EFC302 / EFC304 / EFC306 / EFC308

NAV IP Access Controller

User's Manual

EverFocus

Release Date: February, 2017

EVERFOCUS ELECTRONICS CORPORATION

EFC302

EFC304

EFC306

EFC308

User Manual

www.everfocus.com.tw

Contents

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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

Chapter

1

1. Introduction

The NAV IP access controller is a powerful Linux-based controller with modular design. You can add up to 4 door modules to the NAV controller for expanding the control scale of up to 8 doors / readers. Or you can add one alarm module to the NAV controller to manage up to 10 alarm inputs and 18 alarm outputs.

Moreover, each NAV controller can connect up to 31 EverFocus' Flex series controllers to expand the control scale of up to 256 doors / readers. You can connect to the NAV controller via network to remotely review, monitor all the events on NAV and Flex controllers and configure all 31 Flex series controllers from the same built-in browser-based management software. Furthermore, you can optionally install multiple NAV controllers for a larger scale access control system. By doing so, you will need the enterprise level Navigation software installed as a central server to manage the large access control system.

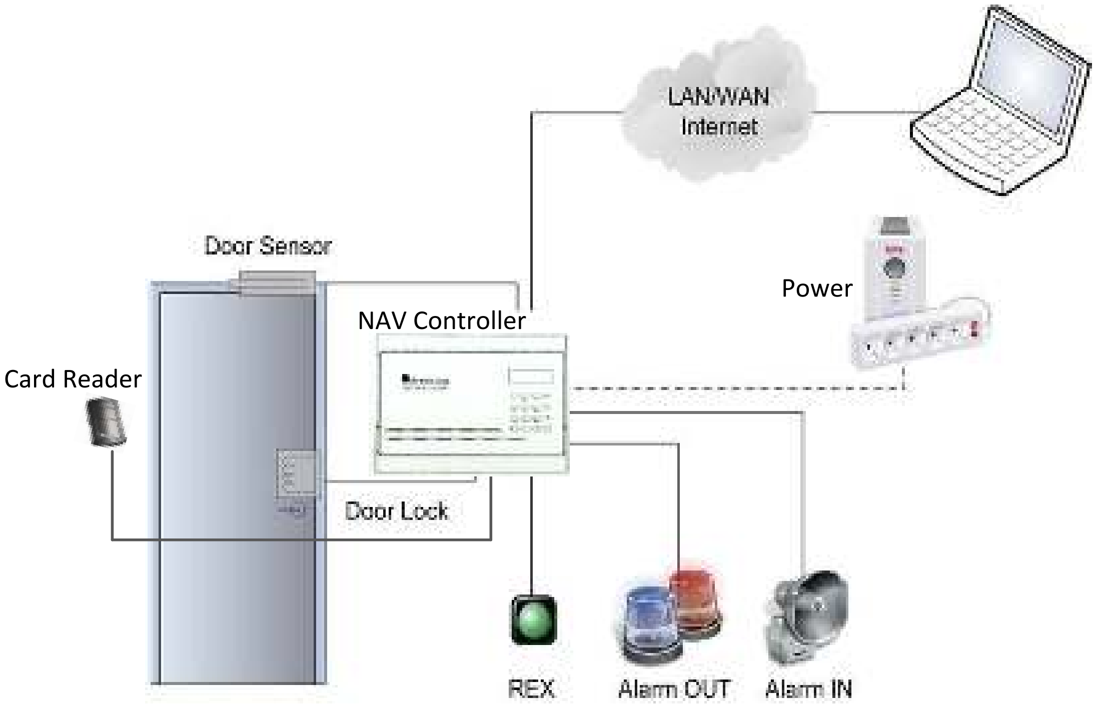


Figure 1-1

The following table lists the models of NAV IP access controllers along with the supported number of doors, readers and alarm inputs / outputs. A description for the supported modules and devices is also provided below.

NAV IP Access Controllers	
Model Name	**Description**
EFC302	• Supports 2 doors, 2 readers • Supports 2 alarm inputs, 4 alarm outputs
EFC304	• Supports 4 doors, 4 readers • Supports 4 alarm inputs, 6 alarm outputs
EFC306	• Supports 6 doors, 6 readers • Supports 6 alarm inputs, 8 alarm outputs
EFC308	• Supports 8 doors, 8 readers • Supports 8 alarm inputs, 10 alarm outputs

Optional Devices / Modules	
Name	**Description**
Door Module	Each NAV controller can add up to 4 door modules. Each door module controls up to 2 readers, 2 relays for door locks, 2 relays for alarm outputs, other door control peripherals, and event signals to the main
Alarm Module	Each NAV controller can add only one alarm module. The alarm module can connect up to 8 alarm inputs and 8 alarm outputs.
Flex Series Controller	Each NAV controller can connect up to 31 Flex series controllers. Each Flex series can connect up to 8 doors and 8 readers.

1.1 Features

- Embedded Linux operating system
- Built-in database engine
- Built-in 512M large-capacity memory
- Modular design for easy expansion of the system, and auto-detection on expansion modules
- Manage up to 31 EverFocus' Flex Series controllers
- Secure access through the Web browser is guaranteed by SSL (Secure Socket Layer)
- Network automatic backup and upgrade
- USB2.0 automatic backup and controller firmware upgrade
- Remote setting, control and management; no software needed to be installed
- Manage up to 100,000 cards and 1,000,000 event records
- Supports 2,048 management groups
- Supports 2,048 access schedule
- Supports 12 kinds of access pattern
- Supports card / group mode to access the door

- Supports 4 x 4 lock level, achieves 4 teams x 4 multi cards access setting on each door
- Each door supports 10 different independent day setting (Sunday to Monday, and 3 kinds of custom day setting). Each day can take 10 time zones with minimum 1 minute duration
- Supports comprehensive access features including interlock, area-based anti passback, multi-card / multi-level access control, panic open, remote door control, system arm / disarm, multiple door verification mode, and first card, etc.
- Multiple languages support: English, Chinese and Russian

1.2 Overview

The diagram below illustrates the controller along with its main components and functions.

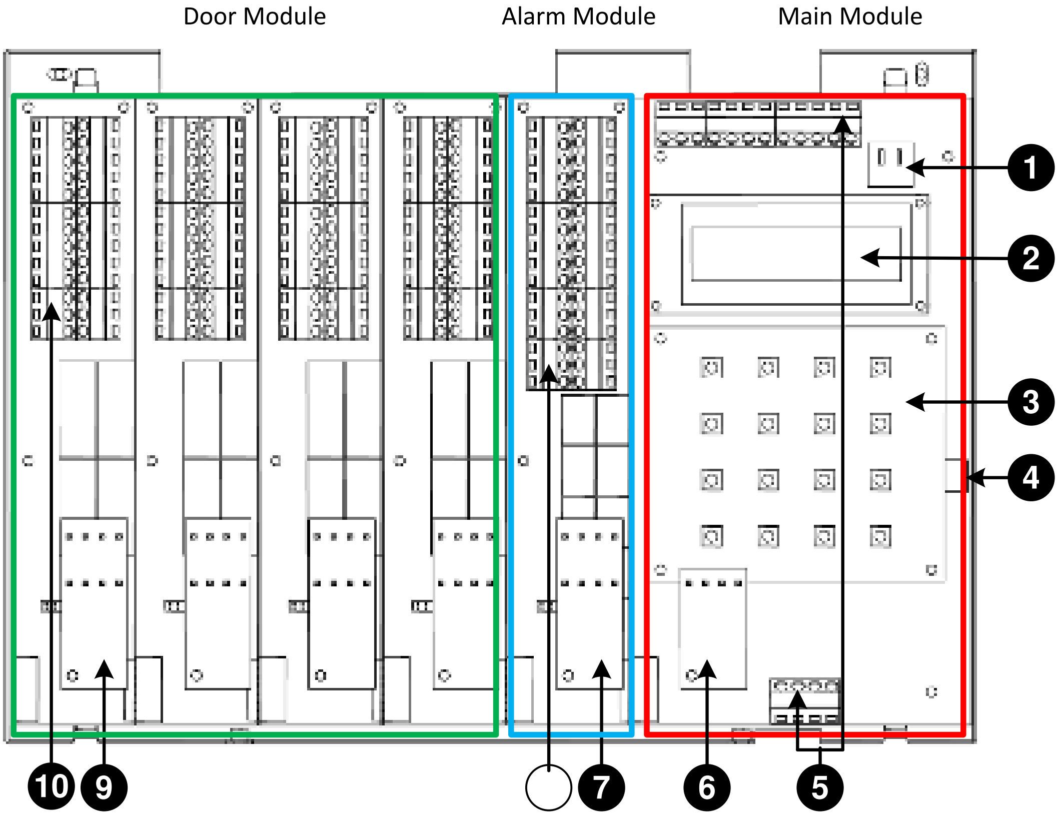


Figure 1-2

Main Module

The main module controls the fundamental functions of the controller, including the built-in browser-based software, the system management, the power supply, event records, built-in Ethernet port, and communication via RS-485 port, two alarm inputs and two alarm outputs. The main module also controls the door modules and alarm module.

No.	Name	Description
1	Network Port	Connects to the network.
2	LCD Screen	Displays the current status of the controller and the menu.
3	Keypad	Provides an interface to operate the controller.
4	USB2.0 Port	For database backup / restore and firmware upgrade.
5	Terminal Block	Connects to power, alarm input / output devices, etc. Please refer to *1.6.1 Terminal Block and LEDs on Main Module.*
6	LEDs	Indicates the controller status. Please refer to *1.6.1 Terminal Block and LEDs on Main Module.*

Alarm Module

The alarm module is used to extend the controller's alarm function, adding up to 8 alarm inputs and 8 alarm outputs. Each controller can only add one alarm module.

No.	Name	Description
7	LEDs	Indicates the alarm status. Please refer to *1.6.2 Terminal Block and LEDs on Alarm Module.*
8	Terminal Block	Connects to alarm input / output devices. Please refer to *1.6.2 Terminal Block and LEDs on Alarm Module.*

Door Module

The door module is used to control up to 2 readers, 2 relays for door locks, 2 relays for alarm outputs, other door control peripherals, and event signals to the main module. Each controller can add up to 4 door modules.

No.	Name	Description
9	LEDs	Indicates the door module status. Please refer to *1.6.3 Terminal Block and LEDs on Door Module.*
10	Terminal Block	Connects to door sensors, door locks, request-to-exit devices and alarm outputs. Please refer to *1.6.3 Terminal Block and LEDs on Door Module.*

1.3 Specification

System	
Operating System	Linux embedded
Database	Built-in
Memory	512M
Management Software	Built-in browser-based software, EFS2000, ENS2000
Built-in Software	Supports system management, device configuration, live event list view and map view, CCTV integration
Operation	
Maximum Card Amount	100,000
Maximum Even Records	1,000,000
Supporting Readers	2 (expandable up to 8)
Supporting Door Control	2 (expandable up to 8)
Max. Flex Controllers Connected via RS-485	Up to 31 controllers
Reader Communication Format	Wiegand26 / RS-232
Card / System PIN	8 digits
Alarm PIN	8 digits
Alarm Input	2 (expandable to 10, each alarm input can be set as firmware alarm or regular alarm.)
Alarm Output	2 alarm outputs on main module, 2 alarm outputs on each door module and 8 alarm outputs on alarm
Network Interface	100M adaptive Ethernet interface
Baud Rate	9600 bps
Programmable Duration	Maximum 10 per day with minimum duration of 1 min.
Programmable Date	Sunday to Saturday and 3 customized date types on each individual door.
Access Group	2,048
Access Schedule	2,048
Door Access Verification	12 modes
Other Functions Support	Supports multiple doors interlock, card expiration, anti-passback, backup battery connection, backup battery charger, real-time clock and 4 x 4 lock level (achieves 4 teams x 4 multi cards access setting on
Mechanical	
LCD Display Screen	2 × 9(for Chinese / Russian characters), 2 x 18(for English characters)
Buzzer	Built-in
Keypad	4 x 4 key

General	
Current for Door Control Relay	5A (Max.)
Current for Alarm Relay	2A (Max.)
Power Supply	DC11V ~ 16V (DC 15V when backup battery is
Maximum Current	2A
Dimension (L x W x H)	300 × 216 × 33 mm / 11.8 x 8.5 x 1.3 in
Temperature	14°F~122°F
Humidity	<90%
Weight	1.2 kg / 2.65 lbs

1.4 Packing List

Please check that there is no missing item in the package before installing.

- NAV Controller x 1 (EFC302)
- Supporting Frames (left and right) x 2
- Mounting Template x 1
- 3 x 6 mm screw x 2 (for mounting the controller to the frame)
- User's Manual x 1

Note: Contact the shipper if any items appear to have been damaged in the shipping process. If any items are missing, notify your EverFocus Electronics Corp. Sales Representative or Customer Service Branch. Please also keep the shipping carton for possible future use.

1.5 Optional Device

Optional device can expand your controller's capabilities and versatility. Please contact your dealer for more information.

- EverFocus mental enclosure (EPN-871-B)
- EverFocus USB reader (ERU871)
- EverFocus proximity readers (ERR-871, ERK-871, ERM-871)

1.6 Definitions of Terminal Block and LEDs

1.6.1 Terminal Block and LEDs on Main Module

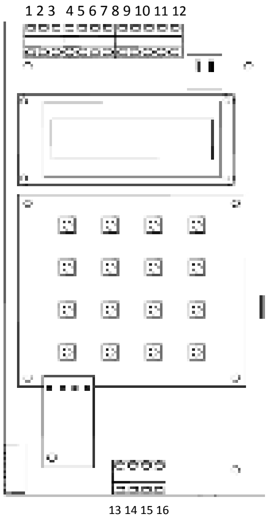


Figure 1-3

Terminal Block Definitions

No	Terminal Name	Function	No.	Terminal Name	Function
1	Alarm In 0	General alarm input 0	10	RS485_A	Signal A of RS-485 bus
2	GND	Alarm input GND	11	COMM_GND	GND of RS-485
3	FireIn	Fire alarm input	12	RS485_B	Signal B of RS-485 bus
4	AUXAlarmOutNo	Normally open pin of auxiliary alarm output	13	Power	Power input
5	AUXAlarmOutCom	Common pin of auxiliary alarm output	14	GND	Power GND
6	AUXAlarmOutNC	Normally close pin of auxiliary alarm output	15	BATT+	Battery positive pin
7	AUXAlarmOutNo	Normally open pin of main alarm output	16	BATT-	Battery negative pin
8	AUXAlarmOutCom	Common pin of main alarm output	17	USB	USB port
9	AUXAlarmOutNC	Normally close pin of main alarm output	18	Ethernet	Ethernet port

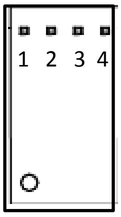


Figure 1-4

LED Definitions

No	Description	No	Description
1	The power is on when the light is on.	3	The data is received when the light is on.
2	The fire alarm is triggered when the light is on.	4	The data is transmitted when the light is on.

1.6.2 Terminal Block and LEDs on Alarm Module

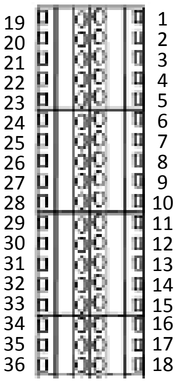


Figure 1-5

No	Terminal Name	Function	No.	Terminal Name	Function
1	Alarm1_In	Alarm signal input 1	19	Alarm5_In	Alarm signal input 5
2	GND	GND	20	GND	GND
3	Alarm2_In	Alarm signal input 2	21	Alarm6_In	Alarm signal input 6
4	Alarm3_In	Alarm signal input 3	22	Alarm7_In	Alarm signal input 7
5	GND	GND	23	GND	GND
6	Alarm4_In	Alarm signal input 4	24	Alarm8_In	Alarm signal input 8
7	Alarm1_NO	Alarm 1 output for NO	25	Alarm5_NO	Alarm 5 output for NO
8	Alarm1_COM	Alarm 1 output in common	26	Alarm5_COM	Alarm 5 output in common
9	Alarm1_NC	Alarm 1 output for NC	27	Alarm5_NC	Alarm 5 output for normally-close
10	Alarm2_ NO	Alarm 2 output for NO	28	Alarm6_ NO	Alarm 6 output for NO
11	Alarm2_ COM	Alarm 2 output in common	29	Alarm6_ COM	Alarm 6 output in common
12	Alarm2_ NC	Alarm 2 output for NC	30	Alarm6_ NC	Alarm 6 output for NC
13	Alarm3_ NO	Alarm 3 output for NO	31	Alarm7_ NO	Alarm 7 output for NO
14	Alarm3_ COM	Alarm 3 output in common	32	Alarm7_ COM	Alarm 7 output in common
15	Alarm3_ NC	Alarm 3 output for NC	33	Alarm7_ NC	Alarm 7 output for NC
16	Alarm4_ NO	Alarm 4 output for NO	34	Alarm8_ NO	Alarm 8 output for NO

17	Alarm4_ COM	Alarm 4 output in common	35	Alarm8_ COM	Alarm 8 output in common
18	Alarm4_ NC	Alarm 4 output for NC	36	Alarm8_ NC	Alarm 8 output for NC

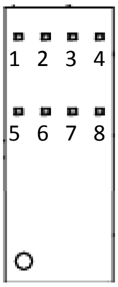


Figure 1-6

LED Definitions

No	Description	No	Description
1	Alarm 1	5	Alarm 5
2	Alarm 2	6	Alarm 6
3	Alarm 3	7	Alarm 7
4	Alarm 4	8	Alarm 8

1.6.3 Terminal Block and LEDs on Door Module

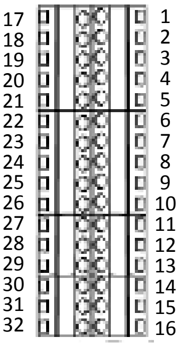


Figure 1-7

No	Terminal Name	Function	No.	Terminal Name	Function
1	Reader1_Data0	Reader 1 Wiegand Data 0	17	Reader2_Data0	Reader 2 Wiegand Data 0
2	Reader1_Data1	Reader 1 Wiegand Data 1	18	Reader2_Data1	Reader 2 Wiegand Data 1
3	Reader1_DC	Power supply for reader 1	19	Reader2_DC	Power supply for Reader
4	Reader1_GND	GND for the Reader 1	20	Reader2_GND	GND for the Reader 2
5	Reader1_Ctrl	Control line for reader 1	21	Reader2_Ctrl	Control line for Reader 2
6	RX_1	Port to TX signal to reader 1	22	RX_2	Port to TX signal to Reader 2
7	TX_1	Port to RX signal from reader 1	23	TX_2	Port to RX signal from Rader 2

8	Door1_ Button	The request-to-exit button for Door 1	24	Door2_ Button	The request-to-exit button for Door 2
9	Door1_GND	GND for terminal 8 & 10	25	Door2_GND	GND for terminal 24 & 26
10	Door1_ Sensor	Door sensor input for Door 1	26	Door2_ Sensor	Door sensor input for Door 2
11	Door1_NO	Normally open pin for door control relay 1	27	Door2_NO	Normally open pin for door control relay 2
12	Door1_COM	Common pin for door control relay 1	28	Door2_COM	Common pin for door control relay 2
13	Door1_NC	Normally close pin for door control relay 1	29	Door2_NC	Normally close pin for door control relay 2
14	Alarm1_NO	Normally open pin for alarm output relay 1	30	Alarm2_NO	Normally open pin for alarm output relay 2
15	Alarm1_COM	Common pin for alarm output relay 1	31	Alarm2_COM	Common pin for alarm output relay 2
16	Alarm1_NC	Normally close pin for alarm output relay 1	32	Alarm2_NC	Normally close pin for alarm output relay 2

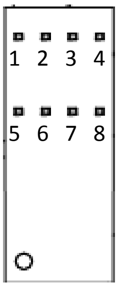


Figure 1-8

LED Definitions

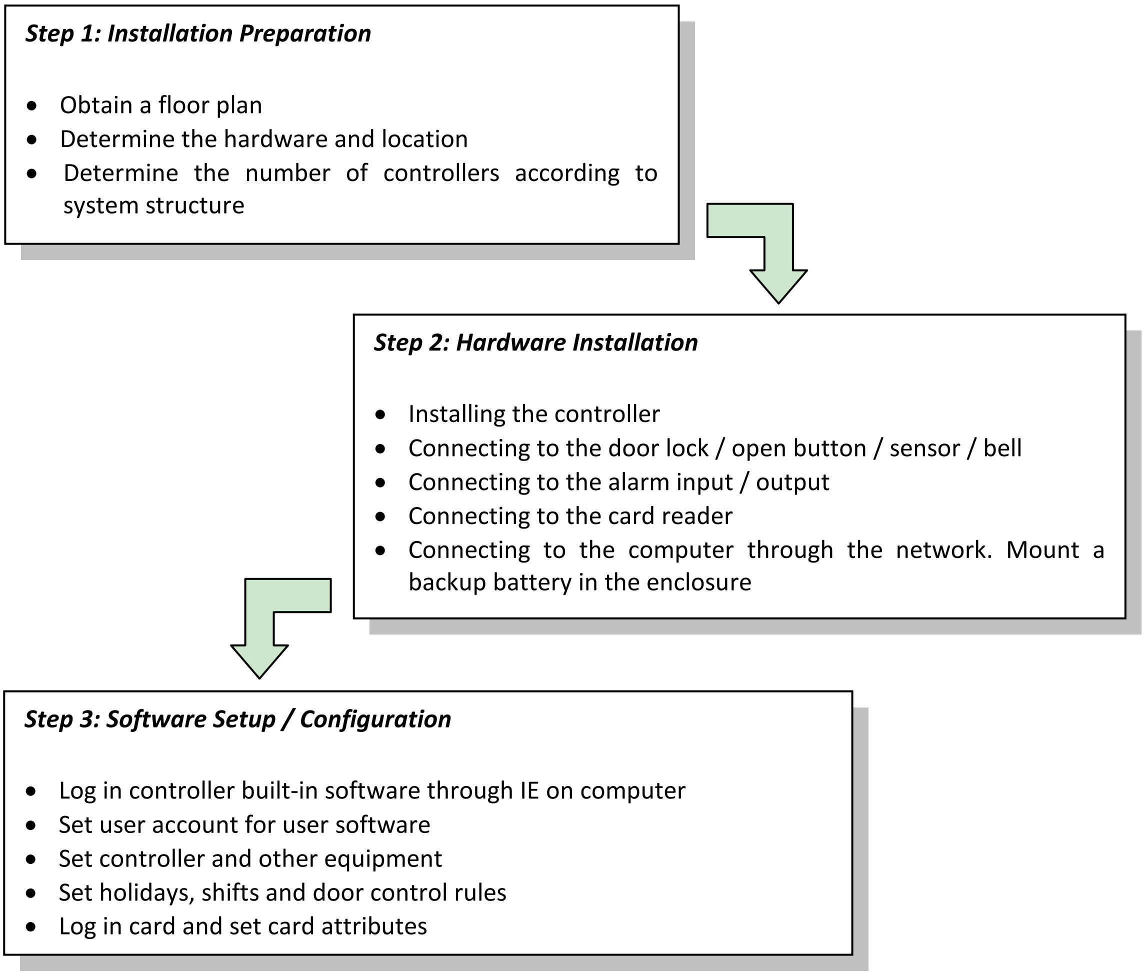
No	Description	No	Description
1	Indicates the alarm relay #2 is energized.	5	Indicates the alarm relay #1 is energized.
2	Indicates the reader #2 is connected.	6	Indicates the reader #1 is connected.
3	Indicates the door sensor #2 is off (the door’s open).	7	Indicates the door sensor #1 is off (the door’s open).
4	Indicates the door control relay #2 is energized.	8	Indicates the door control relay #1 is energized.

Chapter

2

2. Installation

The Installation has three procedures described as below. Each procedure will be introduced in the following sections in detail.



Step 1: Installation Preparation

- Obtain a floor plan
- Determine the hardware and location
- Determine the number of controllers according to system structure

Step 2: Hardware Installation

- Installing the controller
- Connecting to the door lock / open button / sensor / bell
- Connecting to the alarm input / output
- Connecting to the card reader
- Connecting to the computer through the network. Mount a backup battery in the enclosure

Step 3: Software Setup / Configuration

- Log in controller built-in software through IE on computer
- Set user account for user software
- Set controller and other equipment
- Set holidays, shifts and door control rules
- Log in card and set card attributes

2.1 Installation Preparation

Before installation, users are advised to collect information properly which will make the installation more smoothly and helps to reduce time and energy cost. For professional constructors, the information below will be of great use.

2.1.1 Obtain a Floor Plan

Obtain a floor plan of the building in which the access control system is to be installed. Obtaining a floor plan helps the installer determine what components need to be installed, and where. It also is essential in determining the length of cable needed to connect readers to the controller. A floor plan can be a blue print of the building, a design, or simply a drawing of the facility. Any document showing the footprint of the building can be used. The dimensions are important to note, especially when determining cable lengths. A floor plan may be obtained from your local city hall.

2.1.2 Determine the Hardware and Location

Determine which hardware to use and where it will be installed. This is the most crucial step in the preparation stage. First, determine how many access points, or doors, need to be managed by the access control system. These access points will control the security of the facility, and can limit the entry and exit to and from any given area of the building. After deciding which doors need to be controlled, the user must also determine the level of security needed at each door. There are many ways to manage each door, using different resources. These resources include, but are not limited to: proximity readers, mag strip readers, relays, and request to exits. A few common door configurations are described below:

- **One Set of NAV Controller+ One Reader – The Basic Door Entry Control**

The most basic configuration involves one NAV controller, a reader and an electric strike. In this configuration, a person presents a card to the reader, and is either granted or denied access. The electric strike unlocks if the system grants access. Another variation of this scenario involves setting the system up to monitor whether the door is open, which allows the system to protect against propped open doors, or doors being held open for too long.

- **One Set of NAV Controller+ One Reader + One Door Open Button – Control of Exit**

Adding a door open button to the above scenario allows the system to control when to allow people to exit through a door. The door open button equipment includes a button which has to be pressed when a card holder exits, or a door sensor. The equipment should be arranged on the secure side of the door.

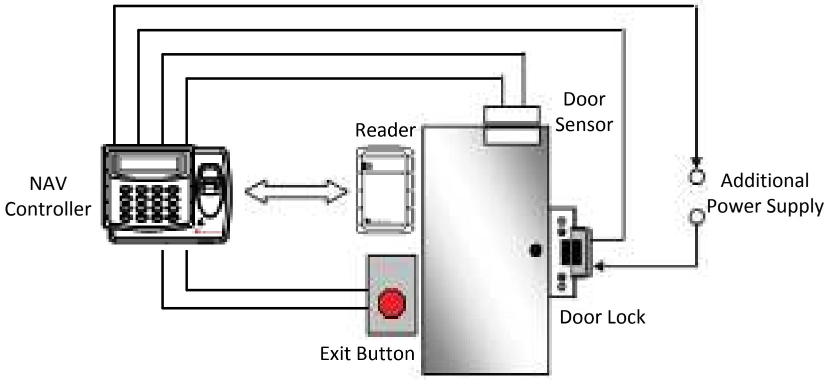


Figure 2-1

- **One Set of NAV Controller+ Two Readers – Control of both Entry and Exit**

When the security grade is relatively high or the administrator requires the card holders to get in or out at fixed time or date through specific door, two sets of EFC301 are needed. Additional installation of one set of EFC301 on the side of the door requires the card holders to swipe the card when exiting and entering. This rule has more reliable security regarding who can enter and who can exit and the administrator canal so master the entry and exit time of card holders.

2.1.3 Determine the Number of Controllers/ Modules According to System Structure

Determine how many controllers / modules and network interface are required.

1. Each NAV controller can accommodate up to 8 readers. If the system to be installed requires more than 8 readers, additional controllers are necessary. E.g. Flex series controllers.
2. If one or more controllers are installed at a different location, then the system computer is to be installed, and an Ethernet interface is required to connect over the internet. An Ethernet interface may also be used in locations at which the controllers are installed a long distance away from the system computer. Software is required to manage these NAV controllers.

2.2 Hardware Installation

After the preparation work is finished, user can start installation. This chapter mainly introduces how to install the hardware part, which is divided into six steps:

1. Mounting the enclosure (optional) and controller.
2. Installing and connecting the readers.
3. Connecting to door lock, sensor and open button.
4. Connecting to the alarm input / output.
5. Connecting to the computer.
6. Mounting a backup battery in the enclosure (optional).

2.2.1 Mounting the Enclosure (Optional) and Controller

The NAV controller should be installed in an easily-accessible position. However, it should be noticed that the controller is the core part of the entire system and can be used to change database. After the installation site is selected, a relative secure clean position in which the administrator is easy to operate should be selected.

Due to the controller is an essential part of the access control system. It is recommended to mount the NAV controller in a metal enclosure (EPN-871-B). If you are using the enclosure, additional AC power supply is required. The enclosure uses a 24V AC power supply with a built-in 15V DC converter.

If the system requires additional door or alarm modules, install them in the controller before mounting the controller in the enclosure or on the wall.

Note: If the screw holes of the controller do not line up properly with the enclosure, some filling may be required for adjustment.

1. Use the supplied mounting template to position the holes for the support frames and then mount the two support frames on a wall.

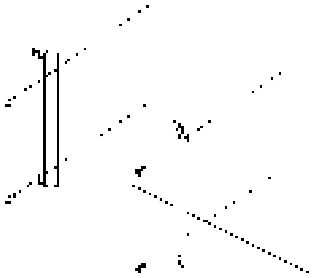


Figure 2-2

Note: If using the metal enclosure, use the four pre-drilled holes on the back wall of the enclosure and then mount the two support frames on the interior of the enclosure.

2. Mount the controller base board to the support frames.

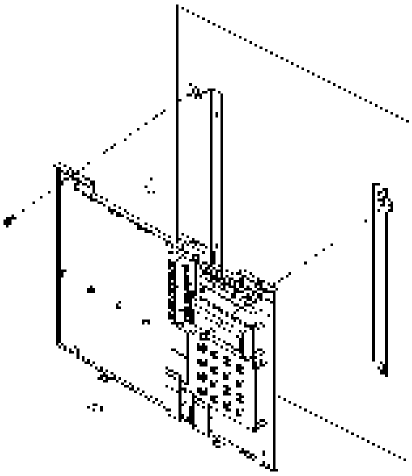


Figure 2-3

  a. Place the controller base board on the support frames. Line up the four latches on the support frames with the holes on the controller base board. Once lined up, slide the controller base board down to secure it in place.
  b. Secure the controller base board to the support frames using the supplied two screws.

3. Install and mount additional door modules or the alarm module.

Note: The controller can hook up to 4 door modules and only 1 alarm module. Each door module is cascaded to its left side module till the main module. The door modules and the alarm module can be placed in any sequence.

a. Connect the pins on the lower right corner of the new module to the connector on the bottom left corner of the installed module. Make sure that the pins fit snugly into the receiving module.

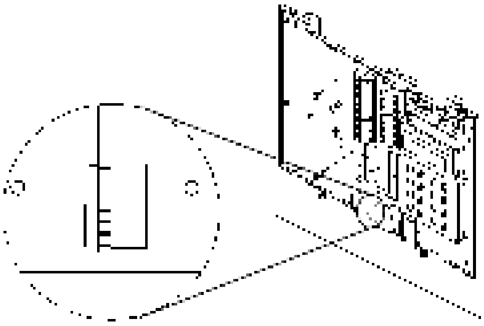


Figure 2-4

b. Secure the module to the controller base board using the three screws provided in the module package.

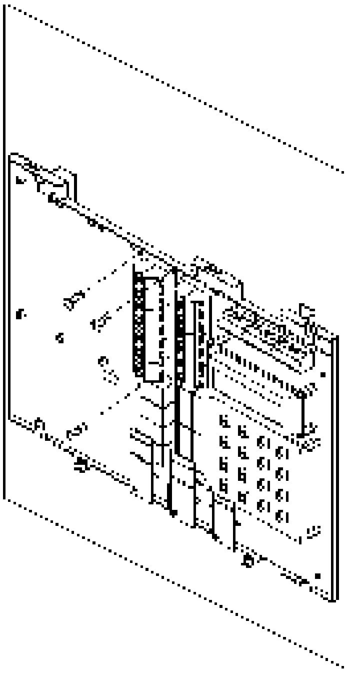


Figure 2-5

The Reader / Door Index Conversion

The index conversion of readers is displayed as below. The readers / doors are counted 1 to 8 from right to left.

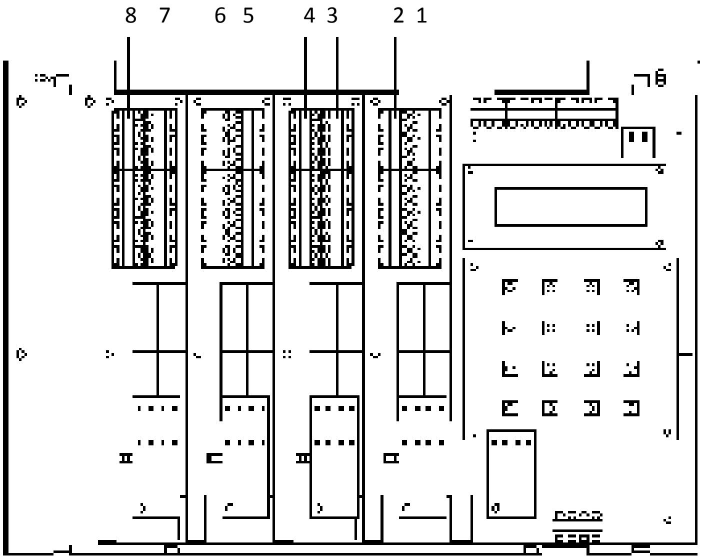


Figure 2-6

4. Placing back the cover of controller.

   a. The cover has two latches on the interior of the top horizontal edge. Place these latches in the corresponding holes on the top horizontal edge of the controller base board.

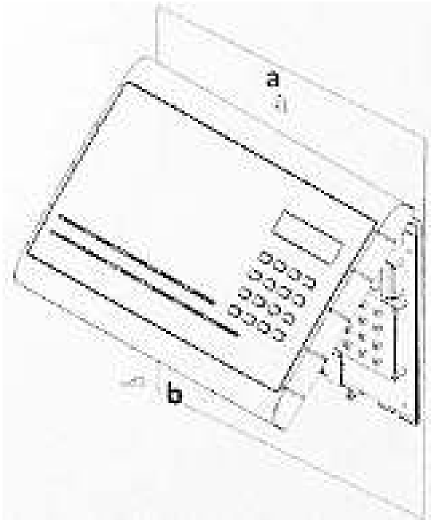


Figure 2-7

   b. Once the latches are in place, the bottom portion of the cover will fit easily over the rest of the controller base board.

   c. Secure the cover to the controller base board along the exterior of the horizontal bottom edge.

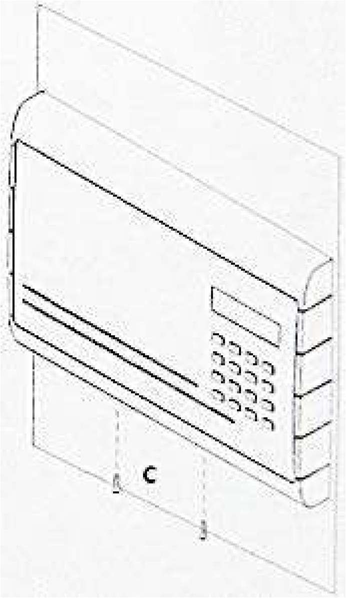


Figure 2-8

2.2.2 Installing and Connecting the Readers

The readers must be mounted near each door and connected directly to the door module(s) in the controller. Each door module can control up to two readers. The supported reader formats are Wiegand and RS-232.

RS-232 Connection

Connect the RS-232 wires from the reader to the terminal block on the door module. You can either connect the wires from the reader to **Pin 3 ~ 7** (Door 1) or **Pin 19 ~ 23** (Door 2) on the terminal block.

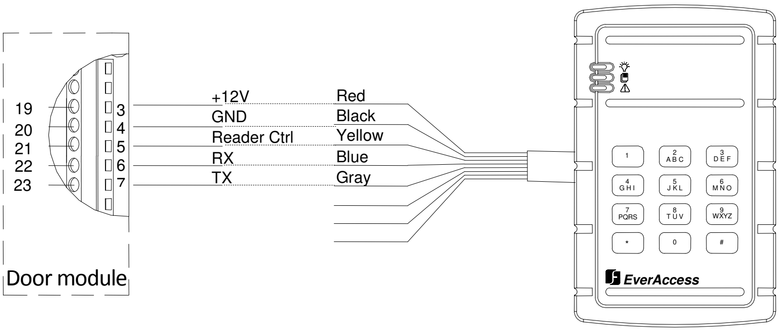


Figure 2-7

Wiegand Connection

Connect the Wiegand wires from the reader to the terminal block on the door module. You can either connect the wires from the reader to **Pin 1 ~ 5** (Door 1) or **Pin 17 ~ 21** (Door 2) on the terminal block.

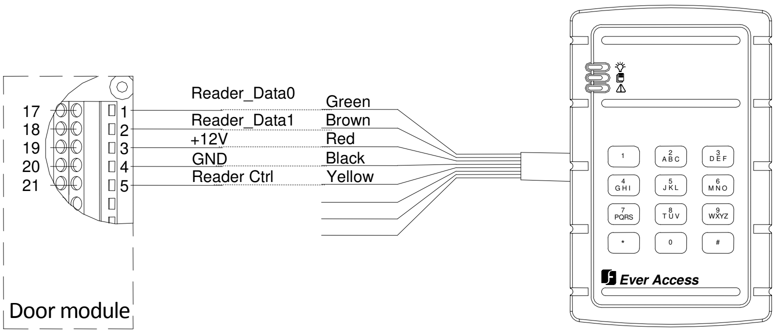


Figure 2-8

Each door module can provide +12V voltage for two readers. Twisted cable is recommended to connect the controller and readers. The maximum transmission distance between the reader and controller depends on the gauge of the cable and the specification of the reader. Please read the reader user manual carefully before installing the cable for the readers.

Note: It is strongly recommended to use one connection format in a multi-reader system, i.e. all the readers are connected to the door modules through RS-232 or Wiegand connection. Multiple connection formats could cause compatibility problems to the system.

2.2.3 Connecting to the Door Lock, Sensor and Open Button

Connecting to the Door Lock

The Electric strikes and magnetic locks are used to keep doors locked unless the system grants access or the user sets the doors to remain unlocked. One strike or magnetic lock is required for each door. These locks must be powered separately from the readers. The mounting instructions for strikes and magnetic locks vary depending on the manufacturer and type of lock. Please consult the instructions included with the door hardware when installing. Once the locks are installed, follow the instructions below to connect them to the controller.

- **Electric Strike**

  Connect the wires from the electric strike to the terminal block on the door module. You can either connect the wires to **Pin 11 and 12** (Door 1) or **Pin 27 and 28** (Door 2) on the terminal block.

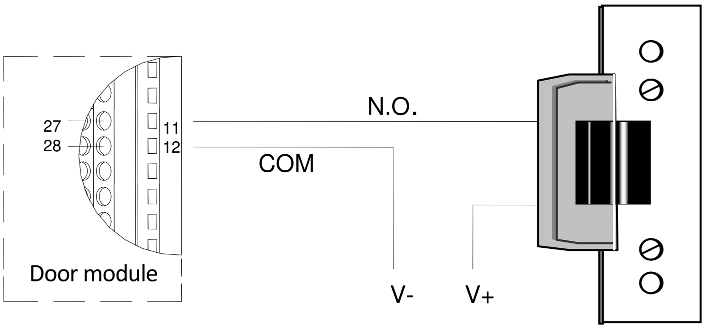


Figure 2-9

- **Magnetic Lock**

  Connect the wires from the magnetic lock to the terminal block on the door module. You can either connect the wires to **Pin 12 and 13** (Door 1) or **Pin 28 and 29** (Door 2) on the terminal block.

