HƯỚNG DẪN SỬ DỤNG WEB PASS E

WebPass IP Reader:

Nguồn điện: 9 ~ 24VDC/1A
Công suất tiêu thụ: 560mA
Bộ nhớ trong quản lý: 20,000 thẻ
Lưu trữ:65,535 giao dịch offline, 1.536 logs devices
Kết nối máy tính: TCP/IP
Kết nối thiết bị ngoại vi: 1.RS-485 + 1.WG
Ngõ Ra: 1
Ngõ Vào: 3
Thời gian mở cửa 1~65.535 secs
Nhiệt độ hoạt động: 0~55 đô C.
Kích thước / trọng lượng: 120x8028mm/150g

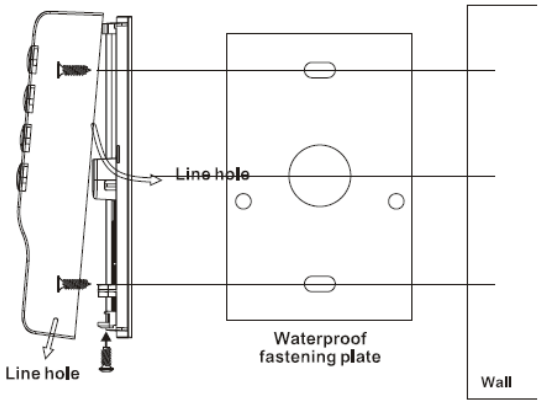
A. HƯỚNG DẪN SỬ DỤNG WEBPASS:

I. Hướng dẫn cơ bản:

I.1. Thông số kỹ thuật:

Software	Somac
Card Capacity	20,000 Cards (Options 50,000 Cards)
Varifiaction Mode	Card / Password
Communications	TCP/IP, RS-485 / Wiegand
DI/O Support	DI: 3 / DO: 1
Inbuilt Relay (Max Power Loading)	Door lock / Ring (0.5A 120Vac / 1A 30Vdc)
Power Over Ethernet	(Option)
Entry Log	65,535 Events
System Log	1,536 Events
Time zone / Time Set / Group	255 / 120 / 255 Sets
Anti Pass Back / Anti Duress	Yes / Yes
Holiday / Ring Setting	Yes / Yes
Dimension / Weight	120x80x28mm / 150g
OutDoor Application	IP65
Power	9 – 24 Vdc, 1A

I.2. Lắp đặt:



Hình 1

- Khoan và bắt vít treo thiết bị trên tường.
- Lắp đặt hoàn chỉnh thiết bị theo đúng sơ đồ đấu nối.

*** Chú ý:**

- Lắp đặt hoàn chỉnh, kiểm tra đấu nối chính xác, kiểm tra nguồn, đo thông mạch, kiểm tra hệ thống hoàn chỉnh trước khi đóng nguồn điện.
- Lắp đặt nơi khô ráo, thoáng mát tránh mưa nắng.
- Lắp đặt tránh các thiết bị bị nhiễm từ: nam châm, tủ điện động lực tòa nhà,…
- Nên khóa tủ bảo vệ khi lắp đặt xong để tránh bụi bẩn và tác động từ bên ngoài.
- Bảo trì thường xuyên để kiểm tra thiết bị và đảm bảo thiết bị hoạt động tốt nhất.

I.3. Cách quét thẻ:

Quét thẻ từ vào vị trí có biểu tượng “Card” ở trên đầu đọc thẻ Chiyu.

II. Sơ đồ kết nối:

II.1. Ký hiệu mầu dây và cáp kết nối:

a. **Jack cắm nguồn DC:**

J8	1	VIN−	BLACK	POWER
	2	VIN+	RED	

Hình 2

b. **Jack cắm TCP/IP:**

	Cable			LAN Cable	
J1	1	TX+	BLACK	ORANGE WHITE	RJ-45
	2	TX−	RED	ORANGE	
	3	RX+	GREEN	GREEN WHITE	
	4	RX−	YELLOW	GREEN	

Hình 3

c. **Jack kết nối khóa, nút nhấn, cảm biến:**

J4	1	SENR	BLUE	SENSOR
	2	GND	ORANGE	GND
	3	DOOR	VIOLET	EXIT BUTTON
	4	NC	YELLOW	DOOR RELAY
	5	COM	GREEN	
	6	NO	WHITE	

Hình 4

d. **Jack kết nối RS-485, Fire Alarm, Wiegand Out Put:**

J9	1	485−	GREY	485
	2	485+	BROWN	
	3	FGND	ORANGE	GND
	4	OD0	RED WHITE	WIEGAND OUT
	5	OD1	BLACK WHITE	
	6	GND	ORANGE	GND
	7	OUT	YELLOW WHITE	TTL(5V) output
	8	IN	BLUE WHITE	FIRE ALARM INPUT

Hình 5

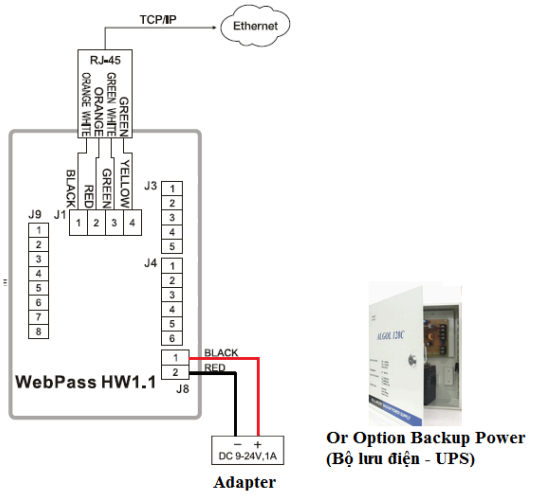
e. Jack kết nối Wiegand In Put:

J3	1	WID0	VIOLET WHITE	WIEGAND IN
	2	WID1	GREEN WHITE	
	3	GND	ORANGE	GND
	4	BUZZ	BLUE BLACK	Control LED and Buzzer
	5	LED	YELLOW BLACK	

Hình 6

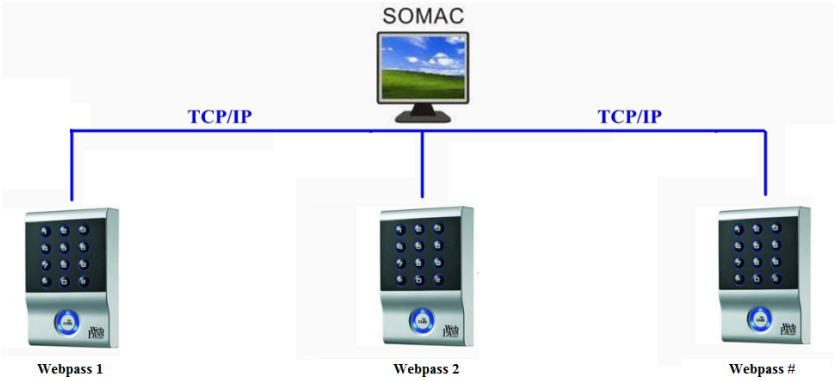
II.2. **Kết nối nguồn:**

Bộ nguồn sử dụng cho Chiyu Webpass là nguồn **9 – 12 Vdc,** có thể sử dụng nguồn Adapter hoặc Bộ lưu điện



Hình 7

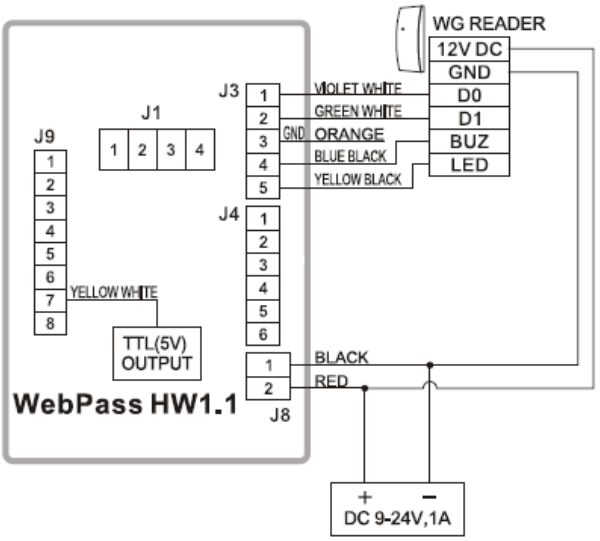
II.3. **Kết nối với máy tính:**



Hình 8

II.4. **Kết nối đầu đọc thẻ phụ:**

Chú ý: Khi sử dụng 2 nguồn khác nhau giữa đầu đọc chính và phụ thì dây GND phải đấu chung.

