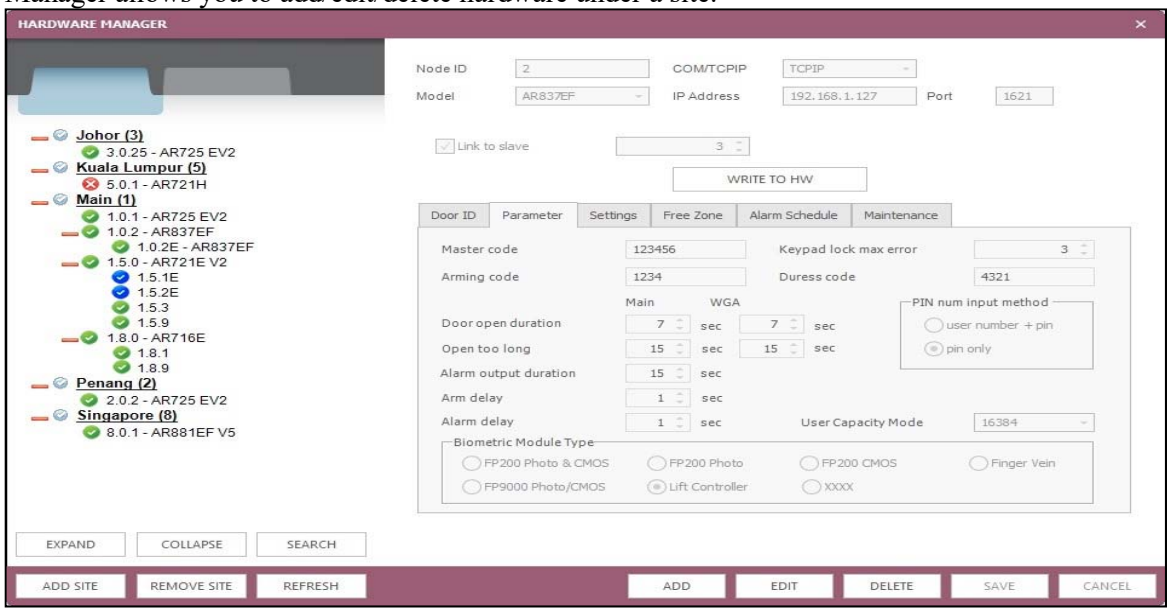


Fig 3.1.1: ***The Hardware Manager settings and operations.***

Controller that is online (connected) under each site is indicates as **GREEN** tick. Controller that is offline (disconnected) under each site is indicates as **RED** cross. Controller offline might be caused by possible failure on hardware, wiring or communication network. Hardware Manager will mark controller as offline if controller failed to respond within defined Time Out period. Time Out setting is defined in Preference.

Note:

Expand: Use to expand all items under the Site Manager.

Collapse: Use to close all items under the Site Manager.

3.1.1 Site Manager

Select communication port (COM or TCPIP) for each site. Each site **can only have 1 COM port and 1 TCPIP port**. Multiple TCPIP port can be allowed when using purchased licensing. If not, all the reader will be reset into main default IP.

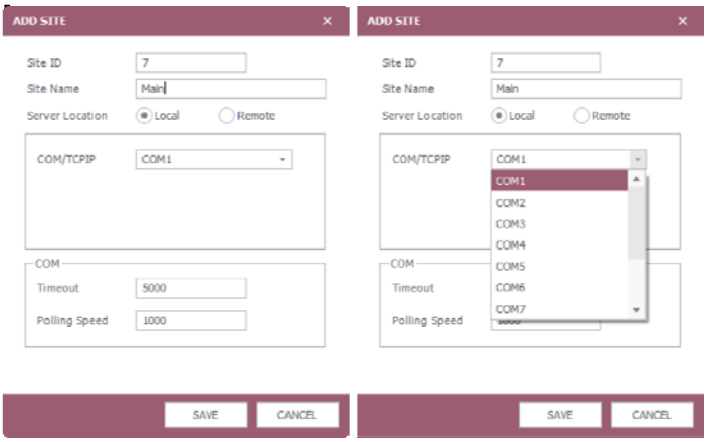


Fig 3.1.2: ***The COM port selection which will be used as communication port to interface with controllers.***

Note:

*** For example, if COM3 was selected, all controllers under this site shall be connected to COM3.*

***If there is a controller connected to COM6, it has to be added under another new site that uses COM6 as communication port.*

Adding Site

For Com Port selection*:*

(Com Port means all hardware is connected thru USB converter(**AR321CM**) to this PC).

1) Click on **ADD SITE** button.
2) Insert the Site Name and click on **SAVE** button. *(Refer Fig 3.1.2)*
3) Go to *COM/TCPIP*, click menu box and scroll down to select the correct COM port or communication port that will connect to the controllers.
   Note: The connected port can be check through device manager →Port (Refer to Prolific USB-to-Serial COM Port).
4) Click **SAVE** button to save it and the site will appear on the left panel.

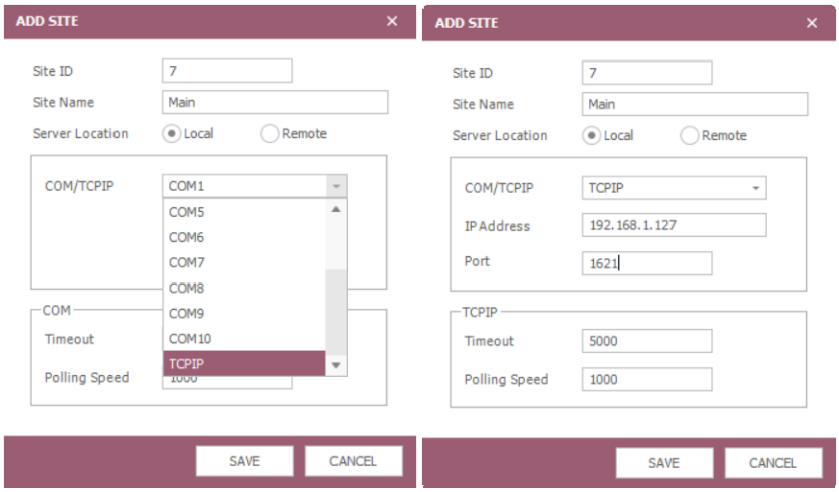


Fig 3.1.3: ***Select TCPIP and fill in the IP address and TCPIP port.***

Important Note:

*** TCPIP will auto-enable the Independent IP base on the license.*

*** For using trial or lite, all controllers under this site shall be connected through same IP and same port.*

*** For using Pro Basic or Adv, the readers under this site can be changed with different IP's and ports. For those readers was not change will use the default IP and port.*

For TCPIP selection:

(TCPIP means all hardware is connected thru LAN (**Local Area Network**)/WAN (**Wide Area Network**) to this PC.

1) Click on the **Add Site** button.
2) Insert the *Site Name*.
3) Go to COM/TCPIP, click menu box and scroll down to select the TCPIP. *(Refer Fig 3.1.3)*
4) Make sure that you key in the IP address and Port number. *(Refer Fig 3.1.3).*
5) Click **Save** button to save it and the site will appear on the left panel.

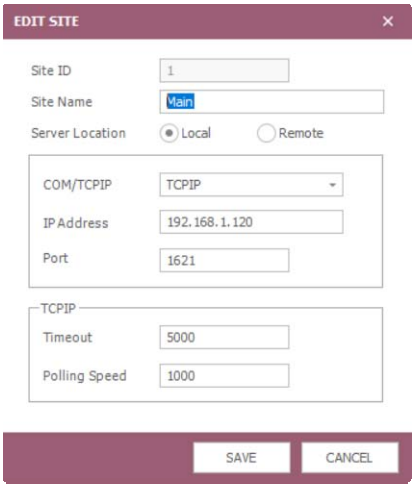


***Fig 3.1.3a:* Edit Site for changing TCP/IP**

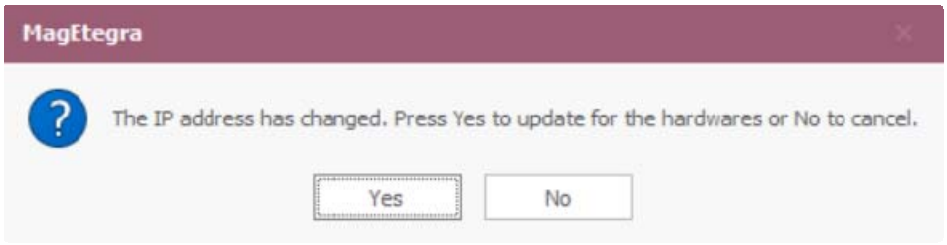


***Fig 3.1.3b:* Notification to update multiple hardware**

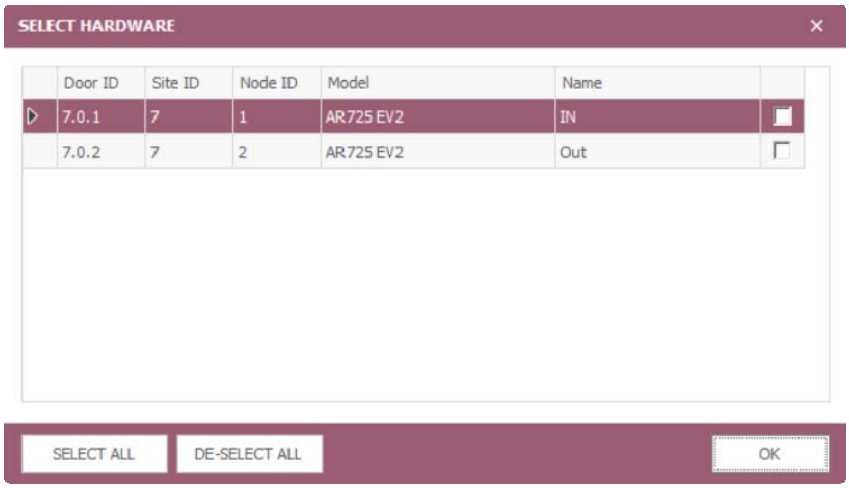


***Fig 3.1.3c:* Hardware selection for updating IP address**

Edit Site for Trial/Lite license

1) Right click on the site names under the controller list tab.
2) Click on the **Edit** button.
3) Edit the changes from the pop up Edit Site screen. *(Refer Fig 3.1.3a)*
4) Click on **Save** button to update the changes.

Edit Site for TCP/IP or Dynamic DNS (Standard/Pro Basic/Advance)

1) Right click on the site names under the controller list tab.
2) Click on the **Edit** button.
3) Edit the changes from the pop up Edit Site screen. *(Refer Fig 3.1.3a)*
4) Upon click on **Save** button notification will prompt *(Refer fig 3.1.3b)*
   a) Cick on **Yes** button to change multiple hardware IP address *(Refer fig 3.1.3b)*
   b) Select the hardware and click **OK** button to update selected controller *(Refer fig 3.1.3c)*
   Note
   *** For using **AR727CM** only*
   b) Click **No** button for changing site DDNS only
   Note
   *** For connection using DDNS only*

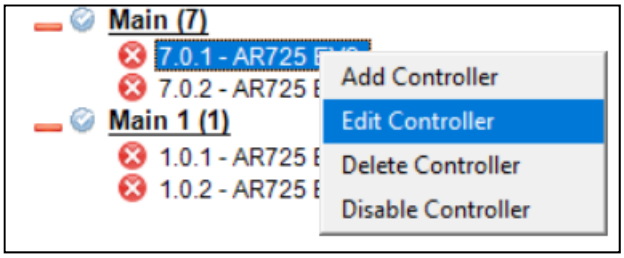


Fig 3.1.3d: ***Edit Controller selection***

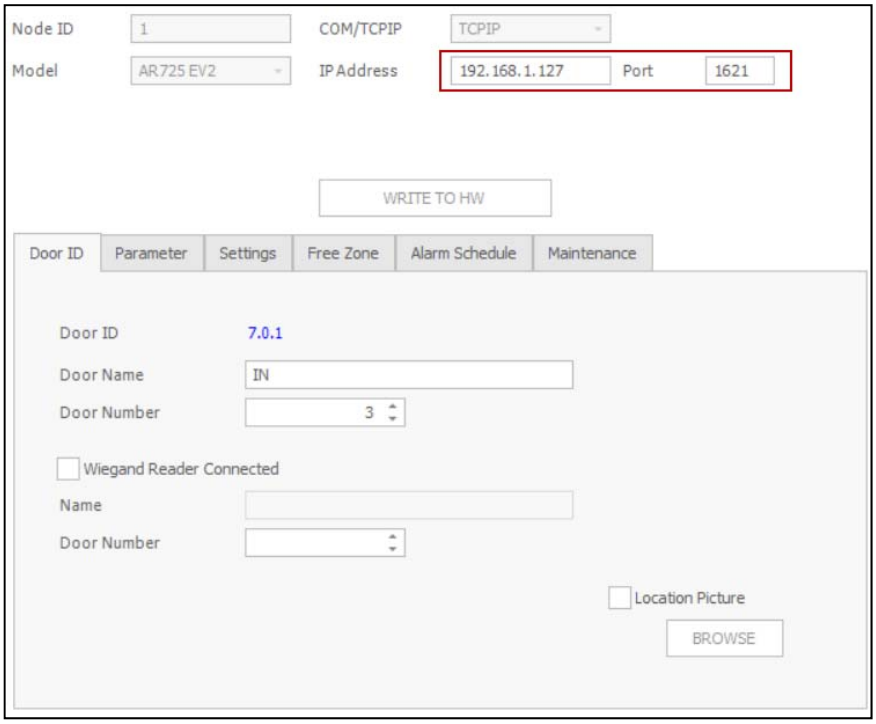


Fig 3.1.3e: ***Controller Management for setting and IP address***

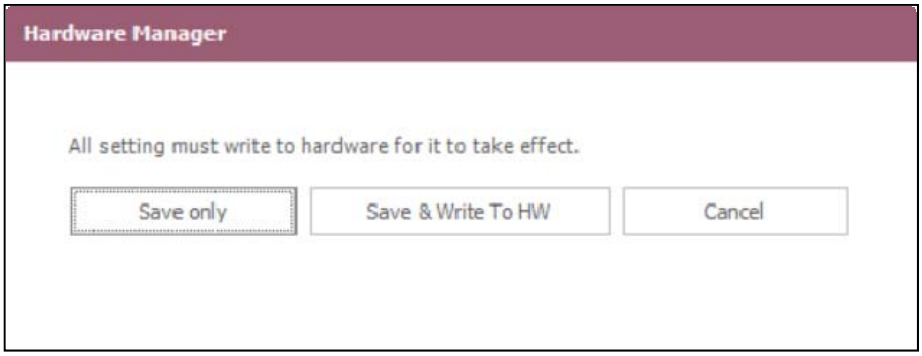


Fig 3.1.3f: ***Controller Management for setting and IP address***

Edit Controller TCP/IP (Standard/Pro Basic/Advance)

1) Right click on the controller under the controller list tab.
2) Click on the **Edit Controller** button. (*Refer fig 3.1.3d)*
3) Insert IP address and Port on the highlighted box*(Refer Fig 3.1.3e)*
4) Click **Save** button and notification will prompt. *Refer fig 3.1.3f)*
   a) Click on **Save only** button for update IP address.
   b) Click on **Save & Write to HW** button for update the controller setting and IP address
   c) Click on **Cancel** button to return controller management.

Remove Site

1) Select a site.
2) Click on the **Remove Site** button.
3) Click on **Save** button to update the changes or cancel to ignore the changes.

3.1.2 Controller Manager

Adding Hardware

1) Select the Site name that you want to add hardware and then click on **Add** button
2) Ignore the Node id input, if you want it to be assigning automatically or else key in the node id. It will prompt if any duplicate node id found.
3) Choose the Hardware model that you want to add.
4) Choose the COM port or TCPIP for the device. If you choose the TCPIP, then make sure that you key in the IP address and the Port number. *(Refer 3.1.4a)*
5) Configure the settings as per the need for the related hardware (The controller settings will be explained below).
6) Click **Save** button and able to write it to the hardware.

Editing Hardware

1) Select the Site name and the targeted hardware that you want to edit. Click on **Edit** button.
2) Click **Save** button after the edit done or **Cancel** to ignore the changes.

Delete Hardware

1) Select the Site name and the targeted hardware that you want to delete. Click on the **Delete** button.
2) Click **Save** button to update the changes or **Cancel** to ignore the changes.

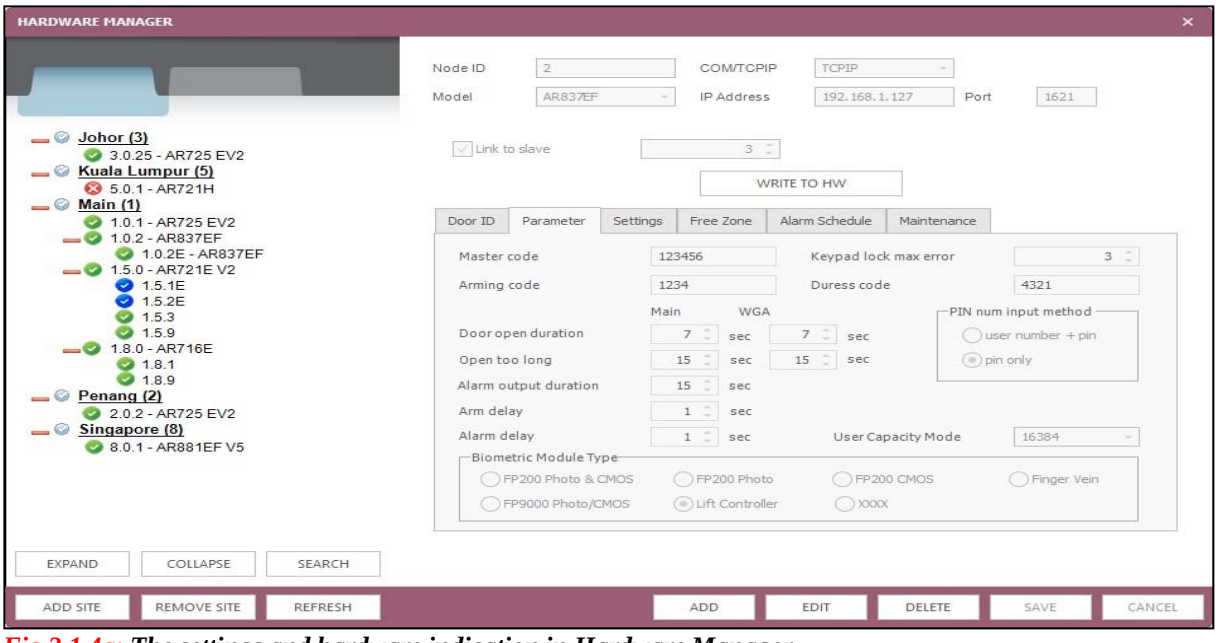


***Fig 3.1.4a:* The settings and hardware indication in Hardware Manager.**

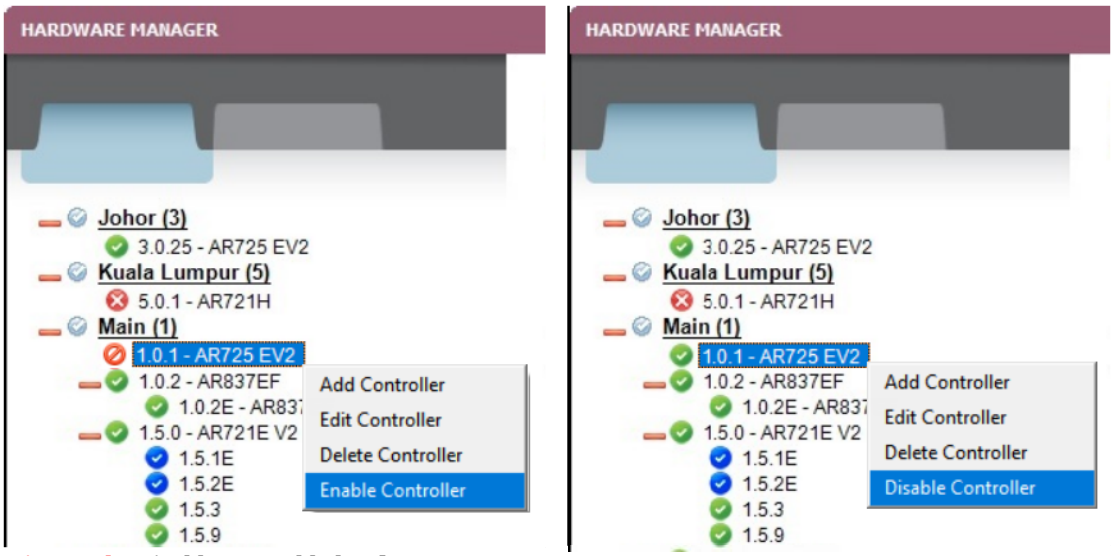


Fig 3.1.4b: ***Disable & Enable hardware.***

Disable Hardware

1) Select the hardware/reader under the controller list tab.
2) Then right-click and select **Disable** to disable the hardware/reader. *(Refer Fig 3.1.4b)*

Enable Hardware

1) Select the hardware/reader under the controller list tab.
2) Then right-click and select **Enable** to enable the hardware/reader. *(Refer Fig 3.1.4b)*

There are many types of controllers currently supported by ME-ACS:

Type 1) AR721H, AR727H, AR331HT, AR331HS, AR725H & AR721E
Type 2) AR716E
Type 3) AR837EF
Type 4) AR725E v2
Type 7) AR721E v2

Parameter setting is different for each time of controller. Following is detailed explanation for each type of controller setting.

Type 1: AR721H / AR727H / AR331HT / AR331HS / AR725H / AR721E

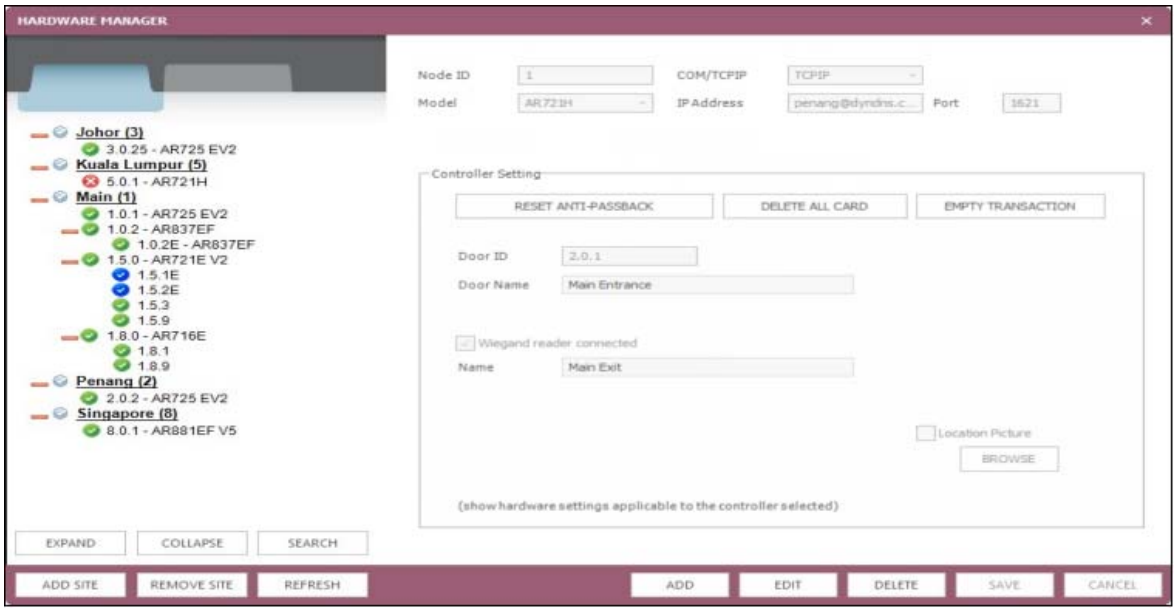


Fig 3.1.5: ***AR721H / AR727H / AR331HT / AR331HS / AR725H / AR721E.***

Controller Settings Group Box

Field	Description
Door ID	Door ID is derived from controller and reader node ID. Door ID is used to uniquely address each door in the system.
Door Name	Insert the door name.
Weigand Reader Connected	Tick the check box if any Weigand Reader Connected.
Name	Insert the name for Weigand reader.
Location Picture	Tick and browse the picture that you want to add. This picture will pop out during alarm event to show the location of alarm event. Any contact information can be added into the picture composition.

Type 2: AR716E

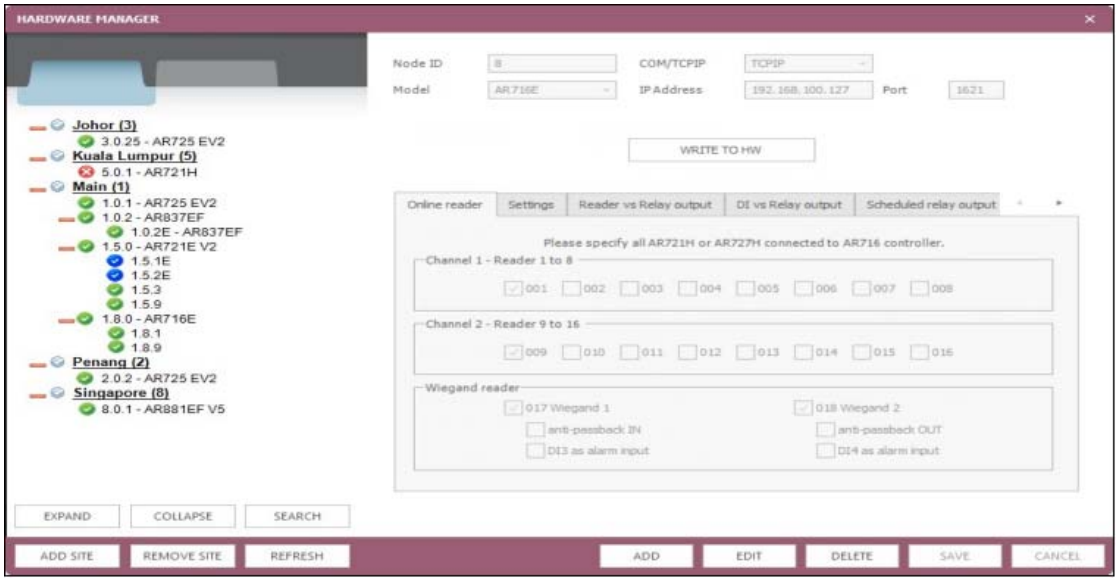


Fig 3.1.6: ***AR716E.***

Online Reader Tab (Refer 3.1.7)

Specify how many readers are connected to each bus. Basically, AR716E has two RS485 bus each supporting 8 readers per bus. AR716E also support two weigand port for auxiliary reader.

1. Reader 1-8 is the door number of the CH1 RS-485 readers.
(The CH1 can only connect to on-line reader Node ID 1-8).

2. Reader 9-16 is the door number of the CH2 RS-485 readers.
(The CH2 can only connect to on-line reader Node ID 9-16).

3. Node ID of WG reader port 1 is fixed to no.17 on the 716E.
If enable anti-pass-back, Node ID 17 is fixed to be in door.

4. Node ID of WG reader port 2 is fixed to no.18 on the 716E.
If enable anti-pass-back, Node ID 18 is fixed to be out door.

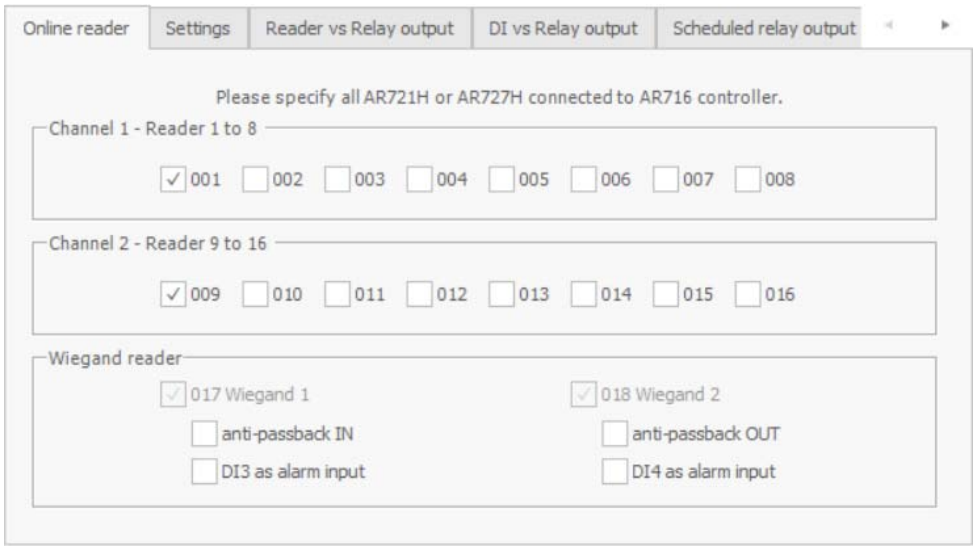


Fig 3.1.7: ***AR716E (Online reader).***

Settings Tab (Refer 3.1.8)

This tab allows you to configure setting for AR716E general operation.

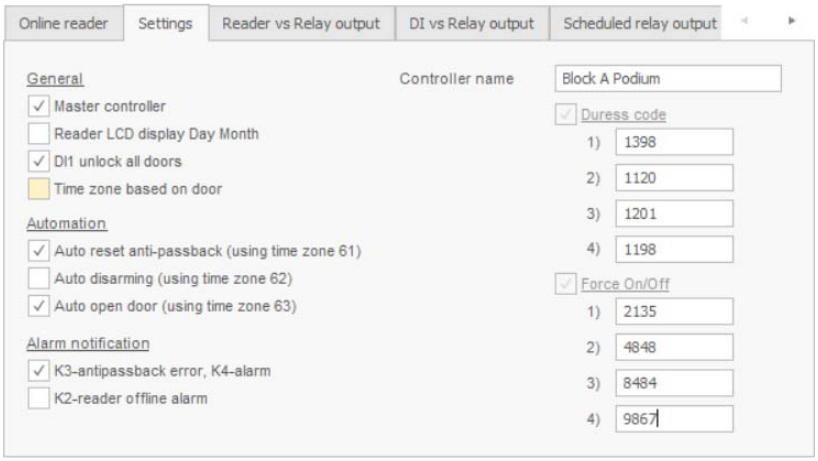


Fig 3.1.8: AR716E (Settings).

Controller name - insert the controller name.
Check/ Tick the appropriate settings for General, Automation and Alarm notification settings.
Check/ Tick and specify the duress code and force on/off functions.

****Note:**
User can assign up to 4 Force On/Off Codes for all the readers that connected to this controller. These codes can be used to on/off the relays on the controller After card access successfully, input 4 Force On/Off Codes, Relay Number, and F1 to activate (F2 to deactivate) a specified 716EV2/Ei Controller Relay.

User can assign up to 4 Duress Codes for all the readers that connected to this controller. Instead of user Card Code, input Duress Codes on reader panel for access, computer will instruct to open door, at the same time a message will be sent for help.

DI vs Relay Output Tab (Refer 3.1.9)

The controller has 4 DI inputs, it can be programmed to activate the K1 ~ K4 relays, EK1 to EK8 or readers Door Relays. Specify the DI input, activation relay online reader, onboard output and expanded relay output on AR716EIO for reader relay activation.

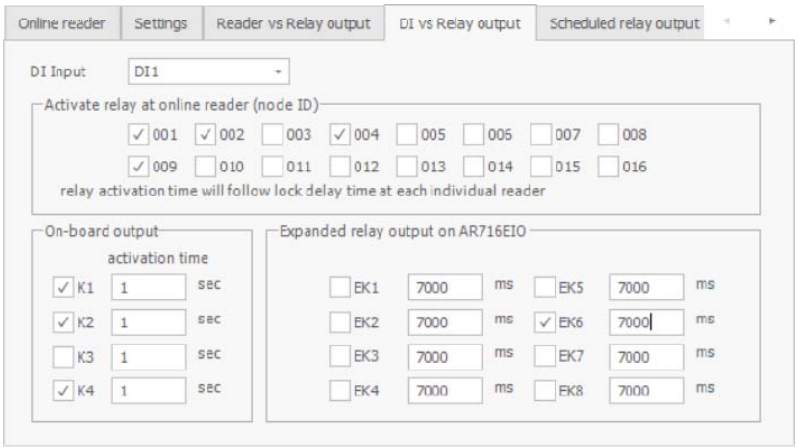


Fig 3.1.9: AR716E (DI vs Relay output).

If DI input set to the reader, once the DI input is activated, the reader Door Relays are activated following Door Relay setting on the reader itself.

If DI input set to Relays K1 ~ K4, once the DI input is activated, the Relays K1 ~ K4 are activated according to the duration time setting (001 ~255 seconds) of this menu.

If DI input set to EK1 ~ EK8 Relays, once the DI input is activated, the relays on the AR716EIO are activated according to the duration time setting (001 ~255 seconds).

If the time setting is 000, then the relay is in LATCH-ON/LATCH-OFF toggle mode, and the situation will be changed until DI input being activated next time.

Reader vs Relay Output Tab (Refer 3.1.10)

This function allows you to select which reader to trigger which internal relay on AR716E. Instead of using Reader Door Relay situated outside of the door, you can use Controller Relay to open the door (from inside). Opening the lock from inside avoid tampering and therefore increase the safety of the system. User can assign up to 12 relays on the AR716E controller to synchronize with the Door Relay of each reader. Once triggered, the AR716E relay will follow the lock time delay set inside the corresponding reader.

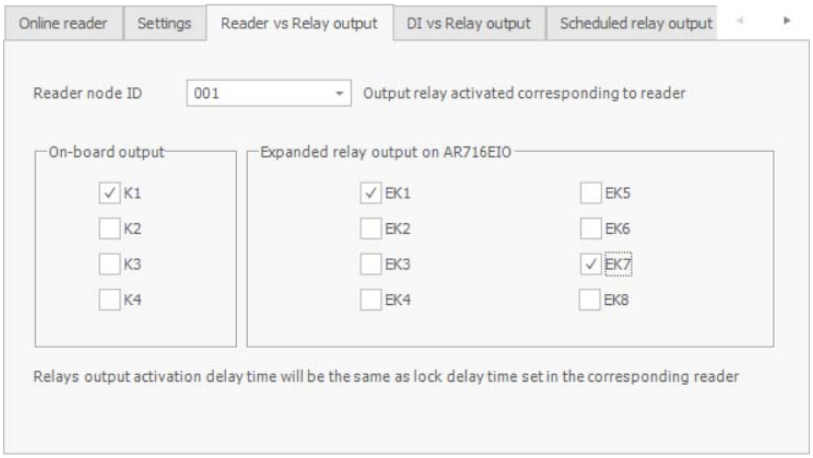


Fig 3.1.10: AR716E (Reader vs Relay output).

Select reader node ID and assign its corresponding relay K1 to K4 and EK1 to EK8.

Schedule Relay Output Tab (Refer 3.1.11)

This is an automation function in AR716E. K1 to K4 relay can be programmed to turn on at a specific time for a specific duration on a weekly schedule (Monday to Sunday).

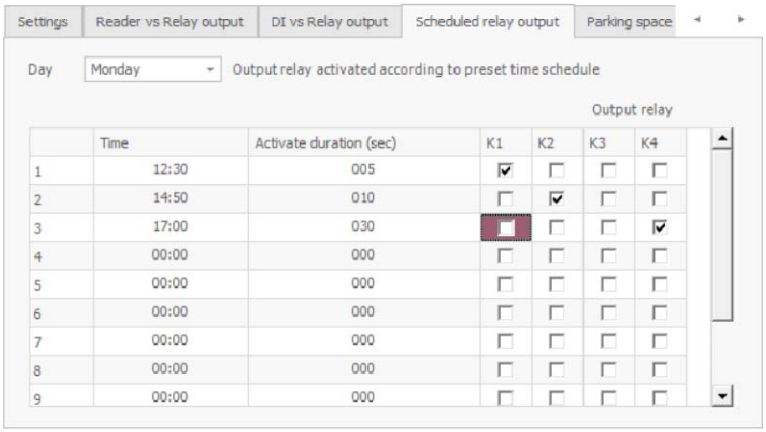


Fig 3.1.11: AR716E (Scheduled relay output).

Select "Weekday".
Specify what time to trigger the relay. There are 12 designated programmable times scheduled.
Activate duration specify how long (in sec) the relay shall hold upon trigger. 000 means no activated time. The activate duration ranges from 001 ~ 250 seconds.
Select which Relays K1 ~ K4 to trigger.

Parking Space Output Tab (Refer 3.1.12)

The controller provides parking spaces with All Full or All Empty notification. Assign any one of the 20 controller relays for its All Full or All Empty indication respectively. Before use, you need to enter initial total car spaces, total car inside parking lots. Anti-passback features must be activated for this function to provide accurate car IN / OUT count. In the event of car park full or empty, assigned relay will be triggered. You can connect any sounding or lightning device to the output relay for audio / visual notification.

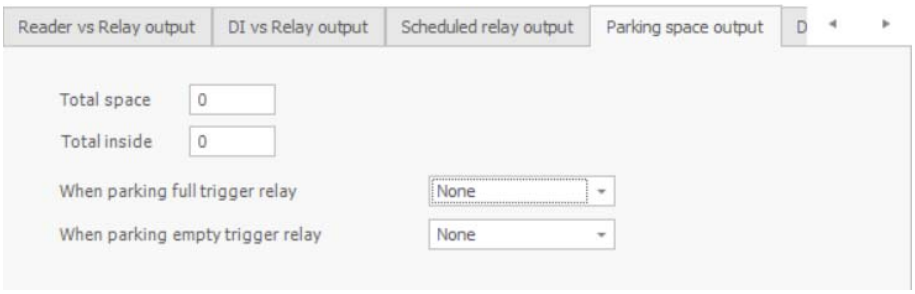


Fig 3.1.12: ***AR716E (Parking space output).***

Total Space - Specify the total parking space allocated or available.
Total Inside - Specify the total vehicle parked.
When parking full trigger relay - Specify which relay to be triggered when the parking space is full.
When parking empty trigger relay - Specify which relay to be triggered when the parking space is empty.

Door Number Tab (Refer 3.1.13.1)

The door number is integrated with door group function. The number can be assigned are between 3 to 255 without duplicated with each other. Door number = 0 is assigned for not door is assigned. By default, the door number is assigned automatically by system. For certain circumstance, the door number can be edit manually with condition not duplicated with existing door number. If the new number is duplicated with existing door number, the system will prompt for errors.

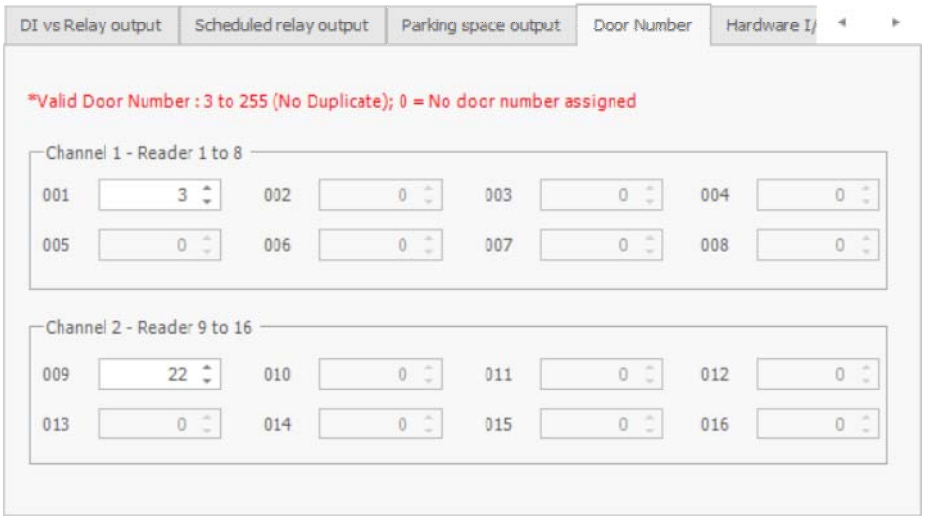


Fig 3.1.13.1: ***AR716E (Door Number).***

Hardware I/O Monitoring Tab (Refer 3.1.13.2)

This function is integrated with I/O Monitoring to control the digital input (DI). On board already got 4 digital input (DI) and can be expanded with another 8 extra digital input (DI).

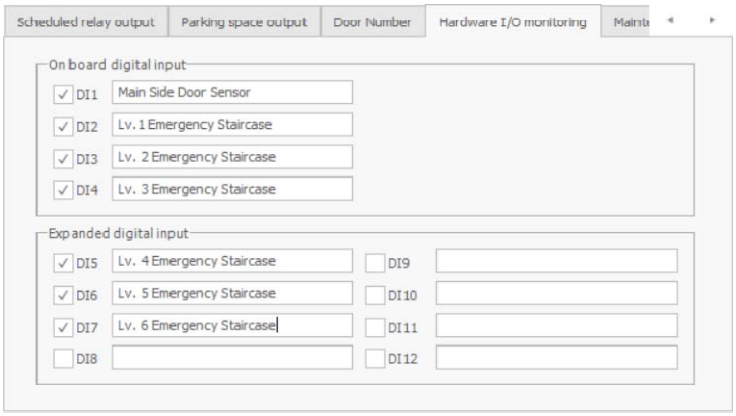


***Fig 3.1.13.2:* AR716E (Hardware I/O Monitoring).**

Type 3: AR881EF / AR837EF

Door ID Tab (Refer 3.1.24)

Specify the door id, door name, weigand connected and its details. Specify the JPG picture to be shown when alarm is triggered on this door.

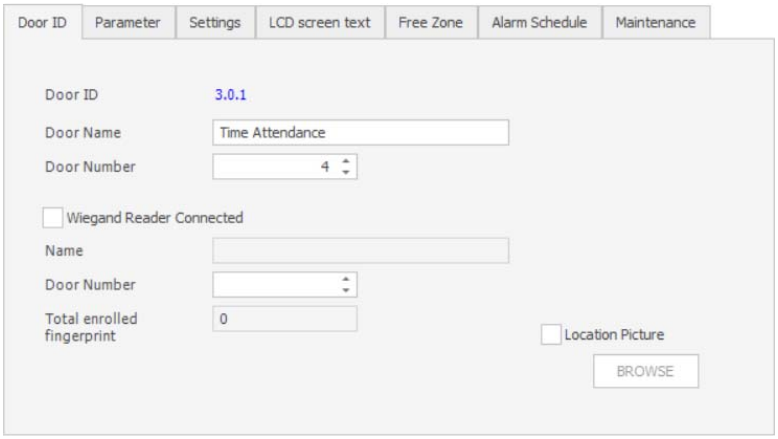


***Fig 3.1.24a:* AR837EF v5 (Door ID).**

For master/slave: (For fingerprint reader in series v5 only)

Specify the master and slave reader, activate the feature by enable the **Link to master** *(master reader node id).*

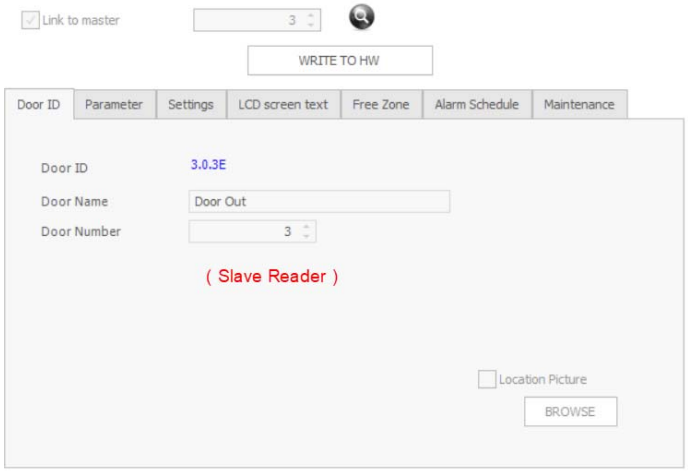


***Fig 3.1.24b:* Slave reader.**

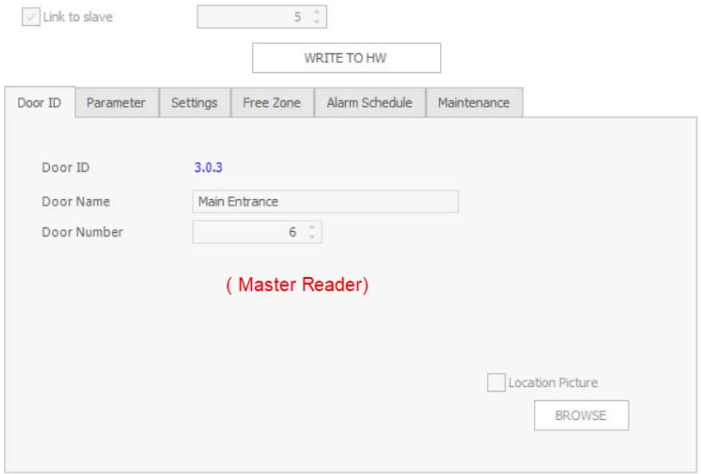


***Fig 3.1.24c:* Master reader.**

The master reader also can be searched by click on search icon *(highlight in red box)* to show the available fingerprint readers.

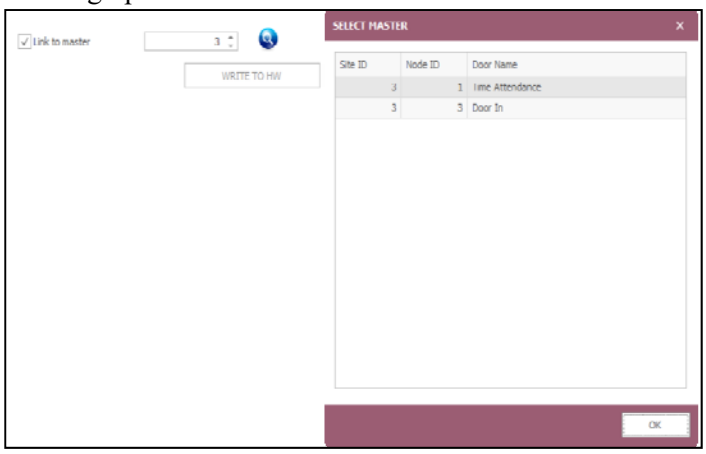


***Fig 3.1.24d:* Search for fingerprint readers.**

Parameter Tab (Refer 3.1.25)

Specify the new node ID, master code, arming code, door open duration, alarm output duration, wait delay, arm delay, alarm delay, key lock maximum error and duress code.
Choose the external reader format and pin number input method.

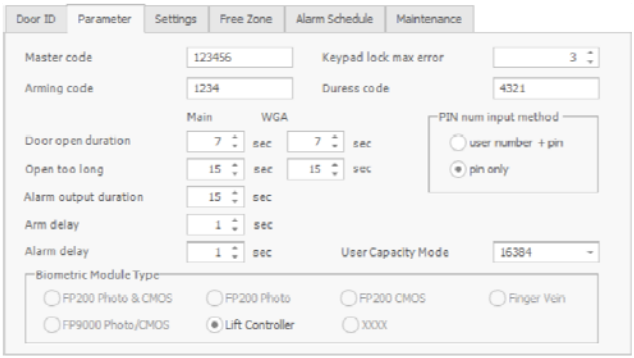


***Fig 3.1.25:* AR837EF v5 (Parameter).**

Settings Tab (Refer 3.1.26)

Specify the settings for the controller reader and wiegand reader.
The settings are Master Node, Enable Push button, Enable antipassback and Enable Auto Relock, Share Door Relay, Is Entry Door, Enable Free Zone, Free Zone Open Imm. and specify which controller reader or wiegand reader is connected.
And also set the other settings such as enable alarm, auto disarm, close stop alarm after door closed, activate alarm on expired user, enable open alarm output to door and specify beep sound overflow warning limitations.

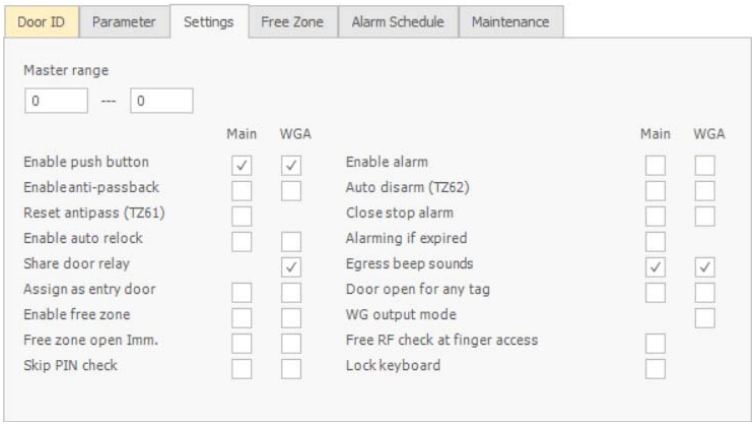


***Fig 3.1.26:* AR837EF v5 (Settings).**

LCD Screen Text Tab (Refer 3.1.27)

Options to display the date under DDMM format and to be in English menu.
Able to assign the idle message on the screen.

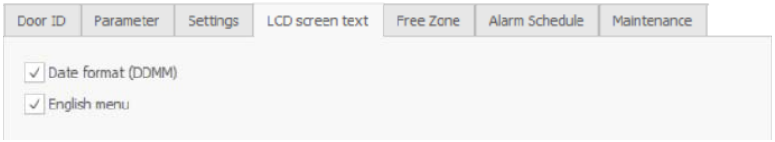


***Fig 3.1.27:* AR837EF v5 (LCD screen text).**

Free Zone Tab (Refer 3.1.28)

Choose/Specify the day, Begin/End time for auto open zone schedule.

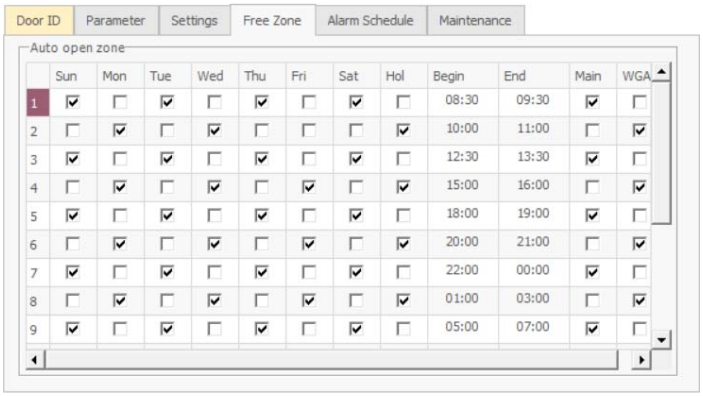


***Fig 3.1.28:* AR837EF v5 (Free Zone).**

Alarm Schedule Tab (Refer 3.1.29)

Choose/Specify the day, time, activation duration for the alarm trigger as per preset schedule.

