



User Manual



EFS2000 Flex II Series Access Control Management Software Version 2.5

EverFocus Electronics Corporation

EFS2000

Instruction Guide

2007~2009 EverFocus Electronics Corp

Room 609 Technology Trade Building, ShangDi Haidian, Beijing China

Phone 86.10.62973336 • Fax 86.10.62971423

Table of Contents

Table of Contents.....	i
1 Software Introduction	1
1.1 Main Features.....	1
1.2 Feature Highlights.....	1
1.3 Compatible Controller List	2
1.4 System Layout	3
1.5 Hardware Requirements	3
1.6 Install and Uninstall.....	4
1.6.1 Preparation.....	4
1.6.2 Main Program Installation Process.....	5
1.6.3 Uninstall the Program.....	10
1.7 Use of Different Types of Database	12
2 Start to Use Software	15
2.1 Quick Start	15
2.1.1 Add and Configure a Controller	15
2.1.2 Set Access Rule	15
2.1.3 Add Cards to the System	17
2.1.4 Department and Cardholder Setup.....	18
2.1.5 Configure and Manage Attendance	19
2.1.6 Real-time Monitoring	20
2.2 First Time Program Use	21
2.2.1 Launch the Program.....	21
2.2.2 Database Configuration	21
2.3 Software Interface.....	23
2.3.1 Main Window	23
2.3.2 Start Menu	24
2.3.3 Quick Access ToolBar.....	27
2.3.4 Menu.....	28
2.3.5 System Selection Bar.....	29
2.3.6 Control Panel.....	31
2.3.7 Real-time Monitoring	33
2.3.8 System Event Record.....	33
2.3.9 System Status.....	36
3 Basic Management.....	38
3.1 Configure Users and Authorities	38
3.2 Authority Group Setting.....	40
3.2.1 Add an Authority Group.....	40
3.2.2 Edit an Authority Group	41

3.2.3	View Authority Groups	42
3.2.4	Delete an Authority Group	43
3.3	User Setting.....	43
3.3.1	Add a User	44
3.3.2	Edit a User	45
3.3.3	Delete a User	45
4	Cardholder Management	46
4.1	Department Setting.....	46
4.1.1	Add a Department.....	46
4.1.2	Edit a Department.....	47
4.1.3	Delete a Department	47
4.2	Cardholder Setting.....	48
4.2.1	Add a Cardholder	49
4.2.2	Fingerprint Information	52
4.2.3	Import Cardholder Information	58
4.2.4	Edit Cardholder Information	59
4.2.5	Batch-Edit Cardholder Information.....	59
4.2.6	View Cardholder Information.....	60
4.2.7	Delete Cardholders	61
4.2.8	Search Cardholder	62
4.2.9	Refresh Cardholder Information.....	65
4.2.10	Export Cardholder Information	65
4.2.11	Print Cardholder Information	65
5	Controller Management	67
5.1	Add a Controller	69
5.2	Edit a Controller	70
5.3	Delete a Controller	70
5.4	Search Controller(s).....	70
5.4.1	Search a Controller	70
5.4.2	Search all Controllers	70
5.5	Controller Setting.....	71
5.5.1	Door/Floor Setting.....	71
5.5.2	Anti-Passback (APB) Setting	75
5.5.3	Reader Setting	76
5.5.4	Arm Zone Setting	79
5.5.5	Alarm Input Setting	80
5.5.6	Alarm output Setting	82
5.5.7	Alarm Output Time Setting	86
5.5.8	System Setting.....	88
6	Access Rules	93
6.1	Date Setting.....	93
6.1.1	Date Type	93
6.1.2	Recurrent Type	94
6.1.3	Add a Date.....	94
6.1.4	Edit a Date	95
6.1.5	Delete Date(s).....	95

6.2 Door Setting.....	96
6.3 Door Schedule Setting.....	97
6.3.1 Advanced Setting.....	98
6.3.2 Add a Door Schedule.....	98
6.3.3 Rename a Door Schedule	98
6.3.4 Delete a Door Schedule	99
6.3.5 Edit a Door Schedule.....	99
6.3.6 Quick Door Schedule Setting	103
6.3.7 View Details of a Door Schedule	104
6.4 Access Group Setting	104
6.4.1 Add an Access Group	105
6.4.2 Rename an Access Group.....	106
6.4.3 Delete an Access Group	106
6.4.4 Edit an Access Group	106
6.5 Access Group Schedule Setting.....	115
6.5.1 Add an Access Group Schedule	117
6.5.2 Rename an Access Group Schedule	117
6.5.3 Delete an Access Group Schedule.....	117
6.5.4 Edit an Access Group Schedule.....	117
6.5.5 Advanced Setting.....	119
6.5.6 Quick Access Group Schedule Setting	119
6.6 Control Rules for new Controllers	119
6.6.1 To satisfy Control Rules	120
6.6.2 To Satisfy Unlock Condition(s).....	120
7 Card Setting.....	121
7.1 Add a Card	122
7.1.1 Card Format.....	122
7.1.2 Register Cards	123
7.1.3 Card Property.....	123
7.2 Import Card Information.....	125
7.3 Edit Card Information.....	125
7.4 Batch Edit Card Information.....	126
7.5 View Card Information	127
7.5.1 View Card List	127
7.5.2 View Details of Card Infomation	127
7.6 Delete Card(s).....	128
7.6.1 Delete a Card	128
7.6.2 Delete All Cards	128
7.7 Download Card Information.....	128
7.8 Search Card.....	129
7.8.1 Basic Search	129
7.8.2 Advanced Search	130
7.9 Refresh Card Information.....	132
7.10 Export Card Information	132

7.11	Print Card Information	132
8	Data Communication with Controllers	134
8.1	Upload Data to Computer	134
8.2	Download Data to Controller	135
8.3	Acquire Card and Fingerprint Information from Controller	136
8.4	Uploading/downloading Error	136
9	Electronic Map (E-Map) Management.....	138
9.1	Add an E-Map	139
9.2	Add an E-Map link	139
9.3	Add Devices to an E-map	139
9.3.1	Add Controllers	140
9.3.2	Add Doors	140
9.3.3	Add ARM Zones	140
9.3.4	Add Alarm Inputs	141
9.3.5	Add Alarm Outputs	141
9.3.6	Add Fire Alarms	142
9.4	Edit an E-Map	142
9.5	Delete an E-map	143
10	Event Report	144
10.1	View Event Report	144
10.2	Sort Event Report.....	144
10.3	Search Event Report	145
10.3.1	Search Criteria for Each Event Type	145
10.3.2	Search Condition	146
10.3.3	Search for Single Event Type	147
10.3.4	Search for Multiple Event Types	148
10.4	Refresh Event Report.....	148
10.5	Export Event Report.....	148
11	Device Control	149
11.1	Resources List.....	149
11.2	Remote Set/Reset Alarm	150
11.3	Remote ARM/disarm	151
11.4	Remote Open Door.....	151
11.5	Remote Lock/Unlock Exterior Area	152

12 Attendance Management.....	153
12.1 Holiday Setting	153
12.1.1 Department Week Holiday Setting.....	154
12.1.2 Department Special Holiday Setting	154
12.1.3 Add a Holiday.....	155
12.1.4 Edit a Holiday.....	155
12.1.5 Delete Holiday(s).....	156
12.2 Event Management	156
12.2.1 No-Access-Attendance Enrollment	156
12.2.2 Overtime Enrollment.....	160
12.2.3 Time-off Enrollment.....	165
12.3 Attendance Report	169
12.3.1 Attendance Statistics Report.....	169
12.3.2 Detailed Attendance Report.....	173
13 Database Management	176
13.1 Configure Database.....	176
13.2 Backup Database	177
13.3 Restore Database	178
13.4 Import Database.....	179
13.4.1 Import Cardholder Information	179
13.4.2 Import Card Information	180
13.5 Purge out-of-date data	182
14 Concept Interpretation.....	184
14.1 Area Anti-Passback (APB)	184
14.1.1 Concept of Area.....	184
14.1.2 Exterior Area and Exterior Doors.....	184
14.1.3 Areas and Readers	185
14.1.4 APB Enabled	185
14.1.5 Card APB Enabled	186
14.1.6 Example of APB Event.....	187

Chapter 1

1 Software Introduction

1.1 Main Features

EFS2000 Flex II Access Control Management Software (hereinafter referred to as "Software") is designed to manage EverAccess 1, 2, 4, & 8 zone door controllers and fingerprint readers developed by EverFocus. The Software also stores and maintains system data, and provides attendance management functions.

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

The Software offers different levels of operating authority. To prevent unauthorized access, a user name and password are required to login to the Software, and the system database is encrypted. User settings are designed to distinguish between users with different operating authority levels. Users belonging to different authority groups will have different operating privileges in the Software. In addition, panic PIN access and multi-card access enhances the efficiency as well as the security of the access control system.

1.2 Feature Highlights

- ❖ Support different series of controllers
 - ✧ Support ELA82x, ELA85x, ELA890, Flex I, Flex II series controllers
- ❖ Support accessory hardware
 - ✧ Support desktop reader, USB card reader and 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
- ❖ Supports a wide range of databases Engines
 - ✧ Support databases by: MS SqlServer (2000 or higher), Oracle (9i or higher), MS Access (2003 or higher) and MySQL. User can choose a database type based on their needs and company standards.
 - ✧ Supports database backup and restoration
 - ✧ Users can switch between two types of databases to ensure data integrity
- ❖ Supports multiple language options
 - ✧ Users can edit the Software language package to match the local language.
- ❖ Software features
 - ✧ Supports customized interface design including user defined software title, company name and Logo; users can create shortcuts for commonly used commands

- ✧ Real-time monitoring of controllers, doors, zone arming status, alarm input/output and fire alarm activation on user defined E-maps, enabling operators to directly monitor system status and respond accordingly
- ✧ Supports remote control of controllers, doors, arm zones and alarms
- ✧ Supports panic PIN access and multi-card access
- ✧ Size of operating windows and panels can be adjusted
- ✧ Simple and practical attendance management

1.3 Compatible Controller List

The following table gives the compatibility between the Management Software and different controller models. A check mark “√” in the cells indicates the software can manage that controller.

		Access control Software	ENS800 WEB Access control Software	EFS2000 Flex II Access control Software	ENS2000 WEB Access control Software
ELA82x	ELA831		√	√	√
	ELA822				
	ELA808				
	ELA828				
ELA85x	ELA852		√	√	√
	ELA854				
	ELA858				
EFC-I	EFC-02-1A	√	√	√	√
	EFC-04-1A				
	EFC-06-1A				
	EFC-08-1A				
EFC-II	EFC-01-2A			√	√
	EFC-02-2A				
	EFC-04-2A				
	EFC-06-2A				
	EFC-08-2A				
Fingerprint	ELA900	√		√	√
	EBC900			√	√
EFC-Lift	EFC-Lift	√	√	√	√

1.4 System Layout

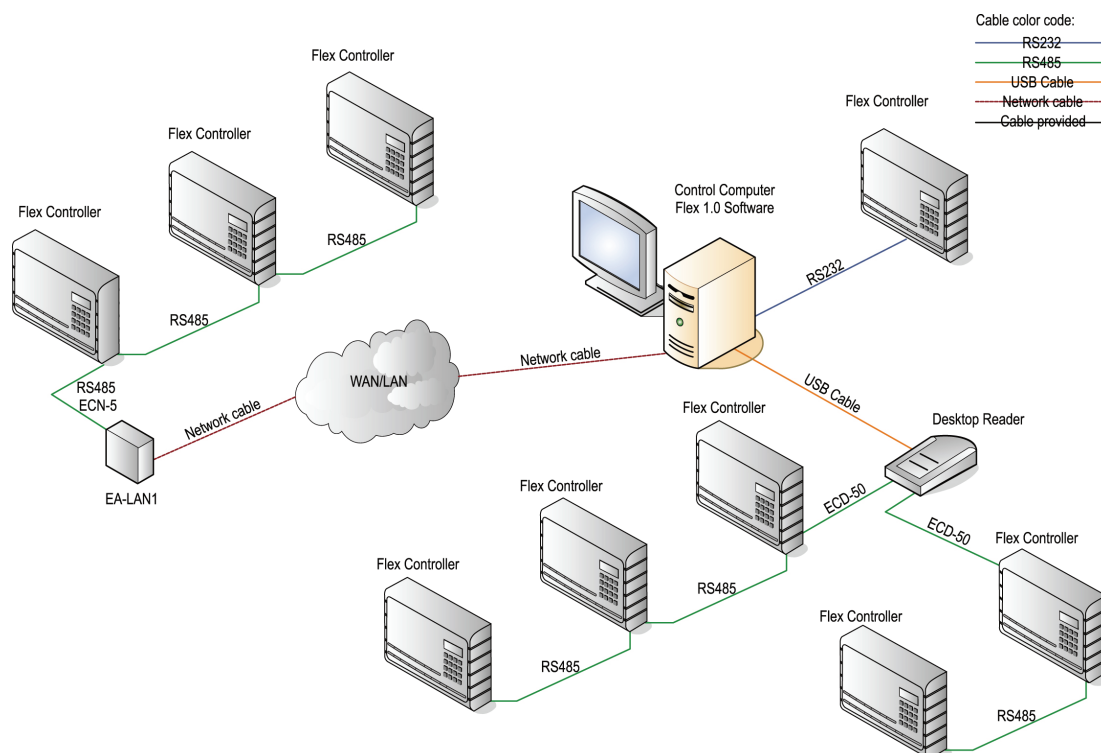


Fig. 1-1 System layout

1.5 Hardware Requirements

The minimum hardware requirements for a PC to run the main Access Control Management System software are listed below. To achieve better Software performance, please use the recommended equipment.

System requirements for installation of the Software

Content	Requirements
Processor	Intel Pentium III processor, 800MHz, Recommended: Intel Pentium IV or higher, 1GHz
Memory	256MB, Recommended: 512MB
Hard disk	Available space: 100MB on the drive that the operating system is installed and 1GB on the drive that the software is installed
Operating system	Windows2000 or higher
Browser	Microsoft Internet Explorer 5.0 or higher
Display	1024 x 768, 32 bit color

USB interface	USB1.0 or higher
---------------	------------------

For installation, the default installation location is the system drive. Users can also choose other drives for the installation. To protect the operating system and ensure good Software performance, make sure that the system drive (usually the C drive) has enough available space. In addition, extra storage space may be needed for future data and image storage; system planning should account for future growth.

1.6 Install and Uninstall

Before starting installation, make sure that the computer meets the system requirements above. It is strongly recommended to close all applications during installation. If an earlier version of the Software has been installed in the computer, uninstall the earlier version through “Install or Uninstall Programs”. Please back up any user data in a separate folder or on another drive. Failure to properly remove an earlier version may prevent the Software from installing correctly. Refer to section 1.6.3 Uninstall the program for details.

1.6.1 Preparation

The software is based on *Microsoft .Net Framework* (Version 2.0). Data export and print-related functions are based on *Crystal Reports for Visual Studio.NET* (Version 10.0). The required software is included in the installation CD. Please install the software in the folder recommended by the installation process. You may also visit the Microsoft official website to download the latest version of the software for your system.

1. Install .Net Framework: Insert the installation CD to the computer’s CD-ROM drive. Open "My Computer" > “CD drive” and run the "dotnetfx.exe" file in the corresponding folder. The installation window is shown below:

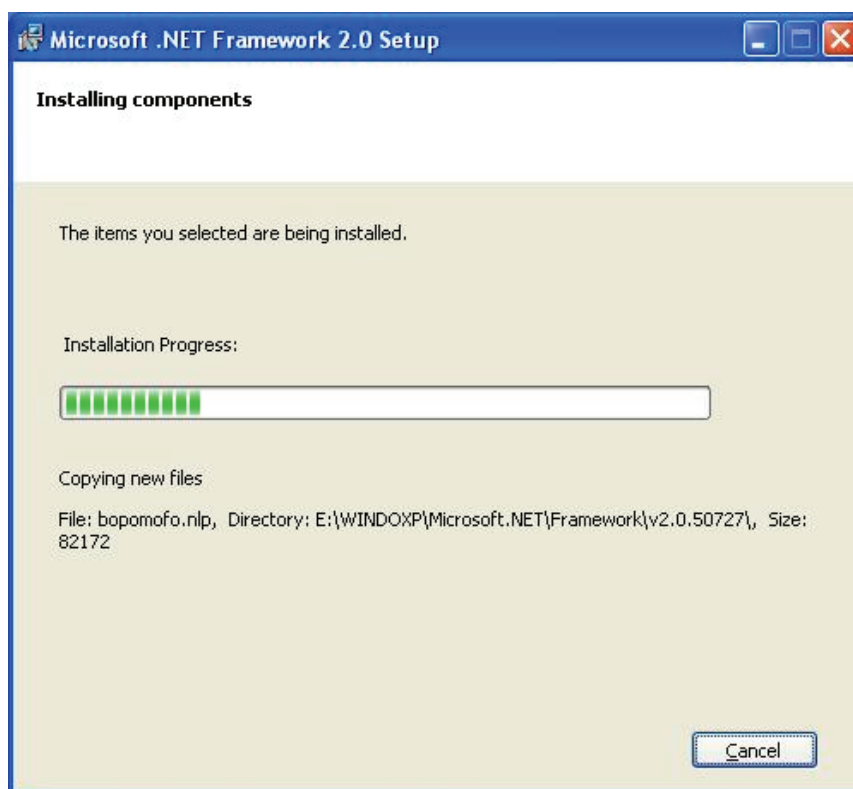


Fig. 1-2 Installation Window

2. Install Crystal Reports: Insert the installation CD to the computer's CD-ROM drive. Open "My Computer" > "CD drive:" and run the "CRRedist2005_x86.msi" file in the corresponding folder. Follow instructions to finish the installation.

1.6.2 Main Program Installation Process

1. Insert the installation CD to the computer's CD-ROM drive. Open "My Computer" and double click "Setup.exe" file under the CD drive to start the installation. If the Windows system version is not updated to the required level. Login to the Microsoft Windows official site to download the latest version of the Software and install.

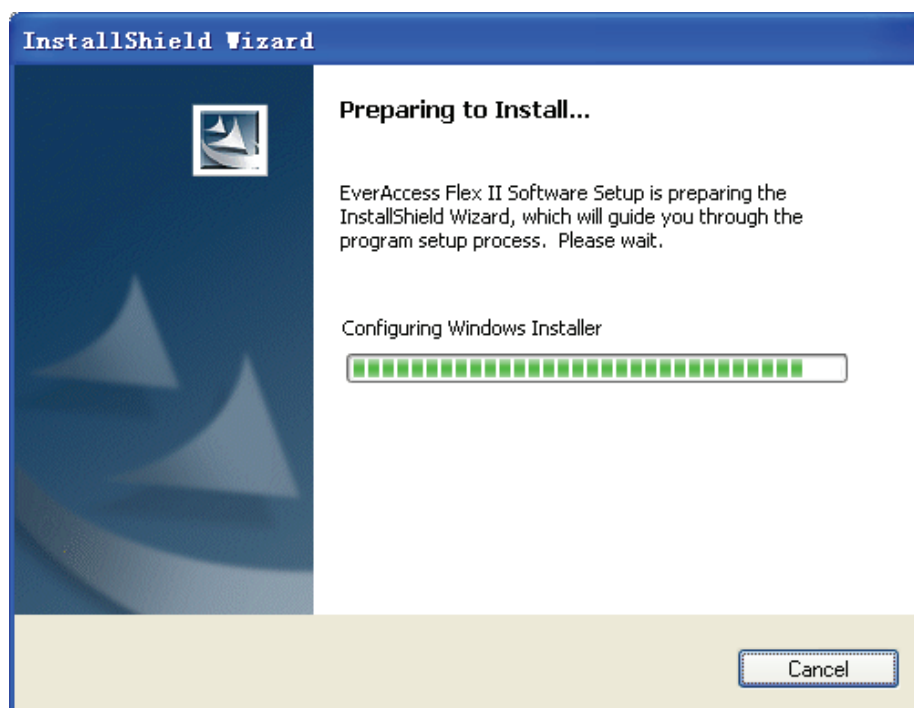


Fig. 1-3 Install the Software

2. The Installer program will collect system parameters, which may take a few seconds to a few minutes depends on the computer configuration and system performance. The following Welcome window will be shown when that process completes.

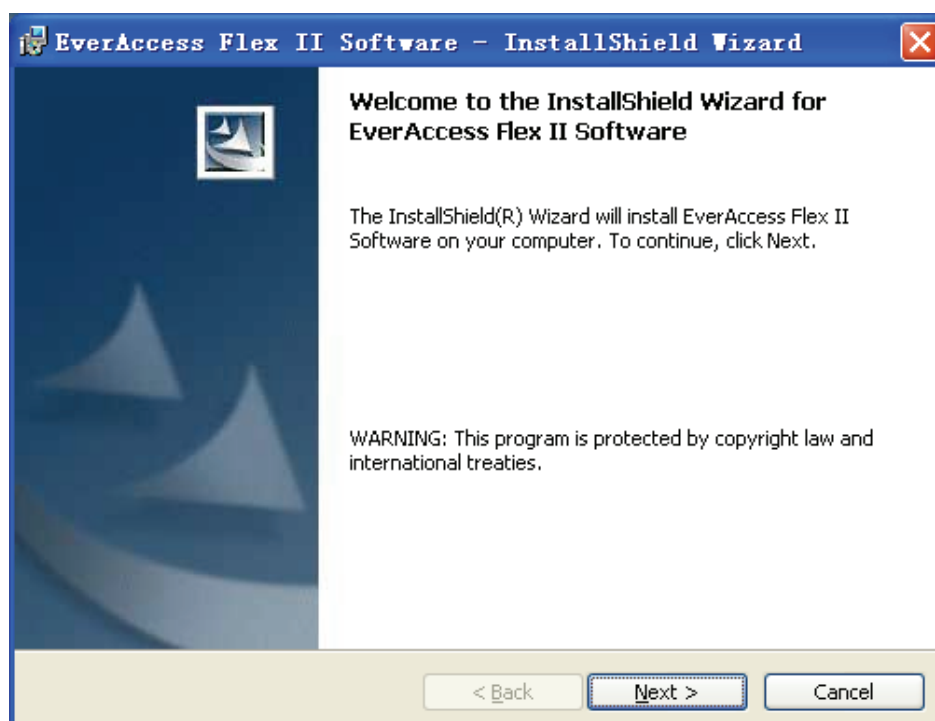


Fig. 1-4 Welcome window

Please click "Next" to continue the installation. Otherwise, click "Cancel" to exit the installation. In all following steps, the window will offer "Back", "Next", "Cancel" and other

installation options. Click “Next” after selecting each installation option, or click “Cancel” to exit the installation. Click “Back” will return to the previous window.

3. Click “Next” to view “license agreement” (see below), please read the contents carefully. Users must accept the terms in the agreement by checking “I accept terms in the license agreement” to continue the installation.

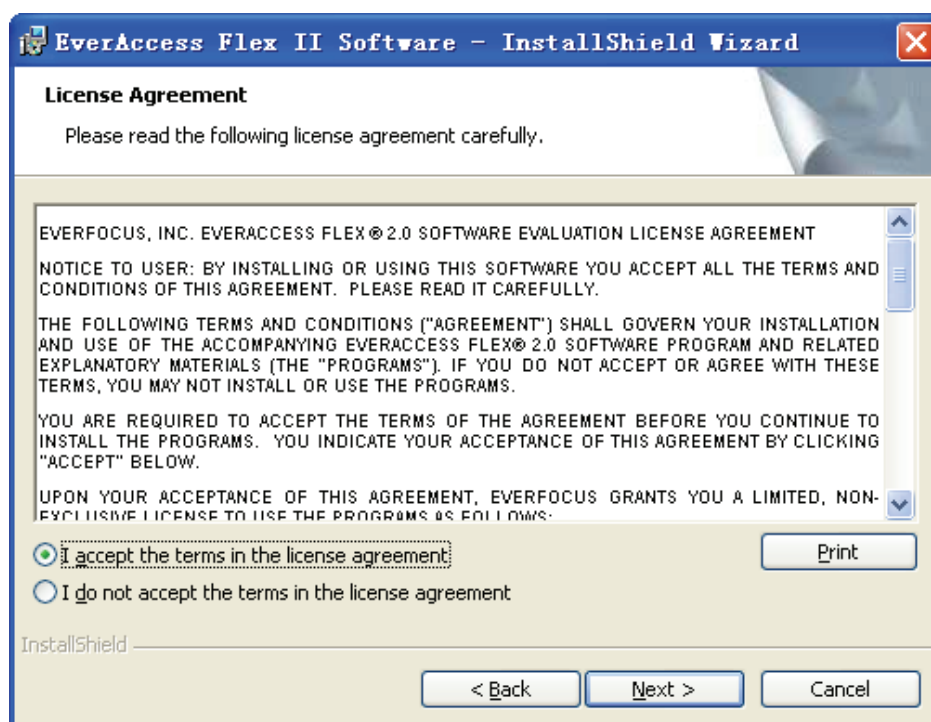
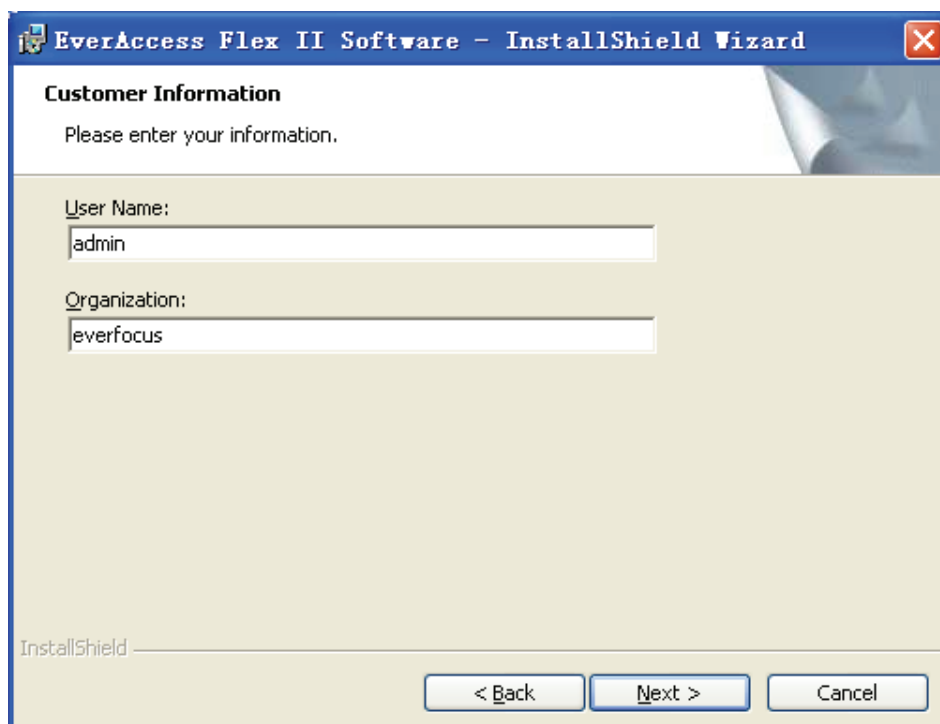


Fig. 1-5 license agreement

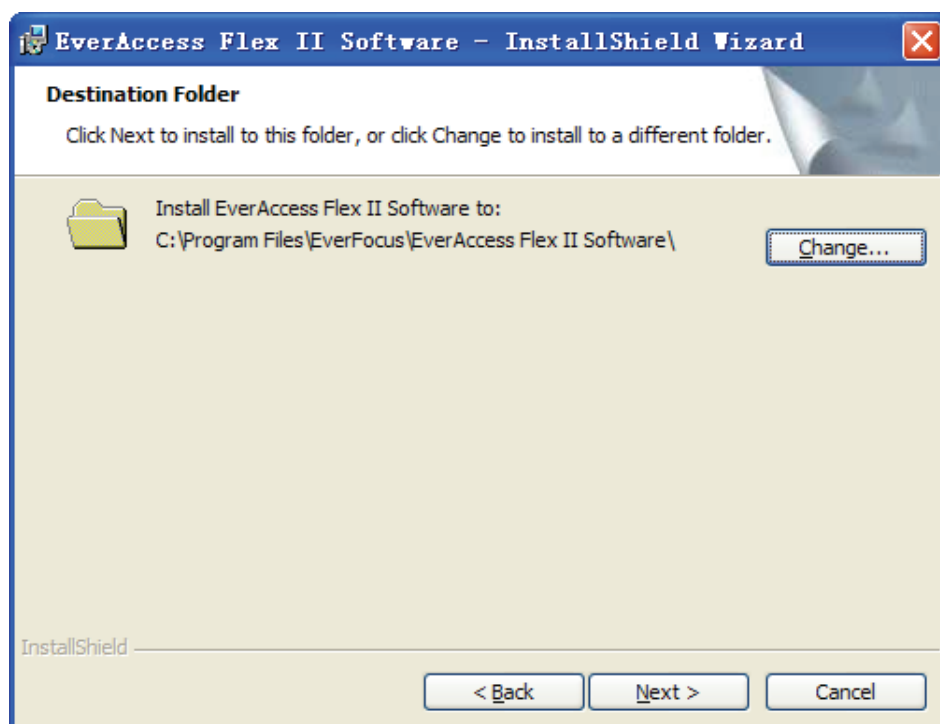
4. Click “Next” to enter the “Customer Information” window (see below). Enter user name and organization or leave the fields empty.



The screenshot shows the 'Customer Information' screen of the 'EverAccess Flex II Software - InstallShield Wizard'. The window has a blue title bar with the text 'EverAccess Flex II Software - InstallShield Wizard' and a red close button. Below the title bar, the text 'Customer Information' is displayed in bold, followed by the instruction 'Please enter your information.' There are two text input fields: 'User Name:' with the value 'admin' and 'Organization:' with the value 'everfocus'. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'InstallShield' logo is visible in the bottom left corner.

Fig. 1-5 Customer Information

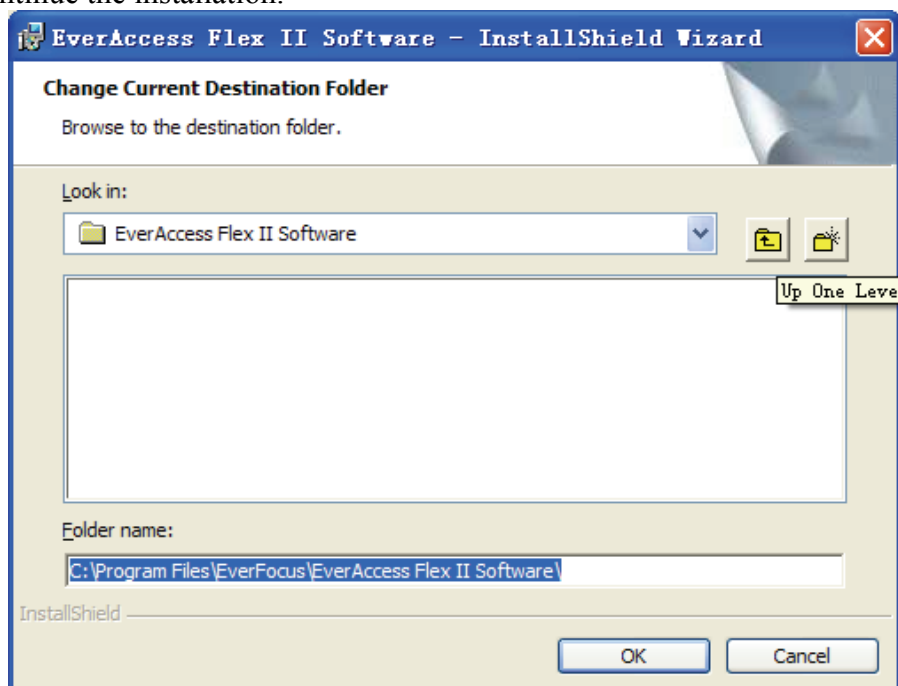
5. In the following step, the installation process will prompt you to choose a destination folder for the Software (see below). The default folder is the Program Files folder on the system drive. It is important to choose a drive with enough storage space for the installation and operation of the Software.



The screenshot shows the 'Destination Folder' screen of the 'EverAccess Flex II Software - InstallShield Wizard'. The window has a blue title bar with the text 'EverAccess Flex II Software - InstallShield Wizard' and a red close button. Below the title bar, the text 'Destination Folder' is displayed in bold, followed by the instruction 'Click Next to install to this folder, or click Change to install to a different folder.' There is a folder icon next to the text 'Install EverAccess Flex II Software to:' and the default path 'C:\Program Files\EverFocus\EverAccess Flex II Software\'. A 'Change...' button is located to the right of the path. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'InstallShield' logo is visible in the bottom left corner.

Fig. 1-5 Select Installation Folder

If necessary, click “Change” and choose a new destination folder from the folder menu. Click “OK” to continue the installation.



6. Click “Next” and the installer program will show “Ready to Install the Program” (see below). If correct, click “Install” to start the installation. Or click “Back” to return to previous pages to change installation options. Click “Cancel” to exit the installation.

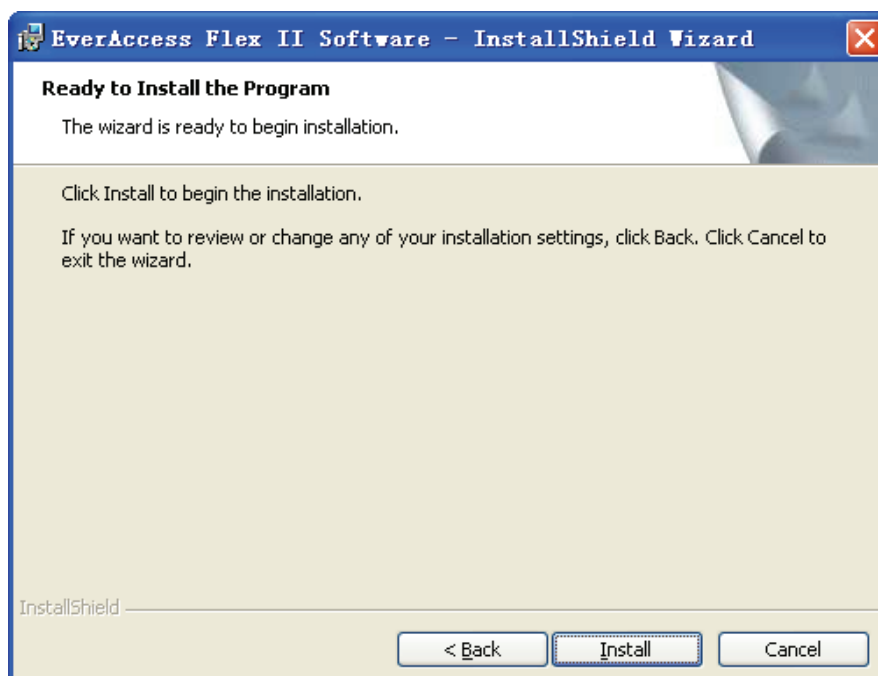


Fig. 1-8 Installation Option

7. After clicking “Install”, the system will automatically install the Software and database. The process may take several minutes depending on the computer configuration and system performance. Should you wish to stop the installation, click “Cancel”.

8. The following window will be shown after installation.

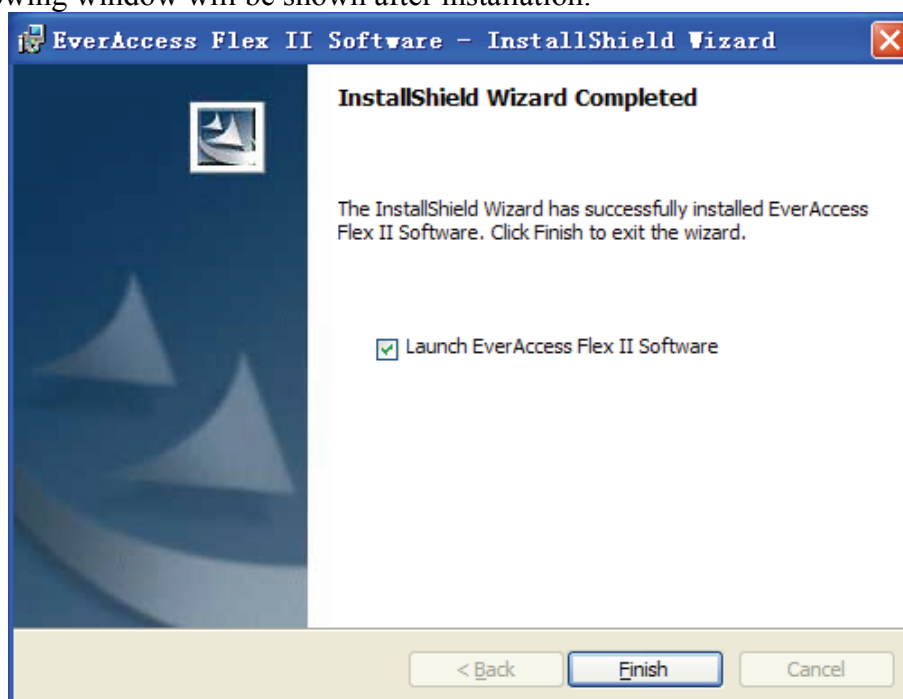


Fig. 1-9 Installation Complete

The installation is now complete. Click “Finish” to exit. If “Launch EverAccess Flex II Software” is checked, the system will automatically launch the Software after installation (a USB dongle needs to be inserted before the Software can be launched; each Software package comes with a different dongle). To launch the program, the user can also double click the shortcut icon  on the desktop or choose “Start” → “Programs” → “EverFocus” → “EverAccess Flex II Software” to launch the Software.

1.6.3 Uninstall the Program

To uninstall the program, enter “Control Panel” and double click “Add/Remove Programs” and select “EverAccess Flex II Software” from the program list. Click “Modify/Remove” button to operate.

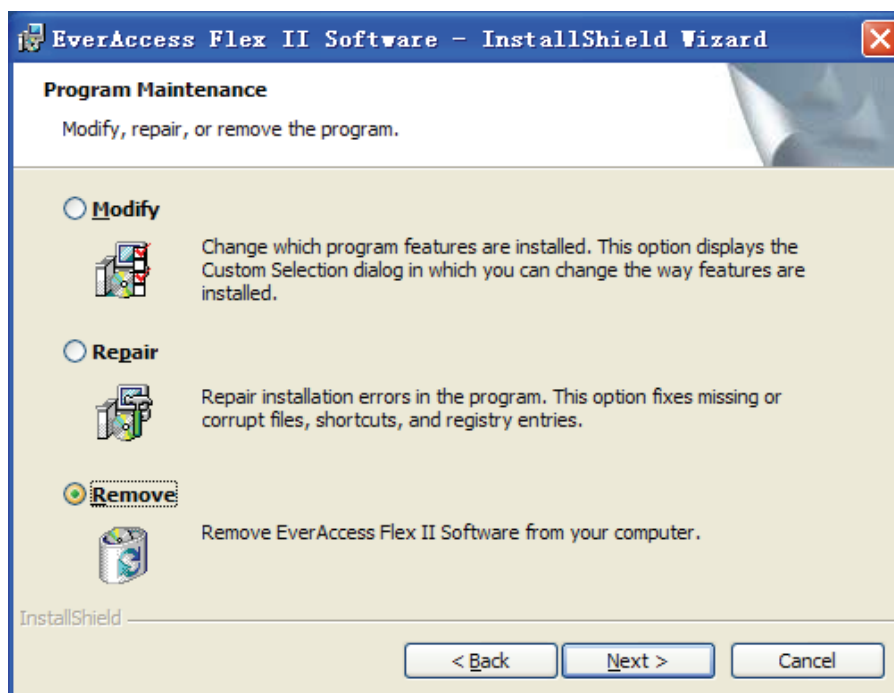


Fig. 1-10 Uninstall the Program

Select "Remove" and click "Next". The Software will prompt the user to confirm the intent to uninstall the program, as in Fig. 1-11.

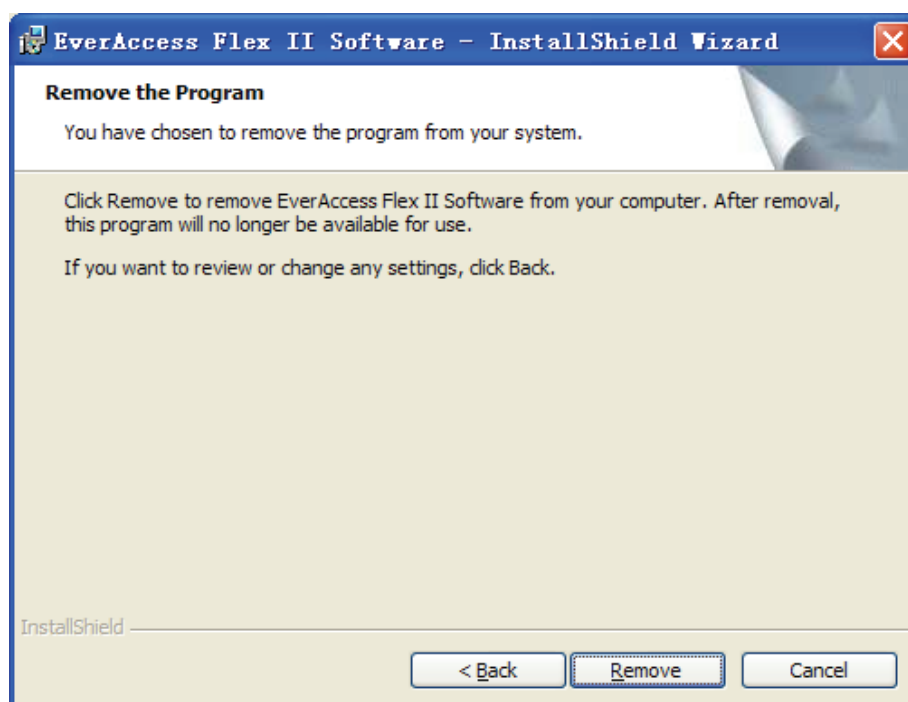


Fig. 1-11 Prompt to confirm uninstalling the Program

Click "Remove" to confirm. An "uninstall succeeded" dialog box will be shown (Fig. 1-12). Click "Finish" to exit. All programs related to the Software are removed from the computer. (The .Net Framework and Crystal Reports won't be removed, they must manually uninstall if you want.)

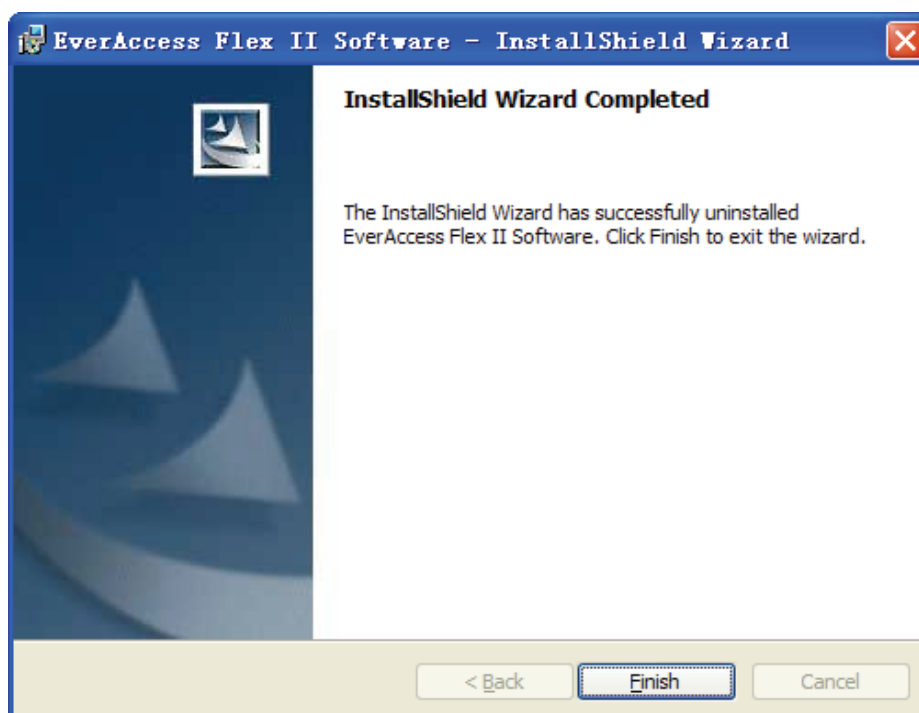


Fig. 1-5 Removal Complete

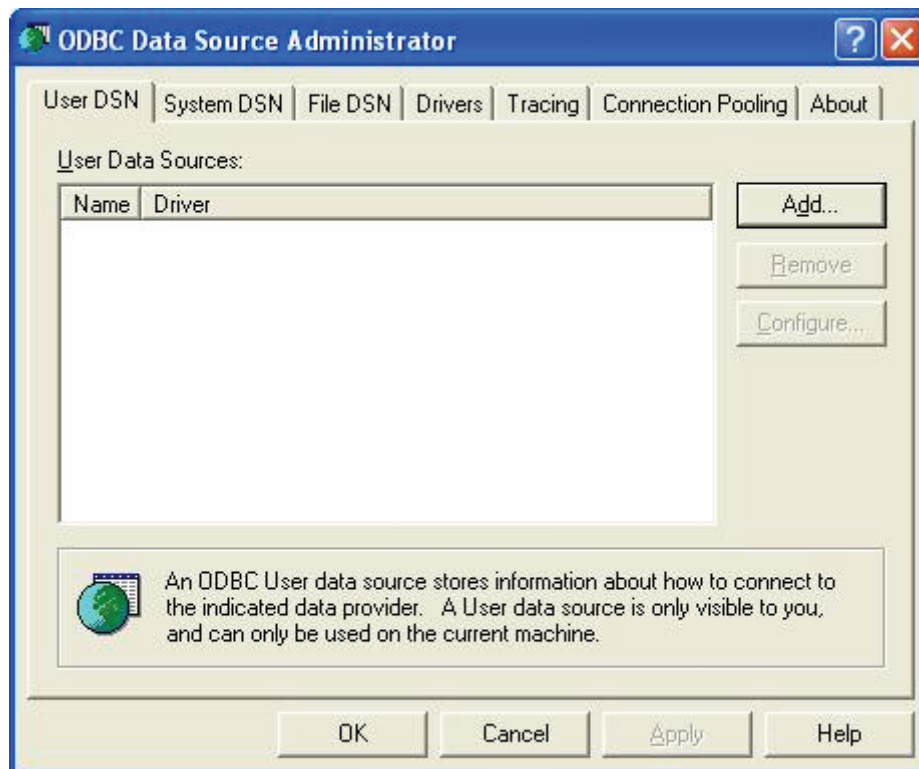
1.7 Use of Different Types of Database

Users need to configure their database engine before using it in the Software. There are 4 types of database systems supported by the Software:

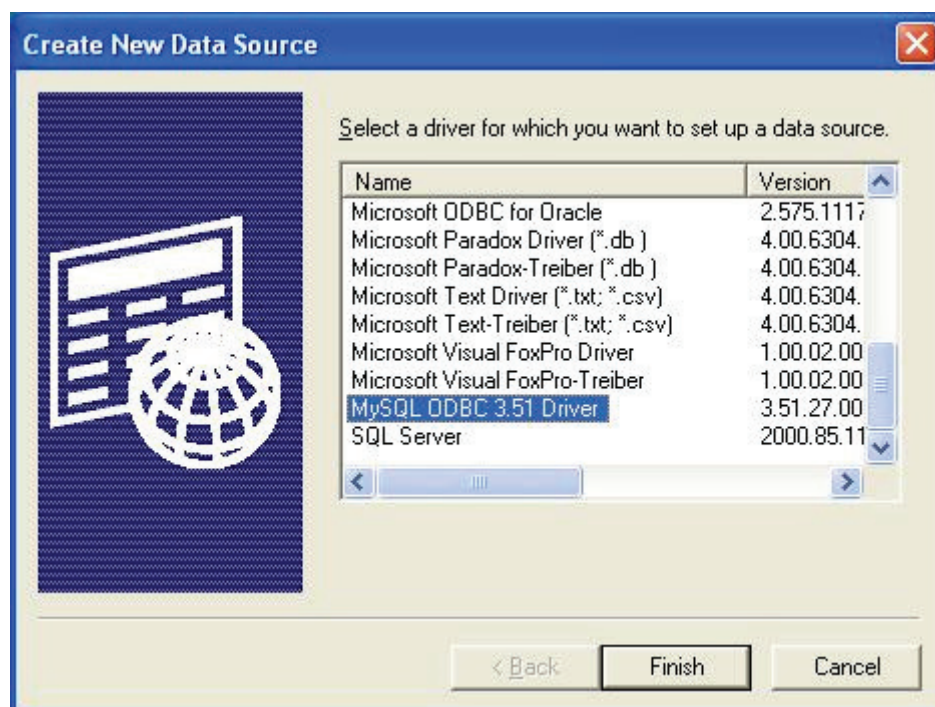
- ✧ MS SqlServer: can be directly used in the Software without special configuration. Database IP (Computer IP of the data source), login name and password are needed.
- ✧ Oracle (version 9i or higher): can be directly used in the Software without configuration. Database server name, login name and password are needed.
- ✧ Access (version 2003 or higher): can be directly used in the Software without configuration. Users can create a database password.
- ✧ Mysql: it is necessary to first configure the ODBC data source. Computer IP of the data source, database login name and password are needed.

To configure an ODBC data source:

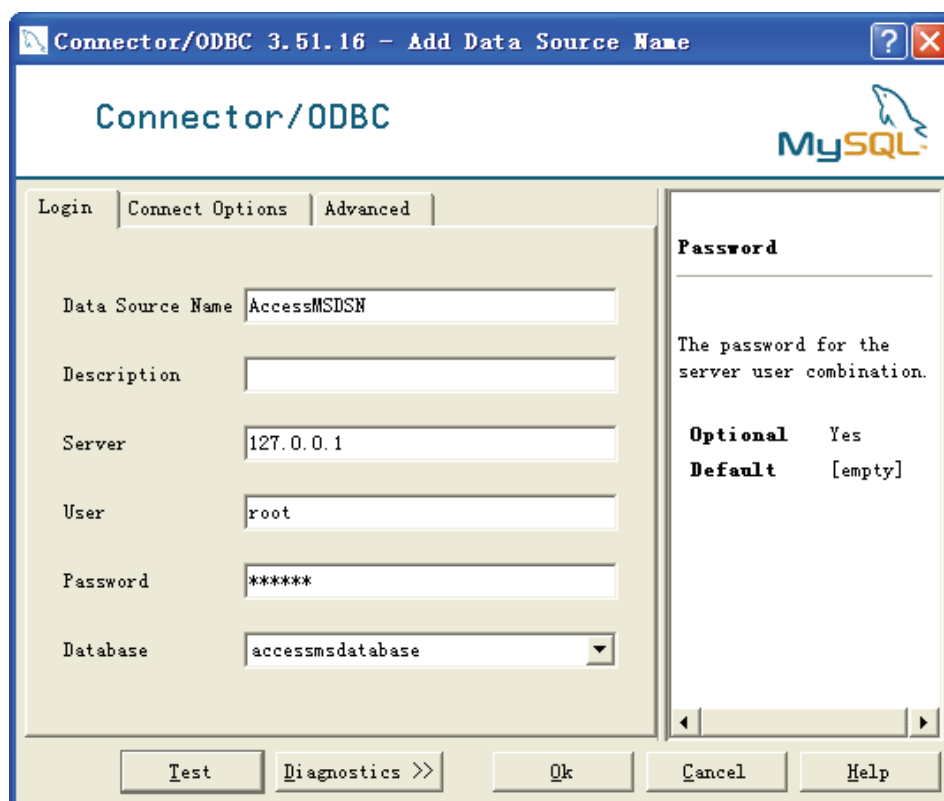
1. Create Database: create an empty database in MySql database with the name "AccessMSDatabase"
2. Open data sources (ODBC): through "Start" → "Settings" → "Control Panel" → "Administrative Tools" → "Data sources (ODBC)".
3. Create a data source: select tab "User DSN" and click "Add".



4. Select the driver "MySQL ODBC 3.51 Driver", and click "Finish". If the driver cannot be found, download the "MySQL ODBC driver" and install before proceeding with database configuration.



5. Configure data source: the “data source name” must be “AccessMSDSN”. Enter the appropriate information in “server”, “user” and “password” fields. Those will be the database computer’s IP, login name and password respectively. Enter “AccessMSDatabase” in “Database” field, as shown below:



Click “Test”, if the success dialog box pops up, the configuration of the data source is complete.



Otherwise, edit the content according to any error messages until the success dialog box pops up.

Chapter 2

2 Start to Use Software

This chapter describes how to quickly set up a controller in the Software (the example is based on the user having the authority level of a super administrator) and using the controller to control doors and collect attendance records. Please follow these steps to get familiar with the software. For a more comprehensive understanding of each function, please refer to chapters on related topics.

2.1 Quick Start

2.1.1 Add and Configure a Controller

Click “Access Control Management” ➔ “Controller Setting” to access the controller setting window. Follow the steps described below to add a controller. Refer to Section 5.1 Add a Controller for details.

Operation Steps:

1. Click “Add” button on the upper right corner. Enter controller serial port, address, type and location.
2. If the controller is online, click “Search and Save” button.
3. If the controller is offline, click “Save”. Search the controller by “Search” button after the controller is connected.

2.1.2 Set Access Rule

2.1.2.1 Date Setting

Click “Access Control Management” ➔ “Access Rule” ➔ “Date Setting” to open the window for setting date. Follow the steps described below to add a date. Refer to Section 6.1 Date Setting for details.

Operation Steps:

1. Click “Add” button on the upper right corner.
2. Select type or frequency of recurrence, date and date type, and click “save” to add the new date. The setting will be downloaded to all controllers. Priority of date types: floating holiday> day off> legal holiday.
3. If a controller is offline, the setting will be saved in the database. You will need to download the new setting manually to the controller when the controller is connected.

2.1.2.2 Door Schedule Setting

Create door schedules first, and then assign a door schedule to each door in the door setting window. Click “Access Control Management” ➔ “Access Rule” ➔ “Door Schedule Setting” to open the window for door schedule setting. Follow the steps described below to add a door schedule. Refer to Section 6.3 Door Schedule Setting for details.

Operation Steps:

1. Click “Add” button on the upper right corner.
2. Enter a name for the door schedule in the text box, and click “save” to add the new door schedule.
3. Click the “Edit” button . Set time zone and door verification mode in the pop up dialog box. Click “Save” and close the dialog box.

2.1.2.3 Door Setting

Click “Access Control Management” ➔ “Access Rule” ➔ “Door Setting” to open the window for door setting. Follow the steps described below to add a door. Refer to Section 6.2 Door Setting for details.

Operation Steps:

1. Select a controller from the controller list on the left.
2. On the right panel, name each door zone and assign a door schedule for each door zone under the controller.
3. Click “Save” and the door setting will be downloaded to the controller.

2.1.2.4 Access Group Schedule Setting

Create access group schedules first, and then assign an access group schedule to each door in the door setting window. Click “Access Control Management” ➔ “Access Rule” ➔ “Access Group Schedule Setting” to open the window for access group schedule setting. Follow the steps described below to add an access group schedule. Refer to Section 6.5 Access Group Schedule Setting for details.

Operation Steps:

1. Click “Add” button on the upper right corner.
2. Enter a name for the new access group schedule in the text box, and click “save” to add the new access group schedule.
3. Click the “Edit” button . Set time zone and access permission in the pop up dialog box. Click “Save” and close the dialog box.

2.1.2.5 Access Group Setting

Click “Access Control Management” ➔ “Access Rule” ➔ “Access Group Setting” to open the window for access group setting. Follow the steps described below to add an access group. Refer to Section 6.4 Access Group Setting for details.

Operation Steps:

1. Click “Add” button on the upper right corner.
2. Enter the name of the new access group in the text box, and click “save” to add the new access group.
3. Click “Access group Schedule” button , and a dialog box for access group schedule setting will pop up.
4. Select a controller from the controller list on the left.
5. Assign a controller group for the access group.
6. Assign an access group schedule to each door zone under the controller.
7. Click “Save” button and the door schedule setting will be downloaded to the controller.

2.1.3 Add Cards to the System

The Software provides multiple ways to add a card to the system. Users can choose any of them. Follow the instruction below to add a card to the system and assign an access group for the card. The Software will automatically set the card properties to the default setting when adding cards to the system except in the method described in 2.1.3.2. The default access group is “Full Granted” (Refer to Section 6.4 Access Group Setting for details); the default PIN is “000000”; the options of “First Card” and “Enable Card” are enabled. Select card index from the pop-up dialog box for the card format selection window (the card Index will be shown in the “card number” text box after selecting a card format). The validation date is the current time (accurate to the minute).

2.1.3.1 Quick Add a Card

If controllers have been added to the Software, they will be shown in the resources list located on the left of the main window. If one presents a card to a controller, an event will be shown in the event report list. Users can quick enroll that card into the Software and all controllers by following the steps described below. Refer to Section 2.3.8.1 Granted Access Record for details.

Operation Steps:

1. If necessary enter the “controller setting” window and add a controller (Refer to Section 5.1 Add a Controller for details). The added controller will be shown in the resources list located on the left of the main window.
2. Swipe the card to be added through a reader managed by the controller.
3. The swiped card will be shown in the system event record (granted access record or denied access record), choose “Enroll card” from the right-click menu.
4. Choose card format based on the card number, click “Save” to complete the operation.

2.1.3.2 Card Setting Window

Click “Access Management” ➔ “Card Setting” to enter the card setting window. Follow the steps described below to add a card and assign an access group to the card. Refer to Section 7.1 Add a Card for details.

Operation Steps:

1. Click “Add” button on the upper right corner to open the window for adding a card.
2. Select card format and enter values for each card property item.
3. If there are cardholders in the system, users can assign the card to a cardholder.
4. Select an access group for the card from the “access group” drop-down menu.
5. Alternatively, click “Card Schedule” and assign a special access schedule for the card. If a “Card Schedule” is applied to a card, the card schedule will be used for that card, i.e. the card schedule has the highest priority.
6. Click “Save” to complete the operation.

2.1.3.3 Import Card Information from Excel File

Enter card information in an Excel file (there is no limit on the number of cards), and save the Excel file. Import the cards to the Software and associated controllers by the “import card information” operation (whether a card is registered to a controller depends on the access group setting of the card. If no access group is assigned for the card, the default access group “Full Granted” will be assigned to the card. Refer to Section 13.4.2 Import Card Information for details).

Click “Database Management” ➔ “Import Data” ➔ “Import Card Information”

Operation Steps:

1. Click the "Browse" button, and select the Excel file to be imported.
2. Select the related data fields
3. Click “Import”, select card format, and enter contents for each option
4. Click “Save” to finish the operation.

2.1.3.4 Upload Card Information from Controllers

If a card has been enrolled to the controller, users can upload card information from the controller to the Software (the default access group is “Full Granted”. Refer to Section 8.1 Upload Data to Computer for details). Click “Access Control Management” ➔ “Data Communication” ➔ “Upload data to Computer” to open the window for uploading data to computer (If there have other cards in the controller, they will be uploaded.)

Operation Steps:

1. Enroll the card to a controller
2. Select the address of the controller, and card setting
3. Click “Save” button, select card format and enter contents for each items.

2.1.4 Department and Cardholder Setup**2.1.4.1 Department Setting**

Click “Cardholder Management” ➔ “Department Setting” to open the window for department setting. Follow the steps described below to add a department (Refer to Section 4.1 Department Setting for details).

The first you use the Software to add a department, the Software prompts that the first-level parent department is the company. Click “Yes” if users need to edit company information, otherwise, click “No”.

Operation Steps:

1. Click the “Add” button on the upper right corner
2. Select a parent department.
3. Enter department name.
4. Click “Save” to complete the operation.

2.1.4.2 Cardholder Setting

Click “Cardholder Management” ➔ “Cardholder Setting” to open the window for setting the cardholder. Follow the steps described below to add a cardholder. Refer to Section 4.2.1 Add a Cardholder for details.

Operation Steps:

1. Click the “Add” button on the upper right corner to open the window for adding a cardholder.
2. Enter cardholder number, full name and department etc, upload the cardholder’s photo and fingerprint.
3. User can choose to assign a card to the cardholder.
4. Click “Save” to complete the operation.

2.1.5 Configure and Manage Attendance

2.1.5.1 Holiday Setting

Click “Attendance Management” ➔ “Holiday Setting” to open the window for holiday setting. Follow the steps described below to add a holiday. Refer to Section 12.1 Holiday Setting for details.

Operation Steps:

1. Select workdays and holidays for each department on the right panel.
2. Select a department, and click “Add” on the upper right corner to add a holiday for the department.
3. Select date and attendance type.
4. Click “Save” to complete the operation.

2.1.5.2 No-Access-Attendance Enrollment

If an employee cannot swipe cards for reasons of business travel or others, a “no-access-attendance” should be recorded to reflect the actual attendance.

Click “Attendance Management” ➔ “Event Management” ➔ “No-Access-Attendance Enrollment” to open the window for no-access-attendance enrollment. Follow the steps described below to add a no-access-attendance record. Refer to Section 12.2.1 No-Access-Attendance for details.

Operation Steps:

1. Click “Add” on the upper right corner to open the window for adding a no-access-attendance record.
2. Enter the cardholder manually, or select the cardholder from department.
3. Enter enrollment time and remarks.
4. Click “Save” to complete the operation.

2.1.5.3 Overtime Enrollment

If an employee cannot swipe cards for reasons of business travel or others, an “overtime enrollment” should be recorded to reflect the actual overtime.

Click “Attendance Management” ➔ “Event Management” ➔ “Overtime Enrollment” to open the window for overtime enrollment. Follow the steps described below to add an overtime record. Refer to Section 12.2.2 Overtime Enrollment for details.

Operation Steps:

1. Click “Add” on the upper right corner to enter to window for adding an overtime record.
2. Type in the cardholder manually, or select the cardholder from department.
3. Enter overtime date, hours and remarks.
4. Click “Save” to complete the operation.

2.1.5.4 Time-off Enrollment

If an employee cannot swipe cards because of time off, a “time off enrollment” should be recorded to reflect the scheduled time off.

Click “Attendance Management” ➔ “Event Management” ➔ “Time-off Enrollment” to open the window for time-off enrollment. Follow the steps described below to add a time-off record. Refer to Section 12.2.3 Time-off Enrollment for details.

Operation Steps:

1. Click “Add” on the upper right corner to enter to window for adding a time-off record.
2. Type in the cardholder manually, or select the cardholder from a department.
3. Enter time-off start time, end time, hours and remarks.
4. Click “Save” to complete the operation.

2.1.6 Real-time Monitoring

Click “Real-time Monitoring” on the upper right corner of the window. The real-time status of E-maps in the system is shown on the upper panel. Click the E-maps on the left to view details.

On the lower panel, the real-time system status is shown in “system status bar”; click each item to view details.

2.2 First Time Program Use

2.2.1 Launch the Program

Before launching the program, make sure that the program is installed in the computer. Refer to Section 1.6.2 Main Program Installation Process for installation. In addition, make sure the dongle included in the Software package has been inserted in a USB port on the computer (dongles from different Software package cannot be interchanged). Refer to dongle user manual for details. Double click the shortcut icon on the desktop  or choose “Start” → “Programs” → “EverFocus” → “EverAccess Flex II Software” to launch the Software.

2.2.2 Database Configuration

Upon starting, a database configuration dialog box will pop up as shown below. The Software supports 4 types of commonly used database. Refer to Section 1.7 Use of Different Types of Databases for details.

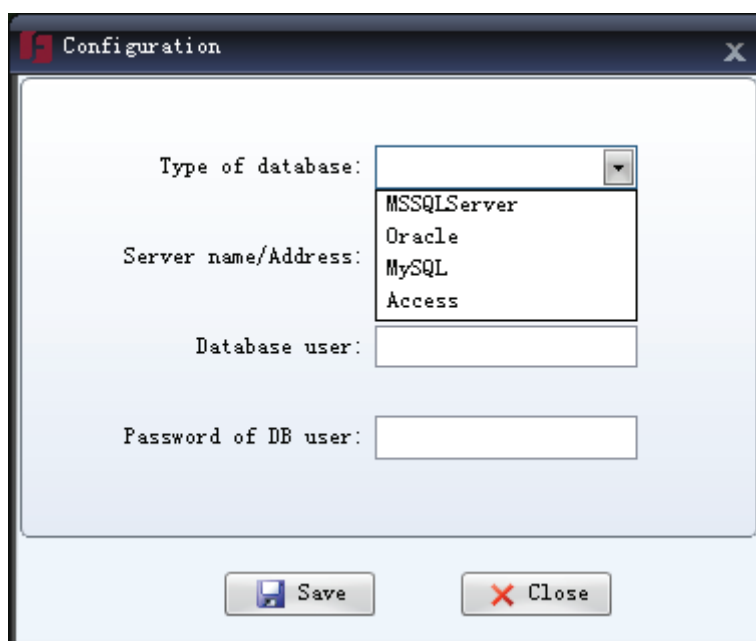


Fig. 2-1 Database Configuration Window

Select the right database type and fill in data fields for each item. Click “Save”. If there are errors in database configuration (Fig. 2-2), a message will pop up (Fig. 2-3). Correct the errors according to the message and enter the login window.

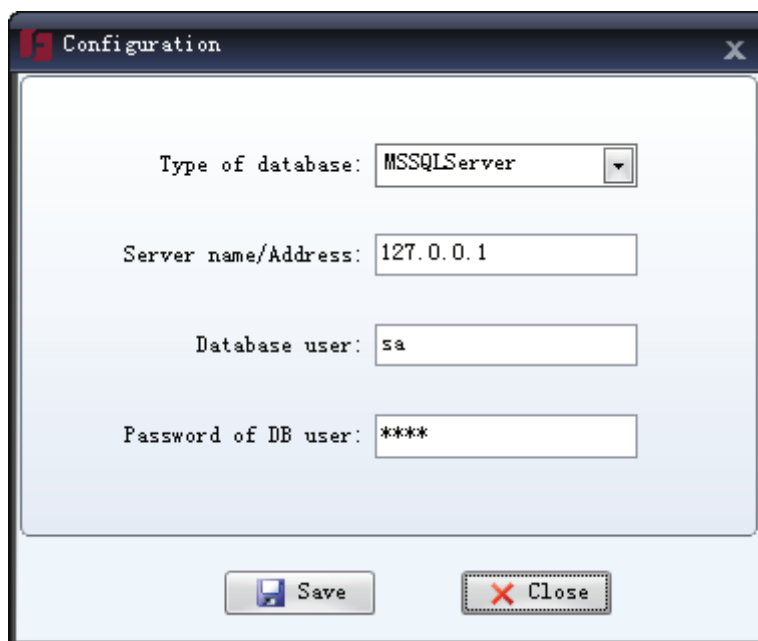


Fig. 2-2 Database Configuration



Fig. 2-3 Database Configuration Fail

The login window requires users to enter user name and password (Fig. 2-4)

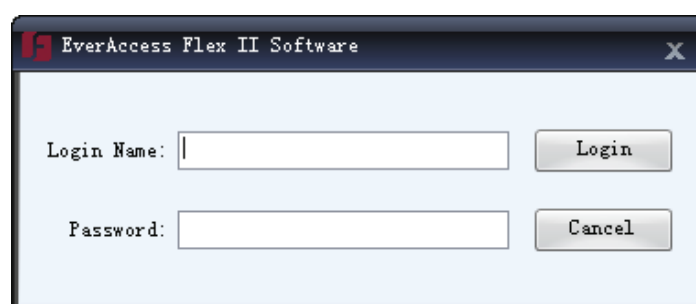


Fig. 2-4 Enter User Name and Password

The factory default login name is “admin” and password is “admin”.

Note: admin is a “Super administrator”. It is used for installation and restoration of the system. Admin can execute all the functions of the software; it cannot be modified or deleted. Users can only change the password for admin. Change the password after initial login and keep the password in a safe place. Create individual user IDs and passwords for day to day operation and maintenance of the system.

