



**ACCESS CONTROL
INTEGRATED SYSTEM
MANUAL**

VAULT Enterprise Professional

CONTACT DETAILS

MALAYSIA

KLA TECH (M) SND BHD

28, JALAN SS4D/14, TAMAN PEOPLES'S PARK, 47301 PETALING JAYA.

SELANGOR DARUL EHSAN. MALAYSIA

Tel : 603-78040343

Fax : 603-78040317

Email : ivyphang_kla@falco-ecom.com

Skype Contact : kla_ivy

INDONESIA

PT FALCO

RUKO SALEMBA MAS No. 34-36 H, 3RD FLOOR,

Jl. SALEMBA RAYA, JAKARTA PUSAT, 10320, INDONESIA.

Tel. : 6221 97 777 121 / 6221 3192 7779

Skype Contact: Ari Wirantoko

Email : a.wirantoko@falco-ecom.com

SINGAPORE

ASCENDO PTE LTD

85 PLAYFAIR ROAD #06-02 TONG YUAN BUILDING

368000 SINGAPORE

Tel : 02-67411218

Fax : 02-67418991

E-mail : falco@pacific.net.sg

BRAZIL

GLASS SENTINAL DO BRAZIL LTDA

CNPJ: 04.615.088/0001-07

RUA DOS MISSIONARIOS, 306 - SANTO AMARO

SANTO AMARO - SAO PAULO- SP

04729-000 BRAZIL

Tel : (11)3846 7087/(11)5641 2811

Fax : (11)5643 7028

E-mail : natan@vaultbr.com

HONG KONG

KLA SYSTEMS PTE LIMITED

ROOM2309,23/F,

HO KING COMM CTR, 2-16 FAYEUN ST,

MONGKOK KOWLOON, HONG KONG

Tel : +852 6529 5680

Email: cml_kla@falco-ecom.com

TABLE OF CONTENTS

INTRODUCTION.....	4
CHAPTER 1 – STARTING POINT.....	5
1.1 PCs Requirements.....	5
CHAPTER 2 – SOFTWARE INSTALLATION.....	6
2.1 Software Download.....	6
2.2 Software Installation.....	7
CHAPTER 3 – ADMIN LOGIN.....	9
3.1 Admin Login.....	9
3.2 First Time Setup.....	9
CHAPTER 4 – LICENSE ACTIVATION.....	10
4.1 Online Activation.....	10
4.2 Offline Activation.....	10
CHAPTER 5 – VAULT BASIC DOOR CONFIGURATION.....	12
5.1 Add Controller.....	12
5.2 Controller Setting.....	13
5.2.1 Basic Controller Setting.....	13
5.2.2 Controller Mode.....	14
5.2.3 Card & Pin.....	14
5.2.4 Dual Card Mode.....	15
5.2.5 Auto Pin No.....	15
5.3 Network configuration.....	15
5.4 Card Access Level.....	15
5.4.1 Time Set & Time Zone	15
5.4.2 Group access level.....	17
5.5 Add Card User.....	17
5.5.1 Card Info.....	18
5.5.2 Employee Details.....	21

Manual – VAULT Enterprise Professional

5.5.3 Access Level.....	24
5.5.4 Custom Fields.....	24
5.6 Live Transaction.....	25
5.6.1 Transaction Sign.....	25
5.6.2 Live Transaction Tab.....	25
5.6.3 Alarm List Tab.....	26
5.6.4 Card User Monitoring Tab.....	26
5.6.5 Controller Status Tab.....	26
5.6.6 Live Transaction Additional Feature.....	26
5.7 Transaction Server Software.....	27
5.7.1 Setting Tab.....	28
5.7.2 Database Maintenance.....	29
5.7.3 Preferences.....	29
5.7.4 Import Tool.....	30
5.8 Report.....	30
5.8.1 Time Zone Report.....	31
5.8.2 Audit Trial Report.....	31
5.8.3 Access Category.....	31
5.8.4 Manual Entry Report.....	32
5.8.5 Transaction History.....	32
5.8.6 Time Attendance.....	32
CHAPTER 6 – DOOR CONTROL.....	33
6.1 Overview.....	33
6.2 Door Control Option.....	33
CHAPTER 7 – ALARM & IO CONTROL.....	34
7.1 Overview.....	34
7.2 Alarm & IO Control Option.....	34
CHAPTER 8 – VIDEO CAMERA.....	35
8.1 Add Camera Server.....	35
8.2 Add Camera.....	35

Manual – VAULT Enterprise Professional

CHAPTER 9 – FINGERPRINT.....	37
9.1 Add Fingerprint Device.....	37
9.2 Fingerprint Enrollment.....	37
CHAPTER 10 – CONTROL PANEL.....	38
10.1 Card Management.....	38
10.2 Controller Management.....	38
10.3 Group Management.....	39
10.4 Video Camera.....	39
10.5 Fingerprint.....	40
10.6 User Management.....	40
10.7 Time Attendance.....	40
10.8 Site Management.....	41
10.9 Tool & Settings.....	41
10.10 Data Maintenance.....	42
CHAPTER 11 – TIME ATTENDANCE SETTING.....	43
11.1 Working Time Configuration.....	43
11.1.1 General Setting.....	43
11.1.2 Working Hour.....	43
11.1.3 Lunch & Break Time.....	44
11.2 Manual Entry.....	44
11.3 Attendance Reason.....	44
11.4 Attendance Report.....	44
CHAPTER 12 – RACK CONTROLLER CONFIGURATION.....	46
12.1 Controller configuration.....	46
CHAPTER 13 – I/O ALARM CONFIGURATION.....	48
13.1 Controller Configuration.....	48
CHAPTER 14 – LIFT CONTROLLER CONFIGURATION.....	49
14.1 Controller Configuration.....	49
CHAPTER 15 – GLOBAL ANTIPASSBACK CONFIGURATION.....	50
15.1 Antipassback Configuration.....	50

Manual – VAULT Enterprise Professional

15.2 Global Antipassback Configuration.....	50
CHAPTER 16 – FIRE ALARM CONFIGURATION.....	51
16.1 Fire Alarm Configuration.....	51
16.2 Group Fire Alarm Configuration.....	51
CHAPTER 17 – FLOOR PLAN.....	52
17.1 Floor Plan List.....	52
17.2 Floor Plan Online.....	52
CHAPTER 18 – DATABASE BACKUP AND RESTORE.....	54
18.1 Backup and Restore using transaction server.....	54
18.2 Backup and Restore using Microsoft SQL Management Studio.....	54

INTRODUCTION

The VAULT Enterprise Pro software is a practical tool for PCs that enables total management of Access Controllers.

Functions:

- Several Access levels for the software user, with ample possibilities for permission and privilege programming.
- Totally programmable access levels for different users, through the total access control system. Each different card user may have several different combinations of access levels on each controller. There are presently 999 programmable access levels.
- In case the computer power is turned off, the controller has its own memory to store the information on transactions or events. As soon as the power is restored, the information on each controller will be received by the Server and will be available to the operator.

Characteristics:

- 99 Time programming Configurations.
- 99 Time Zone programming.
- 50 Holiday List programming.
- Enables opening each floor directly from a PC.
- Enables the inclusion of blue-prints for a better visualization of alarms generated by: Forced door, Door left open, Controller crash, and Low battery.
- Up to 4 readers (according to the firmware) can be connected to each controller, 2 Entry readers and 2 Exit readers. The readers may be proximity readers, Smart-card readers (mifare), Biometric readers, Barcode readers, card + password readers, etc. The system supports most technologies for unit readers with Wiegand 26, 34 or 42 bit exits. In case of need for another type of exit, please consult our commercial / technical department.

CHAPTER 1 – STARTING POINT

1.1 PCs Requirements

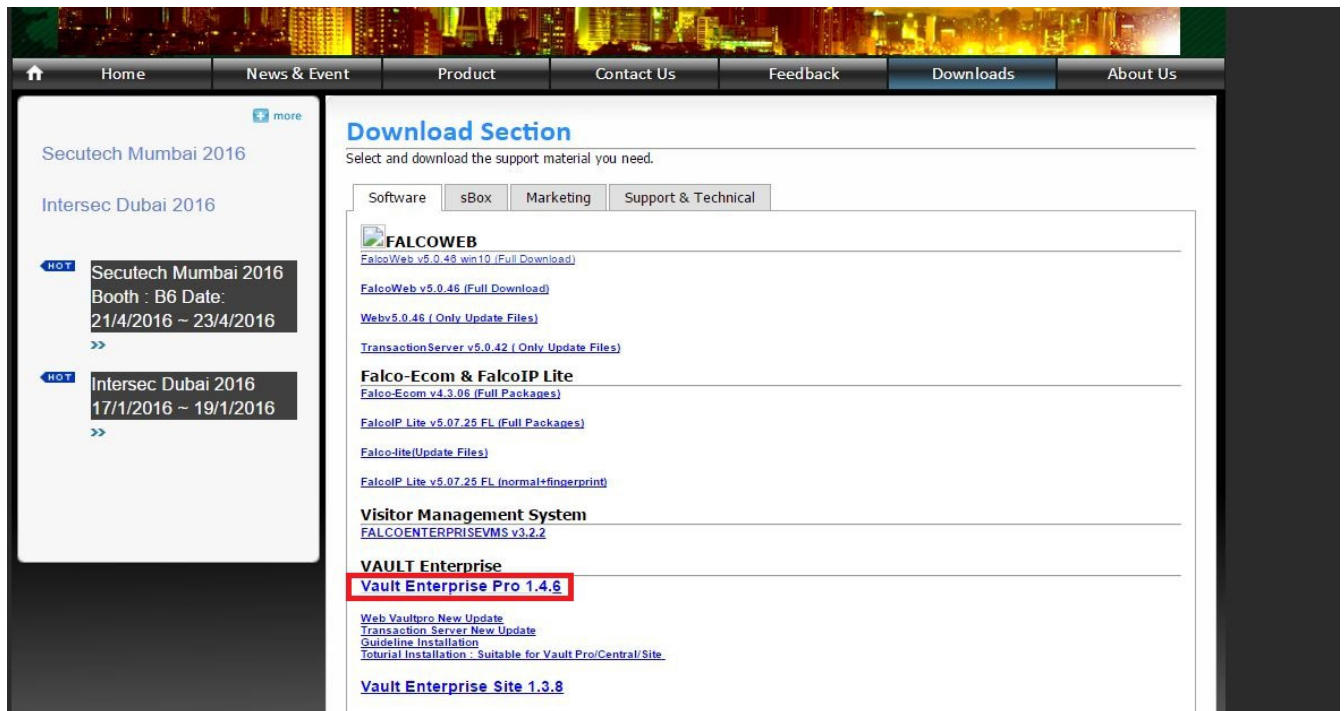
The System Requirements are specify below:

Specification	Recommended
Operating System	<ul style="list-style-type: none"> - Windows 7 Business (32-bit/64-bit) - Windows 7 Professional (32-bit/64-bit) - Windows 7 Ultimate (32-bit/64-bit) - Windows 7 Enterprise (32-bit/64-bit) - Windows 8 Professional (32-bit/64-bit) - Windows 8.1 Professional (32-bit/64-bit) - Windows 10 Professional (64-bit) - Windows server 2012 (32-bit/64) <p style="color: red; margin-top: 10px;">*Windows XP, Window 7 Home & Window 7 Starter Edition not supported</p>
Processor	- INTEL Core i5 and higher or equivalent
Memory (RAM)	- Minimum 8GM RAM or more
Hard Disk Space / Type	- Minimum 500 Gb Disk Space / 5200 rpm
Software	<ul style="list-style-type: none"> - Microsoft Internet Information Service (IIS) 7.0 or above - Microsoft .NET Framework Version 4.0
Browser	- To use all the advanced feature of the Vault Pro Web, you will need to be using the latest version of Microsoft Internet Explorer, Firefox or Opera on a Window system.

CHAPTER 2 – SOFTWARE INSTALLATION

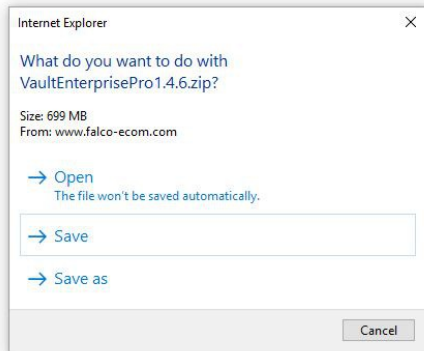
2.1 Software Download

Step 1 - Download the VAULT Enterprise Professional installation setup through <http://www.falco-ecom.com/Download.aspx>



Step 2 - Click on the link as shown in diagram above and save it.

Manual – VAULT Enterprise Professional

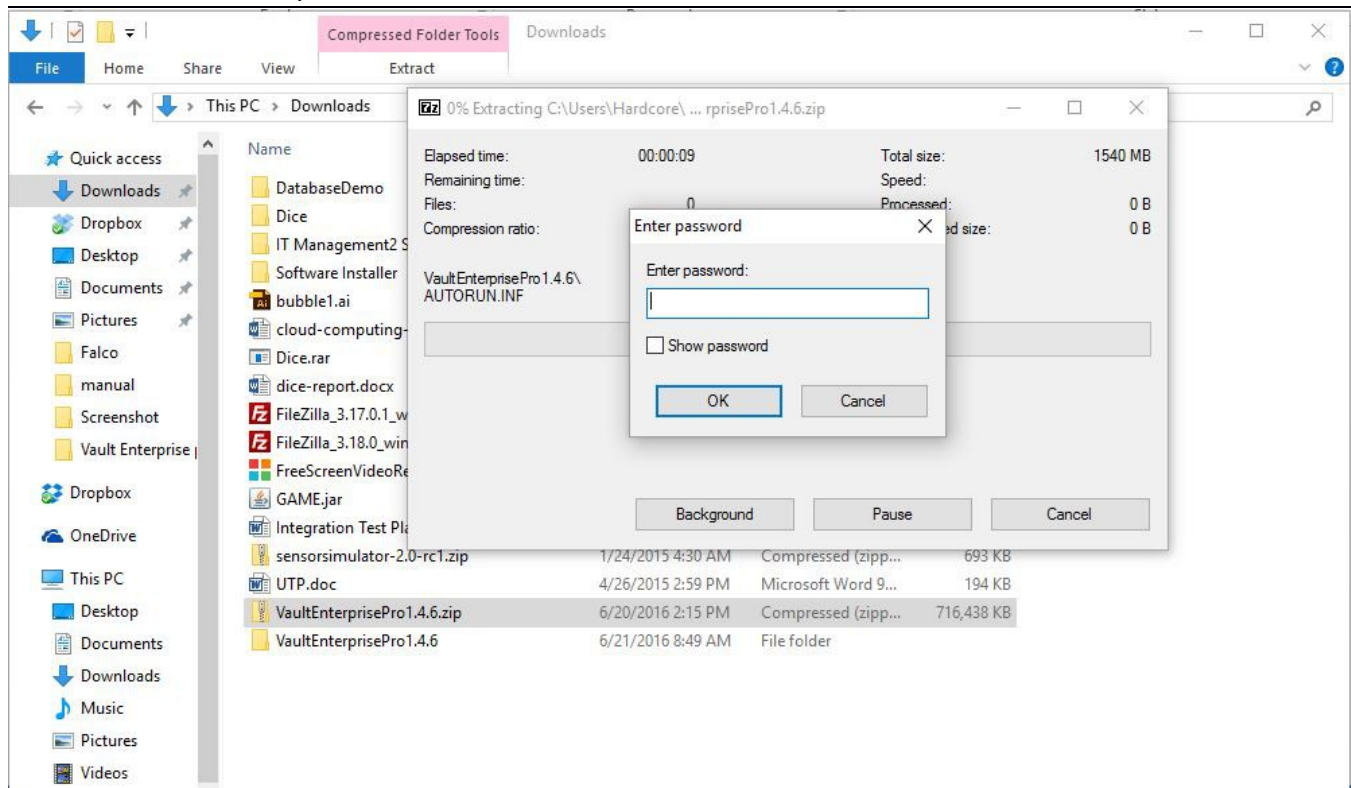


Step 3 – Click on the ‘Open folder’ button as illustrated in diagram below



Step 4 – Extract the zipped folder using any unzip tools and the password for the file extract is
‘Vaultpro1234’

Manual – VAULT Enterprise Professional



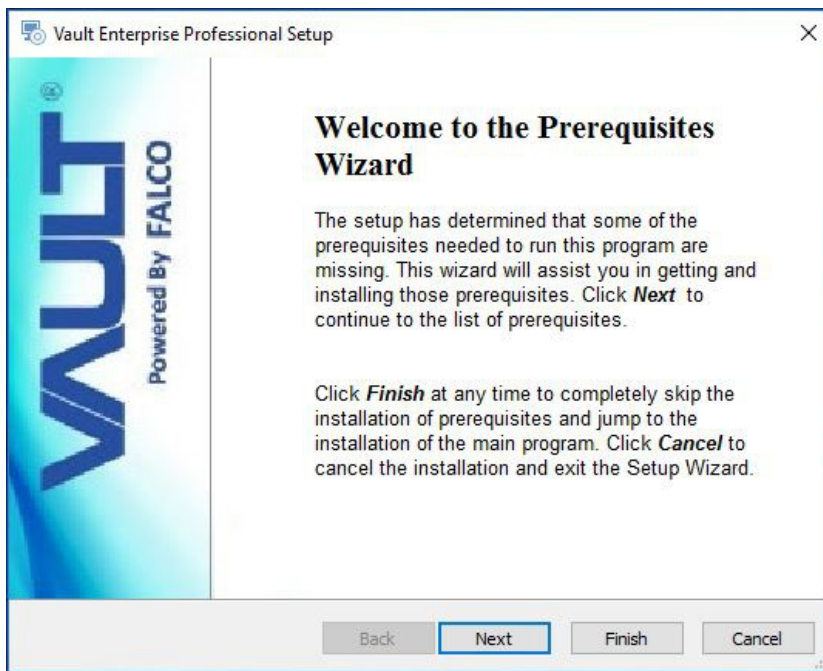
Step 5 – After the file is extracted, open the folder and double click the setup file.



2.2 Software Installation

Manual – VAULT Enterprise Professional

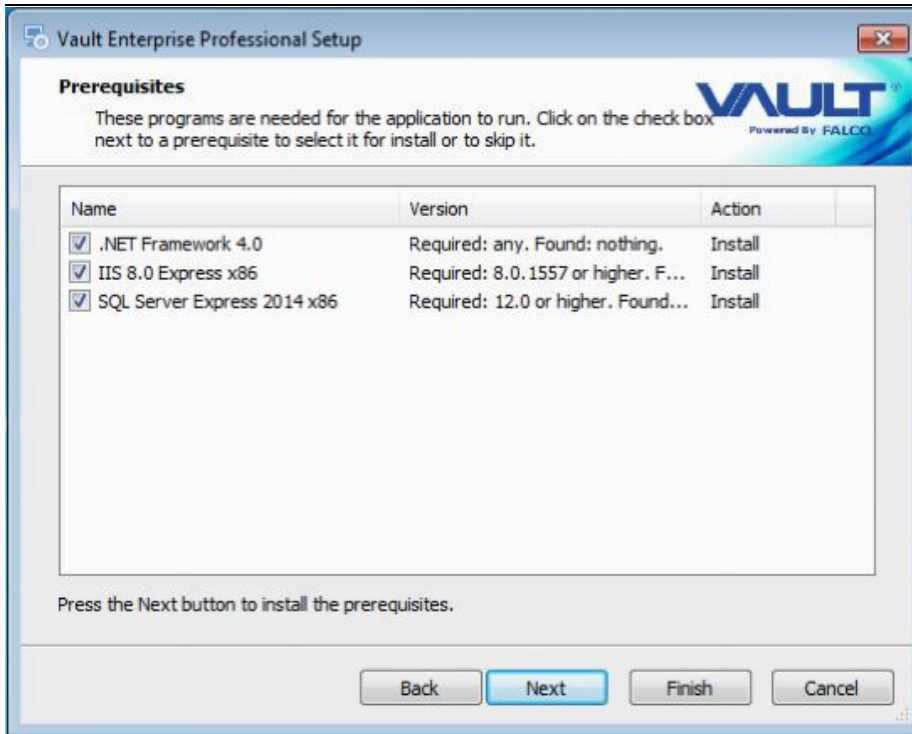
Step 1 – After running the setup file, click 'next' button to proceed as illustrated in the figure below.



