



FALCO

VAULT ENTERPRISE SITE

Software User Manual

Version 5.7.4

07/01/2020

Table of Contents

- Starting With Vault Enterprise Site..... 1**
 - Installation 1
 - Configuration File..... 7
 - Registration 8

- Starting With Transaction Server..... 10**
 - Sync with Vault VMS Cloud 10
 - Cloud Listing 12
 - Backup/ Restore Database..... 13
 - Import Card Data 14
 - VMS Integration 15

- Add Software User 16**
 - Add Tenant User 17

- Adding Controller 18**
 - Controller Setting..... 20
 - Network Configuration 23

- Fingerprint Device 24**
 - Fingerprint Enrollment..... 24
 - Fingerprint Utility..... 25

- Face Device 27**
 - Add Face Device 27
 - Face Access Level 28
 - Face Utility 29

License Plate Recognition	30
Installation LPR Software	30
Configuration LPR Setting	31
Adding LPR Camera	32
LPR Utility	33
Reader Bit Configuration.....	34
Time Zone	35
Lift Access Interval.....	37
Holiday.....	38
Card User	39
Group Controller Access Level	39
Group Lift Access Level	40
Department.....	41
Adding Card User	42
Access Level	44
Install Card.....	45
Manage Access Level of The Card.....	46
Temporary Reserve Card.....	47
Temporary Card.....	48
Download Utility	50
Upload Utility	51
Door Controls	52
Floor Plan.....	53
Floor Plan Online	54
Monitor Online.....	56
Event Configuration	58
System Setting.....	59
Reports.....	61

Additional Module	64
Global Antipassback.....	64
Fire Alarm.....	65
Group Delete Card	66
Integration with camera	67
Setting Work Time For Attendance	70
Working Time Configuration.....	70
Manual Entry.....	72
Attendance Reason	73

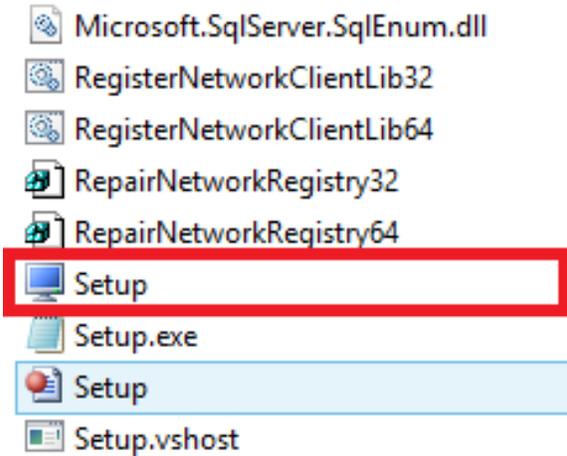


Starting VAULT Enterprise Site

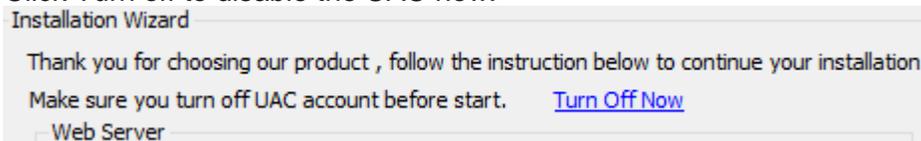


Software Requirements for the Enterprise Vault software Site / Central		
Operational System Approves	Software and Tools Needed	Approved Browser
Microsoft Windows 7 Professional SP1 (x86/x64) Microsoft Windows Server 2008 R2 (x86/x64) Microsoft Windows 8 Professional (x86/x64) Microsoft Windows 8.1 Professional (x86/x64) Microsoft Windows 10 Professional (x86/x64)	Microsoft Internet Information Service 5.1 o superior(IIS) Microsoft .Net Framework 4.5	Internet Explorer 11 Mozilla Firefox version 31.0 Google Chrome version 36.0.1985.143 (All With CCTV Integration)

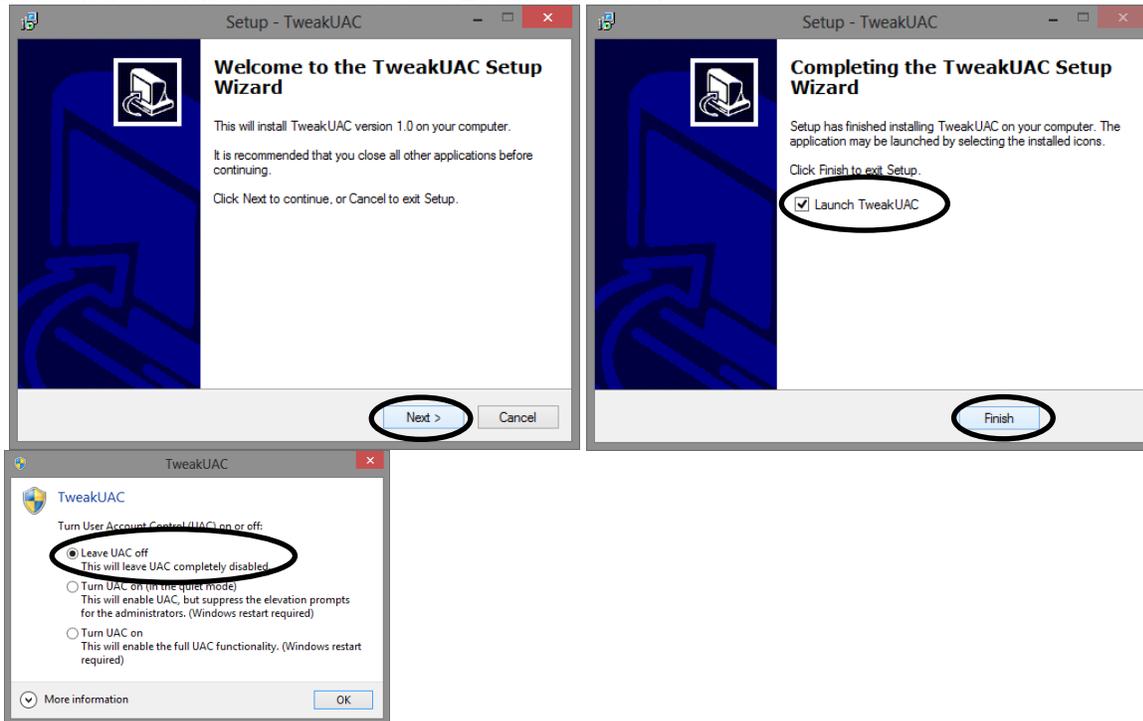
1. In the installation folder, click SETUP.EXE. Use the option to install as a system administrator.



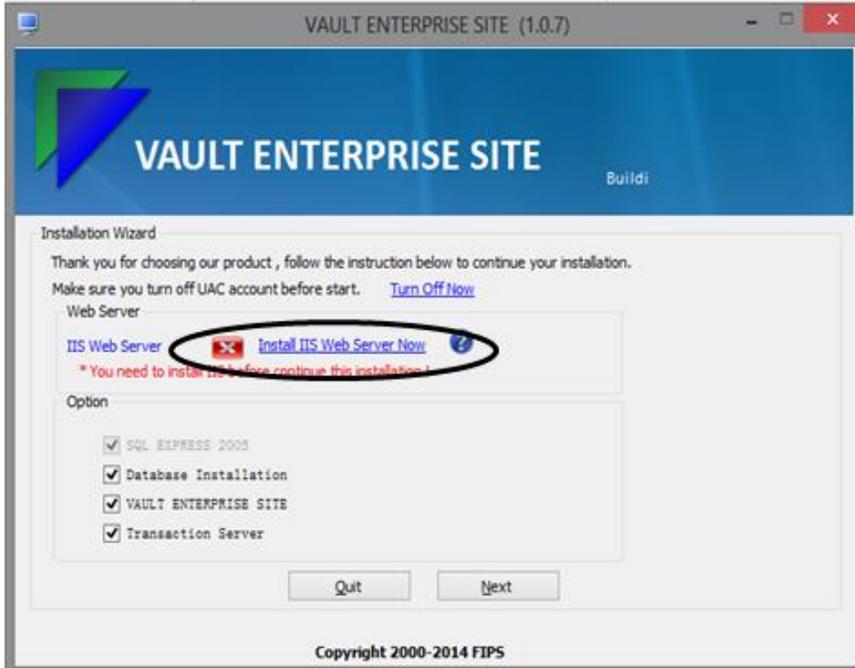
2. Click Turn off to disable the UAC now.



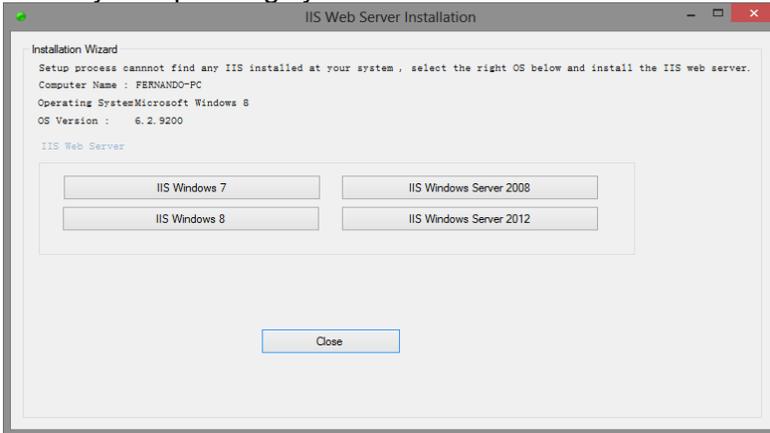
3. Install the software and select the Leave UAC Off.



4. For the Operation of Enterprise Vault, the Internet Information Service (IIS) must be installed. Click Install Now IIS Web Server to install.



5. Select your operating system and wait for the end of the installation.



6. Select all option and click next



7. Select where you want to install

Database Configuration

Computer Name : FERNANDO-PC
 Operating System : Microsoft Windows 8
 OS Version : 6. 2. 9200
 DB Server Name : FERNANDO-PC\SQLEXPRESS

Back Next

8. Installing SQL Server express

Microsoft SQL Server 2005 Setup

Installing Prerequisites
 Installs software components required prior to installing SQL Server.

SQL Server Component Update will install the following components required for SQL Server Setup:

- Microsoft SQL Native Client
- Microsoft SQL Server 2005 Setup Support Files

Configuring components...

Install Cancel

9. At the end of the installation, verify that all items are installed correctly.

Microsoft SQL Server 2005 Setup

Setup Progress
 The selected components are being configured

Product	Status
SQL Setup Support Files	Setup finished
SQL Native Client	Configuring components...
SQL VSS Writer	
SQL Server Database Services	

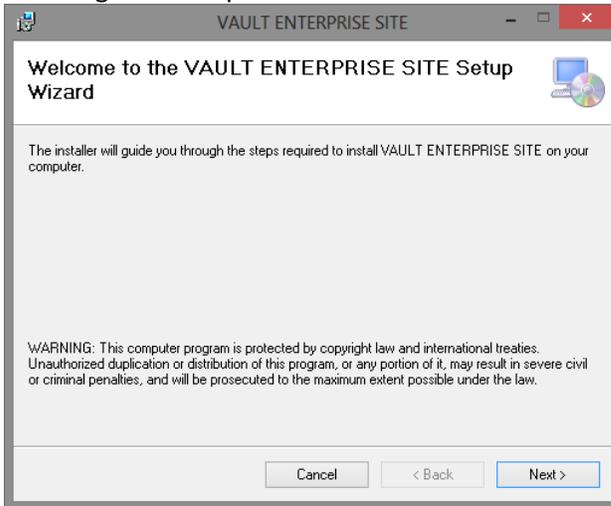
Status

Copying new files

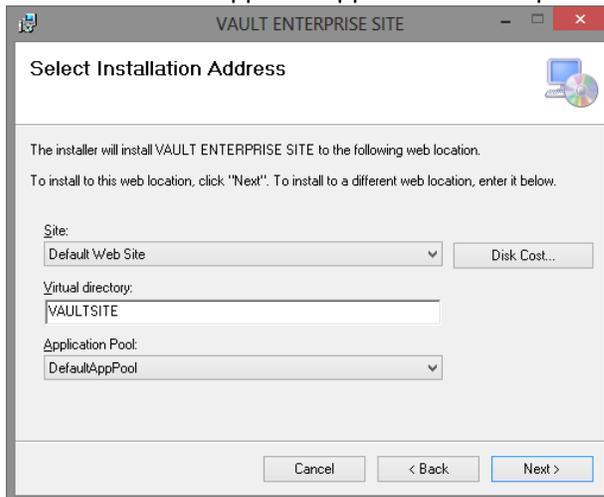
File: msmd.h, Directory: C:\Program Files\Microsoft SQL Server\90\SDK\Ind...: 37774

Help << Back Next >> Cancel

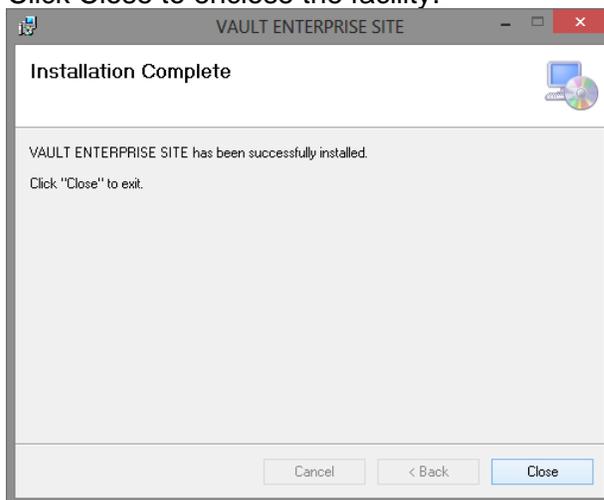
10. Installing the Enterprise Vault Site software. Click Next to install.



11. Select the DefaultAppPool Application Pool option and click Next



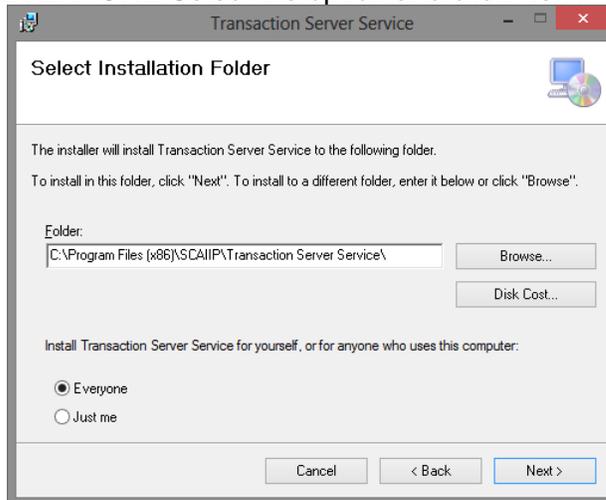
12. Click Close to enclose the facility.



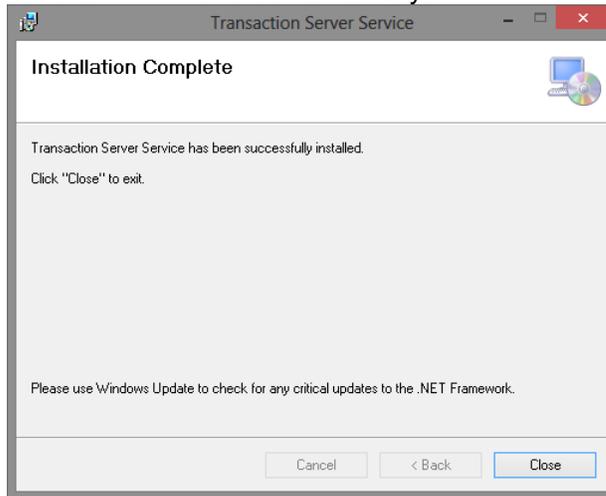
13. Installing the Service Transaction Server software. Click Next to install.



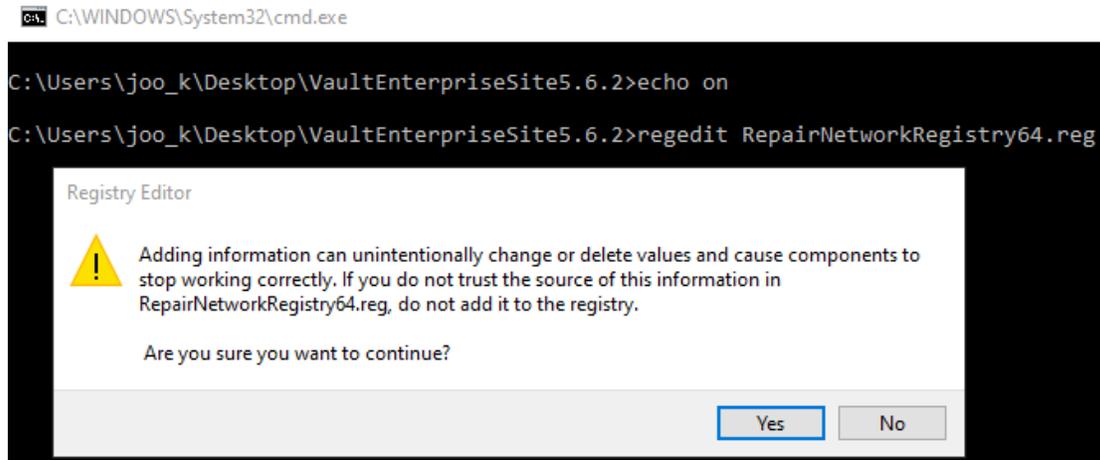
14. **EVERYONE** Select the option and click Next.



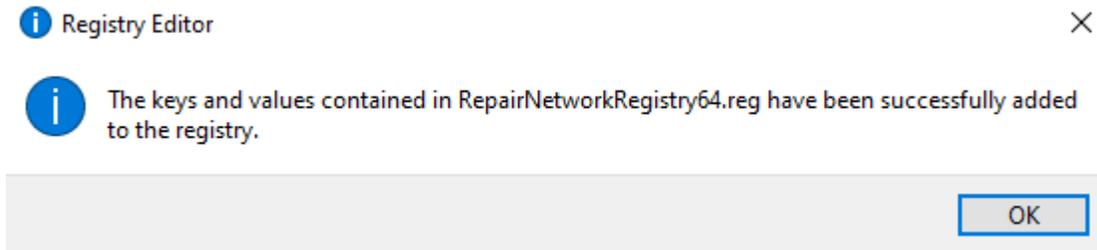
15. Click Close to enclose the facility.



