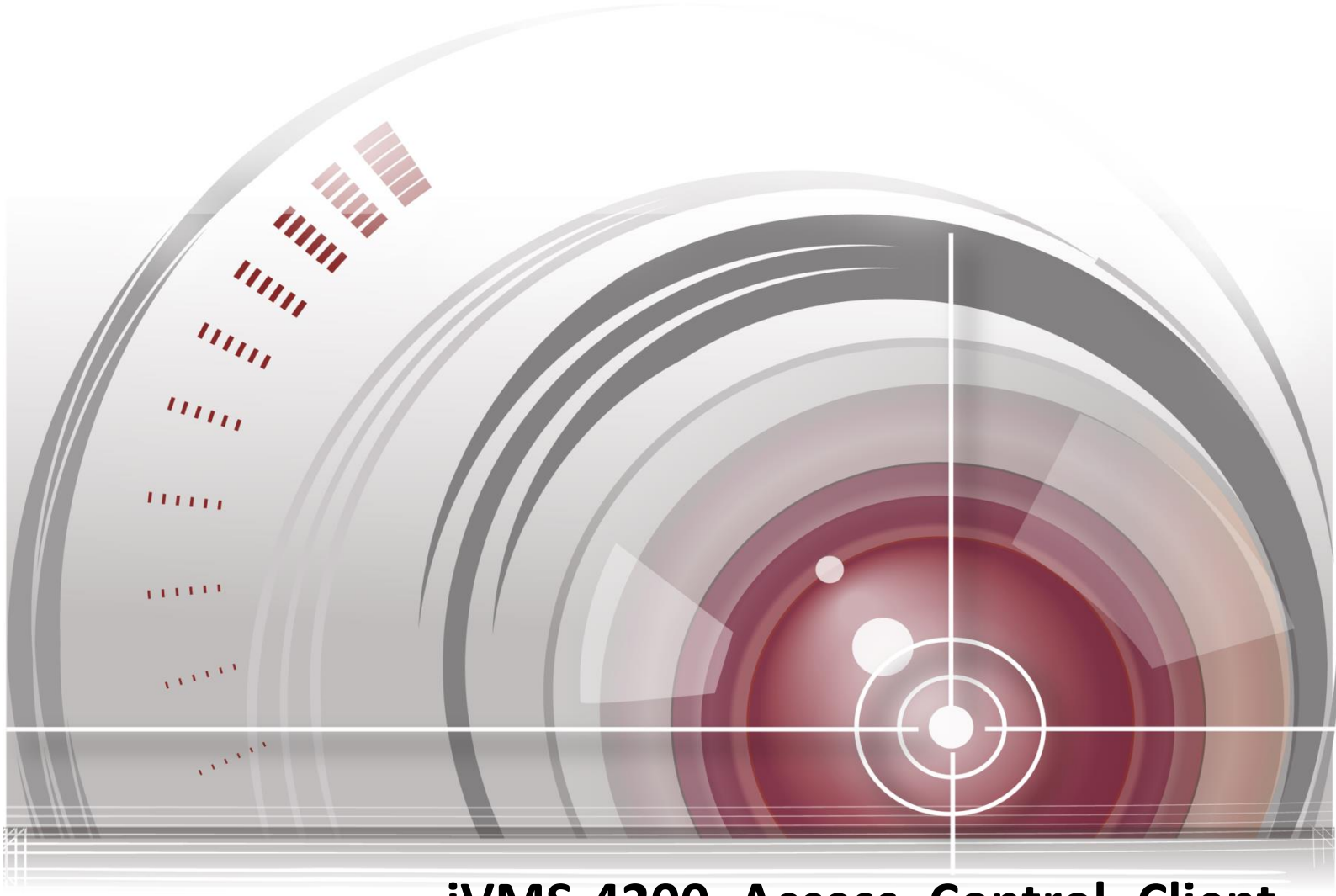


iVMS-4200 Access Control Client

User Manual

UD00895N

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

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.

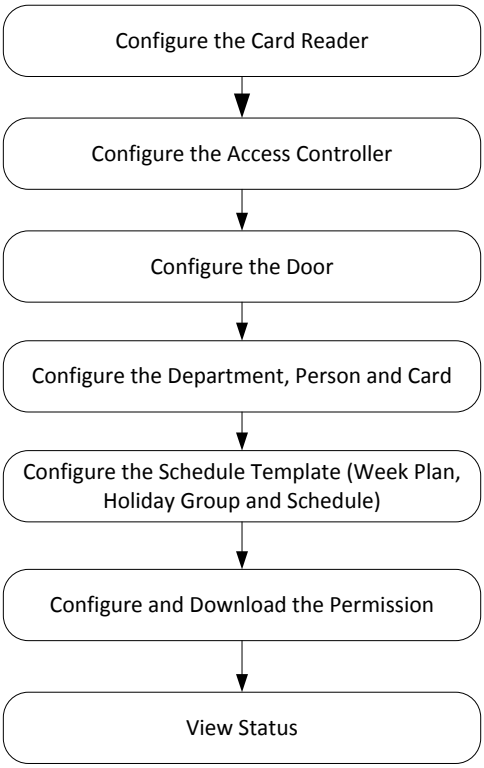
1.2 Running Environment

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.


Configure the Card Reader
Configure the Access Controller
Configure the Door
Configure the Department, Person and Card
Configure the Schedule Template (Week Plan, Holiday Group and Schedule)
Configure and Download the Permission
View Status

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 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.

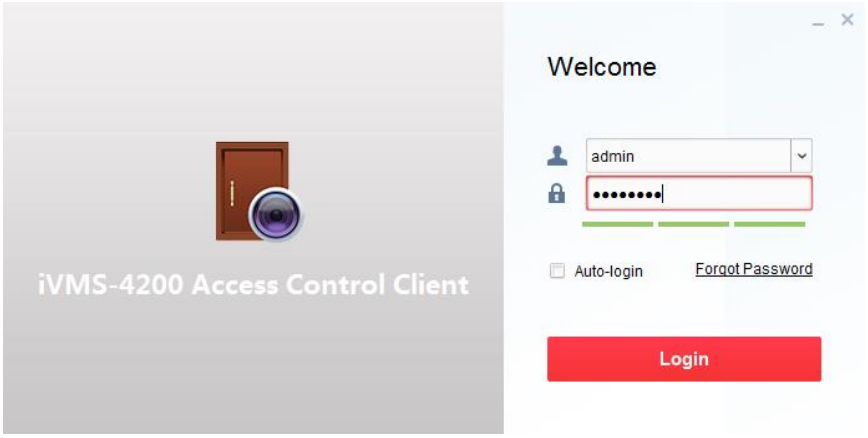
- *A user name cannot contain any of the following characters: / \ : * ? " < > |. And the length of the password cannot be less than 8 characters.*
- *For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case 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.



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

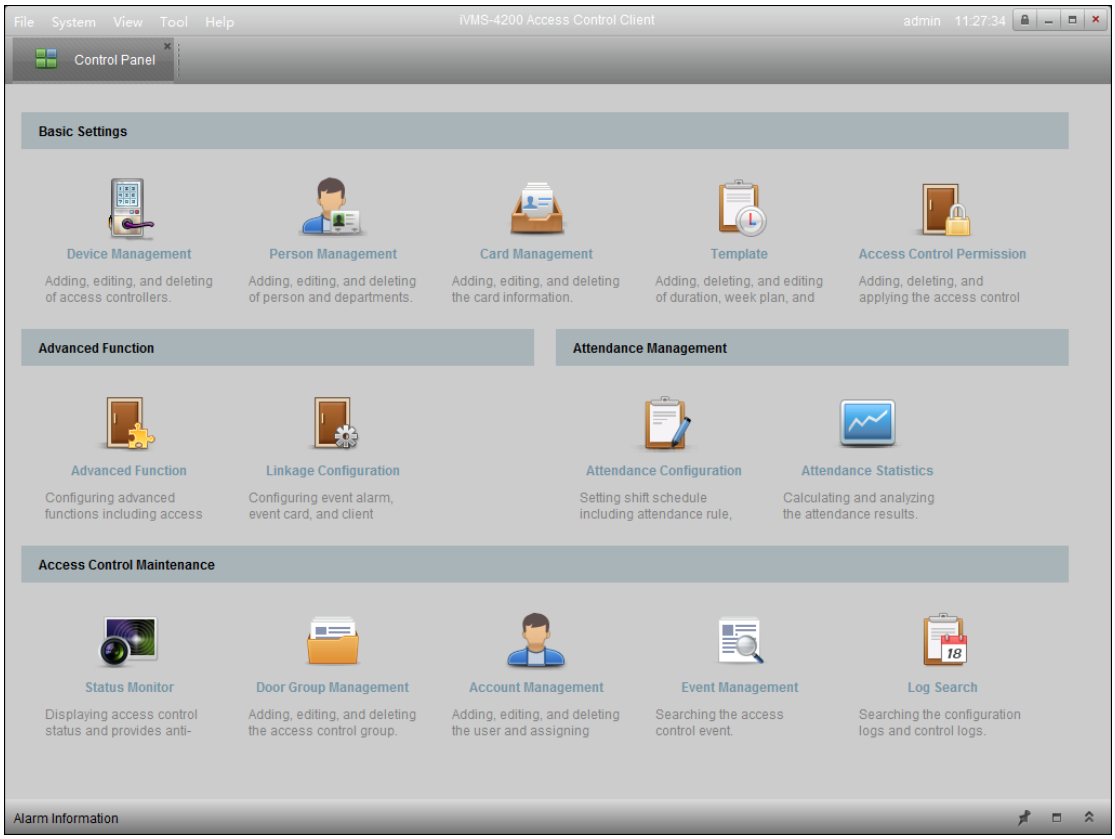
to reset your password.

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:



Menu Bar:

File	**Exit**	Exit the iVMS-4200 Access Control Client.
System	**Lock**	Lock screen operations. Log in the client again to unlock.
	Switch User	Switch the login user.
	Import Parameters	Import client configuration file from your computer.
	Export Parameters	Export client configuration file to your computer.
View	**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.
	Card Management	Open the Card Management page.
	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.
Tools	**Search Access Control Permission**	Search the added access control permission.
	Card Reader	Configure the card reader parameters.
	Fingerprint Machine	Configure the fingerprint machine parameters.
	Storage Server	Configure the storage server parameters.
	System Configuration	Enter the System Configuration page.
	Download Parameters	Apply the settings on the client to the corresponding access controller.
Help	**User Manual (F1)**	Click to open the User Manual; you can also open the User Manual by pressing **F1** on your keyboard.
	Language	Select the language for the client software and reboot the 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.

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.

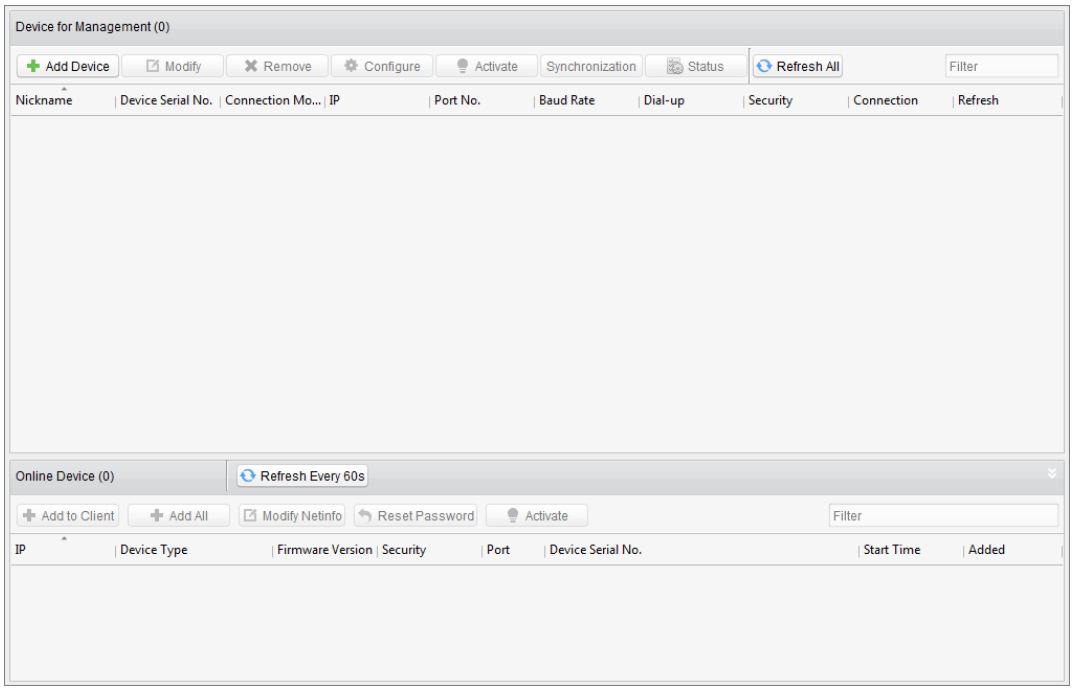
Chapter 3 Hardware Management

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 

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



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

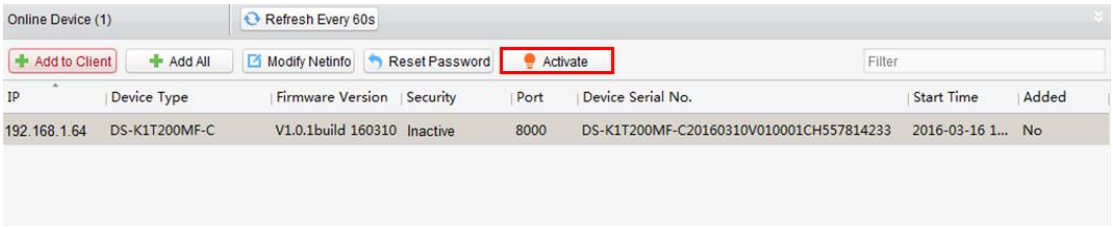
Activating Device and Creating Password

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.

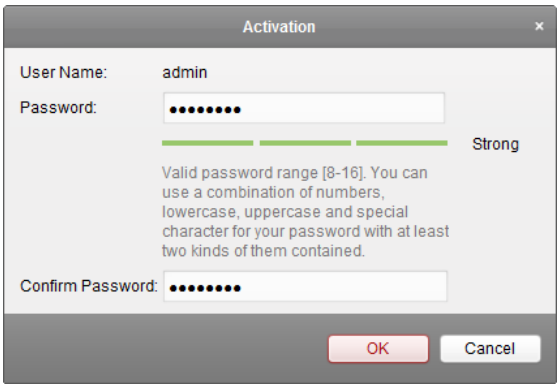
Steps:

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

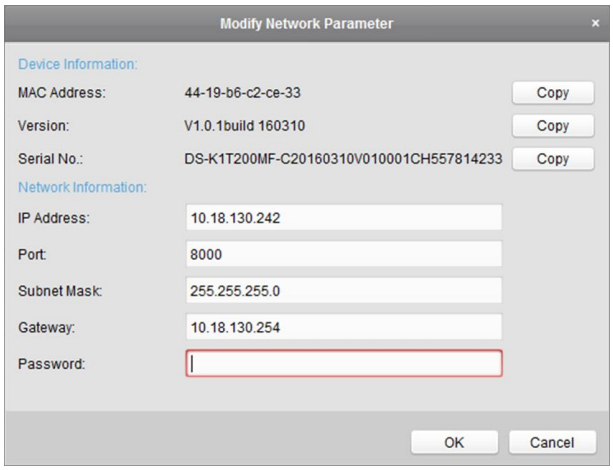


2. Click the **Activate** button to pop up the Activation interface.
3. Create a password in the password field, and confirm the password.

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.*



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.
   1) 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.



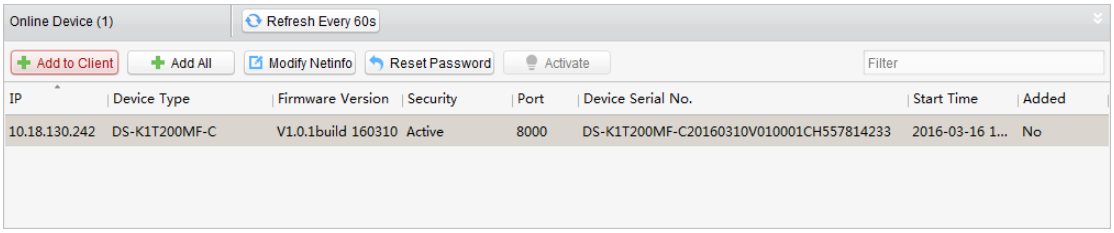
3) Click **OK** to save the settings.

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.

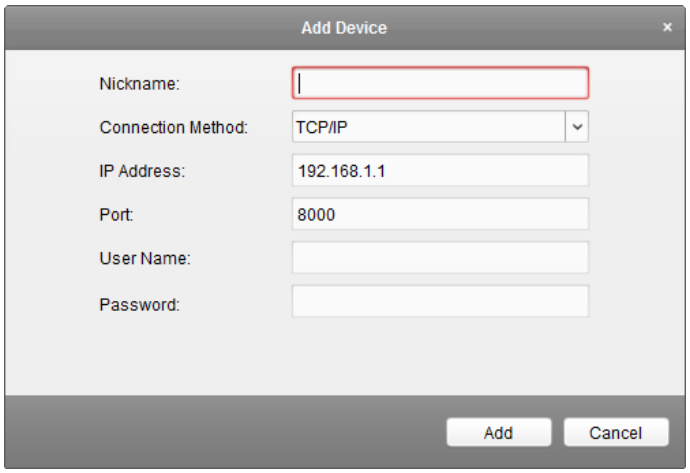


Steps:

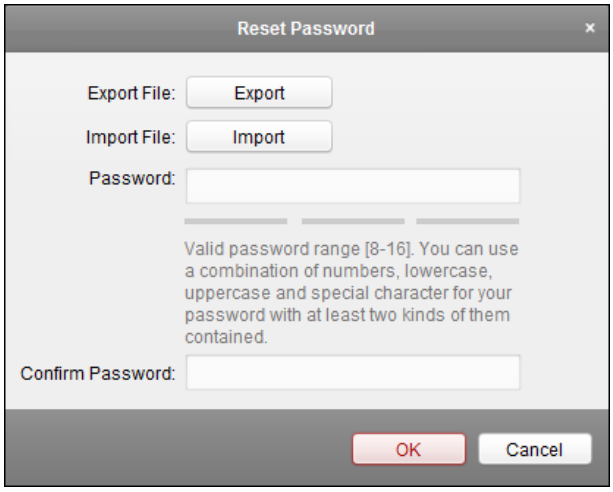
1. Select the devices to be added from the list.

   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.



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.



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 ... 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.

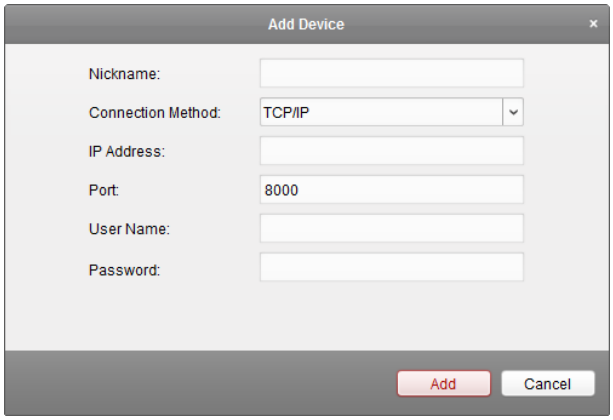
The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in

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.



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.

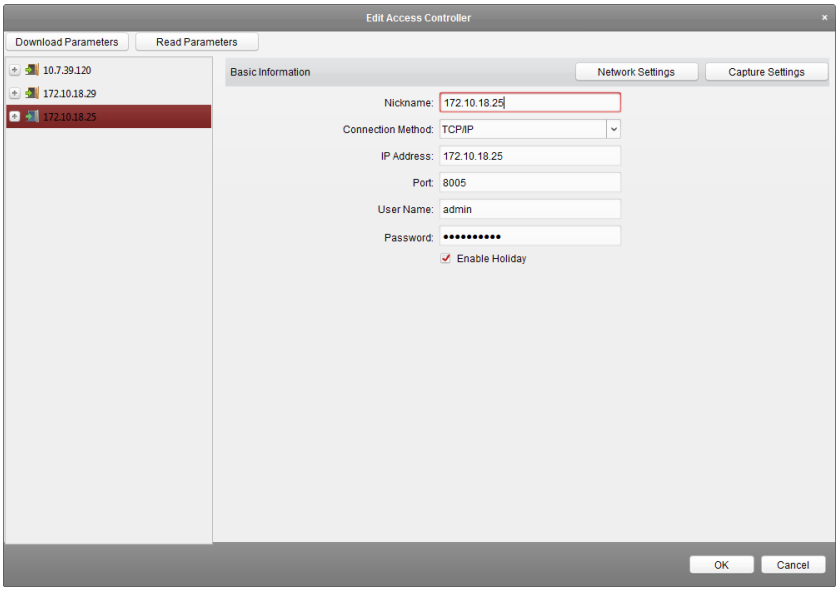
Modifying Device (Basic Information)

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.

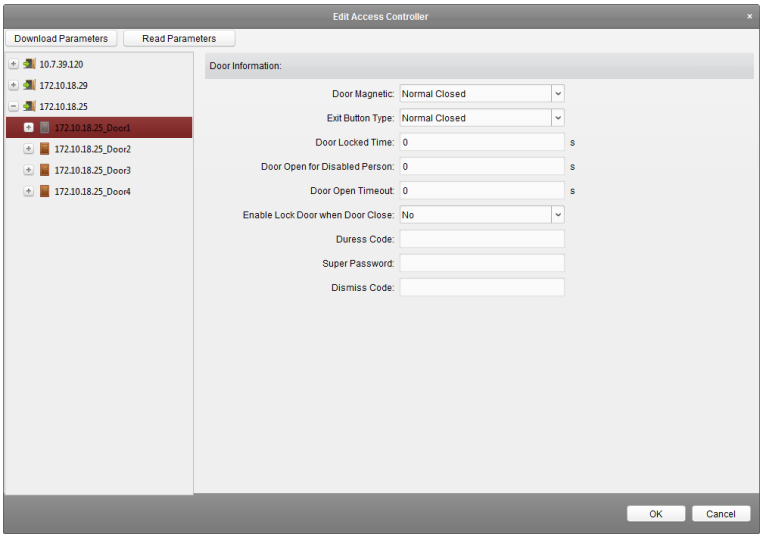
Steps:

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



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.

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.