To change the password for admin: click “Basic management” → “User Setting” → “Edit”. Admin can add users and change users’ authority through “Basic management” → “User Setting” → “Add”. If all other users are deleted and the password for “admin” is lost, the Software cannot be used!!.

After entering the login name and password, click “OK” to open the Software, or click “Cancel” to exit. If the wrong login name and/or password are entered, an illegal login dialog box will pop up (Fig. 2-5).

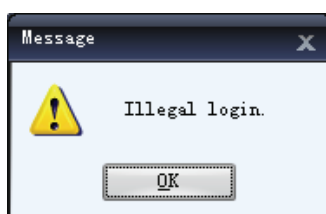


Fig. 2-5 Illegal login

2.3 Software Interface

2.3.1 Main Window

The Software is based on a Vista program interface style and supports customized window color schemes. The interface is user-friendly and easy to use. Users can customize the quick access toolbars at the top of the window. After login, the main window will be shown as in Fig. 2-6.

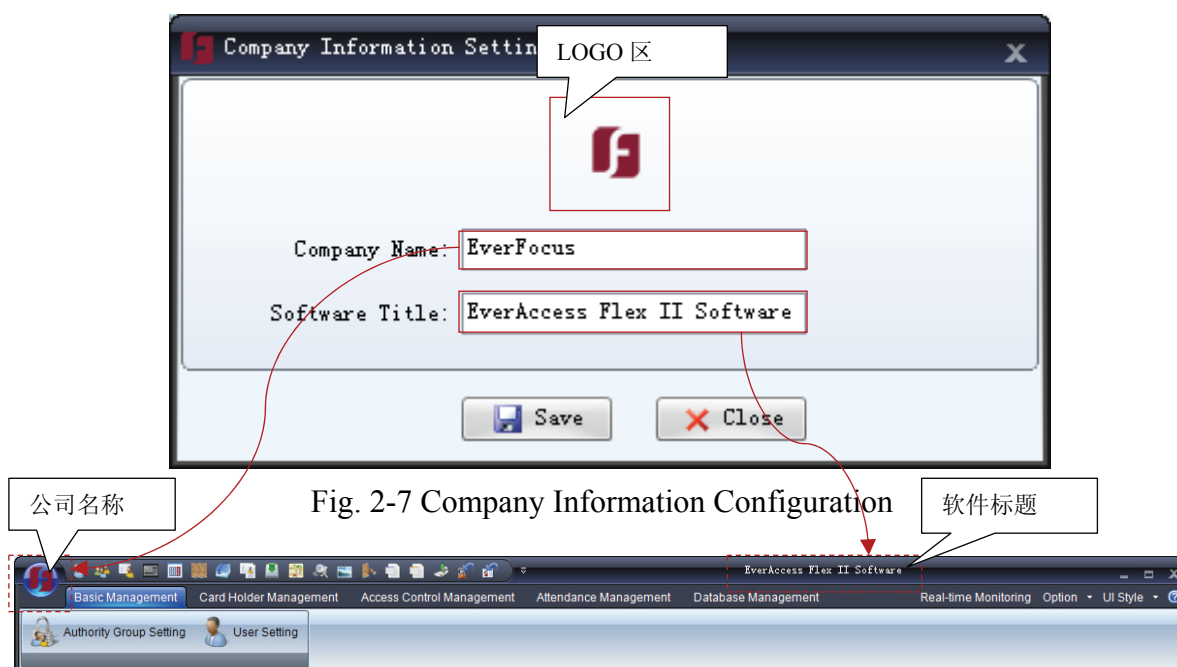


Fig. 2-6 Main Window

2.3.2 Start Menu

2.3.2.1 Company Information

The Software supports uploading a customized company logo and change the Software titles. Click the  icon on the upper left corner of the window and select “Company Information Setting” from the drop-down menu. A dialog box as in Fig 2-7 will be shown. Click on the logo and an upload dialog box will pop up. Select the picture file (the maximum supported size is 32x32 pixels) and click on the “Open” button to complete the upload. When the cursor is placed on top of the company logo located on the upper left corner, the content in the “company name” field will be shown. Content in “Software title” field is shown on the title bar of the Software.



2.3.2.2 Language Selection

Upon initial login, the the Software will automatically check the language used by the computer and set it as the language for the Software. To change the language setting, click “Start menu” → “language setting” and select the language. The new language selection will be in effect upon the next login. If the language used by the computer is not supported by the Software, English will be used.

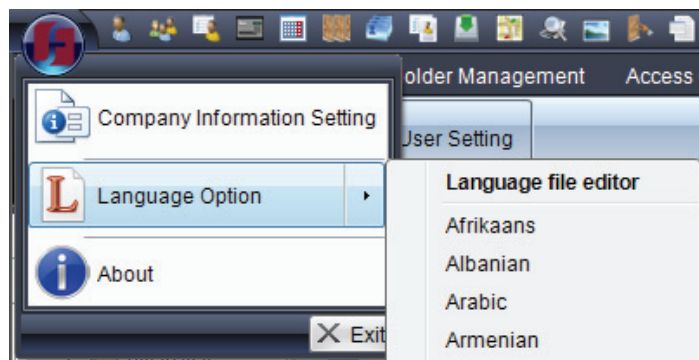


Fig. 2-8 Language Setting

The Software also provides an option for “Editing language”, by which users can edit the language file in the Software. Click “Language Setting” → “Edit language file” and a dialog box will pop up (Fig. 2-9).

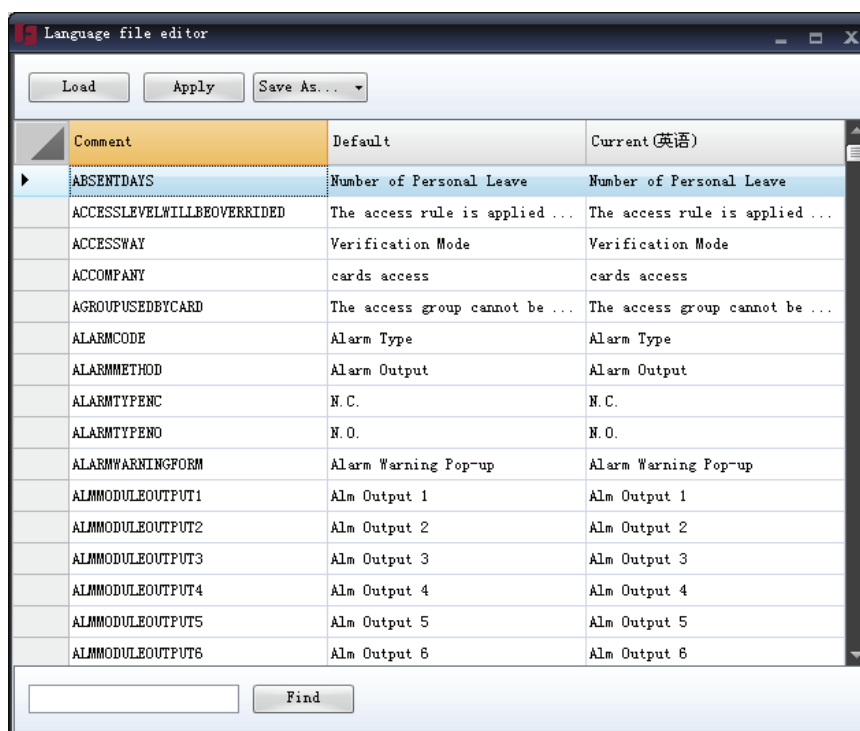
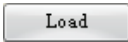
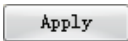


Fig. 2-9 Edit Language File

Load: to edit language package to use in the Software. Click the “Load”  button and select the language file with an extension of .DLL.

Apply: after editing the current file, click the “Apply”  button and a dialog box will pop up to confirm whether to overwrite the current language file, as in Fig. 2-10.

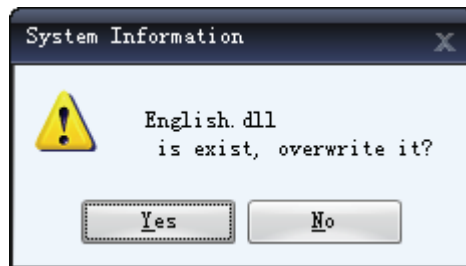
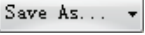


Fig. 2-10 Confirm overwrite of the language file

Save as: to generate another language file, edit each item in the current dialog box, click the button  on right of "Save as" and select the language from the drop-down menu. Click the "Save as" button  to save the language file with a new name. The selected language will be used upon the next login.

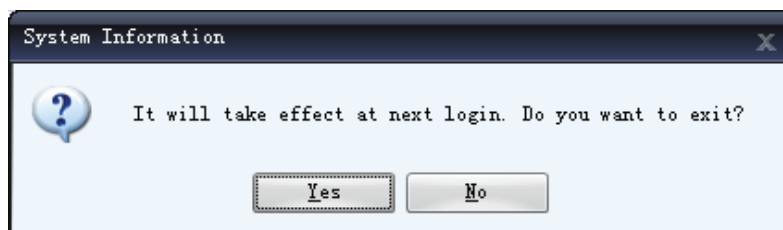


Fig. 2-11 New Language Selection is saved

Search: to search items by keywords. All three columns are included in searching field.

2.3.2.3 About (Software Information)

Click "Start menu" → "about" and a dialog box showing the Software name, version, copyright and EverFocus website etc, as Fig. 2-12, will be displayed.



Fig. 2-12 about the Software

2.3.3 Quick Access ToolBar

The Quick access toolbar contains a set of intuitive graphic buttons representing commonly used commands (Fig. 2-13). Though the most commonly used commands are included in the Quick access toolbar, users can also customize the toolbar by adding or deleting commands.

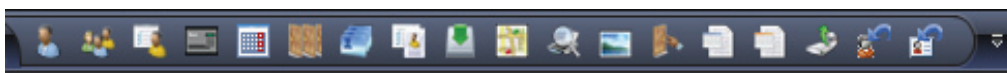


Fig. 1.13 Quick Access Toolbar

Click the button  at the end of the quick access toolbar. From the drop-down menu (as in Fig. 2-14), users can add, delete, self-define commands and hide menu items.

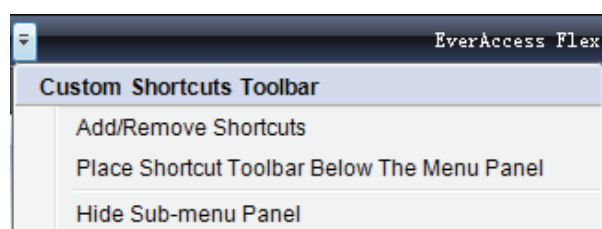


Fig. 2-14 Customize Quick Access Toolbar

2.3.3.1 Add/Delete Shortcuts

From the drop-down menu in Fig. 2-14, select “Add/delete shortcuts”. A selection dialog box will pop up (Fig. 2-15). Select commands from the main menu for each functional module on the left and add the shortcuts to the list on the right. Users can also delete unused shortcuts from the shortcut list.

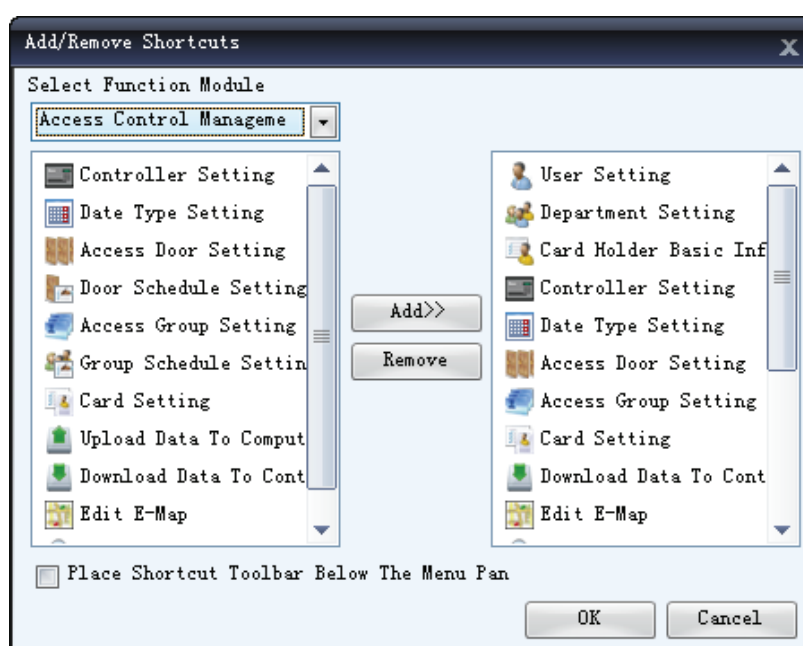


Fig. 2-15 Add/Delete Shortcuts

2.3.3.2 Move the Quick Access Toolbar to the bottom

From the drop-down menu in Fig. 2-14, select “Move the quick access toolbar to the bottom of the window” or check the box on the lower left corner of the “Add/delete shortcuts” window. The quick access toolbar will be moved from top of the window for the bottom (Fig. 2-16).

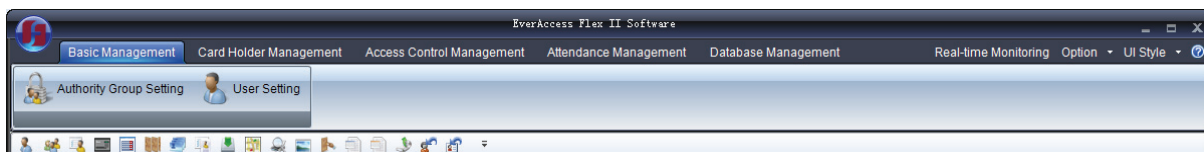


Fig. 2-16 Move the quick access toolbar to the bottom of the control Panel

2.3.3.3 Hide Submenu

From the drop-down menu in Fig. 2-14, select “Hide submenu” or double click any main menu, all submenus will be hided (Fig. 2-17).

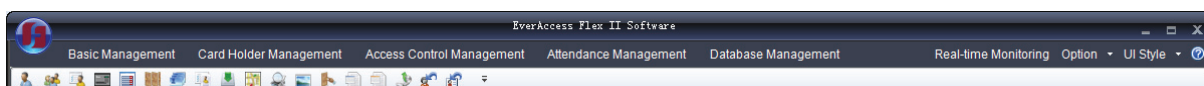


Fig. 2-17 Hide Submenus

2.3.4 Menu

The main window contains 5 main menus: basic management, cardholder management, access control management, attendance management and database management (Fig. 2-18). Clicking on any main menu item will show its submenu. Click any command in the submenu to perform the related task. Detailed descriptions about each command will be provided in related chapters.

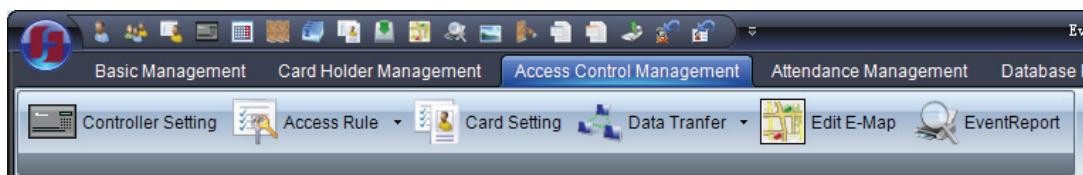


Fig. 2-18 Menu Bar

If the login user does not have authority to execute certain functions, a dialog box reporting “Insufficient authority to operate” will pop up, as Fig. 2-19.



Fig. 2-19 Insufficient Authority to operate

2.3.5 System Selection Bar

The “system selection bar” controls real-time monitoring, alarm warnings and user interface style. Click “real-time monitoring”, the interface changes to real-time monitoring of E-maps and event record. User can monitor the system status in real time.

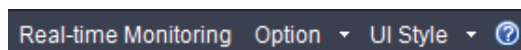


Fig. 2-20 System Selection Bar

2.3.5.1 System Selection

Users can choose whether to enable “real-time communication” and “alarm warning message” in the system selection (Fig. 2-21).

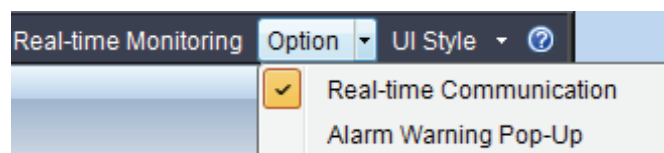


Fig. 2-21 System Selection

Real-time communication: when enabled (as in Fig. 2-21), the Software is in continuous communication with the controllers. The real time status of devices in the system will be shown on E-maps and all real time events will be shown in the “event record” at the bottom of the window.

Access Granted Access Denied Operation Record Alarm Record System Record System Log		
Date/Time	Controller Address	Event
09-06-25 14:36:48	0011	System menu entered
09-06-25 14:36:48	0011	System menu entered
09-06-25 14:36:48	0011	System menu entered
09-06-25 14:36:48	0011	System menu entered
09-06-25 14:36:48	0011	System menu entered
09-06-25 14:36:48	0011	System menu entered
09-06-25 14:36:48	0011	System menu entered
09-06-25 14:36:48	0011	System menu entered
09-06-25 14:36:48	0011	System menu entered
09-06-25 14:36:48	0011	System menu entered

Fig. 2-22 System Record

Alarm Warning Message: when enabled (as in Fig. 2-21), an “Alarm warning” dialog box will pop up for any alarm input in the system (Fig. 2-23). A warning sound is also generated (the

default setting is speaker enabled). Users can choose to disable future “alarm warning message” and “alarm sound warning” in the dialog box.

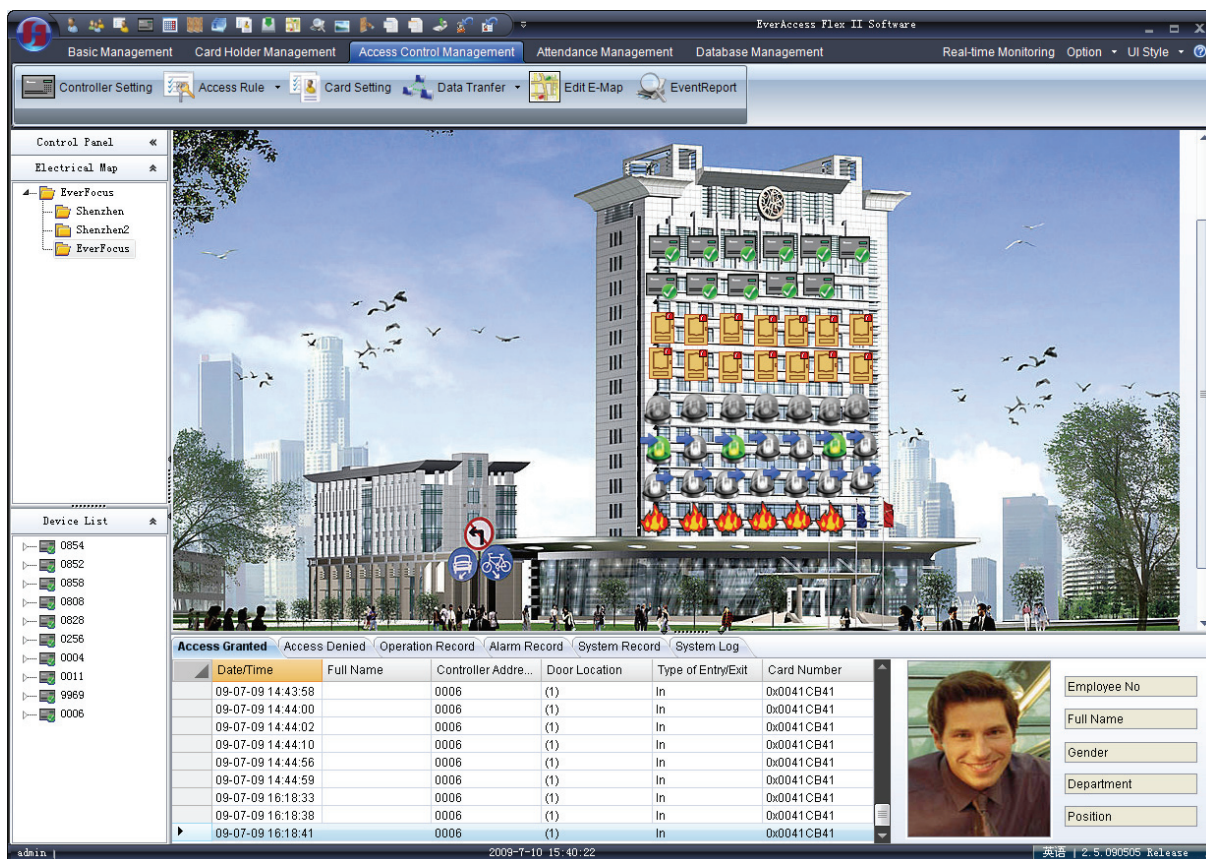


Fig. 2-23 Alarm Warning Message Display

2.3.5.2 Interface Style

The Software provides for user-friendly customized user interface style setting (Fig. 2-24). The default interface style is Vista Classic. The interface color scheme can be changed to users' preference. A few customized interface styles are shown below.

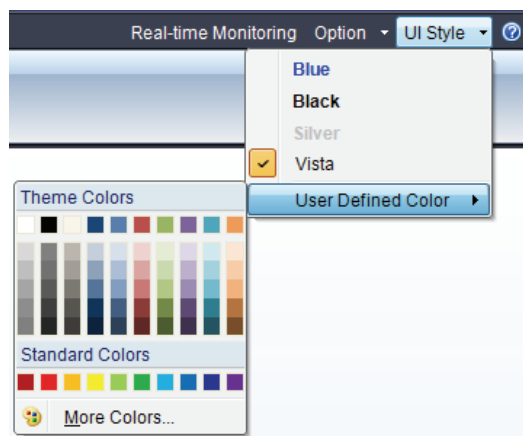
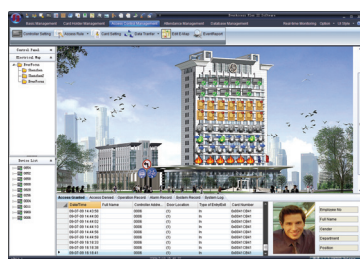
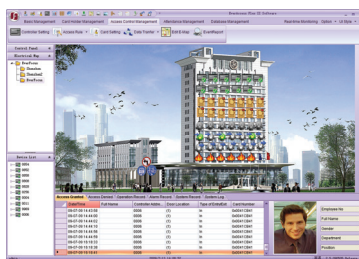


Fig. 2-24 Interface Style

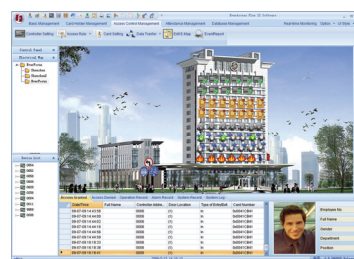
Some customized interface styles as follow:



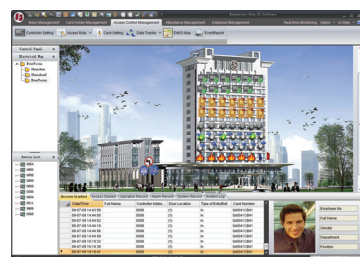
Vista (Default)



Purple



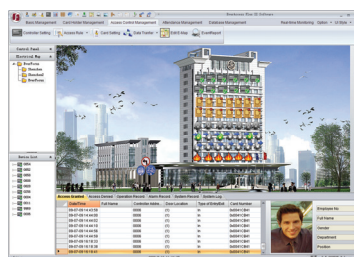
Blue



Black



Green



Silver

2.3.6 Control Panel

If a user clicks the “Control Panel” button  underneath the menu, “E-map list” and “resources list” on the left of the window will be hidden (Fig. 2-25). Click the “Control panel” button area or double click the hidden bar, the hidden lists will be displayed.



Fig. 2-25 List Hidden at Left Side

2.3.6.1 Electronic Map (E-Map) List

The E-map list contains the E-map structure of all E-maps in the system (Fig. 2-26). Refer to Electronic Map (E-Map) Management to add, delete and edit E-maps.

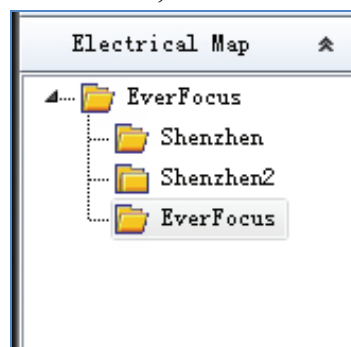


Fig. 2-26 E-Map List

2.3.6.2 Resources List

The Resources list contains all valid controllers in the system (Fig. 2-27). Valid controllers refer to controllers that are found by the Software. Refer to Section 5 Controller Management to add, delete and edit controllers.

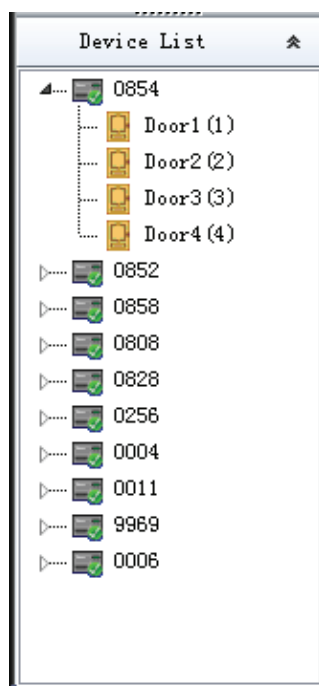


Fig. 2-27 Resources List

2.3.7 Real-time Monitoring

This function shows the real-time status of the system on the E-maps. Click “E-map list” on the left to display E-maps and view it’s the graphical status display. Refer to Section 9 Electronic Map (E-Map) Management to add, delete and edit E-maps.

2.3.8 System Event Record

This area shows all event records in the system, including granted access records, denied access records, operation records, alarm records, system records and system log entries. On top of the panel is a button to hide the panel. When the cursor is placed on top of the bar, “click to hide panel” is shown (Fig. 2-28). Click the bar to hide the event record panel and click it again to show the event record panel when needed. Right click the first column of the list to select whether to show line numbers. Click the first title line, and the events will be sorted in ascending or descending order. The operation is similar for other parts in the Software and will not be described again.

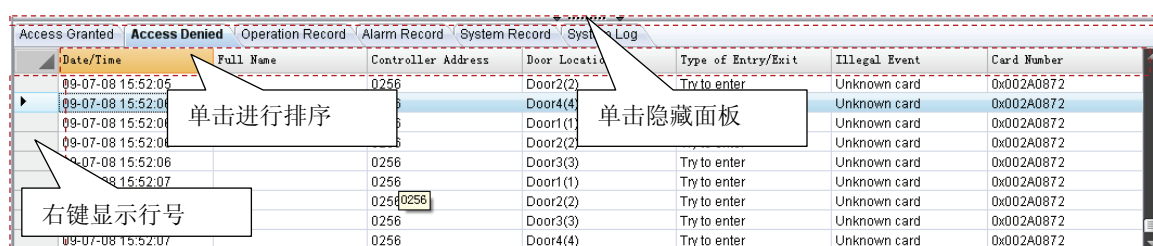


Fig. 2-28 Hide panel

2.3.8.1 Granted Access Record

Granted access records include regular card read records, PIN door open records and APB (Anti-Pass Back) doors opened. Refer to Section 14.1 Area Anti-Passback for details.

The content of granted access records includes the event time, cardholder name, controller address, door No., In/Out type and card number. Select an event record to view details on the right panel.

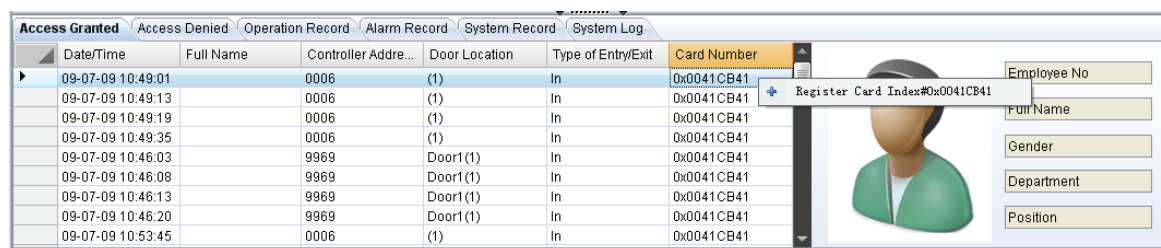


Fig. 2-29 Granted Access Record

Access granted using cards that have been enrolled in controllers, but not in the Software, will be shown in the event record list. Users can easily add the card to the Software through the right click menu as described in “Quick Add a Card”. In addition, users can employ this method to check whether a card is registered in the Software.

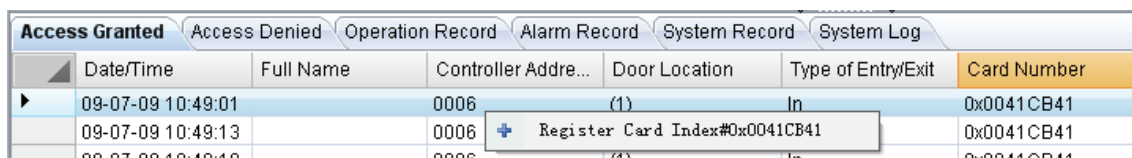


Fig. 2-30 Quick Add a Card

If an operator chooses registering the card, the card is then added to the Software. The default access group is “Full Granted” and the card setting is downloaded to all valid controllers in the system.

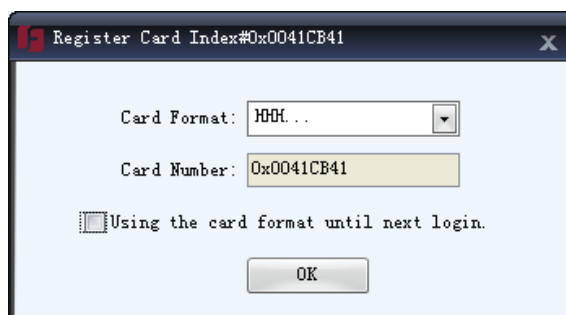


Fig. 2-31 Select Card Format

Note: There are two other methods to add cards to the system (See Sections 7.2 Import Card Information and 8.1 Upload Data to Computer) for similar methods. The option of “Use the same card format setting until next login” is available in all three methods.

2.3.8.2 Denied Access Record

Denied access records include unknown card, expired card, invalid card, card PIN fail, PIN fail more than allowed attempts, cancel waiting, invalid door, invalid time, card APB fail, interlock, door left open (propped door), unregistered fingerprint, attempting access by unregistered fingerprint and no fingerprint information for the cardholder. Refer to Section 5.5.6 Alarm output Setting for details.

The content of a denied access record includes event time, cardholder name, controller address, door No., In/Out type, event type and card number.

Denied access resulting from cards that have been enrolled in controllers, but not in the Software, will be shown in the event record list. Users can add the card to the Software from the right click menu as described in “QuickAdd a Card”. The process is similar to that for the “Granted Access Record” described above.

Access Granted		Access Denied	Operation Record	Alarm Record	System Record	System Log	
	Date/Time	Full Name	Controller Address	Door Location	Type of Entry/Exit	Illegal Event	Card Number
▶	09-07-08 15:52:05		0256	Door2(2)	Try to enter	Unknown card	0x002A0872
	09-07-08 15:52:06		0256	Door4(4)	Try to enter	Unknown card	0x002A0872
	09-07-08 15:52:06		0256	Door1(1)	Try to enter	Unknown card	0x002A0872
	09-07-08 15:52:06		0256	Door2(2)	Try to enter	Unknown card	0x002A0872
	09-07-08 15:52:06		0256	Door3(3)	Try to enter	Unknown card	0x002A0872
	09-07-08 15:52:07		0256	Door1(1)	Try to enter	Unknown card	0x002A0872
	09-07-08 15:52:07		0256	Door2(2)	Try to enter	Unknown card	0x002A0872
	09-07-08 15:52:07		0256	Door3(3)	Try to enter	Unknown card	0x002A0872
	09-07-08 15:52:07		0256	Door4(4)	Try to enter	Unknown card	0x002A0872

Fig. 2-32 Denied Access Records

2.3.8.3 Operation Records

Operation records include remote operation of controllers via the Software, arm/disarm controllers, and reset alarm, door open by request-to-exit button and interlock. Refer to Section 5.5.6 Alarm output Setting for details.

The content of an operation record includes event time, operator, controller address, door number and event type.

Access Granted					Access Denied		Operation Record		Alarm Record		System Record		System Log	
Date/Time		Operator			Controller Address			Door Location			Event			
09-07-09 14:42:46					0006						Disarm from controller			
09-07-09 14:42:48					0006						Arm from controller			

Fig. 2-33 Operation Records

2.3.8.4 Alarm Records

Alarm records include armed zone alarm, fire alarm, system PIN fail, arm PIN fail, tamper alarm, remote alarm, door opened without prior access nor request to exit (forced door), door left open (propped door), door held open and reader communication lost. Refer to Section 5.5.6 Alarm output Setting for details.

The content of an alarm record includes event time, controller address, arm zone number and event type.

Access Granted Access Denied Operation Record Alarm Record System Record System Log			
Date/Time	Controller Address	Arm No.	Event
09-07-09 17:54:21	0004		Reader#1 lost
09-07-09 17:54:21	0004		Reader#2 lost
09-07-09 17:54:25	0004		Reader#1 lost
09-07-09 17:54:25	0004		Reader#2 lost
09-07-09 17:54:28	0004		Reader#1 lost
09-07-09 17:54:28	0004		Reader#2 lost
09-07-09 17:54:31	0004		Reader#2 lost
09-07-09 17:54:31	0004		Reader#1 lost
09-07-09 17:54:34	0004		Reader#1 lost

Fig. 2-34 Alarm Record

2.3.8.5 System Records

System records are for events related to controller setting, including access to the controller menu, add/delete/edit cards in controllers, controller online/offline, controller power-off and controller communication lost etc.

The content of a system record includes event time, controller address and event.

Access Granted Access Denied Operation Record Alarm Record System Record System Log		
Date/Time	Controller Address	Event
09-07-09 22:03:36	0852	加入读卡器#2
09-07-09 22:27:38	0852	加入读卡器#2
09-07-09 22:29:25	0852	加入读卡器#2
09-07-09 23:44:25	0852	加入读卡器#2
09-07-10 00:47:04	0852	加入读卡器#2
09-07-10 02:04:48	0852	加入读卡器#2
09-07-10 15:08:57	0854	进入控制器菜单
09-07-10 15:09:03	0852	进入控制器菜单
09-07-10 15:09:13	0858	System menu entered

Fig. 2-35 System Record

2.3.8.6 System Log

System log refers to the login and logout records for the Software. The content of the system log includes login/logout time, login name and event type.

Access Granted Access Denied Operation Record Alarm Record System Record System Log		
Log DateTime	Login Name	Log Type
09-07-13 11:22:16	admin	Login System
09-07-13 11:22:52	admin	Logout System
09-07-13 11:23:32	admin	Login System
09-07-13 11:32:37	admin	Logout System
09-07-13 11:34:00	view	Login System
09-07-13 11:34:43	view	Logout System
09-07-13 11:34:54	admin	Login System
09-07-13 14:38:20	admin	Logout System
09-07-13 15:05:00	admin	Login System

Fig. 2-36 System Log

2.3.9 System Status

System status includes login name, current time, and displayed language and Software version information.



Fig. 2-37 System Status

Chapter

3

3 Basic Management

This chapter introduces the concept of managing users and authority groups in detail.

Authority Group Setting: adding, deleting and editing authority groups in the software. There is no limit to the number of authority groups and users can define authority groups based on needs.

User Setting: adding, deleting and editing users who operate the software. The software default user “admin” belongs to super authority group, which can execute all the functions of the software. Users can only change the password for a super user.

3.1 Configure Users and Authorities

A **User** of the Software is a person who operates the software at any user interface. Each user is defined by four properties: name, login name, password and the authority group to which the user belongs.

The “name” should be the real name of the user. The “login name” is the identity that users need to type into the login dialog to enter the system. The “password” is the password that users need to provide when they login the system. The “authority group” is discussed in details below.

Note: users are different from cardholders. Cardholders are the people who enter or exit through points monitored by the physical access control system, such as employees of the company. But users operate the software to monitor or configure the physical access control system.

The authority group defines the user’s access level to control the operation of the Software. Different authority groups have different operating privileges in the Software.

Click the menu bar “Basic Management”➔ “Authority Group Setting” to enter the authority group setting window. Please refer to Section 3.2 Authority Group Setting for details. The Software will automatically initialize authority groups upon first entering “Authority Group”

The Software offers four authority group types: Super, System, Operate and View. There is no limit to the number of users in each group.

Super: Users in the super group can execute all the functions of the software, including basic management, cardholder management, access control management, attendance management and database management etc.

System: Users in the system group have access to all functions **except** basic management.

Operate: Users in the operate group have access to all functions **except** basic management and database management.

View: Users in the view group can view the event list and monitor the system in real-time.

The following table gives the detailed authority list for each group. “√” in the cells indicates the function is available to this group.

Functionality		Super	System	Operate	View
Basic Management	Authority group Setting	√			
	User Setting	√			
Cardholder Management	Department Setting	√	√		
	Cardholder Information	√	√		
Access Control Management	Controller Setting	√	√	√	
	Date Setting	√	√	√	
	Door Setting	√	√	√	
	Door Schedule Setting	√	√	√	
	Access group Setting	√	√	√	
	Access group Schedule Setting	√	√	√	
	Card Setting	√	√	√	
	Upload Data	√	√	√	
	Download Data	√	√	√	
	Edit E-Map	√	√	√	
	Event Report	√	√	√	
Attendance Management	Holiday Setting	√	√	√	
	No-Access-Attendance Enrollment	√	√	√	
	Overtime Enrollment	√	√	√	
	Time-Off Enrollment	√	√	√	
	Attendance Statistics	√	√	√	
	Attendance Reports	√	√	√	
Database Management	Create Database	√	√		
	Backup Database	√	√		
	Restore Database	√	√		
	Import Cardholder Information	√	√		

	Import Information Card	✓	✓		
	Purge out-of-date data	✓	✓		

Table 3.1 Functionality Map for Authority Groups

Except for Super, the other 3 authority groups can be modified or deleted.

3.2 Authority Group Setting

To access “Authority Group Setting”, right click to open the operation box (Fig.3.1). The commands in the operation box are the same as those in the “function editing area”. All other operation windows have the same format, and thus will not be described again.

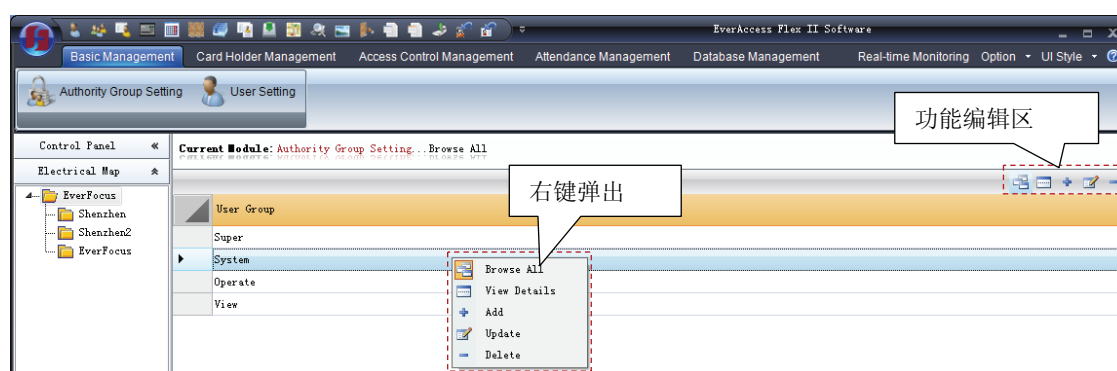


Fig. 3-1 Authority Group Setting

3.2.1 Add an Authority Group

Click the “Add” button  in the “function editing area” (Fig. 3-5) to open the window for add an authority group (Fig.3.6). Fill in the name of the new authority group in the “Authority Group Name” (Fig.3.2) and choose the functions that the new group will have access to. When finished, click the “Save” button and a dialog box indicating “Operation succeeded” will pop up (Fig. 3-3).

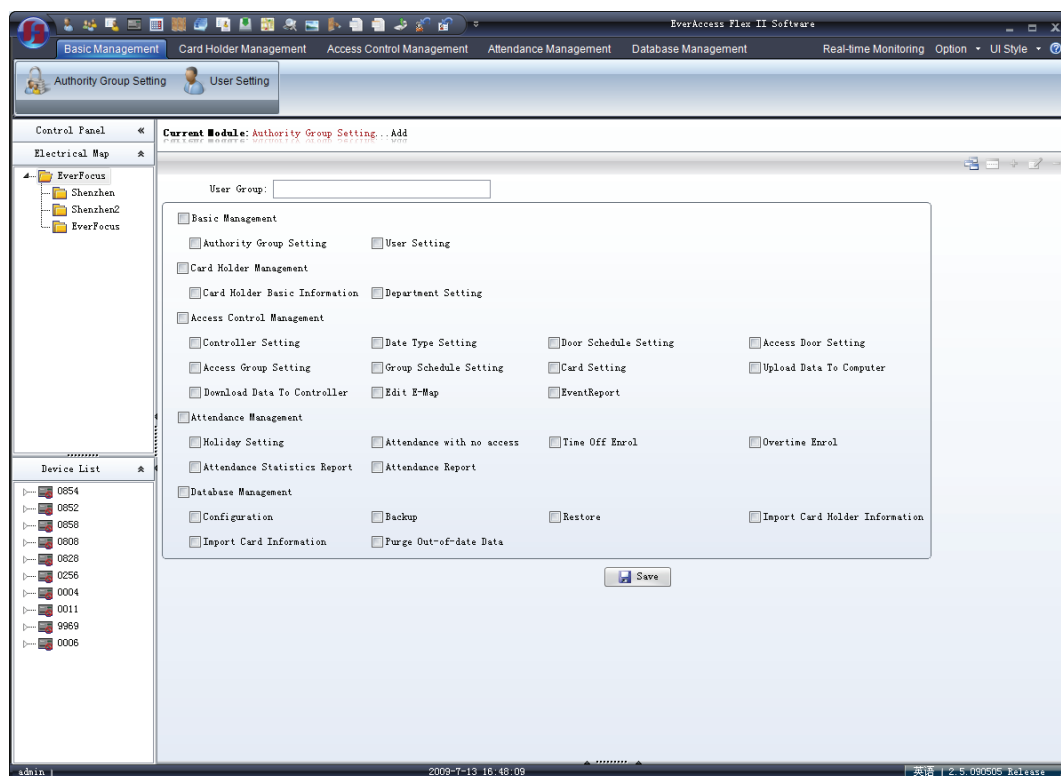


Fig. 3-2 Add An Authority Group

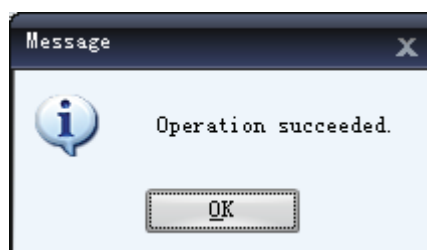


Fig. 3-3 Operation succeeded

3.2.2 Edit an Authority Group

Click the “Edit” button  in the “function editing area” (Fig. 3-5) to open the window for editing authority groups (Fig.3-4). A user can edit the name as well as the functions that an authority group has access to. When finished, click “Save” button and a dialog box indicating “operation succeeded” will pop up. Users can choose other authority groups to edit by using the navigation buttons “BW” and “FW” at the bottom of the window.

Note: Make sure to save the changes before using any of the navigation buttons. Otherwise, the changes will not be saved.

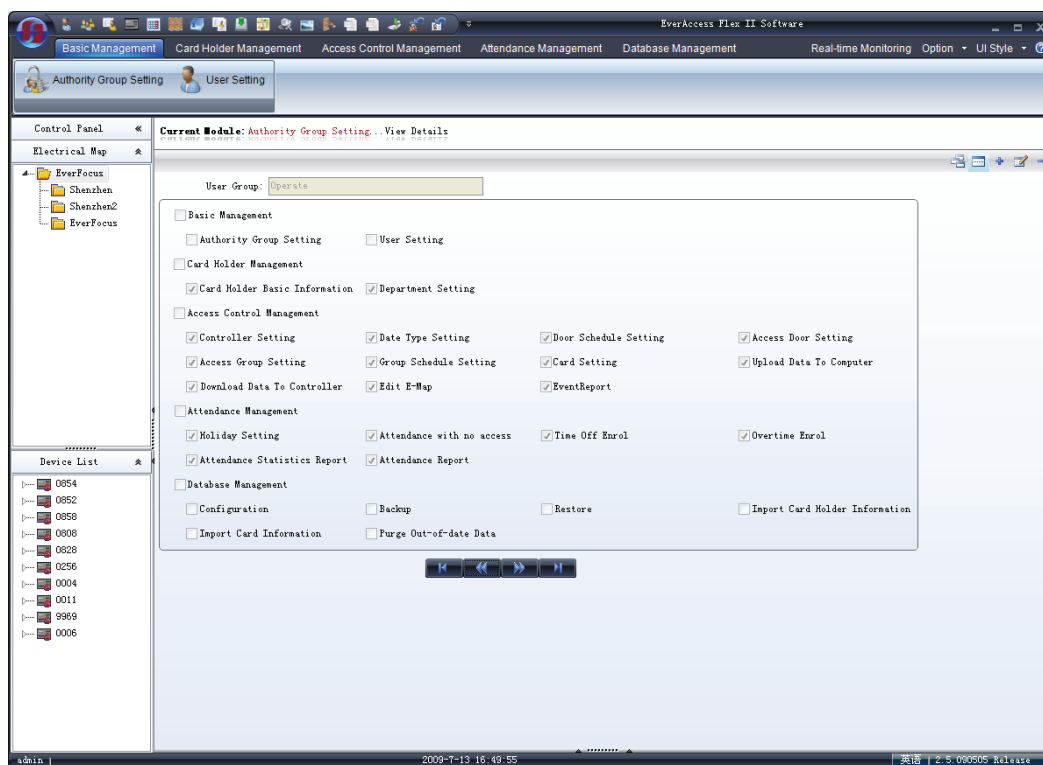


Fig. 3-4 Edit an Authority Group

3.2.3 View Authority Groups

3.2.3.1 View All

Click “Basic Management” ➔ “Authority Group Setting” to view all authority group settings (Fig. 3-5).

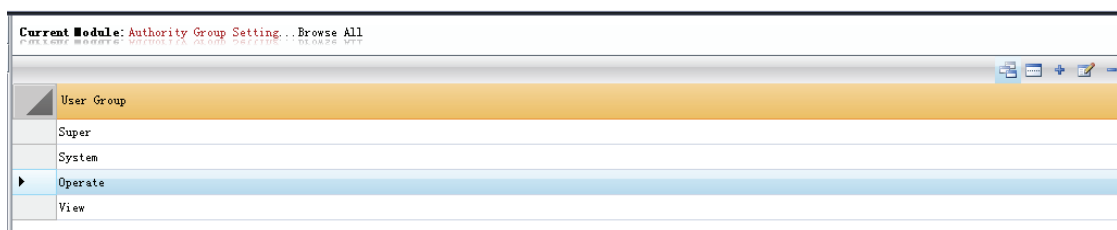


Fig. 3-5 View All Authority Groups

3.2.3.2 View Details

Click the “View Details” button  in the “function editing area” (Fig. 3-5) to open the window for viewing details of an authority group (Fig. 3-6). Users can choose to view details of a different authority group by using the navigation buttons “BW” and “FW” at the bottom of the window.

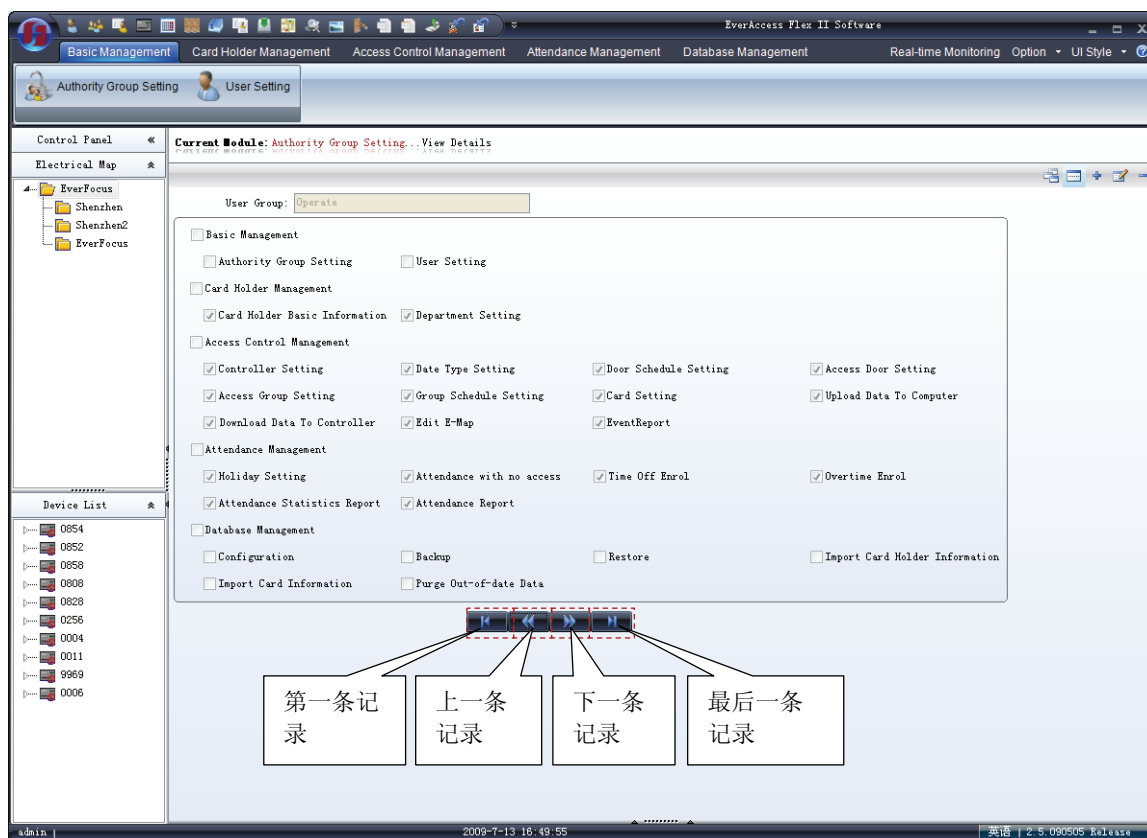


Fig. 3-6 View Details of an authority Group

3.2.4 Delete an Authority Group

Select the authority group to be deleted in the “View All” window for Authority Groups (Fig. 3-5), then click the “Delete” button in the “function editing area”. A dialog box will be shown to prompt users to confirm the deletion (Fig. 3-7). Click “Yes” to delete the authority group and another dialog box confirming “Operation succeeded” will pop up.

Note: The authority group that is currently in use cannot be deleted.

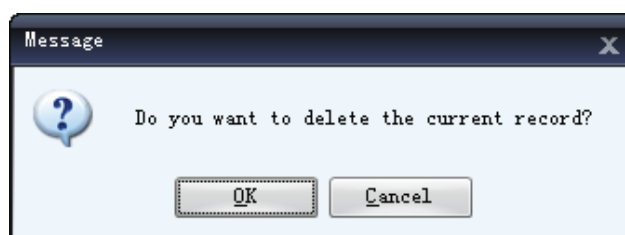


Fig. 3-6 Delete the selected Authority Group

3.3 User Setting

User Setting is used to add, edit, delete users and assign authority groups for users. The *User* here refers to the person who can login and operate the Software. It is different from cardholders. User properties consist of user name, login name, password and the authority

group to which the user belongs. The software default user “admin” belongs to the super authority group and cannot be deleted.

Click “Basic Management” → “User Setting” to open the window for setting users (Fig. 3-8).

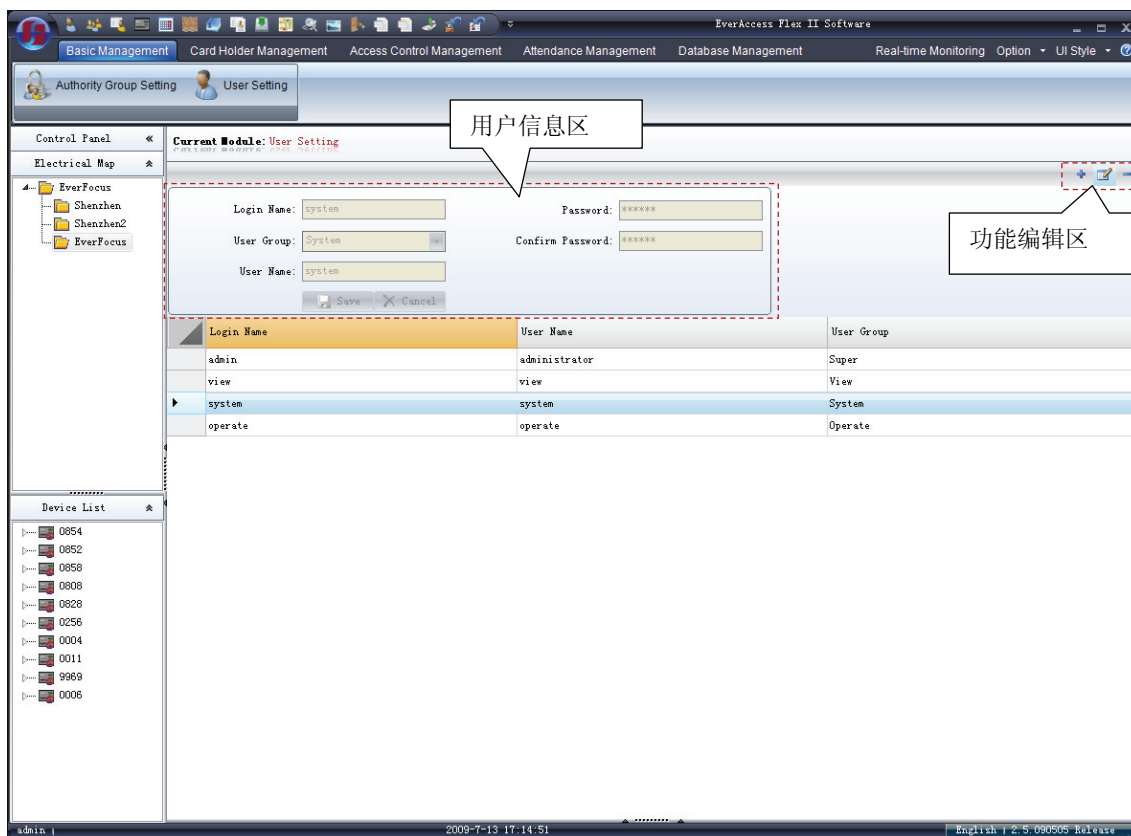


Fig. 3-8 User Setting

3.3.1 Add a User

Click the “Add” button  in the “function editing area” (Fig. 3-8) to open the window for adding users (Fig. 3-9). In the user property area, fill in the login name, password, the authority group and user name, then click the “Save” button and a dialog box confirming “operation succeeded” will pop up.

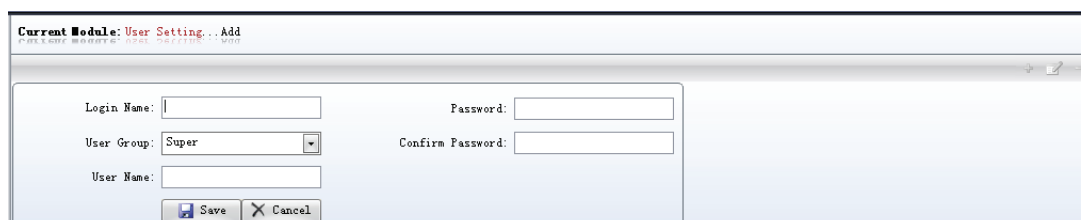


Fig. 3-9 Add a User

Definitions:

Login name: login name is the identity that users need to type into the login dialog to enter the system. It can be numbers, letters, spaces and any combination of the above. The maximum length of a login name is 20 characters. The login name is **case-insensitive**. It cannot be the same as login names that already exist in the system and cannot be left blank. If user enters a login name that already exists, the system will report “login name already exists”.

Password: a password can be numbers, letters, spaces and any combination of the above. The maximum length is 20 characters. **Password is case-sensitive. It cannot be blank.**

Confirm Password: The same password has to be entered here. If the two passwords are different, the system will prompt “Passwords do not match”.

Authority Group Name: The authority group to which the user belongs. Administrators can assign any authority group for a new user. A Super user can execute all the functions of the Software.

User Name: The user name should be the actual name of the user. This item is for system management and cannot be left empty.

3.3.2 Edit a User

Select the user to be edited in the “User Setting” window (Fig. 3-8) and click the “Edit” button  in the “function editing area” (Fig. 3-9) to open the window for editing a user (Fig.3-10). The login name, password, authority group name and user name can all be modified. When finished, click “Save” button and a dialog box reporting “operation succeeded” will pop up. Otherwise, click “Cancel” to return to “User Setting” window.

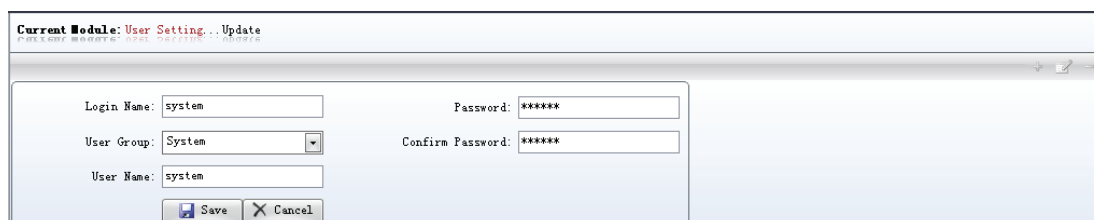


Fig. 3-10 Edit a User

3.3.3 Delete a User

Select the user to be deleted in the “User Setting” window (Fig. 3-8), then click the “Delete” button  in the “function editing area”. A dialog box will be shown to prompt users to confirm the deletion. Click “Yes” to delete the user and another dialog box confirming “Operation succeeded” will pop up. Otherwise, click “Cancel” to exit.

Note: The default user “admin” cannot be deleted.

Chapter 4

4 Cardholder Management

4.1 Department Setting

Department setting has no effects on the operation of the system. However, to use functions such as search and attendance management etc., it is recommended to create departments as they exist in real situations, and assign cardholders to their department accordingly.

Click “Cardholder Management” ➔ “Department Setting” to open the window for setting departments (Fig. 4-1).

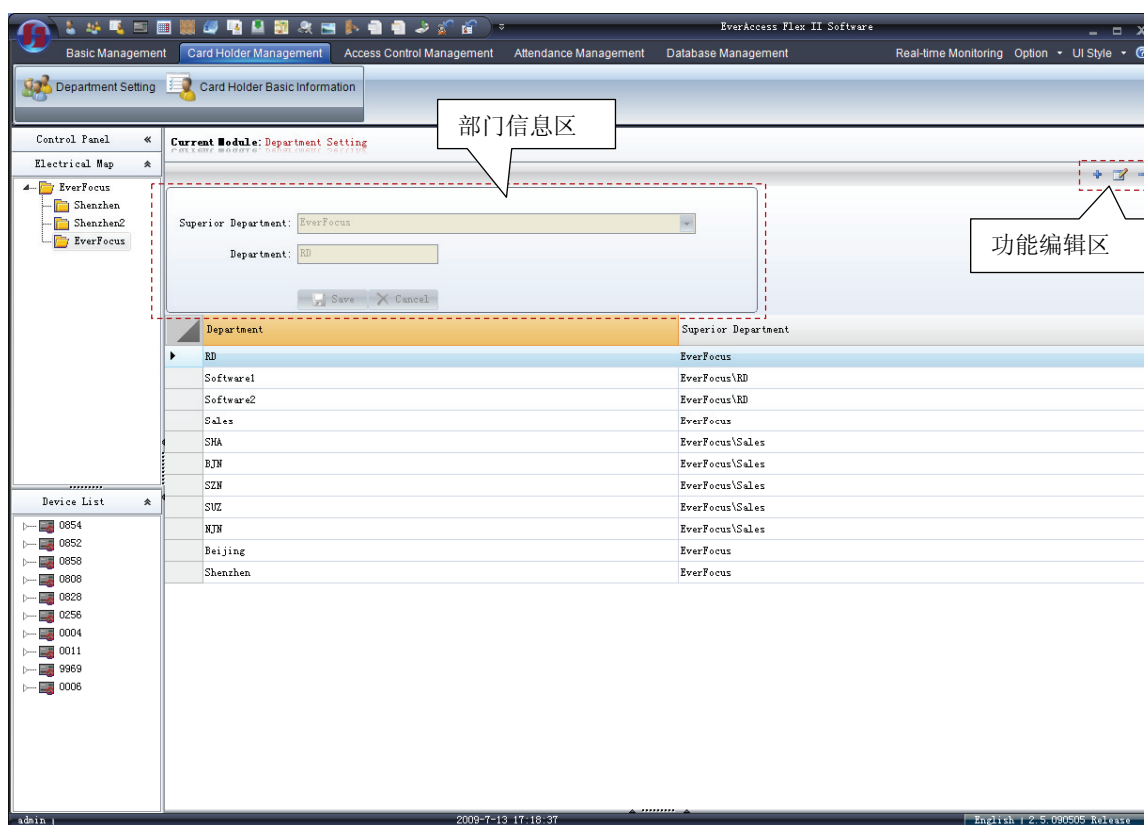


Fig. 4-1 Department Setting

4.1.1 Add a Department

Departments in the Software can be structured into three levels (not including the company level). The highest level is the company. The first time a user adds a department, the system will prompt whether to change the company information.

Click the “Add” button  in the “function editing area” to open the window for adding a department (Fig. 4-2). Fill in the name of the “parent department” and the name of the newly added department in the related field. When finished, click “Save” button and a dialog box confirming “operation succeeded” will pop up.

Note: Subsidiary departments under the same parent department cannot have the same name. Departments under different parent department can have same name.

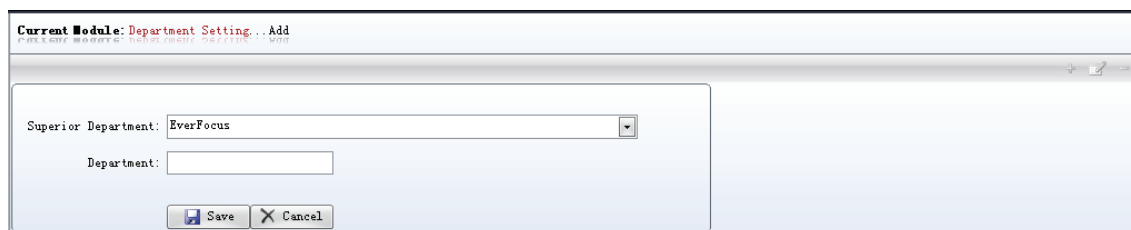


Fig. 4-2 Add a Department

4.1.2 Edit a Department

Select the department to be edited in the “Department Setting” window (Fig. 4-1) and click the “Edit” button  in the “function editing area” to open the window for editing a department (Fig.4-3). Both the name of the department and the parent department can be modified. When finished, click the “Save” button and a dialog box reporting “operation succeeded” will pop up. Otherwise, click “Cancel” to return to “Department Setting” window.

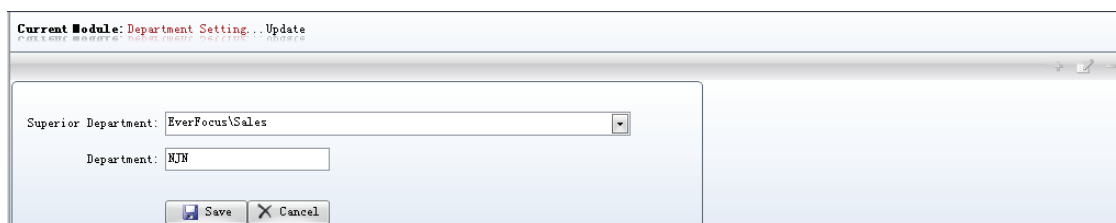


Fig. 4-3 Edit a Department

Note: A Department cannot be its own child department; a department cannot be edited if it contains child departments.

4.1.3 Delete a Department

Select the department to be deleted in the “Department Setting” window (Fig. 4-1), then click the “Delete”  button in the “function editing area”. A dialog box will be shown to prompt users to confirm the deletion. Click “Yes” to delete the department and another dialog box reporting “Operation succeeded” will pop up. Otherwise, click “Cancel” to exit.

Note: A department that contains child departments or cardholders cannot be deleted. The system will prompt “Contains child departments” or “Contains cardholders” respectively.

4.2 Cardholder Setting

This Section covers the concepts and management of cardholders. Click “Cardholder Management” → “Cardholder Setting” to open the window for cardholder setting (Fig. 4-4).



Fig. 4-4 Cardholders' Profile

Function editing area: To view all, view details, add, edit and delete cardholders.

Search toolbar: To search cardholders using search criteria and keywords. It also provides options of advanced search, refreshing the view, exporting and printing of cardholders. As all other search functions in the Software, the simple search function is based on *exact* match. Advanced search is used for more complicated search tasks and will be described in detail below.

Browsing toolbar: To view cardholder information using the navigation buttons “First Page”, “Backward”, “Forward” and “Last Page”. The system default setting is to display 15 cardholders per page.

Right-click menu: The system provides a right-click menu for quick editing options. Right click on the item to be edited, and a menu that contains the same commands as those in the “function editing area” will pop up.

Cardholders are the people who enter or exit from the physical access control system. Each cardholder will be assigned at least one card and will be registered in the system. Click

“Cardholder Management” ➔ “Cardholder Setting” to open the window for cardholder setting (Fig. 4-4).

Note: The access rights of a card are determined by the access group to which it belongs. It is recommended to configure access groups before assigning cards to cardholders. Click “Access Control Management” ➔ “Access Rule” ➔ “Access Group Setting” to open the window for access group setting (Refer to Section 6.4 Access Group Setting)

4.2.1 Add a Cardholder

Click the “Add” button  in the “function editing area” (Fig. 4-4) to open the window for adding a cardholder (Fig. 4-5). Cardholder information includes employee number, name, department, gender, position and employment date etc.

The Software provides an window to quickly assign cards to a cardholder. This function includes assigning one card or multiple cards to a cardholder, setting card properties and selecting access groups etc. When finished, click the “Save” button.