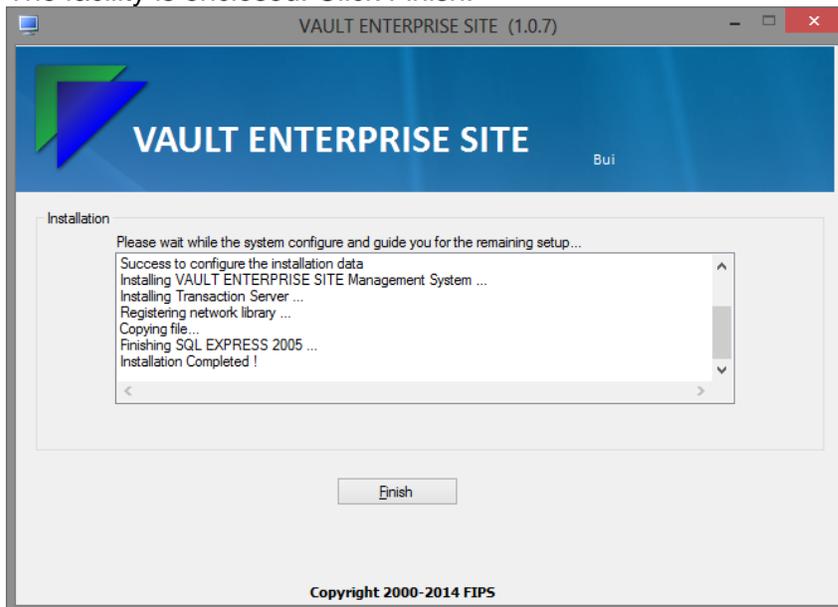
16. Click Yes to continue register the registry file



17. Check if registry was made successfully

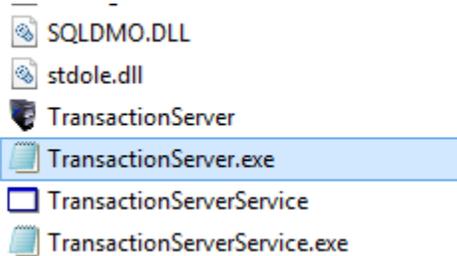


18. The facility is enclosed. Click Finish.

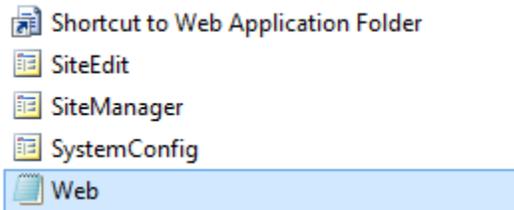


1. If the installation is divided in two servers, an application and a database, we must change two files connection to the database, they are:

- TransactionServer.exe.config
C:\Program Files (x86)\VAULT\Transaction Server Service



- Web.config
C:\inetpub\wwwroot\VAULTSITE



TransactionServer.exe.config

```

</setting>
<setting name="FVMSConnStr" serializeAs="String">
  <value>server=. \SQLEXPRESS;uid=sa;pwd=passw@rd1234;database=VisDB</value>
</setting>
<setting name="ConnStr" serializeAs="String">
  <value>server=. \SQLEXPRESS;uid=sa;pwd=passw@rd1234;database=DataDBEnt</value>
</setting>

```

Server = Database \ Instance
Uid= user database

Pwd= user's password database
Database= Name of the database

Web.config

```

<add key="ReportMaxDays" value="60"/>
<add key="connStr" value="server=. \SQLEXPRESS;uid=sa;pwd=passw@rd1234;database=DataDBEnt"/>
<add key="CamServer" value="N"/>
<add key="GT" value="No"/>

```

Server = Database \ Instance
Uid= user database

Pwd= user's password database
Database= Name of the database

1. Open Vault Site with any Browser



2. Setup Administrator for Vault Enterprise Site

**Never use id:admin | password: admin

Welcome - VAULT ENTERPRISE SITE

VAULT® English

* First time login detected, please enter your unique administrator Login ID and Password to continue.

New Login ID :*
Enter you New Login ID

New Password :*
Enter your new password

Retype Password :*
Retype your new password

Continue

2020 © Copyright by VAULT

3. Login with Administrator account

Login Screen - VAULT ENTERPRISE SITE

VAULT® English

Login ID :* ! Name is required
Enter you Login ID

Password :* ! Please enter your password
Enter your password

Login

2020 © Copyright by VAULT

4. Setup Site Management Credential, click save after finish filling

Site Management

Welcome, make sure you register the below correct information during the first time setup. Once saved, it can not be changed.

Site Setting

Site Code:* OFFA

Site Description: OFFICE

Site GMT:* (UTC+08:00) Kuala Lumpur, Singapore

Site Port No:* 2003

Site Reader Mode:* 03 - Wiegand 34 bits (with)

Type: Network NDVR

URL: Enter NDVR URL if applicable

Login ID: NDVR Login ID Login Password:

Country:* Malaysia

Address:

Adjunct:

City: State:

Postal Code: Email:

Phone: Extension:

Fax No:

Contact Person: Mobile No:

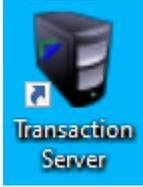
Remark:

5. Appear Vault Enterprise Site Dashboard

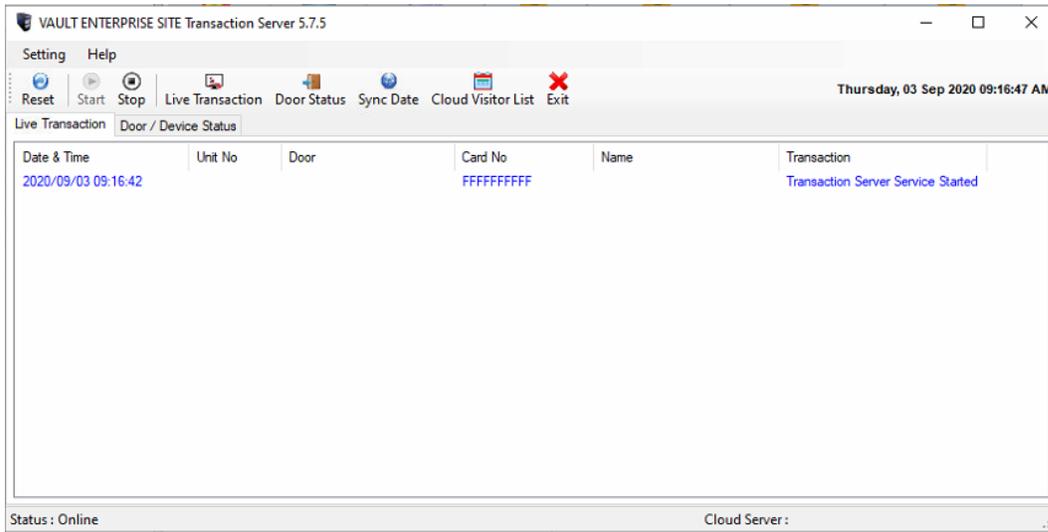
The dashboard features a top navigation bar with icons for Live Transaction, Card User, Controller, Door Control, Floor Plan, Control Panel, Report, and Logout. A 'Quick Access' sidebar on the left lists these same functions. The main dashboard area is divided into several sections:

- Welcome:** Displays site statistics: Total Site Registered: 1, Total Card Registered: 0, Total Controllers Registered: 0, and Card Due To Expiry: 0.
- Recent joined staff:** A table with one empty row.
- Calendar:** Shows the current date as Friday, July 3, 2020, with a digital clock at 12:26:36. It includes a calendar grid for July 2020 and an 'Upcoming Holiday' section.
- Latest News:** A section titled 'Upcoming birthdays' with one empty row.

1. Open Transaction Server

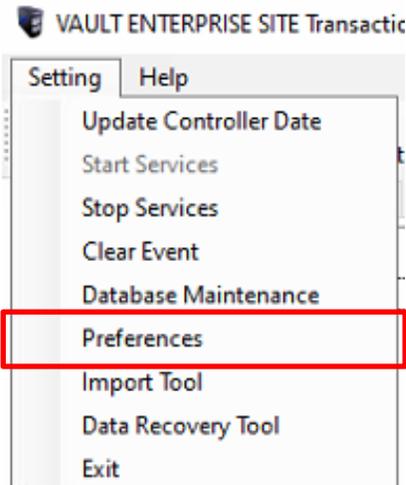


2. Select the START button to start the service of communication with the database.

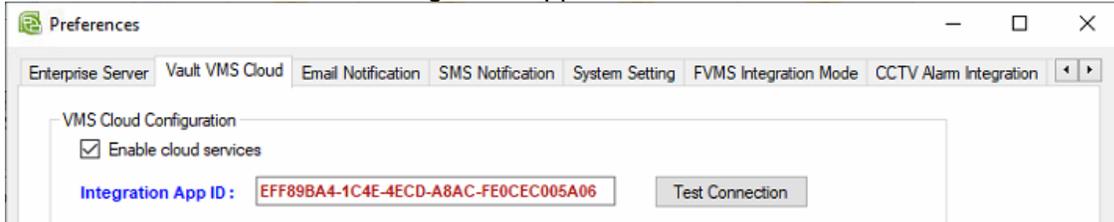


Sync with Vault VMS Cloud

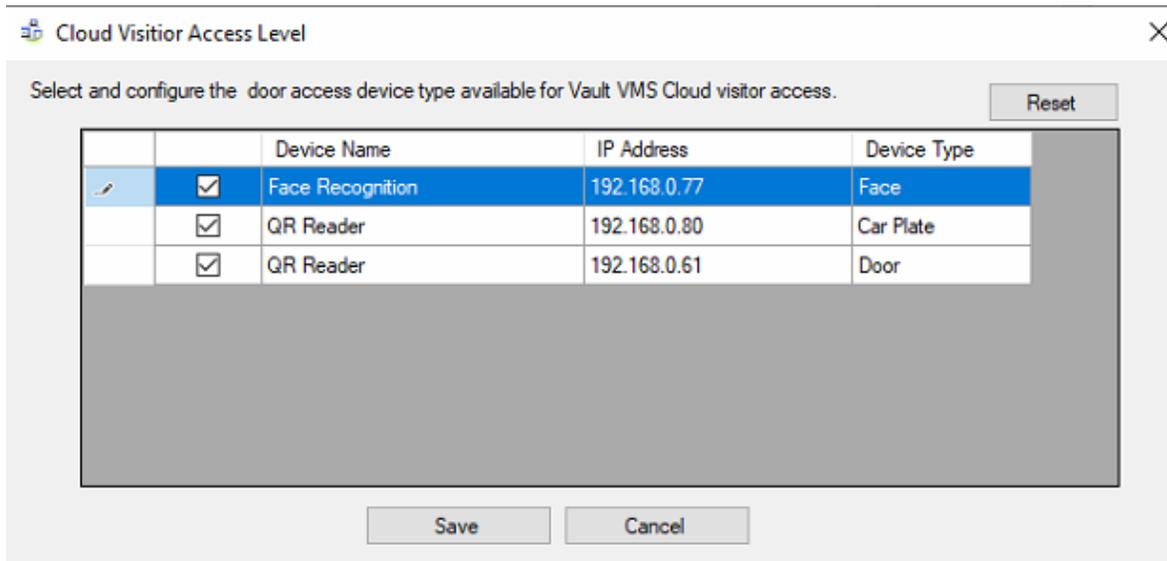
1. Go to setting > Preference > Vault VMS Cloud



2. Enable cloud services, insert Integration Apps ID and test the connection



3. Set Cloud Visitor Accessible Device to enable controller, LPR and face reader for visitor Integration. Tick enable QR code, Car Plate & Face Reader as you provide



Cloud Visitor Listing

1. Go to Cloud Visitor List in main page



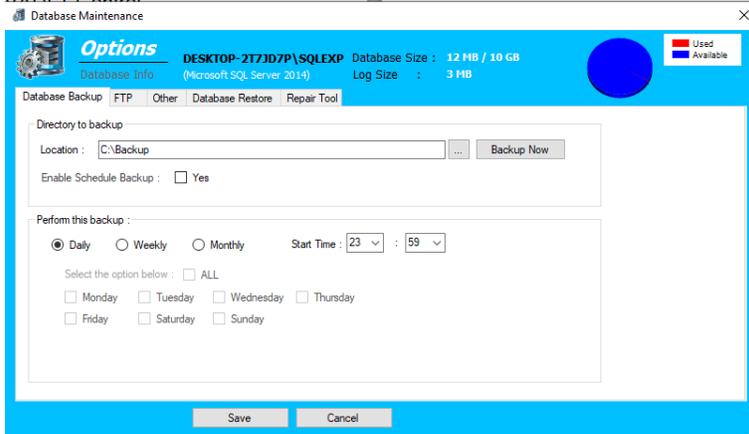
2. Admin can see all visitor active here, we can redownload back visitor to controller by click **Refresh**

The screenshot shows the 'Cloud Visitor List' application window. It includes a legend with 'Pending' (red) and 'Downloaded' (green) status indicators. The table below lists visitor information, with a refresh icon highlighted in a red box in the 'Is Download' column for the 'joe' entry.

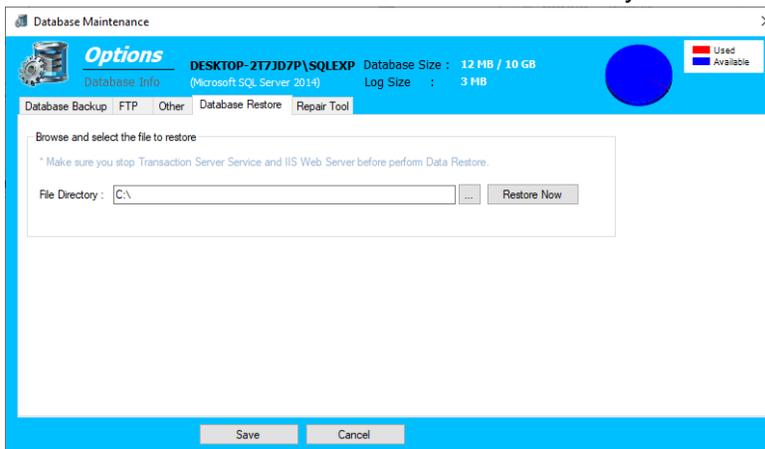
Name	ID No / Passport No	Vehicle No	Visit Date	Visit Date End	Contact No	Host Name	Is Download
joe		VBW8908	03-Sep-2020 08:47	03-Sep-2020 11:17		Izzat, Rahman	<input checked="" type="checkbox"/>
joji		KL2020	03-Sep-2020 09:03	03-Sep-2020 11:33		Izzat, Rahman	<input checked="" type="checkbox"/>

Backup/Restore Database

1. Go to Setting> Database Maintenance> Database Backup

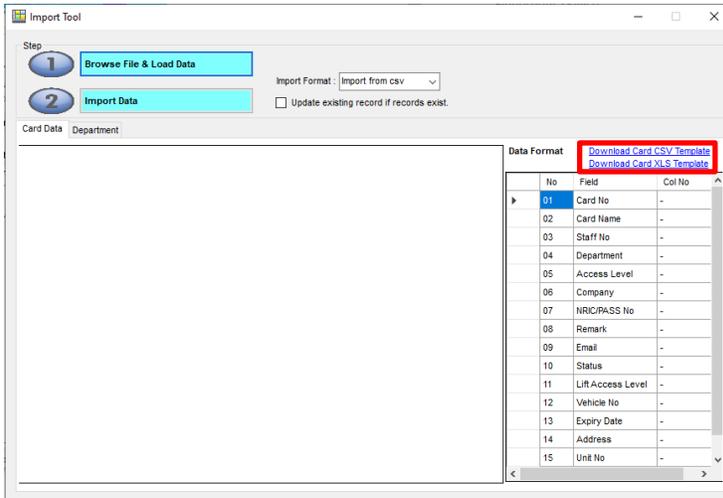


2. Select folder **make sure in c drive and click backup now
 3. For schedule backup, just click daily for everyday backup with start time
 4. To restore database, go to Setting> Database Maintenance> Database Restore
- **make sure the database in c** choose directory and click restore now



Import Card Data

1. Go to Setting> Import Tools> Database Backup
2. Download card CSV/XLS Template



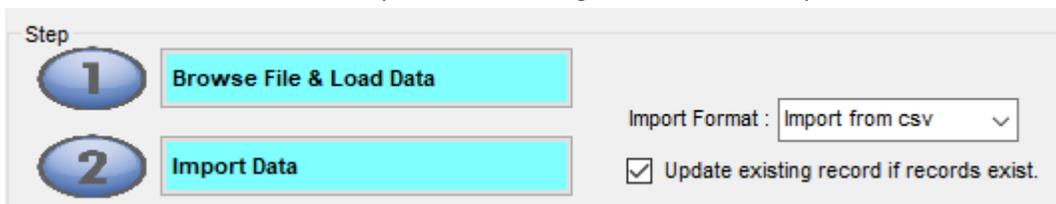
3. Find the file at Desktop



4. Fill in Card credential and save the file

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Card No #	Card Nam	Staff No	[I] Departme	Access Lev	Company	NRIC/Pass	Remark	[I] Email	[Ma] Status	[Tr] Lift Access	Vehicle N	ExpiryDat	Address	[Unit No]
12345	User1	EMP1000	New Depa	1	Your Com	888888-88	Remark H	test@em	TRUE	1	WWW8888		Add	Unit
12346	User2								TRUE	1				
12347	User3	EMP1001	New Depa	2	Your Com	888888-88	Remark H	test@em	TRUE	1	WWW8889		Add	Unit
12348	User4								TRUE	1				
12349	User5	EMP1002	New Depa	3	Your Com	888888-88	Remark H	test@em	TRUE	1	WWW8890		Add	Unit
12350	User6								TRUE	1				
12351	User7	EMP1003	New Depa	4	Your Com	888888-88	Remark H	test@em	TRUE	1	WWW8891		Add	Unit
12352	User8								TRUE	1				
12353	User9	EMP1004	New Depa	5	Your Com	888888-88	Remark H	test@em	TRUE	1	WWW8892		Add	Unit
12354	User10								TRUE	1				
12355	User11	EMP1005	New Depa	6	Your Com	888888-88	Remark H	test@em	TRUE	1	WWW8893		Add	Unit
12356	User12								TRUE	1				

5. Browse and load the file, Tick Update for existing user then click Import Data



6. Browse and load the file, Tick Update for existing user then click Import Data

7. The data already Inside the Vault Enterprise Site

Import Tool

Step 1 **Browse File & Load Data**

Step 2 **Import Data**

Import Format : Import from csv

Update existing record if records exist.