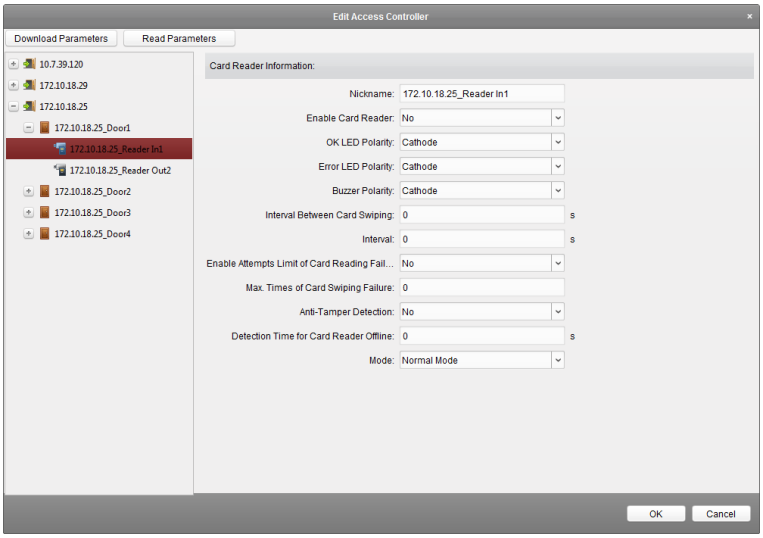
Super Password: The specific person can open the door by inputting the super password.

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.
3. 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.).

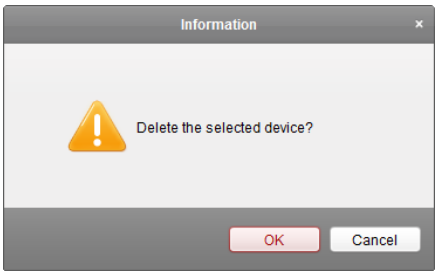
3. Click **OK** button to save parameters.
4. Click **Download Parameters** button to download the updated parameters to the local memory of the device.

Deleting Device

Steps:

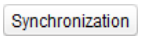
1. In the device list, click to select a single device, or select multiple devices by pressing *Ctrl* button on your keyboard and clicking them one by one.
2. Click 

button to delete the selected device(s).
3. Click **OK** button in the pop-up confirmation dialog to finish deleting.



Time Synchronization

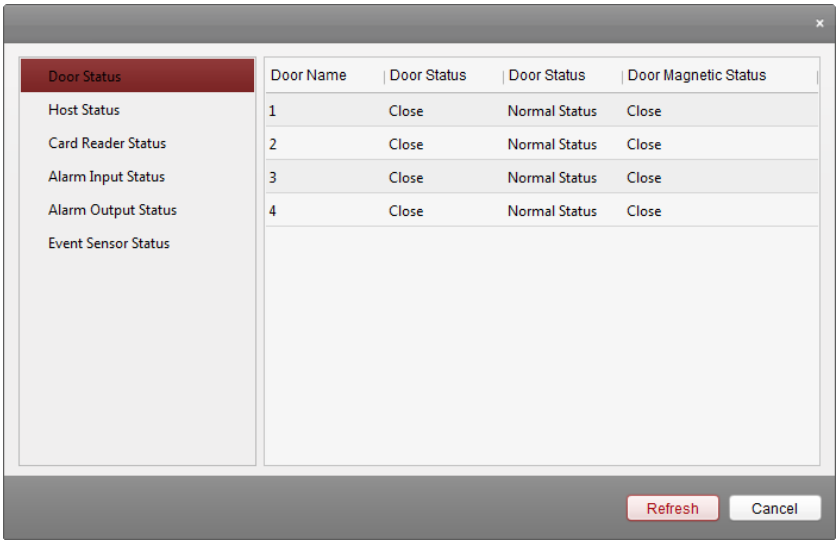
Steps:

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 

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: 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.

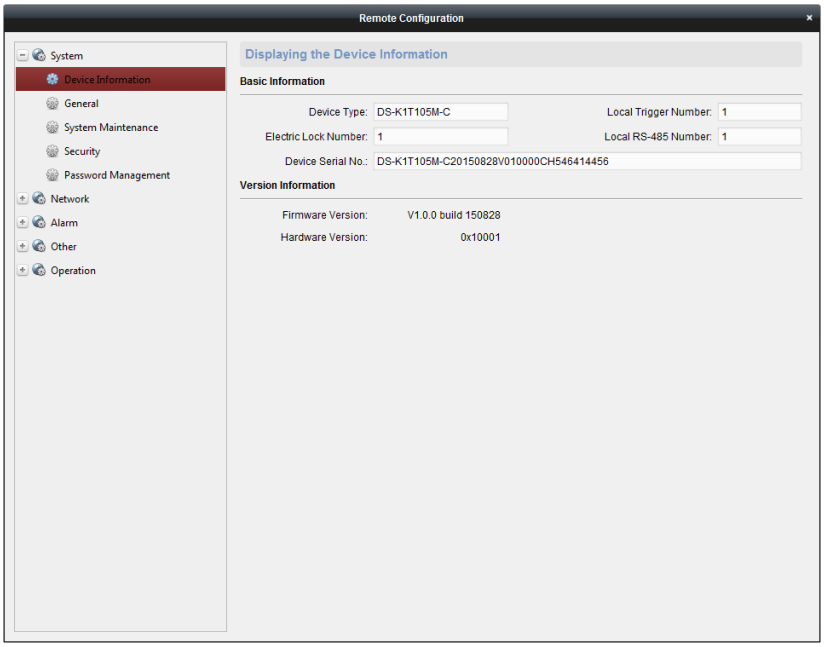
Alarm Input Status: The alarm input status of each port.

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

Event Sensor Status: The event status of each port.

Remote Configuration

In the device list, select the device and click Configure button to enter the remote configuration interface. On this interface, you can set the detailed parameters of the selected access controller. For details about the remote configration, please refer to the User Manual of the Access Controller.

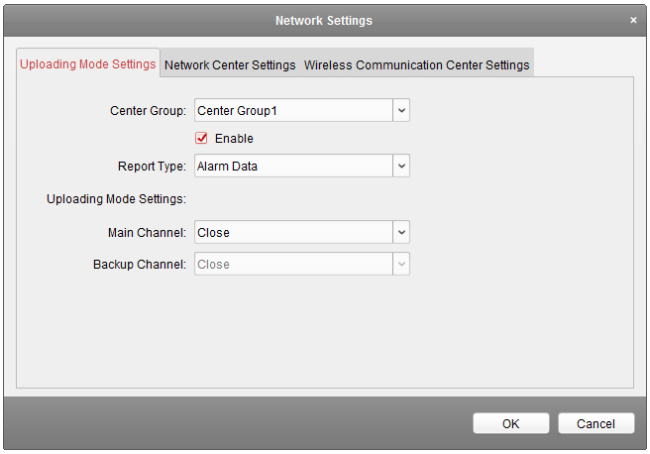


3.1.2 Network Settings

Purpose:

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

Uploading Mode Settings

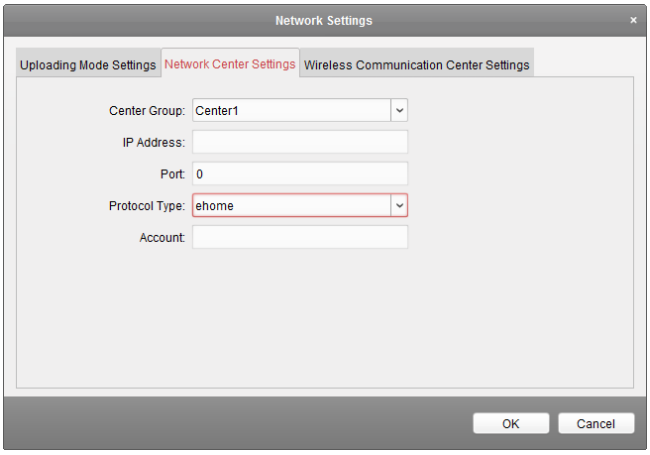


Steps:

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.
6. 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



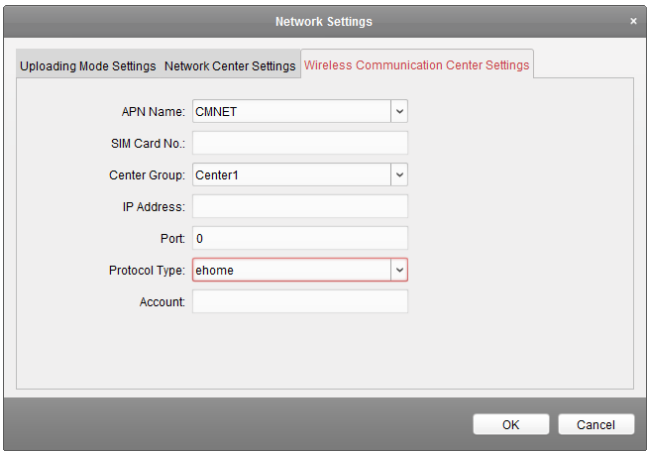
Steps:

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



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.

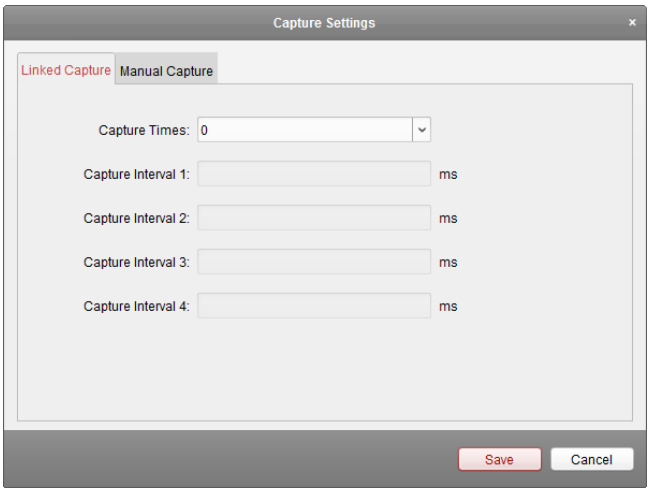
3.1.3 Capture Settings

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



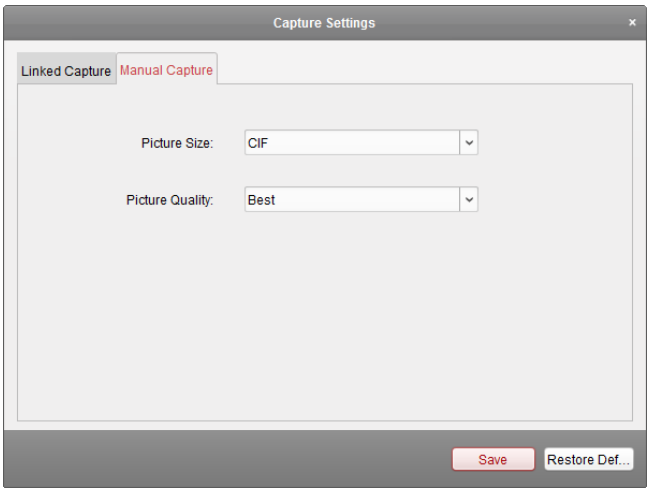
Steps:

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

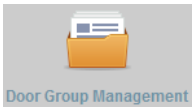
Manual Capture

Steps:

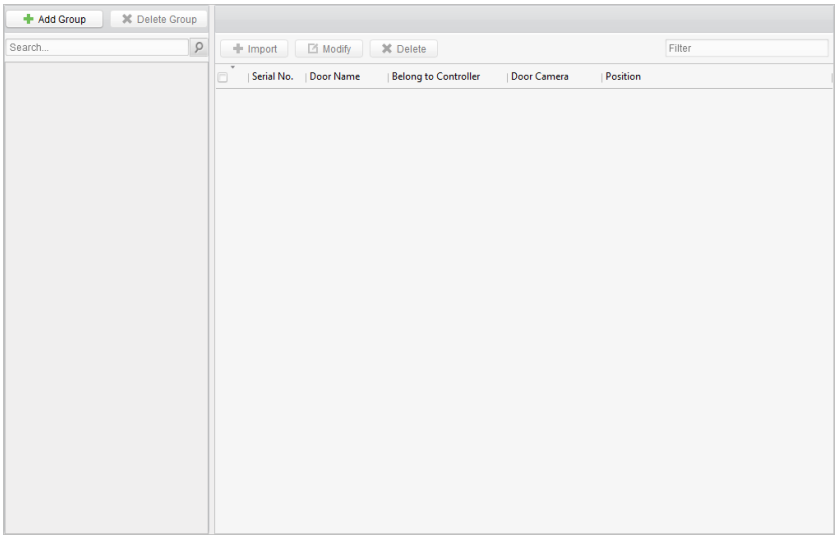
1. In the Edit Access Controller interface, click **Capture Settings** button to enter the capture settings interface.
2. Select the **Manual Capture** tab.
3. Select the resolution of the captured pictures from the dropdown list.
   Note: The supported resolution types are CIF, QCIF, 4CIF/D1, SVGA, 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.



3.2 Door Group Management

Click 

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



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

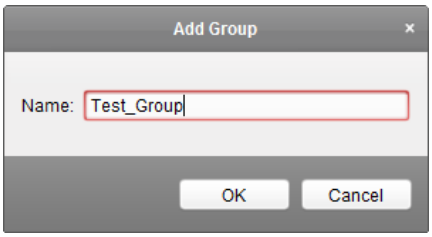
Adding Group

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

Steps:

1. Click 

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



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 

to delete it.

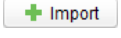
Note: All the access control point in the group will be deleted.

3.2.2 Access Control Point Management

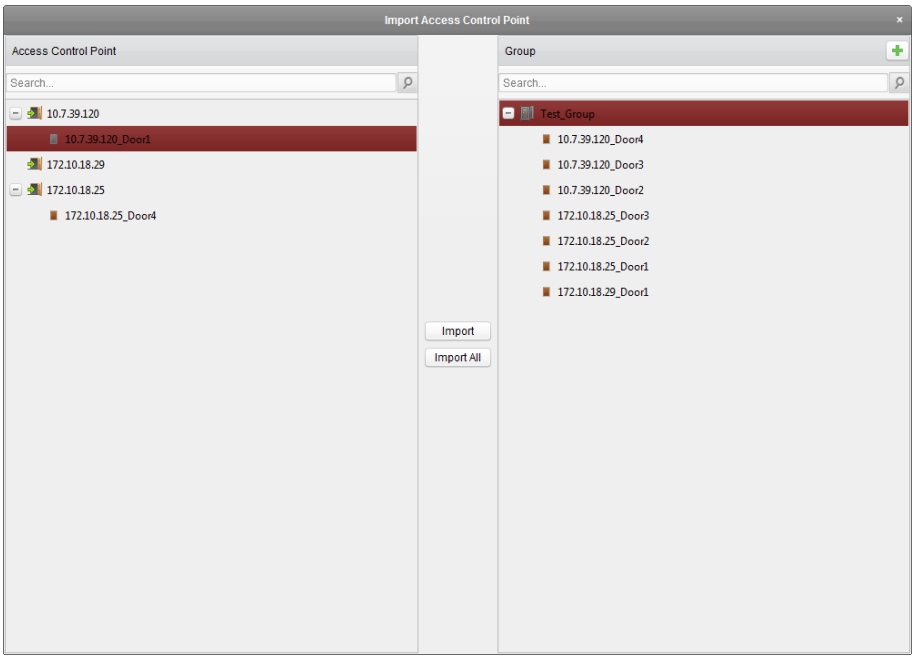
After adding the group, you can import the access control point of the added access controller to the group.

Importing Access Control Point

Steps:

1. Select the added group, and click 

button to pop up the access control point importing interface as follows.



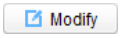
2. Select the access control point to import from the access control point list on the left.
3. Select an added group to import the access control point on the right.
4. Click **Import** button to import the selected access control points or you can click **Import All** to import all the available access 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  or  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  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  button to delete the selected access control point.

Chapter 4 Permission Configuration

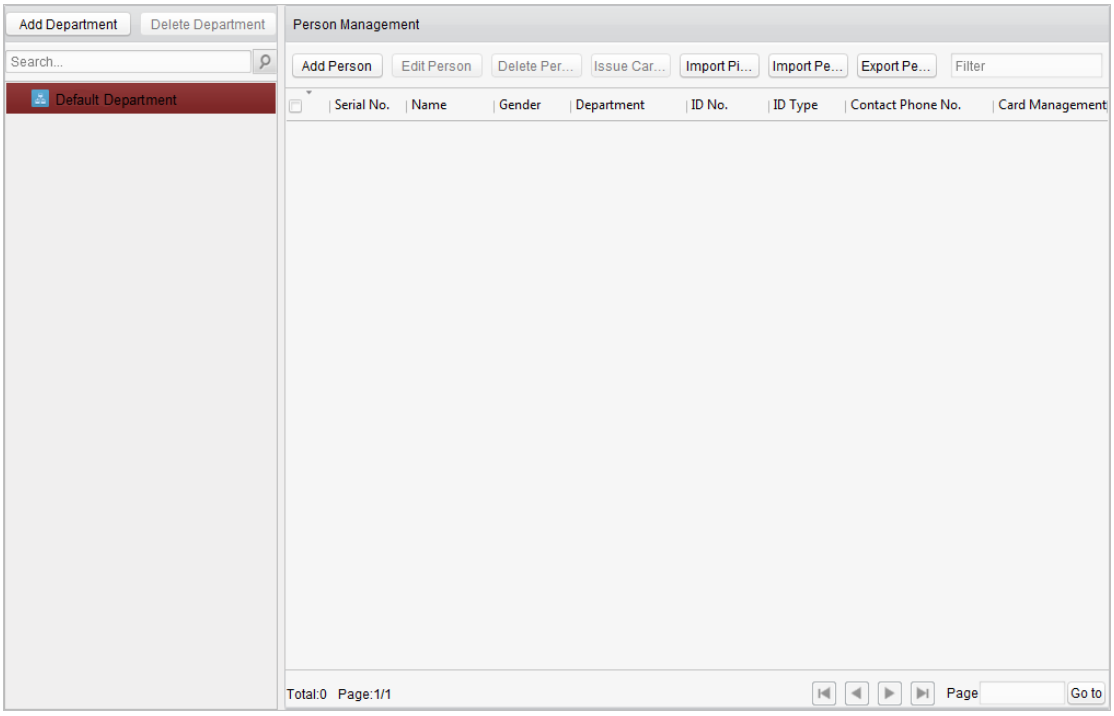
You can add the department and person to the client for management, and add card for access control. You can set the schedule template and configure the access control permission via the client.

4.1 Person Management

Click 

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.



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.

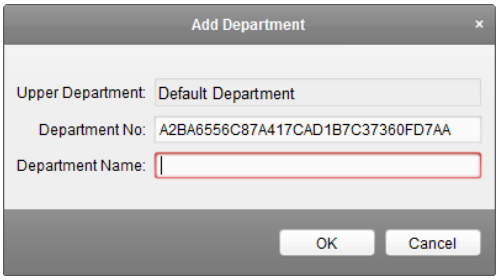
4.1.1 Department Management

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.



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

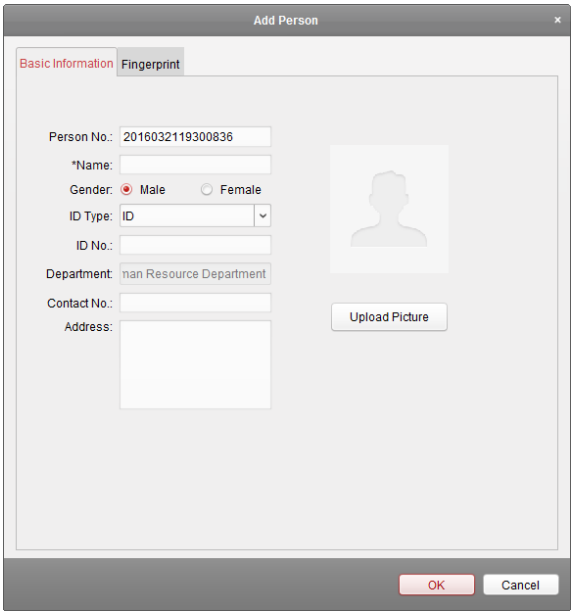
After adding the department, you can add person to the department and manage the added person such as issuing card in batch, importing and exporting person information in batch, etc..

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.



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.
5. 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.

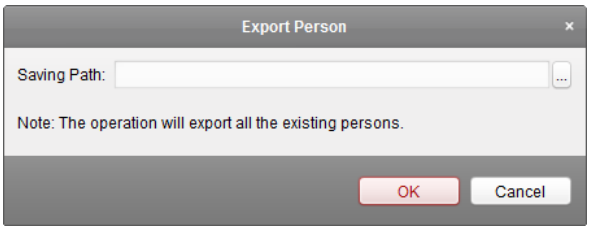
Editing and Deleting Person

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.

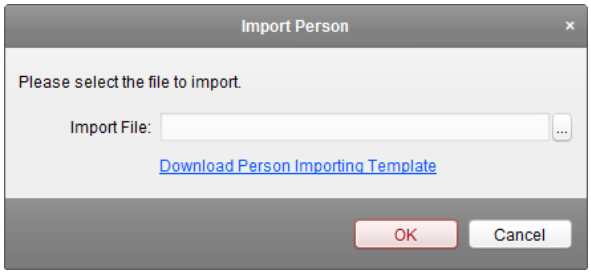
Importing and Exporting Person Information

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

1. 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.



   Click ... 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.



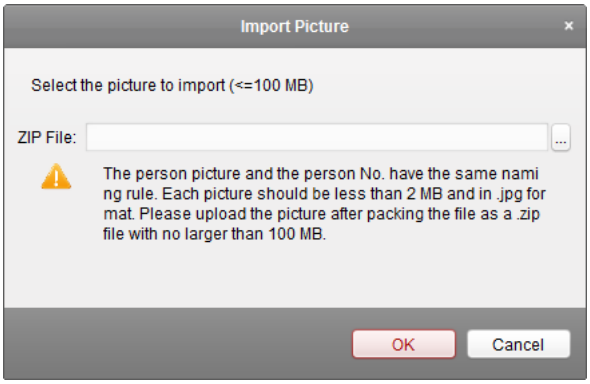
   You can click **Download Person Importing Template** to download the template first.
   Input the person information to the downloaded template.
   Click ... to select the Excel file with person information.
   Click **OK** to start importing.

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.



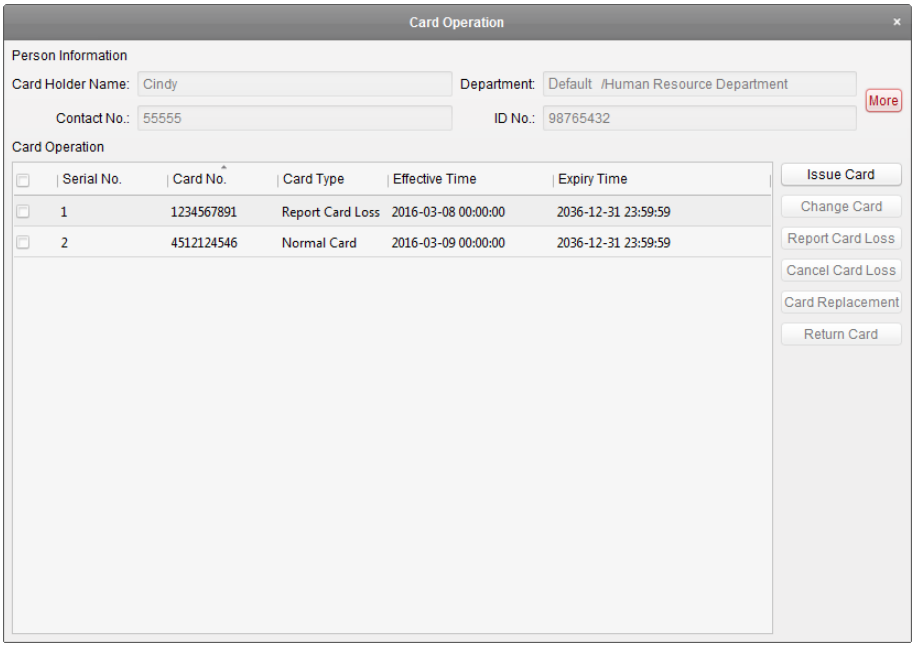
2. Click ... to select the package with person pictures and click **OK** to start importing.