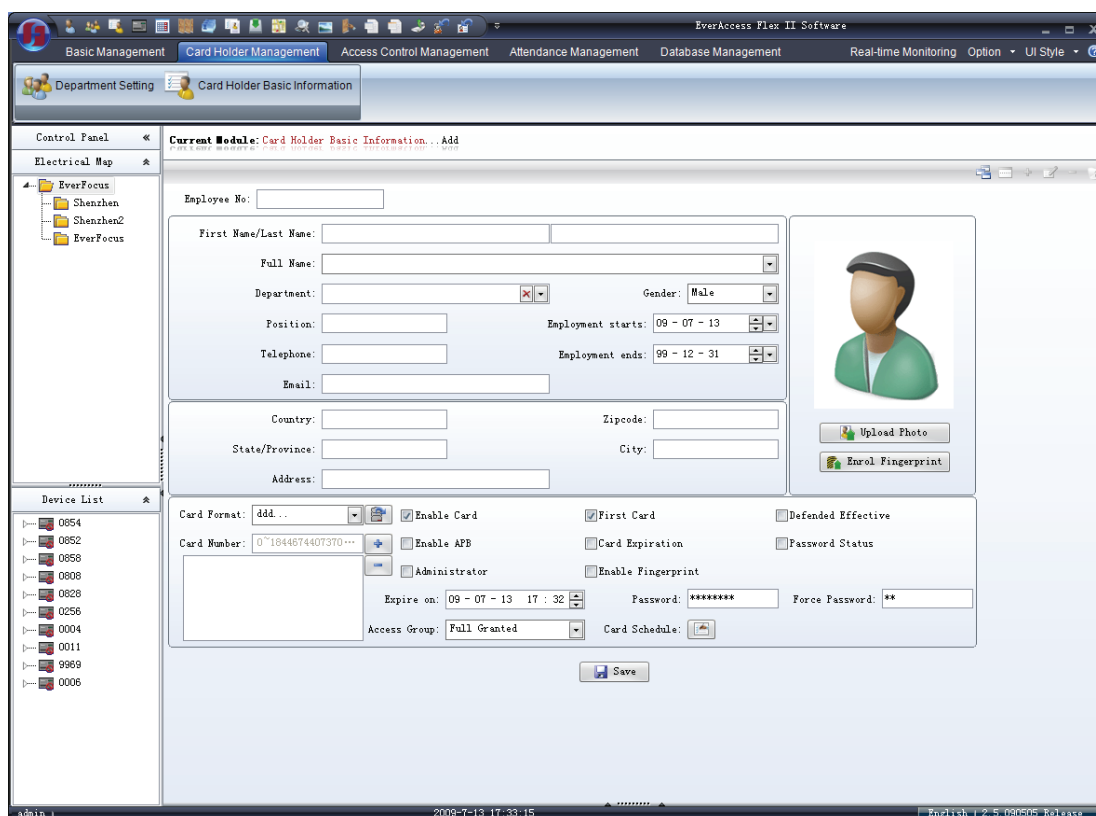


Fig. 4-5 Add a Cardholder

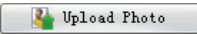
4.2.1.1 Cardholder Information

An employee number can be any printable character. The employee number is a unique index number, and so MUST BE UNIQUE for each cardholder in the system. When adding or

editing cardholder information, if the employee number is the same as an employee number that already exists in the system, the system will prompt “Employee number already exists”.

Employee number and name must be entered. The other properties are optional. It is recommended to enter all properties to facilitate searching.

4.2.1.2 Upload Cardholders’ Photo

Click “Upload Photo” , and a photo selection dialog box will pop up (Fig. 4-6). Choose the photo file (supporting formats: BMP, JPG, GIF, ICO, PNG) and click “Open” to upload the photo to the cardholder’s profile.

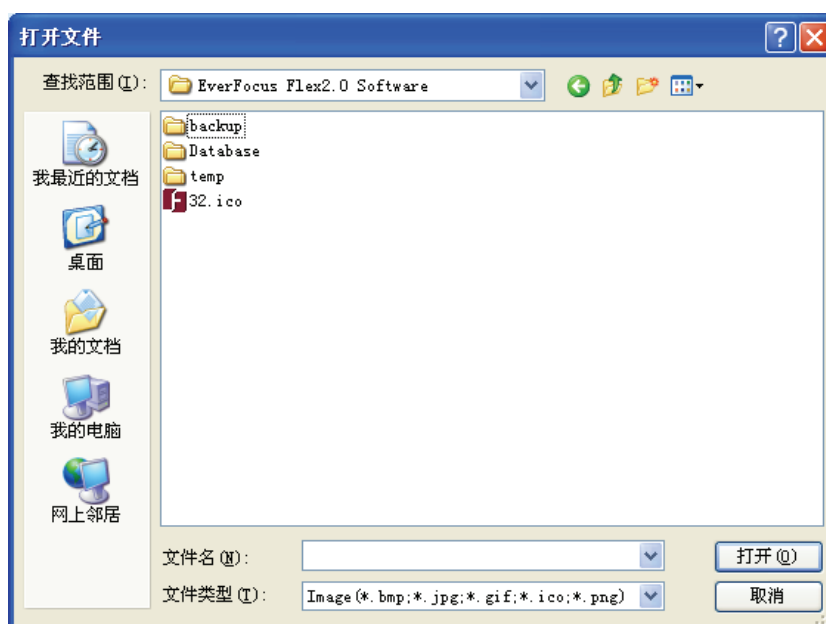


Fig. 4-6 Upload a Cardholder’s Photo

4.2.1.3 Quick Add Cards

The “Quick Add Cards Area” is for quickly assigning cards to the cardholder when adding a new cardholder. Adding cards can also be performed at “Access Control Management” → “Card Setting” (Refer to Section 7. Card Setting).

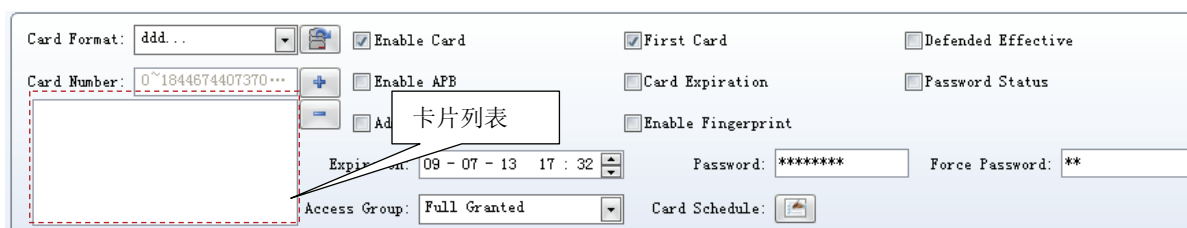


Fig. 4-7 Quick Add Cards

This function may be used to assign one card or multiple cards to the cardholder. The card number can be entered manually (the card number digits or symbols are typically printed on

the card) or by swiping the card through a desktop card reader (such as ERS-871 desktop reader or ERU series USB desktop reader). Please refer to hardware manuals for details.

Steps to use ERS-871 desktop card reader:

- a) Install drivers for ERS-871 desktop reader
- b) Connect ERS-871 desktop card reader to the computer
- c) Press the icon for desktop card reader , the following dialog box will pop up (Fig. 4-8).

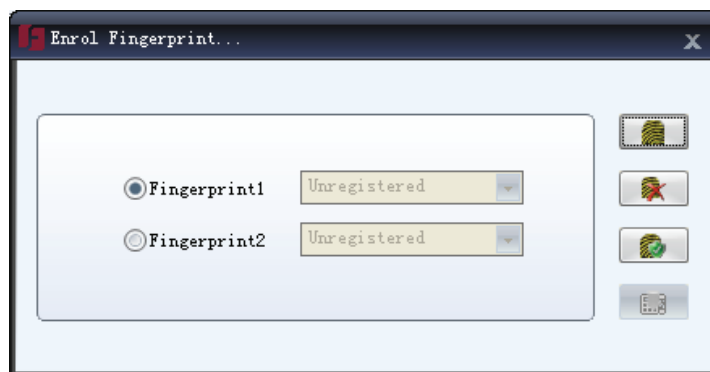


Fig. 4-8 Acquire Card Number from a Card Reader

- d) Select serial port and card format
- e) Put the cursor on the “card number” text box and swipe the card through the card reader.
- f) Press OK to confirm.

Card Format: The Software supports 3 card formats: ddd-ddddd (8 decimal), dddddddd (8 decimal) and HHHHHH (six hexadecimal). Refer to section 7.1 Add a Card for details.

Add a Card: Choose the appropriate card format, enter card number and the click “add” . The card is now added to the card list. If the card number already exists in the system, the system will prompt “card number already exists”. A cardholder can have one or multiple cards.

Delete a Card: Select the card to be deleted in the card list, click “delete” , and the card will be deleted from the list.

Card Property: Card property includes 8 items: **Defended Effective**. Check the check box in front of the item to enable the function. Refer to Section 7.1 Add a Card for details.

When finished, click “save” and the new card(s) will be registered to all valid controllers to which the cardholder is permitted access (defined by the access group to which the card belongs). A dialog box reporting “Operation succeeded” will pop up. If other dialog boxes pop up during the process, please check the controller based on the information contained in the message. For example, if the controller is not connected to the computer, a dialog box will pop up to show “Timeouts when connecting to controller”. Verify the connection from the controller to the computer and then click “Yes”. The user can register other cards with the controller. Otherwise, click “No” and the card will not be registered to the controller.

4.2.2 Fingerprint Information

Fingerprint information is part of cardholder description. Each cardholder can have 2 fingerprints stored in the system.

4.2.2.1 Acquire Fingerprints

There are two methods of acquiring fingerprints:

- ✧ Capture fingerprint from a fingerprint scanner.
- ✧ If a fingerprint controller is installed in the system, user can upload a fingerprint from the controller via the Software.

Capture from a fingerprint scanner

Click “Enroll fingerprint”  Enrol Fingerprint, and the enroll fingerprint window will pop up (Fig. 4-10).

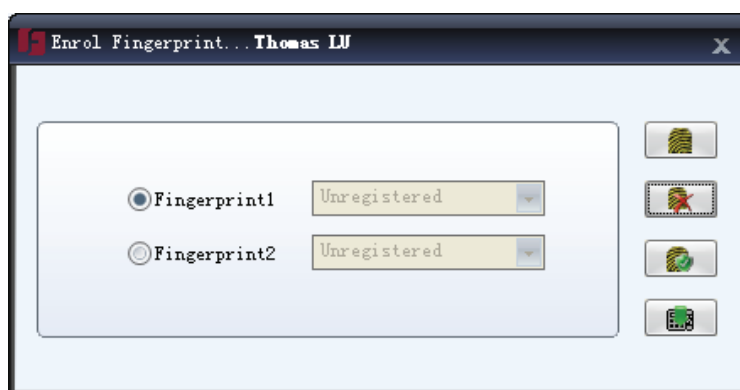


Fig. 4-10 Enroll Fingerprint Window

Select the fingerprint to capture (such as fingerprint 1), and click “capture fingerprint”  to open the window for capturing fingerprints (Fig. 4-11).

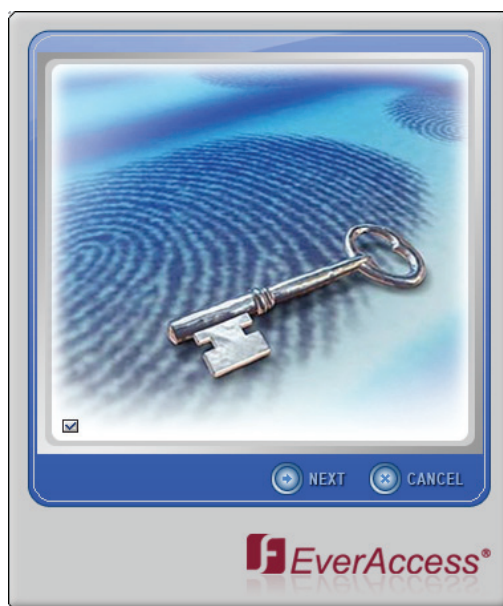


Fig. 4-11 Capture Fingerprint

Click “Next” button to open the window as shown in Fig. 4-12, click the dot on top of the finger from which a fingerprint will be collected (the right index finger is selected in this example).



Fig. 4-12 Select a Finger

The system will then open the window for registering fingerprints (Fig. 4-13).



Fig. 4-13 Place the finger

Place the selected finger on the scanner. When finished scanning, the system will prompt to remove the finger (Fig. 4-14).



Fig. 4-14 Remove the Finger

After removing the finger, the system will prompt to place the finger on the scanner for a second time.

After finishing the second fingerprint collection, the system will prompt "In process of establishing fingerprint features" (Fig. 4-16).



Fig. 4-16 Establishing Fingerprint Features

After finishing, the system will return to the enroll fingerprint window (Fig. 4-16).



Fig. 4-17 Enroll Fingerprint

Click "Next" button to finish enrolling the fingerprint (Fig. 4-18).



Fig. 4-18 Fingerprint Enrolled

Click "Finish" button to return to the window for enrolling fingerprint (Fig. 4-19). Repeat the process to enroll the 2nd fingerprint of the cardholder. Or, choose the corresponding finger at the step associated with figure 4-17 above.....

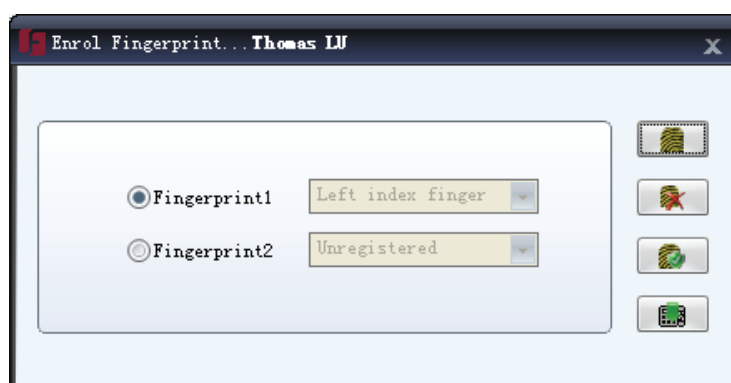


Fig. 4-19 Enroll Fingerprint 1 Complete

Note: If the fingerprint scanner is not connected to the computer or if drivers are not installed, a dialog box will pop up as shown in Fig. 4-20.

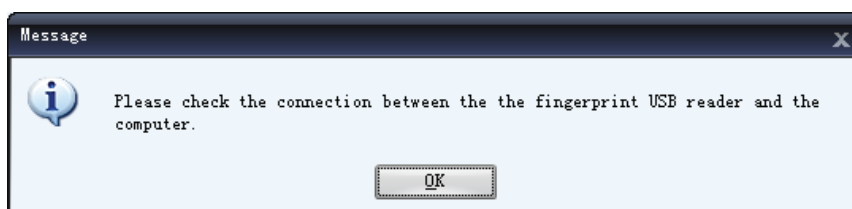


Fig. 4-20 To Confirm that the Fingerprint Scanner is connected to the Computer

Upload from a fingerprint controller

When a fingerprint controller is installed in the system and the cardholder has registered fingerprint information in the fingerprint controller, the fingerprint information can be uploaded from the fingerprint controller.

In a fingerprint controller, each card can be associated with 2 fingerprints, which can be either identical or different. Fingerprint information is part of card information. Therefore, in order to use this function, the cardholder needs a fingerprint card. If a cardholder has multiple cards or if multiple fingerprint controllers are installed in the system, the latest fingerprint information will overwrite the previous data. Click “Access Control Management” → “Data Communication” → “Upload data to computer”. Select the fingerprint controller from the controller list on the left, check “Upload from a fingerprint controller” on the right and click “Save”. All the fingerprint information from the controller will be uploaded to the computer (Fig.4-21).

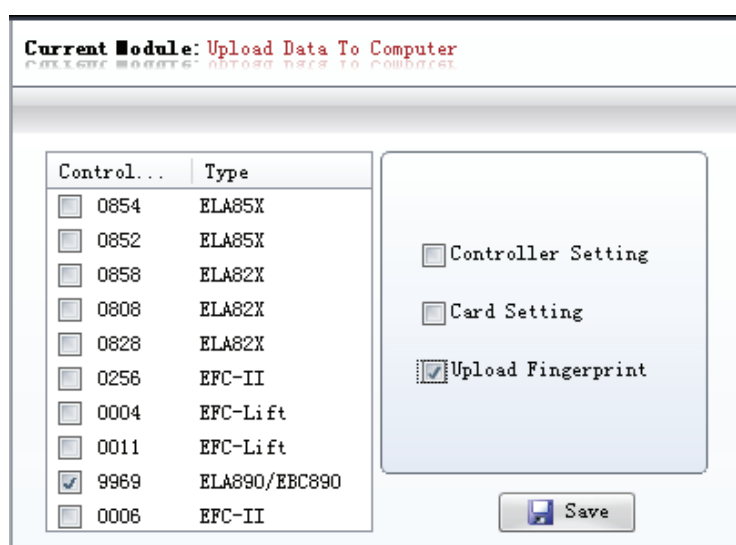


Fig. 4-21 Upload All Fingerprints from the Controller

User can also choose to upload fingerprint information from a single card. Click “Upload from a fingerprint controller”  to open the window as shown in Fig. 4-22

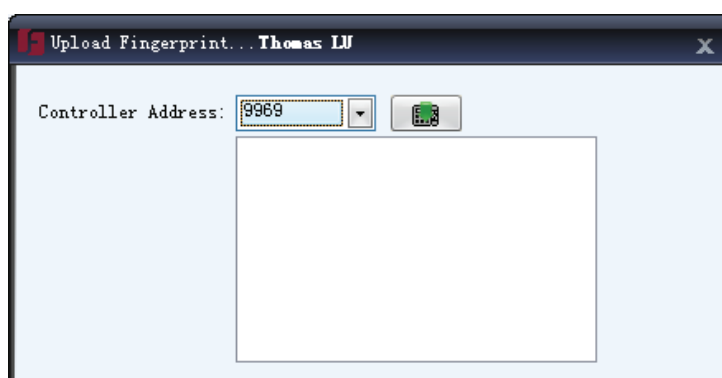


Fig. 4-22 Upload one Fingerprint from the Controller in the Cardholder Window

The fingerprint is “unknown type” if it is uploaded from the controller, as shown in Fig. 4-23.

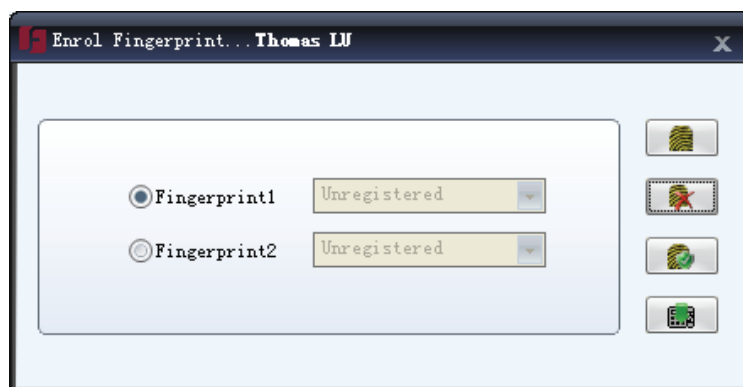


Fig. 4-23 Uploading Complete

4.2.2.2 Delete a Fingerprint

Select the fingerprint to be deleted (such as fingerprint 1), and then click “Delete Fingerprint” . The fingerprint will be deleted and the fingerprint type is unregistered.

4.2.2.3 Verify Fingerprint

Select the fingerprint to be verified (such as fingerprint 1), then click “Verify Fingerprint”  to open the window for verifying fingerprint (Fig. 4-24).

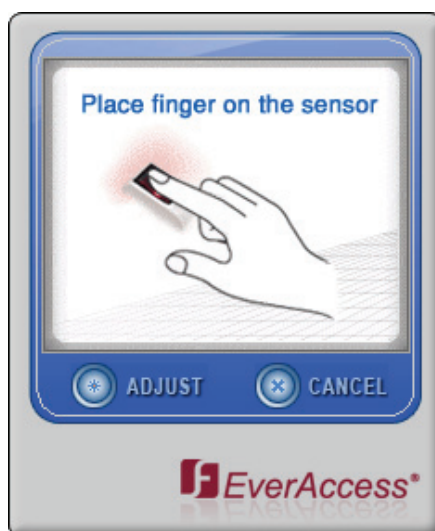


Fig. 4-24 Verify Fingerprint

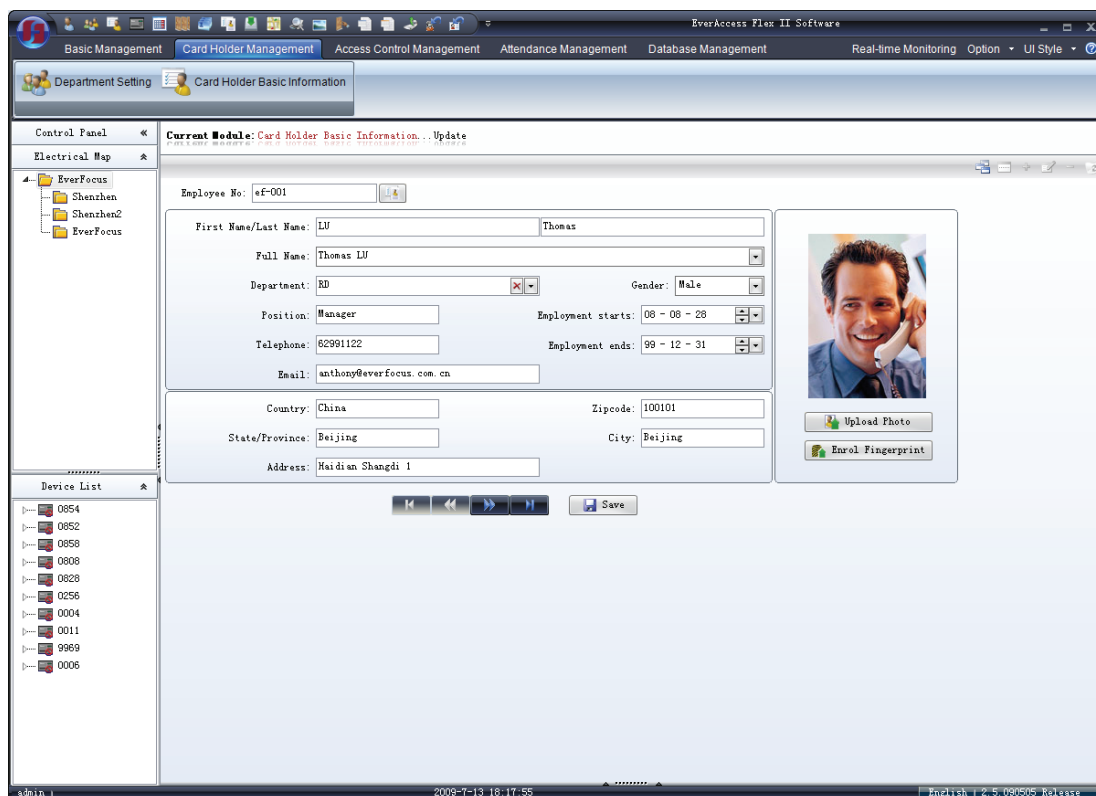
Proceed as prompted by the instruction on the window for the cardholder to scan their fingerprint for comparison. When finished, the system will prompt “Verification succeeded” or “Verification Failed” to verify if the stored fingerprint is correct.

4.2.3 Import Cardholder Information

Click “Database Management” → “Importing Data” → “Import Cardholder Information”, Refer to section 13.4.1 Importing Cardholder Information for details.

4.2.4 Edit Cardholder Information

In the window for “Cardholder Setting” (Fig. 4-26), select the cardholder to be changed, and then click “Edit”  in the “function editing area” or select “Edit” from the right-click menu to open the window for editing cardholder information (Fig. 4-25). After editing, click “Save” and a dialog box confirming “operation succeeded” will pop up. Otherwise, click “View All” to return to the window for “Cardholder Setting”.



The screenshot shows the 'EverAccess Flex II Software' interface. The main window is titled 'Current Module: Card Holder Basic Information... Update'. It contains a form for editing cardholder information. The form fields are as follows:

- Employee No.: eF-001
- First Name/Last Name: LUV Thomas
- Full Name: Thomas LUV
- Department: RD
- Gender: Male
- Position: Manager
- Employment starts: 08 - 08 - 28
- Employment ends: 99 - 12 - 31
- Telephone: 62991122
- Email: anthony@everfocus.com.cn
- Country: China
- Zipcode: 100101
- State/Province: Beijing
- City: Beijing
- Address: Haidian Shangdi 1

There is a photo upload section on the right with a photo of a man and buttons for 'Upload Photo' and 'Enrol Fingerprint'. A 'Save' button is at the bottom right. The left sidebar shows a 'Device List' with various card IDs.

Fig. 4-25 Edit Cardholder Information

4.2.5 Batch-Edit Cardholder Information

The Software offers the option of batch editing cardholder information. This function provides an efficient way to edit a certain item for multiple cardholders at the same.

Drag the mouse down the cardholder list to select multiple adjacent cardholders or use the “Ctrl” key on the keyboard to select nonadjacent cardholders. After selecting the cardholders to be edited, right click to open the menu (Fig. 4-26) and select “Edit”. The window for batch editing cardholder information will be shown.

Employee No	Full Name	Department	Position	Employment starts	Employment ends
ef-001	Thomas LU	RD	Manager	08-08-28	99-12-31
ef-002	Lisa Yang	RD	PM	08-08-28	99-12-31
ef-003	Keary	RD\Software1	engineer	08-08-21	99-12-31
ef-004	John Ma	RD\Software2	engineer	08-08-21	99-12-31
ef-005	William Pan	Sales\SHA	Manager	08-08-21	99-12-31
ef-006	Irene Mei	Sales	Accountant	08-08-21	99-12-31
ef-007	Jeff Huang	Sales	engineer	08-08-21	99-12-31
ef-008		Beijing	Manager	08-08-21	99-12-31
ef-009		Sales\BJN	sales	08-08-28	99-12-31
ef-010		Sales\SZN	Sales	08-08-28	99-12-31
ef-011		Sales\SUZ	Manager	08-08-28	99-12-31
ef-012		Shenzhen	Manager	08-08-28	99-12-31
ef-013		Sales\SHA	Engineer	08-08-28	99-12-31
ef-014	Chair	Sales\NHN	engineer	08-08-28	99-12-31

Fig. 4-26 Batch Editing

The public information of the selected cardholders will be shown and the item name is highlighted (Fig. 4-27). After editing, click “Save” and a dialog box will pop up to prompt that “The operation cannot be undone”. Click “OK” to confirm and the information for all selected cardholders will be changed.

Update... Card Holder Basic Information

Department: Gender: Male

Position: Employment starts: 08 - 08 - 21

Telephone: Employment ends: 99 - 12 - 31

Email: yang@everaccess.com

Country: CHINA Zipcode: 100101

State/Province: City:

Address:

Save Reset Close

Fig. 4-27 Batch Editing Cardholders

Note: This operation only changes the profile items for those cardholders whose names are highlighted. The rest of the cardholders' information remains unchanged.

4.2.6 View Cardholder Information

4.2.6.1 View Cardholder list

Click “Cardholder Management” ➔ “Cardholder Setting” to view all the cardholders in the system.

4.2.6.2 View Details of Cardholder Information

Click the “View Details” button  in the “function editing area” (Fig. 4-4) to open the window for viewing cardholder information details (Fig. 4-28). Users can choose to view the details of a different cardholder by using the navigation buttons “BW” and “FW” at the bottom of the window. Clicking the “Edit” button  in the “function editing area” allows editing of the cardholder Information (Fig. 3-10).

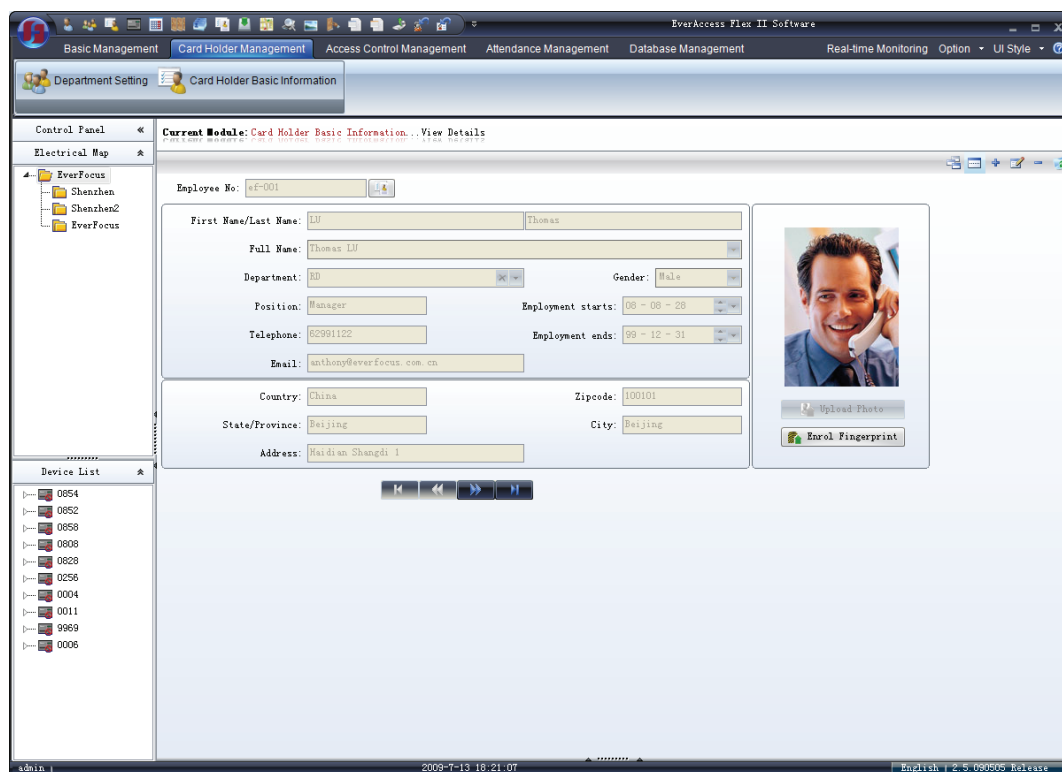


Fig. 4-28 View Details of Cardholder's Profile

4.2.7 Delete Cardholders

4.2.7.1 Delete Selected Cardholder(s)

Using the Cardholder Setting window (Fig. 4-4), drag the mouse down the cardholder list to select multiple adjacent cardholders or use the “Ctrl” key on the keyboard to select nonadjacent cardholders. After selecting the cardholders to be deleted, click the “Delete” button  in the “function editing area”. A dialog box will be shown to prompt users to confirm the deletion (Fig. 4-29). Click “Yes” to delete the cardholder(s) and another dialog box confirming “Operation succeeded” will pop up. Otherwise, click “Cancel” to exit.

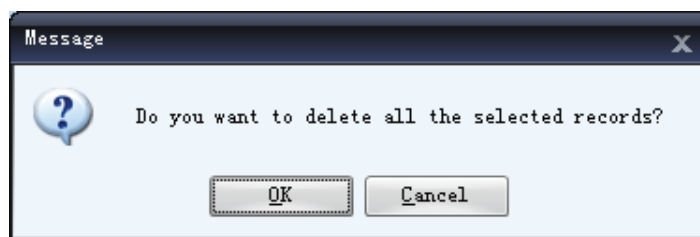


Fig. 4-29 Prompt to Confirm Deletion of Selected Cardholder(s)

4.2.7.2 Delete All Cardholder

Using the Cardholder Setting window (Fig. 4-4), click the “Delete All”  button in the “function editing area”. A dialog box will be shown to prompt users to confirm the deletion (Fig. 4-30). Click “Yes” to delete **all** the cardholders and another dialog box reporting “Operation succeeded” will pop up. Otherwise, click “Cancel” to exit.

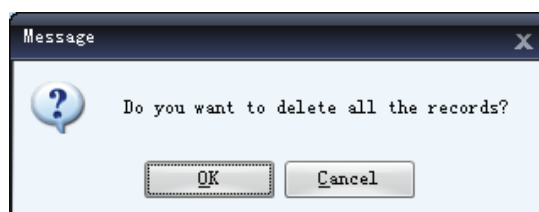


Fig. 4-29 Prompt to Confirm Deletion of All Cardholders

4.2.8 Search Cardholder

4.2.8.1 Basic Search

In the “search toolbar”, select search criteria from employee number, name, department name and position and enter the values in the “keywords” textbox(es). Click the “Search” button  to start searching. If there are cardholders matching the search criteria, they will be shown in the cardholder list (Fig. 4-31).

Note: The search function here is exact match. For example, to search a cardholder belonging to “Sales Department → Service Group”, select “Department Name” in the search criteria and type in “Sales Department/Service Group” in the “keyword” text box, then click  to start searching. If one needs ‘fuzzy’ searching with multiple search criteria, please use the “Advanced Search” function (Refer to section 4.2.8.2 for details).

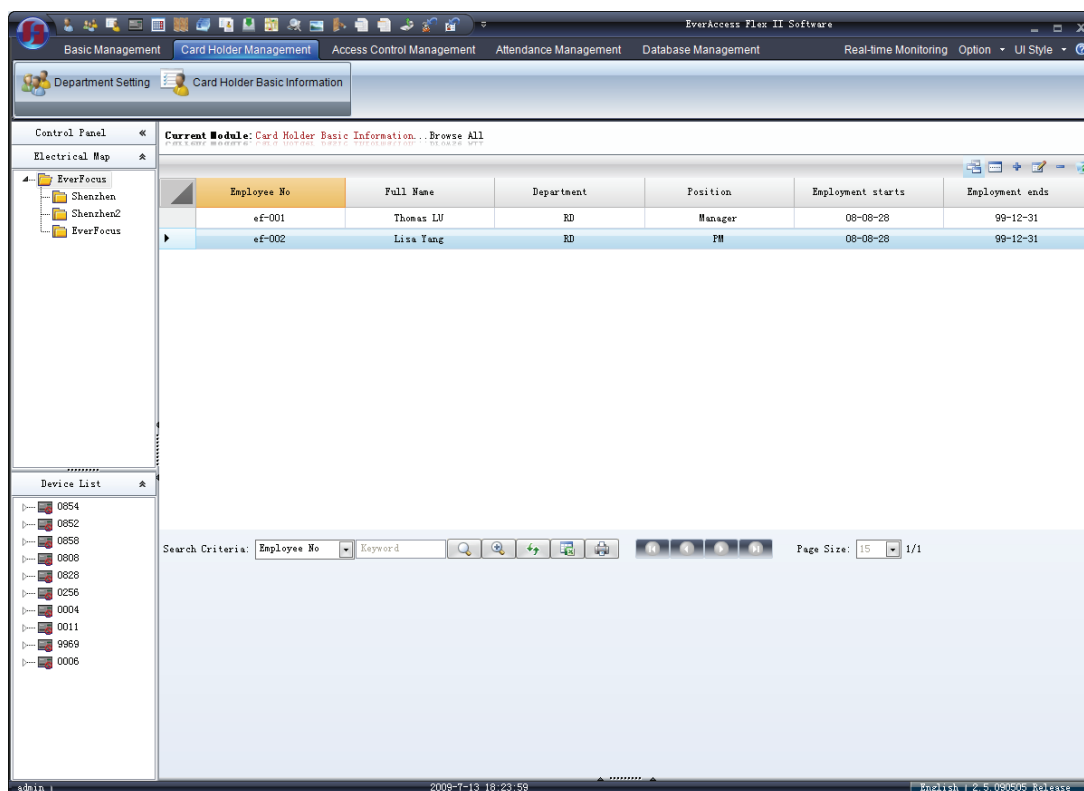


Fig. 4-31 Search Cardholder

4.2.8.2 Advanced Search

Click “Advanced Search”  in the “search toolbar” to open the window for advanced search (Fig. 4-32). Fill in the search criteria, and click “Search”  to start searching. If there are cardholders matching the search criteria, they will be shown in the cardholder list. When finished, click “Close”  return to the “Cardholder Setting” window.

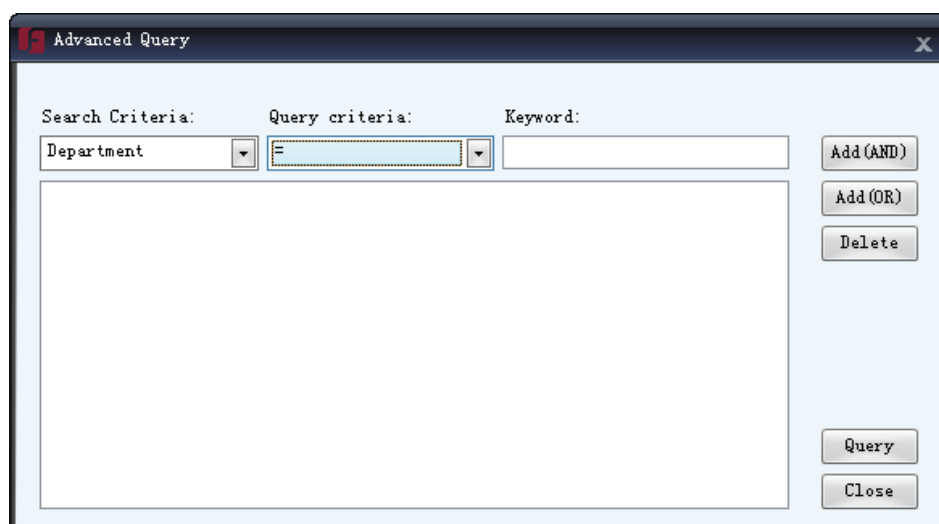


Fig. 4-32 Advanced Search

Search criteria: the name of search fields, including department name, employee number, last name, first name, name, gender, position, phone, email, employment start date, employment end date, fingerprint 1, fingerprint 2, nation, state/province, city, zip code and address.

Condition: the matching condition for the search criteria, such as “=” (equal), “<>” (not equal), “>” (greater than), “>=” (greater than or equal”, “<” (less than”, “<=” (less than or equal), “includes (in any position)” “includes (starts with)”, “includes (ends with)”.

Keywords: enter or select the data that define the search criteria. For example, if the search criteria is “fingerprint 1” and “fingerprint 2”, select the fingerprint type in the keywords text box (Fig. 4-33).

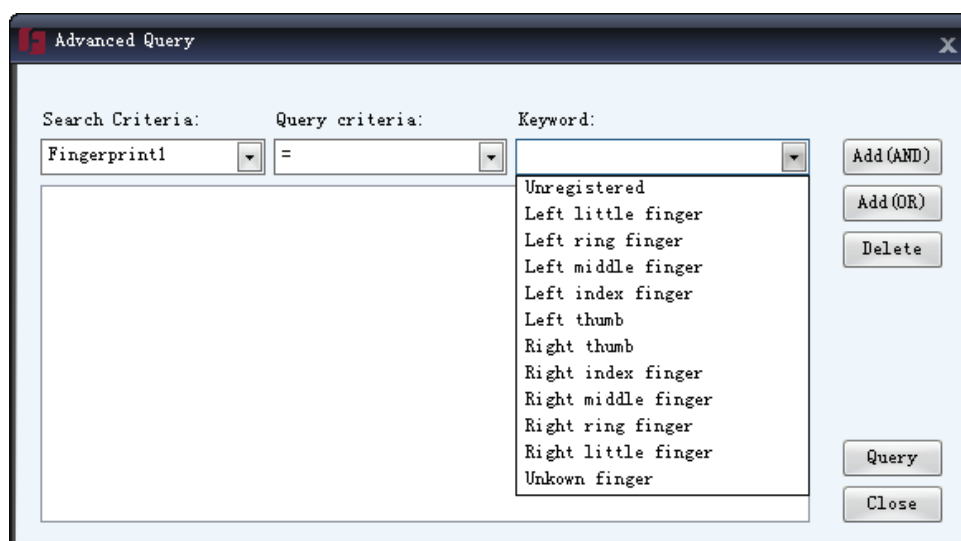


Fig. 4-33 Keywords for search criteria “Fingerprint 1”

Add (and): search for cardholders that match two or more search criteria.

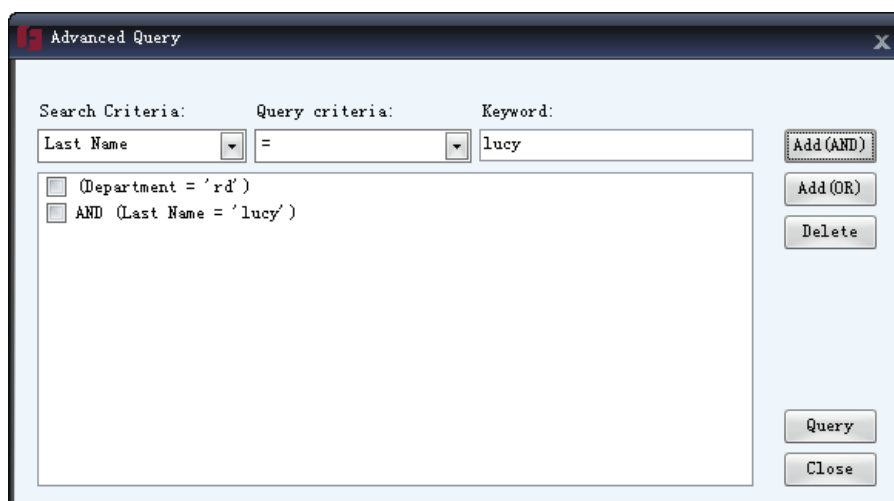
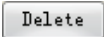


Fig. 4-34 Advanced Search-“and”

Add (or): search for cardholders that match any of the search criteria.

Delete: select the search criteria in the search criteria list, click “Delete”  to delete the selected search criteria.

4.2.9 Refresh Cardholder Information

Click “Refresh”  in the “search toolbar” to show the current cardholder list.

4.2.10 Export Cardholder Information

Click “Export”  in the “search toolbar”; a dialog box will pop up to show that the cardholder information is being exported as an Excel file. When finished exporting, another dialog box will pop up to ask whether to open the file (Fig. 4-35). To open the file, Excel must be installed on the PC.

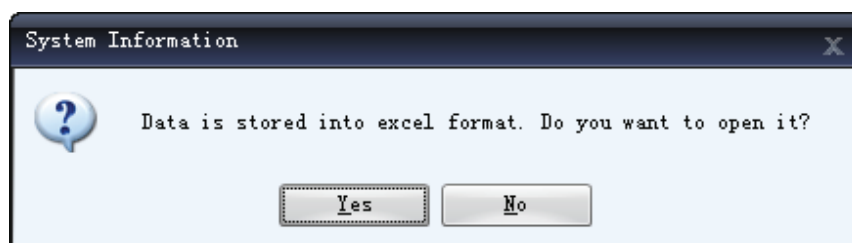


Fig. 4-35 Open Excel File

4.2.11 Print Cardholder Information

Click “Print”  in the “searching toolbar” to open the window for printing cardholder information (Fig. 4-36). The menu bar includes: export, print, refresh, switch nodes, go to the first page, go to last page, go to next page, go to the last page, go to page N, close, search text, zoom in/out etc.

Print Card Holder Basic Information

主报表

Card Holder Basic Information

Employee No	Full Name	Department	Position	Employment star	Employment end
ef-001	Thomas LU	RD	Manager	2008-08-28	2099-12-31
ef-002	Lisa Yang	RD	PM	2008-08-28	2099-12-31
ef-003	Keary	RD\Software1	engineer	2008-08-21	2099-12-31
ef-004	John Ma	RD\Software2	engineer	2008-08-21	2099-12-31
ef-005	William Pan	Sales\SHA	Manager	2008-08-21	2099-12-31
ef-006	Irene Mei	Sales	Accountant	2008-08-21	2099-12-31
ef-007	Jeff Huang	Sales	engineer	2008-08-21	2099-12-31
ef-008	Jason Li	Beijing	Manager	2008-08-21	2099-12-31
ef-009	Dick Wang	Sales\BJN	sales	2008-08-28	2099-12-31
ef-010	Tommy Tang	Sales\SZN	Sales	2008-08-28	2099-12-31
ef-011	Cindy	Sales\SUZ	Manager	2008-08-28	2099-12-31
ef-012	Allen	Shenzhen	Manager	2008-08-28	2099-12-31
ef-013	Liking	Sales\SHA	Engineer	2008-08-28	2099-12-31
ef-014	Chair	Sales\NUN	engineer	2008-08-28	2099-12-31
ef-015	Peter	Sales\SUZ	sales	2008-08-28	2099-12-31
ef-016	Susan	Sales	sales	2008-08-28	2099-12-31
ef-017	Color	Sales	sales	2008-08-28	2099-12-31
ef-018	Yuki	Sales	sales	2008-08-28	2099-12-31
ef-019	Yubo	Sales	sales	2008-11-21	2099-12-31
ef-020	Vincent	Sales	sales	2008-11-21	2099-12-31
ef-021	Bill	Sales	sales	2008-11-21	2099-12-31

当前页码: 1 总页数: 1 缩放系数: 100%

Fig. 4-36 Print Cardholder Information

Chapter 5

5 Controller Management

This chapter introduces how to configure a controller, including adding or deleting a controller, door settings, reader settings, arm zone settings and alarm output settings, etc.

Controller management is the basis of access control system administration, as controllers perform the vast majority of system functions. The Software provides a simple window for controller management. The Software is designed to work with ELA82x, ELA85x, Flex I and Flex II series controllers developed by Everfocus. The specific products include: ELA831 single-door controller, ELA822/808/828 2/4/8-door controller, ELA852/854/858 2/4/8 door controller, ELA890 fingerprint controller, elevator controller, EFC-02-1A 2/4/8-door controller, EFC-01-2A single-door controller and EFC-02-2A 2/4/8-door controller.

After connecting the controller to the computer (Refer to the provided hardware manual for details), users can use “Controller Management” to add the controller to the system and configure controller parameters. Click “Access Control Management” → “Controller Setting” (Fig. 5-1).

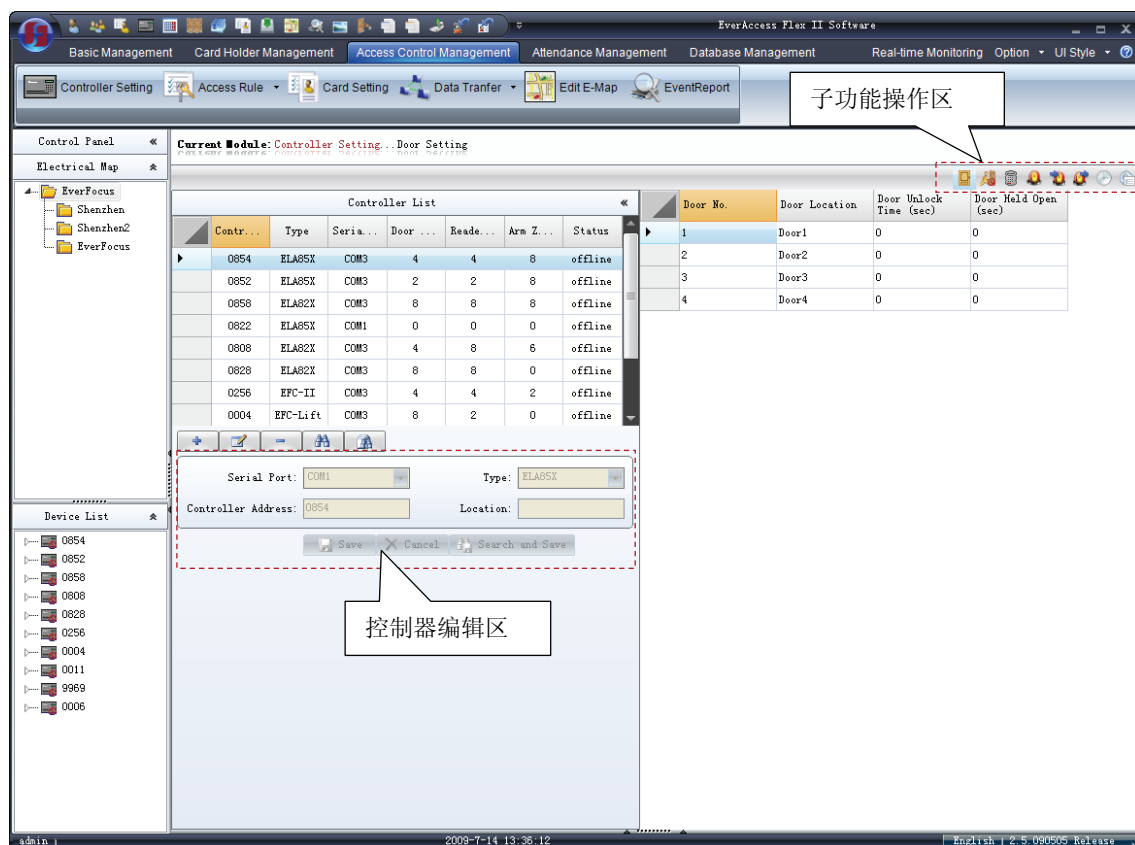


Fig. 5-1 Controller Setting

Sub function operation buttons:

-  Door/Floor Setting
-  APB Setting
-  Reader Setting
-  Arm Zone Setting
-  Alarm Input Setting
-  Alarm Output Setting
-  Alarm Output Time Setting
-  System Setting

The following table gives the detailed function list for each controller type. “√” in the cells indicates the function is available to this controller.

Controller Type	Door/Floor or Setting	APB Setting	Reader Setting	Arm zone Setting	Alarm Input Setting	Alarm Output Setting	Alarm Output Time Setting	System Setting
ELA82X	√			√				√
ELA85X	√		√	√		√		√
EFC-Lift	√		√					√

ELA890	✓			✓		✓	✓	✓
EFC-I	✓	✓	✓	✓		✓	✓	✓
EFC-II	✓	✓	✓		✓	✓	✓	✓

5.1 Add a Controller

Click the “Add” button  in the “controller editing area” to open the window for adding a controller. The “controller editing area” is displayed (Fig. 5-2). Select the serial port, controller type, controller address and location.

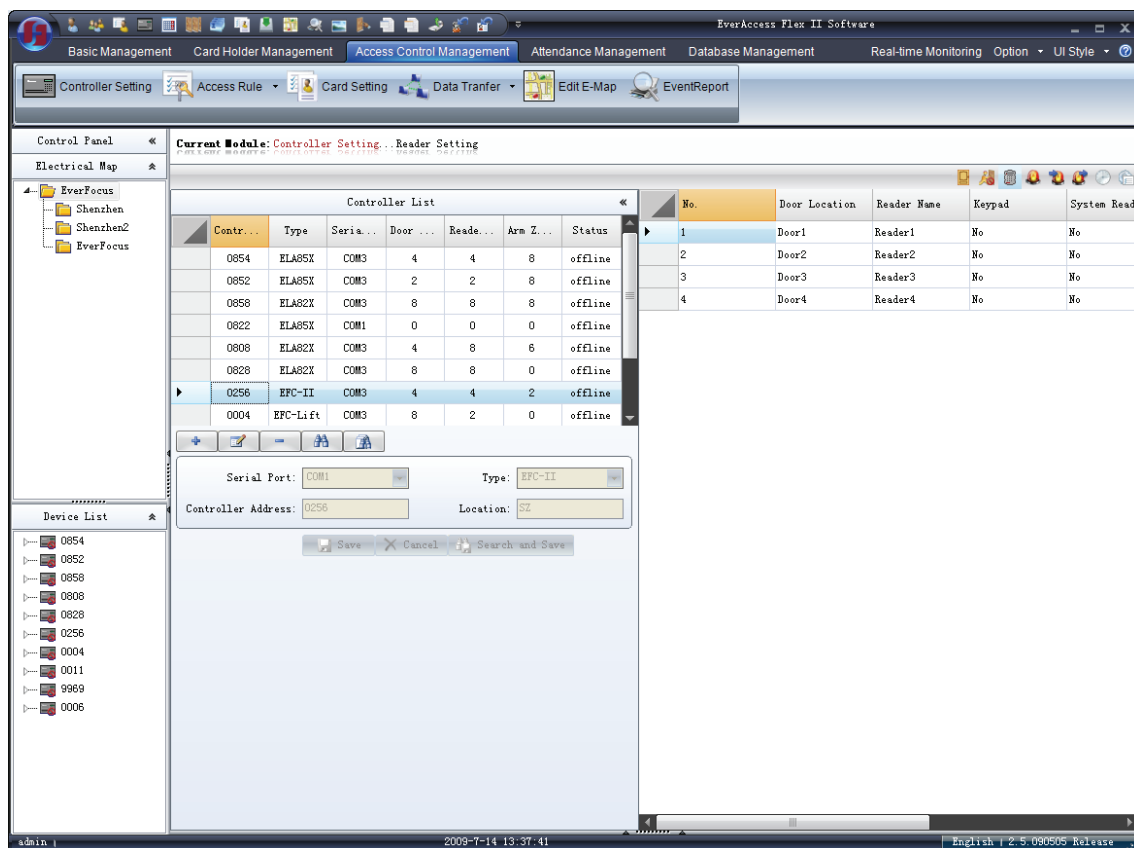
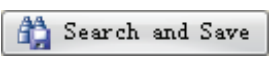


Fig. 5-2 Add a Controller

Note: The door schedule is set to be “default” in a newly added controller. Refer to Section 6.2 Door Setting to modify the door schedule.

If the added controller is offline, click “Save”  and a dialog box confirming “operation succeeded” will pop up. The controller is added to the system and the status is automatically set as “offline”. The controller is not valid at the moment and will not show up in the controller list on the left panel until communication is established.

If the added controller is online, click “Search and Save”  to search for it. If found, the controller is then added to the system; If not found, a dialog box reporting “Timeout when connecting to controller” will pop up (Fig. 5-3). Check the connection between the controller and the computer and search again.

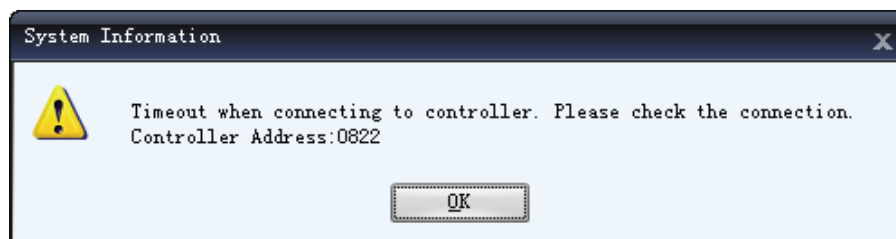


Fig. 5-3 Timeout when connecting to controller

Note: The “Save” button is only to save the newly added data to database, but will not to search for the controller to establish communication; the “Search and Save” button is to search for the controller setting as well as to save thenew data to database. It serves both the function of “Search” and “Save”. Refer to section 5.4.1 for searching controllers.

5.2 Edit a Controller

Select the controller to be edited in the controller list. Click “Edit” button  and the “controller editing area” becomes editable. User can then edit the serial port, controller type, controller address and location. When finished, click “Save”  or “Search and Save”  and a dialog box reporting “Operation succeeded” will pop up.

5.3 Delete a Controller

Select the controller to be deleted in the controller list. Click “Delete” button  and a dialog box prompting “Delete the controller?” will pop up. Click “OK” to delete the controller and another dialog box reporting “operation succeeded” will pop up. Otherwise, click “Cancel” to exit.

When a controller is deleted, all related data, including sub-functionality setting and schedule settings on each door zone, are deleted as well.

5.4 Search Controller(s)

5.4.1 Search a Controller

This function is to update the controller settings including basic parameters, door settings, reader settings, arm zone settings, APB settings, alarm output settings, alarm output time settings and system settings etc. In the controller list, select the controller to be updated, then click the “Search” button .

5.4.2 Search all Controllers

This function is to update the settings of all controllers. Click the “Search All Controllers” button . If a controller cannot be found, a dialog box reporting “Timeout when

connecting to controller” will pop up. Click “Yes” to continue searching other controllers, otherwise, click “No” to exit.

5.5 Controller Setting

5.5.1 Door/Floor Setting

Select the controller in the controller list on the left, click the “Door/Floor Setting” button  in the “sub function operation area”. All door zones associated with the selected controller will be shown on the right. Edit door settings using functions offered in the “sub function editing area”.

Door/Floor Setting includes door/floor No., door/floor location, door open time, door held open time, interlock and location of door etc. (Fig. 5-4).

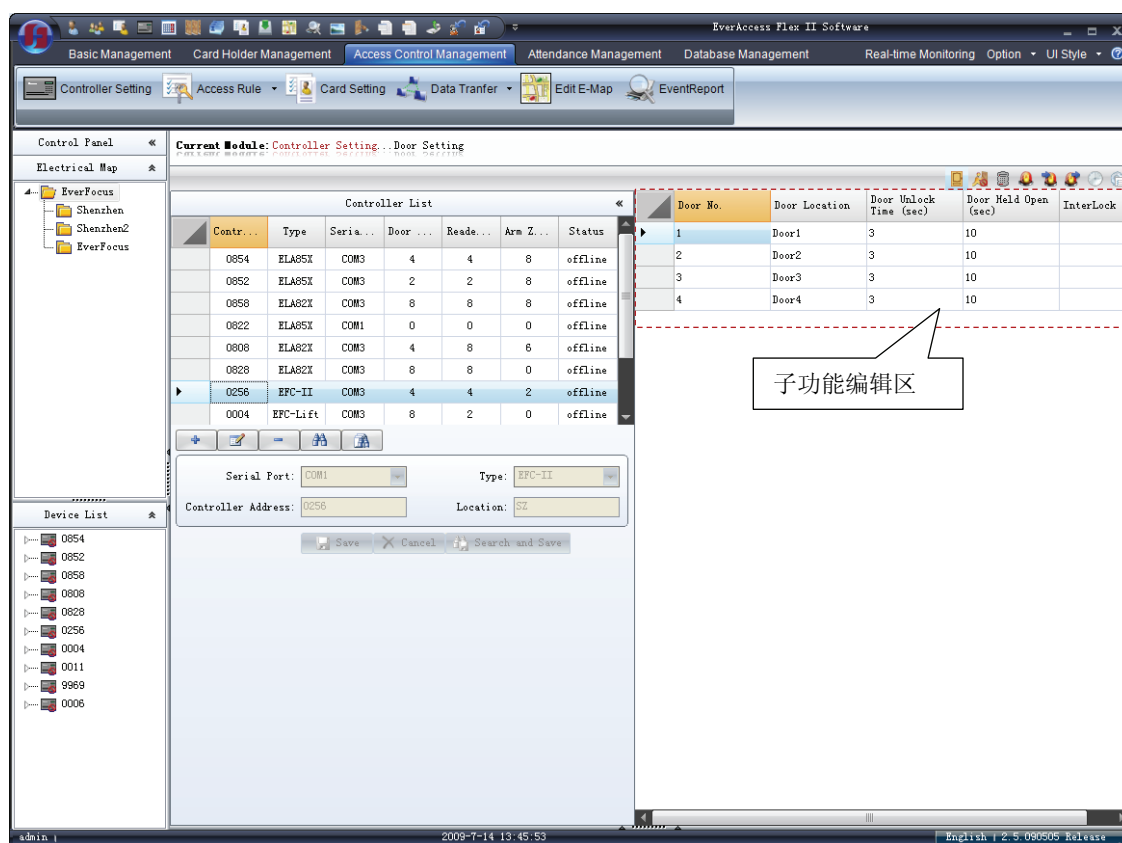


Fig. 5-4 Door/Floor Setting

The following table gives the door/floor setting options available for each controller type. “√” in a cell indicates the option is available in this controller.

Controller Type	Door/floor No.	Door/floor location	Door open time	Door Held Open time	Interlock	Location to door
ELA82X (single-door)	√	√				√
ELA82X	√	√				

(multi-door)						
ELA85X	✓	✓	✓	✓		
EFC-Lift	✓	✓	✓	✓		
ELA890	✓	✓	✓	✓		✓
EFC-I	✓	✓	✓	✓	✓	
EFC-II	✓	✓	✓	✓	✓	

Door/Floor No.: the number of the current door/floor.

Door/Floor Location: to describe the actual location of the current door/floor.

Door Open Time: This function is used for setting the door open time when a valid card is swiped or Request-to-Exit button is pressed. The door remains unlocked as long as the RTX button is pressed down. The door open time does not begin until the button is released. If two cards are swiped successively, the door open time does not begin until after the second card has been swiped. The default time is 3 seconds. The maximum door open time is 59999 seconds.

Door Held Open Time: A door sensor monitors the open/close status of a door. If an “unlock” state is not set by the system (door is normally considered closed), then door should close automatically (controlled doors should be equipped with closers) after remaining open for a nominal time. It is considered abnormal if controller does not receive the door closed signal from door sensor within a reasonable amount of time after the door is opened. This time period is called the door held open time (or door over time). Based on this setting, the controller will determine when to generate an alarm after the door held open time period elapses. The default value of door held open time is 5 seconds. The maximum door held open time is 59999 seconds.

Interlock: If two or more doors are interlocked, they cannot both be opened the same time. If one of the interlocked doors is open, the other door cannot be opened until the first door is closed. In short, there can be only one door open at any time for a set of interlocked doors. Users can set the interlock function when an interlock compatible controller operates two or more doors. This setting is particularly suitable to an environment that requires high-level security, such as banks and prisons. Fig. 5.5 shows a diagram of two interlocked doors.

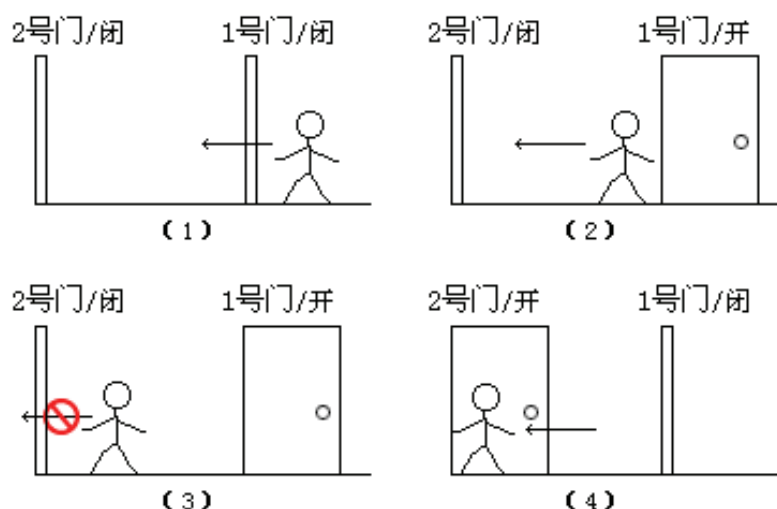


Fig. 5-5 Diagram of Two Interlocked Doors

In the diagram above, door 1 and door 2 are a pair of interlocked doors.

- (1) Both door 1 and 2 are locked, and a cardholder enters through door 1.
- (2) Door 1 is opened and the cardholder enters through door 1. Door 2 is closed.
- (3) If door 1 remains open, the cardholder cannot open door 2 (due to interlock rules).
- (4) Once door 1 is closed, door 2 can then be opened.

Note: Interlocking is only applicable to doors operated by the same controller. One controller can control interlocking among multiple doors.

The Door Setting Window for different controller types is listed below:

✧ ELA82X Series Controller

An ELA808 4-door controller is used as an example here (Fig. 5-6). An ELA808 4-door controller can connect to 8 card readers that control one way (entry *or* exit) for 8 doors or two way (entry *and* exit) for 4 doors.

In the “sub function editing area” on the right, users can edit door location names. Click “Save”  after editing the item.

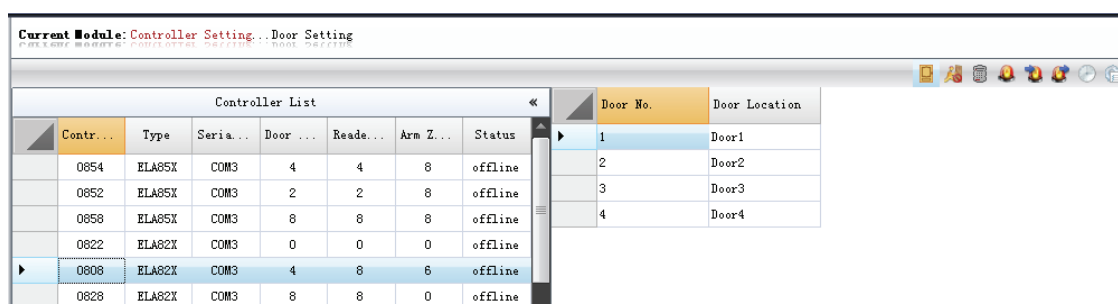


Fig. 5-6 ELA82x Controller Door/Floor Setting

✧ ELA85X Series Controller

An ELA858 8-door controller is used as an example here (Fig. 5-7). An ELA858 8-door controller can connect to 8 card readers that control one way (entry *or* exit) for 8 doors or two ways (entry *and* exit) for 4 doors.

In the “sub function editing area” on the right, users can edit door location, door open time and door held open time. Click “Save”  after editing each item.

Current Module: Controller Setting...Door Setting

Controller List								Door No.	Door Location	Door Unlock Time (sec)	Door Held Open (sec)
Contr...	Type	Serial...	Door ...	Reade...	Arm Z...	Status					
0854	ELA85X	COM3	4	4	8	offline	1	Door1	0	0	
0852	ELA85X	COM3	2	2	8	offline	2	Door2	0	0	
0858	ELA82X	COM3	8	8	8	offline	3	Door3	0	0	
0822	ELA85X	COM1	0	0	0	offline	4	Door4	0	0	

Fig. 5-7 ELA85x Controller Door/Floor Setting

✧ Fingerprint Controller

An ELA890 fingerprint controller is used as an example here (Fig. 5-8). An ELA890 fingerprint controller can control a single door.

In the “sub function editing area” on the right, users can edit door location, door open time, door held open time and location of door. In the drop-down menu of “location of door”, select interior or exterior. Click “Save”  after editing each item.

Current Module: Controller Setting...Door Setting

Controller List								      				
	Door No.	Door Location	Door Unlock Time (sec)	Door Held Open (sec)	Position to door							
1	Door1	3	5	Outside								

Contr...	Type	Serial...	Door ...	Reade...	Arm Z...	Status
0808	ELA82X	COM3	4	8	6	offline
0828	ELA82X	COM3	8	8	0	offline
0256	EFC-II	COM3	4	4	2	offline
0004	EFC-Lift	COM3	8	2	0	offline
0011	EFC-Lift	COM3	2	2	0	offline
9969	ELA890...	COM3	1	1	4	offline
0006	EFC-II	COM3	1	0	5	offline

Fig. 5-8 Fingerprint Controller Door/Floor Setting

✧ Flex Series Controller

An EFC-08-2A 8-door controller is used as an example here (Fig. 5-9). An EFC-08-2A 8-door controller can connect to 8 card readers that control one way (entry *or* exit) for 8 doors or two ways (entry *and* exit) for 4 doors.

In the “sub function editing area” on the right, users can edit door location, door open time, door held open time and interlock. In the drop-down menu for “interlock”, select the doors that will be interlocked with the current door. For example, if door 2, 3 and 5 are selected for door 1, door 1 cannot be opened when any of the linked doors 2, 3 or 5 is opened. Click “Save”  after editing each item.

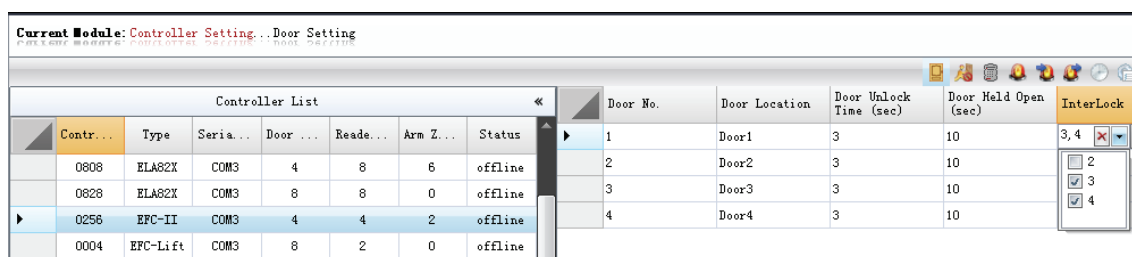


Fig. 5-9 Flex Series Controller Door/Floor Setting

✧ EFC Series Elevator Controller

An EFC-08-lift 8-floor elevator controller is used as an example here (Fig. 5-10). An EFC-08-lift controller can connect to 8 card readers that control access to an elevator from 8 floors.

In the “sub function editing area” on the right, users can edit floor location. Click “Save”  after editing each item.