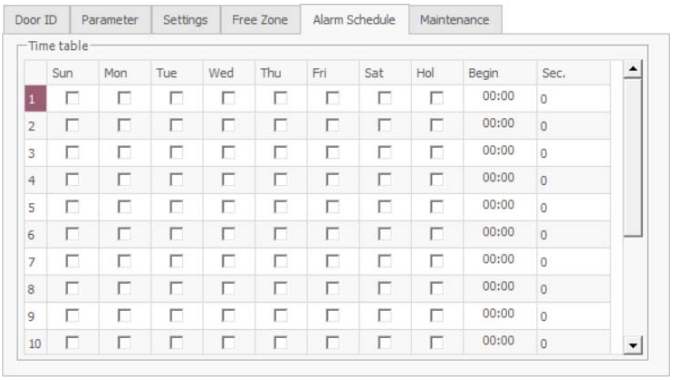


***Fig 3.1.29:* AR837EF v5 (Alarm Schedule).**

Maintenance (Refer 3.1.30)

This section provides the tools to clean the data inside the reader, there are DELETE ALL CARD, EMPTY TRANSACTION and DELETE ALL FP.

***Fig 3.1.30:* AR837EF v5 (Maintenance).**

Type 4: AR837E / AR725E v2

Door ID Tab (Refer 3.1.31)

Specify the door id, door name, weigand connected and its details. Specify the JPG picture to be shown when alarm is triggered on this door.

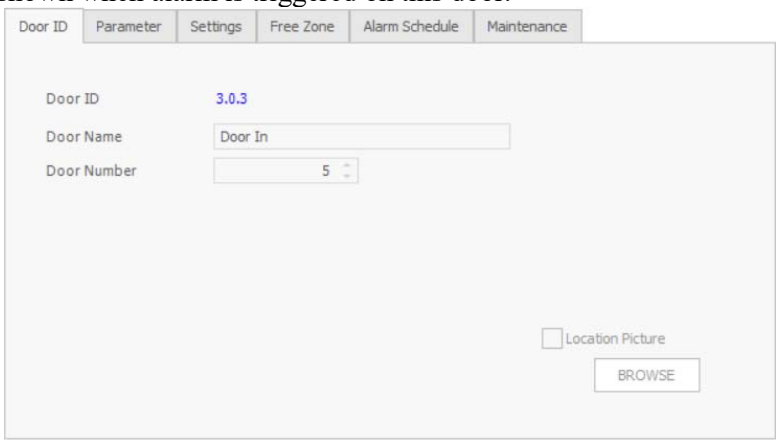


Fig 3.1.31: AR837E / AR725E v2 (Door ID).

Parameter Tab (Refer 3.1.32)

Specify the new node ID, master code, arming code, door open duration, alarm output duration, wait delay, arm delay, alarm delay, key lock maximum error and duress code.
Choose the external reader format and pin number input method.

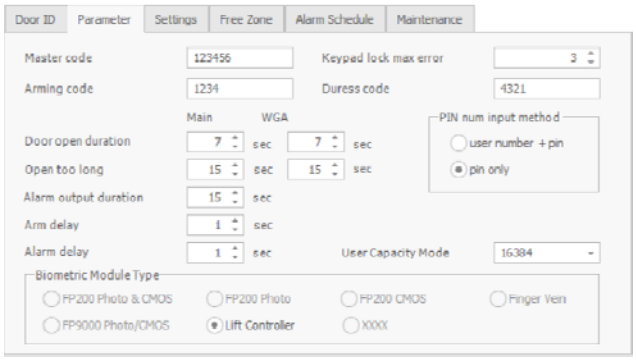


Fig 3.1.32: AR837E / AR725E v2 (Parameter).

Settings Tab (Refer 3.1.33)

Specify the settings for the controller reader and wiegand reader.
The settings are Master Node, Enable Push button, Enable antipassback and Enable Auto Relock, Share Door Relay, Is Entry Door, Enable Free Zone, Free Zone Open Imm. and specify which controller reader or wiegand reader is connected.
And also set the other settings such as enable alarm, auto disarm, close stop alarm after door closed, activate alarm on expired user, enable open alarm output to door and specify beep sound overflow warning limitations.

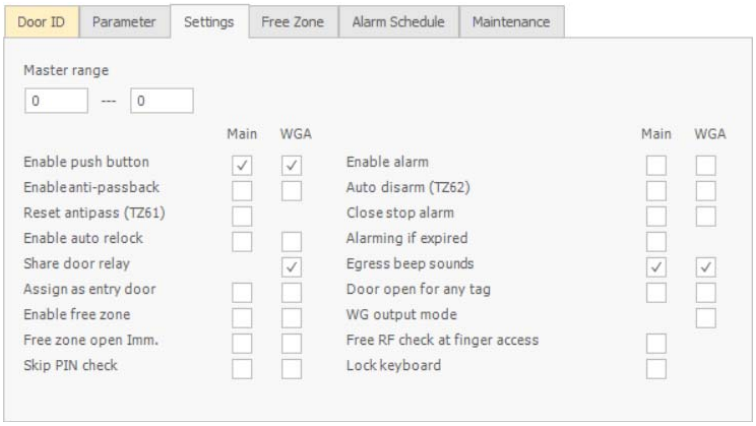


Fig 3.1.33: AR837E / AR725E v2 (Settings).

LCD Screen Text Tab (Refer 3.1.34)

Options to display the date under DDMM format and to be in English menu.
Able to assign the idle message on the screen.

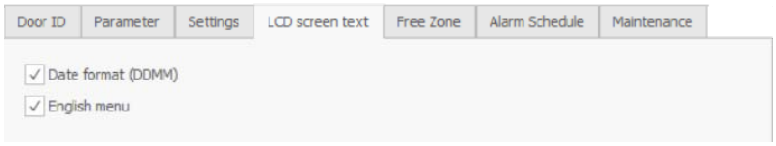


***Fig 3.1.34:* AR837E (LCD screen text).**

Free Zone Tab (Refer 3.1.35)

Choose/Specify the day, Begin/End time for auto open zone schedule.

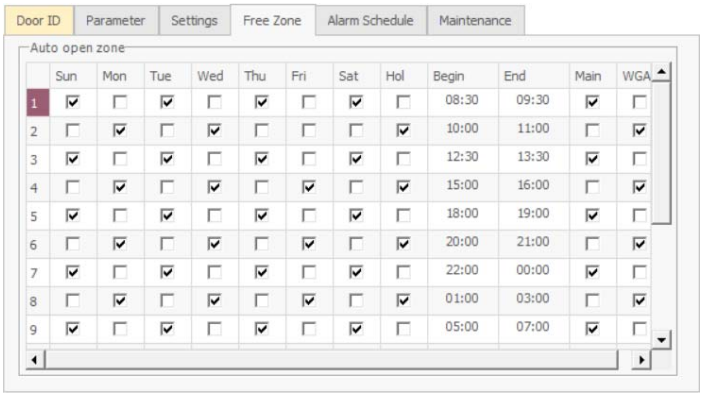


***Fig 3.1.35:* AR837E / AR725E v2 (Free Zone).**

Alarm Schedule Tab (Refer 3.1.36)

Choose/Specify the day, time, activation duration for the alarm trigger as per preset schedule.

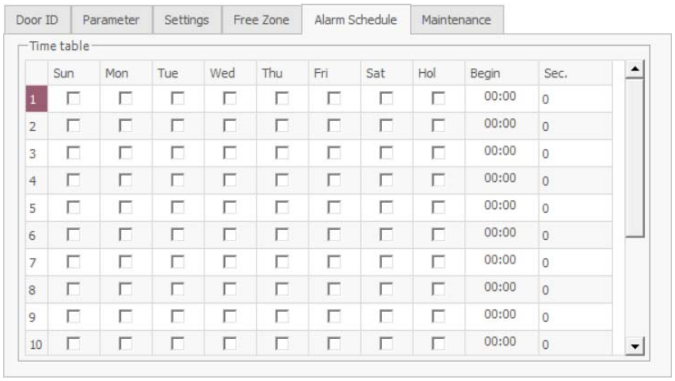


***Fig 3.1.36:* AR837E / AR725E v2 (Alarm Schedule).**

Maintenance (Refer 3.1.37)

This section provides the tools to clean the data inside the reader, there are DELETE ALL CARD and EMPTY TRANSACTION.

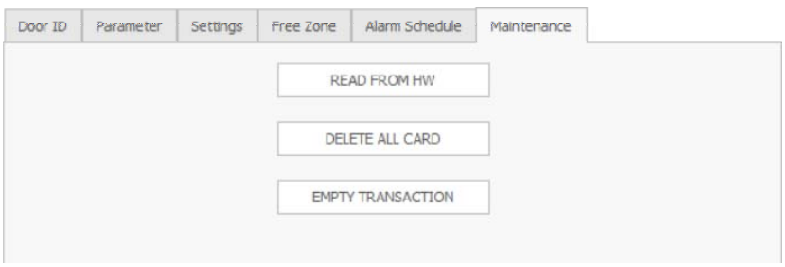


***Fig 3.1.37:* AR837EF v5 / AR725E v2 (Maintenance).**

Type 5: AR721E v2

Door ID Tab (Refer 3.1.38)

Specify the door id, door name, weigand connected and its details. Specify the JPG picture to be shown when alarm is triggered on this door.

Fig 3.1.38: AR721E v2 (Door ID).

Online Reader Tab (Refer 3.1.39)

Specify how many readers are connected to each bus. Basically, AR721E v2 has two RS485 bus and two weigand port for auxiliary reader.

1. Reader 3-8 is the door number of the CH1 RS-485 readers.
(The CH1 can only connect to on-line reader Node ID 3-8).

2. Reader 9-16 is the door number of the CH2 RS-485 readers.
(The CH2 can only connect to on-line reader Node ID 9-16).

3. Node ID of WG 1 is fixed to node id 01 and WG 2 is fixed to node id 02.

4. Reader with node id is 3 or 9 only able communicated with build-in relay K1~K3.

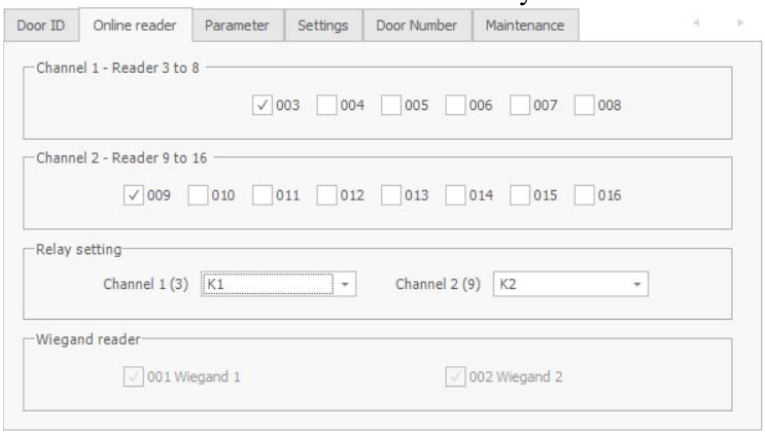


Fig 3.1.39: AR721E v2 (Online reader).

Parameter Tab (Refer 3.1.40)

Specify the new node ID, master code, arming code, door open duration, alarm output duration, wait delay, arm delay, alarm delay, key lock maximum error and duress code.
Choose the external reader format and pin number input method.

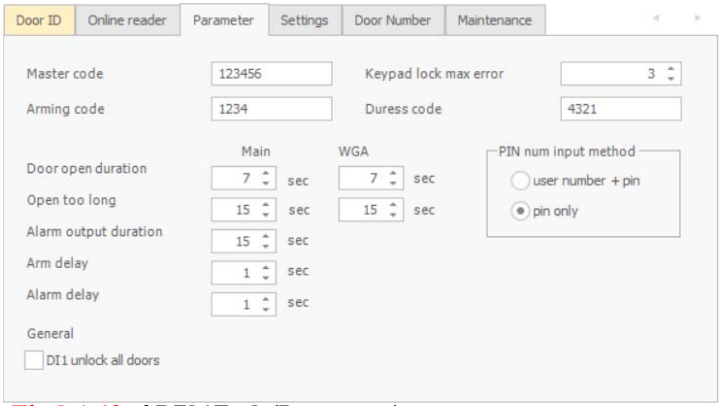


Fig 3.1.40: AR721E v2 (Parameter).

Settings Tab (Refer 3.1.41)

Specify the settings for the controller reader and wiegand reader.
The settings are Master Node, Enable Push button, Enable antipassback and Enable Auto Relock, Share Door Relay, Is Entry Door, Enable Free Zone, Free Zone Open Imm. and specify which controller reader or wiegand reader is connected.
And also set the other settings such as enable alarm, auto disarm, close stop alarm after door closed, activate alarm on expired user, enable open alarm output to door and specify beep sound overflow warning limitations.

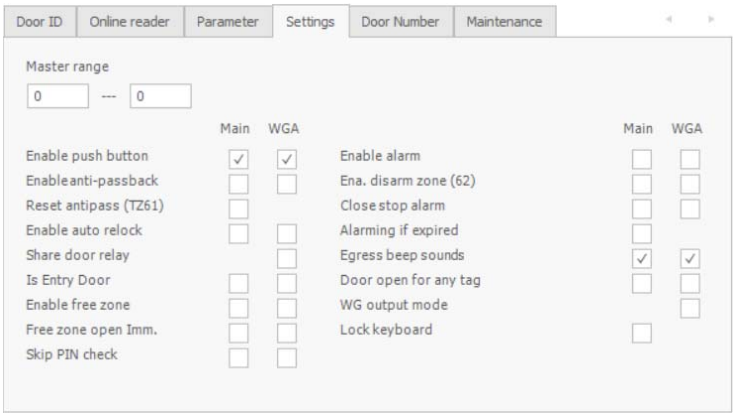


Fig 3.1.41: AR721E v2 (Settings).

Door Number Tab (Refer 3.1.42)

The door number is integrated with door group function. The number can be assigned are between 3 to 255 without duplicated with each other. Door number = 0 is assigned for not door is assigned. By default, the door number is assigned automatically by system. For certain circumstance, the door number can be edit manually with condition not duplicated with existing door number. If the new number is duplicated with existing door number, the system will prompt for errors.

Fig 3.1.42: AR721E v2 (Door Number).

Maintenance (Refer 3.1.43)

This section provides the tools to clean the data inside the reader, there are DELETE ALL CARD and
EMPTY TRANSACTION.

Fig 3.1.43: AR721E v2 (Maintenance).

3.2 Preferences

Provides options for the operator to change the appearance or actions in SACS system or in the hardware.

Setup Company Name

Enter the Company name1, Company name2, Address, Telephone number, Fax number and email address.
Click on the **SAVE** button to save the details or **CANCEL** button to ignore the changes.

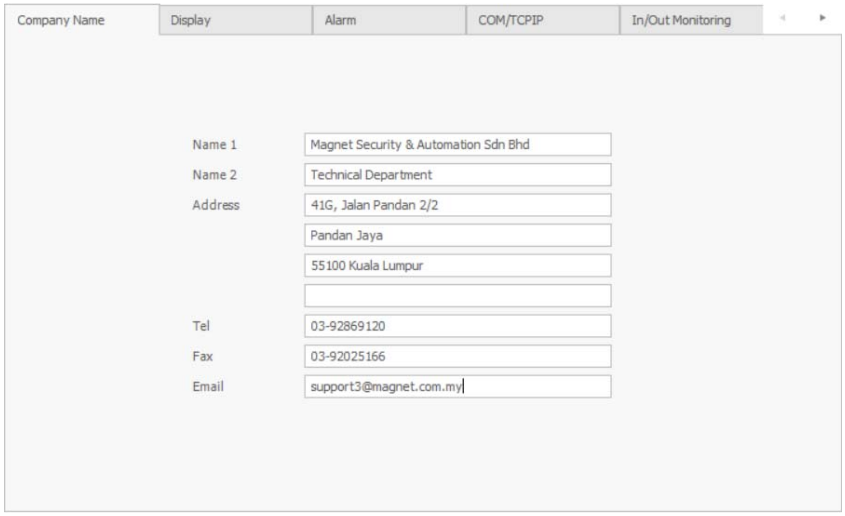


Fig 3.2.1: ***The company information.***

Setup Display

Select the time display 24 hours or AM/PM time display from the radio box.
Select the date format options from the dropdown box.
View the sample display and date format from the sample group box below.
Enable/disable “Show ABA card format in user profile” to activate this feature.
Click on the SAVE button to save the details or CANCEL button to ignore the details.

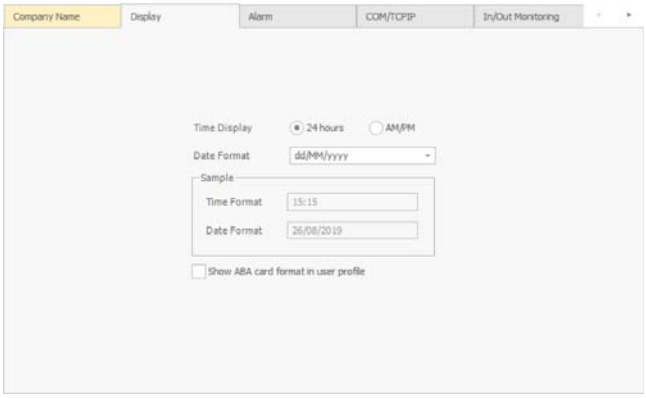


Fig 3.2.2: ***The time and date display format.***

Setup Alarm

Insert the SMTP server name, port, account name and password from the SMTP group box. This allows alarm notification to be emailed out.
Click the first checkbox to enable email sending when alarm notification.
Click the second checkbox to enable pop up JPG file of door location. The JPG file for each door is specified in Hardware Manager.
Click the third checkbox to enable alarm continuously until all alarm events have been acknowledged.
Click the fourth checkbox to enable alarm sound with a defined period of time (sec) for each alarm event.
Click the firth checkbox to enable send email upon alarm trigger and specified maximum of 5 email addresses.
Click on the **SAVE** button to save the details or **CANCEL** button to ignore the details.

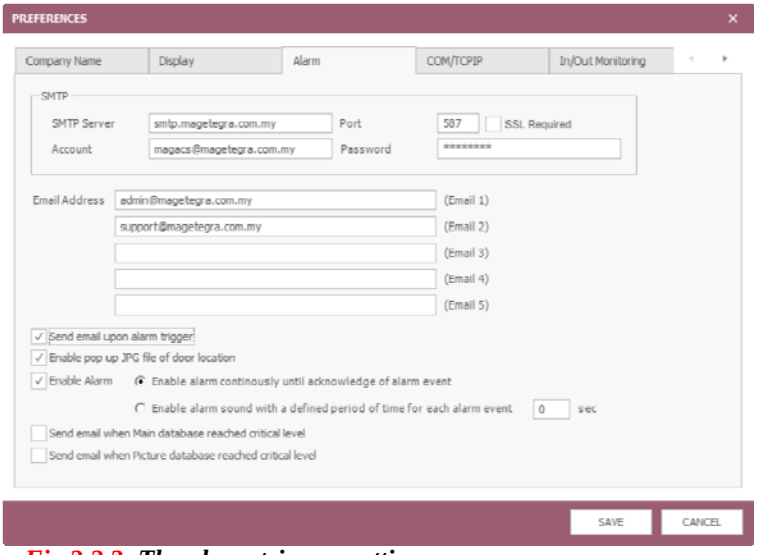


Fig 3.2.3: ***The alarm triggers settings.***

Setup COM/TCPIP

Polling speed means what is the time interval to wait before new command is sent out. Time out means how long the software should wait before the reader reply. COM port and TCPIP port can be programmed to have different polling speed and different timed out to suits the network bandwidth.
Enter the TCPIP timeout and polling speed in the TCPIP group box. Enter the polling speed for Current Event Log, In/Out Monitoring, Single Profile Monitoring and Triple Profile Monitoring.
Enter the COM timeout and polling speed in the COM group box.
Enter the TCPIP timeout and polling speed in the TCPIP group box.
Click on the **SAVE** button to save the details or **CANCEL** to ignore the details.

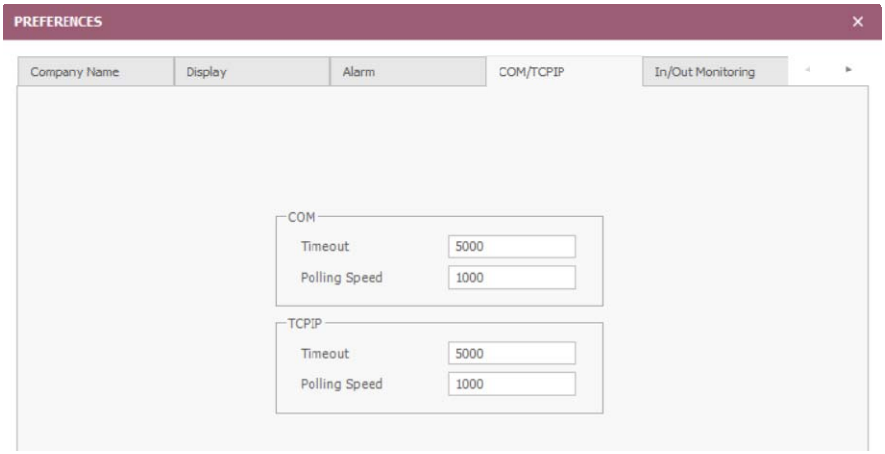


Fig 3.2.5: ***The polling speed for COM or TCPIP settings.***

Setup In/Out Monitoring

Specify which doors to be included for In/Out monitoring function.
Choose the Door that will be assigned for in/out monitoring by selecting it from the dropdown menu
Click on the **SAVE** button to save the details or **CANCEL** button to ignore the details

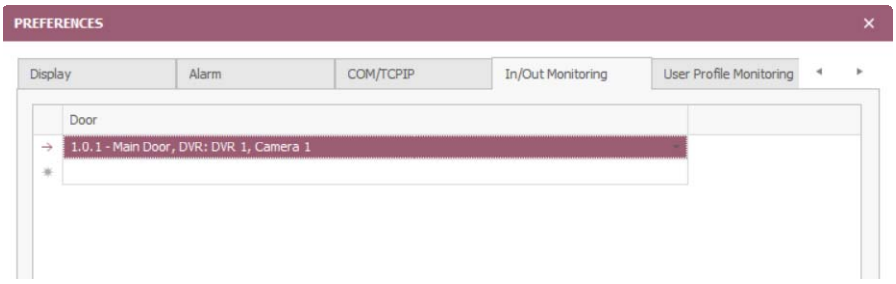


Fig 3.2.6: ***The In / Out controllers or readers monitoring.***

Setup User Profile Monitoring

Specify which doors to be included for User Profile Monitoring function. Make sure the selected door(s) is not duplicated.
Choose the Door that will be assign for User Profile Monitoring by selecting it from the dropdown menu.
Click on the **SAVE** button to save the details or **CANCEL** button to ignore the details.

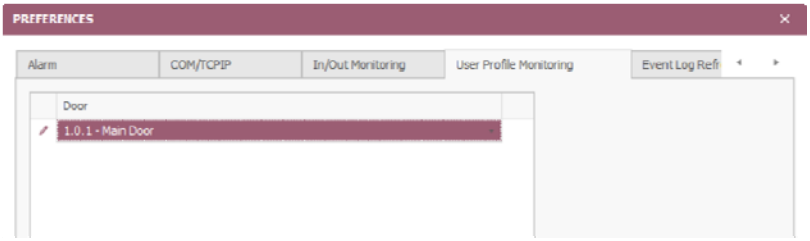


*Fig 3.2.7: **The User Profile Monitoring.***

Event Log Refresh

Event log refresh will be used to identify the speed of current event Log, in/out monitoring, single profile monitoring and triple profile monitoring during event log update and to set maximum rows of event are displayed.
Enter the time (in milliseconds) for current event Log, in/out monitoring, single profile monitoring and triple profile monitoring.
Enter the maximum rows will be displayed.
Click on the **SAVE** button to save the details or **CANCEL** button to ignore the details.

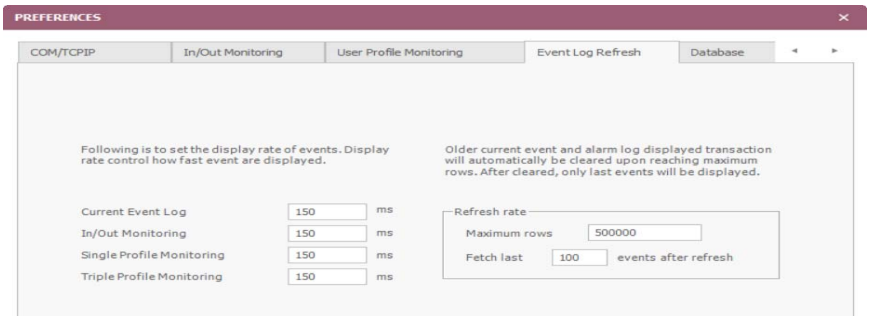


*Fig 3.2.8: **The Event Log Refresh setting.***

Database

Database will be used to identify the notification of database capacity. The alert will prompt when the size of database is reach critical condition (default is 90%). The real condition about database capacity status can be checked under database management *(Housekeeping →Database management → Purge).* The picture(s) can be store in another database by enable *Store picture in separate database.*

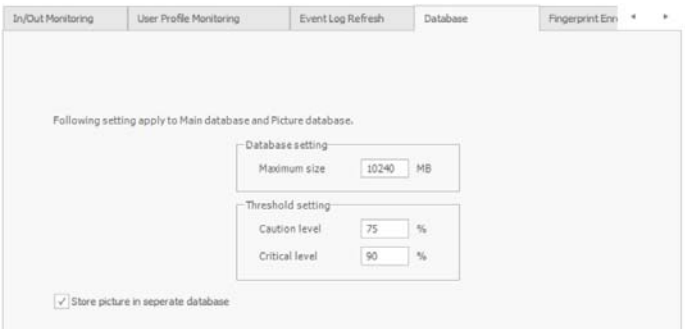


*Fig 3.2.9: **The Database setting.***

Fingerprint Enroll

Fingerprint Enroll used to setting automatically which reader that could capture thump print through software. That function will help user that install with a few reader we advice to setting at preferences as a default reader for enroll fingerprint. After user already set default reader, they no need to select during during enroll fingerprint.

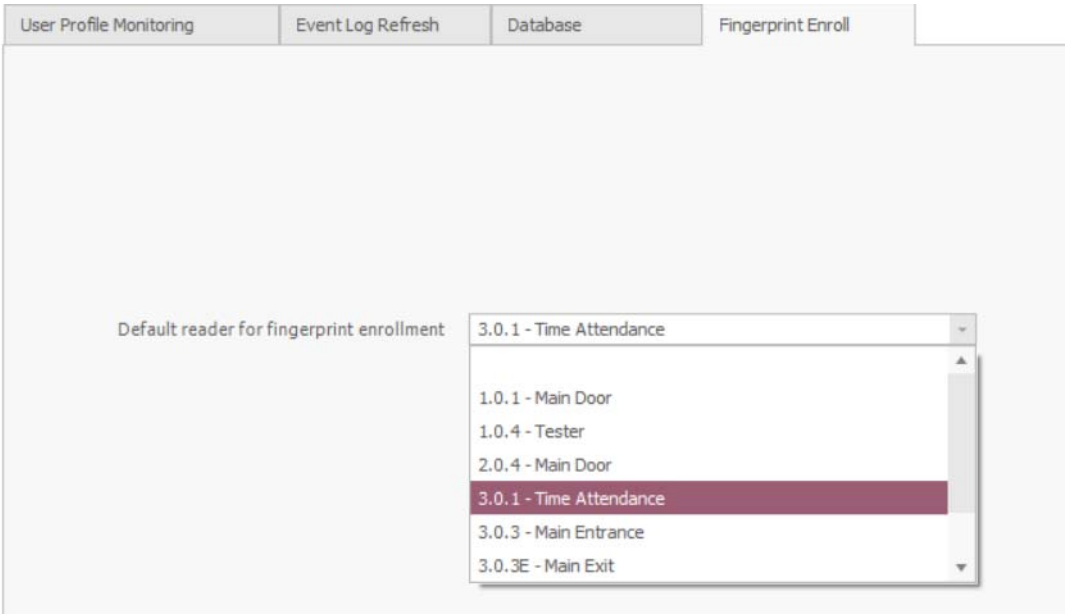
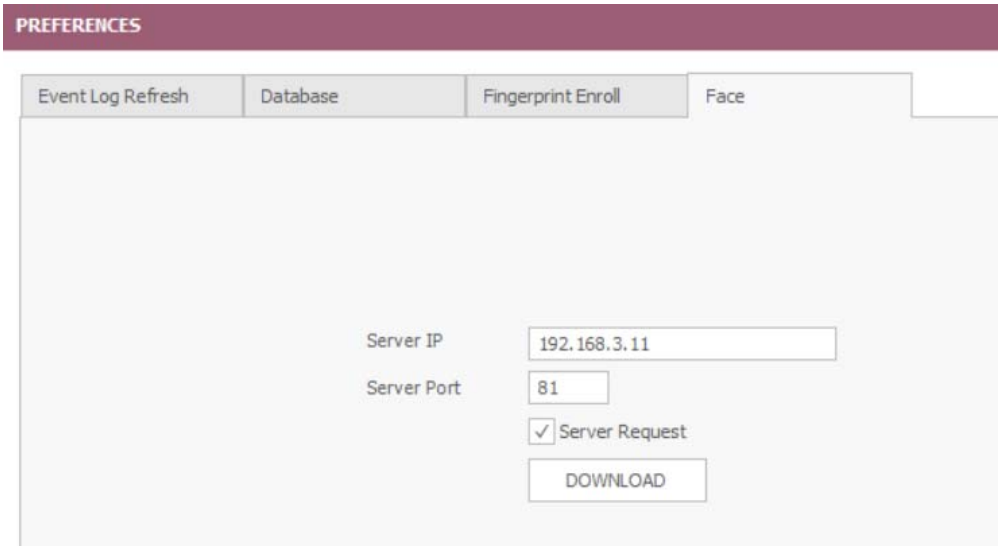


Fig 3.2.10: ***Fingerprint Enroll setting***

Face server

Face server used to setting the server IP address for the Face Recognition where the device will post the event to software. This function is to help user that can update the server IP address to single or multiple Face Recognition when there is a IP changes on the Server or Computer.



3.3 CCTV

This function allows you set up the DVR/IP-cam and assign camera to door for picture capture function. There are 3 model of IP-cam that can be supported by ME-ACS software. The following model are CM55002, CM45002 and CM44006

3.3.1 DVR / IP Cam Setting

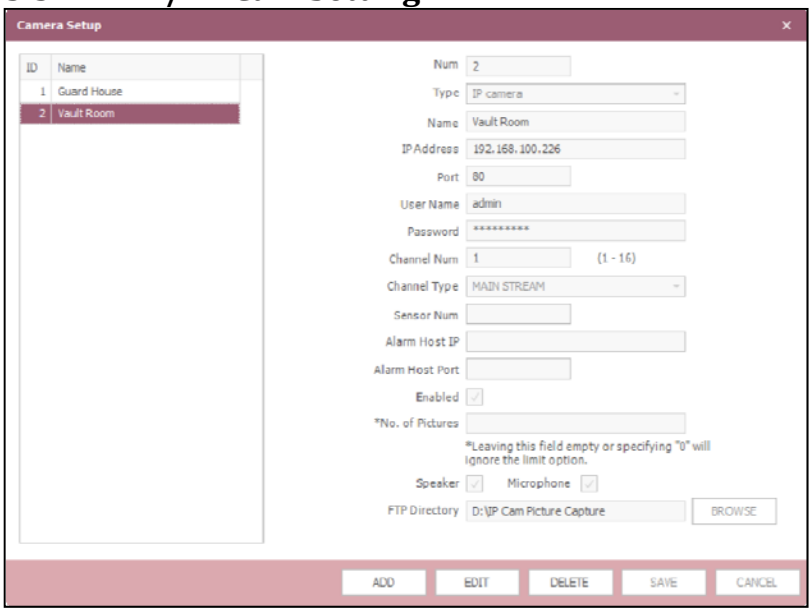


Fig 3.3.1: The DVR / IP Cam settings.

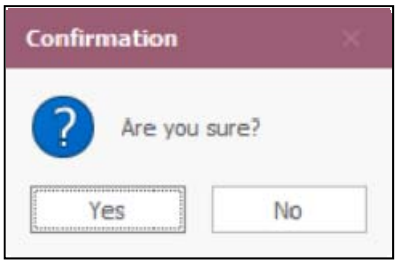


Fig 3.3.2: Confirmation.

Adding DVR/ IP Cam

1) Click on the **ADD** button.
2) The column do not need to be assigned because it is automated..
3) Select the Type column, choose between AVR or IP camera
4) Enter the name, IP address, port, user name, password and channel num.
5) Select the channel type (Main Stream or Sub Stream).
   -Main Stream (High Quality, High Bandwidth Speed Usage)
   -Sub Stream (Low Quality, Low Bandwidth Speed Usage)
7) Tick the **Enable** to enable picture capture function.
8) Fill in the No. Of Picture column for picture limitation. Excseeding this limitation, older pictures will be replaced.
9) Tick the Speaker and/or Microphone if in use. *(For IP Cam only)*
10) Click on **Browse** for FTP Directory *(For IP Cam only)*
10) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 3.3.2)*

Editing DVR / IP Cam

1) Select the DVR/IP Cam that you want to edit from the left panel list by clicking on it.
2) Once Selected, click on the **Edit** button.
3) After editing the necessary fields, click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 3.3.2)*

Delete DVR / IP Cam

1) Select the DVR/IP Cam that you want to delete from the left panel list by clicking on it.
2) Once Selected, click on the **Delete** button.
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 3.3.2)*

Cancel DVR / IP Cam

1) Click on the **Cancel** button to reject any entries while Adding or Editing before.

3.2.2 Camera Location Setting

This function allow operator to assign each camera (or sensor) to its corresponding door.

For MVR type:

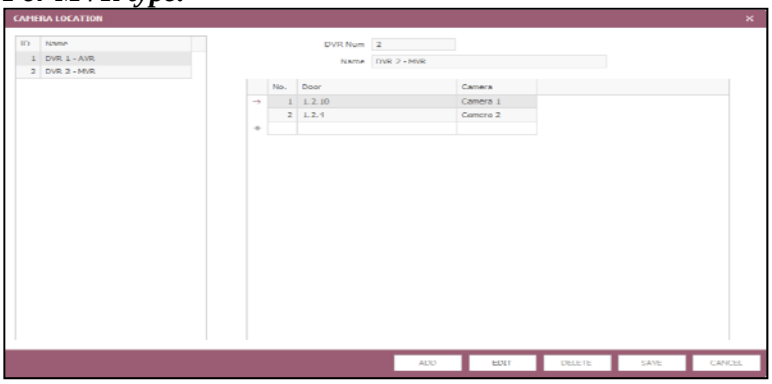


***Fig 3.3.3a:* The MVR door and camera matching selection.**

For AVR type:

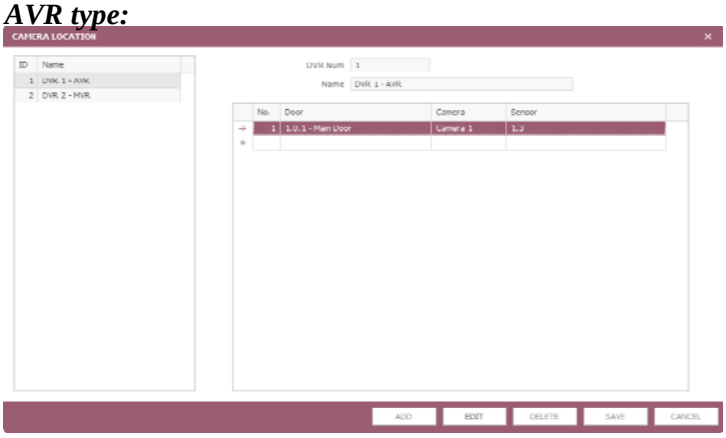


***Fig 3.3.3b:* The AVR door and camera matching selection.** *(For version 4.91 and above)*

Editing DVR Camera Location

1) Select the DVR that you want to edit from the left panel list by clicking on it.
2) Once Selected, click on the **Edit** button.
3) After editing the necessary fields, click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 3.3.3)*

Delete DVR Camera Location

1) Select the DVR that you want to delete from the left panel list by clicking on it.
2) Once Selected, click on the **Delete** button.
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 3.3.3)*

Cancel DVR / IP Cam Camera Location

1) Click on the **Cancel** button to reject any entries while Adding or Editing before.

***Attention:**

*(Before access the DVR / IP Cam by the PC through the internet explorer, **please set the DVR /IP Cam on the IP Address, Port, Gateway and HTTP Port**. Then, only continue the settings below and it is **compulsory** to make the connection between the ME-ACS and DVR / IP Cam image capture function under access control system).*

For IP Camera configuration type:

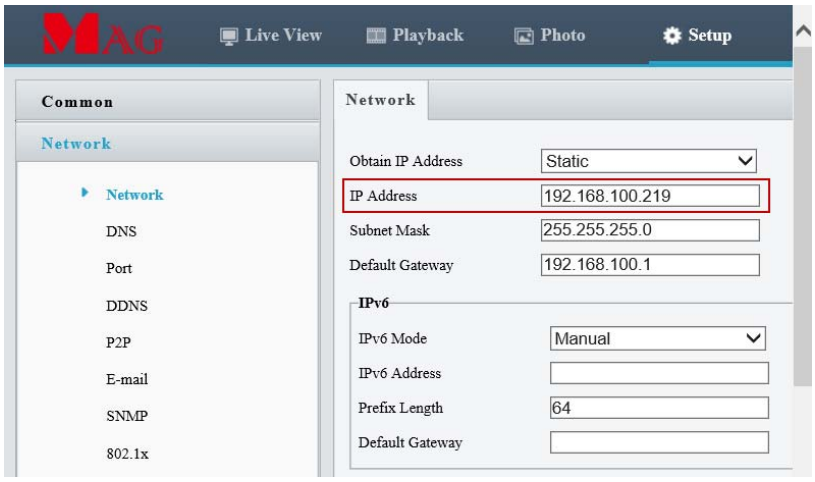


***Fig 3.3.4:** The basic network configuration information of IP Camera.*

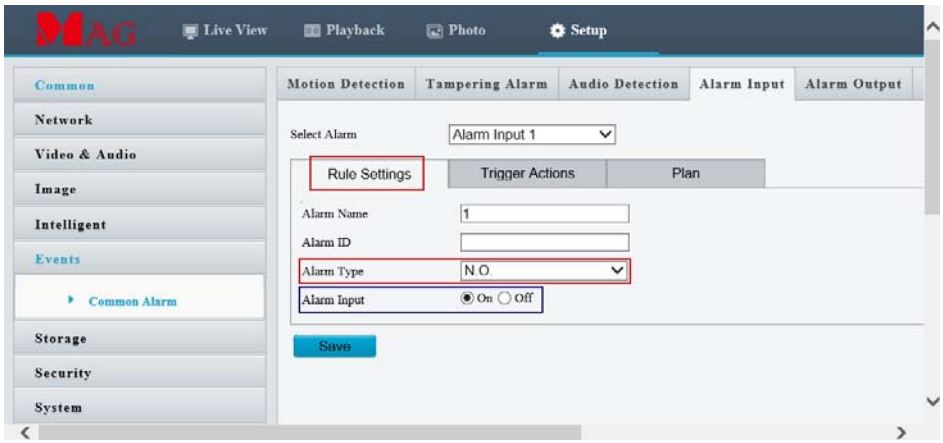


***Fig 3.3.5:** The IP Cam alarm input Rules setting.*

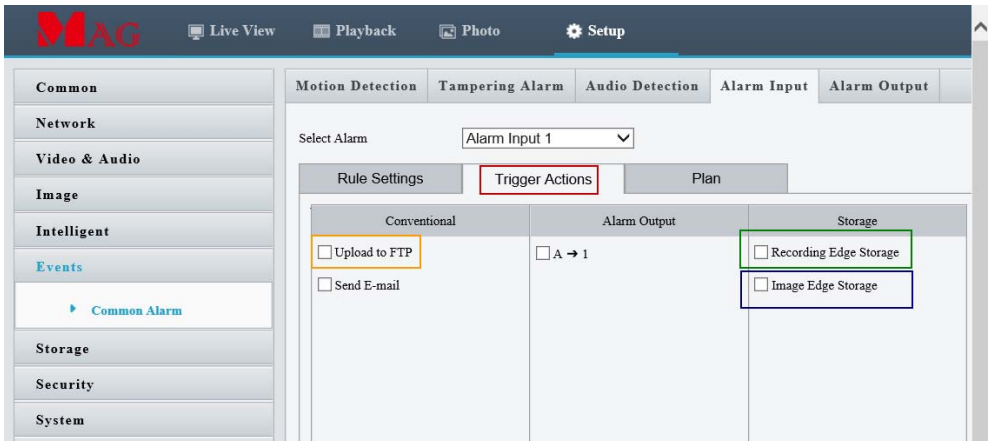


***Fig 3.3.6:** The IP Cam alarm input Rules setting.*

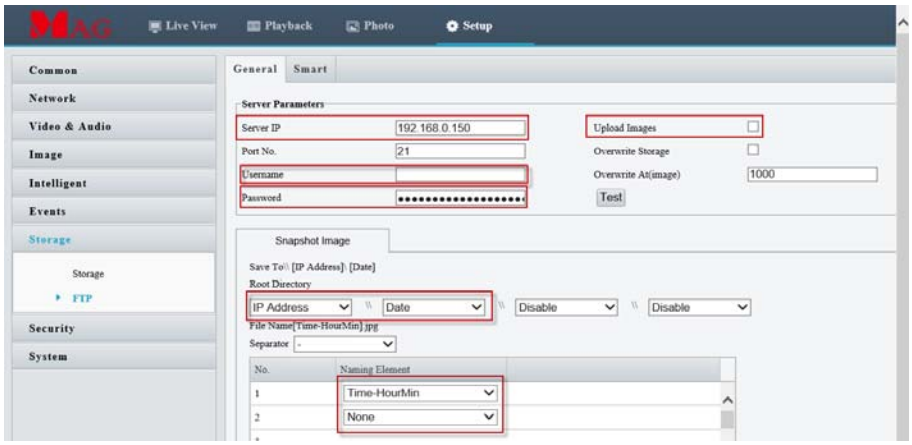


Fig 3.3.7: The IP Cam FTP configuration..

a) Go to ***Network*** tab, click on ***Network*** and change the IP Address. *(refer Fig 3.3.4)*
b) Go to ***Events tab***, click on ***Common Alarm***. Go to **Alarm Input** tab to change **Alarm type** and **Alarm Input**.*(refer Fig 3.3.5)*
c) Go to ***Trigger Actions*** Tab and tick the ***Upload to FTP, Recording Edge Storage*** and ***Image Edge*** Storage*(refer Fig 3.3.6)*
d) Go to Storage, click FTP and enter the ***Server IP, local PC username and Passwords, tick Upload Images,*** s***elect the directories and file names format*** and click Save.*(refer Fig 3.3.7)*

For AVR type:

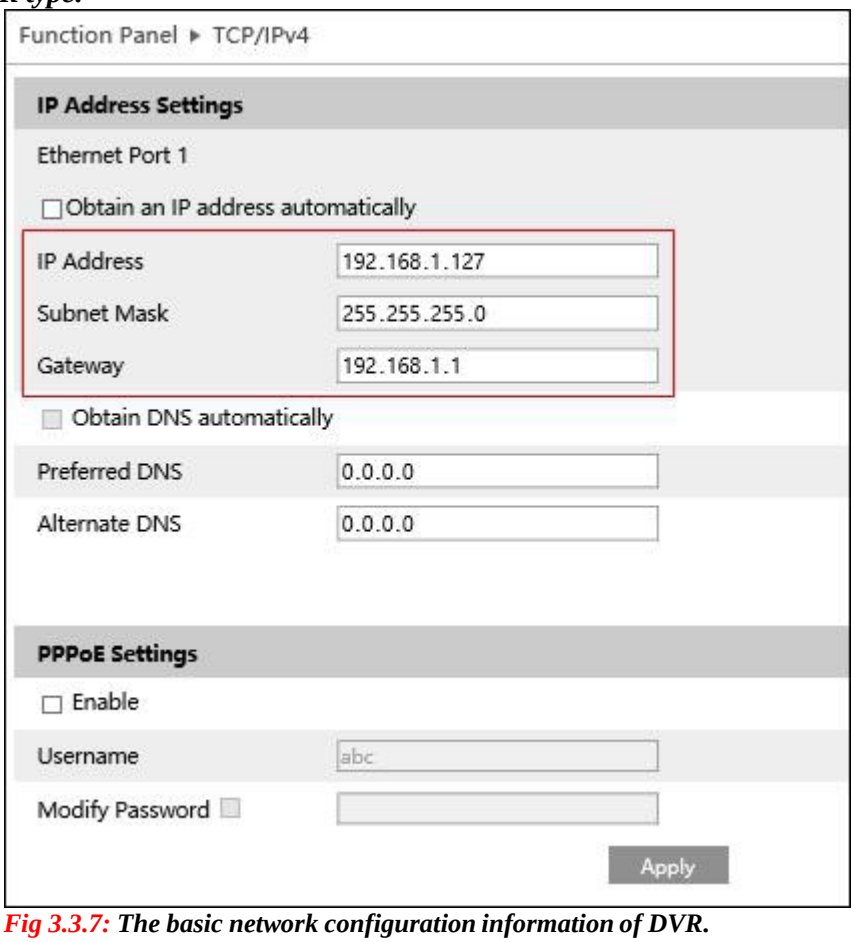


Fig 3.3.7: The basic network configuration information of DVR.

a) Select Function Panel → Network, change the network correctly.
b) Select Function Panel → Alarm → Sensor Alarm, on enable and tick for sensor, snapshot and alarm out.

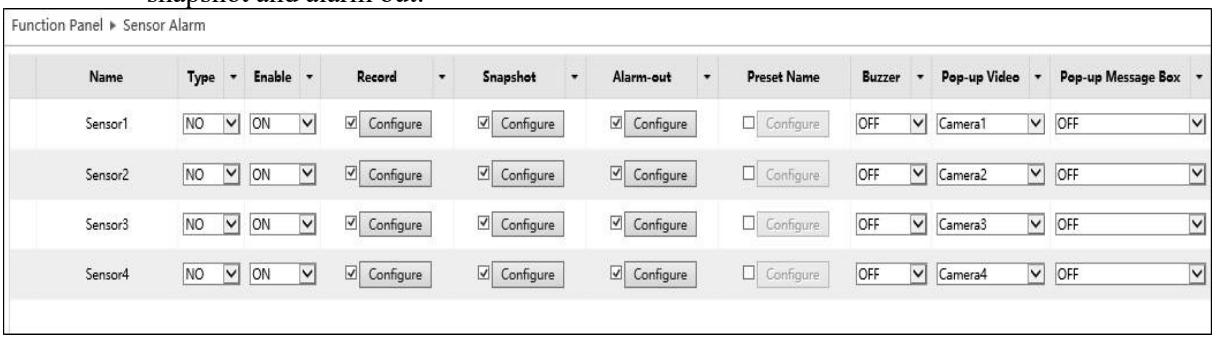


***Fig 3.3.8:* The DVR alarm input schedule setting.**

c) Click on **Apply** button to apply all the changes of DVR.

3.4 Anti-Passback Map

This function list out the user's current in and out anti-passback status inside the controller. This function is only available for AR829E, AR837EF and AR716E.

By filtering the user, the entire door allowed to access for this user will be listed out along with its anti-pass back status. It will indicate whether user is currently outside or still inside the building.

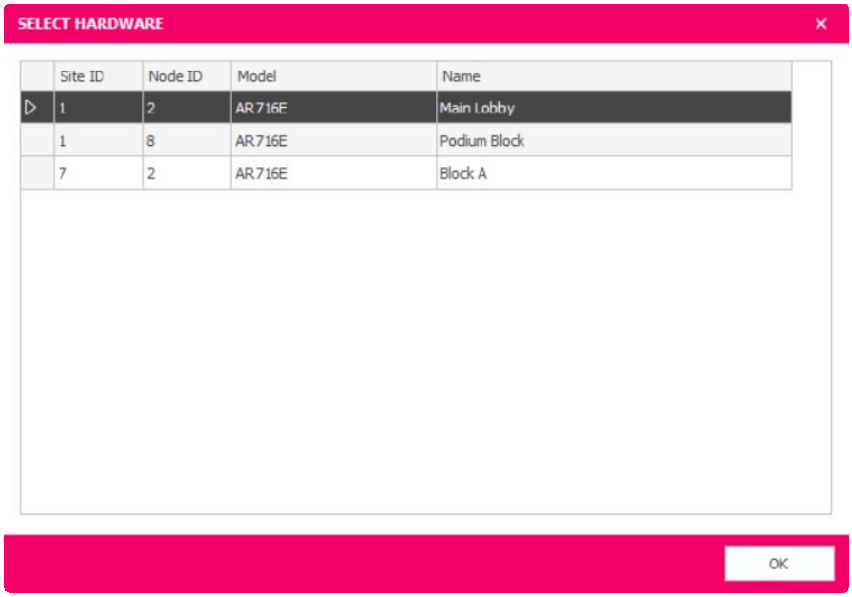


***Fig 3.4.1:* The selection hardware or controller for anti-passback function.**

3.5 Control Panel

Control Panel is simplified interactive menu access in graphical and in functionality order flow. Software routine task from settings to monitoring has been summarized into an intuitive logical flow. This greatly reduces learning time and help to have ME-ACS up and running with minimal effort. New operator can follow this flow chart and easily learn ME-ACS with minima guidance from fellow operator. This ensures continuity of SACS as operator resigned and new operator joined the organization.