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.



You can click **More** to view the person details.

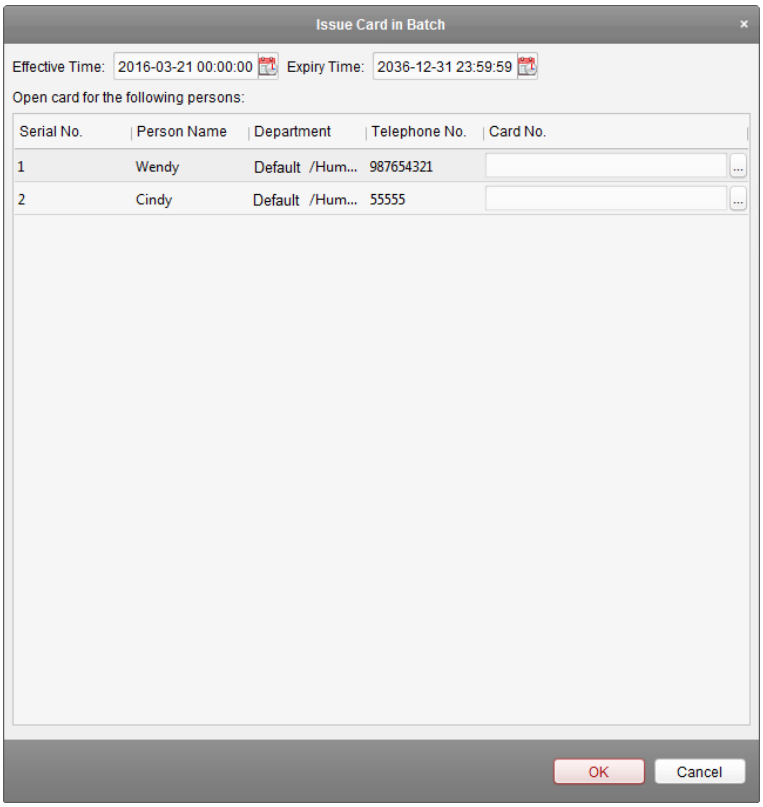
For details about these operation, please refer to *Chapter 4.2 Card Management*.

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*.

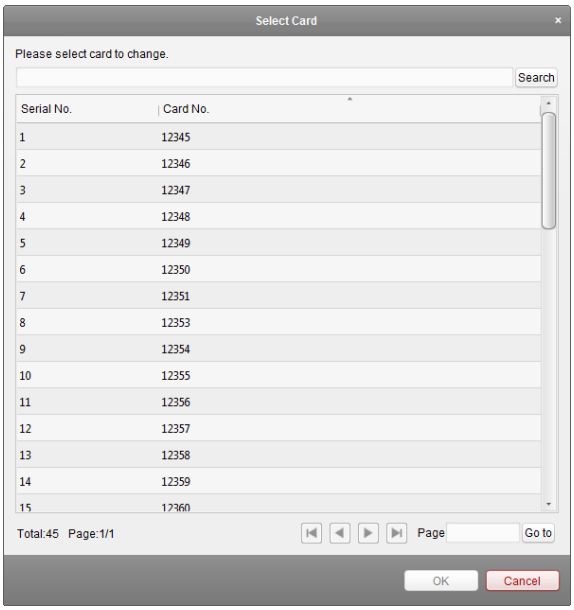
Steps:

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



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.

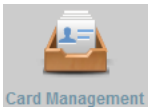


Select the card from the card list and click **OK** to save the settings.

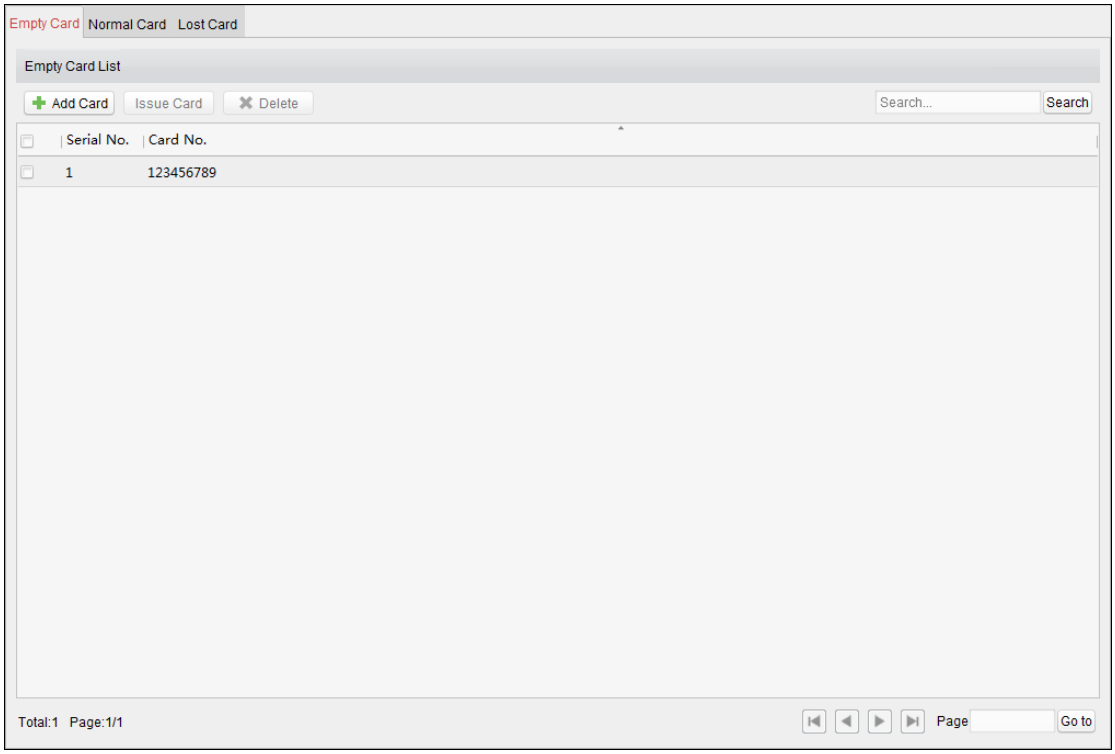
You can input the card No. and click **Search** button to search the card.

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

4.2 Card Management

Click 

on the control panel to enter the card management interface.



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

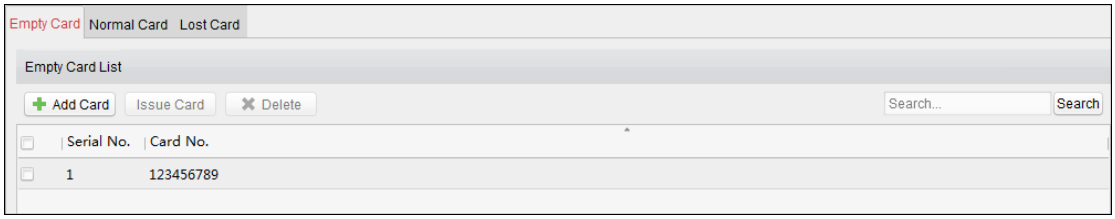
Empty Card: A card has not been issued with a person.

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.



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.

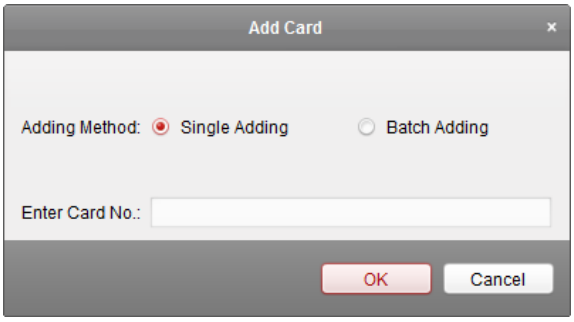
Steps:

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.

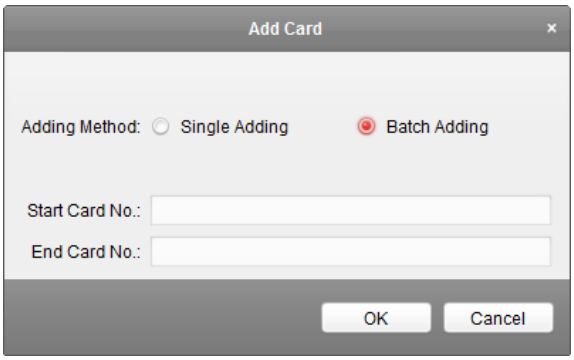


   ✧ **Batch Adding Cards**

   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.



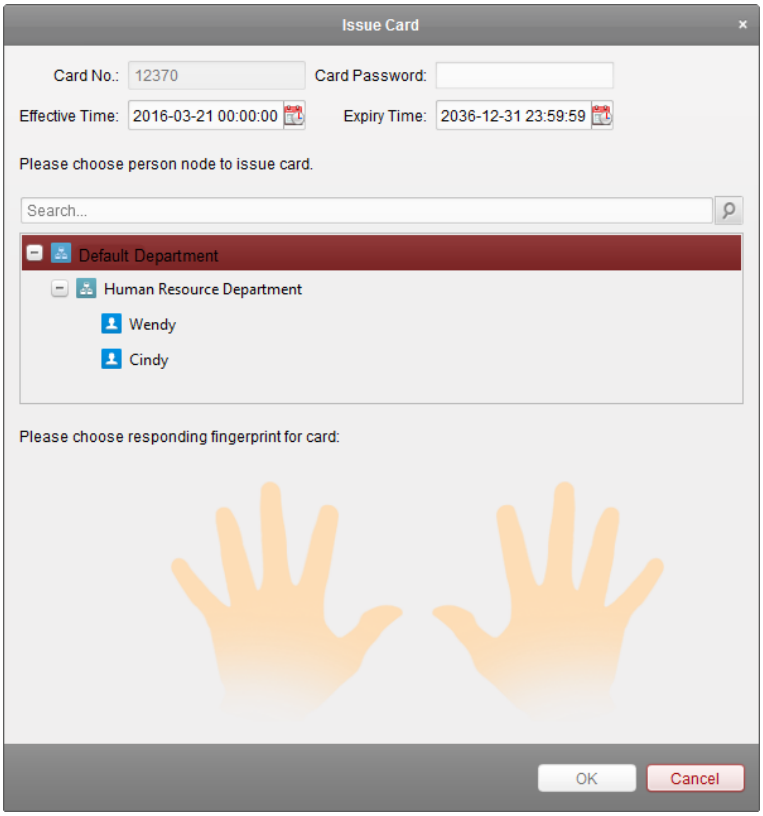
3. Click **OK** button to finish adding.
4. You can check the checkbox of the added card and click Delete to delete the card.

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.



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.

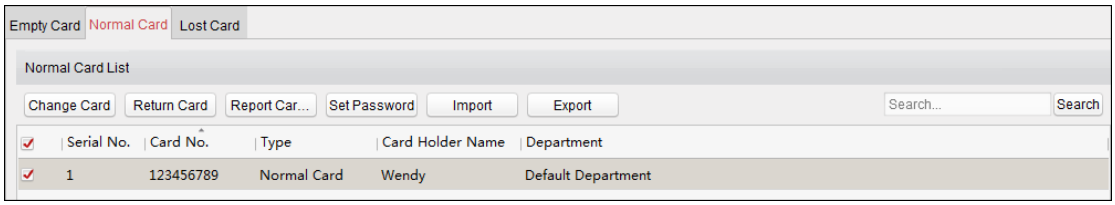
Notes:

- 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

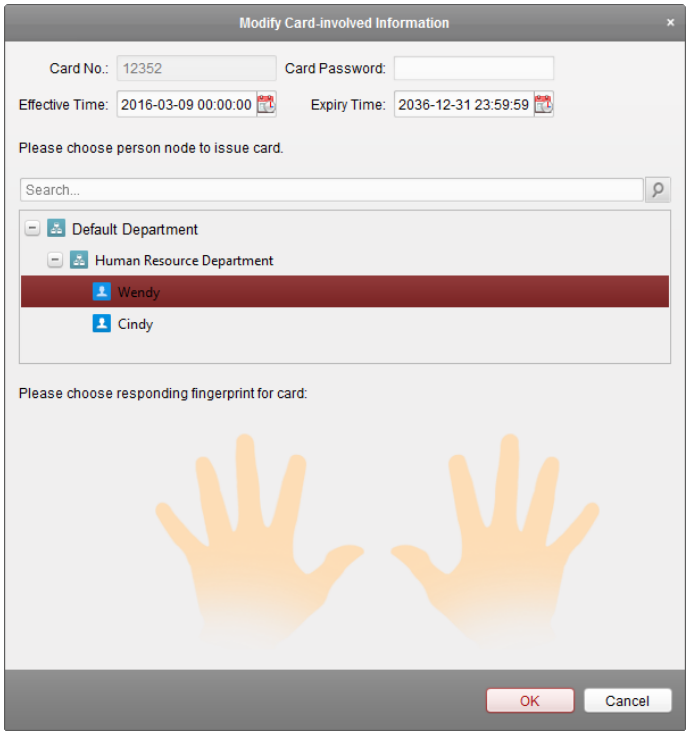
After adding the empty card to the client and issue the card to the person, the card will be displayed in the Normal Card list.

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.



Editing Card

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

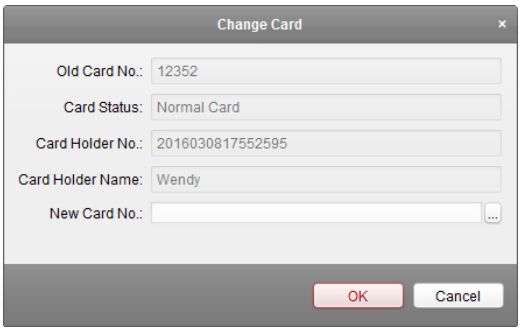


You can modify the card effective time and expiry time, and you can change the person and select the conrresponding fingerprint to issue the card again.

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.



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:

1. 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

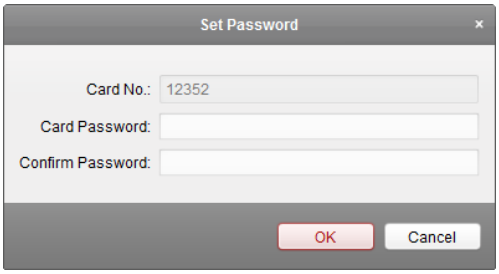
Steps:

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.



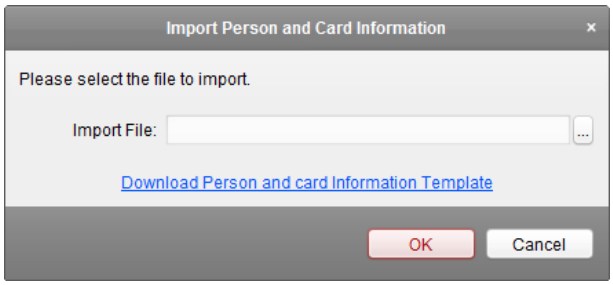
2. Input the card password and confirm the password. The card password should contain 4 to 8 digits.
3. Click **OK** to save the settings.

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.



   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..

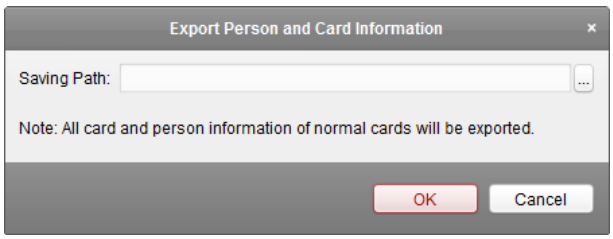
   Note: The Card No. should be 1 to 10 digits

   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.

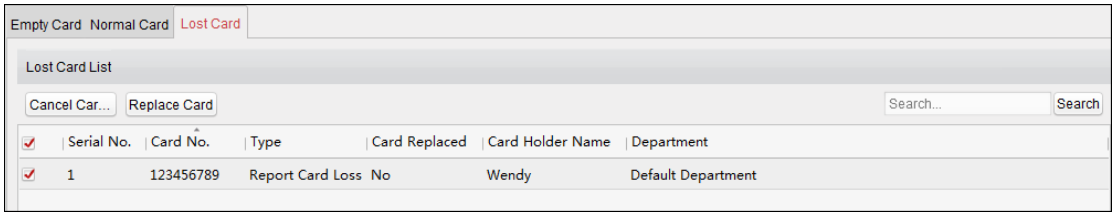
   Click ... to select the path to save the exported file.



   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.



Canceling Card Loss

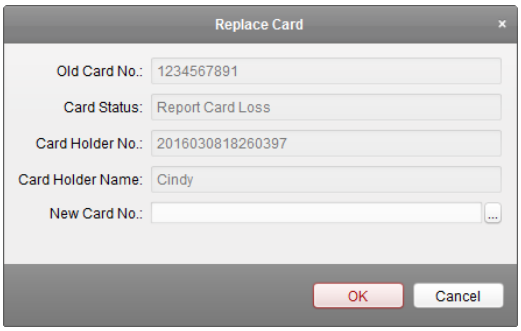
Steps:

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

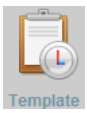
Steps:

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.

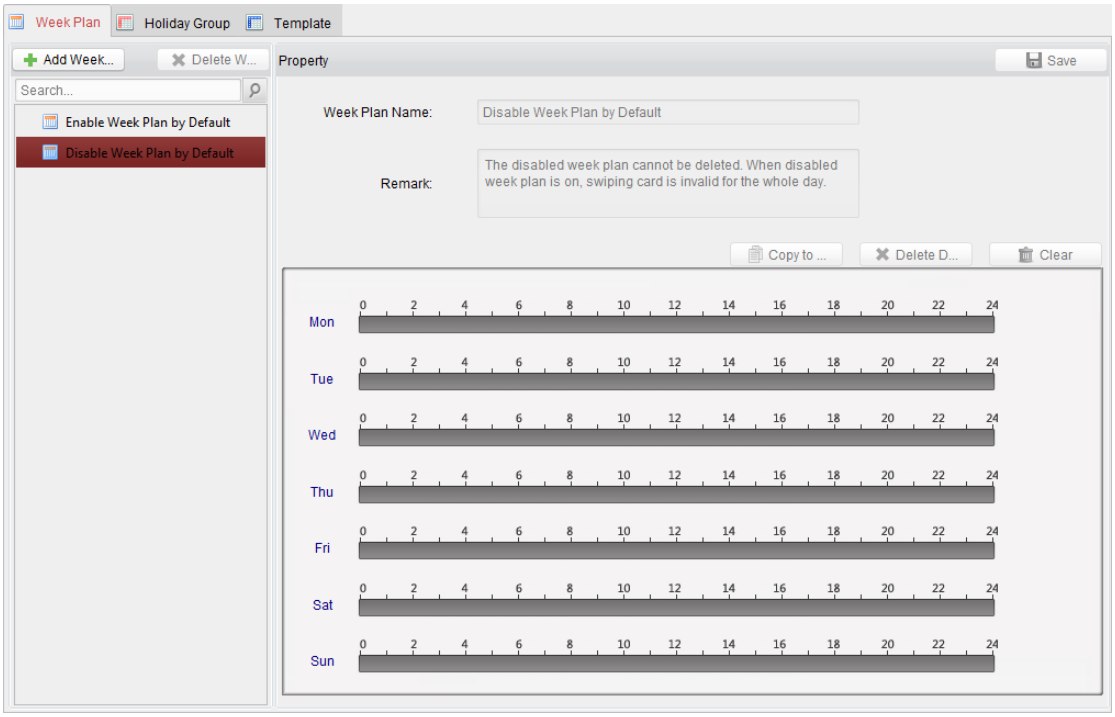


3. Click ... button to select another card in the popup window as the new card and the predefined permissions of the lost card will be copied to the new one automatically.
4. Click **OK** to save the changes.

4.3 Schedule Template

Click 

on the control panel to enter the schedule template interface.



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

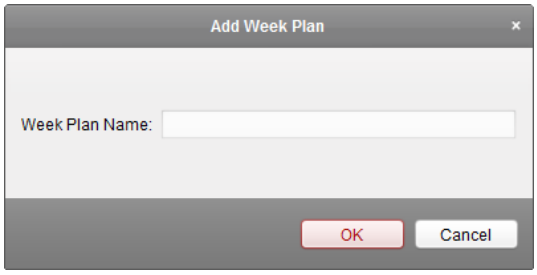
4.3.1 Setting Week Plan

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.



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.

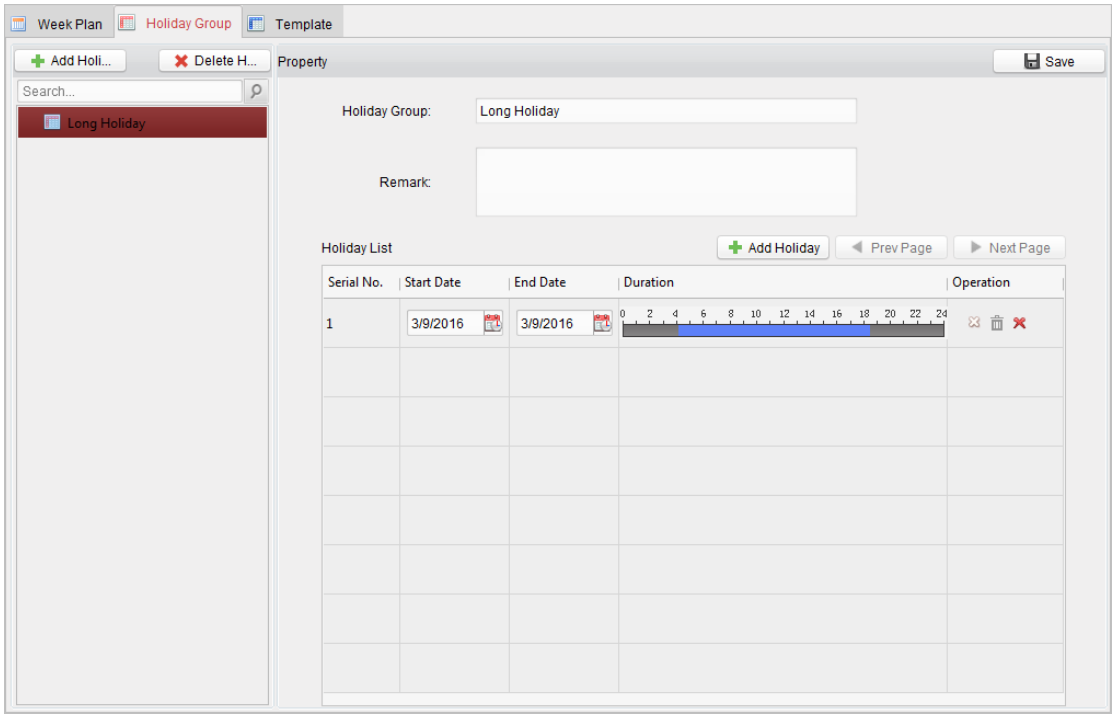
   Note: Up to 8 time periods can be set for each day in the schedule.
6. When the cursor turns to , you can move the selected time bar you just edited. You can also edit the displayed time point to set the accurate time period.