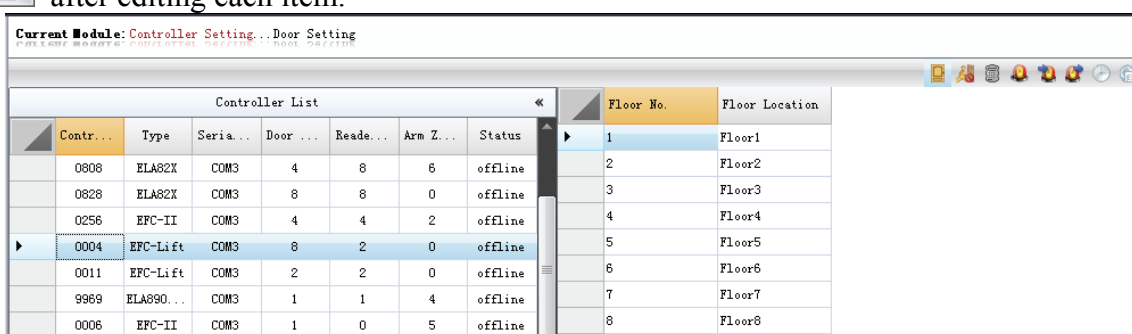


Fig. 5-10 EFC Series Elevator Controller Door/Floor Setting

5.5.2 Anti-Passback (APB) Setting

Select the controller in the controller list on the left, click the “APB Setting” button  in the “sub function operation area”. All door zones connected to the selected controller will be shown on the right. Edit the APB settings using the commands offered in “sub function editing area”.

APB Settings includes Area No., Area Name, APB enabled and Exterior Area etc. (Fig. 5-11).

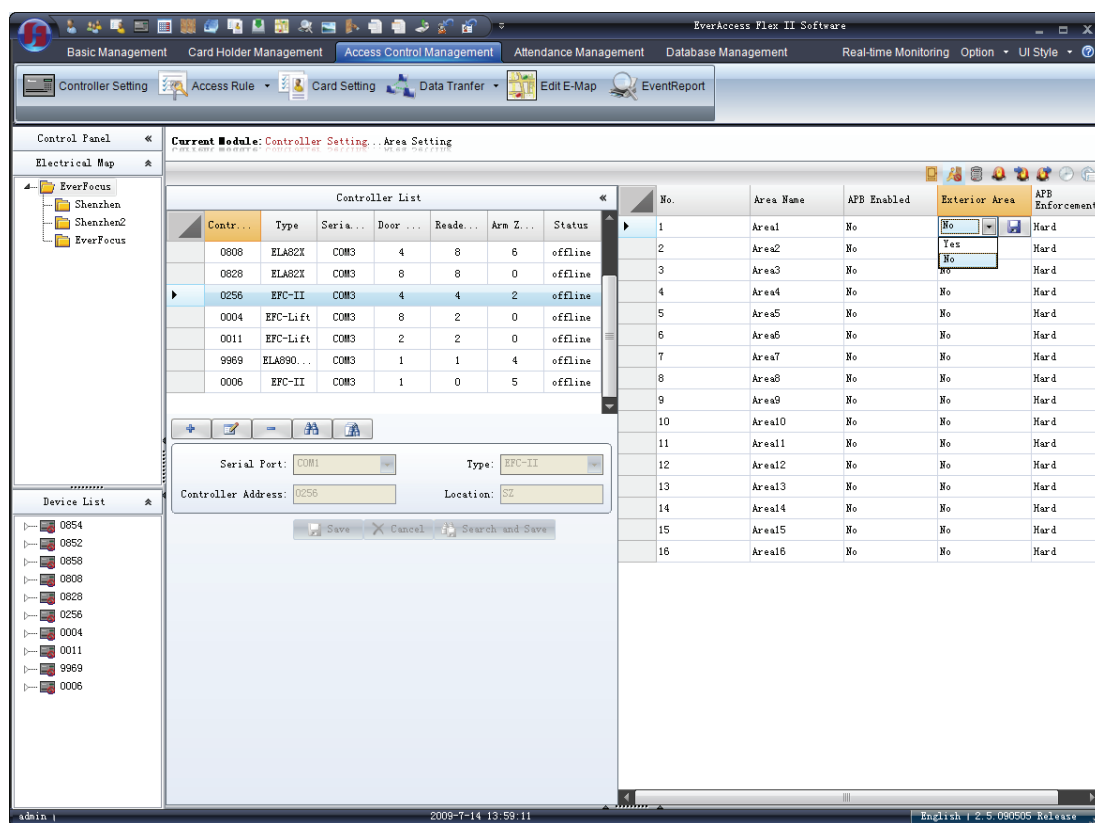


Fig. 5-11 APB Setting

Area No.: the number of the current area

Area Name: name of the current area

APB enabled: “Yes” means the APB is enabled; “No” means APB is disabled.

Exterior Area: Users can define an area as an exterior area; this function is used to control exterior doors in an emergency. Each reader has a source area and a destination area. If any of the two areas is an exterior area, the door on which the reader is installed is an exterior door. From the controller list on the left, users can remotely control exterior doors using the right-click menu. (Refer to Section 14.1.2 Exterior Area and Exterior Doors for details)

Door behavior under APB event: “Open” means the door is opened when an APB event is triggered; “Close” means the door is closed when an APB event is triggered.

Note: APB function is only applicable to EFC-I and EFC-II Series Controllers

5.5.3 Reader Setting

A card reader recognizes a card presented to it, either by users swiping their card or entering card PIN on a keypad reader, and transmits the code to a controller. In “one door, two ways” setting, a door is equipped with 2 readers that control entry and exit respectively. A more common setting is “one door, one way”, in which one reader is used to control entry only.

Reader Settings includes Reader No., door location, reader name, keypad reader or not, system reader or not, In/Out type, source area and destination area (Fig. 5-12).

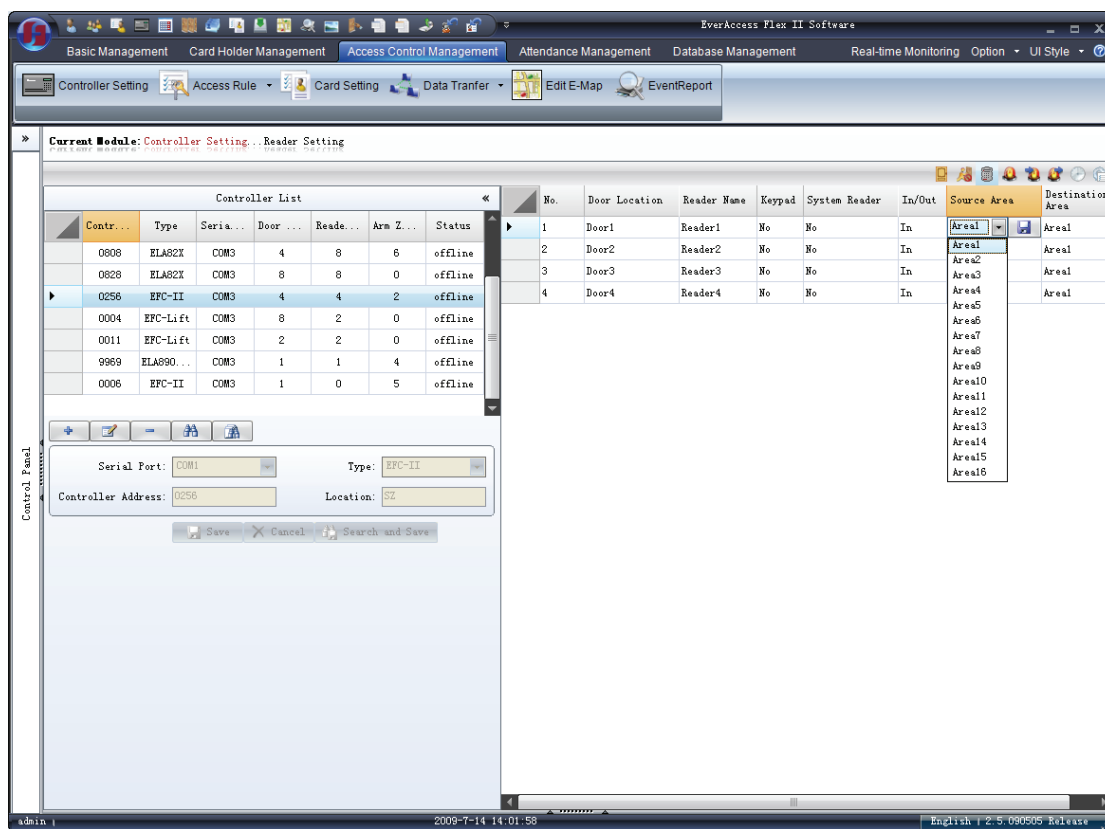


Fig. 5-12 Reader Setting

The following table gives the reader setting options available for each controller type. “√” in the cells indicates the option is available when using this controller.

Controller Type	Reader No.	Door Location	Reader Name	Keypad Reader	System Reader	In/Out Type	Source Area	Destination Area
ELA85X	√	√	√	√	√	√		
EFC-Lift	√			√	√			
EFC-I	√	√	√	√	√	√	√	√

Reader No.: the number of the current reader

Door location: description of the actual location of the door on which the reader is installed. The default setting is that each reader is installed on the door with the same number. Users can change this setting.

Reader name: name of the reader.

Keypad reader: whether the current reader is a keypad reader. For a keypad reader, if a card PIN is enabled and the verification level is “card plus PIN”, one must also enter the card PIN using the keypad to gain access to the door.

System reader: whether the current reader is a system reader. A system reader can transmit a card number to the controller to enroll cards in the controller. Any reader connected to the controller can be set as a system reader.

In/Out type: whether the reader is an entry reader or an exit reader.

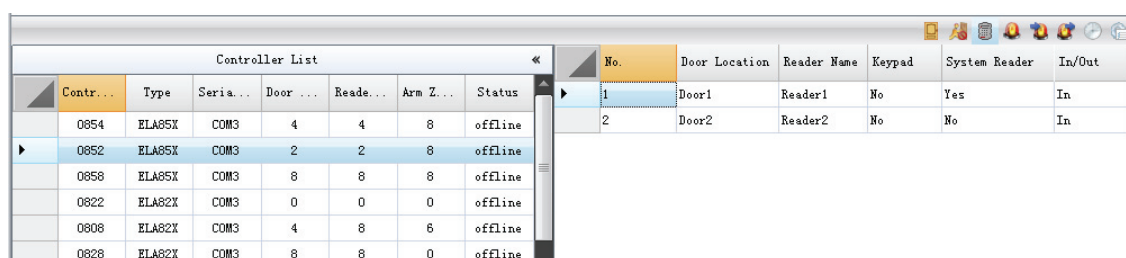
Source area and Destination area: These settings are for APB function. Refer to Section 14.1 Area Anti-Passback (APB) for details.

The Reader Setting Window of different controller types is listed below:

✧ ELA85X Series Controller

An ELA858 8-door controller is used as an example here (Fig. 5-13). An ELA858 8-door controller can connect to 8 card readers that control one way (entry or exit) for 8 doors or two ways (entry and exit) for 4 doors.

In the “sub function editing area” on the right, users can edit door location, reader name, keypad reader, system reader and In/Out type. Click “Save”  after editing each item.



Controller List						
Contr...	Type	Serial...	Door ...	Reade...	Arm Z...	Status
0854	ELA85X	COM3	4	4	8	offline
0852	ELA85X	COM3	2	2	8	offline
0858	ELA85X	COM3	8	8	8	offline
0822	ELA82X	COM3	0	0	0	offline
0808	ELA82X	COM3	4	8	6	offline
0828	ELA82X	COM3	8	8	0	offline

No.	Door Location	Reader Name	Keypad	System Reader	In/Out
1	Door1	Reader1	No	Yes	In
2	Door2	Reader2	No	No	In

Fig. 5-13 ELA85X Series Controller Reader Setting

✧ Flex Series Controller

An EFC-08-2A 8-door controller is used as an example here (Fig. 5-14). An EFC-08-2A 8-door controller can connect to 8 card readers that control one way for 8 doors or two ways for 4 doors.

In the “sub function editing area” on the right, users can edit door location, reader name, keypad reader, system reader, In/Out type, source area and destination area. Click “Save”  after editing each item.

APB Setting for the reader example: Reader 1 and Reader 2 are a pair of APB readers. Reader 1 is an entry reader with source area “Area 1” and destination area “Area 2”; Reader 2 is an exit reader with source area “Area 2” and destination area “Area 1” (Fig. 5-14). Refer to Section 5.5.2 Anti-Passback (APB) Setting for APB rules.

Controller List							No.	Door Location	Reader Name	Keypad	System Reader	In/Out	Source Area	Destination Area
Contr...	Type	Serial...	Door ...	Reade...	Arm Z...	Status								
0854	ELA85X	COM3	4	4	8	offline	1	Door1	Reader1	No	No	In	Area1	Area2
0852	ELA85X	COM3	2	2	8	offline	2	Door2	Reader2	No	No	In	Area1	Area1
0858	ELA85X	COM3	8	8	8	offline	3	Door3	Reader3	No	No	In	Area1	Area1
0822	ELA82X	COM3	0	0	0	offline	4	Door4	Reader4	No	No	In	Area1	Area1
0808	ELA82X	COM3	4	8	6	offline								
0828	ELA82X	COM3	8	8	0	offline								
0256	EFC-II	COM3	4	4	2	offline								
0004	EFC-Lift	COM3	8	2	0	offline								

Fig. 5-14 Flex Series Controller Reader Setting

❖ EFC Series Elevator Controller

An EFC-08-lift 8-floor elevator controller is used as an example here (Fig. 5-15). An EFC-08-lift controller can connect to 8 card readers that control an 8-floor elevator.

In the “sub function editing area” on the right, users can edit keypad reader and system reader settings. Click “Save”  after editing each item.

Controller List							No.	Keypad	System Reader
Contr...	Type	Serial...	Door ...	Reade...	Arm Z...	Status			
0852	ELA85X	COM3	2	2	8	offline	1	Yes	Yes
0858	ELA85X	COM3	8	8	8	offline	2	Yes	Yes
0822	ELA82X	COM3	0	0	0	offline			
0808	ELA82X	COM3	4	8	6	offline			
0828	ELA82X	COM3	8	8	0	offline			
0256	EFC-II	COM3	4	4	2	offline			
0004	EFC-Lift	COM3	8	2	0	offline			
0011	EFC-Lift	COM3	2	2	0	offline			

Fig. 5-15 EFC Series Elevator Controller Reader Setting

5.5.4 Arm Zone Setting

Arm zone setting is used to edit arm zone names for the selected controller. When placing the mouse over an arm zone in an electronic map (E-Map), the name of the arm zone will be shown. Refer to Section 5.5.8 System Setting for details on how to enable an arm zone.

Select a controller from the controller list on the left, click the “Arm Zone Setting” button  in the “sub function operation area”. All arm zones for the selected controller will be shown on the right. Click “Save”  after editing each item.

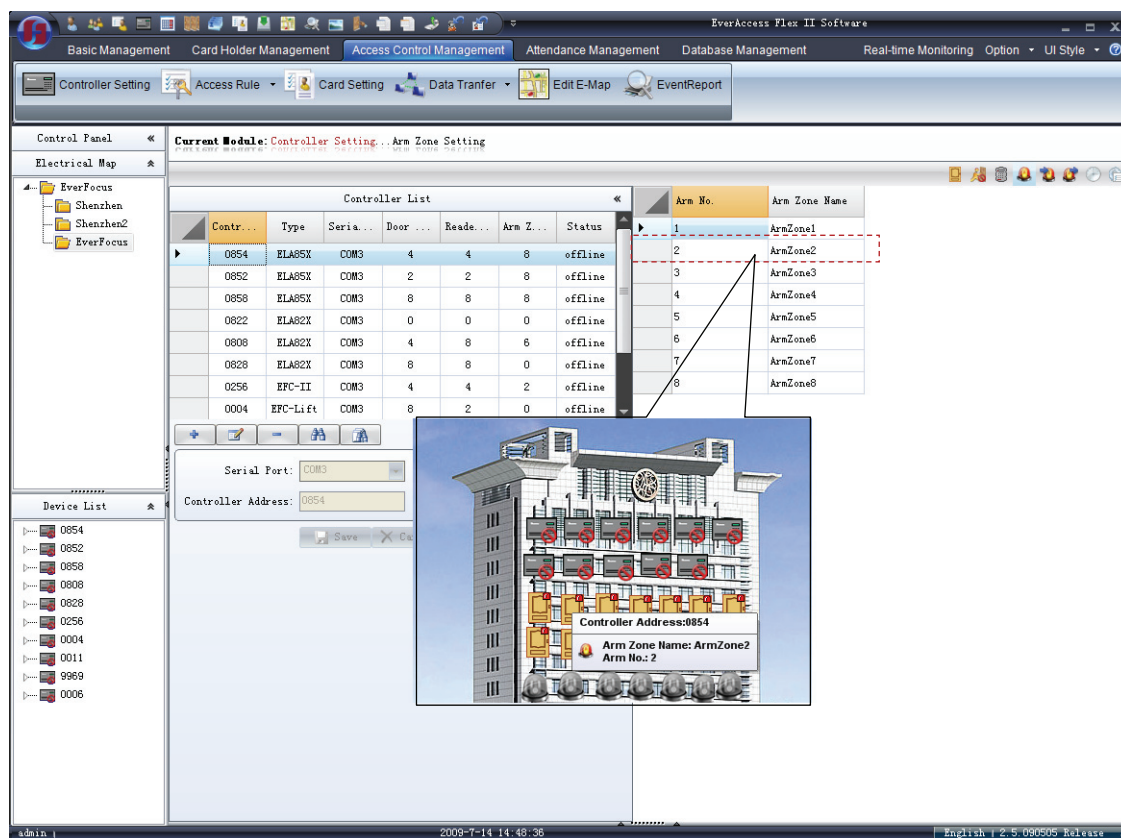


Fig. 5-16 Arm Zone Setting

5.5.5 Alarm Input Setting

Alarm Input Setting is only applicable to Flex II Series Controllers. With alarm modules and door modules fully installed, a Flex II controller can accommodate 1 fire alarm input, 1 general alarm input and 8 external alarm inputs. At the same time, Flex II controllers provide very powerful configuration options. A detailed description is given below:

❖ Components for Alarm Input

The main module and alarm module of Flex II controllers have several alarm input terminals. The main module has 2 alarm inputs, corresponding to 1 fire alarm and 1 general alarm. The alarm module has 8 alarm inputs, which can connect to external alarm input devices, such as PIR motion sensors and glass break sensors, etc.

The above mentioned are physical devices supplied by others, providing an alarm function. Users can freely define the allocation of any input to any output.

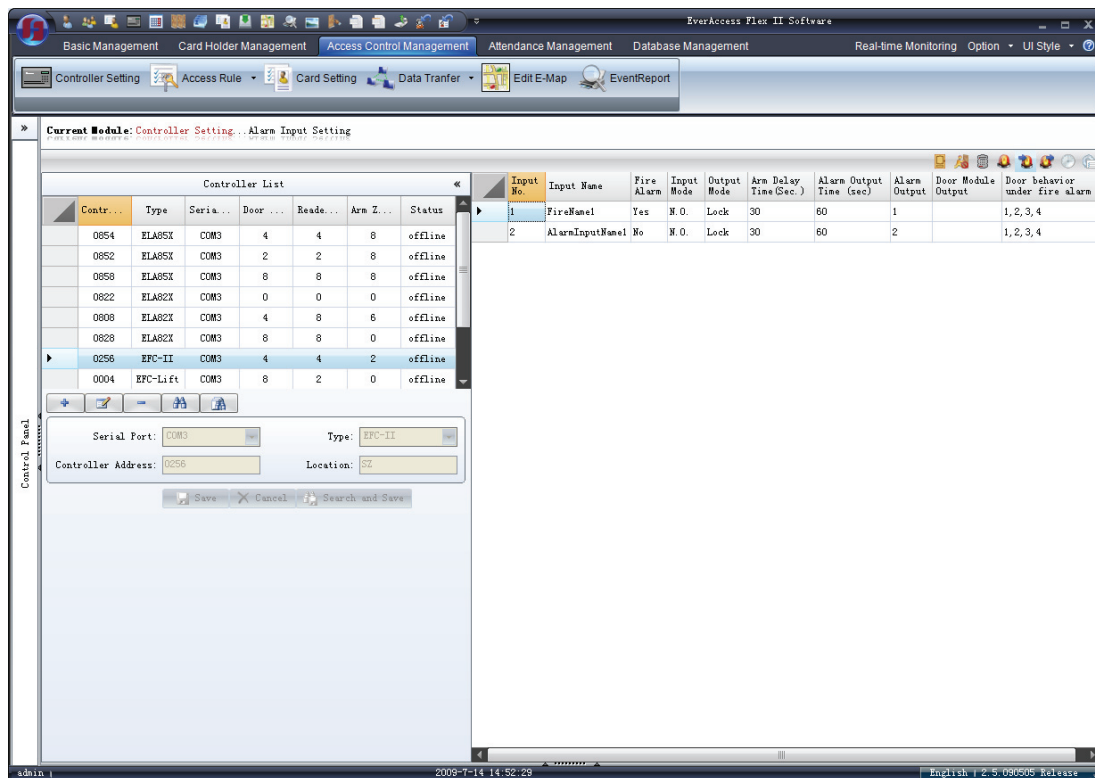


Fig. 5-17 Alarm Input Setting

Alarm Input Name: Assign a name to the alarm input

Fire Alarm: “Yes” means the alarm is a fire alarm, “No” means it is not a fire alarm. *The first alarm input by default is a fire alarm and cannot be modified.*

Alarm Input Mode: “Invalid” means the current alarm input is disabled. “Normally Open” means the circuit is not connected during normal conditions (i.e. no input) and an alarm will be triggered if circuit is closed. Normally open circuits are ‘unsupervised’, since there is no way to determine if some portion of the wiring has been cut or broken. “Normally Closed” is the opposite; this is a supervised circuit, in that it will be triggered if the wiring is broken for any reason.

Alarm Output Mode: “Lock” mode means an alarm output remains triggered if there is an alarm condition. Once triggered, the alarm output remains till the alarm output time has elapsed or has been reset manually. If the alarm input signal lasts longer than the alarm output time, a new alarm output will be triggered. “Direct” mode means there will be an alarm output only as long as there is an active input signal; the alarm output stops when the alarm input signal stops.

Alarm Delay Time (s): in the range of 1-59999 seconds

Alarm Output Time (s): in the range of 1-59999 seconds

Alarm Output: the terminal(s) assigned to the alarm output

Door Module Output: the terminal(s) of the door module for the alarm output

Door behavior under fire alarm: which doors will be opened during fire alarm

5.5.6 Alarm output Setting

Flex II Series Controllers are equipped with powerful alarm functions. With alarm modules and door modules fully installed, a Flex II controller can accommodate 10 alarm inputs and 18 alarm outputs. At the same time, Flex II controllers provide flexible configuration options. Users can freely define the allocation of any input to any output. A detailed description is given below:

❖ Components for Alarm Output

A Flex II controller consists of two basic components: the main module and the door module. Users can install up to 4 door modules and 1 alarm module into a main module.

These three types of modules are all equipped with alarm functions. The main module has 2 alarm outputs, corresponding to a main alarm output and an auxiliary alarm output.

Each door module has 2 alarm outputs, which usually react to alarm events on the corresponding door. However, they 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 outputs, which can connect to 2A external alarm devices.

The external alarm devices mentioned above are physical devices, supplied by others, providing alarm functions. User can freely define the allocation of any input to any output. Events, alarms and output configuration are introduced below:

❖ Alarm Setting Basic

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

Some events are critical which must trigger the alarm output, like a fire alarm input, a zone alarm input, etc. However, some events are not as important and should not trigger an alarm output, like denied access due to an invalid time, for example. These settings all depend on the users' requirements. The Software collects all events that might trigger an alarm output and provides the full capacity to determine whether or not to enable an 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 functionality 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 a main module, door module and/or alarm module. The Alarm output setting window is presented in a table format and every column represents an alarm output device. 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 a door. “Yes” indicates there is alarm output triggered (relay energized), “No” indicates there is no alarm output triggered (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 an alarm output will be generated only if the events occurs on the corresponding door module.

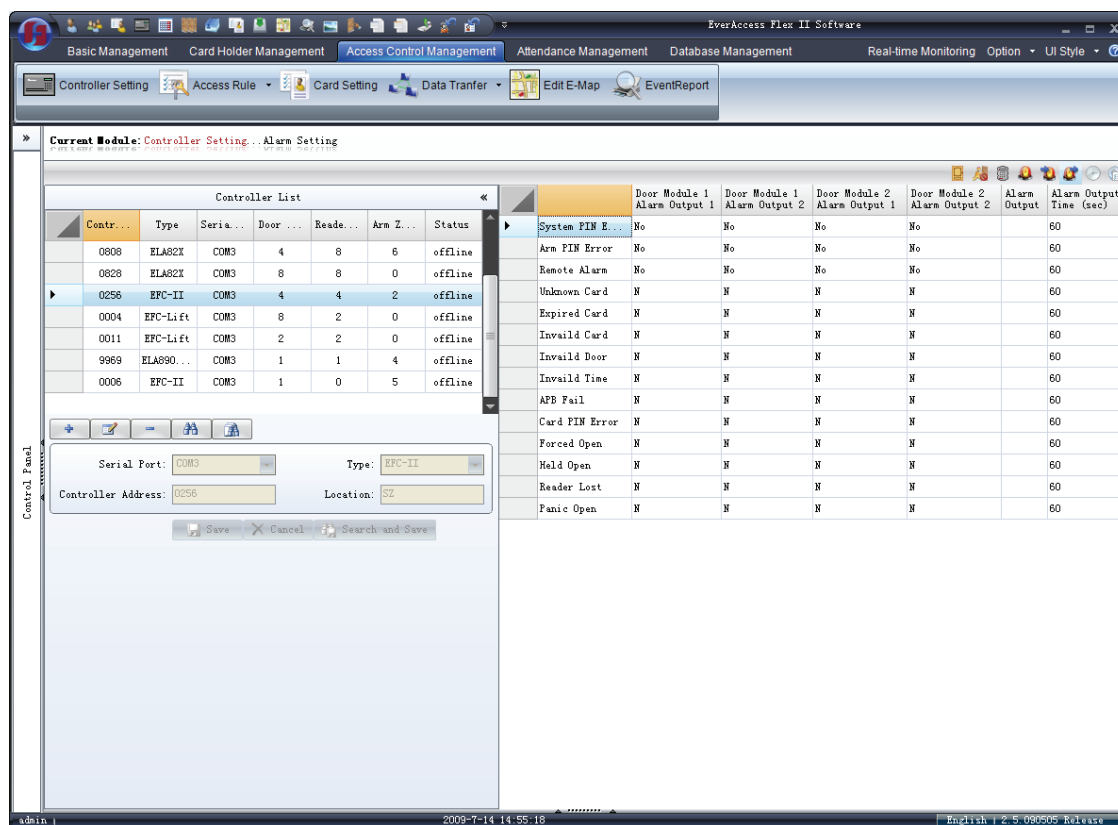


Fig. 5-18 Alarm Output Setting

Zone Alarm: The zone alarm reacts to one or more of 8 alarm inputs on the alarm module. Any events in an arm zone may trigger a zone alarm event. The controller generates an alarm output according on the settings in the “Zone Alarm” column.

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

System PIN Fail: A user is required to enter system PIN to enter 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 settings 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 settings 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 settings 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 settings in the “Remote Alarm” column.

Unknown Card: Unknown card refers to a card that was 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 an expiration date. After the expiration 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 settings in the “Expired Card” column.

Invalid Card: Users 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 settings 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. An Invalid Door event will be generated when a card is presented at any door at which it does not have the right to pass regardless of time zone. The controller generates alarm output(s) according to the settings 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 during certain time zones. An invalid time event will be generated if a card is presented during a time period in which it does not have the right to pass. The controller generates alarm output(s) according to the settings 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 settings in the “APB Fail” column. Refer to Section 5.5.2 APB setting for detail. Not clear.

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 settings 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 nor has a Request-to-Exit button been pressed. The controller generates alarm output(s) according to the

settings in the “Door Forced Open”. In practice, a door forced open event will be generated if a door is kicked open, or if the lock has been left unlocked or otherwise defeated.

Door panic Open: A door panic open event is generated if a cardholder enters a panic PIN to unlock a door when under panic. The controller generates alarm output(s) according to the setting in the “Door panic Open”. Panic means that someone is being forced by others to unlock this door, so he/she is opening it in a way to send an alarm without revealing the alarm to the person forcing his/her actions.

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 remains open for longer than the allowed door held open time. The controller generates alarm output(s) according to the settings 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.

The Alarm Output Setting Window for different controller types is listed below:

✧ Fingerprint Controller

An ELA890 fingerprint controller is used as an example here. An ELA890 fingerprint controller has alarm outputs only on the main module, corresponding to the main alarm output and auxiliary alarm output.

In the “sub function editing area” on the right, users can edit arm zone, fire alarm, system PIN fail, ARM PIN fail, remote alarm, unknown card, expired card, invalid time, card PIN fail, door forced open and door held open. Click “Save”  after editing each item (Fig. 5-19).

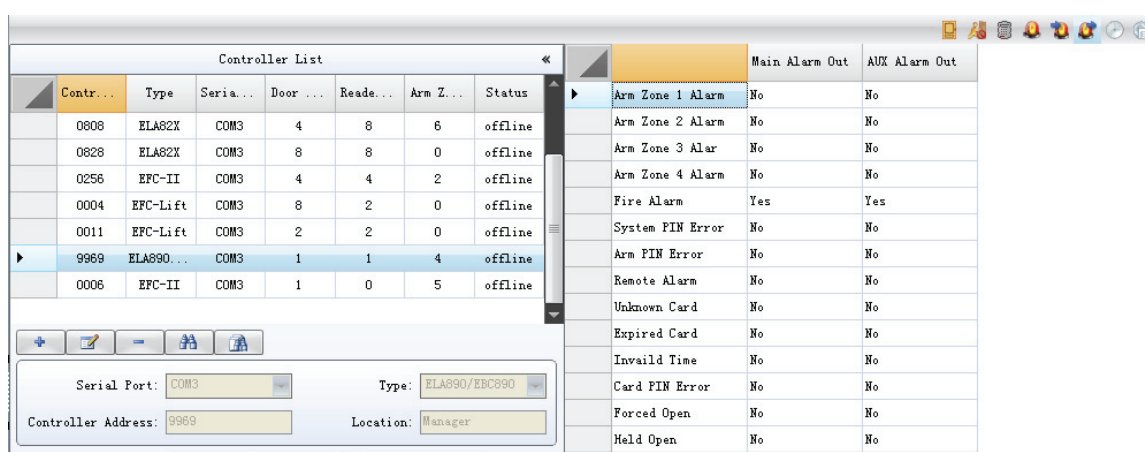


Fig. 5-19 Fingerprint Controller: Alarm Output Setting

✧ Flex Series Controller

An EFC-08-2A 8-door controller is used as an example here.

In the “sub function editing area” on the right, users can edit arm zone, fire alarm, system PIN fail, ARM PIN fail, remote alarm, unknown card, expired card, invalid card, invalid door,

invalid time, APB fail, card PIN fail, door forced open, door held open, reader lost and panic door open. Click “Save”  after editing each item (Fig. 5-20).

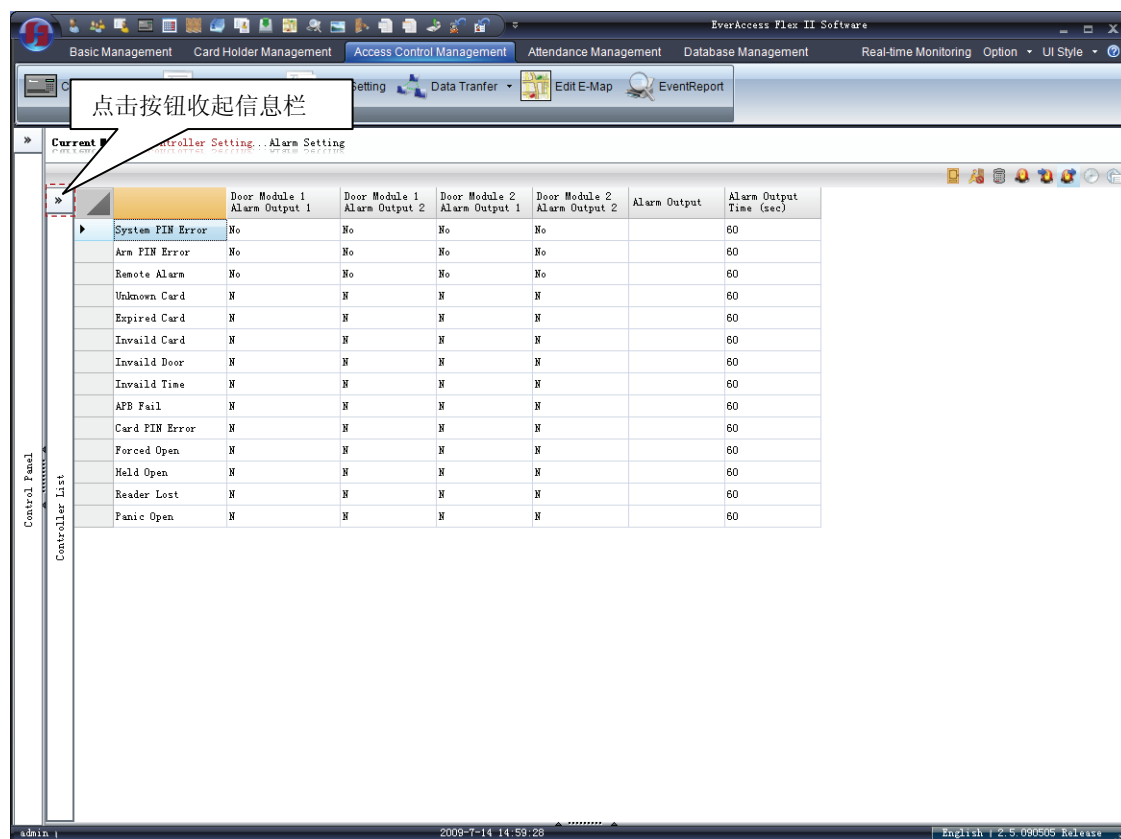


Fig. 5-20 Flex Series Controller: Alarm Output Setting

5.5.7 Alarm Output Time Setting

Select the controller from the controller list on the left, click “Alarm Output Time Setting” button . The list of alarm output times for the selected controller will be shown on the right.

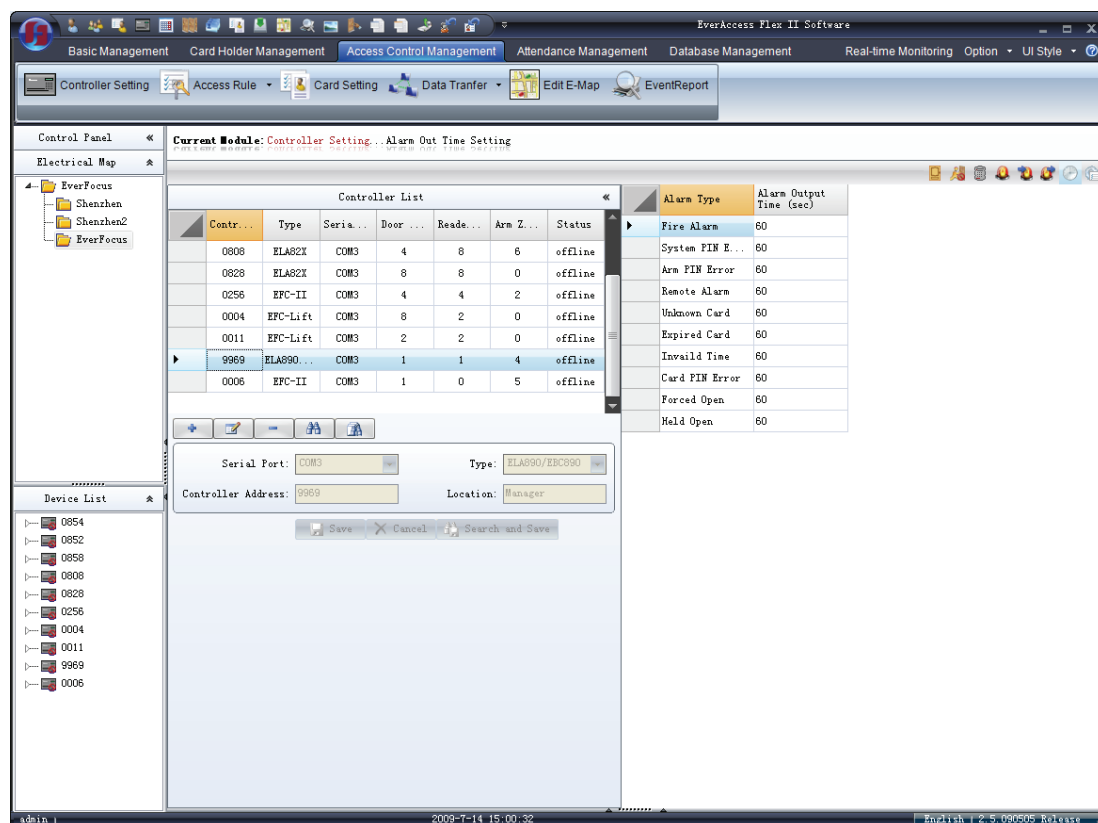


Fig. 5-21 Alarm Output Time Setting

The Alarm Output Time Setting Window for different controller types is listed below:

✧ Fingerprint Controller

An ELA890 fingerprint controller is used as an example here.

In the “sub function editing area” on the right, users can edit fire alarm, system PIN fail, ARM PIN fail, remote alarm, unknown card, expired card, invalid time, card PIN fail, door forced open and door held open. Click “Save”  after editing each item (Fig. 5-22).

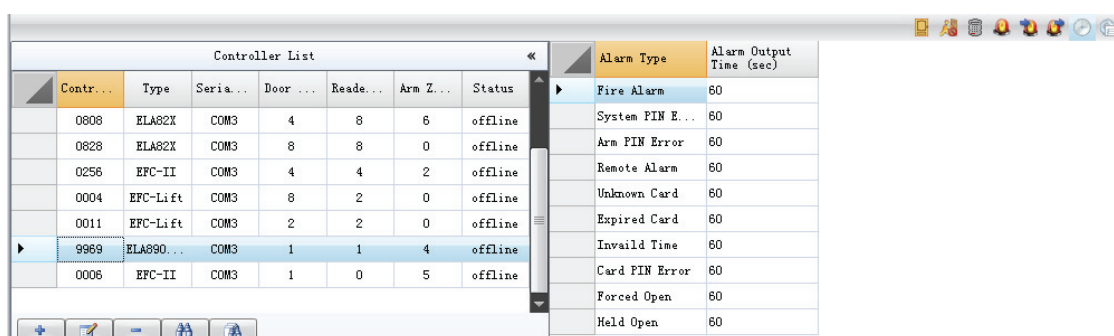


Fig. 5-22: Fingerprint Controller: Alarm Output Time Setting

✧ Flex I Series Controller

An EFC-08-1A 8-door controller is used as an example here.

In the “sub function editing area” on the right, users can edit arm zone, fire alarm, system PIN fail, ARM PIN fail, tamper alarm, remote alarm, unknown card, expired card, invalid card, invalid door, invalid time, APB fail, card PIN fail, door forced open, door held open, reader lost and panic door open. Click “Save”  after editing each item (Fig. 5-23).

5.5.8 System Setting

Select the controller from the controller list on the left, click “System Setting” button . The sub-functionalities of the selected controller will be shown on the right. Edit each sub-functionality in this field.

System Setting is for the overall setting of the controller. System setting includes overall APB, door behavior under APB; alarm input 0 type, First Card-In, arm delay time, time zone, and arm zone, door behavior under fire alarm, time synchronization server, date type and daylight saving time (Fig. 5-23).

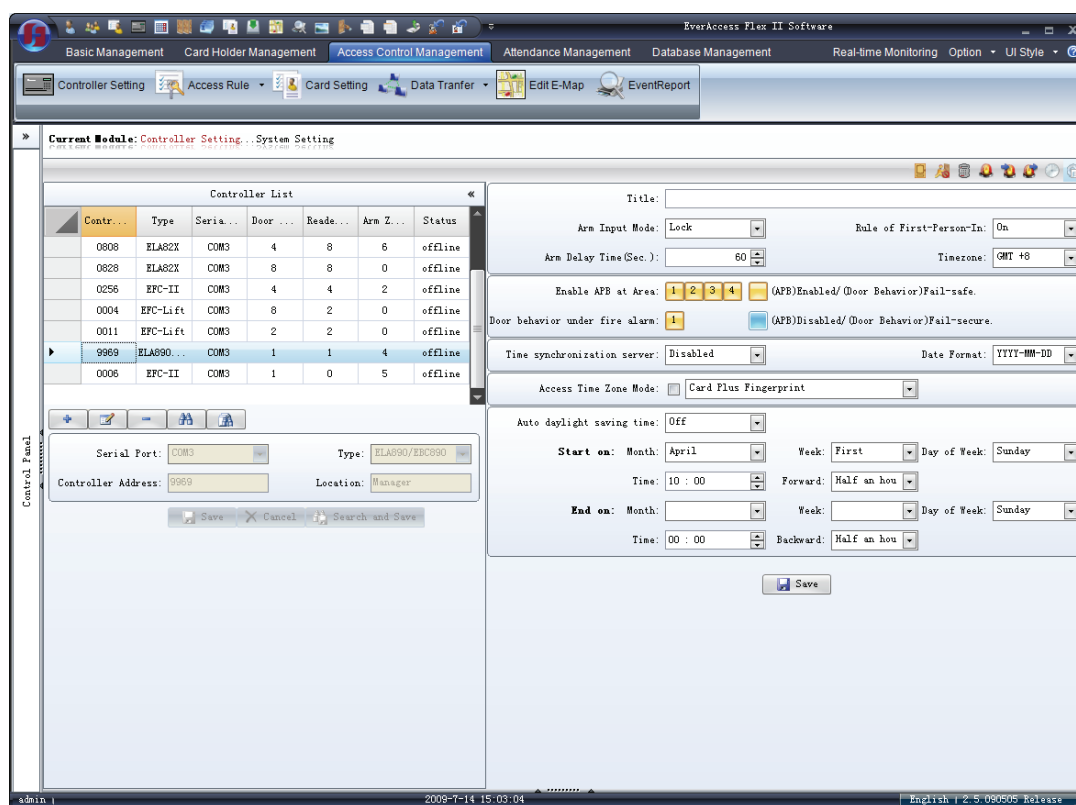


Fig. 5-23 System Setting

Overall APB: This setting applies to all readers connected to the current controller. Only when overall APB is enabled, individual APB setting can be enabled.

Door behavior under APB: The options are “door open” and “door lock”. This function is related to APB Fail event. When “door open” is selected, a cardholder may normally enter or exit doors under APB event. The system generates a granted access event record of

“enter/exit (APB fail)”. When “door lock” is selected, a cardholder cannot enter or exit doors under APB event. The system generates a denied access record of “APB”.

Alarm input 0 type: choose from Normally Open or Normally Close. This setting applies to alarm input 0 on the main module. Alarm input signal is controlled by an external alarm input device.

First Card-IN: choose from enabled or disabled. When First Card-in is enabled, in a door zone of which the schedule is set as “normally open”, only after a First Card enabled card has been presented to the reader, will other cards be able to unlock the door.

Arm delay time: When an arm operation is executed, all active arm zones will enter ARM enabled status only after a certain time delay called “arm delay time”. This time period is for the administrator who arms the system to leave the arm zone without triggering an alarm. Arm delay time is in the range 1~59999 seconds. Users can use button  to change the time or enter the time directly. Also, when an ARM enabled card is presented to the reader, the cardholder can enter or exit the arm zone during the arm delay time without triggering an alarm.

Time zone: Choose based on the time zone where the controller is located.

Arm zone: The arm zones are listed according to the selected controller. Click the arm zone button to change its status.  Indicates the arm zone is valid and  indicates the arm zone is invalid. An arm zone can be armed only when it is a valid arm zone.

Door behavior under fire alarm: The controller allows users to choose which doors to open and close during a fire alarm. “Open under fire alarm” means the door is automatically opened during a fire alarm and “Close under fire alarm” means the door is closed during a fire alarm. Click the door button to change its setting.  Indicates the door is opened under fire alarm and  indicates the door is closed under fire alarm.

Time synchronization server: indicates whether the controller is the time synchronization server in the system. All controllers in the system will automatically adjust their 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 settings. If the controller is connected to a PC with Flex software installed, 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 formats: “YYYY-MM-DD” and “MM-DD-YYYY” and users can choose the desired format.

Daylight saving time: Choose whether auto Daylight Saving Time (DST) is enabled. When auto DST is enabled, users need define the start and end dates for DST, including month, week, date, and time, forward or backward. When auto DST is enabled, the controller will default to automatically adjusting DST one hour forward from 1:59:59am to 3:00:00am on the first Sunday in April, and adjusting it backward one hour from 1:59:59am to 1:00:00am on the last Sunday in October.

The System Setting Window for different controller types is listed below:

✧ ELA82X Series Controller

An ELA808 4-door controller is used as an example here (Fig. 5-24).

In the “sub function editing area” on the right, users can edit time zone. Click “Save”  after editing the item.

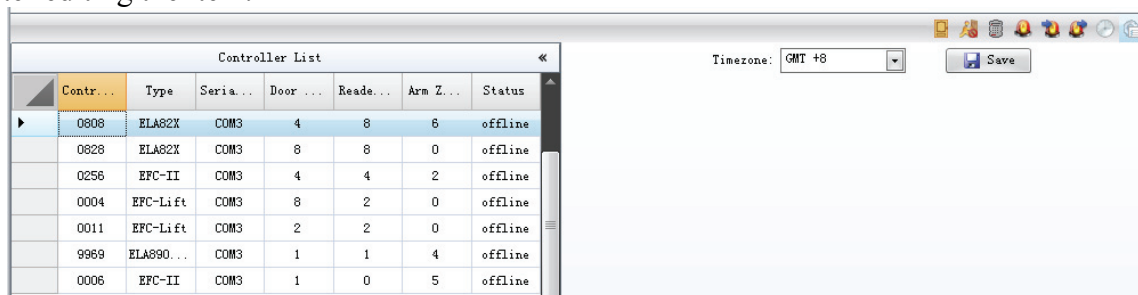


Fig. 5-24 ELA82X Series Controller: System Setting

✧ ELA85X Series Controller

An ELA858 8-door controller is used as an example here (Fig. 5-25).

In the “sub function editing area” on the right, users can edit time zone, arm delay time, arm zone, date format and door sensor status. Click “Save”  after editing each item.

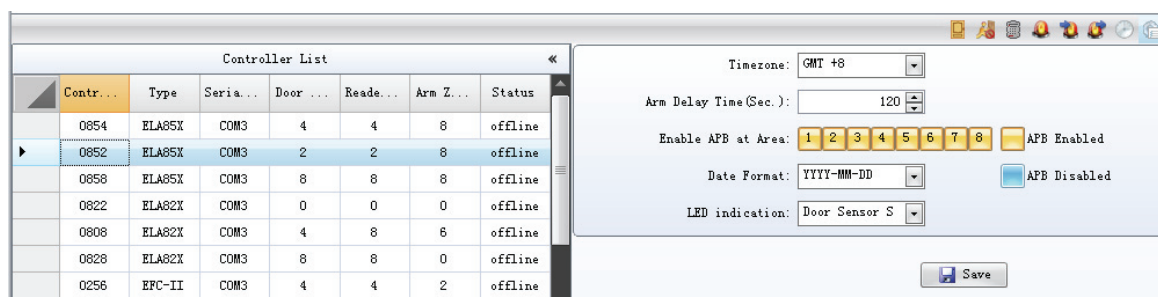


Fig. 5-25 ELA85X Series Controller: System Setting

✧ Fingerprint Controller

An ELA890 fingerprint controller is used as an example here (Fig. 5-26).

In the “sub function editing area” on the right, users can edit title, time zone, date format, time synchronization server, arm delay time, arm zone, First Card-in, door behavior under fire alarm, time zone mode, time zone setting mode and auto daylight saving. Click “Save”  after editing each item.

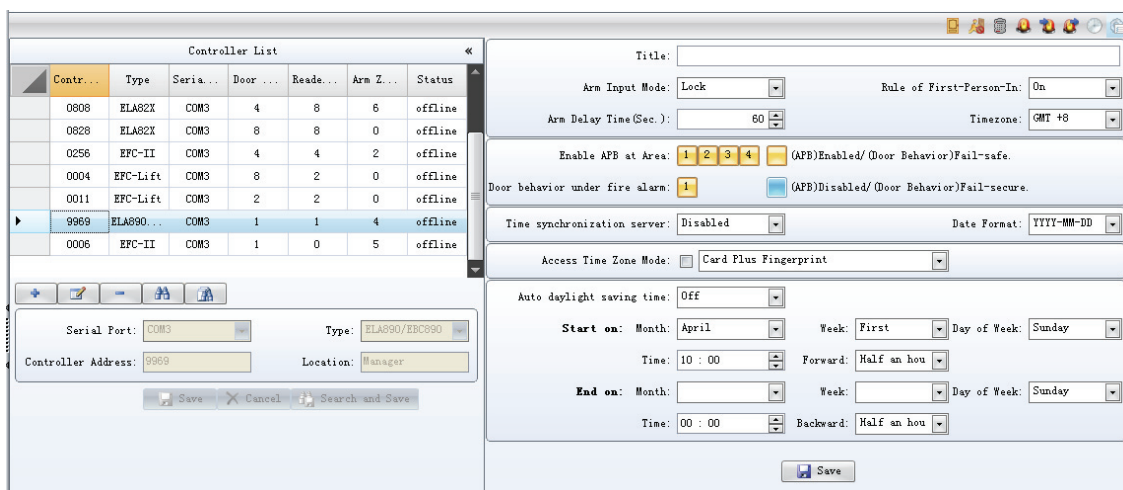


Fig. 5-26 Fingerprint Controller: System Setting

✧ Flex I series Controller

An EFC-02-1A 2-door controller is used as an example here (Fig. 5-27).

In the “sub function editing area” on the right, users can edit time zone, date format, time synchronization server, arm delay time, arm zone, First Card-in, door behavior under fire alarm and auto daylight saving. Click “Save”  after editing each item.

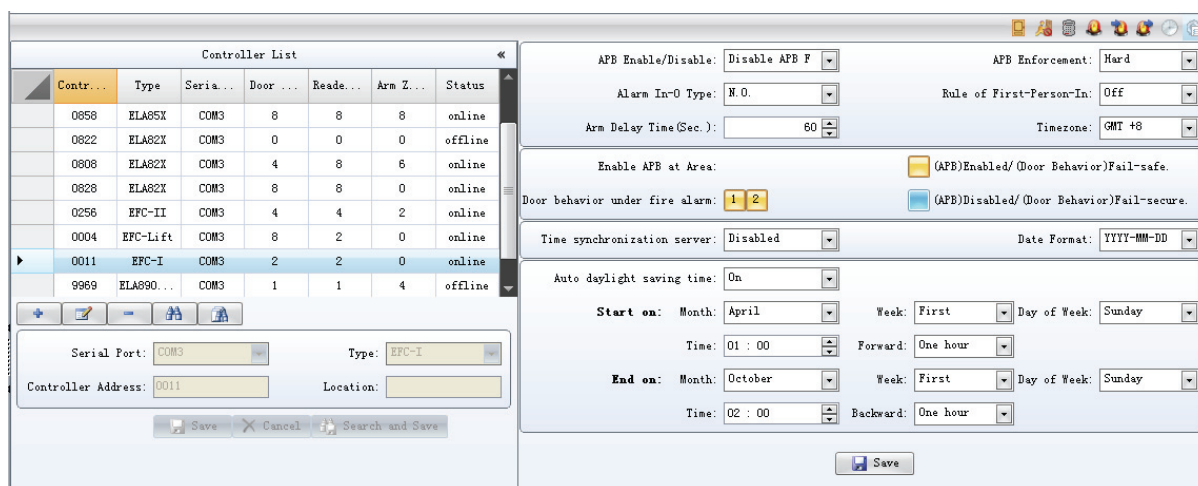


Fig. 5-27 Flex I Series Controller: System Setting

✧ Flex II series Controller

An EFC-08-2A 8-door controller is used as an example here (Fig. 5-28).

In the “sub function editing area” on the right, users can edit time zone, date format, time synchronization server, First Card-in and daylight saving time. Click “Save”  after editing each item.

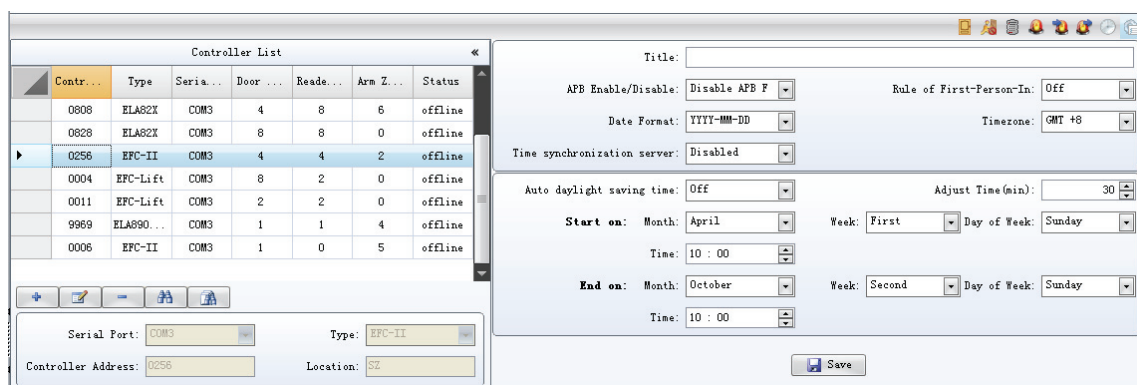


Fig. 5-27 Flex II Series Controller: System Setting

✧ EFC Series Elevator Controller

An EFC-08-lift 8-floor elevator controller is used as an example here (Fig. 5-28).

In the “sub function editing area” on the right, users can edit time zone. Click “Save”  after editing the item.

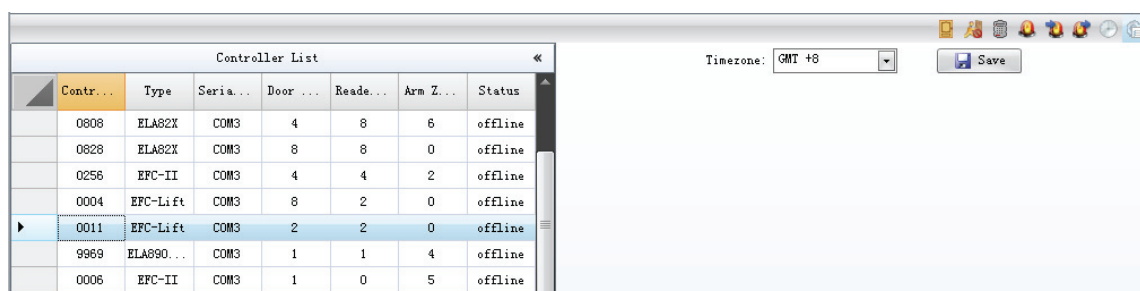


Fig. 5-29 EFC Series Elevator Controller: System Setting

Chapter

6

6 Access Rules

6.1 Date Setting

Click “Access Control Management” → “Access Rule” → “Date Setting” to open the window for date setting (Fig. 6-1).

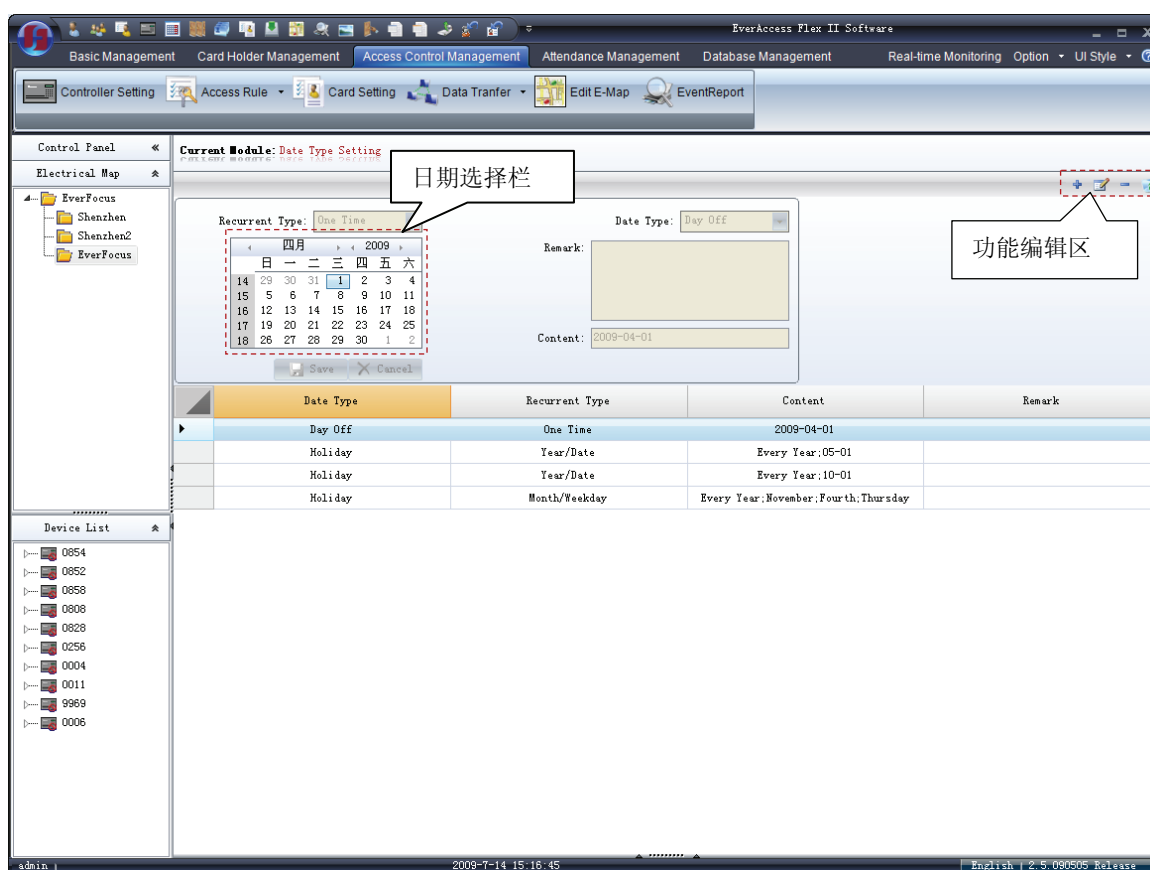


Fig. 6-1 Date Setting

6.1.1 Date Type

There are 3 types of dates defined in the Software: legal holiday, day off and floating holiday. Users can customize date type settings according to their needs. “Floating holiday” has the highest priority in the system, followed by “day off” and finally “legal holiday”.

Legal holiday: refers to the holidays authorized by law or custom

Day off: can be recurrent date types, such as a company anniversary

Floating holiday: a temporary occurrence, such as a company organized travel event.

6.1.2 Recurrent Type

There are three recurrent types defined in the software: one-time holiday, date holiday and day of week holiday. Users can customize the setting according to their needs.

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.

6.1.3 Add a Date

Click the “Add” button  in the “function editing area” to open the window for adding a date (Fig. 6-2). In the “Date selection field” on the left, select year, month and date. Click the “forward”  or “backward”  button beside “year” and “month” to select year and month, and click the date in the field to select a date. The selected date will be highlighted in yellow . Click the triangle button  at the right of “date type” and “recurrent type” to open a drop-down menu to select the corresponding date type and recurrent type. Remarks can be added for easy viewing and management. After setting each item, click the “save” button  and a dialog box reporting “Operation succeeded” will pop up.

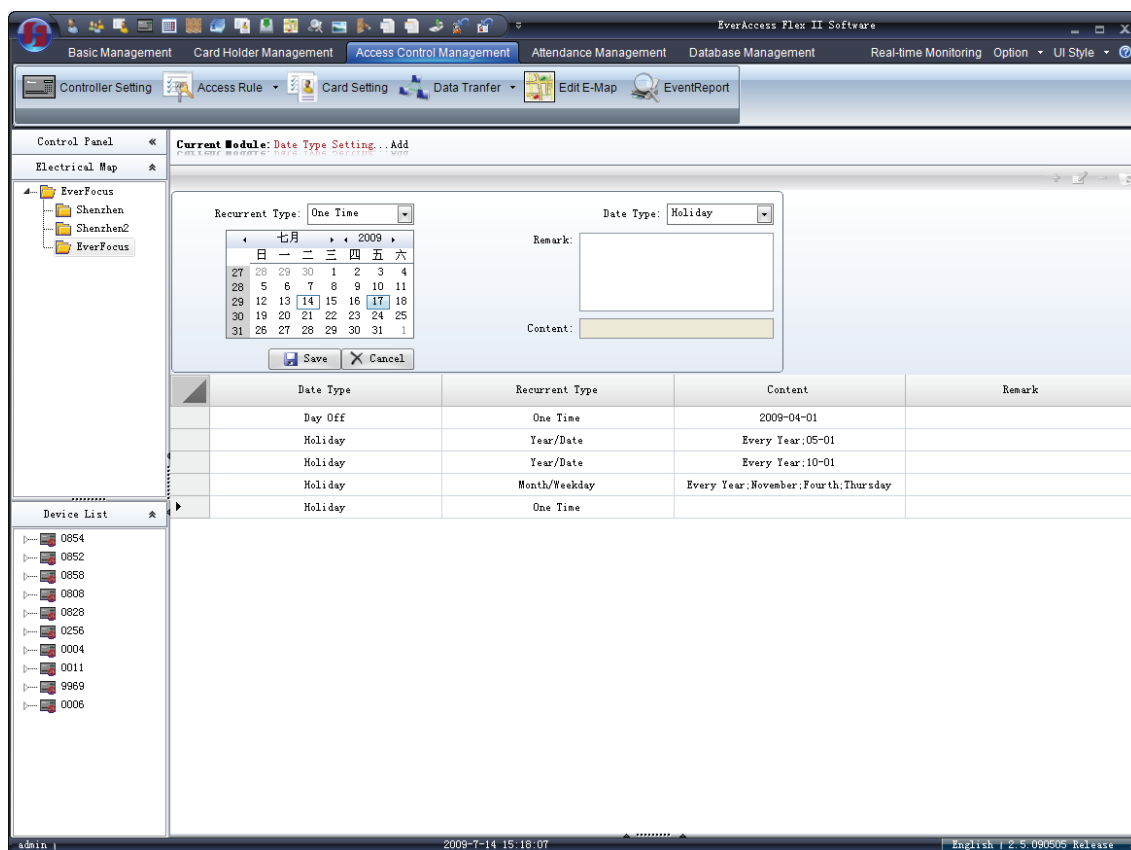


Fig. 6-2 Add a Date

6.1.4 Edit a Date

Select the date to be edited from the date list, click the “Edit” button  in the “function editing area”. Users can edit date type, recurrent type, date and remarks. When finished, click the “Save” button  and a dialog box reporting “Operation Succeeded” will pop up.

6.1.5 Delete Date(s)

6.1.5.1 Delete a Date

Under the “Date Setting” window (Fig. 6-1), drag the mouse across the date list to select multiple adjacent dates, or use the “Ctrl” key on the keyboard to select nonadjacent dates. After selecting the dates to be deleted, click the “Delete”  button in the “Function editing area”. A dialog box will be shown to prompt users to confirm the deletion. Click “Yes” to delete the date and another dialog box reporting “Operation succeeded” will be shown. Otherwise, click “Cancel” to exit.

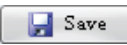
6.1.5.2 Delete All Dates

Under the “Date Setting” window (Fig. 6-1), click the “Delete All”  button in the “Function editing area”. A dialog box will be shown to prompt users to confirm the deletion.

Click “Yes” to delete all dates and a dialog box reporting “Operation succeeded” will be shown. The number of deleted dates will also be shown in the dialog box. Otherwise, click “Cancel” to exit.

6.2 Door Setting

Click “Access Control Management” → “Access Rule” → “Door Setting” to open the window for door setting.

Select a controller in the controller list on the left, and contents of door setting of the selected controller will be shown on the right, which includes door No., door location and door schedule (Refer to section 6.3 Door Schedule Setting for details on door schedule). The system default door schedule for all doors is “Default”. The system default verification level for all doors is “Card” (Refer to section 6.3.5 edit a Door Schedule for details on verification level). Under “Schedule Name”, select the desired door schedule from the drop-down menu (Fig. 6.3). When finished editing door schedule, click “Save” button  and a dialog box reporting “Operation succeeded” will pop up.

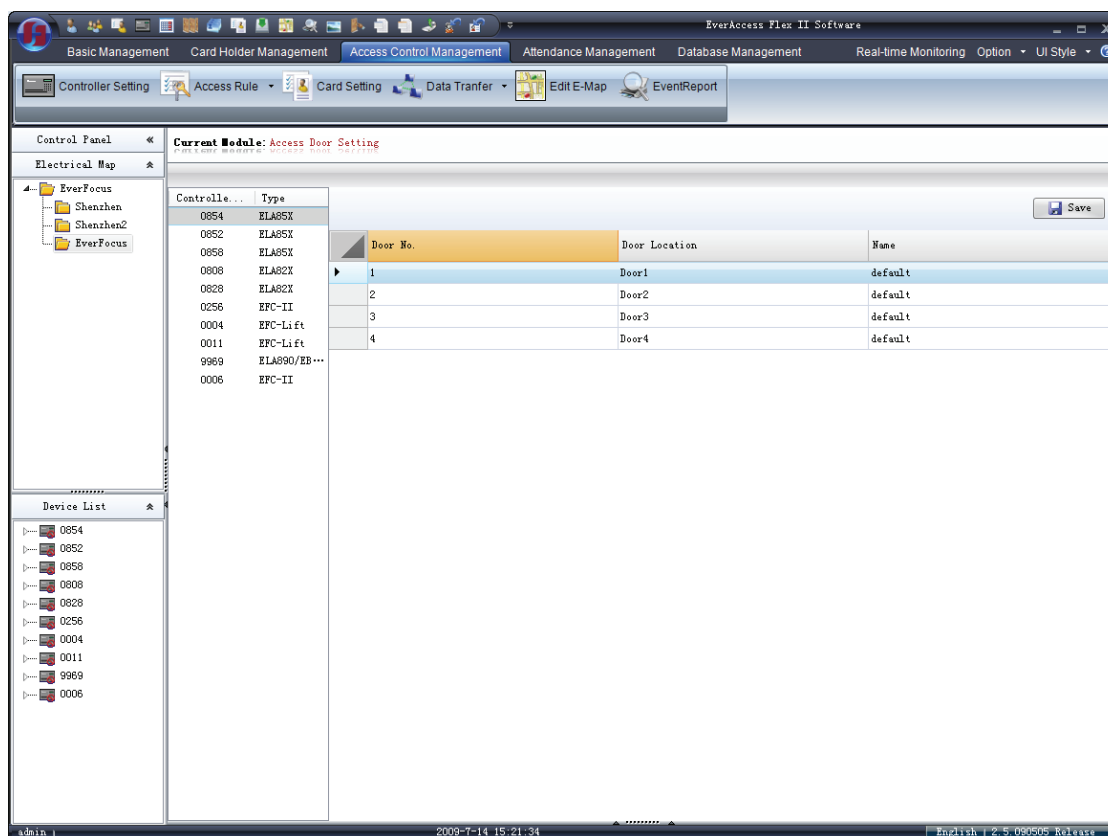


Fig. 6-3 Door Setting

If the controller is not connected to the computer, a dialog box reporting “Timeout when connecting to controller” will pop up. Click “Yes”, the setting will be saved to the database, but not to the controller. To update the controller, users need to download data to the controller manually after the controller is connected (Refer to section 8.2 Download data from Computer to Controller for details). The current setting will be applied only after the data is downloaded to the controller.