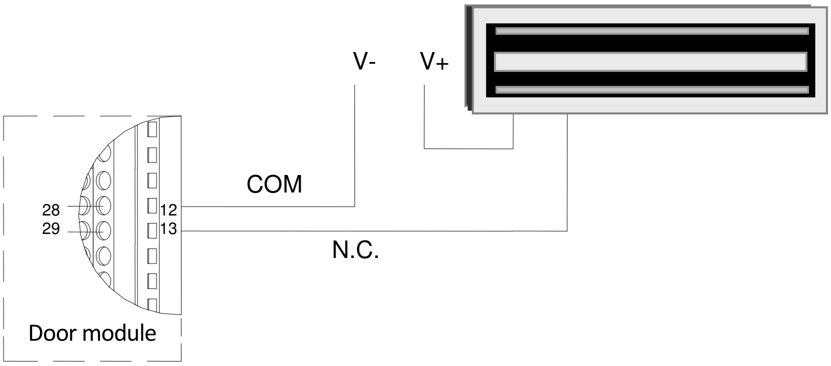


Figure 2-10

Note:

1. The maximum current output of the door lock relay is 5A. If the current of the door lock is over this value, an external power relay will be required.
2. When using a DC power source to power the lock, connect the positive lead to V+. When using an AC power source, the leads are interchangeable.

Connecting to the Door Sensor

Connect the wires from the door sensor to the terminal block on the door module. You can either connect the wires to **Pin 9 and 10** (Door 1) or **Pin 25 and 26** (Door 2) on the terminal block.

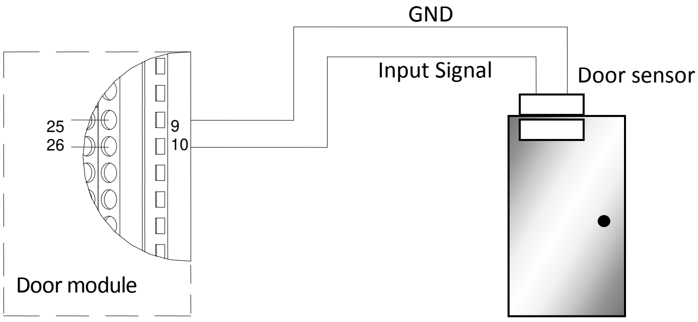


Figure 2-11

Connecting to the Door Open Button

Connect the wires from the door open button to the terminal block on the door module. You can either connect the wires to **Pin 8 and 9** (Door 1) or **Pin 24 and 25** (Door 2) on the terminal block.

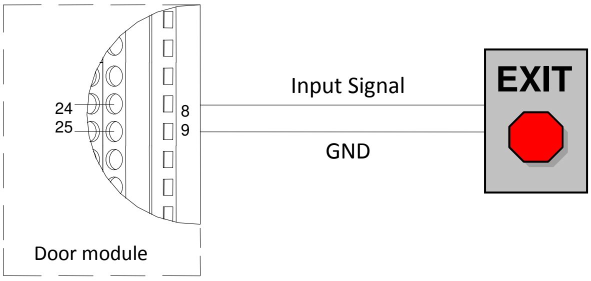


Figure 2-12

2.2.4 Connecting to the Fire Alarm/ Alarm Input

You can either connect the alarm inputs to the main module or the alarm module.

- **On the Main Module**

  The main module provides two general alarm inputs, connecting to **Pin 1** and **2** or **Pin 2** and **3** on the terminal block. The GND terminal is shared by these two input signals. Both inputs can be configured as either fire alarm input or general alarm input.

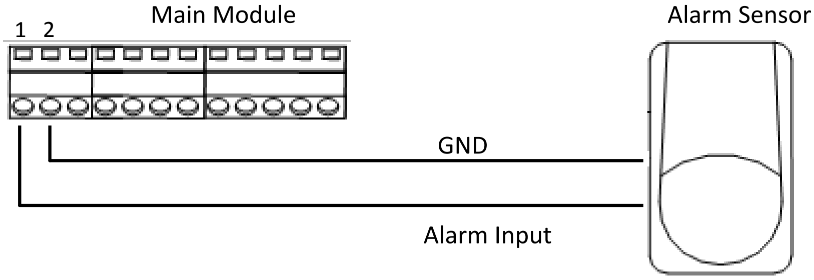


Figure 2-13

- **On the Alarm Module**

  The alarm modules provide 8 alarm inputs. The alarm input pins provided by the alarm module includes Pin 1, 3, 4, 6, 19, 21, 22, 24. For details on pin assignment, please refer to *1.6.2 Terminal Block and LEDs on Alarm Module*. Following is an example on connecting the alarm input to the alarm module.

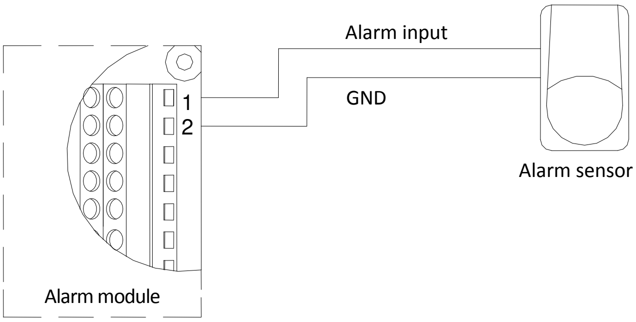


Figure 2-14

2.2.5 Connecting to the Fire Alarm/ Alarm Output

The alarm modules provide 8 alarm outputs. You can assign the corresponding relay status to the different events. There are three terminals: **COM**, **NO** and **NC**. The wiring depends on the alarm device. Please read the user manual of the external alarm devices before wiring. Following are examples on connecting the alarm output to the alarm module. For details on pin assignment, please refer to *1.6.2 Terminal Block and LEDs on Alarm Module*.

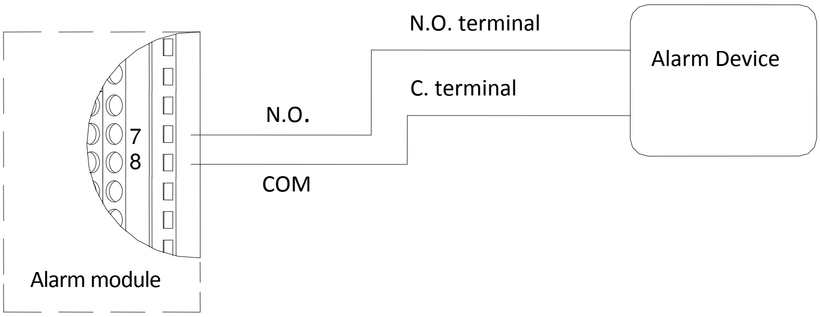


Figure 2-15

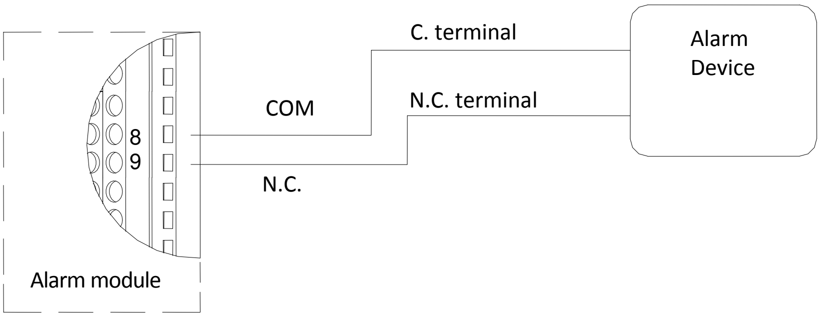


Figure 2-16

2.2.6 Connecting to the Computer through the Network

User can carry out basic setting through the keypad on the EFC301 controller or connection with the computer via TCP/IP. User can carry complicated system administration by accessing the embedded system in the controller through various browsers.

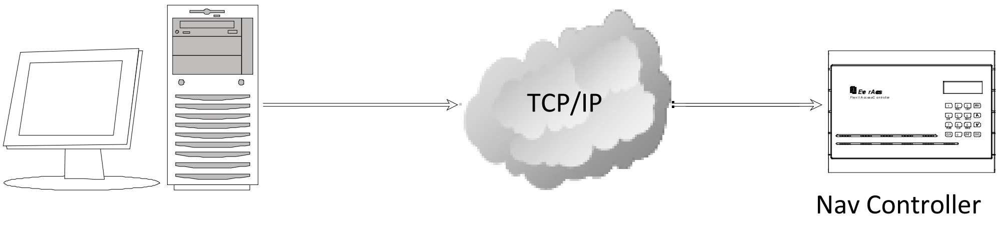


Figure 2-17

2.2.7 Mounting a Backup Battery in the Enclosure (Optional)

You can optionally connect a backup battery in the enclosure to provide backup power to the controller. Once the battery is installed, it will charge off the external power until it is needed, at which time it will automatically be used to power the system.

Connecting to the Backup Battery

Connect the wires from the backup battery to the terminal block on the main module. Connect the positive lead to **Pin 15** and negative lead to **Pin 16** on the terminal block of the main module.

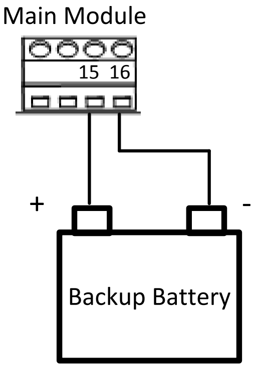


Figure 2-18

If a backup battery is connected, the controller will automatically switch to backup power in the event that the external power is lost. The backup battery will charge while external power is being supplied.

In general, the larger the battery capacity, the longer it can support the controller. A 12AH battery can provide 4 hours of energy for a controller containing 4 door modules, one alarm module and 8 readers.

Chapter

3

3 · System Architecture and Connections

EverAccess® NAV Controller runs the embedded Linux and includes the built-in browser-based management software. No dedicated computer needs to be running to capture and store the events. Users can access and manage the controller or the system from any computer on the network.

This chapter introduces the 3 types of system architectures in order of system scale. Additionally, the RS485 Bus extension is introduced for extending more door controls with EverAccess Flex controllers.

3.1 Small System for 8 Doors

As introduced in chapter 1, NAV Controller provides a flexible, modulated installation up to 8 doors or readers directly. No additional controller or computer needed.

The network settings can be configured directly from the LCD and keypad on the controller. As long as the network settings are correct, users can access it by typing the controller IP address in the browser from a computer on the network. The built-in browser based software will provide the full comprehensive functions to manage and monitor the system.

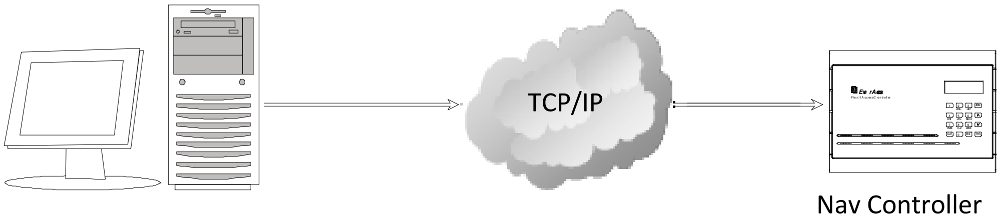


Figure 3-1 Connecting the Controller to a PC

3.2 System for 256 Doors

Each NAV Controller can connect and control up to 31 EverAccess Flex controllers via RS485 bus. Each Flex controller can hook up to 8 doors/readers, so total 256 doors/readers can be controlled under the architecture of one NAV Controller plus 31 Flex controllers.

Users can connect to the NAV Controller via a computer to remotely review, and monitor all the events on NAV and Flex controllers. Users can also all 31 Flex controllers from the browser-based management software.

The system structure is illustrated in the below figure:

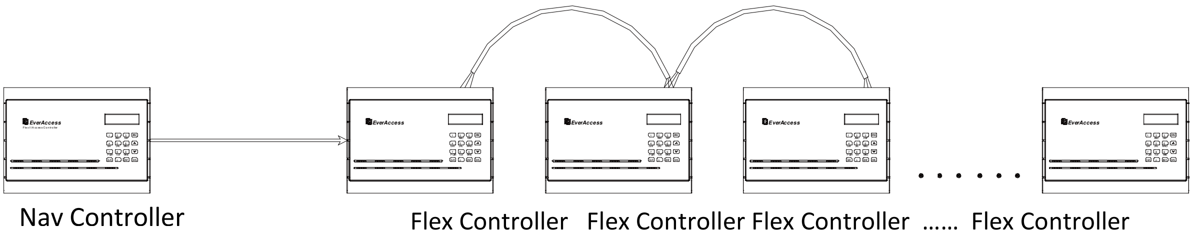


Figure 3-2 System Structure for 256 doors

3.3 System for More theN 256 Doors

Each NAV Controller can control up to 31 Flex controllers. And multiple NAV Controllers can be controlled and communicate with a Navigation software central server. Navigation software is the enterprise level software to manage middle to large scale access control system. Navigation software can be installed as central server mode or node server mode. All NAV Controllers can synchronize data and events to the central server. As a result, a larger scale system can be built with many NAV Controllers (each can control 31 Flex controllers) under the Navigation software. This large scale system is illustrated in the below figure:

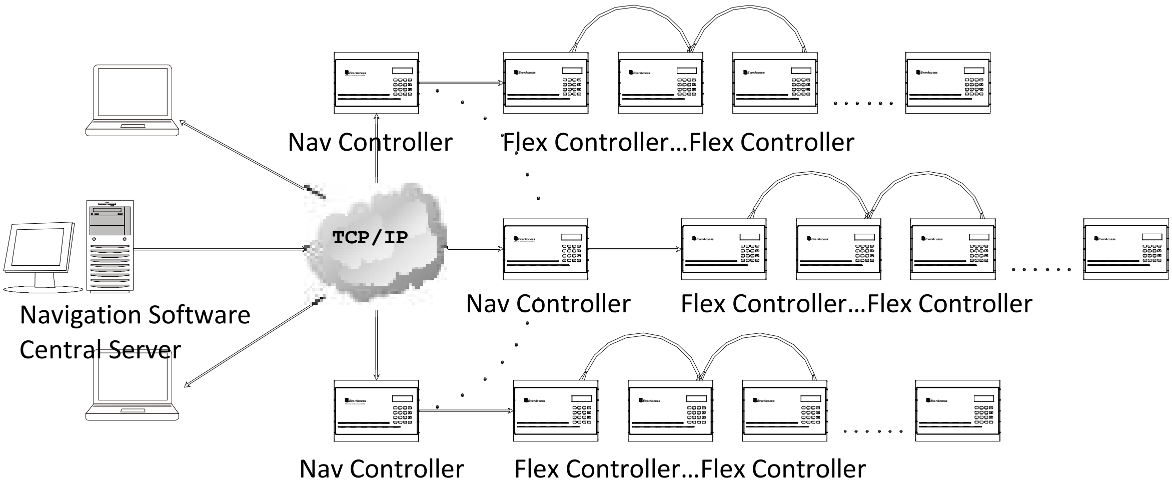

Nav Controller
Flex Controller…Flex Controller
TCP/IP
Nav Controller
Flex Controller…Flex Controller
Navigation Software
Central Server
Nav Controller
Flex Controller…Flex Controller

Figure 3-3 System Structure for more than 256 doors

3.4 RS485 Bus Extension

NAV Controller can connect multiple Flex controllers via RS485 bus. It is shown in the below figure:

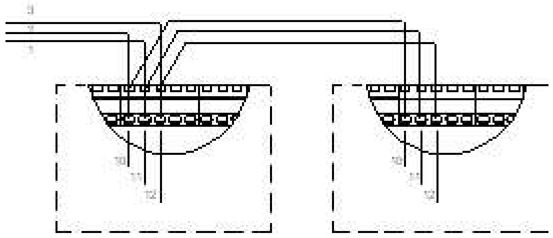


Figure 3-4 Connections to Multiple Controllers via RS485

In order to correctly transfer data, the controllers on the RS485 bus must be connected in a daisy chain format, as shown in Figure 3.5.

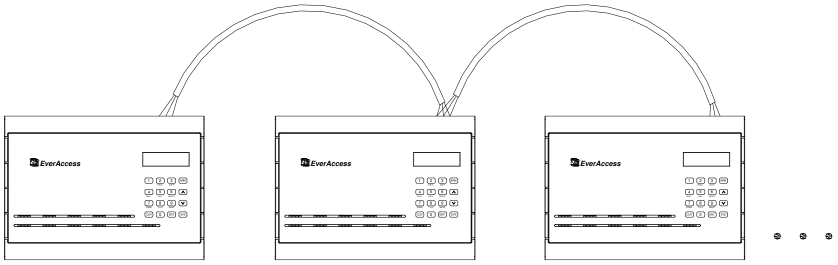


Figure 3-5 The Daisy Chain Connection Controller to Controller

Two common INCORRECT connection methods are displayed in Figure3-6 as well.

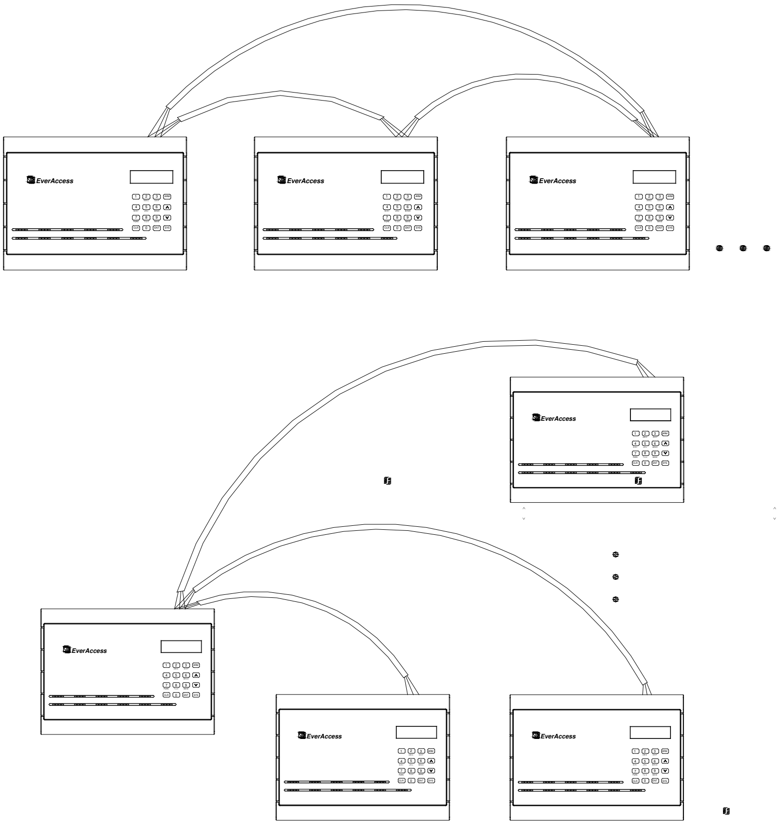


Figure 3-6 Two INCORRECT Connections

Chapter

4

4. Starting Up the Controller

4.1 Connecting to Power

You can power the NAV controller by connecting the power source to Pin 13 and 14 on the terminal block on the main module.

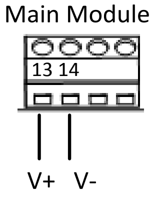


Figure 3-1

The voltage range of the NAV controller is between DC 11V and 16V. The maximum current is 500mA. If the backup battery is connected to the controller, a power supply with DC 15V is required. The power supply in the enclosure is DC 15V. In addition, the controller provides a 12V power supply for the readers. It should be noted that if a controller powers multiple readers, the current draw will be increased. The total current draw can be calculated as below:

Current (controller) **= 500 + Current** (reader) **x Number of Readers**

Important Tips:

1. The voltage supply should be located no more than 2 meters from the controller.
2. The electric locks and alarm devices must be powered separately. The controller's power supply can power the controller with the mounted modules and the readers only, but **not** the locking hardware nor the alarm devices.

4.2 Restoring the Controller

To restore the controller to the factory default settings, switch the power on while holding the **Reset** button on the main module.

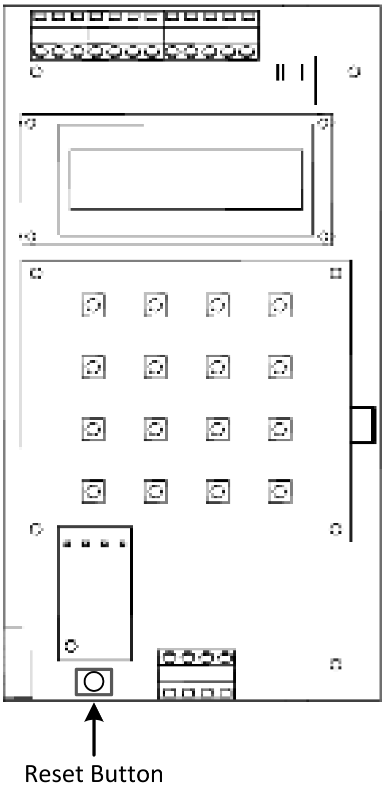


Figure 4-2

4.3 Before First Use

Before first use, please follow the instructions below:

1. Set up the IP address, date and time of the controller.
2. Set up the controller network settings.
3. Configure reader properties.
4. Configure alarm settings.
5. Configure door settings.
6. Configure date types and schedules.

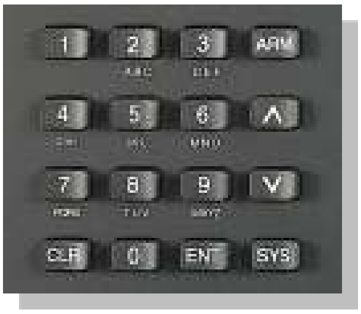
Chapter

5

5． Controller Configuration and Operation

This chapter introduces system functions and their corresponding operations. Most basic operations can be performed on EverAccess® NAV Controller keypad. Some advanced functions require the built-in browser-based management software. Please refer to the later chapters for more details.

5.1 General Operation Guideline



The Controller's 4x4 Keypad is shown above:

Press SYS to enter to the system menu

Press ARM to arm or disarm the system, and reset the alarm

Press ∧ and ∨ to toggle between the same level menu

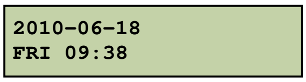
Press ∧ to move the digit input position to left when inputting numbers

Press CLR to cancel or exits back to the higher level menu

Press ENT to confirm the operation

5.2 Home Screen

After the system installation is complete, the controller LCD will display the current date and time. This display is the home screen (also called default screen in this manual), and will be displayed until the user logs in to the system configuration by entering a password.



```
2010-06-18
FRI  09:38
```

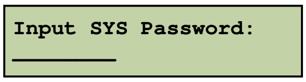
After one minute of inactivity, the controller will automatically log the user out, and back to the home screen.

5.3 Direct Operations from Keypad

This section introduces the functions that can be accessed directly from the keypad on the NAV Controllers.

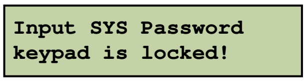
5.3.1 Enter System Configuration

Press SYS on the keypad will bring up a prompt to enter a password, as shown below:



```
Input SYS Password:
______
```

Input the system password and press ENT. If an incorrect password is entered three times successively, the controller will alarm automatically and lock the keypad for one minute, shown as following:



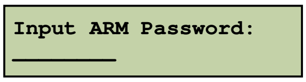
```
Input SYS Password
keypad is locked!
```

The factory default password is 000000. When Logging into the system, pressing the CLR key in each menu level will log the user out.

Note: It is highly recommended to secure the controller, change the default PIN after the first login, and keep the password in a safe place.

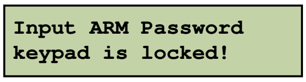
5.3.2 Enter Arm/Disarm Menu

Press ARM button under the default date/time screen, the below screen will pop up to prompt users to input the arm PIN:



```
Input ARM Password:
______
```

After entering the arm PIN, press ENT to confirm and input the ARM menu. The default arm PIN is 00000000. If an incorrect arm PIN is entered three times successively, the system will alarm automatically and lock the keypad for a period of one minute, shown as the below sample window:

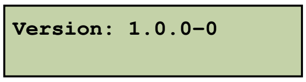


```
Input ARM Password
keypad is locked!
```

Note: It is highly recommended to secure the controller, change the default PIN after the first login, and keep the password in a safe place.

5.3.3 Display Firmware Version

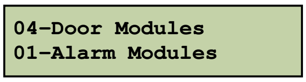
Press 0 to show the version information of the currently installed firmware. An example is shown below:



```
Version: 1.0.0-0
```

5.3.4 Display the Number of Installed Modules

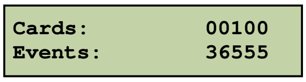
Press 1 to show the number of installed door modules and alarm modules. For example, 4 door modules and 1 alarm module are installed in the controller. The example window is shown below:



```
04-Door Modules
01-Alarm Modules
```

5.3.5 Display the Current Card and Event Number

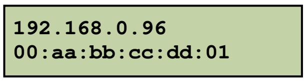
Press 2 to show the number of currently enrolled card and currently stored events. For example, right now the controller stored 100 cards and 36,555 events. The example window is shown below:



```
Cards:         00100
Events:        36555
```

5.3.6 Display the Controller IP Address

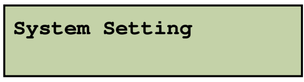
Press 3 to show the IP address, MAC address of the controller. An example window is shown below:



```
192.168.0.96
00:aa:bb:cc:dd:01
```

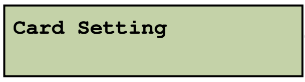
5.4 Level One System Configuration Items

The first level menus are displayed after entering the system menu. Use ∧ and ∨ to toggle between menu options. The first level menu items are shown below:



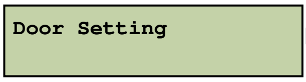
```
System Setting
```

System Setting Menu



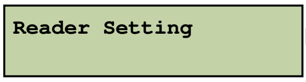
```
Card Setting
```

Card Setting Menu



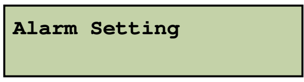
```
Door Setting
```

Door Setting Menu



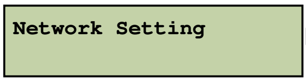
```
Reader Setting
```

Reader Setting Menu



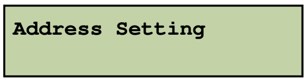
```
Alarm Setting
```

Alarm Setting Menu



```
Network Setting
```

Network Setting Menu


Address Setting

Address Setting Menu

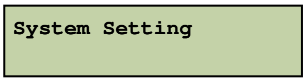
Once the desired item is displayed, press ENT to enter into the corresponding menu. And press CLR in the corresponding menu to return the level one menu.

5.5 System Setting

In the System Setting menu, the user can set basic functions, including date format, system date, time, password, auto daylight saving, system PIN, arm PIN, language, backlight, event erasing and load factory default.

5.5.1 Enter System Setting Menu

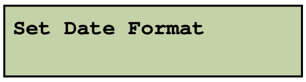
The following window appears after entering the system menu:


System Setting

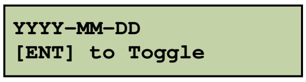
Press ENT to enter System Setting menu. Use ∧ and ∨ to choose from different menu options. All menu options in the System Setting Menu are introduced below.

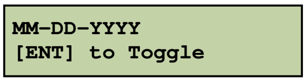
5.5.2 Set Date Format

The user can choose between two date formats: ‘MM-DD-YYYY’ or ‘YYY-MM-DD’. To change this option, use the arrow keys to display “Set Date Format”, and press ENT once the window below is displayed.


Set Date Format

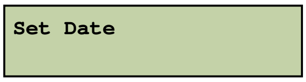
The current date format used will appear. Press ENT to toggle between two formats. Press CLR to exit. The selected format is the one shown on window when exiting.


```
YYYY-MM-DD
[ENT] to Toggle
```

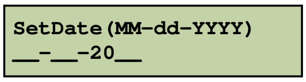

```
MM-DD-YYYY
[ENT] to Toggle
```

5.5.3 Set Date

Press ENT at the window below to set the date.


Set Date

The LCD will display the following menu. Use the numerical keys to input the current date as a six-digit number: (MM-DD-20YY). The year must be in the range 2000-2038. Press ENT to confirm the new date.

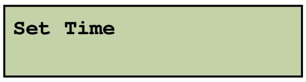


```
SetDate(MM-dd-YYYY)
__-__-20__
```

The date and time can be set either at the controller or from the built-in management software remotely.

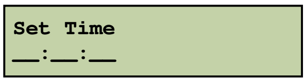
5.5.4 Set Time

Press ENT at the below window to set the time.



```
Set Time
```

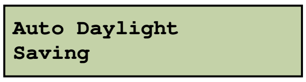
The LCD will display the following menu. Use the numerical keys to input the current time as a six-digit number (HH: MM: SS). The time must be in the range 00:00:00--23:59:59. After entering the time, press ENT to confirm.



```
Set Time
__:__:__
```

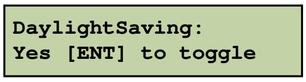
5.5.5 Auto Daylight Saving Time

Press ENT at the below window to adjust the settings for Auto Daylight Savings:

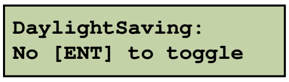


```
Auto Daylight
Saving
```

Press ENT to toggle the setting between Enabled/Disabled, Press CLR to exit



```
DaylightSaving:
Yes [ENT] to toggle
```



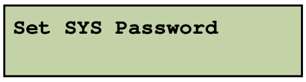
```
DaylightSaving:
No [ENT] to toggle
```

When auto daylight savings is turned on, set the auto daylight start/end time from the built-in management software remotely.

5.5.6 Set System PIN

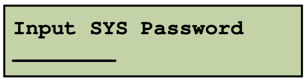
A System PIN must be entered before the user can make management changes via the controller keypad. The factory default System PIN is 00000000. It is recommended that the password is changed after the initial log-in for maximum security. Be sure to secure the new password; if lost, the system can only be accessed after purging all stored data using the reset button on the main board.

Press ENT at the below window to set system PIN.



```
Set SYS Password
```

The LCD will display the following menu.



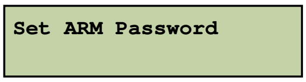
```
Input SYS Password
________
```

Enter a new system PIN. Enter it a second time to confirm. Press ENT to set the new system PIN. Pressing CLR at any time will exit the menu without changing the system PIN.

5.5.7 Set Arm PIN

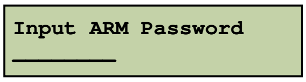
Arm PIN must be entered before the controller can be armed or disarmed via controller keypad. The factory default arm PIN is 00000000.

Press ENT at the window below to set arm PIN.



```
Set ARM Password
```

The LCD will display the following menu.

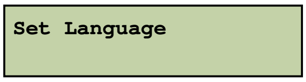


```
Input ARM Password
________
```

Enter a new arm PIN. Enter it a second time to confirm. Press ENT to set the new arm PIN. Pressing CLR at any time will exit the menu without changing the arm PIN.

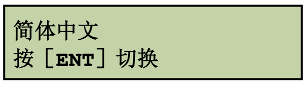
5.5.8 Set Language

Press ENT at the below window to adjust the language setting:

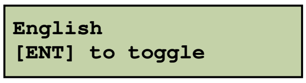


```
Set Language
```

Press ENT to toggle among Chinese, English and Russian, Press CLR to exit. The selected language is the one shown on window when exiting.



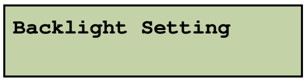
```
简体中文
按［ENT］切换
```



```
English
[ENT] to toggle
```

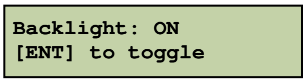
5.5.9 Backlight Setting

Press ENT at the below window to change the backlight setting

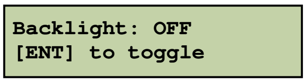


```
Backlight Setting
```

Press ENT to toggle between enabling and disabling backlight. Press CLR to exit



```
Backlight: ON
[ENT] to toggle
```

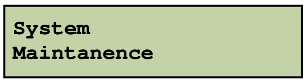


```
Backlight: OFF
[ENT] to toggle
```

5.5.10 System Maintanence

NAV Controller supports two ways to update firmware, backup and restore database: via USB drive or FTP. This section introduces how to use system maintenance with a USB drive.

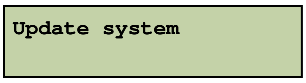
Press ENT at the below window to enter to the system maintenance menu.



```
System
Maintanence
```

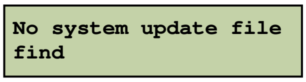
5.6.4.1 Firmware update

Plug the USB drive that contains the firmware file into the USB port of the controller. Press ENT at the below screen of system maintenance menu to start the firmware updating process.



```
Update system
```

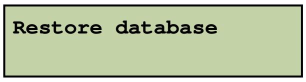
The controller will show the below screen if no valid firmware is found from the plugged USB drive.



```
No system update file
find
```

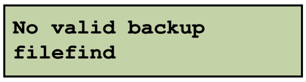
5.6.4.2 Database restore

Plug the USB drive that has the previous backup database file into the USB port of the controller. Press at the below screen to start database storing process.



```
Restore database
```

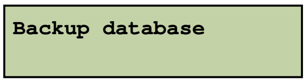
If no valid database data available, the controller shows the below information:



```
No valid backup
filefind
```

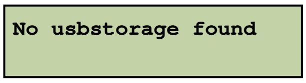
5.6.4.3 Database backup

Plug the USB drive into the USB port of the controller. Press ENT under the below screen to backup the database to the USB drive:



```
Backup database
```

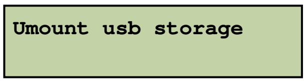
If no USB drive presented when the menu item is selected.



```
No usbstorage found
```

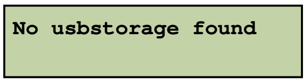
5.6.4.4 Unmount USB storage

USB drive can be hot swapped, but sometime the data will be loss caused by pulling out directly. It is safer that removed from the controller. Press ENT under the below screen to unmount the USB drive when finishing backup and restoring the database from the backup file on USB drive:



```
Umount usb storage
```

If no USB drive presented when the menu item is selected.

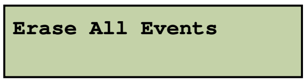


```
No usbstorage found
```

5.5.11 Erase All Events

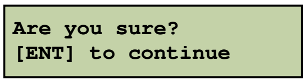
The controller will record all events that occur, beginning immediately upon powering on. These events can be purged by following the instructions below. The old records will be automatically overwritten when storage space is full (1,000,000 events max.).

Press ENT at the window below to erase all events.



```
Erase All Events
```

LCD will prompt the user to confirm the action:



```
Are you sure?
[ENT] to continue
```

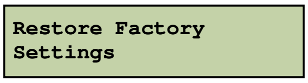
Pressing ENT will result in all events being permanently erased.

⚠ **Caution**: this operation will permanently delete ALL events from the controller database. This operation is NOT undoable.

5.5.12 Load Factory Default

This function is used to reset all settings to factory set default values.

Press ENT at the window below to reset all settings.



```
Restore Factory
Settings
```

The LCD will prompt the user to confirm the action. Press ENT to confirm and perform the reset action.

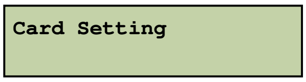
⚠ **Caution**: this operation will recover all the settings to the factory default. This operation is NOT undoable.

5.6 Card Setting

Card setting can be configured using either the controller or the built-in management software. Using the built-in management software is the easiest way to enroll cards. However, enrolling at the controller can be useful if the controller is offline. The process is described below.

5.6.1 Enter Card Setting Menu

Under the System Menu, press V once to bring up the following window:



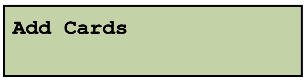
```
Card Setting
```

Press ENT to enter to the Card Setting menu. Use ∧ and V to choose from different menu options. All menu options under the Card Setting menu are introduced below:

5.6.2 Add Cards

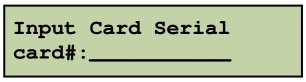
When a new card is added, the controller will automatically assign an index number in the order of enrollment. The index number here is not related to the card number in the software. Users do not need to take care of this number.

Under the Card Setting menu, press ENT at the window below to add a card:



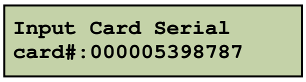
```
Add Cards
```

Press ENT and enter a serial number on the card, as shown below:



```
Input Card Serial
card#:____________
```

User input card serial number, or swipe card via system reader, system reader will automatically read the card serial number to the controller.

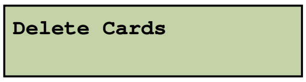


```
Input Card Serial
card#:000005398787
```

Press ENT to confirm and the system will add the card to the controller database. The user can also present the card at the system reader at this time, which will automatically acquire the index number of the new card, show the card number and add it to the controller. It will show “card exists already” if the same card number is in the database already.

5.6.3 Delete Cards

The user can directly delete an individual card with a specific index or card number from the controller, or delete all cards at once. Under the Card Setting menu, press V once to bring up the following window:

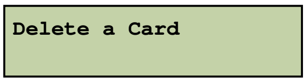


```
Delete Cards
```

Press ENT to enter to the submenu for the following two methods of deleting cards.

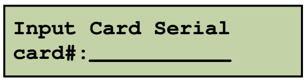
5.6.4.5 Delete a Card

The controller can delete a card according to its serial number, which is printed on the face of each card. At the following window:



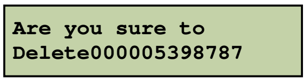
```
Delete a Card
```

Press ENT and the system will prompt the user to enter a card serial number, as shown below:



```
Input Card Serial
card#:___________
```

After entering the serial number, press ENT to delete this card. The system will prompt users to confirm again like the below screen:

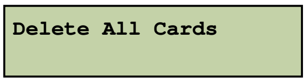


```
Are you sure to
Delete000005398787
```

Press ENT to confirm or press CLR to exit from the "delete card" menu.

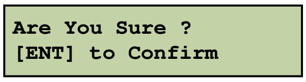
5.6.4.6 Delete All Cards

All cards can be deleted at once. At the following window:



```
Delete All Cards
```

Press ENT and system will prompt the user to confirm deletion:



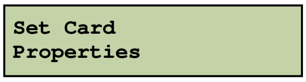
```
Are You Sure ?
[ENT] to Confirm
```

Press ENT again to delete all cards.

⚠ **Caution**: this operation will permanently delete ALL cards from the controller database. This operation is NOT undoable.

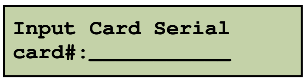
5.6.4 Set Card Properties

Under the Card Setting menu, press V twice to bring up the following window:



```
Set Card
Properties
```

Press ENT and system will prompt the user to enter serial number, as shown below:

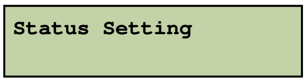


```
Input Card Serial
card#:__________
```

After entering the serial number, press ENT to enter to the submenu for setting card properties. Each card has 6 properties that can be modified. Use ∧ and ∨ to choose desired properties.

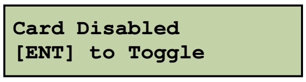
5.6.4.7 Status Setting

A card can be set as enabled or disabled at the following submenu:

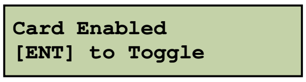


```
Status Setting
```

Press ENT and system will show the status of current card as the figure below. Press ENT to toggle between the two statuses. Press CLR to exit. The selected value is the one shown on window when exiting.



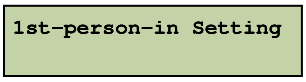
```
Card Disabled
[ENT] to Toggle
```



```
Card Enabled
[ENT] to Toggle
```

5.6.4.8 First Card Setting

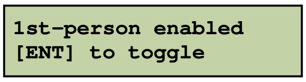
A card can be set as either first card or not from the below submenu:



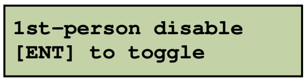
```
1st-person-in Setting
```

Note: First card property indicates if the card can trigger the scheduled door verification rules. For example, even when the doors are configured as always open during the office hour, but it will still remain locked if NO card with enabled "First card" property yet presented and gained the access to the doors in the office hour. For each day, the door verification schedule will be triggered (in this example, become to unlocked in office hour) only after a card with enabled "first card" presented and gained the access.

