

iVMS-4200 Access Control Client

User Manual

<u>UD00895N</u>

User Manual

About this Manual

This Manual is applicable to iVMS-4200 Access Control Client.

The Manual includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website.

Please use this user manual under the guidance of professionals.

Legal Disclaimer

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. OUR COMPANY SHALL NOT TAKE ANY RESPONSIBILITES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, OUR COMPANY WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. OUR COMPANY SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER

PREVAILS.

Contents

Chapter	1	Overview	4
1.1		Description	4
1.2		Running Environment	4
1.3		Configuration Flow	4
Chapter	2	User Registration and Login	6
2.1		User Registration	6
2.2		Login	6
2.3		Function Modules	7
Chapter	3	Hardware Management	10
3.1		Device Management	10
	3.1.1	Access Controller Management	11
	3.1.2	Network Settings	19
	3.1.3	Capture Settings	20
3.2		Door Group Management	22
	3.2.1	Access Control Group Management	23
	3.2.2	Access Control Point Management	23
Chapter	4	Permission Configuration	25
4.1		Person Management	25
	4.1.1	Department Management	25
	4.1.2	Person Management	26
4.2		Card Management	31
	4.2.1	Empty Card	32
	4.2.2	Normal Card	
	4.2.3	Lost Card	
4.3		Schedule Template	37
	4.3.1	Setting Week Plan	
	4.3.2	Setting Holiday Group	
	4.3.3	Setting Schedule Template	40
4.4		Door Status Duration Management	41
4.5		Linkage Configuration	43
	4.5.1	Event Alarm Linkage	44
	4.5.2	Event Card Linkage	45
	4.5.3	Client Linkage	46
4.6		Access Permission Configuration	48
	4.6.1	Adding Permission	48
	4.6.2	Downloading Permission	50
	4.6.3	Importing/Exporting Permission	51
	4.6.4	Searching Access Control Permission	51
4.7		Advanced Functions	52
	4.7.1	Access Control Type	53
	4.7.2	Card Reader Authentication	55
	4.7.3	Multiple Authentication	56

	4.7.4	Open Door with First Card	58
	4.7.5	Anti-Passing Back	59
	4.7.6	Multi-door Interlocking	60
	4.7.7	White List	61
	4.7.8	Authentication Password	62
Chapter !	5	Attendance Management	64
5.1		Attendance Configuration	64
	5.1.1	Shift Group Management	64
	5.1.2	Shift Management	65
	5.1.3	Holiday Management	68
	5.1.4	Shift Schedule Management	69
	5.1.5	Attendance Check Point Management	70
	5.1.6	Adjustment Management	71
	5.1.7	Card Swiping Log Query	75
	5.1.8	Parameters Configuration	75
	510	Data Management	70
	5.1.9		/6
5.2	5.1.5	Attendance Statistic	76 77
5.2 Chapter	6	Attendance Statistic Status and Event	76 77 78
5.2 Chapter 6.1	6	Attendance Statistic Status and Event Status Monitor	76 77 78 78
5.2 Chapter 6.1	6 6.1.1	Attendance Statistic Status and Event Status Monitor Anti-control the Access Control Point (Door)	
5.2 Chapter 6.1 6.2	6.1.1	Attendance Statistic Status and Event Status Monitor Anti-control the Access Control Point (Door) Real-Time Access Event Alarm	
5.2 Chapter 6.1 6.2 6.3	6.1.1	Attendance Statistic Status and Event Status Monitor Anti-control the Access Control Point (Door) Real-Time Access Event Alarm Event Management	
5.2 Chapter 6.1 6.2 6.3 Chapter 1	6 6.1.1	Attendance Statistic Status and Event Status Monitor Anti-control the Access Control Point (Door) Real-Time Access Event Alarm Event Management System Maintenance	
5.2 Chapter 6.1 6.2 6.3 Chapter 7.1	6.1.1 7	Attendance Statistic Status and Event Status Monitor Anti-control the Access Control Point (Door) Real-Time Access Event Alarm Event Management System Maintenance Log Management	
5.2 Chapter 6.1 6.2 6.3 Chapter 7 7.1	6 6.1.1 7 7.1.1	Attendance Statistic Status and Event Status Monitor Anti-control the Access Control Point (Door) Real-Time Access Event Alarm Event Management System Maintenance Log Management Searching Configuration Logs	
5.2 Chapter 6.1 6.2 6.3 Chapter 7 7.1	6 6.1.1 7 7.1.1 7.1.2	Attendance Statistic Status and Event Status Monitor Anti-control the Access Control Point (Door) Real-Time Access Event Alarm Event Management System Maintenance Log Management Searching Configuration Logs Searching Control Logs	
5.2 Chapter 6.1 6.2 6.3 Chapter 7 7.1	6 6.1.1 7 7.1.1 7.1.2	Attendance Statistic Status and Event Status Monitor Anti-control the Access Control Point (Door) Real-Time Access Event Alarm Event Management System Maintenance Log Management Searching Configuration Logs Searching Control Logs Account Management	
5.2 Chapter 6.1 6.2 6.3 Chapter 7 7.1 7.2 7.2	6 6.1.1 7 7.1.1 7.1.2	Attendance Statistic Status and Event Status Monitor Anti-control the Access Control Point (Door) Real-Time Access Event Alarm Event Management System Maintenance Log Management Searching Configuration Logs Searching Control Logs Account Management System Configuration	
5.2 Chapter 6.1 6.2 6.3 Chapter 7.1 7.2 7.3	6 6.1.1 7 7.1.1 7.1.2 7.3.1	Attendance Statistic Status and Event Status Monitor Anti-control the Access Control Point (Door) Real-Time Access Event Alarm Event Management System Maintenance Log Management Searching Configuration Logs Searching Control Logs Account Management System Configuration General Settings	
5.2 Chapter 6.1 6.2 6.3 Chapter 7 7.1 7.2 7.3	6 6.1.1 7 7.1.1 7.1.2 7.3.1 7.3.2	Attendance Statistic Status and Event Status Monitor Anti-control the Access Control Point (Door) Real-Time Access Event Alarm Event Management System Maintenance Log Management Searching Configuration Logs Searching Control Logs Account Management System Configuration General Settings Card Reader Configuration	
5.2 Chapter 6.1 6.2 6.3 Chapter 7.1 7.2 7.2 7.3	6.1.1 7 7.1.1 7.1.2 7.3.1 7.3.2 7.3.3	Attendance Statistic Status and Event Status Monitor Anti-control the Access Control Point (Door) Real-Time Access Event Alarm Event Management Event Management System Maintenance Log Management Searching Configuration Logs Searching Control Logs Account Management System Configuration General Settings Card Reader Configuration Fingerprint Machine Configuration	

Chapter 1 Overview

1.1 Description

The iVMS-4200 Access Control Client is a client of configuring permission of door access. It provides multiple functionalities, including access controller management, person/card management, permission configuration, door status management, attendance management, event search, etc. This user manual describes the function, configuration and operation steps of Access Control Client. To ensure the properness of usage and stability of the client, please refer to the contents below and read the manual carefully before installation and operation.

1.2 Running Environment

Operating System: Microsoft Windows 7/Windows 2008 (32-bit or 64-bit), Windows XP/Windows 2003 (32-bit), Windows 8/Windows 8.1/Windows Server 2012/Windows 10 (64-bit) CPU: Intel Pentium IV 3.0 GHz or above Memory: 1G or above Video Card: RADEON X700 Series or above GPU: 256 MB or above Notes:

- For high stability and good performance, these above system requirements must be met.
- The software does not support 64-bit operating system; the above mentioned 64-bit operating system refers to the system which supports 32-bit applications as well.

1.3 Configuration Flow

Refer to the following flow chart for the configuration order.



Chapter 2 User Registration and Login

For the first time to use the client software, you need to register a super user for login.

2.1 User Registration

Steps:

- 1. Double-click **b** on the desktop to run the client.
- 2. Input the super user name, password and confirm password in the pop-up window.
- 3. Optionally, check the checkbox **Auto-login** to log in to the software automatically.
- 4. Click Register. Then, you can log in to the software as the super user.



- A user name cannot contain any of the following characters: / \ : * ? " <> |. And the length of the password cannot be less than 8 characters.
- For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

When opening iVMS-4200 access control client after registration, you can log in to the client software with the registered user name and password.

2.2 Login

Steps:

1. Input the user name and password you registered.

	Welcome	-
	▲ admin A •••••••	~
iVMS-4200 Access Control Client	🗖 Auto-login 🤄	Forgot Password
	1000	

- 2. Optionally, check the checkbox Auto-login to log in to the software automatically.
- 3. Optionally, if you forget your password, please click **Forgot Password** and remember the encrypted string in the pop-up window. Contact your dealer and send the encrypted string to him

to reset your password.

4. Click Login.

2.3 Function Modules

After login, the control panel of the access control client is shown as follows:

Control Panel of iVMS-4200 Access Control Client:

File System View Tool Hel				admin 11:27:34 🔒 -	- = ×
Control Panel					
Decis 6-there					
Basic Setungs					
	2	<u> </u>			
Device Management	Person Management	Card Management	Template	Access Control Permission	
Adding, editing, and deleting of access controllers.	Adding, editing, and deleting of person and departments.	Adding, editing, and deleting the card information.	Adding, deleting, and editing of duration, week plan, and	Adding, deleting, and applying the access control	
Advanced Function		Attendanc	e Management		
Advanced Function	Linkage Configuration	Attenda	nce Configuration Atten	dance Statistics	
Configuring advanced functions including access	Configuring event alarm, event card, and client	Setting st including	nift schedule Calculati attendance rule, the atten	ing and analyzing dance results.	
Access Control Maintenance					
	-	2		18	
Status Monitor	Door Group Management	Account Management	Event Management	Log Search	
Displaying access control status and provides anti-	Adding, editing, and deleting the access control group.	Adding, editing, and deleting the user and assigning	Searching the access control event.	Searching the configuration logs and control logs.	
Alarm Information				<i>f</i> t	• *

Menu Bar:

File	Exit	Exit the iVMS-4200 Access Control Client.		
	Lock	Lock screen operations. Log in the client again to unlock.		
Sustan	Switch User	Switch the login user.		
System	Import Parameters	Import client configuration file from your computer.		
	Export Parameters	Export client configuration file to your computer.		
	Device Management	Open the Device Management page.		
	Attendance Configuration	Open the Attendance Configuration page.		
	Attendance Statistics	Open the Attendance Statistics page.		
	Person Management	Open the Person Management page.		
Mienu	Card Management	Open the Card Management page.		
view	Template	Open the Template page.		
	Access Control Permission	Open the Access Control Permission page.		
	Advanced Function	Open the Advanced Function page.		
	Status Monitor	Open the Status Monitor page.		
	Linkage Configuration	Open the Linkage Configuration page.		

	Door Group Management	Open the Door Group Management page.	
	Account Management	Open the Account Management page.	
	Event Management	Open the Event Management page.	
	Log Search	Open the Log Search page.	
	Control Panel	Enter Control Panel interface.	
	Search Access Control	Search the added access control permission	
	Permission	Search the added access control permission.	
	Card Reader	Configure the card reader parameters.	
Tools	Fingerprint Machine	Configure the fingerprint machine parameters.	
	Storage Server	Configure the storage server parameters.	
	System Configuration	Enter the System Configuration page.	
	Download Devenentors	Apply the settings on the client to the corresponding	
	Download Parameters	access controller.	
	Licer Menuel (F1)	Click to open the User Manual; you can also open the User	
	Oser Manual (F1)	Manual by pressing F1 on your keyboard.	
Help	Language	Select the language for the client software and reboot the	
	Language	software to activate the settings.	
	About	View the basic information of the client software.	

The iVMS-4200 access control client is composed of the following function modules:



The Device Management module provides adding, editing, and deleting of access controllers.



The Person Management module provides adding, editing, and deleting of person and departments.

The Card Management module provides adding, editing, and deleting the card information.

The Template module provides adding, deleting, and editing of duration, week plan, and holiday.



The Access Control Permission module provides adding, deleting, and applying the access control permissions.



The Advanced Function module provides configuration of advanced functions including access control type, anti-passing back, multiple interlocking, etc..



The Linkage Configuration module provides event alarm, event card, and client linkage configuration.



The Attendance Configuration module provides shift schedule settings including attendance rule, attendance check point, holiday schedule, etc..



The Attendance Statistics module provides calculating and analyzing the attendance results.



The Status Monitor module displays access control status and provides anti-control function.



The Door Group Management module provides adding, editing, and deleting the access control group.



The Account Management module provides adding, editing, and deleting the user and assigning permission.



18

The Event Management module provides searching the access control event.

The Log Search module provides searching the configuration logs and control logs.

The function modules are easily accessed by clicking the navigation buttons on the control panel or by selecting the function module from the **View** menu.

You can check the information, including current user and time, in the upper-right corner of the main page.

Chapter 3 Hardware Management

After running the iVMS-4200 access control client, the access controller should be added to the client for the remote configuration and management.

3.1 Device Management



Click Device Management icon on the control panel to enter the access controller management interface.

	Filter ion Refresh
Nickname Device Serial No. Connection Mo IP Port No. Baud Rate Dial-up Security Connection	ion Refresh
Online Device (0) ORefresh Every 60s	
+ Add to Client + Add All 🗹 Modify Netinfo 🦘 Reset Password 🔮 Activate Filter	
P Device Type Firmware Version Security Port Device Serial No. Start Tim	

The interface is divided into two parts: Device Management area and Online Device detection area.

Device Management

Manage the access control devices, including adding, editing, deleting, and batch time synchronizing functions.

Online Device Detection

Automatically detect online devices in the same subnet with the access control client, and the detected devices can be added to the client in an easy way.

Note: The control client can manage 16 access controllers at most.

3.1.1 Access Controller Management

Activating Device and Creating Password

Purpose:

If the access controller is not activated, you are required to create the password to activate them before they can be added to the software and work properly.

Steps:

1. On the **Device for Management** or **Online Device** area, check the device status (shown on **Security** column) and select an inactive device.

