Star4Live Web Manager User Manual

V1.12

Contents

Introduction

The Star4Live supports unified device management, live view, playback and provides small and medium-sized enterprises with video-based smart, convenient and secure information service.

1 Registration and Login

Open a Web browser, enter http://www.star4live.com in the address bar, and then press **Enter** to open the login page.

Note: Please use Google Chrome 60 or later, Firefox 60 or later versions of browser.

- For unregistered users: Click **Sign Up**, follow on-screen instructions to complete the account registration. You'll log in automatically when registration is completed.
- For registered users: There are 2 options for login.
  - Password: ① Enter the username or the mobile phone number/ email associated with your account. ② Enter the password. ③ Read and accept the service agreement and privacy policy. ④ Click **Log In**.

    Note:
    - Click **Log in Using Mobile Phone Number** or **Log in Using Email** in the bottom left corner to switch the login method.
    - Login using mobile phone number is only available in some regions. Please select your region first.
  - Verification Code: ① Enter the mobile phone number/ email associated with your account. ② Get and enter the verification code. ③ Read and accept the service agreement and privacy policy. ④ Click **Log In**.

    Note: Click **Log in Using Mobile Phone Number** or **Log in Using Email** in the bottom left corner to switch the login method.

Note:
A cloud account registered on one client can be used on another.

Help: View user manual and privacy policy.

Language switch: The system offers multiple languages, such as English, Italian, and French. You can switch languages in the upper-right corner of the page.

2 End User Version

Upon logging in, the end user version is displayed by default, where you can manage the devices associated with your account.

Note: For the mobile client, please download the Guard Live app.

2.1 Organization Management

Add devices in the same region or of the same type to one Organization for efficient management. An organization that includes sub organization(s) is known as a parent organization. For example, a school includes classroom, playground, etc, and you can set "school" as the parent organization and set "classroom" as a sub organization.

Go to **Organization Management**.

Add Organization

1. Click **Add**.
2. Set the organization name and parent organization.

3. Click **OK**.

More Actions

Function	Operation
Search	1. Select the organization owner and organization name on the top of the page. 2. Click **Search** to search the target organization.
Delete	Click in the **Operation** column, or select the target organization and click **Delete**.
Rename	Click in the **Operation** column.
Share organization	Click in the **Operation** column (see Sharing).

2.2 Device Management

2.2.1 Add Device

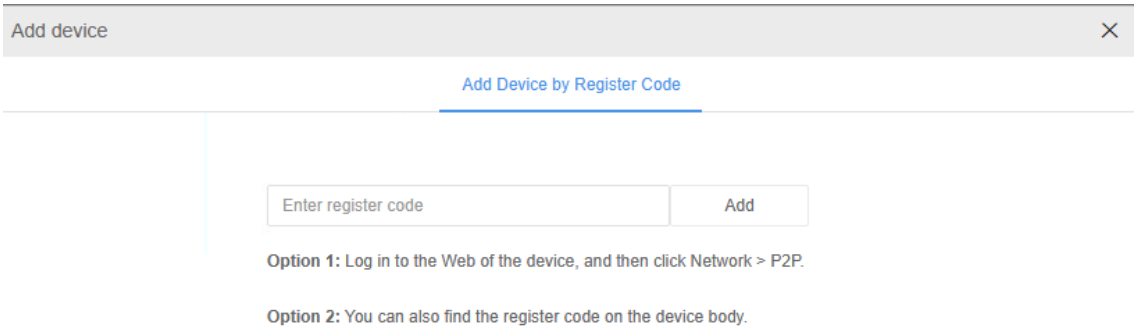
Add devices to a cloud account for unified management, including NVR, IPC, AI BOX, access control device, parking management server, entrance/exit camera, access control system all-in-one machine, NAS, NSW, etc.

Note:

- The functions available may vary depending on the device type.
- AI BOX devices only support reporting alarm messages.
- For access control devices, you can only click to access its Web interface.
- For security, each device can only be bound with one cloud account. A device cannot be bound with a second cloud account before its current binding is cancelled.

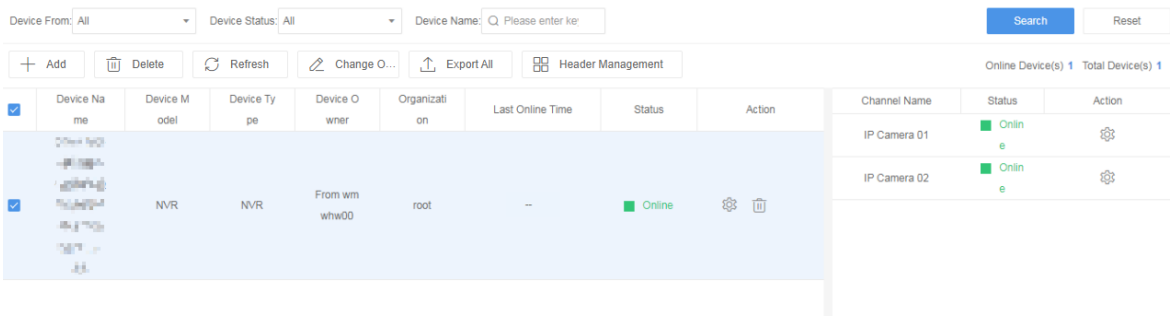
Add Device

1. On **Device Management** page, click **Add** in the top left corner.



2. Enter the device's register code, click **Add**.
3. (Optional) Change the device name and organization.
4. Click **OK**.

More Actions



- To search devices, set the search criteria such as device owner, device status and device name, and click **Search**.
- To configure a device, click .
- To delete a device, click .
- To go to the online device's Web interface, click .

  If an NVR device is shared from another user (From *xxx* in the **Device Owner** column) and only has shared with **function permissions**, when you **first** click to go to the device's Web interface, for security concerns, you must enter the device's username and password for verification. Once succeeded, you will be redirected to the device's **Live View** page automatically.
- To change the organization of devices in batches, select the desired devices and then click **Change Organization**.

  Note:
  - Devices in a shared organization cannot be transferred to other organizations.
  - You cannot change the organization of a shared channel.
- To export the device list, click **Export**.
- To display device information in the list, click **Header Management**, and then select the information to be displayed as needed.

2.2.2 Device Configuration

Manage devices, transfer, rename, delete, configure, export, and share the added devices.

Note: The channels shared from others can only be renamed or deleted.

In **Device Management** page, click in the **Action** column, go to **Device Configuration**.

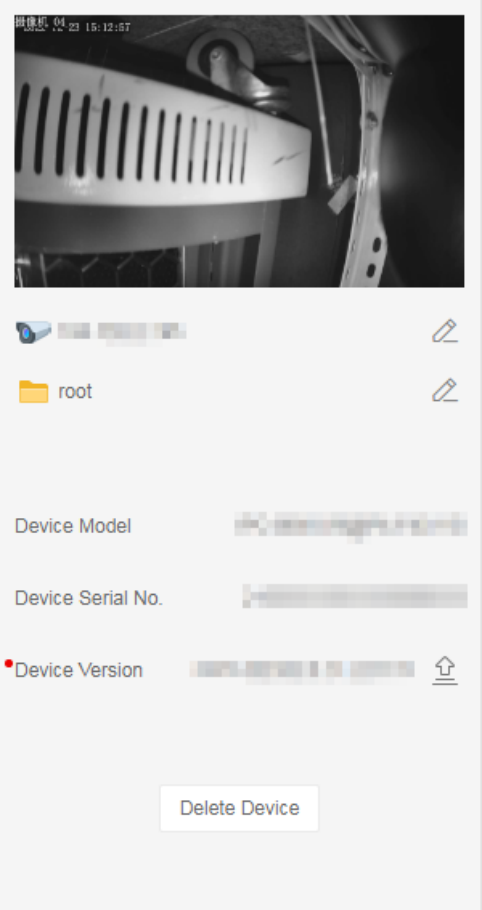
Note: The functions available may vary with device model.

2.2.2.1 Basic Configuration

Purpose

Set device name, view device model, serial number, version number, delete or transfer devices.

Steps



- Click to rename a device. You need to enter the new name in the pop-up dialog box and then click **OK** to apply the new name.
- Click to change the organization of the device. The new organization applies immediately.
- Click **Transfer Device** to transfer the device to another cloud account.
- Click **Delete Device** to delete the device from the current cloud account.
- The system will automatically detect version updates. If there is a new version available, click next to the device version to upgrade.

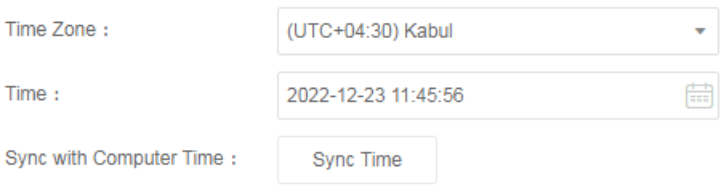
2.2.2.2 Time Configuration

Purpose

Configure the time zone or time manually for a device.

Steps

1. Click to display the **Time Configuration** page.
2. Complete time settings.
   - Set the time zone, date and time.
   - Click **Sync Time** to synchronize the computer's system time to the device.



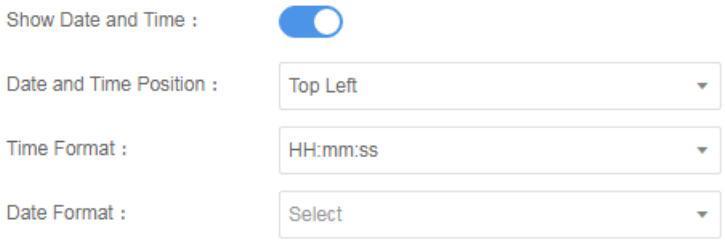
2.2.2.3 OSD Configuration

Purpose

Overlay date and time on the live image.

Steps

1. Click to display the **OSD Configuration** page.
2. Click to enable **Show Date and Time**.
3. Set date/time position and format.



2.2.2.4 Storage Configuration

Purpose

Configure a storage policy and recording schedule for a device, so the device can record and store video as configured.

Steps

Click to display the **Storage Configuration** page.

Note: Only NVR supports recording type configuration.

- Storage status: view storage status and storage capacity.
- Storage policy
  - Overwrite when storage full: The previous recording will be overwritten when the storage capacity is used up.
  - Stop when storage full: The recording will be stopped when the storage capacity is used up.
- Format: Format device SD card.
- Recording schedule: Configure recording schedule for device/channel.

Table 2-1: Storage Configuration

Parameter		Description
Recording Type	Normal Recording	Video is recorded automatically during the set time.
	Event Recording	Video recording is triggered by events that are configured on the device side. See the corresponding user manual of the device for details.
Recording Time		Set the recording time. Video will be recorded during the set time only.

Note:

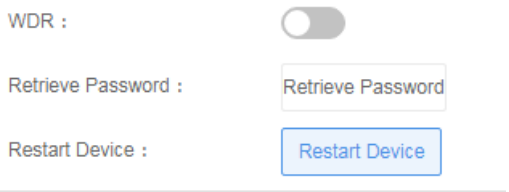
- Only NVR supports recording type configuration.
- For an NVR, you need to choose a channel to configure.

2.2.2.5 Audio Configuration

Set MIC and speaker sound volume on the device.

2.2.2.6 Other Configuration

Enable WDR to have a clear view of objects in both bright and dark areas in the image. Retrieve device passwords or restart devices.



2.2.3 Arming Configuration

Note: NVRs do not support arming configuration. Choose channels of an NVR to configure.

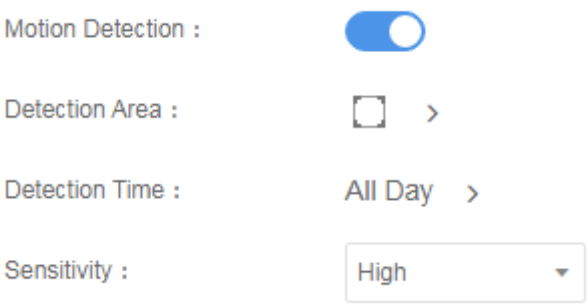
2.2.3.1 Motion Detection

Purpose

Enable motion detection to detect object movements in the image and be alerted by an alarm when motion is detected. You can search alarm messages on the **Message** page on the C/S client.

Steps

1. Click to display the **Arming Configuration** tab.
2. Click to display the **Motion Detection** page.
3. Click to enable motion detection.
4. (Optional) Set alarm-triggered snapshot to automatically capture an image when an alarm occurs. Only channels of an NVR can be configured.
5. Set a detection area. Only motion within this area will be detected. By default, the detection area covers the entire screen.
6. Set the time when detection will take place.
7. Set detection sensitivity. The higher the sensitivity, the more likely motion can be detected.



2.2.3.2 Human Body Detection

Enable human body detection to detect human bodies in the video and be alerted by an alarm when a human body is detected. You can search alarm messages on the **Message** page on the C/S client.

2.2.3.3 Auto Tracking

Purpose

Enable auto tracking to let the PTZ camera automatically track moving objects on the image.

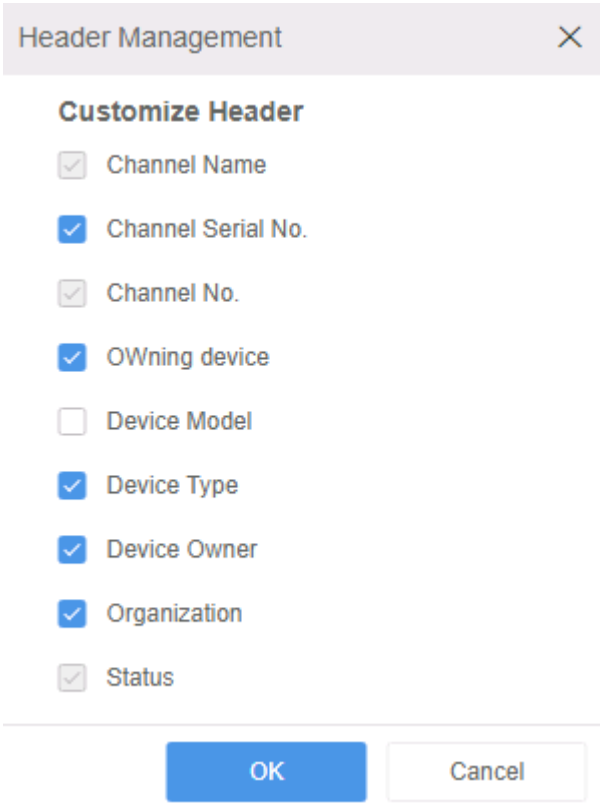
Steps

1. Click to display the **Auto Tracking** tab.
2. Click to enable auto tracking.
3. Set detection time.

2.3 Channel Management

Customize the display contents of the channel list.

1. Click  in the upper right corner.



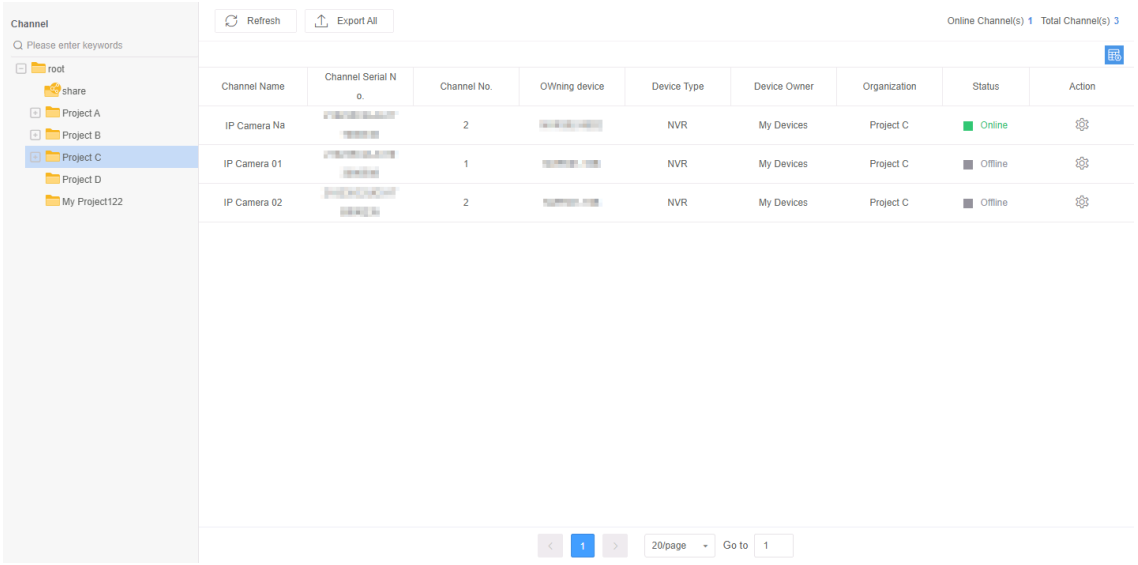
2. Select the channel information to display. Click on an item to select/deselect it.
   -  : Mandatory item, which cannot be deselected.
   -  : Selected item, which will be displayed in the list.
   - : Unselected item, which will not be displayed in the list.
3. Click **OK**.

2.3.1 Search Channel

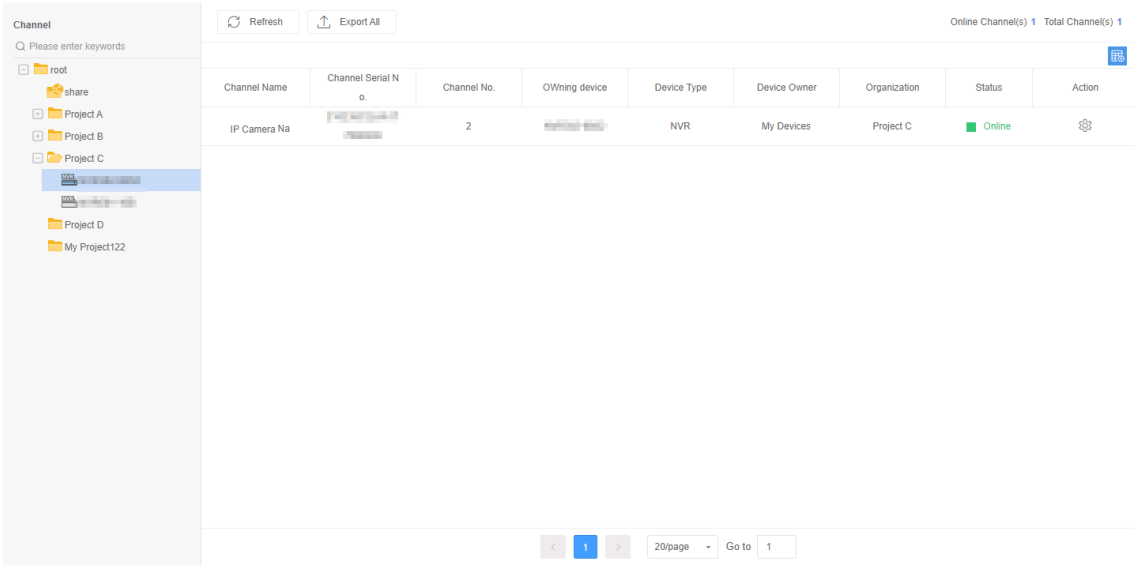
You can search for all devices and device channels under the organization.

Note: You can search channels of NVR (including video channels and radar channels), AIBOX, and multi-channel IPC.

1. In the left organization list, expand the organization list to show all the devices under the organization, and then click an organization to view the channels of devices under the organization.



2. Click the device to view the device channel list on the right side.



3. (Optional) Click **Export All** to export all device channel information under the root organization.

2.3.2 Channel Configuration

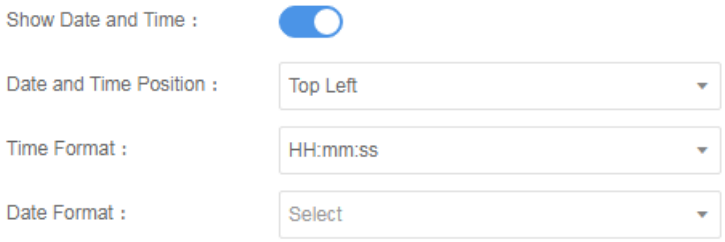
In the channel list, configure device channels using the operation column.

Note: The configuration items may vary with channels. Please refer to the actual interface.

Channel Configuration

Overlay time and date on the channel image.

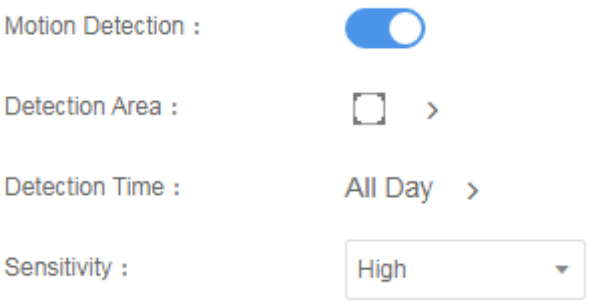
1. Click to display the **Channel Configuration** tab.
2. Click next to **Show Date and Time** to display the date and time.
3. Set the position and format for date and time as needed.



Arming Configuration

Enable motion detection to detect object movements in the image and be alerted by an alarm when motion is detected.

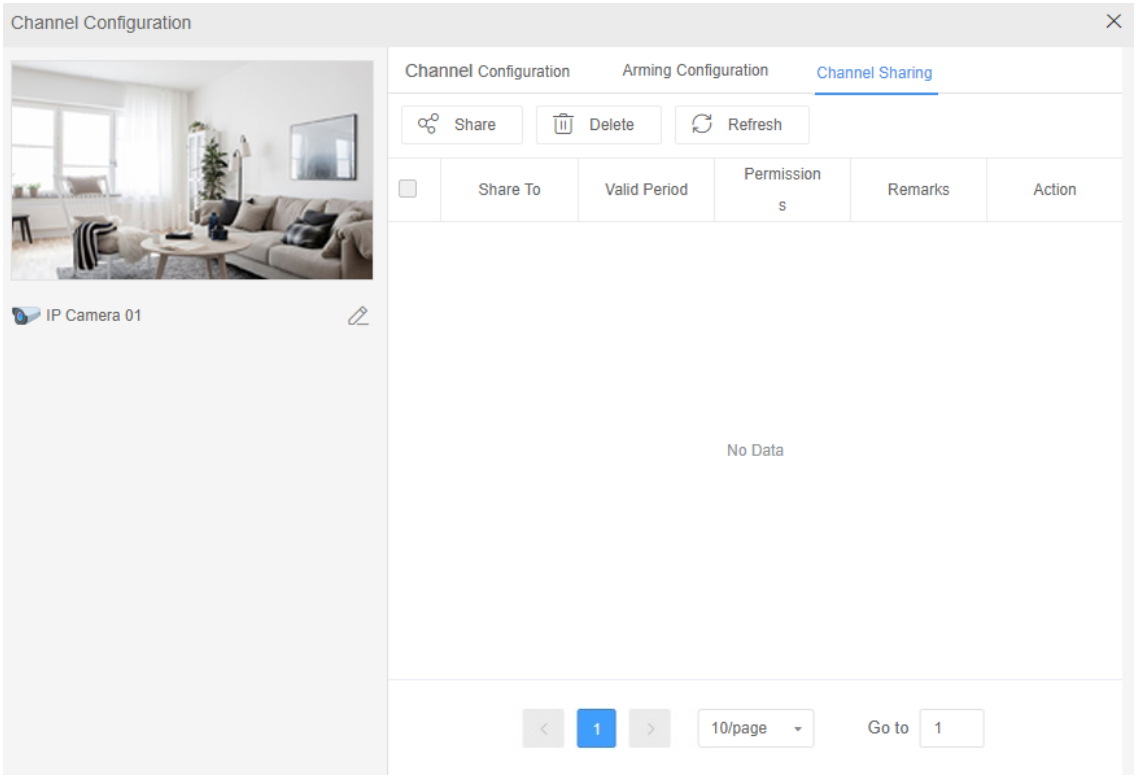
1. Click to display the **Arming Configuration** tab.
2. Click next to **Motion Detection** to enable motion detection alarm notification.
3. (Optional) Set alarm-triggered snapshot to automatically capture an image when an alarm occurs. Only channels of an NVR can be configured.
4. Set a detection area. Only motion within this area will be detected. By default, the detection area covers the entire screen.
5. Set the time when detection will take place.
6. Set the detection sensitivity. The higher the sensitivity, the more likely motion can be detected.



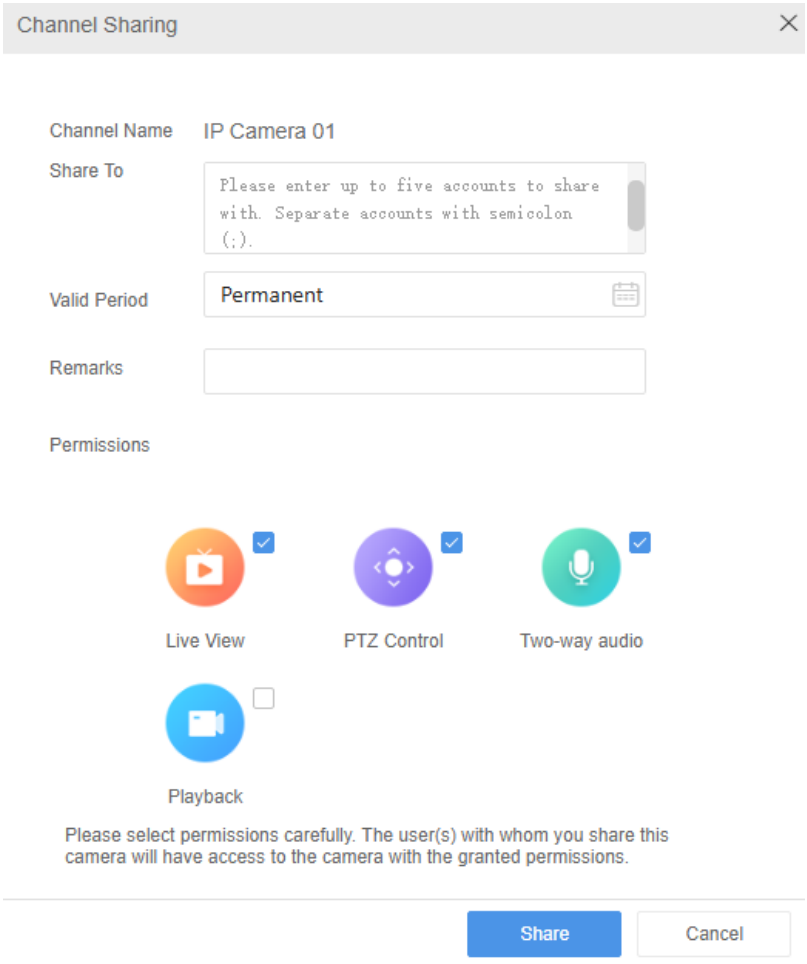
Channel Sharing

Share device channels with other users.

1. Click to display the **Channel Sharing** tab.



2. Click **Share**. A page as shown below appears.



3. Select the user(s) to share with and valid period, and enter remarks as needed.
4. Select the permission(s) to share. The user(s) with whom you share the channel will have access to the channel with the granted permission(s).
5. Click **Share**.

2.4 Sharing Management

2.4.1 Sharing

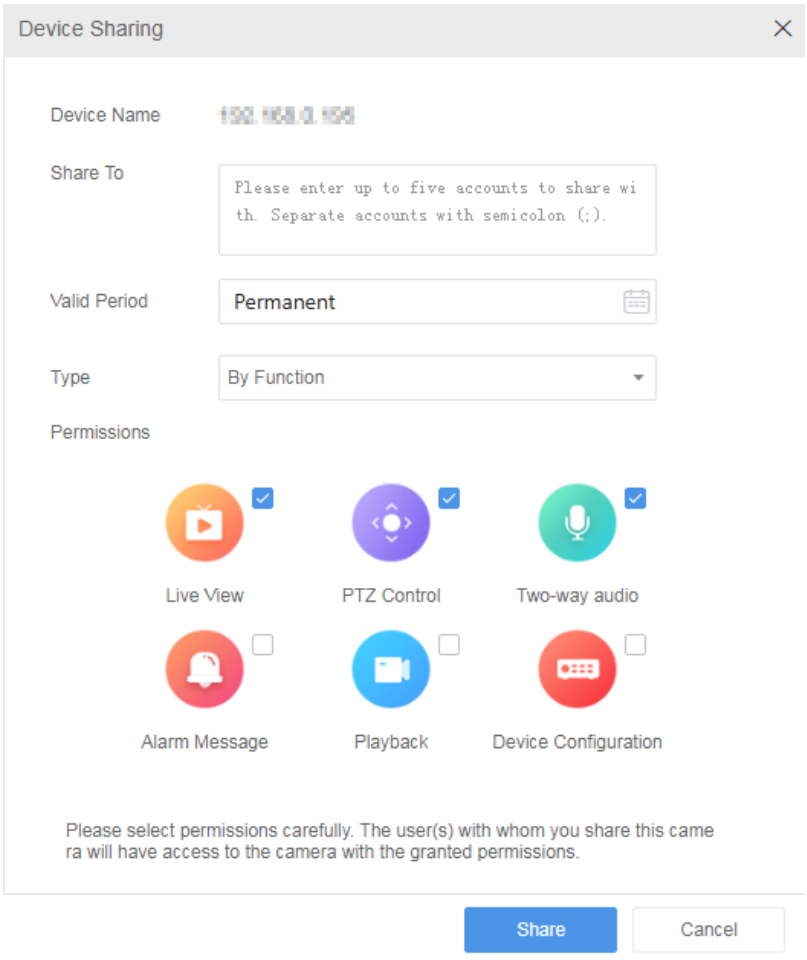
Purpose

Share resources under your cloud account with other cloud accounts and assign these accounts permissions.

- Device: Share devices with other cloud accounts.
- Channel: Share channels under a device with other cloud accounts. Permissions to configure devices and view alarm messages cannot be shared.
- Organization: Share an organization and devices in the organization with other cloud accounts.

Share devices/channels

1. In **Device Management** page, click ⚙ for the device you want to share.
2. Click the **Device Sharing** tab.
3. Click Share .



4. (Optional) Select the channels you want to share.
5. Set the accounts to share with, set a period for the sharing, and enter remarks as needed.
6. Select the sharing type.
   - By function: Select the function(s) directly, and then the user you share with can access the specified function(s).

     The user you share functions with must log in to his/her account on Guard Live APP, Guard Viewer APP, Star4live Web, or Guard Station in order to access and use the shared contents.

- By role: Select a role for the user you want to share with, and the user will have the corresponding role permissions. This function requires you to configure role permissions on the device side in advance.

  The user you share roles with must log in to his/her account on Guard Viewer APP, Star4live Web, or Guard Station in order to access and use the shared contents.

  Note: When you share by role, only the admin role will have the permission to operate on Star4Live web and software clients.