Card Data Department

	Col1	Col2	Col3	Col4	Col5	Col6
▶	12345	User1	EMP10000	New Department	1	Your Co
	12346	User2				
	12347	User3	EMP10001	New Department	2	Your Co
	12348	User4				
	12349	User5	EMP10002	New Department	3	Your Co
	12350	User6				
	12351	User7	EMP10003	New Department	4	Your Co
	12352	User8				
	12353	User9	EMP10004	New Department	5	Your Co
	12354	User10				
	12355	User11	EMP10005	New Department	6	Your Co
	12356	User12				

Visitor Management System Integration

1. Go to Setting> Preference> FVMS Integration mode

Enterprise Server | Email Notification | SMS Notification | System Setting | **FVMS Integration Mode** | CCTV Alarm Integration | Atte

Enable Integration with FVMS

FVMS Database Connection

Server Instance Name : .\SQLEXPRESS

Login ID : sa

Password :

Test Connection

2. Tick Enable Integration with FVMS and test the connection

3. Click okay if the connection successful and save

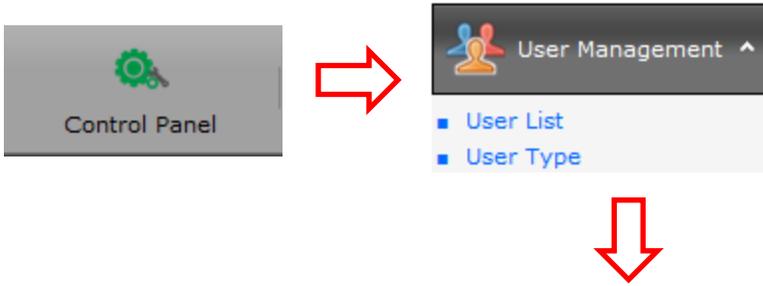
System - Test Connection

i Connect Successfull !

OK

Add Software User

1. Go to Control Panel > User Management > User Type



User Type

Drag a column header here to group by that column

<input type="checkbox"/>	No	User Type	Description
<input type="checkbox"/>	1	Enterprise System Admin	Enterprise System Admin

2. Here you can add new types of users with permissions distinct

User Type

User Type:

Description:

General Module **Tool & Other**

<input type="checkbox"/> All	<input type="checkbox"/> View	<input type="checkbox"/> Add	<input type="checkbox"/> Edit	<input type="checkbox"/> Delete	<input type="checkbox"/> Export
Site Manager	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Card User	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Temporary Card	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Temporary Access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Temporary Card Reserv List	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Controller	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Time Zone	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Time Set	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Lift Access Interval	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Holiday	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Alarm holiday	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Floor Plan	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System User	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System User Type	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Type of User

Permits

3.

Add Software User

Add Tenant User



Tenant User Access List

No	Login ID	Company Name
1	tenant	complicated

2. Here you can add new types of Tenant users with few controls only.

Tenant User Access

User Detail

User Login ID :

Login Password:

Company Detail

Company Name:

Building: Floor / Unit No:

Address 1:

Address 2:

Office No: Ext:

Fax No: Contact Person:

Remark:

Door Access Controller Group

Door Controller:

User must change password at next login

User cannot change password

Password never expires

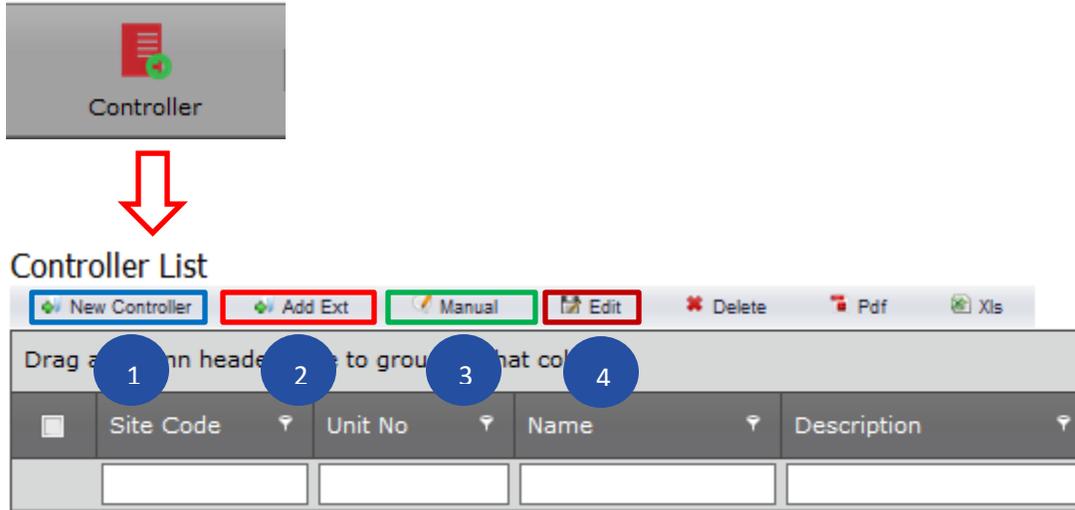
Account is disabled

Tenant ID and Password

Selected Controller only

Save and User is ready to Login to the software

1. Go to Controller

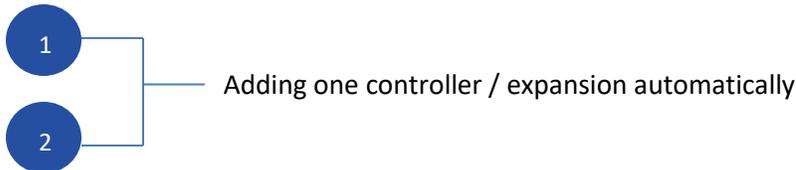


2. Add ID 0 controller *first door* using the automatic search for the Broadcast command.

3. Add ID 1 controller *second door* using the automatic search for the Broadcast command.

4. Add ID 0 or 1 controller using *manual IP* UDP unicast

5. Edit controllers.



Network

Controller Detected : 192.168.0.99 . Change the setting to your desired network configuration and press next to continue.

IP Address*	192.168.0.99	Firmware*	TS.99.6A957F1
Mac Address*	0:0:21:74:213:99	Subnet Mask*	255.255.255.0
Gateway*	192.168.0.1	Dest TCP Port*	1008
Server IP Address*	192.168.0.140	SRC UDP Port*	2003
SRC IP*	255.255.255.255	Info Desk Port*	2003
Info Desk IP*	255.255.255.255		

Next >>>



Controller Searching

IP Address	Mac Address	Firmware	Type	Controller ID	Status
192.168.0.99	0:0:21:74:213:99	TS.99.6A957F1	D	0	●
192.168.0.54	0:26:21:43:144:54	RS.91.6A957F1	D	0	●
192.168.0.50	0:26:21:53:212:50	RS.91.6A957F1	D	0	●
192.168.0.51	0:26:21:53:212:51	RS.91.6A957F1	D	0	●
192.168.0.200	0:50:21:113:124:200	RS.99.6A957F1	D	0	●
192.168.0.201	0:50:21:113:124:201	TS.99.6A957F1	D	0	●
192.168.0.47	0:50:21:13:201:47	TA.99.6205AFL	S	0	●
192.168.0.44	0:50:21:13:204:44	TA.99.6205AFL	D	0	●

Refresh Add Cancel



Sistema

Cancelar

Notas : Por favor, espere cuando los datos son procesados en el sistema. No oprima el botón Volver o cierre hasta que termine.

3 → Adding one controller / manual expansion.

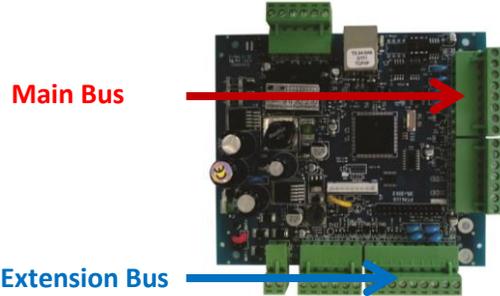
Controller Wizard

Please enter the controller IP Address you want to register. Door Wizard w

Controller IP Address :

Controller Type : Main Bus Next >>

- Main Bus
- Extension Bus



Network

Controller Detected : 192.168.0.99 . Change the setting to your desired network configuration and press next to continue.

IP Address:*	<input type="text" value="192.168.0.99"/>				
Mac Address:*	<input type="text" value="0.0.21.74.213.99"/>	!	*	Firmware:*	<input type="text" value="T5.99.6A9STFI"/>
Gateway:*	<input type="text" value="192.168.0.1"/>	!	*	Subnet Mask:*	<input type="text" value="255.255.255.0"/>
Server IP Address:*	<input type="text" value="192.168.0.140"/>	!	*	Dest TCP Port:*	<input type="text" value="1008"/>
SRC IP:*	<input type="text" value="255.255.255.255"/>			SRC UDP Port:*	<input type="text" value="2003"/>
Info Desk IP:*	<input type="text" value="255.255.255.255"/>			Info Desk Port:*	<input type="text" value="2003"/>

<< Back
Next >>

Adding a controller

1. Adding a controller / manual expansion.

General Module.

Controller Profile

192.168.0.99 :

Controller Details
Setting
Network Configuration
Camera Setting
Alarm Config
IO Config

Controller Name: *

Description: *

Site Control: * OFFA Unit No: *

IP Address: Mac Address:

Controller ID: Firmware:

Controller Status : Active

Controller Type

Alarm: I/O: Lift:

LCD: Rack:

2. The Menu and other tools

192.168.0.99 :

Controller Details	Setting	Network Configuration	Camera Setting	Alarm Config	IO Config
Controller Configuration					
Open Time (s) : <input type="range" value="5"/>		Release Time (s) : <input type="range" value="2"/>			
Open Time (s) : <input type="text" value="5"/>		Release Time (s) : <input type="text" value="2"/>			
Lock Release TZ: <input type="text" value="00"/>		Push Button TZ: <input type="text" value="01"/>			
Antipassback: <input type="text" value="00"/>		Global Antipassback Group: <input type="text" value="Disable"/>			
Rack Control: <input type="text" value="1-16"/>					

Open Time : How long can the door be left open until an alarm is generated.

Release Time: time relay control lock.

Lock Release TZ : Can be programmed a TZ for the lock becomes unlocked for that time period. 00 -> Always shut / 01-> Always released.

Antipassback: Each parent has antipassback location that can be enabled by TZ. (anti dual input / dual output).

Push Button TZ: TZ to release the door by Button (00 -> Always disabled / 01-> Always enabled).

Global Antipassback Group: When we have more than one way to enter / exit a room and want to make the control antipassback, you must create a group with controllers belonging to this environment. Ex .: Group turnstiles reception.

Control of Rack: Only used for Rack controllers.

3. The menu tools and other

Mode

Fire Alarm: <input type="checkbox"/> Enable	Guard Tour: <input type="checkbox"/> Enable
Buzzer Door Release: <input type="checkbox"/> Enable	Card Lockout: <input type="checkbox"/> Enable
Auto Pin Access: <input type="checkbox"/> Enable	Report Mode: <input type="checkbox"/> Enable
Emergency Card Mode: <input type="checkbox"/> Enable	

Card & Pin

Card & Pin : Enable

Card & Pin Entry TZ:

Card & Pin Exit TZ:

Mode

Fire Alarm : Enables parent to be part of a group of fire.

Open Door Buzzer: Enables or disables buzzer during Lock Release TZ.

Auto Pin: Enables password function to the parent. Passwords up to 10 pre-programmed by the parent.

Guard Tour : Enables guard tour controller .

Card Lock : Blocks user card after 3 attempts to circumvent the antipassback.

Report Mode : Writes markings point in text format, separating them by day.

Emergency Card Mode : special card, when touched onto a reader on a specific controller, will trigger the “security off”

Card & Pin

Card & Pin: Enables dual authentication for card use and password. (* Keyboard should work in Rosslare format)

Card & Pin Entry TZ : set the time to enable card and pin mode by TZ for the entry reader.

Card & Pin Exit TZ: set the time to enable card and pin mode by TZ for the Exit reader.

4. The Menu tools and other tools

Dual Card Mode

Dual Card: Enable

Entry Reader Dual Card TZ: Exit Reader Dual Card TZ:

Pin No

1.) Pin No: <input type="text" value="0000"/>	TZ: <input type="text" value="00"/>	6.) Pin No: <input type="text" value="0000"/>	TZ: <input type="text" value="00"/>
2.) Pin No: <input type="text" value="0000"/>	TZ: <input type="text" value="00"/>	7.) Pin No: <input type="text" value="0000"/>	TZ: <input type="text" value="00"/>
3.) Pin No: <input type="text" value="0000"/>	TZ: <input type="text" value="00"/>	8.) Pin No: <input type="text" value="0000"/>	TZ: <input type="text" value="00"/>
4.) Pin No: <input type="text" value="0000"/>	TZ: <input type="text" value="00"/>	9.) Pin No: <input type="text" value="0000"/>	TZ: <input type="text" value="00"/>
5.) Pin No: <input type="text" value="0000"/>	TZ: <input type="text" value="00"/>	10.) Pin No: <input type="text" value="0000"/>	TZ: <input type="text" value="00"/>

Double Authentication Mode

Double Authentication : Enables dual authentication to the parent. This feature is specific to the firmware T5.96DAFI.

Entry Reader Dual Card TZ: Enables authentication for double entry into a particular TZ configured by the user.

Exit Reader Dual Card TZ : Enables authentication to double Exit in a given TZ configured by the user.

Pin No

Per controller, we can have up to 10 pre-programmed passwords for access in a particular time zone. To use this feature you need to use a keyboard and enable Auto Pin mode.

5. Config Network Configuration

192.168.0.99 :

Controller Details	Setting	Network Configuration	Camera Setting	Alarm Config	IO
<input type="button" value="Retrive Network Setting"/> <input type="button" value="Set Network Setting"/>					
IP Address:	<input type="text" value="192.168.0.99"/>				
Mac Address:	<input type="text" value="0.0.21.74.213.99"/>	Firmware:	<input type="text" value="T5.99.6A9STFI"/>		
Gateway:	<input type="text" value="192.168.0.1"/>	Subnet Mask:	<input type="text" value="255.255.255.0"/>		
Server IP Address:	<input type="text" value="192.168.0.140"/>	Dest TCP Port:	<input type="text" value="1008"/>		
SRC IP:	<input type="text" value="255.255.255.255"/>	SRC UDP Port:	<input type="text" value="2003"/>		
Info Desk IP:	<input type="text" value="255.255.255.255"/>	Info Desk Port:	<input type="text" value="2003"/>		

IMPORTANT

After modifying the parameters of the parent network, the user must click the Set Network Configuration to the new parameters are sent to the controller.

To learn the current configuration of the network controller, the user must click on the Retrive Network Setting

6. Camera Setting

192.168.0.99 :

Controller Details	Setting	Network Configuration	Camera Setting	Alarm Config	IO Config
Entry Camera:	<input type="text" value="Null"/>	<input type="text" value="Null"/>	<input type="text" value="Null"/>		
Exit Camera:	<input type="text" value="Null"/>	<input type="text" value="Null"/>	<input type="text" value="Null"/>		

You can add a camera input and output for each parent, so that when the access is kept a log of the event with video. (Images are always stored in the CCTV server.)

Adding Fingerprint Reader

1. Go to setting > Fingerprint > Fingerprint Device

Fingerprint Device

Detail

Site Code:	<input type="text" value="OFFA"/>	
Device Name:	<input type="text" value="192.168.0.110"/>	
IP Address:	<input type="text" value="192.168.0.110"/>	
Port No:	<input type="text" value="4370"/>	Model: <input type="text" value="ZK B&W"/>
Status:	<input checked="" type="checkbox"/> Active	

2. After configure the device details, click Save

Fingerprint Enrollment

3. Go to setting > Fingerprint > Fingerprint Enrollment



Use USB fingerprint device to use this module

Fingerprint Registration

Click the browse button to select the card user.

Site Code:

1. Browse card user
2. Tick Fingerprint 1 and enroll 1st Fingerprint
3. Tick Fingerprint 2 to enroll 2nd Fingerprint

	Position	
Card No:	Department:	Staff No:
Mobile No:	Joining Date:	NRIC:
Email:		Home No:
		Age:

Fingerprint Enrolled

Fingerprint 1: Fingerprint 2:

Fingerprint Utility

4. Go to setting > Fingerprint > Fingerprint Utility

Fingerprint Utility

Utility Option

Site Code: OFFA

- Download Fingerprint
- Delete Fingerprint
- Upload Fingerprint
- Clear all fingerprint

Fingerprint Device List

<input type="checkbox"/>	Device Name	IP Address	Port No	Site Code
<input type="checkbox"/>				
<input type="checkbox"/>	192.168.0.110	192.168.0.110	4370	OFFA

Next >>

Download to send fingerprint template to fingerprint device

Delete to delete all fingerprint template inside the system

Upload to callback fingerprint template from fingerprint device and backup to system

Clear to clear all fingerprint

Fingerprint Utility

Action

Download Fingerprint

Device Selected

Device: 192.168.0.110

Card Detail

Card No: 0000040886

<< Back Start >>

5. Select certain User

Fingerprint Utility

Action

Upload Fingerprint
Upload & Backup to System

Device Selected

Device: 192.168.0.110

<< Back

Start >>

6. Click start to take the template

Adding Face Recognition Reader



1. Add Device Information

Details Network Configuration

Device Name: * Face Recognition

Description: * Stand Alone

Site Control: * jo Unit No: * 1

IP Address: 192.168.0.155 Password: *****

Dest IP: 192.168.0.9

Device Status: Active

Time Zone

Device Time Zone: Asia/Kuala_Lumpur

Controller Configuration

Release Time (ms): 500	Multi-Face Detection: Recognize Multiple Faces
Recognition Distance: No limits	Recognition Score: 80
Recognition Interval: 0	Stranger Voice Mode: No Voice Announcement
Stranger Detection: <input checked="" type="checkbox"/>	Stranger Voice Customization: Unauthorized Access
Stranger Threshold: 3	Voice Customization: {name}
Voice Mode: No Voice Announcement	Display Customization: {name}
Display Mode: Display Name	Wiegand Output: Disable
Liveness: <input type="checkbox"/>	
Enable Transaction: <input checked="" type="checkbox"/>	

2. Change Device IP

Details Network Configuration

Set Network Setting.