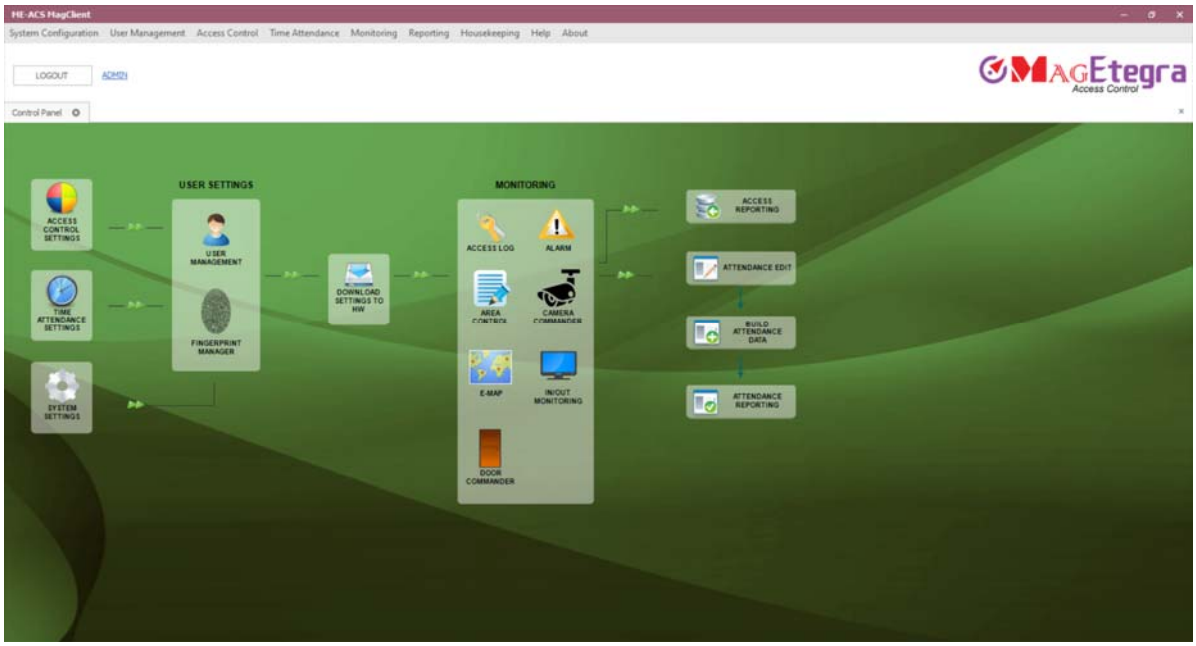


***Fig 3.5.1:* The overall processes of system can be checked through the system Control Panel.**

Easy to navigate the system according to the flow that appear on the control panel. The corresponding function menu will pop up after clicking on icons in control panel.

3.6 Download

All the settings saved in the ME-ACS will not be activated if they are not downloaded into hardware controller(s). Any new users, deletion of users, changes of time zone must be downloaded into hardware via Download function for the new changes to take effect. Download function transfers settings from ME-ACS to hardware controller(s). You can easily select which settings (left side) to be downloaded to which controller (right side).

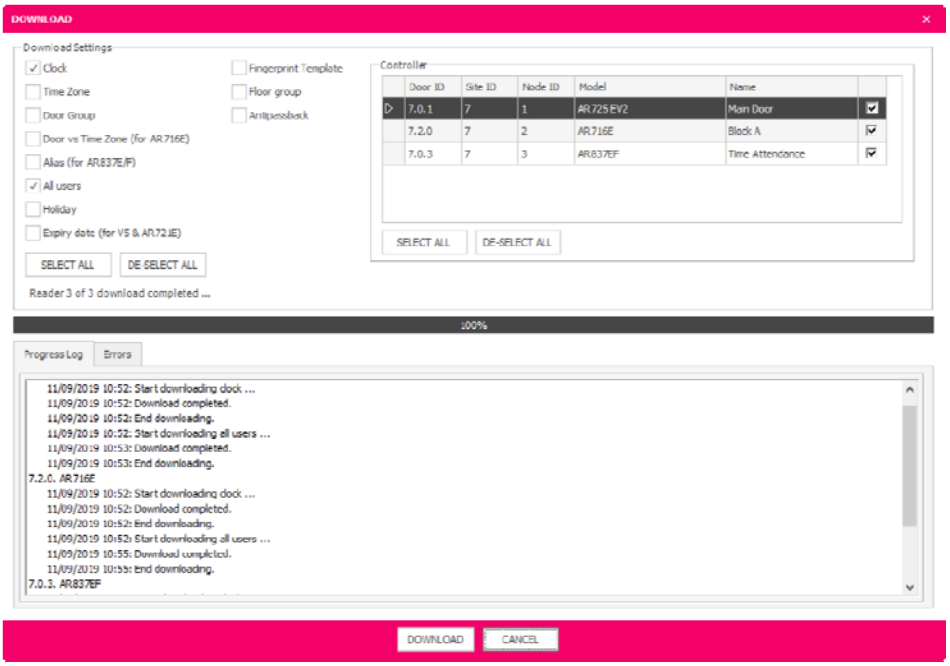


***Fig 3.6.1:* The process of download updating information to the controllers.**

ME-ACS only support specific version of SOYAL controller. If ME-ACS detect incompatible or non-genuine SOYAL controller, Download menu will prompt error notification. If this happens, please contact your re-seller to confirm hardware version. Connect back genuine / correct hardware version will resume download function.

3.7 Operator Management

Multiple operators from anywhere in the network can manage hardware, setting, monitoring and reporting of multiple remote sites (branches) in any location. Each operator can be assigned login with limited function access. All operation performed by operator in entire network is recorded in audit trail for review. This powerful networking architecture allows multiple security personnel to work together easily and keep a closer eye on organization's security protection while maintaining scalability to easily add more hardware or operator in coming future.

Operator Management is used to manage the ME-ACS operators login account functionality. Each operator is allowed to have their own color skin and background pictures for more personalized look and feel. Sample background picture is included in installer CD under Driver & Tools / background picture. Function Access authority is assigned to limit the functions allowed for each operator. Operator login to Server PC from any Client PC will also follow the login ID, password and function authority as assigned in Server PC's Operator Management.

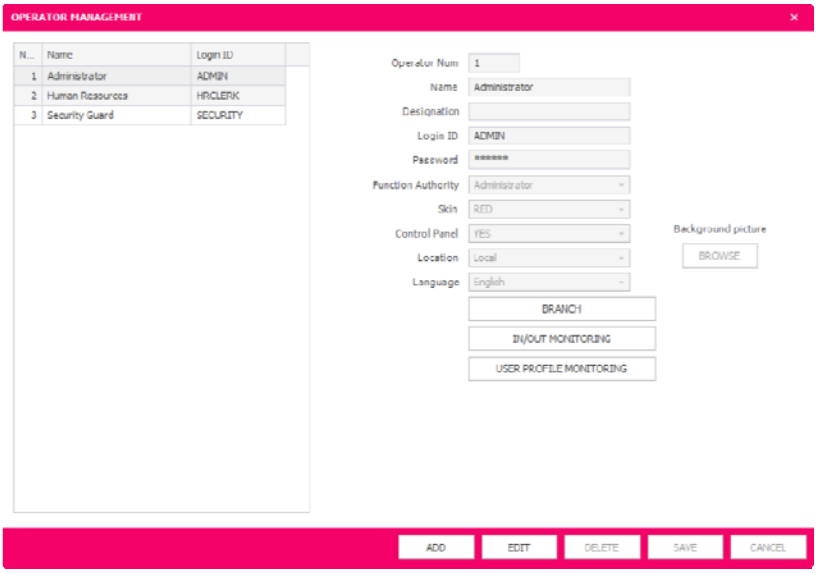


Fig 3.7.1: ***Operator Management.***

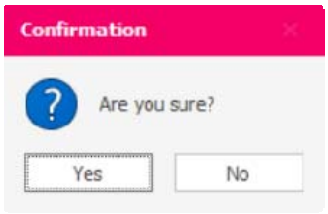


Fig 3.7.2: ***Confirmation.***

Adding Operator

1) Click on the **ADD** button.
2) The operator numbers no need to be assign since it is automated.
3) Enter the name, designation, login id, password of the branch.
4) Select the function authority, skin, control panel, branch and language from the dropdown menu.
5) Click on the **BROWSE** button and browse for preferred control panel background image.
6) Click on the **Save** button and it will prompt for confirmation.
7) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer 3.7.2)*

Editing Operator

1) Select the operator number that you want to edit from the left panel list by clicking on it.
2) Once selected, click on **Edit** button.
3) After editing the necessary fields, click on **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer 3.7.2)*

Deleting Operator

1) Select the operator number that you want to delete from the left panel list by clicking on it.
2) Once selected, click on the **Delete** button.
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer 3.7.2)*

Cancel Operator Management

1) Click on the **Cancel** button to reject any entries while Adding or Editing before

3.8 Function Access Authority

SACS is a multi-function multi-user application that can be simultaneous used by operator of different role – HR Administrator, Security Guard, Building Manager, Security Supervisor, IT Manager and etc. It is important to define proper privilege rights of each operator to perform their job with minimum interference to other operators. Defined Function Authority is assigned to an operator to limit its access to function is SACS. This allows proper control of what each operator can do to ensure integrity of entire system. For example, security guard might be limited view IN/OUT monitoring function only. HR clerk might be limited to only use time attendance function and not allowed to use hardware manager. IT manager might not be allowed to access time attendance function. Security Manager might be allowed to only use alarm monitoring and reporting function.

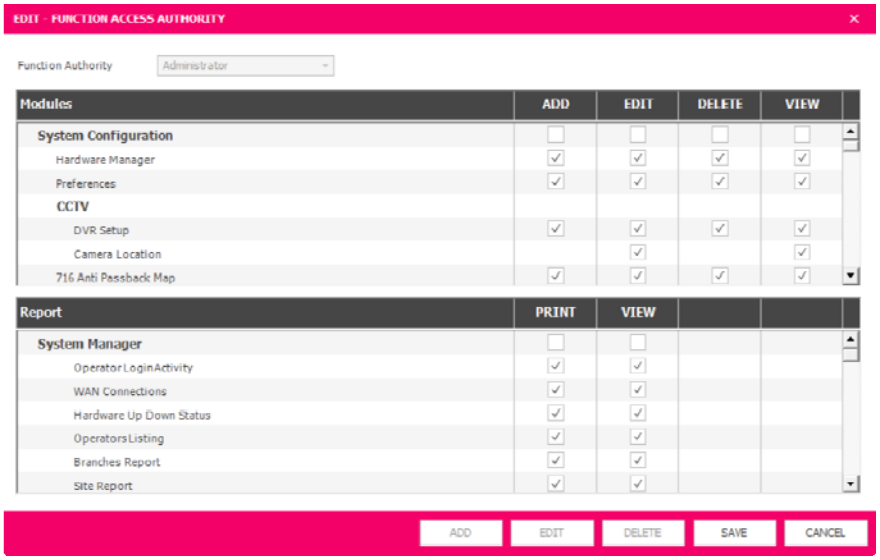


Fig 3.8.1: ***Function Access Authority.***

Fig 3.8.2: ***Confirmation.***

Adding Function Access Authority

1) Click on **ADD** button.
2) Enter the new Function Authority title.
3) Click on the checkbox as per the access that you want want to assign for the function access authority group. To grant access to the whole module just click on the module title. Access also can be granted for print or a view a particular report.
4) Click on **Save** button and it will prompt for confirmation.
5) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 3.8.2)*

Edit Function Access Authority

1) Select the Function Authority that you want to edit from the dropdown menu.
2) Once selected, click on the **Edit** button.
3) After editing the necessary fields, click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 3.8.2)*

Delete Function Access Authority

1) Select the Function Authority that you want to delete from the dropdown menu.
2) Once selected, click on the **Delete** button.
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 3.8.2)*

Cancel Function Access Authority

1) Click on the **Cancel** button to reject any entries while Adding or Editing before.

3.9 Branch

This is to add branch to be used for card user profiling.

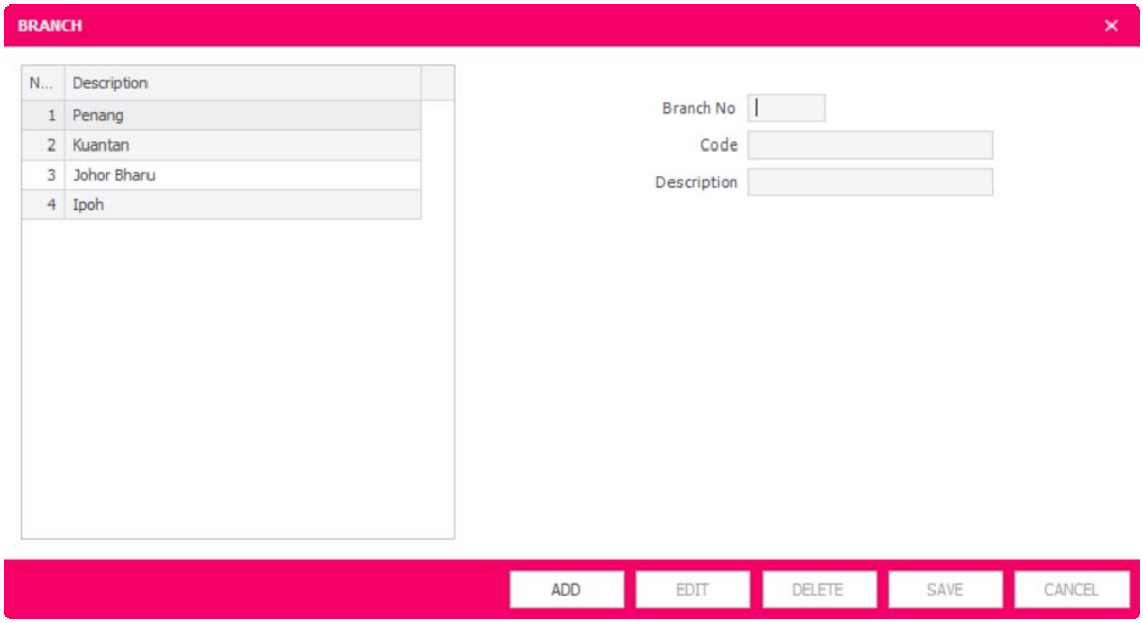


Fig 3.9.1: ***To add or delete the departments for card user .***

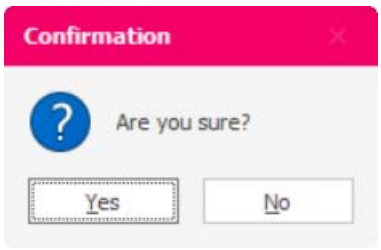


Fig 3.9.2: ***Confirmation.***

Adding Branch

1) Click on the **ADD** button.
2) The number no need to be assign since it is automated.
3) Enter the description of the branch
4) Click on the **Save** button and it will prompt for confirmation.
5) Click on **Yes** button to save the changes or **No** button to reject the changes. (Refer 3.10.2)

Editing Branch

1) Select the branch that you want to edit from the left panel list by clicking on it.
2) Once selected, click on the **Edit** button.
3) After editing the necessary fields, click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. (Refer 3.10.2)

Delete Branch

1) Select the branch that you want to delete from the left panel list by clicking on it.
2) Once selected, click on the **Delete** button.
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. (Refer 3.10.2)

Cancel Branch

1) Click on the **Cancel** button to reject any entries while Adding or Editing before

3.10 Department

This is to add departments to be used for card user profiling.

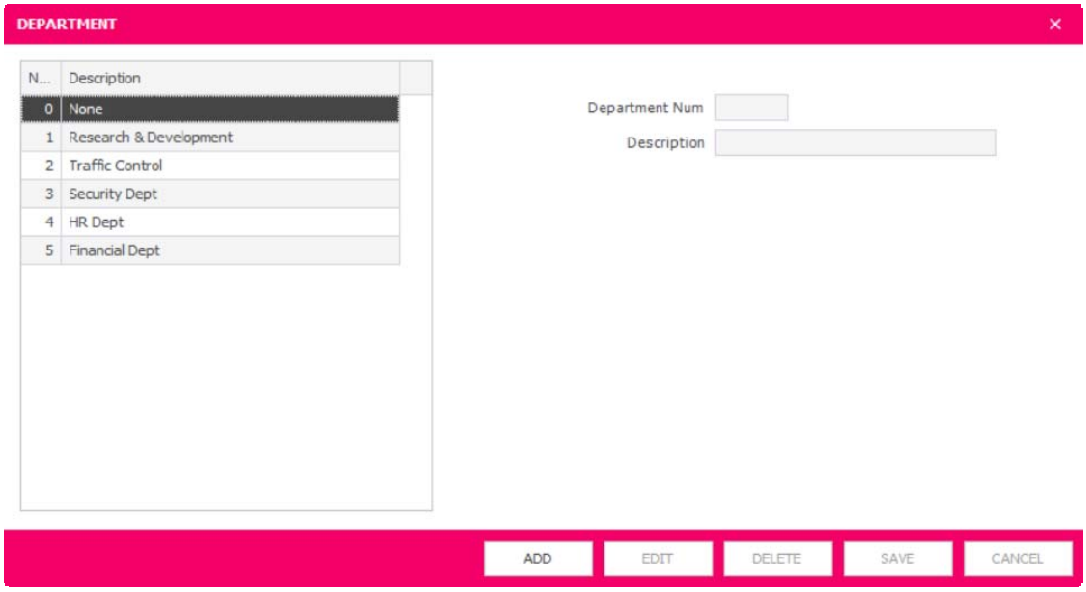


Fig 3.10.1: To add or delete the departments for card user profiling.

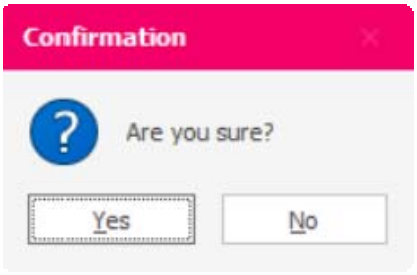


Fig 3.10.2: Confirmation.

Adding Department

1) Click on the **ADD** button.
2) The number no need to be assign since it is automated.
3) Enter the description of the department
4) Click on the **Save** button and it will prompt for confirmation.
5) Click on **Yes** button to save the changes or **No** button to reject the changes. (Refer 3.10.2)

Editing Department

1) Select the department that you want to edit from the left panel list by clicking on it.
2) Once selected, click on the **Edit** button.
3) After editing the necessary fields, click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. (Refer 3.10.2)

Delete Department

1) Select the department that you want to delete from the left panel list by clicking on it.
2) Once selected, click on the **Delete** button.
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. (Refer 3.10.2)

Cancel Department

1) Click on the **Cancel** button to reject any entries while Adding or Editing before.

3.11 Designation

This is to add designations to be used for card user profiling.

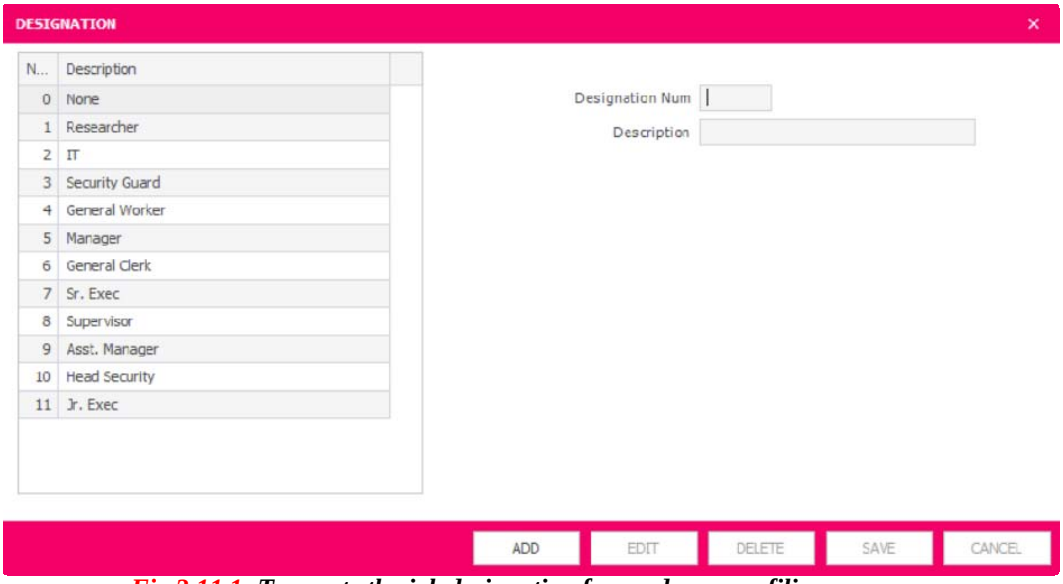


Fig 3.11.1: ***To create the job designation for card user profiling.***

Fig 3.11.2: ***Confirmation.***

Adding Designation

1) Click on the **ADD** button.
2) The number no need to be assign since it is automated.
3) Enter the description of the designation
4) Click on the **Save** button and it will prompt for confirmation.
5) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 3.11.2)*

Editing Designation

1) Select the designation that you want to edit from the left panel list by clicking on it.
2) Once selected, click on the **Edit** button.
3) After editing the necessary fields, click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 3.11.2)*

Delete Designation

1) Select the designation that you want to delete from the left panel list by clicking on it.
2) Once selected, click on the **Delete** button.
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 3.11.2)*

Cancel Designation

1) Click on the **Cancel** button to reject any entries while Adding or Editing before.

4) User Management

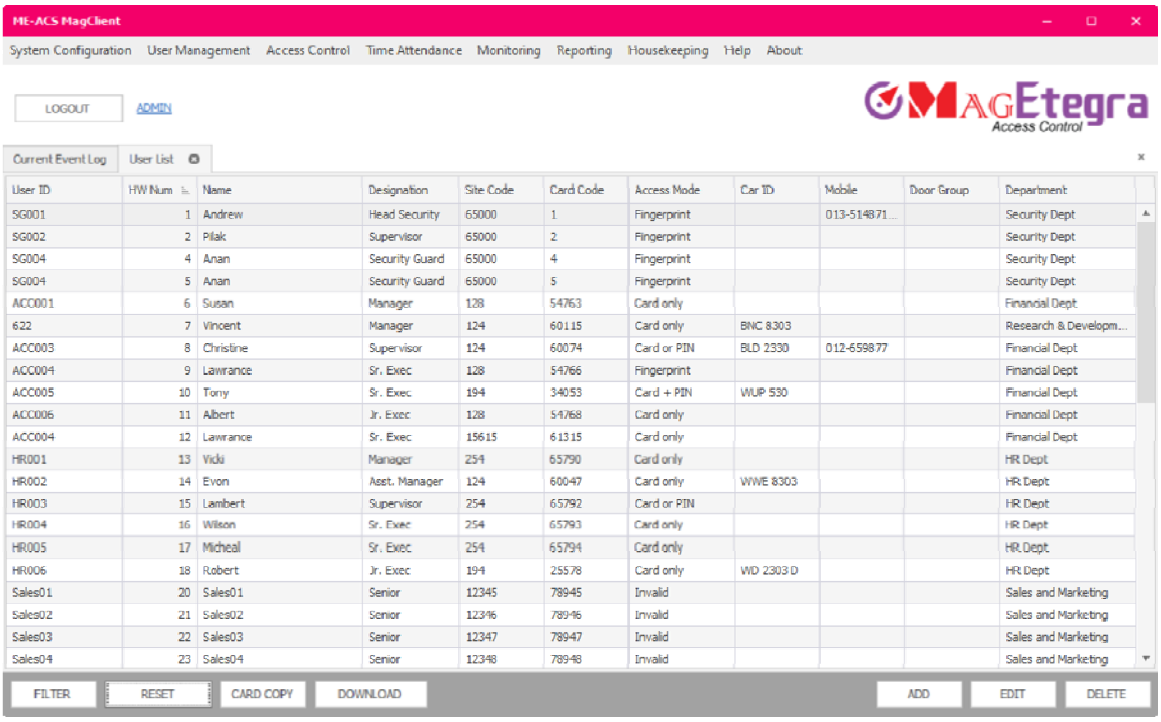
ME-ACS's user oriented access permission allows you to specify Who (card number) can access Where (door group) at What Time (time zone) using What Method (card and/or pin, fingerprint). Multiple cards with different access permission can be assigned to each user profile. One card could be used for parking and another card for door access. Card number can be auto-captured for super fast bulk enrollment. Advanced access permission give you the ultimate control to ensure that only authorized user can enter their authorized door(s).

The user management module is responsible for managing the card user settings profile. The module functionality is described as follows:

4.1 User List

All users will be listed out in tabular form here. Right click on the top row to select which field to hide or show. Each column field can be drag and drop to change its arrangement at top row. Every operator can choose which field to show and how each field is arranged. Field width and arrangements will remain the same every time the same operator login to the system. Click on the field for alpha numerical sort up and down. Pressing letter "L" on a field column will scroll to transaction that starts with "L".

The fields that will be displayed in the user list tab are *User ID, User Num, Name, Card num, Department, Designation, Branch, Shift, shift group, access mode, time zone, floor group, door group, pin change, anti- passback, holiday, skip FP, car id, legal id, address, telephone, mobile, email, gender, birth date, start date, special remark, guard patrol, expiry ending date, expiry starting date, alias, user level and advance.*



User ID	HW Num	Name	Designation	Site Code	Card Code	Access Mode	Car ID	Mobile	Door Group	Department
SG001	1	Andrew	Head Security	65000	1	Fingerprint		013-514871...		Security Dept
SG002	2	Pilak	Supervisor	65000	2	Fingerprint				Security Dept
SG004	4	Anain	Security Guard	65000	4	Fingerprint				Security Dept
SG004	5	Anain	Security Guard	65000	5	Fingerprint				Security Dept
ACC001	6	Susan	Manager	128	54763	Card only				Financial Dept
622	7	Vincent	Manager	124	60115	Card only	BNC 8303			Research & Developm...
ACC003	8	Christine	Supervisor	124	60074	Card or PIN	BLD 2330	012-6598877		Financial Dept
ACC004	9	Lawrance	Sr. Exec	128	54766	Fingerprint				Financial Dept
ACC005	10	Tony	Sr. Exec	194	34053	Card + PIN	WUP 535			Financial Dept
ACC006	11	Albert	Jr. Exec	128	54768	Card only				Financial Dept
ACC004	12	Lawrance	Sr. Exec	15615	61315	Card only				Financial Dept
HR001	13	Vicki	Manager	254	65790	Card only				HR Dept
HR002	14	Evon	Asst. Manager	124	60047	Card only	WWE 8303			HR Dept
HR003	15	Lambert	Supervisor	254	65792	Card or PIN				HR Dept
HR004	16	Wilson	Sr. Exec	254	65793	Card only				HR Dept
HR005	17	Micheal	Sr. Exec	254	65794	Card only				HR Dept
HR006	18	Robert	Jr. Exec	194	25578	Card only	WD 2303 D			HR Dept
Sales01	20	Sales01	Senior	12345	78945	Invalid				Sales and Marketing
Sales02	21	Sales02	Senior	12346	78946	Invalid				Sales and Marketing
Sales03	22	Sales03	Senior	12347	78947	Invalid				Sales and Marketing
Sales04	23	Sales04	Senior	12348	78948	Invalid				Sales and Marketing

***Fig 4.1.1:* The User list profiles.**

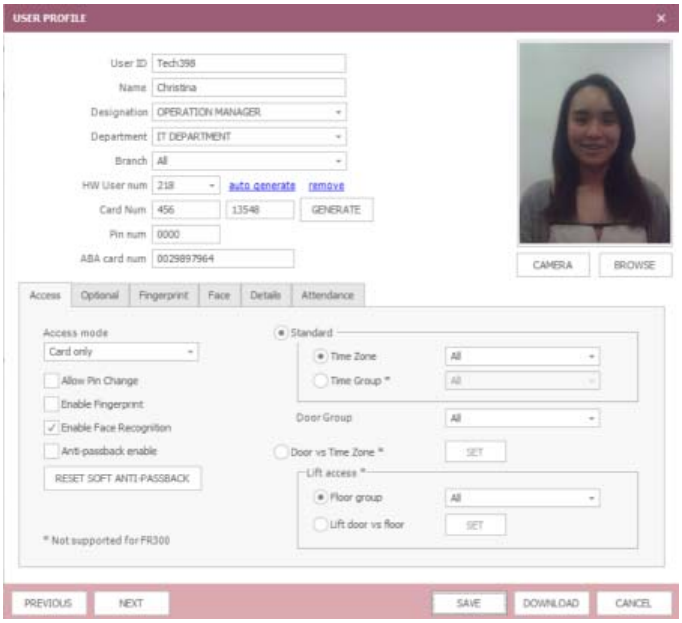


Fig 4.1.2: ***User profile.***

If this face photo will be enrolled into the MAG face recognition reader, it is important to ensure your face is positioned as big as possible at the center of the box. Please ensure even lighting to see the face clearly without any strong backlight. A proper face picture will ensure accurate and fast face recognition for the reader. A small, dark and blurry face picture will cause a lot of recognition problems for the reader.

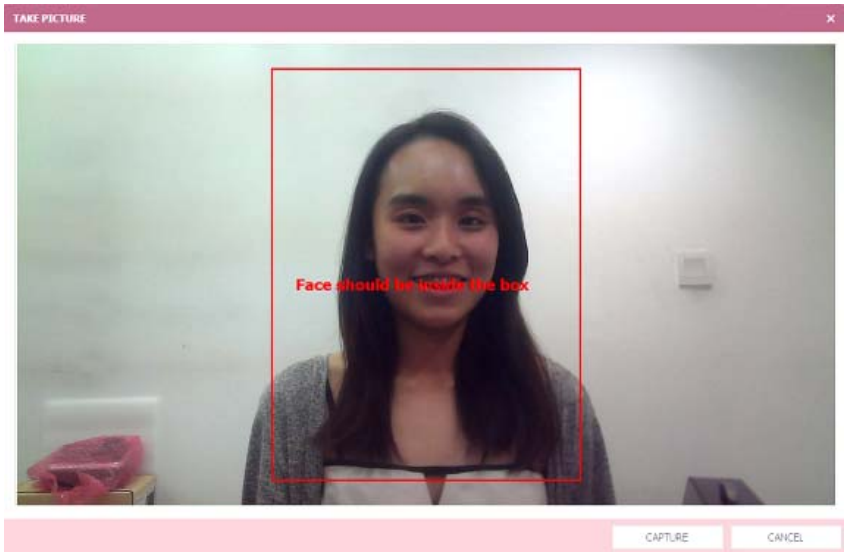


Fig 4.1.3: ***Take Picture.***

Note: ***The DOWNLOAD button inside the User Profile is download individual setting into reader. For those already be deleted and need to do All User download to clear the deleted user.***

Field name	Description
User ID	User ID is typically used as Employee ID in an organization. User ID is **unique** in entire organization and only represents specific single user profile in the system. User ID is used as main reference in reporting therefore it is important to assign User ID correctly from the beginning.
Branch	Branch indicate the user belong to which branch.
HW User num	**HW user number** is the **memory location** where the card and access permission is actually **stored in hardware**. This number is assigned automatically by system by clicking ***auto generate***. System will automatically find the next available empty slots. Each user profile is allowed to have more than one HW user num therefore enabling the possibility to have multiple cards with difference access permission under a same user profile. Click on remove will delete the HW User number. Once assigned HW User num, card number field cannot be empty.
Card number	This is typically the number printed on the proximity card or mifare card. *Format WG26:* **123,12345** *Format WG34:* **12345,12345** *Format ABA:* **1234512345**
Pin num	This is the pin code number for “card & pin” and “card or pin” access mode.

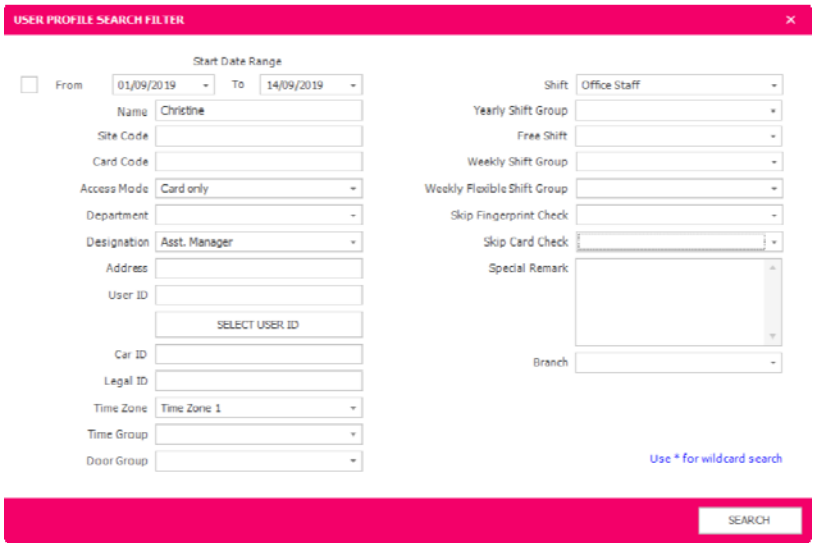


Fig 4.1.4: ***The indicated user profile will be show out by regarding the selected item during filter process.***

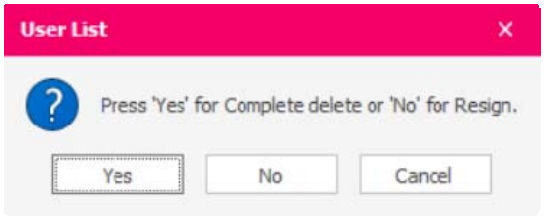


Fig 4.1.5: ***“No for Complete delete” is removes all record for the deleted user. “Yes for Resign” is the deleted user profile data can be retained and remark as resign.***

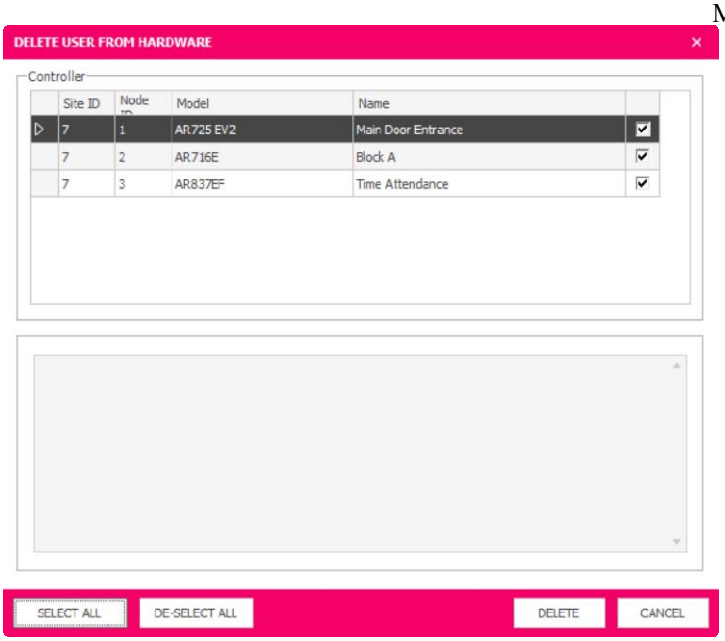


Fig 4.1.6: ***The process to download the updating information to selected controllers / readers.***

Adding User

1) Click on the **ADD** button.
2) A empty User Profile window will popup
3) User ID will be automatically assigned. But you also can assign the User ID number manually.
4) Insert the name of the user.
5) Select the Designation, Department and Branch from the dropdown.
6) The HW user num able to be auto generated or removed by the operator.
7) It is compulsory to insert card num after a HW user number is assigned to this user profile.
8) After saving this new profile, click on the **Download** button. Select target controller and download this new user profile to activate this new user on the controller *(Refer Fig 4.1.6).*

Enroll Face

1) Click on the **Camera** button. *(Refer Fig 4.1.2)*
2) A **Take Picture** window will popup*(Refer Fig 4.1.3)*
3) User face must be inside the red box when taking picture. *(Refer Fig 4.1.3)*
4) Click on **Capture** button to obtain the picture. *(Refer Fig 4.1.2)*
5) Click **Save** button to keep the picture. *(Refer Fig 4.1.2)*

Editing User

1) Select the User that you want to edit by single click
2) Once selected, click on the **Edit** button. You can also double click onto in user list to edit it.
3) The User Profile window wills popup.
4) Edit the necessary details from the user profile popup window.
5) After editing the necessary fields, click on the **Save** button. It will prompt for confirmation.
6) Click on **Yes** button to confirm accept the changes or **No** button to reject the changes.*(Refer Fig 4.1.4)*
7) After saving this edited profile, click on the **Download** button. Select target controller and download this new changes to be activated in the controller. *(Refer Fig 4.1.6)*

Delete Single User

1) Double click the user to edit it.
2) User profile will pop up.
3) Set the access mode to become “Invalid” then click on download button to download these changes to controller. When done, close user profile.
4) Select the User that you want to delete by single clicking on it
5) Once selected, click on the **Delete** button.
6) It will prompt *Press Yes for Completely or Press Delete No for Resign. (Refer 4.1.5)*
7) By default click **Yes** button to completely remove all transaction and data related to this user profile.

Click on **No** button if you want still want to retain all transactions and data for this user profile – this user profile will be marked as "**resigned**" status.

8) A menu will pop up to inform deletion in progress. Do not press any key to interrupt deletion process.

Delete Multiple Users

1) Select multiple User that you want to delete by single clicking on it while holding CTRL key
2) Once selected, click on the **Delete** button.
3) It will prompt *Press Yes for Completely or Press Delete No for Resign. (Refer 4.1.5)*
4) By default click **Yes** button to completely remove all transaction and data related to this user profile. Click on **No** button if you want still want to retain all transactions and data for this user profile – this user profile will be marked as "resigned" status.
5) A menu will pop up to inform deletion in progress. Do not press any key to interrupt deletion process.
6) Go to *System Configuration* →*Download* → select *all users* and download to all target controllers so that deleted user will be removed from hardware as well.

Download Multiple Users

1) Select multiple User that you want to delete by single clicking on it while holding CTRL/Shift key
2) Once selected, click on the **Download** button.
3) It will prompt **Hardware Selection** page.
4) Click on **Select All** button to download the selected user to all controller. If not select the controller to download the selected user to designated controller
5) Click **OK** button to proceed download.

IMPORTANT note:

All adding, editing and deleting of user profile is only applied to database. All these new changes will not be activated if is not downloaded into hardware. Newly created user will not be recognized by controller if it is not downloaded. Deleted user will not be removed from hardware if changes are not downloaded to controller. If you need to do a lot of changes in user profile, after you finalized all your changes, download all users to hardware from system configuration to ensure all changes is synchronized between database and hardware.

Cancel User

1) Click on the **Cancel** button to reject any entries while Adding or Editing before.

Filter User

This function allow operator to search for user profile(s) in a very fast and efficient manner.

1) Click on the **Filter** button.
2) The User Profile Search Filter window wills popup. *(Refer 4.1.3)*
3) Choose the date range you want to filter.
4) The filtering searches also consist of name, card number, access mode, department, designation, address, user id, duty shift and special remark.

Reset User

1) It is to reset all filtered result and resume back to full user list.
2) Click on the **Reset** button.

Card Copy User

This function allow selected field in a user profile to be copied to multiple other user profile. This is a very useful tool during batch user enrollment. After bulk auto-capture card number, common field such as department, designation, expiry date and access mode can be copied to group of similar user profile in batches. This function save you the hassle and time to assign all this field into each user profile one by one. For example user 1 to 50 is for marketing department. User 51 to 100 is for technical department. Card copy can be used to copy Department field from user 1 to 50. Card copy can be used again to copy Department field from user 51 to 100.

1) Select and highlight the user for card copy process, then click on **CARD COPY** button. *(Refer 4.1.6a)*

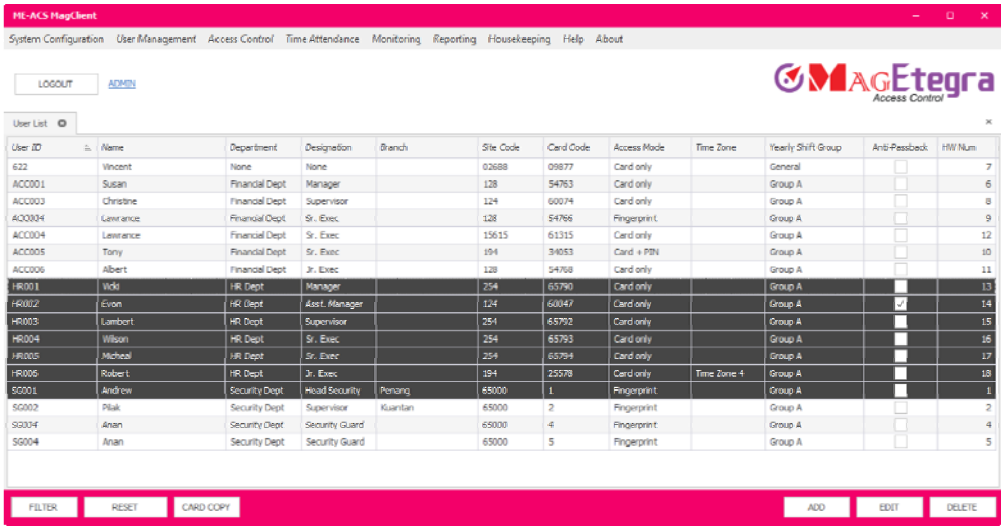


***Fig 4.1.6a:* The selected users for card copy process.**

2) Select one of the user to be as main source for card copy process. *(Refer 4.1.6b)*

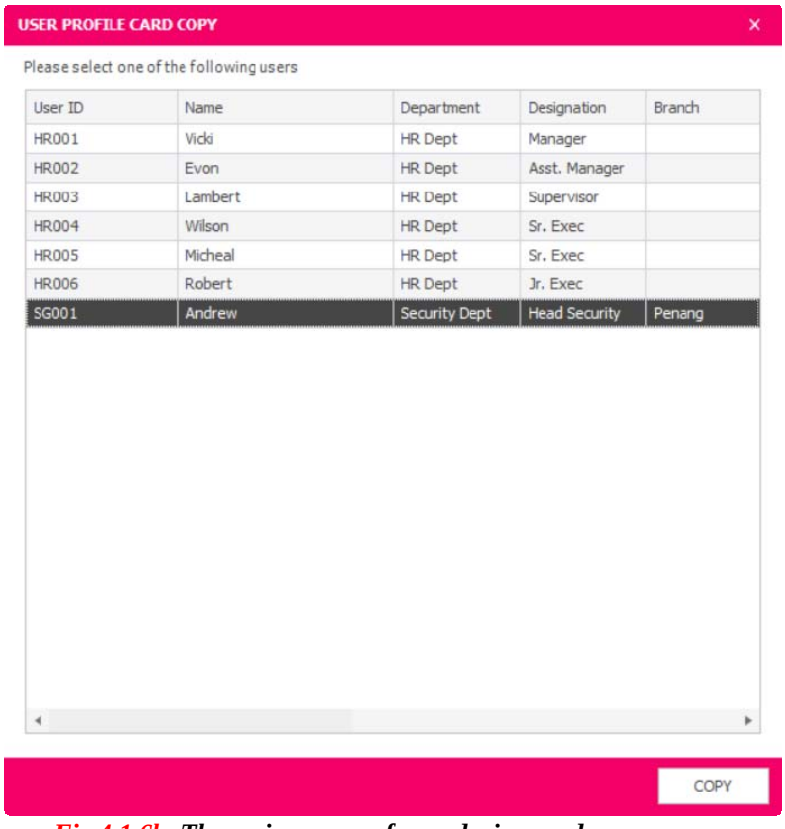


***Fig 4.1.6b:* The main source of user during card copy process.**

3) Click on the item want to be copy and click on COPY button to start copy. *(Refer 4.1.6c)*

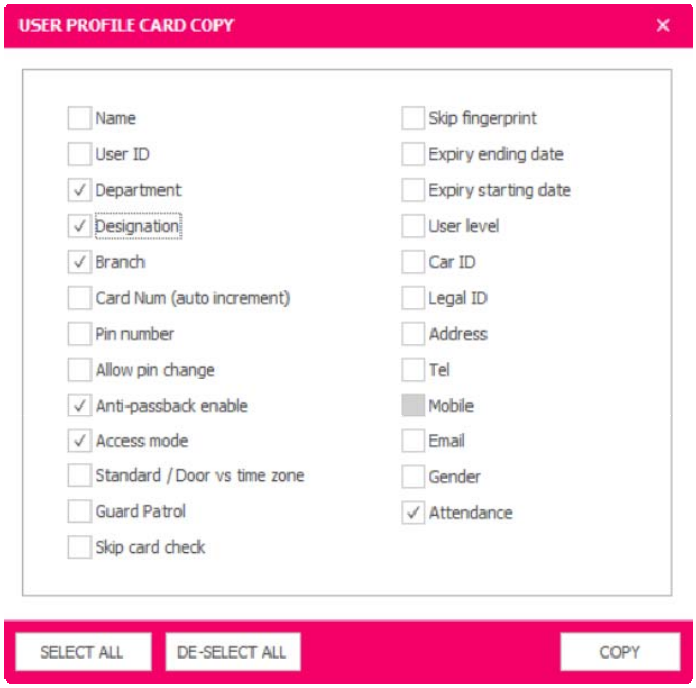


***Fig 4.1.6c:* The User Profile Card Copy selected field for card copy process.**

There are 5 tabs in user profile:

Tab 1) Access
Tab 2) Optional
Tab 3) Details
Tab 4) Fingerprint
Tab 5) Attendance

Tab 1) Access

This tab contains all the access security permission for this user profile.

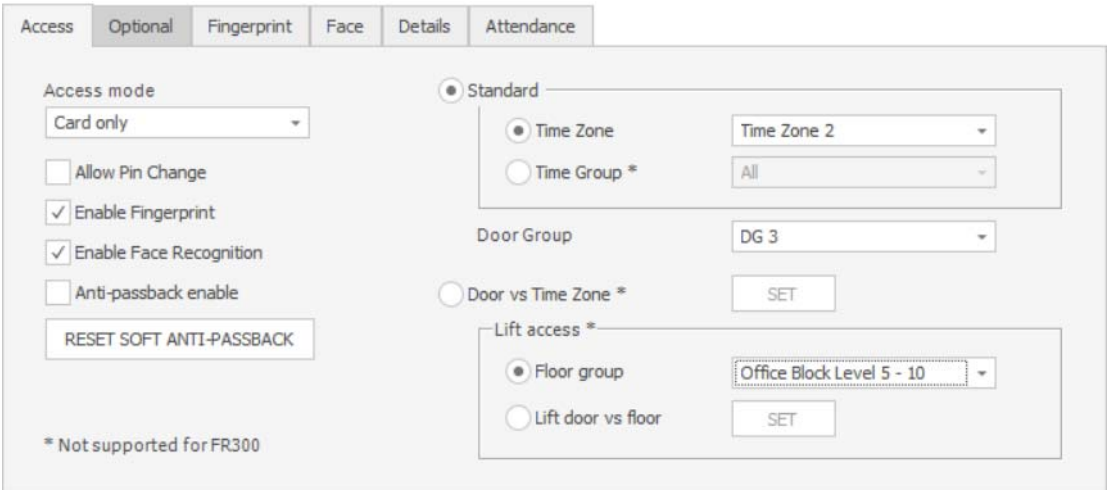


***Fig 4.1.7:* The access security permission for user profile.**

Field name	Description
Allow pin change	Allow user to change their pin number by themselves at keypad reader.
Enable Face Recognition	Allow the user to use the Face Recognition Device FR300
Enable Fingerprint	Allow the user to use the Fingerprint Device AR837EF
Anti-passback enable	Enable / disable anti passback checking for this user profile
Access mode	What method shall be used by user to access their authorized door? Card only, Card or Pin (either one), Card and Pin (both). Invalid means they are not allowed to enter any doors.
Standard	This is standard access permission setting. Time Zone – define weekly time interval of allowed access Door group – define which doors is allowed to access. The time zone is applied universally across all doors defined in door group. All doors can be access with the same Time Zone.
Door vs time zone	This is advance access permission setting. This user profile is only allowed to access specific door at specific time. Each door can be assigned with a different Time Zone.
Floor group	This is to set which floors are allowed to enter in elevator access control. This function must be used together with AR401R016 lift relay controller.
Lift door vs floor	This is to set which doors are allows to access which floors.

Note:

1) *Door vs Time Zone only can be download with Download All User for AR837EF, AR829E and AR721H, except the AR716E controller.*
2) *For the AR716 controller, Door vs Time Zone is need download individually inside the User Profile.*
3) *Each Door only can assign with 1 Time Zone or Time Zone Group.*

Tab 2) Optional

This tab contains access permission that is only available in certain model of controller.

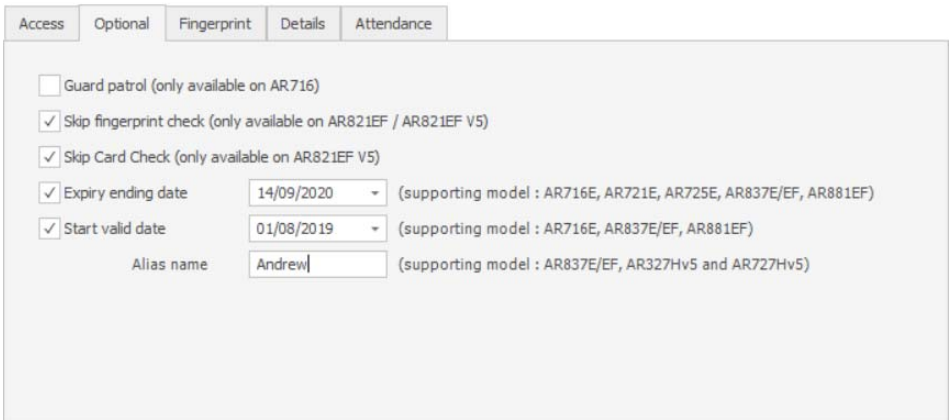


***Fig 4.1.8:* The access security permission for user profile in certain model controller.**

Field name	Description
Guard patrol	If enabled, door will not open after flash card. Transaction will still be recorded as Normal Access. This is typically assigned to security guard. Security guards flash their card as they pass by doors to register their guard tour time. When printed out on report, operator will know if the guards have visited all doors within the specified time to fulfill their guard tour schedule.
Skip fingerprint check	If enabled, AR837EF (fingerprint reader) will not check for fingerprint after flash card. Access is granted just by flashing card.
Expiry ending date	After this date, the card will no longer be valid. No access will be granted for this user after this date elapsed.
Valid starting date	Card will only be valid after this date.
Alias name	This is the name that will be displayed on the LCD screen. Typically this is a short name of the user as there is only limited character supported by LCD screen.

Tab 3) Details

This tab allow operator to enter more information to correctly identified user profile. This information is not critical and does not affect the access control security function. These additional fields allow easier searching and filtering.

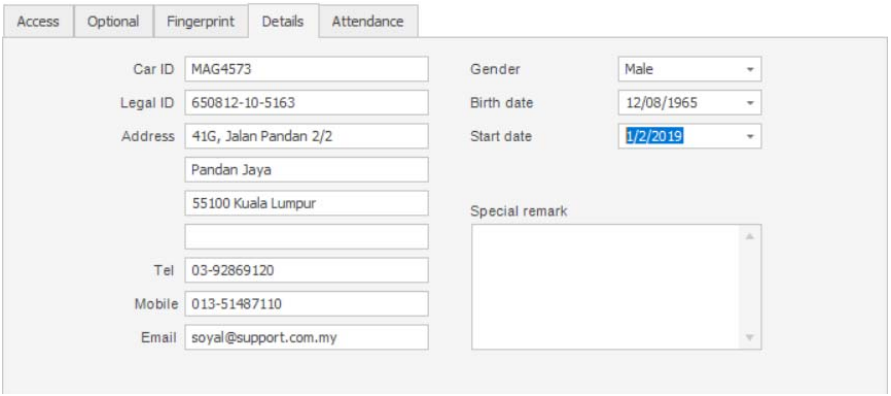


Fig 4.1.9: ***The basic information about the user profile but not related to access security.***

Tab 4) Fingerprint

This is especially useful when you have a lot of users and multiple fingerprint reader to distribute user traffic. For example, if you have 7000 users. Each fingerprint reader can support only 2250 users (each user 2 x fingerprints). It is also impossible for 7000 users to enter using a single fingerprint reader. The traffic has to be distributed among a few fingerprint readers. This function allows you to define fingerprint template for this user profile to be downloaded to which fingerprint reader. This way we can send 2000 users to reader 1, another 2000 users to reader 2 and so on until all users has been evenly divided among all readers. ME-ACS will automatically distribute the correct fingerprint template to its assigned fingerprint reader in System Configuration → Download → Fingerprint template.