7. Click **Share**.

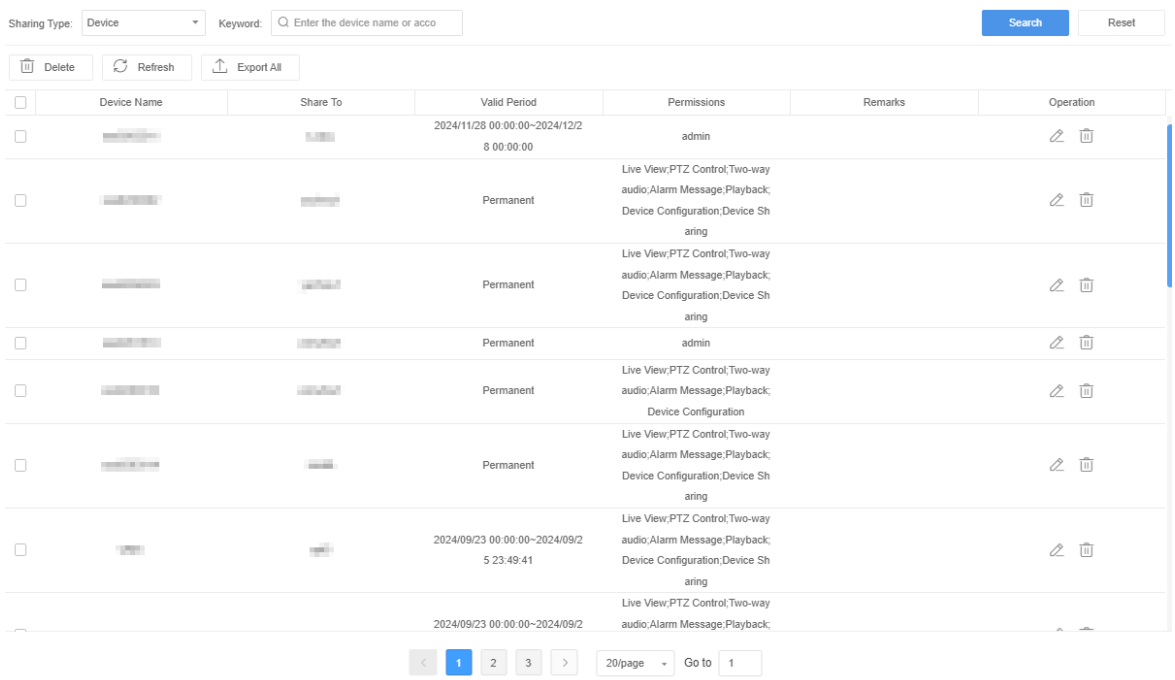
Share organizations

1. Go to **Organization Management**.
2. Click in the **Operation** column.
3. Set the accounts to share with, set a period for the sharing, and enter remarks as needed.
4. Select the sharing type.
   - By function: Select the function(s) directly, and then the user you share with can access the specified function(s).
   - By role: Select a role for the user you want to share with, and the user will have the corresponding role permissions. This function requires you to configure role permissions on the device side in advance.

     Note: When you share by role, only the admin role will have the permission to operate on Star4Live web and software clients.
5. Click **Share**.

2.4.2 View Sharing Records

View records of sharing with other cloud accounts. Go to the **My Sharing** tab.



Search: Select a sharing type (device/channel/organization), enter keywords, and click **Search**.

Export: Click **Export All** to export the sharing device list. This operation is available only when the **Sharing Type** is set to **Device** or **Channel**.

Edit: Click in the **Operation** column to modify the sharing validity period, remarks, and permissions.

Delete: Click in the **Operation** column or select item(s) and click **Delete**, and confirm the operation to cancel the sharing.

2.4.3 Cancel Sharing

Purpose

Cancel sharing manually before the end of the sharing period.

Steps

1. Click my picture in the top right corner on the homepage.
2. Choose **My Sharing** from the drop-down list.
3. In the **Operation** column, click for the device that you want to stop sharing.

2.5 My Profile

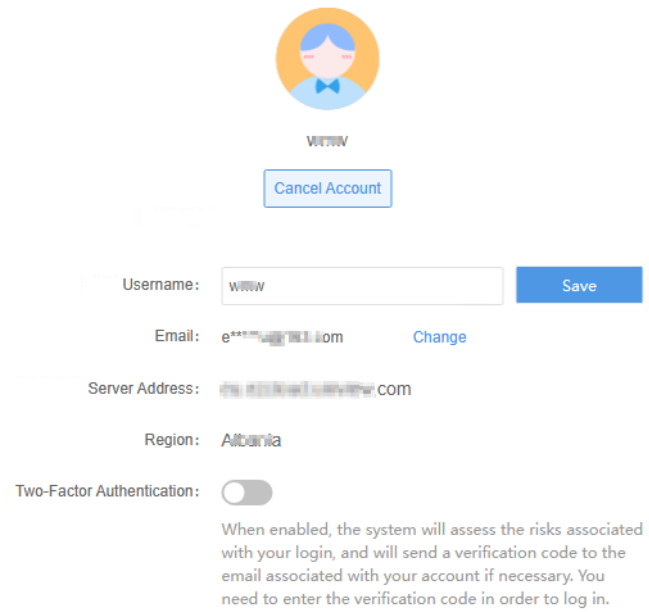
Click my picture in the top right corner on the homepage. You can change your account password, mobile phone number, and email address.

Note: Distinctions exist between end users and installers on this page. Please refer to the actual interface.

Personal Information

You can change your account information, including the username and email address.

Go to **My Profile** > **Personal Information**.

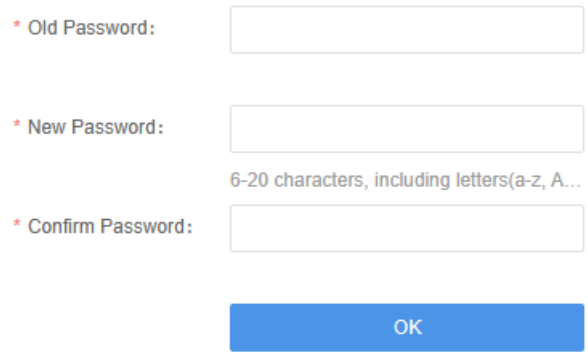


- Change Username: Enter the new username and click **Save**.
- Change Email Address: Click **Change** for the email address. After verification, you can set the new email address.
- Two-Factor Authentication: When enabled, the system will assess the risks associated with your login, and will send a verification code to the email associated with your account if necessary. You need to enter the verification code in order to log in.

  Note: When two-factor authentication is enabled, login is only allowed on clients that support two-factor authentication.
- Cancel Account: Click **Cancel Account**. After cancellation, you will not be able to log in to any client.

Change Password

Go to **My Profile** > **Change Password**.

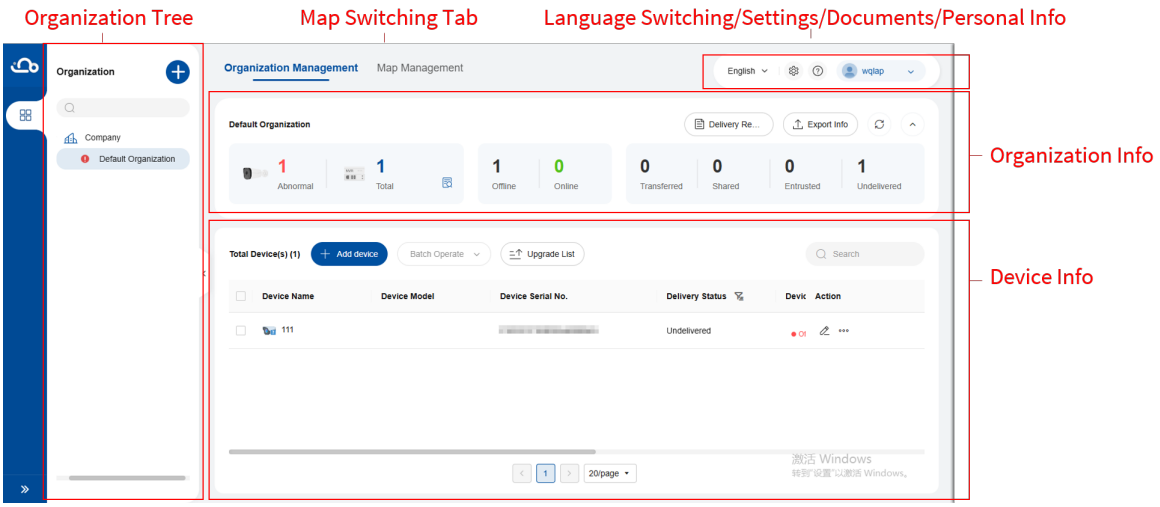


1. Enter the old password, new password and confirm the new password.
2. Click **OK**.

3 Installer Version

Installer can manage and configure devices by organization. Once services are completed, installer can deliver devices to end user, after which all installer permissions are revoked.

Note: For the mobile client, please download the Guard Live Pro app.



- Organization Tree: All organizations under the installer are displayed in a tree structure. Tap ‹ to hide; tap › to expand. You can use the top search bar to search for an organization.

  Icons before organization names indicate:

  - : There are undelivered devices under the organization.
  - : There are no devices under the organization.

  Each organization includes its organization information, device information, and map information. Select an organization in the left-side tree. The related information will display on the right side.

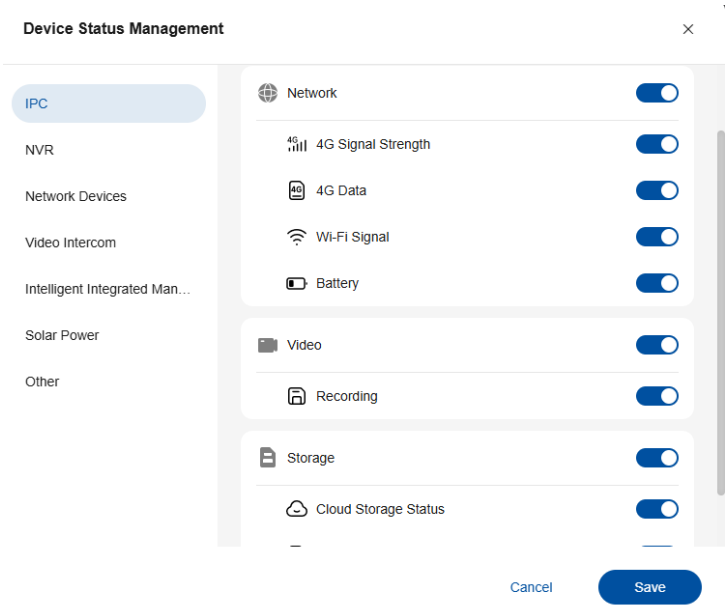
  For detailed instructions, see Organization Management.

- Map Switching: Select an organization in the left-side tree. Go to the **Map Management** tab. You can view the corresponding map information.

  For detailed instructions, see Map Management.
- Organization Information: Select an organization in the left-side tree. The organization information will display on the right side, including the organization name, device delivery status, etc. Tap to hide; tap to expand.

  For detailed instructions, see Manage Organization.
- Device Information: Select an organization in the left-side tree. The device list will display on the right side. Supported operations including device adding, batch restarts, etc.

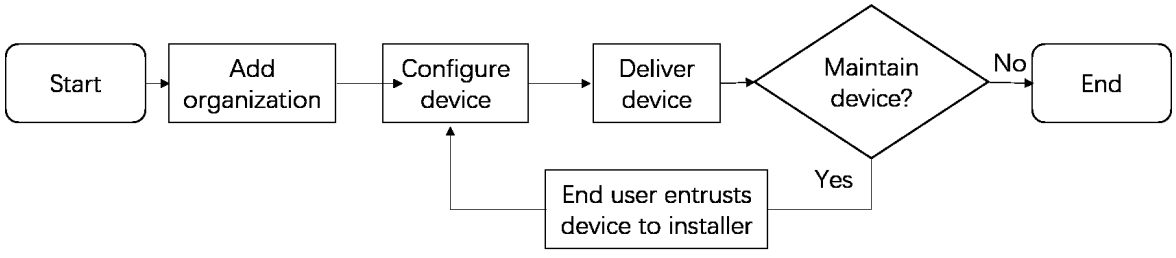
  For detailed instructions, see Device Management.
- Settings: Select > **Device Status Management**. You can choose the statuses to be displayed according to device groups. The statuses will be shown in the **Device Status** column of the device list below. For detailed instructions, see Device Status.



- Language Switching: Supports switching languages.
- Documents: Hover the mouse over . Here, you can choose to view the user manual, access the privacy policy (also available in My Profile).
- Personal Information
  - Click on the user information/**My Profile** to set the personal information, configure the account security and view the privacy policy.
  - Switch to End User: Click to switch to the end user version.
  - Logout: Click and confirm to log out.

3.1 Organization Management

The following flowchart illustrates the O&M services provided by installers to end users:



Function	Operation
Add Organization	Create organizations for different end users. See details in Add Organization.
Configure Device	Install and configure newly added devices. Operations such as device upgrades and renaming are allowed. See details in Device Management.
Deliver Device	Once services are completed, installer can deliver devices to end user, after which all installer permissions are revoked. See details in (Batch) Deliver.
Maintain Device	If an end user encounters issues after device transfer, they can entrust devices to an installer via the Guard Live app. The installer can then perform operations such as device upgrades and renaming. See details in Device Management.

The default organization (Company) cannot be deleted or edited. Devices under the default organization must be moved to other organizations before they can be delivered.

Organization status: The number next to each status indicates the number of devices in that status.

- Undelivered: The device has not been transferred to an end user.
- Transferred: The device has been transferred to an end user.
- Shared: The device has been shared with other users but has not been transferred to an end user.
- Handling: The device has been transferred to the end user. But due to the need for O&M, the end user can entrust devices to installer via the Guard Live app.

  Note: If the end user didn't select the **Device Config** permission during entrustment, the installer cannot access the device's Web interface for maintenance.

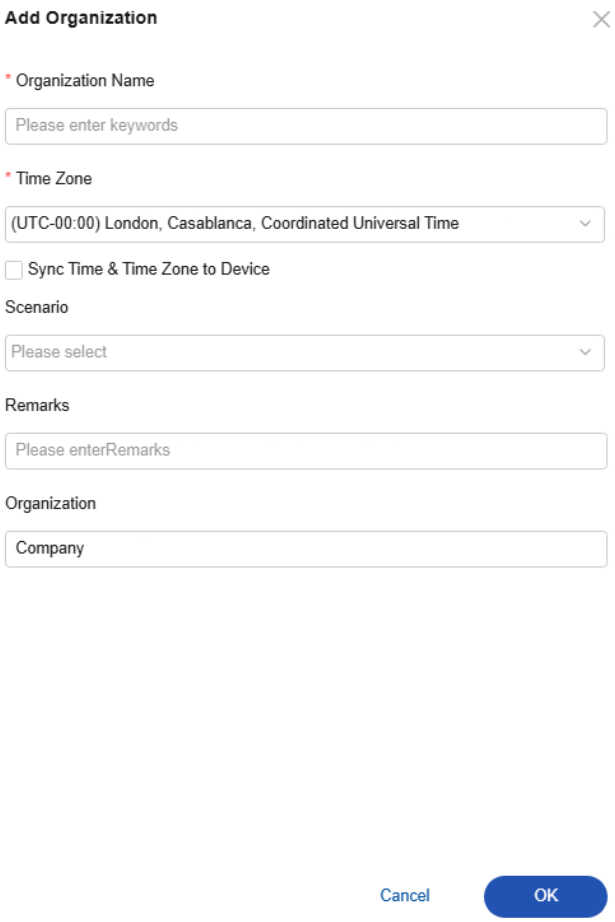
3.1.1 Add Organization

Up to 8 levels of organizations are allowed.

1. Select an organization in the left-side tree as the parent organization.

   Note: The parent organization cannot be changed once saved. Please choose carefully.

2. Click  . A window pops up on the right side.



3. Configure the organization parameters.
   - Organization Name (required): Set a custom organization name.
   - Scenario (optional): Select a scenario as needed.
   - Remarks (optional): Set the remarks as needed.
4. Click **OK**.

3.1.2 Edit Organization

The default organization (Company) cannot be edited.

1. Hover the mouse over an organization in the left-side tree and click ; or select an organization and click in the upper-right corner of the organization information. A window pops up on the right side.
2. Edit parameters as needed. The **Organization** field cannot be edited.
3. Click **OK**.

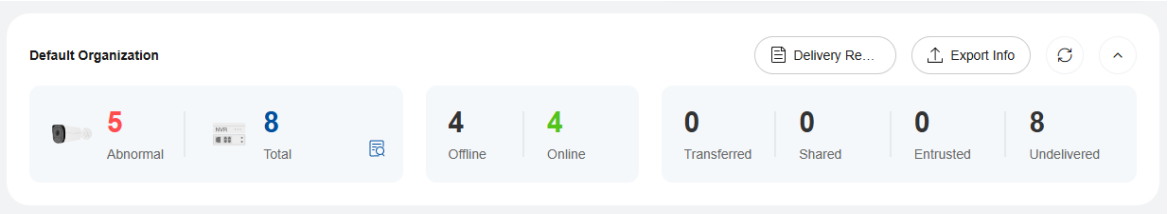
3.1.3 Delete Organization

The default organization (Company) cannot be deleted.

1. Hover the mouse over an organization in the left-side tree and click ; or select an organization and click in the upper-right corner of the organization information.
2. Click **OK** to confirm the deletion.

3.1.4 Manage Organization

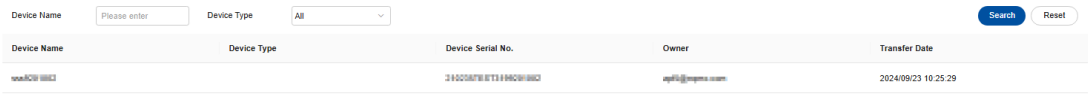
Select an organization in the left-side tree. The organization information will display on the right side.



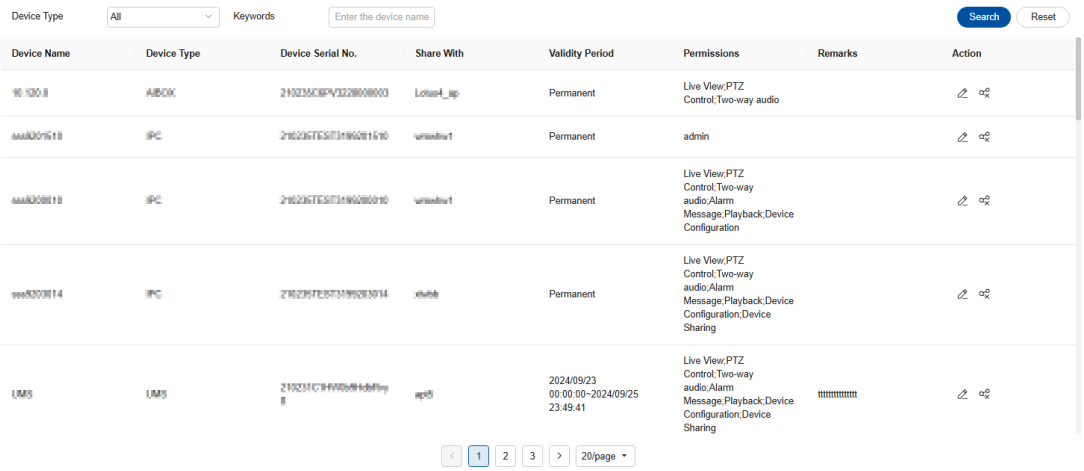
- Device status quantity display: The quantities of devices are displayed according to four delivery statuses: abnormal, all, online, and offline.

  Hover the cursor over to view the device count for each group.

- Deliver To: After transfer/sharing occurred, all recipient user information will be displayed here.
- Scenarios/Remarks: Customizable. You can click in the upper-right corner to edit them.
- Delivery Records: View records of device transfer and sharing.
  - Transfer Records: Search by device name and device type.



  - Sharing Records:

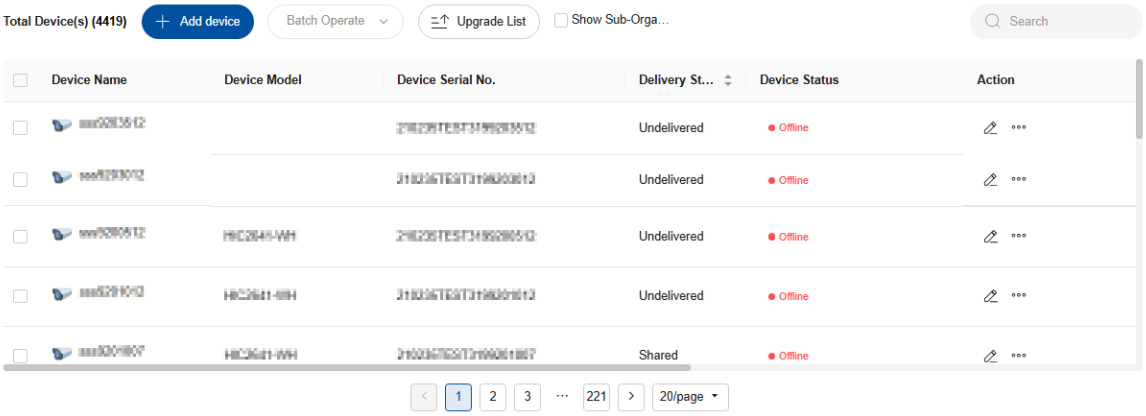


    - Search: Search by device type, device name, and sharing recipient.
    - Edit Permission: Click to edit the sharing validity period, remarks, and permissions.
    - Cancel Sharing: Click and confirm to cancel the sharing.

- Export Info: Click **Export Info** to export the organization information, excluding the **Parent Organization**.
- Refresh: Click to refresh the organization information and the device list, excluding the **Parent Organization**.
- Edit/delete: See Edit Organization and Delete Organization.

3.2 Device Management

Select an organization in the left-side tree. The device information displays on the right side.

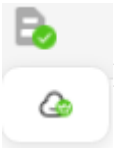


- For multi-channel devices, you can click **+** before the device name to expand its channel information; click **-** to collapse.
- Both **Delivery Status** and **Device Status** support clicking to filter by status (deselecting/selecting all indicates displaying all statuses). After filtering, the statistical data above will update accordingly.
- Physical topology: If switches exist under the organization, you can view the topology.
- If the organization contains sub-organizations, devices within sub-organizations are not displayed by default. To display these devices, select **Show Sub-Organization Devices** above the list.

3.2.1 Device Status

Only level-1 icons are displayed. The icon badge indicates there are no alarms in all level-2 functions; while indicates an alarm exists in the level-2 functions.

The device status can be shown or hidden. For detailed instructions, see Installer Version.

Click on a level-1 icon to display the included level-2 icon (e.g., ).

General Icons

Level-1 Icon	Description	Level-2 Icon	Description
Online / Offline	Device online/offline		
	Network status	/ / / / /	4G signal: strong -> weak/no signal
		/	4G data: data available (hover to view remaining data)/no data available
		/ / / / /	Wi-Fi signal: strong -> weak/no signal
		84 / 20	Battery level: > 20%/≤20%
	Video status	/	Recording status: recording channel exists (number indicates: number of recording channels/total channels)/no recording channel
		/	Online channel count (IPC/NVR/Switch only): no offline channel/offline channel exists Number indicates: number of online channels/total channels
	Storage status	/ / /	Cloud storage status: free trial available/in use/expire soon/expired

		/ /	SD card status: normal/SD card not inserted/ abnormal (hover to view abnormal info)
		/ / /	Disk status: normal/offline/damaged/disk not inserted

Icons Specific to Video Intercom Products

Level-1 Icon	Description	Level-2 Icon	Description
	Channel status	/	All normal/abnormal channel(s) detected The number means Normal Channels / Total Channels

Switch Icons

Level-1 Icon	Description
/	Power supply: normal/overload
/ /	Port bandwidth utilization: normal/busy (uplink bandwidth: 40%-80%)/congested (uplink bandwidth > 80%)
/	Loop: no loop/looped

SMBOX Icons

The SMBox consists of five types: Intelligent Cloud Management Server, Power Management Module, IPC, IP Speaker, and Solar.

You can expand the SMBOX to view all its included products.

Level-1 Icon	Description	Level-2 Icon	Description	
	Power supply	/ /	Voltage: normal/overvoltage/undervoltage Not applicable to the DC version of SMBox	
		/	Box leakage current status: normal/ leakage current	Available to AC models only
		/	Socket output: normal/overcurrent	
		/	Lightning: not hit by lightning/hit by lightning	
		/	Battery status: charging/discharging, charge/discharge protection or overcharge/overdischarge, charging/ discharging overcurrent, unable to charge, other abnormality triggered alarms	Applicable to the DC version only
	Operating environment	/ /	Temperature: normal/overtemperature/ undertemperature	
		/	Humidity: normal/humidity too high	
	Box door status			
	Channel list			
	Sub-list status			

	Battery	/	Battery status: charging/discharging, charge/ discharge protection or overcharge/overdischarge, charging/discharging overcurrent, unable to charge, other abnormality triggered alarms
			Battery voltage (numeric value representing the current voltage).
			Charging current (numeric value representing the current current).
			Discharging current (numeric value representing the current current)
			Remaining Battery Time, unit: hours
	Solar panel	/	Power generation status: active/inactive
			Solar voltage (numeric value representing the current voltage)

3.2.2 Search

Enter keywords (device name/device model/device serial number) in the upper-right corner of the device information to search.

3.2.3 Add

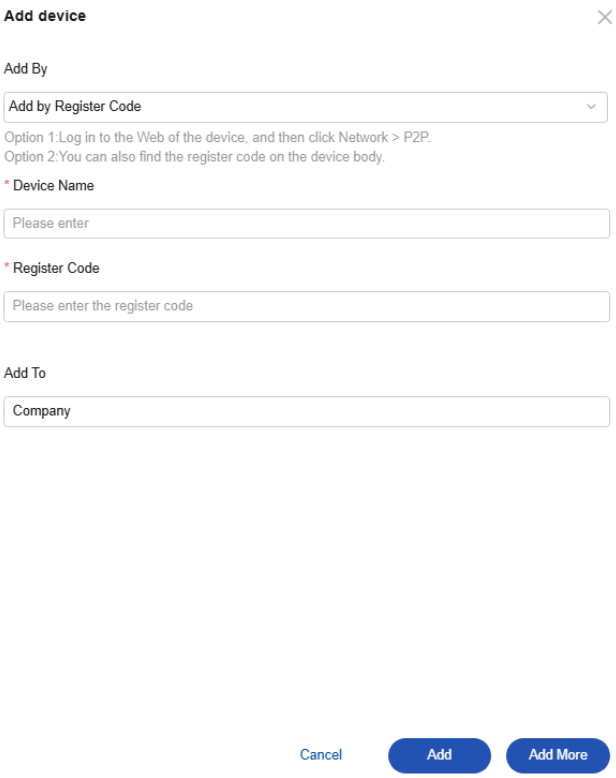
Note:

- A device can only be bound to one organization at a time.
- If a device is already bound to Organization A with a status of Undelivered or Shared, binding it to Organization B will automatically remove the device information from Organization A.

Choose a method to add device.

By Register Code

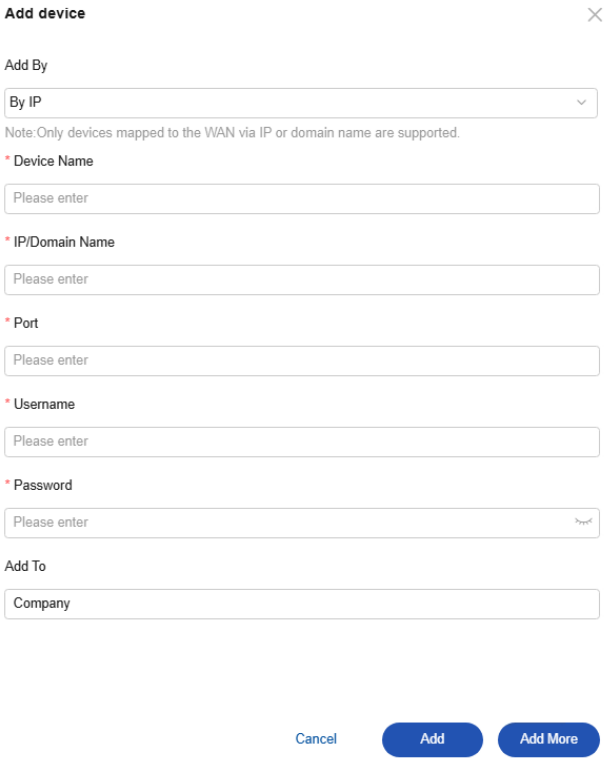
1. Click **Add device**. In the pop-up window, select **Add by Register Code** for **Add By**.



2. Enter the device name and register code (find it by referring to the descriptions on the actual interface).
3. Click **Add** to add the device and exit. To add more devices, click **Add More**.

By IP

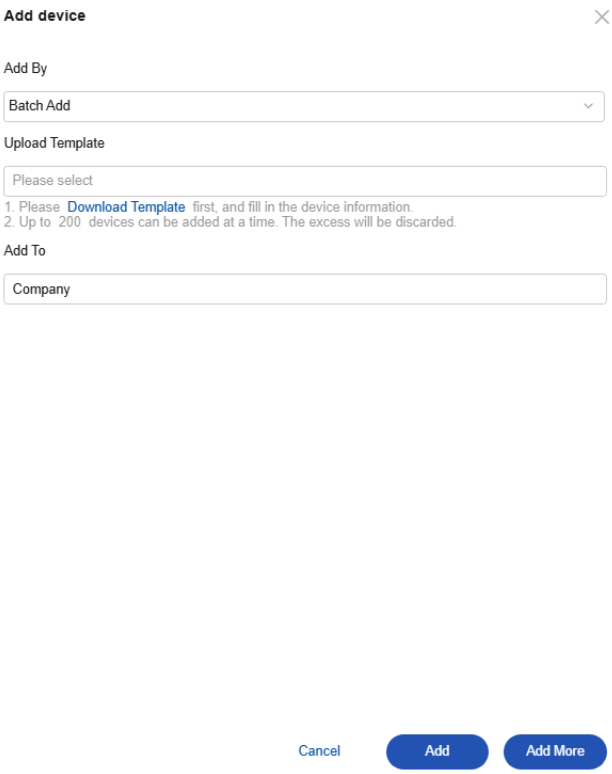
1. Click **Add device**. In the pop-up window, select **By IP** for **Add By**.



2. Enter the device name, IP/domain name, port, username, and password.
3. Click **Add** to add the device and exit. To add more devices, click **Add More**.

Batch Add

1. Click **Add device**. In the pop-up window, select **Batch Add** for **Add By**.



2. Click **Download Template** and follow the instructions in the template to fill in the device information.

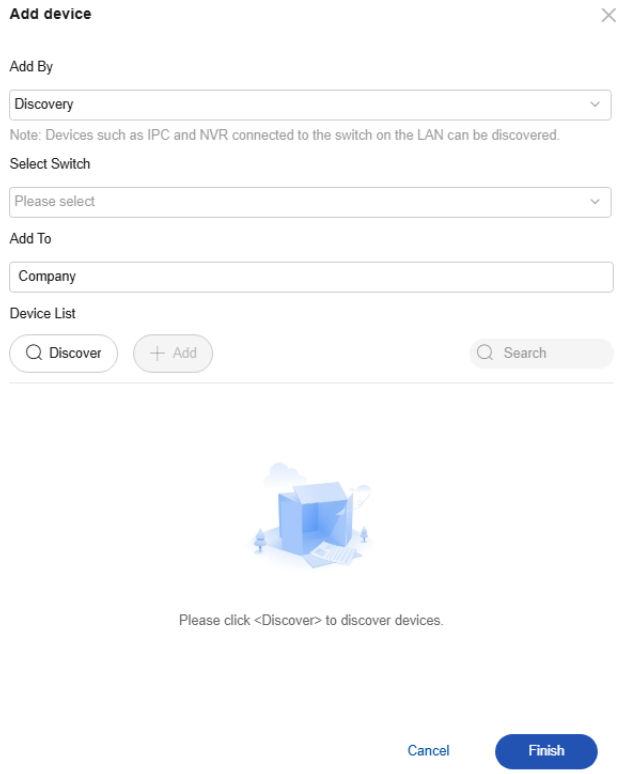
   Note: Up to 200 devices can be added at a time. The excess will be discarded.

3. Click **Please select** to upload the modified template.
4. Click **Add** to add the device and exit. To add more devices, click **Add More**.

By Discovery

Discover devices such as IPCs and NVRs connected to the switch on the LAN and add them in batches.

1. Click **Add device**. In the pop-up window, select **Discovery** for **Add By**.



2. Select switch(es) for discovery.
3. Click **Discover** to start the discovery. The system will attempt to add devices using the default username (admin) and password (123456). The discovered devices will be listed.
4. Select device(s) and click **Add**.
   - If the device status is **Correct username and password**, the device will be added automatically, and the status will change to **Added**.
   - If the device status is **Incorrect username and password**, enter the correct username and password in the pop-up window. After successful verification, the status will change to **Added**.

     Note: The device will be locked after 4 consecutive failed login attempts. Please check carefully.

5. Click **Finish**.

3.2.4 Edit

Click for a device. Edit the device name, and then click **OK** to save.

3.2.5 (Batch) Delete

Note: The **transferred** devices cannot be deleted.

Click for a device and click **Delete**; or select device(s) and click **Batch Operate** > **Batch Delete**. Then confirm the deletion.