Step 2 – Install the required software for the VAULT Enterprise Professional. By default, this installation wizard will automatic check on the software required which are not exist in the target machine.

So it is recommended to click the 'next' button to proceed with default setting.

Manual – VAULT Enterprise Professional



Step 3 – Install the required software before proceed to Vault Pro installation

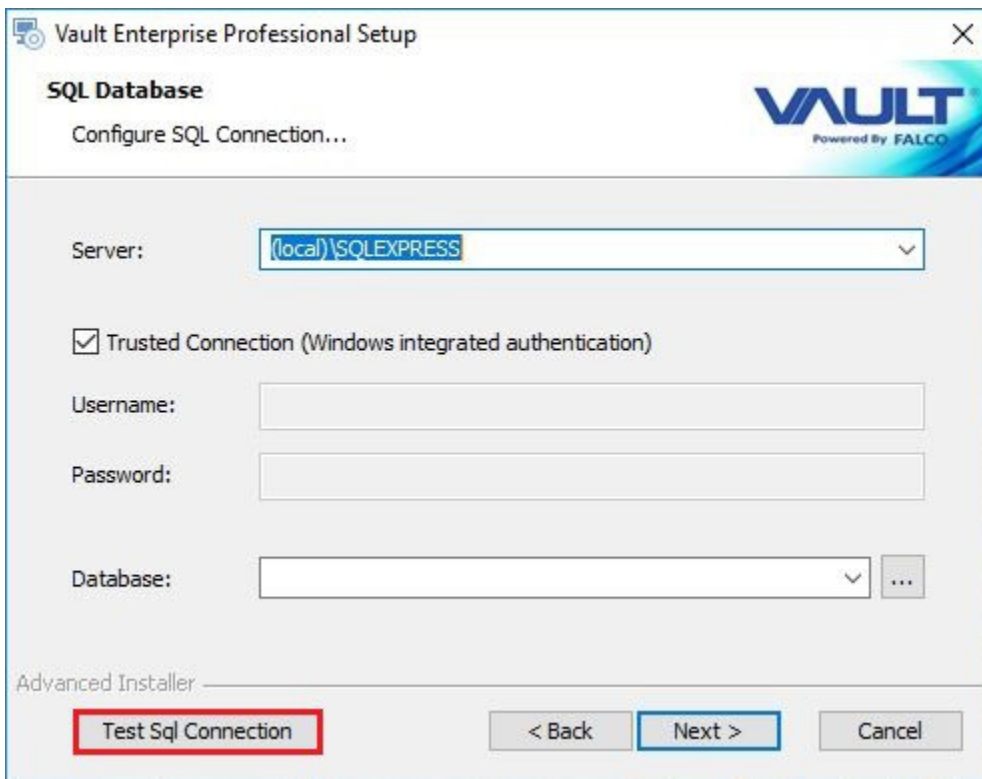
Step 4 – Wait for the installation finish and proceed to VAULT Enterprise Professional Installation.

Click the 'next' button to proceed as illustrated below.

Manual – VAULT Enterprise Professional

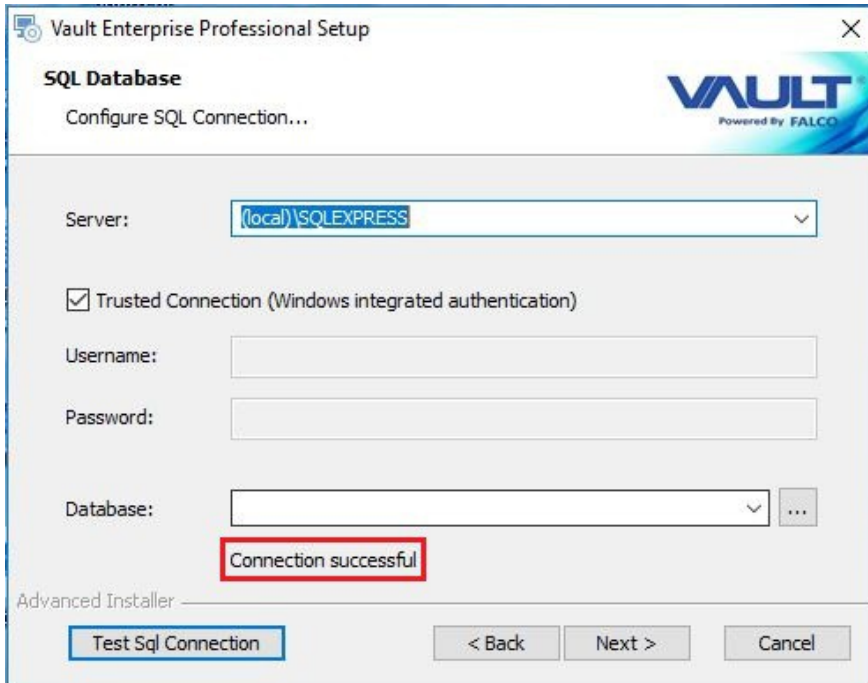


Step 5 – Select the server and test the sql connection by select the 'Test Sql Connection'

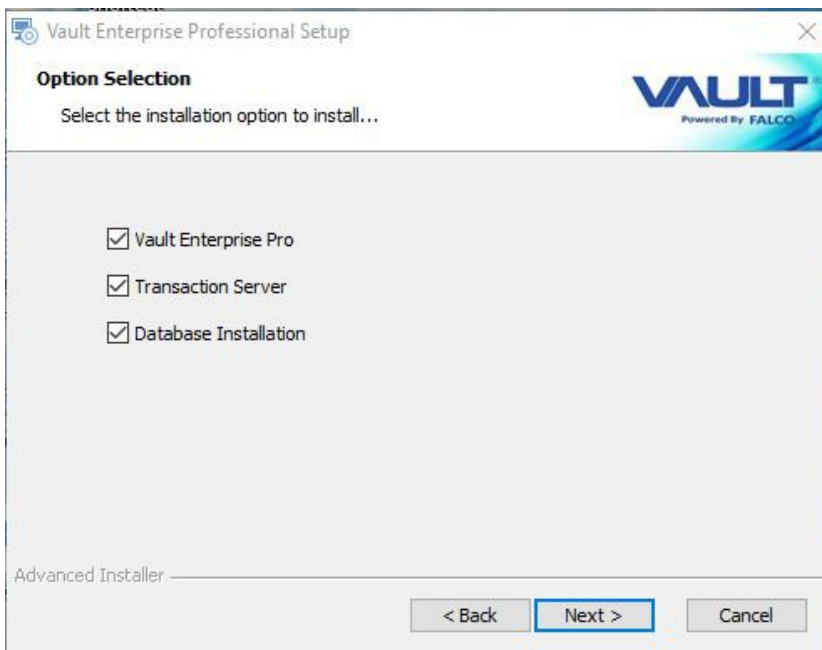


Manual – VAULT Enterprise Professional

Step 6 – Click next if the connection successful. If failed, check the sql server service is running on the target PC.

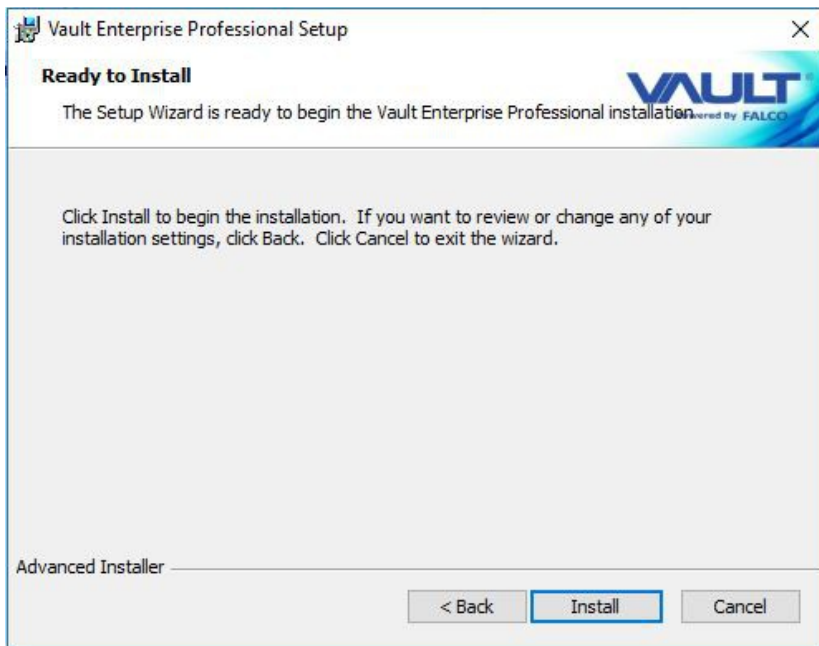


Step 7 – Select the installation option to install



Manual – VAULT Enterprise Professional

Step 8 – Click on the install button to start the VAULT Enterprise installation



Step 9 – After the installation complete, open this icon in desktop to start the VAULT Enterprise Pro.

CHAPTER 3 – ADMIN LOGIN

3.1 Admin Login

Login Screen - VAULT ENTERPRISE PRO

VAULT[®] English

Login ID :*
Enter you Login ID

Password :*
Enter your password

Login

2016 © Copyright by VAULT

The default login id is **admin** and the password is also **admin**.

3.2 First Time Setup

Manual – VAULT Enterprise Professional

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:* CENTRAL

Site Description: CENTRAL SERVER

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

Site Port No:* 2003

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

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:

2016 © Copyright by VAULT

This is the page where it will prompt out for the first time login. The site code is not able to change once the information, so it is advised to decide carefully before you save site code.

The Site GMT and the Site Reader Mode is set for the default value of the site. When download setting to the controller this time zone and reader mode will be downloaded based on the site selected.

Those * icon marked behind the field is the required fields. User must key in the data before it is saved while the other fields which are not marked in * are additional fields, these fields can be edit afterward in the site management under the control panel section.

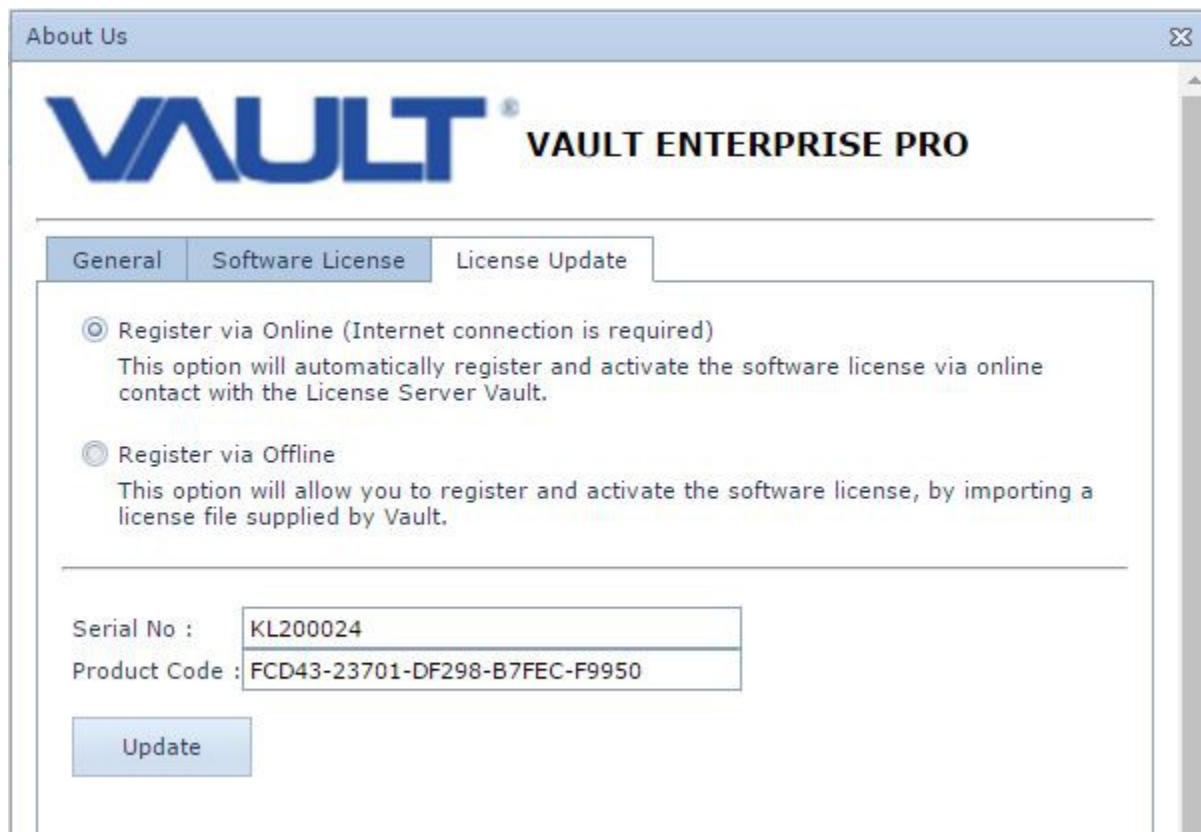
CHAPTER 4 – LICENSE ACTIVATION

4.1 Online Activation

Step 1 – Make sure your machine is connected to the internet.

Step 2 – Go to 'Help' > 'License Manager', then select the 'Register via Online' option

Step 3 – Enter the 'Serial No' and 'Product Code' given upon license purchased



The screenshot shows a software window titled "About Us" with a close button in the top right corner. The window content features the VAULT logo and the text "VAULT ENTERPRISE PRO". Below this, there are three tabs: "General", "Software License", and "License Update". The "License Update" tab is selected and active. Inside this tab, there are two radio button options: "Register via Online (Internet connection is required)" which is selected, and "Register via Offline". Below the options, there are two input fields: "Serial No" containing the text "KL200024" and "Product Code" containing the text "FCD43-23701-DF298-B7FEC-F9950". At the bottom left of the dialog, there is a blue "Update" button.

Step 4 – Click update button to update the license for the software.

4.2 Offline Activation

Step 1 – Go to ‘Help’ > ‘License Manager’, then select the ‘Register via Offline’ option

Step 2 – Enter the ‘Serial No’ and ‘Product Code’ given upon license purchased

Step 3 – Click on the ‘Download’ button to download the activation file and send the downloaded file through email to VAULT (suporte@vaultbr.com)

Step 4 – The Vault Enterprise will send a license file back to you. Browse the license file by clicking the ‘Browse...’ button and find the path where the license file is saved.

The screenshot shows the 'About Us' window of VAULT Enterprise Pro. The 'License Update' tab is active, showing two registration options: 'Register via Online' (selected) and 'Register via Offline' (selected). Below the options are input fields for 'Serial No' (KL200024) and 'Product Code' (FCD43-23701-DF298-B7FEC-F9950). Instructions for offline activation are provided, including a 'Download' button. A file browser shows 'MasterFIPS.lic' with a 'Browse...' button. An 'Update' button is at the bottom.

Step 5 – Click the ‘Update’ button to update the license for the software.

CHAPTER 5 – VAULT BASIC DOOR CONFIGURATION

5.1 Add Controller

Button Name	Explanation
New Controller	- To add new controller
Add Ext	- Only for Add the Double Door Controller
Manual	- Manually to key in a controller IP without auto detect function
Pointer	- Roll back the previous transaction
Edit	- For Edit the Door Controller Setting
Delete	- Delete a Controller
Pdf	- Download as PDF
Xls	- Download as Excel file

Step 1 – Make sure the firewall is turn off and the controller is able to ping from your computer by typing 'ping [Your controller IP]' in command prompt as illustrated below.

```

C:\Users\Hardcore>ping 192.168.0.48

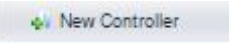
Pinging 192.168.0.48 with 32 bytes of data:
Reply from 192.168.0.48: bytes=32 time=1ms TTL=128
Reply from 192.168.0.48: bytes=32 time<1ms TTL=128
Reply from 192.168.0.48: bytes=32 time<1ms TTL=128
Reply from 192.168.0.48: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.0.48:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Users\Hardcore>
  
```

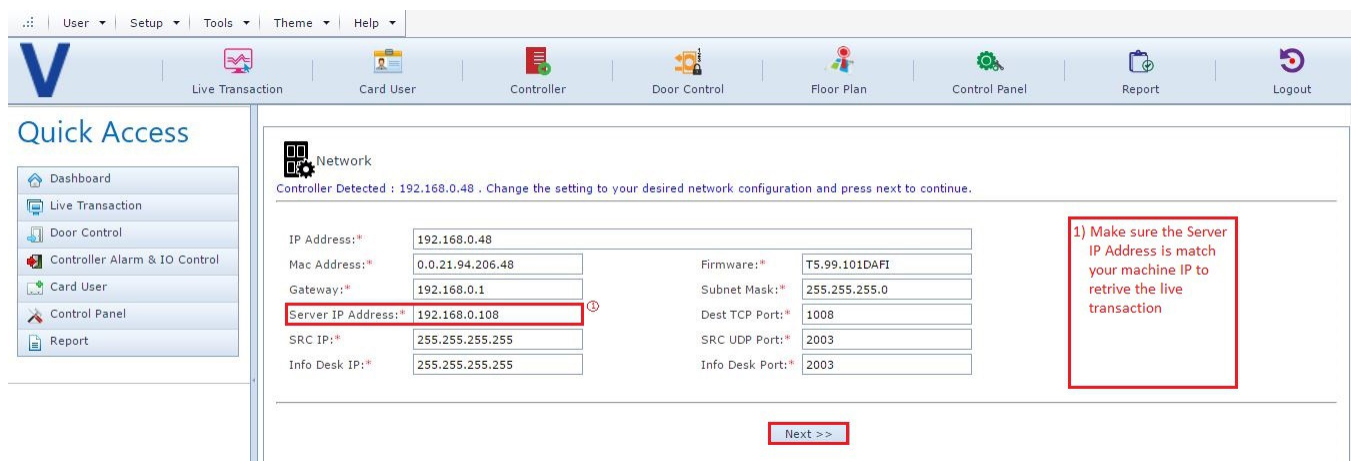
The Controller is able to ping

Manual – VAULT Enterprise Professional

Step 2 – Go to the controller tab, click the  button in the controller list to add a new controller

Step 3 – Choose the controller from the controller searching list and click the  button.

Step 4 – Configure the newly added controller network setting and click the 'Next' button. Make sure the server IP address is match your current PC's IP address. You can check the PC IP by typing 'IPCONFIG' in the command prompt and look for the 'IPv4 Address'.



Network

Controller Detected : 192.168.0.48 . Change the setting to your desired network configuration and press next to continue.

IP Address:*	192.168.0.48	Firmware:*	T5.99.101DAFI
Mac Address:*	0.0.21.94.206.48	Subnet Mask:*	255.255.255.0
Gateway:*	192.168.0.1	Dest TCP Port:*	1008
Server IP Address:*	192.168.0.108	SRC UDP Port:*	2003
SRC IP:*	255.255.255.255	Info Desk Port:*	2003
Info Desk IP:*	255.255.255.255		

1) Make sure the Server IP Address is match your machine IP to retrieve the live transaction

Next >>

Step 5 – Set your controller name, description and site of the control where it belong in the controller Details tab.