Press ENT and system will show the "First card" setting of the card as the figure below. Press ENT to toggle between ON/OFF status of the first card setting.



```
1st-person enabled
[ENT] to toggle
```

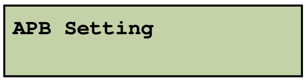


```
1st-person disable
[ENT] to toggle
```

5.6.4.9 Anti-Passback (APB) setting

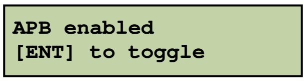
NAV Controller features the Anti-Passback (APB) function on each card. If APB is enabled, cardholder must pass the door in the alternating enter/exit. That is, if the card is swiped to access the door, then next time the card can only be allowed to exit that door. If cardholder attempts to access the same door again without first swipe the card to exit the door, access is denied and the door will not open.

At the following submenu, press ENT to enter Anti Passback setting:

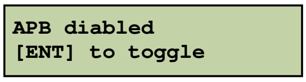


```
APB Setting
```

The APB status of the current card is enabled or disabled, will be displayed as shown below. Press ENT to toggle between two statuses. Press CLR to exit.



```
APB enabled
[ENT] to toggle
```



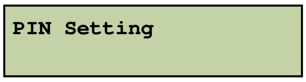
```
APB diabled
[ENT] to toggle
```

Note: Anti-Passback (APB) is an access control function whereby a cardholder is prevented from “passing back” his card to another person to gain entry into the same area twice, without leaving. Facilities are typically fitted with both Entry and Exit readers when Anti-Passback is implemented. A cardholder must alternate usage between entry and exit readers. If the cardholder attempts to pass through an entry reader twice consecutively, his access will be denied and the system will generate an illegal event when the cardholder’s card is configured as APB enabled. Be careful to enable this function in the system with only single side readers installed somewhere.

5.6.4.10 Card PIN Setting

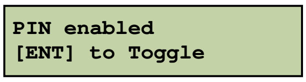
Each card in the NAV Controller is associated with an 8-digit PIN. The PIN status can be set as enabled or disabled and if enabled, A cardholder is required to input the PIN every time when enters/exit the door if the reader is a keypad reader.

At the following submenu, press ENT to enter PIN setting:

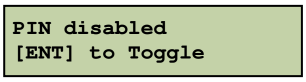


```
PIN Setting
```

The PIN status of the current card, i.e., enabled or disabled, will be displayed as shown below. Press ENT to toggle between two statuses. Press CLR to exit.



```
PIN enabled
[ENT] to Toggle
```

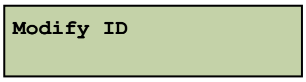


```
PIN disabled
[ENT] to Toggle
```

5.6.4.11 Change Card Serial Number

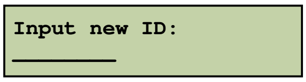
Each card in the NAV Controller has a unique serial number, it can be modify. Usually if the cardholder lost the card and doesn’t want to add a new one again, it can be modified from the old serial number to the new one.

At the following submenu, press ENT to change card ID:



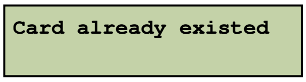
```
Modify ID
```

The below screen will be shown to prompt users to input new ID.



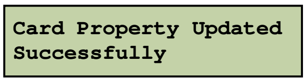
```
Input new ID:
```

The user can either swipe the card through a system reader to get a new ID, or input it manually. Press ENT to confirm the input of new ID. If input ID already exists, the system will prompt:



```
Card already existed
```

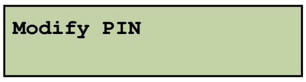
Otherwise, system will show the below information:



```
Card Property Updated
Successfully
```

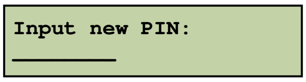
5.6.4.12 Modify card pin

Each card in the NAV Controller system is associated with an 8-digit PIN. Card PIN can be modified from the below screen. At the following submenu, press ENT enter to Modify Card PIN.

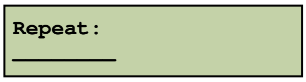


```
Modify PIN
```

Press ENT to prompt to input new PIN, press ENT to repeat new PIN.

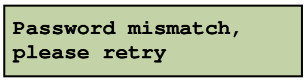


```
Input new PIN:
```



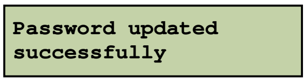
```
Repeat:
```

If repeat PIN is different from first time input, it will prompt,



```
Password mismatch,
please retry
```

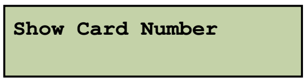
After modify, it will prompt,



```
Password updated
successfully
```

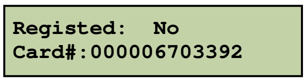
5.6.5 Show Card Number

This function can be used to show the serial number of a card when it is swiped on the system reader. Under Card Setting menu, press V three times to bring up the following window:



```
Show Card Number
```

Press ENT and swipe the card on the system reader. The serial number of the card will be displayed as shown below. Press CLR to exit.



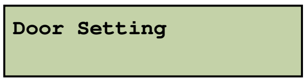
```
Registed:  No
Card#:000006703392
```

5.7 Door Setting

Every door module controls two door relays. NAV Controller can control up to 8 doors in total, defined as door 1 to 8 from right to left. According to reader setting above, users can allocate multiple readers to one single door. User can directly set door unlock time, door held open time and the door control at fire alarm on the controller.

5.7.1 Enter Door Setting Menu

Under System menu, press V three times to bring up the following window:



```
Door Setting
```

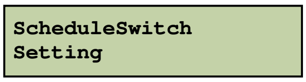
Press ENT to enter Door Setting menu. Use Λ and V to choose from different menu options. All menu options under Door Setting are introduced below.

5.7.2 Schedule Switch Setting

Door verification indicates the access mode when a cardholder enrolls the card on the reader in order to enter/exit the door, for example, a dual security method could require both card and PIN, or both card and fingerprint.

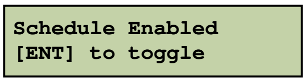
NAV Controller supports a comprehensive door verification schedule on each door. The door verification can be defined individually on a schedule with 10 types of date, 6 time zones on each type of date. If the user just wants to have a consistent access mode all the time every day, schedule switch can be set as OFF to have only one door verification mode, defined in the next section.

At the following submenu, press ENT to enter to the setting for door verification schedule:

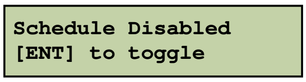


```
ScheduleSwitch
Setting
```

Press ENT to toggle between enable/disable door verification schedules. Press CLR to exit.



```
Schedule Enabled
[ENT] to toggle
```

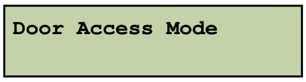


```
Schedule Disabled
[ENT] to toggle
```

5.7.3 Door Access Mode

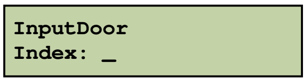
As described in previous section, NAV Controller will use the controller door access mode if the schedule switch is turned off. NAV Controller supports 13 types of door access modes, for example: always open, card only, fingerprint only and so on.

At the following submenu, press ENT to set the controller door access mode:



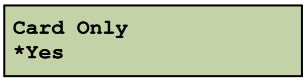
```
Door Access Mode
```

Before setting the door verification mode, users first have to select the door to be set, refer to the below window:

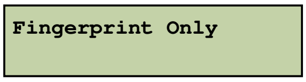


```
InputDoor
Index: _
```

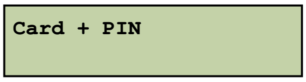
After the door number is entered, press ENT to toggle among all available door verification modes. The modes followed with a star "*" mark is the currently selected mode. All the door verification modes are listed below:



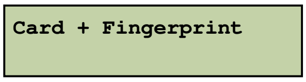
```
Card Only
*Yes
```



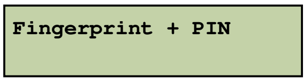
```
Fingerprint Only
```



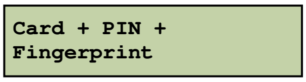
```
Card + PIN
```



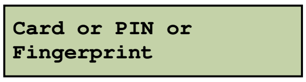
```
Card + Fingerprint
```



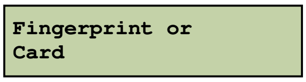
```
Fingerprint + PIN
```



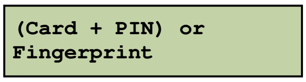
```
Card + PIN +
Fingerprint
```



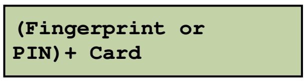
```
Card or PIN or
Fingerprint
```



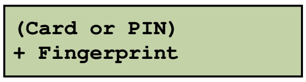
```
Fingerprint or
Card
```



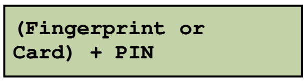
```
(Card + PIN) or
Fingerprint
```



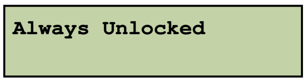
```
(Fingerprint or
PIN)+ Card
```



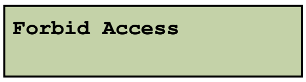
```
(Card or PIN)
+ Fingerprint
```



```
(Fingerprint or
Card) + PIN
```



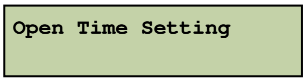
```
Always Unlocked
```



```
Forbid Access
```

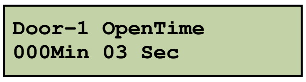
5.7.4 Open Time Setting

This sets the door open time when the card is swiped or request-to-exit button is pushed. The default time is 3 seconds. The maximum door open time supported by the controller is 999 minutes and 59 seconds. The door remains open as long as the request-to-exit button is pushed down. The door open time does not count until the button is released. In the following submenu:



```
Open Time Setting
```

Press ENT to enter door Open Time setting. Use ∧ and ∨ to choose from different door.



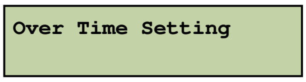
```
Door-1 OpenTime
000Min 03 Sec
```

Input the desired door open time: enter minutes as a 3-digit number 0~999, and enter seconds as a 2-digit number 0~59. Press ENT to confirm. Press CLR to exit without effecting any change.

5.7.5 Over TimeSetting

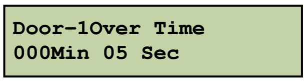
Door sensor monitors the open/close status of a door. If normally open is not set by the system (door is normally considered closed), then door should close after opening for a while. It is considered abnormal if controller does not receive the door close signal from door sensor in a reasonable amount of time after the door is opened. This time period is called door hold open time or door over time. According to this setting, NAV Controller will determine whether to generate an alarm or not after the door sensor timeouts. The default value of door hold open time is 5 seconds. The maximal door hold open time supported by the controller is 999 minutes and 59 seconds.

At the following submenu:



```
Over Time Setting
```

Press ENT to enter Over Time setting. Use ∧ and ∨ to choose from different door.



```
Door-1Over Time
000Min 05 Sec
```

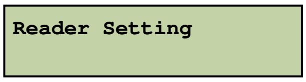
Input the desired door hold open time in the Open Time field: enter minutes as a 3-digit number 0~999, and enter seconds as a 2-digit number 0~59. Press ENT to confirm. Press CLR to exit without effecting any change.

5.8 Reader Setting

Card reader properties can be directly set on the controller, including whether the reader is keypad reader, the allocation of readers to doors, and system reader etc.

5.8.1 Enter Reader Setting Menu

Under System menu, press ∨ twice to bring up the following window:

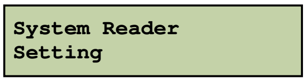


```
Reader Setting
```

Press ENT to enter Reader Setting menu. Use ∧ and ∨ to choose from different menu options. All menu options under Reader Setting are introduced below:

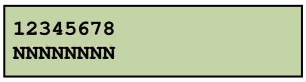
5.8.2 System Reader Setting

System reader can be used to acquire the card's serial number when controller configures the card. User can set any reader that connects to the controller as the system reader. At the following submenu:



```
System Reader
Setting
```

Press ENT to enter System Reader setting. System will show current status of all readers as shown below. Y means the reader is the system reader, N means it's not. By default, no reader is set as the system reader. Users have to set it manually.

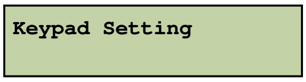


```
12345678
NNNNNNNN
```

Press any of the 1-8 numeric keys to change the system reader setting of corresponding readers. Press CLR to exit.

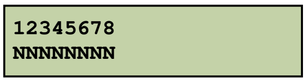
5.8.3 Keypad Setting

Keypad Setting defines whether the reader is a keypad reader. For a keypad reader, if the PIN property of the card is set as enabled, and the access rights of the door are set as card plus PIN, then the user is asked to enter password when the card is swiped on the keypad reader. At the following submenu:



```
Keypad Setting
```

Press ENT to enter keypad setting. System will show keypad setting status of all installed readers. Y means the reader is a keypad reader, and N means the reader is a non-keypad reader. By default, every reader is set as a non-keypad reader. Flex controller will display the door number according to the number of installed door modules. In the following example, 4 door modules (8 readers) have been installed on the controller.

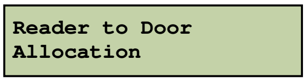


```
12345678
NNNNNNNN
```

Press numeric keys to toggle the keypad setting of corresponding reader. Press ENT to confirm. Press CLR to exit without effecting any change.

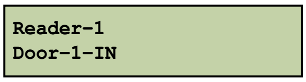
5.8.4 Reader to Door Allocation

NAV Controller can be flexibly configured. Readers can be allocated to different doors, and can be set as ENTER only or EXIT only. By default, each reader is allocated as ENTER only to the door with the reader's number. At the following submenu:



Reader to Door
Allocation

Press ENT to enter Reader to Door Allocation setting. System will show the allocation of the first reader to door as following:



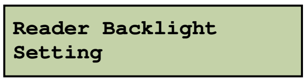
Reader-1
Door-1-IN

Press any of the 1-8 numeric keys to allocate the current reader to corresponding doors. (This depends on the actual door modules installed on the controller) Press the same numeric key to toggle between ENTER only (IN) and EXIT only (OUT).

Press the ∧ or ∨ to select the different readers. Press CLR to exit.

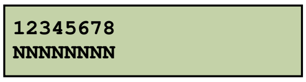
5.8.5 Reader Backlight Setting

At the following submenu:



Reader Backlight
Setting

Press ENT to enter Reader Backlight Setting. As shown below, the system will show if the backlight setting of all readers are turned on or off. Y indicates ON, N indicates OFF. The default setting of backlight is OFF. Note this feature only applies the reader released after Q3, 2010.

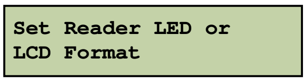


12345678
NNNNNNNN

Press any of the 1-8 numeric keys to change the backlight setting of each reader. Press CLR to exit.

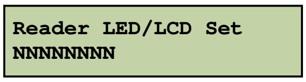
5.8.6 Set Reader LED or LCD format

At the following submenu:



Set Reader LED or
LCD Format

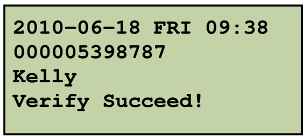
Press ENT to enter Reader LED/LCD format. As shown below, the system will display if the showing format of all readers are LCD or LED. Y indicates LED, N indicates LCD. The default setting is LCD. Note this feature only applies the reader released after Q3, 2010.



Reader LED/LCD Set
NNNNNNNN

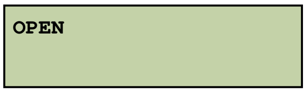
Press any of the 1-8 numeric keys to change the format setting of each reader. Press CLR to exit.

NOTE: LCD format will display more information, include current time, card serial number, employee full name (if value is set), success or failure of current access verification. The screen of the reader must be an LCD, shown as following:



```
2010-06-18 FRI 09:38
000005398787
Kelly
Verify Succeed!
```

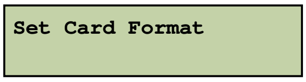
If the screen of the reader is LCD, but set the format is LED, it is shown as following:



```
OPEN
```

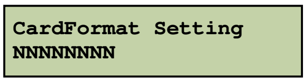
5.8.7 Set Card Format

At the following submenu:



```
Set Card Format
```

Press ENT to enter Card Format Setting. As shown below, the system will show what the reading card direction of all readers is. The default setting of card format is N. Note: this feature only applies the reader released after Q3, 2010.



```
CardFormat Setting
NNNNNNNN
```

Press any of the 1-8 numeric keys to change the format setting of each reader. Press CLR to exit.

NOTE: Users do not need to take care of what is the detail of this reading direction. The user just chooses the correct format when the card serial number shown on the LCD screen matching the number printed on the card self.

5.9 Alarm Setting

NAV Controller is equipped with powerful alarm functions. With alarm modules and door modules fully installed, the controller can accommodate up to 10 alarm inputs and 18 alarm outputs. In the meantime, the controller also provides a very flexible configuration. Any event can be arbitrarily allocated to single or multiple alarm outputs. Alarm components, configuration basics, and menu settings are introduced below.

5.9.1 Components for Alarm

NAV Controller consists of two basic components: one main module and one door module. Users can additionally install three more door modules and one alarm module.

These three types of modules are all equipped with alarm function. The main module has 2 alarm inputs and 2 alarm outputs, called Main Alarm Output and Auxiliary Alarm Output respectively.

Each door module has 2 alarm outputs, which usually react to alarm events on the corresponding door. However, it can be set to react to other alarm events as well. Alarm outputs on the door module can connect up to 5A external alarm devices.

The alarm module has 8 alarm inputs and 8 alarm outputs. 8 alarm inputs can connect to external alarm input devices, such as PIR motion sensor, glass sensor and etc. 8 alarm outputs can connect up to 2A external alarm devices.

The above mentioned are physical devices providing alarm functions

User can freely define the allocation of any input to any output. The following section outlines basic concepts for events, alarm and configuration.

5.9.2 Alarm Configuration Basics

NAV Controller keeps track of all events in the access control system, either legal or illegal, either normal or abnormal. For example, access granted, access denied and so on.

Some events are critical which must trigger the alarm output, like the firm alarm input, the zone alarm input and etc. But some events are not that important to trigger the alarm output, like the denied access due to the invalid time. These settings all depend on the users' requirements. NAV Controller collects all events that might trigger the alarm output and provides the full capacity to enable or disable the alarm output on these events.

Sometimes user wants to allocate a particular event to a particular alarm output, or allocate alarm inputs in certain area to multiple alarm outputs. NAV Controller delivers all the function and flexibility user need. User can define whether certain event will trigger an alarm, and can further specify to which alarm output that event is allocated.

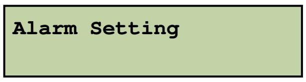
All events that might trigger an alarm are listed below:

Alarm input 0~9, unknown card, expired card, invalid card, invalid door, invalid time, card anti-pass back fail, card PIN fail, SYS PIN fail, ARM PIN fail, door forced open, door held open, reader lost, and remote alarm.

All these events can be allocated to any alarm relay output on main module, door module, and alarm module. The detailed configuration method is introduced in the following section.

5.9.3 Enter Alarm Setting Menu

Under System menu, press V four times to bring up the following window:

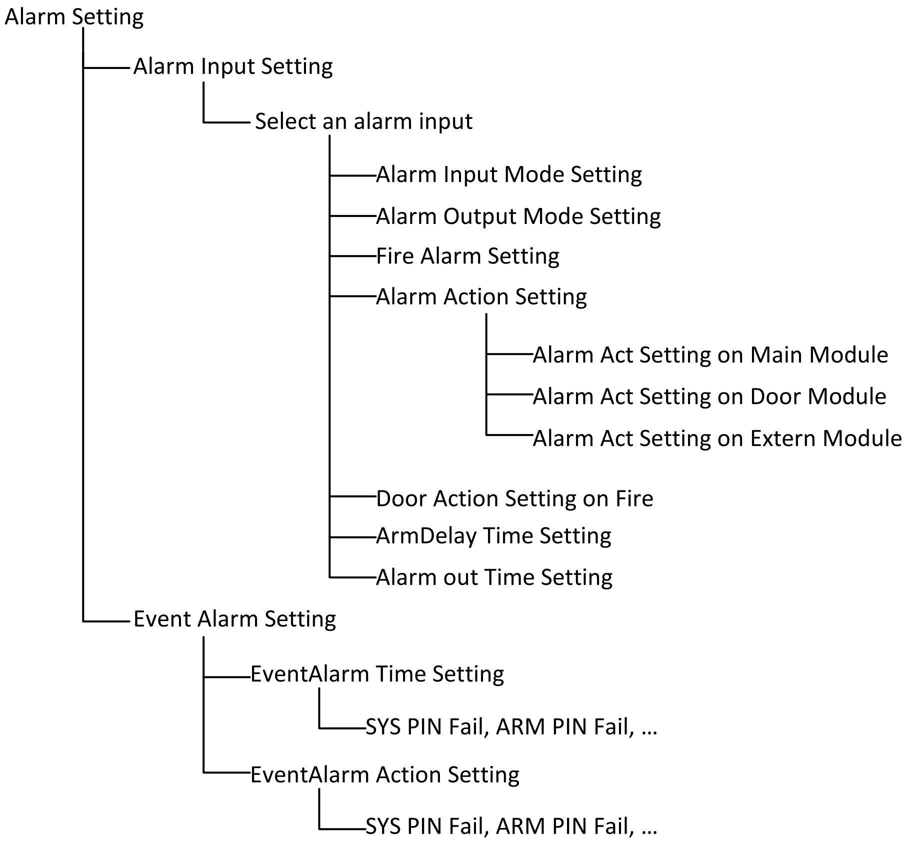


```
Alarm Setting
```

Press ENT to enter Alarm Setting menu. Use ∧ and V to choose from different menu options. All menu options under Alarm Setting are introduced below:

5.9.4 Alarm Setting Menu Structure

There are two submenus under Alarm Setting, as shown below:

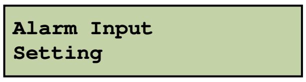

Alarm Setting
Alarm Input Setting
Select an alarm input
Alarm Input Mode Setting
Alarm Output Mode Setting
Fire Alarm Setting
Alarm Action Setting
Alarm Act Setting on Main Module
Alarm Act Setting on Door Module
Alarm Act Setting on Extern Module
Door Action Setting on Fire
ArmDelay Time Setting
Alarm out Time Setting
Event Alarm Setting
EventAlarm Time Setting
SYS PIN Fail, ARM PIN Fail, …
EventAlarm Action Setting
SYS PIN Fail, ARM PIN Fail, …

Alarm input setting menu is used to configure the settings of the physical alarm inputs on main module and alarm module, including input mode, output mode, fire alarm input, alarm output actions, door behavior under fire alarm, arm delay time, and alarm output duration.

Event alarm setting menu is used to configure alarm outputs and output duration for all events on main module and door module.

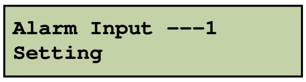
5.9.5 Alarm Input Setting

From the Alarm Setting menu, go to the below window:



```
Alarm Input
Setting
```

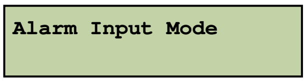
Press ENT to enter to the alarm input setting, the system will first prompt users to select an alarm input, like the below window. Total 10 alarm inputs (0-9) available in NAV Controller.



```
Alarm Input ---1
Setting
```

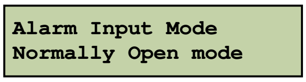
5.9.5.1 Alarm Input Mode

At the above window, press ENT to enter to the setting for alarm input #1. The 1st submenu is the alarm input mode submenu, use ∧ and ∨ to switch to other submenus.

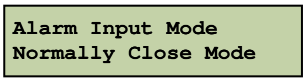


Alarm Input Mode

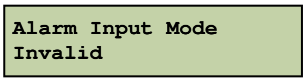
Three alarm input modes are available: N.O., N.C, and Invalid. Press ENT to toggle among the three modes.



Alarm Input Mode
Normally Open mode



Alarm Input Mode
Normally Close Mode

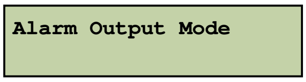


Alarm Input Mode
Invalid

- N.O. mode indicates the normal status (no alarm input signal) of circuit is disconnected. It will be alarmed if the alarm input is active and the circuit will be closure.
- N.C. mode is the inversed case of N.O. It means the normal status of circuit is closure. It will be alarmed if the alarm input is active and the circuit will be disconnected.
- Invalid input indicates the related alarm input is disabled.

5.9.5.2 Alarm Output Mode

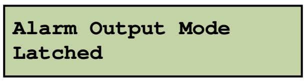
At the following window, press ENT to configure the alarm output mode



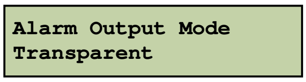
Alarm Output Mode

There are two alarm output modes: latched mode and transparent mode.

Press ENT to toggle between the two modes.



Alarm Output Mode
Latched

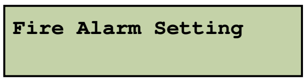


Alarm Output Mode
Transparent

- Transparent mode indicates the alarm output will present as long as the alarm input is valid, and alarm output will disappear when the alarm input is invalid. The duration of alarm output is purely controlled by the duration of valid alarm input, not related with the timeout configuration.
- Latched mode indicates that alarm output can only be triggered by the valid alarm input after the arm delay duration. And the alarm output will be last for the specified alarm timeout duration.

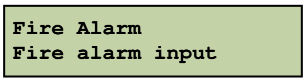
5.9.5.3 Fire Alarm Setting

Under the below window, press ENT to configure the fire alarm feature of an alarm input:

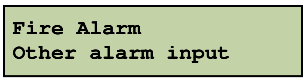


Fire Alarm Setting

Fire alarm setting is used to configure other alarm inputs as the fire alarm input. Fire alarm input does not follow the arm delay time, it has the highest priority. It is triggered as long as the alarm input defined as fire alarm is configured. All 10 alarm inputs can be defined fire alarm input.



```
Fire Alarm
Fire alarm input
```

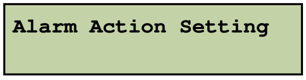


```
Fire Alarm
Other alarm input
```

5.9.5.4 Alarm Action Setting

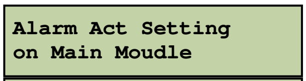
Alarm Action Setting is used to configure the allocation between the physical alarm input and the output on main module, door module and alarm module.

Press ENT to configure alarm action setting when the following window appears.

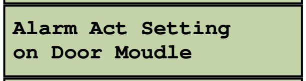


```
Alarm Action Setting
```

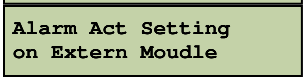
NAV Controller provides total 18 alarm outputs: 2 alarm outputs on main module, 8 alarm outputs on door module, 8 alarm outputs on alarm module. They are allocated in 3 submenus, shown as the below windows:



```
Alarm Act Setting
on Main Moudle
```

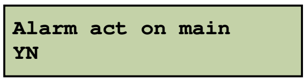


```
Alarm Act Setting
on Door Moudle
```



```
Alarm Act Setting
on Extern Moudle
```

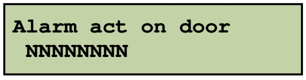
The first menu is “Alarm Act Setting on Main Module”. Press ENT to enter to the setting, LCD screen shows the current status of the alarm output. Y indicates the alarm output is enabled; N indicates the alarm output is disabled.



```
Alarm act on main
YN
```

The main module provides two alarm outputs, press key “1” and “2” to toggle the alarm output 1, 2 ON and OFF

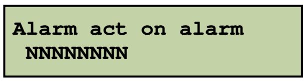
Press V to switch to “Alarm Act Setting on Door Module” submenu. Press ENT to enter to the setting, LCD screen shows the current status of the alarm relay outputs on the door module.



```
Alarm act on door
 NNNNNNNN
```

Up to 4 door modules can be installed on the NAV Controller. 2 alarm outputs are available on each door module. As a result, up to 8 alarm outputs can be available if 4 door modules are installed. Press numeric key 1~8 to toggle the alarm output on door module between ON and OFF.

Press V to switch to “Alarm Act Setting on Extern Module” submenu. Press ENT to enter to the setting, LCD screen shows the current status of the alarm outputs on alarm module.



```
Alarm act on alarm
 NNNNNNNN
```

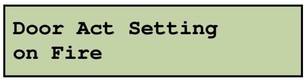
One alarm module can be installed on the NAV Controller. 8 alarm outputs are available on alarm module. Press numeric key 1~8 to toggle the alarm output on alarm module between ON and OFF.

Note the “Alarm Output on Alarm Module” is only shown when alarm module is installed on the controller.

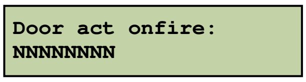
5.9.5.5 Door Act Setting On Fire

The controller allows the user to choose one of two behaviors to occur when a fire alarm is triggered: fail-safe or fail-secure. Door fail-safe at fire alarm means the door will be kept unlocked when there is a fire alarm input. Door fail-secure at fire alarm means the door will be locked when the fire alarm comes in.

In submenu list of “Alarm Input Setting”, press ∧ and ∨ to navigate to the below submenu to set the door behavior at fire alarm:


Door Act Setting
on Fire

Press ENT to enter to the setting, LCD screen shows the current setting status of the door action when firm alarm is triggered.


Door act onfire:
NNNNNNNN

In the menu shown above, press numeric key 1~8 to toggle the door action between fail-safe and fail-secure. (The numbers correspond to the number of door modules installed in the controller) “Y” indicates fail-safe; “N” indicates fail-secure.

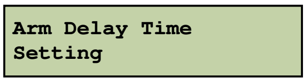
The default setting for door control at fire alarm is all the doors are fail-safe, *i.e.* all the doors will be unlocked during a fire alarm.

5.9.5.6 Arm Delay Time Setting

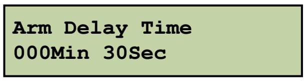
When an arm operation is executed, all active arm zones will enter ARM enabled status only after a certain time delay, which is called ARM delay time. When a card with ARM enabled is swiped to pass a door, system will not generate an alarm within the arm delay period so that cardholder has time to disarm the system.

The details to set ARM delay time is as following. And the alarm delay time can be set to different durations. In submenu list of “Alarm Input Setting”, press ∧ and ∨ to navigate to the below submenu to set the arm delay time:

Press ENT to set ARM delay time at the following window:


Arm Delay Time
Setting

System will display the current delay time as shown below. Use numeric keys to input the desired ARM delay time. Enter minutes as a 3-digit number 0~999 and seconds as a 2-digit number 0~59. The default value of ARM delay time is 30 seconds.

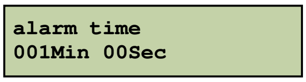

Arm Delay Time
000Min 30Sec

Press ENT to confirm. Press CLR to exit without effecting any change.

5.9.5.7 Alarm Out Time Setting

As described in alarm input mode, alarm timeout defines the duration of alarm output being presented (alarm relay energized), when triggered by the specified alarm input and if the alarm output mode is configured as "Latched" mode. After the alarm timeout duration, the alarm output will be reset to normal. The default alarm timeout duration is 60 seconds.

Note fire alarm has to be manually reset. It does not limited by the alarm timeout duration.

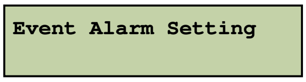


```
alarm time
001Min 00Sec
```

5.9.6 Alarm Event Setting

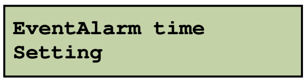
The physical alarm inputs can trigger alarm outputs. As described in previous section, the logic events, for example, unknown card, invalid card, expired card, invalid door and etc., can trigger the alarm outputs as well.

Press ENT at the below window to configure the event alarm setting.

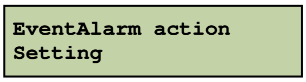


```
Event Alarm Setting
```

Two submenus are included in event alarm setting: event alarm time setting and event alarm action setting, explained in the following sections. The screens of the two settings are shown below:



```
EventAlarm time
Setting
```



```
EventAlarm action
Setting
```

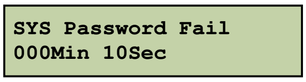
5.9.6.1 Event Alarm Time Setting

Press ENT at the screen of "Event Alarm Time Setting" to configure event alarm time setting. As introduced earlier, NAV Controller allows a logical event to trigger an alarm output. The duration of the alarm output can be specified per event type. Different event types can generate the different duration of the alarm output. The default value of event alarm time is 1 minute.

The following windows show the event alarm time setting on different events. All events will be explained one by one.

SYS PIN Fail

Please refer to section "Gain Access to System Configuration" in this chapter. A SYS PIN Fail event will be generated when user enters the PIN to enter system setting and a wrong PIN is entered three times consecutively. The time setting for system PIN failure event is shown in the below figure:

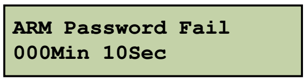


```
SYS Password Fail
000Min 10Sec
```

Press the numeric keys to input the specified alarm time for system password failure. Press ENT to confirm and press CLR to discard the change just made.

ARM PIN Fail

User is required to enter PIN when pressing ARM key to arm or disarm the system. An ARM PIN Fail event will be generated when a wrong PIN is entered three times consecutively. Please refer to the section “ARM/DISARM”. The time setting for ARM PIN failure event is shown in the below figure:

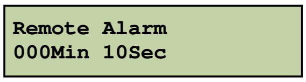


```
ARM Password Fail
000Min 10Sec
```

Press numeric keys to input the specified alarm time for event of ARM PIN failure Press ENT to confirm and press CLR to discard the change just made.

Remote Alarm

System administrator can directly generate alarm signal using the Control Software when he observes abnormal condition through surveillance system such as CCTV. This is defined as a Remote Alarm event. The time setting for remote alarm event is shown in the below figure:

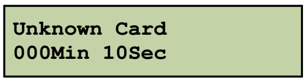


```
Remote Alarm
000Min 10Sec
```

Press numeric keys to input the specified alarm time for event of remote alarm. Press ENT to confirm and press CLR to discard the change just made.

Unknown Card

Unknown card refers to a card that hasn’t been registered in the system. An Unknown Card event will be generated when an unknown card is swiped on the reader. The time setting for unknown card event is shown in the below figure:

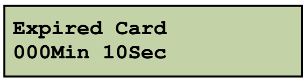


```
Unknown Card
000Min 10Sec
```

Press numeric keys to input the specified alarm time for event of unknown card. Press ENT to confirm and press CLR to discard the change just made.

Expired Card

Any card in the system is usually assigned a valid date. After the valid date has passed, the controller will automatically set the card as an expired card. An expired card cannot gain access to the system. At the same time, an Expired Card event will be generated when an expired card is swiped on the reader. The time setting for expired card event is shown in the below figure:

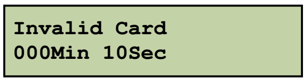


```
Expired Card
000Min 10Sec
```

Press numeric keys to input the specified alarm time for event of expired card. Press ENT to confirm and press CLR to discard the change just made.

Invalid Card

To disable a card, user can directly set the card as invalid card. An invalid card cannot gain access to the system. At the same time, an Invalid Card event will be generated when an invalid card is swiped on the reader. The time setting for invalid card event is shown in the below figure:

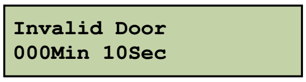


```
Invalid Card
000Min 10Sec
```

Press numeric keys to input the specified alarm time for event of Invalid Card. Press ENT to confirm and press CLR to discard the change just made.

Invalid Door

Each door on the controller can be set its own access schedule, when a card is swiped on the reader. An Invalid Door event will be generated when a card is swiped at any door it can't gain access to system by the access schedule. The time setting for invalid door event is shown in the below figure:

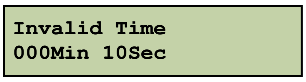


```
Invalid Door
000Min 10Sec
```

Press numeric keys to input the specified alarm time for the event. Press ENT to confirm and press CLR to discard the change just made.

Invalid Time Section

Each card belongs to an access group. Each group has its own allowed doors and time zones. That is, cards in the group have rights to pass which door at which time. An Invalid Time event will be generated when a card is swiped at any time it does not have right to pass. The time setting for invalid time event is shown in the below figure:

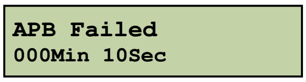


```
Invalid Time
000Min 10Sec
```

Press numeric keys to input the specified alarm time for the event. Press ENT to confirm and press CLR to discard the change just made.

Card Anti-Passback Fail

For more info on Anti-Passback, please refer to section Anti-Passback (APB) setting in this chapter. A Card Anti-Passback Fail event will be generated when the APB property of a card is set as enabled and that card is swiped twice consecutively on any enter-door reader or exit-door reader. The time setting for card APB fail event is shown in the below figure:

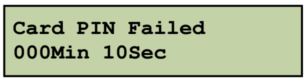


```
APB Failed
000Min 10Sec
```

Press numeric keys to input the specified alarm time for the event. Press ENT to confirm and press CLR to discard the change just made.

Card PIN Fail

For password setting, please refer to section "Set Card PIN Setting" in this chapter. A Card PIN Fail event will be generated when the card is swiped at the reader and PIN is required to gain access but the cardholder enters wrong PIN three times consecutively. The time setting for card PIN fail event is shown in the below figure:

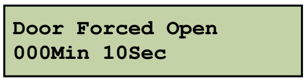


```
Card PIN Failed
000Min 10Sec
```

Press numeric keys to input the specified alarm time for the event. Press ENT to confirm and press CLR to discard the change just made.

Door Forced Open

A Door Forced Open event will be generated when controller detects that a door is opened from the door sensor without any legitimate swipe card or door open button push operation taking place. The time setting for door forced open event is shown in the below figure:

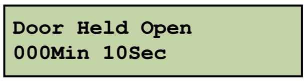


```
Door Forced Open
000Min 10Sec
```

Press numeric keys to input the specified alarm time for the event. Press ENT to confirm and press CLR to discard the change just made.

Door Held Open

A Door Held Open event will be generated when a door is opened by legitimate swipe card or door open button push operation but is still not closed after the “over time” in door setting has elapsed. The time setting for door held open event is shown in the below figure:

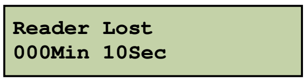


```
Door Held Open
000Min 10Sec
```

Press numeric keys to input the specified alarm time for the event. Press ENT to confirm and press CLR to discard the change just made.

Reader Lost

A Reader Lost event will be generated when controller detects that the reader has no signal. The time setting for reader lost event is shown in the below figure:



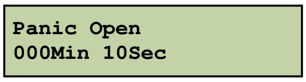
```
Reader Lost
000Min 10Sec
```

Press numeric keys to input the specified alarm time for the event. Press ENT to confirm and press CLR to discard the change just made.

Panic Open

Panic Open alarms are designed to allow users who are forced to enter a building under duress to silently trigger an alarm. When the door’s access schedule is configured as PIN needed, for example: “Card or PIN” or “Card plus PIN”, cardholders can type in their panic PIN to trigger a panic open event in the system.

The panic PIN is the cardholder’s original PIN plus any two digits. For example, Sam’s PIN is 12345678. He can type in any two more digits following“12345678” as the panic PIN, such as “1234567800”.The time setting for panic open event is shown in the below figure:

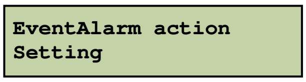


```
Panic Open
000Min 10Sec
```

Press numeric keys to input the specified alarm time for the event. Press ENT to confirm and press CLR to discard the change just made.

5.9.6.2 Event Alarm Action Setting

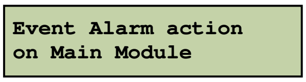
Press ENT at the below screen to configure event alarm action setting.



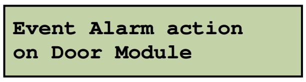
```
EventAlarm action
Setting
```

The event alarm action defines which alarm output can be triggered by the event. As we explained before, NAV Controller can take main modules, up to 4 door modules and 1 alarm module, total 18 alarm output. Users will be able to configure the event to trigger any one or multiple outputs from those 18 alarm outputs.