3.2.6 Batch Restart

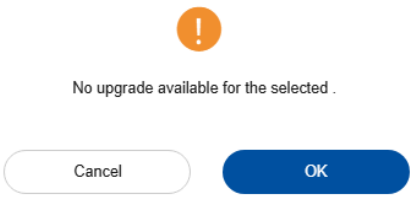
1. Select device(s).
2. Click **Batch Operate** > **Batch Restart**.
3. Click **OK** in the pop-up window.

3.2.7 Batch Upgrade

When a new software version is detected for an **Online** device, an icon will appear next to the version number. To upgrade the device, follow these steps:

1. Select device(s).
2. Click **Batch Operate** > **Batch Upgrade**.

- If no upgrades are available: Click **OK** in the pop-up window and select different devices.



- If an upgrade is available: The number of devices that can be upgraded is displayed in the pop-up window. Click **OK** to start the upgrade.

  The upgrade progress 

 is shown in the **Version No.** column. You can also check the progress by clicking **Upgrade List**.

  Once the upgrade is completed, the device will restart automatically. (If you click **Refresh** during this period, the device status is **Offline**.) After approximately 3-5 minutes, click **Refresh** to update the list. If the device status is to **Online**, the upgrade was successful.

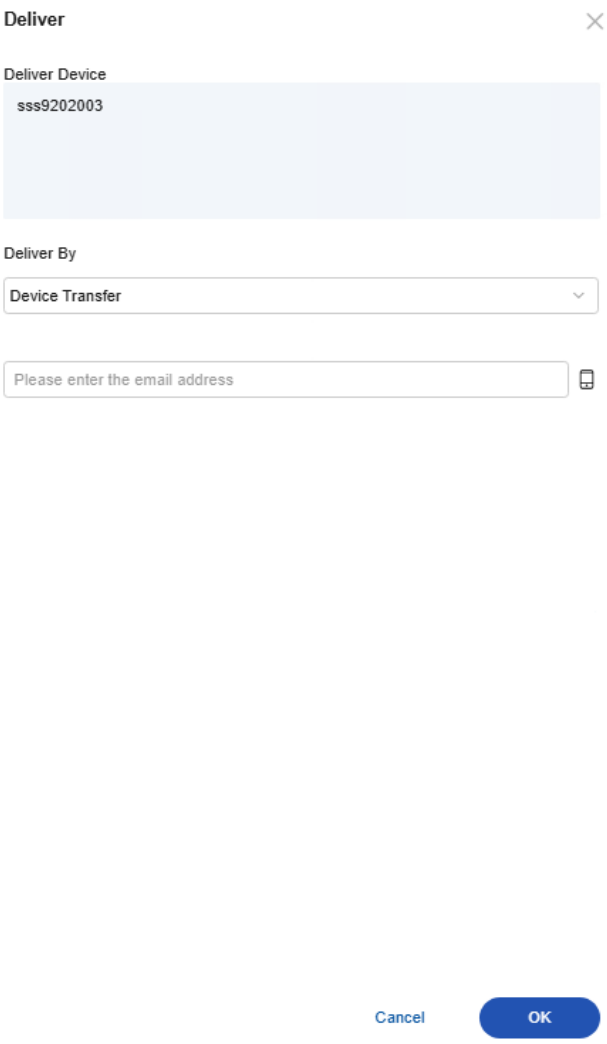
3.2.8 (Batch) Deliver

Deliver devices to end users via transfer and sharing.

- Transfer: After transferring a device to a specific user, the installer will no longer have any operation permissions on that device.
- Sharing: Share devices with multiple Star4Live users or unregistered users to allow for functions such as live view and two-way audio. The installer retains all operation permissions on that device. Also, the sharing can be cancelled.

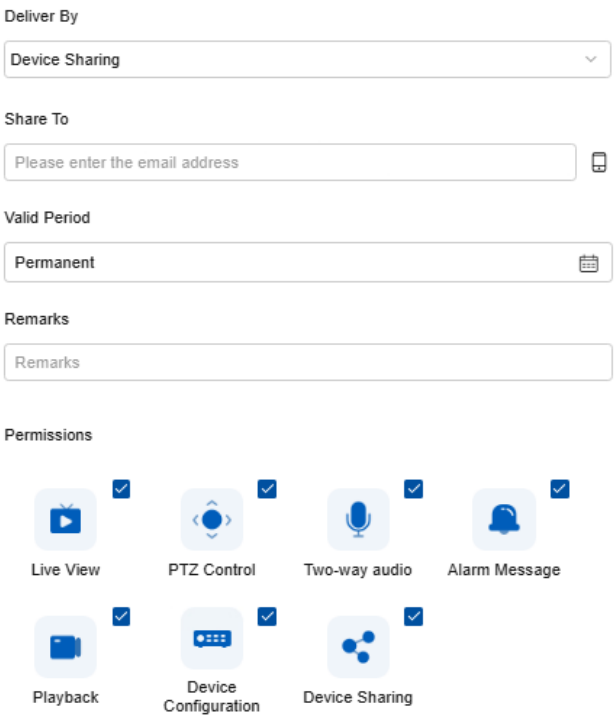
Note: Devices under the root organization, devices that have already been transferred, and devices in handling status cannot be delivered.

1. Click ••• for a device and click **Deliver**; or select device(s) and click **Batch Operate** > **Batch Deliver**. A configuration window pops up on the right side.



2. In the **Deliver By** field, select the transfer method (Device Transfer/Device Sharing). Configure the corresponding parameters.
   - Device Transfer: Enter the recipient's account.
   - Device Sharing: Set the user account you want to share the device with, the validity period (default is permanent; click the text box to set a custom start and end time), remarks, and permission(s) for sharing.

     Note: If any recipients have not yet registered, they must first complete the registration process as prompted. After logging in, they can access the shared devices according to their assigned permissions.



3. Click **OK**.

You can view historical transfer and sharing records by clicking **Delivery Records**.

3.2.9 Batch Export

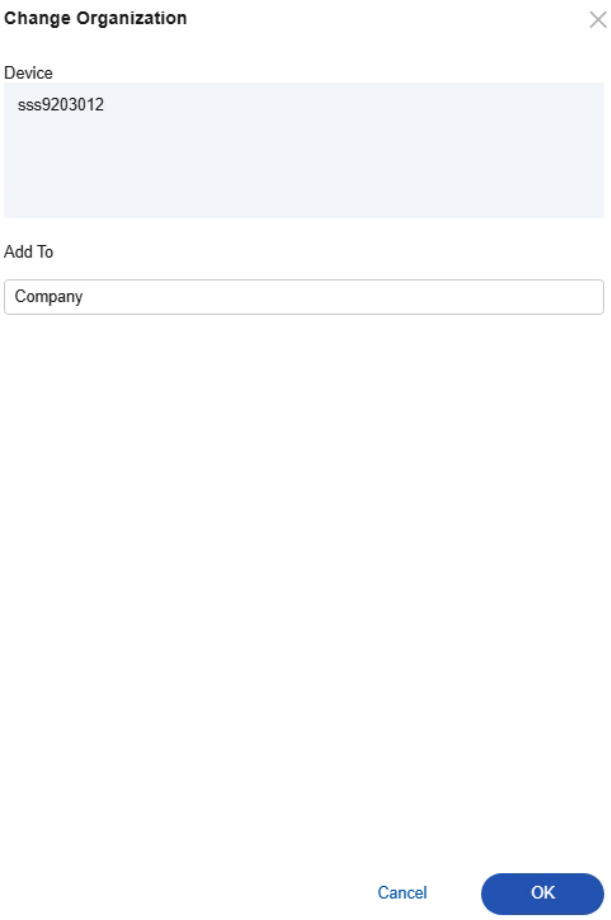
Export device information (device name, device model, serial number, type, delivery status, organization information, etc.) to local.

1. Select device(s).
2. Click **Batch Operate** > **Batch Export** to download the device information. Filename: DeviceDetail.

3.2.10 Change Organization

You can move devices with a delivery status of Undelivered or Shared to another organization.

1. Select device(s).
2. Click **Batch Operate** > **Change Organization**. A configuration window pops up on the right.



3. Click on the current organization name to display the organization tree.
4. Select a new organization.
5. Click **OK**.

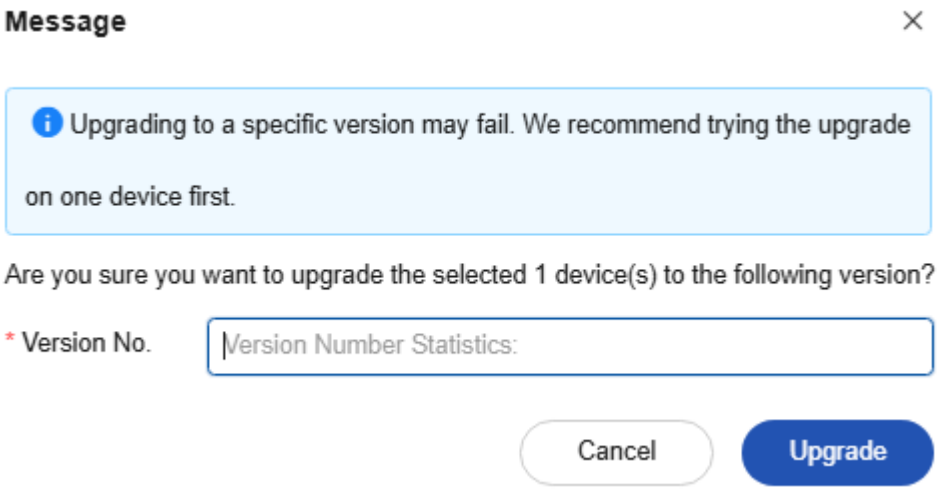
3.2.11 Specify Upgrade Version

This function is intended for on-site service personnel and can help resolve on-site anomalies.

Note:

- The target software version must be uploaded to the designated platform by a technician first.
- Upgrading to a specific version may fail. We recommend trying the upgrade on one device first.

1. Select device(s).
2. Click **Batch Operate** > **Specify Upgrade Version**. A window pops up.



3. Enter the target software version number.
4. Click **Upgrade**.

3.2.12 Access Device's Web Interface

Only **online** devices' Web interface can be accessed.

Click ⊖ for an online device to access its login page. You can perform operations on the device after login.

If the system detects that the plug-in is not installed, a Message window will pop up. You can click **Download** to download the plug-in.

3.2.13 Restart

If the device is online, you can click ✳ for the device and confirm the operation to restart the device.

Note: Restarting the system will affect the ongoing device services. Please handle with caution.

3.2.14 Live View

You can view the live video of the **online** IPCs, NVR channels, and IPC channels under the box.

Tap the corresponding ••• **> Live View**. A pop-up window appears.

Note: If the plug-in is not installed, please follow the on-screen instructions to complete the installation and then replay.

If the video continues playing for 20 minutes, it will stop automatically. Tap **Resume** to continue.

When you place the cursor on the live video image, operation buttons will appear as explained below.

	Description
Window Layout	• : Display the video image in the full window. • : Display the video image adaptively.
Snapshot	Tap to capture the current image and save it locally.
Volume Adjustment	Tap to adjust audio volume.
PTZ Control	Available to PTZ cameras only. Place the cursor at an edge of the image to display directional arrows, and then tap to rotate the camera.
Full Screen/Exit Full Screen	Tap to enter full screen mode, tap or press **Esc** to exit.

3.2.15 Device Details

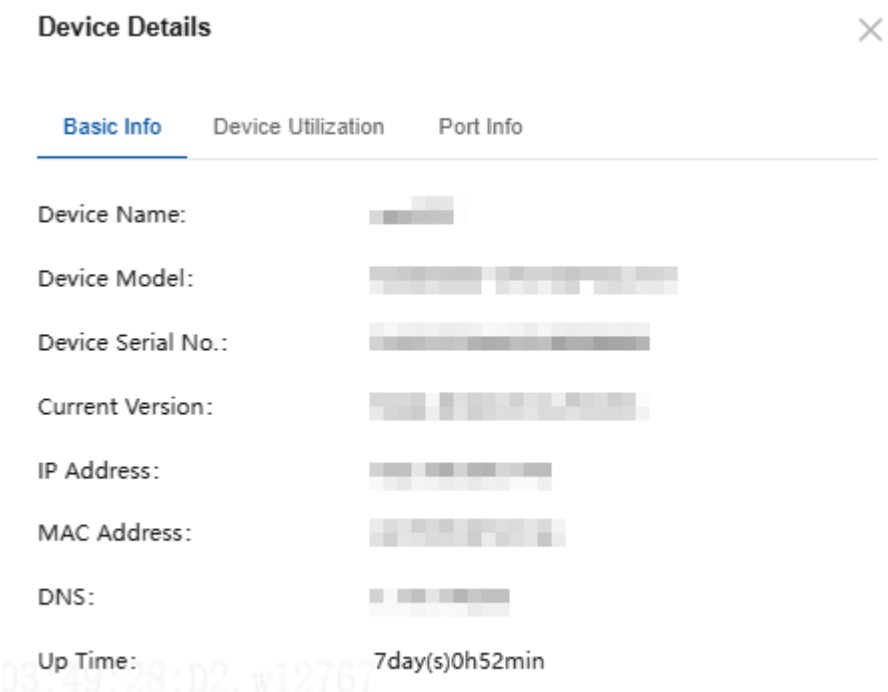
Device details are available for wireless bridges and switches.

Note: For wireless bridges, this feature is only available in versions that support LAPI. If the feature is not displayed, please upgrade your device to the latest version.

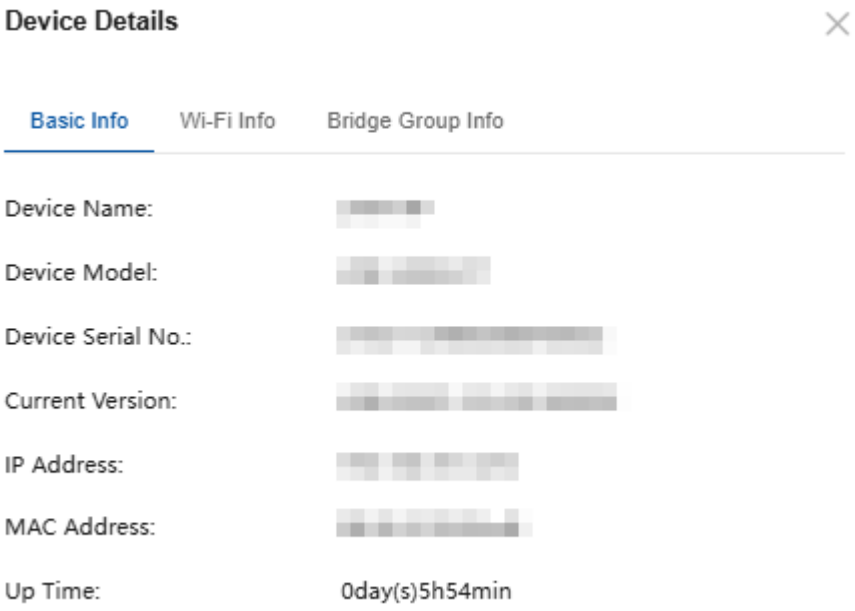
Click the corresponding ••• **> Device Details**

The specific details displayed vary by device type. Please refer to the actual user interface.

- Switch



- Wireless bridge



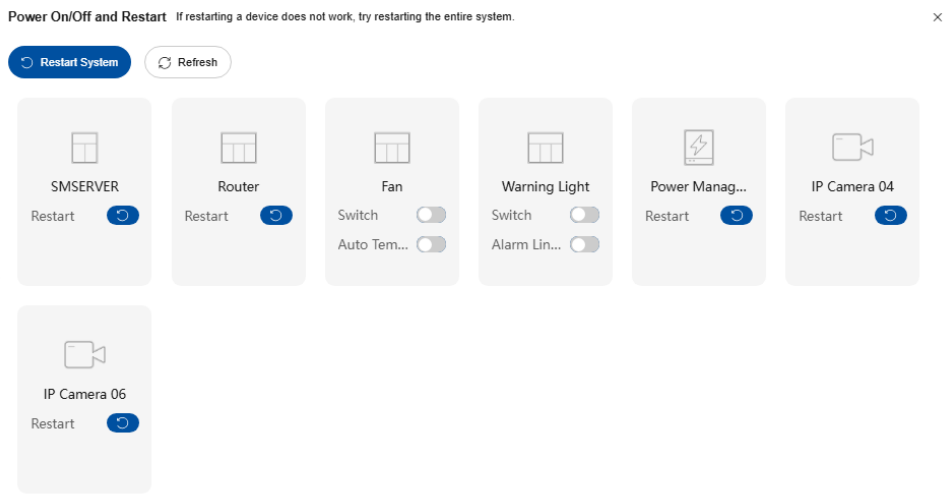
3.2.16 Port Management

If the **power management module** is **online**, port management is supported.

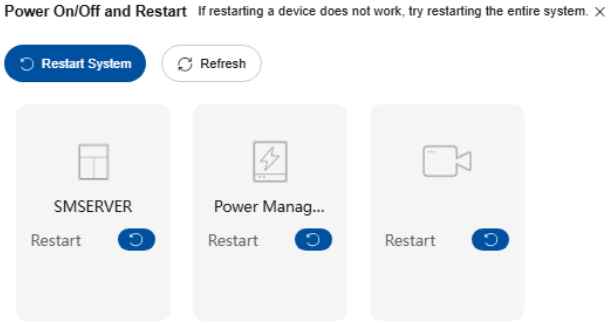
Click ⏻ for a power management module, a window pops up.

Note: The supported functions may vary with the power supply method of the power management module. The figure below only shows an example.

AC models



DC models



- Restart System: Restart all the devices in the list.
- Refresh: Refresh the status of all the devices in the list.
- : Click and confirm the operation to restart the device.
- : Status: Enabled. Click to disable the corresponding function.
- : Status: Disabled. Click to enable the corresponding function.

3.2.17 Load Restart

Solar system load: Refers to devices connected to the solar system for power, such as cameras, O&M modules, etc.

If the **solar system** is **online** and it is loaded with devices, you can restart the connected devices that are online by one click.

Click the corresponding ••• **> Load Restart**, and then confirm to restart.

3.2.18 Enable/Disable Battery Level OSD

When the **solar system** loads the IPC, the battery information can be displayed on the IPC's live view page. You can enable/disable OSD remotely as needed.

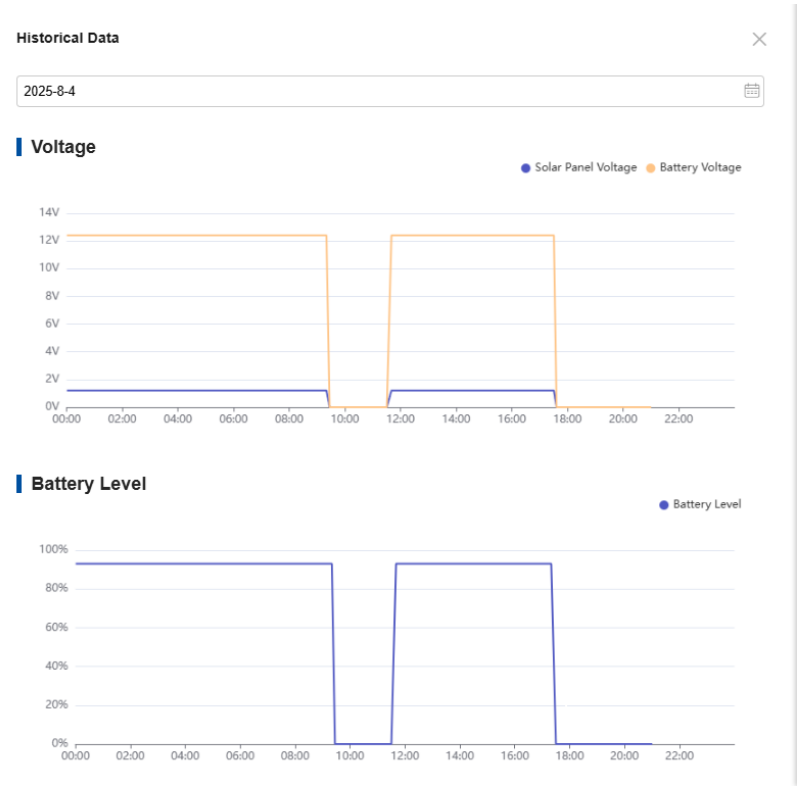
Click the corresponding ••• **> Enable/Disable Battery Level OSD**. The command will be sent to the IPC.

Note: If it indicates that the operation is completed but it does not take effect on the IPC's web interface, please go to the OSD configuration page on the solar system's web interface to check if the parameters have been successfully set.

3.2.19 Historical Data

You can view the daily changes in **solar system's** voltage and battery level.

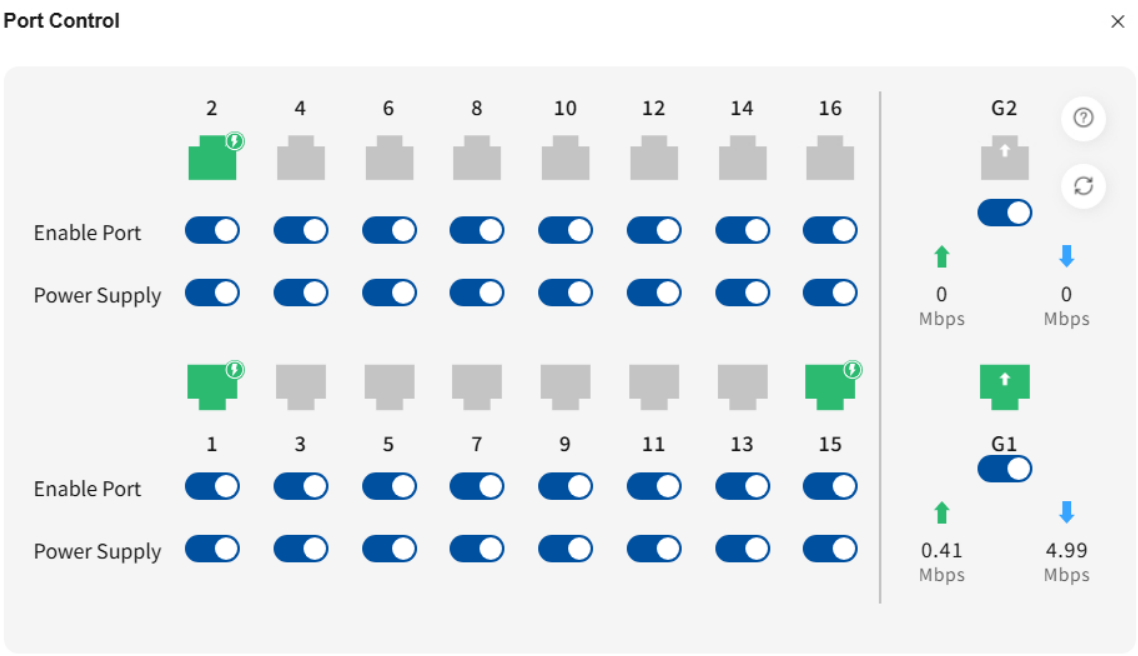
Click the corresponding ••• **> Historical Data**, and a pop-up window appears.



3.2.20 Port Control

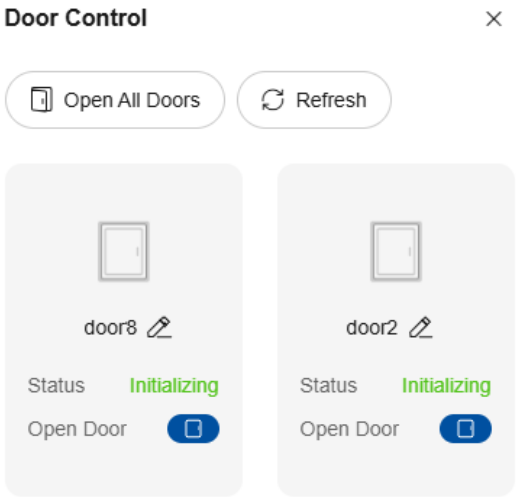
You can control the port switch and power supply switch of certain switch models.

Click the corresponding ••• **> Port Control**.



3.2.21 Door Control

Click the corresponding ••• **> Door Control**. A window appears.



- Open All Doors: Click to open all doors.
- Refresh: Click to refresh door status.

Status	Description
Initializing	The door has just been installed and powered on, and has not been opened or closed yet.
Closed	The door is closed and can be opened manually.
Not Closed after Timeout	The door is open but has not closed within the set time period.

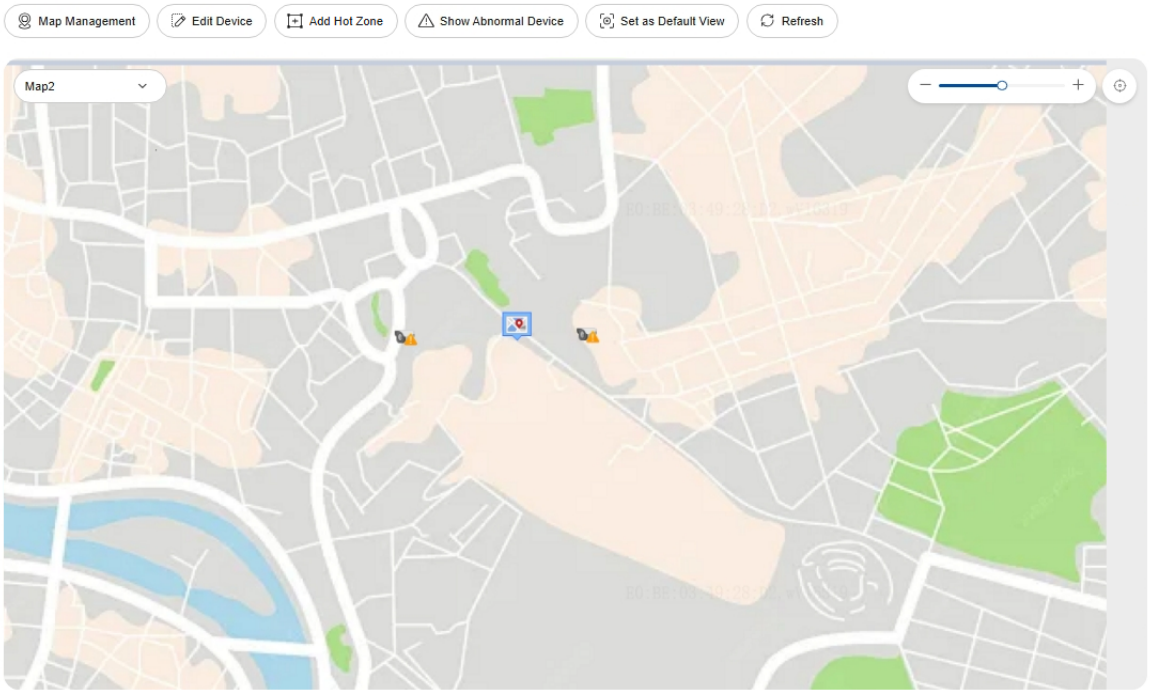
- Change door name: Click to change the name of a door.

- Open door: Click  to open the corresponding door.

3.3 Map Management

Mark device installation locations on map to visualize device distribution and promptly find any abnormal devices.

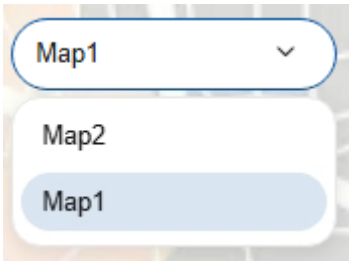
Select an organization in the left-side tree, and then go to the **Map Management** tab.



For the first-time use, you need to add a map and a device first.

Switch Map

By default, the first map in the list is displayed. You can switch between maps in the drop-down list.



The map display order in the list can be adjusted in Map Management > Switch Display Order.

Zoom on Map

Use the mouse wheel, **-/+** buttons in the upper-right corner of the map, or the slider in the upper-right corner of the map to zoom in or out.

Move Map

Hover the mouse over the map, hold the left mouse button, and drag to move the map.

Back to Default View

Click  in the upper-right corner to reset the map to the default view.

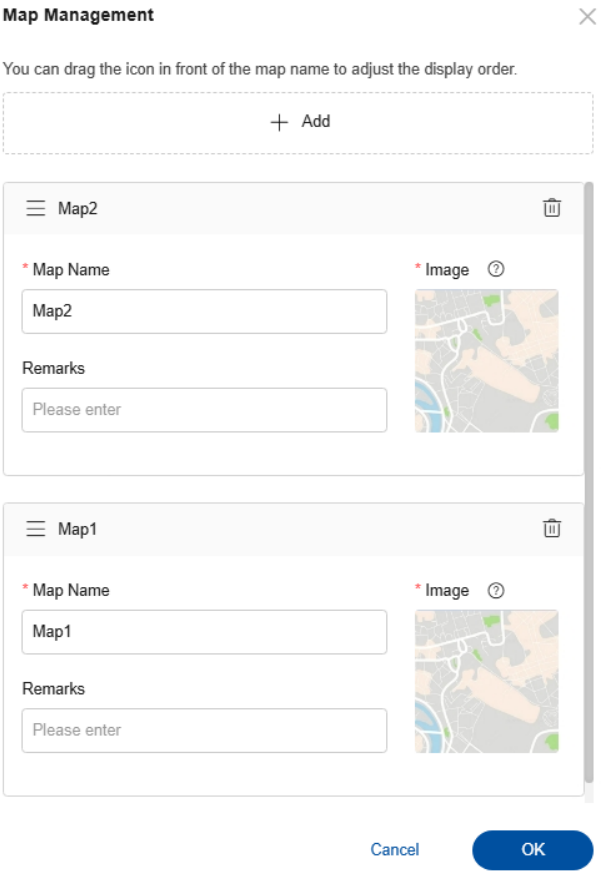
You can also set a custom default view. See Set Default View.

Refresh

Click **Refresh** to update the status of all devices.

3.3.1 Map Management

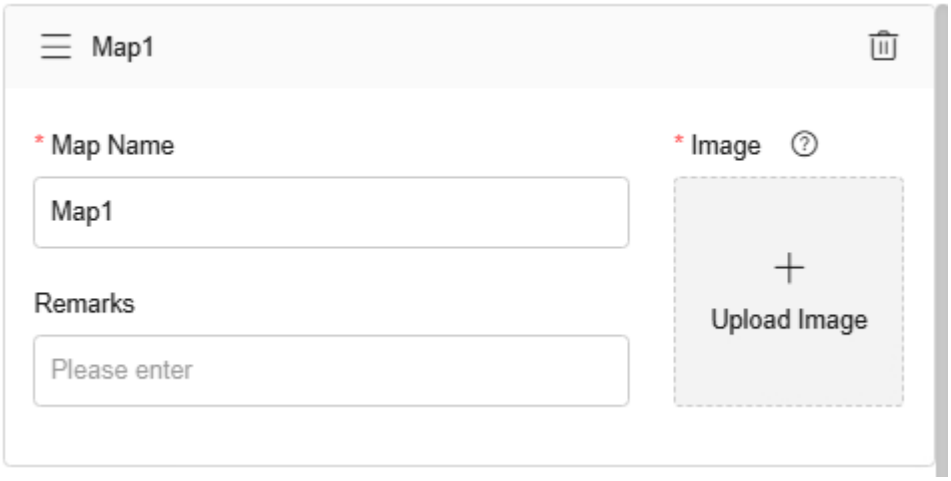
For the first-time use, please click **Add Map** to add a map first; If there is already a map, click **Map Management** to display the configuration window on the right side.



Add

Up to 10 maps are allowed per organization.

1. (Skip on first-use) Click **Add**.



2. Set a custom map name. By default, the map will be named as “Map 1”, “Map 2”, etc.
3. Click **+** to upload a map. Please upload a JPG/JPEG/PNG image. Max. size: 10M. Max. resolution: 8190*8190px.
4. (Optional) Enter remarks.
5. Click **OK**. The latest added map will be displayed first. You can also Switch Display Order.

Edit

Edit the map parameters as needed. Click **OK**.

Delete

Click for a map and click **OK**.