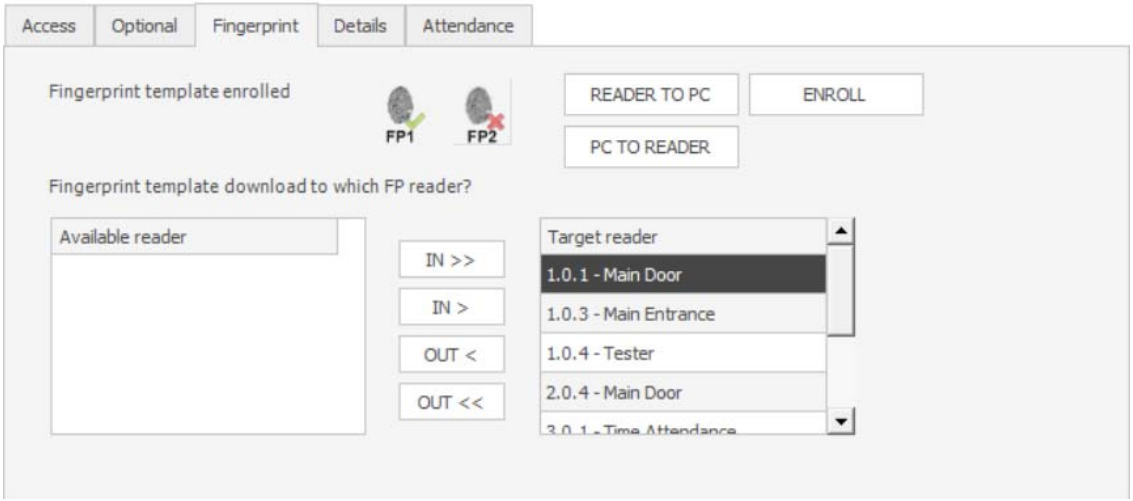


Fig 4.1.10: ***The access security permission for user profile using fingerprint system.***

Show the number of fingerprint enrolled.
Select the reader which you want the fingerprint template to be downloaded.
Enroll function is to enroll fingerprint by Etegra Software

Tab 5) Attendance

This tab assigned the working shift or shift group to be applied to this user profile when calculating time attendance data.

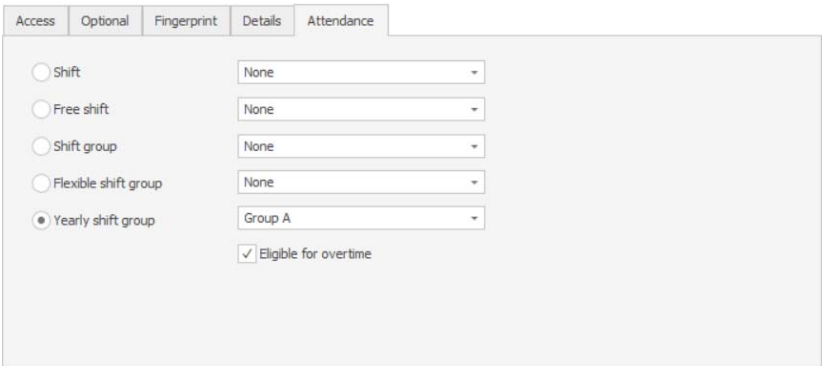


Fig 4.1.11: ***The working shift or shift group for user profile.***

Tab 6) Face

This tab allows operator to identify the user actual ID in the FR300 and update or retrieve the user photo. Hence it also allows the operator to distribute the photo to multi device along with access permission.

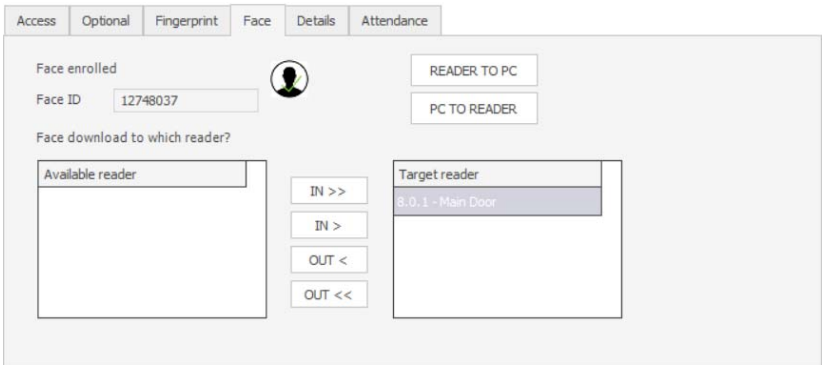


Fig 4.1.10: The access security permission for user profile using face system.

4.2 Resigned User List

All resigned users will be listed out in tabular form here. Right click on the top row to select which field to hide or show. Each column field can be drag and drop to change its arrangement at top row. Every operator can choose which field to show and how each field is arranged. Field width and arrangements will remain the same every time the same operator login to the system. Click on the field for alpha numerical sort up and down. Pressing letter "L" on a field column will scroll to transaction that starts with "L".

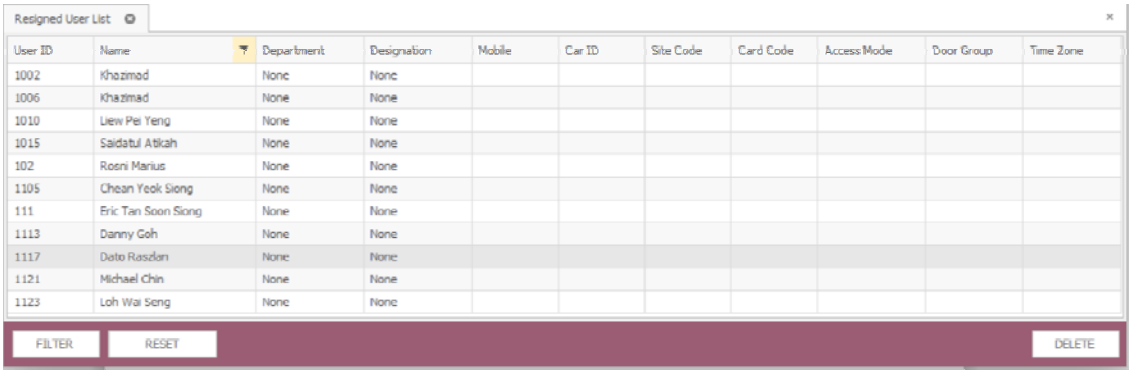


Fig 4.2.1: The Resigned User List

Restore User ID

Select the user and click **Delete** button for reuse the User ID.

4.3 Fingerprint Interface

Fingerprint interface help manage and maintain fingerprint templates of all users. Fingerprint Interface retrieve fingerprint template of all users from multiple AR837EF and stored it in centralized database. Fingerprint in centralized database can then be uploaded to any other AR837EF fingerprint reader. In the event of reader failure, these fingerprint templates can be easily transferring to new replacement reader without the hassle of re-enrolling everybody fingerprint again. Selected fingerprint templates can be exported text file as backup storage.

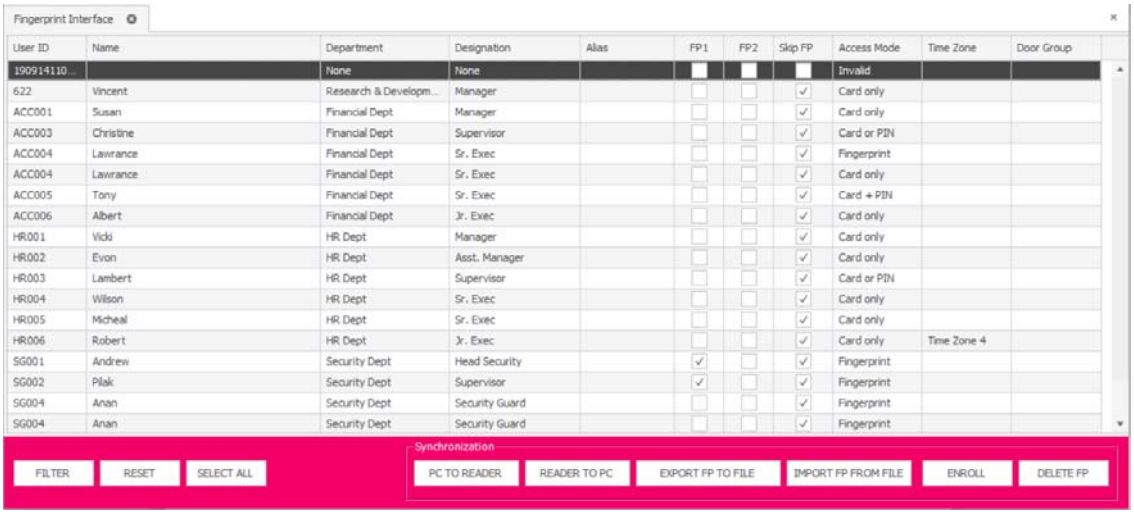


Fig 4.2.1: ***The data of fingerprint users profile transaction in Fingerprint Interface system settings.***

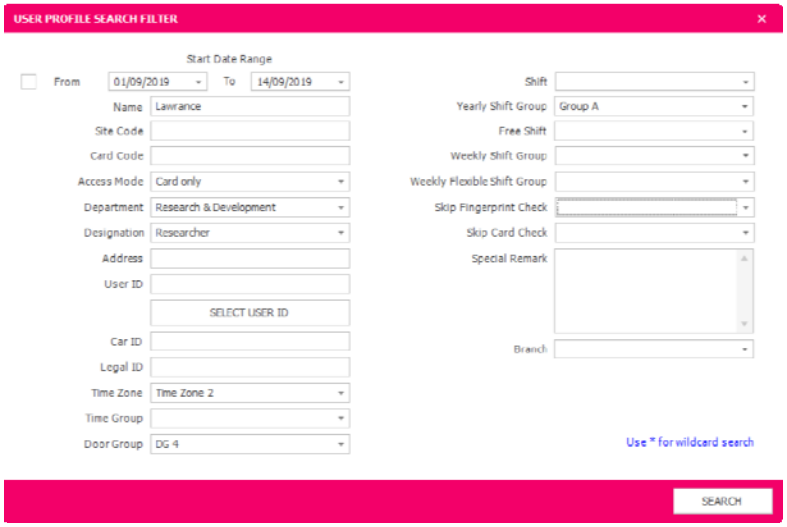


Fig 4.2.2: ***The user profile search filter will filter out all the information regarding the selected fields.***

Sync PC to Reader

Send fingerprint template of selected users from database to hardware reader.

Sync Reader to PC

Retrieve fingerprint template of selected users from hardware reader to database.

Export Fingerprint to File

Export fingerprint template stored in database to txt file.

Import Fingerprint to File

Import fingerprint template from a txt file to database.

Filter User

Click on the **Filter** button.
The User Profile Search Filter window wills popup. *(Refer Fig 4.2.2)*
Choose the date range you want to filter.
The filtering search also consists of name, card number, access mode, department, designation, address, user id, duty shift and special remark.

Reset User

(It is to reset according to the current user list)
Click on the RESET button.

4.4 Face Interface

Face interface helps to manage and maintain photo templates of all users. Face Interface retrieve face template of all users from multiple FR300 and stored it in a centralized database. Face template in the centralized database can then be uploaded to any other FR300 face recognition reader. In the event of reader failure, these face templates can be easily transferring to new replacement reader without the hassle of re-enrolling everybody face template again. Selected face templates can be exported in text file format as backup storage.

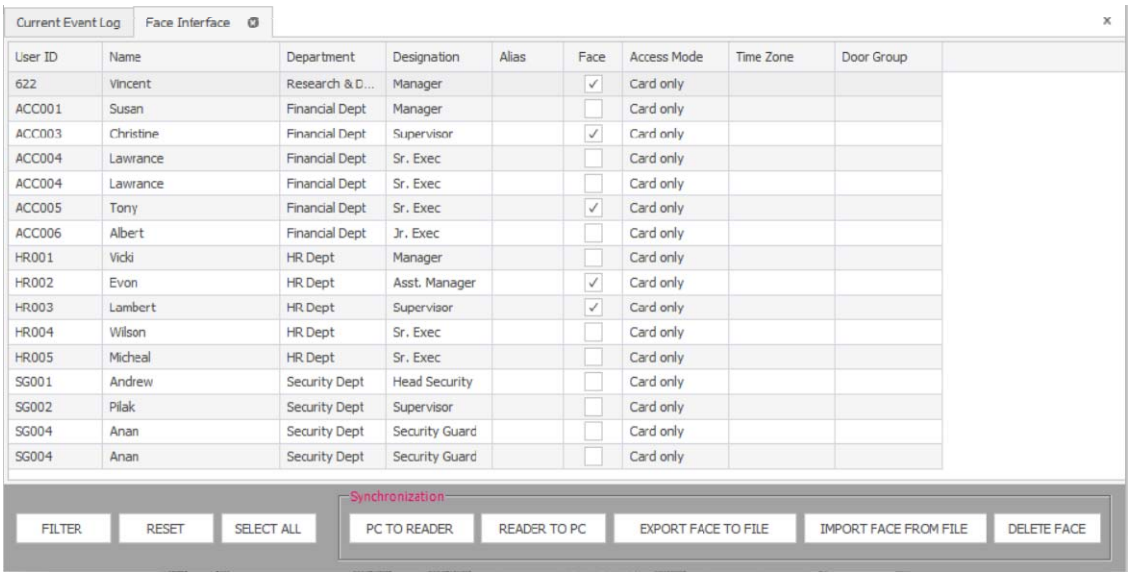


***Fig 4.2.1:* The data of face template users profile transaction in face Interface system settings.**

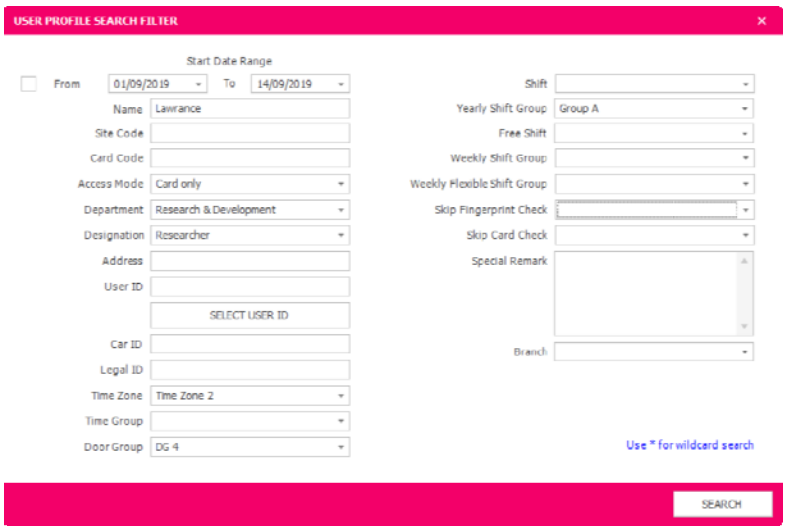


***Fig 4.2.2:* The user profile search filter will filter out all the information regarding the selected fields.**

Sync PC to Reader

Send face template of selected users from database to hardware reader.

Sync Reader to PC

Retrieve face template of selected users from hardware reader to database.

Export Face to File

Export Face template stored in database to txt file.

Import Face to File

Import face template from a txt file to database.

Filter User

Click on the **Filter** button.
The User Profile Search Filter window wills popup. *(Refer Fig 4.2.2)*
Choose the date range you want to filter.
The filtering search also consists of name, card number, access mode, department, designation, address, user id, duty shift and special remark.

Reset User

(It is to reset according to the current user list)
Click on the RESET button.

4.5 Fast Batch Enrollment

Fast batch enroll help to manage and generate users profiles more faster. Fast batch enrollment provides 2 alternatives way to generate or modify user's profiles more faster and easily, that is Auto Capture Card Number and Auto Generate User Profile. The Auto Capture Card Number is used to capture card number directly from reader during card enrollment (or during tag the card at reader). The Auto Generate User Profile is used to generate the User Profiles within certain range of user number. A list of User List can be generated base on the selected items more easily and efficiently.

User Management → Fast Batch Enrollment → Auto Capture Card Number ***or*** *Auto Generate User Profile.*

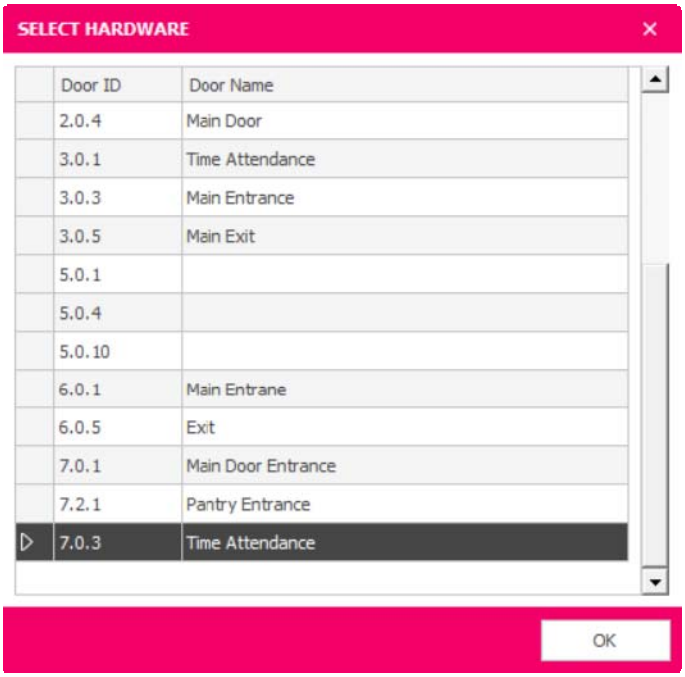


Fig 4.3.1: ***The hardware selection for card number capture.***

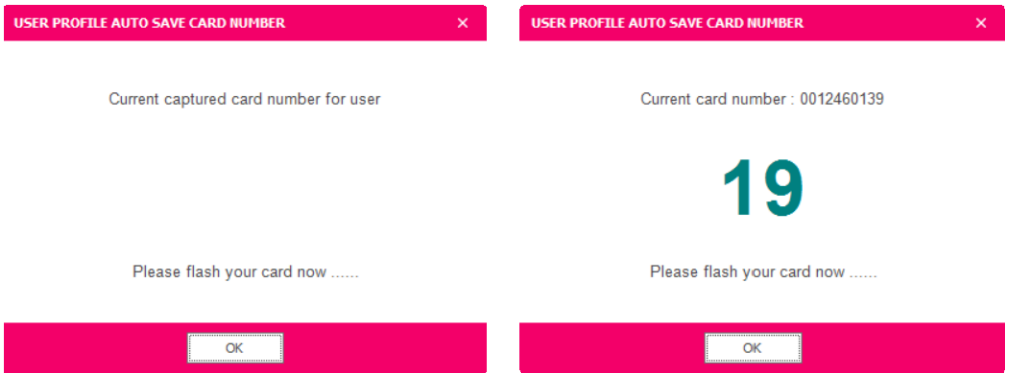


***Fig 4.3.2:* Before and after NEW card number capture.**

Auto Capture Card Number

This function allow easy enrollment of large number of users. The card number as printed on proximity card can be automatically captured as they are flashed on selected controller reader. This saves you the hassle of typing in the long card number one by one.

1) *User Management --> Fast Batch Enrollment --> Auto Capture Card Number.*
2) The **SELECT HARDWARE** window is prompt, select the hardware / reader is used for capturing the new users cards, then click on **OK** button to confirm it.
3) The **USER PROFILE AUTO SAVE CARD NUMBER** is prompt *(Refer Fig 4.3.2),* then start flash NEW card on the selected hardware / reader.
4) Continue flash the 2nd, 3rd, 4th ... new card users. Each time you flash a card, the card number will be captured and create a new user profile.

> ***Note:** If the card number **already exist** in User List, the card will cannot be captured again and notification of card duplication will prompt to avoid same user card number happen.*

5) When done, just click on **OK** button to exist this function.

IMPORTANT note:

*All adding, editing and deleting of user profile is only the records apply in database. All these new changes **will not take effect** if the latest updates or changes is not download to the controller / hardware. If not do **DOWNLOAD** to controller / hardware, for all new users will not be recognized by controller / hardware. For those deleted user will still able to log in if the changes are not downloaded to controller / hardware**. ALL the changes can be download all together by select the correct field and targeted controller / hardware.***

Auto Generate User Profiles

This function is used to generate large number of users within certain range of user number with include selected fields of user profile. The fields include the user ID, name, pin number, card number (Site Code + Card Code), department, designation, access mode, enable anti-passback, guard petrol, skip fingerprint check and skip card check. This function save your and time to assign the selected fields into each user profile one by one. This is a very useful tool during batch user enrollment. For example user 1 to 50 is for marketing department and user 51 to 100 is for technical department. Then, use this tool to generate Department field from user 1 to 50 and Department field from user 51 to 100.

1) Fill in the repeat count number that is the number of user want to be generated.
2) Select and fill in the fields want to be generate for user profiles. *(Refer Fig 4.3.3)*
   - ✓ *User ID* must be unique
   - ✓ *Format* indicates the number of digit for *start number*.

3) Click on **SAVE** button to save the existing auto-generate setting.
4) Click on **GENERATE** button to generate the users profile list.

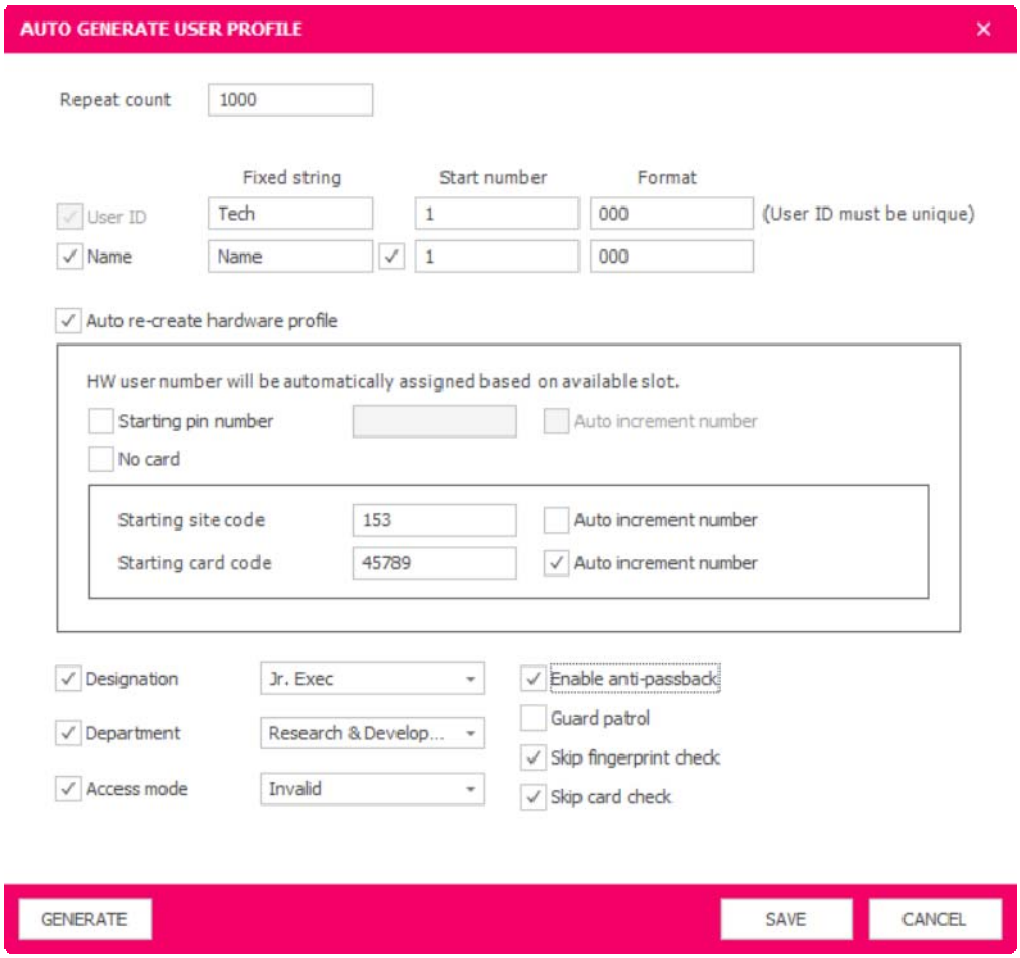


***Fig 4.3.3:* The Auto Generate User Profile**

5) Access Control

The access control module is responsible for managing the holiday, door group, time zone, floor group and time group settings as per the requirements. These are the settings that define access control permission - when user can enter which door? These permissions are then assigned to each user in User Profile. SACS is user-oriented access control system.

IMPORTANT note:
All access control permission defined here must be downloaded to hardware for it to become activated. ***Download Holiday, Time Zone or Door Group first*** *before does ALL USER download or download user individual from User Profile. Saving all these settings in software will not activate the features. All permission setting can be downloaded to hardware via System configuration →Download.*

5.1 Holiday

The holiday calendar is to define the company authorized holidays. It allows selection of multiple days simultaneously and grouped under a single holiday name by single clicking on the days. Able to select multiple or individual dates. All date will be able to select and un-select by clicking on it again. Holiday is taken into consideration during time attendance calculation. No clocking during holiday will not be regarded as absent. If a time zone is assigned to user profile, **by default all controllers will deny the user entry during holiday**.

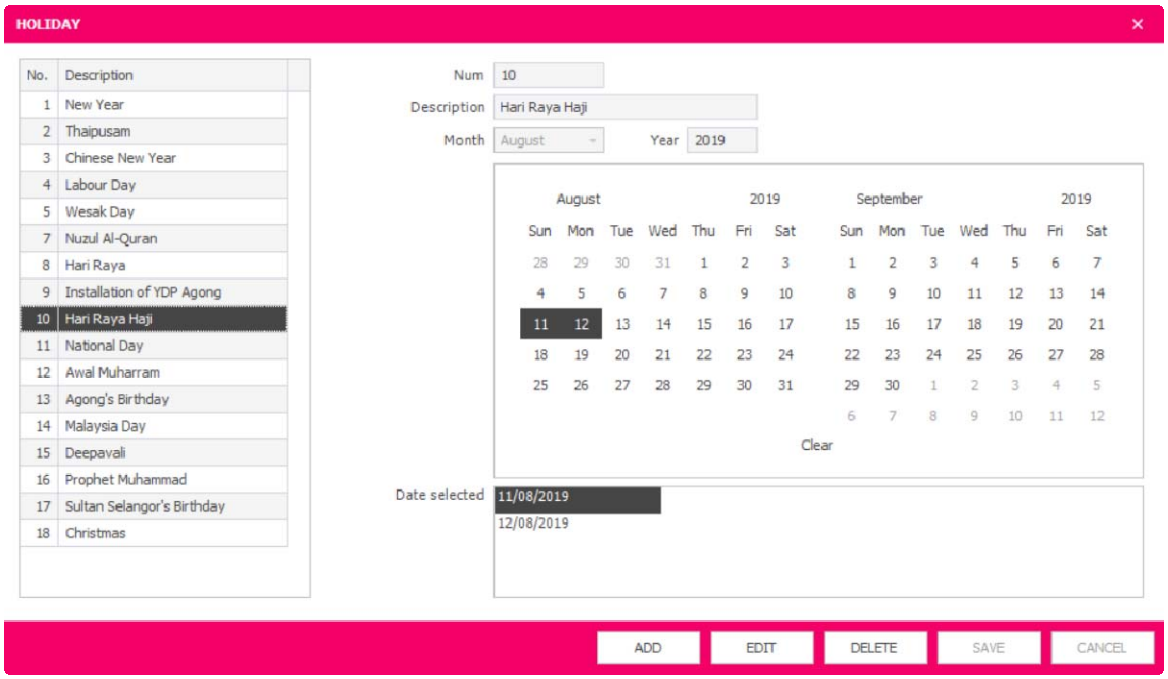


Fig 5.1.1: ***The Holiday setting and description.***

Fig 5.1.2: ***Confirmation.***

Adding Holiday

1) Click on the **ADD** button.
2) The number no need to be assign since it is automated.
3) Enter the description of the holiday.
4) Select the Year and the Month.
5) Click on the calendar date to select date. If for multiple date setting, use CTRL + click on the selected date.
6) Click on the **Save** button and it will prompt for confirmation.
7) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 5.1.3)*

Editing Holiday

1) Select the holiday that you want to edit from the left panel list by clicking on it.
2) Once selected, click on the **Edit** button.
3) After editing the necessary fields, click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 5.1.3)*

Delete Holiday

1) Select the holiday that you want to delete from the left panel list by clicking on it.
2) Once selected, click on the **Delete** button.
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 5.1.3)*

Cancel Holiday

1) Click on the **Cancel** button o reject any entries while Adding or Editing before

5.2 Door Group

Door Group is to define the single or multiple doors allowed to enter by user. Each door group will be identified uniquely using "Door Group Number".

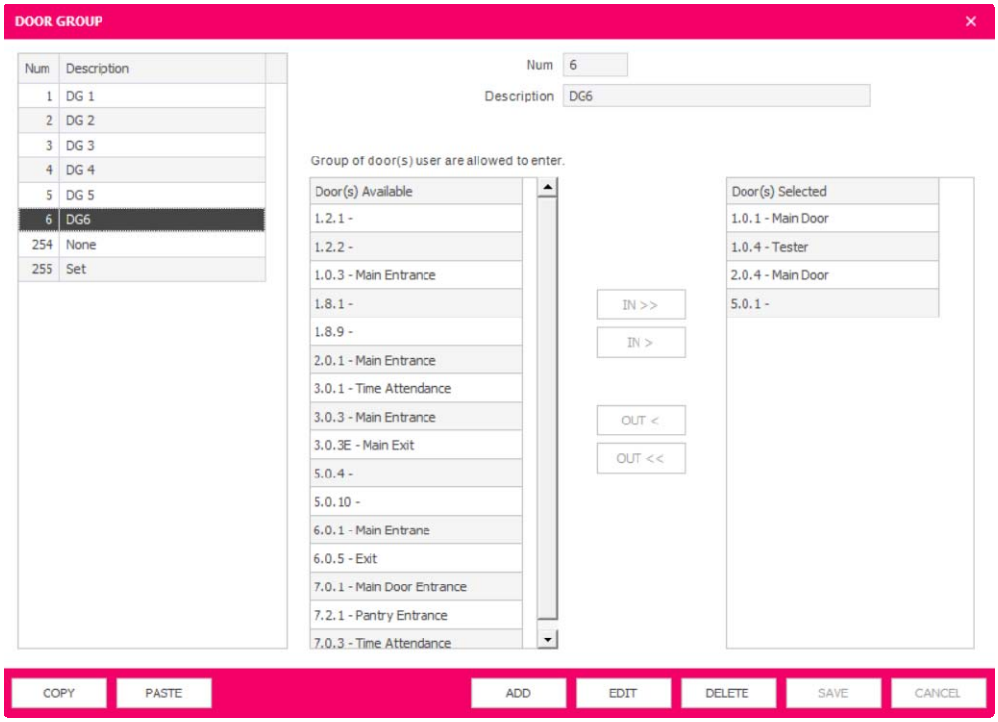


Fig 5.2.1: ***The selection multiples doors to form the door group.***

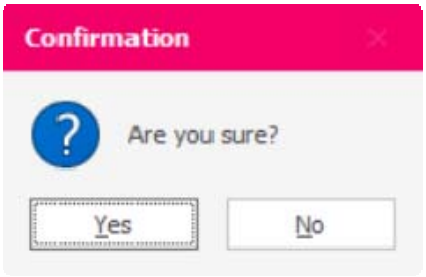


Fig 5.2.2:
Confirmation.

Adding Door Group

1) Click on the **ADD** button.
2) All the doors will be available in the list box. *(Refer 5.2.1)*
3) The number no need to be assign since it is automated. But you also can assign the number manually
4) Enter the description of the door group
5) Select the door in the door available list and click **IN >>** for in all or **IN >** for in only the selected door or vice versa.
6) Click on the **Save** button and it will prompt for confirmation.
7) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 5.2.2)*

Edit Door Group

1) Select the door group that you want to edit from the left panel list by clicking on it.
2) Once selected, click on the **Edit** button.
3) After editing the necessary fields, click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 5.2.2)*

Delete Door Group

1) Select the door group that you want to delete from the left panel list by clicking on it
2) Once Selected, click on the **Delete** button.
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 5.2.2)*

Cancel Door Group

1) Click on the **Cancel** button to reject any entries while Adding or Editing before.

5.3 Time Zone

The time zone defines weekly time interval that the user is allowed to enter the door. Multiple time zones can be linked together under "Time Group". Each Time Group is uniquely identified by "Time Group Number". Time group allow user to access the door on multiple interval within same day. You are able to sort ascending or descending by clicking on the tab. You are able to sort according to time group, time zone and time zone description.

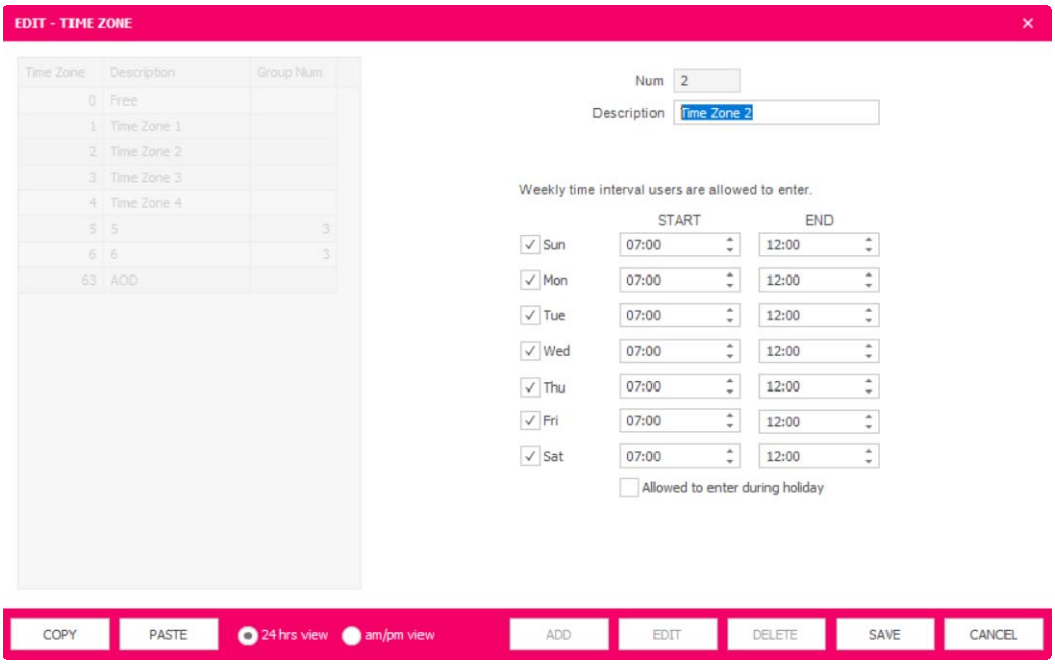


Fig 5.3.1: ***Time zones setting for access security control.***

Fig 5.3.2: ***Confirmation.***

Adding Time Zone

1) Click on the **ADD** button.
2) The number no need to be assign since it is automated.
3) Enter the description of the time zone.
4) Tick/Choose the days for the time zone and also insert Start time and End time.
5) Tick/Choose the checkbox if allowed to enter during holiday.
6) Click on the **Save** button and it will prompt for confirmation.
7) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 5.3.2)*

Edit Time zone

1) Select the time zone that you want to edit from the left panel list by clicking on it.
2) Once selected, click on the **Edit** button.
3) After editing the necessary fields, click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 5.3.2)*

Delete Time zone

1) Select the time zone that you want to delete from the left panel list by clicking on it
2) Once Selected, click on the **Delete** button.
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 5.3.2)*

Cancel Time zone

1) Click on the **Cancel** button to reject any entries while Adding or Editing before.

Time Format View

1) The radio button able to change the time format, either 24hrs or 12hrs (am/pm) format.

Copy & Paste

1) Select the Time zone settings that wanted to duplicate to a new time zone.
2) Click the **COPY** button.
3) Click on the **ADD** button.
4) Click on the **PASTE** button.
5) Enter the new time zone name in the description.
6) Click on the **Save** button. It will prompt for confirmation.
7) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 5.3.2)*

5.4 Time Group

The time group defines multiple time zone(s) that are group together to form multi interval within the same day.

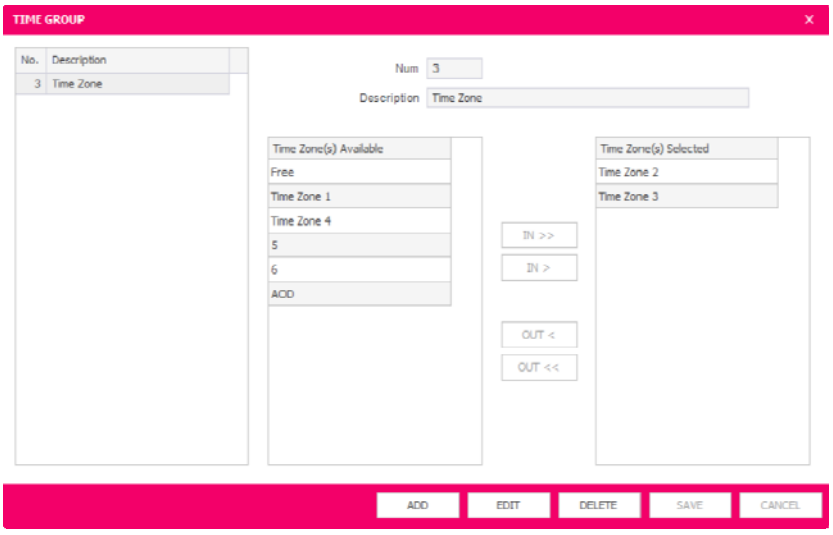


Fig 5.4.1: ***The selection of multiple time zones to form a time group.***

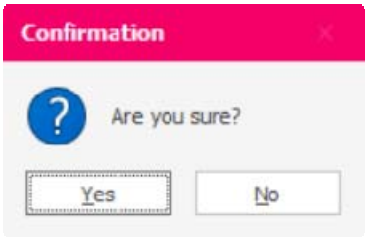


Fig 5.4.2:
Confirmation

Adding Time Group

1) Click on the **ADD** button.
2) All the time zones will be available in the list box. *(Refer Fig 5.4.1)*
3) The number no need to be assign since it is automated. But you also can assign the number manually
4) Enter the description of the time group.
5) Select the door in the door available list and click **IN >>** for in all or **IN >** for in only the selected time zones or vice versa.
6) Click on the **Save** button and it will prompt for confirmation.
7) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 5.4.2)*

Editing Time Group

1) Select the time group that you want to edit from the left panel list by clicking on it.
2) Once Selected, click on the **Edit** button.
3) After editing the necessary fields, click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 5.4.2)*

Delete Time Group

1) Select the time group that you want to delete from the left panel list by clicking on it.
2) Once Selected, click on the **Delete** button.
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 5.4.2)*

Cancel Time Group

1) Click on the **Cancel** button to reject any entries while Adding or Editing before.

5.5 Floor Group

The floor group defines which floor(s) can be accessed by user within the approved door group.

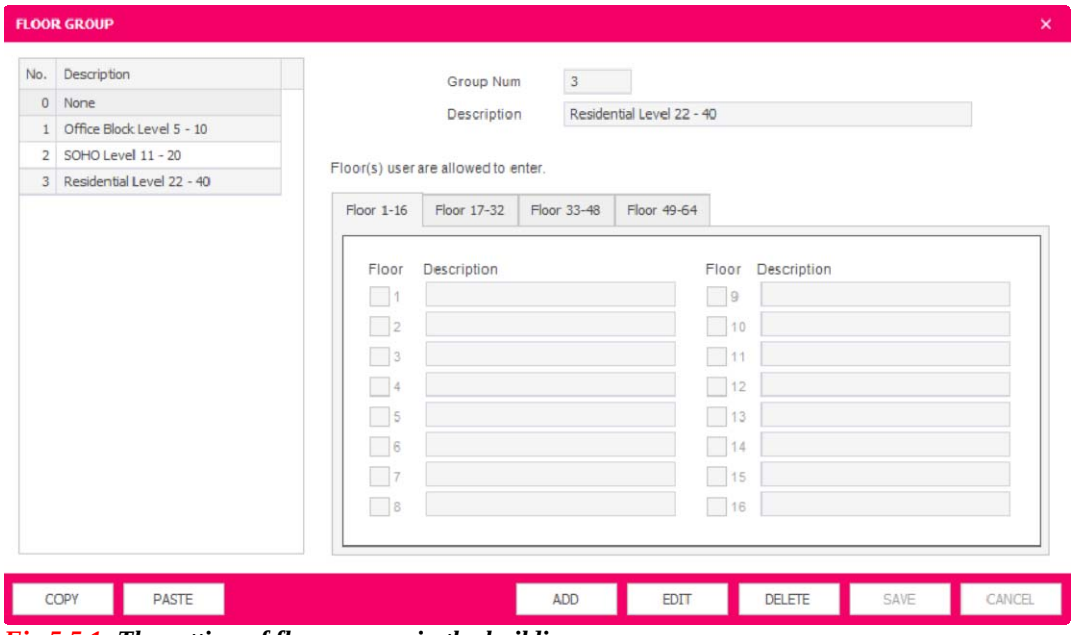


*Fig 5.5.1: **The setting of floor groups in the building.***

Fig 5.5.2: ***Confirmation.***

Adding Floor Group

1) Click on the **ADD** button.
2) The number no need to be assign since it is automated.
3) Enter the description of the floor group.
4) Tick/Choose the floors. (Can navigate the floors by using the tabs).
5) Enter the description for each floor selected.
6) Click on the **Save** button and it will prompt for confirmation.
7) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 5.5.2)*

Edit Floor Group

1) Select the floor group that you want to edit from the left panel list by clicking on it
2) Once selected, click on the **Edit** button.
3) After editing the necessary fields, click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 5.5.2)*

Delete Floor Group

1) Select the floor group that you want to delete from the left panel list by clicking on it.
2) Once selected, click on the **Delete** button.
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on Yes **button** to save the changes or No **button** to reject the changes. *(Refer Fig 5.5.2)*

Cancel Floor Group

1) Click on the **Cancel** button to reject any entries while Adding or Editing before.

5.6 Lift Door Selection.

The feature is used by the system during the download process with aim to reduce download process time involve lift settings. Lift Door Selection is used to identify which readers are used for lift security control only.

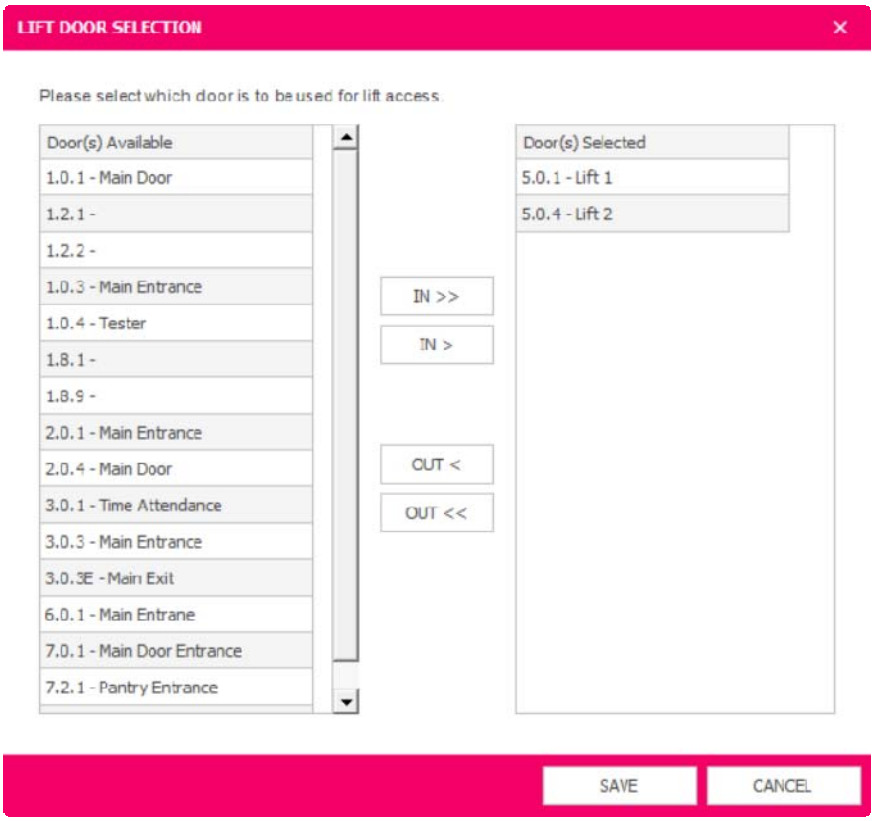


***Fig 5.6.1:* The selection door of Lift Door Selection.**

Fig 5.6.2:
Confirmation

Adding Lift Door Selection

1) Click on the **ADD** button.
2) All the selected doors will be available in the list box. *(Refer Fig 5.6.1)*
3) The number no need to be assign since it is automated. But you also can assign the number manually
4) Enter the description of the lift door selection.
5) Select the door lift in the door available list and click **IN >>** for in all or **IN >** for in only the selected door or vice versa.
6) Click on the **Save** button and it will prompt for confirmation.
7) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 5.6.2)*

Editing Lift Door Selection

5) Select the lift door selection that you want to edit from the left panel list by clicking on it.
6) Once Selected, click on the **Edit** button.
7) After editing the necessary fields, click on the Save button. It will prompt for confirmation.
8) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 5.6.2)*

Delete Lift Door Selection

5) Select the lift door selection that you want to delete from the left panel list by clicking on it.
6) Once Selected, click on the **Delete** button.
7) Click on the **Save** button. It will prompt for confirmation.
8) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 5.6.2)*

Cancel Lift Door Selection

2) Click on the **Cancel** button to reject any entries while Adding or Editing before.

5.8 Soft Global Anti-Pass (SGA)

The Soft Global Anti-Passback is a software simulated global anti-passback for TCPIP reader such as **AR725Ev2, AR837EF and AR881EF.** SGA will keep track of each user whether they are currently inside our outside based on the defined entry and exit reader. User that is already inside is not allowed to flash card on entry reader again. User will need to flash card at exit reader before they are allowed to flash card on entry reader again. User that are already outside is not allowed to flash card on exit reader again.

Operator need to define entry and exit reader of each sub group. Global anti-passback is maintained among the entry and exit reader defined within the sub group.Operator can define many sub group to mimic the door configuration in actual building.

SGA **does not support AR716E** multi door controller and **AR721E** 2-door controller.

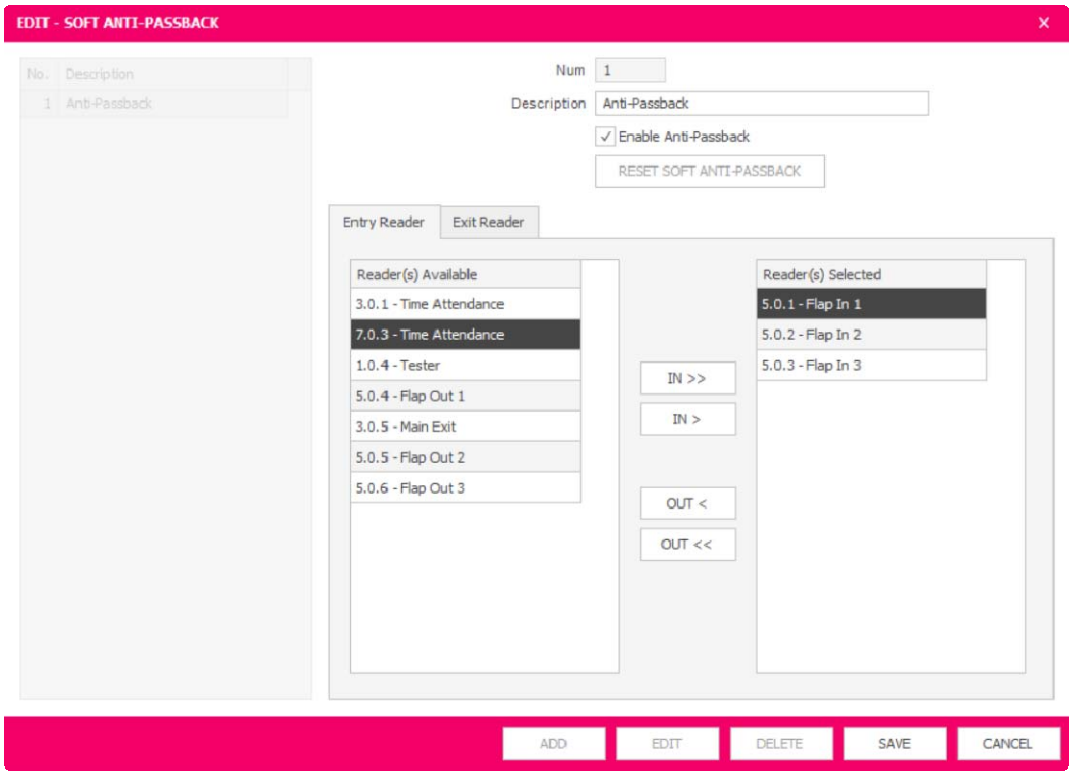


Fig 5.8.1: ***The selection multiples door to indicate Entry and Exit Reader***

Fig 5.8.2: ***Confirmation***

Creating Soft Global Anti-Pass

1) Click on the **ADD** button.
2) All the reader will be available in the list box. *(Refer 5.8.1)*
3) The number no need to be assign since it is automated. But you also can assign the number manually
4) Enter the description of the Soft Global Anti-Pass
5) Click on the Entry Reader tab to assign which reader as Entry Reader or vice versa
6) Select the reader in the reader available list and click **IN >>** for in all or **IN >** for in only the selected reader or vice versa.
7) Click on the **Save** button and it will prompt for confirmation.
8) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 5.8.2)*

Edit Soft Global Anti-Pass

1) Select the Soft Global Anti-Pass Group that you want to edit from the left panel list by clicking on it.
2) Once selected, click on the **Edit** button.
3) After editing the necessary fields, click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 5.8.2)*

Delete Soft Global Anti-Pass

1) Select the Soft Global Anti-Pass Group that you want to delete from the left panel list by clicking on it
2) Once Selected, click on the **Delete** button.
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 5.8.2)*

Cancel Soft Global Anti-Pass

1) Click on the **Cancel** button to reject any entries while Adding or Editing before.

