iVMS-4200 AC Client Software

User Manual

Legal Information

User Manual

About this Manual

This Manual is subject to domestic and international copyright protection. Hangzhou Hikvision Digital Technology Co., Ltd. ("Hikvision") reserves all rights to this manual. This manual cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision.
Please use this user manual under the guidance of professionals.

Trademarks

HIKVISION and other Hikvision marks are the property of Hikvision and are registered trademarks or the subject of applications for the same by Hikvision and/or its affiliates. Other trademarks mentioned in this manual are the properties of their respective owners. No right of license is given to use such trademarks without express permission.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THIS MANUAL. HIKVISION DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE OF THE MANUAL, OR THE CORRECTNESS, ACCURACY, OR RELIABILITY OF INFORMATION CONTAINED HEREIN. YOUR USE OF THIS MANUAL AND ANY RELIANCE ON THIS MANUAL SHALL BE WHOLLY AT YOUR OWN RISK AND RESPONSIBILITY.
REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION 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. HIKVISION 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.

Port List

For more details about port list, enter Hikvision official website.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
⚠ **Danger**	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
⚠ **Caution**	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
ℹ **Note**	Provides additional information to emphasize or supplement important points of the main text.

Contents

Chapter 1 Introduction

The software provides multiple functionalities, including person management, access control, video intercom, time & attendance, etc., for the connected devices to meet the needs of monitoring task. With the flexible distributed structure and easy-to-use operations, the client software is widely applied to the surveillance projects of medium or small scale.

This user manual describes the functions, configurations and operation steps of the client software. To ensure the properness of usage and stability of the software, refer to the contents below and read the manual carefully before installation and operation.

Chapter 2 Service Management

iVMS-4200 AC Service is mainly applicable for data storage, data management, and data calculation. With continuous running and processing, it can manage the data, such as event records and attendance records, received by the iVMS-4200 AC Client Software. iVMS-4200 AC Service also provides management for user permissions, devices, groups, logs, etc.

You can view the module running status and edit its ports, including HTTP port and EHome port. You need to restart the iVMS-4200 AC Service to take effect.

Check **Auto-Launch** to enable launching the iVMS-4200 AC Service automatically after the PC started up.

Note

- The iVMS-4200 AC Service will not show after running it. Enter the system tray and click △ to open the service window.
- After closing the service window, the client will logout and return to the login page. You need to run the service and then login again.
- The service and the client should be installed on the same PC.

Chapter 3 Device Management

You can manage devices on the client, including adding, editing, and deleting the devices. You can also perform operations such as checking device status.

3.1 Add Device

After running the client, devices including access control devices, video intercom devices, etc., should be added to the client for the remote configuration and management, such as controlling door status, attendance management, event settings, etc.

3.1.1 Activate Devices

For some devices, you are required to create the password to activate them before they can be added to the software and work properly.

Steps

Note

This function should be supported by the device.

1. Enter the Device Management page.
2. Click **Online Device** to show the online device area.

   The searched online devices are displayed in the list.
3. Check the device status (shown on **Security Level** column) and select an inactive device.
4. Click **Activate** to open the Activation dialog.
5. Create a password in the password field, and confirm the password.

   Caution

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.
   Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
6. Click **OK** to activate the device.

3.1.2 Add Online Device

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

Add Single Online Device

You can add single online device to the client software.

Steps

1. Enter the Device Management module.
2. Click **Online Device** to show the online device area.

   The searched online devices are displayed in the list.
3. Select an online device from the **Online Device** area.

   Note

   For the inactive device, you need to create the password for it before you can add the device properly. For detailed steps, refer to ***Activate Devices*** .
4. Click **Add** to open the device adding window.
5. Enter the required information.

   Name

   Enter a descriptive name for the device.

   Address

   The IP address of the device is obtained automatically in this adding mode.

   Port

   The port number is obtained automatically.

   User Name

   By default, the user name is admin.

   Password

   Enter the device password.

   Caution

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

6. **Optional:** Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. **Optional:** Check **Import to Group** to create a group by the device name.

Note

You can import all the channels of the device to the corresponding group by default.

8. Click **OK** to add the device.

Add Multiple Online Devices

You can add multiple online devices to the client software.

Steps

1. Enter the Device Management module.
2. Click **Online Device** to show the online device area.

   The searched online devices are displayed in the list.
3. Select multiple devices.

Note

For the inactive device, you need to create the password for it before you can add the device properly. For detailed steps, refer to ***Activate Devices*** .

4. Click **Add** to open the device adding window.
5. Enter the required information.

User Name

By default, the user name is admin.

Password

Enter the device password.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

6. **Optional:** Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the devices to the client.
7. **Optional:** Check **Import to Group** to create a group by the device name.

Note

You can import all the channels of the device to the corresponding group by default.

8. Click **OK** to add the devices.

3.1.3 Add Device by IP Address or Domain Name

When you know the IP address or domain name of the device to add, you can add devices to the client by specifying the IP address (or domain name), user name, password, etc.

Steps

1. Enter Device Management module.
2. Click **Device** tab on the top of the right panel.

   The added devices are displayed on the right panel.
3. Click **Add** to open the Add window, and then select **IP/Domain** as the adding mode.
4. Enter the required information.

   Name

   Create a descriptive name for the device. For example, you can use a nickname that can show the location or feature of the device.

   Address

   The IP address or domain name of the device.

   Port

   The devices to add share the same port number. The default value is ***8000***.

   User Name

   Enter the device user name. By default, the user name is ***admin***.

   Password

   Enter the device password.

   Caution

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. **Optional:** Check **Transmission Encryption (TLS)** to enable transmission encryption using TLS (Transport Layer Security) protocol for security purpose .

Note

- This function should be supported by the device.
- You can log into the device to get the certificate file by web browser.

6. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. **Optional:** Check **Import to Group** to create a group by the device name.
8. Finish adding the device.
   - Click **Add** to add the device and back to the device list page.
   - Click **Add and New** to save the settings and continue to add other device.
9. **Optional:** Perform the following operation(s).

Remote Configuration

Click ⚙ on Operation column to set remote configuration of the corresponding device.

Note

For detail operation steps for the remote configuration, see the user manual of the device.

Device Status

Click ▤ on Operation column to view device status, including cameras, recording status, signal status, hardware status, etc.

Edit Device Information

Click ✎ on Operation column to edit the device information, such as IP address, user name, and password.

Check Online User

Click 👤 on Operation column to check the online users who access the device, such as user name, user type, user's IP address, and login time.

Refresh

Click ⟳ on Operation column to get the latest device information.

Delete Device

Select one or multiple devices and click **Delete** to delete the selected device(s) from the client.

3.1.4 Add Devices by IP Segment

If the devices share the same port No., user name and password, and their IP addresses are sharing an IP segment. You can specify the start IP address and the end IP address, port No., user name, password, etc of the devices to add them to the client.

Steps

1. Enter the Device Management module.
2. Click **Device** tab on the top of the right panel.

   The added devices are displayed on the right panel.
3. Click **Add** to open the Add window.
4. Select **IP Segment** as the adding mode.
5. Enter the required information.

   Start IP

   Enter a start IP address.

   End IP

   Enter an end IP address in the same network segment with the start IP.

   Port

   Enter the device port No. The default value is ***8000***.

   User Name

   By default, the user name is ***admin***.

   Password

   Enter the device password.

   ⚠ **Caution**

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.
   Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
6. **Optional:** Check **Transmission Encryption (TLS)** to enable transmission encryption using TLS (Transport Layer Security) protocol for security purpose .

   Note

   - This function should be supported by the device.
   - You can log into the device to get the certificate file by web browser.

7. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
8. **Optional:** Check **Import to Group** to create a group by the device name.
9. Finish adding the device.
   - Click **Add** to add the device and back to the device list page.
   - Click **Add and New** to save the settings and continue to add other device.
10. **Optional:** Perform the following operation(s).

Remote Configuration

Click ⚙ on Operation column to set remote configuration of the corresponding device.

> **Note**
>
> For detail operation steps for the remote configuration, see the user manual of the device.

Device Status

Click ▤ on Operation column to view device status, including cameras, recording status, signal status, hardware status, etc.

Edit Device Information

Click ✎ on Operation column to edit the device information, such as IP address, user name, and password.

Check Online User

Click 👤 on Operation column to check the online users who access the device, such as user name, user type, user's IP address, and login time.

Refresh

Click ⟳ on Operation column to get the latest device information.

Delete Device

Select one or multiple devices and click **Delete** to delete the selected device(s) from the client.

3.1.5 Add Device by EHome Account

For areas where devices using dynamic IP addresses instead of static ones, you can add access control device connected via EHome protocol by specifying the EHome account.

Before You Start

Set the network center parameter first. For details, refer to ***Set Network Parameters*** .

Steps

1. Enter Device Management module.

   The added devices are displayed on the right panel.
2. Click **Add** to open the Add window.
3. Select **EHome** as the adding mode.
4. Enter the required information.

   Device Account

      Enter the account name registered on EHome protocol.

EHome Key

Enter the EHome key if you have set it when configuring network center parameter for the device.

Note

This function should be supported by the device.

5. **Optional:** Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
6. **Optional:** Check **Import to Group** to create a group by the device name.
7. Finish adding the device.
   - Click **Add** to add the device and go back to the device list.
   - Click **Add and New** to save the settings and continue to add other device.
8. **Optional:** Perform the following operation(s).

Device Status	Click ▤ on Operation column to view device status.
Edit Device Information	Click ✎ on Operation column to edit the device information, such as device name, device account, and EHome key.
Check Online User	Click 👤 on Operation column to check the online users who access the device, such as user name, user type, user's IP address, and login time.
Refresh	Click ⟳ on Operation column to get the latest device information.
Delete Device	Select one or multiple devices and click **Delete** to delete the selected device(s) from the client.

3.1.6 Import Devices in a Batch

The devices can be added to the software in a batch by entering the device information in the pre-defined CSV file.

Steps

1. Enter the Device Management page
2. Click **Add** to open the adding device window.
3. Select **Batch Import** as the adding mode.
4. Click **Export Template** and then save the pre-defined template (CSV file) on your PC.
5. Open the exported template file and enter the required information of the devices to be added on the corresponding column.

Adding Mode

You can enter ***0*** or ***1*** which indicated different adding modes. ***0*** indicates that the device is added by IP address or domain name; ***1*** indicates that the device is added via EHome.

Address

Edit the address of the device. If you set ***0*** as the adding mode, you should enter the IP address or domain name of the device; if you set ***1*** as the adding mode, this filed is not required.

Port

Enter the device port No. The default value is 8000.

Device Information

If you set ***0*** as the adding mode, this field is not required. If you set ***1*** as the adding mode, enter the EHome account.

User Name

Enter the device user name. By default, the user name is admin.

Password

If you set ***0*** as the adding mode, enter the password. If you set ***1*** as the adding mode, enter the EHome key.

⚠ **Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

Import to Group

You can enter ***1*** to create a group by the device name. All the channels of the device will be imported to the corresponding group by default. ***0*** indicates disabling this function.

6. Click ⋯ and select the template file.
7. Click **Add** to import the devices.

3.2 Edit Device's Network Information

After activating device, you can edit the network information (including IP address, port number, gateway, etc.) for the online device.

Before You Start

Activate the device if the device status is inactivated.

Steps

1. Enter Device Management page.
2. Click **Device** tab on the top of the right panel.

3. Click **Online Device** to show the online device area.

   All the online devices sharing the same subnet will be displayed in the list.
4. Select an activated device in **Online Device** area.
5. Click on the Operation column to open the Modify Network Parameter window.

   Note

   This function is only available on the **Online Device** area.
6. **Optional:** Change the device IP address to the same subnet with your computer if you need to add the device to the client.
   - Edit the IP address manually.
   - Check **DHCP** to set the IP address as a static IP address.
7. Enter the password created when you activate the device.

   Caution

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.
   Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
8. Click **OK** to complete the network settings.

3.3 Reset Device Password

If you forgot the password of the detected online devices, you can reset the device password through the client.

Steps

1. Enter Device Management page.
2. Click **Online Device** to show the online device area.

   All the online devices in the same subnet will display in the list.
3. Select the device from the list and click on the Operation column.
4. Click **Export** to save the device file on your PC and then send the file to our technical support.

   Note

   For the following operations for resetting the password, contact our technical support.

⚠ **Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

3.4 Upgrade Device Firmware Version

When there is a new firmware version available for the added device, you can upgrade its firmware version via the client.

Note

- The device should support this function.
- You can configure upgrading mode in System Configuration. See ***Set General Parameters*** for details.

Enter the Device Management module, and then click **Device** tab to show the device list.

Perform the following operations according to different upgrading modes.

Disable

On the Device for Management panel, if there is a new firmware version available, the status in the Firmware Upgrade column of the device will turn to **Upgradeable**.
Select the upgradeable device and click **Upgrade** to start upgrading the device firmware.

Note

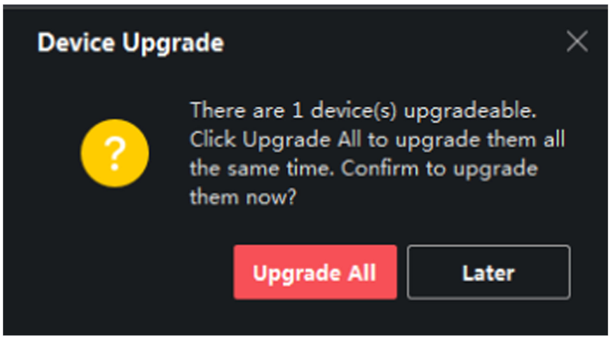
The upgrade progress will show. When the upgrade is completed, the status in the Firmware Upgrade column of the device will turn to **Upgraded**.

Prompt Me If Download and Upgrade

If there is a new firmware version available, a prompt window will pop up. Click **Upgrade All** to start downloading and upgrading.

Download and Prompt Me If Upgrade

A dialog will pop up for selecting whether to upgrade after downloading package of new version. Click **Upgrade All** to start upgrading the device firmware.



Device Upgrade

There are 1 device(s) upgradeable. Click Upgrade All to upgrade them all the same time. Confirm to upgrade them now?

Figure 3-1 Device Upgrade Prompt

Note

After clicking **Upgrade All**, a prompt will pop up for viewing details. If you are not in Device Management page, click **View Details** to jump to Device Management page; if you are in Device Management page, close the prompt.

Download and Update Automatically

After the client detects the new version of the devices, it will download the new version and upgrade the new version without noticing the user.

On the device management page, the following updating status will be shown in the Firmware Update column.

No Available Version

No new firmware version available.

Upgradeable

A new firmware version available.

Note

Move the cursor on ⓘ to view the current version, latest version, and upgrade content of the firmware version.

Waiting

The device is waiting for upgrade.

Downloading

The client is downloading the package of the new firmware version.

Upgrading

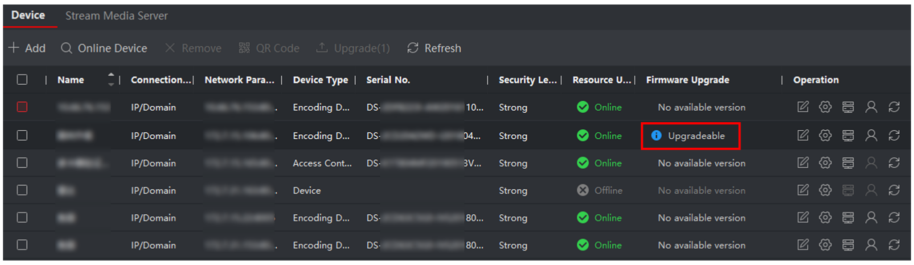
The upgrading of the device firmware is going on.

Upgraded

Hover the cursor on **Upgraded** to show the version after upgrading.

Upgrading Failed

When the upgrade fails, a prompt will pop up for viewing details. If you are not in Device Management page, click **View Details** to jump to Device Management page; if you are in Device Management page, close the prompt. Hover the cursor on **Upgrading Failed** to show the error details, and click **Upgrade Again** to try again.



□	Name	Connection...	Network Para...	Device Type	Serial No.	Security Le...	Resource U...	Firmware Upgrade	Operation
□	[redacted]	IP/Domain	[redacted].	Encoding D...	DS-[redacted]10...	Strong	✓ Online	No available version	
□	[redacted]	IP/Domain	[redacted].	Encoding D...	DS-[redacted]04...	Strong	✓ Online	ⓘ Upgradeable	
□	[redacted]	IP/Domain	[redacted].	Access Cont...	DS-[redacted]3V...	Strong	✓ Online	No available version	
□	[redacted]	IP/Domain	[redacted].	Device		Strong	☒ Offline	No available version	
□	[redacted]	IP/Domain	[redacted]	Encoding D...	DS-[redacted]80...	Strong	✓ Online	No available version	
□	[redacted]	IP/Domain	[redacted].	Encoding D...	DS-[redacted]80...	Strong	✓ Online	No available version	

Figure 3-2 Firmware Upgrade

Chapter 4 Group Management

The resources added should be organized into groups for convenient management, such as access points. You can do some further operations of the device through the groups.

4.1 Add Group

You can add group to organize the added device for convenient management.

Steps

1. Enter the Device Management module.
2. Click **Device Management → Group** to enter the group management page.
3. Create a group.
   - Click **Add Group** and enter a group name as you want.
   - Click **Create Group by Device Name** and select an added device to create a new group by the name of the selected device.

4.2 Import Resources to Group

You can import the device resources to the added group in a batch.

Before You Start
Add a group for managing devices. Refer to ***Add Group*** .

Steps

1. Enter the Device Management module.
2. Click **Device Management → Group** to enter the group management page.
3. Select a group from the group list and select the resource type such as **Access Control Point**.
4. Click **Import**.
5. Select the channel names from the To Be Imported area.
6. Click **Import** to import the selected resources to the group.

4.3 Edit Resource Parameters

After importing the resources to the group, you can edit the resource parameters. For access points, you can edit the resource name.

Before You Start
Import the resources to group. Refer to ***Import Resources to Group*** .

Steps

1. Enter the Device Management module.
2. Click **Device Management → Group** to enter the group management page.

All the added groups are displayed on the left.

3. Select a group on the group list and click a resource type.

   The resource channels imported to the group will display.
4. Click ✎ in the Operation column to open the Edit Camera window.
5. Edit the required information.
6. Click **OK** to save the new settings.

4.4 Remove Resources from Group

You can remove the added resources from the group.

Steps

1. Enter the Device Management module.
2. Click **Device Management → Group** to enter the group management page.

   All the added groups are displayed on the left.
3. Click a group to show the resources added to this group.
4. Select the resource(s) and click **Delete** to remove the resource(s) from the group.

Chapter 5 Event Center

You can configure the event of the added resources and set the linkage actions so that when the event is triggered, the software client can notify the security personnel and record the event details for checking afterwards.

In the event management page, you can configure access control event. For details about access control event configuration, refer to ***Configure Linkage Actions for Access Control*** .

In the event center, you can view the real-time events and search the historical events. For details, refer to ***View Real-Time Events*** and ***Search Historical Events*** .

5.1 Enable Receiving Events from Devices

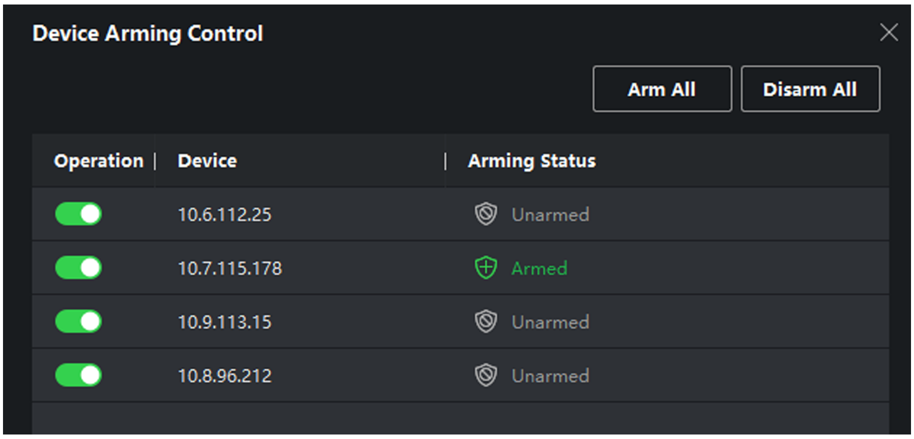
Before the client can receive the event information from the device, you need to arm the device first.

Steps

1. Click ☰ → **Tool** → **Device Arming Control** open Device Arming Control page.

   All the added devices display on this page.

2. In the Operation column, turn on the switch to enable auto-arming, or click **Arm All** to arm all the devices.



Operation	Device	Arming Status
●	10.6.112.25	Unarmed
●	10.7.115.178	Armed
●	10.9.113.15	Unarmed
●	10.8.96.212	Unarmed

Figure 5-1 Device Arming Control

3. View the arming status of each device in the Arming Status column.

Result

The events of armed device(s) are automatically uploaded to the client when the event is triggered.