Note: The “Save” function applies only to those of which the door schedule is changed. This is illustrated in the following example. Suppose, a user wants to change door schedule for “Door 1” from “default” to “A”, but timeouts when connecting to controller, therefore the door schedule for “Door 1” is still “Default” on the controller. If the user does not change the door schedule for “Door 1” next time he enters the window, direct click “Save” will not change the setting for “Door 1”. In this situation, even the Software shows that “Door 1” is under schedule “A”, it is actually under schedule “Default” in the controller. One has to download the data to the controller manually to activate the new setting.

6.3 Door Schedule Setting

Click “Access Control Management” → “Access Rule” → “Door Schedule Setting” to open the window for door schedule setting (Fig. 6-4)

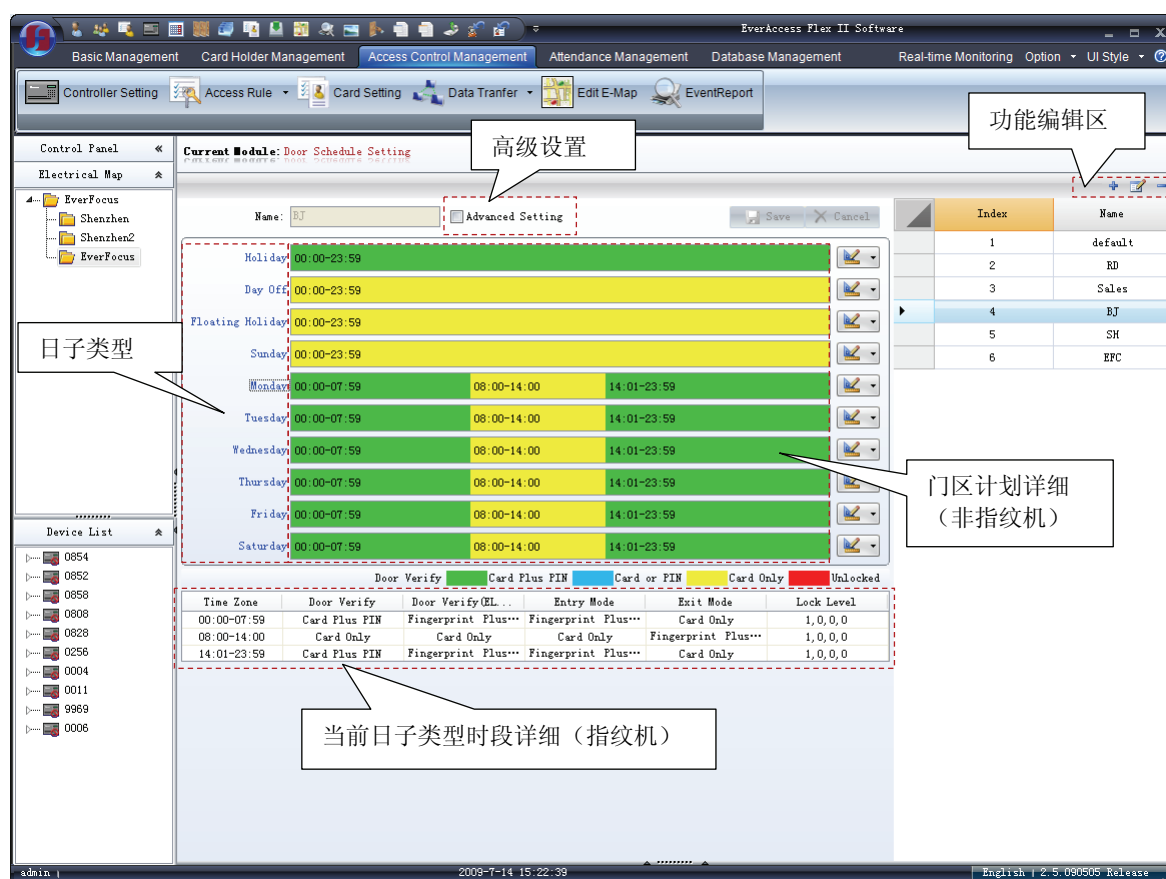


Fig. 6-4 Door Schedule Setting

In the detailed view of door schedule setting, each time zone is marked by start time, end time and verification level encoded by bars of different colors. If the start time and end time are not shown, place the cursor on top of the color bar and the time information will be shown.

Note: The default door schedule “Default” cannot be renamed, but user can edit its content.

6.3.1 Advanced Setting

For Flex II series controllers, user can choose different verification level for entry (In) and exit (Out). Check “Advanced Setting” on top of the page to open the window for advanced setting (Fig. 6-5).

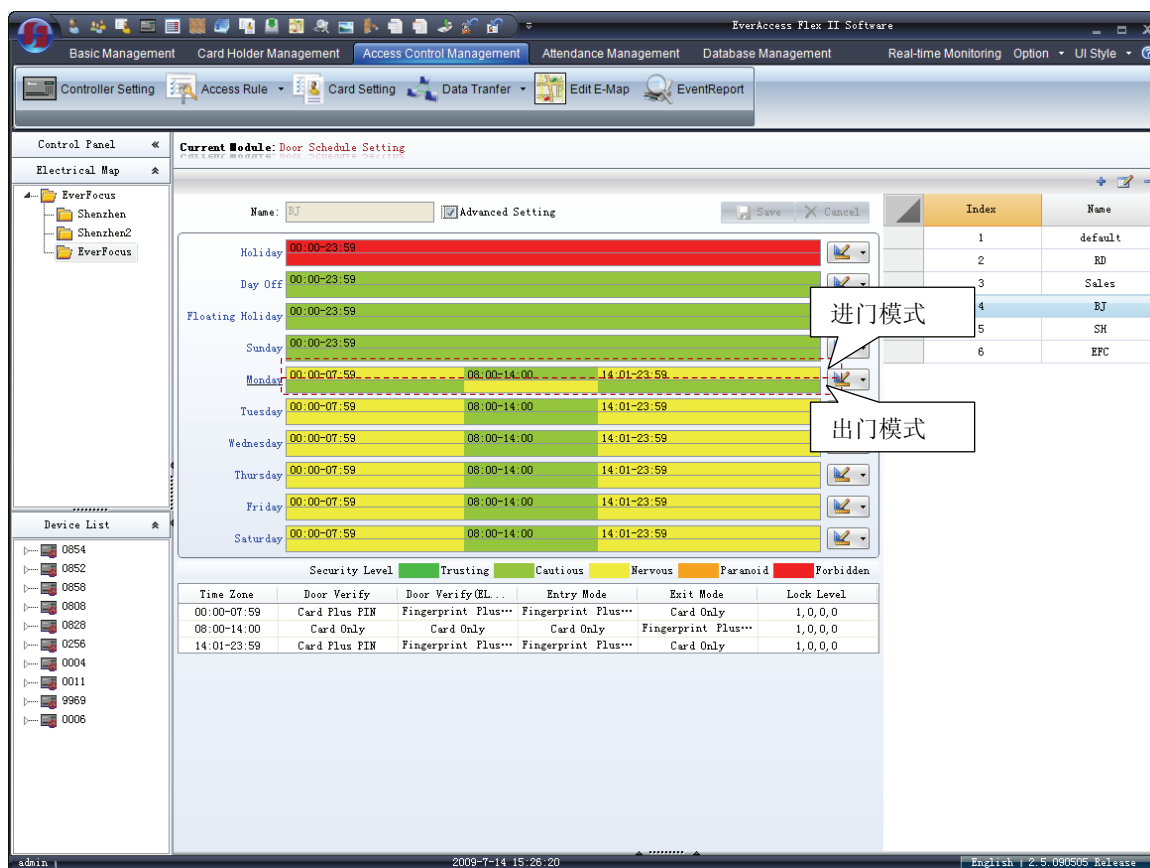


Fig. 6-5 Advanced Setting

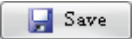
Each date is divided to two parts with the upper part corresponding to “In” and the lower part corresponding to “Out”.

6.3.2 Add a Door Schedule

Click the “Add” button  in the “function editing area”, and enter the name of the door schedule in the field of “Schedule Name”. Click “save” button  and a dialog box reporting “Operation succeeded” will pop up. Schedule name must be unique.

6.3.3 Rename a Door Schedule

Select the door schedule to be renamed in the schedule list, click the “Edit” button  in the “function editing area”, and enter the new name in the field of “Schedule Name”. Click

“save” button  and a dialog box reporting “Operation succeeded” will pop up. Schedule names must be unique.

Note: The default door schedule “Default” cannot be renamed.

6.3.4 Delete a Door Schedule

Select the door schedule to be deleted in the schedule list, and click the “Delete” button  in the “function editing area”. A dialog box will be shown to prompt users to confirm the deletion. Click “Yes” to delete the door schedule.

Note: The default door schedule “Default” and door schedules that have been assigned to a controller cannot be deleted.

6.3.5 Edit a Door Schedule

The Software provides two setting modes: door verification and advanced setting. ELA82x, ELA85X, EFC-I series controller can only be configured in the door verification setting. Flex II series and fingerprint controllers support advanced setting in which different verification levels can be chosen for entry and exit.

For each door schedule, there are 10 date types that belong to either special types or normal types. Special types include legal holiday, day off and temporary change; Normal types include Monday to Sunday. Each date type can be divided into multiple time zones and different verification levels can be assigned to each time zone.

Note: The maximum number of time zones is 10 for each date type. The minimum duration of each time zone is 1 minute for Flex II series controller and 5 minutes for other types of controller.

6.3.5.1 Labeling for Door Verification

The Software offers 4 different levels for door verification:  Unlocked (red);  Card or PIN (blue);  Card (yellow);  Card plus PIN (green). The default verification level is “Card”.

6.3.5.2 Labeling for Advanced Setting

There are 5 types of security level in the advanced setting windows:  trusting (green);  level 1 (light green);  level 2 (yellow);  level 3 (orange);  No permission (red). The default verification level is level 1.

5 types of security level:

 Trusting: unlocked

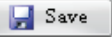
 Level 1: one item required for verification, such as Card

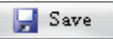
■ Level 2: two items required for verification, such as Card plus PIN or Card plus fingerprint

■ Level 3: three items for verification, such as Card plus PIN Plus Fingerprint

■ No permission: no access permitted

6.3.5.3 Add/Edit Door Verification

To add: In the door schedule editing window (Fig. 6-8), click the “Add” button , and select the verification level, start and end time. Click “save” button  to save the new Time zone.

To edit: select the time zone from the list on the left, click “Edit”  to modify. After editing, click “Save” .

The Software will automatically divide or combine time zones according to the users’ settings. For example, if an added time zone “13:00-14:00” is set to “unlocked” and the time zone “15:00 –16:00 is edited to be “Card Plus PIN”. The new time zone is shown as in Fig. 6-6.

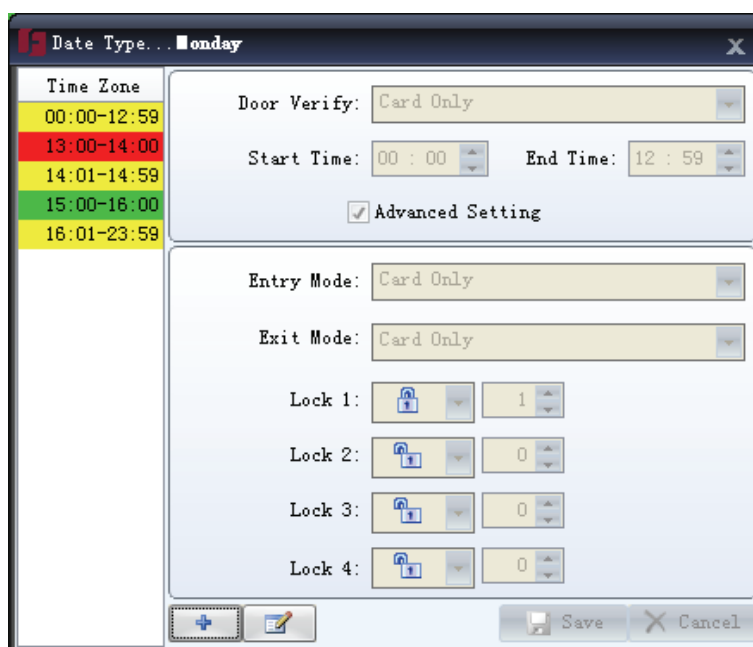


Fig. 6-6 Edit “Monday” Time Zone

Note: Using a Flex I controller as an example, the minimum time zone duration is 5 minutes. The system default start time of each time zone is 00s and the end time is 59s. Therefore, for the time zone 9:00-18:00, the system treats the time zone as 9:00:00-18:00:59. If editing a time zone makes a time zone duration less than 5 minutes, the system will automatically combine this time zone to the time zone that follows it until the combined time zone is longer than 5 minutes; If the start time of a time zone is later than 23:54, the system will combine it with the time zone that proceeds it until the combined time zone is longer than 5 minutes.

6.3.5.4 Advanced In/Out Setting

If different verification level is required for entry (In) and exit (Out), check “Advanced Setting” in the window. Select “In” type and “out” type individually from the drop-down

menu. If the controller is a fingerprint controller, the system offers 13 types of verification levels. Click “Save”  Save after editing.

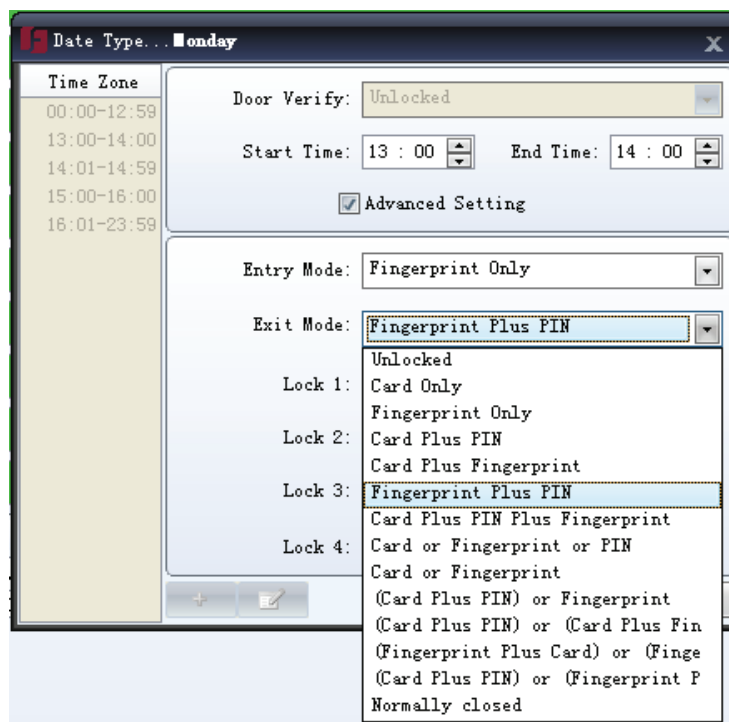


Fig. 6-7 Advanced In/Out Setting

If a door schedule has been assigned to a door zone, the system will automatically update the controller setting when a time zone is added or edited. If the controller is offline, the user needs to download the data to the controller manually.

6.3.5.5 Advanced Unlock Level Setting

Under “Door Schedule Setting” window (Fig. 6-4), select a door schedule from the list on the right, and the detailed setting of the selected door schedule will be shown on the left. Click “Edit” , and the door-schedule editing window will pop up (Fig. 6-8).

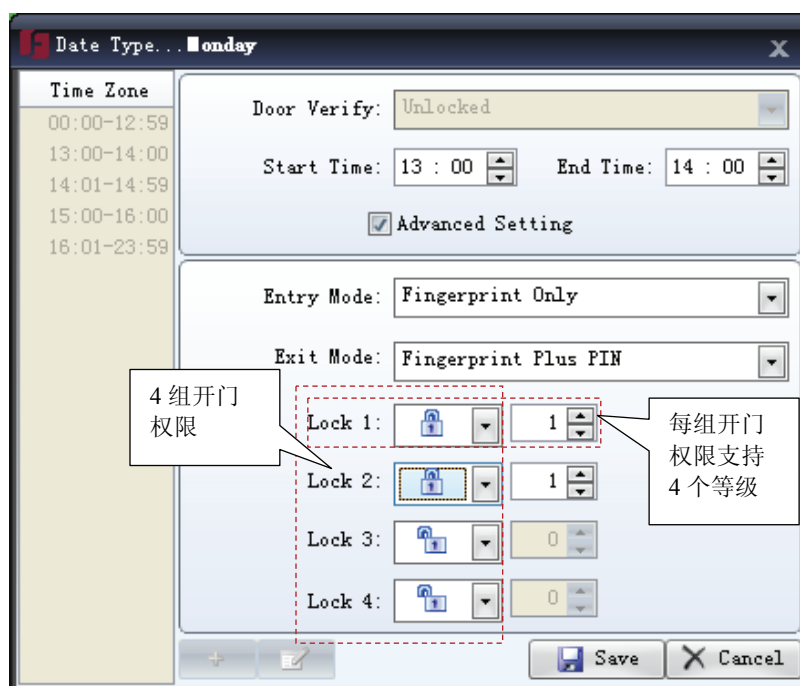


Fig. 6-8 Monday Time Zone Setting

Users can choose different verification levels for entry (In) and exit (Out) by checking “Advanced Setting”. If a fingerprint controller is used, the system offers 13 types of verification levels.

“Lock” here indicates the access authority that can be assigned to each door. Each door can be assigned up to 4 groups of access authority and each access authority supports up to 4 levels. In other words, a door can have 4 locks and each lock can have 4 keys. The related setting is described in “Access Group Schedule Setting”. Refer to 6.4.4 Edit Access Group for details.

For example, if a door is assigned to 4 access authorities (4 locks) and each lock has 4 levels, suppose each cardholder in an access group has authority level 1; then 16 cards have to be presented to the reader successively before the door can be opened.

Note: Only Flex II series controllers support different verification levels for “In” and “Out”.

6.3.5.6 Door Setting and Conversion for Fingerprint Controllers

Note: Users can choose only one setting mode, either “Door Verification” or “Advanced Setting” by checking the box labeled “Advanced Setting”. The conversion between these two settings is described below. Different setting modes can be applied to different time zones with the same date type.

Under “Door Verification” mode, when a door schedule is applied to non-fingerprint controllers, the selected verification level is used as the verification level for door access; when a door schedule is applied to fingerprint controllers, conversion for fingerprint controllers is needed, as described in the table below.

Door Verification (non-fingerprint controllers)	Advanced Setting (fingerprint controllers)
Card	Card
Card Plus PIN	Card Plus PIN Plus fingerprint
Card or PIN	Card or PIN or fingerprint
Unlocked	Unlocked

Table 6-1 Conversion of verification levels for fingerprint controllers

Under “Advanced Setting” mode, when a door schedule is applied to fingerprint controllers, the selected verification level is used as the verification level for access; when a door schedule is applied to non-fingerprint controllers, the conversion for non-fingerprint controllers is described in the table below.

Advanced Setting (fingerprint controllers)	Door Verification (non-fingerprint controllers)
Card	Card
Fingerprint	
Card Plus PIN	Card Plus PIN
Card Plus Fingerprint	
Fingerprint Plus PIN	
Card Plus PIN Plus fingerprint	
(Card Plus fingerprint) or PIN	
(Card Plus PIN) or (Card Plus Fingerprint)	
(Fingerprint Plus Card) or (Fingerprint Plus PIN)	
(PIN Plus card) or (PIN Plus Fingerprint)	
Card or PIN or Fingerprint	Card or PIN
Card or Fingerprint	
Unlocked	Unlocked

Table 6.2 Conversion of verification levels for non-fingerprint controllers

6.3.6 Quick Door Schedule Setting

If the time zone setting among different date types under a door schedule is the same, users can copy and paste the time zone settings by clicking the  button on the right of the “Edit” button  (Fig. 6-9). Users can also copy and paste time zone settings between different door schedules. The copy and paste function is valid as long as one entry remains in the door schedule setting window.

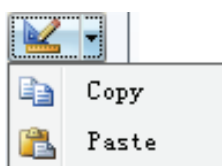


Fig. 6-9 Copy and Paste

6.3.7 View Details of a Door Schedule

Select a door schedule from the list on the right, and the details for non-fingerprint controllers of each date type under the selected door schedule will be shown on the left panel. Click on the name of a date type, such as Thursday, and the details for fingerprint controllers of the selected date type will be shown at the lower panel (Fig. 6-10). When selecting a door schedule, the details of “Legal Holiday” will be shown at the lower panel by default.

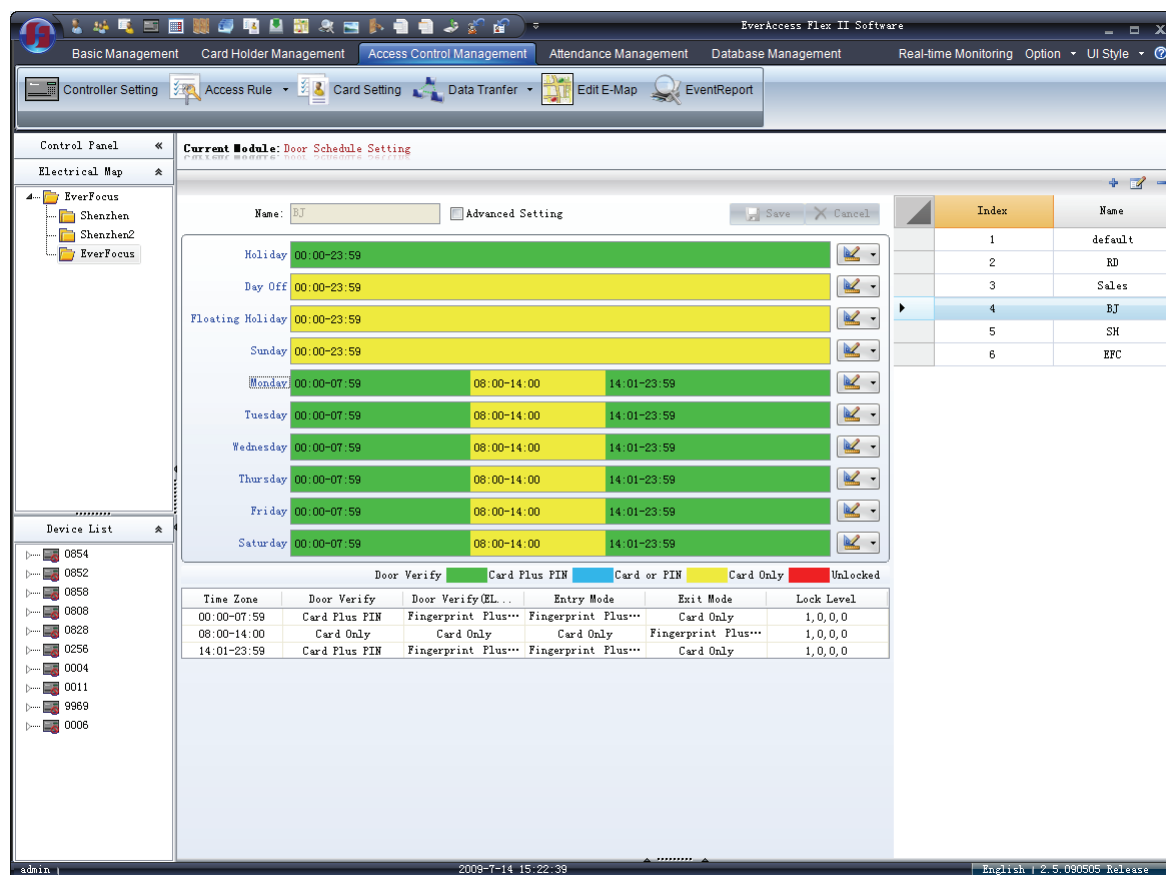


Fig. 6-10 View Details of a Door Schedule

6.4 Access Group Setting

Click “Access Control Management” → “Access Rule” → “Access Group Setting” to open the window for access group setting (Fig. 6-11).

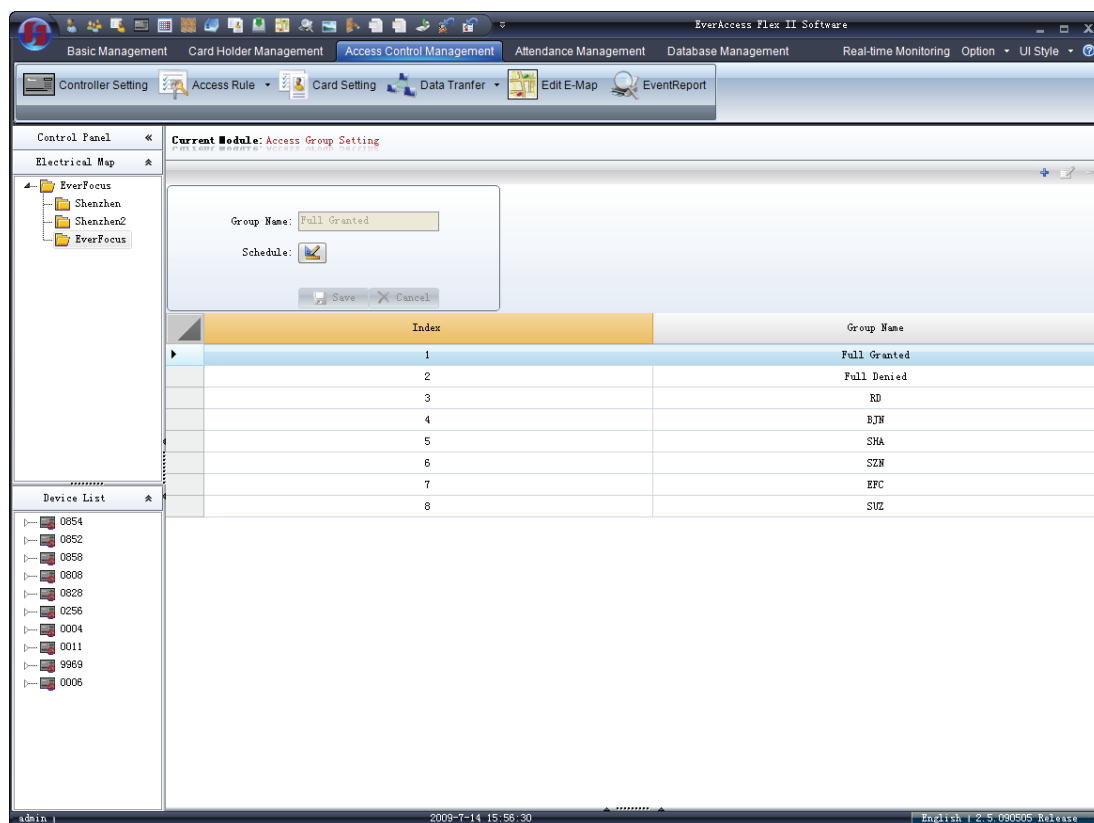


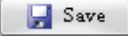
Fig. 6-11 Access Group Setting

Note: There are two default access groups defined in the Software: access group “Full Granted”, which is authorized to all controllers, and access group “Full Denied”, which is unauthorized to all controllers.

“Full Granted”: cards in the access group “Full Granted” are authorized to all controllers. A card will be enrolled to all valid controllers if it is assigned to access group “Full Granted”. In the event log of the main window, the quick added cards belong to this group (Refer to section 2.3.8). In addition, when importing card information, if the access group to which the card belongs cannot be found in the Software, the card will be assigned to “Full Granted” (Refer to section 13.4.2 Importing Card Information).

“Full Denied”: cards in the access group “Full Denied” are unauthorized to all controllers. A card will not be enrolled to any valid controllers if it is assigned to access group “Full Denied”. If a card is not to be used in the system right away, the card can be assigned to “Full Denied”.

6.4.1 Add an Access Group

Click the “Add” button  in the “function editing area”, and enter the name of the access group in the field of “Group Name”. Click “save” button  and a dialog box reporting “Operation succeeded” will pop up. Schedule names must be unique.

6.4.2 Rename an Access Group

Select the access group to be renamed in the group list, and click the “Edit” button  in the “function editing area”. Enter the new name in the field of “Group Name”. Click “save” button  and a dialog box reporting “Operation succeeded” will pop up. Access group names must be unique.

Note: The two default access groups cannot be renamed.

6.4.3 Delete an Access Group

Select the access group to be deleted in the group list, and click the “Delete” button  in the “function editing area”. A dialog box will be shown to prompt users to confirm the deletion. Click “Yes” to delete the access group.

Note: The two default access groups and any access groups that contain cards cannot be deleted.

6.4.4 Edit an Access Group

Select the access group to be edited in the group list, click “Edit”  and the access group editing window will pop up (Fig. 6-12). In the window, user can edit the corresponding controller group and the access group schedule for each door zone (Refer to section 6.5 Access group schedule setting for details).

Note: The Software supports a maximum of 2048 groups. Controllers other than the Flex II series controllers support a maximum of 64 groups. As a result, the controller group and the Software group may not be a one-to-one match. Except for the default access group, the Software will display the corresponding relationships between the controller group and the Software group.

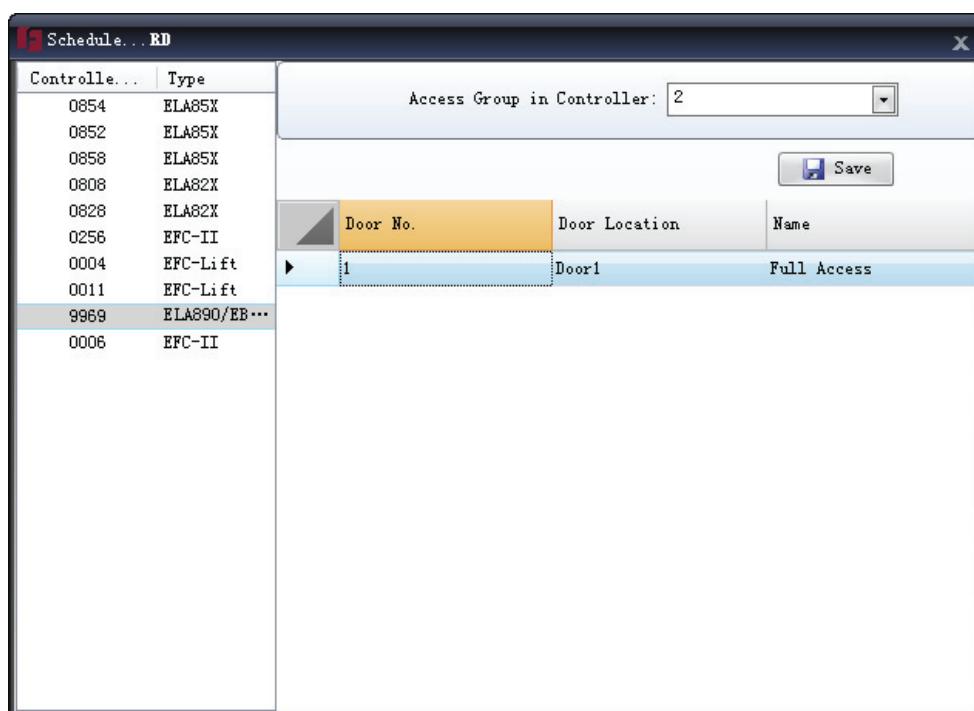


Fig. 6-12 Edit Access Group Schedule

The default access group “Full Granted” can only be viewed, but cannot be edited (Fig. 6-13). Specifically, the corresponding controller group is “1” for all controllers; the door schedule is “Full Access” for all door zones; the access permission is “Entry/Exit” (Refer to section 6.5)

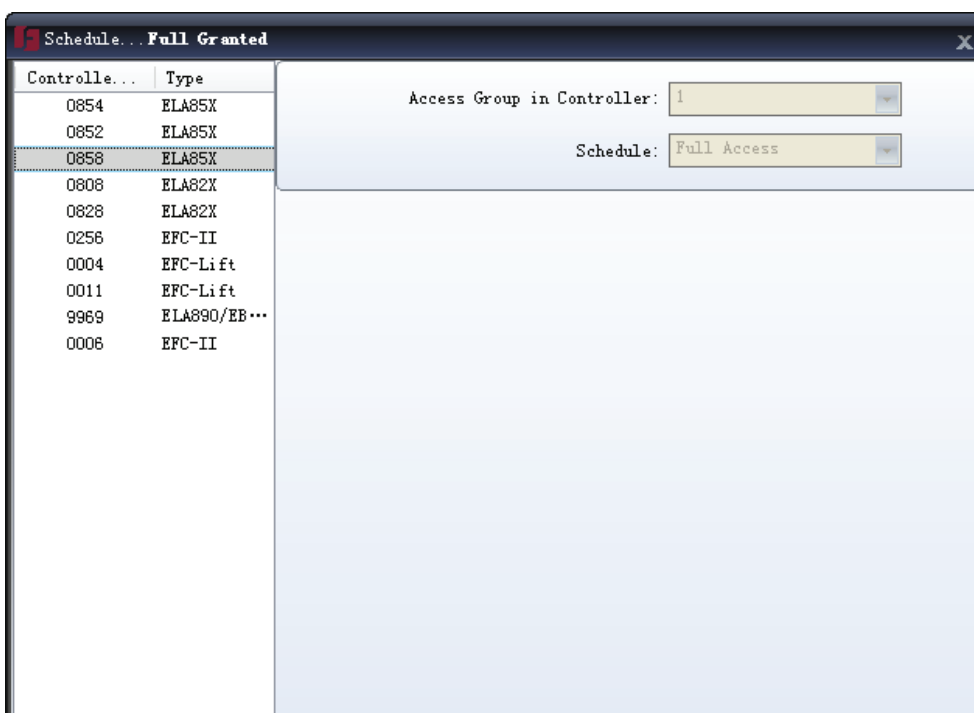


Fig. 6-13 Access Group “Full Granted”

The default access group “Full Denied” can only be viewed, but cannot be edited (Fig. 6-14). Specifically, the corresponding controller group is “Unauthorized” for all controllers; the

door schedule is “Full Access” for all door zones; the access permission is “No Entry/No Exit” (Refer to section 6.5)

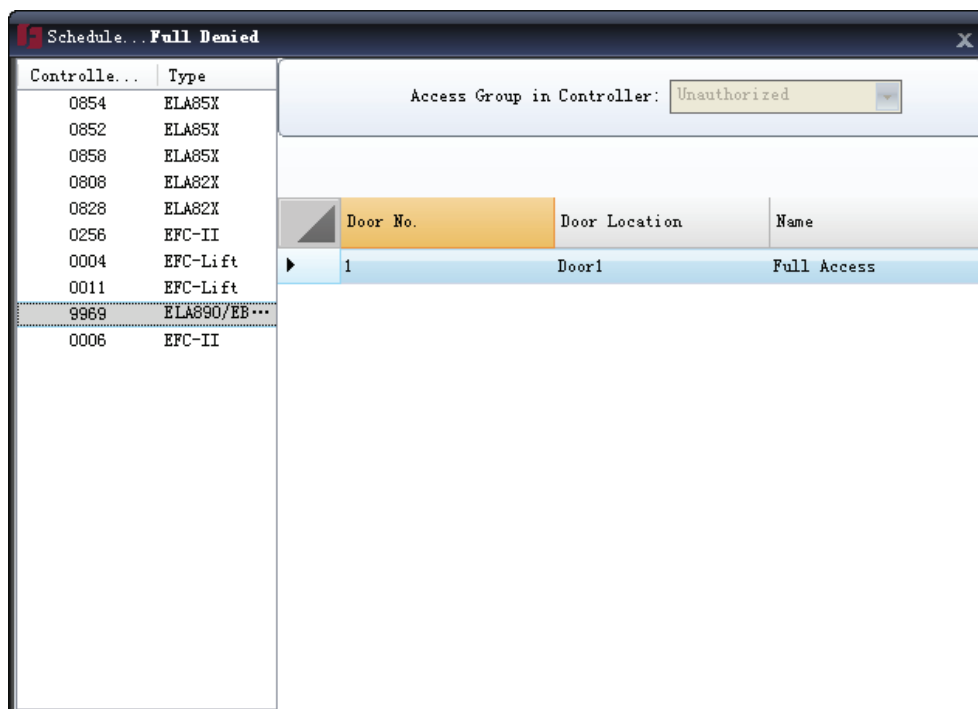


Fig. 6-14 Access Group “Full Denied”

Under the access group editing window, select a controller from the controller list on the left, and the content of access group schedule will be shown on the right, which includes the corresponding controller group, Door No., Door location and Access group schedule. There are two types of corresponding controller groups: Authorized (group 2-64, group 1 is preset as the default access group “Full Granted” for all controllers) and Unauthorized. If “unauthorized” is selected, the cards in the access group will not be enrolled to the corresponding controller and the access group schedule cannot be edited. If the selected controller group has been assigned to another access group in the Software, the system will prompt users to confirm whether to replace the previous setting for the Software access group (Fig. 6-15)

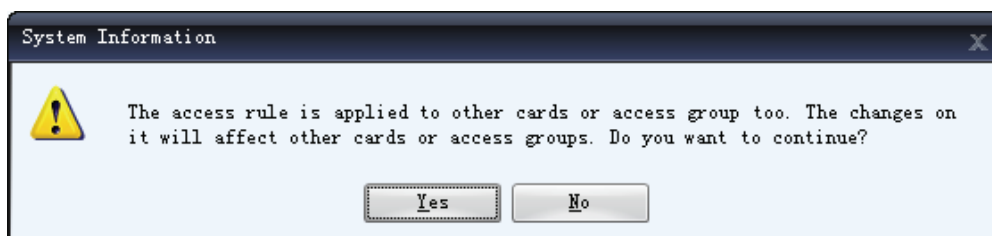


Fig. 6-15 Replace previous setting

This is illustrated in the following example. Suppose there are two access groups in the Software, Group A and Group B. The corresponding controller group for Group A on controller 0858 is “10”. When editing access group schedule for Group B on controller 0858, if the corresponding controller group is set to “10”, the system will prompt users to confirm whether to replace the access group schedule for Group A. Select “Yes” and the access group

schedule for Group A on controller 0858 will be replaced to be the same as that for Group B. The process is shown in Fig. 6-16, 6-17 and 6-18.

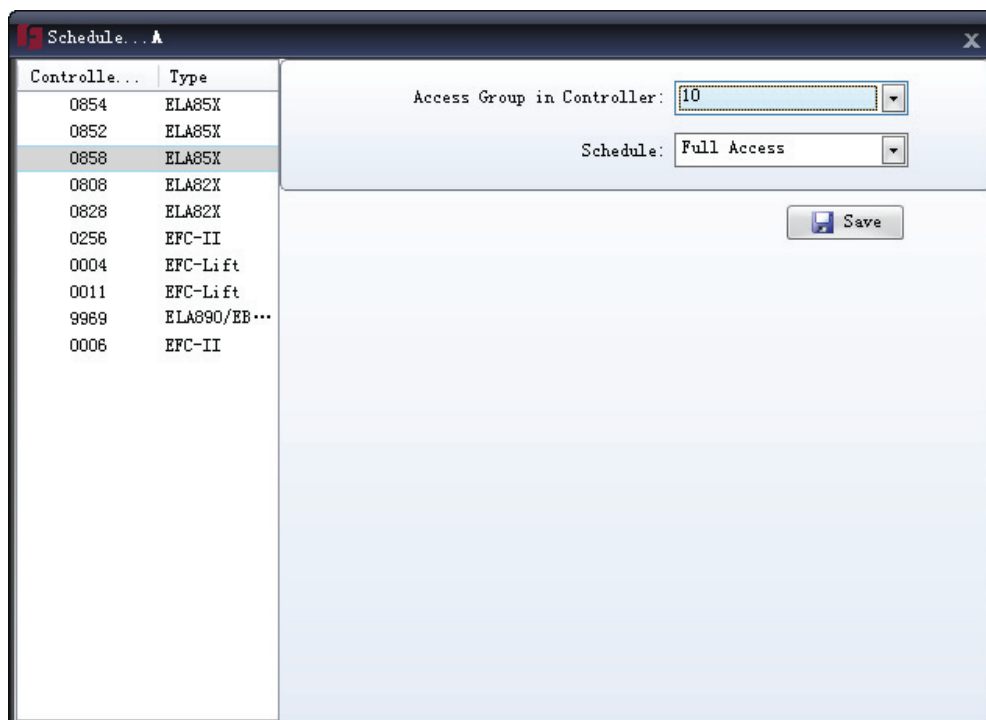


Fig. 6-16 Group A Setting on Controller 0858 (Before editing Group B)

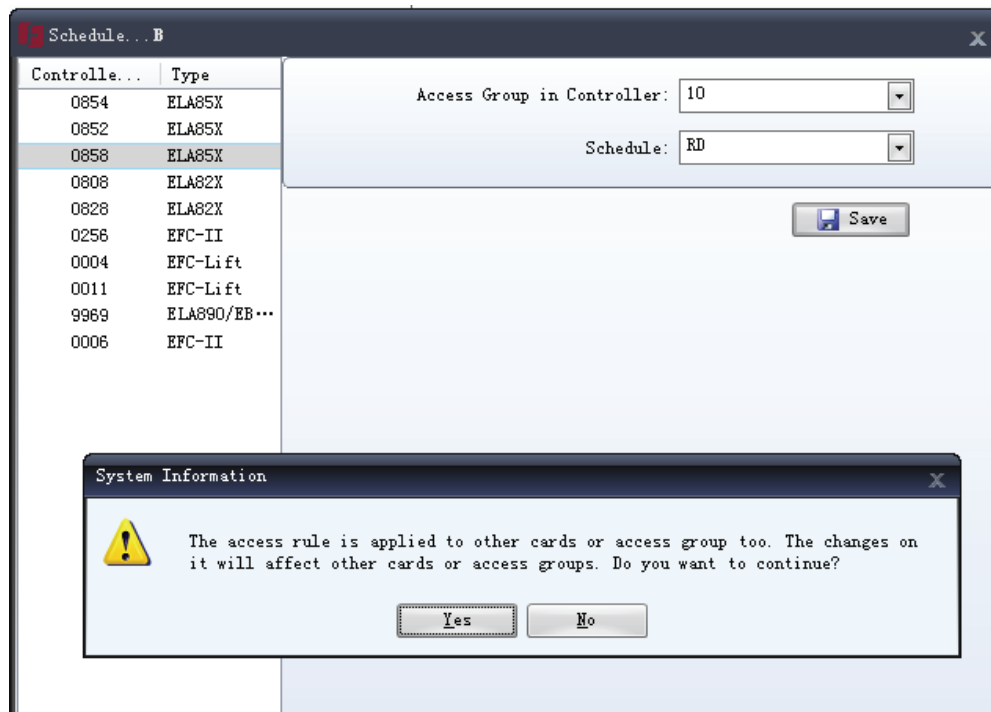


Fig. 6-17 Group B Setting on Controller 0858

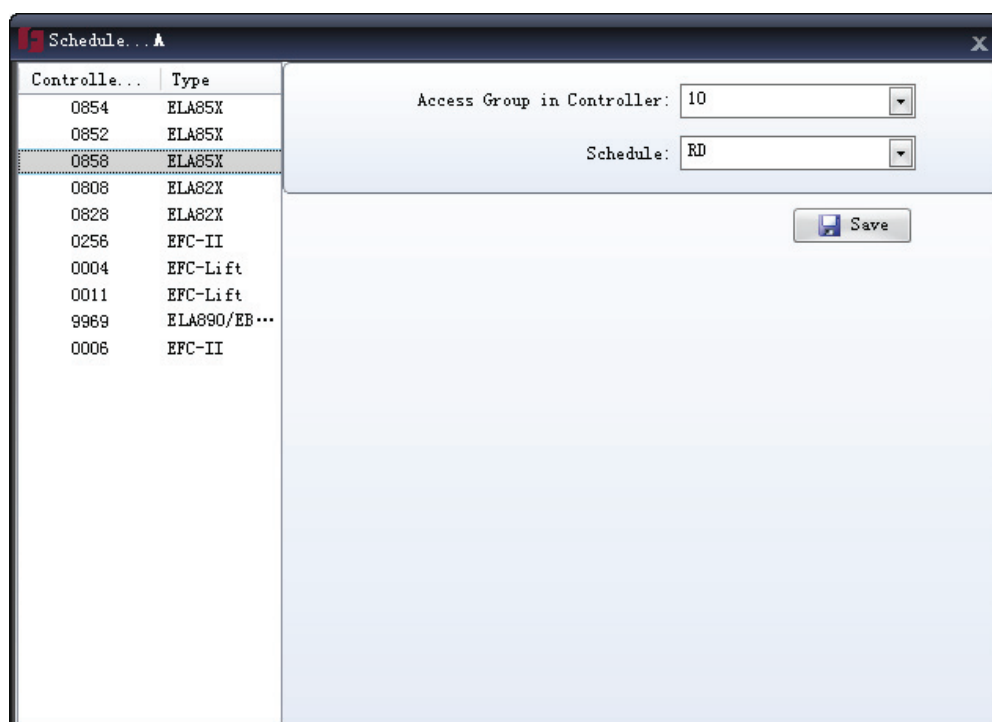


Fig. 6-18 Group A Setting on Controller 0858 (After Editing Group B)

The Access group schedule setting Window of different controller types is listed below:

✧ ELA82X Series Controller

An ELA808 4-door controller is used as an example here (Fig. 6-19). In an ELA808 4-door controller, access group schedules are shared among all door zones. Therefore, users only need to configure an access group schedule for one door zone, and this setting will be applied automatically to all the other door zones. Edit “Access group schedule” for one of the corresponding controller group, and click “Save”  after editing.

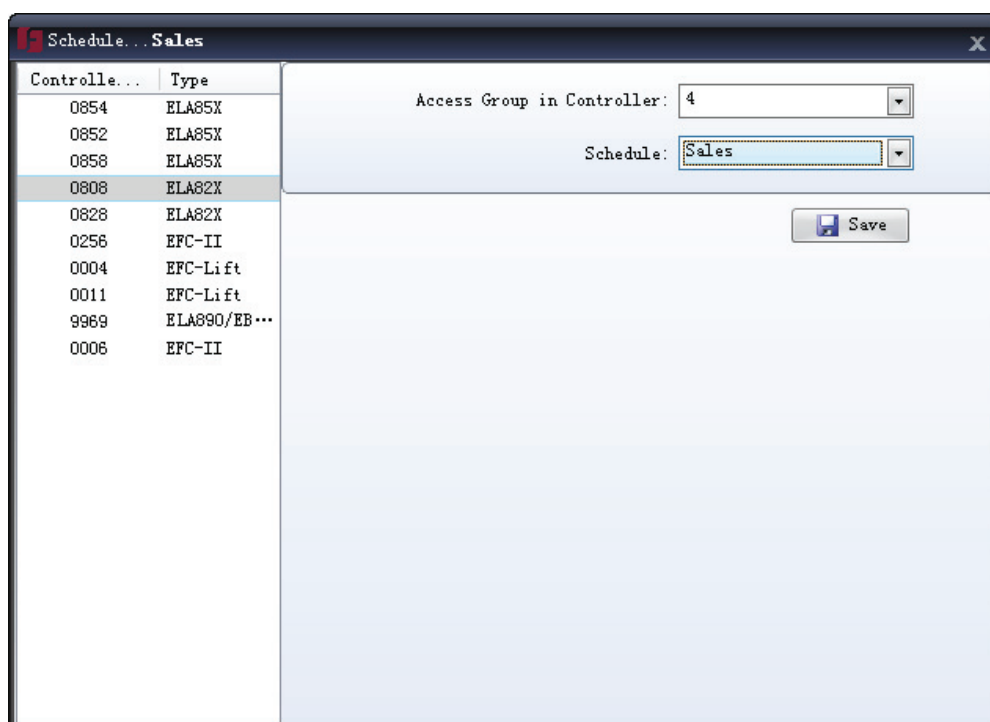


Fig. 6-19 ELA82X Series Controller: Access Group Schedule

✧ ELA85X Series Controller

An ELA858 8-door controller is used as an example here (Fig. 6-20). Similar to the ELA82X series controllers, access group schedules are shared among all door zones in an ELA85X controller. Edit “Access group schedule” for one of the corresponding controller groups, and click “Save”  after editing.

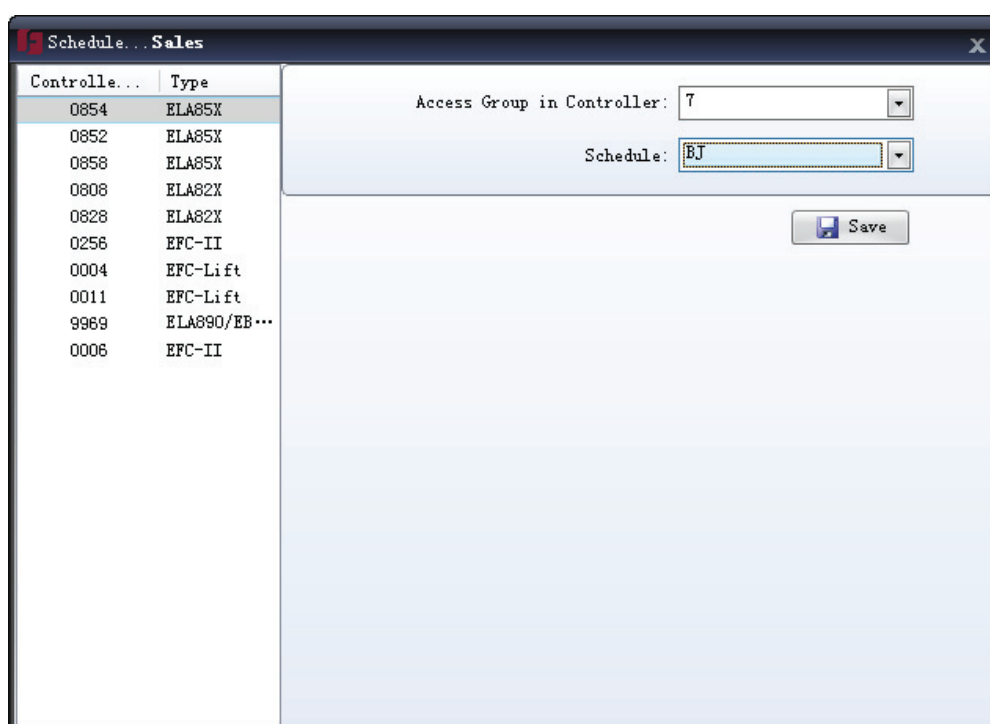


Fig. 6-20 ELA85X Series Controller: Access Group Schedule

✧ Fingerprint Controller

An ELA890 fingerprint controller is used as an example here (Fig. 6-21). Edit “Access group schedule” for one of the corresponding controller groups, and click “Save”  after editing.

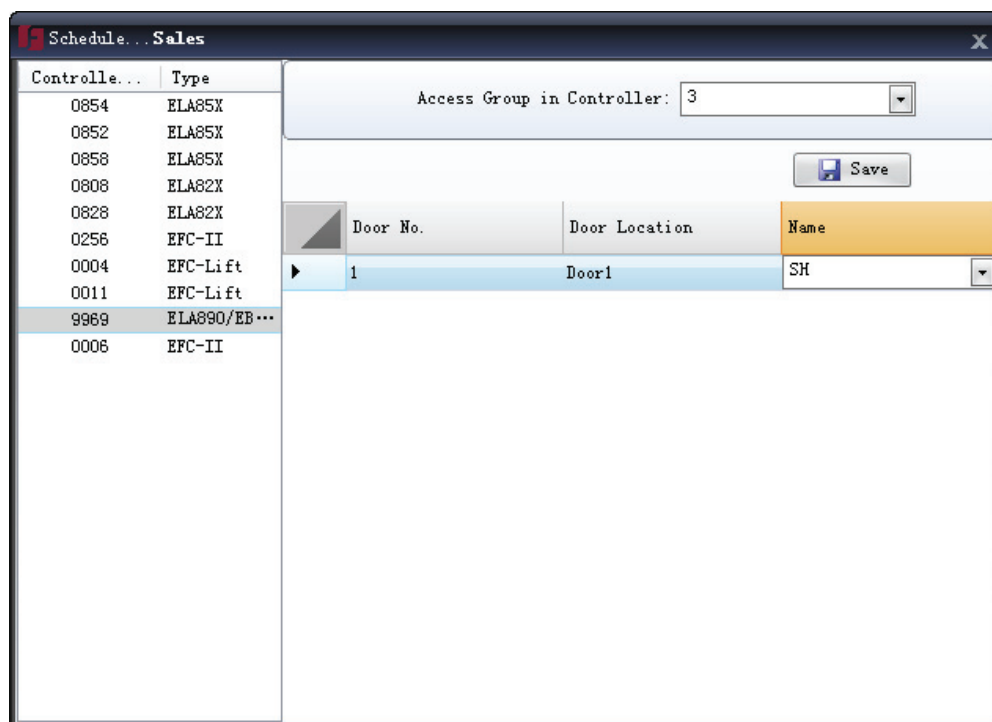


Fig. 6-21 Fingerprint Controller: Access Group Schedule

✧ Flex I Series Controller

An EFC-08-1A 8-door controller is used as an example here (Fig. 6-22). Flex I series controllers support different “Access Group Schedules” for different door zones. Edit “Access group schedule” for each of the corresponding controller group, and click “Save”  after editing.

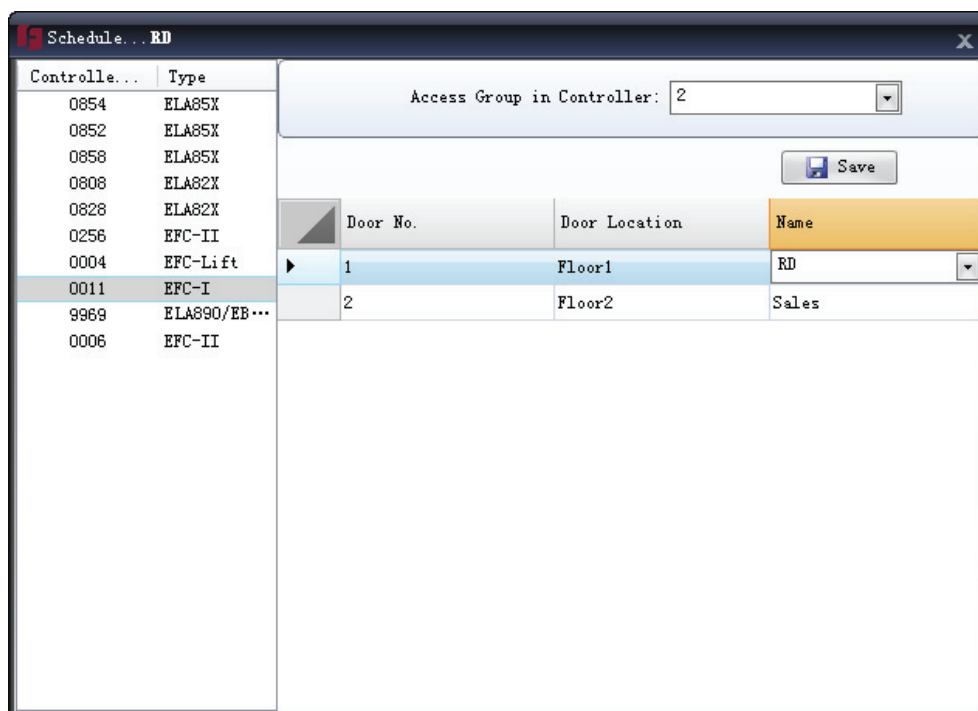


Fig. 6-22 Flex I Series Controller: Access Group Schedule

✧ EFC Series Elevator Controller

An EFC-08-Lift 8-floor elevator controller is used as an example here (Fig. 6-23). There are two controller groups: Authorized and Unauthorized. If “unauthorized” is selected, the cards in the access group will not be enrolled to the controller (see earlier descriptions in this section). As this type of controller determines whether each floor is authorized or not, there is no access group schedule setting. The cards in the access group will not be enrolled to the controller unless at least one of the floors is set to “Authorized”. “PIN required” means the verification level is “Card Plus PIN”. This setting applies to all floors. Click “Save”  after editing.

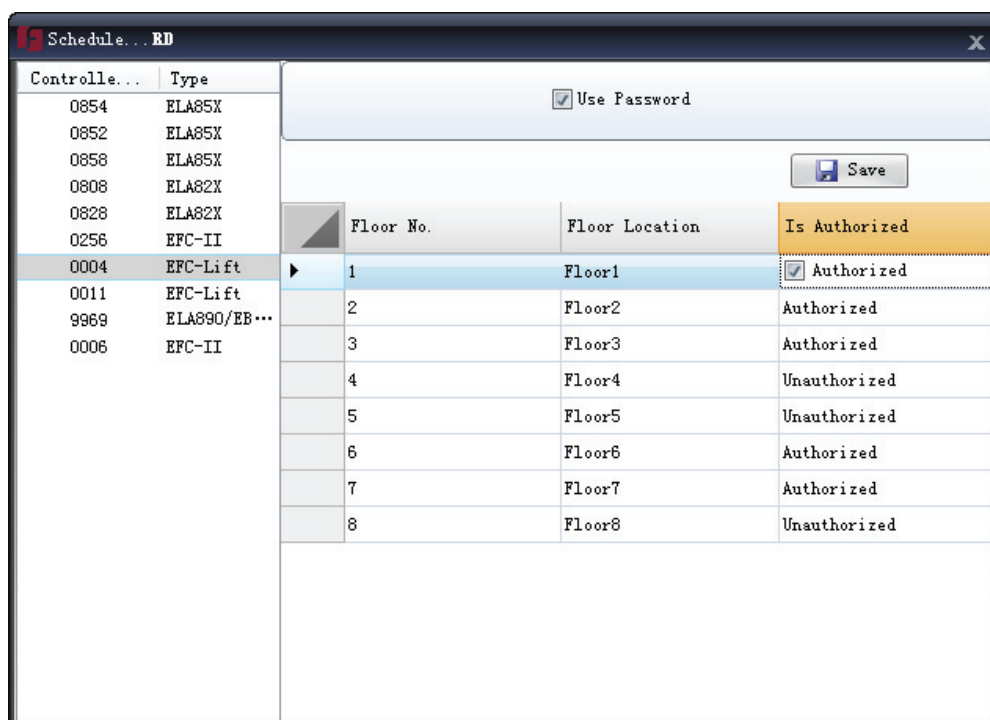


Fig. 6-23 EFC Series Elevator Controller: Access Group Schedule

✧ Flex II Series Controller

An EFC-08-2A 8-door controller is used as an example here (Fig. 6-23).

There are two types of verification: door verification and access group verification. The system default setting is door verification. If “access group verification” is selected, special verification levels are applied to the access group at the current door zone, and thus the door verification levels otherwise set for the door zone will not be applied. “Schedule Name” is set in “Access Group Schedule Setting”. Both Door verification and access group verification share the total of 2048 schedules that may be set in the controller. “Unlock level” corresponds to the door verification level in “Door Schedule Setting”. If the door verification level is set to 2 locks, and each lock has 2 levels, the unlock level can be indicated as 2, 2, 0, 0. If the unlock level of an access group at the current door is 1, 1, 0, 0. The door will be unlocked after two cards are presented to the reader successively. Click “Save”  after editing each item.

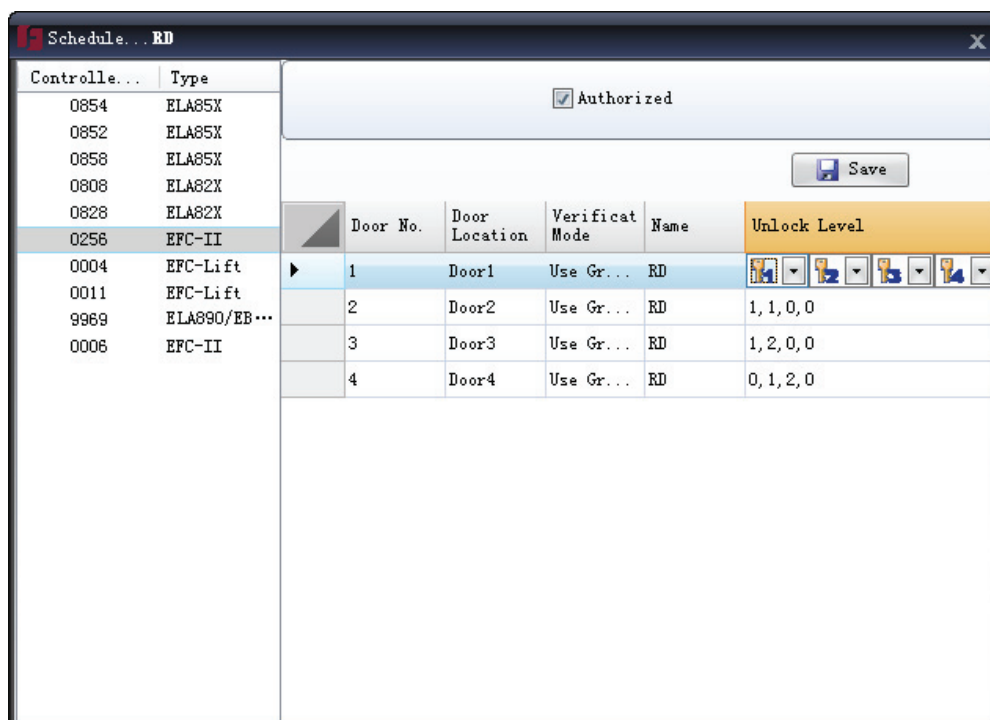


Fig. 6-24 Flex II Series Controller: Access Group Schedule

This is of the procedure for setting up unlocking. Setting up unlocking is described in “Door Schedule Setting” (Refer to section 6.3.5.5 Advanced unlock level Setting).

6.5 Access Group Schedule Setting

Click “Access Control Management” → “Access Rule” → “Access Group Schedule Setting” to open the window for access group schedule setting (Fig. 6-25).

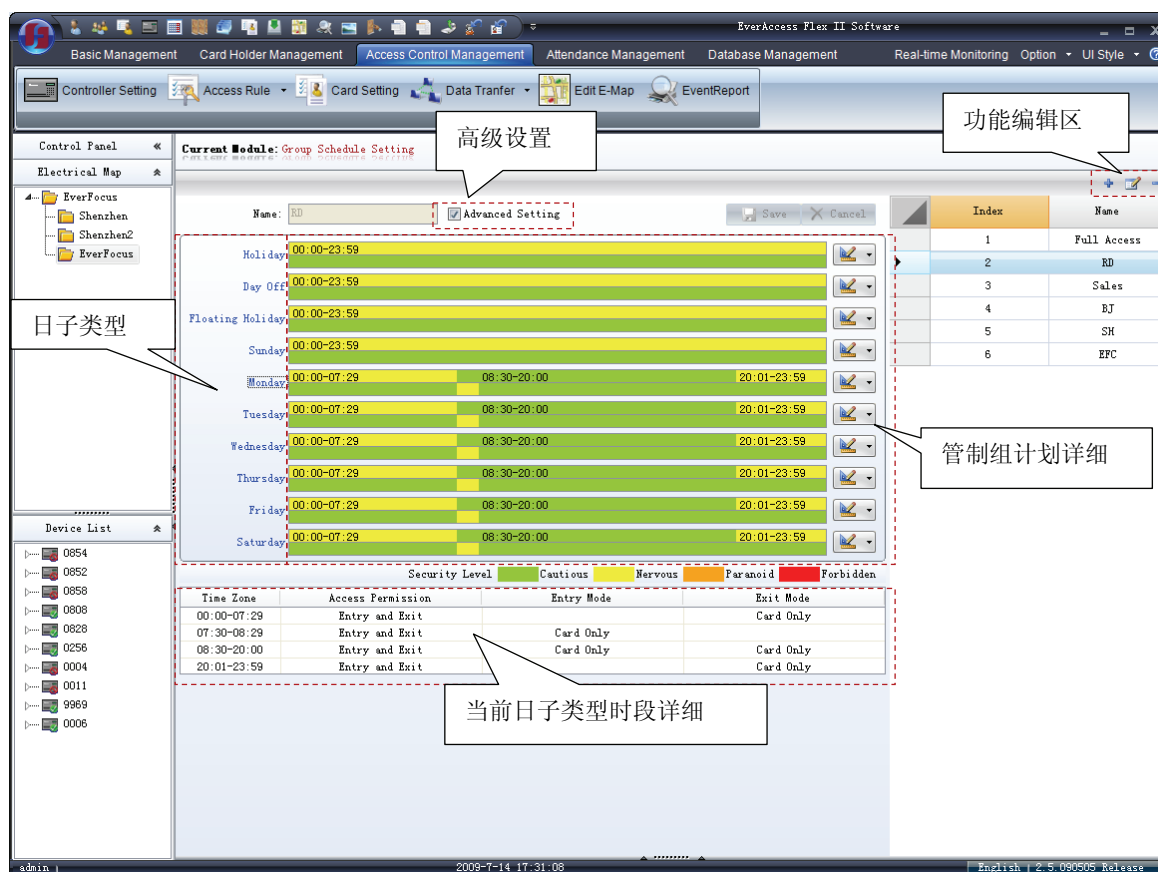


Fig. 6-25 Access Group Schedule Setting

There are two setting modes: Basic Setting and Advanced Setting. Under “Advanced Setting” mode, each date is divided into two parts with the upper part corresponding to “Entry (In)” and the lower part corresponding to “Exit (Out)”.

Basic Setting is based on access permission. There are 4 types of access permission: Entry/Exit (green), Entry/No Exit (blue), No Entry/Exit (yellow), No Entry/No Exit (red). The default access permission for a new schedule is “Entry/Exit”

Advanced Setting is based on security level. There are 4 types of security level: level 1 (light green), level 2 (yellow), level 3 (orange) and No permission (red). The default verification level for a new schedule is “Card” (level 1).

4 types of security level:

- Level 1: one item for verification, such as Card
- Level 2: two items for verification, such as Card plus PIN, (Card plus PIN) or fingerprint
- Level 3: three items for verification, such as Card plus PIN plus Fingerprint
- No Permission: access permitted.

For each access group schedule, there are 10 date types that may belong to either special types or normal types. Special types include legal holiday, day off and temporary change; Normal types include Monday to Sunday. Each date type can be divided into multiple time zones and different verification levels can be assigned to each time zone.

Note: The maximum number of time zones is 10 for each date type. The minimum time zone duration is 5 minutes.

In the detailed view of access group schedule setting, each time zone is marked by start time, end time and access permission displayed by bars of different colors. If the start time and end time are not shown, place the cursor on top of the color bar and the time information will be shown.

Note: The default access group schedule “Full Access” cannot be renamed or edited. The access permission for “Full Access” is Card for both Entry and Exit.

6.5.1 Add an Access Group Schedule

Click the “Add” button  in the “function editing area”, and enter the name of the access group schedule in the field labeled “Schedule Name”. Click the “save” button  and a dialog box reporting “Operation succeeded” will pop up. Schedule names must be unique.

6.5.2 Rename an Access Group Schedule

Select the access group schedule to be renamed in the schedule list, click the “Edit” button  in the “function editing area”, and enter the new name in the field labeled “Schedule Name”. Click “save” button  and a dialog box reporting “Operation succeeded” will pop up. Schedule names must be unique.

Note: The default access group schedule “Full Access” cannot be renamed.

6.5.3 Delete an Access Group Schedule

Select the access group schedule to be deleted in the schedule list, and click the “Delete” button  in the “function editing area”, A dialog box will be shown to prompt users to confirm the deletion. Click “Yes” to delete the access group schedule.

Note: The default access group schedule “Full Access” and access group schedules that have been assigned to a controller cannot be deleted.

6.5.4 Edit an Access Group Schedule

Under “Access Group Schedule Setting” window (Fig. 6-25), select an access group schedule from the list on the right, and the detailed settings of the selected schedule will be shown on the left. Click “Edit” , and the schedule editing window will pop up (Fig. 6-26).