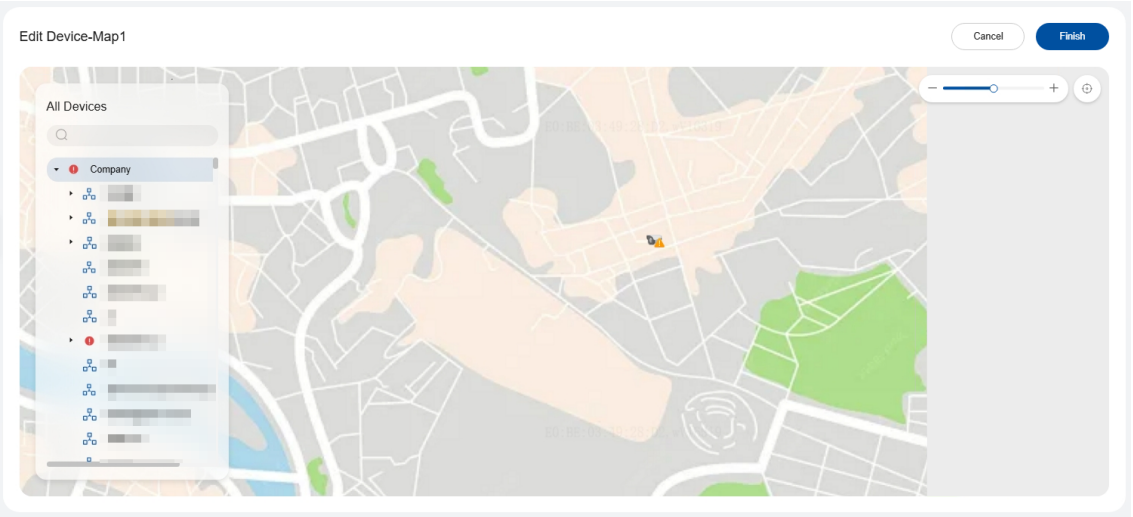
Switch Display Order

Drag the icon before the map name to adjust the display order as needed.

3.3.2 Edit Device

Add, delete, and move devices on the map.

1. Choose a map.
2. Click **Edit Device**. The organization tree displays on the left side.



3. Follow the instructions below to perform operations.
   - Add

     (1) Zoom and move the map to the device installation location.

(2) Select a device in the organization tree. You can also search for the device using the top search bar.

(3) Drag the device to the desired location on the map.

- Delete

  (1) Click on the device icon and verify the device name.

  (2) Click .

- Move: Drag the device icon to the desired location on the map.

4. Click **Finish**.

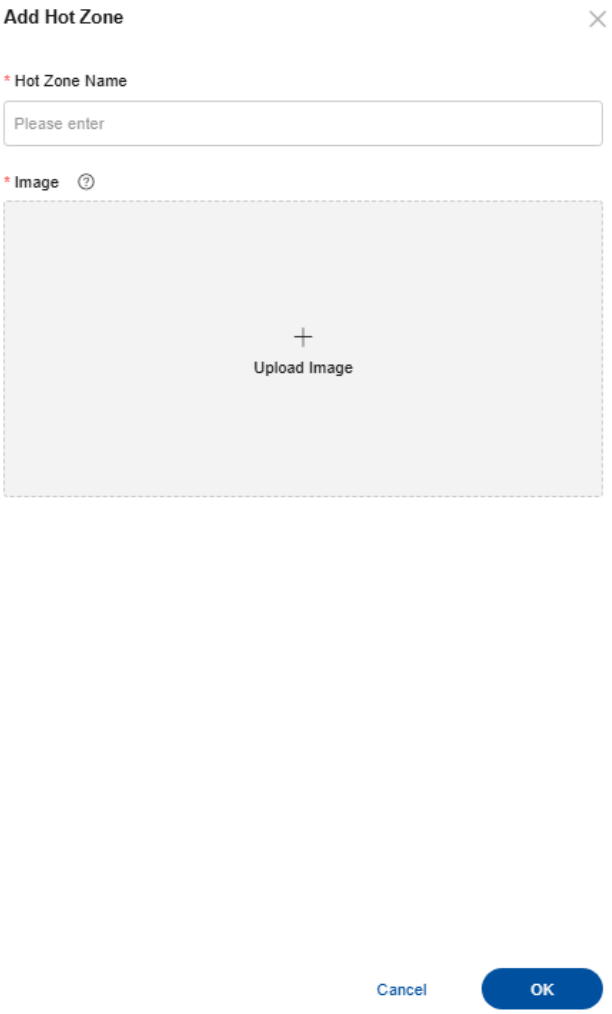
3.3.3 Hot Zone

A hot zone is a specific area on the map where activities, events, or certain phenomena occur more frequently than in other areas, such as malls and tourist attractions.

Supports zooming in again on the hot zone for enhanced detail control.

Add Hot Zone

1. Click **Add Hot Zone**.
2. Click on the desired location on the map (excluding device icons). A configuration window pops up on the right side.



3. Set the hot zone name and upload a hot zone image (must meet the requirements on the actual interface).
4. Click **OK**.
5. (Optional) To add more hot zones, repeat the steps 2-4.
6. Click **Cancel** to exit.

Enter Hot Zone

Double-click a hot zone icon ; or select > .

You can add device information to the hot zone. See instructions in Edit Device.

Move Hot Zone

Move a hot zone to a different location on the map.

1. Click a hot zone icon, and then click .
2. Click on the new desired location on the map.

Edit Hot Zone

1. Double-click a hot zone icon , click **Edit Hot Zone**; or select > .
2. Edit the hot zone name and update the hot zone image as needed.
3. Click **OK**.

Delete Hot Zone

Deleting a hot zone will also delete any devices within it.

Click a hot zone icon, click , and then confirm the deletion.

3.3.4 Show Abnormal Device

1. Choose a map.
2. Click **Show Abnormal List**. A list of abnormal devices will be displayed on the right side, summarizing all faulty device information.

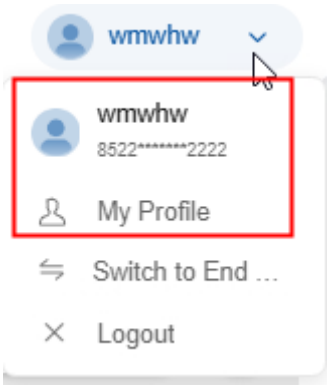
3.3.5 Set Default View

Each map has a default view. When you switch to the map, the default view is displayed. After zooming or moving the map, you can Back to Default View.

1. Choose a map.
2. Zoom and move the map to the desired view.
3. Click **Set as Default View**.

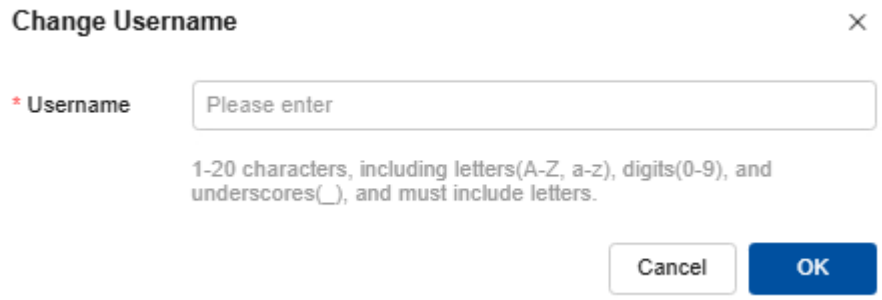
3.4 My Profile

Click in the red box to access **My Profile**. To exit, click on the left side.

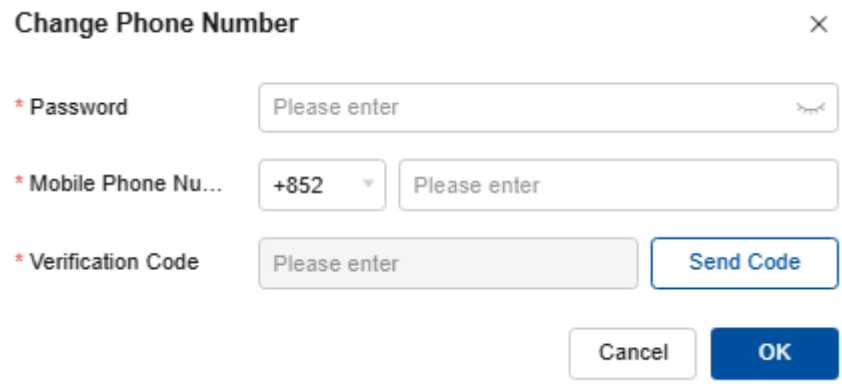


Personal Information

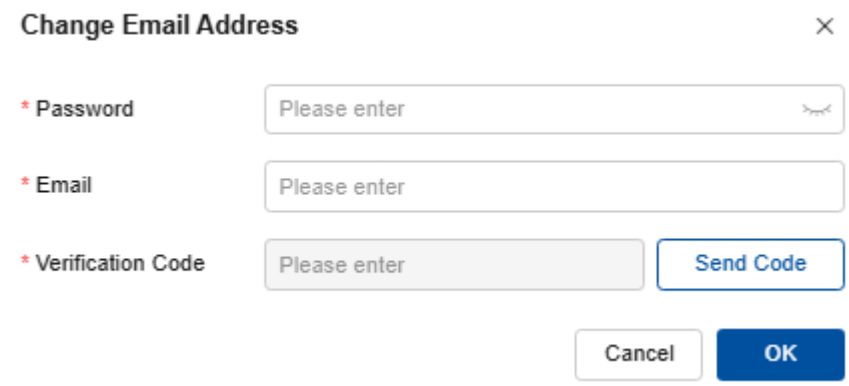
- Change Username: Click **Change** for **Username**. Enter a new username (1-20 characters, including letters, digits, and underscores(_), and must include letters), and then click **OK**.



- Change Phone Number: Click **Change** for **Phone No.**. Enter the login password and the new phone number, click **Send Code**, enter the received verification code, and then click **OK**.

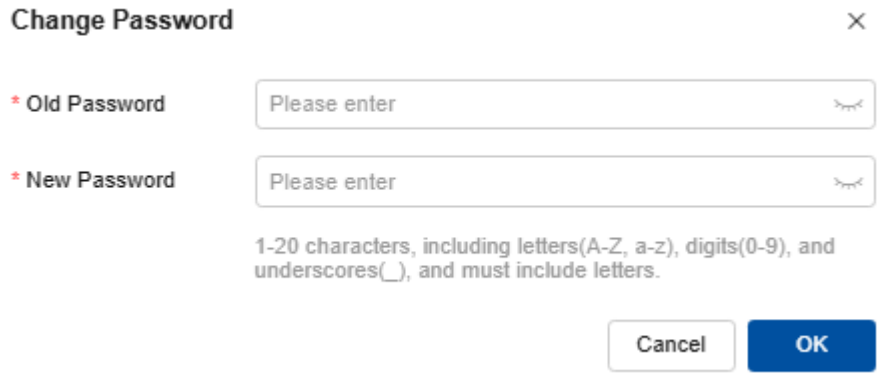


- Change Email: Click **Change** for **Email**. Enter the login password and the new email address, click **Send Code**, enter the received verification code, and then click **OK**.



Account Security

- Change Password: Click **Change**. Enter the old password and new password (1-20 characters, including letters, digits, and underscores (_), and must include letters), and then click **OK**. Please keep the new password properly.



- Cancel Account: Click **Cancel Account** and confirm the operation.

  Note: Once cancelled, your account and all related data will be permanently deleted. Please proceed with caution.

- Two-Factor Authentication: When enabled, the system will assess the risk associated with your login, and will send a verification code to the email associated with your account if necessary. You need to enter the verification code in order to log in.

  Click **On** and confirm the operation.

Privacy Center

View the privacy policy. You can also access it by clicking ⓘ in the upper-right corner and selecting **Privacy Policy**.

4 Team Mode

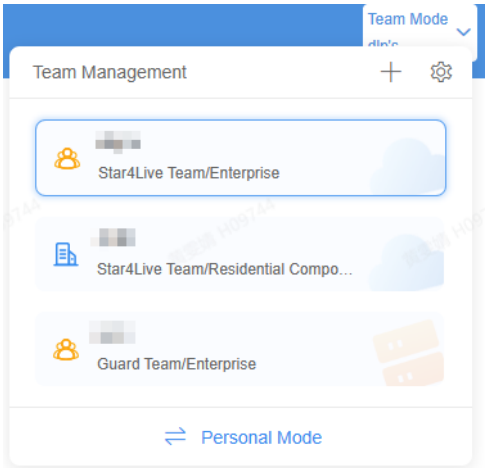
The platform allows you to manage users and devices in teams. A team contains devices and users.

A user can belong to multiple teams, including a default team, teams they have created, and teams they have been invited to join.

Once you switched your identity as an end user, click **Team Mode** at the top of the page to enter team mode.

Hover your mouse over ˅ (as shown in the figure below) to display all the teams you're a member of. Click on a team name to switch to the team. Then, the relevant applications will display.

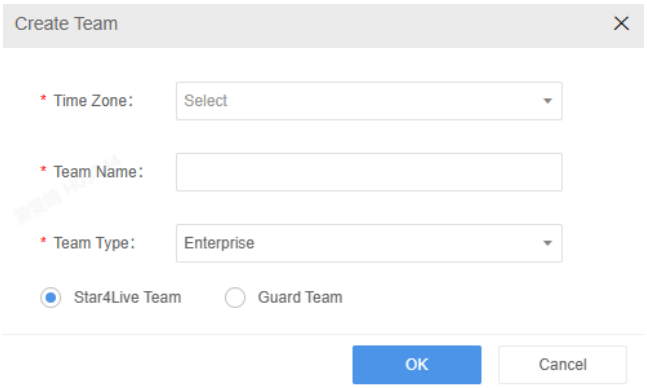
Note: The available applications may vary based on the team type and your account permissions. Please refer to the actual page.



Create Team

An account can create up to 4 teams (excluding the default team). The total number of teams (default, created, invited) cannot exceed 10.

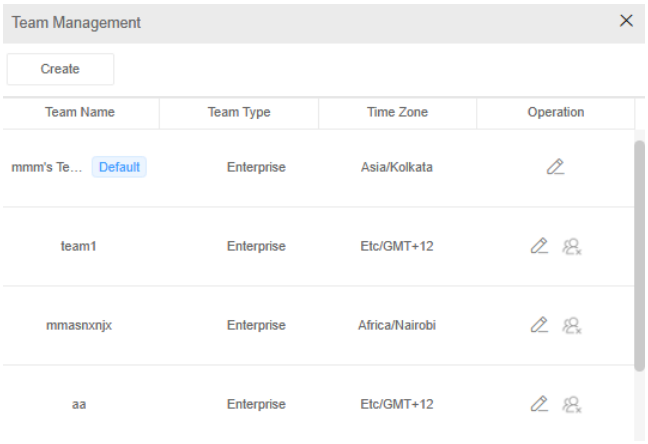
1. Hover your mouse over ᵛ, and click ＋ or click ⚙ > **Create**.



2. Set the team time zone, team name, and team type.
3. Select the team affiliation.
   - Star4Live Team: Deployed on Star4Live. All services are executed exclusively on the cloud, with no interactions with other products.
   - Guard Team: Built on Star4Live team. In addition, Guard teams can be bound to Guard to realize cloud-edge data sync, ensuring data consistency.
4. Click **OK**.

Configure Team

Hover the mouse over ᵛ, and click ⚙.



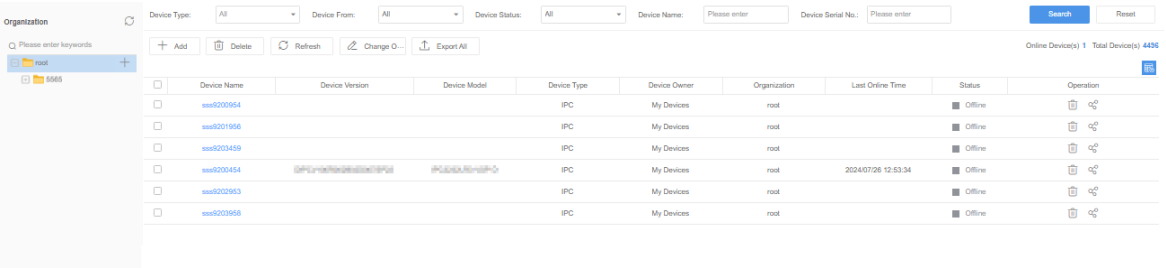
- Leave team: Leave the teams that you have been invited to join. Click ⎋ in the **Operation** column and confirm the operation.
- Edit team: Modify the name of teams you have created. Click ✎ in the **Operation** column and enter the new team name in the pop-up window.
- Remove team: Remove the teams that you have created. Click 👤✕ in the **Operation** column and confirm the operation.

4.1 Device Management

A team can be divided into multiple organizations. Devices can be assigned to either the root organization (default) or other customized organizations, allowing for efficient management and maintenance.

4.1.1 Device Management

Go to **Device Management** > **Device Management**.



Devices are grouped by organization.

4.1.1.1 Organization Management

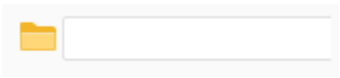
The left-side of the **Device Management** page displays an organization list. There is a default organization (root).

Search

Enter keywords in the top search bar on the left-side list to search.

Add

Up to 10 levels of organizations (including root) are allowed.

1. Click + for an organization, a new organization folder  is displayed below.
2. Set the organization name. Click on the blank area or press the Enter key to save.

   Note: Once saved, the parent organization cannot be changed. Please proceed with caution.

Delete

Click for an organization and confirm the deletion.

Edit

Click for an organization to edit its name.

4.1.1.2 Device Management

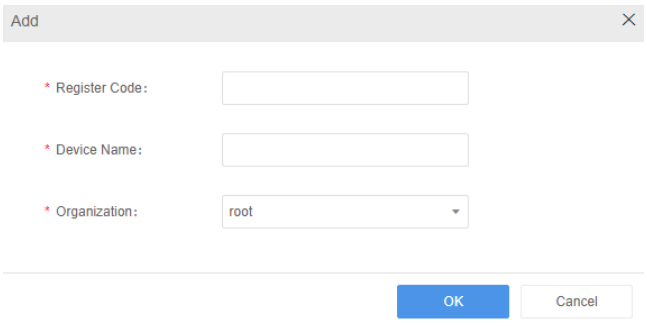
Select an organization from the left-side list to display all devices under it.

Search

Set search criteria including device type, device source, device status, device name, and device serial number to search.

Add

1. Click **Add**.



2. Enter the device’s register code and device name, then select an organization for it.

   Note: Once saved, the register code cannot be changed.

3. Click **OK**.

Delete

Click in the **Operation** column or select device(s) and click **Delete**, and confirm the deletion.

Change Organization

1. Select device(s) and click **Change Organization**.
2. Select a desitination organization and click **OK**. The selected device(s) will be moved to the specified organization.

Export All

Click **Export All** to export all device information within the organization.

Redirect to Device's Web Interface

Only **online** devices' Web interface can be acceesed.

Click in the **Operation** column to redirect to the device's login page.

Share

If the current team is created by the current user, the user can perform batch sharing and click the corresponding to share devices with other cloud accounts.

Note: When performing batch sharing and selecting "Role Permissions" as the permission type, only the "admin" role permissions can be shared.

Retrieve Password

Click in the **Operation** column. Generate a security code using the bound email address and use it as a temporary password to log in to the device's Web interface. After login, you can reset the password.

Restart

Only **online** devices support restart.

Click in the **Operation** column and confirm the operation. The device restarts.

Upgrade

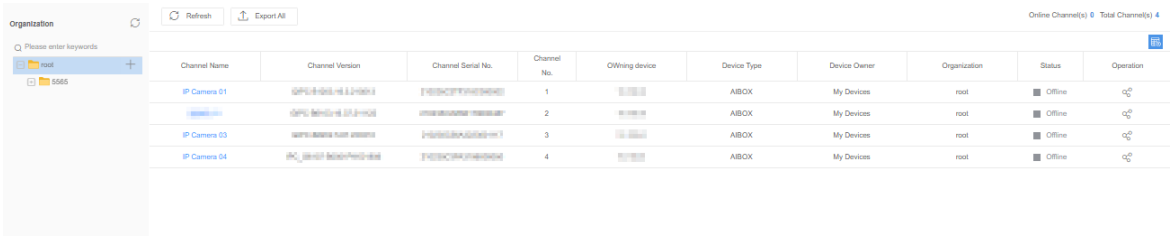
Only **Online** devices support cloud upgrades.

Click in the **Operation** column. The system will automatically detect the current software version. If the version is not the latest, you can click **Start Upgrade** to upgrade the device. During the upgrade process, do not perform any operations on the device.

4.1.2 Channel Management

Channel is the minimum unit for management. Select an organization from the left-side list to display all channels under it.

Go to **Device Management** > **Device Management** > **Channel Management**.



Export All

Click **Export All** to export all channel information within the organization.

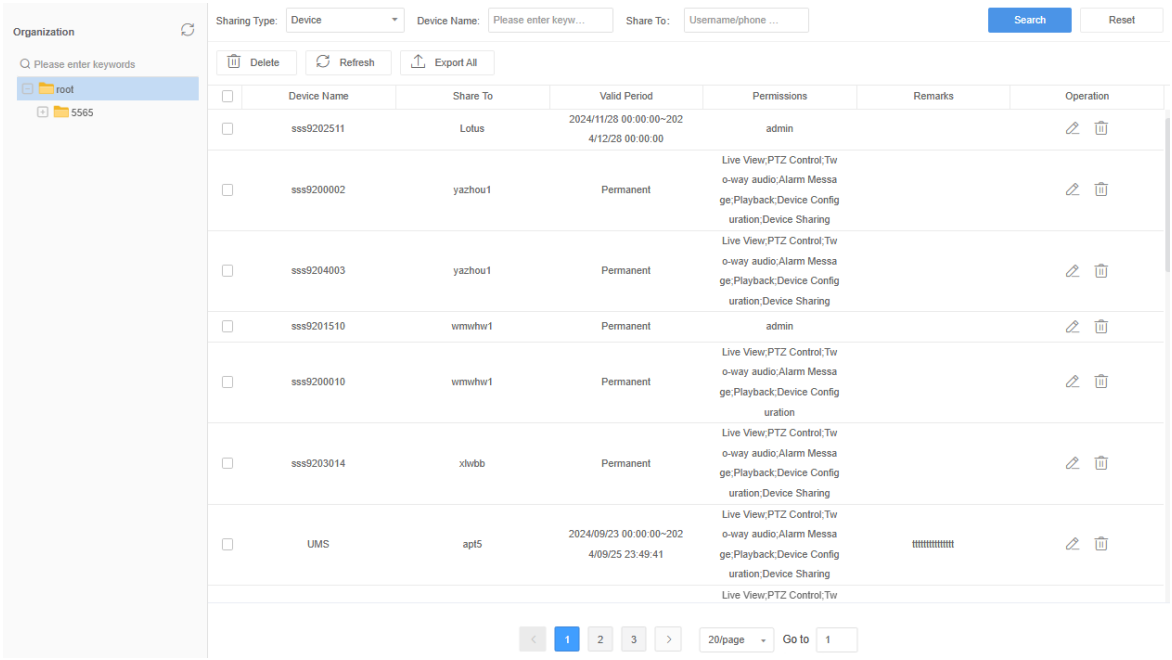
Share

If the current team is created by the current user, the user can perform batch sharing and click the corresponding to share channels with other cloud accounts.

4.1.3 My Sharing

View device sharing records.

Go to **Device Management** > **My Sharing**. Select an organization from the left-side list to display all devices under it.



Search

Set search criteria including sharing type, device name, and sharing target to search.

Edit

Click in the **Operation** column to modify details including the sharing validity period, remarks, and permissions.

Delete

Click in the **Operation** column or select item(s) and click **Delete**, and confirm the deletion.

Export All

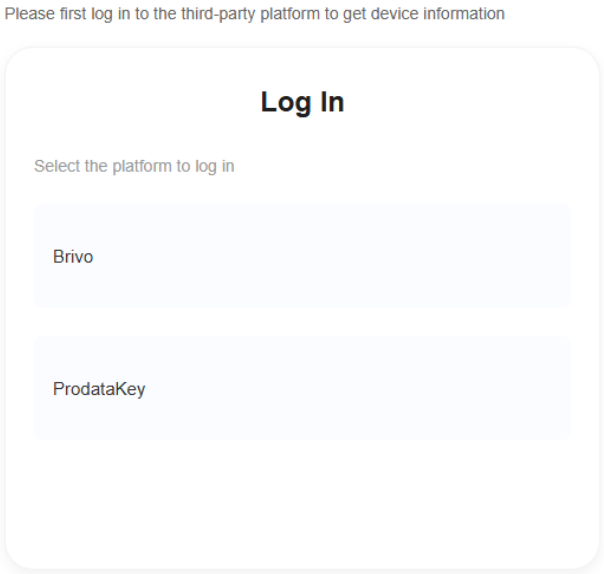
Click **Export All** to export all sharing records.

4.1.4 Third-Party Device

You can add devices from third-party platforms to this platform for management.

First-time Use

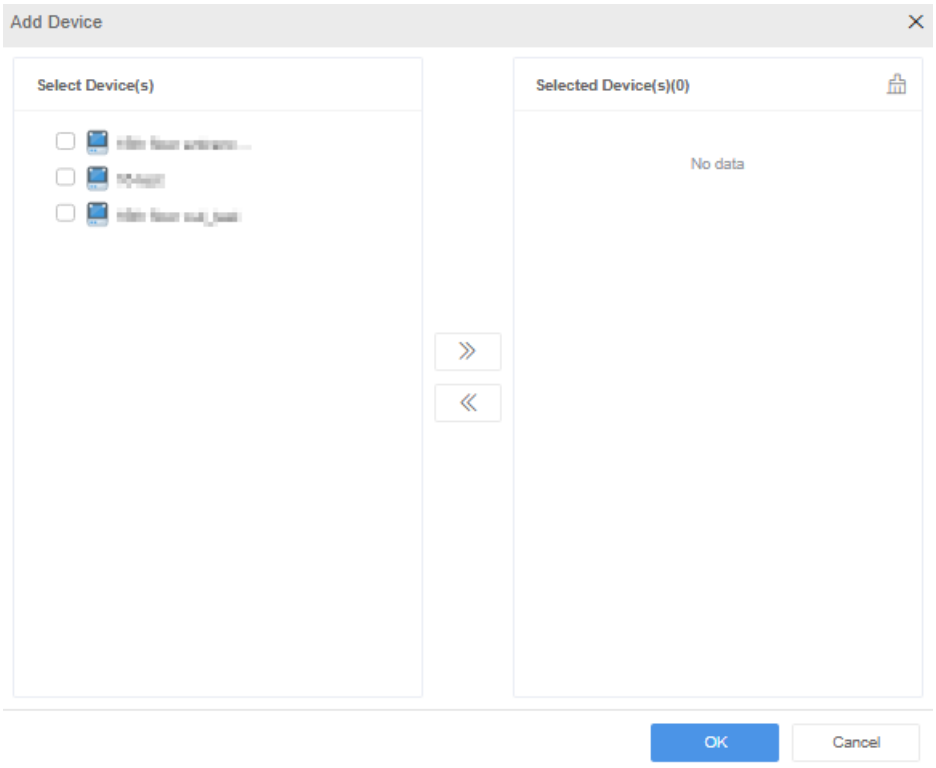
1. Go to **Device Management > Third-party Device**.



2. Select the platform to use and log in.
   - Brivo: Log in using your platform account and password.
   - ProdataKey: Log in using your system ID.

Note: If you are unable to enter the account after the redirection, please clear your browser cache and refresh the page to try again.

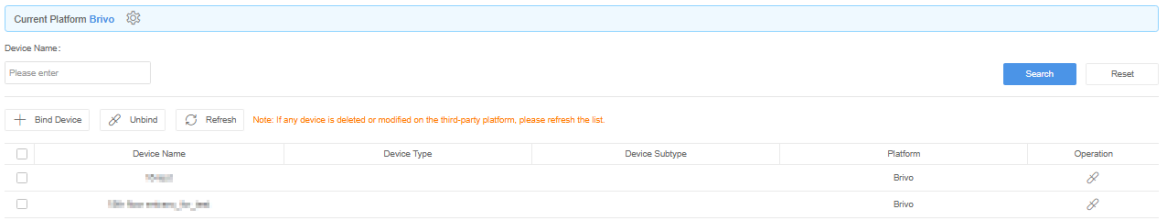
3. After successful login, go back to the **Third-party Device** page. A pop-up window prompts you to select devices for binding



4. From the list on the left, select the devices to be added to the cloud platform, click » , and then click **OK**.

The device is added as shown below. Click **Bind Device** to continue adding devices. You can also Unbind Device as needed.

Note: When continuing to add devices, if you have logged in to multiple platforms simultaneously, you must first select a platform as prompted on the screen, and then bind devices from that platform to Star4Live.



Unbind Device

Click the corresponding 🔗 and then confirm; or select multiple devices, click **Unbind**, and then confirm.

Refresh

After a device is deleted or modified on the third-party platform, you need to click **Refresh** to update the list.

Platform Login/Logout

You can log in to multiple platforms simultaneously. The upper left corner of the page shows information of currently logged-in platforms.

- Login: Click ⚙. Unlogged platforms display "Log In" on the right. Click this button and enter your platform account information to log in.
- Logout: After logging out, all devices bound to that platform will be deleted, and alarm messages from that platform will no longer be received.

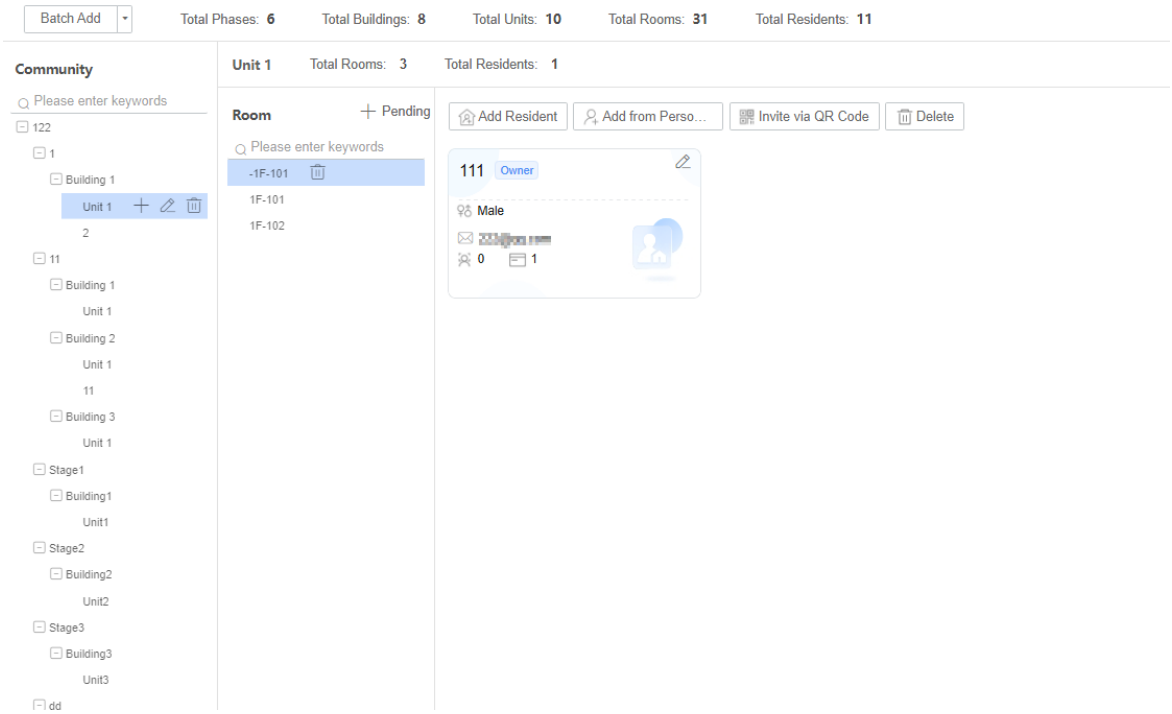
  Click ⚙. The logged-in platforms display "Logout" on the right. Click this button and confirm again to proceed.

4.2 Room Management

4.2.1 Room Management

This function is available only when the team type is **Residential Compound**.