Online Device	(1)	Refresh Every 60s					
+ Add to Clie	ent 🕂 Add All	🛛 Modify Netinfo 🥱 Reset Password	🥊 Acti	Filte	er		
IP [*]	Device Type	Firmware Version Security	Port	Device Serial No.	Start Time	Added	
192.168.1.64	DS-K1T200MF-C	V1.0.1build 160310 Inactive	8000	DS-K1T200MF-C20160310V010001CH557814233	2016-03-16 1	No	

- 2. Click the **Activate** button to pop up the Activation interface.
- 3. Create a password in the password field, and confirm the password.



STRONG PASSWORD RECOMMENDED— We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

	Activation		
User Name:	admin		
Password:	•••••		
		Strong	
	Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.		
Confirm Password			
	ОК	Cancel	

- 4. Click **OK** to create the password for the device. A "The device is activated." window pops up when the password is set successfully.
- 5. Perform the following steps to modify the device's network parameters.
 - Click Modify Netinfo to pop up the Modify Network Parameter interface.
 Note: This function is only available on the Online Device area. You can change the device IP address to the same subnet with your computer if you need to add the device to the software.
 - 2) Input the password set in step 3 and click **OK** to complete the network settings.

	Modify Network Parameter	
Device Information:		
MAC Address:	44-19-b6-c2-ce-33	Сору
Version:	V1.0.1build 160310	Сору
Serial No.:	DS-K1T200MF-C20160310V010001CH557814233	Сору
Network Information:		
IP Address:	10.18.130.242	
Port:	8000	
Subnet Mask:	255.255.255.0	
Gateway:	10.18.130.254	
Password:	I	
	ок	Cancel

3) Click **OK** to save the settings.

Adding Online Devices

Purpose:

The active online devices in the same local subnet with the client will be displayed on the **Online Device** area. You can click the **Refresh Every 60s** button to refresh the information of the online devices.

Note: You can click to hide the **Online Device** area.

Online Device (1)	O Refresh Every 60s					
+ Add to Clie	nt 🕂 Add All	🗹 Modify Netinfo 🦘 Reset Password	Activ	vate	Filter		
IP	Device Type	Firmware Version Security	Port	Device Serial No.		Start Time	Added
10.18.130.242	DS-K1T200MF-C	V1.0.1build 160310 Active	8000	DS-K1T200MF-C20160310V010001CH55781	4233	2016-03-16 1	No

Steps:

1. Select the devices to be added from the list.

Note: For the inactive device, you need to create the password for it before you can add the device properly. For detailed steps, please refer to *Creating the Password*.

2. Click Add to Client to open the device adding dialog box.

	Add Device	×
Nickname:		
Connection Method:	TCP/IP ~	
IP Address:	192.168.1.1	
Port:	8000	
User Name:		
Password:		
		_
	Add	Cancel

3. Input the required information.

Nickname: Edit a name for the device as you want.

Connection Type: Select TCP/IP as the connection type.

IP Address: Input the device's IP address. The IP address of the device is obtained automatically in this adding mode.

Port: Input the device port No.. The default value is *8000*.

User Name: Input the device user name. By default, the user name is admin.

Password: Input the device password.

- 4. Click **Add** to add the device to the client.
- 5. (Optional) If you want to add multiple online devices to the client software, click and hold *Ctrl* key to select multiple devices, and click **Add to Client** to open the device adding dialog box. In the pop-up message box, enter the user name and password for the devices to be added. If you want to add all the online devices to the client software, click **Add All** and click **OK** in the pop-up message box. Then enter the user name and password for the devices to be added.
- 6. (Optional) You can select the device from the list and click **Reset Password** to reset the device password.

	Reset Password	×
Export File:	Export	
Import File:	Import	
Password:		
	Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.	
Confirm Password:		
	OK Cancel	

Perform the following steps to reset the device password.

- 1) Click **Export** to save the device file on your PC.
- 2) Send the file to our technical engineers.
- 3) Our technical engineer will send you a file or an eight-digit number to you.
 - If you receive a file from the technical engineer, select **Import File** from Key Importing Mode drop-down list and click is to import the file.
 - If you receive an eight-digit number from the technical engineer, select **Input Key** from Key Importing Mode drop-down list and input the number.
- 4) Input new password in text fields of **Password** and **Confirm Password**.
- 5) Click **OK** to reset the password.



The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in

order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Adding Access Controller Manually

Steps:

1. Click + Add Device to enter the Add Device interface.

		Add Device ×
	Nickname: Connection Method: IP Address: Port: User Name: Password:	TCP/IP v
- 1		Add Cancel

- 2. Input the device name.
- 3. Select the connection mode in the dropdown list: TCP/IP or COM port (1 to 5). **TCP/IP:** Connect the device via the network.

COM1 to COM5: Connect the device via the COM port.

4. Set the parameters of connecting the device.

If you select the connection method as TCP/IP, you should input the device **IP Address**, **Port No.**, **User Name**, and **Password**.

If you select the connection method as COM port, you should input the **Baud Rate** and **Dial-up** value.

5. Click Add button to finish adding.

After adding the device successfully, you can click **Status** to check the detailed status of the access controller, and you can click **Configure** to configure the settings of the access controller.

Modifying Device (Basic Information)

Purpose:

After adding the device, you can configure the device basic information including IP address, port No., etc., and you can also download or read the hardware parameters.

Steps:

1. In the device list, click Modify button to enter the Edit Access Controller interface.

		ntroller		
Download Parameters 🛛 🦳 Rea	d Parameters			
* 📶 10.7.39.120	Basic Information		Network Settings	Capture Settings
4 172.10.18.29	Nickname:	172.10.18.25		
172.10.18.25	Connection Method:	ТСРЛР	~	
	IP Address:	172.10.18.25		
	Port	8005		
	User Name:	admin		
	Password			
		Enable Holiday		
				OK Cancel

- 2. In the device list on the left, select the access controller device and you can edit its basic parameters on your demand, which are the same as the ones when adding the device.
- 3. (Optional) Check the checkbox of **Enable Holiday** to enable the holiday parameters when downloading permissions.
- 4. Click **OK** button to finish editing.
- 5. You can click **Download Parameters** button to download the updated parameters to the local memory of the device.

Download Parameters Read Param	neters		
· 🗐 10.7.39.120	Door Information:		
• 🚮 172.10.18.29	Door Magnetic:	Normal Closed 🗸	
- 172.10.18.25	Exit Button Type:	Normal Closed ~	
* 172.10.18.25 Door2	Door Locked Time:	0	s
172.10.18.25_Door3	Door Open for Disabled Person:	0	s
🔹 🧧 172.10.18.25_Door4	Door Open Timeout:	0	s
	Enable Lock Door when Door Close:	No ~	
	Duress Code:		
	Super Password:		
	Dismiss Code:		
			OK Cancel
			Galcer

Modifying Device (Door Information)

Steps:

1. In the device list on the left, click 📩 to expand the access controller, select the door (access control point) and you can edit the information of the selected door on the right.

Door Magnetic: The Door Magnetic is in the status of **Normal Closed** (excluding special conditions).

Exit Button Type: The Exit Button Type is in the status of Remain Open (excluding special

conditions).

Door Locked Time: After swiping the normal card and relay action, the timer for locking the door starts working.

Door Open for Disabled Person: The door magnetic can be enabled with appropriate delay after disabled person swipes the card.

Door Open Timeout: The alarm can be triggered if the door has not been close

Enable Lock Door when Door Close: The door can be locked once it is closed even if the Door Locked Time is not reached.

Duress Code: The door can open by inputting the duress code when there is duress. At the same time, the client can report the duress event.

Super Password: The specific person can open the door by inputting the super password.

Dismiss Code: Input the dismiss code to stop the buzzer of the card reader.

Note: The Duress Code, Super Code, and Dismiss Code should be different.

- 2. Click **OK** button to save parameters.
- Click Download Parameters button to download the updated parameters to the local memory of the device.

Modifying Device (Card Reader Information)



Steps:

- 1. In the device list on the left, click 🖆 to expand the door, select the card reader name and you can edit the card reader information on the right.
- 2. You can editing the following parameters:

Enable Card Reader: Select Yes to enable the card reader. OK LED Polarity: Select the OK LED Polarity of the card reader mainboard. Error LED Polarity: Select the Error LED Polarity of the card reader mainboard Buzzer Polarity: Select the Buzzer LED Polarity of the card reader mainboard Interval between Card Swiping: If the interval between card swiping of the same card is less than the set value, the card swiping is invalid. You can set it as 0 to 255.

Max. Interval When Inputting Password: When you inputting the password on the card reader, if the interval between pressing two digits is larger than the set value, the digits you pressed before will be cleared automatically.

Enable Attempts Limit of Card Reading Failure: Enable to report alarm when the card reading attempts reach the set value.

Max. Times of Card Swiping Failure: Set the max. failure attempts of reading card.

Anti-Tamper Detection: Enable the anti-tamper detection for the card reader.

Detection Time for Card Reader Offline: When the access controller cannot connect with the card reader for longer than the set time, the card reader will turn offline automatically.

Mode: Select the card reader mode as normal mode (reading card) or issuing card mode (getting the card No.).

- 3. Click **OK** button to save parameters.
- 4. Click **Download Parameters** button to download the updated parameters to the local memory of the device.

Deleting Device

Steps:

- 1. In the device list, click to select a single device, or select multiple devices by pressing *Ctrl* button on your keyboard and clicking them one by one.
- 2. Click Remove button to delete the selected device(s).
- 3. Click **OK** button in the pop-up confirmation dialog to finish deleting.



Time Synchronization

Steps:

- 1. In the device list, click to select a single device, or select multiple devices by pressing *Ctrl* button on your keyboard and clicking them one by one.
- 2. Click Synchronization button to start time synchronization.

A message box will pop up on the lower-right corner of the screen when the time synchronization is compeleted.

Viewing Device Status

In the device list, you can click Status button to enter view the status.

Door Status Host Status Card Reader Status Alarm Input Status Alarm Output Status	Door Name 1 2 3 4	Close Close Close Close	Normal Status Normal Status Normal Status	Close Close Close
Host Status Card Reader Status Alarm Input Status Alarm Output Status	1 2 3 4	Close Close Close	Normal Status Normal Status Normal Status	Close Close
Card Reader Status Alarm Input Status Alarm Output Status	2 3 4	Close Close	Normal Status Normal Status	Close
Alarm Input Status Alarm Output Status	3	Close	Normal Status	Close
Alarm Output Status	4			
Frank Concer Status	-	Close	Normal Status	Close
event sensor status				

Door Status: The status of the connected door.

Host Status: The status of the host, including Storage Battery Power Voltage, Device Power Supply Status, Multi-door Interlocking Status, Anti-passing Back Status, Host Anti-Tamper Status.

Card Reader Status: The status of card reader.

Alarm Input Status: The alarm input status of each port.

Alarm Output Status: The alarm output status of each port.

Event Sensor Status: The event status of each port.

Remote Configuration

	Rei	mote Configuration		
- 🗞 System	Displaying the Device	Information		
🔮 Device Information	Basic Information			
 Derect and Mildon General Security Password Management Alarm Alarm Other Operation 	Easic Information Device Type: Electric Lock Number: Device Serial No: Version Information Firmware Version: Hardware Version:	D5-K1T105M-C 1 D3-K1T105M-C20150828V0 V1.0.0 build 150828 0x10001	Local Trigger Number: Local RS-485 Number: 10000CH546414456	1

3.1.2 Network Settings

Purpose:

In the network settings interface, the network settings of the device can be uploaded and reported.

Uploading Mode Settings

	Network Settings ×
Uploading Mode Settings Netw	ork Center Settings Wireless Communication Center Settings
Center Group:	Center Group1
Report Type:	Alarm Data
Uploading Mode Settings:	
Main Channel:	Close
Backup Channel:	Close
	OK Cancel

Steps:

- 1. In the Edit Access Controller interface, click **Network Settings** button to enter the network settings interface.
- 2. Click the Uploading Mode Settings tab.
- 3. Select the center group in the dropdown list.
- 4. Check the **Enable** checkbox to enable the selected center group.
- 5. Select the report type in the dropdown list.
- Select the uploading mode in the dropdown list. You can enable N1/G1 for the main channel and the backup channel, or select off to disable the main channel or the backup channel.

Note: The main channel and the backup channel cannot enable N1 or G1 at the same time.

7. Click **OK** button to save parameters.

Network Center Settings

	Netv	vork Settings	×
Uploading Mode Settings	Network Center Settings	Wireless Communication Center	Settings
Center Gr	oup: Center1	~	
IP Addre	ess:		
F	Port: 0		
Protocol T	ype: ehome	~	
Acco	unt		
			OK Cancel

Steps:

1. In the Edit Access Controller interface, click **Network Settings** button to enter the network settings interface.

- 2. Click the Network Center Settings tab.
- 3. Select the center group in the dropdown list.
- 4. Input IP address and port No..
- 5. Select the protocol type as Ehome. The default port No. for Ehome is 7661.
- 6. Set an account name for the network center. A consistent account should be used in one platform.
- 7. Click **OK** button to save parameters.

Note: The port number of the wireless network and wired network should be consistent with the port number of Ehome.

Wireless Communication Center Settings

APN Name:	CMNET
SIM Card No.:	
Center Group:	Center1 ~
IP Address:	
Port	0
Protocol Type:	ehome 👻
Account	

Steps:

- 1. In the Edit Access Controller interface, click **Network Settings** button to enter the network settings interface.
- 2. Click the Wireless Communication Center Settings tab.
- 3. Select the APN name as CMNET or UNINET.
- 4. Input the SIM Card No..
- 5. Select the center group in the dropdown list.
- 6. Input the IP address and Port No.
- 7. Select the protocol type as Ehome. The default port No. for Ehome is 7661.
- 8. Set an account name for the network center. A consistent account should be used in one platform.
- 9. Click **OK** button to save parameters.

Note: The port number of the wireless network and wired network should be consistent with the port number of Ehome.

3.1.3 Capture Settings

Purpose:

In the capture settings interface, you can set the parameters of capture linkage and manual capture. *Note:* Before setting the capture setting, you should configure the storage server for picture storage. For details, refer to *Chapter 7.3.4 Storage Server Configuration*.