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

7. 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.

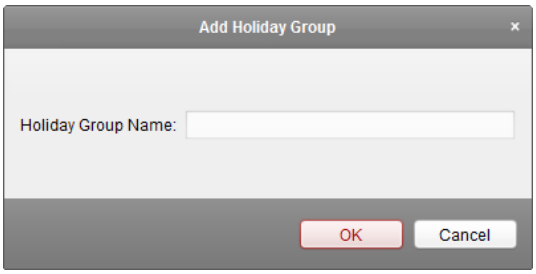
4.3.2 Setting Holiday Group

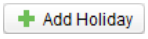
Click **Holiday Plan** tab to enter the Holiday Plan Management interface.



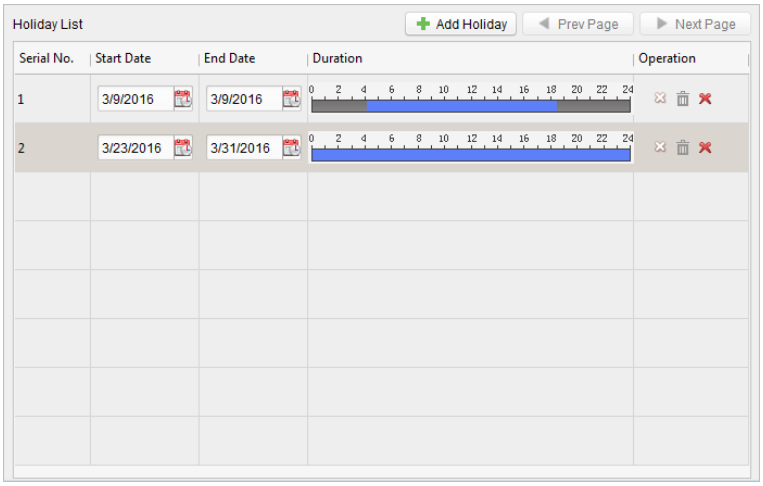
Steps:

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



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 

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.



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 , 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 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

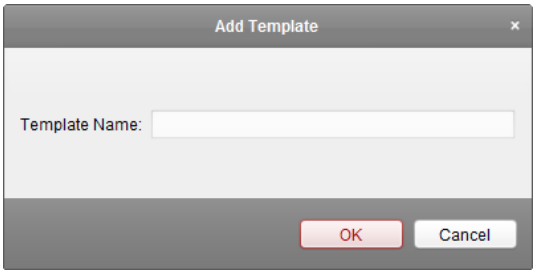
After setting the week plan and holiday plan, you can configure the schedule template.

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.

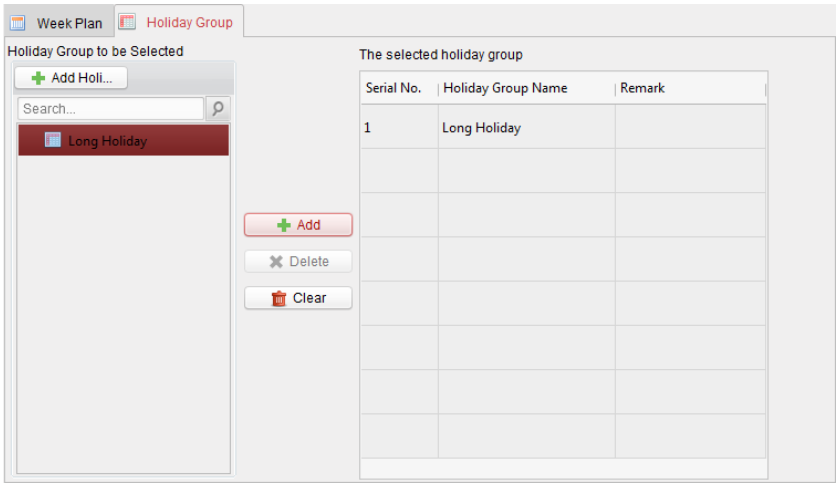
4. Select a week plan to apply to the schedule.

   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*.

5. Select holiday groups to apply to the schedule.

   Note: Up to 4 holiday groups can be added.



   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 to delete it.

   You can click Clear to delete all the added holiday groups.

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

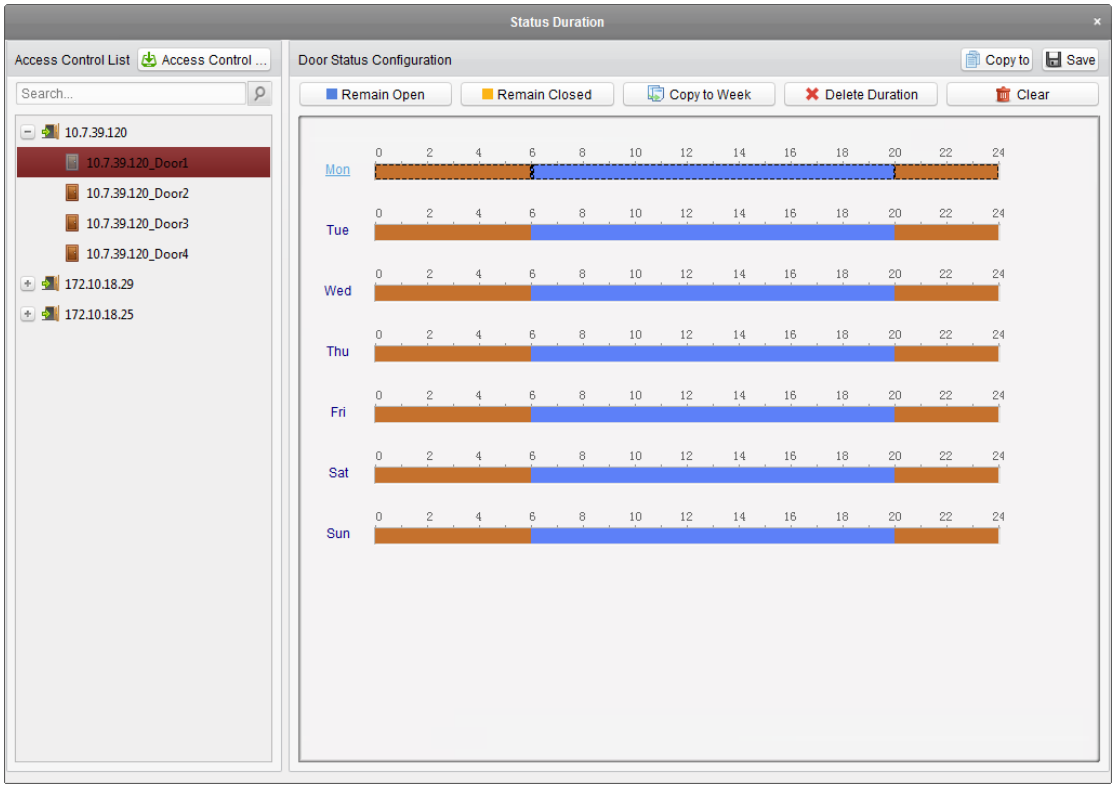
4.4 Door Status Duration Management

Purpose:

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

Click 

icon on the control panel and click Status Duration button to enter the Status Duration interface.



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.
   1) Select a door status brush as Remain Open or Remain Closed.

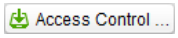
      Remain open: The door will keep open during the configured time period. The brush is marked as .

      Remain Closed: The door will keep closed during the configured duration. The brush is marked as .
   2) Click and drag on the timeline to draw a color bar on the schedule to set the duration.

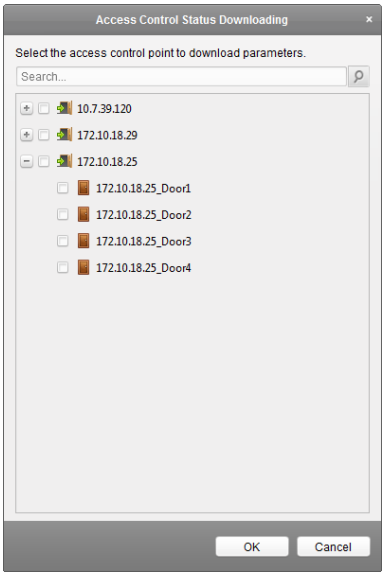
Note: The min. segment of the schedule is 30min.

When the cursor turns to  , 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
4. 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 

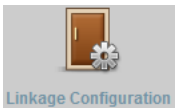
to popup the Access Control Status Downloading dialog box.



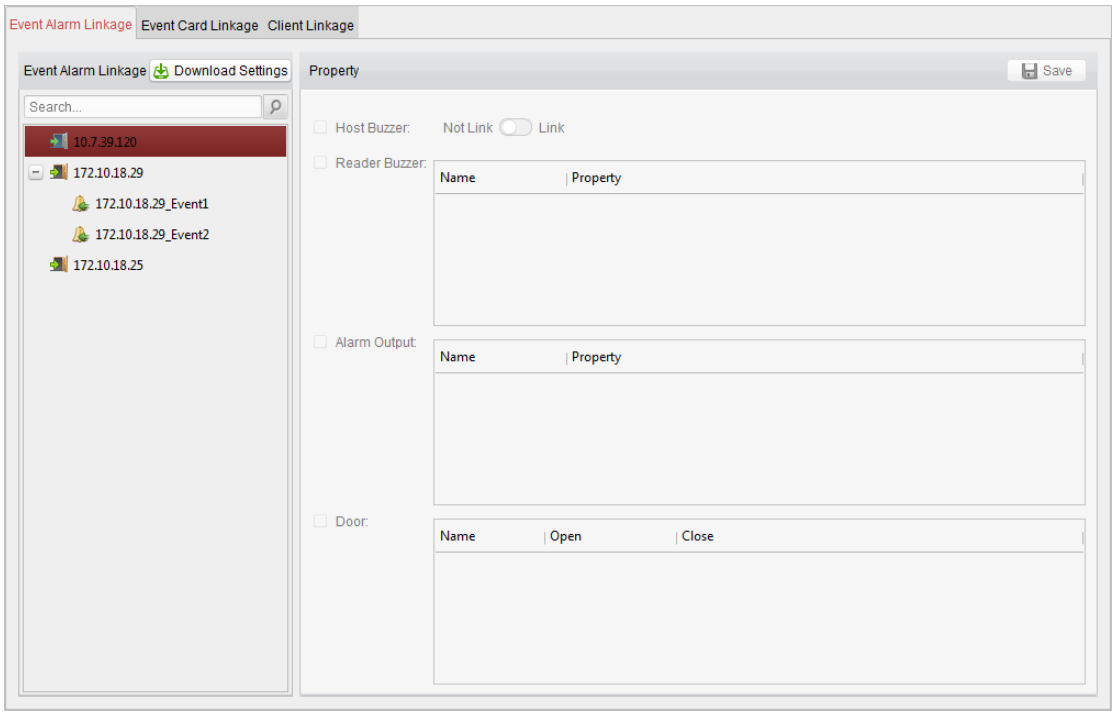
Select a control point and click **OK** to download the settings to access control point.

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

4.5 Linkage Configuration

Click 

on the control panel to enter the Linkage Configuration interface.



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

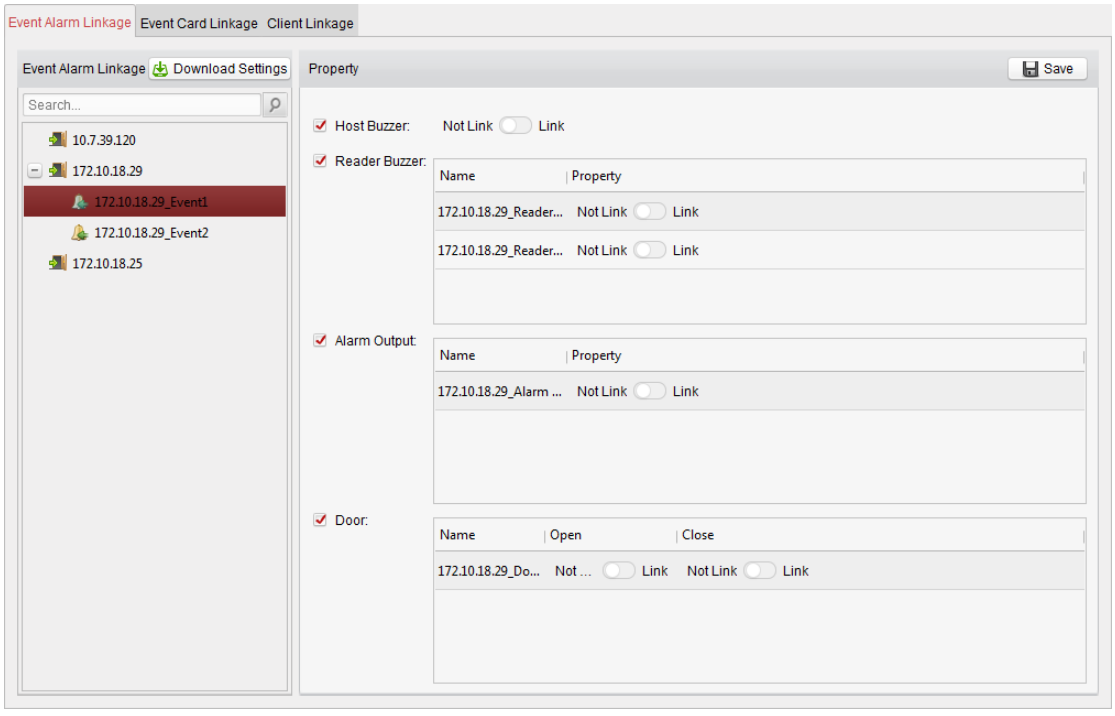
4.5.1 Event Alarm Linkage

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.



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  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.

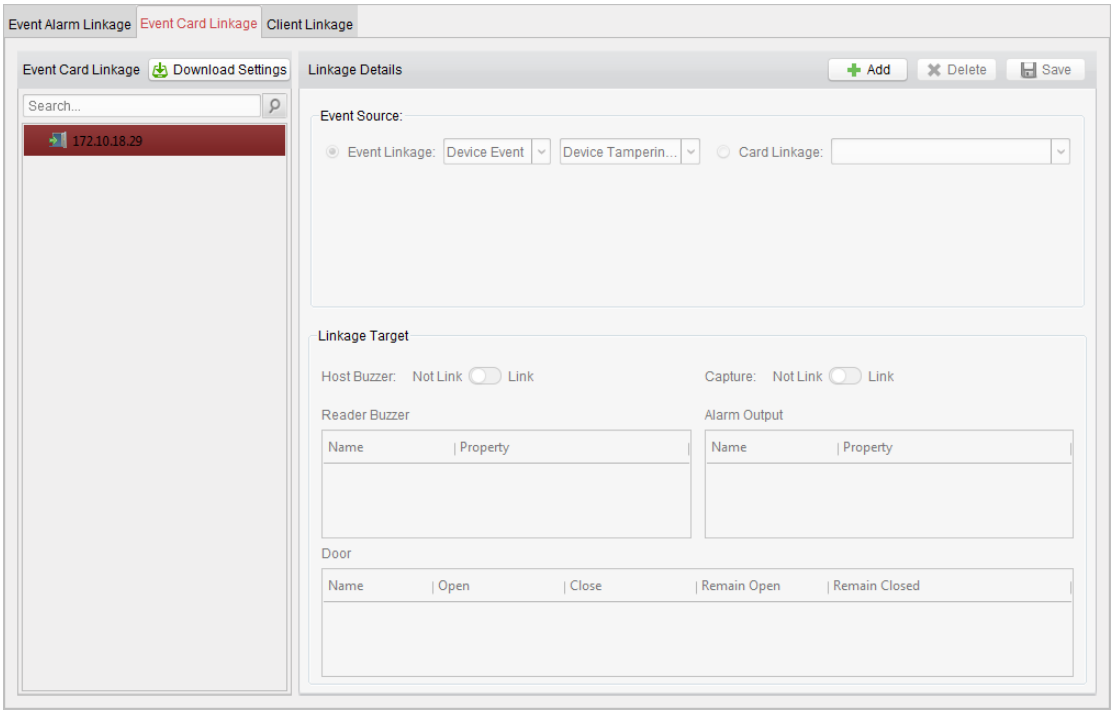
   Door (Open/Close): The door will be open or closed when the case is triggered.

   Note: The Door cannot be configured as open or closed at the same time.
4. Click **Save** button to save the settings.
5. Click 

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.



Select the access controller from the list on the left.

Click 

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.

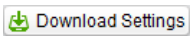
Steps:

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 to  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 

to download the updated parameters to the local memory of the device to take effect.

Card Linkage

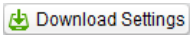
Steps:

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 to  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 

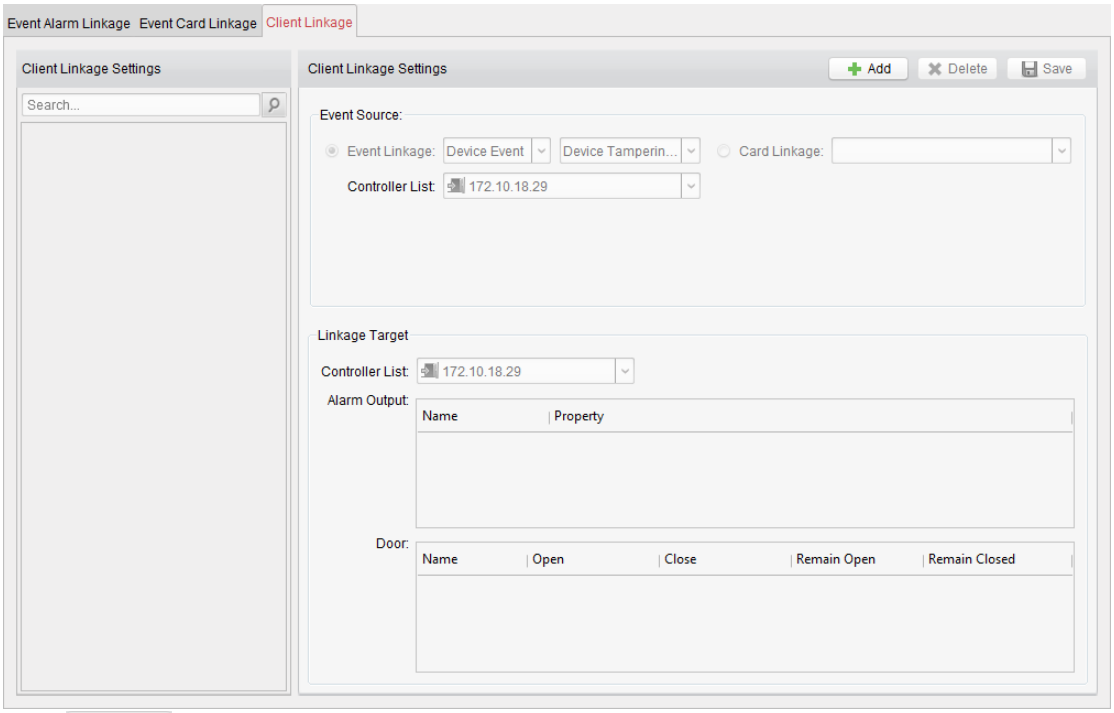
to download the updated parameters to the local memory of the device to take effect.

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.



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 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.

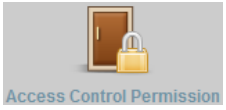
Card Linkage

Steps:

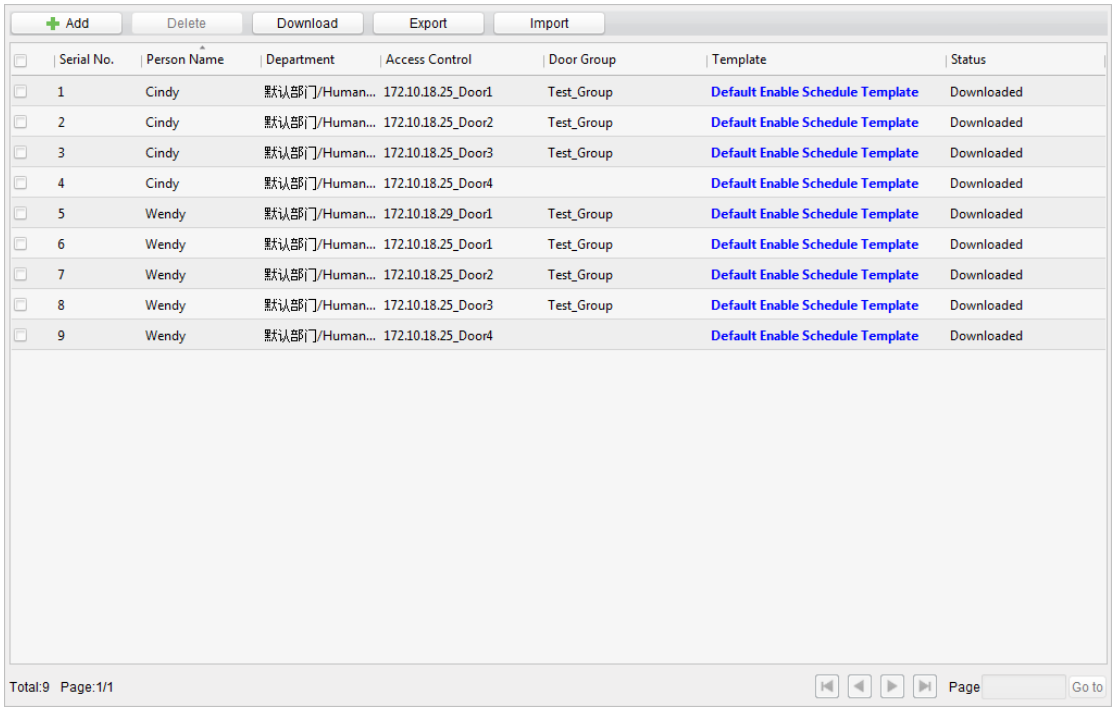
1. Click to select the linkage type as **Card Linkage**.
2. Select the card from the dropdown list and select the access controller as event source.