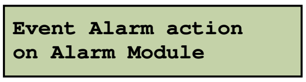
The event alarm action setting includes three submenus, shown in below.



```
Event Alarm action
on Main Module
```

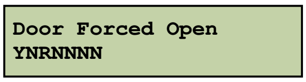


```
Event Alarm action
on Door Module
```



```
Event Alarm action
on Alarm Module
```

The alarm output setting on these three screens are the similar. For example, the fire alarm event actions on door module will look like:



```
Door Forced Open
YNRNNNN
```

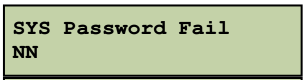
The top line indicates the event to be configured. The bottom line is the setting of alarm outputs on 4 door modules. Y indicates there is alarm output (relay energized) and N indicates there is no alarm output (relay not energized). R refers specifically to alarm output on the door module, indicating that alarm output will be generated only if the event occurs on the corresponding door. The above example means the alarm output relay at door 1 will be energized if door forced open event happens on any door, the alarm output relay at door 2 does not respond to any door forced open event, and same as door 4 to 8. Door 3 indicates the alarm output relay on door 3 will be energized if and only if the door 3 got a forced open event.

Note "R" option for alarm output does not apply to alarm module and main module, since they don't naturally correspond to a door control.

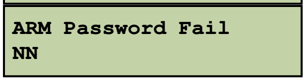
In the above menu, press numeric key 1~8 to toggle the alarm output actions of this event on the door module among Y, N, and R (only for door module). Press ∧ and ∨ to navigate to other alarm action settings.

The default setting of all the event alarm actions on main module, door module and alarm modules are all disabled. The event alarm actions for main module and door modules are listed below. Default settings for event alarm actions on alarm module are same as door module, not listed here.

Main module

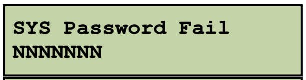


```
SYS Password Fail
NN
```

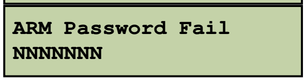


```
ARM Password Fail
NN
```

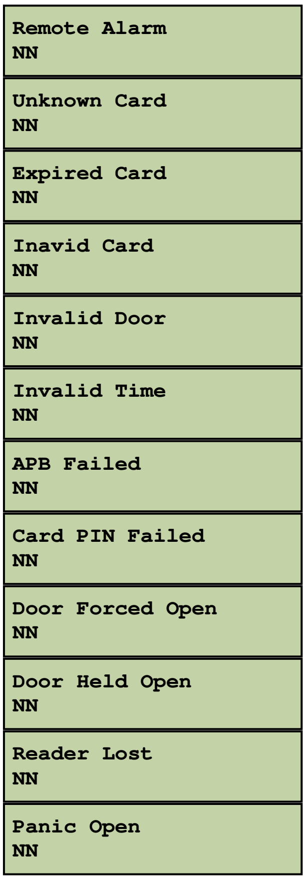
Door module



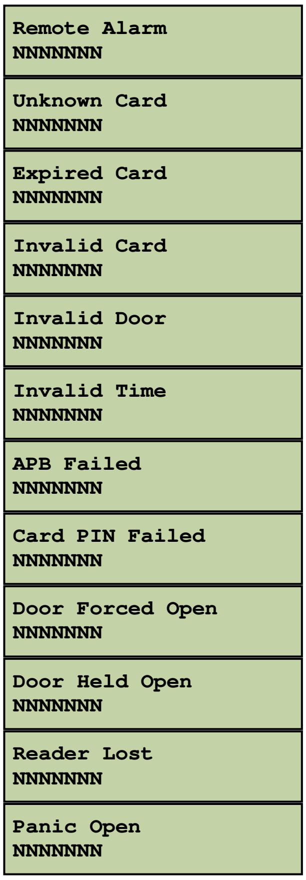
```
SYS Password Fail
NNNNNNN
```



```
ARM Password Fail
NNNNNNN
```



```
Remote Alarm
NN

Unknown Card
NN

Expired Card
NN

Inavid Card
NN

Invalid Door
NN

Invalid Time
NN

APB Failed
NN

Card PIN Failed
NN

Door Forced Open
NN

Door Held Open
NN

Reader Lost
NN

Panic Open
NN
```

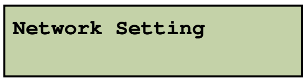


```
Remote Alarm
NNNNNNN

Unknown Card
NNNNNNN

Expired Card
NNNNNNN

Invalid Card
NNNNNNN

Invalid Door
NNNNNNN

Invalid Time
NNNNNNN

APB Failed
NNNNNNN

Card PIN Failed
NNNNNNN

Door Forced Open
NNNNNNN

Door Held Open
NNNNNNN

Reader Lost
NNNNNNN

Panic Open
NNNNNNN
```

5.10 Network Setting

Correct network settings are needed for NAV Controller to get online and be accessible remotely. Network setting includes DHCP setting, IP address setting.

Press V five times from main menu items to view the below screen:

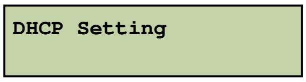


```
Network Setting
```

In the above screen, press ENT to enter the network setting submenus.

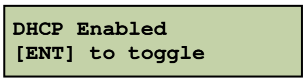
5.10.1 DHCP Setting

DHCP setting is the first submenu under network setting. Press ENT from the below screen to configure DHCP setting.



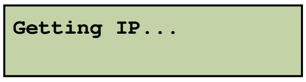
```
DHCP Setting
```

The below screen will be shown in the DHCP setting submenu. Press ENT key to toggle between DHCP (DHCP enabled) and static IP (DHCP disabled). The default DHCP setting is disabled by default.



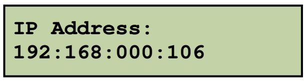
```
DHCP Enabled
[ENT] to toggle
```

When DHCP is enabled, press CLR to exit and NAV Controller will update the IP address from DHCP server and show the below screen, indicating the controller is getting IP address:



Getting IP...

After the IP address has been obtained, controller shows the IP address in the below window:

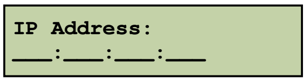


IP Address:
192:168:000:106

At this window, press ENT to update the IP address again. Press CLR to exit to “DHCP Setting” window.

5.10.2 Set IP Address

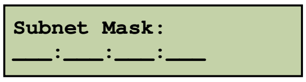
For a static IP setting, users need to manually set an IP address. Press ENT under the below submenu of Network Setting to set IP address:



IP Address:
___:___:___:___

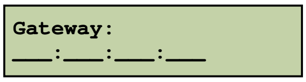
Input the desired IP address and press ENT to confirm. The default IP address is 192.168.1.200

When using static IP (DHCP disabled), NAV Controller will require the subnet mask and gateway setting automatically after the IP address is set here.



Subnet Mask:
___:___:___:___

Input the desired subnet mask and press ENT to confirm.



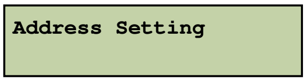
Gateway:
___:___:___:___

Input the desired gateway IP address and press ENT to confirm.

5.11 Address Setting

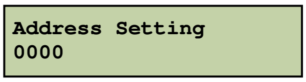
NAV Controller is connected to network for remote accessibility by IP Address, but it must have a unique address for the purpose of communications and control by the Management Software when there is more than one controller.

Press V six times from main menu items to view the below screen:



Address Setting

Press ENT to enter to the address setting menu, as shown below:



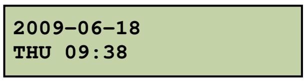
Address Setting
0000

5.12 Arm/Disarm

After an alarm module is installed, it defines 10 arm zones for its 10 alarm inputs (including the 2 alarm inputs on main module). NAV Controller can treat alarm inputs in 10 arm zones in a very flexible manner. These 10 arm zones can be armed or disarmed on the controller as described below.

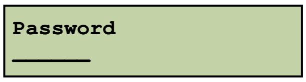
5.12.1 Arm the Systemusing the Controller Keypad

User must have the ARM PIN in order to utilize this function. Please refer to the section “Set ARM PIN” in this chapter for instructions on how to set ARM PIN. After system installation, the date and time information will be displayed on the LCD, as shown below:



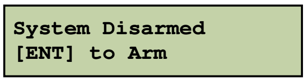
```
2009-06-18
THU 09:38
```

When ARM on the keypad is pressed, the system prompts the user to enter a password, as shown below:



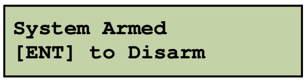
```
Password
______
```

After entering the password, press ENT to confirm. The default password is 00000000. Once the password is verified, the current system ARM status will be displayed as shown below:



```
System Disarmed
[ENT] to Arm
```

Press ENT to arm all active arm zones. The following message is displayed:



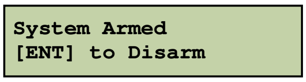
```
System Armed
[ENT] to Disarm
```

Press CLR to exit. The controller will wait for the period of time defined as “alarm delay” and then arm all active arm zones.

5.12.2 Disarm the Systemusing the Controller Keypad

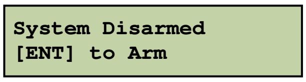
In order to utilize this function, the user must have the ARM PIN and the card must be logged in as ARM enabled. Assuming the system is in armed status, the user swipes the card to access the door. The controller will disarm all active arm zones in arm delay time. For example, if the system is in armed status and a card is presented, the controller will disarm all active arm zones for the amount of time assigned as the arm delay. During this time, no alarm outputs will be generated even if an alarm input is triggered.

Similar to the procedure to arm the system, press ARM on the keypad. Input the ARM password and press ENT to confirm. After the password is verified the current system ARM status will be displayed as shown below:



```
System Armed
[ENT] to Disarm
```

Press ENT to disarm all active arm zones. The following message is displayed:



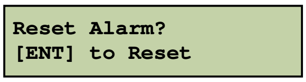
```
System Disarmed
[ENT] to Arm
```

Press CLR to exit.

5.12.3 Reset Alarm

When system is generating an active, ongoing alarm output, follow the procedure below to reset the alarm.

At the window showing the system time, press ARM on the keypad. Input the ARM password and press ENT to confirm. After password is verified the following menu window appears:



```
Reset Alarm?
[ENT] to Reset
```

Press ENT to clear the alarm. If system is currently armed user will be prompted to disarm the system first. Please refer to previous section for how to disarm the system.

5.12.4 Arm/Disarm the System using a Keypad Reader

The whole system can also be armed and disarmed using a keypad reader. (The reader must have an integrated keypad, and the keypad and system reader settings must be enabled on the controller in order to utilize this feature. Please refer to subsection "Reader Setting" for instructions on enabling these features.) The part number for the EverAccess keypad reader is ERK-871.

The user must first enter a command to get into the arm operation mode. (The command is introduced in step 1 below.) In the arm operation mode, the yellow LED on the ERK-871 will show the four different system modes outlined below:

Yellow LED Status	System ARM Status
OFF	Indicates that the system is disarmed
ON	Indicates that the system is armed
Flashing Slowly	Indicates that the system is in arm delay period
Flashing Quickly	Indicates that the system is armed and some alarm input has triggered the alarm output.

The steps to arm or disarm the system at a keypad reader are as followed:

1. Press"*" key on the keypad and input 8 digits ARM password, then press "#" key to arm/disarm the system.

2. If the system is in disarmed mode (the yellow LED is OFF), press"#" to arm the system. The system will enter the arm delay period (the yellow LED will slowly flash).

   If the system is in armed mode (the yellow LED is ON) or in the arm delay period (the yellow LED is flashing slowly), press "#" to disarm the system. Then the system will enter the disarmed mode (the yellow LED will be off).

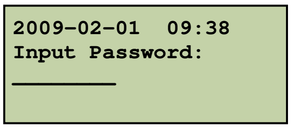
3. In any system mode, press "*" to exit the arm operation. If no key is pressed for 20 seconds, the reader will automatically log out of the arm operation mode.

5.12.5 Arm/Disarm the System using a LCD Reader

New model of readers, ERL-871 in EverAccess series was released to provide a more intuitive user interface to interact with the system. ERL-871 provides a large LCD to show more information from controller.

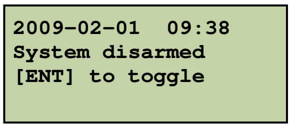
The steps to arm/disarm system with ERL-871 are explained below:

1. Press “*” on keypad, input 8 digits ARM password and press “#” to confirm.



```
2009-02-01  09:38
Input Password:
________
```

2. After entered the ARM menu, press “#” key to arm/disarm the system. Press “*” to exit the system.



```
2009-02-01  09:38
System disarmed
[ENT] to toggle
```

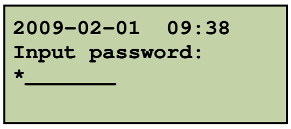
5.13 Use Reader as Keypad

Access control system provides a keypad to control a door and approve or deny an access request. NAV Controller provides the same function with the correct setting.

To use PIN only to access a door, set the door verification mode as “Card or PIN or fingerprint”, and set the keypad reader with the enabled keypad property. When these setting are all configured right, users can key in the valid card PIN at the keypad reader and press # to gain the access. If the PIN matches the records in the system and the door verification mode allows, the controller will unlock the door.

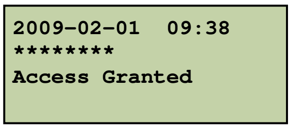
Take the operation on ERL871 LCD keypad reader as example, the steps to use PIN only to access are listed below:

1. Press any numeric key on ERL871 keypad, the below screen will show and the first inputted key will be stored there already:



```
2009-02-01  09:38
Input password:
*_______
```

2. Press “#” key to confirm the inputted PIN. If the PIN is verified OK, the below screen will be shown. If PIN retry failed 3 times, system will show “ERR” on screen and return to the main page of ERL871.



```
2009-02-01  09:38
********
Access Granted
```

Chapter

6

6. Software Introduction

6.1 Main Feature

EverAccess® NAV Controller not only can do basic setting configurations on it, but also can login through the browser (Here and later referred to as “Software”) for system setting configurations. NAV Controller can manage EverAccess Flex I/II/Fingerprint series controller, and also store and maintain the system data.

The Software interface contains clearly defined functional modules. Windows-based structure design facilitates effective management. The main interface provides an over view of operation options and graphical toolbar allows a more intuitive operation.

The Software offers different levels of operation authority to prevent unauthorized access. User name and password is required to login to the Software. The system database is encrypted. User setting is designed to distinguish users with different operation authorities. Users belonging to different authority groups have different operating privileges in the Software. In addition, endures PIN access and multi-card access enhances the efficacy as well as the security of the access control system.

6.2 Hightlight Performance Overview

- Manage different Series Controllers
  - Support ELA890, Flex I, Flex II Access controllers.
- Supports accessory Hardware
  - Support Desktop reader, USB card reader, fingerprint scanner etc.
- Support multiple operating system platforms
  - Compatible with Windows2000 operating system or higher.
- Good user interface design, easy to operate
  - Vista-style user interface
  - New icon design
- Database Management
  - Support for FTP, the local database backup, restore function
- Supports Multiple Language Mode

- ✧ Support Chinese, English, Russian

❖ Software Features

- ✧ Real-time monitoring of controllers, doors, arm zones, alarm input/output and fire alarm on electrical maps, allowing operators to directly monitor system status and responds accordingly.
- ✧ Support remote control of controllers, doors, arm zones and alarms.
- ✧ Support endures PIN access and multi-card access.
- ✧ Size of operating windows and panels can be adjusted.

6.3 Based on TCP/IP Access Conttrol System Architecture

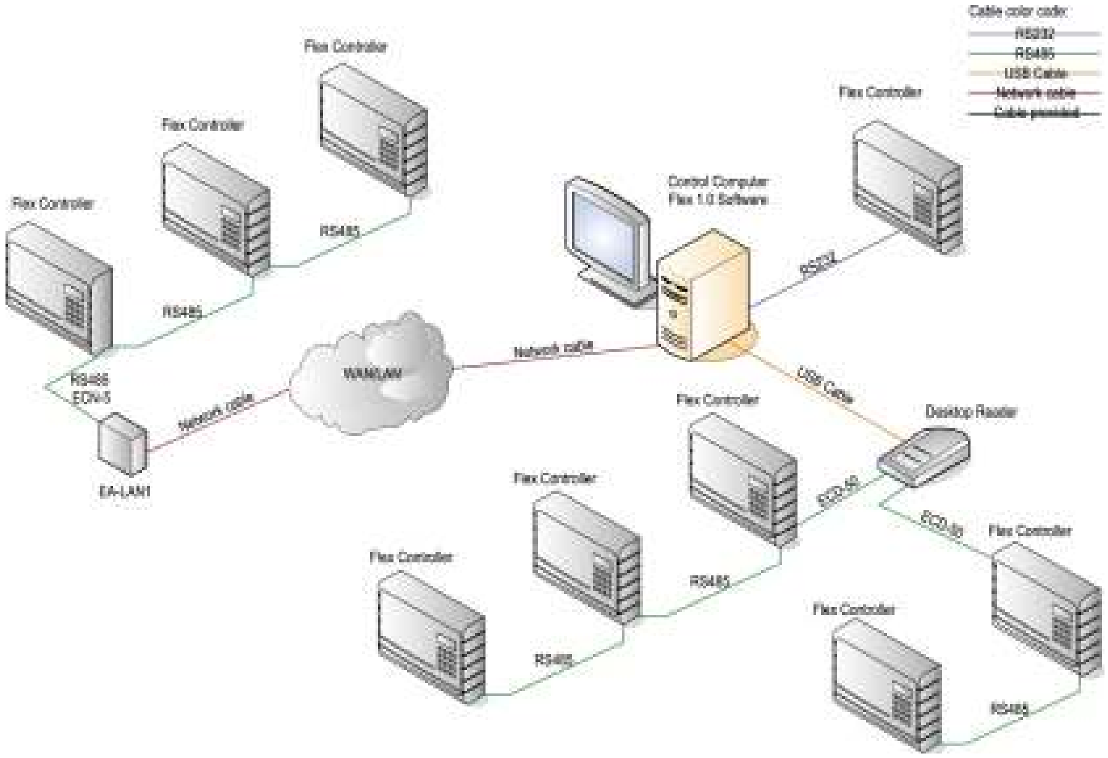


Figure 6-1 System Architecture Diagram

Chapter

7

7. Start to Use

This chapter will instruct how to rapidly set the EverAccess® NAV Controller through the browser using the identity of a super administrator and how to realize door open by swiping a card. For a more comprehensive understanding of each function, refer chapters on related topics.

7.1 Quick Start

7.1.1 Set Access Rule

7.1.1.1 Set Date

Click on the menu bar "Access Control" ➔ "Access Rule" ➔ "Date Type", enter to date type page. Below is how to add a date type (for details, please refer to *13.1.1*)

Steps：

1) Select a recurrent type.
2) Select the date in calendar.
3) Select date type
4) Input a date remark.
5) Click the "Save" button.

7.1.1.2 Set Door Schedule

Please set door schedule before distribute different schedules to each door. Click on the menu bar "Access Control" ➔ "Access Rule"➔ "Door Schedule", enter to the door schedule setting page. Below is how to set a door schedule (for details, please refer to *13.4.1*).

Steps：

1) Click the "Add" button.
2) Input the name of new schedule in the text box.
3) Click the time period of "Daysetting," set time period and entry/exit mode in the pop-up dialog box, save and close the dialog box.
4) Click "Save" and save the completed plan.

7.1.1.3 Set Access Door

Click on the menu bar “Access Control” ➔ “Access Rule” ➔ “Access Door”, enter Access Door Setting page. (for details, please refer to *13.5*)

Steps：

1) Select a door schedule for each door location of controller.
2) Completed setting of door schedule for each door, click the “Save” button and system will prompt a pop-up window “modified successfully”.
3) Click the “Save” button to finish the setting for Door Access.

7.1.1.4 Set Group Schedule

Click on the menu bar “Access Control” ➔ “Access Rule”➔ “Group Schedule”, enter Group Schedule Setting page. Bellow is how to add a group schedule (for details, please refer to *13.2.1*).

Steps：

1) Click the “Add” button to enter the adding page.
2) Input the name of a new schedule in the textbox of “Schedule Name.”
3) Click the time period of “Daysetting,” a dialog box will pop up, in which the time period and the door entry/exit mode can be set.
4) After settings the mode of various date types, click the “Save” button, then the new schedule is added into the Group Schedule list.

7.1.1.5 Set Access Group

Click on the menu bar “Access Control” ➔ “Access Rule”➔ “Access Group”, enter Access Group Setting page. Bellow is how to add an access group (for details, please refer to *13.3.1*).

Steps：

1) Click the “Add” button to enter the adding page.
2) Input the name of a new access group in the “access group name“ textbox.
3) Select the unlocking levels corresponding to the locks.
4) Select a schedule name.
5) Click the “Save” button to finish the settings.

7.1.2 A Variety of Ways to Add Cards

The Web UI provides a variety ways to add the card to the system. Users can choose any way to achieve this functionality. Following are instructions for how to add a card and allocate it into the corresponding control group.

The default control group is “Full Granted” and the default password is “000000.” First, select a format of the card to be added.

7.1.2.1 Rapid Card Addition

When a user logs in to the software and swipes a card on the controller, the card swiping record will be displayed in the system event records and can be copied (for details, please refer to *7.3.5.1*).

Steps：

1) Swipe the card to be added to the card reader connected with the controller in which the card is added.
2) Log in to the Web UI, the card swiping record will appear in the system event records (entry/exit card swiping records or illegal card swiping records). Copy the card number.
3) Select the correct card format.
4) Add one new card in the card page, paste the card number in and click the “Save” button to finish addition.

7.1.2.2 Card Setting Interface

Click on the menu bar “Access Control” ➔ “Card” ➔ “Card Setting”, enter to cards setting. Below is how to add a card and the allocation of access groups (for details, please refer to *14.2.1*).

Steps：

1) Click the “Add” button to enter the card adding page.
2) Fill in card attributes.
3) If the Cardholder member is already in the system, allocate the card to one employee.
4) Select the access group to which the card belongs in the pull-down menu of the “Access Group.”
5) Or click the “Private Schedule” to allocate a special control scheme for the card. When the card has a “Private Schedule” applied, the design is used for authentication in case of door entry/exit and it has the highest control priority.
6) Click the “Save” button to finish addition.

7.1.2.3 Import Cards Using Excel File

In Excel, edit the card data (no quantitative restrictions), save as CSV file to import the card through software features to complete the registration card to the controller (whether registered to the controller of this card depends on the access group setting, if there is no choice access group options, they are given the default access group “Full Granted”).

Click on the menu bar “Access Control” ➔ “Card”➔“Import Cards”

Steps：

1) Export the card report file (.csv) to your computer. Go to ”Access Control” → “Report” → “Card report”, and then click the “Export” button.
2) Open and then edit the card file. Ensure to save the file in **.xls** format.
3) On the Import Cards page, click the “Browse” button and select the Excel file to be imported.
4) Select the desired card info fields to be imported.
5) Click the “Import” button to import the selected card data.

7.1.3 Setup and Cardholder

7.1.3.2 Add a Cardholder

Click on the menu bar “System” ➔ “Cardholder”➔ “Cardholder Setting”, enter to Cardholder Setting page. Here’s how to add a cardholder (for details, please refer to *9.2.1*).

Step：
1) Click the “Add” button, pop-up a page to add cardholder.
2) Fill out employee number, name and other information.
3) You can also add a new card to this cardholder in the Card field.
4) Click the “Save” button to save the setting.

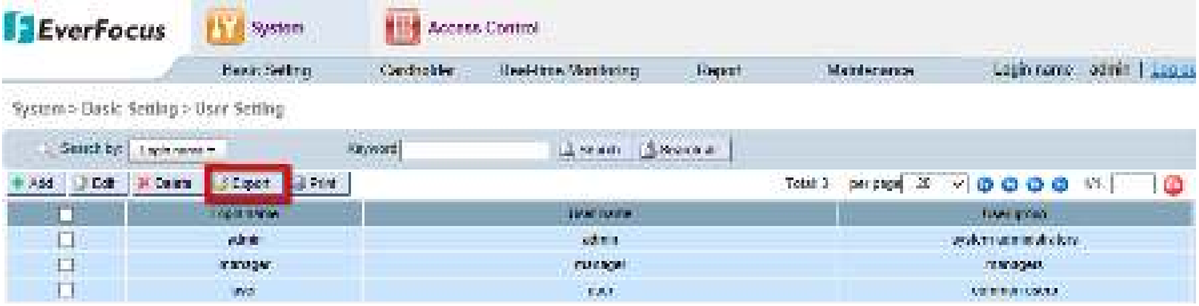
7.1.4 Real-time Monitoring

Click on the menu bar “System” ➔ “Real-time Monitoring” ➔ “Real-time Event”, enter to the Real-time Event page. The upper page displays the real-time status of the electronic map. Users can select different map in the map list on the left hand side of the page.

On the bottom page, it displays the real-time events. Users can click to check the event details.

7.1.5 Export Function

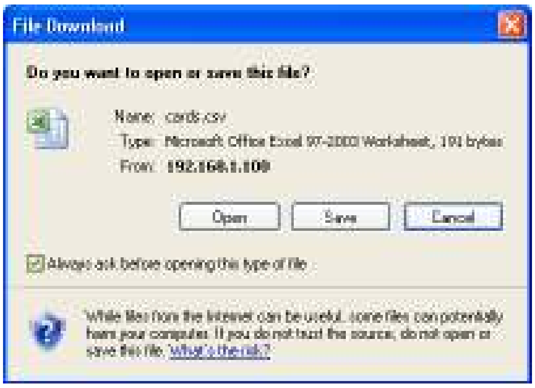
Most setting pages in the system provide an “Export” function for users to export the data on the page.



□	[illegible]	[illegible]	[illegible]
□	admin	admin	[illegible]
□	manager	manager	manager
□	[illegible]	[illegible]	[illegible]

Figure7-1Export Button

Click the “Export” button in any of the pages to export the data in csv format, then the file save dialog box will pop up. See the figure below:



Do you want to open or save this file?

Name: cards.csv

Type: Microsoft Office Excel 97-2003 Worksheet, 191 bytes

From: 192.168.1.100

☑ Always ask before opening this type of file

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

Figure7-2 Export

Click the “Save” button; select a path to save the exported document, shown as following:

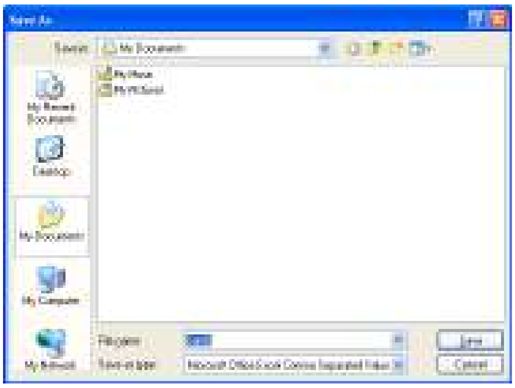


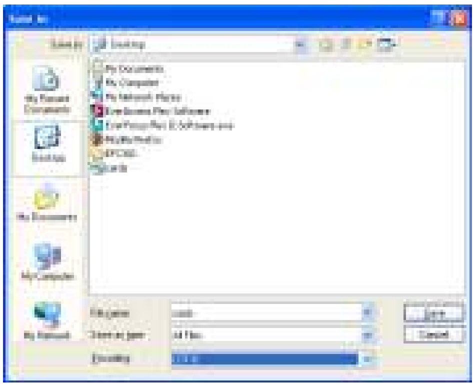
Figure7-3 Save

Select the path and click “Save” button, export CSV format file to complete.

! Note: If Chinese characters are included in the content, file conversion will be required or the Chinese characters will be garbled. Please refer to the instructions below to convert the import/export files.

Steps:

1) Right-click the saved CSV file, select “Edit” in the drop-down menu.
2) By default, the file will be opened using Notepad. Select “File” in the menu bar → “Save as,” then the dialog box will pop up. See the figure below:



File name: user

Save as type: All Files

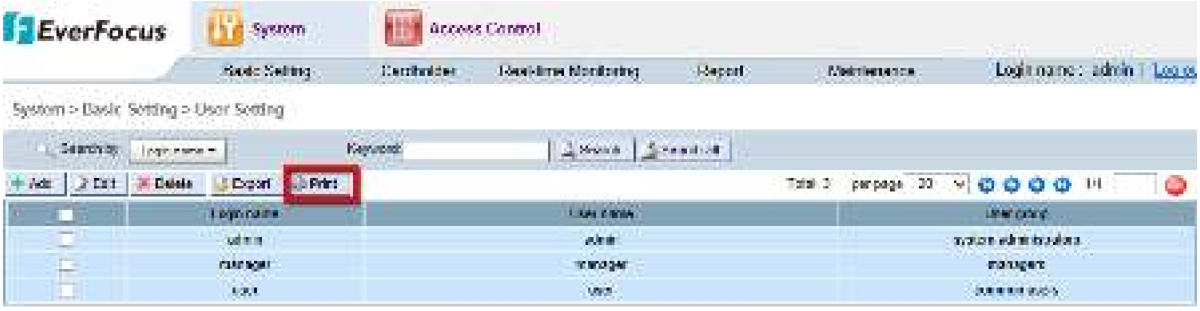
Encoding: UTF-8

Figure 7-4 Convert the Exported File

3) In the dialog box, select Save as type “All Files”, select encoding “UTF-8”.
4) Click the “Save” button, the conversion is completed.
5) Open the converted file via Excel, the Chinese characters are normally displayed.

7.1.6 Print Function

Most setting pages in the system provide a “Print” function. Click the “Print” button to enter the printing page (Figure 7-2) and then you can print the data on the current page.



System > Basic Setting > User Setting

□	Login name	User name	User group
□	admin	admin	system administrators
□	manager	manager	managers
□	user	user	common users

Figure7-3 Print Button

7.2 Login

Open browser and input the IP address of the controller in the address bar. If the user does not carry out any settings for the IP address, the default IP address of the controller will be 192.168.1.200. Following the prompts on the page, input login name, password and identifying code and Click the "Log on" button to login. See Figure 7-4:

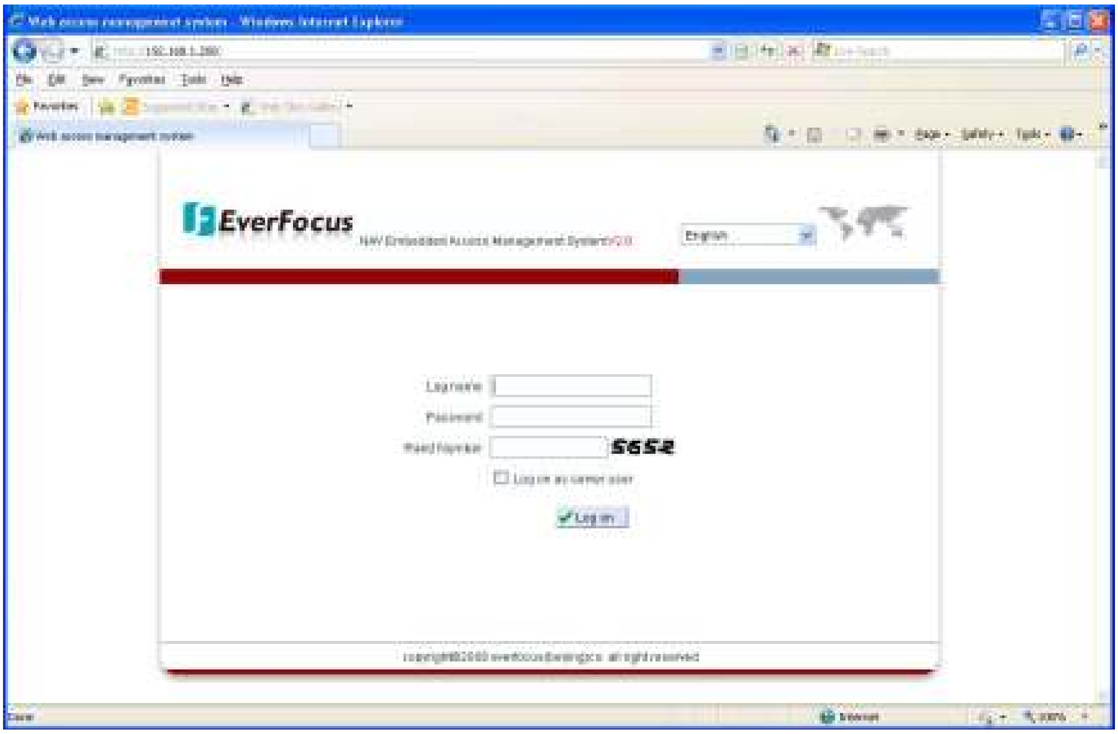


Figure 7-6Login Page

You can select the language of the operation page at the upper right corner of the page. The default login setting shown as following:

User Name: admin
Password: admin

Note: admin is a special "super administrator" which is mainly used for system installation and restoration. The "super administrator" has all authority for operating the software and is unchangeable. The user itself can not be deleted and only the password can be changed. Please change and remember well the password after the first login to ensure the security of the software.

The password of the super administrator is carried out through "System" ➔ "Basic Setting" ➔ "Change Password." The super administrator can create users and change the authority of the user through "Basic Setting" ➔ "User Group" ➔ "Add." If all other users are deleted and the password of the super administrator is lost, then the software cannot be accessed.

After inputting a username and password in the login page, select whether "login with the identity of central server user," and then click the "Login" button to enter the browser page of the controller.

If the username or password is wrong, a dialog box indicating illegal login will pop up. See Figure 7-7:

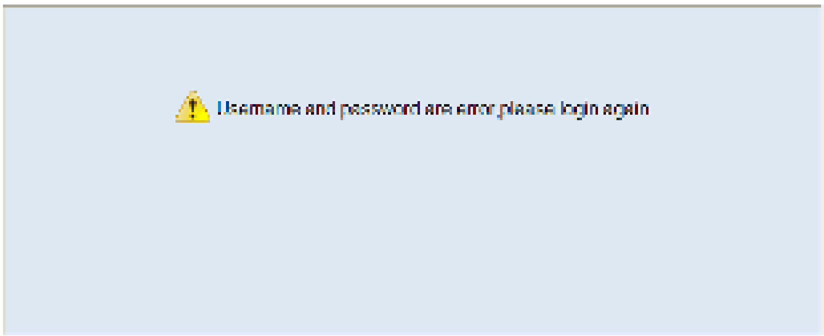

Username and password are error,please login again

Figure7-7 Illegal Login

7.3 Get Familiar with the Browser Page

7.3.1 Main Page Introduction

The page adopts a humanized design concept to ensure users get familiar with it as soon as possible. After logging in to the system, the user will enter the main page of the program. See the figure below:

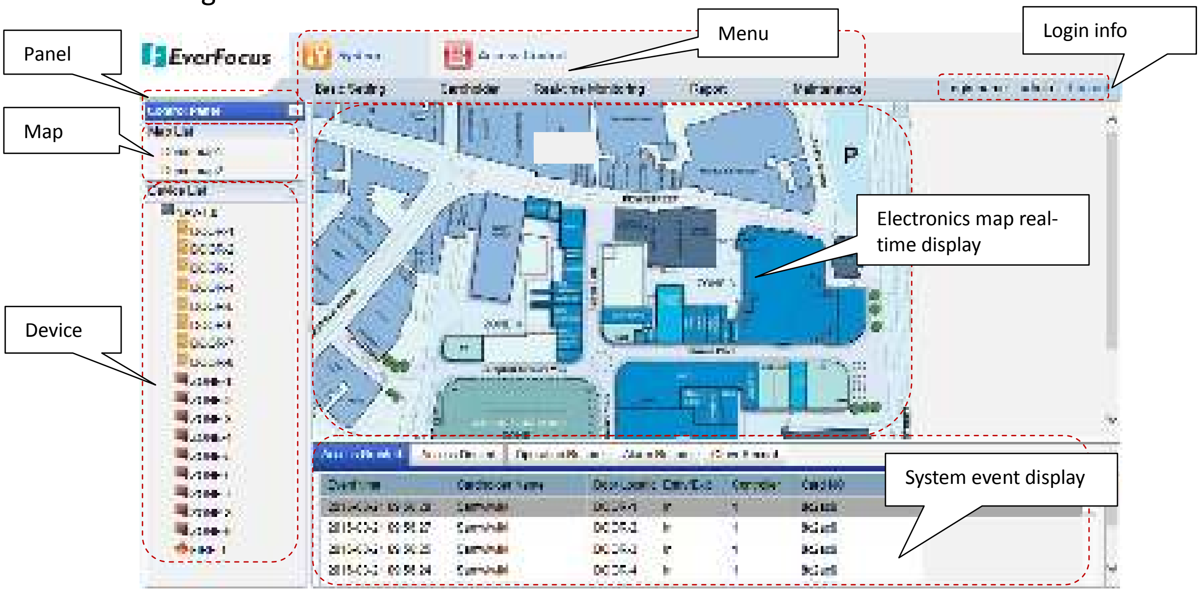


Figure 7-5Main Page

7.3.2 Menus

The menu is composed of the System and Access Control (see Figure 7-9). Click each main menu item to expand its submenu options and click each option of the submenu to start the corresponding function. The specific functions will be introduced in detail in the latter chapters.

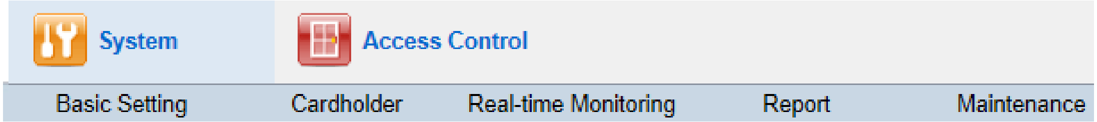


Figure7-6Menu

If a login user has no access authority to a certain module function, the function will not be displayed on the menu bar.

7.3.3 Control Pannel

Click Control Panel below the menu, then the "Control Panel" on the left side of the main page will be hidden (see Figure 7-11). When user clicks the button or double clicks the hidden bar, the list will be displayed and the main page is restored to the original.

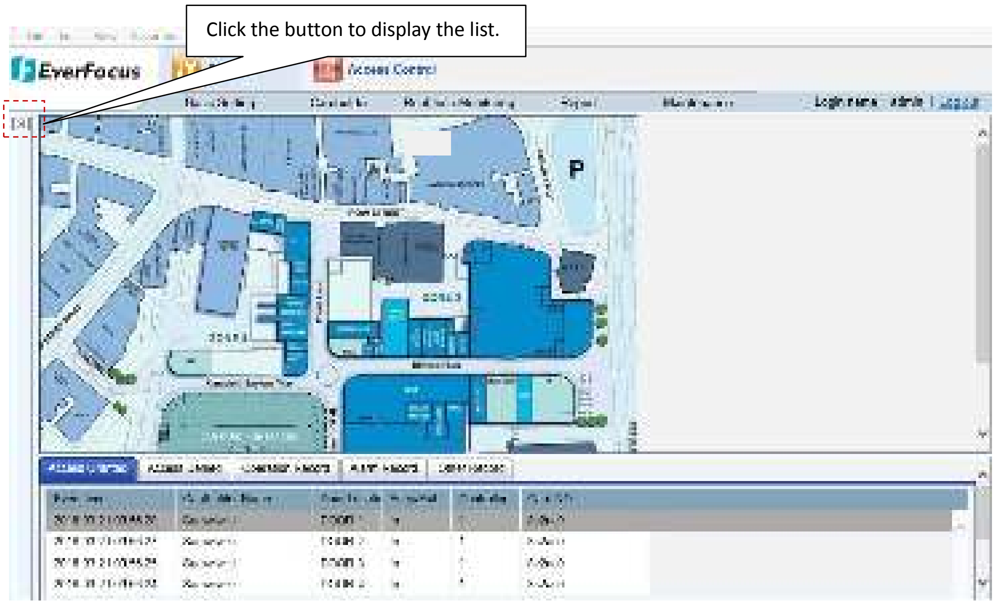

Click the button to display the list.