Manual – VAULT Enterprise Professional

Controller Profile
192.168.0.48 :

Controller Details | **Setting** | Network Configuration | Camera Setting | Alarm Config | ID Config

Controller Name: Door 1
Description: Door 1
Site Control: CENTRAL
Unit No: 1
IP Address: 192.168.0.48
Mac Address: 0.0.21.94.206.48
Controller ID: 0
Firmware: T5.99.101DAFI
Controller Status: Active

Controller Type

Alarm: I/O: Lift:
LCD: Rack:

Select the controller type if the controller type is other than door controller, barrier or turnstile

Save Cancel

Step 6 – Go to the Setting tab to configure the door setting such as open time, release time, Antipassback, fire alarm and etc.

Controller Profile
192.168.0.48 :

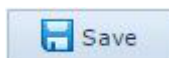
Controller Details | Setting | **Network Configuration** | Camera Setting | Alarm Config | ID Config

Controller Configuration

Open Time (s) : [Slider] Release Time (s) : [Slider]
Open Time (s) : 5 Release Time (s) : 2
Lock Release TZ: 00 Push Button TZ: 01
Antipassback: 00 Global Antipassback Group: Disable
Rack ID / Group : 1 Rack Control: 1-16

Mode

Fire Alarm: Enable Guard Tour: Enable
Buzzer Door Release: Enable Card Lockout: Enable
Auto Pin: Enable Report Mode: Enable
Emergency Card Mode: Enable Interlocking Mode: Enable
Car Park Max Spot: Enable Car Park Group: 1
Minimum Population: Enable Minimum Population Group: 1
Turnstile Penalty: Enable Canteen Mode: Enable



Step 7 – Click button to save the setting and download the setting to the controller.

5.2 Controller Setting

Most of the controller setting for the controller can be found here. The detail explanation is specify in the following sub-chapter.

5.2.1 Basic Controller Setting

Features	Explanation
Open Time (sec)	<ul style="list-style-type: none"> - The time for the door to close after it is opened, if the open time exceed, the buzzer sound will be triggered.
Release Time (sec)	<ul style="list-style-type: none"> - The time for the EM-Lock to release when valid entry/exit. * The release time can't be larger than open time
Lock Release TZ	<ul style="list-style-type: none"> - The period for the EM – Lock remain release based on Time Zone.
Push Button TZ	<ul style="list-style-type: none"> - The period to use the push button to entry/exit the building based on Time Zone
Antipassback	<ul style="list-style-type: none"> - Enable or disable the Antipassback for the controller based on Time Zone - Antipassback is a feature where the card user must follow the rule where he/she only can entry once and he/she must exit before the next entry.
Global Antipassback Group	<ul style="list-style-type: none"> - Group multiple controller into a group to apply the Antipassback rule. * In order to use Global Antipassback Group, the antipassback feature must be enabled
Rack ID / Group	<ul style="list-style-type: none"> - Specify the Id for multiple rack controller into a group
Rack Control	<ul style="list-style-type: none"> - Specify the available rack connected to the controller

5.2.2 Controller Mode

Features	Explanation
Fire Alarm	<ul style="list-style-type: none"> - Enable this feature if the controller type is fire alarm type - When fire alarm detected, the controller will be set the security off.
Buzzer Door Release	<ul style="list-style-type: none"> - Enable/disable the buzzer sound when the Lock Release TZ feature is enabled <p style="color: red; margin-top: 10px;">* Must work with Lock Release TZ feature</p>
Auto pin	<ul style="list-style-type: none"> - Enable/disable to use the auto pin for the current controller
Emergency Card Mode	<ul style="list-style-type: none"> - Enable/disable the controller utilize the emergency card mode when the emergency card is swipe to the controller the security will off directly, just like the fire alarm feature.
Car Park Max Spot	<ul style="list-style-type: none"> - Enable/disable for the maximum car park counter feature to limit the entry into the car park
Minimum Population	<ul style="list-style-type: none"> - Enable/disable for people counter feature
Turnstile Penalty	<ul style="list-style-type: none"> - After flashed card, within one minute if the card is are not entering the door card will be suspended or disabled. (Disallow to access)
Guard Tour	<ul style="list-style-type: none"> - Enable/disable to integrate with the guard tour monitoring system
Card Lockout	<ul style="list-style-type: none"> - Enable/disable the card to be suspended under 3 condition (3 times incorrect pin entered, 3 times wrong time zone transaction received and 3 times antipassback violation transaction received.)
Report Mode	<ul style="list-style-type: none"> - Enable/disable the activity report function, so that if the card user is set to have a report for accessed, then if he/she didn't make a report. He/she will not be allowed to go out from the door.
Interlocking Mode	<ul style="list-style-type: none"> - Enable/disable the interlocking mode for the controller.

Manual – VAULT Enterprise Professional

	- The rule of the interlocking is one door must be completely closed before entering another door with interlocking mode enable.
Car Park Group	- group the relevant car park controller in the group
Minimum Population Group	- group the relevant controller in the group
Canteen Mode	- Enable/disable to use the canteen mode for the controller

5.2.3 Card & Pin

Card and pin is a feature that allow user to use reader which have scan card and auto pin feature. Tick the checkbox to enable the card & pin mode if the reader is using card and pin together to access the building. Set the entry time zone and/or exit time zone to use the Card & Pin Mode for the period of time.

Card & Pin

Card & Pin : Enable

Entry TZ: Exit TZ:

5.2.4 Dual Card Mode

Dual card mode is a feature that provide a more secured solution to access a building.

Dual Card Mode

Dual Card: Enable

Entry TZ: Exit TZ:

5.2.5 Auto Pin No

Auto Pin Number is a feature that allows user to set a preset pin number to access to a building. There are total 10 different pin number are allowed to preset with its time zone to allow the user to use respective pin number to access into a building.

Manual – VAULT Enterprise Professional

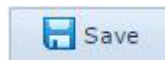
Auto Pin No

1.) Pin No: <input type="text" value="1234"/>	TZ: <input type="text" value="01"/>	6.) Pin No: <input type="text" value="0000"/>	TZ: <input type="text" value="00"/>
2.) Pin No: <input type="text" value="6584"/>	TZ: <input type="text" value="01"/>	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"/>

5.3 Network configuration

Go to the network configuration tab to set the controller IP address, Gateway, Server IP address, Subnet Mask and Destination TCP Port. By default, these network setting is automatically configured when the controller is added with its default value. Just in case if the user want to manually change the network settings, the user can configure the setting here. After the all the network setting is configured, press



the ‘Set Network Setting’ button before pressing the  button. The user also can retrieve the network setting from the controller by pressing the ‘Retrieve Network Setting ’ button to double check the network setting is set correctly.

*** The Server IP Address must match the target PC IP address which the VAULT System is installed to retrieve live transaction. To check the PC’s IP address, please refer to chapter 3.1, step 4.**

The screenshot shows the VAULT web interface. At the top, there is a navigation bar with icons for Live Transaction, Card User, Controller, Door Control, Floor Plan, Control Panel, Report, and Logout. Below this is a 'Quick Access' sidebar with links to Dashboard, Live Transaction, Door Control, Controller Alarm & IO Control, Card User, Control Panel, and Report. The main content area is titled 'Controller Profile' and shows the IP address '192.168.0.49'. Below this, there are tabs for Controller Details, Setting, Network Configuration (which is selected), Camera Setting, and IO Control. In the Network Configuration tab, there are two buttons: 'Retrieve Network Setting' and 'Set Network Setting', both of which are highlighted with a red box. Below the buttons is a form with the following fields:

IP Address:	<input type="text" value="192.168.0.49"/>	Firmware:	<input type="text" value="T5.99.101DAFI"/>
Mac Address:	<input type="text" value="0.0.21.94.206.48"/>	Subnet Mask:	<input type="text" value="255.255.255.0"/>
Gateway:	<input type="text" value="192.168.0.1"/>	Dest TCP Port:	<input type="text" value="1008"/>
Server IP Address:	<input type="text" value="192.168.0.108"/>	SRC UDP Port:	<input type="text" value="2003"/>
SRC IP:	<input type="text" value="255.255.255.255"/>	Info Desk IP:	<input type="text" value="255.255.255.255"/>
Info Desk IP:	<input type="text" value="255.255.255.255"/>		

At the bottom of the form, there are 'Save' and 'Cancel' buttons.

5.4 Card Access Level

Card access level is a feature used to classify the levels for different group of people with different access level. In order to predefined the group access level, use the group card access level feature to predefined the authorize access to specific controllers for each of the access level.

5.4.1 Time Set & Time Zone


‘Time Set’ is the period of time to access in a day while ‘Time Zone’ is the period of time to access in a week with ‘Time Set’ set on each of the day. This time zone is important to give authorized access for particular group of user in a specified period.

To set ‘Time Set’ follow the following step:

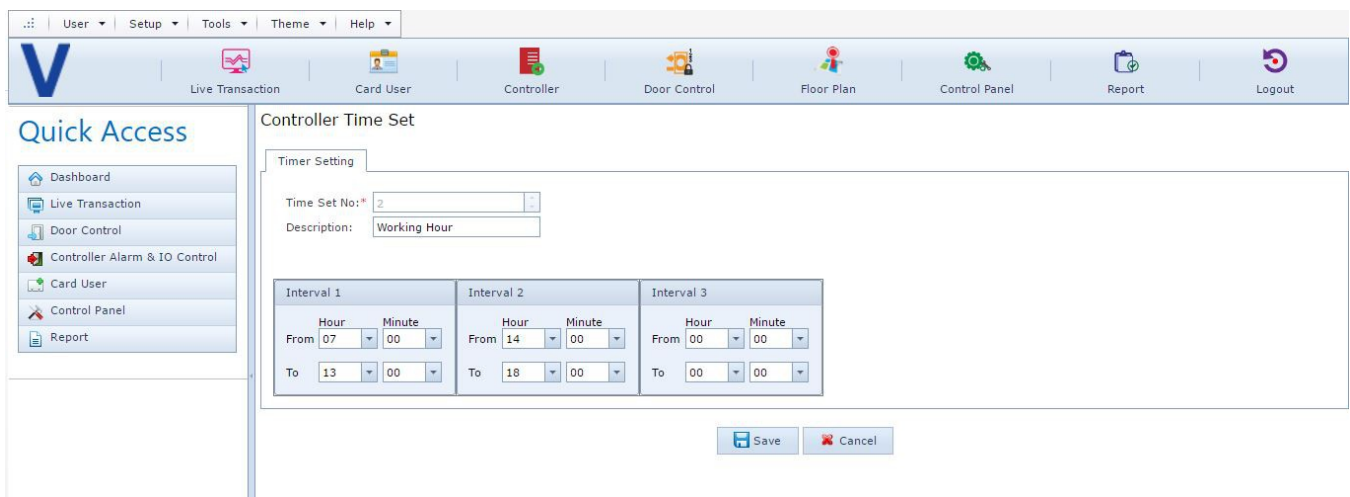
Step 1 – Go to controller panel and click on the ‘Time Set’ link under the controller management category or go to ‘Setup’ and click on the ‘Time Set’


The screenshot displays the VAULT Enterprise Professional web interface. At the top, there is a navigation bar with tabs for 'User', 'Setup', 'Tools', 'Theme', and 'Help'. Below this is a main menu with icons for 'Card User', 'Controller', 'Door Control', 'Floor Plan', 'Control Panel', 'Report', and 'Logout'. The 'Control Panel' tab is active. On the left side, there is a 'Quick Access' sidebar with various icons. The main content area is titled 'Which feature would you like to work with?' and contains several category tiles: 'Card Management', 'Group Management', 'User Management', 'Tool & Settings', 'Time Attendance', 'Site Management', 'Video Camera', and 'Fingerprint'. The 'Controller Management' category is expanded, showing a list of options including 'Controller List', 'Time Set', 'Time Zone', 'Lift Access Interval', 'Holiday', 'Alarm Holiday', 'IO Output Type', 'IO Output Trigger Group', 'Rack Access Level', 'Canteen Time Set', and 'Canteen Time Zone'. The 'Time Set' option is highlighted with a red box.



Step 2 – Click on the  button to add a new time set. By default, there are two time set is predefined which are 00 – 24 hours no access and 01 – 24 hours valid access.

Step 3 – Set the time interval and description for the new time set. The interval 1, interval 2 and interval 3 is used to set different time interval in a day. For example, working hour start from 7 am to 6pm and lunch time at 1pm to 2pm as shown in diagram below.

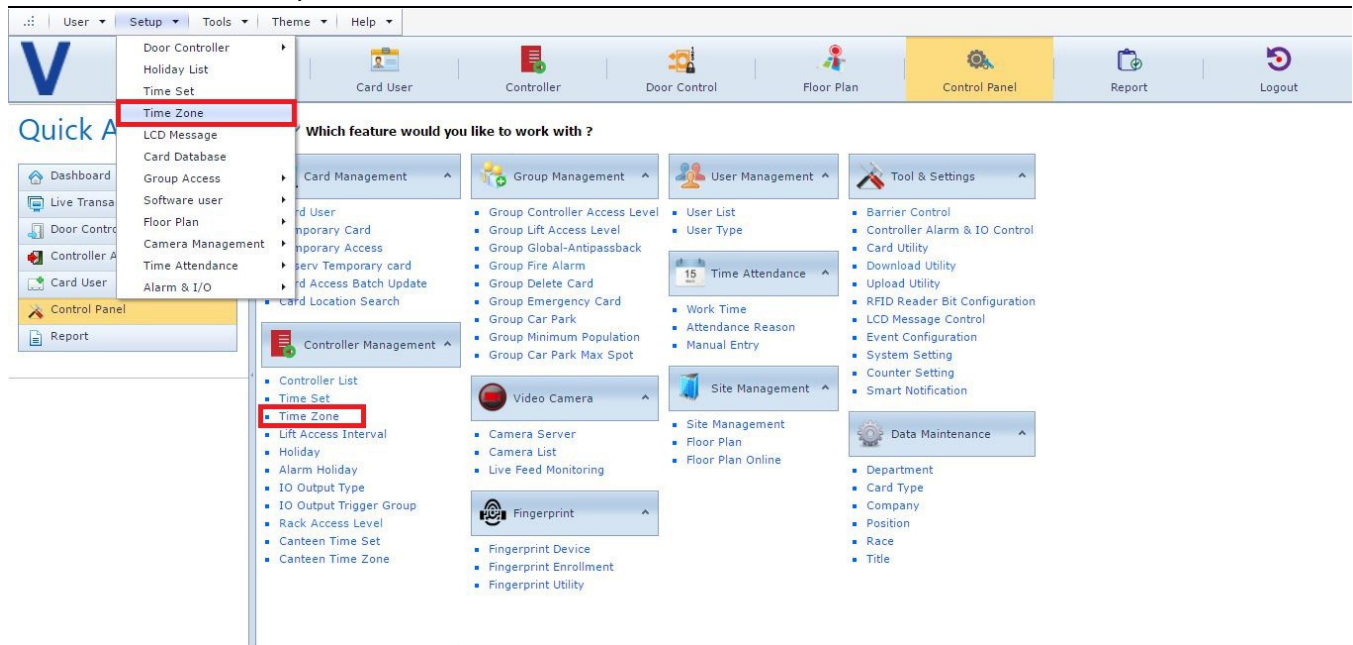



Step 4 – Click  button to save the time set and download it into the controller

To set Time Zone follow the following step:

Step 1 - Go to controller panel and click on the 'Time Zone' link under the controller management category or go to 'Setup' and click on the 'Time Zone'

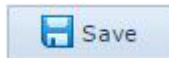
Manual – VAULT Enterprise Professional




Step 2 - Click on the  button to add a new time zone. By default, there are two time zone is predefined which are 00 – 24 hours a week no access and 01 – 24 hours a week valid access.

Step 3 – fill in the description and select the time set for each day of the time zone.

Manual – VAULT Enterprise Professional

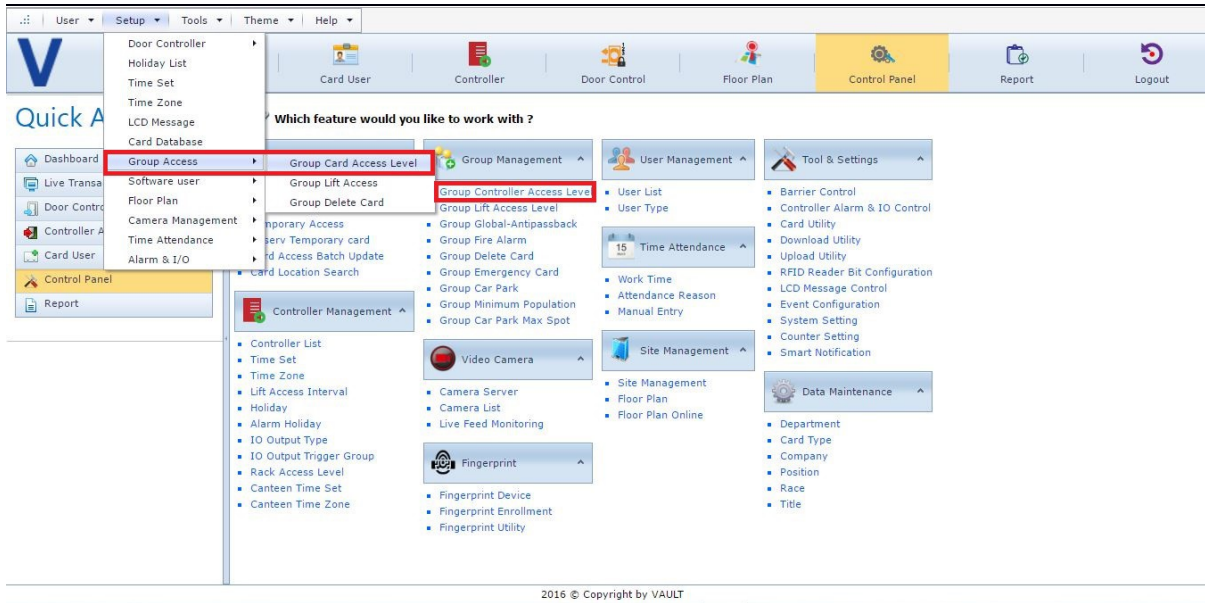


Step 4 – Click  button to save the time zone and download it into the controller.

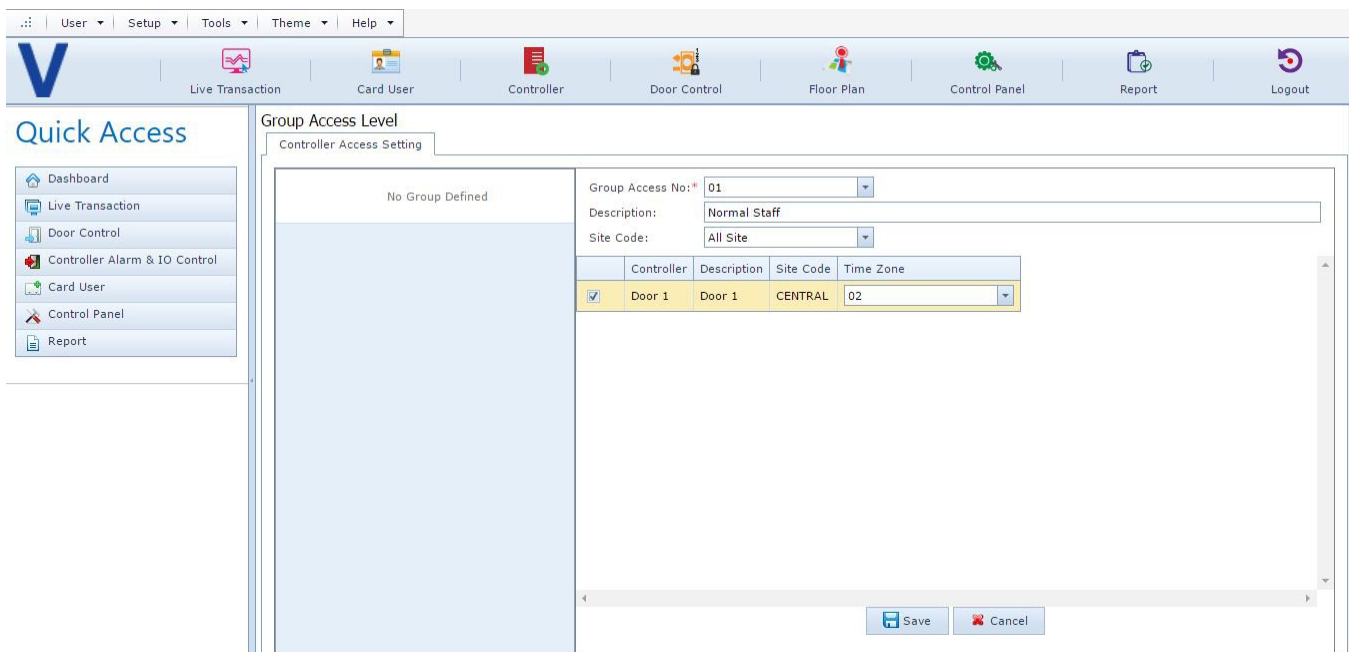
5.4.2 Group access level


Step 1 – Go to 'control panel' > 'Group Controller Access Level' under group management category or got to 'setup' > 'Group Access' > 'Group Card Access Level'

Manual – VAULT Enterprise Professional



Step 2 – Select the group access number and then fill in the description for the group. Tick the controllers to and select the time zone to give authorize access to the group.