Enable/Disable Soft Global Anti-Pass

1) Check on the **Enable Anti-Passback** to activate the anti-passback.
2) If uncheck the **Enable Anti-Passback**, all the card user will revert back to normal.

6) Time Attendance

Time attendance module support flexible multi shift, overnight shift and multi breaks to capture employee clocking as accurate as possible. Captured clocking data is analyzed to provide total work time, break time, overtime, late to work, early home and long lunch. This information allow HR department to monitor their employee punctuality efficiently to maintain high productivity yield. HR also able to quickly identify discipline issue such as late to work or long lunches
at early stage and correct this behavior before it becomes more serious. Leave management is available that allow employee to apply leave in advance. Comprehensive reports summarize employee attendance, leaves and punctuality into a tabular format for easy fast review. Time attendance module is a value added function to help you better manage human resources in your organization.

The module functionality is described as follows:

6.1 Weekly Shift Setting

This function is used to set the overnight shift and multiple break time. Time attendance module uses Time In and Time Out interval defined in shift to capture the correct clocking from employee. Employee must clock in or clock out within the time interval defined here to be captured as valid clocking. Any clocking outside the range of interval defined here will NOT be considered as valid clocking. Time attendance module also uses the Actual time defined here to decide where employee come late or go home earlier than they should be

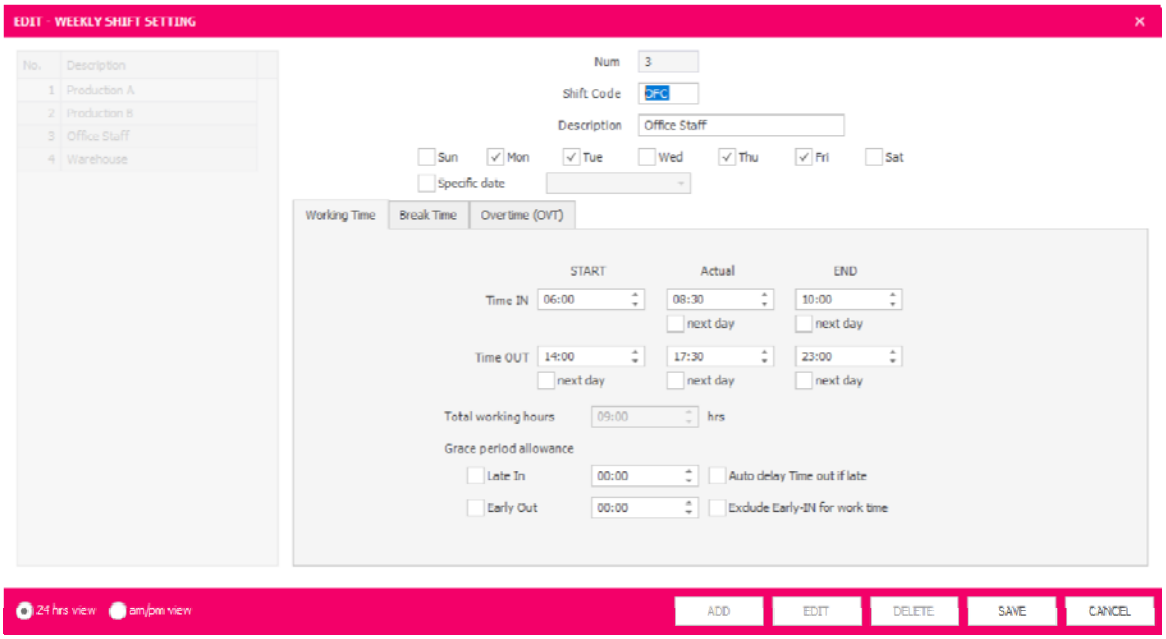


***Fig 6.1.1:* The settings of working shift include the working time, break time and overtime.**

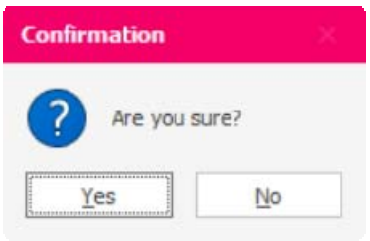


***Fig 6.1.2:* Confirmation**

Adding Shift

1) Click on the **ADD** button.
2) The number no need to be assign since it is automated. But you also can assign the number manually.
3) Enter the shift code and the description.
4) Select the days for the shift by tick/check the checkbox.
5) Select the specific for the shift by tick/check the checkbox and choose the date from the dropdown calendar by clicking the down arrow.
6) The dates also can be inserted without using the calendar and multiple dates is not allowed.
7) Navigate between the Working Time, Break Time And Overtime tabs to configure the settings.

Editing Shift

1) Select the shift that you want to edit from the left panel list by clicking on it
2) Once selected, click on the **Edit** button.
3) After editing the necessary fields, click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 6.1.2)*

Delete Shift

1) Select the holiday that you want to delete from the left panel list by clicking on it.
2) Once Selected, click on the **Delete** button.
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 6.1.2)*

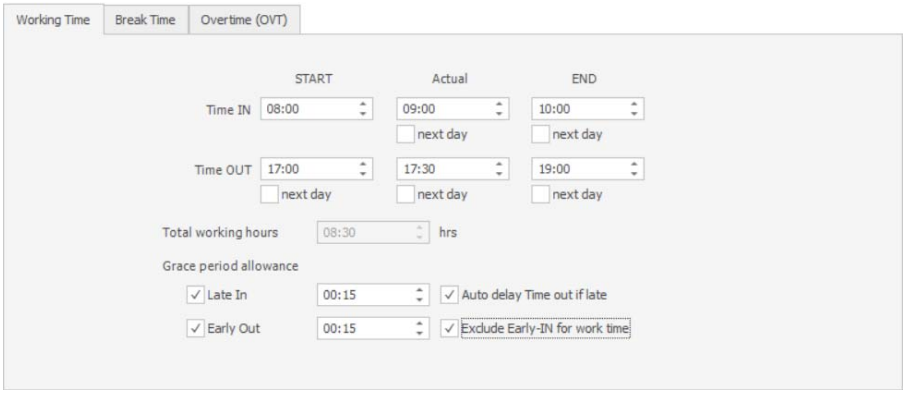
Cancel Shift

1) Click on the **Cancel** button to reject any entries while Adding or Editing before.

There are 3 tabs of shift setting:

Tab 1) Working Time
Tab 2) Break Time
Tab 3) Overtime

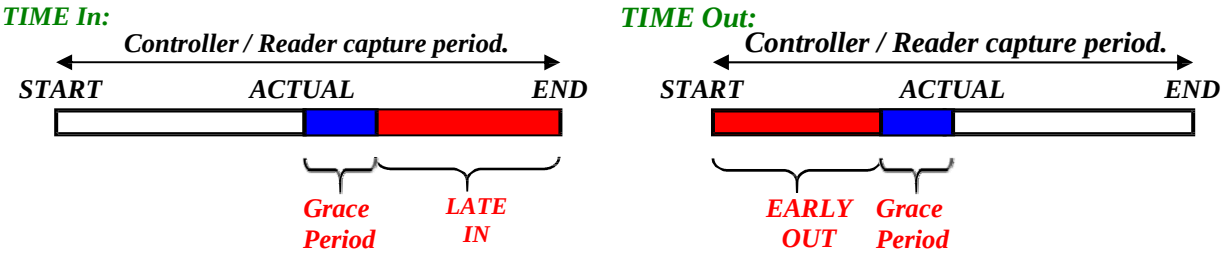
Tab 1) Working Time



1) Clocking period for Time In: 8:00 am - 10.00 am
Late In Period: After 9:15 am

2) Clocking period for Time Out: 5:00pm - 7.00 pm
Early Out Period: 5.00 – 5.45 pm

The grace period allowance: Late In: 15 minutes Early Out : 15 minutes



Function	Description
Time IN	To capture earliest **clocking within the START and END as Time IN**. If capture time is later than actual, it is considered Late IN.
Time OUT	To capture latest **clocking within the START and END as Time OUT**. If capture time is later than actual, it is considered Early Out. Next day need to be specified if it crossed 12 am midnight.
Next day	Tick **Next day** option if the time belongs to next day. This is to support **overnight shift** where the working shift crossed midnight 12am to the next day.
Auto delay time out if late	Late In is auto added into actual time out. If got employee is **late 10 min**, then he should **go home 10 min later**. If he goes home at actual Time Out, he is shall be considered 10 min early Out.
Exclude Early-IN for work time	The working time is excluded for the times of employee are come to work early.
Grace Period allowed	Grace period allowed before a clocking is considered as Late-In or Early out. Grace period is considered from ACTUAL time defined.

Tab 2) Break Time

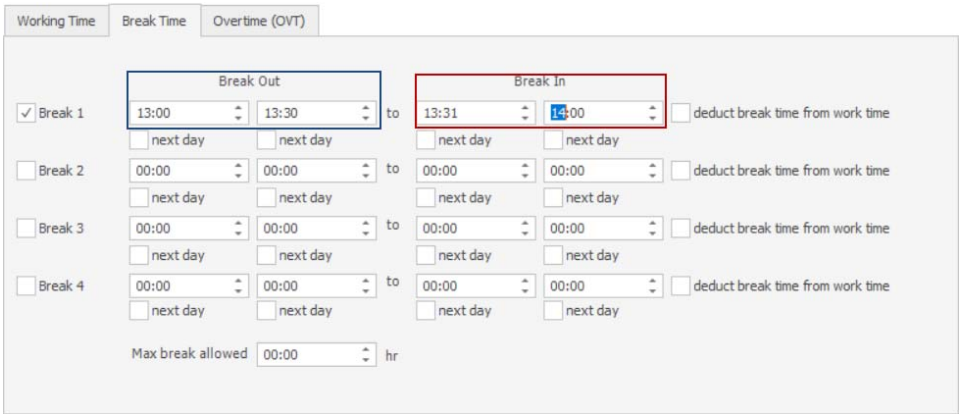
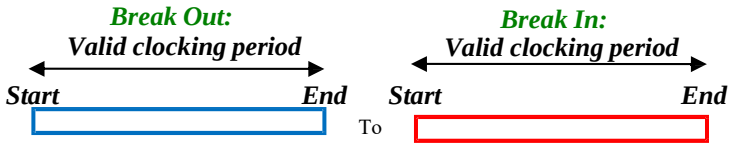


Fig 6.1.4: ***The Break Time idea of Break Out & Break In are captured by the controller or hardware.***

1) Clocking period for Break Out: 1.00 pm - 1.30 pm

2) Clocking period for Break In: 1.31 pm - 2.00 pm

The Max break allowed is 1 hour. Let say the user go out early and come in late, if the break/lunch period is more than 1 hour, will remark as Long Break in attendance report.



Let say:
Clocking 12.50 pm (As invalid data) Clocking 1.25 pm (As Break Out) Clocking 1.45 pm (As Break In) Clocking 2.02 pm (As invalid data)

Function	Description
BRK OUT	Brk Out is actual "official" time employee shall take break. The box at the front shall indicate how much min ahead the SOY shall start capturing for actual BRK OUT clocking. For example, if specified as **30 min**, then BRK OUT time is **1.00pm**, that employee shall clock for **break out between 12.30pm to 1.29 pm**. Otherwise it shall be considered as No Break Out in the report.
BRK IN	Brk In is actual "official" time employee shall take break. The slot at the front shall indicate how much min ahead the SOY shall start capturing for actual BRK IN clocking. For example, if specified as **30 min**, then **BRK IN time is 2.00pm**, that employee shall clock for **break in between 1.30pm to 2.30 pm**. Otherwise it shall be considered as No Break In in the report.
Next day	Tick **Next day** option if the time belongs to next day. This is to support **overnight shift** where the working shift crossed midnight 12am to the next day.
Deduct break time from work time	This option will **deduct from actual working time if break time is more then max break allowed.** Deducted work time will reflected in the report as total work time.
Max break allowed	If break time calculated from the actual clocking is **greater than the max break allowed**, then it shall be indicated in reporting as **Long Break.**

Tab 3) Over Time

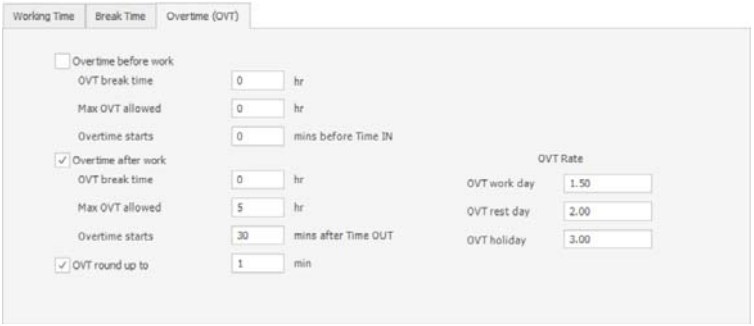


Fig 6.1.5: The settings of overtime calculation.

The Overtime is base on the Working Time setting, especially the Time Out: END period setting.

The period is set the range of clocking period controller to take record. If the user Time Out is out of the range of clocking period, the controller will not record in attendance report.

Function	Description
Overtime before work	Does the overtime calculation need to include the time when employee is early to work?
Overtime after work	Does the shift allow overtime after work?
Overtime start time	Overtime shall start at a delayed time after Actual Time-Out. **Entering 0 means overtime starts immediately after Actual Time-Out**. Overtime start time must be after Time-Out`s START before Time-Out`s end.
Overtime break time	This break time shall be deducted from the total overtime worked
Max OVT allowed	Example, max OVT is 5 hrs. If employee overtime is 8 hrs, report will only show 5 hrs. The additional overtime will be ignored. **Max OVT must be within Time Out end time**. SOY shall indicate this as an error if MAX OVT exceeded end time.
OVT round up nearest min	Example, 15 min. If total overtime is 3hrs 5 min and the auto round up will become 3 hrs 15 min.
OVT Rate	If attendance setting enables OVT rate calculation, actual overtime will be multiplied to these rates and final result shall appear in report.

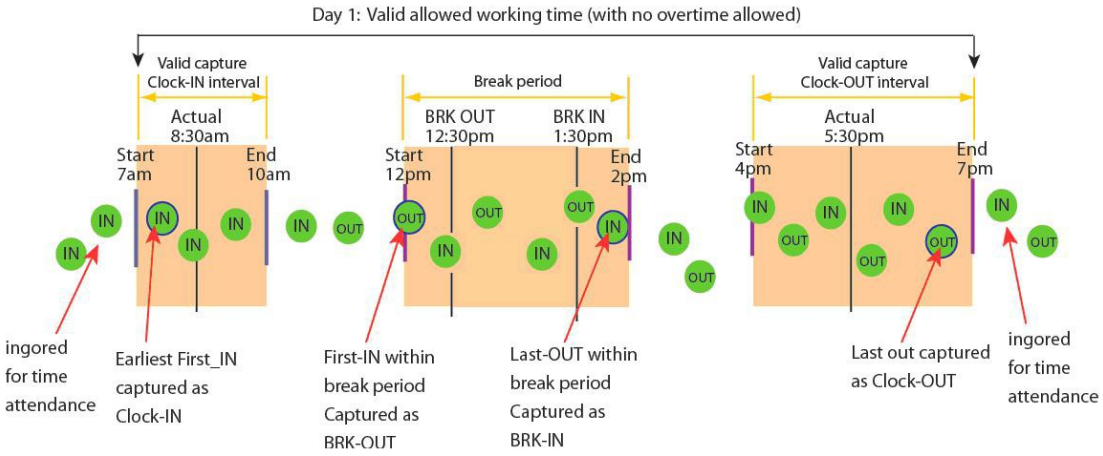
Click on the **Save** button and it will prompt for confirmation.
Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 6.1.2)*

How clocking time is captured based on clocking interval defined in shift?

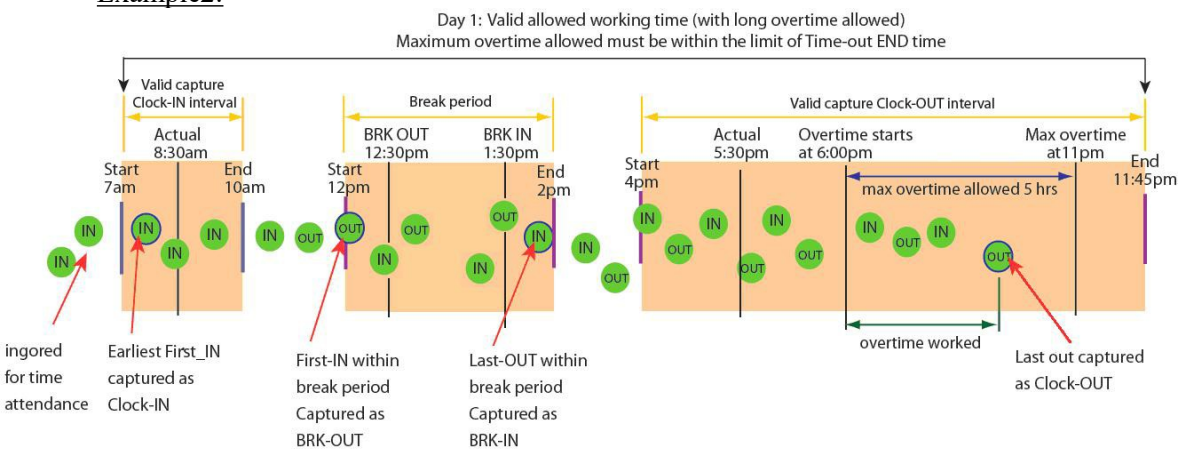
Following time line diagrams show all card badging activity within a working day. Assuming a employee badge their card multiple time during a day as they go out and back through main entrance. So multiple event transactions will be recorded in access event transaction - indicated by Green circle. Only one of the green circle that fall within the defined time interval in shift settings will be chosen as valid clocking time. Following diagram illustrate which green circle will be chosen as valid clocking and why they are chosen.

Yellow region indicate valid region to capture

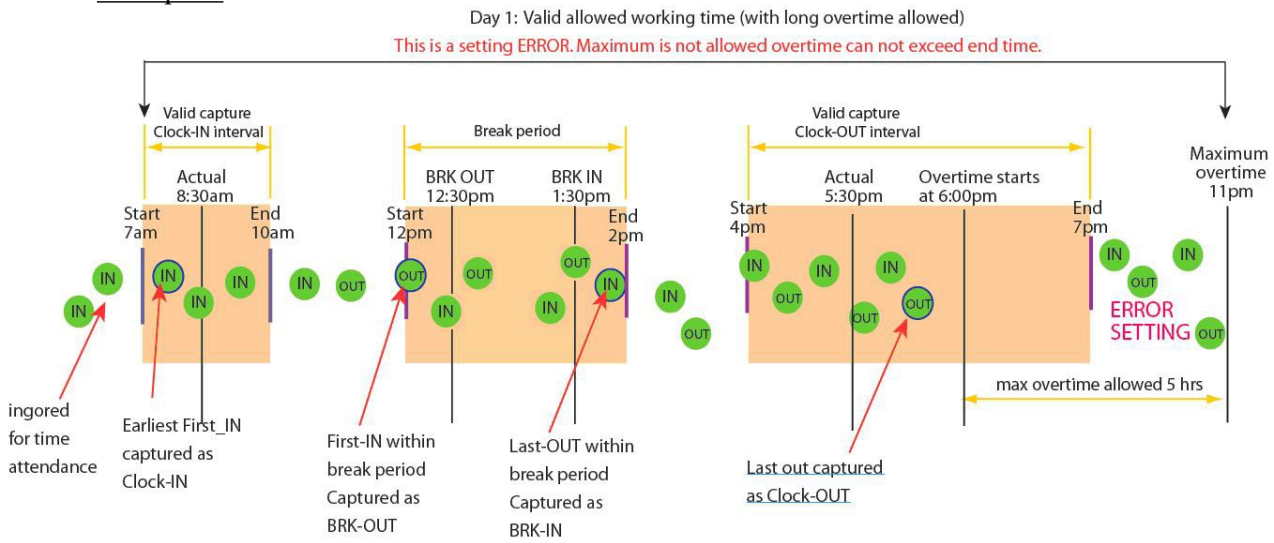
clocking. Example1:



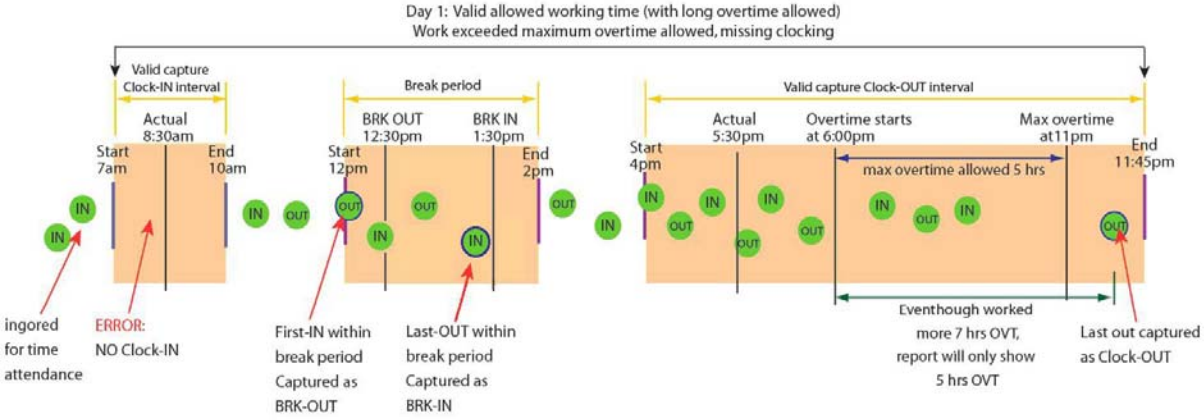
Example2:



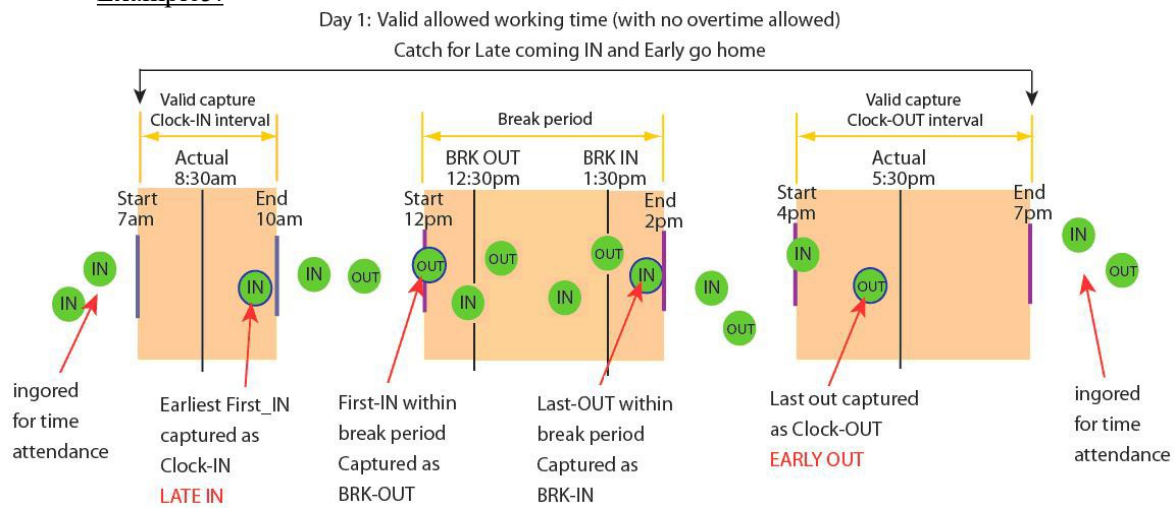
Example3:



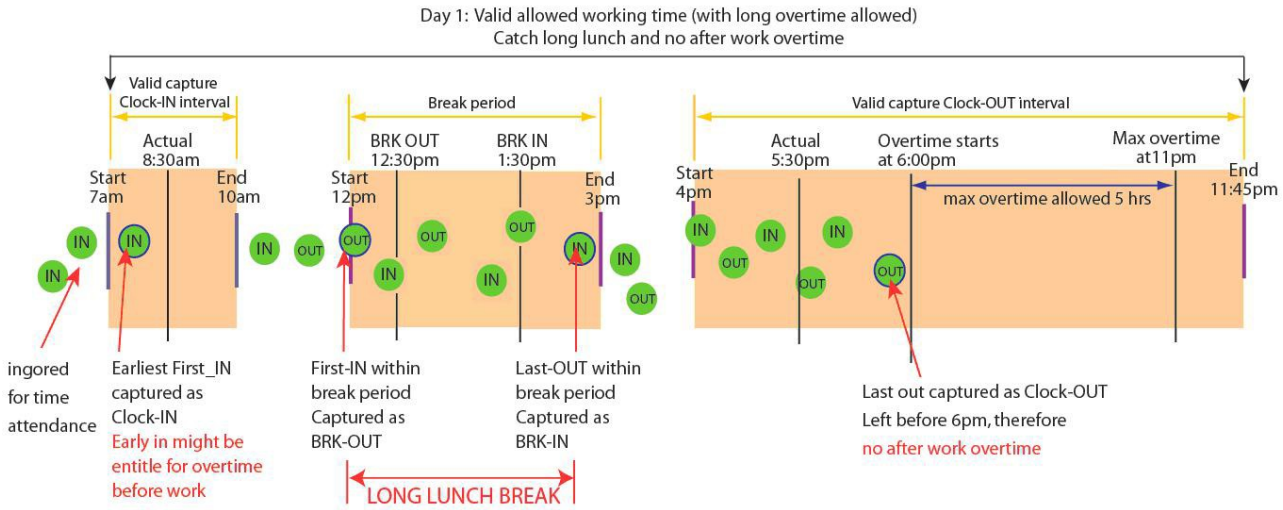
Example4:



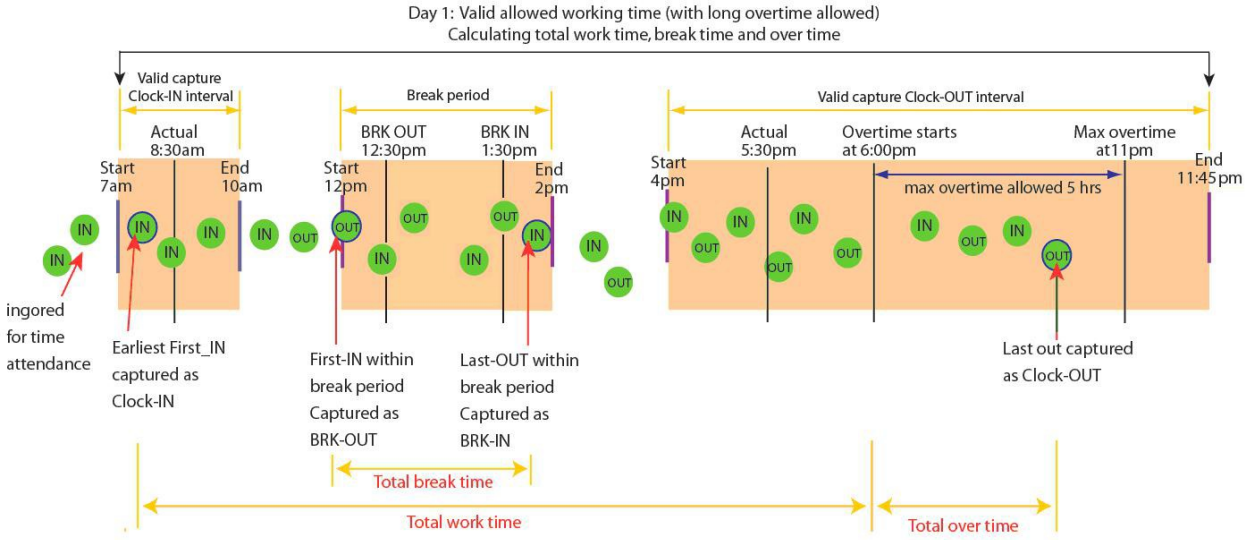
Example5:



Example 6:



Example7:



6.2 Weekly Shift Group

The shift group is to be assigned and combine multiple shifts into a group. Days that are not covered any of the grouped shift will be automatically assumed as "*Rest day*". The objective of shift group is to allow different working hours for different days within a week. For example, Production A define morning working shift for Monday, Tuesday and Wednesday. Production A1 define night working shift for Thursday, Friday and Saturday. When both shifts is combined into shift group Production A all, this user will work morning on Monday, Tuesday, Wednesday and work at night for Thursday and Friday every week.

Each day can only be assigned 1 shift. You can not assign 2 overlapping shift for the same day.

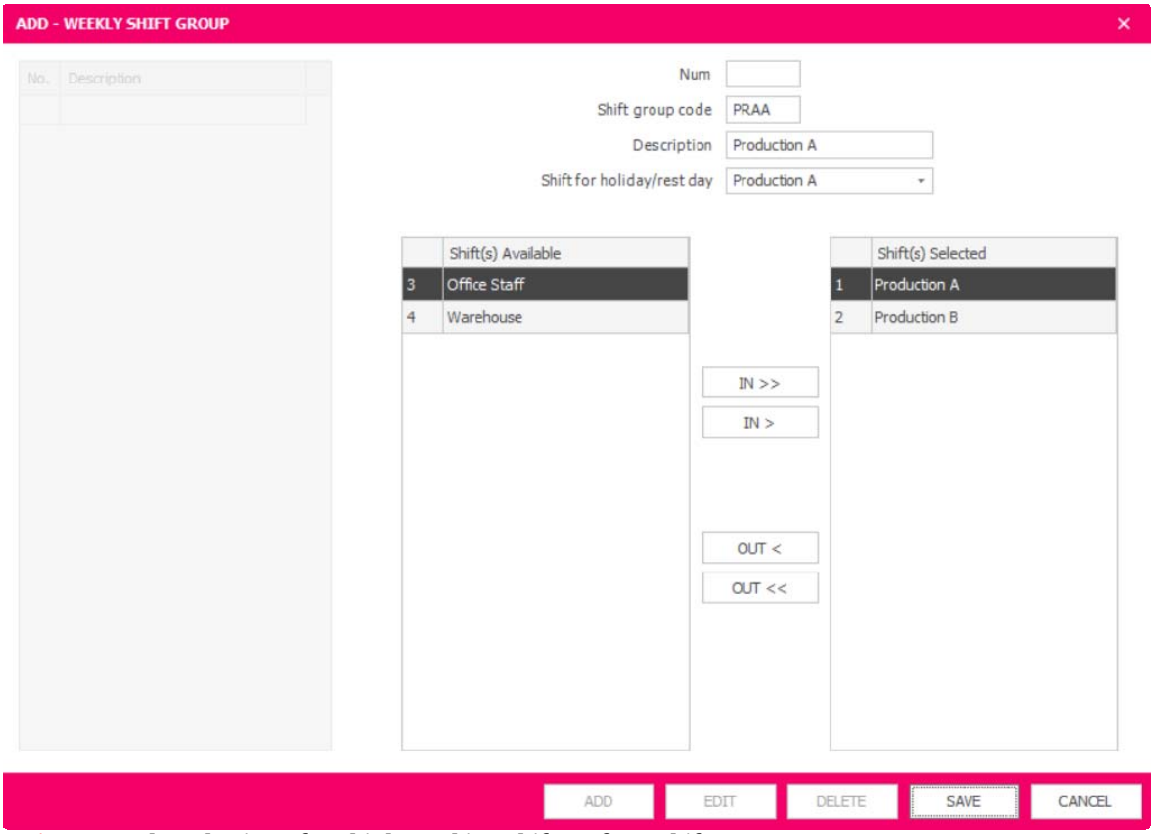


Fig 6.2.2: ***The selection of multiple working shifts to form shift group.***

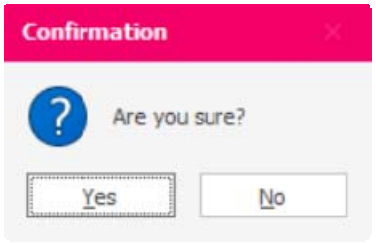


Fig 6.2.3: ***Confirmation***

Adding Shift Group

1) Click on the **ADD** button.
2) All the shifts will be available in the list box. *(Refer Fig 6.2.2)*
3) The number no need to be assign since it is automated. But you also can assign the number manually.
4) Enter the shift group code & description of the shift group.
5) Choose the shift for the holiday or rest day from the dropdown. This is the shift that will be used for calculation is that day is a holiday or rest day.
6) Select the shift in the shift available list and click **IN >>** for in all or **IN >** for in only the selected shift or vice versa.
7) Click on the **Save** button and it will prompt for confirmation.
8) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 6.2.3)*

Edit Shift Group

1) Select the shift group that you want to edit from the left panel list by clicking on it.
2) Once selected, click on the **Edit** button.
3) After editing the necessary fields, click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 6.2.3)*

Delete Shift Group

1) Select the shift group that you want to delete from the left panel list by clicking on it.
2) Once selected, click on the **Delete** button.
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 6.2.3)*

Cancel Shift Group

1) Click on the **Cancel** button to reject any entries while Adding or Editing before.

6.3 Weekly Flexible Shift Group

The flexible shift group is assigned for those the working shifts is flexible for certain period, or change after that. Multiple working shifts can create for 1 day by combines multiple shifts together to form flexible shift group. Due to the working hours got multiple shifts for 1 day, the system will automatically detect and match the working hour regarding the available shift for that day base on the in/out clocking (base on START/END actual working time). The working days that are not covered by any of the flexible shift grouped will be automatically assumed as “Rest Day” and remark as "Shift Mismatch". The objective of flexible shift group is to allow different working hours in 1 day.

For example, the users working shift is morning shift for 1st week, then night shift for 2nd week and afternoon shift for 3rd week and so on. 3 different working hours can be created and group together within the day. Although each user can have different working shift from day to day, but each user only can be assigned for 1 shift per day.

Pre-requisite to build up the flexible shift group:

*a) The grouping of multiple shift groups, the working day must **include whole week**.*

b) The shift group period cannot overlap each other, base on the START/END actual working time.

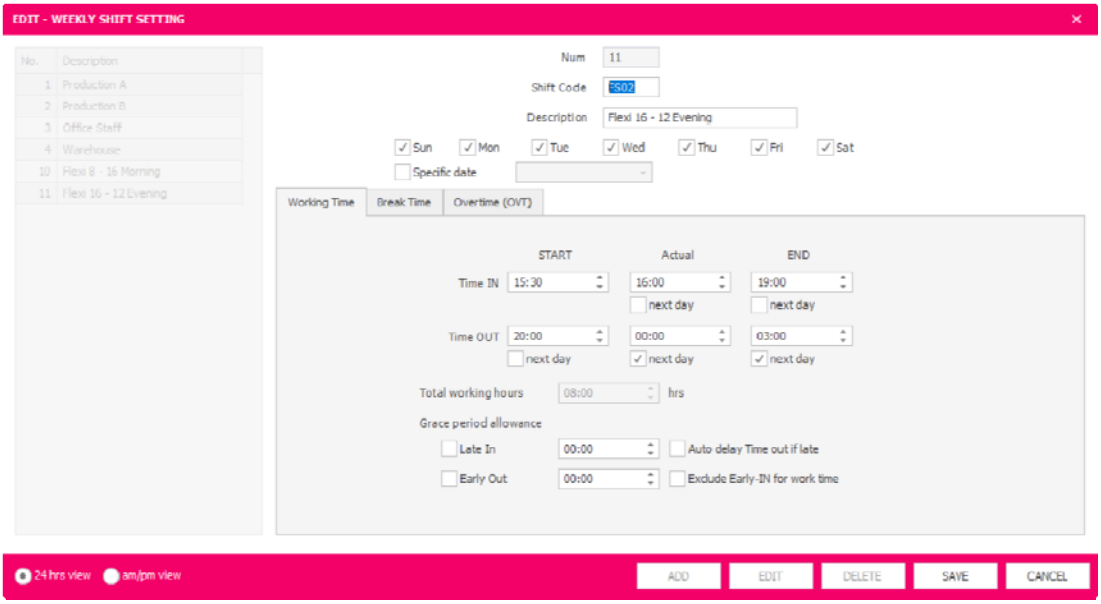


***Fig 6.3.1:** The selection of multiple working shifts to form flexible shift group.*

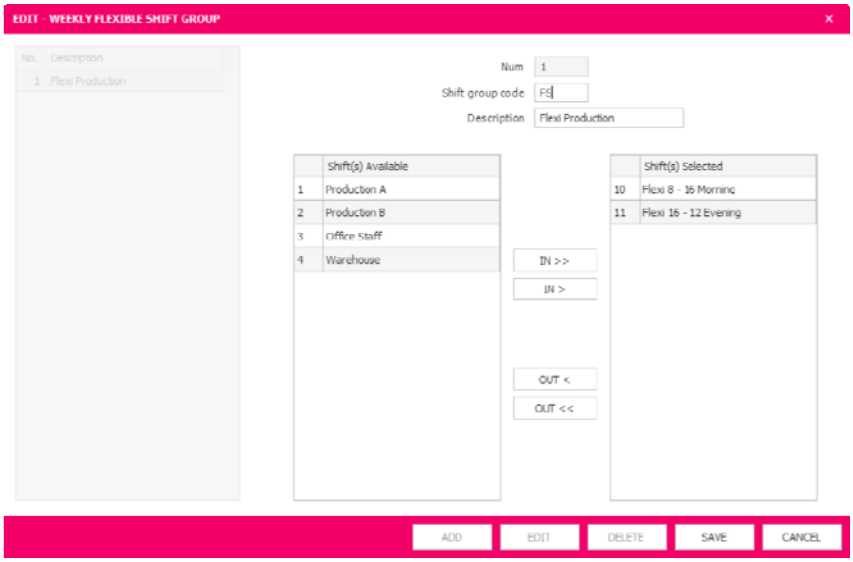


***Fig 6.3.2:** The selection of multiple working shifts to form flexible shift group.*

Fig 6.3.3:
Confirmation

Adding Flexible Shift Group

1) Click on the **ADD** button.
2) All the shifts will be available in the list box. *(Refer Fig 6.3.2)*
3) The number no need to be assign since it is automated. But you also can assign the number manually.
4) Enter the shift group code & description of the shift group.
5) Select the shift in the shift available list and click **IN >>** for in all or **IN >** for in only the selected shift or vice versa.
6) Click on the **Save** button and it will prompt for confirmation.
7) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 6.3.3)*

Edit Flexible Shift Group

1) Select the shift group that you want to edit from the left panel list by clicking on it.
2) Once Selected, click on the **Edit** button.
3) After editing the necessary fields, click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 6.3.3)*

Delete Flexible Shift Group

1) Select the shift group that you want to delete from the left panel list by clicking on it.
2) Once Selected, click on the **Delete** button.
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 6.3.3)*

Cancel Flexible Shift Group

1) Click on the **Cancel** button to reject any entries while Adding or Editing before.

6.4 Yearly Shift Setting

This function is similar with Weekly Shift where it used to set the overnight shift and multiple break time. Time attendance module uses Time In and Time Out interval defined in shift to capture the correct clocking from employee. Employee must clock in or clock out within the time interval defined here to be captured as valid clocking. Any clocking outside the range of interval defined here will NOT be considered as valid clocking. Time attendance module also uses the Actual time defined here to decide where employee come late or go home earlier than they should be

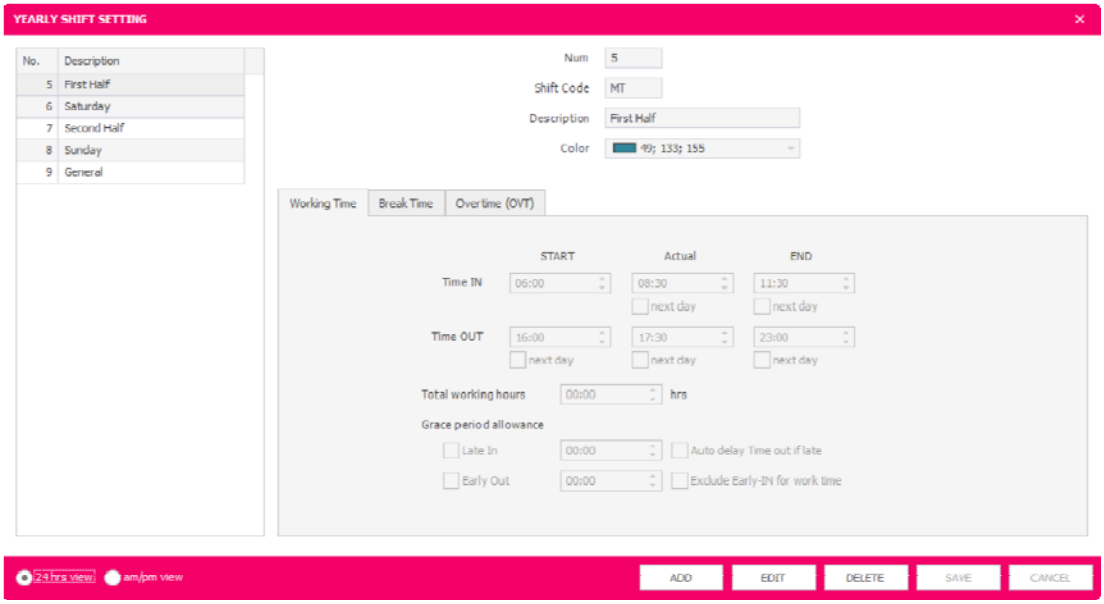


Fig 6.3.1: ***The selection of multiple working shifts to form Yearly shift group.***

Fig 6.3.3:
Confirmation

Adding Yearly Shift Setting

1) Click on the **ADD** button.
2) All the shifts will be available in the list box. *(Refer Fig 6.3.2)*
3) The number no need to be assign since it is automated. But you also can assign the number manually.
4) Enter the shift group code & description of the shift group.
5) Select the shift in the shift available list and click **IN >>** for in all or **IN >** for in only the selected shift or vice versa.
6) Click on the **Save** button and it will prompt for confirmation.
7) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 6.3.3)*

Edit Yearly Shift Setting

1) Select the shift group that you want to edit from the left panel list by clicking on it.
2) Once Selected, click on the **Edit** button.
3) After editing the necessary fields, click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 6.3.3)*

Delete Yearly Shift Setting

1) Select the shift group that you want to delete from the left panel list by clicking on it.
2) Once Selected, click on the **Delete** button.
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 6.3.3)*

Cancel Yearly Shift Setting

2) Click on the **Cancel** button to reject any entries while Adding or Editing before.

6.5 Yearly Shift Group

The yearly shift group is assigned for those the working shifts is flexible for certain period, or change after that. Multiple working shifts can create for 1 day by combines multiple shifts together to form yearly shift group. Due to the working hours got multiple shifts for 1 day, the system will automatically detect and match the working hour regarding the available shift for that day base on the in/out clocking (base on START/END actual working time). The working days that are covered by any of the yearly shift grouped will be automatically assumed as "Work Day" and allow the operator to customize when to be "Rest Day". The objective of yearly shift group is to allow different working hours in 1 day.

For example, the users working shift is morning shift for 1st week, then night shift for 2nd week and afternoon shift for 3rd week and so on. 3 different working hours can be created and group together within the day. Although each user can have different working shift from day to day, but each user only can be assigned for 1 shift per day.

Pre-requisite to build up the yearly shift group:

*a) The grouping of multiple shift groups, the working day must **include whole year**.*
b) The shift group period allow to overlap each other, base on the START/END actual working time.

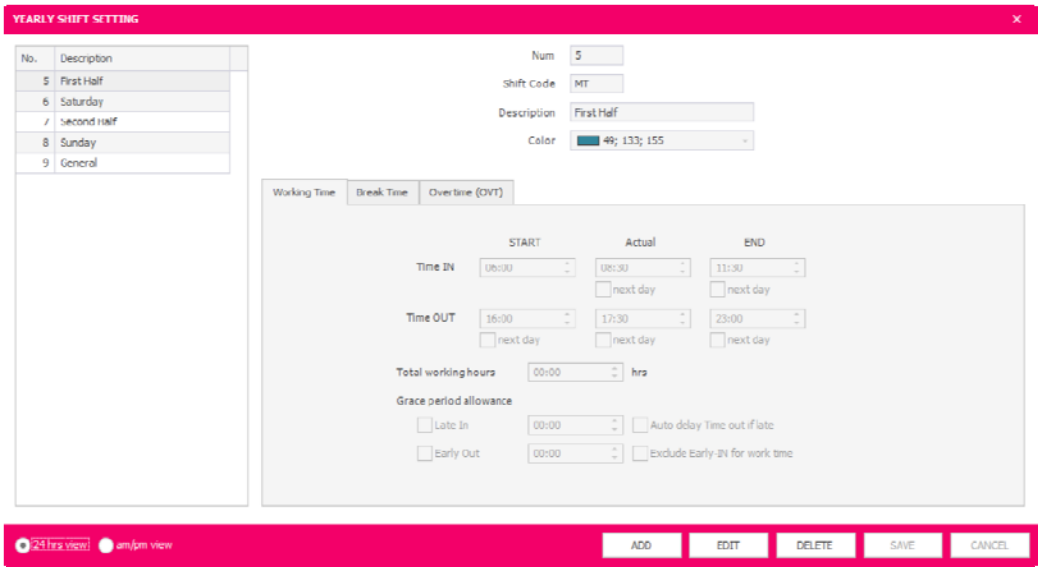


***Fig 6.3.1:** The selection of multiple working shifts to form yearly shift group.*

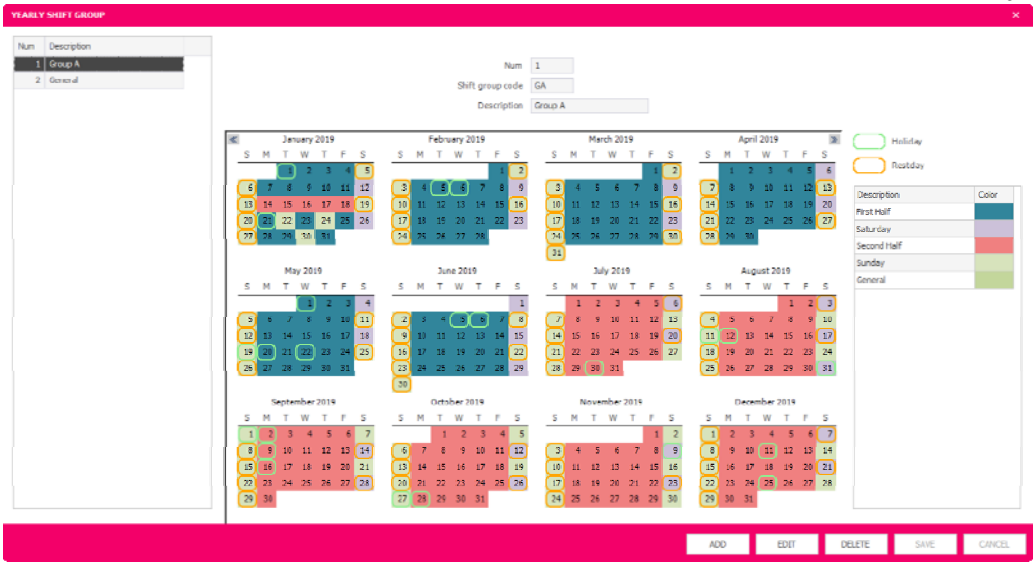


Fig 6.3.2: ***The selection of multiple working shifts to form flexible shift group.***

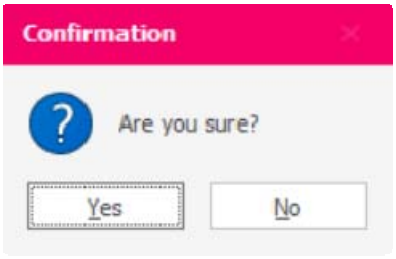


Fig 6.3.3:
Confirmation

Adding Yearly Shift Group

1) Click on the **ADD** button.
2) All the shifts will be available in the list box. *(Refer Fig 6.3.2)*
3) The number no need to be assign since it is automated. But you also can assign the number manually.
4) Enter the shift group code & description of the shift group.
5) Select the shift and click assign shift to date then highlight the date to be assigned, and click apply.
6) Select the date to assign as rest day then click apply.
6) Click on the **Save** button and it will prompt for confirmation.
7) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 6.3.3)*

Edit Flexible Shift Group

1) Select the shift group that you want to edit from the left panel list by clicking on it.
2) Once Selected, click on the **Edit** button.
3) After editing the necessary fields, click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 6.3.3)*

Delete Flexible Shift Group

1) Select the shift group that you want to delete from the left panel list by clicking on it.
2) Once Selected, click on the **Delete** button.
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 6.3.3)*

Cancel Flexible Shift Group

3) Click on the **Cancel** button to reject any entries while Adding or Editing before.

6.6 Attendance Edit

Attendance edit is used to verify that all employees clocking has been properly captured and if any erroneous in the clocking. Operator shall manually amend clocking accordingly after verification with employee. The raw captured clocking data will not be altered. Only attendance data will be amended. It is important for operator to verify and correct all erroneous transaction highlighted in RED color. The reporting module is based on Garbage-In-Garbage-Out. To ensure correct and accurate reporting, all time attendance data must be verified to be correct via Attendance edit before proceed to reporting.

- Attendance edit allow operator to create new attendance transaction.
- Able to filter by types of functions allowed.
- The remark will be update and validate the field automatically. For example, if there is no clocking captured for a work day then automatically updates the remark as "ABSENT". This remark can be edited upon supervisor finding out the actual reason for absent.
- The option fixed record is used for all modified clocking and remarks will not be re-calculated in order to build attendance data.
- The missing clocking will be indicated in red colour.