LAN Network

IP Address: 192.168.0.144

Subnet Mask: 255.255.255.0

Gateway: 192.168.0.1

DNS: 255.255.255.255

DHCP:

3. Click network setting and save

Face Access Level

1. Go to setting > Face Device > Face Access Level



2. Set to 01 for free access

Access Level Setting

Group Access No:* 01

Description: Free Access

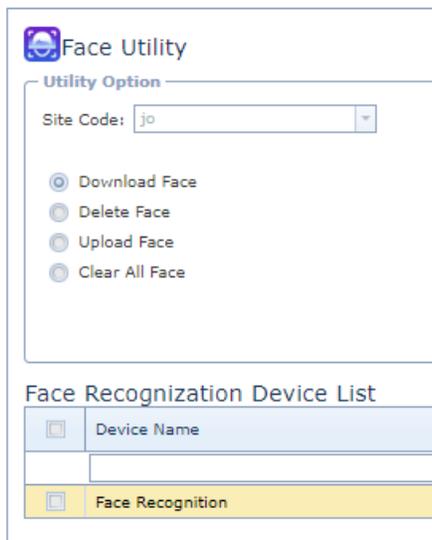
#	Face Device	Time Set
<input checked="" type="checkbox"/>	Face Recognition	01

3. Click Save

Face Utility



1. Go to setting > Face Device > Face Access Level



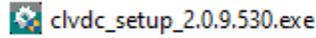
2. Click download/ Delete/ Upload or clear all face from device



3. Select card and continue click Start

4. To add Face, Add new card and Upload Image via webcam or device

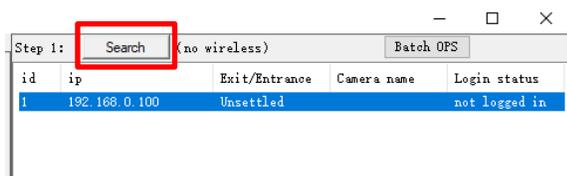
Install LPR Software



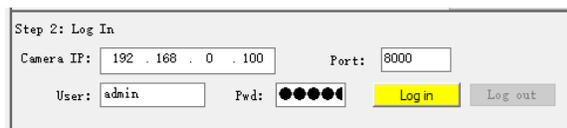
1. Vault Installation File > LPR Software > Run Above Software for camera configuration



2. After Installation, open the software

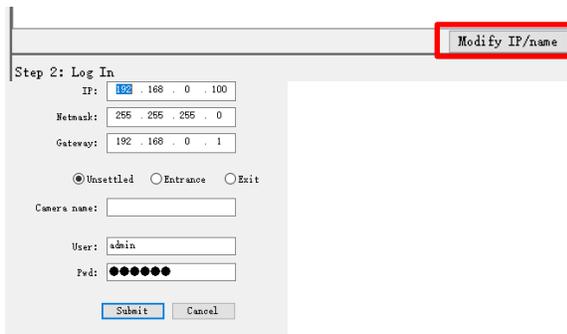


3. Search the LPR camera with Lan **skip this step if already know the device IP



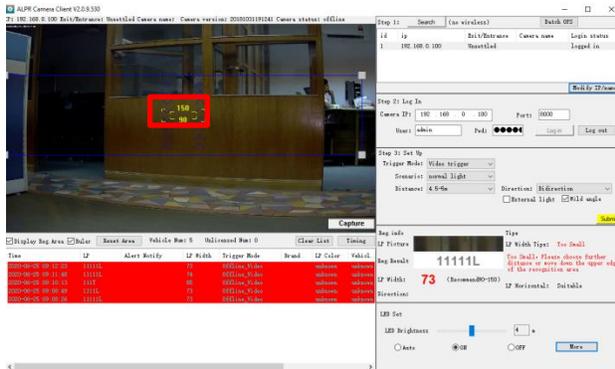
User: **admin** | Password: **123456**

4. Login with Camera IP, Port No, User and Password

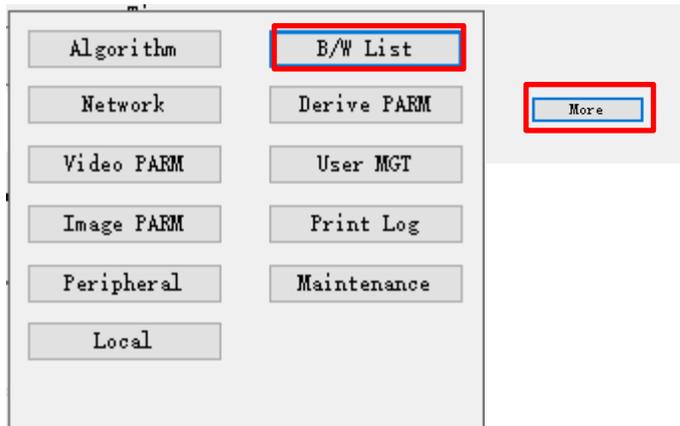


5. Modify to change IP and Password

Configure LPR Setting



6. The Live feed is on, adjust yellow box to detect Vehicle License plate



7. Click more for more option and choose B/W List



8. Make sure to tick controlled gate all the time for white list and submit

9. Go to More > Local > time settings |Synchronize time to sync camera with local time

Device Date: 2020-06-25 Device Time: 09:21:16 **Time synchronized**

Local Date: 2020-06-25 Local Time: 09:21:17

Synchronized with NTP NTP server IP address: 192.168.55.166

10. The Cam is ready to add on VAULT

Adding LPR Camera

Video Camera

- Camera Server
- Camera List
- Live Feed Monitoring
- Car Plate Integration**
- Car Plate Utility

1. Go to setting > Video Camera > Car Plate Integration

Car Plate Binding

Access Controller:* LPR

Description:* Entry

Camera Brand: FALCO Direction: Entry

Site Control:* jo

Camera Network Setting

IP Address:* 192.168.0.89 Port No:* 8000

Login ID:* admin Password:* 123456

Save Cancel

2. Fill in all LPR credential

3. Save

Car Plate Utility

Video Camera ^

- [Camera Server](#)
- [Camera List](#)
- [Live Feed Monitoring](#)
- [Car Plate Integration](#)
- [Car Plate Utility](#)

1. Go to setting > Video Camera > Car Plate Utility

Car Plate Utility

Utility Option

Site Code:

Download Vehicle No
 Delete Vehicle No
 Clear All Vehicle No

Car Plate Camera Device List

	Device Name	IP Address
<input type="checkbox"/>	CAR PARK CTRL	192.168.0.94
<input type="checkbox"/>	LPR	192.168.0.89

2. Tick Download/ delete and clear all the vehicle no.

3. Click LPR Camera then next

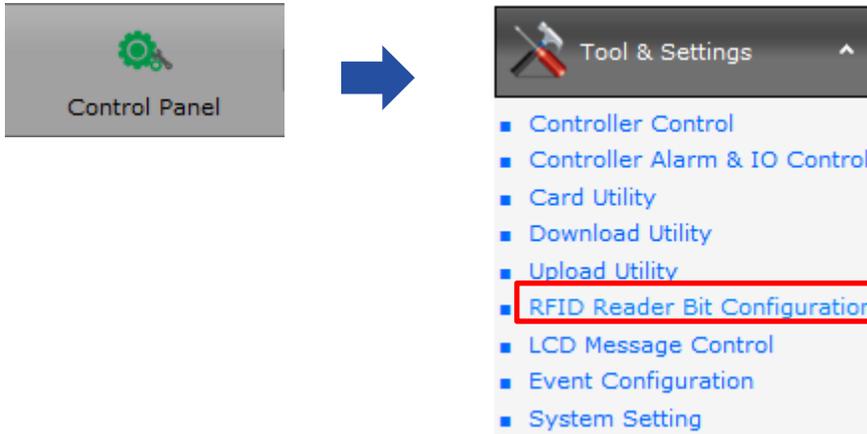
Card Detail

Card No:

4. Select Card and continue click Start

5. To register user car plate no. Go to card user list > Plate No.

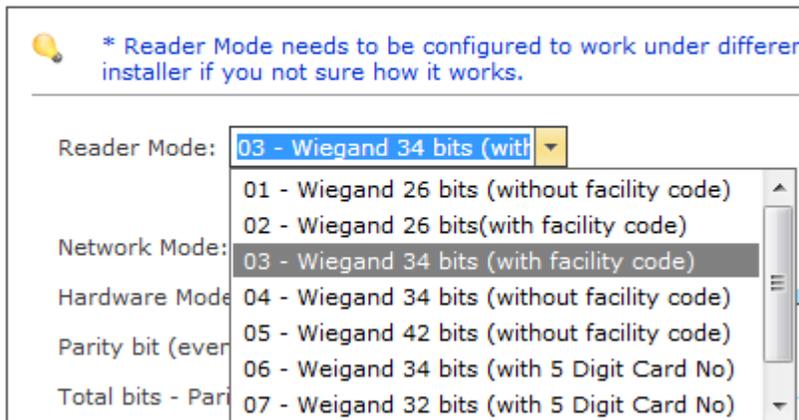
1. Go to control panel > Tools & Setting > RFID Reader Bit Configuration



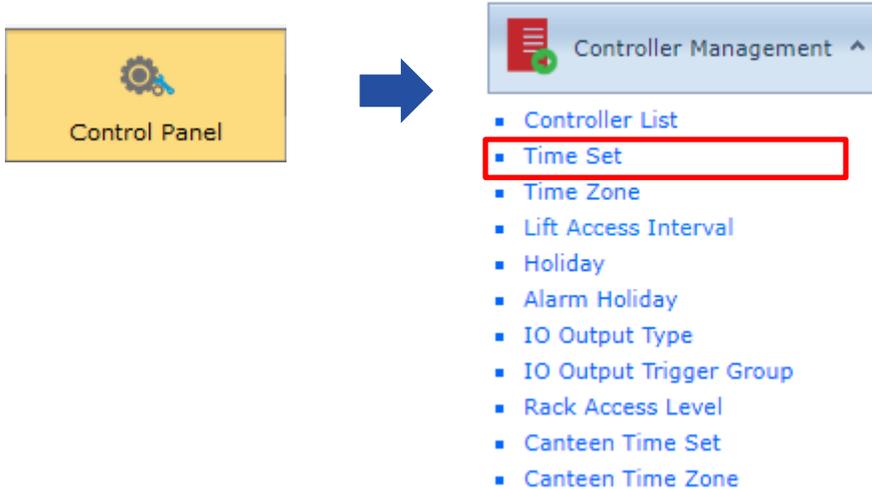
2. Protocols available to controllers

Wiegand 26, 32 , 34 or 42 bits

Settings



1. Go to control panel > Controller Management > Time Set



2. Create new Time Set

The screenshot shows a table with the following data:

Time Set No	Time Interval 01	Time Interval 02	Time Interval 03	Description
00	00:00 - 00:00	00:00 - 00:00	00:00 - 00:00	No Access Time Set
01	00:00 - 23:59	00:00 - 00:00	00:00 - 00:00	Free Access Time Set

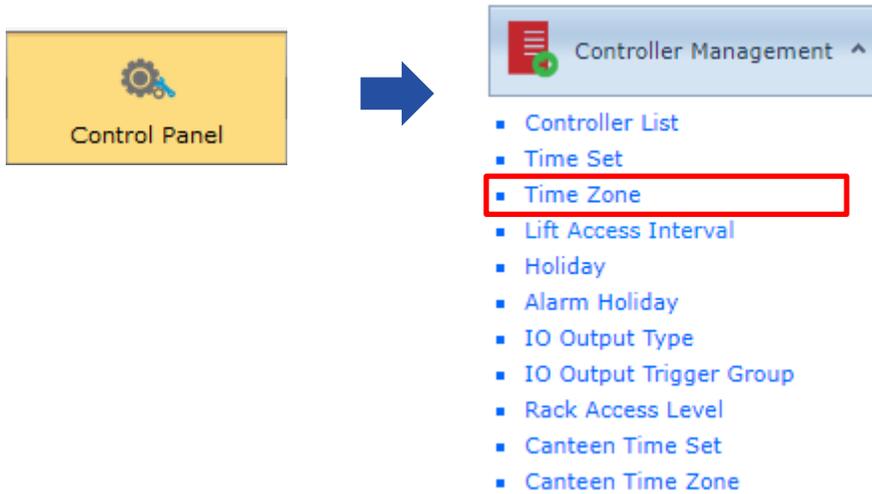
Controller Time Set

The 'Timer Setting' form contains the following fields:

- Time Set No: * 2
- Description: Enter time set description ..
- Interval 1: From 00:00 To 00:00
- Interval 2: From 00:00 To 00:00
- Interval 3: From 00:00 To 00:00

You can store up to 99 Time Set on the controller settings, and each can have up to three valid intervals.

1. Go to Control Panel > Controller Management > Time Zone



2. Create new time zone

Controller Time Zone

Time Zone

Time Zone No:

Description:

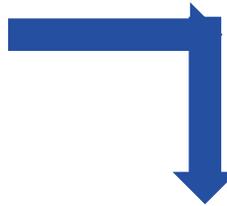
Week View

Monday: Friday:

Tuesday: Saturday:

Wednesday: Sunday:

Thursday:



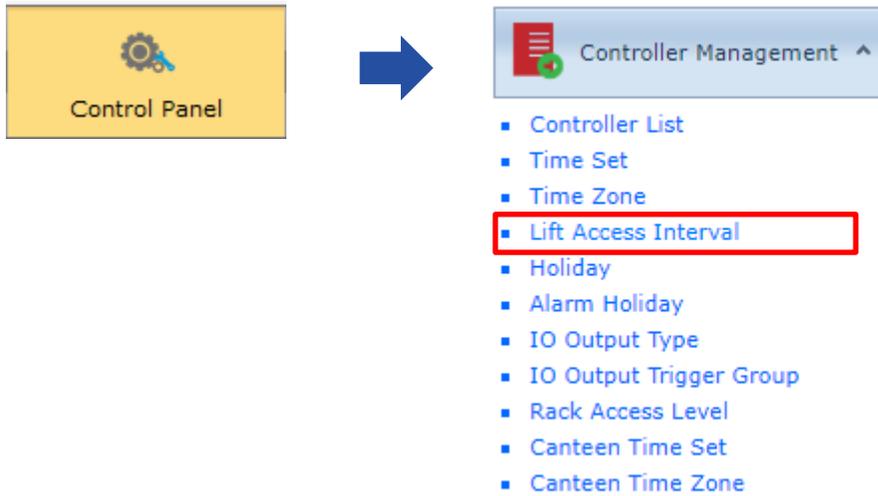
Time Zone Detail

Time Zone No : 02

Day	Time Set No:	Time Setting Value		
Monday	02	08:00 - 17:00	00:00 - 00:00	00:00 - 00:00
Tuesday	02	08:00 - 17:00	00:00 - 00:00	00:00 - 00:00
Wednesday	02	08:00 - 17:00	00:00 - 00:00	00:00 - 00:00
Thursday	02	08:00 - 17:00	00:00 - 00:00	00:00 - 00:00
Friday	02	08:00 - 17:00	00:00 - 00:00	00:00 - 00:00
Saturday	00	00:00 - 00:00	00:00 - 00:00	00:00 - 00:00
Sunday	00	00:00 - 00:00	00:00 - 00:00	00:00 - 00:00

In this example, the User TZ will be Monday to Friday working hours using previously created, and weekend and holidays will default to 00 (No Access) level.

1. Go to control panel > Controller Management > Lift Access Time Zone



2. Create new Lift Access Interval and this is example to set lift interval

Controller Lift Interval

Lift Interval Setting

Site Code:*

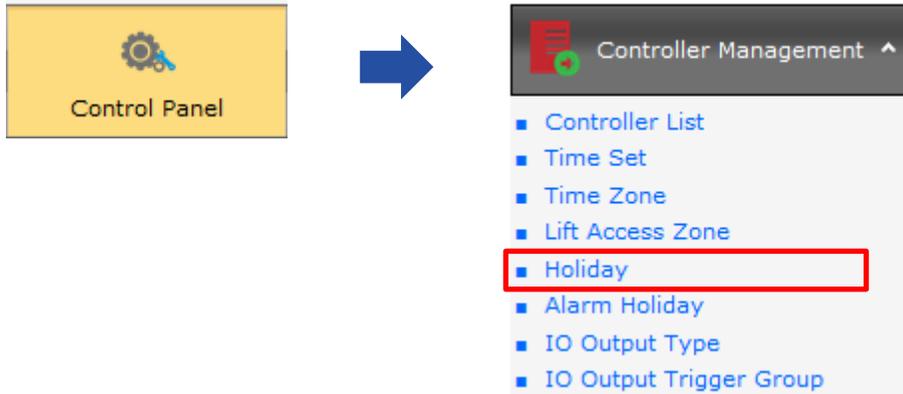
Lift Interval No:*

Description:

Interval 1	Interval 2	Interval 3
Floor / Level From <input type="text" value="03"/>	Floor / Level From <input type="text" value="05"/>	Floor / Level From <input type="text" value="00"/>
To <input type="text" value="03"/>	To <input type="text" value="06"/>	To <input type="text" value="00"/>

Interval 4	Interval 5	Interval 6
Floor / Level From <input type="text" value="00"/>	Floor / Level From <input type="text" value="00"/>	Floor / Level From <input type="text" value="00"/>
To <input type="text" value="00"/>	To <input type="text" value="00"/>	To <input type="text" value="00"/>

1. Go to controller > Controller Management > Holiday



2. In this example, on 24/12 and 25/12 will be considered as a holiday. In this case, for visitors and contractors. Employees to be obeyed their respective TZ.