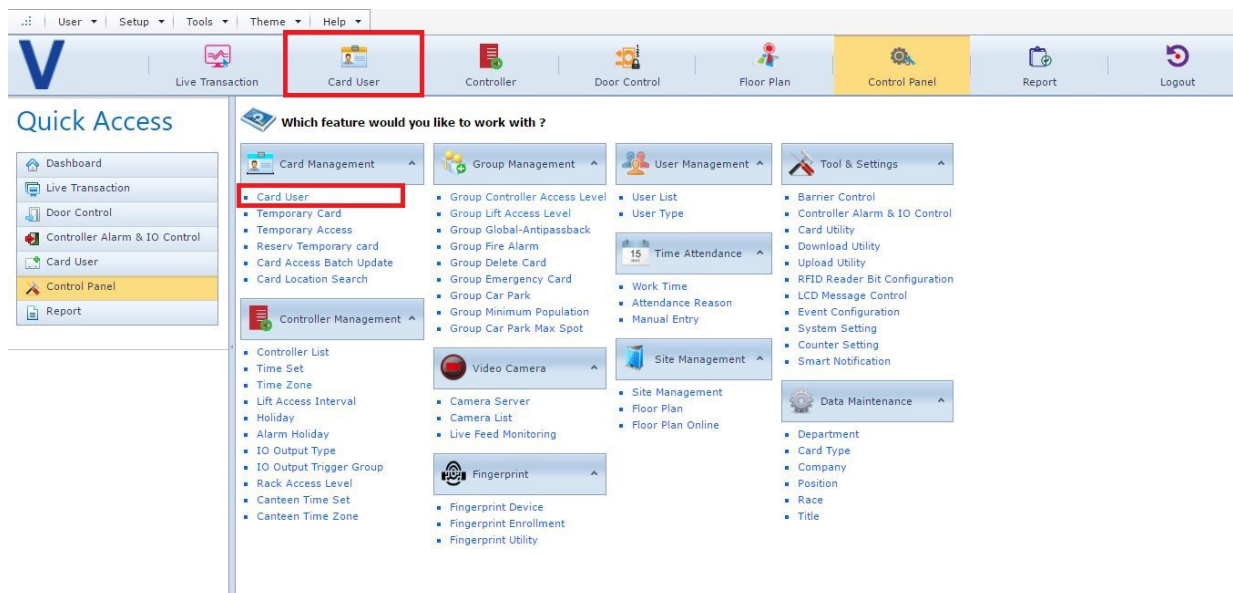


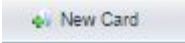
Step 3 – Click the  button to save the setting

5.5 Add Card User

Button Name	Explanation
New Card	- Add new card user
Batch Add	- Add a batch of continuous card number with the same setting
Edit	- Edit card user setting
Delete	- Delete card user
Back	- Back to dashboard page
Pdf	- Download as PDF
Xls	- Download as Excel file

Step 1 – Click the ‘Card User’ or go to ‘Control Panel’ > ‘Card User’ under card management category

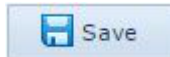


Step 2 – Click the  button in the card user list

Manual – VAULT Enterprise Professional

Step 3 – Fill in the card info, employee details and access level granted for the card user. The setting detail will be explain in the following sub-chapter.



Step 4 – Click the  button to save the settings and download the settings to the controller.

5.5.1 Card Info

Features	Explanation
Card No	- Card identity number.
Name	- Name of the card holder.
Site Code	- Site for the card holder belongs. - The option can be added in control panel under site management category.
Card Type	- Card type hold by the card holder. - The option can be added in control panel under data maintenance category.
Card Pin No	- Pin number specified for a card holder
Bypass Antipassback	- Authorize the card holder to bypass the antipassback rule (entry once and exit before the next entry)
Guard Tour Card	- Enable/disable to be the guard tour card for the tours and inspection performed by security officer at specific location
Dual Card Group	- Assign the card holder to a group for access. - The combination for the card to valid entry is master card + card in one of the group or 2 cards in the same group.
Card Expiry Status	- Enable/disable the card expiry date for the card
Expired Date	- Set the expired date of the card

Manual – VAULT Enterprise Professional

	<ul style="list-style-type: none"> - Must be enable the Card Expiry Status before set the expired date
Expired Time	<ul style="list-style-type: none"> - Set the expired time of the card - Must be enable the card expiry status before set the expired date
Car Park Max Spot Group	<ul style="list-style-type: none"> - Assign the card holders to the car park max spot group - If the counter already reach the max spot, the current card holder is unable to enter the card park
Biometric Authentication	<ul style="list-style-type: none"> - Option selection of the authentication mode for the card holder (Fingerprint/pin/card)
Alarm Card	<ul style="list-style-type: none"> - Enable/disable the card to be an alarm card to arm and disarm alarm.
Card Status	<ul style="list-style-type: none"> - Activate or deactivate the card
Rack Access Level	<ul style="list-style-type: none"> - Option selection for the rack zone for the card holder
Emergency Card Type	<ul style="list-style-type: none"> - Enable/disable the emergency card
Canteen TZ	<ul style="list-style-type: none"> - Option selection for the canteen time zone
Attendance Control	<ul style="list-style-type: none"> - <i>Please refer chapter 8 for time attendance setting</i>
Floor No.	<ul style="list-style-type: none"> - Floor number for the card holder is staying
Unit No.	<ul style="list-style-type: none"> - Unit number for the card holder is staying
Plate	<ul style="list-style-type: none"> - Car plate number
Parking Lot No.	<ul style="list-style-type: none"> - Parking lot number for the card holder

5.5.2 Employee Details

Features	Explanation
Staff no.	<ul style="list-style-type: none"> - Identity number for a staff
Title	<ul style="list-style-type: none"> - Card holder appellation (Mr/Mrs)
Position	<ul style="list-style-type: none"> - Position of the card holder

Manual – VAULT Enterprise Professional

	- The option can be added in control panel under data maintenance category
NRIC no.	- National identity number
Passport no.	- Passport number
EPF no.	- Employee Provident Fund number
Socco no.	- Employee's insurance number
Department	- Department of the card holder belong - The option can be added in control panel under data maintenance category
Company name	- Name of the company - The option can be added on control panel under data maintenance category
Gender	- Sex of the card holder (male/female)
Race	- Race of the card holder - The option can be added in control panel under data maintenance category
Date of birth	- Birthday of the card holder
Marital status	- Marriage status of the card holder (single/married)
Joining date	- Date of the card holder joining the company
Resign date	- Date of the card holder resign the company
Address	- Address of the card holder
Adjunct	- Additional address information
Postal code	- Postcode of the card holder living
City	- City name of the card holder living
State	- State name of the card holder living
Country	- Country of the card holder staying
Email	- Email address of the card holder
Phone	- Phone number of the card holder

Manual – VAULT Enterprise Professional

Extension	- Extension of the phone number (e.g. +06)
Fax no.	- Fax number of the card holder
Mobile no.	- Mobile number of the card holder
Remarks	- Additional information about the card holder (Optional)
Emergency Contact No	- Additional contact number for emergency use
Contact person	- The person name of the emergency contact



5.5.3 Access Level


There are two type of access level is able to choose which are controller and lift access level.

Controller access level:



This controller access level is a feature which give the current selected user the authorization to enter certain doors or barrier gate using the card. The administrative can give the card user authorization using group access number or custom mode.

The group access no is based on the number of the group card access level. Please refer to 3.4.2 to configure the group access level. Select the access group for the current user to add the user into the

group and click  button and the predefine setting will be set automatically based on the setting in the group access level selected. Then click  to save the setting and download to the controller.

To use the custom mode to set the user access level, tick on the custom mode and custom the access level manually and click  to save the settings and download to the controller.

Lift access level:

Select the group lift access level number desired and click on the  button to set the predefined setting and click  button to save the setting and download to the lift controller.

5.5.4 Custom Fields

Custom field is a feature where you can add extra fields that is not in the ‘Employee Details’ tab. There are 5 custom field are able to add. You need to enable it first before entering the data. The following are the steps to add a custom field.



Step 1 – Go to ‘Control Panel’ > ‘System Setting’ under ‘Tool & Settings Category’, and then go to ‘Card User Custom Field’ tab to enable the custom field.

System Preference and Configuration

General Setting | Email Notification | **Card User Custom Field** | Report Setting

Custom Field Setting

Enable: <input checked="" type="checkbox"/>	Field name: <input type="text" value="Field1"/>	<input type="checkbox"/> Required field
Enable: <input checked="" type="checkbox"/>	Field name: <input type="text" value="Field2"/>	<input type="checkbox"/> Required field
Enable: <input type="checkbox"/>	Field name: <input type="text" value="Max 50 character"/>	<input type="checkbox"/> Required field
Enable: <input type="checkbox"/>	Field name: <input type="text" value="Max 50 character"/>	<input type="checkbox"/> Required field
Enable: <input type="checkbox"/>	Field name: <input type="text" value="Max 50 character"/>	<input type="checkbox"/> Required field

Step 2 – Click  to save the settings


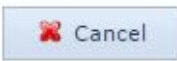
Step 3 – Go back to ‘Card User’ > ‘Custom Fields’ tab and go to the ‘Custom Fields’ tab to fill in the data.

Card Profile


Card Info Employee Details **Access Level** Custom Fields

Field1:

Field2:

 Save  Cancel




Step 4 – Click  button to save the data and download to the controller.

5.6 Live Transaction

Step 1 – Make sure the firewall is turned off, transaction server is running and the controller's server IP address is set correctly. To set the controller server IP address, please refer to 3.3 network configuration.



Step 2 – If the transaction server is not running, double click  icon in desktop. Click on the 'Start' button to start the service.

Manual – VAULT Enterprise Professional

VAULT ENTERPRISE PRO Transaction Server 1.4.6

Setting Help

Reset Start Stop Live Transaction Door Status Sync Date Exit

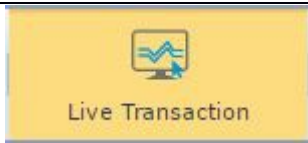
Thursday, 23 Jun 2016 10:33:17 AM

Live Transaction Door Status

Date & Time	Unit No	Door	Card No	Name	Transaction
2016/06/23 10:32:52			FFFFFFFF		Transaction Server Service Stop...
2016/06/23 10:26:04			FFFFFFFF		Transaction Server service online

Status : Offline

Manual – VAULT Enterprise Professional



Step 3 – Go to **Live Transaction** tab to view the live transaction.

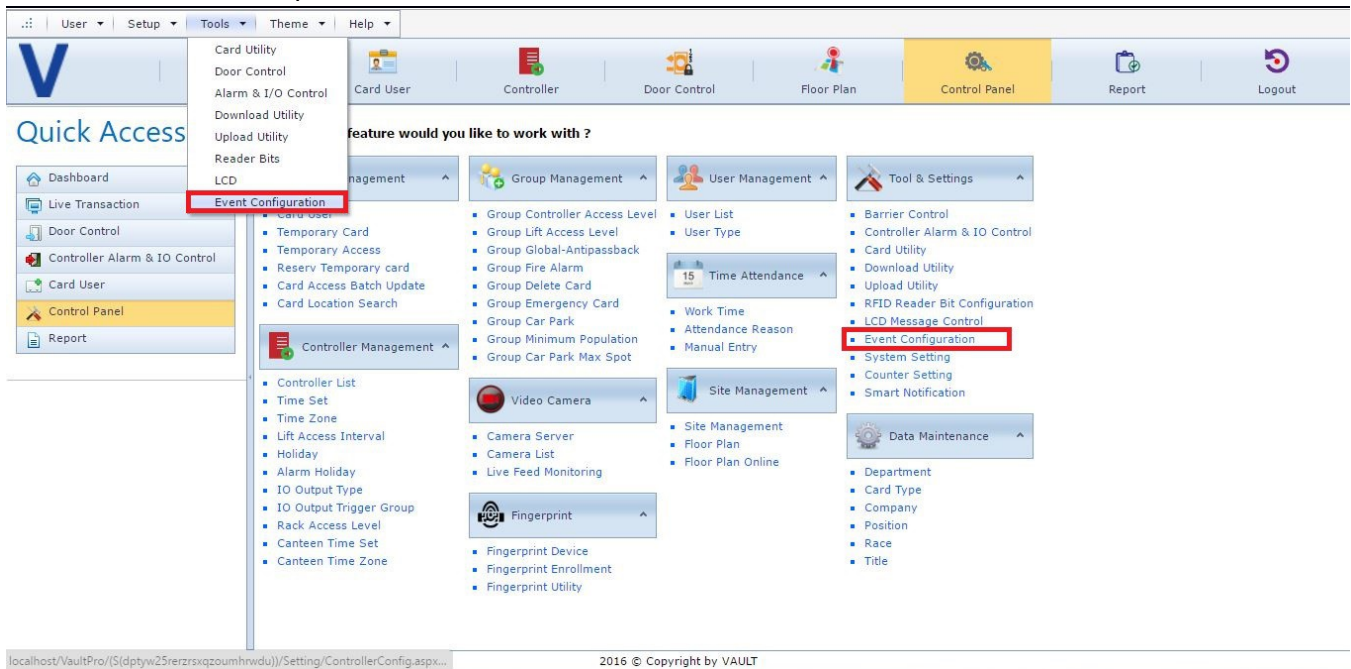
#	Date & Time	Site	Controller	Card No	Name	Staff No	Transaction
23:29:02	2016/06/22	CENTRAL	Door 1	FFFFFFFF			Controller Down
22:14:00	2016/06/22	CENTRAL	Door 1	FFFFFFFF			Controller Down
20:58:57	2016/06/22	CENTRAL	Door 1	FFFFFFFF			Controller Down
19:43:55	2016/06/22	CENTRAL	Door 1	FFFFFFFF			Controller Down
17:29:45	2016/06/22	CENTRAL	Door 1	FFFFFFFF			Battery Low
16:58:48	2016/06/22	CENTRAL	Door 1	FFFFFFFF			Battery Low
16:27:52	2016/06/22	CENTRAL	Door 1	FFFFFFFF			Battery Low
15:56:55	2016/06/22	CENTRAL	Door 1	FFFFFFFF			Battery Low
15:25:56	2016/06/22	CENTRAL	Door 1	FFFFFFFF			Battery Low
14:54:59	2016/06/22	CENTRAL	Door 1	FFFFFFFF			Battery Low
14:33:37	2016/06/22	CENTRAL	Door 1	FFFFFFFF			Pulse Door Open
14:24:02	2016/06/22	CENTRAL	Door 1	FFFFFFFF			Battery Low
14:10:06	2016/06/22	CENTRAL	Door 1	0000061084	Test		Valid Entry Access
13:53:05	2016/06/22	CENTRAL	Door 1	FFFFFFFF			Battery Low
12:55:28	2016/06/22	CENTRAL	Door 1	FFFFFFFF			Pulse Door Open
12:51:10	2016/06/22	CENTRAL	Door 1	FFFFFFFF			Battery Low
12:20:13	2016/06/22	CENTRAL	Door 1	FFFFFFFF			Battery Low

5.6.1 Transaction Sign

The color of the transaction sign is able to customize using the Event Configuration to set preferences color for each of the transaction event.


Step 1 – Go to ‘Control Pane’ > ‘Event Configuration’ under the tools & settings category or ‘tools’ > ‘Event Configuration’

Manual – VAULT Enterprise Professional



Step 2 – Set the preference color for each of the transaction event.



Step 3 – Click  to save the settings.

5.6.2 Live Transaction Tab

Filter – Filter the transaction record based on the criteria.

Start – Start the transaction server

Stop – Stop the transaction server

Acknowledge All Alarm Event – A shortcut to acknowledge all the alarm instead of one by one through the additional feature describe in the following chapter

Alarm Manual Entry – Manually add the alarm transaction to acknowledge alarm instead of the predefined transaction

5.6.3 Alarm List Tab

Show only the alarm transaction that is triggered only such as controller down, unknown card, battery low and etc. for a quicker access to the alarm triggered around the premises.

5.6.4 Card User Monitoring Tab


Monitor the card access transaction for the entry and exit of each of the card user with the picture registered with the card to let the security officer recognize the valid card holder when the card user entry or exit the building

5.6.5 Controller Status Tab

Check the status of all the controller is online/offline through the status to ensure the communication between the software and controller is established in order to receive transaction from controller.

5.6.6 Live Transaction Additional Feature










Click on the  on a transaction record to open up the transaction view dialog as shown in figure below.

Manual – VAULT Enterprise Professional

- Click to view the playback with the time according to the time when the transaction happened.
- Video Comparison
 - Compare the Entry and Exit of the card holder to verify it is the same card holder.
 - The button is enable in the exit transaction only.

5.7 Transaction Server Software

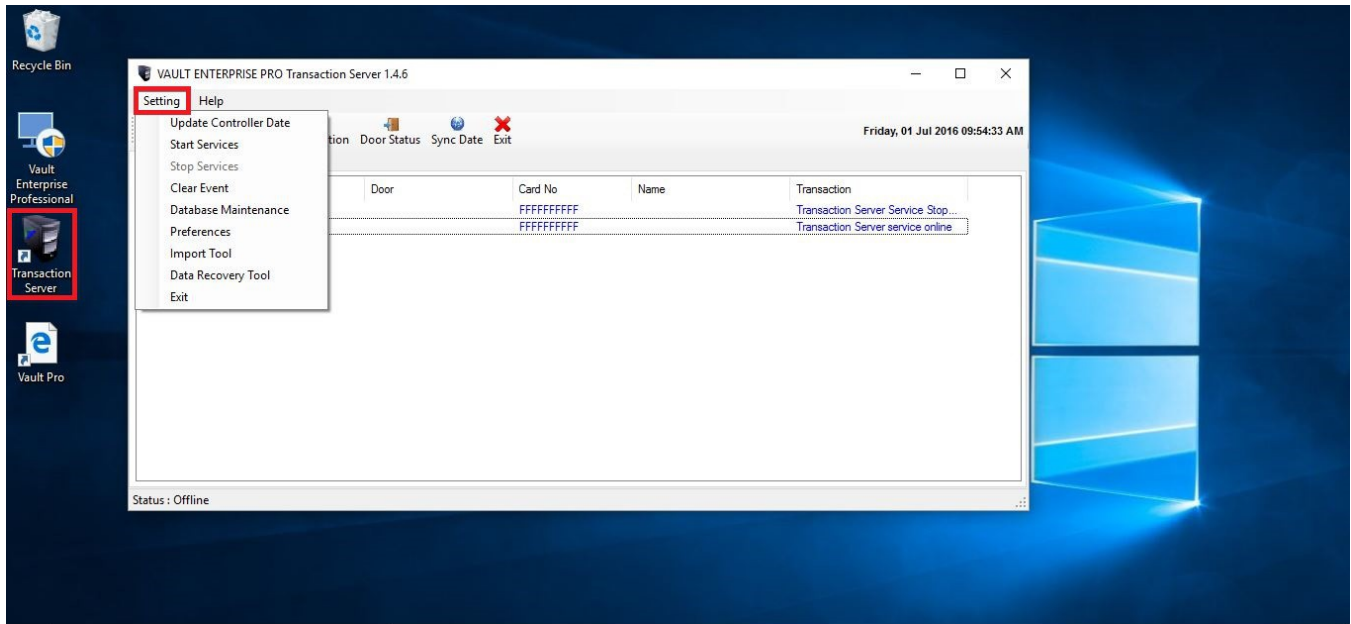
Transaction server software is a software that is installed with the Vault Enterprise Professional to receive the transaction from the controller. Besides, this software also provide few features for the user to manage the database and notification easily. The table below explain the quick icon button in the transactions server software.