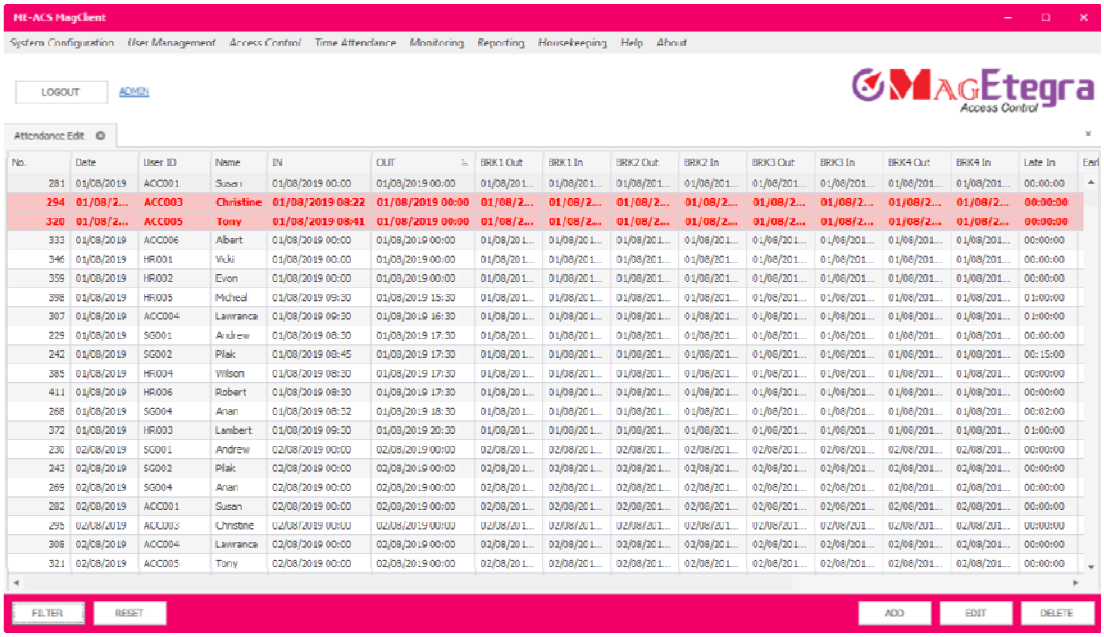


Fig 6.4.1: ***The Attendance Edit is used to edit manually the time clocking for attendance.***

Adding Attendance

This function allows creating attendance records from scratch - meaning that the clocking data does not exist. This might happened if the employee is on an oversea trip and unable to flash card on attendance terminal in office to clock in and out. Attendance records can be manually created for this employee to create consistent reporting.

1) Click on the **ADD** button.
2) New Attendance record window will pop up. *(Refer Fig 6.4.2)*
3) Choose the date in the calendar.
4) Click on the Search user here link.
5) The user screen with list of users will pop up. *(Refer Fig 6.4.4)*
6) Double click on user from the list in order to add the new attendance record.
7) The Shift can be changed from the drop down menu.
8) Able to change the *IN, OUT, BRK1 OUT* and *BRK1 IN* from the Capture clocking.
9) Able to change the Leaves code, duration, remark1, remark2 from the Attendance results.
10) If want to auto generate the settings to assign shift, Click on the *auto generate* according to assigned shift. *(Refer Fig 6.4.5)*
11) If want to see the detailed clocking, Click on see detailed clocking. *(Refer Fig 6.4.6)*
12) If want to see the assigned shift, Click on see assigned shift. *(Refer Fig 6.4.7)*
13) Click on the auto re-calculate result to *auto recalculate* the result.

14) After editing the necessary fields, select “Fixed” field to avoid changes made to be reset when performing build attendance data.
15) Click on the **Save** button and it will prompt for confirmation.
16) Click on Yes button to save the changes or **No** button to reject the changes. *(Refer Fig 6.4.9)*

Edit Attendance

This function is used to correct error highlight in Red. Common error detected is missing clocking time. Operator will need to call up the employee and confirm clocking time. Operator can then manually enter this clocking time into the attendance record to ensure correct reporting later on.

1) Select the user that you want to edit from the Attendance Edit tab by clicking on it
2) Once selected, click on the **Edit** button.
3) After editing the necessary fields, select “Fixed” field to avoid changes made to be reset when performing build attendance data.
4) Click on the **Save** button. It will prompt for confirmation.
5) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 6.4.9)*

Delete Attendance

1) Select the user that you want to delete from the Attendance Edit tab by clicking on it.
2) Once Selected, click on the **Delete** button.
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 6.4.9)*

Cancel Attendance

1) Click on the **Cancel** button to reject any entries while Adding or Editing before.

***Fig 6.4.2:* The New Attendance Record.**

Fig 6.4.3: ***To edit the record manually.***

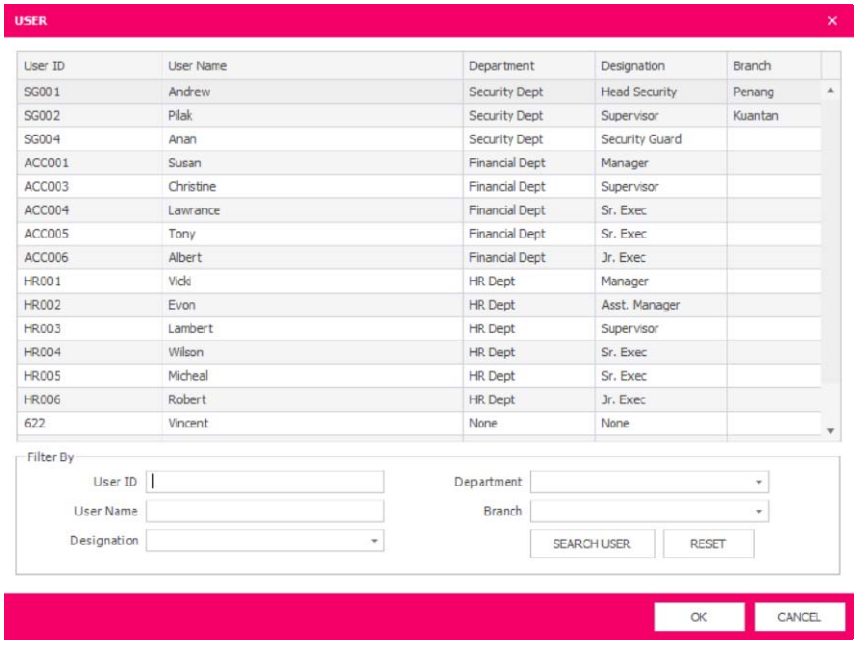


Fig 6.4.4: ***The users can be filtered out regarding the selected fields.***

Fig 6.4.5: ***Confirmation for auto generation.***

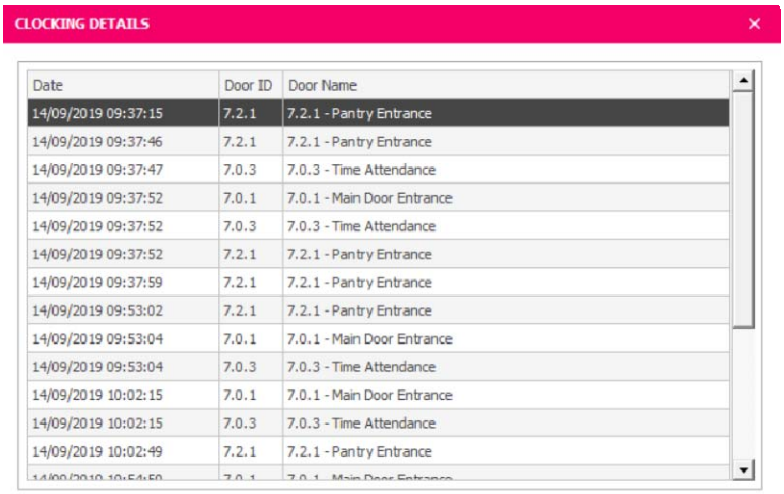


Fig 6.4.6: ***The clocking details.***

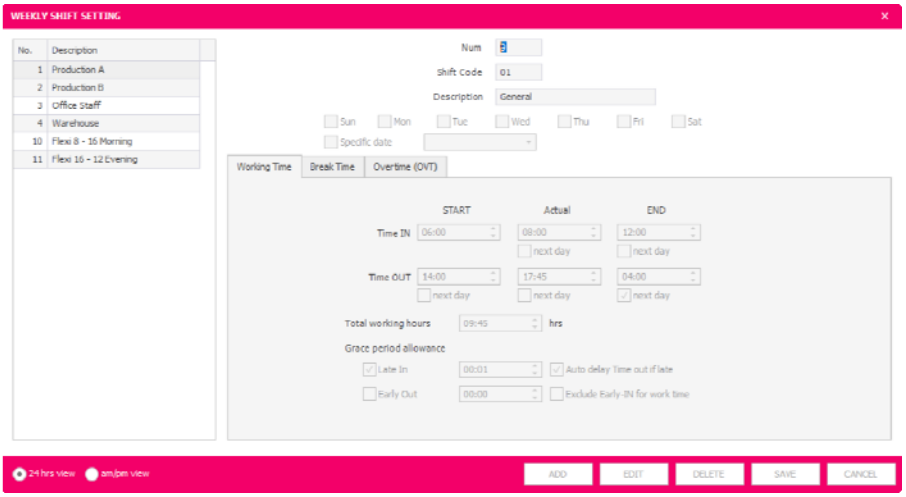


Fig 6.4.7: ***The shift settings.***

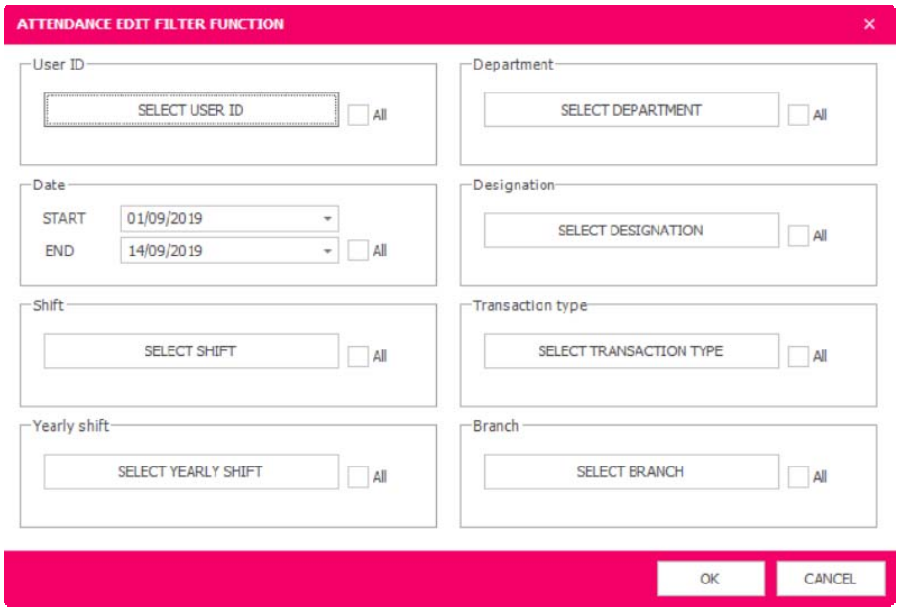


Fig 6.4.8: ***Attendance Edit Filter Function.***

Fig 6.4.9: ***Confirmation.***

6.7 Free Shift Setting

This feature Free-Shift will not be capturing break time as the FS will only keep track on the user working time. The FS report wont be show in the normal report as they have their own standard report. The feature itself only have 2 type of Reports whereby is 'Daily Time Attendance' and 'Time Card Report'. FS will not be supporting import/export time attendance feature. The only method the operator can be export it via Print Preview. FS report also able to use the attendance edit for editing. This feature Free-Shift is only available in all Professional version and not available for Lite version.

This Free Shift is not suitable for door access usage

The following will be the logic diagram for how does the 'F' key works in this Free-Shift.

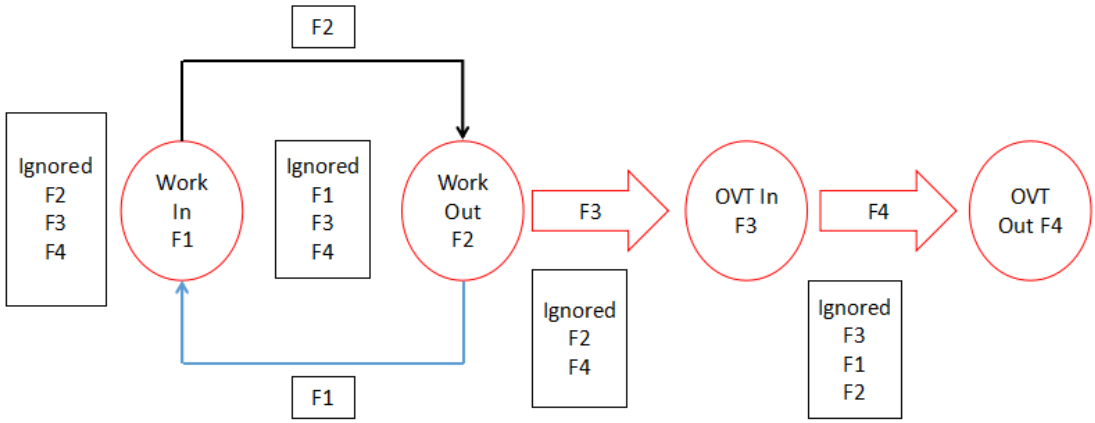


Fig 6.7.1: ***The logic diagram for Free Shift.***

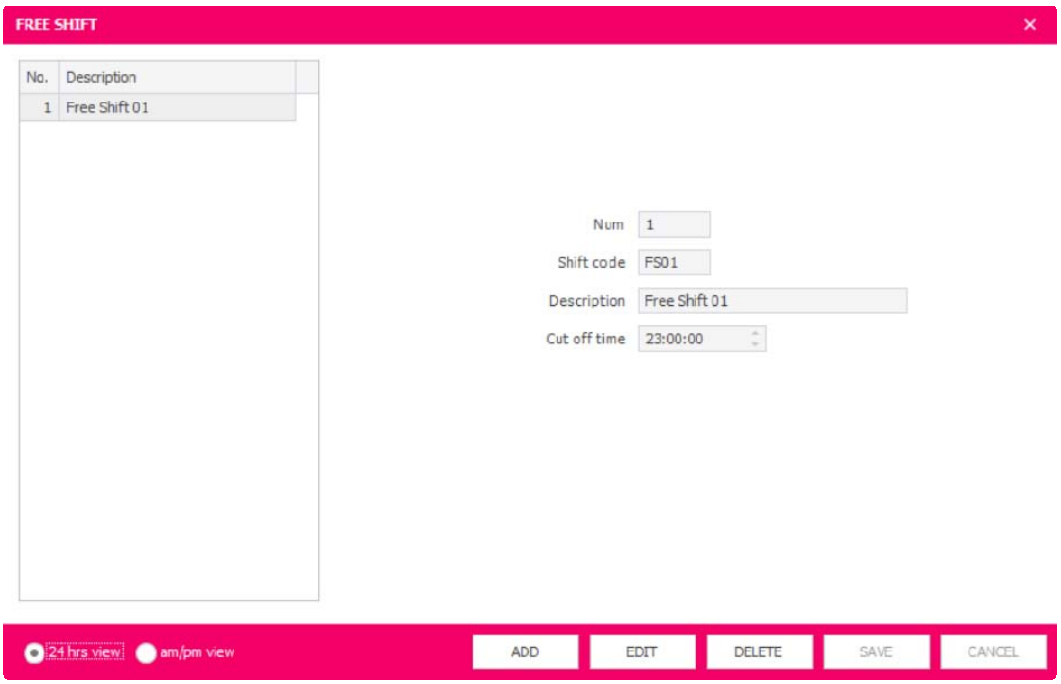


Fig 6.7.2: ***The Free Shift Setting.***

Fig 6.7.2: ***The Free Shift Setting.***

Adding Shift

1) Click on the **ADD** button.
2) The number no need to be assign since it is automated. But you also can assign the number manually.
3) Enter the shift code and the description.
4) Assign the Cut Off time
5) Click on the **Save** button. It will prompt for confirmation.
6) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 6.7.3)*

Editing Shift

1) Select the shift that you want to edit from the left panel list by clicking on it
2) Once selected, click on the **Edit** button.
3) After editing the necessary fields, click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 6.7.3)*

Delete Shift

1) Select the holiday that you want to delete from the left panel list by clicking on it.
2) Once Selected, click on the **Delete** button.
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 6.7.3)*

Cancel Shift

1) Click on the **Cancel** button to reject any entries while Adding or Editing before

6.8 Attendance Edit - Free Shift

Attendance edit is used to verify that all employees clocking has been properly captured and if any erroneous in the clocking. Operator shall manually amend clocking accordingly after verification with employee. The raw captured clocking data will not be altered. Only attendance data will be amended. It is important for operator to verify and correct all erroneous transaction highlighted in RED color. The reporting module is based on Garbage-In-Garbage-Out. To ensure correct and accurate reporting, all time attendance data must be verified to be correct via Attendance edit before proceed to reporting.

- Attendance edit allow operator to create new attendance transaction.
- Able to filter by types of functions allowed.
- The remark will be update and validate the field automatically. For example, if there is no clocking captured for a work day then automatically updates the remark as "ABSENT". This remark can be edited upon supervisor finding out the actual reason for absent.
- The option fixed record is used for all modified clocking and remarks will not be re-calculated in order to build attendance data.
- The missing clocking will be indicated in red colour.

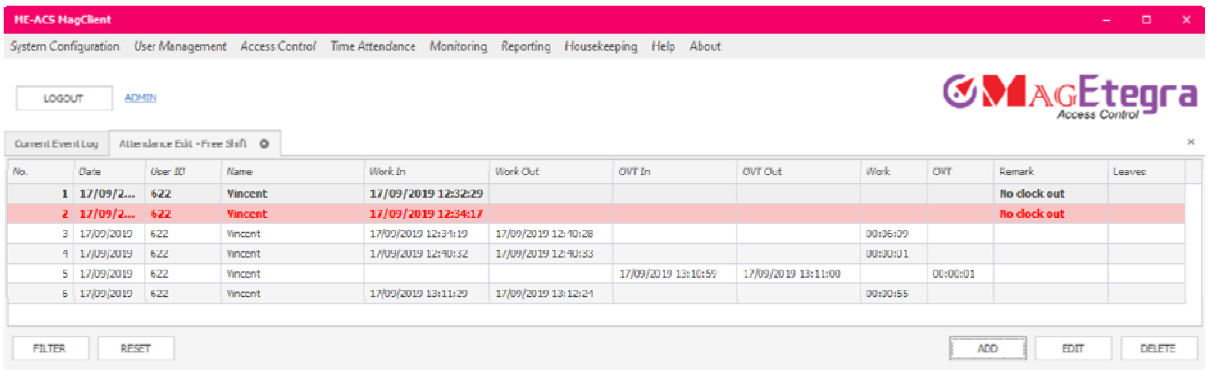


Fig 6.4.1: ***The Attendance Edit is used to edit manually the time clocking for attendance.***

Adding Attendance

This function allows creating attendance records from scratch - meaning that the clocking data does not exist. This might happened if the employee is on an oversea trip and unable to flash card on attendance terminal in office to clock in and out. Attendance records can be manually created for this employee to create consistent reporting.

1) Click on the **ADD** button.
2) New Attendance record window will pop up. *(Refer Fig 6.4.2)*
3) Choose the date in the calendar.
4) Click on the Search user here link.
5) The user screen with list of users will pop up. *(Refer Fig 6.4.4)*
6) Double click on user from the list in order to add the new attendance record.
7) The Shift can be changed from the drop down menu.
8) Able to change the *IN, OUT, BRK1 OUT* and *BRK1 IN* from the Capture clocking.
9) Able to change the Leaves code, duration, remark1, remark2 from the Attendance results.
10) If want to auto generate the settings to assign shift, Click on the *auto generate* according to assigned shift. *(Refer Fig 6.4.5)*
11) If want to see the detailed clocking, Click on see detailed clocking. *(Refer Fig 6.4.6)*
12) If want to see the assigned shift, Click on see assigned shift. *(Refer Fig 6.4.7)*
13) Click on the auto re-calculate result to *auto recalculate* the result.
14) After editing the necessary fields, select “Fixed” field to avoid changes made to be reset when performing build attendance data.
15) Click on the **Save** button and it will prompt for confirmation.
16) Click on Yes button to save the changes or **No** button to reject the changes. *(Refer Fig 6.4.9)*

Edit Attendance

This function is used to correct error highlight in Red. Common error detected is missing clocking time. Operator will need to call up the employee and confirm clocking time. Operator can then manually enter this clocking time into the attendance record to ensure correct reporting later on.

1) Select the user that you want to edit from the Attendance Edit tab by clicking on it
2) Once selected, click on the **Edit** button.
3) After editing the necessary fields, select "Fixed" field to avoid changes made to be reset when performing build attendance data.
4) Click on the **Save** button. It will prompt for confirmation.
5) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 6.4.9)*

Delete Attendance

1) Select the user that you want to delete from the Attendance Edit tab by clicking on it.
2) Once Selected, click on the **Delete** button.
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 6.4.9)*

Cancel Attendance

1) Click on the **Cancel** button to reject any entries while Adding or Editing before.

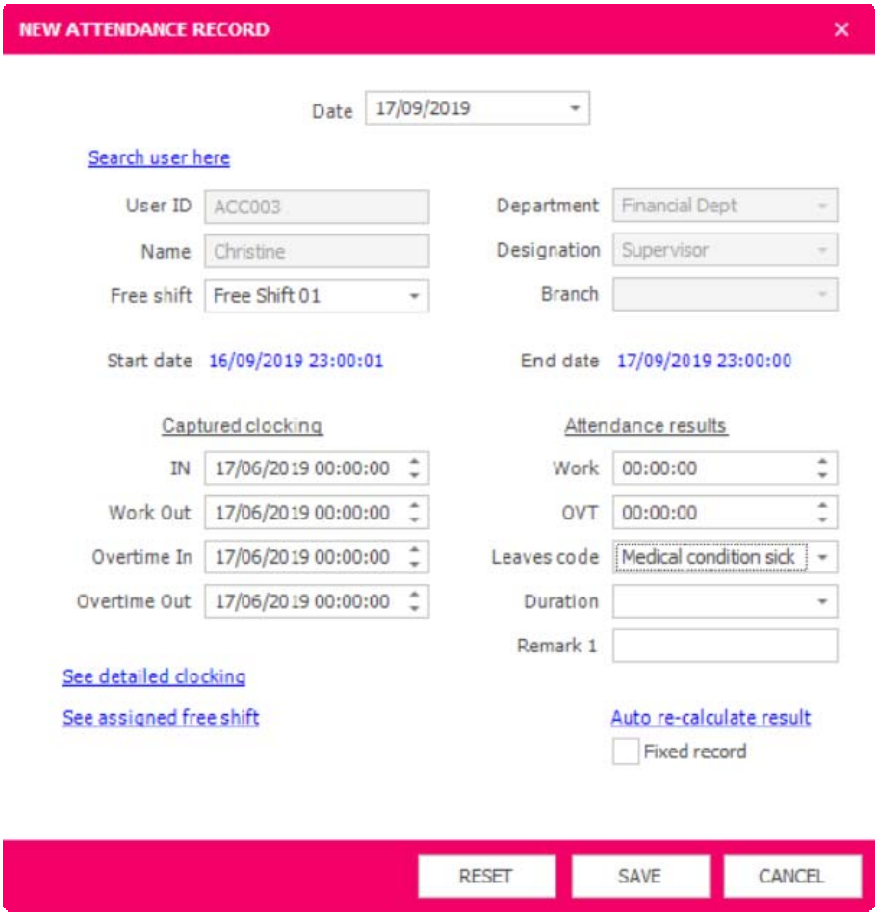


***Fig 6.4.2:* The New Attendance Record.**

Fig 6.4.3: ***To edit the record manually.***

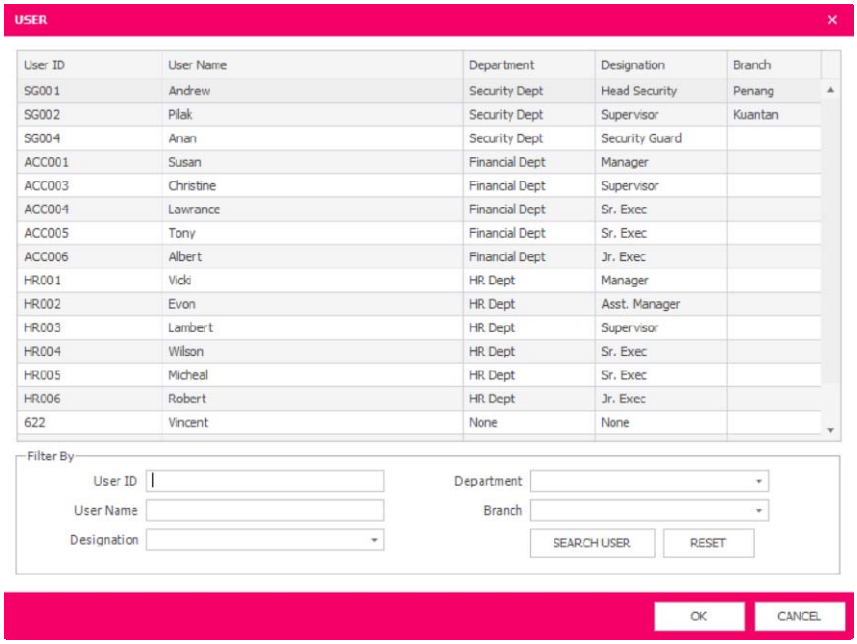


Fig 6.4.4: ***The users can be filtered out regarding the selected fields.***

Fig 6.4.5: ***Confirmation for auto generation.***

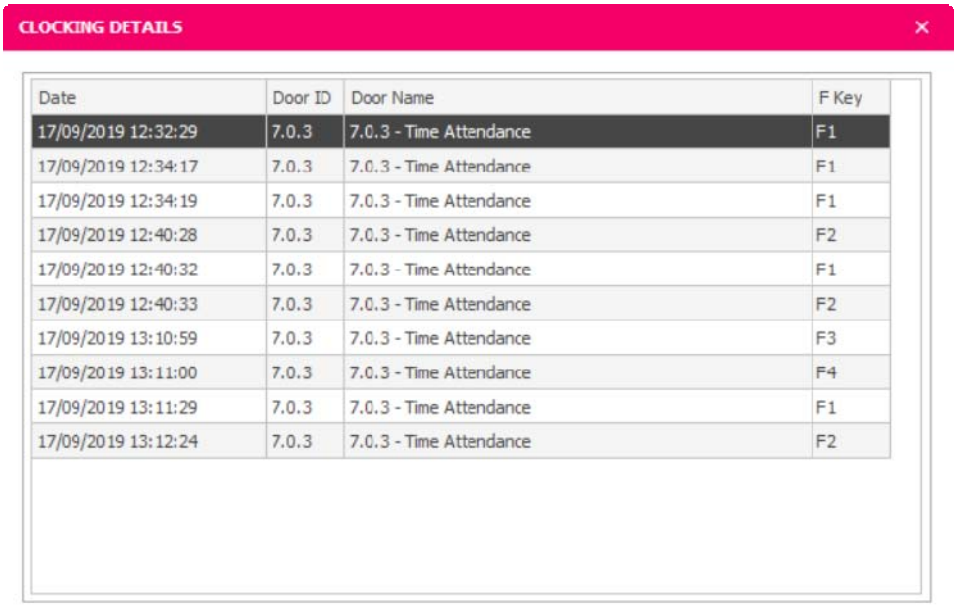


Fig 6.4.6: ***The clocking details.***

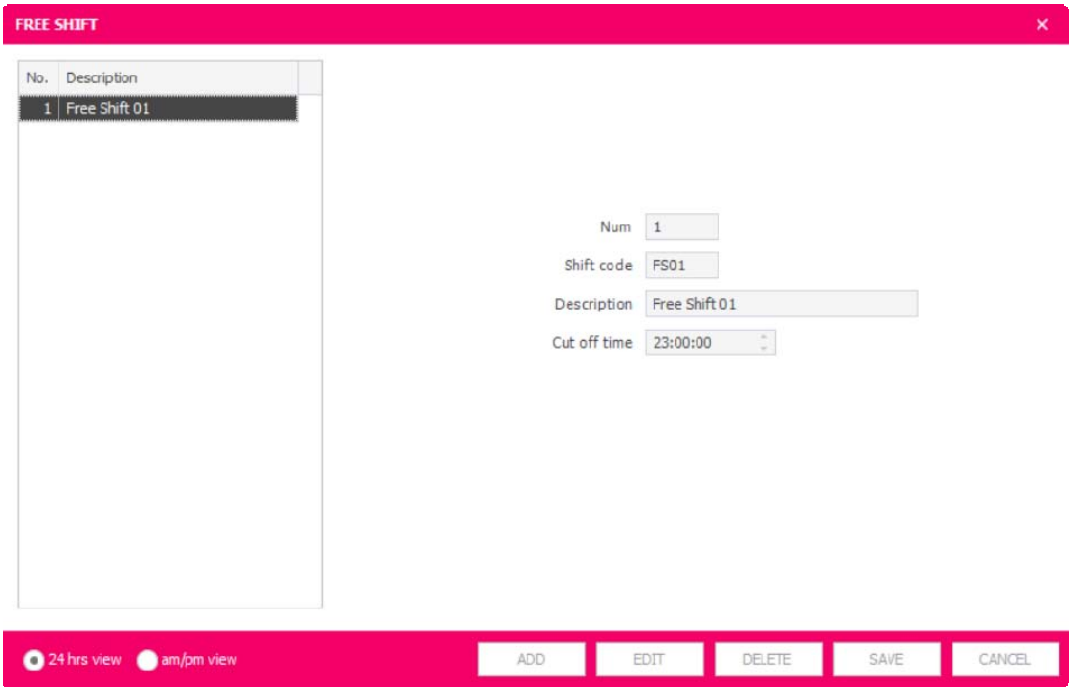


Fig 6.4.7: ***The shift settings.***

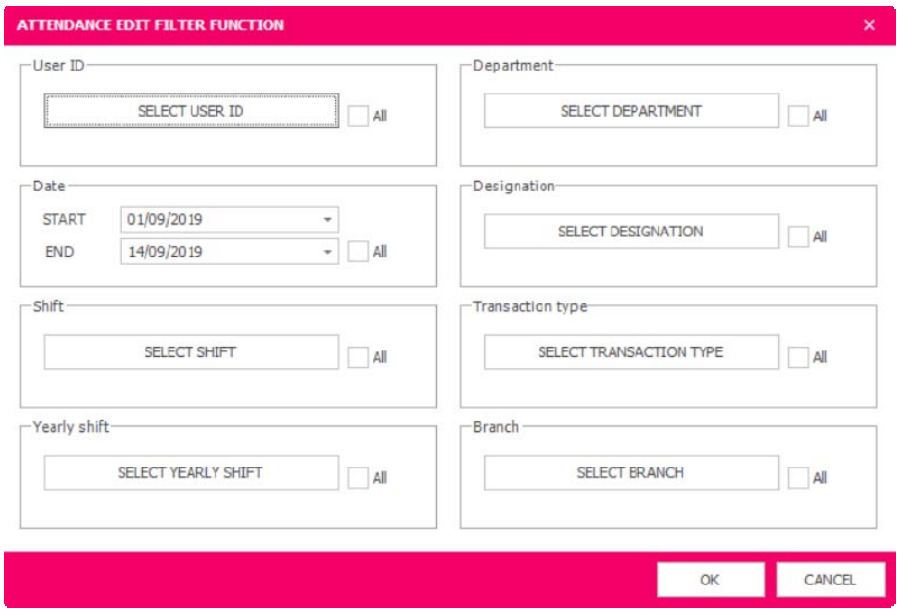


Fig 6.4.8: ***Attendance Edit Filter Function.***

Fig 6.4.9: ***Confirmation.***

6.8 Attendance Settings

This **F-keys definition is** define the Duty based clocking method.

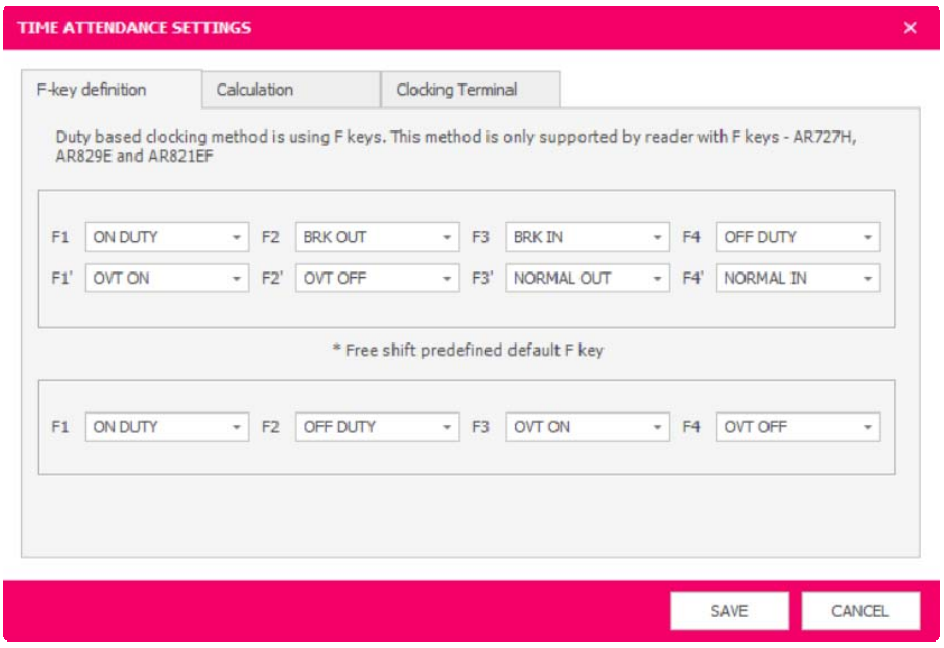


Fig 6.5.1: ***F-key definition.***

Choose the F1, F2, F3, F4, F1', F2', F3', F4' duty based clocking from the dropdown menu and click on SAVE button.

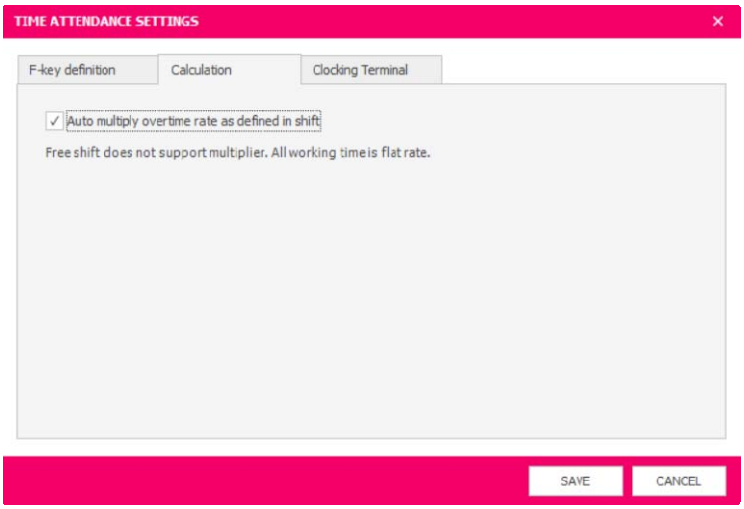


Fig 6.5.2: ***Overtime rate calculation.***

Tick or check the checkbox for auto multiply overtime rate as defined in Shift and click on **SAVE** button.

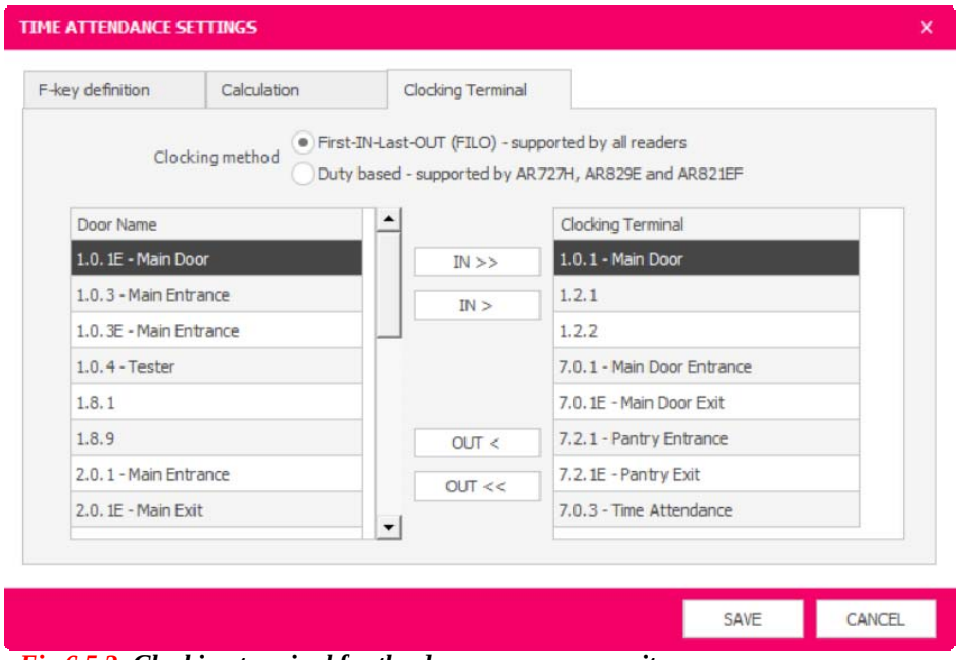


Fig 6.5.3: ***Clocking terminal for the door or access security.***

Choose the clocking method either *FILO or Duty based* by clicking the radio button. Select the door name that will be assign as a clocking terminal and click on **SAVE** button.

6.9 Leave Type

This is to define type of leaves generally "paid leave" and "unpaid leave".

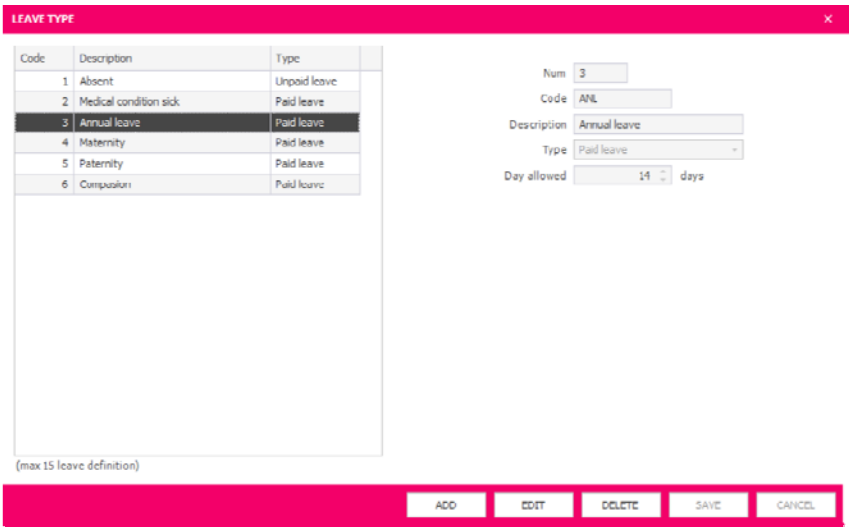


Fig 6.6.1: ***The type of leaves and the limit of days are allowed.***

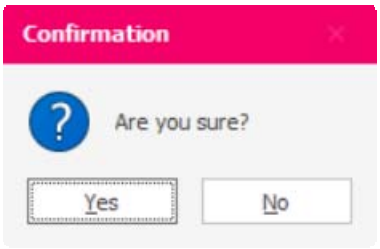


Fig 6.6.2: ***Confirmation.***

Adding Leave Type

1) Click on the **ADD** button.
2) The number no need to be assign since it is automated.
3) Enter the code, description and the number of days allowed.
4) Select the leave type from the type dropdown menu.
5) Click on the **Save** button and it will prompt for confirmation.
6) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 6.6.2)*

Edit Leave Type

1) Select the leave type that you want to edit from the left panel leave type list by clicking on it
2) Once Selected, click on the **Edit** button.
3) After editing the necessary fields, click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 6.6.2)*

Delete Leave Type

1) Select the leave type that you want to delete from the left panel leave type list by clicking on it
2) Once Selected, click on the **Delete** button.
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** to reject the changes. *(Refer Fig 6.6.2)*

Cancel Leave Type

1) Click on the **Cancel** button to reject any entries while Adding or Editing before.

6.10 Advance Leave

This is to be able to assign leave for an employee in advance. For example, John can apply for annual leave on
12, 13, 14 September one month in advance. When 12, 13, 14 September arrives, there will not be any clocking from John. System will recognize that John is on annual leave instead of absent from work. System will highlight the attendance transaction as error (RED) if there is clocking captured from John on 12, 13 and
14 September. Operator will need to call up John to check if he decided cancel the leaves and came for work or someone is tampering with John's proximity card.

- The operator will be able to assign the leave in advance. The time attendance will automatically take the leave assigned into consideration when building attendance data.
- The advance leave will be able to indicate how many hours employee take leave. The filtering will includes the date range, duration and leave type filtering.
- By default there will be a column on the left to show only the leaves that have not elapsed yet. Shifts that have elapsed will be search using filtering.

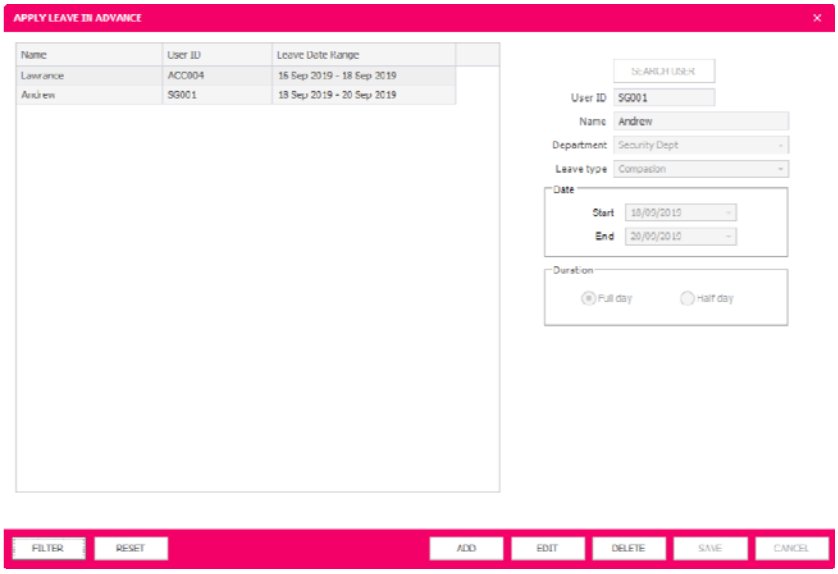


Fig 6.7.1: ***The advance leaves.***

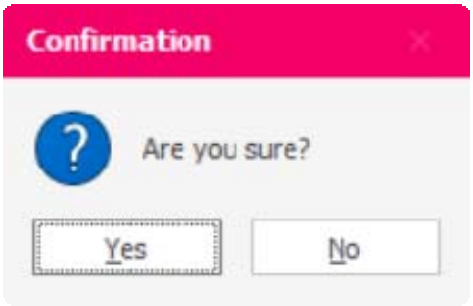


Fig 6.7.2: ***Confirmation.***

Adding Advance Leave

1) Click on the **ADD** button.
2) Enter the User ID, User num and Name. Select the Department and Leave type from the type dropdown menu.
3) Choose the start date and end date for the advance leave.
4) Choose the duration Full day or Half day from the radio button.
5) Click **Save** button and it will prompt for confirmation.
6) Click on **Yes** button to save the changes or **No** button to reject the changes. *(Refer Fig 6.7.2)*

Edit Advance Leave

1) Select the advance leave that you want to edit from the left panel user list by clicking on it.
2) Once selected, click on the **Edit** button.
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to confirm accept the changes or **No** to reject the changes. *(Refer Fig 6.7.2)*

Delete Advance Leave

1) Select the advance leave that you want to edit from the left panel user list by clicking on it.
2) Once selected, click on the **Delete** button.
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes (Refer Fig 6.7.2)

Cancel Advance Leave

1) Click on the **Cancel** button to reject any entries while Adding or Editing before.

Attendance edit will show RED error if there is clocking activity during leave days. Operator will need to check with employee why there is still badging activity on the day that they are supposed to be on leave.

6.11 Build Database

This function is to generate time attendance data within specified date range. Calculations will be based on latest settings and shift schedule. All previous attendance records will be overwritten. All existing attendance transactions marked "Fixed" shall not be updated and remained as it is. Build attendance data will automatically skip user profile that does not have any shift/shift group assigned to it.

Time attendance data will not be available for reporting before build database is executed. Therefore to achieve accurate reports, you must perform build database prior to viewing reports. After building attendance data, operator needs to verify all error calculated attendance transaction (highlighted in RED color) via Attendance Edit.

Choose the start date and end date to build the attendance data.
Click **OK** button to start build the attendance data.

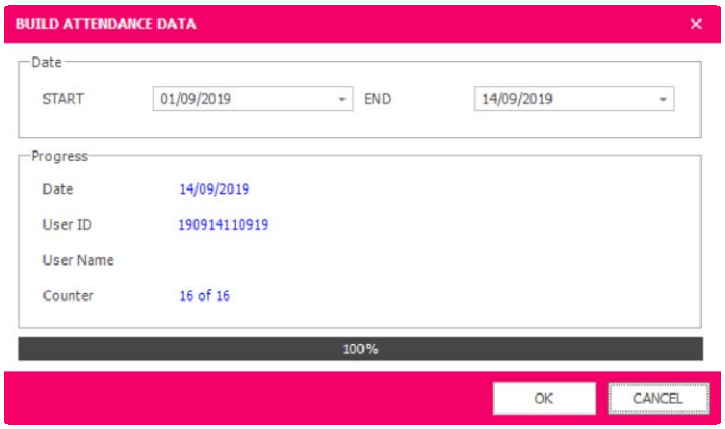


***Fig 6.8.2:* The process of building database is running.**

The attendance data being built. All user profile that is not assigned with a shift will be skipped automatically.

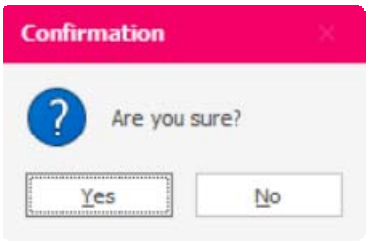
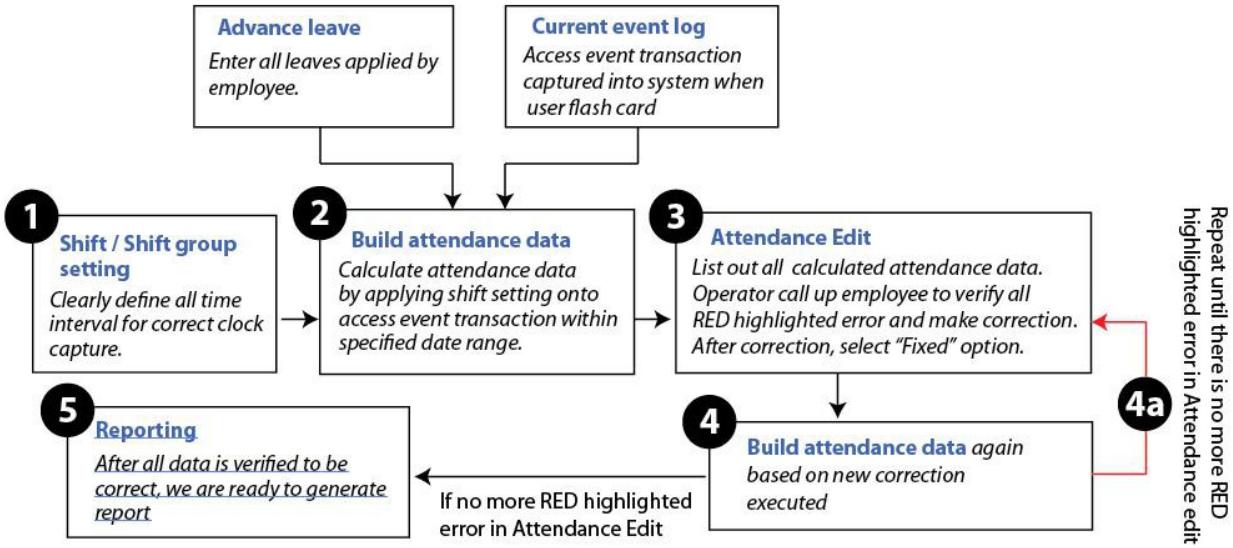


***Fig 6.8.3:* The attendance database is build successful.**

Upon completion of attendance data building, build attendance data successfully will be prompt. *(Refer 6.8.3)*. Then click OK to close it.

6.12 Time attendance summarized process flow

Following is the process flow to illustrate Standard Operating Procedure (SOP) to process time attendance.



7) Monitoring

The Monitoring Module is responsible for managing the monitoring status for Current Event Log, Alarm Event Log, Camera Commander, Door Commander, In/Out Monitoring, User Tracking, Ticketing Terminal , Area Control & E- map Control. All this functions can integrated each other under 1 control system and make access controlled process become more secure and easy, especially the door commander, camera commander, In/Out monitoring, Area Control, I/O monitoring can be integrated ***with E-MAP*** *function.*

7.1 Current Event Log

To show normal and error transaction for current day. Current event log by default will only show today transactions. Flexible filter function allow operator to efficiently search for pass records to investigate security breach.

The fields that will be displayed in the user list tab are User ID, User Num, Name, Card num1, Card num2, Department, Designation, Branch, Shift, shift group, access mode, time zone, floor group, door group, pin change, anti-passback, holiday, skip FP, car id, legal id, address, tel, mobile, email, gender, birth date, start date, special remark, guard patrol, expiry ending date, expiry starting date, alias, user level and advance.