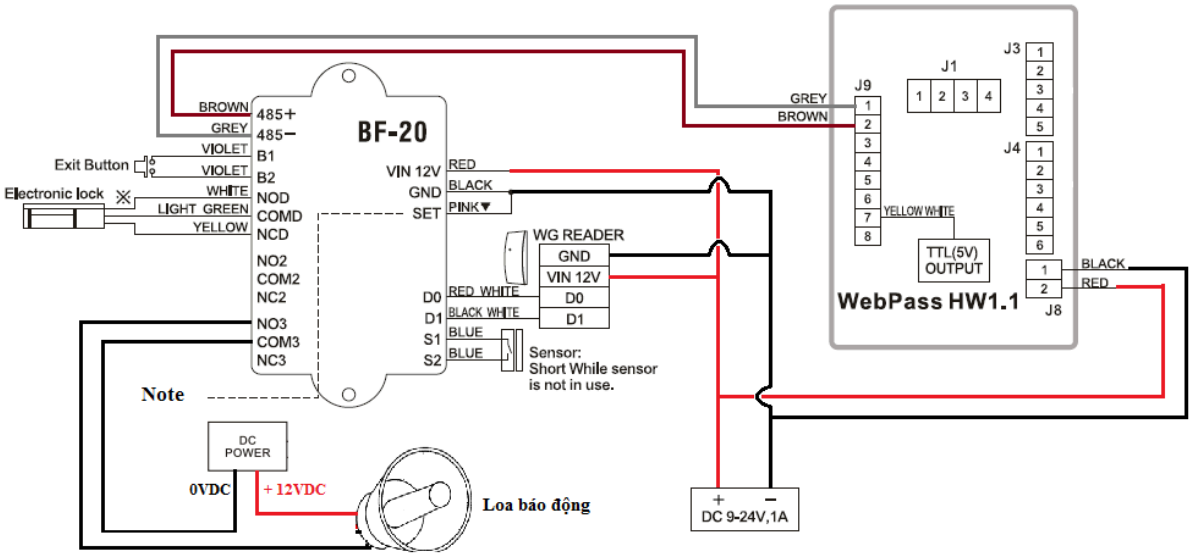


Hình 9

II.5. Kết nối bộ IO Secure BF-20:

Bộ BF-20 (được trang bị 3 Relay) được sử dụng khi mở rộng các IO: khóa, nút nhấn, cảm biến, loa ngoài báo động.

Và khi sử dụng BF-20/50 thì khóa, nút nhấn, Exit, Cảm biến đều phải được kết nối về BF-20/50. Các IO trên Webpass không sử dụng được.



*** Dip Switch**

Khi sử dụng BF-20/50 thì phải chỉnh Door Number Setting ở ID = 1 như trong hình.

Khi sử dụng 2 nguồn của đầu đọc chính và phụ là khác nhau thì phải đấu GND chung.

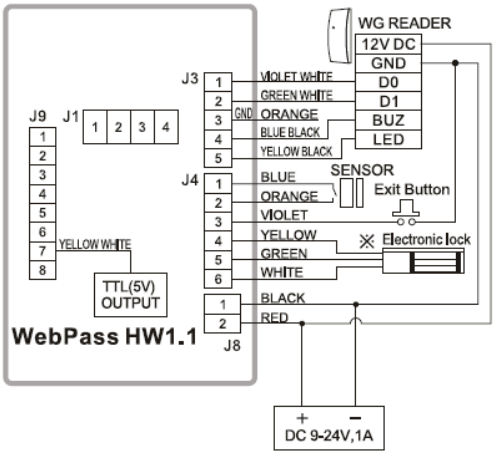
Emergency Mode:

- Khi dây "SET" được nối xuống GND có nghĩa là kích hoạt. Khi BF-20 mất kết nối đến Webpass E thì nhấn nút "Exit" sẽ mở cửa được.

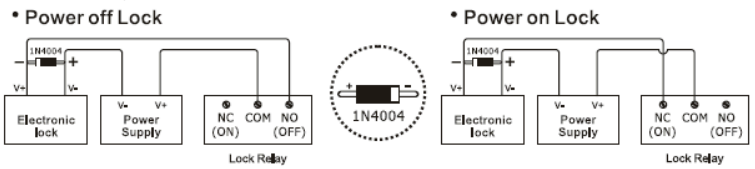
- Khi dây "SET" để trống có nghĩa là ngưng kích hoạt. Khi BF-20 mất kết nối đến Webpass E thì nhấn nút "Exit" sẽ không mở cửa được.

Hình 10

II.6. Kết nối khóa, cảm biến và nút nhấn:



*** Kết nối nguồn cho khóa Electric Lock**



Hình 11

II.7. Kết nối hệ thống báo động:

Để sử dụng chức năng báo động, nghĩa là báo ra loa ngoài, hoặc còi,… ta phải sử dụng thêm bộ BF-20 và kết nối cảm biến cửa. **Xem hình 10**

Hoặc sử dụng: ngõ ra TTL (5V) để điều khiển, bình thường nó đang ra nguồn 5V, khi có báo động phá cửa thì nó sẽ về 0V.

- Door setup – chọn Normal Open / Close

- Event Handle – Event Type chọn Door Intruded – Latech time (nhập số giây báo động) – chọn Level = 5 – Alarm chọn Enable.

II.8. Kết nối Cửa trượt tự động – Auto Slidding Door:

Khi kết nối với Auto Slidding Door thì sử dụng tiếp điểm NO và COM trên Webpass để điều khiển. Khi quét thẻ thành công thì sẽ kích hoạt Relay này, từ đó sẽ gửi tín hiệu đến Auto Door để mở cửa.

II.9. Kết nối Tripod:

Kết nối với Tripod cũng giống như Cửa tự động, lấy tiếp điểm NO & COM trên Webpass đấu vào tiếp điểm hướng đi vào của Tripod, muốn kiểm soát 2 chiều thì phải thêm 1 thiết bị để quét thẻ đi ra nữa.

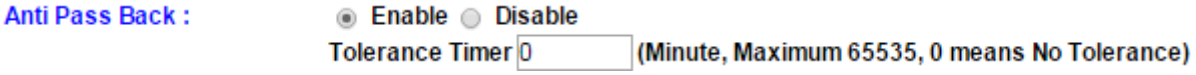
III. Tính năng mở rộng:

III.1. Phân quyền người dùng – Anti Pass Back:

Anti Pass Back là chế độ kiểm soát truy cập ra vào ở mức cao, khi sử dụng chức năng này thì người sử dụng muốn đi vào thì phải quét thẻ đầu đọc bên ngoài, đi ra phải quét đầu đọc thẻ ở bên trong. Trong trường hợp đi theo người khác Vào / Ra thì không thể quét thẻ để đi tiếp được.

a. **Kích hoạt / hủy APB trên thiết bị:**

- Mở trình duyệt Web → Terminal Setup → Anti Pass Back → Kích chọn Enable / Disable để Chọn / Tắt chế độ APB.



Hình 12

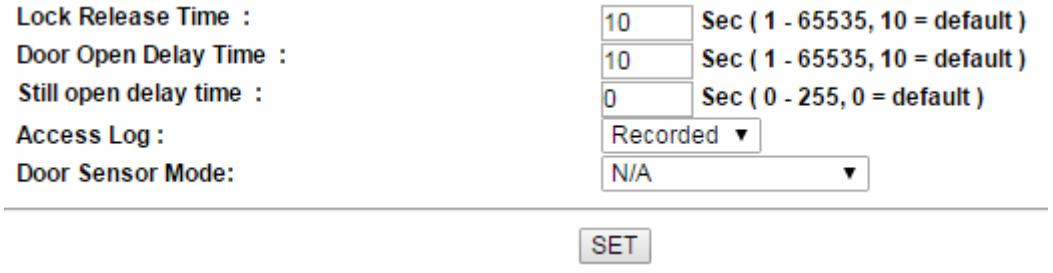
- Tolerance Timer: là khoảng thời gian thiết lập (0 ~ 65.535 giây), khi hết thời gian này thì chế độ APB tự động Reset lại ban đầu, nếu đặt là 0 thì sẽ không Reset cho đến khi nào tắt chế độ APB.
- Thiết lập xong chọn Save để lưu lại.

- **Next Webpass (for APB):** thiết lập APB cho Semac S2 muốn APB, nhưng trong hệ thống phải có nhiều Semac S2. Khi thiết lập xong và lưu lại thì tất cả các Level thiết lập trên Semac S2 hiện tại sẽ được Copy đến Semac S2 tiếp theo.

III.2. Báo động mở cửa quá lâu:

Được áp dụng trong tường hợp cửa được mở ra nhưng quên đóng lại, thiết lập này nhằm nhắc nhở người sử dụng.

- Mở trình duyệt web → Door Setup: điều chỉnh các thông số: Lock Release Time (thời gian mở cửa), Door Open Delay Time (thời gian trì hoãn đóng cửa), Still Open Delay Time, Door Sensor Mode: Normal Open / Close → chọn Set để lưu thiết lập.



Hình 13

- Mở trình duyệt Web → Access Control → Event Handle:

- Event type – chọn loại Sự kiện: [Door Open Too Long]
- Latched time: khoảng thời gian hoạt báo động, nếu = "0" thì báo động liên tục đến khi nào tắt bằng phần mềm [Remote Control] – [Alarm Off]
- Event Level: phải lớn hơn hoặc bằng với Alarm Level thì mới kích hoạt báo động.

→ Lúc này trên BF-20 / Webpass sẽ phát ra âm thanh "di di" sau mỗi 1 giây và liên tục cho đến khi đóng cửa lại. Nếu

cho phép Event Handle thì sẽ kích hoạt Relay 3, khoảng thời gian được điều chỉnh tính bằng giây (0~65.535 giây) trong mục Latched time.

III.3. **Báo động tháo gỡ thiết bị:**

- Tính năng này hoạt động khi kết nối với cảm biến từ gắn tại cửa. Kích hoạt tính năng này bằng cách: Mở trình duyệt web → Door Setup → chọn Door → trong mục Door Sensor Mode chọn Normal Open / Close → chọn Set để lưu thiết lập

Hình 14

- Mở trình duyệt Web → Access Control → Event Handle:
- Event type – chọn loại Sự kiện: [Door Intruded]
- Latched time: khoảng thời gian hoạt báo động, nếu = "0" thì báo động liên tục đến khi nào tắt bằng phần mềm [Remote Control] – [Alarm Off]
- Lúc này trên Webpass sẽ phát ra âm thanh "di di" liên tục cho đến khi đóng cửa lại. Nếu sử dụng BF-20 thì trên BF-20 cũng tương tự.
- Nếu cho phép Event Handle thì sẽ kích hoạt Relay 3 (trên BF-20), khoảng thời gian được điều chỉnh tính bằng giây trong mục Latched time.