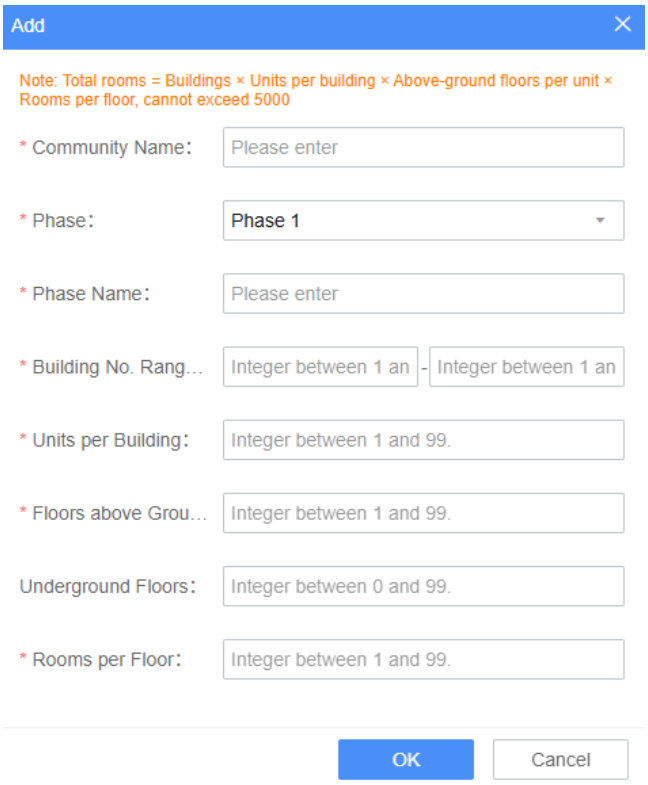
Go to **Room Management** > **Room Management**.



Hierarchy (from highest to lowest): Community (only one) - Phase - Building - Unit - Room.

Configure Room Info

For the first-time use, please click **+** on the upper-left corner or **Add Now** to add a community first.



Add: To add a phase/building/unit/room, hover the mouse over a community/phase/building/unit, and click +.

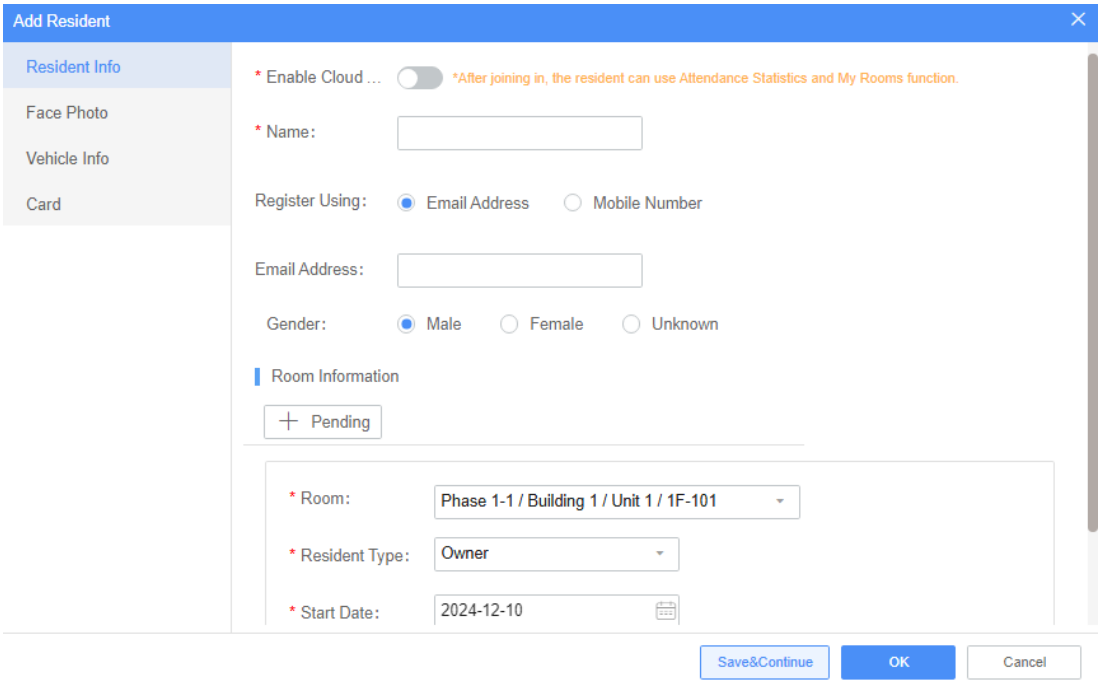
Edit: Hover the mouse over a community/phase/building/unit name and click .

Delete: Hover the mouse over a community/phase/building/unit/room name, click , and confirm the deletion.

Add Resident

Add resident info for each room.

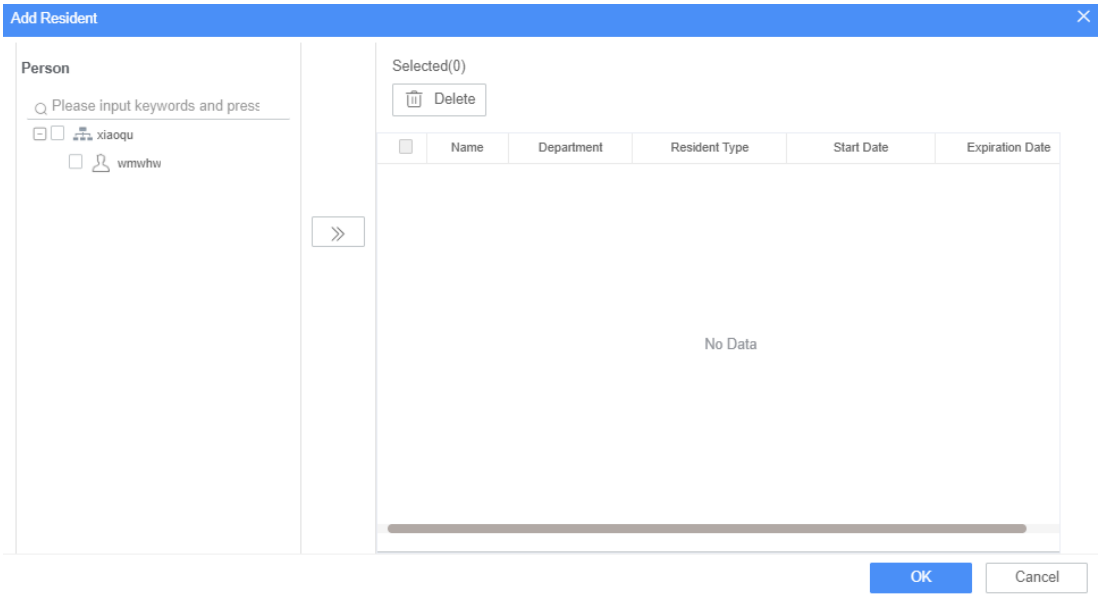
- Add Manually
  1. Click **Add Resident**.



  2. Configure the resident information, face photo, vehicle information, and card information.
  3. Click **Save**. The resident is added. If the resident has an active cloud account, the resident will be automatically assigned a "Resident" role by the system. However, if the resident already has 10 roles, the adding will fail. Please remove some roles and try again.

     To add more, click **Save&Continue**.

- Add from Personnel
  1. Select a room from the left-side list and click **Add from Personnel**.



  2. In the pop-up window, select person(s) from the left-side list, and click **>>** to add them to the selected list. One person can only be matched with one room.
  3. Click **OK**.

- Invite via QR Code: Invite persons to scan the QR code to submit their information. Once approved, they can be added as resident via Add from Personnel.

- Batch Add
  1. Select **Import** > **Export Template**.
  2. Complete the resident information in the template and save it.
  3. Click the drop-down arrow next to **Batch Add** and select **Import Residents**. Upload the modified template file from local and click **OK**.
  4. (Optional) Click the drop-down arrow next to **Batch Add** and select **Import Image**. Package all resident images (must be the requirements instructed in the pop-up window) into a ZIP format file (Resident Image.zip). In the pop-up window, upload the packaged file and click **OK**.

Edit Resident Info

Click on the card's upper-right corner to modify the resident information.

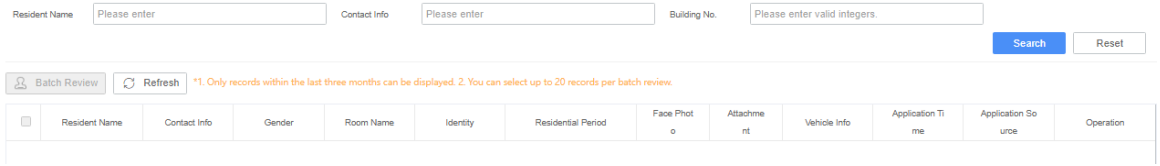
Delete

Select resident(s), click **Delete**, and confirm the deletion.

4.2.2 Resident Review

Review applications submitted by residents within the last 3 months.

Go to **Room Management** > **Resident Review**.



Review

1. Review the application contents.
   - Residential Period: If you want to change the resident's residential period, click in the **Residential Period** column, edit the period, and then click **OK**.
   - Face Photo/Attachment: If a photo/attachment is included in the application, the corresponding column (**Face Photo/Attachment**) will display the specific count; otherwise, **-** will be displayed. You can click to view the uploaded information.
   - Vehicle Info: Click in the Vehicle Info column to view details.
2. In the Operation column, click to approve the resident application, or click to decline (reason required).

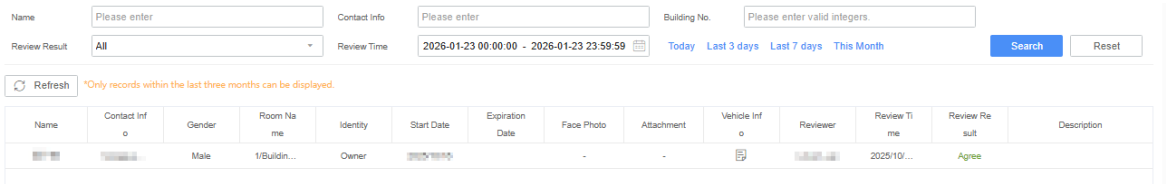
   Note: You can batch approve/decline applications. Up to 20 applications can be approved/declined at a time.

   Review records can be viewed in Review Records.

4.2.3 Review Records

Displays all review records within the last three months.

Go to **Room Management** > **Review Records**.



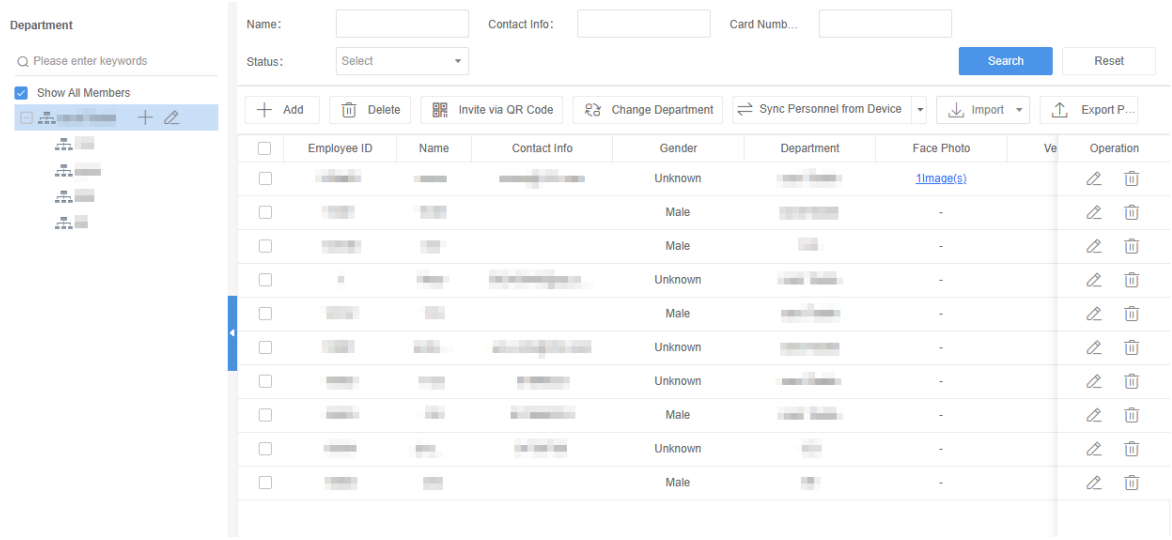
Click on the corresponding face photo link, attachment link, and to view the face photo, uploaded attachment, and vehicle information respectively.

4.3 Personnel Management

4.3.1 Personnel Management

Manage personnel and departments within teams, even for those without a P2P account.

Go to **Personnel Management** > **Personnel Management**.



4.3.1.1 Department Management

A team can have multiple departments, with personnel managed by respective departments.

Select a department from the left-side list, the person list under the department will be displayed on the right. To view the personnel from its sub-departments as well, select **Show All Members**.

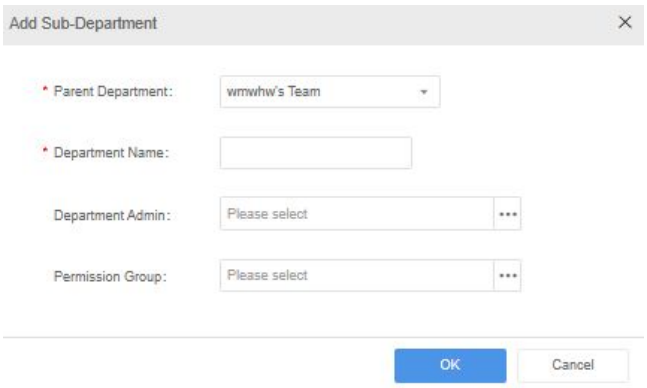
Search

Enter keywords in the top search bar on the left-side list to search.

Add

A team allows for up to 10 levels of departments and up to 3,000 departments.

1. On the left-side list, click ＋ next to the department name.



2. Select a parent department and enter a custom department name.

   Note: The parent department cannot be changed once selected.

3. (Optional) Select up to 5 department admin(s).
4. If you have access control management permissions, the permission group parameter will be displayed. After selecting a permission group, all members added to that department will be granted the corresponding permissions.

5. Click **OK**.

Delete

Departments that still contain personnel or sub-departments cannot be deleted.

On the left-side list, click next to the department name, and confirm the deletion.

Edit

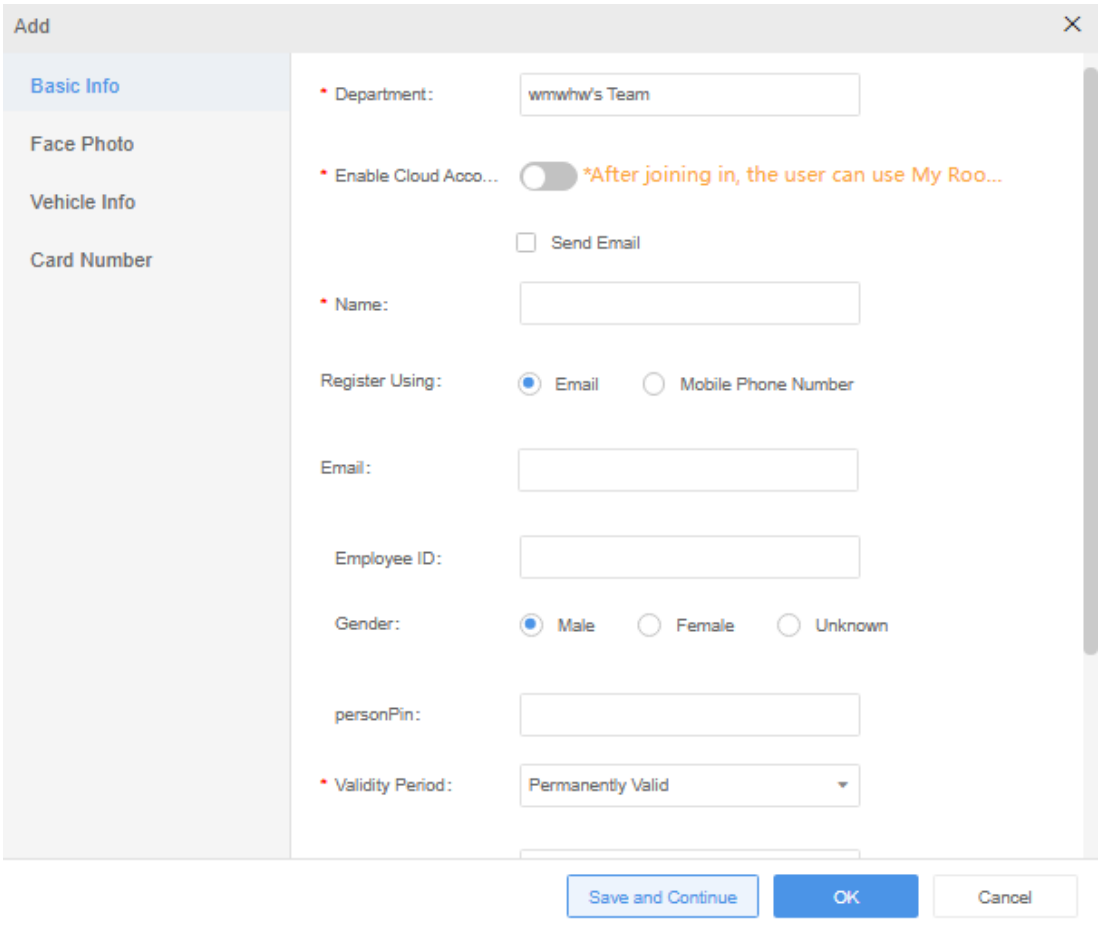
On the left-side list, click next to the department name to edit the department parameters except **Parent Department**.

4.3.1.2 Personnel Management

Add

A team allows for up to 100,000 persons.

- Add one by one
  1. Click **Add**.



  2. Set the person's basic information, face photo, vehicle information, and card information as needed.
     - Basic Info: * indicates required fields. You must complete the required fields before configuring face photo, vehicle info, and card info.
     - Vehicle Info: Up to 6 vehicles are allowed. No validity period means permanently valid.
     - Card: Before enrolling card number, please check card enrollment parameters first.

       Note: If you want to read a common card locally, only the card readers in the list are supported.
  3. Click **OK**. The person is added. To add more, click **Save and Continue**.
- Sync personnel from device: See Sync Personnel from Device.

- Add in batches

  Note: Personnel imported in each batch must belong to the same department. If personnel need to be imported into multiple departments, please perform separate imports for each department.

  1. Select **Import** > **Download Template** to download the template.
  2. Fill in the template with person information as instructed, and then save.
  3. Select **Import > Import Personnel**, select the completed template, select the target department for the import, and click **OK**.
  4. (Optional) Import person images: 1. Name the images as **Person ID.jpg** in local. Each size: 10KB to 512KB. Max. resolution: 1080*1920px. 2. Pack all images into a **Person Image.zip** file. 3. Click **Import** > **Import Image**, upload the zip file from local, and then click **OK**.

Delete

Deleting a person will also remove their access control permissions and attendance information. Please proceed with caution.

Click in the **Operation** column or select item(s) and click **Delete**, and confirm the deletion.

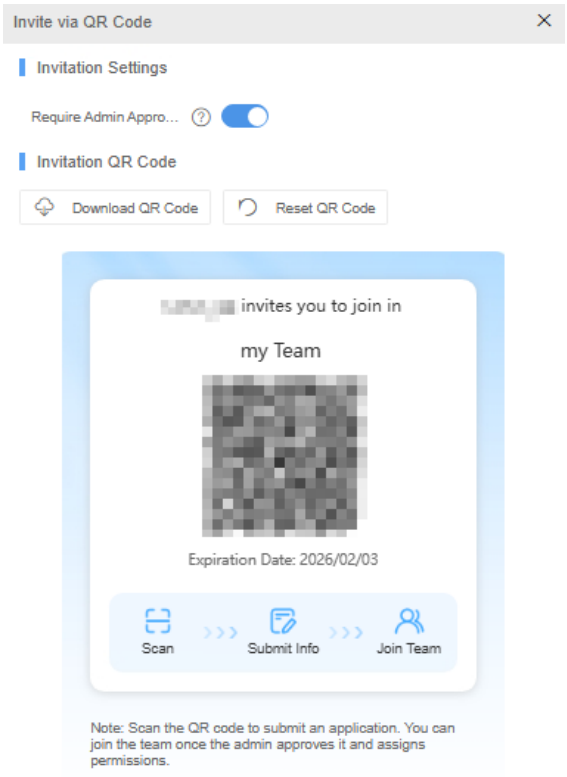
Edit

Click in the **Operation** column to edit the person information.

Invite via QR Code

Click **Invite via QR Code** and complete the invitation settings. Once configured, the invited persons can apply to join the team by scanning the QR code and submitting their information before the expiration time.

Require Admin Approval for Applications: Enabled by default. When enabled, all applications must be reviewed and approved by the admin before the applicants can join the team. When disabled, new applicants can join the team directly after submitting their information.



Change Department

1. Select person(s) and click **Change Department**.
2. Select the destination department.

3. Click **OK**.

Sync Personnel from Device

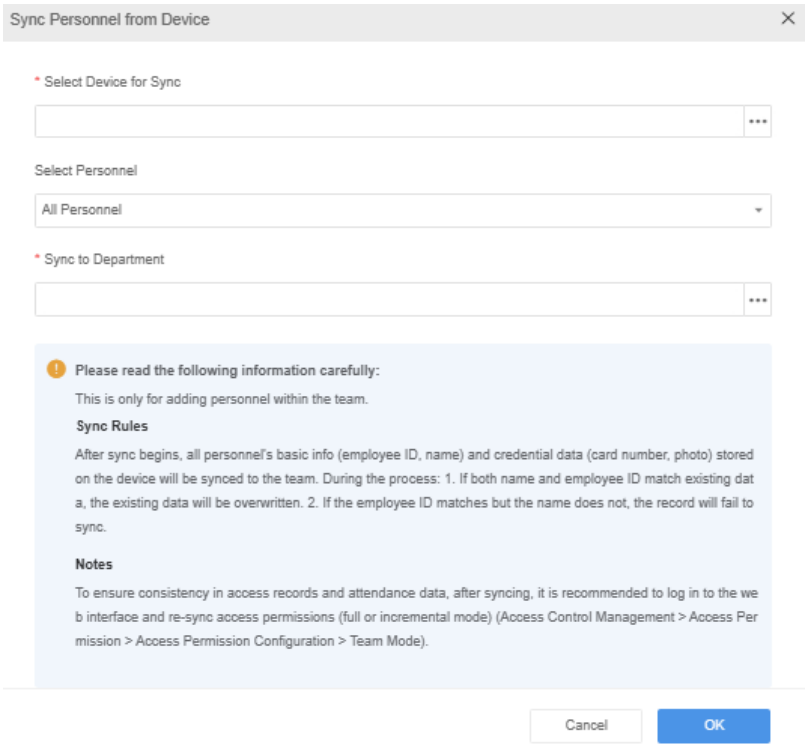
Collect personnel information (including names, facial images, etc.) through enrollment devices such as access control devices, then sync the collected information to the cloud (Web/App) to address the challenge of manual data entry in the cloud, achieving unified management of personnel data across platforms.

Sync rules: After the sync begins, the basic information (employee ID, name) and credential information (card number, photo) of all personnel on the device will be synced to the team. During the data entry process: 1. If the name and employee ID match existing data, the existing data will be overwritten; 2. If the employee ID matches but the name does not match, the data will fail to sync.

Note: To ensure consistency between access records and attendance data, it is recommended to enter the team mode on the Web interface after sync is completed, go to **Access Control Management > Access Permission > Pass Permission Configuration** and resync access permissions for the personnel (in full sync mode or incremental sync mode).

Prerequisites: The information input has been completed on the enrollment device, and the department for receiving the data has been created in the cloud.

1. Select **Sync Personnel from Device > Sync Personnel from Device**, read and clearly understand the sync rules and precautions, and then click **OK**.
2. Select the device for sync, the range of personnel, and the department to which the data will be synced.



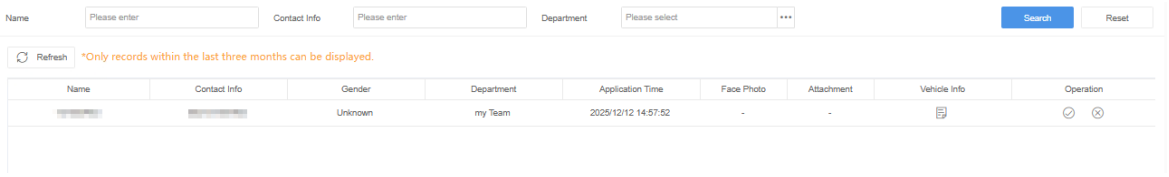
3. Click **OK**. You can view the sync results at **Sync Personnel from Device > Sync Records**.

Note: Sync records only show data of the last 7 days.

4.3.2 Personnel Review

An administrator can review requests to join the team that were initiated via QR code scanning within the departments in the past three months.

Go to **Personnel Management** > **Personnel Review**.



View Face Photo/Attachment

If a photo/attachment is included in the application, the corresponding column (**Face Photo/Attachment**) will display the specific count; otherwise, **-** will be displayed. You can click to view the uploaded information.

View Vehicle Info

Click in the **Vehicle Info** column to display the license plate number and its validity period.

Review

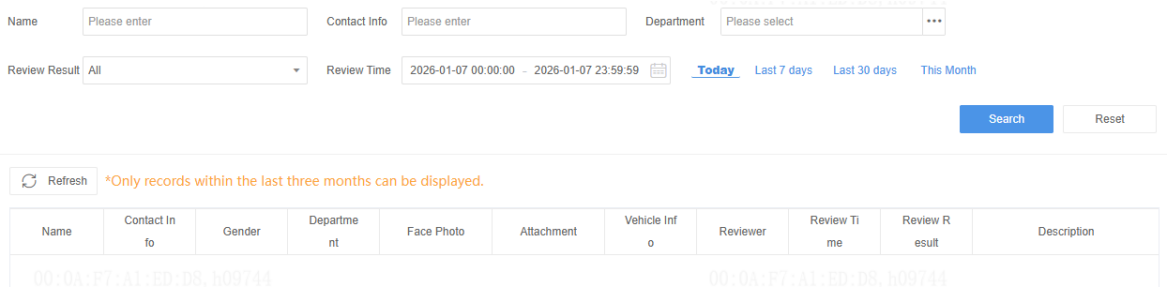
Click to approve the application, and then assign role(s) and specify a department.

Click in the **Operation** column to decline the application. You need to provide a reason for the rejection.

4.3.3 Review Records

Displays review records within the last 3 months.

Go to **Personnel Management** > **Review Records**.



View Face Photo/Attachment

If a photo/attachment is included in the application, the corresponding column (**Face Photo/Attachment**) will display the specific count; otherwise, **-** will be displayed. You can click to view the uploaded information.

View Vehicle Info

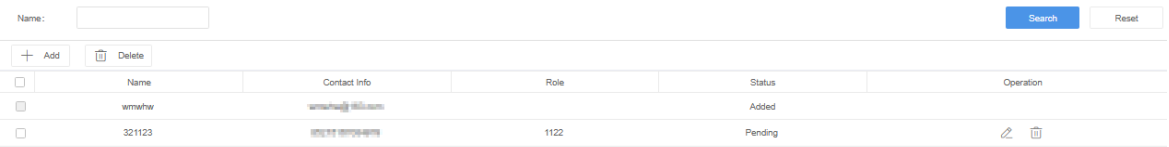
Click in the **Vehicle Info** column to display the license plate number and its validity period.

4.4 Team Management

4.4.1 User Management

Manage user information (P2P account required) within teams.

Go to **Team Management** > **User Management**.



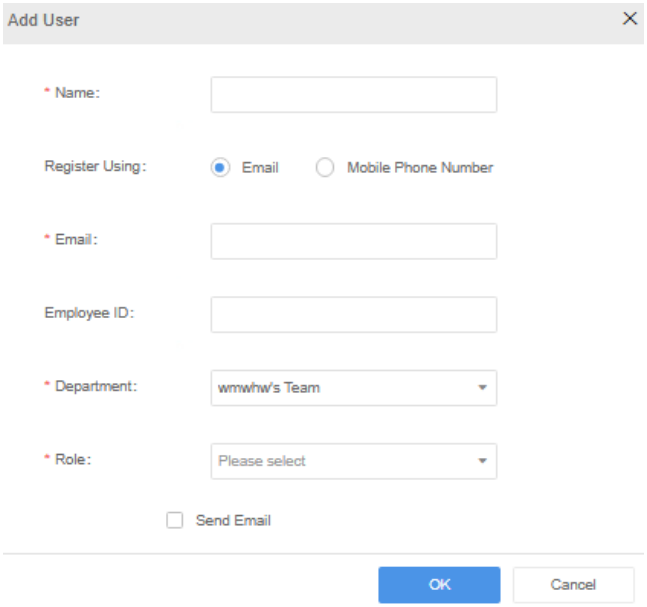
- Added: The user has successfully joined the team.
- Pending: An invitation to join the team has been sent to the user and is awaiting confirmation.

Search

Enter a person's name in the top search bar, and click **Search**.

Add

1. Click **Add**.



2. Complete the settings, including employee ID, name, registration method, email address/mobile phone number, department (source: Personnel Management), and role (optional; source: Role Management).
3. (Optional) If **Send Email** is selected, an email will be sent to notify the user.
4. Click **OK**. The user's status will be **Pending**. Once the user logs in using the provided email address and accepts the team invitation in the app, their status will change to **Added**.

Delete

The super admin account cannot be deleted.

Click in the **Operation** column or select user(s) and click **Delete**, and confirm the deletion.

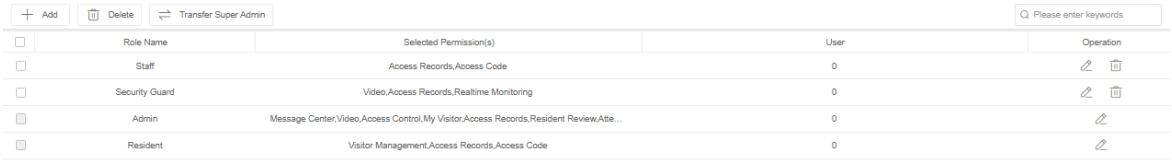
Edit

Click to modify the role information.

4.4.2 Role Management

Different roles have varying permissions. When a user is assigned to a specific role, they are granted all permissions associated with that role.

Go to **Team Management** > **Role Management**.



Once teams are created in Create Team, some default roles are automatically generated based on the team type.

- Non-deletable Roles:
  - Admin: The team manager, with permissions second only to the team creator. The role name and permissions cannot be edited, but you can assign users to the role.
  - Resident: Allows for room management. Applicable only to teams of the Community type. The role name cannot be edited, and the role is automatically assigned upon a creation of resident. Manual assignment is not allowed.
- Deletable Roles: Team admin can edit the name and permissions for these roles.
  - Staff: For permanent staff members. In typical, admin can assign access-related permissions to the role.
  - Security Guard: For persons responsible for monitoring and maintaining security. Admin can edit the permissions for the role.

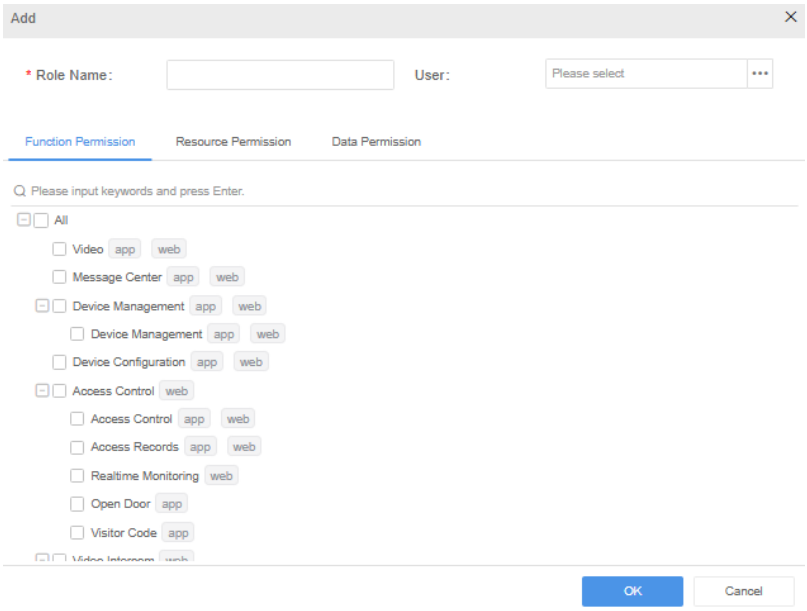
Search

Enter a role name in the search bar in the upper-right corner to search.