Linked Capture

	Capture Settings	
Linked Capture Manual Capt	ure	
Capture Times:	0 ~	
Capture Interval 1:		ms
Capture Interval 2:		ms
Capture Interval 3:		ms
Capture Interval 4:		ms
		Save Cancel

Steps:

- 1. In the Edit Access Controller interface, click **Capture Settings** button to enter the capture settings interface.
- 2. Select the Linked Capture tab.
- Set the linked capture times once triggered.
 Set the capture interval according to the capture times.
- 4. Click **Save** to save the settings.

Manual Capture

Steps:

- 1. In the Edit Access Controller interface, click **Capture Settings** button to enter the capture settings interface.
- 2. Select the Manual Capture tab.
- Select the resolution of the captured pictures from the dropdown list. *Note:* The supported resolution types are CIF, QCIF, 4CIF/D1, SVGA, HD720P, VGA, WD1, and AUTO.
- 4. Select the picture quality as Best, Better, or Normal.
- 5. Click **Save** to save the settings.
- 6. You can click **Restore Default Value** to restore the parameters to default settings.

	Capture Settings	×
Linked Capture Manual Capture		
Picture Size:	CIF	
Picture Quality:	Best	
		Save Restore Def

3.2 Door Group Management



Click **Door Group Management** icon on the control panel to enter the Door Group Management interface.

+ Add Group X Delete Group							
Search	P + Import	☑ Modify	X Delete			Filter	
	Serial No.	Door Name	Belong to Controller	Door Camera	Position		

The interface is divided into two parts: Group Management area and Access Control Point Management area.

Group Management

The access control points can be added to different groups to realize the centralized management.

• Access Control Point Management

Manage the specific access control point (door) under the group, including importing, editing and deleting access control point.

3.2.1 Access Control Group Management

Adding Group

Before you can manage the doors, you need to create groups first.

Steps:

1.

Click Add Group button on the left to pop up the Add Group dialog.

	Ado	l Group		×
Name:	Test_Group			
		ОК	Cancel	

2. Input the group name in the text field and click **OK** button to finish adding.

Editing Group

After adding the group, you can move the mouse to the group name and click 🔟 to pop up the Modify Group dialog box.

Or you can double click the group to edit the group name.

Deleting Group

You can move the mouse to the group name and click to delete the selected group. Or you can click to select the group and click **Celete Group** to delete it. **Note:** All the access control point in the group will be deleted.

3.2.2 Access Control Point Management

After adding the group, you can import the access control point of the added access controller to the group.

Importing Access Control Point

Steps:

1. Select the added group, and click **here import** button to pop up the access control point importing interface as follows.

Import Access Control Point ×							
Access Control Point		Group	+				
Search		Search	۶				
- 💷 10.7.39.120		- 🔟 Test_Group					
0.7.39.120_Door1		10.7.39.120_Door4					
A 172.10.18.29		10.7.39.120_Door3					
. 41 172.10.18.25		10.7.39.120_Door2					
172.10.18.25_Door4		172.10.18.25_Door3					
		172.10.18.25_Door2					
		172.10.18.25_Door1					
		172.10.18.29_Door1					
	Import						
	Import All						

- 2. Select the access control point to import from the access control point list on the left.
- 3. Select an added group to import the access control point on the right.
- 4. Click **Import** button to import the selected access control points or you can click **Import All** to import all the available access control points to the selected group.
- 5. (Optional) You can click 📩 button on the upper-right corner of the window to create a new group.

Move the mouse to the added group or access control point and click \mathbf{M} or \mathbf{M} to edit or delete it.

Note: Up to 64 access control points can be imported to the door group.

Editing Access Control Point

Steps:

- 1. Check the checkbox to select the imported access control point in the list and click Modify button to edit the access control point.
- 2. You can edit the access control point name and the position.
- 3. You can view the card reader under the selected access control point.
- 4. Click **OK** to save the settings.

Deleting Access Control Point

Check the checkbox to select the imported access control point and click the selected access control point.

Chapter 4 Permission Configuration

You can add the department and person to the client for management, and add card for access control. You can set the schedule template and configure the access control permission via the client.

4.1 Person Management



Click Person Management icon on the control panel to enter the Person Management interface.

You can add, edit, and delete the department and person in Person Management module.

Add Department	Delete Department	Person Manager	nent						
Search	9	Add Person	Edit Person	Delete Per	r Issue Car	Import Pi	Import Pe	Export Pe Filt	er
🗾 Default Depa	artment	Serial No.	Name	Gender	Department	ID No.	ID Type	Contact Phone No.	Card Management
		Total:0 Page:1/1						Page	Go to

The interface is divided into two parts: Department Management and Person Management.

Department Management

You can add, edit, or delete the department as desired.

Person Management

After adding the department, you can add the person to the department for further management.

4.1.1 Department Management

Adding Department

Steps:

1. In the department list on the left, the Default Department already exists in the client as the parent department of all departments.

2. Select the upper department and click Add Department button to pop up the adding department interface to add the lower department.

_	Add Department	×
Upper Department:	Default Department	
Department No:	A2BA6556C87A417CAD1B7C37360FD7AA	
Department Name:	[٦
	21/ 0-2-2-1	-
	OK Cancel	

- 3. Input the Department Name as desired.
- 4. Click **OK** to save the adding.

Notes:

- You can add multiple levels of departments according to the actual needs. Click a department as the upper-level department and click Add Department button, and then the added department will be the sub-department of it.
- Up to 10 levels can be created.

Editing and Deleting Department

You can double-click the added department to edit its name.

You can click to select a department, and click Delete Department button to delete it. **Notes:**

- The lower-level departments will be deleted as well if you delete a department.
- Make sure there is no person added under the department, or the department cannot be deleted.

4.1.2 Person Management

After adding the department, you can add person to the department and manage the added person such as issuing card in batch, importing and exporting person information in batch, etc.. *Note:* Up to 3000 persons can be added.

Adding Person (Basic Information)

Steps:

- 1. Select a department in the department list and click **Add Person** to pop up the adding person interface.
- 2. Click **Basic Information** tab to input the person's basic information.

		Add Pers	GON	×
Basic Information	Fingerprint			
Person No.:	2016032119	300836		
*Name: Gender:	Male	Female		
ID Type:	ID	v		
ID No.:				
Department:	nan Resourc	e Department		
Contact No.:			Upload Picture	
Address.				
			ОК	Cancel

- 3. The Person No. will be generated automatically and is not editable.
- 4. Input the basic information including person name, gender, ID type, ID No., contact No., and address.
- Click Upload Picture to select the person picture from the local PC to upload it to the client. *Note:* The picture should be .jpg, or .jpeg format.
- 6. Click **OK** to finish adding.

Adding Person (Fingerprint)

Before inputting the fingerprint, you should connect the fingerprint machine to the PC and set its parameters first. For details, refer to *Chapter 7.3.3 Fingerprint Machine Configuration*. *Steps:*

1. In the Add Person interface, click Fingerprint tab.



2. Click Start Register button, click to select the fingerprint to start collecting.

3. Lift and rest the corresponding fingerprint on the fingerprint scanner twice to collect the fingerprint to the client.

You can select the registered fingerprint and click **Delete Fingerprint** to delete it.

You can click **Delete All** to clear all fingerprints.

4. Click **OK** to save the fingerprints.

Editing and Deleting Person

You can double-click the added person to edit its basic information and fingerprint.

Or you can check the checkbox to select the person and click Edit Person to edit it.

You can click to select a person, and click **Delete Person** to delete it.

Note: If a card is associated with the current person, the association will be invalid after the person is deleted.

Importing and Exporting Person Information

The person information can be imported and exported in batch. *Steps:*

 After adding the person, you can click **Export Person** button to export all the added person information to the local PC including person No., person name, gender, ID type, ID No., Department, telphone No., and contact address.

	Export Person	
Saving Path:		
Note: The ope	eration will export all the existing persons.	
	ок	Cancel

Click Loss to select the path of saving the exported Excel file. Click **OK** to start exporting.

2. To import the Excel file with person information in batch from the local PC, click **Import Person** button.

	Import Person	×
Please select the fi	le to import.	
Import File:		
	Download Person Importing Template	
	OK	Cancel
		Cancer

You can click Download Person Importing Template to download the template first.

Input the person information to the downloaded template.

Click 📃 to select the Excel file with person information.

Click **OK** to start importing.

Importing Person Picture

After adding the person information to the client, you can also import person picture to the client in batch.

Steps:

1. Click Import Picture button.



2. Click select the package with person pictures and click **OK** to start importing. *Notes:*

- The picture name should be the same as the corresponding person's person No..
- Each picture should be less than 2 MB and should be in .jpg format.
- The package file should be .zip file.
- The package file should be less than 100 MB.

Card Operation

Select the person and click 🧧 for further operation such as issuing card, editing card No., , reporting card loss, card replacement, and returning card.

				Card Op	eration		
Pers Card	on Information Holder Name: Contact No.:	Cindy 55555			Department: ID No.:	Default /Human Resource D 98765432	epartment More
	Serial No.	Card No.	Card Type	Effective Ti	me	Expiry Time	Issue Card
	1	1234567891	Report Card Los	s 2016-03-08	00:00:00	2036-12-31 23:59:59	Change Card
	2	4512124546	Normal Card	2016-03-09	00:00:00	2036-12-31 23:59:59	Report Card Loss
							Cancel Card Loss
							Card Replacement
							Return Card

You can click More to view the person details.

For details about these operation, please refer to Chapter 4.2 Card Management.

Issuing Card in Batch

After adding the card information to the client, you can issuing card for the person in batch. For details about adding the card, please refer to *Chapter 4.2 Card Management*.

Steps:

- 1. Check the checkbox to select the person for issuing card.
- 2. Click Issur Card in Batch button to enter the following interface.

		Issue	Card in Batch			
Effective Time:	2016-03-21 00:00:0	00 📆 Expiry Time	2036-12-31 23	:59:59 武		
Open card for th	ne following persons	:				
Serial No.	Person Name	Department	Telephone No.	Card No.		
1	Wendy	Default /Hum	987654321			
2	Cindy	Default /Hum	55555			
					ок	Cancel

- 3. Click 📅 to set the effective time and expiry time of the card. Click **OK** to save the time settings.
- 4. In the person list, you can view the selected person details including person name, department, and telephone number.

Click 🔄 to select card to be issued to the person.

		Select Card	
Please select card to c	hange.		
			Search
Serial No.	Card No.	*	Ê
1	12345		
2	12346		
3	12347		
4	12348		
5	12349		
6	12350		
7	12351		
8	12353		
9	12354		
10	12355		
11	12356		
12	12357		
13	12358		
14	12359		
15	12360		
Total:45 Page:1/1		M A D Page	Go to
		ок	Cancel

Select the card from the card list and click **OK** to save the settings. You can input the card No. and click **Search** button to search the card.

5. Click **OK** to complete the card issuing.

4.2 Card Management



Click Card Management on the control panel to enter the card management interface.

Empty Card Normal Card Lost Card		
Empty Card List		
+ Add Card Issue Card X Delete	Search	Search
Serial No. Card No.		
1 123456789		
Total:1 Page:1/1	Page	Go to

There are three card types: Empty Card, Normal Card, and Lost Card.

Empty Card: A card has not been issued with a person.

Normal Card: A card is issued with a person and is under normal using. **Lost Card:** A card is issued with a person and is reported as lost.

4.2.1 Empty Card

Click **Empty Card** tab to manage the empty card first.

Empty Card Normal Card Lost Card		
Empty Card List		
+ Add Card Issue Card X Delete	Search	Search
Serial No. Card No.		
1 123456789		

Adding Card

Before you start:

Make sure a card reader is connected to the PC and is configured already. Refer to *Chapter 7.3.2 Card Reader Configuration* for details.

Steps:

- 1. Click Add Card button to pop up the Add Card dialog box.
- 2. Two adding methods are supported.
 - ♦ Adding Single Card

Select Single Adding as the adding mode and input the card No..

Note: The Card No. should be 1 to 10 digits.

Add Ca	ard ×
Adding Method: 💿 Single Adding	Batch Adding
Enter Card No.:	
	OK Cancel

♦ Batch Adding Cards

Select Batch Adding as the adding mode. Input the start card No. and the end card No..

Notes:

- The start card No. and the last card No. should be the with same length. E.g., the last card No. is 234, then the start card No. should be like 028.
- The Card No. should be 1 to 10 digits.

	Add Car	ď	×
Adding Method:	Single Adding	e Batch Adding	
Start Card No.: End Card No.:			
		OK Cancel	1

- 3. Click **OK** button to finish adding.
- 4. You can check the checkbox of the added card and click **Pelete** to delete the card.

Issuing Card

After adding the card to the client, you can issue it to the corresponding added person. You can also issuing the cards to persons in batch. For details, refer to *Chapter 4.1.2 Person Management*. *Steps:*

1. Click an added empty card in the list and click Issue Card button to issue the card with a person. You can also double click the empty card in the card list to enter the **Issue Card** interface as follows.

		Issue Card		
Card No.:	12370	Card Password:		
Effective Time:	2016-03-21 00:00:00 🛅	Expiry Time:	2036-12-31 23:59:59 📸	
Please choose	person node to issue card	i.		
Search				٩
🖃 🔝 Default	t Department			
🖃 🔝 Hur	man Resource Department			
	Wendy			
	Cindy			
Please choose	responding fingerprint for	card:		
			ОК	Cancel

- 2. Input the password of the card itself. The card password should contain 4 to 8 digits.
- 3. Click 🏙 to set the effective time and expiry time of the card. Click **OK** to save the time settings.
- 4. Click to select a person and select a fingerprint for the card.

5. Click **OK** to finish issuing card.

Notes:

- The issued card will disappear from the Empty Card list, and you can check the card information in the Normal Card list.
- Up to 2000 cards can be added.

4.2.2 Normal Card

After adding the empty card to the client and issue the card to the person, the card will be displayed in the Normal Card list.

Click **Normal Card** tab in the card managemet interface to show the Normal Card list. You can view all the issued card information, including card No., card holder, and the department of the card holder.