Holiday

Holiday Detail

Holiday Name:

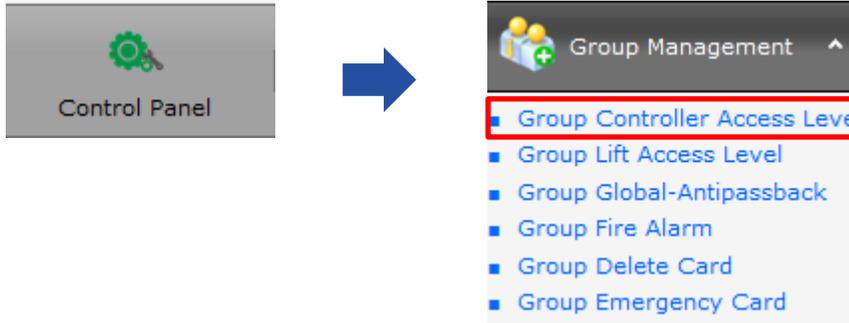
Site Code:

Date

From	Month	Day
	12	/ 24
To	Month	Day
	12	/ 25
Time Set :	<input type="text" value="00 - No Access Time Set"/>	

Group Controller Access Level

1. Go to Control Panel > Group Management > Group Controller Access Level



2. Create Group for Free Access level because it is mandatory.

Add the controllers for each pattern group you want to create, placing their desired time zone for each parent. Can add up to 999 standard groups.

IMPORTANT: To delete an access level, we must clear the controller, delete the description and click Save.

Group Access Level

Controller Access Setting

Group No: 01 (Total : 4 Controller)			Site Code: <input type="text" value="KLA TECH SDN BHD"/>																																
<table border="1"> <tr> <td>office main door</td> <td>KLA TECH SDN BHD</td> <td>01</td> </tr> <tr> <td>office staircase</td> <td>KLA TECH SDN BHD</td> <td>01</td> </tr> <tr> <td>store</td> <td>KLA TECH SDN BHD</td> <td>01</td> </tr> <tr> <td>testing 1234</td> <td>KLA TECH SDN BHD</td> <td>00</td> </tr> </table>	office main door	KLA TECH SDN BHD	01	office staircase	KLA TECH SDN BHD	01	store	KLA TECH SDN BHD	01	testing 1234	KLA TECH SDN BHD	00	Group Access No: <input type="text" value="01"/>	Description: <input type="text" value="All Access"/>	<table border="1"> <thead> <tr> <th>Controller</th> <th>Description</th> <th>Site Code</th> <th>Time Zone</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>office main door</td> <td>KLA TECH SDN BHD</td> <td><input type="text" value="01"/></td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>office staircase</td> <td>KLA TECH SDN BHD</td> <td><input type="text" value="01"/></td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>store</td> <td>KLA TECH SDN BHD</td> <td><input type="text" value="01"/></td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>testing 1234</td> <td>KLA TECH SDN BHD</td> <td><input type="text" value="00"/></td> </tr> </tbody> </table>	Controller	Description	Site Code	Time Zone	<input checked="" type="checkbox"/>	office main door	KLA TECH SDN BHD	<input type="text" value="01"/>	<input checked="" type="checkbox"/>	office staircase	KLA TECH SDN BHD	<input type="text" value="01"/>	<input checked="" type="checkbox"/>	store	KLA TECH SDN BHD	<input type="text" value="01"/>	<input checked="" type="checkbox"/>	testing 1234	KLA TECH SDN BHD	<input type="text" value="00"/>
office main door	KLA TECH SDN BHD	01																																	
office staircase	KLA TECH SDN BHD	01																																	
store	KLA TECH SDN BHD	01																																	
testing 1234	KLA TECH SDN BHD	00																																	
Controller	Description	Site Code	Time Zone																																
<input checked="" type="checkbox"/>	office main door	KLA TECH SDN BHD	<input type="text" value="01"/>																																
<input checked="" type="checkbox"/>	office staircase	KLA TECH SDN BHD	<input type="text" value="01"/>																																
<input checked="" type="checkbox"/>	store	KLA TECH SDN BHD	<input type="text" value="01"/>																																
<input checked="" type="checkbox"/>	testing 1234	KLA TECH SDN BHD	<input type="text" value="00"/>																																
> Group No: 02 (Total : 3 Controller)																																			
> Group No: 03 (Total : 3 Controller)																																			
> Group No: 04 (Total : 3 Controller)																																			

Group Lift Access Level

1. Go to Control Panel > Group Management > Group Lift Access Level



2. Tick on the controllers for the group, and select the timezone

Group Lift Access Level

Lift Access Setting

Site Code:

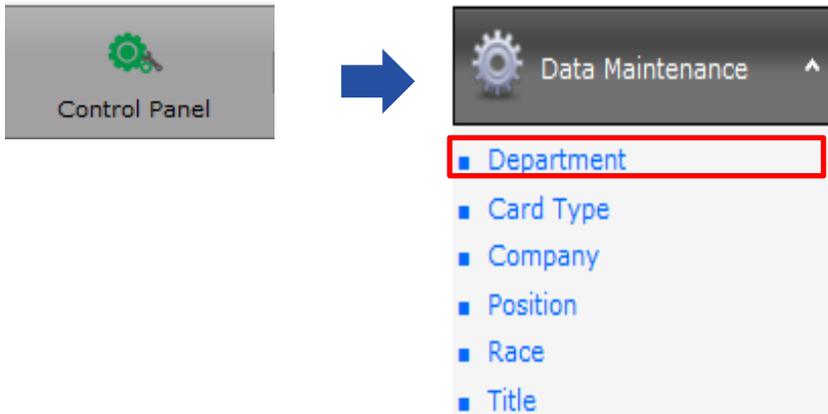
Group Access No:*

Description:

#	Controller	Description	Site Code	Time Zone
<input checked="" type="checkbox"/>	lift		Joo Site	02

Time Zone	Description
00	No Access Lift Zone
01	Free Access Lift Zone
02	level 3 , 5 & 6

1. Go to Control Panel > Data Maintenance > Department

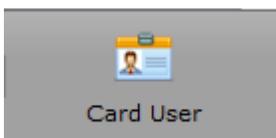


2. First, we register all departments, types of word cards, Company, Position, Race and Title, then do the card registration

Department List

Drag a column header here to group by that column			
No	Department Code	Description	
1	Department	Department	
2	AD	ADMIN	
3	ACC	ACCOUNT	

3. Go to Card User



Card User List

4. New Card Batch Add Edit Delete Back Pdf Xls

- New Card** – Add new card
- Batch Add** – Add batch of cards (Ex. 1 - 1000)
- Edit** – to edit card
- Delete** – to delete card
- PDF** – export to PDF
- Xls** – export to Excel

5. Upload or scan thru Webcam for user that use Face Recognition Reader **3 Photos

Photo 1
Photo 2
Photo 3

Upload
 Scan
 Reset

6.

Card No:* **1**

Name:*

Site Code:*

Card Properties

Card Type:	<input style="width: 90%;" type="text" value="Normal Card"/>		
Card Pin No:*	<input style="width: 90%;" type="text" value="0"/>	Biometric Authentication:	<input style="width: 90%;" type="text" value="FP"/>
Bypass Antipassback:	<input type="checkbox"/> Enable	Alarm Card:	<input type="checkbox"/> Enable
Guard Tour Card:	<input type="checkbox"/> Enable	Card Status:	<input checked="" type="checkbox"/> Enable
Face Access Level:	<input style="width: 90%;" type="text" value="None"/>	Rack Access Level:	<input style="width: 90%;" type="text" value="00 - No Access Rack Zone"/> 3
Card Expiry Status:	<input checked="" type="checkbox"/> Non Expired	Emergency Card Type:	<input type="checkbox"/> Enable
Bypass Holiday:	<input type="checkbox"/> Enable	Dual Card Group:	<input style="width: 90%;" type="text" value="Master Card"/> 4
Expired Date (dd-MM-yyyy):	<input style="width: 90%;" type="text" value="09-07-2020"/>	Expiry Time (HMS):	<input style="width: 90%;" type="text" value="10:39 AM"/> 5
Car Park Max Spot Group:	<input style="width: 90%;" type="text" value="None"/>	Canteen TZ:	<input style="width: 90%;" type="text" value="00"/>

Attendance Control

System

Other

Floor No: <input style="width: 90%;" type="text"/>	Unit No: <input style="width: 90%;" type="text"/>
Plate: <input style="width: 90%;" type="text"/> 6	Parking Lot No: <input style="width: 90%;" type="text"/>

- 1** -Card Number and Name
- 2** -Releasing Antipassback
- 3** -Rack Access Level
- 4** -Dual Card Group
- 5** -Expiry Date & Time
- 6** -Card Plate Number for LPR System

7. General information Card Holder

Card Profile

Card Info	Employee Details	Access Level	Custom Fields
Employment			
Staff No:	<input type="text"/>	Position:	Manager <input type="text"/>
Title:	Mr <input type="text"/>	Passport No:	<input type="text"/>
NRIC No:	<input type="text"/>	Socco No:	<input type="text"/>
EPF No:	<input type="text"/>	Company Name:	Company <input type="text"/>
Department:	Department <input type="text"/>	Race:	Unknow <input type="text"/>
Gender:	Male <input type="text"/>	Marital Status:	Single <input type="text"/>
Date Of Birth (dd-MM-yyyy):	<input type="text"/>	Resign Date (dd-MM-yyyy):	<input type="text"/>
Joining Date (dd-MM-yyyy):	10-10-2014 <input type="text"/>		
Contact			
Address :	<input type="text"/>		
Adjunct:	<input type="text"/>		
Postal Code:	<input type="text"/>	City:	<input type="text"/>
State:	<input type="text"/>	Country:	<input type="text"/>
Email:	<input type="text"/>		

8. Access Level

Card Profile

Card Info Employee Details Access Level Custom Fields

Door Access Lift Access

Group Access No: 01 Custom Mode
Site Code: OFFA

Ex. -> 01 = Access 24 hrs

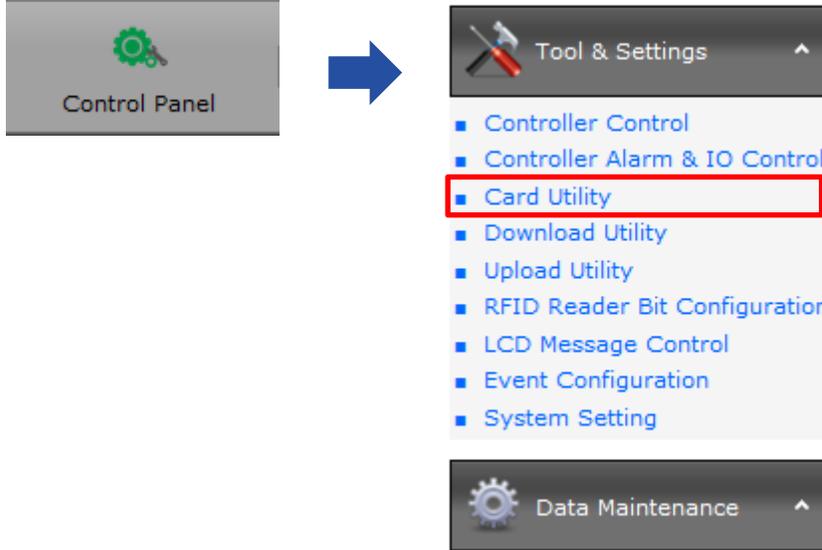
#	Controller	Description	Site Code	Time Zone
<input type="checkbox"/>	189		OFFA	00
<input type="checkbox"/>	ALARM CONTROLLER	TEST ALARM & I/O	OFFA	00
<input type="checkbox"/>	BACK DOOR CONTROLLER	BACK DOOR TESTING CONTROLLER	OFFA	00
<input type="checkbox"/>	BARRIER CONTROLLER	BARRIER TESTING CONTROLLER	OFFA	00

Custom mode for flexible controller and time zoned

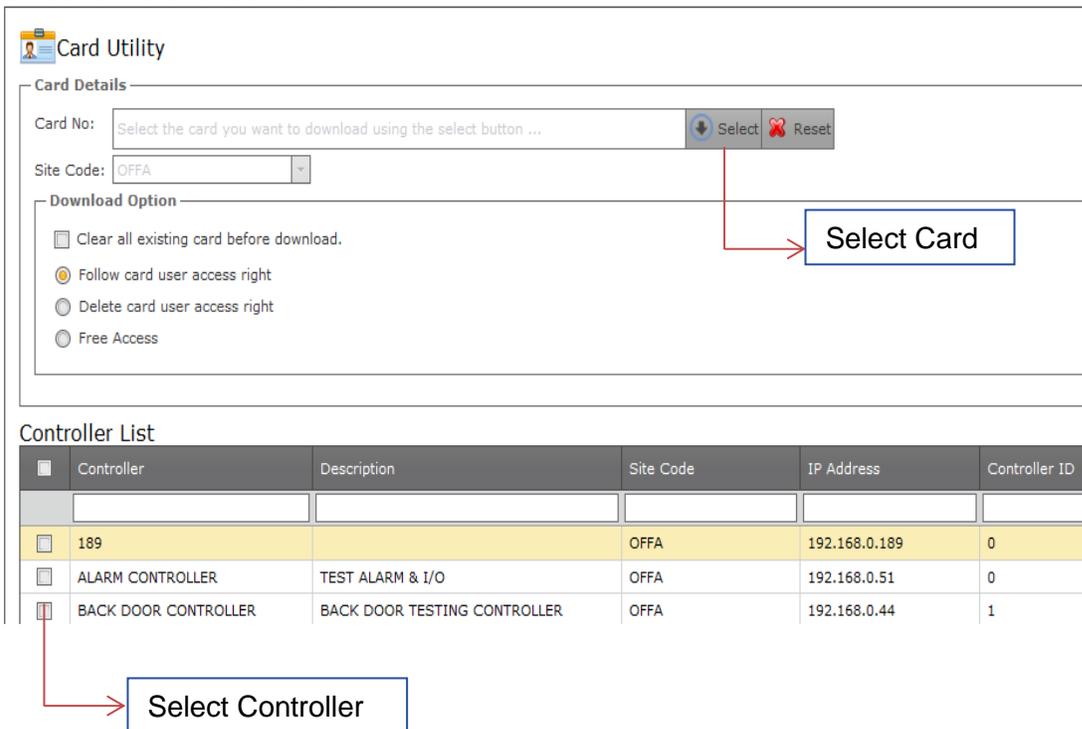
Apply is for search the information of the group

Configuring the group for access

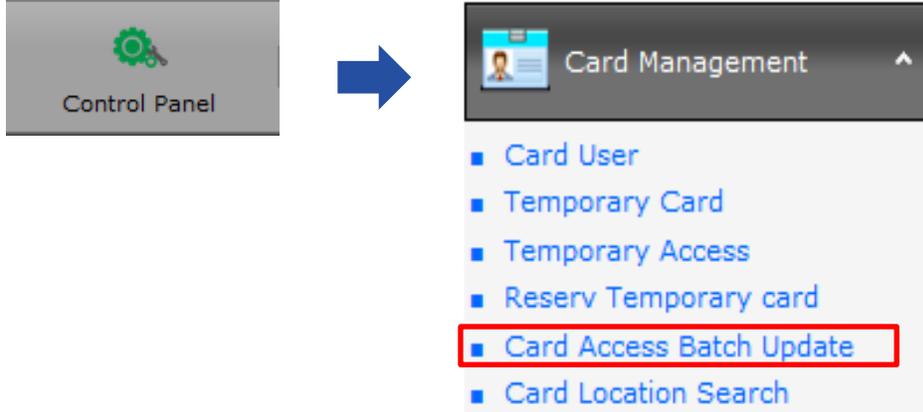
1. Go to Control Panel > Tools & Settings > Card Utility



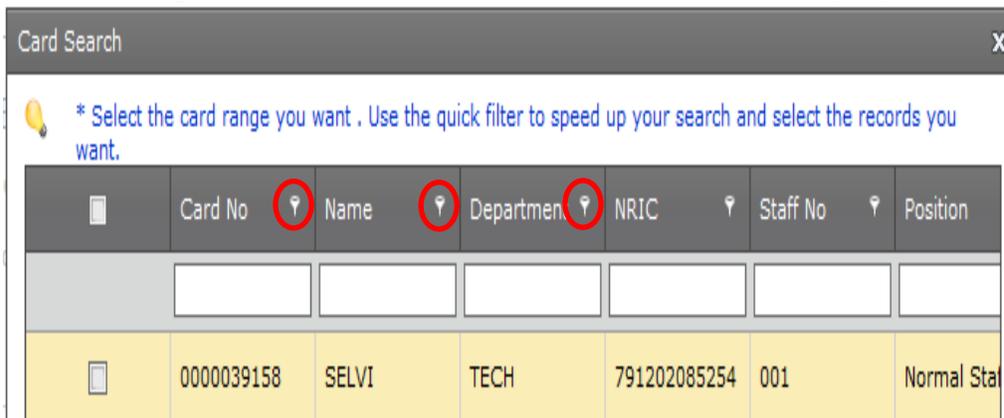
2. Select Card and Controller



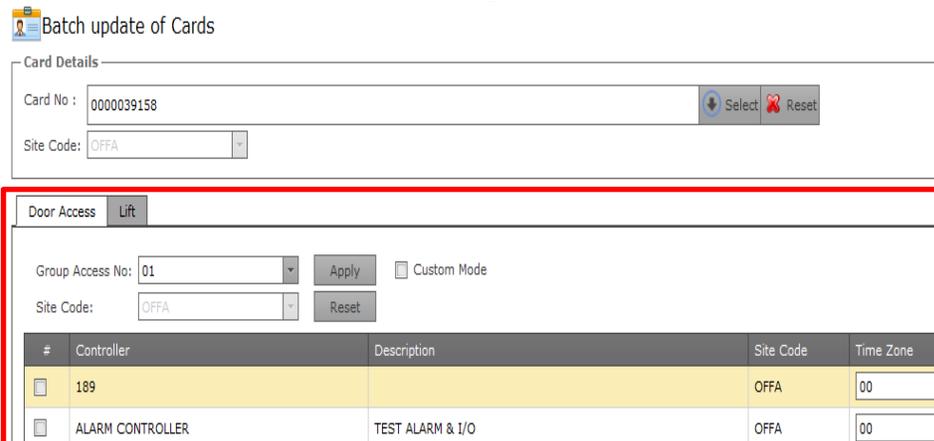
1. Go to Control Panel > Card Management > Card Access Batch Update