5.2 View Real-Time Events

In the Real-time Event module of the event center page, you can view the real-time event information, including event source, event time, priority, event key words, etc.

Before You Start

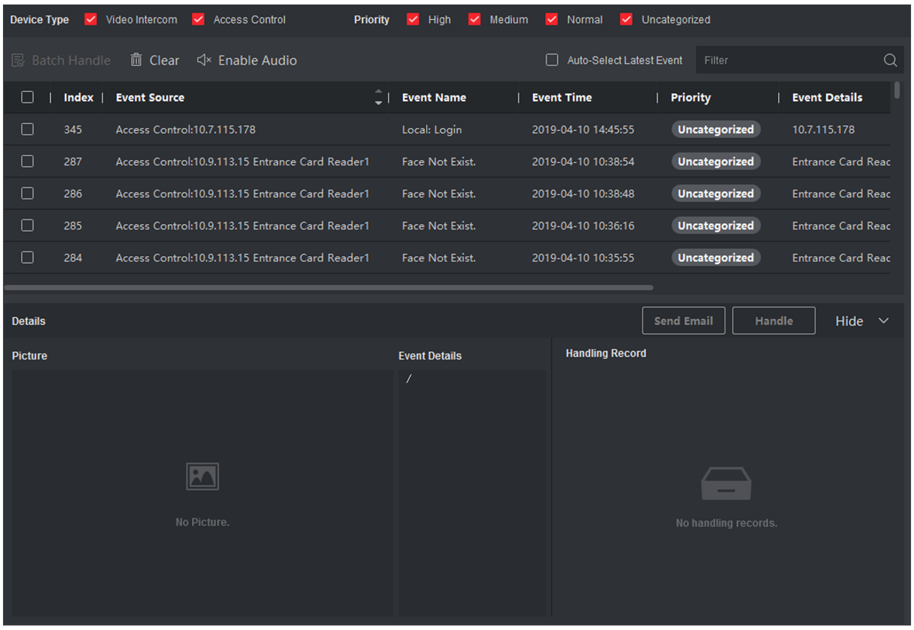
Enable receiving events from devices before the client can receive event information from the device, see ***Enable Receiving Events from Devices*** for details.

Steps

1. Click **Event Center → Real-time Event** to enter the real-time event page and you can view the real-time events received by the client.

   Event Time

   For video device, event time is the client time when it receives the event. For none-video device, event time is the time when the event is triggered.



Device Type ☑ Video Intercom ☑ Access Control Priority ☑ High ☑ Medium ☑ Normal ☑ Uncategorized

☐ Auto-Select Latest Event

☐	Index	Event Source	Event Name	Event Time	Priority	Event Details
☐	345	Access Control:10.7.115.178	Local: Login	2019-04-10 14:45:55	Uncategorized	10.7.115.178
☐	287	Access Control:10.9.113.15 Entrance Card Reader1	Face Not Exist.	2019-04-10 10:38:54	Uncategorized	Entrance Card Reac
☐	286	Access Control:10.9.113.15 Entrance Card Reader1	Face Not Exist.	2019-04-10 10:38:48	Uncategorized	Entrance Card Reac
☐	285	Access Control:10.9.113.15 Entrance Card Reader1	Face Not Exist.	2019-04-10 10:36:16	Uncategorized	Entrance Card Reac
☐	284	Access Control:10.9.113.15 Entrance Card Reader1	Face Not Exist.	2019-04-10 10:35:55	Uncategorized	Entrance Card Reac

Figure 5-2 View Real-Time Events

2. Set the filter conditions or enter the event key word in the Filter text field to display the required events only.

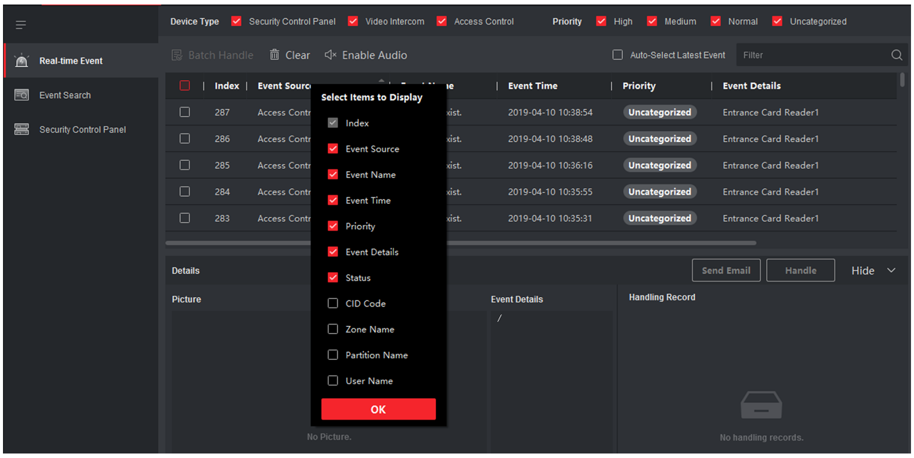
   Device Type

   The type of device that occurred the event.

   Priority

   The priority of the event that indicates the urgent degree of the event.

3. **Optional:** Right click the table header of the event list to customize the event related items to be displayed in the event list.



Device Type ☑ Security Control Panel ☑ Video Intercom ☑ Access Control

Priority ☑ High ☑ Medium ☑ Normal ☑ Uncategorized

□ Auto-Select Latest Event

□	Index	Event Sourc	e	Event Time	Priority	Event Details
□	287	Access Contr	xist.	2019-04-10 10:38:54	Uncategorized	Entrance Card Reader1
□	286	Access Contr	xist.	2019-04-10 10:38:48	Uncategorized	Entrance Card Reader1
□	285	Access Contr	xist.	2019-04-10 10:36:16	Uncategorized	Entrance Card Reader1
□	284	Access Contr	xist.	2019-04-10 10:35:55	Uncategorized	Entrance Card Reader1
□	283	Access Contr	xist.	2019-04-10 10:35:31	Uncategorized	Entrance Card Reader1

Select Items to Display

☑ Index
☑ Event Source
☑ Event Name
☑ Event Time
☑ Priority
☑ Event Details
☑ Status
□ CID Code
□ Zone Name
□ Partition Name
□ User Name

Figure 5-3 Customize Event Related Items to be Displayed

4. View the event information details.

1) Select an event in the event list.
2) Click **Expand** in the right-lower corner of the page.
3) View the related picture, detail description and handing records of the event.
4) **Optional:** Hover the cursor on the related picture, and then click the download icon on the upper-right corner of the picture to download it to the local PC. You can set the saving path manually.

5. Optional: Perform the following operations if necessary.

Handle Single Event
Click **Handle** to enter the processing suggestion, and then click **Commit**.

Note

After an event is handled, the **Handle** button will become **Add Remark**, click **Add Remark** to add more remarks for this handled event.

Handle Events in a Batch
Select events that need to be processed, and then click **Handle in Batch**. Enter the processing suggestion, and then click **Commit**.

Enable/Disable Alarm Audio
Click **Enable Audio/Disable Audio** to enable/disable the audio of the event.

Select the Latest Event Automatically
Check **Auto-Select Latest Event** to select the latest event automatically and the event information details is displayed.

Clear Events
Click **Clear** to clear the all the events in the event list.

Send Email
Select an event and then click **Send Email**, and the information details of this event will be sent by email.

Note

You should configure the email parameters first, see ***Set Email Parameters*** for details.

5.3 Search Historical Events

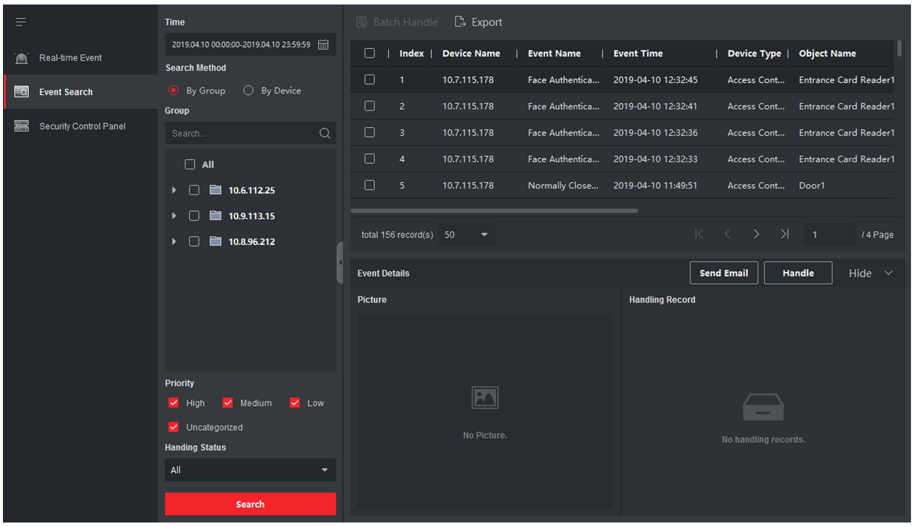
In the Event Search module of the event center page, you can search the historical events via time, device type, and other conditions according to the specified device type, and then process the events.

Before You Start

Enable receiving events from devices before the client can receive event information from the device,see ***Enable Receiving Events from Devices*** for details.

Steps

1. Click **Event Center → Event Search** to enter the event search page.



Time: 2019.04.10 00:00:00-2019.04.10 23:59:59

Search Method: ● By Group ○ By Device

Group: Search...

□ All
□ 10.6.112.25
□ 10.9.113.15
□ 10.8.96.212

Priority: ☑ High ☑ Medium ☑ Low ☑ Uncategorized

Handing Status: All

□	Index	Device Name	Event Name	Event Time	Device Type	Object Name
□	1	10.7.115.178	Face Authentica...	2019-04-10 12:32:45	Access Cont...	Entrance Card Reader1
□	2	10.7.115.178	Face Authentica...	2019-04-10 12:32:41	Access Cont...	Entrance Card Reader1
□	3	10.7.115.178	Face Authentica...	2019-04-10 12:32:36	Access Cont...	Entrance Card Reader1
□	4	10.7.115.178	Face Authentica...	2019-04-10 12:32:33	Access Cont...	Entrance Card Reader1
□	5	10.7.115.178	Normally Close...	2019-04-10 11:49:51	Access Cont...	Door1

total 156 record(s) 50 1 / 4 Page

Event Details

Picture

Handling Record

Figure 5-4 Search History Event

2. Set the filter conditions to display the required events only.

   Time

   The client time when the event starts.

   Search by

   Group: Search the events occurred on the resources in the selected group.

   Device: Search the events occurred on the selected device.

   Device Type

   The type of device that occurred the event.

All

All the device types, and you can set the following filter conditions: group, priority, and status.

Video Intercom

For the events of video intercom, you need to select searching scope: All Record and Only Unlocking.

- **All Records**: You can filter the events from all the video intercom events, and you need to set the following filter conditions: device, priority, status.
- **Only Unlocking**: You can filter the events from all the video intercom unlocking events, and you need to set the following filter conditions: device, unlocking type.

Access Control

For the events of access control, you can set the following filter conditions: device, priority, status, event type, card reader type, person name, card no., organization.

Note

Click **Show More** to set the event type, card reader type, person name, card no., organization.

Group

The group of the device that occurred the event. You should set the group as condition only when you select the Device Type as **All**.

Device

The device that occurred the event.

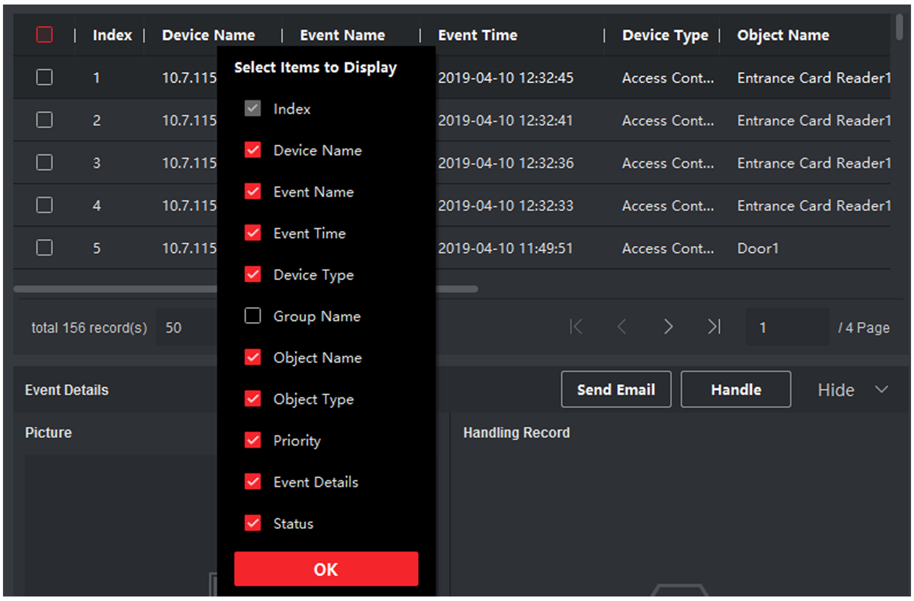
Priority

The priority including low, medium, high and uncategorized which indicates the urgent degree of the event.

Status

The handling status of the event.

3. Click **Search** to search the events according the conditions you set.
4. **Optional:** Right click the table header of the event list to customize the event related items to be displayed in the event list.



□	Index	Device Name	Event Name	Event Time	Device Type	Object Name
□	1	10.7.115		2019-04-10 12:32:45	Access Cont...	Entrance Card Reader1
□	2	10.7.115		2019-04-10 12:32:41	Access Cont...	Entrance Card Reader1
□	3	10.7.115		2019-04-10 12:32:36	Access Cont...	Entrance Card Reader1
□	4	10.7.115		2019-04-10 12:32:33	Access Cont...	Entrance Card Reader1
□	5	10.7.115		2019-04-10 11:49:51	Access Cont...	Door1

total 156 record(s) 50

1 / 4 Page

Select Items to Display

- ☑ Index
- ☑ Device Name
- ☑ Event Name
- ☑ Event Time
- ☑ Device Type
- □ Group Name
- ☑ Object Name
- ☑ Object Type
- ☑ Priority
- ☑ Event Details
- ☑ Status

Figure 5-5 Customize Event Related Items to be Displayed

5. **Optional:** Handle the event(s).
   - Handle single event: Select one event that need to be processed, and then click **Handle** in the event information details page, and enter the processing suggestion.
   - Handle events in a batch: Select the events which need to be processed, and then click **Handle in Batch**, and enter the processing suggestion.

Note

After an event is handled, the **Handle** button will become **Add Remark**, click **Add Remark** to add more remarks for this handled event.

6. **Optional:** Select an event and then click **Send Email**, and the information details of this event will be sent by email.

Note

You should configure the email parameters first, see ***Set Email Parameters*** for details.

7. **Optional:** Click **Export** to export the event log or event pictures to the local PC in CSV format. You can set the saving path manually.
8. Hover the cursor on the related picture, and then click the download icon on the upper-right corner of the picture to download it to the local PC. You can set the saving path manually.

Chapter 6 Person Management

You can add person information to the system for further operations such as access control, video intercom, time and attendance, etc. You can manage the added persons such as issuing cards to them in a batch, importing and exporting person information in a batch, etc.

6.1 Add Organization

You can add an organization and import person information to the organization for effective management of the persons. You can also add a surbodinate organization for the added one.

Steps

1. Enter **Person** module.
2. Select a parent organization in the left column and click **Add** in the upper-left corner to add an organization.
3. Create a name for the added organization.

   Note

   Up to 10 levels of organizations can be added.

4. **Optional:** Perform the following operation(s).

   Edit Organization
   Hover the mouse on an added organization and click ✎ to edit its name.

   Delete Organization
   Hover the mouse on an added organization and click ✕ to delete it.

   Note

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

   Show Persons in Sub Organization
   Check **Show Persons in Sub Organization** and select an organization to show persons in its sub organizations.

6.2 Add Single Person

You can add persons to the client software one by one. The person information contains basic information, detailed information, profiles, access control information,credentials, custom information, etc.

6.2.1 Configure Basic Information

You can add person to the client software one by one and configure the person's basic information such as name, gender, phone number, etc.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person.
3. Click **Add** to open the adding person window.

   The Person ID will be generated automatically.
4. Enter the basic information including person name, gender, tel, email address, etc.
5. **Optional:** Set the effective period of the person. Once expired, the credentials and access control settings of the person will be invalid and the person will have no authorization to access the doors\floors.

   Example

   For example, if the person is a visitor, his/her effective period may be short and temporary.
6. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons.

6.2.2 Issue a Card to One Person

When adding person, you can issue a card with a unique card number to the person as a credential. After issued, the person can access the doors which he/she is authorized to access by swiping the card on the card reader.

Steps

Note

Up to five cards can be issued to one person.

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .
3. In the **Credential → Card** panel, click **+**.
4. Enter the card number.
   - Enter the card number manually.
   - Place the card on the card enrollment station or card reader and click **Read** to get the card number. The card number will display in the Card No. field automatically.

Note

You need to click **Settings** to set the card issuing mode and related parameters first. For details, refer to ***Set Card Issuing Parameters*** .

5. Select the card type according to actual needs.

   Normal Card

   The card is used for opening doors for normal usage.

   Duress Card

   When the person is under duress, he/she can swipe the duress card to open the door. The door will be unlocked and the client will receive a duress event to notify the security personnel.

   Patrol Card

   This card is used for the inspection staff to check the their attendance of inspection. By swiping the card on the specified card reader, the person is marked as on duty of inspection at that time.

   Dismiss Card

   By swiping the card on the card reader, it can stop the buzzing of the card reader.

6. Click **Add**.

   The card will be issued to the person.

7. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons.

6.2.3 Upload a Face Photo from Local PC

When adding person, you can upload a face photo stored in local PC to the client as the person's profile.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. Click **Add Face** in the Basic Information panel.
4. Select **Upload**.
5. Select a picture from the PC running the client.

Note

The picture should be in JPG or JPEG format and smaller than 200 KB.

6. **Optional:** Enable **Verify by Device** to check whether the facial recognition device managed in the client can recognize the face in the photo.
7. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons .

6.2.4 Take a Photo via Client

When adding person, you can take a photo of the person by the webcam of the PC running the client and set this photo as the person's profile.

Before You Start

Add at least one access control device checking whether the face in the photo can be recognized by the facial recognition device managed by the client.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. Click **Add Face** in the Basic Information panel.
4. Select **Take Photo**.
5. Connect the face scanner to the PC running the client.
6. **Optional:** Enable **Verify by Device** to check whether the facial recognition device managed in the client can recognize the face in the photo.
7. Take a photo.
   1) Face to the webcam of the PC and make sure your face is in the middle of the collecting window.
   2) Click 📷 to capture a face photo.
   3) **Optional:** Click ↺ to capture again.
   4) Click **OK** to save the captured photo.
8. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons.

6.2.5 Collect Face via Access Control Device

When adding person, you can collect the person's face via access control device added to the client which supports facial recognition function.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. Click **Add Face** in the Basic Information panel.
4. Select **Remote Collection**.
5. Select an access control device which supports face recognition function from the drop-down list.
6. Collect face.
   1) Face to the camera of the selected access control device and make sure your face is in the middle of the collecting window.
   2) Click 📷 to capture a photo.
   3) Click **OK** to save the captured photo.
7. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons .

6.2.6 Collect Fingerprint via Client

Collecting fingerprints locally means you can collect the fingerprint via the fingerprint recorder connected directly to the PC running the client. The fingerprints recorded can be used as credentials of the persons to access the authorized doors.

Before You Start

Connect the fingerprint recorder to the PC running the client.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. In the **Credential → Fingerprint** panel, click **+**.
4. In the pop-up window, select the collection mode as **Local**.

5. Select the model of the connected fingerprint recorder.

   Note

   If the fingerprint recorder is DS-K1F800-F, you can click **Settings** to select the COM the fingerprint recorder connects to.

6. Collect the fingerprint.
   1) Click **Start**.
   2) Place and lift your fingerprint on the fingerprint recorder to collect the fingerprint.
   3) Click **Add** to save the recorded fingerprint.
7. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons.

6.2.7 Collect Fingerprint via Access Control Device

When adding person, you can collect fingerprint information via the access control device's fingerprint module. The fingerprints recorded can be used as credentials of the persons to access the authorized doors.

Before You Start

Make sure fingerprint collection is supported by the access control device.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. In the **Credential → Fingerprint** panel, click **+**.
4. In the pop-up window, select the collection mode as **Remote**.
5. Select an access control device which supports fingerprint recognition function from the drop-down list.
6. Collect the fingerprint.
   1) Click **Start**.
   2) Place and lift your fingerprint on the fingerprint scanner of the selected access control device to collect the fingerprint.
   3) Click **Add** to save the recorded fingerprint.
7. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons .

6.2.8 Configure Access Control Information

When adding a person, you can set her/his access control properties, such as setting the person as visitor or as blacklist person, or as super user who has super authorization.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. In the **Access Control** panel, set the person's access control properties.

   PIN Code

   The PIN code must be used after card or fingerprint when accessing. It cannot be used independently. It should contain 4 to 8 digits.

   Super User

   If the person is set as a super user, he/she will have authorization to access all the doors/floors and will be exempted from remaining closed restrictions, all anti-passback rules, and first person authorization.

   Extended Door Open Time

   When the person accessing door, grant this person more time to pass through doors which have been configured with extended open duration. Use this function for the persons with reduced mobility.

   For details about setting the door's open duration, refer to ***Configure Parameters for Door/ Elevator*** .

   Add to Blacklist

   Add the person to the blacklist and when the person tries to access doors/floors, an event will be triggered and send to the client to notify the security personnel.

   Mark as Visitor

   If the person is a visitor, set the maximum times of authentications, including access by card and fingerprint to limit the visitor's access times.

   Note

   The maximum times of authentications should be between 1 and 100.

   Device Operator

   For person with device operator role, he/she is authorized to operate on the access control devices.

Note

The Super User, Extended Door Open Time, Add to Blacklist, and Mark as Visitor functions cannot be enabled concurrently. For example, if one person is set as super user, you cannot enable extended door open time for her/him, add her/him to the blacklist, or set her/him as visitor.

4. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons.

6.2.9 Customize Person Information

You can customize the person properties which are not pre-defined in the client according to actual needs, e.g., place of birth. After customizing, when add a person, you can enter the custom information to make the person information complete.

Steps

1. Enter **Person** module.
2. Set the fields of custom information.
   1) Click **Custom Property**.
   2) Click **Add** to add a new property.
   3) Enter the property name.
   4) Click **OK**.
3. Set the custom information when adding a person.
   1) Select an organization in the organization list to add the person and click **Add**.

      Note

      Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .
   2) In the **Custom Information** panel, enter the person information.
   3) Click **Add** to add the person and close the Add Person window, or click **Add and New** to add the person and continue to add other persons.

6.2.10 Configure Resident Information

If the person is resident, for video intercom purpose, you need to set the room number for her/him and bind an indoor station. After bound, you can call this person by calling the indoor station and perform video intercom with her/him.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. In the **Resident Information** panel, select the indoor station to bink it to the person.

Note

If you select **Analog Indoor Station**, the **Door Station** field will display and you are required to select the door station to communicate with the analog indoor station.

4. Enter the floor No. and room No. of the person.
5. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons.

6.2.11 Configure Additional Information

When adding person, you can configure the additional information for the person, such as person's identity type, identity No., country, etc., according to actual needs.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. In the **Additional Information** panel, enter the additional information of the person, including person's ID type, ID No., job title, etc., according to actual needs.
4. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons .

6.3 Import and Export Person Identify Information

You can import the information and pictures of multiple persons to the client software in a batch. Meanwhile, you can also export the person information and pictures and save them in your PC.

6.3.1 Import Person Information

You can enter the information of multiple persons in a predefined template (a CSV file) to import the information to the client in a batch.

Steps

1. Enter the Person module.
2. Select an added organization in the list, or click **Add** in the upper-left corner to add an organization and then select it.
3. Click **Import** to open the Import panel.
4. Select **Person Information** as the importing mode.
5. Click **Download Template for Importing Person** to download the template.
6. Enter the person information in the downloaded template.

Note

- If the person has multiple cards, separate the card No. with semicolon.
- Items with asterisk are required.
- By default, the Hire Date is the current date.

7. Click … to select the CSV file with person information.
8. Click **Import** to start importing.

Note

- If a person No. already exists in the client's database, delete the existing information before importing.
- You can import information of no more than 10,000 persons.

6.3.2 Import Person Pictures

After importing face pictures for the added persons to the client, the persons in the pictures can be identified by an added face recognition terminal. You can either import person pictures one by one, or import multiple pictures at a time according to your need.

Before You Start

Be sure to have imported person information to the client beforehand.

Steps

1. Enter the Person module.
2. Select an added organization in the list, or click **Add** in the upper-left corner to add an organization and then select it.
3. Click **Import** to open the Import panel and check **Face**.
4. **Optional:** Enable **Verify by Device** to check whether face recognition device managed in the client can recognize the face in the photo.
5. Click … to select a face picture file.

Note

- The (folder of) face pictures should be in ZIP format.
- Each picture file should be in JPG format and should be no larger than 200 KB.
- Each picture file should be named as "Person ID_Name". The Person ID should be the same with that of the imported person information.

6. Click **Import** to start importing.

   The importing progress and result will be displayed.

6.3.3 Export Person Information

You can export the added persons' information to local PC as a CSV file.

Before You Start
Make sure you have added persons to an organization.

Steps

1. Enter the Person module.
2. **Optional:** Select an organization in the list.

   Note

   All persons' information will be exported if you do not select any organization.

3. Click **Export** to open the Export panel and check **Person Information** as the content to export.
4. Check desired items to export.
5. Click **Export** to save the exported CSV file in your PC.

6.3.4 Export Person Pictures

You can export face picture file of the added persons and save in your PC.

Before You Start
Make sure you have added persons and their face pictures to an organization.

Steps

1. Enter the Person module.
2. **Optional:** Select an organization in the list.

   Note

   All persons' face pictures will be exported if you do not select any organization.

3. Click **Export** to open the Export panel and check **Face** as the content to export.
4. Click **Export** to start exporting.

Note

- The exported file is in ZIP format.
- The exported face picture is named as "Person ID_Name_0" ("0" is for a full-frontal face).

6.4 Get Person Information from Access Control Device

If the added access control device has been configured with person information (including person details, fingerprint, and issued card information), you can get the person information from the device and import them to the client for further operations.

Steps

Note

- If the person name stored in the device is empty, the person name will be filled with the issued card No. after importing to the client.
- The gender of the persons will be **Male** by default.
- If the card number or person ID (employee ID) stored on the device already exists in the client database, the person with this card number or person ID will not be imported to the client.

1. Enter **Person** module.
2. Select an organization to import the persons.
3. Click **Get from Device**.
4. Select the access control device from the drop-down list.
5. Click **Get** to start importing the person information to the client.

   The person information, including person details, person's fingerprint information (if configured), and the linked cards (if configured), will be imported to the selected organization.

6.5 Move Persons to Another Organization

You can move the added persons to another organization if you need.

Before You Start

- Make sure you have added at least two organizations.
- Make sure you have imported person information.

Steps

1. Enter **Person** module.
2. Select an organization in the left panel.

   The persons under the organization will be displayed in the right panel.
3. Select the person to move.
4. Click **Change Organization**.
5. Select the organization to move persons to.

6. Click **OK**.

6.6 Issue Cards to Persons in Batch

The client provides a convenient way to issue cards to multiple persons in a batch.

Steps

1. Enter **Person** module.
2. Click **Batch Issue Cards**.

   All the added persons with no card issued will display.
3. Set the card issuing parameters. For details, refer to ***Set Card Issuing Parameters*** .
4. Click **Initialize** to initialize the card enrollment station or card reader to make it ready for issuing cards.
5. Click the card number column and enter the card number.
   - Place the card on the card enrollment station.
   - Swipe the card on the card reader.
   - Enter the card number manually and press **Enter** key on your keyboard.

   The card number will be read automatically and the card will be issued to the person in the list.
6. Repeat the above step to issue the cards to the persons in the list in sequence.

6.7 Report Card Loss

If the person lost his/her card, you can report the card loss so that the card's related access authorization will be inactive.

Steps

1. Enter **Person** module.
2. Select the person you want to report card loss for and click **Edit** to open the Edit Person window.
3. In the **Credential → Card** panel, click on the added card to set this card as lost card.

   After reporting card loss, the access authorization of this card will be invalid and inactive. Other person who gets this card cannot access the doors by swiping this lost card.
4. **Optional:** If the lost card is found, you can click to cancel the loss.

   After cancelling card loss, the access authorization of the person will be valid and active.
5. If the lost card is added in one access group and the access group is applied to the device already, after reporting card loss or cancelling card loss, a window will pop up to notify you to apply the changes to the device. After applying to device, these changes can take effect on the device.

6.8 Set Card Issuing Parameters

The client provides two modes for reading a card's number: via card enrollment station or via the card reader of the access control device. If a card enrollment station is available, connect it to the PC running the client by USB interface or COM, and place the card on the card enrollment to read the card number. If not, you can also swipe the card on the card reader of the added access control device to get the card number. As a result, before issuing a card to one person, you need to set the card issuing parameters including the issuing mode and related parameters.

When adding a card to one person, click **Settings** to open the Card Issuing Settings window.

Local Mode: Issue Card by Card Enrollment Station

Connect a card enrollment station to the PC running the client. You can place the card on the card enrollment station to get the card number.

Card Enrollment Station

Select the model of the connected card enrollment station

Note

Currently, the supported card enrollment station models include DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, and DS-K1F180-D8E.

Card Type

This field is only available when the model is DS-K1F100-D8E or DS-K1F180-D8E.

Select the card type as EM card or IC card according to the actual card type.

Serial Port

It is only available when the model is DS-K1F100-M.

Select the COM the card enrollment station connects to.

Buzzing

Enable or disable the buzzing when the card number is read successfully.

Card No. Type

Select the type of the card number according to actual needs.

M1 Card Encryption

This field is only available when the model is DS-K1F100-D8, DS-K1F100-D8E, or DS-K1F180-D8E.

If the card is M1 card, and if you need to enable the M1 Card Encryption function, you should enable this function and select the sector of the card to encrypt.

Remote Mode: Issue Card by Card Reader

Select an access control device added in the client and swipe the card on its card reader to read the card number.

Chapter 7 Access Control

The Access Control module is applicable to access control devices and video intercom device. It provides multiple functionalities, including access group configuration, video intercom, and other advanced functions.

Note

For the user with access control module permissions, the user can enter the Access Control module and configure the access control settings. For setting the user permission of Access Control module, refer to ***Add User*** .

7.1 Configure Schedule and Template

You can configure the template including holiday and week schedule. After setting the template, you can adopt the configured template to access groups when setting the access groups, so that the access group will take effect in the time durations of the template.

Note

For access group settings, refer to ***Set Access Group to Assign Access Authorization to Persons*** .

7.1.1 Add Holiday

You can create holidays and set the days in the holidays, including start date, end date, and holiday duration in one day.

Steps

Note

You can add up to 64 holidays in the software system.

1. Click **Access Control → Schedule → Holiday** to enter the Holiday page.
2. Click **Add** on the left panel.
3. Create a name for the holiday.
4. **Optional:** Enter the descriptions or some notifications of this holiday in the Remark box.
5. Add a holiday period to the holiday list and configure the holiday duration.

   Note

   Up to 16 holiday periods can be added to one holiday.

   1) Click **Add** in the Holiday List field.
   2) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.

Note

Up to 8 time durations can be set to one holiday period.

3) **Optional:** Perform the following operations to edit the time durations.
   - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to ✋ .
   - Click the time duration and directly edit the start/end time in the appeared dialog.
   - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to ⇔ .
4) **Optional:** Select the time duration(s) that need to be deleted, and then click ⊗ in the Operation column to delete the selected time duration(s).
5) **Optional:** Click 🗑 in the Operation column to clear all the time duration(s) in the time bar.
6) **Optional:** Click ✕ in the Operation column to delete this added holiday period from the holiday list.

6. Click **Save**.

7.1.2 Add Template

Template includes week schedule and holiday. You can set week schedule and assign the time duration of access authorization for different person or group. You can also select the added holiday(s) for the template.

Steps

Note

You can add up to 255 templates in the software system.

1. Click **Access Control → Schedule → Template** to enter the Template page.

Note

There are two default templates: All-Day Authorized and All-Day Denied, and they cannot be edited or deleted.

All-Day Authorized

The access authorization is valid in each day of the week and it has no holiday.

All-Day Denied

The access authorization is invalid in each day of the week and it has no holiday.

2. Click **Add** on the left panel to create a new template.

3. Create a name for the template.

4. Enter the descriptions or some notification of this template in the Remark box.

5. Edit the week schedule to apply it to the template.

1) Click **Week Schedule** tab on the lower panel.
2) Select a day of the week and draw time duration(s) on the timeline bar.

> **Note**
>
> Up to 8 time duration(s) can be set for each day in the week schedule.

3) **Optional:** Perform the following operations to edit the time durations.
   - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to ✋ .
   - Click the time duration and directly edit the start/end time in the appeared dialog.
   - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to ⇔ .
4) Repeat the two steps above to draw more time durations on the other days of the week.

6. Add a holiday to apply it to the template.

> **Note**
>
> Up to 4 holidays can be added to one template.

1) Click **Holiday** tab.
2) Select a holiday in the left list and it will be added to the selected list on the right panel.
3) **Optional:** Click **Add** to add a new holiday.

> **Note**
>
> For details about adding a holiday, refer to ***Add Holiday*** .

4) **Optional:** Select a selected holiday in the right list and click ✕ to remove the selected one, or click **Clear** to clear all the selected holiday(s) in the right list.

7. Click **Save** to save the settings and finish adding the template.

7.2 Set Access Group to Assign Access Authorization to Persons

After adding the person and configuring the person's credentials, you can create the access groups to define which person(s) can get access to which door(s) and then apply the access group to the access control device to take effect.

Steps

- For one person, you can add up to 4 access groups to one access control point of one device.
- You can add up to 128 access groups in total.
- When the access group settings are changed, you need to apply the access groups to the devices again to take effect. The access group changes include changes of template, access group settings, person's access group settings, and related person details (including card number, fingerprint, face picture, linkage between card number and fingerprint, linkage between card number and fingerprint, card password, card effective period, etc).

1. Click **Access Control → Access Group** to enter the Access Group interface.
2. Click **Add** to open the Add window.
3. In the **Name** text field, create a name for the access group as you want.
4. Select a template for the access group.

Note

You should configure the template before access group settings. Refer to ***Configure Schedule and Template*** for details.

5. In the left list of the Select Person field, select person(s) and the person(s) will be added to the selected list .
6. In the left list of the Select Door field, select door(s) or door station(s) for the selected persons to access, and the selected door(s) or door station(s) will be added to the selected list.
7. Click **OK**.
8. After adding the access groups, you need to apply them to the access control device to take effect.
   1) Select the access group(s) to apply to the access control device.

      To select multiple access groups, you can hold the **Ctrl** or **Shift** key and select access groups.
   2) Click **Apply All to Devices** to start applying all the selected access group(s) to the access control device or door station.

      Caution

      - Be careful to click **Apply All to Devices**, since this operation will clear all the access groups of the selected devices and then apply the new access group, which may brings risk to the devices.
      - You can click **Apply Changes to Devices** to only apply the changed part of the selected access group(s) to the device(s).
   3) View the apply status in the Status column or click **Applying Status**to view all the applied access group(s).

   The selected persons in the applied access groups will have the authorization to enter/exit the selected doors/door stations with their linked card(s) or fingerprints.
9. **Optional:** Click ✎ to edit the access group if necessary.

7.3 Configure Advanced Functions

You can configure the advanced functions of access control to meet some special requirements in different scene, such as multi-factor authentication, anti-passback, etc.

Note

- For the card related functions(the type of access control card/multi-factor authentication), only the card(s) with access group applied will be listed when adding cards.
- The advanced functions should be supported by the device.
- Hover the cursor on the Advanced Function, and then Click ⚙ to customize the advanced function(s) to be displayed.

7.3.1 Configure Device Parameters

After adding the access control device, you can configure the parameters of access control device (access controller), access control points (door or floor), alarm inputs, alarm outputs, card readers and lane controller.

Configure Parameters for Access Control Device

After adding the access control device, you can configure its parameters, including overlaying user information on picture, uploading pictures after capturing, saving captured pictures, etc.

Steps

1. Click **Access Control → Advanced Function → Device Parameter** .

   Note

   If you can find Device Parameter in the Advanced Function list, Hover the cursor on the Advanced Function, and then Click ⚙ to select the Device Parameter to be displayed.

2. Select an access device to show its parameters on the right page.
3. Turn the switch to ON to enable the corresponding functions.

   Note

   - The displayed parameters may vary for different access control devices.
   - Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.

   RS-485 Comm. Redundancy

   You should enable this function if you wire the RS-485 card reader to the access control device redundantly.

   Display Detected Face

   Display face picture when authenticating.

   Display Card Number

   Display the card information when authenticating.

   Display Person Information

   Display the person information when authenticating.

   Overlay Person Info. on Picture

   Display the person information on the captured picture.

   Voice Prompt

   If you enable this function, the voice prompt is enabled in the device. You can hear the voice prompt when operating in the device.

Upload Pic. After Linked Capture

Upload the pictures captured by linked camera to the system automatically.

Save Pic. After Linked Capture

If you enable this function, you can save the picture captured by linked camera to the device.

Press Key to Enter Card Number

If you enable this function, you can input the card No. by pressing the key.

Wi-Fi Probe

If you enable this function, the device can probe the surrounding communication devices' MAC address and upload the MAC address to the system. If the MAC address match the specified MAC address, the system can trigger some linkage actions.

3G/4G

If you enable this function, the device can communicate in 3G/4G network.

4. Click **OK**.
5. **Optional:** Click **Copy to**, and then select the access control device(s) to copy the parameters in the page to the selected device(s).

Configure Parameters for Door/Elevator

After adding the access control device, you can configure its access point (door or floor) parameters.

Steps

1. Click **Access Control → Advanced Function → Device Parameter** .
2. Select an access control device on the left panel, and then click ▸ to show the doors or floors of the selected device.
3. Select a door or floor to show its parameters on the right page.
4. Edit the door or floor parameters.

Note

- The displayed parameters may vary for different access control devices.
- Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.

Name

Edit the card reader name as desired.

Door Contact

You can set the door sensor as remaining closed or remaining open. Usually, it is remaining closed.

Exit Button Type

You can set the exit button as remaining closed or remaining open. Usually, it is remaining open.

Door Locked Time

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

Extended Open Duration

The door contact can be enabled with appropriate delay after person with extended accesss needs swipes her/his card.

Door Left Open Timeout Alarm

The alarm can be triggered if the door has not been closed in a configured time period. If it is set as 0, no alarm will be triggered.

Lock Door when Door Closed

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

Create a dismiss code which can be used to stop the buzzer of the card reader (by entering the dismiss code on the keypad).

Note

- The duress code, super code, and dismiss code should be different.
- The duress code, super password, and the dismiss code should be different from the authentication password.
- The length of duress code, super password, and the dismiss code is according the device, usually it should contains 4 to 8 digits.

5. Click **OK**.
6. **Optional:** Click **Copy to** , and then select the door/floor(s) to copy the parameters in the page to the selected doors/floor(s).

Note

The door or floor's status duration settings will be copied to the selected door/floor(s) as well.

Configure Parameters for Card Reader

After adding the access control device, you can configure its card reader parameters.

Steps

1. Click **Access Control → Advanced Function → Device Parameter** .
2. In the device list on the left, click ▸ to expand the door, select a card reader and you can edit the card reader's parameters on the right.
3. Edit the card reader basic parameters in the Basic Information page.

Note

- The displayed parameters may vary for different access control devices. There are part of parameters listed as follows. Refer to the user manual of the device for more details.
- Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.

Name

Edit the card reader name as desired.

OK LED Polarity/Error LED Polarity/Buzzer Polarity

Set OK LED Polarity/Error LED Polarity/Buzzer LED Polarity of main board according to the card reader parameters. Generally, adopts the default settings.

Minimum Card Swiping Interval

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 Entering PWD

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.

Alarm of Max. Failed Attempts

Enable to report alarm when the card reading attempts reach the set value.

Max. Times of Card Failure

Set the max. failure attempts of reading card.

Tampering Detection

Enable the anti-tamper detection for the card reader.

Communicate with Controller Every

When the access control device cannot connect with the card reader for longer than the set time, the card reader will turn offline automatically.

Buzzing Time

Set the card reader buzzing time. The available time ranges from 0 to 5,999s. 0 represents continuous buzzing.

Card Reader Type/Card Reader Description

Get card reader type and description. They are read-only.

Fingerprint Recognition Level

Select the fingerprint recognition level in the drop-down list.

Default Card Reader Authentication Mode

View the default card reader authentication mode.

Fingerprint Capacity

View the maximum number of available fingerprints.

Existing Fingerprint Number

View the number of existed fingerprints in the device.

Score

The device will score the captured picture according to the yaw angle, pitch angle, and pupillary distance. If the score is less than the configured value, face recognition will be failed.

Face Recognition Timeout Value

If the recognition time is more than the configured time, the device will remind you.