Empty C	ard Normal (Card Lost Card					
Norm	Normal Card List						
Chan	ge Card R	teturn Card R	eport Car Set Pa	assword Import	Export	Search	Search
	Serial No.	Card No.	Туре	Card Holder Name	Department		
•	1	123456789	Normal Card	Wendy	Default Department		

Editing Card

You can double click the normal card in the list to modify the card linked person information.

	Modif	y Card-involved Inf	ormation	×
Card No.:	12352	Card Password:		
Effective Time:	2016-03-09 00:00:00 📸	Expiry Time:	2036-12-31 23:59:59 📸	
Please choose	person node to issue card	d.		
Search				9
🖃 🔠 Defaul	t Department			
🖃 🚠 Hu	man Resource Department			
2	Wendy			
1	Cindy			
Please choose	responding fingerprint for	card:		
			ОК	Cancel

You can modify the card effective time and expiry time, and you can change the person and select the conrresponding fingerprint to issue the card again.

Changing Card

Steps:

1. Check the checkbox to select a normal card and click **Change Card** button to change the associated card for card holder.

Change Card		
Old Card No.:	12352	
Card Status:	Normal Card	
Card Holder No.:	2016030817552595	
Card Holder Name:	Wendy	
New Card No.:		
	OK Cancel	

- 2. In the pop-up window, click and select another card in the popup window to replace the current card.
- 3. Click **OK** to save the changes.

Returning Card

Steps:

- Check the checkbox to select an issued card and click **Return Card** button to cancel the assotiation of the card. Then the card will disappear from the Normal Card list, and you can find it in the Empty Card list.
- 2. Click **OK** to comfirm the operation.

Reporting Card Loss

Steps:

- 1. Check the checkbox to select an issued card and click **Report Card Loss** button to set the card as the Lost Card, that is, an invalid card.
- 2. Click **OK** to comfirm the operation.

Setting Card Password

Steps:

1. Check the checkbox to select an issued card and click **Set Password** button to set the password for the card.

	Set Password	
Card No.:	12352	
Card Password:		
Confirm Password:		
	OK Cancel	

- 2. Input the card password and confirm the password. The card password should contain 4 to 8 digits.
- 3. Click **OK** to save the settings.
Note: The password will be required when the card holder swiping the card to get enter to or exit from the door if you enable the card reader authentication mode of **Card and Password**, **Password and Fingerprint**, and **Card**, **Password**, **and Fingerprint**. For details, refer to *Chapter 4.7.2 Card Reader Authentication*.

Importing and Exporting Cards

Steps:

1. To import the card and person information from the local PC, click **Import** button to pop up the following dialog box.

	Import Person and Card Information	
Please select the fil	e to import.	
Import File:		
Down	load Person and card Information Template	
	ОК	Cancel

Click **Download Person and Card Infotmation Template** to download the template for importing. In the template file, input the card holder name and the corresponding card No..

Note: The Card No. should be 1 to 10 digits

Click 🔄 to select the template file with card and person information.

Click **OK** to start importing.

2. To export all the normal card information to the local PC, click **Export** button to pop up the following dialog box.

Click 🔤 to select the path to save the exported file.



Click **OK** to start exporting. All the normal cards with card holder name and card No. will be exported to the Excel file.

4.2.3 Lost Card

You can manage the card which is reported as lost, including canceling card loss and replacing card. Click **Report Card Loss** tab in the card managemet interface to show the Lost Card list. You can view all the lost card information, including card No., card holder, and the department of the card holder.

1	Empty (Card Normal	Card Lost Card						
	Lost	Card List							
	Can	cel Car R	eplace Card					Search	Search
	•	Serial No.	Card No.	Туре	Card Replaced	Card Holder Name	Department		
	•	1	123456789	Report Card Loss	No	Wendy	Default Department		
	<	1	123456789	Report Card Loss	No	Wendy	Default Department		

Canceling Card Loss

Steps:

- 1. Check the checkbox to select the lost card in the list.
- 2. Click Cancel Card Loss button to resume the card to the normal card.
- 3. Click **OK** to confirm the operation.

Card Replacement

Steps:

- 1. Check the checkbox to select the lost card in the list.
- 2. Click Replace Card button to issue a new card to the card holder replacing for the lost card.

	Replace Card	
Old Card No.:	1234567891	
Card Status:	Report Card Loss	
Card Holder No.:	2016030818260397	
Card Holder Name:	Cindy	
New Card No.:		
	ок	ancel

- 3. Click button to select another card in the popup window as the new card and the predefined permissions of the lost card will be copied to the new one automatically.
- 4. Click **OK** to save the changes.

4.3 Schedule Template



Click Template on the control panel to enter the schedule template interface.

📰 Week Plan 🔳 Holiday Group 🔳	Template				
+ Add Week X Delete W	Property				- Save
Search 9 Enable Week Plan by Default	Wee	k Plan Name:	Disable Week Plan	by Default	
Disable Week Plan by Default		Remark:	The disabled week week plan is on, sw	plan cannot be deleted. When disabled iping card is invalid for the whole day.	
				Copy to	X Delete D 💼 Clear
	Mon	0 2 4	6 8	10 12 14 16 18	20 22 24
	Tue	0 2 4	6 8	10 12 14 16 18	20 22 24
	Wed	0 2 4	6 8	10 12 14 16 18	20 22 24
	Thu	0 2 4	6 8	10 12 14 16 18	20 22 24
	Fri	0 2 4	6 8	10 12 14 16 18	20 22 24
	Sat	0 2 4	6 8	10 12 14 16 18	20 22 24
	Sun	0 2 4	6 8	10 12 14 16 18	20 22 24

You can manage the schedule of access control permission including Week Plan, Holiday Plan, and Template.

4.3.1 Setting Week Plan

Click Week Plan tab to enter the Week Plan Management interface.

The client defines two kinds of week plan by default: **Enable Week Plan by Default** and **Disable Week Plan by Default**, which cannot be edited. You can define custom plans on your demand.

Steps:

1. Click Add Week... button to pop up the adding plan interface.

	Add Week Plan	×
Week Plan Name:		
	OK Cancel	1

- 2. Input the name of week plan and click **OK** button to add the week plan.
- 3. Select the added week plan in the plan list on the left and you can view its property on the right.
- 4. You can edit the week plan name and input the remark information.
- 5. On the week schedule, click and drag on a day to draw on the schedule, which means in that period of time, the configured permission is activated.

Note: Up to 8 time periods can be set for each day in the schedule.

6. When the cursor turns to 🕅, you can move the selected time bar you just edited. You can also edit the displayed time point to set the accurate time period.

When the cursor turns to 🖼, you can lengthen or shorten the selected time bar.

- Optionally, you can select the schedule time bar, and then click **Delete Duration** to delete the selected time bar, or click **Clear** to delete all the time bars, or click **Copy to Week** to copy the time bar settings to the whole week.
- 8. Click **Save** to save the settings.

4.3.2 Setting Holiday Group

Click Holiday Plan tab to enter the Holiday Plan Management interface.

📰 Week Plan 🔳 Holiday Group	Template					
+ Add Holi X Delete H	Property					H Save
Search 9	Holiday Gr	oup: Long	g Holiday			
	Ren	nark:				
	Holiday List			+ Add Holid	ay Prev Page	▶ Next Page
	Serial No.	Start Date	End Date	Duration		Operation
	1	3/9/2016 🔀	3/9/2016	0 2 4 6 8 10 12	14 16 18 20 22 24	🛛 📩 🔀

Steps:

1. Click Add Holiday Group button on the left to pop up the adding holiday group interface.

	Add Holiday Group	×
Holiday Group Name:		
	OK Cancel	1

- 2. Input the name of holiday group in the text filed and click **OK** button to add the holiday group.
- 3. Select the added holiday group and you can edit the holiday group name and input the remark information.
- 4. Click + Add Holiday icon on the right to add a holiday period to the holiday list and configure the duration of the holiday.

Note: Up to 16 holiday can be added to one holiday group.

Holiday List					+ Add Holiday	Prev Page	Next Page
Serial No.	Start Date	ļ	End Date	Duration			Operation
1	3/9/2016	<u></u>	3/9/2016	0 2 4	6 8 10 12 14 1	6 18 20 22 2	4 🛛 💼 🗙
2	3/23/2016	<u>**</u>	3/31/2016	10 2 4	6 8 10 12 14 1	6 18 20 22 2	4 🛛 💼 🗙

1) On the period schedule, click and drag to draw the period, which means in that period of time, the configured permission is activated.

Note: Up to 8 time durations can be set for each period in the schedule.

- 2) When the cursor turns to X, you can move the selected time bar you just edited. You can also edit the displayed time point to set the accurate time period.
- 3) When the cursor turns to 😚, you can lengthen or shorten the selected time bar.
- 4) Optionally, you can select the schedule time bar, and then click is to delete the selected time bar, or click to delete all the time bars of the holiday,

or click 🏋 to delete the holiday directly.

5. Click **Save** to save the settings.

Note: The holidays cannot be overlapped with each other.

4.3.3 Setting Schedule Template

After setting the week plan and holiday plan, you can configure the schedule template. *Note:* The priority of holiday group schedule is higher than the week plan.

The client defines two kinds of template by default: **Default Enable Schedule Template** and **Default Disable Schedule Template**, which cannot be edited. You can define custom templates on your demand.

Steps:

1. Click **Add Template** to pop up the adding template interface.



- 2. Input the template name in the text filed and click **OK** button to add the template.
- 3. Select the added template and you can edit its property on the right. You can edit the template

name and input the remark information.

4. Select a week plan to apply to the schedule.

Click Week Plan tab and select a plan in the dropdown list.

You can also click **Add Week Plan** to add a new week plan. For details, refer to *Chapter 4.3.1 Setting Week Plan*.



Select holiday groups to apply to the schedule.
 Note: Up to 4 holiday groups can be added.

Holiday Group to be Selected	The selecte	d holiday group		
+ Add Holi	Serial No.	Holiday Group Name	Remark	
Search	1	Long Holiday		
Long Holiday	-	Long Honday		
+ Add				
X Delete				
💼 Clear				

Click to select a holiday group in the list and click Add to add it to the template. You can also click Add Holiday Group to add a new one. For details, refer to *Chapter 4.3.2 Setting Holiday Group*.

You can click to select an added holiday group in the right-side list and click delete it.

You can click **clear** to delete all the added holiday groups.

6. Click **Save** button to save the settings.

4.4 Door Status Duration Management

Purpose:

You can schedule weekly time periods for a door to remain open or closed.



Click Status Monitor icon on the control panel and click Status Duration button to enter the Status

Duration interface.

					Status [Ouration								
Access Control List 🛃 Access Control	Door Statu	s Confi	guration											📄 Copy to 🖶 Save
Search P	Re	main O	pen	R	emain C	losed		Copy to	Week		Delete	Duration		💼 Clear
- 4 10.7.39.120		0	2	4	6	8	10	12	14	16	18	20	22	24
10.7.39.120_Door2	Mon	0	2	4	6	8	10	12	14	16	18	20	22	24
■ 10.7.39.120_Door4	Tue	0	2	4	6	8	10	12	14	16	18	20	22	24
	Wed	0	2	4	6	8	10	12	14	16	18	20	22	24
	Thu	0	2	4	6	8	10	12	14	16	18	20	22	24
	Fri	0	2	4	6	8	10	12	14	16	18	20	22	24
	Sat		2	4	6	8	10	12	14	16	18	20	22	24
	Sun		2				10	12	14	10	10	20		

Steps:

- 1. Click to select a door from the access control list on the left.
- 2. On the Door Status Configuration panel on the right, draw a schedule for the selected door.
 - Select a door status brush as <a>Remain Open or <a>Remain Closed.
 Remain open: The door will keep open during the configured time period. The brush is marked as <a>Remain Open.

Remain Closed: The door will keep closed during the configured duration. The brush is marked as **marked**.

2) Click and drag on the timeline to draw a color bar on the schedule to set the duration.



Note: The min. segment of the schedule is 30min.

When the cursor turns to \mathbb{R}^{n} , you can move the selected time bar you just edited. You can also edit the displayed time point to set the accurate time period.

When the cursor turns to 🚰, you can lengthen or shorten the selected time bar.

- 3. Optionally, you can select the schedule time bar and click **Copy to Other Day** to copy the time bar settings to the other dates
- You can select the time bar and click Delete Duration to delete the time period. Or you can click Clear to clear all configured durations on the schedule.
- 5. Click **Save** to save the settings.
- 6. You can click **Copy to** button to copy the schedule to other doors.
- 7. Click 🛃 Access Control to popup the Access Control Status Downloading dialog box.



Select a control point and click **OK** to download the settings to access control point.

Note: The door status duration settings will take effect after downloading the settings to the access control point.

4.5 Linkage Configuration



Click Linkage Configuration on the control panel to enter the Linkage Configuration interface.

Event Alarm Linkage Event Card Linkage Clien	t Linkage				
Event Alarm Linkage 🛃 Download Settings	Property				H Save
Search 10.7.39.120 172.10.18.29 172.10.18.29_Event1 172.10.18.29_Event2 172.10.18.25	Host Buzzer: Reader Buzzer: Alarm Output:	Not Link D Lin	k Property Property		
	Door:	Name C	pen	Close	1

You can set alarm linkage modes of the access controller, including event alarm linkage, event card linkage, and client linkage.

4.5.1 Event Alarm Linkage

Purpose:

The event alarm (refer to the triggers of the access controller) can be linked to some actions (e.g., alarm output, host buzzer) when it is triggered.