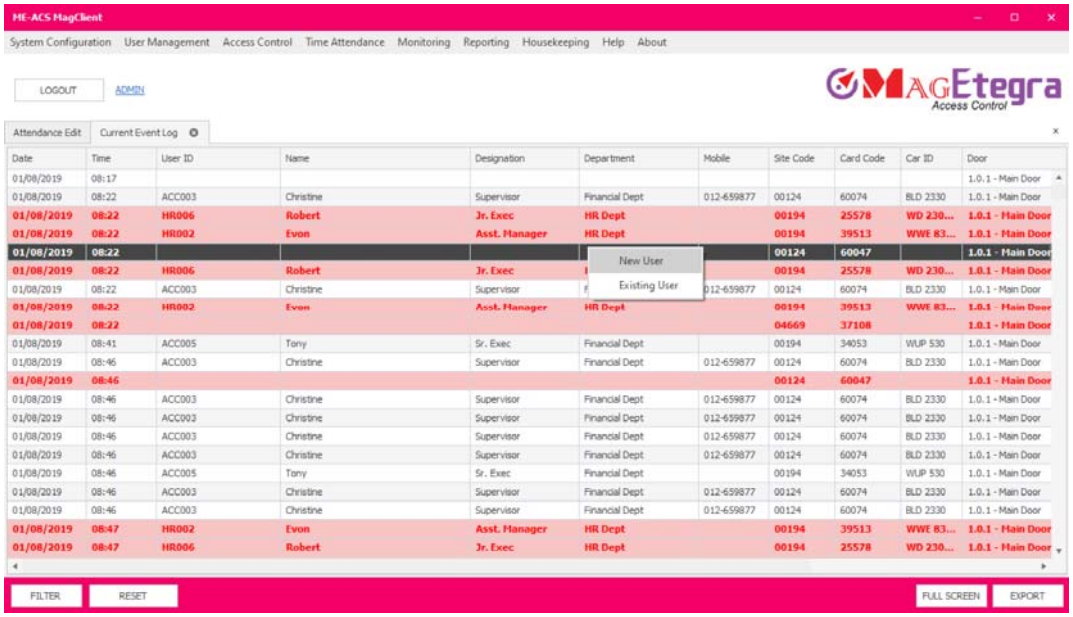


Fig 7.1.1: ***Current event log.***

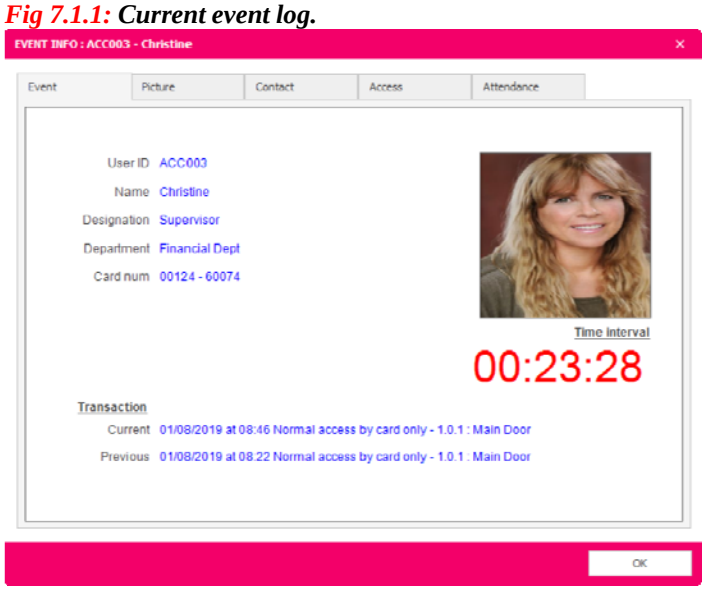


Fig 7.1.2: ***Event info.***

Double-click one of the transaction events in the Current Event Log *(Refer Fig 7.1.1).* It will pop up summary of events info for selected event. *(Refer Fig 7.1.2).* Click on **OK** button to close.

Right-click and select New User to add new user *(Refer Fig 7.1.1).* Right-click and select Existing user to search for existing user. Then fill in the user information of User Profile.

7.2 Alarm Event Log

Displays all the alarm event reported by hardware. Forced entry, door opened too long; are situations that are captured as alarm event. Captured picture and recorded video during alarm can be directly reviewed from alarm event log without the hassle of searching in DVR for playback. This helps guards to response quicker during an alarmed event. Supervisor can review video / picture evidence captured and acknowledgement can be entered into each detected alarm to verify and counter future alarm event.

The fields that will be displayed in the user list tab are User ID, User Num, Name, Card num1, Card num2, Department, Designation, Branch, Shift, shift group, access mode, time zone, floor group, door group, pin change, anti-passback, holiday, skip FP, car id, legal id, address, tel, mobile, email,gender, birth date, start date, special remark, guard patrol, expiry ending date, expiry starting date, alias, user level and advance.

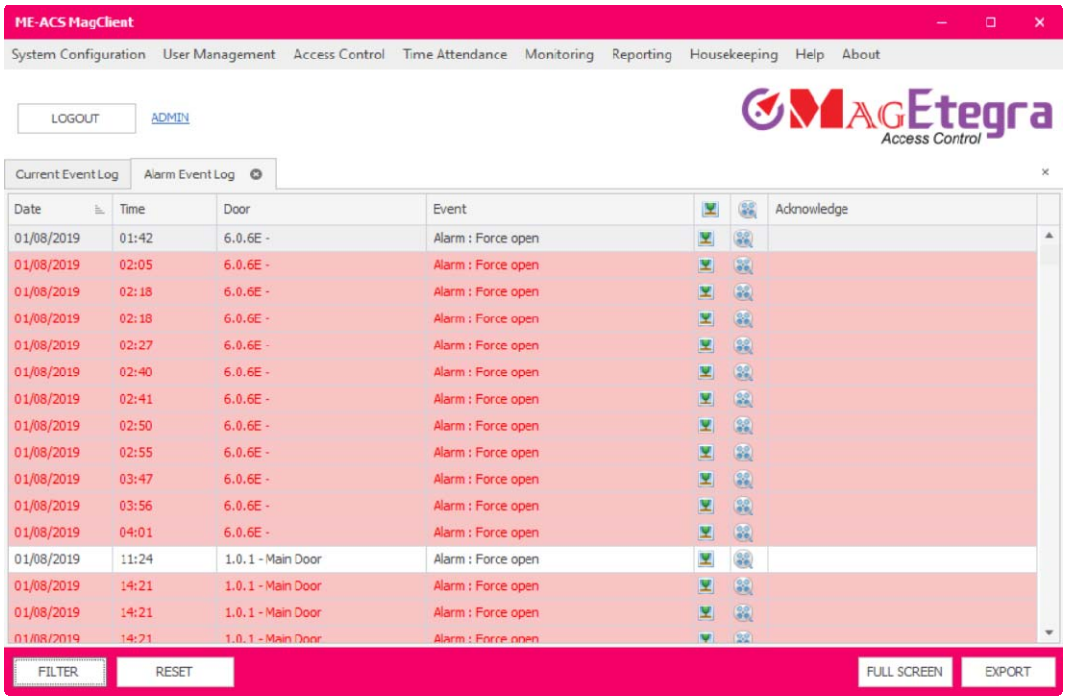


***Fig 7.2.1:* The alarm event log.**

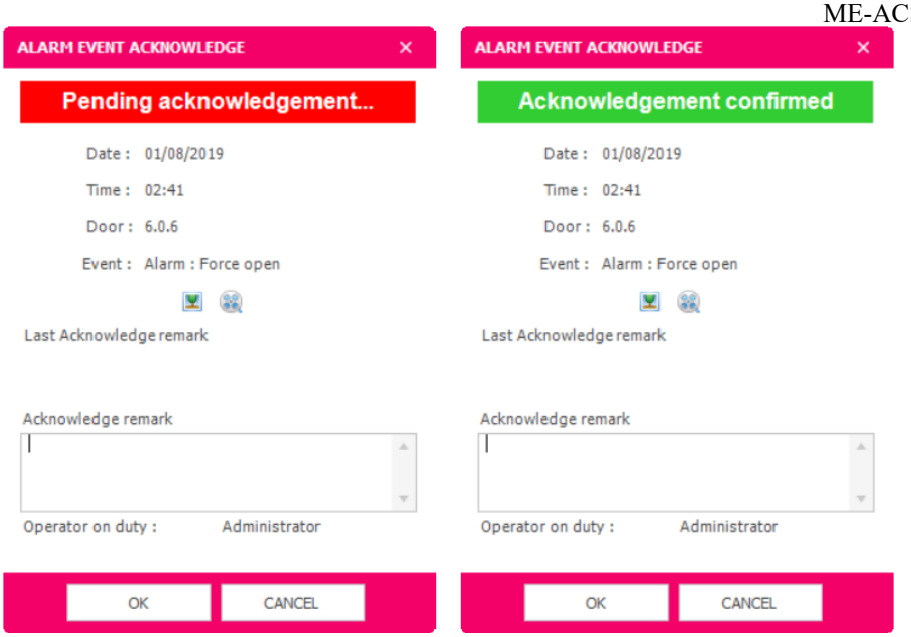


***Fig 7.2.2:* The acknowledgement of alarm event..**

For Acknowledged Transaction (Grayed background)

1) Double click on the transaction which is background grayed colour in the Alarm Event Log. *(Refer Fig7.2.1)*
2) It will pop up Alarm event acknowledgement window with pending acknowledgement title. *(Refer Fig7.1.2)*
3) This will show the last event reported and last acknowledgement done.

For Unacknowledged Transaction (Red background)

1) Double click on the transaction which is background red colour in the Alarm Event Log. *(Refer Fig 7.1.1).*
2) It will pop up Alarm event acknowledgement window. *(Refer Fig 7.1.3)*
3) This will show the last event reported and need to be acknowledged.
4) This transaction will be changed status to the grayed background colour upon successful acknowledgement.

For Picture

1) Click on the Picture Logo  of a particular transaction. Picture captured will be displayed in a pop up window

***Fig 7.2.4:* The camera is capture picture during alarm trigger, and the picture can be reviewed by click on the PICTURE LOGO.**

FOR VIDEO

1) Click on the Video Logo  of a particular transaction.

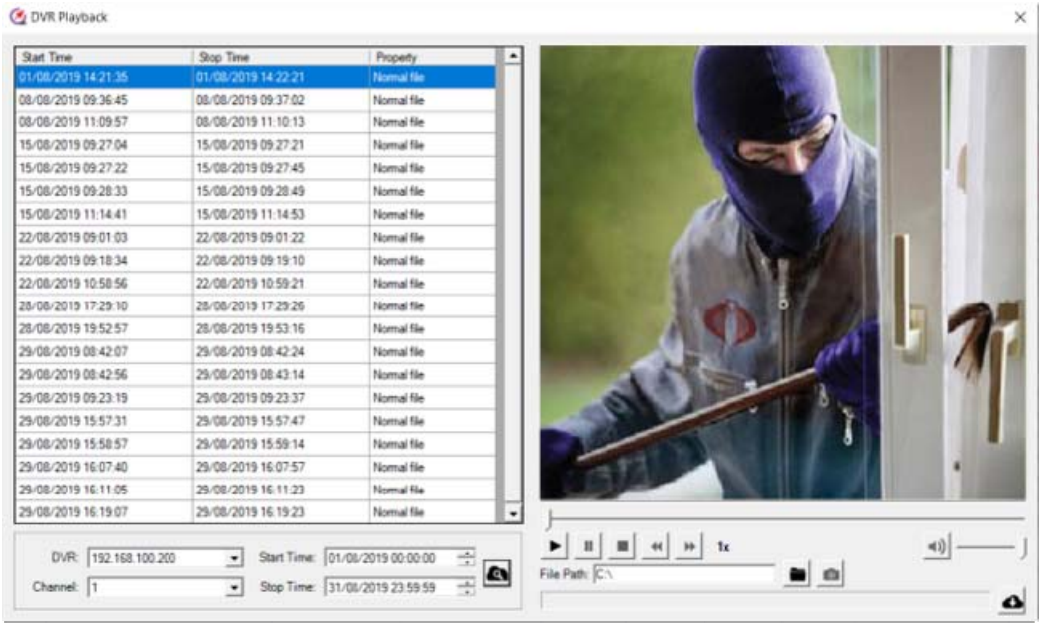
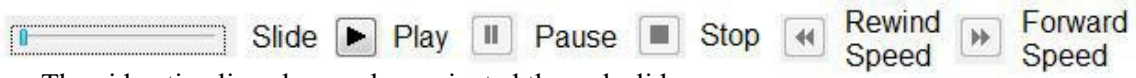


Fig 7.2.5: The clicking on Video Logo is able connect to DVR for playback.

2) It will pop up the DVR playback dialog window.
3) Select the DVR IP address.
4) Select the channel that wanted to be playback.
5) The start and end date range able to be assign.
6) Click on the Search/Filter image  .
7) Select on any of the video from the list and Click on Play.
8) The video can be control by play, stop, pause, rewind speed, forward speed.



9) The video timeline also can be navigated through slide.
10) The video can be downloaded to the local hard disk from the DVR. 

7.3 Door Commander

The door commander function allows the operator to control and monitor the door status.

- Operator can arm/disarm and lock/unlock the door.
- Operator can see live view video for specific door (include wiegand or WG) for visual verification.
- Operator can review captured picture or playback all recorded video for selected door (include wiegand or WG).
- During emergency event, operator can select multiple doors to lock/unlock in order to facilitate fast escape.

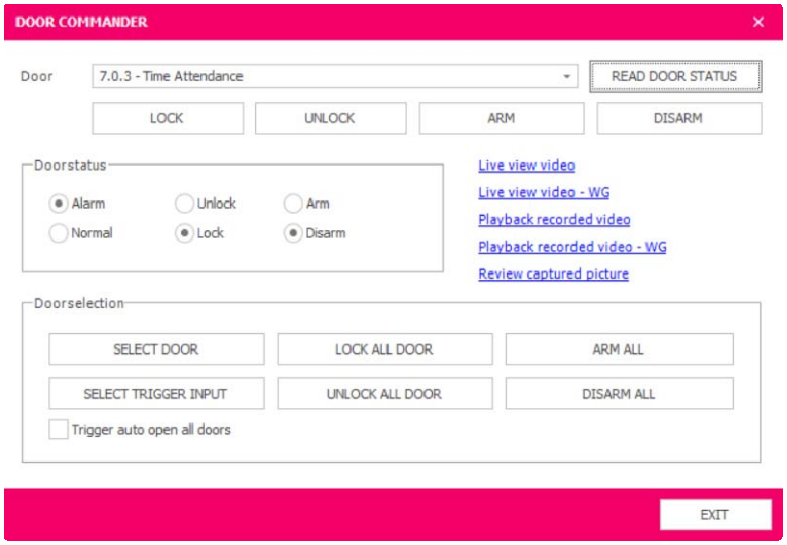


Fig 7.3.1: ***Door commander.***

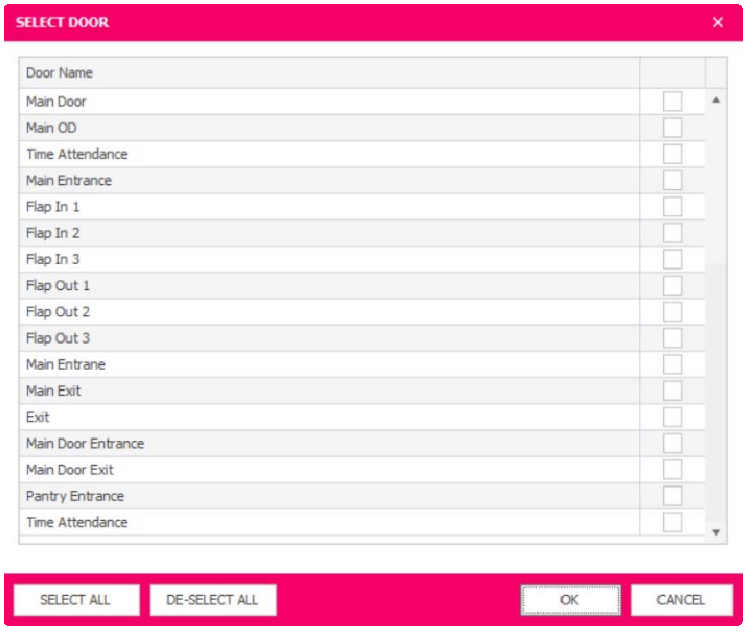


Fig 7.3.2: ***The selection of doors that will be controlled by Door Commander.***

READ DOOR STATUS
Click READ DOOR STATUS button will read the status of the door (Alarm, Normal, Lock, Unlock, Arm and Disarm).
WRITE DOOR STATUS
Click WRITE DOOR STATUS button will write the status of the door (Alarm, Normal, Lock, Unlock, Arm and Disarm).
LOCK
Click LOCK button will lock the selected door.

UNLOCK
Click UNLOCK button will unlock the selected door.

ARM
Click ARM button will arm the selected door.

DISARM
Click DISARM button will disarm the selected door(s).

SELECT DOOR
Select the door(s) and will be used for LOCK ALL DOOR, UNLOCK ALL DOOR, ARM ALL and DISARM ALL.

LOCK ALL DOOR
Click LOCK ALL DOOR button will lock all the selected door(s).

UNLOCK ALL DOOR
Click UN LOCK ALL DOOR button will unlock all the selected door(s).

ARM ALL
Click ARM ALL button will arm all the selected door(s).

DISARM ALL
Click DISARM ALL button will disarm all the selected door(s).

ACKNOWLEDGE ALARM
Click ACKNOWLEDGE ALARM button will acknowledge alarm for the doors.

EXIT
Click EXIT button will exit the window.

LIVE VIEW VIDEO

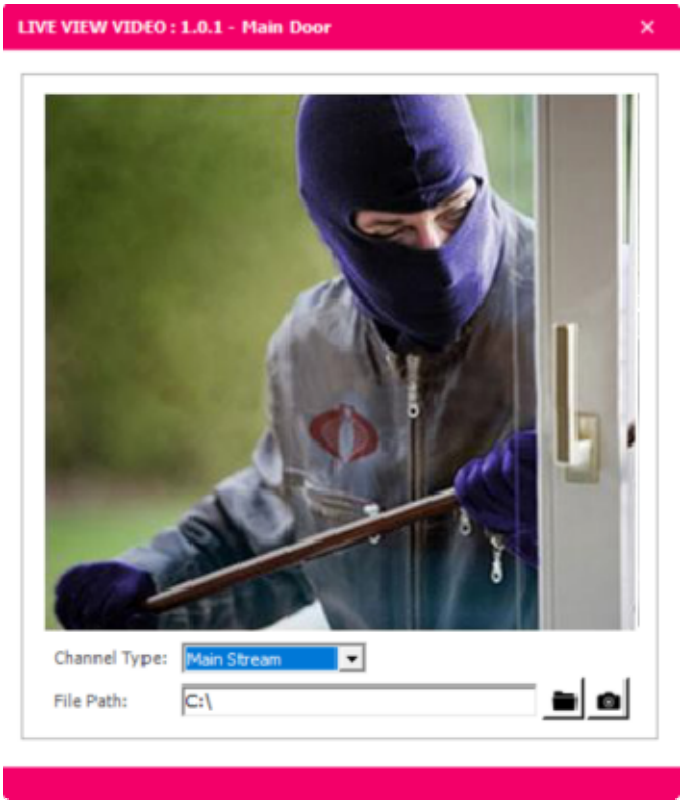


Fig 7.3.3: ***The Live View Video gives instant view from selected camera.***

PLAYBACK RECORDED VIDEO
Click on the **PLAYBACK RECORDED VIDEO** link.

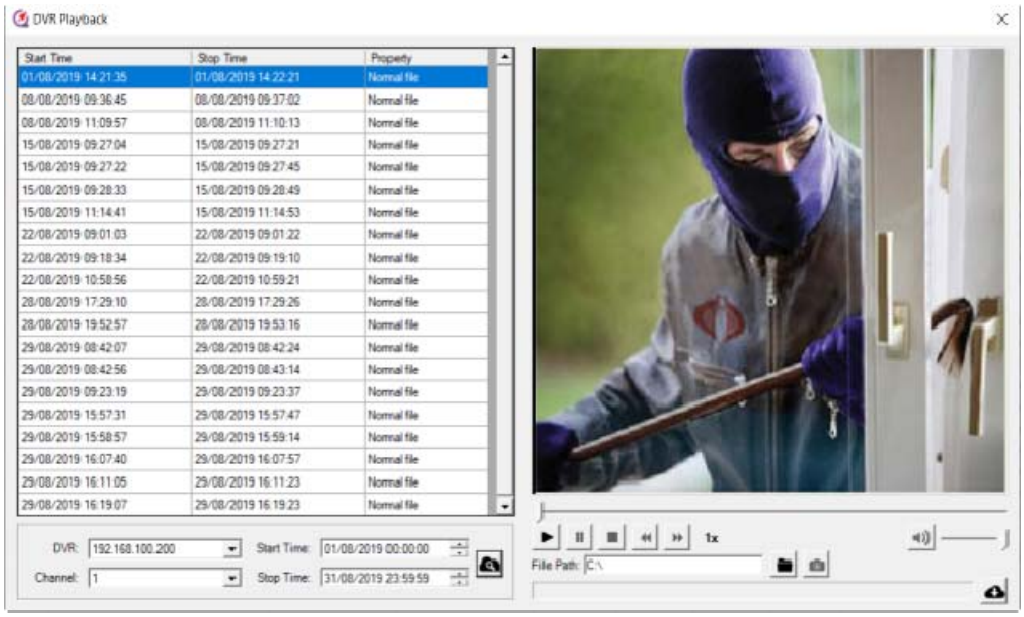
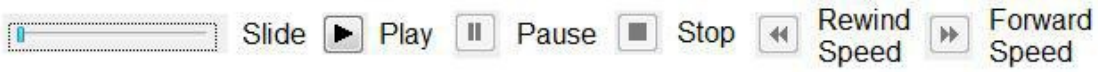


***Fig 7.3.4:* The clicking on Video Logo is able connect to DVR for playback.**

- It will pop up the DVR playback dialog window.
- Select the DVR IP address.
- Select the channel that wanted to be playback.
- The start and end date range able to be assign.
- Click on the Search/Filter image .
- Select on any of the video from the list and Click on Play.
- The video can be control by play, stop, pause, rewind speed, forward speed.
- 

- The video timeline also can be navigate through slide
- The video can be downloaded to the local hard disk from the DVR.

- **REVIEW CAPTURED VIDEO**

7.4 Trigger Auto Unlock All Door (TUAD)

The **Trigger Auto Unlock All Door** is software stimulated auto unlock all door for TCPIP reader such as **AR725Ev2**, **AR837EF** and **AR881EF.** TUAD will keep track on the selected reader alarm event based on the defined reader. When the software received alarm event from the defined reader, it will send an unlock command to the selected door.

Operator require to define which reader will send the alarm event to be monitor and which door to receive the unlock command from the software. Operator can define which door to be auto unlock when there is an alarm event send out from the defined reader to be trigger.

TUAD does not support AR716E multi door controller and **AR721E** 2-door controller.

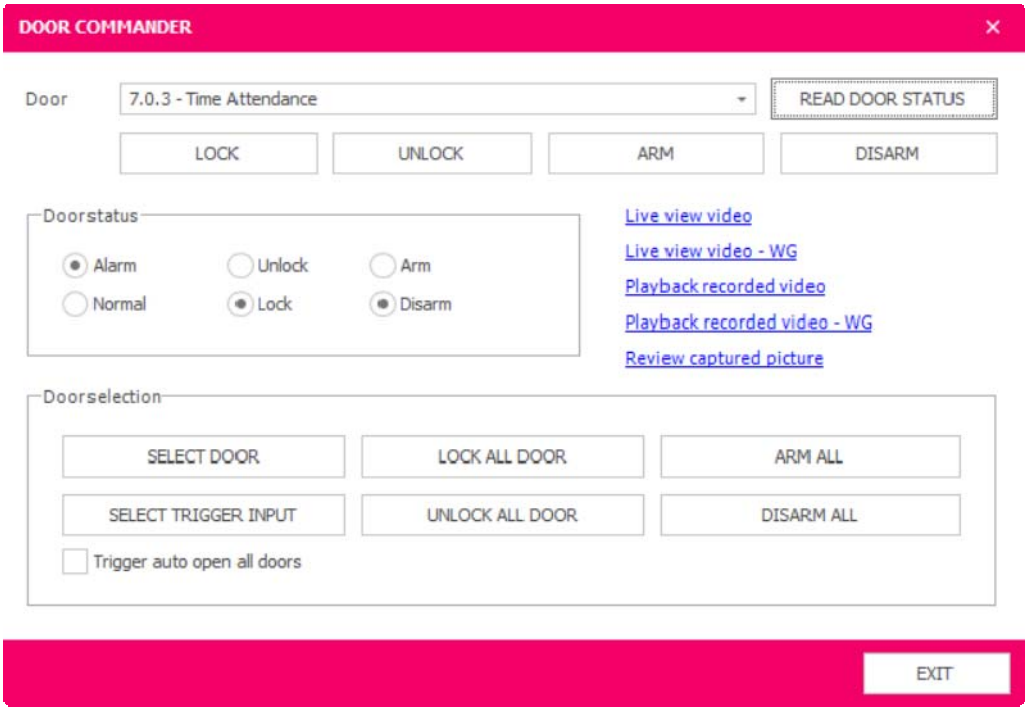


Fig 7.4.1: ***Door Commander***

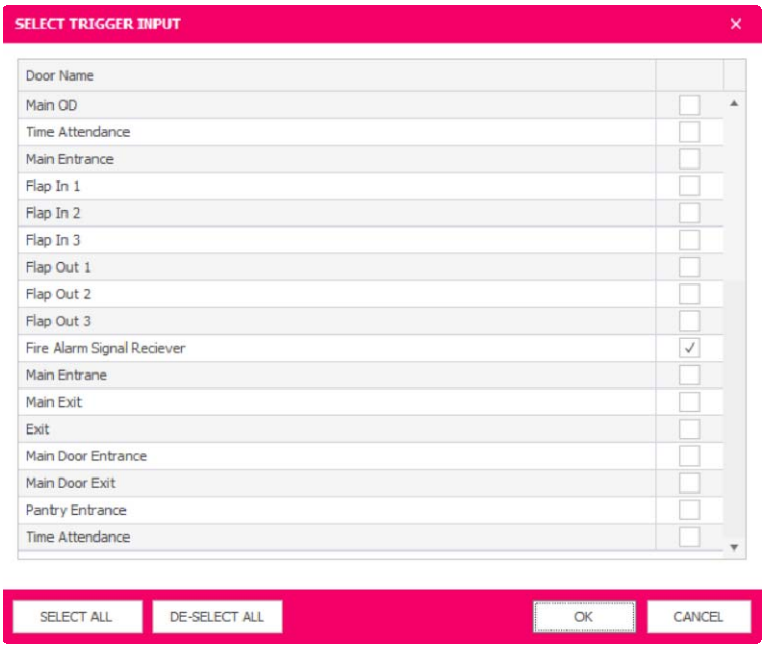


Fig 7.4.2: ***Select Trigger Input***

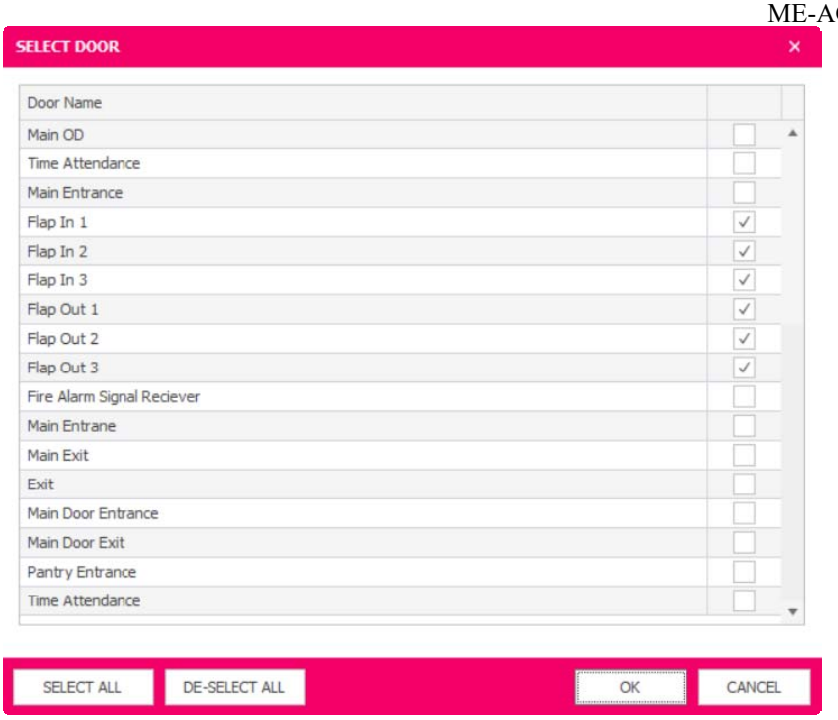


Fig 7.4.3: ***Select Door***

Create Trigger Auto Unlock All Door

1) Click on the **Select Trigger Input** button.(*Refer 7.4.1*)
2) All the reader will be available in the list box. *(Refer 7.4.2*)
3) Tick the selected reader for **Trigger Input.** (*Refer 7.4.2*)
4) Tick the **Trigger Auto Open All Door** (*Refer 7.4.1*)
5) Click on the **Select Door** for indicated which door will be release (*Refer 7.4.1*)
6) Select the door where operator want to unlock (*Refer 7.4.3)*
7) Click **OK** once the door is selected

Enable/Disable Trigger Auto Unlock All Door

1) Tick the **Trigger Auto Open All Door** to enable the function (*Refer 7.4.1*)
2) Untick the **Trigger Auto Open All Door to** disable the function (*Refer 7.4.1*

7.5 Camera Commander

The camera commander function provides live view video for the selected camera and can switch from one camera to another camera easily. The operator can view and check surrounding more efficient. This function can integrate with ***E-Map function***.

Monitoring → Camera Commander →Select camera

Fig 7.5.1: ***The Camera Commander provides the live view video for the selected camera.***

7.6 I/O Commander

This function ONLY can work when integrated AR716E digital input (DI). With I/O monitoring, the door sensor arming/disarming process can be more easily. This function can integrate with ***E-Map function***. This function only can use when active it in AR716E.

Monitoring → I/O Commander →Select DI →ARM or DISARM

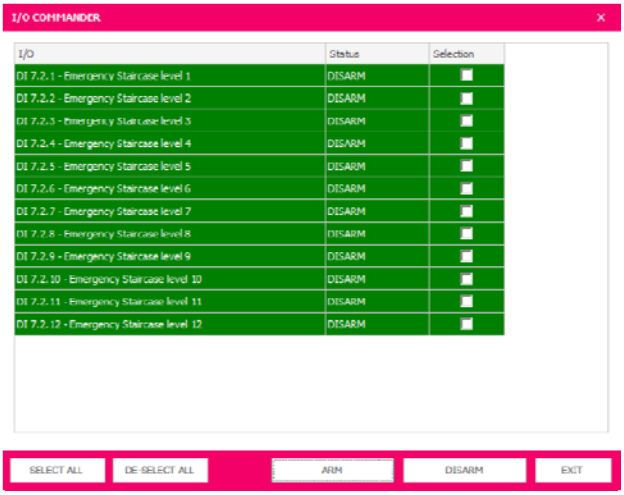


Fig 7.6.1: ***The arming / disarming process for I/O commander.***

Note: *Please active the Hardware I/O monitoring in the AR716E before use the I/O commander.*

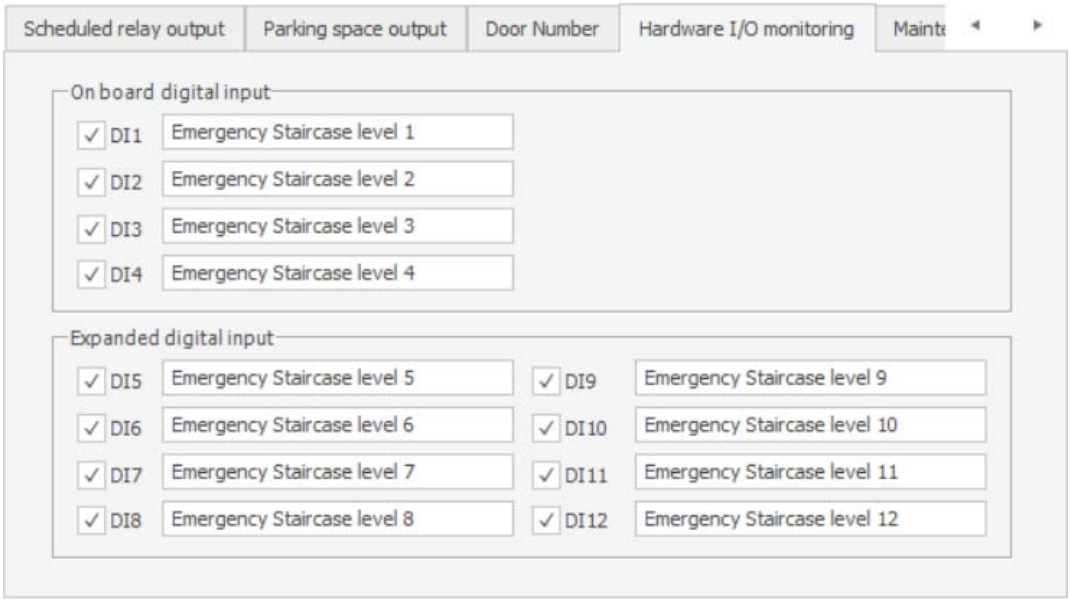


Fig 7.6.2: ***The arming / disarming process for I/O commander.***

Adding Digital Input (DI)

1) System Configuration → Hardware Manager → Select AR716E controller. *(Refer Fig 7.6.2)*
2) Click on the **EDIT** button.
3) Select *I/O Hardware Monitoring* tab, tick on the digital input (DI) to activate it.
4) Click on **Save** button and it will prompt for confirmation.
5) Click on **Yes** button to save the changes or **No** button to reject the changes.

Note: *This I/O Hardware Monitoring is* ***not need*** *to do WRITE TO HW process.*

Edit Digital Input (DI)

1) Select the AR716E that you want to edit digital input (DI). *(Refer Fig 7.6.2)*
2) Click on the **Edit** button and modified the setting.
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to confirm accept the changes or **No** to reject the changes.

Deactivate Digital Input (DI)

1) Select the AR716E that you want to edit digital input (DI). *(Refer Fig 7.6.2)*
2) Click on the **Edit** button, deselected all the digital input (DI).
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes.

7.8 In/Out Monitoring

The In/Out Monitoring is use to monitor the assigned door. In/Out monitoring effectively show the picture user's current entry and previous entry for visual comparison with picture in database. This help
operator verify if the person badge at the door is actually the correct person. In time interval of the last entry or exit will also be display for operator to verify if the timing look suspicious. In/Out monitoring is a great
function that increases the effectiveness of access control with visual verification at guard house point.

Monitoring → In / Out Monitoring

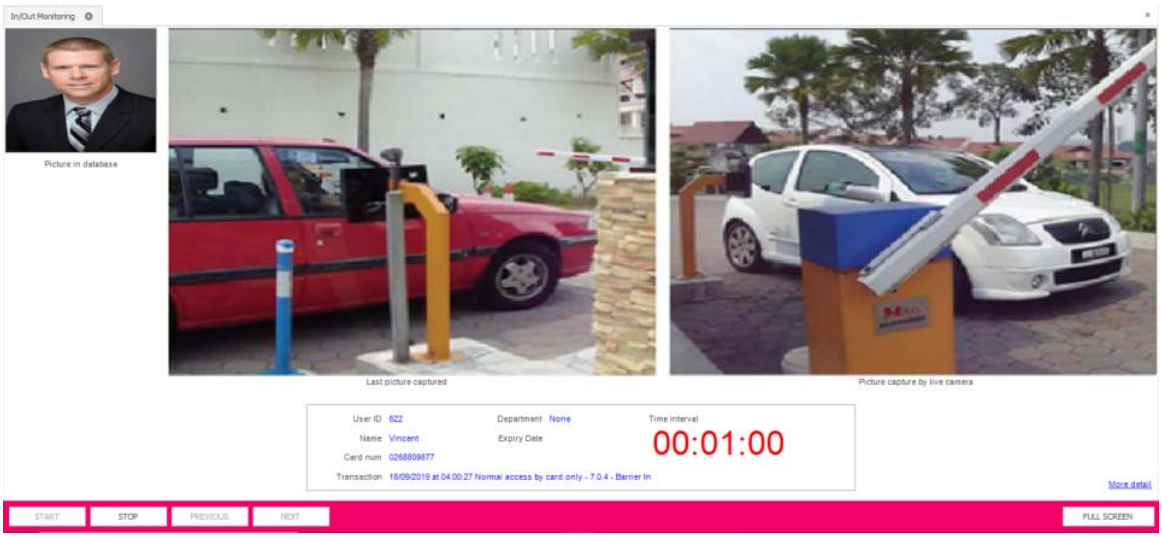


***Fig 7.8.1:* The In / Out monitoring provide the latest images are captured when each time the camera capture the picture or got user login.**

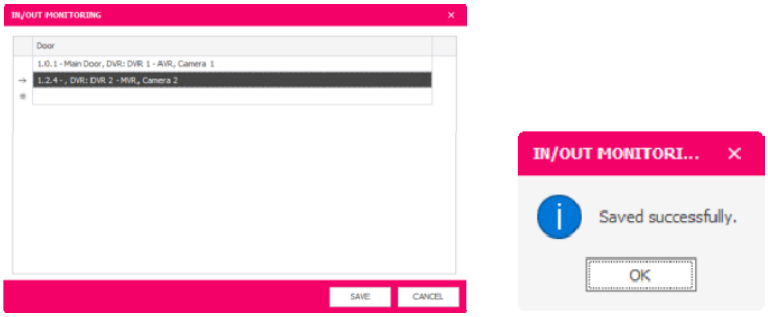


***Fig 3.7.3:* IN / OUT Monitoring Door(s) selection.**

IN/OUT Monitoring

Note: *This function is purposely use for multiple operators in the different PC when integrate with CCTV monitoring. Each operators can monitor base on selected doors. Different PC login with different accounts then can monitor IN / OUT records base on selected doors.*

1) Highlight the operator(s) and click on **EDIT** button to edit it.
2) Click on **IN / OUT MONITORING** button to select the door(s) for CCTV monitoring purpose. *(Refer 3.7.3)*
3) Click on the **Save** button. It will prompt for confirmation.
4) Click **Yes** to confirm accept the changes or **No** to reject the changes. *(Refer 3.7.3)*

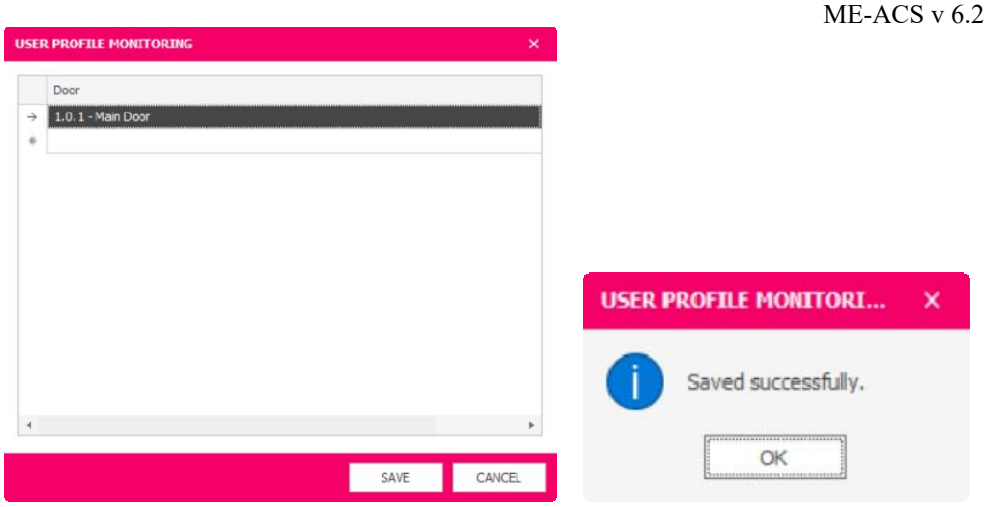


Fig 3.7.5: ***User Profile Monitoring Door(s) selection.***

User Profile Monitoring

Note: *This function is purposely use to identified users IN / OUT record for selected door(s). For each events log, the personal user profiles detail will be displayed out and to avoid other person use other user card's owner to access.*

1) Highlight the operator(s) and click on **EDIT** button to edit it.
2) Click on **USER PROFILE MONITORING** button to select the door(s) for user profile monitoring purpose. *(Refer 3.7.5)*
3) Click on the **Save** button. It will prompt for confirmation.
4) Click **Yes** to confirm accept the changes or **No** to reject the changes. *(Refer 3.7.5)*

7.9 User Tracking

User tracking also known as "roll call" function. It is able to monitor in which location is the user. This will be very helpful during emergency to locate the staffs and to pass any call to the nearest intercom line.

Monitoring → User Tracking

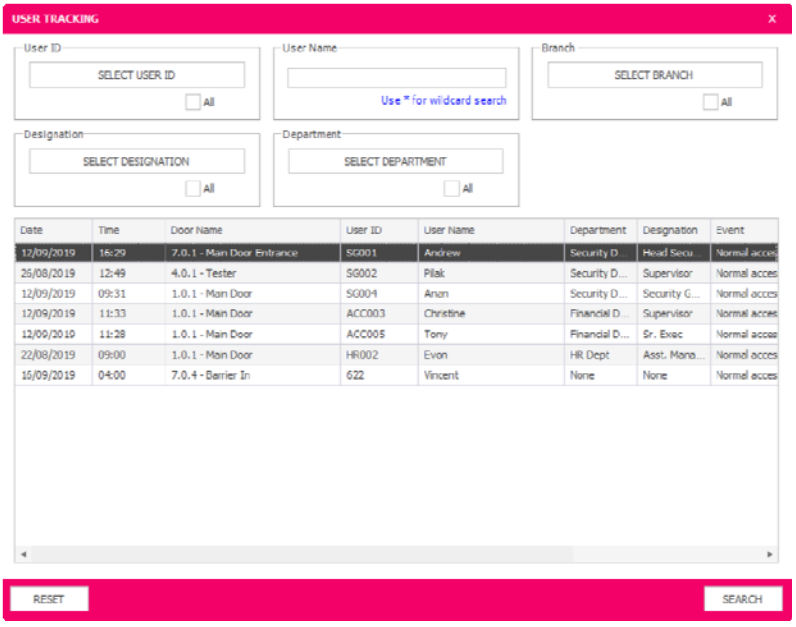


Fig 7.9.1: ***User tracking.***

- Filter the user by selecting the user num, user id, user name, department or designation.
- Click on the SEARCH button.
- A list will appear as per the filtering.

7.10 Area Control

Area control is use to check the number of user in certain area or to identify the user status in that area, is inside or outside. The multiple areas can be assigning different in/out reader/wiegand or selected door. The history record inside this function is update from time to time once got in/out event happen to show the latest status of user. This function can be used as checking list during emergency **TO IDENTIFY WHO STILL INSIDE and LOCATION**. Otherwise, this function also can as a tool to track user latest in/out record. All the user in/out event for selected area also is summarize and show as pie chart for references.

Monitoring → Area Control →Area Monitoring

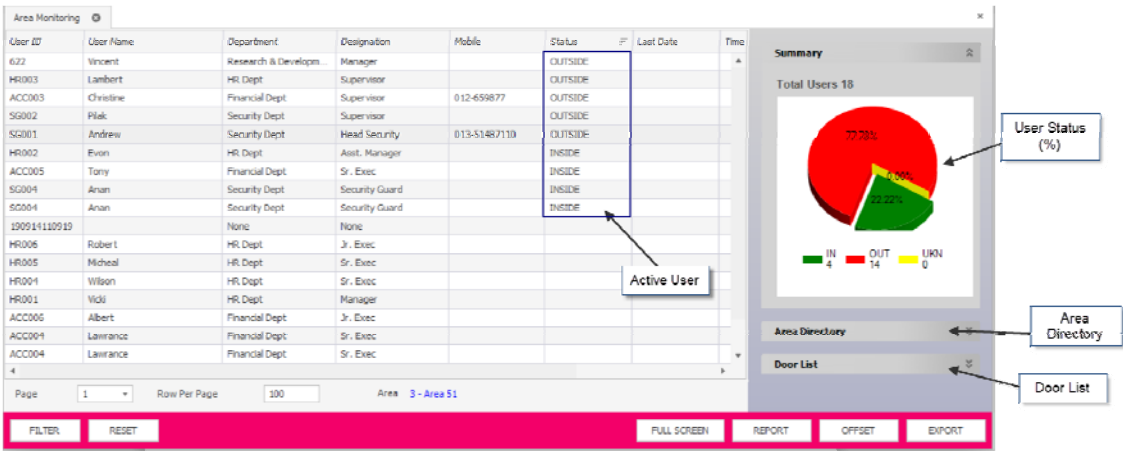


***Fig 7.10.1:* Area Monitoring.**

Note:

User Status (%): *The percentage of User in selected area include IN, OUT & UNKNOWN with base on the total of users under Area Monitoring List.*

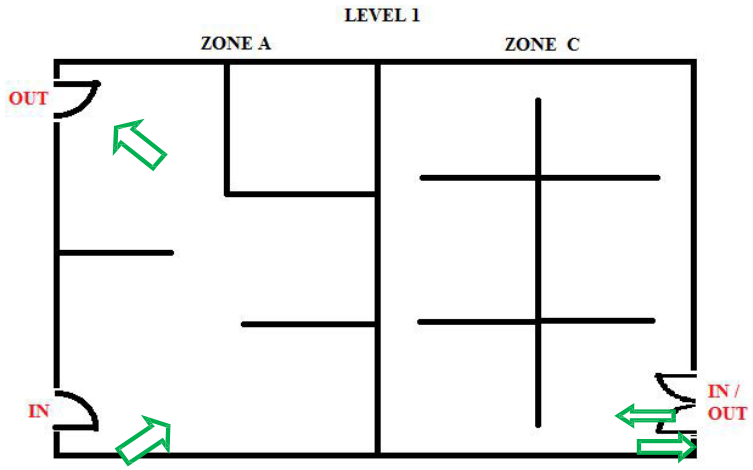
Area Directory: *The directory for all the areas.*

Door List: *The item of doors list, is group as IN or OUT doors.*

Active User: *For those users got in/out clocking transaction in current log is consider as active user.*

Row Per Page: *The number users is shown in the Area Monitoring List.*

Filter: *The tool to do filtering base on the user information.*



LEVEL 1:

ZONE A:
(Involve 2 readers)

- ***Zone A Main Door IN***
- ***Zone A Main Door OUT***

ZONE C:
(Involve 1 reader & 1 wiegand)

- ***Zone C Main Door IN***
- ***Zone C Main Door WG OUT***

***Fig 7.10.2:* Sample map - Area Monitoring.**

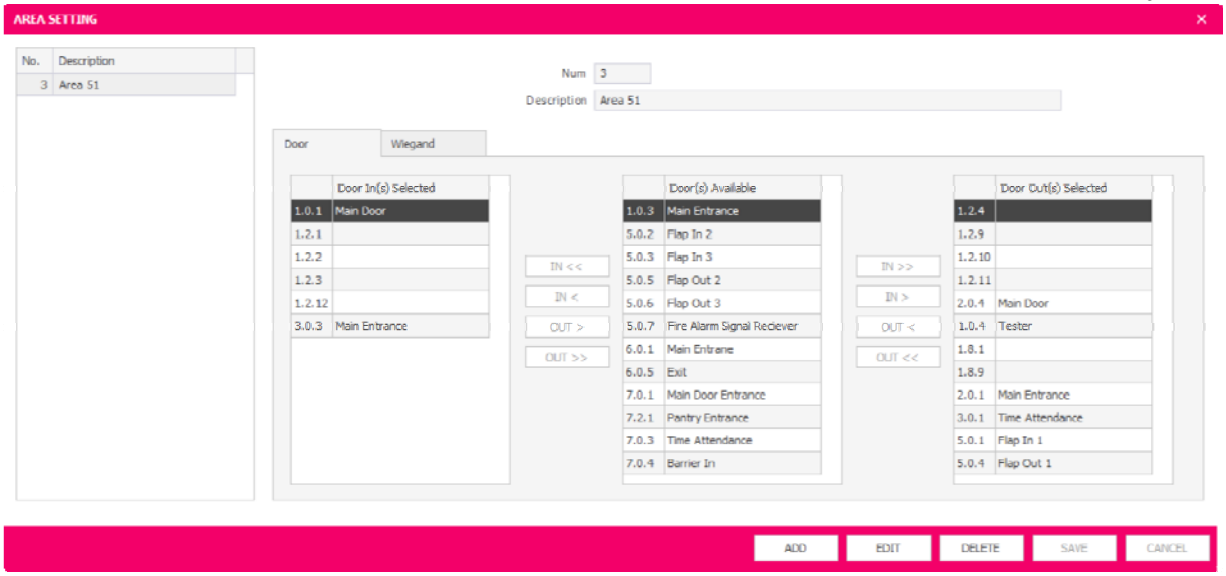


***Fig 7.11.3:* Area Control Setting.**

Adding Area

1) *Monitoring* → *Area Control* →*Area Setting. (Refer Fig 7.10.3)*
2) Click on the **ADD** button.
3) The number no need to be assign since it is automated. But you also can assign the number manually.
4) Enter the description.
5) Select the door by click on **<<IN** or **<IN** for *Door IN* and **IN>>** or **IN>** for *Door OUT*.
6) Click on the **Save** button. It will prompt for confirmation.
7) Click on **Yes** button to save it or **No** button to reject it.

Editing Area

1) Select the Area Control that you want to edit from the left panel list by clicking on it. *(Refer Fig 7.10.3)*
2) Once selected, click on the **Edit** button.
3) After editing the necessary fields, click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes.

Delete Area

1) Select the area that you want to delete from the left panel list by clicking on it. *(Refer Fig 7.10.3)*
2) Once Selected, click on the **Delete** button.
3) Click on the **Save** button. It will prompt for confirmation.
4) Click on **Yes** button to save the changes or **No** button to reject the changes.

Cancel Area

1) Click on the **Cancel** button to reject any entries while Adding or Editing before.

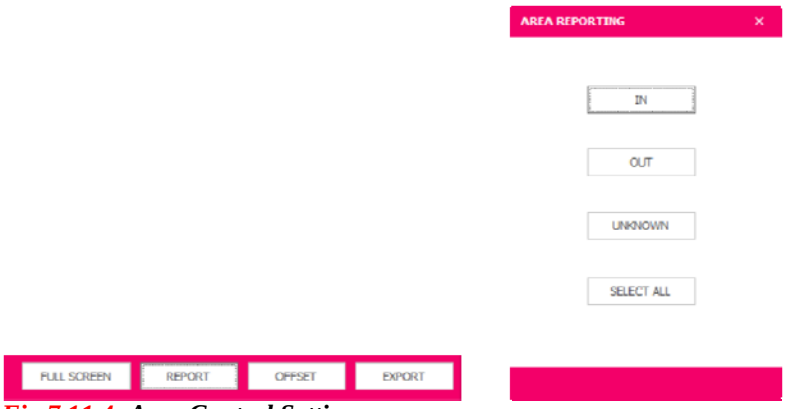


Fig 7.11.4: ***Area Control Setting.***

Full Screen Area Control

1) Click on the **FULL SCREEN** button to expand area control full screen view. *(Refer Fig 7.10.4)*

Area Control Report

2) Click on the **REPORT** button to open area control report. *(Refer Fig 7.10.4)*
3) Select type of report (*IN, OUT, UNKNOWN or SELECT ALL*) wants to be generated. *(Refer Fig 7.10.4)*

Offset Area Control

1) Click on **OFFSET** button to reset all the *active user status* for selected area to become *UNKNOWN*. *(Refer Fig 7.9.4)*

Export Area Control Data

1) Click on the **EXPORT** button to open export the area control data. *(Refer Fig 7.10.4)*
2) Select the path of file and click on **Save** button to save the data file.

7.11 E-map Control

Under the E-map control, *door commander, camera commander and I/O monitoring can be integrated together* to make the access control become more secure and more easy to handle by the operator. The map of building can be attached together to get the overall image of control area or location. With the I/O monitoring commander or door commander then can use it to make sure where or which door got incidents or problems happen. Then, can use camera commander to view the situation where the incident is happening to identify the main cause. After that, the suitable action can be taken to make sure the surrounding area or location is secure and safe.