Figure 7-7Hide the Left Side of Control Panel

7.3.3.1 Electronic Map list

This area shows the complete setting of electronic map structure in the software (Figure 7-9). Please refer to 10.2 for detail of adding, deleting and revising of electronic map.

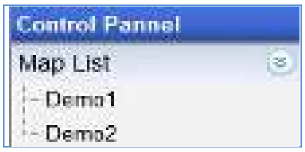
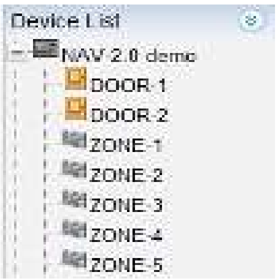


Figure 7-8Electronic Map

7.3.3.2 Device List

This area displays effective devices which have been configured by the software. If controller have been added or deleted or revised, it will be showed in this area.



Device List

- NAV 2.0 demo
  - DOOR-1
  - DOOR-2
  - ZONE-1
  - ZONE-2
  - ZONE-3
  - ZONE-4
  - ZONE-5

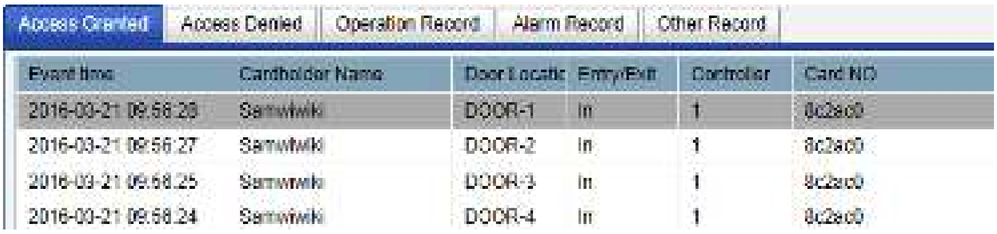
Figure 7-9 Device List

7.3.4 Real-time Monitoring

This feature displays real-time electronic map status, users can click on "Electronic list" to switch different electronics maps and keep track of system state. For more detail about adding, revising and deleting of electronic map, please refer to 10.2.

7.3.5 System Event Record

The region displays all the event records of the system, including access granted, access denied, operation record, alarm record, other record.

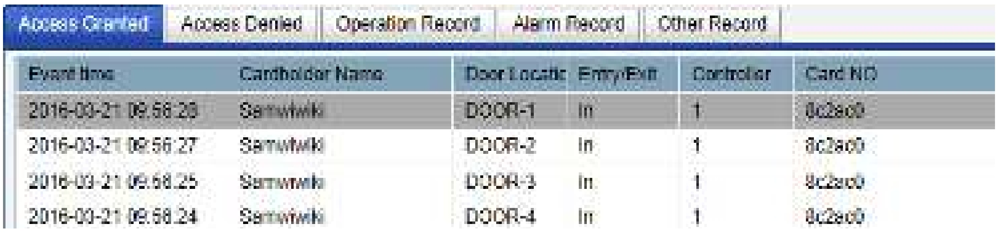


Event time	Cardholder Name	Door Locatic	Entry/Exit	Controller	Card NO
2016-03-21 09:56:28	Samwiwiki	DOOR-1	In	1	8c2ac0
2016-03-21 09:56:27	Samwiwiki	DOOR-2	In	1	8c2ac0
2016-03-21 09:58:25	Samwiwiki	DOOR-3	In	1	8c2ac0
2016-03-21 09:58:24	Samwiwiki	DOOR-4	In	1	8c2ac0

Figure 7-10 Event Record

7.3.5.1 Access Granted

This type of record includes normal card swiping records and password door open records. The content of the entry/exit card swiping records includes event time, cardholder name, entry or exit and card number.

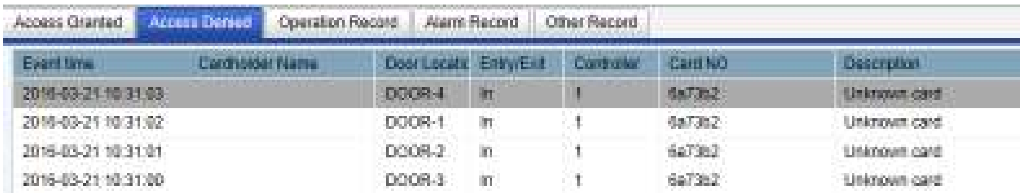


Event time	Cardholder Name	Door Locatic	Entry/Exit	Controller	Card NO
2016-03-21 09:56:28	Samwiwiki	DOOR-1	In	1	8c2ac0
2016-03-21 09:56:27	Samwiwiki	DOOR-2	In	1	8c2ac0
2016-03-21 09:58:25	Samwiwiki	DOOR-3	In	1	8c2ac0
2016-03-21 09:58:24	Samwiwiki	DOOR-4	In	1	8c2ac0

Figure 7-11 Access Granted

7.3.5.2 Access Denied

This type of record includes Unknown card, Expired card, Invalid card, Password retry failed, Enter with panic PIN, Insufficient multi-card access, Invalid time,. Invalid door, APB fails, No PIN inputted, Man trap violation, Access denied due to unknown card PIN.

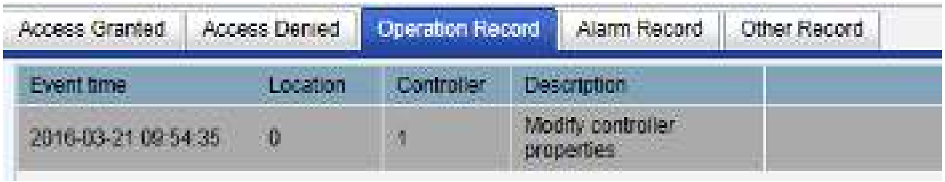


Event time	Cardholder Name	Door Locati	Entry/Exit	Controller	Card NO	Description
2016-03-21 10:31:03		DOOR-4	in	1	6a73b2	Unknown card
2016-03-21 10:31:02		DOOR-1	in	1	6a73b2	Unknown card
2016-03-21 10:31:01		DOOR-2	in	1	6a73b2	Unknown card
2016-03-21 10:31:00		DOOR-3	in	1	6a73b2	Unknown card

Figure7-12 Access Denied

7.3.5.3 Operation Record

This type of record includes the records of the remote operation of the controller in the software, the records of protection setup/withdrawal on the controller, the records of restore alarm, the records of door open with the door open button, etc.

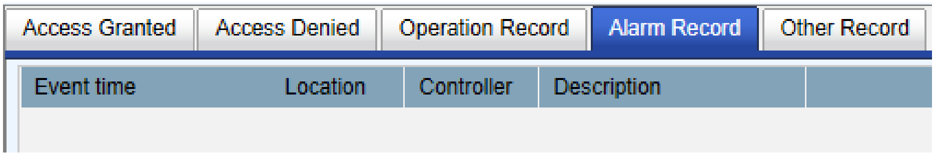


Event time	Location	Controller	Description
2016-03-21 09:54:35	0	1	Modify controller properties

Figure 7-13 Operation Record

7.3.5.4 Alarm Record

This type of record includes zone alarm, fire alarm, system password error, zone password error, tamper alarm, remote alarm, forced open door, panic open door, open door overtime and reader lose

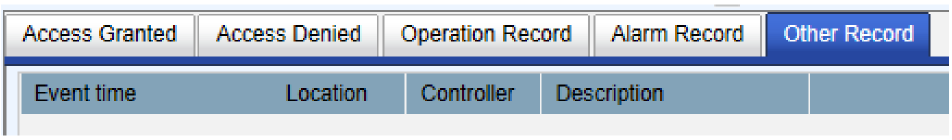


Event time	Location	Controller	Description

Figure 7-14 Alarm Record

7.3.5.5 Other Record

In the system, other records which related to the controller setting, including event loss, power-down, add reader, controller on line, controller off line and controller power-up.



Event time	Location	Controller	Description

Figure 7-15 Other Record

Chapter

8

8. Basic Setting

This chapter will introduce the Basic Setting of the EverAccess® NAV controller in detail, which includes changing passwords, User Group, User Setting, Local Server, system upgrade and central server configuration.

Change password: Change login password.

User Group: Add, delete and change the User Groups in the software. The quality of the User Groups has no limit and the user can add the User Group(s) as required.

User Setting: Add, delete and change the user who can log in to and use the software. By default, the software generates admin as a super user who has all the operation authorities of the software. The user can only change the password of the super user.

Local Server: Set the IP type, address, gateway, date, time, etc. of NAV controller.

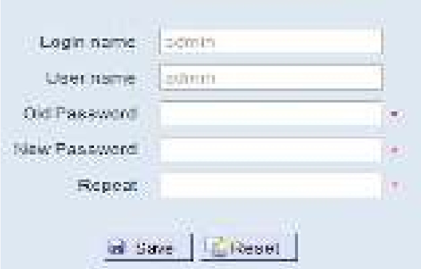
System upgrade: Support online upgrade and local upgrade.

Central server configuration: Configure the system settings.

8.1 Change Password

The changed password is the login password by which the user logs in to the embedded software of NAV Controller through the browser and only the current login password can be changed.

First, input the old password, then input the new password and input the new password again and then click the "Save" button. The contents of the new password and repeat password must be the same. If the input content has an error, click the "Reset" button to fill it in again.



Login name	admin
User name	admin
Old Password	*
New Password	*
Repeat	*

Figure 8-1 Change Password

8.2 Set up User Group and User

In the system, one user means one person who operates the software. Due to different authorities, the used pages may be different. Each user is defined by four attributes: Name, login name, password and authority.

“Name” should be the true name of the user. “Login Name” is the identity to be input when the user accesses the login dialog box of the system. “Password” is the password to be input when the user accesses the login dialog box of the system. “Authority” will be introduced in detail below.

Note: “User” and “Cardholder” are different. A cardholder is a person who goes in or out of the Access Control system (such as a common employee of a company), while the user is the person who monitors or configures the Access Control system through the software.

Authority defines the limited level of the user operating the software. Different authorities have different software operation limits.

Click the menu bar “System” ➔ “Basic Setting” ➔ “User Group” to enter the User Group page. For detailed settings, please refer to *8.3 User Group*. When entering the “User Group” in case of first use of the software, the system will automatically initialize the User Group.

The software has three default authorities: System administrator, manager, common user. Each authority has no limit on the user quantity.

System administrator: The user can use all functions of the software system, including Basic Setting, Cardholder, Access Control, database management, etc.

Manager: The user can use all functions of the software system except Basic Setting.

Common user: The user can use all functions of the software system except Basic Setting and database management.

The table below lists the specific functions of each authority, and “√” indicates if the function is available in the corresponding authority.

Function		system administrator	manager	common user
System	Change Password	√	√	√
	User Groups setting	√		
	User Setting	√		
	Local Server	√	√	
	System Update	√		
	Center Server	√		
	Cardholder Setting	√	√	
	Real-time Event	√	√	√
	Edit Electronic Map	√	√	
	Cardholder Report	√	√	√

	Data Backup	√	√	
	Data Recovery	√	√	
	Purge Out-of-date Data	√	√	
Access	Controller Setting	√	√	
	Date Type Setting	√	√	
	Access Door Setting	√	√	
	Door Schedule Setting	√	√	
	Access Group Setting	√	√	
	Group Schedule Setting	√	√	
	Card Setting	√	√	
	Import Card	√	√	√
	Card Report	√	√	√
	Card-dependent Event	√	√	√
	Card-independent Event	√	√	√

Figure8-1Feature List of Each Group

The group “system administrator” cannot be edited or deleted. The other two groups can be edited or deleted.

8.3 User Group

In the User Group page, the current User Group list in the system is displayed on the left side. The user who has the authority of User Group can carry out User Group creation, change and deletion operations in this page.

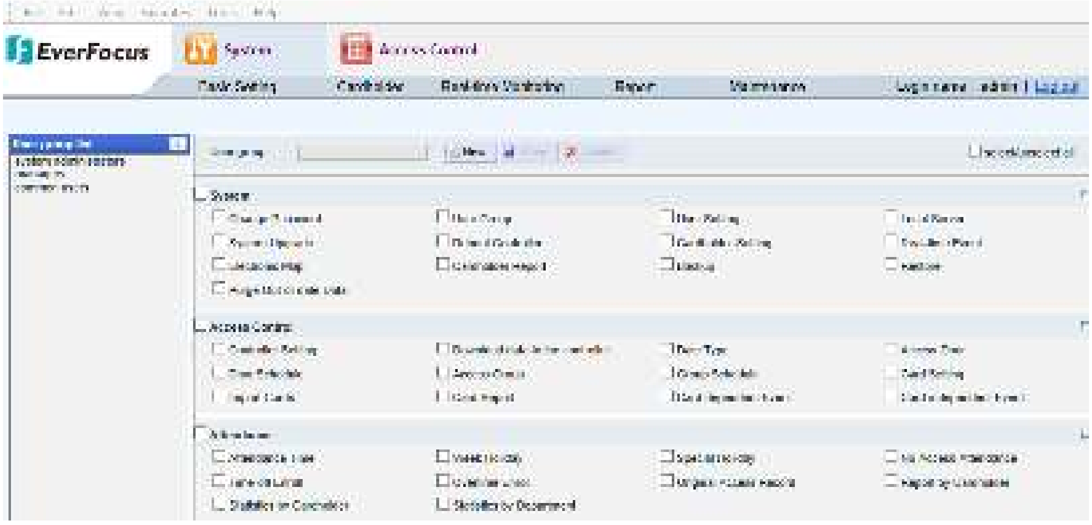


Figure 8-2 User Groups

8.3.1 Add a Group

Click the "New" button on the upper side of the page, input the name of the new User Group in the box of "Name of User Group," tick off the detailed operation authorities of the User Group, edit and click the "Save" button to finish the operations.

8.3.2 Edit a Group

Select the name of the User Group to be changed in the left-side User Group list, change the name and detailed operation authorities of the User Group, edit and click the "Save" button to finish the operation.

8.3.3 Delete a Group

Select the name of the User Group to be deleted in the left-side User Group list, click the "Delete" button, then the confirmation dialog box "Confirm Delete?" pops up. If it is confirmed to delete the User Group, click the "OK" button, then the system displays a dialog box reading, "Deleted Successfully."

NOTE: The User Group which is being used by the user cannot be deleted.

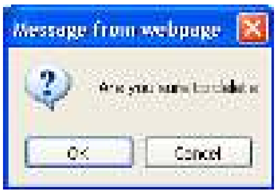


Figure 8-3 Confirm to Delete a Group

8.4 User Setting

User Setting are used to create, change and delete users and define the authority types of these users. The user herein actually refers to the account which can log in to and use the software. Please distinguish with “Employer.” The user includes login name, password, User Group, username, etc. The software has a default super user, “admin,” which belongs to the User Group of system administrator and cannot be deleted.

Click the menu “System” ➔ “Basic Setting” ➔ “User Setting” to open the User Setting page. See Figure 8-4.

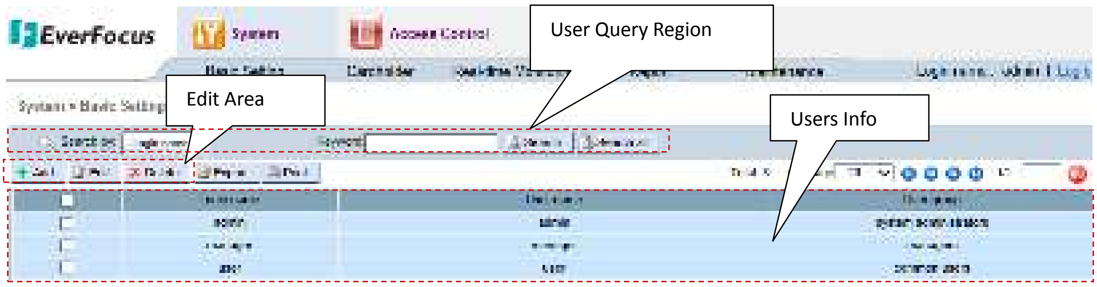


Figure8-4 User Setting

8.4.1 Add a User

In the page, click the “Add” button in “Function Editing Region,” then the user addition page pops up (see Figure 8-5). Input the login name, username, password and User Group name and click the “Save” button to add a new user to the user list in the page.

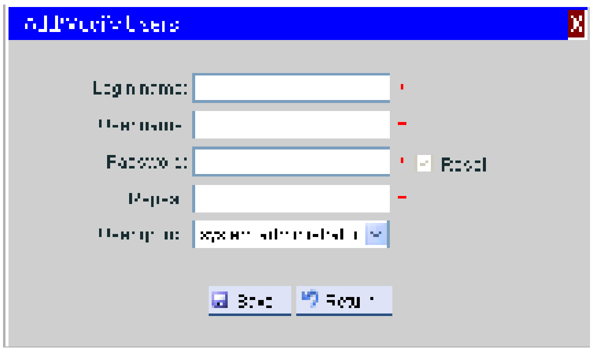


Figure8-5 Add a User

Login name: The name for the user to log in and use the software, which can be any combination of figures, letters, spaces, Chinese characters and other displayable characters. The longest login name is 20 bits and any character occupies 1 bit. **The letters of the login name are case sensitive.** The login name cannot be the same as an existing user login name and cannot be empty. If the user inputs an existing login name, the system will prompt that the login name has already been used when saving it.

User name: The true name of user. This item is for facilitating system management and must be filled in.

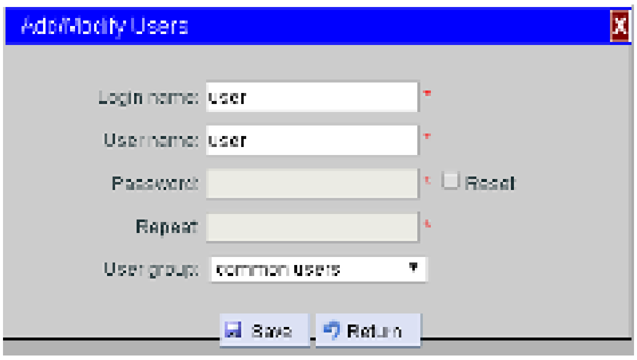
Password: Any combination of figures, letters, spaces, Chinese characters and other displayable characters. The longest login name is 20 bits and any character occupies 1 bit. **The letters of the login name are case sensitive.**

Repeat: Must be the same as the input content of the password. If the two passwords input are not consistent with each other, the system will prompt that "Input Password Do Not Match."

User Group: Name of the User Group to which the user belongs. The administrator can allocate the new user to any User Group and the User Group of the system administrator can operate all functional modules.

8.4.2 Edit a User

Select the column in which the user to be changed is located and click the "Edit" button, then the user edition dialog box pops up (see Figure 8-6).The login name, username, password and User Group of the user can all be changed. In case of resetting the login password of the user, check "Reset Password," edit, and click the "Save" button, then the system displays a dialog box reading, "Operation Successfully." In case of not changing, click the "Cancel" button to return to the "User Setting" page.



Login name: user *
Username: user *
Password: * □ Reset
Repeat: *
User group: common users

Figure8-6Edit a User

8.4.3 Delete a User

Select a user to be deleted, click the "Delete" button, the system will pop-up a box to confirm "Are you sure to delete?", click "OK" to delete.

Note: The default user "admin" cannot be deleted.

8.4.4 Export Users

Click the “Export” button to export all user information in the system in the csv format, then the file save dialog box pops up. Select the path to save the file and click “OK.” For detailed operation procedures, please refer to 7.1.7.

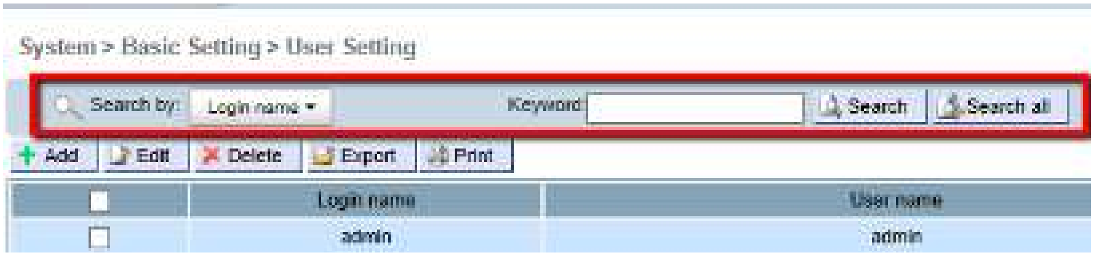
8.4.5 Print Users

Click the “Print” button to enter the user information printing page. Please refer to 7.1.8 for detail.

8.4.6 Search Users

Select login name or username in the pull-down menu of “Search” in “Search Editing Region,” input the content to be searched for and then click the “Search” button. If there is information meeting the conditions in the system, the information will be displayed in the user information list region below (see Figure 8-7). If you want to look over all the users in the current controller after searching, click the “All” button.

Note: “Search” herein refers to a precise search.

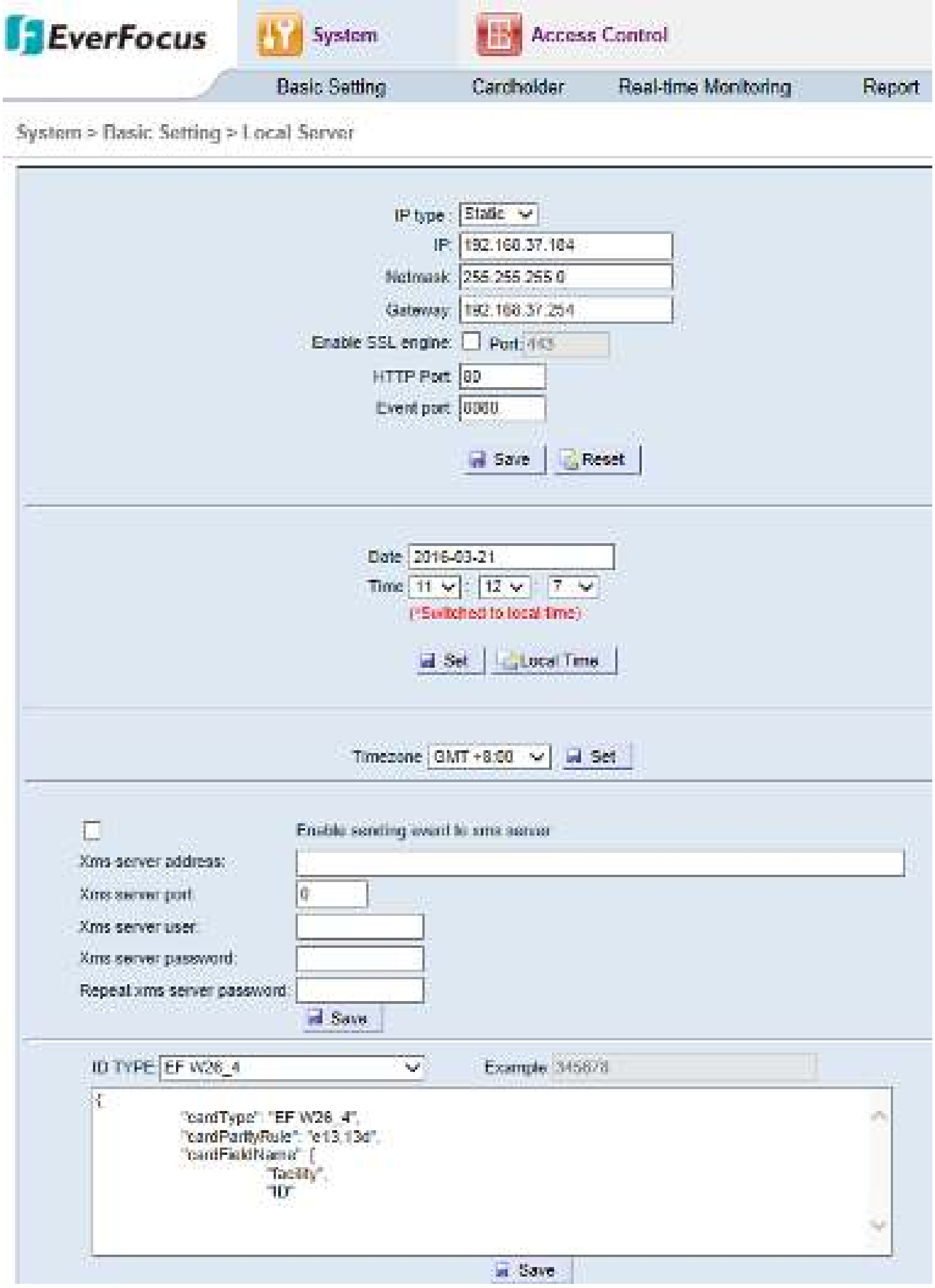


□	Login name	User name
□	admin	admin

Figure 8-7 Search Users

8.5 Local Server

The Local Server can set the IP, time, data and time zone of the currently logged-in controller. Click the system main menu “System” → “Basic Setting” → “Local Server” to enter the Local Server page.



IP type : Static

IP: 192.168.37.184

Netmask: 255.255.255.0

Gateway: 192.168.37.254

Enable SSL engine: □ Port: 443

HTTP Port: 80

Event port: 8080

Date: 2016-03-21

Time: 11 : 12 : 7

(*Switched to local time)

Timezone: GMT +8:00

□ Enable sending event to xms server

Xms server address:

Xms server port: 0

Xms server user:

Xms server password:

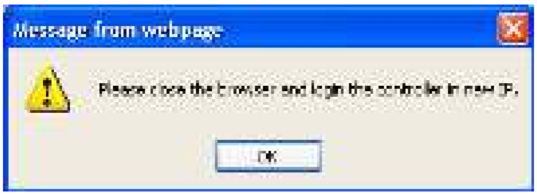
Repeat xms server password:

ID TYPE: EF W26_4 Example: 345678

```
{
        "cardType": "EF W26_4",
        "cardParityRule": "e13,13o",
        "cardFieldName": [
                "facility",
                "ID"
```

Figure8-8 Local Server

Click the IP type as in the above figure, select static or dynamic type, input IP, subnet mask and gateway in the textbox, confirm and click the “OK” button. The page will display this prompt dialog box:


Message from webpage

Please close the browser and login the controller in new IP.

Click “OK” again and re-log in to the controller using the changed IP address.

Click the “Reset” button to read and display the network settings in the current controller in the page input box.

Click the “Local Time” button and the time of the controller will synchronize with the local time. The required time can also be set by the user. Click the “Set” button to save the time settings.

Select the required time zone or the time zone where the location is located, click the “Set” button to complete the controller time zone settings.

Enable sending event to xms server: Check the box to enable sending events from controller to the XMS server.

Xms server address: Input the IP address of the XMS server.

Xms server port: Input the port number of the XMS server. The default port number is 80.

Xms server user: Input the user name of the XMS server.

Xms server password: Input the password of the XMS server.

Repeat xms server password: Input the password of the XMS server again.

ID Type: Before adding cards to the controller, select an ID type (card format) from the drop-down list for this controller and then click the “Save” button. The card format information will be displayed in the Example and below column fields which cannot be modified.

Note: If you also adopt EverFocus’ ENS2000 software for central management, you can edit or add new card formats to the controller through ENS2000. For more details, please refer to *4.3.1 Card Format* in *ENS2000 User’s Manual*.

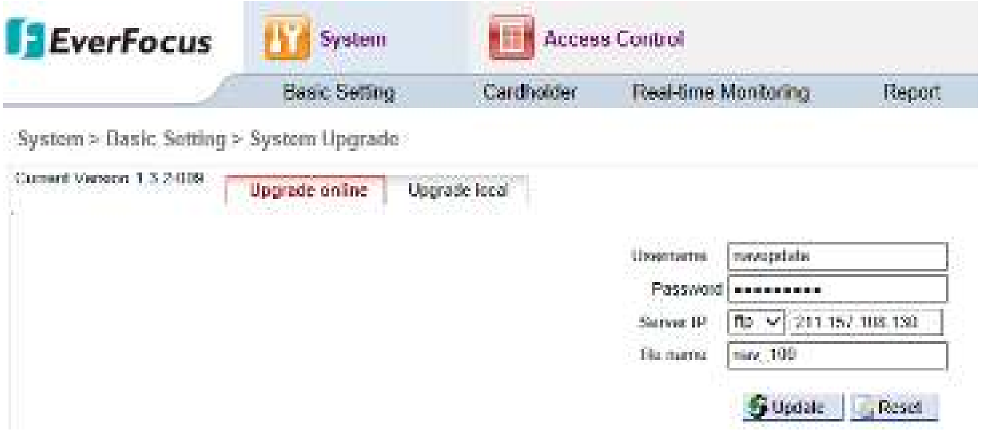
Note: If your controllers have been connected to the ENS2000 software, once the card format has been set up in the ENS2000 software, the connected controllers will be automatically applied with the same card format.

Note: You can further configure the event settings for ENS2000 in the XMS server. For more details, please refer to *4.3 Event* in *Genie XMS User’s Manual*.

8.6 System Upgrade

The firmware of controller and built-in software can be upgraded to the latest version as the user needs by the operation. There are two ways including remote on-line system update and local update.

Click system main menu "System" →"Basic Setting" →"System Upgrade", enter to the system upgrade page, as following (Figure 8-10), the default entry is online upgrade page.



Current Version 1.3.2408

Username: navupdate

Password: ••••••••••

Server IP: ftp 211.157.108.130

File name: nav_100

Figure8-9Online Upgrade

8.6.1 Online Upgrade

The upgrade is carried out through the FTP or HTTP address and account provided by the service provider. As in the above figure, after inputting the accurate address and account, click the "Update" button, then online upgrade starts. After the online upgrade is finished, please re-log in.

8.6.2 Local Upgrade

The upgrade is carried out locally through the upgrade package provided by the service provider. Click the "Browse" button, select the upgrade package, click the "Upload" button, then the local upgrade starts. After the local upgrade is finished, please re-log in.

Chapter

9

9. Cardholder

This chapter will introduce the Cardholder Setting of the NAV Controller in detail, including setting up employee number, name and other information of a Cardholder, and allocate one or more card for Cardholder and set the attributes.

9.1 Cardholder Setting

Click on the menu bar “System” ➔ “Cardholder” ➔ “Cardholder Setting” to enter the Cardholder Setting page; see the figure below:

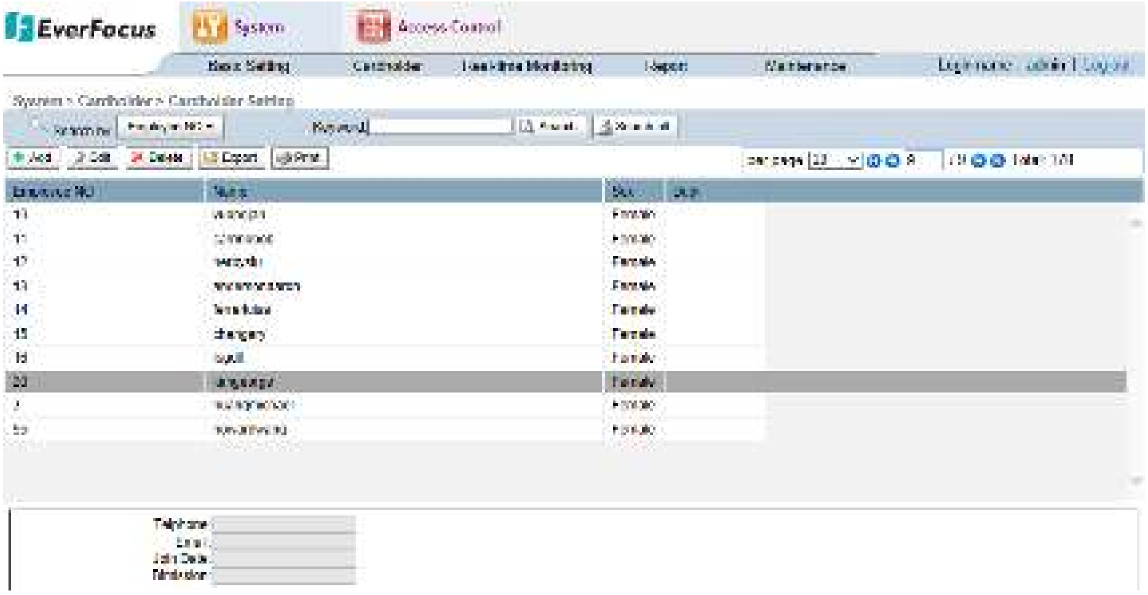


Figure9-1 Cardholder Setting

As in the above figure, the upper part of the page is the query region, the middle line is the operation region and the lower part is the Cardholder information list.

In the operation region on the upper right corner of the page, the number of Cardholder information items displayed per page can be set. By default, 20 records are displayed per page. In addition, the page turn button and jump button are helpful for users to rapidly access the desired page. See the figure below:

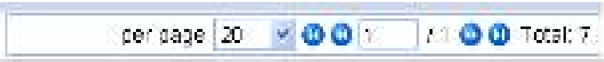
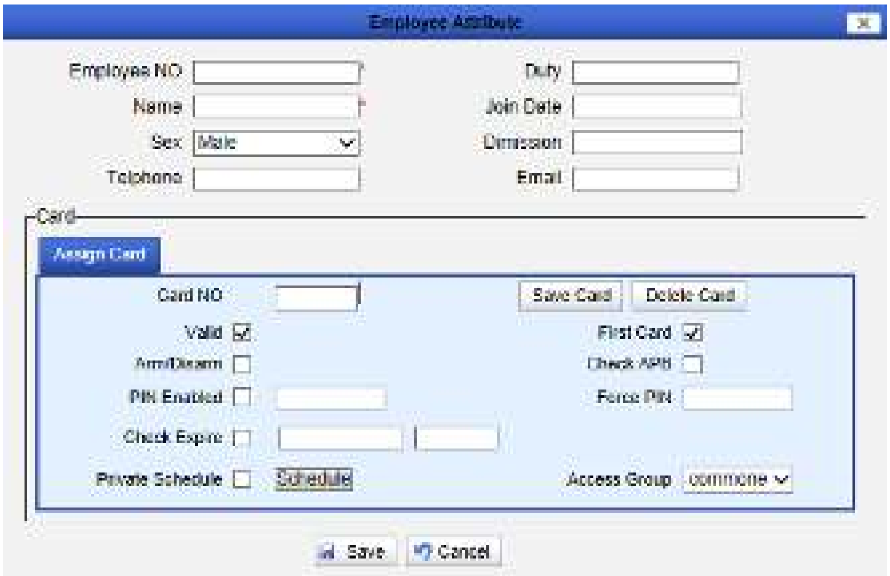


Figure9-2 Operation Area

9.1.1 Add a Cardholder

Click the “Add” button and the Cardholder Setting registration page pops up; see the figure below:



Employee Attribute

Employee NO □ *
Name □ *
Sex: Male
Telphone □
Duty □
Join Date □
Demission □
Email □

Card

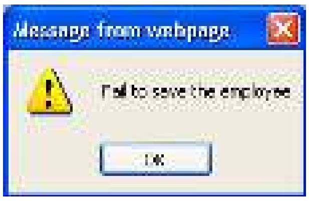
Assign Card

Card NO □
Valid ☑
Arm/Disarm □
PIN Enabled □
Check Expire □
Private Schedule □
First Card ☑
Check APB □
Force PIN □
Access Group: commone

Figure9-3 Add a Cardholder

1) **Cardholder Information Area:** This area is setting cardholder’s basic information.

Employee number: can be any printable character, it is a unique number for a cardholder. If new member joined, the new number cannot be same as existing number. System will prompt “Fail to save the employee”.

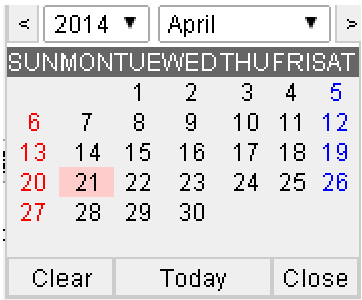


Message from webpage

Fail to save the employee

Figure9-1Fail to save the employee

Name: input cardholder’s real name.
Sex: input the cardholder’s gender. The system default setting is “Male”.
Telephone: input the cardholder’s telephone number.
Duty: input the cardholder’s duty.
Join Date/Demission date: When clicking the input box with mouse, a time selection box pops up, in which the employment date of Cardholder is selected; year and month are selected in the upper part and the day is selected in the middle part.



SUN	MON	TUE	WED	THU	FRI	SAT
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Figure 9-2Pop-up the Calendar Box

Email: input the cardholder’s email address.

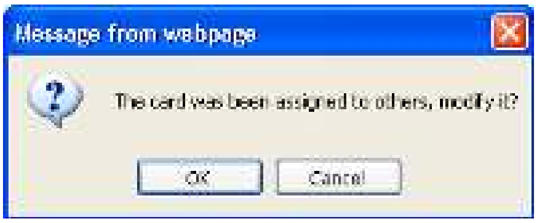
! Note: The employee number and name of Cardholder must be filled in; other parameters are optional. However, we recommend that you fill in all information so as to display more visual information in case of querying.

2) **Card Information Area：**The items in this region can rapidly add one or more cards for the currently added Cardholder and can set the related attributes of the card(s).

The card information is mainly to correlate the Cardholder and the card. You can directly input the internal code (in most cards, a string of figures or symbols printed on the back of the card) of the card to be correlated, or connect with the ERU Series USB desktop card reader (please refer to the operating instruction manual for ERU Series hardware) and read the internal code of the card by swiping the card.

Add a Card: Input card number, click the “Save Card” button to save the card number. If the card to be registered is the same as the card in the system, the system will display a dialog box as below. One user can hold one or more cards.

! Note: Before adding a card, please ensure the card format you want to add is the same with the one of controller’s. To check the card format, see “ID Type” in *8.5 Local Server.*



Message from webpage

The card was been assigned to others, modify it?

Figure 9-3 Assigned to other cardholder’s Card

Delete an assigned Card: Select the tab of the card to be deleted, click the “Delete Card” button to delete the card.！ **Note: This operation is real-time processing.**

All the properties of a card are shown as below. Check or uncheck the boxes to enable or disable the functions.

Valid: Indicates whether the registered card is activated. Check this item to activate the card. The other attributes of the card may not act until the card is activated. The card will be invalid in case of not checking.

First Card: It indicates that the card held by the Cardholder is the first card and is used for opening the door when setting normally opened function of the door region. If the controller 0001 sets the door to be normally opened at a.m. 9:00-11:00, during this period of time, the Cardholder holding the card with the first card attribute swipes the card on the card reader under the controller to activate the normally opened state of the door in the corresponding door region.

Arm/Disarm: Whether the cardholder has the right to arm/disarm the system on a keypad reader. When an arm enabled card is presented to the reader, the system will be disarmed for a time period so that the cardholder can enter/exit the arm zone without triggering an alarm. This time period is defined by arm delay time in the system.

Check APB: Whether anti-passback (APB) is enabled for the card. If APB_EN is enabled for a card, and the controller APB function is enabled, the APB setting is in effect for the card. Refer to Anti-Passback (APB) setting for details

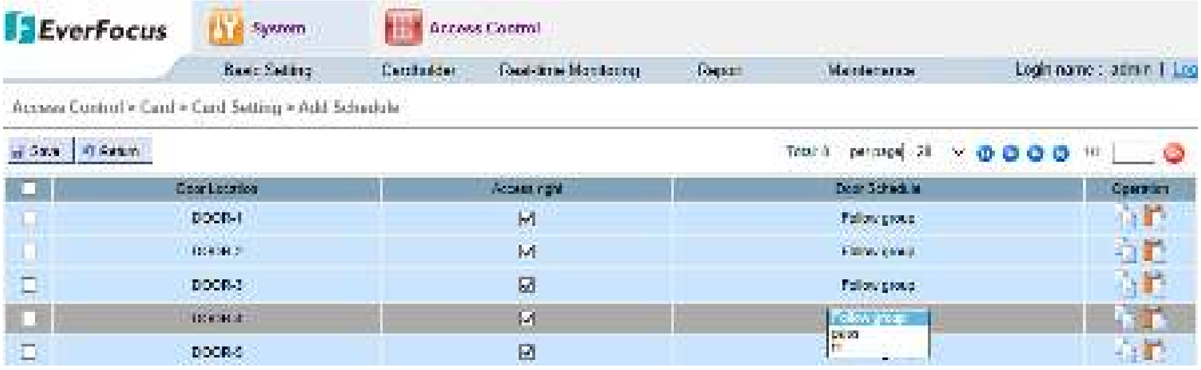
PIN Enabled: Cardholder can set up an 8-digit door password for NAV Controller. To enable/disable, use functions in door setting, access authority setting or card schedule setting.