III.4. **Tự động mở cửa trong thời gian cho phép:**

Chế độ này được sử dụng trong trường hợp nơi có nhiều nhân viên ra vào liên tục, và chỉ cần kiểm soát ngoài giờ làm việc. Thiết lập như sau: Mở trình duyệt Web → Access Control:

- Time set: thiết lập các khoảng thời gian tự động mở cửa.
- Time zone setup: thiết lập các khoảng thời gian để áp dụng cho các ngày trong tuần.
- Door setup → Lock Release Time Zone → chọn Time zone áp dụng.
- First Card: chọn No need đối với trường hợp tự động mở cửa mà không cần người quét thẻ lần đầu tiên
- First Card: chọn Needed đối với trường hợp tự động mở cửa mà cần người quét thẻ lần đầu tiên.

Nhấn [Set] để lưu lại.

Hình 10

III.5. **Hết hạn và gia hạn thẻ:**

Mở trình duyệt Web → View User List - user đã đăng ký (hoặc Add User đối với đăng ký user mới) → chọn ID user:

Hình 11

- Expire Date Check: là khoảng thời gian hợp lệ cho user, ngoài khoảng thời gian này là hết hạn.
- Chọn [enable] để cho phép, [disable] để ngừng.
- From: thời điểm bắt đầu
- To: thời điểm kết thúc.

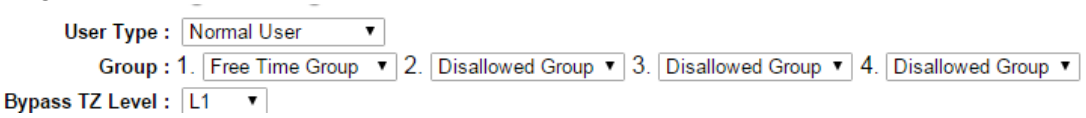
Khi hết thời điểm này có thể gia hạn bằng cách nhập lại thời gian gia hạn thẻ.

III.6. **Time zone:**

Là các khoảng thời gian do người sử dụng tạo ra để ứng dụng: tự động mở cửa, cho phép user truy cập trong các khoảng thời gian cho phép,

- Hỗ trợ lên đến 120 Time zones, 255 Time Sets
- Mỗi user được hỗ trợ tối đa 4 Timezone Groups, áp dụng đối với 7 ngày trong tuần.
- Áp dụng Time zone cho user: Mở trình duyệt Web → Access Control:
- Time set: thiết lập các khoảng thời gian áp dụng.
- Time zone setup: thiết lập các khoảng thời gian để áp dụng cho các ngày trong tuần.
- Tiếp đến chọn user (View user list – chọn User ID): chọn các Group từ 1 – 4, nhưng lưu ý các nhóm này phải

không trùng thời điểm với nhau.

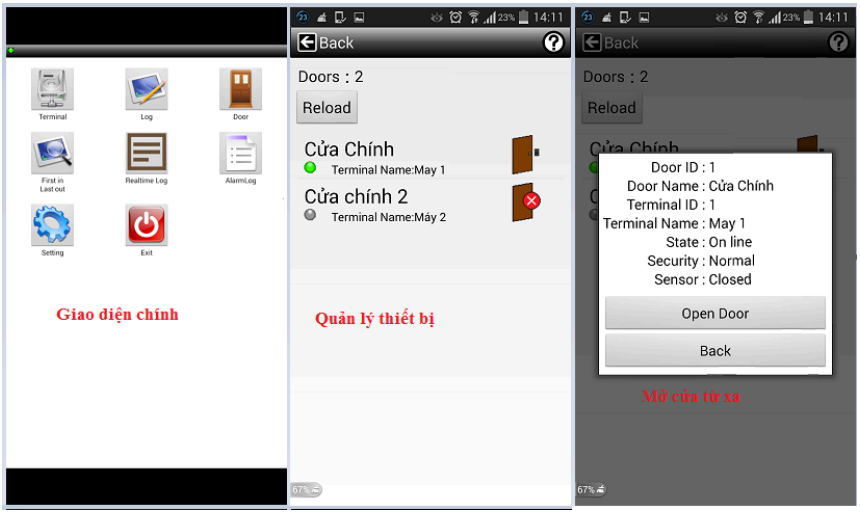


Hình 12

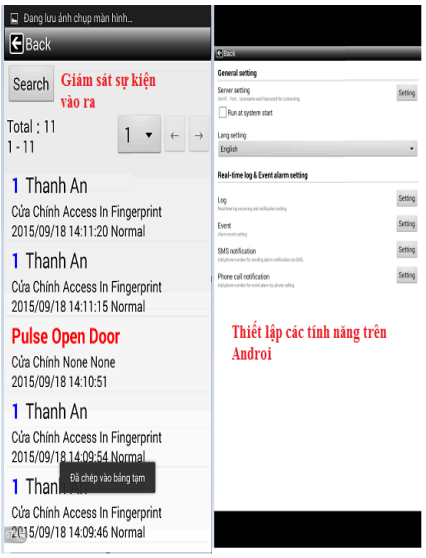
→ lúc này user quét thẻ hoặc vân tay nhưng chỉ cho phép truy cập trong các khoảng Time zones được thiết lập trước.

III.7. **Điều khiển mở cửa từ xa trên điện thoại Androi / Phần mềm / Trình duyệt Web:**

a. Trên điện thoại Androi: trên phần mềm trên Smart phone có tính năng gửi SMS và Gọi điện



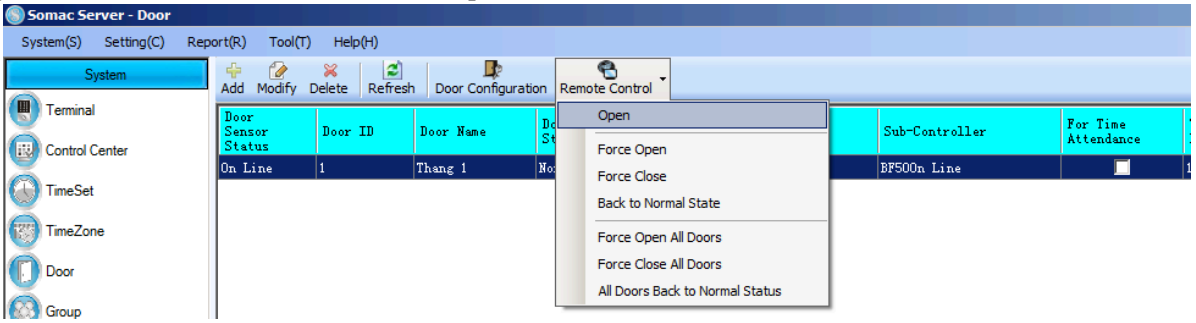
Hình 13



Hình 13

b. Mở cửa từ xa sử dụng phần mềm:

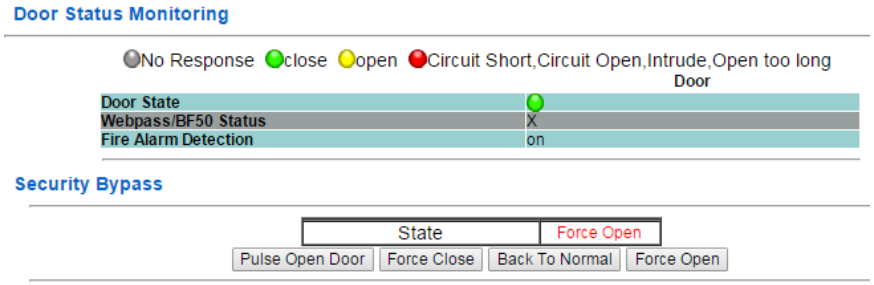
- System → Door → Remote Control → Open:



Hình 14

c. **Mở cửa từ xa dùng Web:**

Access control → Remote Control → Pulse Open Door:



Hình 16

IV. Sử dụng độc lập không sử dụng phần mềm:

Webpass hỗ trợ bàn phím để cài đặt thẻ, password. Một số ký hiệu sử dụng:

UUUUUU – User ID: 1~6 ký tự

QQQQQQ – Số lượng thẻ cần đăng ký: 1~6 ký tự

PPPPPPPP – mật khẩu user: 4~8 ký tự

Thao tác mặc định:

*Master Code# : đăng nhập vào Menu thiết bị (mặc định Master Code: 123456)

"thao tác lệnh"

*#: Thoát Menu

IV.1. Thiết lập thời gian đóng cửa

- Bước 1: Nhấn * 123456 #
- Bước 2: Nhấn **02 * TTTTT #**

TTTTT = 1 đến 65535 giây/ mặc định 10 giây.

- Bước 3: Nhấn * #

IV.2. Thiết lập thời gian chờ mở cửa – thời gian trì hoãn mở cửa

- Bước 1: Nhấn * 123456 #
- Bước 2: Nhấn 03 * **TTTTT** #

TTTTT = 1 đến 65535 giây/ mặc định 10 giây.

- Bước 3: Nhấn * #

IV.3. Thiết lập giờ trên thiết bị

- Bước 1: Nhấn * 123456 #
- Bước 2: **04 * HHMMSS #**

HHMMSS: Giờ/Phút/Giây(24H)

- Bước 3: Nhấn * #

IV.4. Thiết lập ngày trên thiết bị

- Bước 1: Nhấn * 123456 #

05 * YYMMDDX #

WWMMDDX: Năm/Tháng/Ngày/Ngày trong tuần.

YY=AD: lấy 2 số cuối=2009=09

IV.5. Thay đổi Mastercode mặc định

- Bước 1: Nhấn * 123456 #
- Bước 2: 06*AAAAAA*BBBBBB*BBBBBB#

AAAAAA: master code cũ

BBBBBBB: Mastercode mới

Master code 6 số.