Features	Explanation
 Reset	- Reset/clear the transaction event
 Start	- Start the transaction server service
 Stop	- Stop the transaction server service
 Live Transaction	- View the live transaction
 Door Status	- View the status of every door controller (Online/Offline)
 Sync Date	- Synchronize the controller data time from software
 Exit	- Close the Transaction Server

5.7.1 Setting Tab

Manual – VAULT Enterprise Professional

This setting tab allow you to set your own preference for notification, system setting and data management. In order to go to this tab, open the 'Transaction Server.exe' on your desktop and then go to setting tab.



Update Controller Date – Allows you to synchronize the date time of your controller from pc

Start Service – Start the transaction service

Stop Service – Stop the transaction service

Clear Event – Clear all the transaction event on the live transaction

Database Maintenance – Allow you to manage the server database such as restore or backup database. *This will be cover in the chapter 4.7.2.*

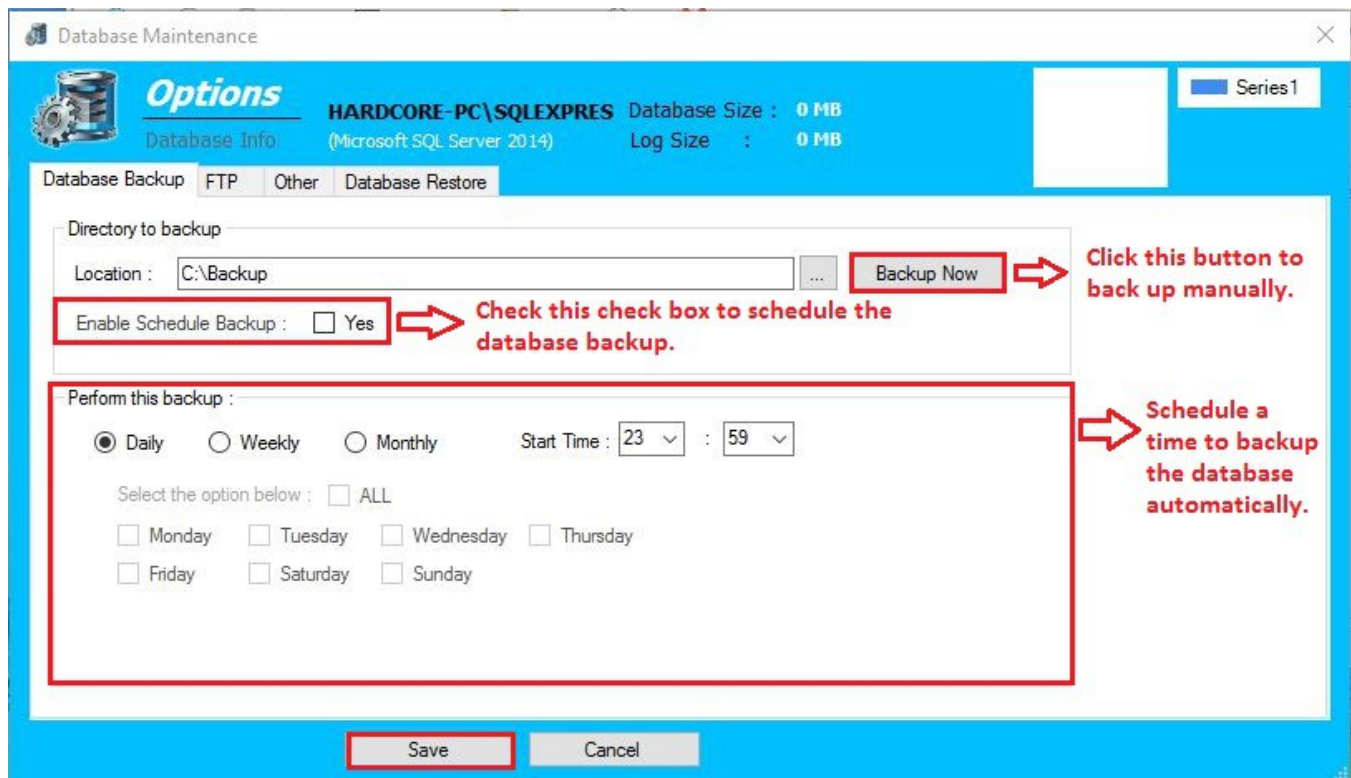
Preference – System configuration setting for notification, database connection and etc. *This will be cover in chapter 4.7.3.*

Import Tool – Allows you to import the card data and department data. *This will be cover in chapter 4.7.4.*

Data Recovery Tool – This is the feature allows you to restore the data back to the database if the data insert to database is failed.

5.7.2 Database Maintenance

Database Backup tab – Backup the vault enterprise database manually or scheduled. Browse for the directory to store the backup file and click the ‘Backup Now’ button to backup manually or enable the schedule Backup by checking the ‘Enable Schedule Backup’ checkbox and schedule the database backup.



FTP tab – Allow to save the schedule backup file into the FTP Server instead of local PC

Other tab – Allow to manage the transaction event to specify a time to keep the transaction record or delete the transaction directly with a specified time period. Besides, you also can reduce database log file in here.

Database Restore tab – Allow to restore the Vault database by browsing the backup file and click 'Restore Now' button to restore the database

5.7.3 Preferences

Email Notification tab – Configure the email server setting to send alarm notification to few specified recipients to notify them when alarm event is detected.

SMS Notification tab – Configure the phone Short Message Service (SMS) setting to send alarm notification to few specified recipients to notify them when alarm event is detected.

System Setting tab – Provide feature to sync the time in a schedule time. Besides, it also have a feature to enable guard tour mode to integrate with Guard tour management system. It also allows to set database connection to the database server to store the data to the database server.

FVMS Integration Mode tab – Allows the configuration to integrate with the Visitor Management System (VMS) software to connect to the VMS database.

CCTV Alarm Integration tab – Allows the configuration to integrate with the CCTV server and alarm integration.

Attendance Log tab – Allows to export the time attendance log to a specified file location in text document format.

5.7.4 Import Tool

There are two data are available to import into the system which are card data and department data. Before import the data, you need to generate an excel file with all the card data / department data included in the excel file. You can download the template from the system and then follow the template format to fill in the all the card / department data.

Manual – VAULT Enterprise Professional

The screenshot shows the 'Import Tool' window. At the top, there are two steps: '1 Browse Excel File & Load Data' and '2 Import Data'. A red box highlights these steps, with an arrow pointing to the text: '3) Click the buttons following the sequence of the steps to complete the data import process'. Below the steps, there are two tabs: 'Card Data' and 'Department'. A red arrow points to the 'Department' tab with the text: '1) Switch between the data type to import'. To the right, there is a link: 'Download Department Excel Template'. A red arrow points to this link with the text: '2) Click this link to download the template based on the date type you have chosen to import'. Below the tabs, there is a large empty area. To the right, there is a table with the following data:

No	Field	Col No
01	Department ID	-
02	Department Code	-
03	Department Desc...	-
*		

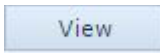
5.8 Report

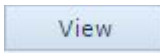


Step 1 – Go to **Report** Tab.

Step 2 – Select the category report to view in the category option and select the type of data to generate.

Step 3 – Filter the data using the filter tools to view specific data.



Step 4 – Click the  button to view the report data.

Step 5 – Export the report (Pdf, Xls, Xlsx, Rtf, Mht, Html, Text, Csv, Image)

5.8.1 Time Zone Report

Report Data Type	Explanation
Time Zone Report	- View the time zone of the system
Time Set Report	- View the time set of the system

5.8.2 Audit Trial Report

Report Data Type	Explanation
Audit Trial Report	- Track on the action done by the user on the software (add, delete, update)
Alarm Acknowledgement Report	- View the acknowledged alarm record on a specified time
Alarm Manual Entry Report	- View the acknowledged alarm record with manual entry that is key in manually in the live transaction.

5.8.3 Access Category

Report Data Type	Explanation
User Card Report	- View the card user in current system
Temporary Card Report	- View the temporary card in current system
Access Level Report	- View the group access level in current system
Card Access Audit Report	- View only card access data

Manual – VAULT Enterprise Professional

User Card Report (Custom Field)	- View only card user data for custom field
---------------------------------	---

5.8.4 Manual Entry Report

Report Data Type	Explanation
Manual Entry Report	- View a detailed manual entry record on a specified time.
Manual Entry Summary Report	- View a summary manual entry record on a specified time (without card number, date time of the record, transaction and site)

5.8.5 Transaction History

Report Data Type	Explanation
Transaction History	- View the transaction record
Roll Call Report	<ul style="list-style-type: none"> - Track on the card user who is not leaving the building - This Report usually used in emergency circumstances to track on the card user last location and card user who is not leaving the building yet

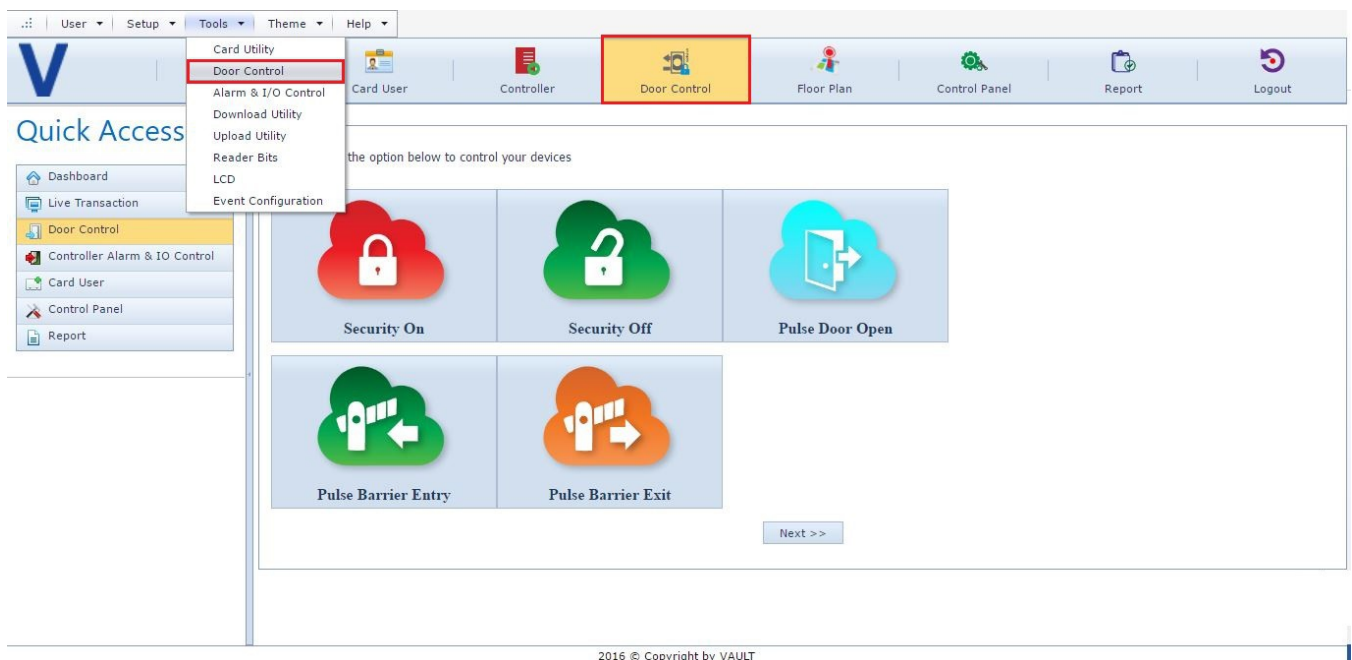
5.8.6 Time Attendance

Report Data Type	Explanation
Time Attendance Report	- View the attendance for the card holder

CHAPTER 6 – DOOR CONTROL

6.1 Overview

Door control is a feature that is used to control the controller through the web application. The door control can be access through the 'Door Control' tab or go to 'Tools' > 'Door Control'



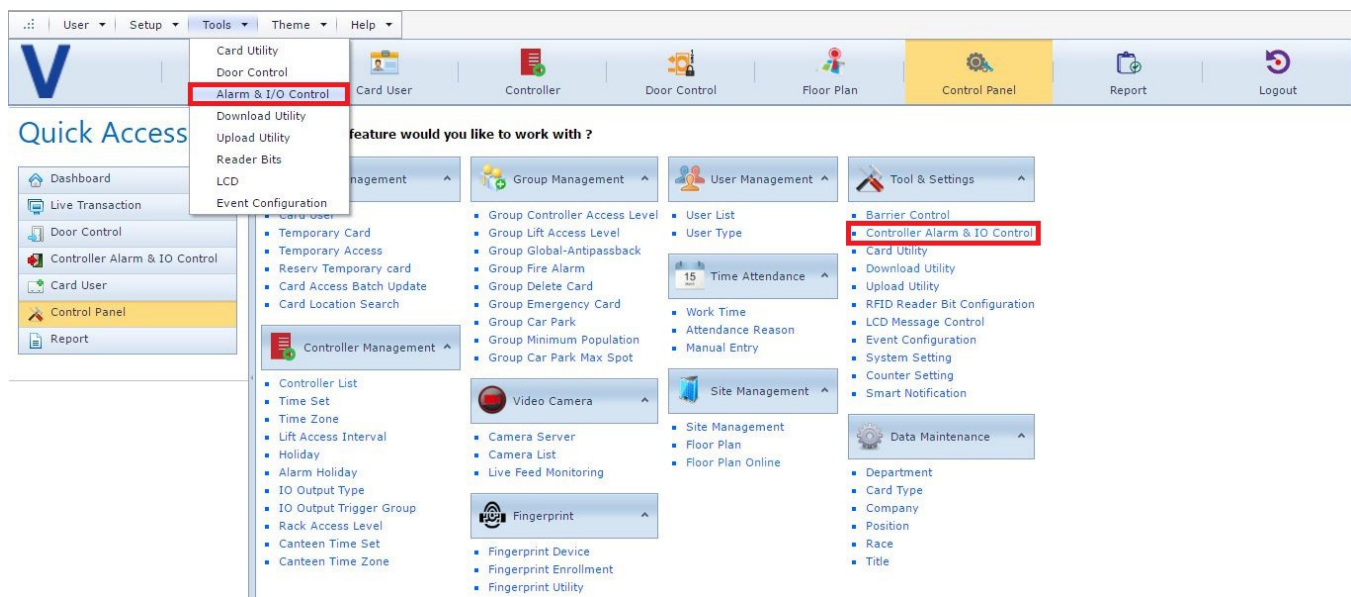
6.2 Door Control Option

Features	Explanation
Security On	- Turn on the controller security
Security Off	- Turn off the controller security
Pulse Door Open	- Open controller door
Pulse Barrier Entry	- Open entry barrier
Pulse Barrier Exit	- Open exit barrier

CHAPTER 7 – ALARM & IO CONTROL

7.1 Overview

Alarm & IO control is a feature that is used to control the controller I/O and alarm through the web application. The door control can be access through the ‘Control Panel’ > ‘Tool & Settings’ > ‘Controller Alarm & IO Control’ or go to ‘Tools’ > ‘Alarm & IO Control’.



7.2 Alarm & IO Control Option

Features	Explanation
Arm Alarm	- Arm alarm
Disarm Alarm	- Disarm Alarm
Active Alarm Output	- Activate the alarm output
Deactive Alarm Output	- Deactivate alarm output
Active I/O Output	- Activate IO output
Deactive IO Output	- Deactivate IO output

Manual – VAULT Enterprise Professional


Active Rack Output	- Activate Rack IO output
Deactive Rack Output	- Deactivate Rack IO output

CHAPTER 8 – VIDEO CAMERA

8.1 Add Camera Server

Step 1 – Make sure the Camera Server is connected on the local area network (LAN). To check the connection type 'ping [Camera Server IP]' in command prompt.

Step 2 – Go to 'Control Panel' > 'System Setting' under tool & settings category, to make sure the 'Video Server Type' is correct under the 'CCTV & Video Integration Mode' section.

Step 3 – Go to 'Control Panel' > 'Camera Server' under 'Video Camera' category to add the camera server. Click  button to add camera server.

Step 4 – Fill in the camera sever connection detail and click  to save the settings.

8.2 Add Camera

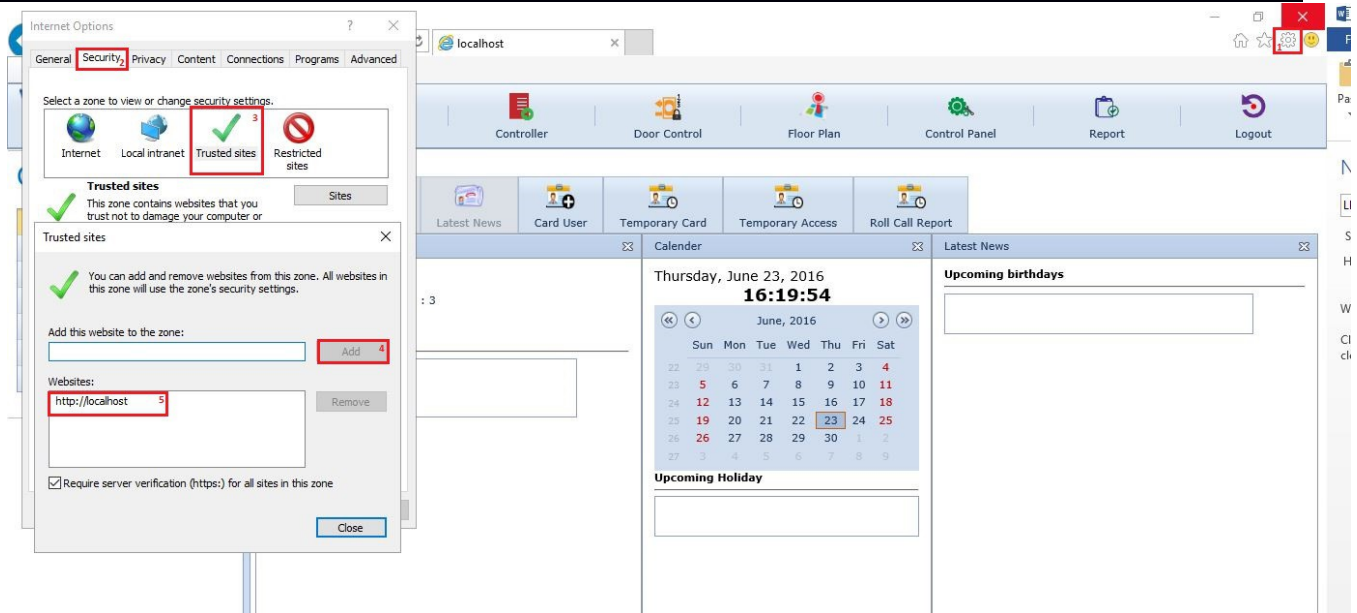
Step 1 – Make sure the IP Camera is connected on the local area network (LAN). To check the connection type 'ping [Camera IP]' in command prompt.