Note: To use the password feature, the reader connected to the controller must feature a keypad function.

Force Pin: The duress password is used for raising an alarm when the cardholder opens the door under duress and is only valid when the door is set to open with a password. The duress password has 2 digits. In case of using the duress password, first input the first 6 digits of the normal password and then input the duress password and confirm, then the alarm is generated and the door is opened.

Check Expire: whether the card has an expiration date. If Card Expiration is checked, the card can only be used within the expiration date. An expired card cannot gain access to the system and an “expired card” event will be generated if an expired card is swiped on a reader. The time set in the expiration date is the end of the expiration date. It can be accurate to minute.

Private Schedule: refers to the verification mode for cardholders to enter/exit doors. Card schedule setting is shared with access group schedule setting. To select a special card schedule for a card, user needs to add a new schedule in “access group schedule setting” and then apply the schedule for the card in “card schedule”. If "card schedule" is enabled, the system will follow the card schedule. In this situation, door verification control will not be applied to this card.



Access Control » Card » Card Setting » Add Schedule

☐	Door Location	Access right	Door Schedule	Operation
☐	DOOR-1	☑	Follow group	
☐	DOOR-2	☑	Follow group	
☐	DOOR-3	☑	Follow group	
☐	DOOR-4	☑	Follow group	
☐	DOOR-5	☑		

Figure9-4Card Schedule Setting

Select different access schedule for different door zone. Different access schedule will specify the card which has one kind entry rule for each door zone.

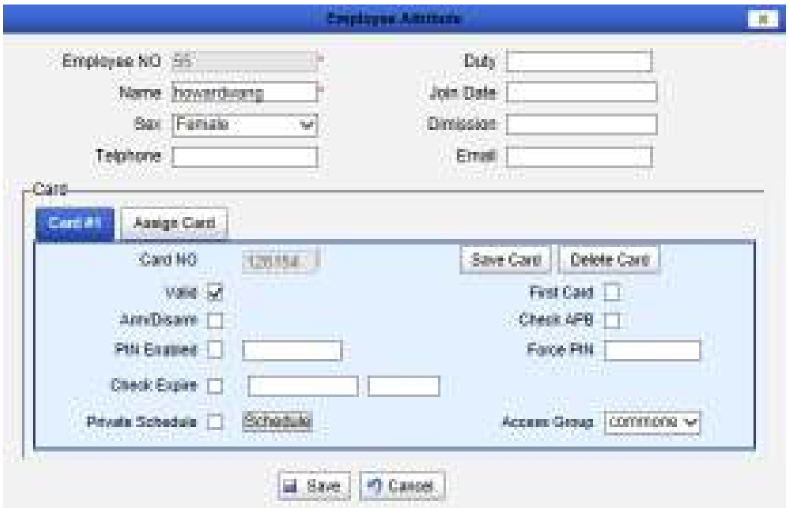
Note: All cards in one group can be assigned to different access group in different controller.

Access Group: The card can be assigned to 2048 kinds of access groups, different groups will be set a different access rules.

When all the information is filled in and the card setting is finished, click the “Save” button to save the settings.

9.1.2 Edit a Cardholder

Select a cardholder in the cardholder list to be edited, click the “Edit” button. Enter to the cardholder edit page, shown as following.



Employee NO	55	Duty	
Name	howardwang	Join Date	
Sex	Female	Dimission	
Telphone		Email	

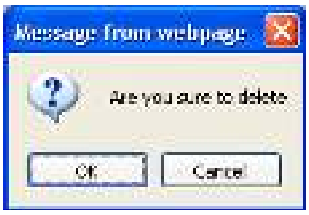
Card NO	126154		
Valid	☑	First Card	☐
Arm/Disarm	☐	Check APB	☐
PIN Enabled	☐	Force PIN	
Check Expire	☐		
Private Schedule	☐	Access Group	commons

Figure 9-5Edit a Cardholder

Edit a cardholder’s information is similar to adding a cardholder. After edition is complete, click the “Save” button to save the changes.

9.1.3 Delete a Cardholder

Select a cardholder in the cardholder list to be deleted, click the “Delete” button, op-up as below:



Message from webpage

Are you sure to delete

Figure 9-6Confirm to Delete a Cardholder

Click the “OK” button to confirm.

In case of deleting the information of several Cardholder members, press “Shift” on the keyboard while selecting the columns of the Cardholder to be deleted and click the “Delete” button, then the confirmation box “Confirm delete?” pops up. Click “OK” to delete the information of all of the selected Cardholder.

9.1.4 Export Cardholder Information

Click the “Export” button to export all user information in the system in the csv format, then the file save dialog box pops up. Select the path to save the file and click “OK.” For detailed operation procedures, please refer to *7.1.7 Export Function*.

9.1.5 Print Cardholder Information

Click the “Print” button to enter the user information printing page. For detailed operation procedures, please refer to *7.1.8 Print Function*.

9.1.6 Search Cardholders

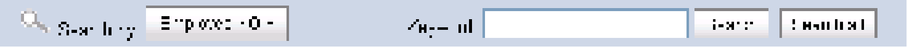


Figure9-7 Search Cardholders

The “Query” condition includes employee number and name. First select query condition, and input the keyword related to the character field in the textbox after “Keyword.” After inputting the query condition, click the “Search” button, then the system will list the results meeting the condition. Click the “All” button, then the system will list all Cardholder information in the system. The query herein is a precise query and the result will not be listed unless the query condition and the keyword are completely met.

9.3 Import Cardholders

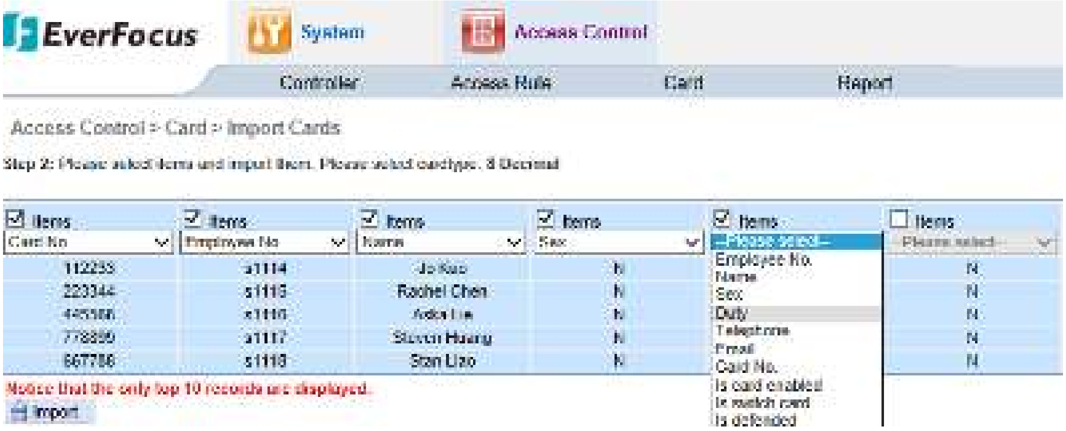
You can import multiple cardholder information together with card information to the controller through csv file. Please follow the steps below:

Steps:

1) Export the excel format from “Card Setting” page (Access Control < Card < Card Setting). Go to the “Card Setting” page, click the “Export” button, save the csv file in your computer.
2) Open the exported csv file to edit the cardholder and card information. The file size is limited to 1M.

   ! Note: If Chinese characters are included in the csv content, file conversion will be required or the Chinese characters will be garbled. Please refer to *7.1.5 Export Function* to convert the exported files.

3) To import the csv format file, go to the “Import Cards” page (Access Control < Card < Import Cards), click the “Browse” button to import the edited csv file.
4) Click the “Next” button to enter the operation page.



Access Control > Card > Import Cards

Step 2: Please select items and input them. Please select cardtype. 8 Decimal

☑ Items	☑ Items	☑ Items	☑ Items	☑ Items	□ Items
Card No	Employee No	Name	Sex	--Please select--	--Please select--
112233	s1114	Jo Kao	N		N
223344	s1115	Rachel Chen	N		N
445566	s1116	Aida Lie	N		N
778899	s1117	Steven Huang	N		N
667788	s1118	Stan Liao	N		N

Notice that the only top 10 records are displayed.

Figure9-8Import Cardholders

5) Check the items you wish to add to the controller and then select each attribute of the item from the drop-down list.
6) Click the “Import” button to start importing.
7) After the Import process is complete, a “xxx records have been imported.” message will be displayed. You can click the “Return” button to return to the Import Cards page.

Chapter

10

10. Real-Time Monitoring

10.1 Real-Time Event

Click on system menu bar "System" → "Real-time Monitoring" → "Real-time Event", to enter the Real-time events page; see figure below:

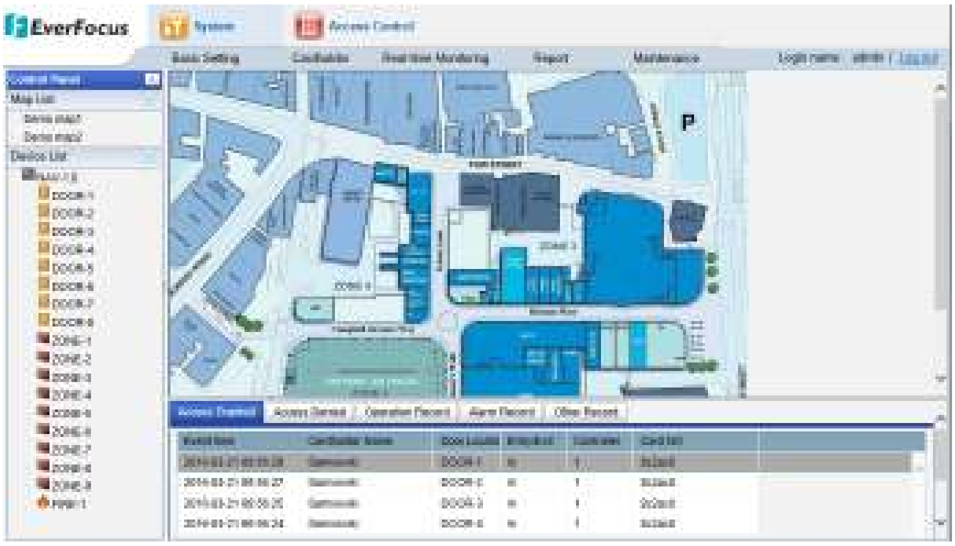


Figure10-1Real-time Event

As shown in the above figure, the real-time monitoring page is divided into three areas:

Control Panel: The Map list and device list located on the left side Control Panel, which contains the map list, controllers and doors, arm zones, DVR, CAM and View. Users can remotely control open/close, set alarm etc.

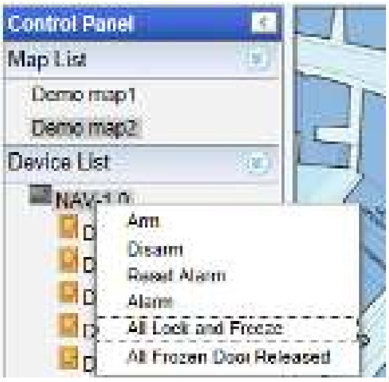
Electronic Map: Electronic map is located on the center page.

Real-time Event: The real-time event records are located at the bottom page. It automatically receives the event information of the controller and scrolls the event information to display in real time. In case of accessing the page for the first time, the events of the controller are sequentially listed according to the sequence of being received. When receiving a new event, it automatically lists the latest event in the first line.

! Note: substation only caches some real-time event records. When the user enters the real-time event record page at the first time, it only displays some real-time event record of the station. For previous events, users need to go to card access inquiry page to search events.

10.1.1 Remote Operation

Left-click a controller node in the Device List and its corresponding function menu pops up. You can remotely operate the functions from the menu, such as arm, disarm, reset alarm and add map etc. Left-click a door node in the Device List and its corresponding function menu pops up. You can remotely operate the functions from the menu, such as "Open Door" and "Close Door".



10.2 Edit the Electrical Map

Click on the menu bar "System" → "Real-time Monitoring" → "Electronic Map" to enter the Electronic Map edit page:

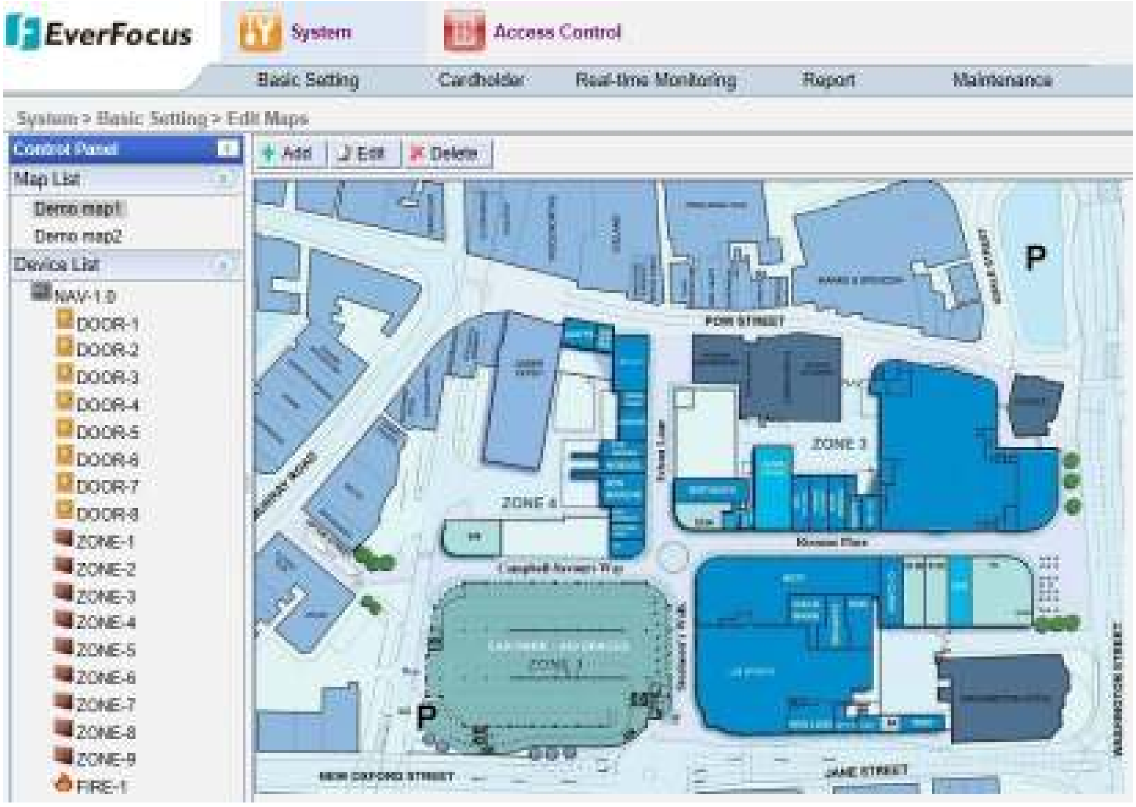


Figure10-2Edit Electronic Map

10.2.1 Add an Electronic Map

Click the “Add” button, the below window pops-up:

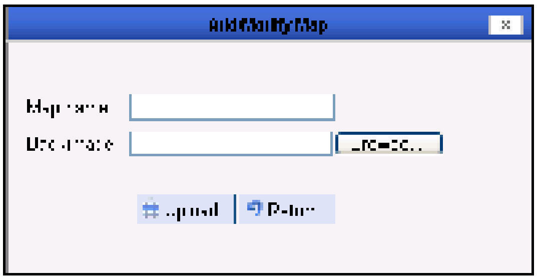


Figure10-3 Add an Electronic Map

Map name: name for a new electronic map.

Back Image: click the “Browse” button to add a floor plan image to this map. After loading an image, click the “Upload” button to upload the image. Click the “Return” button to return to the previous page.

10.2.2 Edit an Electronic Map

Select a map to be edited from the Map List and then click the “Edit” button to enter the edit page.

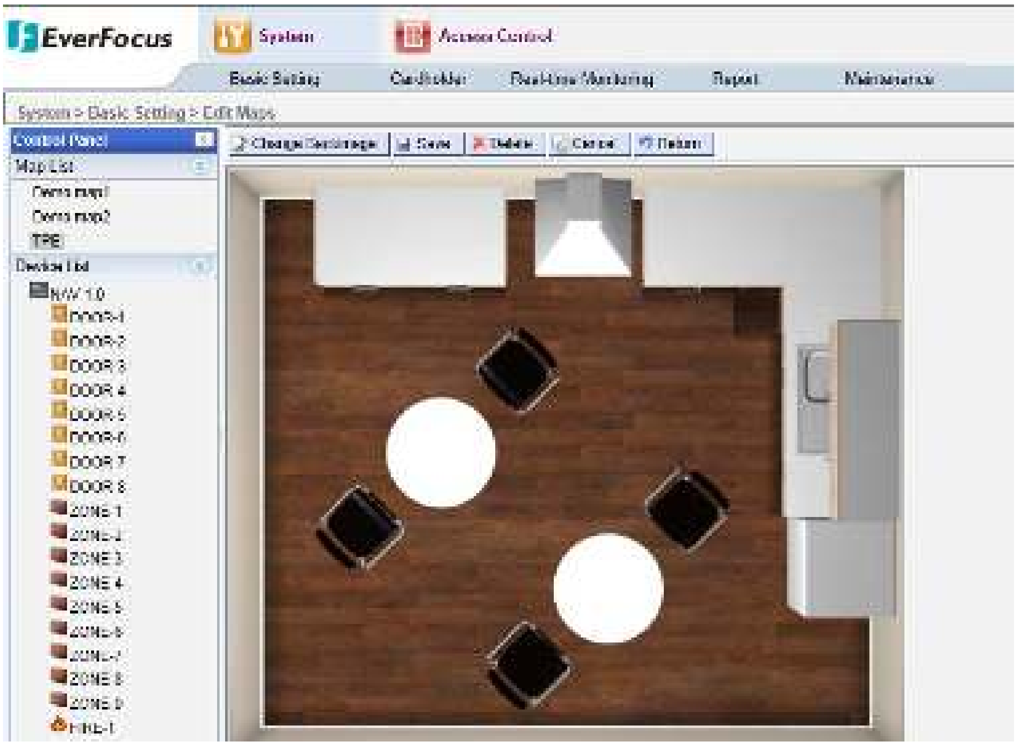


Figure10-4 Edit an Electronic Map

There are 5 operating buttons in the edit area: Change Backimage, Save, Delete, Cancel and Return. See figure below:

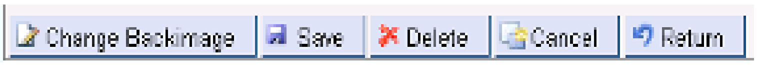


Figure 10-5 Operating Button

To change a floor plan image:

Click the Change "Backimage" button, click the "Browse" button to add a floor plan image to this map. After loading an image, click the "Upload" button to upload the image. Click the "Return" button to return to the previous page and then click the "Save" button to save the changes.

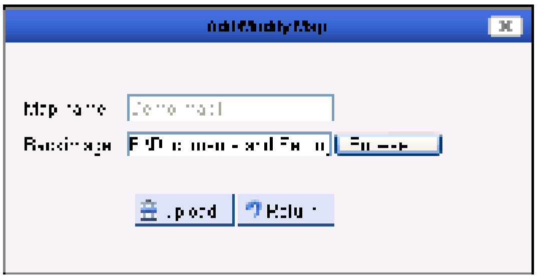


Figure10-6Back Image Setting

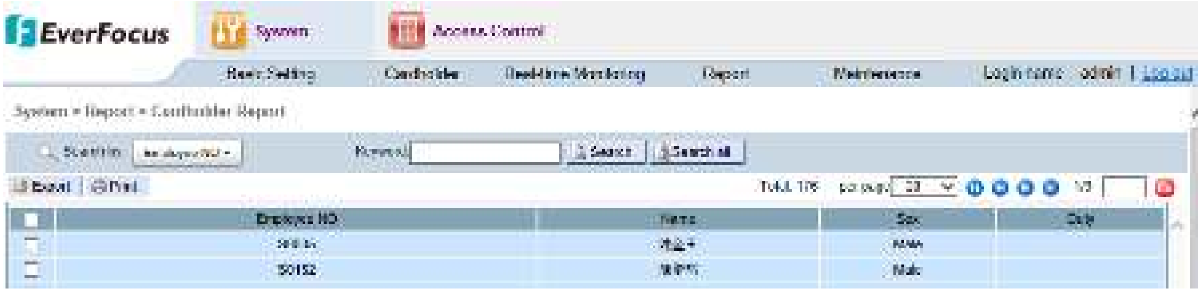
To delete a map:

Select a map to be deleted from the Map List and then click the "Delete" button. Click "Ok" to confirm.

10.3 Report

10.3.1 Cardholder Report

Click on system menu "System" → "Report" → "Cardholder Report" to enter the page below:



□	Employee NO	Name	Sex	Duty
□	[illegible]	[illegible]	[illegible]	
□	50152	[illegible]	Male	

Figure10-7Search Cardholders

Input the employee number or name to do precise queries.

Search condition is divided into employee number, name. Input the keyword in the box, click the "Search" button, will show all the related results with keyword. Click "All" button, to get back to the all cardholder list. The query is exact and the results listed will fully match the keyword.

For example, employee numbers “ef-001” and “ef-002” are available in the system. If you want to query “ef-001,” select “employee number” as a query condition, input “ef-001” in the keyword input box and Click the “Search” button. In case any character is missing, the user cannot be found.

10.3.2 Export Cardholder Information

Click the “Export” button, and the download file box will pop-up. All cardholders’ information will be exported to a CSV file. Select a path to save the document. Please see *7.1.7 Export Function*.

10.3.3 Print Cardholder Information

Click the “Print” button to enter the cardholder printed page, for the specific operation methods see *7.1.8 Print Function*.

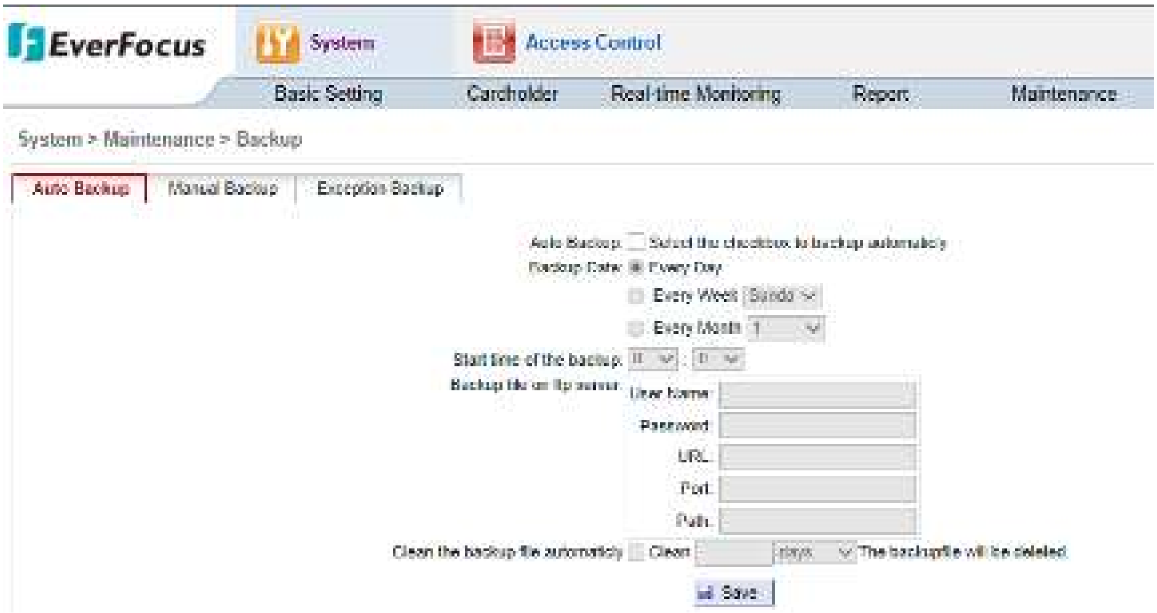
Chapter

11

11. Maintenance

11.1 Backup

Click the menu “System” → “Maintenance” → “Backup” to enter the backup page; shown as below:



Auto Backup: □ Select the checkbox to backup automaticly

Backup Date: ● Every Day

○ Every Week Sunda

○ Every Month 1

Start time of the backup: 0 : 0

Backup file on ftp server: User Name: Password: URL: Port: Path:

Clean the backup file automaticly □ Clean days The backupfile will be deleted

Figure11-1Backup

11.1.1 Manual Backup

Manual backup refers to backup of system data in the local server through the operation of the administrator. Select the “Manual Backup” item and click the “Backup” button, then the backup file will be saved in the local computer.

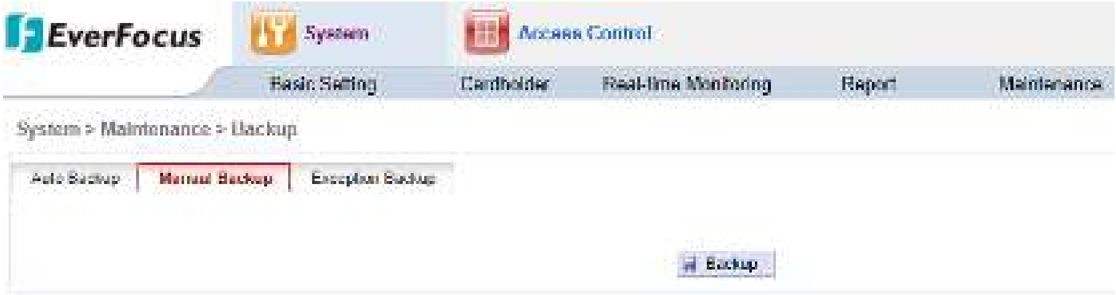
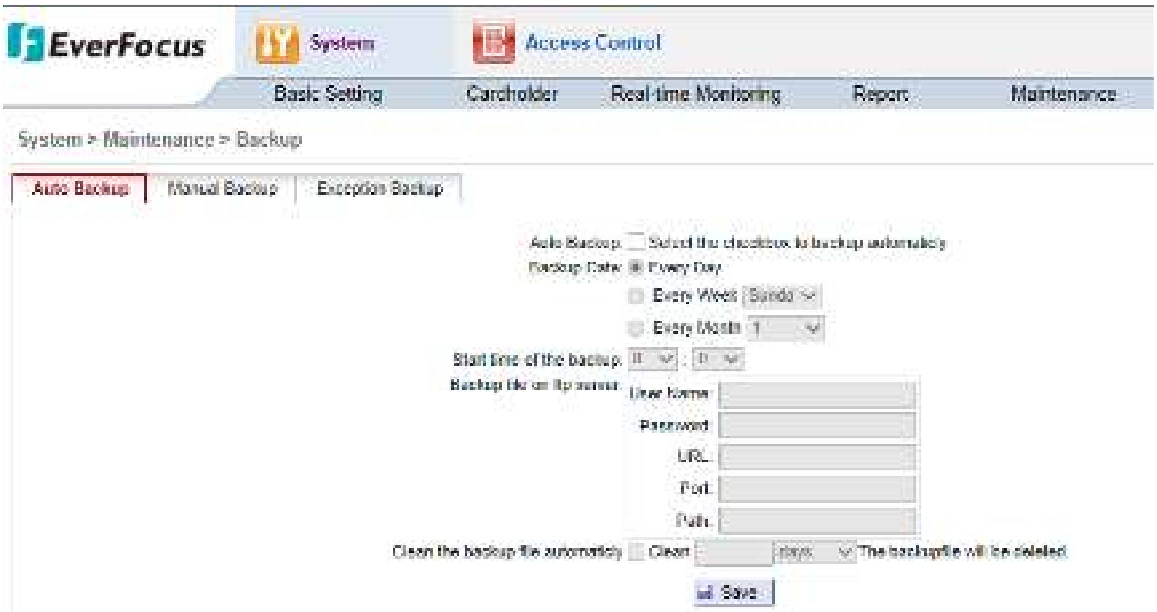


Figure11-2Manual Backup

11.1.2 Auto Backup

You can automatically back up the system data. The automatic backup page is shown as below:



Auto Backup: □ Select the checkbox to backup automaticly
Backup Date: ● Every Day
○ Every Week Sunda
○ Every Month 1
Start time of the backup: 0 : 0
Backup file on ftp server: User Name: Password: URL: Port: Path:
Clean the backup file automaticly □ Clean days The backupfile will be deleted

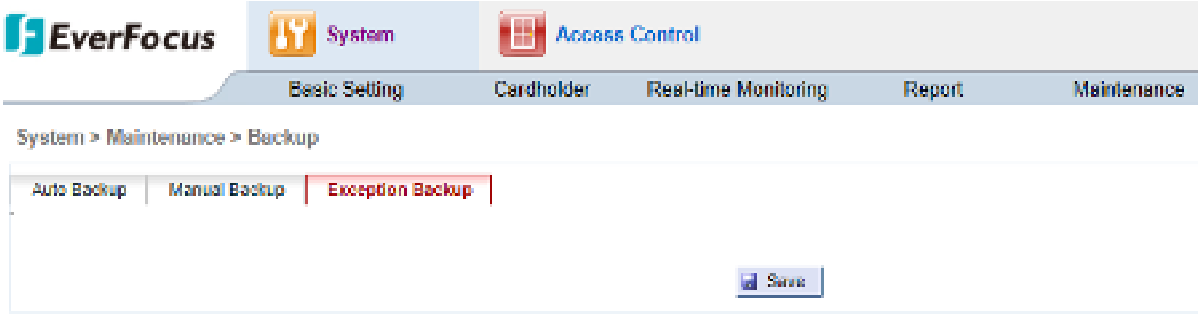
Figure11-3Auto Backup

Steps:

1) Check to enable automatic backup.
2) Select the date and start time of automatic backup.
3) Set the username, password, URL, port and file save path of the backup file in the FTP server. (FTP server refers to remote server)
4) Select whether to clean the expired backup file during the automatic backup period.
5) Click the “Save” button to finish operation.

11.1.3 Exception Backup

The Exception Backup is for EverFocus’ technical team to analyze system data. If you encounter some problems required EverFocus technical team to help, you can contact EverFocus along with this Exception Backup file.



11.2 Restore

Click “System”→ “Maintenance” → “Restore” to enter the page to restore data. The system provides two methods: Restore the database from a FTP server, or from the local computer.

11.2.1 Restore from a FTP Server

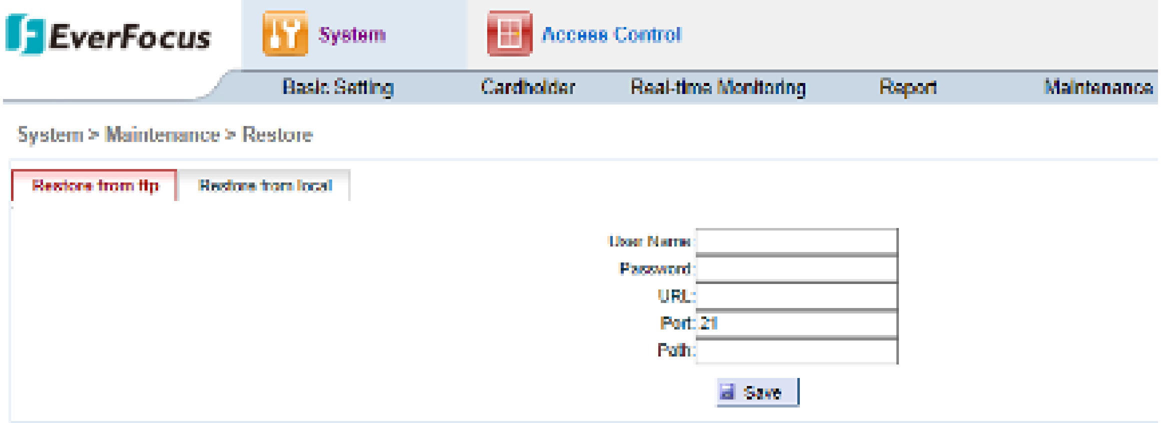


Figure11-4 Restore the Databasefrom a FTP Server

Steps:

1) Fill in the username and password to log in to the FTP server.
2) Input the FTP server’s URL, port, and file path (e.g.: abcd/nav_0808183801).
3) Click the “Save” button.

11.2.2 Restore from Local Computer

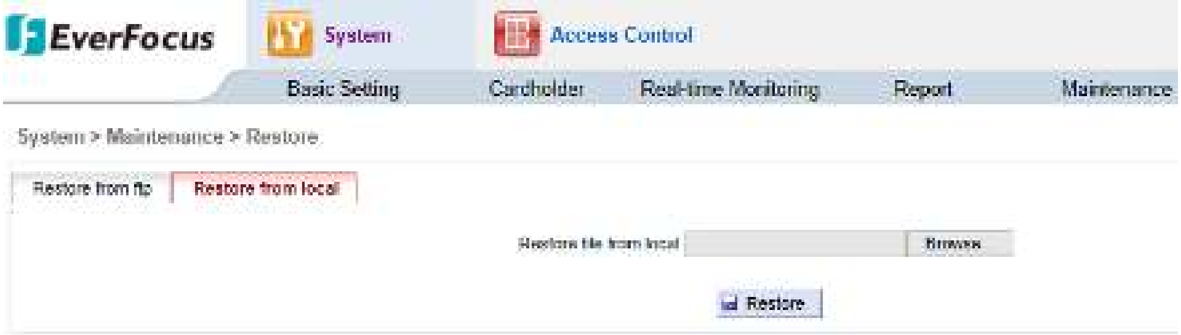


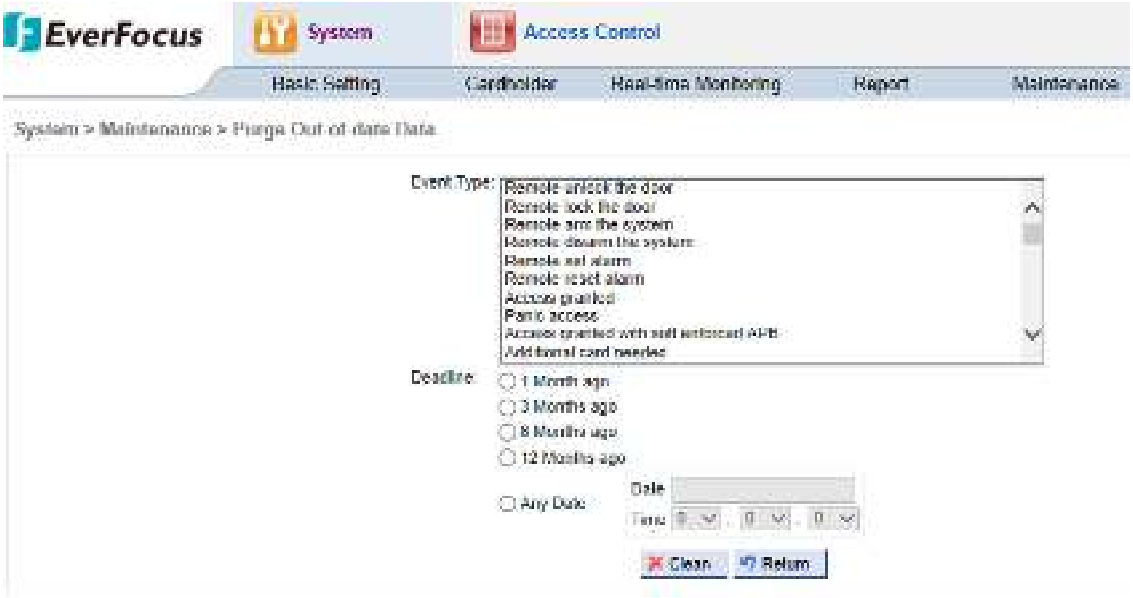
Figure11-5 Restore the Databasefrom Local

Steps:

1) Click the “Browse” button and select the database file to restore.
2) Click the “Restore” button to begin the restoration.
3) The system will display “restore the database succeeded.” when completed.

11.3 PurgeOut-of-date Data

Click on the menu bar “System” → “Maintenance” → “Purge Out-of-date Data”, to enter the purge page.



Select the event type and cut-off date of data and click the “Clean” button, then the system will completely clear all the events with the selected event type category according to the selection time.
For example, select the “Remote Door Open” events occurring 3 months ago and click the “Clean” button, then the system will delete all the “Remote Door Open” events occurring 3 months ago.

! Note: Expired data clear only clears the event records, operation control records, etc. in the software system and may not clear the configuration information of the system software; the cut-off time can be any time and the current selection time is exclude.

Chapter

12

12. Controller

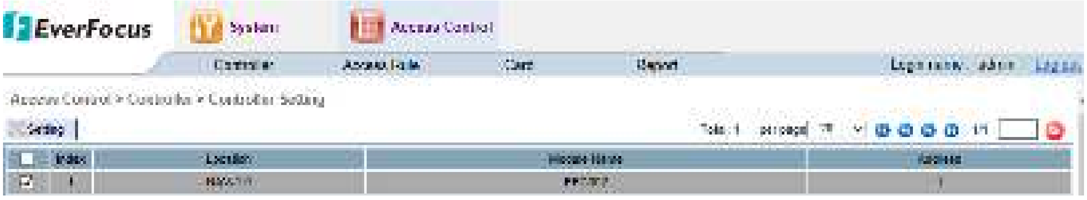
This chapter describes how to set up controller. In this chapter you will learn:

✧ How to configure the controller settings.

✧ How to download data to the controller.

12.1 Controller Setting

You can configure the controller settings through this page. Click “Access Control” → “Controller” → “Controller setting” from the menu bar to enter the controller settings page, shown as below:



Access Control > Controller > Controller Setting

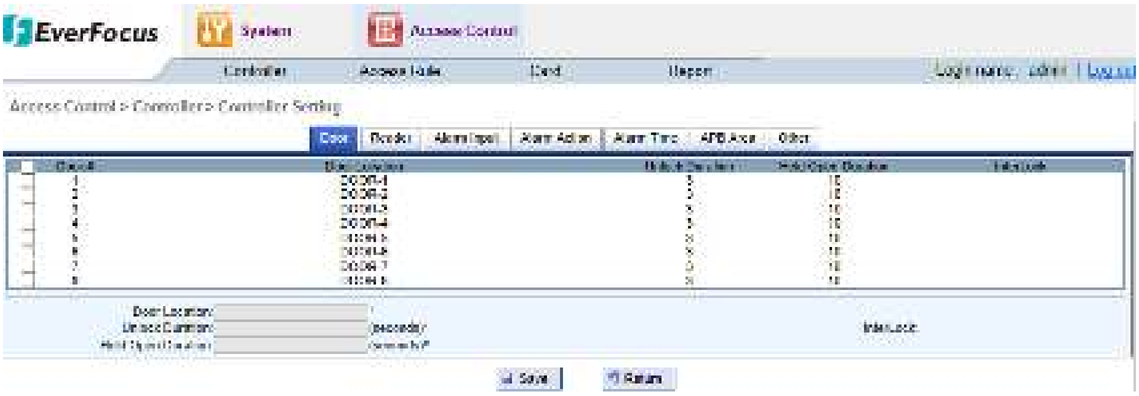
□	Index	Location	Model Name	Address
☑	1	[illegible]	[illegible]	1

Figure12-1Controller Setting

To configure the controller settings, select the controller on the list and then click the “Setting” button, and the setting page appears.
You can configure the Door, Reader, Alarm Input, Alarm Action, Alarm Time, APB Area and Other settings on this page.