Add

Up to 1,000 roles can be added per user.

1. Click **Add**.



2. Enter a custom role name.
3. (Optional) Select role member(s) (source: User Management). The selected users will be granted all permissions of this role.
4. Select function permission(s) and resource permission(s) to specify which functions members will have access to.
5. Configure data permissions. This is used to define the scope of service data management and takes effect in personnel and department management.

   This applies only to Star4Live teams.

   - Only Me: Can only view your own data.
   - All Departments: Can view data from all departments. Department management is also supported.
   - Current Department & Sub Departments: Can view data from your own department and all sub-departments under it. Department management is also supported.
   - Specified Departments: Can view data from specified departments. Department management is also supported.
6. Click **OK**.

Delete

Click in the **Operation** column or select role(s) and click **Delete**, and confirm the deletion.

Edit

Click in the **Operation** column to modify the role information.

Transfer Super Admin

The default super admin is the user who created the team and holds the highest level of permissions.

1. Click **Transfer Super Admin**. In the pop-up window, click **Send Code** to send a verification code to the email address/mobile phone number of the current super admin. Enter the received the verification code to verify.

2. After successful verification, select the user to whom you wish to transfer the super admin to and confirm in the pop-up window.

4.4.3 Team Settings

Configure the basic parameters for the team. Once completed, click **Save**.

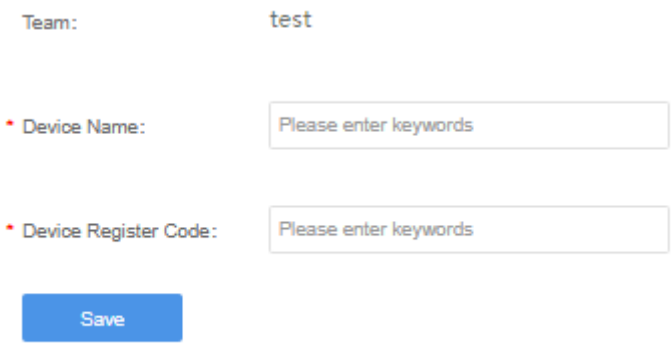
Go to **Team Management** > **Team Settings**.

Notification

Choose whether to push notifications to the app for convenient alerts on your mobile client.

Edge Service Configuration

For Guard teams, you can bind them to Guard to realize edge-cloud data sync, ensuring data consistency.

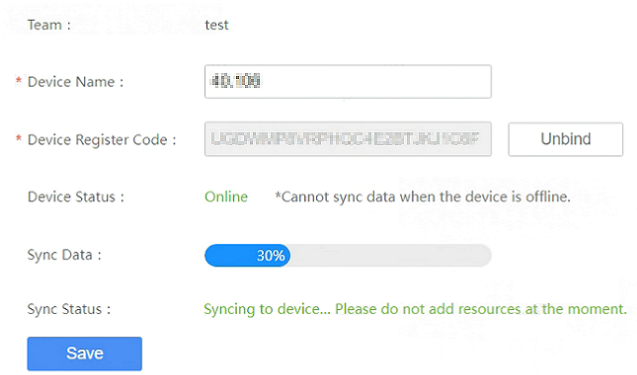


- Bind:
  1. Enter the name and register code of Guard. Click **Save**.
  2. When added for the first time, you need to sync the data manually. Click **Go to Sync** in the pop-up window. For the subsequent operations, please refer to **Data Sync**.
- Unbind: Click **Unbind** and confirm.
- Data Sync: Data sync is supported only when Guard is **online**.
  1. Click **Sync Data**.
  2. Select a sync method.
     - Sync data:
       - The existing rooms, visitors, personnel, rooms linked with video intercom devices, and holiday information on Guard will be cleared.
       - The exiting permission groups and schedule templates on Guard and Star4Live will be cleared and need to be reconfigured on Star4Live.
       - Rooms, visitors, personnel, and holiday information configured on Star4Live will be synced to Guard.
       - Users can only add, delete, and edit devices, organizations, channels, and rooms linked with video intercom devices on Guard; data will be automatically synced to Star4Live.
       - Users can only add, delete, and edit rooms, personnel, visitors, permission groups, schedule templates, and holidays on Star4Live; data will be automatically synced to Guard.
     - Get data:
       - The existing team members on Star4Live will be cleared and need to be re-invited to join the team on Star4Live.
       - Data such as devices, organizations, channels, rooms, personnel, visitors, permission groups, rooms linked with video intercom devices, schedule templates, and holiday information will be synced from Guard to Star4Live.

- Users can only add, delete, and edit devices, organizations, channels, and rooms linked with video intercom devices on Guard; data will be automatically synced to Star4Live.
- Users can only add, delete, and edit rooms, personnel, visitors, permission groups, schedule templates, and holidays on Star4Live; data will be automatically synced to Guard.

3. Click **OK** and confirm. Now, you can check the data sync progress and status.

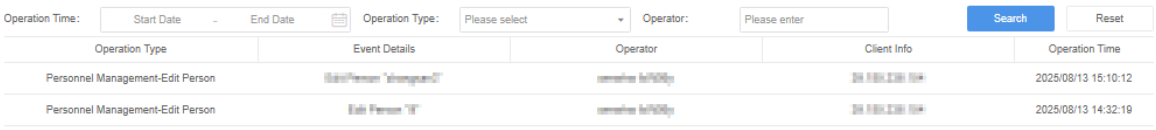
Note: Do not perform any addition operations during data sync.



4.4.4 Operation Logs

You can search operation logs within the team.

Go to **Team Management > Operation Logs**.



You can set search criteria including time range, operation type, and operator name.

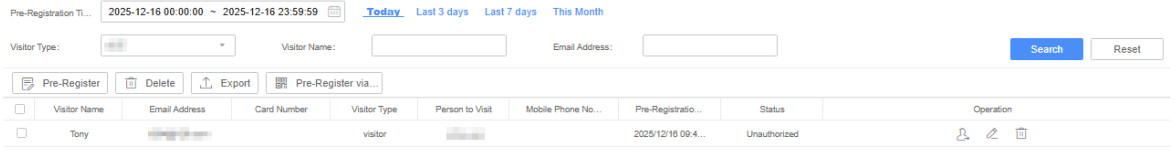
4.5 Visitor Management

You can pre-register visitor information, review visitor details, search visitor records, etc.

4.5.1 Visitor Pre-registration

The list displays all pre-registered visitors who have not yet signed out.

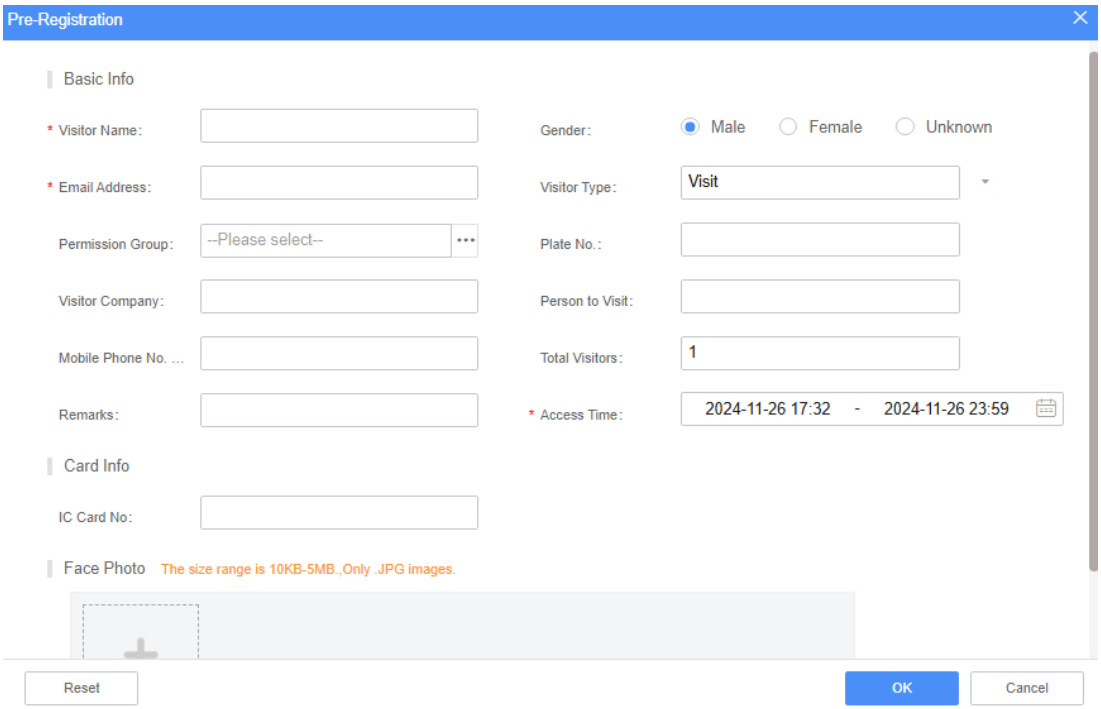
Go to **Visitor Management** > **Visitor Management** > **Pre-Registration**.



Pre-Register

Choose a way to pre-register visitors:

- Register Manually
  1. Click **Pre-Register**.

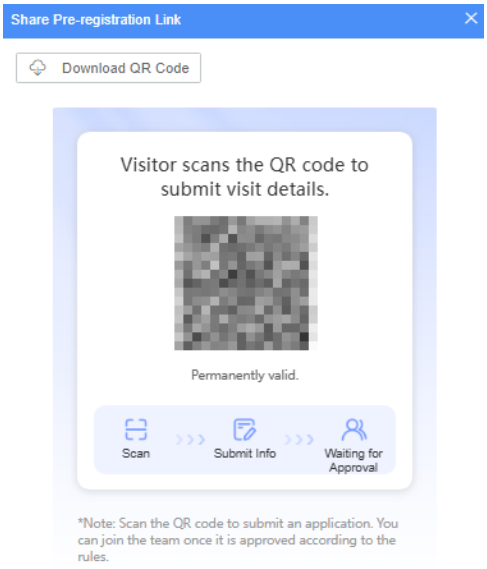


2. Fill in the visitor information. You need to specify a permission group for the visitor. Otherwise, the visitor's status is **Unauthorized**, and access will be denied.

   Note: Once saved, the visitor type cannot be changed.

3. Click **OK**.

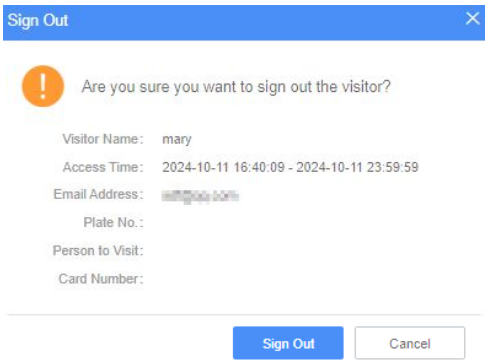
- Invite via QR Code: Click **Pre-Register via QR Code**. Share the QR code with visitors so they can scan it to submit their information.



Sign Out

When a visitor is signed out, his/her access permission will be revoked.

Click in the **Operation** column, click **Sign Out**, and confirm the operation.



Edit

Click in the **Operation** column to modify the information, excluding the visitor type.

Delete

Click in the **Operation** column or select item(s) and click **Delete**, and confirm the deletion.

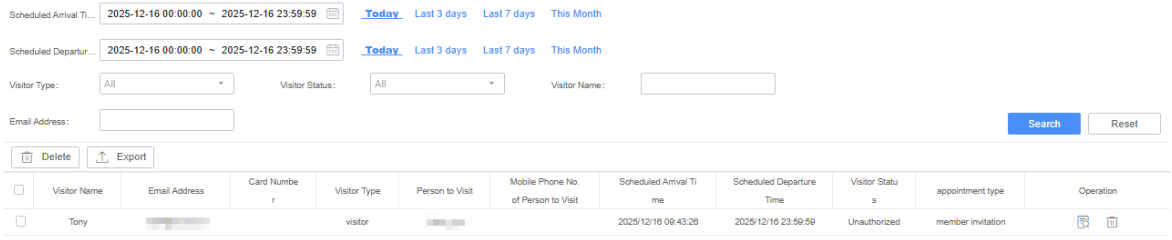
Export

Select item(s) to export, and click **Export**.

4.5.2 Visitor Records

Displays visitor pre-registration and sign-out records.

Go to **Visitor Management** > **Visitor Management** > **Visitor Records**.



Search

Filter based on the criteria listed at the top, and then click **Search**.

View Visitor Details

Click in the **Operation** column to view the visitor information.

Delete

Click in the **Operation** column or select item(s) and click **Delete**, and confirm the deletion.

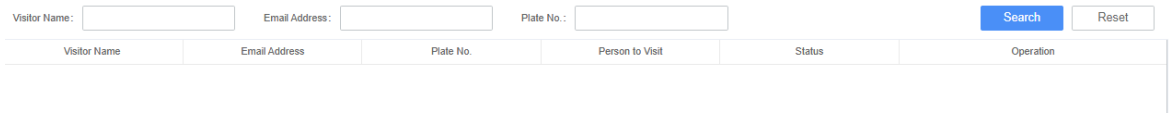
Export

Select item(s) to export, and click **Export**.

4.5.3 Visitor Review

Review applications submitted by visitors via QR code.

Go to **Visitor Management** > **Visitor Management** > **Pre-registration Review**.



- Normal: The applied visit end time is after the current time.
- Expired: The applied visit end time is before the current time.

Review

1. Click .
2. Review the visitor information and choose **Approve** or **Reject**.
   - Approve: Assign a permission group to grant access rights.
   - Reject: Provide a reason for the declining the application.
3. Click **OK**.

View Expired Visitor Applications

If the applied visit end time is before the current time, the application will be **Expired**.

Click to view the details of the expired application.

Delete

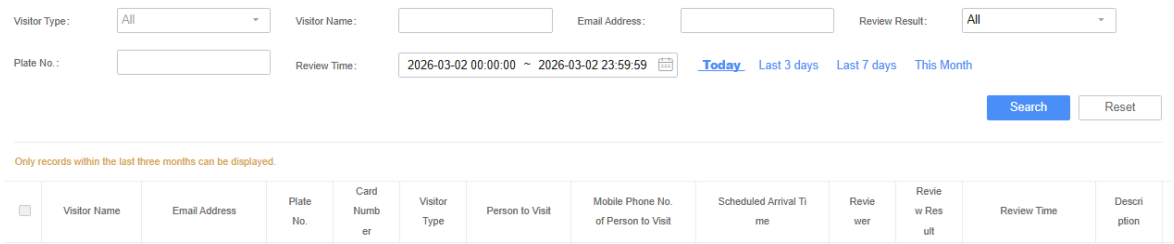
Only **Expired** applications can be deleted.

Click in the **Operation** column and confirm the deletion.

4.5.4 Review Records

After a visitor scans the QR code and submits an application, you can view the approval records here.

Go to **Visitor Management > Review Records**.

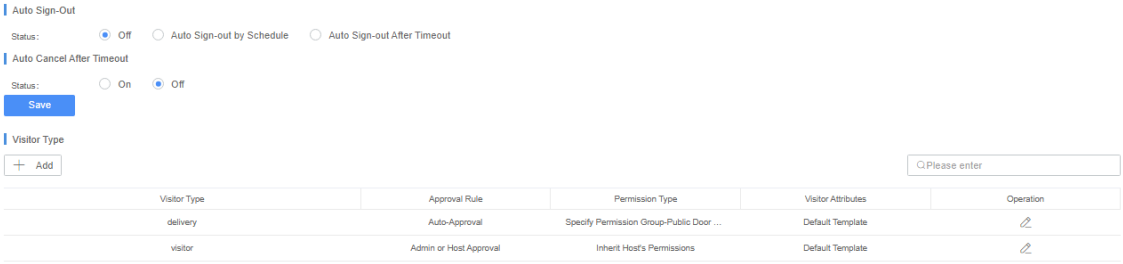


4.5.5 Visitor Setting

4.5.5.1 Visitor Access

Auto Sign-Out by Schedule, Auto Sign-out After Timeout

1. Go to **Visitor Management > Visitor Settings > Visitor Access**.



2. Select the auto sign-out status:
   - Off: Visitors will not be signed out automatically.

- Auto Sign-out by Schedule: If a visitor has not signed out by the configured time, the visitor will be automatically signed out. You must specify the auto sign-out time.
- Auto Sign-out After Timeout: If a visitor has not signed out by the end of the configured access period, the visitor will be automatically signed out.

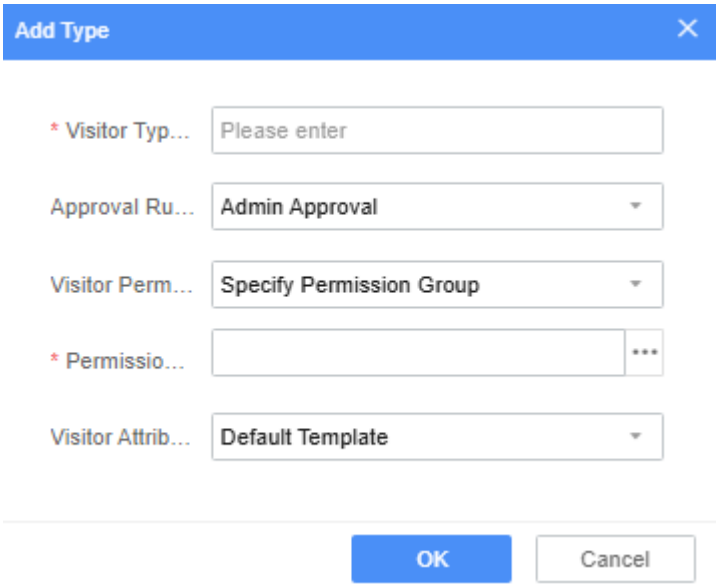
3. Enable or disable **Auto Cancel After Timeout**:
   - Enabled: Set a timeout period. The countdown starts from the scheduled arrival time. If the visitor has not arrived by the end of this period, the appointment will be automatically canceled.

     Note: If the administrator has not yet approved the visit request by the end of the timeout, the appointment will not be canceled. Once approved, the visitor may still access within the configured valid time period.
   - Disabled: The appointment will not be canceled, even if the visitor arrives after the scheduled time.
4. Click **Save**.

Visitor Types

You can configure up to 32 visitor types.

1. Click **Add**.



2. Set the visitor type. Once saved, the visitor type cannot be modified—please review carefully before saving.
3. Select an approval rule:
   - Admin Approval: Admin Approval: Approval is granted if any one of the following roles approves: ① A user with "Visitor Management" permissions; ② The department administrator of the host.
   - Host or Admin Approval: Approval is granted if any one of the following roles approves: ① The host with "My Visitors" permissions; ② A user with "Visitor Management" permissions; ③ The department administrator of the host.
   - Host and Admin Approval: Approval requires sequential confirmation from both: ① The host, AND ② Either the department administrator of the host or a user with "Visitor Management" permissions。

     Note:
     - If the visitor application does not specify a host, or the specified host does not have "My Visitors" permissions, the host approval step is skipped.
     - If the host is a department administrator and has "My Visitors" permissions, only one approval by the host is required.
   - Auto Approval: Visitor appointments are approved automatically without review.

Note: If no department administrator exists, the approval is handled by the administrator of the parent department; if the parent department administrator still does not exist, it continues up to the next level, and so on, until reaching the root department administrator (i.e., the team creator).

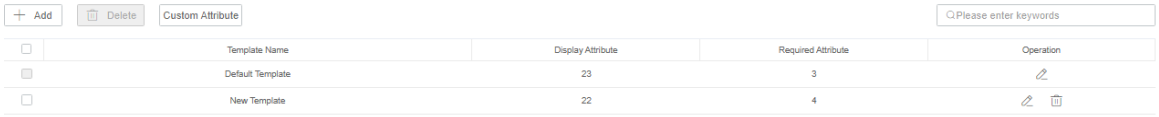
4. Set the permission mode:
   - Inherit Host's Permissions: Permissions follow those of the host.
   - Specify Permission Group: Specify a set of access permissions for this visitor type.
5. Select visitor attributes, which can be configured in Visitor Attributes. When inviting a visitor or when a visitor uses self-service booking, a form will be generated based on these attributes—consistent across both PC and mobile clients.
6. Click **Save**.

4.5.5.2 Visitor Attributes

After configuring visitor attributes, the system will generate a form based on these settings when inviting visitors or during self-service appointment booking. Additionally, you can perform searches in Visitor Pre-registration using these custom visitor attributes.

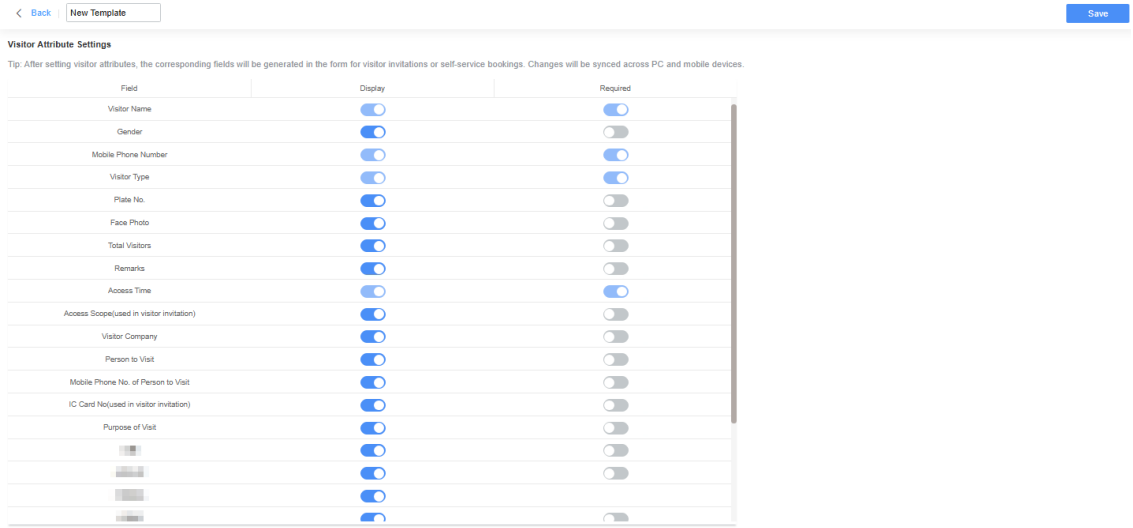
A default template is provided and cannot be deleted.

Go to **Visitor Management > Visitor Settings > Visitor Attributes**.



Add Visitor Attributes

1. Click **Add**.

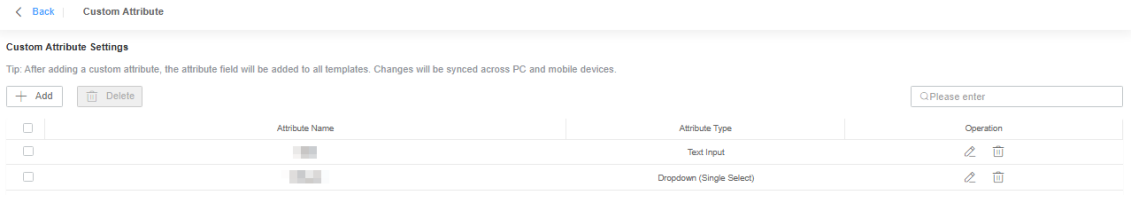


2. Select the fields you want to display. Some fields are mandatory and will always appear.
3. (Optional) For any displayed field, you can specify whether it is required or optional.
4. Click **Save**.

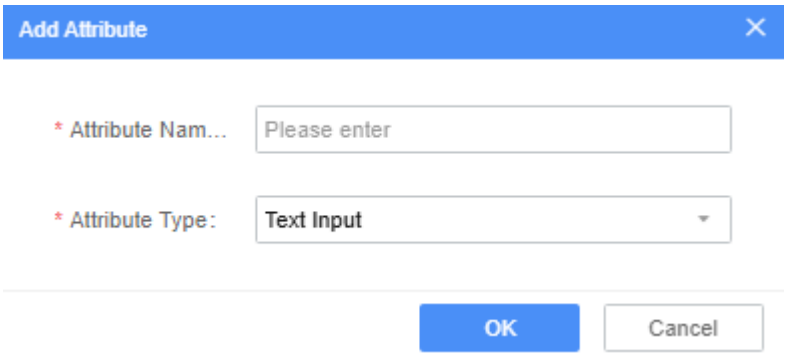
Add Custom Attributes

If the existing attributes in the template do not meet your needs and you require additional data collection, you can add custom attributes.

1. Click **Custom Attribute**.



2. Click **Add**.



3. Enter the attribute name.
4. Select the attribute type.
   - Text Input (default): Displayed as a text box.
   - Dropdown (Single Select): Three options are generated by default. You can add or remove options as needed. No option is selected by default.
   - Dropdown (Multiple Select): Three options are generated by default. You can add or remove options as needed.
5. Click **OK**.

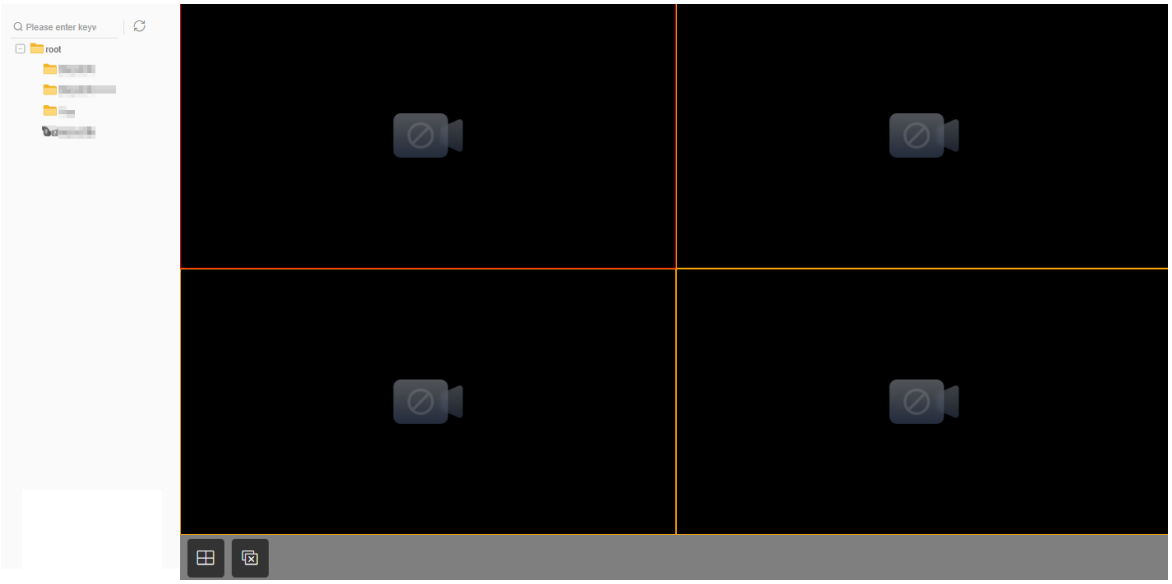
4.6 Video

View live and recorded videos.

Click **Video**. The left-side list shows devices that support video playing in the team (offline devices are shown in grey). On the right side is the live view window.

Note:

- Users need to be assigned **video** permissions.
- Before playing videos, follow on-screen instructions to download and install UPlayer; otherwise live video is not available.



Live View

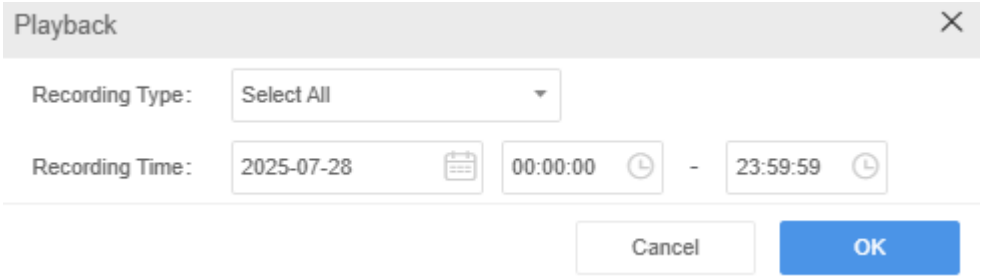
- To play in a specified window
  1. Click the window. If the window border changes to orange, it means the window has been selected.
  2. Double-click an online device in the device list to start playing its live video in the selected window.

- If no window is specified, double-clicking an online device in the device list will play its live video in the first window.

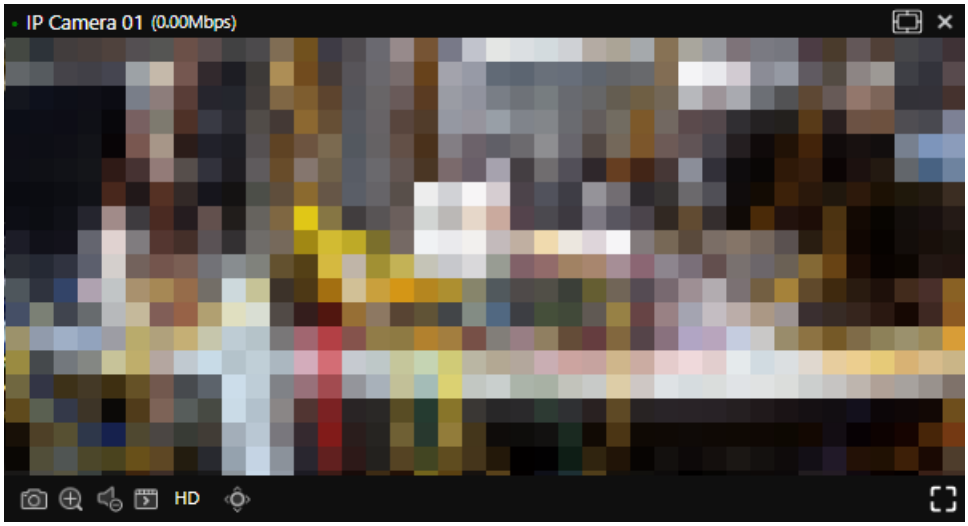
Note: If live video is already playing in the first window, it will be replaced by the current live video.

Playback

1. Click an online device in the device list, and then click the corresponding .
2. Choose the recording type, set the time range, then click **OK**.



Single-Window Operation

Operation	Description
Play in a single window	To play in a single window: Double-click a window to switch to single-window layout and display only the content of that window. Double-click again to restore the original window layout.
Place the cursor on the image	
Switch window layout	• : Switch to full-window display mode. • : Switch to adaptive display mode.
Close window	Click to close the live view window.
Snapshot	Click to take a snapshot of the current image and save the image locally. Name: catch.jpg.
Digital zoom	Click , then drag in the window to select an area (red rectangular). The image in the selected area will be magnified.
Audio adjustment	Click to adjust the sound volume.
Recording	Click to start recording video, then click to stop recording and save the recorded video locally.
Switch clarity	Choose live video clarity (from high to low: HD, SD, LD).

Operation		Description
		Actual options available may vary with devices. See the actual UI for details.
	PTZ control	Only for PTZ cameras. Click to place the cursor on a side of the image, and an arrow will appear. Click to control the movement direction.
	Full screen/ exit	Click to enter full screen, press **Esc** to exit.

Multi-Window Operation

Operation	Description
	Switch the live view layout to 1/9/16 windows as needed. By default, it displays in a 4-window layout.
	Click to close all live videos.
	Select a window with live video playing, then click this icon to start two-way audio.
	Download the recording during playback.