3. Select the card reader from the table for triggering.
4. 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 

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



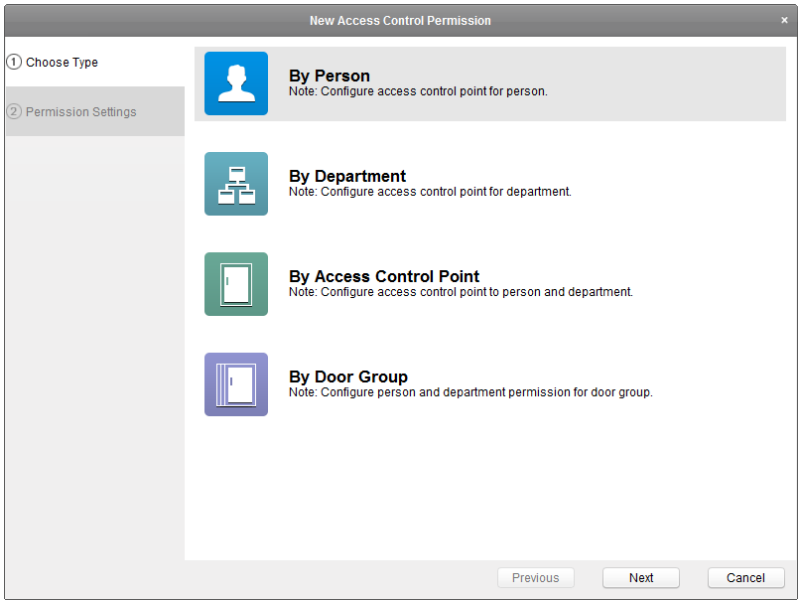
4.6.1 Adding Permission

Purpose:

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

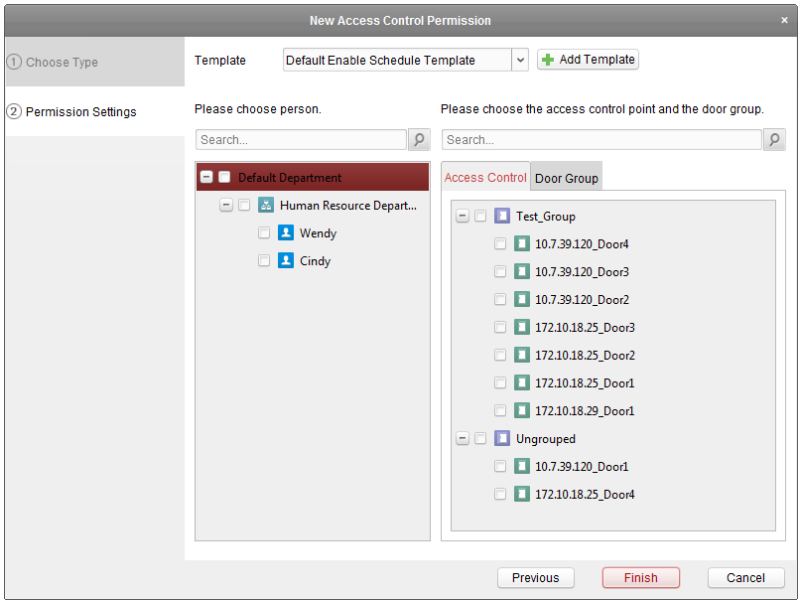
Steps:

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



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.

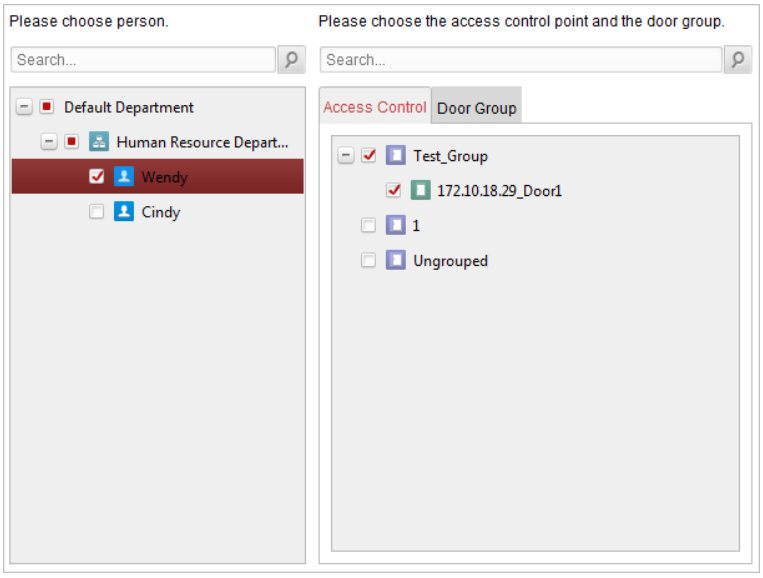


4. Click on the dropdown menu to select a schedule template for the permission.

   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.

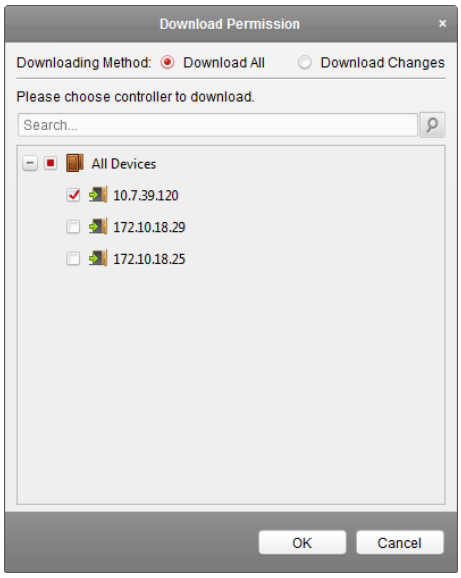
   You can select the added permission in the list and click **Delete** to delete it.

4.6.2 Downloading Permission

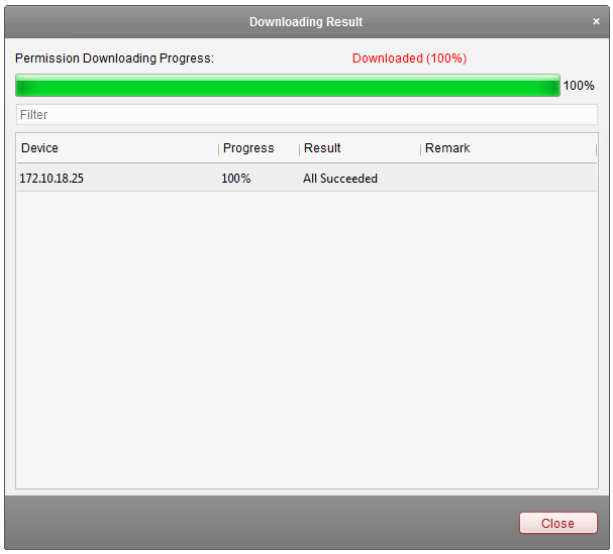
You can apply the added permission to the access control to take effect.

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.

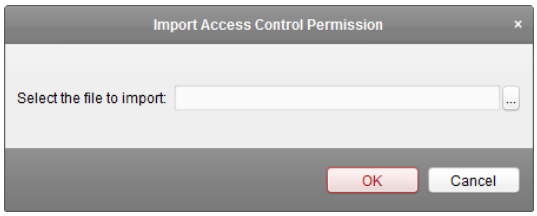


4.6.3 Importing/Exporting Permission

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

Steps:

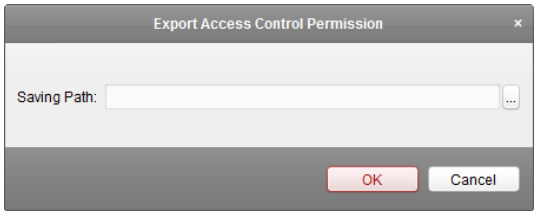
1. To import the permission in batch, click **Import** button to pop up the following dialog box.



   Click ... 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.

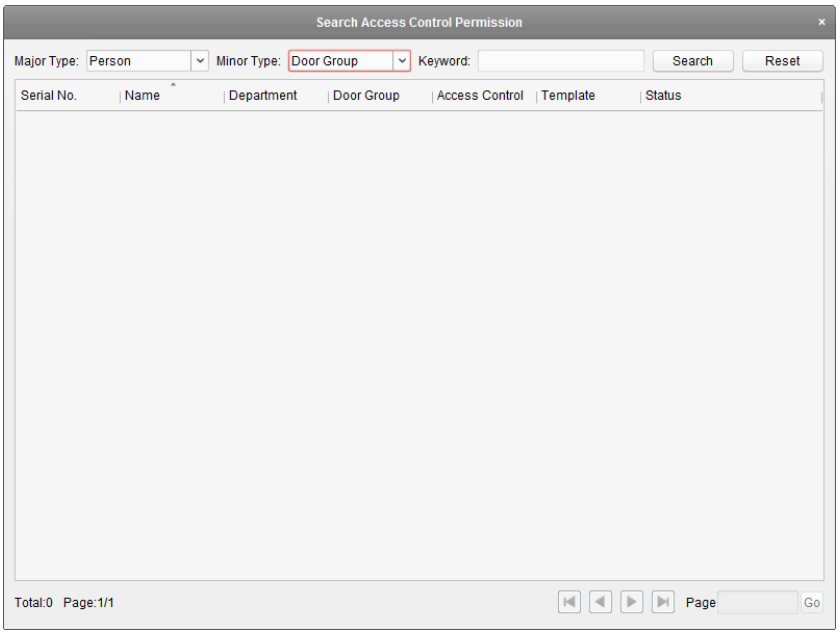
   Note: The exported permission file is not editable.

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.

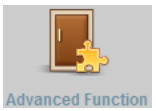


2. Set the major type as the main search condition from the dropdown list. You can set it as by person, department, door group, or access control point.
3. Set the minor type as the second search condition from the dropdown list. You can set it as by door group or access control point.
4. You can also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

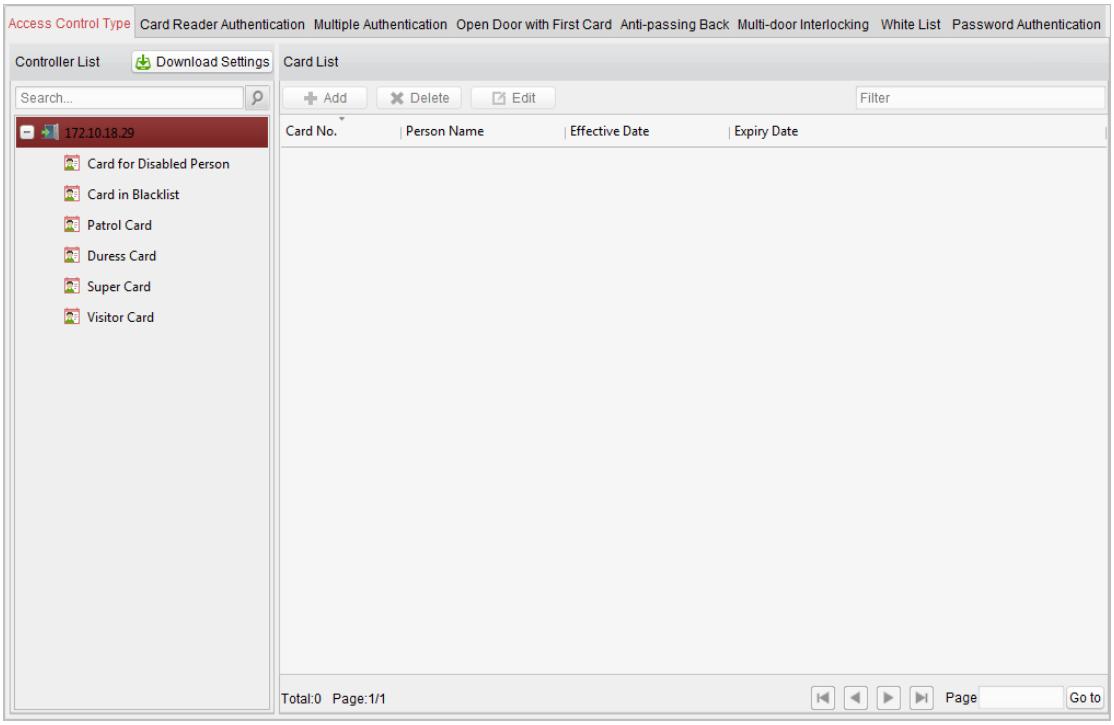
4.7 Advanced Functions

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 

icon on the control panel to enter the following interface.



4.7.1 Access Control Type

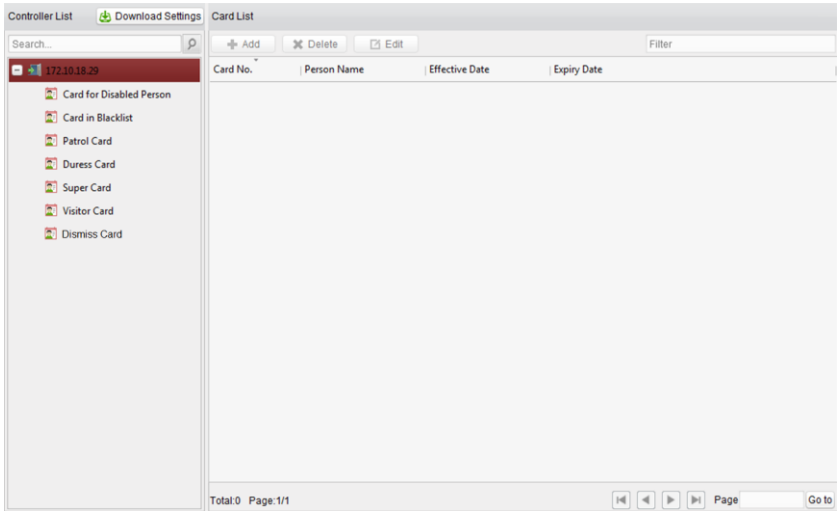
Purpose:

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.

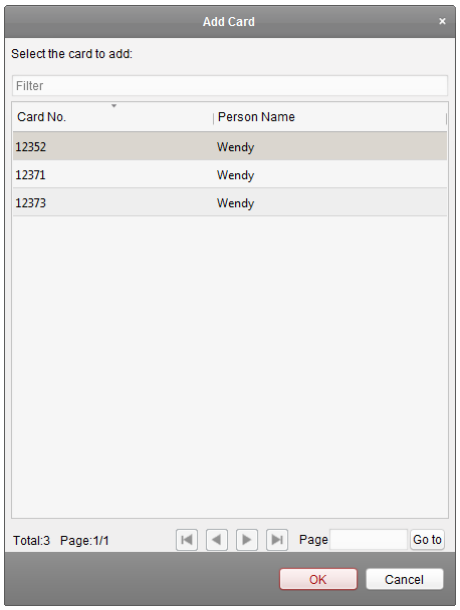
Visitor Card: The card is assigned for visitors.

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

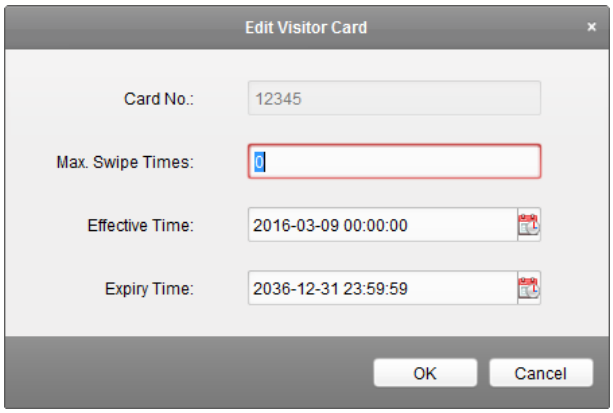
Notes:

- 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.



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 Edit to edit the Max. Swipe Times, card Effective Time and Expiry Time.



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

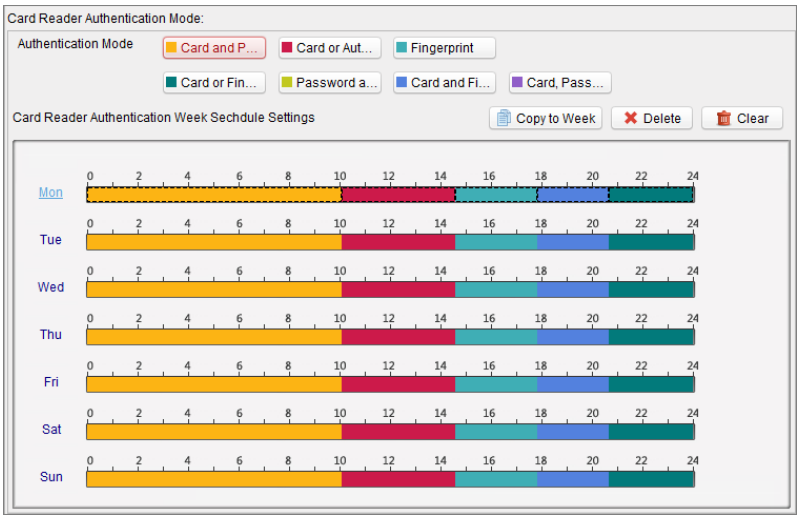
5. Click Download Settings button to take effect of the new settings.
6. (Optional) You can click **Delete** to remove the card from the card type and the card can be available for being re-assigned.

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.

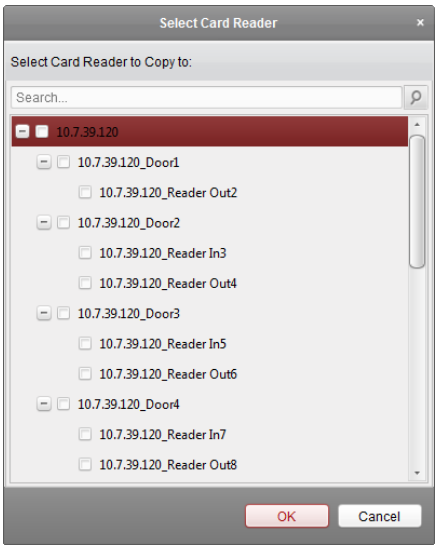


4. Repeat the above step to set other time periods.

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.



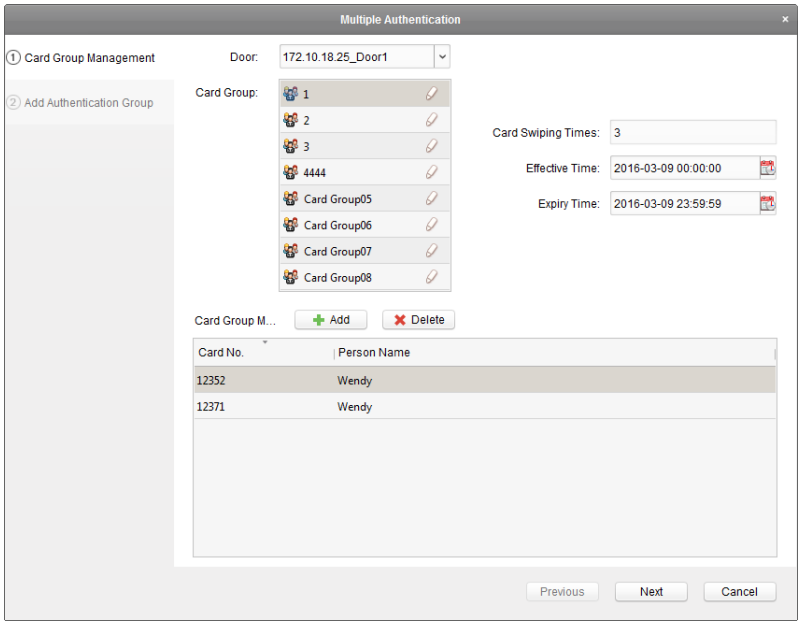
6. Click **Save** button to save parameters.
7. Click Download Settings button to take effect of the new settings.

4.7.3 Multiple Authentication

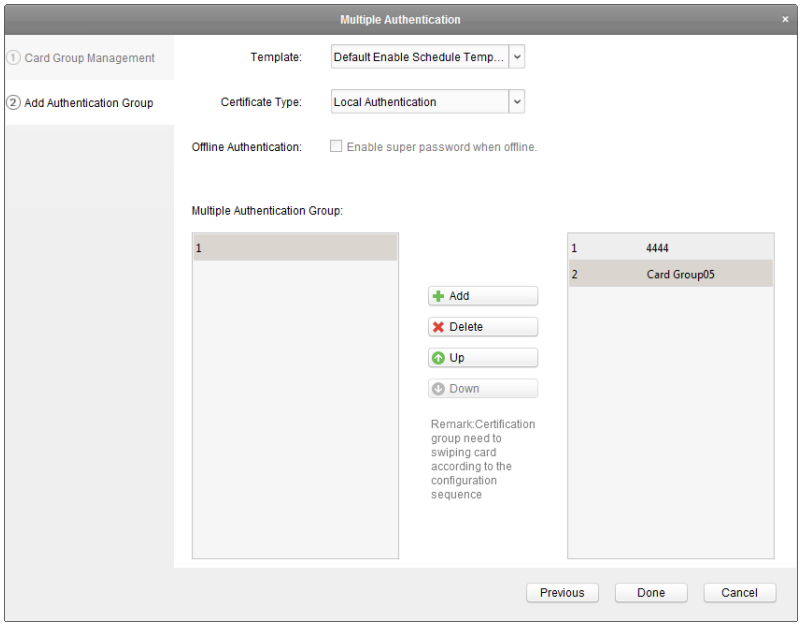
You can manage the cards by group and set the authentication for multiple cards for one access control point (door).

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:



3. 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.
4. 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.
5. 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.



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*.
8. 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:

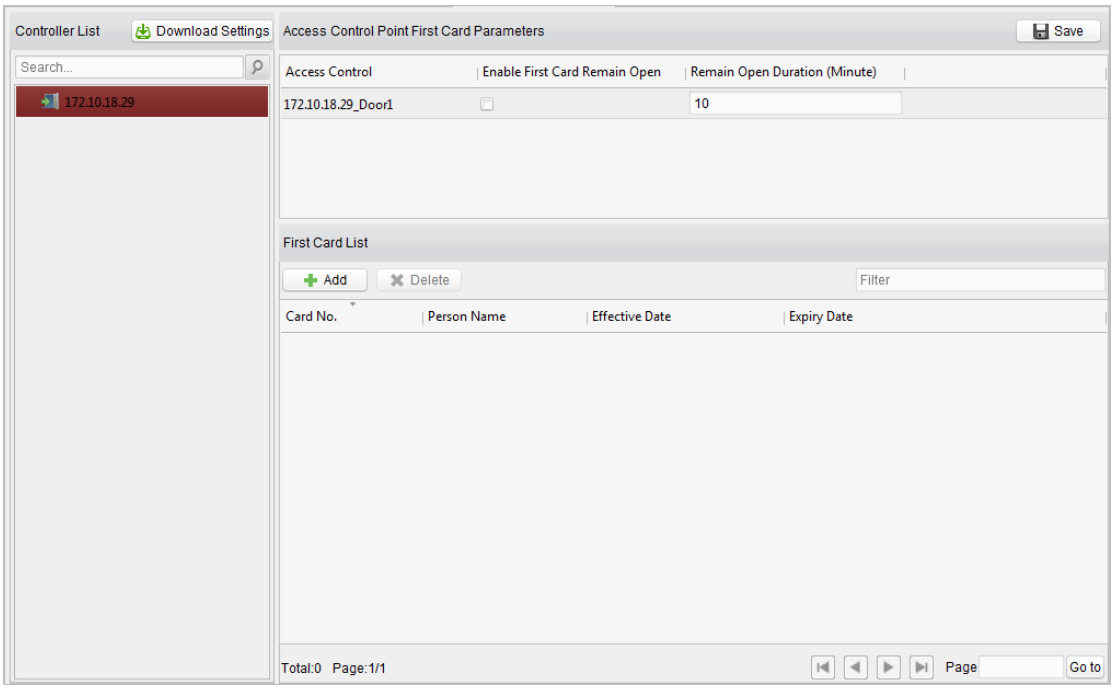
- For each access control point (door), up to four authentication groups can be added.