Face Recognition Interval

The time interval between two continuous face recognitions when authenticating. By default, it is 2s.

Face 1:1 Matching Threshold

Set the matching threshold when authenticating via 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate when authentication.

1:N Security Level

Set the matching security level when authenticating via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate when authentication.

Live Face Detection

Enable or disable the live face detection function. If enabling the function, the device can recognize whether the person is a live one or not.

Live Face Detection Security Level

After enabling Live Face Detection function, you can set the matching security level when performing live face authentication.

Max. Failed Attempts for Face Auth.

Set the maximum live face detection failed attempts. The system will lock the user's face for 5 minutes if the live face detection is failed for more than the configured attempts. The same user cannot authenticate via the fake face within 5 minutes. Within the 5 minutes, the user can authenticate via the real face twice continuously to unlock.

Lock Authentication Failed Face

After enabling the Live Face Detection function, the system will lock the user's face for 5 minutes if the live face detection is failed for more than the configured attempts. The same user cannot authenticate via the fake face within 5 minutes. Within the 5 minutes, the user can authenticate via the real face twice continuously to unlock.

Application Mode

You can select indoor or others application modes according to actual environment.

4. Click **OK**.
5. **Optional:** Click **Copy to**, and then select the card reader(s) to copy the parameters in the page to the selected card reader(s).

Configure Parameters for Alarm Input

After adding the access control device, you can configure the parameters for its alarm inputs.

Steps

Note

If the alarm input is armed, you cannot edit its parameters. Disarm it first.

1. Click **Access Control → Advanced Function → Device Parameter** .
2. In the device list on the left, click ▸ to expand the door, select an alarm input and you can edit the alarm input's parameters on the right.
3. Set the alarm input parameters.

   Name

   Edit the alarm input name as desired.

   Detector Type

   The detector type of the alarm input.

   Zone Type

   Set the zone type for the alarm input.

   Sensitivity

   Only when the duration of signal detected by the detector reaches the setting time, the alarm input is triggered. For example, you have set the sensitivity as 10ms, only when the duration of signal detected by the detector reach 10ms, this alarm input is triggered.

   Trigger Alarm Output

   Select the alarm output(s) to be triggered.

4. Click **OK**.
5. **Optional:** Click the switch on the upper-right corner to arm or disarm the alarm input.

Configure Parameters for Alarm Output

After adding the access control device, if the device links to alarm outputs, you can configure the parameters.

Steps

1. Click **Access Control → Advanced Function → Device Parameter** to enter access control parameter configuration page.
2. In the device list on the left, click ▸ to expand the door, select an alarm input and you can edit the alarm input's parameters on the right.
3. Set the alarm output parameters.

   Name

   Edit the card reader name as desired.

   Alarm Output Active Time

   How long the alarm output will last after triggered.
4. Click **OK**.
5. **Optional:** Set the switch on the upper right corner to **ON** to trigger the alarm output.

Configure Parameters for Lane Controller

After adding the lane controller to the client, you can configure its parameters for passing through the lane.

Steps

1. Click **Access Control → Advanced Function → Device Parameter** to enter Parameter Settings page.
2. In the device list on the left, select a lane controller and you can edit the lane controller's parameters on the right.
3. Edit the parameters.

   Passing Mode

   Select the controller which will control the barrier status of the device.

   - If you select **According to Lane Controller's DIP Settings**, the device will follow the lane controller's DIP settings to control the barrier. The settings on the software will be invalid.
   - If you select **According to Main Controller's Settings**, the device will follow the settings of the software to control the barrier. The DIP settings of the lane controller will be invalid.

   Free Passing Authentication

   If you enable this function, when both entrance and exit's barrier mode is Remain Open, the pedestrians should authenticate each time passing through the lane. Or an alarm will be triggered.

   Opening/Closing Door Speed

Set the barrier's opening and closing speed. You can select from 1 to 10. The greater the value, the faster the speed.

Note

The recommended value is 6.

Audible Prompt Duration

Set how long the audio will last, which is played when an alarm is triggered .

Note

0 refers to the alarm audio will be played until the alarm is ended.

Temperature Unit

Select the temperature unit that displayed in the device status.

4. Click **OK**.

7.3.2 Configure Remaining Open/Closed

You can set the status of the door as open or closed and set the elevator controller as free and controlled. For example, you can set the door remaining closed in the holiday, and set the door remaining open in the specified period of the work day.

Before You Start

Add the access control devices to the system.

Steps

1. Click **Access Control → Advanced Function → Remain Open/Closed** to enter the Remain Open/ Closed page.
2. Select the door or elevator controller that need to be configured on the left panel.
3. To set the door or elevator controller status during the work day, click the **Week Schedule** and perform the following operations.
   1) For door, click **Remain Open** or **Remain Closed**.
   2) For elevator controller, click **Free** or **Controlled**.
   3) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.

   Note

   Up to 8 time durations can be set to each day in the week schedule.

   4) **Optional:** Perform the following operations to edit the time durations.
      - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
      - Click the time duration and directly edit the start/end time in the appeared dialog.
      - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .

5) Click **Save**.

Related Operations

Copy to Whole Week Select one duration on the time bar, click **Copy to Whole Week** to copy all the duration settings on this time bar to other week days.

Delete Selected Select one duration on the time bar, click **Delete Selected** to delete this duration.

Clear Click **Clear** to clear all the duration settings in the week schedule.

4. To set the door status during the holiday, click the **Holiday** and perform the following operations.
   1) Click **Remain Open** or **Remain Closed**.
   2) Click **Add**.
   3) Enter the start date and end date.
   4) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.

   Note

   Up to 8 time durations can be set to one holiday period.

   5) Perform the following operations to edit the time durations.
      - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to ✋ .
      - Click the time duration and directly edit the start/end time in the appeared dialog.
      - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to ⟺ .
   6) **Optional:** Select the time duration(s) that need to be deleted, and then click ⊗ in the Operation column to delete the selected time duration(s).
   7) **Optional:** Click 🗑 in the Operation column to clear all the time duration(s) in the time bar.
   8) **Optional:** Click ☒ in the Operation column to delete this added holiday period from the holiday list.
   9) Click **Save**.
5. **Optional:** Click **Copy to** to copy the door status settings of this door to other door(s).

7.3.3 Configure Multi-Factor Authentication

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

Before You Start

Set access group and apply the access group to the access control device. For details, refer to ***Set Access Group to Assign Access Authorization to Persons*** .

Perform this task when you want to set authentications for multiple cards of one access control point (door).

Steps

1. Click **Access Control → Advanced Function → Multi-Factor Auth** .
2. Select an access control device in device list on the left panel.
3. Add a person/card group for the access control device.
   1) Click **Add** on the right panel.
   2) Create a name for the group as desired.
   3) Specify the start time and end time of the effective period for the person/card group.
   4) Select members(s) and card(s) in the Available list, and the selected member(s) and card(s) will be added to the Selected list.

   Note

   Make sure you have issue card to the person.
   Make sure you have set access group and apply the access group to the access control device successfully.

   5) Click **Save**.
   6) **Optional:** Select the person/card group(s), and then click **Delete** to delete it(them).
   7) **Optional:** Select the person/card group(s), and then click **Apply** to re-apply access group that failed to be applied previously to the access control device.
4. Select an access control point (door) of selected device on the left panel.
5. Enter the maximum interval when entering password.
6. Add an authentication group for the selected access control point.
   1) Click **Add** on the Authentication Groups panel.
   2) Select a configured template as the authentication template from the drop-down list.

   Note

   For setting the template, refer to ***Configure Schedule and Template*** .

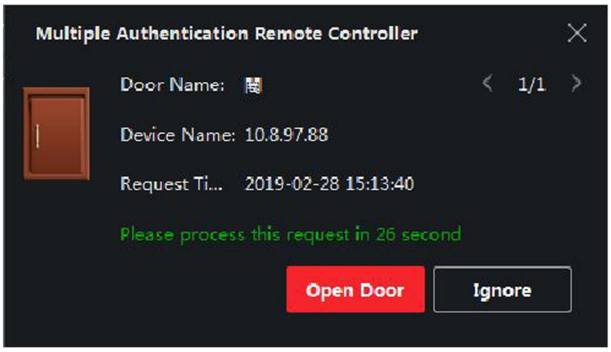
   3) Select the authentication type as **Local Authentication**, **Local Authentication and Remotely Open Door**, or **Local Authentication and Super Password** from the drop-down list.

   Local Authentication

   Authentication by the access control device.

   Local Authentication and Remotely Open Door

   Authentication by the access control device and by the client. When the person swipes the card on the device, a window will pop up. You can unlock the door via the client.



Multiple Authentication Remote Controller

Door Name:

Device Name: 10.8.97.88

Request Ti... 2019-02-28 15:13:40

Please process this request in 26 second

Figure 7-1 Remotely Open Door

Note

You can check **Offline Authentication** to enable the super password authentication when the access control device is disconnected with the client.

Local Authentication and Super Password

Authentication by the access control device and by the super password.

4) Select the added person/card group in the left list below and it will be added to the Selected list on the right as the authentication group.

5) Click the added authentication group in the right list to set authentication times in the Auth Times column.

Note

- The authentication times should be larger than 0 and smaller than the added personnel quantity in the personnel group.
- The maximum value of authentication times is 16.

6) Click **Save**.

Note

- For each access control point (door), up to four authentication groups can be added.
- For the authentication group of which authentication type is **Local Authentication**, up to 8 person/card groups can be added to the authentication group.
- For the authentication group of which authentication type is **Local Authentication and Super Password** or **Local Authentication and Remotely Open Door**, up to 7 person/card groups can be added to the authentication group.

7. Click **Save**.

7.3.4 Configure Custom Wiegand Rule

Based on the knowledge of uploading rule for the third party Wiegand, you can set multiple customized Wiegand rules to communicate between the device and the third party card readers.

Before You Start

Wire the third party card readers to the device.

Steps

Note

- By default, the device disables the custom wiegand function. If the device enables the custom Wiegand function, all wiegand interfaces in the device will use the customized wiegand protocol.
- Up to 5 custom Wiegands can be set.
- For details about the custom Wiegand, see ***Custom Wiegand Rule Descriptions*** .

1. Click **Access Control → Advanced Function → Custom Wiegand** to enter the Custom Wiegand page.
2. Select a custom Wiegand on the left.
3. Create a Wiegand name.

   Note

   Up to 32 characters are allowed in the custom Wiegand name.
4. Click **Select Device** to select the access control device for setting the custom wiegand.
5. Set the parity mode according to the property of the third party card reader.

   Note

   - Up to 80 bits are allowed in the total length.
   - The odd parity start bit, the odd parity length, the even parity start bit and the even parity length range from 1 to 80 bit.
   - The start bit of the card ID, the manufacturer code, the site code, and the OEM should range from 1 to 80 bit.
6. Set output transformation rule.

   1) Click **Set Rule** to open the Set Output Transformation Rules window.

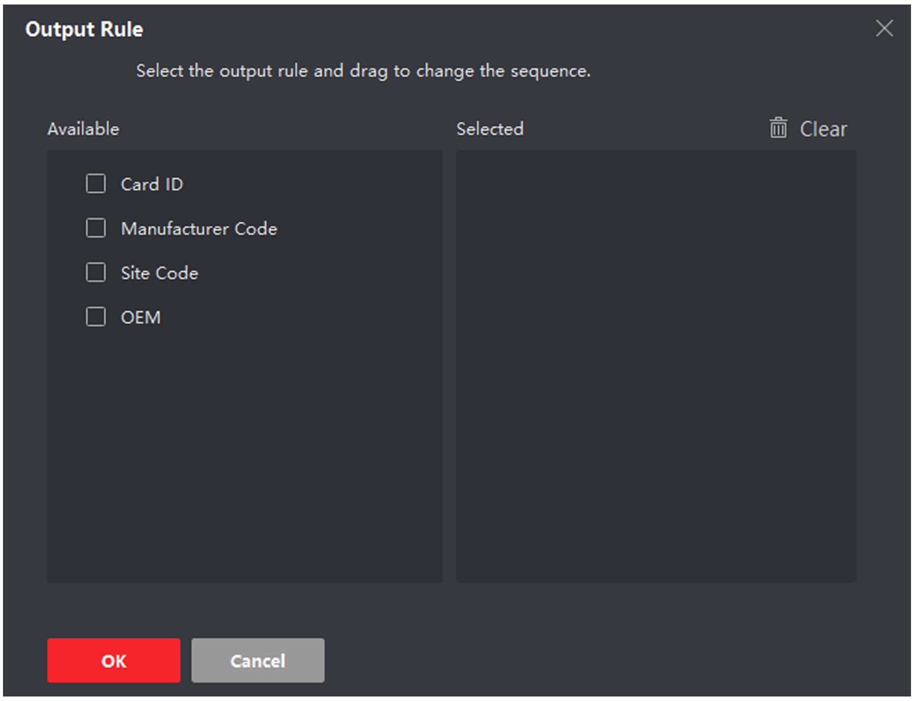


Figure 7-2 Set Output Transformation Rule

2) Select rules on the left list.

   The selected rules will be added to the right list.

3) **Optional:** Drag the rules to change the rule order.
4) Click **OK**.
5) In the Custom Wiegand tab, set the rule's start bit, length, and the decimal digit.

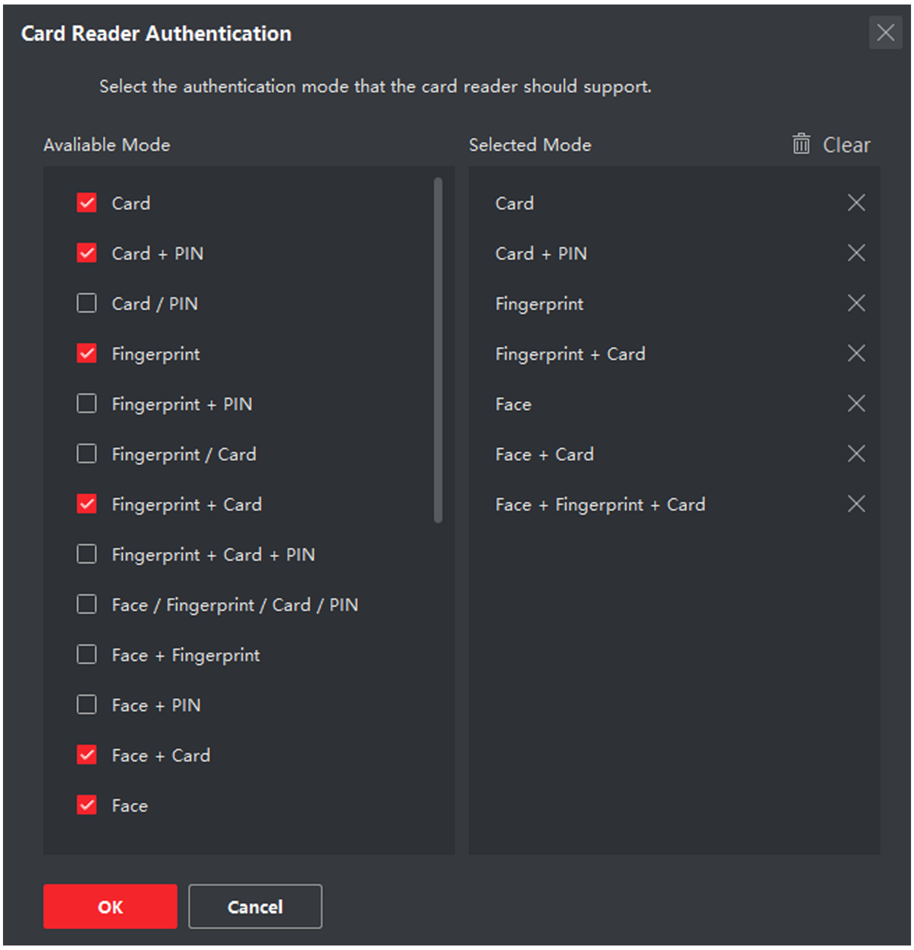
7. Click **Save**.

7.3.5 Configure Card Reader Authentication Mode and Schedule

You can set the passing rules for the card reader of the access control device according to your actual needs.

Steps

1. Click **Access Control → Advanced Function → Authentication** to enter the authentication mode configuration page.
2. Select a card reader on the left to configure.
3. Set card reader authentication mode.
   1) Click **Configuration**.



Card Reader Authentication

Select the authentication mode that the card reader should support.

Avaliable Mode

- ☑ Card
- ☑ Card + PIN
- ☐ Card / PIN
- ☑ Fingerprint
- ☐ Fingerprint + PIN
- ☐ Fingerprint / Card
- ☑ Fingerprint + Card
- ☐ Fingerprint + Card + PIN
- ☐ Face / Fingerprint / Card / PIN
- ☐ Face + Fingerprint
- ☐ Face + PIN
- ☑ Face + Card
- ☑ Face

Selected Mode

- Card
- Card + PIN
- Fingerprint
- Fingerprint + Card
- Face
- Face + Card
- Face + Fingerprint + Card

Figure 7-3 Select Card Reader Authentication Mode

Note

PIN refers to the PIN code set to open the door. Refer to ***Configure Access Control Information*** .

2) Check the modes in the Available Mode list and they will be added to the selected modes list.

3) Click **OK**.

After selecting the modes, the selected modes will display as icons with different color.

4. Click the icon to select a card reader authentication mode, and drag the cursor to draw a color bar on the schedule, which means in that period of time, the card reader authentication is valid.

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

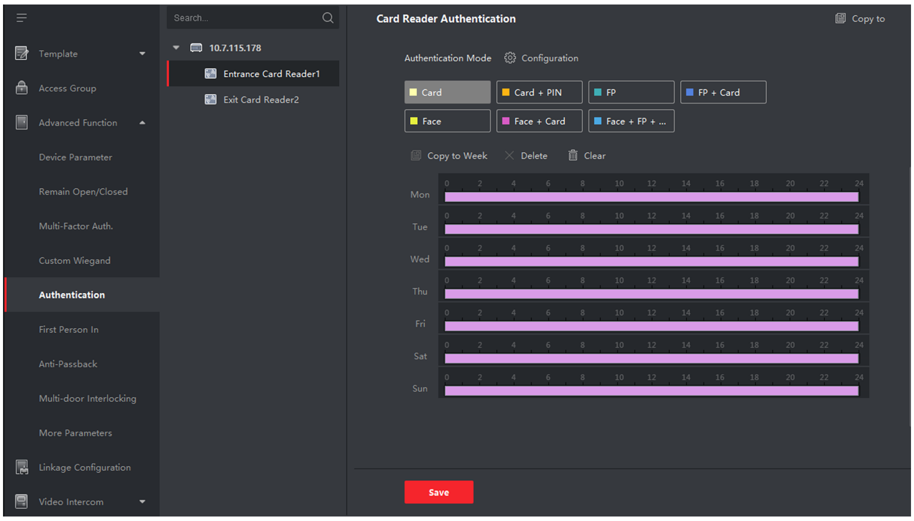


Figure 7-4 Set Authentication Modes for Card Readers

6. **Optional:** Select a configured day and click **Copy to Week** to copy the same settings to the whole week.
7. **Optional:** Click **Copy to** to copy the settings to other card readers.
8. Click **Save**.

7.3.6 Configure Person Authentication Mode

You can set the passing rules for person to the specified the access control device according to your actual needs.

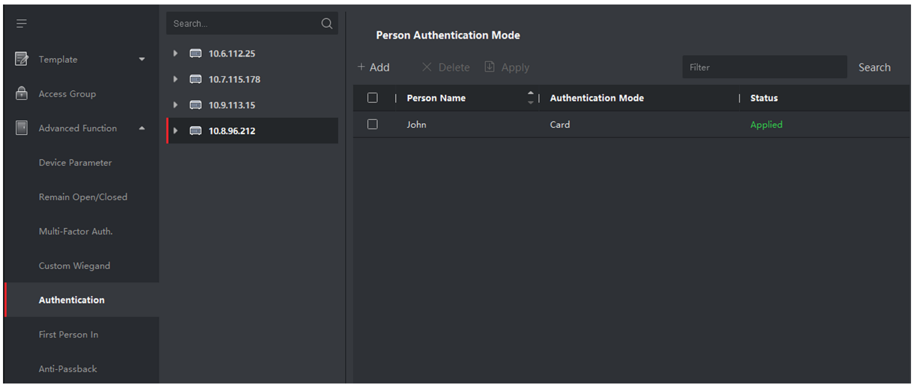
Before You Start

Make sure the access control device support the function of person authentication.

Steps

1. Click **Access Control → Advanced Function → Authentication** .
2. Select an access control device (support the function of person authentication) on the left panel to enter the person Authentication Mode page.
3. Click **Add** to enter the Add window.
4. Select the person(s) need to be configured on the left panel.

   The selected person(s) will be added to the right panel.
5. Select the authentication mode on the drop-down list of **Authentication Mode**.
6. Click **OK**.