- Bước 3: Nhấn * #

IV.6. Thiết lập ID của thiết bị

- Bước 1: Nhấn * 123456 #
- Bước 2: 07*TTTTT#

TTTTT: id của thiết bị từ 1 đến 65535

- Bước 2: *#

IV.7. **Thiết lập chế độ của thiết bị**

- Bước 1: Nhấn * 123456 #
- Bước 2: 08*T#
  T=0/1/2 □ thường mở/thường đóng/bình thường.
- Bước 3: *#

IV.8. **Mode sử dụng của thiết bị**

- Bước 1: Nhấn * 123456 #
- Bước 2: 09*T#
  T=1 đến 4.
  1:Thẻ, passord mặc định, password cá nhân.
  2: Thẻ.
  3: Password mặc định, password cá nhân.
  4:Thẻ and password cá nhân.
- Bước 3: *#

IV.9. **Password mặc định**

- Bước 1: Nhấn * 123456 #
- Bước 2: 10*PPPPPPPP#
  Mặc định 1234, có thể dùng web xóa.
- Bước 3: *#

IV.10. **Đăng ký 1 thẻ**

- Bước 1: Nhấn * 123456 #
- Bước 2: 11*UUUUUU# quét thẻ qua đầu đọc
  UUUUUU: user id của user (như là Số thứ tự trong danh sách).
- Bước 3: *#

IV.11. **Đăng ký thẻ + password**

- Bước 1: Nhấn * 123456 #
- Bước 2: 11*UUUUUU*PPPPPPPP# Quét thẻ. Nếu chỉ đăng ký password thì sau lệnh này bấm thêm [*] rồi tiếp bước 3
- Bước 3: *#

IV.12. **Đăng ký nhiều thẻ (Thẻ có mã thẻ liên tục).**

- Bước 1: Nhấn * 123456 #
- Bước 2: 12*UUUUUU*QQQQQQ# Quét thẻ.
- Bước 3: *#

IV.13. **Đăng ký nhiều thẻ (Quét thẻ liên tiếp lên đầu đọc).**

- Bước 1: Nhấn * 123456 #
- Bước 2: 13*UUUUUU*QQQQQQ# Quét lần lượt thẻ qua đầu đọc. UUUUUU ở đây là user ID đầu tiên, và tự động tăng số thứ tự sau mỗi lần quét thẻ.
- Bước 3: *#

IV.14. **Ngưng sử dụng thẻ (User status: Cancel)**

- Bước 1: Nhấn * 123456 #
- Bước 2: 14*UUUUUU#
- Bước 3: *#

IV.15. **Phục hồi thẻ ngưng sử dụng (User status: Active)**

- Bước 1: Nhấn * 123456 #
- Bước 2: 15*UUUUUU#
- Bước 3: *#

IV.16. **Thay đổi password**

- Bước 1: Nhấn * 123456 #
- Bước 2: 16*UUUUUU*PPPPPPPP#
  PPPPPPPP: password người dùng 4 – 8 chữ số.
- Bước 3: *#

IV.17. **Thay đổi thẻ**

- Bước 1: Nhấn * 123456 #
- Bước 2: 17*UUUUUU# Quét thẻ mới
- Bước 3: *#

IV.18. **Xóa 1 thẻ người dùng**

- Bước 1: Nhấn * 123456 #
- Bước 2: 21*UUUUUU#
- Bước 3: *#

IV.19. **Xóa 1 khoảng thẻ người dùng**

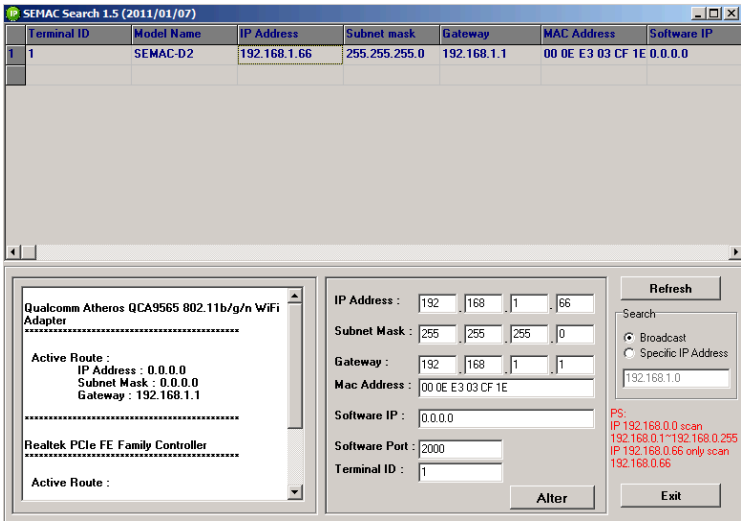
- Bước 1: Nhấn * 123456 #
- Bước 2: 22*UUUUUU*QQQQQQ#
- Bước 3: *#

IV.20. **Xóa tất cả thẻ người dùng.**

- Bước 1: Nhấn * 123456 #
- Bước 2: 23*29*#
- Bước 3: *#

B. HƯỚNG DẪN SỬ DỤNG TRÊN TRÌNH DUYỆT WEB – WEBBASE

Dùng phần mềm Somac Search (kèm theo đĩa) để dò tìm thiết bị:



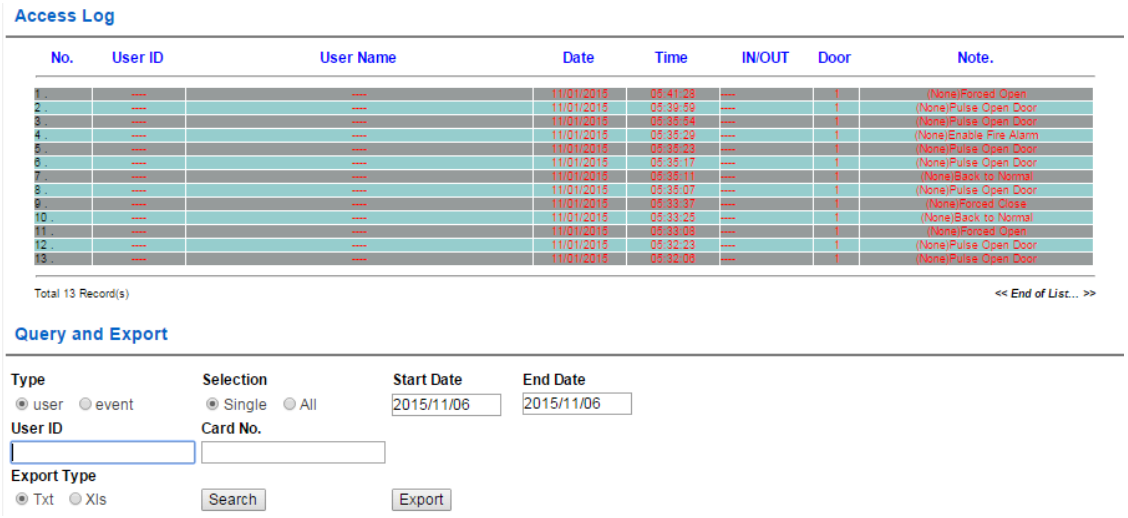
Hình 15

Thay đổi các thông số:
IP Address, Subnet mask, Gateway, Software IP, Termial, Port, sau đó nhấn Alter để lưu lại.
Sau đó mở trình duyệt Web IE, Chrome, Firefox gõ địa chỉ IP vào màn hình thiết lập:
Đăng nhập vào thiết bị:
Mở trình duyệt IE và gõ vào ip của thiết bị. Ví dụ: http://192.168.0.66, nếu yêu cầu password thì nhập vào, mặc định:
Username: admin
Password: admin

I. Quản trị user (User Administration)

I.1. **Xem lại dữ liệu vào ra (Access Log)**

Xem lại toàn bộ dữ liệu vào ra: Access Log → tùy chọn các thông số để xem lại: ID, Type, khoảng ngày tháng → [Search] → [Export] nếu muốn xuất ra file.



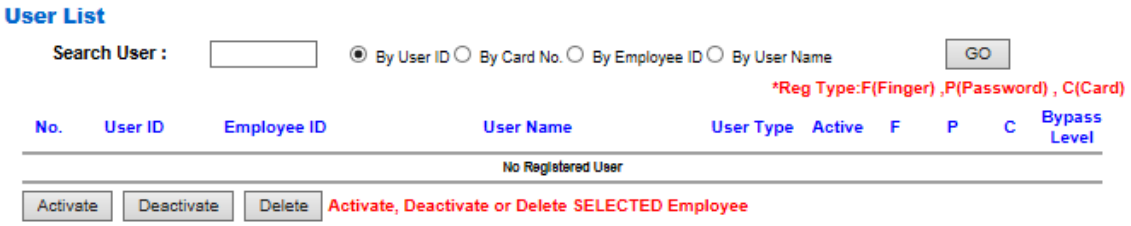
Hình 16

I.2. **Xem trực tiếp dữ liệu quét thẻ (Auto Refresh Log)**

Xem dữ liệu trực tiếp khi quét thẻ / vân tay.