Steps:

1. Click Event Alarm Linkage tab to enter the following interface.

rent Alarm Linkage 🛃 Download Settings	Property	
earch 10.7.39.120 17.2.10.18.29 172.10.18.29_Event1 172.10.18.29_Event2 172.10.18.25	 ✓ Host Buzzer: ✓ Reader Buzzer: 	Not Link Link Name Property 172.10.18.29_Reader Not Link Link 172.10.18.29_Reader Not Link Link
	Alarm Output:	Name Property 172.10.18.29_Alarm Not Link Link
	✓ Door:	Name Open Close 172.10.18.29_Do Not Link Not Link

2. In the event alarm linkage on the left, select an event alarm.

3.	Check the checkbox of the corresponding linkage actions and switch the property from to					
	C to enable this function.					
	Host Buzzer: The audible warning of controller will be triggered.					
	Reader Buzzer: The audible warning of card reader will be triggered.					
	Alarm Output: The alarm output will be triggered for notification.					
	Door (Open/Close): The door will be open or closed when the case is triggered.					
	<i>Note:</i> The Door cannot be configured as open or closed at the same time.					
4.	Click Save button to save the settings.					

5. Click Download Settings to download the updated parameters to the local memory of the device to take effect.

4.5.2 Event Card Linkage

In the Linkage Configuration interface, click **Event Card Linkage** tab to enter the following interface.

ent Card Linkage 🔬 Do	wnload Settings	Linkage Details				+ Add X D	elete 🕞 Save
earch	9	 Event Source: - Event Linka 	age: Device Event	v Device Tamperin	 Card Linkag 	e:	v
		-Linkage Target Host Buzzer: Reader Buzzer	Not Link 🕖 Linł	¢	Capture: Not Lir Alarm Output	nk 🔘 Link	
		Name	Property		Name	Property	
		Door					
		Name	Open	Close	Remain Open	Remain Closed	

Select the access controller from the list on the left.

Click **Add** button to add a new linkage. You can select the event source as **Event Linkage** or **Card Linkage**.

Event Linkage

For the event linkage, the alarm event can be divided into four types: device event, alarm input, door event, and card reader event.

Steps:

- 1. Click to select the linkage type as **Event Linkage**, and select the event type from the dropdown list.
 - For Device Event, select the detailed event type from the dropdown list.
 - For Alarm Input, select the type as alarm or alarm recovery and select the alarm input name

from the table.

- For Door Event, select the detailed event type and select the door from the table.
- For Card Reader Event, select the detailed event type and select the card reader from the table.
- 2. Set the linkage target, and switch the property from \bigcirc to \bigcirc to enable this function.
 - **Host Buzzer**: The audible warning of controller will be triggered.
 - **Capture**: The real-time capture will be triggered.
 - **Reader Buzzer**: The audible warning of card reader will be triggered.
 - Alarm Output: The alarm output will be triggered for notification.
 - Door: The door status of open, close, normally open, and normally close will be triggered.
 Note: The door status of open, close, normally open, and normally close cannot be triggered at the same time.
- 3. Click Save button to save parameters.
- 4. Click Download Settings to download the updated parameters to the local memory of the device to take effect.

Card Linkage

Steps:

- 1. Click to select the linkage type as Card Linkage.
- 2. Select the card from the dropdown list.
- 3. Select the card reader from the table for triggering.
- 4. Set the linkage target, and switch the property from I to I to enable this function.
 Host Buzzer: The audible warning of controller will be triggered.
 Capture: The real-time capture will be triggered.
 Reader Buzzer: The audible warning of card reader will be triggered.
 Alarm Output: The alarm output will be triggered for notification.
- 5. Click Save button to save parameters.
- 6. Click Download Settings to download the updated parameters to the local memory of the device to take effect.

4.5.3 Client Linkage

Purpose:

You can assign other access controller linkage actions to the trigger by setting up a rule in client linkage.

In the Linkage Configuration interface, click Client Linkage tab to enter the following interface.

ient Linkage Settings	Client Linkage Settings	🕂 Add 🗶 Delete 🔚 Save
earch 🖇	Event Source: Event Linkage: Device Event Device Tamperin Controller List 172.10.18.29	Card Linkage: v
	Linkage Target Controller List 172.10.18.29 V Alarm Output Name Property	
	Door: Name Open Close	Remain Open Remain Closed

Click + Add button to add a new client linkage. You can select the event source as **Event Linkage** or **Card Linkage**.

Event Linkage

For the event linkage, the alarm event can be divided into four types: device event, alarm input, door event, and card reader event.

Steps:

- 1. Click to select the linkage type as **Event Linkage**, select the access controller as event source, and select the event type from the dropdown list.
 - For Device Event, select the detailed event type from the dropdown list.
 - For Alarm Input, select the type as alarm or alarm recovery and select the alarm input name from the table.
 - For Door Event, select the detailed event type and select the door from the table.
 - For Card Reader Event, select the detailed event type and select the card reader from the table.
- 2. Set the linkage target, select the access controller from the dropdown list as the linkage target, and switch the property from to **C** to enable this function.
 - Alarm Output: The alarm output will be triggered for notification.
 - Door: The door status of open, close, normally open, and normally close will be triggered.
 Note: The door status of open, close, normally open, and normally close cannot be triggered at the same time.
- 3. Click Save button to save parameters.

Card Linkage

Steps:

- 1. Click to select the linkage type as **Card Linkage**.
- 2. Select the card from the dropdown list and select the access controller as event source.

- 3. Select the card reader from the table for triggering.
- Set the linkage target, select the access controller from the dropdown list as the linkage target, and switch the property from to to enable this function.
 Alarm Output: The alarm output will be triggered for notification.
- 5. Click Save button to save parameters.

4.6 Access Permission Configuration



Click Access Control Permission icon on the control panel to enter the Access Control Permission interface.

	+ Add	Delete	Download	Export	Import		
	Serial No.	Person Name	Department	Access Control	Door Group	Template	Status
	1	Cindy	默认部门/Human.	172.10.18.25_Door	Test_Group	Default Enable Schedule Template	Downloaded
	2	Cindy	默认部门/Human.	172.10.18.25_Door	2 Test_Group	Default Enable Schedule Template	Downloaded
	3	Cindy	默认部门/Human.	172.10.18.25_Door	3 Test_Group	Default Enable Schedule Template	Downloaded
	4	Cindy	默认部门/Human.	172.10.18.25_Door	L	Default Enable Schedule Template	Downloaded
	5	Wendy	默认部门/Human.	172.10.18.29_Door	Test_Group	Default Enable Schedule Template	Downloaded
	6	Wendy	默认部门/Human.	172.10.18.25_Door	Test_Group	Default Enable Schedule Template	Downloaded
	7	Wendy	默认部门/Human.	172.10.18.25_Door	2 Test_Group	Default Enable Schedule Template	Downloaded
	8	Wendy	默认部门/Human.	172.10.18.25_Door	B Test_Group	Default Enable Schedule Template	Downloaded
	9	Wendy	默认部门/Human.	172.10.18.25_Door	l .	Default Enable Schedule Template	Downloaded
Total:9	9 Page:1/1						Page Go to

4.6.1 Adding Permission

Purpose:

You can allocate permission for people/department to enter/exist the control points (doors) in this section.

Steps:

1. Click Add icon on the upper-left side of the page to enter following interface.

		New Access Control Permission ×
Choose Type Permission Settings	1	By Person Note: Configure access control point for person.
	A	By Department Note: Configure access control point for department.
	1	By Access Control Point Note: Configure access control point to person and department.
	I	By Door Group Note: Configure person and department permission for door group.
		Previous Next Cancel

- 2. Select the permission type.
 - **By Person:** You can select people from the list to enter/exit the door.
 - **By Department:** You can select departments from the list to enter/exit the door. Once the permission is allocated, all the people in this department will have the permission to access the door.
 - By Access Control Point: You can select doors from the door list for people to enter/exit.
 - **By Door Group:** You can select groups from the door list for people to enter/exit. The permission will take effect on the door in this group.

Note: The Door Group Permission will be available after the door group is added. For details about the door group, refer to *Chapter 3.2 Door Group Management*.

3. Click Next to enter the Permission Settings interface.

	Ne	w Access Control F	Permission	×
① Choose Type	Template Default	Enable Schedule T	emplate 🗸 🕂 Add Template	
Permission Settings	Please choose person. Search Default Departm Human I Cind Cind	ent Resource Depart dy y	Please choose the access control point and the d Search Access Control Door Group Test_Group Test_Group Tot.739120_Door3 Tot.739120_Door3 Tot.739120_Door3 Tot.739120_Door2 Tot.739120_Door2 Tot.739120_Door1 Tot.739120_Door1 Tot.739120_Door1 Tot.739120_Door1 Tot.739120_Door1 Tot.739120_Door1 Tot.739120_Door4	oor group.
			Previous Finish	Cancel

4. Click on the dropdown menu to select a schedule template for the permission.

Note: The schedule template must be configured before any permission settings. You can click **Add Template** button to add the schedule template. Refer to *Chapter 4.3 Schedule Template* for

details.

5. Select people/department and corresponding doors/door groups from the appropriate lists.



- 6. Click Finish button to complete the permission adding.
- 7. (Optional) You can double click **Template** column of the added permission in the list to edit its permission schedule template.

You can select the added permission in the list and click **Delete** to delete it.

4.6.2 Downloading Permission

You can apply the added permission to the access control to take effect. *Steps:*

1. Click **Download** to enter the Download Permission interface as follows.



- 2. Select the Downloading Method.
 - Download All: Download all the permissions in the list to the selected access controller.
 - **Download Changes:** Download the changed permissions to the selected access controller.
- 3. Select an access controller and click **OK** button to start downloading the permission to the device.

	Downlo	oading Result		
Permission Downloading Progress	c	Downloa	aded (100%)	
				100%
Filter				
Device	Progress	Result	Remark	
172.10.18.25	100%	All Succeeded		
				Close

4.6.3 Importing/Exporting Permission

You can also export the added permissions information to the local PC and import the permissions in batch from the local PC.

Steps:

1. To import the permission in batch, click Import button to pop up the following dialog box.

Imp	port Access Control Permission	×
Select the file to import:		
	ОК	Cancel

Click led to select the package file containing the permission information. Click **OK** to start importing.

2. To export the permissions to the local PC, click Export button to pop up the following dialog box.



Click , input the permission file name as desired and select the saving path of the exported package file containing the permission information.

Click **OK** to start exporting.

Note: The exported permission file is not editable.

4.6.4 Searching Access Control Permission

You can search the added access control permission via the client. *Steps:*

1. Click Tool->Search Access Control Permission on the menu to enter the following interface.

			Search Access Co	ontrol Permission			×
Major Type: P	erson	Minor Type: Door	r Group 🗸 I	Keyword:		Search	Reset
Serial No.	Name	Department	Door Group	Access Control	Template	Status	1
Total:0 Page:	1/1					Page	Go

- 2. Set the major type as the main search condition from the dropdown list. You can set it as by person, department, door group, or access control point.
- 3. Set the minor type as the second search condition from the dropdown list. You can set it as by door group or access control point.
- 4. You can also input the keyword of the permission.
- Click Search to start searching the result.
 You can click Reset the set the search condition to the default value.

4.7 Advanced Functions

Purpose:

After configuring the person, card, template, status duration, alarm linkage, and access permission, the advanced functions of the access control client can be configured, such as access control type, authentication password and first card.



Click Advanced Function icon on the control panel to enter the following interface.

Access Control Type Card Reader Authenti	ication Multiple Authentication Open Door with	First Card Anti-passing Back Multi-door Inter	locking White List Password Authentication
Controller List 🛃 Download Settings	Card List		
Search	🕂 Add 🛛 🗶 Delete 🛛 🗹 Edit		Filter
- 🛃 172.10.18.29	Card No. Person Name	Effective Date Expiry Date	
🔯 Card for Disabled Person			
🔯 Card in Blacklist			
🔯 Patrol Card			
🔯 Duress Card			
🔯 Super Card			
🔯 Visitor Card			
	Total:0 Page:1/1	[4	Go to

4.7.1 Access Control Type

Purpose:

The added cards can be assigned with different card type for the corresponding usage. *Note:* Please set the card permission and download the permission setting to the access controller first. For details, refer to *Chapter 4.6 Access Permission Configuration*.

Steps:

1. Click Access Control Type tab and select a card type.



Card for Disabled Person: The door will remain open for the configured time period for the card holder.

Card in Blacklist: The card swiping action will be uploaded and the door cannot be opened.

Patrol Card: The card swiping action can used for checking the working status of the inspection staff. The access permission of the inspection staff is configurable.

Duress Card: The door can open by swiping the duress card when there is duress. At the same time, the client can report the duress event.

Super Card: The card is valid for all the doors of the controller during the configured schedule. **Visitor Card**: The card is assigned for visitors.

Dismiss Card: The card can be swiped to stop the buzzer of the card reader.

Notes:

- The available card types depend on the access controller type.
- If the card is not assigned as any of the above card types, it is assigned as normal card by default.
- 2. Click Add and select the available card.

	Add Card	
Select the card to add:		
Filter		
Card No.	Person Name	
12352	Wendy	
12371	Wendy	
12373	Wendy	
Total:3 Page:1/1	Page	Go to
	ОК	Cancel

- 3. Click **OK** to confirm assigning the card(s) to the selected card type.
- 4. For the Visitor Card, you can click the added card and click Times, card Effective Time and Expiry Time.

	Edit Visitor Card	×
Card No.:	12345	
Max. Swipe Times:	٥	
Effective Time:	2016-03-09 00:00:00	21
Expiry Time:	2036-12-31 23:59:59	2
	ОК	Cancel

Note: The Max. Swipe Times should be between 0 and 255.

- 5. Click Download Settings button to take effect of the new settings.
- 6. (Optional) You can click **Delete** to remove the card from the card type and the card can be available for being re-assigned.

4.7.2 Card Reader Authentication

You can set the passing rules for the card reader.

Steps:

- 1. Click Card Reader Authentication tab and select a card reader on the left.
- 2. Select a card reader authentication mode. The available authentication modes depend on the card reader type:
 - **Card and Password**: The door can open by both inputting the card password and swiping the card.

Note: Here the password refers to the password set when issuing the card. Refer to *Chapter 4.2.1 Empty Card.*

• **Card or Authentication Password**: The door can open by inputting the authentication password or swiping the card.

Note: Here the authentication password refers to the password set to open the door. Refer to *Chapter 4.7.8 Authentication Password*.

- **Fingerprint**: The door can open by only inputting the fingerprint.
- **Card or Fingerprint:** The door can open by inputting the fingerprint or swiping the card.
- Password and Fingerprint: The door can open by both inputting the card password and inputting the fingerprint.