	Person Name	Authentication Mode	Status
□	John	Card	Applied

Figure 7-5 Set Authentication Modes for Persons

7. **Optional:** Select person(s) on the Person Authentication mode page, and then click **Apply** to apply the person authentication mode to the device.

Note

Person authentication has higher priority than other authentication mode. When the access control device has been configured person authentication mode, the person should authenticate on this device via person authentication mode.

7.3.7 Configure Relay for Elevator Controller

For elevator controller, you can manage the relationship between the floor and the relay and configure the floor's relay type. Different relay type can implement different functions. By configuring the relationship between the floor and the relay, you can assign different functions to the elevator and control the elevator.

Configure Relationship between Relay and Floor

You can assign different relay types to the target floors, and each floor can be assigned with 3 relay types. By this way, you can call the elevator, and assign the operations for different floors.

Before You Start

Add the elevator controller to the client.

Steps

1. Click **Access Control → Advanced Function → Elevator Configuration** to enter the Relay Settings page.
2. Select an elevator controller on the left.
3. Select an unconfigured relay in the Unconfigured Relay panel on the right.

   There are three types of relay available.

   Button

Control the validity for buttons of each floor.

Note

🟥 represents button relay.

Call Elevator

Control to call the elevator to go to the specified floor by indoor station or outdoor station.

Note

🟧 represents the call elevator relay.

Auto

Control to press the button when the user swipes card inside the elevator. The button of the floor will be pressed automatically according to the user's permission.

Note

🟦 represents the auto button relay.

Example

Take the following picture as an example. In the number 1-2, 1 represents the distributed elevator controller number, 2 represents the relay, and the icon 🟥 represents the relay type. You can change the relay type. For details, refer to ***Configure Relay Type*** .

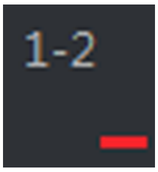
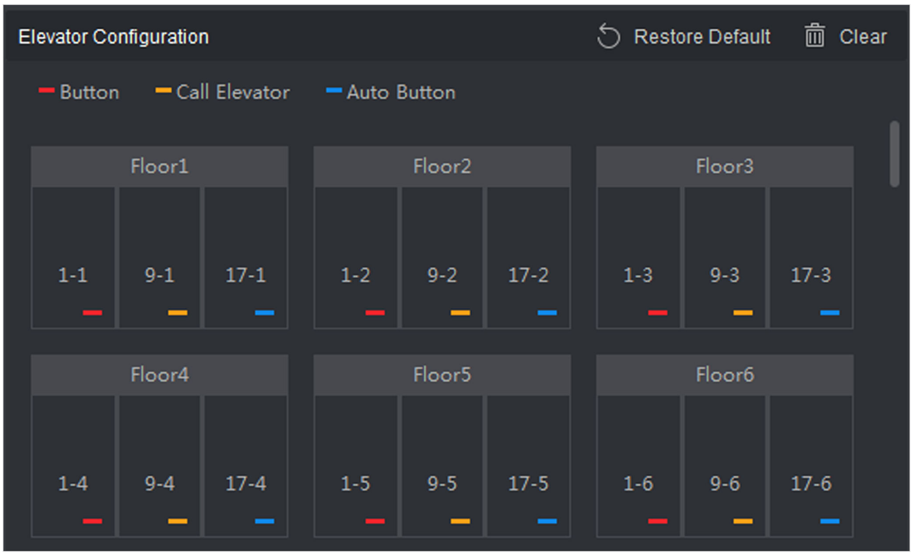


Figure 7-6 Relay

4. Configure the relationship between the relays and the floors.
- Drag the unconfigured relay from the Unconfigured Relay panel to the target floor in the Floor List panel.
- Drag the relay from the Floor List panel to the Unconfigured Relay panel.
- Drag the relay from one floor to another floor in the Floor List panel. If the target floor has already configured with a relay of the same type as the dragged one, it will replace the existed one of the same type.



Elevator Configuration

Restore Default Clear

🟥 Button 🟨 Call Elevator 🟦 Auto Button

Floor1			Floor2			Floor3		
1-1	9-1	17-1	1-2	9-2	17-2	1-3	9-3	17-3
🟥	🟨	🟦	🟥	🟨	🟦	🟥	🟨	🟦
Floor4			**Floor5**			**Floor6**		
1-4	9-4	17-4	1-5	9-5	17-5	1-6	9-6	17-6
🟥	🟨	🟦	🟥	🟨	🟦	🟥	🟨	🟦

Figure 7-7 Relationship between Relay and Floor

Note

- An elevator controller can link to up to 24 distributed elevator controllers. A distributed elevator controller can link up to 16 relays.
- By default, the relay total amount is the added floor number *3 (three types of relay).
- Up to 3 types of relay can be dragged to one floor.
- If you change the floor number in the door group management, all relays in the Relay Settings interface will restore to the default settings.

5. Click **Save** to apply the settings to the selected elevator controller.

Configure Relay Type

To implement different functions, you can configure different relay type, including: button relay, call elevator relay and auto button relay. Different relay type can implement different functions. The button relay is to control the validity for buttons of each floor.. The call elevator relay is to call the elevator to the specified floor by indoor station or outdoor station. The auto button relay is to control to press the button when the user swipes card inside the elevator, the button of the floor will be pressed automatically according to the user's permission.

Steps

1. Click **Access Control → Advanced Function → Elevator Configuration** to enter the Relay Settings page.
2. Select an elevator controller on the left of the page.
3. Click **Relay Type Settings** to open the Relay Type Settings window.

Note

- All relays in the Relay Type Settings window are unconfigured relays.
- Three types of relay are available: 🟥 represents the button relay, 🟧 represents the call elevator relay, and 🟦 represents the auto button relay.

4. Drag the relay from one relay type panel to the target one.

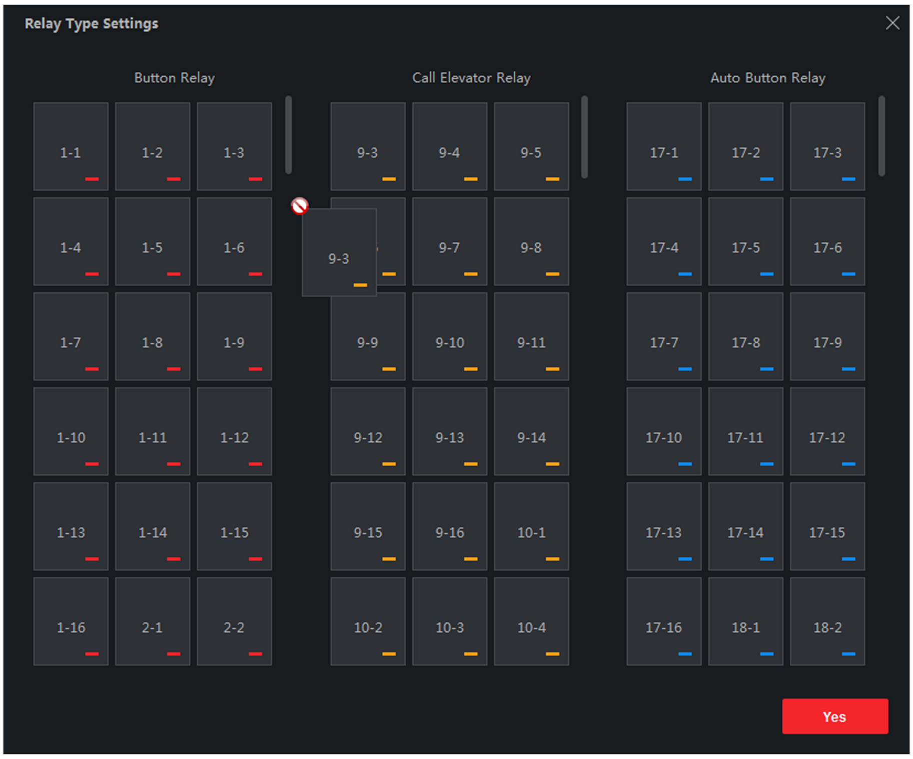


Figure 7-8 Configure Relay Type

5. Click **OK**.

7.3.8 Configure First Person In

You can set multiple first persons for one access control point. After the first person is authorized, it allows multiple persons access the door or other authentication actions.

Before You Start

Set the access group and apply the access group to the access control device. For details, refer to ***Set Access Group to Assign Access Authorization to Persons*** .

Perform this task when you want to configure opening door with first person.

Steps

1. Click **Access Control → Advanced Function → First Person In** to enter the First Person In page.
2. Select an access control device in the list on the left panel.

3. Select the current mode as **Enable Remaining Open after First Person**, **Disable Remaining Open after First Person**, or **Authorization by First Person** from the drop-down list for each access control point of the selected device.

   Enable Remaining Open after First Person

   The door remains open for the configured time duration after the first person is authorized until the remain open duration ends. If you select this mode, you should set the remain open duration.

   Note

   The remain open duration should be between 0 and 1440 minutes. By default, the remain open duration is 10 minutes.

   Disable Remaining Open after First Person

   Disable the function of first person in, namely normal authentication.

   Authorization by First Person

   All authentications (except for the authentications of super card, super password, duress card, and duress code) are allowed only after the first person authorization.

   Note

   You can authenticate by the first person again to disable the first person mode.

4. Click **Add** on the First Person List panel.
5. Select person(s) in the left list and the person(s) will be add to the selected persons as the first person(s) of the doors.

   The added first person(s) will list in the First Person List
6. **Optional:** Select a first person from the list and click **Delete** to remove the person from the first person list.
7. Click **Save**.

7.3.9 Configure Anti-Passback

You can set to only pass the access control point according to the specified path and only one person could pass the access control point after swiping the card.

Before You Start

Enable the anti-passing back function of the access control device.

Perform this task when you want to configure the anti-passing back for the access control device.

Steps

Note

Either the anti-passing back or multi-door interlocking function can be configured for an access control device at the same time. For the configuration of multi-door interlocking, refer to ***Configure Multi-door Interlocking*** .

1. Click **Access Control → Advanced Function → Anti-Passback** to enter the Anti-Passpack Settings page.
2. Select an access control device on the left panel.
3. Select a card reader as the beginning of the path in the **First Card Reader** field.
4. Click ✎ of the selected first card reader in the **Card Reader Afterward** column to open the select card reader dialog.
5. Select the afterward card readers for the first card reader.

   Note

   Up to four afterward card readers can be added as afterward card readers for one card reader.
6. Click **OK** in the dialog to save the selections.
7. Click **Save** in the Anti-Passback Settings page to save the settings and take effect.

Example

Set Card Swiping Path

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 point by swiping the card in the order as Reader In_01, Reader In_02 and Reader Out_04.

7.3.10 Configure Multi-door Interlocking

You can set the multi-door interlocking between multiple doors of the same access control device. 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.

Perform this task when you want to realize interlocking between multiple doors.

Steps

Note

- Multi-door Interlocking function is only supported by the access control device 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 control device at the same time. For the configuration of anti-passing back function, refer to ***Configure Anti-Passback*** .

1. Click **Access Control → Advanced Function → Multi-door Interlocking** .
2. Select an access control device on the left panel.

3. Click **Add** on the Multi-door Interlocking List panel to open Add Access Control Point to open the Add window.
4. Select at least two access control points(doors) from the list.

   Note

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

5. Click **OK** to add the selected access control point(s) for interlocking.

   The configured multi-door interlocking combination will list on the Multi-door Interlocking List panel.
6. **Optional:** Select an added multi-door interlocking combination from the list and click **Delete** to delete the combination.
7. Click **Apply** to apply the settings to the access control device.

7.4 Configure Other Parameters

After adding the access control device, you can set its parameters such as network parameters, capture parameters, RS-485 parameters, Wiegand parameters, etc.

7.4.1 Set Multiple NIC Parameters

If the device supports multiple network interfaces, you can set the network parameters of these NICs via the client, such as IP address, MAC address, port number, etc.

Steps

Note

This function should be supported by the device.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and click **NIC** to enter Multiple NIC Settings page.
4. Select an NIC you want to configure from the drop-down list.
5. Set its network parameters such as IP address, default gateway, subnet mask, etc.

   MAC Address

   A media access control address (MAC address) is a unique identifier assigned to the network interface for communications on the physical network segment.

   MTU

   The maximum transmission unit (MTU) of the network interface.
6. Click **Save**.

7.4.2 Set Network Parameters

After adding the access control device, you can set the device log uploading mode, and create EHome account via wired or wireless network.

Set Log Uploading Mode

You can set the mode for the device to upload logs via EHome protocol.

Steps

Note

Make sure the device is not added by EHome.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and enter **Network → Uploading Mode** .
4. Select the center group from the drop-down list.
5. Check **Enable** to enable to set the uploading mode.
6. Select the uploading mode from the drop-down list.
   - Enable **N1** or **G1** for the main channel and the backup channel.
   - Select **Close** 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 **Save**.

Create EHome Account in Wired Communication Mode

You can set the account for EHome protocol in wired communication mode. Then you can add devices via EHome protocol.

Steps

Note

- This function should be supported by the device.
- Make sure the device is not added by EHome.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and enter **Network → Network Center** .
4. Select the center group from the drop-down list.
5. Select the **Address Type** as **IP Address** or **Domain Name**.

6. Enter IP address or domain name according to the address type.
7. Enter the port number for the protocol.

Note

The port number of the wireless network and wired network should be consistent with the port number of EHome.

8. Select the **Protocol Type** as **EHome**.
9. Set an account name for the network center.
10. Click **Save**.

Create EHome Account in Wireless Communication Mode

You can set the account for EHome protocol in wireless communication mode. Then you can add devices via EHome protocol.

Steps

Note

- This function should be supported by the device.
- Make sure the device is not added by EHome.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and enter **Network → Wireless Communication Center** .
4. Select the **APN Name** as **CMNET** or **UNINET**.
5. Enter the SIM Card No.
6. Select the center group from the drop-down list.
7. Enter the IP address and port number.

Note

- By default, the port number for EHome is ***7660***.
- The port number of the wireless network and wired network should be consistent with the port number of EHome.

8. Select the **Protocol Type** as **EHome**.
9. Set an account name for the network center.
10. Click **Save**.

7.4.3 Set Device Capture Parameters

You can configure the capture parameters of the access control device, including manual capture and event triggered capture.

Note

- The capture function should be supported by the device.
- Before setting the capture parameters, you should set the picture storage first to define where the event triggered pictures are saved. For details, refer to ***Set Picture Storage*** .

Set Triggered Capture Parameters

When an event occurs, the camera of the access control device can be triggered to capture picture(s) to record what happens when the event occurs. You can view the captured pictures when checking the event details in Event Center. Before that, you need to set the parameters for the capture such as number of pictures captured for one time.

Before You Start

Before setting the capture parameters, you should set the picture storage first to define where the captured pictures are saved. For details, refer to ***Set Picture Storage*** .

Steps

Note

This function should be supported by the device

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters → Capture** .
3. Select an access control device in the device list and select **Linked Capture**.
4. Set the picture size and quality.
5. Set the capture times once triggered which defines how many pictures will be captures for one time.
6. If the capture times is more than 1, set the interval for each capture.
7. Click **Save**.

Set Manual Capture Parameters

In Status Monitoring module, you can capture a picture manually the access control device's camera by clicking a button. Before that, you need to set the parameters for the capture such as picture quality.

Before You Start

Before setting the capture parameters, you should set the saving path first to define where the captured pictures are saved. For details, refer to ***Set File Saving Path*** .

Steps

Note

This function should be supported by the device

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters → Capture** .
3. Select an access control device in the device list and select **Manual Capture**.
4. Select the resolution of the captured pictures from the drop-down list.
5. Select the picture quality as **High**, **Medium**, or **Low**. The higher the picture quality is, the larger size the picture will be.
6. Click **Save**.

7.4.4 Set Parameters for Face Recognition Terminal

For face recognition terminal, you can set its parameters including face picture database, QR code authentication, etc.

Steps

Note

This function should be supported by the device.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and click **Face Recognition Terminal**.
4. Set the parameters.

   Note

   These parameters displayed vary according to different device models.

   COM

   Select a COM port for configuration. COM1 refers to the RS-485 interface and COM2 refers to the RS-232 interface.

   Face Picture Database

   select Deep Learning as the face picture database.

   Authenticate by QR Code

   If enabled, the device camera can scan the QR code to authenticate. By default, the function is disabled.

   Blacklist Authentication

   If enabled, the device will compare the person who want to access with the persons in the blacklist.

If matched (the person is in the blacklist), the access will be denied and the device will upload an alarm to the client.

If mismatched (the person is not in the blacklist), the access will be granted.

Save Authenticating Face Picture

If enabled, the captured face picture when authenticating will be saved on the device.

MCU Version

View the device MCU version.

5. Click **Save**.

7.4.5 Enable M1 Card Encryption

M1 card encryption can improve the security level of authentication.

Steps

Note

The function should be supported by the access control device and the card reader.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and click **M1 Card Encryption** to enter the M1 Card Encryption page.
4. Set the switch to on to enable the M1 card encryption function.
5. Set the sector ID.

   The sector ID ranges from 1 to 100.
6. Click **Save** to save the settings.

7.4.6 Set RS-485 Parameters

You can set the access control device's RS-485 parameters including the baud rate, data bit, the stop bit, parity type, flow control type, communication mode, work mode, and connection mode.

Steps

Note

The RS-485 Settings should be supported by the device.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and click **RS-485** to enter the RS-485 Settings page.
4. Select the serial port number from the drop-down list to set the RS-485 parameters.

5. Set the baud rate, data bit, the stop bit, parity type, communication mode, working mode, and connection mode in the drop-down list.
6. Click **Save**.
   - The configured parameters will be applied to the device automatically.
   - After changing the working mode or connection mode, the device will reboot automatically.

7.4.7 Set Wiegand Parameters

You can set the access control device's Wiegand channel and the communication mode. After setting the Wiegand parameters, the device can connect to Wiegand card reader via Wiegand communication.

Steps

Note

This function should be supported by the device.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and click **Wiegand** to enter the Wiegand Settings page.
4. Set the switch to on to enable the Wiegand function for the device.
5. Select the Wiegand channel No. and the communication mode from the drop-down list.

   Note

   If you set **Communication Direction** as **Sending**, you are required to set the **Wiegand Mode** as **Wiegand 26** or **Wiegand 34**.
6. Click **Save**.
   - The configured parameters will be applied to the device automatically.
   - After changing the communication direction, the device will reboot automatically.

7.4.8 Set Attendance Status

You can set the attendance mode on the device via the client. You can also set the attendance parameters as check in, check out, break out, break in, overtime in, and overtime out on the device according to your actual needs.

Note

This function should be supported by the device.

Disable Attendance Mode

Disable the attendance mode and the system will not display the attendance status on the device initial page.

Before You Start
Add at least one person, and set the person's authentication mode. For details, see ***Person Management*** .

Steps

1. Click **Access Control → Advanced Function → More Parameters** to enter the More Parameters page.
2. Select a device from the left panel.
3. Click **Attendance Status**.
4. Set the attendance mode as **Disable**.
5. Click **Save**.

Result

The attendance status function is disabled, and you will not view or configure the attendance status on the device initial page.

Set Manual Attendance

Set the attendance mode as manual, and you can select a status manually when you take attendance on the device.

Before You Start
Add at least one person, and set the person's authentication mode. For details, see ***Person Management*** .

Steps

1. Click **Access Control → Advanced Function → More Parameters** to enter the More Parameters page.
2. Select a device from the left panel.
3. Click **Attendance Status**.
4. Set the attendance mode as **Manual**.
5. Make sure **Attendance Status Required** is enabled.

   Note

   By default, **Attendance Status Required** is enabled.
6. Set shortcut key from the drop-down list for the attendance status.
7. Click **Save**.

Result

Press a key on the device keypad to select an attendance status and authenticate. The authentication will be marked as the configured attendance status according to the defined shortcut key.

Or when you authenticate on the device initial page, you will enter the Select Status page. Select a status to take attendance.

Note

If you do not select a status for about 20 s, the authentication will be failed and it will not be marked as a valid attendance.

Set Auto Attendance

Set the attendance mode as auto, and you can set the attendance status and its available time duration. The system will auto change the attendance status according to the configured parameters.

Before You Start

Add at least one person, and set the person's authentication mode. For details, see ***Person Management*** .

Steps

1. Click **Access Control → Advanced Function → More Parameters** to enter the More Parameters page.
2. Select a device from the left panel.
3. Click **Attendance Status**.
4. Set the attendance mode as **Auto**.
5. Make sure **Attendance Status Required** is enabled.

   Note

   By default, **Attendance Status Required** is enabled.
6. Set available time for the target attendance status.
   1) Move the cursor on the target time and the enable checkbox will display.
   2) Check the checkbox and set the available time.
   3) Click anywhere on the page to confirm the settings. The configured time will be displayed in white.
7. Set shortcut key from the drop-down list for the attendance status.
8. Click **Save**.