- 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

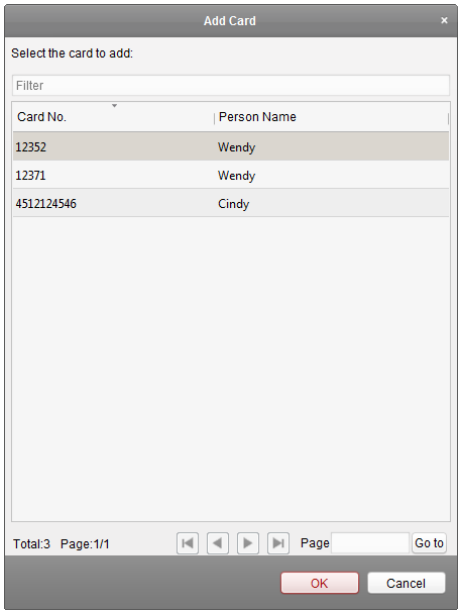
Purpose:

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



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.
3. 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.



1) 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.

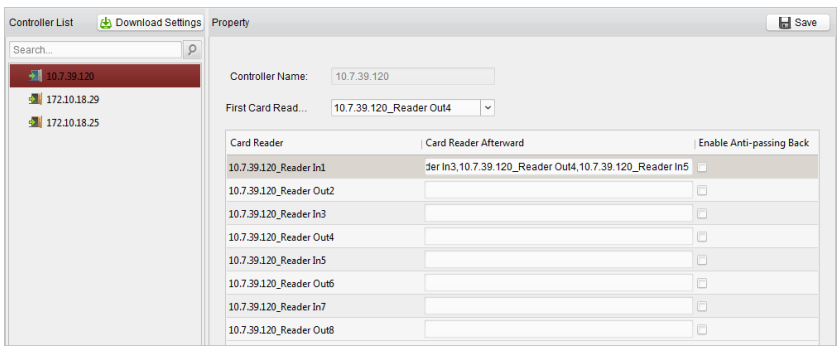
Notes:

- 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)

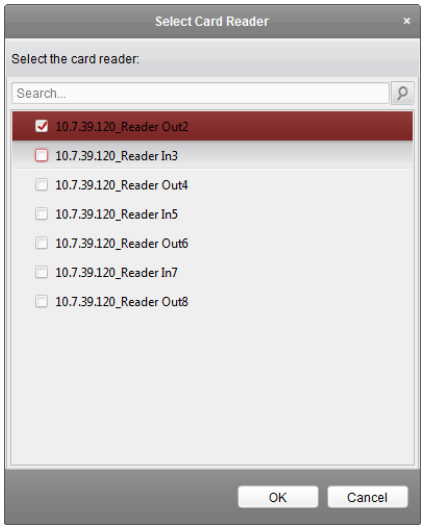
Steps:

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



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 Download Settings button to take effect of the new settings.

4.7.6 Multi-door Interlocking

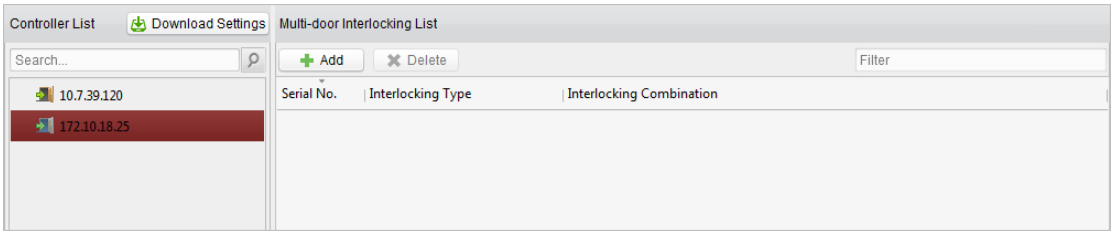
You can set the multi-door interlocking between multiple doors of the same access controller. To open one of the doors, other doors must keep closed. That means in the interlocking combined door group, up to one door can be opened at the same time.

Notes:

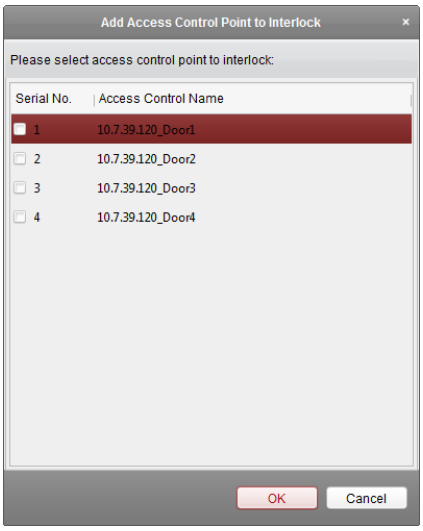
- The Multi-door Interlocking function is only supported by the access controller which has more than one access control points (doors).
- Either the anti-passing back or multi-door interlocking function can be configured for an access controller at the same time.

Steps:

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



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



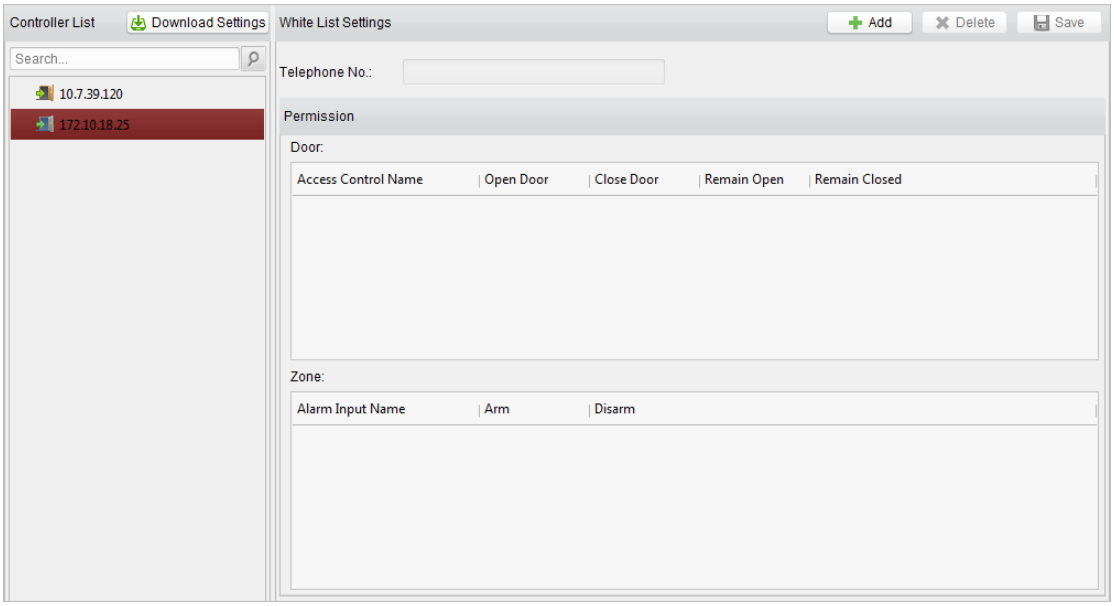
3. Select the access control point (door) from the list.
   Note: Up to four doors can be added in one multi-door interlocking combination.
4. Click **OK** to save the adding.
5. (Optional) After adding the multi-door interlocking combination, you can select it from the list and click Delete to delete 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.



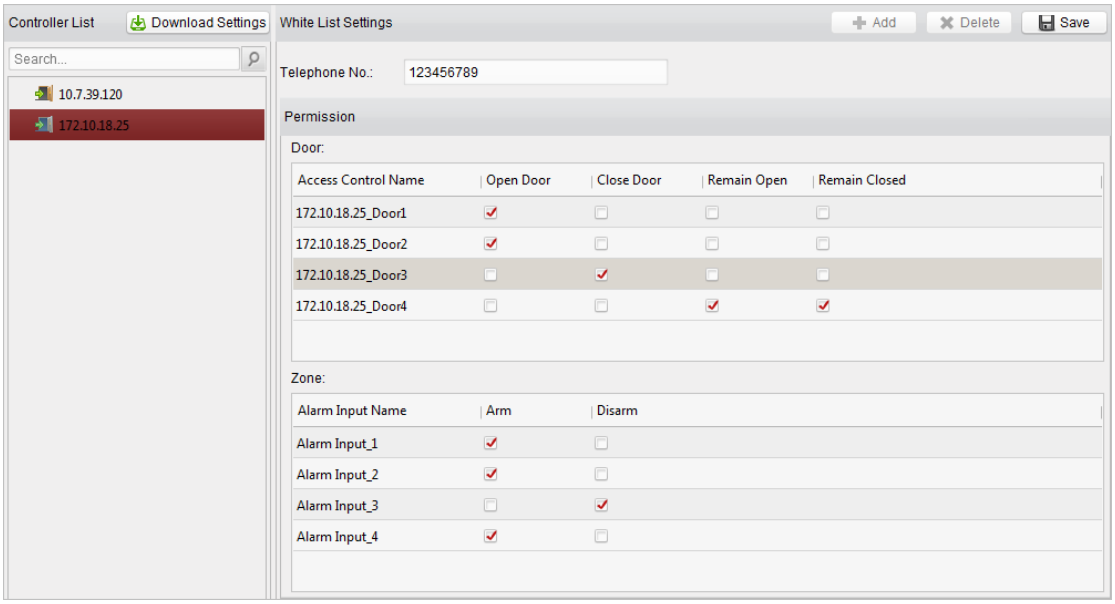
2. Select the access controller from the list and click **Add** button.
3. Input the mobile number.

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

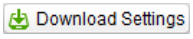
   Door: The mobile can control the door (open, closed, normally open, or normally closed).

   Zone: The mobile can arm and disarm the zone.

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



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

7. Click  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

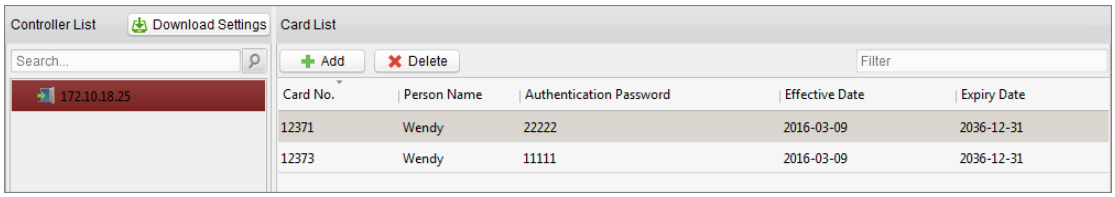
Purpose:

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

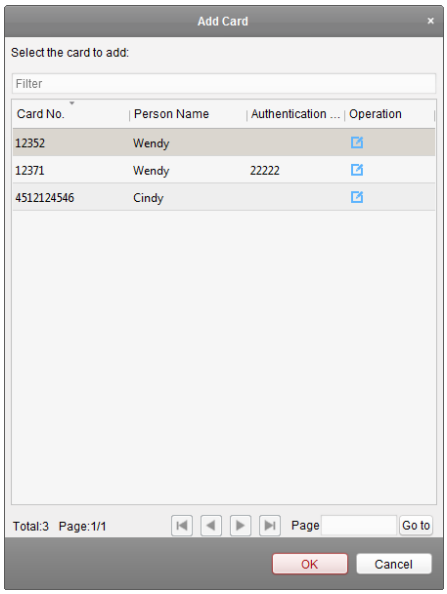
Note: This authentication password function is only valid during the schedules when the card reader authentication mode for the access controller is set as **Card or Authentication Password**. For details, please refer to *Chapter 4.7.2 Card Reader Authentication.*

Steps:

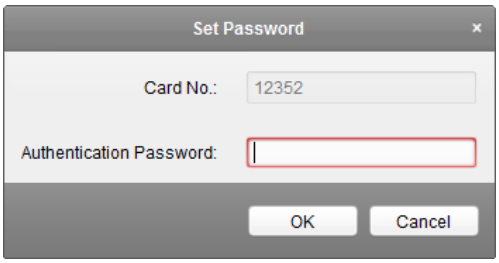
1. Click **Authentication Password** tab and select an access controller from the list.



2. Click **Add** button to enter card adding interface.



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



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.
5. (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  button to modify the authentication password.

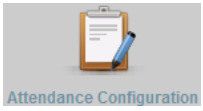
Note: Up to 500 cards with authentication password can be added to one access controller. The password should be unique and cannot be same with each other.

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 

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

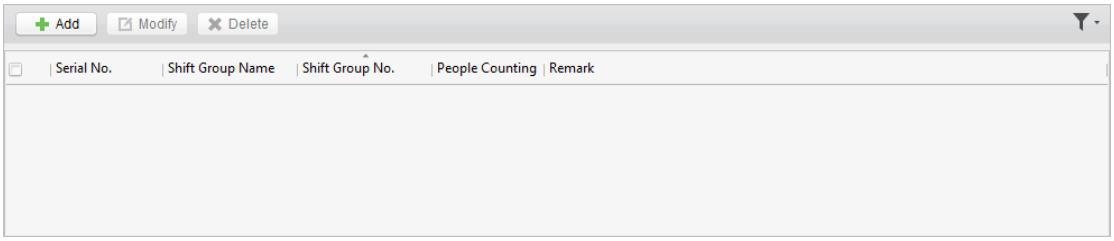
5.1.1 Shift Group Management

Purpose:

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

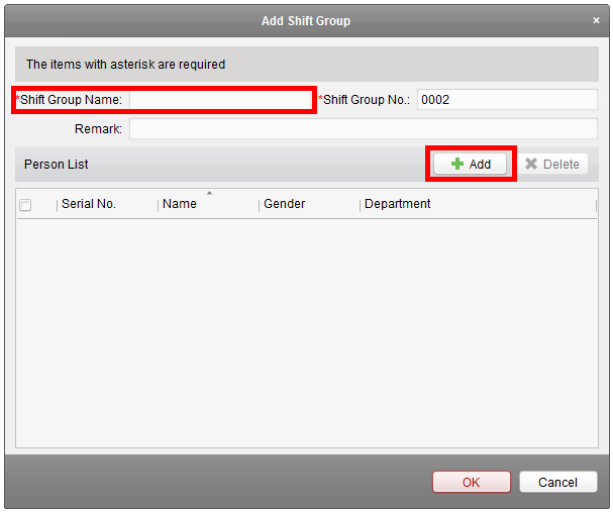
Steps:

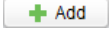
1. Click **Shift Group** tab to enter the following page.



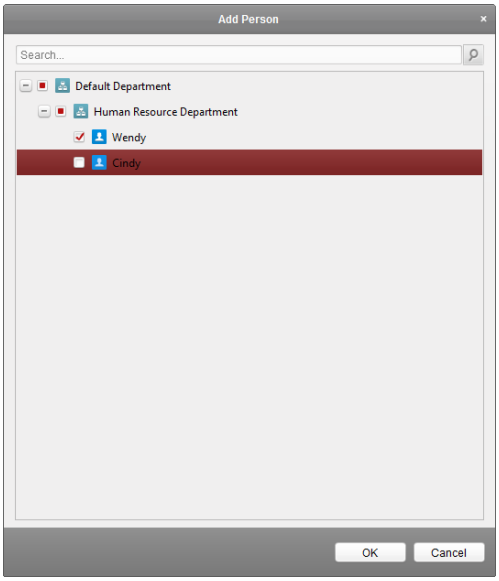
2. Click 

button to pop up the adding shift group window.



3. Enter the shift group name, and add 

button on the person list area to pop up the person adding window.



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

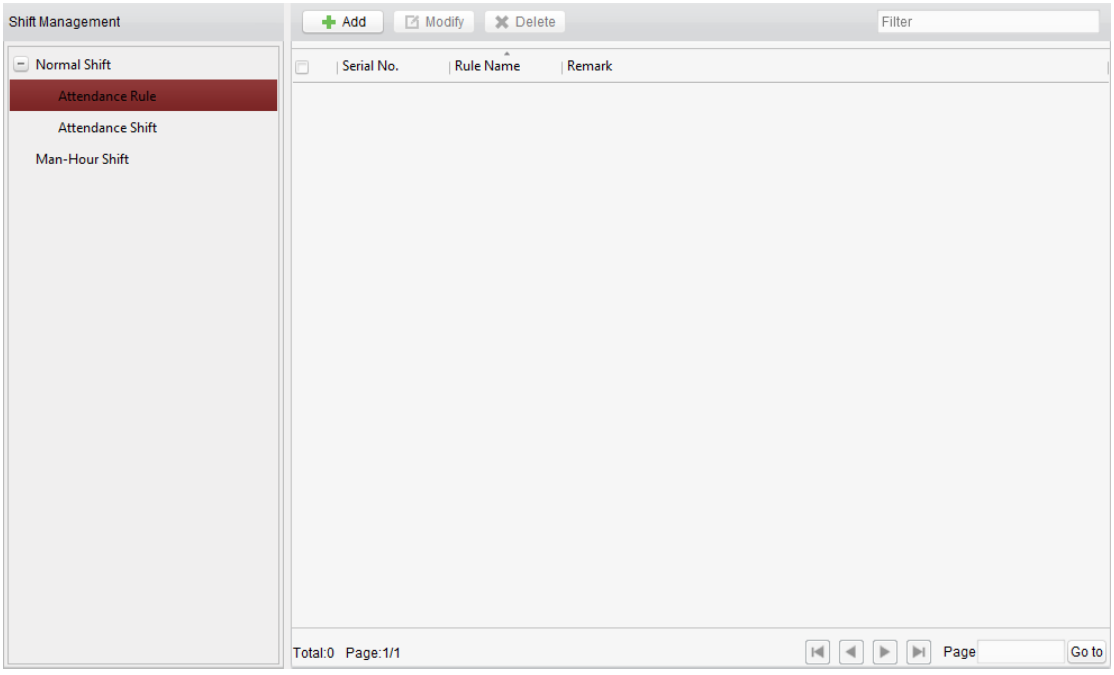
   To delete the added person, check the person from the person list, and click Delete button.
5. Click **OK** button to complete the operation.
6. You can edit or delete the added shift groups by clicking Modify or Delete button.

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 the shift management interface.



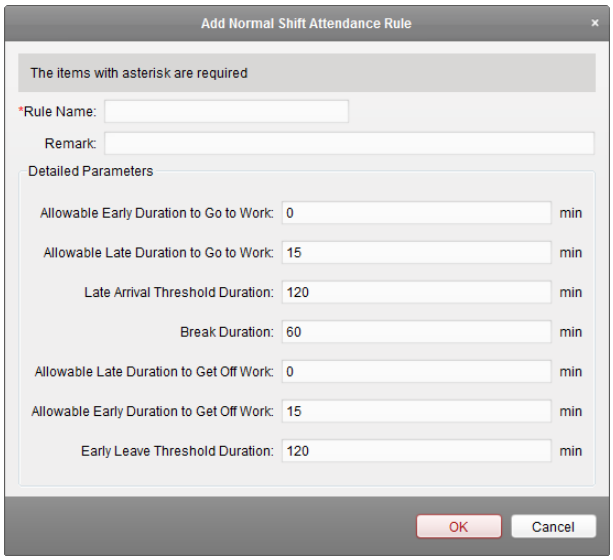
There are two kinds of shifts in this interface: **Normal Shift**, and **Man-Hour Shift**.

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.



3. Set a rule name.
4. Set detailed parameters for the attendance rule according to actual needs.
5. Click **OK** to save the rule.
6. (Optional) You can edit or delete the rule by clicking Modify or Delete button.

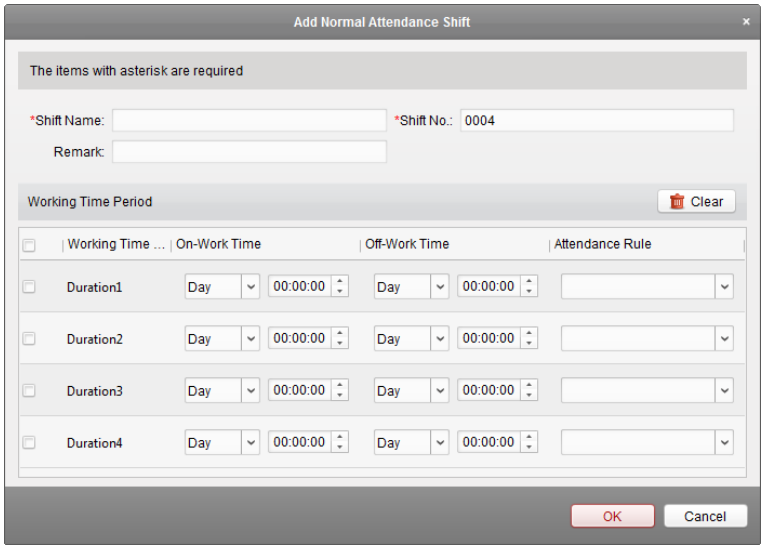
Notes:

- 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.

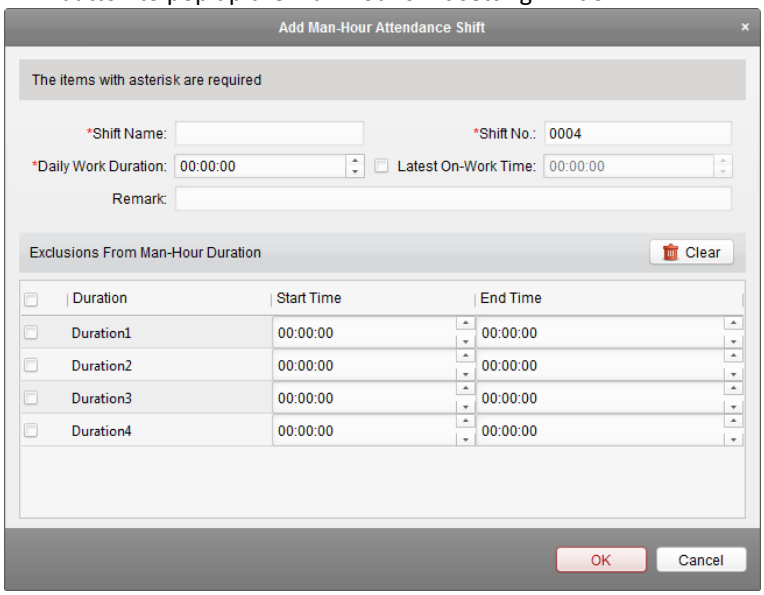


3. Set a shift name.
4. Set on-work duration for the shift, and select the attendance rule from the dropdown list.
5. Click **OK** button to complete the operation.
6. (Optional) You can edit or delete the shift by clicking Modify or Delete button.
   Note: After deleting the shift, its shift schedule 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.