Step 2 – Make sure the web application is opened using Internet Explorer (IE).

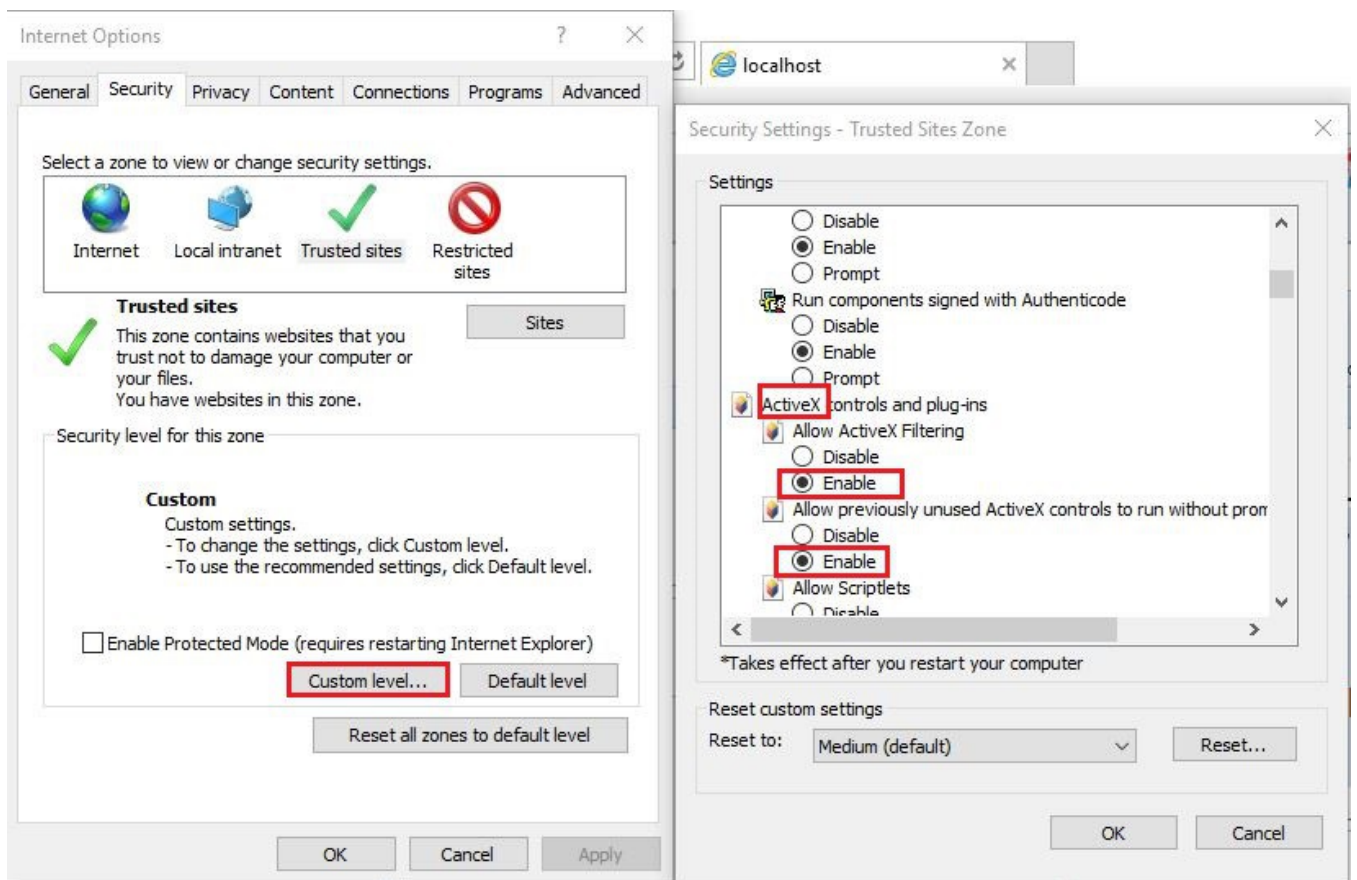
Step 3 – Go to 'setting' > 'Internet Option' > 'Security' tab in IE.

Step 4 – Click on 'Sites' button and click 'Add' to add the site as trusted site.

Manual – VAULT Enterprise Professional



Step 5 – Click on the 'Custom Level...' button in the internet option and Enable all the ActiveX Control.



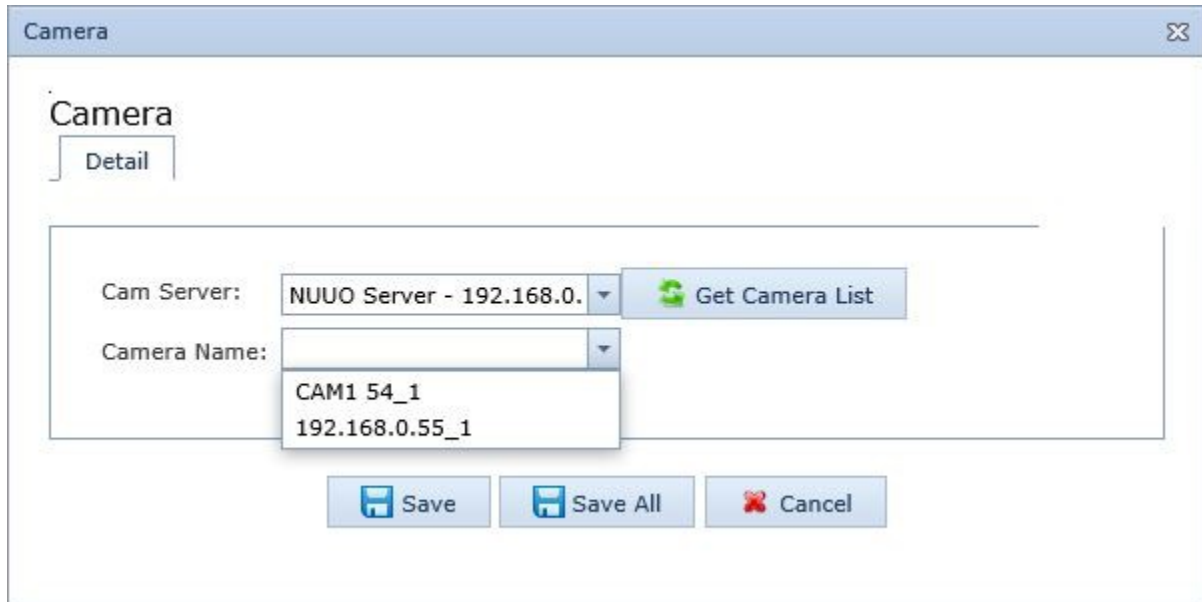
Manual – VAULT Enterprise Professional

Step 6 – Go to 'Control Panel' > 'Camera List' under 'Video Camera' category to add camera. Click



button to add camera.

Step 7 – Select the cam sever and select the camera name to add.



Step 8 – Click on to add the camera in to the VAULT Pro

Step 9 – Go to 'Controller' tab > 'Camera Setting' add the camera to the controller from the option

Step 10 – View the live view in 'Control Panel' > 'Live Feed Monitoring' under 'Video Camera' category or view in transaction additional features, refer 3.6.2 for transaction additional feature

2016/06/23 17:44:28
Door 1

Transaction : **Battery Low**
Name :
Card No : FFFFFFFF
Site : CENTRAL

Date & Time	Controller	Card No	Name	Transaction
2016/06/23 17:44:28	Door 1	FFFFFFFF		Battery Low
2016/06/23 17:40:59	Door 1	0000061084		Valid Exit Access
2016/06/23 17:13:31	Door 1	FFFFFFFF		Battery Low
2016/06/23 16:42:33	Door 1	FFFFFFFF		Battery Low
2016/06/23 16:11:37	Door 1	FFFFFFFF		Battery Low
2016/06/23	Door 1	FFFFFFFF		Battery Low

192.168.0.35
camera 1
23-06-2016 17:53:57

PAGE 54

ER 9 – FINGERPRINT

9.1 Add Fingerprint Device

Step 1 – Make sure all the fingerprint devices are connected to local area network (LAN).

Step 2 – Go to 'Control Panel' > 'Fingerprint Device' under 'Fingerprint' category.

Step 3 – Click the  button to add the fingerprint device.

Step 4 – Fill in the detail for the fingerprint device connection

Step 5 – Click the  to save the settings

9.2 Fingerprint Enrollment

Step 1 – Open Internet Explorer (IE) for the fingerprint enrollment.

Manual – VAULT Enterprise Professional

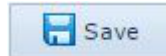
Step 2 – Set as trusted site and enable all the ActiveX Control. Please refer to 5.2 for the steps to set as trusted site and enable ActiveX Control in IE.

Step 3 – Go to 'Control Panel' > 'Fingerprint Enrollment' under 'Fingerprint' category.

Step 4 – Select the site code and click 'Browse' button to browse the card user to enroll fingerprint.

Step 5 – Click 'Enroll 1st Fingerprint' button to enroll first fingerprint

Step 6 – Place finger on the fingerprint device and click



button after the fingerprint scan completed.

CHAPTER 10 – CONTROL PANEL

10.1 Card Management

There are several features in this section that allow you to manage the card user easily. The functionality of these features are describe in table below.

Features	Explanation
Card User	<ul style="list-style-type: none"> - Manage and configure the card user access - For more detail please refer chapter 3.5
Temporary Card	<ul style="list-style-type: none"> - Assign and manage all the staff temporary card for temporary access.
Temporary Access	<ul style="list-style-type: none"> - Assign and manage all the staff short term access or temporary access.
Reserve Temporary Card	<ul style="list-style-type: none"> - Card reserved list for temporary card registration only.
Card Access Batch Update	<ul style="list-style-type: none"> - Quick update access right for group of the card.
Card Location Search	<ul style="list-style-type: none"> - Search and locate the person remain in building when emergency cases. - This feature is same with the roll call report.

10.2 Controller Management

Controller Management provide a full control on the controller to manage the control such as adding controller, time set and time zone. The detail feature is explain in the table below.

Features	Explanation
Controller List	<ul style="list-style-type: none"> - Manage and configure the controller device.

Manual – VAULT Enterprise Professional

	<ul style="list-style-type: none"> - Please refer chapter 3.1 and 3.2 for more detail
Time Set	<ul style="list-style-type: none"> - View and manage all the door controller time interval for entrance purpose - <i>Please refer chapter 3.4.1 for more detail</i>
Time Zone	<ul style="list-style-type: none"> - Configure and manage time zone for controllers - <i>Please refer chapter 3.4.1 for more detail</i>
Lift Access Interval	<ul style="list-style-type: none"> - Configure and manage all the lift zone or floor to access.
Holiday	<ul style="list-style-type: none"> - Manage and configure the holiday days access
Alarm Holiday	<ul style="list-style-type: none"> - Manage and configure the alarm holiday time interval to arm / disarm the alarm during holiday
IO Output Type	<ul style="list-style-type: none"> - Setup the Output Type for IO Controller
IO Output Trigger Group	<ul style="list-style-type: none"> - Setup the Output Trigger Group for IO Controller
Rack Access level	<ul style="list-style-type: none"> - Setup the Rack Access Zone
Canteen Time Set	<ul style="list-style-type: none"> - View and manage all the canteen door controller time interval for entrance purpose
Canteen Time Zone	<ul style="list-style-type: none"> - Configure and manage canteen time zone for door access purpose

10.3 Group Management

Group Management allows configuration and management on the grouping for multiple items into a group. The detail explanation for each of the feature as table below.

Features	Explanation
Group Controller Access level	<ul style="list-style-type: none"> - Predefine and group the door access right
Group Lift Access level	<ul style="list-style-type: none"> - Predefine and group the lift access right
Group Global-Antipassback	<ul style="list-style-type: none"> - Configure and set the global-antipassback group

Manual – VAULT Enterprise Professional

Group Fire Alarm	- Configure and set the fire alarm group
Group Delete Card	- Set the controller for auto delete visitor. This setting only applicable for visitor card on exit event.
Group Emergency Card	- Group multiple relevant controller into a group, when the emergency card is swipe on the reader from one of the controller in this group, all the controller in this group will be security off.
Group Car Park	- Group relevant car park controller into a group
Group Minimum Population	- Group the relevant controller with the minimum population feature enable for the person counter feature
Group Car Park Max Spot	- Group the relevant controller with the Car Park Max Spot feature enable for the Car Park Max Spot counter feature

10.4 Video Camera

Video Camera provide the integration for the camera server with VAULT Enterprise Pro.

Please refer to chapter 5 for a more detail explanation and the step to configure the video camera settings.

Each of the feature are explain in the table below.

Features	Explanation
Camera Server	- Configure and manage the video server for video integration purpose.
Camera List	- Configure and manage all the camera integrated.
Live Feed Monitoring	- View the live feed transaction with video online.

10.5 Fingerprint

Fingerprint provide fingerprint biometric authentication where user can manage and configure fingerprint device with the ability to save the card user fingerprint and download to the finger print system. The following table explain each of the feature's functionality.

Features	Explanation
Fingerprint Device	- Manage and configure the fingerprint integrated device.
Fingerprint Enrollment	- Enroll fingerprint using the USB desktop reader.
Fingerprint Utility	- Use Fingerprint utility to upload and download the fingerprint templates.

10.6 User Management

User Management provide the ability to manage the VAULT Enterprise user by giving the right from the administrator based on the user type given by the administrator. The following table is the explanation of each feature in this section.

Features	Explanation
User List	- Manage the user type to access system.
User Type	- Manage the user type to access system.

10.7 Time Attendance

Time Attendance provide the ability to manage and configure manually the working time, attendance reason and manual entry for the transaction to generate the time attendance report. A brief explain for the time attendance feature is explain in the table below.

Please refer to chapter 8 for more details on time attendance setting.

Features	Explanation
Work Time	- Manage and configure all the working time available for card user.
Attendance Reason	- Add, Edit , View and Delete the reason for time attendance
Manual Entry	- Manually record or register the card user transaction.

10.8 Site Management

Site Management provide the ability to manage multiple site under a single system. Beside, this section also provide a floorplan function to visualize the environment of a particular site with each of the controller place on top of the floorplan. A brief explanation for the Site Management section is explain in table below.

Features	Explanation
Site Management	- Manage and control the site information. This feature will allow you easily control or group the controller at certain area, organization or building.
Floor Plan	- Manage and setup the floor plan for your site, area, floor or company.
Floor Plan Online	- View your site, office or company floor plan for monitoring purpose.

10.9 Tool & Settings

Tool & Settings provide the ability to make communication between the system and controller. It able to download data to the controller and upload back to the system from the controller to check the setting. Besides that, this section is also provide system configuration features which allow the

Manual – VAULT Enterprise Professional

user to set the system setting based on user preference. A brief explanation for each of the setting for the tool & settings section is as table below.

Features	Explanation
Barrier Control	<ul style="list-style-type: none"> - Quick access to control the door operation currently active in the network. - <i>Please refer to chapter 4 for more detail explanation for each of the function</i>
Controller Alarm & IO Control	<ul style="list-style-type: none"> - Quick access to control the alarm & I/O operation currently active in the network.
Card Utility	<ul style="list-style-type: none"> - Card utility to download, install and delete card.
Download Utility	<ul style="list-style-type: none"> - Download settings to controller
Upload Utility	<ul style="list-style-type: none"> - Download settings from controller
RFID Reader Bit Configuration	<ul style="list-style-type: none"> - Configure and set the RFID reader reading mode.
LCD Message Control	<ul style="list-style-type: none"> - Setup LCD type controller LCD screen message.
Event Configuration	<ul style="list-style-type: none"> - Configure Event color, Email Notification, Alarm popup.
System Setting	<ul style="list-style-type: none"> - Set the system default setting. Customize field / SMTP Server / Video Server Type / Facility Code and etc.
Counter Setting	<ul style="list-style-type: none"> - Set the car park group counter / person group counter.
Smart Notification	<ul style="list-style-type: none"> - Door access event/alarm notification.

10.10 Data Maintenance

Data maintenance allows user to manage the additional data such as department, Company, Race and etc. A brief explanation is as in the table below.

Features	Explanation
----------	-------------

Manual – VAULT Enterprise Professional

Department	- Quick access to manage department.
Card Type	- Quick access to manage user type.
Company	- Quick access to manage company.
Position	- Quick access to manage position.
Race	- Quick access to manage race.
Title	- Quick access to manage title.

CHAPTER 11 – TIME ATTENDANCE SETTING

11.1 Working Time Configuration

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

Attendance Control

System Normal ▼

To start using attendance control, a working time have be configured first.

Go to 'Control Panel' > 'Work Time' under 'Time Attendance' to add a custom work time.

By default, the system come with a default setting (Normal Work Time) which preset the system with standard working time. E.g. Office Hours, Monday to Friday, 08.30am – 17:30pm.

11.1.1 General Setting

General Working Hour Lunch & Breaktime

Work Time Name:*

Description:

Site Code: CENTRAL ▼

Grace Period

Time In: 15 Time Out: 15

Minimum Lapse Hour: 4

Over Time Setting

Auto None

Minimum Overtime: 15

Save Cancel

At the work time general setting tab, you can define the normal setting like Work Time Name and Description for the work time.

Manual – VAULT Enterprise Professional

In the Grace Period section, this 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 when 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.

11.1.2 Working Hour

	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 type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Next Day	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Time Out	01 ▾	01 ▾	01 ▾	01 ▾	01 ▾	01 ▾	01 ▾

The following table is a brief description of each of the settings for working hour.

Features	Explanation
Time IN	- Time start to work
Time OUT	- Time end to work
Work Day	- Check for working days or uncheck for non-working days
Next Day	- Use this option for those working time start at late / night shift / overnight where the attendance the part involve for the second day calculation. E.g. 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 generate the OT report.
--	----------------------------------

11.1.3 Lunch & Break Time

This feature enable you to set the lunch and break time on weekly basis. You can configure the Time Out & Time In for the lunch/break time.

The time out is the time when the employee go out for lunch while time in is the time when the employee should be back to work.

11.2 Manual Entry

Go to 'Control Panel' > 'Manual Entry' under 'Time Attendance'.

Here is where the operator / system admin can register or add in transaction manually using the system. For example, a staff taken annual leave today and the administrator don't want the card user to be appear as absent for the day, so the admin can manually enter the transaction and put the remark as annual leave. So, the system will pretend the card user who is on leave is coming to work.

Under Manual Entry Form, select 'New' to add in the new record. Record added (Valid Entry / Valid Exit) will be take place in calculation for the attendance report.

Manual – VAULT Enterprise Professional

Manual Entry Form

Detail

Site Code:

Date:

Time: Time To:

Card No: 0000046043

Staff Name : Test

NRIC:

Department: Department

Transaction:

Reason:

Remark:

11.3 Attendance Reason

Go to 'Control panel' > 'Attendance Reason' under 'Time Attendance' category

The screenshot shows the VAULT Enterprise Professional web interface. At the top, there is a navigation bar with icons for Live Transaction, Card User, Controller, Door Control, Floor Plan, Control Panel (highlighted with a red box), Report, and Logout. Below the navigation bar is a 'Quick Access' sidebar on the left with a list of menu items: Dashboard, Live Transaction, Door Control, Controller Alarm & IO Control, Card User, Control Panel (highlighted with a yellow box), and Report. The main content area is titled 'Which feature would you like to work with?' and contains several expandable categories: Card Management, Group Management, User Management, Tool & Settings, Controller Management, Video Camera, Fingerprint, Time Attendance, and Site Management. The 'Time Attendance' category is expanded, showing sub-items: Work Time, Attendance Reason (highlighted with a red box), and Manual Entry. The 'Tool & Settings' category is also expanded, showing a list of settings including Barrier Control, Controller Alarm & IO Control, Card Utility, Download Utility, Upload Utility, RFID Reader Bit Configuration, LCD Message Control, Event Configuration, System Setting, Counter Setting, and Smart Notification. The 'Data Maintenance' category is also expanded, showing a list of data types: Department, Card Type, Company, Position, Race, and Title.