Hình 17

I.3. **Xem danh sách user (View User List)**

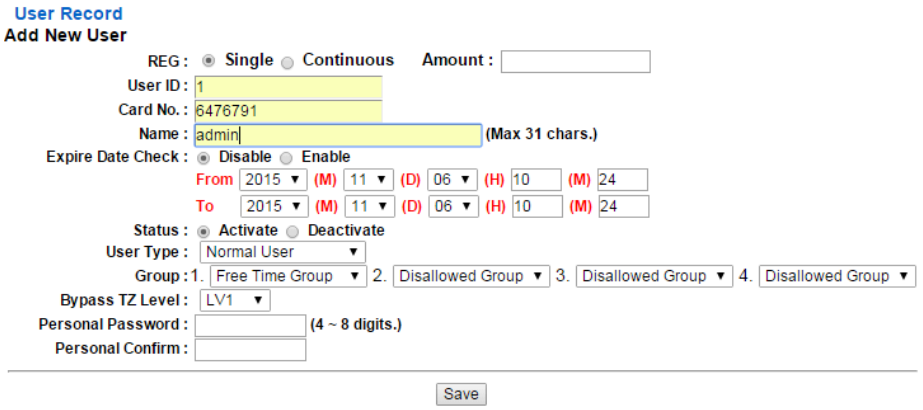


Hình 18

Trong mục này có thể:

- Cho phép user hoạt động: Active
- Ngưng hoạt động của user: Deactive
- Xóa user: Delete
- Chỉnh sửa user: double click vào user

I.4. **Đăng ký user (Add User)**



Hình 19

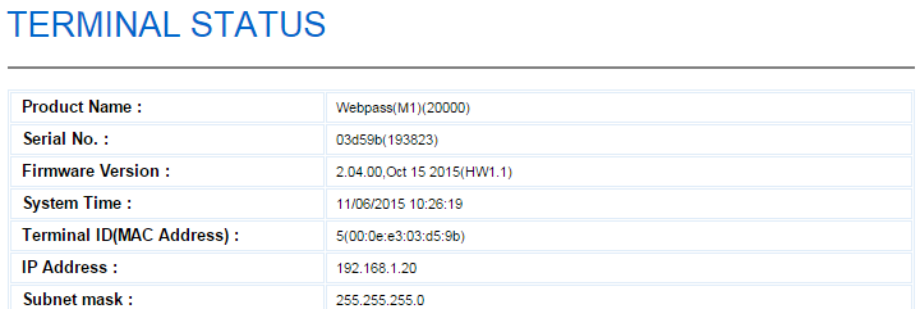
Nhập vào các thông số:

- User ID: Mã chấm công, phải trong giới hạn 1 ~ 20.000
- Card No.: Mã thẻ
- Name: họ tên
- Expire Date: Hạn sử dụng thẻ
- Status: Trạng thái user. Active: kích hoạt, Deactive: ngưng hoạt động
- User Type: tùy chọn theo quyền truy cập.
- Group: chọn Group cho user. Trong group được chọn thì user có thể đi được các cửa, các khoảng thời gian đã được định sẵn.
- Bypass TZ Level: mỗi user được quy định từ L1~L10. Khi nào Level "Bypass Time Zone Level" của user lơn hơn hoặc bằng "Bypass Time Zone" của Door thì Door sẽ vô hiệu, lúc này user level cao hơn sẽ đi được cửa có level thấp hơn.
- Personal Password: nhập 2 lần từ 4 – 8 ký tự số.

  Sau đó lưu lại

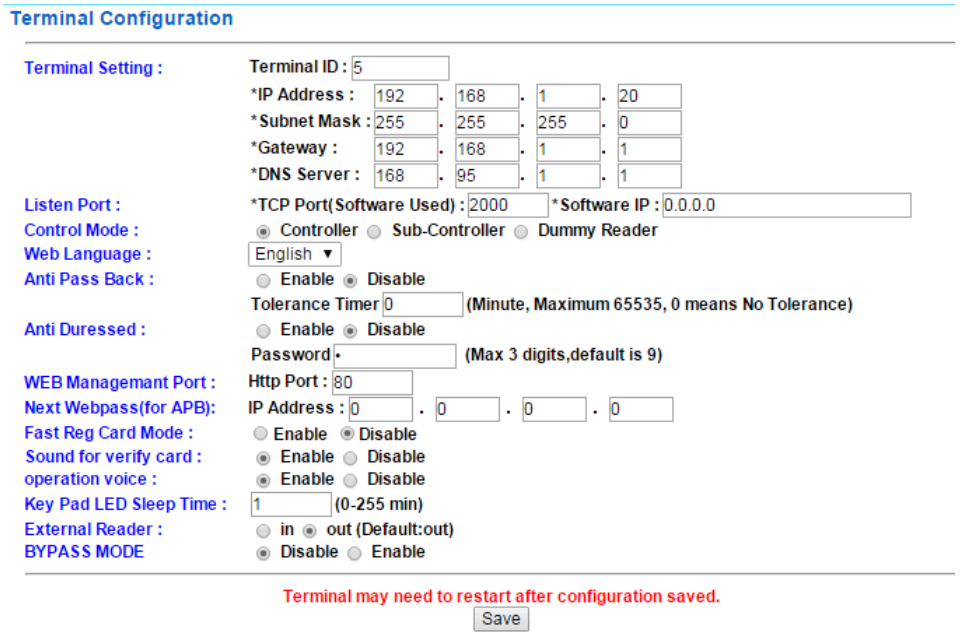
II. Quản trị thiết bị (Terminal)

II.1. Trạng thái thiết bị (Terminal Status)



Hình 20

II.2. Cài đặt thông số thiết bị (Terminal Setup)

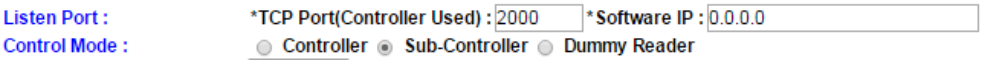


Hình 21

- **Terminal Setting**: nhập vào các thông số Terminal ID: từ 1 đến 65535, IP. Subnet Mask,…
- **Software IP**: là IP cửa máy tính có phần mềm kết nối.
- **Control Mode**:

Controller: hoạt động ở trạng thái controller

Sub-Controller: hoạt động ở trạng thái Controller phụ, được sử dụng khi kết hợp với Semac S2 (Webpass vẫn connect tới hệ thống mạng dùng TCP/IP chứ không phải là đầu đọc thẻ phụ như wiegand reader). Nguyên tắc sử dụng như sau:



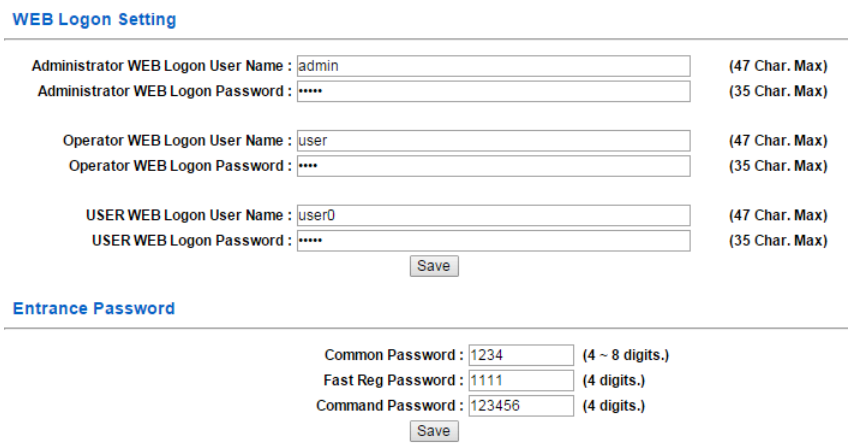
Chuyển Software IP là của Semac S2, ID của webpass cũng trùng với ID của Semac S2. Lúc này quét thẻ trên Webpass dữ liệu truyền về Semac S2 xem có đúng không, sau đó mới mở cửa (khóa cửa tại Webpass vẫn được kết nối tại Webpass).

Dummy Reader: đổi thành Wiegand Reader

- **Web Language:** chọn ngôn ngữ hiển thị
- **Anti-Passback:** chế độ quản lý Vào – Ra, phải check thiết bị Vào thì mới check thiết bị Ra được. [Tolerance Time]: Thời gian phục hồi chế độ Anti-Passback.
- **Anti Duressed:**
- **Web Managerment Port:**
- **Next Webpass** (for APB): thiết lập IP cho bộ Semac S2 kế tiếp sử dụng APB, khi thiết lập xong tất cả Level của Semac S2 hiện tại sẽ được copy sang Semac S2 kế tiếp.
- **Fast Reg. Card Mode:** cho phép đăng ký user nhanh bằng cách quét thẻ liên tục
- **Sound for verify card:** âm thanh xác thực khi quét thẻ
- **Operation voice:** âm thanh xác thực khi thao tác lệnh.
- **Bypass Mode:**

Nhấn Save sau khi thiết lập xong.

II.3. Cài đặt password thiết bị (Password Setup)

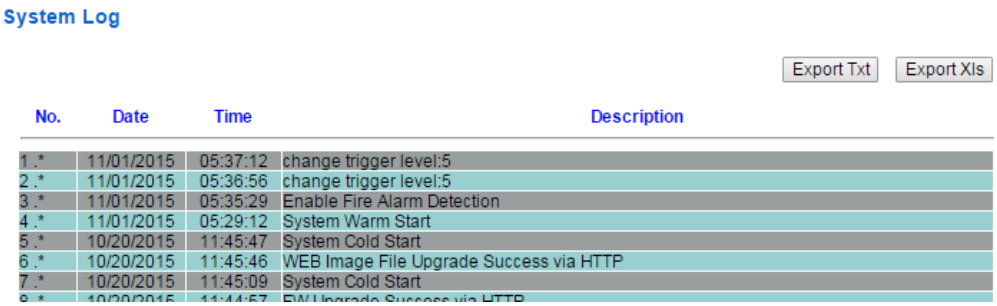


Hình 22

- **Administrator web**: user toàn quyền thao tác trên webpage
- **Operator Web logon user Name:** user đăng nhập webpage nhưng không có chức năng thay đổi thông tin thiết bị.
- **User web Logon User Namer:** user chỉ có quyền xem báo cáo
- **Common password:** password dùng chung để mở cửa
- **Fast Reg Password:** password dùng để đăng ký user thẻ nhanh.
- **Command password:** password để đăng nhập vào menu đăng ký Master Code.