Note: Here the password refers to the password set when issuing the card. Refer to *Chapter 4.2.1 Empty Card.*

- **Card and Fingerprint**: The door can open by both inputting the fingerprint and swiping the card.
- **Card, Password and Fingerprint**: The door can open by both inputting the fingerprint, inputting the card password, and swiping the card.

Note: Here the password refers to the password set when issuing the card. Refer to *Chapter 4.2.1 Empty Card.*

3. Click and drag your mouse on a day to draw a color bar on the schedule, which means in that period of time, the card reader authentication is valid.



4. Repeat the above step to set other time periods.

Or you can select a configured day and click **Copy to Week** button to copy the same settings to the whole week.

You can click **Delete** button to delete the selected time period or click **Clear** button to delete all the configured time periods.

5. (Optional) Click **Copy to** button to copy the settings to other card readers.



- 6. Click Save button to save parameters.
- 7. Click Download Settings button to take effect of the new settings.

4.7.3 Multiple Authentication

You can manage the cards by group and set the authentication for multiple cards for one access control point (door).

Steps:

- 1. Click **Multiple Authentication** tab and select an access control point (door) from the list on the left.
- 2. Click Add Authentication Group button to pop up the following interface:

		Multiple Aut	hentication			2
1) Card Group Management	Door:	172.10.18.25_Door1	~			
2) Add Authentication Group	Card Group:	😵 1	0			
		2	Ø	Cord Swiping Times:	2	
		88 3	0	Card Swiping Times.	3	
		85 4444	Ø	Effective Time:	2016-03-09 00:00:00	1
		😵 Card Group05	Ø	Expiry Time:	2016-03-09 23:59:59	2
		😵 Card Group06	0			
		Sard Group07	Ø			
		Sard Group08	0			
	Card Group M.	🕂 Add 🗙	Delete			
	Card No.	Person Nam	е			
	12352	Wendy				
	12371	Wendy				
				Deview		
				Previous	INEXL Cal	icei

- Click the card group from the list, and Add to select the card to add the card group.
 Note: Please set the card permission and download the permission setting to the access controller first. For details, refer to *Chapter 4.6 Access Permission Configuration*.
 You can click of the card group to edit the group name.
- Input the Card Swiping Times for the selected card group.
 Note: The Card Swiping Times should be larger than 0 and no more than the added card number in the group.
- Select the effective time and expiry time for the selected card group.
 Note: You can also click Card Group Management button on the Multiple Authentication tab page to set the card group.
- 6. Click **Next** to enter the Add Authentication Group interface.

		Multiple Au	thentication		
(1) Card Group Management	Template:	Default Enal	ole Schedule Temp 🗸		
2 Add Authentication Group	Certificate Type:	Local Auther	v		
	Offline Authentication:	Enable su	per password when offline.		
	Multiple Authentication G	roup:			
	1			1	4444
				2	Card Group05
			+ Add		
			🗙 Delete		
			🕢 Up		
			Down		
			Remark:Certification group need to swiping card according to the configuration sequence		
			Pri	evious	Done Cancel

- 7. Select the template of the authentication group from the dropdown list. For details about setting the template, refer to *Chapter 4.3 Schedule Template*.
- Select the certificate type of the authentication group from the dropdown list.
 Local Authentication: Authentication by the access controller.
 Local Authentication and Remotely Open Door: Authentication by the access controller and by the client.

Local Authentication and Super Password: Authentication by the access controller and by the super password.

For Local Authentication and Remotely Open Door type, you can check the checkbox to enable the super password authentication when the access controller is disconnected with the client.

9. In the list on the left, the card group name will be displayed. You can click the card group and click
Add to add the group to the authentication group.
You can click the added card group and click Delete to remove it from the authentication group.

You can also click **Up** or **Down** to set the card swiping order.

10. Click **Done** to save the settings.

11. Click Download Settings button to take effect of the new settings.

Notes:

• For each access control point (door), up to four authentication groups can be added.

- For the authentication group which certificate type is **Local Authentication**, up to 8 card groups can be added to the authentication group.
- For the authentication group which certificate type is **Local Authentication and Super Password** or **Local Authentication and Remotely Open Door**, up to 7 card groups can be added to the authentication group.

4.7.4 Open Door with First Card

Purpose:

The door remains open for the configured time duration after the first card swiping.

Controller List 🛃 Download Settings	Access Control Point First Card	Parameters		Save
Search 9	Access Control	Enable First Card Remain Open	Remain Open Duration (Minute)	
172.10.18.29	172.10.18.29_Door1		10	
	First Card List			
	+ Add X Delete		Filter	
	Card No. Person	Name Effective Date	Expiry Date	
	Total:0 Page:1/1			Page Go to

Steps:

- 1. Click **Open Door with First Card** tab and select an access controller from the list on the left.
- 2. Check the checkbox of Enable First Card Remain Open to enable this function.
- In the Remain Open Duration (min), input the time duration for remaining open the door.
 Note: The Remain Open Duration should be between 0 and 1440 minutes. By default, it is 10 minutes.
- 4. In the First Card list, Click **Add** button to pop up the following dialog box.

	Add Card	×
Select the card to add:		
Filter		
Card No.	Person Name	
12352	Wendy	
12371	Wendy	
4512124546	Cindy	
Total:3 Page:1/1	H I I Page	Go to
	ОК	Cancel

- Select the cards to add as first card for the door and click **OK** button.
 Note: Please set the card permission and download the permission setting to the access controller first. For details, refer to *Chapter 4.6 Access Permission Configuration*.
- 2) You can click **Delete** button to remove the card from the first card list.
- 5. Click **Save** and then click download Settings button to take effect of the new settings.

4.7.5 Anti-Passing Back

Purpose:

You can set to only pass the access control point according to the specified path.

Notes:

- Either the anti-passing back or multi-door interlocking function can be configured for an access controller at the same time.
- You should enable the anti-passing back function on the access controller first.

Setting the Path of Swiping Card (Card Reader Order)

Steps:

1. Click Anti-passing Back tab and select an access control point.

Controller List 👍 Download Settings	Property		🛃 Sa
Search			
10.7.39.120	Controller Name: 10.7.3	9.120	
 172.10.18.29 172.10.18.25 	First Card Read 10.7.39	9.120_Reader Out4	
	Card Reader	Card Reader Afterward	Enable Anti-passing Back
	10.7.39.120_Reader In1	der In3,10.7.39.120_Reader Out4,10.7.39.120_Rea	der In5
	10.7.39.120_Reader Out2		
	10.7.39.120_Reader In3		
	10.7.39.120_Reader Out4		
	10.7.39.120_Reader In5		
	10.7.39.120_Reader Out6		
	10.7.39.120_Reader In7		
	10.7.39.120_Reader Out8		

- 2. You can select the card reader as the beginning of the path.
- 3. In the list, click the text filed of Card Reader Afterward and select the linked card readers.

Example: If you select Reader In_01 as the beginning, and select Reader In_02, Reader Out_04 as the linked card readers. Then you can only get through the access control client by swiping the card in the order as Reader In_01, Reader In_02 and Reader Out_04.



Note: Up to four afterward card readers can be selected for one card reader.

- 4. Check the **Enable Anti-Passing Back** checkbox to enable the anti-passing back function of the card reader.
- 5. (Optional) You can enter the Select Card Reader dialog box again to modify its afterward card readers.
- 6. Click **Save** and then click *bownload* Settings button to take effect of the new settings.

4.7.6 Multi-door Interlocking

You can set the multi-door interlocking between multiple doors of the same access controller. To open one of the doors, other doors must keep closed. That means in the interlocking combined door group, up to one door can be opened at the same time.

Notes:

- The Multi-door Interlocking function is only supported by the access controller which has more than one access control points (doors).
- Either the anti-passing back or multi-door interlocking function can be configured for an access controller at the same time.

Steps:

1. Click Multi-door Interlocking tab and select an access control point from the list.

Controller List 🛃 Download Settings	Multi-door Interlocking List	
Search 9	+ Add X Delete	Filter
3 10.7.39.120	Serial No. Interlocking Type Interlocking Combination	
172.10.18.25		

2. Click Add to pop up the Add Access Control Point to Interlock interface.



3. Select the access control point (door) from the list.

Note: Up to four doors can be added in one multi-door interlocking combination.

- 4. Click **OK** to save the adding.
- (Optional) After adding the multi-door interlocking combination, you can select it from the list and click *Pelete* to delete the combination.
- 6. Click download Settings button to take effect of the new settings.

4.7.7 White List

You can add the mobile phone number to the access controller for access permissions. The mobile phone can control the door and the zones by sending SMS control instructions.

Steps:

1. Click the White List tab to enter the white list interface.

Controller List 🛃 Download Settings	White List Settings	🕂 Add 🗶 Delete 🕞 Save
Search	Telephone No.:	
172.10.18.25	Permission	
	Door:	
	Access Control Name Open Door Close Door Remain Open	Remain Closed
	Zone:	
	Alarm Input Name Arm Disarm	

- 2. Select the access controller from the list and click Add button.
- 3. Input the mobile number.

4. Select the access control permission. You can check the corresponding checkbox to enable the permission.

Door: The mobile can control the door (open, closed, normally open, or normally closed). **Zone:** The mobile can arm and disarm the zone.

5. Click **Save** button to save parameters.

Controller List 🛃 Download Settings	White List Settings	White List Settings + Add X Delete								
Search 2	Telephone No.: 1234567									
172.10.18.25	Permission	ermission								
	Door:									
	Access Control Name	Open Door	Close Door	Remain Open	Remain Closed					
	172.10.18.25_Door1	✓								
	172.10.18.25_Door2									
	172.10.18.25_Door3		✓							
	172.10.18.25_Door4			✓	✓					
	Zone:									
	Alarm Input Name	Arm	Disarm							
	Alarm Input_1	 Image: A set of the set of the								
	Alarm Input_2									
	Alarm Input_3									
	Alarm Input_4									

6. You can select the added white list and click **Delete** button to delete it.

7. Click download Settings button to take effect of the new settings.

Notes:

- Up to 8 white lists can be added for one access controller.
- The mobile can control the door and the zones by sending SMS control instructions. The SMS control instruction is composed of Command, Operation Range, and Operation Object.

Instruction Content	Digit	Description	Format
Command	3	010-Open, 011-Closed, 020-Normally open, 021-Normally Closed, 120-Disarm, 121-Arm	
Operation Range	1	1-all objects with permission, 2-single operation	Command#1#
Operation Object	3	Starts from 1 (corresponding to different doors or arming regions according to commands)	Command#2#Operation Object#

4.7.8 Authentication Password

Purpose:

You can open the door by inputting the authentication password on the card reader keypad after finishing the operation of setting authentication password.

Note: This authentication password function is only valid during the schedules when the card reader authentication mode for the access controller is set as **Card or Authentication Password**. For details, please refer to *Chapter 4.7.2 Card Reader Authentication*.

Steps:

Controller List 🛃 Download Settings	Card List			
Search 9	+ Add X Delete		Filter	
172.10.18.25	Card No. Person Name	Authentication Password	Effective Date	Expiry Date
	12371 Wendy	22222	2016-03-09	2036-12-31
	12373 Wendy	11111	2016-03-09	2036-12-31

- 1. Click Authentication Password tab and select an access controller from the list.
- 2. Click **Add** button to enter card adding interface.

	Add C	Card	×
Select the card to ad	d:		
Filter			
Card No.	Person Name	Authentication	Operation
12352	Wendy		2
12371	Wendy	22222	2
4512124546	Cindy		2
Total:3 Page:1/1		▶ ▶ Page	Go to
		ОК	Cancel

3. Select the card to add and click 🗹 button to pop up the password setting dialog box.

Set P	assword	×
Card No.:	12352	
Authentication Password:	[
	OK Cancel	

Input the password for authentication. The authentication password should contain 4 to 8 digits. Click **OK** to confirm the password.

- 4. Click **OK** button to finish adding the card.
- (Optional) The added card, having added the authentication password, will display in the card list. You can select the card in the card list, and click **Delete** button to delete the authentication password settings of the selected card.
- 6. (Optional) You can click **Add** button to enter the card adding interface again and click is button to modify the authentication password.

Note: Up to 500 cards with authentication password can be added to one access controller. The password should be unique and cannot be same with each other.

Chapter 5 Attendance Management

Purpose:

After adding the device and person, you can set the person shift, set the holiday, manage the person attendance and view the card swiping log.

5.1 Attendance Configuration



Click Attendance Configuration icon on the control panel to enter the Attendance Configuration interface.

5.1.1 Shift Group Management

Purpose:

On the shift group management interface, you can add, edit, and delete shift groups for attendance management.

Steps:

1. Click **Shift Group** tab to enter the following page.



2. Click + Add

Add button to pop up the adding shift group window.

		Add Shift Gro	up	×
The items with aster	risk are required			
*Shift Group Name:		*Sh	ift Group No.: 0002	
Remark:				
Person List			+ Add	X Delete
Serial No.	Name	Gender	Department	
			ОК	Cancel

3. Enter the shift group name, and add Add button on the person list area to pop up the person adding window.

Add Person	×
Search	٦
- 🔲 🔝 Default Department	
🖃 🔳 🔣 Human Resource Department	
🗹 🛃 Wendy	
Cindy	
ОК	Cancel

4. Check the checkbox to select the person and click **OK** button and return to the shift group settings interface.

To delete the added person, check the person from the person list, and click **Pelete** button.

5. Click **OK** button to complete the operation.

6. You can edit or delete the added shift groups by clicking Modify or Holete button. Notes:

- After deleting the shift group, the shift schedule of the shift group will be deleted as well. For details about shift schedule, refer to *Chapter 5.1.4 Shift Schedule Management*.
- If the person has been added to one shift group, he/she cannot be added to other shift groups.

5.1.2 Shift Management

Click Shift tab to	enter th	e shift	management	interface.
---------------------------	----------	---------	------------	------------

Shift Management	+ Add Modify X Delete	Filter
 Normal Shift 	Serial No. Rule Name Remark	
Attendance Rule		
Attendance Shift		
Man-Hour Shift		
	Total:0 Page:1/1	Go to

There are two kinds of shifts in this interface: Normal Shift, and Man-Hour Shift.