2. Filter to change the access level of a particular department/ company

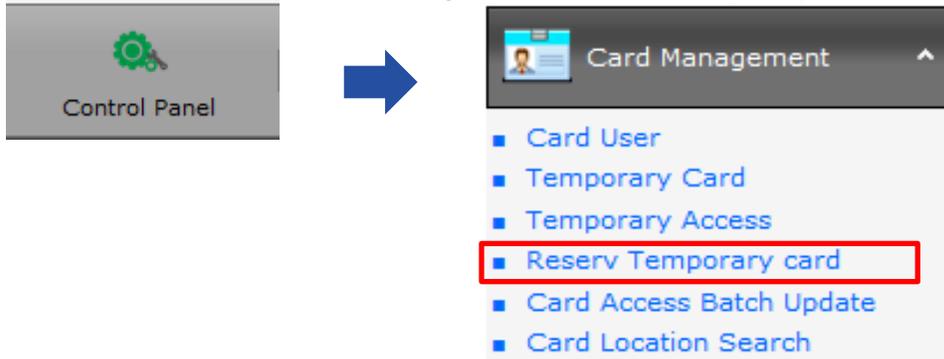


3. New Access Level to be used for the group

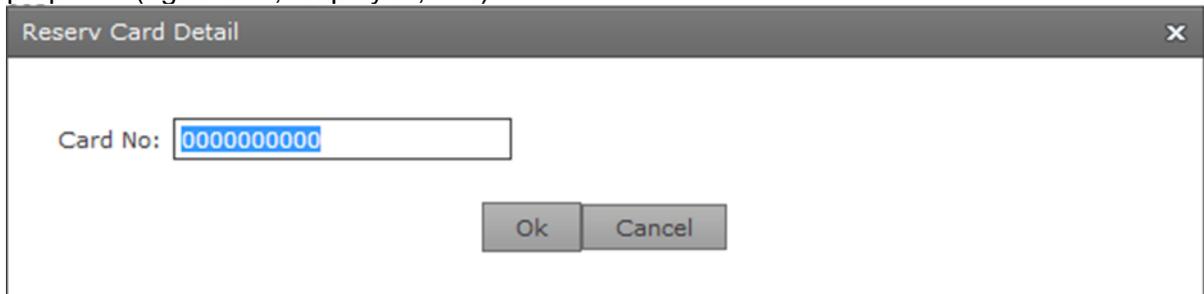


Temporary Reserve Card

1. Go to Control Panel > Card Management > Reserv Temporary Card

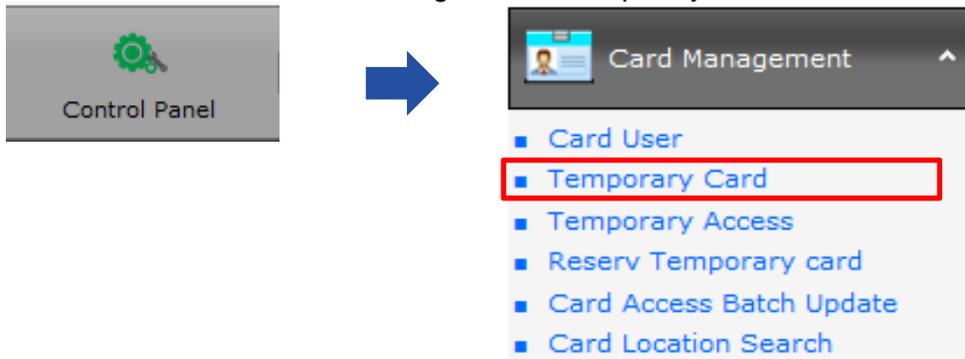


2. The reservation of temporary cards makes the operator can not use this card for other purposes (eg. Visitor, employee, etc.)



Temporary Card

1. Go to Control Panel > Card Management > Temporary Card



2. Choose cards
Temporary Card

A screenshot of the 'Card Detail' form. The 'Card Detail' tab is active. It contains several fields: 'Site Code' (OFFA), 'Existing Card No' (0000039158), 'Staff Name' (SELVI), 'NRIC' (791202085254), and 'Department' (TECH). A 'Search Card' button is next to the Existing Card No. A red arrow points from the NRIC field to a box labeled 'User Information'. Below this is the 'Temporary Card Info' section, which includes 'Temporary Card No' (45987), 'Expiry Date' (13/10/2014), and a 'Remark' text area. A red arrow points from the Expiry Date field to a box labeled 'The date to be expired for the Temp card'.

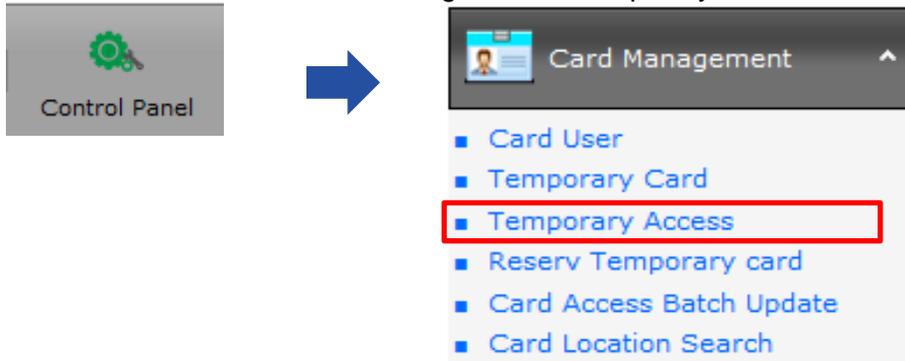
3. Return button to return card to the employee

Temporary Card



Temporary Access Level

1. Go to Control Panel > Card Management > Temporary Access



2. Temporary Details

Card Detail

Site Code: OFFA

Existing Card No: 0000039158

Staff Name : SELVI
NRIC: 791202085254 User Information

Department: TECH

Duration Time

Date From: 13-10-2014 Time: 12 00 AM
Date To: 23-10-2014 Time: 11 59 AM

Remark: VACATION Temporary Access Period

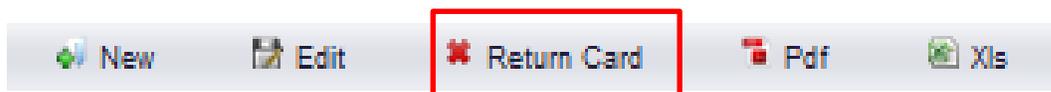
Door Access Lift Access

#	Controller	Description	Site Code	Time Zone
<input type="checkbox"/>	189		OFFA	00
<input type="checkbox"/>	ALARM CONTROLLER	TEST ALARM & I/O	OFFA	00

Temporary Permission

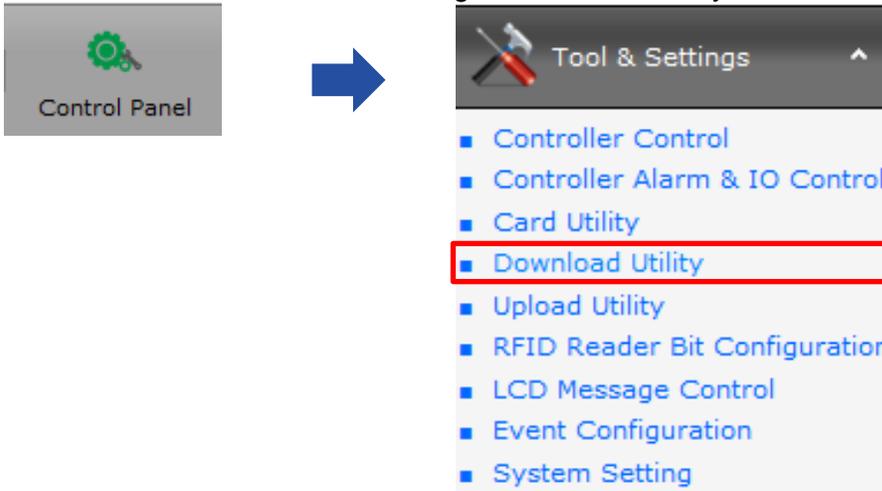
3. Return Button to return card to the employee

Temporary Card

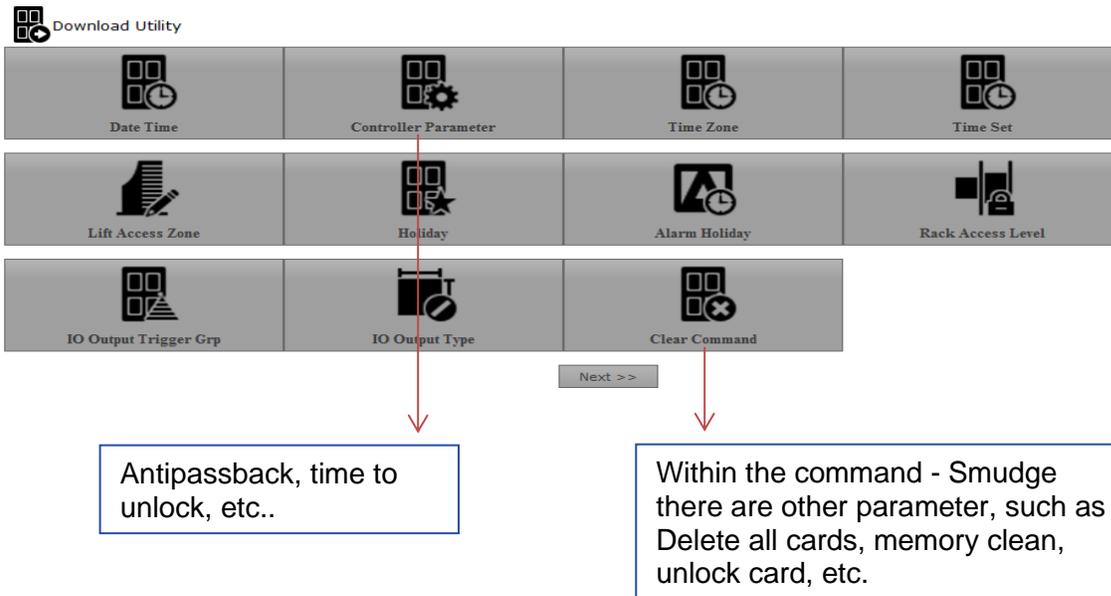


Download Utility

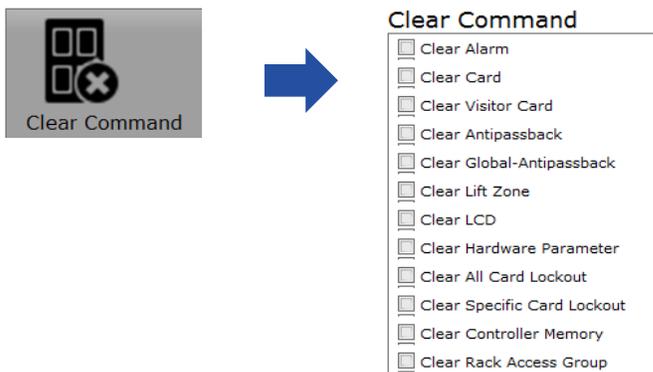
1. Go to Control Panel > Tool & Settings > Download Utility



2. Command use to send data from database to the controller



3.



1. Go to Control Panel > Tool & Settings > Upload Utility



2. Command used to check the data recorded in the controller.

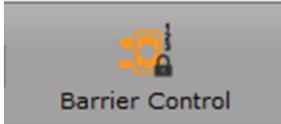


Select the option below to upload the setting from controller.



Next >>

1. Go to Door Control



2. Type of control



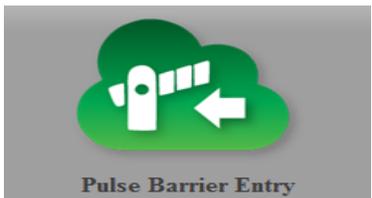
Used to lock the doors or barriers after a fire alarm.



Used to release the lock/ bypass lift



Release the lock like push button



Open the barrier gate

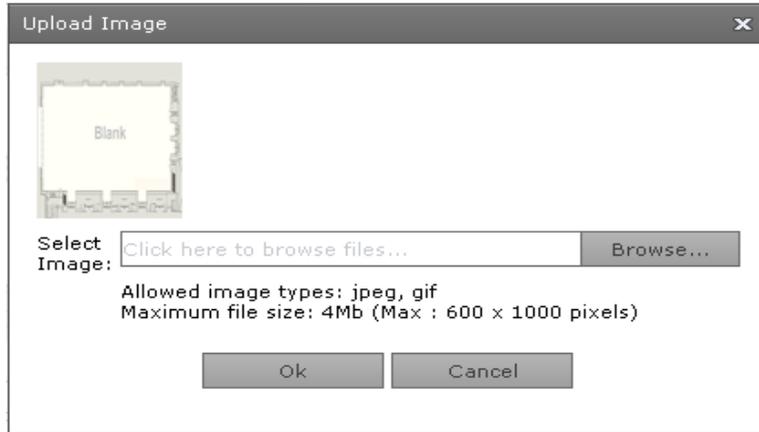


Close the barrier gate

1. Go to Control Panel > Site Management > Floor Plan



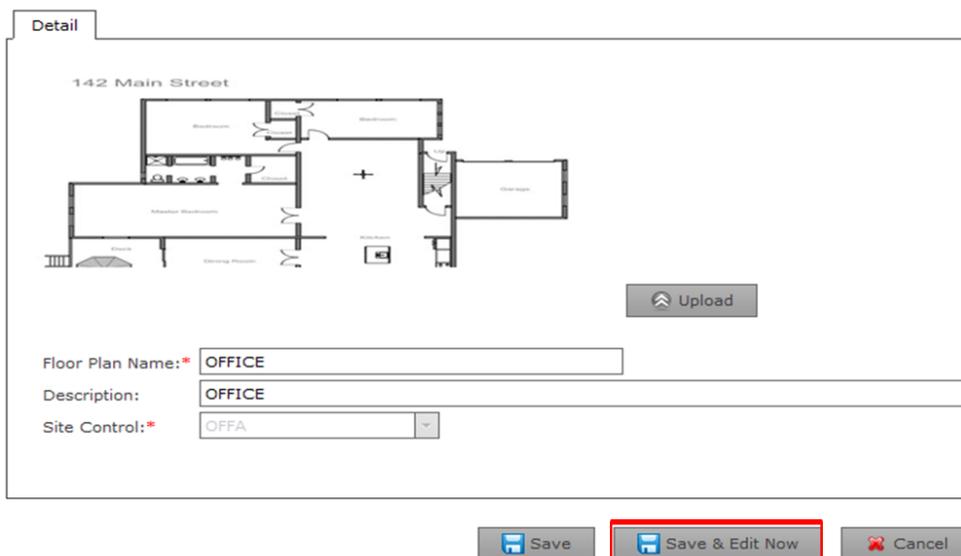
2. Browse and select Image



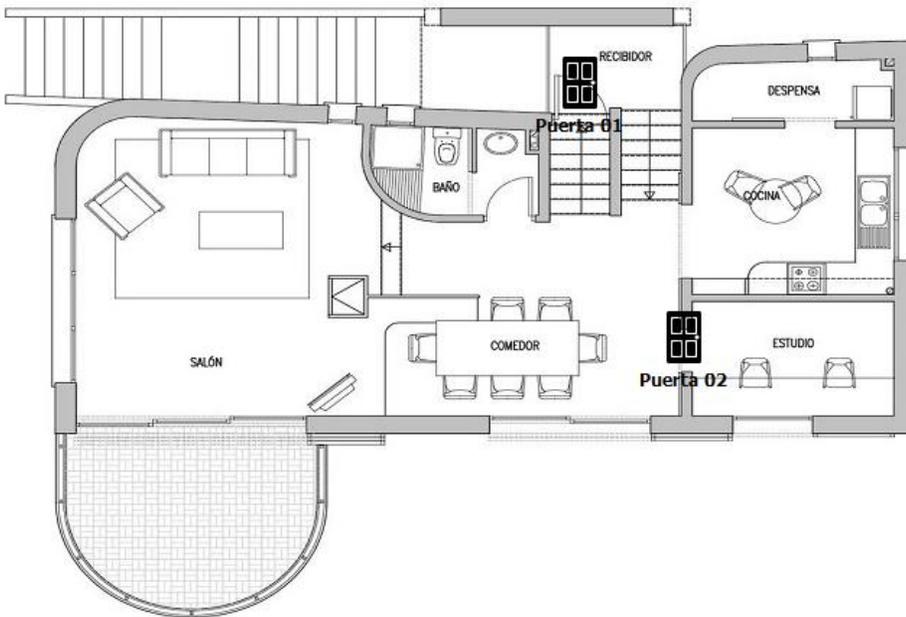
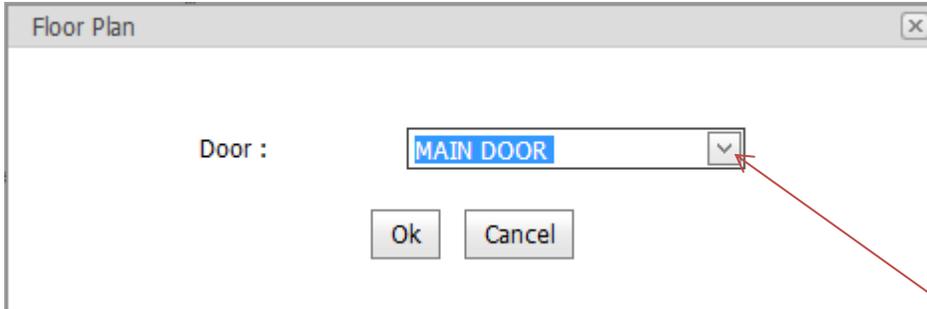
**** Important: You must give full permission (read, modify, delete, write) in the VAULT Enterprise folder so that the user can add a floor plan****

3. Click Save and Edit

Floor Plan



1. Click add and the controller will appear.
2. Put the controller/ camera where it places in real plan
3. After finish designing click save.