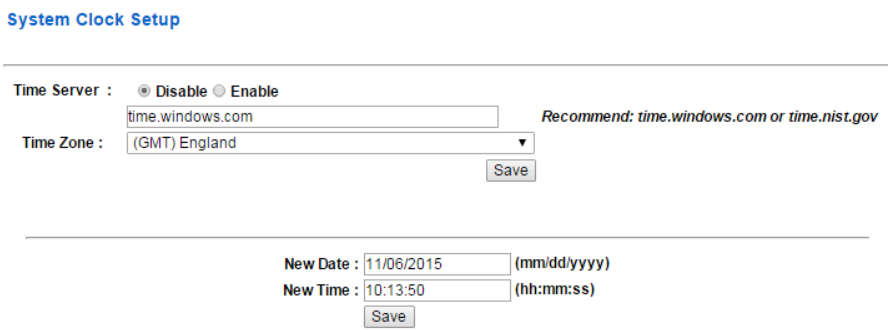
II.4. Sự kiện hệ thống (System Log)

Là những dữ liệu các sự kiện của thiết bị: Alarm, Power.



Hình 23

II.5. Cài đặt ngày giờ (Clock Setup)

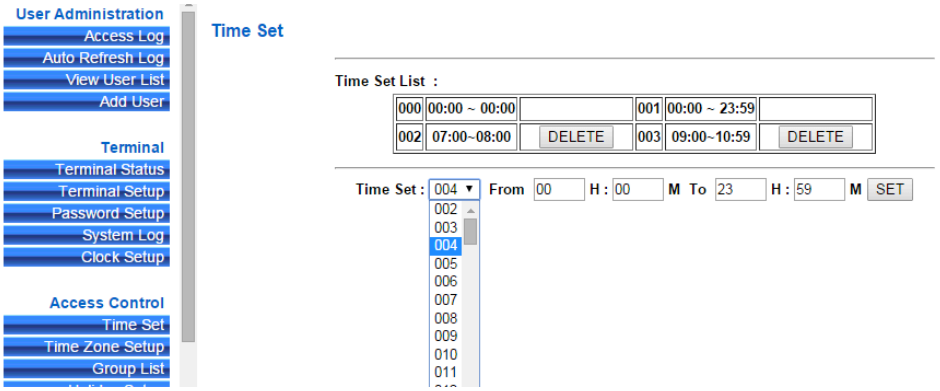


Hình 24

III. Cài đặt kiểm soát ra vào (Access Control)

III.1. Thiết lập các khoảng thời gian cho Time Zone (Time Set)

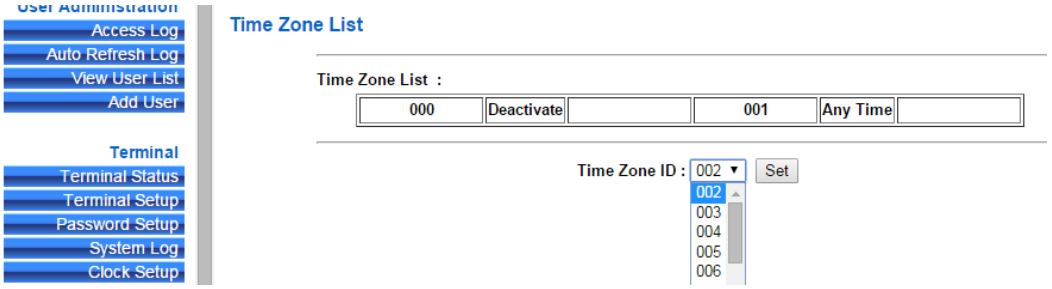
Thiết bị hỗ trợ 255 khoảng thời gian: Time Set → chọn Set để lưu lại



Hình 25

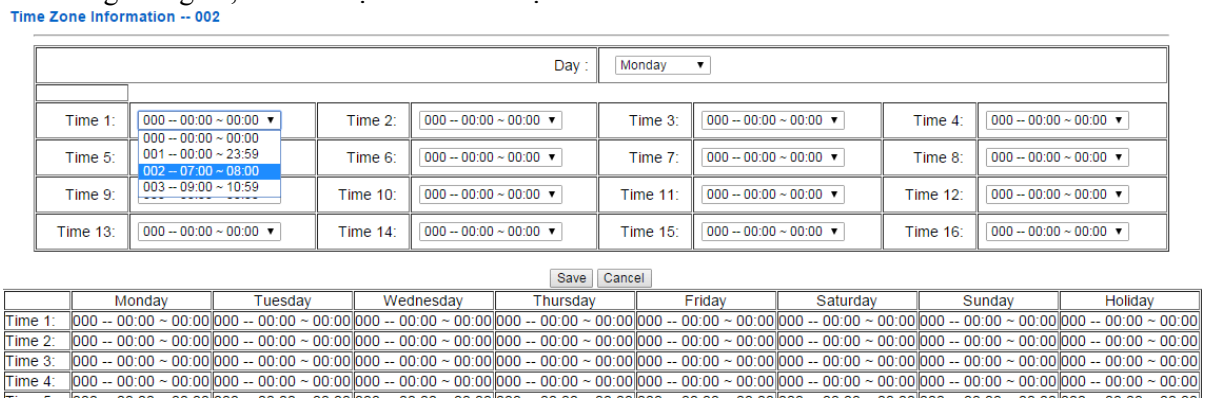
III.2. Cài đặt Time Zone (Time Zone Setup)

Thiết bị hỗ trợ 120 khoảng thời gian: chọn Time Zone ID → chọn Set



Hình 26

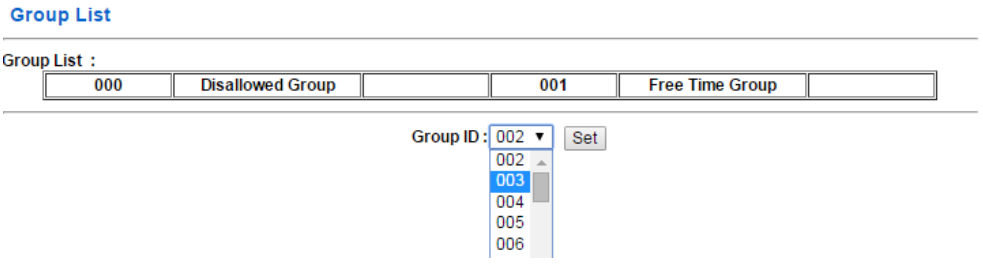
Chọn các khoảng thời gian, sau đó chọ Save để lưu lại



Hình 27

III.3. Cài đặt nhóm (Group List)

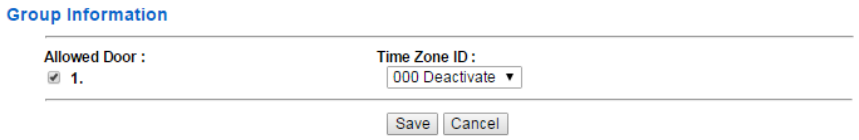
Chọn Group ID → chọn Set để cài đặt, hỗ trợ 255 Group



Hình 38

Khi bảng Group Information xuất hiện:

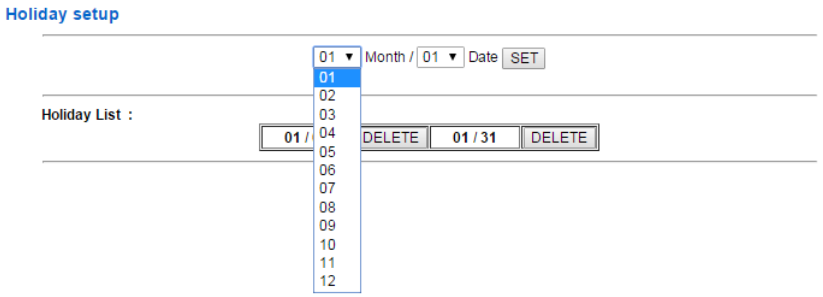
- Allowed Door: chọn Door 1 thì user trong Group này chỉ đi được Cửa 1
- Time zone ID: chọn Time Zone ID nào tương ứng với Group thì user chỉ được đi trong khoảng Time Zone và Door này.
- Sau đó chọn Save để lưu



Hình 29

III.4. Cài đặt ngày nghỉ (Holiday Setup)

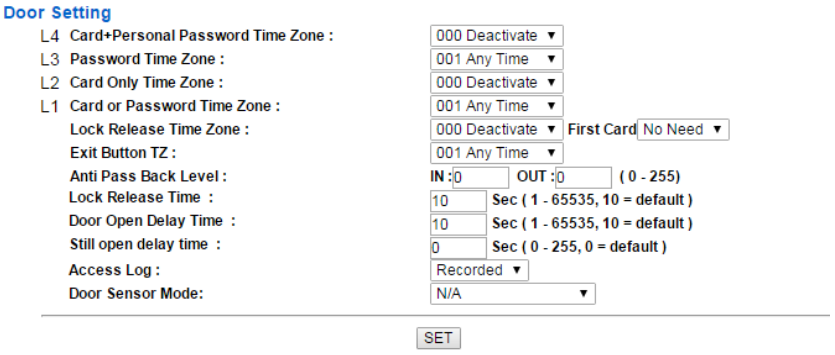
Chọn ngày, chọn tháng và Save để lưu lại



Hình 30

III.5. Cài đặt cửa (Door Setup)

Chọn Door Setting để thiết lập các thông số cho cửa:



Hình 31

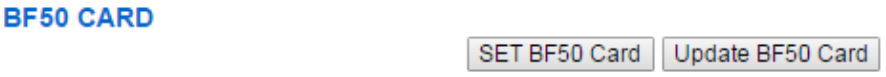
- Card + Personal Password Time Zone (L4): mặc định là không sử dụng (Deactivate), khi Time Zone này được chọn thì user muốn truy nhập được thì user phải quét thẻ và nhập password user mới truy cập cửa được. User có thể nhập password trước rồi quét thẻ hoặc ngược lại. Nếu Lever của user là L4, thì user có thể truy nhập vào các cửa chỉ dùng Card. Và nếu "Card + Personal Password Time Zone (L4)" là "Lock Release Time Zone" thì user có thể truy nhập không giới hạn.
- Password Time Zone (L3): mặc định là không sử dụng (Deactivate), khi Time Zone này được chọn thì user muốn truy nhập được thì user phải nhập password Common (password dùng chung) mới truy cập cửa được. Nếu Lever của user là L3~L4, thì user có thể truy nhập vào các cửa chỉ dùng Card. Và nếu "Password Time Zone (L3)" là "Lock Release Time Zone" thì user có thể truy nhập không giới hạn.
- Card Only Time Zone (L2): mặc định là không sử dụng (Deactivate), khi Time Zone này được chọn thì user muốn truy nhập được thì user quét thẻ mới truy cập cửa được. Nếu Lever của user là L2~L4, thì user có thể truy nhập vào các cửa chỉ dùng Card. Và nếu "Card Only Time Zone (L2)" là "Lock Release Time Zone" thì user có thể truy nhập không giới hạn.
- Card or FP Time Zone (L1): mặc định là không sử dụng (Deactivate), khi Time Zone này được chọn thì user muốn truy nhập được thì user quét thẻ hoặc nhập password Common (password dùng chung) mới

truy cập cửa được. Nếu Lever của user là L1~L4, thì user có thể truy nhập vào các cửa bằng cách quét thẻ mà không cần password Common. Và nếu "Card or FP Time Zone (L1)" là "Lock Release Time Zone" thì user có thể truy nhập không giới hạn.

- Lock Release Time Zone: mặc định là không sử dụng (Deactivate), khi Time Zone này được chọn thì có 2 trường hợp: nếu "First Card" là "No Need" thì cửa sẽ tự động mở trong Time Zone này, nếu "First Card" là "Needed" thì cửa sẽ tự động mở Time Zone này nhưng phải có một user quét thẻ 1 lần đầu tiên.
- Exit Button TZ: mặc định là luôn luôn (Any Time), không sử dụng thì chọn "Deactive", khi Time Zone này được chọn thì nút Exit sẽ chỉ sử dụng được trong Time Zone này.
- Anti Pass Back Level: thiết lập Level cho Anti Pass Back In/Out từ 0~255, mặc định là "0"
- Lock Release Time: cài đặt thời gian mở cửa. Mặc định là 10 giây (từ 1~65535s).
- Door Open Delay Time: cài đặt thời gian trì hoãn mở cửa. Mặc định là 10 giây (từ 1~65535s).
- Still Open Delay Time: thời gian vẫn còn tính là cửa còn mở. Mặc định là 0 giây (từ 0~255s).
- Access Log: trạng thái của dữ liệu quét thẻ / vân tay. Chọn Igored để không lưu, Recorded để lưu, TA chỉ dữ liệu chấm công.
- Door Sensor Mode: trạng thái cảm biến cửa. N/A: không sử dụng. Normal Open/Close: cảm biến thường đóng/mở. Circuit Short/Open: ngắn mạch / hở mạch.

Các biểu tượng chức năng:

- Set BF50 Card: BF-50 là bộ IO Secure, nó có khả năng lưu trữ 50 Cards trong trường hợp mất kết nối đến Biosense, nhưng 50 thẻ này vẫn quét thẻ trên đầu đọc phụ để truy cập được.
- Update BF50 Card: chọn để lưu các trạng thái của BF-20/50

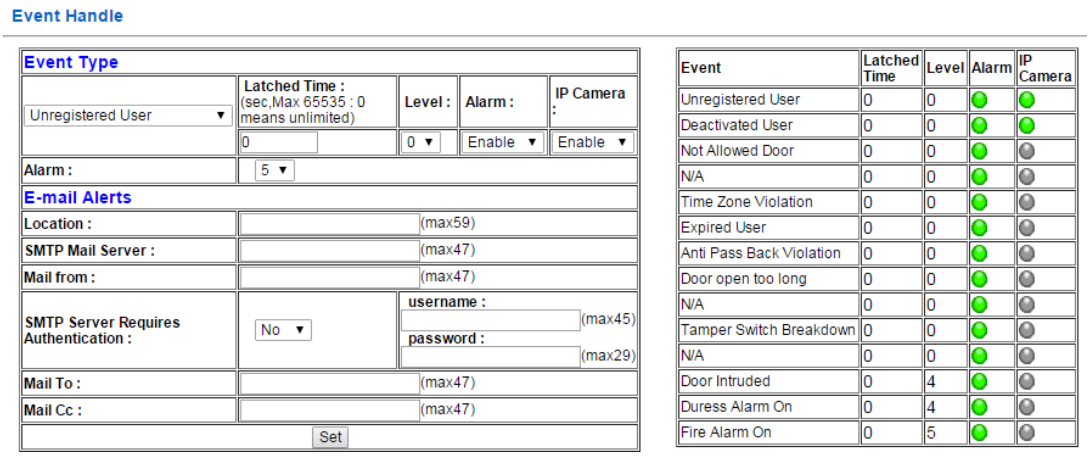


Hình 32

III.6. Điều khiển mở cửa từ xa (Remote Control)

Xem hình 16

III.7. Thiết lập sự kiện báo động (Event Handle)



Hình 33

a. **Thiết lập loại sự kiện:**

- Unregistered User: Nếu sự kiện này được chọn, khi người sử dụng thẻ chưa đăng ký để truy cập thì sẽ tự động ghi lại và hiển thị sự kiện đó trong mục Access Log. Khi level kích hoạt sự kiện "Even Trigger Level" được thiết lập lớn hơn hoặc bằng level kích hoạt báo động "Alarm Trigger Level" của thiết bị thì Relay sẽ kích hoạt (theo thời gian trong mục Latched Time, từ 1~65535 giây) và ngay lập tức gửi Email đến người dùng. Khi [Latched Time] = [0] thì sẽ báo động liên tục và chỉ được tắt khi vào [Remote Control] – [Alarm Off]. Mặc định [Event Trigger Level] = 0
- Deactived User: Nếu sự kiện này được chọn, khi người sử dụng thẻ chưa được kích hoạt để truy cập thì sẽ tự động ghi lại và hiển thị sự kiện đó trong mục Access Log. Khi level kích hoạt sự kiện "Even Trigger Level" được thiết lập lớn hơn hoặc bằng level kích hoạt báo động "Alarm Trigger Level" của

thiết bị thì Relay sẽ kích hoạt (theo thời gian trong mục Latched Time, từ 1~65535 giây) và ngay lập tức gửi Email đến người dùng. Khi [Latched Time] = [0] thì sẽ báo động liên tục và chỉ được tắt khi vào [Remote Control] – [Alarm Off]. Mặc định [Event Trigger Level] = 0