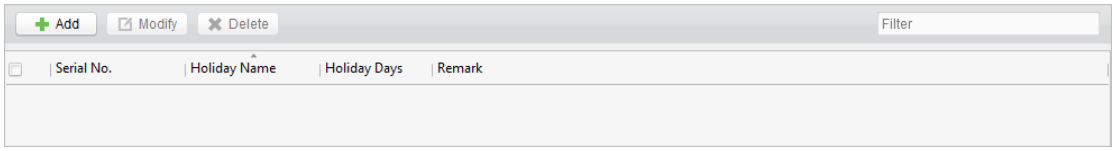
3. Set a shift name, and daily work duration.
4. (Optional) Check the checkbox of latest on-work time, and set the latest on-work time.
5. (Optional) Set the durations excluded from man-hour duration.
6. Click **OK** button to complete the operation.
7. (Optional) You can edit or delete the shift by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

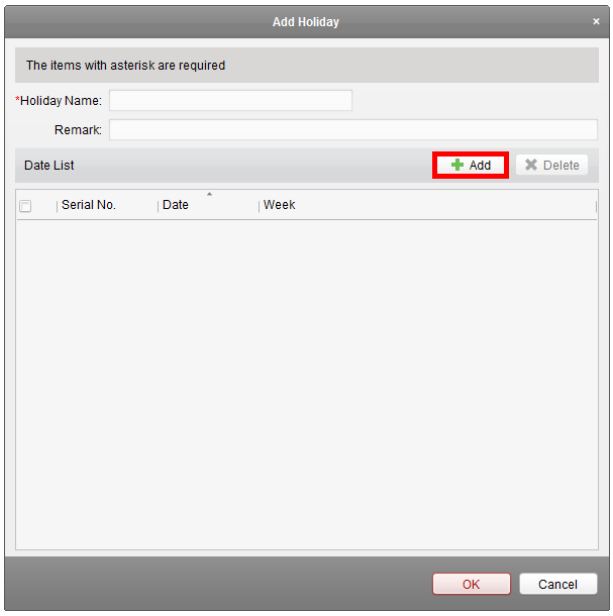
5.1.3 Holiday Management

Steps:

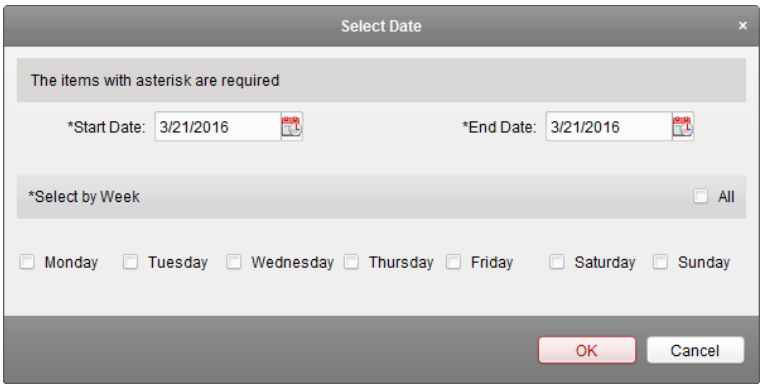
1. Click **Holiday** tab to enter the holiday management interface.



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



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



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

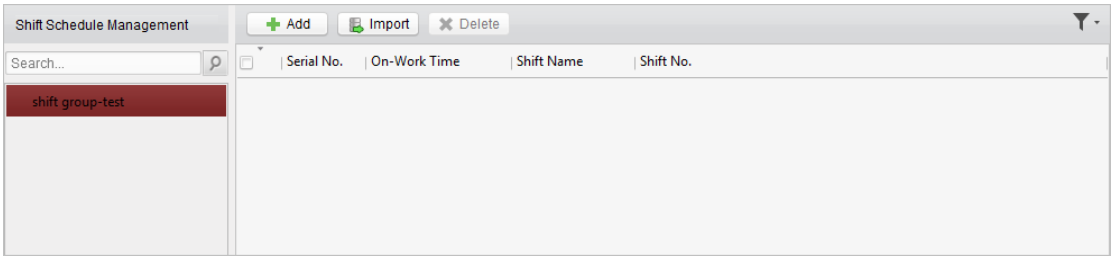
5.1.4 Shift Schedule Management

Purpose:

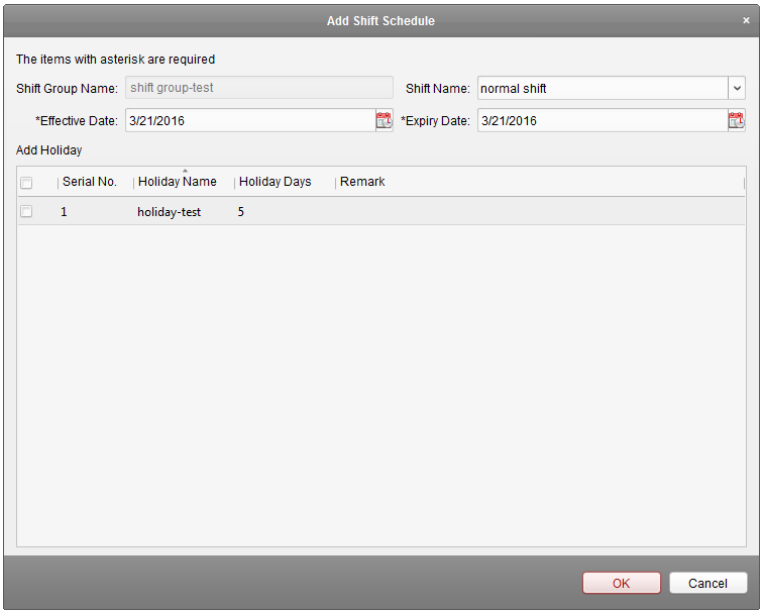
After setting the shift group and the corresponding shift and shift rule, you can set the shift schedule for the shifts.

Steps:

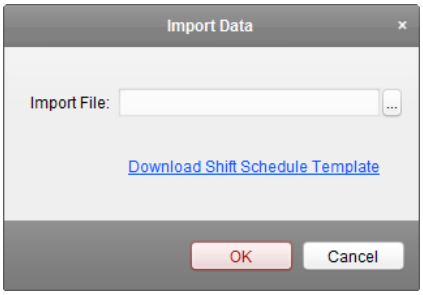
1. Click **Shift Schedule** tab to enter the shift schedule management interface.



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



4. 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.



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

Group No., Date, and Shift No. in the template.

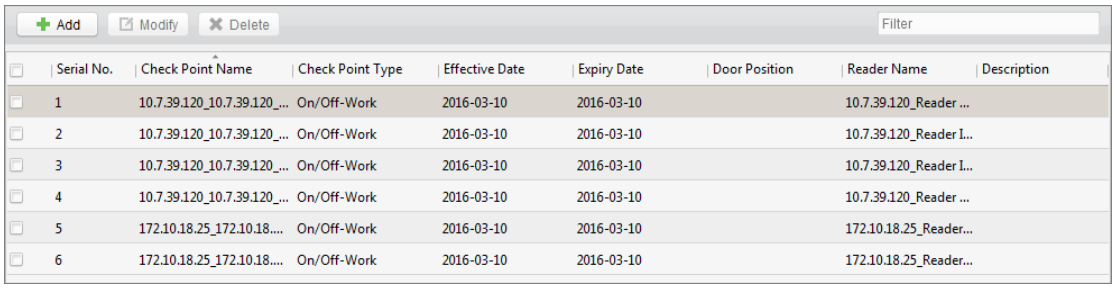
Click ... to select the file for importing

Click **OK** to start importing.

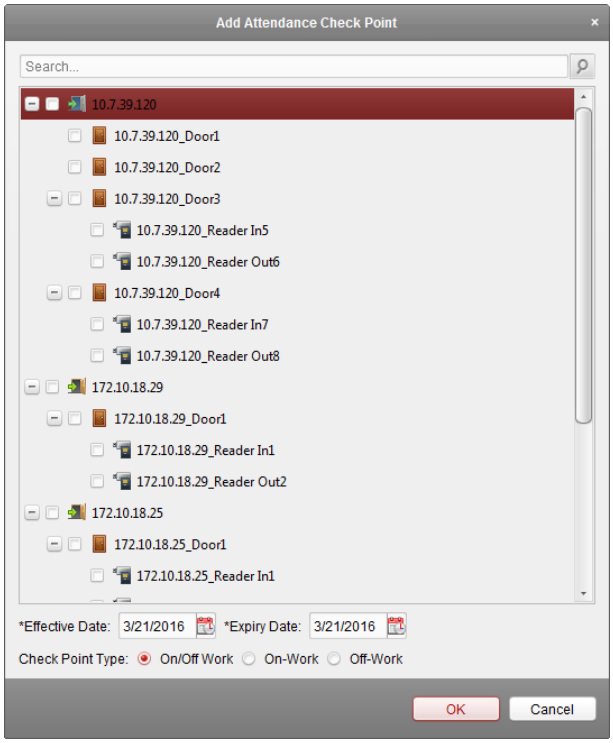
5.1.5 Attendance Check Point Management

Steps:

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



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.

3. You can check the checkbox of a check point, and click Modify button to pop up the 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 Delete 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.

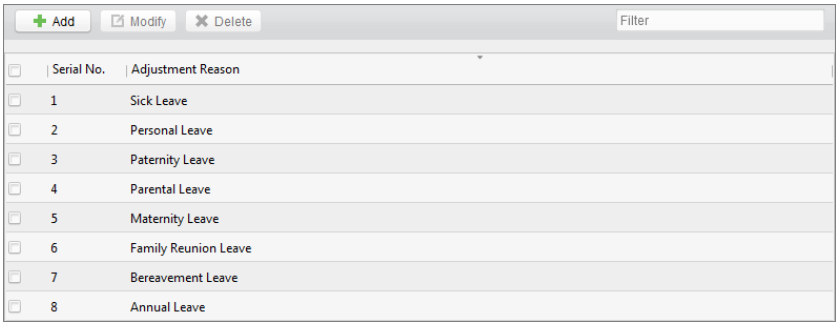
Reason Management

✧ **Leave**

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

Steps:

1. Click **Leave** tab to enter the leave interface.



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

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

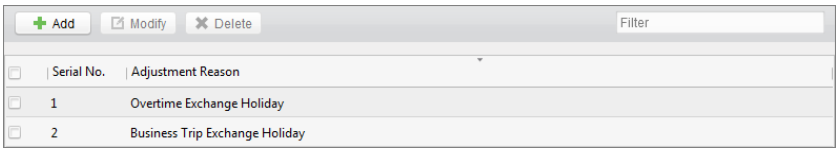
Notes:

- The default adjustment reasons include leave for personal affairs, sick leave, marriage leave, 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.

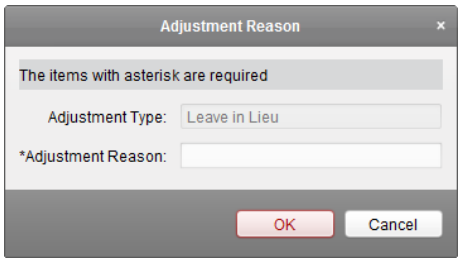
✧ **Leave in Lieu**

Steps:

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



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



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

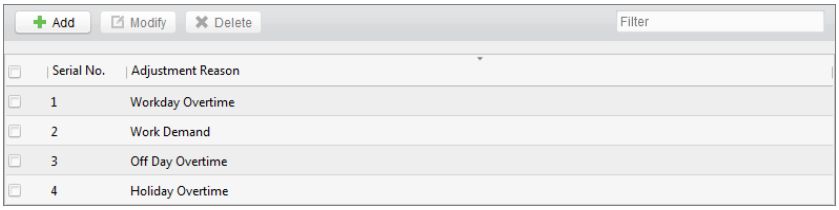
Notes:

- The default adjustment reasons for 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 Delete button to delete the reason.

✧ Overtime

Steps:

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



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

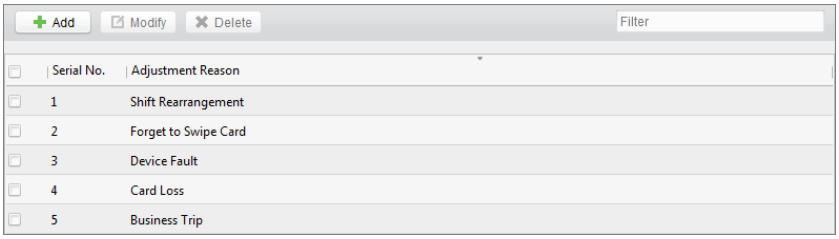
Notes:

- 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.



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 Modify button to edit the reason, and click

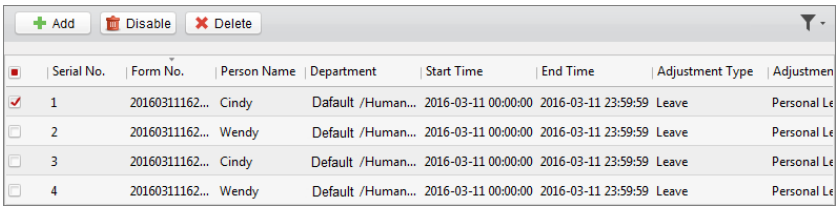
Delete button to delete the reason.

List Management

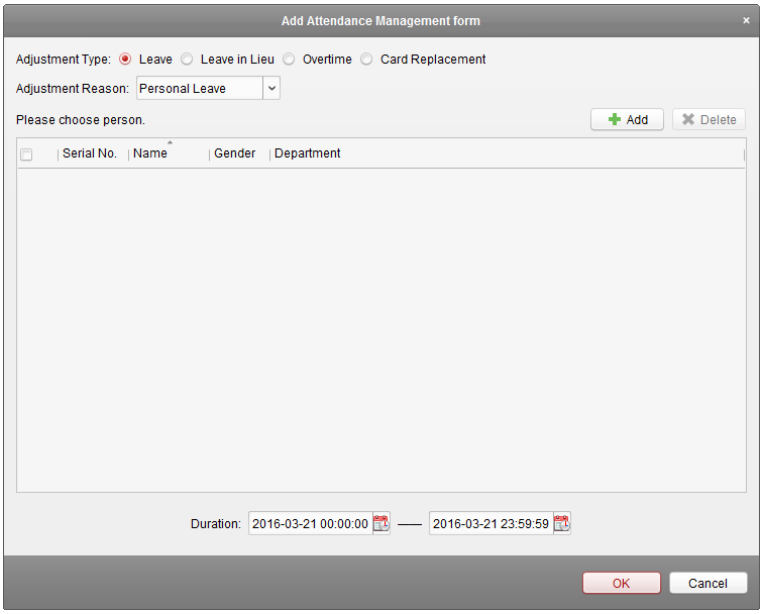
✧ **Enabled List**

Steps:

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



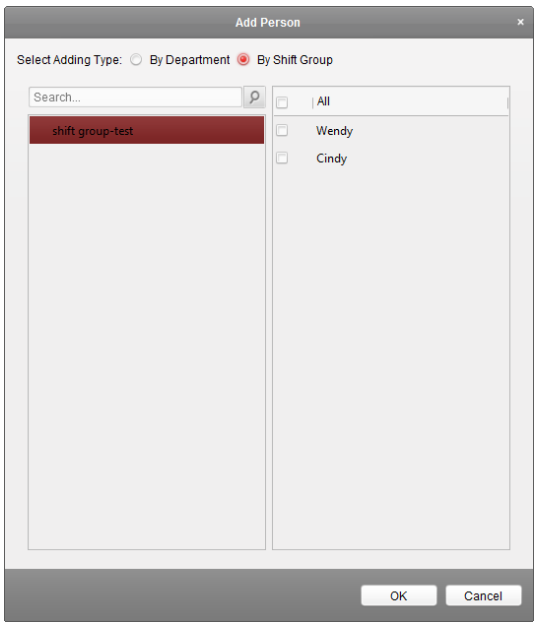
2. Click Add button to add an attendance management form.



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.



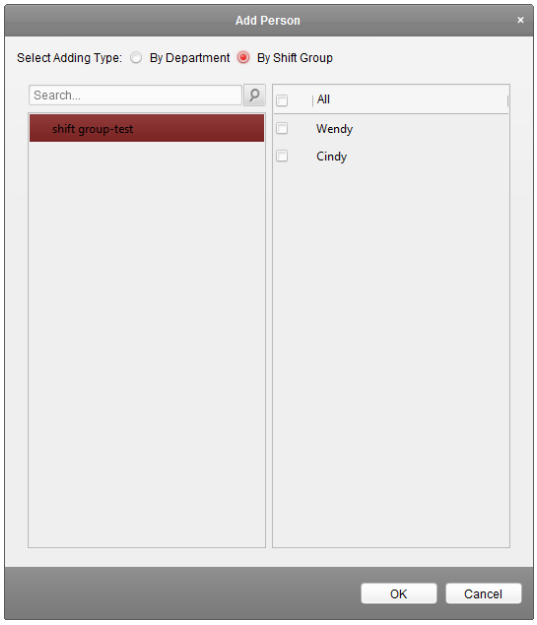
3) Select the adding type as by department or by shift group. Select the person and click **OK** button.

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.



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

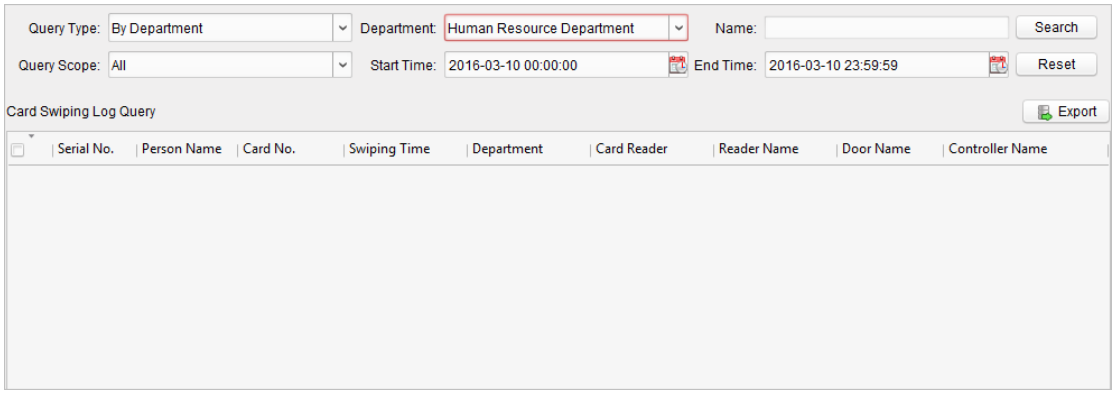
button to disable the list.

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

3. You can check the checkbox and click Delete 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.



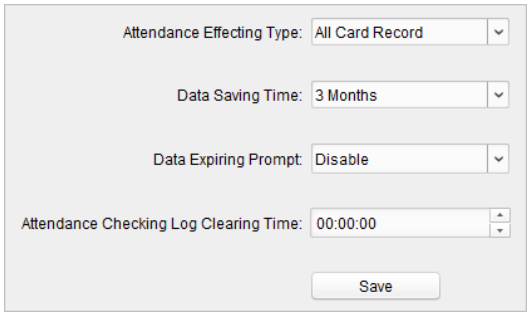
You can search the card swiping log by two query types: **By Shift Group**, and **By Department**.

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.

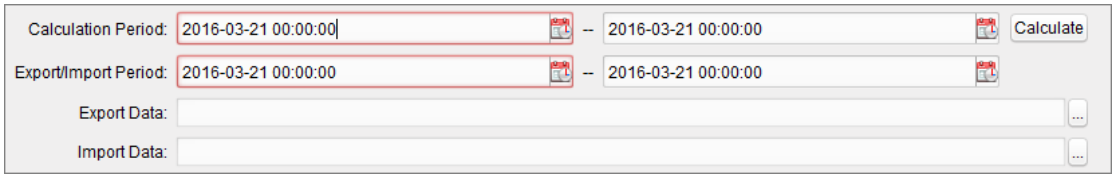


2. Select the attendance effecting type, data saving time, data expiring prompt.
3. Set the attendance checking log clearing time.
4. Click **Save** to save the parameters.

5.1.9 Data Management

Steps:

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



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 

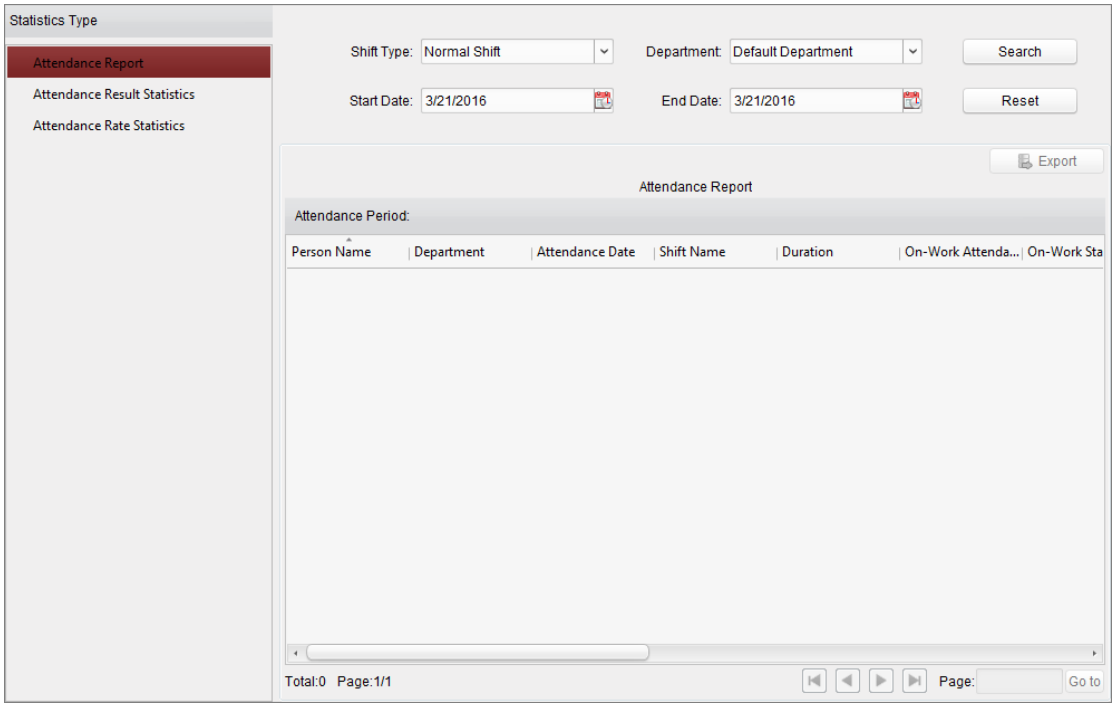
icon on the control panel to enter the Attendance Statistics interface.