How ALL this function integrated each other to give more secure and safe access control system?

- I/O monitoring behave as a sensor or control unit and notify when got force open incident happen or system breakdown.
- Door commander behave as door access control and picture capture for those access the door. This function gives the alternative way to checking the user is the owner or not in door access activity.
- Door commander also provide live view video and recording during door access activity.
- Camera commander provide the live view video and recording base on the location of camera be installed. Switching between the cameras can use to check the monitoring area from time to time.

Monitoring → E-map Control →E-Map Monitoring

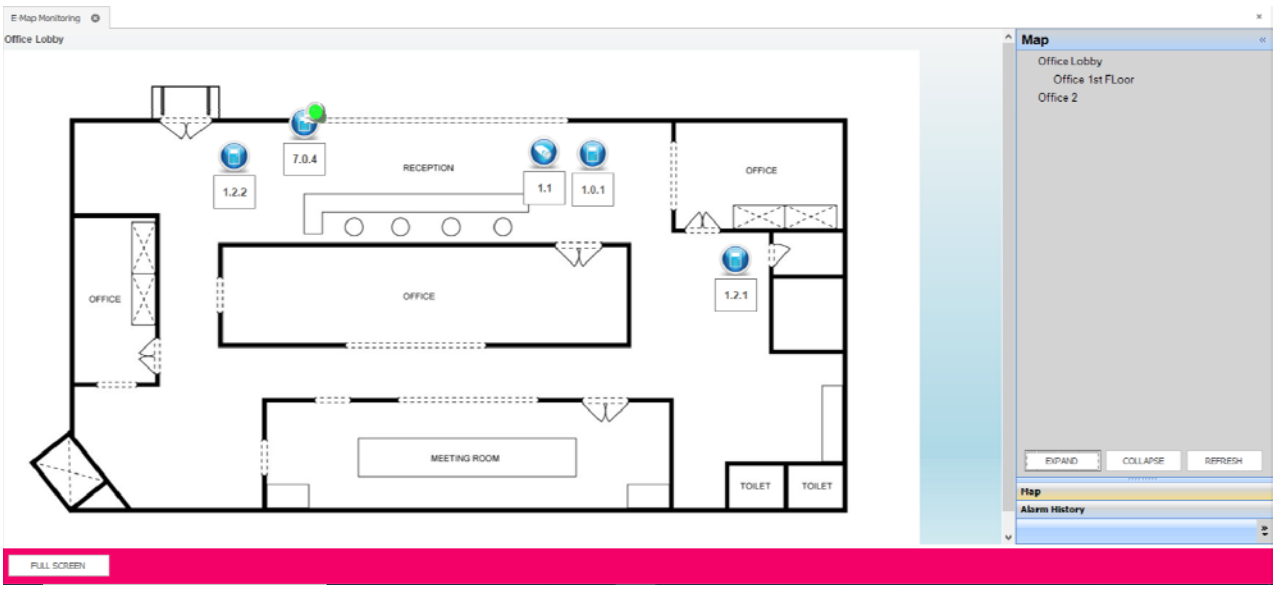


***Fig 7.11.1:* E-map Monitoring.**

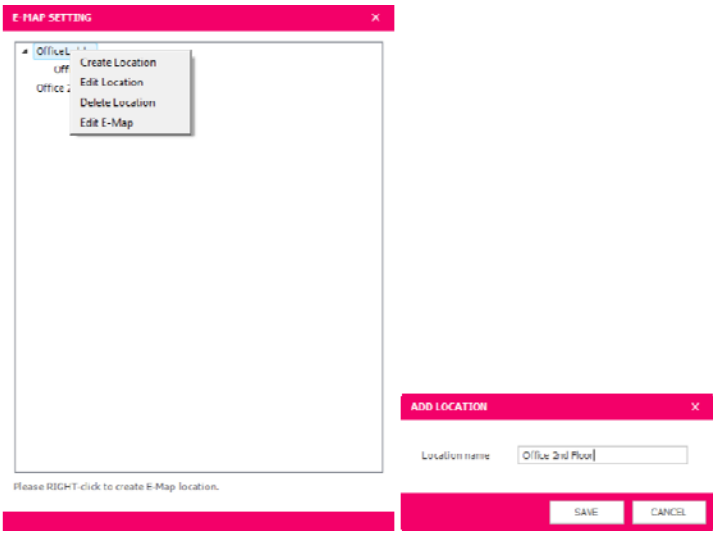


***Fig 7.11.2:* E-Map Setting.**

Adding E-Map

1) *Monitoring → E-Map Control →E-Map Setting. (Refer Fig 7.11.2)*
2) Right-click inside the E-Map Setting window, and select *Create Location* to open *ADD LOCATION*.
3) In the *ADD LOCATION* window, fill in the *Location name* and click on **SAVE** button to save it. *(Refer Fig 7.11.2)*

***Note:** To create **sub-location** with highlight on main location and right-click to select Create Location. Then key in the location name and click on SAVE button to save it.*

Editing E-Map Location Name

1) Select the E-Map Location that you want to edit the name by clicking on it and then right-click to select *Edit Location. (Refer Fig 7.11.2)*
2) In the *EDIT LOCATION* window, fill in the new location name and click on **SAVE** button to save it.

Editing E-Map

(Note: Edit E-Map is use to add in the Door Commander icon, I/O Monitoring icon and Camera commander icon.)

1) Select the E-Map Location that you want to add in other functions as state above by clicking on it and then right-click to select *Edit E-Map. (Refer Fig 7.11.2)*

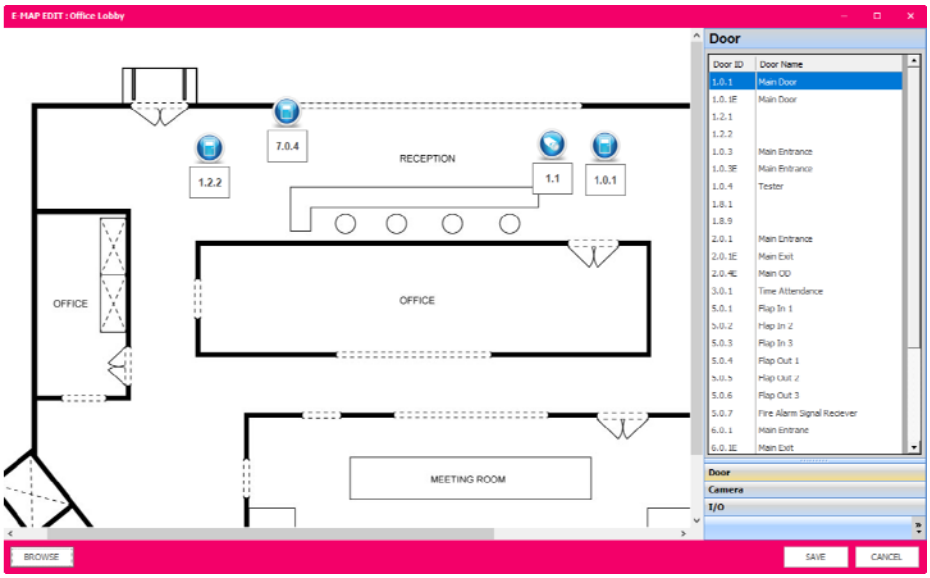


Fig 7.11.4:** **E-Map Edit.

2) Click on **Browse** button to browse the picture or map of the selected location. Click on **OPEN** button to attach the picture or map. *(Refer Fig 7.11.4)*
3) Click on *Door*, a list of doors is show. Click on the door is match with selected picture or map, then right-click to hold the door and drag it into the map.
4) Click on *Camera*, a list of cameras is show. Click on the camera is match with selected picture or map, then right-click to hold the camera and drag it into the map.
5) Click on *I/O*, a list of digital input (DI) of I/O point is show. Click on the DI is match with selected
picture or map, then right-click to hold the DI and drag it into the map.
6) After finish all things, and then click on **SAVE** button to save all the changes or **CANCEL** button to cancel it.

Delete E-Map

1) Select the E-Map location that you want to delete by clicking on it and then right-click to select
Delete Location. (Refer Fig 7.11.2)
2) In the *REVOME LOCATION*, click on the **SAVE** button to remove it or **CANCEL** button to cancel it.

7.12 User Profile Monitoring

User Profile Monitoring is use to monitor user IN / OUT for selected door(s). In the User Profile Monitoring can be classified into Single User Profile and Triple Users monitoring. Each time the users go in or out, the user personal detail will be display out. With the User Profile Monitoring then can be used as an evidence when incidents or problems is happening. After that, the suitable action can be taken to find the main cause or solution.

Monitoring →User Profile Monitoring → Single Profile ***or*** *Triple Profile*

Single User Profile Monitoring

Fig 7.12.1: ***The Single User Profile.***

Triple Users Profile Monitoring

Fig 7.12.2: ***The Triple Users Profile.***

8) HouseKeeping

The housekeeping module is responsible for managing routine tasks and procedures carried out in the functioning of a system or ME-ACS. The module functionality is described as follows:

Important Note :-

All auto function such as export access transaction, time attendance, user list and back up will execute by MagServer. Does not require the MagClient to execute the auto function.

8.1 Database Management

There are 3 tabs of database management:
Tab 1) Backup Tab 2) Restore Tab 3) Purge

Tab 1) Backup

For DVR picture backup:

- Choose the destination drive path to keep the records of DVR pictures are capture by camera.

(It is not recommended to activate this feature if the PC is not i7 with 5G Ram or above).

For Picture Database backup:

- Choose the destination drive path where the backup file needs to be placed or click on the **BROWSE** button.
- Insert the file name or tick the checkbox to auto generate new file name
- Click on the **BACKUP NOW** button

For Main Database backup:

- Choose the destination drive path where the backup file needs to be placed or click on the **BROWSE** button.
- Insert the file name or tick the checkbox to auto generate new file name
- Click on the **BACKUP NOW** button
- Tick on the **auto schedule backup** checkbox to enable auto database backup and insert the time for auto backup.

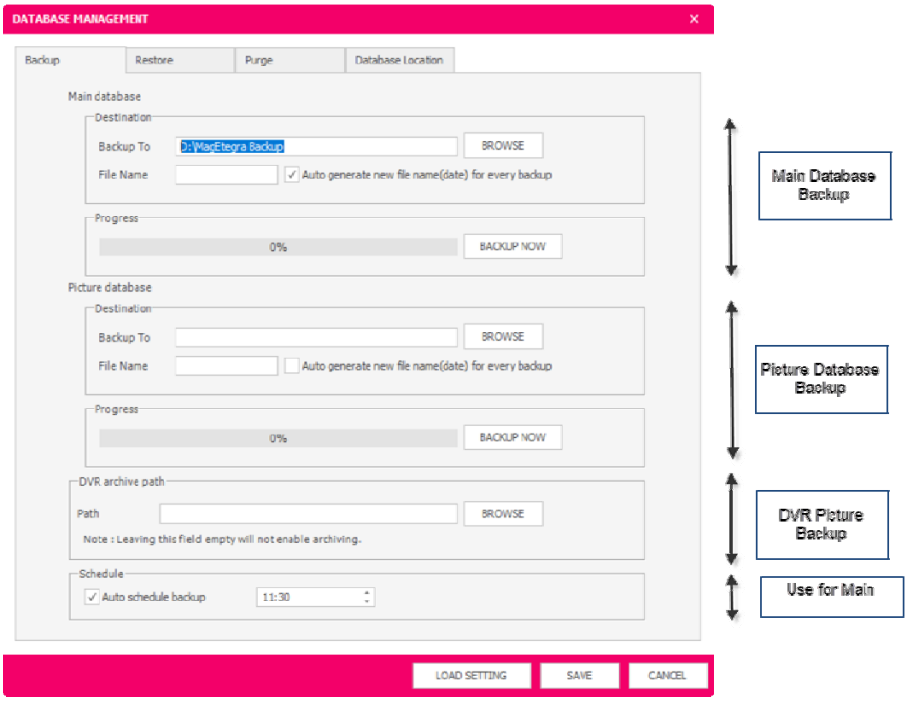


*Fig 8.1.1: **The DVR or database backup system.***

Tab 2) Restore

- Choose the destination drive path & file name where the backup file placed or click on the BROWSE button. Process database restoration cannot fully be executed for path in C:\ due the file protection by Win 7. It is recommended *to store database file in D:* to make is available for restore purpose.
- Enable / disable "Keep existing license and preferences" to select which of one information is preferred.
- Click on the **RESTORE NOW** button

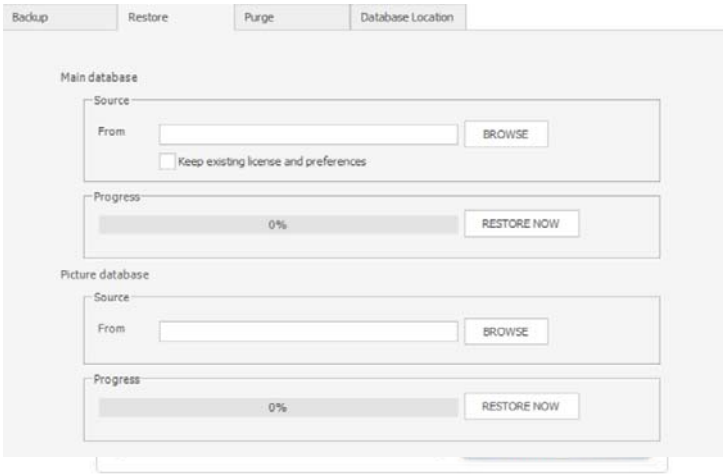


***Fig 8.1.2:* The restoration from backup database file.**

Tab 3) Purge

- Choose the option to purge. (All/Transaction/Time Attendance)
- Click on the **PURGE** button and all the selected info will be deleted.
- The percentage of database capacity display bar: *Normal (green), Caution (yellow), Critical (Red)*.

Note :

*** When the percentage of database capacity is reach critical condition. Alert will prompt to do data purge to release some database space. The Event logs will be blocked from being transfer into system database.*

*** Auto purge is used to purge the certain amounts of records form database automatically when the main database/picture database is full.*

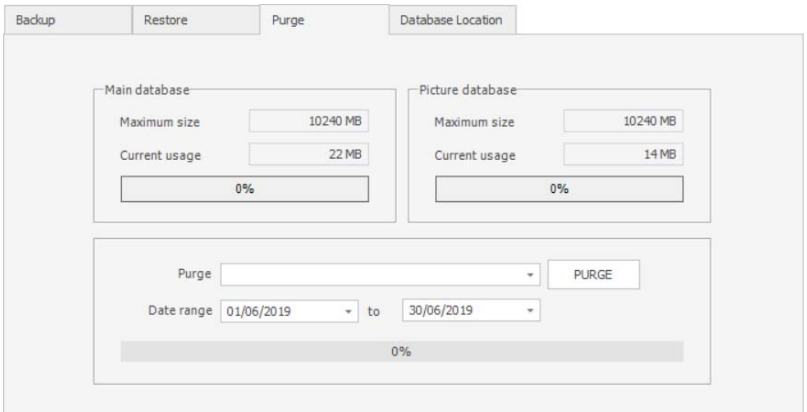


***Fig 8.1.3:* The cleaning for database along certain periods for all fields.**

8.2 Import/Export Access Transaction

Comprehensive reporting with flexible filtering is available. If current reporting is not sufficient to meet the requirement, ME-ACS offer extensive export function that condition the data into any format or column arrangement to match target application. Access control transaction is typically exported to third party time attendance application or advanced ERP system for more comprehensive reporting that cater additional needs of the organization.

Choose the start date and end date from the dropdown menu in the Date group box.
Choose the start user num and end user number from the dropdown box in the User num group box or select the ALL checkbox to choose all user num.
Choose the start user id and end user id from the dropdown box in the User ID group box or select the ALL
checkbox to choose all users ID.

There are 5 tabs of Import/Export Access Transaction:
Tab 1) Field Arrangement Tab 2) Department Tab 3) Output
Tab 4) Duty Label Tab 5) Formatting

Tab 1) Field Arrangement

Choose the fields from the fields available box and click on in to appear in the field selected box. This few fields are compulsory to be selected, include Transaction Type, Date, Time, User ID and Door ID.

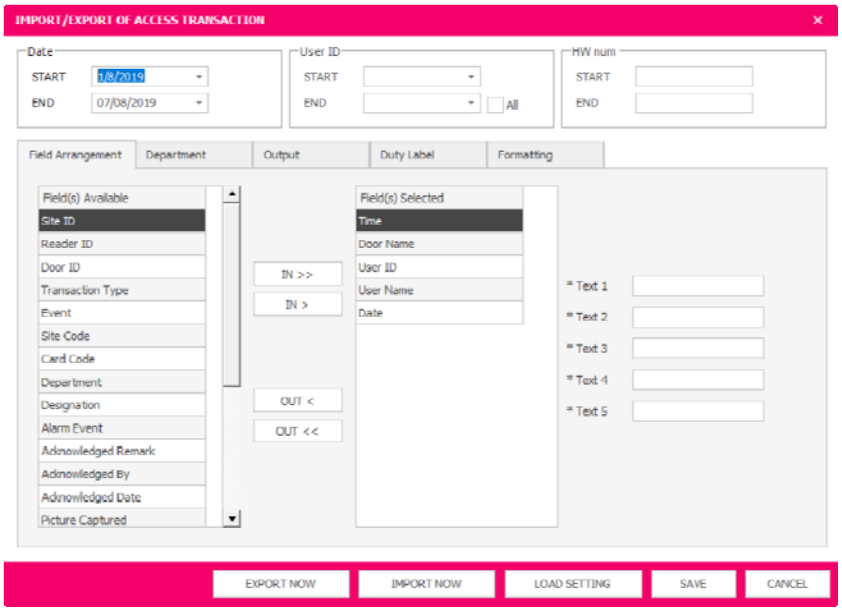


***Fig 8.2.1:* The fields' arrangement in import / export of access transaction.**

Tab 2) Department

Select the criteria to be filtered. (For example by department, designation, transaction type, door) Click on the button *Select Department* and choose the options or check *ALL* to select all the departments.

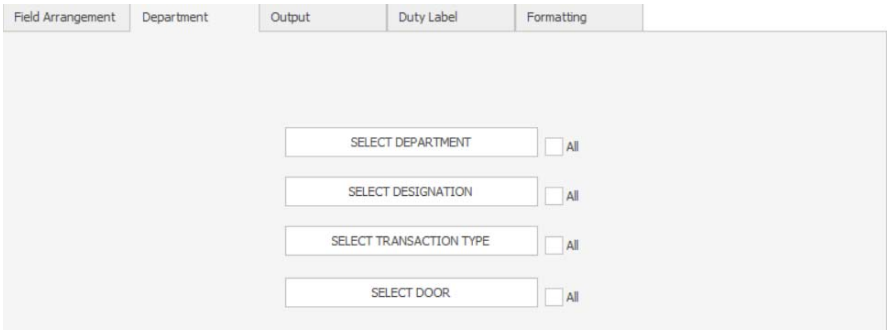
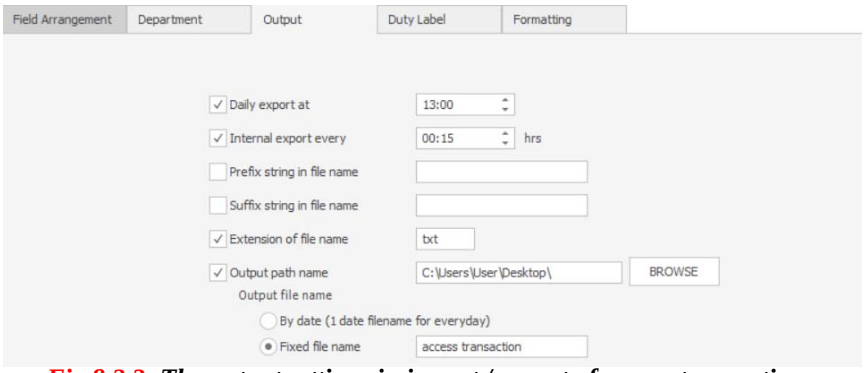


***Fig 8.2.2:* The department settings in import / export of access transaction.**

Tab 3) Output

Set the output setting for the access transaction file.



The file is automatically export at 12:00 am daily to the file path F:\. Then the file is updated for every each 1 hour. The format file is csv with name by refer to PC date system.

***Fig 8.2.3:* The output settings in import / export of access transaction.**

- *Daily export at hh:mm AM*: Automatically export file at specified time daily.
- *Internal export every xxx hrs*: Automatically export file for every interval hours from daily export time.
- *Extension of file name*: csv (crystal report format), txt (text format) or xls (Microsoft excel format).
- *Output path name*: The location of file is exported. **(Can export to another PC through file sharing with WRITE authorities).**

Tab 4) Duty Label

Set the duty based clocking for F1, F2, F3, F4, F1', F2', F3', F4'.

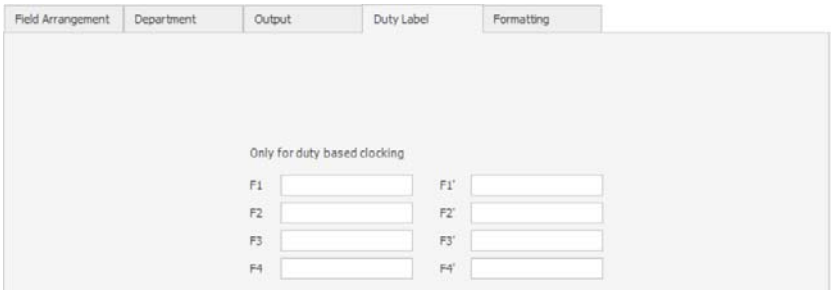


***Fig 8.2.4:* The duty label in import / export of access transaction.**

Tab 5) Formatting

Set the format such as date and time.

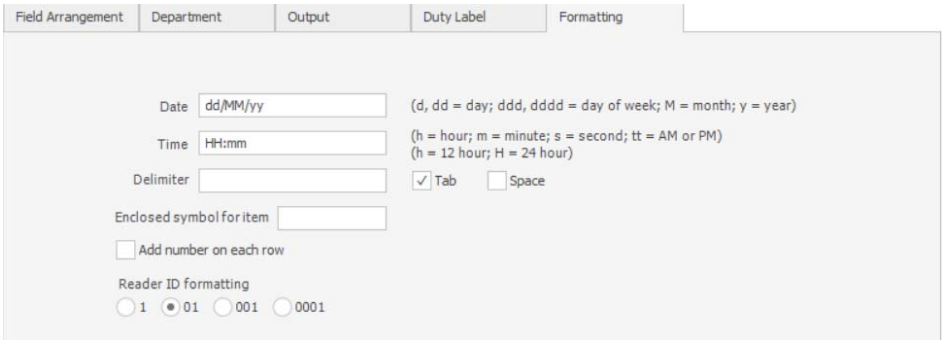


Fig 8.2.5: The output formatting in import / export of access transaction.

8.3 Import/Export Time Attendance

Comprehensive reporting with flexible filtering is available. If current reporting is not sufficient to meet the requirement, ME-ACS offer extensive export function that condition the data into any format or column arrangement to match target application. Payroll function is not available in ME-ACS. Calculated time attendance data can be exported out to third party payroll software for salary pay slip processing.

Choose the start date and end date from the dropdown menu in the Date group box.
Choose the start user num and end user number from the dropdown box in the User num group box or select the ALL checkbox to choose all user num.
Choose the start user id and end user id from the dropdown box in the User ID group box or select the ALL
checkbox to choose all users ID.

There are 5 tabs of Time Attendance:
Tab 1) Field Arrangement Tab 2) Filter Tab 3) Output
Tab 4) Duty Label Tab 5) Formatting

Tab 1) Field Arrangement

Choose the fields from the fields' available box and click on in to appear in the field selected box. Able to define the field name maximum 5.

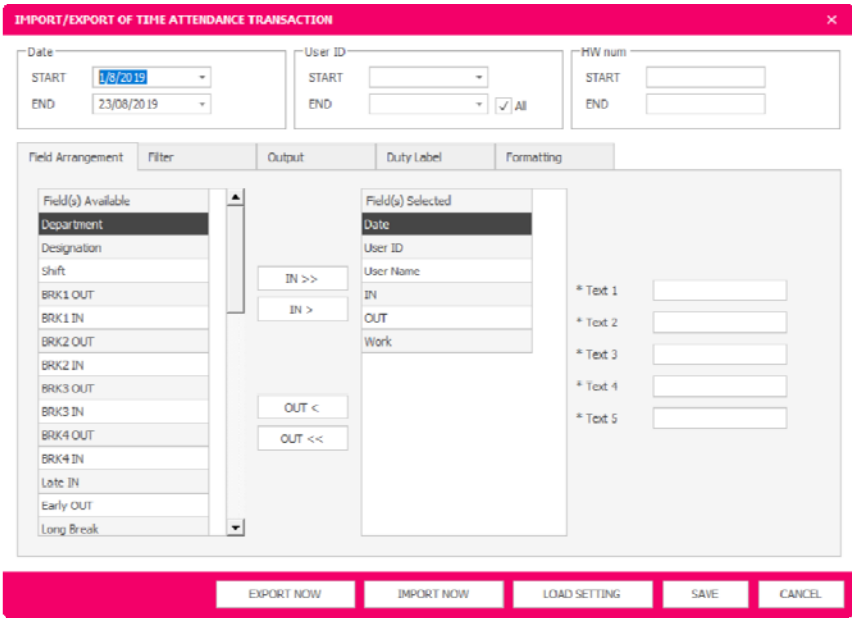


Fig 8.3.1: The field arrangement in import / export of time attendance transaction.

Tab 2) Filter

Select the criteria to be filtered. (For example by department, designation, transaction type, door)

Click on the button *Select Department* and choose the options or check *ALL* to select all the departments.

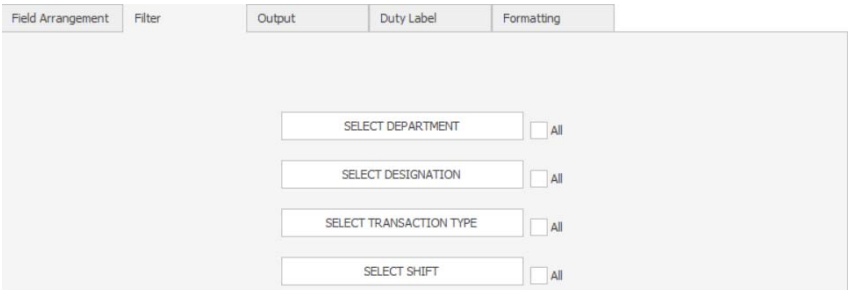


***Fig 8.3.2:* The department settings in import / export of time attendance transaction.**

Tab 3) Output

Set the output setting for the access transaction file.

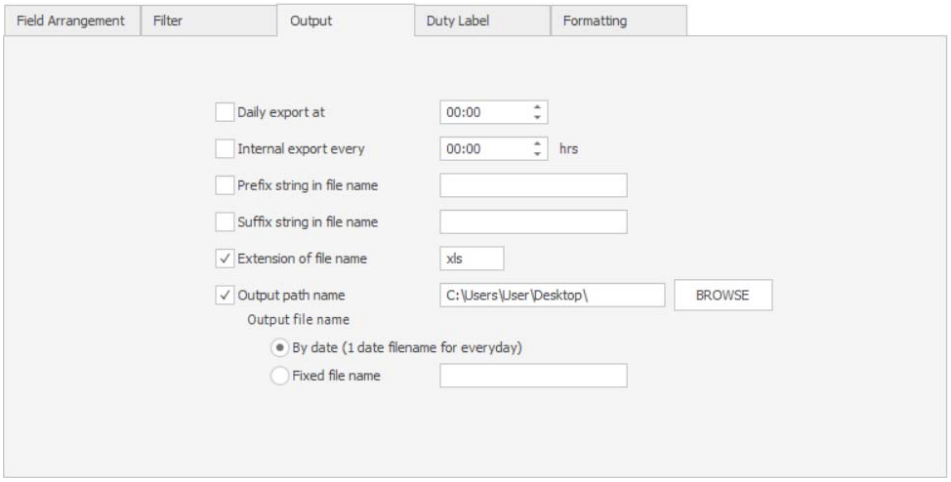


***Fig 8.3.3:* The output settings in import / export of time attendance transaction.**

Tab 4) Duty Label

Set the duty based clocking for F1, F2, F3, F4, F1', F2', F3' & F4'.

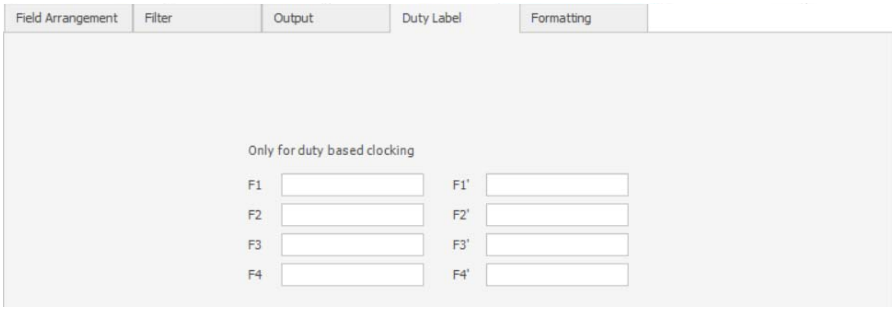


***Fig 8.3.4:* The duty label in import / export of time attendance transaction.**

Tab 5) Formatting

Set the format such as date and time.

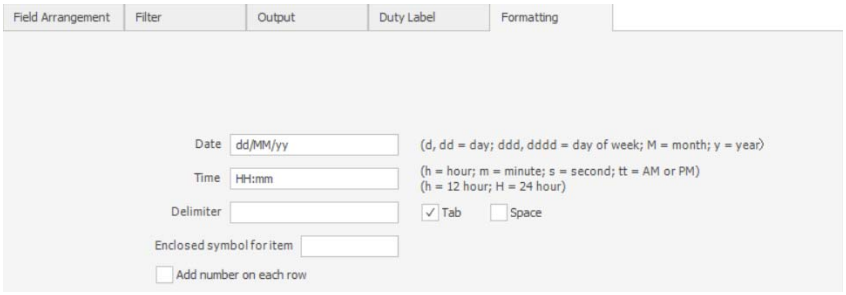


***Fig 8.3.5:* The output format in import / export of time attendance transaction.**

8.4 Import/Export User Profile

User profile can be exported or imported for backup purposes. ME-ACS user profile can be exported into a text file. This text file can then be imported into third party time attendance or payroll software to avoid the hassle of entering all the users again during integration works.

Choose the start date and end date from the dropdown menu in the Date group box.
Choose the start user num and end user number from the dropdown box in the User num group box or select the ALL checkbox to choose all user num.
Choose the start user id and end user id from the dropdown box in the User ID group box or select the ALL
checkbox to choose all user ID.

There are 5 tabs of User Profile:

Tab 1) Field Arrangement Tab 2) Department Tab 3) Output
Tab 4) Duty Label Tab 5) Formatting

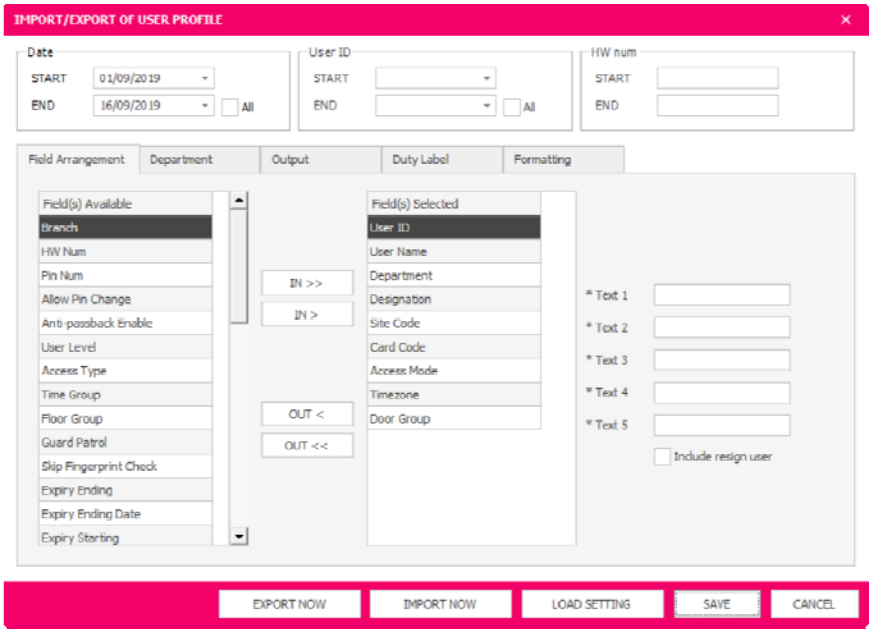


***Fig 8.4.1:* The field arrangement in import / export of user profile.**

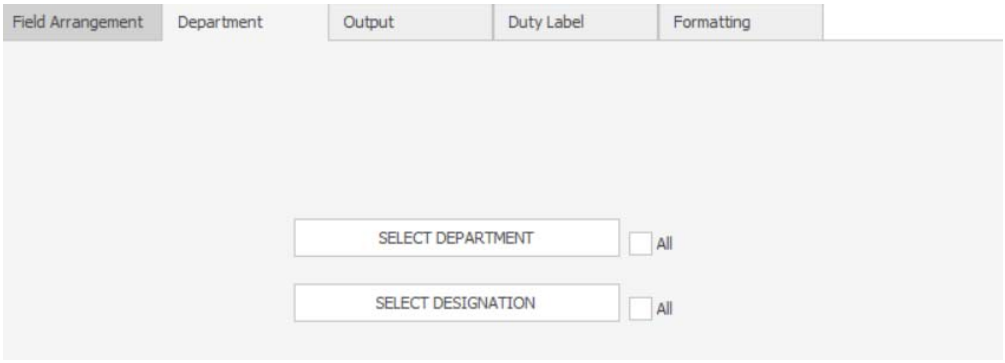


Fig 8.4.2: ***The departments in import / export of user profile.***

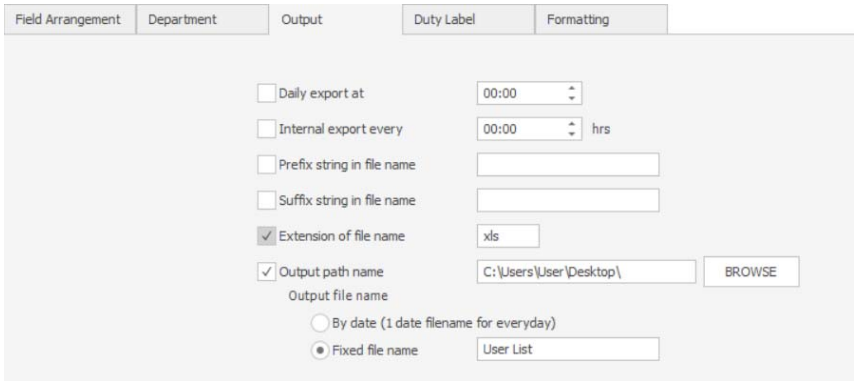


Fig 8.4.3: ***The output settings in import / export of user profile.***

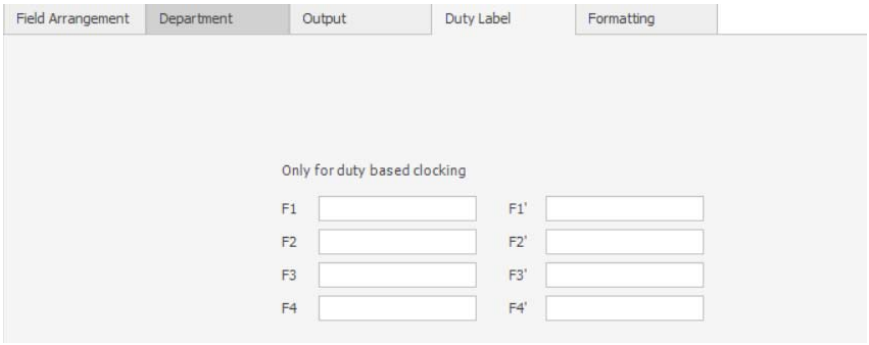


Fig 8.4.4: ***The duty label in import / export of user profile.***

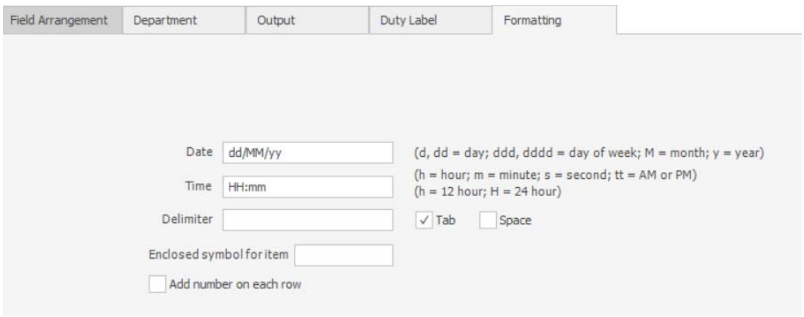


Fig 8.4.5: ***The output format in import / export of user profile.***

8.5 Import User Profile From 701Server

User profile can be imported through 701Server user card backup. The user profiles only able to be imported by following the format already define in the system. Any changes or mistake can cause the import process fail. Here are few conditions need to be achieved during import process:

- Not card duplicated happen
- Not user duplicated happen
- The users profile information must be filled correctly

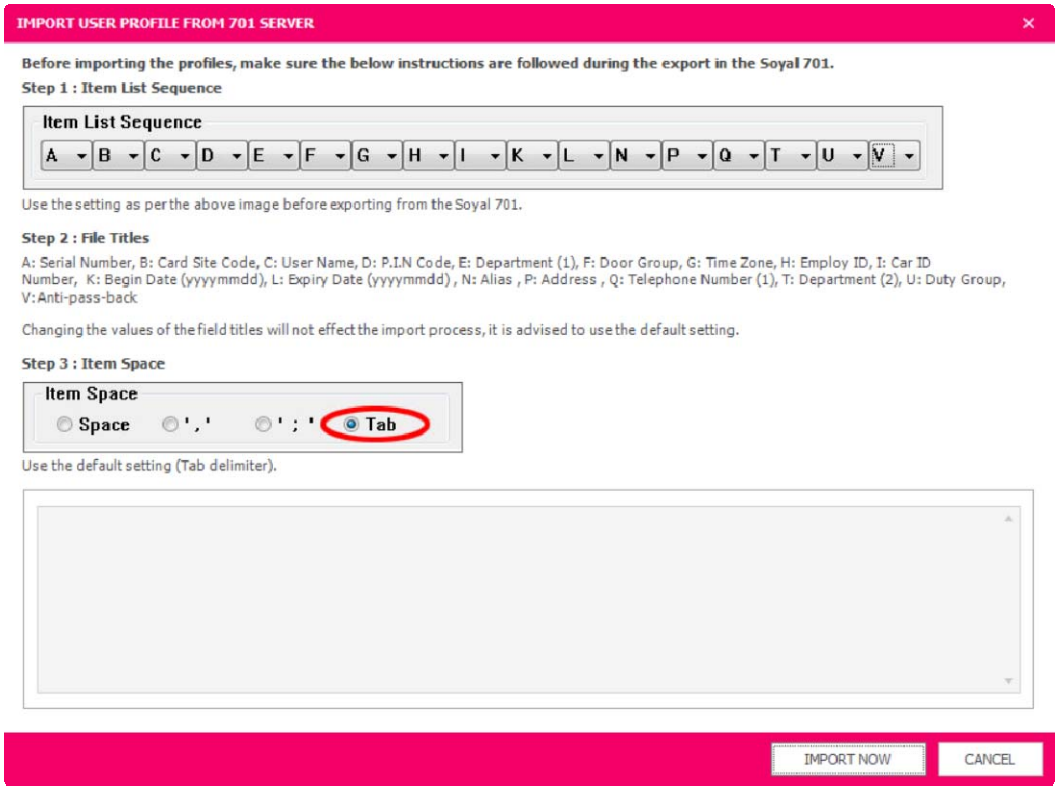


Fig 8.5.1: The users profile import from 701server.

8.6 Import User Profile From Text

User profile can be imported through text file, excel file or csv format file. The field arrangements need to be matched correctly. Here are few conditions need to be considered during import process:

- Not card duplicated happen
- Not user duplicated happen
- The users profile information must be filled correctly, mainly name, card number, address and so on.

Housekeeping → Import User Profile From Text

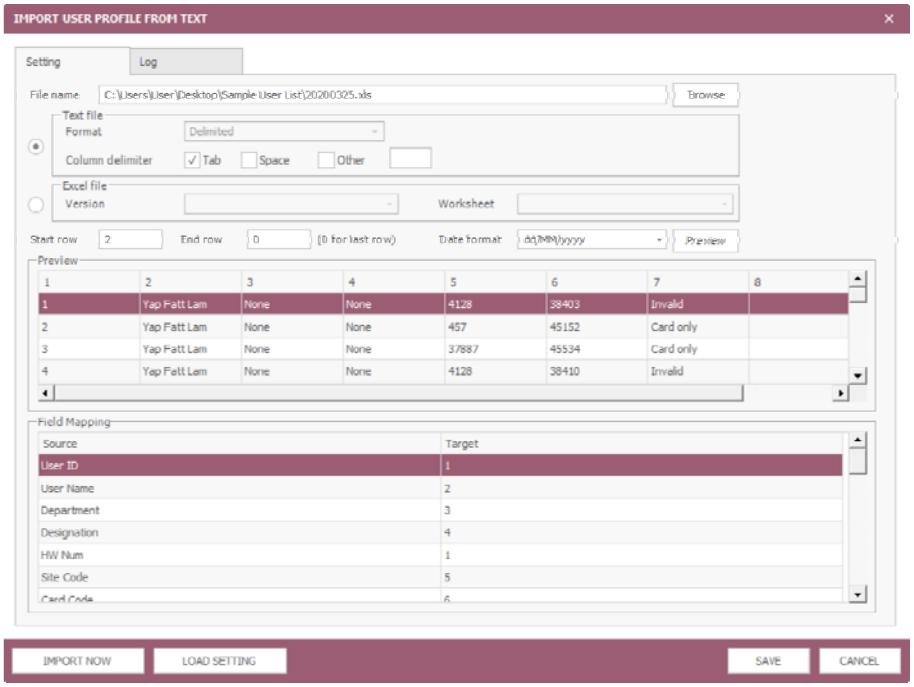


***Fig 8.6.1:* The users profile import from text.**

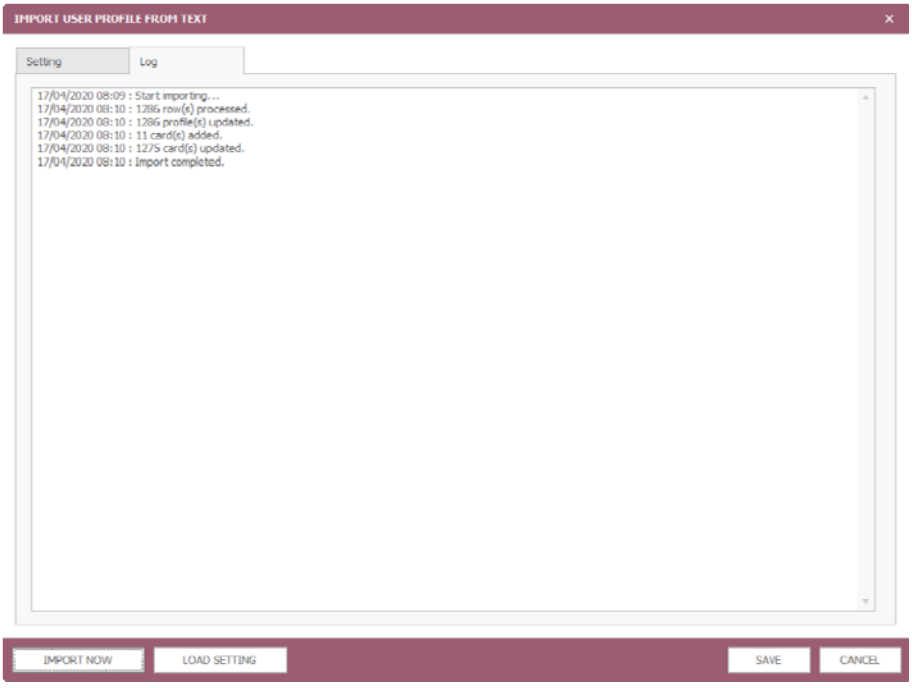


***Fig 8.6.3:* The results of users profile import process**

Adding Import User Profile From Text

1) Click on **Browse** button to open the user profile file (.txt, .xls, xlsx or .csv) wants to be imported.
2) Key in the *start row* and *end row* to be imported. Click on **Preview** button to see the imported file field.
3) Select and match the fields at *Target* column.
4) Click on **SAVE** button to save it and then select IMPORT NOW button to start users profile file import process. *(Refer Fig 8.6.1)*
5) All the result about users profile file import process is show in the Log tab. *(Refer Fig 8.6.3)*

Cancel Import User Profile From Text

1) Click on the **Cancel** button to reject any entries while Adding or Editing before.

8.7 Licensing Management

Each ME-ACS software purchased will come with a Serial Number. Serial number is prompt when you first run Client. Entering the serial number will register the software and process to initialize all parameters for first time run. Upon entering the serial number, you have 30 days to activate the software. Please send serial number, MAC address as displayed in Licensing Module to activate@soyal.com.my to request for activation key.

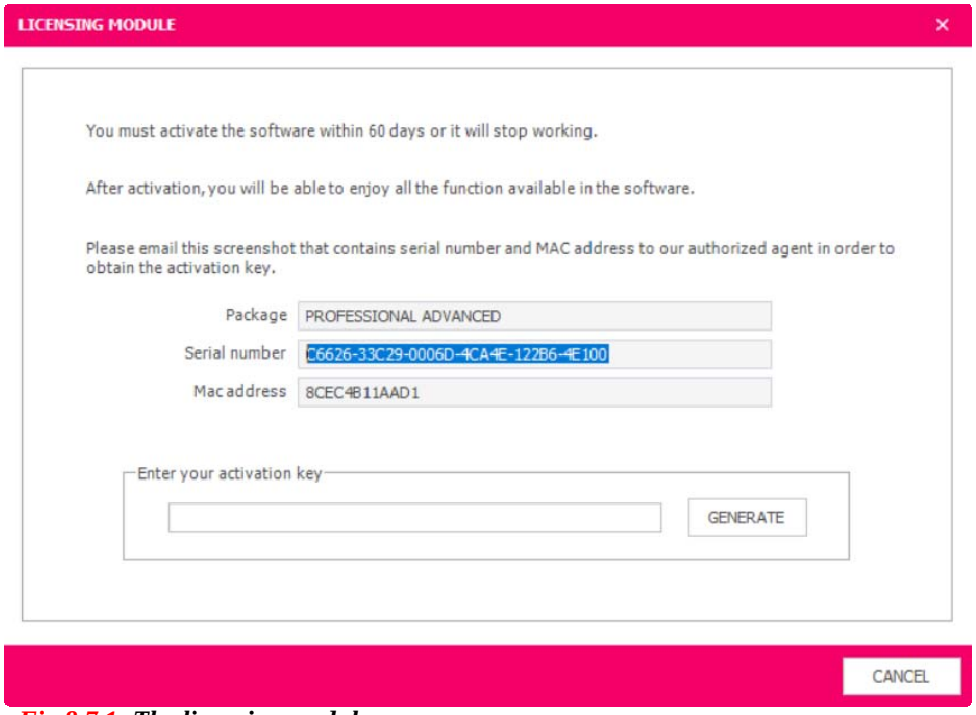


Fig 8.7.1: ***The licensing module.***

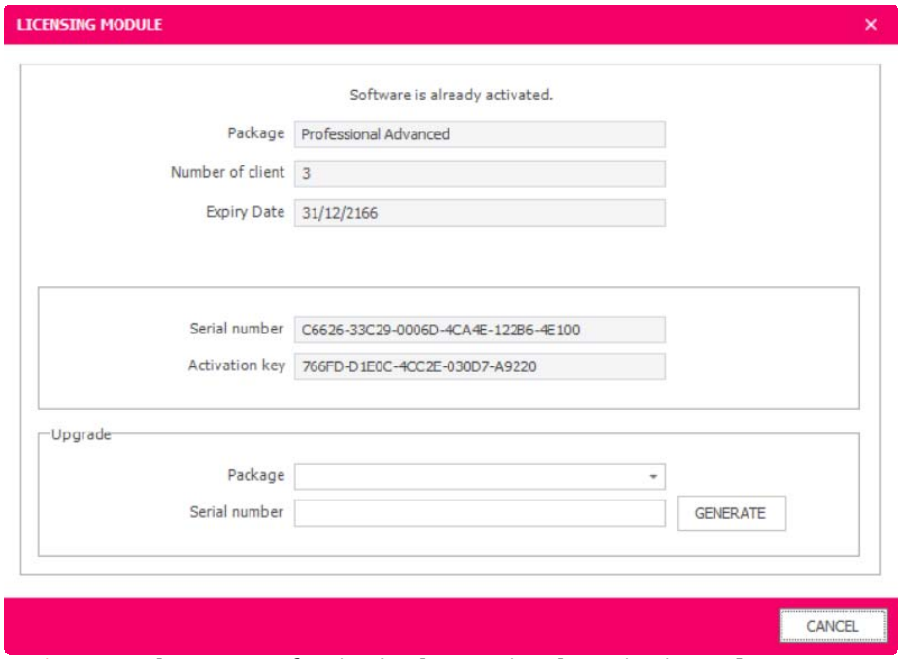


Fig 8.7.2: ***The process of activation by entering the activation code.***

Upon receiving the activation code, key in the activation code and click on the GENERATE button The next screen will show the software purchase details and expiry date. Every PC has a different MAC address therefore you will need to request activation key for every PC installed with ME-ACS Client. Activation keys for multiple clients will be listed out on display.

After purchasing a software upgrade, a new serial number will be given. Enter this new upgrade purchased and its serial number in the Upgrade section then click Generate. This will upgrade the current version. Upgraded version will need to be activated again with a new activation key. Therefore you have to submit new serial number, MAC address as displayed in licensing module together with company name to your dealer/installer to request for new activation key.

Support

You can find the latest product information, product updates, and answers to common questions at www.magnet.com.my

Copyright

The copyright and intellectual property rights of this software, MagEtegra, and all its documentation, including this online help system, are protected by copyright laws and international intellectual property right treaties. You may not copy any portion of the software or documentation in any form, except to use this software in accordance with the terms of the agreement or to make one copy for backup purposes. You may not alter the software in any way. If copies of the documentation must be made, you should make them in printed form only.