- Not Allowed Door: Nếu sự kiện này được chọn, khi người sử dụng thẻ thuộc nhóm [Door Group] khác với [Door Group] hợp lệ để truy cập thì sẽ tự động ghi lại và hiển thị sự kiện đó trong mục Access Log. Khi level kích hoạt sự kiện "Even Trigger Level" được thiết lập lớn hơn hoặc bằng level kích hoạt báo động "Alarm Trigger Level" của thiết bị thì Relay sẽ kích hoạt (theo thời gian trong mục Latched Time, từ 1~65535 giây) và ngay lập tức gửi Email đến người dùng. Khi [Latched Time] = [0] thì sẽ báo động liên tục và chỉ được tắt khi vào [Remote Control] – [Alarm Off]. Mặc định [Event Trigger Level] = 0
- Time Zone Violation: Nếu sự kiện này được chọn, khi người sử dụng thẻ có Time Zone thuộc nhóm [Door Group] khác với [Door Group] hợp lệ để truy cập thì sẽ tự động ghi lại và hiển thị sự kiện "(1) Open Time Error" trong mục Access Log. Khi level kích hoạt sự kiện "Even Trigger Level" được thiết lập lớn hơn hoặc bằng level kích hoạt báo động "Alarm Trigger Level" của thiết bị thì Relay sẽ kích hoạt (theo thời gian trong mục Latched Time, từ 1~65535 giây) và ngay lập tức gửi Email đến người dùng. Khi [Latched Time] = [0] thì sẽ báo động liên tục và chỉ được tắt khi vào [Remote Control] – [Alarm Off]. Mặc định [Event Trigger Level] = 0
- Expired User: Nếu sự kiện này được chọn, khi người sử dụng xác thực "Multi Badge" không thành công để truy cập thì sẽ tự động ghi lại và hiển thị sự kiện đó trong mục Access Log. Khi level kích hoạt sự kiện "Even Trigger Level" được thiết lập lớn hơn hoặc bằng level kích hoạt báo động "Alarm Trigger Level" của thiết bị thì Relay sẽ kích hoạt (theo thời gian trong mục Latched Time, từ 1~65535 giây) và ngay lập tức gửi Email đến người dùng. Khi [Latched Time] = [0] thì sẽ báo động liên tục và chỉ được tắt khi vào [Remote Control] – [Alarm Off]. Mặc định [Event Trigger Level] = 0
- Anti Pass Back Violation: Nếu sự kiện này được chọn, khi người sử dụng xác thực "Anti Pass Back" không thành công để truy cập thì sẽ tự động ghi lại và hiển thị sự kiện "(1) ANTI_PB REJ" trong mục Access Log. Khi level kích hoạt sự kiện "Even Trigger Level" được thiết lập lớn hơn hoặc bằng level kích hoạt báo động "Alarm Trigger Level" của thiết bị thì Relay sẽ kích hoạt (theo thời gian trong mục Latched Time, từ 1~65535 giây) và ngay lập tức gửi Email đến người dùng. Khi [Latched Time] = [0] thì sẽ báo động liên tục và chỉ được tắt khi vào [Remote Control] – [Alarm Off]. Mặc định [Event Trigger Level] = 0
- Door Open Too Long: Nếu sự kiện này được chọn, khi người sử dụng xác thực thành công để truy cập, nhưng hết thời gian đóng cửa mà cửa chưa được đóng lại thì sẽ tự động ghi lại và hiển thị sự kiện "(O) Open Too Long" trong mục Access Log. Khi level kích hoạt sự kiện "Even Trigger Level" được thiết lập lớn hơn hoặc bằng level kích hoạt báo động "Alarm Trigger Level" của thiết bị thì Relay sẽ kích hoạt (theo thời gian trong mục Latched Time, từ 1~65535 giây) và ngay lập tức gửi Email đến người dùng. Khi [Latched Time] = [0] thì sẽ báo động liên tục và chỉ được tắt khi vào [Remote Control] – [Alarm Off]. Mặc định [Event Trigger Level] = 0
- Tamper Switch Breakdown: Nếu sự kiện này được chọn, khi thiết bị bị tháo gỡ / phá hoại sẽ tự động ghi lại và hiển thị sự kiện "CASE OPENED" trong mục Access Log. Khi level kích hoạt sự kiện "Even Trigger Level" được thiết lập lớn hơn hoặc bằng level kích hoạt báo động "Alarm Trigger Level" của thiết bị thì Relay sẽ kích hoạt (theo thời gian trong mục Latched Time, từ 1~65535 giây) và ngay lập tức gửi Email đến người dùng. Khi [Latched Time] = [0] thì sẽ báo động liên tục và chỉ được tắt khi vào [Remote Control] – [Alarm Off]. Mặc định [Event Trigger Level] = 0
- Door Intruded: Nếu sự kiện này được chọn, khi cửa bị mở mà không quét thẻ hợp lệ (cây cửa) thì sẽ tự động ghi lại và hiển thị sự kiện "(O) Door Intruded" trong mục Access Log. Khi level kích hoạt sự kiện "Even Trigger Level" được thiết lập lớn hơn hoặc bằng level kích hoạt báo động "Alarm Trigger Level" của thiết bị thì Relay sẽ kích hoạt (theo thời gian trong mục Latched Time, từ 1~65535 giây) và ngay lập tức gửi Email đến người dùng. Khi [Latched Time] = [0] thì sẽ báo động liên tục và chỉ được tắt khi vào [Remote Control] – [Alarm Off]. Mặc định [Event Trigger Level] = 0
- Duress Alarm On: Nếu sự kiện này được chọn, khi "Duress Alarm" của cửa được kích hoạt (Chú ý: bạn phải nhập password "Duress Code" và nhấn "Enter" trước khi quét thẻ để truy cập mới chính xác) sẽ tự động ghi lại và hiển thị sự kiện "ANTI DURESS" trong mục Access Log. Khi level kích hoạt sự kiện "Even Trigger Level" được thiết lập lớn hơn hoặc bằng level kích hoạt báo động "Alarm Trigger Level" của thiết bị thì Relay sẽ kích hoạt (theo thời gian trong mục Latched Time, từ 1~65535 giây) và ngay lập tức gửi Email đến người dùng. Khi [Latched Time] = [0] thì sẽ báo động liên tục và chỉ được tắt khi vào

[Remote Control] – [Alarm Off]. Mặc định [Event Trigger Level] = 0

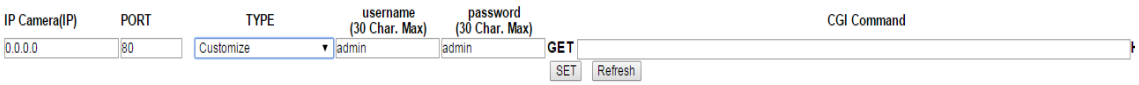
- Fire Alarm On: Nếu sự kiện này được chọn, khi có tín hiệu "Fire Alarm" được kích hoạt sẽ tự động ghi lại và hiển thị sự kiện "FIRE ALARM" trong mục Access Log. Khi level kích hoạt sự kiện "Even Trigger Level" được thiết lập lớn hơn hoặc bằng level kích hoạt báo động "Alarm Trigger Level" của thiết bị thì Relay sẽ kích hoạt (theo thời gian trong mục Latched Time, từ 1~65535 giây) và ngay lập tức gửi Email đến người dùng. Khi [Latched Time] = [0] thì sẽ báo động liên tục và chỉ được tắt khi vào [Remote Control] – [Alarm Off]. Mặc định [Event Trigger Level] = 0
- Latched Time: thời gian kích hoạt báo động cho phép từ 1~65535 giây. Khi [Latched Time] = [0] thì sẽ báo động liên tục và chỉ được tắt khi vào [Remote Control] – [Alarm Off]. Mặc định [Event Trigger Level] = 0
- Level: Event Trigger Level.
- Alarm: Alarm Trigger Level.

b. **Gửi Email báo động:**

- Location: Tên thiết bị / tên ứng dụng trên thiết bị.
- SMTP Mail Server: nhập server mail
- Mail From: Email người gửi
- SMTP Server Requires Authentication: nhập password của Email người gửi thư.
- Mail To: Email người nhận thư
- Mail Cc: Email người nhận thư thứ 2

IV. Công cụ (Tools)

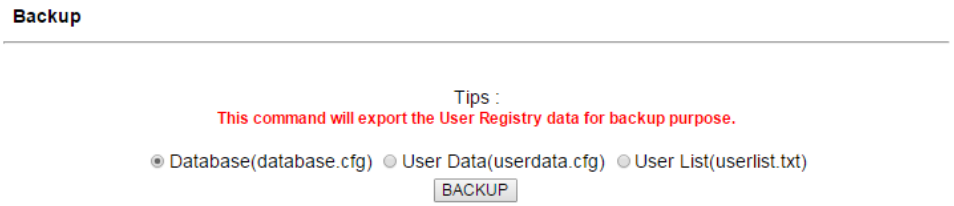
IV.1. Cài đặt Camera IP (IP Camera)



Hình 34

- IP Camera: nhập vào IP camera IP (Surveon) tương ứng với các cửa
- Set: Lưu thiết lập.
- Refress: làm mới trình duyệt.

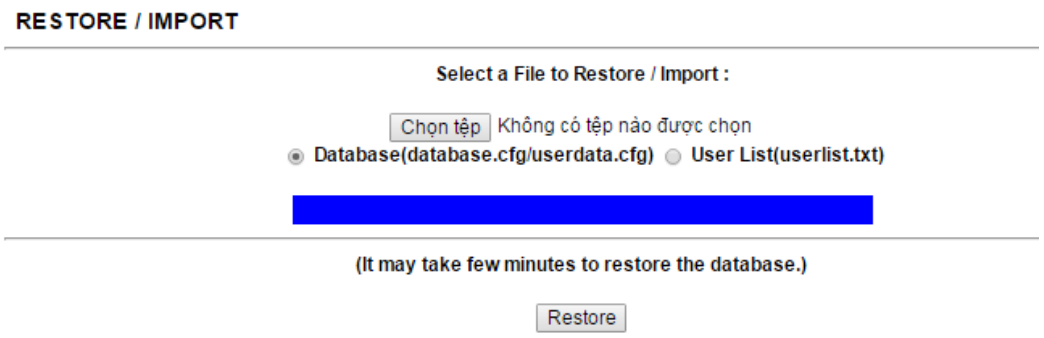
IV.2. Sao lưu dữ liệu (Bakup)



Hình 34

Chọn các mục một cách lần lượt → [Backup] và chọn nơi lưu trữ để sao lưu dữ liệu

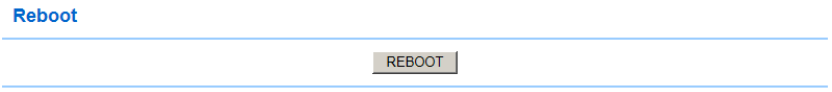
IV.3. Khôi phục dữ kiệu (Restore)



Hình 35

- [Browse]: chọn file đã backup trước đó (Database hoặc User)
- [Restore]: nhấn chọn để bắt đầu quá trình khôi phục dữ liệu.

IV.4. Khởi động lại thiết bị (Reboot)



Hình 36

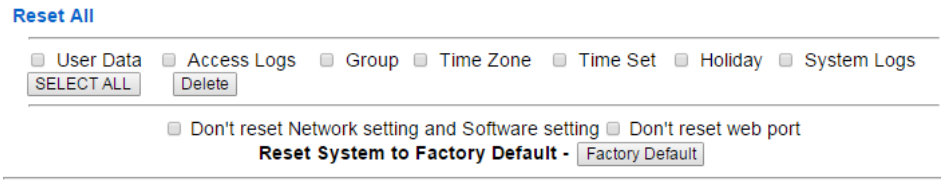
- Nhấn [Reboot] để khởi động lại thiết bị.

IV.5. Upgrade Firmware

Hình 37

Cập nhật Firmware mới nhất cho thiết bị.

IV.6. Reset thiết bị về mặc định (Reset)



Hình 38

- Reset: lựa chọn các mục (User Data, Access Logs,…) rồi chọn Delete để xóa các dữ liệu cần xóa.
- Reset System to Factory defaut: khởi tạo thiết bị về mặc định của nhà sản xuất.

IV.7. Làm mới webpass (Refresh)

Nhấn vào [Refress] để làm mới trình duyệt

IV.8. Thoát khỏi thiết bị (Logout)

Nhấn vào [Logout] để thoát khỏi thiết bị

IV.9. **Thay đổi giao diện sử dụng (Home Mode / Advance Mode)**