Tool Bar

Save

Close

OFFICE
OFFA

Door		
Alarm		
Camera		
IO Input		
IO Output		

Max : 600 x 1000 pixels

1. Go to Floor Plan > Click start for monitoring



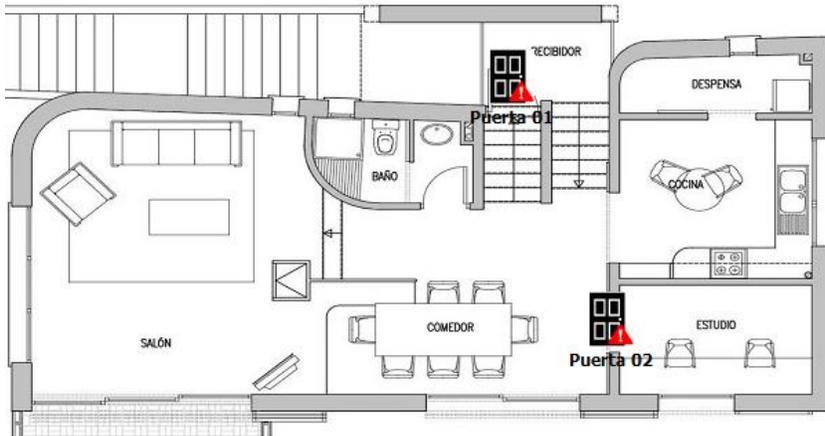
Tool Bar

Floor Plan Name :

Site Code :

ALARM MONITOR :

2. Acknowledge Alarm from floor plan

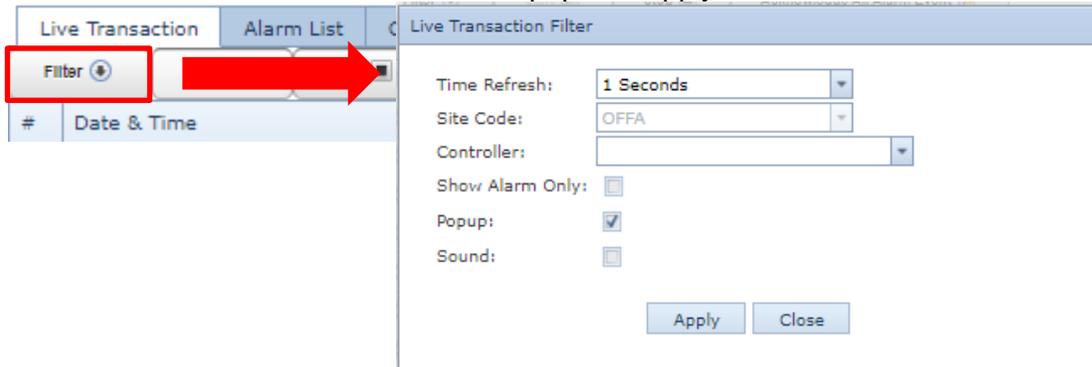


Transaction View

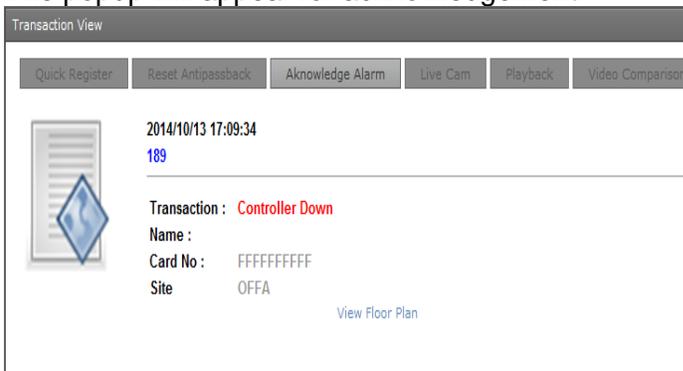
2014/10/13 08:30:17
MAIN DOOR

Transaction : **Controller Down**
Name :
Card No : FFFFFFFF
Site : OFFA

1. Go to Live Transaction > Filter > tick Popup and Apply



2. The popup will appear for acknowledgement



3. Alarm List for Alarm transaction only

#	Date & Time	Site	Controller	Card No	Name	Facility Code	Transaction
	2014/10/13 17:19:55	OFFA	EMERGENCY DOOR CONTROLLER	FFFFFFFF			Controller Down
	2014/10/13 17:19:52	OFFA	189	FFFFFFFF			Controller Down
	2014/10/13 17:14:46	OFFA	EMERGENCY DOOR CONTROLLER	FFFFFFFF			Controller Down

4. Card User Monitoring

Location	BARRIER CONTROLLER	Date Time	2014/10/07 15:48:35
Valid Entry Access			
Name	SELVI	Department	TECH
Card No	0000039158	Position	Normal Staff
Staff No	001	Company	KLA TECH
Location	BARRIER CONTROLLER	Date Time	2014/10/07 15:48:33
Valid Exit Access			
Name	SELVI	Department	TECH
Card No	0000039158	Position	Normal Staff
Staff No	001	Company	KLA TECH

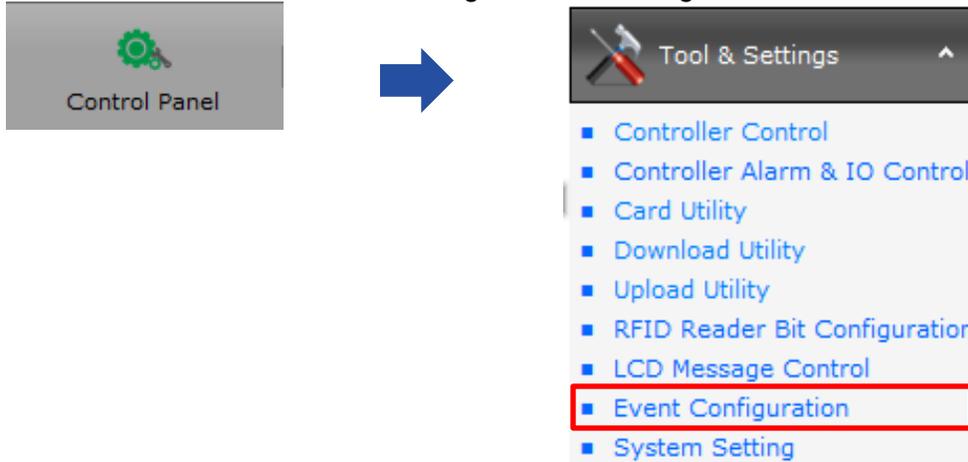
5. Controller Status shows whether the controller is online or offline

Live Transaction Alarm List Card Monitoring **Controller Status**

Site: OFFA Controller: Refresh

#	Controller	Site	IP Address	Controller ID	Status
189		OFFA	192.168.0.189	0	Offline -
	ALARM CONTROLLER	OFFA	192.168.0.51	0	Online -
	BACK DOOR CONTROLLER	OFFA	192.168.0.44	1	Online -

1. Go to Control Panel > Tool & Settings > Event Configuration



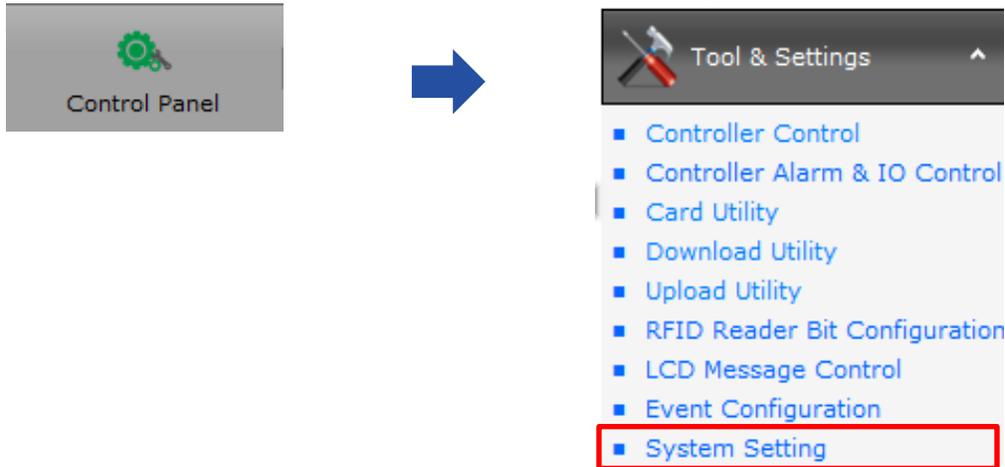
2. To facilitate monitoring, we can set so that when an alarm occurs, a pop-up is displayed on the screen along the local sound. Besides the possibility to send an email and SMS to preconfigured people.

Settings

* Event setting and notification.

Event	Event Color	Pop-up	Email	SMS
Acknowledge alarm	#FF0000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Alarm Activated	#FF0000	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Alarm Disable	#000000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Alarm Enable	#000000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Alarm Normal	#000000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ALARM TYPE OUTPUT OFF	#000000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ALARM TYPE OUTPUT ON	#000000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Alarm Zone Activated	#FF0000	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Alarm Zone Deactivated	#00FF00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
AntiPassback Entry	#FF0000	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

1. Go to Control Panel > Tool & Settings > System Settings



2. General Setting > Each site can have up to 8 facility code.

The screenshot shows the 'General Setting' page with three tabs: 'General Setting', 'Email Notification', and 'Card User Custom Field'. The 'Facility Code' section contains an 'Enable Facility Code' checkbox and eight input fields for Facility Code 1 through 8, all containing '0000'. Below this is the 'CCTV & Video Integration Mode' section with a 'Video Server Type' dropdown set to 'NUUO'. The 'Biometric Device' section has a 'Biometric Model' dropdown set to 'ZK'. The 'User Login' section has 'Number of day to change password' set to 30 and 'Number of time to retry login' set to 5.

3. Email Notification > Setup Email Notification System Preference and Configuration

General Setting Email Notification Card User Custom Field

SMTP Mail Server

SMTP Server:

Outgoing Port:

Authentication Required: Required SSL:

Username: Password:

Email Account

Send email to below receipt(s) when alarm event detected.

Email 1:

Email 2:

Email 3:

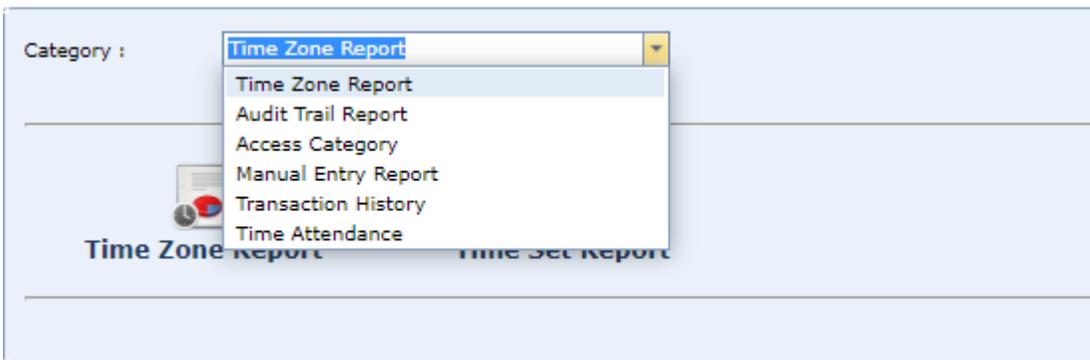
Email 4:

Email 5:

1. Go to Report



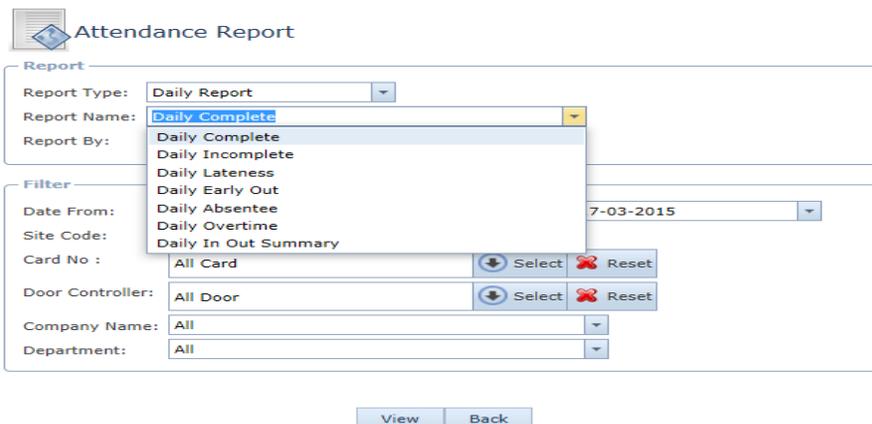
2. Multi choice of reports



3. To view the attendance report , go to Report > Time Attendance Report



4. Select the report you want to view and input the criteria for report you want to filter. See screen capture below for the report type available.



5. Report Window Tool Bar



Tuesday, March 17, 2015

Daily Complete Report

Site Code : MORUMBI
Date : 17/03/2015 **To** 17/03/2015 **Company :** All
Card : All Card **Department :** All

Date	Department	Card No	Name	Staff No	Time In	Time Out
------	------------	---------	------	----------	---------	----------

Section	Description
a	Search the content in the report
b	Print the report.
c	Print the current page
d	Page Navigation. Navigate and select the page you want to view.
e	Export the current report to the document type you want. (PDF,Excel,CSV,HTML,RTF)

6. Daily Report – Report type

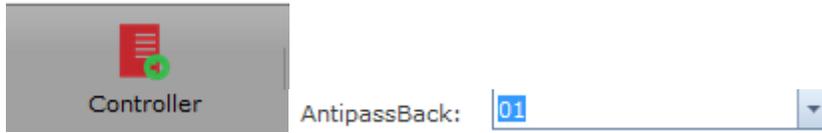
Report Name	Description
Daily Complete	Daily staff attendance with In and Out record. Transaction for both valid entry and valid exit.
Daily Incomplete	Daily staff attendance incomplete with In or Out record. Eg : Entry record found but without Exit record.
Daily Lateness	Daily staff attendance with lateness
Daily Early Out	Daily staff attendance where the staff left early or back before the end work time.
Daily Absentee	Daily staff report for those who are absent
Daily Overtime	Daily staff Over time report.
Daily In Out Summary	Daily staff In & Out records summary report.

7. Monthly Report – Report type

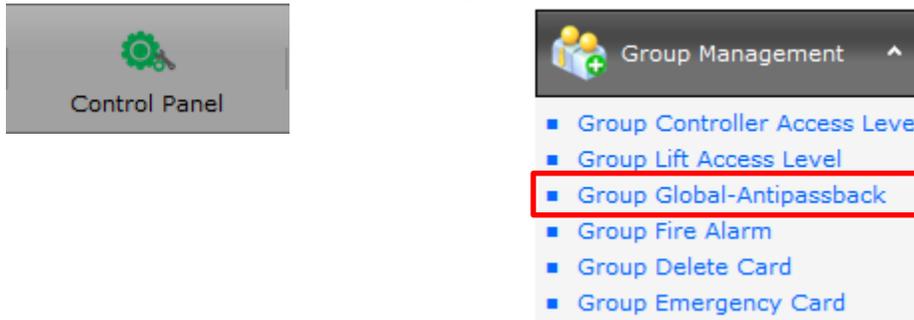
Report Name	Description
Attendance Checklist	
Attendance Summary	
Staff In Out Report	

Global Antipassback

1. Go to controller > make sure AntipassBack is in 01



2. Go to Control Panel > Group Management > Group Global-Antipassback



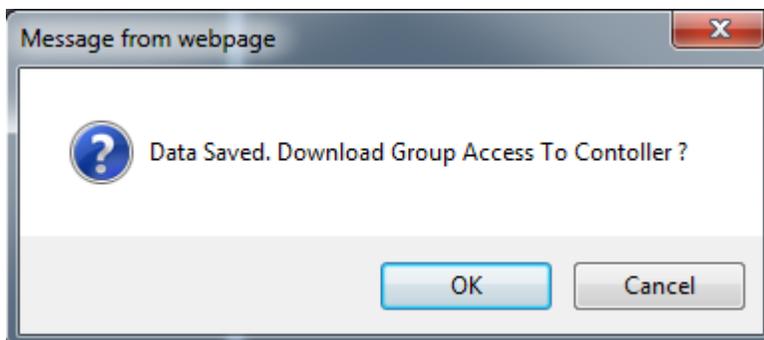
3. Create new Group Access No

Group Access No:*

Site Code:

<input type="checkbox"/>	Controller	Description	Site Code
<input checked="" type="checkbox"/>	ALARM CONTROLLER	TEST ALARM & I/O	OFFA
<input checked="" type="checkbox"/>	EMER-2		OFFA
<input checked="" type="checkbox"/>	MAIN DOOR	TESTING DOOR CONTROLLER	OFFA

4. Download to Controller



Global Antipassback Group:

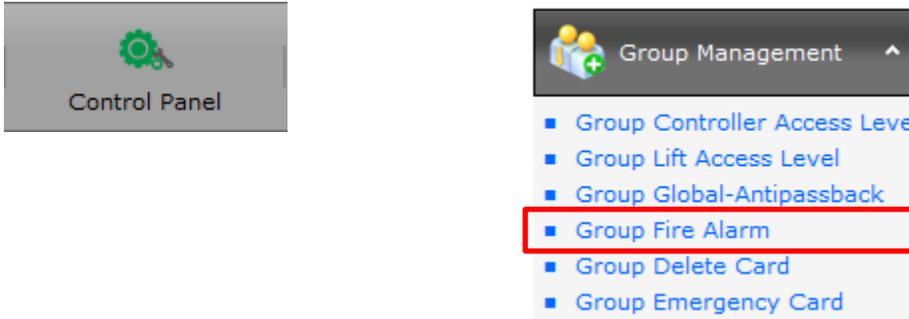
Additional Module

Fire Alarm

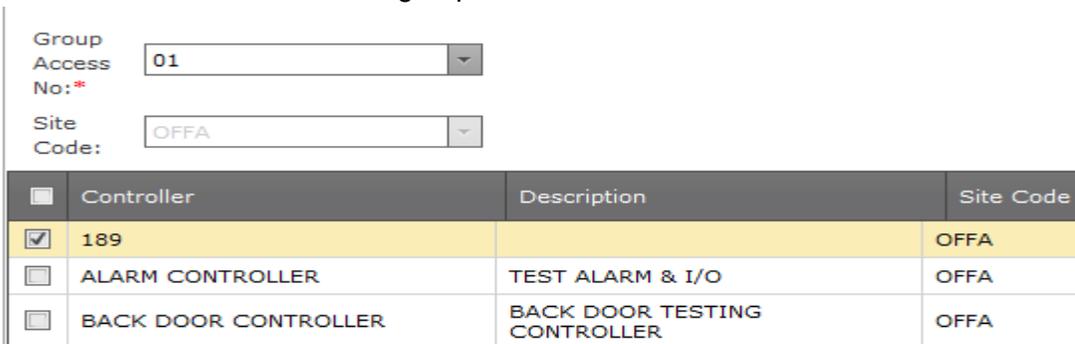
1. Go to controller > make sure Fire Alarm is enable



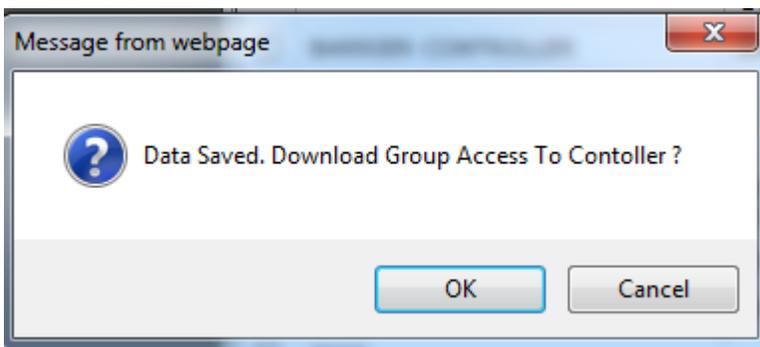
2. Go to Control Panel > Group Management > Group Fire Alarm



3. Tick controller that in the same group



4. Download to controller



Additional Module

Group Delete Card

1. Go to Control Panel > Group Management > Group Emergency Card



2. Feature only applies to controllers enable at Auto delete group. When the visitor card to deposit in the ballot box, it will be automatically deleted from the system

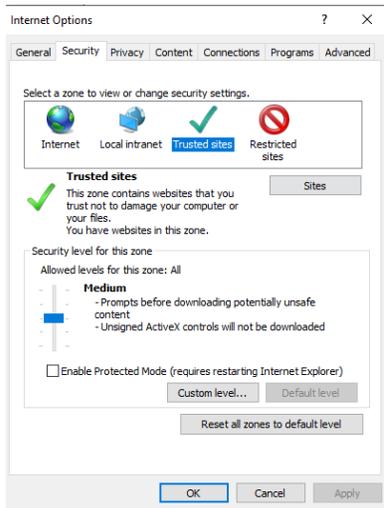
Controller List

Site Code: OFFA

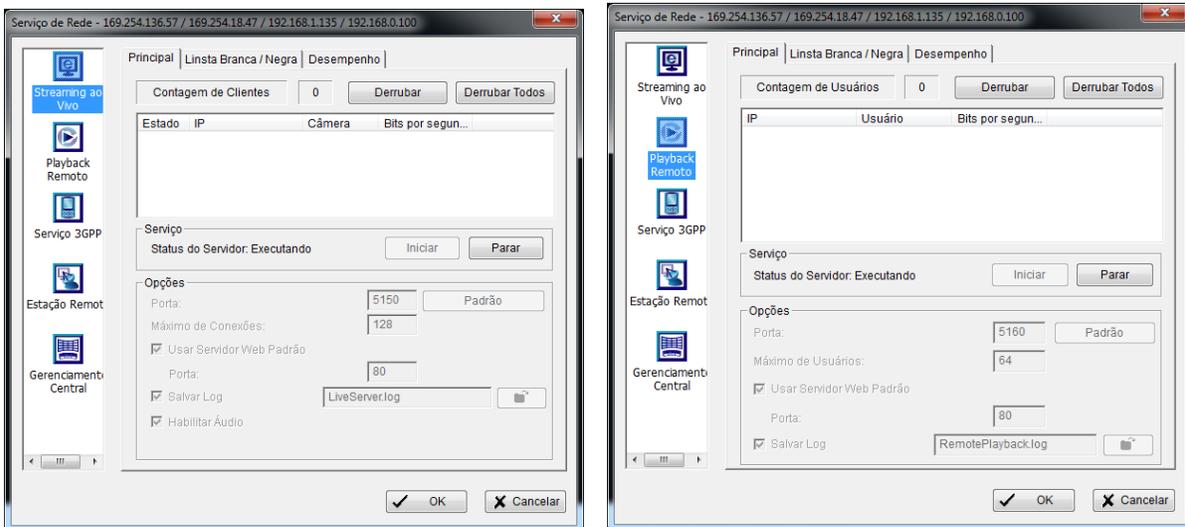
<input checked="" type="checkbox"/>	Controller	Description	Site C
<input checked="" type="checkbox"/>	189		OFFA
<input checked="" type="checkbox"/>	ALARM CONTROLLER	TEST ALARM & I/O	OFFA
<input checked="" type="checkbox"/>	BACK DOOR CONTROLLER	BACK DOOR TESTING CONTROLLER	OFFA
<input checked="" type="checkbox"/>	BARRIER CONTROLLER	BARRIER TESTING CONTROLLER	OFFA
<input checked="" type="checkbox"/>	EMER-2		OFFA

Integration with Camera

1. CCTV integration module is not available in the free versions of Enterprise Vault. For integration, check if your license is already activated and follow these steps:
2. Integrating video only works in Internet Explorer, so we must enable all ActiveX, disable popups (pop-up) and include enterprise Vault in the list of trusted sites.
3. To set up that way, open the Tools tab of Internet Explorer and click Internet Options.



4. In the MAIN CONSOLE software, check if the network services and have begun recording:



Integration with Camera

5. Go to Control Panel > Video Camera > Camera Server



6. Fill in the camera credential and save into database

Video Server

Detail

Cam Server Name: NUUO SERVER

IP Address: 192.168.0.145

Site Code: OFFA

Live View Port: 5150

Playback Port: 5160

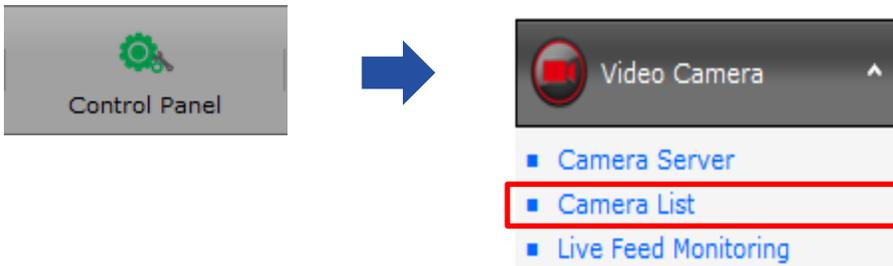
Authentication

Login ID: admin

Password: [masked]

Save Cancel

7. Go to Control Panel > Video Camera > Camera List



8. Important: Camera names cannot be changed!

Camera

Detail

Cam Server: NUUO OFFICE - 192.168.1

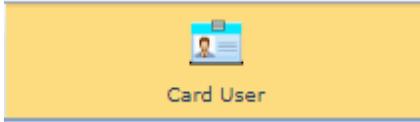
Get Camera List

Camera Name: Hotel_1

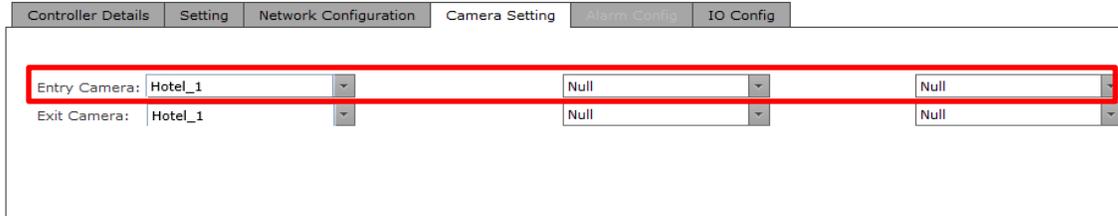
Save Cancel

Cameras video server

9. Go to Controller > Camera setting

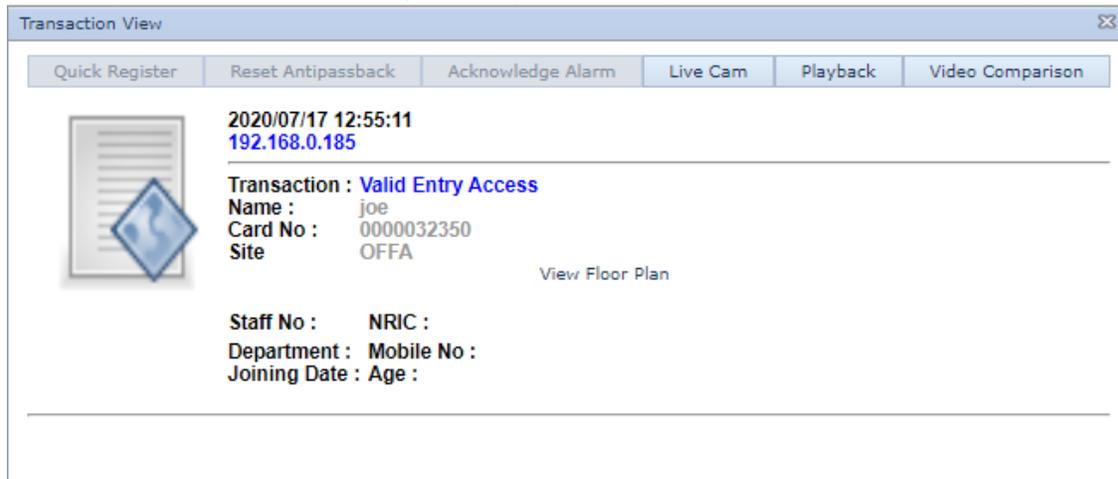


192.168.0.51 :



10. **Important:** We can have up to 3 cameras Associated input and for output.

11. To check the operation, click on the online transaction access in / out of the door and set the Video option select Live or Playback.



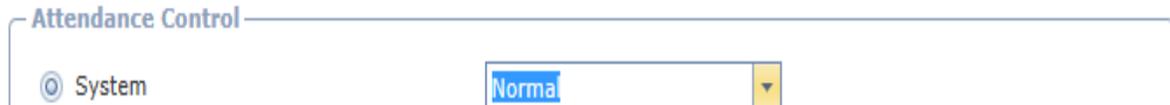
ONLINE



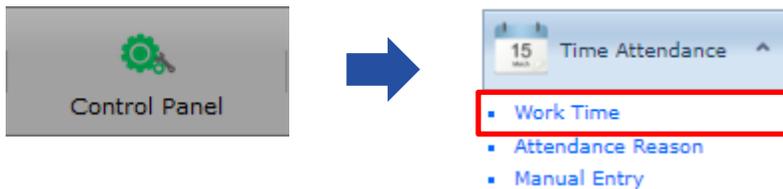
PLAYBACK

1. Working Time Configuration

Every card user are linked to the specific work time mode like below, for the calculation of attendance report purpose.



- a. To start using attendance control , you need to configure the Working Time .
Under the Control Panel > Time Attendance > Work Time



- b. By default system come with a default setting (Normal Work Time) which preset the system with standard working time.

Eg :Office Hours , Monday to Friday , 08:30am – 17:30pm

Work Time

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
Time In	08:30	08:30	08:30	08:30	08:30	00:00	00:00
Time Out	17:30	17:30	17:30	17:30	17:30	00:00	00:00
Work Day	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
Next Day	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
Time Out	01	01	01	01	01	01	01

- c. At General tab, you can find the normal setting like Work Time Name and Description.

General Working Hour Lunch & Breaktime

Work Time Name: * Normal

Description: Normal

Site Code: MORUMBI

Grace Period

Time In: 15 Time Out: 15

Minimum Lapse Hour: 0

Over Time Setting

Auto None

Minimum Overtime: 0

- d. Grace Period ,here is the option where you could allow discretion period in late-IN or early-OUT.

When an employee who supposed to check in at 8:30am checks in at 8:45am, or checks out at 5:15pm when the time of check out is 5:30pm, the short in time is not considered as lateness in the overall report, if you put its Grace period at 15 minutes. If the grace period is 15 minute, the check in time at 8:46am will be considered as 1 minute late. preview in the report.

Time In will set the lateness time and **Time Out** will set the early out time.

Minimum Overtime (in min) will determine when it is consider as overtime limit.

**** Make sure Server 24/7 turn on for attendance time accuracy**

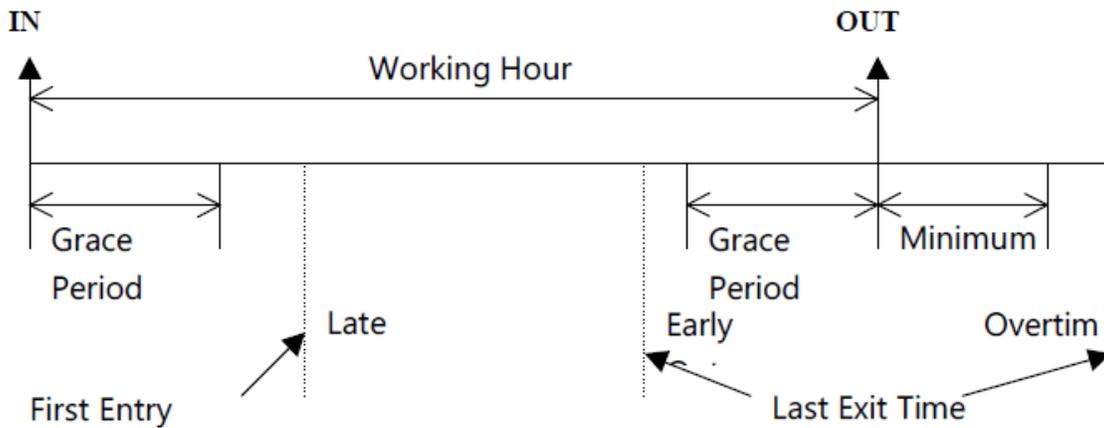
Work Time

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
Time In	08:30	08:30	08:30	08:30	08:30	00:00	00:00
Time Out	17:30	17:30	17:30	17:30	17:30	00:00	00:00
Work Day	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
Next Day	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
Time Out	01	01	01	01	01	01	01

- e. Under Working Hour tab, you will see the Time In ,Time Out, Work Day, Next Day, OT Type this is the area where you can configure the working time in the weekly basis.

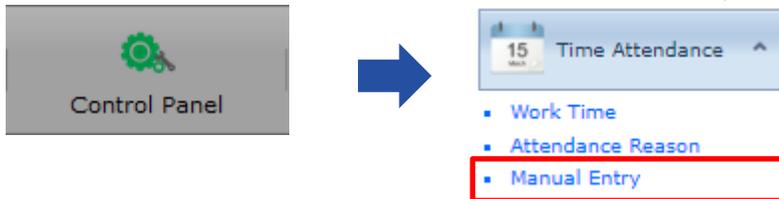
Field	Description
Time In	Time start to work.
Time Out	Time end to work.
Work Day	Check it for working days or uncheck it for non working days.
Next Day	Use this option for those working time start at late / night shift / over night where the attendance the part involve for the second day calculation. Eg : Work from 10:00pm – 06:00am
OT Type	By default , system predefined with OT Type = 1, OT Type can be category from 1 – 4. Company who intend to use or category out the OT type for different user type can make use of this OT Type to differentiate out . It will appear as OT 1, OT 2 ,OT3 or OT4 when using generate the OT report.

- f. The diagram below shows the further details in setting the Grace Period, Working Hour and Minimum Overtime.



2. Manual Entry

- a. Go to Control Panel > Time Attendance > Manual Entry.



- b. Here is where the **operator / system admin** can register or add in the transaction manually in case the system need extra manual transaction or staff forget to swipe the card for attendance purpose. Under **Manual Entry Form** , select **New** to add in the new record. Record added (Valid Entry / Valid Exit) will be take place in calculation under attendance report.

Manual Entry Form

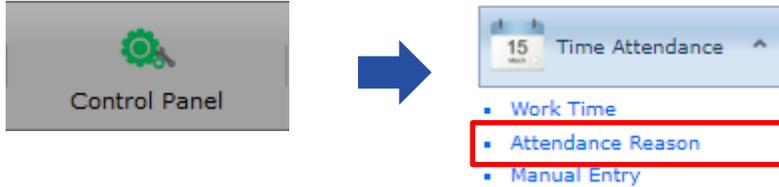
Detail

Site Code:	MORUMBI	Date:	17-03-2015	Date To:	17-03-2015
Time:	00:00:00	Time To:	23:59:59	...	
Card No:					
Staff Name :					
NRIC:					
Department:					
Transaction:	Valid Entry Access				
Reason:	Normal Transaction				
Remark:	Forget to swipe card.				

Save Cancel

3. Attendance Reason

- a. Go to Control Panel > Time Attendance > Attendance Reason.



- b. The Attendance Reason will display or appear in Manual Entry Section only. Operator / System Admin can manage all the Reason profile under this section.

Eg : Forget to bring card , Oversea Training and etc.

Late Reason List

Drag a column header here to group by that column			
No	Code	Description	
1	Normal	Normal Transaction	
2	MC	Medical CheckUp	
3	AL	Annual Leave	
4	NPL	No Pay Leave	
5	NPH	No Pay Hour	