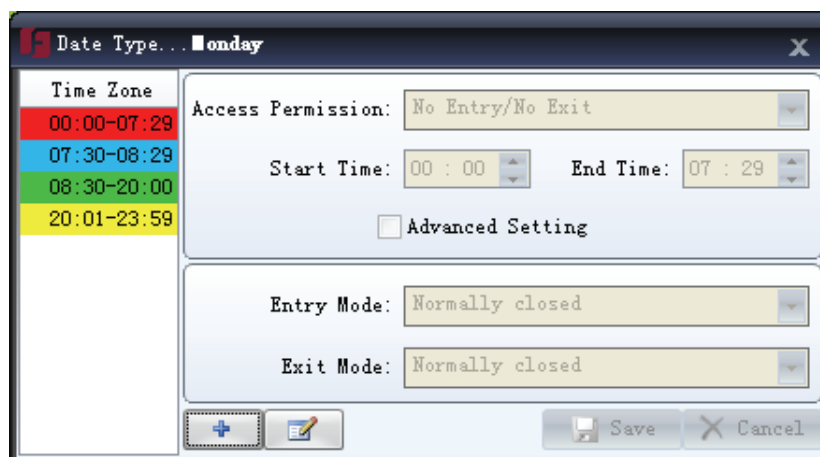


Fig. 6-26 Edit Access Group Schedule

In the window as shown in Fig. 6-26, click the “Add” button  or “Edit” , choose an access permission, start and end time. Click the “save” button  to save those settings. The Software will automatically divide or combine time zones according to the setting for access permission. For example, if an added time zone “13:00-14:00” is set to “Entry/No Exit” and an edited time zone “15:00 –16:00 is set to “No Entry/No Exit”. The new time zone is shown as in Fig. 6-27.

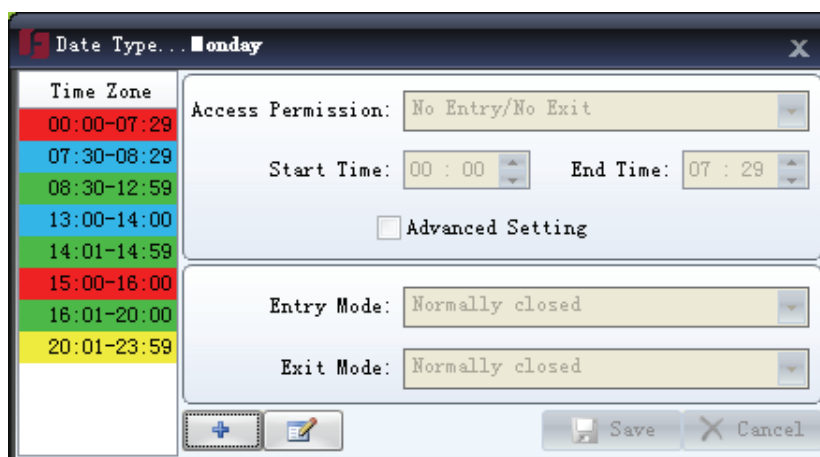


Fig. 6-27 Edit “Monday” Time Zone

If an access group schedule has been assigned to a door zone, the system will automatically update the schedule to the controller when a time zone is added or edited. If the controller is offline, users need to download the data to the controller manually.

Note: The system default start time of each time zone is 00s and the end time is 59s. Therefore, for the time zone 9:00-18:00, the system treats the time zone as 9:00:00-18:00:59. If editing a time zone makes a time zone duration less than 5 minutes, the system will automatically combine this time zone to the time zone that follows it until the combined time zone is longer than 5 minutes; If the start time of a time zone is later than 23:54, the system will combine it with the time zone that proceeds it until the combined time zone is longer than 5 minutes.

6.5.5 Advanced Setting

In the access group schedule setting, the system offers advanced settings, in which different verification levels can be assigned to entry (In) and exit (Out). Users can also choose In/Out verification levels for fingerprint controllers in the advanced setting mode. Fingerprint controllers support 13 types of verification level. Check “Advance Setting” and open the drop-down menu under “In mode” or “Out mode” (Fig. 6-28).

Note: Only Flex II series controllers support different In/Out verification level.

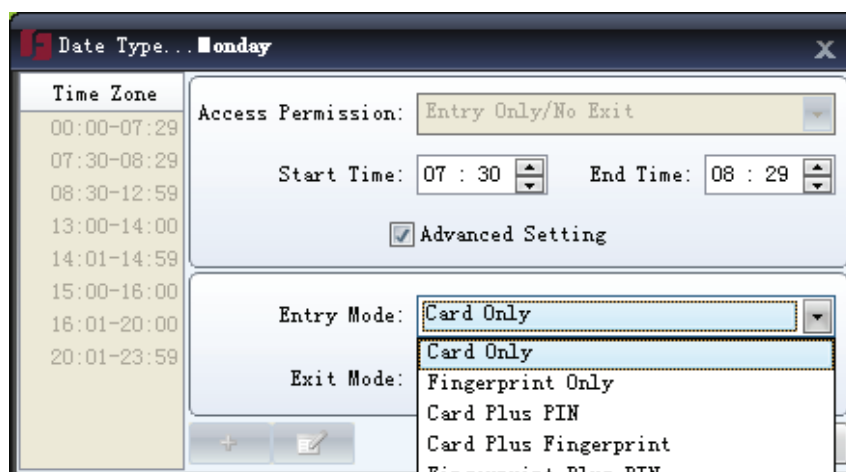


Fig. 6-28 Advanced Access Group Schedule Setting

6.5.6 Quick Access Group Schedule Setting

If the time zone setting among different date types under an access group schedule is the same, users can copy and paste the time zone settings by clicking the  button on the right of the “Edit” button  (Fig. 6-29). Users can also copy and paste time zone settings between different access group schedules. The copy and paste function is valid as long as one entry remains in the access group schedule setting window.

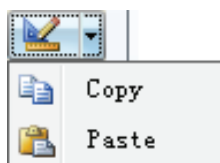


Fig. 6-29 Copy and Paste

6.6 Control Rules for new Controllers

The system offers flexible configuration options to achieve users’ specific needs under complex situations. Two conditions must be satisfied to open a door: control rules and unlock condition(s).

6.6.1 To satisfy Control Rules

Fig. 6-30 shows a flowchart to determine the priority level of control rules:

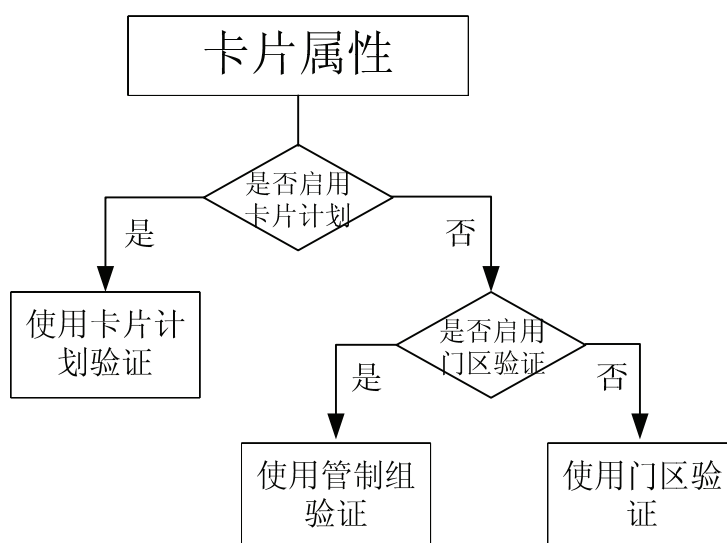


Fig. 6-30 Flowchart of Access Rule Priority

To determine priority level:

- 1) Whether "card schedule" in "card property" is enabled. Card schedule setting is shared with access group schedule setting. To select a special card schedule for a card, users need to add a new schedule in "access group schedule setting" and then apply the schedule for the card in "card schedule".
- 2) If "card schedule" is enabled, the system will follow the card schedule. In this situation, door verification control will not apply to this card.
- 3) If "card schedule" is disabled and "access group schedule" is enabled, the system will follow the access group schedule to which the card belongs, i.e. the access group to which the card belongs is authorized in the controller and the verification mode is "access group verification".
- 4) If "access group schedule" is disabled, the system will follow the "door schedule" for verification.

6.6.2 To Satisfy Unlock Condition(s)

To unlock a door, the unlock level of the access group to which the card belongs must be greater than or equal to the access authority level.

The Lock setting is related to unlock authority levels in "Door Schedule Setting". Refer to Section 6.3.5.5 Advanced Unlock level Setting.

The Unlock setting is related to unlock level in "Access Group Schedule Setting". Refer to Section 6.4.4 Edit Access Group.

Chapter 7

7 Card Setting

Click “Access Management” → “Card Setting” to open the window for card setting (Fig.7.1)

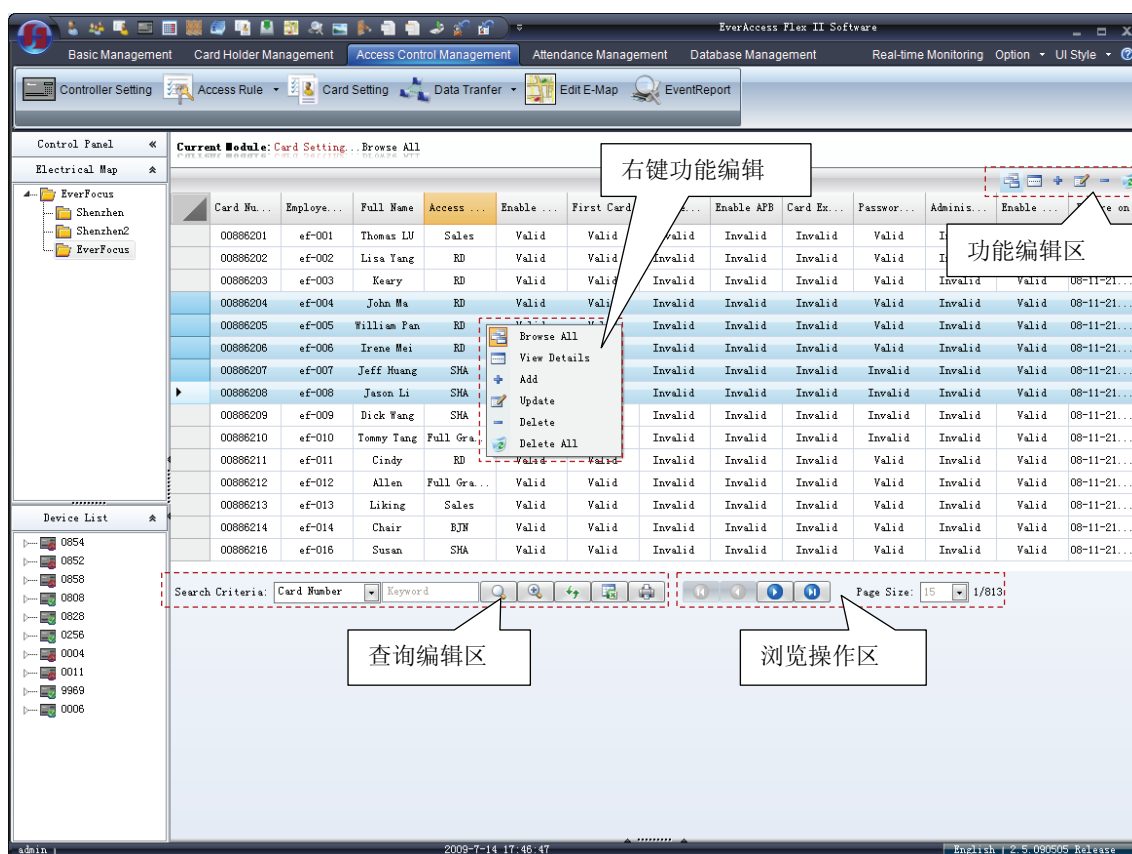


Fig. 7-1 Card Setting

Function editing area: To view all, view details of, add, edit, delete and delete all cards.

Search toolbar: To search cards using search criteria and keywords. It also provides advanced search, refreshing, exporting and printing functions.

Browsing toolbar: To view card list using navigation buttons “First Page”, “Backward”, “Forward” and “Last Page”. The system default setting is to display 15 cards per page.

Right-click menu: The system provides right-click menu for quick editing functions. Right click on the item to be edited, and a menu that contains the same commands as those in the “function editing area” will pop up.

7.1 Add a Card

Click the “Add” button  in the “function editing area” to open the window for adding a card (Fig. 7-2).

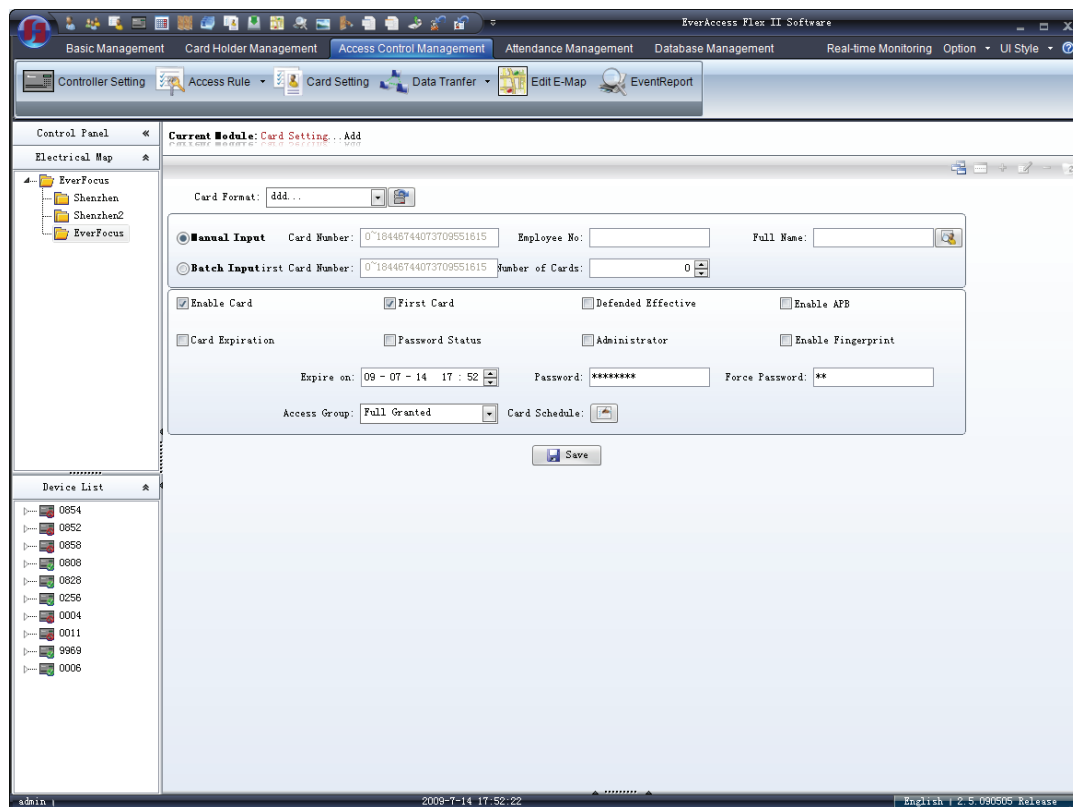


Fig. 7-2 Add a Card

7.1.1 Card Format

✧ ddd-ddddd: indicates an 8-digit decimal card number where each d represents a decimal number between 0-9. The form is divided into two parts with the first part consisting of a 3-digit decimal number (high), and the latter part consisting of a 5-digit decimal number (low). The two parts are spaced by symbol "-" or a space. Examples of this type are "075 09039" and "154-58742".

✧ dddddddd: indicates an 8-digit decimal card number where each d represents a decimal number between 0-9. The form is a continuous 8-digit decimal number. An example of this type is "00492423".

✧ HHHHHH: indicates a 6-digit hexadecimal card number where each H represents a hexadecimal number between 0-F (0-9, A-F). The form is a continuous 6-digit hexadecimal number. Examples of this type are "44EA5B" and "256871".

7.1.2 Register Cards

Register Cards Manually: register cards manually by typing in a card number or swiping the card through a reader, and then assign the card to a cardholder. To assign the card to a cardholder, enter the cardholder's employee number and/or name, and click the "Search Cardholder" button . If the cardholder is not found in the database, the system will prompt that the cardholder does not exist. Check the search criteria to make sure it is correct. When the cardholder is found, the employee number and name will be shown in the related field.

Note: When a cardholder is found, the employee number and name will be shown in the related field. Editing the employee number and/or name without clicking the "search cardholder" button will not change the card assignment. In other words, the system will assign the card based on the last search result of "search cardholder". This rule also applies to search functions under other functional modules in the Software.

Registering cards manually is suitable when registering multiple cards with non-continuous numbers and assigning each card to a cardholder. If users do not assign the card to a cardholder, when clicking "Save", the system will prompt that the cardholder information is empty for the registered card (Fig.7-3).

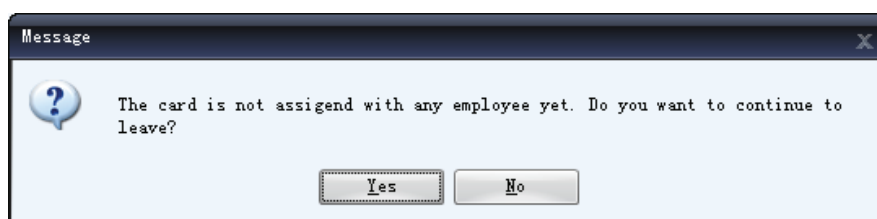


Fig. 7-3 Reminder Message: no cardholder assigned

Batch Register Cards: type in the card number or swipe the first card in a series of cards to be registered, and enter the number of cards in the series. The system will automatically register all the cards in the series to the database. Batch registering cards is suitable when registering multiple cards with continuous card numbers. However, *this method does not assign cards to cardholders*, which can be achieved by editing card information (Refer to section 7.3 Edit Card Information).

Note: To register cards by swiping cards, a card reader (such as ERU series USB desktop card reader) needs to be connected to the computer. ERU desk card readers support different card formats. Before swiping the card, put the cursor on the field where the card number needs to be entered, and swipe the card through the card reader, the card number will then be inserted in the field.

7.1.3 Card Property

Card properties include Card Enabled, First Card, Arm Enabled, APB Enabled, Card Expiration, PIN Enabled, Administrator and Fingerprint Enabled. Check the item to enable the property.

Card Enabled: whether the registered card is valid. Check the check box to enable the card. The assigned card properties will work only if the card is enabled. Swiping a card that is not registered with the controller generates an “unknown card” record. Swiping a card that is registered but disabled generates an “invalid card” record. Note: Card is optional for fingerprint controllers. Card Enabled does not affect fingerprint controllers.

First Card: whether the card is a “First Card” that can trigger unlocking based on door setting options (Refer to Section 6.2 door setting) and the “First Card-in” function in controller setting (Refer to Section 5.5.8 system setting). For example, suppose door 1 under controller 0001 is set to “unlock” in time zone 9:00-11:00. During this time period, swiping a First Card enabled card unlocks the door. In addition, if “First Card-in” function is enabled for controller 0001, only after a First Card enabled card has been presented to a reader under controller 0001, will other (First Card disabled) cards be able to unlock the door, even though those (First Card disabled) cards satisfy all other conditions to unlock the door.

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

APB Enabled: whether anti-passback (APB) is enabled for the card. If APB Enabled is enabled for a card, and the controller APB function is enabled, the APB setting is in effect for the card. Refer to Section 5.5.2 Anti-Passback (APB) Setting for details.

Card Expiration: 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 the minute. This function is not applicable to ELA82x series controllers.

PIN Enabled: for ELA82x, ELA85x and Flex I series controllers, this function refers to whether a personal PIN is enabled. If PIN Enabled is checked, PIN entry is enabled for the cardholder, and the cardholder will be *required* to input their personal PIN when swiping the card to enter/exit the door. PIN is a number from 4 digits to 8 digits. ELA82x and ELA85x series controllers support a 4-digit PIN and Flex I series controllers support a 6-digit PIN. When enrolling a card to controllers, ELA82x and ELA85x series controllers will truncate a PIN longer than 4 digits, and Flex I series controllers will add “0” at the end if the PIN is shorter than 6 digits.

For Flex II series controllers, this function is used to set the card PIN. Flex II series controllers support an 8-digit PIN. To enable/disable card PIN for a Flex II series controller, use the functions in door setting, access authority setting or card schedule setting.

Administrator: whether the cardholder is an administrator for fingerprint controllers. When the administrator function is checked, the cardholder has the authority to manage fingerprint controllers in the system.

Fingerprint Enabled: whether the registered fingerprint is valid. Similar to the “Card Enabled” property, if a registered fingerprint is disabled, the registered fingerprint is treated as invalid. Attempting to gain access with an invalid fingerprint generates a “no registered fingerprint for the cardholder” record.

Panic PIN: this function is only applicable to Flex I and Flex II series controllers. The panic PIN is a 2 digit number. When a cardholder is forced to unlock a door, the cardholder can enter the panic PIN. For Flex I controllers, use the card PIN (6 digits) plus the 2-digit panic PIN. For Flex II controllers, use the first 6 digits of the card PIN plus the 2-digit panic PIN.

Access Group: access authority setting. The system applies different access control rules for different access groups (Refer to Section 6.4 Access group setting).

Card 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. This function is only applicable to Flex II series controllers.

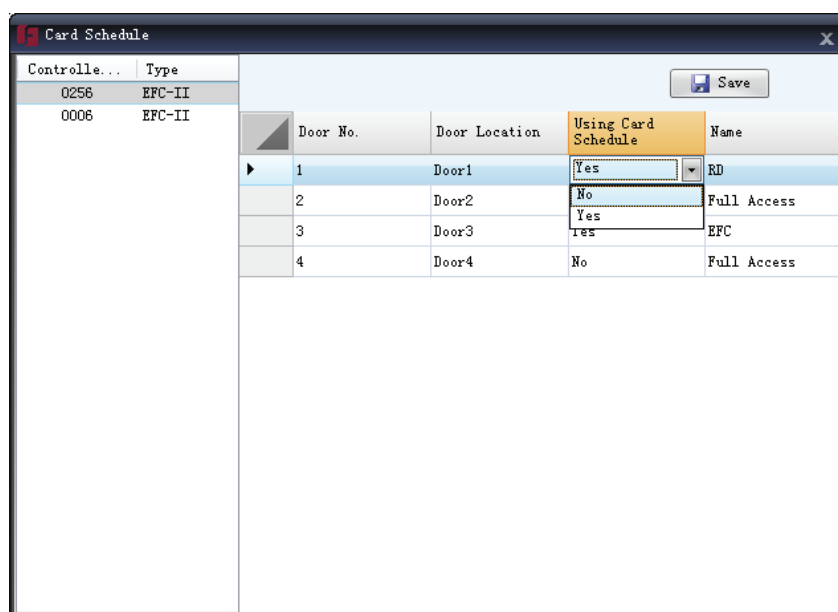


Fig. 7-4 Card Schedule

7.2 Import Card Information

Click “Database Management” → “Import Data” → “Import Card Information”. Refer to Section 13.4.2 Import Card Information

7.3 Edit Card Information

In the window for “Card Setting” (Fig. 7-1), select the card to be edited, then click “Edit”  in the “function editing area” or choose “Edit” from the right-click menu to open the window for editing card information (Fig. 7-5). After editing, click “Save” and a dialog box reporting “Operation succeeded” will pop up. Otherwise, click “View All” to return to the window for “Card Setting”.

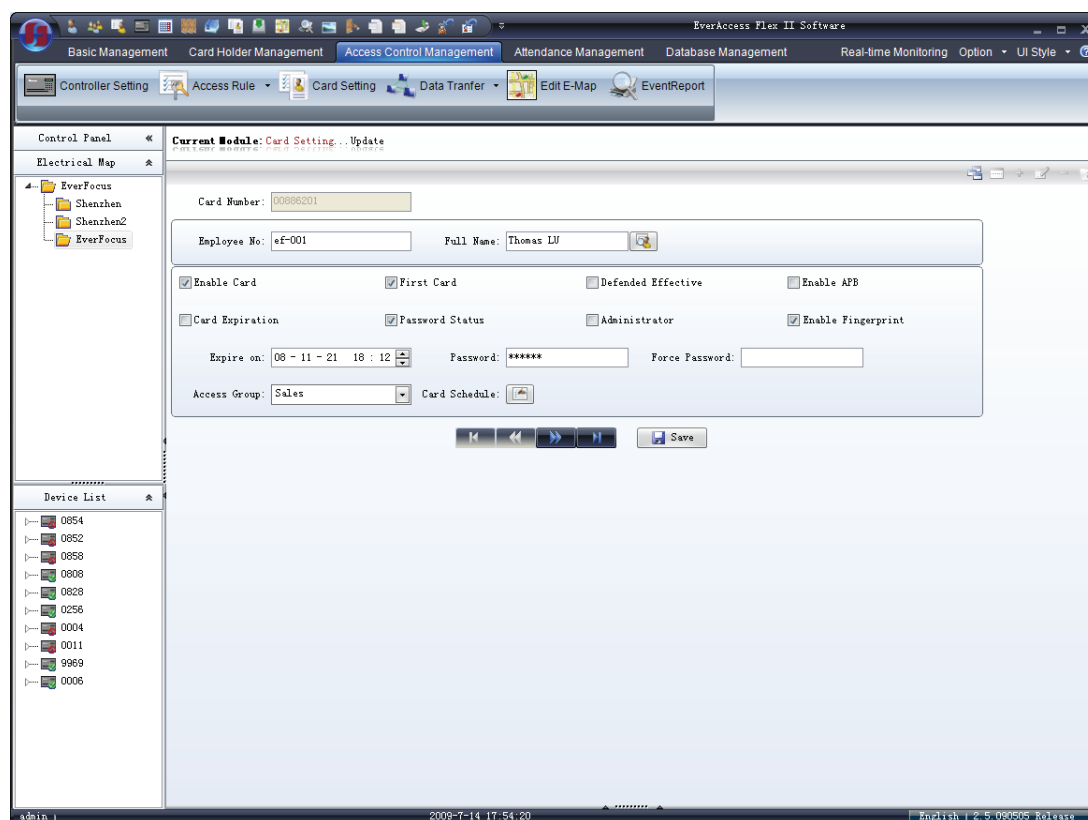


Fig. 7-5 Edit Card Information

7.4 Batch Edit Card Information

The Software offers the option of batch editing card information. This function provides an efficient way to modify a certain item of multiple cards to be the same.

Drag the mouse across the card list to select multiple adjacent cards or use the “Ctrl” key on the keyboard to select nonadjacent cards. After selecting the cards to be edited, right click to open the menu (Fig. 7-6) and select “Edit”. The window for batch editing card information will be shown (Figure 7-7).

Card Nu...	Employee...	Full Name	Access	Enable ...	First Card	Defende...	Enable AFB	Card Ex...	Passwor...	Adminis...	Enable ...	Expire on
00886201	ef-001	Thomas LU	Sales	Valid	Valid	Invalid	Invalid	Invalid	Valid	Invalid	Valid	08-11-21...
00886202	ef-002	Lisa Yang	RD	Valid	Valid	Invalid	Invalid	Invalid	Valid	Invalid	Valid	08-11-21...
00886203	ef-003	Keary	RD	Valid	Valid	Invalid	Invalid	Invalid	Valid	Invalid	Valid	08-11-21...
00886204	ef-004	John Ma	RD	Invalid	Invalid	Invalid	Invalid	Invalid	Valid	Invalid	Valid	08-11-21...
00886205	ef-005	William Pan	RD	Invalid	Invalid	Invalid	Invalid	Invalid	Valid	Invalid	Valid	08-11-21...
00886206	ef-006	Irene Mei	RD	Invalid	Invalid	Invalid	Invalid	Invalid	Valid	Invalid	Valid	08-11-21...
00886207	ef-007	Jeff Huang	SHA	Invalid	Invalid	Invalid	Invalid	Invalid	Invalid	Invalid	Valid	08-11-21...
00886208	ef-008	Jason Li	SHA	Invalid	Invalid	Invalid	Invalid	Invalid	Invalid	Invalid	Valid	08-11-21...
00886209	ef-009	Dick Wang	SHA	Invalid	Invalid	Invalid	Invalid	Invalid	Invalid	Invalid	Valid	08-11-21...
00886210	ef-010	Tommy Tang	Full Gra...	Valid	Valid	Invalid	Invalid	Invalid	Invalid	Invalid	Valid	08-11-21...
00886211	ef-011	Cindy	RD	Valid	Valid	Invalid	Invalid	Invalid	Valid	Invalid	Valid	08-11-21...
00886212	ef-012	Allen	Full Gra...	Valid	Valid	Invalid	Invalid	Invalid	Valid	Invalid	Valid	08-11-21...
00886213	ef-013	Liking	Sales	Valid	Valid	Invalid	Invalid	Invalid	Valid	Invalid	Valid	08-11-21...
00886214	ef-014	Chair	BJN	Valid	Valid	Invalid	Invalid	Invalid	Valid	Invalid	Valid	08-11-21...
00886216	ef-016	Susan	SHA	Valid	Valid	Invalid	Invalid	Invalid	Valid	Invalid	Valid	08-11-21...

Fig. 7-6 Batch Edit Card Information

The public information of the selected cardholders will be shown and the selected cardholders are highlighted (Fig. 7-6). After editing, click “Save” and a dialog box will pop up to prompt that “You will not be able to undo this operation, do you want to continue?” Click “OK” to confirm and the information of all selected cards will be changed.

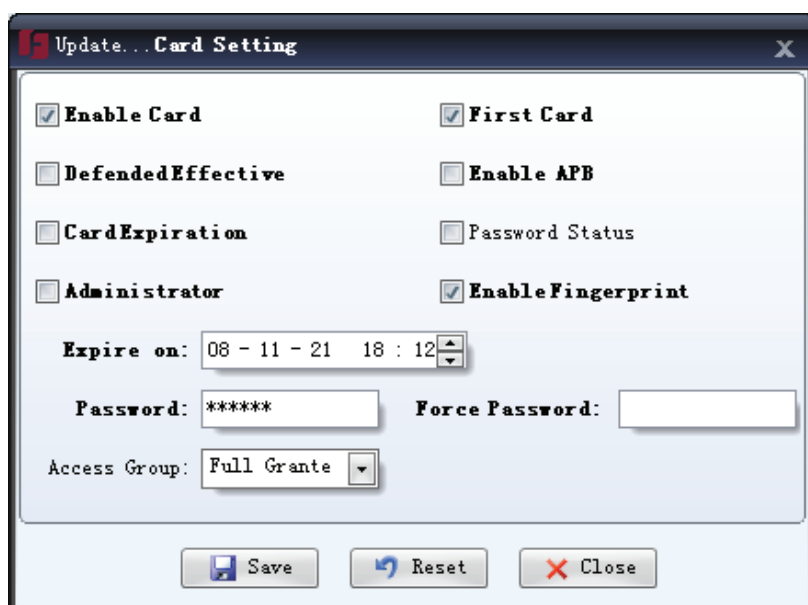


Fig. 7-7 Batch Edit Cards

Note: This operation only changes the items whose titles are highlighted. The rest of the card information remains unchanged.

7.5 View Card Information

7.5.1 View Card List

Click “Access Control Management” → “Access Rule” → “Card Setting” to view all the cards in the system (Fig. 7-1).

7.5.2 View Details of Card Information

Click the “View Details” button  in the “Function editing area” (Fig. 7-1) to open the window for viewing the details of card information (Fig. 7-8). Users can choose to view details of a card using the navigation button “BW” and “FW” at the bottom of the window. Click the “Edit” button  in the “function editing area” to edit the card information in view (Fig. 7-5).

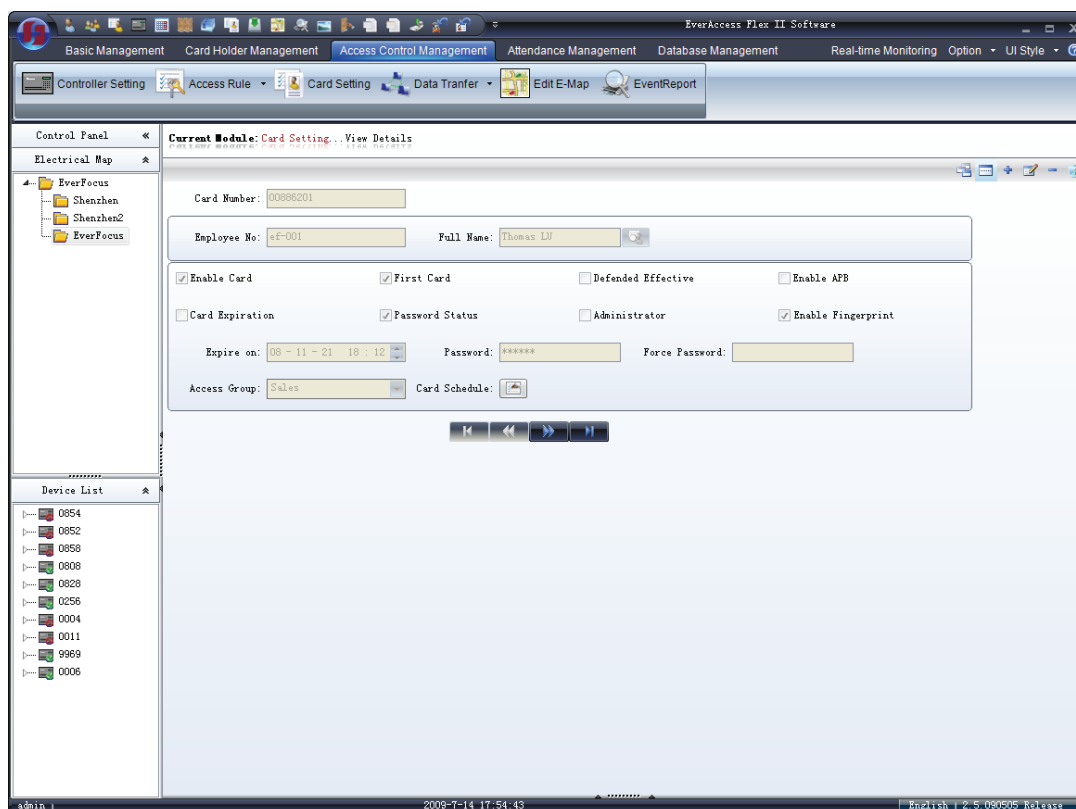


Fig. 7-8 View Details of Card Information

7.6 Delete Card(s)

7.6.1 Delete a Card

In the window for Card Setting (Fig. 7-1), select the card to be deleted, and click the “Delete” button in the “Function editing area”. A dialog box will be shown to prompt users to confirm the deletion. Click “Yes” to delete the card and another dialog box will be shown to confirm that the deletion is successful. Otherwise, click “Cancel” to exit.

7.6.2 Delete All Cards

In the window for Card Setting (Fig. 7-1), click the “Delete All” button in the “Function editing area”. A dialog box will be shown to prompt users to confirm the deletion. Click “Yes” to delete all cards and another dialog box will be shown to confirm that the deletion is successful. The number of deleted cards will also be shown. Otherwise, click “Cancel” to exit.

7.7 Download Card Information

1) Download one card to multiple controllers

During the process of downloading, if any controller cannot be found, the system will show a pop-up window as below. Click “Yes” and the system will continue to download the card

information to other controllers. Click “Cancel” and the system will cancel the operation. The card information will not be downloaded to other controllers.

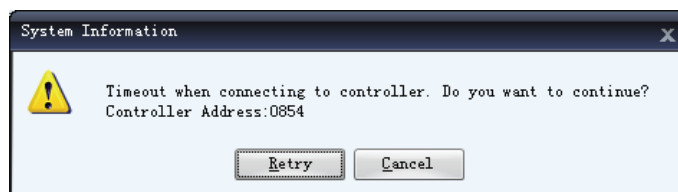


Fig. 7-9 Download one card to multiple controllers: Timeout Warning

2) Download multiple cards to one controller

During the process of downloading, if that controller cannot be found, the system will show a pop-up window as below. Click “Retry” and the system will try to reconnect to the controller. Otherwise, click “Cancel” and the remaining card information will not be downloaded to the controller.

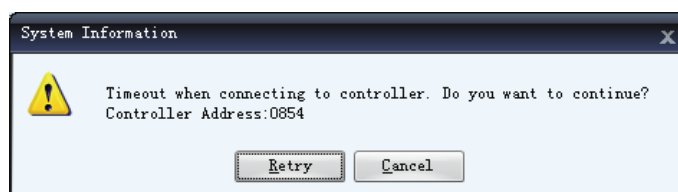


Fig. 7-10 Download multiple cards to one controller: Timeout Warning

3) Download multiple cards to multiple controllers

During the process of downloading, if any controller cannot be found, the system will show a pop-up window as below. Click “Cancel” to cancel the download and remaining cards will not be downloaded. Click “Retry” and the system will try to reconnect to the controller. Click “Ignore” and the system will continue to download the card information to other controllers.

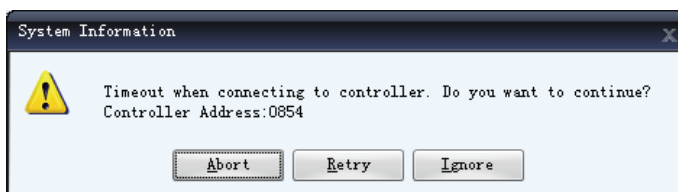


Fig. 7-11 Download multiple cards to multiple controllers: Timeout Warning

7.8 Search Card

7.8.1 Basic Search

In the “search tool bar”, select search field from card number, card Index, employee number, employee name and access group and enter the search criteria in the “keyword” text box. Click the “Search” button  to start searching. If there are cards matching the search criteria, they will be shown in the card list (Fig. 7-12).

Note: The search function here is *exact match*. If one needs complex or ‘fuzzy’ searches for multiple search fields, please use the “Advanced Search” function (Refer to section 7.8.2 for details).

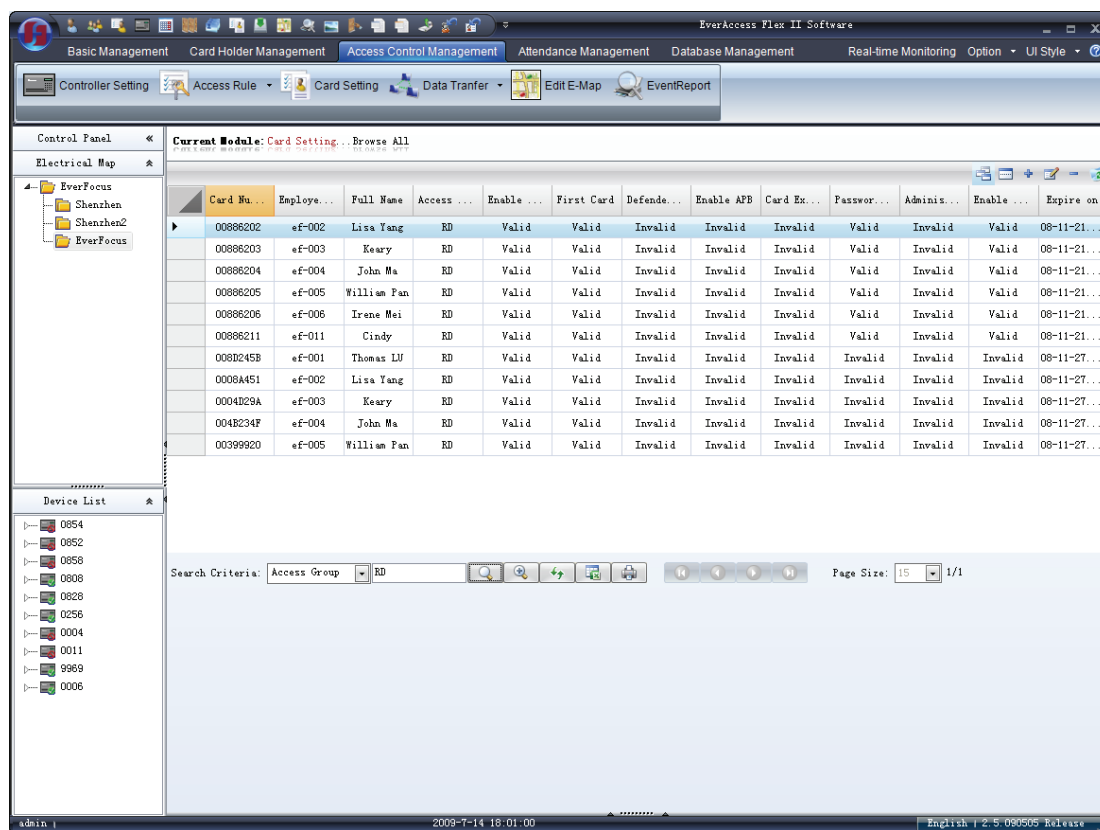
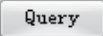
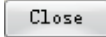


Fig. 7-12 Search Card

7.8.2 Advanced Search

Click “Advanced Search”  in the “searching toolbar” to open the window for advanced search (Fig. 7-13). Fill in the search criteria, and click “Search”  to start searching. If there are cards matching the search criteria, they will be shown in the card list. When finished, click “Close”  to return to the “Card Setting” window.

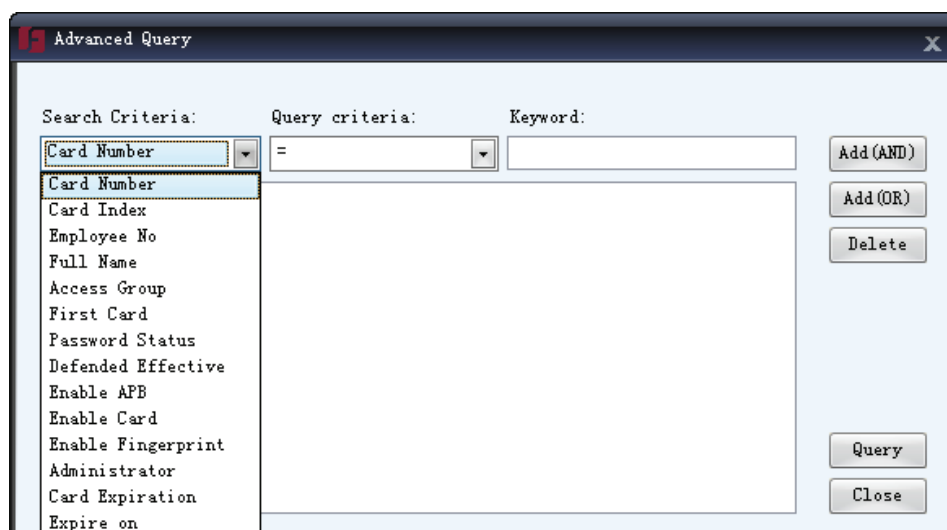


Fig. 7-13 Advanced Search

Search criteria: the name of search items, including card Index, card number, employee number, employee name, access group, Card Enabled, First Card, Arm Enabled, APB Enabled, Card Expiration, PIN Enabled, Administrator and Fingerprint Enabled..

Condition: the matching condition to the search criteria, such as “=” (equal), “<>” (not equal), “>” (greater than), “>=” (greater than or equal”, “<” (less than”, “<=” (less than or equal), “includes (in any position)” “includes (starts with)”, “includes (ends with)”.

Keywords: enter or select the search criteria that match the search condition. For example, if the search field is “First Card Enabled” and “Card Enabled”, users can select “enabled” or “disabled” from the keywords text box (Fig. 7-14). enabled

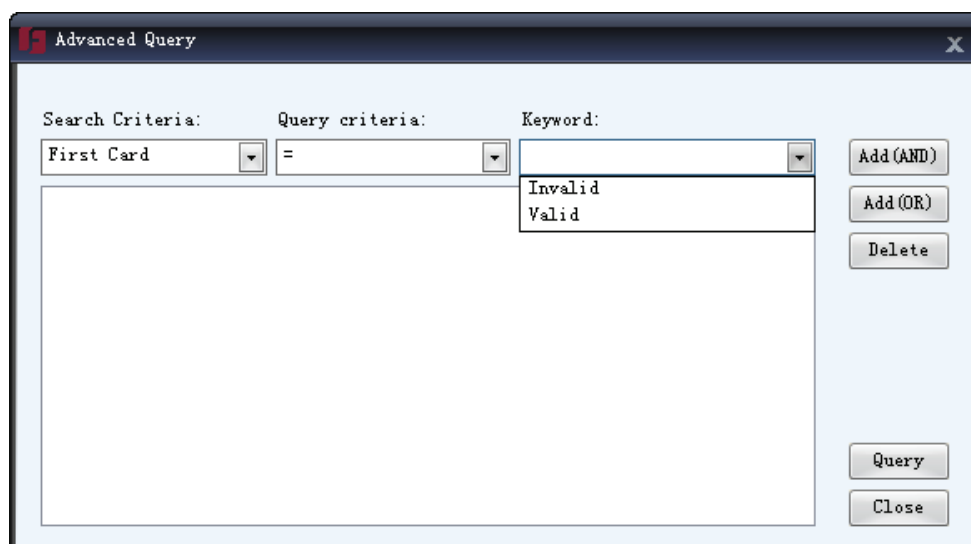
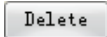


Fig. 7-14 Search Criteria: Keywords for “First Card Enabled”

Add (and): search for cards that match all conditions in two or more search fields.

Add (or): search for cards that match any of the conditions in two or more search fields.

Delete: Select the search condition in the search field list, click “Delete”  to delete the selected search field.

7.9 Refresh Card Information

Click “Refresh”  in the “search tool bar” to show the current card list.

7.10 Export Card Information

Click “Export”  in the “search tool bar”, a dialog box showing “Card Exporting Format” will pop up. User can choose whether to keep the card format to be the same as in the Software. If user wants to keep the card format, check the box “Keep card format”. User can also choose to export the card in a desired format. For example, user can choose to export the cards in hexadecimal format by choose export format “HHH...”

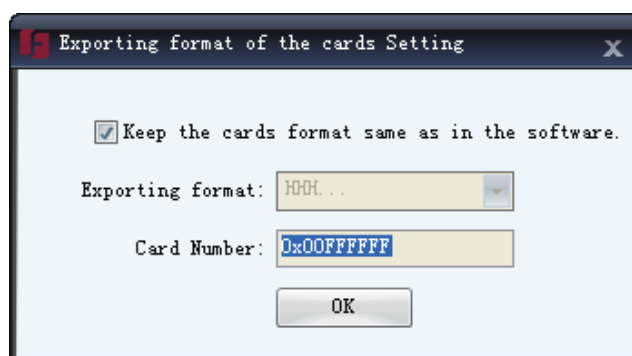


Fig. 7-15 Exporting Format of Cards Setting

After selecting the export format, click “Yes” and a dialog box will pop up to show that the card information has been exported as an Excel file. When finished exporting, another dialog box will pop up to ask whether to open the file.

7.11 Print Card Information

Click “Print”  in the “search tool bar” to open the window for printing card information (Fig. 7-16). The menu bar includes: export, print, refresh, switch node, go to the first page, go to last page, go to next page, go to the last page, go to page, close, search text, zoom in/out etc.

Print Card Setting

主报表

Card Setting

Card Number	Employee	Full Name	Access C	Enable Cs	First Cs	Defende	Enable AF	Card Exy	Password S	Administ	Enable Fingerprint	Expire on
00886201	ef-001	Thomas LU	Sales	Valid	Valid	Invalid	Invalid	Invalid	Valid	Invalid	Valid	2008-11-21 18:12:00
00886202	ef-002	Lisa Yang	RD	Valid	Valid	Invalid	Invalid	Invalid	Valid	Invalid	Valid	2008-11-21 18:12:00
00886203	ef-003	Keary	RD	Valid	Valid	Invalid	Invalid	Invalid	Valid	Invalid	Valid	2008-11-21 18:12:00
00886204	ef-004	John Ma	RD	Valid	Valid	Invalid	Invalid	Invalid	Valid	Invalid	Valid	2008-11-21 18:12:00
00886205	ef-005	William Pan	RD	Valid	Valid	Invalid	Invalid	Invalid	Valid	Invalid	Valid	2008-11-21 18:12:00
00886206	ef-006	Irene Mei	RD	Valid	Valid	Invalid	Invalid	Invalid	Valid	Invalid	Valid	2008-11-21 18:12:00
00886207	ef-007	Jeff Huang	SHA	Valid	Valid	Invalid	Invalid	Invalid	Invalid	Invalid	Valid	2008-11-21 18:12:00
00886208	ef-008	Jason Li	SHA	Valid	Valid	Invalid	Invalid	Invalid	Invalid	Invalid	Valid	2008-11-21 18:12:00
00886209	ef-009	Dick Wang	SHA	Valid	Valid	Invalid	Invalid	Invalid	Invalid	Invalid	Valid	2008-11-21 18:12:00
00886210	ef-010	Tonny Tang	Full Granted	Valid	Valid	Invalid	Invalid	Invalid	Invalid	Invalid	Valid	2008-11-21 18:12:00
00886211	ef-011	Cindy	RD	Valid	Valid	Invalid	Invalid	Invalid	Valid	Invalid	Valid	2008-11-21 18:12:00
00886212	ef-012	Allen	Full Granted	Valid	Valid	Invalid	Invalid	Invalid	Valid	Invalid	Valid	2008-11-21 18:12:00
00886213	ef-013	Liking	Sales	Valid	Valid	Invalid	Invalid	Invalid	Valid	Invalid	Valid	2008-11-21 18:12:00
00886214	ef-014	Chair	BJN	Valid	Valid	Invalid	Invalid	Invalid	Valid	Invalid	Valid	2008-11-21 18:12:00
00886216	ef-016	Susan	SHA	Valid	Valid	Invalid	Invalid	Invalid	Valid	Invalid	Valid	2008-11-21 18:12:00
00886217	ef-017	Color	BJN	Valid	Valid	Invalid	Invalid	Invalid	Valid	Invalid	Valid	2008-11-21 18:12:00
00886218	ef-018	Yuki	BJN	Valid	Valid	Invalid	Invalid	Invalid	Valid	Invalid	Valid	2008-11-21 18:12:00
00886219	ef-019	Yubo	BJN	Valid	Valid	Invalid	Invalid	Invalid	Valid	Invalid	Valid	2008-11-21 18:12:00
00886220	ef-020	Vincent	BJN	Valid	Valid	Invalid	Invalid	Invalid	Valid	Invalid	Valid	2008-11-21 18:12:00
00886301	ef-021	Bill	BJN	Valid	Valid	Invalid	Invalid	Invalid	Valid	Invalid	Invalid	2008-11-21 18:12:00
008D245B	ef-001	Thomas LU	RD	Valid	Valid	Invalid	Invalid	Invalid	Invalid	Invalid	Invalid	2008-11-27 9:45:00
0008A451	ef-002	Lisa Yang	RD	Valid	Valid	Invalid	Invalid	Invalid	Invalid	Invalid	Invalid	2008-11-27 10:11:00
0004D29A	ef-003	Keary	RD	Valid	Valid	Invalid	Invalid	Invalid	Invalid	Invalid	Invalid	2008-11-27 10:11:00

当前页码: 1 总页数: 1+ 缩放系数: 100%

Fig. 7-16 Print Card Information

Chapter

8

8 Data Communication with Controllers

8.1 Upload Data to Computer

Click “Access Control Management” → “Data Communication”, and select “Upload data to Computer” from the drop-down menu to open the window for uploading data to computer (Fig. 8-1).

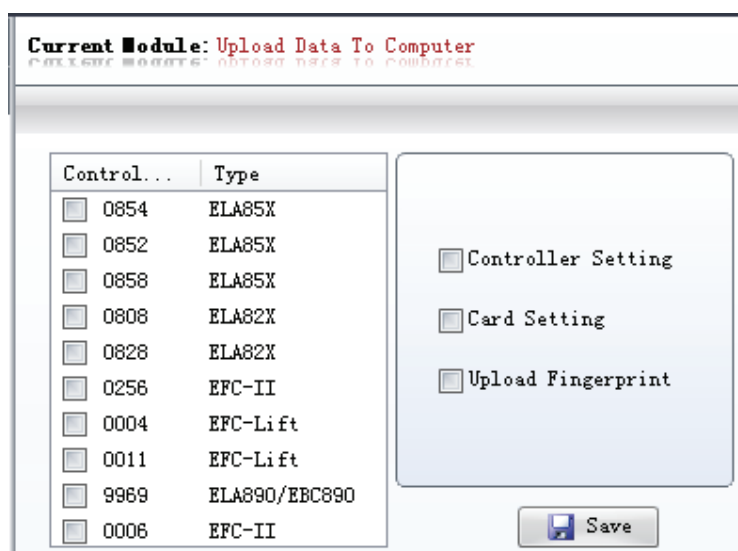
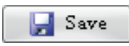


Fig. 8-1 Upload Data to computer

This operation is to upload controller-stored data, including controller setting, card setting and fingerprint information, from the controller(s) to the management computer. Select the controller from the controller list on the left, and then select the data to be uploaded on the right. Click “Save”  and a dialog box reporting “Operation succeeded” will pop up to confirm the uploading is complete.

Controller Setting: includes door setting, reader setting, arm zone and APB setting, alarm output setting, alarm output time setting and system setting etc. If the controller already exists in the system, the current setting in the Software will be replaced. The operation is the same as in section 5.25.2 “Search and Save”.

Card Setting: If a card already exists in the system, the current setting in the Software will not be overwritten. If the controller is a fingerprint controller and the card has been assigned to a cardholder, the fingerprint information will be uploaded. The cardholder’s fingerprint information and fingerprint type (“unknown type”) will be updated in the Software. This operation is the same as the second method of acquiring fingerprint information as described in section 4.2.2.1. If a card does not exist in the system, the card will be registered to the

Software automatically. The default access group is “Full Granted”; the default PIN is “000000”; the default setting for “First Card Enabled” and “Card Enabled” is enabled; the default card index is the same as card number; the default valid date is the current time (to the minute). Even if the controller is a fingerprint controller, because the card has not been assigned to a cardholder, fingerprint information will not be uploaded.

Acquire fingerprint from controller: this function only applies to fingerprint controllers. Only when a card exists in the Software, and the card has been assigned to a cardholder, will the card information stored in the controller be uploaded. The cardholder’s fingerprint information and fingerprint type (“unknown type”) will be updated in the Software. As described in the Card Setting above, this function is part of the card setting function. If multiple fingerprint controllers are selected, the fingerprint information from the last controller will be the information saved in the Software

8.2 Download Data to Controller

Click “Access Control Management” ➔ “Data Communication”, and select “Download data to Controller” from the drop-down menu to open the window for downloading data to controller (Fig. 8-2).

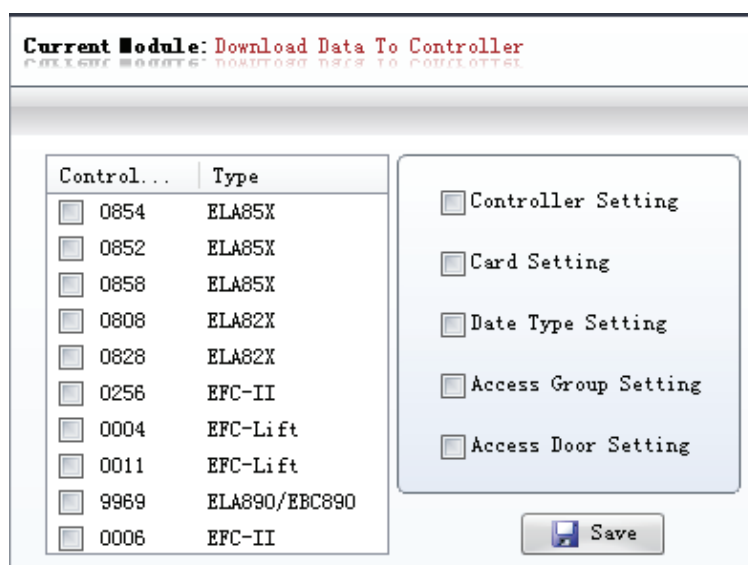
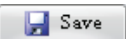


Fig. 8-2 Download Data to Controller

This operation is to download data from the Software, including controller setting, card setting, date setting, access group setting and door setting etc, to controllers. Select the controller from the controller list on the left, and then select the data to be downloaded on the right. Click “Save”  and a dialog box reporting “Operation succeeded” will pop up to confirm the downloading is complete.

Controller Setting: includes door setting, reader setting, arm zone setting, APB setting, alarm output setting, alarm output time setting and system setting etc.

Card Setting: downloads card settings from the Software to the selected controller. If the controller is a fingerprint controller, the fingerprint information will be downloaded to the

controller. **Note:** downloading card setting to controllers is different than enrolling cards to the controller. Whether a card is enrolled to a controller is determined by the access group to which the card belongs. A card is enrolled to a controller only when the access group to which it belongs is authorized to the controller. Refer to Section 6.4.4 Edit Access Group for details.

Date Setting: downloads date setting from the Software to the selected controller.

Access Group Setting: downloads access group setting from the Software to the selected controller.

Door Setting: downloads door setting from the Software to the selected controller.

8.3 Acquire Card and Fingerprint Information from Controller

If a card is enrolled to a controller and the fingerprint information is set in the controller, users can acquire card and fingerprint information from the controller by following the steps below. Fingerprint information is part of card information in the controller, but it is stored under cardholder information in the Software. To acquire card and fingerprint information:

1. Acquire card information: follow section 8.1 “card setting” to upload card information from the selected controller
2. Assign cardholders: Assign cardholders to the cards acquired from the controller. Follow section 7.3 Edit Card Information for details.
3. Acquire fingerprint: follow section 8.1 “Acquire fingerprint from controller” to upload fingerprint information to the cardholder in the Software.

8.4 Uploading/downloading Error

During uploading or downloading data, if the controller is not connected to the computer, a dialog box reporting “Timeout connecting controller to computer” will pop up. Check the communication system to make sure the controller is connected to the computer.

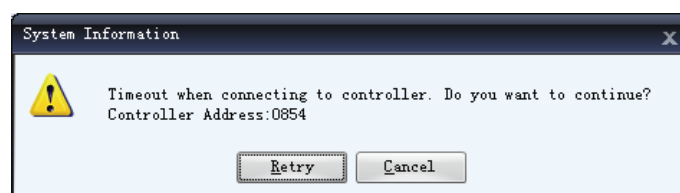


Fig. 8-3 Timeout when connecting to controller

During downloading data to controller, if the maximum number of cards allowed in the controller has been reached, a dialog box reporting “Fail to download data” will pop up. Check the cards in the controller and adjust accordingly.



Fig. 8-4 Download Data Fail

9 Electronic Map (E-Map) Management

Click “Access Control Management” → “Edit E-Map” to open the window for editing E-Map (Fig. 9-1).

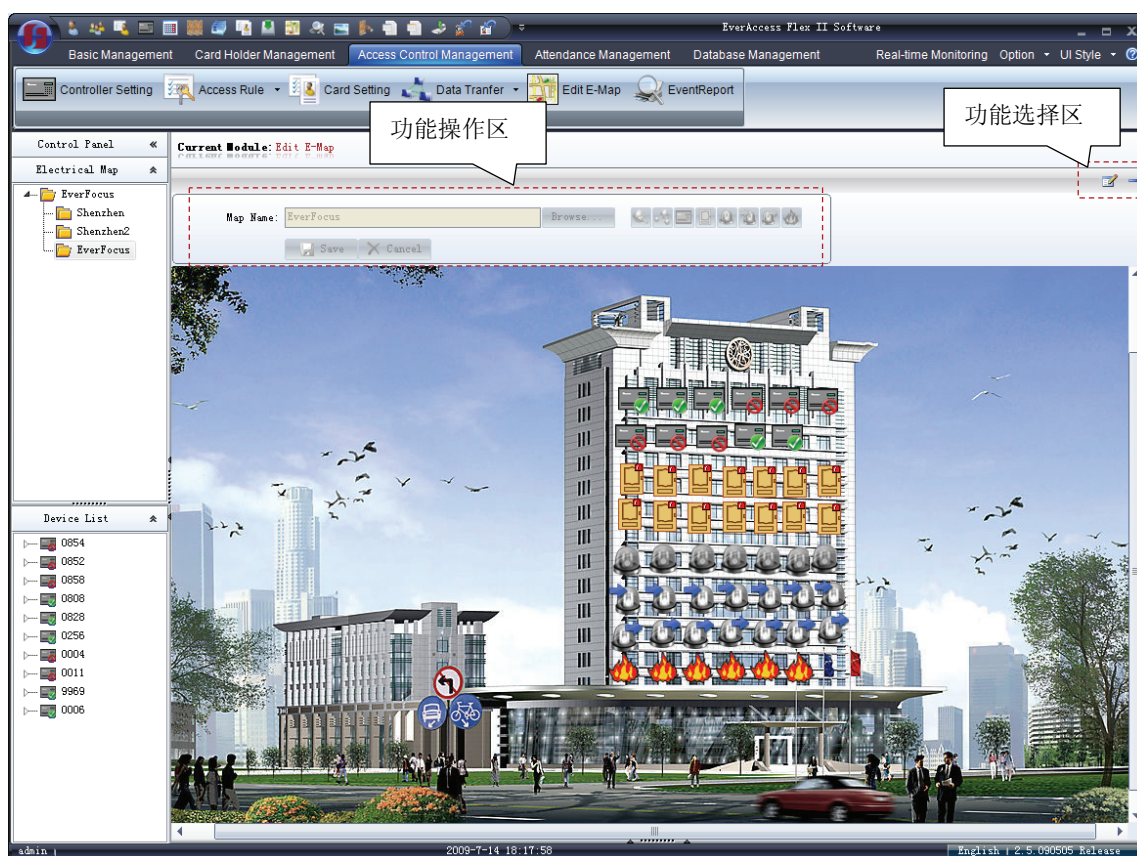


Fig. 9-1 Edit Electronic Map

Users can add child maps to an E-map and add links to other maps to show the layout of the entire area controlled by the System. Users can add controllers, doors, arm zones and fire alarms on the map to reflect their actual locations. In real-time monitoring mode, the status of devices will be shown in real time. Users can also exercise remote control over controllers and door zones in real time monitoring mode.

E-maps can be organized in a three-level menu (excludes the default root node). The default root node is “EleMap”. Users can rename the default root node. All added E-maps are child maps of the root node map.

9.1 Add an E-Map

From the E-map list on the left, select a node as the parent map of the map to be added. Click

“Edit” button  to enter editing mode. Click “Add link of child maps” button , and type in the name of the new map in the pop-up dialog box (Fig. 9-2). The default name is “Unknown Name”. Click “Browse” button and select the picture for the map, and then click

“Save”. Child-map link icon  will be added to the E-map, drag the mouse to appropriate position and click “Save”. A dialog box reporting “Operation succeeded” will pop up. The name of any E-map under the same parent map must be unique.

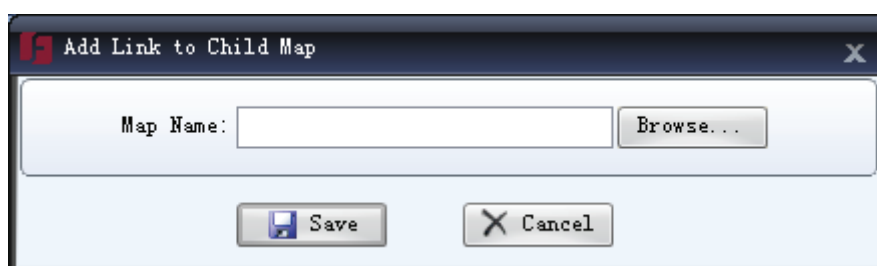


Fig. 9-2 Add E-Map Link

9.2 Add an E-Map link

Select a node from the E-map list on the left, under editing mode, click “Add E-map link” button , and select the map to be linked from the drop-down menu. A map-link icon



will be added on the map; drag the icon to the desired position and click “Save”.

This feature is mainly applicable when the map is too large, or covers multiple buildings and/or floors, and needs to be shown in multiple blocks. For example, if a company has a large production area that cannot be shown in one map, users can make two separate maps to represent “factory 1” and “factory 2” respectively. These two maps can then be linked using the above method for easy reference.

9.3 Add Devices to an E-map

Devices including controllers, door zones, arm zones and fire alarms can be added to an E-map. After adding the devices, click “Save”  and a dialog box reporting “Operation succeeded” will pop up.

9.3.1 Add Controllers

Click “Add Controllers” button , and all controllers in the system will be shown in a drop-down menu (Fig. 9-3). Select the controller to be added and a controller icon  will be shown on the upper left corner of the map. Drag the icon to the desired location.

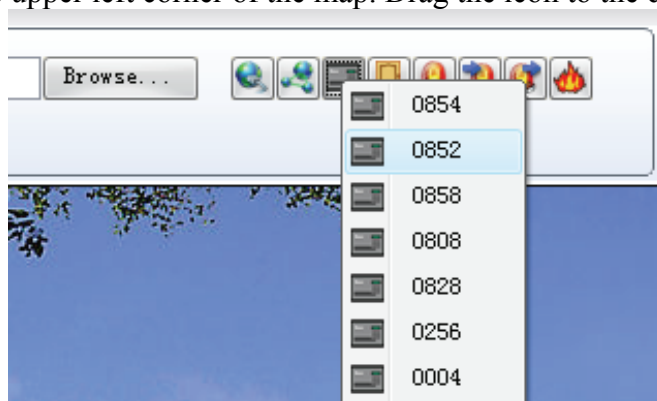


Fig. 9-3 Add Controllers

9.3.2 Add Doors

Click “Add Doors” button , and all doors in the system will be shown in a drop-down menu (Fig. 9-4). Select the door to be added and a door icon  will be shown on the upper left corner of the map. Drag the icon to the desired location.

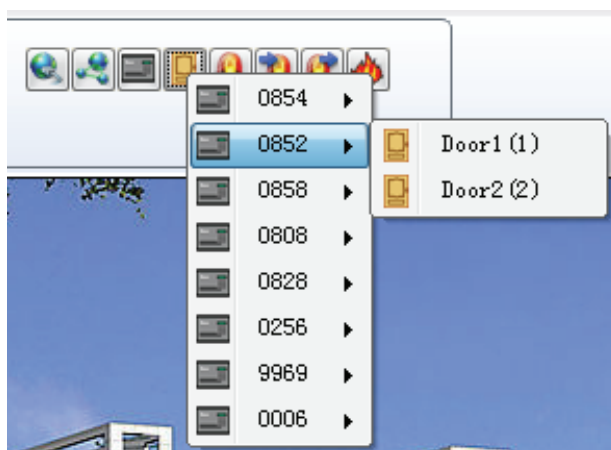


Fig. 9-4 Add Doors

9.3.3 Add ARM Zones

Click “Add ARM Zones” button , and all ARM zones corresponding to controllers other than Flex II controllers will be shown in a drop-down menu (Fig. 9-5). Select the arm zone to

be added and an arm zone icon  will be shown on the upper left corner of the map. Drag the icon to the desired location.

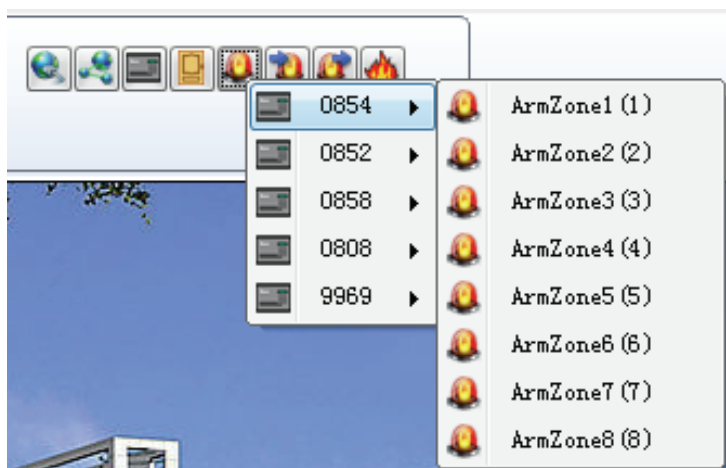


Fig. 9-5 Add ARM Zones

9.3.4 Add Alarm Inputs

Click “Add Alarm Inputs” button , and alarm inputs corresponding to Flex II controllers will be shown in a drop-down menu (Fig. 9-6). Select the alarm inputs to be added and an alarm input icon  will be shown on the upper left corner of the map. Drag the icon to the desired location.