12.1.1 Door

Click the “Door” tab, the setting page appears as below:



Access Control > Controller > Controller Setting

□	Door #	Door Location	Unlock Duration	Hold Open Duration	Interlock
□	1	DOOR-1	5	10	
□	2	DOOR-2	5	10	
□	3	DOOR-3	5	10	
□	4	DOOR-4	5	10	
□	5	DOOR-5	5	10	
□	6	DOOR-6	5	10	
□	7	DOOR-7	5	10	
□	8	DOOR-8	5	10	

Door Location:
Unlock Duration: (seconds)
Hold Open Duration: (seconds)
Interlock:

Figure12-2Controller Setting

You can set up the door location, door unlocks time and door held open time here.

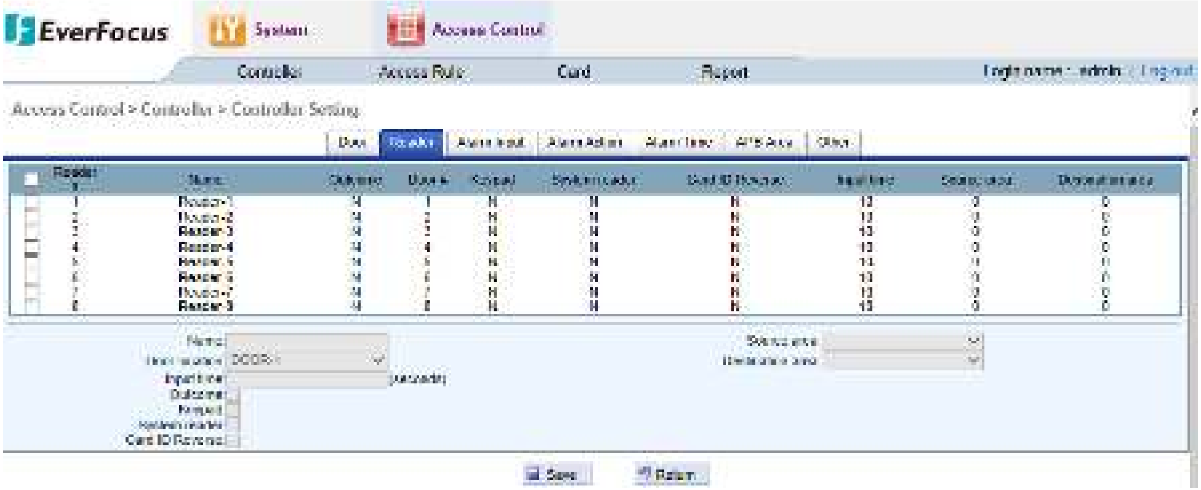
Door Location: indicates the location of the door. Input a desired location name of the door.
Unlock Duration: Set the door open time when a valid card is swiped or the Request-to-Exit button is pressed. The door remains open as long as the RTX button is pressed . The door open time does not count until the button is released. If two cards are swiped successively, the door open time does not count until the second card has been swiped. The default time is 3 seconds. The maximal door open time is 59999 seconds.
Held Open Duration: Door sensor monitors the open/close status of a door. If "unlock" is not set by the system (door is normally considered closed), then door should close after opening. It is considered abnormal if controller does not receive the door close signal from door sensor for a reasonable amount of time after the door is opened. This time period is call door held open time or door over time. According to this setting, the controller will determine whether to generate an alarm or not after the door sensor timeouts. The default value of door held open time is 10 seconds. The maximal door held open time is 59999 seconds.
Interlock: to set up an interlock door with the selected door. The interlocked door cannot be opened when either one of the interlocked door is opened. For example, if you interlock door1 with door4, door5, door6; when any of the door4, door5 or door6 is opened, door1 cannot be opened.

Steps:

1) Click the "Door" tab.
2) Select a door which needs to be set.
3) Input door information including: door location, unlock duration, held open duration and interlock.
4) Click the "Save" button to save your changes.

12.1.2 Reader

Click the "Reader" tab, the setting page appears as below:



Access Control > Controller > Controller Setting

□	Reader #	Name	Outgoing	Door #	Keypad	System enable	Card ID Reverse	Input time	Source area	Destination area
□	1	Reader-1	N	1	N	N	N	10	0	0
□	2	Reader-2	N	2	N	N	N	10	0	0
□	3	Reader-3	N	3	N	N	N	10	0	0
□	4	Reader-4	N	4	N	N	N	10	0	0
□	5	Reader-5	N	5	N	N	N	10	0	0
□	6	Reader-6	N	6	N	N	N	10	0	0
□	7	Reader-7	N	7	N	N	N	10	0	0
□	8	Reader-8	N	8	N	N	N	10	0	0

Name:
Door location: DOOR-1
Input time: (seconds)
Outgoing: □
Keypad: □
System enable: □
Card ID Reverse: □
Source area:
Destination area:

Figure12-3Reader

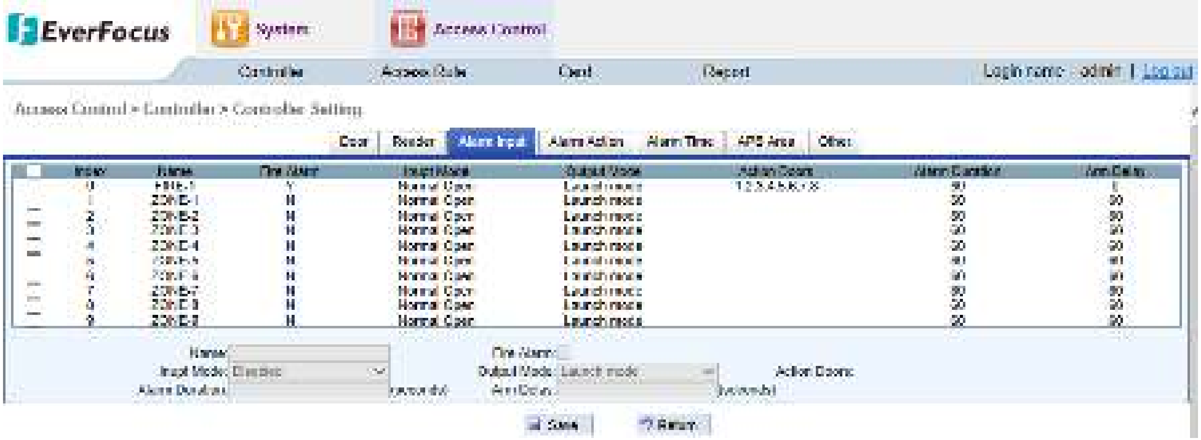
Name: input a name for the reader.
Door location: indicates the location of the reader. Input a desired location name of the reader (corresponding to the assigned door).
Input time: set up a max waiting time for inputting the password when the verification needs to input a password. If more than the time, the controller display will go back to main screen.
Outcome: indicates if the card reader is in door entry position or door exit position. If the item is checked, it indicates that the card reader is in the door exit position.
Keypad: Indicates the reader features a keypad. For a keypad reader, if a card PIN is enabled and the verification level is "card plus PIN", one must enter card PIN using the keypad to gain access to the door.
System reader: indicates if the card reader is a system reader. A system reader can transmit a card number to the controller to enroll cards to the controller. Any reader connected to the controller can be set as a system reader.
Source area /Destination area: These settings are for APB function. Select the source area (entry) and destination area (exit) from the drop-down list. To set up the APB area, please efer to Anti-Passback (APB Area) page for details.

Steps:

1) Click the "Reader" tab.
2) Select the reader which needs to be set.
3) Input reader information including: reader name, door location, input time, keypad reader, system reader, source area, destination area etc.
4) Click the "Save" button to save your changes.

12.1.3 Alarm Input

Click the "Alarm Input" tab, the setting page appears as below:



☐	Index	Name	Fire Alarm	Input Mode	Output Mode	Action Doors	Alarm Duration	Arm Delay
	0	FIRE-1	Y	Normal Open	Launch mode	1,2,3,4,5,6,7,8	30	0
	1	ZONE-1	N	Normal Open	Launch mode		30	30
	2	ZONE-2	N	Normal Open	Launch mode		30	30
	3	ZONE-3	N	Normal Open	Launch mode		30	30
	4	ZONE-4	N	Normal Open	Launch mode		30	30
	5	ZONE-5	N	Normal Open	Launch mode		30	30
	6	ZONE-6	N	Normal Open	Launch mode		30	30
	7	ZONE-7	N	Normal Open	Launch mode		30	30
	8	ZONE-8	N	Normal Open	Launch mode		30	30
	9	ZONE-9	N	Normal Open	Launch mode		30	30

Name:
Input Mode: Disabled
Alarm Duration: (seconds)
Fire Alarm: ☐
Output Mode: Launch mode
Arm Delay: (seconds)
Action Doors:

Figure12-4Alarm Input

Name: input a name of the alarm input.
Fire Alarm: indicates whether this alarm input is a fire alarm or not.

Input Mode: indicates the alarm input mode.

Disabled: the defence alarm input is invalid.

Normally Open: this input opened in normal state, alarm input enabled after closing.

Normally Close: this input closed in normal state, alarm input enabled after being opened.

Output Mode: the mode that the alarm output responds to the input when an alarm occurs.

Launch: when alarm input is triggered, the alarm output is activated at once; no matter the alarm input stops or not, alarm output continues until the alarm duration is over.

Transparent: when alarm input is triggered, the alarm output is activated at once; after alarm input stops, the alarm output stops immediately. At this time, alarm duration (delay time) does not work.

Alarm Duration: set up a delay duration time for the alarm input to trigger. When an alarm input event occur, the alarm input will only be triggered until the setup delay time.
Arm Delay: set up a duration time for the alarm outputs to be triggered. When an alarm input is triggered, the corresponding alarm relay outputs will be triggered based on the setup duration time.
Action Doors: select the door(s) respond to the alarm input.

Steps:

1) Click the “Alarm Input” tab.
2) Select the alarm input which needs to be set.
3) Input alarm input information.
4) Click the “Save” button to save your changes.

12.1.4 Alarm Action

On the alarm action settings page, users can configure the alarm output, including: the main modules output, door module output and alarm module output etc.

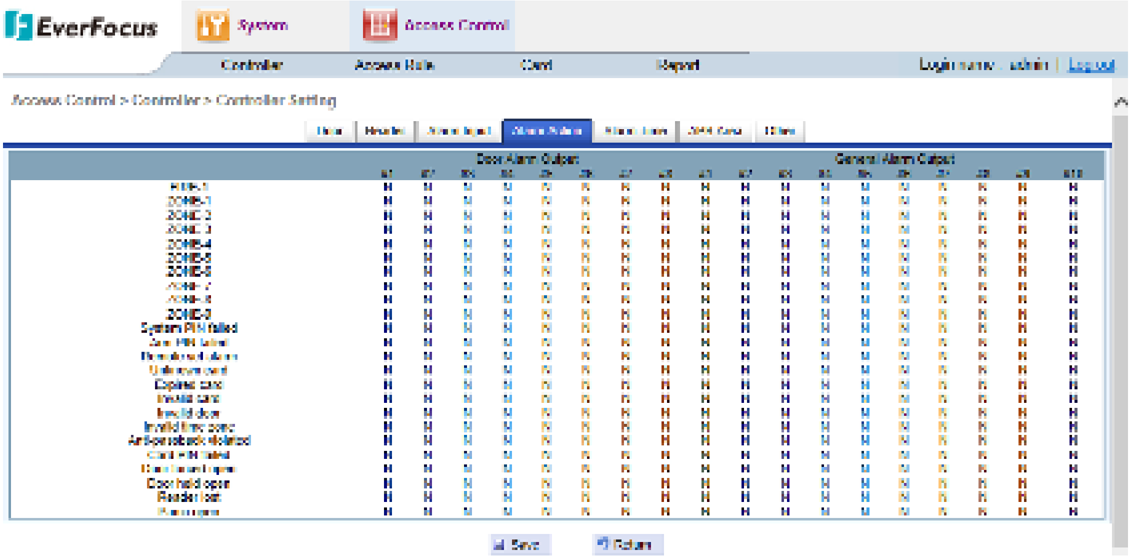


Figure12-5 Alarm Action

A NAV controller consists of two basic components: the main module and the door module. User can install up to 4 door modules and 1 alarm module. These three types of module are all equipped with alarm function.

Main module has 2 alarm inputs (figure 12-5 fire-1 and Zone-1), they response for fire alarm and tamper alarm. It also has 2 alarm outputs, corresponding to main alarm output and auxiliary alarm output.

Each door module has 2 alarm outputs, which usually react to alarm events on the corresponding door. However, it can be set to react to other alarm events as well. Alarm outputs on the door module can connect up to 5A external alarm devices.

Alarm module has 8 inputs and 8 alarm outputs, 8 alarm inputs can be connected to an external alarm input devices, such as PIR motion sensor, glass break sensors, etc. 8 alarm output can be connected to the maximum current 2A (amps) and external alarm device.

NAV controllers keep tracking all events in the access control system, whether allowed or disallowed, normal or abnormal. For example, all granted access events and all denied access events are recorded.

Some events are critical which must trigger the alarm output, like the firm alarm input, the zone alarm input, etc. But some events are not important and should not trigger an alarm output, like denied access due to an invalid time. These settings all depend on the users' requirements. The controller collects all events that might trigger the alarm output and provides the full capacity to enable or disable the alarm output based on these events.

Sometimes a user may wish to allocate a particular event to a particular alarm output, or allocate alarm inputs in certain area to multiple alarm outputs. The Flex controller delivers all the function and flexibility needed to do so. Users can define whether certain event will trigger an alarm, and can further specify to which alarm output that event is allocated.

An alarm can be triggered by events such as fire alarm, zone alarm 1~8, unknown card, expired card, invalid card, invalid door, invalid time, card APB fail, card PIN fail, SYS PIN fail, ARM PIN fail, door forced open, door held open, reader lost, alarm input 0, and remote alarm.

All these events can be allocated to any alarm relay output on main module, door module and alarm module. Alarm output setting interface is given in a table format and every column represents an alarm output source. The alarm output is shown in a drop-down menu.

If there are two options in the drop-down menu, it means the alarm output is not related to door. "Yes" indicates there is alarm output (relay energized), "No" indicates there is no alarm output (relay not energized).

If there are three options in the drop-down menu, it means the alarm output is related to door. "Y" indicates there is an alarm output (relay energized), "N" indicates there is no alarm output (relay not energized), "R" refers specifically to alarm output relay on the door module, indicating that alarm output will be generated only if the events occurs on the corresponding door module.

- **Fire Alarm:** A fire alarm event is generated when there is a fire alarm input. The controller generates an alarm output according on the setting in the “Fire Alarm” column.

- **Zone Alarm:** The zone alarm reacts to 8 alarm inputs on the alarm module. Any events in the arm zone may trigger a zone alarm event. The controller generates an alarm output according on the setting in the “Zone Alarm” column.

- **System PIN Fail:** User is required to enter system PIN to enter to the system setting menu. If an incorrect system PIN is entered three times consecutively, the system will generate a “system PIN fail” event. The controller generates alarm output(s) according to the setting in the “system PIN fail” column.

- **ARM PIN Fail:** User is required to enter ARM PIN when pressing the “ARM” key on the controller to arm/disarm the system. If an incorrect ARM PIN is entered three times consecutively, the system will generate an “ARM PIN fail” event. The controller generates alarm output(s) according to the setting in the “ARM PIN fail” column.

- **Tamper Alarm:** A tamper alarm event will be generated if there is a temper alarm input. The controller generates alarm output(s) according to the setting in the “Tamper Alarm” column.

- **Remote Alarm:** A system administrator can directly generate alarm signals using the control software when he observes an abnormal condition through a surveillance system. This is defined as a Remote Alarm event. The controller generates alarm output(s) according to the setting in the “Remote Alarm” column.

- **Unknown Card:** unknown card refers to a card that is never enrolled in the system. An unknown card event will be generated when an unknown card is presented to any reader. The controller generates alarm output(s) according to the setting in the “Unknown Card” column.

- **Expired Card:** any card in the system is usually assigned a valid date. After the valid date passes, the controller will automatically set the card as an expired card. An expired card cannot gain access to the system. An expired card event will be generated if an expired card is swiped on the reader. The controller generates alarm output(s) according to the setting in the “Expired Card” column.

- **Invalid Card:** User can directly set a card as an invalid card to disable the card. An invalid card cannot gain access to the system. An invalid card event will be generated if an invalid card is swiped on the reader. The controller generates alarm output(s) according to the setting in the “Invalid Card” column.

- **Invalid Door:** Each card belongs to an access group. For each group, the system can assign access rights to certain doors for certain time zones. An Invalid Door event will be generated when a card is swiped at any door at which it does not have the right to pass. The controller generates alarm output(s) according to the setting in the “Invalid Door” column.

- **Invalid Time:** Each card belongs to an access group. For each group, the system can assign access rights to certain doors for certain time zones. An invalid time event will be generated if a card is swiped during a time period in which it does not have the right to pass. The controller generates alarm output(s) according to the setting in the "Invalid Time" column.

- **APB Fail:** If the card APB property is enabled, and door behavior under APB is set to "unlock". A cardholder will be able to enter/exit any doors by swiping the card. The system generates an APB fail event if an APB event is triggered. The controller generates alarm output(s) according to the setting in the "APB Fail" column.

- **Card PIN Fail:** A card PIN fail event is generated when a PIN-enabled card is presented at a reader and an incorrect PIN is entered three times consecutively. The controller generates alarm output(s) according to the setting in the "Card PIN Fail" column.

- **Door Forced Open:** A door forced open event is generated when the door sensor indicates to the controller that a door is opened, but no legitimate card has been presented and a Request-to-Exit button has not been pressed. The controller generates alarm output(s) according to the setting in the "Door Forced Open". In practice, a door forced open event will be generated if a door is kicked open.

- **Door endures Open:** A door endures open event is generated if a cardholder enters endures PIN to unlock a door when under endures. The controller generates alarm output(s) according to the setting in the "Door endures Open".

- **Door Held Open/Overtime:** the system keeps tracking of the door status when a card is presented to a reader or Request-to-Exit button is pressed. A door held open/overtime event occurs when a door is held open for longer than the allowed door held open time. The controller generates alarm output(s) according to the setting in the "Door Held Open" column.

- **Reader Lost:** A reader lost event is generated when the controller detects that the card reader appears to have been disconnected from the system. The controller generates alarm output(s) according to the setting in the "Reader Lost" column.

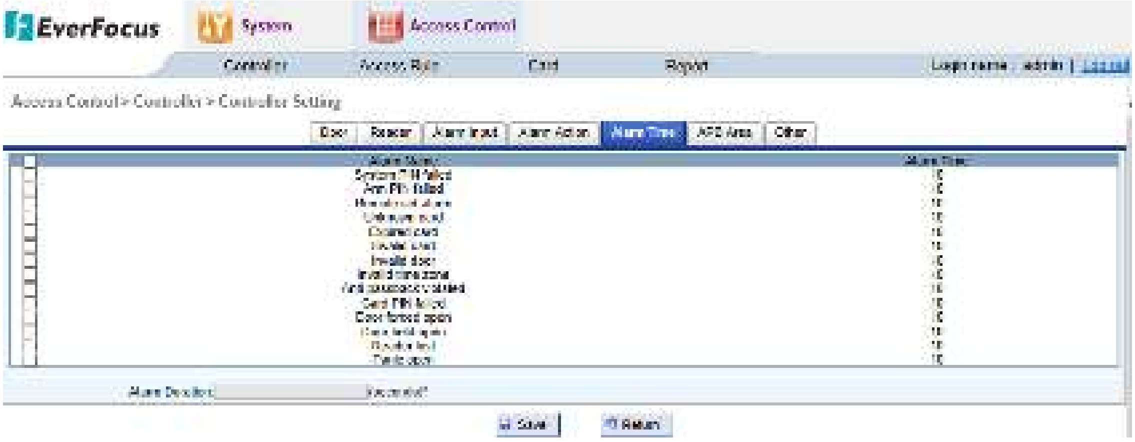
- **Panic door:** When an access denied appears and request open did not implement, however, door magnetic sensor is displayed the door have been opened, it will lead a "panic door" event. The controller generates alarm output(s) according to the setting in the "Panic Door" column.

Steps:

1) Click the "Alarm Action" tab.
2) Select an alarm to be set in the alarm list.
3) In the corresponding, click the position to show drop-down menu of alarm output, select the output value: R, Y, N.
4) Click the "Save" button to save your changes.

12.1.5 Alarm Time

On the alarm time setting page, users can set the alarm duration time for the specified controller. Click the “Alarm Input” tab, the setting page appears as below:



Access Control > Controller > Controller Setting

□	Alarm Name	Alarm Time
□	System PIN failed	10
□	Arm PIN failed	10
□	[illegible]	10
□	Unknown card	10
□	Expired card	10
□	Invalid card	10
□	Invalid door	10
□	Invalid time zone	10
□	Anti passback violated	10
□	Card PIN failed	10
□	Door forced open	10
□	Door held open	10
□	Reader lost	10
□	Panic open	10

Alarm Duration (seconds)?

Figure12-6Alarm Time

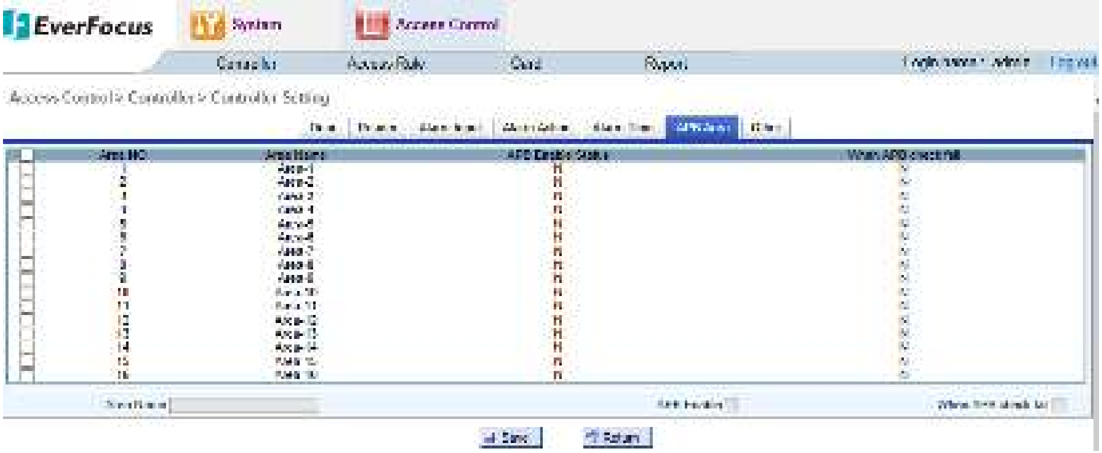
Steps:

1) Click the “Alarm Time” tab.
2) Select an alarm to be set in alarm list.
3) Input alarm time.
4) Click the “Save” button to save the change.

12.1.6 APB Area

On the APB Area page, users can configure the APB area, including: area name, enable or not, open door when APB check fail or not. The APB function is a control function to prevent the cardholder from repeatedly using the card for entry into the same area without leaving. To perform anti-Pass-Back, two card readers for entrance/exit can be designed. The cardholder must swipe the card on the entrance and exit card readers alternately.

Click the “APB Area” tab, the setting page appears as below:



Access Control > Controller > Controller Setting

□	Area NO	Area Name	APB Enable Status	When APB check fail
□	1	Area-1	N	N
□	2	Area-2	N	N
□	3	Area-3	N	N
□	4	Area-4	N	N
□	5	Area-5	N	N
□	6	Area-6	N	N
□	7	Area-7	N	N
□	8	Area-8	N	N
□	9	Area-9	N	N
□	10	Area-10	N	N
□	11	Area-11	N	N
□	12	Area-12	N	N
□	13	Area-13	N	N
□	14	Area-14	N	N
□	15	Area-15	N	N
□	16	Area-16	N	N

Area Name

APB Enable □

When APB check fail □

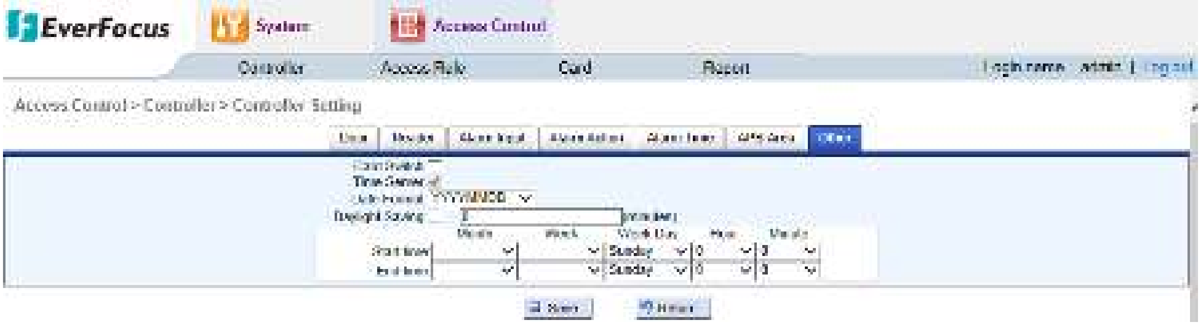
Figure12-7 APB Area

Steps:

1) Click the “APB area” tab.
2) Select an area to be set.
3) Input area information.
4) Click the “Save” button and save the changes.

12.1.7 Other Setting

You can configure the overall settings on the page. Click the “Other” tab and the page below appears:



Card Switch □
Time Server ☑
Date Format YYYYMMDD
Daylight Saving

	Month	Week	Week Day	Hour	Minute
Start time			Sunday	0	3
End time			Sunday	0	3

Figure12-8Other Setting

- **Card Switch:** check/uncheck to enable/disable the first-card-in function. After opening the door using the first card, the status of the door is normal or normally opened.

- **Time server:** indicates whether the controller is the time synchronization server in the system. All controllers in the system will automatically adjust its date and time setting to match that of the time synchronization server. There can be only one time synchronization server in the system and the last assigned time synchronization server will replace any previous setting. If the controller is connected to a PC installed with Flex software, the software will automatically modify the controller date and time to match the PC setting. If the controller date and time are found to be incorrect, check the date and time on the control PC.

- **Date format:** the system offers two date format: “YYYY-MM-DD” and “MM-DD-YYYY” and users can choose the desired format.

- **Daylight saving time:** check/uncheck to enable/disable the auto Daylight Saving Time function. When auto DST is enabled, user need to define the start and end dates of DST, including month, week, date, and time, forward or backward. When auto DST is enabled, the controller will automatically adjust DST one hour forward from 1:59:59am to 3:00:00am on the first Sunday in April, and adjust it backward one hour from 1:59:59am to 1:00:00am on the last Sunday in October.

Steps:

1) Click the “Other” tab.
2) Select and change the setting.
3) Click the “Save” button to save the changes.

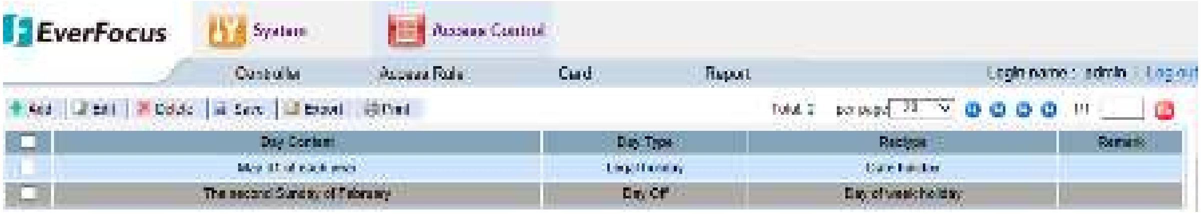
Chapter

13

13. Access Rule

13.1 Date Type

Click “Access Control” → “Access Rule” → “Date Type” to enter the page below:

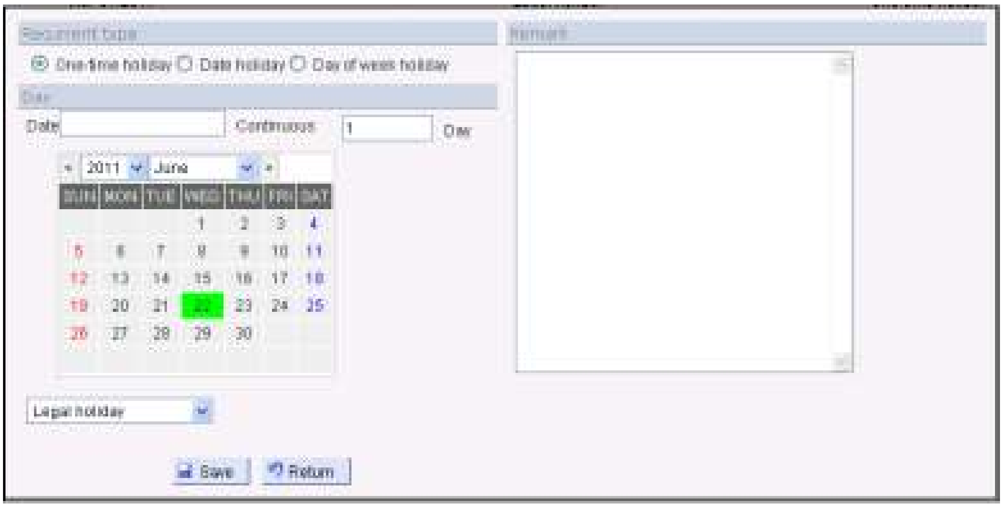


☐	Day Content	Day Type	Recycle	Remark
☐	May 1st of each year	Legal holiday	Date holiday	
☐	The second Sunday of February	Day Off	Day of week holiday	

Figure13-1Date Type

13.1.1 Add a Date

In the date type page, click the “Add” button and will pop-up below screen:



● One-time holiday ○ Date holiday ○ Day of week holiday

Date:

Continuous: 1 Day

Legal holiday

Figure13-2Add a Date

Controller supports 10 date types, including: Sunday to Saturday (7 types), custom 1-3. Sunday to Saturday is automatically set based on the calendar. Users can customize according to their own needs custom 1-3. In this manual, custom 1-3 are holidays. Holiday setting is these 3 holiday type. The NAV controller supports up to 255 holiday setting.

- **Recurrent type**

Software allows set the holiday flexibility in accordance with the standard set of three different Holiday. There three types of cycles are as following:

- ✧ **One-time holiday:**

A one-time holiday is a holiday that will occur once, and will not recur in subsequent years. An example is a company organized travel event during Oct. 10, 2008 to Oct. 15.

- ✧ **Date Holiday**

A date holiday is a recurrent holiday that occurs on the same date every year. For instance, the New Year holiday, which occurs on January 1, is a date holiday.

- ✧ **Day of week Holiday**

Day of week holiday is another recurrent holiday type. It defines a certain day of a certain week, in a certain week of a month. Thanksgiving is an example of a Day of Week holiday, falling on the 4th Thursday of November.

! Note: These holidays should be allocated during system initialization and re-checked at the beginning of every year.

Steps:

1) Select day of recurrent type.
2) Select the date in calendar.
3) In the day type.
4) Input remarks (optional).
5) Click the “Save” button to add a new date in the list.

13.1.2 Delete a Date

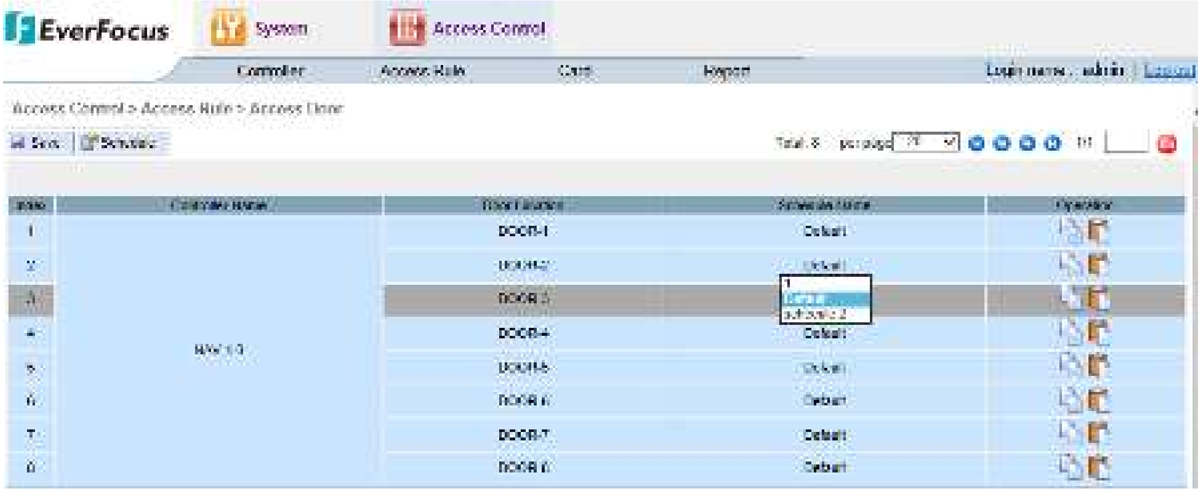
Steps:

1) Check the date(s) (one, part or all) to be deleted in the date list.
2) Click “Delete,” then the prompt dialog box “Are you sure to delete?” pops up.
3) Click “OK,” then the selected control date is deleted.

！Note: After addition or deletion of a date, the system will automatically “Save” the changed information.

13.2 Access Door

Click on the menu bar “Access Control” → “Access Rule” → “Access Door” to enter the below page:



Index	Controller Name	Door Name	Schedule Name	Operation
1	NAV 1-3	DOOR-1	Default	
2		DOOR-2	Default	
3		DOOR-3	1 Default schedule 2	
4		DOOR-4	Default	
5		DOOR-5	Default	
6		DOOR-6	Default	
7		DOOR-7	Default	
8		DOOR-8	Default	

Figure 13-3 Access Door

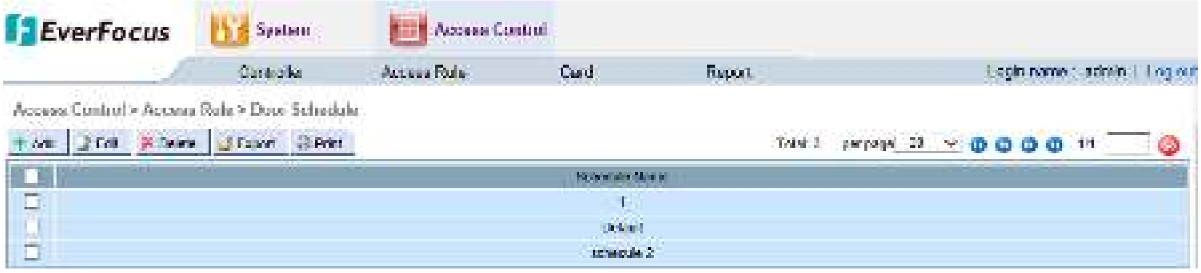
Steps:

1) Select a door schedule for each door.
2) After completed, click the “Save” button. It will display a “Modify successfully” message when completed.
3) Click the “Ok” to confirm the data update.

The user can also use the function “copy” and “paste” buttons in the Operation column between different doors, the two doors will be used the same door schedule.

13.3 Door Schedule

Click on the menu bar “Access Control” → “Access Rule” → “Door Schedule” to enter the door schedule setting page:

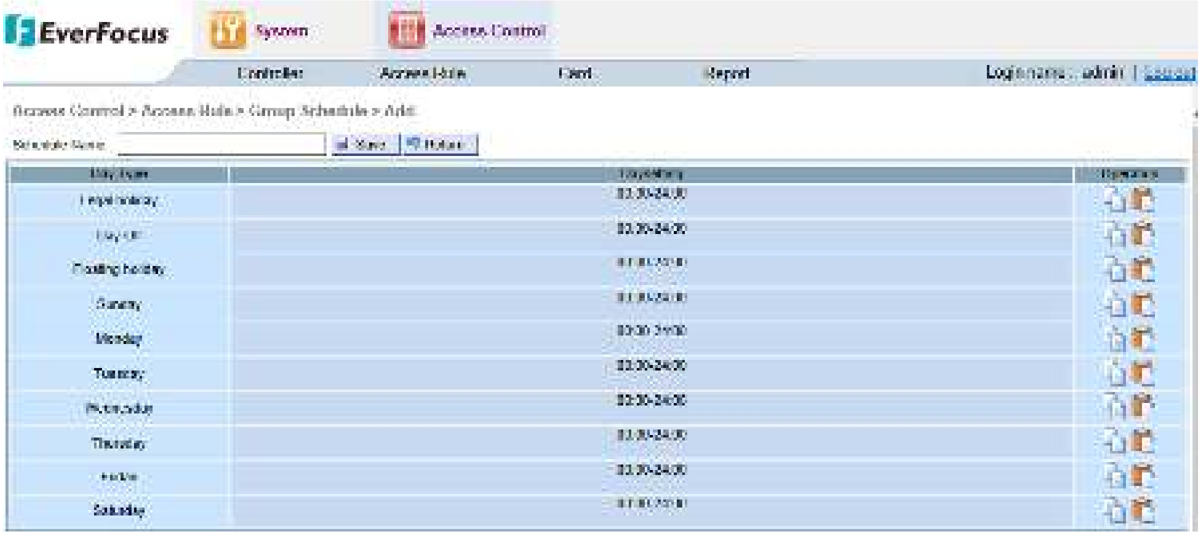


□	Schedule Name
□	1
□	Default
□	schedule 2

Figure13-4Door Schedule

13.3.1 Add a Door Schedule

On the door schedule setting page, click the “Add” button to enter to the setting page.



Access Control > Access Rule > Group Schedule > Add

Schedule Name:

Day type	Day setting	Operation
Legal holiday	00:00-24:00	
Day off	00:00-24:00	
Floating holiday	00:00-24:00	
Sunday	00:00-24:00	
Monday	00:00-24:00	
Tuesday	00:00-24:00	
Wednesday	00:00-24:00	
Thursday	00:00-24:00	
Friday	00:00-24:00	
Saturday	00:00-24:00	

Figure13-5 Add a Door Schedule

Steps:

1) Input a new schedule name in the text box.
2) Click on one cell in the column “Day setting”, a pop-up box appears. You can set the time sections and entry/exit mode, multi-card for each door, shown as Figure13-7.
3) After completed, click the “save” button and the new door schedule have been created.

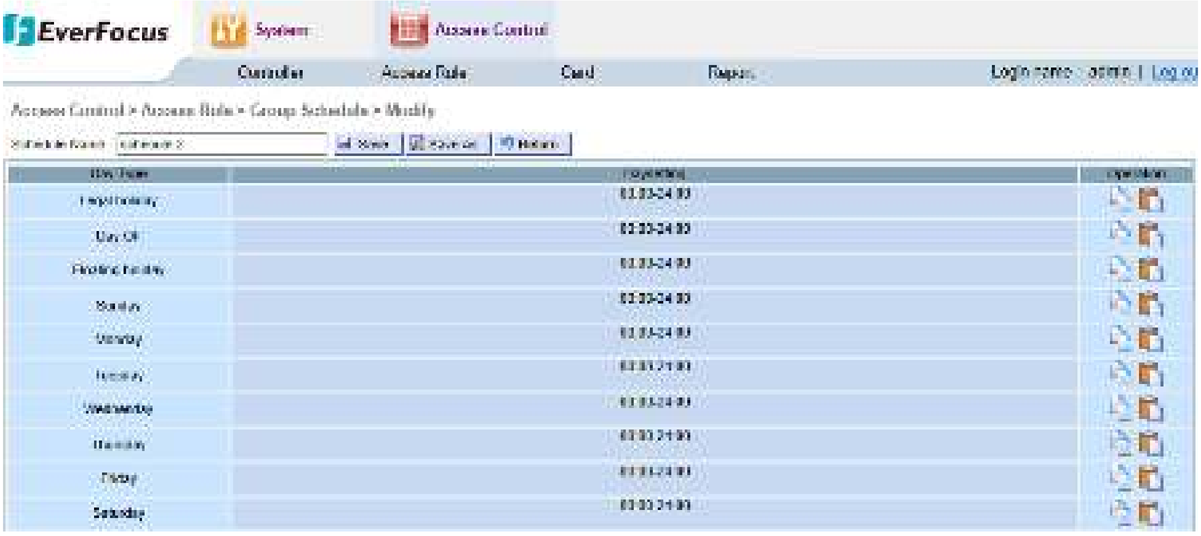
13.3.2 Delete a Door Schedule

Steps:

1) In the door schedule setting page, select one or more schedule to be deleted.
2) Click the “Delete” button.
3) Confirm to delete.
4) Click the “Ok” button.