Normal Shift

♦ Setting Attendance Rule

Steps:

- 1. Click Attendance Rule to set the rule for the attendance management.
- 2. Click Add button to pop up the following dialog box.

Add Normal 3	Shift Attendance Rule	
The items with asterisk are required		
*Rule Name:		
Remark:		
Detailed Parameters		
Allowable Early Duration to Go to Work:	0	min
Allowable Late Duration to Go to Work:	15	min
Late Arrival Threshold Duration:	120	min
Break Duration:	60	min
Allowable Late Duration to Get Off Work:	0	min
Allowable Early Duration to Get Off Work:	15	min
Early Leave Threshold Duration:	120	min
	ОК Са	ncel

- 3. Set a rule name.
- 4. Set detailed parameters for the attendance rule according to actual needs.
- 5. Click **OK** to save the rule.
- (Optional) You can edit or delete the rule by clicking Modify or Delete button.
 Notes:
 - After deleting the rule, the normal attendance shift which has enabled the rule will be deleted as well.
 - If the shift which has enabled the rule has already set the shift schedule, the shift will not be deleted.
- ♦ Setting Attendance Shift

Steps:

- 1. Click Attendance Shift to set the normal attendance shift.
- 2. Click **Add** button to pop up the attendance shift setting window.

	_		Add Normal	Attendance St	nift		×
The	items with asterisk	are required					
*Shi	ift Name: Remark:			*Shift No.:	0004		
Work	king Time Period						💼 Clear
	Working Time	On-Work Time		Off-Work Time		Attendance Rule	
	Duration1	Day ~ 0	00:00:00	Day 🗸	00:00:00 ‡		~
	Duration2	Day 🗸	00:00:00	Day ~	00:00:00		~
	Duration3	Day 🗸	00:00:00	Day 👻	00:00:00 +		~
	Duration4	Day 🗸	00:00:00	Day ~	00:00:00		~
						ОК	Cancel

- 3. Set a shift name.
- 4. Set on-work duration for the shift, and select the attendance rule from the dropdown list.
- 5. Click **OK** button to complete the operation.
- 6. (Optional) You can edit or delete the shift by clicking Modify or Pelete button.
 Note: After deleting the shift, its shift schedule will be deleted as well. For details about shift schedule, refer to Chapter 5.1.4 Shift Schedule Management.

Man-Hour Shift

Steps:

- 1. Click Man-Hour Shift to set the man-hour shift details.
- 2. Click Add button to pop up the man-hour shift setting window.

Add Man-Hour Attendance Shift ×						
The items with asterisk	are required					
*Shift Name: *Daily Work Duration: Remark:	00:00:00	÷	Latest On-W	*Shift No.: /ork Time:	0004	
Exclusions From Man-H	lour Duration					💼 Clear
Duration		Start Time		End Time		
Duration1		00:00:00	* *	00:00:00		* *
Duration2		00:00:00	* *	00:00:00		* •
Duration3		00:00:00	×	00:00:00		× •
Duration4		00:00:00	×	00:00:00		×
					ОК	Cancel

- 3. Set a shift name, and daily work duration.
- 4. (Optional) Check the checkbox of latest on-work time, and set the latest on-work time.
- 5. (Optional) Set the durations excluded from man-hour duration.
- 6. Click **OK** button to complete the operation.
- 7. (Optional) You can edit or delete the shift by clicking Modify or Kelete button.

Note: After deleting the shift, its shift schedule will be deleted as well. For details about shift schedule, refer to Chapter 5.1.4 Shift Schedule Management.

5.1.3 Holiday Management

Steps:

1. Click Holiday tab to enter the holiday management interface.



2. Click + Add button to pop up the holiday setting window.

		Add Holiday		×
The items with asteri	sk are required			
*Holiday Name:				
Remark:				
Date List			+ Add	X Delete
Serial No.	Date	Week		
			ОК	Cancel

3. Click **Add** button to pop-up holiday adding window.

Select Date	×
The items with asterisk are required	
*Start Date: 3/21/2016 🗮 *End Da	te: 3/21/2016 📆
*Select by Week	All
🗌 Monday 📄 Tuesday 📄 Wednesday 📄 Thursday 📄 Friday	🗆 Saturday 📄 Sunday
	OK Cancel

- 4. Set the start date and end date, select the date of week, and click **OK** button.
- 5. Click **OK** to save the settings.

5.1.4 Shift Schedule Management

Purpose:

After setting the shift group and the corresponding shift and shift rule, you can set the shift schedule for the shifts.

Steps:

1. Click Shift Schedule tab to enter the shift schedule management interface.

Shift Schedule Management	+ Add B Import X Delete					
Search 9	Serial No. On-Work Time Shift Name Shift No.					
shift group-test						

- 2. Select the shift group from the list on the left.
- 3. Click Add button to pop up the shift schedule settings window.

		_	Add Shift Sc	hedule	_	_	
The items with ast	erisk are required						
Shift Group Name:	shift group-test			Shift Name:	normal shift		~
*Effective Date:	3/21/2016		1	*Expiry Date:	3/21/2016		1
Add Holiday							
Serial No.	Holiday Name	Holiday Days	Remark				
1	holiday-test	5					

- Select the shift name from the drop-down list and set the start data and end data. (Optional) You can check the checkbox of holiday to add the holiday shift. Click **OK** button to complete the operation.
- 5. Click **OK** to save the settings.
- 6. You can also click [Import] to import the shift schedule from the local PC in batch.

	Import Data	×
Import File:		
	Download Shift Schedule Template	
	OK Cancel	

Click Download Shift Schedule Template to download the template and you can input the Shift

Group No., Date, and Shift No. in the template. Click 📃 to select the file for importing Click **OK** to start importing.

5.1.5 Attendance Check Point Management

Steps:

1. Click Attendance Check Point tab to enter the attendance check point management interface.

+ Add Modify X Delete						Filter		
	Serial No.	Check Point Name	Check Point Type	Effective Date	Expiry Date	Door Position	Reader Name	Description
	1	10.7.39.120_10.7.39.120	On/Off-Work	2016-03-10	2016-03-10		10.7.39.120_Reader	
	2	10.7.39.120_10.7.39.120	On/Off-Work	2016-03-10	2016-03-10		10.7.39.120_Reader I	
	3	10.7.39.120_10.7.39.120	On/Off-Work	2016-03-10	2016-03-10		10.7.39.120_Reader I	
	4	10.7.39.120_10.7.39.120	On/Off-Work	2016-03-10	2016-03-10		10.7.39.120_Reader	
	5	172.10.18.25_172.10.18	On/Off-Work	2016-03-10	2016-03-10		172.10.18.25_Reader	
	6	172.10.18.25_172.10.18	On/Off-Work	2016-03-10	2016-03-10		172.10.18.25_Reader	

2. Click Add to pop up the adding attendance check point interface as follows.



Check the select the card reader of the access control point and set the start date and end date. Select the check point type.

Click **OK** to save the adding.

The added check points will be displayed in the attendance check point list.

- You can check the checkbox of a check point, and click Modify button to pop up the 3. attendance check point editing window. You can edit the attendance check point name, start date, end date, and check point type, controller name, door position, and card reader name.
 - Click **OK** button to complete the operation.
- 4. You can check the checkbox of a check point and click Related button to delete the added

check point.

5.1.6 Adjustment Management

Click Adjustment tab to enter the adjustment management interface. In this module, Reason Management and List Management can be realized.

Reason Management

Leave ∻

You can add, edit, and delete reasons for leave on the leave interface.

Steps:

1. Click Leave tab to enter the leave interface.

	Add	1 Modify X Delete	Filter
0	Serial No.	Adjustment Reason	
	1	Sick Leave	
	2	Personal Leave	
	3	Paternity Leave	
	4	Parental Leave	
	5	Maternity Leave	
	6	Family Reunion Leave	
	7	Bereavement Leave	
	8	Annual Leave	

2. Click Add button to pop up the adjustment reason adding dialog box.

Ac	ljustment Reason				
The items with asterisk are required					
Adjustment Type:	Leave				
*Adjustment Reason:					
		i,			
	OK Cancel	1			

3. Enter the adjustment reason, and click **OK** button to save the adding.

Notes:

- The default adjustment reasons include leave for personal affairs, sick leave, marriage leave, ۰ funeral leave, home leave, annual leave, maternity leave, and paternity leave.
- You can check the checkbox of a reason and click Modify button to edit the reason, and click . * Delete button to delete the reason.

∻ Leave in Lieu

Steps:

1. Click Leave in Lieu tab to enter the leave-in-lieu interface.

Add	Modify X Delete	Filter
Serial No.	Adjustment Reason	
1	Overtime Exchange Holiday	
2	Business Trip Exchange Holiday	

2. Click + Add button to pop up the adjustment reason adding dialog box.
| A | djustment Reason × |
|------------------------|--------------------|
| The items with asteris | k are required |
| Adjustment Type: | Leave in Lieu |
| *Adjustment Reason: | |
| | |
| | OK Cancel |

3. Enter the adjustment reason, and click **OK** button.

Notes:

- The default adjustment reasons for leave in lieu include overtime, and business trip.
- You can check the checkbox of a reason and click Modify button to edit the reason, and click
 X Delete button to delete the reason.

♦ Overtime

Steps:

1. Click **Overtime** tab to enter the overtime interface.

+ Add	Image: Modify X Delete Filter
Serial No.	Adjustment Reason
1	Workday Overtime
2	Work Demand
3	Off Day Overtime
4	Holiday Overtime

- 2. Click Add button to pop up the adjustment reason adding dialog box.
- 3. Enter the adjustment reason, and click **OK** button.

Notes:

- The default adjustment reasons for overtime include work requirement, working day overtime, rest day overtime, and holiday overtime.
- You can check the checkbox of a reason and click Modify button to edit the reason, and click
 Delete button to delete the reason.

♦ Card Replacement

Steps:

1. Click **Card Replacement** tab to enter the following interface.

Add	Modify X Delete Filter
Serial No.	Adjustment Reason
1	Shift Rearrangement
2	Forget to Swipe Card
3	Device Fault
4	Card Loss
5	Business Trip

- 2. Click Add button to pop up the adjustment reason adding dialog box.
- 3. Enter the adjustment reason, and click **OK** button.

Notes:

- The default adjustment reasons for card replacing include forget to swipe card, attendance card lost, device fault, shift adjustment, and business trip.
- You can check the checkbox of a reason and click ^{I Modify} button to edit the reason, and click

X Delete button to delete the reason.

List Management

♦ Enabled List

Steps:

1. Click **Enabled List** tab to enter the enabled list interface.

	🕇 Add 🛛 🍵	Disable 🗙	Delete					
	Serial No.	Form No.	Person Name	Department	Start Time	End Time	Adjustment Type	Adjustmen
•	1	20160311162	Cindy	Dafault /Human	2016-03-11 00:00:00	2016-03-11 23:59:59	Leave	Personal Le
	2	20160311162	Wendy	Default /Human	2016-03-11 00:00:00	2016-03-11 23:59:59	Leave	Personal Le
	3	20160311162	Cindy	Default /Human	2016-03-11 00:00:00	2016-03-11 23:59:59	Leave	Personal Le
	4	20160311162	Wendy	Default /Human	2016-03-11 00:00:00	2016-03-11 23:59:59	Leave	Personal Le

2. Click **Add** button to add an attendance management form.

Add Attendance Management form		
Adjustment Type: Leave Leave in Lieu Overtime Card Replacement Adjustment Reason: Personal Leave		
Please choose person.	+ Add	X Delete
Serial No. Name Gender Department		
Duration: 2016-03-21 00:00:00 🛅 —— 2016-03-21 23:59:59 🛅		
	ок	Cancel

- 3. Select the adjustment type: leave, leave in lieu, overtime, and card replacement. Leave, Leave in Lieu, and Overtime
 - 1) Select the adjustment reason from the drop-down list.
 - 2) Click Add button to pop up the person adding window.

	Add P	erson				×
Select Adding Type: 🔘 By Departme	ent 🖲 Bj	Shift G	Group			
Search	9		All			
shift group-test			Wendy			
			Cindy			
				ок	Cancel	

- 3) Select the adding type as by department or by shift group. Select the person and click **OK** button.
- 4) Set the time duration.

Card Replacement

- 1) Select the adjustment reason from the drop-down list.
- 2) Click Add button to pop up the person adding window.

Add Person ×									
Select Adding Type: 🔘 By Department 🖲 By Shift Group									
Search P		All							
shift group-test		Wendy							
		Cindy							
			ок	Cancel					

- 3) Select the adding type as by department or by shift group. Select the person and click **OK** button.
- 4) Set the date, attendance shift type, and card replacing time.
- 4. Click **OK** button to complete the operation

♦ Disabled List

Steps:

1. In the Enabled List interface, check the checkbox of a piece of enabled list and click Disable

button to disable the list.

2. Click Disabled List tab and the disabled list will be listed on the disabled interface.

×	Delete							
	Serial No.	Form No.	Person Name	Department	Start Time	End Time	Adjustment Type	Adjustmen
•	1	20160310132	Wendy	默认部门/Human	2016-03-10 00:00:00	2016-03-10 23:59:59	Leave	Personal Le
	2	20160310132	Cindy	默认部门/Human	2016-03-10 00:00:00	2016-03-10 23:59:59	Leave	Personal Le

3. You can check the checkbox and click **Pelete** to delete the disabled list.

5.1.7 Card Swiping Log Query

Click Swiping Log tab to enter the card swiping log searching and viewing interface.

Query Type:	By Department	~	Department:	Human Resource Dep	oartment ~	Name:		Search
Query Scope:	All	~	Start Time:	2016-03-10 00:00:00	2	End Time: 2016-	03-10 23:59:59	📆 Reset
Card Swiping Lo	og Query							Export
Serial No	p. Person Name	Card No.	Swiping Time	Department	Card Reader	Reader Name	Door Name	Controller Name

You can search the card swiping log by two query types: **By Shift Group**, and **By Department**. Input other search conditions and click **Search** to start query the card swiping log.