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.



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.

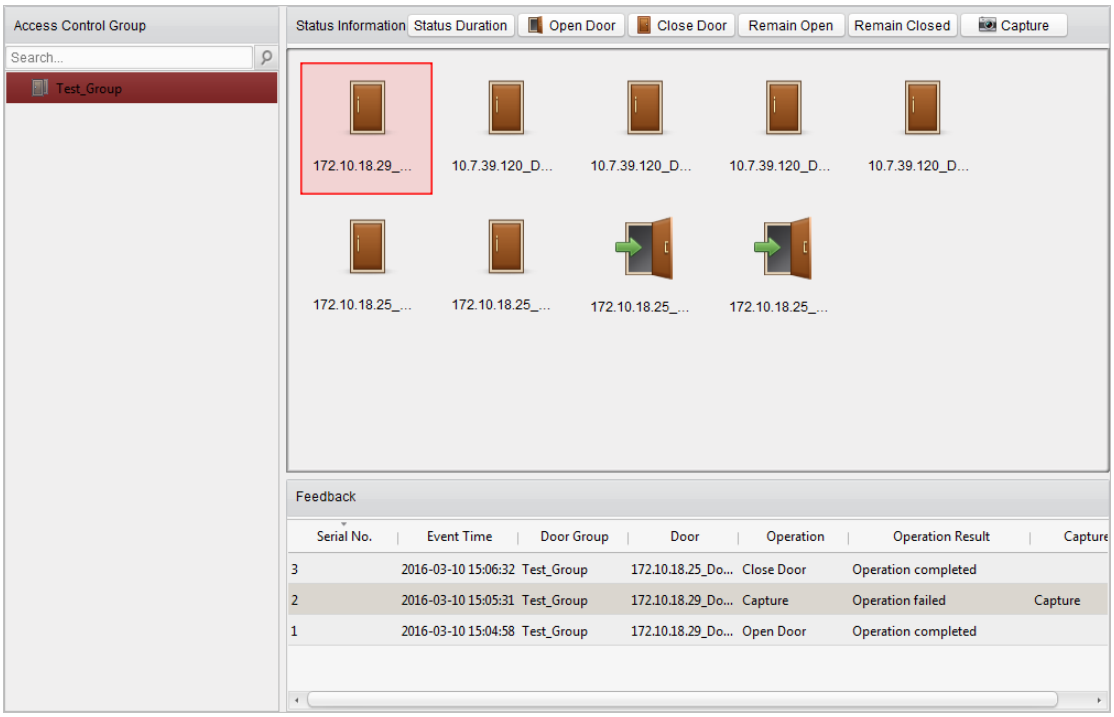
6.1 Status Monitor

Purpose:

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

Click 

icon on the control panel to enter the interface.



6.1.1 Anti-control the Access Control Point (Door)

Purpose:

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

Steps:

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.

Click icon  on the Status Information panel to select a door.

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.

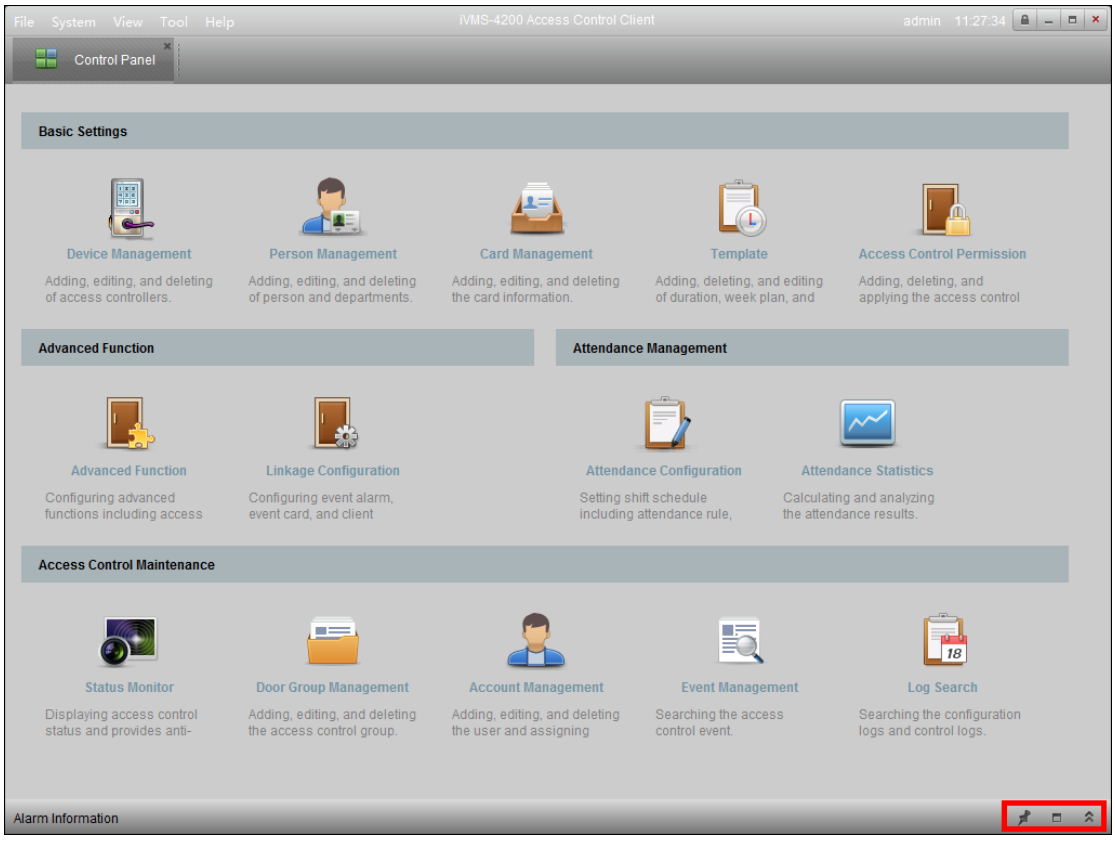
4. You can view the anti-control operation result in the Operation Log panel.

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  in Alarms and Events Toolbar to show the Alarms and Events panel. Or click  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.

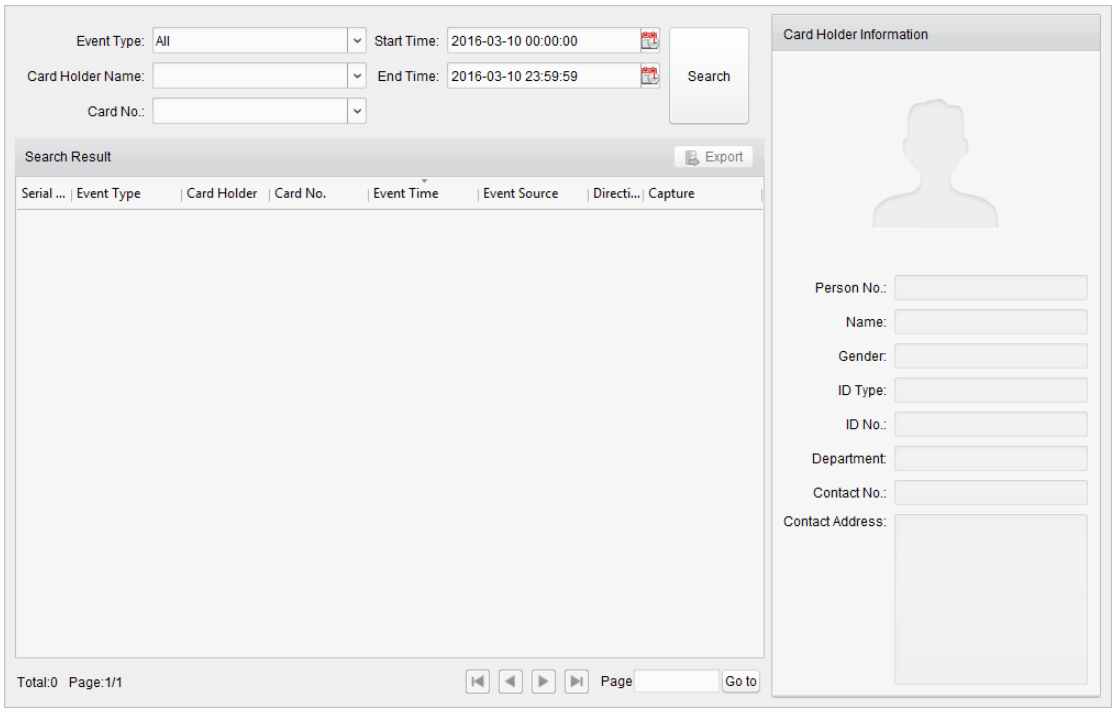
6.3 Event Management

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 

icon on the control panel to enter the interface.



Steps:

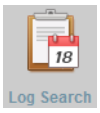
1. Enter the search condition (event type/card holder name/card No./start&end time).
2. Click **Search** to get the search results.
3. View the event information in the event list.
4. Click an event to view the information of the card holder on the **Card Holder Information** panel on the left side of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

Chapter 7 System Maintenance

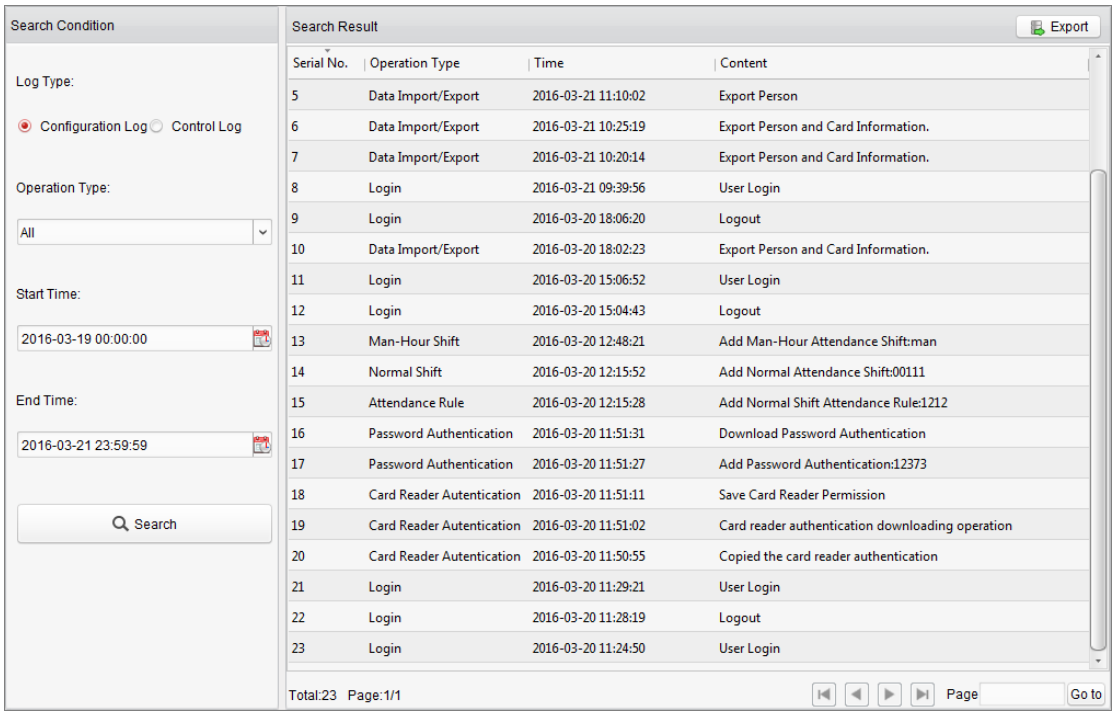
7.1 Log Management

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 

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



7.1.1 Searching Configuration Logs

Purpose:

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

Steps:

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.
5. 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.
5. 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.

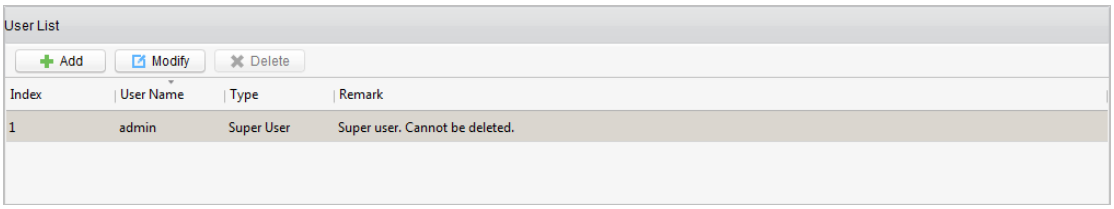
7.2 Account Management

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 

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



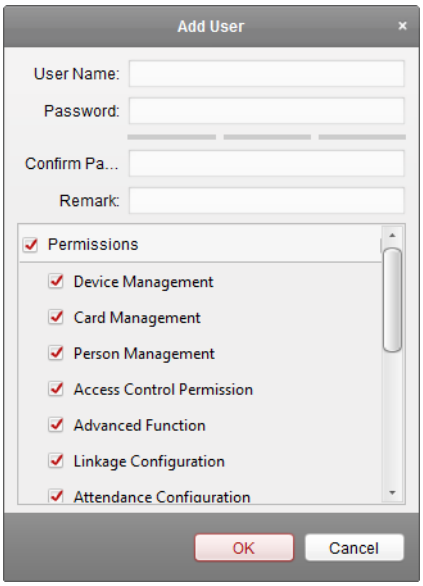
Note: The user account you registered to log in to the software is set as the super user.

Adding the User

Steps:

1. Open the Account Management page.
2. Click 

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.



- *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

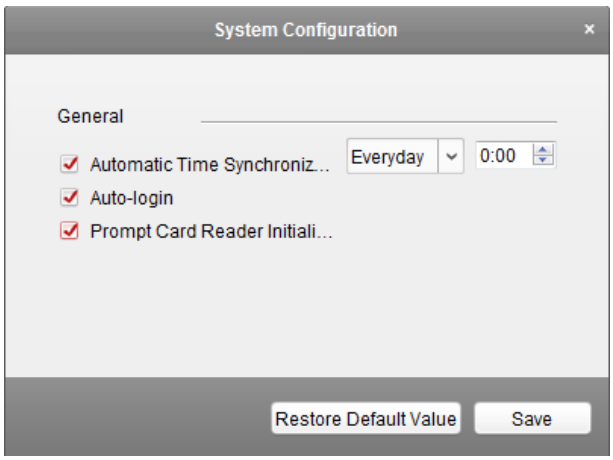
Purpose:

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.



2. 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

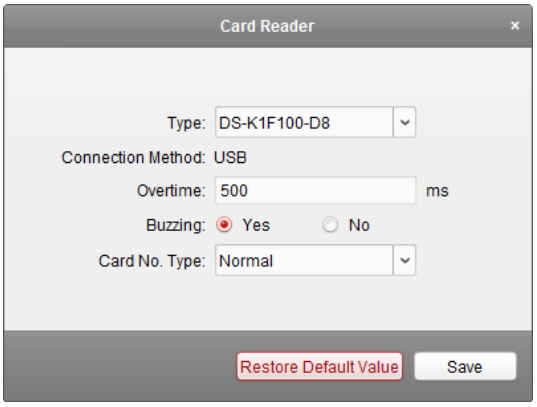
Purpose:

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.



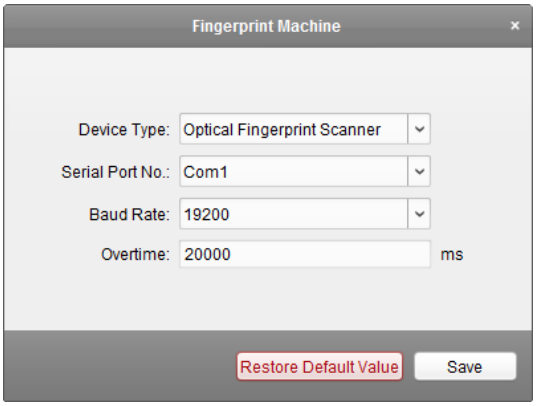
2. Set the parameters about the connected card reader.
3. Click **Save** button to save the settings.
   You can click **Restore Default Value** button to restore the defaults.

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.



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:

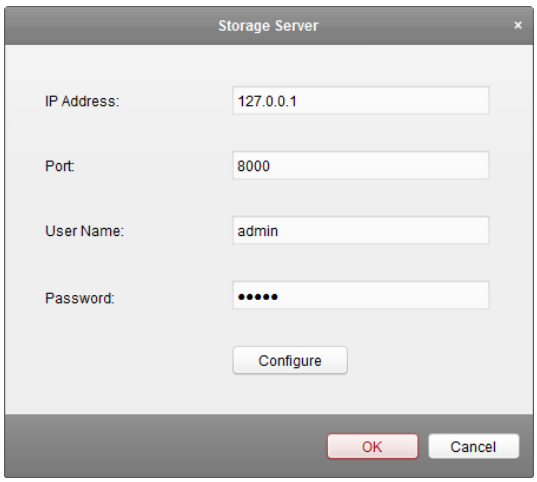
- It is supported using device type as Optical Fingerprint Scanner and Capacitive Fingerprint Scanner.
- The serial port number should correspond to the serial port number of PC.
- The baud rate should be set according to the external fingerprint card reader. The default value is 19200.
- Overtime refers 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

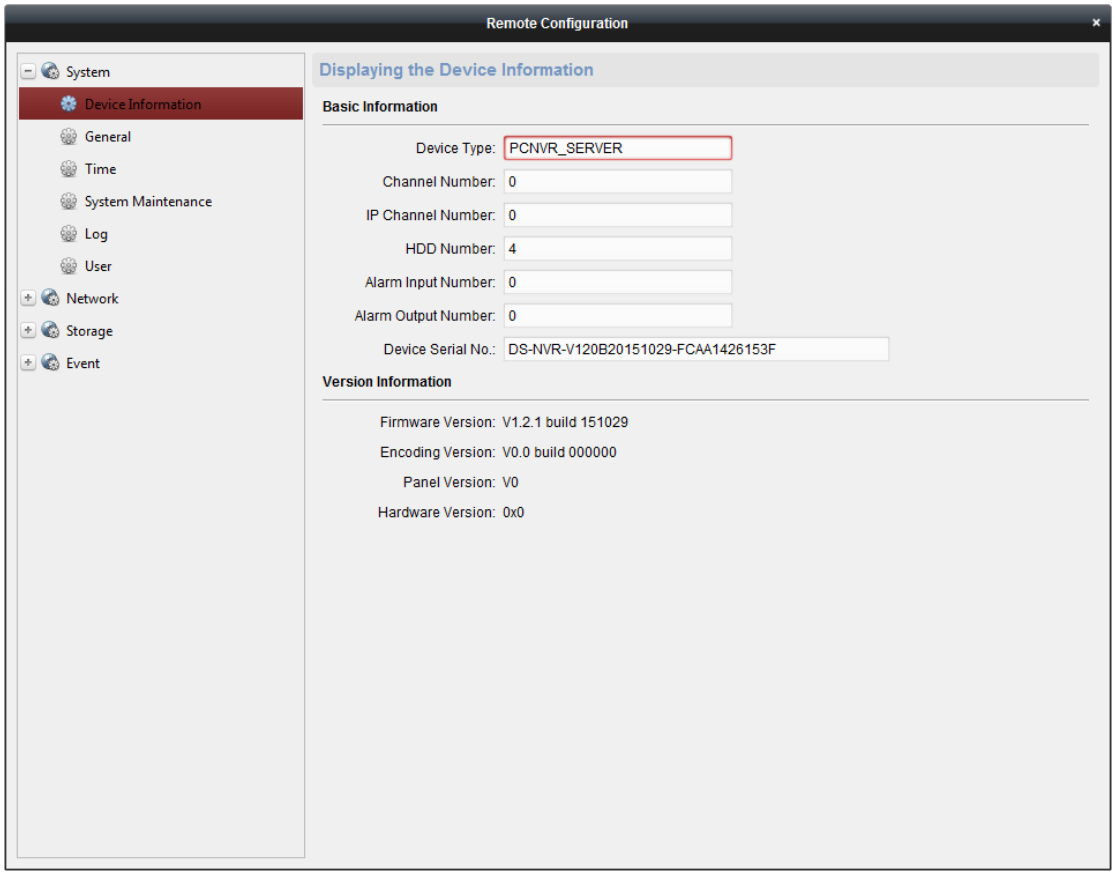
You should configure the storage server before capturing the pictures for the storage of captured pictures.

Steps:

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

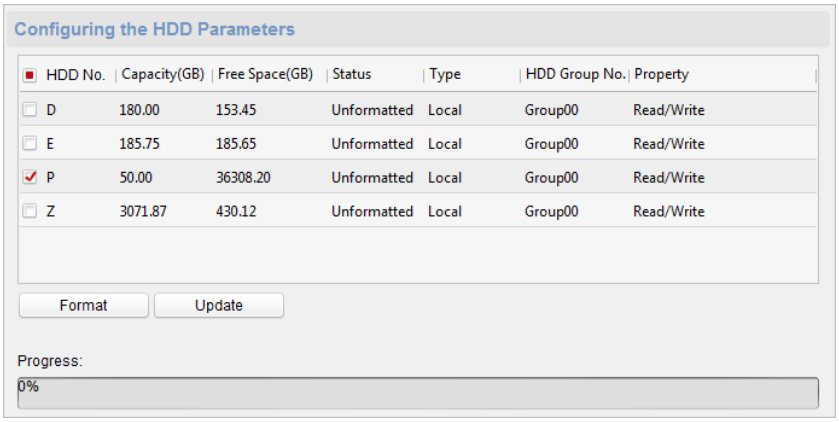


2. Input the storage server parameters including IP address, port No., user name, and password.
3. Click **Configure** button to enter the Remote Configuration interface as follows.

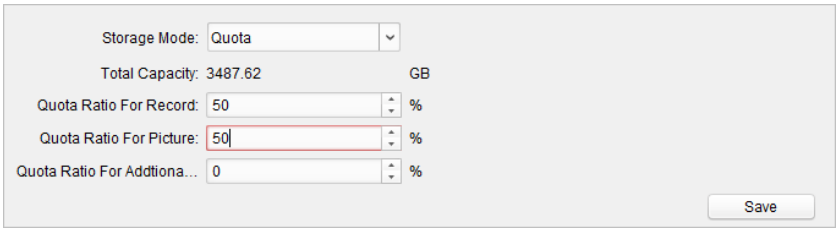


4. The HDDs of the storage server need to be formatted for the video file and picture storage.
   1) Click **Storage**->**General**, to enter the HDD Formatting interface.
   2) Select the HDD from the list and click **Format**. You can check the formatting process from the process bar and the status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



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



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.