13.3.3 Edit a Door Schedule

Select a door schedule and click the “Edit” button to enter the door schedule setting page:

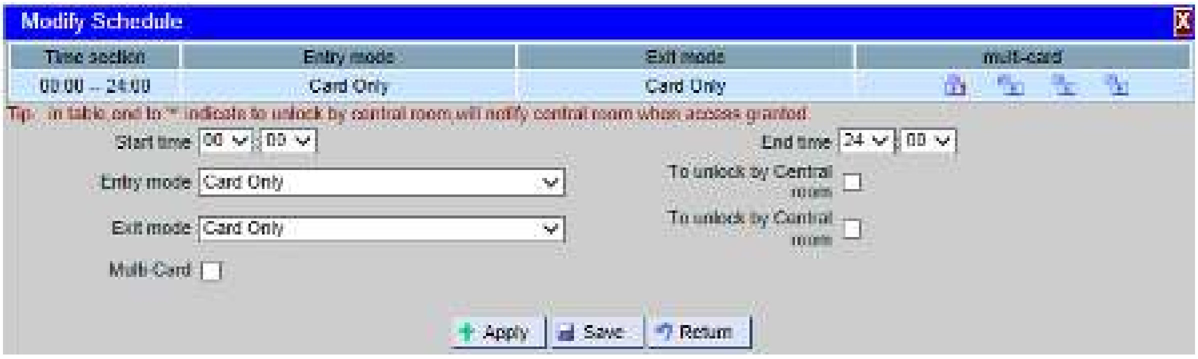

EverFocus
System
Access Control
Controller
Access Rule
Card
Report
Login name : admin | Log out
Access Control > Access Rule > Group Schedule > Modify
Save
Save as
Return

Schedule Name: schedule 3

Day Type	[illegible]	Operation
Legal holiday	00:00-24:00	
Day Off	00:00-24:00	
Floating holiday	00:00-24:00	
Sunday	00:00-24:00	
Monday	00:00-24:00	
Tuesday	00:00-24:00	
Wednesday	00:00-24:00	
Thursday	00:00-24:00	
Friday	00:00-24:00	
Saturday	00:00-24:00	

Figure13-6 Edit a Door Schedule

The default entry/exit mode is “Card only”, if you need to set the mode in different time sections, click the time bar to enter the “Modify Schedule” page, shown as following:



Time section	Entry mode	Exit mode	multi-card
00:00 -- 24:00	Card Only	Card Only	

Tip: in table,and to '*' indicate to unlock by central room,will notify central room when access granted.

Start time 00 : 00　End time 24 : 00

Entry mode: Card Only　To unlock by Central room □

Exit mode: Card Only　To unlock by Central room □

Multi-Card □

Figure13-7 Modify Schedule

Input the start and end time, select the entry/exit mode for current time section, set the lock level for the door if using the multi-card access, and click the “Apply” and “Save” button. Click “Return” back to group schedule setting page.

After back to the page, click “Save”, the door schedule have been saved, shown as below:

Data updating...

100%

Figure13-8Data Updating

After the current date type is set, the user want to be set the other date as same, just need to click the “copy” button to copy the pervious setting in the “Operation” column of the first one, and then click the “paste” button for the second one, the setting will be applied to the second one.

13.3.4 Save As a New Schedule

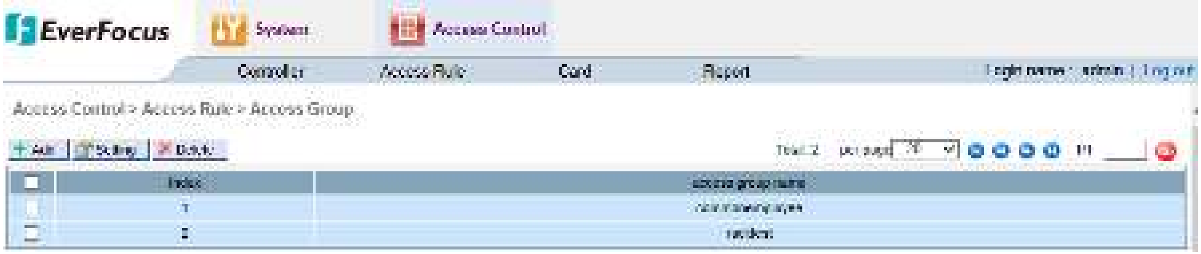
A door schedule can be edited and it can be saved as a new schedule. This feature is used to add a similar setting for other door schedules.

Steps:

1) Edit the schedule name on the box or not.
2) Click "Save as" to create a new schedule.

13.4 Access Group

Click the menu "Access Control" → "Access Rule" → "Access Group" to enter the access group setting page:

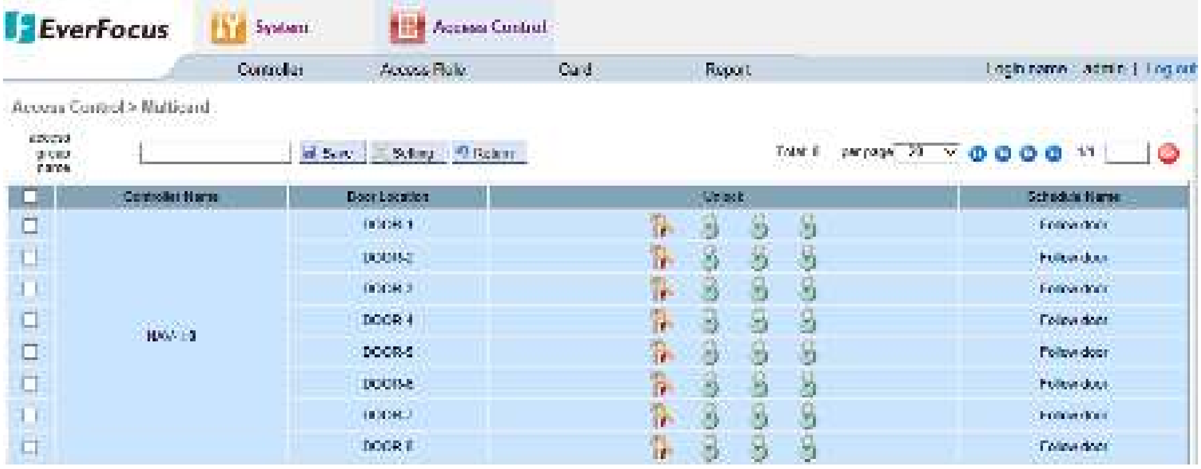


□	Index	access group name
□	1	[illegible]
□	2	[illegible]

Figure13-3Access Group

13.4.1 Add an Access Group

In "Access Group" page, click the "Add" button, the group setting screen pop-up.



□	Controller Name	Door Location	Unlock	Schedule Name
□	NAV-13	DOOR 1		Follow door
□		DOOR 2		Follow door
□		DOOR 3		Follow door
□		DOOR 4		Follow door
□		DOOR 5		Follow door
□		DOOR 6		Follow door
□		DOOR 7		Follow door
□		DOOR 8		Follow door

Figure13-4Add a Access Group

Steps:

1) Enter a new group name.
2) Select each door's unlock level, group schedule (or following door's schedule).
3) Click "Save" and return to the setting page.

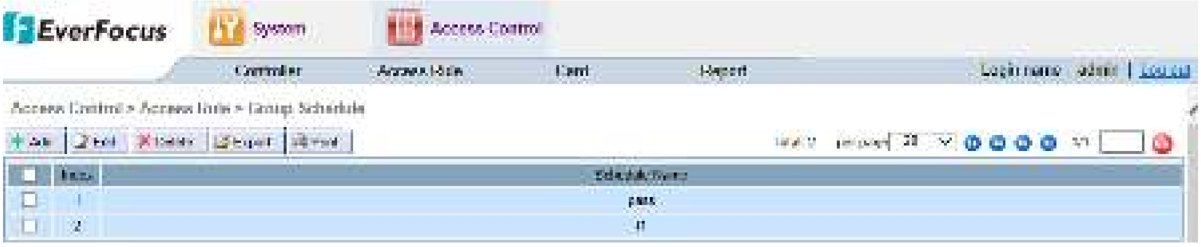
13.4.2 Delete an Access Group

Steps:

1) Select one or more access group to be deleted.
2) Click the “Delete” button.
3) Confirm deletion.
4) Click “OK”.

13.5 Group Schedule

Click on the menu bar, select “Access Control” → “Access Rule” → “Group Schedule” to enter the Group Schedule page:



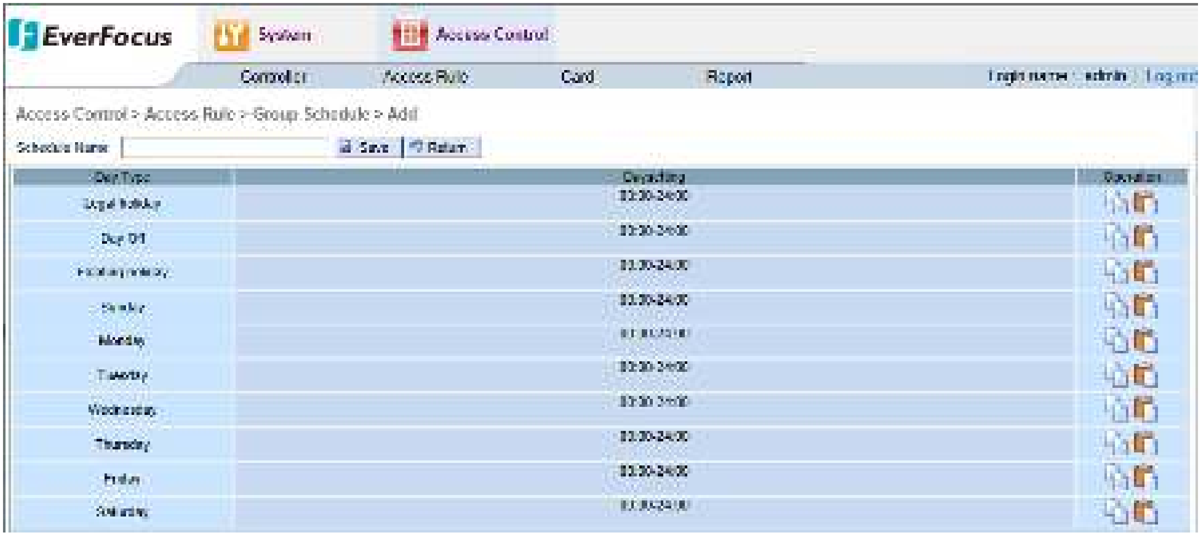
Access Control > Access Rule > Group Schedule

□	Index	Schedule Name
□	1	pass
□	2	ff

Figure13-11User Group Schedule

13.5.1 Add a Group Schedule

In the group schedule setting page, click the “Add” button to add a new schedule.



Access Control > Access Rule > Group Schedule > Add

Schedule Name

Day Type	Day setting	Operation
Legal Holiday	00:00-24:00	
Day Off	00:00-24:00	
[illegible]	00:00-24:00	
Sunday	00:00-24:00	
Monday	00:00-24:00	
Tuesday	00:00-24:00	
Wednesday	00:00-24:00	
Thursday	00:00-24:00	
Friday	00:00-24:00	
Saturday	00:00-24:00	

Figure13-12 Add a Group Schedule

Steps:

1) Enter a new name in the box.

2) Click on one cell in the column "Day setting", a pop-up box appears. You can set the time sections and entry/exit mode, shown as Figure13-14.
3) After completed, click the "Save" button and the new group schedule have been created.

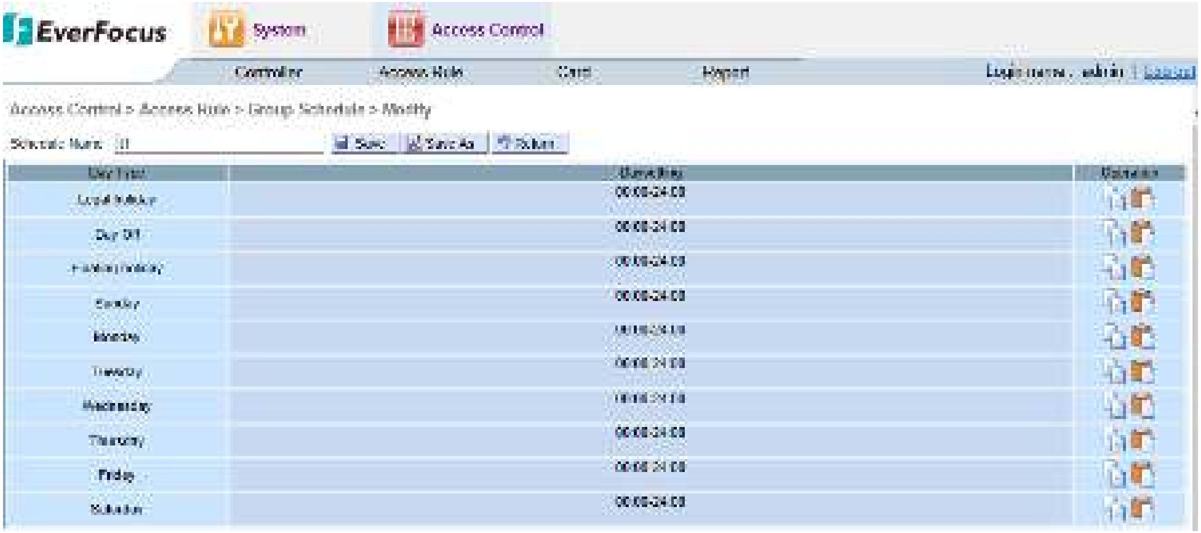
13.5.2 Delete a Group Schedule

Steps:

1) In the group schedule setting page, select one or more schedule to be deleted.
2) Click the "Delete" button.
3) Confirm to delete.
4) Click the "Ok" button.

13.5.3 Edit a Group Schedule

Select a group schedule and click the "Edit" button to enter the group schedule setting page, shown as following:



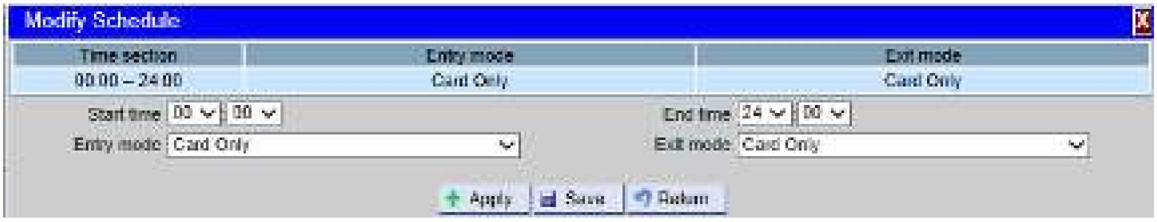
Access Control > Access Rule > Group Schedule > Modify

Schedule Name: 0

Day Type	Day setting	Operation
Legal holiday	00:00-24:00	
Day Off	00:00-24:00	
Floating holiday	00:00-24:00	
Sunday	00:00-24:00	
Monday	00:00-24:00	
Tuesday	00:00-24:00	
Wednesday	00:00-24:00	
Thursday	00:00-24:00	
Friday	00:00-24:00	
Saturday	00:00-24:00	

Figure13-13 Edit a Group Schedule

The default entry/exit mode is "Card only", if need to set the mode in different time sections, click the time bar, enter to the "Modify Schedule" page, shown as following:



Time section	Entry mode	Exit mode
00:00 – 24:00	Card Only	Card Only

Start time: 00 : 00

End time: 24 : 00

Entry mode: Card Only

Exit mode: Card Only

Figure13-14 Modify a Schedule

Input the start and end time, select the entry/exit mode for current time section, and click the "Apply" and "Save" button. Click "Return" back to group schedule setting page.
After back to the page, click "Save" button, group schedule have been saved, shown as following:

Figure13-15 Data Updating

After the current date type is set, the user want to be set the other date as same, just need to click the "copy" button to copy the pervious setting in the "Operation" column of the first one, and then click the "paste" button for the second one, the setting will be applied to the second one.

13.5.4 Save As a New Schedule

A group schedule can be edited and it can be saved as a new schedule. This feature is used to add a similar setting for other group schedules.

Steps:

1) Edit the schedule name on the box or not.
2) Click "Save as" to create a new schedule.

Chapter

14

14. Card

This section describes how to add, edit cards, through this section you will learn:

- How to add, delete and edit one or more cards.
- Import cards to the controller

14.1 Card Setting

Click on the menu bar “Access Control” → “Card” → “Card Setting” to enter the below page:

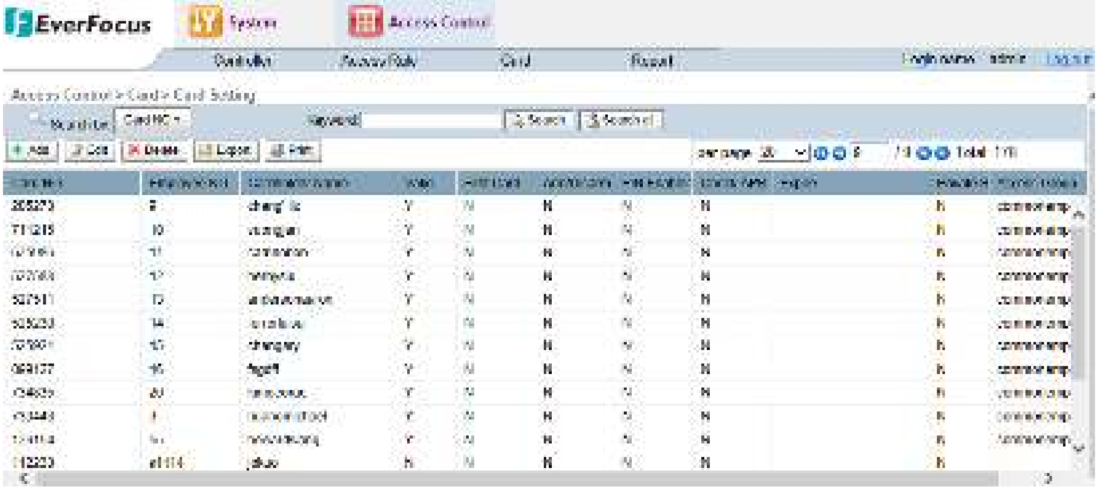


Figure14-1Card Setting

In the card setting page, the top is query area and operation button list, the below is card list.

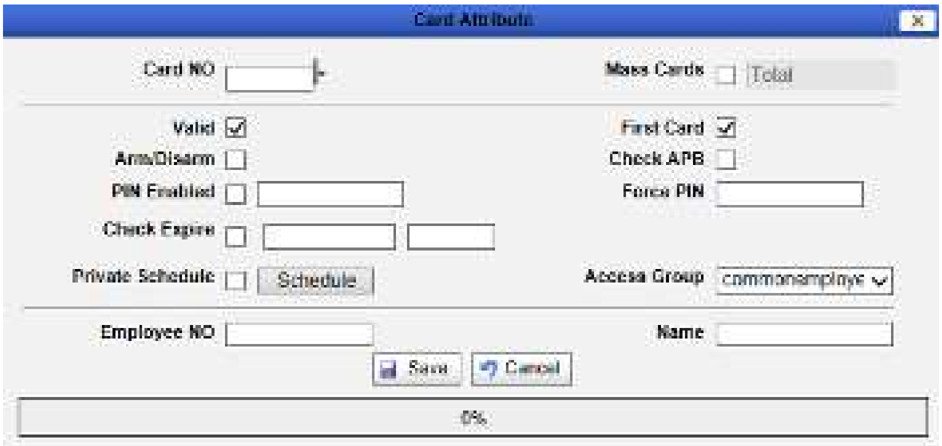
- **Query Operation Area:**
  Select a search field and input the search criteria in the “keyword” text box, click the “Search” button to start searching. If there are cards matching, they will be shown in the card list.

- **Operation Button List:**
  Including add, edit, delete, export and print buttons, used to operate the card.

- **Card List:**
  Shown all the card information including: card number, employee number, cardholder name, access group and its properties etc.

14.1.1 Add a (Batch) Card

In the card setting page, click the “Add” button and a pop-up window appears



Card Attribute

Card NO

Mass Cards □ Total

Valid ☑

First Card ☑

Arm/Disarm □

Check APB □

PIN Enabled □

Force PIN

Check Expire □

Private Schedule □ Schedule

Access Group commonemploye

Employee NO

Name

Save Cancel

0%

Figure14-2Add a (batch) Card

Steps:

1) In the window, input the card number, if users want to add more than one card that its serial number is consecutive, please check the “Mass Cards” first, and then input the batch number, the inputted serial number will be as the start number.
2) Set the card’s properties including valid, first card, arm/disarm, APB, password status and use the expiration etc. then input the password and force PIN , select the access group, if using the card’s schedule, please check the “Private Schedule” first.
3) Assign one or more cards to one cardholder, after inputted the employee number, the matched name will automatically pop-up, click to select it. Empathy the user can also input employee name first.
4) Click the “Save” button, the card will be added to the list.

Note: To know the details about added, modified and deleted operations please refer to 5.2.19.

Card number: Input the number, the software supports various kinds of card type. Each type will be converted to according format. Use 10 decimal to be a sample, if its length is shorter than 10, the software will add “0” at the beginning of the number.

ID card is Wiegand-26 format, which means 26 bits. Discarded the first 2 and last 2 parity numbers, the remaining 24 digit will be converted to 10 decimal.

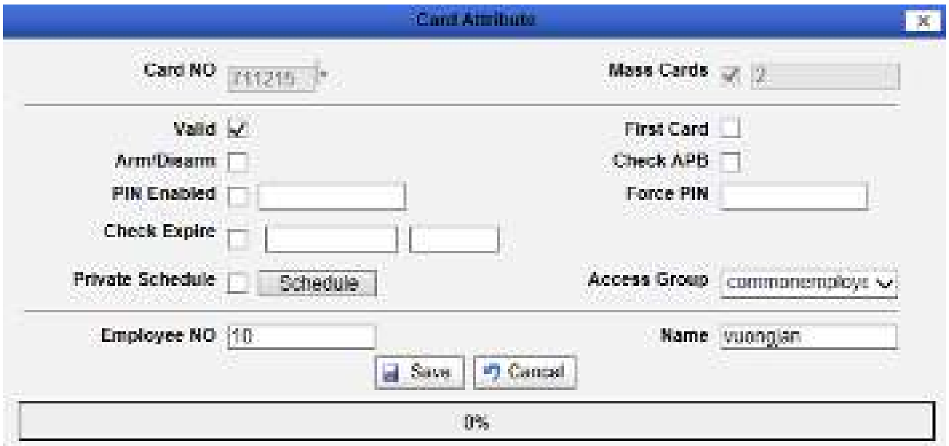
- Users can read the number printing on the card.
- Swipes the card on the reader, then user can find the card number in the access denied record list on monitoring event page of the software.

- The card can be added to the controller by the system reader in the controller’s menu.

If the added cards’ quantity is more one which number is continual, input the starting number and quantities to batch add.

14.1.2 Edit a (Batch) Card

Edit a Card: In the card setting page, click the card which needs to be edited and a pop-up window appears, shown as following:


Card Attribute

Card NO 711215 *

Mass Cards ☑ 2

Valid ☑

First Card □

Arm/Disarm □

Check APB □

PIN Enabled □

Force PIN

Check Expire □

Private Schedule □ Schedule

Access Group commonemploye

Employee NO 10

Name vuongjan

Save Cancel

0%

Figure14-3Edit a Card

Modify the relevant properties of the card, select and click the “Save” button, when the progress bar becomes 100%, click the “Back” button to close the window.

Edit batch Card: Press the Shift key to select more than one cards, click the “Edit” button and pop-up a window to modify the relevant attributes. Click the “Save” button after edit. Click the “Back” button to close the window.

14.1.3 Delete a (Batch) Card

Steps:

1) In the card setting page, select the cards which need to be deleted.
2) Click the “Delete” button.
3) Confirm to delete.
4) Click “OK” to finish.

14.1.4 Export Cards

Click the “Export” button, a pop-up download file window appears. All cards will be exported to CSV format. Select a path to save the file. Click “OK” to confirm. Please see 7.1.7 Export Function.

14.1.5 Print Cards

Click the “Print” button to enter the printing page, the specific operation method see 7.1.8 Print Function.

14.1.6 Search Cards

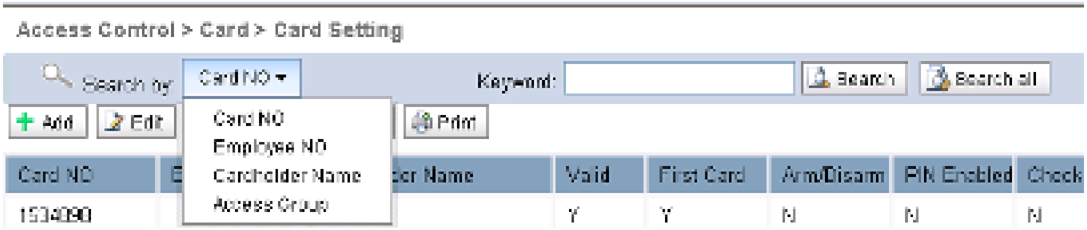
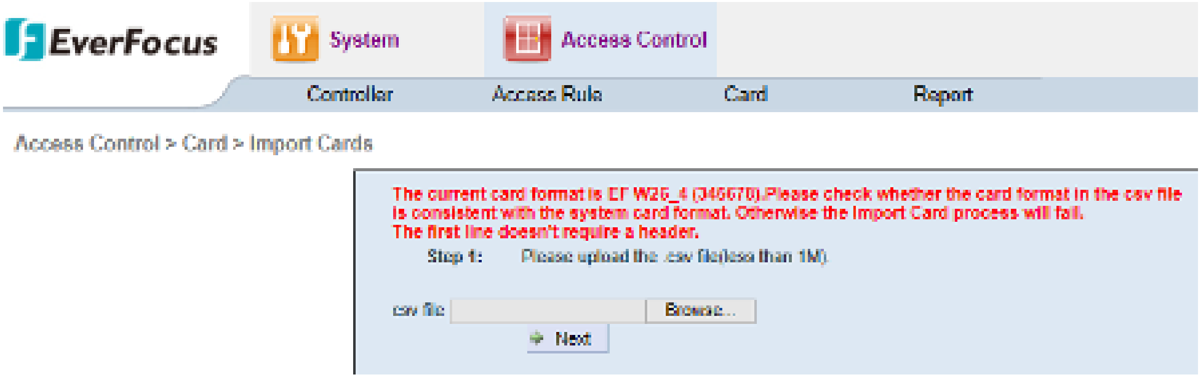


Figure 14-4 Search Cards

Select a search field and input the search criteria in the “keyword” text box, click the “Search” button to start searching. If there are cards matching, they will be shown in the card list. Click “Search All” button, back to the all card list.

14.2 Import Cards

Select System menu bar “Access Control”→ “Cardholder” → “Import Cards” to enter the below page:



The current card format is EF W26_4 (345670).Please check whether the card format in the csv file is consistent with the system card format. Otherwise the Import Card process will fail.
The first line doesn't require a header.

Step 1: Please upload the .csv file(less than 1M).

Figure14-5 Update Excel File

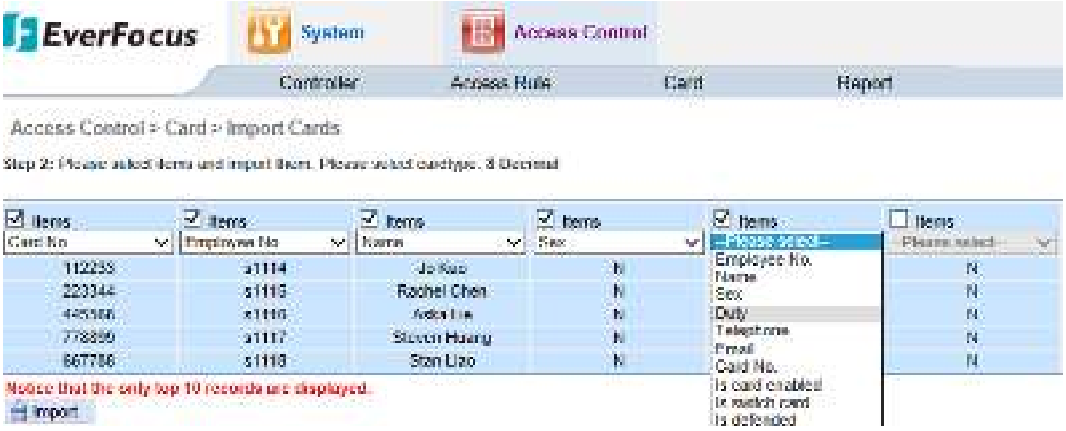
You can import multiple card information together with cardholder information to the controller through csv file. Please follow the steps below:

Steps:

1) Export the excel format from “Card Setting” page (Access Control < Card < Card Setting). Go to the “Card Setting” page, click the “Export” button, save the csv file in your computer.
2) Open the exported csv file to edit the cardholder and card information. The file size is limited to 1M.

   ! Note: If Chinese characters are included in the csv content, file conversion will be required or the Chinese characters will be garbled. Please refer to *7.1.5 Export Function* to convert the exported files.

3) To import the csv format file, go to the “Import Cards” page (Access Control < Card < Import Cards), click the “Browse” button to import the edited csv file.
4) Click the “Next” button to enter the operation page.



Access Control > Card > Import Cards

Step 2: Please select items and input item. Please select cardtype. 8 Decimal

☑ Items Card No	☑ Items Employee No	☑ Items Name	☑ Items Sex	☑ Items --Please select--	□ Items --Please select--
112233	s1114	Jo Kuo	N		N
223344	s1115	Rachel Chen	N		N
445566	s1116	Aida Lin	N		N
778899	s1117	Steven Huang	N		N
667788	s1118	Stan Liao	N		N

Notice that the only top 10 records are displayed.

Figure9-1Import Cardholders

5) Check the items you wish to add to the controller and then select each attribute of the item from the drop-down list.
6) Click the “Import” button to start importing.
7) After the Import process is complete, a “xxx records have been imported.” message will be displayed. You can click the “Return” button to return to the Import Cards page.

Chapter

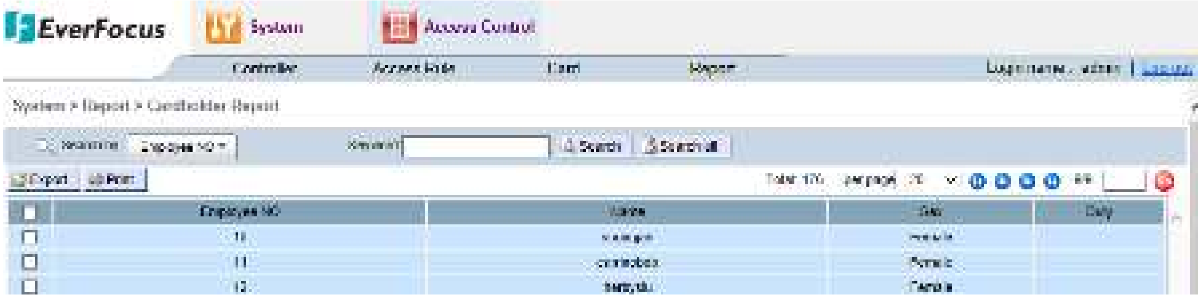
15

15. Report

This chapter describes how to query, print the cards, and access events.

15.1 Card Report

Click on the menu bar “Access Control” → “Report” → “Card Report” to enter the below page:



□	Employee NO	Name	Sex	Duty
□	10	[illegible]	Female	
□	11	[illegible]	Female	
□	12	[illegible]	Female	

Figure15-1 Card Report

15.1.1 Search Cards

Steps:

1) In the search drop-down menu, select a field, including card number, employee number, and cardholder name, access group.
2) Input the search criteria in the “keyword” text box.
3) Click the “Search” button, the matching cards will be shown in card list.
4) If the user wants to view all the cards in the controller, click the “Search All” button.

15.1.2 Export Cards

Click the “Export” button, a pop-up download file box appears, all cards will be exported to CSV format, select a path to save the file. Click “OK” to confirm. Please see 7.1.7 Export Function.

15.1.3 Print Cards

Click the “Print” button to enter the printing page, the specific operation method see 7.1.8 Print Function.

15.2 Card-dependent Event

Click on the menu bar “Access” → “Report” → “Card-dependent Event” to enter the card-dependent event home page, shown as following:

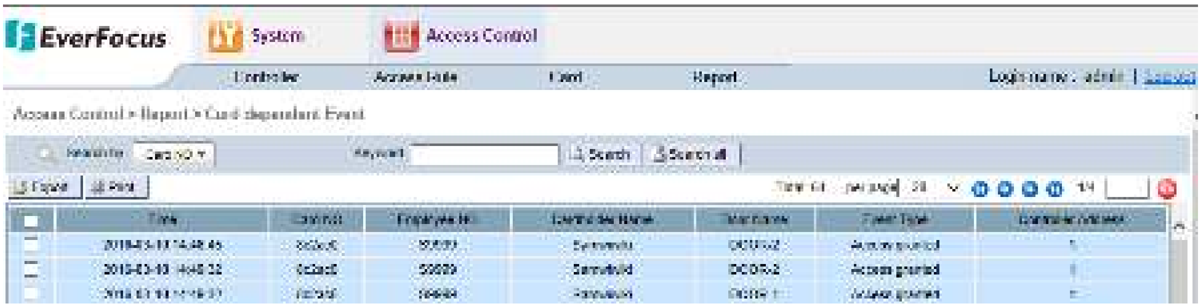


Figure15-2Card-dependent Event

15.2.1 Search Events

Steps:

1) In the search drop-down menu, select a field, including card number, employee number, and cardholder name, event type.
2) Input the search criteria in the “keyword” text box.
3) Click the “Search” button, the matching cards will be shown in card list.
4) If the user wants to view all the cards in the controller, click the “Search All” button.

15.2.2 Export Events

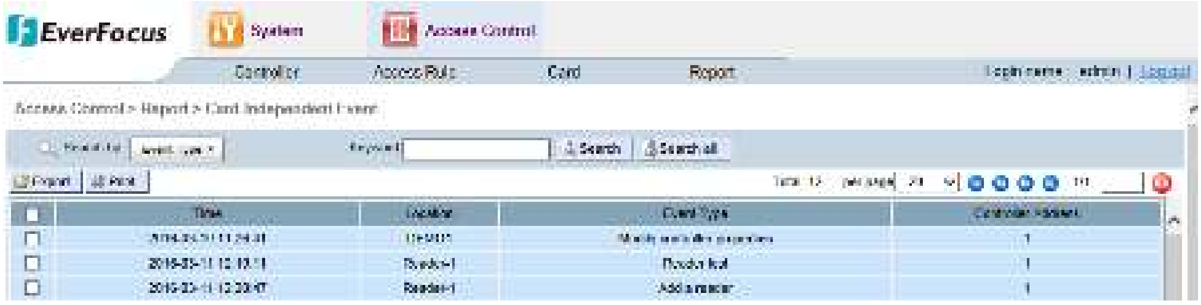
Click the “Export” button, a pop-up download file box appears, all cards will be exported to CSV format, select a path to save the file. Click “OK” to confirm. Please see 7.1.7 Export Function.

15.2.3 Print Events

Click the “Print” button to enter the printing page, the specific operation method see 7.1.8 Print Function.

15.3 Card-independent Event

Click on “Access Control” → “Report” → “Card-independent Event” to enter the card-independent event page.



□	Time	Location	Event Type	Controller Address
□	[illegible]	[illegible]	[illegible]	1
□	2016-03-11 12:[illegible]	Reader-1	[illegible]	1
□	2016-03-11 12:[illegible]	Reader-1	Add a reader	1

Figure15-3 Card-independentEvent

15.3.1 Search Events

Steps:

1) Select the field “event type”.
2) Input the search criteria in the “keyword” text box.
3) Click the “Search” button, the matching cards will be shown in card list.
4) If the user wants to view all the cards in the controller, click the “Search All” button.

15.3.2 Export Events

Click the “Export” button, a pop-up download file box appears, all cards will be exported to CSV format, select a path to save the file. Click “OK” to confirm. Please see 7.1.7 Export Function.

15.3.3 Print Events

Click the “Print” button to enter the printing page, the specific operation method see 7.1.8 Print Function.

EverFocus Electronics Corp.

EverFocus Taiwan:
12F-1, No.79, Sec. 1, Shin-Tai Wu Road,
Hsi-Chih, New Taipei City, Taiwan
TEL: +886 2 2698 2334
FAX: +886 2 2698 3943
www.everfocus.com.tw
marketing@everfocus.com.tw

EverFocus Europe - Germany:
Albert-Einstein-Strasse 1, D-46446
Emmerich, Germany
TEL: +49 2822 93940
FAX: +49 2822 939495
www.everfocus.de
sales@everfocus.de

EverFocus China - Beijing:
Room 609, Technology Trade Building,
Shangdi Information Industry Base,
Haidian District, Beijing 100085, China
TEL: +86 10 6297 3336~39
FAX: +86 10 6297 1423
www.everfocus.com.cn
marketing@everfocus.com.cn

EverFocus China - Shenzhen:
4F, No. 2, D4 Building, Wan Yelong
Industrial Park, Tangtou Road, Shiyan,
Baoan, Shenzhen, Guangdong 518101, China
TEL: +86 755 2765 1313
FAX: +86 755 2765 0337
www.everfocus.com.cn
marketing@everfocus.com.cn

EverFocus USA - California:
1801 Highland Avenue, Unit A, Duarte, CA 91010, USA
TEL: +1 626 844 8888
FAX: +1 626 844 8838
www.everfocus.com
sales@everfocus.com

EverFocus Japan:
3F, Kuramochi, Building II, 2-2-3 Koto-Bashi,Sumida-Ku, Tokyo, 130-0022, Japan
TEL: +81 3 5625 8188
FAX: +81 3 5625 8189
www.everfocus.co.jp
info@everfocus.co.jp

Your EverFocus product is designed and manufactured with high quality materials and components which can be recycled and reused.
This symbol means that electrical and electronic equipment, at their end-of-life, should be disposed of separately from your household waste.
Please, dispose of this equipment at your local community waste collection/recycling centre.
In the European Union there are separate collection systems for used electrical and electronic product.
Please, help us to conserve the environment we live in!

Ihr EverFocus Produkt wurde entwickelt und hergestellt mit qualitativ hochwertigen Materialien und Komponenten, die recycelt und wieder verwendet werden können.
Dieses Symbol bedeutet, dass elektrische und elektronische Geräte am Ende ihrer Nutzungsdauer vom Hausmüll getrennt entsorgt werden sollen.
Bitte entsorgen Sie dieses Gerät bei Ihrer örtlichen kommunalen Sammelstelle oder im Recycling Centre.
Helfen Sie uns bitte, die Umwelt zu erhalten, in der wir leben

EverFocus

PN: 4605PNC302X020A_V 3.0