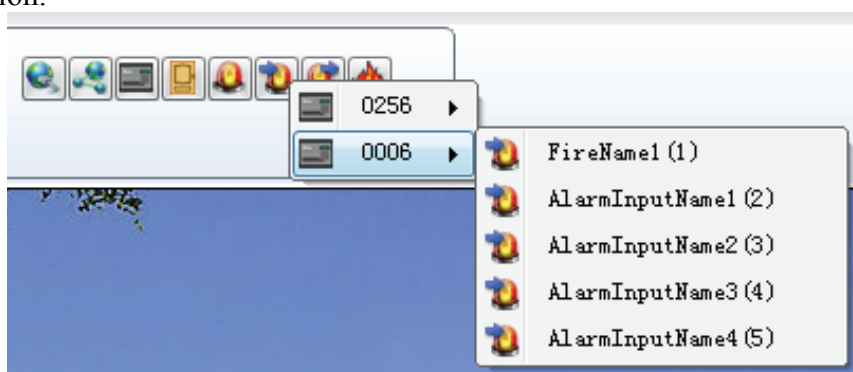


Fig. 9-6 Add Alarm Inputs

9.3.5 Add Alarm Outputs

Click “Add Alarm Outputs” button , and alarm outputs corresponding to Flex II controllers will be shown in a drop-down menu (Fig. 9-7). Select the alarm outputs to be added and an alarm output icon  will be shown on the upper left corner of the map. Drag the icon to the desired location.

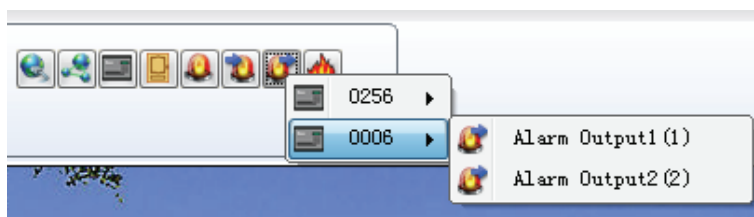


Fig. 9-7 Add Alarm Outputs

9.3.6 Add Fire Alarms

Click “Add Fire Alarms” button , and all fire alarms in the system will be shown in a drop-down menu (Fig. 9-8). Select the fire alarms to be added and a fire alarm icon  will be shown on the upper left corner of the map. Drag the icon to the desired location.

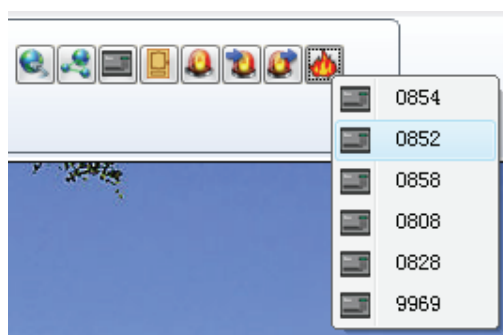


Fig. 9-8 Add Fire Alarms

9.4 Edit an E-Map

Select the map to be added from the E-map list on the left.

Edit name and picture file of an E-map

In editing mode, enter the name in the “Map Name” text box. Click the “Browse” button and select a picture file from the picture selection dialog. The system supported picture formats are BMP, JPG, GIF, ICO, and PNG. The maximum size of the image is 2048 * 1536. After selection, click “Save” to finish editing. Map names under the same parent map must be unique.

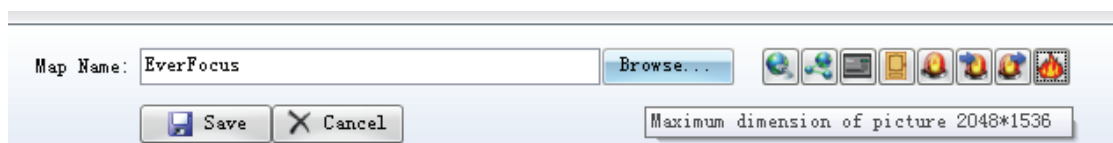


Fig. 9-9 Select E-map picture file

Remove icons from E-map

In editing mode, select the icon to be removed on the map, and then select “Remove” from the right-click menu (Fig. 9-10). Click “Save” when finished editing.

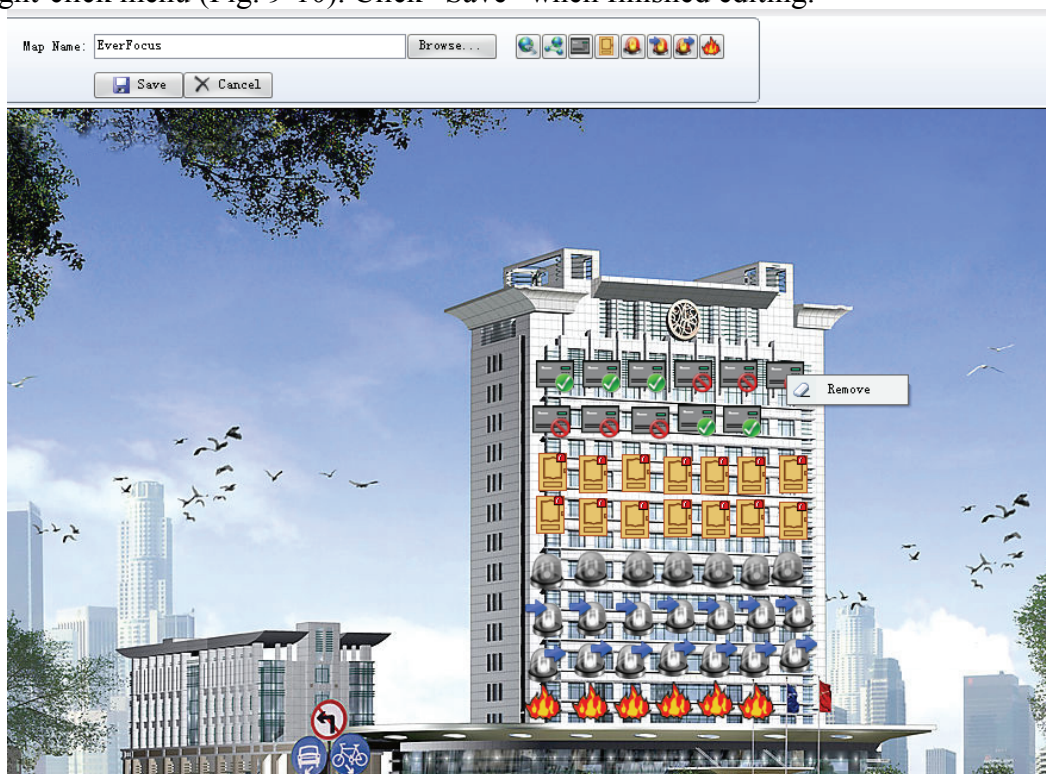


Fig. 9-10 Remove icons from an E-map

Note: When removing a link to a child map, the child map will be deleted. If the child map is a parent to its own child map, the link cannot be removed. If the child map does not refer to any child map, the link can be removed. At the same time, any link to the deleted map on other maps will be removed as well. Other icons such as controllers, doors, arm zones, fire alarms and links can be removed directly. Removing a link to a map that is a child of another map does not affect the linked map. For example, for map A and map B, map A contains child maps C and D. Map B has a link to map C. When editing map A, removing the link to map C will delete map C. Meanwhile, the link to map C on map B will be removed as well, because map C no longer exists. Please use care when taking steps that will delete files as well as links..

9.5 Delete an E-map

Select the map to be deleted from the map list on the left, click “Delete” button  in the function editing area and a dialog box will pop up to prompt users to confirm the deletion

Note: Deleting a map will delete all icons on the map. Links on other maps that connect to the deleted map will be removed as well. A map that contains child maps cannot be deleted.

Chapter 10

10 Event Report

Event report is used to record all events in the system. Click “Access Control Management” → “Event Report” to open the window for event report (Fig. 10-1).

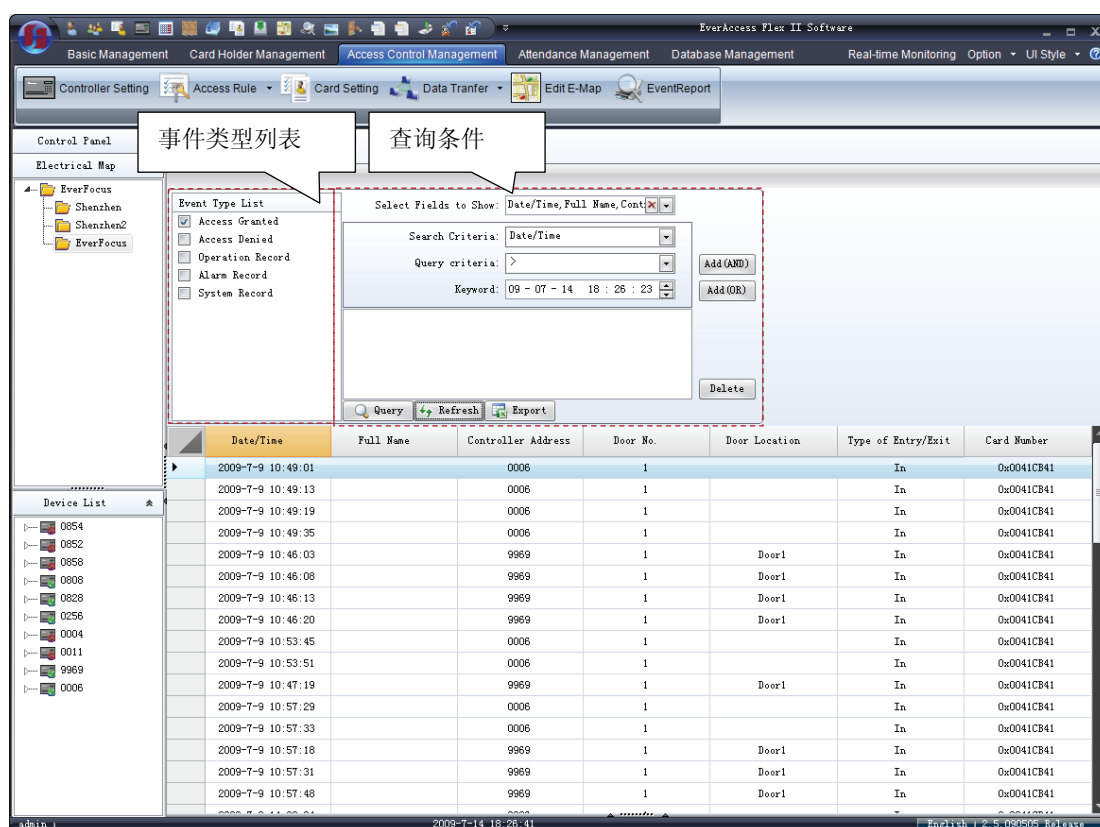


Fig. 10-1 Event Report

10.1 View Event Report

Select the event type from the event type list, click “Search”  button and all events of the selected type will be shown in the event list below. If multiple event types are selected, only search criteria shared by the selected event type will be shown in the resulted event list.

10.2 Sort Event Report

Click the title of a row at the top of the event list, and the displayed results will be sorted in ascending or descending order based on the selected item.

	Date/Time	Full Name	Controller Address	Door No.	Door Location	Type of Entry/Exit	Card Number
▶	2009-7-9 10:49:01		0006	1		In	0x0041CB41
	2009-7-9 10:49:13		0006	1		In	0x0041CB41
	2009-7-9 10:49:19		0006	1		In	0x0041CB41
	2009-7-9 10:49:35		0006	1		In	0x0041CB41
	2009-7-9 10:46:03		9969	1	Door1	In	0x0041CB41
	2009-7-9 10:46:08		9969	1	Door1	In	0x0041CB41
	2009-7-9 10:46:13		9969	1	Door1	In	0x0041CB41

Fig. 10-2 Sort Event Report

10.3 Search Event Report

Event reports contain event types and other search criteria.

There are 5 event types: access granted, access denied, operation record, alarm report and system record.

10.3.1 Search Criteria for Each Event Type

Search criteria are different for each event type. For access granted, the search criteria are: event date/time, cardholder name, controller address, Door No., Door Location, Entry/Exit type and card number, as shown in the figure below:

The screenshot shows a search criteria dialog box. On the left, under 'Event Type List', 'Access Granted' is selected with a checked checkbox. In the center, there are labels for 'Search Criteria:', 'Query criteria:', and 'Keyword:'. On the right, a list of search fields is shown with checkboxes: Date/Time, Full Name, Controller Address, Door No., Door Location, Type of Entry/Exit, and Card Number. All these checkboxes are checked. Above this list, a 'Select Fields to Show:' dropdown menu is open, displaying 'Date/Time, Full Name, Cont...' with a red 'X' icon and a downward arrow.

For access denied, the search criteria are: event date/time, cardholder name, controller address, Door No., Entry/Exit type, illegal event and card number, as shown in the figure below:

The screenshot shows the same search criteria dialog box, but now 'Access Denied' is selected in the 'Event Type List'. The search fields list on the right has been updated: 'Illegal Event' has been added with a checked checkbox, and 'Type of Entry/Exit' remains checked. All other checkboxes (Date/Time, Full Name, Controller Address, Door No., Door Location, Card Number) are still checked. The 'Select Fields to Show:' dropdown menu remains open, showing 'Date/Time, Full Name, Cont...'.

For operation record, the search criteria are: event date/time, operator name, controller address, door No., door location and event, as shown in the figure below:

The screenshot shows a search window with the following components:

- Event Type List:** A list of checkboxes where 'Operation Record' is selected (checked).
- Select Fields to Show:** A dropdown menu showing 'Date/Time, Operator, Contr'.
- Search Criteria:** A text input field.
- Query criteria:** A list of checkboxes where 'Date/Time', 'Operator', 'Controller Address', 'Door No.', 'Door Location', and 'Event' are all selected (checked).
- Keyword:** A text input field.

For alarm record, the search criteria are: event date/time, controller address, ARM No. and event type, as shown in the figure below:

The screenshot shows a search window with the following components:

- Event Type List:** A list of checkboxes where 'Alarm Record' is selected (checked).
- Select Fields to Show:** A dropdown menu showing 'Date/Time, Controller Add'.
- Search Criteria:** A text input field.
- Query criteria:** A list of checkboxes where 'Date/Time', 'Controller Address', 'Arm No.', and 'Event' are all selected (checked).
- Keyword:** A text input field.

For system record, the search criteria are: event date/time, controller address and event type, as shown in figure below:

The screenshot shows a search window with the following components:

- Event Type List:** A list of checkboxes where 'System Record' is selected (checked).
- Select Fields to Show:** A dropdown menu showing 'Date/Time, Controller Add'.
- Search Criteria:** A text input field.
- Query criteria:** A list of checkboxes where 'Date/Time', 'Controller Address', and 'Event' are all selected (checked).
- Keyword:** A text input field containing the value '09 - 07 - 14 18 : 32 : 45'.

10.3.2 Search Condition

Search conditions are different for each search criteria. For event time, the search conditions include: “=” (equal), “<” (not equal), “>” (greater than), “>=” (greater than or equal), “<” (less than”, “<=” (less than or equal), as shown below:

Select Fields to Show: Date/Time, Controller Address [X] [v]

Search Criteria: Date/Time [v]

Query criteria: [=] [v]

Keyword: [=] [v]

Options: Add (AND), Add (OR), Delete

The dialog box shows search criteria for 'Date/Time, Controller Address'. The 'Search Criteria' dropdown is set to 'Date/Time'. The 'Query criteria' and 'Keyword' dropdowns are both set to '='. To the right are buttons for 'Add (AND)', 'Add (OR)', and 'Delete'.

For cardholder name, the search conditions include: “=” (equal), “<” (not equal), “>” (greater than), “>=” (greater than or equal), “<” (less than), “<=” (less than or equal), includes (in any position), includes (starts with), and includes (ends with), as shown below:

Select Fields to Show: Date/Time, Full Name, Controller Address [X] [v]

Search Criteria: Full Name [v]

Query criteria: [=] [v]

Keyword: [=] [v]

Options: Add (AND), Add (OR), Delete

Buttons: Query, Refresh, Export

The dialog box shows search criteria for 'Date/Time, Full Name, Controller Address'. The 'Search Criteria' dropdown is set to 'Full Name'. The 'Query criteria' and 'Keyword' dropdowns are both set to '='. To the right are buttons for 'Add (AND)', 'Add (OR)', and 'Delete'. At the bottom are buttons for 'Query', 'Refresh', and 'Export'.

Search conditions for controller address, door No, In/Out type are the same as “Event Time”; search conditions for illegal events, card number and events are the same as “Cardholder Name”.

10.3.3 Search for Single Event Type

Steps to search for single event type:

- Select the event type from the event type list on the left
- Select display items and search criteria. If multiple criteria are needed, click “Add (And)” or “Add (Or)” to add additional search criteria to the

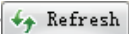
- search box. To delete a search criteria, check the box next to the search criteria, and click “Delete”  to delete the checked search criteria.
- c) After selecting all search criteria, click “Search” ; events that satisfy the search criteria will be shown in the event list.

10.3.4 Search for Multiple Event Types

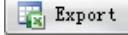
Steps to search for multiple event types:

- Select (check) multiple event types from the event type list on the left
- The system will automatically show the search criteria shared by the selected event type. Selected search criteria and use “Add (Add)”  or “Add (or)”  to add additional search criteria.
- After selecting all search criteria, click “Search” , events that satisfy the search criteria will be shown in the event list.

10.4 Refresh Event Report

Click “Refresh” , a fresh Event Report window will be populated, including the most recent events. All previously selected event types and event search criteria will be cleared. This operation is used to reset data.

10.5 Export Event Report

Event report can be exported in EXCEL file format. Click “Export”  to save the file. After the file is saved, the system will prompt to ask whether to open the file. If the user wants to view the file, click “Yes”.

Chapter 11

11 Device Control

11.1 Resources List

The resources list is located at the lower left of the main window (Fig. 11-1). The resources list contains real time information about all controllers and their attached devices in the system. Users can remotely operate controllers and doors including remote set/reset alarm, remote arm/disarm, remote unlock door, remote open/close/reset exterior area etc.

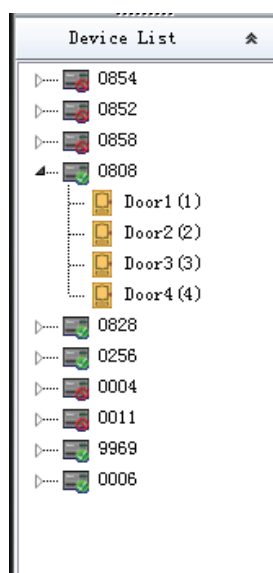


Fig. 11-1 Resources List

To show information about a controller, place mouse over the controller and a pop-up window will appear, as shown below:

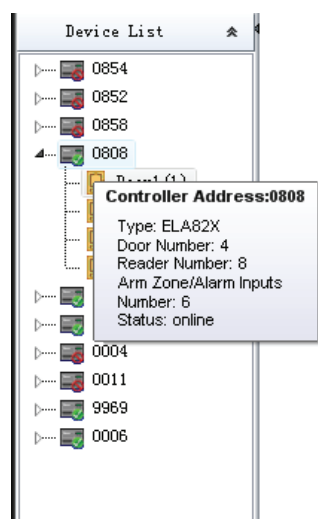


Fig. 11-2 Controller Information

11.2 Remote Set/Reset Alarm

In special circumstances, operators can remotely cause a controller to generate an alarm; for example, to warn other people in an area of an emergency situation.

Reset alarm is used to turn off *all* outputs, including alarm outputs, door-unlock control and door sensor outputs related to controller output relays (different types of controllers have different numbers of outputs). When a controller receives an alarm input, which can be generated if a door sensor detects unusual door opening or if there is an external alarm input, the controller will trigger the output relay to activate external alarm output devices and/or unlock doors. This controller operation depends on alarm settings (no door sensor setting is needed as door sensor detection is directly related to the door sensor output relay). When an alarm is reset, all output relays reset to turn off external alarm output devices and/or door-unlock control.

Right click on the icon for the controller to be operated, select “Remote Set Alarm” or “Remote Reset Alarm”, as shown below:

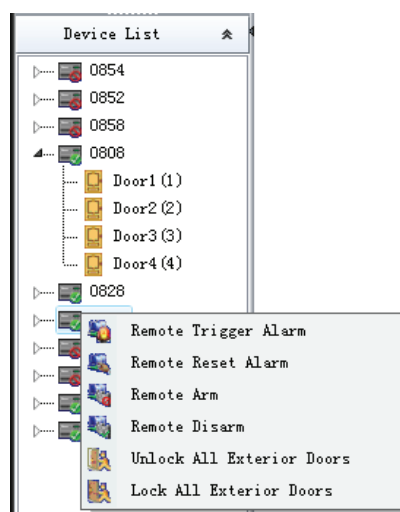


Fig. 11-3 Remote Set/Reset Alarm

11.3 Remote ARM/disarm

Remote arm/disarm is used to remotely enable/disable an ARM zone to change its arm/disarm setting.

Right click on the icon for the controller to be operated, select “Remote ARM” or “Remote Disarm” as shown below:

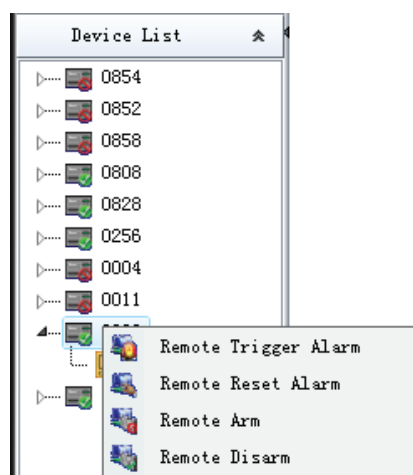


Fig. 11-4 Remote Arm/Disarm

11.4 Remote Open Door

Users can remotely open a door through the Software. Remote operation is necessary as the doors controlled by the Software are often at a long distance from the management computer. Remote open door can be used in several ways. For example, in the situation that a cardholder or visitor's identity needs to be verified before a door can be opened, managers can verify the cardholder's identity through closed circuit TV monitoring devices, and then remotely open the door once they are satisfied. Right click on the icon for the door to be operated, and select “Remote Open Door” as shown in below:

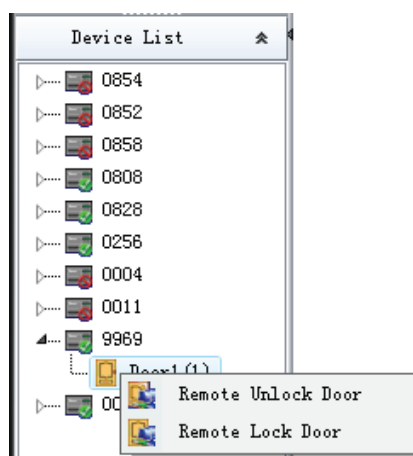


Fig. 11-5 Remote Open Door

Note: After a door is opened remotely, the door will be in a state of card permission access. This is different from a forced door open. EFC II controllers cannot be remotely controlled during a fire alarm condition; and the system returns operation timeouts

11.5 Remote Lock/Unlock Exterior Area

Users can remotely lock/unlock exterior areas on special occasions. For example, users can remotely lock all exterior areas if an intruder enters, or unlock all exterior areas in the event of a fire alarm. The doors can be reset to normal card permission access after the emergency condition no longer exists. Right click on the doors that need to be operated, select “Unlock All Exterior Doors” or “Lock All Exterior Doors”. To reset doors to normal card permission access, select “Reset”, as shown below:

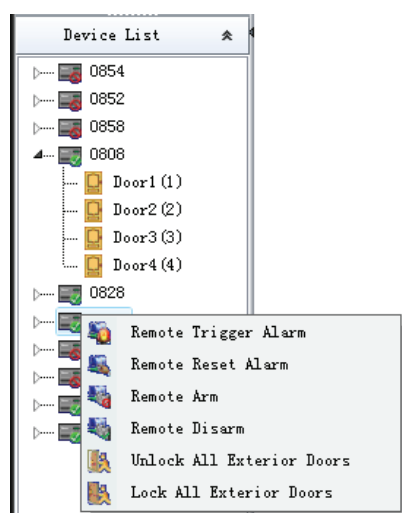


Fig. 11-6 Remote Unlock/Lock exterior area

Note: This operation is only applicable to Flex I series controllers that support exterior area operation.

Chapter 12

12 Attendance Management

12.1 Holiday Setting

Click “Attendance Management” ➔ “Holiday Setting” to open the window for holiday setting (Fig. 12-1).

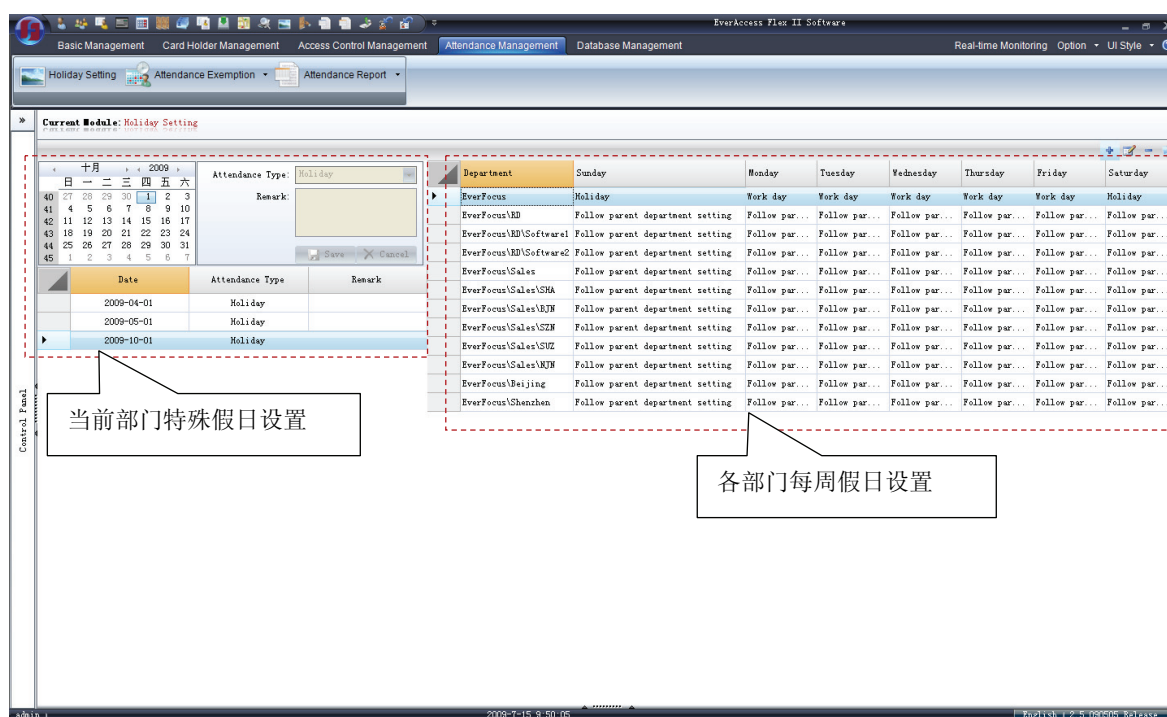


Fig. 12-1 Holiday Setting

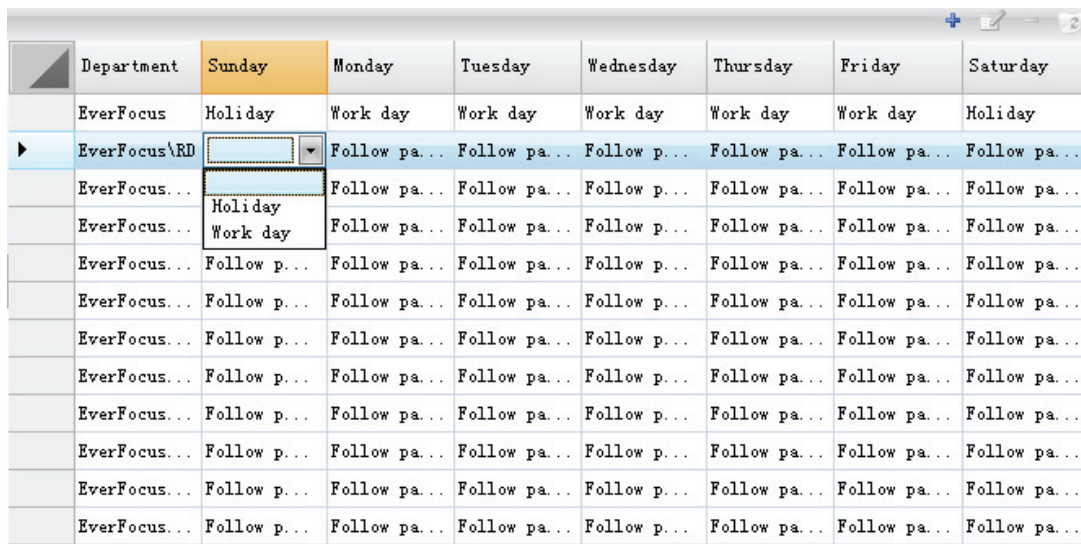
There are two parts in holiday setting in the Software: the first part is to set workdays and weekends during each week for every department (right panel), and the second part is to set special holidays for every department (left panel). The second part (special holiday setting) has higher priority than the first part (regular holiday setting). For example, if Thursday, April 2nd is set as a workday in the first part and a holiday in the second part, it is treated as a holiday. The default setting for the first part is: Monday to Friday is workdays and Saturday and Sunday are weekends (holidays).

Holiday setting priority: child department > department > company. The holiday setting in the company is the overall setting. If the setting is different for a department, the department setting is used for attendance management.

In the above figure, The company “Everfocus” Monday to Friday is set as workdays and Saturday and Sunday as weekend (holiday) days (the system default setting). Three departments, Research and Development, Production Group A and Production Group B set

Saturday as a workday. Based on the rule “department > company”, for Research and Development, Production Group A and Production Group B, Monday to Saturday are workdays. All other departments follow the company’s setting in which Monday to Friday are workdays, and Saturday and Sunday are ‘holidays’ (non working days).

12.1.1 Department Week Holiday Setting

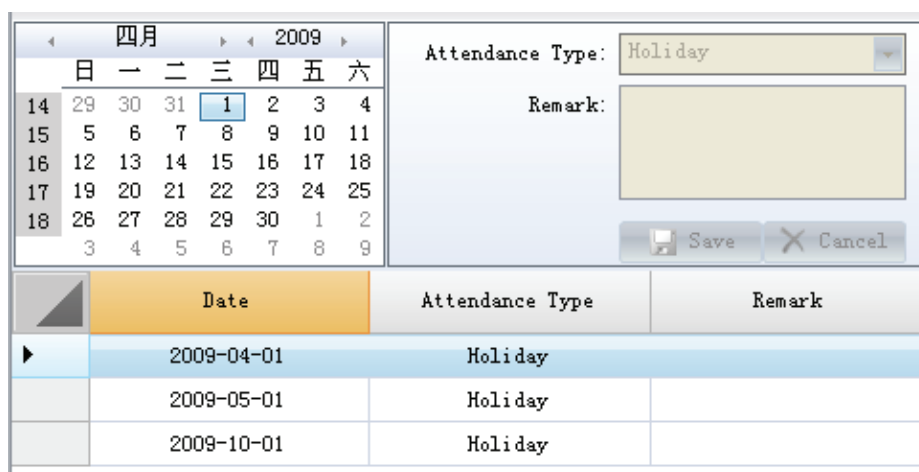


Department	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
EverFocus	Holiday	Work day	Work day	Work day	Work day	Work day	Holiday
EverFocus\RD	Holiday	Follow pa...	Follow pa...	Follow p...	Follow pa...	Follow pa...	Follow pa...
EverFocus...	Holiday	Follow pa...	Follow pa...	Follow p...	Follow pa...	Follow pa...	Follow pa...
EverFocus...	Holiday	Follow pa...	Follow pa...	Follow p...	Follow pa...	Follow pa...	Follow pa...
EverFocus...	Work day	Follow pa...	Follow pa...	Follow p...	Follow pa...	Follow pa...	Follow pa...
EverFocus...	Follow p...	Follow pa...	Follow pa...	Follow p...	Follow pa...	Follow pa...	Follow pa...
EverFocus...	Follow p...	Follow pa...	Follow pa...	Follow p...	Follow pa...	Follow pa...	Follow pa...
EverFocus...	Follow p...	Follow pa...	Follow pa...	Follow p...	Follow pa...	Follow pa...	Follow pa...
EverFocus...	Follow p...	Follow pa...	Follow pa...	Follow p...	Follow pa...	Follow pa...	Follow pa...
EverFocus...	Follow p...	Follow pa...	Follow pa...	Follow p...	Follow pa...	Follow pa...	Follow pa...
EverFocus...	Follow p...	Follow pa...	Follow pa...	Follow p...	Follow pa...	Follow pa...	Follow pa...
EverFocus...	Follow p...	Follow pa...	Follow pa...	Follow p...	Follow pa...	Follow pa...	Follow pa...
EverFocus...	Follow p...	Follow pa...	Follow pa...	Follow p...	Follow pa...	Follow pa...	Follow pa...
EverFocus...	Follow p...	Follow pa...	Follow pa...	Follow p...	Follow pa...	Follow pa...	Follow pa...
EverFocus...	Follow p...	Follow pa...	Follow pa...	Follow p...	Follow pa...	Follow pa...	Follow pa...
EverFocus...	Follow p...	Follow pa...	Follow pa...	Follow p...	Follow pa...	Follow pa...	Follow pa...
EverFocus...	Follow p...	Follow pa...	Follow pa...	Follow p...	Follow pa...	Follow pa...	Follow pa...
EverFocus...	Follow p...	Follow pa...	Follow pa...	Follow p...	Follow pa...	Follow pa...	Follow pa...
EverFocus...	Follow p...	Follow pa...	Follow pa...	Follow p...	Follow pa...	Follow pa...	Follow pa...

Fig. 12-2 Department Week Holiday Setting

In the above figure, below the yellow bar one sees the overall holiday setting for the company. To change the holiday setting for a department, highlight the cell for that Department and day, then select from “default”, “workday” and “holiday” from the drop-down menu for each day of the week.

12.1.2 Department Special Holiday Setting



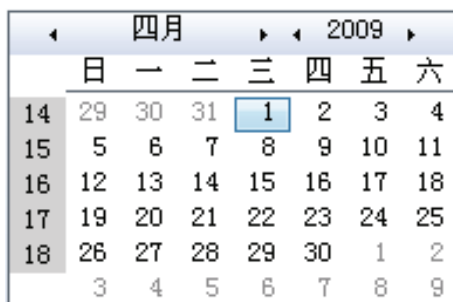
Date	Attendance Type	Remark
2009-04-01	Holiday	
2009-05-01	Holiday	
2009-10-01	Holiday	

Fig. 12-3 Special Holiday Setting for current department

The section above is to set the routine work week and weekend days off (holiday_ for each department, while this section is to set special holidays for each department.

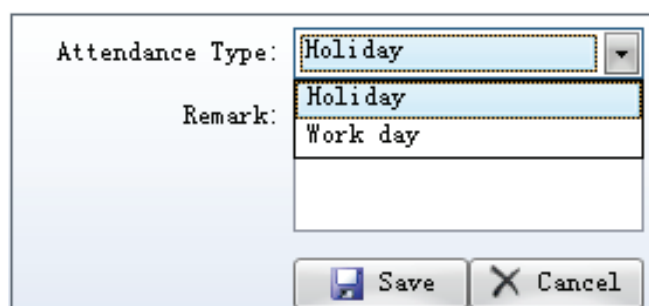
12.1.3 Add a Holiday

Select “EverFocus” from the department list. This row is used for company setting. Click the “Add” button  in the “function editing area” (the icons in  represent add, edit, delete and delete all respectively from left to right). Select a Year, Month and Date from the calendar on the left (Fig. 12-4). Click “forward”  or “backward”  button besides “year” and “month” to select year and month, and click the date in the field to select a date. The selected date will be highlighted in yellow. Click “Attendance type” on the right and select “holiday” from the drop-down menu. Users can enter remarks in the remark field, such as “National Holiday” (Fig. 12-5). When finished, click the “save” button  and a dialog box reporting “Operation succeeded” will pop up. The setting of October, 1, 2009 as a company holiday for EverFocus is now complete.



		四月				2009	
	日	一	二	三	四	五	六
14	29	30	31	1	2	3	4
15	5	6	7	8	9	10	11
16	12	13	14	15	16	17	18
17	19	20	21	22	23	24	25
18	26	27	28	29	30	1	2
	3	4	5	6	7	8	9

Fig. 12-4 Holiday Setting: Date Selection



Attendance Type:

Remark:

 Save  Cancel

Fig. 12-5 Holiday Setting: Attendance Type

12.1.4 Edit a Holiday

To edit a holiday for a department, select the department and the date to be edited, click the “Edit” button . User can edit date selection, attendance type and remarks. When finished, click “Save” button  and a dialog box reporting “Operation succeeded” will pop up.

12.1.5 Delete Holiday(s)

To delete holiday(s) for a department, select the holiday or use the “Ctrl” key on the keyboard to select multiple holidays, and click the “Delete” button. A dialog box will be shown to prompt users to confirm the deletion. Click “Yes” to delete the holiday(s) and another dialog box reporting “Operation succeeded” will be shown.

To delete all holidays for a department, select the department and click “Delete All” button. A dialog box will be shown to prompt users to confirm the deletion. Click “Yes” to delete all holidays and another dialog box reporting “Operation succeeded” will be shown.

12.2 Event Management

12.2.1 No-Access-Attendance Enrollment

If an employee cannot swipe their card due to business travel or other reasons, a “no-access-attendance” event should be recorded to reflect the actual attendance. Click “Attendance Management” → “Event Management”, and select “No-Access-Attendance Enrollment” from the drop-down menu to open the window for no-access-attendance enrollment (Fig. 12-6).

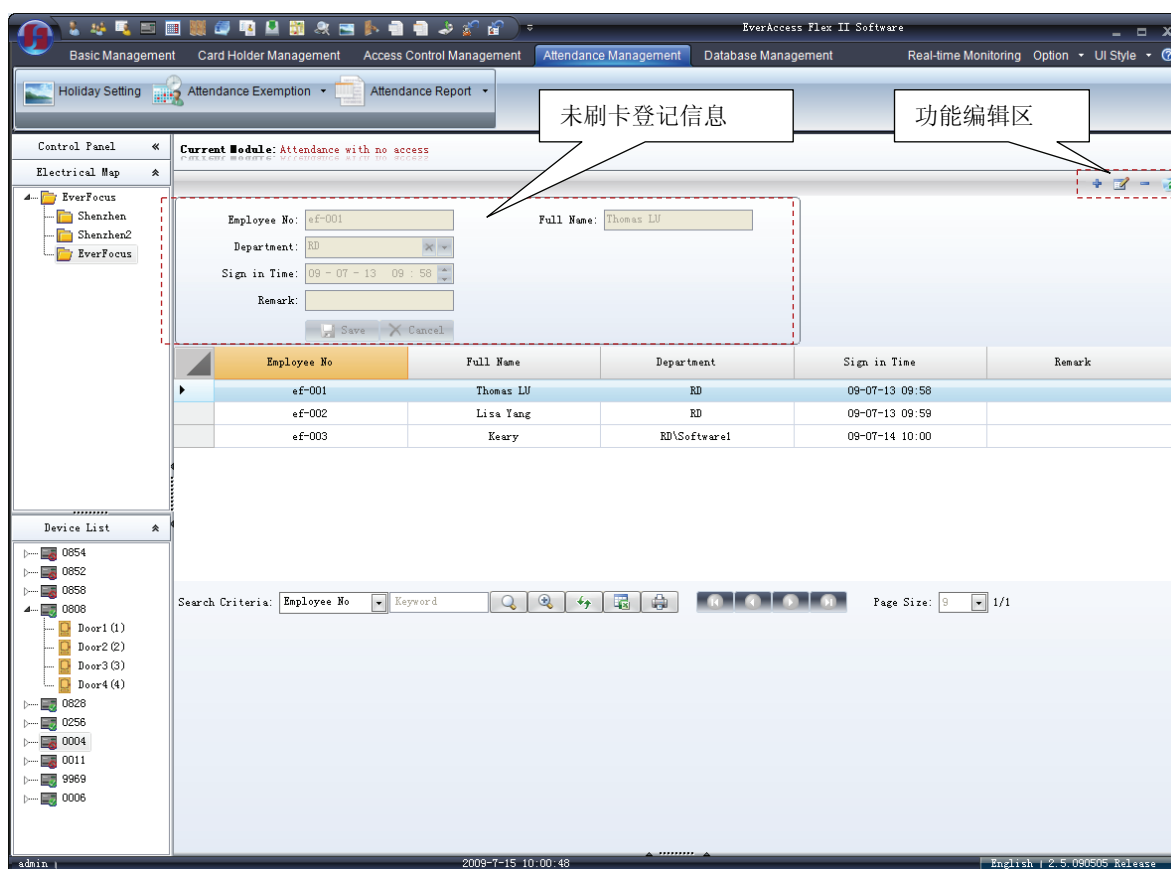


Fig. 12-6 No-access-attendance Enrollment

12.2.1.1 Add a No-Access-Attendance enrollment

Click the “Add” button  in the “function editing area” (Fig. 12-6), and the window for no-access-attendance enrollment will be shown (Fig. 12-7).

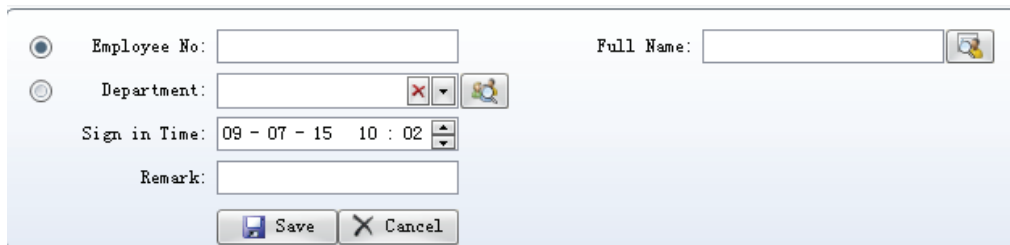


Fig. 12-7 Add a No-Access-Attendance

✧ Search by employee’s information

Check the button  in front of “employee number”, and enter the employee number and/or employee name in the related field. Click “search employee” button . If the employee cannot be found based on the search criteria, the system will return “employee not found or incomplete information”. Check to make sure the information entered is correct. When found, employee number and name will be shown in their respective fields.

Note: When an employee is found, the employee number and name will be shown in the related field. Editing the employee number and/or name without clicking the “search employee” button will not affect the change result. In other words, the system will show the results of the last click of “search employee” button. This rule also applies to search function under other functional modules in the Software.

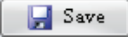
✧ Search by a employee’s department

Check the button  in front of “department”, and select a department from the drop down menu, and then click “search employees by department” button . A dialog box showing the employee list of the selected department and its child departments will pop up. Double click an employee or click on an employee and then click close to close the window. The employee number and name will be shown in the related text field. Users can only select one employee at a time from the employee list dialog box.

Note: If the  button on the line with ‘Department’ is not checked, clicking  will not perform the task. This rule also applies to all types of functions under other modules in the Software.

Edit Attendance Time: click on the item in the time field to be edited, enter the new time from the keyboard or by using the up-and-down buttons  on the right to choose a time. When finished, click “Save”  on the right and a dialog box reporting “Operation succeeded” will pop up.

12.2.1.2 Edit a No-Access-Attendance Enrollment

Select the no-access-attendance to be edited, click the “Edit” button  to edit the time and/or remarks. When finished, click “Save” button  and a dialog box reporting “Operation succeeded” will pop up.

12.2.1.3 Delete No-Access-Attendance Enrollment(s)

✧ Delete specific no-access-attendance enrollment(s)

Select one no-access-attendance enrollment from the list, or drag the mouse across multiple adjacent enrollments, or use the “Ctrl” key on the keyboard to select nonadjacent enrollments. After selecting the enrollments to be deleted, click the “Delete”  button in the “Function editing area”. A dialog box will pop up to prompt users to confirm the deletion. Click “Yes” to delete the enrollment(s) and another dialog box reporting “Operation Succeeded” will pop up. Otherwise, click “Cancel” to exit.

✧ Delete all no-access-attendance enrollments

Click the “Delete All”  button in the “Function editing area”. A dialog box will pop up to prompt users to confirm the deletion. Click “Yes” to delete all no-access-attendance enrollments and another dialog box reporting “Operation Succeeded” will pop up. The number of the enrollments deleted will also be shown. Otherwise, click “Cancel” to exit.

12.2.1.4 Search No-Access-Attendance Enrollments

Users can search, export and print no-access-attendance enrollments using the search tool bar located at the bottom of the window (Fig. 12-8).

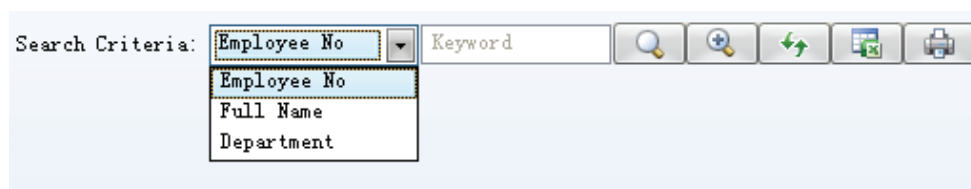


Fig. 12-8 Search, Export and Print No-Access-Attendance Enrollments

There are 3 search criteria for no-access-attendance enrollments. Select a search criterion from the drop-down menu and enter related keywords. This quick search function does not support inexact or ‘wildcard’ search. See Advanced Search below for those capabilities. Click “Search” button  and the employee’s enrollment records will be shown on the event list in the middle.

12.2.1.5 Advanced Search of No-Access-Attendance Enrollments

To search by multiple search criteria, click “Advanced Search”  to open the window for advanced search (Fig. 12-9).

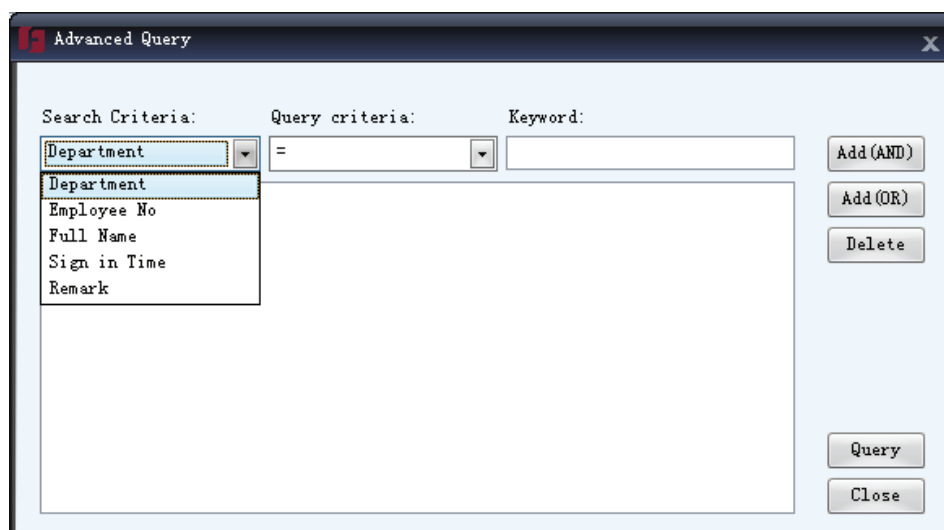


Fig. 12-9 Advanced Search

Search criteria: the name of search items, including department name, employee number, name and attendance time.

Condition: the matching condition to the search criteria, such as “=” (equal), “<>” (not equal), “>” (greater than), “>=” (greater than or equal”, “<” (less than”, “<=” (less than or equal), “includes (in any position)” “includes (starts with)”, “includes (ends with)”.

Keywords: enter or select the contents that match the search criteria.

Add (and): search for enrollments that match all conditions in two or more search criteria.

Add (or): search for enrollments that match any of the conditions in two or more search criteria.

Delete: to delete the search condition in the searching criteria list. Check the search criteria to be deleted and click “Delete”.

Click on the selection box of search criteria and condition, and select the search criteria and condition from the drop-down menu. Enter keywords matching the search criteria. Then click “Add (and)” or “Add (or)” on the right to add additional search criteria. The search criteria will be listed on the box at the lower left. Click “Search”  and enrollments that satisfy the search criteria will be shown in the event list. To delete search criteria, check the box before the search criteria, and click “Delete”.

12.2.1.6 Refresh No-Access-Attendance Enrollments

Click “Refresh”  in the “search tool bar” to show the current no-access-attendance enrollment list.

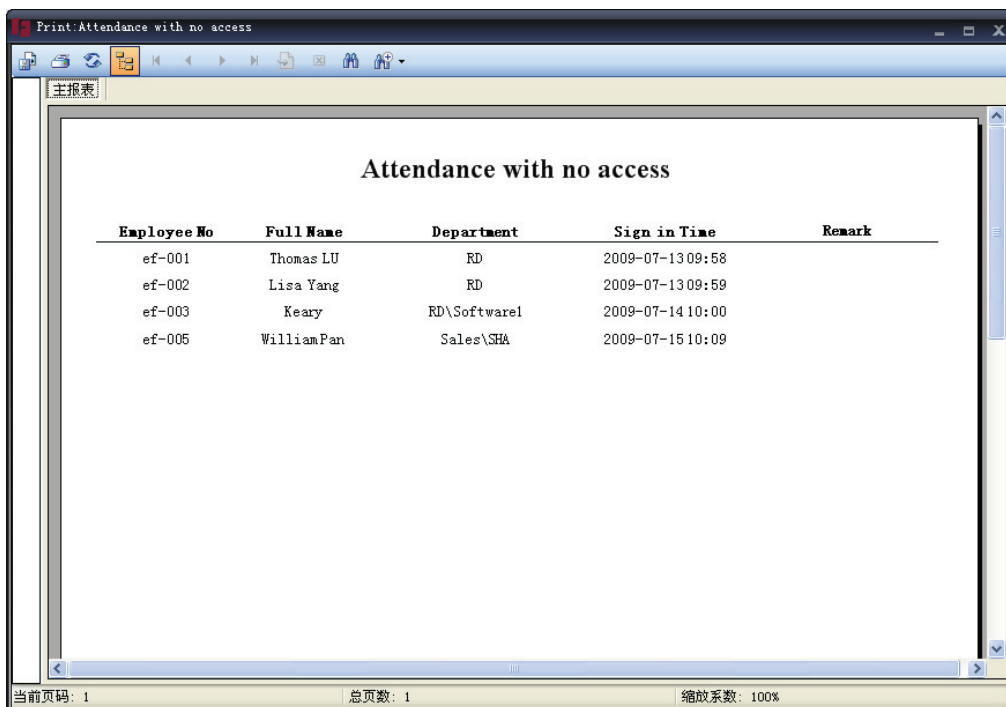
12.2.1.7 Export No-Access-Attendance Enrollments

Click “Export”  in the “search tool bar”, a dialog box will pop up to show that the employee information is being exported as an Excel file. When finished exporting, another

dialog box will pop up to ask whether to open the file. Click “Yes” to view the file, otherwise, click “No”.

12.2.1.8 Print No-Access-Attendance Enrollments

Click “Print”  in the “search tool bar” to open the window for printing no-access-attendance enrollments (Fig. 12-10). The menu bar includes: export, print, refresh, switch node, go to the first page, go to last page, go to next page, go to the last page, go to page, close, search text, zoom in/out etc.



Employee No	Full Name	Department	Sign in Time	Remark
ef-001	Thomas LU	RD	2009-07-13 09:58	
ef-002	Lisa Yang	RD	2009-07-13 09:59	
ef-003	Keary	RD\Software1	2009-07-14 10:00	
ef-005	WilliamPan	Sales\SHA	2009-07-15 10:09	

Fig. 12-10 Print No-Access-Attendance Enrollments

12.2.2 Overtime Enrollment

Click “Attendance Management” → “Event Management”, and select “Overtime Enrollment” from the drop-down menu to open the window for overtime enrollment (Fig. 12-11).

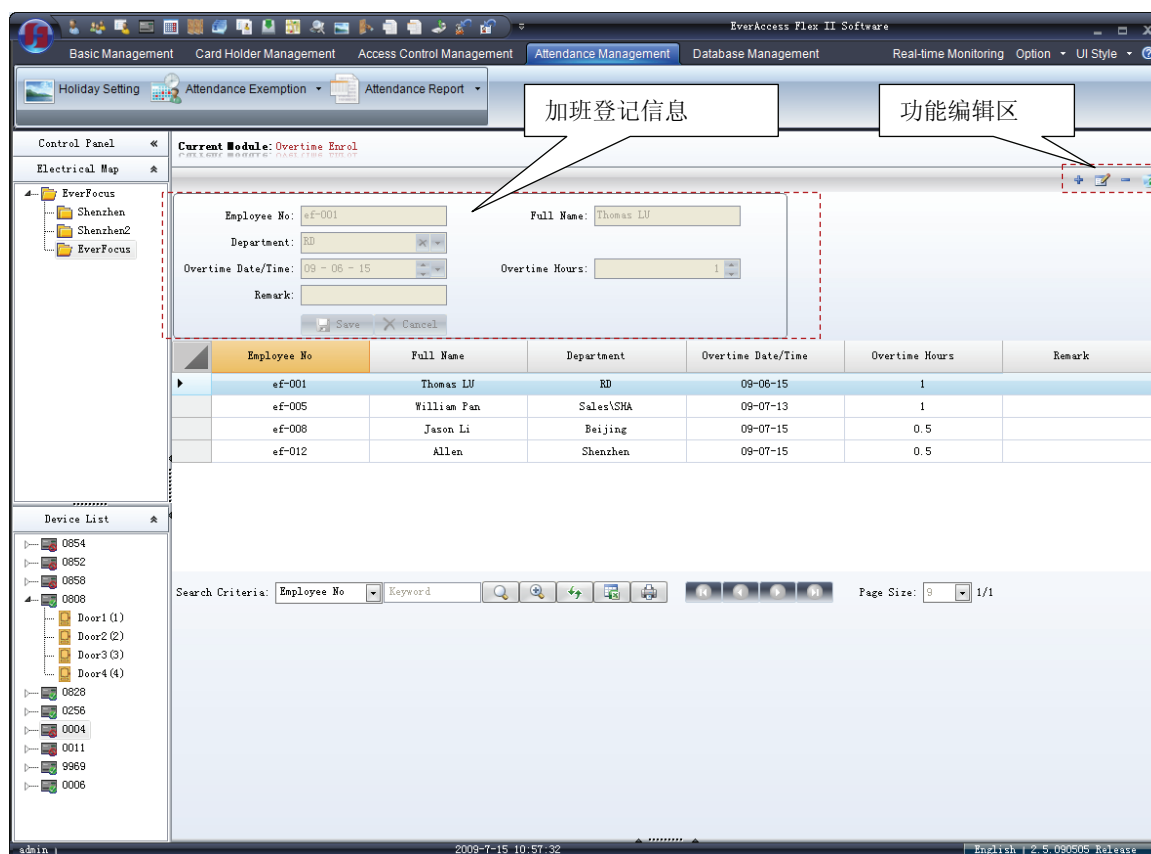


Fig. 12-11 Overtime Record

12.2.2.1 Add Overtime Enrollments

Click the “Add” button  in the “function editing area” to open the window for adding overtime enrollment (Fig. 12-12). Users can select a department and add overtime enrollments for all employees in the selected department and its child department.

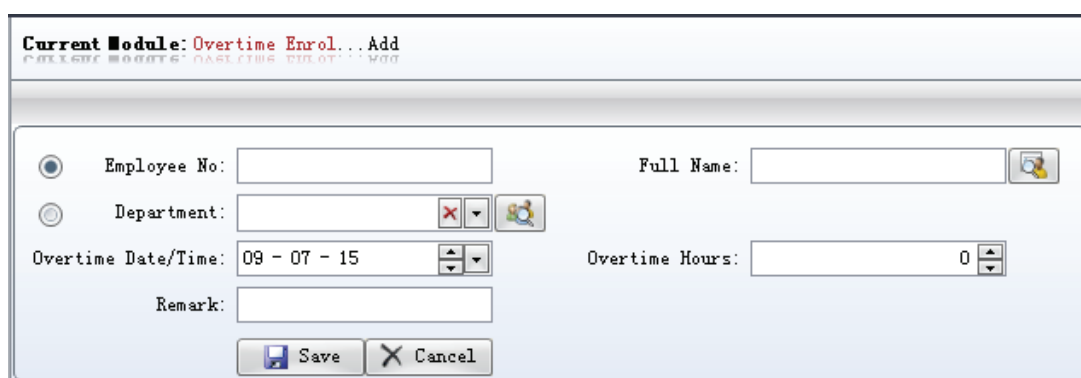


Fig. 12-12 Add Overtime Enrollment(s)

- ✧ Search by employee's information
Similar as “Add a non-access-attendance enrollment”. Refer to Section 12.2.1.1 for details.
- ✧ Select one or multiple employees from a department

Check the button  in front of “department”, and select a department from the drop-down menu, and then click “search employees by department” button . A dialog box showing the employee list of the selected department and its child departments will pop up (Fig. 12-13). Check the boxes in front of the employees to be added or double click an employee. Click the title row of employee number will select/deselect all employees.

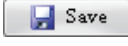
Note: If no boxes are checked, it will be treated as if all employees are selected from the department.



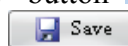
Fig. 12-13 Search Specific Employees

Overtime Date: click on the item to be edited, i.e. click Month if to change month, type in the date from keyboard or using the up-and-down buttons  to select dates.

Overtime Hours: the minimum value is 0.5 hour and the maximum is 24 hours. Overtime hours cannot be left empty.

When finished, click “Save”  on the right and a dialog box reporting “Operation succeeded” will pop up.

12.2.2.2 Edit an Overtime Enrollment

Select the overtime enrollment to be edited, click the “Edit” button  to edit the date, hours and remarks. When finished, click “Save” button  and a dialog box reporting “Operation succeeded” will pop up.

12.2.2.3 Delete Overtime Enrollment(s)

✧ Delete specific overtime enrollment(s)

Select one overtime enrollment from the list, or drag the mouse across multiple adjacent enrollments, or use the “Ctrl” key on the keyboard to select nonadjacent enrollments. After selecting the enrollments to be deleted, click the “Delete”  button in the “Function editing area”. A dialog box will pop up to prompt users to confirm the deletion. Click “Yes” to delete

the enrollment(s) and another dialog box reporting “Operation Succeeded” will pop up. Otherwise, click “Cancel” to exit.

✧ Delete all overtime enrollments

Click the “Delete All”  button in the “Function editing area”. A dialog box will pop up to prompt users to confirm the deletion. Click “Yes” to delete all overtime enrollments and another dialog box reporting “Operation Succeeded” will pop up. The number of the enrollments deleted will also be shown. Otherwise, click “Cancel” to exit.

12.2.2.4 Search Overtime Enrollments

Users can search, export and print overtime enrollments using the search tool bar located at the bottom of the window (Fig. 12-14).

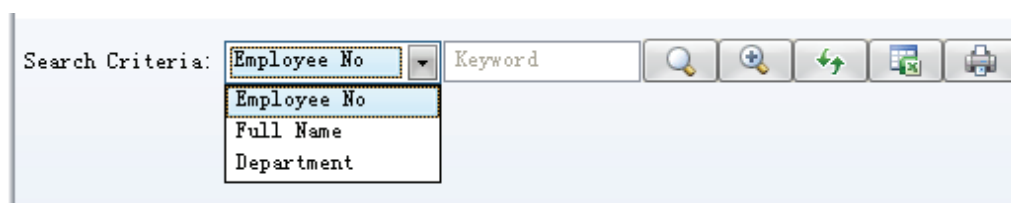


Fig. 12-14 Search, Export and Print Overtime Enrollments

There are 3 search criteria for overtime enrollments. Select a search criterion from the drop-down menu and enter related keywords. This quick search function does not support inexact or ‘wildcard’ search. See Advanced Search below for those capabilities. Click the “Search” button  and the employees’ enrollment records will be shown on the event list in the middle.

12.2.2.5 Advanced Search of Overtime Enrollments

To search by multiple search criteria, click “Advanced Search”  to open the window for advanced search (Fig. 12-15).

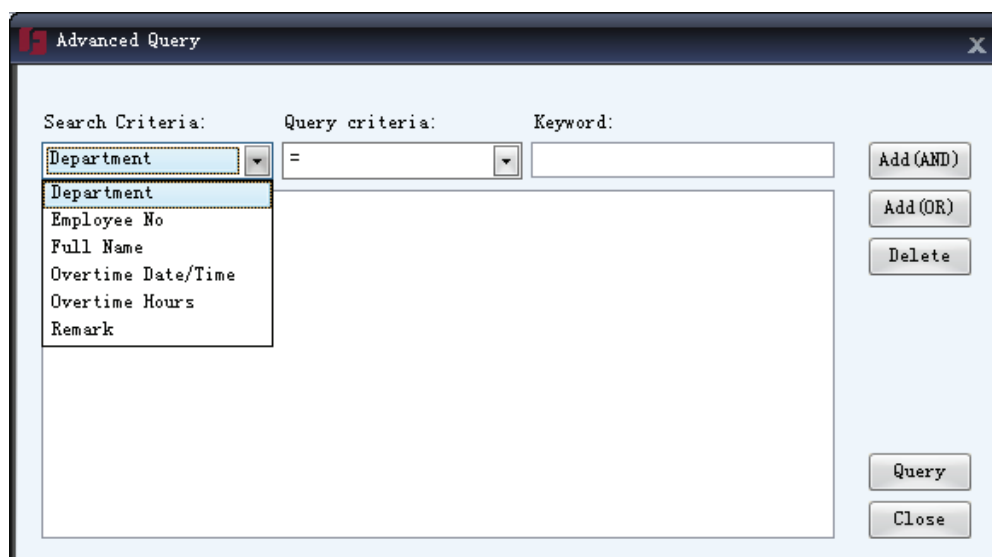


Fig. 12-15 Advanced Search

Search criteria: the name of search items, including department name, employee number, name, overtime date, overtime hours and remarks.

Condition: the matching condition to the search criteria, such as “=” (equal), “<>” (not equal), “>” (greater than), “>=” (greater than or equal”, “<” (less than”, “<=” (less than or equal), “includes (in any position)” “includes (starts with)”, “includes (ends with)”.

Keywords: enter or select the contents that match the search criteria.

Add (and): search for enrollments that match all conditions in two or more search criteria.

Add (or): search for enrollments that match any of the conditions in two or more search criteria.

Delete: to delete the search condition in the searching criteria list. Check the search criteria to be deleted and click “Delete”.

Click on the selection box of search criteria and condition, and select the search criteria and condition from the drop-down menu. Enter keywords match the search criteria. Then click “Add (and)” or “Add (or)” on the right to add additional search criteria. The search criteria will be listed on the box at the lower left. Click “Search”  and enrollments that satisfy the search criteria will be shown in the event list. To delete search criteria, check the box before the search criteria, and click “Delete”.

12.2.2.6 Refresh Overtime Enrollments

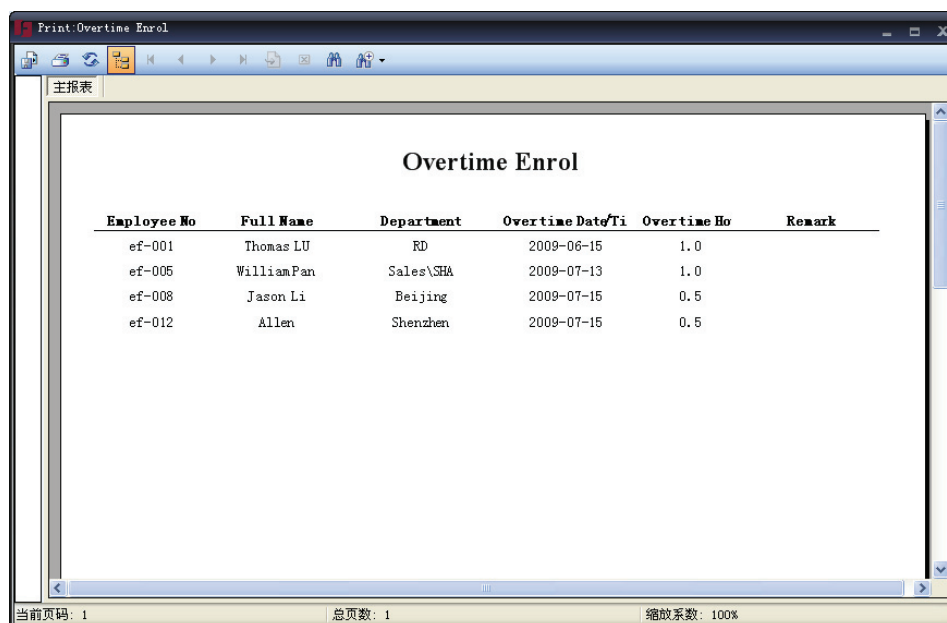
Click “Refresh”  in the “search tool bar” to show the current overtime enrollment list.

12.2.2.7 Export Overtime Enrollments

Click “Export”  in the “search tool bar”, a dialog box will pop up to show that the employee information is being exported as an Excel file. When finished exporting, another dialog box will pop up to ask whether to open the file. Click “Yes” to view the file, otherwise, click “No”.

12.2.2.8 Print Overtime Enrollments

Click “Print”  in the “search tool bar” to open the window for printing overtime enrollments (Fig. 12-16). The menu bar includes: export, print, refresh, switch node, go to the first page, go to last page, go to next page, go to the last page, go to page, close, search text, zoom in/out etc.



The screenshot shows a window titled "Print Overtime Enrol". Inside, there is a table with the following data:

Employee No	Full Name	Department	Overtime Date/Ti	Overtime Ho	Remark
ef-001	Thomas LU	RD	2009-06-15	1.0	
ef-005	William Pan	Sales\SHA	2009-07-13	1.0	
ef-008	Jason Li	Beijing	2009-07-15	0.5	
ef-012	Allen	Shenzhen	2009-07-15	0.5	

At the bottom of the window, there is a status bar with the following information: 当前页码: 1, 总页数: 1, 缩放系数: 100%.

Fig. 12-16 Print Overtime Enrollments

12.2.3 Time-off Enrollment

Click “Attendance Management” → “Event Management”, and select “Time-off Enrollment” from the drop-down menu to open the window for time-off enrollment (Fig. 12-17).