   The attendance status will be valid within the configured time duration.

Result

Enter the device initial page, the current attendance mode will be displayed on the page. When you authenticate on the initial page, the authentication will be marked as the configured attendance status according to the configured time.

Example
If set the Up key as check in and the Down key as check out, and set the check in's schedule as Monday 08:00, and check out's schedule as Monday 17:00, the valid person's authentication before 17:00 on Monday will be marked as check in. And the valid person's authentication after 17:00 on Monday will be marked as check out.

Set Manual and Auto Attendance

Set the attendance mode as manual and auto and the device system will auto change the attendance status according to the configured parameters. At the same time you can manually change the attendance status before the authentication.

Before You Start
Add at least one person, and set the person's authentication mode. For details, see ***Person Management*** .

Steps

1. Click **Access Control → Advanced Function → More Parameters** to enter the More Parameters page.
2. Select a device from the left panel.
3. Click **Attendance Status**.
4. Set the attendance mode as **Manual and Auto**.
5. Make sure **Attendance Status Required** is enabled.

   Note

   By default, **Attendance Status Required** is enabled.

6. Set status lasts time.
7. Set available time for the target attendance status.
   1) Move the cursor on the target time and the enable checkbox will display.
   2) Check the checkbox and set the available time.
   3) Click anywhere on the page to confirm the settings. The configured time will be displayed in white.
8. Set shortcut key from the drop-down list for the attendance status.
9. Click **Save**.

   The attendance status will be valid within the configured time duration.

Result

Enter the device initial page, the current attendance mode will be displayed on the page. If you do not select a status, the authentication will be marked as the configured attendance status according to the configured time. If you press the key on the keypad, and select a status to take attendance, the authentication will be marked as the selected attendance status.

Example

If set the Up key as check in and the Down key as check out, and set the check in's time as Monday 08:00, and check out's time as Monday 17:00, the valid person's authentication before 17:00 on Monday will be marked as check in. And the valid person's authentication after 17:00 on Monday will be marked as check out.

7.5 Configure Linkage Actions for Access Control

The events triggered by the access control devices, doors, card readers, and alarm inputs, as well as the card swiping of persons, mobile terminal's MAC address detected, and employee No. detected, can trigger a series of linkage actions to notify the security personnel and record the events.

Two types of linkage actions are supported: client actions and device actions.

- **Client Actions:** When the event is detected, it will trigger the actions on the client, such as the client playing alarm sound and sending an email to notify the security personnel.
- **Device Actions:** When the event is detected, it will trigger the actions of this device, such as buzzing, door open/closed, audio play, etc., to notify the security personnel and allow/forbid access.

7.5.1 Configure Client Actions for Access Event

Even if you are far away from an access point, you can still know what happens and how urgent the event is by configuring linked actions of access event on the client. You will be notified on the client once an event is triggered, so that you can response to the event instantly. You can also configure client actions of access points in a batch at a time.

Steps

Note

The linkage actions here refer to the linkage of the client software's own actions such as audible warning, email linkage, etc.

1. Click **Event Management → Access Control Event** .

   The added access control devices will display in the device list.
2. Select a resource (including device, alarm input, door/elevator, and card reader) from the device list.

The event types which the selected resource supports will display.

3. Select the event(s) and click **Edit Priority** to define the priority for the event(s), which can be used to filter events in the Event Center.
4. Set the linkage actions of the event.
   1) Select the event(s) and click **Edit Linkage** to set the client actions when the events triggered.

      Audible Warning

      The client software gives an audible warning when alarm is triggered. You can select the alarm sound for audible warning.

      Note

      For setting the alarm sound, please refer to ***Set Alarm Sound*** .

      Send Email

      Send an email notification of the alarm information to one or more receivers.

      For details about setting email parameters, refer to ***Set Email Parameters*** .
   2) Click **OK**.
5. Enable the event so that when the event is detected, en event will be sent to the client and the linkage actions will be triggered.
6. **Optional:** Click **Copy to...** to copy the event settings to other access control device, alarm input, door/elevator, or card reader.

7.5.2 Configure Device Actions for Access Event

You can set the access control device's linkage actions for the access control device's triggered event. When the event is triggered, it can trigger the alarm output, host buzzer, and other actions on the same device.

Steps

Note

It should be supported by the device.

1. Click **Access Control → Linkage Configuration** .
2. Select the access control device from the list on the left.
3. Click **Add** button to add a new linkage.
4. Select the event source as **Event Linkage**.
5. select the event type and detailed event to set the linkage.
6. In the Linkage Target area, set the property target to enable this action.

   Buzzer on Controller

   The audible warning of access control device will be triggered.

   Capture

   The real-time capture will be triggered.

Recording

The recording will be triggered.

Note

The device should support recording.

Buzzer on Reader

The audible warning of card reader will be triggered.

Alarm Output

The alarm output will be triggered for notification.

Alarm Input

Arm or disarm the alarm input.

Note

The device should support alarm input function.

Access Point

The door status of open, close, remain open, and remain close will be triggered.

Note

The target door and the source door cannot be the same one.

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

7. Click **Save**.
8. **Optional:** After adding the device linkage, you can do one or more of the following:

Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.
Delete Linkage Settings	Select the configured linkage settings in the device list and click **Delete** to delete it.

7.5.3 Configure Device Actions for Card Swiping

You can set the access control device's linkage actions for the specified card swiping. When you swipe the specified card, it can trigger the alarm output, host buzzer, and other actions on the same device.

Steps

Note

It should be supported by the device.

1. Click **Access Control → Linkage Configuration** .
2. Select the access control device from the list on the left.
3. Click **Add** button to add a new linkage.
4. Select the event source as **Card Linkage**.
5. Enter the card number or select the card from the dropdown list.
6. Select the card reader where the card swipes to trigger the linked actions.
7. In the Linkage Target area, set the property target to enable this action.

   Buzzer on Controller

   The audible warning of access control device will be triggered.

   Buzzer on Reader

   The audible warning of card reader will be triggered.

   Capture

   The real-time capture will be triggered.

   Recording

   The recording will be triggered.

   Note

   The device should support recording.

   Alarm Output

   The alarm output will be triggered for notification.

   Alarm Input

   Arm or disarm the alarm input.

   Note

   The device should support alarm input function.

   Access Point

   The door status of open, close, remain open, or remain closed will be triggered.

   Audio Play

   The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.
8. Click **Save**.

   When the card (configured in Step 5) swipes on the card reader (configured in Step 6), it can trigger the linked actions (configured in step 7).

9. **Optional:** After adding the device linkage, you can do one or more of the following:

Delete Linkage Settings	Select the configured linkage settings in the device list and click **Delete** to delete it.
Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.

7.5.4 Configure Device Linkage for Mobile Terminal's MAC Address

You can set the access control device's linkage actions for the specified MAC address of mobile terminal. When access control device detects the specified MAC address, it can trigger the alarm output, host buzzer, and other actions on the same device.

Steps

Note

It should be supported by the device.

1. Click **Access Control → Linkage Configuration** .
2. Select the access control device from the list on the left.
3. Click **Add** button to add a new linkage.
4. Select the event source as **Mac Linkage**.
5. Enter the MAC address to be triggered.

   Note

   MAC Address Format: AA:BB:CC:DD:EE:FF.

6. In the Linkage Target area, set the property target to enable this action.

   Buzzer on Controller

   The audible warning of access control device will be triggered.

   Buzzer on Reader

   The audible warning of card reader will be triggered.

   Capture

   The real-time capture will be triggered.

   Recording

   The recording will be triggered.

   Note

   The device should support recording.

   Alarm Output

   The alarm output will be triggered for notification.

Alarm Input

Arm or disarm the alarm input.

Note

The device should support alarm input function.

Access Point

The door status of open, close, remain open, or remain closed will be triggered.

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

7. Click **Save** to save the settings.
8. **Optional:** After adding the device linkage, you can do one or more of the following:

Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.
Delete Linkage Settings	Select the configured linkage settings in the device list and click **Delete** to delete it.

7.5.5 Configure Device Actions for Person ID

You can set the access control device's linkage actions for the specified person ID. When access control device detects the specified person ID, it can trigger the alarm output, host buzzer, and other actions on the same device.

Steps

Note

It should be supported by the device.

1. Click **Access Control → Linkage Configuration** .
2. Select the access control device from the list on the left.
3. Click **Add** button to add a new linkage.
4. Select the event source as **Person Linkage**.
5. Enter the employee number or select the person from the dropdown list.
6. Select the card reader where the card swipes to trigger the linked actions.
7. In the Linkage Target area, set the property target to enable this action.

Buzzer on Controller

The audible warning of access control device will be triggered.

Buzzer on Reader

The audible warning of card reader will be triggered.

Capture

The real-time capture will be triggered.

Recording

The recording will be triggered.

Note

The device should support recording.

Alarm Output

The alarm output will be triggered for notification.

Alarm Input

Arm or disarm the alarm input.

Note

The device should support zone function.

Access Point

The door status of open, close, remain open, or remain closed will be triggered.

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

8. Click **Save**.
9. **Optional:** After adding the device linkage, you can do one or more of the following:

Delete Linkage Settings	Select the configured linkage settings in the device list and click **Delete** to delete it.
Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.

7.6 Door/Elevator Control

In Monitoring module, you can view the real-time status of the doors or elevators managed by the added access control device. You can also control the doors and elevators such as open/close the door, or remain the door open/closed via the client remotely. The real-time access event are displayed in this module. You can view the access details and person details.

Note

For the user with door/elevator control permission, the user can enter the Monitoring module and control the door/elevator. Or the icons used for control will not show. For setting the user permission, refer to ***Add User*** .

7.6.1 Control Door Status

You can control the status for a single door, including opening door, closing door, remaining the door open, and remaining the door closed.

Steps

1. Click **Monitoring** to enter the status monitoring page.
2. Select an access point group on the upper-right corner.

   Note

   For managing the access point group, refer to ***Group Management*** .

   The doors in the selected access control group will display.
3. Click a door icon to select a door, or press **Ctrl** and select multiple doors.
4. Click the following buttons to control the door.

   Open Door

   When the door is locked, unlock it and it will be open for once. After the open duration, the door will be closed and locked again automatically.

   Close Door

   When the door is unlocked, lock it and it will be closed. The person who has the access authorization can access the door with credentials.

   Remain Open

   The door will be unlocked (no matter closed or open). All the persons can access the door with no credentials required.

   Remain Closed

   The door will be closed and locked. No person can access the door even if he/she has the authorized credentials, except the super users.

   Capture

   Capture a picture manually.

   Note

   The **Capture** button is available when the device supports capture function. The picture is saved in the PC running the client. For setting the saving path, refer to ***Set File Saving Path*** .

Result

The icon of the doors will change in real-time according to the operation if the operation is succeeded.

7.6.2 Control Elevator Status

You can control the elevator status of the added elevator controller, including opening elevator's door, controlled, free, calling elevator, etc.

Steps

Note

- You can control the elevator via the current client if it is not armed by other client. The elevator cannot be controlled by other client software if the elevator status changes.
- Only one client software can control the elevator at one time.
- The client which has controlled the elevator can receive the alarm information and view the elevator real-time status.

1. Click **Monitoring** to enter the status monitoring page.
2. Select an access point group on the upper-right corner.

   Note

   For managing the access point group, refer to ***Group Management*** .

   The elevators in the selected access point group will display.
3. Click a door icon to select an elevator.
4. Click the following buttons to control the elevator.

   Open Door

   When the elevator's door is closed, open it. After the open duration, the door will be closed again automatically.

   Controlled

   You should swipe the card before pressing the target floor button. And the elevator can go to the target floor.

   Free

   The selected floor's button in the elevator will be valid all the time.

   Disabled

   The selected floor's button in the elevator will be invalid and you cannot go to the target floor.

Result

The icon of the doors will change in real-time according to the operation if the operation is succeeded.

7.6.3 Check Real-Time Access Records

The access records will display in real time, including card swiping records, face recognitions records, fingerprint comparison records, etc. You can view the person information and view the picture captured during access.

Steps

1. Click **Monitoring** and select a group from the drop-down list on the upper-right corner.

   The access records triggered at the doors in the selected group will display in real time. You can view the details of the records, including card No., person name, organization, event time, etc.
2. **Optional:** Check the event type and event status so that these events will show in the list if the events are detected. The events of unchecked type or status will not be displayed in the list.
3. **Optional:** Check **Show Latest Event** and the latest access record will be selected and displayed at the top of the record list.
4. **Optional:** Click the event to view the accessed person details, including person pictures (captured picture and profile), person No., person name, organization, phone, contact address, etc.

   Note

   You can double click the captured picture to enlarge it to view the details.
5. **Optional:** Right click on the column name of the access event table to show or hide the column according to actual needs.

Chapter 8 Time and Attendance

The Time and Attendance module provides multiple functionalities to track and monitor when employees start and stop work, and full control of employees working hours such as late arrivals, early departures, time taken on breaks and absenteeism.

Note

In this section, we introduce the configurations before you can getting the attendance reports. The access records recorded after these configurations will be calculated in the statistics.

8.1 Configure Attendance Parameters

You can configure the attendance parameters, including the general rule, overtime parameters, attendance check point, holiday, leave type, etc.

8.1.1 Configure General Rule

You can configure the general rule for attendance calculation, such as the week beginning, month beginning, weekend, absence, etc.

Steps

Note

The parameters configured here will be set as default for the newly added time period. It will not affect the existed one(s).

1. Enter Time & Attendance module.
2. Click **Attendance Settings → General Rule** .
3. Set the day as week beginning and the date as month beginning.
4. Select the day(s) as weekend.
5. Set absence parameters.
6. Click **Save**.

8.1.2 Configure Overtime Parameters

You can configure the overtime parameters for workday and weekend, including overtime level, work hour rate, attendance status for overtime, etc.

Steps

1. Enter Time & Attendance module.
2. Click **Attendance Settings → Overtime** .
3. Set required information.

Overtime Level for Workday

When you work for certain period after end-work time on workday, you will reach different overtime level: overtime level 1, overtime level 2 and overtime level 3 . You can set different work hour rate for three overtime levels, respectively.

Work Hour Rate

Set corresponding work hour rates for three overtime levels, which can be generally used to calculate total work hours.

Overtime Rule for Weekend

You can enable overtime rule for weekend and set calculation mode.

4. Click **Save**.

8.1.3 Configure Attendance Check Point

You can set the card reader(s) of the access point as the attendance check point, so that the authentication on the card readers will be recorded for attendance .

Before You Start

You should add access control device before configuring attendance check point. For details, refer to ***Add Device*** .

Steps

Note

By default, all card readers of the added access control devices are set as attendance checkpoint.

1. Enter the Time & Attendance module.
2. Click **Attendance Settings → Attendance Check Point** to enter the Attendance Check Point Settings page.
3. **Optional:** Set **Set All Card Readers as Check Points** switch to off.

   Only the card readers in the list will be set as the attendance check points.
4. Check the desired card reader(s) in the device list as attendance check point(s).
5. Set check point function as **Start/End-Work**, **Start-Work** or **End-Work**.
6. Click **Set as Check Point**.

   The configured attendance check point displays on the right list.

8.1.4 Configure Holiday

You can add the holiday during which the check-in or check-out will not be recorded.

Add Regular Holiday

You can configure a holiday which will take effect annually on regular days during the effective period, such as New Year's Day, Independence Day, Christmas Day, etc.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Settings → Holiday** to enter the Holiday Settings page.
3. Check **Regular Holiday** as holiday type.
4. Custom a name for the holiday.
5. Set the first day of the holiday.
6. Enter the number of the holiday days.
7. Set the attendance status if the employee works on holiday.
8. **Optional:** Check **Repeat Annually** to make this holiday setting effective every year.
9. Click **OK**.

   The added holiday will display in the holiday list and calendar.

   If the date is selected as different holidays, it will be recorded as the first-added holiday.
10. **Optional:** After adding the holiday, perform one of the following operations.

Edit Holiday	Click ✎ to edit the holiday information.
Delete Holiday	Select one or more added holidays, and click **Delete** to delete the holiday(s) from the holiday list.

Add Irregular Holiday

You can configure a holiday which will take effect annually on irregular days during the effective period, such as Bank Holiday.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Settings → Holiday** to enter the Holiday Settings page.
3. Click **Add** to open the Add Holiday page.
4. Check **Irregular Holiday** as holiday type.
5. Custom a name for the holiday.
6. Set the start date of the holiday.

   Example

   If you want to set the forth Thursday in November, 2019 as the Thanksgiving Day holiday, you should select 2019, November, 4th, and Thursday from the four drop-down lists.
7. Enter the number of the holiday days.
8. Set the attendance status if the employee works on holiday.
9. **Optional:** Check **Repeat Annually** to make this holiday setting effective every year
10. Click **OK**.

The added holiday will display in the holiday list and calendar.

If the date is selected as different holidays, it will be recorded as the first-added holiday.

11. **Optional:** After adding the holiday, perform one of the following operations.

Edit Holiday Click ✎ to edit the holiday information.

Delete Holiday Select one or more added holidays, and click **Delete** to delete the holiday(s) from the holiday list.

8.1.5 Configure Leave Type

You can customize the leave type (major leave type and minor leave type) according to actual needs. You can also edit or delete the leave type.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Settings → Leave Type** to enter the Leave Type Settings page.
3. Click **Add** on the left to add a major leave type.
4. **Optional:** Perform one of the following operations for major leave type.

   Edit Move the cursor over the major leave type and click ✎ to edit the major leave type.

   Delete Select one major leave type and click **Delete** on the left to delete the major leave type.
5. Click **Add** on the right to add a minor leave type.
6. **Optional:** Perform one of the following operations for minor leave type.

   Edit Move the cursor over the minor leave type and click ✎ to edit the minor leave type.

   Delete Select one or multiple major leave types and click **Delete** on the right to delete the selected minor leave type(s).

8.1.6 Synchronize Authentication Record to Third-Party Database

The attendance data recorded in client software can be used by other system for calculation or some other operations. You can enable synchronization function to apply the authentication record from client software to the third-party database automatically.

Steps

1. Enter Time & Attendance module.
2. Click **Attendance Settings → Third-Party Database** .
3. Set **Apply to Database** switch to on to enable synchronization function.
4. Set the required parameters of the third-party database, including database type, server IP address, database name, user name and password.

5. Set table parameters of database according to the actual configurations.
   1) Enter the table name of the third-party database.
   2) Set the mapped table fields between the client software and the third-party database.
6. Click **Connection Test** to test whether database can be connected.
7. Click **Save** to test whether database can be connected and save the settings for the successful connection.
   - The attendance data will be written to the third-party database.
   - During synchronization, if the client disconnects with the third-party database, the client will try to reconnect every 30 min. After reconnected, the client will synchronize the data recorded during the disconnected time period to the third-party database.

8.1.7 Configure Break Time

You can add break time and set start time, end time, duration, calculation mode and other parameters for the break. The added break time can also be edited or deleted.

Steps

1. Click **Time & Attendance → Timetable** .

   The added timetables are displayed in the list.
2. Select an added timetable or click **Add** to enter setting timetable page.
3. Click **Settings** in the break time area to enter break time management page.
4. Add break time.
   1) Click **Add**.
   2) Enter a name for the break time.
   3) Set related parameters for the break time.

      Start Time / End Time

      Set the time when the break starts and ends.

      No Earlier Than / No Later Than

      Set the earliest swiping time for starting break and the latest swiping time for ending break.

      Break Duration

      The duration from start time to end time of the break.

      Calculation

      Auto Deduct

      The fixed break duration will be excluded from work hours.

      Must Check

      The break duration will be calculated and excluded from work hours according to actual check-in and check-out time.

> **Note**
>
> If you select **Must Check** as calculation method, you need to set attendance status for late or early returning from break.

5. Click **Save** to save the settings.
6. **Optional:** Click **Add** to continue adding break time.

8.1.8 Configure Attendance Calculation Accuracy

To calculate the attendance data accurately, you can set the attendance calculation accuracy for different attendance items, including the minimum unit for attendance calculation and round-off control rule. For example, you can set the minimum unit as 1 hour for leave duration, and set the round-off control rule as round up.

Steps

1. Enter the Time and Attendance module.
2. Click **Attendance Settings → Advanced Function** to enter the Advanced Function page.
3. Set the minimum units for different statistic items.
4. Set the round-off control rules for different statistic items.
5. Click **Save**.

Example

Set the minimum unit as 1 hour and the round-off control rule as round down for overtime duration, and if the overtime duration is less than 1 hour, it will be calculated as 0. If the overtime duration is 1.5 hour, it will be calculated as 1 hour.

8.1.9 Configure Report Display

You can configure display contents displayed in the attendance report, such as the company name, logo, date format, time format, and mark.