Manual – VAULT Enterprise Professional

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

E.g. forget to bring card, Oversea Training and etc.

Late Reason List		
New Edit Delete Pdf Xls		
Drag a column header here to group by that column		
No	Code	Description
<input type="checkbox"/>		
<input type="checkbox"/>	1	Normal
		Normal Transaction
<input type="checkbox"/>	2	MC
		Medical CheckUp
<input type="checkbox"/>	3	AL
		Annual Leave
<input type="checkbox"/>	4	NPL
		No Pay Leave
<input type="checkbox"/>	5	NPH
		No Pay Hour

11.4 Attendance Report

Please refer to chapter 3.7 for the step to view and print report.

Each of the report type is explain in the table below

Daily Report

Report Name	Explanation
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. E.g. 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.

Monthly Report

Report Name	Explanation
Attendance Check List	<ul style="list-style-type: none"> - Monthly attendance check list for each of the staff selected
Attendance Summary	<ul style="list-style-type: none"> - Monthly attendance check list with data summary - E.g. Calculate total day attended or absent with working time and over time in the data summary
Staff In Out Report	<ul style="list-style-type: none"> - Monthly attendance for In and out record for the month only - E.g. Calculate total day attended or absent only in the data summary

CHAPTER 12 – RACK CONTROLLER CONFIGURATION

12.1 Controller configuration

Step 1 – Add controller to VAULT Pro. *Please refer chapter 3.1 for the steps to add a controller.*


Step 2 – In the ‘Controller Details’ tab, check I/O and Rack as the controller type as shown in figure below.

The screenshot shows a configuration panel titled "Controller Type". It contains five checkboxes arranged in two rows. The first row has "Alarm:" (unchecked), "I/O:" (checked), and "Lift:" (unchecked). The second row has "LCD:" (unchecked), "Rack:" (checked), and an empty space. The "Rack:" checkbox is highlighted with a yellow border.

Step 3 – In the ‘Setting’ tab, select the rack control for the current control and group the controller into a group with Rack ID/ Group is necessary.

The screenshot shows two input fields. The first is labeled "Rack ID / Group :" and contains the value "1". The second is labeled "Rack Control:" and contains the value "1-16". Both fields have small up/down arrows on their right sides.



Step 4 – Click the  to save the controller setting

Step 5 – Go to ‘Controller Panel’ > ‘I/O Output Type’ under ‘Controller Management’ category, add a new IO Output type and set on timer for the rack to release.

Manual – VAULT Enterprise Professional

I/O Output Type

Setting


Output Type ID:*

Description:

Output Type:

On Timer			Off Timer		
Hour	Minute		Hour	Minute	
<input type="text" value="00"/>	<input type="text" value="00"/>	<input type="text" value="05"/>	<input type="text" value="00"/>	<input type="text" value="00"/>	<input type="text" value="00"/>



Step 6 – Click  to save the new I/O Output Type and download to the controller

Step 7 – Go to 'Control Panel' > 'Rack Access Level' under 'Controller Management', add new Rack Access Level and set the access level for the rack controller.

Manual – VAULT Enterprise Professional

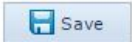
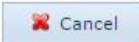
Rack Access Setting

Timer Setting


Rack Access No:*

Description:

Interval 1	Interval 2	Interval 3
From <input type="text" value="01"/>	From <input type="text" value="03"/>	From <input type="text" value="06"/>
To <input type="text" value="02"/>	To <input type="text" value="04"/>	To <input type="text" value="10"/>
Interval 4	Interval 5	Interval 6
From <input type="text" value="00"/>	From <input type="text" value="00"/>	From <input type="text" value="00"/>
To <input type="text" value="00"/>	To <input type="text" value="00"/>	To <input type="text" value="00"/>



Step 8 – Click the  button to save the newly added Rack Access Level and download to controller

Step 9 – Select the Rack Controller added earlier in the ‘Controller’ and click the ‘Edit’ button

Step 10 – Go to ‘IO Config’ to create new I/O Input point and I/O output point. Note that the I/O point must have the same quantity and select the input type as ‘Door Sensor’ for the input point, else the rack will not work.

Manual – VAULT Enterprise Professional

Input Point

Details

Name: IN1

Point No: 1

Input Type: Door Sensor

Output Trigger Group: (empty)

Time Zone: 00

Ok Close

Step 11 – Go to ‘Card User’, select the user to give rack control access, under the ‘Card Info’ tab select the Rack Access Level for the selected user under ‘Card Properties’ section

Card Profile

Card Info Employee Details Access Level Custom Fields

Upload Scan

Card No:* 0000046043

Name:* ALI

Site Code:* Selangor

Card Properties

Card Type: Normal Card

Card Pin No:* 0

Bypass Antipassback: Enable

Guard Tour Card: Enable

Dual Card Group: Master Card

Card Expiry Status: Non Expired

Expired Date (dd-MM-yyyy): 27-07-2016

Car Park Max Spot Group: None

Biometric Authentication: FP

Alarm Card: Enable

Card Status: Enable

Rack Access Level: 01 - Free Access Rack Zo

Emergency Card Type: Enable

Expiry Time (HMS): 12:00 PM

Canteen TZ: 00

Attendance Control

System Normal

Manual – VAULT Enterprise Professional



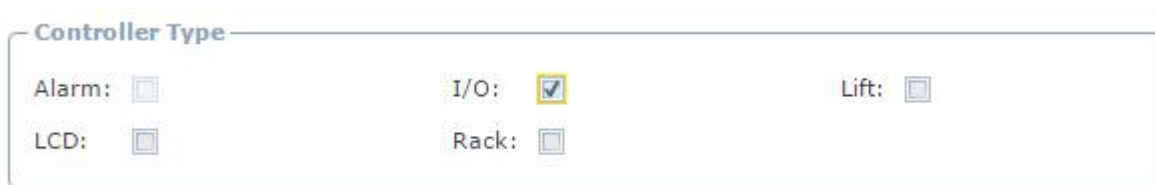
Step 12 – Click to save the setting and download to the controller

CHAPTER 13 – I/O ALARM CONFIGURATION

13.1 Controller Configuration

Step 1 – Add controller to VAULT Pro. *Please refer chapter 3.1 for the steps to add a controller.*

Step 2 - In the 'Controller Details' tab, check I/O as the controller type as shown in figure below.



The screenshot shows a configuration window titled "Controller Type". It contains five checkboxes arranged in two rows. The first row has "Alarm:", "I/O:", and "Lift:". The second row has "LCD:" and "Rack:". The "I/O:" checkbox is checked, while all other checkboxes are unchecked.

Step 3 – Repeat the step 5 and step 6 in chapter 9.1.

Step 4 – Go to 'Control Panel' > 'IO Output Trigger Group' under 'Controller Management' category, add the output trigger group desired. The output trigger group is used to trigger a group of output point when the input point is triggered.

Manual – VAULT Enterprise Professional

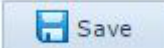
I/O Output Trigger Group

Setting

Group No:*

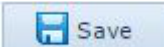
Description:

Output Point No	Enable	Output Point No	Enable
1.	<input checked="" type="checkbox"/>	33.	<input type="checkbox"/>
2.	<input type="checkbox"/>	34.	<input type="checkbox"/>
3.	<input checked="" type="checkbox"/>	35.	<input type="checkbox"/>
4.	<input checked="" type="checkbox"/>	36.	<input type="checkbox"/>
5.	<input type="checkbox"/>	37.	<input type="checkbox"/>
6.	<input checked="" type="checkbox"/>	38.	<input type="checkbox"/>
7.	<input type="checkbox"/>	39.	<input type="checkbox"/>

 Save

Step 5 – Click  button and download to the controller

Step 6 – Repeat Step 10 in chapter 9.1. But the input type set to ‘General Purpose Type’ and select the output trigger group for each of the input point to trigger the output point when the input point is triggered.

Step 7 – Click  button to save the controller setting and download to the controller.

CHAPTER 14 – LIFT CONTROLLER CONFIGURATION

14.1 Controller Configuration


Step 1 – Add new controller and set the controller type to lift by checking the lift check box. *Please refer to chapter 3.1 to understand the step to add a new controller.*

The screenshot shows a window titled "Controller Type" with the following options:

- Alarm:
- I/O:
- Lift:
- LCD:
- Rack:


Step 2 – Go to 'Control Panel' > 'Lift Access Interval' under 'Controller Management' Category, add new lift access interval. This lift access interval is used to manage the floor level which the lift is able to access for specific user.



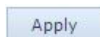
Step 3 – Click  to save the lift access interval download to the controller

Step 4 – Go to 'Control Panel' > 'Group Lift Access Level' under 'Group Management', this feature is same like the Group Card Access Level which is covered in *Chapter 3.4.2*. Assign the controller to the group and set the time zone which is Lift Access Interval to the lift controller.



Step 5 – Click  button to save the group lift access level.

Step 6 – Go to 'Card User' and select a user to give access to the lift. After that go to 'Access Level' > 'Lift' tab under the 'Card User' choose the group access no that the selected user belong and



click  button to apply the default setting set in the 'Group Lift Access Level' in *Step 4*.

Manual – VAULT Enterprise Professional



Step 7 – Click button and download to the controller.

CHAPTER 15 – GLOBAL ANTIPASSBACK CONFIGURATION

15.1 Antipassback Configuration

Step 1 – Go to ‘Controller’ > ‘Setting’, set the time zone to apply the antipassback rule and assign the selected controller to a specific global antipassback group.

Controller Profile

192.168.0.48 :

Controller Details	Setting	Network Configuration	Camera Setting	Alarm Config	IO Config
Controller Configuration					
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="01"/>		Global Antipassback Group: <input type="text" value="1"/>			
Rack ID / Group : <input type="text" value="1"/>		Rack Control: <input type="text" value="1"/>			



Step 2 – Click button to save the setting and download to the controller.

15.2 Global Antipassback Configuration

Step 1 – Go to ‘Control Panel’ > ‘Group Global-Antipassback’ under ‘Group Management’ category

Step 2 – Assign the controller into a group to apply the antipassback rules.

Manual – VAULT Enterprise Professional

Group Antipassback

Group

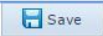

Group No: 01 (Total : 2 Controller)

testing	CENTRAL
DOOR 1	Selangor

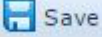
Group Access No:* 01

Site Code: All Site

<input type="checkbox"/>	Controller	Description	Site Code
<input checked="" type="checkbox"/>	DOOR 1	DOOR 1	Selangor
<input checked="" type="checkbox"/>	testing	testing without battery	CENTRAL

 Save  Cancel



Step 3 – Click  button to save the setting and download to the controllers

CHAPTER 16 – FIRE ALARM CONFIGURATION

16.1 Fire Alarm Configuration

Step 1 – Go to ‘Controller’ > ‘Setting’ and uncheck the fire alarm mode for the selected controller

Controller Profile

192.168.0.48 :

Controller Details	Setting	Network Configuration	Camera Setting	Alarm Config	ID Config
Controller Configuration					
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="01"/>		Global Antipassback Group: <input type="text" value="1"/>			
Rack ID / Group : <input type="text" value="1"/>		Rack Control: <input type="text" value="1"/>			
Mode					
Fire Alarm: <input checked="" type="checkbox"/> Enable		Guard Tour: <input type="checkbox"/> Enable			
Buzzer Door Release: <input type="checkbox"/> Enable		Card Lockout: <input type="checkbox"/> Enable			
Auto Pin: <input type="checkbox"/> Enable		Report Mode: <input type="checkbox"/> Enable			
Emergency Card Mode: <input type="checkbox"/> Enable		Interlocking Mode: <input type="checkbox"/> Enable			
Car Park Max Spot: <input type="checkbox"/> Enable		Car Park Group: <input type="text" value="02 -"/>			
Minimum Population: <input checked="" type="checkbox"/> Enable		Minimum Population Group: <input type="text" value="02 -"/>			
Turnstile Penalty: <input type="checkbox"/> Enable		Canteen Mode: <input type="checkbox"/> Enable			

16.2 Group Fire Alarm Configuration

Manual – VAULT Enterprise Professional

Step 1 – Go to ‘Control Panel’ > ‘Group Fire Alarm’ under ‘Group Management’ category

Step 2 – Assign the controller to a specific group by checking on the checkbox of the controller beside the controller name so if the fire alarm is triggered, all the door in the group will also automatic security off.


Group Fire Alarm

Group

Group No: 01 (Total : 2 Controller(s))		Group Access No: * 01																
<table border="1"> <tr> <td>testing</td> <td>CENTRAL</td> </tr> <tr> <td>testing with battery</td> <td>CENTRAL</td> </tr> </table>	testing	CENTRAL	testing with battery	CENTRAL	Site Code: All Site	<table border="1"> <thead> <tr> <th><input type="checkbox"/> Controller</th> <th>Description</th> <th>Site Code</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> DOOR 1</td> <td>DOOR 1</td> <td>Selangor</td> </tr> <tr> <td><input checked="" type="checkbox"/> testing</td> <td>testing without battery</td> <td>CENTRAL</td> </tr> <tr> <td><input checked="" type="checkbox"/> testing with battery</td> <td>testing with battery</td> <td>CENTRAL</td> </tr> </tbody> </table>	<input type="checkbox"/> Controller	Description	Site Code	<input type="checkbox"/> DOOR 1	DOOR 1	Selangor	<input checked="" type="checkbox"/> testing	testing without battery	CENTRAL	<input checked="" type="checkbox"/> testing with battery	testing with battery	CENTRAL
testing	CENTRAL																	
testing with battery	CENTRAL																	
<input type="checkbox"/> Controller	Description	Site Code																
<input type="checkbox"/> DOOR 1	DOOR 1	Selangor																
<input checked="" type="checkbox"/> testing	testing without battery	CENTRAL																
<input checked="" type="checkbox"/> testing with battery	testing with battery	CENTRAL																

Save Cancel

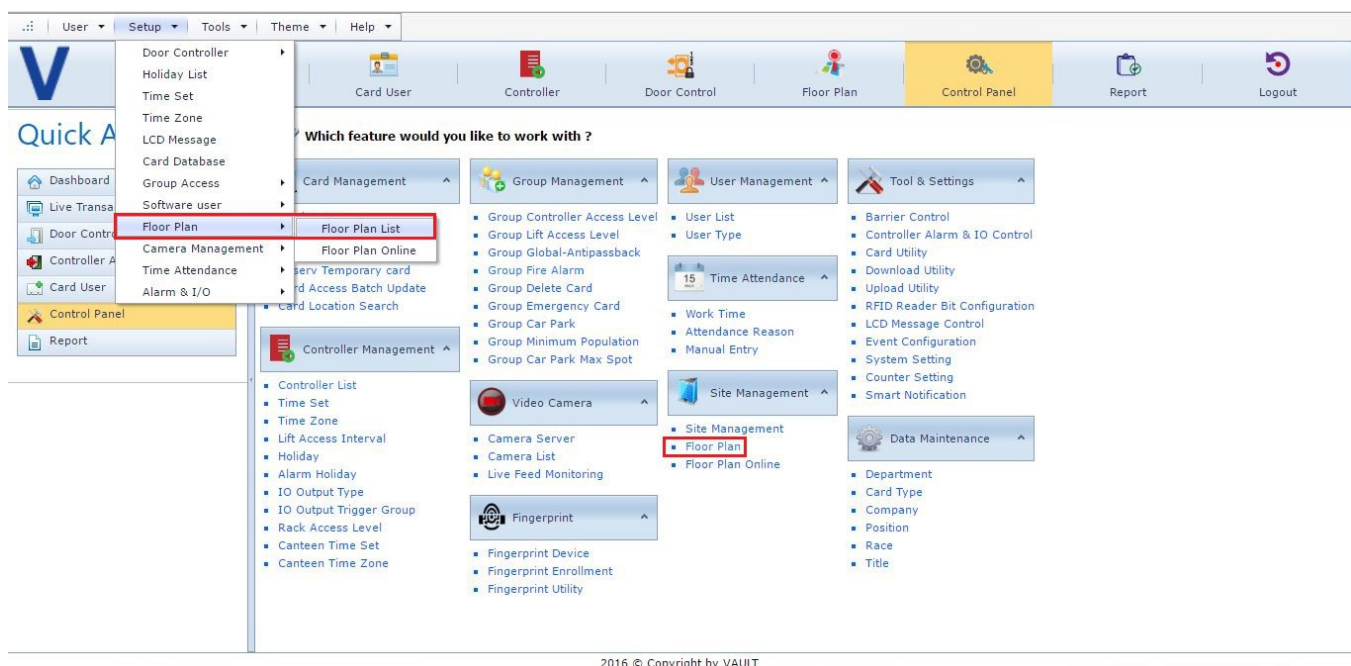



Step 3 – Click  button to save the setting and download to the controller.

CHAPTER 17 – FLOOR PLAN

17.1 Floor Plan List

Step 1 – Go to ‘Control Panel’ > ‘Floor Plan’ under ‘Site Management’ category or go to ‘Setup’ > ‘Floor Plan’ > ‘Floor Plan List’




Step 2 – Click the  button to add a new floor plan

Step 3 – Fill in the floor plan detail and upload a floor plan by clicking the ‘Upload’ button. The maximum dimension for the image is (600 x 1000 pixels).

Manual – VAULT Enterprise Professional

Floor Plan

Detail





Upload


Floor Plan Name:* Floor Plan

Description: Floor Plan

Site Code:* Selangor

Save Save & Edit Now Cancel

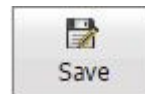
Step 4 – Click  to save the floor plan or click  to add the controller into the floor plan.

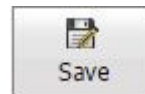
Step 5 – Click on the  button to add the door, alarm or etc. on the floor plan as shown in the diagram

Manual – VAULT Enterprise Professional

Floor Plan Selangor	
Door	<input type="checkbox"/>
Alarm	<input type="checkbox"/>
Camera	<input type="checkbox"/>
IO Input	<input type="checkbox"/>
IO Output	<input type="checkbox"/>

Max : 600 x 1000 pixels

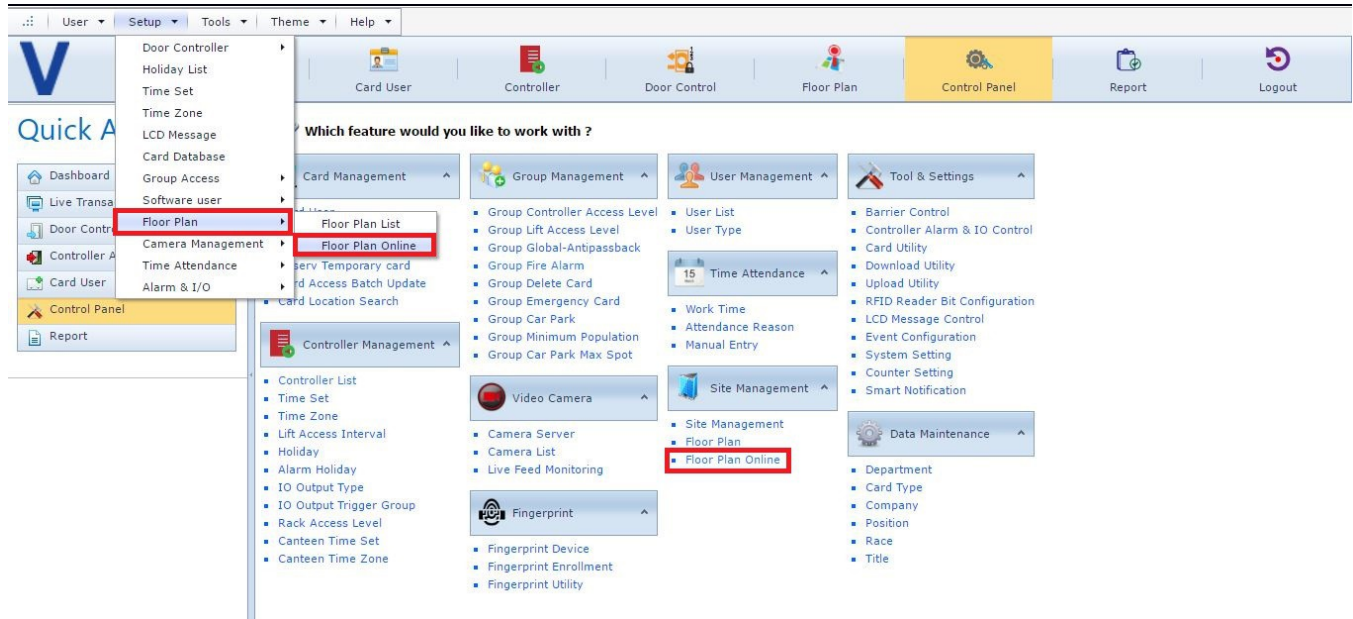


Step 6 – After all the controller is add on the floor plan, click the  button to save the floor plan.