4.7 Message Center

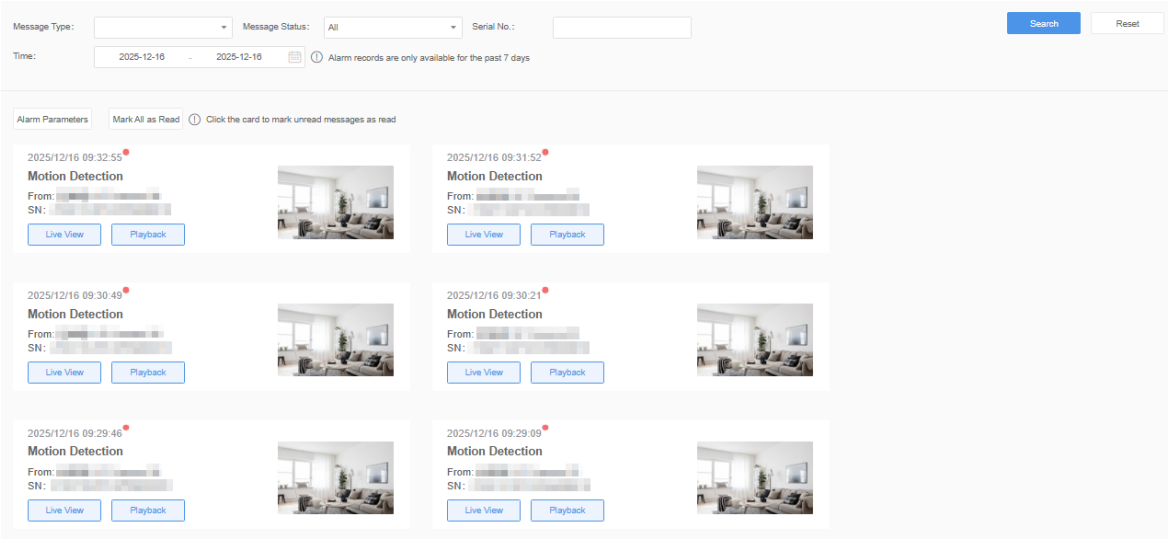
4.7.1 Alarm Messages

Receive real-time notifications of device events and quickly view the live scene to respond promptly to security events.

Note:

- Only users in the **Cloud** team mode who have been assigned the **Message Center** permission can access the screen.
- It is recommended to assign **Video** permissions to users; otherwise, the corresponding functions will not be available.

Go to **Message Center** > **Alarm Message**.



New alarms are displayed on top.

If an alarm message is unread, a red dot will appear in the upper right corner of the message description.

Filter Alarm Messages

Filter alarm messages by alarm type, alarm status, device serial number, and alarm generation time at the top.

Note: Only alarm messages from the past seven days can be retrieved.

Handle Alarm Messages

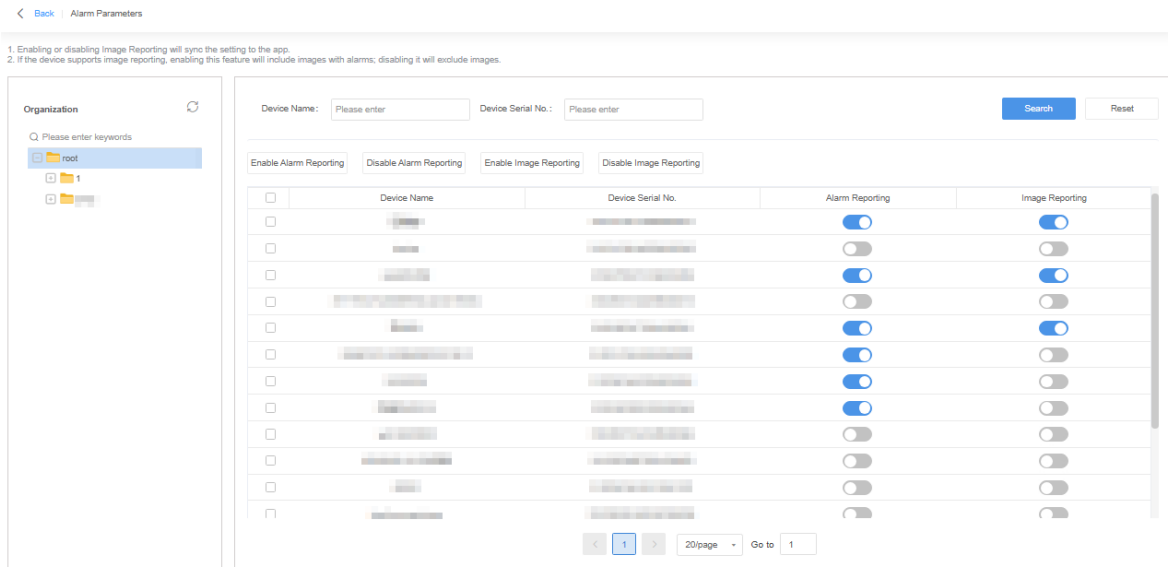
- View live video: Click to go to the corresponding live video screen.
- Playback: Click to view the videos recorded before and after the alarm time.
- View full image: Click the alarm image on the right side of the message to magnify it; zoom and rotate as needed.
- Mark as read: Click **Mark All as Read**at the top of the list to clear all unread messages.

Alarm Configuration

You can enable or disable alarm reporting for multiple devices at a time. Only when alarm reporting is enabled will the platform receive alarm notifications from the device.

If the device supports image reporting: when Image Reporting is enabled, alarms sent by the device will include images. When disabled, alarms will be sent without images.

Note: Enabling or disabling Image Reporting for a device will automatically sync to the account's settings in the mobile app.



4.8 Attendance Management

Attendance management provides an automated and comprehensive solution for tracking attendance of employees and teachers. Companies can install access control devices at entrances and exits and configure attendance schedules according to their policies. When employees sign in and out using face recognition or card swiping, the attendance records are generated automatically. Administrators can view attendance data, handle leaves, and re-sign in/out for abnormal attendance records, ensuring efficient and accurate attendance management.

Configuration Workflow

1. Add access control devices (smart access control device, access controller). SeeDevice Management.
2. Add person information. See Personnel Management.
3. Assign access control permissions to persons. See Access Permission Configuration.
4. Set attendance schedule for persons. See Attendance Config.

5. People sign in/out on access control devices.
6. View attendance records. See Attendance Statistics.

4.8.1 Attendance Config

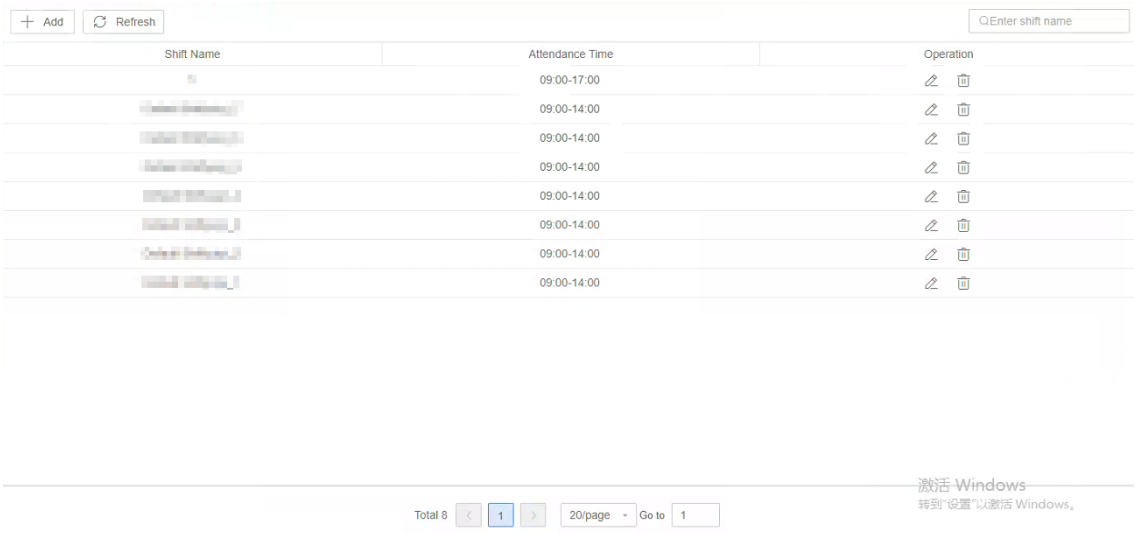
Configuration steps: Shift Configuration→Attendance Group Configuration.

4.8.1.1 Shift Configuration

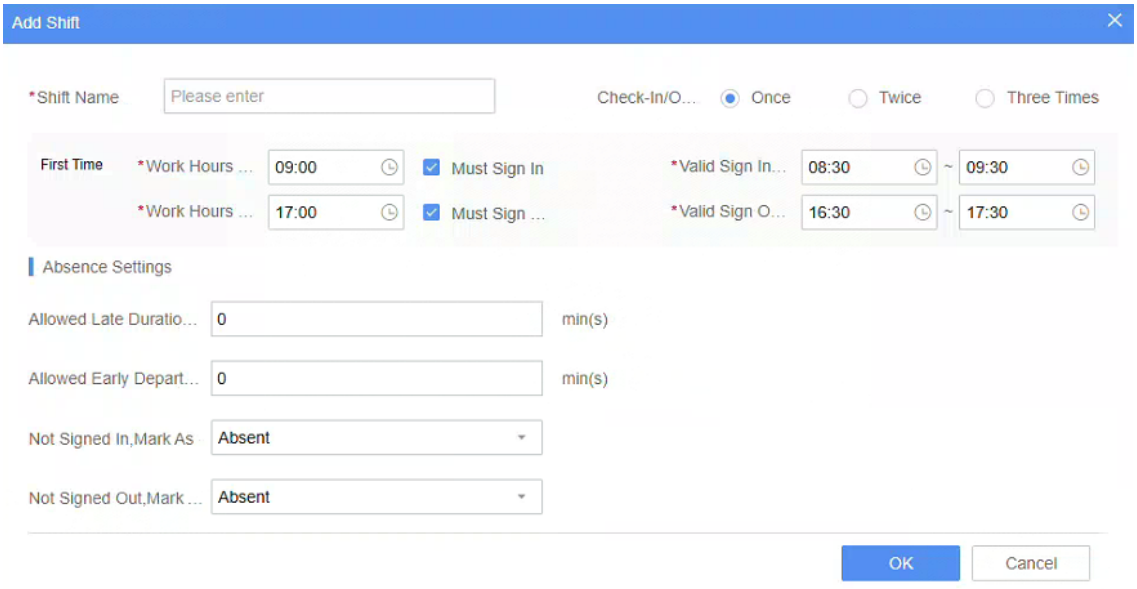
Sets the attendance time periods and absence parameters for a day.

Add Shift

1. Go to **Attendance Application > Attendance Config > Shift Configuration**.



2. Click **Add**.



3. Customize the shift name.
4. Select **Check-In/Out Count**. The default is 1, with a maximum of 3.
5. Configure the work hours start time and work hours end time.
   - Work hours start/end time requirements:
     - The work hours end time cannot be earlier than the corresponding work hours start time.
     - For consecutive periods, the next work hours start time cannot be earlier than the previous work hours end time.

- The span between the first work hours start time and the last work hours end time must not exceed 24 hours.

- Must Check In: Optional. If selected, a valid check-in time **must** be set. Check-ins outside this range are invalid and count as no check-in.
- Must Check Out: Optional. If selected, a valid check-out time must be set. Check-outs outside this range are invalid and count as no check-out.

6. Configure absence parameters. These parameters apply to all check-in/check-out periods in this shift.
   - If **Must Check In** is selected, the following parameters can be set:
     - Allowed Late Duration: If the actual check-in time is later than "Work Hours Start Time + Allowed Late Duration", it is counted as late. Default: 0 minutes.
     - No check-in, record as: Default is **Absent**, with an alternative option of **Late Arrival**.
   - If **Must Check Out** is selected, the following parameters can be set:
     - Allowed Early Departure Duration: If the actual check-out time is earlier than "Work Hours End Time - Allowed Early Departure Duration", it is counted as early departure. Default: 0 minutes.
     - No check-out, record as: Default is **Absent**, with an alternative option of **Early Departure**.
7. Click **OK** to save the settings.

Edit Shift

Click the corresponding to modify parameters. The instructions are the same as Add Shift.

Delete Shift

Note: If the shift is already being used in attendance group configuration, please unbind it before deletion.

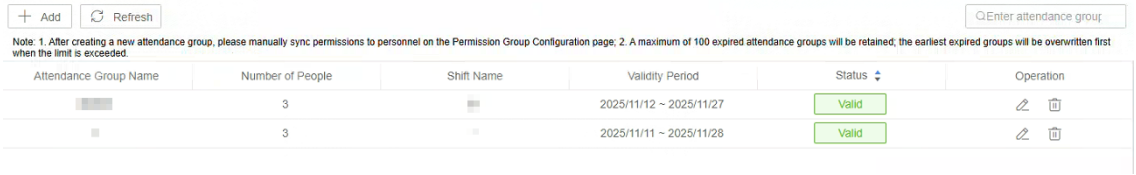
Click the corresponding and confirm the deletion.

4.8.1.2 Attendance Group Configuration

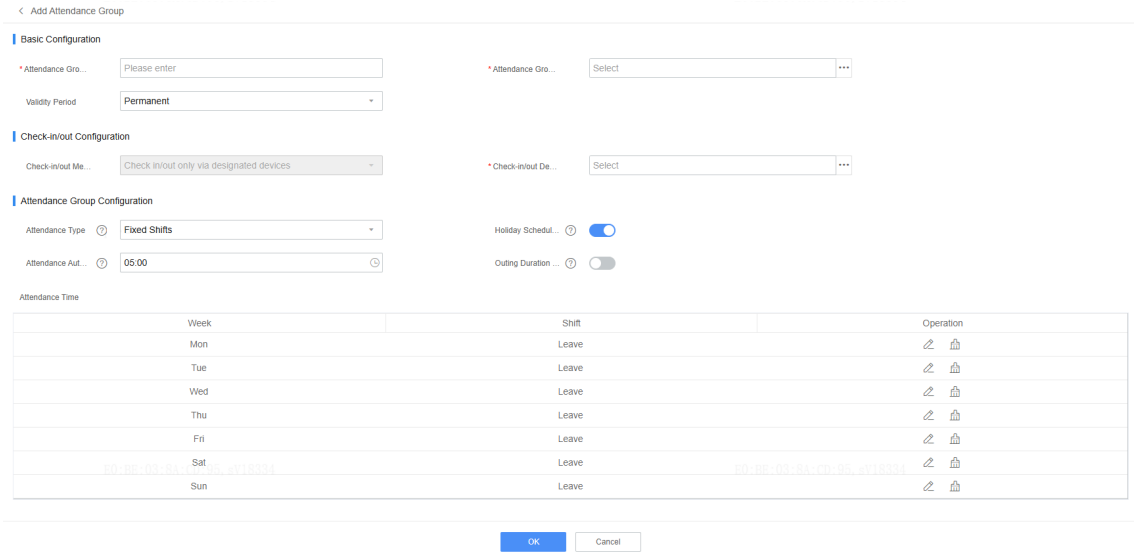
Personnel within the same attendance group use the same check-in/out method each week.

Add Attendance Group

1. Go to **Attendance Application > Attendance Config > Attendance Group Configuration**.



2. Click **Add**.



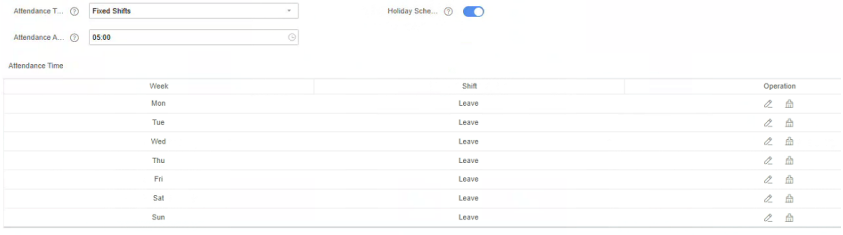
3. Set basic parameters.

Parameter	Description
Attendance Group Name	Customizable.
Attendance Group Members	Members are configured in Personnel Management. **Note:** If the validity period of this attendance group overlaps with that of an existing attendance group, the same person cannot belong to multiple attendance groups simultaneously; otherwise, it is allowed.
Validity Period	Default is permanent. Custom date ranges are supported. Once set, the attendance group is effective only within the specified period.

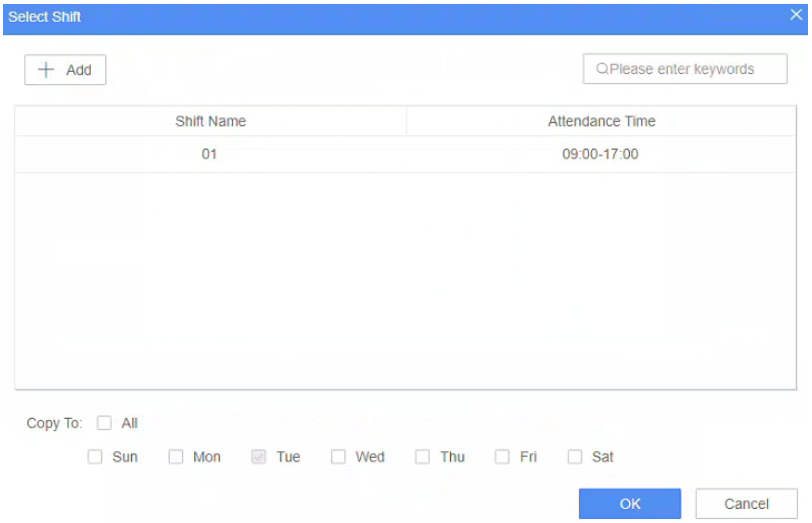
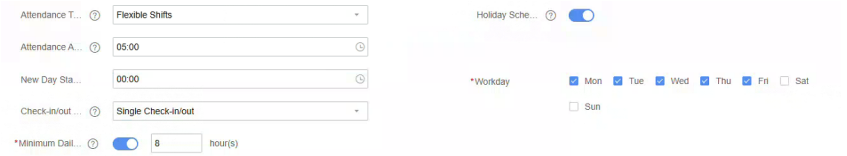
4. Set check-in/out parameters.

Parameter	Description
Check-in/out Method	Default is **Check in/out only via designated devices** and cannot be modified.
Check-in/out Device	Device types include: smart access control device, access controller, which are configured in Device Management. Multiple devices can be selected. Personnel may check in on any one of the selected devices.

5. Set attendance parameters.

Parameter	Description
Holiday Scheduling	Enabled by default. Dates configured in Holiday Management will be excluded from attendance calculation.
Attendance Auto-Calculation Time	Attendance data for the previous day is automatically calculated daily at this time.
Attendance Type	Includes two options: Fixed Shifts and Flexible Shifts. • Fixed Shifts: Default. Work hours are fixed each week. You must configure attendance times for the week, with the requirement that at least one day's shift is not "Leave" 

Parameter	Description

	(1) If the team type is "Guard Team", Outing Duration Statistics must be configured. Disabled by default. Once enabled, the maximum allowed duration for a single outing must be configured. If the outing duration exceeds the set time, one outing will be recorded. The system will then record the number and total duration of outings for members of the attendance group during the attendance period (data can be viewed in **Attendance Statistics > Statistical Report > Outing Statistics**).
	(2) Click .
	 
	(3) Select a shift from the list, or click **Add** to create a new shift (see Add Shift for parameter details).
	(4) (Optional) If the same shift applies to multiple days in the week, you can copy it directly.
	(5) Click **OK**.
	• Flexible Shifts: No fixed work hours; check-in/out can occur at any time. Suitable for roles with flexible scheduling.
	 
	• New Day Start Time: Default is 00:00. Attendance days roll over at this time.
	• Workdays: Days of the week for which attendance is recorded.
	• Check-in/out Mode:
	  • Single check-in/out: Only one round of check-in and check-out per day.
	  • Multiple check-ins/outs: Multiple rounds of check-in and check-out allowed per day. A minimum interval between check-ins/outs must be set. Multiple check-ins/outs within this minimum interval will be counted as a single check-in/out.
	• Minimum Daily Working Hours: If total working time in a day is less than this configured duration, it will be recorded as early departure or absence.

6. Click **OK**.

Edit Attendance Group

Click the corresponding to modify parameters. The instructions are the same as Add Attendance Group.

Delete Attendance Group

Note: Deleting an attendance group may cause today's check-in/out records to become abnormal. Please proceed with caution.

Click the corresponding and confirm the deletion.

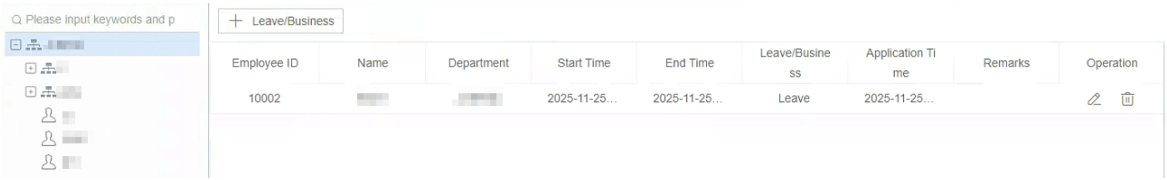
4.8.2 Attendance Management

Administrators can handle leaves and re-sign in&out for personnel.

4.8.2.1 Leave Management

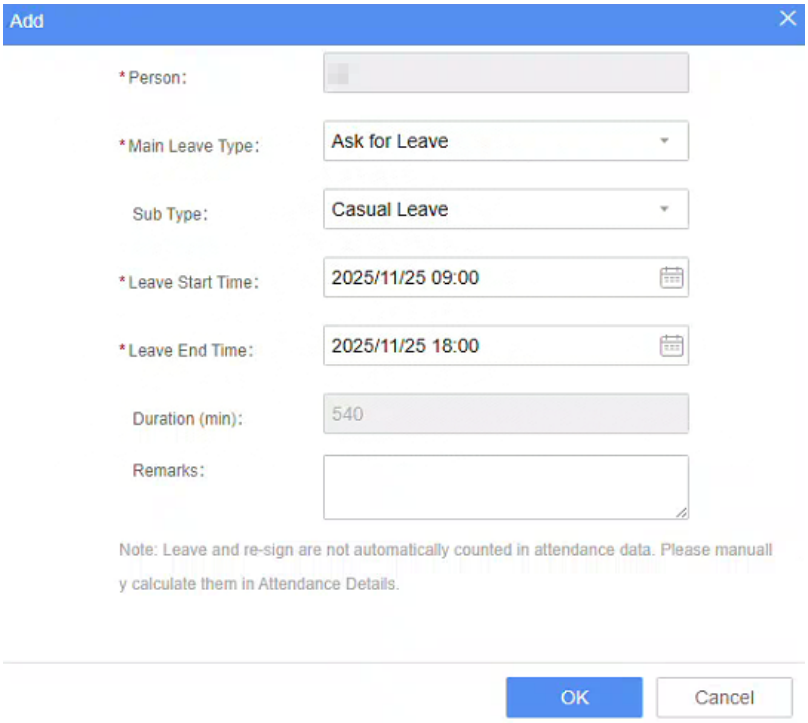
Add leave/business time periods for staff. The recorded durations will not be seen as abnormal attendance. After a new leave/business record is added, you need to click **Calculate** in Attendance Details to update the attendance status and duration.

Go to **Attendance Management** > **Attendance Mgt** > **Leave Mgt**.



Add

1. Select the target person on the left side.
2. Click **Leave/Business**.



3. Select the main leave type (**Ask for Leave**/**Out for Business**). If you select **Ask for Leave**, you need to select the sub type (specific reason for leave).
4. Set the leave start and end times and enter the remarks as needed.
5. Click **OK**.

Edit

Click in the **Operation** column to edit the information such as the leave type and leave start and end time.

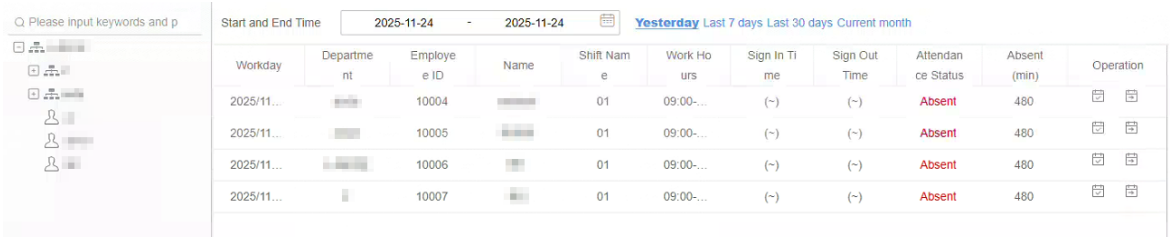
Delete

Click in the **Operation** column and confirm the deletion.

4.8.2.2 Re-Sign In&Out Management

For abnormal attendance records such as absences or late arrivals, you can modify the attendance records by re-signing in or out. After making a re-sign in or out, you need to click **Calculate** in Attendance Details to update the attendance status and absence duration.

Go to **Attendance Management** > **Attendance Mgt** > **Re-Sign In&Out Mgt**.



View

Select the department or person on the left side, and the abnormal attendance records will display on the right.

Filter

Filter data by time.

Re-Sign In

Click in the **Operation** column to modify the sign-in time.

- The re-sign in or out time must be within the effective range. Otherwise, the operation is not effective.
- A person can be re-signed in or out up to 100 times a day. If you need to perform more re-sign operations on this person, you need to clear the person's re-sign records first.
- If there are multiple re-sign records in one day, the earliest and the latest re-sign time within the validity period will be considered as the re-sign time.

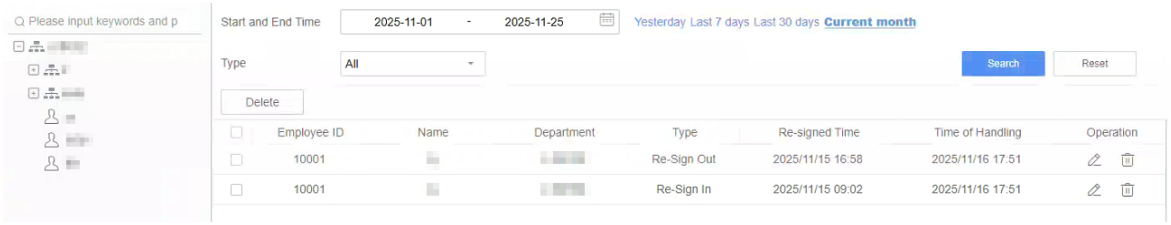
Re-Sign Out

Click in the **Operation** column and modify the sign-out time.

4.8.2.3 Re-Sign In&Out Records

A record is generated each time a sign-in or sign-out time is modified manually. You can search, edit, and delete re-sign records on this page.

Go to **Attendance Management** > **Attendance Mgt** > **Re-Sign In&Out Records**.



View

Select the department or person on the left side, and the re-sign records will display on the right.

Filter

Filter records by time and operation type.

Edit

Click in the **Operation** column to edit the information as needed.

Delete

Click in the **Operation** column or select record(s) and click **Delete** and confirm the deletion.

4.8.3 Attendance Statistics

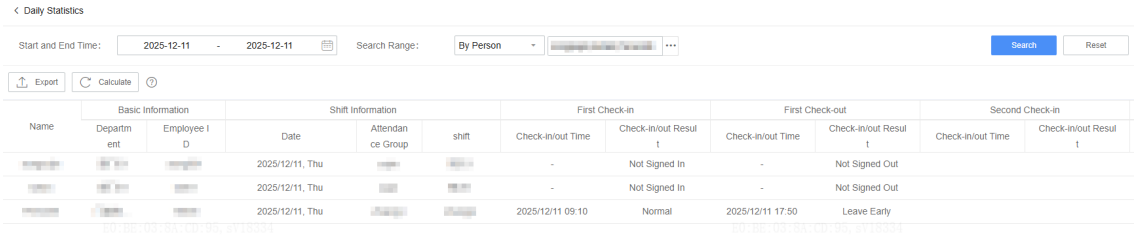
Attendance statistics only include people in the system and do not include strangers.

4.8.3.1 Statistical Report

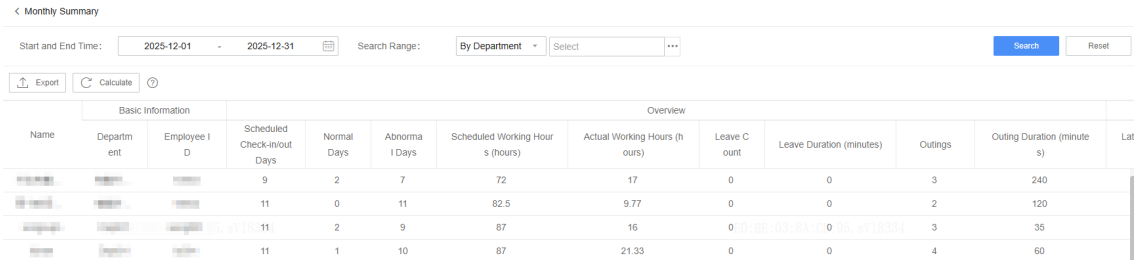
Go to **Attendance Management > Attendance Statistics > Statistical Report**.

Each report type retains attendance data for up to the most recent 12 months. Please export and save data in a timely manner.

- Daily Statistics: Records each employee's daily check-in/out times, results, attendance status, etc.

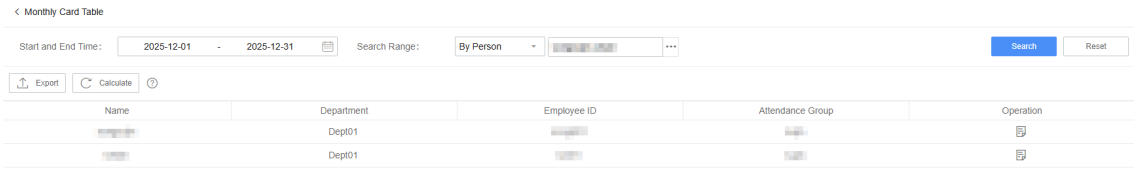


- Monthly Summary: Provides an overview of monthly check-in/out activity, daily results, leave records, etc.



- Monthly Card Table: Logs each employee's monthly check-in/out times, results, attendance status, etc.

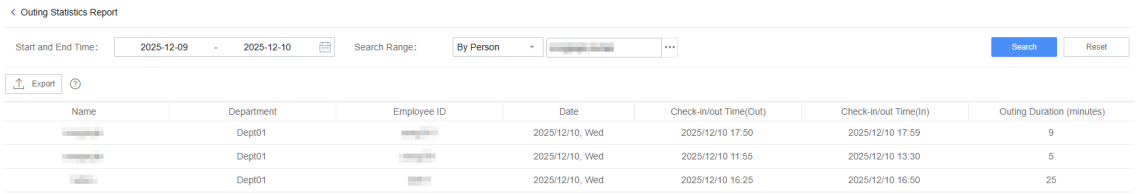
> **Note:** If the amount of data to be exported is too large, it may cause the operation to fail. It is recommended to export a maximum of 300 records at a time



- Outing Statistics: Records the number of times and duration employees leave during attendance tracking periods.

  Outing duration does not include leave time or rest periods between consecutive shifts.

  Outing duration is displayed in full minutes. Any partial minute is not counted.

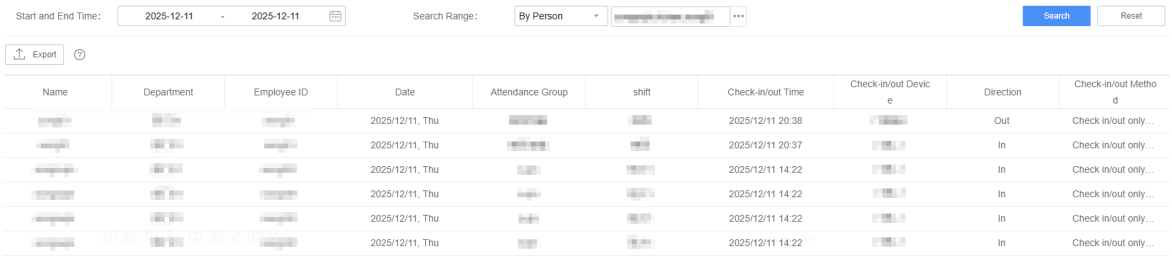


- Search: Supports filtering by check-in/out date range, department/personnel/attendance group.

- Export: Click **Export** to export the currently displayed list contents.
- Calculate Attendance: If automatic attendance calculation fails on a given day or if an employee's shift has changed, click **Calculate Attendance** to reprocess attendance for the listed personnel and regenerate detailed attendance records.
- View Details: Available only for the Monthly Card Table. Click the corresponding to view that employee's detailed attendance record.