Steps

1. Enter Time & Attendance module.
2. Click **Attendance Statistics → Report Display** .
3. Set the display settings for attendance report.

   Company Name

   Enter a company name to display the name in the report.

   Date Format / Time Format

   Set the date format and time format according to the actual needs.

   Attendance Status Mark in Report

   Enter the mark and select the color. The related fields of attendance status in the report will display with the mark and color.

Weekend Mark in Report

Enter the mark and select the color. The weekend fields in the report will display with the mark and color.

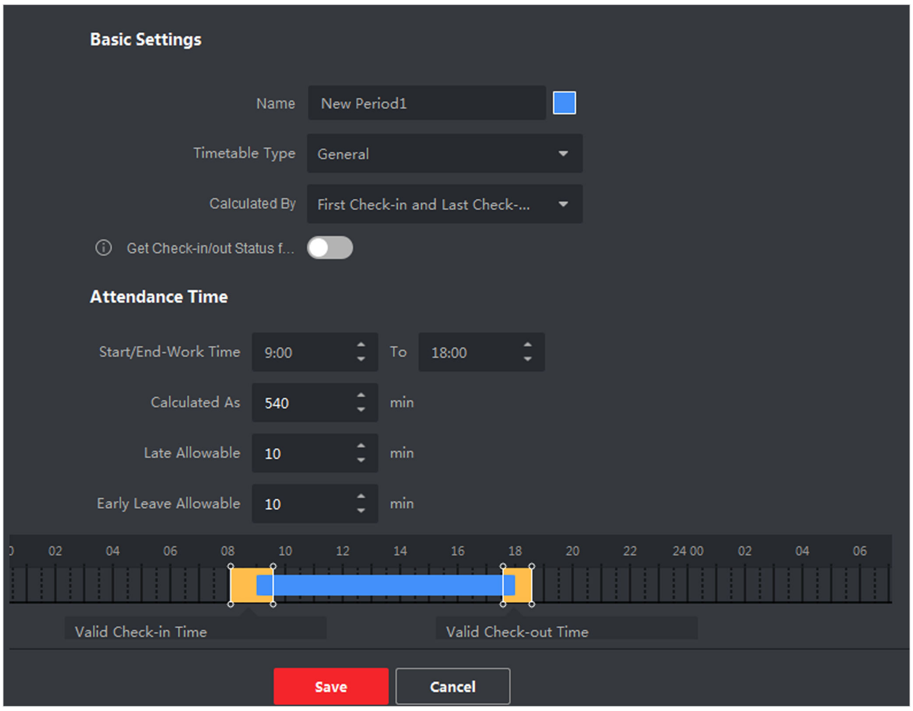
4. Click **Save**.

8.2 Add Timetable

On the timetable page, you can set the start-work time, end-work time and set attendance rules for being late and leaving early, etc.

Steps

1. Click **Time and Attendance → Timetable** to enter the timetable settings page.
2. Click **Add** to enter Basic Settings page.



Basic Settings

Name: New Period1

Timetable Type: General

Calculated By: First Check-in and Last Check-...

Get Check-in/out Status f...

Attendance Time

Start/End-Work Time: 9:00 To 18:00

Calculated As: 540 min

Late Allowable: 10 min

Early Leave Allowable: 10 min

Figure 8-1 Add Timetable

3. Create a name for the timetable.

Note

You can click the color icon beside the name to customize the color for the valid timetable on the time bar on the bottom of the page。

4. Select the timetable type.

General

Suitable for general attendance scene, which requires the fixed start-work time and end-work time, and you can set valid check-in/out time, allowable timetable for being late and leaving early.

Flexible

Suitable for man-hour shift, which does not requires the check-in/out time and only requires the staffs' working time (from the start time you set) is equal or greater than the predefined work hours.

5. Select calculation method.

First Check-in & Last Check-out

The first check-in time is recorded as start work time and the last check-out time is recorded as the end-work time.

Each Check-In/Out

Each check-in time and check-out time is valid and the sum of all periods between adjacent check-in and check-out time will be recorded as the valid working duration.

You need to set **Valid Auth. Interval** for this calculation method. For example, if the interval between card swiping of the same card is less than the set value, the card swiping is invalid.

6. **Optional:** Set **Get Check-in/out Status from Device** switch to on to calculate according to attendance status of the device.

Note

Make sure the device support this function if you need to enable this

7. If you select General as the timetable type, set the related attendance time parameters as the following:

Start/End-Work Time

Set the start-work time and end-work-time.

Valid Check-in/out Time

On the time bar, adjust the yellow bar to set the timetable during which the check-in or check-out is valid.

Calculated as

Set the duration calculated as the actual work duration.

Late/Early Leave Allowable

Set the timetable for late or early leave.

8. If you select **Flexible** as the timetable type, set the related attendance time parameters as the following:

Working Hours

The staffs' working hours should be equal or greater than the set value.

Start Time of Timetable

Calculate the working hours of each day from the set value.

For example, if you have set the working hours as 8 hours, and the start time of timetable as 9:00 am, and the staff A checked-in at 8:00 am and checked-out at 5:00 pm (effective working hours are 9:00 am to 5:00 pm, totally 8 hours), the attendance result for staff A will be calculated as normal.

9. **Optional:** Select break time to exclude the duration from work hours.

Note

You can click **Settings** to manage break time. For more details about configuring break time, refer to ***Configure Break Time*** .

10. Click **Save** to add the timetable.
11. **Optional:** Perform one or more following operations after adding timetable.

Edit Timetable	Select a timetable from the list to edit related information.
Delete Timetable	Select a timetable from the list and click **Delete** to delete it.

8.3 Add Shift

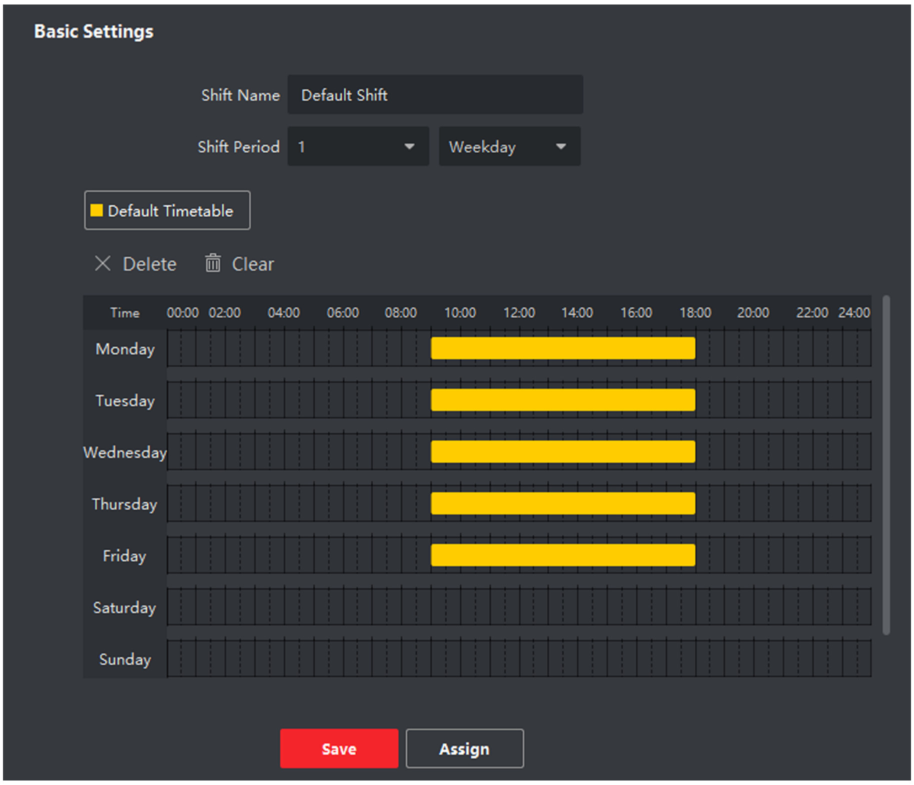
You can add the shift for the shift schedule.

Before You Start

Add a timetable first. See ***Add Timetable*** for details.

Steps

1. Click **Time & Attendance → Shift** to enter shift settings page.
2. Click **Add** to enter Add Shift page.
3. Enter the name for shift.
4. Select the shift period from the drop-down list.
5. Select the added timetable and click on the time bar to apply the timetable.



Basic Settings

Shift Name: Default Shift

Shift Period: 1, Weekday

Figure 8-2 Add Shift

6. Click **Save**.

   The added shift lists on the left panel of the page. At most 64 shifts can be added.

7. **Optional:** Assign the shift to organization or person for a quick shift schedule.
   1) Click **Assign**.
   2) Select **Organization** or **Person** tab and check the desired organization(s) or person(s) box.

      The selected organizations or persons will list on the right page.
   3) Set the effective period for the shift schedule.
   4) Set other parameters for the schedule.

      Check-in Not Required

      Persons in this schedule do not need to check-in when they come to work.

      Check-out Not Required

      Persons in this schedule do not need to check-out when they end work.

      Scheduled on Holidays

      On the holidays, this schedule is still effective and the persons needs to go to work according to the schedule.

      Effective for Overtime

      The persons' overtime will be recorded for this schedule.
   5) Click **Save** to save the quick shift schedule.

8.4 Manage Shift Schedule

Shift work is an employment practice designed to make use of all 24 hours of the clock each day of the week. The practice typically sees the day divided into shifts, set periods of time during which different shifts perform their duties.

You can set department schedule, person schedule, and temporary schedule.

8.4.1 Set Department Schedule

You can set the shift schedule for one department, and all the persons in the department will be assigned with the shift schedule.

Before You Start

In Time & Attendance module, the department list is the same with the organization. You should add organization and persons in Person module first. See ***Person Management*** for details.

Steps

1. Click **Time & Attendance → Shift Schedule** to enter the Shift Schedule Management page.
2. Click **Department Schedule** to enter Department Schedule page.
3. Select the department from the organization list on the left.

   Note

   If **Include Sub Organization** is checked, when selecting the organization, its sub organizations are selected at the same time.

4. Select the shift from the drop-down list.
5. Check the checkbox to enable **Multiple Shift Schedules**.

   Note

   After checking **Multiple Shift Schedules**, you can select the effective time period(s) from the added time periods for the persons in the department.

   Multiple Shift Schedules

   It contains more than one time periods. The person can check in/out in any of the time periods and the attendance will be effective.
   If the multiple shift schedules contains three time periods: 00:00 to 07:00, 08:00 to 15:00 and 16:00 to 23:00. The attendance of the person adopting this multiple shift schedules will be effective in any of the three time periods. If the person checks in at 07:50, it will apply the nearest time period 08:00 to 15:00 to the person's attendance.

6. Set the start date and end date.
7. Set other parameters for the schedule.

   Check-in Not Required

Persons in this schedule do not need to check-in when they come to work.

Check-out Not Required

Persons in this schedule do not need to check-out when they end work.

Scheduled on Holidays

On the holidays, this schedule is still effective and the persons needs to go to work according to the schedule.

Effective for Overtime

The persons' overtime will be recorded for this schedule.

8. Click **Save**.

8.4.2 Set Person Schedule

You can assign the shift schedule to one or more persons. You can also view and edit the person schedule details.

Before You Start

Add department and person in Person module. See ***Person Management*** for details.

Steps

Note

The person schedule has the higher priority than department schedule.

1. Click **Time & Attendance → Shift Schedule** to enter the Shift Schedule page.
2. Click **Person Schedule** to enter Person Schedule page.
3. Select the organization and select the person(s).
4. Select the shift from the drop-down list.
5. Check the checkbox to enable **Multiple Shift Schedules**.

   Note

   After checking the **Multiple Shift Schedules**, you can select the effective timetable(s) from the added timetables for the persons.

   Multiple Shift Schedules

   It contains more than one timetables. The person can check in/out in any of the timetables and the attendance will be effective.
   If the multiple shift schedules contains three timetables: 00:00 to 07:00, 08:00 to 15:00 and 16:00 to 23:00. The attendance of the person adopting this multiple shift schedules will be effective in any of the three timetables. If the person checks in at 07:50, it will apply the nearest timetable 08:00 to 15:00 to the person's attendance.

6. Set the start date and end date.
7. Set other parameters for the schedule.

Check-in Not Required

Persons in this schedule do not need to check-in when they come to work.

Check-out Not Required

Persons in this schedule do not need to check-out when they end work.

Scheduled on Holidays

On the holidays, this schedule is still effective and the persons needs to go to work according to the schedule.

Effective for Overtime

The persons' overtime will be recorded for this schedule.

8. Click **Save**.

8.4.3 Set Temporary Schedule

You can add a temporary schedule for the person and the person will be assigned with the shift schedule temporarily. You can also view and edit the temporary schedule details.

Before You Start

Add department and person in Person module. See ***Person Management*** for details.

Steps

Note

The temporary schedule has higher priority than department schedule and person schedule.

1. Click **Time & Attendance → Shift Schedule** to enter the Shift Schedule Management page.
2. Click **Temporary Schedule** to enter Temporary Schedule page.
3. Select the organization and select the person(s).
4. Click one date or click and drag to select multiple dates for the temporary schedule.
5. Select **Workday** or **Non-Workday** from drop-down list.

   If **Non-Workday** is selected, you need to set the following parameters.

   Calculated as

   Select normal or overtime level to mark the attendance status for temporary schedule.

   Timetable

   Select a timetable from drop-down list.

   Multiple Shift Schedule

   It contains more than one timetables. The person can check in/out in any of the timetables and the attendance will be effective.

   If the multiple shift schedules contains three timetables: 00:00 to 07:00, 08:00 to 15:00 and 16:00 to 23:00. The attendance of the person adopting this multiple shift schedules will be effective in any of the three timetables. If the person checks in at 07:50, it will apply the nearest timetable 08:00 to 15:00 to the person's attendance.

Rule

Set other rule for the schedule, such as **Check-in Not Required**, and**Check-out Not Required**.

6. Click **Save**.

8.4.4 Check Shift Schedule

You can check the shift schedule in calendar or list mode. You ca also edit or delete the shift schedule.

Steps

1. Click **Time & Attendance → Shift Schedule** to enter the Shift Schedule Management page.
2. Select the organization and corresponding person(s).
3. Click ▦ or ☰ to view the shift schedule in calendar or list mode.

Calendar

In calendar mode, you can view the shift schedule for each day in one month. You can click the temporary schedule for one day to edit or delete it.

List

In list mode, you can view the shift schedule details about one person or organization, such as shift name, type, effective period and so on. Check the shift schedule(s), and click **Delete** to delete the selected shift schedule(s).

8.5 Manually Correct Check-in/out Record

If the attendance status is not correct, you can manually correct the check-in or check out record. You can also edit, delete, search, or export the check-in or check-out record.

Before You Start

- You should add organizations and persons in Person module. For details, refer to ***Person Management*** .
- The person's attendance status is incorrect.

Steps

1. Click **Time & Attendance → Attendance Handling** to enter attendance handling page.
2. Click **Correct Check-In/Out** to enter adding the check-in/out correction page.
3. Select person from left list for correction.
4. Select the correction date.
5. Set the check-in/out correction parameters.
   - Select **Check-in** and set the actual start-work time.
   - Select **Check-out** and set the actual end-work time.

Note

You can click ⊕ to add multiple check in/out items. At most 8 check-in/out items can be supported.

6. **Optional:** Enter the remark information as desired.
7. Click **Save**.
8. **Optional:** After adding the check-in/out correction, perform one of the following operations.

View Click ▦ or ☰ to view the added attendance handling information in calendar or list mode.

Note

In calendar mode, you need to click **Calculate** to get the attendance status of the person in one month.

Edit
- In calendar mode, click the related label on date to edit the details.
- In list mode, double-click the related filed in Date, Handling Type, Time, or Remark column to edit the information.

Delete Delete the selected items.

Export Export the attendance handling details to local PC.

Note

The exported details are saved in CSV format.

8.6 Add Leave and Business Trip

You can add leave and business trip when the employee want to ask for leave or go on a business trip.

Before You Start

You should add organizations and persons in the Person module. For details, refer to ***Person Management*** .

Steps

1. Click **Time & Attendance → Attendance Handling** to enter attendance handling page.
2. Click **Apply for Leave/Business Trip** to enter adding the leave/business trip page.
3. Select person from left list.
4. Set the date(s) for your leave or business trip.
5. Select the major leave type and minor leave type from the drop-down list.

Note

You can set the leave type in Attendance Settings. For details, refer to ***Configure Leave Type*** .

6. Set the time for leave.
7. **Optional:** Enter the remark information as desired.
8. Click **Save**.
9. **Optional:** After adding the leave and business trip, perform one of the following operations.

View Click ▦ or ☰ to view the added attendance handling information in calendar or list mode.

Note

In calendar mode, you need to click **Calculate** to get the attendance status of the person in one month.

Edit
- In calendar mode, click the related label on date to edit the details.
- In list mode, double-click the filed in Date, Handling Type, Time, or Remark column to edit the related information.

Delete Delete the selected items.

Export Export the attendance handling details to local PC.

Note

The exported details are saved in CSV format.

8.7 Calculate Attendance Data

You need to calculate the attendance data before searching and viewing the overview of the attendance data, employees' detailed attendance data, employees' abnormal attendance data, the employees' overtime working data, and card swiping log.

8.7.1 Automatically Calculate Attendance Data

You can set a schedule so that the client can calculate the attendance data automatically at the time you configured every day.

Steps

Note

It will calculate the attendance data till the previous day.

1. Enter the Time & Attendance module.
2. Click **Attendance Settings → General Rule** .
3. In the Auto-Calculate Attendance area, set the time that you want the client to calculate the data every day.
4. Click **Save**.

8.7.2 Manually Calculate Attendance Data

You can calculate the attendance data manually by setting the data range.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Statistics → Calculate Attendance** .
3. Set the start time and end time to define the attendance data range.
4. Set other conditions, including department, person name, employee No. and attendance status.
5. Click **Calculate**.

   Note

   It can only calculate the attendance data within three months.

6. Perform one of the following operations.

Correct Check-in/out	Click **Correct Check-in/out** to add check-in/out correction.
Report	Click **Report** to generate the attendance report.
Export	Click **Export** to export attendance data to local PC. **Note** The exported details are saved in CSV format.

8.8 Attendance Statistics

You can check the original attendance record, generate and export the attendance report based on the calculated attendance data.

8.8.1 Get Original Attendance Record

You can search the employee's attendance time, attendance status, check point, etc. in a time period to get an original record of the employees.

Before You Start

- You should add organizations and persons in Person module and the persons has swiped card. For details, refer to ***Person Management*** .
- Calculate the attendance data.

ℹ **Note**

- The client will automatically calculate the previous day's attendance data at 1:00 am on the next day.
- Keep the client running at 1:00 am or it cannot calculate the previous day's attendance data automatically. If not calculated automatically, you can calculate the attendance data manually. For details, refer to ***Manually Calculate Attendance Data*** .

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Statistics → Original Records** .
3. Set the attendance start time and end time that you want to search from.
4. Set other search conditions, such as department, person name, and employee No.
5. **Optional:** Click **Get from Device** to get the attendance data from the device.
6. **Optional:** Click **Reset** to reset all search conditions and edit the search conditions again.
7. Click **Search**.

   The result displays on the page. You can view the employee's required attendance status and check point.
8. **Optional:** After searching the result, perform one of the following operations.

Generate Report	Click **Report** to generate the attendance report.
Export Report	Click **Export** to export the results to the local PC.

8.8.2 Generate Instant Report

It supports to generate the a series of attendance reports manually to view the employees' attendance results.

Before You Start

Calculate the attendance data.

ℹ **Note**

You can calculate the attendance data manually, or set the schedule so that the client can calculate the data automatically every day. For details, refer to ***Calculate Attendance Data*** .

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Statistics → Report** .
3. Select a report type.
4. Select the department or person to view the attendance report.
5. Set the start time and end time during which the attendance data will be displayed in the report.
6. Click **Report** to generate the statistics report and open it.

8.8.3 Custom Attendance Report

The client supports multiple report types and you can pre-define the report content and it can send the report automatically to the email address you configured.

Steps

Note

Set the email parameters before you want to enable auto-sending email functions. For details, refer to ***Set Email Parameters*** .

1. Enter the Time & Attendance module.
2. Click **Attendance Statistics → Custom Report** .
3. Click **Add** to pre-define a report.
4. Set the report content.

   Report Name

   Enter a name for the report.

   Report Type

   Select one report type and this report will be generated.

   Report Time

   The time to be selected may vary for different report type.

   Person

   Select the added person(s) whose attendance records will be generated for the report.
5. **Optional:** Set the schedule to send the report to the email address(es) automatically.
   1) Check the **Auto-Sending Email** to enable this function.
   2) Set the effective period during which the client will send the report on the selected sending date(s).
   3) Select the date(s) on which the client will send the report.
   4) Set the time at which the client will send the report.