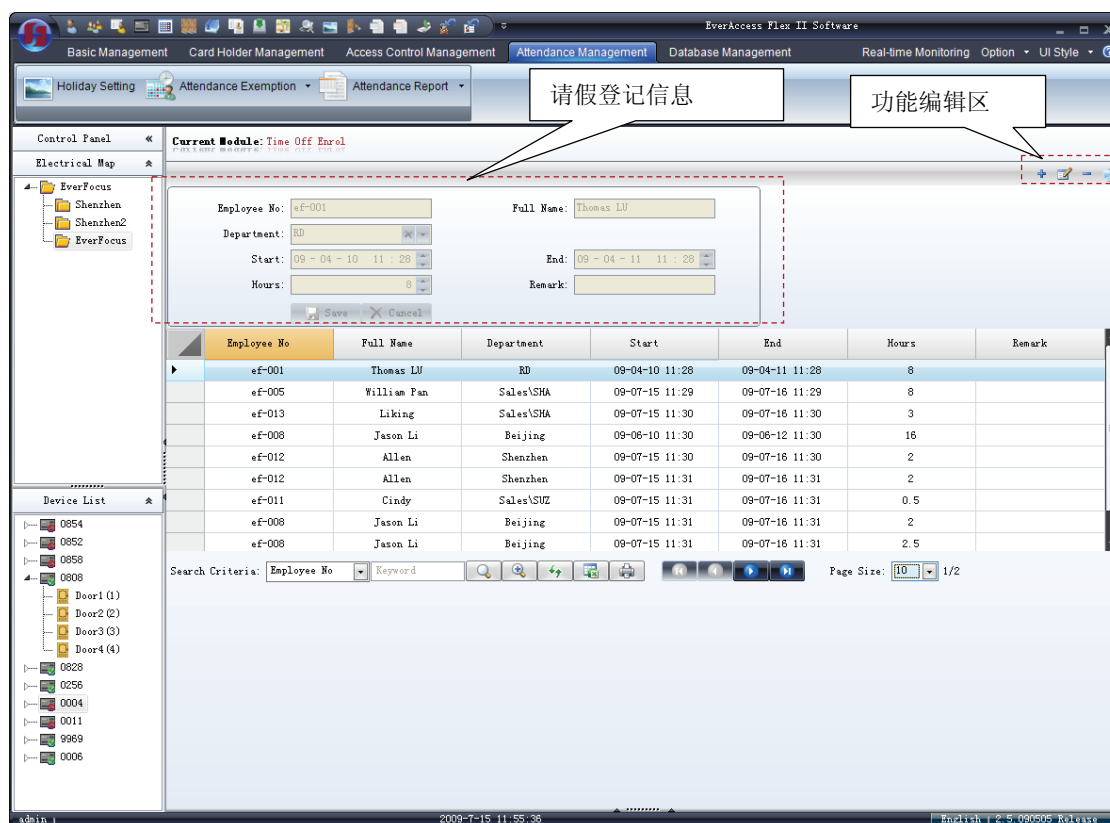


Fig. 12-17 Time-off Enrollment

12.2.3.1 Add a Time-off Enrollment

Click the “Add” button  in the “function editing area” to open the window for overtime enrollment (Fig. 12-18).

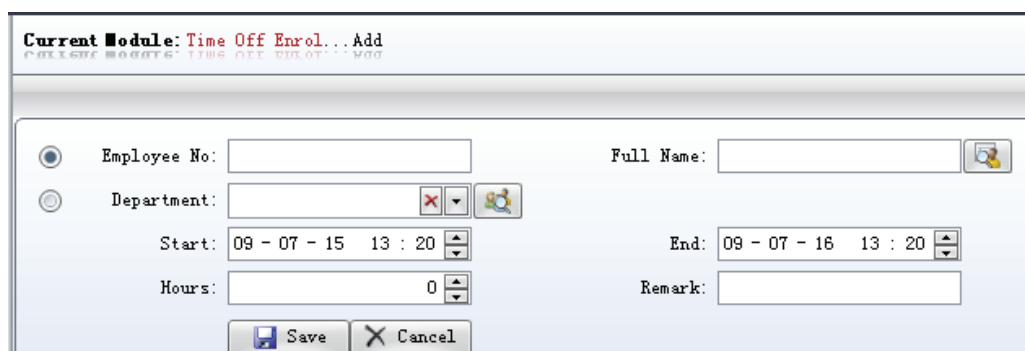


Fig. 12-18 Add Excused Leave Record

✧ Search by employee's information

Similar as “Add a non-access-attendance enrollment”. Refer to Section 12.2.1.1 for details.

✧ Search by a employee's department

Similar as “Add a non-access-attendance enrollment”. Refer to Section 12.2.1.1 for details

Start time/End time: click on the item to be edited, type in the date from keyboard or using the up-and-down button  to select dates.

Hours: the minimum value is 0.5 hour and the maximum is 24 hours. Time-off hours cannot be left empty.

When finished, click “Save”  on the right and a dialog box reporting “Operation succeeded” will pop up.

12.2.3.2 Edit a Time-off Enrollment

Select the time-off enrollment to be edited, click the “Edit” button  to edit the start time, end time, hours and remarks. When finished, click “Save” button  and a dialog box reporting “Operation succeeded” will pop up.

12.2.3.3 Delete Time-off Enrollment(s)

✧ Delete specific time-off enrollment(s)

Select one time-off enrollment from the list, or drag the mouse across multiple adjacent enrollments, or use the “Ctrl” key on the keyboard to select nonadjacent enrollments. After selecting the enrollments to be deleted, click the “Delete”  button in the “Function editing area”. A dialog box will pop up to prompt users to confirm the deletion. Click “Yes” to delete the enrollment(s) and another dialog box reporting “Operation Succeeded” will pop up. Otherwise, click “Cancel” to exit.

✧ Delete all time-off enrollments

Click the “Delete All”  button in the “Function editing area”. A dialog box will pop up to prompt users to confirm the deletion. Click “Yes” to delete all time-off enrollments and another dialog box reporting “Operation Succeeded” will pop up. The number of the enrollments deleted will also be shown. Otherwise, click “Cancel” to exit.

12.2.3.4 Search Time-off Enrollments

Users can search, export and print time-off enrollments using the search tool bar located at the bottom of the window (Fig. 12-19).

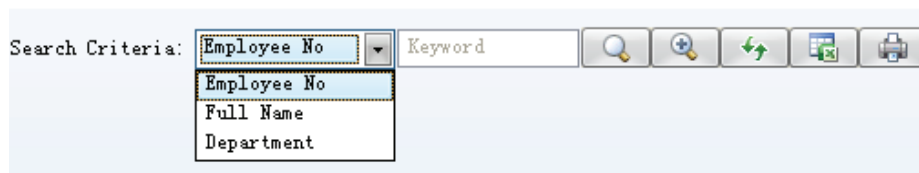


Fig. 12-19 Search, Export and Print Time-off Enrollments

There are 3 search criteria for time-off enrollments. Select a search criterion from the drop-down menu and enter related keywords. This quick search function does not support inexact or ‘wildcard’ search. See Advanced Search below for those capabilities. Click “Search” button  and the employee’s enrollment records will be shown on the event list in the middle.

12.2.3.5 Advanced Search of Time-off Enrollments

To search by multiple search criteria, click “Advanced Search”  to open the window for advanced search (Fig. 12-20).

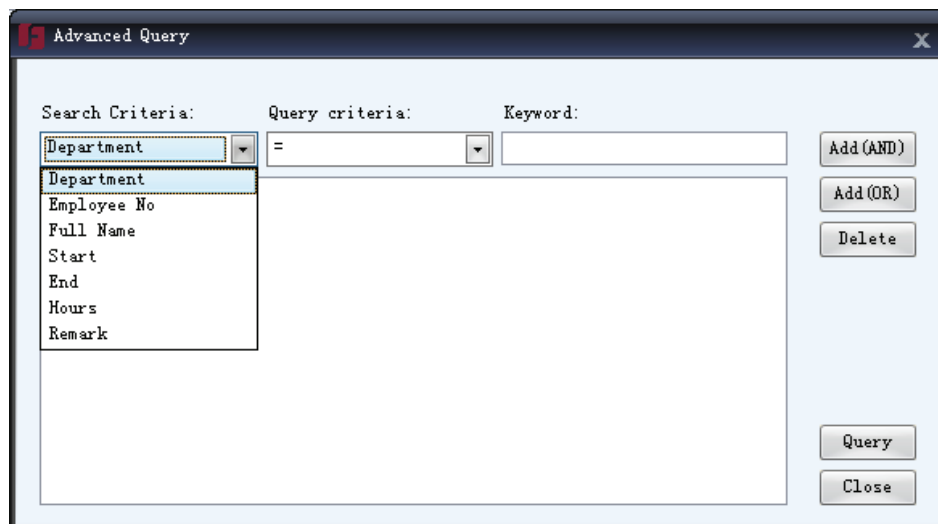


Fig. 12-20 Advanced Search

Search criteria: the name of search items, including department name, employee number, name, start time, end time, time-off hours and remarks.

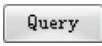
Condition: the matching condition to the search criteria, such as “=” (equal), “<>” (not equal), “>” (greater than), “>=” (greater than or equal”, “<” (less than”, “<=” (less than or equal), “includes (in any position)” “includes (starts with)”, “includes (ends with)”.

Keywords: enter or select the contents that match the search criteria.

Add (and): search for enrollments that match all conditions in two or more search criteria.

Add (or): search for enrollments that match any of the conditions in two or more search criteria.

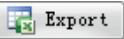
Delete: to delete the search condition in the searching criteria list. Check the search criteria to be deleted and click “Delete”.

Click on the selection box of search criteria and condition, and select the search criteria and condition from the drop-down menu. Enter keywords match the search criteria. Then click “Add (and)” or “Add (or)” on the right to add additional search criteria. The search criteria will be listed on the box at the lower left. Click “Search”  and enrollments that satisfy the search criteria will be shown in the event list. To delete search criteria, check the box before the search criteria, and click “Delete”.

12.2.3.6 Refresh Time-off Enrollments

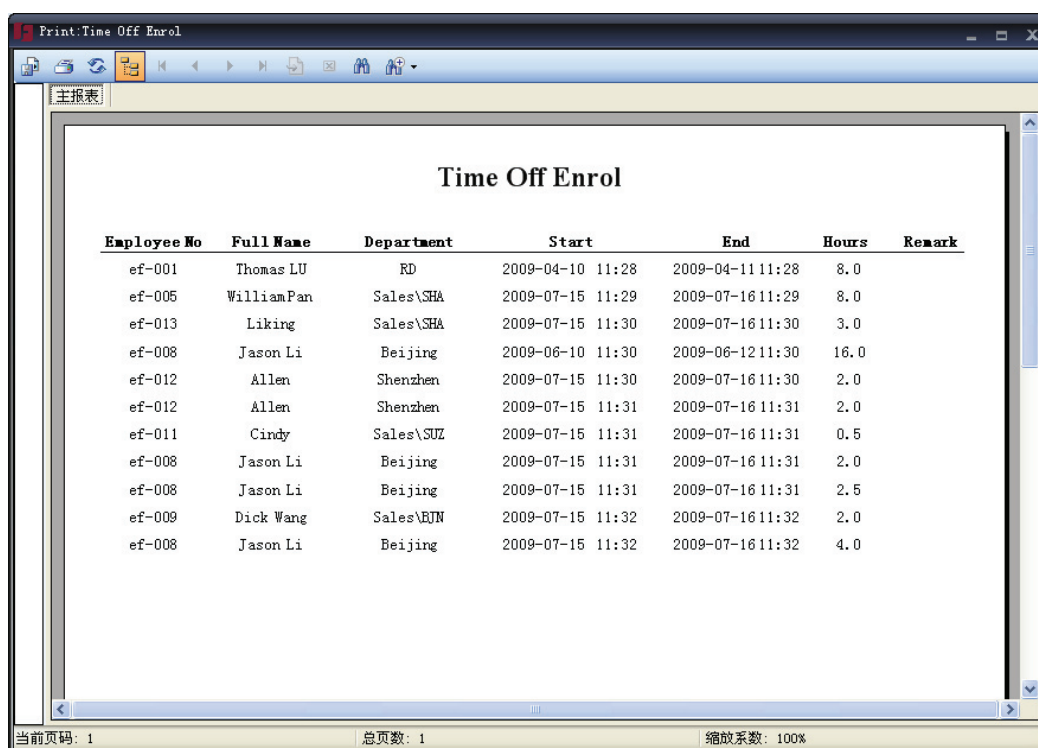
Click “Refresh”  in the “search tool bar” to show the current time-off enrollment list.

12.2.3.7 Export Time-off Enrollments

Click “Export”  in the “search tool bar”, a dialog box will pop up to show that the employee information is being exported as an Excel file. When finished exporting, another dialog box will pop up to ask whether to open the file. Click “Yes” to view the file, otherwise, click “No”.

12.2.3.8 Print Time-off Enrollments

Click “Print”  in the “search tool bar” to open the window for printing time-off enrollments (Fig. 12-21). The menu bar includes: export, print, refresh, switch node, go to the first page, go to last page, go to next page, go to the last page, go to page, close, search text, zoom in/out etc.



The screenshot shows a window titled "Print:Time Off Enrol" with a menu bar and a toolbar. The main content area displays a table titled "Time Off Enrol". The table has the following columns: Employee No, Full Name, Department, Start, End, Hours, and Remark. The data is as follows:

Employee No	Full Name	Department	Start	End	Hours	Remark
ef-001	Thomas LU	RD	2009-04-10 11:28	2009-04-11 11:28	8.0	
ef-005	WilliamPan	Sales\SHA	2009-07-15 11:29	2009-07-16 11:29	8.0	
ef-013	Liking	Sales\SHA	2009-07-15 11:30	2009-07-16 11:30	3.0	
ef-008	Jason Li	Beijing	2009-06-10 11:30	2009-06-12 11:30	16.0	
ef-012	Allen	Shenzhen	2009-07-15 11:30	2009-07-16 11:30	2.0	
ef-012	Allen	Shenzhen	2009-07-15 11:31	2009-07-16 11:31	2.0	
ef-011	Cindy	Sales\SUZ	2009-07-15 11:31	2009-07-16 11:31	0.5	
ef-008	Jason Li	Beijing	2009-07-15 11:31	2009-07-16 11:31	2.0	
ef-008	Jason Li	Beijing	2009-07-15 11:31	2009-07-16 11:31	2.5	
ef-009	Dick Wang	Sales\BJN	2009-07-15 11:32	2009-07-16 11:32	2.0	
ef-008	Jason Li	Beijing	2009-07-15 11:32	2009-07-16 11:32	4.0	

The status bar at the bottom shows: 当前页码: 1, 总页数: 1, 缩放系数: 100%.

Fig. 12-21 Print Time-Off Enrollments

12.3 Attendance Report

12.3.1 Attendance Statistics Report

Click “Attendance Management” ➔ “Attendance Report” and select “Attendance Statistics Report” from the drop-down menu to open the window for attendance statistics report (Fig. 12-22).

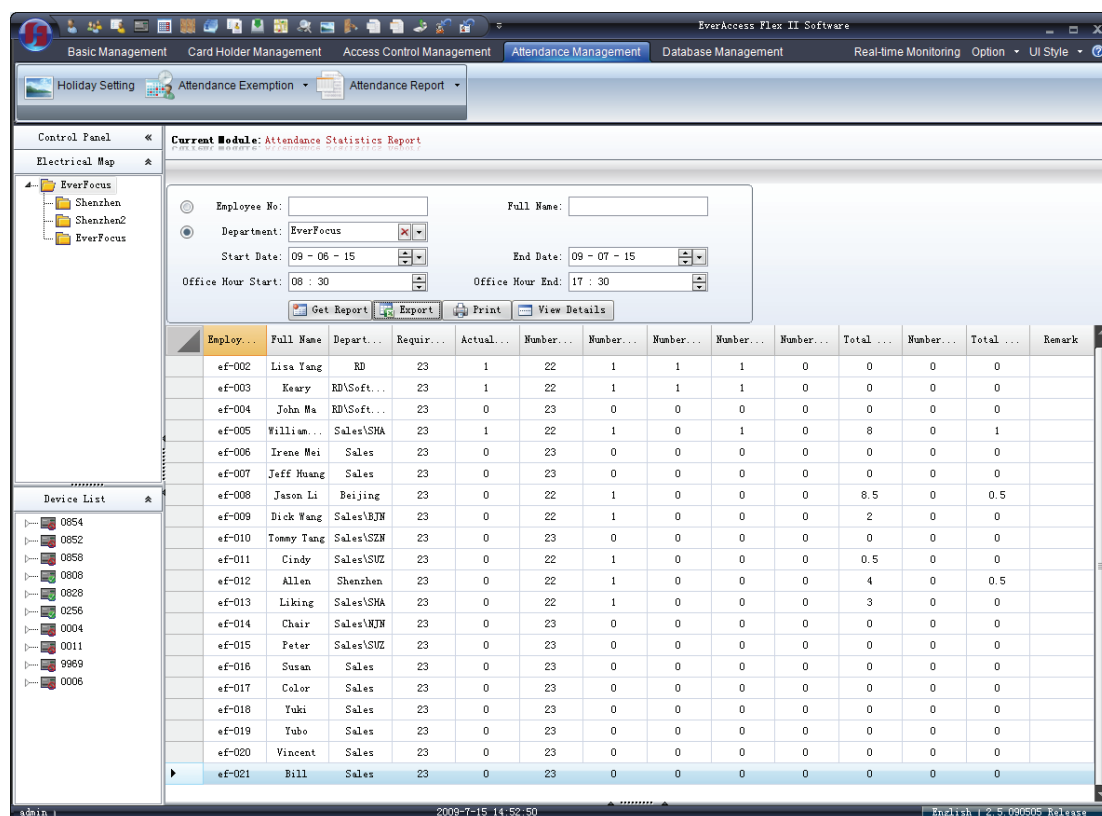


Fig. 12-22 Attendance Statistics Report

Attendance records include granted access records, overtime enrollment records, time-off enrollment records and overtime records. An overtime enrollment record is also counted as one granted access record.

Scheduled attendance days: number of days in the attendance period subtracted by the number of department holidays. This is the number of days an employee is expected to work. If there is no department holiday, the status will follow the parent department's holiday setting. If there is no holiday set for the company, the status follows the system default setting, i.e. Saturday and Sunday are weekends (holidays). If a department to which an employee belongs is a child department, the child department holiday setting has higher priority. Overtime during weekends is counted only toward overtime hours.

Actual attendance days: refers to the total number of effective attendance days among scheduled attendance days. How a determination is made whether a day is an actual attendance day is described below. Both granted access and overtime enrollment records are valid access records. Among valid access records, the earliest entry time is the actual start work time and the latest exit time is the actual end work time. If there is only one event on record, it will be counted as both start work time and end work time. If part of the actual work time falls into the time period between "office hour start" and "office hour end", the day is counted as an effective attendance day.

For example, assume the effective attendance time is 8:30-17:30 and there is no time-off enrollment. If an employee has two access records at 6:00 and 7:00 respectively, the day is counted as absence. If there is only one record at 9:00, it is counted as an effective attendance day. Thus it is advisable for all employees actually in attendance to be sure to present their card at least once during the effective attendance time period.

Time-off enrollment: The process to determine whether a day is time-off is similar to that to determine an effective attendance day. If a portion of the time-off enrollment time falls into the time period between “office hour start” and “office hour end”, the time-off enrollment is valid for the current day. If the start time of time-off is during an attendance day, the total time-off hours are counted towards the attendance day. Otherwise, the total time-off hours are counted towards the first attendance day.

Example 1: assume the effective attendance time is 8:30-17:30. An employee’s time-off enrollment is from 16:30 to 7:00 the next day. The time-off hour is 1 hour for the first day. The time-off for the second day is invalid. If there is no access record of the employee for the second day, the second day is counted as absence.

Example 2: assume the effective attendance time is 8:30-17:30. An employee’s time-off is from 8:30 on April 1 to 17:30 on April 2 for 16 hours. The employee’s attendance record will show time-off hours of 16 hours for April 1, and 0 hours for April 2. Both April 1 and April 2 show “Yes” for time-off enrollment.

Example 3: assume the attendance day is from April 1 to April 30 and the effective attendance time is 8:30-17:30. An employee’s time-off enrollment is from March 31 to April 1 for 16 hours. The employee’s attendance record will show time-off hours of 16 hours for April 1 and April 1 shows “Yes” for time-off enrollment.

Absence: an attendance day is counted as absence if it is neither an effective attendance day, nor a valid time-off day for an employee. It will not be counted as being-late or leaving-early.

Being-Late: it is counted as one being-late if an employee has no valid time-off, and the actual start work time is later than “office hour start” for an attendance day. If the time-off period does not cover “office hour start”, it is counted as one being-late.

Leaving-early: it is counted as one leaving-early if an employee has no valid time-off, and the actual end work time is early than “office hour end” for an attendance day. If the time-off period does not cover “office hour end”, it is counted as one leaving-early.

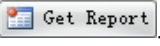
Actual work time: both granted access and overtime enrollment records are valid access records. Among all valid access records, the earliest entry time is the actual start work time and the latest time is the actual end work time. If there is only one event on record, it will be counted as both start work time and end work time.

Total overtime hours: similar to calculation of time-off hours.

12.3.1.1 Generate Attendance Statistics Report

User can generate attendance statistics report for an employee or for a department.

✧ Attendance statistics report for an employee

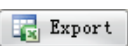
Check the button  in front of “employee number”, and enter an employee number and/or employee name in the related field. Click “Get Report” button . The system will

return the result if an employee satisfying the search criteria is found. Otherwise, there will be no results shown.

✧ Attendance statistics report for a department

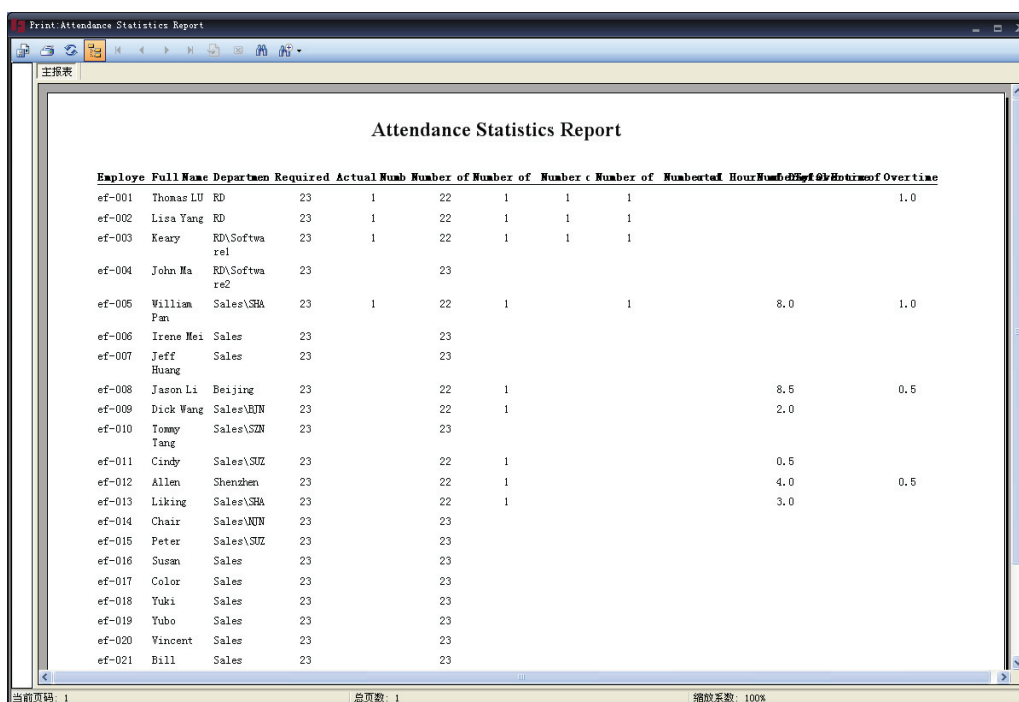
Check the button  in front of “department”, and select a department from the drop-down menu. Click “Get Report” button . The system will return the attendance statistics reports for each individual employee in the selected department if the department contains employee(s).

12.3.1.2 Export Attendance Statistics Report

Click “Export” , a dialog box will pop up to show that the attendance statistics report is being exported as an Excel file. When finished exporting, another dialog box will pop up to ask whether to open the file. Click “Yes” to view the file, otherwise, click “No”.

12.3.1.3 Print Attendance Statistics Report

Click “Print”  to open the window for printing attendance statistics report (Fig. 12-23). The menu bar includes: export, print, refresh, switch node, go to the first page, go to last page, go to next page, go to the last page, go to page, close, search text, zoom in/out etc.



The screenshot shows a window titled "Print Attendance Statistics Report" with a menu bar and a table of employee attendance data. The table has columns for Employee ID, Full Name, Department, Required, Actual Number, Number of, Number of, Number of, Number of, Hour Number, Hour Number, Hour Number, and Overtime. The data is as follows:

Employee	Full Name	Department	Required	Actual Number	Number of	Number of	Number of	Number of	Hour Number	Hour Number	Hour Number	Overtime
ef-001	Thomas LU	RD	23	1	22	1	1	1				1.0
ef-002	Lisa Yang	RD	23	1	22	1	1	1				
ef-003	Keary	RD\Software	23	1	22	1	1	1				
ef-004	John Ma	RD\Software	23		23							
ef-005	William Pan	Sales\GHA	23	1	22	1		1	8.0			1.0
ef-006	Irene Mei	Sales	23		23							
ef-007	Jeff Huang	Sales	23		23							
ef-008	Jason Li	Beijing	23		22	1			8.5			0.5
ef-009	Dick Wang	Sales\UNN	23		22	1			2.0			
ef-010	Tommy Tang	Sales\SZN	23		23							
ef-011	Cindy	Sales\SUZ	23		22	1			0.5			
ef-012	Allen	Shenzhen	23		22	1			4.0			0.5
ef-013	Liking	Sales\GHA	23		22	1			3.0			
ef-014	Chair	Sales\UNN	23		23							
ef-015	Peter	Sales\SUZ	23		23							
ef-016	Susan	Sales	23		23							
ef-017	Color	Sales	23		23							
ef-018	Yuki	Sales	23		23							
ef-019	Yubo	Sales	23		23							
ef-020	Vincent	Sales	23		23							
ef-021	Bill	Sales	23		23							

Fig. 12-23 Print Attendance Statistics Report

12.3.1.4 View Details of Attendance Statistics Report

To view or print an employee’s attendance statistics report, select the employee from the attendance statistics report and click “View Details”  to open the window for viewing details of attendance statistics report (Fig. 12-24). The menu bar includes: export, print, refresh, switch node, go to the first page, go to last page, go to next page, go to the last page, go to page, close, search text, zoom in/out etc.

Note: This function is similar to generate attendance statistics report for an employee, Refer to Section 12.3.1.1.

Print-View Details

主报表

Employee No ef-021 Full Name : Bill Department : Sales

Attendance	Accept signing	Accept signin in	Being Late	Leaving Ear	Number of No	Personal I	Day Off	at al Hour	of Overtime	Remark
2009-06-15			No	No		Yes	No			
2009-06-16			No	No		Yes	No			
2009-06-17			No	No		Yes	No			
2009-06-18			No	No		Yes	No			
2009-06-19			No	No		Yes	No			
2009-06-20			No	No		No	No			Holiday
2009-06-21			No	No		No	No			Holiday
2009-06-22			No	No		Yes	No			
2009-06-23			No	No		Yes	No			
2009-06-24			No	No		Yes	No			
2009-06-25			No	No		Yes	No			
2009-06-26			No	No		Yes	No			
2009-06-27			No	No		No	No			Holiday
2009-06-28			No	No		No	No			Holiday
2009-06-29			No	No		Yes	No			
2009-06-30			No	No		Yes	No			
2009-07-01			No	No		Yes	No			
2009-07-02			No	No		Yes	No			
2009-07-03			No	No		Yes	No			
2009-07-04			No	No		No	No			Holiday
2009-07-05			No	No		No	No			Holiday
2009-07-06			No	No		Yes	No			
2009-07-07			No	No		Yes	No			
2009-07-08			No	No		Yes	No			
2009-07-09			No	No		Yes	No			

当前页码: 1 总页数: 1+ 缩放系数: 100%

Fig. 12-24 View Details

12.3.2 Detailed Attendance Report

Click “Attendance Management” ➔ “Attendance Report”, and select “Detailed Attendance Report” from the drop-down menu to open the window for the detailed attendance report (Fig. 12-25).

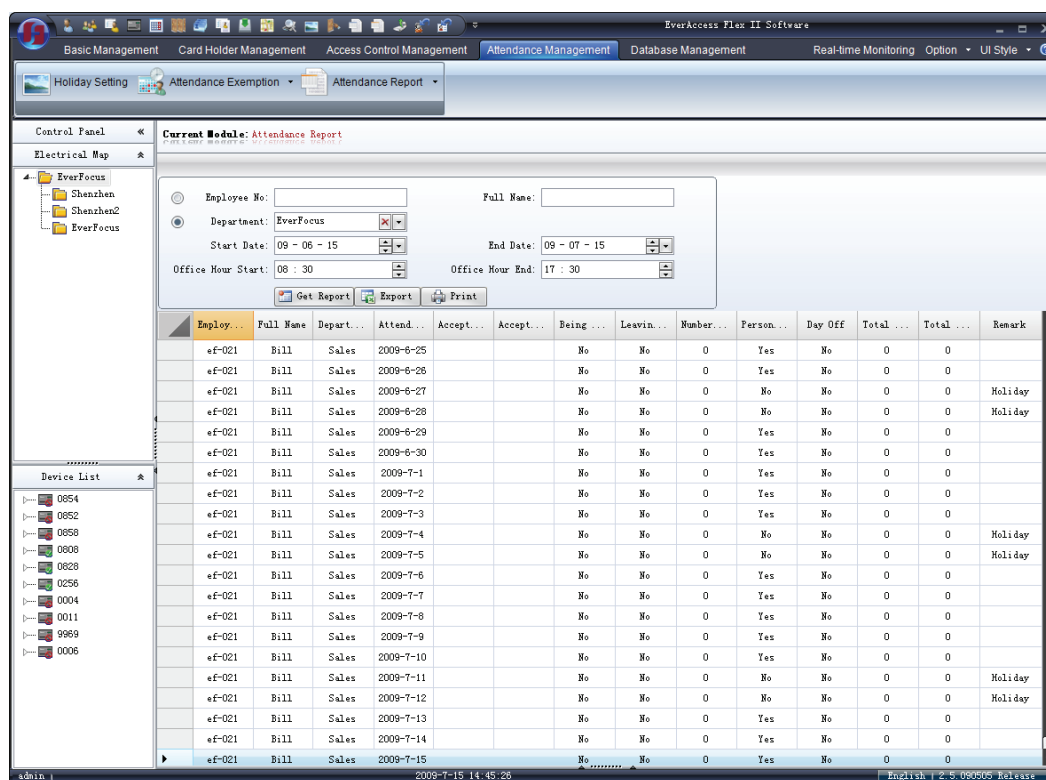


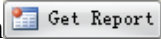
Fig. 12-26 Detailed Attendance Report

Detailed attendance reporting for an employee includes the earliest entry, the last exit, arriving-late, leaving-early, no-access-attendance, absence, time-off, overtime and remarks. Remarks field is used to show whether the day is a holiday.

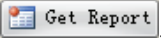
12.3.2.1 Generate Detailed Attendance Report

User can generate a detailed attendance report for an employee or for a department.

✧ Detailed attendance report for an employee

Check the button  in front of “employee number”, and enter employee number and/or employee name in the related field. Click “Get Report” button . The system will return the result if the employee satisfying the search criteria is found. Otherwise, there will be no results shown.

✧ Detailed attendance report for a department

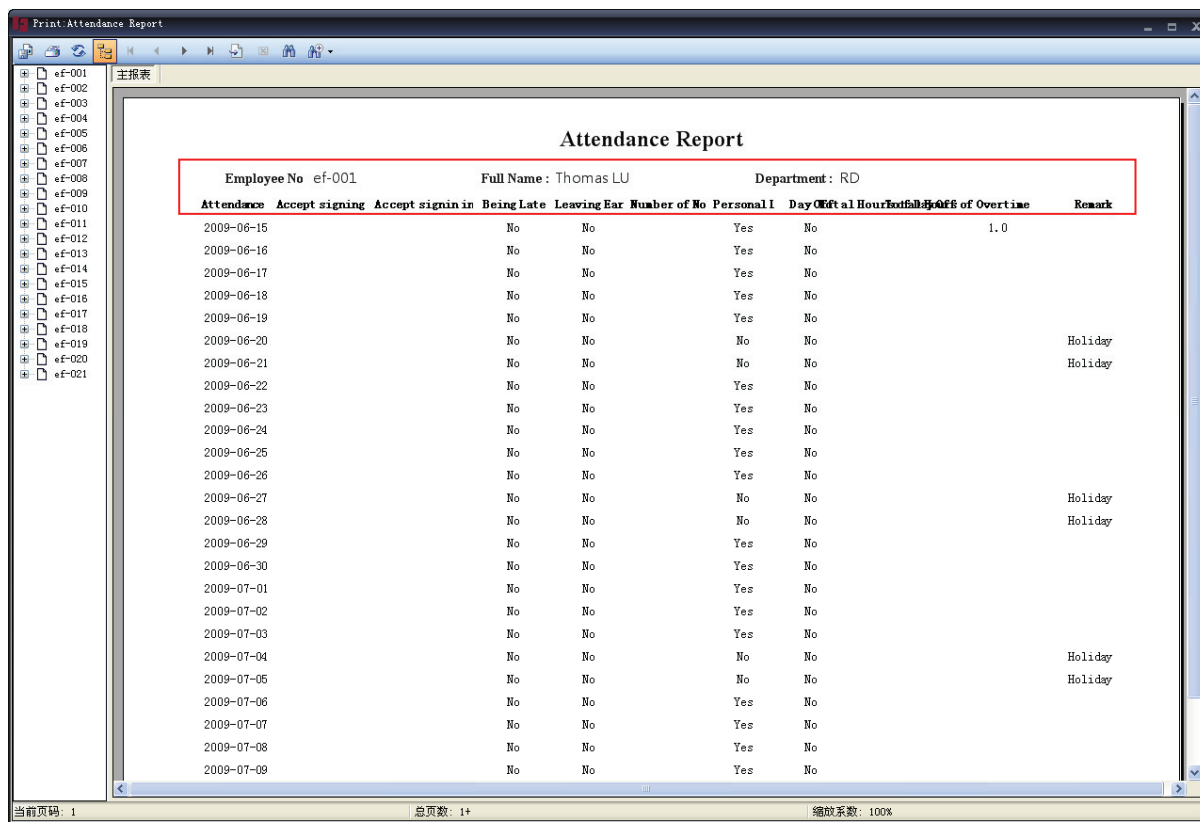
Check the button  in front of “department”, and select a department from the drop-down menu. Click “Get Report” button . The system will return the attendance reports for each individual employee in the selected department if the department contains employee(s).

12.3.2.2 Export Detailed Attendance Report

Click “Export” , a dialog box will pop up to show that the detailed attendance report is being exported as an Excel file. When finished exporting, another dialog box will pop up to ask whether to open the file. Click “Yes” to view the file, otherwise, click “No”.

12.3.2.3 Print Detailed Attendance Report

Click “Print”  to open the window for printing detailed attendance report (Fig. 12-26).



Attendance Report

Employee No ef-001 Full Name: Thomas LU Department: RD

Attendance	Accept signing	Accept sign in	Being Late	Leaving Ear	Number of No	Personal I	Day Off	Total Hour	Total Half Day	Off of Overtime	Remark
2009-06-15			No	No		Yes	No			1.0	
2009-06-16			No	No		Yes	No				
2009-06-17			No	No		Yes	No				
2009-06-18			No	No		Yes	No				
2009-06-19			No	No		Yes	No				
2009-06-20			No	No		No	No				Holiday
2009-06-21			No	No		No	No				Holiday
2009-06-22			No	No		Yes	No				
2009-06-23			No	No		Yes	No				
2009-06-24			No	No		Yes	No				
2009-06-25			No	No		Yes	No				
2009-06-26			No	No		Yes	No				
2009-06-27			No	No		No	No				Holiday
2009-06-28			No	No		No	No				Holiday
2009-06-29			No	No		Yes	No				
2009-06-30			No	No		Yes	No				
2009-07-01			No	No		Yes	No				
2009-07-02			No	No		Yes	No				
2009-07-03			No	No		Yes	No				
2009-07-04			No	No		No	No				Holiday
2009-07-05			No	No		No	No				Holiday
2009-07-06			No	No		Yes	No				
2009-07-07			No	No		Yes	No				
2009-07-08			No	No		Yes	No				
2009-07-09			No	No		Yes	No				

当前页码: 1 总页数: 1+ 缩放系数: 100%

Fig. 12-26 Print Detailed Attendance Report

The menu bar includes: export, print, refresh, switch node, go to the first page, go to last page, go to next page, go to the last page, go to page, close, search text, zoom in/out etc. Users can select a different employee to view or print from the list on the left.

Chapter 13

13 Database Management

13.1 Configure Database

The database is configured upon initial use of the Software. To modify the database, follow the process below.

Click “Database Management” → “Configure Database” to open the window for database configuration (Fig. 13-1).

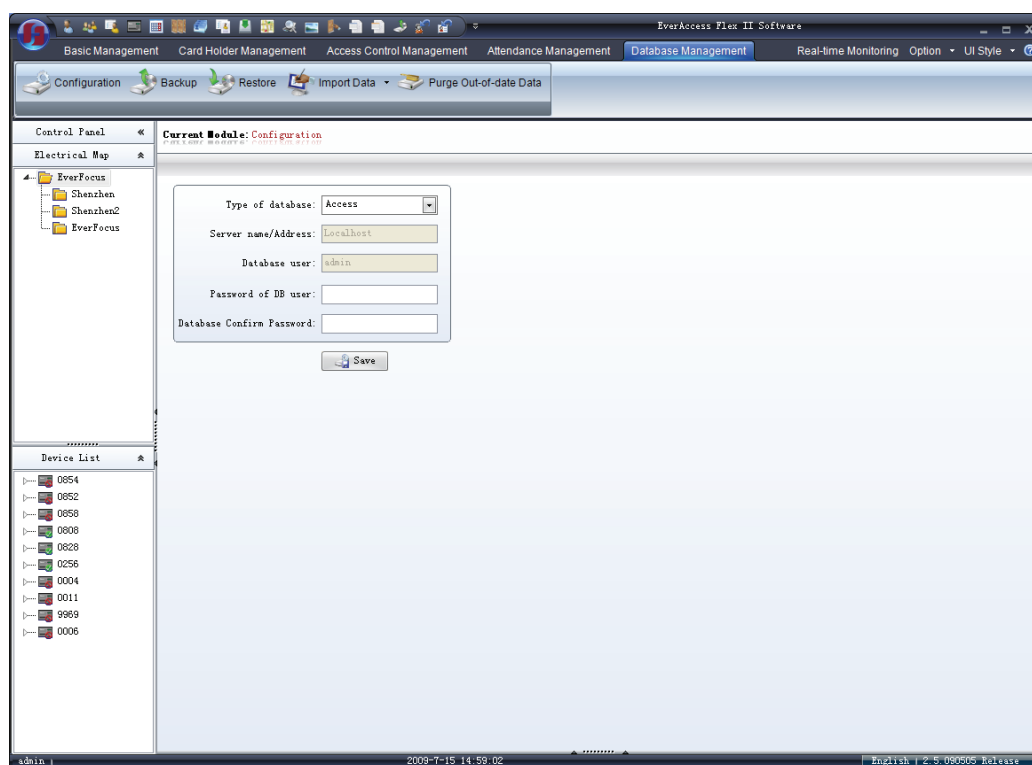


Fig. 13-1 Database Management

The screenshot shows a software configuration window titled "Current Module: Configuration". Inside, there is a section for database configuration with the following fields and options:

- Type of database:** A drop-down menu with "Access" selected. The menu also lists "MSSQLServer", "Oracle", and "MySQL".
- Server name/Address:** A text input field.
- Database user:** A text input field with "Access" entered.
- Password of DB user:** A text input field.
- Database Confirm Password:** A text input field.
- Save:** A button with a floppy disk icon.

Fig. 13-2 Database Type

There are 4 types of database supported by the Software: MySQL, MS SqlServer, Oracle and Access. Click “Database type” and select the database type from the drop-down menu.

Server name/address: The name or IP address of the computer to which the database is stored, such as “127.0.0.1”.

Save configuration: After entering the properties of the database, click the “Save” button. The system will give different prompts based on the database type. Use care when responding to these prompts..

Note: Backup the current database before any database configuration. If errors are generated during database configuration, users can restore the database using the backup. It is recommended to read 13.2 backup database files and 13.3 restore database files before attempting database configuration.

13.2 Backup Database

Database backup is recommended to recover from failures due to computer software problems or hardware damage, or if the database needs to be moved because it occupies too much space in the system. Backing-up the database regularly will ensure safe and efficient system performance. **It is recommended to backup database files at least once every month to be able to restore operation due to unexpected conditions.**

Click “Database Management” ➔ “Backup Database” to open the window for database backup (Fig. 13-3).

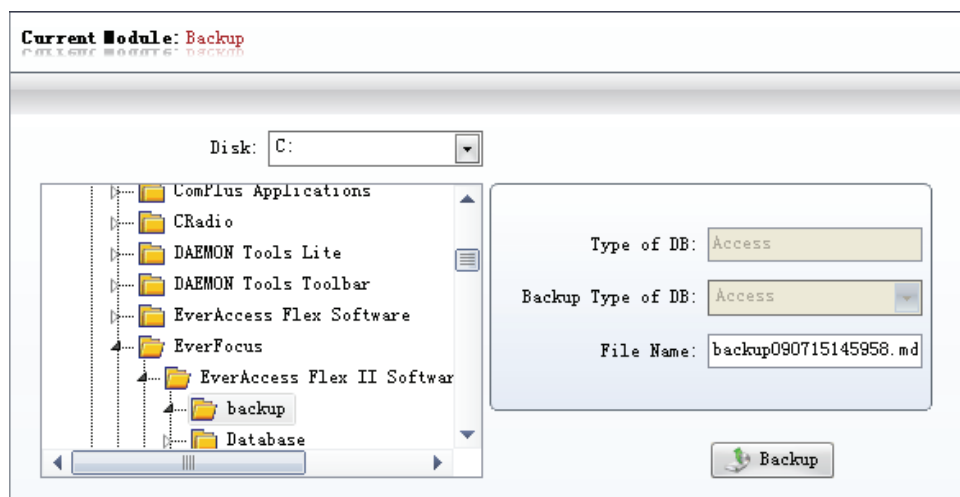


Fig. 13-3 Database Backup

Select the appropriate drive to use for saving database files from the drive pull-down menu (such as E:) and select a destination folder as well. The default backup location is the “backup” folder under the Software installation folder. The default name is the current time, which can be changed by the user. After selecting the path and file name, click “backup” and the system starts backing-up database files. A dialog box reporting “Operation succeeded” will pop up when finished database backup.

Note: Make sure that under the backup folder, there is no file with the same name as the current backup file name. A file with the same name will be overwritten immediately. The only supported file format for backup is Access format, no matter of the type of database in use.

13.3 Restore Database

Click “Database Management” ➔ “Restore Database” to open the window for restoring database (Fig 13-4).

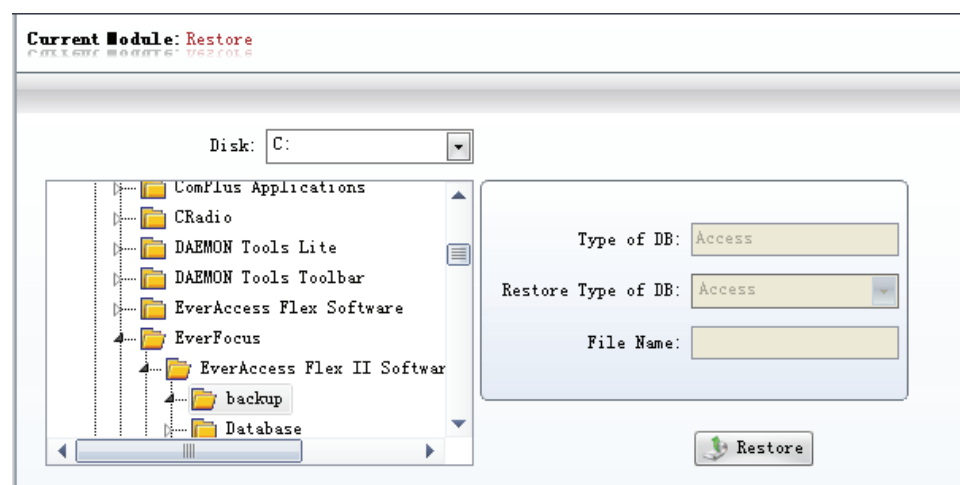


Fig. 13-4 Restore Database

Select the folder in which the backup database files are stored from the pull-down menu. The default location is the backup folder under the Software installation folder. After selecting the file, click “Restore” and the system will prompt to ask whether to overwrite the current database in use with the selected database. Click “Yes” and the system will prompt again to indicate that the operation cannot be undone. Confirm again by clicking “Yes” and the system starts restore the database. A dialog box reporting “Operation succeeded and please log in” will pop up when finished restoring database.

Note: The only supported file format for restoring a database is an Access file.

13.4 Import Database

Users can import EXCEL format files into the database. Two types of files can be imported: cardholder information and card information.

13.4.1 Import Cardholder Information

Click “Database Management” → “Restore Database” → “Import Cardholder Information” to open the window for importing cardholder information (Fig. 13-5).

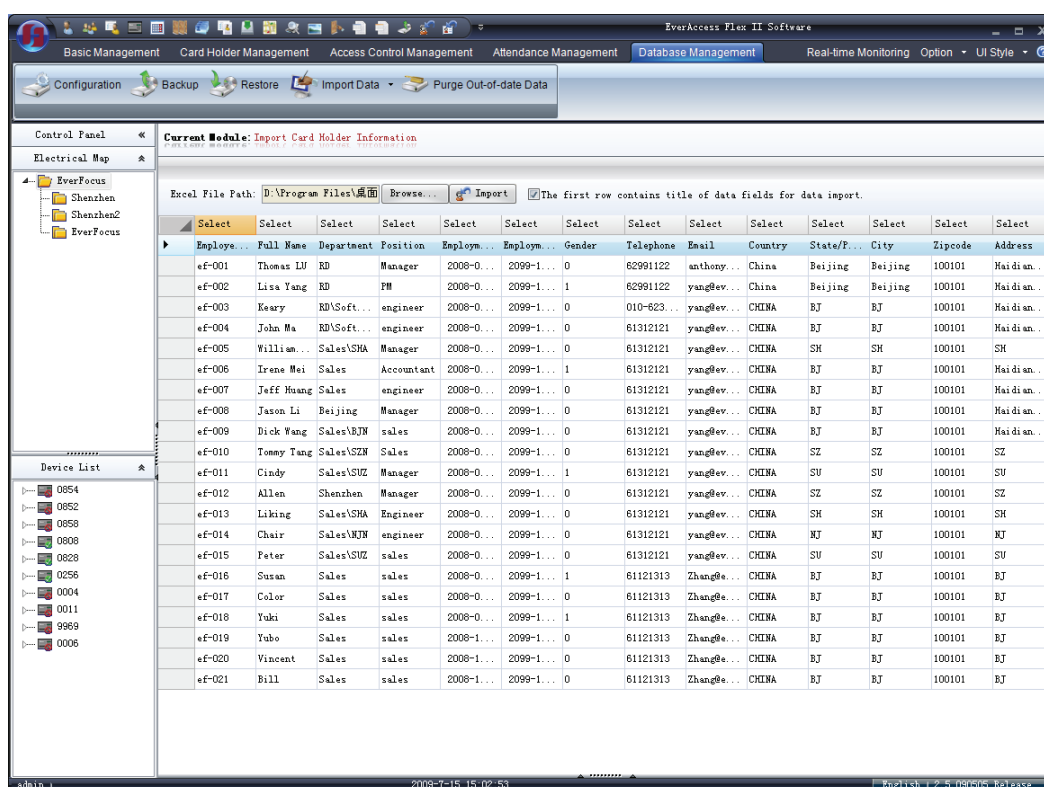
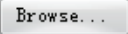


Fig. 13-5 Import Cardholder Information

Click “Browse” button  and a dialog box to “Import Cardholder Information” will pop up. Select the EXCEL file to be imported, and the contents in the file will be uploaded to the window.

Current Module: Import Card Holder Information

Excel File Path: D:\Program Files\桌面 Browse... Import ☒ The first row contains title of data fields for data import.

Select	Select	Select	Select	Select	Select	Select	Select	Select	Select	Select	Select
Select Data	Full Name	Department	Position	Employment Start Date	Employment End Date	Gender	Telephone	Email	Country	State/Province	City
Employee	Thomas LU	RD	Manager	2008-0...	2099-1...	0	62991122	anthony...	China	Beijing	Beijing
First Name	Lisa Yang	RD	PM	2008-0...	2099-1...	1	62991122	yang@ev...	China	Beijing	Beijing
Last Name	Keary	RD\Soft...	engineer	2008-0...	2099-1...	0	010-623...	yang@ev...	CHINA	BJ	BJ
Full Name	John Ma	RD\Soft...	engineer	2008-0...	2099-1...	0	61312121	yang@ev...	CHINA	BJ	BJ
Department	William...	Sales\SHA	Manager	2008-0...	2099-1...	0	61312121	yang@ev...	CHINA	SH	SH
Position	Irene Mei	Sales	Accountant	2008-0...	2099-1...	1	61312121	yang@ev...	CHINA	BJ	BJ
Employment Start Date	Jeff Huang	Sales	engineer	2008-0...	2099-1...	0	61312121	yang@ev...	CHINA	BJ	BJ
Employment End Date	Jason Li	Beijing	Manager	2008-0...	2099-1...	0	61312121	yang@ev...	CHINA	BJ	BJ
Gender	Dick Wang	Sales\BJN	sales	2008-0...	2099-1...	0	61312121	yang@ev...	CHINA	BJ	BJ
Telephone	Tommy Tang	Sales\SZN	Sales	2008-0...	2099-1...	0	61312121	yang@ev...	CHINA	SZ	SZ
Email	Cindy	Sales\SUZ	Manager	2008-0...	2099-1...	1	61312121	yang@ev...	CHINA	SU	SU
Country	ef-012	Allen	Shenzhen	Manager	2008-0...	2099-1...	0	61312121	yang@ev...	CHINA	SZ
State/Province											
City											
Zipcode											
Address											

Fig. 13-6 Select data fields for cardholder information

Data fields for cardholder information include: employee number, name, department name, position, employment start date, employment end date, gender, telephone, Email, county, state/province, city, zip code and address.

If the first row of the imported file is the title row, select “the first row contains titles of data field, do not import”, and the first row will not be imported (Fig. 13-6).

Select data field titles for each column from the drop-down menus of “Select data field”. Employee number must be included. After selecting column titles, click the “Import” button  and the system will prompt that “The operation cannot be undone, confirm to proceed”. Click “OK” and a dialog box reporting “Operation succeeded, XXX records were imported” will be displayed.

Note: Employee numbers that already exist in the system will not be imported. The related record will be highlighted.

13.4.2 Import Card Information

Click “Database Management” → “Import Data” → “Import Card Information” to open the window for importing card information (Fig. 13-7).

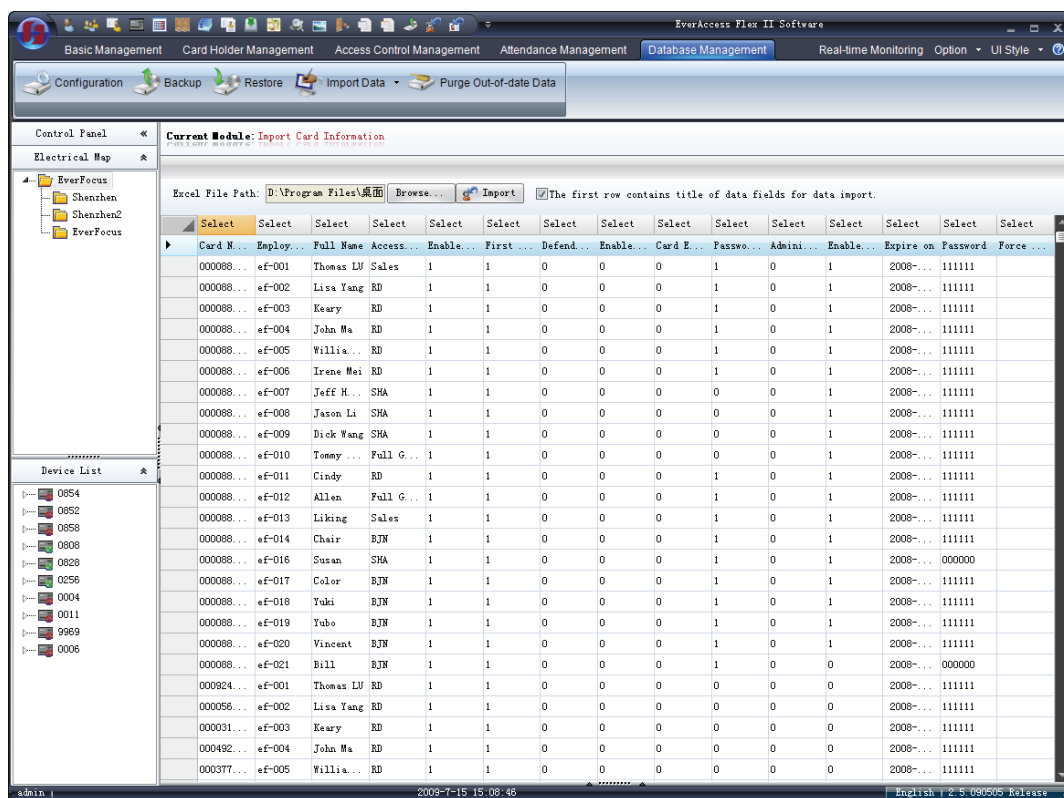


Fig. 13-7 Import Card Information

Click “Browse” button  and a dialog box reporting “Import Card Information” will pop up. Select the EXCEL file to be imported, and the contents in the file will be uploaded to the window.

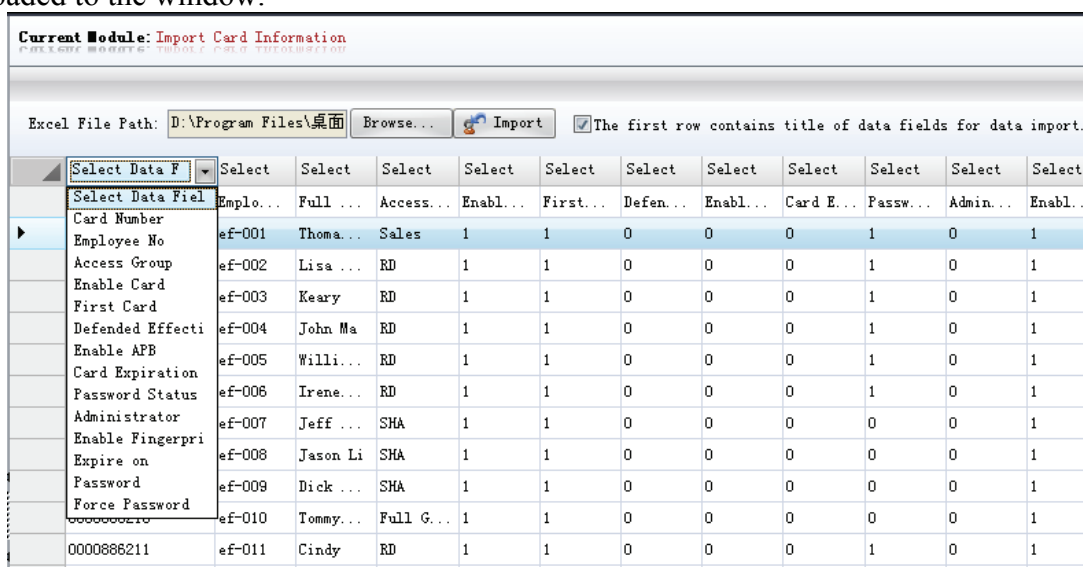


Fig. 13-8 Select data fields for card information

Data fields for card information include: card Index, card number, employee number, access group, Card Enabled, First Card, Arm Enabled, APB Enabled, Card Expiration, PIN Enabled, Administrator and Fingerprint Enabled, validation date. If the first row of the imported file is the title row, select “The first row contains title of data fields, do not import”, and the first row will not be imported.

Select a data field title for each column from the drop-down menus of “Select data field”. Employee number must be included. After selecting titles, click the “Import” button  and the system will prompt that “The operation cannot be undone, confirm to proceed”. Click “OK” and the dialog box for “Card Importing Format” will pop up.

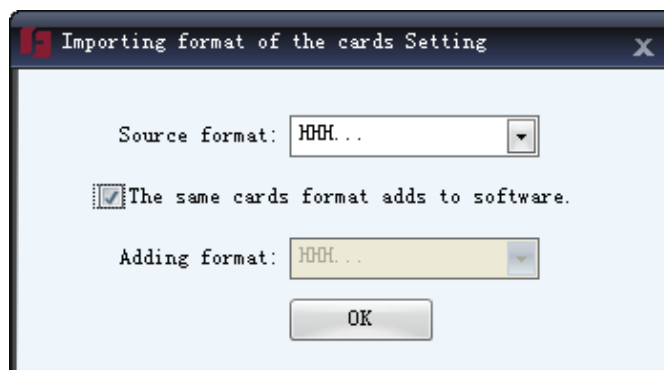


Fig. 13-9 Set Card-Importing Format

Source card format: refers to the card format to be imported. The card formats must be the same for all cards to be imported. Select the correct card format from the drop-down menu, otherwise, the system will not import the cards.

Add cards in the same format: when checked, the “card format after importing” will be the same as “Source card format”

Adding Card format: users can choose any card format to use in the Software. If the Software card format is different from the source card format, do not check “Add cards in the same format” and select the desired format from the drop-down menu.

After selecting the card format, click “OK” and a dialog box reporting “Operation succeeded, XXX records were imported” will pop up.

If certain data fields for the imported cards are empty, the system will assign the default value to the data fields: the default setting for access group is “Full Granted” (Refer to section 6.4 Access group setting for details. If the access group to which an imported card belongs does not exist in the Software, the card will also be assigned to the access group “Full Granted”); the default PIN is “000000”; First Card and Card Enabled is enabled; card Index number is the same as card number; valid date is the current time (accurate to minute).

Note: Card numbers that already exist in the system will not be imported. The related record will be highlighted.

13.5 Purge out-of-date data

Click “Database Management” ➔ “Purge out-of-date data” to open the window for purging out-of-date data (Fig. 13-10).

Fig. 13-10 Purge Out-of-Date Data

This function is used to remove out-of-date records. Large numbers of out-of-date records in the system will increase the login time and increase the time required for attendance management, thus reducing Software performance. It is recommended to backup the database before purging out-of-date data (Refer to section 13.2).

There are 6 types of records in the “Event type list”. Select the event type based on users’ needs. Click the “Event type list” button will select all event types.

There are 5 options of time period on the right:

1 month: Save the records within 1 month and delete all others.

3 months: Save the records within 3 months and delete all others.

6 months: Save the records within 6 months and delete all others.

12 months: Save the records within 12 months and delete all others.

Other time period: save the records after the specified time and delete all records before. The date format is “Year-Month-Date”/YYYY-MM-DD.

After selecting the records to be purged, click “Purge” button, and the system will prompt that “The operation cannot be undone, confirm to proceed”. Click “OK” and all records before the selected time period will be purged. A dialog box reporting “Operation succeeded, and please log in again” will pop up. Click “OK” to exit the system.

Chapter 14

14 Concept Interpretation

14.1 Area Anti-Passback (APB)

14.1.1 Concept of Area

An area in the Software can be a physical area, such as an entrance hall, an office or a dining room etc. It can also refer to an open area defined by users such as an outdoor area. Users can name each area to reflect its actual location. Each area has 3 attributes: name, whether APB is enabled and whether it is an exterior area.

An example of the definition of areas is given below:

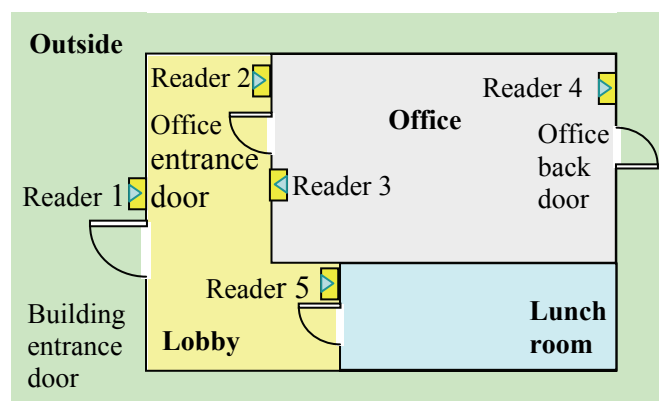


Fig. 14-1 Example of areas

Suppose a building contains an entrance hall, an office and a lunch room (Fig. 14-1). The entrance hall, the office and the lunch room are all physical areas. They are not exterior areas. Whether APB is enabled in these areas depends on users' requirements. The area "Outside" can be an exterior area. APB should be disabled as there is no need to prevent cardholders from entering the building into this "outdoor" area.

14.1.2 Exterior Area and Exterior Doors

It is easy to understand an exterior area. In the example above, the "Outside" area is an exterior area. The Software will automatically determine whether a door is an exterior door based on the area setting. Each reader has a source area and a destination area. If any of those two areas is an exterior area, the door at which the reader is installed is an exterior door. The Software provides a right-click menu of "Lock/unlock/reset all exterior doors" function from the controller list under the main window. In the figure above, the door to the entrance hall

and the back door of the office are exterior doors since “Outside” is defined as an exterior area.

14.1.3 Areas and Readers

Each reader has a source area and a destination area. Source area is the area where a cardholder is located before entering the controlled door and destination area is the area into which the cardholder enters after swiping the card.

In Fig 4-1, the triangle icon indicates the direction of readers. Reader 2 is the reader through which a cardholder enters the office from the entrance hall and reader 4 is the reader through which a cardholder exits to outdoors from the office. Therefore, the source area and destination area for reader 2 are the entrance hall and the office respectively, while the source area and destination area for reader 4 are the office and outdoors respectively.

Flex series controllers can connect up to 8 readers and if every reader has a different source area and a destination area, there will be total 16 areas in the system. Users can define each area in the Software, as shown in Fig. 14-2.

	No.	Door Location	Reader Name	Keypad	System Reader	In/Out	Source Area	Destination Area
▶	1	Door1	Reader1	No	Yes	In	Outside	Lobby
	2	Door2	Reader2	No	No	In	Lobby	Office
	3	Door3	Reader3	Yes	No	Out	Office	Lobby
	4	Door4	Reader4	No	No	Out	Office	Outside

Fig. 14-2 Reader Setting: source area and destination area

14.1.4 APB Enabled

In an area where APB is enabled, if a cardholder with an APB enabled card enters the area, he will not be able to enter the area for a second time without first leaving the area. This function will prevent a cardholder from “passing back” his card to another person for that person to gain entry into the same area twice without the cardholder leaving the area. Users can use the APB function to protect important areas.

To apply the APB function to multiple cards: in “card setting”, select multiple cards and choose “Edit” function. Refer to section 7.3 Edit Card Information for details

Facilities (doors) must be fitted with at least one entry and one exit reader when APB is implemented. Setting APB function in areas fitted with only entry readers or only exit readers will fail. In the example above, APB function cannot be applied to the lunch room as it only has one entry reader.

Recommended setting steps: First, give each area a name and assign whether it is an exterior area. Next, specify source area and destination area for each reader. Last, set whether APB is enabled for each area.

Users can set door behavior, i.e. “door open” or “door lock” unlock in the APB event window. This setting applies to all controllers. “Door lock” under APB means the door remains locked under APB and there is no APB Fail event. “Door open” means the door opens under APB and the system generates an APB Fail record. See Fig. 14-3 for APB setting.

	No.	Door Location	Reader Name	Keypad
▶	1	Door1	Reader1	No
	2	Door2	Reader2	No
	3	Door3	Reader3	Yes
	4	Door4	Reader4	No

Fig. 14-3 Area APB Setting

14.1.5 Card APB Enabled

In an APB enabled area, a cardholder must alternate usage between entry and exit readers. In other words, when a cardholder swipes his card on a reader in an APB enabled area, he should enter the destination area controlled by the reader. Otherwise, he will not be able to use his card to enter the area due to APB rules.

In Fig. 14-1, assume APB is enabled for the office. A cardholder does not enter the office after swiping his card on reader 2, instead he greets one of his colleagues in the entrance hall. There will be an APB event if the cardholder uses his card again on reader 1, 2 or 5 because the system assumes he is inside the office.

The Software provides a simple method to resolve an APB events: disable the card APB setting and save. The card APB setting will be reset. Then enable the card APB setting again. In the example above, disable the card APB setting and then enable it, the cardholder is then able to use his card on reader 2 to enter the office. The operation window is shown in Fig. 14-4.

Fig. 14-4 Edit Card APB Setting

14.1.6 Example of APB Event

In the example of Fig. 14-1, areas are interconnected. Here, an example of APB in two independent areas is given (Fig. 14-5).

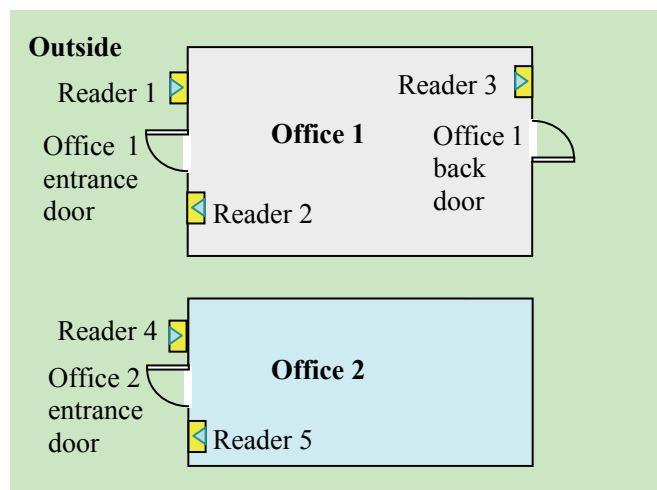


Fig. 14-5 APB of independent Areas

There are two independent offices in this example, office 1 and office 2. Office 1 and office 2 are fitted with both entry readers and exit readers. For office 2, reader 4 is the entry reader and reader 5 is the exit reader. Both areas can be set as APB enabled.

The concept of areas and APB areas has been discussed earlier in this chapter. APB enabled areas should be a physical area and all doors in its perimeter should be controlled by readers. In Fig. 14-1, if a request-to-exit button is installed for the office, a cardholder can enter the office by swiping a card and exit by pressing the request-to-exit button. However, if an APB is enabled for the office, the cardholder will not be able to reenter the office again due to APB rules.

An example of wrong area setting of the areas in Fig. 14-1 is given below. The source area for reader 4 is “office”; however, it is set as “entrance hall” by mistake.

No.	Door Location	Reader Name	Keypad	System Reader	In/Out	Source Area	Destination Area
1	Door1	Reader1	No	Yes	In	Outside	Lobby
2	Door2	Reader2	No	No	In	Lobby	Office
3	Door3	Reader3	Yes	No	Out	Office	Lobby
4	Door4	Reader4	No	No	Out	Office	Outside

Fig. 14-6 Wrong area Setting in Reader

If a cardholder tries to exit the office by swiping his card on reader 4, the access will be denied due to APB rules. This is because the system assumes that the cardholder is in the office, and requires the cardholder to exit to any other areas from the office, but the source area of reader 4 is incorrectly set as entrance hall.

The system setting for APB rule is: if APB is enabled for area B, a cardholder enters area B by swiping his card on a reader with source area A and destination area B. Swiping the card on any readers with a source area other than area B generates an APB violation.

EverFocus Electronics Corp.

Head Office

12F, No.79 Sec.1 Shin-Tai Wu
Road,
Hsi-Chi, Taipei, Taiwan
Tel: + 886-2-2698-2334
Fax: + 886-2-2698-2380

USA Office

1801 Highland Ave, Duarte,
Building
CA 91010, U.S.A
Tel: + 1-626-844-8888
Fax: + 1-626-844-8838

Japan Office

1809 WBG Marive East 18F,
2-6 Nakase, Mihama-ku,
Chiba city 261-7118, Japan
Tel: + 81-43-212-8188
Fax: + 81-43-297-0081

European Office

Albert-Einstein-Strasse 1,
D-46446 Emmerich, German
Tel: + 49-2822-9394-0
Fax: + 49-2822-939495

Beijing Office

Room 609, KEMAO Building,
Shangdi, Haidian, Beijing, China
Tel: + 86-10-6297-3336
Fax: + 86-10-6297-1423

 **EverAccess®**
MEFCG00100C

V 2.0