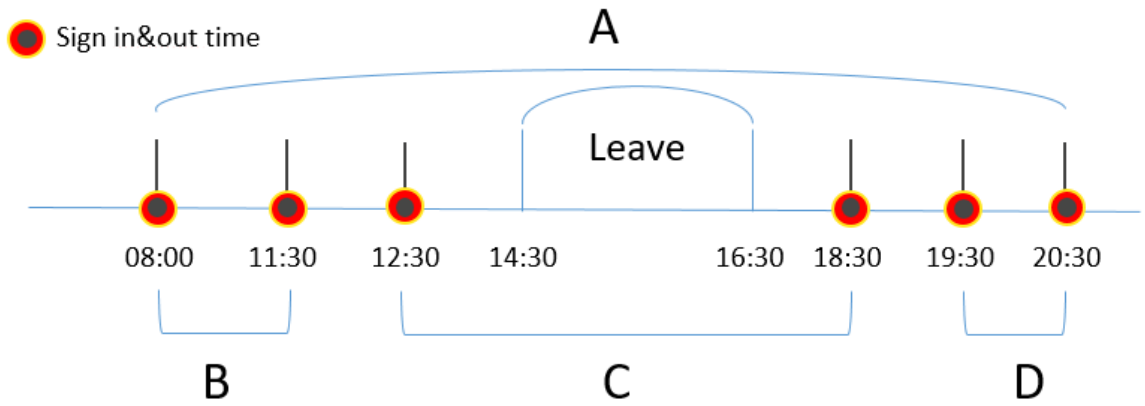
4.8.3.2 Check-in/out Record

Go to **Attendance Management > Attendance Statistics > Check-in/Out Record**.



Attendance data is retained for up to the most recent 12 months. Please export and save your data in a timely manner.

The leave time will not be deducted from the flexible attendance duration. As shown in the figure below, if you select **Calculate by First Sign-in and Last Sign-Out**, the attendance duration is **A**; If you select **Cumulate Duration by Multiple Sign Ins&Outs**, the attendance duration is **B+C+D**. Absence duration = Specified daily attendance duration - Actual attendance duration.



- Search: Supports filtering by check-in/out date range, department/personnel/attendance group.
- Export: Click **Export** to export the currently displayed list contents.

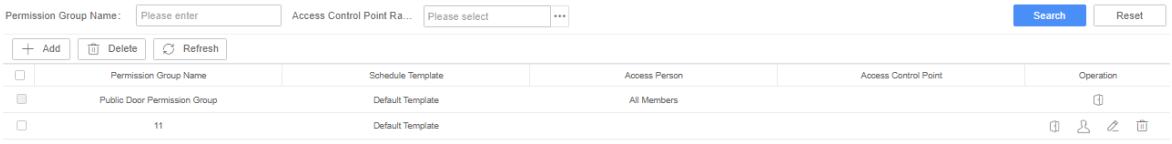
4.9 Access Control Management

4.9.1 Access Permission

4.9.1.1 Access Permission Configuration

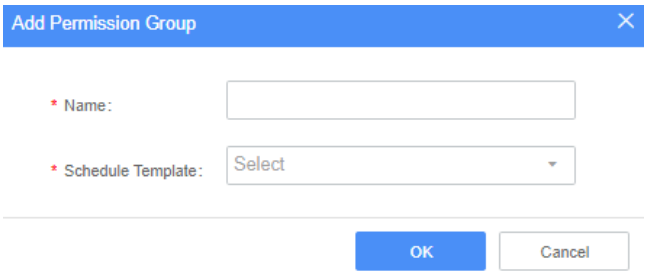
Go to **Access Control Management** > **Access Permission** > **Access Permission Config**.

The public door permission group is open to all persons.



Add permission group

1. Click **Pending**.
2. Enter a custom permission group name and select a schedule template (set in Schedule Template).



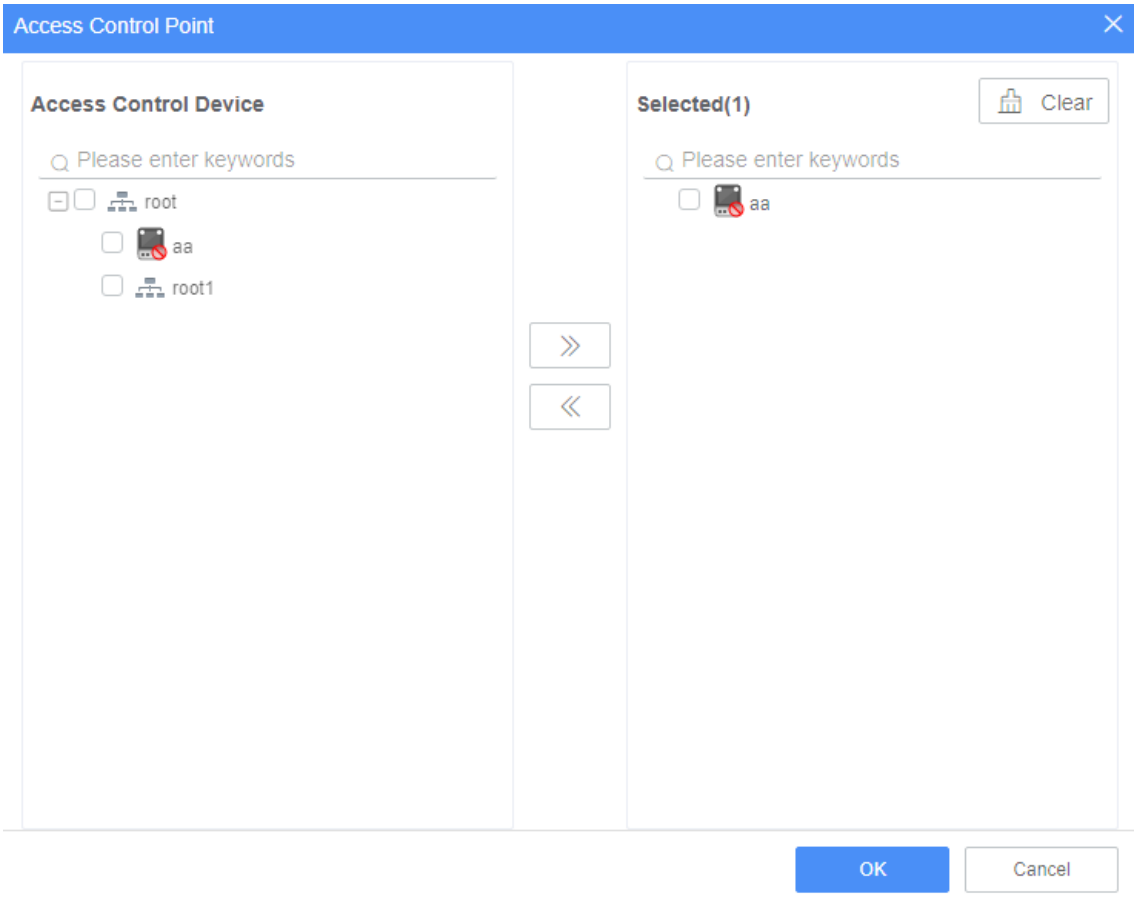
3. Click **OK**.

It is recommended to then follow the on-screen instructions to assign access control devices and persons to the group.

Assign access control device(s)

The selected access control devices will be granted access permission.

1. Click in the **Operation** column.

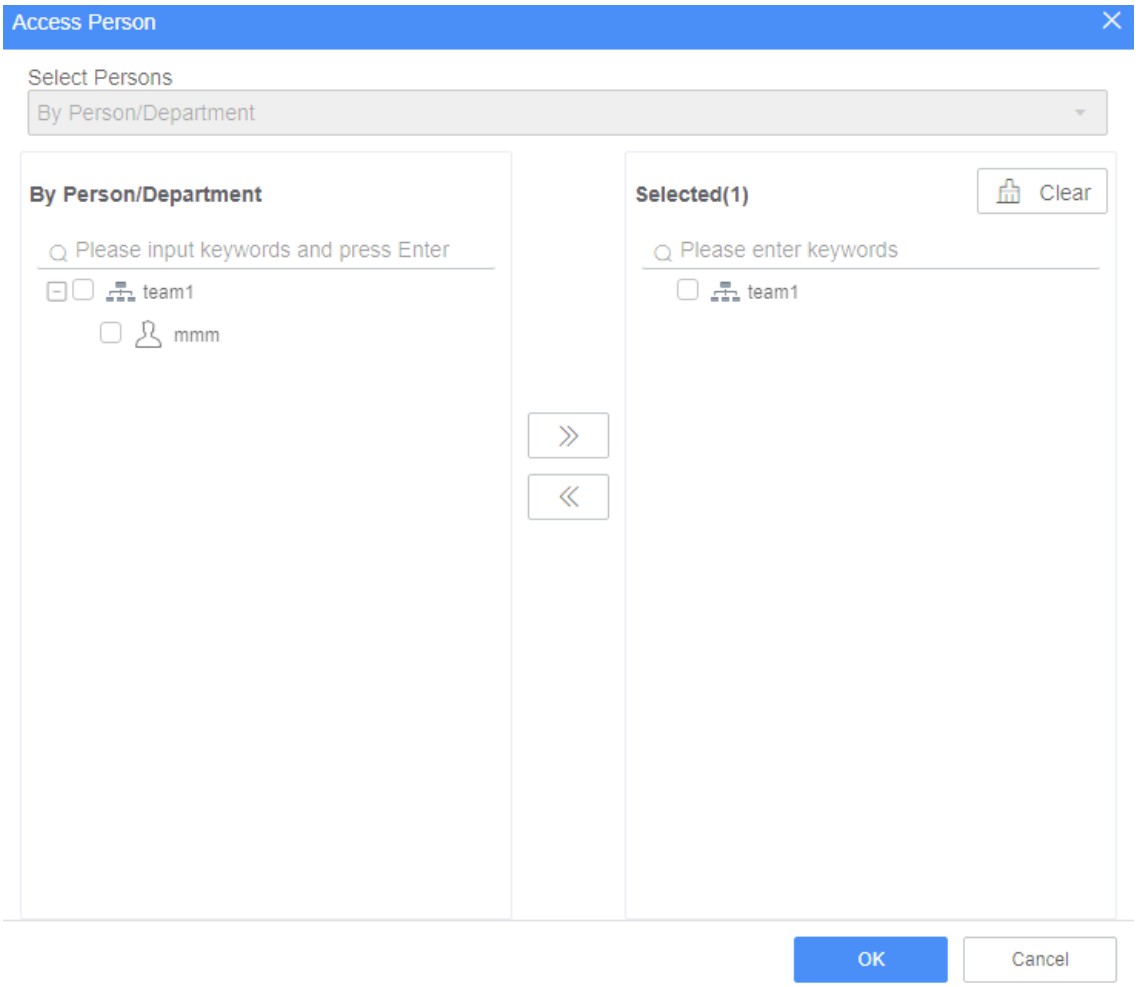


2. Select access control device(s) from the left-side list, and click **>>**.
3. Click **OK**.

Assign person(s)

The selected persons(s) will be automatically granted the access permission for the specified access control devices.

1. Click in the **Operation** column.



2. Select person(s) from the left-side list, and click **>>**.
3. Click **OK**.

Resync

If a schedule template fails to be synced to devices (e.g., after modifying a weekly/holiday schedule already synced to devices, but the updated information fails to be synced), a message will appear at the top of the page: “Schedule template sync partially failed. View Details".

Click **View Details** to display all failure records. Click to resync.

Edit

Click in the **Operation** column to modify the permission group name and the linked schedule template.

Delete

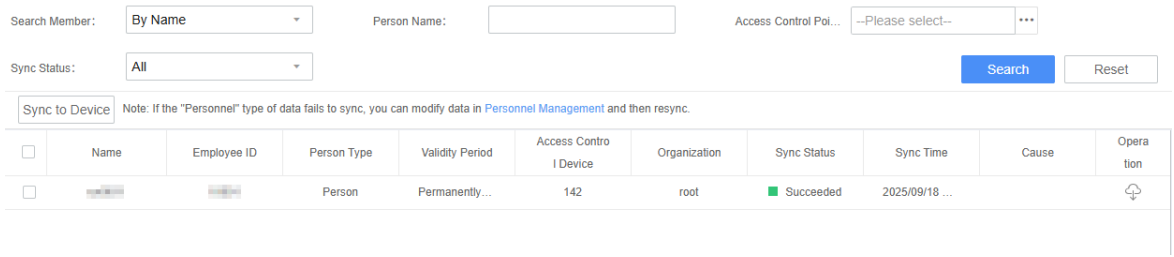
Click in the **Operation** column or select group(s) and click **Delete**, and confirm the deletion.

4.9.1.2 Permission Search

Displays synchronization records of personnel information from the system to device.

Go to **Access Control Management** > **Access Permission** > **Permission Search**.

If the team type is **Guard Team**, then the **Sync Time** column is hidden.



Search

Set person, access control device, and sync status as search criteria as need. and then click **Search**.

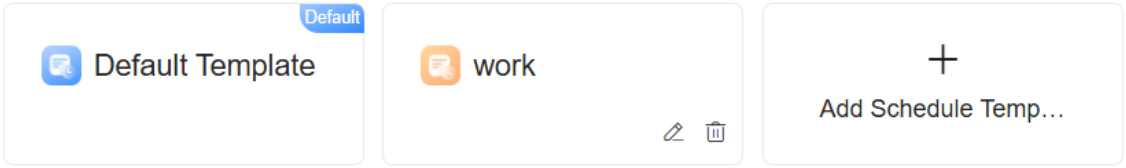
Re-Sync

For failed synchronization of personnel information, you can click in the **Operation** column or select person(s) and click **Sync to Device** to re-sync the personnel information to the device.

4.9.1.3 Schedule Template

Set access time periods using schedule template.

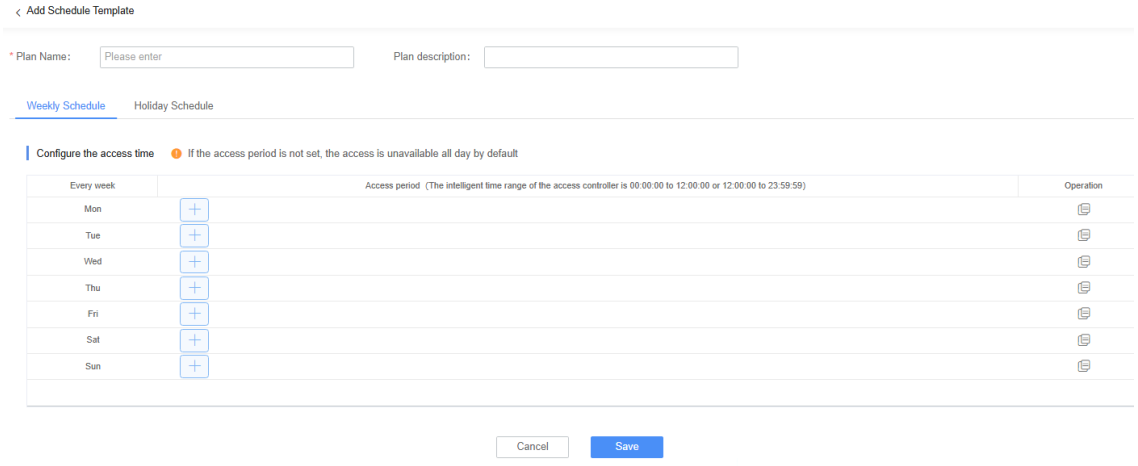
Go to **Access Control Management**> **Access Permission** > **Schedule Template**.



The system includes a default template in the system for all-day access, which cannot be edited or deleted.

Add Schedule Template

1. Click **Add Schedule Template**.



2. Enter a custom template name and enter descriptions as needed.
3. Set the weekly schedule and/or holiday schedule as needed.
   - **Weekly Schedule**: Set fixed access time periods of a week.

     Click **+** to add time period(s). Up to 8 time periods are allowed per day, non-overlapping. If no time periods are set, access is denied for that day.

     You can click in the **Operation** column to copy the configured time settings to other days.

     Note: The access period for access controllers can only be set as 00:00-12:00 or 12:00-23:59.

- Holiday Schedule: Set different access time periods for holidays.

  (1) Select holiday: You can choose the added holidays in Holiday Management or click **Add Holiday** to add a new holiday. Up to 16 holidays are allowed per template. The time periods for each holiday cannot be overlapped.

  Note:

  - Newly added holidays will be automatically synced to Holiday Management.
  - You can click for the holiday to edit the holiday time periods. The modification will also be updated to Holiday Management.

  (2) Click **+** to add time periods for holidays. See other operations in Weekly Schedule.

4. Click **Save**.

Edit

If the template is linked to a permission group, modifications will affect personnel permissions. Please proceed with caution.

Click for the template to modify its details.

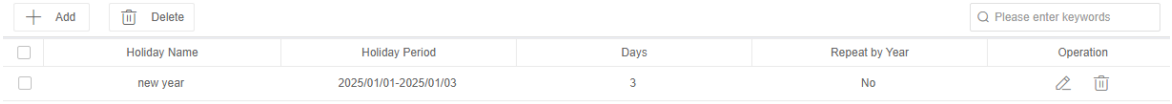
Delete

Cannot delete templates that have been linked to a permission group.

Click for the template and confirm the deletion.

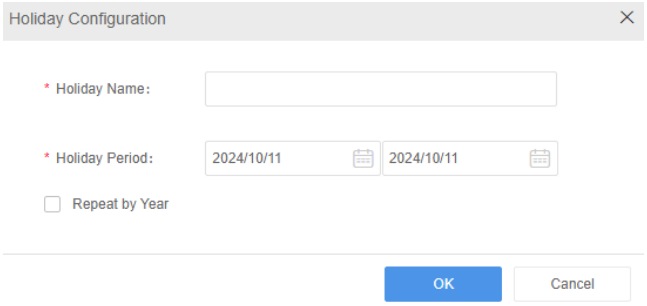
4.9.2 Holiday Management

Go to **Access Control Management**> **Holiday Management**.



Add

1. Click **Add**.



2. Enter a custom holiday name and set the holiday period.
3. (Optional) If **Repeat by Year** is selected, the holiday will repeat every year.
4. Click **OK**.

Edit

Click in the **Operation** column to edit the holiday information.

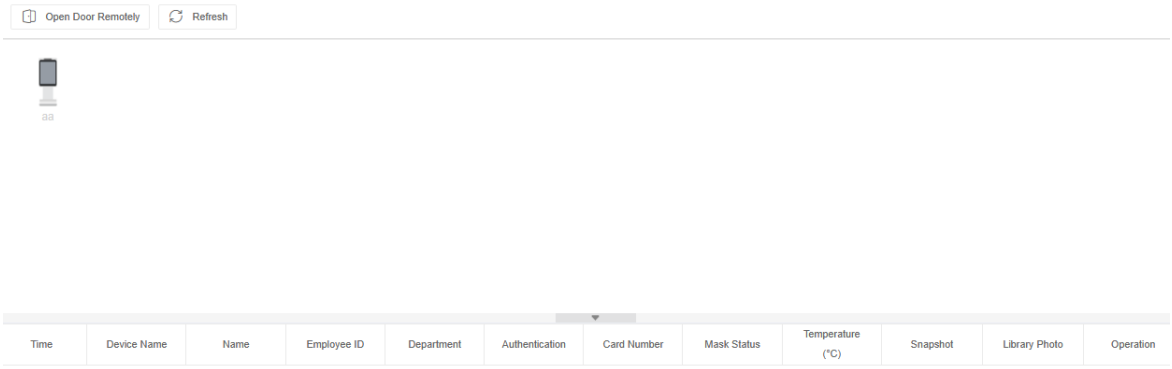
Delete

Click in the **Operation** column or select holiday(s) and click **Delete**, and confirm the deletion.

4.9.3 Real-time Monitoring

You can view pass-thru records of persons remotely control access control devices to open doors.

Go to **Access Control Management** > **Realtime Monitoring**.



Select an organization from the left-side list, the associated access control devices will be displayed on the right.

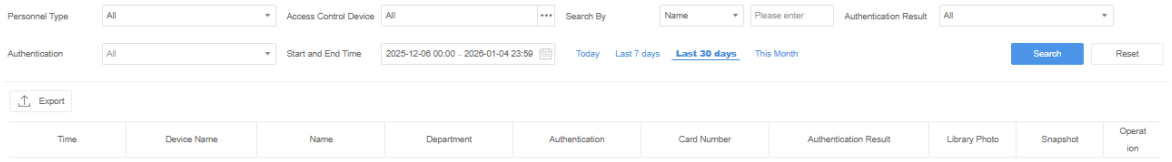
Open door: Select an **Online** device and click **Open Door Remotely** to open the door.

View pass-thru records: Click on a device, and the upper list will display pass-thru records of persons associated with the device, including pass-thru time, device name, person info, etc.

4.9.4 Access Records

Displays pass-thru records of all persons across all devices.

Go to **Access Control Management** > **Access Records**.

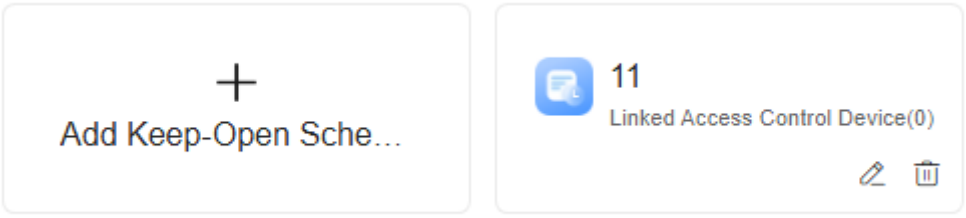


- Export: Select pass-thru record(s) and click **Export**.
- View details: Click to view record details.

4.9.5 Keep-Open Schedule

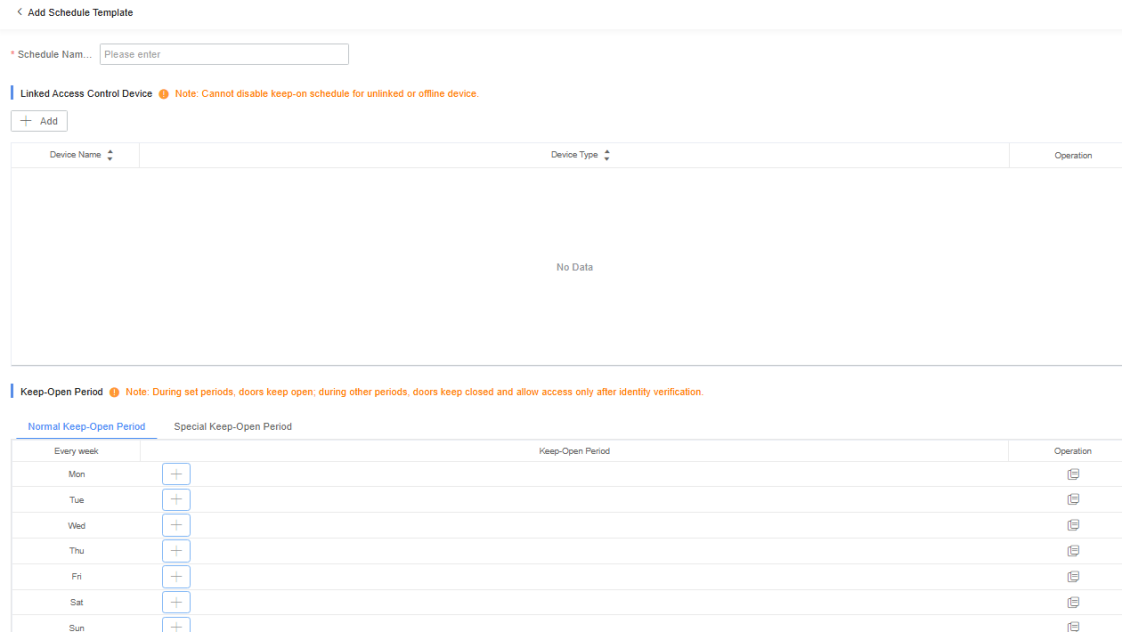
During the set time period, doors will keep open; during other times, doors will keep closed, and individuals will need to be verified before they can pass.

Click **Access Control Management** > **Keep-Open Schedule**.



Add Schedule

1. Click **Add Keep-Open Schedule**.



2. Set the schedule name.
3. Link access control devices to be controlled. Click **Add**, select the access control devices you want to add.
4. Configure keep-open periods, including normal keep-open periods and special keep-open periods.
   - Normal keep-open period: Recurs on weekly basis. You must set keep-open periods for all seven days of the week.
   - Special keep-open period: Specify certain day(s) to use a new keep-open schedule, not the normal keep-open schedule.
5. Click **Save**. The keep-open schedule will be synced to the devices automatically.

Edit Schedule

On the **Keep-Open Schedule** page, click the for the schedule you want to edit. You can change the schedule name, keep-open periods, link/unlink devices, resync data, and enable/disable the keep-open schedule.

- Resync data: If the device status shows "Sync failed", you can click to resync data.
- Unlink device: Unlinking an offline device will not cancel its keep-open schedule. It is recommended to unlink the device when it is online.
- Enable/disable keep-open schedule: By default, a newly added schedule is enabled for the device. It can be disabled manually.

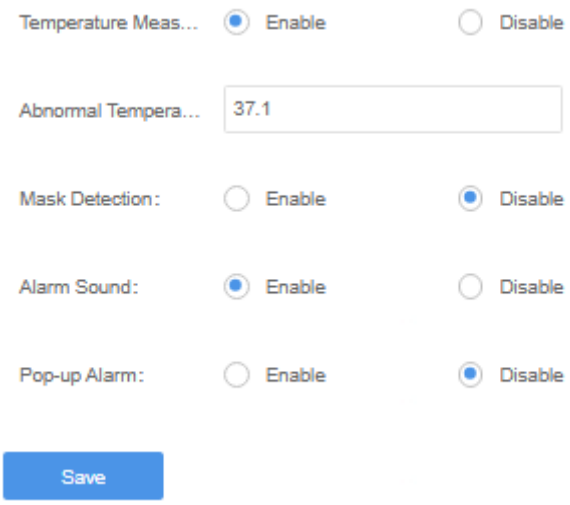
Delete Schedule

On the **Keep-Open Schedule** page, click the for the schedule you want to delete, and then confirm the deletion to complete the operation.

4.9.6 Alarm Parameters

During verification, you can choose whether to perform temperature measurement and mask detection, and whether to enable alarm sounds and pop-up alarm notifications.

Click **Access Control Management** > **Alarm Parameters**.



Item	Description
Temperature Measurement	An alarm will be triggered if the detected temperature exceeds the set threshold.
Mask Detection	An alarm will be triggered if no mask is worn.
Alarm Sound	Enable alarm sounds for abnormal verifications.
Pop-up Alarm	Enable pop-up alarm windows on the interface for abnormal verifications.

4.10 Video Intercom

Video intercom is mainly used in community scenarios, facilitating communication between visitors (via door stations at unit entrance), residents (via indoor stations at home), and security staff (via client in security room or management center). This function provides efficient access control, enhancing the overall security and convenience of the commuity.

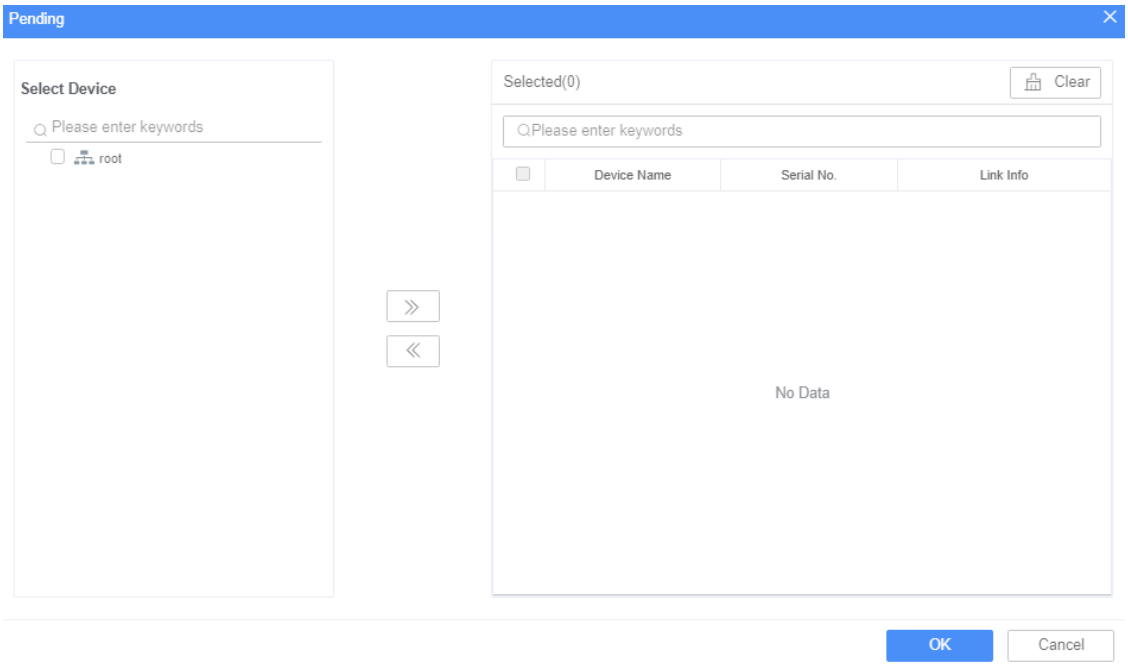
Link door stations and indoor stations with actual installation location (unit/room), so as to match devices with residents and to specify devices used by callers and call recipients.

- To view the added door stations and indoor stations, go to Channel Management.
- To view the detailed location info of the added communities, units, rooms, etc., go to Room Management.

Go to **Video Intercom** > **Video Intercom**.

Add

1. Click **Pending**.



2. Select device(s) to import from the left-side list and click » .
3. Configure the location information for each device in the **Link Info** column on the right side.

   A door station must be linked to a unit, and an indoor station must be linked to a room.

   Each unit can be linked to only one door station, while a room can be linked to multiple indoor stations.
4. Click **OK**.

Edit

Click in the **Operation** column to edit the device's location information.

Delete

Click in the **Operation** column or select device(s) and click **Delete**, and then confirm the deletion.

4.11 Appendix: Adding and Operating Video Intercom Products

Refer to the instructions below to bind video intercom products with the website and assign permissions to enable video intercom service.

1. Configuration on the Device

1. Log in to the device's web interface.
2. Configure call mode.
   - Access control device: Go to **Setup > Intelligent > Advanced Setting**, change **Call Mode** to **Cloud Call V3**, and then click **Save**.
   - Door station: Go to **Setup > Common > Intercom Config**, change **Call Mode** to **Community Cloud Calling**, and then click **Save**.
3. Go to **Setup > Common > Device Info**, change the mode to **Unit Door Station Mode / Zone Station Mode**, click **Save**.

2. Configuration on the Website

1. Open the website (http://www.star4Live.com) and log in. For detailed operations, see Registration and Login.
2. Click **Team Mode** in the upper right corner to switch to this mode.

3. Create Team. The team type must be set to **Community**.
4. Go to **Device Management > Device Management**, and follow instructions to Add Device.

   Note: Ensure the device status shows Online in the list.

5. Go to **Team Management > Room Management > Room Management**. Complete the following configurations in sequence: Configure Room Info (only required for first-time setup), Add Resident.

   After adding residents, visitors can call their room numbers for intercom with the app.

   One room can only have one owner. The same tenant can be added to different rooms.

6. Go to **Access Control > Access Control > Access Permission > Access Permission Config** and complete the following configurations in sequence: Add Permission Group, Add Access Control Devices, Add Persons.

   All persons assigned to a permission group must be added to corresponding rooms. Only then can calls to that room reach the corresponding person.

7. Go to **Video Intercom > Video Intercom** to bind access control devices with the intended units.

3. Video Intercom Operations

1. For residents: Download the Guard Live app and log in using the registered mobile number. Select the team on the home screen to view the bound devices.
2. For visitors: Press the call button on the door station to open the calling screen. Enter the room number and press the call button to initiate a call. The resident's Guard Live app will then display a video intercom invitation pop-up.