5.1.8 Parameters Configuration

Steps:

1. Click Parameters Configuration tab to enter the parameters configuration interface.



- 2. Select the attendance effecting type, data saving time, data expiring prompt.
- 3. Set the attendance checking log clearing time.
- 4. Click Save to save the parameters.

5.1.9 Data Management

Steps:

1. Click Data Management tab to enter the data management interface.

Calculation Period:	2016-03-21 00:00:00	1	2016-03-21 00:00:00	2	Calculate
Export/Import Period:	2016-03-21 00:00:00	1	2016-03-21 00:00:00	*	
Export Data:					
Import Data:					

- 2. Select the date and time period for calculation and click **Calculate** to start calculating the attendance data.
- 3. After calculation, you can also export and import the attendance data.

5.2 Attendance Statistic



Click Attendance Statistics icon on the control panel to enter the Attendance Statistics interface.

On the Attendance Statistics interface, you can search the attendance statistic, attendance result statistics, and attendance rate statistics.

You can input the search condition including shift type, department, start date, and end date, and click

Search button to search the attendance data.

You can click Reset to reset the search condition to the default value.

After searching, you can click **Export** to export the searching report to the local PC.

Statistics Type							
Attendance Report	Shift Type:	Normal Shift	~	Department:	Default Department	~	Search
Attendance Result Statistics	Start Date:	3/21/2016	**	End Date:	3/21/2016	<u></u>	Reset
Attendance Rate Statistics							
							Export
			A	ttendance Re	port		
	Attendance Period:						
	Person Name	Department	Attendance Date	Shift Name	Duration	On-Wo	rk Attenda On-Work Sta
	+ (Þ
	Total:0 Page:1/1					P	age: Go to

Chapter 6 Status and Event

Purpose:

In this section, you are able to anti-control the status of the door and to check the event report of the access control point.

6.1 Status Monitor

Purpose:

You can anti-control the door status via the client.



Click Status Monitor icon on the control panel to enter the interface.

Access Control Group	Status Information Status Duration 📓 Open Door 📲 Close Door Remain Open Remain Closed 🐼 Capture	
Search 2	172.10.18.29 10.7.39.120_D 10.7.39.120_D 10.7.39.120_D 10.7.39.120_D 172.10.18.25 172.10.18.25 172.10.18.25 172.10.18.25	
	Serial No. Event Time Door Group Door Operation Operation Result 3 2016-03-10 15:06:32 Test_Group 172:10.18.25_Do Close Door Operation completed 2 2016-03-10 15:05:31 Test_Group 172:10.18.29_Do Capture Operation failed Capture 1 2016-03-10 15:04:58 Test_Group 172:10.18.29_Do Open Door Operation completed	Capture

6.1.1 Anti-control the Access Control Point (Door)

Purpose:

You can control the status for a single access control point (a door).

- 1. Select an access control group on the left. For managing the access control group, refer to *Chapter 3.2.1 Access Control Group Management*.
- 2. The access control points of the selected access control group will be displayed on the right.



- 3. Click the following button listed on the **Status Information** panel to select a door status for the door.
 - Open Door : Click to open the door once.
 - Close Door : Click to close the door once.
 - Remain Open: Click to keep the door open.
 - Remain Closed: Click to keep the door closed.
 - Capture : Click to capture the picture.
- 4. You can view the anti-control operation result in the Operation Log panel.

Notes:

- If you select the status as Remain Open/Remain Closed, the door will keep open/closed until a new anti-control command being made.
- The function of picture capturing cannot be realized until the storage server is installed.

6.2 Real-Time Access Event Alarm

Click the icon $\[Box]$ in Alarms and Events Toolbar to show the Alarms and Events panel. Or click $\[Dox]$ to display the Alarm Event interface.



You can view real-time access event (such as swiping to open the door, unrecognized card number, duration group error, etc.) information in Alarm Event interface.

6.3 Event Management

Purpose:

You can search historical access event according to the search conditions (such as event type, name of the person, card No. or start/end time).

Click Event Management icon on the control panel to enter the interface.

Event Type: All v Start Time: 2016-03-10 00:00:00 Image: Card Holder Name: v End Time: 2016-03-10 23:59:59 Image: Card No.: v Search	Card Holder Information
Search Result	t
Serial Event Type Card Holder Card No. Event Time Event Source Directi Capture	Person No.:
Tota:0 Page:1/1 Page Go	p to

- 1. Enter the search condition (event type/card holder name/card No./start&end time).
- 2. Click Search to get the search results.
- 3. View the event information in the event list.
- 4. Click an event to view the information of the card holder on the **Card Holder Information** panel on the left side of the page.
- 5. You can click **Export** button to export the search results to the local PC.

Chapter 7 System Maintenance

7.1 Log Management

Purpose:

The log files of the Access Control Client and the devices that connected to the Access Control Client can be searched for checking.



Click Log Search icon on the control panel to open the Log Search page.

Search Condition	Search Res	sult			Export
	Serial No.	Operation Type	Time	Content	*
Log Type:	5	Data Import/Export	2016-03-21 11:10:02	Export Person	
Configuration Log Control Log	6	Data Import/Export	2016-03-21 10:25:19	Export Person and Card Information.	
	7	Data Import/Export	2016-03-21 10:20:14	Export Person and Card Information.	
Operation Type:	8	Login	2016-03-21 09:39:56	User Login	
	9	Login	2016-03-20 18:06:20	Logout	
	10	Data Import/Export	2016-03-20 18:02:23	Export Person and Card Information.	
Start Time:	11	Login	2016-03-20 15:06:52	User Login	
Statt Hille.	12	Login	2016-03-20 15:04:43	Logout	
2016-03-19 00:00:00	13	Man-Hour Shift	2016-03-20 12:48:21	Add Man-Hour Attendance Shift:man	
	14	Normal Shift	2016-03-20 12:15:52	Add Normal Attendance Shift:00111	
End Time:	15	Attendance Rule	2016-03-20 12:15:28	Add Normal Shift Attendance Rule:1212	
2016-03-21 23:59:59	16	Password Authentication	2016-03-20 11:51:31	Download Password Authentication	
	17	Password Authentication	2016-03-20 11:51:27	Add Password Authentication:12373	
	18	Card Reader Autentication	2016-03-20 11:51:11	Save Card Reader Permission	
Q. Search	19	Card Reader Autentication	2016-03-20 11:51:02	Card reader authentication downloading operation	
	20	Card Reader Autentication	2016-03-20 11:50:55	Copied the card reader authentication	
	21	Login	2016-03-20 11:29:21	User Login	
	22	Login	2016-03-20 11:28:19	Logout	
	23	Login	2016-03-20 11:24:50	User Login	Ų
	Total:23 P	age:1/1		Page	Go to

7.1.1 Searching Configuration Logs

Purpose:

The operation logs via the Access Control Client can be searched by time.

- 1. Open the Log Search page.
- 2. Select the radio button of Configuration Logs.
- 3. Select the Operation Type of log files. For cofiguration log, the operation type includes department management, card managemene, access control permission configuration, ect..
- 4. Click 🛄 to specify the start time and end time.
- Click Search. The matched log files will display on the right.
 You can check the operation time, log type and other information of the logs.
- 6. You can click **Export** to export the search result to the local PC.

Note: Please narrow the search condition if there are too many log files.

7.1.2 Searching Control Logs

Purpose:

The logs of controlling access control point via the client can be searched by time.

Steps:

- 1. Open the Log Search page.
- 2. Select the radio button of Control Logs.
- 3. Select the Operation Type of log files. For control log, the operation type includes opening door, closing door, remaining open, remaining closed, and capture.
- 4. Click to specify the start time and end time.
- Click Search. The matched log files will display on the right.
 You can check the operation time, log type and other information of the logs.
- 6. You can click **Export** to export the search result to the local PC.

Note: Please narrow the search condition if there are too many log files.

7.2 Account Management

Purpose:

Multiple user accounts can be added to the client software, and you are allowed to assign different permissions for different users if needed.



Click Account Management icon on the control panel to open the Account Management page.

User List			
+ Add	Modify	X Delete	
Index	User Name	Туре	Remark
1	admin	Super User	Super user. Cannot be deleted.

Note: The user account you registered to log in to the software is set as the super user.

Adding the User

- 1. Open the Account Management page.
- 2. Click Add to open the Add User dialog box.
- 3. Input the user name, password and confirm password as desired. The software will judge password strength automatically, and we highly recommend you to use a strong password to ensure your data security.
- 4. Check the checkboxes to assign the permissions for the created user.
- 5. Click **OK** to save the settings.

Add User	×
User Name:	
Password:	
Confirm Pa Remark:	
✓ Permissions	_
Device Management	
Card Management	
Person Management	U
Access Control Permission	
Advanced Function	
Linkage Configuration	
Attendance Configuration	-
ок	Cancel



- ♦ A user name cannot contain any of the following characters: / \ : * ? " < > |. And the length of the password cannot be less than 8 characters.
- For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

Managing the User

Purpose:

After created successfully, the user account is added to the user list on the Account Management page. You can edit or delete the information of the user accounts.

To edit the information of the user, select the user from the list, and click Modify. To delete the information of the user, select the user from the list, and click Delete. Note: The super user cannot be deleted and its permission cannot be modified.

7.3 System Configuration

Purpose:

The general parameters, card reader, fingerprint machine, and storage server can be configured.

7.3.1 General Settings

Steps:

1. Click Tool->System Configuration to open the System Configuration page.



- Check the checkbox to enable Automatic Time Synchronization.
 The Automatic Time Synchronization can operate auto time adjustment to all access control devices added to the Access Control Client according to specified period and time.
 Select the matched day and input the time to operate the time adjustment.
- 3. You can check the checkbox to enable auto-login.
- 4. You can click the checkbox to enable the message prompt when the card reader initialization is error.
- 5. Click **Save** button to save the settings.

Note: You can click Restore Default Value button to restore the defaults of the general settings.

7.3.2 Card Reader Configuration

Purpose:

The Card Reader should connect with the PC running the client to read the card No.. You should configure the card reader before setting the card.

Steps:

1. Click Tool->Card Reader on the menu to pop up the card reader configuration dialog box.

	Card Reader	
Туре:	DS-K1F100-D8	~
Connection Method:	USB	
Overtime:	500	ms
Buzzing:	🖲 Yes 💿 No	
Card No. Type:	Normal	~
	Restore Default Value	Save

- 2. Set the parameters about the connected card reader.
- 3. Click **Save** button to save the settings.

You can click **Restore Default Value** button to restore the defaults.

7.3.3 Fingerprint Machine Configuration

The fingerprint machine should connect with the PC running the client for collecting the fingerprint. *Steps:*

1. Click **Tool->Fingerprint Machine** on the menu to open the Fingerprint Machine Configuration page.

	Fingerprint Machine		×
Device Type:	Optical Fingerprint Scanner	~	
Serial Port No.:	Com1	~	
Baud Rate:	19200	~	
Overtime:	20000		ms
	Restore Default Value	C	Save

- 2. Select the device type, serial port number, baud rate, and overtime parameters of the fingerprint machine.
- 3. Click **save** button to save the settings.

You can click Restore Default Value button to restore the default settings.

Notes:

- It is supported using device type as Optical Fingerprint Scanner and Capacitive Fingerprint Scanner.
- The serial port number should correspond to the serial port number of PC.
- The baud rate should be set according to the external fingerprint card reader. The default value is 19200.
- Overtime refers to the valid fingerprint collecting time. If the user does not input a fingerprint or inputs a fingerprint unsuccessfully, the device will indicate that the fingerprint collecting is over.

7.3.4 Storage Server Configuration

You should configure the storage server before capturing the pictures for the storage of captured pictures.

Steps:

1. Click **Tool->Storage Server** on the menu to enter the storage server configuration interface.

	Storage Server ×
IP Address:	127.0.0.1
Port:	8000
User Name:	admin
Password:	•••••
	Configure
	OK Cancel

- 2. Input the storage server parameters including IP address, port No., user name, and password.
- 3. Click **Configure** button to enter the Remote Configuration interface as follows.

System Displaying the Device Information Image: System Maintenance Device Type:		Remote Configuration	×
Bevice Information Central Strine System Maintenance Log User Storage Storage Storage Device Serial No.: Device Serial	🖃 🚳 System	Displaying the Device Information	
Image: Construction of the second of the	🔅 Device Information	Basic Information	
	Ime Ime Image: System Maintenance Image: Log Image: User Image: Comparison of the system of the system Image: Comparison of the system	Device Type: PCNVR_SERVER Channel Number: 0 IP Channel Number: 0 HDD Number: 4 Alarm Input Number: 0 Device Serial No.: DS-NVR-V120B20151029-FCAA1426153F Version Information Firmware Version: V1.2.1 build 151029 Encoding Version: V0 Hardware Version: 0x0	

- 4. The HDDs of the storage server need to be formatted for the video file and picture storage.
 - 1) Click **Storage->General**, to enter the HDD Formatting interface.
 - Select the HDD from the list and click Format. You can check the formatting process from the process bar and the status of the formatted HDD changes from Unformatted to Normal Status.

Note: Formatting the HDDs is to pre-allocate the disk space for storage and the original data of the formatted HDDs will not be deleted.

HDD	No. Capacity(G	GB) Free Space(GB)) Status	Туре	HDD Group N	o. Property	
D	180.00	153.45	Unformatted	Local	Group00	Read/Write	
E	185.75	185.65	Unformatted	Local	Group00	Read/Write	
Р	50.00	36308.20	Unformatted	Local	Group00	Read/Write	
z	3071.87	430.12	Unformatted	Local	Group00	Read/Write	
For	mat	Update					

5. After formatting of the HDD, you can set the picture storage quota in the Remote Configuration interface.

Storage Mode:	Quota 🗸	
Total Capacity:	3487.62	GB
Quota Ratio For Record:	50 ‡	%
Quota Ratio For Picture:	50 ‡	%
Quota Ratio For Addtiona	0	%

Click **Save** to save the storage server remote configuration settings.

6. After formatting the HDD and setting the quota, click **OK** to save the settings.