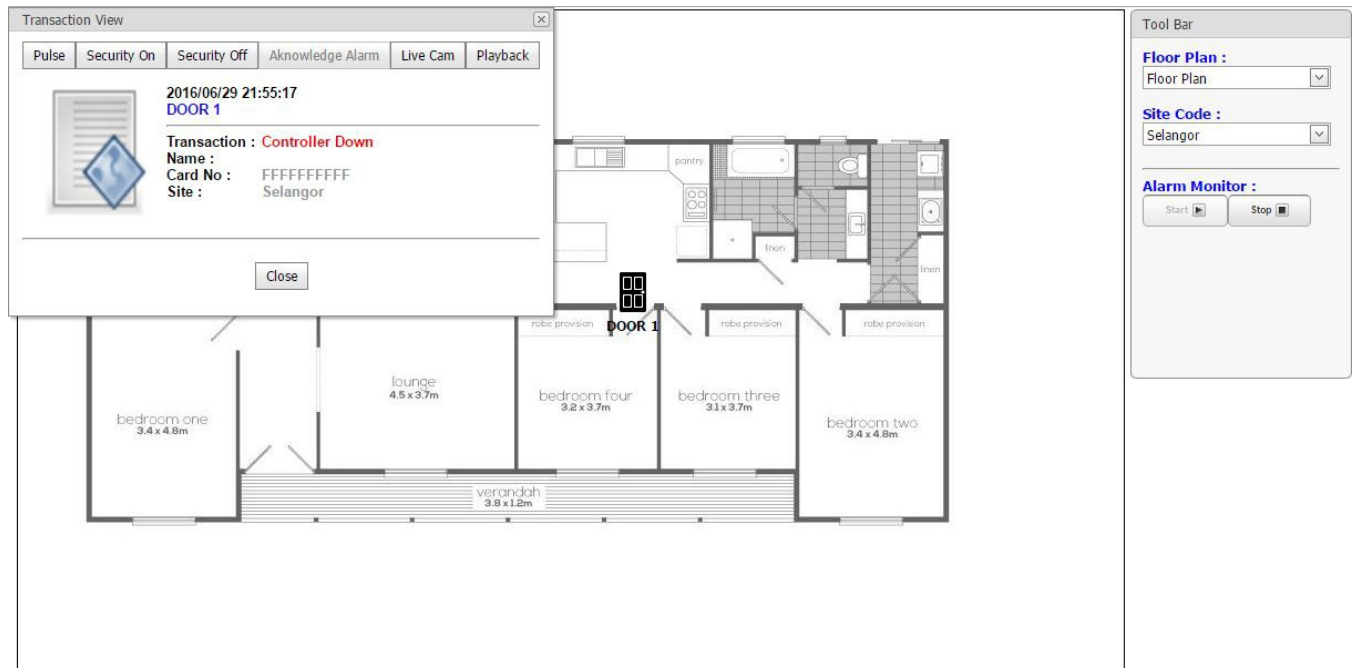
17.2 Floor Plan Online

Step 1 – Go to 'Control Panel' > 'Floor Plan Online' under 'Site Management' or go to 'Setup' > 'Floor Plan' > 'Floor Plan Online'

Manual – VAULT Enterprise Professional



Step 2 – View the floor plan with the controller placed in *chapter 16.1*, click on the controller to view the transaction.



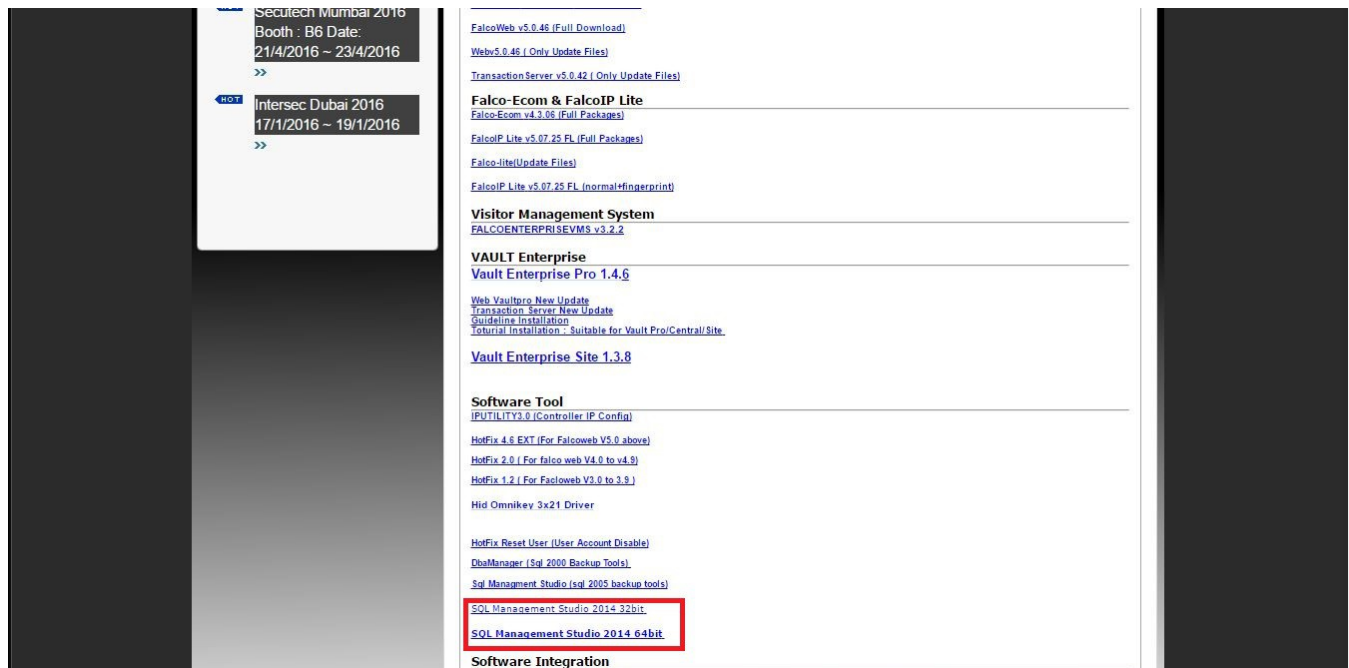
CHAPTER 18 – DATABASE BACKUP AND RESTORE

18.1 Backup and Restore using transaction server

Please refer to chapter 4.7.2 to understand how to backup and restore database using transaction server manually or time schedule.

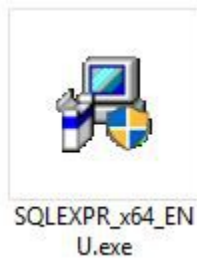
18.2 Backup and Restore using Microsoft SQL Management Studio

Step 1 – Go to ‘www.falco-ecom.com’ website, in the download page under ‘Software Tool’ category to download the Microsoft SQL Management Studio 2014

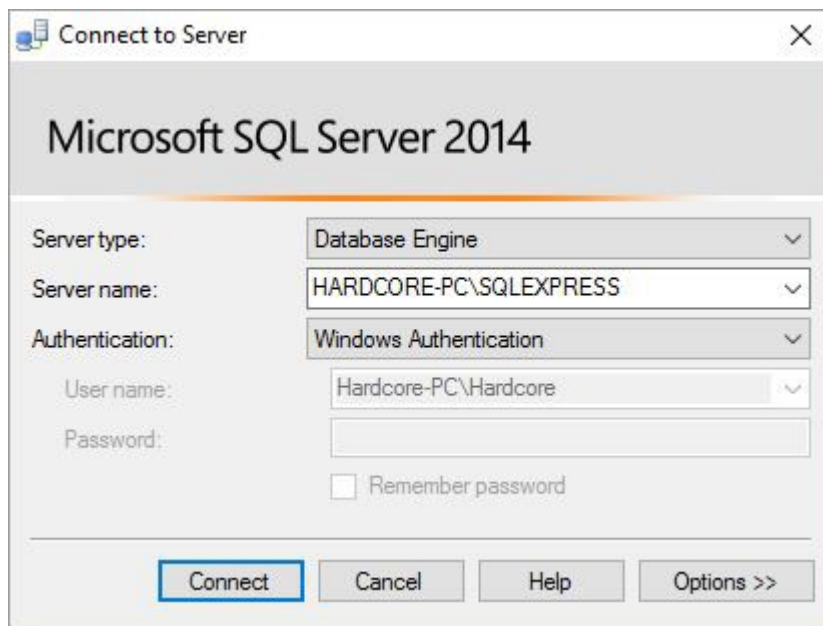


Manual – VAULT Enterprise Professional

Step 2 – Open the file directory where you save the file and then run the windows installer

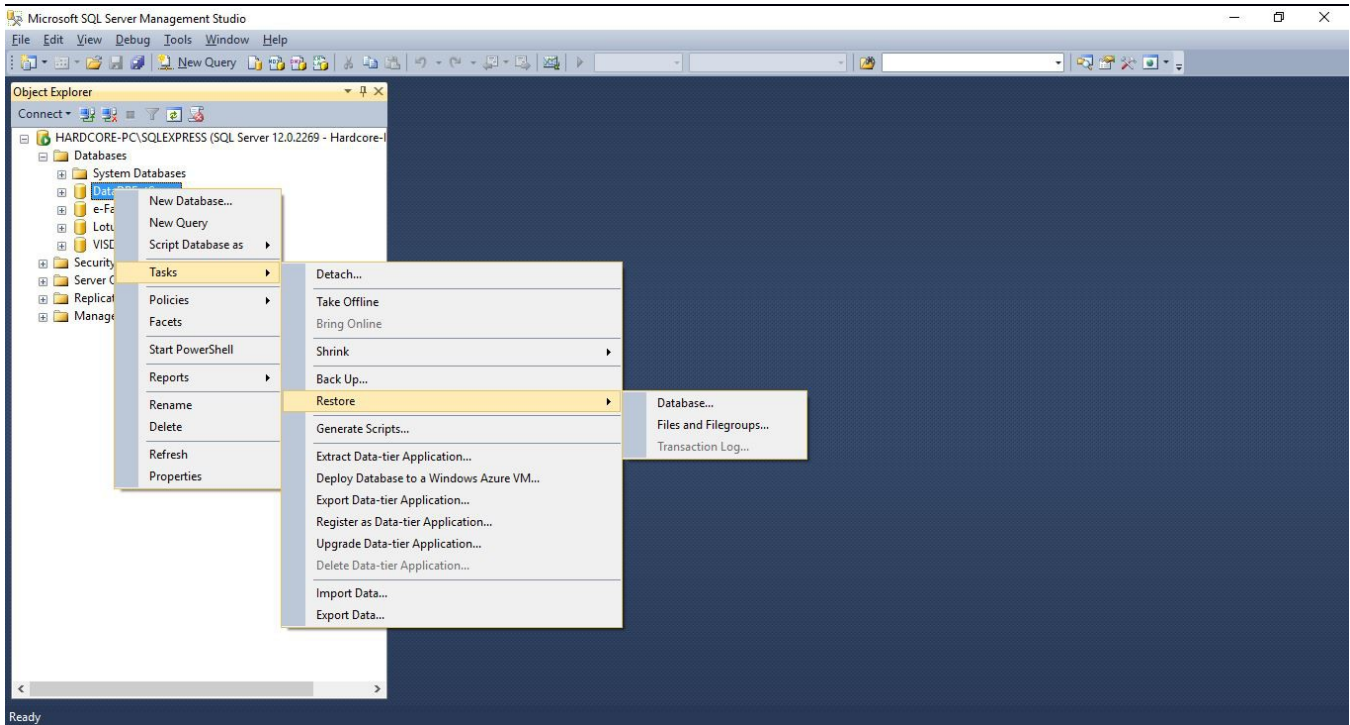


Step 3 – After the installation done, open the program and login to the server.



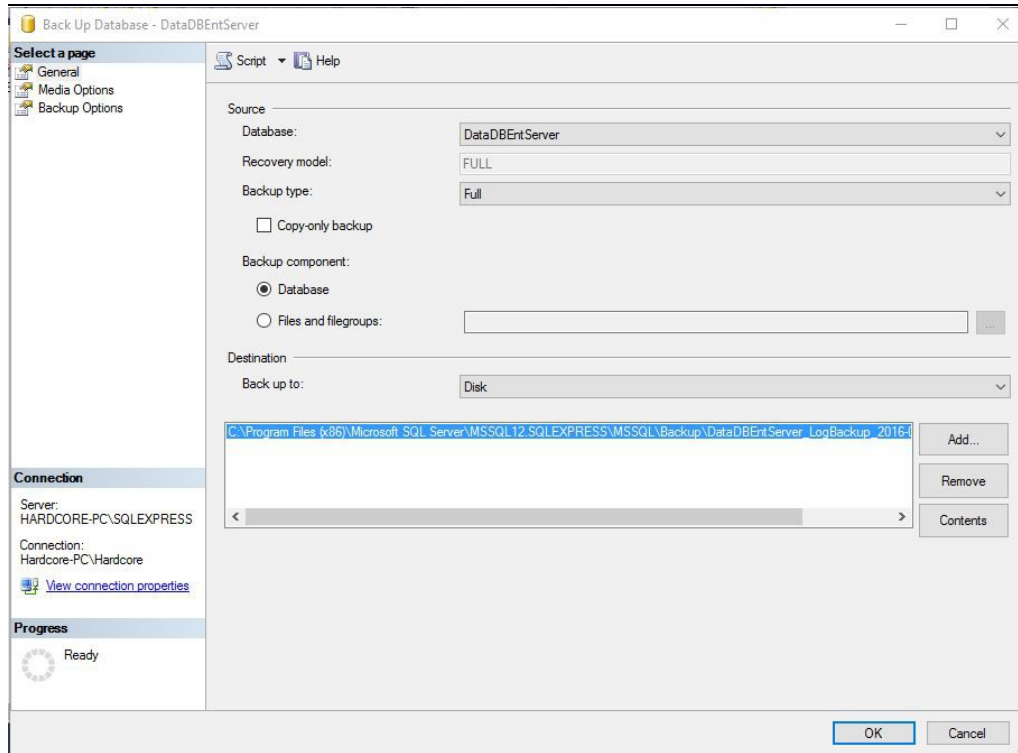
Step 4 – Go to 'Object Explorer', expand the databases folder and then right click on the DataDBEntServer. After that go to 'Tasks' > 'Back up' to backup a database or go to 'Task' > 'Restore' > 'Database' to restore the database.

Manual – VAULT Enterprise Professional

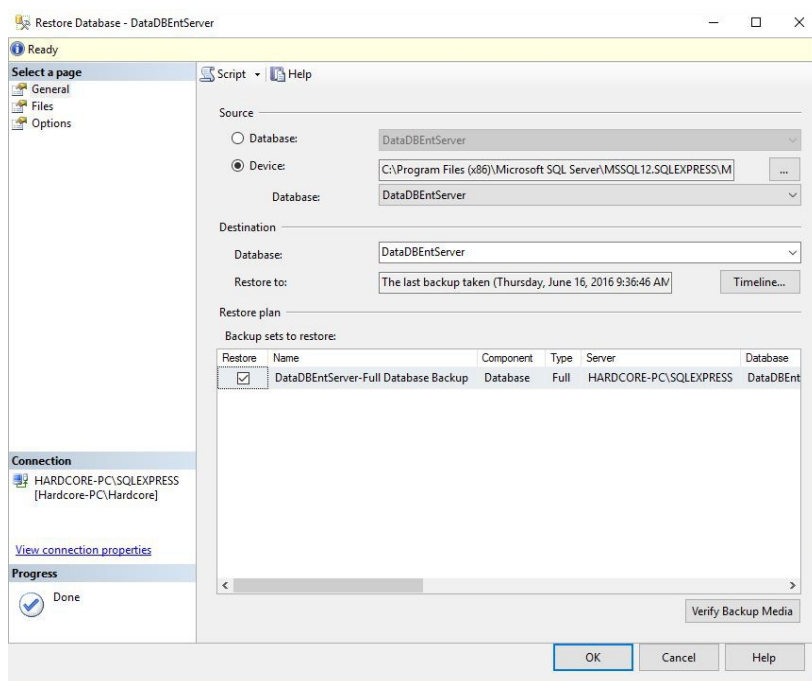


Step 5 – To backup database, go to 'Tasks' > 'Back Up', remove and add the path where the backup file you want to store and then click ok to start back up

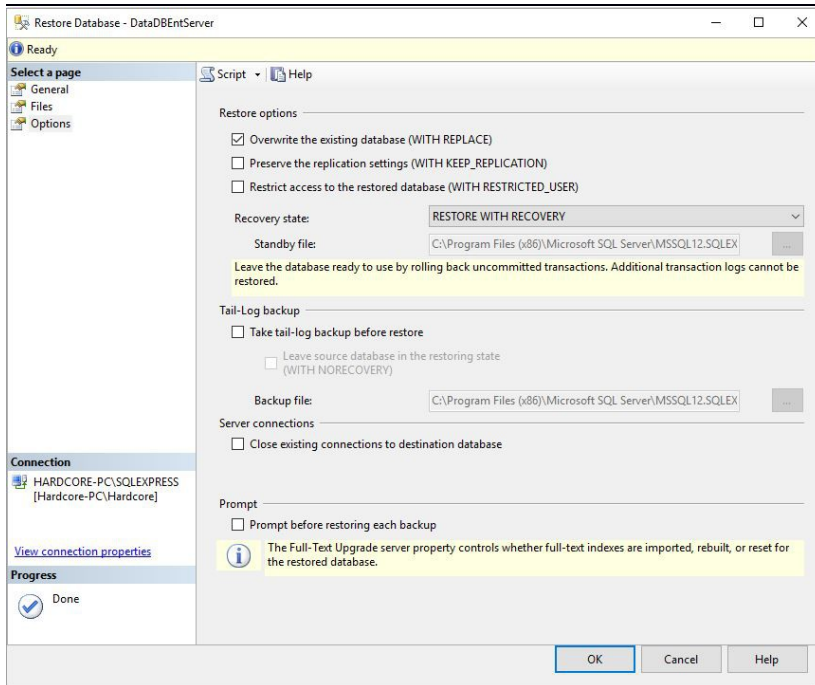
Manual – VAULT Enterprise Professional



Step 6 – To restore the database, go to 'Tasks' > 'Restore' > 'Database', in general page, choose the source of the backup file to restore. After that go to option page, tick the 'Overwrite the existing database' and then untick the 'Take tail-log backup before restore'.



Manual – VAULT Enterprise Professional



Step 7 – Click 'OK' to restore the database