      Example

      If you set the effective period as ***2018/3/10 to 2018/4/10***, select ***Friday*** as the sending date, and set the sending time as ***20:00:00***, the client will send the report at 8 p.m. on Fridays during 2018/3/10 to 2018/4/10.

      Note

      Make sure the attendance records are calculated before the sending time. You can calculate the attendance data manually, or set the schedule so that the client can calculate the data automatically every day. For details, refer to ***Calculate Attendance Data*** .
   5) Enter the receiver email address(es).

Note

You can click **+** to add a new email address. Up to 5 email addresses are allowed.

6) **Optional:** Click **Preview** to view the email details.

6. Click **OK**.
7. **Optional:** After adding the custom report, you can do one or more of the followings:

Edit Report	Select one added report and click **Edit** to edit its settings.
Delete Report	Select one added report and click **Delete** to delete it.
Generate Report	Select one added report and click **Report** to generate the report instantly and you can view the report details.

Chapter 9 Video Intercom

Video intercom is an audiovisual communication system used within a building or a small collection of buildings. With microphones and video camera devices at both sides, it enables the inter-communication via video and audio signals. A video intercom system can provide a safe and easy monitoring solution for apartment buildings and private houses.

Be sure to add video intercom devices to the client and link the indoor stations to the persons beforehand. You should also set the access authorization for the persons to open doors via the linked indoor stations.

Note

- Up to 16 door stations and 512 indoor stations or master stations can be managed in the client. For details about adding video intercom devices, refer to ***Add Device*** .
- For details about adding persons, refer to ***Add Single Person*** .
- For details about setting person's access authorization, refer to ***Set Access Group to Assign Access Authorization to Persons*** .

9.1 Manage Calls between Client Software and an Indoor/Door Station/ Access Control Device

You can call the residents by the client, and vice versa. You can also use an indoor station/door station or specified access control device to call the client.

Before making calls, you can set the parameters such as ring duration and speaking duration. For details, refer to ***Set Access Control and Video Intercom Parameters*** .

9.1.1 Call Indoor Station from Client

You can call the added indoor station by the client to perform video intercom.

Before You Start

- Be sure to have added a resident to the client. For details, refer to ***Add Single Person*** .
- Be sure to have linked the resident with an indoor station and configured the resident information (including floor No. and room No.) in Person module. For details about configuring the linkage and resident information, refer to ***Configure Resident Information*** .

Steps

Note

- A video intercom device can be added to more than one client, but perform video intercom with only one client at a time.
- You can remotely configure the Max. Ring Duration and the Max. Speaking Duration.

1. Click **Access Control → Video Intercom → Contacts** .
2. Unfold the organization list on the left panel and select an organization.

   The information (including resident name, linked device name and device IP address) of all the residents in the selected group will be displayed on the right panel.
3. Select a resident, or enter a keyword in the Filter field to find the desired resident.
4. Click ☎ to start calling the selected resident.

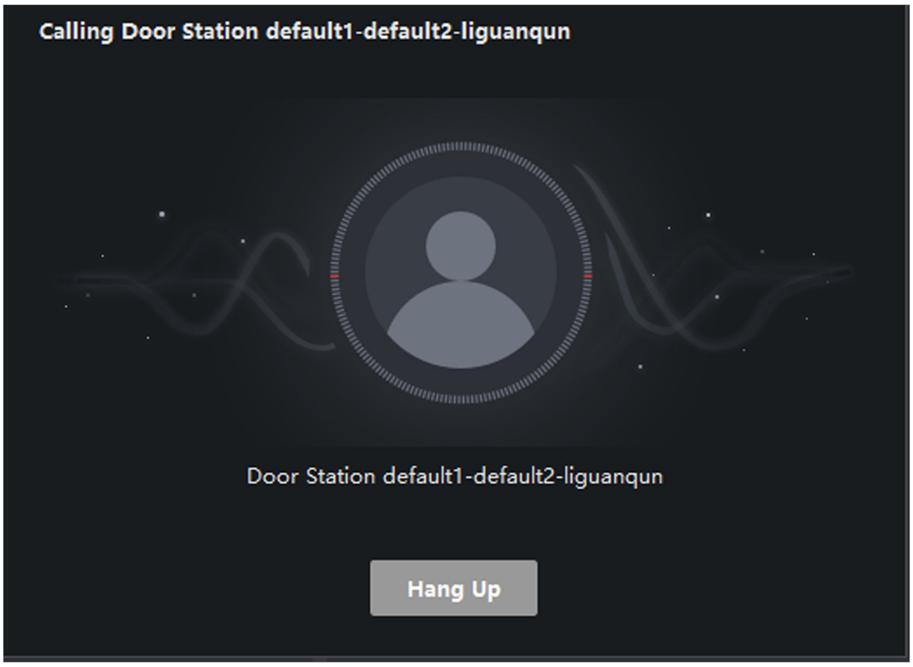

Calling Door Station default1-default2-liguanqun
Door Station default1-default2-liguanqun
Hang Up

Figure 9-1 Start Calling Window

After the call is answered, you will enter the In Call window.

5. **Optional:** After the call is answered, perform the following operation(s).

   Adjust Loudspeaker Volume Click 🔊 to adjust the volume of the loudspeaker.

   End Speaking Click **Hang Up** to end speaking.

   Adjust Microphone Volume Click 🎙 to adjust the volume of the microphone.

9.1.2 Answer Call via Client

The residents can call the client by an indoor station, door station, or specific access control devices and perform video intercom with the client.

Before You Start

- Be sure to have added a resident to the client. For details, refer to ***Add Single Person*** .
- Be sure to have linked the added resident with an indoor station/outdoor station/access control device and configured the resident information (including floor No. and room No.) in Person module. For details about configuring the linkage and resident information, refer to ***Configure Resident Information*** .

Steps

Note

- A video intercom device can be added to more than one client, but perform video intercom with only one client at a time.
- You can remotely configure the Max. Ring Duration and the Max. Speaking Duration.

1. Click **Access Control → Video Intercom → Contacts** .
2. Unfold the organization list on the left panel and select an organization.

   The information (including resident name, linked device name and device IP address) of all the residents in the selected group will be displayed on the right panel.
3. Click ☎ to start calling a desired resident.

   An incoming call dialog will pop up.

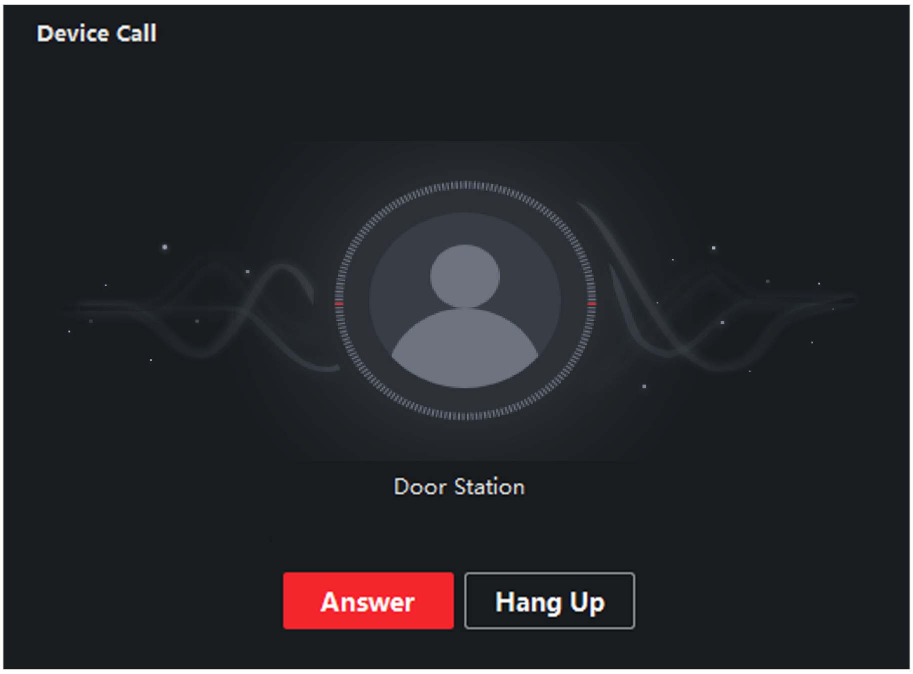


Figure 9-2 Incoming Call

4. Click **Answer** to answer the call.

   After the call is answered, you will enter the In Call window.

5. **Optional:** In the In Call window, perform the following operation(s).

Adjust Loudspeaker Volume	Click 🔊 to adjust loudspeaker's volume.
End Speaking	Click **Hang Up** to end speaking.
Adjust Microphone Volume	Click 🎤 to adjust the microphone's volume.
Open Door	When an indoor station is linked with a door station, click 🚪 to open the door linked with the door station.

9.2 View Real-Time Call Logs

You can view details of all the calls, and you can call the residents or export the logs if they are needed.

Steps

1. Click **Access Control → Video Intercom → Call Log** .

   Details of all the calls will be displayed on the right panel including call status, start time, speaking duration, device type and name, and organization and name of resident.

2. **Optional:** Click ☎ to re-dial the resident.

3. **Optional:** Set search conditions (including call status, device type, and time) on the top of the page to filter call logs.
4. Click **Export** to save the logs (a CSV file) in your PC.

9.3 Release a Notice to Resident

You can send a notice to the residents by one-touch. Four notice types are available: advertising, property, alarm, and notice information.

Steps

1. Click **Access Control → Video Intercom → Notice** .
2. Click **Add** to open the Create Notice panel.
3. Click ⋯ to select the residents you are going to deliver notice to.
4. Enter the required information.

Note

- Up to 63 characters are allowed in the Subject field.
- Up to 1023 characters are allowed in the Content field.
- You can add up to 6 pictures. Each picture should be in JPG format and smaller than 512 KB.

5. Click **Send** to send the notice to the selected resident(s).

   Information about the sent notices will be displayed on the left panel. Click a notice to view its details on the right panel.

6. **Optional:** Click **Export** to save all the notices in your PC.

Chapter 10 Log Search

Two log types are provided: operation log and system log. The operation logs refer to the normal operations that the user did on the client, such as add device, log search, and reset password; and the system logs record the system information, such as login, logout, lock and unlock. You can search the log files and view the log details, including time, user, etc.

Steps

1. Enter the System Log module.
2. Click ▦ to specify the start time and end time.

   Note

   You can search the logs within one month.

3. Select a user to search the log files which are generated when this user log into the client.
4. Select **Operation Log** or **System Log** as log type.
5. Click **Search**.

   The log files between the start time and end time will be displayed on the list. You can check the operation time, type and other information of the logs.

6. **Optional:** Perform one of the following operations.

   Filer Click ▼ on each table header and select to filter the logs.

   Sort Click the table header to sort the logs by the time or letter sequence.

   Backup Click **Backup Log** to back up the search result to local PC.

   Note

   You can view the logs by importing the exported log files. For more details, refer to ***Operation and Maintenance*** .

Chapter 11 User Management

To improve the system security, the administrator should create different account for different user, and assign different permissions to the user. To avoid different people sharing the same user account, we recommend you manage the user accounts periodically.

11.1 Add User

The super user and administrator can add new users, and assign different permissions for different users if needed.

Perform this task to add an user account.

Steps

Note

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

1. Enter the User Management module.
2. Click **Add User** to show user information area.
3. Select the user type from the drop-down list.

   Administrator

   The administrator account has all permissions by default, and can modify the passwords and permissions of all operators and its own.

   Operator

   The operator account has no permission by default and you can assign the permissions manually. An operator can only change the passwords of its own account and the accounts which are added by it.
4. Enter the user name, password, and confirm password as desired.

   Caution

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.
   Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
5. Check the checkboxes to assign the permissions to the created user.
6. **Optional:** Click **Default Value** to restore the default permissions of this user.

7. Click **Save**.

   Note

   Up to 50 user accounts can be added for the client software.

   After created user account successfully, the user account is added to the user list on the Account Management page.

8. **Optional:** Perform the following operations after the user account is created.

   Edit User Click a user from the list to edit the user information.

   Note

   Only the password of the super user can be edited.

   Delete User Select the user from the list and click **Delete User**.

   Note

   You cannot delete the super user.

11.2 Change User's Password

The administrator can change normal user's password without entering the old password, while the administrator should enter the old password when changing the password of itself.

Before You Start

Add user to the software client.

Steps

1. Enter the User Management module.
2. Select the user need to be change password, click **Change**.
3. **Optional:** Enter the old password.

   Note

   When changing the administrator's password, you need to enter the old password first.

4. Enter the new password and confirm the password.
5. Click **OK**.

Chapter 12 System Configuration

The general parameters, picture storage, alarm sound, email settings, file saving path, video intercom and access control parameters can be configured.

12.1 Set General Parameters

You can configure the frequently-used parameters, including log expired time, network performance, etc.

Steps

1. Enter the System Configuration module.
2. Click **General** tab to enter the General Settings page.
3. Configure the general parameters.

   Log Expiry Date

   The time for keeping the log files. Once exceeded, the files will be deleted.

   Maximum Mode

   Select **Maximize** or **Full Screen** as the maximum mode. **Maximize** mode can maximize the display and show the taskbar. **Full Screen** mode can display the client in full-screen mode.

   Network Performance

   Set the network conditions to **Normal**, **Better** or **Best**.

   Detect New Software Version

   After enabled, the client can automatically detect the new software version and remind the customer to upgrade the software or not.

   Auto-Upgrade Device

   Set the processing methods after the new version of device are detected.

   Disable

   Disable auto-upgrade device.

   Prompt Me If Download and Upgrade

   After the client detects the new version of the device, it will prompt the user whether to download the new version and upgrade.

   Download and Prompt Me If Upgrade

   After the client detects the new version of the device, it will download the new version automatically, and prompt the user whether to upgrade.

   Download and Prompt Automatically

After the client detects the new version of the devices, it will download the new version and upgrade the new version automatically.

You need to set the **Upgrade Time**, during which the client upgrades the new version automatically.

Automatic Time Synchronization

Automatically synchronize the time of the added devices with the time of the PC running the client at a specified time point.

4. Click **Save**.

12.2 Set Picture Storage

The pictures, captured by the camera of video access control terminal, triggered by events, can be saved in the PC running the iVMS-4200 AC Service.

Steps

1. Enter the System Configuration module.
2. Click **Picture Storage**.
3. Set the **Store Pictures in Server** switch to on.

   All the disks of the PC running the service will show.
4. Select the disk to save the pictures.

   Note

   The default saving path is: Disk/iVMS-4200 ACalarmPicture
5. Click **Save**.

12.3 Set Alarm Sound

When the event, such as access control event, is triggered, the client can be set to give an audible warning and the sound of the audible warning can be configured.

Steps

1. Open the System Configuration page.
2. Click **Alarm Sound** tab to enter the Alarm Sound Settings page.
3. **Optional:** Click ⋯ and select the audio files from the local path for different events.
4. **Optional:** Add customized alarm sound.
   1) Click **Add** to add customized alarm sound.
   2) Double click the **Type** field to customize the alarm sound name as desired.
   3) Click ⋯ and select the audio files from the local path for different alarms.
5. **Optional:** Click 🔊 for a testing of the audio file.
6. **Optional:** Click ✕ in the Operation column to delete the custom sound.
7. Click **Save**.

Note

The format of the audio file can only be WAV.

12.4 Set Access Control and Video Intercom Parameters

You can configure the access control and video intercom parameters according to actual needs.

Steps

1. Open the System Configuration page.
2. Click the **Access Control & Video Intercom** tab.
3. Input the required information.

   Ringtone

   Click ··· and select the audio file from the local path for the ringtone of indoor station. Optionally, you can click 🔊 for a testing of the audio file.

   Max. Ring Duration

   Specify the seconds that the ring will last for at most. The maximum ring duration can be set from 15s to 60s.

   Max. Speaking Duration with Indoor Station

   Specify the seconds that the call with indoor station will last for at most. The maximum speaking duration between indoor station and the client can be set from 120s to 600s.

   Max. Speaking Duration with Door Station

   Specify the seconds that the call with door station will last for at most. The maximum speaking duration between door station and the client can be set from 90s to 120s.

   Max. Speaking Duration with Access Control Device

   Specify the seconds that the call with access control device will last for at most. The maximum speaking duration between access control device and the client can be set from 90s to 120s.
4. Click **Save**.

12.5 Set File Saving Path

The system configuration files and the pictures manually captured in Status Monitoring are stored on the local PC. The saving paths of these files can be set.

Steps

1. Open the System Configuration page.
2. Click **File** tab to enter the File Saving Path Settings page.
3. Click ··· and select a local path for the files.
4. Click **Save**.

12.6 Set Email Parameters

An email notification can be sent when an event occurs. To send the email to some specified receivers, the settings of the email need to be configured before proceeding.

Steps

1. Enter the System Configuration module.
2. Click **Email** tab to enter the Email Settings interface.
3. Enter the required information.

    STMP Server

    The STMP server IP address of host name (e.g., smtp.263xmail.com)

    Encryption Type

    You can check the radio to select **Non-Encrypted**, **SSL**, or **STARTTLS** .

    Port

    Enter the communication port used for SMTP. The port is 25 by default.

    Sender Address

    The email address of the sender.

    Security Certificate (Optional)

    If your email server requires authentication, check this checkbox to use authentication to log into the server and enter the login user name and password of your email account.

    User Name

    Enter the user name of the sender email address if **Server Authentication** is checked.

    Password

    Enter the password of the sender Email address if **Server Authentication** is checked.

    Receiver 1 to 3

    Input the email address of the receiver. Up to 3 receivers can be set.

4. **Optional:** Click **Send Test Email** to send an email to the receiver for test.
5. Click **Save**.

Chapter 13 Operation and Maintenance

You can perform maintaining operations in the menu to ensure a smooth and convenient usage of the client.

Click ☰ in the upper-right corner, and then click **File**/**System**/**Tool** to perform the following operations.

Open Log File

You can open a log file saved in your local PC or log files of the client.

Import/Export Configuration File

You can import configuration files from local PC to the client if needed, and vice versa.

Auto Backup

Select day and time to backup configuration files and data in database, or restore the backed up data.

Skin

Change the skin of the client, including bright-color series and black-color series.

Batch Time Sync

Synchronize selected devices' time with your PC time.

Message Queue

After configuring email linkage, the triggered event(s) will be displayed here. Select an event and cancel sending the an email to the receiver.

Appendix A. Custom Wiegand Rule Descriptions

Take Wiegand 44 as an example, the setting values in the Custom Wiegand tab are as follows:

Custom Wiegand Name	Wiegand 44				
Total Length	44				
Transformation Rule (Decimal Digit)	byFormatRule[4]=[1][4][0][0]				
Parity Mode	XOR Parity				
Odd Parity Start Bit		Length			
Even Parity Start Bit		Length			
XOR Parity Start Bit	0	Length per Group	4	Total Length	40
Card ID Start Bit	0	Length	32	Decimal Digit	10
Site Code Start Bit		Length		Decimal Digit	
OEM Start Bit		Length		Decimal Digit	
Manufacturer Code Start Bit	32	Length	8	Decimal Digit	3

Wiegand Data

Wiegand Data = Valid Data + Parity Data

Total Length

Wiegand data length.

Transportation Rule

4 bytes. Display the combination types of valid data. The example displays the combination of Card ID and Manufacturer Code. The valid data can be single rule, or combination of multiple rules.

Parity Mode

Valid parity for Wiegand data. You can select either odd parity or even parity.

Odd Parity Start Bit, and Length

If you select Odd Parity, these items are available. If the odd parity start bit is 1, and the length is 12, then the system will start odd parity calculation from bit 1. It will calculate 12 bits. The result will be in bit 0. (Bit 0 is the first bit.)

Even Parity Start Bit, and Length

If you select Even Parity, these items are available. If the even parity start bit is 12, and the length is 12, then the system will start even parity calculation from bit 12. It will calculate 12 bits. The result will be in the last bit.

XOR Parity Start Bit, Length per Group, and Total Length

If you select XOR Parity, these items are available. Depending on the table displayed above, the start bit is 0, the length per group is 4, and the total length is 40. It means that the system will calculate from bit 0, calculate every 4 bit, and calculate 40 bits in total (10 groups in total). The result will be in the last 4 bits. (The result length is the same as the length per group.)

Card ID Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. Depending on the table displayed above, the card ID start bit is 0, the length is 32, and the decimal digit is 10. It represents that from bit 0, there are 32 bits represent the card ID. (The length here is calculated by bit.) And the decimal digit length is 10 bits.

Site Code Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. For detailed information, see the explanation of the card ID.

OEM Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. For detailed information, see the explanation of the card ID.

Manufacturer Code Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. Depending on the table displayed above, the manufacturer code start bit is 32, length is 8, and decimal digit is 3. It represents that from bit 32, there are 8 bits are manufacturer code. (The length here is calculated by bit.) And the decimal length is 3.

See Far, Go Further